HIGH SECURITY CENTER

Guia do Administrador

HSC MailInspector 5.x

Baseado na versão 5.5.1

COPYRIGHT

Copyright © 2018 HSC Brasil. Não copie sem permissão.

INFORMAÇÕES DA LICENÇA

Contrato de Licença

AVISO A TODOS OS USUÁRIOS: LEIA ATENTAMENTE O CONTRATO LEGAL CORRESPONDENTE À LICENÇA QUE VOCÊ COMPROU, QUE ESTABELECE OS TERMOS E CONDIÇÕES GERAIS DE UTILIZAÇÃO DO SOFTWARE LICENCIADO. SE VOCÊ NÃO SABE O TIPO DE LICENÇA ADQUIRIDA, CONSULTE O CANAL DE VENDAS, O CONTRATO LEGAL OU OS DOCUMENTOS DA ORDEM DE COMPRA QUE ACOMPANHAM O PACOTE DE SOFTWARE. SE VOCÊ NÃO CONCORDAR COM TODOS OS TERMOS DO ACORDO, NÃO INSTALE O SOFTWARE. SE FOR O CASO, VOCÊ PODE DEVOLVER O PRODUTO À HSC BRASIL.

Sumário MailInspector

Prefácio 18

Sobre este guia 18

Público-alvo 18

Convenções 18

Encontre a documentação do produto 19

Trabalhando com o seu HSC MailInspector 20

Múltiplas formas de trabalho 25

Segurança 25

Arquitetura Unificada da Solução 27

AntiSPAM 28

Nível de Conexão 28

Nível de Processamento 30

Como o HSC MailInspector processa o tráfego de internet através da sua rede 31

Precisão e qualidade 31

Machine Learning 31

Proteção a ataque com TLD 32

Proteção contra Prompt Injection 32

Anti Spoofing 33

IDN Protection 33

Sistema Generativa (IA) para Análise de E-mails Bloqueados 34

Fácil administração 34

Response-Based Phishing (RBP) 37

Sistema de CDR e SandBox de documentos 37

CDR 37

Sandbox de Documentos 37

Administração Centralizada e Quarentena 38

Custo x benefício 39

Auditoria & DLP 40

Criptografia de E-mail e TLS/SSL 40
Continuidade de Serviço de E-mail 42
Backup e Restore 42
Formas de uso do MLI 43
Como Software 43
Como Appliance Físico 43
Em Virtual Appliance 44
Integração com Sistemas padrão Office (Microsoft, G-Suite e Zimbra) 44
Monitoramento e Alerta 46
Suporte a cluster 47
Cluster em datacenters distintos 49
Múltiplos clusters em datacenters distintos 51
Múltiplos Clusters Unificados 51
Exemplos de Configuração do MailInspector 53
Toda a solução em uma única máquina (virtual ou físico) 53
Solução em cluster com dois pontos de filtragem em DMZ 54
Solução em cluster com dois pontos de filtragem (nodes) 55
Solução em Cluster com duas máquinas completas (físico ou virtual) e quarentena separada 56
Solução com cluster e quarentena separada Administração com logs centralizados 57
Solução com cluster em DMZ com servidor de e-mail na LAN 58
Implementação 59
Integração com outros sistemas 59
Sistemas de Monitoramento 60
HSC MailInspector Archive 61
Message Reputation 62
HSC SmartDefender 63
HSC SmartDefender Local (no ponto de filtragem) 63
HSC SmartDefender Cloud (na nuvem da HSCBRASIL em datacenter no Brasil) 65
Antivírus presentes no MailInspector 67
Retornos da consulta no site de SmartDefender da HSCBRASIL 71

MailInspector e seus módulos em Datacenter brasileiro 73
Certificações dos DataCenters 75
Global "Endpoint Detection and Response" 76
Gartner - Solução de E-mail Gateway 77
Mail Behavior Analysis 78
Global Sender Reputation & Threat Response 78
URL Categorization & Reputation 78
Análise de links apresentados por QRCode 79
Sistema de detecção de arquivos 81
Políticas de segurança individuais e por grupos 81
HSC SandBox 84
Forma Estática de trabalho do SandBox 85
Forma Dinâmica de trabalho do SandBox 85
HSC Targeted Attack Protection 87
Análise de URLs em tempo real 87
Funcionamento da proteção por reescrita de URLs 87
Proteção contra ameaças que surgem após a entrega 87
Análise de anexos e ameaças desconhecidas 88
Proteção em múltiplas etapas 88
Múltiplas Engines de anti-malware (de uso opcional) 88
HSC Outbreak Filter 90
Alinhamento com Boas Práticas de Segurança 90
Framework MITRE ATT&CK 90
Aderência ao padrão Traffic Light Protocol (TLP) 93
Proteção nativa a vulnerabilidade a SMTP Smuggling 94
Proteção a Contas Invadidas - Account TakeOver (ATO) 94
Módulos Adicionais/Opcionais 95
Analisador de DMARC 95
M-SOAR / DeepIntegration / Add-On 95
Risk Management para Microsoft 365 98

AutoWhitelist 102
Algumas RFC's atendidas pelo MailInspector 102
Arquitetura de implantação 103
Fluxo de tráfego de mensagens 104
Integração com sistemas seguros de autorização com MFA (Múltiplo Fator de Autenticação) 104
Acessando o MailInspector 105
Conhecendo a interface administrativa 107
Analisar e/ou modificar regras e configurações 111
O que é importante saber sobre as regras e configurações 111
Aplicar Configuração 113
Trabalhando com expressões regulares 114
Menu - RealTime 116
E-mails 116
Visão geral dos e-mails 116
Dashboards 146
Visão geral dos dashboards 146
Conexões 152
Logs do MTA 152
Fila de E-mails 163
Mail Tracker 169
Controle de Fluxo 173
Greylist 174
Aguardando Liberação 174
Whitelist de E-mails (GreyList) 177
Whitelist de Domínios (GreyList) 179
Status 181
Performance do Sistema 181
Painel de Controle 186
Visão geral Status Painel de Controle 186
Segurança 191

SandBox 191
Ameaças 198
Fraude de E-mail 205
M-SOAR 208
SmartDefender 210
Visão geral do SmartDefender 210
Consultas 212
DMARC 222
Sumário 222
Forense 229
Portal 236
Visão Dashboard 236
Menu - Painel de Controle 240
Block List 240
Visão geral da Block List 240
Allow List 244
Visão geral da Allow List 244
Menu - Gestão de Risco 248
Visão Geral 248
Indicador de risco por usuário 249
Severidade das ameaças 249
Perfil de Risco 250
Inteligência de Ameaças 250
Contas Prioritárias 251
Cadastro manual 252
Importação do diretório 252
Importação e exportação em arquivo 253
Ações em lote 253
Menu - Relatórios 254
Relatórios Gerenciais 254

Visão geral dos relatórios gerenciais 254
Exemplo de Relatórios 264
Resumo Executivo 266
Análise Geral 267
Domínios 267
Eficácia 268
Ameaças Neutralizadas 269
Fontes de Ataque 270
Alvos e Risco 271
Tendência 272
Histórico 273
IA Insights 273
Log de Eventos 275
Visão geral do log de eventos 275
Agendados 279
Visão geral Agendados 279
Capacity Planning 281
Visão Capacity Planning 281
Menu - Configurações 283
Cadastros 283
Grupos Usuários 283
Anexos 288
Mime-Types/Fingerprint 290
Dicionário de Palavras 291
RBLs Externas 294
Controle de Conexão 296
Configurações do MTA 296
POP3/IMAP Protection 315
Mail Split 316
TLS/SSL 317

Controle de Bounce 325
SPAM Throttling 327
Quota/Controle de Fluxo 329
Relay Autenticado 332
Reescrita de E-mails 334
Outbreak Filter 336
Reputação 338
Filas Personalizadas 340
Quarentena 343
Segurança de Quarentena 343
Configurações 343
Customizada 352
Filtros de Conteúdo 355
Configurações Gerais 355
Controle de Anexos 361
Compactação de Anexos 372
Controle de Ameaças 375
Antivírus 375
AntiPhishing 384
CDR (Content Disarm and Reconstruction) 387
Reputação 393
Ataque Dirigido 398
Filtros de SPAM 412
Configurações Gerais 412
Machine Learning 418
Identificação de Idiomas 420
Pontuação 422
Ações 424
Controle Avançado 429
Anti Spoofing 437

Configurações Gerais 437
Sender ID 440
SPF 441
DKIM / Domain Key 445
DMARC 448
Notificações 455
Configurações Gerais 455
Padronização 459
Modificação do Assunto 465
E-mail Compliance 469
Gerenciar Fingerprint 469
Regras de Compliance 471
M-SOAR / Deep Integration 481
Office 365 481
G-Suite 483
Zimbra 485
HSC Extended Mailbox Integration 487
Integração POP e IMAP para Gerenciamento de Quarentenas 487
Sincronização Bidirecional de Agendas 488
Continuidade de Acesso 489
Menu - Administração 491
Ponto de Acesso 491
Visão geral do ponto de acesso 491
Configurações de Rede 498
Visão geral de Configurações de Rede 498
Usuários do Sistema 500
Visão geral dos usuários do sistema 500
Política de senhas 508
Administrador Customizado 510
Permissões dos Perfis de Usuários do Sistema 514

Conectores Externos 517
Visão geral do cadastro de servidores LDAP 517
Configuração do Cluster 526
Visão geral da configuração do ambiente de cluster 526
Notificação de Quarentena 529
Visão geral da Notificação de Quarentena 529
Ferramentas 545
Central de Atualizações 545
Backup 549
Restore 552
Banco de Dados 553
Diagnóstico 556
Suporte 561
Tunning 562
Certificado SSL 564
Restrição de Acesso 567
Branding 569
Integrações 570
Visão geral de Integração com Zimbra 570
Visão geral de Integração com Microsoft 365 (Office 365) 573
Visão geral de Integração com Crowd Strike 590
Visão geral de Integração com Google Workspace 591
Visão geral de Integração com Serviços Externos STIX/TAXII 593
Post-delivery Action 595
Configurações Gerais 596
Ações por IOC 597
Fontes de Consulta 598
Performance e Concorrência 598
Exceções de Reanálise 599
Notificações 600

Execução em modo Análise 601
Administração por Linha de Comando 602
Comandos via SSH (Secure Shell) 602
Configurações 602
Alterar configurações de rede 602
Alterar configurações DATA/HORA 602
Serviços 602
Ferramentas 603
PING 603
TRACEROUTE 603
DIG 603
Status 603
Uso de Memória 603
Uso CPU 603
Uso Disco 604
Estatísticas de Rede 604
Rastrear E-mail 604
Forçar Reenvio da Fila de E-mails 604
Reiniciar/Desligar 604
Reiniciar 604
Desligar 604
Acesso ao Terminal 604
Estrutura de Diretório da Console de Administração 605
Arquivos de LOG dos agentes e Console de Administração 606
MIBS de Controles 607
MIBS de Hardware 608
Scripts e Comandos 611
Scripts de Automatização de Serviços - Agentes 612
Monitoramento de filas com Zabbix (através dos parâmetros do usuário) 613
Alguns comandos úteis para o MailInspector 616

Lista de Comandos Individuais 620
Alterar Senha de Acesso 621
Sair 621
Acessando MLI pelo menu de configuração no SSH 622
Requisitos Mínimos de Hardware 626
Requisitos Mínimos para Pontos de Acesso 626
Requisitos Mínimos para Interface de Administração 627
Processo de Instalação em VM's 628
Premissas na instalação 628
Liberação de portas necessárias para o bom funcionamento da solução 628
Comunicação entre Agentes de Filtragem ao Servidor de e-mail e Servidores de E-mail ao Cluster 629
Liberação de IP's e portas de comunicação 630
Instalação 635
API de integração com outras aplicações 649
Autenticação 651
Requisições 653
Lista de rotas 654
Login da API 656
Pontos de Acesso 656
E-mails 657
M-SOAR 662
Remover Anexos 662
Remover Links 662
Mover para Lixo Eletrônico 663
Bloquear Conteúdo 664
Apagar Permanentemente 664
Modo Rewrite 665
Integração com outros produtos da HSCBRASIL 667
MindAware 667
Apêndice 1 - Glossário 668

Apêndice 2 - RFC's Suportadas 697
RFC's de SMTP 697
RFC's de IMAP 698
RFC's de POP3 698
RFC's IDN (Internationalized Domain Names) 698
Outros RFC's 699
Apêndice 3 – Expressões Regulares 700
Expressão regular para casar com a frase "TESTE hscbrasil" 700
Expressão regular para detecção de qualquer palavra ou frase em lista 701
Expressão regular que corresponde à palavra com variantes. 702
Expressão Regular para Corresponder a e-mail de um domínio específico 703
Expressão Regular para Corresponder início de uma URL 704
Expressão Regular para Corresponder ao meio de um e-mail 705
Expressão regular para detecção de extensões de arquivos 706
Expressão Regular para Corresponder a qualquer endereço IP em um intervalo 707
Outras expressões regulares úteis 709
Expressão Regular para block list/allow list casando com subdomínios 713
Expressão Regular para detectar repetição de mesmo caractere em e-mail 716
Estrutura de Data e hora 718
Dicionário de Palavrões – Evitando que palavra seja detectada no meio de outras palavras 720
Metacaracteres do RegEx 722
Apêndice 4 – DLP 726
Modelos de DLP 726
Exemplo de DLP – Cartão de Crédito 726
Apêndice 5 – FAQ's e HowTo's 735
Adicionando subdomínios 735
Criptografando e-mails quando começa com o assunto [CRIPTOGRAFADO] 737
ByPass total no MailInspector 742
Aumento de pontuação de SPAM em Imagens diretamente por assinatura 745
Bloqueio de SPAM em Imagens diretamente por assinatura 748

Bloqueio de E-mails pelo módulo E-mail Compliance 751

Bloqueio de E-mails Vazios 754

Colocar e-mail em uma quarentena específica 758

Modificando a pontuação de e-mail devido a reputação de origem do IP 761

Saída de e-mail por IP específico 764

Criando contador de número de destinatários de um e-mail 767

Redirecionamento de e-mails para outro servidor de e-mail (que não é o padrão de entrega para o mesmo domínio) em regra de DLP 769

Exceção para Arquivos Compactados com Senha 773

Remoção de Anexos 779

Remoção de Anexo Cifrado, mas sem Compactação 791

Proteção de Display Names (Usuários VIPs) Verificação no FROM do Header 795

Aumentando segurança com detecção de phishing por FakeBounce (Boas Práticas) 802

Regra para contar número de remetentes 807

Aumentar a pontuação dos e-mails que possuem palavras de conotação de BitCoin no corpo 810

Proteção a VIP (Very Important Person) e Look-aLike Domains 815

Configuração de uso com proteção a VIP (Very Important Person) 815

Configuração de uso com proteção a Look-alike Domains/Cousin Domains 824

Ativação de Sincronismo com Azure e do M-SOAR para Office 365 832

Ativação de Add-On do MLI no Office 365 840

Bloqueio de e-mails com liberação pelo supervisor de e-mails 847

Regras com base nos Cabeçalhos de TO do Header ou TO do Envelope e ambos 851

Apêndice 6 - Integração do MailInspector com Microsoft Office365 sem alteração no apontamento MX/DNS 860

Entrada de E-mails Office365 sem alteração de MX 860

Configuração de conexão com Office365 via API 861

Configuração Entrada de E-mails para Office365 Inline (sem alteração de MX) 866

Configuração Saída de E-mails para Office365 Inline 870

Comunicação segura entre MailInspector e Microsoft 365 / G-Suite 872

Configuração de Orquestração (M-SOAR) 874

Ativação de Add-On do MLI no Office 365 877

Apêndice 7 - Integração do MailInspector com G-Suite sem alteração no apontamento MX/DNS 885
Entrada de E-mails G-Suite sem alteração de MX 885
Configuração de conexão com G-Suite via API e configuração de M-SOAR 886
Configuração Entrada e Saída de E-mails para G-Suite Inline (sem alteração de MX) 892
Comunicação segura entre MailInspector e Microsoft 365 / G-Suite 904
Apêndice 8 – Assinaturas 906
Principais assinaturas do MailInspector 909
Apêndice 9 – Notas de Versão 933
Release 5.4.2-3 (01/06/2026) 933
Release 5.4.1 (08/05/2026) 933
Release 5.4 934
Release 5.3.3 (17/11/2025) 935
Release 5.3.2 (04/09/2025) 936
Release 5.3.1 (17/07/2025) 937
Release 5.2.20-5 (16/11/2024) 938
Release 5.2.20-3 (30/10/2024) 940
Release 5.2.20 (08/07/2024) 940
Release 5.2.19 (18/04/2024) 940
Release 5.2.18 (11/01/2024) 940
Release 5.2.17 (24/10/2023) 941
Release 5.2.16 (15/08/2023) 942
Release 5.2.13-1 (27/03/2023) 943
Release 5.2.12-1 (27/01/2023) 944
Release 5.2.11-1 (07/11/2022) 944
Release 5.2.10-1 (18/08/2022) 944
Release 5.2.7-1 (05/04/2022) 944
Release 5.2.6-2 (27/01/2021) 945
Release 5.2.6-1 (07/12/2021) 945
Release 5.2.0-18 (27/08/2020) 945
Release 5.2.0-10 (22/06/2020) 948

Release 5.1.9-1 (23/12/2020) 949
Release 5.1.8-1 (11/12/2020) 949
Release 5.1.16 (24/11/2020) 950
Release 5.1 (15/10/2020) 950
Release 5.0.30-7 (29/07/2020) 952
Release 5.0.30-6 (08/07/2020) 952
Release 5.0.30-5 (24/06/2020) 953
Release 5.0.30-4 (21/06/2020) 953
Release 5.0.30-3 (06/05/2020) 953
Release 5.0.30-1 (23/03/2020) 953
Release 5.0.27-4 (09/12/2019) 954
Release 5.0.26-1 (13/11/2019) 955
Release 5.0.25-3 (01/11/2019) 955
Release 5.0.24-1 (29/10/2019) 955
Release 5.0.23-1 (16/10/2019) 956
Release 5.0.22-1 (14/10/2019) 956
Release 5.0.21-2 (14/10/2019) 956
Release 5.0.20-1 (09/10/2019) 956
Release 5.0.19-1 (08/10/2019) 956
Release 5.0.18-1 (07/10/2019) 956
Release 5.0.17-1 (24/09/2019) 956
Release 5 956

Prefácio

Sobre este guia

Este item descreve o público-alvo, as convenções tipográficas, os ícones utilizados e como o guia está organizado.

Público-alvo

A documentação da HSC Brasil foi cuidadosamente pesquisada e escrita para o seu público-alvo.
As informações contidas neste guia são destinadas principalmente para:

- Administradores - Pessoas responsáveis por implementar e fazer cumprir as políticas de segurança da empresa.

Convenções

Este guia utiliza as seguintes convenções tipográficas e ícones.

Título de livro ou Ênfase	Título de livro, capítulo ou tópico; introdução de um novo termo; ênfase.
Negrito	Texto fortemente enfatizado.
Entrada do usuário ou caminho	Comando ou outros textos que devem ser digitados pelo usuário, ou caminho de um diretório ou programa.
Código	Um exemplo de código.
Interface do usuário	Palavras utilizadas na interface do usuário, incluindo opções, menus, botões e caixas de diálogo.
Hipertexto azul	Um link para um tópico ou para um site.
	Nota: Informações adicionais, como um método alternativo de acessar uma opção.
	Dica: Sugestões e recomendações.
	Importante: Conselhos para proteger o sistema, para instalação do software, para rede, para os negócios ou para manutenção dos seus dados.
	Atenção: Dicas essenciais para evitar danos físicos ao manipular o hardware do produto.
	Informa as limitações das licenças Standard e Free (para no caso de estarem com estes produtos instalados).

Encontre a documentação do produto

A HSCBRASIL fornece todas as informações necessárias para cada fase de implementação e uso do produto, da instalação à solução de problemas.

Manuais oficiais que acompanham o MailInspector, disponibilizados pela HSCBRASIL:

- Manual do administrador em português do Brasil;
- Manual do usuário final (Manual de uso da notificação de quarentena e do painel da ferramenta para o usuário) em português do Brasil;
- Materiais como:
    - Guias de ativação de módulos;
    - Orientação em Configurações;
    - Comunicado de atualizações;
    - Avisos disparados pela HSCBRASIL;
    - News letters;
    - FAQ's;
    - HowTo's;
    - Bases de conhecimento;
    - Bases de soluções;
    - Entre outros

  São todos fornecidos em língua portuguesa (português do Brasil)
- Caso precise de outros materiais, além dos manuais (outras documentações, tais como HowTo`s, folders, guias, etc), devem ser solicitados para HSCBRASIL

Depois que uma nova versão/release do produto for lançada, as informações sobre o produto podem ser encontradas no site da HSC Brasil e no fórum de suporte.

Trabalhando com o seu HSC MailInspector

O HSC MailInspector® é um Gateway de E-mails "MTA" next generation com protocolos SMTP/SMTPS e POP3, que foi desenvolvido para prover segurança e performance no fluxo de entrada e saída de e-mails de sua empresa, oferecendo proteção em tempo real através da utilização de mais de 40 camadas de filtragem, protegendo os e-mails nas mais diversas camadas e efetuando o registro dos logs das atividades do MTA.

O sistema MailInspector foi projetado respeitando a legislação brasileira (mais especificamente LGPD – Lei Geral de Proteção de Dados - nº 13.709/2018) em toda a sua plenitude.

O MailInspector oferece múltiplas camadas de proteção, tais como:

- SPAM;
- SPAM em Imagem;
- Phishing, Spear Phishing, Clone Phishing;
- BEC (Business E-mail Compromise)/Fraude de E-mail;
- Detecção de newsletters/Informativos/fóruns;
- Malwares (vírus, worms, ransomwares, trojans, spywares, etc);
    - Links maliciosos em imagens;
    - APT;
    - Zero-Day/Zero-Hour;
- Análise avançado nos anexos, inclusive a nível de SandBox;
- Remoção de código programável (CDR) e análise de anexos do tipo documentos;
- Proteção a sistemas de coleta de usuário e senha sobre o próprio MailInspector;
- Proteção a Bulk Mail/Mail Marketing, com detecção através de análise heurística e por reputação da origem do e-mail;
- Proteção a GrayMail;
- Proteção a Mail Bomb;
- Proteção a ataques do tipo DoS/DDoS, a nível de sistema operacional e a nível de MTA (conexão);
- Controle (limite de tráfego) a nível de conexão (MTA), utilizando múltiplos campos de filtragem, tais como:
    - Domínio/subdomínio, nome parcial do domínio;
    - Endereço de IP/Rede (Subnet)/Range de IP/Classe de IP;
    - Reputação da Origem. Entende-se como reputação análise de vários fatores sobre o IP de origem, bem como o e-mail em si. Segue alguns modelos de verificação de reputação:
        - Lista de IP’s identificados como propagadores de ransomware;
        - Lista de IP’s de fontes de SPAM;
        - Lista de IP’s de fontes de Phishing;
        - Listas de IP’s de propagadores de malware;
        - Lista de IP’s de sistemas de formulários utilizados para coleta de senhas;
        - Listas de IP’s de sites contaminados;
        - Listas de IP’s utilizados em BOTs;
        - Listas de IP’s utilizados em campanhas criminosas (diversas fontes de ataque);
        - Conformidade de padrões legais;
        - Em caso de envio de e-mail marketing, se o mesmo utiliza regulamentação para prática de E-mail Marketing (CAPEM) ou CAN-SPAM padrão Estados Unidos;
        - País de origem do e-mail;
        - Diversas outras listas de IP utilizados de forma indevida;

Importante salientar que as listas são atualizadas dinamicamente, ou seja, um IP que estiver na lista pode em qualquer momento sair dela e vice-versa.

- Proteção a e-mails adultos, com detecção por análise heurística do e-mail, bem como por reputação da origem do e-mail (Origem de Conteúdo Adulto);
- Detecção de imagens pornográficas;
- Uso de Inteligência Artificial e sistema de Machine Learning para análise contextual e detecção de ameaças;
- Proteção a links contaminados, inclusive em links encurtados ou oculto em HTML, verificando se é link de download, link para formulário com senha, qual a categoria da URL, etc;
- Proteção a phishing HTTPS;
- Proteção a e-mails de origem com má reputação;
- Proteção a adulteração de cabeçalho do e-mail (análise SMTP MAIL FROM em relação SMTP ENVELOPE FROM);
- Proteção a Spoofing de e-mail de entrada (fingindo ser do próprio domínio);
- Proteção a Spoofing de e-mail de saída (quando manda e-mails de saída não pertencentes aos domínios protegidos pelo MailInspector);
- Proteção a e-mails vindos de domínios recentemente adquiridos;
- Proteção a ataques com formulários que solicitam preenchimento de senha e/ou informações de servidor de e-mail;
- Proteção a ataques do tipo Indirect Prompt Injection, ao qual são inseridos códigos “invisíveis” no e-mail;
- Proteção a ataque de dicionário/DHAP, verificando a real existência do e-mail de destino e anulando ataques do tipo Harvest Directory;
- Proteção a e-mails oriundos de domínios inexistentes e/ou não resolvidos no reverso do DNS (reverse DNS LookUp - rDNS);
- Todas as proteções acima indicadas são baseadas em mais de 60 idiomas diferentes, dentre eles as mais comuns (Português do Brasil, Inglês, Espanhol, Alemão, Italiano, Francês);
- Detecção automática de look-alike domain. O MailInspector já possui diversos look-alike domains cadastrados, entre eles:
    - Principais Bancos;
    - Principais lojas virtuais;
    - Dicionário de look-alike;
- Proteção a aquisição indevida de contas, também conhecida como Account TakeOver, através de controle de fluxo e e-mail reputation, associado a bloqueio de usuário no AD/Azure direto pelo MailInspector, fazendo a ação de Takedown da conta comprometida (maiores informações em *Proteção a Contas Invadidas - Account TakeOver (ATO)*);
- Proteção a Display Name e VIP/Whaling, onde é possível utilizar duas técnicas distintas para proteção a falsos Display Names, protegendo usuários críticos na empresa, tais como CEO, CFO, diretores, etc;

O MailInspector não possui uma limitação de suporte a número máximo de caixas postais na solução, nem de processamento de mensagens por hora ou dia, uma vez que o seu crescimento é escalonável, bastando incluir mais um ponto de filtragem (ponto de acesso) à solução, dessa forma aumentando exponencialmente a capacidade de processamento e filtragem dos e-mails.

Este produto utiliza as mais avançadas tecnologias contra spams, e-mail marketing, e-mails não solicitados, malwares, riskwares, spywares, phishing, trojans, worms, ransomwares, vírus e outras ameaças e ataques

existentes no mercado, para impedir e/ou controlar a entrada e saída de e-mails não autorizados ou nocivos à sua organização.

A solução permite o uso de alias de e-mails, listas de distribuição ou grupos para criação de regras e rotas, tanto na entrada de e-mails, como na saída.

Em solução inloquo, o MailInspector por padrão trabalha na forma de bridge, ficando entre o firewall e o servidor de e-mails, dessa forma não há a necessidade por parte do usuário final de configuração de rotas, proxy ou outra forma de redirecionamento dos e-mails. O usuário final e/ou usuário externo, receberá os e-mails filtrados, livre de ameaças, de forma transparente.

Com base na análise de comportamentos e na autoaprendizagem, esta ferramenta se adapta ao comportamento exclusivo das mensagens trafegadas em sua organização, possibilitando um forte controle sobre as mesmas, além de permitir a auditoria e criação de regras personalizadas para o fluxo de entrada e saída de e-mails, inclusive com regras granulares pelos seguintes atributos do e-mail:

- Domínio/Subdomínio, nome parcial de domínio;
- E-mails específicos;
- IP/Rede/Range de IP/Classe de IP;
- IP de Origem/IP de Destino;
- Número de destinatários;
- Número de destinatários inválidos;
- Expressões regulares;
- E-mail de Origem/E-mail de Destino;
- Grupos de Usuários/Grupos de LDAP;
- Remetentes e Destinatários específicos;
- Listas e Alias;
- Anexos (Extensão, nome parcial ou nome completo, RegEx, tamanho, número de anexos, anexo compactado, anexo compactado com senha, número de compactação, formato de compactação, entre outros campos de anexos)/MIME Type/TrueType;
- Dicionário de palavras;
- Entre muitos outros atributos;

Combata os SPAM através de um sofisticado sistema de análise de e-mails através de assinaturas (também chamada de fingerprint) fornecidas pelo sistema de atualização da HSC ou personalizadas, análise heurísticas, imagens, url, anexos, reputação, análise adaptativa em todos os campos dos e-mails (Cabeçalho RFC 821, RFC 822, RFC 2822, Envelope SMTP, DKIM (RFC 6376), SPF (RFC 7208), DMARC (RFC 7489), ARC (Authenticated Received Chain) (RFC 8617), URL, Corpo, Anexos e Conteúdo Completo).

O MailInspector segue orientações de órgãos e empresas com relação a padrões internacionais de segurança, tais como DMTF (Distributed Management Task Force), antispam.br, CGI (Comitê Gestor da Internet no Brasil), Spamlaws, entre outros, que definem e referenciam as boas práticas de proteção ao e-mail, incluindo total aderência a LGPD (Lei Geral de Proteção de Dados).

Em relação a anexos, o MailInspector consegue identificar os tipos originais de arquivos através de Mime-Type, bem como se o arquivo está compactado (com diversos formatos de compactação – ZIP, RAR, CAB, ACE, ARJ, BH, HA, JAR, PAK, LHA, LZH, PKZIP, BZIP, GZIP, ZOO, 7Z, BZ2, BZIP2, TZH, TGZ, TAR, etc), além de possuir a capacidade de permitir ao administrador trabalhar somente com extensões de arquivos ou detecção por nome, em ambos os casos através de uso de dicionários tanto por palavras ou expressões regulares, se o administrador assim desejar, também deixando aberta a opção de trabalhar com Allow List/Block List de arquivos, tanto a nível de bloqueio/remoção direto do anexo, quanto a aumento de pontuação de SPAM por

tipo de anexo no e-mail. Portanto é possível determinar a ação sobre o anexo ou e-mail, de acordo com a necessidade do administrador, podendo ser desde:

- Bloqueio/remoção de anexo por tipo de arquivo;
- Bloqueio/remoção de anexo por nome de arquivo ou nome parcial do arquivo;
- Bloqueio/remoção de anexo por tamanho de arquivo;
- Bloqueio/remoção de anexo por mime/type ou truetype do arquivo;
- Bloqueio/remoção por condição do arquivo (se está com malware, se está compactado e em quantos níveis de profundidade de compactação, se possui link de phishing ou simplesmente possui alguma URL bloqueada pelo administrador dentro do arquivo em anexo, etc);
- Entre outras condições do anexo;

O MailInspector por padrão quarentena automaticamente os e-mails classificados como prováveis spam (suspeitos) e spam. Ele já vem pré-configurado com as boas práticas de segurança de e-mail, para que eventual intervenção do administrador seja somente para ajustes finos na configuração. É possível o administrador da solução mudar as classificações de acordo com a sua necessidade (ou até mesmo mudar a pontuação de classificação), inclusive quarentenando mensagens em pastas customizadas por ele e/ou definindo ações a serem tomadas de acordo com a classificação do e-mail.

Caso o administrador queira, o MailInspector suporta armazenamento externo/remoto através de encaminhamento ou adição de disco externo integrado com tecnologia: HBA, Fibre Channel, Storages Externos com discos do tipo SAS, iSCSI, FC, etc. O sistema de storage remoto pode ser utilizado tanto para armazenamento de dados, quanto para a parte de Archiving.

É possível também importar configurações de outras soluções para o MailInspector, tais como:

- Lista de remetentes a serem bloqueados (Blocklist);
- Lista de remetentes confiáveis (Allowlist);
- Relays a serem liberados;
- Lista de Grupo de Usuários;
- Lista de IP/Range de IP;
- Dicionários/RegEx;
- Regras* de pontuação de SPAM;
- Regras* de bloqueio direto via DLP;
- Regras* de Controle de Fluxo;
- Regras* de Compliance;
- Entre outras configurações;

* Necessária análise da regra para a importação dela, para verificar necessidade real da importação (uma vez que o próprio MailInspector pode já estar tratando da regra nativamente, sem necessidade de recriar a regra), bem como compatibilidade de módulo a ser utilizado na regra.

No MailInspector na entrada de e-mails é possível configurar múltiplos domínios/múltiplos tenants e múltiplos servidores de e-mails (sem limitação), roteando as mensagens como um mapa de transporte, de acordo com a necessidade da empresa. Também pode-se configurar a saída de e-mails por um específico IP virtual, isso sendo atrelado a um determinado e-mail ou domínio.

Apesar de poder trabalhar em modo de multi-tenant, o MailInspector garante acesso exclusivo para ferramenta ao administrador do tenant, não sendo possível acesso cruzado entre administradores de tenants, dessa forma garantindo privacidade e segurança aos administradores e empresas que usem a mesma estrutura.

O MailInspector é totalmente responsivo, inclusive permite ao administrador trabalhar todos os módulos da Interface Gráfica, tanto as notificações de quarentena (Digest), quanto o módulo de e-mail criptografado,

sendo responsivo em celulares, tablets e afins, com ajuste automático do tamanho da tela, dessa forma, dando maior flexibilidade, independentemente do sistema operacional executado no dispositivo, podendo ser desde iOS, MacOS, Windows, Linux, ou mesmo Android ou outro.

Todos os módulos utilizados pelo MailInspector, desde o MTA, o sistema operacional HSC OS, até os agentes de antivírus/antiphishing, bem como todas as atualizações de assinaturas aplicadas, são homologados pela HSCBRASIL para o bom funcionamento em conjunto com toda a solução apresentada.

Todo o MailInspector é gerenciado de uma única interface gráfica, atingindo todos os módulos, sem necessidade de abrir novas janelas e/ou aplicativos para acesso a módulos específicos, nem uso de linha de comando (CLI) para efetuar configurações.

A instalação do MailInspector já contempla em toda a sua plenitude de funcionalidades, sendo ativado os módulos de acordo com o perfil adquirido pelo cliente, dessa forma, não há necessidade de reinstalação ou instalação extra de módulos, bastando mudar a chave de ativação para ativar eventuais módulos “extras”, assim não gerando nenhum impacto no ambiente de produção.

Para maior comodidade de administração, o MailInspector também permite múltiplos logins do mesmo usuário (por exemplo usuário administrador), permitindo execução de múltiplas tarefas de forma simultânea com o mesmo usuário cadastrado.

O MailInspector é compatível com todos os sistemas de MTA e correio eletrônico do mercado, tais como:

- Zimbra (todas as versões, desde que utilizem padrão SMTP para recebimento e envio de e-mails);
- Microsoft Exchange local (todas as versões, desde que utilizem padrão SMTP para recebimento e envio de e-mails);
- Microsoft Exchange com Office 365 – tanto em modo NUVEM (CLOUD) ou HÍBRIDO;
- G-Suite;
- IBM Lotus Domino / IBM Lotus Notes;
- Novell GroupWise;
- Sendmail (todas as versões, desde que utilizem padrão SMTP para recebimento e envio de e-mails);
- Postfix, etc.

Também possui **integração nativa** com os principais sistemas de colaboração do mercado, entre eles:

- Microsoft Exchange com Office 365®;
- Zimbra Collaboration Suite®;
- IBM Lotus Domino®;
- Google G-Suite/Google WorkSpace;
- Novell GroupWise®;

Integração por API (via Add-On) para os principais sistemas de e-mail, através de M-SOAR e Add-On dedicado a gerenciamento individual de e-mails, bem como ações para o usuário poder reportar ao administrador e-mails de phishing, spam, não spam, etc:

- Microsoft Exchange com Office 365®;
- Zimbra Collaboration Suite®;
- Google G-Suite/Google WorkSpace;

O MailInspector atua como E-mail Gateway e com isso, o administrador é capaz de:

- Redirecionar os e-mails para um IP específico, baseado no e-mail/domínio de origem;
- Redirecionar os e-mails para um IP específico, baseado no IP de origem;
- Efetuar bypass na solução, baseado em vários critérios;

- Conectar a diversas VLAN's através de instalação de placas de rede físicas ou virtuais, cada qual em uma VLAN distinta;
- Entre outras características próprias do MailInspector;

A solução MailInspector, pode ser instalada como:

- Servidor Físico Dedicado;
- Appliance Físico;
- Appliance Virtual;
- Misto da solução (parte servidor físico dedicado, parte virtual, ou até mesmo parte como appliance físico da HSCBRASIL), por exemplo:
  Gerenciador em Servidor Físico Dedicado, com um cluster montando sendo o primeiro node (ponto de acesso 01) em appliance virtual e o segundo node (ponto de acesso 02) em Appliance Físico da HSCBRASIL, dessa forma, cabe ao administrador a melhor forma de instalação, não sendo limitado a um único tipo de meio de instalação (somente físico ou somente virtual).

Múltiplas formas de trabalho

O MailInspector permite trabalho com diversas formas configuradas, de acordo com a necessidade da empresa, podendo ser:

- Filtragem;
- Monitoramento, efetuando somente análise dos e-mails, sem tomada de ação;
- **Tomada de ações com base em regras específicas configuradas pelo administrador**, permitindo definir comportamentos distintos para diferentes tipos de mensagens. Por exemplo, o sistema poderá ser configurado para **bloquear exclusivamente e-mails que contenham conteúdo malicioso ou palavras-chave classificadas como maliciosas em seus anexos**, enquanto os demais e-mails deverão ser processados normalmente e entregues aos respectivos destinatários;
- Monitoramento e filtragem mediante regra específica de DLP;
- Ativação somente para criptografar e-mails (com determinadas condições especificadas pelo administrador);
- Entre outros diversos modos de operação;

Segurança

Bloqueie mais de 99% das ameaças e spams. Com mais de 28 camadas de proteção contra vírus, trojans, spams, e-mail marketing, e-mails não solicitados, malwares, phishing, ransomware, spywares e outras ameaças.

O **MailInspector** conta com uma arquitetura de proteção baseada em **múltiplas engines de antivírus**, que podem atuar de forma independente ou integrada, proporcionando maior flexibilidade na configuração da solução e ampliando as camadas de proteção contra ameaças.

A solução possui a **HSC SmartDefender**, engine nativa e proprietária da HSC, desenvolvida especificamente para a proteção de ambientes de e-mail. O SmartDefender pode operar de forma autônoma, sem depender da execução de outra engine de antivírus, garantindo a capacidade de detecção e análise com base em seus próprios mecanismos, inteligência e modelos de segurança.

De forma **opcional**, o administrador pode habilitar a utilização integrada de uma segunda engine, como a **ESET**, adicionando uma camada complementar de análise. Nesse cenário, as engines atuam de maneira independente e os resultados de suas análises podem ser correlacionados pela solução, ampliando a

capacidade de identificação de ameaças e reduzindo a possibilidade de que um conteúdo malicioso passe despercebido por uma única tecnologia de detecção.

Quando utilizada em conjunto com a ESET, a **HSC SmartDefender** pode complementar seus próprios mecanismos de análise com informações provenientes da inteligência de ameaças disponibilizada pela ESET. Esse ecossistema inclui **IOCs (Indicators of Compromise)** e **IOAs (Indicators of Attack)** identificados por sua infraestrutura global de segurança (mais de 200 milhões de senders e milhões de honeypots), além de informações relacionadas a remetentes e outras fontes de inteligência utilizadas na identificação de ameaças. A abordagem de **defesa multicamadas**, portanto, permite que o administrador escolha entre utilizar exclusivamente a engine nativa da HSC ou habilitar engines adicionais, conforme os requisitos de segurança do ambiente. A utilização conjunta proporciona uma análise mais abrangente, combinando diferentes mecanismos, bases de inteligência e técnicas de detecção para aumentar a **assertividade, a cobertura e a capacidade de resposta** diante de ameaças direcionadas ao e-mail.

Quando o MailInspector detecta alguma ameaça, é possível efetuar múltiplas ações, de acordo com a configuração indicada pelo administrador, tais como:

- Adicionar cabeçalho customizado/tag no e-mail, quando ele for classificado como SPAM, PROVÁVEL SPAM, BULK MAIL, MAIL MARKETING e/ou E-MAIL LIMPO (permitindo integração com outros sistemas tais como Office 365, Zimbra, Microsoft Exchange, etc);
- Descartar a mensagem;
- Remover o anexo e prosseguir com a entrega;
- Quarentenar em pasta de quarentena especificado pelo administrador;
- Enviar notificações (para o remetente, destinatário ou ambos), com texto customizável, incluindo até o nome da ameaça encontrada;

Oferece a possibilidade de integrar o antivírus utilizado na empresa com o MailInspector*.

O HSC SmartDefender possui módulo exclusivo de detecção contra-ataques direcionados aos usuários, seja por método de Engenharia Social ou similar, entre eles:

- Virtual baiting;
- Pretexting;
- Quid pro quo;
- Redirecionamento a formulários de alteração de senha;
- Entre outros.

Dessa forma previne-se roubos, perda de dados e informações sigilosas. O MailInspector não atua somente como proteção, mas também como sistema de análise forense desses ataques, podendo fazer a rastreabilidade das mensagens afetadas por esse tipo de ataque.

Por padrão o MailInspector já vem fechado para as conexões do tipo TCP e UDP nas portas que não são usadas para comunicação de e-mail e/ou portas de uso exclusivo para o funcionamento da ferramenta, dessa forma, a solução já vem protegido contra tentativas de uso de portas indevidas, incluindo proteção a port scanning. Quanto a porta de e-mail (TCP 25/SMTP), o MailInspector por padrão possui suporte a ilimitado número de conexões SMTP, mas junto a essa funcionalidade, já vem com controle de conexões máximas oriundas de um único IP e proteção a quantidade excessiva de e-mails indevidos da mesma origem.

O MailInspector conta com proteção a ataques do tipo DOS/DDoS, ao qual verifica número excedente de conexões “pendentes” e bloqueia os IP’s de origem, para proteção a ataques de negação de serviço. Essas proteções são efetuadas tanto diretamente no sistema operacional (proprietária da HSCBRASIL - HSC OS), quanto a nível de MTA, com controle de conexão SMTP/SMTPS (máximo de conexões simultâneas globais e máximo de conexões por IP de origem), controle de e-mails do tipo Daemon SMTP, proteção a Non-Delivery Report Attack efetuando o bloqueio a nível de conexão, rejeição de conexões abertas na porta 25 pelo

protocolo TCP através de comando “HELO”/”EHLO” sem que existam entrada do tipo MX e/ou A no DNS, dentre outros tipos de controle e proteção, sendo os parâmetros totalmente configurável pelo administrador da solução.

O MailInspector passa por constantes auditorias de segurança, por pentests de empresas de auditoria independentes, por análise de código por terceiros e outros sistemas de teste, dessa forma assegurando que tenha sempre as eventuais vulnerabilidades sanadas e mantendo as cifras utilizadas dentro de padrões de segurança exigidos pelo mercado internacional, bem como possui endereço de email para recebimento de alertas de CVEs (Common Vulnerabilities and Exposures).

Em termos de análise de e-mail, o MailInspector faz a verificação de todo o conteúdo:

- Cabeçalhos (FROM/TO/SUBJECT, tanto a nível de envelope, quanto a nível de Header, entre outros campos do cabeçalho);
- Corpo do e-mail;
- Anexos;

Toda a verificação é baseada em normas RCF 821, RFC 2821, RFC 822 e RFC 2822 do protocolo SMTP.

O MailInspector permite ao administrador escolher o que deseja bloquear, permitindo composição de elementos a serem bloqueados/restritos de acordo com a política de segurança da empresa, como por exemplo, composição de regra de bloqueio com:

- E-mails contendo imagens, arquivo de áudio, vídeo, documentos padrão office, casando com regras de extensões, que podem ser definidos em *Anexos, Dicionário de Palavras* ou *Mime-Types/Fingerprint,* além de palavras INSERIDAS em documentos do tipo Office (SCR, DOC, DOCX, DOCM, XLS, XLSX, SLK, PPT, PPS, PPTX, PDF, XML, HTML, etc – mesmo estando dentro de arquivos compactados com senha ou sem senha).

Para maior garantia de segurança e aderência ao LGPD, no MailInspector é permitido ao administrador definir quais tipos de arquivos serão permitidos para envio para o SandBox da HSCBRASIL (evitando dessa forma o envio de dados sensíveis), bem como configurar o SandBox para uso local.

O MailInspector além de contar com os sistemas de proteção de ameaças do tipo vírus, malwares, utilizando a própria engine HSC SmartDefender antivírus e opcionalmente a engine da ESET para uma segunda camada de verificação de ameaça, dessa forma garantindo uma maior detecção sobre qualquer anexo e/ou ameaças presente nos e-mails analisados.

* Consulte o setor de suporte e desenvolvimento para verificar as necessidades quanto a possibilidade de integração (o fabricante do antivírus deve fornecer acesso ao código e/ou API’s utilizados para a ativação de varredura e limpeza, bem como retorno dos resultados de análises).

Importante salientar que ESET, é engine “extra” já licenciada, para aumento da segurança da ferramenta. Ela pode ser executada de forma independente, sem nenhuma interdependência do principal sistema de proteção do MailInspector que é HSC SmartDefender antivírus.

Arquitetura Unificada da Solução

O HSC MailInspector é uma solução integralmente desenvolvida, mantida e suportada pela HSC. Todos os módulos de proteção — Antivírus, Antimalware, Antispam, Sandbox, Análise de Ameaças, DLP, Criptografia, entre outros — são tecnologias próprias da HSC e operam de forma nativa dentro do ecossistema da plataforma.

A solução pode incluir parcerias tecnológicas com fornecedores externos, exclusivamente para complementar e ampliar a camada de segurança. Esses componentes adicionais, como o módulo ESET AV, são totalmente opcionais, já vêm devidamente licenciados e são integrados de forma controlada, sem descaracterizar a arquitetura unificada do Secure E-mail Gateway. Toda a responsabilidade técnica, suporte e evolução da solução permanece sob gestão exclusiva da HSC.

AntiSPAM

O HSC MailInspector possui duas engines de análise de e-mails contra SPAM. As engines filtram todos os campos do e-mail em busca de identificar SPAM, tais como: Cabeçalhos, Corpo, URL's, Imagens, Anexos e Hash/Fuzzy Hash.

O MailInspector por padrão trabalha em dois níveis:

1. Nível de Conexão (HSC SPAM Filter Ahead);
2. Nível de Processamento (HSC Filter Technology);

Nível de Conexão

Onde é efetuada toda a verificação se o e-mail possui o mínimo de requisitos para que o MailInspector possa prosseguir com a entrega dele.

O e-mail passa por mais de 40 camadas de proteção no MailInspector

HSC SPAM FIlter Ahead

É efetuada toda a análise das conexões e os dados do Envelope do SMTP para verificar se a origem é um possível emissor de SPAM e/ou se o e-mail possui requisito mínimo de segurança, desta forma os bloqueios realizados nesta camada são efetuados antes da mensagem ser recebida, economizando Banda e tempo de processamento. Em compensação, todo bloqueio efetuado nessa camada não tem possibilidade de quarentena, uma vez que o e-mail ainda não "entrou" no MailInspector (é barrado antes do mesmo ser aceito).

Nessa camada (controle de MTA) são efetuadas diversas verificações, tais como:

- Se o cabeçalho está de acordo com o padrão de SMTP (RFC 5321 e RFC 5322);

- Se o e-mail não extrapola o tamanho máximo (não há limitação para configuração de tamanho máximo da mensagem, nem tão pouco exigência de um tamanho mínimo da mensagem para que este controle esteja ativado);
- RBLs (RealTime Blackhole List) - Known Spam Source a nível de conexão;
- DNSBL/DNS Blacklist;
- Open RBL;
- Reputação Dinâmica (Dynamic Reputation);
- Análise de inexistência de DNS reverso/Forwarded-Confirmed Reverse DNS (FCrDNS);
- **Verificação de consistência do DNS reverso (FCrDNS – Forward-Confirmed Reverse DNS)**, com análise das informações retornadas pelo serviço DNS, em conformidade com as recomendações da **RFC 1912**.
  O MailInspector realiza uma **comparação aprofundada entre as informações presentes no cabeçalho da mensagem e os dados obtidos por meio das consultas DNS**, incluindo endereço IP, hostname e registros de DNS reverso, permitindo identificar inconsistências e possíveis indícios de falsificação ou comportamento suspeito na origem da mensagem;
- Zona do DNS do remetente;
- SenderID;
- SPF;
- DKIM;
- DMARC;
- DUL (Dial-up User List/Dynamically Assigned IP): Para detecção de listas dinâmicas de IP (listas de IP's de operadoras com serviços residenciais);
- ETL (Emerging Threat Block List): Listas baseadas em ameaças detectadas por firewall;
- Análise do domínio do remetente;
- Verificação de existência do e-mail destino através de conector LDAP/AD (verificando como possível ataque de dicionário pelo módulo OutBreak Filter e prevenção a Non-Delivery Report Attack), dessa forma, é executada uma consulta a um ou vários servidores de caixa de correio posicionados no "backend", antes de aceitar e-mails de entrada para os destinatários;
- Verificação de listas negras criadas pelo administrador (a nível de conexão);
  - Por IP;
  - Por Domínio;
  - Por Endereço de E-mail de Origem (envelope do e-mail);
  - Lista DNS;
- Verificação de listas brancas criadas pelo administrador (a nível de conexão);
  - Por IP;
  - Por Domínio;
  - Por Endereço de E-mail de Origem (envelope do e-mail);
  - Lista DNS;
- Comparação do cabeçalho do e-mail com o Banner da conexão, verificando possível cabeçalho falso;
- Entre outras diversas análises na camada de conexão (MTA);

As ações pertinentes ao nível de conexão (MTA) são:

- Bloqueio do e-mail;
- Rejeição (descarte direto);
- Liberação (deixar passar, mesmo que possua alguma anormalidade na verificação a nível de MTA);
- Temporariamente recusadas (gerando atraso na entrega);

Dessa forma, é possível limitar o envio/recebimento de mensagens, direto na camada de conexão, sem ter que acionar a parte de processamento, reduzindo consumo de CPU e memória no MailInspector.

O MailInspector permite que o administrador desative as verificações da camada de conexão (ação de liberação) por:

- IP;
- Range de IP;
- Classe de IP;
- Hostname;
- Domínio;
- Subdomínio;
- País de Origem;

Nível de Processamento

Onde é efetuada as outras verificações do e-mail, ao qual "consomem" recursos do MailInspector, tais como processamento e memória, bem como disco para armazenamento de eventual quarentena do e-mail.

HSC Filter Technology

Essa camada é a responsável por efetuar todas as demais análises depois que a mensagem é recebida.

É possível efetuar uma série de análises sobre os e-mails (tanto de entrada, quanto de saída). Tais fatores a serem analisadas englobam:

- Excedido número máximo de anexo;
- Excedido tamanho máximo do anexo;
- Excedido o tamanho máximo do e-mail;
- Excedido número máximo de anexos compactados;
- Excedido número máximo de arquivos dentro de um arquivo compactado;
- Bloqueado e-mail com anexo criptografado;
- Quarentena por regra de DLP;
- Manipulação na pontuação do e-mail, customizável por grupos, remetentes, domínios de origem/destino, entre outros parâmetros;
- Bloquear o e-mail por regras customizadas;
- Modificação da mensagem;
- Inclusão/modificação/remoção de cabeçalhos do e-mail;
- Modificação do Assunto;
- Remoção de anexos;
- Retenção do e-mail em quarentena (inclusive com opção de quarentena customizada);
- Exclusão do e-mail;
- Gerar notificação ao destinatário e/ou remetente do e-mail;
- Verificação de RBLs (RealTime Blackhole List) em nível de processamento;
- Verificação de malware em anexos e tomar as ações configuradas pelo administrador;
- Verificação comportamental do e-mail/anexos em SandBox e tomar as ações configuradas pelo administrador;
- Verificação de Zero Hour/Zero Day e tomar as ações configuradas pelo administrador;
- Verificação do e-mail quanto a pontuação de SPAM (análise do e-mail em relação as assinaturas e heurística);
- Verificação de links/URLs presentes no e-mail e em seus anexos (verifica-se por padrão 5 níveis de recursividade, ou seja, análise de URL dentro de URL e arquivos anexos, mesmo que estejam compactados ou integrados a arquivos tipo Office). São verificados os links e o comportamento deles:
    - Se há um redirecionamento;
    - Download de executável;
    - Download de conteúdo malicioso;
    - Categorização da URL;
    - Se é link de formulário;

  - Se o link é de coleta de dado do usuário;
  - Se é link de troca de senha;
  - Entre outros;
- Reescrita de URLs contidos no e-mail;
- Prosseguir com a entrega da mensagem, inclusive com opção de gerar cópia em auditoria;
- Incluir o remetente da mensagem/domínio/IP em block list pessoal ou de toda a empresa;
- Incluir o remetente da mensagem/domínio/IP em allow list pessoal ou de toda a empresa;
- Entre diversas outras ações;

Como o HSC MailInspector processa o tráfego de internet através da sua rede

O MailInspector trabalha em dois níveis:

- Nível de Conexão: Ao qual chamamos de HSC SPAM Filter Ahead
  O nível de conexão é o nível onde são verificados se os e-mails atendem os requisitos mínimos de segurança, tais como:
- Nível de Processamento: Ao qual chamamos de SPAM Filter Technology
  Nesse nível é onde podemos quarentenar ou descartar as mensagens que não estão de acordo com a pontuação ou nas regras impostas pelo administrador, como por exemplo:
  Colocar em quarentena qualquer mensagem que venha com a palavra "VIAGRA" no corpo do e-mail, mesmo que esteja em HTML.

Precisão e qualidade

O MailInspector garante bloqueio de mais 99% de detecção das ameaças e spams (spam catchig rate), com grande precisão quanto a sua filtragem, garantindo uma taxa mínima de 99,9999% de precisão, dessa forma compondo uma das soluções com melhor índice do mercado mundial.

O MailInspector possui antivírus nativo e proprietário (HSC SmartDefender antivírus), ao qual tem a possibilidade de trabalhar em conjunto com outro antivírus secundário (ESET), já licenciado para o uso, sem necessidade de aquisição de novas licenças.

No sistema de E-mail Gateway Local trabalham simultaneamente duas engines, a HSC SmartDefender antivírus e a ESET atuando como antivírus adicional, de forma autônoma, bem como sistema adicional de threat intelligence de forma autônoma no SandBox Cloud (através de inclusão de dados de IOC's e IOA's pegos dos sistemas distribuídos) auxiliando o antivírus proprietário da HSC Brasil (HSC SmartDefender antivírus).

O MailInspector consegue detectar e bloquear ameaças, tanto a nível de spams, quanto em relação a ameaças contidas nos anexos. O MailInspector garante a verificação de todas as URL`s contidas no e-mail e reescrita dos mesmos (com a função Targeted Attack Protection).

É possível também efetuar análise forense das ameaças, com a geolocalização da origem e indicação dos e-mails afetados pela ameaça.

Machine Learning

O HSC MailInspector possui um sistema avançado de detecção de SPAM e novas ameaças baseado em um sistema local de auto aprendizado. Ele é capaz de lidar com um enorme volume de dados e processar

informações que identificam a atividade de e-mails da sua corporação, aprendendo dinamicamente o que são e-mails confiáveis e o que são e-mails suspeitos, agindo de forma automática na prevenção de Surtos de vírus, spam e phishings.

O sistema utiliza algoritmos avançados de análise textual e semântica para identificar anomalias e padrões suspeitos no conteúdo dos e-mails. Para isso, a solução avalia o contexto e as características das mensagens, permitindo uma análise mais precisa das ameaças. À medida que o sistema é utilizado e recebe novos dados, sua capacidade de aprendizado e adaptação é aprimorada, contribuindo para aumentar continuamente a precisão e a assertividade na identificação de comportamentos anômalos.

Uma vez que o sistema de Machine Learning esteja em funcionamento, ele é capaz de verificar a composição e conteúdo da mensagem, bem como a sua semântica, ou seja, efetua a análise do contexto da mensagem em busca de anomalia.

Proteção a ataque com TLD

O Domínio de Nível Superior (TLD, na sigla em inglês - Top Level Domain) é o sufixo que você pode encontrar no final do endereço de site. Basicamente é a palavra após o "." . (ponto) Por exemplo, o TLD de www.hscbrasil.com.br é ".br".

Existem hoje mais de 1.500 domínios genéricos de nível superior (gTLDs), o nome que vai depois do ultimo ponto (.), muitos dos quais são mais longos do que os tradicionais nomes de dois e três caracteres tradicionais (por exemplo .com, .edu, .br, .org, .br, .me, .it, .pe, .fr, etc.).

Como exemplos brasileiros podemos citar os novos domínios de empresas, como o .globo (http://loja.globo) .ipiranga (https://portal.ipiranga) .itau (http://nic.itau) e .bradesco (http://banco.bradesco).

Infelizmente o uso do TLD abriu novas formas de ataques, ao qual o atacante compra um domínio válido com o TLD, por exemplo temos a URL válida **americanas.com** e com a entrada do TLD, pode-se comprar o domínio **americanas.cam** para efetuar um ataque, que é parecido com o original e que enganaria um usuário mais distraído.

Para prevenir este tipo de ataque o MailInspector conta com assinatura propria de TLD comparando com os domínios originais, bem como técnicas de WHOIS do domínio com TLD em compração com o WHOIS original.

Proteção contra Prompt Injection

O MailInspector **detecta tentativas de Prompt Injection** inseridas ou ocultadas no conteúdo de mensagens de e-mail, identificando instruções maliciosas ou manipuladas que possam ser interpretadas indevidamente por **sistemas automatizados, assistentes virtuais, agentes de IA ou mecanismos de processamento baseados em Inteligência Artificial**.

A análise considera não apenas o conteúdo explícito da mensagem, mas também instruções inseridas de forma dissimulada em **textos, HTML, cabeçalhos, assinaturas, links, metadados e arquivos anexados**, quando aplicável, identificando padrões que tenham como objetivo alterar o comportamento, as instruções, o contexto ou as decisões de sistemas automatizados que venham a processar o conteúdo da mensagem.

Quando identificada uma tentativa de **Prompt Injection**, a mensagem é classificada de acordo com a política de segurança definida pelo administrador, possibilitando a aplicação de ações como **bloqueio, rejeição,**

quarentena, alerta ou encaminhamento para análise, mantendo o registro do evento para fins de rastreabilidade e investigação.

Anti Spoofing

Com o HSC MailInspector sua empresa estará protegida contra-ataques de falsificação de e-mails tais como: E-mail Impostor, BEC "business e-mail compromise", fraude de e-mail, Ataques de Engenharia Social, Spoofing de Domínio, Spoofing de IP, etc.

O MailInspector usa as principais técnicas para garantir que o remetente da mensagem é legítimo e que não é um ataque de falsificação de remetente.

Através de validação de DKIM, SPF, SenderID, DMARC, Domain Spoofing, Subject Spoofing, Look-A-Like Domain e New Domains, o sistema identifica as mais avançadas técnicas de tentativa de ataques direcionados.

O MailInspector detecta Spoofing de IP (Forged IP), através de uma série de verificações, tais como:

- Comparação do IP do e-mail em relação a DNS reverso;
- Verificação de entrada A, entrada AAAA, entrada MX no DNS em relação ao IP de Origem e MAIL FROM, bem como validação do EHLO/HELO;
- Comparação do IP do e-mail em relação a geolocalização;
- Comparação do IP do e-mail em relação ao range de IP do domínio de origem;
- Consulta de rede neural quanto a IP's forjados, aumentando a sensibilidade quando o e-mail vier de um IP com alto risco de ser forjado;
- Verificação de uso de técnica de X-Forwarded-For (XFF);
- Entre outros métodos de detecção de Forged IP;

Em proteção contra fraudes de e-mail/BEC, no MailInspector é possível cadastrar usuários, domínios e/ou Display Names para uso com regra de proteção contra esse tipo de ataque, dessa forma aumentando a efetividade da proteção em relação a usuário/e-mails críticos, protegendo tanto em relação ao FROM, quanto ao TO, independente da forma de ataque.

IDN Protection

A partir do lançamento das RFC 3454, RFC 3490, RFC 3491 e RFC 3492 em 2003, os protocolos de DNS permitem caracteres de idiomas locais na resolução de nomes. No Brasil, por exemplo, podemos registrar domínios com caracteres como Ç. Em países hispano falantes a utilização de Ñ é regularizada para registro de domínios.

Estes caracteres locais são compatibilizados pelos recursos IDN (Internacionalized Domain Names) ou internacionalização de nomes de domínios os quais codificam os domínios com caracteres especiais.

Sistemas de filtragem e categorização de URLs podem não estar preparados para tratar caracteres locais corretamente, facilitando aos atacantes a evasão das técnicas de proteção tradicionais. Assim, projetando seu uso em campanhas de SPAM e Phishing internacionais.

MailInspector identifica e bloqueia ataques que exploram vulnerabilidades na decodificação de domínios (incluindo URL encurtadas), garantindo o funcionamento em todas suas camadas de proteção.

Sistema Generativa (IA) para Análise de E-mails Bloqueados

O HSC AI Cyber Assistant é uma tecnologia proprietária da HSCBRASIL, desenvolvida para apoiar usuários finais e administradores do MailInspector na detecção de ameaças cibernéticas. Utilizando Inteligência Artificial avançada, o sistema analisa automaticamente mensagens, identificando elementos inseguros, URLs suspeitas e variações de sentimentos que podem sinalizar risco e por último indica o veredito sobre a análise dos pontos citados.

Com a análise precisa da inteligência artificial, o HSC AI Cyber Assistant facilita a tomada de ação pelos usuários, permitindo uma resposta rápida e eficaz a potenciais ameaças, reforçando a segurança digital de forma proativa, com indicação de decisão a ser tomada, dessa forma o próprio usuário final conseguirá entender o motivo do bloqueio do e-mail, sem necessidade dele se tornar um expert em e-mail gateway.

É importante salientar que o sistema de Inteligência Artificial (IA) utilizado pelo MailInspector é uma base própria treinada com a finalidade específica de análise de e-mails, dessa forma garantindo veracidade e confiabilidade nas informações do treinamento do sistema de Inteligência Artificial utilizado. Nesse modelo não corre risco de aprendizagem com informações falsas (fake news) ou errôneas, bem como não é utilizada a consulta de bases abertas, tais como ChatGPT, Bard, BingChat, etc.

Fácil administração

Administração centralizada de forma simples e intuitiva. Integração com os principais sistemas de correio eletrônico e sistemas de diretórios existentes no mercado. Relatórios simplificados e gráficos de fácil compreensão e agendados conforme a sua necessidade, podendo ser filtrados por domínios, rotas de entrada ou saída, etc. Também contamos com um relatório consolidado (com possibilidade de agendamento de envio por e-mail), ao qual em um único relatório pode-se extrair os seguintes dados:

- Volume de Mensagens por Data, indicando a qualidade dos e-mails, separando por:
  - Total de E-mails;
  - Volume de mensagens;
  - Tamanho médio;
  - E-mails confiáveis;
  - Provável SPAM;
  - SPAM;
  - Phishing;
  - Allow List;
  - Block List;
  - Ameaças (Malwares/Virus);
  - Tamanho Excedido;
  - Conteúdo Bloqueado;
  - Outros Bloqueios;
- TOP e-mails Relays;
- TOP 10 remetentes por quantidade;
- TOP remetentes por domínio;
- TOP destinatários por quantidade;
- TOP 10 destinatários por volume;
- TOP 10 principais remetentes de spam;

- Relatório de vírus;

Os relatórios por padrão são enviados à partir da máquina de console de gerenciamento, onde fica instalada o Banco de Dados centralizado, sendo possível o envio nos formatos PDF, HTML e CSV, com agendamento de envio de acordo com a necessidade definida pelo administrador.

Os relatórios do MailInspector seguem os modelos padrões encontrados no mercado, conforme as boas práticas de: SOA, SOX (Sarbanes-Oxley), HIPAA, GLBA (Gramm-Leach-Bliley Act), GDPR, PIPEDA (Personal Information Protection and Electronic Documents Act) e LGPD, entre outros modelos conhecidos de segurança da informação e ainda permite que o administrador customize esses modelos, conforme a sua necessidade.

Ainda para maior facilidade, os e-mails quarentenados podem ser gerenciados pelos próprios usuários finais do sistema. Este gerenciamento pode ser feito através do próprio e-mail de notificação de quarentena (por link de liberação do e-mail quarentenado, inclusão do remetente em block list individual, inclusão do remetente em whitelist individual ou até mesmo reportar o e-mail quarentenado como falso positivo).

Também é possível utilizar portal web (HTTPS), ao qual o usuário poderá ter acesso a sua pasta de quarentena, permitindo a visualização dos e-mails quarentenados e solicitação da liberação dos mesmos ao administrador do sistema. É possível ainda efetuar outras configurações, tais como inclusão/exclusão/edição de registros em Allow List e Block List individual, mudança do idioma do portal (Português do Brasil, Inglês, Espanhol, Espanhol do Paraguai ou Finlandês), mudança do nível de sensibilidade do sistema de proteção a e-mails (baixo, médio ou alto). O usuário final pode ainda configurar a ativação de notificação de quarentena individual e a configuração de frequência do envio da notificação de quarentena individual, sendo possível a marcação dos dias de semana a serem enviados e os horários desejados. Na interface do usuário é possível realizar pesquisas avançadas usando tags de quarentena ou classificação de mensagens.

Na solução HSC é possível criar exceções por rotas, usuários específicos, grupos de usuários, IP's, range de IP's, classe de IP, domínios, subdomínios, redes e até mesmo expressões regulares. Não há limitação de criação de regras. Dessa forma conseguimos dar maior maleabilidade ao administrador do sistema. Muitas das regras de maleabilidade foram estendidas aos usuários finais da sua empresa, tais como classificação de níveis de sensibilidade de detecção de spam (Baixo, Médio e Alto), dessa forma o próprio usuário pode parametrizar a sensibilidade do anti-spam, de forma única e em conjunto com a allowlist/blocklist individual.

O sistema de gerenciamento poderá ser configurado para que possa utilizar administradores customizados, sendo os mesmos separados na administração de determinados domínios ou e-mails, criando políticas únicas por domínio ou por e-mail ou ainda por grupos de usuários, dessa forma esse administrador customizado somente enxergará o(s) domínio(s) que ele estiver gerenciando, bem como acesso somente aos módulos liberados para ele. Para maiores informações vá para o tópico Administração Centralizada e Quarentena.

É possível efetuar a troca da logomarca do MailInspector pela logomarca da empresa (branding) nas telas de gerenciamento, notificação de quarentena individual (digest) e relatórios, bastando selecionar a nova logomarca e efetuar a devida troca.

Toda e qualquer troca de configuração/criação ou modificação de regras, ao selecionar aplicação das mesmas, toma um tempo máximo de 60 segundos para serem aplicadas em toda a solução.

O MailInspector também trabalha como “backup” do servidor de e-mail, para caso de queda do servidor de e-mail da sua empresa, os seus e-mails não serão perdidos, ficando armazenado no MailInspector na fila de saída (para o sentido do servidor de e-mail da sua empresa). Quando o sistema de e-mail é reestabelecido, a entrega ocorrerá normalmente e a fila esvaziada.

O MailInspector permite ao administrador criar regras customizadas e exceções, para efetuar ações sobre os mesmos, desde alterar pontuação, sensibilidade de detecção, bloquear, mudar o assunto e/ou utilizar as regras para DLP e/ou Criptografia de e-mails e/ou Quarentena Customizada (até mesmo quarentena temporária utilizada pelo Supervisor de E-mail), entre outras ações. As regras customizadas são criadas de acordo com a necessidade do administrador. Essas regras podem ser baseadas em:

- Rotas e/ou Sentido (E-mail de Entrada/Saída e/ou E-mails Internos);
- Endereço de IP de Origem;
- Sender HELO/EHLO Domain;
- Nome DNS reverso do e-mail (hostname);
- Sender Envelope;
- Sender Header;
- E-mail de Origem;
- E-mail do Destinatário;
- Domínio do Remetente;
- Domínio do Destinatário;
- Quantidade de Destinatários contidos no e-mail;
- Subdomínio do remetente;
- Subdomínio do destinatário;
- Grupo de Usuários de Origem;
- Grupo de Usuários de Destino;
- País ou Grupo de Países;
- Linguagem do e-mail;
- IP de Origem;
- IP de Destino;
- Range de IP;
- Classe de IP;
- Qualquer Cabeçalho do protocolo SMTP, incluindo cabeçalhos customizados;
- Assunto/Subject;
- Anexos (Tamanho, extensão, quantidade, tipo – Mime-Type, se é compactado, quantidade de arquivos contidos em anexo compactado, quantidade de níveis de compactação, arquivos compactados com senha, etc);
- Dicionário de palavras (RegEx – Expressão Regular) casando com conteúdo do e-mail, assunto, nome completo ou parcial dos anexos ou em outros campos do e-mail (tais como Cabeçalho SMTP);
- Vários outros campos.

Após verificadas as condições são efetuadas as ações (no caso de política de DLP), podendo ser:

- Bloqueio do e-mail (quarentena);
- Remoção/substituição do(s) anexo(s) específicos ou todos;
- Mudança no conteúdo do e-mail;
- Mudança no assunto (Subject) do e-mail;
- Reencaminhamento do e-mail a terceiro;
- Remoção do e-mail;
- Inclusão de Disclaimer / Alerta no corpo do e-mail, podendo ser no final ou no começo do e-mail;
- Inclusão/edição de cabeçalho do e-mail;
- Remoção/substituição de URLs/links contidos no e-mail;

É possível a criação de regras compostas combinando-se múltiplas condições com o uso de operadores booleanos.

Quanto a inclusão de registros em Allow List e Block List, o administrador conta com Wizard, ao qual permite que ele acione registros sem necessidade de digitar nenhum caracter, dessa forma facilitando o entendimento e evitando eventuais entradas errôneas de allow list e/ou block list.

Response-Based Phishing (RBP)

O **Response-Based Phishing (RBP)** é um módulo de proteção do MailInspector voltado à identificação de ataques de phishing que buscam ***induzir a vítima a iniciar uma interação com o atacante***, através de Engenharia Social, reduzindo a dependência de links ou anexos maliciosos tradicionais.

O módulo contido no MailInspector atua especialmente sobre duas técnicas:

1. **TOAD / CallBack Phishing (Telephone-Oriented Attack Delivery):**
   Identifica mensagens que utilizam engenharia social para induzir o usuário a realizar uma ***ligação telefônica***, normalmente associada a falsas cobranças, renovações, suporte técnico, cancelamentos ou alertas de segurança.
2. **Reply Harvest:** identifica mensagens cujo objetivo é provocar uma ***resposta direta por e-mail***, permitindo ao atacante validar contas ativas, estabelecer confiança e iniciar uma segunda etapa do ataque, como BEC, fraude financeira, roubo de credenciais ou envio posterior de conteúdo malicioso. Esse processo se dá sem uso de links maliciosos ou anexos, comumente utilizados em ataques.

O **RBP** utiliza análise de conteúdo, contexto, intenção da mensagem, padrões linguísticos e indicadores comportamentais para detectar essas abordagens, ampliando a proteção do MailInspector contra ataques de engenharia **social sem payload (entrega de pacote/arquivo) malicioso aparente**.

Sistema de CDR e SandBox de documentos

CDR

O **CDR (Content Disarm and Reconstruction – Desarme e Reconstrução de Conteúdo)** realiza, em tempo real, a análise, desarme e reconstrução dos arquivos recebidos, removendo elementos potencialmente ativos ou executáveis e gerando uma **nova versão higienizada do arquivo**, preservando, sempre que possível, seu conteúdo legítimo e sua funcionalidade.

Como princípio de segurança, os **elementos ativos e potencialmente executáveis são tratados como não confiáveis**, sendo removidos ou neutralizados durante o processo de reconstrução. Dessa forma, o CDR processa os arquivos recebidos, desconstrói sua estrutura, identifica componentes ativos e elimina elementos que possam ser utilizados para exploração de vulnerabilidades ou execução de código malicioso.

Essa abordagem proporciona uma camada adicional de proteção contra **ameaças Zero-Day e Zero-Hour**, inclusive aquelas relacionadas a ameaças emergentes identificadas por mecanismos de inteligência, reduzindo proativamente a possibilidade de entrega de conteúdo malicioso aos usuários.

Sandbox de Documentos

Como complemento ao CDR, o **MailInspector** disponibiliza um mecanismo integrado de **Sandbox para análise de documentos**, no qual a análise dinâmica dos arquivos é realizada diretamente pelo próprio agente do MailInspector, no **ponto de filtragem da mensagem**.

Essa arquitetura elimina a necessidade de instalação ou operação de um agente exclusivo para a funcionalidade de Sandbox, permitindo que os arquivos sejam submetidos à análise como parte do próprio fluxo de processamento e proteção do e-mail.

O Sandbox permite analisar documentos e seus respectivos componentes e objetos incorporados, incluindo elementos potencialmente executáveis ou ativos, tais como **EXE, DLL, JPG, JPEG, BMP, GIF, JavaScript (JS), VB/VBS, código HTML, arquivos de áudio, arquivos de vídeo e imagens**, entre outros.

Entre os principais formatos e suítes de documentos suportados, destacam-se:

- **PDF**;
- **Microsoft Office**, incluindo documentos, planilhas e apresentações;
- **Apache OpenOffice**;
- **LibreOffice**;
- **OnlyOffice**;
- **Calligra Suite**;
- **Outros formatos de documentos**, inclusive aqueles que contenham objetos ou componentes incorporados.

A combinação das tecnologias de **CDR e Sandbox** proporciona uma abordagem em múltiplas camadas para a proteção de documentos, permitindo tanto o **desarme preventivo de conteúdos potencialmente perigosos** quanto a **análise comportamental e dinâmica dos arquivos**, contribuindo para a identificação e mitigação de ameaças conhecidas, desconhecidas e emergentes antes que o conteúdo seja disponibilizado ao usuário final.

O CDR previne ameaças oriundas de múltiplas fontes, como por exemplo:

- E-mail;
- Data Diodes;
- Web Browsers;
- Endpoints;
- File Servers;
- FTP;
- Cloud e-mail ou webmail programs;
- SMB/CIFS;
- Removable media scanning (CDR Kiosk);

Além de detecção, as ações possíveis sobre os arquivos atuados pelo modulo CDR são:

- Quarentena do e-mail;
- Entrega do e-mail, mantendo o conteúdo;
- Bloqueio somente do anexo e prosseguir com a entrega do e-mail;

Tanto o módulo de CDR, quanto o módulo de SandBox (Network SandBox, File SandBox, Document SandBox) atuam sobre arquivos compactados, desde que consigam descompactá-los.
Se o anexo estiver compactado com senha e não tiver como descompactá-lo, o MailInspector tomará a ação sobre arquivos compactados com senha.

Administração Centralizada e Quarentena

Permite ao administrador gerenciar um ou mais Pontos de Filtragem de uma única console, incluindo suporte a cluster de Alta disponibilidade e Load Balancing. Com único ponto de gerenciamento, é possível rastrear e-mails, criar políticas, filtros, ajuste em assinaturas, modificar configurações, visualizar logs, configurar o módulo de DLP, configurar regras de criptografia, tomar ações, sem necessidade de abrir outro ponto de

gerenciamento ou instalação de novos aplicativos para esse processo ou ainda instalar um ponto de armazenamento específico para quarentena. O administrador através do gerenciamento centralizado, pode escolher gerenciar um único cluster, múltiplos clusters da solução ou até mesmo gerenciar um único ponto de filtragem/acesso da solução. É possível que a quarentena seja direcionada em outro local/máquina, de acordo com a necessidade do administrador da solução (servidor remoto).

Também é possível liberar acesso externo ao sistema, sem necessidade de instalação de pontos extras para essa finalidade.

O Sistema suporta tanto armazenamento da Quarentena de forma centralizada no próprio Appliance ou em uma máquina dedicada a armazenamento de quarentena.

A quarentena é armazenada de forma criptografada a fim de garantir total segurança do acesso aos dados armazenados.

O sistema possui quarentena individual por usuário, permitindo que o mesmo acesse e administre suas configurações, tais como: Liberar mensagens retidas na quarentena, rastrear e-mails, adicionar endereços na Allow List e Block List, reportar bloqueios indevidos, excluir e-mail da quarentena, etc. Essa mesma quarentena, pode ser acessado pelo administrador geral da ferramenta, ao qual terá acesso a TODAS as quarentenas.

Caso tenha sido criado um administrador customizado, é possível configurar o acesso da quarentena específica para ele, por exemplo a quarentena de VÍRUS é somente liberado para o "*administrador de ameaças*", enquanto a mesma quarentena continua inacessível ao "*administrador de mail marketing*".

O Acesso a quarentena e a autenticação do MailInspector, pode ser integrado via autenticação nos principais sistemas de diretórios padrão LDAP, tais como:

- Microsoft Active Directory (através de qualquer um dos protocolos: LDAP, LDAPs, RADIUS ou SAML 2.0);
- Microsoft Azure;
- OpenLDAP;
- Zimbra;
- Novel Edirectory;
- Sun iPlanet Directory;
- Oracle Internet Directory;
- Oracle Unlimited Directory;
- Apache Directory Server;
- Red Hat Dictory;
- OpenDS;
- OpenDJ;
- IBM Tivoli Directory;
- Lotus Notes/Lotus Domino;
- Nexor Directory;
- Apple Open Directory;
- Critical Path Directory;
- Todos que usam sistemas de diretório compatíveis com padrão LDAP (Lightweight Directory Access Protocol);

Custo x benefício

Aumente a produtividade de seus funcionários, reduzindo o tempo gasto com informações desnecessárias. Economize banda de internet, eliminando os e-mails indesejados antes de chegarem até você. Suporte a alta disponibilidade e balanceamento de carga. A alta disponibilidade pode ser por cluster ativo/ativo ou ativo/passivo, lembrando que as configurações são sempre sincronizadas entre a console de gerenciamento e os pontos de acesso. Essa sincronização pode ser manual ou automática. Ao sincronizar, o sistema sincroniza as quarentenas, logs, políticas de segurança, diversas regras customizadas, block list, allow list, regras de DLP, regras de criptografia, regras de quarentena customizada, regras de pontuação de spam, regras específicas de verificação, regras de controle de fluxo, logs de auditoria, sincronização de mineração de dados para relatórios, entre diversas outras configurações.

Auditoria & DLP

Monitore todo o conteúdo das mensagens e evite o mau uso das informações. Conformidade com as principais normas de segurança do mercado e LGPD.

Sistema de DLP - Data Loss Prevention - integrado, que permite criar regras robustas a fim de identificar mensagens com conteúdo sigiloso. O MailInspector já vem com modelos padrão HIPAA, PCI-DSS, entre outros modelos de detecção de conteúdo.

O sistema de auditoria permite armazenar dados pelo período necessário da política de segurança de cada empresa, sendo para isso permitido o uso de discos externos "Storages" conforme a necessidade da empresa.

No MailInspector o DLP já vem licenciado e habilitado para uso, sem necessidade de aquisição de módulos adicionais ou licenças extras.

O sistema de auditoria também consegue suprir a função de webmail secundário para o caso de queda no seu sistema de e-mail principal, pois uma vez ativada, é possível liberar ao usuário o acesso a visualização dos e-mails, download dos e-mails, bem como forçar eventual reenvio do mesmo para a sua caixa postal.

Já quando a solução é em nuvem, o mesmo automaticamente serve como sistema de retenção e continuidade, integrando a quarentena de auditoria a interface do usuário.

Criptografia de E-mail e TLS/SSL

Criptografe automaticamente os e-mails sem a necessidade da interação dos usuários, garantindo a confidencialidade na troca de mensagens. O Administrador pode configurar quais e-mails deverão ser criptografados baseados em regras por:

- Endereço de IP de Origem;
- Sender HELO Domain;
- Sender Envelope;
- Sender Header;
- E-mail do destinatário;
- Domínio do Remetente;
- Domínio do Destinatário;
- Subdomínio do remetente;
- Subdomínio do destinatário;
- Grupo de Usuários de Origem;
- Grupo de Usuários de Destino;
- País;
- IP de Origem;

- IP de Destino;
- Range de IP;
- Classe de IP;
- Qualquer Cabeçalho do protocolo SMTP, incluindo cabeçalhos customizados;
- Assunto/Subject;
- Anexos (Tamanho, quantidade, tipo – Mime-Type, Extensão, nome do anexo, se é compactado, etc),
- Conteúdo do e-mail, entre vários outros campos.

As mensagens que forem criptografadas serão armazenadas na ferramenta usando o algoritmo de criptografia configurado na quarentena, usando uma chave única e exclusiva por mensagem, dispensando instalação de certificado ou chave PSK, isto é, suporta-se mensagens baseadas em identidade (Identity Based Encryption IBE), ao qual não requer uma PSK ou certificado instalado anteriormente para que o e-mail seja descriptografado.

O Acesso a estas mensagens são efetuadas através de uma console Web HTTPS customizável e compatível com qualquer Browser de forma segura e sem cache via Cookies. O usuário destino para poder visualizar a mensagem criptografada, deve efetuar a autenticação de seus dados.

Tanto para a criptografia, quanto ao protocolo TLS/SSL, o MailInspector possui suporte a todos algoritmos de criptografia usados pelos clientes de e-mail para protocolos S/MIME e PGP. Com capacidade de Opportunistic TLS (STARTTLS).

A criptografia utilizada pelo MailInspector, respeita as normas de conformidade internacional, como: HIPAA, PCI-DSS, SOX, PIPEDA (Personal Information Protection and Electronic Documents Act), GLB.

O MailInspector suporta múltiplos algoritmos de criptografia, dentre eles podemos citar alguns:

- DES (Data Encryption Standard);
- IDEA (International Data Encryption Algorithm);
- Blowfish;
- RC (Ron's Code ou Rivest Cipher);
- RSA (Rivest, Shamir and Adleman);
- DSA (Digital Signature Algorithm);
- AES (Advanced Encryption Standard);
- DHE (Diffie-Hellman);
- ADH (Anonymous Diffie-Hellman);

Com ou sem uso de verificação da integridade por MD5.
Com ou sem uso de verificação de assinatura digital por DSS (Digital Signature Standard).
Com ou sem uso de função de dispersão criptográfica SHA (Secure Hash Algorithm).
Com ou sem uso de cadeia de blocos (CBC - Cypher-Block Chaining).
Suporta praticamente qualquer tamanho de chave (32 bits, 64 bits, 128 bits, 192 bits, 256 bits, 512 bits, 1024 bits, 2048 bits e superiores).

O MailInspector possui suporte a TLS versão 1.0, 1.1, 1.2 e 1.3.

No MailInspector o sistema de Criptografia de e-mails já vem licenciado e habilitado para uso (tanto para uso do método pull, como para o método push), sem necessidade de aquisição de módulos adicionais, nem licenças extras.

O uso de criptografia de e-mails no MailInspector não requer chave PSK ou certificado instalado na máquina do destinatário, pois a criptografia utilizada é baseada em identidade (Identity Based Encryption - IBE). Todo

o processo de criptografia e transações é registrado em logs de auditoria, para consulta no módulo de auditoria (log de Eventos) do MailInspector.

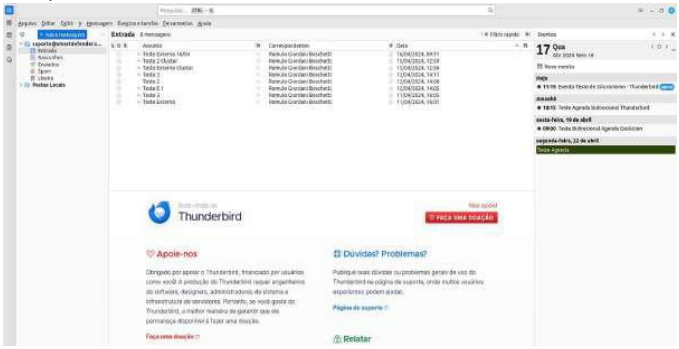
Continuidade de Serviço de E-mail

O MailInspector possui serviço de continuidade de e-mail, dessa forma caso o servidor de e-mails da empresa por algum motivo saia do ar, o MailInspector pode atuar como servidor de webmail. Esse módulo de mailbox permite fornecer aos usuários uma continuidade no serviço de e-mail, incluindo e-mails em quarentena, agenda, tarefas e calendários, criando uma experiência completa e simplificada.

Para a continuidade do serviço de e-mail, o MailInspector oferece:

- **Mailbox:** Servidor completo de e-mail próprio MailInspector, com mailbox integrada, com webmail e ferramentas de colaboração. Suporte a cliente de e-mail e a celulares Android e iPhone;

- **Protocolos:** Mailbox server completo, com acessos via IMAP/S, POP3/S, SMTP/TLS, dessa forma, é possível configurar o seu leitor de e-mail para uso junto com o MailInspector;
- **Sincronização:** Sincronismo bidirecional de contatos, calendários e tarefas. Opera com clientes de e-mail MUA, como Thunderbird, Outlook e Evolution, clientes de Android e iPhone, e com os padrões CalDAV, CardDAV e WebDAV;
- **Disponibilidade:** Disponibilidade contínua do serviço de e-mail reduzindo o risco de inatividade e perda de produtividade;



Backup e Restore

No MailInspector é possível efetuar backup somente das configurações e políticas ou backup completo (incluindo logs e quarentena), dessa forma fica a critério do administrador a escolha do conteúdo do backup. É possível com um simples clique no botão de restaurar a restauração de backups.

Também possui a opção de envio de backup por FTP/FTPS para outra máquina, dessa forma efetuando backup remoto.

Com um simples clique em Disaster Recovery, o sistema é totalmente restaurado no último ponto de backup, sem qualquer necessidade de configuração ou intervenção.

O backup pode ser agendado em diversos horários e dias da semana, além de permitir ao administrador baixar na sua máquina ou enviar ao MailInspector algum backup específico.

Não existe um limite para quantidade/data limite de backup, dependendo unicamente de disponibilidade de espaço em disco para o backup, ao qual pode ser até mesmo armazenado em outro local por FTP/FTPS.

O **MailInspector** permite realizar a **exportação e importação individualizada das configurações de seus módulos**, proporcionando maior flexibilidade e agilidade na administração da solução. Dessa forma, não é necessário executar um processo de restauração completa do sistema quando houver a necessidade de recuperar ou transferir apenas configurações, dados ou tabelas específicas de determinado módulo.

As configurações podem ser exportadas e posteriormente importadas de forma seletiva, facilitando processos de **backup, migração, replicação e recuperação de configurações**, sem impactar os demais componentes da solução.

Por padrão, o MailInspector disponibiliza a exportação das configurações em, no mínimo, um dos seguintes formatos:

- **XML**;
- **CSV**.

Essa abordagem permite ao administrador maior controle sobre os dados e configurações que serão exportados ou restaurados, reduzindo a complexidade operacional e o tempo necessário para manutenção e recuperação do ambiente.

Formas de uso do MLI

O HSC MailInspector possui Sistema Operacional próprio, o "HSC OS", que pode ser instalado em 32 ou 64 Bits (depende unicamente de o cliente solicitar qual das versões desejadas), customizado, especializado e otimizado para trabalhar como e-mail gateway, provendo maior segurança e robustez para operações do produto, sendo compatível com os principais fabricantes de Hardwares e sistemas de Virtualização do mercado. O sistema operacional HSC OS já vem “pré-hardenizado” para melhor proteção e desempenho específico para sistema de proteção a e-mail.

O HSC MailInspector pode administrar mais de 300.000 usuários em uma mesma console de administração podendo receber/enviar mais de 500.000 e-mails por hora (de fato não possui limitação de e-mails enviados e recebidos, dependendo unicamente de número de pontos de filtragem utilizados e capacidade de hardware disponibilizado), sem enfileiramento ou retenção na entrega/envio e suportando mais de 30.000 (trinta mil) conexões simultâneas por ponto de acesso (por node).

O desempenho do MailInspector depende da configuração (número de pontos de filtragem, tamanho de disco utilizado, número de processadores reservados e quantidade de memória reservada ao sistema) disponibilizada pelo administrador.

Como Software

É possível a instalação direto no equipamento (baremetal) como software. Para isso, basta o administrador efetuar boot baseado no ISO disponibilizado pela HSCBRASIL. É importante lembrar que o equipamento utilizado deve ser homologado pela HSCBRASIL.

Como Appliance Físico

Solução em hardware customizado de alta performance. Maior desempenho e comodidade de instalação.

Em Virtual Appliance

Solução completa compatível com os principais sistemas de virtualização do mercado, entre eles:

- VMWare 5 ou superior (VSphere, vCloud, ESX e ESXi);
- Microsoft Hyper-V 2008R2 ou superior;
- Citrix Xen Server 5 ou superior;
- Red Hat OpenShift 4.14 ou superior;
- Red Hat Virtualization 3.1 ou superior;
- KVM;
- Oracla VM VirtualBox 4.0.4 ou superior;
- Nutanix Hyperconvergence Acropolis;
- Microsoft Virtual PC 6.0 ou superior;
- Parallels Desktop 7 ou superior;
- Entre outros

Todos os sistemas virtuais podem trabalhar em 32 ou 64 bits, conforme a sua necessidade.

A instalação em Virtual Appliance caracteriza-se pelo uso do sistema operacional próprio da HSCBRASIL (HSC OS) e pela disponibilidade de virtual appliance já pré-configurado (padrão OVA – consulte o suporte para a disponibilização do arquivo).

Integração com Sistemas padrão Office (Microsoft, G-Suite e Zimbra)

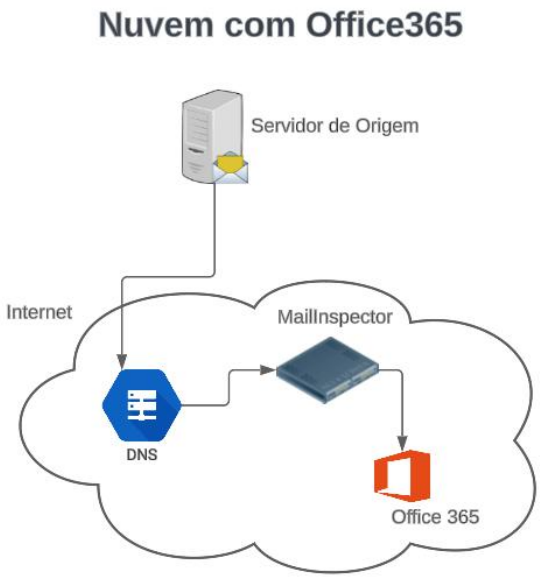
Atualmente várias empresas utilizam sistemas de e-mail integrado ao sistema colaborativo Microsoft e Google, sendo que o MailInspector é totalmente compatível a ambas as plataformas e integra-se de várias formas, desde uso de APIs, autenticação direto pelo Office365/G-Suite, sistema de orquestração (SOAR) e até redirecionamento de e-mails, sem a necessidade de mexer no DNS da empresa.

Além de todas as proteções do MailInspector sobre os e-mails de entrada/saída, a integração com Office365/G-Suite/Zimbra também conta com:

1. Remoção/edição de qualquer e-mail entregue diretamente na caixa do usuário;
2. Bloqueio da conta do usuário diretamente pelo MailInspector, dispensando o acesso ao Office365/G-Suite/Zimbra;
3. Permite ainda que o administrador faça:
    a. Bloqueio de acesso aos anexos contidos no e-mail;
    b. Bloqueio do conteúdo do e-mail;
    c. Envio do e-mail para a pasta de SPAM/Lixeira Eletrônica;
    d. Remoção dos links contidos no e-mail;
4. Permite que seja disponibilizado ao usuário o gerenciamento de suas próprias quarentenas, diretamente na interface do WebMail do Office365/G-Suite/Zimbra e/ou Outlook 2019 ou mais recente;
5. Integração de acesso do MailInspector com a autenticação pelo Office365, com a opção de uso de múltiplo fator;

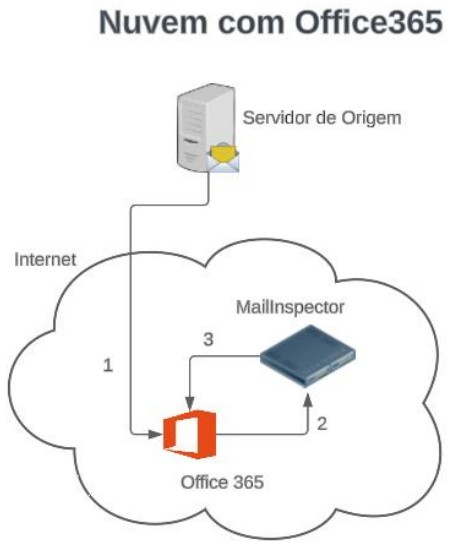
6. Basca fácil e eficaz de busca e gerenciamento dos e-mails, dessa forma não há a necessidade de acesso ao Exchange do Office365 ou Sistema de Gerenciamento de e-mails do G-Suite, para gerenciamento dos e-mails bloqueados e para os que foram entregues, pode-se utilizar o sistema *M-SOAR* / DeepIntegration;
7. Integração com o Office365/G-Suite, para entrega de e-mails mesmo sendo considerados Bulk Mails, mas com marcação de cabeçalho, para que eles caiam diretamente para a caixa de Lixeira Eletrônica ou pasta de SPAM;
8. Análise e proteção de ameaças em pastas públicas/pastas compartilhadas/shared mailbox;

Segue o desenho da solução padrão utilizado para a filtragem dos e-mails com a solução do MailInspector integrado com o Office365, com modificação do apontamento de MX no DNS da empresa.



Solução com redirecionamento dos e-mails pelo DNS da empresa

É possível efetuar o envio dos e-mails diretamente do Office365/G-Suite para o MailInspector, dessa forma dispensa-se qualquer modificação no DNS da empresa, bastando para isso, criar regras de movimentação dos e-mails no Office365/G-Suite.



Solução com redirecionamento dos e-mails sem necessidade de alteração do DNS da empresa

1. Os e-mails são direcionados ao Office365/G-Suite (que é o padrão quando se usa Office365 ou G-Suite), portanto, não há necessidade de mexer no DNS;
2. No Office365/G-Suite/Zimbra é feita uma regra para o redirecionamento dos e-mails de entrada para o MailInspector;
3. O MailInspector filtra os e-mails e devolve ao Office365/G-Suite/Zimbra;
4. Ao receber novamente os e-mails, verifica-se que são oriundos do MailInspector, então o Office365/G-Suite/Zimbra recebe-os, sem qualquer bloqueio, uma vez que os e-mails já foram filtrados (passaram pelo MailInspector);

Se optado pelo modelo de filtragem sem alteração do DNS da empresa, perde-se a camada de proteção de verificação de reputação do IP de origem, RBL e outras filtragens utilizadas na camada de conexão (uma vez que para o MailInspector, os e-mails vêm do Office365/G-Suite/Zimbra e não diretamente do servidor de origem, dessa forma não tem como averiguar o IP de origem), portanto, recomenda-se o uso do modelo com a alteração do apontamento de MX no DNS da empresa.

Monitoramento e Alerta

O **MailInspector** permite ao administrador realizar o **monitoramento contínuo e a geração de alertas em tempo real** sobre o comportamento e o volume de mensagens provenientes das diferentes origens de e-mail ou até mesmo de um único IP/remetente/destinatário e/ou rede de origem. A solução acompanha padrões de tráfego, histórico de conexões e indicadores de reputação, permitindo identificar comportamentos anômalos e potenciais fontes de ameaça antes que possam comprometer o ambiente.

Entre os principais indicadores analisados estão o **volume de mensagens**, o histórico de conexões realizadas pela origem, os endereços IP utilizados e a reputação associada a essas origens. Dessa forma, é possível verificar, por exemplo, se determinado IP já esteve envolvido em campanhas anteriores de spam, phishing, malware ou outras atividades maliciosas.

O sistema também mantém e correlaciona informações relacionadas ao histórico de mensagens **válidas e inválidas**, incluindo a taxa de aceitação de e-mails, ocorrências de limites de envio anteriormente excedidos, quantidade e frequência de conexões e utilização de **múltiplos endereços IP por uma mesma origem em períodos curtos**, comportamento que pode indicar comprometimento de infraestrutura ou tentativa de evasão dos mecanismos de proteção.

Adicionalmente, o MailInspector considera indicadores relacionados à presença de **vírus e malwares**, ao volume de mensagens classificadas como **newsletter**, sistemas de disparo previamente autorizados, além do histórico de **Bulk Mail e Greymail**. Essas informações são utilizadas em conjunto para estabelecer um contexto de reputação e comportamento para cada origem.

Com as informações de fluxo de campanhas a nível mundial, é possível gerar alertas sempre que disponíveis, informações relevantes sobre a campanha, incluindo sua **finalidade, comportamento e impacto potencial**, permitindo ao usuário compreender o risco associado à mensagem recebida.

Entre os objetivos que poderão ser apresentados, destacam-se:

- **Acesso remoto** ao dispositivo ou ambiente corporativo;
- **Instalação e execução de Ransomware**;
- **Roubo ou comprometimento de credenciais**;
- **Coleta e exfiltração de informações**;
- **Instalação de outros tipos de Malware**;
- **Comprometimento de contas ou sistemas corporativos**;
- Outras atividades maliciosas associadas à campanha identificada.

Com base nesses dados, o administrador pode configurar **limiares, critérios e políticas de alerta**, permitindo que a solução realize o monitoramento de forma contínua e gere notificações quando determinados padrões ou condições forem identificados. Essa abordagem proporciona maior **visibilidade sobre o comportamento das origens de e-mail, capacidade de detecção de anomalias e resposta preventiva a possíveis campanhas maliciosas**, de acordo com as políticas definidas para o ambiente. Os alertas configurados para disparo podem ser por:

- E-mail;
- Sistema de mensagem instantânea (Telegram);
- Sistema de coleta de logs (Syslog);
- Sistema de alerta de terceiros (tais como Zabbix, CACTI, Nagios, etc);
- SNMP;
- MIB II;

Suporte a cluster

Suporte a cluster de alta disponibilidade "Tolerância a falhas" e loadbalancing (o licenciamento abrange todos os nodes, sem custo adicional e sem limitação de número de nodes a serem adicionados ao cluster), permitindo os seguintes modos de funcionamento:

- Single View: Dois ou mais servidores trabalhando simultaneamente, replicando os recursos de quarentena, configurações, atualizações e registros de mensagens em banco de dados relacional. Desta forma o administrador visualiza todas as configurações, DLP, criptografia, e-mail compliance, relatórios, registros do banco de dados, quarentena, block list, allow list e demais recursos de forma unificada (em uma única console gráfica - GUI), garantindo que os mesmos dados estejam replicados em mais de um servidor. Este modo contempla alta disponibilidade e loadbalancing simultaneamente podendo ser adicionado quantos nodos forem necessários a fim de suportar a

carga de e-mails da sua empresa.

- Split View: Dois ou mais servidores trabalhando simultaneamente, replicando apenas os recursos de configurações e atualizações. Desta forma o administrador visualiza todas as configurações, block list e allow list de forma individual. Outros recursos como relatórios, registros de mensagens do banco de dados e quarentena são visualizados de forma individual por nodo do cluster.
  Este modo contempla alta disponibilidade e loadbalancing simultaneamente.

O cluster do MailInspector foi projetado para suportar mais de 7 milhões de mensagens por dia, sendo que em **cada ponto de filtragem (node)** possui capacidade de processamento de mais de 500.000* mensagens/hora (com todas as funcionalidades habilitadas e considerando as mensagens sendo do tamanho médio de até 300kB) sem gerar fila para atraso de entrega das mensagens ou retenção na entrega/envio, dessa forma se cai um ponto de filtragem (node) do cluster, o(s) outro(s) que assumir a carga, possuirá total capacidade para suportar todo o volume de e-mails.

O MailInspector possui capacidade de processamento de envio de mais de 100.000 (cem mil) mensagens com anexos de 50MB no intervalo inferior a 5 minutos, dessa forma garantindo envio massivo de e-mails, mesmo com anexos de grande porte.

O MailInspector permite configurações de conexão granular, sendo gerenciado por cluster e ponto de acesso.

O MailInspector não possui uma limitação quanto ao número máximo de caixas postais na solução, dessa forma o cluster já é projetado para suportar a número ilimitado de caixas postais (com todas as funcionalidades ativas e sem perda de desempenho). Para aumentar a capacidade de processamento e armazenamento, basta incluir novos nodes ao cluster que compõem a solução E-mail Gateway. Se um dos pontos de filtragem (node) ficar indisponível, a carga é automaticamente redistribuída entre os outros pontos de filtragem (nodes).

A solução conta com capacidade para instalação de múltiplos pontos de filtragem SMTP (nodes), sendo todos gerenciados por um único sistema administrativo centralizado via HTTPS, isto é, toda a administração dos componentes da solução é gerenciada de forma centralizada em uma única interface gráfica, sem necessidade de abrir múltiplas telas de gerenciamento.

O cluster utilizado pode ser configurado como ativo/ativo e ativo/passivo, em ambos os modos as configurações e os dados são sincronizados forma automática e com garantia de funcionamento da solução mesmo com a falha de ponto de filtragem, mantendo a fila de e-mails (queue) e processamento para entrega dos mesmos.

O controle da fila (em relação a continuidade do funcionamento), também cobre falha de conexão de saída, falha de conexão de entrega do e-mail ao servidor de e-mails da empresa, atrasos (TimeOut) e outros erros de entrega.

Tanto no modo ativo/ativo, quanto no modo ativo/passivo o MailInspector consegue manter a integridade dos dados mesmo quando houver queda de um dos nodes, garantindo dessa forma o funcionamento sem qualquer interrupção ou perda de informação.

O sistema em cluster (alta disponibilidade) proporciona:

- Sincronização dos e-mails e configurações, de modo seguro;
- Sincronização de políticas, regras, filtros e listas;
- Segurança de funcionamento, mesmo em caso de falha de rede;

A alta disponibilidade no MailInspector também é capaz de detectar e notificar falha de dispositivo/cluster, monitorando:

- Link do cluster;
- FailOver de Rede;
- Queda do node do cluster;

O Cluster do MailInspector pode ser formado por appliances físicos e virtuais simultaneamente, isto é, em um mesmo cluster, é possível encontrar nodes físicos e nodes virtuais.

É possível incluir mais pontos de filtragem no mesmo cluster, sem limites de quantidade de pontos a serem acrescentados e sem custo adicional ao cliente (o licenciamento adquirido já inclui instalação de número ilimitados de pontos de acesso/filtragem).

Caso utilize o cluster em modo passivo, todas a informações do nó em que houve a queda são acessíveis no nó passivo, incluindo as seguintes informações:

- Políticas de segurança;
- Regras de Filtragens;
- Listas;
- Configurações do cluster;
- Sistema de monitoramento;
- Mensagens na fila;
- Logs de MTA e de eventos monitorados pelo MailInspector;

* Pode-se ultrapassar ao número de 500.000 mensagens/hora, dependendo unicamente da configuração de número de processadores/quantidade de memória/tamanho de armazenamento disponibilizado pelo administrador da solução.

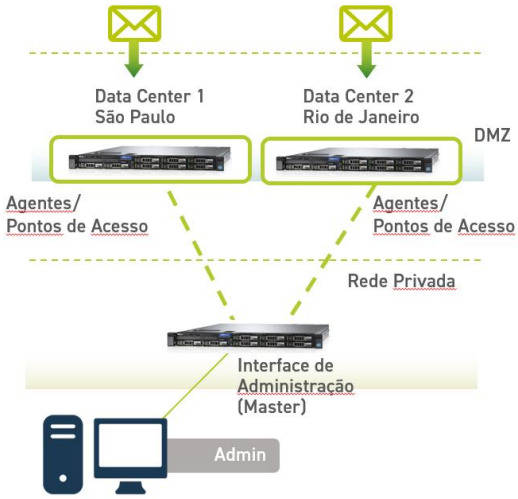
O licenciamento do MailInspector garante o roteamento das mensagens, com as configurações de filtragem e vacinas até a data do vencimento da licença, dessa forma, mesmo que a licença esteja vencida, o MailInspector continua filtrando os e-mails, de forma “parcial”, pois não terá as últimas assinaturas de vacinas, nem de outras atualizações (somente as assinaturas e atualizações até a data de vencimento da licença). O administrador também perde o acesso ao sistema de gerenciamento das mensagens, bem como qualquer configuração na caixa.

É possível efetuar a instalação do MailInspector com múltiplas interfaces de rede e/ou múltiplos IPs atreladas a solução, segmentando-os de acordo com a finalidade de cada um, por exemplo:

- Segmentação de rede para Gerenciamento da Solução;
- Segmentação de rede para Filtragem (SMTP);
- Segmentação para o VIP do Cluster;

Cluster em datacenters distintos

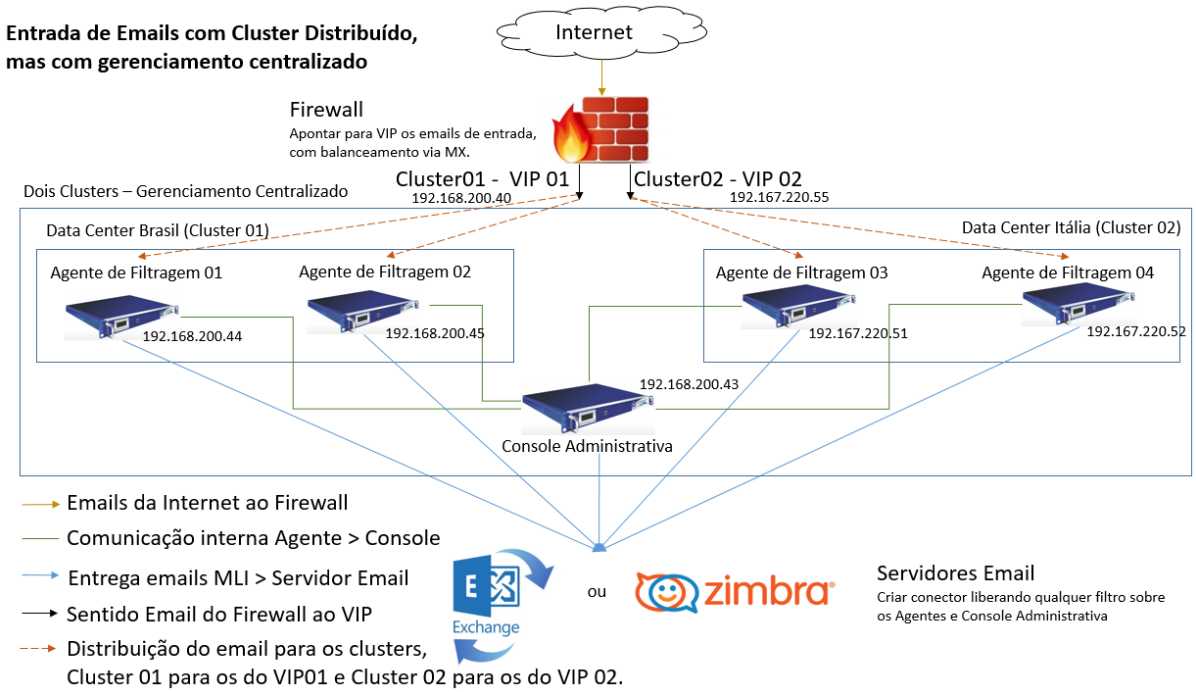
Os nodes de um mesmo cluster podem ser localizados fisicamente em datacenters distintos, sem perda de desempenho, uma vez que o cluster utiliza tecnologia de Virtual IP.



Modelo de implementação em Datacenters distintos

Múltiplos clusters em datacenters distintos

Além dos nodes de um mesmo cluster estarem localizados fisicamente em datacenters distintos, também é possível configurar múltiplos clusters na mesma solução, dessa forma é possível ter configurações distintas (inclusive com idiomas distintos) entre os clusters, por exemplo Cluster 1 em português e Cluster 2 em italiano.

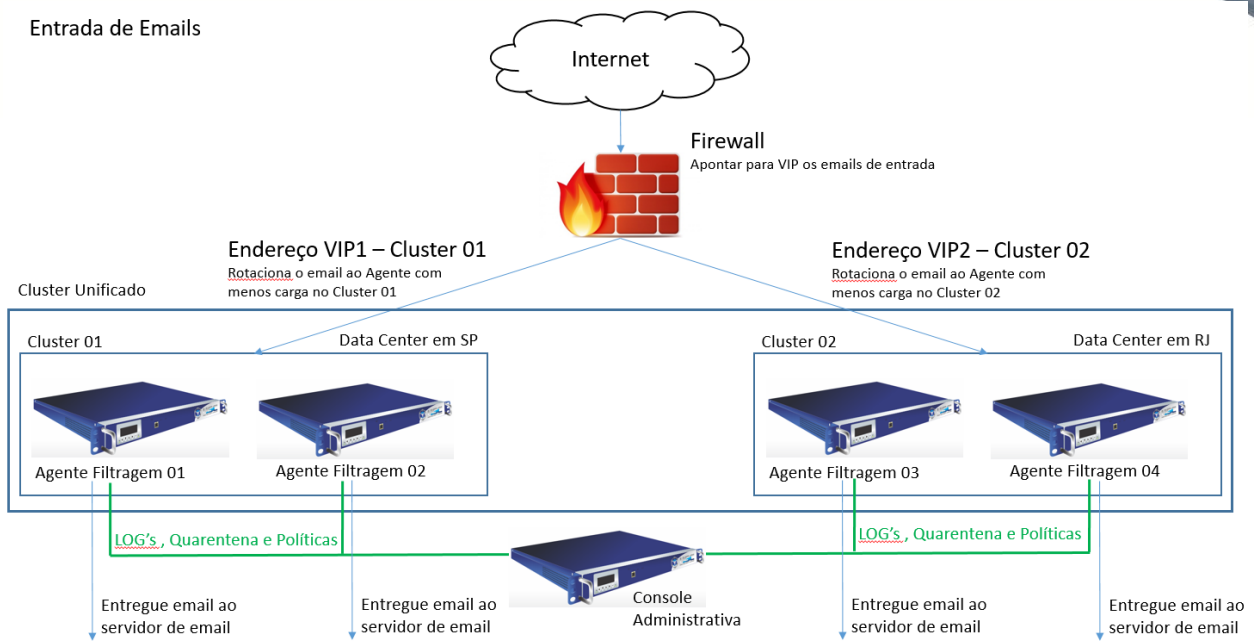


Exemplo de implementação de Cluster distribuído e em Datacenters distintos

Múltiplos Clusters Unificados

No MailInspector é possível também criar cluster "dentro" de clusters, ou seja, criar múltiplos clusters e unificá-los, dessa forma, mesmo sendo clusters separados, o sistema de gerenciamento é único e ao aplicar uma regra/política a mesma é distribuída a todo cluster e por consequência os "subclusters".

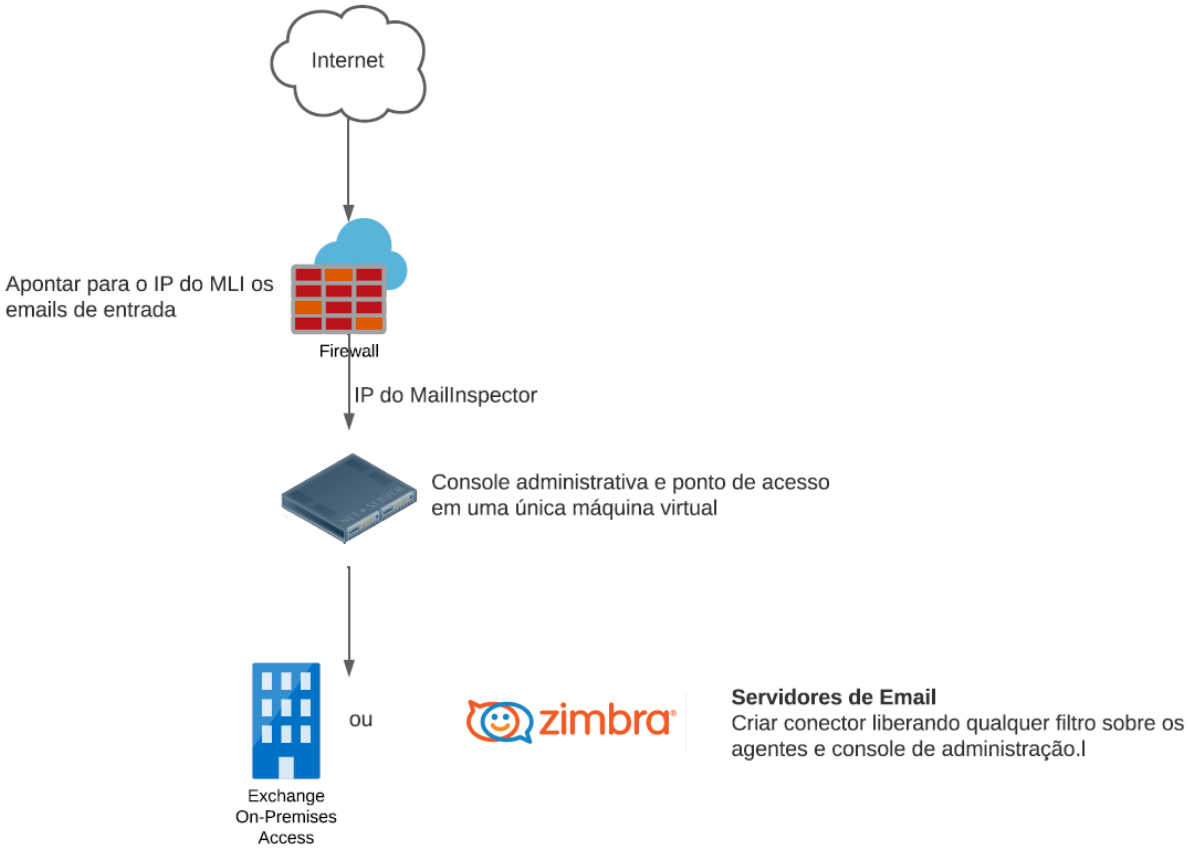
Todo o cluster é gerenciado em uma única interface, sem necessidade de criar novas instâncias para gerenciamento das regras e políticas.



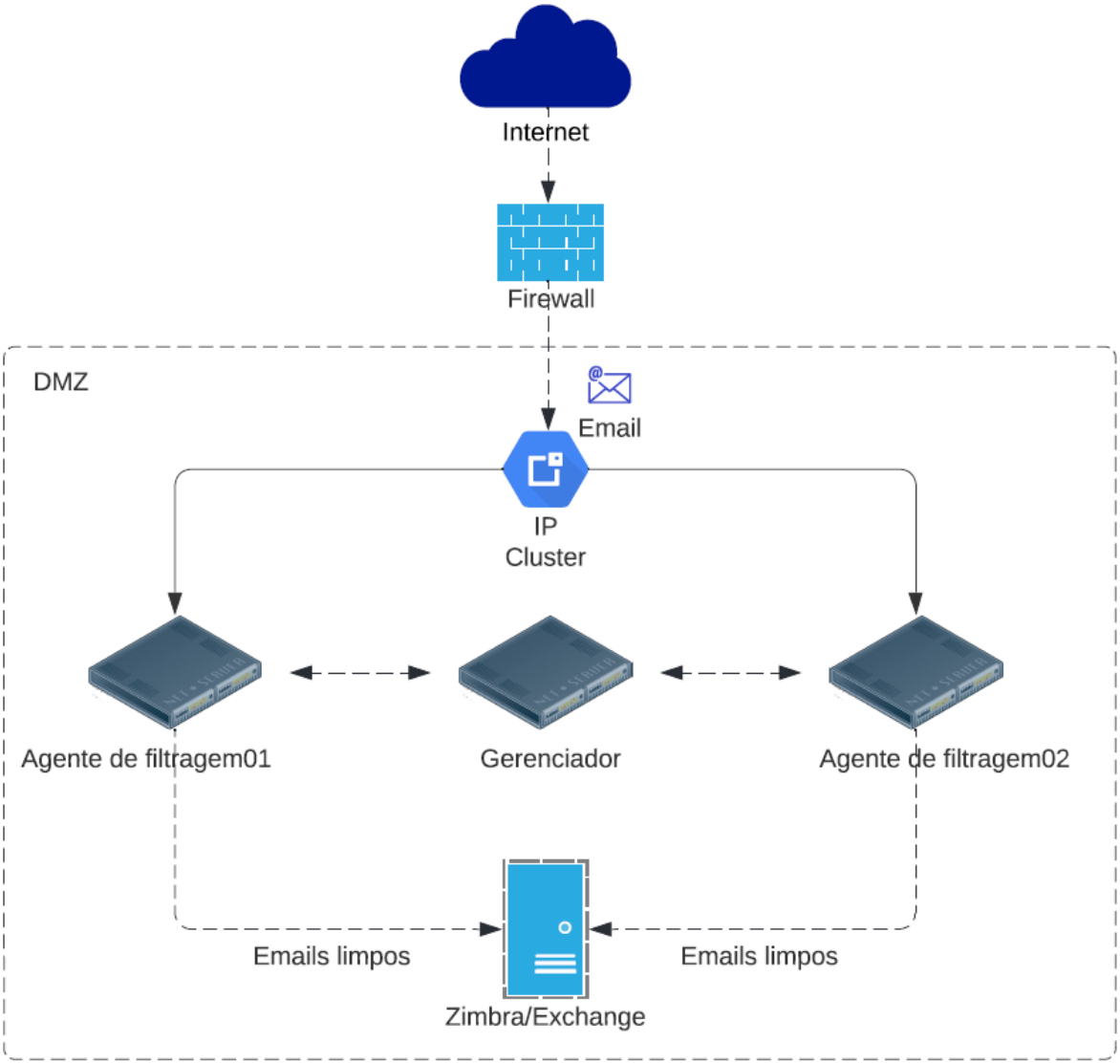
Exemplo de implementação de Cluster Unificado e em Datacenters distintos

Exemplos de Configuração do MailInspector

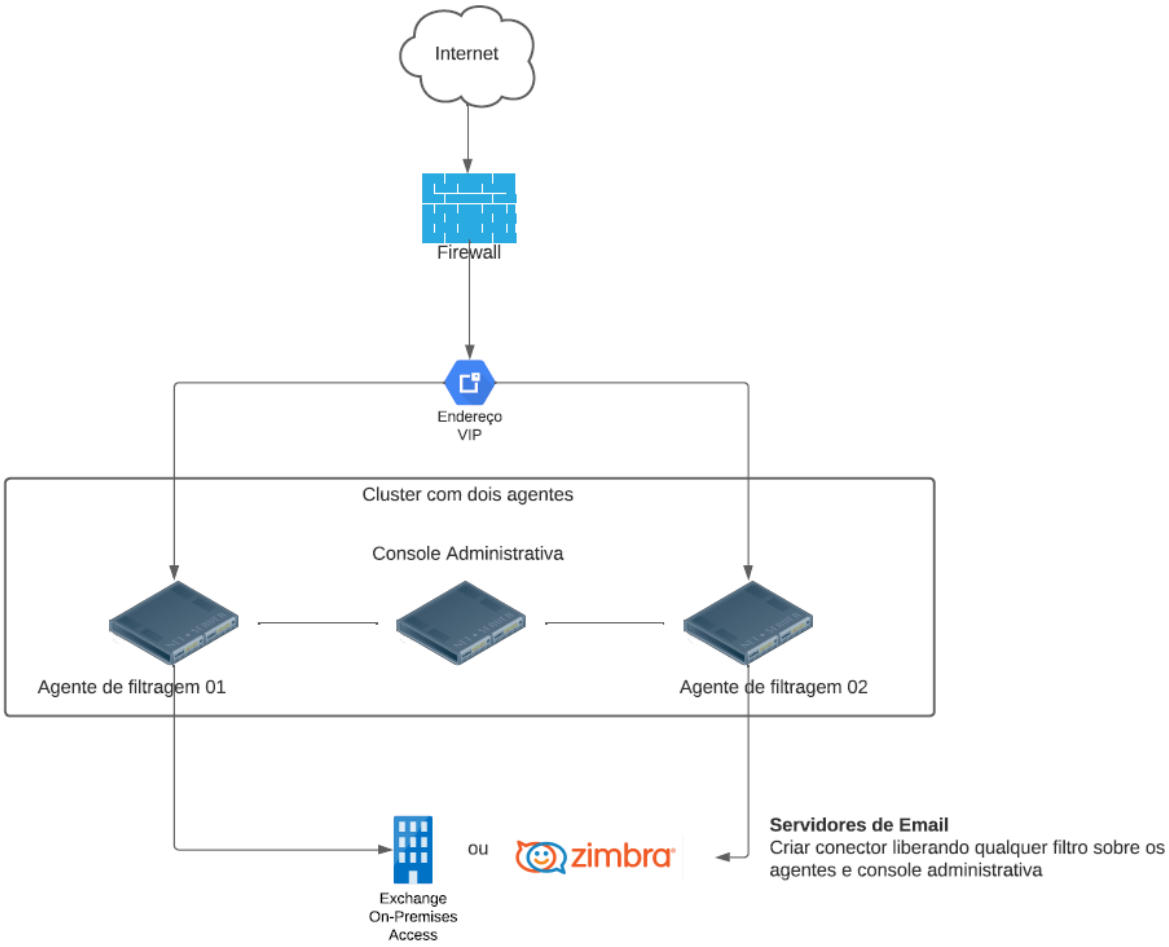
Toda a solução em uma única máquina (virtual ou físico)



Solução em cluster com dois pontos de filtragem em DMZ

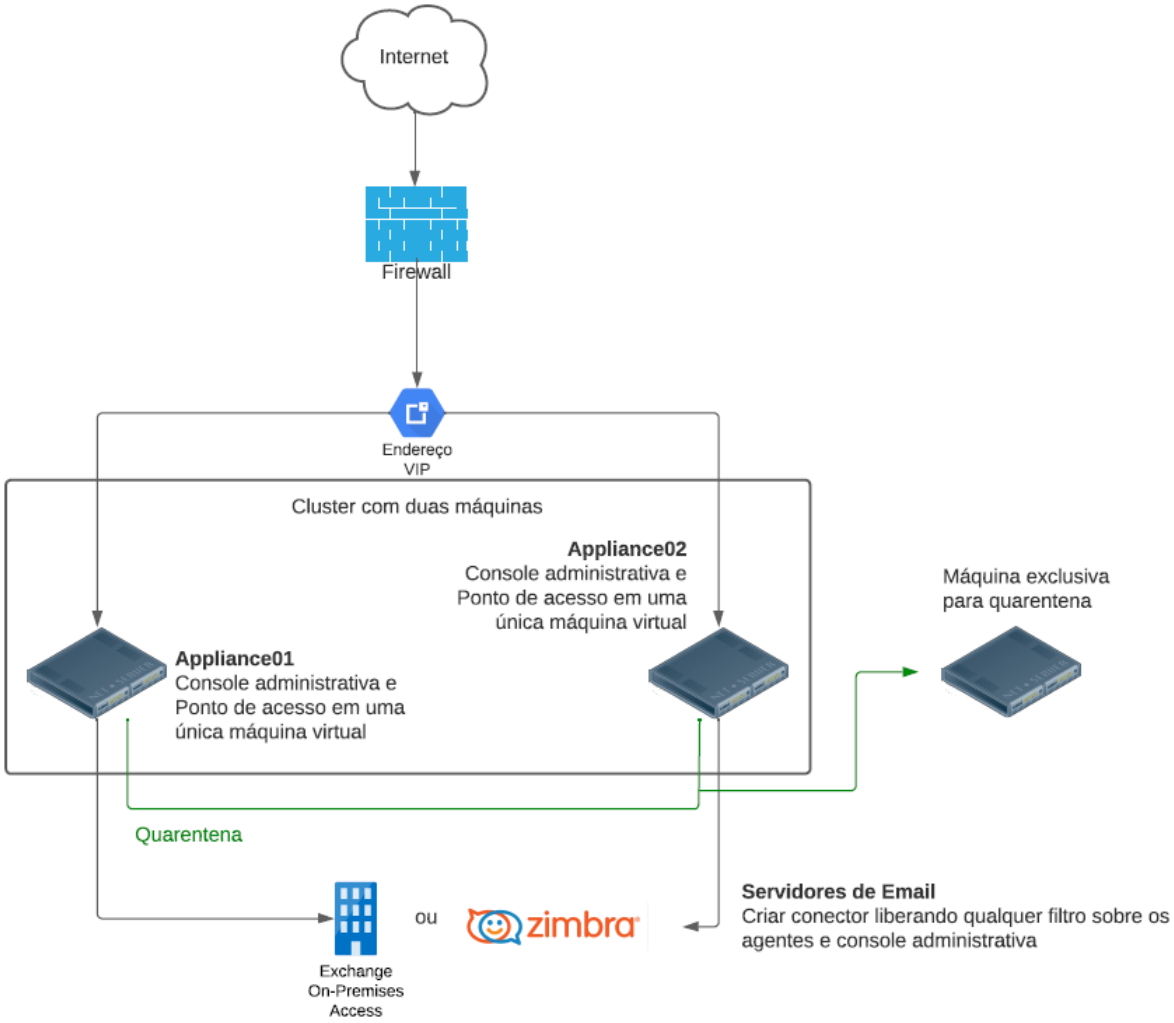


Solução em cluster com dois pontos de filtragem (nodes)



Solução em Cluster com duas máquinas completas (físico ou virtual) e quarentena separada

Instalação com duas administrações (unificadas, sendo gerenciado pela mesma console administrativa) e pontos de filtragem incorporada a cada uma delas, jogando a quarentena em outra máquina.



Solução com cluster e quarentena separada
Administração com logs centralizados

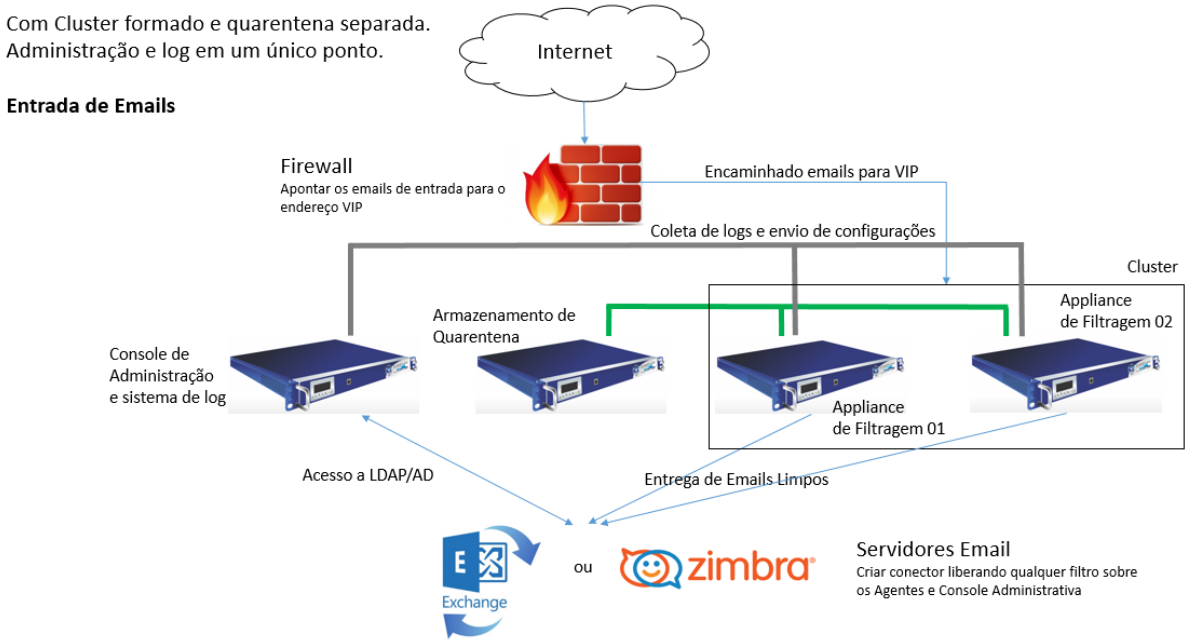
É possível criar um modelo de implementação, onde são instalados os pontos de filtragem, jogando a quarentena em outra máquina e os logs e a central de administração em uma terceira máquina, conforme desenho indicado.

Para esse processo, basta o administrador efetuar a instalação de duas consoles de administração e o restante como pontos de filtragem. Durante a criação do cluster, basta indicar qual dos dois consoles de administração será utilizado como área exclusiva de quarentena.

No desenho abaixo, foram instalados:

- Dois pontos de filtragem;
- Duas consoles de administração (uma delas foi elencada como Armazenamento de Quarentena).

Nos dois pontos de filtragem, foi formado um cluster e durante esta formação, basta indicar o IP da máquina montada para Armazenamento de Quarentena.



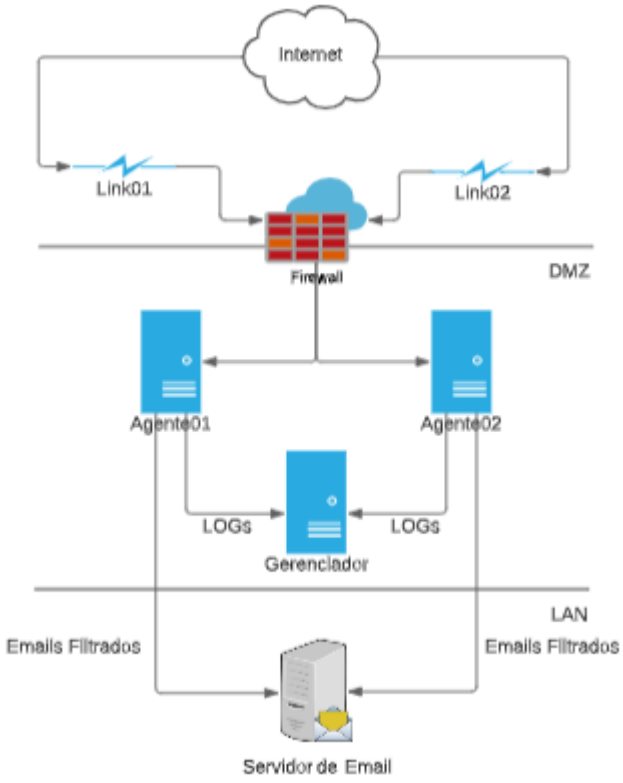
Obs: A máquina específica para o armazenamento de quarentena, pode ser um Storage externo com HBA e discos FC.

Solução com cluster em DMZ com servidor de e-mail na LAN

É possível criar um modelo de implementação, onde são instalados os pontos de filtragem e o gerenciador na DMZ e o servidor de e-mail na LAN.

Para esse processo, basta o administrador efetuar a instalação dos agentes e do gerenciador na DMZ e efetuar as devidas regras para entrega dos e-mails para o servidor de e-mail localizado na LAN, lembrando que é montado um cluster utilizando os agentes.

No firewall da rede da LAN, será necessária a criação de regras para entrega dos e-mails vindos dos agentes ao servidor de e-mail, bem como regra de firewall e NAT para o conector LDAP/Microsoft AD, entre o gerenciador e servidor de e-mail.



Implementação

Após selecionada o modelo a ser implementado, o impacto na produção é mínimo, ou seja, não há parada de recebimento/envio de e-mails, uma vez que o MailInspector somente entra em atividade após o redirecionamento dos e-mails para ele e ainda para termos uma segurança, é possível efetuar toda a configuração de política ANTES desse redirecionamento.

A expansão do ambiente também é de forma transparente, uma vez que se a solução já estiver trabalhando em cluster estabelecido, para a ampliação do mesmo, basta instalar novo ponto de filtragem e incluí-lo ao cluster, dessa forma aumentando a capacidade de processamento de e-mails, sem parada e nem impacto.

Durante a vigência do contrato de uso do MailInspector, a empresa terá direito a:

- Todas as atualizações de segurança;
- Atualização para última versão liberada do MailInspector;
- Atualização a todos os módulos do MailInspector;
- Atualização a melhorias;
- Acesso a base de inteligência do MailInspector (SmartDefender);
- Suporte técnico;

Integração com outros sistemas

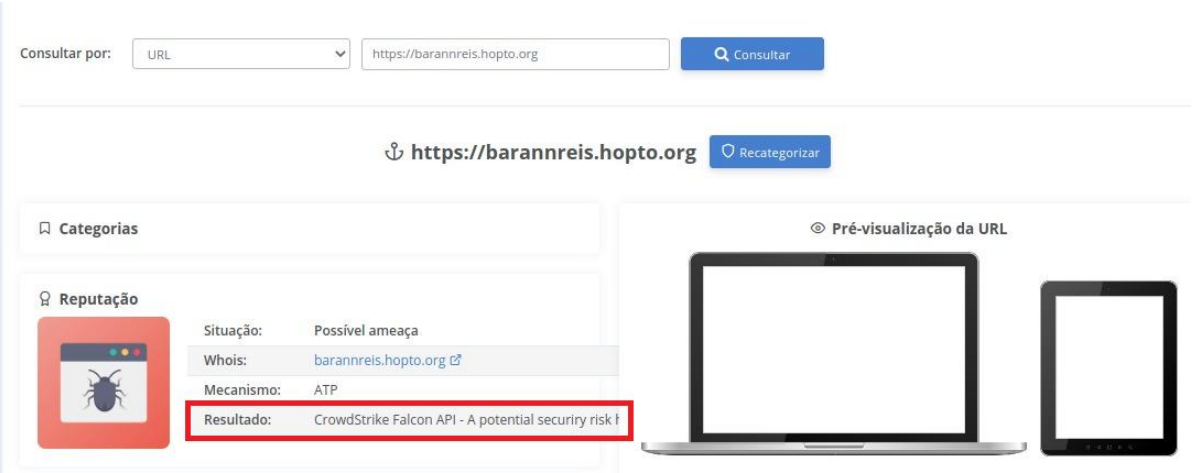
O MailInspector permite a integração com outros sistemas tais como SIEM (Security Information and Event Management), monitoramento ou sistemas de BI (Business Inteligence). Essa integração pode ser desde API's, exportação de dados, consulta direta via Banco de Dados relacional, instalação de agentes no MailInspector, exportação de LOGs/SYSLOG, protocolo SNMP, exportação em arquivos TXT/CSV, correlação através de template, envio de e-mails de alertas, disparo de mensagem instantânea (Telegram), entre outras diversas formas de integração.

Alguns sistemas suportados:

Ferramentas de BI	Ferramentas de SIEM	Ferramentas de Monitoramento	Outras Ferramentas
Microsoft Power BI®	SPLUNK®	Zabbix®	Servidor de Logs Kibana®
IBM Watson Analytics®	ArcSight®	Nagios®	OpenVas
Google Data Studio®	IBM QRadar®	Icinga®	ForeScout NAC EVAS®
Tableau®	Securonix®	Shinken®	Elastic Search
BIRT®	Exabeam®	Naemon®	Telegram
Entre outros	Alien Vault®	Cacti®	Entre Outros
	Microsoft® Defender	Entre outros	
	Sentinel®		
	Securonix®		
	RSA Netwitness®		
	Entre outros		

O uso de API para integração com diversos sistemas, abre um leque infinito de possibilidade de integração do MailInspector com diversas ferramentas presentes nas empresas. Com essa integração, o MailInspector passa a "conversar" com praticamente qualquer outro sistema de segurança, sendo desde anti-vírus, firewall, até sistemas de Detecção e Resposta Estendida (XDR), com inteligência e detecção de terceiros, tais como:

- CrowdStrike Falcon®;
- OneVision®;
- MVision®;
- FireEye XDR®;
- Cortex XDR®;
- Cynet 360®;
- Singularity XDR®;
- Cyber Defense Platform®;
- Symantec XDR®;
- Sentinel One ®;
- SecureX And Secure Endpoint®;
- Mandiant Automated Defense®;
- Carbon Black Cloud®;
- Intercept X Endpoint®;
- Rapid7 XDR®;
- CheckPoint Open Plataform for Security®;
- Palo Alto Panorama/Firewall®, integração através de PAN-OS e XML/REST API;
- Fortinet FortiGuard® / FortiXDR®;
- McAfee® IPS Network Security Plataform / Trellix IPS;
- McAfee® EndPoint / Trellix EndPoint
    - Endpoint Security Threat Prevention
    - Endpoint Security Adaptive Threat Protection
    - HIPS – Host IPS
    - Endpoint Security Firewall
- McAfee ePO®;
- McAfee Web Gateway®;
- Microsoft 365 Defender XDR®;
- Trellix XDR Plataform®;
- Trend Micro Vision One®;
- Diversos outros sistemas de segurança, integrando através de API;



Tela indicando integração do MailInspector com API da CrowdStrike Falcon®

Sistemas de Monitoramento

O MailInspector permite a instalação de agentes de monitoramento, para sistemas de terceiros, dentre os principais conhecidos do mercado, tais como:

- Zabbix;
- Nagios;
- Icinga;
- Shinken;
- Naemon;

Também é possível trabalhar com sistemas que não são necessárias instalação de agentes, tais como:

- Cacti (via SNMP v2 ou v3);

O MailInspector permite envio de alertas por sistema de mensagem instantânea, como:

- Telegram;

Como o administrador da solução possui privilégio para instalação de agentes/plug-ins na solução, o MailInspector é praticamente compatível com qualquer sistema de monitoramento remoto. Além de instalação de agentes/plug-ins, os dados do MailInspector podem ser exportados via SNMP v2 e v3, Syslog. Também é possível configurar o envio de dado de logs através de FTP e/ou SFTP em horário pré-definido.

O MailInspector ainda conta com integração com sistema SIEM (Gerenciamento e Correlação de Eventos de Segurança), ao qual permite que seja enviado os dados de logs e eventos para qualquer local desejado pelo administrador, bastando informar o IP/host e a porta utilizada.

Para uma maior comodidade, o sistema do MailInspector ainda conta com sistemas de dashboard, ao qual o administrador poderá criar qualquer tipo de painel para consulta em tempo real das informações sobre o appliance, desde número de mensagens na fila, consumo de rede, consumo de CPU/memória RAM, até mesmo sobre a quantidade e qualidade dos e-mails recebidos.

Além dos sistemas de monitoramento, o MailInspector possui integração com diversos sistemas, tais como SIEM e BI. Essa integração pode ser efetuada através de API's, acesso direto das informações ao Banco de Dados, exportação de tabelas, integração de tabelas existentes no MailInspector com a aplicação, interação com o sistema de gerência do MailInspector, SYSLOG, exportação de dados via CSV/TXT, SNMP, instalação de agentes no MailInspector (conforme anteriormente indicado), entre outros.

HSC MailInspector Archive

Permite que seja instalado um servidor exclusivo para administração dos Pontos de Acesso de filtragem de e-mails. Desta forma é possível configurar o sistema para coletar as informações dos registros de e-mails e quarentena, a fim de centralizar os dados para que os mesmos possam ser armazenados por períodos de tempo mais prolongados (definido pelo administrador). Este recurso é ideal para empresas que necessitam auditar e controlar os e-mails. O recurso de archiving pode ser incorporado ao sistema de DLP "Data Loss Prevention" aumentando a capacidade de controle.

Importante salientar que o sistema de Archiving engloba também os e-mails auditados, dessa forma todos os e-mails (tantos os que foram quarentenados, quanto aos que foram entregues), sejam arquivados de forma inteligente, separadas por tipo de e-mail. O MailInspector trabalha o Archiving tanto a nível de entrada,

quanto a nível de saída de e-mails, sendo todo gerenciado pela interface única do MailInspector via HTTPS, sem necessidade de módulo extra ou equipamento adicional.

Message Reputation

Algumas campanhas de SPAM e PHISHING partem de diversos servidores ao mesmo tempo, geralmente usando ataques "Command Control Centers, Zombies, Botnets", desta forma somente a reputação de origem "Sender Reputation" pode não ser o bastante para detectar e responder a um ataque em um curto período de tempo. Estes tipos de ataques são conhecidos como "Campanhas".

Pensando nisso, a HSC desenvolveu uma tecnologia de Reputação de E-mail!

Quando uma mensagem chega no seu MailInspector o sistema cria o metadado desta mensagem baseado em "Strings Tokens" e consulta a nuvem da HSC (usando o metadado, sem registro, nem identificação do cliente ou do e-mail). A nuvem da HSCBRASIL contabiliza quantas vezes este e-mail já foi visto e começa a criar uma reputação deste e-mail, quando ele chega a um número X ele automaticamente tem sua reputação colocada como ruim e todos MailInspector tem disponível esta informação (vale a pena ressaltar que o registro somente contém o metadado e a contagem de recorrência).

Além de uso da base de conhecimento entre caixas do MailInspector instaladas, o sistema de reputação também conta com análise de tráfego de Volume Global de e-mails, dessa forma, integrando as tecnologias das caixas de MailInspector com Global Threat Protection Network (SmartDefender).

A reputação analisada sempre é priorizada a relevância da reputação local (do appliance) de acordo com as peculiaridades da empresa e em segundo plano a reputação Global.

Com esta tecnologia o HSC MailInspector consegue responder em tempo real e aprender novas campanhas de SPAM e PHISHING, sem precisar de NENHUMA ASSINATURA para isto!

Com as informações da assinatura de Message Reputation, o MailInspector toma a decisão entre e-mail com reputação aceitável ou e-mail de reputação duvidosa, permitindo ao administrador ficar ciente e alerta de campanhas de ataques globais e ataques dirigidos. Para a resolução da assinatura de Message Reputation são analisados uma série de fatores, entre eles:

- Volumetria: Verifica o histórico de volume de e-mails enviados e recebidos, gerando tendência/comportamento de uso do e-mail (conforme já citado no texto anterior);
- Horário de disparo dos e-mails;
- Tipo de e-mail enviado;
- Tamanho médio do e-mail enviado;
- Listas de endereços IP de servidores de correio que são conhecidos por serem fontes de spam;
- Listas de endereços IP de servidores de correio que são conhecidos por serem fontes de phishing;
- Listas de endereços IP de servidores de correio que são conhecidos por serem fontes de ataques de ransomware;
- Listas de endereços IP de servidores de correio que são conhecidos por serem fontes de ataques que incluem malwares;
- Listas de endereços IP de servidores de correio que são conhecidos por terem sido utilizados para campanhas de ataques diversos;
- DUL (Dynamically Assigned IP – para detecção de listas dinâmicas de IP);
- ETL (Emerging Threat Block List – listas baseadas em ameaças detectadas por firewall);
- Análise de Inteligência Artificial: Com todos os indicadores acima mencionados, é feita uma análise da reputação, através de sistema de IA, registrando dessa forma o comportamento do remetente e tomando as devidas ações sobre pontuação/bloqueio do e-mail;

- Análise de Inteligência Artificial sobre os links/anexos: Análise de Inteligência Artificial sobre os links contidos no e-mail, seja link direto, como link por QRCode, verificando a reputação do link, classificação e comportamento;
- Comparação do e-mail recebido com campanhas de ataques globais;

HSC SmartDefender

O HSC SmartDefender, é um dos módulos de proteção existente na solução MailInspector, sendo solução única e exclusiva da HSCBRASIL, que faz a análise local dos arquivos e URL's, em uma segunda etapa a comparação dos metadados gerados localmente na nuvem da HSCBRASIL e em terceira etapa efetua a comparação desses metadados com a rede global de múltiplos fabricantes.

O HSC SmartDefender trabalha em dois planos:

1. HSC SmartDefender Local;
2. HSC SmartDefender Cloud;

Alguns módulos da HSC SmartDefender podem ser executados localmente ou em nuvem, de acordo com a configuração efetuada pelo administrador, ou seja, o próprio administrador pode escolher onde executar esses módulos:

- NetWork SandBox: Também conhecido como Behaviour Analysis.
  Esta avançada técnica de detecção vai onde as demais técnicas não conseguiram detectar, ela se baseia em rodar os anexos em um ambiente controlado (emulando múltiplos sistemas operacionais, tais como: MacOS, Windows, Linux e Android) e analisar o comportamento do aplicativo (desde arquivos do pacote Office, pacote padrão Open Office, até APK's do Android) a fim de detectar comportamentos maliciosos, sem a utilização de uma base de assinaturas, dessa forma detectando e bloqueando novos ataques (Zero Hour).
  Entre as diversas técnicas de analises que rodam nesta cama podemos citar:
  - Following activities;
  - File system;
  - Evasion techniques detection;
  - Registry;
  - Process, network;
  - System calls;
  - Memory Analysis, etc.

  Esta camada pode rodar tanto na nuvem da HSC ou no Appliance Local do cliente de acordo com a preferência do administrador.

HSC SmartDefender Local (no ponto de filtragem)

O SmartDefender processa os SPAM's recebidos e gera automaticamente novos filtros e assinaturas tornando o combate a novas ameaças mais rápido e eficaz. Além do recurso de segurança, o SmartDefender ainda conta com:

- Engine proprietária de antivírus:
  A HSC Brasil tem engine própria onde são alimentados diariamente com novas vacinas, registros de IOC's e IOA's, além de contar com o próprio sistema de BigData interligado através de rede global da HSCBRASIL. A engine proprietária tem capacidade de detectar ameaças de dia zero/zero hour, vulnerabilidades conhecidas e outras ameaças usadas em ataques direcionados;
- É possível (opcionalmente) ativar a segunda engine de antivírus no ponto de filtragem (ESET), parametrizando de acordo com a necessidade do administrador, deixando-o mais ou menos sensível na detecção de ameaças.

- Local File SandBox: Também conhecido como Static Analysis, o file sandbox roda localmente no próprio appliance do cliente e traz avançadas técnicas de análises de engenharia reversa de malwares, tais como:
    - "Disassembler": Roda o executável e busca o código fonte de execução em tempo real;
    - Detecção real de File Type;
    - Strings Encoded;
    - Obfuscations techniques;
    - File Reputation (local por assinaturas);
    - Hash Comparison;
    - Fuzzy Hashes Comparison;

  A análise do Local File SandBox é totalmente local e baseada em assinaturas.

O módulo de SmartDefender também é responsável pela análise de imagens pornográficas com técnicas de redes neurais, sistema de Machine Learning, Inteligência Artificial e Deep Learning.

O Mailinspector verifica se a imagem está cadastrada em uma rede global de imagens pornográficas. Após essa verificação, é acionado o modelo de Inteligência Artificial, que através de métodos de machine learning, modelos matemáticos, redes neurais e deep learning, verifica de forma automatizada diferentes parâmetros da imagem (incluindo o contexto da mensagem), para que se possa detectar a probabilidade da imagem ser um conteúdo pornográfico.

Para a análise da imagem pornográfica são considerados vários parâmetros, dentre eles:

- Cor da pele;
- Tamanho da imagem analisada (cobertura) em relação ao tamanho total;
- Curvatura do corpo;
- Comparação da imagem com o fundo;
- Comparação da imagem com o contexto do e-mail;
- Controle granular da imagem;
- Se a imagem possui outros elementos humanos, tais como outra pessoa nua, partes do corpo humano, etc;

O sistema de análise de imagem, detecta imagens em diversos formatos, inclusive verificando a imagem original em arquivo por FileType e MIME Type, junto ao corpo do e-mail e em anexos. Também é verificado spams em formato de imagem, utilizando técnicas avançadas, entre elas a granularidade. Ainda em relação a imagens, o MailInspector detecta imagens dentro de arquivos padrão Office e em arquivos compactados (com controle sobre taxa de compactação, chegando a limite de 300 e controle de número de arquivos em um arquivo compactado, podendo chegar até 500), incluindo controle sobre número de subarquivos em arquivos padrão Office (permite até 500 subarquivos) e detecção de links contidos dentro de imagens, além de permitir ao administrador a utilização de allow list/block list de imagens e outros tipos de arquivos.

Segue abaixo algumas extensões detectadas automaticamente no sistema de imagens (tanto em imagens pornográficas e adultos, quanto em imagens de SPAM/propaganda/phishing):

- JPEG
- TIFF
- PNG
- AVIF
- WEBP
- JPG
- GIF
- PDF
- EXIF
- Entre outras extensões
- BMP
- TGA
- EPS
- PSD
- PCX
- ICO
- SVG
- RAW

HSC SmartDefender Cloud (na nuvem da HSCBRASIL em datacenter no Brasil)

De forma online e com funcionamento 24x7, feeds de segurança da rede mundial (através de parceria com diversos fabricantes), contendo listas de URLs não confiáveis (block list), listas de URLs confiáveis (allow list), IP's e faixas de IP's comprometidos e confiáveis, listas de equipamentos comprometidos, dados analíticos de volume tráfego, reputação da origem de e-mails (recebendo amostras e análises de mais de 200 milhões de senders), histórico e categorização de sites são analisados e disponibilizados instantaneamente pelo sistema, a fim de bloquear a proliferação de vírus, spam, websites maliciosos, malwares, phishing, ransomware, trojans e outras ameaças, impedindo que estes sites e e-mails infectem ou roubem informações dos computadores da sua rede.

O sistema de reputação contida no módulo SmartDefender utiliza BigData, baseado em modelos estatísticos (da HSCBRASIL e de outros fabricantes) e outros sistemas, já incluindo DUL (Dynamically Assigned IP – para detecção de listas dinâmicas de IP) e ETL (Emerging Threat Block List – listas baseadas em ameaças detectadas por firewall), dessa forma, ela é constantemente atualizada detectando ameaças crescentes na sua origem.

O sistema HSC SmartDefender Cloud retorna as informações sobre:

- Sistema de reputação online, mas permitindo que a reputação local definida pelo administrador se sobreponha a reputação apresentada pelo MailInspector;
- Categorização de websites por assuntos;
- Assinatura de detecção de aplicativos web;
- Controle de ameaças;
- Fontes de SPAM;
- Assinatura de Vírus;

O SmartDefender é totalmente integrado com o MailInspector, dessa forma garantido maior fidelidade na informação, não somente quanto a análise do e-mail, imagens e documentos, DNS reverso, verificação de IP em WHOIS, fluxo de e-mail do emissor, mas também quanto a reputação de origem, conforme listas e históricos do emissor, dessa forma é possível comparar a situação atual da reputação do emissor com o histórico dele, verificando se é um caso isolado de ataque ou se é, ou era fonte constante de ameaça.
O SmartDefender faz consulta a múltiplas bases de dados na HSCBRASIL, dentre elas:

- Base de reputação;
- Base de assinaturas de ameaças;
- Base de assinaturas de spam;
- Base de fluxo de origem;
- Base de RBL (RealTime Blackhole List/Know Spam Source) / ORBL (Open RBL's) / DNSBL-DNS Blacklist, utilizando dados importados de Big Data externos (antivirus, listas de RBL, etc), quanto de dados coletados das interações do SmartDefender com diversos sistemas de MailInspector instalados;
- Base de nawsletters;
- Base de mail marketing;
- Base de domínios conhecidos;
- Base de categorias de website;
- Base de assinaturas de aplicativos web;
- Base de assinaturas com características anômalas de e-mail, tais como:
    - Remetente vazio;
    - Remetente sem domínio indicado;
    - Conteúdo vazio no corpo do e-mail;
    - Palavras desconexas no corpo do e-mail;

- País de origem suspeito;
- Entre outras peculiaridades;

O MailInspector permite ao administrador manipular as assinaturas das bases acima citadas, do jeito que o administrador desejar, influenciando na tomada de decisão sobre a confiabilidade do e-mail, por exemplo, modificar a pontuação de um e-mail, quando o mesmo vier sem remetente ou ainda modificar a reputação de um e-mail de acordo com o seu país de origem, ou somente bloquear o e-mail quando estiver no mínimo em duas ou mais de listas de RBL.

O SmartDefender Cloud utiliza múltiplas técnicas de proteção em tempo real, tais como:

- Categorização de Website: Detecta os links e verifica de qual categoria elas pertencem, pontuando o e-mail de acordo com a classificação do site, por exemplo: Se o e-mail possuir link para sites com conteúdo de pedofilia, ou conteúdo adulto, ele poderá receber maior pontuação (de acordo com a decisão do administrador da ferramenta);
- Reputação de e-mail: Verifica se o e-mail está vindo de um emissor com boa reputação ou não, permitindo ao administrador decidir o que fazer com o e-mail caso ele esteja vindo de uma reputação ruim;
- Reputação do domínio: Através de Redes Neurais e consultas a bases internacionais com os parceiros fabricantes, é detectado o nível da reputação do domínio emissor do e-mail em tempo real.
- URL Sandbox: Abre em uma sandbox o destino da URL e faz os testes onclick, verificando o comportamento de toda a URL. Também é reservando localmente o metadado do resultado. É possível (opcionalmente) o administrador indique a consulta de esse metadados em nuvem Global de URL's, para maior precisão do resultado da análise efetuada. O metadados gerado é em SHA-1.
- URL Reputation: É verificada a reputação de todas as URL's contidas no e-mail, principalmente para prevenção de phish attack.
- Hash e Fuzzy Hash: No caso de metadados dos anexos, é feita a comparação utilizando técnicas de *Hash* e *Fuzzy Hashing*, garantindo maior certeza do resultado e detectando possíveis variações dos anexos (detectando dessa forma possíveis variantes de malwares, antes mesmo de criação de vacina). Também é feita a identificação de metadados já presentes nos arquivos, para verificação de reputação desses dados em compração com o resultado de técnica de hash e fuzzy hashing.
- File Reputation Global: O sistema verificação da reputação de arquivos utiliza o metadado gerado anteriormente no Local File SandBox para comparação com BigData, tendo com resultado se o anexo já foi registrado anteriormente como ameaça ou não.
- Proteção a sistemas Stealth (técnica de tentativas de inserção de instruções maliciosas ocultas em conteúdos de mensagens de e-mail): O MailInspector por contar com duplo SandBox (virtual e físico), consegue efetuar dupla varredura sobre os sistemas que utilizam sistemas Stealth, para burlar a camada de SandBox. Com o uso de Inteligência Artificial, focando em Machine Learning, o MailInspector além de conseguir efetuar o bloqueio, o sistema aprimora a curvatura de aprendizado para esse tipo de ataque emergente.

Algumas técnicas de Stealth que o MailInspector detecta e neutraliza:
Texto invisível: O texto malicioso usa a mesma cor do fundo do e-mail (por exemplo, letras brancas em fundo branco).
Fontes microscópicas: O tamanho da letra é reduzido para zero ou para um tamanho tão pequeno que o olho humano não consegue enxergar.
Esconderijo em HTML: O comando perigoso é inserido no código do e-mail (em áreas de metadados ou comentários) que o programa de correio eletrônico processa, mas o usuário não vê na tela.

- O SmartDefender conta com integração com sistema de antivírus da HSCBRASIL, bem como integração com outros fabricantes de antivírus, detectando códigos de ataques do tipo Fileless,

protegendo-se de ataques Stealth tanto na camada de SandBox, quanto na camada de antivírus, classificado esse tipo de ataque como Advanced Threat Attack.

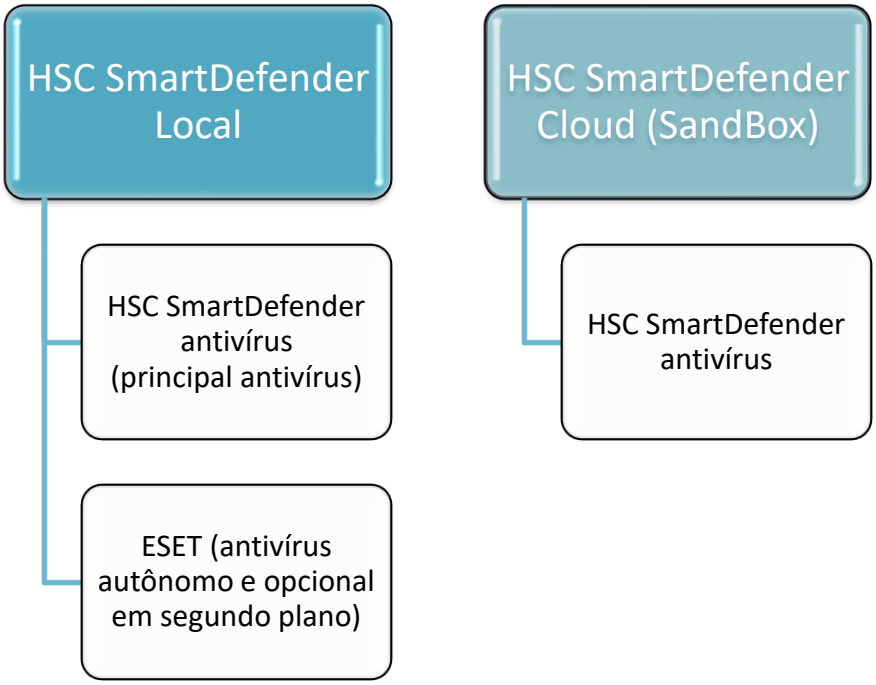
Obs: Todos dados enviados a nossa nuvem seguem as mais restritas regulamentações do mercado, os dados são enviados de forma anônima e criptografada, a HSC não salva o conteúdo do arquivo, depois de sua execução os dados são automaticamente removidos.

Antivírus presentes no MailInspector

A HSCBRASIL possui sistema proprietário de antivírus (HSC SmartDefender antivírus), ou seja, é a própria HSCBRASIL que fornece o antivírus e opcionalmente, o administrador pode ativar e configurar uma segunda engine de antivírus (de outro fabricante – ESET), dessa forma tendo múltiplas engines de antivírus na ferramenta e com total autonomia do administrador escolher se deseja ativar ou não o sistema de múltiplo engine.

É importante salientar que essa segunda engine de antivírus, é somente utilizado no HSC SmartDefender Local, pois no HSC SmartDefender Cloud é utilizado o HSC SmartDefender antivírus.

Todos os antivírus ativados são executados simultaneamente, sem perda de desempenho do sistema.
Em termos de antivírus temos no MailInspector:



O sistema de BIGData da HSC cataloga diariamente mais de **2 Bilhões** de eventos de segurança "IOC´s" por dia, além de possuir no cadastro de mais de **200 Milhões** de senders (remetentes) maliciosos. A HSCBRASIL trabalha em conjunto com outros fabricantes de antivírus, dessa forma, é importado a base de assinaturas de ameaças desses fabricantes, incorporando essas assinaturas a própria base da HSCBRASIL. Com isso é importado mais de 1 trilhão de assinaturas de ameaças. Esse número é acrescido a base da HSCBRASIL, que **inicialmente já era de mais de 1 Bilhão** de assinaturas.

Em tempo real, os dados são analisados instantaneamente pelo sistema, a fim de bloquear a proliferação de vírus, ransomware, malwares, phishing, spear-phishing, spams, trojans, APTs (ameaças persistentes

avançadas) e outras ameaças, impedindo que estes sites ou e-mails infectem ou roubem informações dos computadores da sua rede. Uma das camadas de proteção que as engines de antivírus utilizam é a camada de SandBox virtual, ao qual é executado o arquivo em uma área segura e isolada da memória para análise comportamental do mesmo, dessa forma apresentando o resultado da análise em tempo real.

Em termos de antivírus, o administrador pode ativar uma segunda engine de outro fabricante (ESET) e configurar de acordo com a sua necessidade o nível de detecção dessa engine, dessa forma deixando-a mais rígido na detecção de ameaças.

O **MailInspector** conta com a proteção do antivírus proprietário **HSC SmartDefender**, que utiliza mecanismos avançados de detecção de ameaças **Zero-Day/Zero-Hour**, incluindo **Emerging Threat List (ETL)** e análise heurística, para identificar ameaças ainda desconhecidas ou para as quais não existem assinaturas de detecção disponíveis.

Como camada adicional de proteção, o sistema permite **reter temporariamente as mensagens identificadas como potencialmente maliciosas em uma quarentena**, por período configurável pelo administrador. Durante esse período, a mensagem permanece impedida de ser entregue ao destinatário, possibilitando que novas assinaturas ou informações de inteligência sobre a ameaça sejam disponibilizadas e utilizadas em uma nova análise.

Após o período de retenção, o sistema poderá realizar uma **nova verificação da mensagem**, de acordo com as políticas configuradas pelo administrador, permitindo determinar se ela poderá ser liberada ou deverá permanecer bloqueada.

Os mecanismos tradicionais de antivírus, baseados exclusivamente em assinaturas, já não são suficientes para garantir, de forma isolada, a proteção dos ambientes computacionais das organizações.

Novas ameaças e variantes de malware surgem continuamente, muitas vezes antes que existam assinaturas capazes de identificá-las. Para enfrentar esse cenário, é fundamental contar com mecanismos avançados de **detecção e análise em tempo real**, capazes de identificar comportamentos e padrões associados a ameaças emergentes.

A dependência exclusiva de assinaturas limita a capacidade de resposta diante de ameaças desconhecidas, ataques direcionados e variantes ainda não catalogadas. Por isso, uma proteção moderna deve combinar diferentes técnicas de análise, permitindo **detectar, identificar e responder automaticamente** a comportamentos potencialmente maliciosos.

A abordagem é simples: Analisar, Identificar e Responder — de forma automatizada e em tempo real.

O HSC SmartDefender antivírus é a tecnologia de detecção e reposta a ameaças sofisticadas, trabalhando com múltiplas etapas, passando pelas seguintes etapas:

- Verificação por assinatura;
- Comparação por Fuzzy Hash para detecção de possível malware polimórfico;
- Verificação por reputação;
- Verificação por SandBox (com múltiplos sistemas operacionais) e Heurística;

Tudo em tempo real, sem depender somente de sistemas de assinatura.

Os sistemas de antivírus possuem detecção e bloqueio, tais como:

- Sistemas de anti-evasão de SandBox (detecção de máquina virtual, delay na entrega do e-mail, geolocalização, etc);
- Sistemas de anti-evasão de análise heurística;

- Algoritmos avançados para detecção e prevenção de análise comportamental agressivo;
- Sistemas de prevenção de malwares avançados;
- Ferramentas para descoberta de senhas;
- Sistemas de coleta de usuário e senha;
- Sistemas de bloqueio acesso da memória;

A HSCBRASIL, além da Engine própria (HSC SmartDefender antivírus) também conta com a Engine da ESET (já licenciada e de uso opcional para aumento de segurança), além de estar presente em organizações do mundo inteiro, é uma das mais consagradas e premiadas do mercado. Já foram reconhecidas com premiações por vários anos seguidos em diferentes instituições como:

- AV Comparatives;
- AV Test;
- Virus Bulletin (VB100 e VBSpam+);
- CRN entre outros.

Para a nuvem de SandBox (HSC SmartDefender Cloud), o MailInspector utiliza o antivírus próprio (HSC SmartDefender antivírus). A base de amostras contém mais de 1 trilhão e é constantemente atualizado com os mais de 500 milhões de dispositivos que reportam constantemente novas ameaças. Somente na parte de Ransomware, o nosso BigData conta com mais de 2,8 milhões de amostras.

O MailInspector possui integração com o sistema YARA, que auxilia na pesquisa e na detecção de malwares, identificando arquivos que atendem a certas condições e fornecendo uma abordagem baseada em regras para a criação de descrições de famílias de malware com base em padrões textuais ou binários. Dessa forma, o MailInspector permite ao administrador inserir novas assinaturas e padrões de detecção de arquivos maliciosos, bastando ao administrador inserir novas assinaturas/regras no formato YARA.

É possível facilmente detectar ameaças e comportamentos anômalos em arquivos comumente utilizados para payloads maliciosos, nas extensões Flash, Java, PDF, Microsoft Office, Microsoft Siverlight, portable executables, font type, anexos executáveis, entre outros (mesmo estando dentro de arquivos compactados), além de dentro de aplicações ricas (RIA – Rich Internet Applications).

As principais extensões que o MailInspector verifica (tanto a nível de anti-vírus/anti-malware, Zero Hour/Zero Day, quanto a nível de SandBox) são:

- .386;
- .7Z;
- .ACE;
- .ACM;
- .APK;
- .ARJ;
- .ASP;
- .AVP;
- .BAT;
- .BH;
- .BZ2;
- .BZIP;
- .BZIP2;
- .CAB;
- .CGI;
- .CHM;
- .CLA;
- .CLASS;
- .CMD;
- .CNV;
- .COM;
- .CPL;
- .CRT;
- .CS;
- .DLL;
- .DOC;
- .DOCM;
- .DOCX;
- .DOT;
- .DOTM;
- .DOTX;
- .DRV;
- .DVB;
- .EML;
- .EXE;
- .GZ;
- .GZIP;
- .HA;
- .HLP;
- .HTA;
- .HTM;
- .JAR;
- .JS;
- .LHA;
- .LNK;
- .LZH;
- .MD;
- .MSI;
- .OCX;
- .ODF;
- .OPO;
- .OTP;
- .OXT;
- .PAK;

- .PHP;
- .PIF;
- .PKZIP;
- .PL;
- .PPA;
- .PPS;
- .PPAM;
- .PPSM;
- .PPSX;
- .PPT;
- .PPTM;
- .PPTX;
- .RAR;
- .REG;
- .RTF;
- .SCR;
- .SH;
- .SLK;
- .SWF;
- .SYS;
- .TAG;
- .TGZ;
- .TZH;
- .VBE;
- .VBS;
- .VXD;
- .WBS;
- .WIZ;
- .WSF;
- .WSH;
- .XL;
- .XLA;
- .XLAM;
- .XLC;
- .XLK;
- .XLL;
- .XLM;
- .XLR;
- .XLS;
- .XLSB;
- .XLSM;
- .XLSX;
- .XLT;
- .XLTM;
- .XLTX;
- .ZIP;
- .ZOO;
- Entre Outros;

É possível configurar o sistema de proteção de anexos para efetuar a limpeza do arquivo e entregar ao usuário o arquivo sem a ameaça, ou bloquear a entrega ao usuário de eventual arquivo contaminado.

O link a seguir efetua o acesso ao SmartDefender de forma On-Line pela página da HSCBRASIL. Na página são apresentadas as ameaças em tempo real, onde as fontes são os e-mails. Esse portal diferencia-se dos outros por apresentar informações das ameaças detectadas por sistemas de proteção de e-mails e não em relação a firewalls e/ou antivírus em servidores/estações de trabalho, como é feito em muitos portais de monitoramento de ameaças.

No mesmo portal é possível solicitar recategorização de URL's, dessa forma a URL ao qual é solicitada a recategorização, sofre nova verificação e recategorizado se houver a real necessidade (a verificação é feita tanto por sistema automático de crawler, quanto por verificação humana).
https://smartdefender.cloud/search

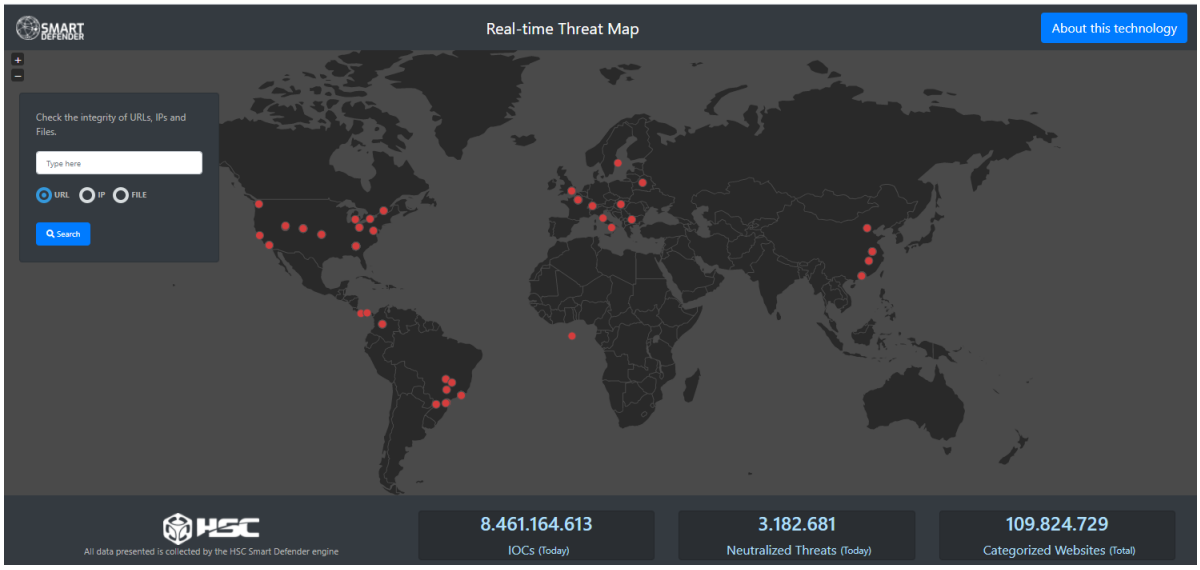
Além de permitir a solicitação de recategorização por site (portal Smart Defender), o MailInspector também permite a recategorização diretamente pela interface gráfica do produto:

- *Recategorizar o IP*;
- *Recategorizar a URL*;
- *Recategorizar o Arquivo*;

No portal é possível efetuar consultas para verificação de integridade de:

- URL's;
- Arquivos;
- IP's;

E visualizar em tempo real as ameaças nos e-mails, do mundo todo.



Tela de análise e classificação de URL/Arquivos/IP's pelo site da HSCBRASIL

Importante salientar que ESET, é engine "extra", para aumento da segurança da ferramenta. Ela é executada de forma independente, sem nenhuma interdependência do principal sistema de proteção do MailInspector que é **HSC SmartDefender antivírus**.

Retornos da consulta no site de SmartDefender da HSCBRASIL

Consulta de IP:

- Situação do IP em relação a RBL's;
- Histórico do IP em relação a RBL's;
- Geolocalização;
- Dados de WHOIS;
- Dados de SPF e DKIM;
- DNS Reverso;

Consulta de URL:

- Host;
- Mecanismo utilizado na consulta;
- Dados de WHOIS;
- Dados do certificado SSL;
- Categorização da URL;
- Preview da página;

Consulta de Arquivo:

- Status (Analisado ou, em análise);

- Mecanismo utilizado na análise;
- Tamanho do arquivo enviado;
- Tipo de arquivo enviado;
- Resultado da análise;

MailInspector e seus módulos em Datacenter brasileiro

Tanto o módulo SmartDefender, quanto em sistemas de comercialização do MailInspector por SaaS ou em ambientes em que sejam necessários a utilização da estrutura da HSCBRASIL, eles são executados em Datacenters no Brasil, pois a HSCBRASIL somente utiliza as suas estruturas em Datacenters homologados nível tier 3 e em no mínimo dois datacenters distintos em território nacional, em atendimento da normativa da Lei Geral de Proteção a Dados - LGPD.

A estrutura utilizada no ambiente SaaS é projetada para oferecer **escalabilidade e elasticidade**, permitindo processar todo o fluxo de e-mails de acordo com a quantidade de caixas postais configuradas pelo administrador. À medida que o número de caixas postais aumenta, a capacidade de processamento pode ser ampliada de forma dinâmica, por meio do incremento de recursos computacionais, como **memória, capacidade de processamento e/ou novos nós (nodes)**. Dessa forma, o ambiente mantém o desempenho, a disponibilidade e a capacidade de processamento mesmo diante do crescimento da demanda.

Além dos Datacenters serem nível tier 3, possuímos certificações de segurança e normativas internacionais de auditoria, tais como:

- ISO 27001 (Gestão de Segurança da informação);
- ISSO 22301 (Gestão de Continuidade de Negócios);
- ISAE 3402 (Norma internacional de auditoria);
- ISO 20000 (padrão internacional de gerenciamento de serviços em TI);
- ISO 27017 (regras e orientações de segurança da informação específicas para o uso e a oferta de serviços em nuvem);
- ISO 27018 (boas práticas para a proteção de dados pessoais e informações de identificação pessoal);
- ISAE 3402 (SOC1, SOC2 e SOC3);
- ISO 14001 (Gestão ambiental);
- ISO 45001 (requisitos para um Sistema de Gestão de Saúde e Segurança Ocupacional);

Caso seja adotada a solução no modelo SaaS, os nós de filtragem de e-mail (MX) poderão ser distribuídos em datacenters distintos, permitindo a composição de um cluster com dois ou mais nós, preferencialmente alocados em diferentes localidades e faixas de endereçamento IP, sem perda de desempenho, nem latência na entrega dos e-mails.

O cluster foi projetado para operar em alta disponibilidade, podendo utilizar os modos ativo/ativo ou ativo/passivo, conforme a arquitetura e a configuração definidas pelo administrador da solução.

A arquitetura oferece balanceamento de carga (load balancing) e mecanismos de redundância que permitem a continuidade do processamento mesmo diante da indisponibilidade de um dos nós. Em caso de falha, seja por interrupção de conectividade, indisponibilidade do datacenter ou perda de energia, os demais nodes assumem automaticamente a carga de processamento, de forma transparente para o ambiente, sem perda ou quebra de informações.

Dessa maneira, a arquitetura proporciona alta disponibilidade, resiliência e continuidade operacional, reduzindo o impacto de eventuais falhas de infraestrutura e garantindo a manutenção do serviço de proteção e filtragem de e-mails.

O sistema de **Sandbox da HSCBRASIL** está hospedado em infraestrutura localizada no Brasil, proporcionando maior precisão na detecção de ameaças que utilizam a **geolocalização como fator de ativação**.

Algumas campanhas de phishing e outros tipos de malware empregam mecanismos de evasão que verificam a localização geográfica do ambiente de execução antes de ativar seu comportamento malicioso. Dessa

forma, uma ameaça direcionada especificamente a usuários no Brasil pode apresentar um comportamento aparentemente legítimo quando executada em ambientes localizados em outros países, dificultando sua identificação.

Com a infraestrutura de Sandbox localizada fisicamente no Brasil, a solução consegue reproduzir de forma mais próxima as condições do ambiente-alvo. Assim, quando uma ameaça utiliza a localização geográfica como critério para ativação, o comportamento malicioso tende a ser exposto durante a análise, permitindo sua **identificação, classificação e neutralização**.

Por exemplo, um phishing direcionado a usuários brasileiros pode verificar a geolocalização do ambiente de execução e, quando identifica que está sendo analisado fora do Brasil, apresentar um conteúdo inofensivo, como o redirecionamento para um site legítimo. Em um Sandbox localizado no Brasil, a mesma ameaça possui maior probabilidade de reconhecer o ambiente como pertencente à sua região-alvo e revelar seu comportamento malicioso, aumentando significativamente a **assertividade da detecção**.

É possível implementar o SmartDefender localmente, sem ônus de nova licença. Para configurar o uso do SmartDefender localmente, é necessário implementar uma máquina local exclusivamente para fins de SandBox, sem necessidade de envio de amostra para HSCBRASIL.

Segue abaixo alguns dados dos Datacenters utilizado pela HSCBRASIL (inclusive para a solução Security Enterprise Cloud, sistema SmartDefender e sistemas SaaS):

Energia

- ✓ Três níveis de disponibilidade de energia, podendo atingir até 99,99974%.
- ✓ 5 geradores elétricos a Diesel, que proporcionam fornecimento de energia
- ✓ por tempo ilimitado.
- ✓ UPSs paralelas redundantes de última geração.

Climatização / Ar condicionado

- ✓ Sistema Split de Condensador Remoto de 30TRs (cada unidade – total 15).
- ✓ Controle de temperatura e umidade com precisão de +/- 5%.
- ✓ Filtros de ar de alta eficiência para controle de sujidade.
- ✓ Detecção automática de vazamentos.

Segurança Física

- ✓ Monitorada 24 horas por dia de uma central de segurança.
- ✓ Mais de 70 câmeras com armazenamento digital de imagem.
- ✓ Sistema composto de três níveis de controle de acesso.

Detecção e Combate a Incêndio

- ✓ Extinção de incêndio feita em 3 níveis.
- ✓ Extintores de CO2.
- ✓ Gás Inergem.
- ✓ Sprinklers tipo “Pré Action Dry Pipe”
- ✓ Bombeiro 24 horas por dia.

Hardware de Última Geração

- ✓ Equipamentos de última geração, para melhor desempenho de análise de e-mails.

Certificações dos DataCenters

INFORMATION SECURITY MANAGEMENT SYSTEMS
ISO
ISO/IEC 27001:2013

ISAE 3402
CERTIFIED TYPE II

TIER III DESIGN®
CenturyLink Brasil Ltda.
São Paulo Datacenters DCs 6 to 10
Expires 30 September 2021
UPTIME INSTITUTE CERTIFIED

International Organization for Standardization
ISO
22301

Padrão máximo de qualidade e segurança

Segurança

Rede protegida contra ataques DDoS. Segurança reforçada com controle de acessos, sistema anti-incêndio e câmeras de vigilância com monitoramento 24h.

Tier III

Ambiente dentro dos padrões internacionais de qualidade, com as principais certificações do mercado (Tier III Design Documents e Tier III Constructed Facility), que garantem confiabilidade em nossos serviços e máximo uptime (99,5%).

Outras certificações

Certificações que atestam a qualidade de nossa estrutura: ISO 9001, ISO 20000-1, ISO 27001, ISO 27017, ISO 27018, ISO 22301, ISAE3402 SOC 1, ISAE3402 SOC 2, ISAE3402 SOC 3, PCI-DSS, ISO 14001, ISO 45001.

Global "Endpoint Detection and Response"

Todos Endpoints agrupados pelas Engines de antivírus utilizado pelo MailInspector (aproximadamente 500 milhões de usuários no mundo inteiro) agem e contribuem com um sistema de análise e resposta integrados, funcionando como honeypots e detecção de IOC's.

Desta forma, quando uma estação de trabalho com o Endpoint da mesma Engine utilizado pelo MailInspector, executa um arquivo o mesmo é analisado pela estação usando a tecnologia de "BEHAVIOR ANALYSIS " e "EXPLOIT INTERCEPTION" (Tecnologia Similar a um SandBox na Estação de Trabalho) em tempo real detectando um arquivo malicioso e reportando para a nuvem.

A nuvem recebe a notificação em menos de 60 SEGUNDOS, identifica e disponibiliza a informação de metadado do arquivo malicioso e deixa disponível para consulta dos demais agentes no mundo inteiro.

Agora imaginem uma nova ameaça que surge em qualquer lugar do mundo, assim que chega em um cliente com a mesma engine utilizado pelo MailInspector, ele automaticamente identifica a ameaça e reporta para nuvem de segurança que por sua vez cria uma REPUTAÇÃO DO ARQUIVO. Tudo isso em menos de 60 SEGUNDOS. Todos os demais sensores, incluindo o HSC MailInspector, podem checar a reputação deste arquivo e tomar uma decisão de bloquear ou remover esta ameaça.

É possível compreender a dimensão da inteligência de segurança utilizada pelo **Big Data da HSCBRASIL** ao considerar o volume e a diversidade de informações processadas continuamente. A plataforma consolida, correlaciona e analisa dados provenientes de múltiplas fontes de inteligência e mecanismos de detecção, criando uma base de conhecimento continuamente atualizada para o **HSC SmartDefender**.

Como exemplo, a infraestrutura de inteligência da **ESET** conta com centenas de servidores dedicados à análise em tempo real, processando um grande volume de amostras provenientes de sensores, mecanismos de detecção e outras fontes de telemetria de segurança. Esse ecossistema gera informações sobre arquivos, hashes, indicadores de comprometimento (IOCs), indicadores de ataque (IOAs) e outros artefatos relacionados a ameaças, contribuindo para a identificação de padrões e comportamentos maliciosos.

Essas informações, quando integradas ao ecossistema de inteligência da **HSCBRASIL**, podem ser correlacionadas com os dados próprios da plataforma, permitindo ampliar a capacidade de análise, contextualização e identificação de ameaças. O objetivo é transformar grandes volumes de dados de segurança em **inteligência acionável**, utilizada pelo SmartDefender para aprimorar continuamente seus mecanismos de proteção.

A área de **Pesquisa e Desenvolvimento (P&D) da HSCBRASIL** atua nesse processo de forma contínua, concentrando esforços na identificação de vulnerabilidades, análise e descoberta de novas ameaças, correlação de eventos de segurança, desenvolvimento de mecanismos de detecção e evolução das tecnologias de resposta e prevenção.

Dessa forma, o Big Data da HSCBRASIL não representa apenas um grande repositório de informações, mas uma **camada de inteligência de segurança continuamente alimentada e processada**, capaz de transformar dados provenientes de diferentes fontes em conhecimento aplicado à proteção dos ambientes de e-mail e à antecipação de novas técnicas de ataque.

As Engines de antivírus atuam diretamente no corpo da mensagem em códigos contidos, tais como:

- HTML;
- JSE;
- Jscript;
- Java Script;
- VBE;
- Flash;
- VBScript;
- WSF;
- PDF;

- Java;
- Microsoft Silverlight;
- FBJS;
- AJAX;
- Bash Code;
- RIA – Rich Internet Applications;
- Phyton;
- Qualquer outro tipo de código programável;

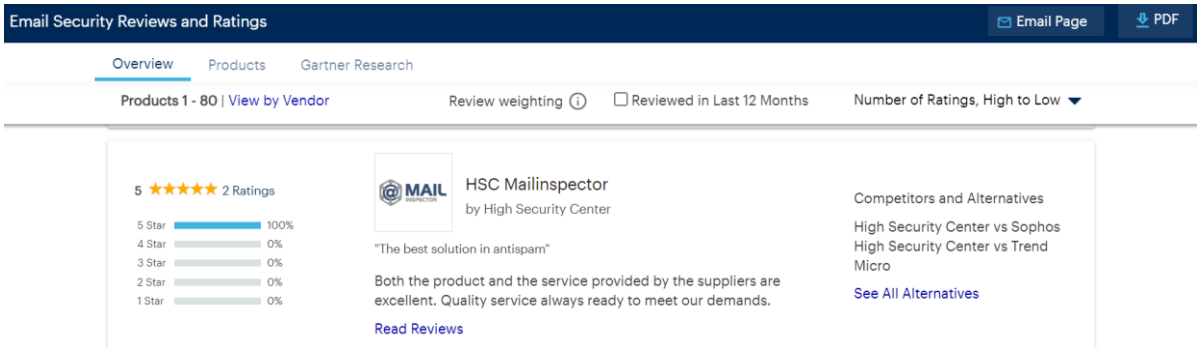
Também são verificados os anexos das mensagens, mesmos compactados pelos diversos sistemas de compactação, tais como ZIP, RAR, CAB, ACE, ARJ, BH, HA, JAR, PAK, LHA, LZH, PKZIP, BZIP, BZ2, BZIP2, GZIP, ZOO, 7Z, TZH, TGZ, TAR, GZ, etc, também efetua análise de URL's e outros campos/anexos contidos nos e-mails.

É possível configurar ações a serem tomadas a nível de antivírus, tais como:

- Apagar a mensagem e/ou anexo, com a opção de notificar o remetente e/ou destinatário;
- Rejeitar a mensagem com a opção de notificar o remetente e/ou destinatário;
- Encaminhar a mensagem a terceiro;
- Entregar a mensagem ao destinatário, sem aviso algum a terceiros;
- Bloquear e quarentenar o e-mail;
- Modificar o assunto do e-mail em caso de infecção;
- Adicionar/criar novos cabeçalhos no e-mail e/ou adicionar conteúdos;
- Continuar o processamento, ignorando a ameaça encontrada;

Gartner - Solução de E-mail Gateway

O MailInspector está posicionado entre os sistemas de proteção de e-mails aprovados pela Gartner Group.



Fonte: https://www.gartner.com/reviews/market/e-mail-security

Mail Behavior Analysis

A HSC Desenvolveu uma tecnologia capaz de identificar anexo maliciosos que tem como objetivo iludir, confundir e prejudicar os usuários. O mecanismo não necessita de assinaturas, como um antivírus, ele detecta o comportamento dos anexos de e-mails e bloqueia os anexos possivelmente perigosos.

Global Sender Reputation & Threat Response

Os sensores da HSC em conjunto com o da ESET recebe mais de 1 Milhão de informações de e-mails por hora, através de mais de 200.000 redes globais participantes!

Alimentando estatísticas com os registros de IP's de quem mais manda SPAM no mundo em tempo real. Essa informação é constantemente alimentada no appliance do cliente, dessa forma qualquer e-mail que chegar ao cliente, já se tem a informação da qualidade dele (pelo IP de origem).

O HSC Machine Learning identifica em tempo real os remetentes "IP/Redes de Origens" que estão disseminando um novo ataque ou campanha de SPAM/Phishing e calcula localmente a Reputação do "Sender" do e-mail.

O Sistema aprende de forma automática baseando-se em métricas de volumes de mensagens, quantidade de SPAM, Vírus, Phishing e tipos de e-mails, para calcular uma reputação para cada servidor de origem.

Com esta tecnologia o HSC MailInspector consegue identificar de forma eficaz novos surtos de proliferações de vírus, spam e phishing, podendo bloquear, alertar ou mesmo controlar o fluxo de e-mails recebidos destas origens.

O sistema de reputação de IP's permite um controle granular e efetivo, com um sistema de reputação com sensibilidade de 10 níveis, em conjunto com 4 tipos de classificação, dessa forma é possível classificar 40 variações.

URL Categorization & Reputation

Os principais ataques de e-mails hoje usam URLs como base.

Mais de 90% dos ataques no mundo executados por e-mail usam URL's maliciosas, sejam para um Phishing ou um possível Download de Conteúdo malicioso.

A HSC Recebe mais de 10 Milhões de URL's por dia para serem analisadas e processadas. Com esta gama de dados é possível criar um dos melhores sistemas de reputação e categorização do mundo garantindo uma maior segurança.

Todas URL's contidas nos e-mails são processadas uma a uma pelos filtros do HSC MailInspector verificando as assinaturas baixadas no appliance.

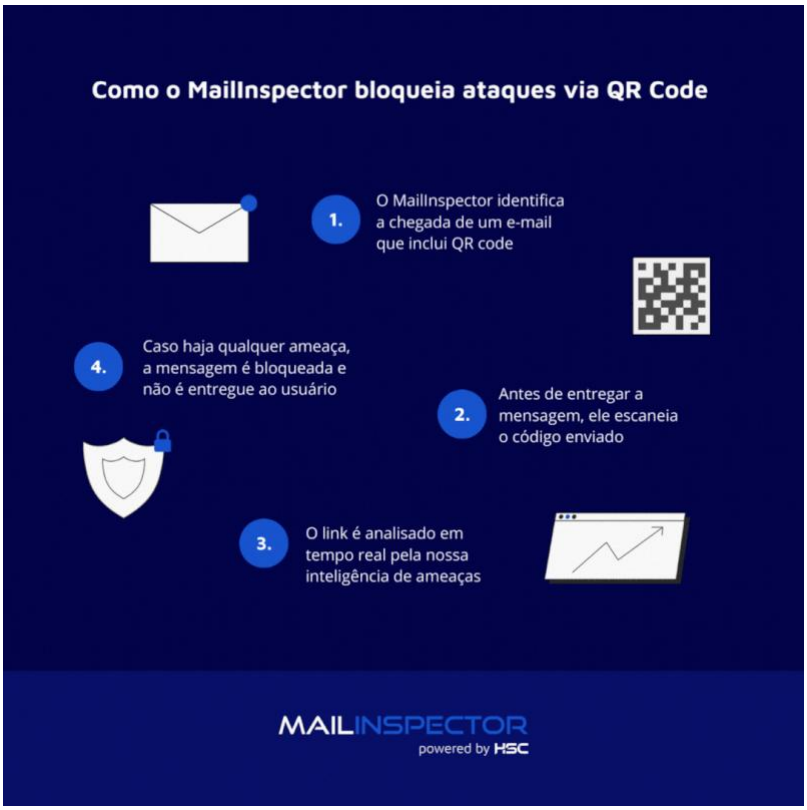
Nosso sistema ainda conta com um mecanismo de categorização que permite identificar uma URL pelo seu conteúdo, podendo o administrador decidir o que fazer com as mais de 50 categorias, tais como:

- Conteúdo Pornográfico
- Abuso Infantil
- Racismo e Ódio
- Redes Sociais
- P2P
- Pesquisa de Emprego
- Command Control Center
- Sites Comprometidos
- Sites Governamentais
- CDN – Servidor de Conteúdos
- Instituições de Ensino
- Humor
- TV & Filmes
- Turismo
- Namoro e Relacionamento
- Seguros
- Saúde e Medicina
- Arquitetura e Construção
- Notícias
- Compras Online
- Segurança de Informação
- Conteúdo Erótico
- Hacking
- Pirataria e Roubo de Direitos Autorais
- Bate Papo
- Relacionamento Profissional
- Anonymizer
- Malwares
- SPAM
- Militar
- Reserva de Domínios
- Wikis
- Streaming de Áudio
- Esportes
- Restaurantes
- Bancos
- Farmácia e Medicamentos
- Suplementos Alimentares
- Fábricas e Indústrias
- Propaganda ADS
- Opinião e Comparativos de Produtos
- Tecnologia Geral
- Aborto
- Atividades Potencialmente Criminosas
- Violência
- Armazenamento Pessoal
- Páginas Pessoais e Blogs
- Botnet
- Phishing
- Spyware & Keyloggers
- Organizações Sociais e Associações
- Sites Inalcançáveis
- Entretenimento
- Streaming de Vídeo
- Veículos Motorizados
- Moda e Beleza
- Finanças
- Nutrição e Dieta
- Agricultura
- Imóveis
- Receber para Navegar
- Acesso Remoto
- Entre outras categorias

Análise de links apresentados por QRCode

Um dos ataques mais comuns é o envio de links contaminados através de QRCode no corpo ou anexo do e-mail.

Como funciona ataque com QRCode contendo link malicioso



Como o MailInspector bloqueia o ataque por QRCode

Para a **detecção e prevenção de ataques que utilizam QR Codes como vetor de ataque**, o MailInspector realiza a identificação e análise dos QR Codes presentes nas mensagens e nos respectivos anexos. A solução extrai os links incorporados e verifica tanto sua **categorização e reputação** quanto o conteúdo e o destino associado ao endereço.

Durante a análise, o MailInspector pode identificar se o QR Code direciona para **sites maliciosos ou comprometidos**, páginas utilizadas para **phishing**, downloads de arquivos potencialmente maliciosos ou conteúdos não autorizados, bem como formulários e páginas destinados à **coleta indevida de credenciais, senhas e outras informações sensíveis**.

A análise é realizada independentemente do local em que o QR Code esteja inserido. Ele pode estar presente:

- No corpo da mensagem;
- Em arquivos anexos, como PDF, DOC, DOCX, XLS, XLSX, PPT, PPTX, entre outros;
- Incorporado em imagens anexadas;
- Conteúdo presente em anexos compactados;
- Em documentos ou imagens que contenham múltiplos elementos gráficos simultaneamente.

Dessa forma, o MailInspector amplia a proteção contra técnicas de **Quishing (phishing por QR Code)**, evitando que uma mensagem aparentemente legítima utilize um QR Code para contornar mecanismos tradicionais de análise de URLs e conduzir o usuário a conteúdos maliciosos.

Sistema de detecção de arquivos

No MailInspector é possível trabalhar com múltiplas formas de detecção de arquivos, tanto a nível de spams e phishings, quanto ao processo de antivírus. As formas detectadas de anexos podem ser:

- MIME Type;
- Tipo real do arquivo;
- Nome do arquivo;
- HASH;
- Extensão;
- Detecção de arquivos do tipo texto;
- Arquivos Executáveis, incluindo executáveis do tipo portable executable (PE), podendo ser PE32 e PE32+;
- Arquivos compactados;
- Planilhas;
- Documentos do MS Office, OpenOffice, LibreOffice, Calligra Suite, OnlyOffice e afins;
- Arquivos de imagem;
- Links contidos dentro de imagem;
- Arquivos de banco de dados (Access, dBase, tabelas de banco de dados em geral);
- Conteúdo em metadados de arquivos;
- Objetos .EXE, .DLL, JPEG, .GIF, .BMP dentro de arquivos de programas de escritório (Word, Excel etc.);
- Arquivos PDF;
- Anexos programáveis tipo VB Script, Java Script e afins;

Políticas de segurança individuais e por grupos

No MailInspector é possível trabalhar com múltiplas políticas de segurança para o tráfego de e-mail (sem limite de número de políticas), isto é, é possível criar políticas por grupos de usuários, bem como sentidos distintos do e-mail (entrada e saída, ou até mesmo e-mails internos), sempre casando e combinando operadores lógicos, tais como **E (AND)**, **OU (OR)**, **OCORRER (OCCUR)**, **NÃO (NOT)**, **APROXIMADO (NEAR), (,), [,]** e **expressões regulares (REGEX)**, como por exemplo:

- Política específica para e-mails oriundos da diretoria da empresa **E** com destino a sistemas de faturamento da empresa Y;
- Política de não verificação de anexos compactados com senha **E** cujos e-mails sejam originários DE um e-mail específico **E** com destino PARA um grupo de e-mails;
- Bloqueio e quarentena de e-mails que ultrapassem a X Bytes **E** oriundos DE um e-mail específico, mas para o resto da empresa o limite do tamanho do e-mail continua sendo de tamanho Y;
- Entre outras políticas possíveis;

Seguindo o mesmo raciocínio, ainda no MailInspector é possível quarentenar mensagens de entrada ou saída e de determinados grupos de usuários. Quando as mensagens forem maiores que X bytes, as mesmas serão armazenadas em uma fila específica ao qual serão somente liberadas em horário de menor carga, definido pelo administrador do sistema.

Dessa forma é possível criar políticas corporativas de tráfego de e-mail de acordo com o perfil de risco de cada usuário/grupos de usuários (deixando mais restritiva ou mais relaxada), com uso de compliance (DLP, criptografia de E-mail, quarentena customizada), módulos de filtragem (ex: módulo de antivírus, módulo de phishing, módulo de controle de anexo, etc), manipulação de pontuação de SPAM ou outros módulos do MailInspector com algumas das variáveis abaixo apresentadas:

- Sentido do e-mail;
- DE origem para DESTINO (E-mails, Domínios, subdomínios, etc);
- IP de Origem da Mensagem;
- Quantidade de mensagens;
- Domínios, subdomínios;
- Anexos:
    - Quantidade de anexos;
    - Tamanho de anexos;
    - Conteúdo/anexo criptografado;
    - Anexos compactados;
        - Quantidade de níveis de compactação;
        - Anexos compactados com senha;
        - Quantidade de arquivos no anexo compactado;
    - Anexos por Mime-Type/TrueType/Tipo do anexo (se é executável, se é arquivos padrão Office, etc);
    - Extensão dos Anexos;
    - Diversos outros filtros de anexos;
- Regras específicas por grupos distintos, podendo ser por usuários, e-mails, grupos LDAP, grupos do AD, IP's, range de IP, classe de IP, expressão regular, domínios, etc;
- Hostname de ORIGEM;
- Hostname de DESTINO;
- Filtros de dicionários (inclusive por dicionários de REGEX);
- País de Origem / País de Destino / Região;
- Linguagem do e-mail;
- Conteúdo no corpo do e-mail (tanto HTML, quanto texto plano);
- Conteúdo no cabeçalho do e-mail (tais como From do Envelope, From do Header, To do Envelope, Subject, etc);
- Tamanho do e-mail;
- Palavras chaves no assunto;
- Conexão com HELO/EHLO;
- DNS Reverso (também conhecido como Forwarded-Confirmed Reverse DNS - FCrDNS);
- Pontuação obtida pela reputação do IP de origem do e-mail;
- URL's no corpo, assunto ou dentro de anexos contidos na mensagem;

- Horários;
- Tempo de armazenamento;
- Entre muitas outras variáveis, incluindo a utilização de WildCards;

Podem ser criadas políticas individuais ou por grupos, de acordo com o tipo de ameaça encontrada ou peculiaridades do e-mail, tais como:

- Vírus;
- Malwares;
- Phishing;
- SPAM;
- Provável SPAM;
- E-mails de Formulários;
- Ataque de Dicionário;
- Ataque por bounce mail;
- URL contaminadas;
- De acordo com a categoria da URL contida no e-mail;
- Fraude de E-mail / BEC;
- Spoofing de domínio;
- Remetentes diferentes no cabeçalho do e-mail;
- Remetentes oriundos de servidores gratuitos de e-mail;
- E-mails oriundos de mídia social;
- Reputação do remetente perante a HSCBRASIL;
- Entre outros tipos de ataque ou características do e-mail;

As regras são aplicadas conforme as variáveis acima apresentadas, dessa forma não é efetuada a leitura de regra que não seja aplicada a variável indicada, evitando dessa forma leitura desnecessária de regras e otimizando o processamento e garantindo sigilosidade.

Caso o administrador queira aplicar uma política global, basta aplicar a regra de sentido de Todos para Todos, dessa forma ignorando o sentido e o destino da aplicação da regra. Se desejar criar uma regra clássica do tipo Inbound, basta efetuar a regra do sentido DE (Todos) para (Domínios Internos), assim, aplicando regras para e-mails oriundos de “fora” para “dentro”. Já para o sentido contrário (Outbound), bastaria fazer a regra de sentido DE (Domínios Internos) PARA (Todos).

O MailInspector é ilimitado quanto ao número de políticas criadas (não possui limite por usuário – remetente/destinatário, nem por domínio, nem por appliance/sistema ou qualquer outro tipo de parâmetro que possa limitar), dessa forma, somente cabe ao administrador criar as políticas necessárias para a sua parametrização, sem se preocupar com eventual necessidade de instalar novos pontos e/ou bases de dados para incluir mais políticas.

As políticas criadas podem ser simuladas antes de aplicação definitiva, dessa forma evitando que seja criada regra indevida ou erada na solução. Também permite ao administrador acompanhar e visualizar a operação da política na medida em que a política é simulada.

É possível a alteração automática de políticas no MailInspector devido a epidemias e/ou ataques sofridos (desde que esteja ativa essa função), o sistema altera as políticas em tempo real, de acordo com as políticas baixadas pelo Extreme Update, bloqueando dessa forma ataques de possíveis hackers, através de bloqueio de IPs/redes, Range de IP e/ou domínios/subdomínios.

Também é possível criar assinaturas em e-mails (disclaimer) a serem inseridos tanto como HTML ou texto plano no começo do e-mail ou no final. O disclaimer pode ser criado para grupos (usuários, LDAP, subdomínios, domínios, IP, range de IP, regex, etc – Ver *Grupos Usuários*) em e-mails de entrada ou saída, com orientação a origem de um grupo ou destino de um grupo, de acordo com a necessidade indicada pelo administrador. O disclaimer pode ser atrelado a políticas de segurança, por exemplo assinatura do tipo alerta, ao qual indica ao usuário tomar maior cuidado com o conteúdo do e-mail, por ele se de origem externa em relação a empresa, ou aviso de alerta ao usuário do setor financeiro, quando o e-mail vier de "fora" com destino ao setor financeiro e conter palavras chaves utilizadas pelo setor bancário.

HSC SandBox

Essa é a última e talvez a mais interessante das camadas de análise e resposta. Nela todas URL's e os arquivos anexos suspeitos são analisados **localmente** e se o administrador desejar, **opcionalmente** podem ser enviados para a nossa nuvem (localizada em datacenter no Brasil, seguindo legislação de LGPD) para que possam ser analisados e comparados com os resultados do BigData.

O HSC SandBox é considerado um modo de análise avançado de anexos e URL's, uma vez que ele faz uma camada "extra" de verificação sobre os arquivos e links presentes nos e-mails.

Se optado pelo uso do SandBox na nuvem da HSCBRASIL, é importante ressaltar que o arquivo enviado é de forma anônima, de acordo com a Lei Geral de Proteção de Dados.

As URL's são recebidas e passadas para o nosso "URL Smart Crawling" onde todas URL's são analisadas em tempo real, através de uma sofisticada Engine de segurança que analisa várias características desta URL, tais como:

- Tipo do conteúdo: "Se é um conteúdo Texto ou um Download de arquivo";
- Antivírus e Reputação "Integrado com a base do BitDefender";
- Características de PHISHING com roubo de dados "Através de análise de formulários, reputação de links, texto e dados solicitados" e/ou formulários de coleta de usuário/senha;
- Machine Learning exclusivo da HSC para detecção de Sites de Phishing;
- Malicious Redirect "Sites comprometidos e Encurtadores de URLS que redirecionam para outros conteúdos";
- Códigos maliciosos HTML/JavaScript/CSS/Outros e muitas outras tecnologias;
- URL's contidos em documentos do tipo Microsoft Office (Word, Excel, Power Point, etc), PDF's, inclusive verificação de URL's encurtados;

Enquanto os arquivos são analisados no SandBox, o e-mail fica retido e não é entregue ao usuário enquanto não for finalizado o processo de análise e categorização. O tempo de análise é questão de milissegundos.

O SandBox File é processado em duas etapas distintas (Estática e Dinâmica).

Em resultado de análise de URL's e Anexo, é possível enviar o HASH, URL's e anexos, para sistemas de terceiros para reanálise, tais como VirusTotal e AlienVault, dessa forma, basta clicar em um botão de envio de amostra, que o objeto será enviado para o sistema a ser analisado (VirusTotal e/ou AlienVault).

Além do SandBox da HSCBRASIL, o MailInspector possibilita ao administrador integrar com SandBox de outros fabricantes*

* Maiores informações da forma de integração com SandBox de outros fabricantes, é necessário consultar a HSCBRASIL ou agente autorizado.

Forma Estática de trabalho do SandBox

A forma estática é efetuada localmente (no próprio appliance) e consiste em fazer engenharia reversa do binário, carregando o executável em um desmontador, para obter o código-fonte da linguagem de montagem a partir do código do programa original. Depois disso é feita a análise para saber o que o programa faz.

Algumas das técnicas utilizadas na análise estática são:

- Determinação do tipo real do arquivo;
- Cadeias codificadas no arquivo binário;
- Busca de técnicas de ofuscação de códigos;
- Busca de técnicas de redirecionamentos e uso de arquivos de terceiros, inclusive acionamento de arquivos e links externos;
- Verificação de ofuscações de arquivos para determinar se o arquivo foi compactado ou se foi utilizado criptografia;
- Hash e comparação;
- Fuzzy Hash e comparação;
- Verificação de hash em relação a assinatura de vírus.

Forma Dinâmica de trabalho do SandBox

A técnica de análise dinâmica envolve a execução do arquivo e a observação de seu comportamento no sistema, em que o sistema é configurado em um ambiente isolado.

A análise dinâmica nos ajuda a remover a infecção, produzir assinaturas efetivas ou ambas. O ambiente é totalmente isolado e se o arquivo estiver enviando solicitações de rede ou estiver esperando uma resposta, a resposta geralmente é simulada. O processo todo é efetuado em múltiplos idiomas, de acordo com o idioma utilizado pelo artefato analisado.

A análise dinâmica geralmente se concentra nas seguintes atividades:

- Análise de Sistema Operacional (em qual tipo de sistema operacional o artefato opera, bem como se não é imagem de S.O. ou outro tipo de componente);
- Sistema de arquivos;
- Registro;
- Processo;
- Acesso a Rede;
- Chamadas do sistema;

Obs: A forma dinâmica pode ser trabalhada de duas maneiras: localmente OU usar a nuvem da HSCBRASIL.

Caso o administrador opte pelo uso com a nuvem da HSCBRASIL, é importante salientar que todos dados enviados a nossa nuvem seguem as mais restritas regulamentações do mercado, os dados são enviados de forma anônima e criptografada, a HSC não salva o conteúdo do arquivo, depois de sua execução os dados são automaticamente removidos.

Na análise dinâmica, é possível indicar se o arquivo será analisado localmente OU enviado a nuvem da HSCBRASIL. É possível a configuração dessa opção pelo administrador da solução.

Caso seja configurado o uso da nuvem da HSCBRASIL, o arquivo é enviado de forma anônima, não sendo rastreável a origem da informação, atendendo a Lei Geral de Proteção de Dados.

Ainda na etapa dinâmica é feita a análise forense da memória. Na simulação é feita a execução do arquivo, emulando os ambientes MacOS, Windows, Linux e Android.

Na investigação de ataques avançados de computador, que são furtivos o suficiente para evitar deixar dados no disco rígido do computador, a memória do computador deve ser analisada em busca de informações vitais.

As etapas de análise forense da memória:

- Aquisição de Memória: Esta etapa envolve a descarga da memória da máquina de destino.
- Análise de Memória: Uma vez que uma imagem de memória é adquirida, o próximo passo é analisar o despejo de memória para artefatos forenses. A análise forense da memória nos ajuda a coletar as seguintes informações:
    - Lista de todas as conexões de rede antigas e atuais;
    - Lista de todo o processo em execução;
    - Lista de DLLs carregadas;
    - Teclas digitadas;
    - Versão descompactada / não criptografada do arquivo de malware;
    - Lista de arquivos abertos associados a um processo;
    - Lista de chaves de registro abertas associadas a um processo;
    - Módulos do Kernel;
    - Injeção de código;
    - Detecção de Rootkits;
    - Detectar artefatos ocultos;

Com as informações de memória coletadas, podemos determinar se o arquivo possui características maliciosas ou não.

Além das etapas já indicadas, diversas técnicas de detecção de Malwares são executados, tais como:

- Análise comportamental (Behaviors).

Quando é detectado uma possível ameaça o sistema notifica a nuvem e reage a ameaça bloqueando o conteúdo perigoso e notificando a nuvem para criar uma Reputação deste Arquivo, desta forma todos outros sensores de MailInspector quando efetuarem uma consulta, já saberão previamente deste ataque sem a necessidade de reenviar o arquivo para novo análise.

O arquivo quando é enviado ao SandBox, ele não é liberado ao usuário enquanto não finalizar o processo de análise. O e-mail pode ser liberado antes disso, mas o usuário não terá acesso ao anexo enquanto o SandBox não finalizar a análise.

HSC Targeted Attack Protection

O **HSC MailInspector** dispõe de uma engine especializada na proteção contra **ataques direcionados (Targeted Attacks)** e ataques oportunistas, com foco na proteção do usuário final contra ameaças distribuídas por meio de mensagens eletrônicas.

A tecnologia foi desenvolvida para identificar e bloquear diferentes tipos de ameaças, incluindo **Phishing, Malware, Ransomware, URLs maliciosas, arquivos potencialmente perigosos e outras técnicas utilizadas em ataques direcionados**.

Análise de URLs em tempo real

O sistema realiza a **análise em tempo real das URLs presentes no corpo das mensagens e nos arquivos anexados**, avaliando sua reputação, comportamento e possíveis indicadores de comprometimento.

Como mecanismo adicional de proteção, o MailInspector realiza a **reescrita das URLs** contidas nas mensagens, direcionando-as para o mecanismo de proteção e Sandbox integrado ao próprio MailInspector.

Dessa forma, o usuário não acessa diretamente o endereço original ao clicar no link. Antes do acesso ser efetivamente liberado, a URL é submetida novamente a uma **verificação em tempo real**, permitindo identificar alterações posteriores no comportamento ou na reputação do endereço.

Esse mecanismo é especialmente importante para combater ataques nos quais uma URL inicialmente considerada legítima ou inofensiva passa a hospedar conteúdo malicioso posteriormente.

Funcionamento da proteção por reescrita de URLs

O processo ocorre da seguinte forma:

1. **Recebimento e análise da mensagem**
   O e-mail é recebido pelo MailInspector e submetido à análise de segurança. Todas as URLs identificadas são verificadas, tanto aquelas presentes no corpo da mensagem quanto as encontradas nos arquivos anexados.
2. **Reescrita das URLs**
   As URLs são reescritas pelo MailInspector, fazendo com que o acesso futuro passe pelo mecanismo de proteção da solução.
3. **Entrega da mensagem**
   Após a conclusão das análises e caso a mensagem esteja de acordo com as políticas de segurança configuradas, o e-mail é entregue ao usuário com as URLs protegidas e reescritas.
4. **Verificação no momento do acesso**
   Quando o usuário clicar em uma URL reescrita, o acesso não é realizado diretamente ao endereço original. O MailInspector realiza uma **nova análise em tempo real da URL de destino** e, somente se os critérios de segurança forem atendidos, permite o prosseguimento para o endereço solicitado.

Proteção contra ameaças que surgem após a entrega

Um dos principais benefícios da reescrita de URLs é a capacidade de realizar uma nova avaliação **no momento em que o usuário efetivamente acessa o link**.

Assim, uma URL que tenha sido considerada segura no momento do recebimento da mensagem poderá ser novamente analisada posteriormente. Isso é particularmente relevante em ataques nos quais o criminoso altera o conteúdo ou o comportamento de um endereço após a mensagem já ter sido entregue ao destinatário.

Dessa forma, mesmo que o usuário clique no link **horas, dias ou semanas após o recebimento da mensagem**, a URL poderá ser submetida novamente aos mecanismos de segurança antes da liberação do acesso.

Análise de anexos e ameaças desconhecidas

A **HSC Targeted Attack Protection** também utiliza o mecanismo de **Sandbox integrado ao MailInspector** para análise de arquivos anexados às mensagens.

Os arquivos podem ser submetidos à análise comportamental, permitindo identificar características suspeitas ou comportamentos maliciosos **mesmo quando a ameaça ainda não possui uma assinatura conhecida**.

Essa capacidade amplia a proteção contra **Malware, Ransomware, ameaças Zero-Day/Zero-Hour e outras ameaças emergentes**, complementando os mecanismos tradicionais de detecção baseados em assinaturas.

Proteção em múltiplas etapas

A combinação entre **análise inicial da mensagem, verificação de URLs, reescrita de links, análise em Sandbox e nova validação no momento do acesso** proporciona uma camada adicional de proteção ao usuário final.

O modelo reduz o risco de que uma ameaça passe pela análise inicial e posteriormente comprometa o usuário em razão de uma alteração realizada pelo atacante no conteúdo ou destino da URL.

O MailInspector não verifica apenas se o link era seguro quando o e-mail foi recebido; ele também pode verificar se continua seguro no momento em que o usuário tenta acessá-lo.

Múltiplas Engines de anti-malware (de uso opcional)

E-mail Gateway – HSC SmartDefender antivírus e ESET

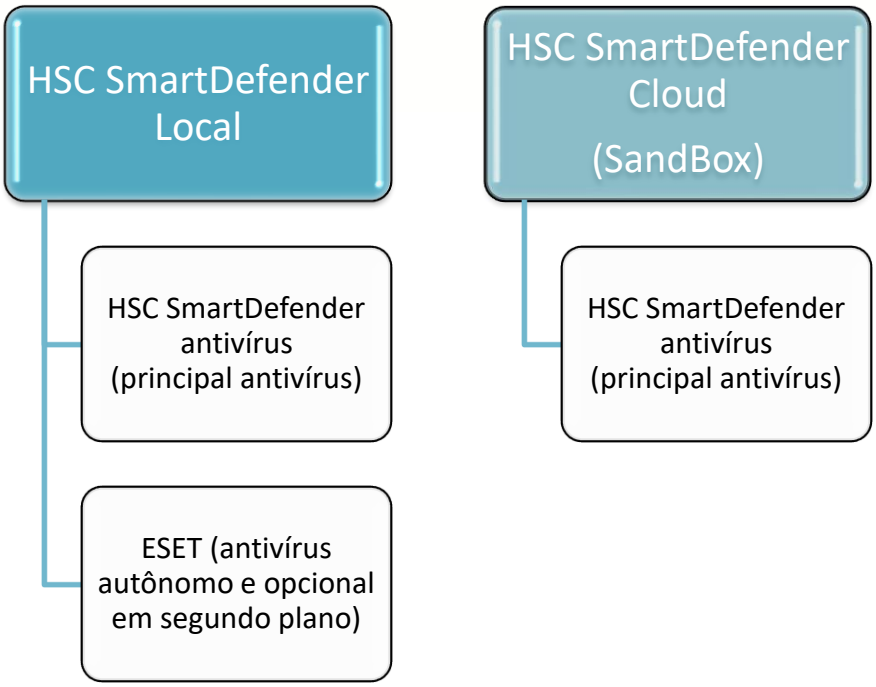
Cloud Global – HSC SmartDefender antivírus e ESET

O HSC MailInspector faz toda a análise e proteção através do módulo HSC SmartDefender, com integração (opcional) com a nuvem de segurança da ESET. Em tempo real são feitas as seguintes análises:

- Arquivos/Anexos;
- URL's;
- IP's;
- "Reputação";
- Entre outras análises de segurança;

A ESET é utilizada como antivírus secundário (opcional), a nível de camada de proteção de Nuvem Global (que já conta com o antivírus HSC SmartDefender antivírus).

Obs: Importante salientar que a atuação da ESET, é para importação de IOA's e IOC's, bem como análise de ameaças locais, trabalhando em conjunto com o HSC SmartDefender antivírus (antivírus independente da HSCBRASIL).



Tanto a ESET, quanto a HSC SmartDefender antivírus são nuvens de segurança que permitem uma análise em tempo real reagindo a ataques em menos de 60 Segundos!

Contando com uma vasta gama de sensores e amostras, o HSC SmartDefender antivírus e o ESET trazem o que há de mais moderno em termo de segurança e resposta a incidentes!

Eles de imediato já detectam em diversos arquivos os ataques do tipo:

- Exploits;
- Powershell e outros ataques baseados em scripts;
- Phishing;
- Ataque do tipo Fileless (Stealth);
- Hidden codes;
- Códigos encapsulados;
- Ransomware;
- Malwares desconhecidos (sem assinaturas);

Maiores Informações:
https://www.bitdefender.com/business/enterprise-products/elite-security.html#protection
https://www.eset.com/us/about/technology/

Também é possível configurar o envio de anexos suspeitos (automaticamente) para análise comportamental, comparação de assinaturas e outras tecnologias incorporadas à solução, para depuração de qualquer anomalia.

Como as soluções de anti-malware são integrados no MailInspector (as bases de assinaturas dos fabricantes parceiros são incorporadas no Banco de Dados da HSCBRASIL, incluindo as próprias assinaturas da HSCBRASIL, dessa forma formando um BigData único e sempre atualizado com as últimas vacinas).

Além da parte viral/malware (vacinas e análise de ameaças), a integração com a ESET, passa por verificação de URL's, IP's de origem do e-mail, reputação do remetente, entre outros parâmetros de segurança, detectando inclusive técnicas de steath, ameaças polimórficas, técnicas de esteganografia, etc.

Importante salientar que a ESET, é engine "extra", para aumento da segurança da ferramenta. Ela é executada de forma independente, sem nenhuma interdependência do principal sistema de proteção do MailInspector que é HSC SmartDefender antivírus.

HSC Outbreak Filter

O HSC MailInspector possui um sistema de detecção avançado de surto de novas ameaças, permitindo ao administrador configurar as ações que serão tomadas em tempo real quando um novo surto de ataque iniciar. Este controle é feito na camada SMTP durante o diálogo, trabalhando como um Firewall a nível de protocolo SMTP.

As análises de surtos baseiam-se em:

- Quantidade de e-mails com código malicioso enviados por uma única fonte de origem;
- Quantidade de e-mails com destinatários inválidos de uma única fonte de origem;
- Quantidade de SPAM's enviados da mesma origem;

Podemos definir a quantidade ou percentual de e-mails enviados por uma determinada origem (por IP ou domínio) durante um período específico. Uma vez ultrapassado o limite, é efetuado o bloqueio automático e gerado alerta ao administrador (caso tenha sido configurado para tal ação).

Alinhamento com Boas Práticas de Segurança

Framework MITRE ATT&CK

Aproveitando as táticas e técnicas dessa estrutura, o MailInspector ajuda as organizações a aprimorarem seus protocolos de segurança contra ameaças avançadas, seguindo os preceitos indicados pelo Framework MITRE ATT&CK:

Mitigação	
Auditoria	As soluções de e-mail corporativo têm mecanismos de monitoramento que podem incluir a capacidade de auditar regras de encaminhamento automático regularmente. Em um ambiente Exchange, os administradores podem usar Get-InboxRule para descobrir e remover regras de encaminhamento automático potencialmente maliciosas. O MailInspector possui auditoria completa sobre o sistema, desde quem fez, quando e o que foi feito no MailInspector, podendo ser desde criação de regras, até mesmo leitura de e-mails e exclusão de dados. Também pode criar regras de DLP, para alertas de redirecionamento de e-mail ou bloqueio.
Criptografia de Dados Sensíveis	O uso de criptografia fornece uma camada adicional de segurança para informações confidenciais enviadas por e-mail. A criptografia usando criptografia de chave pública exige que o adversário obtenha o certificado privado junto com uma chave de criptografia para descriptografar as mensagens.

	O MailInspector possui criptografia tanto na base de dados (e-mails quarentenados, permitindo ao administrador selecionar o tamanho da chave e o sistema de criptografia utilizado), quanto a opção de criptografar dados sensíveis, tais como criptografia de e-mails específicos e/ou sigilosos.
Autenticação com Múltiplos Fatores	O uso de autenticação múltiplos fatores para servidores de webmail voltados para o público é uma prática recomendada para minimizar a utilidade de nomes de usuário e senhas para adversários. Para atender esse ponto, o MailInspector possui integração com os seguintes sistemas de MFA: • Google Authenticator; • Microsoft Authenticator;

Detecção	
Application / Log Content	A detecção é desafiadora porque todas as mensagens encaminhadas devido a uma regra de encaminhamento automático têm a mesma apresentação de uma mensagem encaminhada manualmente. Também é possível que o usuário não esteja ciente da adição de tal regra de encaminhamento automático e não suspeite que sua conta tenha sido comprometida; as regras de encaminhamento de e-mail sozinhas não afetarão os padrões de uso ou operações normais da conta de e-mail. As mensagens encaminhadas automaticamente geralmente contêm artefatos detectáveis específicos que podem estar presentes no cabeçalho; tais artefatos seriam específicos da plataforma. Os exemplos incluem X-MS-Exchange-Organization-AutoForwarded definido como verdadeiro, X-MailFwdBy e X-Forwarded-To. O parâmetro forwardingSMTPAddress usado em um processo de encaminhamento gerenciado por administradores e não por ações do usuário. Todas as mensagens da caixa de correio são encaminhadas para o endereço SMTP especificado. No entanto, ao contrário das regras típicas do lado do cliente, a mensagem não aparece como encaminhada na caixa de correio; parece que foi enviado diretamente para a caixa postal de destino especificada. Grandes volumes de e-mails com o cabeçalho X-MS-Exchange-Organization-AutoForwarded (indicando encaminhamento automático) sem um número correspondente de e-mails que correspondam à aparência de uma mensagem encaminhada podem indicar que é necessária uma investigação mais aprofundada no nível do administrador, em vez de nível de usuário. O MailInspector possui análise completa do cabeçalho, incluindo cabeçalhos customizados. Dessa forma, é possível o administrador criar regras de detecção de cabeçalhos com redirecionamento de e-mail, dessa forma, se sair um e-mail do servidor de e-mail da empresa, com redirecionamento automático, o MailInspector o detectará e tomará as devidas providências, definidas pelo administrador do sistema.
Command Execution	Monitore processos executados e argumentos de linha de comando para ações que podem ser executadas para coletar arquivos de e-mail locais. As ferramentas de acesso remoto com recursos integrados podem interagir diretamente com a API do Windows para coletar informações. As informações também podem ser adquiridas por meio de ferramentas de gerenciamento do sistema Windows, como Windows Management Instrumentation e PowerShell.

	Em sistemas Windows, monitore a criação de regras de caixa de entrada suspeitas por meio do uso dos cmdlets New-InboxRule, Set-InboxRule, New-TransportRule e Set-TransportRule do PowerShell. O MailInspector possui monitoramento completo do e-mail, através de linha de comando, permitindo o administrador visualizar os comandos executados na filtragem do e-mail, bem como efetuar buscar através do Mail Tracker, onde são apresentadas em tempo real os comandos executados sobre o e-mail, bem como o resultado da resposta da instrução. Também é possível efetuar integração com outras ferramentas do tipo SIEM ou integração via API.
File Access	Monitorar o acesso de processos incomuns de arquivos de e-mail do sistema local para Exfiltration, processos incomuns conectando-se a um servidor de e-mail dentro de uma rede ou padrões de acesso incomuns ou tentativas de autenticação em um servidor de webmail público podem ser indicadores de atividade maliciosa. O MailInspector possui sistema de SandBox, onde ele avalia em nuvem a execução de anexos e o comportamento dos mesmos. Caso seja apresentado comportamento anômalo, tais como acesso indevido de área da memória, tentativas de aceso ao registro do Windows, autenticação em sistemas ou outros padrões de ataque, o e-mail por padrão é quarentenado e apresentado o resultado da análise dos anexos.
Logon Session	Monitore atividades de login incomuns de locais desconhecidos ou anormais, especialmente para contas privilegiadas (por exemplo: conta de administrador do Exchange). O MailInspector possui sistema de registro de logins, bem como controle de acesso baseado em redes e privilégios. Caso seja detectado acessos anômalos, o sistema faz o bloqueio da origem do acesso.
Network Traffic	Monitore as conexões de rede recém-construídas que são enviadas ou recebidas por hosts não confiáveis. O MailInspector possui sistema de detecção de DUL attack, ou seja, de redes novas ou que não tenham registros de envio de e-mails. É baseado em reputação do emissor, bem como detecção de redes DULs (IP's públicos de uso residencial, ou de pouco histórico de emissão de e-mails).

Seguindo os protocolos de segurança avançado, o MailInspector ainda conta com:

- **Proteção a ataques direcionados (TAP):** Projetada para detectar e bloquear ataques direcionados por e-mail, mídia social e dispositivos móveis. O TAP usa vários mecanismos de detecção, como análise estática e sandbox dinâmico, para identificar conteúdo malicioso em tempo real.
- **E-mail Fraud Defense (EFD) ou Proteção a BEC (Business E-mail Compromise):** A EFD emprega algoritmos de aprendizado de máquina para detectar anomalias em cabeçalhos de e-mail ou padrões de comportamento do remetente que podem indicar tentativas de representação ou técnicas de falsificação usadas em golpes BEC.
  SmartDefender: Essa plataforma coleta dados de várias fontes de indicação de ameaças (bilhões de IOC's por dia), incluindo o MITRE ATT&CK Framework, e os correlaciona com eventos de rede interna[1] para uma visão completa do cenário de ameaças de uma organização. Conta também com BigData da ESET e CrowdStrike[2], portanto o cliente MailInspector conta com BigData de dois fabricantes (ESET e HSCBRASIL), para auxílio no monitoramento de ameaças tanto por e-mail, quanto

por ocorrências anômalas na sua rede, através de comparações dos resultados obtidos entre MailInspector e rede interna, dessa forma formando uma rede informações de ameaças, conhecida como Threat Intelligence.

- **M-SOAR:** Sistema de integração completa com Office365, permitindo ao administrador tomar ações sobre e-mails que foram entregues, como por exemplo apagar e-mail entregue ao usuário, dessa forma, mitigando eventual falso negativo que tenha passado pelo sistema, ou até mesmo bloquear conta de usuário, através do painel do MailInspector, sem necessidade do administrador acessar o Office 365 para atuar nas contas comprometidas.

[1] Necessário uso de SIEM ou sistema de orquestração integrados ao MailInspector
[2] Necessário que o cliente possua licença de uso do CrowdStrike Falcon Complete

As referências do Framework MITRE ATT&CK é utilizado junto o módulo *Risk Management para Microsoft 365*

Aderência ao padrão Traffic Light Protocol (TLP)

Em atendimento ao **CTIR Gov (Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos do Governo)**, o MailInspector possui compatibilidade com o padrão TLP.

Referência: https://www.gov.br/ctir/pt-br/assuntos/tlp

É possível usar as TAGs de TLP sobre o assunto, anexos e conteúdo dos e-mails, casando-se com o sistema DLP, tanto para gerar alertas, quanto para bloqueio de e-mails indevidos.

Lembrando que o conceito de TLP é possuir a TAG de TLP em arquivos, textos e anexos, bem como assunto do e-mail, para indicação de possível compartilhamento do conteúdo, de acordo com a sensibilidade do conteúdo.

	RGB: font			RGB: background			CMYK: font				CMYK: background				Hex: font	Hex: background
	R	G	B	R	G	B	C	M	Y	K	C	M	Y	K		
TLP:RED	255	43	43	0	0	0	0	83	83	0	0	0	0	100	#FF2B2B	#000000
TLP:AMBER	255	192	0	0	0	0	0	25	100	0	0	0	0	100	#FFC000	#000000
TLP:GREEN	51	255	0	0	0	0	79	0	100	0	0	0	0	100	#33FF00	#000000
TLP:CLEAR	255	255	255	0	0	0	0	0	0	0	0	0	0	100	#FFFFFF	#000000

TLP:RED = Somente para os olhos e ouvidos dos indivíduos destinatários, não é permitido compartilhamento nenhum.

TLP:AMBER = Divulgação limitada, destinatários só podem disseminar para aqueles que necessitam saber (need-to-know basis) dentro de sua própria organização e com seus clientes.

TLP:GREEN = Divulgação limitada, destinatários podem divulgar dentro de sua comunidade. Fontes podem usar TLP:GREEN quando a informação é útil para a conscientização dentro de sua comunidade mais ampla.

TLP:CLEAR = Destinatários podem disseminar para o mundo, não há limites na divulgação. Fontes podem usar TLP:CLEAR quando há um risco mínimo ou não há previsão de risco de mau uso da informação, de acordo com regras e procedimentos aplicáveis para divulgação pública.

Proteção nativa a vulnerabilidade a SMTP Smuggling

O ataque de SMTP Smuggling tem como alvo uma vulnerabilidade do protocolo SMTP, em que um invasor pode abusar das diferenças na maneira como os servidores SMTP de saída e de entrada interpretam uma sequência que indica o fim dos dados da mensagem. Isso permite a injeção de comandos SMTP em mensagens de e-mail de uma forma que faz com que os servidores de recebimento as tratem como duas mensagens separadas, sendo que uma delas tem seu cabeçalho "De" falsificado. Além disso, como o envelope da mensagem principal passa com êxito nas verificações de protocolos de segurança de e-mails, tais como SPF, DKIM e DMARC, a mensagem falsificada é entregue nas caixas do correio eletrônico.

É importante ressaltar que embora o SMTP Smuggling mesmo que burle os mecanismos de autenticação de servidores de e-mails (caso o administrador desative a proteção contra SMTP Smuggling), o sistema de inteligência do MailInspector captura os falsos e-mails com base em seu contexto e outros fatores.

O MailInspector além de já vir com proteção ativada sobre os ataques de SMTP Smuggling, possui também mecanismos complementares de proteção que atuam em outras etapas no diálogo SMTP, detectando dessa forma muitos outros ataques que exploram a vulnerabilidade do protocolo SMTP, em atendimento ao CVE-2023-51764, CVE-2023-51765, CVE-2023-51766 e CVE-2023-52354.

O HSC MailInspector por utilizar uma abordagem única de Secure E-mail Gateway + API é capaz de entender os diferentes vetores de ataque e agir de forma efetiva, independentemente do tipo de ataque.

Proteção a Contas Invadidas - Account TakeOver (ATO)

O MailInspector por meio de integração direta ao Office365/G-Suite, permite que a solução faça bloqueio direto na conta do usuário na Microsoft/Google quando é detectado o roubo de credencial dele (detecção efetuada por meio de controle de fluxo e Message Reputation - que verifica vários fatores comportamentais, tais como volumetria, frequência de envio, horários de envio, tipo de e-mail enviado, etc), dessa forma, dá ao administrador uma maior agilidade na prevenção de maiores prejuízos gerados pelo roubo de credencial, evitando disparo de e-mails maliciosos a e-mail de outros colaboradores da empresa, bem como possível bloqueio do IP da empresa em RBL's devida a uma conta roubada.

Módulos Adicionais/Opcionais

Analisador de DMARC

O sistema DMARC é uma excelente ferramenta como camada de proteção e prevenção de ataques que as empresas sofrem através de fraudes com o domínio da empresa atacada.

O grande problema é a interpretação do grande volume dos e-mails padrão XML e/ou MIME que são enviadas para a empresa dona do domínio pelos ISPs. Os relatórios do DMARC podem indicar:

- Quais servidores ou remetentes de terceiros estão enviando e-mails usando o seu domínio;
- Qual a porcentagem de mensagens de seu domínio que passam no DMARC;
- Quais servidores ou serviços estão enviando mensagens que falham no DMARC;
- Quais ações DMARC o servidor receptor realiza em mensagens não autenticadas de seu domínio:
    - None;
    - Quarantine;
    - Reject;

Por que usar o Analisador de DMARC do MailInspector?

- Os relatórios XML DMARC são muito difíceis de ler;
- É praticamente impossível interpretar as informações em XML puro, dessa forma não é possível resolver problemas de entrega de e-mail (Spoofing de criminosos usando o seu domínio como origem);
- Facilidade de ter tudo em um único sistema, sem ter que sair do MailInspector e a necessidade de adquirir e acessar solução de terceiro, para obtenção das informações e relatórios de DMARC;

O MailInspector possui o sistema de análise de relatórios emitidos pelo DMARC, dessa forma basta configurar o sistema de coleta do e-mail (IMAP), que o analisador verificará todos os XMLs (tanto os agregados/RUA, quanto os foreneses/RUF) e apresenta os dados tabulados e de forma gráfica de fácil interpretação.

O Analisador de DMARC atende o número de domínios que estiverem configurados para proteção na solução, dessa forma não há necessidade de comprar licenças por limite de domínios, nem por limite de e-mails.

O processamento de número de e-mails passa de 10.000.000 de mensagens de DMARC por mês, deixando unicamente a cargo da capacidade de armazenamento de relatórios da caixa postal, configurada para recebimento dos e-mails de RUF e RUA.

O módulo Analisador de DMARC é um módulo do HSC MailInspector licenciado à parte, para o uso do mesmo é necessário aquisição da licença específica para este fim.

M-SOAR / DeepIntegration / Add-On

O SOAR tem como foco ajudar na resposta a incidente. No SOAR é possível orquestrar um SOC, automatizarmos ações, análises e muito mais e além disso responder incidentes, tudo isso de forma simples e fácil, e em alguns casos, sem a necessidade de interação humana.

O MailInspector nativamente já trabalha com verificação de conteúdo malicioso diretamente sobre o e-mail e seus anexos na sua camada de anti-vírus e efetua a análise em SandBox, integrando o resultado da análise via API e/ou GarphQL.

O sistema M-SOAR atua na remediação de ameaças no cenário pós-delivery, realizando a avaliação e correlação de diferentes elementos de segurança. Além dos recursos próprios da HSCBRASIL, como o SmartDefender, assinaturas de IoCs e IoAs, entre outros indicadores de comprometimento e comportamento, a solução também conta com integrações externas, incluindo o VirusTotal, AlienVault e servidores STIX/TAXII, ampliando a capacidade de análise, enriquecimento de informações e resposta a incidentes de segurança.

O MailInspector utiliza o M-SOAR como componente especializado na automação e remediação de ameaças relacionadas a e-mails. Dessa forma, a solução permite automatizar ações sobre mensagens já entregues aos usuários, incluindo processos de identificação, análise e remediação. O M-SOAR integra com ambientes como Microsoft Office 365, Google Workspace (antigo G Suite) e Zimbra, ampliando a capacidade de resposta a incidentes e permitindo ações automatizadas diretamente sobre os e-mails.

O **administrador** do MailInspector poderá definir as seguintes ações para os e-mails que foram entregues ao usuário:

- Remoção de Anexos nos e-mails já entregues;
- Remoção de links em e-mails já entregues ao servidor de e-mail;
- Mover o e-mail entregue para a lixeira eletrônica;
- Bloqueio de conteúdo de mensagem entregue;
- Apagar na caixa de correio eletrônico uma ou mais mensagens já entregues;
- Bloquear usuário no Active Directory, por um botão no MailInspector;

A integração é de modo transparente, sem necessidade de intervenção do usuário. Todo o conjunto de ações é efetuada diretamente por GraphQL, dessa forma, o administrador ao decidir uma ação sobre o e-mail, o mesmo é efetuado diretamente na caixa postal do usuário, sem qualquer interação por parte dele.

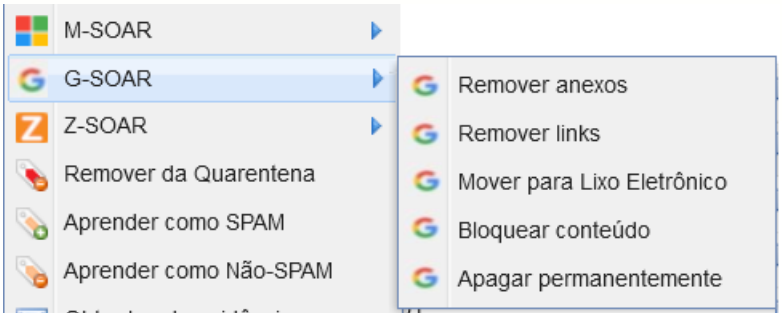
A integração com o Microsoft Office 365, Google G-Suite e Zimbra com GraphQL, permite evoluir a API da aplicação sem prejudicar as consultas existentes (além de permitir o uso sobre a API REST existente), garantindo a integridade dos dados, ou seja, não corre risco de executar uma ação sobre o e-mail errado.

Tanto em Microsoft Office365 quanto em Google G-Suite, o MailInspector permite adição de botão (através de Add-On) de ação visível a todos os usuários na sua caixa de correio, permitindo que o usuário tome ações sobre os e-mails **ENTREGUES**. Tais ações podem ser:

- Aprender Mensagem como SPAM;
- Aprender Mensagem como NÃO SPAM;
- Enviar amostra de Phishing, Vírus ou outra ameaça ao administrador, contendo uma cópia do e-mail original (com preservação do cabeçalho original, corpo e anexos) para que o administrador possa analisar e tomar as devidas providencias;

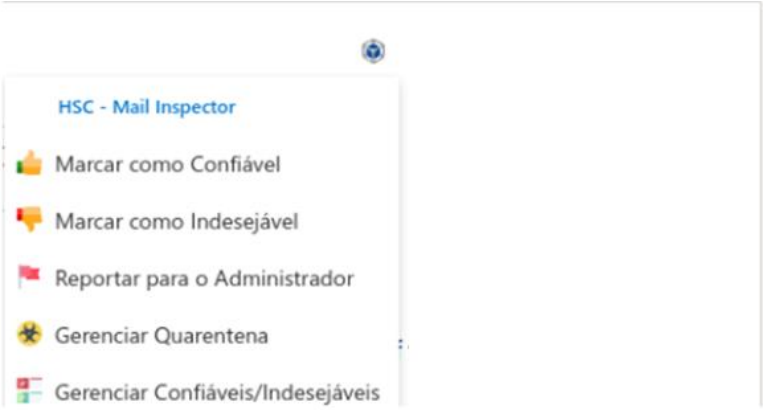
Já em relação aos e-mails **NÃO ENTREGUES** (quarentenados), os usuários de Microsoft Office365, Google G-Suite e Zimbra, poderão tomar ações sobre eles, ou seja, o próprio usuário poderá definir ações sobre os e-mails que foram para a sua própria quarentena individual. As ações permitidas são:

- Liberar o e-mail da quarentena (falso positivo);
- Marcar o remetente como confiável;
- Marcar o remetente como indesejável;
- Realizar pesquisa pelo Remetente e/ou Assunto do e-mail sobre os e-mails quarentenados;



Tela de ações possíveis no módulo M-SOAR (Microsoft Office 365, Google G-Suite e Zimbra)

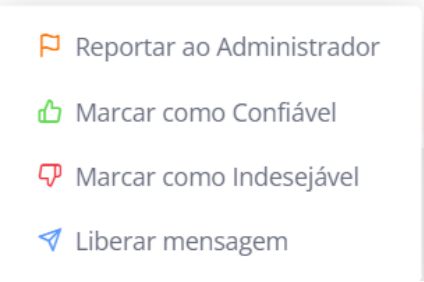
Com a integração do API através do Add-On, ao clicar no ícone da HSCBRASIL, presente após a integração do Add-On, aparecerá o menu, com as seguintes ações:



- **Marcar como Confiável:** Marca o remetente como confiável (allow list pessoal).
- **Marcar como Indesejável:** Marca o remetente como não confiável (block list pessoal).
- **Reportar para o Administrador:** Reporta o e-mail como phishing, enviando automaticamente o e-mail como amostra ao administrador e para a HSCBRASIL.
- **Gerenciar Quarentena:** Abre toda a quarentena do usuário, para ele gerenciar os e-mails quarentenados (liberar/excluir/visualizar/reportar/marcar como confiável/marcar como não confiável).
- **Gerenciar Confiáveis/Indesejáveis:** Habilita ao usuário gerenciar a lista dos que estão marcados como remetente confiável e remetente não confiável, permitindo ao usuário remover/incluir qualquer entrada nessa lista.

O usuário ao selecionar a opção de **Gerenciar Quarentena**, o usuário terá acesso ao gerenciamento dos e-mails na quarentena dele, ao qual poderá efetuar as seguintes ações (por padrão):

- **Reportar ao Administrador:** Reporta ao administrador como phishing/spam/outra ameaça;
- **Marcar como Confiável:** Marca o remetente do e-mail como confiável, para os próximos e-mails não serem quarentenados por pontuação de SPAM;
- **Marcar como Indesejável:** Marca o remetente do e-mail como indesejável, para os próximos e-mails do remetente serem quarentenados automaticamente;
- **Liberar Mensagem:** Libera a mensagem quarentenada;



Dessa forma o próprio usuário poderá tomar as ações sobre os e-mails quarentenados, bem como reportar ao administrador qualquer falso negativo e o tipo de e-mail do falso negativos, se é phishing, spam ou outra ameaça.

Risk Management para Microsoft 365

Esse módulo permite a visibilidade detalhada das ameaças e dos usuários, através da integração com o Office365, dessa forma, oferece análises inteligentes, notas de risco comparativas e recomendações de boas práticas de mitigação.

- **Relatórios individuais das ameaças:** Cada incidente é identificado de forma única, com informações completas sobre região/país alvo da ameaça, plataformas impactadas e campanhas de ataque em andamento.
- **Detecção de usuários em risco:** Detecta a plataforma e local utilizado para o acesso ao e-mail, dessa forma é possível efetuar bloqueio de um usuário que esteja acessando o e-mail de um local indevido, ou detecção a usuários que não tem o MFA ativado, bem como indicação de sugestões de melhoria na segurança individual, de acordo com as ações tomadas nos e-mails pelo usuário (como por exemplo cliques em links maliciosos, abertura de e-mails suspeitos, etc).
- **Perfil por usuário:** Visualização do tipo de conta, privilégios, grupos de acesso, status e nota de risco cibernético, verificando atividades anômalas do usuário na plataforma. Também é verificado se o usuário tem real necessidade do perfil atribuído a ele, isto é, se as atividades exercidas pelo usuário condizem com as permissões liberadas a ele. São apresentados:
    - Tipo de conta;
    - Privilégio;
    - Grupo pertencente;
    - Nota de risco cibernético;
    - Status da conta;
- **Nota de risco comparativa:** Análise contínua baseada em frameworks reconhecidos como NIST, comparável por indústria, região ou porte da organização.
  É feita a comparação de Score da Empresa em relação ao Score Global do Setor. De acordo com a comparação de Score, é indicado o nível de risco (Status).
  Os setores analisados para uso comparativo são:
    - Serviços Financeiros e Bancários (bancos, fintechs, seguradoras)
    - Setor Público / Governamental
    - Saúde (hospitais, clínicas, operadoras de planos)
    - Educação (universidades, escolas, institutos de pesquisa)
    - Indústria / Manufatura

- Energia e Utilities (óleo e gás, elétrica, saneamento)
- Tecnologia e Telecomunicações
- Varejo e E-commerce
- Transportes e Logística
- Setor Jurídico e Judiciário

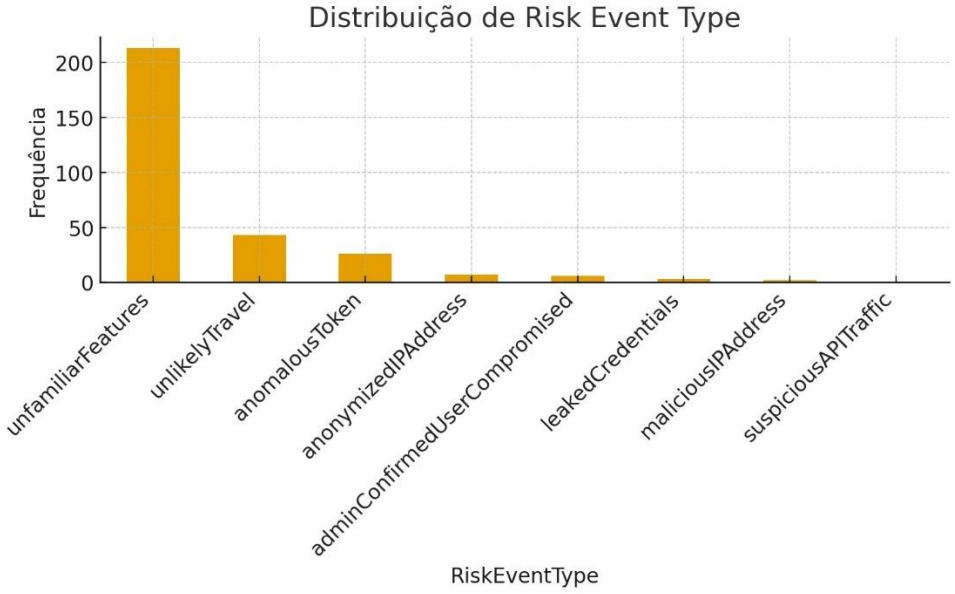
- **Tabela resumo:**

Setor	Score Empresa	Score Médio	Status	Gap
Financeiro	62	55	🔴 Acima	+7
Saúde	58	61	🟢 Abaixo	-3
Governo	65	63	🔴 Acima	+2
Varejo	54	59	🟢 Abaixo	-5

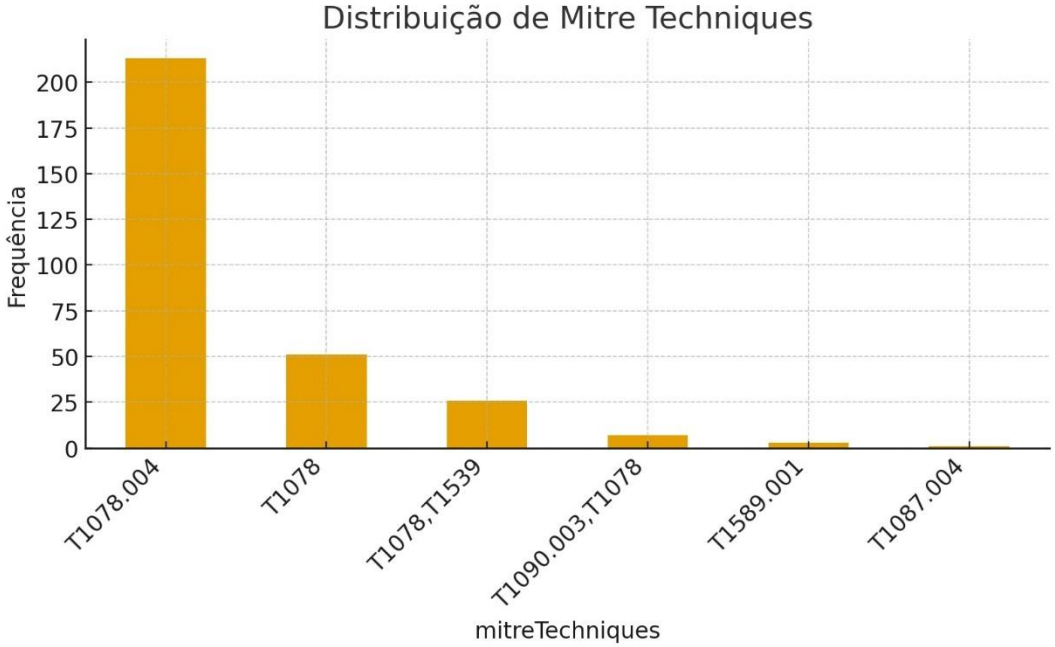
Dashboard de Comparação Global por Setor Empresarial

- **Gestão dinâmica de risco:** Possibilidade de encerrar eventos e recalcular a pontuação sob demanda, além de um índice global de risco para a organização.
- **Recomendações inteligentes:** Sugestões automáticas indicadas pela IA, através de ações de maior impacto para reduzir a exposição.
- **Mapeamento MITRE ATT&CK:** Os principais alertas associados às táticas do MITRE, permitindo alinhar a resposta a padrões globais de segurança.

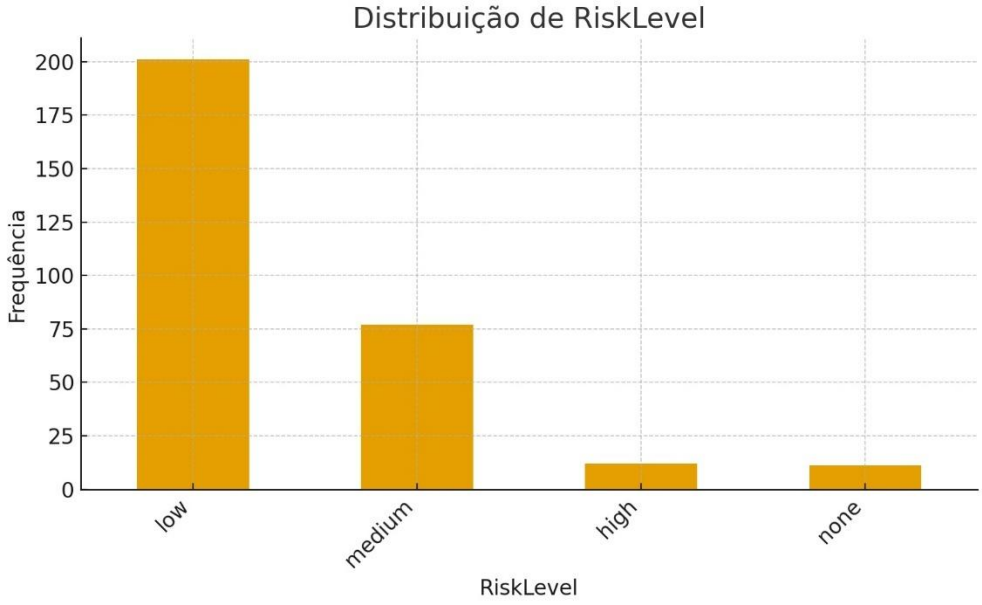
Tela de detecção de ameaças, com indicação de grau de risco, técnicas MITRE empregadas e detecção de risco



Dashboard de distribuição de risco



Dashboard de Técnicas MITRE



Dashboard de Nível de Risco

O Todos os relatórios apresentados pelo módulo de Risk Management para Microsoft 365 são possíveis de serem exportados nos modelos PDF, CSV e XLS.

O módulo Risk Management para Microsoft 365 é alinhado com as boas práticas de segurança utilizado em *Framework MITRE ATT&CK*

AutoWhitelist

Sistema automatizado que monitora o tráfego de dados enviados por cada servidor de origem, aprendendo dinamicamente se ela é um emissor de SPAM ou não. Caso a origem tenha um bom comportamento ela automaticamente será beneficiada e terá sua pontuação reduzida como SPAM. Este sistema é automatizado e a lista de IPs é atualizada dinamicamente através da reputação local e da reputação Global do SmartDefender.

Algumas RFC's atendidas pelo MailInspector

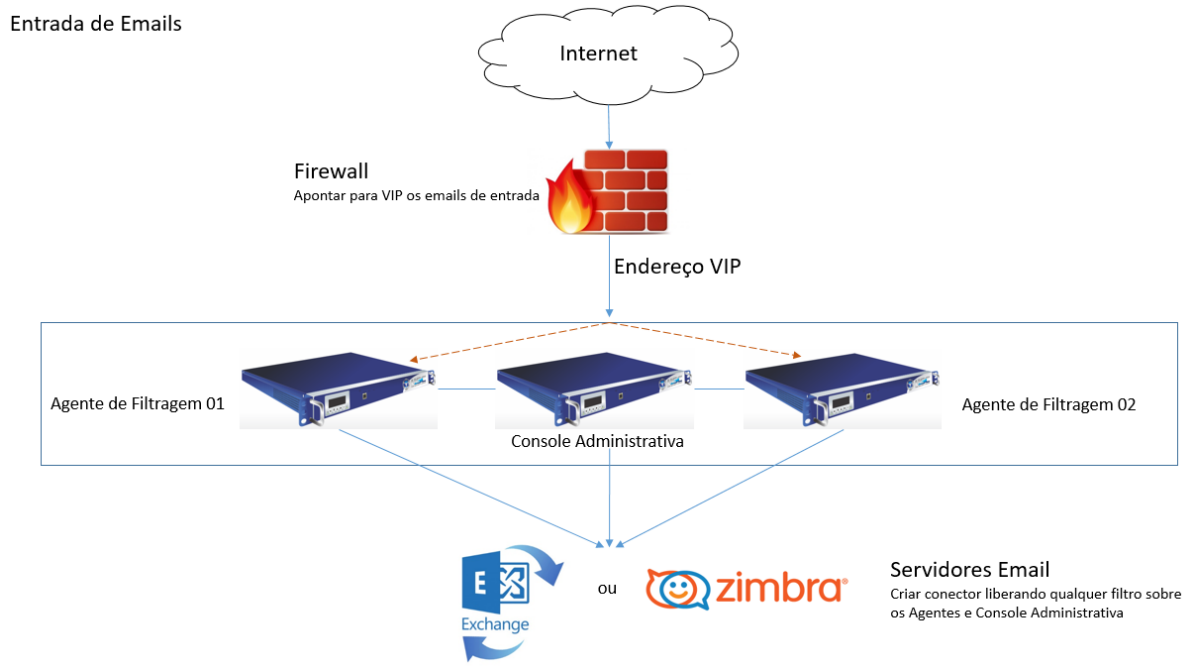
Lista de **algumas** RFC's atendidas pelo MailInspector:
RFC 1213, RFC 1918, RFC 1985, RFC 2034, RFC 2045, RFC 2505, RFC 2634, RFC 2920, RFC 3207, RFC 3461, RFC 3463, RFC 3464, RFC 3635, RFC 4954, RFC 5321, RFC 5322, RFC 6376, RFC 6522, RFC 6409, RFC 2088, RFC 2177, RFC 2221, RFC 2342, RFC 2683, RFC 2971, RFC 2822, RFC 3348, RFC 3501, RFC 3502, RFC 3516, RFC 3691, RFC 4315, RFC 4469, RFC 4731, RFC 4959, RFC 5032, RFC 5161, RFC 5182, RFC 5255, RFC 5256, RFC 5258, RFC 5267, RFC 5819, RFC 6154, RFC 6851, RFC 6854, RFC 7162, RFC 7208, RFC 1939, RFC 2449, RFC 1155, RFC 1157, RFC 2578, RFC 2579, RFC 2595, RFC 3410, RFC 3416, RFC 5336, RFC 6531, RFC 7489;

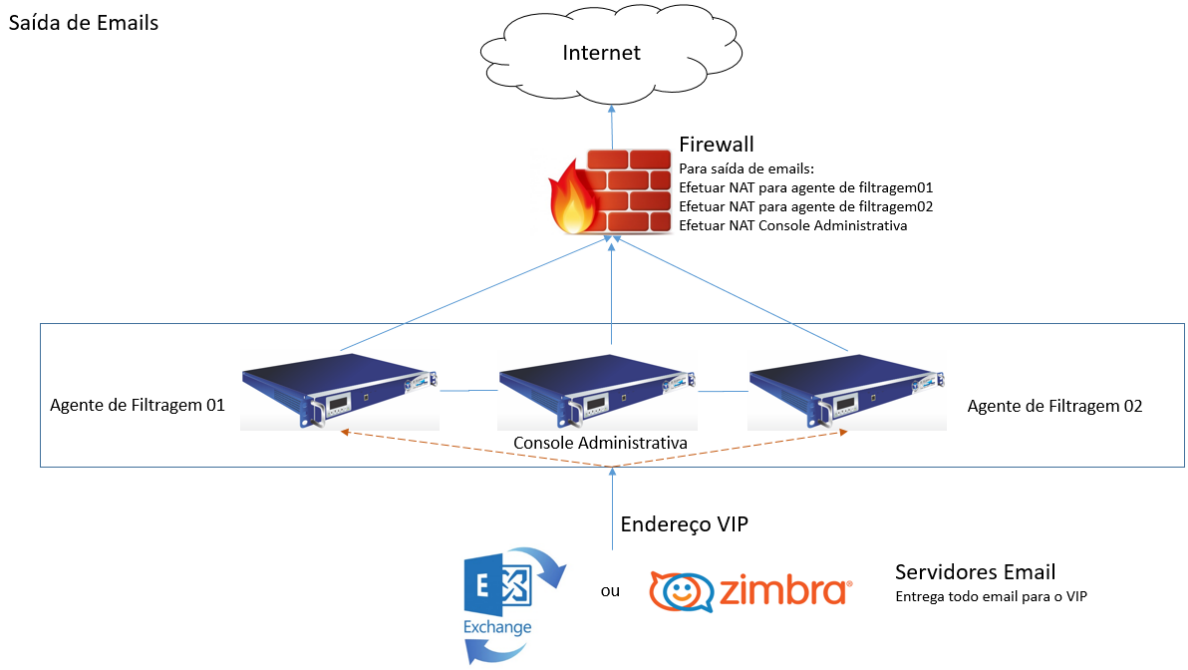
Maiores informações em: *Apêndice 2 - RFC's Suportadas*

Arquitetura de implantação

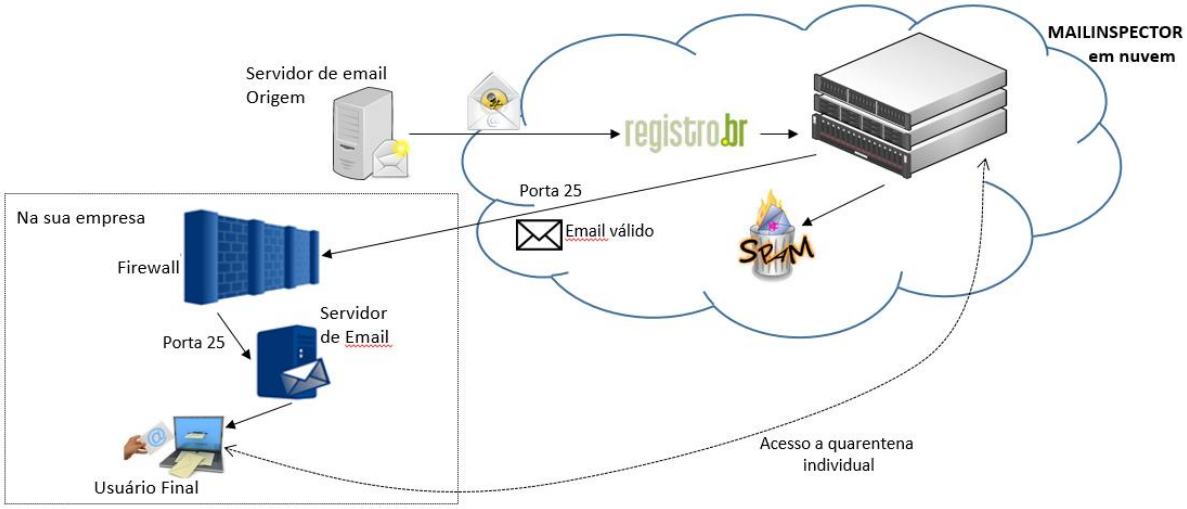
O MailInspector pode ser instalado na empresa de diversas forma, tais como:

- Localmente
  Instalado dentro do datacenter da empresa, ficando entre o firewall e o servidor de e-mail.
  Segue exemplo com o desenho abaixo utilizando dois agentes de filtragem e um gerenciador.





- Nuvem da empresa
  Instalado em um datacenter na nuvem, ao qual os servidores ficam dentro da empresa.
  Então dessa forma os e-mails são apontados pelo DNS aos IP's do MLI na nuvem e filtrados. Após a filtragem, os e-mails são encaminhados aos IP's do firewall da empresa, que por sua vez, encaminha aos servidores de e-mail.



Fluxo de tráfego de mensagens

O HSC MailInspector tem como objetivo permitir ao administrador o total controle e gestão das mensagens enviadas e recebidas pela empresa. Seu poderoso conjunto de filtros permite a realização de uma inspeção profunda de todas as mensagens recebidas e enviadas (entrada e saída) ou até mesmo os e-mails internos da empresa, sem limite de quantidade de mensagens diárias.

Integração com sistemas seguros de autorização com MFA (Múltiplo Fator de Autenticação)

Nativamente o MailInspector já conta com 2FA (Duplo Fator de Autenticação) usando o padrão OTP (One Time Password). O mesmo é compatível com os principais sistemas de duplo fator de autenticação do mercado, tais como:

- Google Authenticator;
- Microsoft Authenticator;

Além de uso com o protocolo OTP (nativo no MailInspector), é possível ativar a autenticação com outras formas de multifator com a empresa parceira **Auth0.** Também possui total integração com provedores de serviço de identificação (iDP) através dos protocolos SAML2 e OpenID, além de integração nativa com Microsoft 365 e Google Workspace.

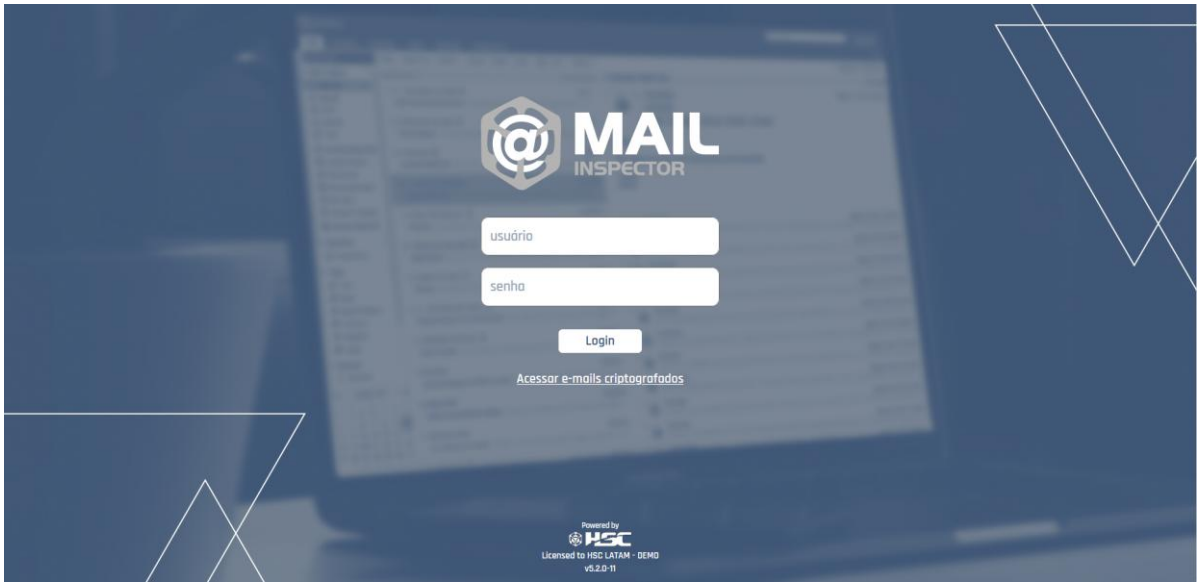
Soluções de MFA oferecem suporte a diferentes fatores de autenticação, como notificações push (Através de Aplicativos de celular Android e IPhone), biometria do dispositivo, QRCode, e-mail, SMS, entre outros meios.

Caso seja optado o uso de MFA (Autenticação por multifator) que não seja através do protocolo OTP (One Time Password), é necessária aquisição de licenças separadas de soluções de terceiros.

Se for optada por ativação de MFA (Autenticação por multifator) pelo protocolo OTP (One Time Password), com uso de Google Authenticator ou Microsoft Authenticator, não haverá a necessidade de aquisição de licenças de uso para autenticação.

Acessando o MailInspector

Para acessar o MailInspector, basta inserir a URL/IP referente ao sistema de gerenciamento dele no seu browser pelo protocolo HTTPS por padrão.



Tela padrão de login do MailInspector

Para efetuar o login insira as credenciais necessárias. Todo o processo de autenticação é efetuado de forma criptografada, garantindo a segurança de acesso aos administradores e usuários do sistema.

Para maiores informação sobre administração dos usuários do sistema: *Usuários do Sistema*

Na tela inicial, é solicitado o login e senha, que por padrão é:
Usuário: **admin**
Senha: **admin**

Recomendamos que a senha do usuário admin, seja trocada o mais rápido possível.

Também é apresentada nesta mesma tela, na parte inferior, a indicação de licença de uso.

Caso o seu usuário estiver com duplo fator de autenticação ativo, após a inserção da senha, o MailInspector irá solicitar o código do autenticador, além da senha padrão.

Tela de autenticação do segundo fator

Dica: Caso não tenha o autenticador instalado no seu celular, a tela de autenticação do segundo fator apresenta o link para download do autenticador, tanto da Apple, quanto do Google.

O sistema de duplo fator de autenticação do MailInspector é compatível com os principais autenticadores do mercado, entre eles:

- Google Authenticator;
- Microsoft Authenticator;
- Entre outros autenticadores;

É possível integrar a autenticação do MailInspector a sistema SSO (Single Sign On) via LDAP ou Microsoft AD, ou ainda através do Microsoft Azure e/ou G-Suite. Para tanto, é necessário configurar conector externo (no caso de autenticação via AD/LDAP) ou através de API, quando usado autenticação através do Azure/G-Suite.

Conhecendo a interface administrativa

A interface web de administração oferece uma forma fácil, intuitiva e centralizada de encontrar e gerenciar informações, registros/logs, quarentena e configurações/regras/políticas do HSC MailInspector. Permite tanto ao administrador, quanto ao usuário final possam gerenciar os e-mails e os recursos da ferramenta de forma remota a partir de estações de trabalho através dos principais Navegadores do mercado sem a necessidade de instalação de nenhum software adicional. As opções liberadas para configuração, administração e acesso aos e-mails, fica limitado de acordo com o perfil utilizado no momento do login.

A interface permite a administração de forma unificada diversos pontos de um cluster podendo o administrador criar regras, tirar relatórios e administrar de forma centralizada.

Interface Web 2.0 (Segura HTTPS SSL/TLS) é compatível com múltiplos navegadores (independente da linguagem utilizada pelo navegador), dentre eles podemos citar:

- Mozilla Firefox;
- Internet Explorer;
- Microsoft Edge;
- Google Chrome;
- Chromium;
- Safari;
- Opera;
- Comodo Dragon;
- Vivaldi;
- Maxthon;
- Outros navegadores;

É compatível com vários sistemas operacionais, entre eles:

- Linux;
- Apple;
- Windows XP ou superior;

O MailInspector permite acesso local ou remoto para manutenção e suporte, conforme as políticas da empresa.

Possui também acesso a interface de linha de comando via protocolo SSH, bem como o protocolo HTTP padrão (se o administrador assim o configurar – NÃO RECOMANDADO), sem a necessidade de uso de SSL/TLS.

A interface de administração pode ser operada nas seguintes línguas (a ser determinada durante a instalação):

- Português do Brasil;
- Inglês;
- Espanhol;
- Espanhol do Paraguai;
- Finlandês (Suomi);

A interface da console de administração do MailInspector possui expiração (encerramento automático) por inatividade.
O tempo padrão da sessão é de 30 minutos. Caso não tenha nenhum registro de atividade após o período de 30 minutos, a sessão no MailInspector é encerrada.

O HSC MailInspector é dividido em Console de Administração e Ponto de Acesso.

Console de Administração - A console é a parte de sistema responsável por toda administração do produto HSC MailInspector, ela possui a parte de configuração centralizada, relatórios, logs, quarentena, interface de quarentena dos usuários, interface de acesso a mensagens criptografadas, etc.

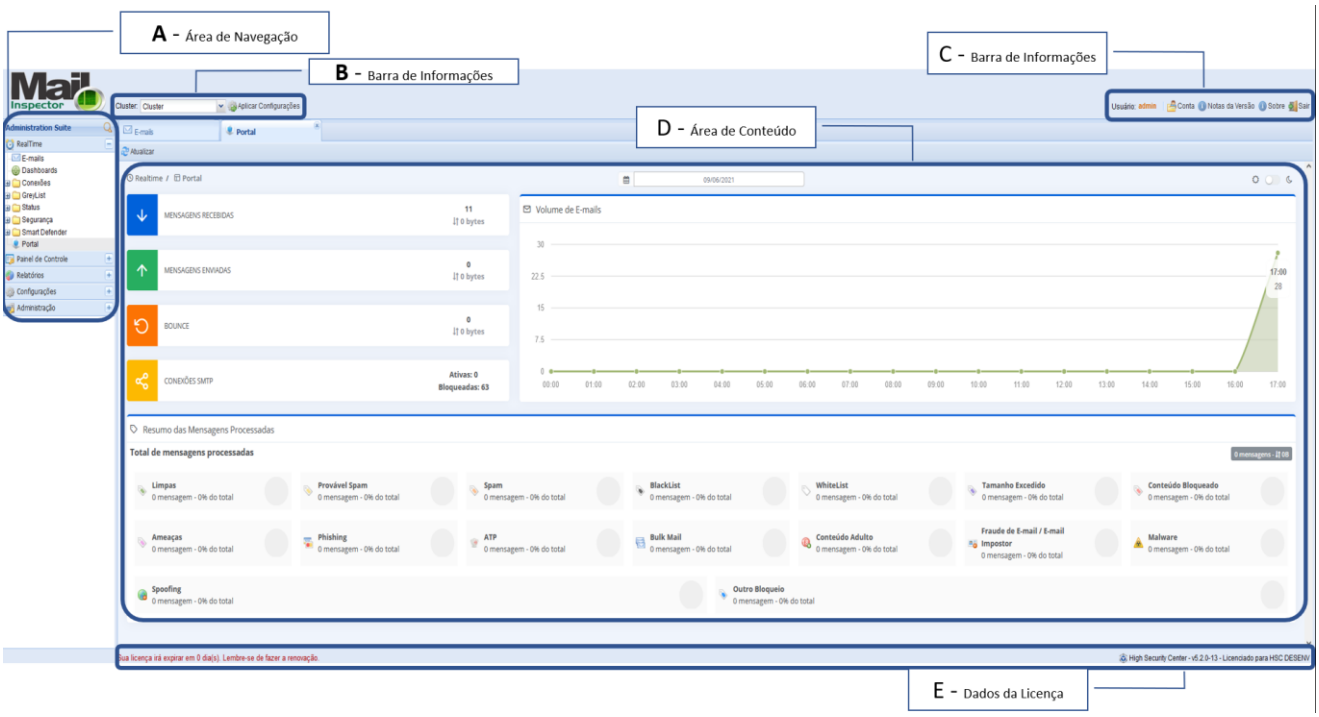
Ela pode ser instalada em um Servidor Físico, Appliance Físico ou Appliance Virtual.

Ponto de Acesso - Componente responsável pelo recebimento, envio e filtragem de todas as mensagens. Ela pode ser instalada separadamente da console de administração, em um ou mais servidores: Físicos, Appliances Virtuais ou Appliances Físicos. Você pode colocar 2 ou mais pontos de acesso a funcionar simultaneamente em modo cluster afim de garantir maior performance e alta disponibilidade.

Os pontos de acesso podem ser instalados em qualquer parte da topologia de rede, DMZ, LAN, Site Backup, conforme a necessidade do administrador.

Os pontos de acesso, também podem ser instaladas em um Servidor Físico, como Appliance Físico ou Appliance Virtual.

A interface que você vê pode ser um pouco diferente da exibida neste documento, pois ela pode variar dependendo da plataforma de hardware, versão do software e da linguagem selecionada.



Portal (Informações dos e-mails recebidos no dia)

A - Área de navegação

A área de navegação contém os seguintes itens:

Menu	Funções
RealTime	Visualiza os e-mails processados pelo produto, os registros e a fila do MTA, e gerencia o sistema da Greylist.
Painel de Controle	Gerencia a Allow List (lista branca) e Block List (lista negra) global, e dos usuários.
Relatórios	Visualiza os relatórios gerenciais e o relatório de eventos ocorridos no produto.
Configurações	Acesso às configurações básicas e avançadas de todos os recursos disponíveis no produto, gerenciamento dos filtros de conteúdo, dos filtros de SPAM, das notificações, da quarentena, das políticas de e-mail, das configurações do MTA, dos grupos de usuários, dos grupos de extensões e dos grupos de mime-types.
Administração	Realiza o cadastro e gerenciamento de servidores, a configuração e execução de cópias de segurança do produto, ferramentas de diagnóstico, gerenciamento dos usuários, entre outras funcionalidades.

B - Barra de informações

A barra de informações permite o acesso rápido aos seguintes itens:

Menu	Funções
Ponto de Acesso	Permite selecionar o servidor que será configurado.
Aplicar Configurações	Permite aplicar manualmente as regras e configurações nos servidores. As mudanças realizadas nas configurações só terão efeito após serem aplicadas no servidor. Maiores informações sobre a aplicação de configuração você pode encontrar em: *Aplicar Configuração*

C - Barra de informações

A barra de informações permite o acesso rápido aos seguintes itens:

Menu	Funções
Conta	Quando configurado para autenticação local, permite a alteração da senha do usuário da interface de administração. Permite ao usuário habilitar ou desabilitar a notificação de quarentena, permitir notificação vazia, configurar o período de envio da notificação e configurar as suas contas de e-mail ou domínios que administra. Linguagem: Português Brasil, Inglês, Espanhol, Castelhano, Alemão, Francês e mais de 30 outras. Sensibilidade do AntiSpam: Permite definir por usuário a sensibilidade do sistema de antispam, conforme definido pelo administrador. Os níveis permitidos são: Permissivo, Normal e Restritivo
Notas da Versão	Permite aos administradores verificar o Release Notes da versão instalada.

Sobre	Exibe informações sobre o licenciamento do produto.
Sair	Efetua a saída segura do sistema.

D - Área de conteúdo

A área de conteúdo é o local de maior interação da interface, todos os itens acessados são exibidos nesta área da tela.

Menu	Funções

Portal	Monitora em tempo real:
	• O volume de e-mails;
	• Mensagens Recebidas;
	• Número de e-mails bounces;
	• Mensagens Enviadas;
	• Conexões SMTP ativas;
	• Conexões SMTP bloqueadas;
	• Qualidade do tráfego de e-mails recebidos, separados por tipo:
	  ○ E-mails válidos (limpos);
	  ○ Provável SPAM;
	  ○ SPAM;
	  ○ Block List;
	  ○ Allow List;
	  ○ Tamanho Excedido;
	  ○ Conteúdo Bloqueado;
	  ○ Ameaças;
	  ○ Phishing;
	  ○ ATP (Ameaças Persistentes);
	  ○ Bulk Mail;
	  ○ Conteúdo Adulto;
	  ○ Controle de Surto / Comportamento Anômalo;
	  ○ Fraude de e-mail / E-mail Impostor;
	  ○ Malware;
	  ○ Spoofing;
	  ○ Outro Bloqueio (ex: Anexo compactado, com executável inserido no anexo);

E - Dados da Licença

Indica se a licença está expirando e para quem o MailInspector está licenciado.

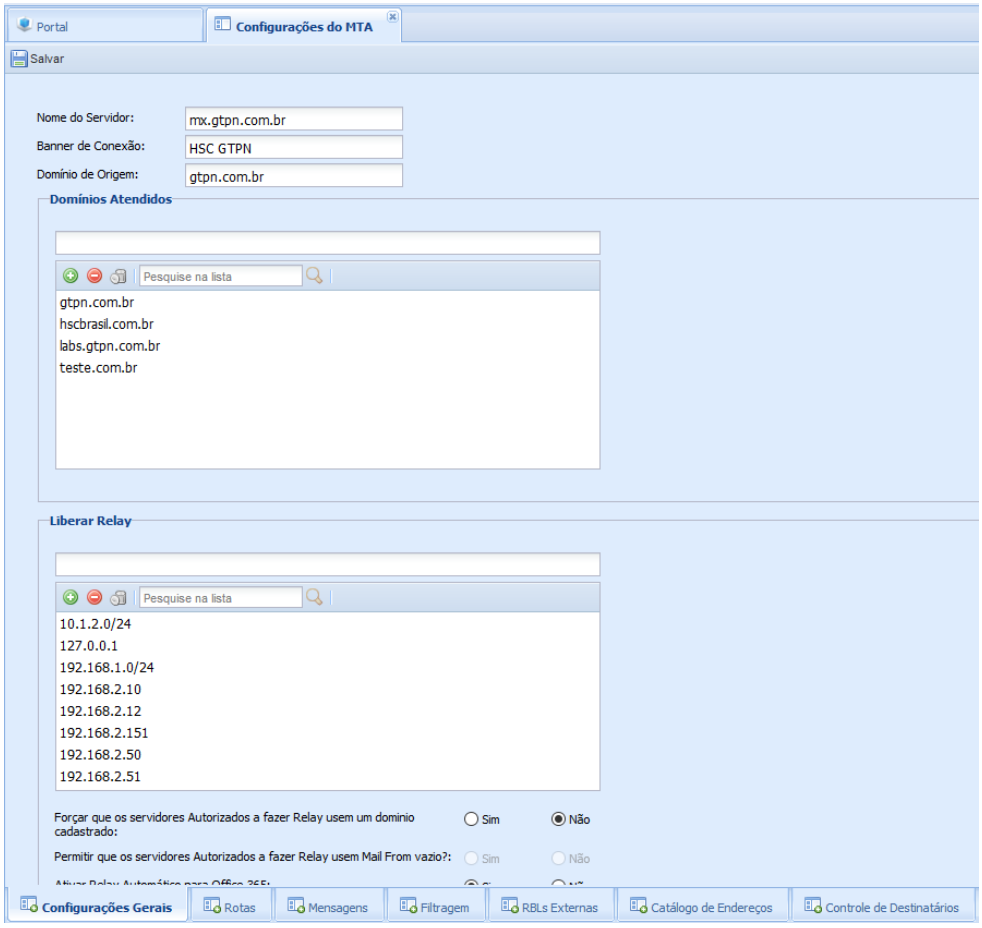
Analisar e/ou modificar regras e configurações

A interface administrativa do HSC MailInspector permite que sejam criadas e configuradas uma grande variedade de regras para a realização do controle de mensagens. Estas regras podem ser criadas através da atribuição de valores diretos digitáveis ou selecionáveis. Estes valores podem ser: usuários, grupos, e-mail, domínios de origem/destino, endereço DNS reverso, listas de distribuição, alias, endereço principal, IP, Rede, Hostname, sender HELO domain, endereço de e-mail de origem/destino, cabeçalho da mensagem, SMTP envelope SENDER, SMTP HELO SENDER, SMTP envelope RECIPIENT, valores de tempo (segundos, minutos, horas), valores de tamanho (bytes, kilobytes, megabytes, etc.), opções selecionáveis (sim, não, etc.). Todas as telas de configurações de todos as camadas de filtragens e funcionalidades de filtros seguem o padrão abaixo, ou seja, todos filtros podem ser configurados respeitando origens e destino "Entrada ou Saída" dependendo de como a regra for criada, permitindo um número ilimitado de regras de entrada ou saída.

O que é importante saber sobre as regras e configurações

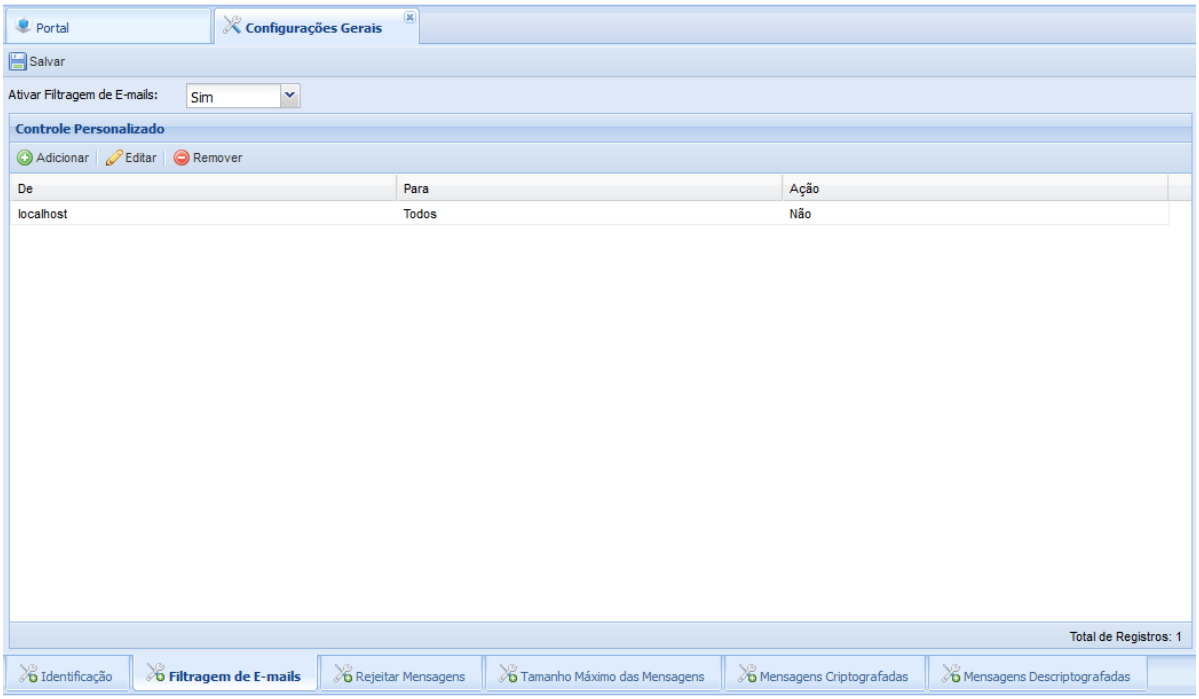
O entendimento das configurações e das composições do controle personalizado é muito importante para o correto funcionamento do produto. Em caso de dúvidas, contate o suporte da revenda, o fórum da HSC Brasil ou o canal de suporte da HSC Brasil.

- Muitas configurações devem ser atribuídas diretamente aos seus respectivos campos, como o exemplo abaixo.



Configurações por atribuição de valor

- Nas telas que permitem o controle através de regras personalizadas, que possuem o Controle Personalizado, primeiro define-se a regra padrão ou controle padrão da configuração, e depois, algum controle personalizado que seja necessário. No exemplo abaixo, a regra padrão Ativar Filtragem de E-mails está configurada como **SIM**, o que significa que todas as mensagens recebidas pelo HSC MailInspector serão processadas pelas camadas de filtragem. Logo abaixo é realizado um controle personalizado que nos diz "que todas as mensagens originadas ou recebidas **DE** origem MailInspector, destinadas a **PARA** qualquer destinatário (Todos) terão a **AÇÃO** Não", não serão processadas pelas camadas de filtragem. Desta forma podemos criar regras especificas por sentido de tráfego, ou seja, entrada ou saída de e-mails podendo personalizar por: usuários, grupos, e-mail, domínios, listas de distribuição, aliases, e-mail principal, expressão regulares, IP, Rede, Hostname, etc.



Configurações com regra padrão e controle personalizado

Aplicar Configuração

Para qualquer mudança nas configurações do MailInspector surtir efeito, é necessário que seja aplicada a configuração.

Ao fazer mudanças de configuração do MailInspector, as alterações são somente feitas no gerenciados, não sendo aplicadas aos pontos de filtragem (agentes). Essas alterações somente serão ativadas nos pontos de filtragem após seleção da opção **Aplicar Configurações**.

Você ainda pode selecionar individualmente quais configurações a serem aplicadas:

- AntiSPAM/Filtro de Conteúdo/Controle de Ameaças
- Block List/Allow List Personalizadas
- Controle de Conexão
- Data Loss Prevention

A área de Aplicar Configurações, todos os itens acessados são exibidos nesta área da tela.

Menu	Funções
AntiSPAM/Filtro de Conteúdo/Controle de Ameaças	Ativa ou desativa a opção de aplicar configurações em AntiSPAM/Filtro de Conteúdo/Controle de Ameaças
Block List/Allow List Personalizadas	Ativa ou desativa a opção de aplicar configurações em Block List/Allow List Personalizadas
Controle de Conexão	Ativa ou desativa a opção de aplicar configurações de Controle de Conexão
Data Loss Prevention	Ativa ou desativa a opção de aplicar configurações de Data Loss Prevention
Histórico	Apresenta todo o histórico de Aplicar Configurações
Aplicar	Aplica a Configuração

Trabalhando com expressões regulares

Uma expressão regular provê uma forma concisa e flexível de identificar cadeias de caracteres de interesse, como caracteres particulares, palavras ou padrões de caracteres.

Expressões regulares são escritas numa linguagem formal, específica para identificação desse tipo de "linguagem".

O HSC MailInspector realiza a análise desta linguagem, identificando as partes que casam com a especificação dada. No MailInspector, as expressões regulares são utilizadas como componente de identificação em regras tanto a nível de regras de spam, quanto a regras de compliance, entre outros.

Em termos de detecção da expressão regular no e-mail, pode-se verificar nos campos do corpo do e-mail, anexos (tanto no nome, quanto no conteúdo), campos do cabeçalho, até mesmo na identificação de extensões de arquivos ou domínios.

Caracteres aceitos na composição de expressão regular:

.	Combina com qualquer caractere único (utilize "\." para casar com ".").
[abc]	Combina com qualquer um dos caracteres informados ("[abc]" combina com "a" ou "b" ou "c").
[c-g]	Combina com qualquer um dos caracteres do intervalo ("[c-g]" combina com "c" ou "d" ou "e" ou "f" ou "g".
"[a-z0-9]"	Combina com qualquer letra ou dígito.
"[-/.:?]"	Combina com qualquer um dos caracteres informados "-" ou "/" ou "." ou ":" ou "?".).
?	Combina com nenhuma ou uma anterior ("palavras?" combina com "palavra" and "palavras".
"[abc]?"	Combina somente com "a" ou "b" ou "c" ou com nada (i.e. "")).
*	Combina com nenhuma ou mais formas anteriores ("palavras*" combina com "palavra", "palavras" e "palavrasssss", mas não caracteres especiais) Já a expressão ".*" combina com qualquer coisa, incluindo nada. Por exemplo: quero colocar em do SmartDefender a URL https://u8kv3.app.goo.gl e seus subdomínios. Então ficaria: https://u8kv3.app.goo.gl/* É errado considerar a seguinte expressão: https://u8kv3.app.goo.gl* Porque o RegEx não contemplaria o caracter / pois é caracter especial, então se tivesse uma URL https://u8kv3.app.goo.gl/teste, ele seria ignorado na expressão.
+	Combina com uma ou mais formas anteriores ("zzz+" combina com uma sequência de três ou mais "z").
(expr1|expr2)	Combina com uma expressão ou outra ("(doo|car)" combina com "doo" ou "car". "(doo|car)? Combina com "doo" ou "car" ou com nada (i.e. "")).
$	O fim de linha ("(doo|car)$" combina com "doo" ou "car" somente no final da linha).
\z	Desativa o significado especial de "z", onde "z" é um caractere especial da expressão regular ".?*+()^$[]{}\" ("\." combina com ".", "\\" combina com "\" etc.)

Exemplos de expressões regulares pearl que podem ser utilizadas nos grupos de usuários.

Combina com todos os usuários do domínio
/[\@\.]domínio\.com\.br$/

Combina com todos endereços governamentais
/\.gov.br$/

Combina com um bloco de endereços de rede
/^192\.168\.13[4567]\./

Maiores informações de como trabalhar com Expressões Regulares, acesse o APÊNDICE 3 deste Manual.

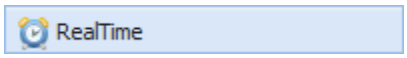
Menu - RealTime

E-mails

Na opção E-mail, permite ao administrador ou usuário com autorização para isso, visualizar e gerenciar os e-mails que foram processados pela caixa, isto é, os que passaram pela camada de conexão (MTA).

Permite ao administrador rastrear, liberar e-mail da quarentena, mover o e-mail de uma quarentena para outra (customizada), excluir e-mails, reprocessar e-mails, encaminhar e-mails, reportar* para HSCBRASIL e-mail como falso positivo ou falso negativo, reportar* para HSCBRASIL e-mail como malware/vírus, download somente dos anexos, download de toda mensagem, entre outras ações.

* Uma vez reportado o e-mail, ele será verificado pelo nosso sistema de Inteligência Artificial, para comprovação de Falso Positivo ou Falso Negativo, ou ainda como Vírus/Malware. Após analisado pela Inteligência Artificial, passa ainda por especialista que confirmará o caso. Também é gerado o report para o Administrador local para avaliação dele. Uma vez confirmado, será gerada devida assinatura dele.



/ **E-mails**

Visão geral dos e-mails

O item E-mails permite visualizar, filtrar, rastrear e aplicar ações de todas as mensagens processadas e/ou quarentenadas pelo HSC MailInspector (consolidando os dados processados pelos pontos de filtragem, através de uma única interface gráfica). Cada perfil administrativo (incluindo o perfil usuário) do produto possui acesso a um conjunto de ações pré-definidas e a níveis de visualização dos detalhes da mensagem. Desta forma é possível que o usuário final tenha acesso somente as suas mensagens, permitindo que o mesmo possa tomar ações como liberar uma mensagem que tenha sido classificada incorretamente como SPAM ou provável SPAM.

A interface web utilizada para visualização e gerenciamento é a mesma tanto para o administrador da solução, quanto para o usuário final. A capacidade de acesso a áreas de gerenciamento e liberação de ações possíveis, depende unicamente do permissionamento instaurado pelo administrador da solução.

Para visualizar as informações detalhadas da mensagem, dê um duplo clique sobre a mensagem desejada na listagem. Nesta tela é possível gerenciar todas as quarentenas, pesquisar e visualizar todos os e-mails que passaram pela ferramenta, identificando o motivo e a regra que ocasionou um possível bloqueio e sua classificação.

Use esta tela para fazer pesquisas e rastreio "Tracking" completo de todas as mensagens de forma online! Quando operando em cluster a tela permite visualizar de forma centralizada ou individual.

É possível visualizar todos os e-mails que foram processados pelo MailInspector nesse módulo, retornando as seguintes informações:

- Ponto de Acesso que filtrou o E-mail;
- País de Origem do E-mail;
- Data e Hora que o E-mail passou pelo MailInspector;
- Assunto do E-mail;
- De (Envelope);
- Para (Envelope);

- Tamanho do E-mail;
- Pontuação que ele atingiu no cálculo de SPAM;
- Se possui anexo;
- Sentido do Tráfego (E-mail oriundos de fora – externos / E-mail Oriundos de dentro – internos / E-mail Interno);
- Se o e-mail foi entregue ou não e o que houve com ele (se foi para quarentena ou se teve uma cópia retina da auditoria);
- Status (toda a classificação que o e-mail teve na análise dele), podendo ser:
    - Allow List;
    - Block List;
    - Arquivos Suspeitos;
    - ATP;
    - BulkMail;
    - CDR;
    - Conteúdo Bloqueado;
    - Criptografada;
    - Domínios Forjados com Free Mail;
    - E-mail Impostor;
    - E-mail Marketing;
    - E-mails Suspeitos;
    - Free Mail;
    - Liberados;
    - Limpa/Auditoria;
    - Malware;
    - Outro Bloqueio;
    - Phishing;
    - Provável SPAM;
    - Redes Sociais;
    - Regras de Compliance;
    - Regras de Controle Avançado;
    - Spam;
    - Spoofing de Domínio;
    - Tamanho Excedido;
    - Vírus;
- ID do E-mail no MailInspector;
- Se tiver sido quarentenado, para qual quarentena ele foi;
- IP de Origem do E-mail;
- De (Header);
- Para (Header);
- Dados de Anexos contidos no E-mail (Mime-Type, Nome dos anexos, se tiver anexo compactado, quais arquivos estão compactados, tamanho de cada anexo);
- Assinaturas que pontuaram o E-mail, com descrição de cada uma delas e a pontuação que cada uma delas atribui ao E-mail;
- Caso tenha alguma ameaça, qual e ameaça encontrada, em qual nível de detecção que foi registrado a ameaça (se foi o anti-vírus, se foi o SandBox da HSCBRASIL ou se foi o SmartDefender Local);
- Indicação de todos os saltos que o E-mail sofreu, com os hostnames dos servidores envolvidos, bem como os IPs de origem e destino e quanto tempo demorou para cada salto executado entre os hops;
- Cabeçalho do E-mail com os dados tabulados;
- E-mail com o conteúdo original no formato texto;
- E-mail com o conteúdo original no formato HTML;

- Anexos contido no E-mail, com indicativo dos nomes dos anexos, tipo (extensão), Mime-Type dos anexos, Tamanho dos Anexos, HASH do anexo, Status da Filtragem do Anexo (se tem código malicioso ou link malicioso no anexo), opção de download do anexo;
- Se tiver casado com alguma regra previamente criada de Data Loss Prevention, indicação da regra que casou com o DLP, bem como palavra e dicionário RegEx envolvido na análise;
- Se tiver casado com a regra de Content Disarm and Reconstrution (CDR), indicação do que foi ativado no módulo CDR em relação aos anexos envolvidos;
- Categorização de todos os domínios, links e anexos que o E-mail tiver, bem como análise pelo SandBox para verificação de comportamento e código malicioso;
- Log de tudo que foi analisado e efetuado no E-mail, desde o momento da sua chegada no MailInspector, até a última ação tomada;
- Histórico de quem e quando acessou ou efetuou alguma ação sobre o E-mail;
- Performance do sistema para a análise do E-mail, com indicativo de tempo de processamento em cada um dos módulos que o E-mail passou;
- Possibilidade de download da mensagem completa;
- Possibilidade de download do cabeçalho original do E-mail;

Definições de Opções - E-mails

Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição
Ponto de Acesso	Quando o sistema estiver configurado para funcionamento em CLUSTER, é possível selecionar por qual ponto de acesso "Servidor" a mensagem passou. Se usar a opção "Todos" listará todos os registros do cluster, de forma centralizada, independentemente do servidor que processou a mensagem.
Pesquisar	Quando clicado, aplica o filtro informado na caixa de pesquisa rápida as mensagens.
Limpar	Quando clicado, remove os filtros informados da caixa de pesquisa rápida e da janela de pesquisa avançada, e recarrega todos os registros de e-mails.
Pesquisa Avançada	Realiza uma pesquisa mais detalhada nos registros. Permitindo um rastreio completo e preciso de uma mensagem, tanto no assunto, corpo do e-mail, bem como nos anexos, assinaturas acionadas, nome de malware ou até mesmo em campos customizados do cabeçalho do e-mail. Quando clicado, abre a caixa de diálogo **Pesquisa Avançada**. Todas as pesquisas podem ser concatenadas e combinadas com os operadores booleanos tais como: AND, OR, NOT, NEAR, OCCUR, (,), [,], etc.
Exportar	Gera um relatório no formato CSV, PDF ou HTML da pesquisa que foi efetuada.
Quarentena	Permite selecionar uma determinada área de Quarentena Customizada ou não, para visualização. Para visualizar uma determinada quarentena é preciso que o usuário logado tenha permissão de acesso. É possível utilizar a combinação de QUARENTENA com Pesquisa Avançada, ou seja, selecionar uma determinada quarentena, e depois selecionar Pesquisa Avançada para aplicar outro filtro, tais como: • Períodos (data inicial e data final); • E-mail de origem (por header do e-mail); • E-mail de origem (por envelope do e-mail); • Domínio de Destino;

	• Domínio de Origem; • E-mail de Destino; • Entre outras várias características (veja *Definições de Opções - Pesquisa Avançada*) As quarentenas disponíveis para filtragem são: • ATP; • Block List; • Bulk Mail; • Conteúdo Adulto; • Conteúdo Bloqueado; • ADP/Auditoria; • Fraude de E-mail/E-mail Impostor; • Outro Bloqueio; • Malware; • Phishing; • Provável SPAM; • SPAM; • Spoofing; • Tamanho Excedido; • Vírus; • Allow List; Também são apresentadas as quarentenas customizadas criadas pelo administrador do sistema.
Ações	Escolha entre: • **Analisar com HSC AI Cyber Assistant** – Faz a análise do e-mail através de inteligência artificial, analisando todos os pontos do e-mail e dando parecer do motivo do bloqueio. O sistema de inteligência artificial, verifica os seguintes pontos do e-mail: ○ Conteúdo; ○ URL's; ○ Cabeçalhos (segue abaixo alguns pontos do cabeçalho analisado pela IA): ▪ Remetente e resposta (return path/reply-to); ▪ SCL/PCL: Spam Confidence Level; ▪ Violações de protocolos de segurança: • SPF; • DKIM; • DMARC; ○ Sentimento: Indicação de urgência, participação de pesquisa, bloqueio de conta, etc. ○ Veredito: Indicação do motivo do bloqueio de forma simples e fácil entendimento, dessa forma o próprio usuário poderá entender o motivo do bloqueio, sem necessidade de que seja um especialista no assunto de segurança de e-mails. • **Reenviar Mensagem** - Permite reenviar/liberar da quarentena a mensagem selecionada para o mesmo destinatário. ⚠ A mensagem deve estar armazenada na quarentena para realizar esta ação. • **Mover Mensagem-** Permite mover uma determinada mensagem para outra área de quarentena**.** • **Reprocessar Mensagem** - Força que a mensagem seja novamente analisada pelos filtros de conteúdo, antispam, antivírus, etc. A mensagem é toda reprocessada, recalculando a pontuação de SPAM, nova verificação de ameaças de anexos e links, bem como gerando as notificações necessárias (caso tenha alguma notificação a ser efetuada), movimentação para a quarentena referida a ela (a quarentena pode ser em outra pasta,

dependendo da nova classificação da mensagem) entre outras ações baseadas no reprocessamento da mensagem.

- **Marcar como Confiável** - Permite adicionar o domínio, e-mail ou IP do remetente da mensagem selecionada a allow list (lista de confiáveis) de um usuário. É aberto um Wizard para facilitar a criação da regra de allow list, compondo Origem e Destino do E-mail:
  - **DE (Origem):**
    - Confiável por E-mail de Origem (Header);
    - Confiável por E-mail de Origem (Envelope);
    - Confiável por Domínio/Subdomínio de Origem;
    - Confiável por IP de Origem;
  - **PARA (Destino):**
    - Confiável para E-mail de Destino;
    - Confiável para Domínio/Subdomínio de Destino;
    - Confiável para Todos os destinatários da empresa;
- **Marcar como Indesejável** - Permite adicionar o domínio, e-mail ou IP do remetente da mensagem selecionada a block list (lista de bloqueados) de um usuário. É aberto um Wizard para facilitar a criação da regra de block list, compondo Origem e Destino do E-mail:
  - **DE (Origem):**
    - Confiável por E-mail de Origem (Header);
    - Confiável por E-mail de Origem (Envelope);
    - Confiável por Domínio/Subdomínio de Origem;
    - Confiável por IP de Origem;
  - **PARA (Destino):**
    - Confiável para E-mail de Destino;
    - Confiável para Domínio/Subdomínio de Destino;
    - Confiável para Todos os destinatários da empresa;
- **Encaminhar Mensagem** - Permite reenviar a mensagem selecionada para outro destinatário de e-mail, sem que o remetente e destinatário receba qualquer aviso de encaminhamento.

A mensagem deve estar armazenada na quarentena para realizar esta ação.

- **Extrair/Importar senhas para catálogo de senhas** – Verifica todo o conteúdo do e-mail em busca de possíveis senhas e faz o cadastro automático dos mesmos no *Banco de Senhas*.
- **Adicionar ao Grupo** - Permite que seja adicionado a um Grupo de Usuários as informações contidas nesta mensagem, tais como:
  - IP;
  - Remetente;
  - Domínio do Remetente e
  - Endereços dos Destinatários.
- **Reportar* para HSC** – Envia o e-mail para a HSC reportando como:
  - SPAM;
  - Não SPAM;
  - Vírus;
  - Phishing.

* Uma vez reportado o e-mail, ele será verificado pelo nosso sistema de Inteligência Artificial, para comprovação de Falso Positivo ou Falso Negativo, ou ainda como

Vírus/Malware. Após analisado pela Inteligência Artificial, passa ainda por especialista que confirmará o caso. Uma vez confirmado, será gerada devida assinatura dele.

- **M-SOAR** – Se estiver usando Microsoft Office 365, é possível efetuar ações sobre os e-mails entregues, com o módulo M-SOAR/Deep Integration. A ação é executada diretamente sobre a caixa de e-mail do usuário. As ações possíveis sobre os e-mails que foram entregues são:
    - Remover Anexos da Mensagem – Remove qualquer anexo contido na mensagem, com opção de deixar aviso no e-mail de anexo removido;
    - Remover links da mensagem – Remove links contido na mensagem, com opção de deixar aviso no lugar do link de URL removida;
    - Mover para o Lixo Eletrônico – Envia a mensagem para o lixo eletrônico;
    - Bloquear Conteúdo – Bloqueia o conteúdo da mensagem, com permissão de incluir um aviso no lugar do conteúdo;
    - Apagar a mensagem – Exclui a mensagem entregue;
- **G-SOAR** – Se estiver usando G-Suite, é possível efetuar ações sobre os e-mails entregues, com o módulo G-SOAR/Deep Integration. A ação é executada diretamente sobre a caixa de e-mail do usuário. As ações possíveis sobre os e-mails que foram entregues são:
    - Remover Anexos da Mensagem – Remove qualquer anexo contido na mensagem, com opção de deixar aviso no e-mail de anexo removido;
    - Remover links da mensagem – Remove links contido na mensagem, com opção de deixar aviso no lugar do link de URL removida;
    - Mover para o Lixo Eletrônico – Envia a mensagem para o lixo eletrônico;
    - Bloquear Conteúdo – Bloqueia o conteúdo da mensagem, com permissão de incluir um aviso no lugar do conteúdo;
    - Apagar a mensagem – Exclui a mensagem entregue;
- **Z-SOAR** – Se estiver usando Zimbra, é possível efetuar ações sobre os e-mails entregues, com o módulo Z-SOAR/Deep Integration. A ação é executada diretamente sobre a caixa de e-mail do usuário. As ações possíveis sobre os e-mails que foram entregues são:
    - Remover Anexos da Mensagem – Remove qualquer anexo contido na mensagem, com opção de deixar aviso no e-mail de anexo removido;
    - Remover links da mensagem – Remove links contido na mensagem, com opção de deixar aviso no lugar do link de URL removida;
    - Mover para o Lixo Eletrônico – Envia a mensagem para o lixo eletrônico;
    - Bloquear Conteúdo – Bloqueia o conteúdo da mensagem, com permissão de incluir um aviso no lugar do conteúdo;
    - Apagar a mensagem – Exclui a mensagem entregue;
- **Remover da Quarentena** - Permite remover uma mensagem que esteja armazenada na quarentena.

A mensagem deve estar armazenada na quarentena para realizar esta ação.

- **Aprender como SPAM** - Permite ensinar ao Machine Learning e ao filtro bayesiano que um determinado tipo de mensagem deve ser considerado como SPAM. Essa aprendizagem é limitada a solução local, isto é, não é enviado nenhuma amostra para HSCBRASIL, para criação de assinatura global.

A mensagem deve estar armazenada na quarentena para realizar esta ação.

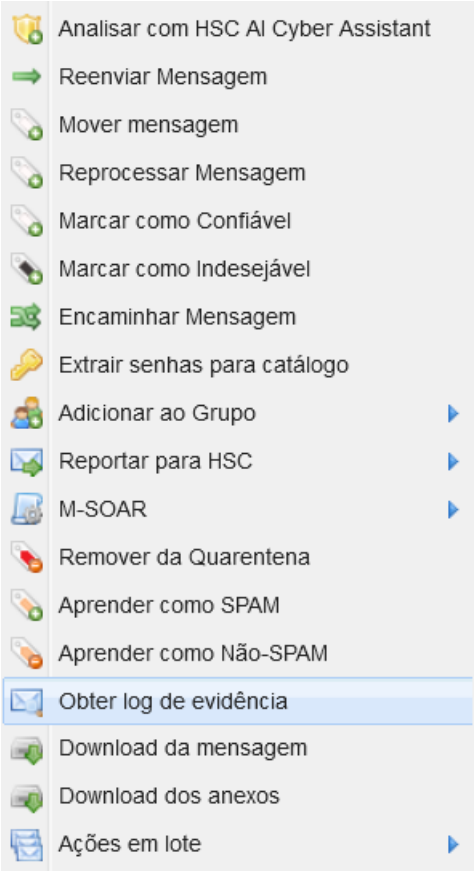
- **Aprender como NÃO SPAM** - Permite ensinar ao Machine Learning e ao filtro bayesiano que um determinado tipo de mensagem deve ser considerado como não sendo SPAM. Essa aprendizagem é limitada a solução local, isto é, não é enviado nenhuma amostra para HSCBRASIL, para criação de assinatura global.

A mensagem deve estar armazenada na quarentena para realizar esta ação.

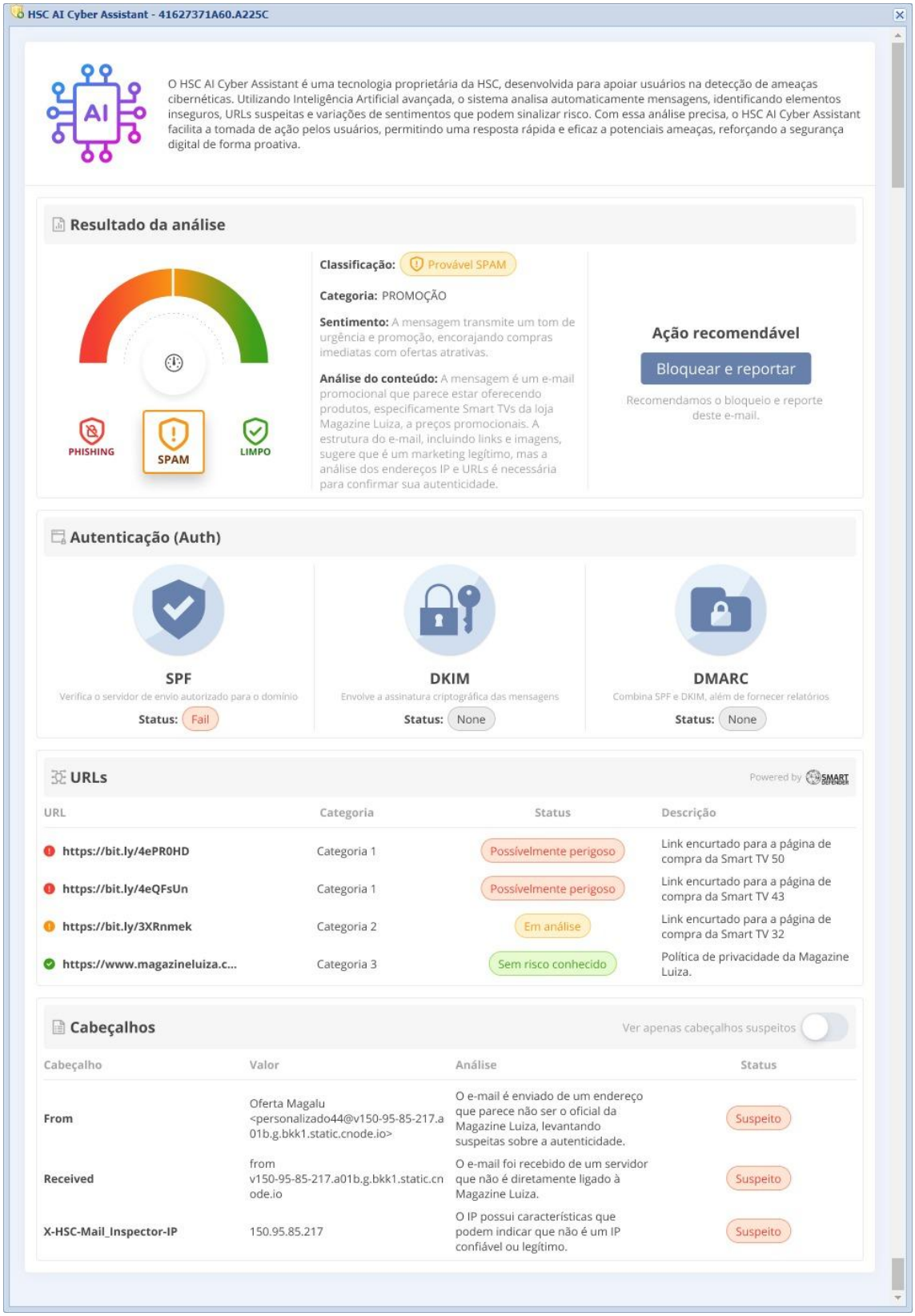
- **Obter Log de Evidências** - Permite ao administrador obter informações precisas dos Logs de filtragem do MailInspector sobre o rastreio completo da Mensagem incluindo as informações de: recebimento, processamento, ações tomadas e entrega/bloqueio da mensagem. É possível efetuar download do log de evidência como arquivo TXT.
- **Download da mensagem** – Permite o download da mensagem em formato .EML/.MSG.
- **Download dos anexos** – Permite o download de eventuais anexos que o e-mail venha a possuir.
- **Ações em Lote** – Permite efetuar ações sobre lotes de mensagens, filtrados através da Pesquisa Avançada. As ações são sobre todos os e-mails filtrados, dessa forma mesmo que uma pesquisa retorne múltiplas páginas de e-mails, a ação definida afetará TODAS esses e-mails previamente filtrados. As ações possíveis são:
    - **M-SOAR:** Todas as ações do módulo M-SOAR
        - Remover Anexos da Mensagem – Remove qualquer anexo contido na mensagem, com opção de deixar aviso no e-mail de anexo removido;
        - Remover links da mensagem – Remove links contido na mensagem, com opção de deixar aviso no lugar do link de URL removida;
        - Mover para o Lixo Eletrônico – Envia a mensagem para o lixo eletrônico;
        - Bloquear Conteúdo – Bloqueia o conteúdo da mensagem, com permissão de incluir um aviso no lugar do conteúdo;
        - Apagar a mensagem – Exclui a mensagem entregue;
    - **G-SOAR:** Todas as ações do módulo G-SOAR
        - Remover Anexos da Mensagem – Remove qualquer anexo contido na mensagem, com opção de deixar aviso no e-mail de anexo removido;
        - Remover links da mensagem – Remove links contido na mensagem, com opção de deixar aviso no lugar do link de URL removida;
        - Mover para o Lixo Eletrônico – Envia a mensagem para o lixo eletrônico;
        - Bloquear Conteúdo – Bloqueia o conteúdo da mensagem, com permissão de incluir um aviso no lugar do conteúdo;
        - Apagar a mensagem – Exclui a mensagem entregue;
    - **Z-SOAR:** Todas as ações do módulo Z-SOAR
        - Remover Anexos da Mensagem – Remove qualquer anexo contido na mensagem, com opção de deixar aviso no e-mail de anexo removido;

	▪ Remover links da mensagem – Remove links contido na mensagem, com opção de deixar aviso no lugar do link de URL removida; ▪ Mover para o Lixo Eletrônico – Envia a mensagem para o lixo eletrônico; ▪ Bloquear Conteúdo – Bloqueia o conteúdo da mensagem, com permissão de incluir um aviso no lugar do conteúdo; ▪ Apagar a mensagem – Exclui a mensagem entregue; ○ **Reenviar Mensagem:** Reenvia todas as mensagens filtradas. ○ **Reprocessar Mensagem:** Reprocessa todas as mensagens filtradas. ○ **Encaminhar Mensagem:** Encaminha todas as mensagens filtradas. ○ **Liberar Todas Mensagens:** Libera todas as mensagens filtradas.

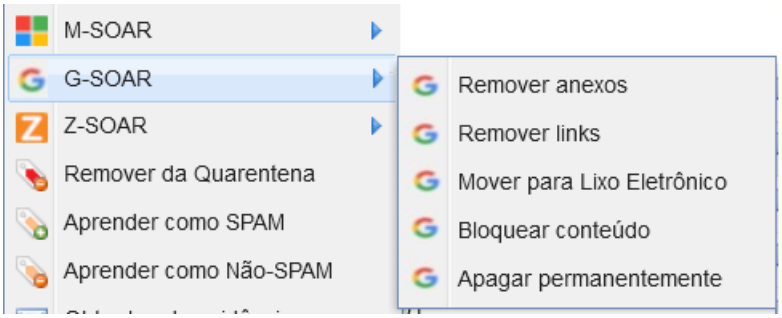
Dica: As opções de Ação, também são liberadas ao clicar com o botão direito do mouse sobre a mensagem.



Ações disponíveis para o administrador



HSC AI Cyber Assistant



Tela indicativa das ações presentes no M-SOAR integrado ao G-Suite

Definições de Opções - Pesquisa Avançada

O **HSC MailInspector** disponibiliza um mecanismo de **pesquisa e filtragem avançada de mensagens**, permitindo ao administrador localizar e analisar e-mails a partir de praticamente qualquer informação associada à mensagem, seus metadados, conteúdo ou resultado do processamento pelos mecanismos de segurança.

A pesquisa pode ser realizada, entre outros critérios, por **remetente, destinatário, assunto, conteúdo do corpo da mensagem, URLs, sentido do tráfego, status de entrega, assinaturas, ameaças identificadas, regras personalizadas de SPAM e DLP**, além de diversos outros atributos relacionados ao processamento do e-mail.

Os critérios de pesquisa podem ser **combinados e correlacionados**, permitindo a criação de consultas específicas para diferentes necessidades operacionais, de segurança, auditoria e investigação. Por exemplo, o administrador pode pesquisar somente **mensagens de entrada encaminhadas para quarentena**, ou **mensagens de saída que contenham determinada palavra no assunto**, entre inúmeras outras combinações.

Também é possível segmentar a pesquisa de acordo com o **sentido do tráfego**, permitindo consultar separadamente mensagens de **entrada, saída ou ambos os sentidos**, proporcionando maior granularidade na análise do fluxo de correio eletrônico.

O MailInspector permite combinar múltiplos campos em uma mesma pesquisa, incluindo:

- E-mail de origem, considerando informações do **Header e Envelope**;
- E-mail de destino, considerando informações do **Header e Envelope**;
- Assunto da mensagem;
- Palavras-chave presentes no corpo da mensagem;
- URLs contidas na mensagem;
- Nome dos arquivos anexados;
- Nome da ameaça identificada;
- Tamanho da mensagem;
- Status de entrega;
- Regra de SPAM aplicada;
- Regra de DLP aplicada;
- Cabeçalhos customizados;
- Hostname;
- Pontuação atribuída pelos mecanismos de análise;
- Data e hora inicial e final (período a ser pesquisado);
- Status de classificação da mensagem;
- Sentido do tráfego;

- Status de quarentena;
- Entre outros campos e atributos disponíveis no sistema.

Os diferentes critérios podem ser combinados por meio de **operadores lógicos E/OU (AND/OR)**, permitindo construir consultas simples ou altamente específicas para investigação de incidentes, auditoria, troubleshooting e análise operacional.

Integração com Archiving

A funcionalidade de **Pesquisa Avançada** também contempla as mensagens armazenadas pelo módulo de **Archiving**, permitindo realizar consultas sobre as mensagens arquivadas juntamente com as mensagens processadas pelo sistema.

Dessa forma, o administrador pode realizar uma **pesquisa centralizada**, obtendo em uma única consulta os resultados relacionados tanto às mensagens processadas quanto àquelas armazenadas no ambiente de arquivamento, sem a necessidade de realizar pesquisas separadas.

Templates e pesquisas personalizadas

O MailInspector permite ainda a utilização de **templates de pesquisa e filtros predefinidos**, disponibilizados pela **HSCBRASIL**, facilitando a execução de consultas recorrentes e de uso comum pelos administradores.

Além dos templates preestabelecidos, o sistema possibilita a criação de **pesquisas e filtros personalizados**, permitindo que a organização adapte os critérios de consulta às suas necessidades específicas e às suas políticas de segurança, auditoria e operação.

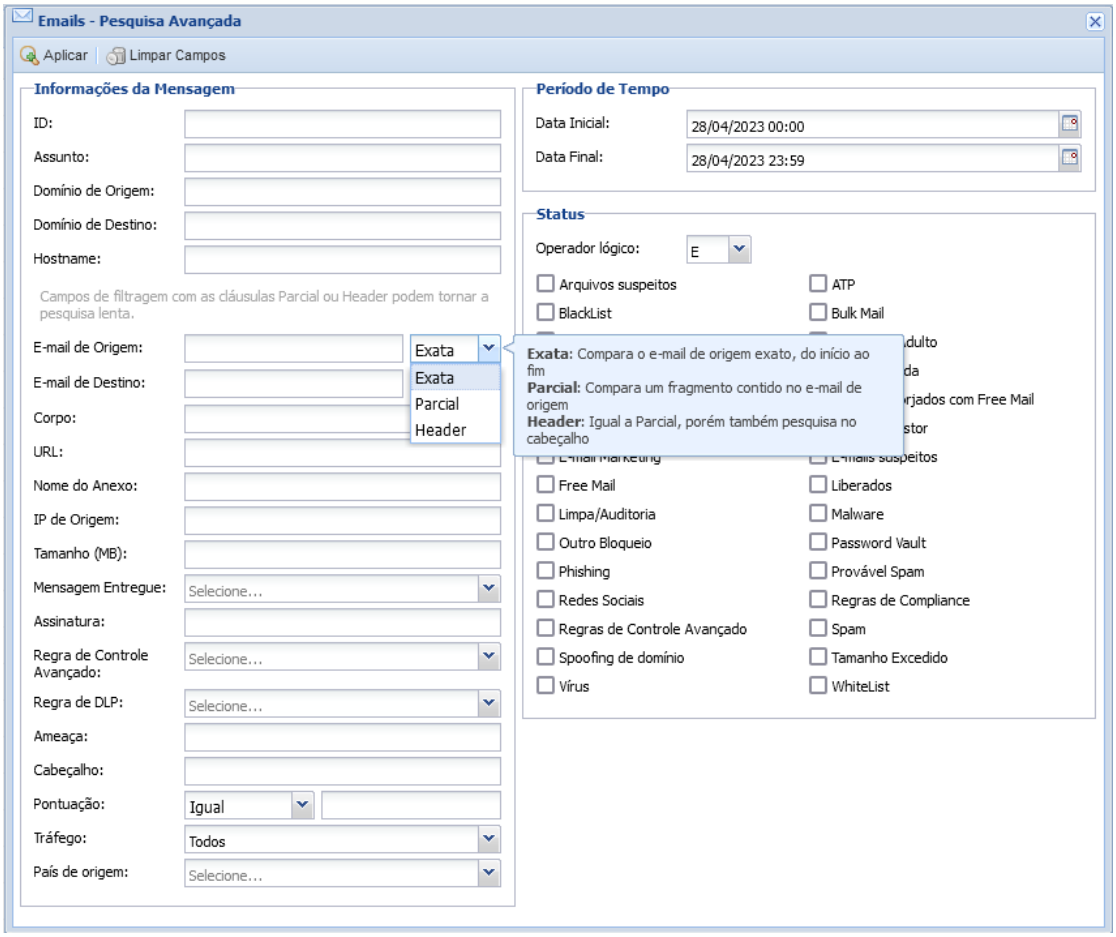
Essa flexibilidade proporciona ao administrador uma ferramenta abrangente para **localizar, filtrar, correlacionar e investigar mensagens de forma rápida e precisa**, independentemente do sentido do tráfego ou da etapa do processamento em que a mensagem se encontra.

Opções	Definição
Aplicar	Quando clicado, aplica os filtros informados e/ou selecionados as mensagens filtradas pelo HSC MailInspector.
Limpar Campos	Quando clicado, remove os valores informados ou selecionados pelo usuário.
ID	Informe o código de identificação completo da mensagem.
Assunto	Informe o assunto completo ou parcial da mensagem.
Domínio de Origem	Informe o domínio de origem do e-mail.
Domínio Destino	Informe o domínio de destino do e-mail.
E-mail de Origem	• **Exata:** Fará a busca pelo e-mail exato inserido, efetuando a busca pelo FROM do Envelope do E-mail. • **Parcial:** Fará busca pelo e-mail parcial inserido. É efetuada a busca pelo FROM do Envelope do E-mail. • **Header:** Efetuará a busca pelo FROM do Header (em vez de efetuar a busca pelo FROM do Envelope) do E-mail. A busca usando o Header pode ser pelo e-mail ou pelo Display Name ou até mesmo e-mail parcial ou Display Name parcial.
E-mail de Destino	• **Exata:** Fará a busca pelo e-mail exato inserido, efetuando a busca pelo TO do Envelope do E-mail.

	• **Parcial:** Fará busca pelo e-mail parcial inserido. É efetuada a busca pelo TO do Envelope do E-mail. • **Header:** Efetuará a busca pelo FROM do Header (em vez de efetuar a busca pelo TO do Envelope) do E-mail. A busca usando o Header pode ser pelo e-mail ou pelo Display Name ou até mesmo e-mail parcial ou Display Name parcial.
Corpo	Informe um valor que possa estar presente no corpo da mensagem, inclusive URL's, links, etc.
Nome do Anexo	Permite pesquisar por um nome do anexo. Permite nome completo ou parcial do anexo na pesquisa
IP de Origem	Permite a busca de e-mails pelo IP de Origem do e-mail.
Tamanho (MB)	Informe um tamanho em megabytes para mensagem.
Mensagem Entregue	Escolha entre: • **Todos** - Filtra por mensagens que foram e não foram entregues ao destinatário. • **Somente Sim** - Filtra por mensagens que foram entregues ao destinatário. • **Somente Não** - Filtra por mensagens que não foram entregues ao destinatário.
Assinatura	Pesquisa por uma determinada regra de SPAM/Assinatura.
Regra de Controle Avançado	Pesquisa por uma regra de Controle Avançado criado pelo Administrador.
Regra de DLP	Pesquisa por uma regra de DLP criado pelo Administrador.
Ameaça	Pesquisa por nome da ameaça.
Cabeçalho	Pesquisa por um campo específico apresentado no cabeçalho do e-mail.
Pontuação	Filtra mensagens por pontuação de SPAM indicada pelo administrador, podendo ser: • Maior; • Maior igual; • Igual; • Menor Igual; • Menor;
Tráfego	Pelo sentido do tráfego do e-mail, podendo ser: **Todos:** Tanto e-mails de entrada, quanto de saída ou mesmo e-mails de circulação interna. **Entrada:** Somente e-mails de entrada (defora para dentro). **Saída:** Somente e-mails de saída (de dentro para fora). **Interno:** E-mails considerados internos, isto é, e-mails de domínio protegido pelo MailInspector para ele mesmo, por exemplo usuário1 manda e-mail para usuário2, sendo que ambos estão usando o mesmo servidor de e-mail.
País de Origem	País de Origem do e-mail.
Data Inicial/Hora Inicial	Permite definir uma data/hora inicial para pesquisa.
Data Final/Hora Final	Permite definir uma data/hora final para pesquisa.
Operador Logico	Permite definir se os campos selecionados em "Status" irão ser "E" ou "OU" na hora de efetuar a pesquisa.

Status	Escolha entre: • **Arquivos Suspeitos** - É a mesma lógica dos E-mails Suspeitos, mas aplicada a anexos, por exemplo: anexo .txt com trechos, ao qual pede alguma senha. • **ATP** - Permite pesquisar por e-mails que foram classificados como ATP (links que foram reescritos que levava a páginas contaminadas ou anexos com código malicioso detectado através de análise comportamental no SandBox). • **BlockList** - Filtra por mensagens que foram processadas e estavam cadastradas na blocklist. • **BulkMail** - Permite pesquisar por e-mail que foram classificados como BulkMail (através de reputação). • **CDR** - E-mails que foram ativadas regras de CDR (Content Disarm and Reconstruction). • **Conteúdo Adulto** - Permite pesquisar por e-mail que foram classificados como Conteúdo Adulto. • **Conteúdo Bloqueado** - Filtra por mensagens processadas que foram classificadas como contendo arquivos anexos com o mime-type ou extensões proibidas. • **Criptografada -** Permite pesquisar por e-mails que foram categorizados como Criptografia. • **Domínios Diferentes no Cabeçalho** – Permite filtrar/pesquisar e-mails que foram detectados com o domínio no campo From do Cabeçalho diferente do domínio do campo From apresentado para o usuário final (From do Body). • **Domínios Forjados com Free Mail** – Permite pesquisar/filtrar por e-mail que foram classificados como forjados e que usaram e-mails gratuitos para essa disseminação. • **Domínios Recentes/Suspeitos** - Permite pesquisar por e-mails que foram classificados como Domínios Recentes ou suspeitos (domínios similares aos domínios cadastrados para uso no appliance). • **E-mail Impostor** - Permite pesquisar por e-mails que soferam aguma falha de protocolo de segurança, tais como DMARC, DKIM, SPF. • **E-mail Marketing** - Permite pesquisar e-mails classificados como campanha de marketing (detectados por análise do e-mail). • **E-mails Suspeitos** - E-mail suspeito são assinatura para identificar possíveis conteúdos textuais perigosos ou maliciosos, por exemplo e-mails que pedem senha. • **Free Mail -** Permite filtrar/pesquisar e-mails enviados de servidores que oferecem serviços de e-mails gratuitos. • **Liberados -** E-mails que foram liberados ou pelo administrador ou pelo usuário. • **Limpa/Auditoria**- Filtra por mensagens processadas que foram classificadas como limpas e as que estão marcadas para cair em auditoria. • **Malware** - Permite pesquisar por e-mails que foram classificados como Malware. • **Outro Bloqueio** - Filtra por mensagens processadas quer foram classificadas em qualquer outro tipo de bloqueio (ex: arquivos compactados com senha). • **Password Vault -** E-mails ativados pelo Banco de Senha. • **Phishing** - Permite pesquisar por e-mails que foram categorizados como Phishing.

	• **Provável SPAM** - Filtra por mensagens processadas que foram classificadas como proveniente de provável fonte de SPAM ou ameaças. • **Redes Sociais -** Permite pesquisar mensagens que estão relacionadas e foram filtradas como Redes Sociais (E-mails oriundos do Twitter, Facebook, Instagram, Snapchat, etc). • **Regras de Compliance** - Permite filtra mensagens que foram ativadas por alguma regra do DLP ou Quarentena Customizada. • **Regras de Controle Avançado** - Detectado uso de regras de customizadas pelo administrador do sistema. • **Spam** - Filtra por mensagens processadas que foram classificadas como proveniente de fonte confirmada de SPAM ou ameaças. • **Spoofing de Domínio** - Permite pesquisar por e-mail que foram classificados como Spoofing de Domínio, isto é, e-mails externos que usam domínios cadastrados na solução. • **Tamanho Excedido** - Filtra por mensagens processadas quer foram classificadas como tendo o tamanho maior que o permitido (configurado pelo administrador da solução). • **Vírus** - Filtra por mensagens processadas que foram classificadas como contendo vírus ou que tenham fontes para vírus ou outras ameaças. • **Allow List** - Filtra por mensagens que foram processadas e estavam cadastradas na allow list. • **Controle de Surto** - Permite pesquisar por e-mails que foram classificados como Controle de Surto (excesso de e-mails de uma única fonte classificados como SPAM / excesso de e-mails de uma única fonte classificados com MALWARES / excesso de e-mails de uma única fonte com destinatários inexistentes).



Tela de pesquisa avançada

Dica: Para melhorar o desempenho da busca, sempre que possível, componha a busca usando o domínio de origem e/ou domínio de destino, junto com outros campos da busca.

Definições de Opções - Visualização dos E-mails

A tela principal mostra em tempo real as mensagens que entram e saem de sua corporação. É possível visualizar os e-mails que passaram pelo sistema de proteção a E-mail, bem como o motivo de sua quarentena ou liberação.

As informações apresentadas na tela são:

- País: Indicação visual da bandeira de país de origem;
- Ponto de acesso: Ponto de filtragem do e-mail;
- Data/Hora: Data e hora de recebimento do e-mail;
- Assunto: Título do e-mail;
- De: Remetente;
- Para: Destinatário(s);
- Tamanho: Tamanho do e-mail;

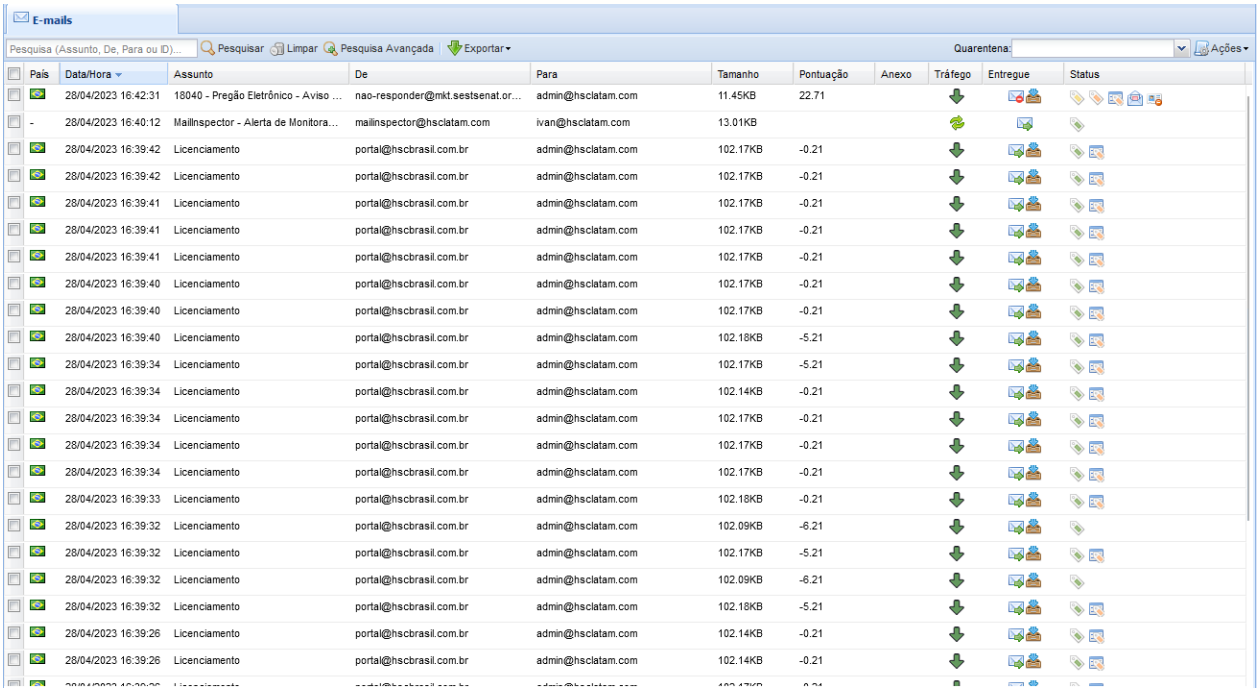
- Pontuação: Quanto recebeu de pontuação a nível de SPAM;
- Anexo: Se o e-mail possui anexo;
- Tráfego: Sentido do e-mail;
- Entregue:
  - E-mail entregue
  - E-mail não entregue
  - E-mail armazenado em pasta de quarentena (podendo ser até mesmo quarentena de auditoria)
- Status: Como foi classificado o e-mail / identificador da regra de bloqueio;

A coluna Status, indica as classificações que o e-mail atingiu (um único e-mail, pode ter múltiplos status, pois ele pode atingir várias classificações), por exemplo: E-mail classificado como PROVÁVEL SPAM, SPAM, BULK MAIL.

Os status podem ser:

STATUS	DESCRIÇÃO
ANEXO BLOQUEADO	Tipo de anexo foi bloqueado pelo administrador do MailInspector.
ARQUIVOS SUSPEITOS	Arquivos com características maliciosas.
ATP	Indica que o e-mail origina de redes que efetuaram ataques persistentes.
BLOCK LIST	E-mail bloqueado por estar registrado em block list no MailInspector.
BULK MAIL	Originam de IP's já cadastrados como Bulk Mail (devido a reputação dos IP's de origem).
CDR	Anexo ativou o módulo de CDR, ao qual efetuou a análise de código em anexos do tipo Office e efetuou a remoção do código.
CONTEÚDO ADULTO	Detectado conteúdo adulto na mensagem.
CONTEÚDO BLOQUEADO	Mensagens processadas que foram classificadas como contendo arquivos anexos com o mime-type ou extensões proibidas.
CRIPTOGRAFIA	E-mail criptografado pelo MailInspector.
DLP	O e-mail infringiu alguma regra de Data Loss Prevention (regra criada pelo administrador da solução).
DOMÍNIOS DIFERENTES NO CABEÇALHO	Detectados diferenças de domínio no From do Envelope e From do Header do e-mail.
DOMÍNIOS FORJADOS COM FREE-MAIL	E-mail enviado de sistemas gratuitos de e-mail (tais como gmail, yahoo, Hotmail, etc) e que sofreu Spoofing.
DOMÍNIOS RECENTES/SUSPEITOS	Domínios recentemente adquirido (tempo para ser considerado domínio novo, é indicado pelo administrador da solução).
E-MAIL IMPOSTOR	Detectados características de e-mail impostor/BEC (Business E-mail compromise).
E-MAIL MARKETING	E-mails classificados como campanha de marketing (detectados por análise do e-mail – heurística, análise contextual e outros parâmetros).
E-MAILS SUSPEITOS	E-mail com conteúdo suspeito, oriundo de IP registrado em listas como IP atacante.
FREE-MAIL	E-mail enviado de servidores gratuitos de e-mail (tais como Gmail, Yahoo, Hotmail, etc).
LIBERADOS	E-mails que foram para a quarentena e liberados pelo administrador ou usuário.
LIMPA/AUDITORIA	E-mail válido e/ou e-mail armazenado para auditoria.

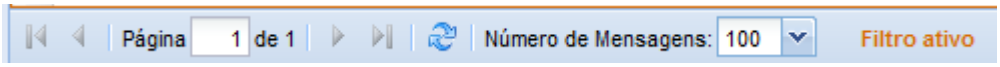
MALWARE	Ameaça encontrada em anexo (Detectado pelo SandBox ou SmartDefender Local).
OUTRO BLOQUEIO	Bloqueio de anexo que não se encaixa nos outros tipos de bloqueio, tais como: • Anexo criptografado com senha; • Anexo compactado com executável inserido; • Entre outras condições;
PASSWORD VAULT	Coletado palavras chaves possíveis de uso em arquivos compactados com senha.
PHISHING	Encontrado no e-mail ameaça do tipo phishing.
PROVÁVEL SPAM	O E-mail atingiu a pontuação para ser considerado como PROVÁVEL SPAM, ou seja, o sistema de análise do e-mail, efetuou análise contextual e heurística, bem como considerado uma série de outros fatores (tais como reputação do emissor, linguagem utilizada, etc) tomando por base todas as características do e-mail e o mesmo foi considerado PROVÁVEL SPAM.
REDES SOCIAIS	E-mails oriundos de redes sociais.
REGRAS DE COMPLIANCE	Casou com uma regra criada pelo administrador no módulo de E-mail Compliance (DLP, Criptografia ou Quarentena Customizada).
REGRAS DE CONTROLE AVANÇADO	Casou com uma regra criada pelo administrador no módulo SPAM > Controle Avançado.
SPAM	O E-mail atingiu a pontuação para ser considerado como SPAM, ou seja, o sistema de análise do e-mail, efetuou análise contextual e heurística, bem como considerado uma série de outros fatores (tais como reputação do emissor, linguagem utilizada, etc) tomando por base todas as características do e-mail e o mesmo foi considerado SPAM.
SPOOFING DE DOMÍNIO	Houve mudança no remetente de e-mail (no domínio), tentando se passar por outra empresa.
TAMANHO EXCEDIDO	Ultrapassou o tamanho máximo permitido (configurado pelo administrador) a nível de processamento do e-mail.
VÍRUS	Ameaça encontrada em anexo (Detectado pelo antivírus ESET).
ALLOW LIST	E-mail contido em allow list.

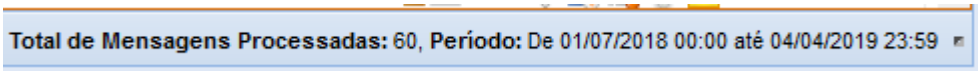


Tela de E-mails processados pelo MailInspector (RealTime > E-mails)

Também é possível verificar na barra inferior as seguintes informações:

- Paginação da tela dos e-mails;
- Configuração de número de mensagens por página;
- Se o filtro de e-mails está ativo ou inativo;
- Total de mensagens filtradas (se estiver com o filtro ativo) ou mensagens processadas no dia (se estiver com o filtro de e-mails inativo);
- Período de pesquisa;



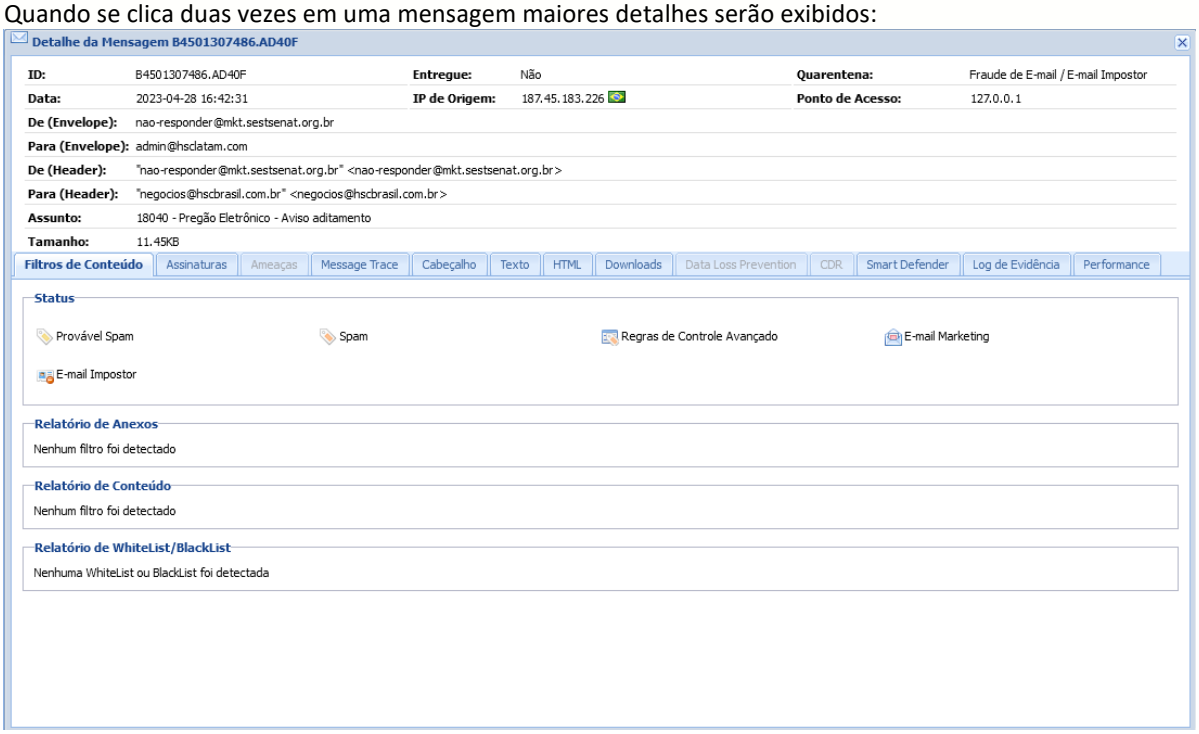


Dica: É possível efetuar um filtro específico e verificar quantas mensagens atingiram a classificação desejada.

Por exemplo, quero saber quantas mensagens foram consideradas SPAM **E** com anexos contaminados entre 01/01/2019 a 01/02/2019, basta criar o filtro em Pesquisa Avançada e verificar os resultados.

Definições de Opções - Detalhe da Mensagem

Quando se clica duas vezes em uma mensagem maiores detalhes serão exibidos:



Maiores detalhes do e-mail selecionado

Estas informações descrevem os campos apresentados ao administrador, ao dar duplo clique sobre o e-mail.

Opções	Definição
Detalhes	Exibe informações gerais da mensagem: • **ID:** Número de identificação (ID da Mensagem); • **Entregue:** Se a mensagem foi entregue ao destino ou não; • **Quarentena:** Indica se o e-mail está em quarentena e em qual quarentena foi classificado e armazenado; • **Hostname:** Nome do servidor de origem do e-mail; • **IP de Origem:** IP da Origem do E-mail, incluindo a bandeira do país de origem do e-mail; • **IP do Ponto:** Qual ponto de filtragem que o e-mail foi processado; • **Data:** Data e hora de processamento; • **De (Envelope):** Remetente Envelope SMTP; • **Para (Envelope):** Destinatário Envelope SMTP; • **De (Header):** Remetente Header SMTP; • **Para (Header):** Destinatário Header SMTP; • **Assunto:** Título/Assunto do E-mail; • **Tamanho:** Tamanho do E-mail;

	ID: 5F0429B5ABF.A9CA8 · Entregue: Sim · Quarentena: SPAM Hostname: mx-balancer.micloud.com · IP de Origem: 187.108.197.233 · Ponto de Acesso do Cluster: mail.gtpn.com.br Data: 2021-07-19 17:02:30 De (Envelope): fatura1626724705@suporteclaro.com Para (Envelope): contato@gtpn.com.br De (Header): Minha CLARO <fatura1626724705@suporteclaro.com> Para (Header): romulo@hscbrasil.com.br Assunto: Fatura Claro em atraso. Tamanho: 172.10KB *Exemplo de detalhes do e-mail*
Status	Exibe informações sobre o processamento e classificação da mensagem. Permite visualizar o relatório do conteúdo de anexo (mesmo possuindo arquivos anexos compactados, apresentando o seu Mime-Type) e indicação de qual whitelist ou block list que ele faz parte (caso o e-mail esteja em allow list ou block list da solução) e os status de classificação, podendo ser: • LIMPA • ALLOW LIST • BLOCK LIST • PROVÁVEL SPAM • SPAM • PHISHING • AMEAÇA • CONTEÚDO BLOQUEADO • ANEXO BLOQUEADO • TAMANHO EXCEDIDO • OUTRO BLOQUEIO • DLP • E-MAIL IMPOSTOR • DOMÍNIOS RECENTES/SUSPEITOS • MALWARE • BULK MAIL • MAIL MARKETING • ATP • SPOOFING DE DOMÍNIO • REGRAS DE CONTROLE AVANÇADO • REGRAS DE COMPLIANCE • CRIPTOGRAFIA • DOMÍNIOS FORJADOS COM FREE-MAIL • FREE-MAIL • DOMÍNIOS DIFERENTES NO CABEÇALHO Status: Provável Spam · Spam · Domínios Recentes / Suspeitos · Bulk Mail *Exemplo de status do e-mail*
Relatório de Anexos	Indica todos os arquivos anexos contidos no e-mail. Relatório de Anexos anexo.html Mimetype: text/plain *Exemplo de indicação de anexos contido no e-mail*
Relatório de Conteúdo	Lista todos os anexos, bem como os arquivos contidos dentro de anexos compactados, indicando seus verdadeiros conteúdos, através de Mime-Types do(s) anexo(s).

	Relatório de Conteúdo (anexo.html) **MimeType:** text/plain *Exemplo de Relatório de Conteúdo do e-mail*
Relatório de Alow List/Block List	Indica se o e-mail está contido em allow list ou block list pessoal e caso esteja, indica qual a regra de allow list ou block list que o filtrou. **Relatório de WhiteList/BlackList** Global Rule Whitelist: From .* To \b.*@interop.com.br\b. Field Check: From Header. *Exemplo de detalhes de allow list/block list do e-mail*
Assinaturas	Nesta Aba é possível visualizar quais Regras de SPAM foram ativadas, cuja pontuação final da mensagem é a somatória das pontuações das regras assinaturas de SPAM. As assinaturas também abrangem pontuação atribuída pelo sistema de Machine Learning, dessa forma você poderá verificar a pontuação recebida pelo e-mail pela assinatura de Bayes. O MailInspector permite ao administrador criar regras customizadas para ignorar e/ou alterar a pontuação das regras de SPAM. Em Pontuação da Mensagem, indica a somatória da pontuação das regras de SPAM e ao lado indica qual o valor mínimo necessário para que o e-mail seja considerado PROVÁVEL SPAM e com isso o bloqueio do mesmo. **Pontuação da Mensagem:** 18.43 (requerido6) **BAYES_99 (Bayes spam probability is 99 to 100%):** 5.00 **DKIM_ADSP_ALL (No valid author signature, domain signs all mail):** 0.80 **DKIM_INVALID:** 0.10 **DKIM_SIGNED (Message has a DKIM or DK signature, not necessarily valid):** -0.30 **HSC_BR_SPAMMER_URI (Texto suspeito):** 1.00 **HSC_MAIL_REPUTATION (Listado Sistema de Reputacao de E-mails HSC SmartDefender):** 4.90 **HSC_SPAM_CUSTOM_RULE_50 (Origem MLI Nuvem):** 0.20 **HSC_SPAM_CUSTOM_RULE_53 ((MLI Nuvem) E (DKIM Invalido)):** 1.00 **HSC_SUSPICIOUS_NEW_DOMAINS (Detect recently registered domains):** 1.00 **HTML_MESSAGE (HTML included in message):** 0.00 **MIME_HTML_ONLY (Message only has text/html MIME parts):** 0.72 **SPF_SOFTFAIL (SPF: sender does not match SPF record (softfail)):** 1.00 **T_DKIM_INVALID:** 3.00 **URIBL_BLOCKED:** 0.00 É possível criar regra específica para ignorar uma ou mais regras que foram avaliadas para pontuação de SPAM. Vá em Configurações > E-mail Compliance > Regras Também são apresentadas as assinaturas de SPAM Customizadas (caso o e-mail tenha sido acionado com alguma assinatura customizada de pontuação).

	Nessa mesma aba apresenta a assinatura de ameaça detectada e/ou análise heurística da ameaça. *Detecção de ameaça por assinatura*
Ameaças	Nesta aba podemos visualizar o relatório de análise de ameaças dos Engines padrão utilizados pelo MailInspector (por default, são executados simultaneamente, mas com administrador tem a opção de configurar e/ou desativar o antivírus secundário – ESET): • ESET; • HSC SmartDefender. Essa aba indica a classificação do malware conforme a detecção do respectivo fabricante, chegando a apresentar o resultado da análise local da caixa. É possível visualizar os resultados de análise dos malwares detectados, mesmo sendo Zero Day, operando nos diferentes sistemas operacionais (Windows, Linux, MacOS e Android) pela análise de SandBox. *Detecção de ameaça pelo antivírus ESET* *Detecção de ameaça pelo HSC SmartDefender*
Message Trace	Monta todos os "saltos" utilizados no percurso do e-mail, dessa forma é possível mensurar o tempo de entrega do e-mail e análise de tempo em cada servidor que o e-mail passou, além de indicação de entrega ou não do e-mail ao servidor destino. Também é possível efetuar análise forense, para verificação de possível ponto de vazamento de informação (caso tenha sido coletada em um dos pontos de salto). Esse recurso apresenta os seguintes dados: • **Date/Time:** Data e hora do registro de entrada do e-mail no node; • **From:** De onde veio o e-mail, apresentando o IP e/ou hostname de origem; • **To:** Destino do salto do e-mail (próximo node), apresentando o IP e/ou hostname de destino;

- **Layer:** Camada de onde foi coletada a informação (geralmente é do cabeçalho/HEADER);
- **Detail:** Outros detalhes;
- **Delay:** Tempo de passagem de um node para outro. Importante lembrar que geralmente o último ponto de node é o MailInspector.
  Com esse componente é possível determinar quanto tempo o e-mail ficou "parado" em fila de processamento, uma vez que por padrão, quando o e-mail cai em esteira de processamento, ele já é processado e enviado, então se o tempo de delay é muito alto, isso indica que o e-mail ficou "parado" em fila aguardando ser processador para entrega;
- **Total:** Tempo total de circulação do e-mail, desde a origem até o último registro de tempo no MailInspector;

Filtros de Conteúdo | Assinaturas | Ameaças | **Message Trace** | Cabeçalho | Texto | HTML | Downloads | Data Loss Prevention | CDR | Smart Defender | Log de Evidência | Performance

Created: 20/07/2021 14:30:36

Date/Time	From		To	Layer	Detalis	Delay
20/07/2021 14:30:36	webmail.hscbrasil.com.br (webmail.hscbrasil.com.br[207.180.249.48])	→	webmail.hscbrasil.com.br (Postfix)	HEADER	-	0s
20/07/2021 14:30:36	webmail.hscbrasil.com.br ([127.0.0.1])	→	localhost (webmail.hscbrasil.com.br[127.0.0.1])	HEADER	-	0s
20/07/2021 14:30:36	localhost (localhost.localdomain[127.0.0.1])	→	webmail.hscbrasil.com.br (Postfix)	HEADER	-	0s
20/07/2021 14:30:35	webmail.hscbrasil.com.br (vmi288705.contaboserver.net[207.180.249.48])	→	mx.gtpn.com.br (Postfix)	HEADER	using TLSv1.2 with cipher AECDH-AES256-SHA (256/256 bits)	0s
					Total	0

Indicação de quantidade de saltos entre servidores e o tempo que ocupou cada um deles

Importante salientar, que quando ocorre a entrega do e-mail, no Message Trace, é apresentado o indicador **SENT** e logo em seguida o ID da entrega do e-mail (fornecido pelo SERVIDOR DESTINO – com indicação do IP do SERVIDOR DESTINO). Segue exemplo na tela a seguir:

Filtros de Conteúdo | Assinaturas | Ameaças | **Message Trace** | Cabeçalho | Texto | HTML | Downloads | Data Loss Prevention | CDR | Smart Defender | Log de Evidência | Histórico

Created (Header Date): 23/10/2023 01:30:19
Received: 23/10/2023 01:30:19

Date/Time	From		To	Layer	Detalis	Delay
23/10/2023 01:30:19	-	→	hsclatam.com (Postfix,fromuserid0)	HEADER	-	0s
23/10/2023 01:30:23	MailInspector	→	127.0.0.1[127.0.0.1]:10028 roberto.chu@hscbrasil.com.br	SMTP	sent- (250 2.0.0 Ok: queued as 50257307483)	4s
23/10/2023 01:30:25	MailInspector	→	mx01.mlicloud.com[187.45.183.226]:25 roberto.chu@hscbrasil.com.br	SMTP	sent- (250 2.0.0 Ok: queued as C256B2C7606)	2s
					Total	6s

Cabeçalho

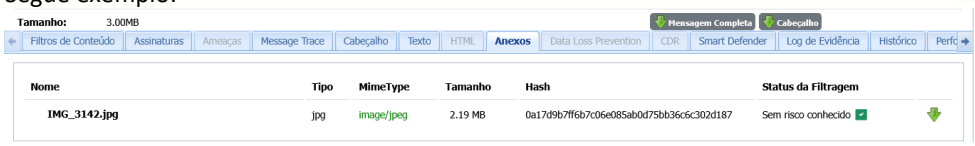
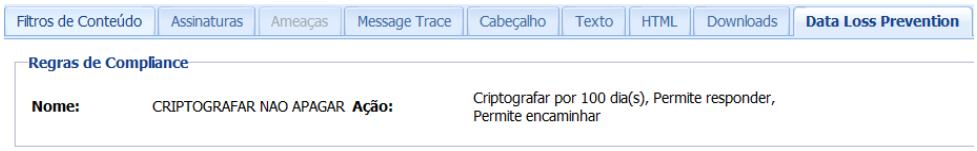
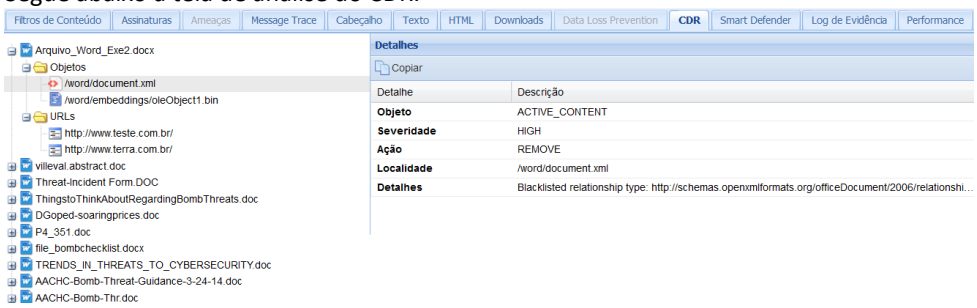
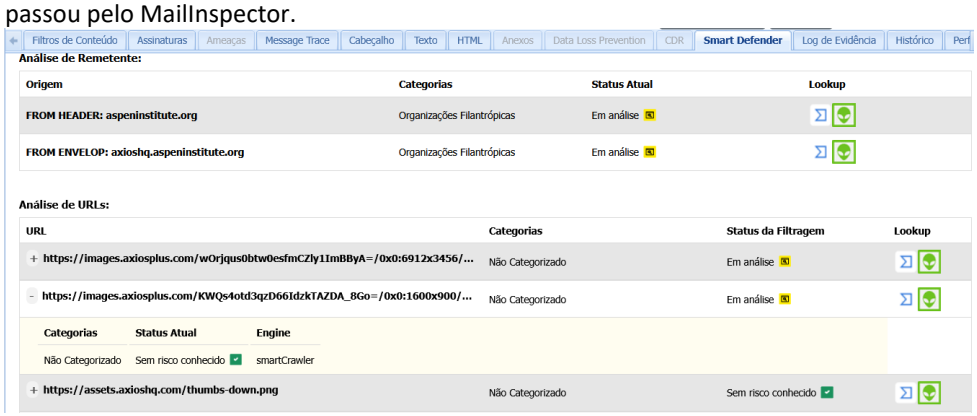
Visualiza o código fonte do cabeçalho da mensagem.
Exemplo de Cabeçalho de e-mail:

Cabeçalho	Conteúdo
Received	from mx-balancer.mlicloud.com (mx02.mlicloud.com [187.108.197.232]) by mx.gtpn.com.br (Postfix) with ESMTPS id 39E40190408 for <contato@gtpn.com.br>; Wed, 20 Feb 2019 03:21:55 -0300 (-03)
Received-SPF	Pass (mailfrom) identity=mailfrom; client-ip=54.37.183.123; helo=cmail37-m20.futurofacts.com.br; envelope-from=return-administrativo=hscbrasil.com.br@futurofacts.com.br; receiver=<UNKNOWN>
Received	from cmail37-m20.futurofacts.com.br (cmail37-m20.futurofacts.com.br [54.37.183.123]) by mx-balancer.mlicloud.com (Postfix) with ESMTPS id C6FA725848F for <administrativo@hscbrasil.com.br>; Wed, 20 Feb 2019 03:21:34 -0300 (-03)
DKIM-Signature	v=1; a=rsa-sha1; c=relaxed/relaxed; s=default; d=futurofacts.com.br; h=To:Subject:Message-ID:Date:From:Reply-To:MIME-Version:List-Unsubscribe: List-ID:Content-Type:Content-Transfer-Encoding; i=emm@futurofacts.com.br; bh=xWu2QzsZBppMZ4RvTq29zb57awA=; b=SCbMrdXxujth4+0tGMkFK2PqWlPFCgGcboGFg++N88pBEDmy8ri2C1aR3/TddAJ/jbvn+s8tHY7C I3ElNwrTOzS+Ebi76h+WDmlarenOXxq6/stTV/19xRODu4TJVrXa7i4T5YeVjLH2xHHA3n54+wnN FJf2BLuSpL1cqnTdFKzp1aznnhZQcUma/sU6v4WLn+MNtU0+Y0oGpDNfCx1MVmG8BBfDz5Yf6Wli ye3SuZMkeCQK7Ulrf4m+yAbEMMJTwIOmWGcsJZbxkMfScoKgT0VXWn6dfBvl6Sm4RthzptHMu4tY F6INW7u1AXoAa6pJmmrSCwL/1ncGKx4BCHJJ1w==

DomainKey-Signature	a=rsa-sha1; c=nofws; q=dns; s=default; d=futurofacts.com.br; b=C5FNdFzyli7HGXprmHzdmggkDn3TZ5sFFMXFxgD/713mbTf0u567/tvDhpB4aAsZVu+DibgMcwf8m21IQQ7q8yRkD5WNOptt+HHtCSQq+VB0ZOqU9c0tktDlkCPO1B84Qiac5f6ybCXnFQjrebwjLYCUXe9Y7dYQyOiRM9XMtiP6p248wOgOCVJsB0BED7Qqr2Yf4FX9P/mivMVsgNOxafNoalzPfNDQ682zHspydY0ffkqZa1EyRC92vrAOFhf9utU5XEqs6Nm0K7DYjKn0o6TvZQnRU+cTKtJ9OfnM06UeQNVqeFKgRimH7hQ0TZNYgvc+ZE7tAld2NDtRCsTw==;
To	administrativo@hscbrasil.com.br
Subject	Heey quer ser surpreendido? Roupas para curtir no carnaval 2019
Message-ID	<3548898632dcbb89789bf8ed7ce63cf3@www.futurofacts.com.br>
Date	Wed, 20 Feb 2019 03:20:19 -0300
Cabeçalho	**Conteúdo**
From	"Zattini Informa" <emm@futurofacts.com.br>
Reply-To	emm@futurofacts.com.br
MIME-Version	1.0
X-Mailer-LID	15,14,13,12
List-Unsubscribe	<http://www.futurofacts.com.br/iem/unsubscribe.php?M=1221187&C=4c2e668795c4c31d4cdded9632d2ddf3&L=12&N=454>, <mailto:unsubscribe@redacaonet.com.br?subject=Unsubscribe>
List-ID	Redacao Net list <redacaonet.list-id>
Abuse-Reports-To	abuse@redacaonet.com.br.com.br
X-Feedback-ID	sdssdf:rthrthrh:sdsf342:bubka
X-Complaints-To	abuse@redacaonet.com.br.com.br
X-Mailer-RecptId	1221187
X-Mailer-SID	454
X-Mailer-Sent-By	1
Content-Type	text/html; charset="UTF-8"
Content-Transfer-Encoding	8bit
X-HSC-Mail_Inspector-From	return-administrativo=hscbrasil.com.br@futurofacts.com.br
X-HSC-Mail_Inspector-IP	54.37.183.123
X-HSC-Mail_Inspector-Point	2
X-HSC-Mail_Inspector-ID	C6FA725848F.A5E26
X-HSC-Brasil-HSC_MailInspector	Mensagem OK
X-HSC-Brasil-HSC_MailInspector-SpamCheck	SPAM, HSC MailInspector (not cached, Pontuacao=20.503, requerido 6, autolearn=spam, BAYES_99 5.00, BAYES_999 0.20, DKIM_SIGNED -0.01, DKIM_VALID -0.20, DKIM_VALID_AU -0.10, HELO_DYNAMIC_DHCP 0.21, HSC_BR_SPAMMER_URI 1.00, HSC_MAIL_REPUTATION 4.90, HSC_RULE_URI_0132 1.00, HSC_URL_REDIRECT 0.80, HSC_URL_REDIRECTS 1.00, HSC_URL_REDIRECT_RECURSE 0.80, HSC_URL_REDIRECT_TOSAME 0.60, HTML_MESSAGE 0.00, MIME_HTML_ONLY 0.72, PYZOR_CHECK 3.70, RDNS_DYNAMIC 0.98, SPF_PASS -0.10, URIBL_BLOCKED 0.00)
X-HSC-Brasil-HSC_MailInspector-SpamScore	20
X-HSC-Brasil-HSC_MailInspector-From	return-administrativo=hscbrasil.com.br@futurofacts.com.br

Indicação do cabeçalho do e-mail

Texto	Exibe o corpo da mensagem original como texto plano.
HTML	Exibe o corpo da mensagem original como HTML.
Anexos	Exibe todos os anexos da mensagem e permite o download deles ou até mesmo da mensagem completa. É possível efetuar o download do anexo da mensagem em quarentena e encaminhar ao fabricante do antivírus ou outra empresa/engine de análise para verificação mais profunda. • **Mensagem Completa:** Baixa o e-mail completo, no formato .eml; • **Cabeçalho:** Download somente do cabeçalho do e-mail; • **Nome:** Nome do arquivo em anexo; • **Tipo:** Tipo do arquivo em anexo (extensão); • **MimeType:** Formato original do arquivo; • **Tamanho:** Tamanho total do anexo; • **HASH:** HASH do anexo utilizando a chave SHA-1; • Status da Filtragem: Se foi detectado como malicioso; • Download do anexo;

	Segue exemplo:  *Exemplo de download disponível no detalhe da mensagem*
Data Loss Prevention	Exibe quais regras de DLP casaram com a mensagem selecionada, reportando os detalhes da regra e as ações que foram tomadas.  *Exemplo de indicação de regra aplicada de DLP no e-mail*
CDR	Exibe quais regras de CDR que se casaram com a mensagem selecionada, reportando os detalhes da regra e as ações que foram tomadas, bem como conteúdo de programas e/ou links contidos em documentos do tipo Office. Por padrão o módulo CDR desarma o código/link e entrega o anexo sem esse conteúdo. Segue abaixo a tela de análise do CDR.  *Exemplo de indicação de CDR aplicado sobre documentos do tipo Office*
SmartDefender	Exibe e consulta o Status atual de todas URLs e Arquivos presente nos e-mail na nuvem da HSC SmartDefender, bem como das URL's analisadas no momento em que o e-mail passou pelo MailInspector.  *Exemplo de indicação de status e classificação das URLs, bem como dos anexos* No retorno do SmartDefender indica os seguintes campos: **Análise do Remetente:** Verifica o domínio de origem, tanto do FROM do ENVELOPE, quanto do FROM do HREADER, indicando: • **Origem:** ORIGEM do FROM; • **Categoria:** Categorização classificada do domínio;

- **Status Atual:** Status na hora da análise;
- **LookUp:** Permite o envio da URL diretamente ao VirusTotal e/ou AlienVault para análise de terceiros e comparar com o resultado obtido pelo SmartDefender;

Análise de URL's: Verifica todas as URLs encontradas no e-mail, indicando a categorização, status da filtragem.

- **URL:** Indicação da URL analisada;
- **Categoria:** Qual categoria a URL foi classificada;
- **Status da Filtragem:** Limpa, Em análise ou Ameaça
  Ao clicar sobre a URL ou anexo, será expandido o resultado indicando o Status ATUAL do Elemento.
- **Status Atual:** Indica o Status Atual do Objeto, dessa forma, é possível comparar o status atual, com o status no momento que o e-mail passou pelo MailInspector.

Botão Lookup	Ação
	Envia o objeto para AlienVault para análise
	Envia o objeto para VirusTotal para análise

Obs: É possível enviar somente o HASH dos objetos para a análise.

Log de Evidência

O **HSC MailInspector** disponibiliza o **rastreio completo das mensagens em formato de log textual**, permitindo ao administrador acompanhar, de forma detalhada, todo o ciclo de processamento do e-mail, desde o seu recebimento até a entrega, bloqueio ou encaminhamento para quarentena.

O log registra as principais etapas e eventos relacionados ao processamento da mensagem, incluindo:

- Recebimento e entrega da mensagem;
- Atividade e resultados dos mecanismos de filtragem;
- Escaneamento pelo antivírus;
- Análise antispam;
- Verificação de URLs;
- Aplicação de **Allowlist** e **Blocklist**;
- Análise de arquivos anexados;
- Pontuação atribuída à mensagem pelos mecanismos de filtragem;
- Decisão final de processamento e filtragem;
- Erros e ocorrências durante o processamento;
- Identificação do **nó (node) responsável pelo processamento e filtragem**;
- Demais informações relevantes relacionadas ao processamento da mensagem.

O **log de evidências** permite ao administrador determinar, de maneira objetiva e auditável, o destino efetivo de cada mensagem processada. É possível verificar se o e-mail **prosseguiu no fluxo e foi efetivamente entregue ao servidor de correio eletrônico de destino**, incluindo informações como o **endereço IP do servidor destinatário e a porta TCP utilizada na entrega**.

Da mesma forma, quando uma mensagem não é entregue, o administrador pode identificar **em qual etapa e por qual mecanismo a mensagem foi bloqueada**, bem como consultar a respectiva pasta ou área de retenção. Nos casos em que a mensagem é encaminhada para **quarentena**, o sistema apresenta essa informação juntamente com o

motivo do bloqueio ou retenção, permitindo a análise detalhada da decisão tomada pelo sistema.

Essa capacidade de rastreabilidade proporciona **visibilidade completa sobre o ciclo de vida da mensagem**, facilitando auditorias, troubleshooting, investigação de incidentes, validação das políticas de segurança e comprovação do processamento e destino efetivo dos e-mails.

A seguir, apresenta-se um exemplo de **log de evidências** gerado pelo sistema:

```
Oct 31 09:49:56 mx02 MTA/smtpd[17431]: E63CE258130:
client=smtp500.bradesco.com.br[200.155.87.225]
Oct 31 09:49:56 mx02 MTA/cleanup[10550]: E63CE258130: hold:
header Received: from smtp500.bradesco.com.br
(smtp500.bradesco.com.br [200.155.87.225])??by mx-
balancer.mlicloud.com (MTA) with ESMTPS id E63CE258130??for
<suzana@xxxx.com.br>; Thu, 31 Oct 2019 09:49 from
smtp500.bradesco.com.br[200.155.87.225];
from=<alessandror.xxxx@bradesco.com.br>
to=<suzana@xxxx.com.br> proto=ESMTP
helo=<smtp500.bradesco.com.br>
Oct 31 09:49:56 mx02 MTA/cleanup[10550]: E63CE258130:
message-id=<6D50B8DF87870048BD5B8FF57DF67E6D69772A0E@MZ-FW-
EX-436.corpr.bradesco.com.br>
Oct 31 09:55:02 mx02 HSC MailInspector[6051]: <A> tag found
in message E63CE258130.AA100 from
alessandror.xxxx@bradesco.com.br
Oct 31 09:55:02 mx02 HSC MailInspector[6051]: HTML Img tag
found in message E63CE258130.AA100 from
alessandror.xxxx@bradesco.com.br
Oct 31 09:55:11 mx02 HSC MailInspector[6051]: Encrypt
Message :
/opt/hsc/mailinspector/quarantine/20191031/msg/E63CE258130.A
A100
Oct 31 09:55:12 mx02 HSC MailInspector[6051]: Requeue:
E63CE258130.AA100 to 954E025811B
Oct 31 09:55:12 mx02 MTA/qmgr[4616]: 954E025811B:
from=<alessandror.xxxx@bradesco.com.br>, size=980924,
nrcpt=1 (queue active)
Oct 31 09:55:12 mx02 HSC MailInspector[6051]: SYSLOG OUTPUT:
{"from_domain":"bradesco.com.br","isrblspam":null,"issaspam"
:0,"sascore":-1.416,"date":"2019-10-
31","time":"09:55:12","hostname":"mx02.mlicloud.com","namein
fected":0,"quarantined":1,"otherinfected":0,"size":"981963",
"to":"suzana@xxxx.com.br","to_domain":"xxxx.com.br","deliver
ed":1,"archiveplaces":"","timestamp":"2019-10-31
09:55:12","from":"alessandror.xxxx@bradesco.com.br","id":"E6
3CE258130.AA100","virusinfected":"0","clientip":"200.155.87.
225","hsc_attach":{"image006.png":{"size":"1398","type":"PNG
image
data"},"":{"size":"15126"},"image011.png":{"size":"17143","t
ype":"PNG image
data"},"image013.png":{"size":"17146","type":"PNG image
data"},"image008.png":{"size":"17117","type":"PNG image
data"},"image004.png":{"size":"202368","type":"PNG image
```

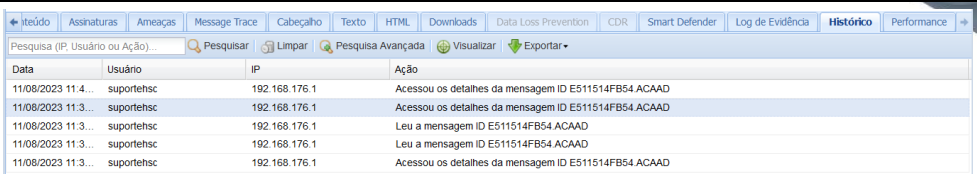
data"},"image009.png":{"size":"17118","type":"PNG image
data"},"image014.png":{"size":"17135","type":"PNG image
data"},"image001.png":{"size":"7227","type":"PNG image
data"},"image012.png":{"si
Oct 31 09:55:12 mx02 HSC MailInspector[6051]: HSC LOG: msg
id E63CE258130.AA100 sent to logger . Total Sent: 24378 ,
Total Size: 24378
Oct 31 09:55:13 mx02 MTA/smtp[17184]: 954E025811B:
to=<suzana@xxxx.com.br>,
relay=180.38.108.51[180.38.108.51]:25, delay=317,
delays=316/0/0.19/0.91, dsn=2.0.0, status=sent (250 2.0.0
Ok: queued as 358921AF175)
Oct 31 09:55:13 mx02 MTA/qmgr[4616]: 954E025811B: removed

Seguindo o modelo acima descrito, segue a descrição dos campos para uso em SIEM ou similares:

SYSLOG OUTPUT:

{
"from_domain":"yammer.com", = Dominio de Origem do E-mail
"isrblspam":null, = Se está listado em Alguma RBL Externa
"issaspam":0, = Se foi Classificado como Possível SPAM
"sascore":-2.81, = Pontuação do Sistema de SPAM
"date":"2020-02-27", = Data de redebimento do e-mail
"time":"14:02:22", = Hora de recebimento do e-mail
"hostname":"pxl0spam0006", = Hostname do Servidor do MLI que recebeu o e-mail
"nameinfected":0, = Se foi Bloqueado por causa de Extensão de arquivo ou Mimetype
"quarantined":0, = Se foi colocado em Quarentena
"otherinfected":0, = Se foi Bloqueado por outro motivo, ex: Tamanho Excedido, Zip com Senha, etc
"size":31029, = Tamanho do E-mail
"to":"user@unimedfortaleza.com.br", = Destinatario do E-mail
"to_domain":"unimedfortaleza.com.br", = Dominio do Destinatário do E-mail
"delivered":1, = Se foi ou não entregue . 0 = Não , 1 = SIM
"archiveplaces":"", = Anexos do E-mail
"timestamp":"2020-02-27 14:02:22", = Timestamp do recebimento do E-mail
"from":"noreply@yammer.com", = Remetente do E-mail
"id":"9F76B436F2D.AB8C9", = ID do e-mail, identificador unico do MailInspector
"virusinfected":"0", = Se foi detectado Virus no e-mail
"clientip":"52.100.138.31", = IP do Servidor de Origem
"subject":"Daniela Borelli, these conversations could help get you up to speedthis week", = Assunto do E-mail
"spamwhitelisted":0, = Se o E-mail foi classificado como Whitelist
"point":"2", = ID do Agente que Filtrou o E-mail
"isspam":0, = Se foi considerado SPAM
"spamblacklisted":0, = Se o E-mail foi classificado como Blacklist
"ishigh":0 = Se foi Considerado SPAM
}

Histórico	Indica toda a interação sobre o registro, ou seja, apresenta quem fez o quê e quando no registro. Dessa forma o administrador poderá visualizar com maior clareza sobre as ações tomadas sobre o registro, dando maior aderência ao LGPD.

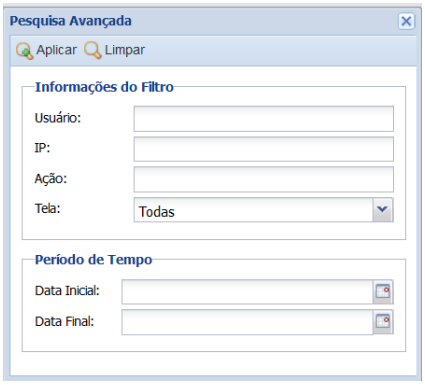


São apresentados os seguintes dados:

- Data e hora;
- Usuário;
- IP;
- Ação executada sobre o registro;

Ainda é possível tomar as ações de:

- **Pesquisar:** Pesquisa algum dado nos campos de data, usuário, IP ou ação;
- **Limpar:** Limpa o campo de pesquisa;
- **Pesquisa Avançada:** Permite a pesquisa sobre algum campo específico, podendo ser:
  - Usuário;
  - IP;
  - Ação;
  - Tela;
  - Período de Tempo;



- **Visualizar:** Visualiza o registro da ação marcada;
- **Exportar:** Exporta para CSV ou PDF;

Performance	Indica quanto tempo levou o processamento do e-mail, bem como quanto tempo consumiu cada um dos módulos aplicados sobre ele.

Filtros de Conteúdo | Assinaturas | Ameaças | Message Trace | Cabeçalho | Texto | HTML | Downloads | Data Loss Prevention | CDR | Smart Defender | Log de Evidência | **Performance**

Date/Time	Layer	Description	Delay
19/07/2021 21:22:50	SMTP	Mensagem recebida	-
19/07/2021 21:22:54	MAIL SPLIT	Processada pelo Mail Split	4s
19/07/2021 21:22:55	CONTENT FILTER	Iniciado processamento da mensagem	1s
19/07/2021 21:22:56	CONTENT FILTER	Analisando conteúdo	0.040s
19/07/2021 21:22:56	CONTENT FILTER	Analisando vírus	0.546s
19/07/2021 21:22:56	CONTENT FILTER	Analisando Anexos	0.010s
19/07/2021 21:23:06	CONTENT FILTER	Filtro de SPAM	10.001s
19/07/2021 21:23:07	CONTENT FILTER	Controle HTML CDR e URL Rewrite	0.211s
19/07/2021 21:23:07	CONTENT FILTER	CDR Documents	0.001s
19/07/2021 21:23:07	CONTENT FILTER	Sandbox	0.004s
19/07/2021 21:23:07	CONTENT FILTER	Finalizado processamento	0s
		Total	17s

Exemplo de apresentação de tempo de processamento em cada módulo eo tempo total de processamento da mensagem

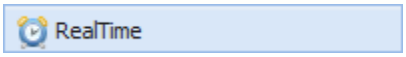
Obs: A apresentação dos módulos depende unicamente do que o e-mail analisado possui, por exemplo, se tiver anexo, será ativado o módulo análise de anexo, caso não tenha nenhum anexo, o módulo não será apresentado, pois não foi ativado. Os módulos possíveis de ativação são:

- **SMTP:** Módulo de conexão;
- **Mail Split:** Módulo de replicação do e-mail, de acordo com o número de pessoas em cópia;
- **Análise de Conteúdo:** Analisa o contexto do e-mail;
- **Análise de vírus:** Verifica vírus em anexos, até mesmo em imagens contidos no corpo do e-mail;
- **Análise de Anexos:** Verificação dos anexos;
- **Filtro de SPAM:** Módulo de Cálculo de pontuação do e-mail;
- **Controle HTML CDR e URL Rewrite:** Reescreve os links e analisa o e-mail pelo módulo CDR de HTML;
- **CDR Documents:** Analisa dos anexos pelo CDR (desde que estejam ativos o CDR e o anexo sejam padrão Office);
- **SandBox:** Análise dos artefatos pelo SandBox;

Os campos apresentados são:

- **Date/Time:** Data e hora do início da análise;
- **Layer:** Camada analisada;
- **Description:** Indicação do módulo analisado;
- **Delay:** Tempo de análise;
- **Total:** Tempo Total de processamento do e-mail;

Dashboards



/ **Dashboards**

Visão geral dos dashboards

Nesta tela cada administrador pode criar seus próprios dashboards para análise em tempo real de vários indicadores do sistema.

Cada usuário pode selecionar como e quais estatísticas gráficas serão exibidas, de forma que cada usuário possa adaptar a interface do MailInspector conforme sua preferência.

Cada administrador poderá customizar quais gráficos e onde eles ficarão localizados na tela, tudo de forma simples e fácil, sem a necessidade de desenvolvimento ou integração com softwares de terceiros. Esta customização é feita através de inclusão de Widgets.

Definições de Opções - Barra de ferramentas

Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição
Adicionar	Permite ao administrador criar um dashboard personalizado. O administrador pode adicionar quantos dashboards ele desejar.
Editar	Edita um Dashboard
Remover	Remove um Dashboard
Dashboard - Selecionar "Combo"	Seleciona e visualiza um dashboard já criado
Exportar	Exporta DashBoard previamente selecionado. A exportação poderá ser em um dos formatos: • PNG; • JPEG; • CSV; • PDF; • HTML;
Abrir Dashboard em nova janela	Permite abrir o Dashboard em uma nova janela, ao qual é independente de estar "logado" no MailInspector, dessa forma permitindo utilização do Dashboard em NOC. Esta janela é atualizada constantemente, de acordo com a indicação de atualização configurado pelo administrador do MailInspector.

Definições de Opções - Adicionar um Dashboard

Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição
Nome	Nome de identificação do Dashboard
Linhas	Número de linhas na tela

Colunas	Número de Colunas na tela, cada coluna é um contêiner específico para um dashboard
Atualizar	Tempo de atualização de dados contidos no Dashboard (é válido para os dashboards com atualização online): • 30 segundos; • 60 segundos; • 5 minutos; • 10 minutos; • 25 minutos; • 30 minutos;
Comparativo	Tempo de comparação: • Última hora; • Último dia; • Última semana; • Último mês;

Após salvar um novo Dashboard, você pode carregar ele selecionando-o no combo seletor. Quando você seleciona um dashboard ele irá automaticamente carregar as estatísticas que você configurou, se você ainda não configurou nenhuma estatística basta selecionar em "Novo Componente" o tipo de estatística que você deseja para cada um dos contêineres. A seguir está a lista de componentes e suas funcionalidades.

Definições de Componentes

Abaixo segue a lista dos componentes e seus dados

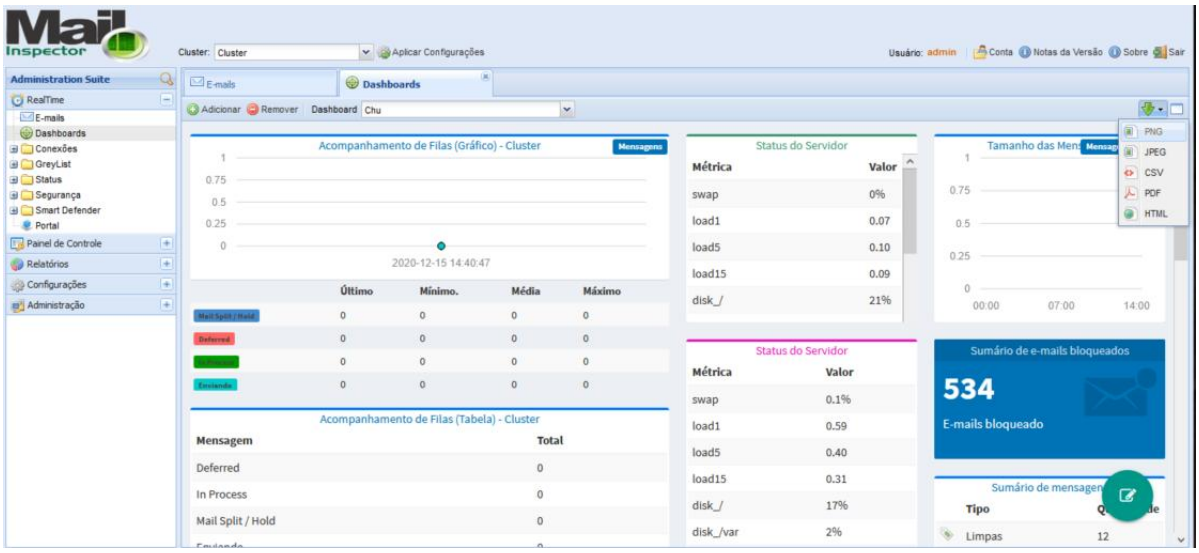
Componente	Definição
Acompanhamento de Filas – Gráfico (Esse mês)	Indica em gráfico de histórico da fila de e-mails no mês, separador por: • **Mail Split/Hold:** E-mails clonados para cada usuário/aguardando processamento; • **Deferred:** E-mails negados; • **In Process:** Em processamento; • **Active:** Ativos na fila;
Acompanhamento de Filas – Gráfico (Essa semana)	Indica em gráfico de histórico da fila de e-mails na semana, separador por: • **Mail Split/Hold:** E-mails clonados para cada usuário/aguardando processamento; • **Deferred:** E-mails negados; • **In Process:** Em processamento; • **Active:** Ativos na fila;
Acompanhamento de Filas – Gráfico (Online)	Indica em gráfico de como anda a fila de e-mails, separador por: • **Mail Split/Hold:** E-mails clonados para cada usuário/aguardando processamento; • **Deferred:** E-mails negados; • **In Process:** Em processamento; • **Active:** Ativos na fila;

Acompanhamento de Filas – Tabela (Esse mês)	Indica em tabela (números totais) o histórico da fila de e-mails no mês, separador por: • **Mail Split/Hold:** E-mails clonados para cada usuário/aguardando processamento; • **Deferred:** E-mails negados; • **In Process:** Em processamento; • **Active:** Ativos na fila;
Acompanhamento de Filas – Tabela (Essa semana)	Indica em tabela (números totais) o histórico da fila de e-mails na semana, separador por: • **Mail Split/Hold:** E-mails clonados para cada usuário/aguardando processamento; • **Deferred:** E-mails negados; • **In Process:** Em processamento; • **Active:** Ativos na fila;
Acompanhamento de Filas – Tabela (Online)	Indica em tabela (números totais) de como anda a fila de e-mails, separador por: • **Mail Split/Hold:** E-mails clonados para cada usuário/aguardando processamento; • **Deferred:** E-mails negados; • **In Process:** Em processamento; • **Active:** Ativos na fila;
Status do Servidor (agora)	Mostra o consumo de recursos por servidor e total com as seguintes informações: • Status; • Load Average (Consumo de carga pelo processamento dos e-mails); • Memória; • Uso de disco; • Número de Mensagens; • Número de Conexões; • Status do sincronismo (Em caso de uso de cluster);
Sumario de Ataques de SPOOFING de e-mails	Mostra o número de mensagens que tentaram forjar o remetente da mensagem, aqui todos é sumarizado todos os ataques verificados pelos mecanismos: DKIM, SPF, Domain Spoofing, E-mail Address Spoofing, E-mail Impostor, BEC (Business E-mail Compromise) e New Domains/Domínios recém adquiridos.
Sumário de e-mails bloqueados	Mostra o total de mensagens bloqueadas. Em caso de cluster pode ser selecionado a visualização por ponto ou total do cluster.
Sumário de e-mails enviados com criptografia	Mostra o total de mensagens que foram criptografadas. Em caso de cluster pode ser selecionado a visualização por ponto ou total do cluster.
Sumário de e-mails enviados e recebidos	Mostra o total de mensagens enviadas e recebidas. Em caso de cluster pode ser selecionado a visualização por ponto ou total do cluster.

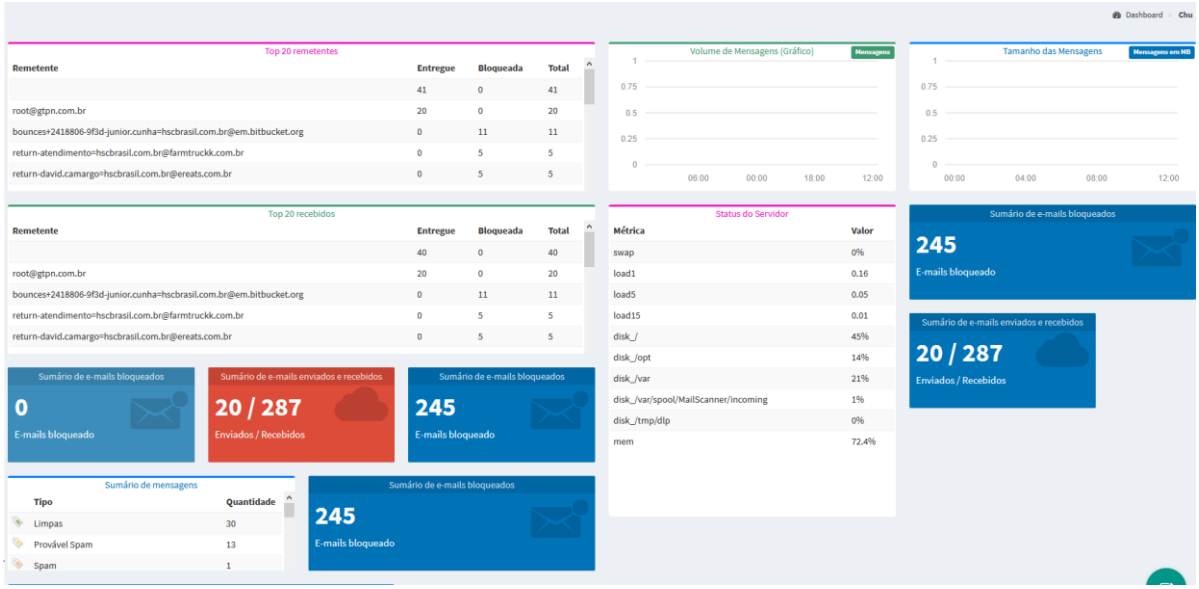
Sumário das mensagens	Mostra os tipos de mensagens, separados por tipo, com indicação de quantidade de mensagens de acordo com as seguintes classificações:
	• Mensagens Limpas;
	• Provável SPAM;
	• Vírus;
	• SPAMs;
	• Bloqueados por block list;
	• Liberados por allow list;
	• Tamanho Excedido;
	• Conteúdo Bloqueado;
	• Ameaças (Malwares, Virus, Ransomwares, etc);
	• Phishing;
	• ATP;
	• Bulk Mail;
	• Conteúdo Adulto;
	• Controle de Surto/Comportamento Anômalo:
	  ○ Ataques por excesso de conexões de uma única fonte;
	  ○ Ataque por DHA (ataque de dicionário);
	  ○ Ataque por vírus de uma única fonte;
	  ○ Ataque por reputação ruim da mesma origem;
	• Fraude de e-mail/E-mail impostor/BEC;
	• Spoofing;
	• SandBox;
	• Outro Bloqueio;
	Em caso de cluster pode ser selecionado a visualização por ponto ou total do cluster.

Sumário de mensagens com SPAM	Mostra o total de mensagens categorizadas como SPAM. Em caso de cluster pode ser selecionado a visualização por ponto ou total do cluster.
Sumário de mensagens com Vírus	Mostra o total de mensagens categorizadas como Vírus, malwares, ransomwares, etc. Em caso de cluster pode ser selecionado a visualização por ponto ou total do cluster.
Tamanho das Mensagens	Mostra o tamanho das mensagens que passaram pelos filtros. Em caso de cluster pode ser selecionado a visualização por ponto ou total do cluster.
Tipos de ataques	Mostra o total de mensagens categorizadas por tipo de ataque. Em caso de cluster pode ser selecionado a visualização por ponto ou total do cluster. Os tipos de ataques considerados são: • Vírus; • E-mails suspeitos; • Arquivos suspeitos; • Spoofing de domínio/E-mail impostor/E-mail Address Spoofing/BEC; • Phishing;

	• Malware; • Ransomware; • ATP (Ataque Persistente); • Ataque de dicionário (DHA);
Top 20 remetentes	Mostra quem são os principais remetentes de e-mail (origem).
Top 20 recebidos	Mostra quem são os principais recebedores de e-mail (destino).
Top 20 enviados	Mostra quem mais enviou e-mail.
Volume de Mensagens / Dados – Gráfico	Mostra o volume total de mensagens enviadas e recebidas, bem como quantidade de dados trafegados. Em caso de cluster pode ser selecionado a visualização por ponto ou todo cluster.
Volume de Mensagens – Gráfico (Esse mês)	Mostra o volume total de mensagens enviadas e recebidas no mês. Em caso de cluster pode ser selecionado a visualização por ponto ou total do cluster.
Volume de Mensagens – Gráfico (Essa semana)	Mostra o volume total de mensagens enviadas e recebidas na semana. Em caso de cluster pode ser selecionado a visualização por ponto ou total do cluster.
Volume de Mensagens / Dados – Tabela	Mostra o volume total de mensagens enviadas e recebidas, bem como quantidade de dados trafegados. Em caso de cluster pode ser selecionado a visualização por ponto ou total do cluster.
Volume de Mensagens – Tabela (Esse mês)	Mostra o volume total de mensagens enviadas e recebidas no mês. Em caso de cluster pode ser selecionado a visualização por ponto ou total do cluster.
Volume de Mensagens – Tabela (Essa semana)	Mostra o volume total de mensagens enviadas e recebidas na semana. Em caso de cluster pode ser selecionado a visualização por ponto ou todo cluster.
Controle de Anexos	Mostra um totalizador de quantas mensagens foram bloqueadas e quantas foram entregues que continham anexos.
Status do Cluster	Indica se o cluster está funcionando corretamente, bem como a comunicação entre os pontos de filtragem em relação ao ponto de gerenciamento. Também indica os recursos utilizados pelos pontos de filtragem (CPU, memória, disco, consumo de rede/banda, etc) e desempenho dos serviços.
Sumário da Console de Administração	Indica o uso dos recursos do gerenciador, isto é, do sistema de administração. Quanto está sendo utilizado do CPU do appliance de gerenciamento, quanto de memória utilizada e disponível, quanto de disco utilizado e disponível, etc. Também apresenta os dados de consumo de espaço da quarentena, separado pelo tipo de quarentena.
Bloqueio no MTA	Apresenta em tempo real as mensagens bloqueadas por conexão rejeitada, limite de número conexões efetuadas e bloqueio por reputação.



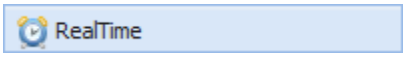
Exemplo de Dashboard



Dashboard aberto em nova janela. Repare que o nome do Dashboard fica no canto direito superior.

Conexões

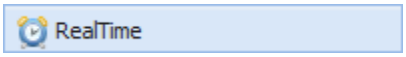
Este menu permite a visualização em tempo real das conexões.



/ Conexões

Logs do MTA

Use esta página para pesquisar, exibir ou executar ações nos registros das mensagens processadas pelo MTA do HSC MailInspector. Permite ao administrador visualizar todos os logs das mensagens que foram rejeitadas.



/ **Conexões / Logs do MTA**

O que é um agente de transporte de e-mail ou MTA?

Um agente de transporte de e-mail (MTA) é um aplicativo de software usado dentro de um sistema de tratamento de mensagem de internet (MHS). É responsável pela transferência e encaminhamento de uma mensagem de correio eletrônico do servidor do remetente para o servidor do destinatário através do protocolo SMTP. A plataforma básica para a MTA é um sistema de troca com a arquitetura cliente/servidor.

No HSC MailInspector, o MTA possui diversas funções, entre elas destacamos:

- Executar as primeiras camadas de filtragem do HSC SPAM Filter Ahead.
- Receber os e-mails enviados por outros servidores, e encaminhá-los para o processamento das outras camadas de filtragem.
  O HSC MailInspector possui Sistema Operacional próprio, o "HSC OS", que pode ser instalado em 32 ou 64 Bits

Visão geral dos logs do MTA

O módulo **Logs do MTA** permite ao administrador visualizar, pesquisar, filtrar e aplicar ações **em tempo real** sobre os registros das mensagens processadas pelo **MTA (Mail Transport Agent)** do HSC MailInspector.

O recurso oferece visibilidade detalhada sobre o fluxo de mensagens por SMTP, auxiliando na **identificação, diagnóstico e resolução de falhas de recebimento de e-mails durante a camada de conexão**.

Por meio dos registros, é possível identificar as causas de recusas, falhas de comunicação, problemas de configuração e outras ocorrências relacionadas ao processamento das mensagens, incluindo:

- **Servidor de origem sem registro de DNS reverso (PTR)** configurado;
- **Destinatário inválido ou inexistente**, conforme validação realizada junto ao diretório **LDAP/EntraID**;
- **Falhas na entrega da mensagem ao servidor de destino**, incluindo erros de comunicação ou indisponibilidade;
- **Servidor ou endereço IP de origem listado em RBL (Real-time Blackhole List)**;
- **Falhas ou recusas durante a comunicação SMTP**;
- **Mensagens bloqueadas ou rejeitadas por políticas de segurança**;
- **Outras ocorrências e códigos de erro registrados durante o processamento da mensagem**.

Dessa forma, o **Logs do MTA** constitui uma importante ferramenta de **troubleshooting e auditoria do fluxo de e-mails**, permitindo ao administrador acompanhar a rejeição das mensagens a nível de MTA e obter informações precisas para análise de incidentes e correção de eventuais problemas no ambiente de correio eletrônico.

Por padrão, o **HSC MailInspector mantém os registros de Logs do MTA referentes aos últimos 7 dias**, permitindo o acompanhamento e a análise do histórico recente de processamento das mensagens.

Após esse período, os logs são submetidos automaticamente ao processo de **rotação (log rotate).**

No módulo LOG do MTA, é possível extrair relatório de LDAP, ou seja, de e-mails enviados a usuários inexistentes ou tentativa de ataques de dicionário (DHA – Directory Harvest Attack)/backscatter/DHAP. Apresentando as origens de envio de e-mails inexistentes na caixa.

Definições da tela de Logs do MTA

Indicação das colunas apresentadas em logs do MTA.

Coluna	Definição
Data	Data de entrada do registro no Logs do MTA
Hora	Hora de entrada do registro no Logs do MTA
Ponto de Acesso	Ponto de filtragem, ao qual passou o registro
IP	IP de Origem do e-mail
De	Remetente do e-mail
Para	Destinatário do e-mail
Motivo	Motivo pelo qual foi barrado a nível de MTA (conexão)
Comando	Referente a qual tipo de comando em que registro foi detectado
Hostname	Nome da máquina de origem do e-mail
Tentativas	Número de tentativas de entrega do e-mail
Status	Tipo de Bloqueio: Bloqueado Temporariamente Bloqueado

Definições de Opções - Logs de MTA

Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição
Ponto de Acesso	Quando o sistema estiver configurado para funcionamento em CLUSTER, é possível selecionar por qual ponto de acesso "Servidor" a mensagem passou. Se usar a opção "Todos" listará todos os registros do cluster independente do servidor que processou a mensagem.
Pesquisar	Quando clicado, aplica o filtro informado na caixa de pesquisa rápida aos registros das mensagens processadas pelo MTA.
Limpar	Quando clicado, remove os filtros informados da caixa de pesquisa rápida e da janela de pesquisa avançada, e recarrega todos os registros de e-mails.

Pesquisa Avançada	Realiza uma pesquisa mais detalhada nos registros. Quando clicado, abre a caixa de diálogo **Pesquisa Avançada**.
Exportar	É possível exportar o resultado de uma pesquisa efetuada sobre o LOG do MTA, podendo ser exportado nos formatos: • CSV; • PDF; • XML;
Ações	Escolha entre: • **Liberar Endereço de IP** - Permite cadastrar o endereço IP do registro selecionado no sistema de filtragem do MTA, para que não sejam realizadas as verificações de controle de fluxo para mensagens originadas deste servidor, tais como: ○ Checagem de endereço IP reverso; ○ Checagem de endereço IP do servidor em RBL; ○ Checagem da reputação do servidor; ○ Demais controles de fluxo de mensagens; Por exemplo, esta ação permite o recebimento de mensagens de servidores bloqueados com o motivo: Client host rejected: cannot find your hostname, que não possuem registro PTR (reverso) corretamente cadastrado. • **Bloquear Endereço de IP** - Permite cadastrar o endereço IP do registro selecionado no sistema de filtragem do MTA, para que este servidor não possa entregar mensagens para o MTA do HSC MailInspector. • **Liberar Hostname** - Permite cadastrar o hostname do registro selecionado no sistema de filtragem do MTA, para que não sejam realizadas as verificações de controle de fluxo para mensagens originadas deste servidor, tais como: ○ Checagem de endereço IP reverso; ○ Checagem de endereço IP do servidor em RBL; ○ Checagem da reputação do servidor; ○ Demais controles de fluxo de mensagens; • **Bloquear Hostname** - Permite cadastrar o hostname do registro selecionado no sistema de filtragem do MTA, para que este servidor não possa entregar mensagens para o MTA do HSC MailInspector. • **Liberar domínio (De)** - Permite cadastrar o domínio de origem, do registro selecionado no sistema de filtragem do MTA, para que não sejam realizadas as verificações de controle de fluxo para mensagens originadas deste servidor, tais como: ○ Checagem de endereço IP reverso; ○ Checagem de endereço IP do servidor em RBL; ○ Checagem da reputação do servidor; ○ Demais controles de fluxo de mensagens; • **Bloquear domínio (De)** - Permite cadastrar o domínio de origem, do registro selecionado no sistema de filtragem do MTA, para que este servidor não possa entregar mensagens para o MTA do HSC MailInspector.

Definições de Opções - Pesquisa Avançada

Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição

Aplicar	Quando clicado, aplica os filtros informados e/ou selecionados aos registros das mensagens processadas pelo MTA.
Limpar Campos	Quando clicado, remove os valores informados ou selecionados pelo usuário.
De	Informe o endereço completo ou parcial do remetente.
Para	Informe o endereço completo ou parcial do destinatário.
IP	Informe o endereço IP completo do servidor de origem.
Hostname	Informa o hostname para a busca do registro do LOG do MTA.
Status	Filtra por Status possível no LOG do MTA: **Todos** — Não ativa o filtro de seleção por status **Bloqueado** — Apresenta somente os logs classificados como bloqueado em definitivo a nível de conexão (MTA); **Temporariamente Bloqueado** — Apresenta somente os logs classificados como bloqueado temporariamente a nível de conexão (MTA);
Motivo	Escolha entre: • **Blacklist bl.spamcop.net** - Conexão rejeitada pois o servidor de origem está listado na blacklist (RBL) spamcop.net. • **Blacklist cbl.abuseat.org** - Conexão rejeitada pois o servidor de origem está listado na blacklist (RBL) abuseat.org. • **Blacklist list.dsbl.org** - Conexão rejeitada pois o servidor de origem está listado na blacklist (RBL) dsbl.org. • **Blacklist sbl.spamhaus.org** - Conexão rejeitada pois o servidor de origem está listado na blacklist (RBL) SBL da spamcop.org. • **Blacklist xbl.spamhaus.org** - Conexão rejeitada pois o servidor de origem está listado na blacklist (RBL) XBL da spamcop.org. • **Blacklist zen.spamhaus.org** - Conexão rejeitada pois o servidor de origem está listado na blacklist (RBL) ZEN da spamcop.org. • **Client host rejected: Access denied** - Conexão rejeitada pois o servidor de origem não está autorizado a fazer relay no HSC MailInspector. • **Client host rejected: cannot find your hostname** - Conexão rejeitada pois o servidor de origem não tem o registro PTR (reverso) configurado corretamente. • **invalid_hostname_reject_code** - Conexão rejeitada pois o servidor de origem informou um nome de host com sintaxe errada no comando HELO ou EHLO. • **multi_recipient_bounce_reject_code** - Conexão rejeitada pois o servidor de origem está enviando uma mensagem que possui um remetente nulo, e é destinada a vários endereços. • **non_fqdn_reject_code** - Conexão rejeita por um dos motivos: nome do host informado durante o HELO ou EHLO não é um domínio qualificado ou foi informado de forma literal, o endereço MAIL FROM não possui um domínio qualificado ou o endereço RCPT TO não possui um domínio qualificado. • **plaintext_reject_code** - Conexão rejeitada pois a conexão não está encriptada.

	• **Recipient address rejected: Greylisted for 5 minutes** - Conexão rejeitada pele camada de antispam da Greylist. • **Recipient address rejected: User unknown** - Conexão rejeitada pois o destinatário não existe. • **Relay access denied** - Conexão rejeitada pois o servidor de origem não está autorizado a fazer relay no HSC MailInspector, por não existirem gravados seus endereços de "MX". • **Sender address rejected: Access denied** - Conexão rejeitada pois o remetente informado não está autorizado a enviar mensagens. • **Sender address rejected: Domain not found** - Conexão rejeitada pois o remetente informado não possui um domínio qualificado. • **unknown_hostname_reject_code** - Conexão rejeitada o nome de host informado durante o HELO ou EHLO não possui um registro DNS do tipo A ou MX. • **unknown_local_recipient_reject_code** - Conexão rejeitada pois o destinatário não existe. • **unknown_virtual_alias_reject_code** - Conexão rejeitada pois o destinatário não existe. • **unknown_virtual_mailbox_reject_code** - Conexão rejeitada pois o destinatário não existe. • **unverified_recipient_defer_code** - Conexão rejeitada pois o destinatário respondeu com um código de erro temporário. • **unverified_recipient_reject_code** - Conexão rejeitada pois o destinatário não está acessível. • **unverified_sender_reject_code** - Conexão rejeitada pois o remetente não está acessível. • **MailInspector throttling - High Risk Reputation** - Sistema de Throttling foi ativado pois o IP de origem tem a reputação de Alto Risco. • **MailInspector throttling - Medium Risk Reputation** - Sistema de Throttling foi ativado pois o IP de origem tem a reputação de Medio Risco. • **MailInspector throttling - Possible Risk Reputation** - Sistema de Throttling foi ativado pois o IP de origem tem a reputação de Possível Risco. • **HSC Directory Harvest Attack Prevention: too many unknown recipients** - Sistema de detecção de ataques do tipo "Harvest" foi ativado para este IP. • **Messages per connection limit reached** - Indica que esta origem enviou mais mensagens do que o permitido em uma única conexão.
Período de Tempo	**Data Inicial:** Ativa o filtro por range de data, começando pela data indicada; **Data Final:** Ativa o filtro por range de data, finalizando pela data indicada;

Portal | Logs do MTA

Ponto de Acesso : Todos | Pesquisa(De ou Para)... | Pesquisar | Limpar | Pesquisa Avançada | Ações

Data	Hora	Ponto de ...	IP	De	Para	Motivo	Comando	Hostname	Tentativas	Status
13/01/2019	01:07:00	mli01	187.108.197....	ubuntu@erio4.solucao-financeir...	contato@gtpn.com.br	4.1.8 : Sender address rejected: Domain not found	RCPT	mx-balancer.mlicloud.com	3	
13/01/2019	01:07:00	mli01	187.108.197....	www-data@rolvell1.accesscam.org	contato@gtpn.com.br	4.1.8 : Sender address rejected: Domain not found	RCPT	mx-balancer.mlicloud.com	3	
13/01/2019	01:02:00	mli01	187.108.197....	nabisexici@fale4.internegocios....	contato@gtpn.com.br	4.1.8 : Sender address rejected: Domain not found	RCPT	mx-balancer.mlicloud.com	3	
13/01/2019	01:02:00	mli01	187.108.197....	hevohegoxe@verificado08.pend...	contato@gtpn.com.br	4.1.8 : Sender address rejected: Domain not found	RCPT	mx-balancer.mlicloud.com	3	
13/01/2019	01:01:00	mli01	187.108.197....	juliano-andrade@nasas.net.br	contato@gtpn.com.br	4.1.8 : Sender address rejected: Domain not found	RCPT	mx-balancer.mlicloud.com	3	
13/01/2019	01:01:00	mli01	187.108.197....	isabelaescobar@filao.net.br	contato@gtpn.com.br	4.1.8 : Sender address rejected: Domain not found	RCPT	mx-balancer.mlicloud.com	3	
13/01/2019	00:50:00	mli01	187.108.197....	carol-barros@a.movelbr.com.br	contato@gtpn.com.br	4.1.8 : Sender address rejected: Domain not found	RCPT	mx-balancer.mlicloud.com	3	
13/01/2019	00:41:00	mli01	187.108.197....	retornos@lentes8.net.br	contato@gtpn.com.br	4.1.8 : Sender address rejected: Domain not found	RCPT	mx-balancer.mlicloud.com	6	
13/01/2019	00:41:00	mli01	187.108.197....	retornos@movelbr.com.br	contato@gtpn.com.br	4.1.8 : Sender address rejected: Domain not found	RCPT	mx-balancer.mlicloud.com	9	
13/01/2019	00:41:00	mli01	187.108.197....	return-conto-6csn8p-romulo=hsc...	contato@gtpn.com.br	4.1.8 : Sender address rejected: Domain not found	RCPT	mx-balancer.mlicloud.com	3	
13/01/2019	00:41:00	mli01	187.108.197....	www-data@chaelsa6.dynu.com	contato@gtpn.com.br	4.1.8 : Sender address rejected: Domain not found	RCPT	mx-balancer.mlicloud.com	3	
13/01/2019	00:41:00	mli01	187.108.197....	thiago.freitas@nasas.net.br	contato@gtpn.com.br	4.1.8 : Sender address rejected: Domain not found	RCPT	mx-balancer.mlicloud.com	3	
13/01/2019	00:40:00	mli01	187.108.197....	nataliabarbosa@t.nuances.net.br	contato@gtpn.com.br	4.1.8 : Sender address rejected: Domain not found	RCPT	mx-balancer.mlicloud.com	3	
13/01/2019	00:30:00	mli01	187.108.197....	laura-monteiro@k.consultae.net.br	contato@gtpn.com.br	4.1.8 : Sender address rejected: Domain not found	RCPT	mx-balancer.mlicloud.com	4	

Logs do MTA com indicação dos bloqueios a nível de conexão

Para obter maiores informações, basta dar um duplo clique sobre a conexão desejada.

Logs do MTA

Data:	13/01/2019
Hora:	00:50:00
IP:	187.108.197.232
De:	carol-barros@a.movelbr.com.br
Para:	contato@gtpn.com.br
Comando:	RCPT
Hostname:	mx-balancer.mlicloud.com
Tentativas:	3
Status:	Temporariamente Bloqueado
Motivo:	*4.1.8 : Sender address rejected: Domain not found*

Informação detalhada sobre o bloqueio efetuado a nível de conexão

Principais códigos de Erros SMTP – Bounce CODES

O MailInspector segue os códigos padrão de SMTP, conforme RFC 5321. Abaixo segue a tabela com possíveis retornos de erro de comunicação/rejeição do MTA.

Código	Descrição	Causa
SMTP Código de Entrega Indica que ocorreu a entrega do e-mail.		
200	E-mail has been delivered to the Inbox	E-mail entregue com sucesso.
215	E-mail has been delivered and moved to another folder due to a filtering rule	E-mail entregue, mas foi movido para outra pasta, devido a regra previamente estabelecida.
220	Server ready	Servidor pronto para comunicação.
250	Request mail action ok	Ação de envio do e-mail efetuado com sucesso.
251	User not local; will forward to <forward-path>	Usuário não é local, o e-mail será reencaminhado.
252	Cannot VRFY user, but will accept message and attempt delivery	O e-mail será aceito, mas a existência do usuário não foi verificado.
SMTP Código de Erro 4.0.0 Indica que o servidor está enfrentando uma falha temporária, mas o comando ainda pode ser concluído se tentar novamente. Os códigos que começam com 4 geralmente são erros relacionados ao sistema de recebimento de correio.		
412	Recipient address rejected: Domain not found	Domínio do destinatário não encontrado.
418	Sender address rejected: Domain not found	Domínio do remetente não encontrado no DNS Reverso.
420		A mensagem foi adiada devido a conteúdo suspeito. Tente mais tarde.
421	Service not available, closing transmission channel (This may be a reply to any command if the service knows it must shut down)	O serviço não está disponível e a conexão será fechada.
431		Espaço de disco insuficiente.
432	System not accepting network messages	Falha do destinatário ou bloqueio. A fila de mensagens recebidas do destinatário foi interrompida.
432 4.7.12	A password transition is needed	

441	No answer from the host	Destinatário está com problemas no recebimento que partem de seu servidor. O servidor destinatário não responde.
442	Bad connection	Falha de recebimento por parte do destino ou algum bloqueio por parte do mesmo (testar com e-mail de domínio público como Gmail ou Outlook). A conexão foi derrubada durante a transmissão.
446		Excedido o número máximo de saltos (hop) para esta mensagem.
447	Delivery time expired	Falha de comunicação com o servidor do destino. Se resolve, em geral, automaticamente, mas não é resolvido pelo servidor de disparos, e sim pelo de recebimento. A mensagem expirou devido a problemas relacionados ao servidor destino.
449		Erro de roteamento.
450	Requested mail action not taken: mailbox unavailable (e.g., mailbox busy or temporarily blocked for policy reasons)	O comando solicitado falhou porque a caixa de correio do usuário não estava disponível (por exemplo, porque estava bloqueada). Tente mais tarde.
450 4.7.1	Recipient address rejected: because...	Você pode saber lendo a mensagem depois de “because” ou “razão”, mas normalmente é relacionado a problemas na conexão ou DNS do servidor do destinatário, portanto tente novamente dentro de algumas horas, pois pode ser um problema temporário.
450 4.7.1	Recipient address rejected: Try again later	Quando a mensagem “Try again later” for retornada geralmente significa que o servidor onde está o e-mail do destinatário está passando por alguma manutenção, ou o seu e-mail está em Greylist, aguardando retorno (retry) para a liberação do mesmo.
451	Requested action aborted: local error in processing	O comando foi interrompido devido a um erro no servidor. Entre em contato com o administrador para alertá-lo sobre o problema.
451 4.4.1	IMAP Server unavailable	Servidor temporariamente desabilitado.
452	Requested action not taken: insufficient system storage	O comando foi interrompido porque o servidor possui armazenamento de sistema insuficiente. Também pode indicar muitos e-mails enviados simultaneamente ou excesso de destinatários.
454		A codificação TLS não está disponível devido a uma condição temporária.
454 4.7.0	Temporary authentication failure	Erro temporário de autenticação.
455	Server unable to accommodate parameters	O servidor não pode lidar com o comando no momento.
471	Client host rejected: cannot find your hostname	Não foi possível efetuar o DNS reverso, para chegar ao hostname de origem do e-mail.
471	Relay access denied	Tentou-se utilizar o MailInspector indevidamente como relay para e-mail.

Código	Descrição	Causa
SMTP Código de Erro 5.0.0 É caracterizado como falha permanente.		
500	Syntax error, command unrecognized (This may include errors such as command line too long)	O servidor não pôde reconhecer o comando devido a um erro de sintaxe.
500 5.5.6	Authentication Exchange line is too long	Erro em autenticação.
501	Syntax error in parameter or arguments	Foi encontrado um erro de sintaxe nos argumentos do comando. Podendo ser erro de autenticação, como por exemplo usuário inválido ou senha inválida ou ainda que o Sender Rewriting Scheme (SRS), de um provedor de e-mail, utiliza verificação de SPF. Isso impede que seja rejeitada a mensagem no servidor do destino.
501 5.5.2	Cannot Base64-decode Client responses	O servidor não responde ao Base Code-64. Não é possível decodificar a resposta.
501 5.5.4		O argumento HELO/EHLO é inválido.
501 5.7.0	Client initiated Authentication Exchange	Only when the SASL mechanism specified that client does not begin the authentication exchange.
502	Command not implemented	Este comando não está implementado.
502 5.5.1		Muitos comandos não reconhecidos. Comando não implementado/comando não reconhecido.
503	Bad sequence of commands	O servidor encontrou uma sequência incorreta de comandos.
504	Command parameter is not implemented	Um parâmetro de comando não está implementado.
504 5.5.4	Unrecognized authentication type	Tipo de autenticação não foi reconhecida.
510	Address reject	Endereço de e-mail inválido.
511	Recipient address rejected: User unknown	Endereço de e-mail inválido ou domínio não existe.
512	Bad destination system: no such domain	O servidor com o nome de domínio do destinatário não pode ser encontrado no DNS.
513	Bad recipient address syntax	Tipo de endereço incorreto. Algum caracter está errado no e-mail do destino. Verificar se não existem caracteres especiais (parênteses ou aspas por exemplo).
521	Server does not accept mail	Servidor não é de Correio Eletrônico ou não aceita e-mails.
523	Encryption needed	Criptografia necessária.

530	Mail server permanently rejected message	É necessário emitir o comando STARTTLS / Erro de autenticação.
530 5.7.0	Authentication required	É necessária autenticação.
530 5.7.8	Authentication credentials invalid	Credenciais inválidas.
530 5.7.9	Authentication mechanism is too weak	Autenticação fraca.
530 5.7.11	Encryption required for requested authentication mechanis	Necessária autenticação com criptografia.
532	System not accepting network messages	Bloqueio por parte do destino ao domínio do remetente.
534	Too long header	Ocorre caso tenha muitos contatos de e-mail (como no CC ou CO) e caso exista uma troca de mensagens e o cabeçalho do e-mail fique muito grande e com muitos campos.
534 5.7.9	Authentication mechanism is too weak	Sistema de autenticação fraca.
535		Falha na autenticação.
535 5.7.8	Authentication credentials invalid	Senha inválida.
538 5.7.11	Encryption required for requested authentication mechanism	Necessária criptografia para autenticação.
541		A mensagem foi rejeitada pelo endereço do destinatário.
544	Internal Domain lookup failed	Problema no domínio do destinatário.
546	Routing Loop detected ou loops back to myself	Ocorre quando uma caixa de e-mail é configurada para enviar cópias para uma caixa de e-mail e a mesma também está configurada para responder para o remetente, gerando um loop de e-mails.
550	User Unknow	O comando solicitado falhou porque a caixa de correio do usuário não estava disponível (por exemplo: Porque não existe ou porque o comando foi rejeitado por motivos de política). Também pode ser que o destinatário não existe no servidor. Pode ser um erro de digitação na hora de inserir a conta.
550 5.1.0	Bad e-mail Address	Endereço com erro. Pode ser erro no PARA, com cópia e/ou cópia oculta. Verifique os destinatários do e-mail.
550 5.1.1	Recipient address rejected: User unknown in virtual mailbox table (in reply to RCPT TO command)	O servidor onde possivelmente estava esta conta de e-mail respondeu que esta conta de e-mail não existe mais. Possivelmente ela foi apagada.

550 5.7.17	Sorry, no mailbox here by that name	Endereço de e-mail incorreto ou conta não existente.
551	User not local; please try <forward-path>	O destinatário não é local para o servidor. O servidor fornece um endereço de encaminhamento para tentar.
552	Requested mail action aborted: exceeded storage allocation	A ação foi interrompida devido à alocação de armazenamento excedida.
552 5.2.3	Message size exceeds fixed maximum message size	Mensagem extrapolou o tamanho máximo permitido. Isso acontece quando o servidor do destinatário tem algum limite de tamanho para o recebimento das mensagens. Seu e-mail ou anexo está muito grande para o servidor.
553	Erro in DNS	O comando foi interrompido porque o nome da caixa de correio é inválido ou Entrada de DNS SMTP não consta no seu servidor, e a mensagem é rejeitada.
553 5.0.0	Possible virus	Possível vírus encontrado no e-mail. O e-mail que você enviou possivelmente está com algum vírus.
554	Relay Access Denied	A transação falhou. Ocorre por dois motivos: • Domínio recente e com DNS propagando • Entrada SMTP não está constando no servidor
554 5.3.4	Message too big for system	Mensagem muito grande.
554 5.7.1	Client host rejected: Access denied	E-mail foi negado. Possível problema é que esteja em uma RBL.
556	Domain does not accept mail	Domínio inválido.
571	HSC MailInspector - Seu servidor de e-mails encontra-se em uma Lista de Bloqueio. Delivery not authorized, message refused	Seu gerenciador de e-mails não tem a permissão de envio de e-mails do destinatário, pois está em Block List.
577	Invalid HELO format	Servidor de destino não reconhece o formato HELO utilizado no e-mail do remente.

Fila de E-mails

Use esta página para pesquisar, exibir ou executar ações na fila de e-mails do MTA do HSC MailInspector.

RealTime / **Conexões / Fila de E-mails**

Visão geral da fila de e-mails

A Fila de E-mails é uma combinação de estruturas de diretórios do sistema de arquivos utilizadas para receber, armazenar, processar e encaminhar os e-mails durante o processamento dos filtros do HSC MailInspector. O sistema de fila de e-mails é totalmente otimizada para que tenha o melhor desempenho possível, dessa forma garantindo a entrega/recebimento de e-mails com maior velocidade.

O Tamanho destas filas é customizável na hora da instalação do Ponto de Acesso e/ou na configuração de Fila Personalizada. As filas de e-mail do HSC MailInspector trabalham de maneira simultânea e podem processar milhares de mensagens por hora sem perda de performance ou atraso de entrega, suportando sobrecarga de mensagens devido a falhas de entrega ou devido a falha de outros pontos da infraestrutura de e-mail da empresa.

Caso ocorra falha na conexão de saída, atrasos ou erros de entrega, ocorrerá nova tentativa de entrega, desde que o erro retornado não seja de falha permanente de entrega, tal como endereço de e-mail inválido, dessa forma é possível garantir a entrega do e-mail, mesmo que o servidor destino fique “fora do ar” por longo período (a ser definido pelo administrador), com o e-mail de saída parado na fila para nova tentativa de entrega. Assim que o servidor destino retornar ao normal, o e-mail será reenviado automaticamente.

O MailInspector permite ao administrador definir para o número máximo de processamento a ser utilizado em paralelo para um grupo de filas ou para uma fila específica.

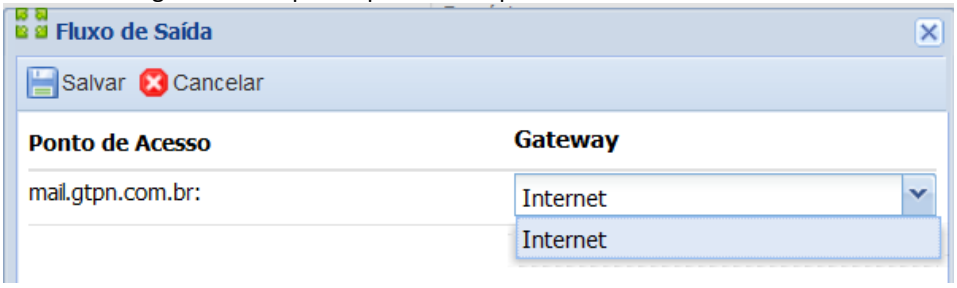
Na fila de e-mails é possível selecionar múltiplas ações:

- Forçar Envio da Mensagem - Permite forçar o envio de uma mensagem selecionada;
  Se houver alguma situação que impeça o e-mail de ser entregue para o destinatário, o MTA coloca este e-mail em modo de espera, por um determinado período pré-configurado. Após este período, o MTA realiza novas tentativas de entregas, se não houver sucesso, o MTA devolve a mensagem para o usuário que a enviou informando o erro.
- Remover Mensagem da Fila - Remove a mensagem selecionada da fila de e-mails, devolvendo-a ao remetente;
- Forçar Reenvio da Mensagem - Força o reenvio de uma mensagem específica;
- Forçar Reenvio da Fila - Permite forçar o envio de todas as mensagens que estão na fila;
- Parar Fila de E-mails - Para/pausa o processamento da fila de e-mails;
- Inicializar Fila de E-mails - Inicializa a Fila Parada/Pausada;
- Filtrar e-mails contidos na fila em tempo real, por fluxo de entrega e fluxo de recebimento;
- Filtrar e-mails por domínio de destino e domínio de origem;
- Filtrar e-mails contidos na fila somente por e-mails de saída ou e-mails de entrada;

Definições de Opções - Fila de E-mails

Estas informações descrevem as opções disponíveis nesta página.

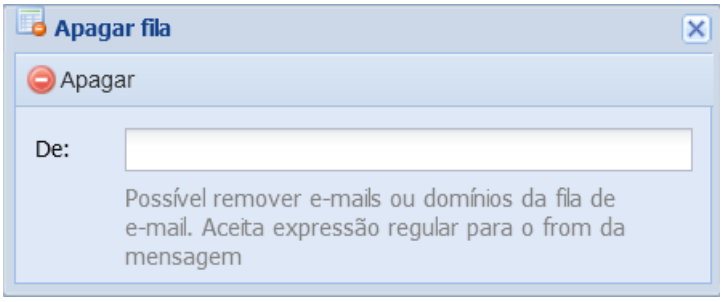
Opções	Definição
Sumário por Domínio	Permite Visualizar de forma agrupada as filas por domínio do destinatário

Sumário por Fila	Permite visualizar e-mails das filas personalizadas, criadas pelo administrador do sistema
Detalhes	Visualização detalhada da fila selecionada. Com essa visualização, é possível ao administrador determinar as ações a serem tomadas nos e-mails que estiverem na fila selecionada.
Fluxo de Saída	Permite ao administrador configurar por qual Gateway o e-mail deve sair: • Internet: Gateway Padrão de saída dos e-mails. • Por Ponto de Acesso: Seleção de saída por ponto de filtragem selecionada, isto é, redireciona a saída de todos os e-mails por um agente específico. Por exemplo: Um cluster onde tenho dois pontos de acesso configurado, sendo os nomes dos agentes (ponto01 e ponto02). É possível indicar a saída de todo o tráfego de e-mail para o ponto02 ou ponto01. 
Agrupar	**Nenhum:** Sem agrupamento de domínios. **Domínio:** Agrupa as filas por domínio.
Ponto de Acesso	**Todos:** Apresenta a fila de Todos os pontos de acesso. **Ponto de Acesso Específico:** Apresenta a fila de um ponto de acesso específico.
Pesquisa por domínio	Insira o domínio a ser filtrado, podendo ser parcial
Pesquisar	Efetua a pesquisa pelo domínio acima indicado.
Limpar	Remove qualquer filtro e recarrega as informações.
Detalhe	É o mesmo que clicar o botão Detalhes, ou seja, se estiver marcado um domínio, será visualizado os detalhes dos e-mails na fila do domínio selecionado.

Definições de Opções - Fila de E-mails

Após clicado em Detalhes (para visualizar a fila de um determinado domínio), será apresentada as seguintes opções.

Opções	Definição
Ponto de Acesso	Quando o sistema estiver configurado para funcionamento em CLUSTER, é possível selecionar por qual ponto de acesso "Servidor" a mensagem passou. Se usar a opção "Todos" listará todos os registros do cluster independente do servidor que processou a mensagem.
Pesquisar	Quando clicado, aplica o filtro informado na caixa de pesquisa rápida aos registros da fila de e-mails do MTA.

Limpar	Quando clicado, remove os filtros informados da caixa de pesquisa rápida e da janela de pesquisa avançada, e recarrega todos os registros de e-mails.
Pesquisa Avançada	Realiza uma pesquisa mais detalhada nos registros, permitindo visualizar e-mails de uma determinada fila de prioridade ou fazer pesquisas por quaisquer campos agrupando o resultado por: • **Domínios do Remetente e/ou;** • **Domínio do Destinatário e/ou;** • **Endereço de e-mail do remetente e/ou;** • **Endereço de e-mail do destinatário e/ou;** • **Qualquer palavra-chave contido nos campos anteriormente citados;** • **Status;** • **Detalhes.** Para maiores detalhes, vide ***Definições de Opções - Pesquisa Avançada.***
Apagar Fila	Quando clicado, abre um campo onde é possível inserir expressões regulares, ou apenas domínios, e-mails e usuários específicos para que sejam deletados da fila de e-mails. 
Exportar	Permite a expostação dos dados da tela, referentes a fila de e-mails.
Ações	Escolha entre: • **Forçar Envio da Mensagem** - Permite forçar o envio de uma mensagem selecionada. Se houver alguma situação que impeça o e-mail de ser entregue para o destinatário, o MTA coloca este e-mail em modo de espera, por um determinado período pré-configurado. Após este período, o MTA realiza novas tentativas de entregas, se não houver sucesso, o MTA devolve a mensagem para o usuário que a enviou informando o erro. • **Remover Mensagem da Fila** - Remove a mensagem selecionada da fila de e-mails, devolvendo-a ao remetente. • **Forçar Reenvio da Fila** - Permite forçar o envio de todas as mensagens que estão na fila.

Definições de Opções - Pesquisa Avançada

A pesquisa avançada permite ao administrador efetuar buscas mais detalhadas, casando múltiplos campos conforme a sua necessidade. Ao selecionar esta opção são apresentados os seguintes dados:

Opções	Definição
Aplicar	Quando clicado, aplica os filtros informados aos registros da fila de e-mails do MTA.

Limpar Campos	Quando clicado, remove os valores informados ou selecionados pelo usuário.
De	Informe o endereço completo ou parcial do remetente.
Para	Informe o endereço completo ou parcial do destinatário.
OPERADOR LÓGICO (E / OU)	Casa as condições do campo DE em relação ao campo PARA.
Status	Filtra por: • Todos: Todas as condições (sem filtro ativo); • Mensagem sendo enviada; • Mensagem sendo processada/filtrada; • Erro/Atraso no envio;
Detalhes	Motivo do e-mail estar parado na fila

Definições da tela de Fila de E-mails (Detalhes)

Indica a fila de e-mail, com os dados dos e-mails que estão aguardando a entrega.

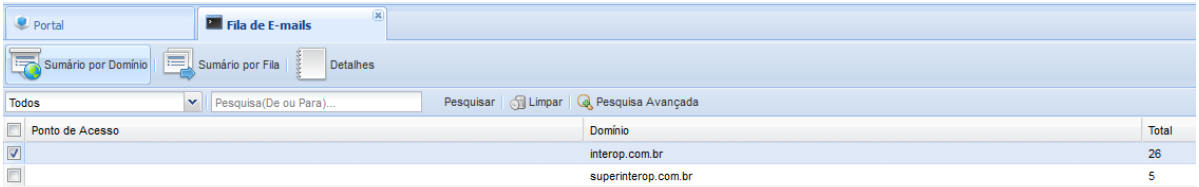
Opções	Definição
Data	Data de chegada do e-mail.
Ponto de Acesso	Ponto de filtragem que está contido e-mail na fila.
De	Informe o endereço do remetente.
Para	Informe o endereço do destinatário.
Detalhes	Motivo do e-mail estar parado na fila.
Tamanho	Tamanho do e-mail.
Tráfego	Sentido do e-mail, isto é, se está parado na fila de entrada ou na fila de saída.
Status	Indica o status do e-mail: • Falha ao enviar a mensagem ou; • Mensagem sendo enviada

Na parte inferior da tela possui indicadores dos totais:

- **Total de saída:** Indica quantos e-mails parados na fila no sentido de SAÍDA;
- **Total de entradas:** Indica quantos e-mails parados na fila no sentido de ENTRADA;
- **Erros na entrega:** Indica total de e-mails parados na fila, por falha na entrega**;**

Visualizar Fila de E-mails por Domínio

É possível efetuar visualizar e conrolar da fila de e-mails por domínio, indicando inclusive total de e-mails na fila por domínio e/ou mostrando somente os e-mails de um determinado domínio selecionado.



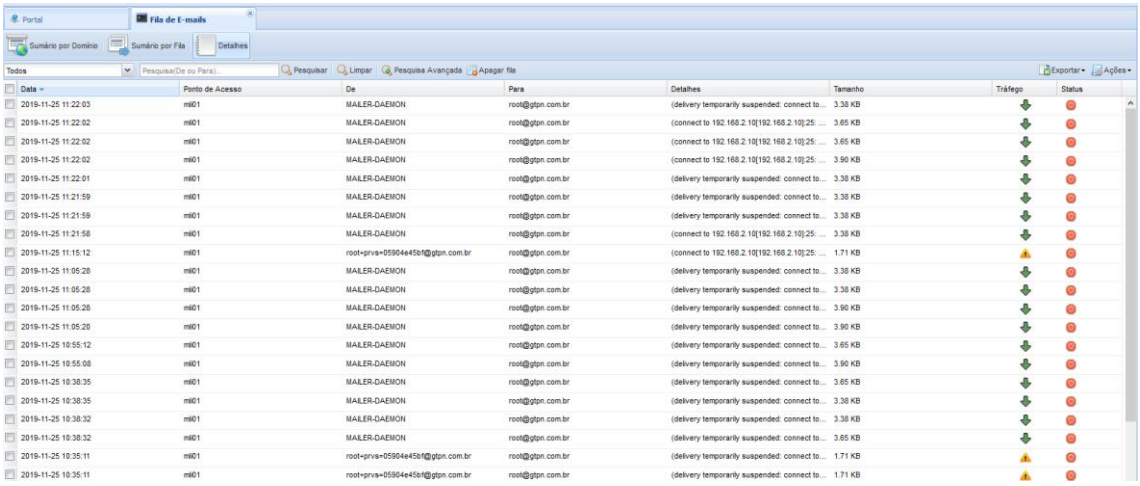
Visão de dashboard da fila de e-mails (Sumário por Domínio)

Definições da tela Sumário por Domínio

Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição
Ponto de Acesso	Ponto de acesso em que está o e-mail enfileirado
Domínio	Qual o domínio atendido
Total	Quantidade de e-mails na fila

Ao dar duplo clique sobre um domínio, é aberto abaixo todos os e-mails referentes ao domínio, dessa forma o administrador poderá verificar todos os e-mails referentes a um domínio em específico e selecionar as ações a serem efetuadas sobre os e-mails na fila. Para melhor organização, também é possível separar por fila de entrada e fila de saída.

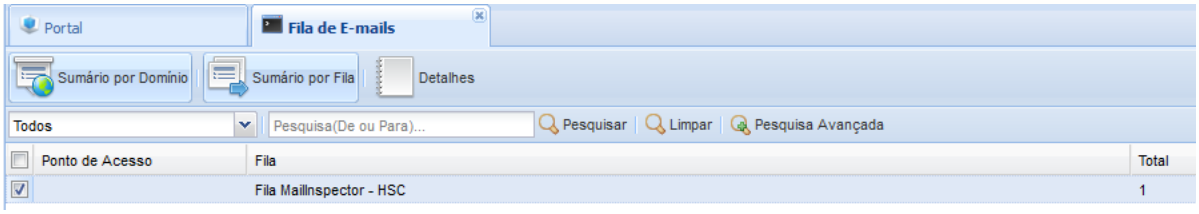


Visão de detalhada da fila de e-mails

É possível ainda customizar a fila de e-mails (efetuar um controle personalizado, indicando prioridade das filas por domínio), indicando filtros específicos de domínios e prioridades na fila. Para isso, vá em: *Filas Personalizadas*

Visualizar Fila de E-mails por Sumário da Fila

Esta opção mostra as filas customizadas criadas pelo administrador. Essa customização permite a otimização da fila de e-mails do MailInspector, priorizando as filas de acordo com a necessidade da empresa.



Visão de dashboard da fila de e-mails (Sumário por Fila)

Definições da tela Sumário por Fila

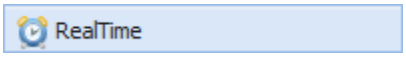
Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição
Ponto de Acesso	Ponto de acesso em que está o e-mail enfileirado
Fila	Nome da fila criada pelo administrador
Total	Quantidade de e-mails na fila

Ao dar duplo clique sobre uma regra customizada, é aberto abaixo todos os e-mails referentes a regra, dessa forma o administrador poderá verificar todos os e-mails referentes a uma determinada regra em específico e selecionar as ações a serem efetuadas sobre os e-mails na fila. Para melhor organização, também é possível separar por fila de entrada e fila de saída.

Mail Tracker

Use esta página para pesquisar ou exibir em tempo real todos as conexões e logs do sistema de filtragem de e-mail.



/ Conexões / Mail Tracker

Visão geral Mail Tracker

Permite visualizar os logs de filtragem, comandos executados, bem como toda a cadeia de análise sobre o e-mail, tanto na entrada, quanto na saída de e-mails em tempo real de processamento da mensagem.

Com o Mail Tracker, o administrador poderá facilmente efetuar debug de qualquer e-mail, em qualquer fase de seu processamento, desde conexão, análise de regulamentação de RFC, aceite do e-mail pelo sistema de processamento de mensagens, filtragem, resultado de consulta de reputação, análise de conteúdo, busca de ameaças e eventuais bloqueios e até mesmo de bloqueio por alguma regra customizada criado pelo administrador. Nos logs também é possível visualizar e-mails que tentam efetuar disseminação em massa de spams, e-mails infectados, malwares e/ou campanhas de phishing/spear phishing. Dessa forma é possível efetuar o rastreamento de uma mensagem por completo visualizando os respectivos logs de eventos, desde o início até ao fim da conexão, sendo utilizado como “debug de e-mails”.

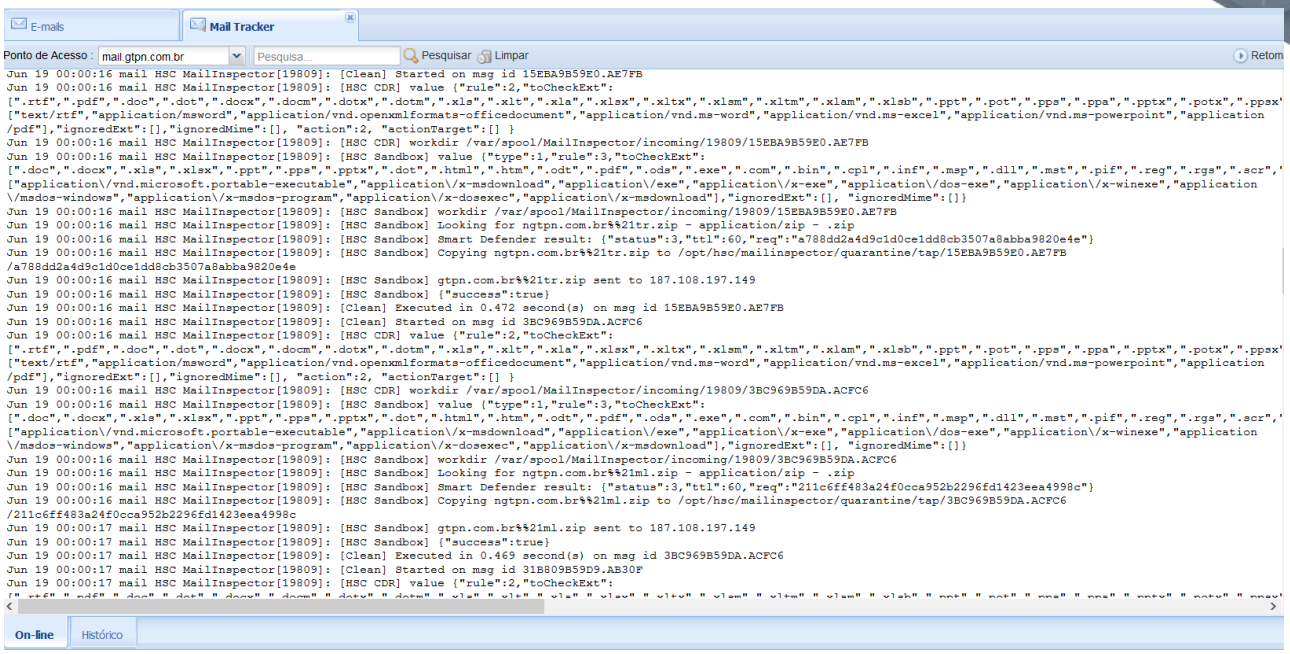
O Mail Tracker é separado em dois modos:
OnLine: Permite visualizar todo o rastreamento em tempo real, para acompanhar um e-mail que esteja já sendo aguardado, com rolagem de tela dos logs de forma automática.
Histórico: Retorna o histórico de rastreamento por logs de um determinado e-mail, permitindo filtragem por alguns campos, tais como data, ponto de filtragem e palavra-chave, permitindo pesquisa por quaisquer dados (ex: ID da mensagem, remetente, destinatário, IP de Origem, IP de Destino, cabeçalho customizado, From do Envelope, From do Header, To do Envelope, To do Header, Display Name, domínio, subdomínio, filtros associados, regras de DLP, pasta de quarentena, assinaturas de spam, etc) usando RegEx.
Conexões SMTP: Apresenta as conexões estabelecidas com outros servidores de e-mail em tempo real.

OnLIne

Definições de Opções - Mail Tracker (OnLine)

Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição
Ponto de Acesso	Quando o sistema estiver configurado para funcionamento em CLUSTER, é possível selecionar qual ponto de acesso "Servidor" o rastreio de uma mensagem será executado.
Pesquisar	Quando clicado, aplica o filtro informado na caixa de pesquisa rápida aos registros das mensagens processadas pelo MTA.
Limpar	Quando clicado, remove os filtros informados da caixa de pesquisa rápida e da janela de pesquisa avançada, e recarrega todos os registros de e-mails.
Parar	Pausa a entrada de logs em tempo real, permitindo ao administrador efetuar a busca de log específico, sem que a tela fique efetuando a rolagem automática.
Retornar	Retorna a rolagem de logs na tela em tempo real, efetuando a rolagem automática.



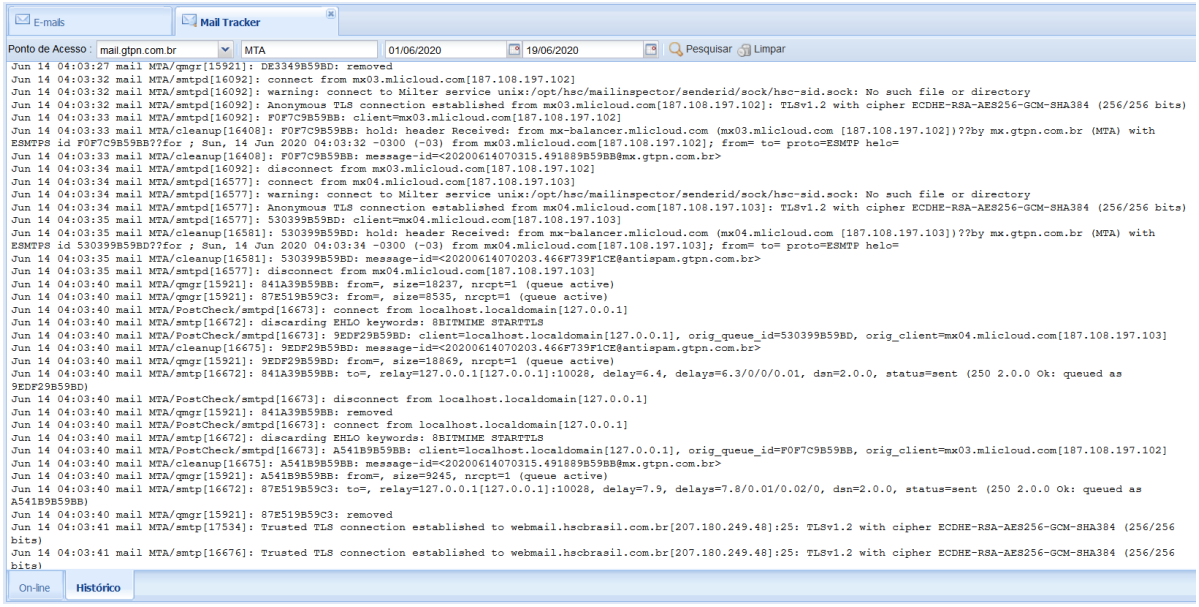
Exemplo de Mail Tracker no modo OnLine

Histórico

Definições de Opções - Mail Tracker (Histórico)

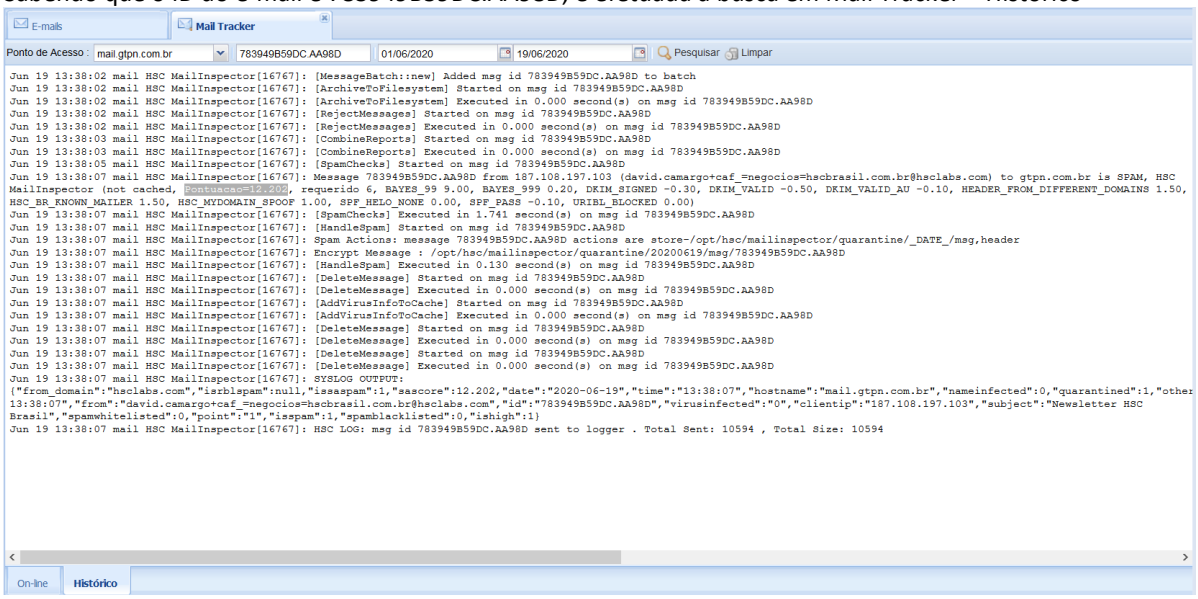
Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição
Ponto de Acesso	Quando o sistema estiver configurado para funcionamento em CLUSTER, é possível selecionar qual ponto de acesso "Servidor" o rastreio de uma mensagem será executado.
Pesquisa Rápida	Campo de inclusão de palavra-chave para busca rápida nos logs, retornando toda e qualquer entrada com a palavra indicada, permitindo pesquisa por quaisquer dados usando RegEx.
Pesquisar	Quando clicado, aplica o filtro informado na caixa de pesquisa rápida aos registros das mensagens processadas pelo MTA.
Data Inicial	Data inicial de busca nos logs do MTA.
Data final	Data final de busca nos logs do MTA.
Limpar	Quando clicado, remove os filtros informados da caixa de pesquisa rápida e da janela de pesquisa avançada, e recarrega todos os registros de e-mails.



Exemplo de Mail Tracker no modo Histórico

Exemplo de busca de logs de um e-mail específico, para detectar a pontuação e a ação efetuada sobre o mesmo.
Sabendo que o ID do e-mail é 783949B59DC.AA98D, é efetuada a busca em Mail Tracker > Histórico



- Verificada a pontuação recebida: Pontuação=12.202, requerido 6
- Efetuada ação de final de quarentena: [HandleSpam] Started on msg id 783949B59DC.AA98D
  Spam Actions: message 783949B59DC.AA98D actions are store-/opt/hsc/mailinspector/quarantine/_DATE_/msg,header

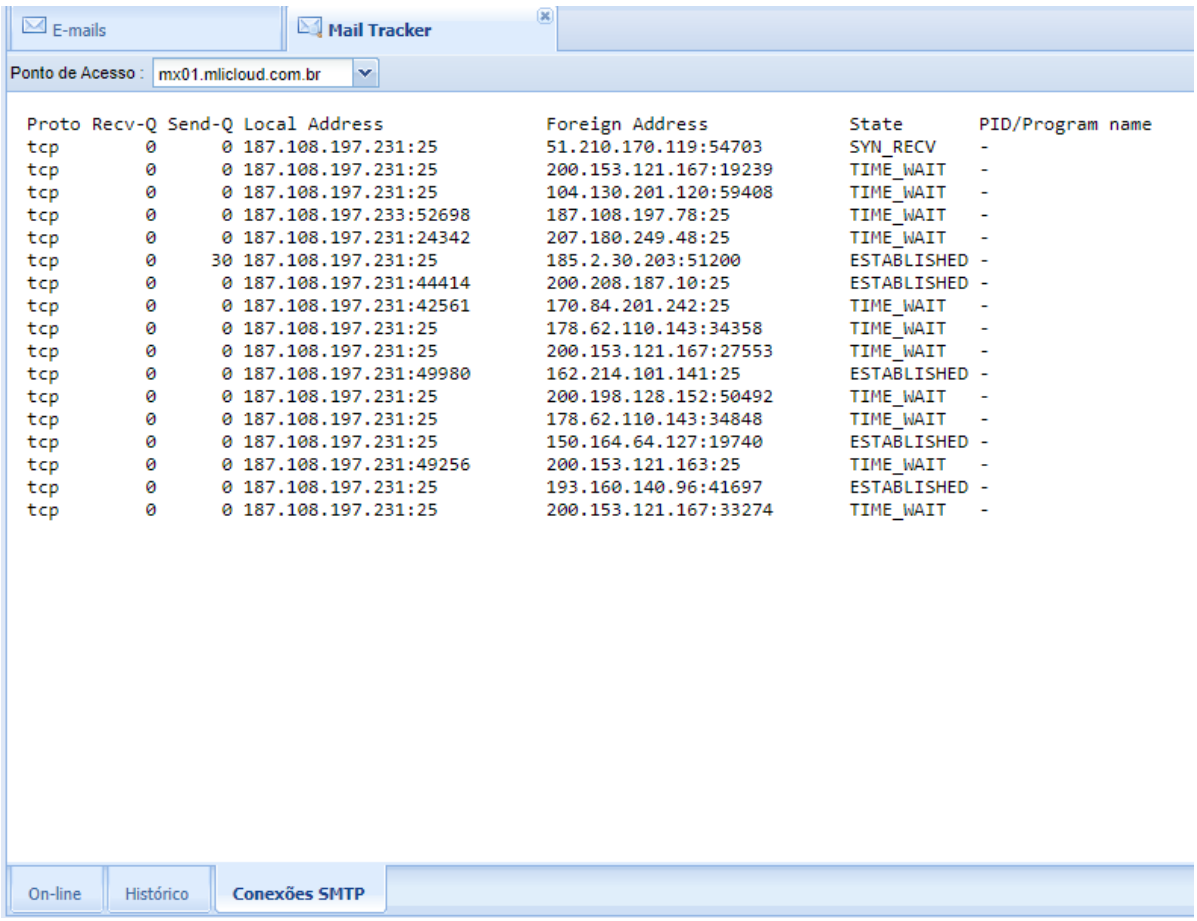
Conexões SMTP

Definições de Opções - Mail Tracker (Conexões SMTP)

Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição

Ponto de Acesso	Quando o sistema estiver configurado para funcionamento em CLUSTER, é possível visualizar as conexões estabelecidas de acordo com o ponto de acesso selecionado.




```
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 187.108.197.231:25      51.210.170.119:54703    SYN_RECV    -
tcp        0      0 187.108.197.231:25      200.153.121.167:19239   TIME_WAIT   -
tcp        0      0 187.108.197.231:25      104.130.201.120:59408   TIME_WAIT   -
tcp        0      0 187.108.197.233:52698   187.108.197.78:25       TIME_WAIT   -
tcp        0      0 187.108.197.231:24342   207.180.249.48:25       TIME_WAIT   -
tcp        0     30 187.108.197.231:25      185.2.30.203:51200      ESTABLISHED -
tcp        0      0 187.108.197.231:44414   200.208.187.10:25       ESTABLISHED -
tcp        0      0 187.108.197.231:42561   170.84.201.242:25       TIME_WAIT   -
tcp        0      0 187.108.197.231:25      178.62.110.143:34358    TIME_WAIT   -
tcp        0      0 187.108.197.231:25      200.153.121.167:27553   TIME_WAIT   -
tcp        0      0 187.108.197.231:49980   162.214.101.141:25      ESTABLISHED -
tcp        0      0 187.108.197.231:25      200.198.128.152:50492   TIME_WAIT   -
tcp        0      0 187.108.197.231:25      178.62.110.143:34848    TIME_WAIT   -
tcp        0      0 187.108.197.231:25      150.164.64.127:19740    ESTABLISHED -
tcp        0      0 187.108.197.231:49256   200.153.121.163:25      TIME_WAIT   -
tcp        0      0 187.108.197.231:25      193.160.140.96:41697    ESTABLISHED -
tcp        0      0 187.108.197.231:25      200.153.121.167:33274   TIME_WAIT   -
```

Controle de Fluxo

Use esta página para visualizar o consumo das regras de fluxo de e-mail

RealTime **/ Conexões / Controle de Fluxo**

Visão geral Controle de Fluxo

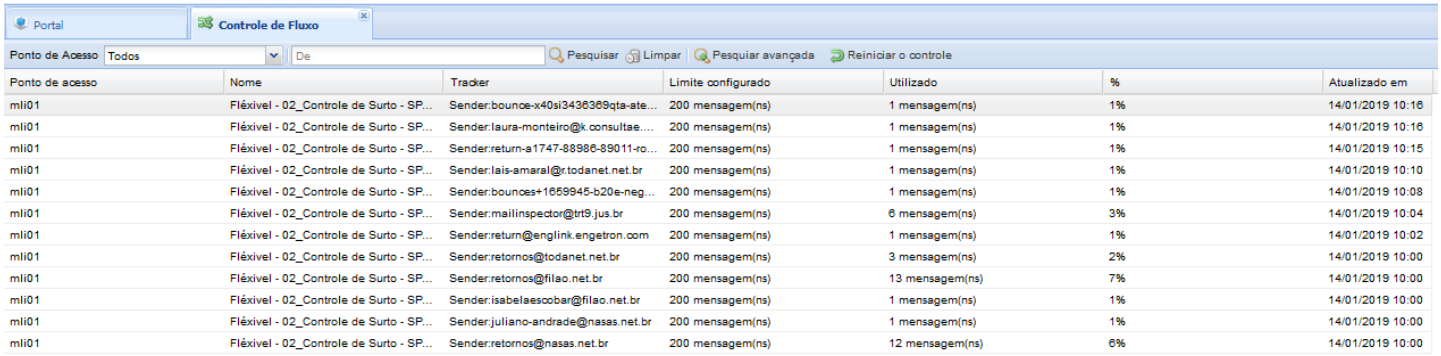
O item Controle de Fluxo permite visualizar em tempo real quanto do controle de fluxo que está sendo consumido, de acordo com regras que o administrador previamente indicou em Fluxo de E-mail.

Com ele o administrado pode facilmente visualizar e resetar o controle de fluxo para um determinado usuário/grupo.

Definições de Opções – Controle de Fluxo

Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição
Ponto de Acesso	Quando o sistema estiver configurado para funcionamento em CLUSTER, é possível selecionar qual ponto de acesso "Servidor" o rastreio de uma mensagem será executado.
Pesquisar	Quando clicado, aplica o filtro informado na caixa de pesquisa rápida aos registros das mensagens processadas pelo MTA.
Limpar	Quando clicado, remove os filtros informados da caixa de pesquisa rápida e da janela de pesquisa avançada, e recarrega todos os registros de fluxo de e-mails.
Pesquisa Avançada	Abre a janela de pesquisa avançada, ao qual pode ser buscada algum fluxo em específico de acordo com os campos disponíveis: • Nome da Quota; • Tracker; • Utilizado: Quanto que foi utilizado da cota (maior ou igual / menor ou igual)
Reinicilizar o controle	Reinicializa o contador da cota para aquele Tracker em específico.



Ponto de acesso	Nome	Tracker	Limite configurado	Utilizado	%	Atualizado em
mli01	Flexível - 02_Controle de Surto - SP...	Sender:bounce-x40si3436369qta-ate...	200 mensagem(ns)	1 mensagem(ns)	1%	14/01/2019 10:16
mli01	Flexível - 02_Controle de Surto - SP...	Sender:laura-monteiro@k.consultae....	200 mensagem(ns)	1 mensagem(ns)	1%	14/01/2019 10:16
mli01	Flexível - 02_Controle de Surto - SP...	Sender:return-a1747-88986-89011-ro...	200 mensagem(ns)	1 mensagem(ns)	1%	14/01/2019 10:15
mli01	Flexível - 02_Controle de Surto - SP...	Sender:lais-amaral@r.todanet.net.br	200 mensagem(ns)	1 mensagem(ns)	1%	14/01/2019 10:10
mli01	Flexível - 02_Controle de Surto - SP...	Sender:bounces+1659945-b20e-neg...	200 mensagem(ns)	1 mensagem(ns)	1%	14/01/2019 10:08
mli01	Flexível - 02_Controle de Surto - SP...	Sender:mailinspector@trt9.jus.br	200 mensagem(ns)	6 mensagem(ns)	3%	14/01/2019 10:04
mli01	Flexível - 02_Controle de Surto - SP...	Sender:return@englink.engetron.com	200 mensagem(ns)	1 mensagem(ns)	1%	14/01/2019 10:02
mli01	Flexível - 02_Controle de Surto - SP...	Sender:retornos@todanet.net.br	200 mensagem(ns)	3 mensagem(ns)	2%	14/01/2019 10:00
mli01	Flexível - 02_Controle de Surto - SP...	Sender:retornos@filao.net.br	200 mensagem(ns)	13 mensagem(ns)	7%	14/01/2019 10:00
mli01	Flexível - 02_Controle de Surto - SP...	Sender:isabelaescobar@filao.net.br	200 mensagem(ns)	1 mensagem(ns)	1%	14/01/2019 10:00
mli01	Flexível - 02_Controle de Surto - SP...	Sender:juliano-andrade@nasas.net.br	200 mensagem(ns)	1 mensagem(ns)	1%	14/01/2019 10:00
mli01	Flexível - 02_Controle de Surto - SP...	Sender:retornos@nasas.net.br	200 mensagem(ns)	12 mensagem(ns)	6%	14/01/2019 10:00

Exemplo de Controle de Fluxo

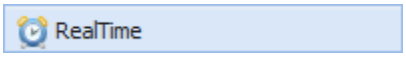
Greylist

A Greylist faz parte das camadas de filtragem do HSC MailInspector. Este filtro consiste em recusar temporariamente uma mensagem e esperar por sua retransmissão, e parte dos seguintes princípios:

- Que e-mails válidos são enviados a partir de MTAs legítimos, que mantém filas e possuem políticas de retransmissão em caso de erros temporários;
- Spammers e códigos maliciosos raramente usam MTAs legítimos.

Contudo, existem spammers que utilizam MTAs legítimos ou mesmo reenviam as mensagens a fim de contornar esta técnica. Ainda assim, o filtro aplicado pela Greylist é muito eficiente, impedindo que muitas mensagens enviadas por vírus, worms e spam zombies sejam recebidas pelo HSC MailInspector. Uma vez que o e-mail não é reenvido pelo servidor de origem, ele é classificado como SPAM e são tomadas as devidas ações sobre ele.

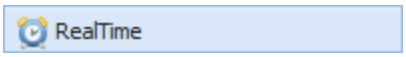
No MailInspector a configuração da GreyList é feita em:



/ Greylist

Aguardando Liberação

Use esta página para pesquisar, exibir ou executar ações nos registros das mensagens que foram temporariamente recusadas pelo MTA.



/ Greylist / Aguardando Liberação

O processo de liberação da Greylist é feito automaticamente pelo sistema, não sendo necessário nenhum processo de interação manual do administrador.

Visão geral dos servidores que estão aguardando liberação

O item Aguardando Liberação permite visualizar, filtrar e aplicar ações nos registros das mensagens que estão aguardando o tempo pré-determinado de auto liberação. Após este período, o sistema da Greylist remove o registro e cadastra este na whitelist de e-mails da greylist. O processo de liberação é automático e gerenciado pelo próprio HSC MailInspector, não sendo necessário a intervenção do administrador, porém caso o administrador queira certificar-se de uma liberação esta tela irá permitir tal ação.

Definições da tela de Greylist > Aguardando Liberação

Indicação das colunas apresentadas em Greylist > Aguardando Liberação.

Coluna	Definição
De	Remetente do e-mail
Domínio	Domínio do e-mail de origem
Para	Destinatário do e-mail
IP	IP de Origem do e-mail (pode ser IPv4 ou IPv6)
Recebido em	Data de entrada do e-mail

Definições de Opções - Aguardando Liberação

Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição
Pesquisar	Quando clicado, aplica o filtro informado na caixa de pesquisa rápida aos registros que estão aguardando o processo de auto liberação.
Limpar	Quando clicado, remove os filtros informados da caixa de pesquisa rápida e da janela de pesquisa avançada, e recarrega todos os registros de e-mails.
Pesquisa Avançada	Realiza uma pesquisa mais detalhada nos registros. Quando clicado, abre a caixa de diálogo **Pesquisa Avançada**.
Ações	Escolha entre: • **Liberar** - Permite liberar o recebimento da mensagem do registro selecionado, antecipando o processo de auto liberação. Ao realizar o processo de liberação, o registro será automaticamente cadastrado na Whitelist de E-mails da Greylist. • **Remover** - Remove o registro de tentativa de entrega da mensagem selecionado. Ao realizar o processo de remover, o servidor que tentou entregar a mensagem, será novamente cadastrado na Greylist, e começará novamente o processo de espera para auto liberação.

Definições de Opções - Pesquisa Avançada

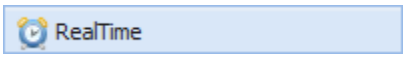
Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição
Aplicar	Quando clicado, aplica os filtros informados aos registros de mensagens que estão aguardando a auto liberação.
Limpar Campos	Quando clicado, remove os valores informados ou selecionados pelo usuário.

De	Informe o endereço completo ou parcial do remetente.
Para	Informe o endereço completo ou parcial do destinatário.
IP	Informe o endereço IP completo do servidor de origem (pode ser IPv4 ou IPv6).
Domínio	Informe o nome completo ou parcial do domínio do remetente.
Data Inicial	Permite definir uma data inicial para pesquisa.
Data Final	Permite definir uma data final para pesquisa.

Whitelist de E-mails (GreyList)

Use esta página para pesquisar, exibir ou executar ações nos registros das mensagens que foram liberadas e adicionadas a Whitelist de E-mails.



/ **Greylist / Whitelist de E-mails**

Visão geral da whitelist de e-mails

O item Whitelist de E-mails permite visualizar, filtrar e aplicar ações nos registros das mensagens que já passaram pelo processo de auto liberação da Greylist. Após receber dez mensagens do mesmo remetente, o sistema da Greylist cadastra o domínio e o servidor na whitelist de domínios, liberando assim todas as mensagens futuras originadas deste servidor sem gerar atraso no recebimento.

Definições de Opções - Whitelist de E-mails (Greylist)

Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição
Pesquisar	Quando clicado, aplica o filtro informado na caixa de pesquisa rápida aos registros que estão na whitelist de e-mails.
Limpar	Quando clicado, remove os filtros informados da caixa de pesquisa rápida e da janela de pesquisa avançada, e recarrega todos os registros de e-mails.
Pesquisa Avançada	Realiza uma pesquisa mais detalhada nos registros. Quando clicado, abre a caixa de diálogo **Pesquisa Avançada**.
Ações	Escolha entre: • **Adicionar** - Quando clicado, abre a caixa de diálogo **Cadastro da Whitelist de E-mails**. • **Remover** - Remove o registro selecionado da whitelist de e-mails.

Definições de Opções - Pesquisa Avançada

Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição
Aplicar	Quando clicado, aplica os filtros informados aos registros de mensagens que estão aguardando a auto liberação.
Limpar Campos	Quando clicado, remove os valores informados ou selecionados pelo usuário.
De	Informe o endereço completo ou parcial do remetente.
Domínio	Informe o nome completo ou parcial do domínio do remetente.
IP	Informe o endereço IP completo do servidor de origem (pode usar tanto IPv4, quanto IPv6).
Primeira Data	Escolha entre: • **Data Inicial** - Permite definir uma data inicial para pesquisa. • **Data Final** - Permite definir uma data final para pesquisa.
Última Data	Escolha entre: • **Data Inicial** - Permite definir uma data inicial para pesquisa. • **Data Final** - Permite definir uma data final para pesquisa.

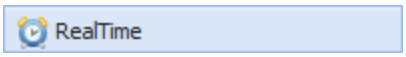
Definições de Opções - Cadastro da Whitelist de E-mails (Greylist)

Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição
Salvar	Quando clicado, grava as configurações realizadas.
Cancelar	Quando clicado, cancela a ação.
De	Informe somente o nome do remetente.
Domínio	Informe somente o domínio do remetente (sem o símbolo de arroba @).
IP	Informe o endereço IP do servidor do remetente (pode ser IPv4 ou IPv6).

Whitelist de Domínios (GreyList)

Use esta página para pesquisar, exibir ou executar ações nos registros das mensagens da Whitelist de Domínios.



/ Greylist / Whitelist de Domínios

Visão geral da whitelist de domínios

O item Whitelist de Domínios permite visualizar, filtrar e aplicar ações nos registros das mensagens da Whitelist de Domínios.

Definições de Opções - Whitelist de Domínios (Greylist)

Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição
Pesquisar	Quando clicado, aplica o filtro informado na caixa de pesquisa rápida aos registros que estão na whitelist de domínios.
Limpar	Quando clicado, remove os filtros informados da caixa de pesquisa rápida e da janela de pesquisa avançada, e recarrega todos os registros de e-mails.
Pesquisa Avançada	Realiza uma pesquisa mais detalhada nos registros. Quando clicado, abre a caixa de diálogo **Pesquisa Avançada**.
Ações	Escolha entre: • **Adicionar** - Quando clicado, abre a caixa de diálogo **Cadastro da Whitelist de Domínios**. • **Remover** - Remove o registro selecionado da whitelist de e-mails.

Definições de Opções - Pesquisa Avançada

Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição
Aplicar	Quando clicado, aplica os filtros informados aos registros de mensagens que estão aguardando a auto liberação.
Limpar Campos	Quando clicado, remove os valores informados ou selecionados pelo usuário.
Domínio	Informe o nome completo ou parcial do domínio do remetente.
IP	Informe o endereço IP completo do servidor de origem (pode ser IPv4 ou IPv6).
Primeira Data	Escolha entre: • **Data Inicial** - Permite definir uma data inicial para pesquisa. • **Data Final** - Permite definir uma data final para pesquisa.
Última Data	Escolha entre: • **Data Inicial** - Permite definir uma data inicial para pesquisa. • **Data Final** - Permite definir uma data final para pesquisa.

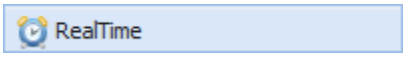
Definições de Opções - Cadastro da Whitelist de Domínios (Greylist)

Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição
Salvar	Quando clicado, grava as configurações realizadas.
Cancelar	Quando clicado, cancela a ação.
Domínio	Informe somente o domínio do remetente (sem o símbolo de arroba @).
IP	Informe o endereço IP do servidor do remetente (pode ser Ipv4 ou IPv6).

Status

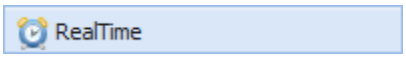
Use esta página visualizar as estatísticas de funcionamento do HSC MailInspector



/ Status

Performance do Sistema

Analisa a performance do seu appliance físico ou virtual do HSC MailInspector.



/ Status /Performance do Sistema

Este Dashboard traz estatísticas de perfomance e status atuais do HSC MailInspector.

Visão geral da Performance do Sistema

O Dashboard de Performance do sistema permite ao administrador visualizar estatísticas de performance e status do HSC MailInspector bem como os principais logs eventos do sistema. Podendo o administrador ainda configurar alertas por e-mail de acordo com a criticidade e para qual e-mail destino será enviado o alerta.

Definições de Opções - Botão de Template Claro/Escuro

Selecione o modelo de template para a apresentação dos dados.

Opções	Definição
Claro	Quando selecionado, mostra a tela utilizando o template no modelo padrão (claro).
Escuro	Quando selecionado, mostra a tela usando o template escuro.

Definições de Opções - Botão Opções de Alerta

Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição
Salvar	Quando clicado, grava as configurações realizadas.
Cancelar	Quando clicado, cancela a ação.
Opções de Alerta **Enviar Alerta Via**	Selecione o tipo de envio de Alerta: • **Desativado:** Não envia alerta algum • **E-mail:** Envia alerta através de e-mail cadastrado. Ao ativar esta opção, é liberado o campo E-mail, ao qual pode ser cadastrado o e-mail para envio dos alertas (vide Itens Monitorados). ○ **E-mail:** Quando selecionado E-mail. Informe o endereço de e-mail que recebera os alertas

	• **SNMP TRAP:** Envia alerta através do protocolo Simple Network Manage Protocol. Ao selecionar esta opção, é liberado o cadastro do Host para envio, bem como a Community, para cadastro da comunidade utilizado pelo SNMP Trap.
	  ○ **Host:** Quando selecionado SNMP TRAP, definir o Host de destino
	  ○ **Community:** Quando selecionado SNMP TRAP, definir a community

Itens Monitorados	Selecione aqui quais itens serão monitorados e serão alertados em caso de falha: • **Espaço em Disco:** Baixo espaço em disco, separado por áreas distintas; Por padrão o sistema alerta quando ocorre consumo de disco maior que 80% da capacidade máxima. • **Filas de E-mails:** Tamanho da fila de e-mails, com indicação de quantidade de e-mails parados; Por padrão o sistema alerta quando a fila de e-mails fica com quantidade maior que 300 e-mails "parados". • **Memória:** Consumo de memória; Por padrão o sistema alerta quando ocorre overflow de memória e gera swap de disco com capacidade maior que 30%. • **Processador:** Grande consumo de processamento (enfileiramento de processo / Carga de LOAD); Por padrão o sistema alerta ocorre quando o consumo de load de processamento ultrapassa a 3 vezes o padrão. • **Serviços de Filtragem:** Incluindo consultas de reputação; Gerado alerta quando o MailInspector não consegue se comunicar com o sistema de reputação e filtragem em nuvem. • **Atualização do Sistema de Segurança**: Verifica se houve falha na atualização de assinaturas de sistema de segurança; São gerados alertas quando o sistema fica mais de 48 horas sem atualização. **Antivírus e AntiSPAM:** Com indicação da última versão de download, bem como a data e também com a informação da última tentativa de download da vacina; São gerados alertas quando o sistema fica mais de 48 horas sem atualização do antivírus. • **Ponto de Acesso indisponível:** Verifica a disponibilidade de pontos de filtragem, bem como do cluster em si; São gerados alertas quando ocorre perda de 99% dos pacotes. • **Sincronização dos Conectores Externos:** Verifica falha de sincronização com LDAP/AD/Zimbra; São gerados alertas quando ocorre falha na sincronização. • **Eventos críticos do sistema:** Detecção e alerta de outros dados críticos;

Definições das Sessões de Informações

Appliance MailInspector

Estas informações descrevem as informações disponíveis nesta sessão.

Item	Definição
Licenciado para	Informações sobre a licença do produto e tempo de expiração
Sistema	Informações sobre plataforma do sistema.
Processador	Informações sobre modelo do processador

Memória / Swap	Informações sobre tamanho da memória física e Swap
Disco	Informações sobre o tamanho do HD.

Serviços

Indica os status dos serviços do MailInspector.

Item	Definição
Controle de Bounce	Informa se a daemon do Controle de Bounce está rodando.
DKIM/Domain Key	Informa se a daemon do DomainKey Signature está rodando.
Cache em Memoria	Informa se a daemon do Sistema de Cache em Memória está rodando.
Reputação de E-mails	Informa se a daemon do Sistema de Reputação de Mensagens está rodando.
Logs do MTA	Informa se a daemon do Logs do MTA está rodando (HSC Logger).
DLP Fingerprint	Informa se a daemon do Sistema DLP para identificação de Fingerprint está rodando.
DLP Attachment	Informa se a daemon do Sistema DLP de varredura de anexos está rodando.
Controle de Conexão	Informa se a daemon do Controle de Conexões está rodando.
MTA	Informa se a daemon do MTA está rodando.
Antivirus ESET LiveGrid	Informa se a daemon do Sistema de Antivírus está rodando (segunda opção de antivírus).
ESET LIveGrid Update (Antivirus Atualização)	Informa se a daemon do Sistema de Update (atualização) do Antivírus está rodando (segunda opção de antivírus).
SmartDefender	Informa se a daemon do Sistema SmartDefender está rodando.

Carga do sistema (Performance da CPU)

Indica o consumo do CPU.

Item	Definição
Load 1min	Informações sobre uso de CPU no último minuto
Load 5min	Informações sobre uso de CPU nos últimos 5 minutos
Load 15min	Informações sobre uso de CPU nos últimos 15 minutos
Swap	Informações sobre uso de Memória Swap

Discos

Contém informações do uso do espaço de cada partição do sistema.

Item	Definição
/	Consumo de disco da área /
/opt	Consumo de disco da área /opt

/var	Consumo de disco da área /var
/var/spool/MailScanner/incoming	Consumo de disco da área /var/spool/MailScanner/incoming
/tmp/dlp	Consumo de disco da área /tmp/dlp

Fila de E-mails

Contém informações dos e-mail que estão na fila de processamento do ponto de filtragem ou cluster selecionado.

Saúde do Banco de Dados

Apresenta informação sobre o status do Banco de Dados dos registros de e-mails do HSC MailInspector.

Total de Mensagens

Apresenta o total de mensagens processadas pelo ponto ou Cluster selecionado.

Volume de Mensagens

Apresenta em tamanho (MB/GB) o volume de mensagens processadas pelo ponto ou Cluster selecionado.

HSC SmartDefender

Apresenta a data da última comunicação com a nuvem da HSCBRASIL.

Antivírus

Apresenta os dados da atualização do antivírus.

Item	Definição
Data da última atualização	Indicação em formato dd/mm/aaaa hh:mm Apresenta-se a data e hora da última atualização de vacinas
Última Tentativa de Update	Indicação em formato dd/mm/aaaa hh:mm Apresenta-se a data e hora da última TENTATIVA de atualização de vacinas

Global Threat Protection Network (SmartDefender)

Apresenta informação sobre a data de última atualização das assinaturas de segurança do HSC MailInspector. Assinaturas tais como: Anti Phishing, Reputação de IPS e URL, SPAM (Heurística, Imagem, Filtros, etc.) e demais componentes do Global Threat Protection Network (SmartDefender).

Coletor de Dados

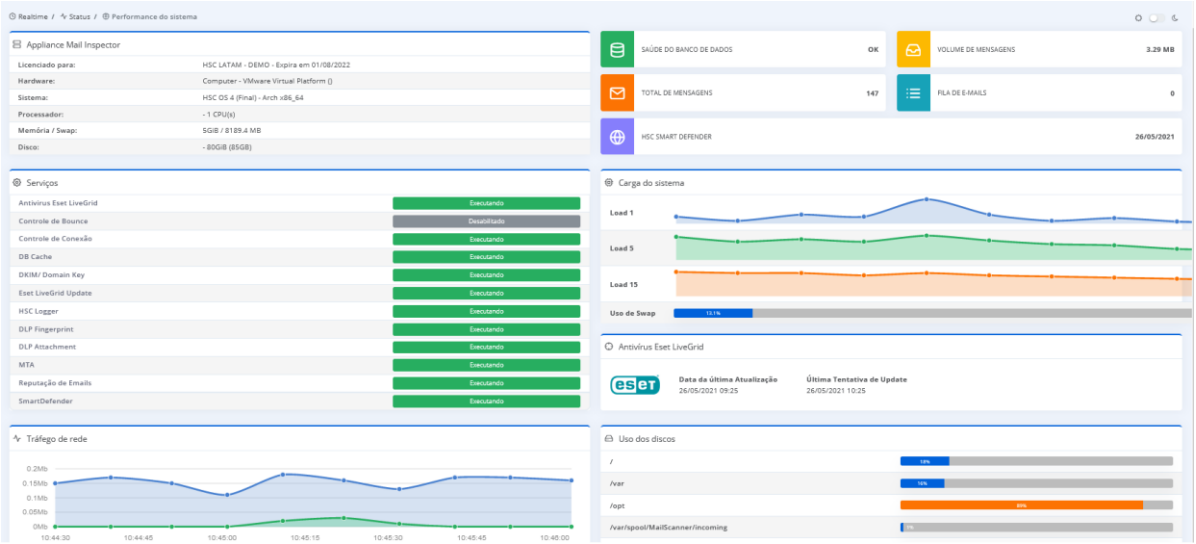
Apresenta informação sobre o status da última coleta de dados (esta função somente é ativada quando o sistema de dados do cluster estiver configurado como distribuído).

Tráfego de Rede

Gráfico em tempo real do consumo de rede (download e upload) e suas configurações.

Item	Definição
Download	Volume de dados recebidos por e-mails.
Upload	Voluma de dados enviados através de e-mails.

Somente irá apresentar valores quando a coleta e o arquivamento ("Ponto Histórico") estiver ativado

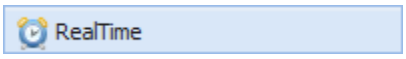


Exemplo de Tela de Performance do Sistema no template Claro

Exemplo de Tela de Performance do Sistema no template Escuro

Painel de Controle

No Painel de Controle é possível verificar os status dos serviços e determinar alguma ação sobre ele.



/ Status / Painel de Controle

Visão geral Status Painel de Controle

Nesta tela o administrador poderá ver o Status de cada serviço da solução MailInspector rodando tanto nos pontos de acesso como na console de administração. Esta tela também permite ao administrador executar em quaisquer serviços as seguintes ações:

- Parar;
- Iniciar;
- Reiniciar.

Lista de Serviços

Opções	Definição
Antivírus	Serviço responsável pelo sistema de filtragem de Vírus e demais ameaças
Controle de Bounce	Serviço responsável pelo sistema de Bounce Address Tag Verification
DB Cache	Serviço responsável pelo sistema de Cache de consultas
DB LOG	Serviço responsável pelo sistema de Armazenamento dos dados "Banco de Dados" de Logs, Relatórios e Quarentena
DLP	Serviço responsável pelo sistema de Data Loss Prevention
DKIM	Serviço responsável pelo sistema de DKIM
DMARC	Serviço responsável pelo sistema de DMARC
HTTP/s	Serviço responsável pelo sistema de Console de Administração da ferramenta, Interface de Gestão para Usuário, Interface de gestão de Criptografia, Interface de Gestão de Relatórios, Interface de Gestão da Quarentena e Interface de Gestão de Pesquisas
Logger	Serviço responsável pelo sistema de Log
MTA	Serviço responsável pelo sistema de Envio e Recebimento de e-mails "SMTP" e filas
MailInspector	Serviço responsável pelo sistema de Filtragem de E-mails e seus módulos, tais como: • Filtro de Conteúdo; • Criptografia; • AntiSpam; • Anti Phishing; • Targeted Attack Protection e etc.
MailSplit	Serviço responsável pelo sistema de Divisão de Destinatários de E-mail
Message Reputation	Serviço responsável pelo sistema de Análise de Reputação de Mensagens
Milter	Serviço responsável pelo sistema de Filtros da Camada MTA
Controle de Fluxo	Serviço responsável pelo sistema de Controle de Fluxo e Anti DOS/DDOS
SNMP	Serviço responsável pelo sistema de monitoramento SNMP
SmartDefender	Serviço responsável pelo sistema de Análise de ameaças em tempo real
SSH	Serviço responsável pela disponibilização de conexão pelo protocolo SSH

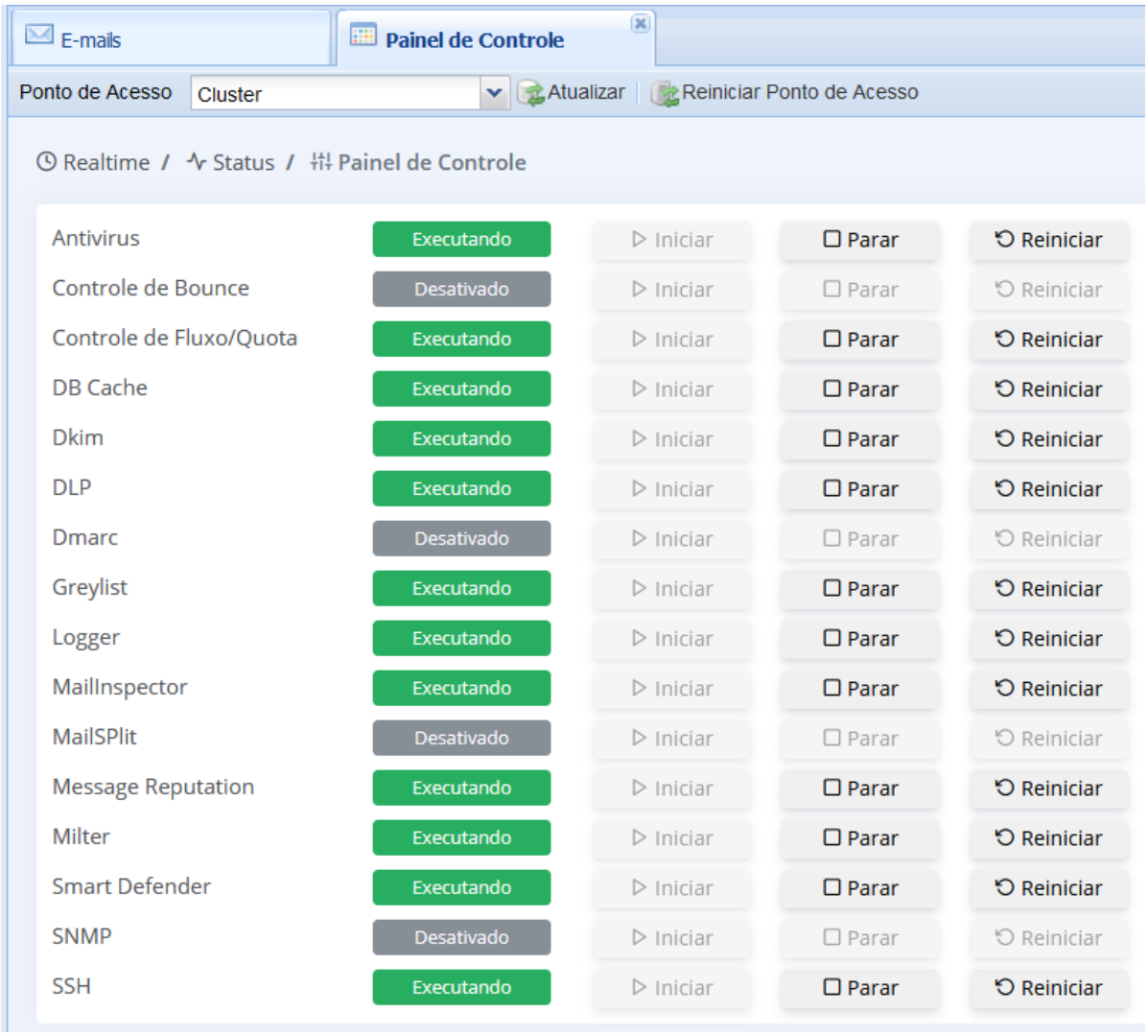
Definições de Opções

Seguem as definições sobre Controle dos Serviços no MailInspector, permitindo ao administrador efetuar as ações dos mesmos, sem necessidade de instruções via linha de comando (CLI).

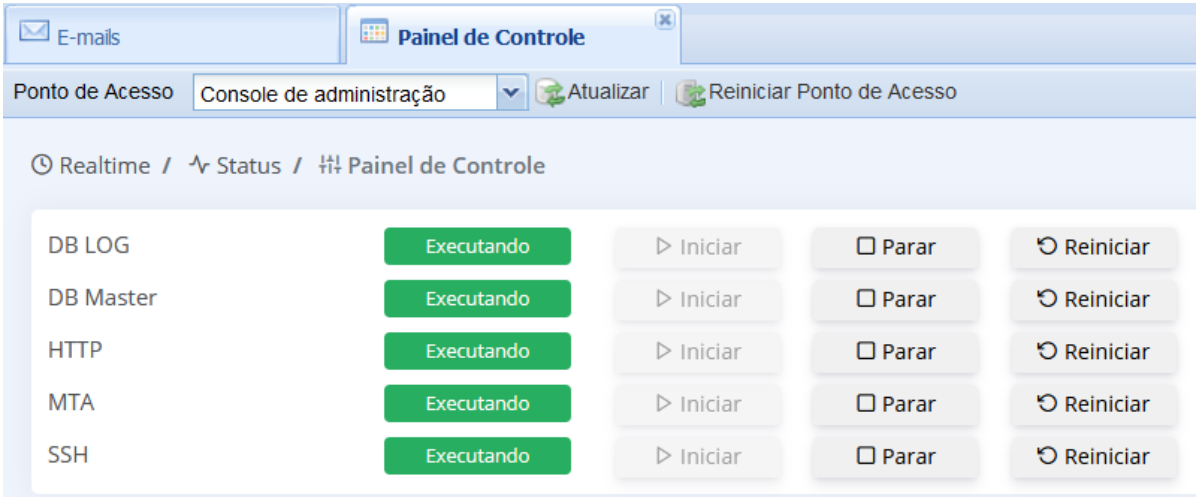
Opções	Definição
Ponto de Acesso	Seleciona o ponto de acesso/interface de gerenciamento para seleção de serviços
Atualizar	Atualiza a tela com os dados carregados
ANTIVÍRUS	Inicia o status do serviço de Antivírus, bem como as opções de suporte ao serviço: • Iniciar; • Parar; • Reiniciar;
CONTROLE DE BOUNCE	Inicia o status do serviço de Controle de Bounce, bem como as opções de suporte ao serviço: • Iniciar; • Parar; • Reiniciar;
CONTROLE DE FLUXO/QUOTA	Inicia o status do serviço de Controle de Fluxo/Quota, bem como as opções de suporte ao serviço: • Iniciar; • Parar; • Reiniciar;
DB CACHE	Inicia o status do serviço do Cache do Banco de Dados, bem como as opções de suporte ao serviço: • Iniciar; • Parar; • Reiniciar;
DKIM	Inicia o status do serviço de DKIM, bem como as opções de suporte ao serviço: • Iniciar; • Parar; • Reiniciar;
DLP	Inicia o status do serviço de DLP, bem como as opções de suporte ao serviço: • Iniciar; • Parar; • Reiniciar;
DMARC	Inicia o status do serviço de DMARC, bem como as opções de suporte ao serviço: • Iniciar; • Parar; • Reiniciar;
LOGGER	Inicia o status do serviço de quarentena, bem como as opções de suporte ao serviço: • Iniciar; • Parar; • Reiniciar;

MAILINSPECTOR	Inicia o status do serviço de MailInspector (interface de gerenciamento), bem como as opções de suporte ao serviço: • Iniciar; • Parar; • Reiniciar;
MAILSPLIT	Inicia o status do serviço de MailSplit (duplicação de e-mails, para análise individual de spam), bem como as opções de suporte ao serviço: • Iniciar; • Parar; • Reiniciar;
MESSAGE REPUTATION	Inicia o status do serviço de Messager Reputation (serviço de reputação dde e-mail), bem como as opções de suporte ao serviço: • Iniciar; • Parar; • Reiniciar;
MILTER	Inicia o status do serviço de Milter, bem como as opções de suporte ao serviço: • Iniciar; • Parar; • Reiniciar;
SMARTDEFENDER	Inicia o status do serviço de SmartDefender, bem como as opções de suporte ao serviço: • Iniciar; • Parar; • Reiniciar;
SMNP	Inicia o status do serviço de SNMP (Simple Network Manager Protocol), bem como as opções de suporte ao serviço: • Iniciar; • Parar; • Reiniciar;
DB LOG	Inicia o status do serviço de pesquisa avançada, bem como as opções de suporte ao serviço: • Iniciar; • Parar; • Reiniciar;
DB MASTER	Inicia o status do serviço de banco de dados, bem como as opções de suporte ao serviço: • Iniciar; • Parar; • Reiniciar;
HTTP	Inicia o status do serviço de interface web, bem como as opções de suporte ao serviço: • Iniciar; • Parar; • Reiniciar;
MTA	Inicia o status do serviço MTA, bem como as opções de suporte ao serviço: • Iniciar; • Parar; • Reiniciar;

SSH	Inicia o status do serviço SSH, bem como as opções de suporte ao serviço: • Iniciar; • Parar; • Reiniciar;



Exemplo de Tela de Painel de controle



Exemplo de Tela de Painel de controle

É possível reinicializar os pontos de filtragem (pontos de acesso), diretamente na interface gráfica, sem necessidade de linha de comando.

Para esse procedimento, basta selecionar o ponto de acesso e clicar em Reiniciar Ponto de Acesso.

Exemplo de Tela de Reinício de Ponto de Acesso

Segurança

RealTime / **Segurança**

SandBox

RealTime / **Segurança / SandBox**

Visão geral do SandBox

Nesta tela o administrador pode ver em tempo real todas ações e detecções ocorridas pelos modulo de segurança avançada. Em formato de uma Linha de tempo, é possível ver em tempo real, todas ameaças detectadas e todas as ações que foram tomadas em cima dela, podendo o administrador acompanhar e rastrear todas as ameaças.

Neste dashboard ficam registrados todas URLs e Arquivos presente nos e-mails, bem como todos os níveis de detecção incluindo a iteração dos usuários através do modulo de Ataque Dirigido "Reescrita de E-mail e Anexos".

Aqui você pode acompanhar o Histórico de um URL e Arquivo e verificar os detalhes de todos os processos de análise do HSC MailInspector, desde o recebimento, processamento, identificação, envio para SandBox, ações dos usuários e reporte dos usuários, contabilizando quantos clicks e quais tipos de ações foram tomadas. Por padrão o MailInspector permite o rastreamento de cliques pelo prazo definido pelo administrador em *Definições de Opções - Controle da Quarentena* que por padrão são 30 dias.

Quando ativado, o sistema de SandBox File, remove o anexo da mensagem que podem ser possivelmente perigosos e efetua a análise localmente (SandBox Estático), em uma segunda etapa, é feita a análise dinâmica, podendo ser local OU na nuvem da HSCBRASIL.

Se optado por análise local, todo o processo é efetuado no appliance indicado pelo administrador, com opção de envio da amostra para HSCBRASIL para a análise. Se for optado pela análise em nuvem o arquivo é enviado para o SandBox da HSCBRASIL para efetuar outros processos de análise e comparar com resultados de arquivos já analisados, para busca de similaridade. Em ambas as opções são efetuadas todas as análises comportamentais do anexo. A única diferença é que se for optado pelo uso local, será consumido mais processamento e memória do equipamento utilizado, já na opção de uso da nuvem da HSCBRASIL, não há essa carga “extra” de processamento e consumo de memória.

O SandBox também indica se houve tentativa de evasão pelo arquivo ou link executado. O SandBox efetua a coleta automática das amostras e registra-se o hash/Fuzzy hash dos artefatos analisados, ficando registrado somente os dados dos resultados da análise, descartando o artefato em si.

O SandBox em nuvem da HSCBRASIL possui capacidade de análise de mais de 100.000 arquivos por mês, dessa forma garantindo desempenho e confiabilidade, pois o mesmo é formado por cluster distribuído em dois datacenters distintos, fisicamente separados.

Caso o administrador opte por utilizar a nuvem do HSCBRASIL para a análise do arquivo, ou optado por envio da amostra (mesmo quando o SandBox estiver configurado para uso local), o mesmo é enviado de forma anônima para análise, uma vez analisada, ela é descartada, mantendo-se somente o registro dos metadados

(que não são identificáveis), dessa forma fica de acordo com a Lei Geral de Proteção de Dados Pessoais, uma vez que é dado sensível para **prevenção à fraude e à segurança da pessoa**.

> Conforme o Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses:
>
> > g) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.

Obs: A configuração da forma de uso do SandBox fica em Configurações > Controle de Ameaças > Ataque Dirigido

> Os registros de cliques dos usuários nas URL's contidas nos e-mails, bem como o resultado de análise dos anexos clicados, ficam registrados no Banco de Dados local (onde a solução está instalada).

Definições de Opções - SandBox

Estas informações descrevem as opções disponíveis nesta página.

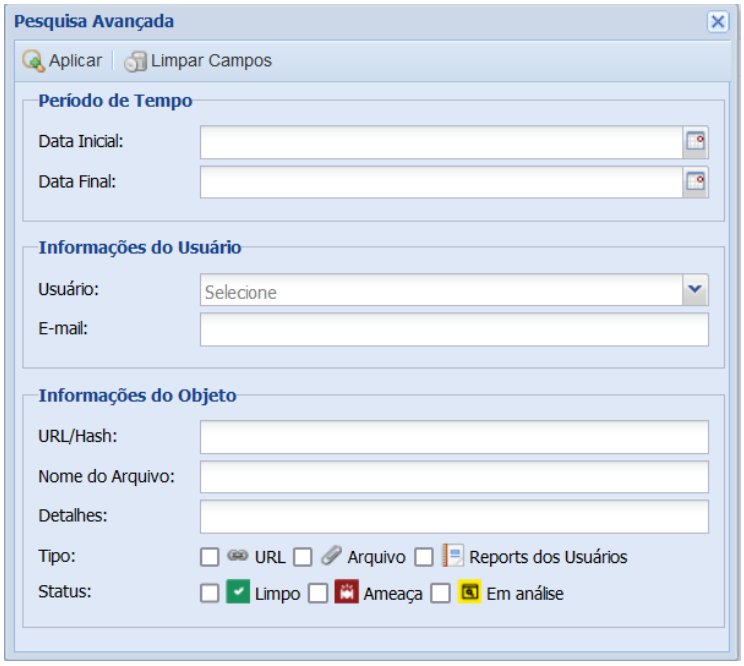
Opções	Definição
Pesquisar	Quando clicado, aplica o filtro informado na caixa de pesquisa rápida as mensagens, sendo possível pesquisa por URL ou HASH.
Limpar	Quando clicado, remove os filtros informados da caixa de pesquisa rápida e da janela de pesquisa avançada, e recarrega todos os registros.
Pesquisa Avançada	Realiza uma pesquisa mais detalhada nos registros. Quando clicado, abre a caixa de diálogo **Pesquisa Avançada**.
Exportar	Exporta todos os detalhes selecionados para um formato CSV.
Checkbox URL	Ao selecionar, realiza um filtro imediato de objetos do tipo URL.
Checkbox Arquivo	Ao selecionar, realiza um filtro imediato de objetos do tipo Arquivo.
Checkbox Reports dos Usuários	Ao selecionar, realiza um filtro imediato de objetos do tipo que contém interação de resposta do usuário.

Definições de Opções - Pesquisa Avançada

A pesquisa avançada é utilizada para buscas de ações sobre URL's/Arquivos/Staus analisados pelo SandBox, dessa forma retornando a indicação de timeline de quem, quando e qual a URL/Arquivo que foi acionado ao clique.

Opções	Definição
Aplicar	Quando clicado, aplica os filtros informados e/ou selecionados as mensagens filtradas pelo HSC MailInspector.
Limpar Campos	Quando clicado, remove os valores informados ou selecionados pelo usuário.

Data Inicial	Permite definir uma data inicial para pesquisa.
Data Final	Permite definir uma data final para pesquisa.
Usuário	Permite definir a busca filtrando por um usuário específico.
E-mail	Permite definir a busca filtrando por um e-mail específico.
URL / HASH	Permite efetuar a filtragem pelo URL ou HASH da mensagem para a busca. Se a filtragem for por HASH, o padrão aceito é SHA-1 e SHA-256.
Nome do Arquivo	Ativa o filtro pelo nome de um arquivo específico.
Detalhes	Informe os detalhes, se existir, para a busca.
Tipo	Informe o tipo, dentre eles: • URL; • Arquivo; • Reports dos usuários.
Status	Informe o status de classificação, dentre eles: • Limpo; • Ameaça; • Em análise.



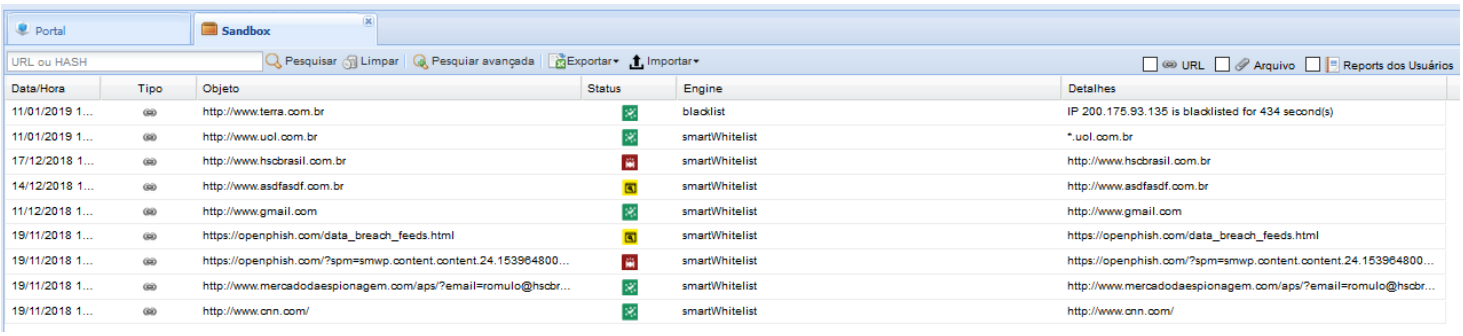
Tela de Pesquisa Avançada no SandBox

Painel do SandBox

Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição
Data/Hora	Informa a data/hora da detecção da URL/anexo

Tipo	URL ou Arquivo
Objeto	URL ou Hash do arquivo
Status	Podendo ser: • Limpo; • Ameaça; • Em análise;
Nome do arquivo	Se for arquivo analisado, este campo indica o nome do arquivo.
Engine	Indica qual a metodologia que foi utilizada sobre o SandBox, bem como indicadores IOC's
Detalhes	Detalhes da detecção, informando tipo de ameaças e as mensagens que foram identificadas. Aqui serão informados qual mecanismo foi ativado para detecção da ameaça, ex: URL SandBox, Phishing, Spear Phishing, Block List, Malware, Malicious Website, Malicious Content, etc.
Total de URLs Reescritas	Localizado na barra inferior este totalizador informa quantas URLs foram reescritas pela ferramenta.
Total de URLs Bloqueadas	Localizado na barra inferior este totalizador informa quantas URLs foram bloqueadas pela ferramenta.
Total de URLs Limpas	Localizado na barra inferior este totalizador informa quantas URLs foram analisadas e nenhuma ameaça foi encontrada.
Total de URLs Enviadas para SandBox	Localizado na barra inferior este totalizador informa quantas URLs foram enviada para análise na nuvem da HSC SmartDefender



Exemplo de Tela de SandBox

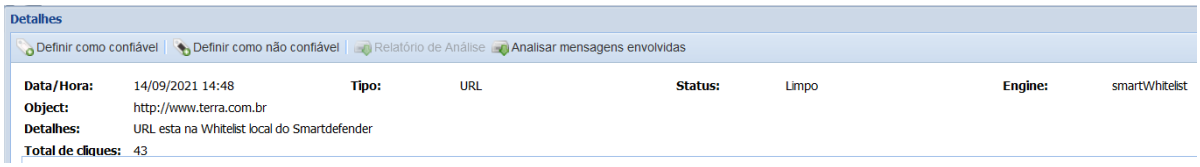
Painel de Detalhes do SandBox

É possível visualizar todos os registros efetuados no SandBox, indicando qual o status de cada um deles.

Ao efetuar duplo clique sobre um registro, é apresentado a TimeLine do registro. Nessa TimeLine, são apresentados os seguintes dados:

Opções	Definição
Definir como confiável	Marca a URL/arquivo ou IP como confiável, incluindo-o em uma whitelist local, que sobrepõe ao resultado da análise do SmartDefender.

Definir como não confiável	Marca a URL/arquivo ou IP como não confiável, incluindo-o em uma block list local, que sobrepõe ao resultado da análise do SmartDefender.
Analisar mensagens envolvidas	Apresenta os e-mails envolvidos com o filtro ativo.
Data/Hora	Data/Hora da chegada do objeto para análise.
Tipo	Tipo de artefato analisado no SandBox: • URL; • Arquivo;
Objeto	URL ou Hash do arquivo
Status	Podendo ser: • Limpo; • Ameaça; • Em análise;
Engine	Qual engine utilizado para rastrear o objeto (engine de URL, engine de para arquivos e/ou engine para rastrear IP's); Se for arquivo: • Mime-Type do arquivo (caso seja um arquivo); • Extensão (caso seja arquivo); • Nome do arquivo;
Detalhes	Detalhes específicos da URL/anexo;
Total de Cliques	Indica quantos cliques foram efetuados sobre a URL;



Exemplo de Tela de Detalhes de arquivo analisado no SandBox

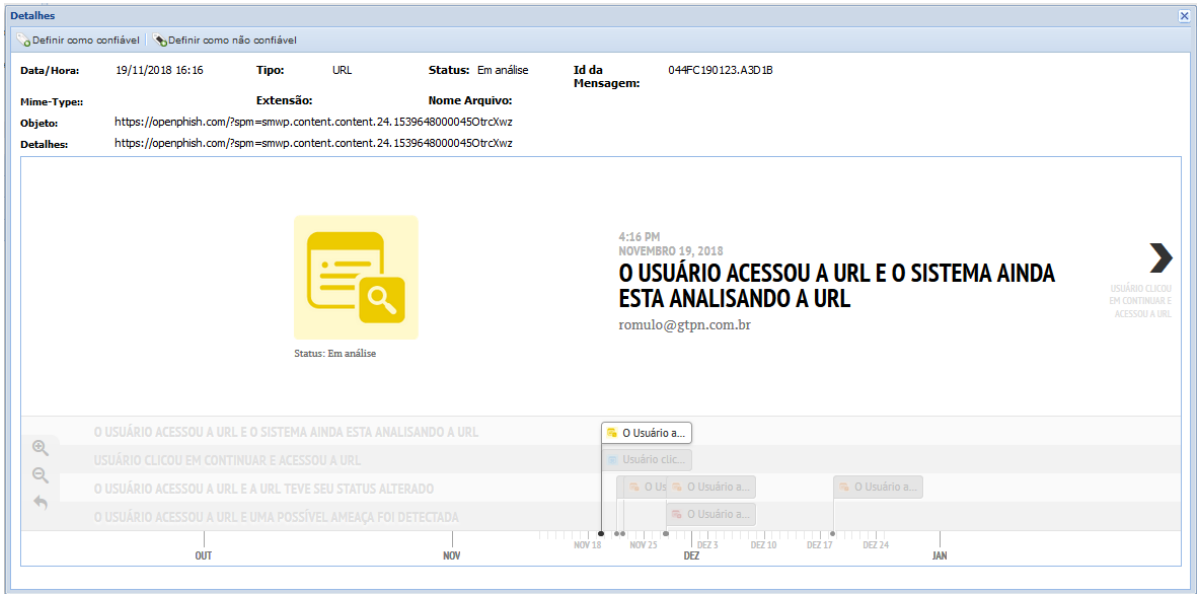
Também é apresentada ainda a informação sobre ação tomada por um usuário específico sobre a URL/arquivo, indicando a data e hora da ação tomada.

A apresentação da Timeline, indica a ação de cada um usuário sobre o link. Isso é possível, porque o MailInspector efetua a divisão do envelope do e-mail, de modo que exista apenas um receptor atrelado a uma URL reescrita, permitindo dessa forma que o administrador possa saber quais usuários clicaram na mesma URL, contabilizando de forma individual as tentativas de clique. Também com siso, é possível saber quais usuários tentaram ignorar o bloqueio de uma URL, com a mesma lógica de contabilização individual.

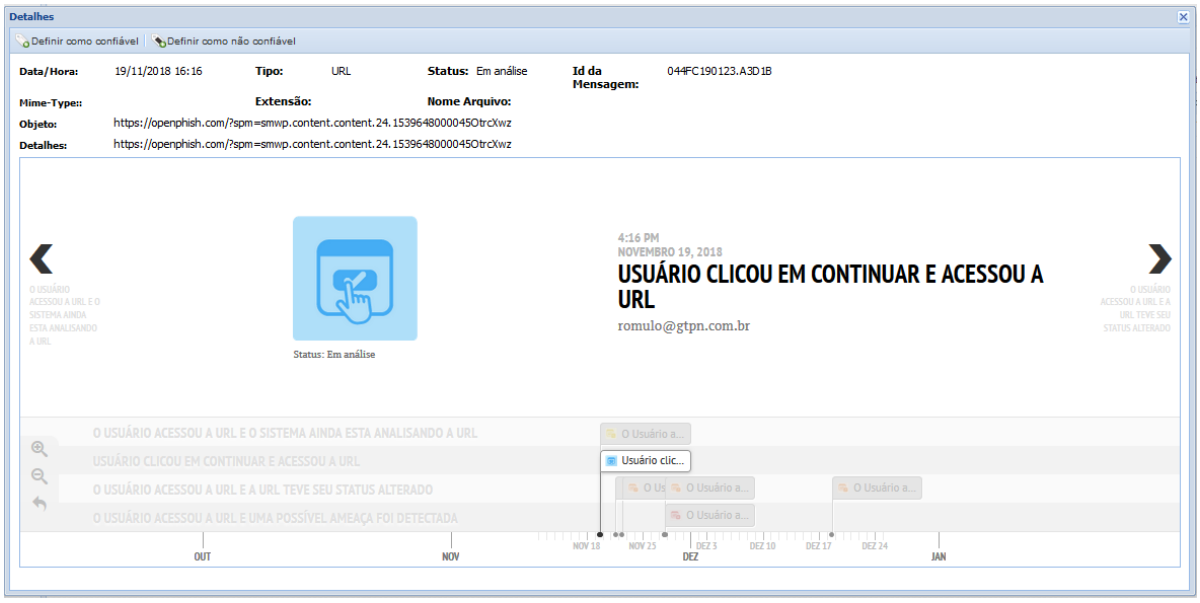
No acompanhamento da Timeline, é possível verificar o total de cliques efetuado pelo usuário com resultado como link válido e total de cliques efetuado pelo usuário como link inválido/malicioso.

Ao clicar duas vezes sobre um arquivo o administrador poderá visualizar maiores detalhes como: Data/Hora, Hash do Arquivo "SHA1", Nome do arquivo, Tamanho, STATUS, Mensagens que tiveram este arquivo anexado podendo ainda decidir se considera a mensagem como confiável ou definir como não confiável. Também irá

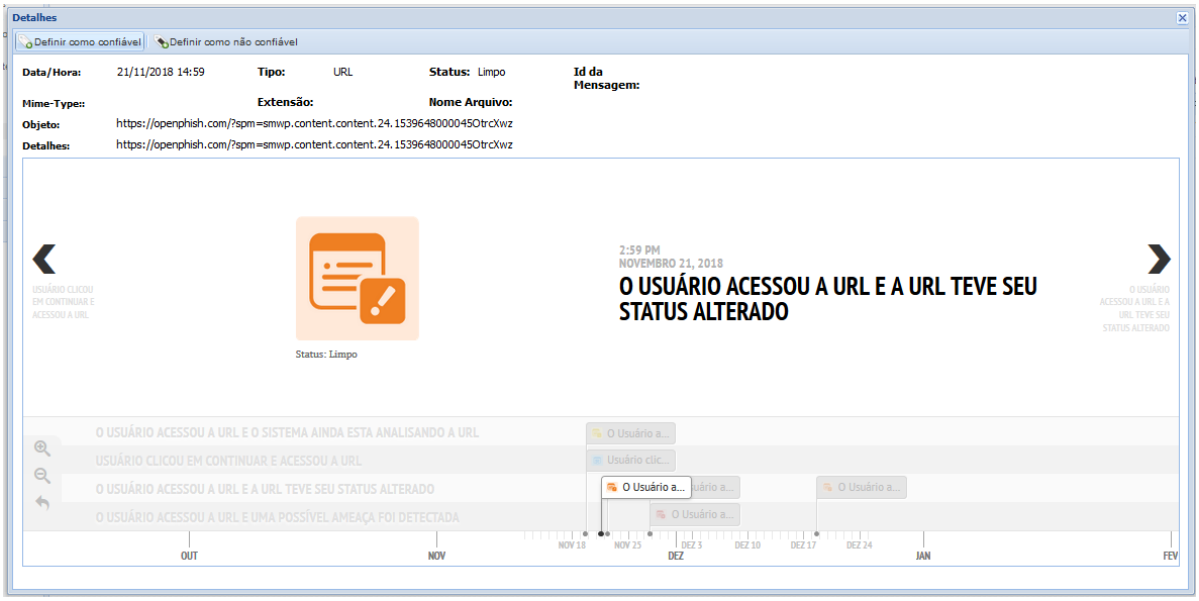
apresentar um Linha de tempo detalhando de modo gráfico e intuitivo todas as ações que a ferramenta teve com cada URL e Arquivo processado. Detalhando quantos clicks um URL teve, quais usuários acessaram e quais ações foram tomadas. Essa visualização é em formato de TimeLine, facilitando o acompanhamento e análise por parte do administrador da solução.



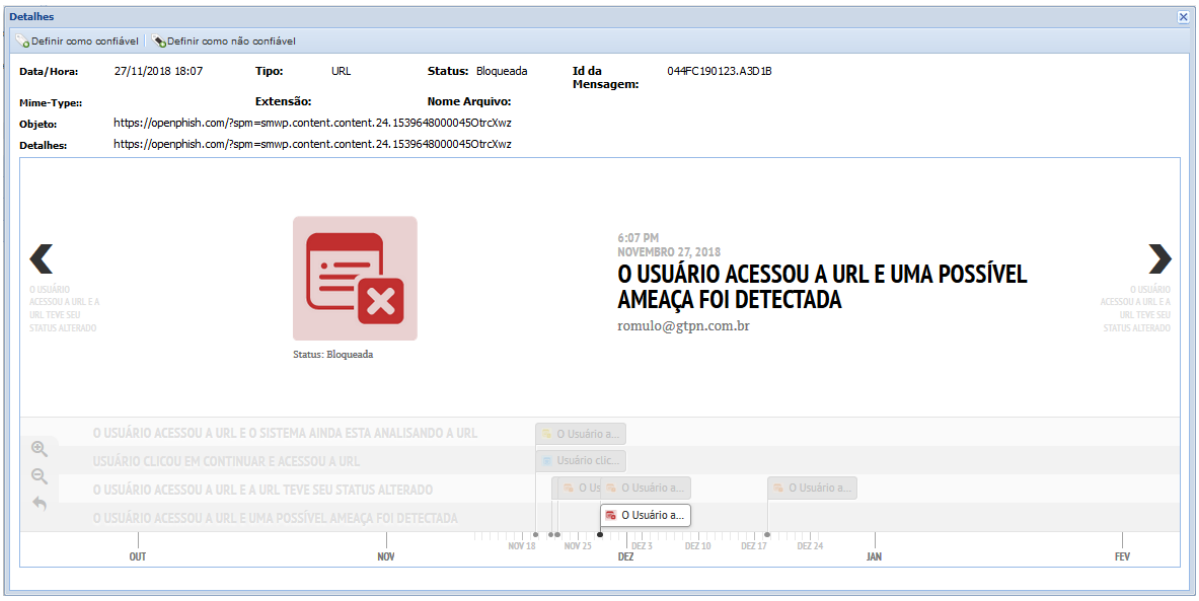
Timeline



Timeline



Timeline



Timeline

Todas as opções apresentadas em relação ao SandBox, também está disponível para o usuário final.

Ameaças

RealTime / **Segurança / Ameaças**

Visão geral das Ameaças

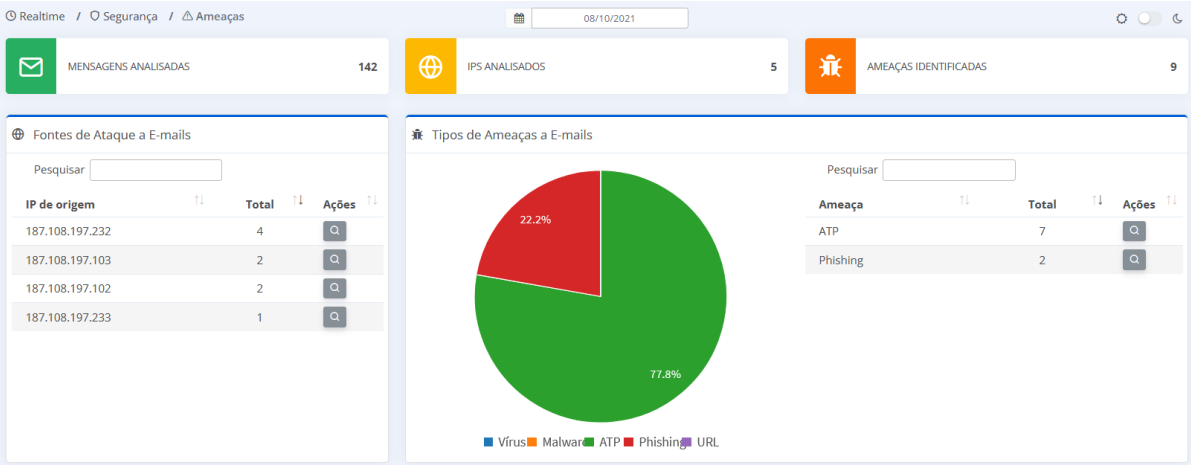
Este dashboard permite ao administrador ter um resumo em tempo real das principais ameaças que foram identificadas por todo o sistema, bem como o rastreamento delas.

À partir da ameaça, é possível separar os e-mails afetados, bem como o rastreamento da origem da ameaça selecionada (geolocalização através de DNS reverso).

A tela tem funcionalidade de Drill Down View que permite ao administrador clicar para obter mais informações sobre uma determinada ameaça e fontes de ameaça e quais usuários foram ou seriam impactados.

Neste módulo é possível correlacionar múltiplos e-mails maliciosos, agrupando-os por tipo de ataque, dessa forma, independente de quem esteja recebendo o ataque, é possível associar múltiplos e-mails a um único incidente/agressor.

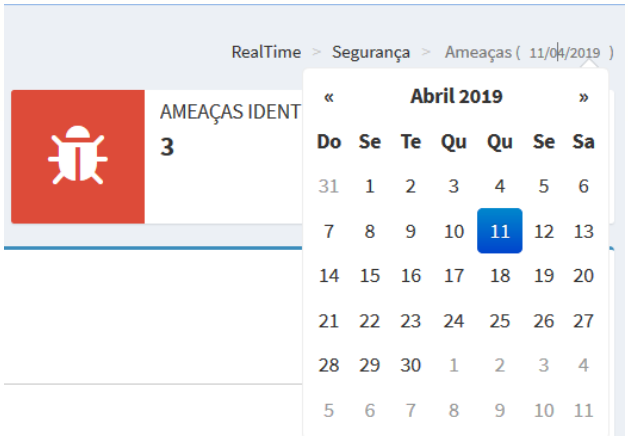
Associando o módulo de Ameaças através de ações para filtragem específico das ameaças encontradas, junto ao sistema de Inteligência Artificial (HSC AI Cyber Assistant - *Sistema Generativa (IA) para Análise de E-mails Bloqueados*), o MailInspector recomenda a ação a ser tomada pelo administrador/usuário.



Dashboard de ameaças

Definições de Opções – Ameaças

É possível selecionar a data das ameaças encontradas.
Para isso, clique no canto direito superior, onde aparece a data indicada das ameaças e mude para a data desejada.

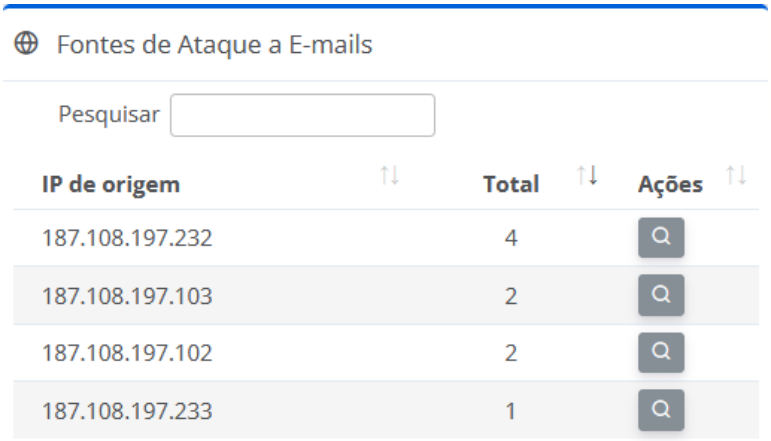


Seleção de data para pesquisa de ameaças

No dashboard inicial é listado:

Gráfico	Definição
Mensagens Analisadas	Total de mensagens processadas pelos módulos de segurança
IPs Analisados	Total de IPs analisados pelos módulos de segurança
Ameaças Identificadas	Total de ameaças identificadas
Fontes de Ataques a E-mails	Lista os principais hosts que enviaram ataques. Ao clicar em um deles mostrará informações detalhadas de todas as ameaças enviadas e detalhes relativo ao IP, tais como: nome, reverso, localização, etc.
Tipo de Ameaças a E-mails	Gráfico quantitativo dividido em classes de ameaças: Vírus, Phishing, Malware, URL, Zero Day, File Reputation, Malicious File, Suspicious File e Spoofing.
Ameaças Encontradas	Grid que contém as principais ameaças encontradas mostrando o nome da ameaça e seu identificador. Ao clicar em um deles mostrará informações detalhadas sobre a ameaça, informando: Gráfico de volume de e-mails por período, e-mails que continham esta ameaça, nome e descrição da ameaça.
Importar e Visualizar	Permite importar uma análise feita anteriormente a fim de verificar detalhadamente os dados exportados. Os dados importados serão visualizados da mesma forma que os dados em tempo real.
Exportar	Permite exportar a visualização atual para uma futura análise. Obs: É necessário selecionar a ameaça para que esta opção seja disponibilizada.

Dashboard Fontes de Ataques a E-mails



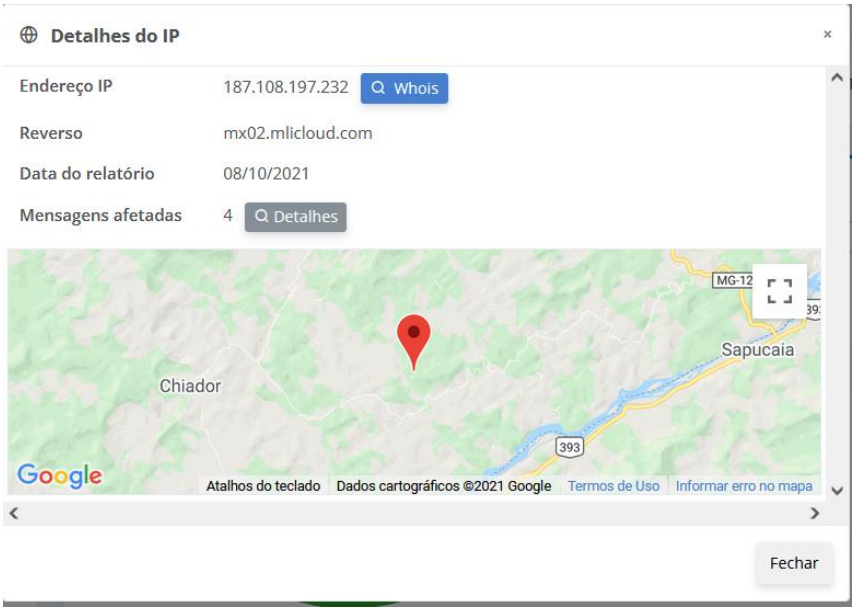
Dashboard de Fontes de Ataque a E-mails

Neste dashboard é listada:

Coluna	Descrição
IP de Origem	IP de Origem das ameaças
Total	Total de ameaças detectadas no período (dia)
Ações	Link que abre maiores informações sobre o IP de Origem da Ameaça, incluindo informação de localização física do IP, informações de whois e detalhamento dos e-mails afetados. A informação dos e-mails afetados engloba ameaças conhecidas e desconhecidas, bem como todo o movimento efetuado.
Pesquisar	Efetua pesquisa sobre as fontes de ataque a e-mails

Detalhes do IP

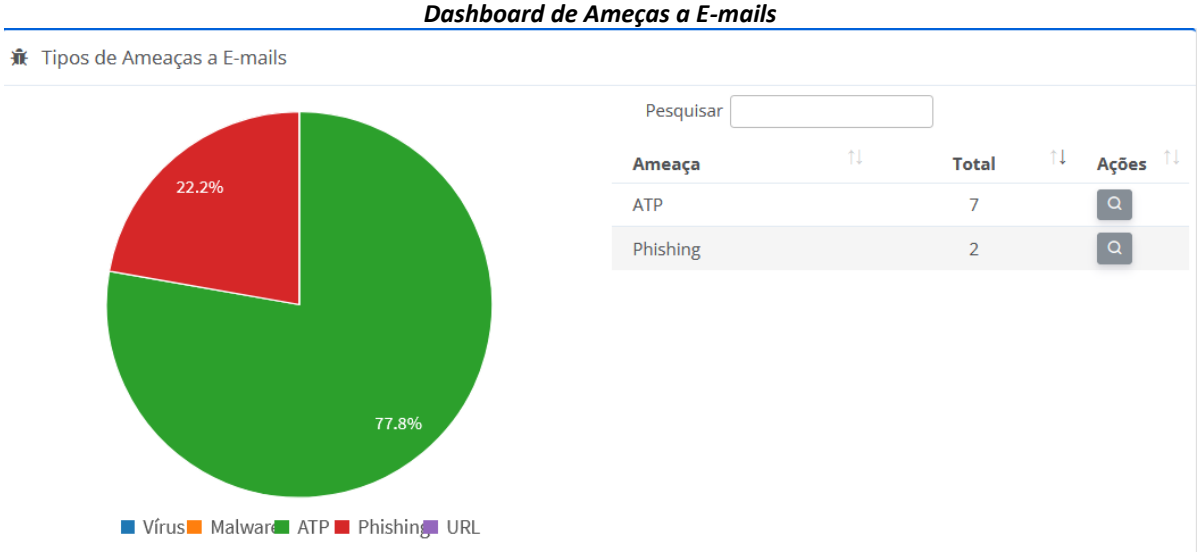
Ao clicar sobre a “lupa”, abre-se nova janela com maiores informações sobre o IP da Origem da Ameaça.



Janela de Detalhes do IP de Origem da Ameaça

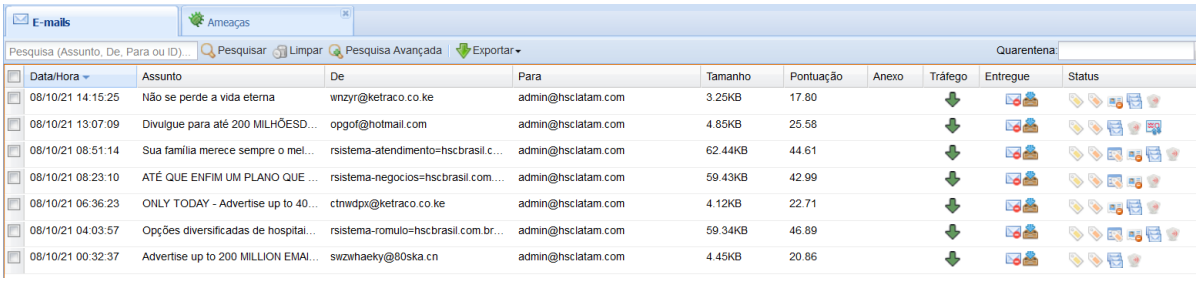
Título	Descrição
Endereço IP	IP da Origem da Ameaça
Reverso	DNS reverso detectado
Data do relatório	Data da geração desta informação
Mensagens Afetadas	Quantidade de Mensagens afetadas. Ao lado desta informação tem um ícone de "lupa" indicando que ao clicar, será efetuado filtro das mensagens afetadas pela ameaça.

Dashboard de Ameaças a E-mails



Dashboard de Ameaças a E-mails

Coluna	Descrição
Ameaça	Classificação da ameaça
Total	Total de ameaças detectadas no período (dia)
Ações	Ao clicar na lupa, o MailInspector isola os e-mails com as ameaças encontradas, podendo ser conhecidos e desconhecidos. Todo o movimento da ameaça (vírus, malware, Zero Day, URL maliciosa, Phishing, File Reputation, Suspicious File, Spoofing, entre outros) é rastreado e apresentado em forma detalhada ao administrador.
Pesquisar	Efetua pesquisa sobre as fontes de ataque a e-mails



Exemplo de tela de e-mails afetados pela ameaça ATP (ao clicar na lupa)

Exportando Ameaças do Painel

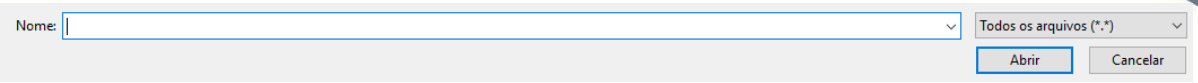
1. Selecione a ameaça encontrda no Painel de **Ameaças Encontradas**
2. Vamos pegar como exemplo a ameaça ATP

3. Após a seleção, é possível visualizar Detalhes da Ameaça e Mensagens Afetadas pela ameaça. No painel de Detalhes de Ameaça, é possível EXPORTAR os dados da ameaça para ser importado em outro painel de ameaças. O arquivo a ser exportado poderá ser no formato XML ou CSV.

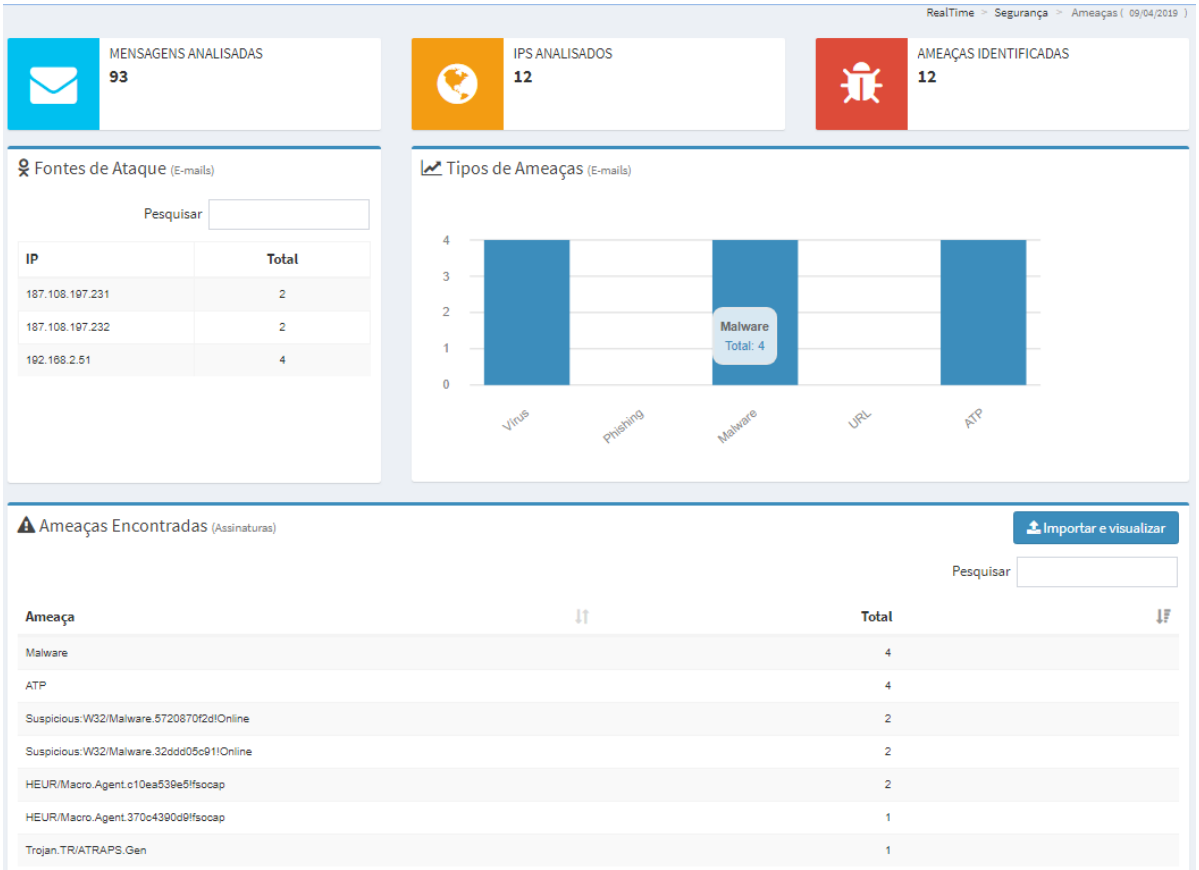
Importando Ameaças previamente Exportadas pelo Painel de Ameaças

1. No Painel de Ameaças, existe o botão Importar e Visualizar (que fica dentro da caixa de diálogo Ameaças Encontradas).
2. Clique no botão Importar e Visualizar

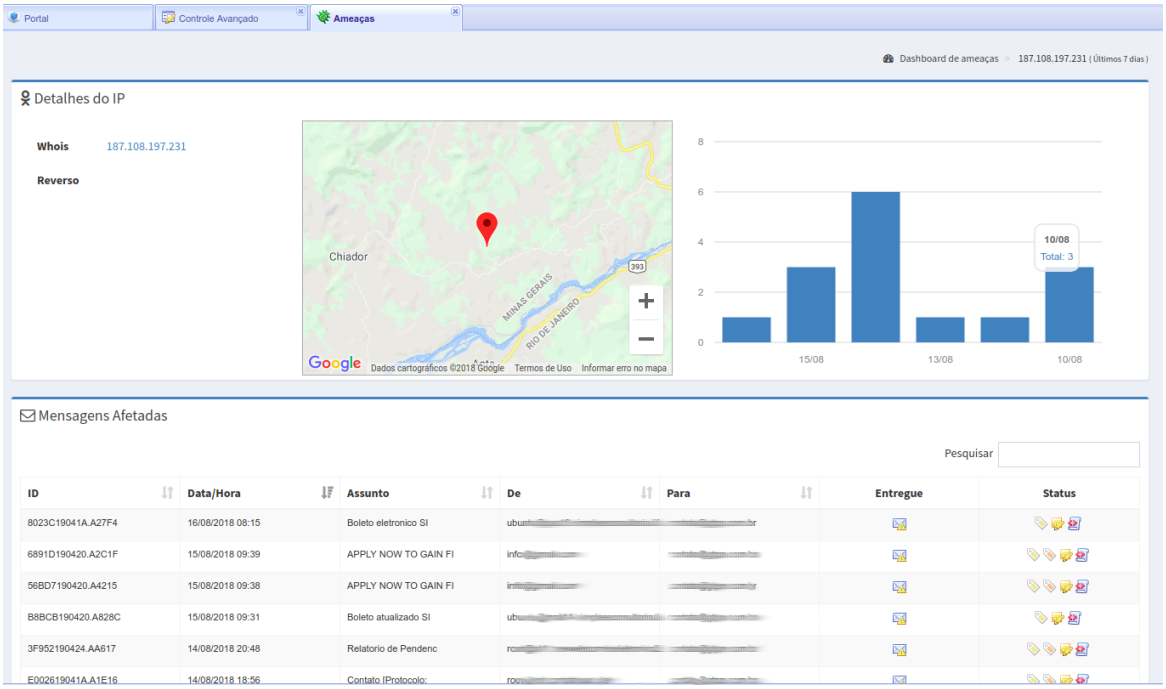
3. Selecione o local onde se encontra o arquivo XML, da ameaça previamente exportada.



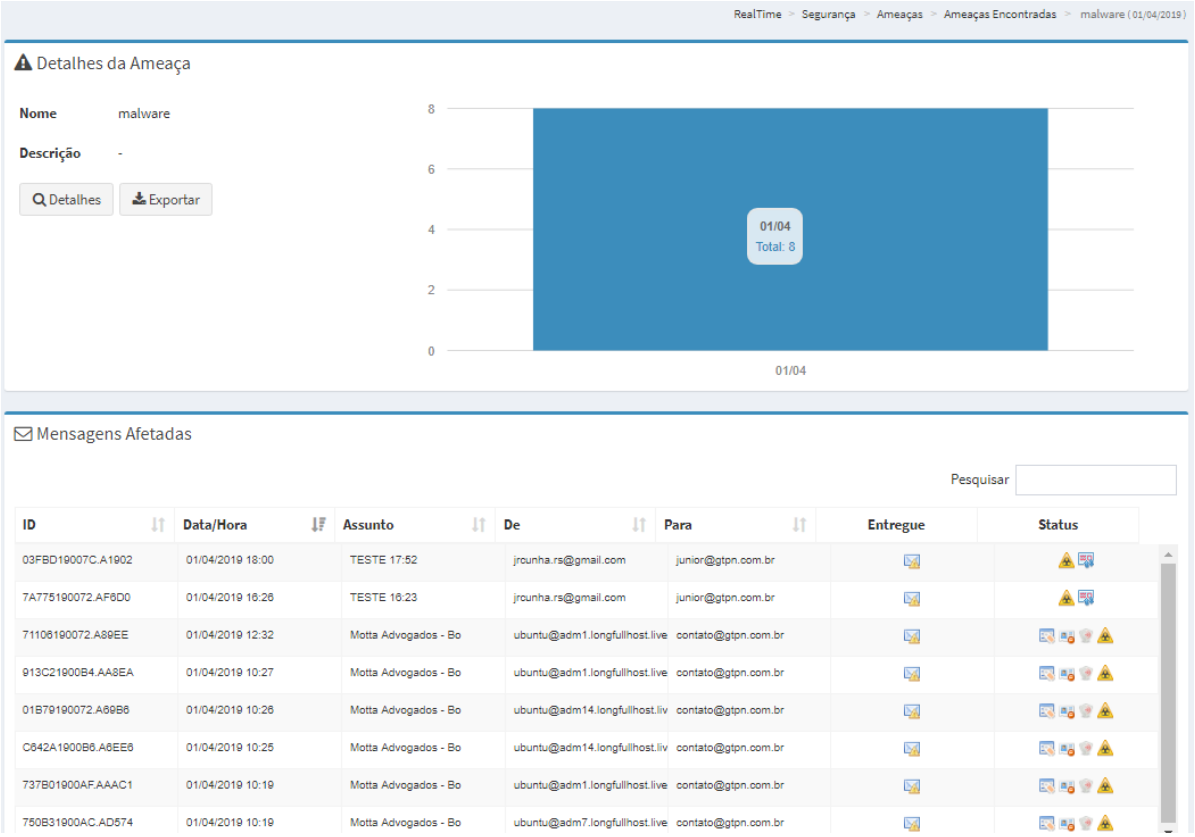
4. Clique em abrir.



Exemplo Gráfico Inicial



Exemplo Drill Down View por Host



Exemplo Drill Down View por Ameaça

Fraude de E-mail

RealTime / **Segurança / Fraude de E-mail**

Visão geral de Fraude de E-mail

Este dashboard permite ao administrador ter um resumo em tempo real dos principais ataques recebidos categorizados como fraude de e-mail. Esses tipos de ameaça vêm crescendo constantemente e por isso, o MailInspector possui função específica para detecção e bloqueio do ataque.

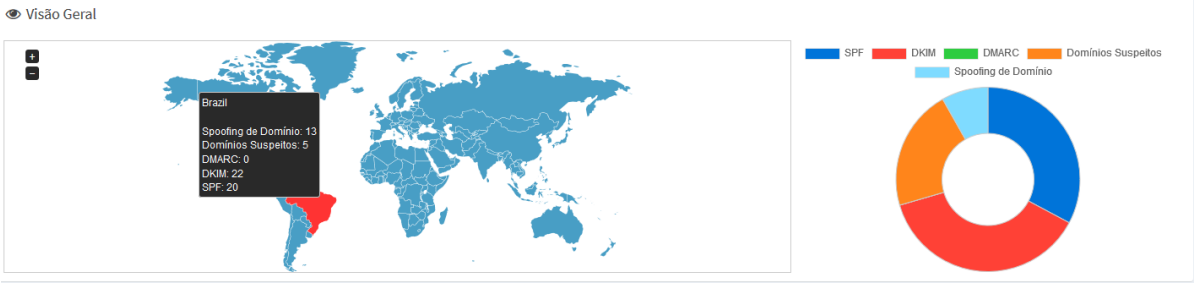
Nessa tela é possível visualizar as seguintes informações:

- Mapa com Geolocalização da origem das ameaças;
- Detalhes das Fraudes:
  - ID da mensagem;
  - Data e hora do recebimento;
  - Assunto;
  - De;
  - Para;
  - IP de Origem, com indicação do país;
  - Status do DMARC;
  - Status do DKIM;
  - Status do SPF;
  - Spoofing de Domínio (SD);
  - Domínios Suspeitos (DS);
- Principais alvos de fraudes de e-mail

Geolocalização

Indica as origens das ameaças, apresentando separação por:

- Quantos foram classificados como Spoofing de domínio;
- Quantos foram classificados como Domínios suspeitos;
- Quantos foram detectados com problemas de DMARC;
- Quantos foram detectados com problemas de DKIM;
- Quantos foram detectados com problemas de SPF;



Exemplo de Geolocalização das ameaças detectadas como fraude de e-mail

Principais Alvos de Fraude de E-mail

Indica quais usuários que mais sofreram ataques com fraudes de e-mail/e-mail impostor, para que o administrador possa efetuar uma análise mais profunda focado nos ataques sofridos por um usuário específico.

Principais Alvos

#	Email	Total
1	contato@gtpn.com.br	29
2	root@gtpn.com.br	4
3	vendas@gtpn.com.br	1

Exemplo de Principais Alvos de fraude de e-mail

Detalhes das Fraudes de E-mail

São apresentadas as principais informações dos e-mails detectados como fraudes/impostor. É possível visualizar informações mais detalhadas sobre um e-mail específico, dando um duplo clique sobre ele.

Ao efetuar essa ação (duplo clique), é apresentada uma janela com as seguintes informações:

- ID do e-mail;
- Assunto;
- Data e hora do recebimento;
- De (Envelope);
- Para (Envelope);
- De (Header – que é o que aparece no leitor de e-mail do usuário);
- Para (Header);
- Tamanho do e-mail;
- IP de Origem;
- Ponto de Acesso que analisou a mensagem;
- Status de categorização do e-mail;

Detalhes das Fraudes

Pesquisar

ID	Data	Assunto	De	Para	Origem	DMARC	DKIM	SPF	SD	DS
F40F3190072.A0DA1	03/04/2019 10:05	Agenda abril dias 15 e 16	contato@acgerente.com.br	contato@gtpn.com.br	187.108.197.231	✔	✖	✔	✔	✖
F3AB719007C.AB66F	03/04/2019 09:30	BALAS/BRINDES/CANETAS	erros@brindesaoseualcance.com.br	contato@gtpn.com.br	187.108.197.231	✔	✖	✔	✔	✔
E78A419007C.A5C67	03/04/2019 09:20	8 Bloqueia e Queima Gordura, Fórmula Avançada	return-conto-c7o948-rh=hscbrasil.com.br@p[illegible]	[illegible]	187.108.197.231	✔	✖	✖	✔	✖
DCFF519007C.A290D	03/04/2019 08:01	MELHORES NOVO MUNDO|Quem disse que s[illegible]	[illegible]	contato@gtpn.com.br	187.108.197.232	✔	✔	✔	✔	✖
DB1AC190072.A2B2B	03/04/2019 10:29	Pregão Eletrônico 00076/2019 (publicação)	portaldecompras@sestsenat.org.br	contato@gtpn.com.br	187.108.197.231	✔	✖	✖	✔	✔
D681319007C.A953D	03/04/2019 07:51	O oculos que resolve seu problema - ADLENS [illegible]	[illegible]@entreredes.com.br	contato@gtpn.com.br	187.108.197.231	✔	✖	✖	✔	✔
D5A44519007C.AF85B	03/04/2019 06:53	O Seguro do seu Carro está Vencendo? APROVEITE!	[illegible]@leadsverificados.com	contato@gtpn.com.br	187.108.197.232	✔	✖	✔	✔	✖
D547919007C.A8866	03/04/2019 09:17	ESPECIAL R$ 5,00 não perca!	return-a1747-90004-90005-romulo=hscbrasil.com.br@p[illegible]	contato@gtpn.com.br	187.108.197.232	✔	✖	✔	✔	✖
D4B9519007C.ABCD8	03/04/2019 00:35	Mais de 6000 Modelos de Planilhas Excel	planilhasexcel@economiadeverdade.com.br	contato@gtpn.com.br	187.108.197.232	✔	✔	✔	✔	✖
D384119007C.A9289	03/04/2019 04:03	Logwatch for mil02 (Linux)	root@gtpn.com.br	root@gtpn.com.br	187.108.197.232	✔	✔	✖	✖	✔

Mostrando de 1 até 10 de 34 registros

Anterior 1 2 3 4 Próximo

Exemplo de Detalhes das Fraudes

Detalhe da fraude

Mensagem	
ID	E78A419007C.A5C67
Assunto	8 Bloqueia e Queima Gordura, Fórmula Avançada
Data	03/04/2019 09:20:46
De (Envelope)	return-conto-c7o948-rh=hscbrasil.com.br@propostaimperdivel.com.b
Para (Envelope)	contato@gtpn.com.br
De (Header)	-
Para (Header)	-
Tamanho	7.95 KB
IP de Origem	187.108.197.231
IP do Ponto	mli01

Status	
✔ Limpa/Auditoria	✔ Provável Spam
✔ Spam	✔ Vírus
✔ Conteúdo Bloqueado	✔ Outro Bloqueio
✖ WhiteList	✔ BlackList
✔ Tamanho Excedido	✖ Em Quarentena
✔ Reenviada	✔ Não Reenviada
✔ Criptografada	✔ Regras de Compliance
✖ Regras de Controle Avançado	✔ Phishing
✔ Redes Sociais	✔ E-mail Marketing
✔ Arquivos suspeitos	✔ E-mails suspeitos
	✖ Domínios Recentes / Suspeitos
✔ Spoofing de domínio	✔ Controle de Surto
✖ E-mail Impostor	✖ Bulk Mail
✔ Conteúdo Adulto	✔ ATP
✔ Malware	✔ Domínios Diferentes no Cabeçalho
✔ Domínios Forjados com Free Mail	✔ Free Mail

Fechar

Tela de detalhes da fraude

M-SOAR

RealTime / **Segurança / M-SOAR**

Visão geral de M-SOAR

Este dashboard permite ao administrador ter um resumo em tempo real de toda a ação efetuada sobre o sistema de Orquestração de ações no Office 365, G-Suite ou Zimbra.

Nessa tela é possível visualizar as ações tomadas pelo administrador, citando a seguir alguns exemplos:

- Habilitação de domínio a serem operados pelo M-SOAR;
- Ativação de Add-On para uso com M-SOAR;
- Alterações de configuração do M-SOAR;
- Download de XML;
- Adição/Edição/Exclusão de regras para o domínio gerenciado pelo M-SOAR;
- Ação sobre mensagens entregues:
    - Bloqueio de Conteúdo;
    - Bloqueio/Remoção de URL (links);
    - Exclusão de anexos;
    - Mover e-mail para a lixeira eletrônica;
    - Apagar e-mail;

Definições de Opções

Barra de ações M-SOAR.

Opções	Definição
Pesquisa	Pesquisa rápida.
Limpar	Remove qualquer filtro de pesquisa efetuada.
Pesquisa Avançada	Habilita o módulo de pesquisa avançada, liberando mais filtros, vide Definições de ***Opções - Pesquisa Avançada***
Visualizar	Visualiza com maiores detalhes a ação efetuada no M-SOAR.
Exportar CSV	Exporta a lista de ações previamente filtrada.

Definições de Opções - Pesquisa Avançada

Pesquisa sobre as ações M-SOAR.

Opções	Definição
Usuário	Filtra o registro das ações de um determinado usuário.
IP	Filtra as ações por um IP específico.
Ação	Filtra registros sobre uma determinada ação, por exemplo: *Habilitou*, irá filtrar todos os registros que contenham a palavra *Habilitou*.
Período de Tempo	**Data Inicial:** Indica a data inicial da pesquisa **Data Final:** Indica a data limite da pesquisa

E-mails | M-SOAR

Pesquisa (IP, Usuário ou Ação) | Pesquisar | Limpar | Pesquisa Avançada | Visualizar | Exportar CSV

Data	Usuário	IP	Ação
25/05/2021 15:35:49	gabriel.sousa	187.108.197.229	Microsoft 365: Habilitou o domínio hsclatam.com
25/05/2021 15:35:30	gabriel.sousa	187.108.197.229	Microsoft 365: Habilitou o domínio gtpn.com.br
25/05/2021 15:35:03	gabriel.sousa	187.108.197.229	Microsoft 365: Desabilitou o domínio hsclatam.com
25/05/2021 15:35:01	gabriel.sousa	187.108.197.229	Microsoft 365: Desabilitou o domínio gtpn.com.br
25/05/2021 15:26:29	gabriel.sousa	187.108.197.229	Microsoft 365: Habilitou o Add-on
25/05/2021 15:26:23	gabriel.sousa	187.108.197.229	Microsoft 365: Desabilitou o Add-on
25/05/2021 15:18:29	ivan.admin	189.6.252.82	Microsoft 365 > Add-on: Fez o download do arquivo XML
25/05/2021 15:18:24	ivan.admin	189.6.252.82	Microsoft 365 > Add-on: Configurou a URL para https://antispam.hsclatam.com/mailinspector/addons/o365
25/05/2021 15:18:08	gabriel.sousa	187.108.197.229	Microsoft 365: Habilitou o Add-on
25/05/2021 15:18:04	gabriel.sousa	187.108.197.229	Microsoft 365: Desabilitou o Add-on
25/05/2021 15:17:38	ivan.admin	189.6.252.82	Microsoft 365 > M-SOAR > gtpn.com.br: Alterou as configurações do M-SOAR
25/05/2021 15:17:31	ivan.admin	189.6.252.82	Microsoft 365: Habilitou o domínio gtpn.com.br
25/05/2021 15:17:10	ivan.admin	189.6.252.82	Microsoft 365: Desabilitou o domínio gtpn.com.br
24/05/2021 16:24:27	ivan.admin	189.6.252.82	Microsoft 365 > Add-on: Editou a regra "Geral"
24/05/2021 16:24:02	ivan.admin	189.6.252.82	Microsoft 365 > M-SOAR > gtpn.com.br: Alterou as configurações do M-SOAR
24/05/2021 16:23:55	ivan.admin	189.6.252.82	Microsoft 365 > M-SOAR > hsclatam.com: Alterou as configurações do M-SOAR
24/05/2021 16:23:46	ivan.admin	189.6.252.82	Microsoft 365 > Add-on: Editou a regra "Geral"
24/05/2021 16:16:50	ivan.admin	189.6.252.82	Microsoft 365 > Add-on: Editou a regra "Geral"
24/05/2021 16:16:40	ivan.admin	189.6.252.82	Microsoft 365 > M-SOAR > gtpn.com.br: Alterou as configurações do M-SOAR
24/05/2021 16:16:32	ivan.admin	189.6.252.82	Microsoft 365: Habilitou o domínio gtpn.com.br

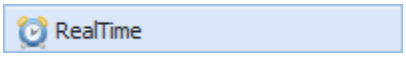
Exemplo de Tela M-SOAR

SmartDefender

O HSC SmartDefender é um mecanismo avançado de proteção contra ataques que tem como foco principal o usuário final e exploram vulnerabilidades de engenharia social entre outras para obter informações sigilosas de seus destinatários.

As análises são realizadas em tempo real utilizando tecnologias como URL SandBox, File SandBox (efetuado localmente e opcionalmente é enviado o arquivo para HSC Brasil efetuar a análise dinâmica, analisando comportamento e comparando com outras ameaças já registradas) e Machine Learning, com isso, uma ameaça consegue ser bloqueada em menos de 60 segundos, mesmo que seja desconhecida.

Também no mesmo módulo de SmartDefender são verificadas as imagens pornográficas, dessa forma uma vez habilitado este módulo pelo administrador, o MailInspector passará a verificar imagens em busca de conteúdo pornográfico e efetuando o bloqueio sobre ele.



/ **Segurança** / **SmartDefender**

Visão geral do SmartDefender

Nesta tela o administrador pode consultar em tempo real a nuvem do **HSC SmartDefender** a reputação e informações sobre:

- URLs;
- Arquivos;
- IPs.

A tela foi projetada para dar todas as informações necessárias para uma tomada de decisão do administrador. Aqui você também pode controlar a Allow List/Block List Local de seu SmartDefender, podendo colocar arquivos, URLs e IPs nestas Listas e administrá-los.

Ao enviar arquivos para a análise pelo SmartDefender e for detectado como ameaça, o sistema adiciona o padrão a base de conhecimento da HSCBRASIL (Big Data), dessa forma automatizando o sistema de envio de amostras.

Definições de Opções - Configuração

Permite ao administrador gerenciar todas as URL's, Arquivos e/ou IP's que foram incluídos manualmente no sistema do HSC SmartDefender.

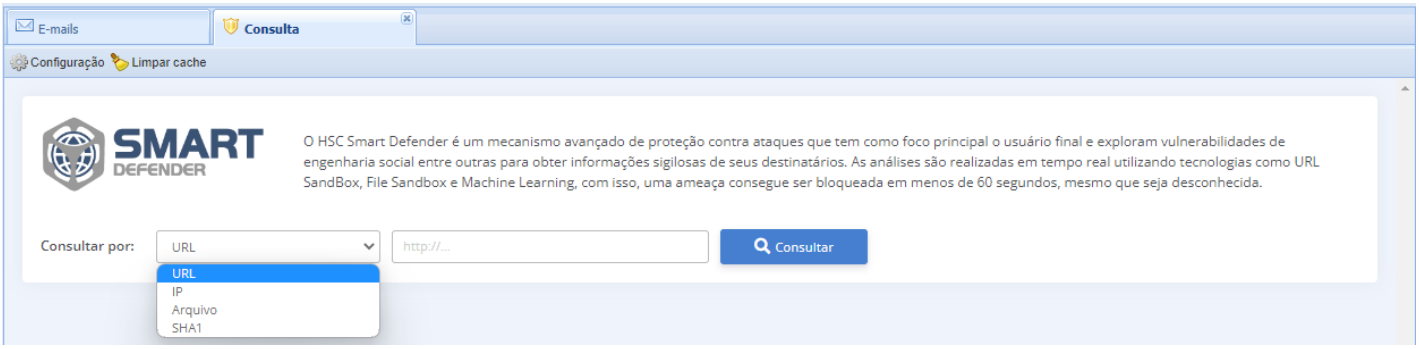
Opções	Definição
Tipo	Permite ao administrador selecionar entre Arquivo, URL ou IP.
Valor	Permite ao administrador inserir o valor que o campo recebe para tomar a ação sob este item.
Ação	Permite ao administrador selecionar se este valor é confiável, ou não confiável.
Comentário	Permite inserir um comentário sobre o registro.

Nessa opção é formada uma tabela de confiável e indesejável de IPs, Arquivos, URLs e HASH (SHA1), ao qual se estivem como confiável, o artefato não é enviado para o SandBox, dando como resultado artefato confiável. Se estiver listado como não confiável, o e-mail com o artefato é bloqueado automaticamente.

Consultas

Aqui podemos efetuar uma consulta por IP, URL ou Arquivo selecionado no campo "Tipo de Consulta".

Quando for selecionado arquivo o administrador deverá fazer Upload de uma amostra do arquivo a ser analisada. Após selecionar o Tipo o administrador deve colocar o valor da consulta, ou seja, a URL, IP ou Arquivo desejado e clicar em Consultar;



Exemplo de Tela de SmartDefender

A análise é feita em tempo real usando todos os mecanismos do SmartDefender.

É possível efetuar a reclassificação de IPs, Arquivos e URL's. Ao reclassificar, o MailInspector já envia a classificação indicada do administrador local ao sistema Global de SmartDefender. É efetuada a análise das categorias indicadas e sendo aprovado, a categorização sugerida é aplicada a nível global da solução, dessa forma, o sistema trabalha de forma colaborativa, além de usar uma base (dinâmica alimentada por outros sistemas de categorização) já estabelecida de categorias, conta também com a reclassificação aplicada pelos administradores locais de todos os sistemas já instalados, dessa forma, é possível o administrador criar lista de confiável e não confiável de IP, URL e Arquivos, sobrepondo ao resultado da análise do BigData da HSCBRASIL.

Depois de analisado uma tela com a resposta será apresentada conforme a descrição a seguir:

Consultas por IP

Na tela da reposta da consulta de um IP será reportado a Reputação Atual, gráfico com Histórico da Reputação, verificação nas principais RBLs Externas, WHOIS, Geolocalização e suas configuração do Reverso IP.

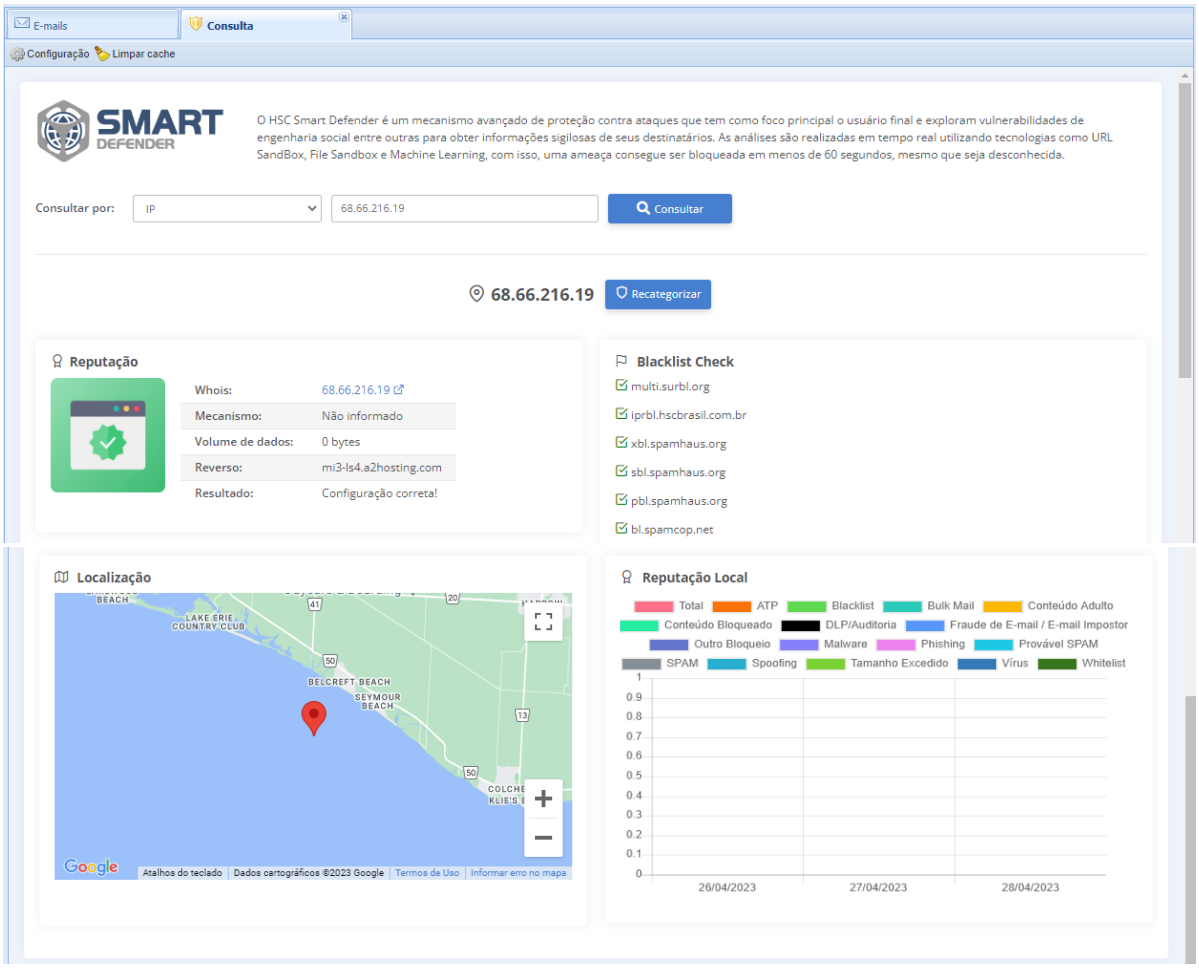
O Botão "Adicionar IP na Whitelist" irá colocar o IP na lista de endereços confiáveis e não mais será verificado pelo sistema do SmartDefender contra Reputação. Essa ação faz com que a reputação local se sobreponha a análise da reputação global apresentada pelo MailInspector.

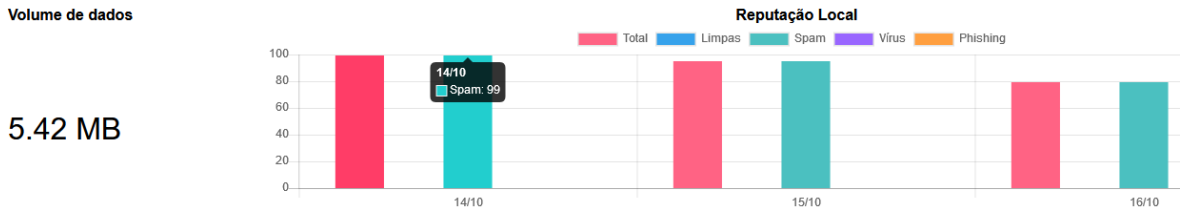
O Botão "Adicionar IP na Blacklist" irá colocar o IP na lista de endereços perigosos e terá sua reputação considerada como "Possivelmente Perigosa". Essa ação faz com que a reputação local se sobreponha a análise da reputação global apresentada pelo MailInspector.

Se for efetuada pesquisa por IP, as informações retornadas são:

- Status da Reputação do IP;
- Indicação de WHOIS;

- Verificação do IP em Block Lists;
- Indicação do reverso e análise;
- Geolocalização do IP;
- Volume de dados: Indicando o fluxo de dados oriundos do IP, dessa forma é possível verificar se o IP não está gerando um surto de e-mails;
- Reputação em relação a:
    - Spam;
    - Vírus;
    - Phishing;
    - Ataque de Dicionário;





Tela de resultado sobre reputação por IP

Recategorizar o IP

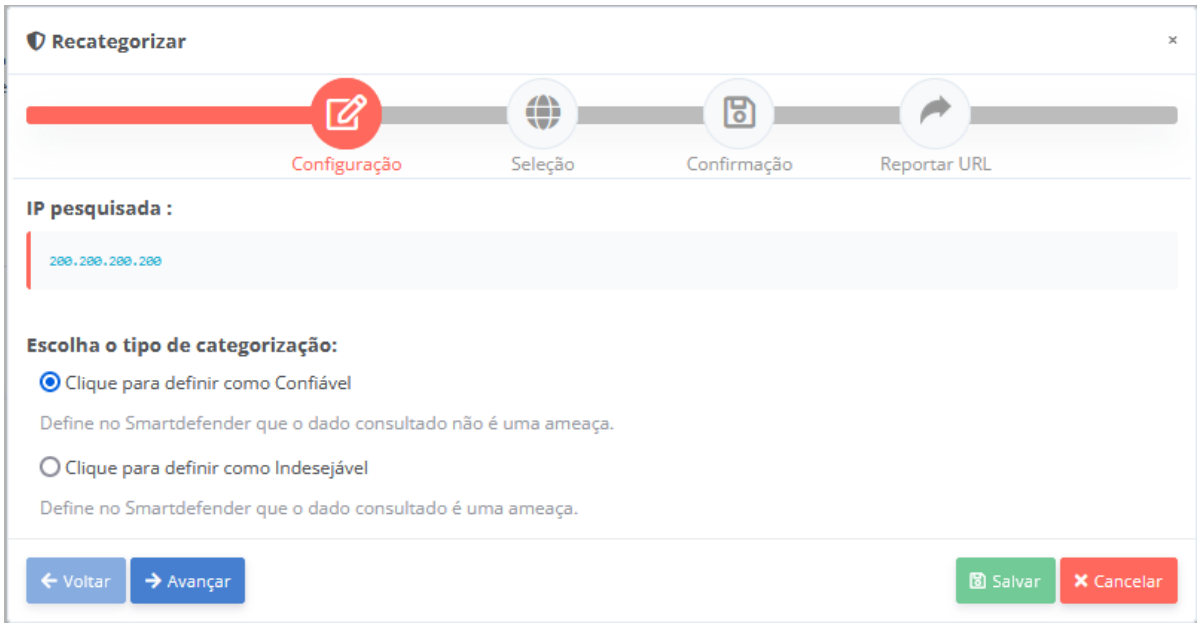
É possível após a consulta por IP a recategorização do IP, marcando-o como confiável ou indesejável.

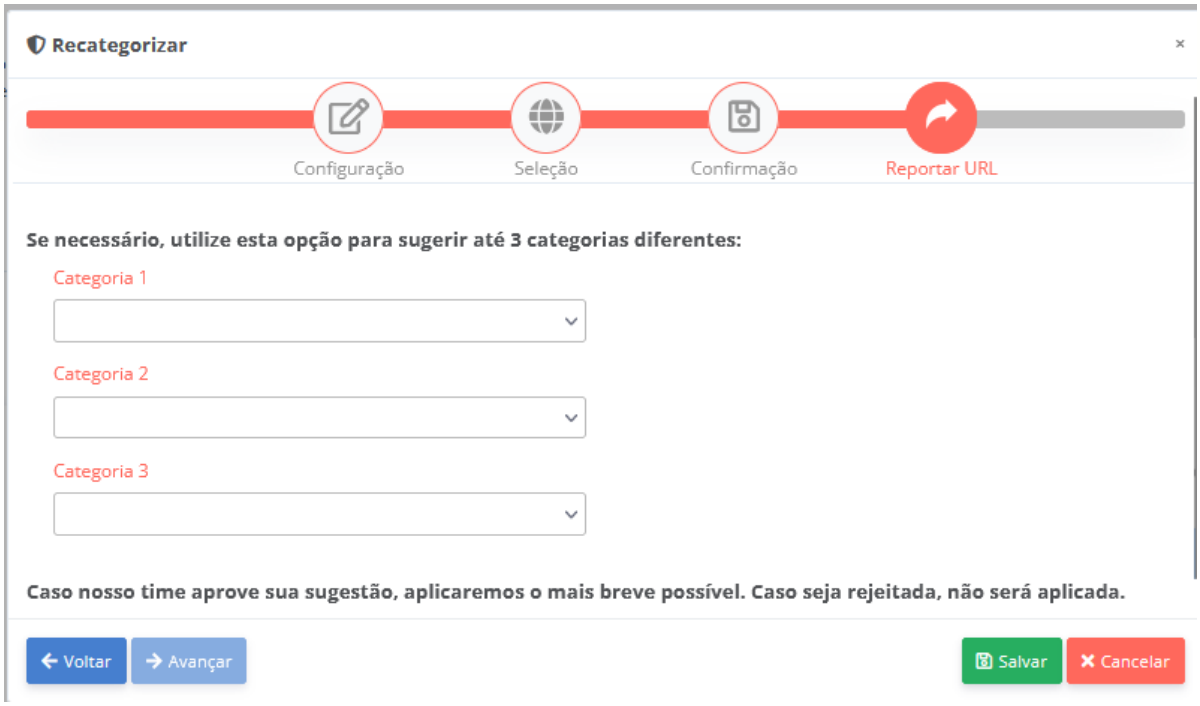
Para a recategorização, clique em Recategorizar e selecione se o IP é confiável ou indesejável, clique em Avançar.

Coloque um comentário sobre esse processo e clique em Avançar.

Selecione a Categoria do IP indicado e clique em Salvar

Obs: Ao salvar, o dado do IP é enviado automaticamente para a HSCBRASIL, para nova verificação e correção de categorização se necessário.





Consultas por URL

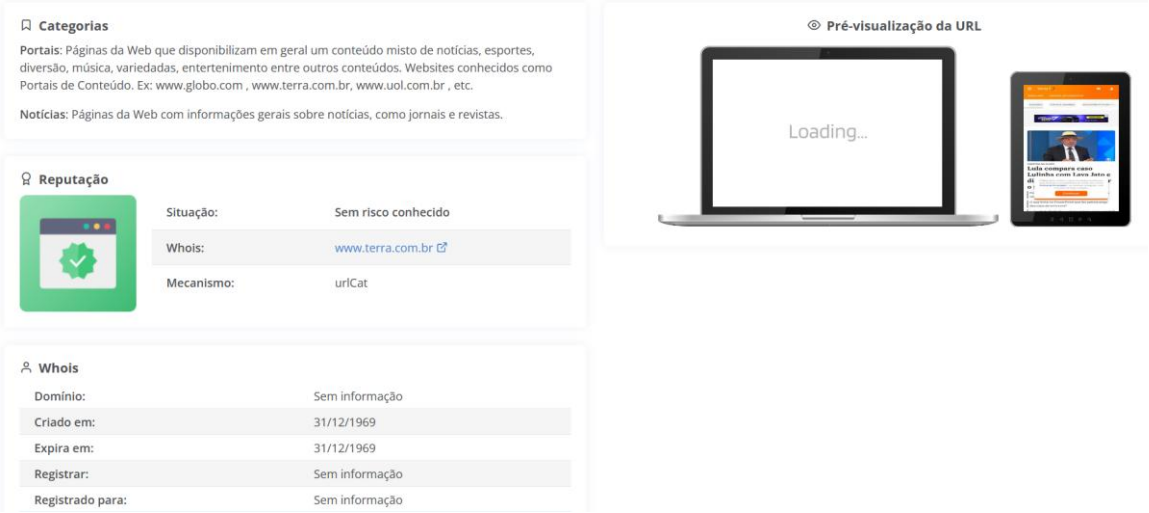
Na tela da reposta da consulta de um URL/Domínio será reportado a Reputação Atual, WHOIS e suas categorizações.

O Botão "Adicionar URL na Allow List" irá colocar o URL na lista de endereços confiáveis e não mais será verificado pelo sistema do SmartDefender contra Reputação. Essa ação faz com que a reputação local se sobreponha a análise da reputação global apresentada pelo MailInspector.

O Botão "Adicionar URL na Block List" irá colocar o URL na lista de endereços perigosos e terá sua reputação considerada como "Possivelmente Perigosa". Essa ação faz com que a reputação local se sobreponha a análise da reputação global apresentada pelo MailInspector.

Se for efetuada pesquisa por URL, as informações retornadas são:

- Categoria da URL;
- Status da Reputação da URL;
- Situação da URL (se possui algum risco ou não);
- Identificação de WHOIS;
- Mecanismo de busca utilizado;
- Preview da página web;
- Dados do WHOIS (data de criação, data de expiração, proprietário, qual o domínio, entre outros dados do WHOIS);



Tela de consulta de URL

Recategorizar a URL

É possível após a consulta por IP a recategorização da URL, marcando-o como confiável ou indesejável.

Para a recategorização, clique em Recategorizar e selecione se o IP é confiável ou indesejável, clique em Avançar.

Escolha a parte da URL a ser classificada, podendo ser:

- URL Completa: A URL do jeito que está apresentada
- Somente Host: É a opção mais utilizada, pois qualquer URL oriunda daquele domínio/host será considerado como indicado pelo administrador
- URL Customizada: Você como administrador, pode customizar a URL do jeito que quiser

Clique em Avançar

Coloque um comentário sobre esse processo (opcional) e clique em Avançar.

Por último selecione a(s) categoria(s) que você deseja que a URL seja reclassificada e clique em Salvar.

Recategorizar

Configuração | Seleção | Confirmação | Reportar URL

URL pesquisada :

http://hscbrasil.com.br

Escolha o tipo de categorização:

- (●) Clique para definir como Confiável

  Define no Smartdefender que o dado consultado não é uma ameaça.

- ( ) Clique para definir como Indesejável

  Define no Smartdefender que o dado consultado é uma ameaça.

Voltar | Avançar | Salvar | Cancelar

Recategorizar

Configuração | Seleção | Confirmação | Reportar URL

Arquivo pesquisado:

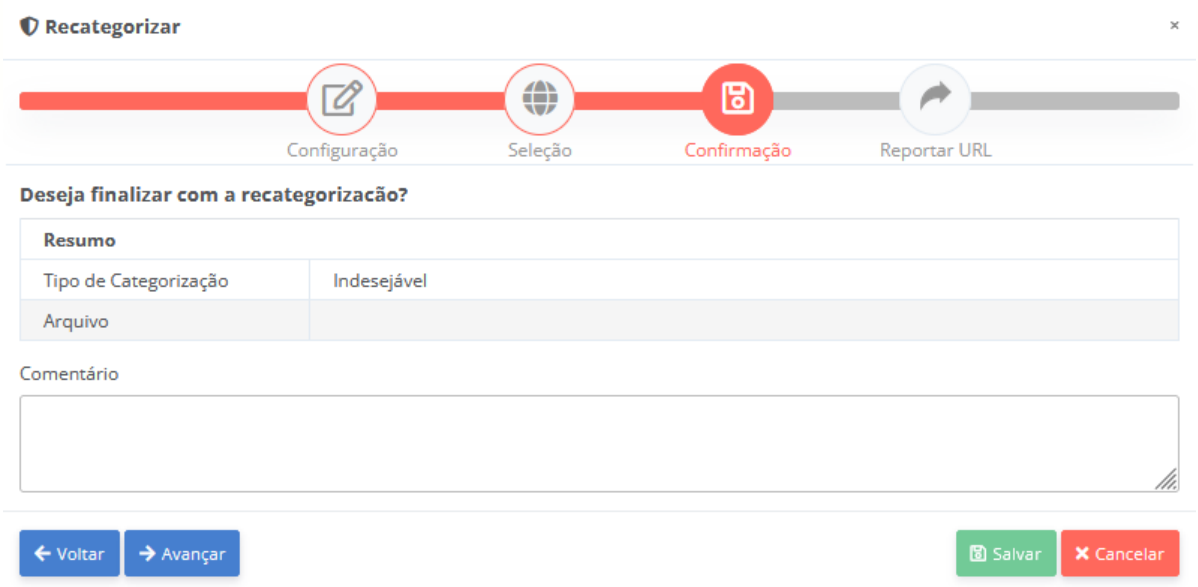
http://hscbrasil.com.br

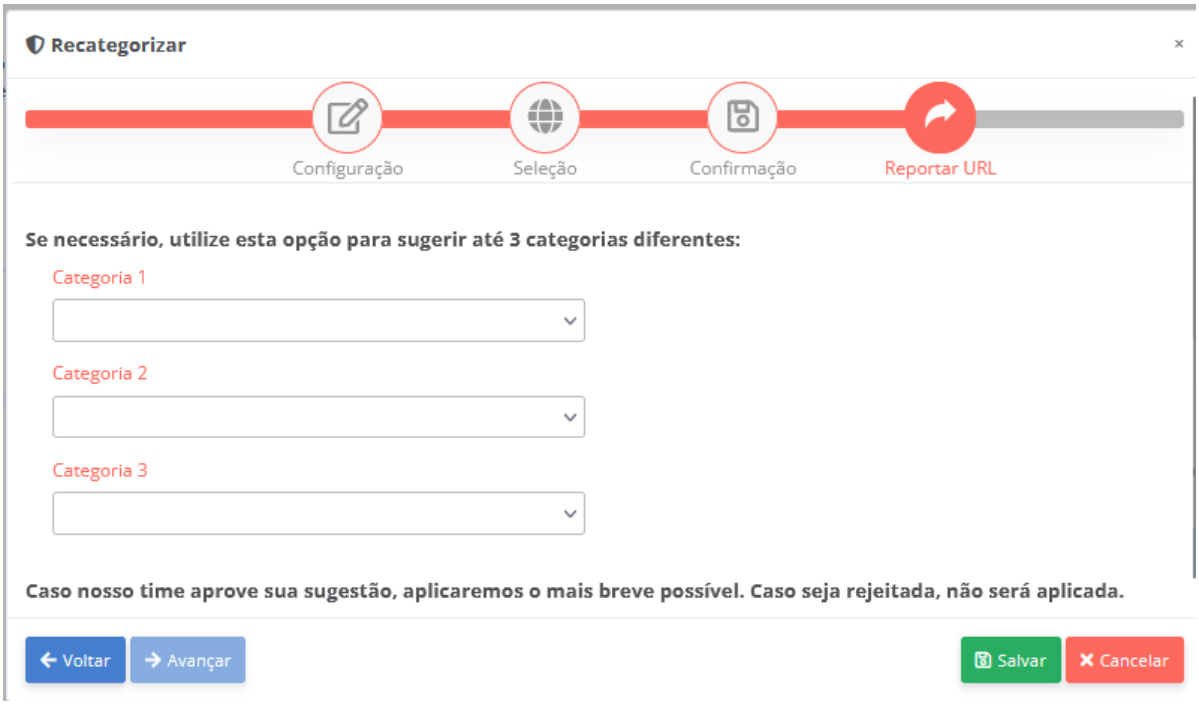
Escolha qual parte da URL será categorizada:

- (●) URL Completa — http://hscbrasil.com.br
- ( ) Somente Host — hscbrasil.com.br
- ( ) URL Customizada — http://hscbrasil.com.br

Suporta o uso do caractere *

Voltar | Avançar | Salvar | Cancelar





A consulta de URL, quando retorna E**m Análise**, o sistema de crawler é acionado, sendo que o link é submetido ao URL SandBox, ao qual finge um ser humano clicando em tudo no URL destino. Dessa forma, obtém-se o resultado mais preciso sobre a URL. O sistema de crawler simula um humano e clica em todos os links contidos no e-mail.

Em determinados links o sistema de crawler pode dar problema, tais como link de remoção de subscrição. Para ignorar o sistema de crawler (URL SandBox), é necessário cadastrar a URL como confiável ou não confiável.

Consultas por Arquivo

Na tela da reposta da consulta de um Arquivo será reportado a Reputação Atual do arquivo, o nome da ameaça detectada, e link para detalhes da ameaça onde o administrador poderá ter todos os detalhes técnicos.

O Botão "Adicionar Arquivo na AllowList" irá colocar o Arquivo na lista de arquivos confiáveis e não mais será verificado pelo sistema do SmartDefender contra Reputação ou Possível Ameaça.

O Botão "Adicionar Arquivo na BlockList" irá colocar o Arquivo na lista de arquivo perigosos e terá sua reputação considerada como "Possivelmente Perigosa".

Se for efetuada pesquisa por Arquivo, as informações retornadas são:

- Situação do anexo, podendo ser:
  - Limpo;
  - Em análise;
  - Comprometido;
- Mecanismo utilizado para a análise;
- Tamanho do anexo;
- Tipo real do anexo (Mime Type);

Reputação

Situação: Em análise
Mecanismo: Não informado
Tamanho: 502.15 KB
Tipo: application/x-msdownload

Reputação ainda em análise

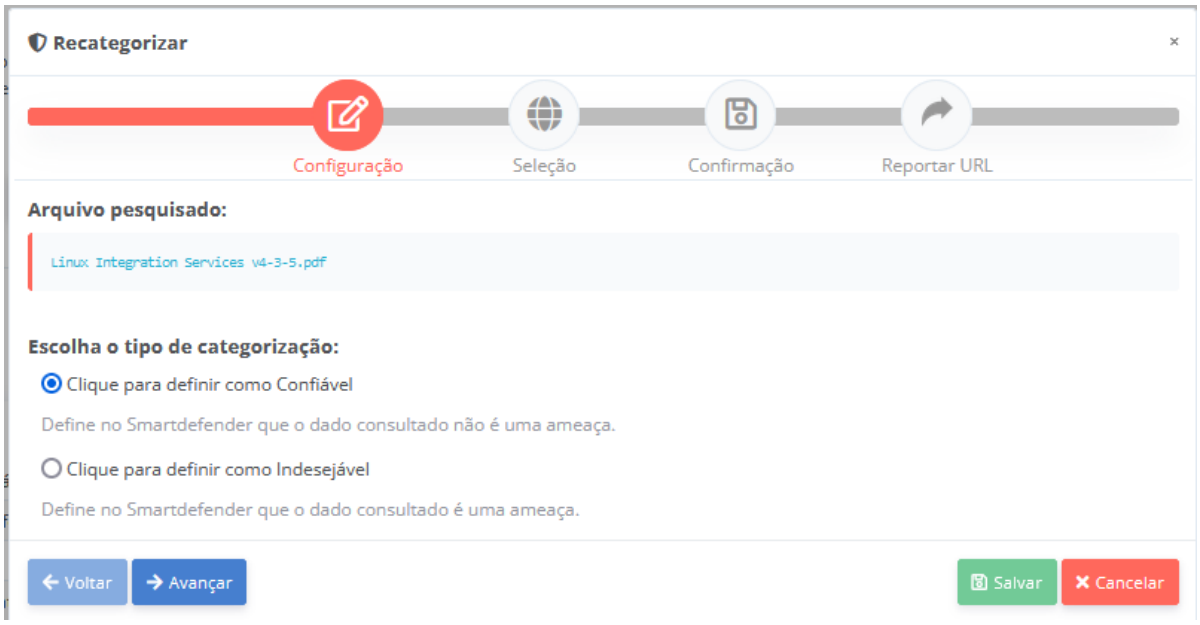
Recategorizar o Arquivo

É possível após a consulta por Arquivo a recategorização do Arquivo, marcando-o como confiável ou indesejável.

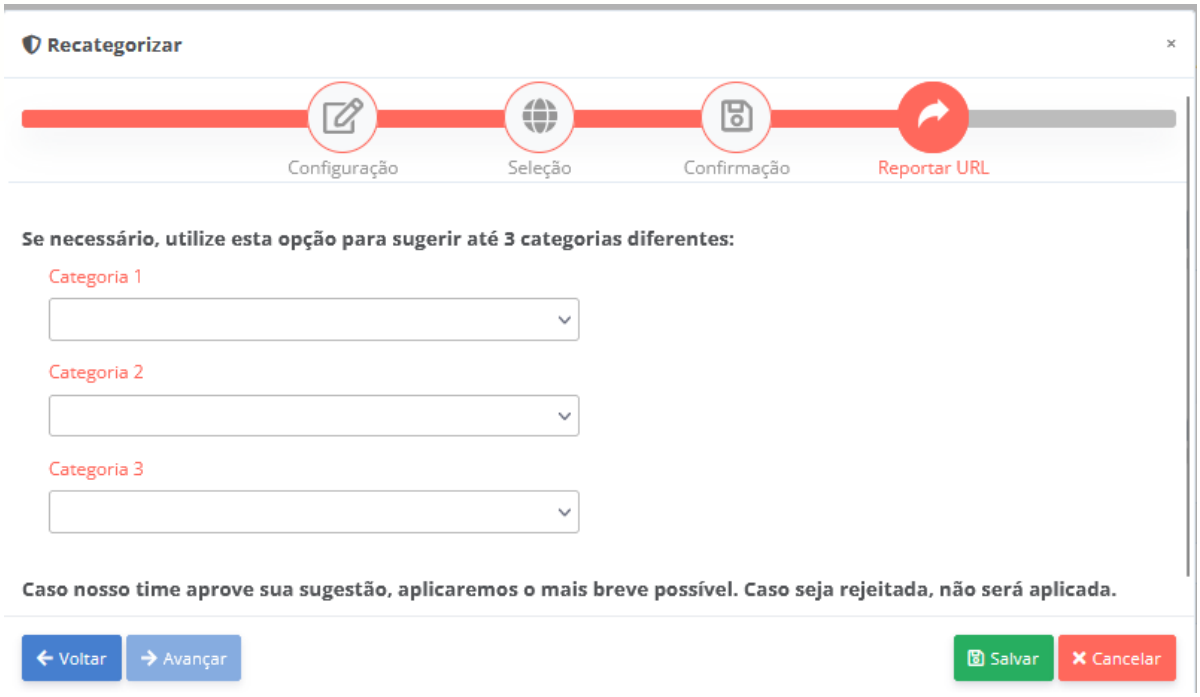
Para a recategorização, clique em Recategorizar e selecione se o arquivo é confiável ou indesejável, clique em Avançar.

Coloque um comentário sobre esse processo (opcional) e clique em Avançar.

Por último selecione a(s) categoria(s) que você deseja que o arquivo seja reclassificado e clique em Salvar.



Comentário


Recategorizar
Configuração
Seleção
Confirmação
Reportar URL
Se necessário, utilize esta opção para sugerir até 3 categorias diferentes:
Categoria 1
Categoria 2
Categoria 3
Caso nosso time aprove sua sugestão, aplicaremos o mais breve possível. Caso seja rejeitada, não será aplicada.
Voltar
Avançar
Salvar
Cancelar

DMARC

Use esta página visualizar as estatísticas de funcionamento do módulo de análise de DMARC em tempo real.

RealTime / **DMARC**

O módulo Analisador de DMARC (DMARC Analyzer) é um módulo do HSC MailInspector licenciado à parte, para o uso do mesmo é necessário aquisição da licença específica para este fim.

Sumário

Apresenta os dados do relatório agregado em tempo real, ou seja, é feita a coleta das informações e apresentada na tela automaticamente.

RealTime **/ DMARC / Sumário**

Este Dashboard traz informações referente aos relatórios agregados fornecidos pelos ISPs.

Visão geral DMARC – Sumário

O **MailInspector** disponibiliza recursos para coleta, processamento e análise de **relatórios agregados DMARC (RUA – DMARC Aggregate Reports)**, permitindo que os administradores e proprietários de domínios obtenham visibilidade sobre a utilização de seus domínios para envio de mensagens na Internet e sobre os resultados dos mecanismos de autenticação de e-mail.

Os relatórios agregados são enviados periodicamente pelos servidores de e-mail dos destinatários e apresentam informações consolidadas sobre as mensagens que **passaram ou falharam nas verificações de DMARC, SPF e DKIM**, incluindo os respectivos resultados de alinhamento exigidos pelo DMARC.

Os relatórios RUA são disponibilizados em **formato XML** e encaminhados para o endereço de e-mail definido no registro DMARC do domínio. O MailInspector permite realizar a **coleta desses relatórios a partir de uma conta de correio eletrônico compatível com IMAP**, processando automaticamente os arquivos recebidos e apresentando as informações de forma estruturada para análise do administrador.

A partir do processamento dos relatórios, o sistema proporciona uma visão consolidada sobre o comportamento do domínio na internet e permite identificar possíveis problemas de autenticação, configurações inadequadas, fontes legítimas de envio e eventuais indícios de utilização indevida do domínio.

Entre as principais informações apresentadas nos relatórios agregados, destacam-se:

- **Organização ou servidor destinatário responsável pelo envio do relatório**, permitindo identificar a origem dos dados reportados;
- **Resultado da autenticação DMARC**, indicando as mensagens que foram aprovadas ou reprovadas;
- **Resultado da autenticação SPF**, incluindo:
  - indicação de sucesso ou falha;
  - informações relacionadas ao alinhamento SPF;
- **Resultado da autenticação DKIM**, incluindo:
  - indicação de sucesso ou falha;

  - informações relacionadas ao alinhamento DKIM;
- **Quantidade de mensagens enviadas utilizando o domínio**, permitindo acompanhar o volume de mensagens reportadas por período;
- **Endereços IP de origem** responsáveis pelo envio de mensagens utilizando o domínio analisado;
- **Geolocalização aproximada das origens de envio**, auxiliando na identificação de localidades e fontes de tráfego inesperadas;
- **Distribuição dos resultados de autenticação**, possibilitando identificar padrões de aprovação, falha e desalinhamento;
- **Informações temporais dos relatórios**, permitindo acompanhar a evolução dos resultados ao longo dos períodos analisados.

Análise e identificação de uso indevido do domínio

Os relatórios RUA são fundamentais para o monitoramento da **postura de autenticação e proteção do domínio**, pois permitem ao administrador identificar quais servidores e endereços IP estão enviando mensagens em nome do domínio e verificar se essas mensagens estão sendo devidamente autenticadas.

A análise dos resultados de **DMARC, SPF e DKIM**, combinada com as informações de origem e geolocalização, possibilita identificar situações como:

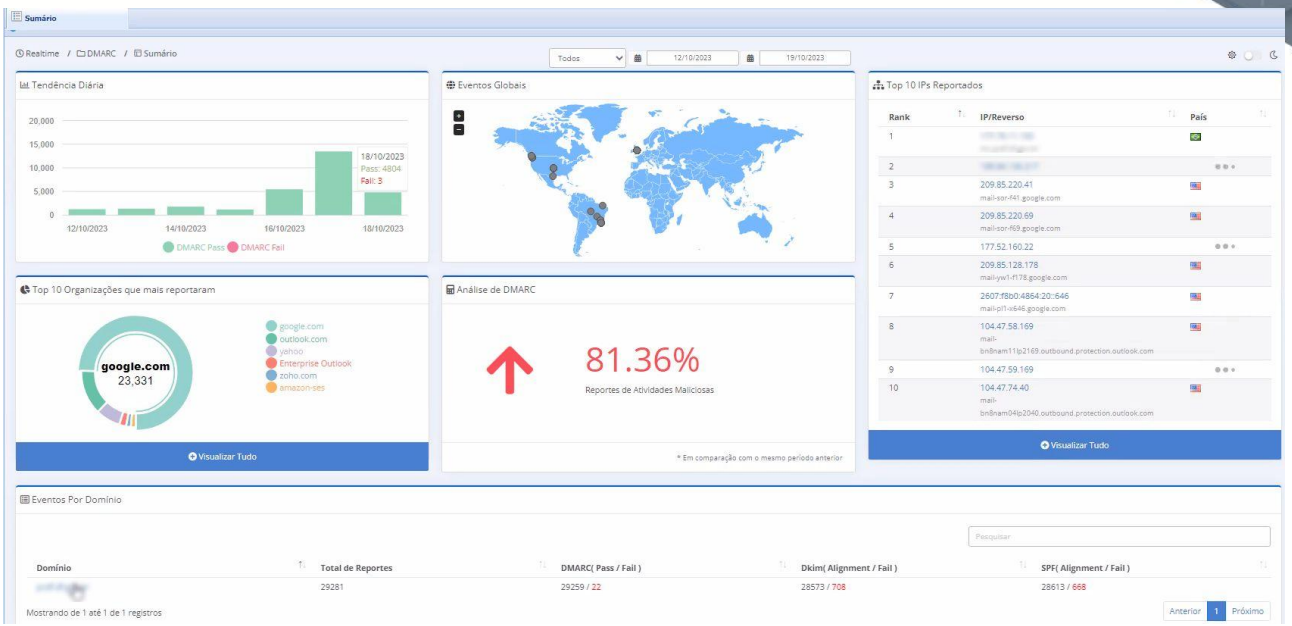
- Servidores legítimos enviando mensagens sem a configuração adequada de SPF ou DKIM;
- Falhas de alinhamento entre os mecanismos de autenticação;
- Problemas de configuração que possam afetar a entrega das mensagens;
- Novas fontes de envio que não fazem parte da infraestrutura autorizada;
- Comportamentos anômalos relacionados ao uso do domínio;
- Possíveis tentativas de **spoofing ou falsificação do domínio**;
- Alterações inesperadas no volume ou na origem das mensagens.

Dessa forma, o MailInspector permite ao administrador obter uma **visão centralizada e histórica da utilização do domínio**, facilitando a identificação de problemas de autenticação e entrega dos e-mails, bem como a investigação de possíveis tentativas de falsificação.

Com essas informações, a organização pode **ajustar suas políticas de DMARC, SPF e DKIM, identificar e autorizar corretamente suas fontes legítimas de envio e adotar medidas preventivas contra o uso indevido do domínio**, contribuindo para o fortalecimento da segurança e da reputação dos canais de correio eletrônico.

O MailInspector apresenta os seguintes gráficos referentes aos sumários dos relatórios agregados recebidos:

- Tendência Diária;
- Eventos Globais;
- TOP 10 Organizações que mais reportaram;
- TOP 10 IPs Reportados: IPs de Origem dos e-mails, com indicação de quantidade de mensagens por IP;
- Análise de DMARC: Com indicação de falha;
- Eventos por Domínio: Com indicação de quantidade de mensagens recebidas x tempo e quantidade de mensagens analisadas agrupadas por domínio;



Definições de Opções - Botão de Template Claro/Escuro

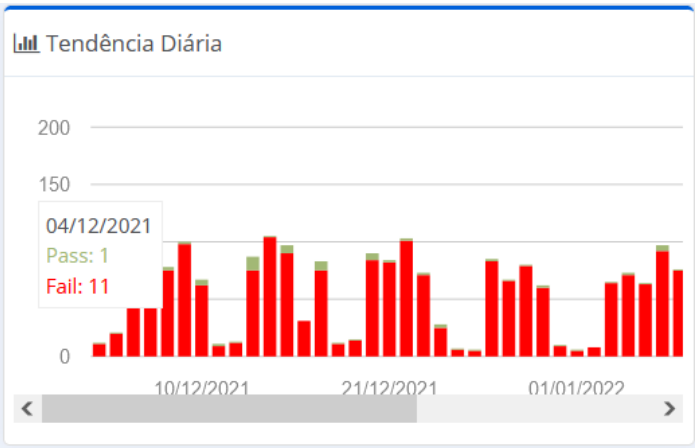
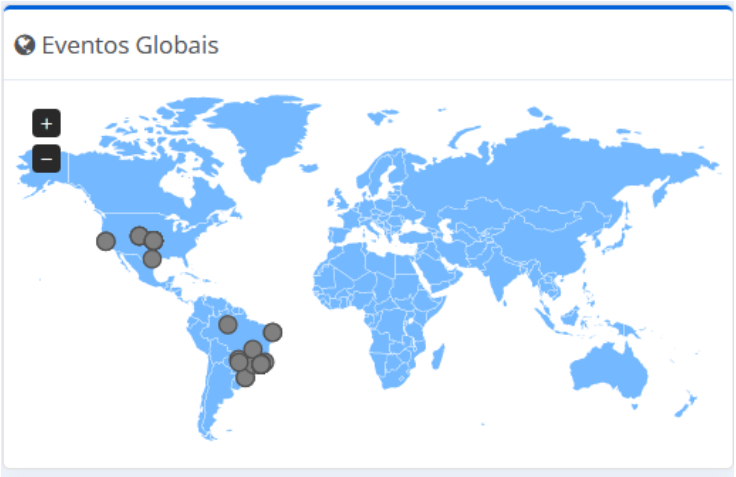
Selecione o modelo de template para a apresentação dos dados.

Opções	Definição
Claro	Quando selecionado, mostra a tela utilizando o template no modelo padrão (claro).
Escuro	Quando selecionado, mostra a tela usando o template escuro.

Legendas dos Gráficos apresentados

Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição
Data Inicial	Data inicial do período a ser selecionado
Data Final	Data final do período a ser selecionado
Tendência Diária	Indica falhas de DMARC por data, dessa forma é possível saber quando ocorreu eventual ataque usando o seu domínio.

	
Eventos Globais	Indica a região/país de origem das maiores falhas de DMARC usando o seu domínio. 
TOP 10 IP's Reportados	Indicação dos dez IP's principais atacantes que originaram falhas de DMARC usando o seu domínio.

Top 10 IPs Reportados

Rank	IP/Reverso	País
1	189.75.117.170 smtp.cassi.com.br	
2	200.169.19.28 mail.trensurb.gov.br	
3	209.85.220.41 mail-sor-f41.google.com	
4	187.108.197.188 mail.gtpn.com.br	
5	187.63.160.4 mli-mta-002.bitcom.psi.br	
6	187.63.160.25 mli-mta-001.bitcom.psi.br	
7	161.148.50.195 mli-02.serpro.gov.br	
8	161.148.50.196 mli-03.serpro.gov.br	
9	187.108.197.243 smtp01.mlicloud.com	
10	161.148.50.198 mli-05.serpro.gov.br	

Ao clicar sobre o IP, é apresentada a tela indicando os seguintes dados:

- Quantas ocorrências que o mesmo IP (sumário) teve sobre as plataformas que mandaram os XMLs para o report do DMARC;
- Reputação Global do IP;
- Reputação Local;
- Geolocalização;
- Qual dos protocolos de segurança teve sucesso ou falha (SPF, DKIM, DMARC), com indicação de percentual sobre esses índices;

Ao clicar no botão Visualizar Tudo, é apresentada uma tabela por IP, indicando o protocolo comprometido em relação aos IPs que mandaram os e-mails com falha.

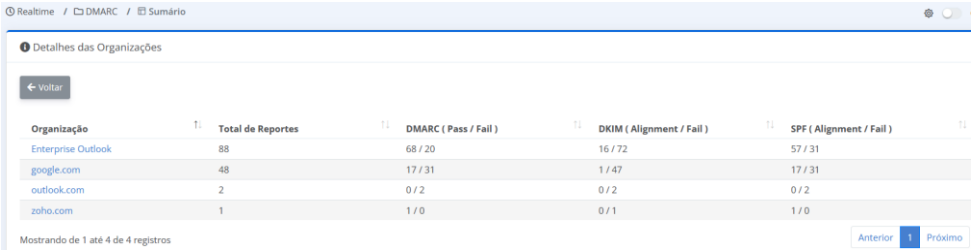
Realtime / DMARC / Sumário

Detalhes dos Ips (13/08/2024 até 20/08/2024)
Período: 13/08/2024 - 20/08/2024

Voltar

Pesquisar

IP	Total de Reportes	DMARC (Pass / Fail)	DKIM (Alignment / Fail)	SPF (Alignment / Fail)
161.148.50.201	1	0 / 1	0 / 1	0 / 1
161.148.50.205	1	0 / 1	0 / 1	0 / 1
177.124.111.207	4	0 / 4	0 / 4	0 / 4
186.232.245.70	6	0 / 6	0 / 6	0 / 6
186.232.245.71	4	0 / 4	0 / 4	0 / 4
187.108.197.102	6	6 / 0	6 / 0	6 / 0
187.108.197.103	8	8 / 0	8 / 0	8 / 0
187.63.160.25	6	0 / 6	0 / 6	0 / 6
187.63.160.3	6	0 / 6	0 / 6	0 / 6
187.63.160.4	2	0 / 2	0 / 2	0 / 2
200.208.187.10	14	14 / 0	14 / 0	0 / 14
209.85.128.202	2	2 / 0	0 / 2	2 / 0

TOP 10 Organizações que mais reportaram	Quais empresas/provedores de serviços que mais apresentaram falhas de DMARC com uso do seu domínio. Ao clicar em Visualizar Tudo, é apresentada a tabela indicado as organizações que geraram os reports, indicando por organização: • Total de Reports; • Falha de DMARC; • Falha de DKIM; • Falha de SPF;  Realtime / DMARC / Sumário Detalhes das Organizações Voltar Mostrando de 1 até 4 de 4 registros Anterior 1 Próximo
Análise de DMARC	Relação de aumento e redução na falha de DMARC em comparação com o mesmo período anterior.
Eventos por Domínio	Número de falhas de DMARC, agrupadas por domínios que mandaram os relatórios, separados por falha de: • DMARC;

Organização	Total de Reportes	DMARC (Pass / Fail)	DKIM (Alignment / Fail)	SPF (Alignment / Fail)
Enterprise Outlook	88	68 / 20	16 / 72	57 / 31
google.com	48	17 / 31	1 / 47	17 / 31
outlook.com	2	0 / 2	0 / 2	0 / 2
zoho.com	1	1 / 0	0 / 1	1 / 0

- DKIM;
- SPF;

Eventos Por Domínio

Domínio	Total de Reportes	DMARC(Pass / Fail)	Dkim(Alignment / Fail)	SPF(Alignment / Fail)
gtpn.com.br	93	50 / 43	50 / 43	50 / 43
hscbrasil.com.br	3006	48 / 2958	24 / 2982	32 / 2974
hsclabs.com	50	30 / 20	0 / 50	30 / 20
hsclatam.com	2	0 / 2	0 / 2	0 / 2

Ao selecionar um domínio, você poderá ver todos os IP's que mandaram e-mails usando o domínio selecionado, dessa forma, poderá visualizar quais os atacantes (IPs) que utilizam o domínio referido, bem como quais protocolos de segurança comprometidos (DMARC, DKIM e SPF).

Realtime / DMARC / Sumário

Domínio - hscbrasil.com.br
Período: 13/08/2024 - 20/08/2024

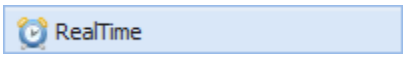
Voltar

Pesquisar

IP	Total de Reportes	DMARC (Pass / Fail)	DKIM (Alignment / Fail)	SPF (Alignment / Fail)
161.148.50.201	1	0 / 1	0 / 1	0 / 1
161.148.50.205	1	0 / 1	0 / 1	0 / 1
177.124.111.207	4	0 / 4	0 / 4	0 / 4
186.232.245.70	6	0 / 6	0 / 6	0 / 6
186.232.245.71	4	0 / 4	0 / 4	0 / 4
187.108.197.102	6	6 / 0	6 / 0	6 / 0
187.108.197.103	8	8 / 0	8 / 0	8 / 0
187.63.160.25	6	0 / 6	0 / 6	0 / 6
187.63.160.3	6	0 / 6	0 / 6	0 / 6
187.63.160.4	2	0 / 2	0 / 2	0 / 2

Forense

Apresenta os dados do relatório forense em tempo real, ou seja, é feita a coleta das informações e apresentada na tela automaticamente.



/ DMARC / RUF – Relatório Forense

Este Dashboard traz informações referente aos relatórios forenses fornecidos pelos ISPs.

Visão geral DMARC – Relatório Forense

O **DMARC Forensic Reporting (RUF)** é um mecanismo de geração de relatórios detalhados sobre mensagens que apresentaram **falhas na validação ou no alinhamento das políticas DMARC**, permitindo ao administrador investigar individualmente as ocorrências e identificar a origem e as possíveis causas da falha.

Diferentemente dos **relatórios agregados RUA**, que apresentam informações estatísticas e consolidadas sobre um conjunto de mensagens durante determinado período, os **relatórios forenses RUF são associados a mensagens ou eventos individuais**. Dessa forma, enquanto o RUA fornece uma visão ampla do comportamento de autenticação do domínio, o RUF oferece informações mais detalhadas para **diagnóstico e investigação de ocorrências específicas**.

Os relatórios RUF são encaminhados para o endereço de e-mail definido no registro **DMARC** do domínio, conforme a configuração do mecanismo de *Forensic Reporting*. O MailInspector permite realizar a **coleta desses relatórios a partir de uma conta de correio eletrônico compatível com IMAP**, processando as informações recebidas e disponibilizando-as de forma estruturada para análise do administrador.

Análise forense das mensagens

As informações presentes nos relatórios RUF são especialmente relevantes para a investigação de **falhas de autenticação, problemas de alinhamento e possíveis tentativas de falsificação do domínio**.

Entre as informações analisadas estão os dados relacionados aos mecanismos **SPF e DKIM**, permitindo verificar se a mensagem foi autenticada corretamente e se os domínios utilizados nesses mecanismos estão devidamente alinhados com a identidade utilizada no envio.

Quando disponibilizado pelo servidor destinatário, o relatório também pode fornecer informações relacionadas à mensagem original, permitindo uma análise mais aprofundada de seu conteúdo e de seus elementos, incluindo pesquisas por **endereço IP de origem, cabeçalhos, partes do corpo da mensagem e URLs presentes no e-mail**.

O endereço IP de origem é particularmente relevante para a investigação, pois permite ao administrador identificar a infraestrutura responsável pelo envio da mensagem e avaliar se ela corresponde a uma fonte legítima autorizada pelo domínio.

Dashboard de análise forense

O MailInspector disponibiliza um **Dashboard de análise dos relatórios RUF**, permitindo visualizar e correlacionar as informações recebidas nos relatórios forenses.

Quando os dados são disponibilizados no relatório pelo servidor destinatário, o administrador pode consultar informações da mensagem original, incluindo o **corpo do e-mail e as URLs presentes na mensagem**. Isso permite realizar uma investigação mais aprofundada de mensagens que apresentaram falhas de autenticação ou alinhamento de **SPF e/ou DKIM**, bem como de outras ocorrências que tenham resultado na geração de um relatório RUF.

Essa capacidade facilita a identificação de situações como:

- Falhas de configuração de SPF;
- Falhas ou problemas de alinhamento de SPF;
- Falhas de assinatura ou validação DKIM;
- Problemas de alinhamento DKIM;
- Fontes de envio não autorizadas;
- Tentativas de **spoofing** ou falsificação do domínio;
- Mensagens potencialmente relacionadas a campanhas de phishing ou outras atividades maliciosas;
- Problemas que possam afetar a autenticação e a reputação do domínio.

Principais informações apresentadas

Entre os principais campos que podem ser disponibilizados e analisados nos relatórios de **DMARC Forensic Reporting (RUF)**, destacam-se:

- **Alinhamento de identidade:** informações relacionadas ao alinhamento das identidades utilizadas nos mecanismos SPF e DKIM;
- **Método de autenticação DMARC:** identificação do mecanismo que resultou na autenticação/alinhamento da mensagem, como SPF ou DKIM;
- **Resultado da entrega:** informação sobre o tratamento aplicado à mensagem pelo servidor destinatário;
- **DKIM Domain:** domínio utilizado na assinatura DKIM;
- **DKIM Identity:** identidade associada à assinatura DKIM;
- **DKIM Selector:** seletor utilizado para localizar a chave pública DKIM no DNS. Esses campos são relevantes quando a mensagem possui assinatura DKIM;
- **DKIM Canonicalized Header:** representação canônica dos cabeçalhos utilizada no processo de validação DKIM, quando disponibilizada;
- **DKIM Canonicalized Body:** representação canônica do corpo da mensagem utilizada no processo de validação DKIM, quando disponibilizada;
- **DNS reverso relacionado ao SPF:** informações obtidas por meio da resolução DNS reversa do endereço IP de origem, utilizadas como elemento adicional de análise;
- **Endereço IP de origem:** identificação da infraestrutura responsável pelo envio da mensagem;
- **Cabeçalhos da mensagem:** informações técnicas da mensagem, quando disponibilizadas pelo relatório;
- **Corpo da mensagem e URLs:** conteúdo da mensagem e seus respectivos endereços, quando fornecidos no relatório e conforme as informações disponibilizadas pelo servidor destinatário.

Importância para segurança e compliance

A análise forense dos relatórios RUF complementa as informações obtidas por meio dos **relatórios agregados RUA**. Enquanto o RUA permite identificar tendências, volumes e padrões de autenticação em larga escala, o RUF possibilita aprofundar a investigação de **ocorrências individuais**.

A combinação das duas modalidades de relatório proporciona uma visão mais completa da segurança do domínio: o **RUA permite identificar onde existe um problema**, enquanto o **RUF fornece informações adicionais para investigar uma ocorrência específica e compreender sua origem e características**.

Dessa forma, o MailInspector auxilia o administrador na identificação e correção de problemas de configuração de **DMARC, SPF e DKIM**, na identificação de fontes legítimas de envio e na investigação de possíveis tentativas de falsificação ou uso indevido do domínio.

Importante salientar que quem tem acesso ao módulo de análise forense e analítico do DMARC é somente o administrador ou administrador customizado, com permissão para acesso ao módulo.

Definições de Opções - Botão de Template Claro/Escuro

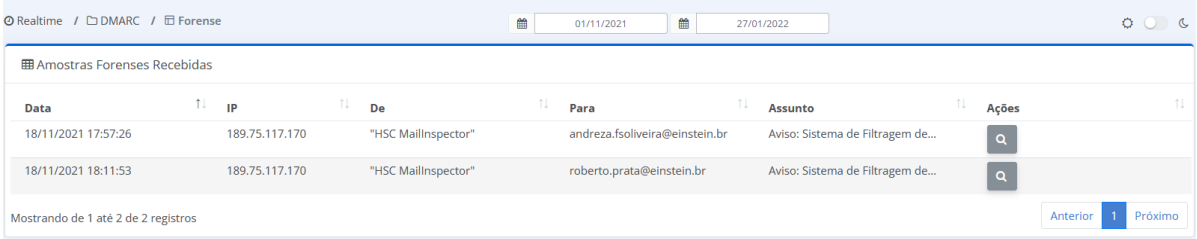
Selecione o modelo de template para a apresentação dos dados.

Opções	Definição
Claro	Quando selecionado, mostra a tela utilizando o template no modelo padrão (claro).
Escuro	Quando selecionado, mostra a tela usando o template escuro.

Legendas dos Gráficos apresentados

Estas informações descrevem as opções disponíveis nesta página.

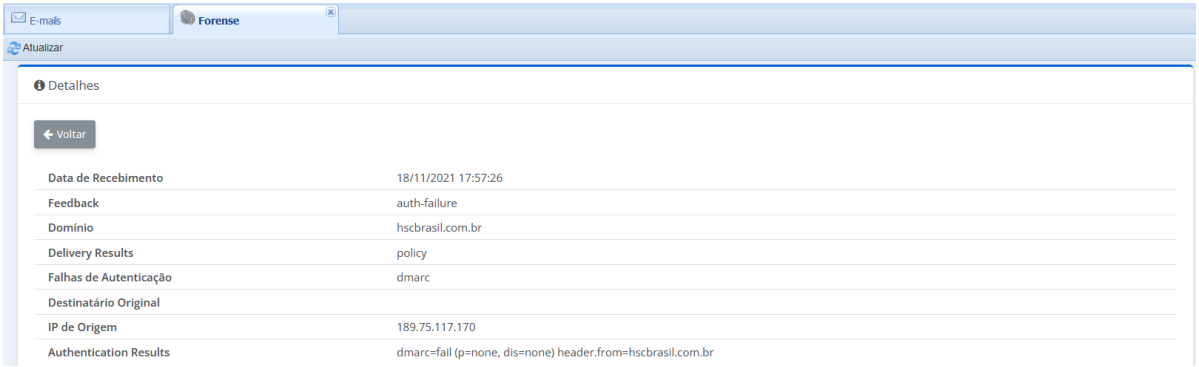
Opções	Definição
Data Inicial	Data inicial do período a ser selecionado
Data Final	Data final do período a ser selecionado
Amostras Forenses Recebidas	Relatório referente a análise das amostras recebidas pelo RUF **Data:** Data do recebimento da amostra **IP:** IP de Origem do e-mail **De:** Display Name do e-mail (FROM) **Para:** E-mail destino **Assunto:** Assunto indicado no e-mail **Ações:** Maiores detelhes sobre o e-mail e as ações tomadas sobre ele



Legendas dos Dados ao Clicar no botão Ação

Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição
Data de Recebimento	Data do recebimento do e-mail
FeedBack	Motivo do registro da falha
Domínio	Domínio de Origem
Delivery Results	Resultado da política utilizada
Falhas de Autenticação	Indica possíveis falhas de protocolo de proteção ao e-mail (SPF/DKIM/DMARC)
Destinatário Original	Destinatário do e-mail
IP de Origem	IP de onde veio o e-mail
Authentication Results	Resultado da análise do DMARC

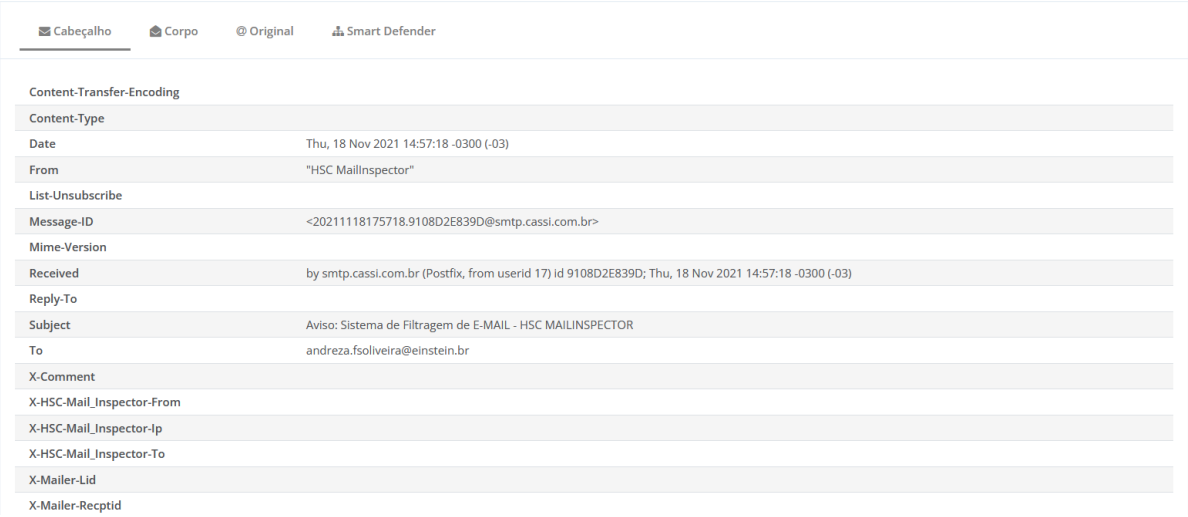


Legendas dos Dados ao Clicar no botão Cabeçalho

Indica os dados de Cabeçalho da Mensagem.

Opções	Definição
Content-Transfer-Encoding	Encode utilizado para a transferência do e-mail (Base 32 ou Base 64)
Content-Type	Tipo de Conteúdo
Date	Data do E-mail
From	E-mail de Origem, pode-se apresentar também o Display Name do E-mail do Campo FROM

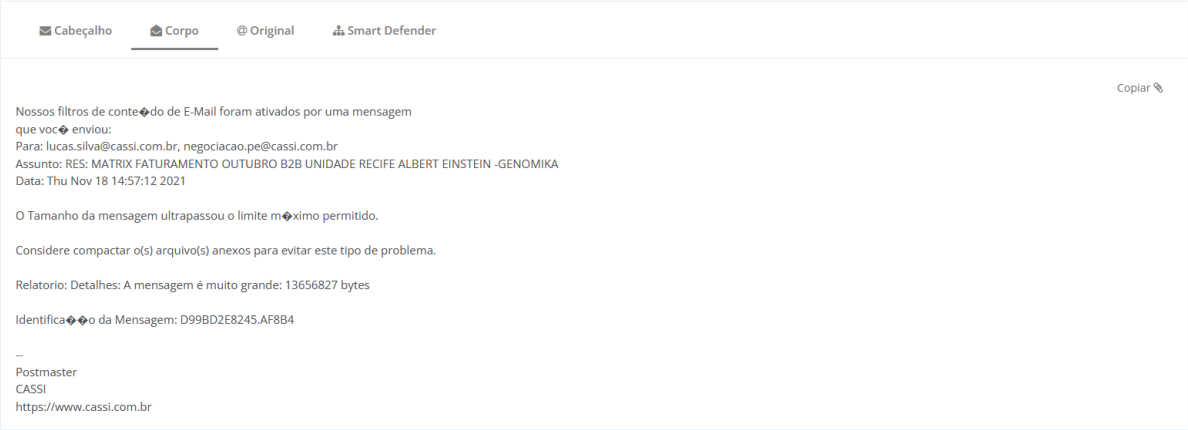
List-Unsubscribe	Remoção do e-mail em listas
Message-ID	Identificador único da mensagem
Mime-Version	Versão do Mime-Type
Received	Resumo de dados de recebimento do e-mail. Data e indicação de Origem do e-mail. Geralmente também indica qual o sistema do servidor de e-mail (PostFix, SandMail, etc)
Reply-To	FROM do Envelope
Subject	Assunto do e-mail
To	TO do Envelope
X-Alguma coisa	Campos começados com o caracter “X”, por convenção, são campos customizados incluídos no e-mail por algum sistema ou por alguém, muitas vezes contendo informações utilizadas pelo sistema que inseriu o campo.



Legendas dos Dados ao Clicar no botão Corpo

Indica os dados do Corpo da Mensagem.

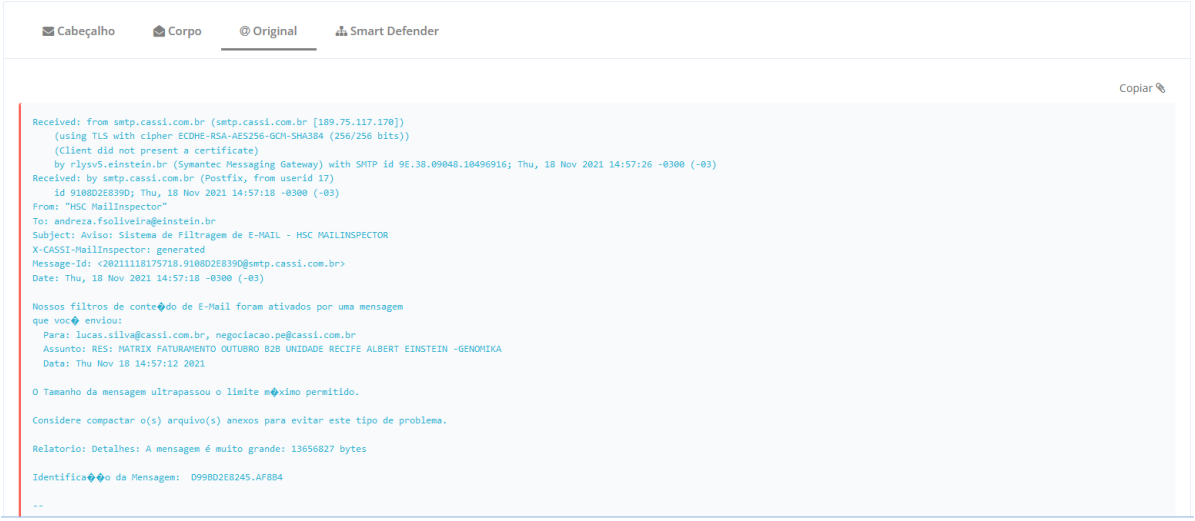
Opções	Definição
Copiar	Permite efetuar cópia do conteúdo do corpo do e-mail, para a memória do computador



Legendas dos Dados ao Clicar no botão Original

Indica os dados de Cabeçalho e todo o Corpo da Mensagem.

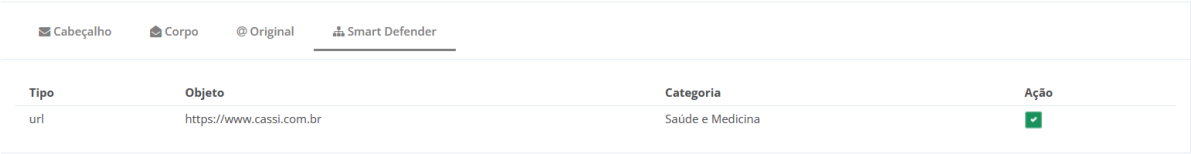
Opções	Definição
Copiar	Permite efetuar cópia tanto do Cabeçalho, quanto do corpo do e-mail, para a memória do computador



Legendas dos Dados ao Clicar no botão SmartDefender

Indica os dados do resultado da análise dos links contidos no e-mail.

Opções	Definição
Tipo	Se é URL ou se é Anexo
Objeto	Nome do Objeto (URL ou Arquivo)
Categoria	Sendo URL, indica a categoria da URL
Ação	Qual ação tomada, se a URL/Arquivo estava OK ou se estava contaminada ou ainda se foi bloqueado pelo como blacklist



Telas de indicação de relatórios RUF(Forenses) e Análise de mensagem com indicação de conteúdo, resposta do módulo SmartDefender

Portal

O Portal apresenta um resumo gráfico em tempo real das principais estatísticas de filtragem de e-mails.

Visão Dashboard

O **HSC MailInspector** disponibiliza um Dashboard com as principais **estatísticas de filtragem e segurança do ambiente de correio eletrônico**, permitindo ao administrador acompanhar, em tempo real, o comportamento e o volume das mensagens processadas pelo sistema.

Por meio de **gráficos e indicadores visuais**, o administrador obtém uma visão consolidada do fluxo de e-mails e dos principais eventos de filtragem, incluindo:

- Destinatários inválidos;
- Mensagens bloqueadas por reputação;
- SPAM identificado e bloqueado;
- Vírus e Malware detectados;
- Mensagens consideradas legítimas e entregues, com possibilidade de análise por **domínio e endereço IP**;
- Mensagens bloqueadas por limites de conexão;
- Mensagens bloqueadas em decorrência de políticas de limite de envio e recebimento;
- Conexões rejeitadas com base em mecanismos de reputação, incluindo **RBL (Real-time Blackhole List)**;
- Volume de dados recebidos e enviados, em bytes, com detalhamento por domínio e endereço IP.

A solução permite ainda analisar a **origem e o destino do tráfego de e-mail**, possibilitando identificar quais domínios e endereços IP apresentam maior volume de envio ou recebimento de mensagens e dados. Essas informações auxiliam o administrador na identificação de padrões de tráfego, comportamentos atípicos e possíveis eventos que demandem investigação.

A visualização do Dashboard é **atualizada em tempo real** e permite a aplicação de diferentes intervalos de análise, possibilitando consultar os indicadores referentes à **última hora, último dia, última semana ou último mês**.

Dessa forma, o Dashboard proporciona uma visão centralizada e dinâmica do ambiente de e-mail, facilitando o **monitoramento operacional, a análise do fluxo de mensagens, a identificação de ameaças e a tomada de decisões de segurança**.

O portal apresenta os dados dos e-mails do dia, desde às 00:00h, até o presente momento.

Volume de E-mails

Este gráfico mostra um resumo do tráfego de e-mails do dia, indicados por hora

Mensagens Eviadas

Quantidades de mensagens enviadas no dia e a quantidade de dado trafegado

Mensagens Recebidas

Quantidades de mensagens recebidas no dia e a quantidade de dado trafegado

Bounce

Quantidades de mensagens retornadas como bounce mail e a quantidade de dado trafegado

Interno

Quantidades de mensagens internas e a quantidade de dado trafegado

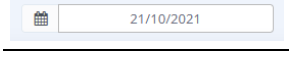
Definições de Opções - Botão de Template Claro/Escuro

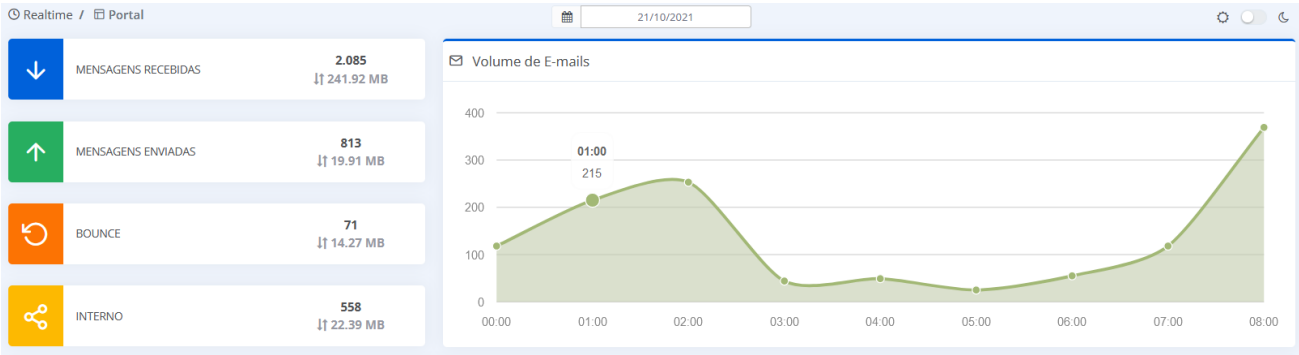
Selecione o modelo de template para a apresentação dos dados.

Opções	Definição
Claro	Quando selecionado, mostra a tela utilizando o template no modelo padrão (claro).
Escuro	Quando selecionado, mostra a tela usando o template escuro.

Definições de Opções – Data do Portal

Selecione a data dos dados do Portal

Opções	Definição
	Selecione a data a ser filtrado pelo Portal.



Tela de visualização do Portal por tipo de e-mails

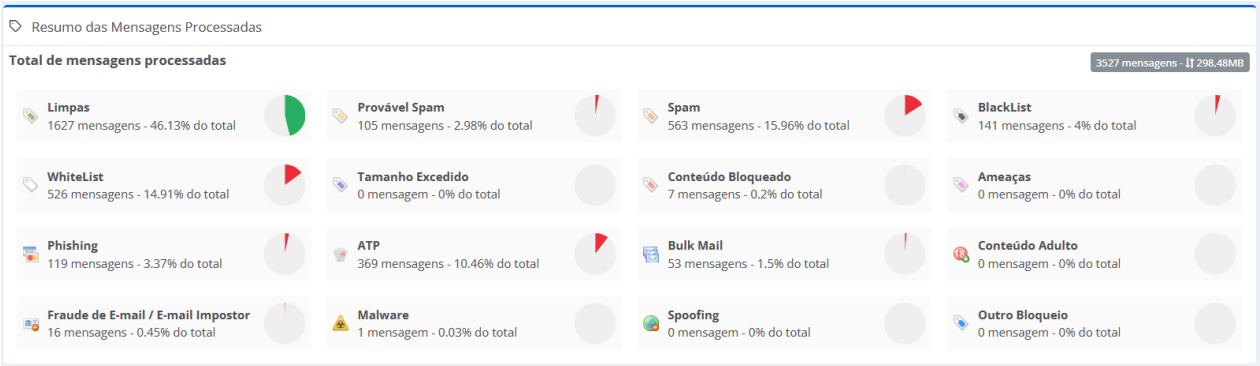
Tráfego de Mensagens por Tipo

Mostra um sumario dos e-mails com quantidade e volume classificados com as seguintes classificações

Opções	Definição
Mensagens Processadas	Total de Mensagens processadas pelo HSC MailInspector.
Com Criptografia	Total de e-mails que foram criptografados Indicação de percentual no período de quantas mensagens foram com criptografia
Ameaças	Total de e-mails que foram identificados com algum a Ameaça

	Indicação de percentual no período de quantas mensagens foram detectadas como ameaças
Block List	Total de e-mails na Block List Indicação de percentual no período de quantas mensagens foram detectadas como pertencentes a block list
Allow List	Total de e-mails na Allow List Indicação de percentual no período de quantas mensagens foram detectadas como pertencentes a allow list
Tamanho Excedido	Total de e-mails com tamanho Excedido Indicação de percentual no período de quantas mensagens foram detectadas como tamanho excedido
Conteúdo Bloqueado	Total de e-mails com Conteúdo Bloqueado Indicação de percentual no período de quantas mensagens foram detectadas com conteúdo bloqueado
Outro Bloqueio	Total de e-mails com Outros Bloqueios (podendo ser por exemplo e-mails com anexos criptografados com senha) Indicação de percentual no período de quantas mensagens foram detectadas com outro tipo de bloqueio
SPAM	Total de e-mails SPAM Indicação de percentual no período de quantas mensagens foram detectadas como spam
Provável SPAM	Total de e-mails classificados como Provável SPAM Indicação de percentual no período de quantas mensagens foram detectadas como Provável SPAM
Phishing	Total de e-mails Phishing Indicação de percentual no período de quantas mensagens foram detectadas como phishing
Limpas	Total de e-mails confiáveis Indicação de percentual no período de quantas mensagens foram analisadas como limpas
ATP	Total de e-mails indicados como ataques persistentes Indicação de percentual no período de quantas mensagens foram classificadas como ATP (ataque persistente)
Bulk Mail	Total de e-mails indicados como bulk mail Indicação de percentual no período de quantas mensagens foram detectadas como Bulk Mail
Conteúdo Adulto	Total de e-mails com conteúdo adulto Indicação de percentual no período de quantas mensagens foram detectadas com Conteúdo Adulto
Controle de Surto/Comportamento Anômalo	Total de e-mails que apresentaram sinais de surto, tais como excesso de e-mails com vírus de um único IP, entre outras características

	Indicação de percentual no período de quantas mensagens foram ativadas pelo controle de surto/comportamento anômalo
Fraude de E-mail/E-mail Impostor	Total de e-mails com características de fraude Indicação de percentual no período de quantas mensagens foram detectadas como E-mail Fraude/E-mail Impostor
Malware	Total de e-mail com ameaças anexas Indicação de percentual no período de quantas mensagens foram detectadas com conteúdo de malware
Spoofing	Total de e-mail que utilizaram técnicas de Spoofing, tais como e-mail de entrada fingindo remetente com o domínio da própria empresa Indicação de percentual no período de quantas mensagens foram detectadas com spoofing



Tela de visualização do Portal por Mensagens Processadas, separadas por qualidade da mensagem

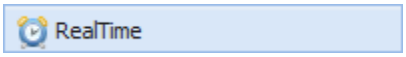
Menu - Painel de Controle

Block List

Define as regras de bloqueio configuradas pelo administrador ou usuário para impedir o recebimento ou o encaminhamento de mensagens provenientes de origens ou destinadas a determinados endereços.
As regras podem ser aplicadas tanto ao **remetente quanto ao destinatário**, utilizando diferentes critérios de identificação e correspondência:

- **Domínios**;
- **Subdomínios**;
- **Endereços de e-mail**;
- **Endereços IP**;
- **Redes e sub-redes**;
- **Expressões regulares (Regex)**;
- **Hostname**, de forma parcial ou completa;
- **Nome DNS reverso (PTR)**.

Essa abordagem permite estabelecer políticas de bloqueio granulares e flexíveis, possibilitando desde restrições específicas para determinados endereços de e-mail até bloqueios abrangentes por domínio, rede, hostname ou padrões definidos por expressão regular.



/ Block List (lista de e-mails não confiáveis)

Visão geral da Block List

O item Block List é utilizado para referenciar uma lista de e-mails, nomes parciais de domínios ou usuários, hostname completo ou parcial, nome reverso, domínios, endereços IP ou mesmo wildcards (spam@*) e expressões regulares reconhecidos como fontes de SPAM. Este recurso é utilizado para bloquear mensagens de origens que foram confirmadas, pelo administrador ou pelo usuário, como sendo fontes de SPAM. Permite a administração pelo usuário, ou seja, o usuário pode adicionar ou remover itens que somente impactem os seus endereços de e-mails, dessa forma é possível ter duas formas de administração, a forma Global (pelo administrador) e a forma individual (por usuário).

Obs: A **Allow list TEM PRECEDÊNCIA SOBRE A BLOCK LIST!**

```
Expressão Regular: ^(root|teste)@.*\.com\.br$
Domínio: hscbrasil.com.br
E-mail suporte@hscbrasil.com.br
IP: 192.168.1.1
Rede: 192.168.1.*
```

Dica:
Coringa para indicação de qualquer caracter (antes ou depois) no RegEx:

.*

Por exemplo, quero bloquar ou liberar qualquer o domínio **hscbrasil.com.br** e qualquer subdomínio que vier antes do string **hscbrasil.com.br**, ficaria:

.*hscbrasil.com.br

Definições de Opções – Block List

Colunas disponíveis na opção de Block List.

Coluna	Definição
De	E-mail de origem
Para	E-mail destino
Data	Data de criação da entrada da lista
Comentário	Comentário/motivo de criação do registro na block list
Tipo	Indicação de quem criou o registro e o status dele, ficando entre: • Administrador; • Usuário; • Se o registro é Bloqueado para Edição;

Estas informações descrevem as opções disponíveis no menu da block list.

Opções	Definição
	Indica quem criou as regras, selecione uma das opções disponíveis: • Todos; • Administradores; • Usuários;
Pesquisar	Quando clicado, aplica o filtro informado na caixa de pesquisa rápida aos registros da block list.
Limpar	Quando clicado, remove os filtros informados da caixa de pesquisa rápida e recarrega todos os registros da block list.
Pesquisa Avançada	Permite efetura busca avançada na lista de block list.
Adicionar	Cadastra um novo registro na block list. Quando clicado, abre a caixa de diálogo **Adicionar/Editar Block List**.
Editar	Edita as configurações de um registro existente. Quando clicado, abre a caixa de diálogo **Adicionar/Editar Block List**.
Remover	Quando clicado, exclui o registro selecionado.

Definições de Pesquisa Avançada

Seguem abaixo as buscas possíveis quando ativada a pesquisa avançada da block list.

Opções	Definição
De	Insira a informação para que a pesquisa seja efetuada pelo filtro do campo DE
Para	Insira a informação para que a pesquisa seja efetuada pelo filtro do campo PARA
Tipo	Ativa o filtro verificando quem criou o registro, se é **Usuário** ou **Administrador** **Usuário:** Apresenta somente os registros criados pelos Usuários; **Administrador:** Apresenta somente os criados feitos pelo Administrador;

Usuário	Filtra somente os registros criados por um determinado usuário.
Comentário	Busca por palavra chave contido no campo comentário.
Período de Tempo	Filtra os registros por um determinado período. **Data Inicial:** Entre com a data inicial do filtro; **Data Final:** Entre com a data final do filtro;

Definições de Opções - Adicionar/Editar Block List

Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição
Salvar	Quando clicado, grava as configurações realizadas.
Cancelar	Quando clicado, cancela a ação.
De	Informe o endereço de e-mail completo do remetente, o domínio, IP, Faixa de IPs ou selecione o grupo Todos(*). O item **Todos(*)** ou caractere ***** são valores coringa dentro do HSC MailInspector, sempre que um destes valores for utilizado, estamos nos referindo a todos os usuários. Utilizando este coringa no campo **De**, significa o mesmo que "quando a mensagem vier de qualquer usuário fora do sistema". É possível fazer entrada deste campo por diversos tipos de entrada, dentre eles: **Expressão Regular:** ^(root|teste)@.*\.com\.br$ **Dominio:** hscbrasil.com.br **E-mail:** suporte@hscbrasil.com.br **IP:** 192.168.1.1 **Rede:** 192.168.1.*
Para	Informe o endereço de e-mail completo do destinatário, o domínio ou selecione o grupo Todos(*). O item **Todos(*)** ou caractere ***** são valores coringa dentro do HSC MailInspector, sempre que um destes valores for utilizado, estamos nos referindo a todos os usuários. Utilizando este coringa no campo **Para**, significa o mesmo que "quando a mensagem for destinada a qualquer usuário do sistema". É possível fazer entrada deste campo por diversos tipos de entrada, dentre eles: **Expressão Regular:** ^(root|teste)@.*\.com\.br$ **Dominio:** hscbrasil.com.br **E-mail:** suporte@hscbrasil.com.br **IP:** 192.168.1.1 **Rede:** 192.168.1.*
Comentário	É possível efetuar a entrada de um comentário referente a inclusão do registro como block list.

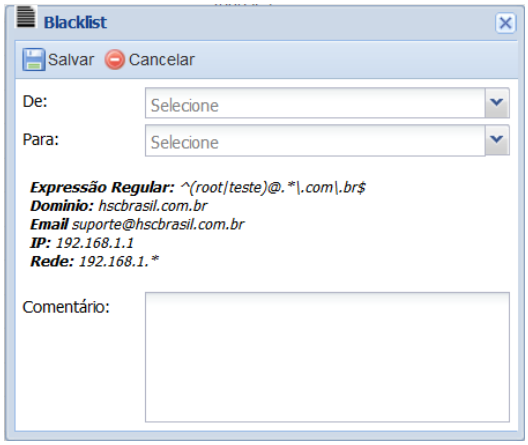
Definições de Opções – Exportar/Importar

É possível efetuar a exportação e importação dos dados contidos na lista de block list (configuração), nos formatos CSV e XML, para que seja utilizado posteriormente ou para consulta.

Opções	Definição
Exportar	Exporta a lista contida na Block List em arquivo CSV e/ou XML
Importar	Importa a lista de Block List no formato CSV e/ou XML

O formato exportado/importado no modelo CSV fica:

"De";"Para";
"spammer@roi360ne.com.br";"destinatario@hscbrasil.com.br";
"teste@criminoso.com.br";"fernanda@hscbrasil.com.br";
"fake-mail@spam.com.br";"romulo@hscbrasil.com.br";



Tela de entrada de registro de block list

O formato exportado/importado no modelo XML fica:

```
<rows><row><from_address>endereço_origem</from_address><to_address>endereço_destino</to_address></row><row><from_address>IP_origem</from_address><to_address>default</to_address></row></rows>
```

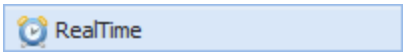
Obs: **default** indica que é para TODOS.

Allow List

Define as regras de liberação configuradas pelo administrador ou usuário para efetuar o recebimento ou o encaminhamento de mensagens provenientes de origens ou destinadas a determinados endereços.
As regras podem ser aplicadas tanto ao **remetente quanto ao destinatário**, utilizando diferentes critérios de identificação e correspondência:

- **Domínios**;
- **Subdomínios**;
- **Endereços de e-mail**;
- **Endereços IP**;
- **Redes e sub-redes**;
- **Expressões regulares (Regex)**;
- **Hostname**, de forma parcial ou completa;
- **Nome DNS reverso (PTR)**.

Essa abordagem permite estabelecer políticas de lista de confiáveis granulares e flexíveis, possibilitando desde liberações específicas para determinados endereços de e-mail até liberação mais abrangente por domínio, rede, hostname ou padrões definidos por expressão regular.



/ Allow List (lista de e-mails confiáveis)

Visão geral da Allow List

O item Allow List é utilizado para referenciar uma lista de e-mails, nomes parciais de domínios ou usuários, hostname completo ou parcial, nome reverso, domínios, endereços IP ou mesmo wildcards (spam@*) e expressões regulares previamente aprovados pelo administrador ou pelo usuário, que não serão submetidos aos filtros de SPAM do HSC MailInspector. Permite a administração pelo usuário, ou seja, o usuário pode adicionar ou remover itens que somente impactem os seus endereços de e-mails, dessa forma é possível ter duas formas de administração, a forma Global (pelo administrador) e a forma individual (por usuário).

Obs: Uma vez que um e-mail case na Allow List ele não será analisado somente pela Engine de SPAM, os demais filtros serão normalmente processados ex: Antivírus, AntiPhishing, Controle de Conteúdo, etc.

Obs: A **Allow List TEM PRECEDÊNCIA SOBRE A BLOCK LIST!**

```
Expressão Regular: ^(root|teste)@.*\.com\.br$
Domínio: hscbrasil.com.br
E-mail suporte@hscbrasil.com.br
IP: 192.168.1.1
Rede: 192.168.1.*
```

Dica:
Coringa para indicação de qualquer caracter (antes ou depois) no RegEx:

.*

Por exemplo, quero bloquar ou liberar qualquer o domínio **hscbrasil.com.br** e qualquer subdomínio que vier antes do string **hscbrasil.com.br**, ficaria:

.*hscbrasil.com.br

Definições de Opções – Allow List

Colunas disponíveis na opção de Allow List.

Coluna	Definição
De	E-mail de origem
Para	E-mail destino
Data	Data de criação da entrada da lista
Comentário	Comentário/motivo de criação do registro na Allow List
Tipo	Indicação de quem criou o registro e o status dele, ficando entre: • Administrador; • Usuário; • Se o registro é Bloqueado para Edição;

Estas informações descrevem as opções disponíveis na parte da allow list.

Opções	Definição
	Indica quem criou as regras, selecione uma das opções disponíveis: • Todos; • Administradores; • Usuários;
Pesquisar	Quando clicado, aplica o filtro informado na caixa de pesquisa rápida aos registros da allow list.
Limpar	Quando clicado, remove os filtros informados da caixa de pesquisa rápida e recarrega todos os registros da allow list.
Pesquisa Avançada	Permite efetuar busca avançada na lista da allow list.
Adicionar	Cadastra um novo registro na Allow List. Quando clicado, abre a caixa de diálogo **Adicionar/Editar Allow List**.
Editar	Edita as configurações de um registro existente. Quando clicado, abre a caixa de diálogo **Adicionar/Editar Allow List**.
Remover	Quando clicado, exclui o registro selecionado.

Definições de Pesquisa Avançada

Seguem abaixo as buscas possíveis quando ativada a pesquisa avançada da allow list.

Opções	Definição
De	Insira a informação para que a pesquisa seja efetuada pelo filtro do campo DE
Para	Insira a informação para que a pesquisa seja efetuada pelo filtro do campo PARA
Tipo	Ativa o filtro verificando quem criou o registro, se é **Usuário** ou **Administrador** **Usuário:** Apresenta somente os registros criados pelos Usuários; **Administrador:** Apresenta somente os criados feitos pelo Administrador;

Usuário	Filtra somente os registros criados por um determinado usuário.
Comentário	Busca por palavra chave contido no campo comentário.
Período de Tempo	Filtra os registros por um determinado período. **Data Inicial:** Entre com a data inicial do filtro; **Data Final:** Entre com a data final do filtro;

Definições de Opções - Adicionar/Editar Allow List

Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição
Salvar	Quando clicado, grava as configurações realizadas.
Cancelar	Quando clicado, cancela a ação.
De	Informe o endereço de e-mail completo do remetente, o domínio, IP, Faixa de IPs ou selecione o grupo Todos(*). O item **Todos(*)** ou caractere ***** são valores coringa dentro do HSC MailInspector, sempre que um destes valores for utilizado, estamos nos referindo a todos os usuários. Utilizando este coringa no campo **De**, significa o mesmo que "quando a mensagem vier de qualquer usuário fora do sistema". É possível fazer entrada deste campo por diversos tipos de entrada, dentre eles: **Expressão Regular:** ^(root|teste)@.*\.com\.br$ **Domínio:** hscbrasil.com.br **E-mail:** suporte@hscbrasil.com.br **IP:** 192.168.1.1 **Rede:** 192.168.1.*
Para	Informe o endereço de e-mail completo do destinatário, o domínio ou selecione o grupo Todos(*). O item **Todos(*)** ou caractere ***** são valores coringa dentro do HSC MailInspector, sempre que um destes valores for utilizado, estamos nos referindo a todos os usuários. Utilizando este coringa no campo **Para**, significa o mesmo que "quando a mensagem for destinada a qualquer usuário do sistema". É possível fazer entrada deste campo por diversos tipos de entrada, dentre eles: **Expressão Regular:** ^(root|teste)@.*\.com\.br$ **Domínio:** hscbrasil.com.br **E-mail:** suporte@hscbrasil.com.br **IP:** 192.168.1.1 **Rede:** 192.168.1.*
Comentário	É possível efetuar a entrada de um comentário referente a inclusão do registro como allow list.

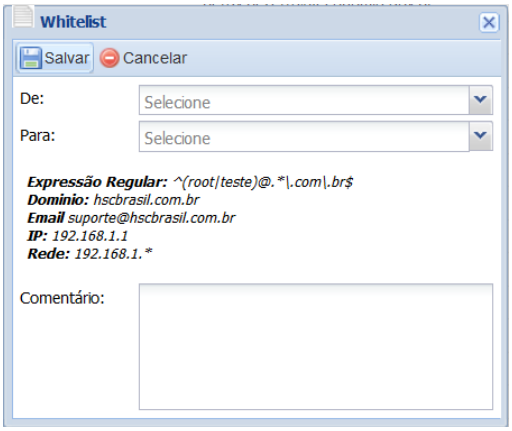
Definições de Opções – Exportar/Importar

É possível efetuar a exportação e importação dos dados contidos na lista de allow list (configuração), nos formatos CSV e XML, para que seja utilizado posteriormente ou para consulta.

Opções	Definição
Exportar	Exporta a lista contida na Allow List em arquivo CSV e/ou XML
Importar	Importa a lista da allow list no formato CSV e/ou XML

O formato exportado/importado no modelo CSV fica:

"De";"Para";
"nf@magazine.com.br";"destinatario@hscbrasil.com.br";
"comercial@canon.com.br";"fernanda@hscbrasil.com.br";
"negocios@dell.com.br";"romulo@hscbrasil.com.br";



Tela de entrada de registro de allow list

O formato exportado/importado no modelo XML fica:

```
<rows><row><from_address>endereço_origem</from_address><to_address>endereço_destino</to_address></row><row><from_address>IP_origem</from_address><to_address>default</to_address></row></rows>
```

Obs: **default** indica que é para TODOS.

Menu - Gestão de Risco

O menu Gestão de Risco reúne a análise de ameaças orientada ao usuário. Enquanto os demais menus mostram o que aconteceu com as mensagens, este mostra o que aconteceu com as pessoas:

- Quem é mais visado;
- Quem interagiu com o que recebeu;
- Quais ameaças chegaram de forma coordenada;

O menu é composto por quatro telas, que se complementam e se ligam entre si.

- A Visão Geral apresenta o retrato do período;
- Perfil de Risco detalha uma pessoa;
- Inteligência de Ameaças agrupa o que chegou por campanha e por ator;
- Contas Prioritárias definem quem recebe peso maior na avaliação.

Todas as telas respeitam o ponto de acesso selecionado no topo da console e o período escolhido na própria tela, e podem ser atualizadas automaticamente em intervalos de 30 segundos, 1 minuto ou 5 minutos.

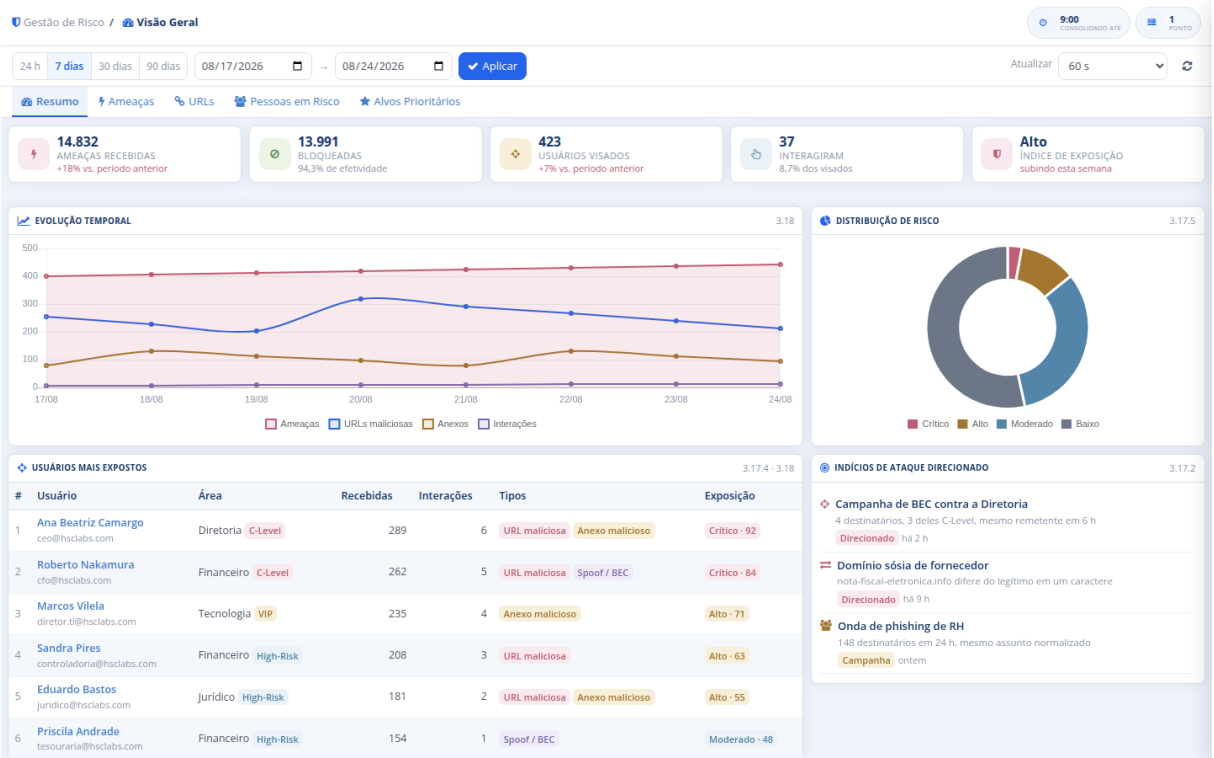
Visão Geral

Use esta página para ter o retrato da exposição do período em uma única tela. Ela responde, na ordem, quatro perguntas: qual o tamanho do problema, que tipo de ameaça chegou, o que aconteceu com as URLs maliciosas e quais pessoas foram atingidas.

O conteúdo está distribuído em cinco abas:

- Resumo — indicadores gerais do período, evolução no tempo, distribuição das pessoas por faixa de risco, ranking dos mais expostos e os alertas que merecem atenção imediata;
- Ameaças — classificação do que chegou por tipo (URL maliciosa, anexo malicioso ou ambos), por vetor de ataque e por severidade, além da matriz que cruza os três;
- URLs — quantas URLs maliciosas foram recebidas, quantas foram bloqueadas e quantas foram efetivamente acessadas, com o histórico do período, as URLs mais recorrentes e a relação de quem clicou;
- Pessoas — indicadores por usuário, ranking completo com busca e ordenação, e a dispersão que relaciona volume recebido e interação;
- Prioritárias — o mesmo recorte, restrito às contas cadastradas como prioritárias, com a comparação entre o que elas recebem e o que a base recebe.

Clicar sobre o nome de um usuário em qualquer lista abre o Perfil de Risco dessa pessoa em uma nova aba, preservando a tela atual.



Gestão de Risco - Visão Geral

Indicador de risco por usuário

O indicador de risco é calculado automaticamente e resume, em um número de 0 a 100, o quanto uma pessoa está exposta no período. Ele combina cinco componentes:

- Volume recebido — quantas ameaças chegaram para o usuário;
- Ameaças entregues — quantas dessas ameaças não foram bloqueadas, ou seja, chegaram à caixa;
- Gravidade — o peso das ameaças recebidas, segundo a severidade atribuída a cada uma;
- Interação — o que o usuário fez com o que recebeu, com peso maior para o clique que prosseguiu até o destino;
- Exposição a campanhas — quantas campanhas direcionadas atingiram o usuário.

O resultado é multiplicado pelo peso do perfil da conta, definido na tela Contas Prioritárias, e classificado em quatro faixas: Baixo (0 a 24), Moderado (25 a 49), Alto (50 a 74) e Crítico (75 a 100). A composição do cálculo é exibida na própria tela, de modo que sempre seja possível auditar porquê uma pessoa recebeu determinada pontuação.

Severidade das ameaças

A severidade é derivada da classificação que a mensagem recebeu na análise, segundo o seguinte critério:

- Crítica — vírus identificado, ameaça avançada (ATP) ou malware;
- Alta — phishing ou falsificação de remetente do próprio domínio;
- Média — domínios suspeitos, arquivos ou mensagens suspeitas, e falhas de autenticação DMARC, DKIM ou SPF;
- Baixa — spam de pontuação alta, mala direta em massa e conteúdo bloqueado por nome de arquivo.

Uma ameaça que foi entregue ao destinatário sobe uma faixa em relação à mesma ameaça que foi bloqueada: o que chegou à caixa representa exposição real, enquanto o que foi barrado representa um incidente evitado.

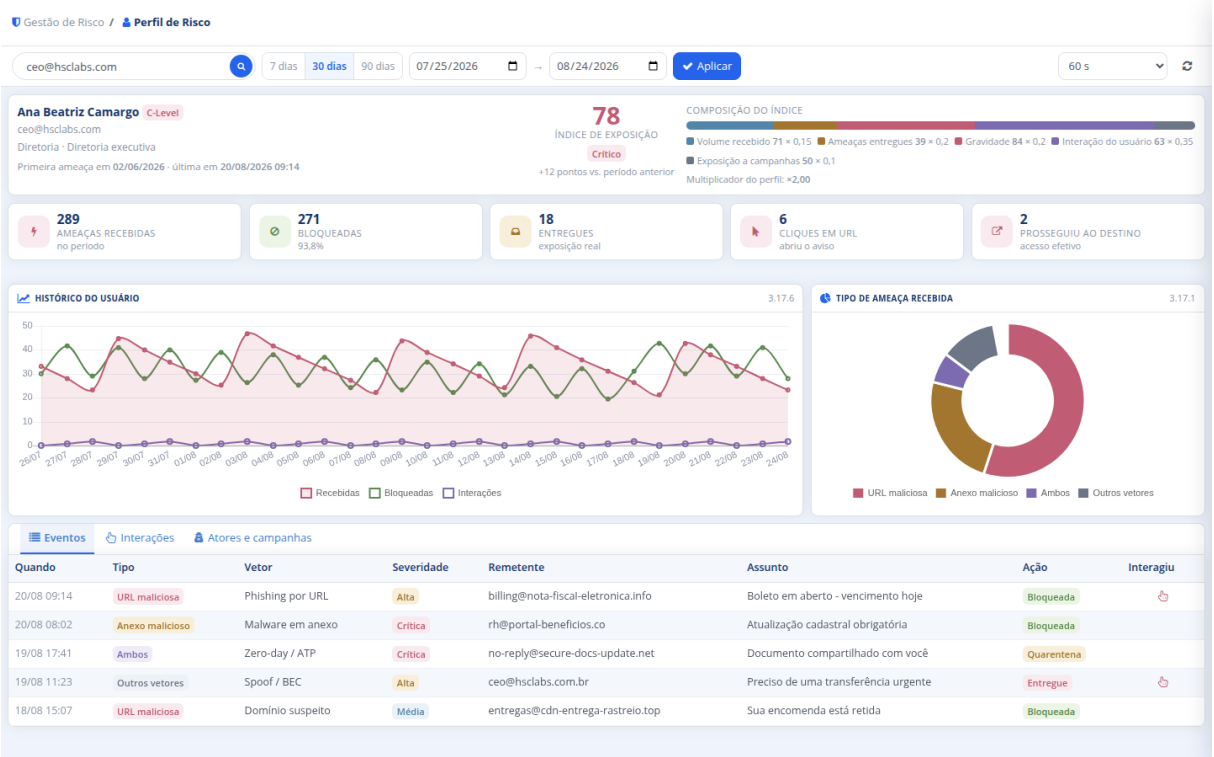
Perfil de Risco

Use esta página para investigar uma pessoa específica. Ela reúne, em um só lugar, tudo o que chegou para aquele usuário no período e tudo o que ele fez com o que recebeu.

A tela é aberta a partir de qualquer lista de usuários das demais telas do menu, ou diretamente, informando o endereço de e-mail no seletor no topo da página. O cabeçalho apresenta o indicador de risco da pessoa, o perfil da conta e a decomposição da pontuação por componente.

Além do cabeçalho, a página apresenta:

- Indicadores do período — total recebido, quanto foi bloqueado, quanto foi entregue e quantas interações houve;
- Evolução no tempo — como o volume de ameaças dirigidas ao usuário se comportou no período;
- Tipos de ameaça — a distribuição do que chegou para essa pessoa;
- Histórico de eventos — a relação das mensagens de ameaça recebidas, com data, remetente, assunto, classificação, severidade e o que aconteceu com cada uma;
- Histórico de interações — a relação cronológica dos cliques e demais interações registradas para o usuário;
- Atores e campanhas — quais remetentes e quais campanhas atingiram essa pessoa.



Gestão de Risco - Perfil de Risco

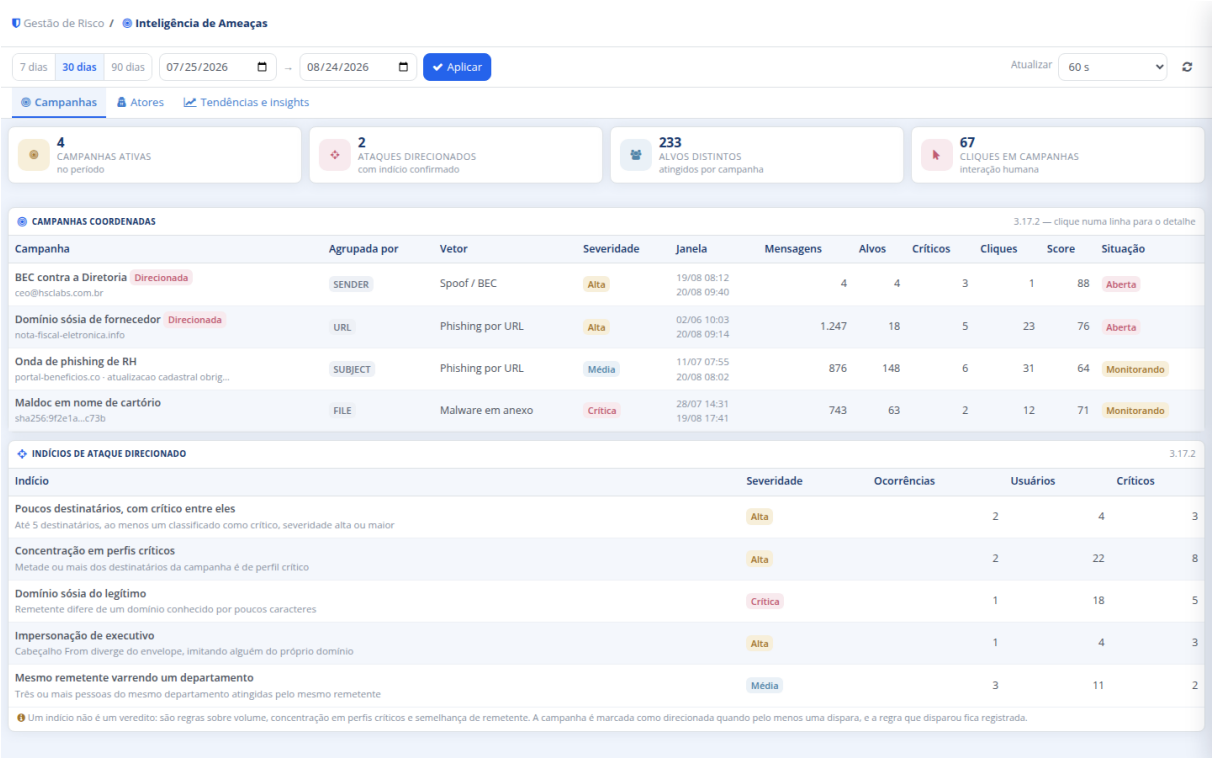
Nas mensagens com mais de um destinatário, o registro de clique é atribuído ao conjunto de destinatários e não a uma pessoa isolada. Isso é uma característica do rastreamento de links, que reescreve um único corpo de mensagem para todos os destinatários da mesma entrega. Esses casos aparecem identificados como interação de atribuição ambígua e não entram no ranking individual.

Inteligência de Ameaças

Use esta página para enxergar o que chegou de forma coordenada, em vez de mensagem a mensagem. Ela agrupa as ameaças do período em campanhas e identifica os ataques direcionados, isto é, aqueles dirigidos a poucas pessoas escolhidas em vez de disparados em massa.

A página apresenta:

- Indicadores de campanha — quantas campanhas foram identificadas no período, quantas são direcionadas e quantas pessoas foram atingidas;
- Relação de campanhas — cada campanha com o critério que a caracterizou, o período de atividade, o número de mensagens e de destinatários distintos, e a severidade;
- Detalhe da campanha — ao selecionar uma campanha, abre-se o painel lateral com os alvos, a linha do tempo e os indícios que a classificaram como direcionada;
- Atores — os remetentes recorrentes, com o volume atribuído a cada um e a tendência no período;
- Origem geográfica — de onde partiram as conexões que entregaram as mensagens;
- Temas recorrentes — os assuntos que mais se repetem, após normalização;
- Distribuição por hora e dia da semana — quando as ameaças chegam com mais frequência;
- Insights — as leituras que o sistema destaca a partir dos dados do período.



Gestão de Risco - Inteligência de Ameaças

Uma campanha é reconhecida quando um mesmo conjunto de indícios — remetente, assunto normalizado, URL ou arquivo — se repete para vários destinatários em uma janela curta de tempo. A caracterização como direcionada considera, entre outros sinais, a concentração em contas prioritárias, a presença de falsificação de remetente e o número reduzido de alvos.

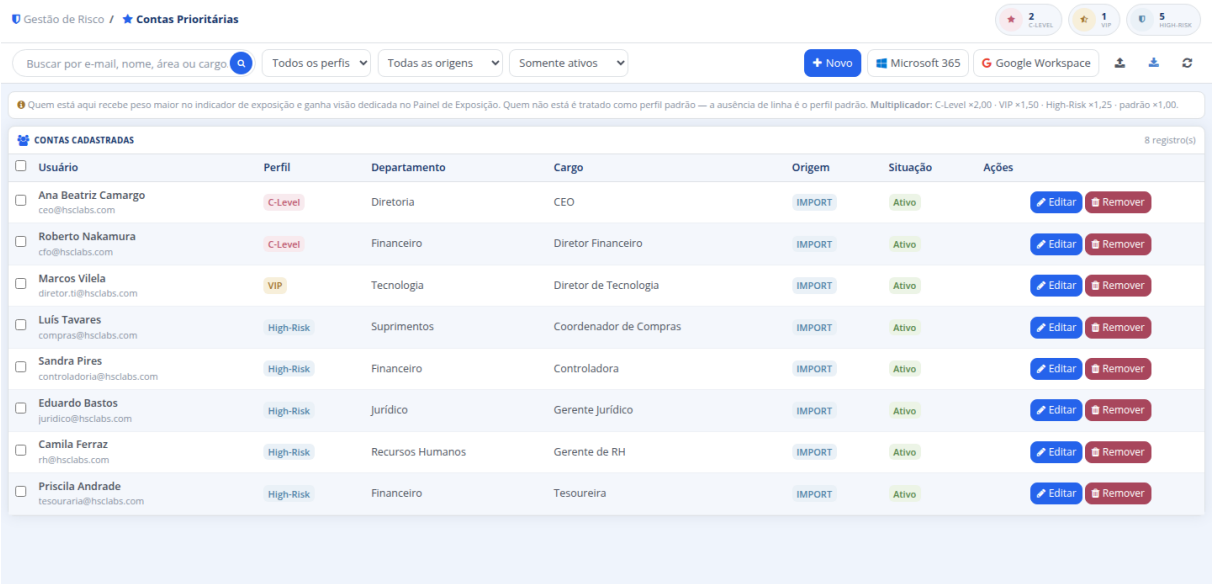
Contas Prioritárias

Use esta página para definir quais caixas postais recebem tratamento diferenciado na avaliação de risco. Quem está cadastrado aqui recebe peso maior no indicador de exposição e ganha visão dedicada na Visão Geral. Quem não está é tratado como perfil padrão: a ausência de cadastro é, ela própria, o perfil padrão. São três perfis, com os seguintes multiplicadores:

- C-Level — o topo da hierarquia da organização, multiplicador 2,00;
- VIP — executivos e liderança, multiplicador 1,50;

- High-Risk — perfis visados por fraude, como tesouraria, controladoria, jurídico e recursos humanos, multiplicador 1,25;
- Padrão — quem não está cadastrado, multiplicador 1,00.

A relação apresenta, para cada conta, o usuário, o perfil, o departamento, o cargo, a origem do cadastro e a situação. As ações de editar e remover ficam disponíveis em cada linha.



Gestão de Risco - Contas Prioritárias

Cadastro manual

O botão Novo abre o formulário de cadastro, no qual são informados o endereço de e-mail, o nome, o departamento, o cargo, o perfil e as observações. O endereço de e-mail é único por ponto de acesso.
Toda edição feita pela tela marca a origem do registro como Manual. Essa marca é o que protege a decisão de quem revisou: registros manuais não são sobrescritos pelas importações automáticas descritas a seguir.

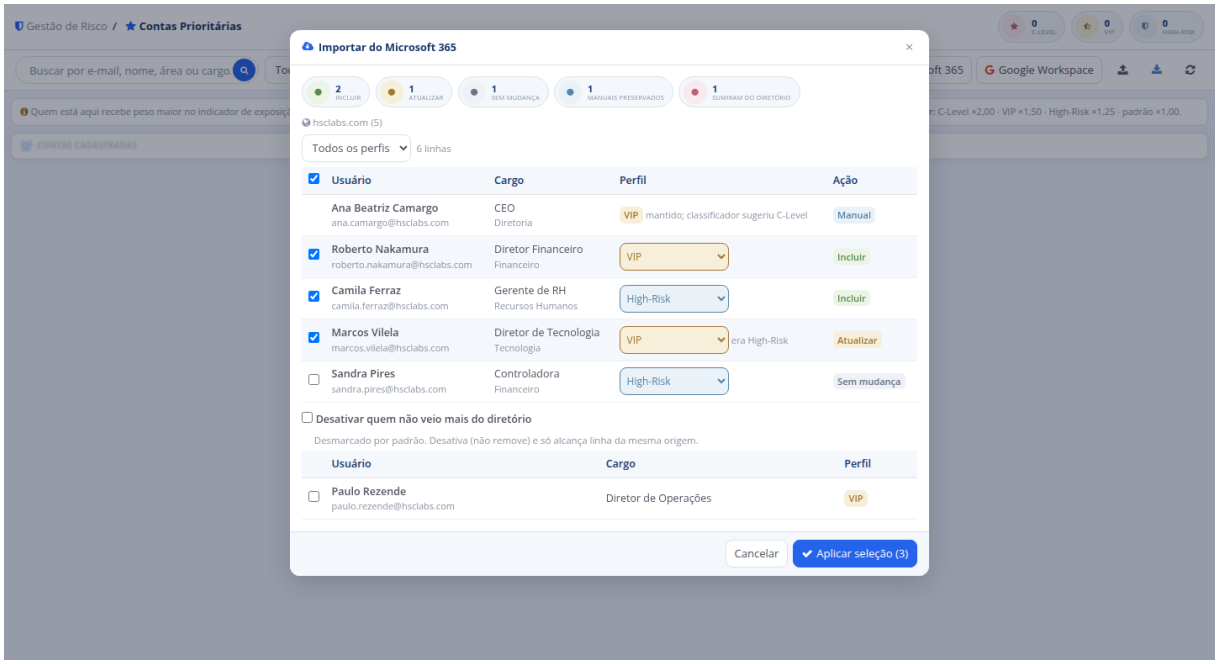
Importação do diretório

Quando há integração ativa com o Microsoft 365 ou com o Google Workspace, a tela oferece a importação automática das contas prioritárias a partir do diretório do cliente. Aparece um botão por integração ativa; se não houver integração com pelo menos um domínio habilitado, o botão não é apresentado.
A importação lê os cargos e, opcionalmente, os grupos de cada usuário do diretório e sugere um perfil para cada conta, aplicando heurísticas de classificação. O processo obedece às seguintes etapas:

- Escolha dos domínios — por padrão são consultados todos os domínios habilitados da integração, sendo possível selecionar um ou mais. Cada domínio corresponde a uma consulta ao diretório, e a tela informa o custo da seleção antes da confirmação;
- Consulta — executada em segundo plano, com indicação do domínio em curso e do progresso. Nada é gravado nesta etapa;
- Prévia — o resultado é apresentado para conferência antes de qualquer gravação, indicando para cada conta se ela será incluída, atualizada, se não há mudança, ou se será preservada por ser um cadastro manual;
- Aplicação — somente as contas selecionadas são gravadas.

Na prévia é possível alterar o perfil sugerido para qualquer conta antes de aplicar. O perfil escolhido manualmente prevalece sobre a sugestão do classificador, e o registro correspondente passa a ter origem Manual, de modo que as importações seguintes não desfaçam a decisão. A pontuação e as regras que levaram à sugestão continuam registradas para consulta.

As contas que constavam do cadastro com aquela origem e não retornaram na consulta são apresentadas separadamente, como sugestão de desativação. A opção vem desmarcada e alcança apenas registros da mesma origem e dos domínios efetivamente consultados.



Gestão de Risco - Prévia da importação do diretório

Importação e exportação em arquivo

A opção de importação em arquivo aceita uma relação em formato CSV, com um registro por linha, separado por vírgula, na ordem: e-mail, nome, departamento, cargo e perfil.
Reimportar a mesma relação atualiza os registros existentes em vez de duplicá-los. Sem o perfil informado, é adotado VIP.
A exportação gera a relação completa das contas cadastradas do ponto de acesso no mesmo formato.

Ações em lote

Selecionando um ou mais registros pela caixa à esquerda de cada linha, a barra de ações em lote é apresentada, permitindo:

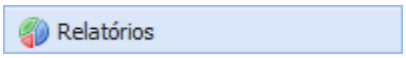
- Alterar perfil — atribui o mesmo perfil a todos os selecionados. A origem dos registros passa a Manual, e com isso as importações seguintes deixam de sobrescrevê-los;
- Desativar — retira os registros do painel e do multiplicador de risco, preservando o cadastro para eventual reativação;
- Reativar — devolve ao cadastro ativo os registros anteriormente desativados;
- Excluir — remove os registros em definitivo. A operação não tem desfazer e é registrada no log de auditoria, com o conteúdo completo de cada registro removido.

Sempre que o objetivo for apenas retirar uma conta do painel, recomenda-se desativar em vez de excluir: o histórico de quem já foi conta prioritária é o que permite explicar as pontuações de risco calculadas no passado.

Menu - Relatórios

Relatórios Gerenciais

Use esta página para emitir relatórios dos registros das mensagens filtradas pelo HSC MailInspector.



/ Relatórios Gerenciais

Visão geral dos relatórios gerenciais

Possuindo mais de trinta relatórios pré-definidos e/ou relatórios customizados através de filtros que permitem a consulta das mensagens processadas pelo HSC MailInspector. Todo o processo é realizado através de um passo a passo intuitivo que conduz o usuário a criação do relatório. Nesta tela também é possível efetuar agendamentos de envio dos relatórios automatizados por e-mail, facilitando a geração de relatórios futuros. Quando o HSC MailInspector estiver operando em modo Cluster os relatórios podem ser tirados de forma consolidada ou por ponto de acesso.

Os relatórios possuem suporte a múltiplos domínios e são apresentados em português do Brasil, em formato gráfico de fácil entendimento (com diferentes tipos de gráficos) com tabelas de linhas e colunas podendo ser exportado por HTML, PDF ou CSV e agendados para envio por e-mail com frequência definida pelo administrador, podendo ser diário, semanal ou mensal.

Todos os relatórios do MailInspector possuem cabeçalho no mínimo as seguintes informações:

- Título do Relatório;
- Data de abrangência do relatório;
- De (origem);
- Para (destino);

Dependendo do relatório, sendo pertinente (por exemplo relatório consolidado de quarentena, com separação por tipo de quarentena, não teria como apresentar o IP de Origem de cada e-mail quarentenado ou o assunto) também são apresentados os dados:

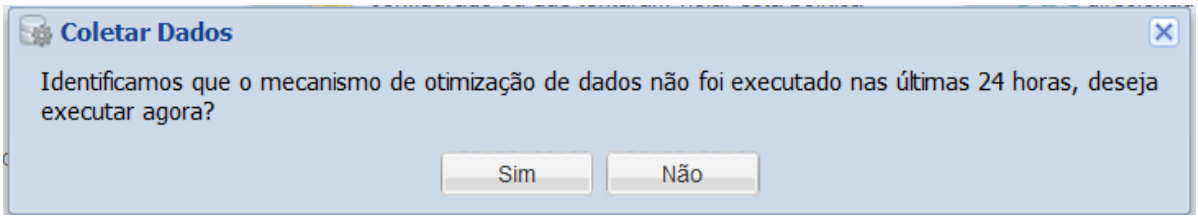
- Remetente;
- Destinatário;
- Assunto;
- Data e hora início;
  Data e hora fim;
- Endereço IP de origem;
- Status da mensagem;
- Política aplicada;
- Classificações pertinentes ao e-mail;
- Pontuação do e-mail;
- Sentido (entrada, saída ou e-mail interno);

Os relatórios são separados em três grupos:

- Segurança;
- SPAM;
- Administração;

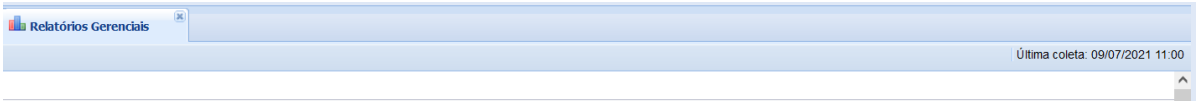
Atualmente o MailInspector conta com sistema de cache de dados para agilizar o processo de relatório.

O cache é atualizado automaticamente, sem necessidade da intervenção do administrador. A única ação que é solicitada ao administrador, é um aviso sobre atualização do cache de dados para relatório e a autorização para a continuidade ou cancelamento do processo.



Tela de atualização de cache de relatório.

Pode-se verificar qual foi a última atualização do cache no canto superior direito da tela de relatórios.



Tela da data de última atualização do cache.

O MilInspector permite criar filtros de acordo com o relatório disponível, podendo ser:

- Intervalo por Data;
- Agrupado por Horas / Dias / Meses;
- Seleção de domínio atendido;
- Ponto de filtragem;
- Indicação de todo o cluster;
- Domínio de Origem;
- Domínio de Destino;
- E-mail de Origem (parcial ou completo);
- E-mail de Destino (parcial ou completo);
- IP específico;
- IP de Origem;
- IP de Destino;
- Nome de Anexo (parcial ou completo);
- Nome da Ameaça (parcial ou completo);
- Seleção de filtragem por usuário ou domínio;

Definições de Opções - Relatórios Gerencias

Os relatórios no MailInspector são separados por três grupos:
Relatórios de Segurança: Atende a requisitos indicativos de segurança, tais como e-mails com vírus/malwares;
Relatório de SPAM: Relatórios indicativos de SPAM, pontuação e classificação, bem como origem de e-mails do tipo spam e/ou destinatário dos e-mails do tipo SPAM;
Relatórios de Administração: Indica os relatórios referentes a administração e gerenciamento do MailInspector, tais como qualidade de e-mail, volume de e-mails com classificação, etc;

Opções	Definição

Voltar	Quando clicado, retorna a página inicial dos relatórios gerenciais.
Avançar	Quando clicado, avança para os filtros do relatório.
Cabeçalho & Rodapé	Permite acionar texto no início das páginas ou no rodapé das páginas a fim de personalizar os relatórios gerados.
Tipo	**Relatórios de Segurança**

Top Remetentes de Vírus	Remetentes que mais enviaram Vírus
Top Destinatários de Vírus	Destinatários que mais enviaram Vírus
Top Ataques de Fraudes de E-mail	Lista os principais destinatários que receberam tentativas de Fraudes de E-mail "E-mail Spoofing". Este relatório trabalha em conjunto com o módulo RealTime > Segurança > SandBox, ao qual consegue traduzir os dados de reescrita de URL's e cliques efetuados.
Fontes de Ataques	Lista das origens que mais realizaram ataques (IP´s/Hostnames), organizados por tipo de ataques tais como: vírus, phishing, malware, URL maliciosas, ATP e outros.
TOP Violações de SPF por Domínio	Exibe os domínios que não possuem SPF configurado ou que tentaram violar esta política.
Ataque Dirigido	Mostra detalhadamente um resumo dos ataques por usuários ou domínio contendo: Nome das ameaças, usuários afetados, tipo das ameaças, URLs Limpas, URLs Maliciosas, quantidade de Cliques em cada tipo de URL, dessa forma com esse relatório é possível acompanhar o histórico de ataques.
Relatório de Vírus	Detalhes dos vírus e ameaças encontrados no período. Contendo detalhes de ataques e proliferações de vírus Zero-Day.
Top Vírus	Os dez vírus mais encontrados nas mensagens.
Relatório Analítico de ameaças	Lista os e-mails com ataques, bem como os IP's e Hostnames das fontes de ataque.
Visão Geral de Sessões TLS	Apresenta uma análise consolidada das sessões TLS estabelecidas com o MailInspector, destacando versões de protocolo utilizadas, padrões de criptografia e volume de conexões seguras, bem como conexões que tiveram falha de TLS. Ele auxilia na verificação do nível de segurança aplicado nas comunicações e na identificação de servidores que utilizam padrões obsoletos de TLS.
Zero Day	Indica a efetividade do sistema de detecção ZeroDay/Zero Hour

Relatórios de SPAM

TOP Hosts Emissores de SPAM	Mostra os principais endereços IPs que enviaram SPAM.
Mensagens SPAM Por Pontuação	Indica a quantidade de mensagens agrupadas por pontuação no período.
Mensagens SPAM Por Regras	Indica a quantidade de mensagens agrupadas pelas regras que foram casadas. Sumarizando as principais regras que foram ativadas por: Corpo, Cabeçalho, Assunto, Mensagem Original e URL.
Principais Destinatários de SPAM	Os dez destinatários e-mails e domínios que mais receberam SPAM por quantidade e volume.
Principais Remetentes de SPAM	Os dez remetentes e-mails e domínios que mais enviam SPAM por quantidade e volume. Ao final do relatório é possível clicar no botão "Incluir os Remetentes na Block List" a fim de adicionar automaticamente todos os remetentes do relatório na Block List do sistema.
Principais Destinatários de Mail Marketing/Bulk Mail	Os dez destinatários e-mails e domínios que mais receberam Mail Marketing/Bulk Mail por quantidade e volume.
Principais Remetentes de Mail Marketing / Bulk Mail	Os dez remetentes e-mails e domínios que mais enviam Mail Marketing/Bulk Mail por quantidade e volume.
Ranking Categorias URL / Ranking SPAM URL	Ranking Categorias URL / Ranking SPAM URL apresenta uma visão consolidada das URLs detectadas nas mensagens analisadas pelo MailInspector, organizando-as em rankings que destacam tanto as categorias mais frequentes quanto a quantidade de URLs identificadas como maliciosas ou associadas a spam. O mecanismo de ranking permite visualizar rapidamente: • As categorias de URL mais recorrentes nas mensagens recebidas; • Volume de URLs classificadas como SPAM ou potencialmente perigosas; Essa funcionalidade facilita a identificação de padrões de ataque, avaliação de risco e otimização das políticas de filtragem baseadas em URLs.
Ranking de Domínios Analisados por DMARC	Ranking de Domínios Analisados por DMARC apresenta uma visão consolidada dos principais domínios enviados ou recebidos pela organização e classificados conforme sua conformidade com as políticas DMARC (Domain-based Message Authentication, Reporting & Conformance).

	Esse relatório permite identificar rapidamente quais domínios demonstram maior segurança no envio de e-mails e quais representam risco, facilitando ações preventivas e estratégias de mitigação.

Relatórios de Administração

Sumário por Domínio	Volume de mensagens agrupadas por domínio e categorizadas pelo tipo: • Quantos e-mails de entrada; • Quantos e-mails de saída; • Quantos e-mails internos • Quantos e-mails foram entregues (e-mails limpos); • Quantos e-mails foram bloqueados; • Qualidade dos e-mails bloqueados como ameaça (quantos são phishing, quantos são vírus, quantos são malware, quantos são ATP e quantos são fraude de e-mail); • Dos e-mails bloqueados como indesejados (Quantos são provável spam, quantos são spam, quantos são block list, quantos são bulk mail e quantos foram bloqueados por outros bloqueios);
Quantidade de mensagens processadas	Indica quantidade de mensagens processadas por hora.
Top Usuários que mais liberam mensagens da Quarentena	Lista os usuários que mais liberaram e-mails de suas quarentenas informando a quantidade por período.
Relatório Consolidado	Relatório unificado com diversas informações consolidadas sobre as mensagens. • Volume de Mensagens por Data; • Top 10 Principais Destinatários de SPAM; • Top E-mail Relays; • Top 10 Remetentes por Quantidade; • Top Remetentes por Domínio; • Top Destinatário por Quantidade; • Top 10 Destinatários por Volume; • Top 10 Principais Remetentes de SPAM; • Relatório de Vírus; • Percentual de Quantidade de E-mails/Estatísticas da Quarentena;
Estatísticas da Quarentena	Mostra informações detalhadas sobre as Quarentenas do sistema informando: Uso atual em quantidades/tamanho, tamanho/tempo definido,

		volume de mensagens quarentenadas, tempo de expiração das quarentenas.
	Volume de Mensagens por Data	Volume de mensagens agrupadas por dia e categorizadas pelo tipo. Apresenta um resumo (sumário) de todas as mensagens agrupadas por dia informando o volume diferenciando por: • Quantidade de e-mails; • Volume de dados em MB; • Tamanho Médio das mensagens; • Total de Ameaças encontradas; • Limpas (DLP/Auditoria); • SPAM; • Provável SPAM; • Ameaças; • Phishing; • Allow List; • Block List; • Tamanho Excedido; • Outro Bloqueio; • Conteúdo Bloqueado (ex: Anexos compactados com senha)
	Top E-mail Relays	Os dez servidores que mais enviaram e-mails.
	Top Remetentes por Quantidade	Os dez endereços que mais enviaram e-mails.
	Top Remetentes por Volume	Os dez endereços que mais consumiram recursos para enviar e-mails, baseados no volume das mensagens.
	Top Destinatário por Quantidade	Os dez endereços que mais receberam e-mails.
	Top Destinatário por Volume	Os dez endereços que mais consumiram recursos para receber e-mails, baseados no volume das mensagens.
	Top Domínio Remetente por Quantidade	Os dez domínios que mais enviaram e-mails.
	Top Domínio Remetente por Volume	Os dez domínios que mais consumiram recursos para enviar e-mails.
	Top Domínio de Destino por Quantidade	Os dez domínios que mais receberam e-mails.
	Top Domínio de Destino por Volume	Os dez domínios que mais consumiram recursos para receber e-mails.
	Conexões Completadas x Bloqueadas	Exibe o total de conexões completadas e bloqueadas.

	TOP Anexos	Exibe quais foram os principais tipos de arquivos que foram anexados nos e-mails.
	Controle de Conexões x Rejeitadas	Mostra uma análise das Conexões que foram rejeitas na Camada de MTA identificando por tipo de rejeição, tais como: • Reputação do Remetente; • Rejeitadas por Controle de Conexão (Reverso, SPF, Ataques de Diretório "Harvest Attack" / Usuários Inexistentes);
	Auditoria de E-mails	Lista todas as mensagens trafegadas no período.
	Mensagens por Domínios Atendidos	Exibe de forma resumida o total de mensagens enviadas e recebidas para os domínios atendidos.
	Disponibilidade, alertas e erros	Indica o tempo de disponibilidade, alertas emitidos e eventuais erros do sistema.
	Falso Positivo	Lista os falsos positivos relatados pelos usuários, bem como a quantidade total.
	Falso Negativo	Lista os falsos negativos reportados pelos usuários, bem como a quantidade total.
	Fluxo de mensagem	Indica o fluxo de mensagens de entrada x mensagens de saída.
	Status do Cluster	Indica todos os componentes do cluster, com os seguintes dados: • Resumo do sistema (Processador, carga de processamento, consumo de memória, uso de disco, etc); • Dados de consumo de rede; • Status dos Serviços do MailInspector; • Comunicação entre os pontos de filtragem; • Comunicação com as portas necessárias para o bom funcionamento do MailInspector;
	Sumário de Conexões por País	Exibe a origem geográfica das conexões recebidas, agrupando-as por país. A visualização permite identificar padrões de envio, comportamentos anômalos e possíveis campanhas maliciosas originadas de regiões específicas, apoiando decisões de segurança e políticas baseadas em geolocalização.
	Sumário de Conexões TLS	Monitora e consolida o uso de criptografia nas conexões de e-mail do MailInspector, analisando o cabeçalho **Received** para identificar se a comunicação ocorreu via **TLS ou texto plano**, bem como a **versão do protocolo e a cifra utilizada**, apresentando a

		quantidade e o volume de mensagens por tipo de conexão.
	Ranking Categorias URL / Ranking SPAM URL	Identifica e consolida as **categorias de URLs presentes nas mensagens analisadas**, avaliando o campo **archive** para gerar um **ranking das categorias mais recorrentes**, com a **quantidade e o volume de mensagens associadas a URLs classificadas como spam ou potencialmente perigosas**.
	Ranking Domínios Analisados DMARC	Apresenta um **ranking dos principais domínios enviados ou recebidos pela organização**, analisando o campo **spamreport** para identificar assinaturas **DMARC** e classificando os domínios conforme sua **conformidade com as políticas DMARC**.
	Violação de Políticas	Indica todas as mensagens que tiveram políticas violadas, tais como bloqueio por DLP, bloqueio por pontuação que tiveram regras customizadas atuando sobre ele.

Definições de Opções - Relatórios Gerenciais - Filtros

Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição
Voltar	Quando clicado, retorna a seleção do relatório.
Gerar Relatório	Quando clicado, gera o relatório. Nesta opção você pode selecionar qual formato será disponibilizado: PDF, HTML ou CSV. Também é possível informar uma conta de e-mail para o envio do relatório.

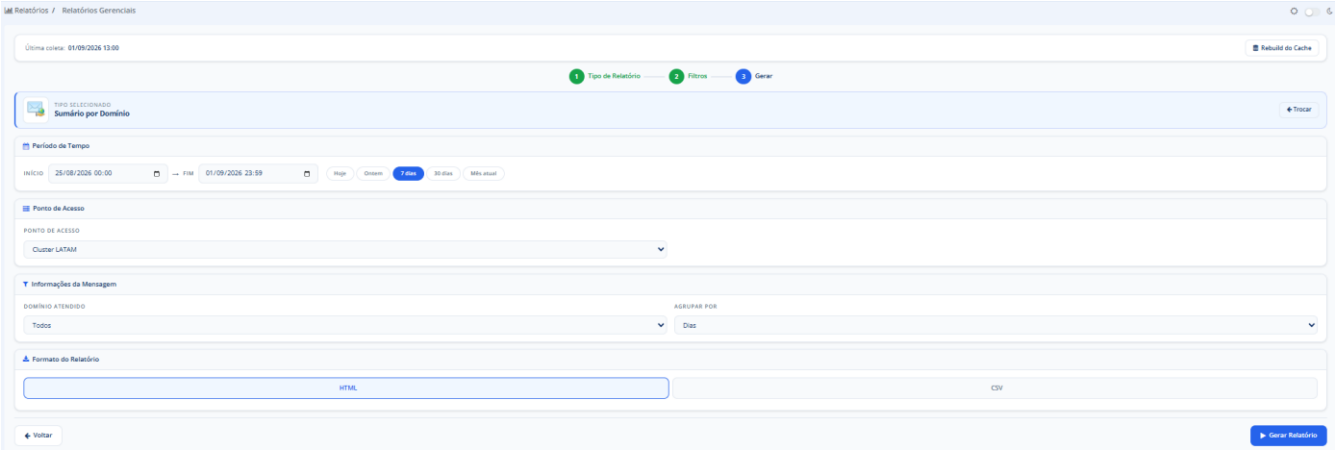
Período de Tempo	Indique o período do relatório (data inicial e data final).
	• **Data Inicial** - Informe a data de início do período a ser pesquisado.
	• **Data Final** - Informe a data de fim do período a ser pesquisado.
	• **Hora inicial** - Permite informar horário de início da pesquisa
	• **Hora Final** - Permite informar horário de fim da pesquisa
	• **Agrupar** – Indica que o relatório será agrupado por:
	  ○ **Dias;**
	  ○ **Horas;**
	  ○ **Mês;**

Ponto de Acesso	Permite selecionar o ponto de acesso ao qual a mensagem foi processada. Quando utilizando cluster permite tirar relatórios específicos por cada nodo do cluster.
Informações da Mensagem	Insira as informações ORIGEM / DESTINO, conforme a necessidade. Importante indicar que pode ser domínio, e-mail, subdomínio, etc. • **Domínio de Origem:** Indique o domínio de origem para melhorar o desempenho do relatório; • **Domínio de Destino:** Indique o domínio de destino para melhorar o desempenho do relatório;

	• **E-mail de Origem** - Informe um endereço de e-mail ou domínio ou grupo do remetente. Esse filtro pode ser no seguinte formato:
	  ○ **Exata:** Compara o e-mail no formato exato, do início ao fim, sendo verificado o FROM do Envelope;
	  ○ **Parcial:** Compara o e-mail/domínio ou parte de string contido parcialmente, sendo verificado o FROM do Envelope;
	  ○ **Header:** Compara o e-mail/domínio ou parte de string contido parcialmente no FROM do Header;
	• **E-mail de Destino** - Informe um endereço de e-mail, domínio ou grupo do destinatário. Esse filtro pode ser no formato:
	  ○ **Exata:** Compara o e-mail no formato exato, do início ao fim, sendo verificado o TO do Envelope;
	  ○ **Parcial:** Compara o e-mail/domínio ou parte de string contido parcialmente, sendo verificado o TO do Envelope;
	  ○ **Header:** Compara o e-mail/domínio ou parte de string contido parcialmente no TO do Header;
	
	Usando delimitadores de De e Para, com operadores lógicos, é possível criar relatórios por um único e-mail, subdomínios, domínios ou somente Inbound (Entrada), somente Outbound (saída) ou de TODOS para um só grupo, entre outras combinações.

Status	Escolha entre: • **Provável SPAM** - Filtra por mensagens processadas que foram classificadas como proveniente de provável fonte de SPAM ou ameaças. • **SPAM** - Filtra por mensagens processadas que foram classificadas como proveniente de fonte confirmada de SPAM ou ameaças. • **Vírus** - Filtra por mensagens processadas que foram classificadas como contendo vírus ou que tenham fontes para vírus ou outras ameaças. • **Conteúdo Bloqueado** - Filtra por mensagens processadas quer foram classificadas como contendo arquivos anexos com o mime-types ou extensões proibidas. • **Outro Bloqueio** - Filtra por mensagens processadas quer foram classificadas em qualquer outro tipo de bloqueio. • **Allow List** - Filtra por mensagens que foram processadas e estavam cadastradas na allow list. • **Block List** - Filtra por mensagens que foram processadas e estavam cadastradas na block list. • **Tamanho Excedido** - Filtra por mensagens processadas quer foram classificadas como tendo o tamanho maior que o permitido. • **Em Quarentena** - Filtra por mensagens que foram processadas e armazenadas na quarentena por configuração do filtro ou para auditoria. • **Phishing** - Filtra pelas mensagens classificadas como Phishing. • **DLP/Auditoria** - Filtra por mensagens processadas que foram classificadas como limpas, não sendo consideradas SPAM ou fonte de ameaça.
Relatório por Usuário/Domínio	**Consultar por:** Seleção de relatório por um usuário específico **Usuário:** Seleção de relatório por um e-mail específico; **Domínio:** Seleção de relatório por um domínio em específico

Formato do Relatório	Podemos gerar o relatório padrão HTML ou CSV
Agendar Envio	Selecione a periodicidade: • Diário; • Semanal; • Mensal; • Customizado; Também indique o e-mail de destino para qual será enviado o relatório agendado.



Exemplo de Tela de Ativação dos filtros desejados para o relatório previamente selecionado

Exemplo de Relatórios

Relatório de Sumário por Domínio

Sumário por Domínio

Consolidação do volume de mensagens processadas por domínio atendido. Apresenta a distribuição entre entrada, saída, bloqueios e entregas, com detalhamento das ameaças detectadas no período selecionado.

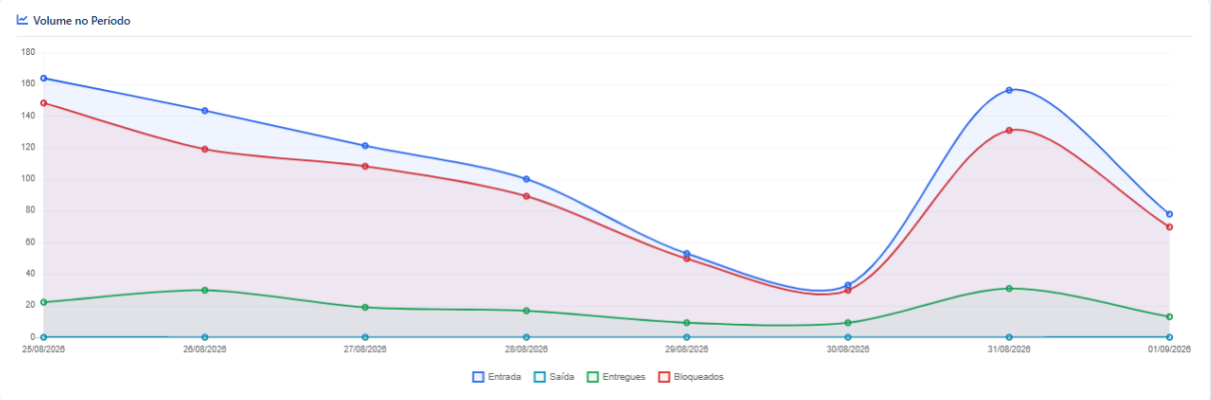
Período: 25/08/2026 00:00:00 - 01/09/2026 23:59:00 **Ponto de Acesso:** Cluster LATAM

No período analisado foram processadas **895** mensagens, com **94,7%** de entrada e **0%** de saída. A taxa de bloqueio foi de **83,2%**, sendo **Fraude / Spoofing** a principal ameaça detectada. Das mensagens processadas, **16,8%** foram entregues com sucesso.

AÇÕES RECOMENDADAS

- Bloqueio elevado (83,2%). Confirme que domínios legítimos estão na AllowList e revise os critérios de AntiSPAM.
- Fraude/Spoofing em destaque. Reforce as políticas DMARC nos domínios atendidos.
- Entrega abaixo de 75%. Analise os relatórios de bloqueio para identificar possíveis falsos positivos.
- Consulte regularmente este relatório para acompanhar tendências e agir preventivamente antes que volumes anômalos se consolidem.

895	848	0	745	150
Total de Mensagens	Entrada (94.7%)	Saída (0.0%)	Bloqueados (83.2%)	Entregues (16.8%)



Volume por Período

DATA	VOLUME	ENTRADA	%	INTERNA	%	SAÍDA	%	BLOQUEADOS	%	ENTREGUE	%	TOTAL
25/08/2026	5.56 MB	164	96,47	-	-	-	-	148	87,06	22	12,94	170
26/08/2026	5.32 MB	143	95,97	-	-	-	-	119	79,87	30	20,13	149
27/08/2026	5.10 MB	121	95,28	-	-	-	-	108	85,04	19	14,96	127
28/08/2026	3.96 MB	100	94,34	-	-	-	-	89	83,96	17	16,04	106
29/08/2026	2.29 MB	53	89,83	-	-	-	-	50	84,75	9	15,25	59
30/08/2026	1.57 MB	33	84,62	-	-	-	-	30	76,92	9	23,08	39
31/08/2026	7.07 MB	156	96,3	-	-	-	-	131	80,86	31	19,14	162
01/09/2026	2.49 MB	78	93,98	-	-	-	-	70	84,34	13	15,66	83
	33.38 MB	848		0		0		745		150		895

Ameaças Bloqueadas

DATA	PHISHING	VÍRUS	MALWARE	ATP	FRAUDE DE EMAILS	TOTAL
25/08/2026	34	2	-	-	41	77
26/08/2026	18	-	-	-	37	55
27/08/2026	11	-	-	-	29	40
28/08/2026	9	-	-	-	30	39
29/08/2026	3	-	-	-	9	12
30/08/2026	3	-	-	-	10	13
31/08/2026	40	-	-	-	36	76
01/09/2026	22	-	-	-	15	37
8 (DIAS)	140	2	0	0	207	349

Mensagens Indesejadas Bloqueadas

DATA	PROVÁVEL SPAM	SPAM	BLOCK LIST	BULK MAIL	OUTROS BLOQUEIOS	TOTAL
25/08/2026	12	52	-	7	-	71
26/08/2026	7	50	-	7	-	64
27/08/2026	15	38	-	15	-	68
28/08/2026	7	31	-	12	-	50
29/08/2026	4	18	-	16	-	38
30/08/2026	4	8	-	5	-	17
31/08/2026	8	21	-	26	-	55
01/09/2026	4	17	-	12	-	33
8 (DIAS)	61	235	0	100	0	396

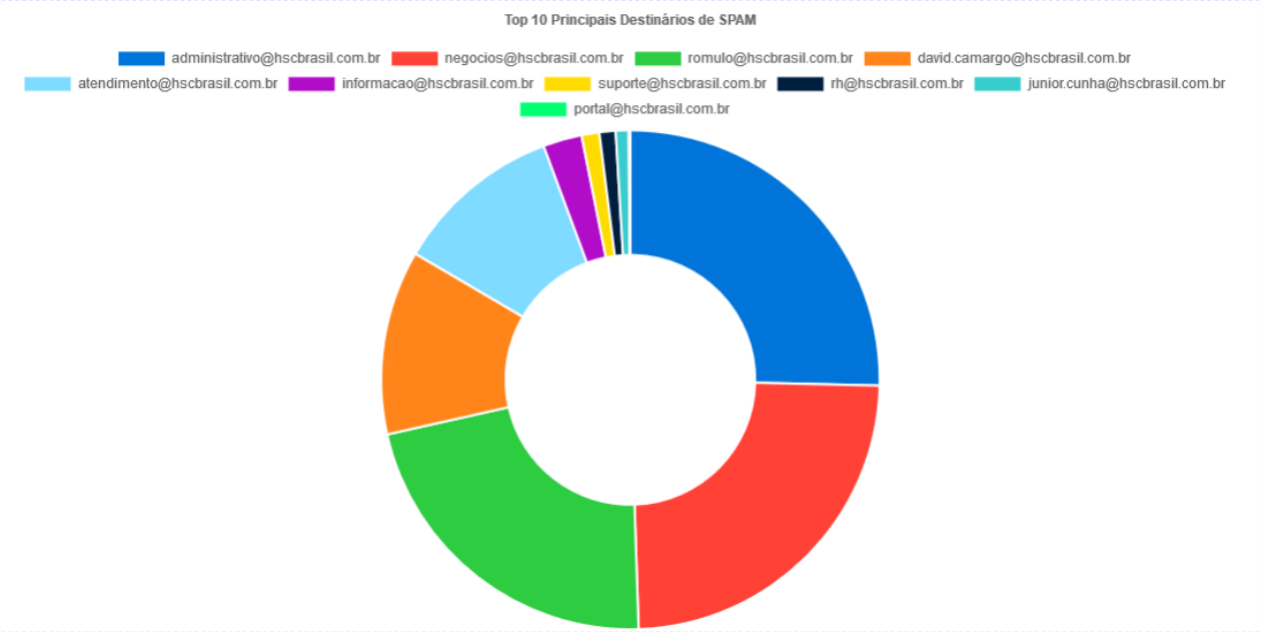
Relatório de Sumário por Domínio – Indica a qualidade dos e-mails recebidos no período selecionado

Relatório Consolidado de Principais Destinatários de SPAM

Filtros

Período: 27/01/2019 00:00:00 - 31/01/2019 23:59:00
Status: DLP / Auditoria (Todos); Provável Spam (Todos); Spam (Todos); Vírus (Todos); Conteúdo Bloqueado (Todos); Outro Bloqueio (Todos); WhiteList (Todos); BlackList (Todos); Tamanho Excedido (Todos); Em Quarentena (Todos); Phishing (Todos);
Informações da Mensagem: de (Contém) para @hscbrasil.com.br (Contém)

Principais Destinatários de SPAM



Destinários	Quantidade
administrativo@hscbrasil.com.br	242
negocios@hscbrasil.com.br	230
romulo@hscbrasil.com.br	210
david.camargo@hscbrasil.com.br	114
atendimento@hscbrasil.com.br	104
informacao@hscbrasil.com.br	24
suporte@hscbrasil.com.br	11
rh@hscbrasil.com.br	10
junior.cunha@hscbrasil.com.br	8
portal@hscbrasil.com.br	1

Destinários	Quantidade
hscbrasil.com.br	956

Relatório de Principais destinatários de spam

Resumo Executivo

O **Resumo Executivo** consiste em um relatório e dashboard gerencial que permite ao administrador acompanhar, de forma **consolidada e dinâmica**, os principais indicadores do ambiente de correio eletrônico, facilitando a identificação de alterações relevantes no comportamento do tráfego e dos mecanismos de segurança.

A solução permite identificar **picos de volume de mensagens, aumentos na quantidade de mensagens retidas ou bloqueadas, variações fora dos padrões históricos e alterações significativas no perfil do tráfego**, proporcionando maior visibilidade sobre eventos que possam indicar anomalias ou ameaças emergentes.

Esses indicadores auxiliam na **antecipação e identificação de incidentes de segurança, campanhas massivas de SPAM ou Malware, tentativas de ataque direcionado e possíveis gargalos operacionais**, permitindo que o administrador adote medidas preventivas antes que os eventos causem impactos significativos ao ambiente.

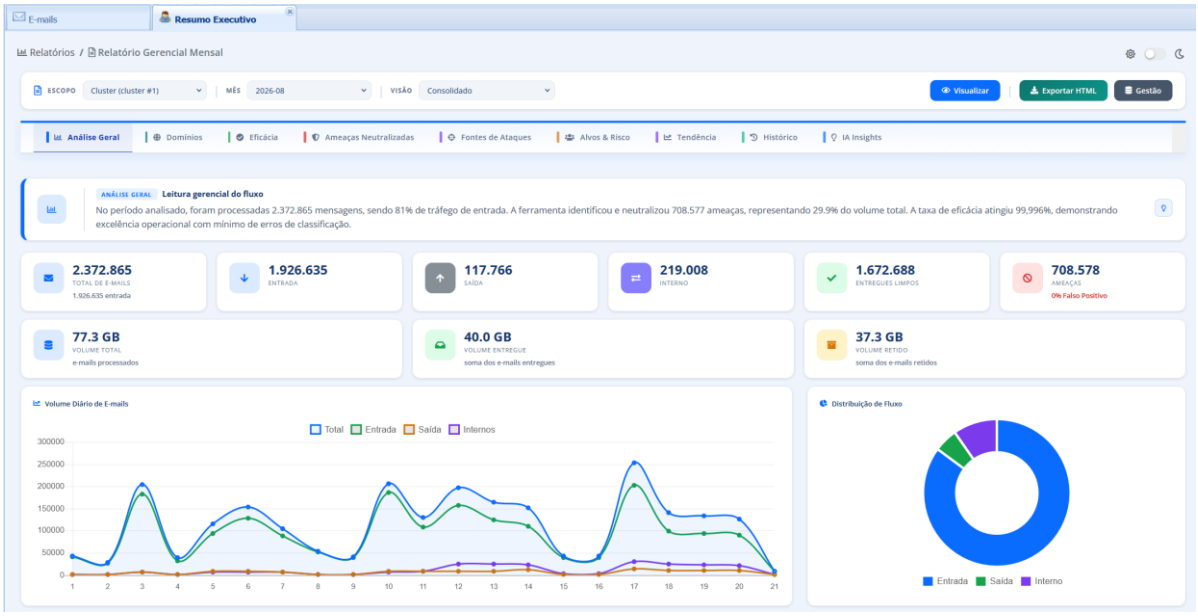
O Resumo Executivo também consolida informações relevantes para o **gerenciamento de riscos e o aprimoramento contínuo das políticas de segurança**, possibilitando identificar tendências, avaliar a efetividade dos mecanismos de detecção e filtragem e apoiar decisões relacionadas à melhoria das configurações de proteção.

A análise histórica e das tendências permite ainda identificar **padrões de comportamento e possíveis indicadores de futuras campanhas ou ataques**, contribuindo para a adoção antecipada de medidas de mitigação e prevenção.

Dessa forma, o Resumo Executivo proporciona uma **visão estratégica do ambiente de e-mail**, transformando os dados coletados pelo MailInspector em informações relevantes para **monitoramento, gestão de riscos, prevenção de incidentes, planejamento e tomada de decisão**.

O Resumo Executivo é composto por 9 partes:

1. Análise Geral;
2. Domínios;
3. Eficácia;
4. Ameaças Neutralizadas;
5. Fontes de Ataque;
6. Alvos e Risco;
7. Tendência;
8. Histórico;
9. IA Insights;



Análise Geral

O módulo **Análise Geral** apresenta uma visão consolidada do fluxo de e-mails da organização, permitindo acompanhar, de forma clara e centralizada, o **volume de mensagens processadas e o resultado das ações de proteção** realizadas pela solução.

Por meio do painel, é possível visualizar a quantidade total de e-mails analisados, segmentada entre **mensagens de entrada, saída e internas**, além de acompanhar quantos e-mails foram **entregues aos destinatários** e quantos foram **retidos ou bloqueados por apresentarem ameaças ou violações das políticas de segurança**.

O módulo também consolida indicadores como **volume total de dados processados, volume entregue, volume retido e quantidade de ameaças identificadas e neutralizadas**, proporcionando uma visão abrangente da operação do sistema de proteção de e-mail.

Além dos indicadores consolidados, a análise do **volume diário e da distribuição do fluxo de mensagens** permite identificar variações de tráfego, picos de utilização e tendências de comportamento ao longo do período.

Dessa forma, o **Análise Geral** fornece uma visão operacional e gerencial da proteção de e-mail, permitindo compreender **quanto tráfego foi processado, quanto foi considerado legítimo, quanto foi bloqueado e qual foi o impacto das camadas de segurança sobre o fluxo de mensagens**.

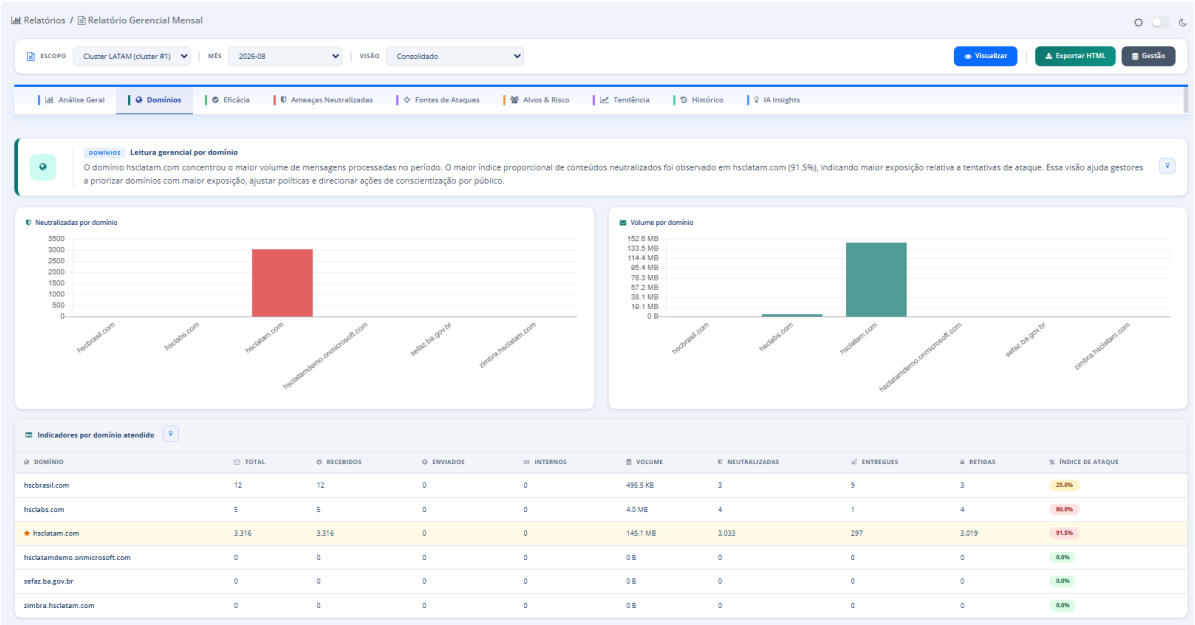
Domínios

A aba **Domínios** apresenta uma visão consolidada da proteção de e-mails por domínio, permitindo acompanhar o **volume de mensagens processadas, o nível de exposição a ameaças e a efetividade das camadas de segurança** aplicadas em cada ambiente.

Por meio dos indicadores, é possível visualizar a quantidade de e-mails **recebidos, enviados e internos**, o volume de dados processados, além do total de mensagens **neutralizadas, entregues e retidas** pela solução. Essa segmentação permite comparar o comportamento e a exposição de diferentes domínios dentro da organização.

A aba também apresenta o **índice de ataque por domínio**, permitindo identificar quais ambientes apresentam maior proporção de mensagens associadas a tentativas de ataque. Esses dados possibilitam **priorizar ações de proteção, investigação e conscientização** nos domínios que apresentam maior nível de risco.

Os gráficos de **volume e ameaças neutralizadas por domínio** complementam a análise, facilitando a identificação de concentrações de tráfego e de ameaças. Dessa forma, a aba **Domínios** fornece uma visão comparativa e estratégica da segurança do correio eletrônico, permitindo avaliar **onde estão os maiores volumes, quais domínios são mais visados e como a proteção está atuando em cada ambiente**.



Eficácia

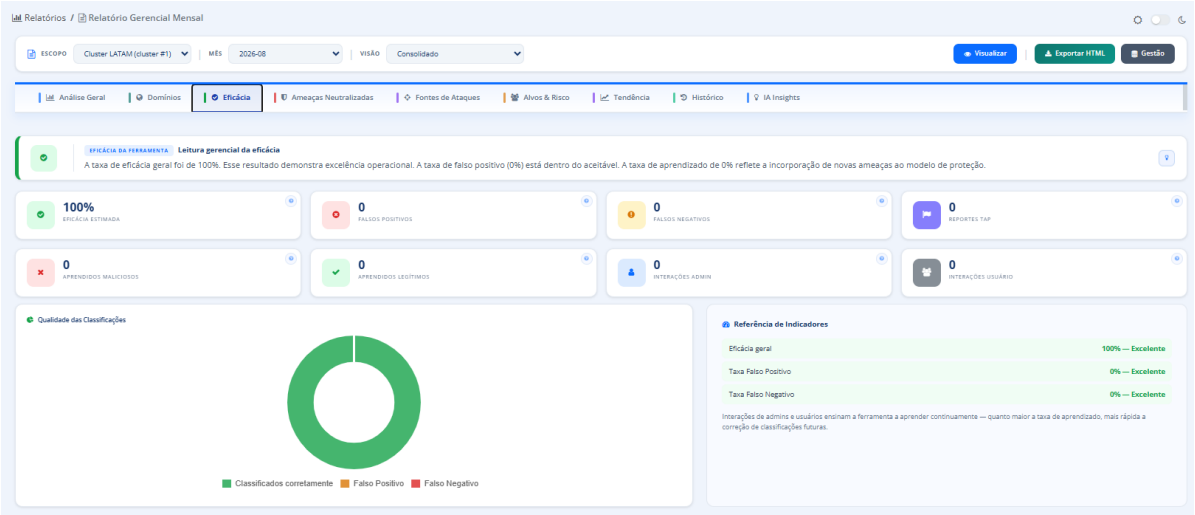
O módulo **Eficácia** apresenta uma visão detalhada sobre a **capacidade da solução de proteção de e-mail em identificar e classificar corretamente as mensagens**, permitindo avaliar a qualidade dos mecanismos de detecção e a efetividade das camadas de segurança aplicadas.

O painel consolida indicadores como **taxa de eficácia, falsos positivos, falsos negativos, ameaças aprendidas e classificações legítimas**, possibilitando acompanhar a precisão do sistema na identificação de mensagens maliciosas e legítimas.

A análise de **falsos positivos** permite identificar mensagens legítimas que foram classificadas incorretamente como ameaças, enquanto o acompanhamento de **falsos negativos** evidencia situações em que ameaças conseguiram passar pelos mecanismos de proteção. Esses indicadores são fundamentais para avaliar a qualidade da classificação e identificar oportunidades de aprimoramento.

O módulo também apresenta informações relacionadas ao **aprendizado do sistema**, registrando novas classificações de conteúdos maliciosos e legítimos. Associado às interações de administradores e usuários, esse processo contribui para o **aperfeiçoamento contínuo dos modelos de detecção**, permitindo que a solução se adapte a novos padrões e ameaças.

Dessa forma, o módulo **Eficácia** permite medir não apenas o volume de ameaças detectadas, mas principalmente **a precisão da proteção, a qualidade das classificações e a evolução contínua da capacidade de detecção**, fornecendo indicadores importantes para a avaliação da efetividade da segurança de e-mail.



Ameaças Neutralizadas

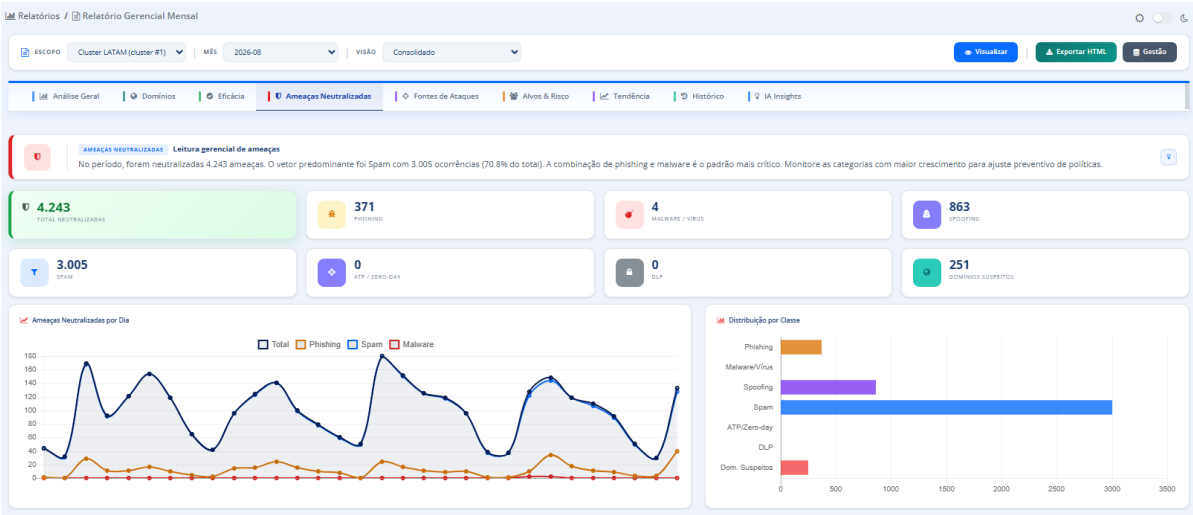
O módulo **Ameaças Neutralizadas** apresenta uma visão consolidada das ameaças identificadas e bloqueadas pela solução de proteção de e-mail, permitindo compreender **quais tipos de ataques estão sendo detectados, sua frequência e sua evolução ao longo do tempo**.

O painel categoriza as ameaças por diferentes vetores, incluindo **Phishing, Malware/Vírus, Spoofing, Spam, ATP/Zero-Day, DLP e Domínios Suspeitos**, proporcionando uma visão detalhada do cenário de segurança do ambiente de e-mail.

Além do volume total de ameaças neutralizadas, o módulo permite analisar a **distribuição das ameaças por categoria** e sua ocorrência diária. Essa visão facilita a identificação de **picos de ataques, padrões recorrentes e categorias predominantes**, apoiando a definição de políticas de proteção e ações preventivas.

O acompanhamento de ameaças avançadas, como **ATP e ataques Zero-Day**, permite ainda identificar tentativas que utilizam técnicas mais sofisticadas e que demandam mecanismos adicionais de análise e detecção.

Dessa forma, o módulo **Ameaças Neutralizadas** transforma os eventos de segurança em uma visão operacional e estratégica, permitindo que as equipes compreendam **quais ameaças estão sendo direcionadas à organização, em que volume ocorrem e como a solução está atuando para bloqueá-las antes que possam causar impacto aos usuários e ao ambiente corporativo**.



Fontes de Ataque

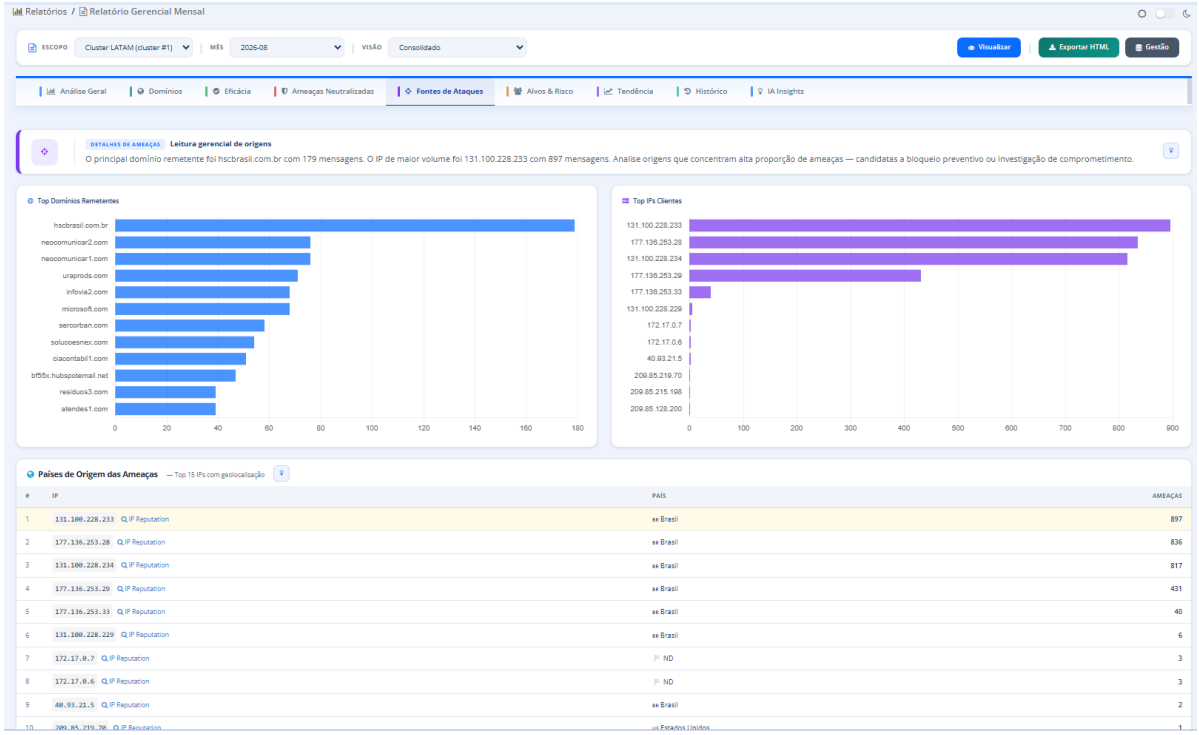
O módulo **Fontes de Ataque** apresenta uma visão detalhada sobre as **origens das ameaças direcionadas ao ambiente de e-mail**, permitindo identificar os principais domínios, endereços IP e países associados às mensagens potencialmente maliciosas ou suspeitas.

A solução consolida e classifica as origens com maior volume de mensagens, destacando os **principais domínios remetentes e IPs de origem**. Essa análise permite identificar fontes que concentram um volume elevado de ameaças e que podem representar **indicadores de comprometimento, campanhas maliciosas ou tentativas recorrentes de ataque**.

O módulo também apresenta a **geolocalização das fontes de ameaça**, permitindo identificar os países de origem dos endereços IP envolvidos. Essas informações podem ser correlacionadas com outros indicadores de segurança, como reputação de IP, frequência de ataques e tipos de ameaças detectadas.

Com essa visão, as equipes de segurança conseguem **investigar a procedência dos ataques, identificar fontes recorrentes, priorizar IPs e domínios para análise e fortalecer políticas de bloqueio e prevenção**.

Dessa forma, o **Fontes de Ataque** amplia a capacidade de análise do ambiente de e-mail, permitindo compreender não apenas **quais ameaças foram detectadas**, mas também **de onde elas estão vindo e quais são as principais origens responsáveis pelas tentativas de ataque**.



Alvos e Risco

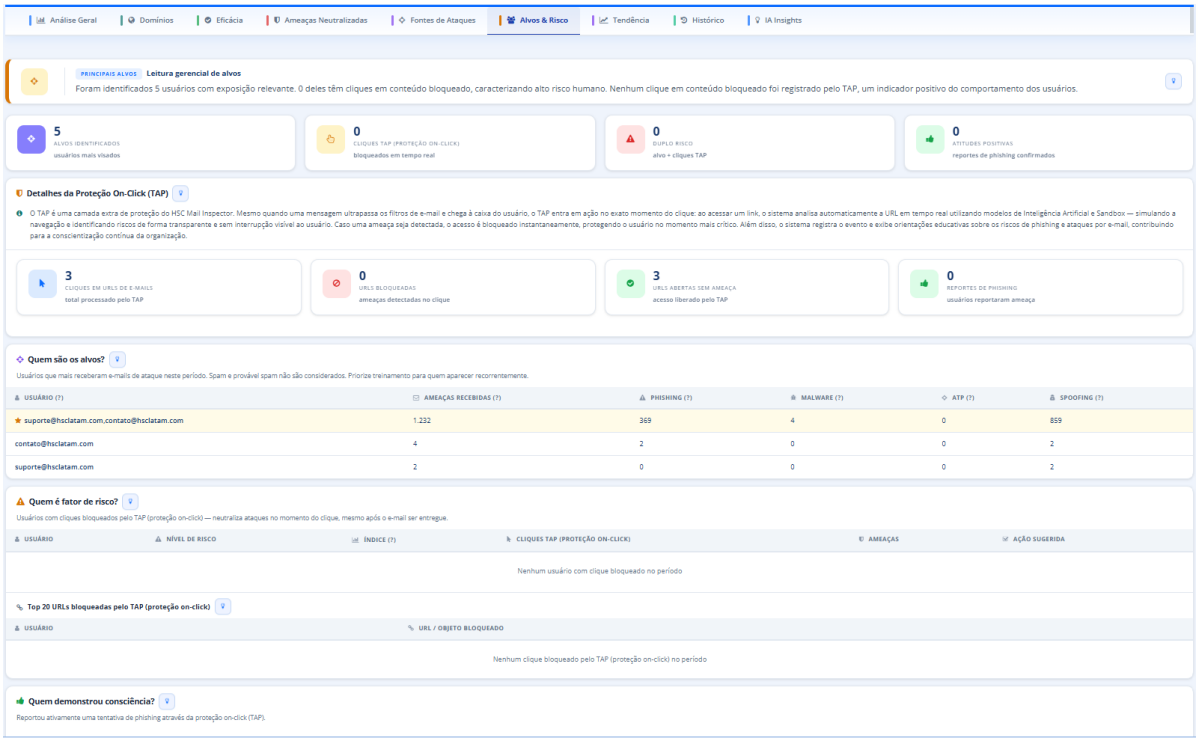
O módulo **Alvos e Risco** permite identificar os usuários mais expostos a ameaças de e-mail, fornecendo uma visão direcionada sobre o **risco associado ao comportamento dos usuários e à frequência de ataques recebidos**.

A solução consolida, por usuário, informações sobre **ameaças recebidas, phishing, malware, ATP, spoofing e demais eventos de segurança**, permitindo identificar quais usuários são mais visados e quais apresentam maior nível de exposição.

O módulo também integra informações da camada de **proteção On-Click (TAP)**, registrando interações com URLs presentes nos e-mails e identificando situações em que usuários tentaram acessar conteúdos potencialmente maliciosos. Quando uma ameaça é detectada durante o acesso, o sistema pode bloquear a URL em tempo real, reduzindo o risco mesmo quando a mensagem já chegou à caixa postal.

A partir desses indicadores, é possível **priorizar usuários para ações de conscientização, treinamento e aplicação de políticas de proteção específicas**, especialmente para usuários críticos ou que apresentam recorrência de exposição.

Dessa forma, o **Alvos e Risco** permite que a equipe de segurança vá além da análise das ameaças e identifique **quem está sendo mais atacado, quais usuários apresentam maior exposição e onde estão os principais riscos humanos no ambiente de e-mail**, direcionando ações preventivas de forma mais eficiente.



Tendência

O módulo **Tendência** permite acompanhar a evolução dos principais indicadores de segurança do ambiente de e-mail ao longo do tempo, comparando o período atual com períodos anteriores. Essa análise possibilita identificar **aumento ou redução no volume de ameaças, alterações na eficácia da proteção e mudanças no comportamento dos usuários**.

O painel apresenta indicadores como **ameaças neutralizadas, volume de e-mails processados, taxa de eficácia, falsos positivos, falsos negativos, tentativas de phishing e interações bloqueadas pelo TAP**, permitindo avaliar a evolução da postura de segurança da organização.

Os gráficos de **volume e ameaças**, **eficácia e qualidade da classificação** e **comportamento do TAP** facilitam a identificação de tendências, variações e possíveis anomalias. A comparação com o período anterior também permite verificar se os controles de segurança estão apresentando evolução ou se determinados indicadores exigem atenção.

O módulo ainda destaca **sinais de melhoria, piora ou estabilidade**, auxiliando a equipe de segurança a identificar rapidamente os indicadores que demandam intervenção. A partir dessas informações, é possível **ajustar políticas de proteção, revisar configurações, investigar mudanças no cenário de ameaças e direcionar ações de conscientização aos usuários**.

Dessa forma, o **Tendência** transforma dados históricos em indicadores de evolução da segurança, permitindo acompanhar continuamente **como o ambiente está se comportando, quais riscos estão aumentando ou diminuindo e onde são necessárias ações preventivas ou corretivas**.

Histórico

O módulo **Histórico** permite acompanhar a evolução do fluxo de e-mails e dos eventos de proteção ao longo dos períodos analisados, proporcionando uma visão consolidada do **comportamento histórico do ambiente de correio eletrônico**.

A solução apresenta a evolução do **volume total de e-mails processados**, permitindo comparar os volumes **entregues e retidos** mês a mês. Também é possível acompanhar a distribuição estimada do tráfego entre **e-mails de entrada, saída e internos**, facilitando a identificação de mudanças no perfil de utilização do ambiente.

Os gráficos históricos permitem visualizar **crescimento ou redução no volume de mensagens**, variações no tráfego e alterações no comportamento de entrega e retenção. A tabela de dados complementa essa análise com os valores consolidados de cada período, permitindo uma avaliação mais precisa da evolução do ambiente.

Essa visão histórica é importante para o planejamento de capacidade, análise operacional e avaliação da efetividade das políticas de proteção, possibilitando identificar **padrões recorrentes, mudanças significativas no fluxo e períodos com maior volume ou maior retenção de mensagens**.

IA Insights

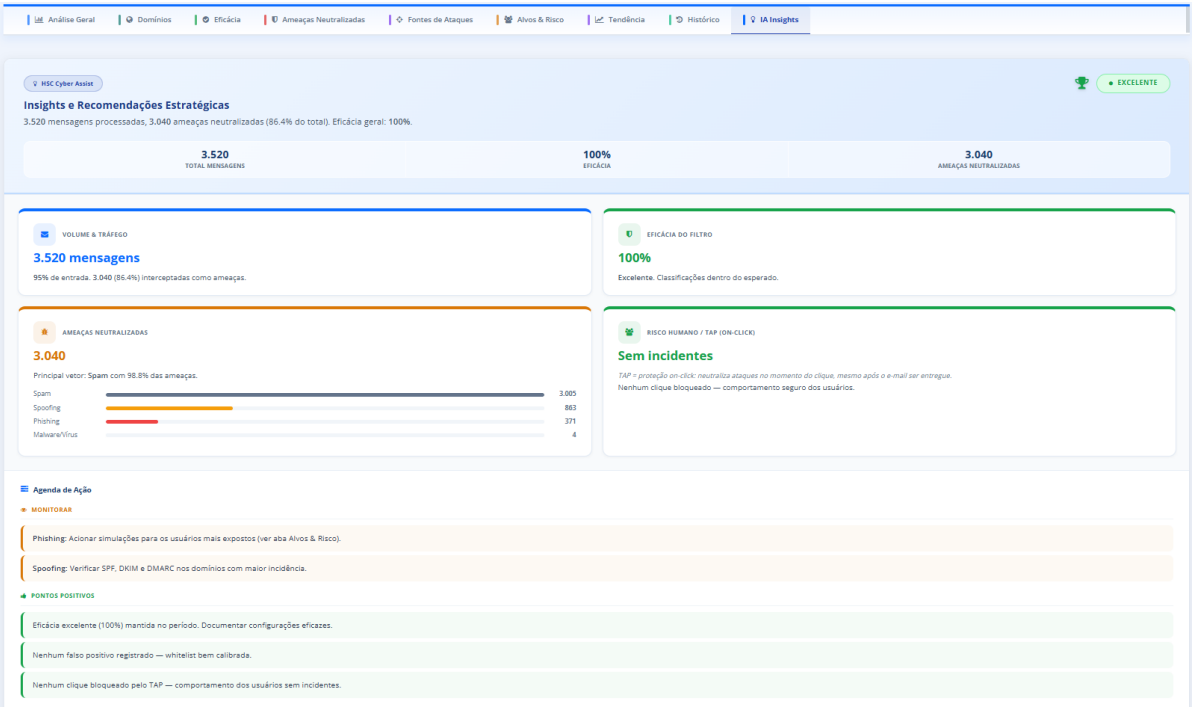
O módulo **IA Insights** utiliza recursos de **Inteligência Artificial, Machine Learning e análise correlacionada dos indicadores de segurança** para transformar os dados do ambiente de proteção de e-mail em **insights estratégicos, recomendações e ações de melhoria**.

A IA analisa informações como **volume de mensagens, ameaças neutralizadas, eficácia dos filtros, falsos positivos e negativos, tipos de ataques, comportamento dos usuários, cliques bloqueados pelo TAP e níveis de risco humano**. A partir da correlação desses dados, identifica padrões, anomalias, tendências e pontos que merecem atenção.

Com base nessa análise, o módulo gera **recomendações contextualizadas**, indicando possíveis ações para aprimorar a postura de segurança. Essas recomendações podem envolver **revisão de políticas, investigação de ameaças avançadas, reforço de controles, integração com outras ferramentas de segurança, ações de conscientização e priorização de usuários de maior risco**.

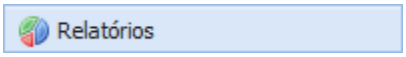
O diferencial está em transformar indicadores isolados em **orientações práticas e priorizadas**, permitindo que a equipe de segurança compreenda não apenas *o que aconteceu*, mas também **o que merece atenção, por que é relevante e quais ações podem ser tomadas para melhorar a proteção**.

Dessa forma, o **IA Insights atua como uma camada de inteligência sobre o MailInspector**, apoiando a tomada de decisão e promovendo a **melhoria contínua das políticas, dos controles de segurança e da capacidade de resposta às ameaças**.


Análise Geral
Domínios
Eficácia
Ameaças Neutralizadas
Fontes de Ataques
Alvos & Risco
Tendência
Histórico
IA Insights
HSC Cyber Assist
EXCELENTE
Insights e Recomendações Estratégicas
3.520 mensagens processadas, 3.040 ameaças neutralizadas (86.4% do total). Eficácia geral: 100%.
3.520
TOTAL MENSAGENS
100%
EFICÁCIA
3.040
AMEAÇAS NEUTRALIZADAS
VOLUME & TRÁFEGO
3.520 mensagens
95% de entrada. 3.040 (86.4%) interceptadas como ameaças.
EFICÁCIA DO FILTRO
100%
Excelente. Classificações dentro do esperado.
AMEAÇAS NEUTRALIZADAS
3.040
Principal vetor: Spam com 98.8% das ameaças.
Spam 3.005
Spoofing 863
Phishing 371
Malware/Virus 4
RISCO HUMANO / TAP (ON-CLICK)
Sem incidentes
TAP = proteção on-click: neutraliza ataques no momento do clique, mesmo após o e-mail ser entregue.
Nenhum clique bloqueado — comportamento seguro dos usuários.
Agenda de Ação
MONITORAR
Phishing: Acionar simulações para os usuários mais expostos (ver aba Alvos & Risco).
Spoofing: Verificar SPF, DKIM e DMARC nos domínios com maior incidência.
PONTOS POSITIVOS
Eficácia excelente (100%) mantida no período. Documentar configurações eficazes.
Nenhum falso positivo registrado — whitelist bem calibrada.
Nenhum clique bloqueado pelo TAP — comportamento dos usuários sem incidentes.

Log de Eventos

Use esta página para exibir e pesquisar ações executadas pelos usuários no sistema do HSC MailInspector.



/ Log de Eventos

Visão geral do log de eventos

O item Logs de Eventos permite visualizar e filtrar os registros das ações realizadas pelos usuários e administradores através da interface de administração do HSC MailInspector. Permite auditar todas as ações tomadas pelos usuários a fim de identificar quaisquer abusos ou ações indevidas. Dessa forma pode-se considerar o log de eventos também como log de auditoria do sistema.

São registrados todos os eventos efetuados pelos usuários e administradores (criação, remoção, edição de qualquer elemento no MailInspector, até mesmo leitura e acesso a e-mails quarentenados e/ou auditados, bem como logs de indicação de recusa na conexão, entre outras informações), tanto por acesso via sistema gráfico do gerenciamento, quanto por SSH, ou até mesmo por eventual acesso remoto.

O log de evento também apresenta o registro do objeto manipulado antes da alteração, para que o administrador possa recriar o registro, caso o mesmo tenha sido removido. Por exemplo, se alguém tiver removido uma entrada na allow list, o log de evento apresentar os dados do registro da allow list removida, para que o administrador possa recriar a entrada.

Basicamente é o sistema de auditoria do MailInspector, onde indica a ação executada por qualquer usuário (desde administrador até usuário final).

Em caso de remoção de alguma regra ou allow list/block list, é possível visualizar os dados da regra removida, dessa forma permitindo ao administrador efetuar a recriação manual da mesma, se houver necessidade.

Os dados apresentados pelos registros por padrão são:

- Data e hora da ação;
- Usuário;
- Ação:
  - Criação de regra;
  - Remoção de regra;
  - Modificação da regra;
  - Acesso a mensagem;
  - Leitura da mensagem (visualização do conteúdo);
  - Download da mensagem;
  - Download dos anexos,
  - Modificação de parâmetros da solução;
  - Entre outras ações;
- IP de quem fez a ação;
- Campo e valor (dados alterados/criados/excluídos);

Não há um limite dos logs de eventos, isto é, os logs não são apagados, dessa forma, todo log de evento fica armazenado “eternamente” no sistema, sem limite quantitativo de registro de eventos, somente podendo ser apagado via linha de comando pelo superusuário (root) do MailInspector,

acessando o Banco de Dados criptografado em tabela específica (é necessária abertura de chamado técnico para esse procedimento).

A capacidade de armazenamento (de toda o sistema, incluindo logs, auditoria e quarentena de e-mails) depende unicamente de quantidade de disco reservada para esse propósito, lembrando que é possível utilizar discos dinâmicos, para aumento da capacidade de armazenamento, sem necesdidade de reinstalação da solução.

O log de eventos apresentado é de acordo com a língua configurada pelo administrador, isto é, se a interface estiver configurada em Espanhol por exemplo, o log será na língua espanhola.

O sistema de log de eventos é totalmente aderente a LGPD, sendo assim, nesse log não é exibido nenhuma informação sensível, como por exemplo dados pessoais ou senhas. No log de Log de Eventos, indica somente data e hora de execução da ação, bem como quem fez a ação indicada.

Definições de Opções - Log de Eventos

Estas informações descrevem as opções disponíveis nesta página.

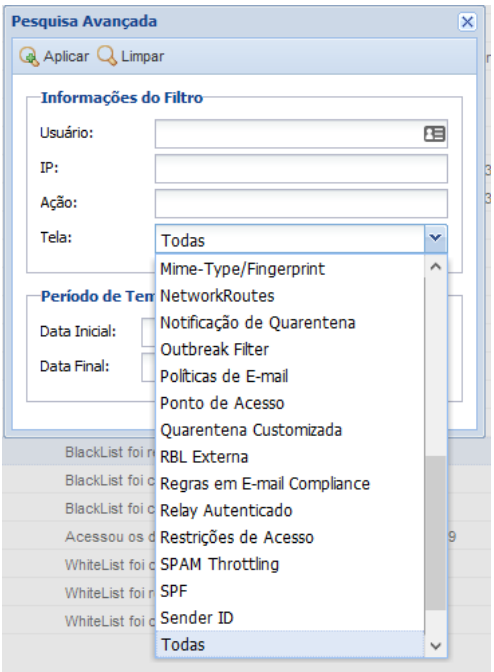
Opções	Definição
Pesquisar	Quando clicado, aplica o filtro informado na caixa de pesquisa rápida aos registros de eventos.
Limpar	Quando clicado, remove os filtros informados da caixa de pesquisa rápida e da janela de pesquisa avançada, e recarrega todos os registros de eventos.
Pesquisa Avançada	Realiza uma pesquisa mais detalhada nos registros. Quando clicado, abre a caixa de diálogo **Pesquisa Avançada**.
Exportar	Permite a exportação do log de eventos em formato CSV ou PDF com o filtro atual ativo.

Definições de Opções - Pesquisa Avançada

Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição
Aplicar	Quando clicado, aplica os filtros informados e/ou selecionados aos registros de eventos.
Limpar Campos	Quando clicado, remove os valores informados ou selecionados pelo usuário.
Usuário	Informe o nome de login completo do usuário.
IP	Informe o endereço IP completo do usuário.
Ação	Informe a ação completa ou parcial executada pelo usuário.
Tela	Informe qual módulo aplicada na ação. Caso não saiba qual módulo que foi a ação, basta selecionar ***Todas***.
Data Inicial	Permite definir uma data inicial para pesquisa.
Data Final	Permite definir uma data final para pesquisa.

Exemplo de uso de consulta com Pesquisa Avançada:
Se eu quiser fazer buscas de registros de e-mails lidos pelo administrador, basta preencher o campo USUÁRIO como admin e o campo AÇÃO com a palavra LEU, sendo em qualquer módulo (Todas)



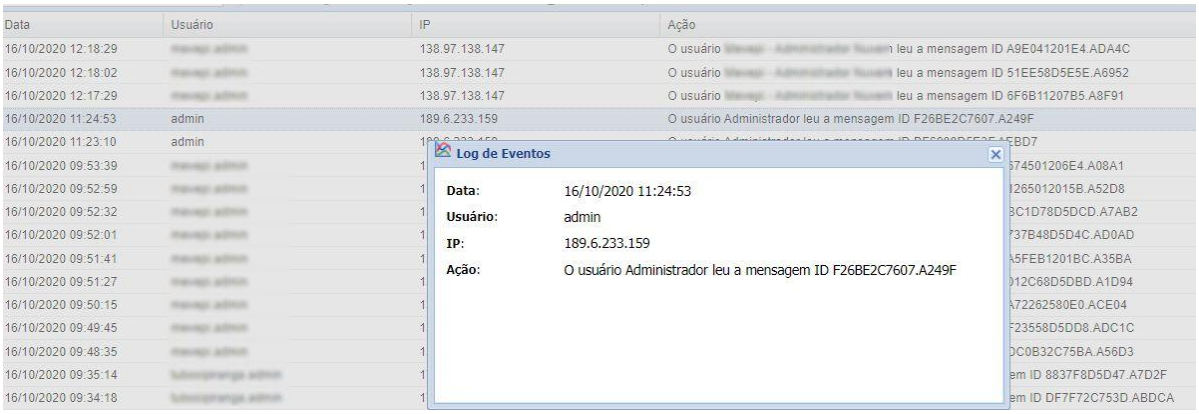
Exemplo de pesquisa avançada.

Resultado da Pesquisa - Log de Auditoria

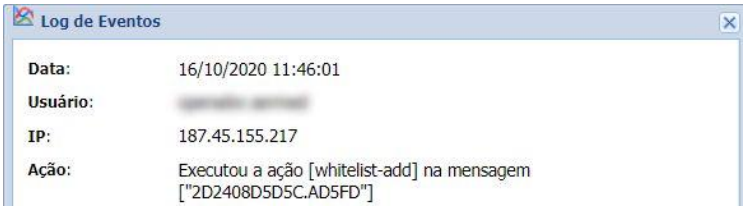
Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição
Data	Data e hora do registro da ação
Usuário	Login do usuário que executou a ação
IP	Endereço IP utilizado pelo usuário para acessar o MailInspector
Ação	Detalhes da ação realizada pelo usuário

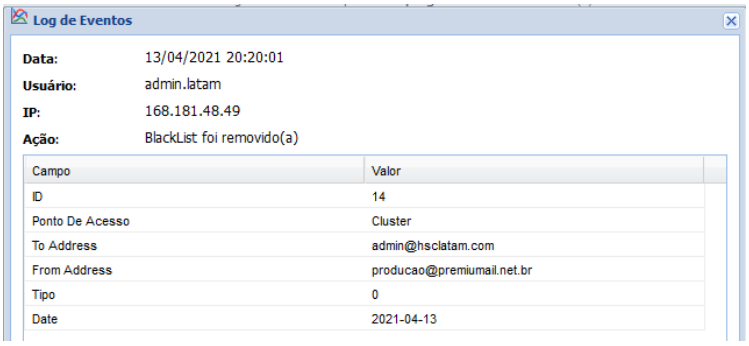
Os resultados apresentados são de TODAS as ações, isto é, também são registradas as ações que não são obrigatoriamente efetuadas somente na Interface de Gerenciamento, como por exemplo Liberação de e-mail quarentenado usando o link de liberação que está no e-mail de notificação de quarentena, ou inclusão de remetente em allow list/block list através do link que está no e-mail de notificação de quarentena.



Lista de eventos executados no MLI. Ao dar duplo clique sobre um evento específico, apresenta-se os dados com maiores detalhes.



Exemplo de que foi efetuada a ação de acréscimo de allow list sobre a mensagem, pelo usuário indicado.

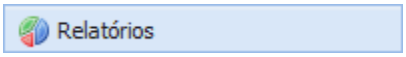


Exemplo de log de remoção de block list, onde aparecem os dados do registro antes da remoção (para caso o administrador precise recriar o registro).

Com o log de eventos, é possível verificar todas as ações efetuadas por qualquer usuário e se for o caso, fazer um roll back "manual", de acordo com os logs indicados na ação executada. Por exemplo, é possível fazer roll back de ação de exclusão de entrada de block list (conforme exemplo da imagem anteriormente apresentada).

Agendados

Use esta página para exibir e pesquisar ações executadas pelos usuários no sistema do HSC MailInspector.



/ Agendados

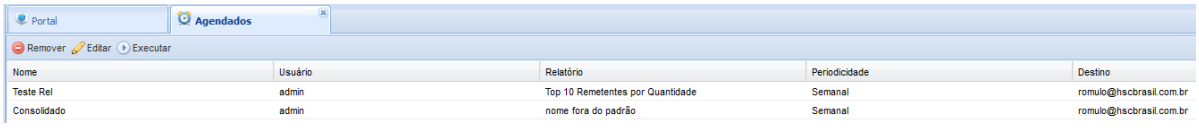
Visão geral Agendados

Nesta tela podemos ver todos os relatórios que foram agendados para o envio automático por e-mails, podendo o administrador remover ou editar o agendamento. Os agendamentos podem ser feitos através da tela de relatórios, após um relatório ser gerado.

Definições de Agendamento

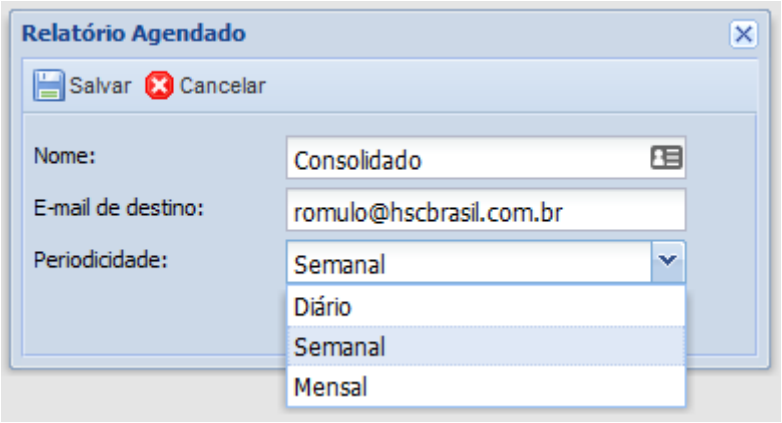
A grid apresenta os dados do relatório agendado, tais como:

- **Nome:** Nome do Agendamento criado;
- Usuário que agendou;
- **Relatório:** Nome do Relatório;
- **Periodicidade:** Diário/Semanal/Mensal;
- **E-mail de Destino:** Para onde será enviado o relatório agendado.



É possível executar as seguintes ações sobre um relatório agendado:

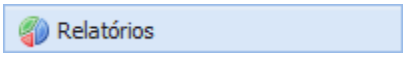
- Remover: Apara o relatório agendado da lista;
- Editar: Permite a edição do relatório agendado, permitindo mudar os campos:
  - **Nome:** Nome do Relatório;
  - **E-mail de destino:** Para qual e-mail será enviado o relatório;
  - **Periodicidade:** Selecione o período de execução;
    - Diário;
    - Semanal;
    - Mensal;
- Executar: Roda o relatório agendado;



Por padrão os relatórios agendados são enviados como anexo em PDF.

Capacity Planning

Com o capacity planning, é possível planejar futuras expansões de disco, update de processador ou aumento de memória do HSC MailInspector, visualizando o crescimento de consumo de recursos pelo tempo de uso.



/ Capacity Planning

Visão Capacity Planning

Nesta tela podemos ver o consumo dos recursos do equipamento em relação a tempo de uso, com isso, o administrador pode planejar crescimento de hardware necessário para manter o bom funcionamento do sistema de proteção a e-mail.

Com a seleção de datas prévias anteriores, é apresentando o histórico de uso de recurso de sistema do mesmo, ou seja, com esse relatório é possível visualizar o consumo de recursos anteriores, comparando com o uso atual, para um planejamento mais eficiente de uso de recurso.

Os relatórios de Capacity Plannig, são separados por:

- Pontos de Acesso;
- Sistema de Gerenciamento;

Definições de Opções – Capacity Planning

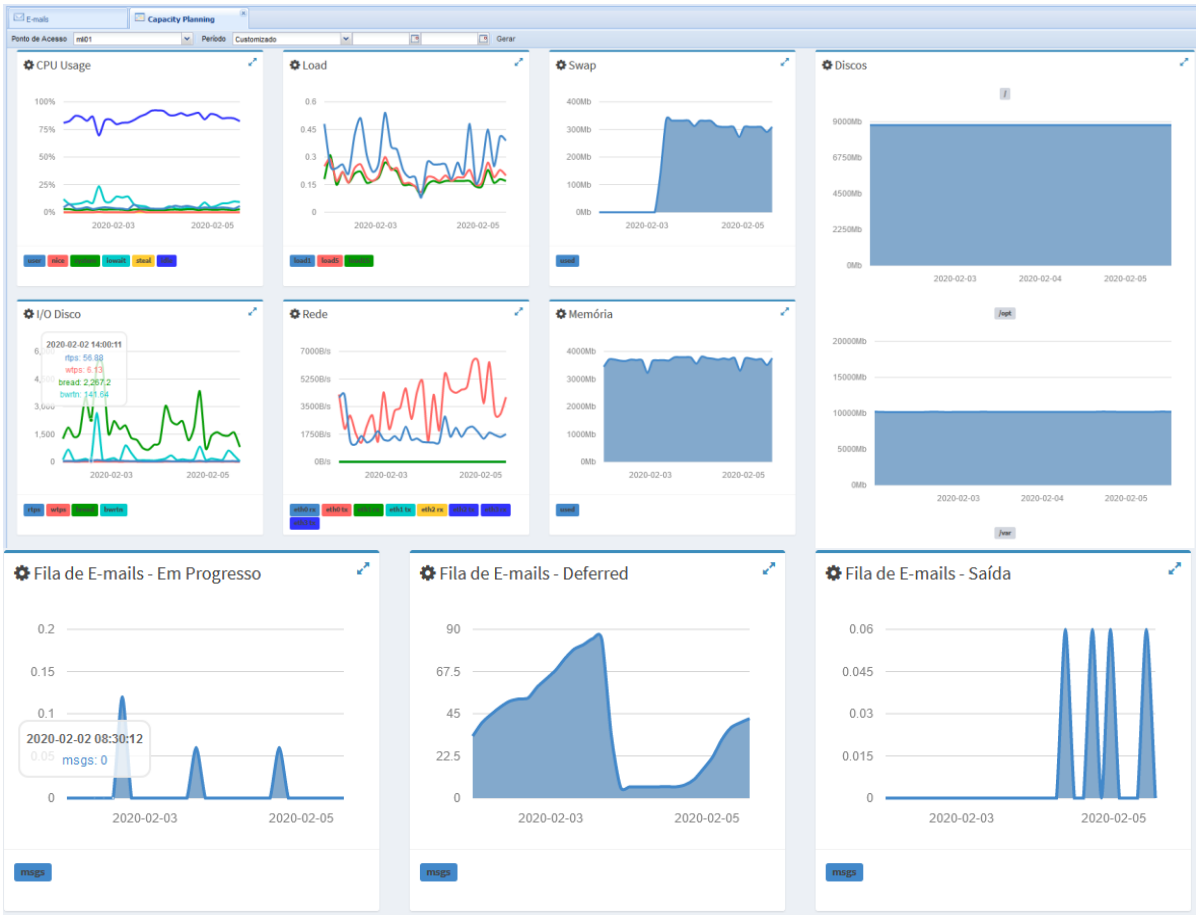
Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição
Ponto de Acesso	Seleção de qual ponto de acesso ou da máquina de gerenciamento que será extraído os dados para análise do relatório de Capacity Planning.
Período	De qual período que o administrador deseja efetuar a análise. É possível visualizar o planejamento para: • Hoje; • Ontem; • Esta semana; • Última semana; • Este mês; • Último mês; • Customizado; Ao selecionar customizado é aberto a opção de selação de data inicial e final, ao qual o administrador deve indicar o período de dados a serem analisados.

Os pontos analisados do Capacity Planning são:

- Uso de CPU;
- Carga de uso;
- Swap;
- Uso de disco;
- I/O de disco;
- Uso de rede;
- Consumo de memória;
- Fila de e-mail em processamento;

- Fila de e-mails negados;
- Fila de e-mails de saída;



Tela de Capacity Planning

Menu - Configurações

Cadastros

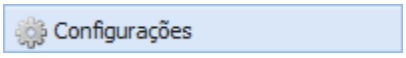
Em Cadastros, o administrador pode efetuar cadastro dos mais diversos tipos de objetos, sendo aplicados posteriormente em regras. Os tipos de cadastros possíveis no MillInspector são:

- Grupos Usuários;
- Anexos;
- Mime-Types / Fingerprint;
- Dicionário de Palavras;
- RBL Externas;

É possível criar regras de políticas para e-mails de entrada e saída, casando qualquer um dos cadastros acima citados com operadores lógicos e condicionadores. As políticas criadas podem ser desde regras simples de spam, até mesmo regras de E-mailCompliance, tais como DLP, ativação de criptografia de e-mail, detecção de vazamento de número de cartão de crédito ou placa de veículo, quarentena customizada, etc.

Grupos Usuários

Use esta página para exibir, adicionar, editar ou excluir grupos endereços de e-mail, domínios, endereços IP, endereços de rede, intervalos de endereços IP, expressão regular (nomes parciais) e grupos de diretórios LDAP, alias, Grupos e Listas de Distribuições.



/ Cadastros / Grupos Usuários

Visão geral do cadastro de grupos de usuários

Os grupos de usuários são utilizados para agrupar:

- Endereços de e-mail;
- Grupos de endereços eletrônicos;
- Usuários;
- Endereços de e-mail de diretórios LDAP, Microsoft Active Directory ou outro sistema que possa ser sincronizado com Conectores Externos;
- Domínios;
- Nomes parciais de domínios;
- Subdomínios;
- Listas de distribuição;
- Aliases de e-mail;
- Endereço principal de e-mail;
- Endereços de IP;
- Endereços de rede;
- Intervalos (range) de endereços IP;
- Expressão Regular (Nomes parciais);
- Grupos de LDAP;

Os grupos criados poderão ser utilizados em regras ou exceções.

A ferramenta permite a criação de grupos mistos, pode-se criar apenas grupos de e-mail, ou apenas grupos de domínio, ou realizar uma combinação entre todos os itens disponíveis.

Uma vez criado um grupo o administrador poderá utilizá-lo em todas as regras podendo compor filtros específicos tanto para filtrar entrada ou saída de e-mails.

Ao criar grupos de usuários, é possível aplicar uso deles para determinar "rotas" de regras, por exemplo:

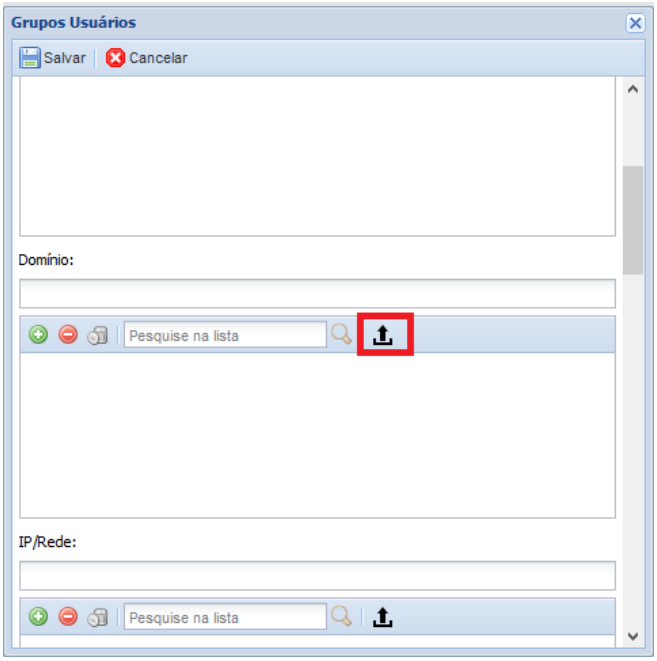
Grupo de Usuários Internos = Domínios Internos na Empresa (ex: hscbrasil.com.br) Sendo considerado rota: **Inbound**: Regra oriunda **DE** Todos **PARA** Grupo de Usuários Internos e **Outbound:** Regra dos e-mails oriunda **DE** Grupo de Usuários Internos **PARA** Todos.

É possível também IMPORTAR as listas de grupos previamente criados, para isso, basta clicar no botão de IMPORTAÇÃO no grupo com os dados.

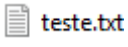
O arquivo para importação deve ser em formato TXT, com os registros um abaixo do outro.
Modelo de formato do arquivo TXT padrão para importação de grupos de domínios, para importação:

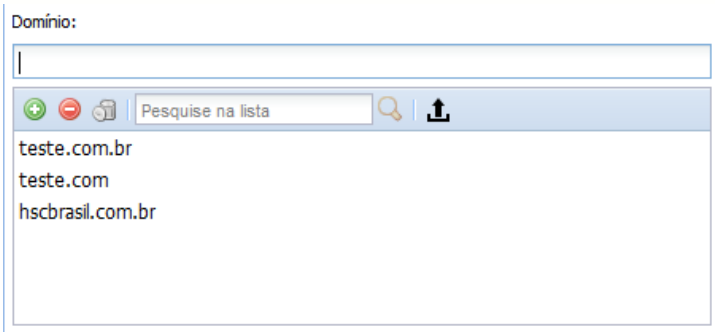
teste.com teste.com.br hscbrasil.com.br

Para exemplo, criamos um arquivo chamado teste.txt com os registros acima citado.
Abaixo efetuada a importação do arquivo TESTE.TXT



Importando arquivo com domínios.




Domínio:
Pesquise na lista
teste.com.br
teste.com
hscbrasil.com.br

Definições de Opções - Gerenciamento de Grupos de Usuários

Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição
Adicionar	Cadastra um novo registro de grupo. Quando clicado, abre a caixa de diálogo **Gerenciar Grupos**.
Editar	Edita as configurações de um registro existente. Quando clicado, abre a caixa de diálogo **Gerenciar Grupos**.
Remover	Quando clicado, exclui o registro selecionado. Ao remover um grupo, todas as regras em que este grupo foi utilizado serão removidas do sistema.
Pesquisar	Quando clicado, aplica o filtro informado na caixa de pesquisa rápida as mensagens.
Limpar	Quando clicado, remove os filtros informados da caixa de pesquisa rápida e da janela de pesquisa avançada, e recarrega todos os registros de Grupos Usuários.
Pesquisa Avançada	Realiza uma pesquisa mais detalhada nos registros. Permitindo um rastreio completo e preciso de um grupo. Quando clicado, abre a caixa de diálogo Pesquisa Avançada.

Definições de Opções - Pesquisa Avançada

É possível efetuar pesquisa nos grupos de usuários através de praticamente qualquer campo do grupo, desde nome/descrição do grupo, até mesmo por e-mails ou domínios contidos no grupo.

Opções	Definição
Nome/Descrição	Informe o nome ou parte do nome ou até mesmo descrição do grupo a ser pesquisado.
Usuários	Informe nome ou parte do nome de um usuário a ser pesquisado, que faça parte do grupo procurado.
E-mails	Informe e-mail completo ou parte do e-mail a ser pesquisado, que faça parte do grupo procurado.
Domínios	Indique o domínio a ser pesquisado.
Aplicar	Efetua a busca de acordo com os campos preenchidos.
Limpar	Quando clicado, remove os todos os filtros informados e recarrega todos os registros de Grupos Usuários.

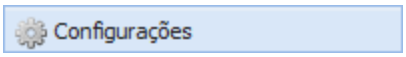
Definições de Opções - Gerenciar Grupos de Usuários

Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição
Salvar	Quando clicado, grava as configurações realizadas.
Cancelar	Quando clicado, cancela a ação.
Nome do Grupo	Informe o nome de identificação do grupo. Ex.: Administração.
Descrição do Grupo	Informe, opcionalmente, uma breve descrição do grupo ou de sua composição.
Ativo	Escolha entre: • Sim - Indica que o grupo está ativo, e as regras em que este grupo foi utilizado serão aplicadas. • Não - Indica que o grupo está inativo, e as regras em que este grupo foi utilizado não serão aplicadas.
E-mail	Informe endereços de e-mail dos usuários pertencentes ao grupo. Ex.: nome@empresa.com.br. Este campo permite especificar um endereço de e-mail, alias ou uma lista de distribuição.
Domínio	Informe nomes de domínio pertencentes ao grupo. Ex.: empresa.com.br.
IP/Rede	Informe endereços IP ou endereços de rede pertencentes ao grupo. Ex.: 192.168.2.0/24.
Range IP	Informe ranges de endereços IP pertencentes ao grupo. Ex.: 192.168.2.1-100.
Expressão Regular (Nomes parciais)	Informe expressões regulares para nomes parciais de domínio pertencentes ao grupo. Ex.: *.empresa\.com\.br.
Usuários	Selecione um usuário criado ou importado na interface de administração. Aqui você poderá informar se quer todos endereços do usuário, somente alias, ou somente endereço principal. Conforme for selecionado a ferramenta é capaz de identificar a diferença entre aliases de e-mail e endereço principal, esta funcionalidade é compatível com os principais sistemas de correio eletrônico, tais como: • Microsoft Exchange; • Zimbra; • Novell GroupWise; • Lotus Notes/Lotus Domino, etc.
Listas de Distribuição	Selecione as listas de distribuição importadas de um servidor LDAP/Microsoft Active Directory/Zimbra.
Grupos LDAP	Permite selecionar grupos de bases LDAP: • Microsoft Active Directory; • Open LDAP; • Zimbra; Distinguindo Usuários, Alias e Listas de Distribuição.

Anexos

Use esta página para exibir, adicionar, editar ou excluir grupos de anexos.



/ **Cadastros / Anexos**

Visão geral do cadastro de anexos

Os grupos de anexos são utilizados para agrupar nomes, extensões ou expressões regulares que serão submetidos a alguma regra. Seguem alguns exemplos de possibilidade de uso no cadastro de anexos:

- Anexos em políticas específicas, tanto na entrada de e-mails, quanto na saída;
- Anexos em regras de E-mail Compliance, entre eles regras de DLP e/ou quarentena customizada;
- Anexos em regras de Criptografia de e-mail, por exemplo criptografar e-mail quando estiver com determinado anexo, sendo o mesmo com destino a diretor da empresa X;
- Determinados anexos, que contenham palavras chaves específicas dentro, tomar alguma ação, tal como por exemplo criptografar o e-mail;

A engine do HSC MailInspector permite analisar anexos dentro de arquivos compactados e efetuar as ações sobre os mesmos, como exemplo a remoção de objetos de dentro do arquivo compactado.

O MailInspector analisa o nome completo do arquivo para um maior controle do administrador, ficando a cargo do administrador criar a expressão regular que desejar para casar com o Anexo.

O MailInspector permite que seja criado **qualquer tipo de agrupamento de anexos**, aplicando-os em regras/políticas, podendo ser nome completo do arquivo ou somente a extensão do anexo. Segue alguns exemplos de grupos de anexos possíveis de serem cadastrados no MailInspector:

- Anexos de extensões para documentos do tipo Office, com e sem senha: .DOC, .DOCX, .XLS, .XLSX, .PPT, .PPTX, .PPS, .RTF, .DOCM, .DOT, .DOTM, .HTM, .HTML, .MHT, .MHTML, .ODT, .PDF, .TXT, .WPS, .XPS, .CSV, .DBF, .DIF, .ODS, .PRN, .SLK, .XLA, .XLAM, .XLSB, .XLSM, .XLT, .XLTM, .XLTX, .XLW, .XPS, .ODP, .POT, .POTM, .POTX, .PPA, .PPAM, PPSM, .PPTM, .THMX
- Anexos de extensões do tipo Imagem: .BMP, .GIF, .JPG, .JPEG, .PNG, .TIF, .WMF, .EMF
- Anexos de extensões do tipo áudio e vídeo: .MP4, MP3, WMA, .MPEG, .MPE, .AVI, .MOV, .WMV, .FLV, .MKV, .RM
- Outros: .386, ACM, .ASP, .AVP, .CGI, .CHM, .CLA, .CLASS, .SWF, .RAM, .VOB, .DAT, .LNK, .SYS, .DLL, .EXE, .COM
- Anexos com extensões de arquivos compactados: .ZIP, .RAR, .CAB, .ACE, .ARJ, .BH, .HA, .JAR, .PAK, .LHA, .LZH, .PKZIP, .BZIP, .GZIP, .BZ2, .BZIP2, .ZOO, .7Z, .TZH, .TGZ, .TAR, .GZ
- Anexos Executáveis: .EXE, .CMD, .BAT, .LNK
- Sistemas de codificação: UUENCODE, UUDECODE, BASE64, etc
- Entre diversas outras extensões (até mesmo extensões “inexistentes”, tais como .ABC, .XYZ) .

Definições de Opções - Gerenciamento de Anexos

Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição

Adicionar	Cadastra um novo registro de grupo. Quando clicado, abre a caixa de diálogo **Gerenciar Anexos**.
Editar	Edita as configurações de um registro existente. Quando clicado, abre a caixa de diálogo **Gerenciar Anexos**.
Remover	Quando clicado, exclui o registro selecionado. Ao remover um grupo, todas as regras em que este grupo foi utilizado serão removidas do sistema.

Definições de Opções - Gerenciar Anexos

Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição
Salvar	Quando clicado, grava as configurações realizadas.
Cancelar	Quando clicado, cancela a ação.
Descrição	Informe o nome de identificação do grupo. Ex.: Anexos Bloqueados.
Expressão Regular	Informe os nomes, extensões ou expressões regulares que serão adicionados ao grupo. Para combinar com um nome de arquivo específico: boleto\.pdf, para combinar com uma extensão: \.asf$, e para formar uma expressão regular: documento\.(doc|xls|ppt).

O MailInspector já vem com algumas configurações de anexos pré-configurados para uso em regras de bloqueio/liberação de anexos. Os anexos pré-configurados são:

- **Possivelmente Perigosos:** .386, .3GR, .ADD, .ADE, .ADP, .ASP, .BAS, .BAT, .CHM, .CMD, .COM, .CPL, . CRT, .DBX, .DLL, .EXE, .FON, .HLP, .HTA, .INF, .INS, .ISP, .JAR, .JS, .JSE, .LIB, .LNK, .MDB, .MDE, .MSC, .MSI, .MSP, .MST, .NSH, .OCX, .PCD, .PIF, .PPA, .PPAM, .REG, .SCR, .SCT, .SHB, .SHS, .SYS, .TMP, .URL, .VB, .VBE, .VBS, .VXD, .WSC, .WSF, .WSH.
- **Proibidos:** .BAT, .CMD, .EXE, .PIF.

Mime-Types/Fingerprint

Use esta página para exibir, adicionar, editar ou excluir grupos de mime-type/fingerprint.

Configurações / **Cadastros / Mime-Types/Fingerprint**

Visão geral do cadastro de mime-types e fingerprints

Os grupos de mime-types/fingerprint são utilizados para agrupar tipos MIME de arquivos que serão submetidos a alguma regra, podendo ser desde regras em políticas específicas, quanto a regras de auditoria, DLP, E-mail Compliance, quarentena customizada, ou até mesmo regras em relação a criptografia de e-mail. Através destes, é possível filtrar anexos baseados nos seu "File Types"/"True Types" ou Fingerprint.

Através do mime-type/fingerprint é possível determinar com precisão o tipo do arquivo, desta forma é possível prevenir que usuários maliciosos anexem arquivos com extensão, por exemplo EXE, de forma renomeada, exemplo TXT, a fim de burlar os filtros de segurança. A engine do HSC inclusive, permite analisar anexos dentro de arquivos compactados.

O HSC MailInspector já vem com uma lista de mais de 300 tipos de arquivos File Type/Finger Print/Mime-Type e extensões reais, dentre as quais arquivos texto, executáveis, compactados, planilhas, documentos padrão Office (MS Word, Excel, PDF, Power Point, arquivos Open Office, etc), arquivos de imagens, banco de dados, ao qual são constantemente atualizados, porém o administrador também poderá adicionar novos tipos, caso ele deseje.

Definições de Opções - Gerenciamento de Mime-Types/Fingerprint

Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição
Adicionar	Cadastra um novo registro de grupo. Quando clicado, abre a caixa de diálogo **Gerenciar Mime-Types/Fingerprint**.
Editar	Edita as configurações de um registro existente. Quando clicado, abre a caixa de diálogo **Gerenciar Mime-Types/Fingerprint**.
Remover	Quando clicado, exclui o registro selecionado. Ao remover um grupo, todas as regras em que este grupo foi utilizado serão removidas do sistema.

Definições de Opções - Gerenciar Mime-Types/Fingerprint

Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição
Salvar	Quando clicado, grava as configurações realizadas.
Cancelar	Quando clicado, cancela a ação.
Nome	Informe o nome de identificação do grupo. Ex.: Mime-Type - Aplicações.

Lista de Mime-Types	Informe os mime-types/fingerprints que serão adicionados ao grupo. Além dos tipos MIME pré-cadastrados, é possível inserir qualquer outro mime-type conforme a sua necessidade. Ex.: application/*.

Dicionário de Palavras

Use esta página para exibir, adicionar, editar ou excluir grupos de dicionários de palavras.

Configurações / **Cadastros / Dicionário de Palavras**

Visão geral do cadastro de dicionários de palavras

Os grupos de dicionários de palavras são utilizados para agrupar expressões que serão submetidos a alguma regra. O HSC MailInspector já vem com alguns dicionários de palavras consideradas sensíveis pela LGPD e dicionários compatíveis com regras de controle de saída/entrada de e-mails, tais como:

- CPF;
- RG;
- CNH;
- CNPJ;
- IPv4, IPv6;
- Placa de Carro padrão Mercosul;
- Números de Passaporte brasileiro;
- E-mails/Lista de e-mails (padrão RFC 5322);
- Dicionários de termos estrangeiros:
  - SIN Canadense (Social Insurance Number - Número de seguridade social canadense);
  - US SSN (Social Security Number - Número de seguridade social americano);
  - ABA Routing (Identificação bancária de cheques americanos);
  - RTN (Bank Routing Transit Number);
  - CUSIP (Identificação de título financeiro americano);
  - ISIN (International Securities Identification Number);
  - DNI (National Identity Number - Argentina);
  - Número de Telefone:
    - Padrão francês;
    - Padrão alemão;
    - Padrão inglês (Reino Unido);
    - Padrão americano;
    - Entre outros;
  - Número do Passaporte:
    - Francês;
    - Alemão:
    - Inglês (Reino Unido);
    - Canadá;
    - Entre outros;
  - Vários outros dicionários de termos estrangeiros;
- TLP (Traffic Light Protocol), com os seguintes termos:
  - TLP:RED
  - TLP:AMBER
  - TLP:GREEN
  - TLP:CLEAR
- Palavras-chave tipicamente utilizados em ataques de phishing;

- Palavras-chave comumente utilizado em formulários de roubo de informações;
- Número de Cartão de crédito (de acordo com a bandeira utilizada):
    - VISA;
    - MASTERCARD;
    - AMEX;
    - Entre outros;
- São mais de 200 templates aplicados como dicionário de palavras

O MailInspector possui mais de 200 templates de dicionários aplicados na solução. Ainda é possível criar novos dicionários baseados em Expressões Regulares, dessa forma, os dicionários poderão ser de praticamente qualquer coisa, faixa de IP, palavras em inglês, palavras que contenham letras e sequência numérica, palavras mais utilizadas em campanhas de spam, palavras mais utilizadas em campanhas de phishing, placas de carro, etc. Também é possível alterar a pontuação do e-mail, mediante detecção de palavras contidas tanto no corpo do e-mail, quanto em anexos. O MailInspector permite limitar a pontuação máxima a ser considerada de acordo com a regra aplicada em relação ao dicionário de palavras. Também é importante ressaltar que criar um dicionário não quer dizer que já esteja sendo ativo e utilizado, é necessário atribuí-lo a regra/política e a regra/política deve estar ativa para que o dicionário criado esteja operacional.

Os dicionários poderão ser utilizados em regras tanto de entrada como de saída de e-mails e em combinação com outras regras de grupos de usuários, podendo ser concatenados com operadores lógicos, na hora da criação das regras, garantindo dessa forma nível elevado de precisão, incluindo peso por palavra repetida. O dicionário de palavras pode atuar em todo o e-mail, desde o assunto do e-mail, conteúdo no corpo, até mesmo conteúdo em anexo e em outros campos do e-mail.

Como o dicionário de palavras atua em todo o e-mail, é possível por exemplo criar nomes de anexos e verificar a presença dos mesmos nos e-mails, efetuando ação desejada sobre os e-mails com os anexos indicados no dicionário de palavras.

Os dicionários no MailInspector também atuam em palavras contidas dentro dos arquivos em anexo, isto é, possui a capacidade de verificar palavras contidas em anexos dos mais variados tipos, mesmo que estes estejam compactados.

É possível delimitar um valor máximo de palavra combinando o valor da palavra com número de repetições, ao qual somente será pontuado quando ocorrer quantidade X de repetições, dessa forma podendo pontuar um valor máximo devido ao número de repetições. Por exemplo: Palavra SPAM terá valor de 5, mas somente quando for repetido pelo menos 5x dentro do e-mail.

Se o administrador desejar, pode-se criar dicionários contendo palavras consideradas banidas (Banned Word), ou até mesmo dicionário contendo palavras “atenuantes”, que baixem a pontuação de spam, para aplicação em regras e outros dicionários conforme necessidade da empresa.

Definições de Opções - Gerenciamento de Dicionários de Palavras

Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição
Adicionar	Cadastra um novo registro de grupo. Quando clicado, abre a caixa de diálogo **Gerenciar Dicionários de Palavras**.
Editar	Edita as configurações de um registro existente. Quando clicado, abre a caixa de diálogo **Gerenciar Dicionários de Palavras**.

Remover	Quando clicado, exclui o registro selecionado. Ao remover um grupo, todas as regras em que este grupo foi utilizado serão removidas do sistema.

Definições de Opções - Gerenciar Dicionários de Palavras

Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição
Salvar	Quando clicado, grava as configurações realizadas.
Cancelar	Quando clicado, cancela a ação.
Nome	Informe o nome de identificação do grupo. Ex.: Documentos.
Descrição	Informe uma descrição para o grupo. Ex.: Identifica documentos do tipo CPF.
Expressões	Informe as expressões regulares que serão adicionadas ao grupo. Ex.: /^\d{3}\.\d{3}\.\d{3}\-\d{2}$/.

RBLs Externas

Use esta página para exibir, adicionar, editar ou excluir RBLs "Real Time Blacklists" externas. É também neste mesmo campo a inclusão de URI (Uniform Resource Identifier) externas.

Configurações / **Cadastros / RBLs Externas**

Visão geral do cadastro de RBLs Externas

O cadastro de RBLs e URI Externas permite adicionar novas RBLs e listas de URI externas para consulta de possíveis fontes de SPAM e ameaças de links, conforme a necessidade do Administrador.

Por padrão o MailInspector já vem com algumas listas de RBL/URI cadastradas:

- HSC Brasil;
- SpamHaus;
- SpamCop;
- SORBS DNSBL.

Definições de Opções - Gerenciamento de RBLs Externas

Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição
Adicionar	Permite adicionar uma nova fonte de consulta RBLs/URI Externas.
Editar	Edita as configurações de um registro existente. Quando clicado, abre a caixa de diálogo RBLs/URI Externas
Remover	Quando clicado, exclui o registro selecionado. Ao remover um grupo, todas as regras em que este grupo foi utilizado serão removidas do sistema.

Definições de Opções - Gerenciar RBLs Externas

Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição
Salvar	Quando clicado, grava as configurações realizadas.
Cancelar	Quando clicado, cancela a ação.
Nome	Informe o nome de identificação da RBL/URI. Ex.: HSC RBL.
Descrição	Informe uma descrição para o grupo.
Servidor FQDN	Endereço FQDN para consulta no servidor Externo. Ex: rbl.hscbrasil.com.br

Lista de algumas RBL's Opcionais

aspews.ext.sorbs.net
b.barracudacentral.org
bl.deadbeef.com
bl.e-mailbasura.org
bl.spamcannibal.org
bl.spamcop.net
blackholes.five-ten-sg.com
blacklist.woody.ch
bogons.cymru.com
cbl.abuseat.org
cdl.anti-spam.org.cn
combined.abuse.ch
combined.rbl.msrbl.net
db.wpbl.info
dnsbl-1.uceprotect.net
dnsbl-2.uceprotect.net
dnsbl-3.uceprotect.net
dnsbl.cyberlogic.net
dnsbl.dronebl.org
dnsbl.inps.de
dnsbl.njabl.org
dnsbl.sorbs.net
drone.abuse.ch
duinv.aupads.org
dul.dnsbl.sorbs.net
dul.ru
dyna.spamrats.com
dynip.rothen.com
http.dnsbl.sorbs.net
images.rbl.msrbl.net
ips.backscatterer.org
ix.dnsbl.manitu.net
korea.services.net
misc.dnsbl.sorbs.net
noptr.spamrats.com
ohps.dnsbl.net.au
omrs.dnsbl.net.au
orvedb.aupads.org
osps.dnsbl.net.au
osrs.dnsbl.net.au
owfs.dnsbl.net.au
owps.dnsbl.net.au
pbl.spamhaus.org
phishing.rbl.msrbl.net
probes.dnsbl.net.au
proxy.bl.gweep.ca
proxy.block.transip.nl
psbl.surriel.com
rdts.dnsbl.net.au
relays.bl.gweep.ca
relays.bl.kundenserver.de
relays.nether.net
residential.block.transip.nl
ricn.dnsbl.net.au
rmst.dnsbl.net.au
sbl.spamhaus.org
short.rbl.jp
smtp.dnsbl.sorbs.net
socks.dnsbl.sorbs.net
spam.abuse.ch
spam.dnsbl.sorbs.net
spam.rbl.msrbl.net
spam.spamrats.com
spamlist.or.kr
spamrbl.imp.ch
t3direct.dnsbl.net.au
tor.dnsbl.sectoor.de
torserver.tor.dnsbl.sectoor.de
ubl.lashback.com
ubl.unsubscore.com
virbl.bit.nl
virus.rbl.jp
virus.rbl.msrbl.net
web.dnsbl.sorbs.net
wormrbl.imp.ch
xbl.spamhaus.org
zen.spamhaus.org
zombie.dnsbl.sorbs.net

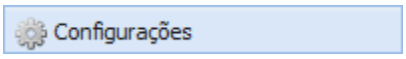
Lista de algumas URI's Opcionais

surbl.org
ubl.nszones.com

Controle de Conexão

Configurações do MTA

Use esta página para exibir, adicionar, editar ou excluir configurações do MTA.



/ Controle de Conexão / Configurações do MTA

Visão geral das Configurações do MTA

Um agente de transporte de e-mail (MTA - Mail Transfer Agent) é um aplicativo de software usado dentro de um sistema de tratamento de mensagem de internet (MHS). É responsável pela transferência e encaminhamento de uma mensagem de correio eletrônico do computador do remetente para o computador do destinatário. A plataforma básica para o MTA é um sistema de troca com a arquitetura cliente / servidor.

Essa camada caracteriza-se por ser a camada inicial, isto é a conexão efetuada a nível de SMTP, ainda sem a conexão final com o sistema de filtragem de e-mail, ou seja, antes de processar anexos, ou até mesmo a pontuação de spam.

O serviço de MTA do HSC MailInspector foi desenvolvido pensando em segurança, performance, alta disponibilidade e escalabilidade. Cada ponto de filtragem MTA tem capacidade de atender mais de 500.000* mensagens por hora (por node de cluster, ou seja, este número é por máquina individualmente implementada). Podendo ainda ser colocado em cluster demais servidores a fim aumentar a capacidade de processamento de mensagens.

O HSC MailInspector é um Gateway de e-mail que funcionando como um Proxy transparente de e-mails, que filtra as mensagens enviadas e recebidas de sua empresa contra todos os tipos de ameaças e ataques existentes, protegendo seu servidor interno de correio.

No HSC MailInspector, o MTA possui diversas funções, entre elas destacamos:

- Executar as primeiras camadas de filtragem do HSC SPAM Filter Ahead, esta camada filtra aos dados da conexão na camada inicial do diálogo SMTP, ou seja, antes de receber o conteúdo da mensagem. O MailInspector suporta os protocolos SMTP, SMTPS e SMTP/TLS;
- Bloqueio a nível de conexão de e-mails oriundos de domínios inexistentes;
- Bloqueio a nível de conexão de e-mails que não existem DNS reverso/Forwarded-Confirmed Reverse DNS (FCrDNS) configurado;
- Bloqueio de excesso de conexões idle (em espera);
- Receber e Enviar os e-mails para outros servidores, e encaminhá-los para o processamento das outras camadas de filtragem;
- Filtragem de Entrada e Saída de e-mails podendo criar regras em qualquer sentido do tráfego baseado em domínios, usuários, e-mails, IPs/Rede e grupo de usuários;
- Roteamento de mensagens de um domínio para múltiplos endereços de IP's;
- Roteamento de mensagens para o próximo servidor diferente do padrão (próximo hop/prioridade em servidores de entrega de e-mail), de acordo com a necessidade do administrador;
- Configuração de tempo limite em conexão SMTP;
- Controle de e-mails com Non-Delivery Report (NDR) ou "bounce message", permitindo limitar o número máximo de bounces por hora através dos seguintes parâmetros:
    - Número de destinatários inválidos por IP, rede ou range;

  - Domínios;
  - Reputação do remetente;
- Roteamento de mensagens de múltiplos domínios para um mesmo IP;
- Customizar o Banner de conexão SMTP conforme necessidade do administrador, podendo indicar o hostname e os códigos de resposta por endereço IP e/ou grupo de remetentes;
- Proteção contra-ataques de DOS "Negação de serviço"
  - Por Endereço de IP de Origem;
  - Domínio de origem;
  - Reputação da Origem, com uso de BigData, RBL, DUL, ETL;
  - Volume excessivo de mensagens (através da função Outbrak Filter);
  - Por número de sessões SMTP;
  - Número excessivo de sessões SMTP simultâneos;
- Proteção contra-ataques do tipo flood, rejeitando as conexões de origem desse tipo de e-mail;
- Proteção contra sistema que fazem a coleta de usuário e senha sobre o MailInspector;
- Proteção a ataques de dicionário (DHA)/backscatter, já no próprio nível de conexão. É feita a verificação da existência do usuário no domínio. Essa verificação é efetuada através de comparação do campo TO do e-mail recebido com a base importada pelos conectores criados no MailInspector. Os conectores fazem essa interface de comunicação entre MLI e os servidores de e-mail/servidores de autenticação, tais como Zimbra/LDAP/Exchange/Microsoft AD/Lotus ou outra base possível de importação e sincronização constante;
- Suporte a "Expanded 8-bit character set" e RCF 821, RFC 2821, RFC 822 e RFC 2822.
- Fila de E-mails: permite manter e-mails na fila por longos períodos em caso de problemas com o servidor do destino. O tamanho da fila pode ser configurado conforme o escalonamento do disco rígido configurado para este fim, ou seja, caso seja necessário armazenar mensagens por um longo período ou um volume grande de mensagens em caso de falha do servidor de destino basta configurar um tamanho maior de disco para esta área;
- Bloqueio de e-mail devido a má reputação de origem (spammers, phishers, etc);
- Proteção de uso do MailInspector como retransmissor de mensagens externas (Open Relay);
- Encaminhar os e-mails limpos, após o processamento, para o servidor de e-mail da empresa. Esse encaminhamento pode ser efetuado para múltiplos IP's de destino (para um mesmo domínio), dessa forma, criando sistema de Load Balance e alta disponibilidade na entrega, permitindo a entrega de e-mails para caixas postais específicos baseados nos domínios destino, conforme a configuração efetuada pelo administrador;
- Possibilidade de criar exceções de verificações na camada de conexão (MTA de entrada), dessa forma formando uma Allow List a nível de conexão, podendo ser por:
  - IP de Origem / IP de Destino;
  - Range de IP;
  - Redes (CIDR);
  - Classe de IP;
  - Domínios;
  - Nome parcial de domínio;
  - Subdomínios;
  - Nome parcial de subdomínio;
  - Hostnames;
  - E-mail de Origem;
  - Nome parcial de E-mail de Origem;
  - E-mail de Destino;
  - Nome parcial de E-mail de Destino;

- Controle de conexão para e-mails com múltiplos destinatários: Quando um e-mail com múltiplos destinatários é enviado, o sistema cria uma única um único processo de MTA, ao qual envia para todos os destinatários, dessa forma evitando conexões desnecessárias e em caso de queda, ao reestabelecer a conexão, só é enviado um único e-mail, evitando duplicidade de envio de e-mails;
- Possibilidade de criar bloqueios na camada de conexão (MTA de entrada), dessa forma formando uma Block List a nível de conexão, podendo ser por:
    - IP de Origem / IP de Destino;
    - Range de IP;
    - Redes (CIDR);
    - Classe de IP;
    - Domínios;
    - Nome parcial de domínio;
    - Subdomínios;
    - Nome parcial de subdomínio;
    - Hostnames;
    - E-mail de Origem;
    - Nome parcial de E-mail de Origem;
    - E-mail de Destino;
    - Nome parcial de E-mail de Destino;

* Pode-se ultrapassar ao número de 500.000 mensagens/hora, dependendo unicamente da configuração de número de processadores/quantidade de memória/tamanho de armazenamento disponibilizado pelo administrador da solução.

Definições de Opções - Configurações do MTA

Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição
Salvar	Quando clicado, grava as configurações realizadas.
Limpar Cache de Controle Dinâmico	Se estive com a função **Controle de Usuários Inválidos no Domínio** configurado como **Dinâmico**, é possível limpar o cache desse controle através desta opção.

Definições de Opções - Configurações Gerais

Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição
Nome do Servidor	Informe o nome F.Q.D.N. do ponto de acesso. Ex.: mx01.empresa.com.br.
Banner de Conexão	Informe a mensagem de saudação para as conexões SMTP (“greeting” SMTP). Normalmente utiliza-se o mesmo valor do campo Nome do Servidor. Ex.: mx01.empresa.com.br.
Domínio de Origem	Informe o nome do principal domínio que será atendido. Ex.: empresa.com.br.
Protocolo de Entrega	Informe qual(ais) protocolo(s) que será(ão) utilizado(s) • **IPv4/IPv6:** Indica o uso dos dois padões de protocolo TCP (IPv4 e IPv6); • **IPv4:** Indica somente o uso do protocolo TCP no formato IPv4; • **IPv6:** Indica somente o uso do protocolo TCP no formato IPv6;

Domínios Atendidos	Informe os nomes de todos os domínios que serão atendidos, dessa forma o MailInspector sabe quais domínios que deve proteger e ativar a proteção anti-spoofing sobre estes domínios. O HSC MailInspector pode gerenciar mais de 10000 domínios simultâneos Ex.: outraempresa.com.br.
Liberar Relay	Informe os endereços IP e/ou endereços de rede que podem enviar mensagens através do HSC MailInspector. Por padrão o MailInspector nega que qualquer servidor utilize o MailInspector como Relay Server evitando assim que qualquer emissor externo possa usar o sistema para envio de mensagens sem autorização. O MailInspector não possui limite de número de cadastros para liberação de relay. O campo Liberar Relay, podem ser utilizados no seguinte formato: • Redes (ex: 192.168.0.0/24); • IP's (ex: 192.168.1.1); • Hostnames (ex: correio.teste.com.br – desde que os mesmos sejam alcançáveis pelo DNS configurado na solução); ⚠ É obrigatório a inserção do endereço 127.0.0.1 nesta configuração. Esta configuração permite que mensagens armazenadas na quarentena, sejam encaminhadas ou liberadas através do próprio HSC MailInspector.
Forçar que os servidores autorizados a fazer Relay usem um usuário cadastrado	• **Sim:** Forçam os e-mails de saída a usarem um dos e-mails cadastrados em Domínios Atendidos. Caso algum e-mail de saída não esteja configurado com um dos domínios cadastrados (Domínios Atendidos), eles serão negados. • **Não:** Permite que sejam enviados e-mails de outros domínios, além dos cadastrados em Domínios Atendidos.
Permitir que os servidores autorizados a fazer Relay usem Mail From vazio?	• **Sim:** Permite envio de e-mails sem o preenchimento do campo From. • **Não:** Não permite o envio de e-mails sem o preenchimento do campo From.
Ativar Relay Automático para Office 365	• **Sim:** Permite que os servidores do Microsoft Office 365 mandem e-mails para o MailInspector (filtragem de saída). • **Não:** Não permite que os servidores do Microsoft Office 365 envie e-mails de saída para o MailInspector.
Ativar Relay Automático para G-Suite	• **Sim:** Permite que os servidores do G-Suite (Google) mandem e-mails para o MailInspector (filtragem de saída). • **Não:** Não permite que os servidores do G-Suite (Google) envie e-mails de saída para o MailInspector.

Nome do Servidor: antispam.fundacaobutantan.org.br

Banner de Conexão: Fundacao Butantan

Domínio de Origem: fundacaobutantan.org.br

Protocolo de Entrega: IPV4

Domínios Atendidos

Pesquise na lista — 1 / 1 registros

fundacaobutanta.org.br

Liberar Relay

Pesquise na lista — 1 / 1 registros

127.0.0.1

Forçar que os servidores Autorizados a fazer Relay usem um usuário cadastrado:	○ Sim	● Não
Permitir que os servidores Autorizados a fazer Relay usem Mail From vazio?:	○ Sim	○ Não
Ativar Relay Automático para Office 365:	○ Sim	● Não
Ativar Relay Automático para G-Suite:	● Sim	○ Não

Exemplo de tela de configuração de MTA

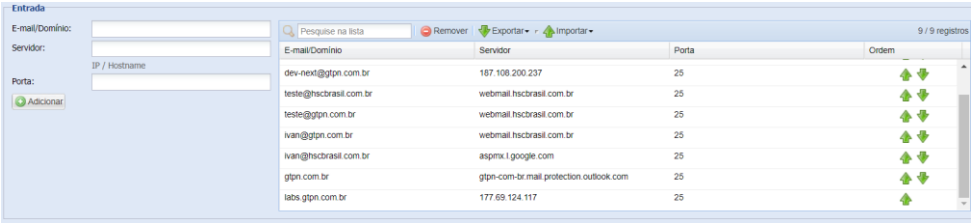
Definições de Opções - Rotas

Configuração de roteamento de mensagens para múltiplos domínios de destino e IP's de entrega.

Opções	Definição

Entrada	As Rotas de Entrada são em Mapas de Transporte é responsável por indicar para qual servidor as mensagens de determinado endereço ou domínio devem ser entregues após serem processadas pelo HSC MailInspector. Ele faz o roteamento final de um Domínio até o servidor Final de MailBox.
	
	É possível efetuar múltiplas ações sobre os registros cadastrados. Entre eles:
	• **Busca/Pesquisa:** Pesquisa de e-mail/domínio, para isso, basta preencher o campo de pesquisa e dar enter.
	• **Remover:** Remove um registro previamente selecionado.
	• **Exportar:** Exporta toda a tabela configurada para a Entrada em formato XML.
	• **Importar:** Importa de um arquivo CSV ou XML a tebela de entrada dos e-mails.
	
	O formato do arquivo (quando em XML) deve ser com a seguinte estrutura:
	<?xml version="1.0" encoding="UTF-8"?><rows><row><domain>dominio01.com.br</domain><host>192.168.250.250</host><port>25</port></row><row><domain>exemplo.com.br</domain><host>servidorde-mail.com.br</host><port>25</port></row><row><domain>hscbrasil.com.br</domain><host>192.168.250.60r</host><port>25</port></row></rows>
	
	DICA: Você pode abrir este arquivo padrão XML no Microsoft Edge, que ele irá indicar qualquer erro de estrutura de XML (não indica erro de digitação em domínio, host ou porta, mas apresentará erro de estrutura no XML).
	
	Na Entrada, para dar entrada de novos registros, são requiridos alguns campos:
	• **E-mail/Domínio** - Informe o endereço de e-mail ou nome do domínio que será entregue no endereço IP do servidor informado. Ex.: empresa.com.br.
	• **Servidor** - Informe o endereço IP ou hostname (baseado na consulta DNS) do servidor para a entrega das mensagens do e-mail/domínio informado. (ex: 192.168.0.10 ou mail.hscbrasil.com.br)
	O campo Entrada, podem ser utilizados no seguinte formato:
	  ○ IP's (ex: 192.168.1.1);
	  ○ Hostnames (ex: correio.teste.com.br – desde que os mesmos sejam alcançáveis pelo DNS configurado na solução);
	• **Porta** - Informe o número da porta TCP para conexão com o servidor informado. Ex.: 25.
	• **Ordem** – Seleção de preferência de entrega de e-mails para um determinado servidor, quando for para o mesmo domínio.
	
	Caso tenha sido informado mais de um Servidor/IP de entrega de e-mail para o mesmo domínio, o sistema dará preferência a entrega para o primeiro da lista, sendo entregue para o segundo, caso ocorra falha de entrega para o primeiro da lista e assim segue subsequentemente.

Todos os domínios informados como Domínios Atendidos devem estar configurados no Mapa de Transporte.



Exemplo de Tela da Tabela de Roteamento dos E-mails de Entrada.

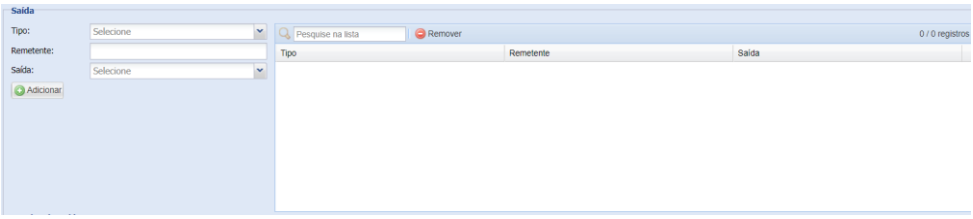
Saída

As Rotas de Saída servem para definir por qual endereço IP será entregue uma mensagem. Desta forma podemos especificar um domínio ou endereço de um determinado remetente e definir regras de saída definindo por qual Endereço IP o mesmo será entregue.

- **Tipo E-mail/Domínio** - Informe se será um Endereço de e-mail ou domínio que será usado na regra.
- **Remetente** - Informe o valor da regra conforme o tipo selecionado.
- **Saída** - Selecione a interface de Saída, selecionando uma interface do Ponto de Acesso.

Para habilitar a saída de e-mail por um IP específico, é obrigatória a configuração de ALIAS de placa de rede em Administração > Configurações de Rede

Por padrão não há necessidade de configuração de uma regra de saída. Quando não for criado nenhuma regra o sistema utilizará a interface e o IP de saída padrão configurado para entregar todas as mensagens (gateway).

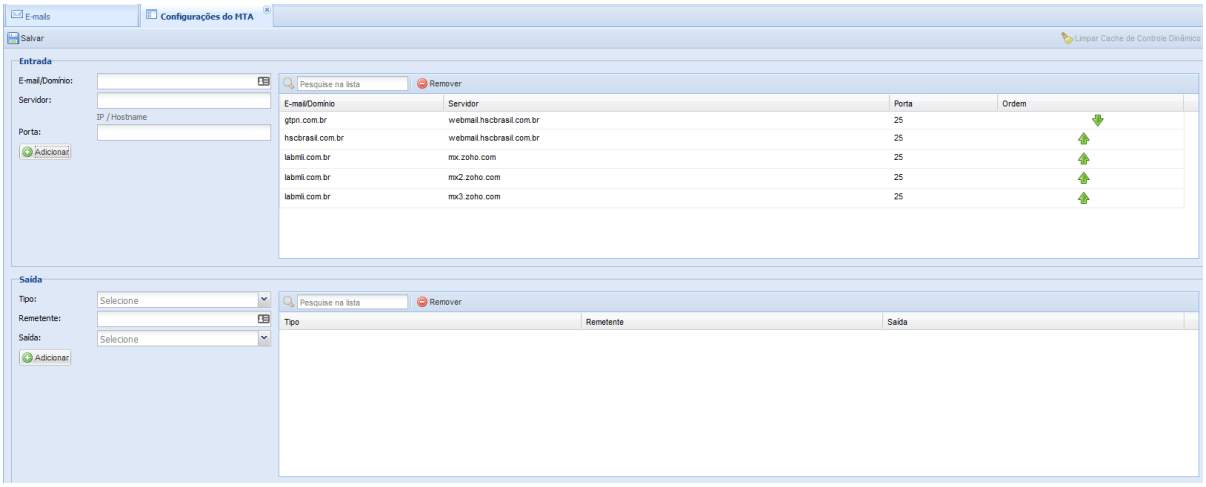


Exemplo de Tela da Tabela de Roteamento dos E-mails de Saída.

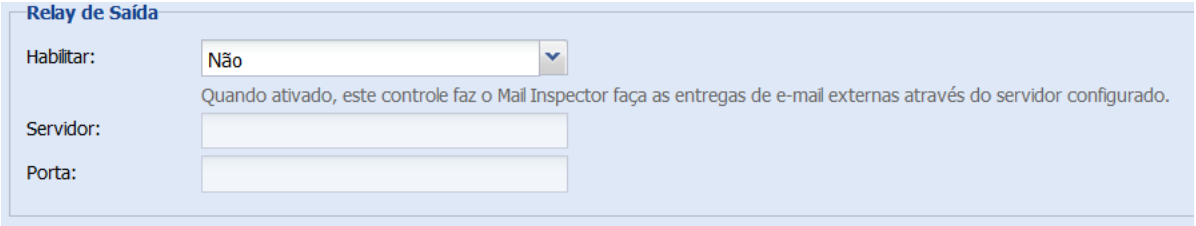
Relay de Saída

Esta função é para fazer a saída de e-mails através de outro servidor, ou seja, em vez de mandar diretamente pelo MailInspector, os e-mails serão “encaminhados” ao SmartHost.

- **Habilitar:**
  - **Sim:** Habilita a funcionalidade. Por padrão esta funcionalidade vem desabilitado.
  - **Não:** Desabilita esta funcionalidade.
- **Servidor:** Indique o IP do servidor destino dos e-mails.
- **Porta:** Informe a porta de comunicação TCP para o protocolo SMTP.



Exemplo de Configuração de entrega de e-mails filtrados.



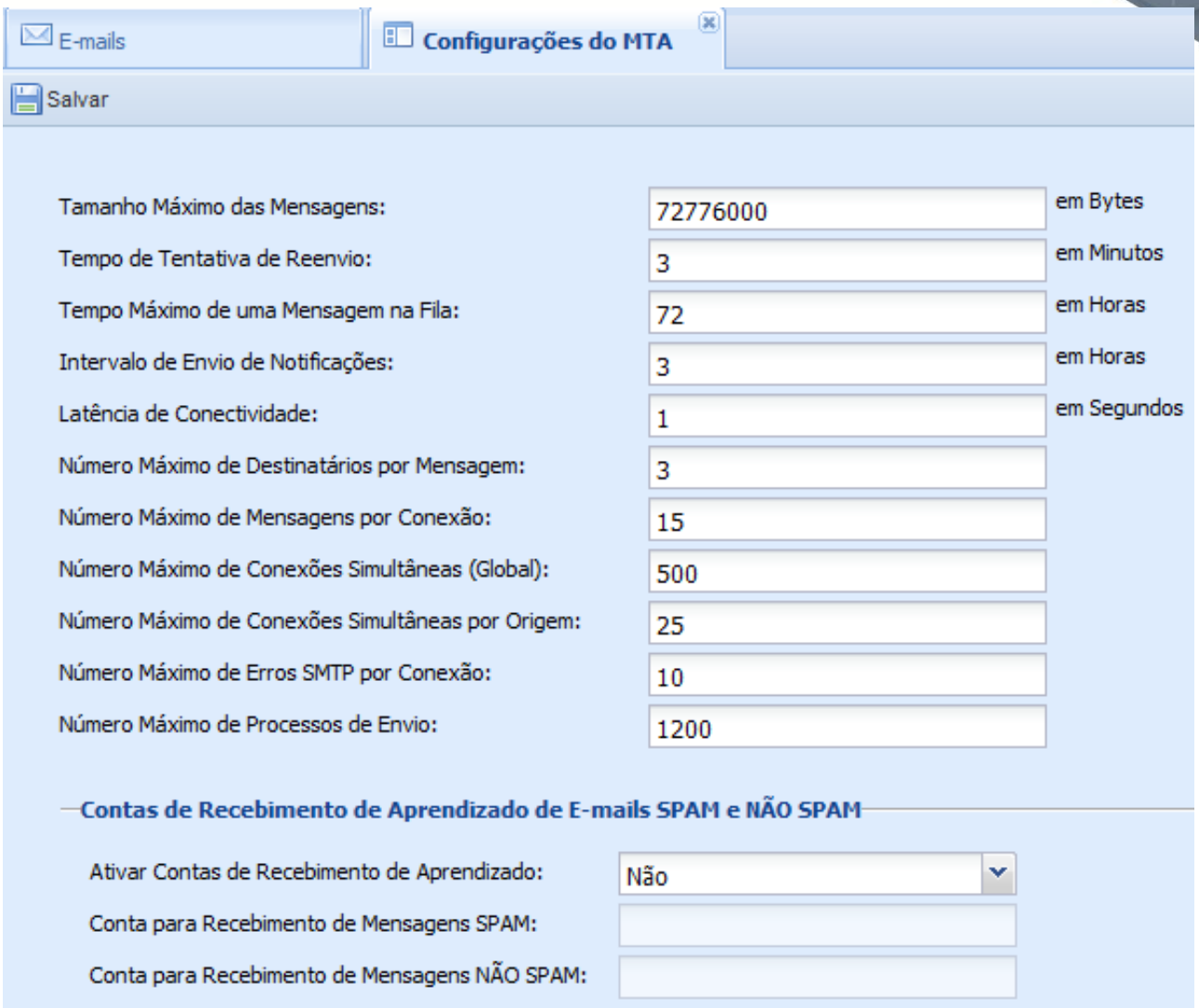
Exemplo de Configuração de Relay de Saída.

Definições de Opções - Mensagens

Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição
Tamanho Máximo das Mensagens	Informe o tamanho máximo, em bytes, que uma mensagem pode ter para ser recebida e processada pelo HSC MailInspector. Neste campo, indica o tamanho máximo da mensagem aceita a nível de conexão (MTA). Se o mesmo for rejeitado, o e-mail não será registrado no MailInspector, ficando somente a indicação do log do evento. Mensagens com o tamanho maior ao definido nesta opção são rejeitadas pelo MTA, isto é, não são exibidas no RealTime.
Tempo de Tentativa de Reenvio	Informe o tempo, em minutos, para que seja realizada uma nova tentativa de reenvio de mensagens que não puderam ser entregues por algum tipo de erro.
Tempo Máximo de uma Mensagem na Fila	Informe o tempo máximo, em horas, para que uma mensagem (Incluindo Bounce), permaneça na fila para tentativa de reenvio. Após o tempo determinado, a mensagem é devolvida para o remetente com informações sobre o erro de entrega.
Tempo de Tentativa de Reenvio de Bounces	Informe o tempo em minutos para a tentativa de reenvio de Bounces de e-mails.
Intervalo de Envio de Notificações	Informe o tempo, em horas, para o envio de notificações caso ocorra algum problema na entrega da mensagem.

Latência de Conectividade	Informe o tempo, em segundos, de intervalo para pedidos de conexão de uma mesma origem.
Timeout SMTP	Informe o timeout da conexão SMTP. Por padrão o timeout de conexão SMTP é de 20s.
Número Máximo de Destinatários por Mensagem	Informe a quantidade máxima de destinatários permitido por mensagem.
Número Máximo de Mensagens por Conexão	Informe a quantidade máxima de mensagens que podem ser enviadas durante uma mesma conexão.
Número Máximo de Conexões Simultâneas (Global)	Informe o número máximo de conexões TCP simultâneas permitidas para o HSC MailInspector. O sistema pode operar com mais de 30.000 (trinta mil) conexões simultâneas por ponto de acesso.
Número Máximo de Conexões Simultâneas por Origem	Informe o número máximo de conexões SMTP simultâneas que serão aceitas de um mesmo servidor de origem.
Número Máximo de Erros SMTP por Conexão	Informe o número máximo de erros SMTP por conexões simultâneas que serão aceitas de um mesmo servidor.
Número Máximo de Processos de Envio	Indica o número máximo de processos de envio de e-mail simultâneos. Cada lote terá no máximo a quantidade de e-mails estipulado para o envio por vez.
Contas de Recebimento de Aprendizado de E-mails SPAM e NÃO-SPAM	As Contas de Recebimento de Aprendizado de E-mails permitem que o usuário ensine ao Machine Learning e ao filtro bayesiano com mensagens que devem ser consideradas SPAM ou com mensagens que não devem ser consideradas SPAM. • **Ativar Contas de Recebimento de Aprendizado** - Ativa as contas de aprendizado. • **Conta para Recebimento de Mensagens SPAM** - Informe o endereço de e-mail da conta de aprendizado para mensagens consideradas SPAM. Ex.: spam@empresa.com.br. • **Conta para Recebimento de Mensagens NÃO SPAM** - Informe o endereço de e-mail da conta de aprendizado para mensagens consideradas SPAM. Ex.: nospam@empresa.com.br. Para o correto funcionamento desta funcionalidade, é necessário que no servidor de e-mail da empresa (Exchange, Zimbra, Lotus, etc.), sejam criados redirecionamento dessas contas para o HSC MailInspector.
Códigos Erro MTA	Permite ao administrador modificar os códigos de erro reportado pela solução. Os códigos de erro seguem as principais normativas e RFC's, só altere algum código em caso de extrema necessidade.



Tela de Configurações de Mensagens no MTA.

Definições de Opções - Filtragem

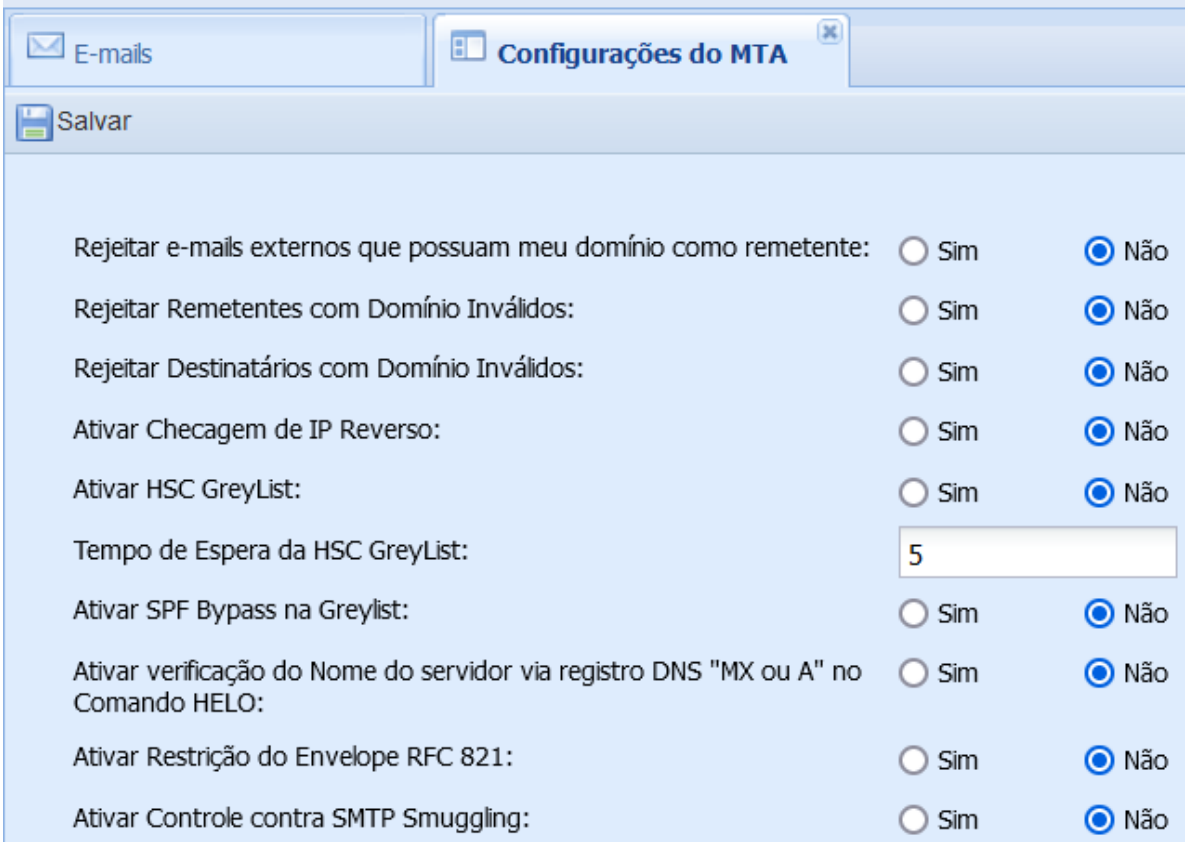
Esta etapa destina-se a filtros de MTA operados no MailInspector. Com essas opções, é possível efetuar liberação/bloqueio de e-mails na camada de conexão.

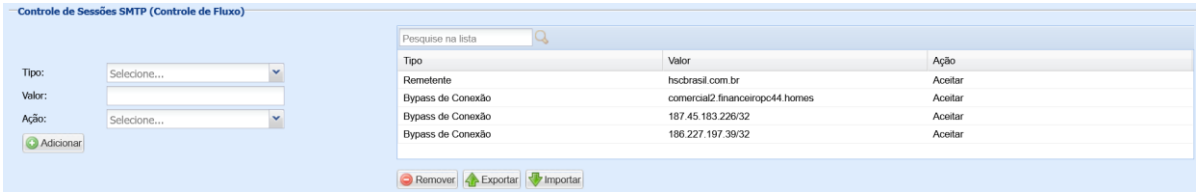
Opções	Definição
Rejeitar E-mails Externos que Possuam meu Domínio como Remetente	Escolha entre: • **Sim** - Indica que a filtragem está ativa. Este recurso impede o recebimento de mensagens externas que estejam mascaradas com os domínios cadastrados da empresa. • **Não** - Indica que a filtragem está desativada.
Rejeitar Remetentes com Domínio Inválidos	Escolha entre: • **Sim** - Indica que a filtragem está ativa. Este recurso impede o recebimento de mensagens externas que não possuem um domínio válido no remetente. Ex.: usuario@dominioinventado.com.br

	Quando ativada essa opção, o bloqueio é feito direto no MTA, sem tentativa de entrega do e-mail, nem processamento (caso o domínio do remetente seja inválido). Não haverá registro do e-mail em RealTime > E-mails (pois foi bloqueado no MTA do MLI, que é ANTES do processamento do e-mail), também **NÃO será gerado o bounce-mail ao usuário.** • **Não** - Indica que a filtragem está desativada.
Rejeitar Destinatários com Domínio Inválidos	Escolha entre: • **Sim** - Indica que a filtragem está ativa. Este recurso impede o recebimento de mensagens externas que não tenham um domínio cadastrado da empresa como destinatário. Quando ativada essa opção, o bloqueio é feito direto no MTA, sem tentativa de entrega do e-mail, nem processamento (caso o domínio do destinatário seja inválido). Não haverá registro do e-mail em RealTime > E-mails (pois foi bloqueado no MTA do MLI, que é ANTES do processamento do e-mail), também **NÃO será gerado o bounce-mail ao usuário.** • **Não** - Indica que a filtragem está desativada.
Ativar Checagem de IP Reverso	Escolha entre: • **Sim** - Indica que a filtragem está ativa. Este recurso impede o recebimento de mensagens externas de servidores que não tenham um registro DNS PTR (reverso) cadastrado corretamente. • **Não** - Indica que a filtragem está desativada.
Ativar HSC GreyList	Escolha entre: • **Sim** - Indica que a filtragem está ativa. Este recurso recusa temporariamente uma mensagem e aguarda por sua retransmissão para o permitir o recebimento da mensagem. • **Não** - Indica que a filtragem está desativada.
Tempo de Espera da HSC GreyList	Informe o tempo de espera, em minutos, que o sistema da GreyList deve aguardar antes de aceitar a próxima tentativa de entrega de uma mensagem.
Ativar SPF Bypass na Greylist	• **Sim** – Verifica SPF nos e-mails em GreyList. • **Não** – Não verifica SPF nos e-mails em Greylist.
Ativar verificação do Nome do servidor via registro DNS "MX ou A" no Comando HELO	Escolha entre: • **Sim** - Indica que a filtragem está ativa. Este recurso valida se na transação do protocolo SMTP na camada de MTA o comando HELO foi passado contendo o nome FQDN válido "Registro MX e A" do servidor que originou a conexão, ou seja, a de rejeitar conexões que tentarem ser abertas pelos comandos “HELO” e “EHLO”, mas sem que existam gravados seus endereços de “MX” e “A” nos servidores de DNS; • **Não** - Indica que a filtragem está desativada.
Ativar restrição do Envelope RFC 821	Escolha entre: • **Sim** - Indica que a filtragem está ativa. Este recurso valida se o e-mail respeita o padrão RFC 821 na parte do Envelope do E-mail. Caso esteja ativada e e o e-mail vier de forma incorreta quanto ao RFC 821, o e-mail é automaticamente descartado;

	• **Não** - Indica que a filtragem está desativada.
Ativar Controle contra SMTP Smuggling	Escolha entre: • **Sim** - Indica que a filtragem está ativa. Este recurso previne ataques que operam sobre a vulnerabilidade do protocolo SMTP. Essa vulnerabilidade permite a injeção de comandos SMTP em mensagens de e-mail de uma forma que faz com que os servidores de recebimento as tratem como duas mensagens separadas sendo que uma delas tem seu cabeçalho "De" falsificado. • **Não** - Indica que a filtragem está desativada.
Controle de Sessões SMTP (Controle de Fluxo)	O Controle de Fluxo permite criar regras personalizadas nas camadas de filtragem do MTA (camada de conexão), permitindo ou negando a entrega de mensagens de um determinado domínio, endereço de e-mail ou endereço IP de servidor. • **Tipo** - Selecione o tipo de regra que será criada: ○ **Remetente:** Permitir ou rejeitar mensagens de um remetente especificando um e-mail, nome parcial do e-mail, domínio ou nome parcial do domínio. ○ **Destinatário:** Permitir ou rejeitar mensagens para um destinatário especificando um e-mail, nome parcial do e-mail, domínio ou nome parcial do domínio. ○ **ByPass de Conexão:** Quando criado uma marcação por Domínio, nome parcial do domínio, Subdomínio, nome parcial de subdomínio,IP, Rede, Subrede de IP, Faixa de IP ou Hostname (Completo ou Parcial), todos os filtros da camada Controle de Conexão serão desativados para estas origens, sendo assim os filtros: ▪ MTA check (Controle de cabeçalho, DNS reverso, tamanho máximo de e-mail a nível de conexão, verificação de ataque de dicionário, etc); ▪ GreyList; ▪ Spam Throttling; ▪ Blacklist/Block List externas; ▪ Quota/Controle de Fluxo; Serão ignorados, sendo sobreposta pela ação marcada (Aceitar ou Ignorar). Para todos os demais filtros de mensagens: ▪ Anti-vírus; ▪ Anti-phishing; ▪ Filtros Heurísticos de SPAM; Serão normalmente processados. Este Bypass garante que a mensagem seja recebida e processada. • **Valor** - Informe um valor conforme o tipo selecionado. ○ **Remetente:** Informe um nome de domínio, nome parcial do domínio ou endereço de e-mail; ○ **Destinatário:** informe um nome de domínio, nome parcial do domínio ou endereço de e-mail; ○ **ByPass de Conexão:** Informe um endereço IP, range ou subnet. • **Ação** - Informe a ação desejada para a regra. ○ **Aceitar:** Aceita a conexão indicada;

	○ **Rejeitar:** Nega a conexão indicada, descartando a mensagem de forma silenciosa; Através do Controle de Fluxo é possível permitir a entrega de mensagens de servidores que não possuem o DNS reverso corretamente cadastrado.
Remover	Excluir o registro selecionado da tabela de Controle de Sessões SMTP
Exportar	Exporta toda a tabela de Controle de Sessões SMTP no formato CSV
Importar	Importa a tabela de Controle de Sessões SMTP. É necessário seguir o formato do CSV. Segue o formato - **Tipo, Valor, Ação** Segue exemplo: 0,"hscbrasil.com.br","A" 2,"comercial2.financeiropc44.homes","A" 2,"187.45.183.226/32","A" 2,"186.227.197.39/32","A" Onde: Tipo é: 0 = Remetente 1 = Destinatário 2 = Bypass de Conexão Valor: Hostname, e-mail, domínio, IP, rede, etc Ação: A = Aceitar R = Rejeitar



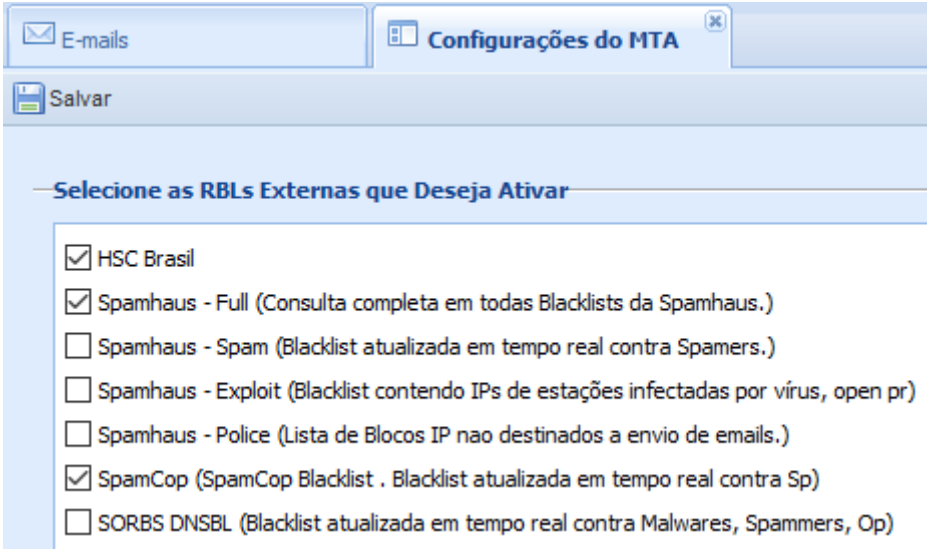


Definições de Opções - RBLs Externas

Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição
Selecione as RBLs Externas que Deseja Ativar	Permite ativar o recurso de filtragem através de listas RBL na camada do MTA. RealTime Blacklist, são listas negras de endereços IP geradas por órgãos internacionais, sua consulta é feita através de protocolo DNS. Cada órgão tem seu critério, forma de inserção e remoção dos endereços, mas sempre obedecendo a ideia de ser um endereço suspeito ou de possível fonte de SPAM. As listas RBL pré cadastradas para utilização nos HSC MailInspector são: • **HSC Brasil** - Lista de endereços IP identificados como fontes de mensagens não solicitadas mantida e fornecida pela HSC Brasil. • **Spamhaus Full** - É a combinação de todos as DNSBLs baseadas em endereços IP da Spamhaus em uma única, poderosa e abrangente lista de bloqueio. Isto permite que as consultas realizadas sejam mais rápidas e mais simples. Ela contém as listas de bloqueio: SBL, SBLCSS, XBL e PBL.

	• **Spamhaus Spam** - Spamhaus Block List ("SBL") Advisory é um banco de dados de endereços IP a partir do qual a Spamhaus não recomenda a aceitação de mensagens de correio eletrônico. A SBL é consultada em tempo real por sistemas de correio eletrônico da toda a Internet, permitindo que os administradores de servidores de correio eletrônico identifiquem, marquem ou bloqueiem conexões de entrada de endereços IP que a Spamhaus considere estar envolvido no envio, hospedagem ou origem de e-mail não solicitado (SPAM). • **Spamhaus Exploit** - Spamhaus Exploits Block List (XBL) é um banco de dados, em tempo real, de endereços IP de PCs sequestrados infectados por exploits, incluindo proxies abertos (HTTP, socks, AnalogX, wingate, etc), worms ou vírus que enviam SPAM, e outros tipos de exploits, como cavalo de tróia (trojan horse). • **Spamhaus Police** - Spamhaus PBL é um banco de dados DNSBL de usuários finais e intervalos de endereços IP, que não devem realizar a entrega ou envio de e-mails através do protocolo SMTP a qualquer servidor de correio eletrônico da Internet, exceto os previstos especificamente pelos próprios provedores de Internet. • **SpamCop** - SpamCop Blocking List (SCBL) lista endereços IP que transmitiram SPAM e foram reportados por usuários da SpamCop como mensagens não solicitadas. A SCBL é uma lista rápida e automática de sites que foram reportados como fonte de SPAM, alimentada por uma série de fontes, incluindo relatórios automatizados e submissões dos usuários da lista SpamCop. • **Outras Listas** – Também é possível cadastrar outras listas de RBL's, de acordo com a preferência e/ou necessidade do administrador do sistema. Exemplo de lsita de RBL disponível você pode encontar em *Lista de algumas RBL's* Opcionais



Definições de Opções - Catálogo de Endereços

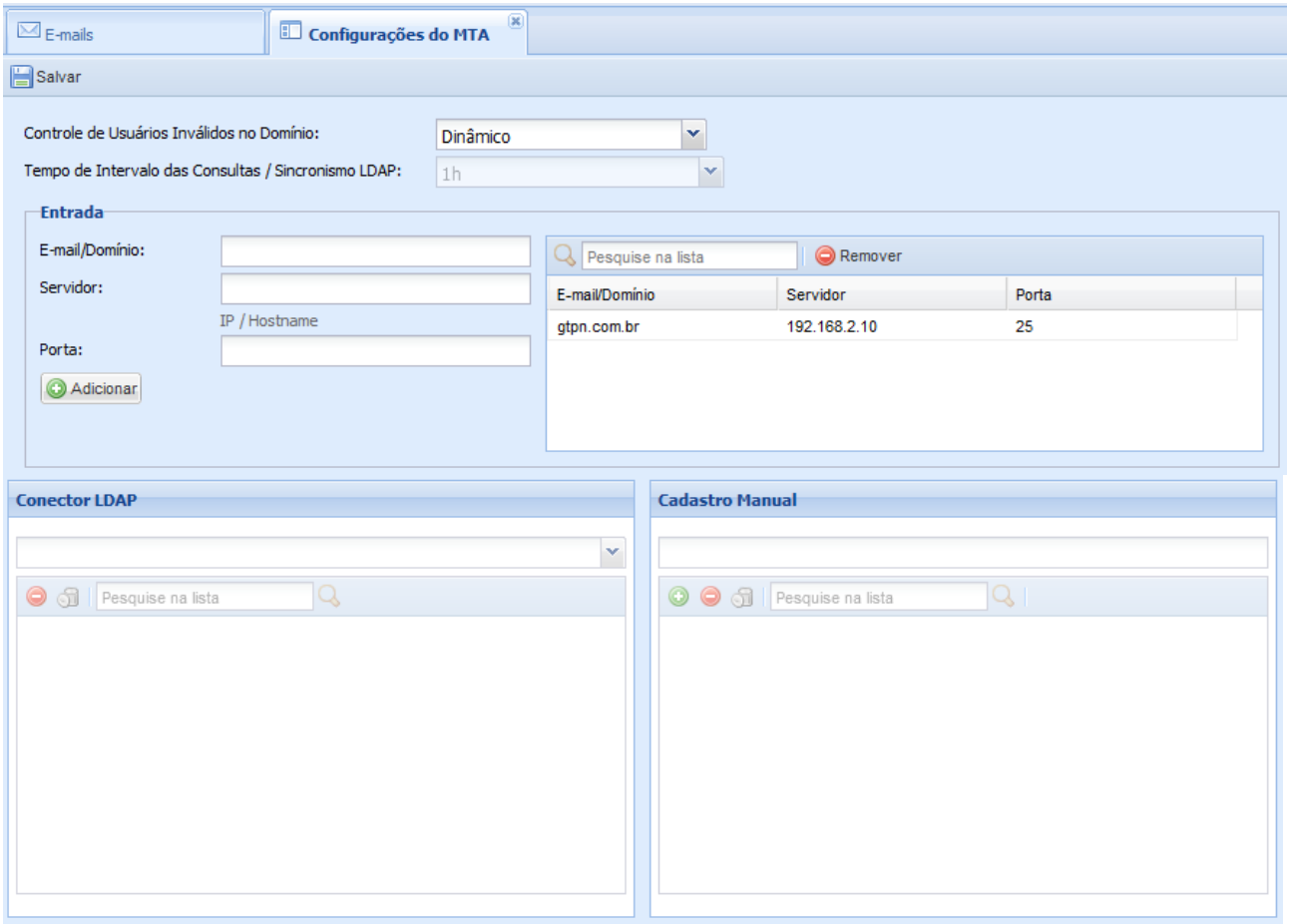
Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição

Controle de Usuários Inválidos no Domínio	Harvest Attack é uma técnica utilizada por spammers, na tentativa de encontrar endereços de e-mail válidos / existentes em um domínio usando força bruta. O ataque é geralmente realizado por meio de um ataque de dicionário padrão, onde os endereços de e-mail válidos são validados através de tentativas de envio, usando diferentes permutações de nomes de usuários comuns. O bloqueio dos usuários inválidos ocorre durante o diálogo SMTP. • **Desabilitar** - Desabilita o controle de usuários, todas as mensagens serão recebidas e processadas, mesmo que os usuários não existam. • **Dinâmico** - Habilita a consulta dinâmica de usuários. É necessário indicar qual o servidor que faz a verificação da existência de usuários (na maioria das vezes é o próprio servidor de e-mail). Com a opção de inserir o servidor MTA, é possível configurar a verificação de existência dos e-mails em um servidor e a entrega dos e-mails filtrados em outro. A opção dinâmica, extingue-se a necessidade de uso de conector externo (LDAP/AD). É importante que servidores de mensagens eletrônicas como Microsoft Exchange, Zimbra e outros, estejam corretamente configurados para responderem com o código de erro de usuário desconhecido/e-mail inexistente (550 5.1.1 User Unknown' Error / Error 550 5.1.1 Recipient address rejected). • **Estático/LDAP** - Habilita a consulta estática de usuários diretamente no banco de dados estático gerado a partir das consultas realizadas nos conectores LDAP configurados. O banco de dados é estático para a consulta, mas é atualizado dinamicamente pelo HSC MailInspector sem a necessidade de intervenção dos usuários ou administradores. Ao selecionar o controle Estático/LDAP, é necessário habilitar a função de *Sincronismo de Usuários*.
Tempo de Intervalo das Consultas / Sincronismo LDAP	É possível indicar de quanto em quanto tempo serão efetuadas as sincronizações dos Conectores Externos em relação a base de usuários da empresa (Microsoft AD/Open LDAP/Zimbra/Plesk/Lotus Notes/Lotus Domino/Entre Outros). A periodicidade pode ser: • 1 hora; • 6 horas; • 12 horas; • 24 horas;
E-mail/Domínio	**Entrada:** Indicação de qual servidor a ser utilizado para verificação de existência da conta de e-mail/usuário. • **E-mail/Domínio** - Informe o endereço de e-mail ou nome do domínio que será entregue no endereço IP do servidor informado. Ex.: empresa.com.br.

	• **Servidor** - Informe o endereço IP do servidor a ser utilizado para a verificação da existência do usuário/e-mail do e-mail/domínio informado. (ex: 192.168.0.10)
	O campo Entrada, podem ser utilizados no seguinte formato:
	  ○ IP's (ex: 192.168.1.1);
	  ○ Hostnames (ex: correio.teste.com.br – desde que os mesmos sejam alcançáveis pelo DNS configurado na solução);
	• **Porta** - Informe o número da porta TCP para conexão com o servidor informado. Ex.: 25.

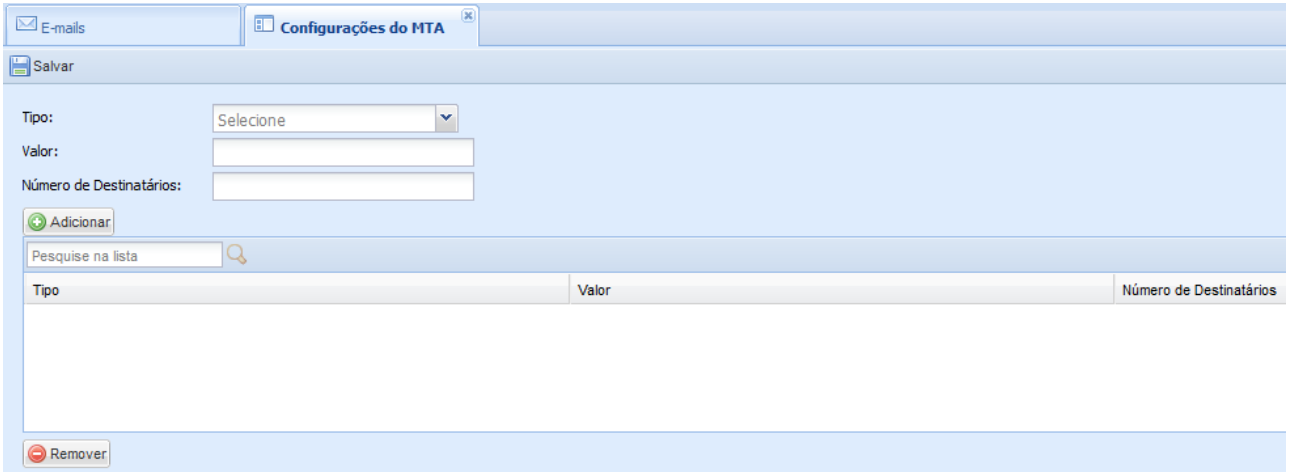
Conector LDAP	Selecione os servidores LDAP que serão utilizados para pesquisa de usuários válidos no controle de Harvest Attack (ataque de dicionário). Esta função somente é habilitada quando o Controle de Usuários Inválidos no Domínio for configurado como Estático/LDAP.
Cadastro Manual	Informe os nomes dos usuários ou dos domínios que são atendidos. Esta função somente é habilitada quando o Controle de Usuários Inválidos no Domínio for configurado como Estático/LDAP. Ex.: nome@empresa.com.br



Definições de Opções - Controle de Destinatários

Opções	Definição

Tipo	Permite controlar o número máximo de destinatários por regras de: • Pais de origem; • Remetente; • Hostname e reverso; • Domínio; • Endereço IP do Emissor; • Saudação SMTP "Helo"
Valor	Informe o Valor da regra conforme o Tipo selecionado
Número de Destinatários:	Número máximo de destinatários;



Definições de Opções – Erros SMTP

Permite a visualização e edição dos códigos de erros SMTP e de mensagens de bounce error, bem como criação de perfis diferentes para gerenciamento de BounceMail (retorno SMTP), podendo ser por:

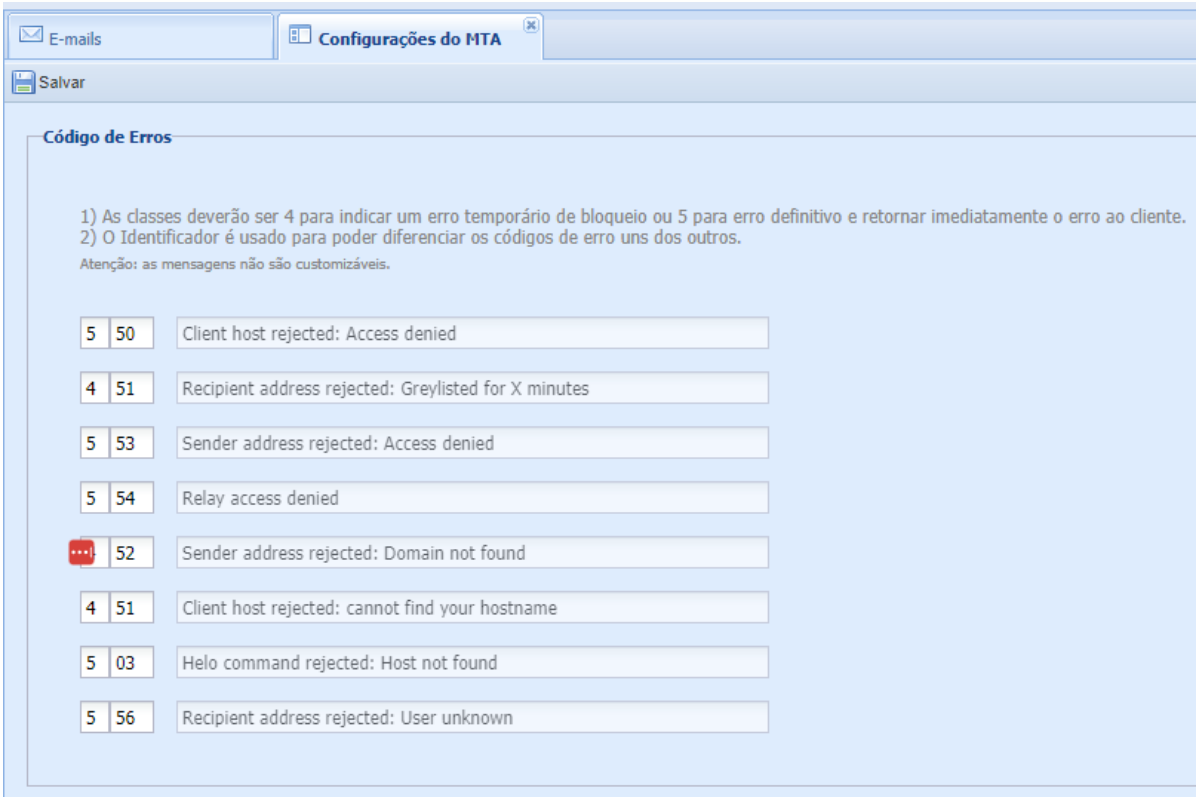
- Domínio Destino;
- IP de Destino;

Também permite criação de limitadores de quantidade de BounceMail enviado, dessa forma impedindo ataques indiretos de BounceMail que força o MTA a propagar ataques a terceiros através de BounceMail, limitando o uso de banda e controlando BounceMail enviado a mensagens com menor importância. Para esse tipo de controle conta-se com:

- Controle de frequência de BounceMail enviado a determinado destino;
- Período máximo de retenção de envio de BounceMail;

Opções	Definição
Classe de retorno	Indica a classe do erro, podendo ser temporário ou permanente. As classes deverão ser 4 para indicar um erro temporário de bloqueio ou 5 para erro definitivo e retornar imediatamente o erro ao cliente.
Identificador	O Identificador é usado para poder diferenciar os códigos de erro uns dos outros.

Obs: Não é possível editar a mensagem, mas é possível atrelar o código a outra mensagem.


E-mails
Configurações do MTA
Salvar
Código de Erros
1) As classes deverão ser 4 para indicar um erro temporário de bloqueio ou 5 para erro definitivo e retornar imediatamente o erro ao cliente.
2) O Identificador é usado para poder diferenciar os códigos de erro uns dos outros.
Atenção: as mensagens não são customizáveis.
5 50 Client host rejected: Access denied
4 51 Recipient address rejected: Greylisted for X minutes
5 53 Sender address rejected: Access denied
5 54 Relay access denied
52 Sender address rejected: Domain not found
4 51 Client host rejected: cannot find your hostname
5 03 Helo command rejected: Host not found
5 56 Recipient address rejected: User unknown

POP3/IMAP Protection

O HSC MailInspector permite escanear e-mails de servidores POP3 e IMAP externos.

Configurações / **Controle de Conexão / POP3/IMAP Protection**

Visão geral do POP3 / IMAP Protection

O HSC MailInspector permite configurar contas de servidores POP3/IMAP externo e baixar elas para que sejam filtradas contra Vírus, SPAMs e demais ameaças.

Definições de Opções - Configurações Globais

Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição
Ativar Proteção	Definir se a proteção POP3/IMAP estará ativada
TimeOut	Define o Timeout de conexão com servidor remoto

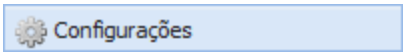
Definições de Opções - Adicionar/Editar/Remover

Aqui é possível adicionar as contas que serão feitos os controles de POP3 e IMAP

Opções	Definição
Salvar	Quando clicado, grava as configurações realizadas.
Cancelar	Quando clicado, cancela a ação.
Protocolo	Selecione o protocolo de comunicação POP3 ou IMAP
Servidor	Informe o Nome ou IP do servidor POP3 / IMAP
Porta	Defina a porta utilizada para conexão com o servidor Por padrão o POP3 é 110 e IMAP 143
Ativar SSL	Ativar Criptografia SSL
Intervalo	Intervalo de checagem automática no servidor. O parâmetro é em segundos.
Usuário	Informe o usuário de login da conta do servidor remoto.
Senha	Informe a senha de login da conta do servidor remoto.
Conta Local	Informe qual será a conta local que receberá os e-mails. Aqui será feito a Reescrita da conta de destino após a filtragem.

Mail Split

O recurso **Mail Split** permite que o MailInspector realize o **processamento individualizado de uma mesma mensagem para cada destinatário**. Quando habilitado, o sistema cria uma cópia lógica da mensagem para cada destinatário identificado.
Por exemplo, caso um e-mail seja enviado para **5 (cinco) destinatários**, o Mail Split realizará a separação da mensagem em **5 cópias para fins de análise**, permitindo que cada cópia seja processada individualmente de acordo com as políticas, regras e critérios de segurança aplicáveis a cada usuário.
Essa funcionalidade é especialmente relevante em ambientes nos quais diferentes destinatários podem estar sujeitos a **políticas de segurança, listas de permissão/bloqueio ou critérios de classificação distintos**.
Quando o **Mail Split não está habilitado**, a mensagem é processada considerando o primeiro destinatário e o resultado da análise é aplicado aos demais destinatários da mesma mensagem. Dessa forma, se a mensagem for classificada como **SPAM** para o primeiro destinatário, a mesma classificação será aplicada aos demais destinatários.
Com o Mail Split habilitado, portanto, o MailInspector proporciona **maior granularidade no tratamento das mensagens**, permitindo que uma mesma mensagem seja analisada e tratada de forma independente para cada destinatário, conforme as políticas de segurança individuais.



/ **Controle de Conexão / Mail Split**

Visão geral do Mail Split

O HSC MailInspector permite dividir as mensagens destinadas a mais de um destinatário através de regras por e-mail, usuário, domínio, subdomínio ou grupo LDAP.

Quando a mensagem é dividia todas as regras possíveis de configurações da ferramenta são tratadas de forma individual, garantindo uma maior granularidade nas configurações.

Definições de Opções - Mail Split

Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição
Salvar	Quando clicado, grava as configurações realizadas.
Habilitar	Escolha entre: • **Sim** - Indica que o sistema de Mail Split será ativado • **Não** - Indica que o sistema de Mail Split será desativado
Grupos Atendidos	Selecione um "Grupo de Usuários" que deverão sofrer Split. Estes grupos podem ser cadastrados em "Configurações > Cadastros > Grupos de Usuários" e podem conter: E-mail, domínio, subdomínio, usuários, aliases, ou Grupo LDAP

Por padrão o Mail Split vem desabilitado.

TLS/SSL

SSL ou TLS são protocolos de criptografia que proporcionam segurança na troca de dados entre aplicativos e servidores, chamados respectivamente de Secure Socket Layer e Transport Layer Security.

Muitas vezes os dois nomes são até usados juntos como em alguns clientes de e-mail, informando que você pode usar uma conexão segura SSL/TLS.

Configurações **/ Controle de Conexão / TLS/SSL**

Visão geral do TLS/SSL

O HSC MailInspector permite que o tráfego entre os servidores MTA, na camada SMTP, seja criptografado através do STARTTLS, dessa forma, é possível garantir que a entrada e a saída das mensagens tenham um canal seguro, TLS/SSL, a fim de evitar que usuários mal-intencionados tenham acesso as mensagens durante a transmissão das mesmas.

O protocolo TLS/SSL não substitui a criptografia de mensagens S/MIME, que permite a criptografia de fim-a-fim através de mecanismo PKI de chave pública e privada.

O suporte a TLS/SSL também pode ser habilitado com o objetivo de garantir um canal seguro para a função Relay Autenticado, fornecendo criptografia para realização de autenticação de clientes externos, bem como o uso do SMTP/TLS e/ou SMTPS em formato de Relay Autenticado, forçando o uso de usuário e senha para permitir envio de e-mails.

O MailInspector possibilita o uso do SSL quando o TLS não estiver disponível na outra ponta da conexão, além de importar o certificado confiável (gerado por uma unidade certificadora) de forma automática. Também permite que o administrador configure quais domínios de remetentes ou destinatários utilizarão de forma obrigatória a criptografia TLS/SSL, bem como envio de alerta em caso de falha de negociação do protocolo TLS.

Definições de Opções - TLS/SSL

Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição
Salvar	Quando clicado, grava as configurações realizadas.
Habilitar suporte a TLS	Escolha entre: • **Sim** - Indica que o suporte a TLS v1.0, v1.1, v1.2, v1.3 está ativo. • **Não** - Indica que outros protocolos como SSL v1.0, SSL v2.0 e SSL v3.0 também estarão disponíveis.
Modo de Operação	Escolha entre: • **Modo de Compatibilidade** – Utiliza todos as versões de TLS, deixando o MailInspector compatível a todas as versões, mas pode causar timeout, pois ele sempre tentará utilizar a versão mais recente e somente depois de timeout dessa tentativa é que ele passará a tentar na versão anteriores, dessa forma dependendo do servidor de envio/recebimento do e-mail, pode ocasionar timeout de conexão.

	• **TLS 1.2 ou Superior** – Utiliza a versão TLS 1.2, se o outro servidor de envio/recebimento de e-mail tiver essa versão funcional e ativa, é compatível com várias cifras de TLS versão 1.2 (ver *Cifras utilizadas pelo TLS*). • **TLS 1.2 ou superior Hardened** – Obriga o uso do TLS 1.2 somente com certas cifras (ECDHE-RSA-AES256-GCM-SHA384 ou DHE-RSA-AES256-GCM-SHA384). Caso o servidor de recebimento/envio de e-mail não tenha uma dessas cifras, a conexão é cancelada.
Certificado	• **Gerado Automaticamente** – O próprio MailInspector gera um certificado TLS/SSL automaticamente, sem necessidade de importação de certificado válido. • **Personalizado** – Permite a importação de certificado gerado por terceiros.
Certificado no formato PEM	Permite selecionar o certificado digital no formato PEM.
Chave no formato PEM	Permite selecionar a chave no formato PEM.

Entrada de E-mails	Configura o suporte a comunicação TLS/SSL para o recebimento de mensagens.
	• **Nível de Segurança** - Selecione o nível de segurança que será utilizado para o recebimento de mensagens.
	  ○ **NENHUM -** Desabilita o suporte TLS/SSL para o recebimento de mensagens.
	  ○ **PERMISSIVO** - Habilita o suporte TLS/SSL para o recebimento de mensagens, e tenta utilizar o método criptografado para todo o diálogo SMTP SMTP (se o servidor que está enviando a mensagem não tiver suporte a TLS/SSL a mensagem será recebida sem a ativação de TLS/SSL).
	  ○ **RESTRITIVO** - Habilita o suporte TLS/SSL para o recebimento de mensagens, e força a utilização do método criptografado para todo o diálogo SMTP (se o servidor que está enviando a mensagem não tiver suporte a TLS/SSL a mensagem não será recebida).
	• **Ativar TLS para Relay Autenticado** – Indica que o suporte a TLS/SSL (SMTPS) está ativo para o **Relay Autenticado**
	  ○ **Sim:** Uso de relay autenticado, forçando o uso de usuário e senha para permitir o envio de e-mails pelo MailInspector pelo protocolo TLS/SSL.
	  ○ **Não:** Permite o envio de e-mails pelo protocolo TLS/SSL sem a necessidade de usuário e senha, integrando de forma anônima (sem senha).
	• **Obrigatório para os seguintes domínios:** Neste campo é possível configurar quais domínios de origem "Remetente" terão o uso do TLS OBRIGATÓRIO, ou seja, todos e-mails recebidos deste domínio deverão ser enviados usando TLS, caso não seja usado TLS pelo servidor de origem o e-mail será rejeitado.

Saída de E-mails	Configura o suporte a comunicação TLS/SSL para o envio de mensagens.
	• **Nível de Segurança** - Selecione o nível de segurança que será utilizado para o envio de mensagens.
	  ○ **NENHUM** - Desabilita o suporte TLS/SSL para o envio de mensagens.
	  ○ **PASSIVO** - Habilita o suporte TLS/SSL para o envio de mensagens, e tenta utilizar o método criptografado para todo o diálogo SMTP SMTP (se o servidor que está enviando a mensagem não tiver suporte a TLS/SSL a mensagem será enviada sem a ativação de TLS/SSL).

- **RESTRITIVO** - Habilita o suporte TLS/SSL para o envio de mensagens, e força a utilização do método criptografado para todo o diálogo SMTP (se o servidor que está recebendo a mensagem não tiver suporte a TLS/SSL a mensagem não será enviada).

- **Obrigatório para os seguintes domínios:** Neste campo é possível configurar quais domínios de destino o uso do TLS será OBRIGATORIO, ou seja, todos e-mails enviados para este domínio deverão ser enviados usando TLS, caso não seja usado TLS pelo servidor de destino o e-mail não será entregue.
- **Política:** Indica a política de segurança empregada no protocolo TLS/SSL
  - **Não Criptografa:** Sem uso de criptografia.
  - **Somente Criptografado:** Ativa a criptografia sem verificação de qualquer autenticidade da chave/certificado utilizado.
  - **Somente Criptografado com Checagem de MX:** Ativa a criptografia com uso de chave/certificado verificando quanto ao MX.
  - **Somente Criptografado com checagem de MX e Certificado Válido:** Ativa a criptografia com uso de chave/certificado verificando tanto o MX, quanto a autenticidade do certificado utilizado (se é válido e se foi emitido por órgão autenticador).

Para gerar um par de chaves auto assinadas você pode gerar através do comando openssl. Caso necessite este comando está presente no Ponto de Acesso ou na Console de Administração que pode ser acessado via SSH.

Para gerar as chaves auto assinadas basta executar o comando abaixo:

```
[root@hsc tmp]# openssl req -new -x509 -days 3650 -nodes -out /tmp/ca.pem
-keyout /tmp/key.pem
```

Este comando irá gerar dois arquivos: ca.pem que deve ser importado no campo "Certificado no Formato PEM" e key.pem que deve ser importado no campo "Chave no Formato PEM"

Caso o SSL/TLS esteja configurado para uso RESTRITIVO ou se for enviado/recebido de um domínio ou a um domínio configurado como OBRIGATÓRIO, se houver falha na comunicação devido a falta de protocolo na outra ponta, o MailInspector enviará alerta ao administrador do sistema sobre o caso.

Cifras utilizadas pelo TLS

TLS v1.0	Cifra		Order	Strengh
Modo Compatibilidade	xc014	ECDHE-RSA-AES256-SHA	ECDH 256	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
	x39	DHE-RSA-AES256-SHA	DH 1024	TLS_DHE_RSA_WITH_AES_256_CBC_SHA
	x88	DHE-RSA-CAMELLIA256-SHA	DH 1024	TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA
	xc019	AECDH-AES256-SHA	ECDH 256	TLS_ECDH_anon_WITH_AES_256_CBC_SHA
	x3a	ADH-AES256-SHA	DH 1024	TLS_DH_anon_WITH_AES_256_CBC_SHA
	x89	ADH-CAMELLIA256-SHA	DH 1024	TLS_DH_anon_WITH_CAMELLIA_256_CBC_SHA

	x35	AES256-SHA	RSA	
	x84	CAMELLIA256-SHA	RSA	
	xc013	ECDHE-RSA-AES128-SHA	ECDH	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
	x33	DHE-RSA-AES128-SHA	DH	TLS_DHE_RSA_WITH_AES_128_CBC_SHA
	x9a	DHE-RSA-SEED-SHA	DH	TLS_DHE_RSA_WITH_SEED_CBC_SHA
	x45	DHE-RSA-CAMELLIA128-SHA	DH	TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA
	xc018	AECDH-AES128-SHA	ECDH	TLS_ECDH_anon_WITH_AES_128_CBC_SHA
	x34	ADH-AES128-SHA	DH	TLS_DH_anon_WITH_AES_128_CBC_SHA
	x9b	ADH-SEED-SHA	DH	TLS_DH_anon_WITH_SEED_CBC_SHA
	x46	ADH-CAMELLIA128-SHA	DH	TLS_DH_anon_WITH_CAMELLIA_128_CBC_SHA
	x2f	AES128-SHA	RSA	
	x96	SEED-SHA	RSA	
	x41	CAMELLIA128-SHA	RSA	
	x07	IDEA-CBC-SHA	RSA	
	xc011	ECDHE-RSA-RC4-SHA	ECDH	TLS_ECDHE_RSA_WITH_RC4_128_SHA
	xc016	AECDH-RC4-SHA	ECDH	TLS_ECDH_anon_WITH_RC4_128_SHA
	x18	ADH-RC4-MD5	DH	TLS_DH_anon_WITH_RC4_128_MD5
	x05	RC4-SHA	RSA	
	x04	RC4-MD5	RSA	
	xc012	ECDHE-RSA-DES-CBC3-SHA	ECDH	TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
	x16	EDH-RSA-DES-CBC3-SHA	DH	TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
	xc017	AECDH-DES-CBC3-SHA	ECDH	TLS_ECDH_anon_WITH_3DES_EDE_CBC_SHA
	x1b	ADH-DES-CBC3-SHA	DH	TLS_DH_anon_WITH_3DES_EDE_CBC_SHA
	x0a	DES-CBC3-SHA	RSA	

TLS v1.1	**Cifra**		**Order**	**Strengh**
Modo Compatibilidade	xc014	ECDHE-RSA-AES256-SHA	ECDH	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
	x39	DHE-RSA-AES256-SHA	DH	TLS_DHE_RSA_WITH_AES_256_CBC_SHA
	x88	DHE-RSA-CAMELLIA256-SHA	DH	TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA
	xc019	AECDH-AES256-SHA	ECDH	TLS_ECDH_anon_WITH_AES_256_CBC_SHA
	x3a	ADH-AES256-SHA	DH	TLS_DH_anon_WITH_AES_256_CBC_SHA
	x89	ADH-CAMELLIA256-SHA	DH	TLS_DH_anon_WITH_CAMELLIA_256_CBC_SHA
	x35	AES256-SHA	RSA	
	x84	CAMELLIA256-SHA	RSA	
	xc013	ECDHE-RSA-AES128-SHA	ECDH	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
	x33	DHE-RSA-AES128-SHA	DH	TLS_DHE_RSA_WITH_AES_128_CBC_SHA
	x9a	DHE-RSA-SEED-SHA	DH	TLS_DHE_RSA_WITH_SEED_CBC_SHA
	x45	DHE-RSA-CAMELLIA128-SHA	DH	TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA

	xc018	AECDH-AES128-SHA	ECDH	TLS_ECDH_anon_WITH_AES_128_CBC_SHA
	x34	ADH-AES128-SHA	DH	TLS_DH_anon_WITH_AES_128_CBC_SHA
	x9b	ADH-SEED-SHA	DH	TLS_DH_anon_WITH_SEED_CBC_SHA
	x46	ADH-CAMELLIA128-SHA	DH	TLS_DH_anon_WITH_CAMELLIA_128_CBC_SHA
	x2f	AES128-SHA	RSA	
	x96	SEED-SHA	RSA	
	x41	CAMELLIA128-SHA	RSA	
	x07	IDEA-CBC-SHA	RSA	
	xc011	ECDHE-RSA-RC4-SHA	ECDH	TLS_ECDHE_RSA_WITH_RC4_128_SHA
	xc016	AECDH-RC4-SHA	ECDH	TLS_ECDH_anon_WITH_RC4_128_SHA
	x18	ADH-RC4-MD5	DH	TLS_DH_anon_WITH_RC4_128_MD5
	x05	RC4-SHA	RSA	
	x04	RC4-MD5	RSA	
	xc012	ECDHE-RSA-DES-CBC3-SHA	ECDH	TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
	x16	EDH-RSA-DES-CBC3-SHA	DH	TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
	xc017	AECDH-DES-CBC3-SHA	ECDH	TLS_ECDH_anon_WITH_3DES_EDE_CBC_SHA
	x1b	ADH-DES-CBC3-SHA	DH	TLS_DH_anon_WITH_3DES_EDE_CBC_SHA
	x0a	DES-CBC3-SHA	RSA	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA

TLS v1.2	**Cifra**		**Order**	**Strengh**
Modo Compatibilidade	xc030	ECDHE-RSA-AES256-GCM-SHA384	ECDH	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
	xc028	ECDHE-RSA-AES256-SHA384	ECDH	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
	xc014	ECDHE-RSA-AES256-SHA	ECDH	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
	x9f	DHE-RSA-AES256-GCM-SHA384	DH	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
	x6b	DHE-RSA-AES256-SHA256	DH	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
	x39	DHE-RSA-AES256-SHA	DH	TLS_DHE_RSA_WITH_AES_256_CBC_SHA
	x88	DHE-RSA-CAMELLIA256-SHA	DH	TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA
	xc019	AECDH-AES256-SHA	ECDH	TLS_ECDH_anon_WITH_AES_256_CBC_SHA
	xa7	ADH-AES256-GCM-SHA384	DH	TLS_DH_anon_WITH_AES_256_GCM_SHA384
	x6d	ADH-AES256-SHA256	DH	TLS_DH_anon_WITH_AES_256_CBC_SHA256
	x3a	ADH-AES256-SHA	DH	TLS_DH_anon_WITH_AES_256_CBC_SHA
	x89	ADH-CAMELLIA256-SHA	DH	TLS_DH_anon_WITH_CAMELLIA_256_CBC_SHA
	x9d	AES256-GCM-SHA384	RSA	
	x3d	AES256-SHA256	RSA	
	x35	AES256-SHA	RSA	
	x84	CAMELLIA256-SHA	RSA	

	xc02f	ECDHE-RSA-AES128-GCM-SHA256	ECDH	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
	xc027	ECDHE-RSA-AES128-SHA256	ECDH	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
	xc013	ECDHE-RSA-AES128-SHA	ECDH	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
	x9e	DHE-RSA-AES128-GCM-SHA256	DH	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
	x67	DHE-RSA-AES128-SHA256	DH	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
	x33	DHE-RSA-AES128-SHA	DH	TLS_DHE_RSA_WITH_AES_128_CBC_SHA
	x9a	DHE-RSA-SEED-SHA	DH	TLS_DHE_RSA_WITH_SEED_CBC_SHA
	x45	DHE-RSA-CAMELLIA128-SHA	DH	TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA
	xc018	AECDH-AES128-SHA	ECDH	TLS_ECDH_anon_WITH_AES_128_CBC_SHA
	xa6	ADH-AES128-GCM-SHA256	DH	TLS_DH_anon_WITH_AES_128_GCM_SHA256
	x6c	ADH-AES128-SHA256	DH	TLS_DH_anon_WITH_AES_128_CBC_SHA256
	x34	ADH-AES128-SHA	DH	TLS_DH_anon_WITH_AES_128_CBC_SHA
	x9b	ADH-SEED-SHA	DH	TLS_DH_anon_WITH_SEED_CBC_SHA
	x46	ADH-CAMELLIA128-SHA	DH	TLS_DH_anon_WITH_CAMELLIA_128_CBC_SHA
	x9c	AES128-GCM-SHA256	RSA	
	x3c	AES128-SHA256	RSA	
	x2f	AES128-SHA	RSA	
	x96	SEED-SHA	RSA	
	x41	CAMELLIA128-SHA	RSA	
	x07	IDEA-CBC-SHA	RSA	
	xc011	ECDHE-RSA-RC4-SHA	ECDH	TLS_ECDHE_RSA_WITH_RC4_128_SHA
	xc016	AECDH-RC4-SHA	ECDH	TLS_ECDH_anon_WITH_RC4_128_SHA
	x18	ADH-RC4-MD5	DH	TLS_DH_anon_WITH_RC4_128_MD5
	x05	RC4-SHA	RSA	
	x04	RC4-MD5	RSA	
	xc012	ECDHE-RSA-DES-CBC3-SHA	ECDH	TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
	x16	EDH-RSA-DES-CBC3-SHA	DH	TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
	xc017	AECDH-DES-CBC3-SHA	ECDH	TLS_ECDH_anon_WITH_3DES_EDE_CBC_SHA
	x1b	ADH-DES-CBC3-SHA	DH	TLS_DH_anon_WITH_3DES_EDE_CBC_SHA
	x0a	DES-CBC3-SHA	RSA	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

TLS v1.2	**Cifra**		**Order**	**Strengh**
TLS 1.2 ou Superior	xc030	ECDHE-RSA-AES256-GCM-SHA384	ECDH	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
	xc028	ECDHE-RSA-AES256-SHA384	ECDH	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384

	xc014	ECDHE-RSA-AES256-SHA	ECDH	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
	x9f	DHE-RSA-AES256-GCM-SHA384	DH	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
	x6b	DHE-RSA-AES256-SHA256	DH	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
	x39	DHE-RSA-AES256-SHA	DH	TLS_DHE_RSA_WITH_AES_256_CBC_SHA
	x88	DHE-RSA-CAMELLIA256-SHA	DH	TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA
	xc019	AECDH-AES256-SHA	ECDH	TLS_ECDH_anon_WITH_AES_256_CBC_SHA
	xa7	ADH-AES256-GCM-SHA384	DH	TLS_DH_anon_WITH_AES_256_GCM_SHA384
	x6d	ADH-AES256-SHA256	DH	TLS_DH_anon_WITH_AES_256_CBC_SHA256
	x3a	ADH-AES256-SHA	DH	TLS_DH_anon_WITH_AES_256_CBC_SHA
	x89	ADH-CAMELLIA256-SHA	DH	TLS_DH_anon_WITH_CAMELLIA_256_CBC_SHA
	x9d	AES256-GCM-SHA384	RSA	
	x3d	AES256-SHA256	RSA	
	x35	AES256-SHA	RSA	
	x84	CAMELLIA256-SHA	RSA	
	xc02f	ECDHE-RSA-AES128-GCM-SHA256	ECDH	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
	xc027	ECDHE-RSA-AES128-SHA256	ECDH	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
	xc013	ECDHE-RSA-AES128-SHA	ECDH	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
	x9e	DHE-RSA-AES128-GCM-SHA256	DH	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
	x67	DHE-RSA-AES128-SHA256	DH	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
	x33	DHE-RSA-AES128-SHA	DH	TLS_DHE_RSA_WITH_AES_128_CBC_SHA
	x9a	DHE-RSA-SEED-SHA	DH	TLS_DHE_RSA_WITH_SEED_CBC_SHA
	x45	DHE-RSA-CAMELLIA128-SHA	DH	TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA
	xc018	AECDH-AES128-SHA	ECDH	TLS_ECDH_anon_WITH_AES_128_CBC_SHA
	xa6	ADH-AES128-GCM-SHA256	DH	TLS_DH_anon_WITH_AES_128_GCM_SHA256
	x6c	ADH-AES128-SHA256	DH	TLS_DH_anon_WITH_AES_128_CBC_SHA256
	x34	ADH-AES128-SHA	DH	TLS_DH_anon_WITH_AES_128_CBC_SHA
	x9b	ADH-SEED-SHA	DH	TLS_DH_anon_WITH_SEED_CBC_SHA
	x46	ADH-CAMELLIA128-SHA	DH	TLS_DH_anon_WITH_CAMELLIA_128_CBC_SHA
	x9c	AES128-GCM-SHA256	RSA	
	x3c	AES128-SHA256	RSA	
	x2f	AES128-SHA	RSA	
	x96	SEED-SHA	RSA	
	x41	CAMELLIA128-SHA	RSA	
	x07	IDEA-CBC-SHA	RSA	

	xc011	ECDHE-RSA-RC4-SHA	ECDH	TLS_ECDHE_RSA_WITH_RC4_128_SHA
	xc016	AECDH-RC4-SHA	ECDH	TLS_ECDH_anon_WITH_RC4_128_SHA
	x18	ADH-RC4-MD5	DH	TLS_DH_anon_WITH_RC4_128_MD5
	x05	RC4-SHA	RSA	
	x04	RC4-MD5	RSA	
	xc012	ECDHE-RSA-DES-CBC3-SHA	ECDH	TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
	x16	EDH-RSA-DES-CBC3-SHA	DH	TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
	xc017	AECDH-DES-CBC3-SHA	ECDH	TLS_ECDH_anon_WITH_3DES_EDE_CBC_SHA
	x1b	ADH-DES-CBC3-SHA	DH	TLS_DH_anon_WITH_3DES_EDE_CBC_SHA
	x0a	DES-CBC3-SHA	RSA	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

TLS v1.2	**Cifra**		**Order**	**Strengh**
TLS 1.2 ou Superior Hardened	xc030	ECDHE-RSA-AES256-GCM-SHA384	ECDH	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
	x9f	DHE-RSA-AES256-GCM-SHA384	DH	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384

A cifra mais indicada para uso é **TLS 1.2 ou Superior Hardened**, conforme indicação de boas práticas, pois as outras versões podem apresentar falhas de segurança, sendo mantido no MailInspector por questão de compatibilidade com servidores de e-mail que usam cifras mais antigas, que não é compatível com a cifra **TLS 1.2 ou Superior Hardened**.

Controle de Bounce

Bounce Mail é o e-mail de retorno de qualquer erro que comprometa a entrega da mensagem ao destinatário (destinatário não existe, falha de servidor, etc). Como os servidores por padrão são configurados para aceitarem os e-mails de bouce (e-mail de retorno com erro de entrega), muitos hackers utilizam dessa fragilidade para atacar os usuários, enviando e-mails que se passam por e-mail de retorno de erro.

Configurações / **Controle de Conexão / Controle de Bounce**

Visão geral do controle de bounce

O Controle de Bounce, ou Bounce Address Tag Validation (BATV), é um método para determinar se o endereço de retorno especificado em uma mensagem é válido. Ele é projetado para rejeitar mensagens que possuem endereços de retorno falsificados por spammers.

Este recurso, quando ativado, assina todas as mensagens com um endereço de retorno que inclui uma marcação e um token criptográfico que não pode ser falsificado. Qualquer mensagem que é devolvida como "Bounce" devido a algum erro no servidor, sem uma assinatura válida pode, então, ser identificada pelo HSC MailInspector.

Com a verificação de TAG do BATV, o MailInspector consegue efetuar a proteção de Non-Delivery Attack, ao qual seria gerado um e-mail de report à partir do Bounce falso recebido. Com o bloqueio do falso Bounce Mail, o relatório de Non-Delivery não é gerado, evitando eventual flood de Non-Delivery Report.

O funcionamento consiste em substituir o envelope remetente como nome@dominio.com.br com prvs=valor-tag=nome@dominio.com.br, onde PRVs, é chamado de "Assinatura Privada Simples".

Estas modificações são realizadas automaticamente, e não afetam ou requerem quaisquer configurações no ambiente onde estão sendo implementadas.

Definições de Opções - Controle de Bounce

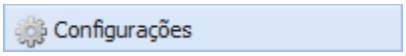
Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição
Salvar	Quando clicado, grava as configurações realizadas.
Regerar Chaves	Permite forçar a geração de uma nova chave de assinatura das mensagens.
Habilitar Controle de Bounce - BATV - Bounce Address TAG Verification	Escolha entre: • **Sim** - Indica que o controle de bounce está ativo. • **Não** - Indica que o controle de bounce está desativado.
Tempo de Validade da Chave	Informe o tempo, em dias, de validade da chave de assinatura das mensagens.
Pontuação	Permite definir a pontuação que será atribuída a mensagens verificadas pelo Controle de Bounce:

	• **Mensagens Válidas** - Mensagens consideradas válidas, quando contém a assinatura no envelope do remetente. • **Mensagens Inválidas** - Mensagens consideradas inválidas, quando não contém a assinatura no envelope do remetente.

SPAM Throttling

O SPAM throttling é uma técnica para limitar a quantidade de e-mails oriunda de uma única fonte, quando ela começa a enviar muitos e-mails classificados como SPAM, dessa forma controlando e “engargalando” os e-mails, evitando sobrecarga no sistema e também prevenindo eventual ataque de e-mail em massa dirigido a sua empresa.



/ Controle de Conexão / SPAM Throttling

Visão geral do SPAM throttling

O SPAM Throttling faz parte da camada de controle de conexão do HSC MailInspector contra SPAM, principalmente contra-ataques de "Envio Mail em Massa”, "Command Control Center"e "Bootnets".

Este filtro consiste em consultar de forma online o sistema HSC SmartDefender, obtendo informações sobre a Reputação do endereço IP de origem da conexão a fim de identificar servidores que distribuem SPAM, vírus, malwares e outras ameaças. Através destas informações, é realizada a penalização dos servidores de origem que possuem algum risco, limitando a quantidade ou percentual de mensagens que estes servidores podem enviar, priorizando assim que mensagens legítimas sejam entregues, enquanto um grande volume de spammers é punido.

São 12 níveis de reputação, que permite uma maior granularidade na configuração.

Definições de Opções - SPAM Throttling

Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição
Salvar	Quando clicado, grava as configurações realizadas.
Reputação de Alto Risco	Informe a quantidade de mensagens que serão aceitas, dentro do intervalo de tempo de uma hora, procedentes de servidores classificados como alto risco. Se for configurado 0 (zero) as mensagens oriundas desta origem serão bloqueadas na camada SMTP e não serão recebidas. Esta categoria tem 4 níveis de reputação afim de aumentar sua granularidade de configuração.
Reputação de Médio Risco	Informe a quantidade de mensagens que serão aceitas, dentro do intervalo de tempo de uma hora, procedentes de servidores classificados como médio risco. Se for configurado 0 (zero) as mensagens oriundas desta origem serão bloqueadas na camada SMTP e não serão recebidas. Esta categoria tem 4 níveis de reputação afim de aumentar sua granularidade de configuração
Reputação de Possível Risco	Informe a quantidade de mensagens que serão aceitas, dentro do intervalo de tempo de uma hora, procedentes de servidores classificados como possível risco. Se for configurado 0 (zero) as mensagens oriundas desta origem serão bloqueadas na camada SMTP e não serão recebidas.

	Esta categoria tem 4 níveis de reputação afim de aumentar sua granularidade de configuração

Quota/Controle de Fluxo

Use esta página para exibir, adicionar, editar ou excluir configurações de Quota/Controle de Fluxo do Controle de Conexão.

Configurações / **Controle de Conexão / Quota/Controle de Fluxo**

Visão geral da quota e controle de fluxo

A Quota/Controle de Fluxo faz parte do sistema de controle de fluxo de conexão, e do controle de quotas de usuários implantado no HSC MailInspector.

O Sistema De Quota/Controle de Fluxo serve para restringir e/ou limitar determinados tipos de tráfego. O sistema permite um controle granular por meio de uma criação de regras que podem ser ativadas por:

- Endereço de IP de Origem;
- Sender HELO Domain;
- Sender Envelope;
- Sender Header;
- E-mail do destinatário;
- Domínio do Remetente;
- Domínio do Destinatário;
- Subdomínio do remetente;
- Subdomínio do destinatário;
- Grupo de Usuários de Origem;
- Grupo de Usuários de Destino;
- País;
- IP de Origem;
- IP de Destino;
- Range de IP;
- Classe de IP;
- Reputação;
- Qualquer Cabeçalho do protocolo SMTP, incluindo cabeçalhos customizados;
- Assunto/Subject;
- Anexos (Tamanho, quantidade, tipo – Mime-Type, Extensão, nome do anexo, se é compactado, etc),
- Conteúdo do e-mail, entre vários outros campos.

O sistema permite criar contadores a fim de limitar o tráfego podendo contabilizar o tráfego por: IP de Origem, Remetente, Domínio do Remetente, Usuário, Domínio do Destinatário, Destinatário, etc. Casando por período de tempo (segundos, minutos ou hora) e/ou quantidade e/ou tamanho total de e-mails.

Desta forma o HSC MailInspector pode auxiliar o controle de fluxo de e-mails de sua empresa de uma forma muito customizável, protegendo inclusive a contas invadidas, uma vez que a conta invadida por padrão efetua múltiplos disparos de e-mails a todos os sentidos (tanto envio de e-mails externos, quanto e-mails internos), sendo detectado pelo controle de fluxo, como volume anômalo de e-mails, bloqueando-os por excesso de volume enviado e gerando alertas.

Definições de Opções - Quota/Controle de Fluxo

Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição
Adicionar	Cadastra um novo registro de alias de e-mail. Quando clicado, abre a caixa de diálogo **Adicionar/Editar Quota/Controle de Fluxo**.
Editar	Edita as configurações de um registro existente. Quando clicado, abre a caixa de diálogo **Adicionar/Editar Quota/Controle de Fluxo**.
Remover	Quando clicado, exclui o registro selecionado.
Configurar Mensagens de Erro	Edita as mensagens de erro que são enviadas aos remetentes. Quando clicado, abre a caixa de diálogo **Adicionar/Editar Configurar Mensagens de Erro**.

Definições de Opções - Adicionar/Editar Quota/Controle de Fluxo

As opções a seguir indicam a definição dos parâmetros de controle de fluxo, podendo ser por:

- IP de Origem;
- E-mail do Remetente;
- Domínio do Remetente;
- Nome do Remetente (Display Name);
- E-mail do Destinatário;
- Domínio do Destinatário;
- Nome do Destinatário (Display Name);

Opções	Definição
Salvar	Quando clicado, grava as configurações realizadas.
Cancelar	Quando clicado, cancela a ação.
Nome	Informe um nome descritivo para a política.
Ação	Escolha entre: • **Atrasar** - Indica que as mensagens que combinarem com as configurações da política terão a entrega atrasada, e permanecerão aguardando o próximo intervalo de tempo para serem entregues ao destinatário. • **Rejeitar** - Indica que as mensagens que combinarem com as configurações da política terão a entrega rejeitada, sendo devolvidas para o remetente.
De	Selecione o grupo pré-cadastrado de remetentes. Os itens Expressão Regular e Grupos LDAP presentes no Grupo de Usuários selecionado, não são utilizados nesta funcionalidade.
Para	Selecione o grupo pré-cadastrado de destinatários. Os itens Expressão Regular e Grupos LDAP presentes no Grupo de Usuários selecionado, não são utilizados nesta funcionalidade.
Tipo	Escolha entre:

	• **Acumulativo** - Permite criar uma política por período de tempo fixo e pré-definido (diário, semanal ou mensal). • **Flexível** - Permite criar uma política por período de tempo variável (segundos, minutos ou horas).
Contabilizar por	É feito o agrupamento de totalização (contador de fluxo) por: • IP de Origem; • E-mail do Remetente; • Domínio do Remetente; • Nome do Remetente (Display Name); • E-mail do Destinatário; • Domínio do Destinatário; • Nome do Destinatário (Display Name);
Total de Mensagens	Permite definir o número total de mensagens para combinar com a política.
Tamanho Total	Permite definir o tamanho total das mensagens trafegadas para combinar com a política.
Total de Destinatários	Permite definir o número total de destinatários para combinar com a política.

Definições de Opções - Adicionar/Editar Configurar Mensagens de Erro

Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição
Salvar	Quando clicado, grava as configurações realizadas.
Cancelar	Quando clicado, cancela a ação.
Rejeitar	Informe a mensagem que será enviada para o remetente em caso de rejeição.
Atrasar	Informe a mensagem que será enviada para o remetente em caso de atraso.

Observação sobre a ação atrasar no Controle de Fluxo
Por exemplo: Se for configurado o controle de fluxo para 200 e-mails/hora, e o MLI receber 250 e-mails, enviará os primeiros 200 e-mails e os 50 e-mails excedentes ficam na fila "atrasados" para enviar quando rodar o novo ciclo da próxima hora.

No caso, você já teria 50 e-mails na fila, podendo nesse intervalo de tempo ainda enviar mais 150. Se tiver outra leva de 200, serão entregues os 50 primeiros da fila do ciclo anterior + 150 do periodo corrente.

Da mesma forma é possível determinar número máximo de destinatários por um determinado tempo (por exemplo 100 destinatários por hora).

Relay Autenticado

Use esta página para exibir, adicionar ou editar configurações de Relay Autenticado.

Configurações / **Controle de Conexão / Relay Autenticado**

Visão geral do relay autenticado

O item Relay Autenticado (Sender Authentication) permite que o HSC MailInspector seja utilizado como servidor SMTP/SMTPS para o envio de e-mails.

Este recurso permite configurar se a autenticação de que usuários será preferida ou obrigatória. Clientes com endereço IP dinâmico ou IP estático podem enviar mensagens através do HSC MLI de forma segura.

Definições de Opções - Relay Autenticado

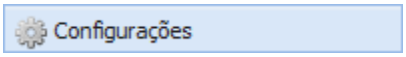
Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição
Salvar	Quando clicado, grava as configurações realizadas.
Ativar	Escolha entre: • **Sim** - Indica que o relay autenticado está ativo. Permitindo que usuários realizem o envio de e-mail autenticado. • **Não** - Indica que o relay autenticado está desativado.
Método	Permite selecionar o tipo de autenticação que será utilizada para validar as credenciais de acesso do usuário. • **IMAP** - Realiza a validação das credenciais do usuário logando em um servidor de correio eletrônico IMAP. • **RADIUS** - Realiza a validação das credenciais do usuário logando em um servidor RADIUS. • **POP3 -** Realiza a validação das credenciais do usuário logando com o protocolo POP3. • **LDAP** - Realiza a validação das credenciais do usuário logando em um servidor com base LDAP ou Microsoft Active Directory.
Servidor	Informe o endereço IP do servidor no formato IPv4.
Porta	Quando selecionado o método **IMAP**, informe o número da porta do serviço SMTP. A porta padrão para servidores SMTP é 25, SMTPS 465 / 587 (com TLS) Quando selecionado o método **RADIUS**, informe o número da porta de consulta. A porta padrão para consultas RADIUS é 1812. Quando selecionado o método **POP3**, informe o número da porta de consulta. A porta padrão para consultas RADIUS é 110.

	Quando selecionado o método **LDAP**, informe o número da porta de consulta. As portas padrões para consultas LDAP é TCP 389, TCP 3268, TCP 636 e TCP 3269.
Base DN	Quando selecionado o método **LDAP**, informe a base DN do domínio. A base DN deve ser informada de maneira completa, no seguinte formato: dc=empresa, dc=com, dc=br
Filtro de Pesquisa	Quando selecionado o método **LDAP**, informe o filtro de pesquisa do usuário. Um exemplo de valor de pesquisa é (uid=%u).
Usuário	Quando selecionado o método **LDAP**, informe o nome de um usuário para consulta no formato: usuario@dominio_da_empresa
Senha	Quando selecionado o método **LDAP**, informe a senha do usuário.

Reescrita de E-mails

Use esta página para exibir, adicionar, editar ou excluir configurações de Reescrita de E-mails.



/ Controle de Conexão / Reescrita de E-mails

Visão geral da reescrita de e-mails

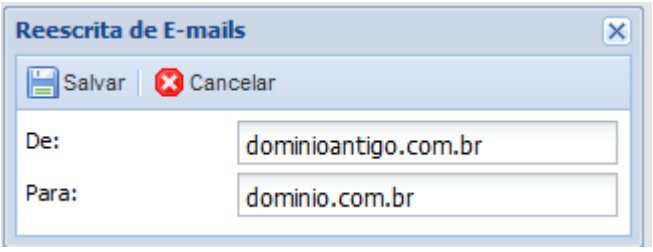
Alias de e-mail (apelido) é um endereço de e-mail alternativo que aponta para uma conta de usuário existente, o sistema permite o também o mascaramento de endereços (Address Aliasing/Masquerading/Rewriting).

Por exemplo, o usuario@empresa.com.br também poderá receber e-mails endereçados a nome@empresa.com.br. Se você criar nome@empresa.com.br como um alias de e-mail para usuario@empresa.com.br, o HSC MailInspector entregará o e-mail destinado ao alias para o endereço principal do usuário.

O item Reescrita de E-mails permite que sejam criados aliases de e-mail (apelidos) para um usuário, grupo de usuários ou conector LDAP que permite consultar em um servidor de diretório externo.

A reescrita de e-mails não fica atrelado somente a e-mails, é possível efetuar a reescrita de todo domínio, por exemplo:

Se a empresa deixou de usar o dominioantigo.com.br e passou a usar domínio.com.br, basta ele efetuar a reescrita dos domínios indicados.



Definições de Opções - Reescrita de E-mails

Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição
Adicionar	Cadastra um novo registro de alias de e-mail. Quando clicado, abre a caixa de diálogo **Adicionar/Editar Reescrita de E-mails**.
Editar	Edita as configurações de um registro existente. Quando clicado, abre a caixa de diálogo **Adicionar/Editar Reescrita de E-mails**.
Remover	Quando clicado, exclui o registro selecionado.
Pesquisar	Efetua a pesquisa rápida no módulo Reescrita de E-Mails, podendo ser por: **DE:** String parcial ou extato do campo DE ORIGEM do e-mail **PARA:** String parcial ou extato do campo PARA DESTINO do e-mail
Limpar	Limpa o filtro de pesquisa rápida e gera refresh da tela de Reescrita de E-Mails.

Importar	Permite importar um arquivo de texto com aliases de e-mail. Quando clicado, abre a caixa de diálogo **Importar Definições de Reescrita**.
LDAP	Informe o servidor LDAP externo de consulta, com a porta, usuário e sua senha.

Definições de Opções - Adicionar/Editar Reescrita de E-mails

Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição
Salvar	Quando clicado, grava as configurações realizadas.
Cancelar	Quando clicado, cancela a ação.
De	Informe o endereço de e-mail completo que será utilizado como alias (apelido) para o endereço válido do usuário.
Para	Informe o endereço de e-mail completo que receberá a mensagem através do alias (apelido).

Definições de Opções - Importar Definições de Reescrita

Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição
Salvar	Quando clicado, grava as configurações realizadas.
Cancelar	Quando clicado, cancela a ação.
Arquivo	Quando clicado, permite selecionar o arquivo com a lista de aliases de e-mail (apelidos) a ser importado. O conteúdo do arquivo deve estar no formato "alias”, “e-mail válido", com um valor por linha.

Outbreak Filter

O HSC MailInspector possui um sistema de detecção avançado de surto de novas ameaças, permitindo ao administrador configurar as ações que serão tomadas em tempo real quando um novo surto de ataque iniciar.

Configurações / **Controle de Conexão / Outbreak Filter**

Visão geral do Outbreak Filter

O HSC MailInspector possui um sistema de detecção avançado de surto de novas ameaças, permitindo ao administrador configurar as ações que serão tomadas em tempo real quando um novo surto de ataque iniciar. Permitindo rejeitar um e-mail ou colocar ele em quarentena.

Através de opções parametrizáveis, o administrador consegue definir quais as características que definem um novo surto de Vírus, surto de SPAM ou Harvest Attack (ataques de dicionário).

Este mecanismo trabalha como um sistema de Reputação Local de remetentes, independente, e se atualiza dinamicamente com dados do tráfego local.

Definições de Opções - Outbreak Filter

Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição
Salvar	Quando clicado, grava as configurações realizadas.
SPAM	Informe quais são os parâmetros que definirão se um novo surto de SPAM está ocorrendo. Você deve informar qual o número de mensagens por "Hora", "Minuto" ou "Dia" recebidos de uma mesma origem que foram categorizados como SPAM e a métrica baseada, “QUANTIDADE” ou “PERCENTUAL”. Se a métrica selecionada for “QUANTIDADE”, uma vez que seja alcançada o sistema irá negar novas conexões oriundas desta origem (IP ou domínio), conforme o "Tempo de Penalidade" que pode ser configurado por "Hora", "Minutos" ou "Dias". Se a métrica for “PERCENTUAL”, é necessário aguardar a primeira hora de análise dos e-mails da mesma origem, após a passagem da primeira hora, começará a contabilizar o “PERCENTUAL“ indicado, uma vez que seja alcançado, o sistema irá negar novas conexões oriundas desta origem (IP ou domínio), conforme o "Tempo de Penalidade" que pode ser configurado por "Hora", "Minutos" ou "Dias".
Vírus e Phishing	Informe quais são os parâmetros que definirão se um novo surto de VÍRUS/PHISHING está ocorrendo. Você deve informar qual o número de mensagens por "Hora", "Minuto" ou "Dia" recebidos de uma mesma origem que foram categorizados como Vírus/Phishing e a métrica baseada, “QUANTIDADE” ou “PERCENTUAL”. Se a métrica selecionada for “QUANTIDADE”, uma vez que seja alcançada o sistema irá negar novas conexões oriundas desta origem (IP ou domínio), conforme o "Tempo de Penalidade" que pode ser configurado por "Hora", "Minutos" ou "Dias".

	Se a métrica for “PERCENTUAL”, é necessário aguardar a primeira hora de análise dos e-mails da mesma origem, após a passagem da primeira hora, começará a contabilizar o “PERCENTUAL“ indicado, uma vez que seja alcançado, o sistema irá negar novas conexões oriundas desta origem (IP ou domínio), conforme o "Tempo de Penalidade" que pode ser configurado por "Hora", "Minutos" ou "Dias".
Harvest Attack	Informe quais são os parâmetros que definirão se um novo surto de Harvest Attack (ataque de dicionário)/DHA/DHAP está ocorrendo. Você deve informar qual o número de mensagens por "Hora", "Minuto" ou "Dia" recebidos de uma mesma origem que foram categorizados como Usuário Inexistente e a métrica baseada, “QUANTIDADE” ou “PERCENTUAL”. Se a métrica selecionada for “QUANTIDADE”, uma vez que seja alcançada o sistema irá negar novas conexões oriundas desta origem (IP ou domínio), conforme o "Tempo de Penalidade" que pode ser configurado por "Hora", "Minutos" ou "Dias". Se a métrica for “PERCENTUAL”, é necessário aguardar a primeira hora de análise dos e-mails da mesma origem, após a passagem da primeira hora, começará a contabilizar o “PERCENTUAL“ indicado, uma vez que seja alcançado, o sistema irá negar novas conexões oriundas desta origem (IP ou domínio), conforme o "Tempo de Penalidade" que pode ser configurado por "Hora", "Minutos" ou "Dias".

Reputação

O HSC MailInspector possui um sistema de reputação global baseado em consulta online na nuvem da HSC SmartDefender, um sistema de BigData com informações em tempo real sobre a reputação de diversos endereços IPs, já incluindo os sistemas DUL (Dynamically Assigned IP) e ETL (Emerging Threat List).

Configurações / **Controle de Conexão / Reputação**

Visão geral do Reputação

O HSC MailInspector possui um sistema de reputação global de 10 níveis de sensibilidade. As consultas são realizadas em tempo real na base global de inteligência do HSC SmartDefender.

É possível configurar limites em nível de MTA "SMTP" para controlar o recebimento de e-mails conforme o nível de reputação desejada.

A reputação obtida (GLOBAL REPUTATION), é efetuada a correlação com a reputação local do appliance (tendo como prioridade a reputação local), com isso, tem-se melhor acerto sobre a acuracidade de acordo com o perfil da empresa.

Definições de Opções - Reputação

Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição
Adicionar	Adiciona nova regra de reputação
Edita	Edita regra de reputação anteriormente criada
Remover	Remove regra de reputação

Definições de Opções - Configurações de Níveis de Reputação

Nesta tela é possível definir para cada nível de forma granular. Define o tipo de reputação que será feito o controle de conexão.

Opções	Definição
Excelente	O IP do emissor possui uma Excelente reputação e não há reportes sobre nenhum caso de Envio de SPAM ou ameaças nos últimos 30 dias. O Emissor possui configurado corretamente DNS Reverso, SPF, DKIM e DMARC.
Muito Bom	O IP do emissor possui uma Excelente reputação e não há reportes sobre nenhum caso de Envio de SPAM ou ameaças nos últimos 15 dias. O Emissor possui configurado corretamente DNS Reverso, SPF, DKIM e DMARC.
Bom	O IP do emissor possui uma Boa reputação e não há reportes sobre nenhum caso de Envio de SPAM ou ameaças nos últimos 7 dias. O Emissor possui configurado DNS Reverso e SPF, porém não faz uso de DKIM e/ou DMARC.

	O Emissor não está reportando em nenhuma das principais RBLs.
Razoável	O IP do emissor possui uma Razoável reputação, mas houve casos de envio de algumas mensagens classificadas como SPAM nos últimos 7 dias. O Emissor possui configurado DNS Reverso e SPF, porém não faz uso de DKIM e/ou DMARC. O Emissor não está reportando em nenhuma das principais RBLs.
Neutro	O IP do emissor ainda não possui volume de dados suficientes para uma classificação efetiva nos últimos 7 dias. Ele está em processo de monitoramento. O Emissor possui configurado DNS Reverso e SPF, porém não faz uso de DKIM e/ou DMARC. O Emissor não está reportando em nenhuma das principais RBLs.
Suspeito	O IP do emissor ainda não possui volume de dados suficientes para uma classificação efetiva nos últimos 7 dias. Ele está em processo de monitoramento. O Emissor possui configurado DNS Reverso porém não faz uso de DKIM e/ou DMARC e/ou SPF. O Emissor está reportado em pelo menos 1 das principais RBLs e/ou o Domínio do DNS Reverso IP não possui nenhuma
Fonte de SPAM	O IP do emissor enviou um volume considerado de e-mails considerados SPAM nos últimos 7 dias. O Emissor possui configurado DNS Reverso porém não faz uso de DKIM e/ou DMARC e/ou SPF. O Emissor está reportado em pelo menos 1 das principais RBLs e/ou o Domínio do DNS Reverso IP não possui nenhuma.
Spammer	O IP do emissor enviou um volume considerado de e-mails considerados SPAM nos últimos 15 dias, o seu IP já é considerado fonte de SPAMMER. O Emissor possui configurado DNS Reverso porém não faz uso de DKIM e/ou DMARC e/ou SPF. O Emissor está reportado em pelo menos 2 das principais RBLs e/ou o Domínio do DNS Reverso IP não possui nenhuma.
Fontes de Ataques	O IP do emissor enviou um volume considerado de e-mails considerados Maliciosos (Vírus, Phishing, Spoofing, Malwares e etc) nos últimos 7 dias. O Emissor possui configurado DNS Reverso porém não faz uso de DKIM e/ou DMARC e/ou SPF. O Emissor está reportado em pelo menos 1 das principais RBLs e/ou o Domínio do DNS Reverso IP não possui nenhuma.
Perigoso	O IP do emissor enviou um volume considerado de e-mails considerados Maliciosos (Vírus, Phishing, Spoofing, Malwares e etc) nos últimos 15 dias, o seu IP já é considerado uma fonte perigosa de ataques. O Emissor possui configurado DNS Reverso porém não faz uso de DKIM e/ou DMARC e/ou SPF. O Emissor está reportado em pelo menos 1 das principais RBLs e/ou o Domínio do DNS Reverso IP não possui nenhuma.

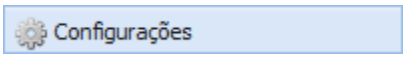
As métricas são baseadas na tabela de níveis de reputação, cruzando os dados com:

- Número máximo de Mensagens por Conexão;
- Número Máximo de Conexões Simultâneas por IP;
- Número máximo de Conexões Simultâneas Globais;

- Mensagens por um período de tempo "Horas e minutos"

Filas Personalizadas

Permite ao administrador criar filas de prioridades de e-mail, ou seja, priorizar determinadas filas de e-mails para melhor desempenho do sistema. Por exemplo criar uma fila específica para um ou mais domínios agregados.



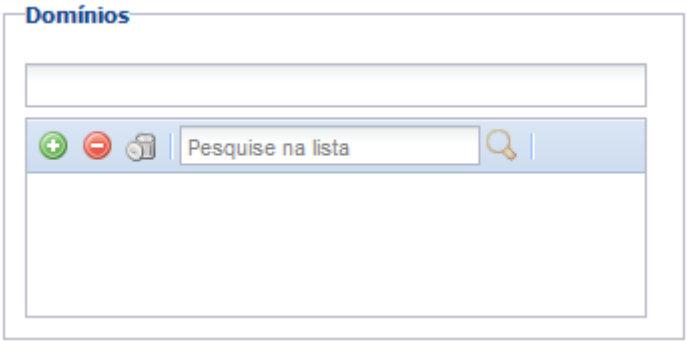
/ Controle de Conexão / Filas Personalizadas

Visão geral do Filas Personalizadas

O HSC MailInspector possui um sistema de controle de fila única e extremamente granular, com isso, é possível criar regras de filas de acordo com a necessidade da sua empresa. O MailInspector permite ao administrador definir para o número máximo de processamento a ser utilizado em paralelo para um grupo de filas ou para uma fila específica, conforme a necessidade de processamento e definição de prioridade da fila.

No controle da fila é possível criar uma fila baseada em:

- Um único domínio atendido;
- Múltiplos domínios atendidos;



Tela de seleção de domínios atendidos

Os controles podem ser:

- Por configurações:
  - Número de processos;
  - Timeout de conexão;
- Controle de Fluxo de Entrega:
  - Controle de tempo por usuário;
  - Controle de tempo por domínio;
  - Enviar X e-mails por X segundos;
  - Número máximo de destinatários por mensagem;
- Destinos inalcançáveis:
  - Número máximo de erros de envio;
  - Tempo de reinício de envio;

Definições de Opções – Botões

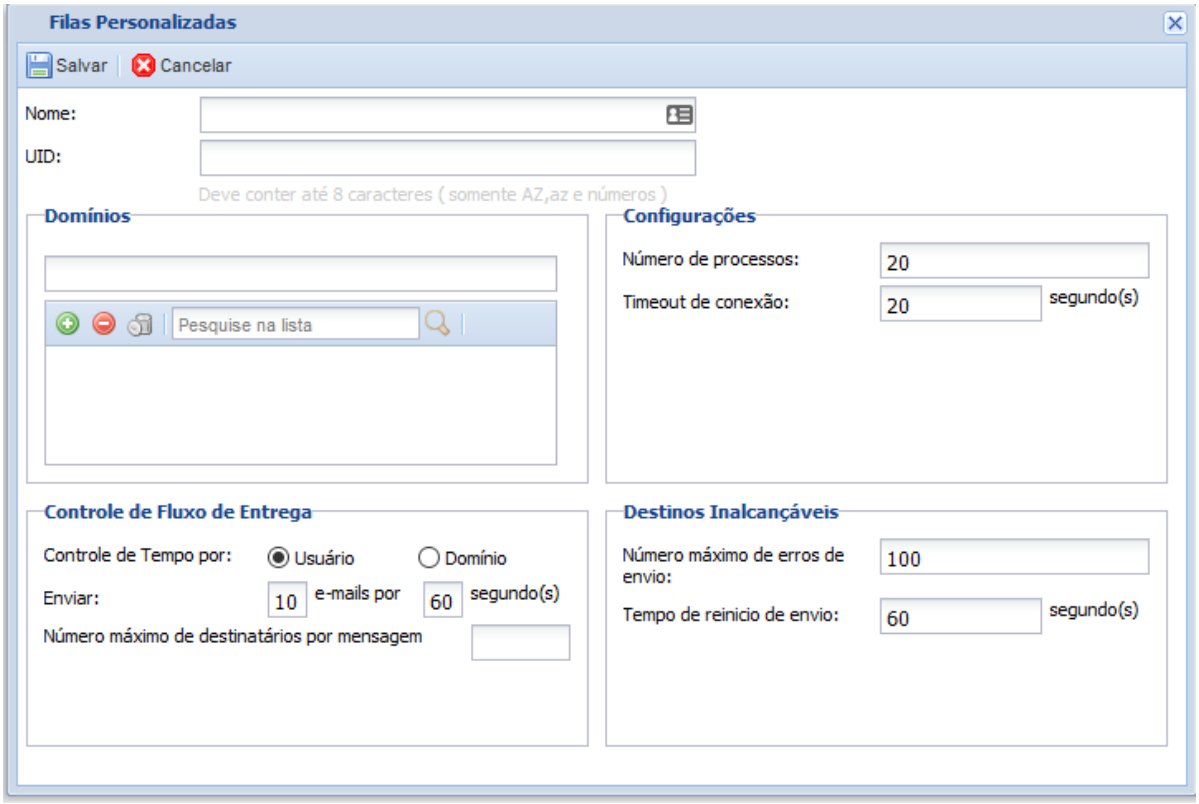
Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição
Adicionar	Adiciona nova regra de fila personalizada
Edita	Edita regra de fila personalizada anteriormente criada
Remover	Remove regra de fila personalizada

Definições de Opções – Filas Personalizadas

Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição
Nome	Insira o nome da regra da fila
UID	Insira uma identificação de até 8 caracteres para a fila criada (somente letras e números)
Domínios	Domínios atendidos por este controle
Número de Processos	Número máximo de processos simunltâneaos para esta fila
Timeout de conexão	Tempo para ser considerado timeout da conexão (em segundos)
Controle de Tempo por	Selecione se você deseja o controle seja por: • **Domínio:** Calcula o número de mensagens enviadas por um período para o mesmo domínio; • **Usuário:** Calcula o número de mensagens enviadas por um período para o mesmo usuário;
Enviar	Envia X e-mails por X segundos. Aqui é possível controlar o envio de e-mails por um determinado período, garantindo um controle de fluxo para envio desta fila. Para desabilitar o controle de fluxo, basta colocar 0 no valor informado, tornando nesta fila o envio de e-mails ilimitado pelo tempo indicado.
Número máximo de destinatários por mensagem	Permite que o administrador fixe um número máximo de destinatários por mensagem
Número máximo de erros de envio	Configure o número máximo de erros de envio
Tampo de reinício de envio	Quanto tempo ele fará nova tentativa de reenvio



Tela de configuração da fila personalizada de e-mails

Quarentena

A capacidade de armazenamento da quarentena é diretamente ligada a capacidade de disco (o HSC MailInspector pode endereçar discos superiores a 64TB), com isso, o MailInspector tem capacidade de armazenamento superior a 100 milhões de mensagens por mês e com armazenamento superior a 365 dias.

Dessa forma, quanto maior a área reservada para a quarentena, maior poderá será o tempo de armazenamento, dependendo unicamente de o administrador efetuar o cálculo de capacidade em relação ao tempo de armazenamento e capacidade de disco. O armazenamento da quarentena poderá ser local ou remoto, ou até mesmo via storage.

Por exemplo:

- Tempo de armazenamento por mês (TA);
- Tamanho médio de mensagem recebida (TM);
- Número de mensagens por mês (MM);

Capacidade Necessária de Disco = TA x TM x MM

No exemplo de 50 milhões de mensagens ao mês, com tamanho médio de 45kB e armazenamento de 120 dias.:

- Tampo de armazenamento (TA): 120 dias = 4 meses;
- Tamanho médio da mensagem (TM): 45kB
- Número de menagens por mês (MM): 50 milhões

Capacidade Necessária de Disco = 4 x 46080 x 50.000.000 = 9.216.000.000.000B = 8.3819TB

O MailInspector permite o uso de disco dinâmico em sistemas de appliances virtuais, dessa forma é possível aumentar dinamicamente o disco de armazenamento, sem necessidade de reinstalação de toda a solução.

Segurança de Quarentena

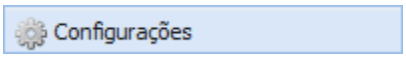
Configurações

O MailInspector possui vários tipos de quarentena, tais como:

- **Quarentena pré-definidas:** São as quarentenas padrões já pré-disponibilizados pelo MailInspector;
- **Quarentena Customizada:** Quarentena criado pelo administrador do sistema e com os filtros customizados;
- **Quarentena Temporária de Atualização de Anti-vírus:** Quarentena utilizado para manter os arquivos com suspeitas de vírus, até que a vacina seja lançada ou até que o prazo limite (tempo máximo de quarentena) seja encerrado;
- **Quarentena Temporária de Atualização de Extreme Update:** Quarentena utilizado para manter os arquivos com suspeitas de outras ameaças (que não seja vírus ou malwares), até que o Extreme Update atualize o sistema ou até que o prazo limite (tempo máximo de quarentena) seja encerrado;
- **Tempo de armazenamento de registro:** Tempo de armazenamento dos registros no Log de Evidência (Log de Filtragem dos e-mails);

Obs: Mesmo em quarentena temporária, os e-mails são continuamente verificados. Após recebimento de novas definições (tanto de vacinas, como de assinaturas de spam), os e-mails em quarentena temporária são novamente analisados, dessa forma podendo mudar a qualquer momento o resultado de sua análise.

Segue as configurações das quarentenas utilizadas pelo MailInspector.



/ **Quarentena / Configurações**

Visão geral das configurações da quarentena

O item Configurações da quarentena permite que o administrador gerencie os itens Tempo de Armazenamento e Controle da Quarentena.

O MailInspector possui quarentena por usuário, integrado e autenticado na base de diretório de usuários (Active Directory e EntraID do O365), possibilitando o usuário administrar sua própria quarentena, lista negada (block list/deny list) e lista permitida (allow list), remover mensagens ou liberá-las de acordo com a sua necessidade.

O controle de acesso a quarentena se dá através de autenticação automática pelo Active Directory/EntraID, dessa forma autentica-se o usuário e senha de forma automática, baseado no usuário e senha designados pelo login do MailInspector ou direto pelo tolken atribuído ao usuário (caso o acesso seja por ação efetuada na notificação de quarentena individual enviado a ele). Assim a quarentena somente é acessada para quem tem permissão para o processo, sendo que algumas quarentenas somente o administrador poderá ter permissão de acesso, conforme configurado por ele.

A quarentena possui integração direta no correio eletrônico do usuário *(Notificação de Quarentena* / DIGEST), permitindo a liberação diretamente no cliente de e-mail (através de envio periódico de relatório de resumo de quarentena individual) e via interface Web (HTTPS) através da console de gerenciamento.

Definições de Opções - Configurações

Estas informações descrevem as opções disponíveis nesta página.

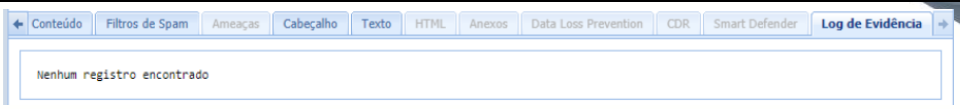
Opções	Definição
Salvar	Quando clicado, grava as configurações realizadas.

Definições de Opções - Controle da Quarentena

Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição
Ativar Armazenamento de E-mails na Quarentena	Escolha entre: • **Sim** - Indica que o armazenamento na quarentena está ativo. Este recurso permite que o HSC MailInspector armazene mensagens processadas na quarentena. • **Não** - Indica que o armazenamento na quarentena está desativado.

	Se este recurso for desativado, nenhuma mensagem será armazenada na quarentena, mesmo se as ações "Armazenar p/ Auditoria" ou "Colocar em Quarentena" estiverem definidas nos filtros de SPAM.
Algoritmo de Criptografia	Por padrão o HSC MailInspector guarda todas as mensagens da quarentena de forma criptografada, podendo o administrador escolher os seguintes algoritmos: • Blowfish; • Serpent; • Rijindael; • AES; • Twofish;
Tamanho da chave Criptográfica	Selecione o tamanho da chave a ser utilizada para criptografia: 128 Bits, 256 Bits e 448 Bits
Aguardar por este número de atualizações de assinaturas do AV	**Sim:** Ativa a quarentena temporária, baseado em atualização da vacina de antivírus. **Não:** Fica inativa a quarentena temporária.
Tempo mínimo de espera	Tempo mínimo de espera de nova atualização de vacinas em horas ou dias.
Tempo máximo de espera	Tempo máximo de espera de nova atualização de vacinas em horas ou dias.
Aguardar por este número de atualizações do Extreme Update	**Sim:** Ativa a quarentena temporária, baseado em atualização do extreme update (assinaturas de spam, etc). **Não:** Fica inativa a quarentena temporária.
Tempo mínimo de espera	Tempo mínimo de espera de atualização de extreme update em horas ou dias.
Tempo máximo de espera	Tempo máximo de espera de atualização de extreme update em horas ou dias.
Log de Evidência	Indica em dias o tempo de armazenamento dos registros apresentados em Log de Evidência (Log de filtragem dos e-mails) e tempo de rastreamento de cliques em links. Por padrão o tempo pré-definido é de 30 dias. RealTime > E-mails > Ações > Obter log de evidência Filtros de Conteúdo | Assinaturas | Ameaças | Cabeçalho | Texto | HTML | Anexos | Data Loss Prevention | CDR | Smart Defender | **Log de Evidência** Jun 16 11:43:08 mli01 MTA/smtpd[23032]: 07236A05807: client=mx-balancer.mlicloud.com[187.108.197.233] Jun 16 11:43:08 mli01 MTA/cleanup[25765]: 07236A05807: hold: header Received: from mx-balancer.mlicloud.com (mx-balancer.mlicloud.com [187.108.197.233])??(using TLSv1.2 with cipher ECDHE-RSA-AES256-GCM-SHA384 (256/256 bits))??(No client certificate requested)??by mx.g from mx-balancer.mlicloud.com[187.108.197.233]; from=<governanca.scf02446@samadhienvi08.advogadospprev.com.br> to=<contato@gtpn.com.br> proto=ESMTP helo=<mx-balancer.mlicloud.com> Jun 16 11:43:08 mli01 MTA/cleanup[25765]: 07236A05807: message-id=<20210616144042.F1ABF6E5D5@samadhienvi08.advogadospprev.com.br> Jun 16 11:43:08 mli01 opendkim[8829]: 07236A05807: no signature data Jun 16 11:43:11 mli01 HSC MailInspector[23022]: [MessageBatch::new] Added msg id 07236A05807.AB00C to batch Jun 16 11:43:11 mli01 HSC MailInspector[23022]: [ArchiveToFilesystem] Started on msg id 07236A05807.AB00C Jun 16 11:43:11 mli01 HSC MailInspector[23022]: [ArchiveToFilesystem] Executed in 0.000 second(s) on msg id 07236A05807.AB00C Jun 16 11:43:11 mli01 HSC MailInspector[23022]: [RejectMessages] Started on msg id 07236A05807.AB00C Jun 16 11:43:11 mli01 HSC MailInspector[23022]: [RejectMessages] Executed in 0.000 second(s) on msg id 07236A05807.AB00C Jun 16 11:43:11 mli01 HSC MailInspector[23022]: <A> tag found in message 07236A05807.AB00C from governanca.scf02446@samadhienvi08.advogadospprev.com.br Jun 16 11:43:11 mli01 HSC MailInspector[23022]: URL LINK tag found in message 07236A05807.AB00C from governanca.scf02446@samadhienvi08.advogadospprev.com.br Jun 16 11:43:11 mli01 HSC MailInspector[23022]: [CombineReports] Started on msg id 07236A05807.AB00C Jun 16 11:43:11 mli01 HSC MailInspector[23022]: [CombineReports] Executed in 0.000 second(s) on msg id 07236A05807.AB00C Jun 16 11:43:11 mli01 HSC MailInspector[23022]: [FindSilentAndNoisyInfections] Started on msg id 07236A05807.AB00C Jun 16 11:43:11 mli01 HSC MailInspector[23022]: [FindSilentAndNoisyInfections] Executed in 0.000 second(s) on msg id 07236A05807.AB00C *Tela de Log de Evidência de um e-mail* Se o e-mail estiver além do tempo configurado para a retenção de Log de Evidência (log de filtragem do e-mail), no lugar do log será apresentada a seguinte mensagem: **Nenhum registro encontrado**



Tela de Log de Evidência com registro além do tempo indicado

Definições de Opções - Controle Personalizado

Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição
Adicionar	Quando clicado, adiciona o controle personalizado ao Controle da Quarentena.
Cancelar	Quando clicado, cancela a ação.
De	Selecione o grupo pré-cadastrado de remetentes.
Para	Selecione o grupo pré-cadastrado de destinatários.
Ação	Escolha entre: • **Sim** - Indica que o armazenamento na quarentena será realizado, quando os remetentes e os destinatários pertencerem aos grupos selecionados. • **Não** - Indica que o armazenamento na quarentena não será realizado, quando os remetentes e os destinatários pertencerem aos grupos selecionados.

Definições de Opções - Tempo de Armazenamento

O tempo de armazenamento das quarentenas podem ser configuradas de três formas:

- Quantidade de mensagens na quarentena;
- Tempo de armazenamento (por hora, dias, semanas ou meses);
- Tamanho total de armazenamento;

Opções	Definição
Configuração de Armazenamento por Tipo	Permite ao administrador definir o modo de armazenamentos das mensagens nas Pastas pré-definidas das quarentenas do sistema. Estes armazenamentos podem ser definidos por **Período**: Horas, Dias, Semanas, Meses ou por **Quantidade de mensagens** ou por **Tamanho** em MB/GB ou ainda por tempo indeterminado para cada uma das quarentenas.* O tempo de armazenamento/quantidade de armazenamento pode ser modificado pelo administrador, de acordo com a sua necessidade e de acordo com a quantidade de disco disponível, não havendo um limite máximo de tempo ou quantidade de armazenamento das mensagens, somente dependendo de disponibilidade de espaço em disco. Dessa forma por exemplo é possível criar uma política de armazenamento de SPAM por 30 dias, enquanto a quarentena de DLP/Auditoria de 0 (zero) mensagens. *Pastas/Quarentenas Pré definidas:* • ATP (Ataques Persistentes); • Block List; • Bulk Mail (também chamado de GrayMail, ao qual é a quarentena de e-mails com características de propaganda, mas que não são necessariamente SPAM –

	pode ser e-mail de propaganda cadastrado e autorizado pelo usuário em sistemas de disparo); • Conteúdo Adulto; • Conteúdo Bloqueado; • Controle de Surto/Comportamento Anômalo; • DLP/Auditoria; • Fraude de E-mail/E-mail Impostor; • Outro Bloqueio; • Malware; • Phishing; • Provável SPAM; • SPAM; • Spoofing; • Tamanho Excedido; • Vírus; • Allow List; * Após estes períodos/quantidade definido pelo administrador, as mensagens serão automaticamente removidas da quarentena. A ordem de prioridade de exclusão (maior prioridade) serão sempre os mais antigos ao mais novo.
Mensagens na Quarentena	Indica a quantidade máxima de mensagens antes de começar a rotacionamento dos mesmos.
Registros no Banco de Dados	Quanto tempo os logs das quarentenas ficarão armazenados. Pode ser por **Período** em horas, dias, semanas, meses ou **mensagens** (quantidade de mensagens indicados no campo anterior). Os relatórios e eventuais consultas de e-mails "antigos" são baseados em tempo de armazenamento deste campo. O tempo de armazenamento/quantidade de armazenamento pode ser modificado pelo administrador, de acordo com a sua necessidade e de acordo com a quantidade de disco disponível, não havendo um limite máximo de tempo ou quantidade de armazenamento das mensagens, somente dependendo de disponibilidade de espaço em disco.
Período	Indicação de Tempo para armazenamento, podendo ser: • Horas; • Dias; • Semanas; • Meses; • Número de Mensagens; Obs: Caso precise usar como archiving e precise guardar por anos, basta colocar o período selecionado em meses, ex: 1 ano = 12 meses. **O MailInspector não obriga um mínimo, nem um máximo de período de retenção tanto de Registro no Banco de Dados, quanto nas mensagens na quarentena, mas por boa prática e de acordo com o Marco Civil, recomendamos que seja colocado no Registro no Banco de Dados período mínimo de 6 meses de retenção dos dados.**
Tamanho	Tamanho máximo de armazenamento (MB ou GB)

É possível definir o tempo de armazenamento, tamanho das áreas pré-definidas de quarentena do sistema ou ainda número máximo de e-mails quarentenados.

O administrador pode definir um limite por período (horas, dias, semanas ou meses), por tamanho de cada área de quarentena ou ainda quantidade máxima de e-mail na caixa de quarentena. Também é possível definir o tamanho de retenção dos logs de cada sistema. Os dados armazenados nos logs (remetente, destinatário, assunto, data, hora, tamanho, status do e-mail, IP de origem, política utilizada, anexos, links, entre outros dados) são os dados utilizados para a formação dos relatórios e consultas dos e-mails (Realtime > E-mails) e SandBox (RealTime > Segurança > SandBox).

Ao ultrapassar o tempo de armazenamento definido pelo administrador, o sistema apagará automaticamente os e-mails que "violaram" a regra de tempo de armazenamento. O mesmo vale para em relação ao tamanho de armazenamento, isto é, ao ultrapassar o limite de tamanho da caixa de quarentena, os e-mails mais antigos serão apagados, liberando o espeço de acordo com o tamanho definido pelo administrador e por ordem de prioridade.

No MailInspector ainda é possível configurar que a quarentena aceite um determinado número máximo de e-mails, isto é, por exemplo, se o administrador tiver definido 100 e-mails como número máximo de e-mails quarentenados, ao chegar o 101 e-mail, o primeiro e-mail será apagado.

É possível indicar tempo ilimitado de armazenamento, bem como ilimitada a quantidade de e-mails quarentenados. Para isso, na variável de dias de armazenamento, basta colocar 0 (zero).

Lista das áreas de quarentena padrões do sistema:

Nome da Quarentena	**Função da quarentena**
ATP "advanced threat protection"	E-mails classificados como ameaças do tipo: • Zero day; • Zero Hour; • Advanced Threat Protection;
Block List	E-mails classificados como Block List
BulkMail	E-mails classificados como BulkMail
Conteúdo Adulto	E-mails classificados como Conteúdo Adulto
Conteúdo Bloqueado	E-mails classificados como Conteúdo Bloqueado, tipo: Extensões, Mime-Types, etc..
Controle de Surto/ Comportamento Anômalo	E-mails classificados como Controle de Surto
DLP/Auditoria	E-mails classificados como DLP ou Auditoria, são os e-mails ou que tiveram regras de DLP aplicadas sobre ele ou e-mails considerados "bons" (e-mails que tiveram uma cópia armazenada para a auditoria).
Fraude de E-Mail/E-mail Impostor	E-mails classificados como E-mails classificados através de mecanismos antifraude, tipo: SPF, DKIM, DMARC, New Domains, Look-A-Like domains, etc.
Outro Bloqueio	E-mails classificados como outros tipos de bloqueios, tipo: Arquivos compactados com senha, ultrapassado número máximo de anexos no e-mail, Conteúdo HTML bloqueado, etc...
Malware	E-mails classificados como Malwares
Phishing	E-mails classificados como Phishing, tais como: URLs maliciosas, E-mails Maliciosos de phishing, etc...

Provável Spam	E-mails classificados como Provável SPAM. Por padrão o usuário final tem acesso a sua própria pasta de quarentena de Provável SPAM.
SPAM	E-mails classificados como SPAM. Por padrão o usuário final tem acesso a sua própria pasta de quarentena de SPAM.
Spoofing	E-mails classificados como Spoofing, tais como: Spoofing de domínio, Spoofing de E-mail, etc...
Tamanho Excedido	E-mails classificados como Tamanho Excedido. Também conhecido como quarentena de Anexos, pois para um e-mail ser classificado como tamanho excedido, por padrão é devido a soma do tamanho dos anexos contidos nele.
Vírus	E-mails classificados como Vírus e outras ameaças do gênero.
Allow List	E-mails classificados como Allow List

O Limite de tempo de armazenamento ou tamanho é define pela capacidade e espaço em disco disponibilizada para a Console de Administração do MailInspector, ou seja, não existe um limite definido basta o administrador disponibilizar um espaço adequado.

Caso o administrador necessite uma nova área "Pasta" de quarentena personalizada o mesmo pode ser feito usando as "Quarentenas Personalizadas".

Algumas áreas de quarentena não permitem que os usuários finais possam efetuar algumas ações tais como: Liberar mensagem, encaminhar e etc. Devido as melhores práticas de segurança. Estas áreas que não são autorizadas ao usuário tomar ações de liberação ou encaminhamento são:

- *Vírus;*
- *Phishing;*
- *Conteúdo Bloqueado;*
- *Outros Bloqueios;*
- *Fraude de E-mail;*
- *Malware;*
- *Tamanho Excedido;*
- *Spoofing;*

A "liberação" do e-mail se dará através da ação REPORTAR, ao qual enviará aviso ao administrador indicando o bloqueio indevido alertado pelo usuário. Dessa forma, o administrador poderá analisar o e-mail e tomar a decisão de liberação.

Tempo de Armazenamento por Tipo

	Mensagens na Quarentena	Registros no Banco de Dados	Período	Tamanho	
ATP:	30	90	Horas	0	GB
Blacklist:	9	90	Dias	0	GB
Bulk Mail:	30	90	Mensagen	0	GB
Conteúdo Adulto:	30	90	Horas	0	GB
Conteúdo Bloqueado:	9	90	Dias	0	GB
Controle de Surto/Comportamento Anômalo:	30	90	Dias	0	GB
DLP/Auditoria:	9	90	Dias	0	GB
Fraude de E-mail / E-mail Impostor:	30	90	Horas	0	GB
Outro Bloqueio:	9	90	Dias	0	GB
Malware:	30	90	Horas	0	GB
Phishing:	30	90	Horas	0	GB
Provável SPAM:	8	90	Dias	0	GB
SPAM:	9	90	Dias	0	GB
Spoofing:	30	90	Horas	0	GB
Tamanho Excedido:	9	90	Dias	0	GB
Vírus:	8	90	Dias	0	GB
Whitelist:	9	90	Dias	0	GB

Tela com indicação de pastas de armazenamento padrão, quantidade de mensagens armazenadas e/ou tempo limite de armazenamento e/ou tamanho máximo de armazenamento por pasta.

Precedência de Quarentena

O MailInspector trabalha com prioridades de quarentena, isto é, existem prioridades sobre quarentenas, por exemplo:

E-mail classificado como SPAM e ATP, o e-mail irá para a quarentena de ATP, para que não corra o risco de ser erroneamente liberado pelo usuário, pois a pasta SPAM é apresentado ao usuário, com possibilidade de liberação do e-mail quarentenado, já a pasta ATP, não tem a opção de liberação do e-mail por parte do usuário.

Em termos de prioridade de quarentena, quanto “pior” a ameaça encontrada, será de maior prioridade a quarentena indicada.

Seguindo a tabela indicada a seguir, se um e-mail for classificado como SPAM e Fraude de E-mail, ela será quarentenada como Fraude de e-mail.

PRECEDÊNCIA DA QUARENTENA (QUANTO MAIS ALTO NA TABELA, MAIOR A PRECEDÊNCIA)

Customizada

Use esta página para exibir, adicionar, editar ou excluir configurações da Quarentena Customizada.

Configurações / **Quarentena / Customizada**

Visão geral das configurações da quarentena customizada

O HSC MailInspector permite que o administrador crie sua própria quarentena customizada onde ele poderá informar: Tipo da quarentena, Tempo de armazenamento, tamanho do armazenamento e definir níveis de controle de acesso.

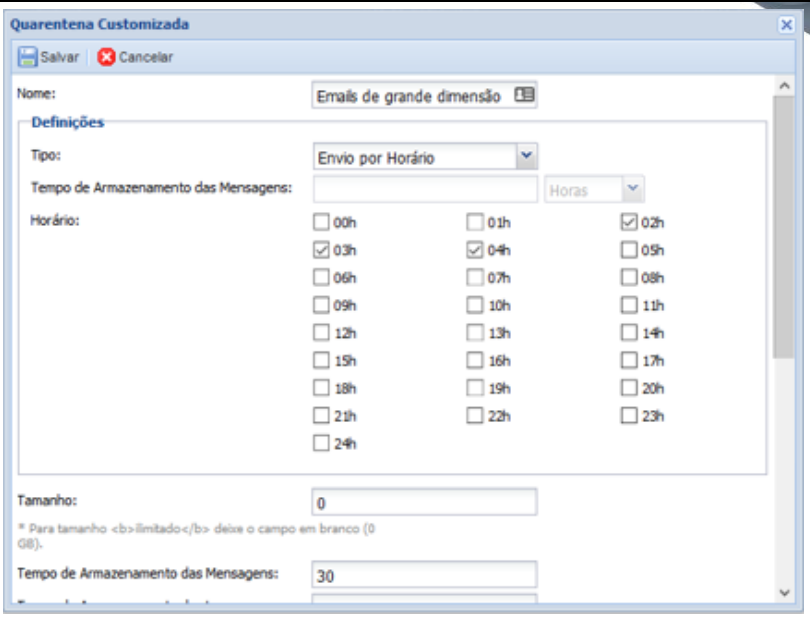
Com as quarentenas customizadas o administrador tem um maior poder de controle tento para definir um período ou tamanho ideal como definir quem terá acesso a uma determinada área de quarentena.

Na quarentena customizada do Tipo Envio por Horário é permitida criação de quarentena com Envio de e-mails por Horário específico, isto é, atrasar a entrega do e-mail e somente liberar em determinados horários (definido pelo administrador).
Os e-mails que serão "quarentenados" na quarentena por horário, são especificamente definidos pelo administrador através de regras de E-mail Compliance/DLP.

Definições de Opções - Adicionar

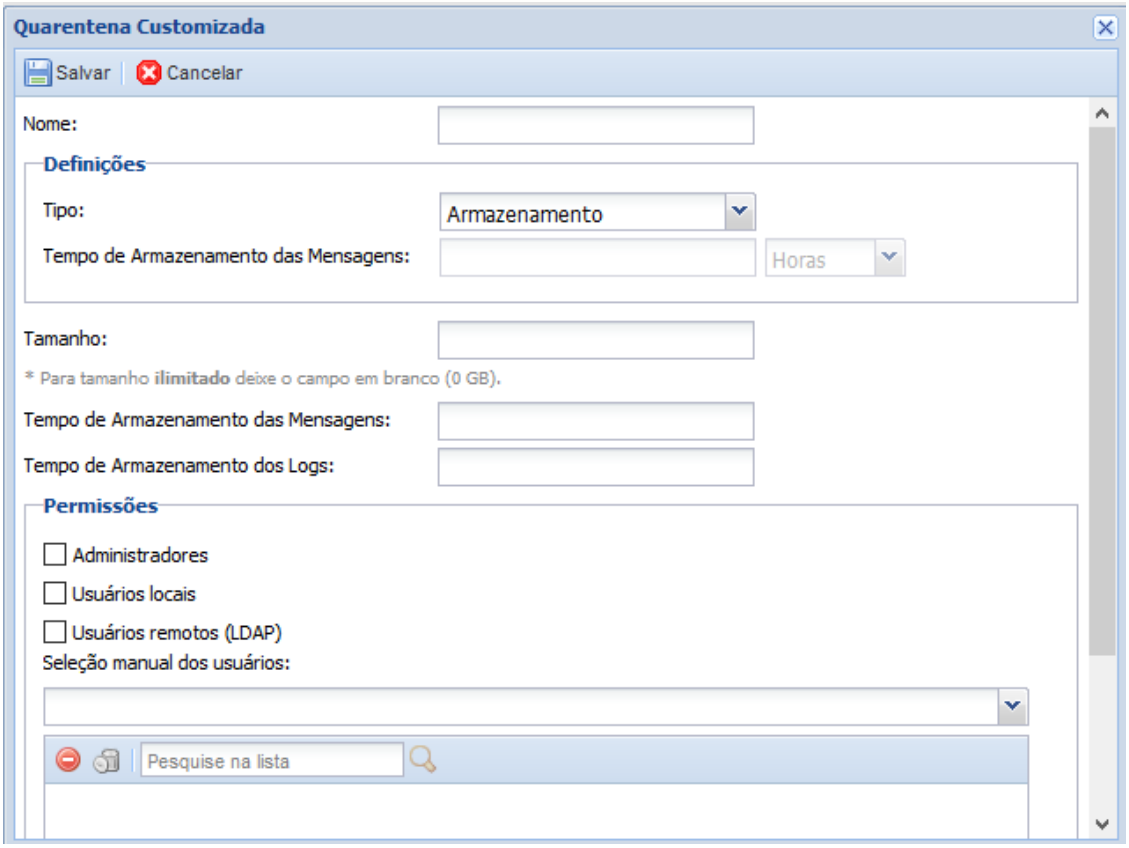
Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição
Nome	Define o nome de identificação da nova quarentena
Tipo	Selecione o Tipo da Quarentena **Armazenamento:** Serve para guardar uma cópia da mensagem conforme o tempo/tamanho de expiração definido **Atrasar Entrega:** As mensagens armazenadas neste tipo de quarentena terão sua entrega retardada, conforme configuração. **Envio por Horário:** Permite criar uma quarentena onde as mensagens quarentenadas são enviadas em um dia e horário específico. Esta quarentena é utilizada em conjunto com regras de quarentena customizada e/ou DLP.
Tempo de Armazenamento das Mensagens	Somente habilitado se for selecionado o tipo de quarentena Atrasar Entrega. Define o tempo de "delay" das mensagens classificadas para ele, podendo ser por horas ou dias.
Tamanho	Define o tamanho desta nova quarentena em MB ou GB. Se for configurado como 0 (zero), o tamanho será ilimitado.
Horário	Ativada somente quando o Tipo de Quarentena Customizada selecionada for Envio por Horário. Nesta opção o administrador deve selecionar o horário para a liberação do e-mail quarentenado.

	
Tempo de Armazenamento das Mensagens	Define quanto tempo (em dias) ficarão retidas as mensagens na quarentena. A mensagem ao ultrapassar esse período, será apagado.
Tempo de Armazenamento dos Logs	Define o tempo de armazenamento dos registros e logs desta quarentena (em dias).
Permissões	Nesta parte o administrador define quais são os usuários ou administradores que terão acesso a esta área de quarentena.
Período de Execução	Indique quando que a mensagem será liberada da quarentena.

Obs: *Uma vez criada uma nova área de quarentena o administrador deverá definir quais mensagens deverão ser enviadas para esta nova área, isto pode ser feito através de diversos critérios através da tela de "E-mail Compliance".*

Obs: *Uma nova área de quarentena terá precedência sobre as áreas de quarentena pré-definidas da ferramenta*



Criação de quarentana customizada

Filtros de Conteúdo

Configurações Gerais

Use esta página para exibir, adicionar, editar ou excluir configurações gerais do Filtro de Conteúdo.

Configurações **/ Filtros de Conteúdo / Configurações Gerais**

Visão geral das configurações gerais

Nesta sessão podemos configurar ativar e desativar filtros como: rejeitar mensagens, tamanho máximo das mensagens, mensagens criptografadas e mensagens descriptografadas. Podendo criar controles globais ou por grupos da ferramenta, controlando a entrada e saída de mensagens.

Definições de Opções - Configurações Gerais

Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição
Salvar	Quando clicado, grava as configurações realizadas.

Definições de Opções - Identificação

Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição
Nome do Servidor	Informe o nome F.Q.D.N. do ponto de acesso. Ex.: mx01.empresa.com.br. Recomendamos utilizar o mesmo nome do servidor informado nas "Configurações do MTA".
Nome da Empresa	Informe o nome da empresa.
Web Site	Informe o web site da empresa. Ex.: http://www.empresa.com.br.
Número Máximo de Processos de Filtragem	Informe a quantidade de processos de filtragem ativos no HSC MailInspector. Processos de filtragem são filas de processamentos paralelos que trabalham simultaneamente processando as mensagens contra todos os filtros da ferramenta. Esse campo está ligado diretamente ao **Número Máximo de Escaneamentos de Mensagens por Processo**. Todos os processamentos de mensagens se interrompidos não afetam a entrega das mensagens, uma vez que todo escaneamento é realizado em um ambiente separado e individual da fila final de entrada e saída de e-mails. Este valor pode ser modificado conforme a capacidade do hardware do servidor.

	Memória consumida pelos processos = ((num. máximo de processos de filtragem * 110MB) * num. máximo de escaneamentos de mensagens por processo * (tamanho máximo da mensagem *2)) + 4GB (reservado pelo macrosistema) Favor consultar o suporte antes de realizar qualquer alteração.
Timeout de Execução de Processamento de Mensagens	Define o tempo máximo que um JOB de escaneamento irá trabalhar em uma única mensagem.
Tempo Máximo de Cache de Escaneamento	Tempo em horas que o cache de arquivos já escaneados ficarão ativos para uso. Se o cache estiver ativo e um arquivo analisado casar com o cache, o resultado da análise anterior será reaproveitado, dessa forma, evita-se checagens constantes do mesmo arquivo.
Número Máximo de Escaneamentos de Mensagens por Processo	Define a quantidade de mensagens que cada processo irá processar (como os e-mails serão liberados por lote, somente quando o último e-mail tiver sido processado, aí sim o lote será liberado). Número máximo de Escaneamentos de Mensagens pro Processo tem que ser no máximo uns 10 (quanto menor melhor). É melhor ter mais número máximo de processos de filtragem e pouco número máximo de escaneamentos de mensagens por processo, de no máximo uns 2 ou 3. Favor consultar o suporte antes de realizar qualquer alteração.
Remetente das Notificações	Indica o remetente apresentado nas mensagens de bounce-mail emitidos pelo MailInspector.
Número Máximo de Tentativas de Filtragem	Indica o número de vezes que o MailInspector irá tentar analisar o e-mail, caso esse número seja superado, o e-mail automaticamente irá para a quarentena (Outros Bloqueios), impedindo que ele fique “eternamente” em processo de análise por looping.

Tela de Filtros de Conteúdo > Configurações Gerais.

Para uma configuração "padrão" de 10GB de memória RAM e 12 processadores na console de gerenciamento e 10GB de memória RAM e 10 processadores nos pontos de filtragem, a configuração é:

- Número máximo de Processos de Filtragem: 10
- TimeOut de Execução de Processamento de Mensagem: 640
- Número Máximo de Escaneamento de Mensagens por Processo: 30

Definições de Opções - Filtragem de E-mails

Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição
Ativar Filtragem de E-mails	Escolha entre: • **Sim** - Indica que o sistema de filtragem está ativo. Esta funcionalidade gerencia todos os recursos de filtragem. • **Não** - Indica que o sistema de filtragem está desativado. ⚠ Se este recurso for desativado, nenhuma filtragem será realizada. Todas as mensagens recebidas serão entregues para os usuários.
Adicionar	Cadastra uma nova regra de filtragem de e-mails. Quando clicado, abre a caixa de diálogo **Cadastro do Controle Personalizado**.
Editar	Edita as configurações de um registro existente. Quando clicado, abre a caixa de diálogo **Cadastro do Controle Personalizado**.
Remover	Quando clicado, exclui o registro selecionado.

Definições de Opções - Rejeitar Mensagens

Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição
Rejeitar Todas as Mensagens	Escolha entre: • **Sim** - Indica que a rejeição de mensagens está ativa. Este recurso permite que todas as mensagens processadas sejam rejeitadas. • **Não** - Indica que a rejeição de mensagens está desativada. ⚠ Se este recurso for ativado, nenhuma mensagem processada será entregue para os usuários.
Adicionar	Cadastra uma nova regra de rejeição de mensagens. Quando clicado, abre a caixa de diálogo **Cadastro do Controle Personalizado**.
Editar	Edita as configurações de um registro existente. Quando clicado, abre a caixa de diálogo **Cadastro do Controle Personalizado**.
Remover	Quando clicado, exclui o registro selecionado.

Definições de Opções - Tamanho Máximo das Mensagens

Configuração do tamanho máximo da mensagem. Importante salientar que é o tamanho da mensagem (em termos de cálculo, é geralmente 40% a maior em relação ao tamanho máximo do anexo), não é do tamanho máximo do anexo.

Opções	Definição
Tamanho Máximo de uma Mensagem	Permite que seja definido o tamanho máximo das mensagens que serão entregues para os usuários. Uma mensagem com o tamanho maior ao definido nesta opção, será bloqueada pelo sistema de filtragem, não sendo entregue ao usuário.
Adicionar	Cadastra uma nova regra de controle de tamanho máximo de mensagens. Quando clicado, abre a caixa de diálogo **Cadastro do Controle Personalizado**.
Editar	Edita as configurações de um registro existente. Quando clicado, abre a caixa de diálogo **Cadastro do Controle Personalizado**.
Remover	Quando clicado, exclui o registro selecionado.

Definições de Opções - Mensagens Criptografadas

Verifica se a mensagem está criptografada e verifica a chave de criptografia utilizada. O MailInspector trabalha com múltiplas cifras de criptografia.

O MailInspector possui suporte a todos algoritmos de criptografia usados pelos clientes de e-mail para protocolos S/MIME (Secure Multi-Purpose Internt Mail) e PGP (Pretty Good Privacy).

O MailInspector suporta múltiplos algoritmos de criptografia, dentre eles podemos citar alguns:

- DES (Data Encryption Standard);
- IDEA (International Data Encryption Algorithm);
- Blowfish;
- RC (Ron's Code ou Rivest Cipher);
- RSA (Rivest, Shamir and Adleman);
- DSA (Digital Signature Algorithm);
- AES (Advanced Encryption Standard);
- DHE (Diffie-Hellman);
- ADH (Anonymous Diffie-Hellman);

Com ou sem uso de verificação da integridade por MD5.
Com ou sem uso de verificação de assinatura digital por DSS (Digital Signature Standard).
Com ou sem uso de função de dispersão criptográfica SHA (Secure Hash Algorithm).
Com ou sem uso de cadeia de blocos (CBC - Cypher-Block Chaining).
Suporta qualquer tamanho de chave (32 bits, 64 bits, 128 bits, 192 bits, 256 bits, 512 bits, 1024 bits, 2048 bits e superiores).

Opções	Definição
Bloquear Mensagens Criptografadas	Escolha entre: • **Sim** - Indica que o bloqueio de mensagens criptografadas está ativo. Este recurso permite que todas as mensagens criptografadas sejam bloqueadas. • **Não** - Indica que o bloqueio de mensagens criptografadas não está ativo, permitindo o envio e recebimento de toda as mensagens criptografadas.

Adicionar	Cadastra uma nova regra de controle de mensagens criptografadas. Quando clicado, abre a caixa de diálogo **Cadastro do Controle Personalizado**.
Editar	Edita as configurações de um registro existente. Quando clicado, abre a caixa de diálogo **Cadastro do Controle Personalizado**.
Remover	Quando clicado, exclui o registro selecionado.

Definições de Opções - Mensagens Descriptografadas

Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição
Bloquear Mensagens Descriptografadas	Escolha entre: • **Sim** - Indica que o bloqueio de mensagens descriptografadas está ativo. Este recurso permite que todas as mensagens descriptografadas sejam bloqueadas. • **Não** - Indica que o bloqueio de mensagens descriptografadas está desativado.
Adicionar	Cadastra uma nova regra de controle de mensagens descriptografadas. Quando clicado, abre a caixa de diálogo **Cadastro do Controle Personalizado**.
Editar	Edita as configurações de um registro existente. Quando clicado, abre a caixa de diálogo **Cadastro do Controle Personalizado**.
Remover	Quando clicado, exclui o registro selecionado.

Definições de Opções – Configuração de Imagem Pornográfica

Permite ao administrador gerenciar todas as configurações de detecção de imagem pornográfica.

Opções	Definição
De	Ativa a detecção de imagem pornográfica respeitando a regra De (Origem).
Para	Ativa a detecção de imagem pornográfica respeitando a regra Para (Destino).
Percentual de probabilidade	Percentual definido pelo administrador para que a imagem passe a ser considerada pornográfica.
Ativar análise em documentos	**Sim:** Verifica imagens dentro de documentos. **Não:** Não verifica imagens dentro de documentos.
Tipo de documento a ser analisado	**TODOS:** Analisa todos os tipos de documentos. **Somente Imagem:** Analisa somente imagens (por exemplo: BMP, JPG, JPEG, TIFF, GIF, PNG, EPS, SVG, entre outros). **Documentos padrão Office:** Analisa imagens dentro de documentos padrão Office e afins (DOC, XLS, PPT, PDF, etc).
Tempo de varredura	Indica quantos segundos para ser considerado TimeOut de verificação.
Tamanho mínimo da imagem	Qual o tamanho mínimo da imagem para ser verificada.
Tamanho máximo da imagem	Qual o tamanho máximo da imagem para ser verificada.

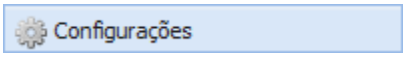
Definições de Opções - Cadastro do Controle Personalizado

Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição
Adicionar	Quando clicado, adiciona o controle personalizado.
Cancelar	Quando clicado, cancela a ação.
De	Selecione o grupo pré-cadastrado de remetentes.
Para	Selecione o grupo pré-cadastrado de destinatários.
Ação	Escolha entre: • **Sim** - Indica que a regra será aplicada, quando os remetentes e os destinatários pertencerem aos grupos selecionados. • **Não** - Indica que a regra não será aplicada, quando os remetentes e os destinatários pertencerem aos grupos selecionados. • **Tamanho** - Indica o tamanho máximo que uma mensagem pode ter para ser entregue, quando os remetentes e os destinatários pertencerem aos grupos selecionados.

Controle de Anexos

Use esta página para exibir, adicionar, editar ou excluir controles de anexos do Filtro de Conteúdo.



/ Filtros de Conteúdo / Controle de Anexos

Visão geral do controle de anexos

Nesta sessão podemos criar diversos filtros para controle de anexos das mensagens, tais como: controle de anexo por tamanho, controle anexo por extensão e/ou nome, controle por tipo MIME (fingerprint), controle de anexos compactados, tamanho máximo de anexos por e-mail, e por quantidade de anexos. Podendo criar controles globais ou por grupos da ferramenta (vide Cadastro), controlando entrada ou saída de mensagens.

Definições de Opções - Controle de Anexos

Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição
Salvar	Quando clicado, grava as configurações realizadas.

Definições de Opções - Anexos por Mensagem

Estas informações descrevem as opções disponíveis nesta página.

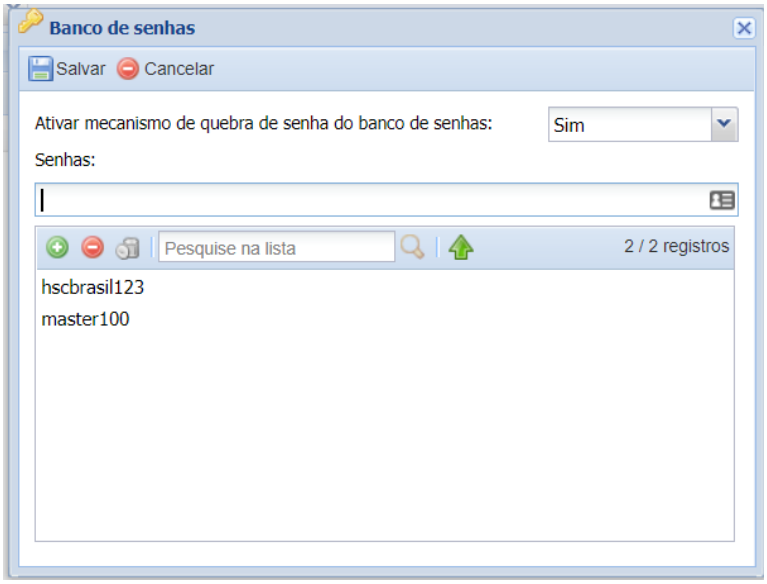
Opções	Definição
Número Máximo de Anexos por Mensagem	Permite que seja definido a quantidade máxima de arquivos anexos que uma mensagem pode conter.
Adicionar	Cadastra uma nova regra de controle de número máximo de arquivos anexos por mensagem. Quando clicado, abre a caixa de diálogo **Cadastro do Controle Personalizado**.
Editar	Edita as configurações de um registro existente. Quando clicado, abre a caixa de diálogo **Cadastro do Controle Personalizado**.
Remover	Quando clicado, exclui o registro selecionado.
Banco de Senhas	Ativa a funcionalidade de quebra de senha em anexos criptografados

Banco de Senhas

O Sistema de Banco de Senhas é responsável pela quebra da senha em arquivos criptografados.

Ao clicar nele, será aberto o Banco de senhas da sua empresa, sendo possível gerenciar as senhas cadastradas nela.

Para efetivar o uso do Sistema Banco de Senhas, o administrador deve ativar a funcionalidade em **Ativar mecanismo de quebra de senha no banco de senhas: Sim**



Tela de Cofre de Senhas

Serão as senhas que estiverem no Banco de Senhas que serão primeiramente testadas para descriptografar anexos com senha.

Importante salientar que o Banco de Senhas não é somente uma tabela contendo senhas utilizadas pela empresa. O administrador ao ativar o Banco de Senhas, ele estará automaticamente ativando as seguintes funcionalidades:

- Banco de Senhas: Tabela de senhas previamente cadastrado pelo administrador e alimentado automaticamente com novas senhas detectadas pelo sistema ou manualmente pelo administrador;
- Dicionário de senhas: Dicionário de palavras pré-concebidas que são historicamente mais utilizadas por usuários;
- Similaridade do Banco de Senhas: Variantes das senhas cadastradas no Banco de Senhas;
- Similaridade do Dicionário de senhas: Variantes de senhas do dicionário de senhas;
- Heurística de Senhas: Verifica no histórico do usuário senhas anteriormente utilizadas e/ou enviadas, bem como senhas encontradas no corpo de e-mails;

Mecanismo Heurístico de Análise de Senha

O MailInspector faz a verificação das senhas na seguinte sequência:

1. Banco de Senhas: Utiliza as senhas contidas no Banco de Senhas para tentar descriptografar o arquivo;
2. Dicionário de Senhas: Utiliza o dicionário de palavras que contém senhas comumente utilizadas;
3. Similaridade do Banco de Senhas: Combinações possíveis do Banco de Senhas;
4. Similaridade do Dicionário de Senhas: Combinações possíveis do Dicionário de Senhas;
5. Heurística de Senha: O MailInspector irá verificar de forma automática usando heurística no corpo do e-mail para busca por possíveis senhas, tomando como base todas possíveis senhas que já foram enviadas anteriormente para o usuário, dessa forma, engloba todo o histórico, bem como análise no corpo da mensagem, para verificar se possui alguma senha digitada, incluindo senhas “escondidas”.

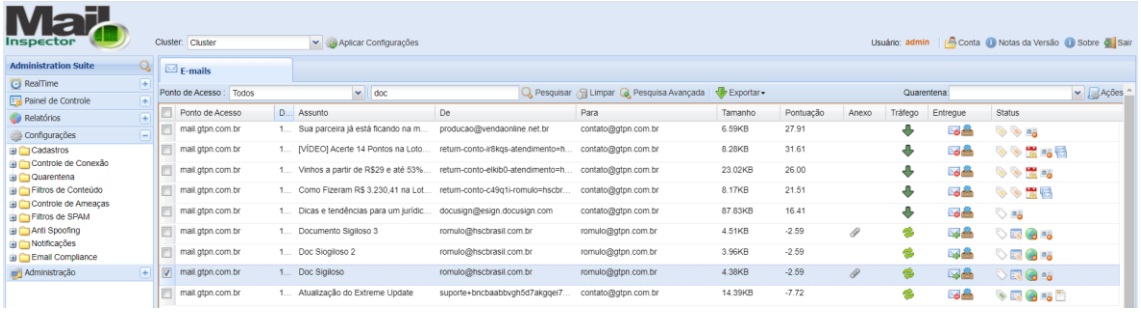
Ao utilizar todas as técnicas de combinação de senhas, o MailInspector faz o teste sobre o arquivo criptografado e em caso de sucesso na quebra da senha, o sistema adiciona automaticamente a senha no Banco de Senhas.

Uma vez quebrada a senha do anexo, o arquivo é processado de acordo com as configurações e analisado com anti-vírus/anti-malware, sistema de SandBox local e na nuvem da HSCBRASIL e tomada a ação devida.

Analisando senha em E-mail Específico

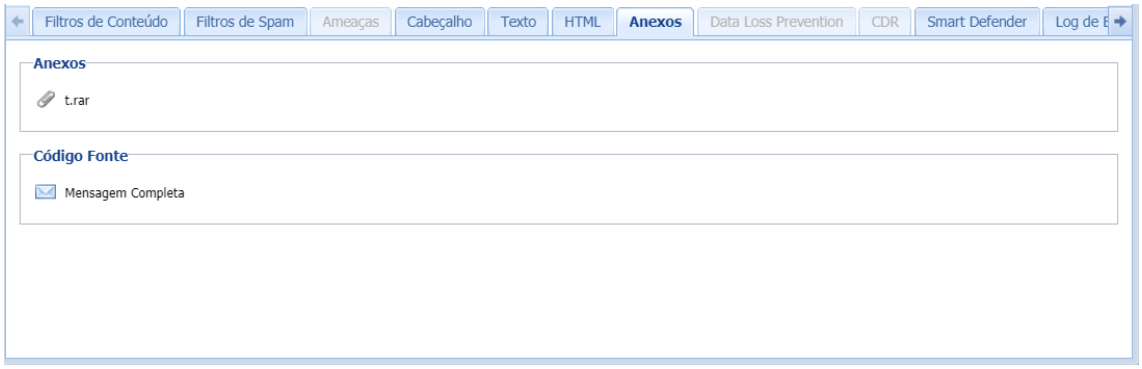
Também é possível efetuar a análise de senha de um e-mail específico com anexo criptografado.

O administrador seleciona o e-mail com anexo criptografado:

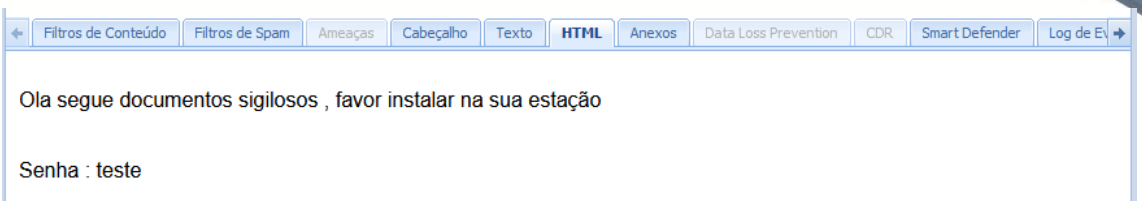


Dados do CORPO do e-mail selecionado:

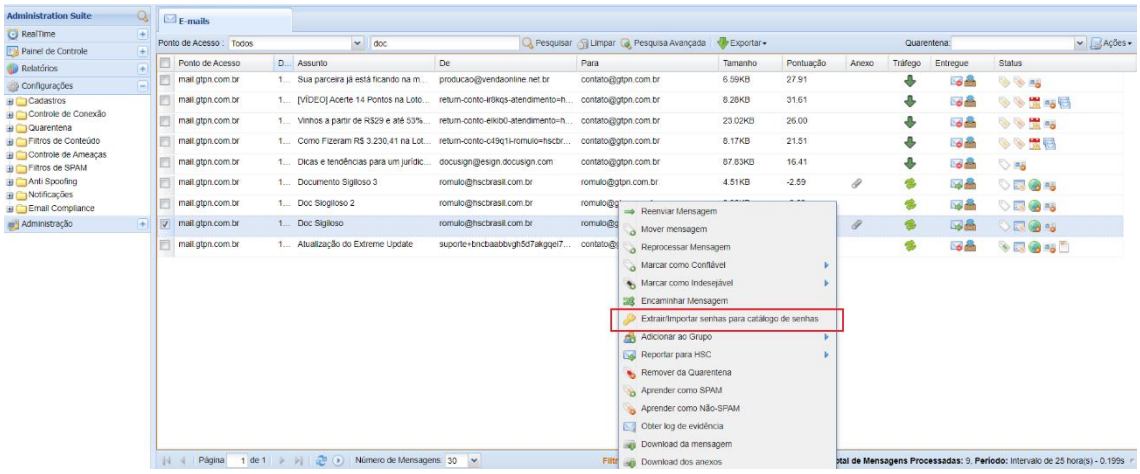
Como pode observar, ele possui um arquivo RAR com senha em anexo.

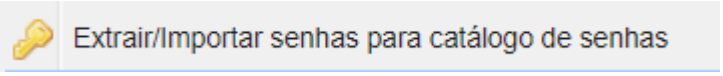


Abaixo o e-mail no formato HTML. Repare que a senha está no corpo do e-mail:

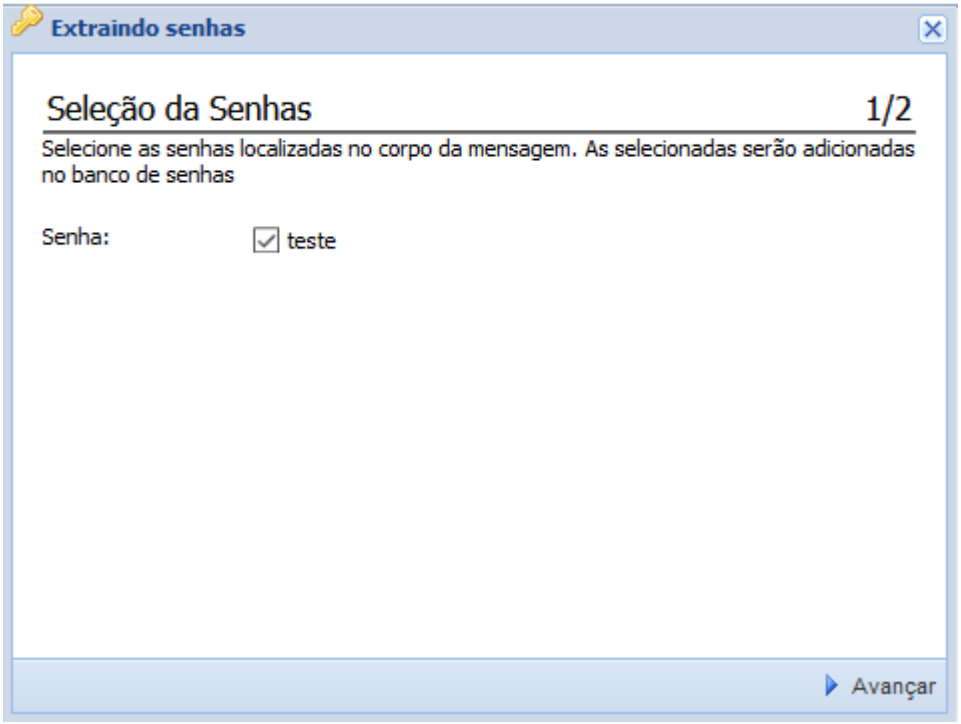


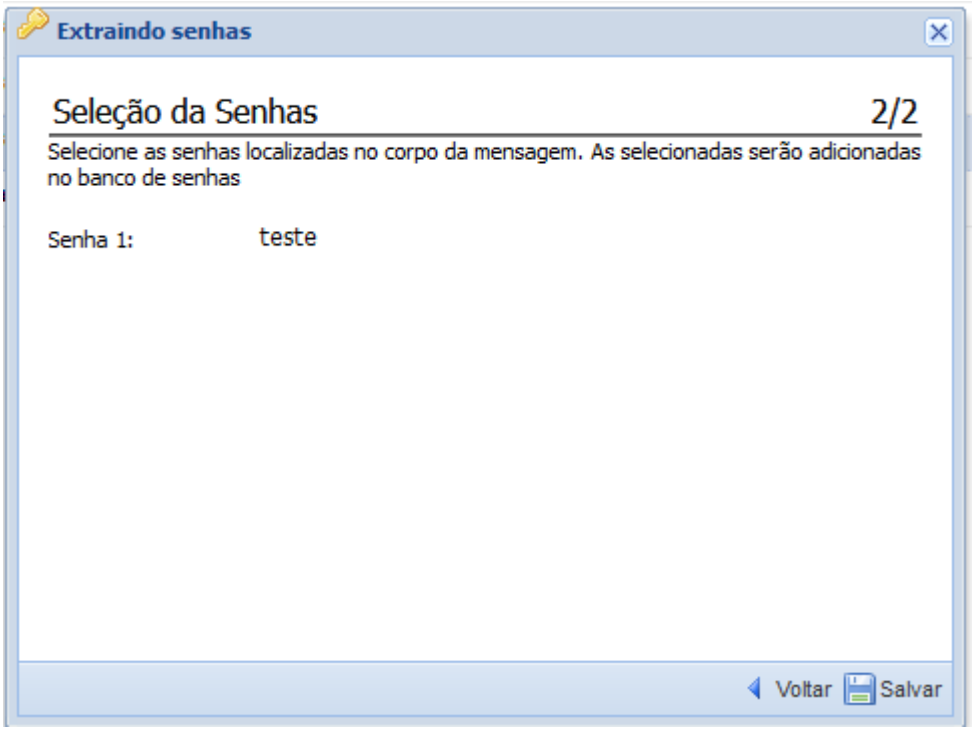
Para ativar o a extração manual da senha, basta clicar o botão direito do mouse sobre o e-mail e selecionar a opção **Exportar/Importar senhas para catálogo de senhas**

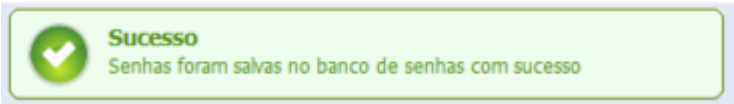


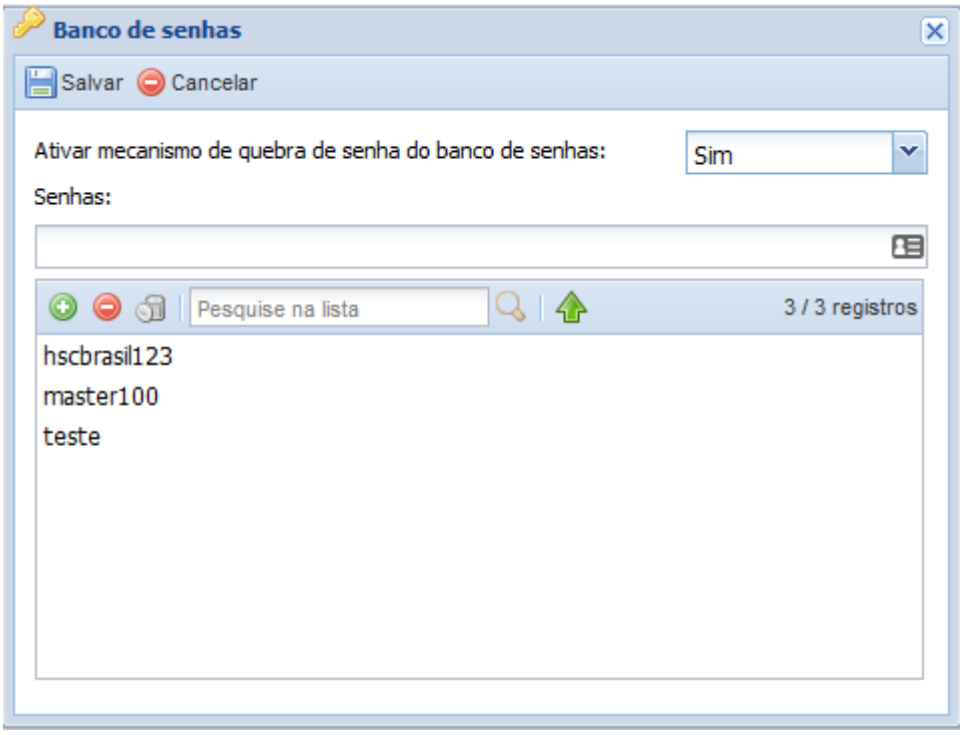


Ao selecionar a opção indicada, o sistema apresentará a senha extraída, permitindo ao administrador adicionar a senha no Banco de Senhas de forma manual, ou simplesmente visualizar a senha do arquivo criptografado. Caso o administrador opte por adicionar a senha ao Banco de Senhas, é só marcar a senha e mandar Salvar a senha no Banco de Senhas, conforme opção indicada a seguir:


Extraindo senhas
Seleção da Senhas
1/2
Selecione as senhas localizadas no corpo da mensagem. As selecionadas serão adicionadas no banco de senhas
Senha:
teste
Avançar


Extraindo senhas
Seleção da Senhas
2/2
Selecione as senhas localizadas no corpo da mensagem. As selecionadas serão adicionadas no banco de senhas
Senha 1:
teste
Voltar
Salvar


Sucesso
Senhas foram salvas no banco de senhas com sucesso



Definições de Opções - Tamanho do Anexo

Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição
Tamanho Máximo de Anexos	Permite que seja definido o tamanho total dos arquivos anexos em uma única mensagem. Uma mensagem que contenha arquivos anexos com o tamanho total maior que o definido nesta opção, será bloqueada pelo sistema de filtragem, não sendo entregue ao usuário.
Adicionar	Cadastra uma nova regra de controle de tamanho total de arquivos anexos. Quando clicado, abre a caixa de diálogo **Cadastro do Controle Personalizado**.
Editar	Edita as configurações de um registro existente. Quando clicado, abre a caixa de diálogo **Cadastro do Controle Personalizado**.
Remover	Quando clicado, exclui o registro selecionado.

Definições de Opções - Anexos Compactados

Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição
Habilitar Filtragem nos Anexos Compactados	Escolha entre:

	• **Sim** - Indica que a filtragem de arquivos anexos compactados está ativa. Este recurso permite que os conteúdos dos arquivos anexos compactados sejam analisados por: ○ Controle de Extensões; ○ Antivírus (Higienização e Bloqueio); ○ DLP, etc. • **Não** - Indica que a filtragem de arquivos anexos compactados está desativada. Anexos Compactados com senha também podem ser verificados pela análise de Extensões, ou seja, mesmo um anexo compactado com senha poder ser bloqueado caso nele contenha um arquivo .EXE e a regra de filtragem de extensões esteja bloqueando .EXE
Profundidade Máxima de Descompactação	Permite que seja definido a profundidade máxima de diretórios que serão analisadas em um arquivo anexo compactado. Permite analisar anexos com até 500 níveis de compactação, dessa forma impondo um limite máximo de níveis de compactação, barrando ataques que usem recursividade de compactação.
Tamanho máximo do anexo compactado	Indicação do tamanho máximo de arquivos compactados (antes da descompactação) anexados nos e-mails, aceitos pelo MailInspector.

Definições de Opções - Anexos Compactados com Senha

O sistema de proteção a e-mails MailInspector, possui múltiplas formas de tratar e-mail com anexo compactado com senha:

1. Controle de anexos compactados com senha;
2. Sistema de análise sobre arquivos CONTIDOS no arquivo compactado com senha;
3. Mecanismo Heurístico de Análise de Senha;

Para fins de referência, o MailInspector considera como arquivo compactado, arquivos que passaram pelos seguintes sistemas de compactação:

• ZIP	• RAR	• CAB	• ACE	• ARJ	• BH	• HA
• JAR	• PAK	• LHA	• PKZIP	• BZIP	• GZIP	• ZOO
• 7Z	• TZH	• TGZ	• TAR	• BZ2	• BZIP2	

O sistema de detecção de conteúdo em anexos, consegue verificar arquivos contidos dentro de anexos compactados com senha, dessa forma já impedindo passagem de arquivos perigosos (bloqueando o e-mail ou removendo o anexo), tais como arquivos executáveis (.EXE, .LNK, .SRC, etc) dentro de ZIP's, RAR, 7Z, entre os outros modelos de compactação (já mencionados anteriormente). Para esse processo o MailInspector faz nativamente, sem necessidade de dicionário de senhas ou heurística, dessa forma bloqueando conteúdos indesejados e/ou arquivos possivelmente perigosos.

Quanto as cifras utilizadas, é possível detecção dos anexos compactados com senha (criptografados), cujas cifras são entre eles:

- DES (Data Encryption Standard);
- IDEA (International Data Encryption Algorithm);
- Blowfish;
- RC (Ron's Code ou Rivest Cipher);
- RSA (Rivest, Shamir and Adleman);

- DSA (Digital Signature Algorithm);
- AES (Advanced Encryption Standard);
- DHE (Diffie-Hellman);
- ADH (Anonymous Diffie-Hellman);

Com ou sem uso de verificação da integridade por MD5.
Com ou sem uso de verificação de assinatura digital por DSS (Digital Signature Standard).
Com ou sem uso de função de dispersão criptográfica SHA (Secure Hash Algorithm).
Com ou sem uso de cadeia de blocos (CBC – Cypher Block Chaining).
Suporta qualquer tamanho de chave (32 bits, 64 bits, 128 bits, 192 bits, 256 bits, 512 bits, 1024 bits, 2048 bits e superiores).

Caso o arquivo não esteja compactado, mas com senha, o processo de detecção e eventual bloqueio é efetuado através do módulo **DLP**, onde pode ser detectado e aplicado a regra conforme necessidade do administrador. As formas de detecção de arquivo sem estar compactado, mas criptografado com senha são:

- **Heurística:** Aplicada sobre diversos arquivos com senha, tais como PDF com senha, DOC com senha, XLS com senha, todos os documentos padrão Office com senha, entre outros;
- **Mime-Type:** Verifica-se através do real tipo de arquivo;
- **Extensão:** Verifica-se através de extensões pré cadastradas no sistema;

Para maiores informações sobre detecção e bloqueio de arquivos não compactados com senha, veja em ***Definições de Opções – Adicionar/Editar Regras de Compliance - Anexos***

Opções	Definição
Permitir Anexos Compactados com Senha	Escolha entre: • **Sim** - Indica que o recurso está ativo. Este recurso permite que arquivos anexos compactados com senha sejam recebidos pelos usuários. • **Não** - Indica que não permitirá passagem de arquivos compactados com senha, colocando o e-mail em quarentena.
Adicionar	Cadastra uma nova regra de controle de mensagens com anexos compactados com senha. Quando clicado, abre a caixa de diálogo **Cadastro do Controle Personalizado**.
Editar	Edita as configurações de um registro existente. Quando clicado, abre a caixa de diálogo **Cadastro do Controle Personalizado**.
Remover	Quando clicado, exclui o registro selecionado.

Definições de Opções - Extensões Permitidas

Permite o administrador efetuar controle sobre os anexos permitidos. Os tipos de anexos permitidos podem ser cadastrados em Configurações > Cadastros > Anexos.

Opções	Definição
Permitir Anexos com Extensões	Escolha entre: • **Nenhum** - Indica que o recurso está desativado. • **Grupo de Extensões** - Indica que as mensagens que contiverem anexos com extensões do grupo de extensões selecionado não serão bloqueadas pela filtragem de anexos. O Anexo é analisado conforme a expressão regular criada no cadastro de "Anexos" e casa com o nome do anexo completo e não somente com a

	extensão. Ou seja, é possível criar expressões que casem com a extensão do arquivo, nome completo, nome parcial, caracteres coringas, etc.
Adicionar	Cadastra uma nova regra de controle de extensões permitidas. Quando clicado, abre a caixa de diálogo **Cadastro do Controle Personalizado**.
Editar	Edita as configurações de um registro existente. Quando clicado, abre a caixa de diálogo **Cadastro do Controle Personalizado**.
Remover	Quando clicado, exclui o registro selecionado.

Definições de Opções - Extensões Bloqueadas

Permite o administrador efetuar controle sobre os anexos bloqueados. Os tipos de anexos bloqueados podem ser cadastrados em Configurações > Cadastros > Anexos.

Opções	Definição
Bloquear anexos com extensões	Escolha entre: • **Nenhum** - Indica que o recurso está desativado. • **Grupo de Extensões** - Indica que as mensagens que contiverem anexos com extensões do grupo de extensões selecionado serão bloqueadas pela filtragem de anexos, O Anexo é analisado conforme a expressão regular criada no cadastro de "Anexos" e casa com o nome do anexo completo e não somente com a extensão. Ou seja, é possível criar expressões que casem com a extensão do arquivo, nome completo, nome parcial, caracteres coringas, etc.
Ação	Selecione uma ação para a regra: • Bloquear Mensagem: Bloqueia a entrega do e-mail; • Remover Anexo: Remove o anexo e prossegue com a entrega do e-mail, mas sem o anexo; • Descartar: Descarta a mensagem; Em caso de Bloqueio ou Remoção de Anexo é possível configurar em "Notificação de Mensagens" se o Remetente e/ou destinatário devem ser notificados, além de poder modificar o assunto do e-mail. No caso de Bloqueio da Mensagem, é possível incluí-lo em uma quarentena customizada pelo administrador.
Adicionar	Cadastra uma nova regra de controle de extensões bloqueadas. Quando clicado, abre a caixa de diálogo **Cadastro do Controle Personalizado**.
Editar	Edita as configurações de um registro existente. Quando clicado, abre a caixa de diálogo **Cadastro do Controle Personalizado**.
Remover	Quando clicado, exclui o registro selecionado.

Definições de Opções - Mime-Types Permitidos

Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição

Permitir Mime-Types	Escolha entre: • **Nenhum** - Indica que o recurso está desativado. • **Grupo de Mime-types** - Indica que as mensagens que contiverem anexos com mime-types do grupo de mime-type selecionado não serão bloqueadas pela filtragem de anexos.
Adicionar	Cadastra uma nova regra de controle de mime-types permitidos. Quando clicado, abre a caixa de diálogo **Cadastro do Controle Personalizado**.
Editar	Edita as configurações de um registro existente. Quando clicado, abre a caixa de diálogo **Cadastro do Controle Personalizado**.
Remover	Quando clicado, exclui o registro selecionado.

Definições de Opções - Mime-Types Bloqueados

Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição
Bloquear Mime-Types	Escolha entre: • **Nenhum** - Indica que o recurso está desativado. • **Grupo de Mime-types** - Indica que as mensagens que contiverem anexos com mime-types do grupo de mime-type selecionado serão bloqueadas pela filtragem de anexos.
Adicionar	Cadastra uma nova regra de controle de mime-types bloqueados. Quando clicado, abre a caixa de diálogo **Cadastro do Controle Personalizado**.
Editar	Edita as configurações de um registro existente. Quando clicado, abre a caixa de diálogo **Cadastro do Controle Personalizado**.
Remover	Quando clicado, exclui o registro selecionado.

Definições de Opções - Cadastro do Controle Personalizado

Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição
Adicionar	Quando clicado, adiciona o controle personalizado.
Cancelar	Quando clicado, cancela a ação.
De	Selecione o grupo pré-cadastrado de remetentes.
Para	Selecione o grupo pré-cadastrado de destinatários.
Ação	Escolha entre: • **Sim** - Indica que a regra será aplicada, quando os remetentes e os destinatários pertencerem aos grupos selecionados. • **Não** - Indica que a regra não será aplicada, quando os remetentes e os destinatários pertencerem aos grupos selecionados.

	• **Máximo de Anexos** - Indica que a regra será aplicada quando a quantidade máxima de arquivos anexos que uma mensagem pode conter, quando os remetentes e os destinatários pertencerem aos grupos selecionados. • **Tamanho Máximo** - Indica que a regra será aplicada quando o tamanho total dos arquivos anexos que uma única mensagem pode conter, quando os remetentes e os destinatários pertencerem aos grupos selecionados. • **Extensões Permitidas** - Indica que a regra será aplicada quando o grupo de extensões permitido em anexos de uma mensagem, quando os remetentes e os destinatários pertencerem aos grupos selecionados. • **Extensões Bloqueadas** - Indica que a regra será aplicada quando o grupo de extensões não permitido em anexos de uma mensagem, quando os remetentes e os destinatários pertencerem aos grupos selecionados. • **Mime-types Permitidos** - Indica que a regra será aplicada quando o grupo de mime-types permitido em anexos de uma mensagem, quando os remetentes e os destinatários pertencerem aos grupos selecionados. • **Mime-types Bloqueados** - Indica que a regra será aplicada quando o grupo de mime-types não permitido em anexos de uma mensagem, quando os remetentes e os destinatários pertencerem aos grupos selecionados.

Compactação de Anexos

Use esta página para exibir, adicionar, editar ou excluir controles de compactação de anexos do Filtro de Conteúdo.

Configurações **/ Filtros de Conteúdo / Compactação de Anexos**

Visão geral da compactação de anexos

A Compactação de Anexos permite automatizar a compactação dos anexos de uma mensagem, criando um único arquivo compactado em formato universal, e sem a necessidade de interação do usuário.

Este recurso pode reduzir em até 60% o consumo de banda de internet.

Se uma mensagem é enviada contendo anexos que somados tenham mais de 20MB, o sistema pode ser configurado para, automaticamente, comprimir todos os anexos, diminuindo assim o tamanho total da mensagem. Podendo criar controles globais ou por grupos da ferramenta, controlando entrada ou saída dos e-mails.

Definições de Opções - Compactação de Anexo

Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição
Salvar	Quando clicado, grava as configurações realizadas.

Definições de Opções - Compactar Anexos

Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição
Ativar Compactação Automática de Anexos	Escolha entre: • **Sim** - Indica que a compactação automática de anexos está ativa. Este recurso permite que arquivos anexos de uma mensagem sejam compactados automaticamente em um único arquivo. • **Não** - Indica que a compactação automática de anexos está desativada.
Nome do Arquivo Anexo Compactado	Permite que seja definido o nome padrão para o arquivo compactado que será gerado.
Adicionar	Cadastra uma nova regra de compactação automática de arquivos anexos. Quando clicado, abre a caixa de diálogo **Cadastro do Controle Personalizado**.
Editar	Edita as configurações de um registro existente. Quando clicado, abre a caixa de diálogo **Cadastro do Controle Personalizado**.
Remover	Quando clicado, exclui o registro selecionado.

Definições de Opções - Tamanho Mínimo para Compactar

Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição
Tamanho Mínimo dos Anexos	Permite que seja definido o tamanho mínimo dos anexos em uma única mensagem para que a compactação automática seja realizada.
Adicionar	Cadastra uma nova regra de controle de tamanho mínimo para compactação de arquivos anexos. Quando clicado, abre a caixa de diálogo **Cadastro do Controle Personalizado**.
Editar	Edita as configurações de um registro existente. Quando clicado, abre a caixa de diálogo **Cadastro do Controle Personalizado**.
Remover	Quando clicado, exclui o registro selecionado.

Definições de Opções - Extensões que Não Devem ser Compactadas

Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição
Extensões que não Devem Ser Compactadas	Escolha entre: • **Nenhum** - Indica que o recurso está desativado. • **Grupo de Extensões** - Indica que as mensagens que contiverem arquivos anexos, com extensões do grupo de extensões selecionado, não serão compactados automaticamente.
Adicionar	Cadastra uma nova regra de controle de extensões que não devem ser compactadas. Quando clicado, abre a caixa de diálogo **Cadastro do Controle Personalizado**.
Editar	Edita as configurações de um registro existente. Quando clicado, abre a caixa de diálogo **Cadastro do Controle Personalizado**.
Remover	Quando clicado, exclui o registro selecionado.

Definições de Opções - Cadastro do Controle Personalizado

Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição
Adicionar	Quando clicado, adiciona o controle personalizado.
Cancelar	Quando clicado, cancela a ação.
De	Selecione o grupo pré-cadastrado de remetentes.
Para	Selecione o grupo pré-cadastrado de destinatários.
Ação	Escolha entre: • **Sim** - Indica que a regra será aplicada, quando os remetentes e os destinatários pertencerem aos grupos selecionados. • **Não** - Indica que a regra não será aplicada, quando os remetentes e os destinatários pertencerem aos grupos selecionados.

	• **Tamanho Mínimo** - Indica que a regra será aplicada quando o tamanho mínimo dos anexos em uma única mensagem para que a compactação automática seja realizada, quando os remetentes e os destinatários pertencerem aos grupos selecionados. • **Extensões Não Compactadas** - Indica que a regra será aplicada quando as mensagens que contiverem arquivos anexos, com extensões do grupo de extensões selecionado, quando os remetentes e os destinatários pertencerem aos grupos selecionados.

Controle de Ameaças

Antivírus

É responsável pela detecção por assinaturas e heurística, bloqueando ameaças do tipo:

- Ameaças em pastas públicas (linkados em e-mails);
- Vírus, com múltiplas variantes;
- Vírus Polimórficos;
- Worms;
- Phishing;
- Spyware;
- Ransomware;
- Trojan (Cavalo de Tróia);
- Jokers;
- Rootkits;
- Riskware;
- Stealth Attacks/Fileless Attack;
- Códigos maliciosos escondidos com técnicas de esteganografia;
- Sistemas de alteração de arquivo Host;
- Ataques de man-in-the-middle;
- Session Hijacking/Cookie Hijacking;
- Ferramentas de hacking;
- Ferramentas de detecção de senhas, por múltiplos métodos, tais como força bruta;
- Adwares;
- Malwares (mesmo empacotados / packed malwares);
- Keyloggers;
- Dialers;
- APT;
- Diversas outras ameaças.

Configurações **/ Controle de Ameaças / Antivírus**

Visão geral do antivírus

O Antivírus verifica todas as mensagens contra vírus, spywares, phishing, trojans e outros tipos de malwares e ameaças. O módulo de Antivírus do **MailInspector utiliza como engine principal o HSC SmartDefender**, tecnologia proprietária da HSCBRASIL desenvolvida para oferecer análise antivírus, antimalware, detecção comportamental, proteção contra todos os tipos de ameaças, até mesmo ameaças do tipo Zero-Day e avaliação avançada de reputação. Toda a lógica de inspeção, correlação e decisão é nativa do produto, garantindo integração total com o Secure E-mail Gateway e alto desempenho na detecção de ameaças.

O mecanismo possui múltiplas engines de verificações a fim de permitir uma maior segurança. Possui mecanismo de análise por assinatura, análise heurística, fingerprint, URLs, cabeçalho da mensagem (header), corpo da mensagem (body), anexos entre outros, combatendo ataques de Vírus Outbreaks e Zero-Hour (Online Detect). O sistema de detecção de ameaças da HSCBRASIL segue as definições da "Cartilha de Segurança do CERT.br".

O sistema analisa anexos compactados com extensões tipo ZIP, RAR, CAB, ACE, ARJ, BH, HA, JAR, PAK, LHA, LZH, PKZIP, BZIP, GZIP, ZOO, 7Z, BZ2, BZIP2, TZH, TGZ, TAR, GZ, etc.

Como camada complementar, o MailInspector disponibiliza a **ESET Scan Engine** como um módulo opcional já licenciado, permitindo ampliar a cobertura de detecção por meio de análise multiscan e reforço adicional contra malware. A engine ESET opera integrada ao fluxo de inspeção do MailInspector, contribuindo com detecções adicionais sem alterar a arquitetura ou o motor principal de proteção.

É possível realizar **a integração com outros sistemas de antivírus do mercado**, para serem executados simultaneamente, dependendo unicamente do cliente a aquisição de outro antivírus que não sejam os padrões utilizadas pela solução (HSC SmartDefender antivírus e opcionalmente ESET). Para maiores informações dos produtos antivírus compatíveis e integração, favor entrar em contato com o suporte da HSC Brasil.

No MailInspector, na parte de antivírus, pode-se criar controles globais ou por grupos, controlando entrada ou saída de mensagens. Todos os anexos das mensagens são analisados. Também é possível criar exceções de escaneamento, dessa forma pode-se criar regras para não verificar e-mails de determinada origem e dirigidos a determinados destinatários.

O sistema de proteção contra **Malware e Vírus** é capaz de identificar e acompanhar **campanhas globais de ataques em andamento**, disponibilizando essas informações aos administradores do MailInspector em tempo real. A solução gera **alertas sobre ameaças e campanhas identificadas**, permitindo o acompanhamento de sua evolução, abrangência e características, além de manter **registros das ocorrências, eventos, ações executadas e comportamentos observados** ao longo do ciclo da campanha.

Dessa forma, os administradores obtêm maior visibilidade sobre ameaças emergentes e podem acompanhar, de forma centralizada, a evolução das campanhas de Malware e seus possíveis impactos sobre o ambiente de correio eletrônico da organização.

Também é possível efetuar ações sobre e-mails detectados com programas/conteúdos maliciosos. Tais ações englobam:

- Limpeza da mensagem;
- Modificação da mensagem;
- Remoção de anexos;
- Retenção do e-mail em quarentena (inclusive com opção de quarentena customizada);
- Exclusão do e-mail;
- Inserir TAG no assunto;
- Gerar notificação ao destinatário e/ou remetente do e-mail;
- Prosseguir com a entrega da mensagem, com opção de gerar cópia em auditoria;

ESET é fabricante de Engine (motor) de antivírus que fornece a inteligência para outros fabricantes, tais como:

- Microsoft;
- IBM;
- Cisco;
- NETGEAR;
- Solar Winds;
- CheckPoint;
- F-Secure;
- GDATA, etc...

ESET participa do programa da Microsoft que recebe avisos de ameaças/vulnerabilidades antecipadamente nas suas ferramentas (Microsoft Active Protections Program) https://www.microsoft.com/en-us/msrc/mapp

Diversas Premiações

Product of the Year
Internet Security 2018
"The highest level of effectiveness"

A plataforma de proteção de última geração em camadas da HSC SmartDefender antivírus e ESET (antivírus autônomos e opcional) são projetadas e construídas de baixo para cima, para proteger contra ataques direcionados avançados e evasivos.

Várias camadas de segurança fornecem proteção tanto na pré-execução (Hyperdetect, Sandbox Analyzer), quanto na execução (Advanced Anti-exploit e Application Control). ESET também possui uma tecnologia inovadora para proteção específica de datacenter (HVI-Hypervisor Introspection). Além de possuir um módulo de proteção AMSI para detecção rápida de código JS indesejado, a ESET também possui técnica de detecção de esteganografia, ao qual visa esconder o código malicioso pelo bit menos significativo (um dos métodos mais utilizados por hackers) dentro de um arquivo. Tanto a ESET, quanto o antivírus proprietário da HSCBRASIL (HSC SmartDefender antivírus), possuem proteção contra ataques que utilizam técnica ROP (Return Oriented Programming), dessa forma protegendo de ataques que não utilizam injeção de códigos.

Com a integração dos melhores antivírus do mercado, a solução MailInspector consegue abranger a proteção, alcançando quase 100% de detecção e bloqueio de códigos maliciosos/mal intencionados.

Além da análise de assinaturas e reputação, o HSC SmartDefender antivírus incorpora tecnologias dinâmicas avançadas que elevam significativamente o nível de segurança da solução:

- **Sandbox de Arquivos** – Executa arquivos suspeitos em ambiente isolado para identificar comportamentos maliciosos que não podem ser detectados apenas por análise estática.
- **Sandbox de Documentos** – Avalia documentos que possam conter macros, scripts ou conteúdo ativo, observando comportamentos anômalos ou tentativas de exploração.
- **Sandbox de URLs** – analisa dinamicamente links suspeitos em ambiente controlado, identificando phishing dinâmico, redirecionamentos maliciosos e carregamento de scripts.
- **Proteção Zero-Day** – utiliza heurística avançada, machine learning e análise comportamental para identificar ameaças inéditas ou ainda sem assinatura disponível.

Essas tecnologias, integradas ao HSC SmartDefender, garantem uma abordagem de defesa em múltiplas camadas, combinando análise estática, dinâmica e comportamental para oferecer um nível superior de proteção no tráfego de e-mail corporativo.

No antivírus é feita a verificação de arquivos padrão Office (tais como documentos, PDF's, planilhas, apresentações, etc), ao qual são extraídos os vírus e malwares de dentro desse tipo de arquivo. Também são verificados os links/URL's externos dos arquivos, analisando o apontamento deles, bem como do seu conteúdo. Dessa forma é possível a detecção de ameaças vindas em hospedagens de arquivos maliciosos linkados em outros locais, bem como se é download de arquivo, se o mesmo está compactado e seu conteúdo compactado é malicioso.

Abaixo segue uma lista de alguns tipos de ameaças que são reconhecidas pelas nossas engines.

A detecção de ameaças é capaz de identificar e bloquear o acesso aos mais diferentes tipos de ameaças, entre elas destacamos:

ActiveX maliciosos
Multipartite Vírus
Applets Java maliciosos
Backdoors
Browser Exploits
File Exploit
Executáveis Windows maliciosos
Flash ActionScripts maliciosos
Boot Vírus
Dialers
Adwares
Stealth Attack (detectado por heurística)
Polymorphic Virus
Infected Website
Java Applications maliciosos
JavaScript maliciosos
Keyloggers
Resident Virus
Password Stealer/Password Tools
Phishing
Malwares
Hacreks Tools
Direct Action Virus
Ransomware
Code Injection
Port Scanning Procedures
Rootkits
Scripts Visual Basic maliciosos
Session Hijackers
Spyware
Directory Virus
Trojans
Vírus
Worms
Virus de Macros
Packed Malwares
Tracking Cookies
Remote Control APPs

Definições de Opções - Configurações Gerais

Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição
Salvar	Quando clicado, grava as configurações realizadas.

Definições de Opções – ESET LiveGrid

Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição
Ativar ESET Scan Engine	**Sim:** Habilita o uso da engine antivírus ESET, incluída no MailInspector já devidamente licenciada como mecanismo adicional de detecção, operando como antivírus LOCAL. Embora a engine principal do sistema seja o HSC SmartDefender antivírus, tecnologia proprietária da HSC para análise antivírus, antimalware e reputação avançada, recomenda-se manter a ESET Scan Engine ativada para ampliar a cobertura e reforçar a segurança por meio de análise multicamadas. **Não:** Não ativa ESET Scan Engine
Tamanho Máximo dos Arquivos Escaneados	Informe o tamanho máximo do arquivo a ser escaneado, indicando o tamanho e a medida de conversão utilizada (kB, MB ou GB)
Número Máximo de Níveis de compactação Escaneados	Informe o número máximo de descompactações que serão permitidas pelo sistema de controle de ameaças quando estiver analisando um arquivo compactado. A quantidade máxima de compactação permitida é de 500.
Ativar Mecanismo de Detecção Zero-Day	**Sim:** Este mecanismo permite identificar novos focos de ataques e proliferações de Vírus e outras ameaças sem que haja uma assinatura de detecção disponível. É efetuada a consulta Online no ESET LiveGrid (antivírus secundário presente no MailInspector), em tempo real, não necessitando que o sistema seja atualizado para identificar estas ameaças. **Não:** Não ativa a checagem acima citado.
Detectar Arquivos Potencialmente Perigosos	**Sim:** O sistema detecta automaticamente eventuais anexos perigosos (de acordo com o seu comportamento) **Não:** O sistema ignora o comportamento anômalo de arquivos, que poderiam ser potencialmente perigosos.
Enviar alerta em caso de Epidemias	Este mecanismo detecta fontes emissoras de ataques e/ou epidemias de ameaças e notifica via e-mail o administrador. Uma vez habilitada este alerta, as opções abaixo serão apresentadas para a configuração: • **E-mail de Alerta:** Insira o e-mail ao qual receberá o alerta de epidemia; O e-mail enviado de alerta indica a campanha, bem como outras informações comportamentais da campanha envolvida. • **Definir Como Epidemia a Ocorrência de:** Insira número mínimo de ocorrências detectadas, para o sistema considerar como epidemia de ameaças. É considerada número de ocorrências **por hora**; Uma vez definida a política de detecção de epidemia, o MailInspector ativa o sistema de proteção e epidemia, mudando automaticamente as configurações para aumento de sensibilidade e restrição e após a epidemia, através de atualização automática, o sistema retorna as configurações antes da epidemia.
Higienizar	**Sim:** Tenta remover o vírus/malware do arquivo se possível, em caso positivo entrega mensagem limpa para o usuário, caso a limpeza não seja possível, a mensagem é bloqueada ou removido o anexo, conforme configuração do administrador do sistema. Caso seja possível a limpeza, o resultado é uma cópia não infectada da mensagem ou anexo original, ao qual é encaminhada ao destinatário(s). **Não:** Não limpa o arquivo, mas considera o mesmo como perigoso e poderá ser bloqueado pelo sistema ou removido o anexo, conforme configuração do administrador do sistema.

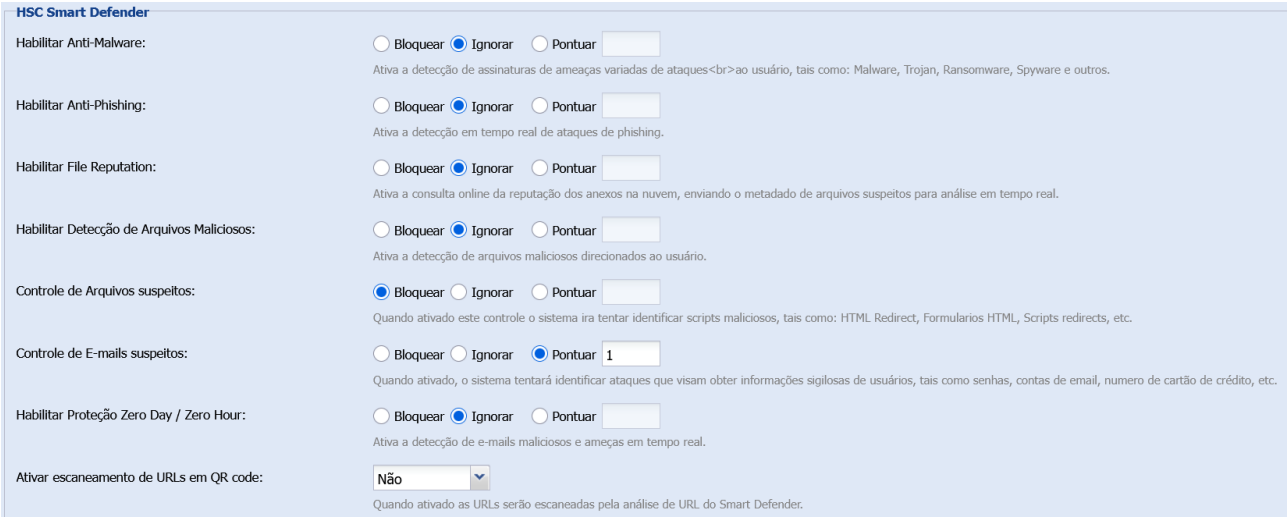
Tempo máximo de Varredura	Indica o tempo máximo suportado para análise do anti-vírus. Se ultrapassar o tempo indicado, a análise de malware sobre o arquivo será ignorado.

Definições de Opções - HSC SmartDefender

Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição
Habilitar Anti-Malware	Ativa a detecção de assinaturas de ameaças variadas de ataques ao usuário, tais como: Malware, Trojan, Ransomware, Spyware e outros. Indica o que será efetuado sobre a ameaça encontrada, podendo ser: **Bloquear**: Bloqueia o e-mail; **Ignorar:** Prossegue com a entrega, ignorando o malware encontrado; **Pontuar:** Aumenta a pontuação do e-mail em relação a esta ameaça;
Habilitar Anti-Phishing	Ativa a detecção em tempo real de ataques de phishing. Indica o que será efetuado sobre a ameaça encontrada, podendo ser: **Bloquear**: Bloqueia o e-mail; **Ignorar:** Prossegue com a entrega, ignorando o phishing encontrado; **Pontuar:** Aumenta a pontuação do e-mail em relação a esta ameaça;
Habilitar File Reputation	Ativa filtragem de Reputação de Arquivo de forma Online usando o HSC SmartDefender. Envia o metadados do arquivo suspeito para análise em tempo real na nuvem do SmartDefender em tempo real. Indica o que será efetuado sobre a reputação do arquivo, podendo ser: **Bloquear**: Bloqueia o e-mail; **Ignorar:** Prossegue com a entrega, ignorando a reputação do anexo; **Pontuar:** Aumenta a pontuação do e-mail em relação a este anexo;
Habilitar Detecção de Arquivos Maliciosos	Ativa a detecção de arquivos maliciosos direcionados ao usuário. Contém uma lista de arquivos maliciosos conhecidos e análise através de técnicas de ofuscamento de anexos. Indica o que será efetuado sobre a reputação do arquivo, podendo ser: **Bloquear**: Bloqueia o e-mail; **Ignorar:** Prossegue com a entrega, ignorando o arquivo malicioso; **Pontuar:** Aumenta a pontuação do e-mail em relação a este anexo;
Controle de Arquivos Suspeitos	Quando ativado este controle o sistema irá tentar identificar scripts maliciosos, tais como: HTML Redirect, Formularios HTML, Scripts redirects, etc. É possível ao administrador escolher a ação a ser tomada: **Bloquear**: Bloqueia o e-mail; **Ignorar:** Prossegue com a entrega, ignorando o arquivo suspeito; **Pontuar:** Aumenta a pontuação do e-mail em relação a este anexo;
Controle de E-mails suspeitos	Quando ativado este controle o sistema irá tentar identificar ataques que tentam obter informações sigilosas de usuários, tais como senhas, contas de e-mail, número de cartão de crédito, etc. É possível ao administrador escolher a ação a ser tomada: **Bloquear**: Bloqueia o e-mail; **Ignorar:** Prossegue com a entrega, ignorando o controle de e-mails suspeitos; **Pontuar:** Aumenta a pontuação do e-mail em relação a este anexo;

Habilitar Proteção Zero Day / Zero Hour	Ativa a detecção de e-mails maliciosos e ameaças em tempo real, sem a necessidade de intervenção do administrador no caso de e-mail detectado com este tipo de ameaça. Esse mecanismo ao detectar uma ameaça sem assinatura, ele é acionado e automaticamente coloca a ameaça em quarentena temporária (quarentena ATP). É possível ao administrador escolher a ação a ser tomada: **Bloquear**: Bloqueia o e-mail; **Ignorar:** Prossegue com a entrega, ignorando a proteção Zero Hour/Zero Day; **Pontuar:** Aumenta a pontuação do e-mail em relação a este anexo;
Ativar escaneamento de URLs em QR code	Ativa a detecção de links maliciosos presentes em QR Codes. Quando ativado as URLs serão escaneadas pela análise de URL do Smart Defender. A análise do QR code é feito tanto no corpo dos e-mails quanto em anexos. **Sim**: Ativa a função de escaneamento de URLs em QR code; **Não:** Não ativa a função de escaneamento de URLs em QR code;



Tela com indicação de configuração em segurança quanto a parte de SmartDefender (antivírus da HSCBRASIL).

Definições de Opções – URL Cloud SandBox

Essas configurações afetam os e-mails com URL's, de acordo com as ações escolhidas pelo administrador do sistema.

Opções	Definição
Malware Categories	Identifica URLs que estejam categorizadas como maliciosas. Ações possíveis atribuídas a URL's classificada como Malware contidas nos e-mails: • Bloquear; • Ignorar; • Pontuar;
HSC URL Reputation	Engine responsável por identificar e categorizar a reputação dos Websites, usando técnicas heurísticas e estatísticas. Ações possíveis: • Bloquear;

	• Ignorar; • Pontuar;
Blacklist Database	Verifica se a URL está em uma base de dados global de URL's não confiáveis. Caso esteja em blacklist, as ações possíveis são: • Bloquear; • Ignorar; • Pontuar;
Lookup Engine	Engine responsável por identificar conteúdos maliciosos nas paginas Web. Caso detecte conteúdo malicioso na página da URL, as ações possíveis são: • Bloquear; • Ignorar; • Pontuar;
Smart Crawler	Realiza a navegação e análise em tempo real das URLs para evitar acesso à conteúdo potencialmente perigoso. É feita a análise do conteúdo da página em tempo real. Caso encontre conteúdo potencialmente perigoso, é possível o administrador efetuar: • Bloquear; • Ignorar; • Pontuar;

Definições de Opções – Controle Avançado - Antivírus

Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição
Salvar	Quando clicado, grava as configurações realizadas.

Definições de Opções - Gerenciar Antivírus

Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição
Ativar Filtragem de Antivírus	Escolha entre: • **Sim** - Indica que o sistema de filtragem de antivírus está ativo. Este recurso permite que todas as mensagens sejam analisadas contra vírus e ameaças. • **Não** - Indica que o sistema de filtragem de antivírus está desativado.
Adicionar	Cadastra uma nova regra de filtragem de antivírus e ameaças. Quando clicado, abre a caixa de diálogo **Cadastro do Controle Personalizado**.
Editar	Edita as configurações de um registro existente. Quando clicado, abre a caixa de diálogo **Cadastro do Controle Personalizado**.
Remover	Quando clicado, exclui o registro selecionado.

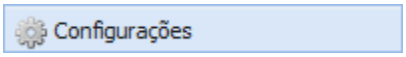
Definições de Opções - Cadastro do Controle Personalizado

O controle personalizado permite ao administrador criar regras específicas ou exceções quanto a filtragem de e-mail no módulo de antivírus, por exemplo é possível criar um grupo de usuários e atrelar esse grupo de usuários tanto aos remetentes, quanto aos destinatários e à partir dessa regra, indicar exceção no antivírus.
Por exemplo:
Regra de quando um e-mail vier de um remetente em específico, direcionado ao meu setor de logística, todos os e-mails que atingirem essa condição, o antivírus (tanto o antivírus, quanto o módulo Zero Day e Zero Hour) não atuará no e-mail.
Seguindo o exemplo acima citado, é possível compor regra de controle de antivírus de acordo com o Grupo de Usuários (vide *Grupos Usuários*).
Outro exemplo de uso de controle personalizado é a possibilidade de criar exceções de ativação do módulo antivírus, Zero Day e Zero Hour de acordo com o tipo de arquivo e/ou extensão do arquivo, dessa forma permitindo ao administrador maior granularidade de configurações sobre o antivírus.

Opções	Definição
Adicionar	Quando clicado, adiciona o controle personalizado.
Cancelar	Quando clicado, cancela a ação.
De	Selecione o grupo pré-cadastrado de remetentes.
Para	Selecione o grupo pré-cadastrado de destinatários.
Filtrar Contra Vírus	Escolha entre: • **Sim** - Indica que a regra será aplicada, quando os remetentes e os destinatários pertencerem aos grupos selecionados. • **Higienizar** - Tenta remover o vírus do arquivo se possível, em caso positivo entrega mensagem limpa para o usuário. • **Não** - Indica que a regra não será aplicada, quando os remetentes e os destinatários pertencerem aos grupos selecionados.

AntiPhishing

Use esta página para exibir, adicionar, editar ou excluir configurações de antiphishing do Filtro de SPAM.



/ Controle de Ameaças / Antiphishing

Visão geral do antiphishing

O mecanismo de antiphishing do HSC MailInspector é um dos mais modernos sistemas de identificações de mensagens suspeitas. Através dele é possível identificar as tentativas de encaminhamento de URLs mal-intencionadas.

O MailInspector possui internamente categorização de phishing, para poder classificar o “tipo” de phishing detectado, entre as categorias estão:

- Phishing Social Engineering;
- Phishing Account Payment Subscription;
- Phishing Banking CreditCard OpenFinance;
- Phishing Ecommerce Delivery Services;
- Fake Official Documents;
- Fake System Communications;
- Fake Billing and Payment Requests;
- Fraud Credit Loan Investment Schemes;
- Fake Promotions Lotteries and Products;
- Fake Courses Trainings and Certifications;
- Fake Jobs and Recruitment Scams;
- Fake Alerts and Threats;
- False Complaints and Fake Reputation;
- Fake Authorities and Institutions;
- Webmails Fake;
- Sex torTion;
- Spear Phishing;
- Generic;

O mecanismo de antiphishing é composto por duas formas de análise:

1) HSC URL’s Purpose: Identifica a tentativa de redirecionamento para URLs Maliciosas presentes nos e-mail. Como mensagens contendo "Click Aqui", "Efetue seu cadastro", etc.

2) HSC URL Reputation: O HSC MailInspector analisa em tempo real, diretamente nos data centers globais da HSC, a reputação de cada URL presente no e-mail, a fim de identificar novos focos de propagação de vírus, phishing e outros conteúdos mal-intencionados.

Definições de Opções - Antiphishing

Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição
Salvar	Quando clicado, grava as configurações realizadas.

Definições de Opções - Gerenciar Antiphishing

Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição
Ativar Filtro Contra Phishing	Escolha entre: • **Sim** - Indica que a filtragem contra phishing está ativa. Esta funcionalidade gerencia todos os recursos de filtragem anti-spam. • **Não** - Indica que a filtragem contra phishing está desativada.
Adicionar	Cadastra uma nova regra de pontuação para provável SPAM. Quando clicado, abre a caixa de diálogo **Cadastro do Controle Personalizado**.
Editar	Edita as configurações de um registro existente. Quando clicado, abre a caixa de diálogo **Cadastro do Controle Personalizado**.
Remover	Quando clicado, exclui o registro selecionado.

Definições de Opções - Antiphishing Numérico

Phishing numérico é o phishing que utiliza IP na URL, por exemplo:

- http://200.200.200.201/xyz.html

Opções	Definição
Ativar Filtro Contra Phishing Numérico	Escolha entre: • **Sim** - Indica que a filtragem contra phishing numérico está ativa. Esta funcionalidade gerencia todos os recursos de filtragem anti-spam. • **Não** - Indica que a filtragem contra phishing numérico está desativada.
Adicionar	Cadastra uma nova regra de pontuação para SPAM. Quando clicado, abre a caixa de diálogo **Cadastro do Controle Personalizado**.
Editar	Edita as configurações de um registro existente. Quando clicado, abre a caixa de diálogo **Cadastro do Controle Personalizado**.
Remover	Quando clicado, exclui o registro selecionado.

Definições de Opções - Notificação de URL Maliciosa

Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição
Adicionar	Cadastra uma nova regra de pontuação para SPAM. Quando clicado, abre a caixa de diálogo **Cadastro do Controle Personalizado**.
Editar	Edita as configurações de um registro existente. Quando clicado, abre a caixa de diálogo **Cadastro do Controle Personalizado**.
Remover	Quando clicado, exclui o registro selecionado.

Definições de Opções - Cadastro do Controle Personalizado

Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição
Adicionar	Quando clicado, adiciona o controle personalizado.
Cancelar	Quando clicado, cancela a ação.
De	Selecione o grupo pré-cadastrado de remetentes.
Para	Selecione o grupo pré-cadastrado de destinatários.
Ação	Escolha entre: • **Sim** - Indica que a regra será aplicada, quando os remetentes e os destinatários pertencerem aos grupos selecionados. • **Não** - Indica que a regra não será aplicada, quando os remetentes e os destinatários pertencerem aos grupos selecionados. • **Desarmar URL** - Indica que as URLs presentes na mensagem serão desabilitadas, quando os remetentes e os destinatários pertencerem aos grupos selecionados. • **Reescrever URL** - Indica que as URLs presentes na mensagem serão modificadas encaminhando o usuário para uma página de confirmação de segurança, quando os remetentes e os destinatários pertencerem aos grupos selecionados. • **Nenhuma Ação** - Indica que a regra não aplicará nenhuma ação nas mensagens quando os remetentes e os destinatários pertencerem aos grupos selecionados.

CDR (Content Disarm and Reconstruction)

Use esta página para exibir, adicionar, editar ou excluir configurações de Content Disarm and Reconstruction.

Configurações **/ Controle de Ameaças / CDR**

Visão geral do controle de conteúdo HTML

Content Disarm & Reconstruction (CDR) é um sistema de filtragem que remove código malicioso de documentos e HTML. Ao contrário de um sistema de Análise de Malware comum, o CDR não determina ou detecta se o arquivo é malicioso, ele irá remover dos Documentos todos componentes que forem possivelmente perigosos tipo: Dados Executáveis como "Macros VBA", "JavaScript", “Embedded Flash”, "Embedded Files", bibliotecas DLL, imagens JPEG, GIF ou BMP, etc, estando ou não dentro de documentos como: .DOC, .DOCX, .SWF, .XLS, .XLSX, .PPT, .PPTX, .PPS, .RTF, .PDF, etc (mesmo caso esteja dentro de arquivos compactados).

Permite efetuar controles em mensagens escritas no formato HTML, sendo possível identificar diversas TAGs tais como: <SCRIPT>, <FORM>, imagem externa, <IFRAME>, <OBJECT CODEBASE> entre outras, podendo: bloquear mensagem, remover, desarmar (desabilitar a ação HTML) ou encaminhar. Podendo criar controles globais ou por grupos da ferramenta, controlando a entrada e/ou a saída de mensagens.

Definições de Opções – Configuração Geral

Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição
Salvar	Quando clicado, grava as configurações realizadas.
Caixa de Seleção	Permitir ou Desarmar o CDR

Definições de Opções - Office Documents

Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição
Habilita controle CDR Documentos Office	Escolha entre: • **Permitir** - Indica que o envio e o recebimento de arquivos Office (possivelmente perigosos) são permitidos. • **Desarmar** - Indica que o envio e o recebimento de arquivos Office (possivelmente perigosos) não são permitidos (será desarmado). • **Bloquear** - Coloca o e-mail em quarentena
Adicionar	Cadastra uma nova regra personalizada de Office Documents. Quando clicado, abre a caixa de diálogo **Cadastro do Controle Personalizado**.
Editar	Edita as configurações de um registro existente. Quando clicado, abre a caixa de diálogo **Cadastro do Controle Personalizado**.
Remover	Quando clicado, exclui o registro selecionado.

Definições de Opções - Mensagens Fragmentadas

Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição
Permitir Mensagens Fragmentadas	Escolha entre: • **Permitir** - Indica que o envio e o recebimento de mensagens fragmentadas são permitidos. • **Não Permitir** - Indica que o envio e o recebimento de mensagens fragmentadas não são permitidos. Mensagens fragmentadas não são analisadas pelos filtros de conteúdo.
Adicionar	Cadastra uma nova regra de mensagens fragmentadas. Quando clicado, abre a caixa de diálogo **Cadastro do Controle Personalizado**.
Editar	Edita as configurações de um registro existente. Quando clicado, abre a caixa de diálogo **Cadastro do Controle Personalizado**.
Remover	Quando clicado, exclui o registro selecionado.

Definições de Opções - Conteúdo Externo

Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição
Permitir Mensagens com Conteúdo Externo	Escolha entre: • **Permitir** - Indica que o envio e o recebimento de mensagens que contenham conteúdo remoto anexado ao corpo da mensagem são permitidos. • **Não Permitir** - Indica que o envio e o recebimento de mensagens que contenham conteúdo remoto anexado ao corpo da mensagem não são permitidos.
Adicionar	Cadastra uma nova regra de conteúdo externo na mensagem. Quando clicado, abre a caixa de diálogo **Cadastro do Controle Personalizado**.
Editar	Edita as configurações de um registro existente. Quando clicado, abre a caixa de diálogo **Cadastro do Controle Personalizado**.
Remover	Quando clicado, exclui o registro selecionado.

Definições de Opções - TAG IFrame

Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição
Permitir TAG IFrame no Corpo da Mensagem	Escolha entre: • **Permitir** - Indica que o envio e o recebimento de mensagens que contenham conteúdo HTML com a TAG IFrame no corpo da mensagem são permitidos.

	• **Não Permitir** - Indica que o envio e o recebimento de mensagens que contenham conteúdo HTML com a TAG IFrame no corpo da mensagem não são permitidos. • **Desarmar** - Indica que o envio e o recebimento de mensagens que contenham conteúdo HTML com a TAG IFrame no corpo da mensagem serão desarmadas, a TAG IFrame será modificada desabilitando o seu funcionamento.
Adicionar	Cadastra uma nova regra de TAG IFrame no corpo da mensagem. Quando clicado, abre a caixa de diálogo **Cadastro do Controle Personalizado**.
Editar	Edita as configurações de um registro existente. Quando clicado, abre a caixa de diálogo **Cadastro do Controle Personalizado**.
Remover	Quando clicado, exclui o registro selecionado.

Definições de Opções - TAG Form

Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição
Permitir TAG Form no Corpo da Mensagem	Escolha entre: • **Permitir** - Indica que o envio e o recebimento de mensagens que contenham conteúdo HTML com a TAG Form no corpo da mensagem são permitidos. • **Não Permitir** - Indica que o envio e o recebimento de mensagens que contenham conteúdo HTML com a TAG Form no corpo da mensagem não são permitidos. • **Desarmar** - Indica que o envio e o recebimento de mensagens que contenham conteúdo HTML com a TAG Form no corpo da mensagem serão desarmados, a TAG Form será modificada desabilitando o seu funcionamento.
Adicionar	Cadastra uma nova regra de TAG Form no corpo da mensagem. Quando clicado, abre a caixa de diálogo **Cadastro do Controle Personalizado**.
Editar	Edita as configurações de um registro existente. Quando clicado, abre a caixa de diálogo **Cadastro do Controle Personalizado**.
Remover	Quando clicado, exclui o registro selecionado.

Definições de Opções - Scripts

Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição
Permitir TAG Script no Corpo da Mensagem	Escolha entre: • **Permitir** - Indica que o envio e o recebimento de mensagens que contenham conteúdo HTML com a TAG Script no corpo da mensagem são permitidos. • **Não Permitir** - Indica que o envio e o recebimento de mensagens que contenham conteúdo HTML com a TAG Script no corpo da mensagem não são permitidos.

	• **Desarmar** - Indica que o envio e o recebimento de mensagens que contenham conteúdo HTML com a TAG Script no corpo da mensagem serão desarmados, a TAG Script será modificada desabilitando o seu funcionamento.
Adicionar	Cadastra uma nova regra de TAG Script no corpo da mensagem. Quando clicado, abre a caixa de diálogo **Cadastro do Controle Personalizado**.
Editar	Edita as configurações de um registro existente. Quando clicado, abre a caixa de diálogo **Cadastro do Controle Personalizado**.
Remover	Quando clicado, exclui o registro selecionado.

Definições de Opções - Small IMG

Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição
Permitir Imagens Pequenas no Corpo da Mensagem	Escolha entre: • **Permitir** - Indica que o envio e o recebimento de mensagens que contenham conteúdo HTML com imagens pequenas incorporadas no corpo da mensagem são permitidos. • **Não Permitir** - Indica que o envio e o recebimento de mensagens que contenham conteúdo HTML com imagens pequenas incorporadas no corpo da mensagem não são permitidos. • **Desarmar** - Indica que o envio e o recebimento de mensagens que contenham conteúdo HTML com imagens pequenas incorporadas no corpo da mensagem serão desarmados, a TAG IMG será modificada desabilitando o seu funcionamento.
Adicionar	Cadastra uma nova regra de imagens pequenas incorporadas no corpo da mensagem. Quando clicado, abre a caixa de diálogo **Cadastro do Controle Personalizado**.
Editar	Edita as configurações de um registro existente. Quando clicado, abre a caixa de diálogo **Cadastro do Controle Personalizado**.
Remover	Quando clicado, exclui o registro selecionado.

Definições de Opções - Object CODEBASE

Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição
Permitir TAG Object CODEBASE no Corpo da Mensagem	Escolha entre: • **Permitir** - Indica que o envio e o recebimento de mensagens que contenham conteúdo HTML com a TAG Object CODEBASE no corpo da mensagem são permitidos. • **Não Permitir** - Indica que o envio e o recebimento de mensagens que contenham conteúdo HTML com a TAG Object CODEBASE no corpo da mensagem não são permitidos. • **Desarmar** - Indica que o envio e o recebimento de mensagens que contenham conteúdo HTML com a TAG Object CODEBASE no corpo da mensagem serão

	desarmados, a TAG Object CODEBASE será modificada desabilitando o seu funcionamento.
Adicionar	Cadastra uma nova regra de TAG Object CODEBASE no corpo da mensagem. Quando clicado, abre a caixa de diálogo **Cadastro do Controle Personalizado**.
Editar	Edita as configurações de um registro existente. Quando clicado, abre a caixa de diálogo **Cadastro do Controle Personalizado**.
Remover	Quando clicado, exclui o registro selecionado.

Definições de Opções - Converter HTML para Texto Plano

Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição
Converter Conteúdo HTML do Texto Plano	Escolha entre: • **Converter** - Indica que o envio e o recebimento de mensagens que contenham conteúdo HTML serão convertidos para o formato de texto plano. • **Não Converter** - Indica que o envio e o recebimento de mensagens que contenham conteúdo HTML não serão convertidos para o formato de texto plano.
Adicionar	Cadastra uma nova regra de conversão de mensagens HTML para texto plano. Quando clicado, abre a caixa de diálogo **Cadastro do Controle Personalizado**.
Editar	Edita as configurações de um registro existente. Quando clicado, abre a caixa de diálogo **Cadastro do Controle Personalizado**.
Remover	Quando clicado, exclui o registro selecionado.

Definições de Opções - Cadastro do Controle Personalizado

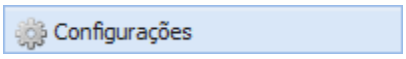
Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição
Adicionar	Quando clicado, adiciona o controle personalizado.
Cancelar	Quando clicado, cancela a ação.
De	Selecione o grupo pré-cadastrado de remetentes.
Para	Selecione o grupo pré-cadastrado de destinatários.
Ação	Escolha entre: • **Permitir** - Indica que a mensagem não será bloqueada, quando os remetentes e os destinatários pertencerem aos grupos selecionados. • **Não Permitir** - Indica que a mensagem será bloqueada, quando os remetentes e os destinatários pertencerem aos grupos selecionados. • **Desarmar** - Indica que a mensagem terá o conteúdo modificado, quando os remetentes e os destinatários pertencerem aos grupos selecionados. • **Converter** - Indica que a mensagem será convertida, quando os remetentes e os destinatários pertencerem aos grupos selecionados.

	• **Não Converter** - Indica que a mensagem não será convertida, quando os remetentes e os destinatários pertencerem aos grupos selecionados.

Reputação

Use esta página para exibir ou editar configurações da Reputação do Controle de Conexão.



/ **Controle de Ameaças / Reputação**

Visão geral da reputação

O sistema de Reputação consiste em consultar de forma online o sistema HSC SmartDefender, que é uma rede global de análise e categorização de website (URLs), análise e reputação de e-mails, análise e reputação de IP's e de ameaças da internet (para maiores informações: *HSC SmartDefender*).
O sistema de reputação é utilizado de três formas no HSC MailInspector:

- **Reputação do Emissor (servidor de origem) das Mensagens:** Verifica qual a reputação do endereço IP/Domínio do servidor que enviou a mensagem, permitindo pontuar a mensagem conforme sua reputação. Este serviço é consultado no sistema HSC SmartDefender, por BigData e outros sistemas já incluindo DUL (Dynamically Assigned IP – para detecção de listas dinâmicas de IP) e ETL (Emerging Threat Block List – listas baseadas em ameaças detectadas por firewall), além de RBL's na camada de conexão e/ou processamento.
- **Reputação das URLs:** O HSC MailInspector extrai todas URLs presentes no corpo da mensagem, verificando a reputação de cada URL, permitindo pontuar a mensagem conforme a reputação das URLs presentes na mensagem. Hoje, o principal mecanismo de proliferação de vírus e outras ameaças são as URLs presentes nas mensagens. Estas URLs maliciosas, geralmente, infectam o computador do usuário ou roubam informações sigilosas.
- **Categorias de URLs:** O HSC MailInspector extrai todas URLs presentes no corpo da mensagem, verificando a categoria de cada URL, permitindo pontuar a mensagem conforme as categorias das URLs presentes na mensagem.
  O sistema de categorização consiste em banco de dados contendo mais de 70 Milhões de URLs, categorizadas em mais de 50 tipos de categorias, divididas por assuntos como: Conteúdo Pornográfico, E-mails Adultos, E-mail Marketing, SPAM, Esportes, Notícias, Negócios, Redes Sociais e muitas outras. Sendo possível personalizar um valor de pontuação por categoria.

Definições de Opções - Reputação

Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição
Salvar	Quando clicado, grava as configurações realizadas.

Definições de Opções - Origem

Permite ao administrador configurar a pontuação para que o sistema defina as mensagens como alto risco, médio risco, possível risco e sem risco conhecido.

Opções	Definição
Ativar	Escolha entre: • **Sim** - Indica que o controle de conexão por reputação da origem está ativo. Permite verificar a reputação do servidor de origem das mensagens, atribuindo uma pontuação customizada as mesmas durante o processo de filtragem.

	• **Não** - Indica que o controle de conexão por reputação da origem está desativado.
Alto Risco	Permite definir a pontuação que será atribuída as mensagens procedentes de servidores classificados como alto risco. Estes servidores **foram fontes de SPAM, vírus, phishing ou algum outro tipo de ameaça** nas **últimas 48 horas**, ou possuem uma infraestrutura de e-mails suspeita (não possui configuração de DKIM, Sender ID, SPF, Domain Key, whois incompleto ou mal configurado, etc). Esta categoria tem 4 níveis de reputação afim de aumentar sua granularidade de configuração.
Médio Risco	Permite definir a pontuação que será atribuída as mensagens procedentes de servidores classificados como médio risco. Estes servidores **foram fontes de SPAM, vírus, phishing ou algum outro tipo de ameaça** na **última semana**, ou possuem uma infraestrutura de e-mails suspeita (não possui configuração de DKIM, Sender ID, SPF, Domain Key, whois incompleto ou mal configurado, etc). Esta categoria tem 4 níveis de reputação afim de aumentar sua granularidade de configuração.
Possível Risco	Permite definir a pontuação que será atribuída as mensagens procedentes de servidores classificados como possível risco. Estes servidores apresentaram **comportamentos suspeitos** no envio de mensagens na **última semana**, ou possuem uma infraestrutura de e-mails suspeita (não possui configuração de DKIM, Sender ID, SPF, Domain Key, whois incompleto ou mal configurado, etc). Esta categoria tem 4 níveis de reputação afim de aumentar sua granularidade de configuração.
Sem Risco Conhecido	Permite definir a pontuação que será atribuída as mensagens procedentes de servidores classificados como sem risco conhecido. Geralmente servidores que possuem uma boa reputação e que não participaram de nenhuma campanha de SPAM, PHISHING ou Vírus conhecido.

Definições de Opções - URL

Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição
Ativar	Escolha entre:

	• **Sim** - Indica que o controle de conexão por reputação da URL está ativo. Permite verificar a reputação de URLs contidas no corpo da mensagem, atribuindo uma pontuação customizada as mesmas durante o processo de filtragem. • **Não** - Indica que o controle de conexão por reputação da URL está desativado.
Alto Risco	Permite definir a pontuação que será atribuída as mensagens que contiverem URL's classificado como alto risco. Estes servidores web **foram fontes de SPAM, vírus, phishing ou algum outro tipo de ameaça** nas **últimas 48 horas**, ou possuem uma infraestrutura de website suspeita.
Médio Risco	Permite definir a pontuação que será atribuída as mensagens que contiverem URLs classificadas como médio risco. Estes servidores web **foram fontes de SPAM, vírus, phishing ou algum outro tipo de ameaça na última semana**, ou possuem uma infraestrutura de website suspeita.
Possível Risco	Permite definir a pontuação que será atribuída as mensagens que contiverem URL's classificados como possíveis riscos. Estes servidores web tiveram **comportamentos suspeitos na última semana**, ou possuem uma infraestrutura de website suspeita.
Sem Risco Conhecido	Permite definir a pontuação que será atribuída as mensagens que contiverem URLs classificadas como sem risco conhecido.

Definições de Opções - Categorias

Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição
Ativar	Escolha entre: • **Sim** - Indica que o controle de conexão por categoria da URL está ativo. Permite verificar a categoria de URLs contidas no corpo da mensagem, atribuindo uma pontuação customizada as mesmas durante o processo de filtragem. • **Não** - Indica que o controle de conexão por categoria da URL está desativado.

Categorias	Permite definir a pontuação que será atribuída as mensagens que contiverem URLs catalogadas em determinada categoria.
	
	As categorias listadas pelo MailInspector são:
	• Conteúdo Adulto:
	  ○ Pornográfico
	  ○ Conteúdo Erótico
	  ○ Aborto
	• Conteúdo Atividades Criminais:
	  ○ Abuso Infantil
	  ○ Hacking
	  ○ Atividades Potencialmente Criminosas
	  ○ Racismo e Ódio
	  ○ Piratária e Roubo de Direitos Autorais
	  ○ Violência
	• Conteúdo Comunicação e Conectividade:
	  ○ Redes Sociais
	  ○ Bate Papo
	  ○ Armazenamento Pessoal
	  ○ P2P
	  ○ Relacionamento Profissional
	  ○ Páginas Pessoais e Blogs
	  ○ Pesquisa de Emprego
	• Conteúdo Malicioso:
	  ○ Anonymizer
	  ○ Botnet
	  ○ Command Control Center
	  ○ Malwares
	  ○ Phishing
	  ○ Sites Comprometidos
	  ○ SPAM
	  ○ Spywares & Keyloggers
	• Conteúdo Público e Governamental:
	  ○ Sites Governamentais
	  ○ Militar
	  ○ Organizações Sociais e Associações
	• Conteúdos Diversos:
	  ○ CDN - Servidores de Conteúdos
	  ○ Reserva de Domínios
	  ○ Sites Inalcansáveis
	• Conteúdos Educacionais:
	  ○ Instituições de Ensino
	  ○ Wikis
	• Conteúdo Entretenimento:
	  ○ Entretenimento
	  ○ Humor
	  ○ Streaming Áudio
	  ○ Streaming Vídeo
	  ○ TV & Filmes
	• Conteúdo Estilo de Vida:
	  ○ Esportes

	○ Veículos Motorizados ○ Turismo ○ Restaurantes ○ Moda e Beleza ○ Namoro e Relacionamento • Conteúdo Finanças: ○ Bancos ○ Finanças ○ Seguros • Conteúdo Medicina e Saúde: ○ Farmácia e Medicamentos ○ Nutrição e Dieta ○ Saúde e Medicina ○ Suplementos Alimentares • Conteúdo Negócios e Serviços: ○ Agricultura ○ Arquitetura e Construção ○ Fábricas e Indústrias ○ Imóveis • Conteúdo Notícias e Propagandas: ○ Notícias ○ Propaganda ADS ○ Receber para navegar • Conteúdo Marketing & Graymail: ○ Compras Online ○ Opinião e Comparativos de Produtos • Conteúdo Tecnologia: ○ Acesso Remoto ○ Segurança da Informação ○ Tecnologia em Geral

Ataque Dirigido

Use esta página para exibir ou editar configurações de Ataque Dirigido do Controle de Conexão.

Configurações / **Controle de Ameaças / Ataque Dirigido**

Visão geral do Ataque Dirigido

O sistema de Ataque Dirigido, analisa as mensagens de e-mails, URL's (em formato HTML e/ou formato texto) e conteúdo em busca de malwares, vírus e informações maliciosas para proteção a ataques dirigidos, com utilização de SandBox.

Estas informações alimentam um grande banco de ameaças constantemente, construindo fluxos e estatísticas analisadas para proteção em tempo real para ataques dirigidos.

O Modulo de Proteção contra-ataque dirigido atua em diversas camadas do produto garantindo uma maior segurança aos usuários finais.

Para a proteção, é efetuada a reescrita de URLs contidas em e-mails, ao qual quando o usuário clicar em uma URL contida no e-mail, o sistema faz a verificação da URL em tempo real, antes de liberar o acesso ao usuário. Não sendo encontrado ameaça, o link é liberado para acesso. Caso seja encontrada qualquer ameaça (ex: página contaminada, ou página com ransomware, ou link para download de arquivo malicioso, entre outras ameaças), é aberta página de bloqueio.

O sistema de Ataque Dirigido é "subdividido" em três sistemas distintos (URL Sandbox, File Sandbox e Documentos do tipo Office), sendo que a parte de URL Sandbox possui três camadas de proteção (Recebimento, On Click e Report), que são descritas a seguir.

1. **URL Sandbox:** A proteção ao ataque dirigido possui tecnologia capaz de avaliar um link recebido em um e-mail, mesmo que escondido em um e-mail HTML e assim verificar o caminho para o qual este link está apontando, efetuando a verificação se nesta página apontada pelo link, se há algum formulário de solicitação de senha, usuário e outras ameaças, efetuando o bloqueio da mensagem sem a necessidade de assinatura, tornando assim a proteção mais proativa no combate a phishing. Além disso, verifica o caminho para o qual este link está apontando, efetuando a verificação se este link encaminha para um sistema que efetua um redirecionamento automático para download de um arquivo (Tipo ZIP, RAR, CAB, ACE, ARJ, BH, HA, JAR, PAK, LHA, LZH, PKZIP, BZIP, GZIP, BZ2, BZIP2, ZOO, 7Z, TZH, TGZ, TAR, GZ, etc), na tentativa de enganar o usuário, efetuando o bloqueio da mensagem sem a necessidade de assinatura.

   Como funciona:
   1. Recebimento: Nesta camada as URLs, Anexos e Conteúdo são verificados na base de reputação Global e local da ferramenta em busca de informações relevantes sobre possíveis ameaças. Também é verificada a categoria da URL. Caso seja identificado alguma ameaça a mensagem é retida na quarentena específica e a mensagem não é entregue ao usuário (Esta é a configuração padrão do sistema, caso o administrador queira mudar este comportamento pode ser feito através da configuração).

   Caso a URL, Anexo ou conteúdo não tenha ainda uma resposta relevante ou mesmo uma confirmação se são considerados confiáveis o sistema automaticamente envia a amostra, conforme as configurações definidas pelo administrador. Então é enviada a amostra (se o administrador tiver configurado para isso), para nuvem do HSC SmartDefender, que irá analisar em tempo real nos

mecanismos de SandBox (File, URLs e Message Reputation). A fim de certificar que o conteúdo analisado é confiável utilizando as mais avançadas técnicas de detecção de ameaças e anomalias.

Caso não seja detectada nenhuma ameaça, os links, anexos e/ou conteúdos são liberados para passar para a próxima etapa.

2. On Click: É executada a reescrita da URLs e Anexos (conforme configuração do administrador da solução) a fim de garantir a proteção ao usuário ON CLICK, ou seja, quando usuário clicar ele será automaticamente redirecionado para nosso sistema de SandBox em busca novas informações sobre o objeto clicado URL ou Anexos, dessa forma sempre é feita nova verificação da integridade das URLs e/ou anexos antes de liberar o acesso ao usuário final.

Esse procedimento, garante ao usuário uma proteção extra em tempo real (ao clicar na URL), independentemente de quando o e-mail tenha sido verificado no sistema de E-mail Gateway.

Caso uma ameaça seja encontrada uma tela de bloqueio será mostrada para o usuário impedindo seu acesso, esta tela é customizável e contém todos informações necessárias para saber qual tipo de ataque foi realizado.

A tela de bloqueio é integrada com o sistema de colaboração explicado abaixo, ao qual permite que o administrador interaja de forma Online com qualquer URL ou Anexos, bem como qualquer report dado pelo usuário.

3. Report: Nesta fase final o administrador terá toda informação, rastreio, relatório e linha do tempo sobre todas as ameaças, através dos dashboards:

SandBox;
Ameaças;

E relatórios tais como: Fontes de Ataque, TOP Ameaças, Ataque Dirigido, entre outros. Desta forma o HSC MailInspector torna-se uma ferramenta completa para estas informações alimentam um grande banco de ameaças constantemente, construindo fluxos e estatísticas analisadas para proteção em tempo real para ataques dirigidos.

Qualquer link (HTTP, HTTPS, FTP ou WWW) contido no e-mail recebido pelo usuário dentro do corpo do e-mail ou conteúdo HTML (Corpo ou Anexo), é analisado antes mesmo de chegar em sua caixa de destino, e reanalisado e reescrito novamente assim que o usuário clique nele, gerando uma nova esteira de análise em tempo real, afim de encontrar informações ou injeção de conteúdo malicioso em sua corporação. O sistema garante que a informação sobre qual usuário clicou e as ações tomadas sejam exclusivas por usuário, mesmo que um determinado e-mail contenha mais de um destinatário.

Além de toda esteira automatizada de detecção de Ataque Dirigido, existe o modelo Colaborativo de Interação do usuário para alimentar o ecossistema de detecção de Ataque Dirigido, dando a opção aos usuários pontuarem, alertarem e alimentarem o sistema, tornando-o assim autossuficiente e muito mais responsivo e preciso.

2. **File Sandbox:** Todo e qualquer arquivo é verificado o comportamento. Para isso, ele é executado em uma área reservada e isolada de memória e verificado o comportamento dele, isto é, verifica-se a nível de memória o que ele faz no registro do Windows, se ele mexe no arquivo de hosts, se ele alteraria algum arquivo essencial para o bom funcionamento do sistema, ou seja, são feitas todas as observações referentes a segurança e em caso de alguma anomalia, o anexo é isolado e registrado

como possível ameaça. Essa análise pode ser efetuada tanto localmente OU na nuvem da HSCBRASIL, para isso, basta o administrador selecionar onde ele quer que seja efetuada esta análise.

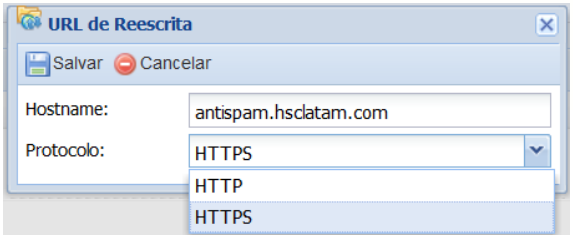
3. **Documento:** Todo e qualquer arquivo do tipo documento é verificado em relação a códigos programáveis no seu interior. O Ataque Dirigido em documentos, verifica o conteúdo do mesmo, verificando desde links, até códigos "escondidos". É possível utilizar para as seguintes ações:
    a. Bloquear: Após análise dos documentos, armazena a mensagem em quarentena, de acordo com a possível ameaça encontrada:
        i. Conteúdo de Alto Risco;
        ii. Conteúdo de Possível Risco;
        iii. URL Perigosas;
    b. CDR: Verifica o risco do código e determina a ação de acordo com a seleção do administrador (na parte de CDR). O CDR utiliza diversas técnicas de análise do documento, verificando inclusive de forma heurística os códigos do documento (detectando dessa forma ataques do tipo Fileless/Stealth, Package Malware, Embeded Codes, entre outros);
    c. Ignorar: Ignora o documento e continua com a entrega do mesmo;

Definições de Opções - URL SandBox

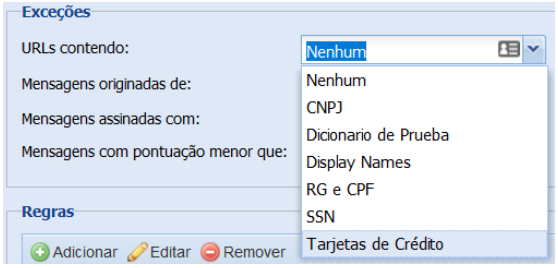
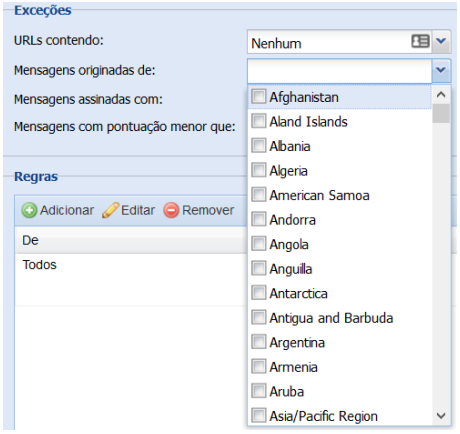
Estas informações descrevem as opções disponíveis na parte de URL SandBox.

Opções	Definição
Registrar reescrita do objeto	Habilita ou não o registro sistema do Ataque Dirigido. Esse registro fica visível em RealTime > Segurança > SandBox, ao qual fica registrado em timeline as ações de cliques dos usuários, tanto em URLs válidas, quanto em URLs contaminadas/maliciosas. O MailInspector acompanha o destinatário na URL reescrita. Quando uma mensagem for dirigida a vários destinatários, o envelope é dividido de modo que existam apenas um receptor associado com uma URL reescrita, dessa forma é possível acompanhar quais usuários clicaram na URL reescrita, mesmo quando o e-mail é destinado a múltiplos destinatários;

Opções	Definição
URL de Reescrita	Define a URL apresentado no link quando é feita a reescrita da URL, dessa forma é possível apontar para um hostname customizável em vez de utilizar o hostname da caixa em si.
Hostname	Indica o hostname apresentada na URL **Obs:** É necessário que essa entrada esteja publicada no DNS da empresa, para que ela faça resolução e redirecione para a console do MailInspector (ou pelo menos interprete pelo proxy reverso) o <hostaname>**/mailinspector/tap/**<ALGUMACOISA>
Protocolo	**HTTP:** Utiliza HTTP para a reescrita **HTTPS:** Utiliza HTTPS para a reescrita



Define as Exceções de reescrita de URL, ou seja, se atender uma das condições abaixo indicadas, a URL não será reescrita.

Exceções	Definição / Opções
URLs contendo:	Indica uma Expressão Regular, ao qual será bloqueada a reescrita de URL, quando for encontrada no e-mail.  Lembrando que Expressão regular pode englobar: • E-mails (tanto destinatário, quanto remetente); • Domínios (destinatário ou remetente); • IP's e Redes; • Faixas de IP's; • Grupos de Usuários; • Listas de distribuição; • Grupos de LDAP; • Display Names;
Mensagens originadas de:	País de origem do e-mail. 
Mensagens Assinadas com:	Ignorar a reescrita de URLS em caso das mensagens estarem assinadas com: • PGP;

	• S/MIME; • DKIM
Mensagens com pontuação menor que:	Ignorar a reescrita de URLS quando as mensagens tiverem uma pontuação menor que a informada.

Definições de Opções - Controle Personalizado URL SandBox

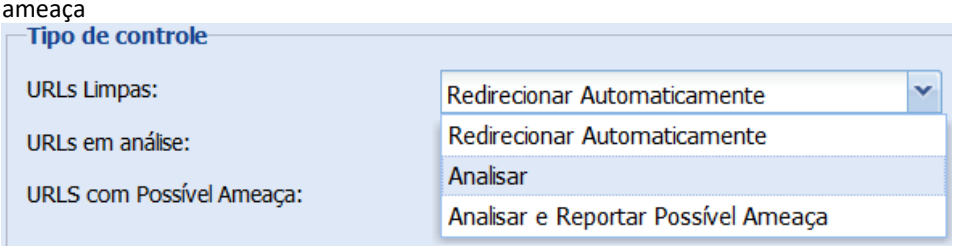
Permite a criação de regras personalizadas a fim de definir quais usuários, e-mail, domínios, grupos LDAP, endereços de IP's, etc, terão a análise ativada e seu comportamento avaliado, bem como a reescrita de URL.

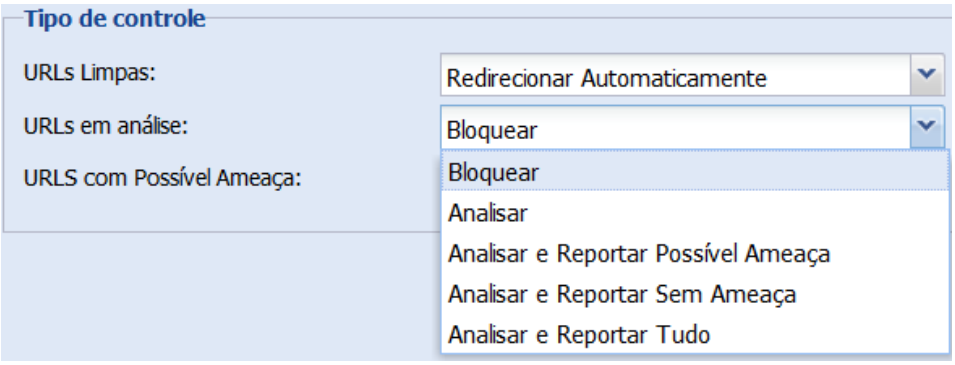
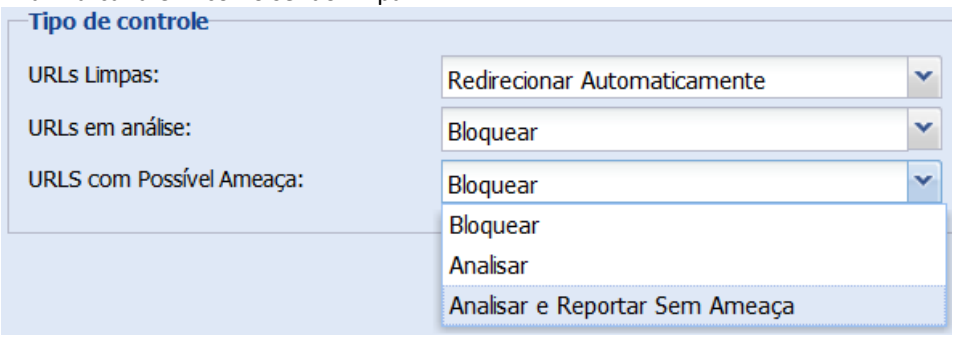
Controle Personalizado	Definição / Opções
De:	Quando o e-mail vier de um determinado grupo de usuários.
Para:	Quando o e-mail estiver destinado para um determinado grupo de usuários
Habilitar Controle:	Habilita ou desabilita a reescrita de URL

Controle Personalizado para URL SandBox

Pode ser criado regras combinando origem (Grupos de Usuários) e destino (Grupos de Usuários) conforme a necessidade do administrador, dessa forma é possível o controle de quais usuários/grupos que terão as URL's reescritas pelo sistema (para poder efetuar a análise On-Click), lembrando que é sempre baseado em DE / PARA (dessa forma englobando a escolha granular de usuários/grupos ou até mesmo de todos os e-mails em rota de inbound, outbound ou ambos).

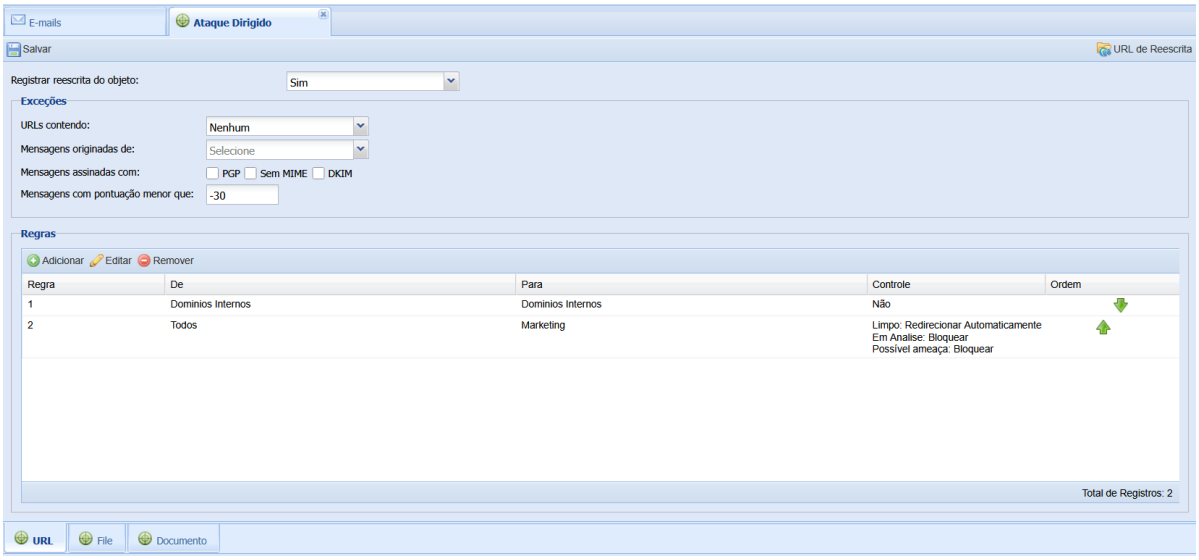
Indica o que deve acontecer quando as URL's atender as seguintes condições:

Tipo de Controle	Ação a ser tomada
URL's Limpas:	**Ações liberadas para o usuário final, quando a URL analisada pelo MailInspector apresentar como limpa.** **Redirecionar Automaticamente:** Redireciona automaticamente a URL destino, sem indicação de observação, ou pop-up para o usuário final **Analisar:** Apresenta a tela de análise de URL **Analisar e Reportar Possível Ameaça:** Permite ao usuário final marcar a URL como ameaça 
URLs em análise:	**Ações liberadas para o usuário final, quando a URL analisada pelo MailInspector apresentar como em análise.** **Bloquear:** Apresenta-se ao usuário final uma tela indicando que a URL está bloqueada e impede ao usuário de acessar a URL **Analisar:** Apresenta a tela de análise de URL

	Analisar e Reportar Possível Ameaça: Apresenta a tela de análise e permite ao usuário final marcar a URL como ameaça **Analisar e Reportar Sem Ameaça:** Apresenta a tela de análise e permite ao usuário final marcar a URL como sendo limpa **Analisar e Reportar Tudo:** Apresenta a tela de análise e permite ao usuário reportar tudo 
URLs com Possível Ameaça:	**Ações liberadas para o usuário final, quando a URL analisada pelo MailInspector apresentar como possível ameaça.** **Bloquear:** Apresenta-se ao usuário final uma tela indicando que a URL está bloqueada e impede ao usuário de acessar a URL **Analisar:** Apresenta a tela de análise de URL **Analisar e Reportar Sem Ameaça:** Apresenta a tela de análise e permite ao usuário final marcar a URL como sendo limpa 

Definições de Opções de Colunas – URL SandBox

Coluna	Objetivo da Coluna
Regra	Número da regra criada
De	Grupo de Origem do TAP
Para	Grupo de Destino do TAP
Controle	Tipo de Controle conforme explicado no item anterior
Ordem	Sequência a ser obedecida na execução do TAP



Definições de Opções - File SandBox

Quando habilitado, o HSC SmartDefender File SandBox irá analisar os arquivos suspeitos em uma área de memória reservada e isolada, fazendo a engenharia reversa do arquivo, chegando ao código fonte para análise (SandBox Estático), que é efetuada localmente no próprio appliance.

Após o processo do SandBox Estático, é efetuada uma segunda etapa de análise (SandBox Dinâmico), ao qual é efetuada a execução do arquivo em uma área reservada e protegida da memória. Essa análise pode ser tanto local, quanto na nuvem da HSCBRASIL, deixando a cargo do administrador essa opção de escolha.

Caso o administrador opte por autorizar o envio do arquivo para HSCBRASIL, o arquivo é mandado para um ambiente controlado ao qual ele é executado e efetuado todas as análises comportamentais e análise do código na memória (SandBox Dinâmico). Uma vez verificado o comportamento dele, é registrado o Hash (metadado) do arquivo no BigData para futuras consultas, dessa forma detectando e classificando dinamicamente novas origens de spams/phishings. Após o registro do hash, o arquivo analisado é apagado da memória do SandBox, sem deixar qualquer vestígio. Todo esse processo é feito de forma anônima, ou seja, não tem como efetuar a identificação do arquivo ou de sua origem, garantindo segurança máxima e privacidade, dessa forma atendendo a legislação brasileira.

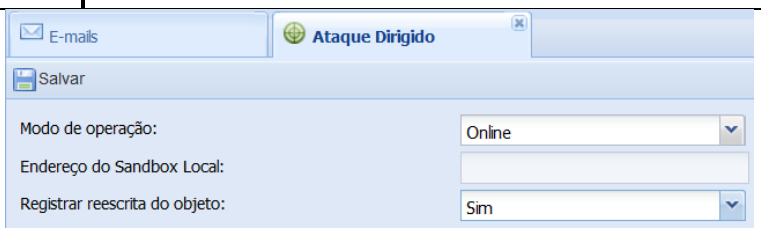
Se for optada o uso do SandBox local, o arquivo não é enviado a HSCBRASIL, ficando a análise para o appliance indicado pelo administrador.

O File SandBox gera um link HTML no lugar do arquivo. O usuário ao clicar neste link, é feita verificação do arquivo em tempo real antes de liberar para o usuário, ao qual é verificado o comportamento (atualizado com o último pacote de sistema de análise). Caso não seja detectado nenhuma anomalia, o arquivo é liberado para utilização. Caso seja identificada alguma anomalia, é efetuado o bloqueio do arquivo.

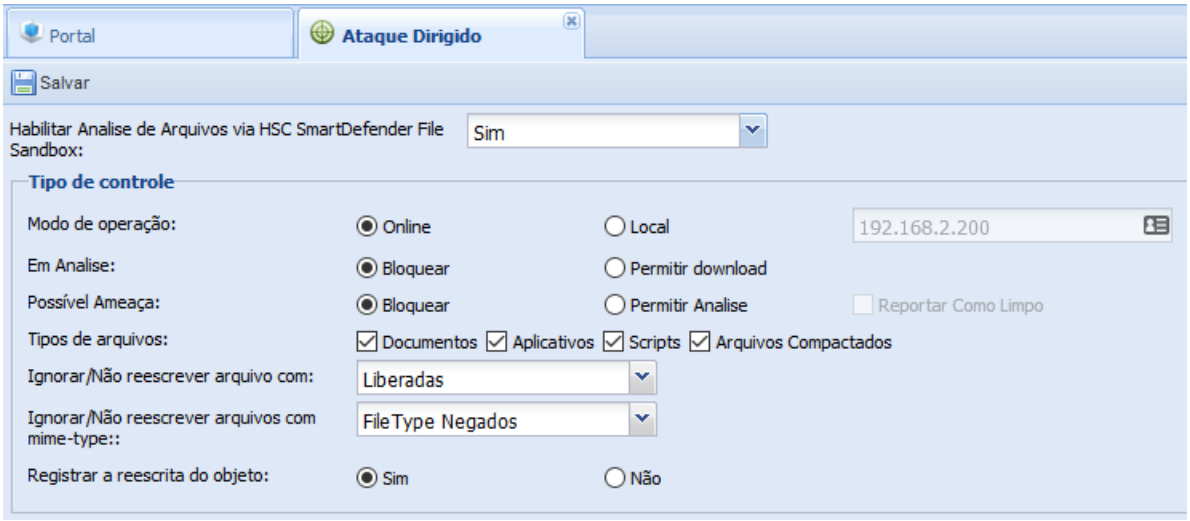
Os arquivos analisados no File SandBox, são analisados em tempo real e o sistema identifica ataques usando as mais avançadas técnicas de detecção de comportamento, identificando malwares, vírus, etc, usando heurística para detecção de anomalias sem assinaturas.

Obs: Todo o processo de File SandBox segue as normativas internacionais de segurança (tais como GDPR, SOX, entre outras) e também a legislação brasileira (mais especificamente LGPD – Lei Geral de Proteção de Dados - nº 13.709/2018) em toda a sua plenitude.

Tipo de controle	Definição / Opções
Modo de Operação	**Online**: Indica que o SandBox será operado na nuvem da HSCBRASIL **Local:** Indica que será operado a nível local (no próprio appliance do cliente). É necessário indicar o IP da máquina que fará a análise do SandBox.
Endereço do SandBox Local:	Indica o IP/hostname da caixa configurada para o processamento do SandBox local.
Registra reescrita do objeto	Registra a reescrita do FileSandBox.

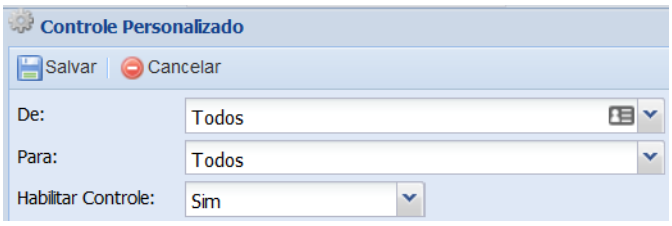
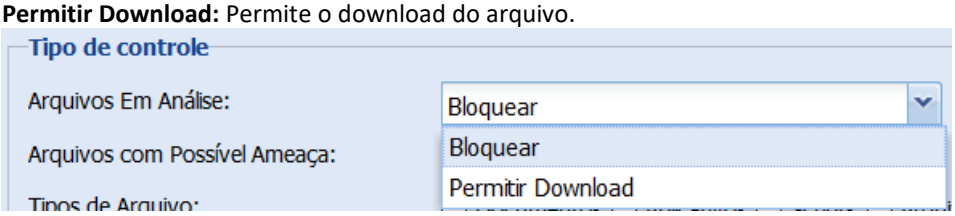


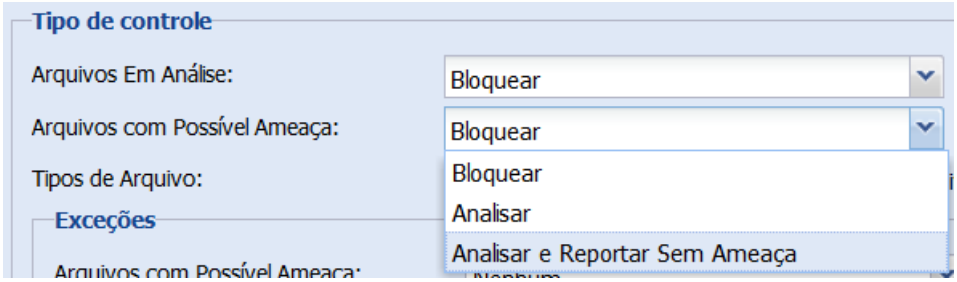
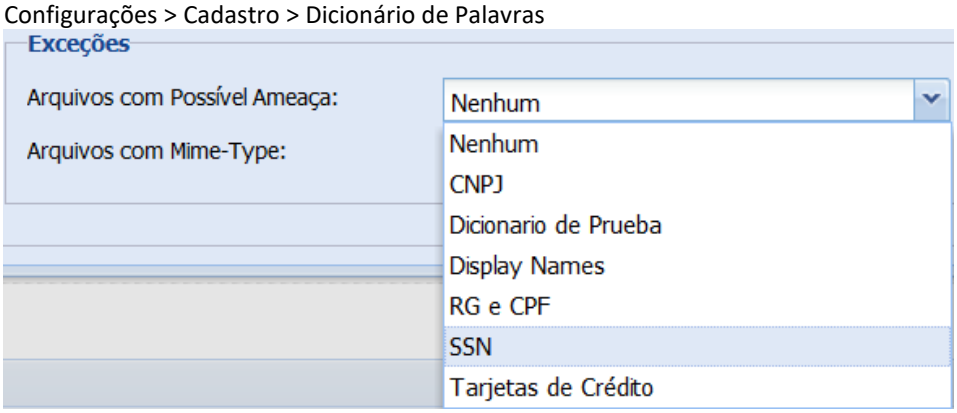
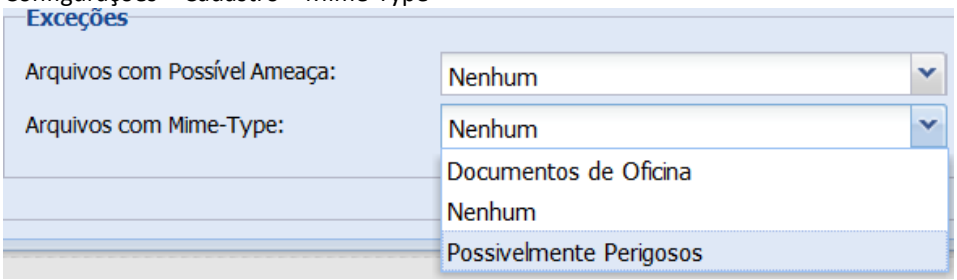
Regras	Definição / Opções
Em análise	Opções disponíveis caso o sistema de Ataque Dirigido detecte que a mensagem está para análise: Bloquear, Permitir download.
Possível ameaça	Opções disponíveis caso o sistema de Ataque Dirigido detecte que a mensagem está como possível ameaça: Bloquear ou Permitir análise, opcionalmente pode Reportar sem ameaça caso permita análise.
Tipos de Arquivos	Poderá ser selecionado os seguintes tipos arquivos que serão enviados para análise: • Documentos; • Aplicativos; • Scripts; • Arquivos compactados
Ignorar/Não reescrever arquivo com:	Grupo de Anexos. Esse grupo de anexos, pode ser criado em: Configurações > Cadastro > Grupo de Anexos
Ignorar/Não reescrever arquivos com mime-type:	Grupo de Mime-Types. Esse grupo de mime-types, pode ser criado em: Configurações > Cadastro > Mime-Type/Fingerprint



Definições de Opções - Controle Personalizado File SandBox

Esta tela permite a criação de regras personalizadas a fim de definir quais usuários, e-mails, domínios, etc, terão a análise ativada e seu comportamento. Pode ser criado regras combinando origem e destinos conforme a necessidade do administrador.

Opções	Definição
De	Grupo de usuários criados para origem.
Para	Grupo de usuários criados para destino.
Habilitar Controle	**Sim:** Habilita o controle do Ataque Dirigido para File SandBox. **Não:** Não habilita o controle do Ataque Dirigido para File SandBox.
	
Arquivos em Análise:	Opções disponíveis caso o sistema de Ataque Dirigido detecte que a mensagem está para análise: **Bloquear:** Bloqueia o arquivo **Permitir Download:** Permite o download do arquivo. 
Arquivos com Possível Ameaça:	Opções disponíveis caso o sistema de Ataque Dirigido detecte que a mensagem está como possível ameaça: **Bloquear:** bloqueia o arquivo sem permitir o acesso do mesmo ao usuário final. **Analisar:** Permite análise.

	Analisar e reportar sem ameaça: Abre a possibilidade do usuário final reportar que o arquivo não possui ameaça. 
Tipos de Arquivos	Poderá ser selecionado os seguintes tipos arquivos que serão enviados para análise: • Documentos; • Aplicativos; • Scripts; • Arquivos compactados
Exceções	Ignora o uso do SandBox File quando alguma condição abaixo é atendida
Arquivos com Possível Ameaça:	Esta função ignora a análise do arquivo quando detectado palavras chaves nele, dessa forma é possível criar um dicionário de palavras e ao casar com algum termo no arquivo, o mesmo não será verificado. Grupo de Dicionário de Palavras. Esse grupo de palavras, pode ser criado em: Configurações > Cadastro > Dicionário de Palavras 
Arquivos com Mime-Type:	Esta função ignora a análise do arquivo quando detectado que casam com o Mime-Type indicado, dessa forma é possível criar um grupo de tipos de arquivo, ao qual não será verificado no File SandBox. Grupo de Mime-Type. Esse grupo de arquivos, pode ser criado em: Configurações > Cadastro > Mime-Type 

Definições de Opções - Documento

Quando habilitado, o(s) documento(s) (Documentos MS Office, Apache Open Office, Libre Office, OnlyOffice, Calligra Suite, PDF, entre outros documentos padrão de escritório) será(ão) analisado(s) e tomada a ação de acordo com a seleção do administrador da ferramenta.

O MailInspector permite a criação de regras personalizadas a fim de definir quais usuários, e-mail, domínios, etc, terão a parte de CDR ativado. Pode ser criado regras combinando origem e destinos conforme a necessidade do administrador.

Opções	Definição
De	Grupo de usuários criados para origem.
Para	Grupo de usuários criados para destino.
Habilitar Controle	**Sim:** Habilita o controle de Documentos do Tipo Office. **Não:** Não habilita o controle de Documentos do Tipo Office.

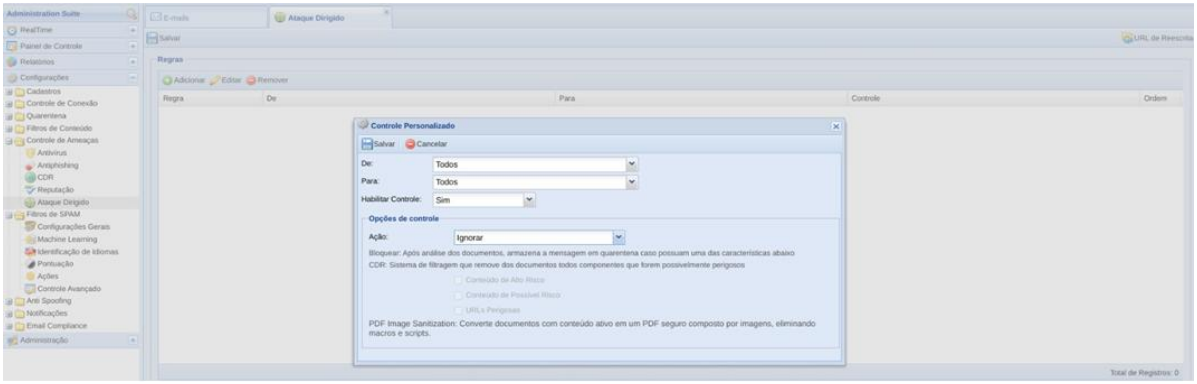
Tipo de controle	Definição / Opções
Ação	**Bloquear:** Efetua a análise e de acordo com o que for encontrado, será bloqueado. O bloqueio do documento será efetuado quando for detectado os seguintes tipos de código nele (selecionado de acordo com o critério do administrador): • Conteúdo de Alto Risco; • Conteúdo de Possível Risco; • URL's Perigosas; **CDR:** Irá analisar os arquivos do tipo Documento em busca de códigos e tomada a ação de acordo com a configuração efetuada na parte de CDR do sistema. No CDR uma vez detectado algum código ou URL, o mesmo é analisado de forma heurística e por assinaturas, para busca de conteúdo possivelmente perigosos e eliminando-os. A análise consiste em filtragem para remoção de todos os componentes possivelmente perigosos nos documentos analisados, desativando dessa forma possíveis conteúdos maliciosos ataques Zero-Day/Zero Hour e entregando um documento limpo sem as ameaças do tipo: • Macro; • DDE; • Imagens Pornográficas; • Scripts (VBScript, PowerShell, etc); • Hyperlinks; • Embedded Media; • Embedded Objects; • Packaged Malwares; • Stealth techniques; • Entre outros; **Ignorar:** Não efetua ação alguma, mesmo se for encontrado códigos com possíveis ameaças, dessa forma ignora completamente os conteúdos perigosos e de alto risco, prosseguindo com a entrega;

PDF Image Sanitization

A funcionalidade PDF Image Sanitization substitui documentos em anexo no e-mail que contenham conteúdo ativo — como macros, scripts, DDL ou elementos executáveis — por um PDF seguro, no qual todo o conteúdo é convertido em imagem, eliminando qualquer possibilidade de execução de código malicioso.
A funcionalidade PDF Image Sanitization adiciona uma camada avançada de proteção ao tratar anexos potencialmente perigosos, como documentos que contenham macros, scripts, DDL, elementos executáveis, campos dinâmicos ou qualquer conteúdo ativo capaz de executar ações automáticas no dispositivo do usuário.

Quando ativado, o MailInspector analisa todos os anexos suportados (como arquivos Microsoft Office, OpenDocument e outros formatos conhecidos por possibilitar conteúdo ativo). Caso o documento apresente algum tipo de risco, ele não é entregue ao usuário final em sua forma original.

Em vez disso, o MailInspector realiza automaticamente a conversão do documento para um PDF seguro, no qual o conteúdo é reproduzido como imagem dentro das páginas.
Este formato impede a execução de qualquer macro, script ou comando embutido, garantindo que apenas o conteúdo visual seja preservado.



Controle personalizado sobre Anexos padrão Documentos Office.

Imagens de exemplo de avisos - Telas Ataque Dirigido

Todas as telas podem ser customizadas com as logomarcas e textos de sua empresa.

Possível fraude ou possível ameaça detectada.

Página exemplo com nenhuma ameaça detectada.

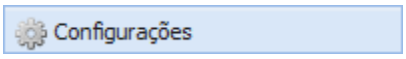
Página com nenhuma ameaça detectada, porém, existem 3 interações de usuários sobre o conteúdo deste e-mail/URL

Página com descrição dos campos do módulo de Ataque Dirigido

Filtros de SPAM

Configurações Gerais

Use esta página para exibir, adicionar, editar ou excluir configurações gerais do Filtro de SPAM.



/ Filtros de SPAM / Configurações Gerais

Visão geral das configurações gerais

Neste item é possível ativar ou desativar as filtragens de SPAM, consultas à Blacklists externas "RBLS" e outros. Podendo criar controles globais ou por grupos da ferramenta, controlando entrada ou saída dos e-mails.

Ainda é possível efetuar múltiplas ações quando o e-mail é classificado como PROVÁVEL SPAM ou SPAM, dentre eles:

- Bloquear o e-mail;
- Modificar a mensagem;
- Remover o anexo (caso contenha anexo);
- Reter em quarentena (inclusive podendo ser quarentena customizada pelo administrador);
- Excluir o e-mail;
- Notificar destinatário e/ou remetente do e-mail;
- Prosseguir com a entrega do e-mail;
- Rejeitar futuras conexões do IP de origem do e-mail;

Definições de Opções - Configurações Gerais

Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição
Salvar	Quando clicado, grava as configurações realizadas.

Definições de Opções - Aba Filtro Anti-Spam

Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição
Ativar Filtragem Anti-Spam	Escolha entre: • **Sim** - Indica que o sistema de filtragem anti-spam está ativo. Esta funcionalidade gerencia todos os recursos de filtragem anti-spam. • **Não** - Indica que o sistema de filtragem anti-spam está desativado. ⚠ Se este recurso for desativado, nenhuma filtragem de SPAM será realizada.
Tamanho Máximo de uma Mensagem para	Permite que seja definido o tamanho máximo de uma mensagem para que a filtragem anti-spam seja realizada.

ser Filtrada pelo Anti Spam	
Adicionar	Cadastra uma nova regra de filtragem anti-spam. Quando clicado, abre a caixa de diálogo **Cadastro do Controle Personalizado**.
Editar	Edita as configurações de um registro existente. Quando clicado, abre a caixa de diálogo **Cadastro do Controle Personalizado**.
Remover	Quando clicado, exclui o registro selecionado.

Definições de Opções - Cadastro do Controle Personalizado

Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição
Adicionar	Quando clicado, adiciona o controle personalizado.
Cancelar	Quando clicado, cancela a ação.
De	Selecione o grupo pré-cadastrado de remetentes.
Para	Selecione o grupo pré-cadastrado de destinatários.
Ação	Escolha entre: • **Sim** - Indica que os filtros de SPAM serão aplicados para esta regra. • **Não** - Indica que os filtros de SPAM não serão aplicados para esta regra.

Definições de Opções - Aba RBLs Externas

Ativa ou desativa RBL's previamente cadastradas para uso no MailInspector em nível de processamento.

Opções	Definição
Ativar Checagem nas RBLs Externas	Escolha entre: • Selecione quais RBL's externas serão consultadas. ⚠ Caso queira cadastrar uma nova RBL para consulta use a tela: Configurações > Cadastros > RBLs Externas
Número de RBLs para ser SPAM	Aqui você deve indicar ao sistema quantas RBLs devem casar para que o sistema a considere como um SPAM.

Definições de Opções - Cadastro do Controle Personalizado

Estas informações descrevem as opções disponíveis nesta página.

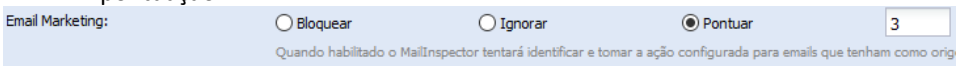
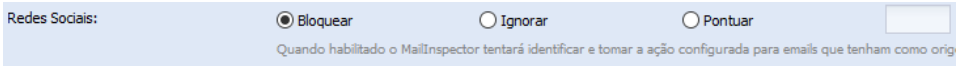
Opções	Definição
Adicionar	Quando clicado, adiciona o controle personalizado.
Cancelar	Quando clicado, cancela a ação.
De	Selecione o grupo pré-cadastrado de remetentes.

Para	Selecione o grupo pré-cadastrado de destinatários.
Ação	Escolha entre: • **Sim** - Indica que a regra será aplicada, quando os remetentes e os destinatários pertencerem aos grupos selecionados. • **Não** - Indica que a regra não será aplicada, quando os remetentes e os destinatários pertencerem aos grupos selecionados. • **Blacklists** - Permite selecionar as Blacklists que serão ativadas na regra.

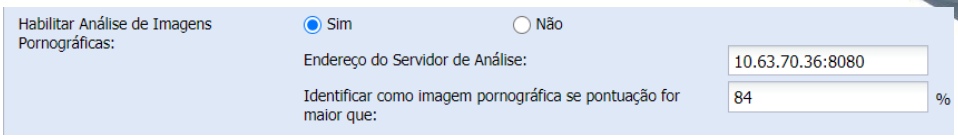
Definições de Opções - Aba Controles Adicionais

Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição
Free Mail	Permite identificar o uso de servidores de e-mails gratuitos no envio de e-mails. As ações possíveis para esta função são: • **Bloquear:** As mensagens classificadas serão BLOQUEADAS e não serão entregues para o destinatário, ficando a cargo do administrador liberar a mensagem quando necessário pela interface de administração. As mensagens ficarão retidas na quarentena mesmo que exista uma entrada na Allow List de SPAM; • **Ignorar:** Ignora o filtro e não toma nenhuma ação; • **Pontuar:** Adiciona o número de pontos informado ao sistema de SPAM e identifica a classe da mensagem na interface de administração. Conforme for configurado as mensagens podem ou não ficar retida na quarentena, dependendo da pontuação final da mensagem. Caso exista uma entrada na Allow List de SPAM, a mesma não receberá pontuação. Free Mail: ○ Bloquear ◉ Ignorar ○ Pontuar Permite identificar o uso de e-mails gratuitos no envio de e-mails.
Whitelist Automática	Sistema que permite identificar automaticamente contatos internos dos usuários. O MailInspector identifica mensagens em que o remetente for interno com destino para um e-mail externo, desta forma quando o mesmo contato externo responder o e-mail o sistema irá automaticamente identificar este contato e executar a ação configurada, para pontuação e dias. As ações possíveis para esta função são: • **Ignorar:** Ignora o filtro e não toma nenhuma ação; • **Pontuar:** Adiciona o número de pontos informado ao sistema de SPAM e identifica a classe da mensagem na interface de administração. Conforme for configurado as mensagens podem ou não ficar retida na quarentena, dependendo da pontuação final da mensagem. Caso exista uma entrada na Allow List de SPAM, a mesma não receberá pontuação. • **Tempo de Ativação:** Quantidade em dias que o remetente estará incluso na whitelist automática. Whitelist Automática: ○ Ignorar ◉ Pontuar -2 Tempo de Ativação 5 dia(s)
E-mail Marketing	Quando habilitado o MailInspector tentará identificar e tomar a ação configurada para e-mails que tenham como origem sistema de E-mail Marketing.

	As ações possíveis para esta função são: • **Bloquear:** As mensagens classificadas serão BLOQUEADAS e não serão entregues para o destinatário, ficando a cargo do administrador liberar a mensagem quando necessário pela interface de administração. As mensagens ficarão retidas na quarentena mesmo que exista uma entrada na Allow List de SPAM; • **Ignorar:** Ignora o filtro e não toma nenhuma ação; • **Pontuar:** Adiciona o número de pontos informado ao sistema de SPAM e identifica a classe da mensagem na interface de administração. Conforme for configurado as mensagens podem ou não ficar retida na quarentena, dependendo da pontuação final da mensagem. Caso exista uma entrada na Allow List de SPAM, a mesma não receberá pontuação. 
Redes Sociais	Quando habilitado o MailInspector tentará identificar e tomar a ação configurada para e-mails que tenham como origem sistema de Redes Sociais, tais como: Facebook, Twitter, Linkedin, Google Plus, Instagram, etc... As ações possíveis para esta função são: • **Bloquear:** As mensagens classificadas serão BLOQUEADAS e não serão entregues para o destinatário, ficando a cargo do administrador liberar a mensagem quando necessário pela interface de administração. As mensagens ficarão retidas na quarentena mesmo que exista uma entrada na Allow List de SPAM; • **Ignorar:** Ignora o filtro e não toma nenhuma ação; • **Pontuar:** Adiciona o número de pontos informado ao sistema de SPAM e identifica a classe da mensagem na interface de administração. Conforme for configurado as mensagens podem ou não ficar retida na quarentena, dependendo da pontuação final da mensagem. Caso exista uma entrada na Allow List de SPAM, a mesma não receberá pontuação. 
GrayMail	**Graymail** São mensagens legítimas, porém de baixo interesse para o usuário, como newsletters, notificações diversas, campanhas de marketing, promoções, atualizações automáticas ou comunicações não essenciais. Embora não representem ameaça direta, esses e-mails podem gerar sobrecarga na caixa de entrada. As mensagens são do tipo boletins informativos/Newsletters, que alguns usuários valorizam e outros preferem bloquear. Muitos consideram graymails como SPAMS autorizados pelos usuários, que ao se cadastrarem em alguma lista, passam a receber propagandas “autorizadas” e informativos. O MailInspector detecta e interpreta GrayMail como BulkMail, que seguem o mesmo princípio e conta com quarentena específica para esse tipo de e-mail. A funcionalidade de Graymail do MailInspector permite que o administrador escolha como essas

	mensagens devem ser tratadas no fluxo de análise, de forma totalmente automática e personalizada. As ações possíveis para esta função são: • **Bloquear:** Quando selecionado, todos os e-mails identificados como possíveis Graymail **são bloqueados**, impedindo que cheguem à caixa do usuário. Essa opção é recomendada para ambientes que exigem foco extremo, alta produtividade ou políticas rígidas de recebimento; • **Ignorar:** Nessa opção, o MailInspector **desconsidera a classificação de Graymail**, permitindo que a mensagem seja tratada normalmente pelo restante das regras e heurísticas do antispam. O e-mail segue o fluxo padrão, sem penalização ou alteração de reputação; • **Pontuar:** Quando configurado para pontuar, o MailInspector **atribui uma pontuação específica** aos e-mails classificados como Graymail. Essa pontuação contribui para o cálculo final de reputação da mensagem, aumentando a chance de que o e-mail seja encaminhado para quarentena, marcado como aviso ou priorizado como mensagem de baixa relevância — conforme a política geral da organização. GrayMail ○ Bloquear ◉ Ignorar ○ Pontuar Quando habilitado o MailInspector tentará identificar e tomar a ação configurada para emails que sejam classificados como possíveis GrayMails.
Conteúdo Adulo	Quando habilitado o sistema tentará identificar e-mails com conteúdo adulto/pornográfico. As ações possíveis para esta função são: • **Bloquear:** As mensagens classificadas serão BLOQUEADAS e não serão entregues para o destinatário, ficando a cargo do administrador liberar a mensagem quando necessário pela interface de administração. As mensagens ficarão retidas na quarentena mesmo que exista uma entrada na Allow List de SPAM; • **Ignorar:** Ignora o filtro e não toma nenhuma ação; • **Pontuar:** Adiciona o número de pontos informado ao sistema de SPAM e identifica a classe da mensagem na interface de administração. Conforme for configurado as mensagens podem ou não ficar retida na quarentena, dependendo da pontuação final da mensagem. Caso exista uma entrada na Allow List de SPAM, a mesma não receberá pontuação. Conteúdo Adulto: ○ Bloquear ○ Ignorar ◉ Pontuar 10 Quando habilitado o sistema tentará identificar emails com conteúdo adulto/pornográfico.
Habilitar Análise de Imagens Pornográficas	Ativa a análise de imagens contidas nos e-mails (mesmo em anexos compactados), detectando se os mesmos são imagens de nudez e/ou pornografia. Para esse tipo de análise, é necessária uma ou mais máquina(s) específica para esse fim. • **Sim:** Ativa a análise de imagem de nudez/pornografia; • **Não:** Ignora a existência de imagens pornográficas/nudez em e-mails; • **Endereço do Servidor de Análise:** Indique o IP da máquina de análise (se for mais de uma máquina, basta coloca-los em cluster e indicar o IP VIP). • **Identificar como imagem pornográfica se pontuação for maior que:** Indicação de percentual de cobertura de "pele" para ser considerado nudez ou pornografia. Geralmente com 80% já é possível detectar imagens de nudez e com 84% ou 85%, imagens de pornografia.



E-mail Reputation

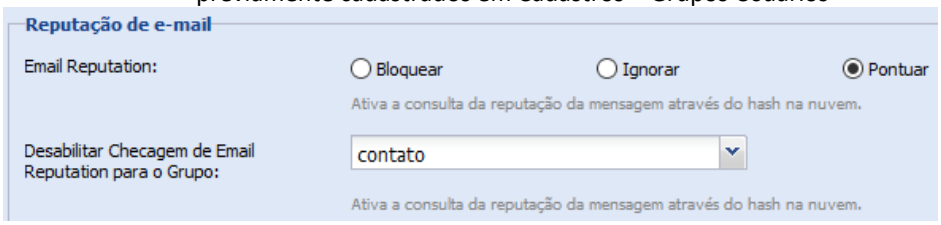
A análise de reputação do e-mail, se dá por dois métodos:

10. **Consulta em Biga Data:** Faz a consulta da reputação da mensagem através do "Hash/Fuzzy Hash" (metadado) do BigData na nuvem da HSCBRASIL e;
11. **Inteligência artificial:** A análise compara todo o histórico e frequência de envio da origem dos e-mails (frequência de envio, quantidade média de e-mails enviados, tipo de e-mail enviado, etc).

Dessa forma, ela junta tanto os dados de BigData como os dados comportamentais resultando em uma análise completa da reputação do e-mail.

As ações possíveis para esta função são:

- **Bloquear:** As mensagens classificadas serão BLOQUEADAS e não serão entregues para o destinatário, ficando a cargo do administrador liberar a mensagem quando necessário pela interface de administração.
  As mensagens ficarão retidas na quarentena mesmo que exista uma entrada na Allow List de SPAM;
- **Ignorar:** Ignora o filtro e não toma nenhuma ação;
- **Pontuar:** Adiciona o número de pontos informado ao sistema de SPAM e identifica a classe da mensagem na interface de administração. Conforme for configurado as mensagens podem ou não ficar retida na quarentena, dependendo da pontuação final da mensagem.
  Caso exista uma entrada na Allow List de SPAM, a mesma não receberá pontuação.
  - **Desabilitar Checagem de E-mail Reputation para o Grupo:** É possível desativar este filtro para determinados grupos de usuários previamente cadastrados em Cadastros > Grupos Usuários



Machine Learning

Use esta página para exibir, adicionar, editar ou excluir configurações filtro Machine Learning e ao filtro bayesiano.

Configurações **/ Filtros de SPAM / Machine Learning**

Visão geral de Machine Learning

O HSC MailInspector possui um sistema avançado de detecção de SPAM e novas ameaças baseado em um sistema local de auto aprendizado. Ele capaz de lidar com um enorme volume de dados e processar informações que identificam a atividade de e-mails da sua corporação, aprendendo dinamicamente o que são e-mails confiáveis e o que são e-mails suspeitos, agindo de forma automática na prevenção de Surtos de vírus, spam e phishings.

O sistema usa algoritmos avançados de análise textuais para identificar anomalias de e-mails. Quando mais se usa o sistema, mais ele aprende e melhora seu resultado e assertividade, dessa forma aumentando a capacidade da tecnologia de Machine Learning Database.

A inferência Bayesiana permite uma eficaz filtragem preditiva de mensagens, através de palavras-chave com um número reduzido de falso positivos. Definindo um limiar conservador, ainda assim grande parte das mensagens consideradas SPAM não são entregues diretamente para os usuários, sendo bastante improvável que uma mensagem seja erroneamente classificada como SPAM, o que seria improvável se fossem utilizados outros tipos de filtros. Este sistema é alimentado com informações dinamicamente ou manualmente, permitindo que o sistema se adapte as necessidades de cada empresa, auxiliando a identificar e-mails que para uma determinada empresa possa ser SPAM e para outras não.

Definições de Opções – Machine Learning

Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição
Salvar	Quando clicado, grava as configurações realizadas.
Limpar Base	Quando clicado, limpa a base de conhecimento coletado através das amostras no sistema de Machine Learning.
Ativar	Escolha entre: • **Sim** - Indica que o filtro Machine Learning (bayes) está ativo. • **Não** - Indica que o filtro Machine Learning (bayes) está desativado. O Machine Learning/Filtro Bayesiano é um poderoso recurso na identificação e classificação de SPAM, recomendamos que este recurso esteja ativo.
Tempo de Expiração	Permite definir o tempo de expiração das entradas menos utilizadas e/ou mais antigas da base de consulta do Machine Learning.
Pontuação Confiável	Permite definir a pontuação que será atribuída a mensagens consideradas pelo filtro do Machine Learning com menor probabilidade de serem SPAM: • **0 -> 4** - Mensagens classificadas com índice de probabilidade de 0% a 4%. • **5 -> 19** - Mensagens classificadas com índice de probabilidade de 0% a 4%.

	• **20 -> 39** - Mensagens classificadas com índice de probabilidade de 0% a 4%. • **40 -> 49** - Mensagens classificadas com índice de probabilidade de 0% a 4%.
Pontuação SPAM	Permite definir a pontuação que será atribuída a mensagens consideradas pelo filtro do Machine Learning com maior probabilidade de serem SPAM: • **50 -> 59** - Mensagens classificadas com índice de probabilidade de 50% a 59%. • **60 -> 69** - Mensagens classificadas com índice de probabilidade de 60% a 69%. • **70 -> 79** - Mensagens classificadas com índice de probabilidade de 70% a 79%. • **80 -> 94** - Mensagens classificadas com índice de probabilidade de 80% a 94%. • **95 -> 98** - Mensagens classificadas com índice de probabilidade de 95% a 98%. • **99 -> 100** - Mensagens classificadas com índice de probabilidade de 99% a 100%.
Auto Aprendizado	Permite definir a pontuação que será utilizada para o auto aprendizado do filtro do Machine Learning: • **Confiável menor que** - Mensagens que atingirem uma pontuação menor do que a informada, terão suas características assimiladas como confiáveis. • **SPAM maior que** - Mensagens que atingirem uma pontuação maior do que a informada, terão suas características assimiladas como SPAM.
Estatísticas	Apresenta as estatísticas do sistema de Machine Learning e Análise Bayesiana dos E-mails. • **Quantidade de mensagens aprendidas como Provável Spam / Spam:** Indica a quantidade de mensagens aprendidas como provável spam/spam no prazo da presente data até o prazo de expiração, configurado pelo administrador. • **Quantidade de mensagens aprendidas como Não Spam:** Indica a quantidade de mensagens apresndidas como NÃO spam no prazo da presente data até o prazo de expiração, configurado pelo administrador. • **Quantidade de tokens analisados:** Indica a quantidade de tolkens/hashes gerados e comparados com a sua base de conhecimento (base de conhecimento local gerado pelo sistema de Machine Learning) e dos novos hashes aprendidos pelo sistema de Machine Learning.

Identificação de Idiomas

Use esta página para exibir ou editar a configuração de idiomas de mensagens suportados pelo HSC MailInspector.

Configurações **/ Filtros de SPAM / Identificação de Idiomas**

Visão geral da identificação de idiomas

Através da Identificação de Idiomas, o HSC MailInspector é capaz de identificar mensagens "Expanded 8-bit character set (double-byte)", (exemplo UTF-8, UTF-16) e em qual idioma uma mensagem foi escrita, é possível atribuir uma pontuação as mensagens que contenham linguagens identificadas pelo usuário como não suportadas pelo HSC MailInspector, a fim de impedir o recebimento de SPAM ou de mensagens indesejadas oriundas de outros países.

Definições de Opções - Identificação de Idiomas

Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição
Salvar	Quando clicado, grava as configurações realizadas.
Pontuação para mensagens com idiomas não suportados	Informe o valor da pontuação atribuída as mensagens que contenham idiomas que não foram selecionados como suportados.
Selecione os idiomas suportados	Selecione os idiomas suportados. Por padrão, todos os idiomas são suportados.

Lista de Idiomas Suportados

- Afrikaans
- Albanês
- Alemão
- Amárico
- Árabe
- Armênio
- Basco
- Bielo-Rússia
- Bósnio
- Búlgaro
- Catalão
- Chinês (Simplificado apenas)
- Chinês (Tradicional apenas)
- Chinês (tradicional e simplificado)
- Coreano
- Croata
- Dinamarquês
- Escocês
- Eslovaco
- Esloveno
- Espanhol
- Esperanto
- Estoniano
- Finlandês
- Francês
- Frísio
- Gaélico escocês
- Gaélico irlandês
- Galês
- Georgiano
- Grego
- Hebraico
- Hindi
- Holandês
- Húngaro
- ídiche
- Indonésio
- Inglês
- Islandês
- Italiano
- Japonês
- Latim
- Letão
- Lituano
- Malaio
- Marathi
- Nepali
- Norueguês
- Persa
- Polonês
- Português
- Quechua
- Reto-romance
- Romeno
- Russo
- Sânscrito
- Sérvio
- Sueco
- Swahili
- Tagalog
- Tâmil
- Tcheco
- Thai
- Turco
- Ucraniano
- Vietnamita

Pontuação

Use esta página para exibir, adicionar, editar ou excluir configurações de pontuação do Filtro de SPAM.

Configurações **/ Filtros de SPAM / Pontuação**

Visão geral do sistema de pontuação

O HSC MailInspector trabalha com um sistema de pontuação heurística para definição se uma mensagem é SPAM ou não.

Estas pontuações são atribuídas por cada componente da ferramenta, de forma incremental, a fim de melhor classificar uma mensagem como sendo SPAM.

Através desta sessão é possível efetuar ajustes finos na sensibilidade, conforme a necessidade de cada empresa, a fim de tornar a ferramenta mais eficaz ao seu ambiente de e-mails. Em geral, não se faz necessário modificar tais configurações, as pontuações padrões foram amplamente testadas nos mais diversos ambientes empresarias.

Obs: Caso seja necessário efetuar ajustes, tenha em mente que os mesmos podem impactar no recebimento das mensagens.

Definições de Opções - Pontuação

Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição
Salvar	Quando clicado, grava as configurações realizadas.

Definições de Opções - Aba Provável SPAM

Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição
Pontuação Mínima para ser Considerado Provável SPAM	Permite que seja definida a pontuação mínima que uma mensagem deve obter para que seja classificada como provável SPAM.
Adicionar	Cadastra uma nova regra de pontuação para provável SPAM. Quando clicado, abre a caixa de diálogo **Cadastro do Controle Personalizado**.
Editar	Edita as configurações de um registro existente. Quando clicado, abre a caixa de diálogo **Cadastro do Controle Personalizado**.
Remover	Quando clicado, exclui o registro selecionado.

Definições de Opções - Aba SPAM

Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição
Pontuação Mínima para ser Considerado Provável SPAM	Permite que seja definida a pontuação mínima que uma mensagem deve obter para que seja classificada como SPAM.
Adicionar	Cadastra uma nova regra de pontuação para SPAM. Quando clicado, abre a caixa de diálogo **Cadastro do Controle Personalizado**.
Editar	Edita as configurações de um registro existente. Quando clicado, abre a caixa de diálogo **Cadastro do Controle Personalizado**.
Remover	Quando clicado, exclui o registro selecionado.

Definições de Opções - Cadastro do Controle Personalizado

Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição
Adicionar	Quando clicado, adiciona o controle personalizado.
Cancelar	Quando clicado, cancela a ação.
De	Selecione o grupo pré-cadastrado de remetentes.
Para	Selecione o grupo pré-cadastrado de destinatários.
Ação	Escolha entre: • **Pontuação** - Indica a pontuação que será aplicada a regra, quando os remetentes e os destinatários pertencerem aos grupos selecionados.

Definições de Opções - Aba Perfil dos Usuários

Nesta tela o administrador definir os perfis de filtragem e sensibilidade do sistema de AntiSpam que estarão disponíveis para que o usuário personalize suas configurações. Uma vez que o administrador defina os perfis de sensibilidade, os usuários poderão selecionar qual perfil mais adequado para ele.

Sensibilidade	Definição
Permissivo	Permite ao administrador definir uma pontuação para o perfil mais **PERMISSIVO**. Por padrão este perfil vem configurado para 7 pontos
Normal	Permite ao administrador definir uma pontuação para o perfil **NORMAL**. Por padrão este perfil vem configurado para 6 pontos
Restritivo	Permite ao administrador definir uma pontuação para o perfil mais **RESTRITIVO**. Por padrão este perfil vem configurado para 5 pontos

Ações

Use esta página para exibir, adicionar, editar ou excluir configurações das ações do Filtro de SPAM.

Configurações **/ Filtros de SPAM / Ações**

Visão geral das ações aplicadas aos e-mails

Nesta sessão podemos definir quais ações serão tomadas para as mensagens que forem classificadas como Confiáveis, Provável SPAM e SPAM. As ações podem ser:

- **Entregar:** Efetua a entrega do e-mail;
- **Deletar:** Exclui a mensagem do sistema, sem possibilidade de eventual encaminhamento ou liberação de quarentena;
- **Encaminhar:** encaminha o e-mail a terceiros ou outro sistema externo (como sandbox de terceiro ou armazenamento externo), sem que o remetente, nem o destinatário sejam alertados;
- **Rejeitar/Retorno da mensagem (Bounce):** Rejeita a mensagem, com erro de retorno ao remetente;
  Obs: Ao efetuar a rejeição, é possível efetuar uma notificação, tanto ao remetente, quanto ao destinatário da mensagem.
- **Adicionar um Header (Modificar):** Adiciona e/ou modifica um cabeçalho a mensagem a nível de HEADER;
  Obs: Não insira espaços na linha do cabeçalho, pois estes são proibidos pelo RFC 2822.
- **Adição de TAGs/textos no corpo do e-mail:** As TAGS são editáveis, de acordo com a mensagem desejada, dessa forma pode-se criar TAGs como por exemplo: (E-mail de origem externa, Remetente com possível risco de fraude, Falha em protocolo de segurança (DMARC/SPF/DKIM), Domínio recentemente adquirido, Remetente desconhecido, etc)**.**
  As situações para associação de TAGs são:
  - Remetente desconhecido ou não recorrente / remetente conhecido e confiável;
  - Domínio recentemente registrado ou domínio conhecido;
  - Falha ou sucesso nos protocolos de segurança SPF/DKIM e DMARC;
  - Mensagem que estiver com a assinatura de e-mail suspeito e/ou remetente suspeito;
  - Mensagem que estiver com a assinatura de inseguro (origem/país considerado possível ameaça);
  - Domínio com caracteres fora de padrão (ataque usando caracteres semelhantes de alfabetos diferentes, para imitar domínios confiáveis) e/ou uso de TLD (Top-Level Domain ou Domínio de Nível Superior) incomuns;
  - Falsificação do remetente (Spoofing do remetente);
- **StripHTML:** Remover o conteúdo HTML, transformando o e-mail em texto plano e removendo eventuais códigos de programação e Links/Hyperlinks;
- **Remover/Substituir Anexos:** Remove anexos específicos contidos no e-mail e/ou substitui o anexo por aviso;
- **Armazenar (Quarentena ou Auditoria):** Guarda o e-mail em quarentena, para que o administrador possa efetuar a manipulação dele;

Ações automáticas tomadas pelo MailInspector sobre o e-mail:

- **Registrar no LOG:** Registra no banco de dados toda as ações tomadas sobre o e-mail. Este registro é efetuado de forma automática, sem necessidade de ativar uma opção para esse procedimento.

Definições de Opções - Ações

Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição
Salvar	Quando clicado, grava as configurações realizadas.

Definições de Opções - Mensagens Confiáveis

Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição
Ações para Mensagens Confiáveis	Permite selecionar as ações para mensagens classificadas como confiáveis. Você pode selecionar e combinar mais de uma ação a ser tomada. • **Armazenar para Auditoria** - Armazena a mensagem na quarentena. Quando ativada esta opção, permite que os e-mails sejam acessados pelo usuário como se fosse um webmail secundário caso o sistema de e-mail estaja fora do ar. Também permite que os e-mails retidos sejam reenviados para os seus destinos. • **Deletar** - Exclui a mensagem. • **Notificar Remetente** - Envia uma notificação ao remetente da mensagem. Envia um Bounce que pode ser personalizado. • **Entregar** - Entrega a mensagem para o destinatário. • **StripHTML** - Converte todo conteúdo HTML da mensagem em texto plano. • **Cabeçalho** - Adiciona parâmetros ao cabeçalho (header) da mensagem. A inclusão de parâmetros de cabeçalhos pode ser utilizada para integração com diversas ferramentas, tais como Zimbra, MS Exchange, Lotus Notes, etc: o X-Spam-Flag; o X-Spam-Score; o X-Spam-Level; o X-Spam-Status; Obs: Não insira espaços na linha do cabeçalho, pois estes são proibidos pelo RFC 2822. • **Encaminhar e-mail para** - Encaminha uma cópia da mensagem para outro destinatário ou outro sistema externo (como sandbox de terceiro ou armazenamento externo). • **Remover/Substituir Anexos:** Remove anexos específicos contidos no e-mail e/ou substitui o anexo por aviso; • **Notificação e-mail para** - Encaminha uma notificação da mensagem para outro destinatário
Adicionar	Cadastra uma nova regra de ação para mensagens classificadas como confiáveis. Quando clicado, abre a caixa de diálogo **Cadastro do Controle Personalizado**.
Editar	Edita as configurações de um registro existente. Quando clicado, abre a caixa de diálogo **Cadastro do Controle Personalizado**.
Remover	Quando clicado, exclui o registro selecionado.

Definições de Opções - Provável SPAM

Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição

Ações para Provável SPAM	Permite selecionar as ações para mensagens classificadas como provável SPAM. Você pode selecionar e combinar mais de uma ação a ser tomada. • **Colocar em Quarentena** - Armazena a mensagem na quarentena. • **Deletar** - Exclui a mensagem. • **Notificar Remetente** - Envia uma notificação ao remetente da mensagem. Envia um Bounce que pode ser personalizado. • **Entregar** - Entrega a mensagem para o destinatário. • **StripHTML** - Converte todo conteúdo HTML da mensagem em texto plano. • **Cabeçalho** - Adiciona parâmetros ao cabeçalho (header) da mensagem. A inclusão de parâmetros de cabeçalhos pode ser utilizada para integração com diversas ferramentas, tais como Zimbra, MS Exchange, Lotus Notes, etc: o X-Spam-Flag; o X-Spam-Score; o X-Spam-Level; o X-Spam-Status; Obs: Não insira espaços na linha do cabeçalho, pois estes são proibidos pelo RFC 2822. • **Remover/Substituir Anexos:** Remove anexos específicos contidos no e-mail e/ou substitui o anexo por aviso; • **Encaminhar e-mail para** - Encaminha uma cópia da mensagem para outro destinatário ou outro sistema externo (como sandbox de terceiro ou armazenamento externo).
Adicionar	Cadastra uma nova regra de ação para mensagens classificadas como provável SPAM. Quando clicado, abre a caixa de diálogo **Cadastro do Controle Personalizado**.
Editar	Edita as configurações de um registro existente. Quando clicado, abre a caixa de diálogo **Cadastro do Controle Personalizado**.
Remover	Quando clicado, exclui o registro selecionado.

Definições de Opções - SPAM

Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição
Ações para SPAM	Permite selecionar as ações para mensagens classificadas como SPAM. Você pode selecionar e combinar mais de uma ação a ser tomada. • **Colocar em Quarentena** - Armazena a mensagem na quarentena. • **Deletar** - Exclui a mensagem. • **Notificar Remetente** - Envia uma notificação ao remetente da mensagem. Envia um Bounce que pode ser personalizado. • **Entregar** - Entrega a mensagem para o destinatário. • **StripHTML** - Converte todo conteúdo HTML da mensagem em texto plano. • **Cabeçalho** - Adiciona parâmetros ao cabeçalho (header) da mensagem. A inclusão de parâmetros de cabeçalhos pode ser utilizada para integração com diversas ferramentas, tais como Zimbra, MS Exchange, Lotus Notes, etc: o X-Spam-Flag; o X-Spam-Score; o X-Spam-Level;

	○ X-Spam-Status; Obs: Não insira espaços na linha do cabeçalho, pois estes são proibidos pelo RFC 2822. • **Remover Anexos:** Remove anexos específicos contidos no e-mail; • **Encaminhar e-mail para** - Encaminha uma cópia da mensagem para outro destinatário ou outro sistema externo (como sandbox de terceiro ou armazenamento externo).
Adicionar	Cadastra uma nova regra de ação para mensagens classificadas como SPAM. Quando clicado, abre a caixa de diálogo **Cadastro do Controle Personalizado**.
Editar	Edita as configurações de um registro existente. Quando clicado, abre a caixa de diálogo **Cadastro do Controle Personalizado**.
Remover	Quando clicado, exclui o registro selecionado.

Definições de Opções - Cadastro do Controle Personalizado

Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição
Adicionar	Quando clicado, adiciona o controle personalizado.
Cancelar	Quando clicado, cancela a ação.
De	Selecione o grupo pré-cadastrado de remetentes.
Para	Selecione o grupo pré-cadastrado de destinatários.
Ação	Selecione as ações: • **Armazenar para Auditoria** - Armazena a mensagem na quarentena. • **Colocar em Quarentena** - Armazena a mensagem na quarentena. • **Deletar** - Exclui a mensagem. • **Entregar** - Entrega a mensagem para o destinatário. • **StripHTML** - Converte todo conteúdo HTML da mensagem em texto plano. • **Cabeçalho** - Adiciona parâmetros ao cabeçalho (header) da mensagem. A inclusão de parâmetros de cabeçalhos pode ser utilizada para integração com diversas ferramentas, tais como Zimbra, MS Exchange, Lotus Notes, etc: ○ X-Spam-Flag; ○ X-Spam-Score; ○ X-Spam-Level; ○ X-Spam-Status; Obs: Não insira espaços na linha do cabeçalho, pois estes são proibidos pelo RFC 2822. • **Remover/Substituir Anexos:** Remove anexos específicos contidos no e-mail e/ou substitui o anexo por aviso; • **Encaminhar e-mail para** - Encaminha uma cópia da mensagem para outro destinatário ou outro sistema externo (como sandbox de terceiro ou armazenamento externo).

Definições de Opções - Ameaças

Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição
Ações para Ameaças	Permite selecionar as ações para mensagens classificadas como uma Ameaça (Vírus, Malware, Trojan, etc). Você pode selecionar e combinar mais de uma ação a ser tomada. • **Remover Anexo** - Remove o Anexo infectado e entrega mensagem para o destinatário. • **Remover o Corpo** - Remove o corpo da mensagem e entrega mensagem para o destinatário. • **Colocar em Quarentena** - Coloca a mensagem em quarentena e NÃO entrega a mensagem para o usuário. Esta opção permite que o sistema de detecção de Vírus Zero Day coloque uma mensagem suspeita na quarentena e depois possa ser escaneada quando uma vacina for disponibilizada. • **Enviar Notificação ao Destinatário** - Envia um aviso que a mensagem foi colocada em quarentena por conter conteúdo perigoso.
Adicionar	Cadastra uma nova regra de ação para mensagens classificadas como ameaças. Quando clicado, abre a caixa de diálogo **Cadastro do Controle Personalizado**.
Editar	Edita as configurações de um registro existente. Quando clicado, abre a caixa de diálogo **Cadastro do Controle Personalizado**.
Remover	Quando clicado, exclui o registro selecionado.

Definições de Opções - Cadastro do Controle Personalizado

Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição
Adicionar	Quando clicado, adiciona o controle personalizado.
Cancelar	Quando clicado, cancela a ação.
De	Selecione o grupo pré-cadastrado de remetentes.
Para	Selecione o grupo pré-cadastrado de destinatários.
Ação	Selecione as ações: • **Remover Anexo** - Remove o Anexo infectado e entrega mensagem para o destinatário. • **Remover o Corpo** - Remove o corpo da mensagem e entrega mensagem para o destinatário. • **Colocar em Quarentena** - Coloca a mensagem em quarentena e NÃO entrega a mensagem para o usuário. Esta opção permite que o sistema de detecção de Vírus Zero Day coloque uma mensagem suspeita na quarentena e depois possa ser escaneada quando uma vacina for disponibilizada. • **Enviar Notificação ao Destinatário** - Envia um aviso que a mensagem foi colocada em quarentena por conter conteúdo perigoso.

Controle Avançado

Use esta página para exibir, adicionar, editar ou excluir regras do controle avançado do Filtro de SPAM.

Configurações **/ Filtros de SPAM / Controle Avançado**

Visão geral do controle avançado

O **Controle Avançado do HSC MailInspector** permite criar, gerenciar e visualizar, em um único local, as **regras avançadas de proteção contra SPAM**, possibilitando a combinação de diferentes critérios de análise e condições para obter um controle mais preciso sobre a classificação e o tratamento das mensagens.

As regras podem utilizar informações provenientes de diferentes componentes da mensagem e dos mecanismos de segurança da solução, incluindo:

- **Cabeçalhos (Headers)** da mensagem, conforme os padrões **RFC 821/822**;
- **Conteúdo da mensagem (Body)**;
- **Mensagem em seu formato original (Raw)**;
- **Arquivos e documentos anexados**;
- **URLs** presentes no corpo da mensagem;
- **Assinaturas e indicadores dos mecanismos antispam**, como reputação, RBLs, DKIM, SPF, entre outros;
- **Endereços IP, domínios e subdomínios** relacionados à origem da mensagem;
- **Remetente e destinatário**, incluindo os campos SMTP Envelope Sender e SMTP Envelope Recipient.

O sistema permite ainda a criação de **dicionários personalizados de palavras e expressões**, utilizando **expressões regulares (Regex)** para identificar padrões em diferentes campos da mensagem. Também é possível determinar a quantidade de ocorrências necessárias de um determinado termo ou padrão para que uma regra seja considerada atendida.

As condições podem ser combinadas por meio de **operadores lógicos**, permitindo a construção de regras complexas e altamente específicas. Entre os operadores disponíveis estão **AND, OR, OCCUR, NOT e NEAR**, além do uso de agrupamentos com **parênteses e colchetes** e expressões regulares.

Políticas Personalizadas por Origem e Destino

O Controle Avançado permite criar políticas diferenciadas de acordo com as características da origem e do destino da mensagem. Dessa forma, o administrador pode **aumentar ou reduzir a pontuação de SPAM**, aplicar condições específicas ou determinar ações distintas com base em atributos como:

- IP de origem;
- Reputação da origem;
- Domínio e subdomínio;
- Remetente — **SMTP Envelope Sender**;
- Destinatário — **SMTP Envelope Recipient**;
- Usuário;

- Aliases;
- Endereço principal;
- Grupos **LDAP**;
- Listas de distribuição;
- Entre outros atributos disponíveis na solução.

Essa granularidade permite adequar o comportamento do antispam às características e às necessidades específicas de cada organização, possibilitando, por exemplo, políticas diferentes para determinados usuários, departamentos, domínios, remetentes ou grupos LDAP.

Combinação de Regras e Inteligência de Análise

As regras podem ser **combinadas e encadeadas** para criar políticas de proteção mais sofisticadas. O administrador pode estabelecer múltiplas condições que, quando atendidas individualmente ou em conjunto, determinam a classificação e a ação aplicada à mensagem.

Essa capacidade de correlação permite ao **HSC MailInspector** analisar simultaneamente diferentes características de uma mensagem — como remetente, reputação, conteúdo, anexos, URLs e cabeçalhos — proporcionando maior **precisão, flexibilidade e aderência às políticas de segurança da organização**.

O Controle Avançado transforma diferentes indicadores de segurança em **regras personalizadas e combináveis**, permitindo que o administrador tenha controle granular sobre a detecção, classificação e tratamento de SPAM, de acordo com a necessidade do administrador.

Definições de Opções - Controle Avançado

Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição
Adicionar	Cadastra um novo registro de controle avançado de SPAM. Quando clicado, abre a caixa de diálogo **Adicionar/Editar Controle Avançado**.
Editar	Edita as configurações de um registro existente. Quando clicado, abre a caixa de diálogo **Adicionar/Editar Controle Avançado**.
Remover	Quando clicado, exclui o registro selecionado.
Conectar	Permite combinar duas regras previamente selecionadas. Quando clicado, abre a caixa de diálogo **Conectar**.
Desconectar	Permite desconectar duas regras previamente conectadas.

Definições de Opções - Adicionar/Editar Controle Avançado - Seleção do Controle

Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição
Cabeçalho	Permite verificar qualquer parte do cabeçalho da mensagem.
Corpo	Permite realizar a análise do conteúdo da mensagem.
Conteúdo Original	Permite verifica a mensagem no formato original que foi recebida.
Anexos	Verifica conteúdo dos anexos e nome / extensão. Permite identificar Dicionário de Palavras no conteúdo de anexos como: DOC, XLS, PDF, DOCX, XLSX, PPT, HTML entre outros.
URL	Permite verifica URLs incluídas no corpo da mensagem.
Localização	Permite a aplicação de regras baseadas na linguagem da mensagem ou no país de origem.
Controle de Assinatura	Possibilita a combinação de regras com ações realizadas em outros filtros da ferramenta. São mais de 10Mil tipos de assinaturas, exemplo: Reputação, SPF, DKIM, RBLs, Assinaturas de Cabeçalhos, Assinatura de Corpo, Anexos, etc.
Avançar	Quando clicado, prossegue para a configuração do tipo de controle selecionado.

Definições de Opções - Adicionar/Editar Controle Avançado - Cabeçalho

Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição
Define o cabeçalho a ser utilizado	Selecione um cabeçalho para ser pesquisado na mensagem.
Cabeçalho Customizado	Quando definido o cabeçalho a ser utilizado como **customizado**. Informe o nome do cabeçalho presente na mensagem para combinar com a regra.
Grupos	Quando definido o cabeçalho a ser utilizado como Received, **From**, **To**, **CC** ou **Bcc**. Selecione o grupo de usuários que contém os endereços presentes na mensagem para combinar com a regra.
Dicionário de Palavras	Quando definido o cabeçalho a ser utilizado como diferente de **Received**, **From**, **To**, **CC** ou **Bcc**. Selecione o dicionário de palavras que contém os termos presentes no cabeçalho da mensagem para combinar com a regra.
Número Mínimo de Ocorrências	Informe o número de ocorrências que devem ser encontradas de grupo de usuários ou dicionário de palavras no cabeçalho da mensagem para combinar com a regra.
Voltar	Quando clicado, retorna a seleção de controle.
Avançar	Quando clicado, prossegue para a configuração das informações e pontuação.

Definições de Opções - Adicionar/Editar Controle Avançado - Corpo

Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição
Dicionário de Palavras	Selecione o dicionário de palavras que contém os termos presentes no corpo da mensagem para combinar com a regra.
Número Mínimo de Ocorrências	Informe o número de ocorrências que devem ser encontradas no dicionário de palavras para combinar com a regra.
Voltar	Quando clicado, retorna a seleção de controle.
Avançar	Quando clicado, prossegue para a configuração das informações e pontuação.

Definições de Opções - Adicionar/Editar Controle Avançado - Conteúdo Original

Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição
Dicionário de Palavras	Selecione o dicionário de palavras que contém os termos presentes no corpo da mensagem, em seu formato original, para combinar com a regra.
Número Mínimo de Ocorrências	Informe o número de ocorrências que devem ser encontradas no dicionário de palavras para combinar com a regra.
Voltar	Quando clicado, retorna a seleção de controle.
Avançar	Quando clicado, prossegue para a configuração das informações e pontuação.

Definições de Opções - Adicionar/Editar Controle Avançado - Anexos

Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição
Tipo de Anexo	Escolha entre: • **Grupo de Anexos** - Cria uma regra de controle avançado realizando a busca por um determinado grupo de anexos, buscando por nome, extensão ou expressão regular no nome do arquivo em anexo. • **Dicionário de Palavras** - Cria uma regra de controle avançado realizando a busca por um determinado dicionário de palavras, buscando por expressões no conteúdo do arquivo em anexo e documentos, tais como: PDF, DOC, DOCX, PPS, PPT, HTML, XLS e etc.
Grupo de Anexos	Selecione o grupo de anexo que contém os nomes, extensões ou expressões regulares presentes no nome do arquivo anexo da mensagem para combinar com a regra.
Dicionário de Palavras	Quando definido o tipo de anexo como **Dicionário de Palavras**. Selecione o dicionário de palavras que contém os termos presentes no conteúdo do anexo para combinar com a regra.
Número Mínimo de Ocorrências	Quando definido o tipo de anexo como **Dicionário de Palavras**. Informe o número de ocorrências que devem ser encontradas no dicionário de palavras para combinar com a regra.

Voltar	Quando clicado, retorna a seleção de controle.
Avançar	Quando clicado, prossegue para a configuração das informações e pontuação.

Definições de Opções – Adicionar / Editar Controle Avançado - URL

Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição
Dicionário de Palavras	Selecione o dicionário de palavras que contém os termos das URLs presentes no corpo da mensagem para combinar com a regra.
Número Mínimo de Ocorrências	Informe o número de ocorrências que devem ser encontradas no dicionário de palavras para combinar com a regra.
Voltar	Quando clicado, retorna a seleção de controle.
Avançar	Quando clicado, prossegue para a configuração das informações e pontuação.

Definições de Opções - Adicionar/Editar Controle Avançado - Localização

Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição
Tipo de controle	Selecione por controle de Linguagem ou por País de origem.
Linguagem ou País de Origem	De acordo com a opção anterior, selecione ou a linguagem ou o País para o filtro.
Voltar	Quando clicado, retorna a seleção de controle.
Avançar	Quando clicado, prossegue para a configuração das informações e pontuação.

Definições de Opções - Adicionar/Editar Controle Avançado - Controle de Assinaturas

Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição
Regras	Select box que possibilita a combinação de regras com ações realizadas em outros filtros da ferramenta.
Operador Lógico	Escolha entre: • **E** - A pontuação será atribuída as mensagens que combinarem com as duas regras selecionadas. • **OU** - A pontuação será atribuída as mensagens que combinarem com qualquer uma das regras selecionadas.
Voltar	Quando clicado, retorna a seleção de controle.
Avançar	Quando clicado, prossegue para a configuração das informações e pontuação.

Definições de Opções - Adicionar/Editar Controle Avançado - Informações e Pontuação

Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição
Nome	Informe um nome descritivo para a regra.
Descrição	Campo livre para comentários.
Pontuação	Informe o valor da pontuação atribuída as mensagens, que combinarem com as configurações de controle da regra.
Voltar	Quando clicado, retorna para a configuração do controle selecionado.
Avançar	Quando clicado, prossegue para a conferência dos itens configuradas na regra.

Definições de Opções – Adicionar / Editar Controle Avançado - Conclusão do Processo

Estas informações descrevem as opções disponíveis nesta página.

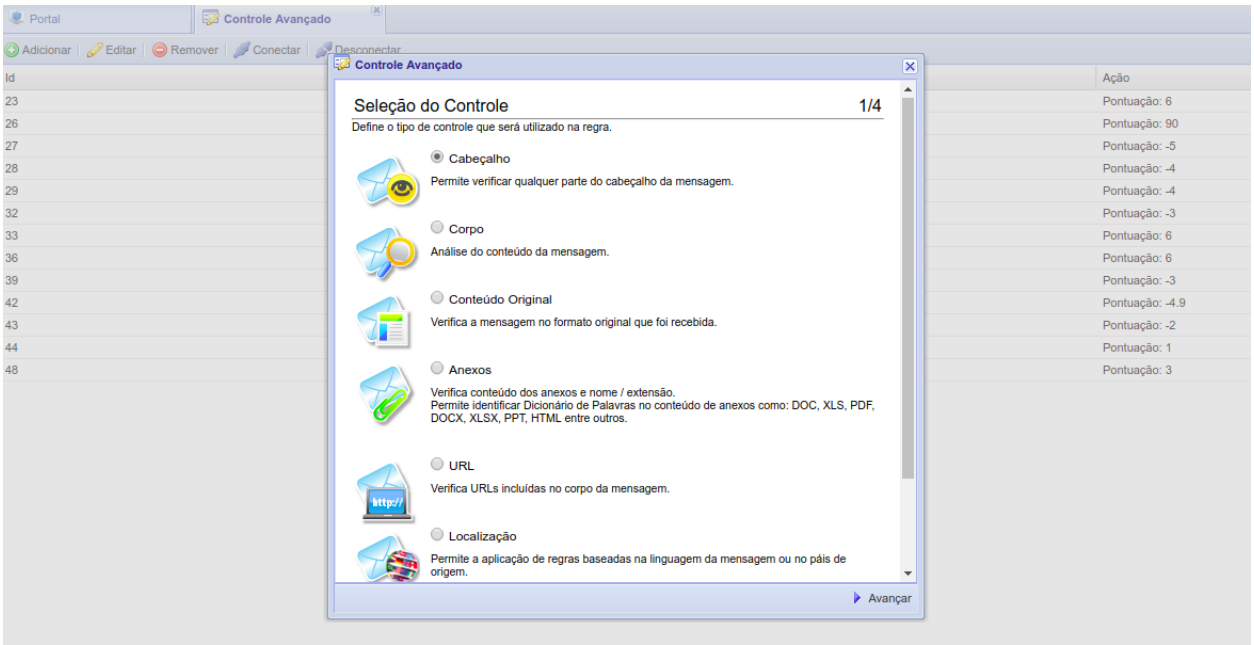
Opções	Definição
Voltar	Quando clicado, retorna para a configuração das informações e pontuação.
Salvar	Quando clicado, grava as configurações realizadas.

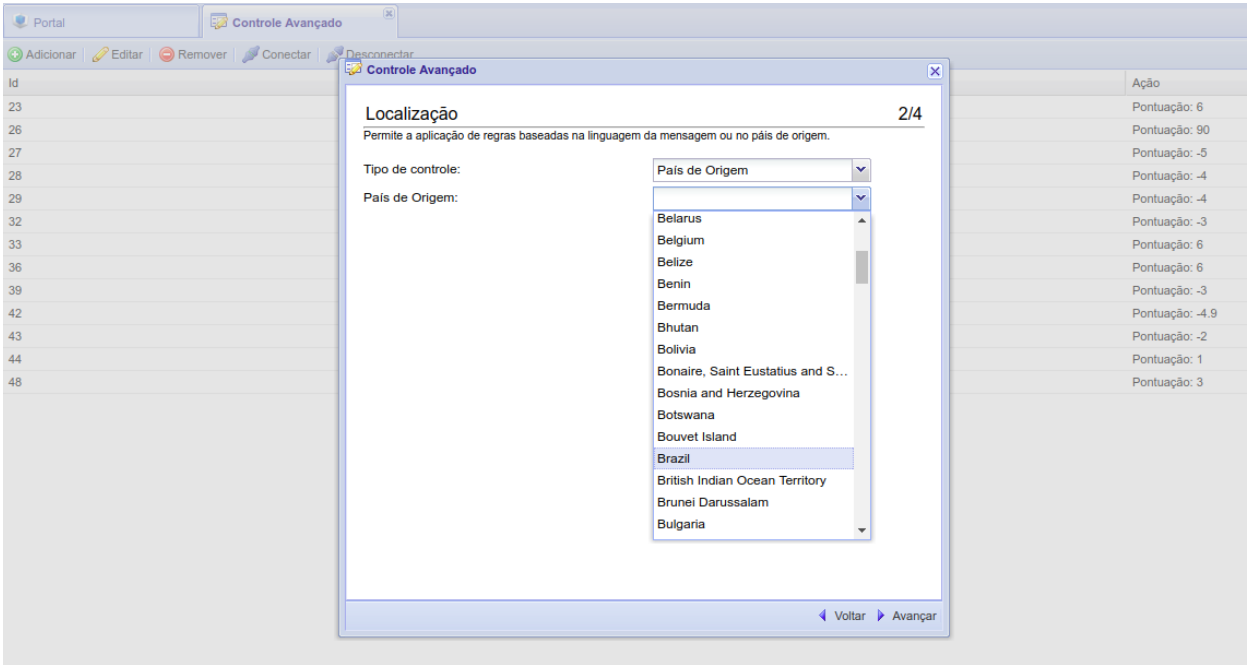
Definições de Opções - Conectar

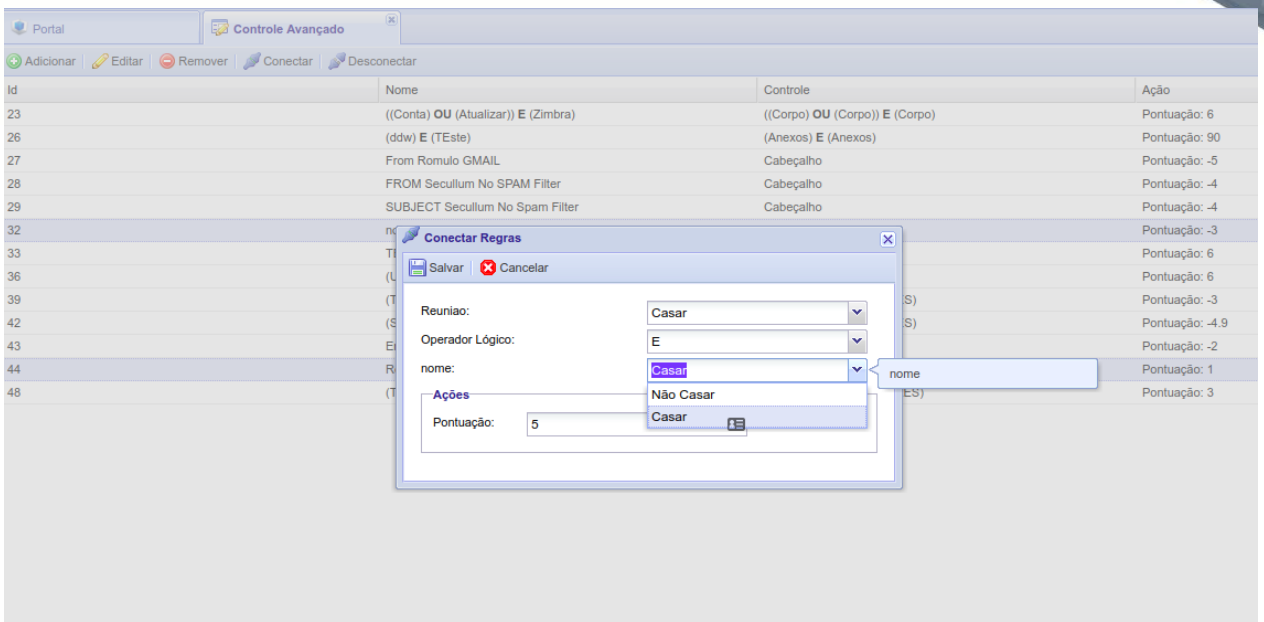
Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição
Salvar	Quando clicado, grava as configurações realizadas.
Cancelar	Quando clicado, cancela a ação.
Regra	Escolha entre: • **Casar** - A pontuação será atribuída as mensagens que combinarem com a regra selecionada. • **Não Casar** - A pontuação será atribuída as mensagens que não combinarem com a regra selecionada.
Operador Lógico	Escolha entre: • **E** - A pontuação será atribuída as mensagens que combinarem com as duas regras selecionadas. • **OU** - A pontuação será atribuída as mensagens que combinarem com qualquer uma das regras selecionadas.
Regra	Escolha entre: • **Casar** - A pontuação será atribuída as mensagens que combinarem com a regra selecionada. • **Não Casar** - A pontuação será atribuída as mensagens que não combinarem com a regra selecionada.
Pontuação	Informe o valor da pontuação atribuída as mensagens que combinem com as regras conectadas.

Exemplo criação de regra






Portal
Controle Avançado
Adicionar
Editar
Remover
Conectar
Desconectar
Id
Nome
Controle
Ação
23
((Conta) OU (Atualizar)) E (Zimbra)
((Corpo) OU (Corpo)) E (Corpo)
Pontuação: 6
26
(ddw) E (TEste)
(Anexos) E (Anexos)
Pontuação: 90
27
From Romulo GMAIL
Cabeçalho
Pontuação: -5
28
FROM Secullum No SPAM Filter
Cabeçalho
Pontuação: -4
29
SUBJECT Secullum No Spam Filter
Cabeçalho
Pontuação: -4
32
Pontuação: -3
33
Pontuação: 6
36
Pontuação: 6
39
Pontuação: -3
42
Pontuação: -4.9
43
Pontuação: -2
44
Pontuação: 1
48
Pontuação: 3
Conectar Regras
Salvar
Cancelar
Reuniao:
Casar
Operador Lógico:
E
nome:
Casar
Não Casar
Casar
nome
Ações
Pontuação:
5

Anti Spoofing

O HSC MailInspector possui um sofisticado mecanismo de detecção de tentativas de Fraudes de e-mail que são usadas por Hackers a fim de ludibriar os usuários de sua empresa.

Estes mecanismos são muito eficazes como ataques de:

- BEC "business e-mail compromise";
- Mail Spoofing (Spoofing de Domínio, Spoofing de E-mail de Remetente, entre outros);
- Mail Impostor;
- E tantos outros que tentam enganar os usuários usando informações falsas de origens.

São diversos mecanismos e controles específicos que irão auxiliar ao administrador identificar e tomar a decisão contra estes ataques, que vêm crescendo exponencialmente.

O sistema de anti-spoofing do MailInspector protege os usuários do tipo CEO/VIP, para ataques ao qual o hacker utiliza técnicas de Spoofing no Display Name, passando-se por usuário de grande importância na empresa. Para isso, é efetuado o cadastro dos usuários VIP's para que a solução possa monitorar com maior precisão os e-mails com diferença de Display Name e técnicas de fraude sobre eles. O MailInspector também conta com sistema de proteção de Look-ALike, onde o hacker efetua o ataque enviando e-mails similares ao domínio da empresa e outros tipos de ataque de spoofing, tais como Remetente similar ao original.

Também é utilizado **Machine Learning associado à Inteligência Artificial (IA)** para a detecção de ameaças relacionadas a **Engenharia Social**, por meio da análise contextual e semântica do conteúdo presente no corpo dos e-mails. Essa abordagem permite identificar padrões de comportamento, intenção e linguagem potencialmente associados a tentativas de fraude, manipulação ou comprometimento de usuários.

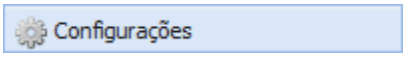
Combinada à **classificação de usuários VIP e à aplicação de políticas de proteção específicas**, essa tecnologia amplia significativamente a capacidade de detecção e prevenção contra ataques de **Business Email Compromise (BEC)** e Engenharia Social, inclusive em mensagens que **não possuem links ou anexos maliciosos** e que poderiam passar despercebidas pelos mecanismos tradicionais de segurança.

Além de uso de IA e Machine Learning, o MailInspector detecta ataques de BEC através de diversos outros métodos, tais como:

- Diferenças entre o campo FROM do Header, FROM do Envelope e Reply-To;
- Análise e detecção de diferenças sutis no Display Name;
- Look-Alike Domain atack (domínios similares);
- Detecção de novos domínios;

Configurações Gerais

Use esta página para exibir ou editar configurações gerais do sistema de AntiSpoofing.



/ Anti Spoofing / Configurações Gerais

Visão geral do Configurações Gerais

Nesta tela poderemos definir como o sistema irá tratar os ataques que tentam utilizar os domínios da empresa como remetentes de mensagens externas. O controle poderá ser realizado

Definições de Opções - Controle contra Falsificação de Remetentes Mail Spoofing

Este mecanismo identifica ataques que tentam utilizar os dominios da empresa como remetentes das mensagens externas.

Opções	Definição
Salvar	Quando clicado, grava as configurações realizadas.
Bloquear	Bloqueia todas as mensagens externas identificadas com um dos domínios da empresa, jogando-os para a quarentena específica
Ignorar	Ignora (sem ação) as mensagens externas identificadas com um dos domínios da empresa
Pontuar	Pontua as mensagens externas identificadas com um dos domínios da empresa

Definições de Opções - Controle de novos Domínios

Este filtro identifica domínios que foram recentemente criados e permite que o administrador possa definir o que fazer com a mensagem.

Opções	Definição
Tempo mínimo do domínio	Define qual o tempo mínimo aceito para data de criação do domínio. Padrão 6 meses
Bloquear	Bloqueia todas as mensagens externas identificadas como New Domains/Novos Domínios, jogando-os para a quarentena específica
Ignorar	Ignora (sem ação) as mensagens externas identificadas como New Domains/Novos Domínios
Pontuar	Pontua as mensagens externas identificadas como New Domains/Novos Domínios

Definições de Opções - Controle de Remetentes Envelope SMTP x From Header

Este filtro identifica domínios forjados, comparando os cabeçalhos Envelope SMTP do From Header. Nessa categoria possuímos dois modos de detecção específico:

- Domínios Forjados com Free Mail;
- Domínios Diferentes no Cabeçalho;

Domínios Forjados com Free Mail:

Identifica domínios forjados utilizando os principais e-mails gratuitos do mercado (tais como: yahoo, gmail, Hotmail, etc). Ele compara o Remetente do Envelope SMTP e do Header a fim de identificar o uso indevido de sistema de e-mail gratuitos.

Opções	Definição
Bloquear	Bloqueia todas as mensagens externas identificadas como Forjados com Free Mail, jogando-os para a quarentena específica

Ignorar	Ignora (sem ação) as mensagens externas identificadas como Forjados com Free Mail.
Pontuar	Pontua as mensagens externas identificadas como Forjados com Free Mail.

Domínios Diferentes no Cabeçalho:

Quando habilitado o sistema tentará identificar diferenças nos domínios informados no Cabeçalho From e no Envelope SMTP.

Opções	Definição
Bloquear	Bloqueia todas as mensagens externas identificadas como Domínios diferentes no cabeçalho, jogando-os para a quarentena específica
Ignorar	Ignora (sem ação) as mensagens externas identificadas como Domínios diferentes no cabeçalho
Pontuar	Pontua as mensagens externas identificadas como Domínios diferentes no cabeçalho

Validar DNS A e MX de Domínios do Remetente do Cabeçalho:

Verifica no From do Header se o dominio do From existe e se ele possui um endereço A e MX válido.

Essa entrada permite que os servidores DNS identifiquem e localizem um site, contas de e-mail, os mantendo onlines.

Ao utilizar a entrada tipo A sempre a associe o domínio ou subdomínio a um endereço IPv4. É permitido ter múltiplas entrada do tipo A no mesmo domínio/subdomínio.

Opções	Definição
Bloquear	Bloqueia todas as mensagens externas identificadas como remetente inválido no DNS, jogando-os para a quarentena específica
Ignorar	Ignora (sem ação) as mensagens externas identificadas como remetente inválido no DNS
Pontuar	Pontua as mensagens externas identificadas como remetente inválido no DNS

Todas as mensagens que obtiverem pontuação acima da que foi configurada pelo administrador do MailInspector, serão bloqueados por pontuação e dessa forma é possível gerar alertas ao administrador por quebra da política da pontuação máxima do e-mail.

Sender ID

Use esta página para exibir ou editar configurações do Sender ID.

Configurações **/ Anti Spoofing / Sender ID**

Visão geral do Sender ID

O Sender ID (definido na RFC 4406) é um protocolo da Microsoft derivado do SPF (de sintaxe idêntica), que valida o campo do endereço da mensagem no cabeçalho, de acordo com RFC 2822. A validação segue um algoritmo chamado PRA (Purported Responsible Address, RFC 4407).

O algoritmo certifica se o campo do cabeçalho com o endereço do e-mail é responsável por enviar a mensagem. Como ele deriva do SPF, pode também validar o MAIL FROM, mas ele irá definir uma nova identidade, PRA e novos campos de política de envio, substituindo o MAIL FROM (MFROM por Sender ID), PRA, ou os dois.

O HSC MailInspector pode ser configurado para identificar a autenticidade de mensagens através da verificação do protocolo Sender ID, porém, este protocolo é menos utilizado, este mecanismo permite:

- **ao administrador de um domínio:** definir e publicar uma política Sender ID, onde são designados os endereços das máquinas autorizadas a enviar mensagens em nome deste domínio; e
- **ao administrador do HSC MailInspector:** estabelecer critérios de pontuação de mensagens em função da checagem das políticas Sender ID publicadas para cada domínio. O processo de publicação de uma política Sender ID é independente da implantação de checagem de Sender ID por parte do HSC MailInspector, estes podem ou não ser feitos em conjunto.

Para maiores informações sobre o protocolo Sender ID visite o website http://www.microsoft.com/mscorp/safety/technologies/senderid/default.mspx

Definições de Opções - Sender ID

Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição
Salvar	Quando clicado, grava as configurações realizadas.
Habilitar Checagem	Escolha entre: • **Sim** - Indica que a filtragem de Sender ID está ativa. • **Não** - Indica que a filtragem de Sender ID está desativada.
Pontuação	Permite definir a pontuação que será atribuída a mensagens verificadas pelo Sender ID: • **Mensagens Válidas** - Mensagens consideradas válidas, quando o endereço IP do servidor de origem da mensagem pertence ao registro Sender ID configurado para o domínio. • **Mensagens Inválidas** - Mensagens consideradas inválidas, quando o endereço IP do servidor de origem da mensagem não pertence ao registro Sender ID configurado para o domínio.

SPF

Use esta página para exibir ou editar configurações do SPF.

Configurações / **Anti Spoofing / SPF**

Visão geral do SPF

O SPF (Sender Policy Framework) é uma tecnologia utilizada para combater a falsificação de endereços de retorno dos e-mails (return-path).

O HSC MailInspector pode ser configurado para identificar a autenticidade de mensagens através da verificação do SPF, o protocolo SPF é similar ao protocolo do Sender ID, porém, mais amplamente utilizado, este mecanismo permite:

- **ao administrador de um domínio:** definir e publicar uma política SPF, onde são designados os endereços das máquinas autorizadas a enviar mensagens em nome deste domínio; e
- **ao administrador do HSC MailInspector:** estabelecer critérios de pontuação de mensagens em função da checagem das políticas SPF publicadas para cada domínio.

O processo de publicação de uma política SPF é independente da implantação de checagem de SPF por parte do HSC MailInspector, estes podem ou não ser feitos em conjunto.

Para maiores informações sobre o protocolo SPF visite o website http://www.openspf.org/.

Definições de Opções - SPF

Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição
Salvar	Quando clicado, grava as configurações realizadas.
Habilitar Checagem	Escolha entre: • **Sim** - Indica que a filtragem de SPF está ativa. • **Não** - Indica que a filtragem de SPF está desativada.
Pontuação	Permite definir a pontuação que será atribuída a mensagens verificadas pelo SPF: • **Mensagens Válidas (Pass):** Mensagens consideradas válidas, quando o endereço IP do servidor de origem da mensagem pertence ao registro SPF configurado para o domínio. • **Mensagens Classificadas como FAIL:** Mensagens consideradas inválidas, quando o endereço IP do servidor de origem da mensagem não pertence ao registro SPF configurado para o domínio. • **Mensagens Classificadas como SOFT FAIL:** Mensagens consideradas inválidas, quando o endereço IP do servidor de origem da mensagem informado SMTP não pertence ao registro SPF configurado para o domínio, porém o registro DNS foi configurado como final "?all".

	• **Mensagens Classificadas como NEUTRAL**: O proprietário do domínio declarou explicitamente que não pode ou não deseja afirmar se o endereço IP está autorizado ou não. • **Mensagens Classificadas como PERMERROR**: Ocorreu um erro permanente (por exemplo, registro SPF mal formatado). • **Mensagens Classificadas como TEMPERROR**: Ocorreu um erro transitório. • **Mensagens Classificadas como NONE**: O resultado "NONE" significa que nenhum registro foi publicado pelo domínio ou que o domínio não pôde ser determinado.

Controle de Respostas - SPF

As ações podem ser:
Bloquear = efetua bloqueio na camada MTA, ou sejam a mensagens não é recebida pelo HSC MailInspector.
Pontuar = define quantos pontos na mensagem será somada ou subtraída para os filtros de controle de SPAM.
Ignorar = ignora a resposta e não toma nenhuma ação.

Opções	Ações Disponíveis
PASS	Pontuar e Ignorar
Fail	Bloquear, Pontuar e Ignorar
SoftFail	Bloquear, Pontuar e Ignorar
Neutral	Bloquear, Pontuar e Ignorar
PermError	Bloquear, Pontuar e Ignorar
TemError	Bloquear, Pontuar e Ignorar
None	Pontuar e Ignorar

Pontuação e ação para SPF

Whitelist

Neste campo podem ser adicionados os endereços de e-mail, domínios e IPs que NÃO serão validados contra o SPF.

É possível ao administrador customizar uma ação especifica baseado em uma resposta de SPF em relação a um remetente/destinatário:

Configurações > Filtros de SPAM > Controle Avançado

Definições de Opções - Validação Whitelist

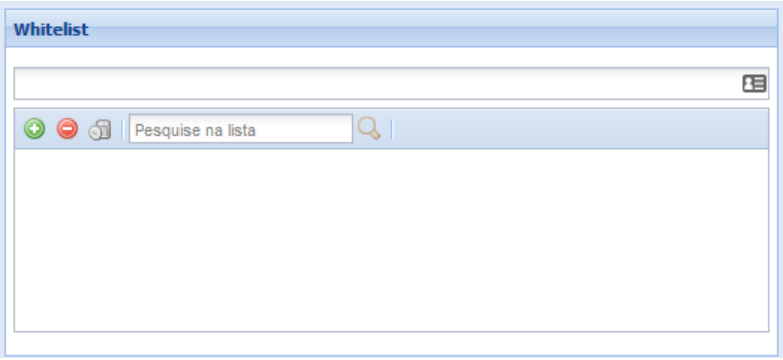
Quando ativada esta função o HSC MailInspector irá efetuar uma validação extra na Whitelist, verificando se o servidor de origem da mensagem é autorizado a enviar e-mails por este domínio, usando a consulta SPF, garantindo assim uma segurança extra na validação das entradas contidas na Whitelist. Este procedimento NÃO impacta na checagem de SPF de pontuação de cálculo de SPAM.

Opções	Definição
Ativar validação extra na Whitelist	Sim: Ativa funcionalidade de validação na whitelist Não: Não ativa a funcionalidade de validação na whitelist

Ações de acordo com a consulta SPF:

Pass	O servidor é autorizado e a entrada na Whitelist será válida.
Fail	O servidor não é autorizado e a entrada na Whitelist será ignorada.
SoftFail	O servidor pode não ser autorizado e a entrada na Whitelist será ignorada.
Neutral	O servidor é autorizado e a entrada na Whitelist será válida.
PermError	Ocorreu um erro na consulta SPF não sendo possível validar o servidor, desta forma a entrada na Whitelist será válida.
TempError	Ocorreu um erro temporário na consulta SPF não sendo possível validar o servidor, desta forma a entrada na Whitelist será válida.

* Quando uma entrada na **Whitelist** contiver um endereço IP de um servidor, a **validação extra de SPF NÃO será efetuada**.



Tarefa - Publicando uma política SPF para o domínio

Descreve os passos necessários para publicar uma política de SPF para um determinado domínio.

Esta configuração é um exemplo de complemento da filtragem SPF, não sendo realizada dentro do HSC MailInspector, e sim no gerenciador de DNS do domínio de e-mails.

Ao publicar uma política de SPF, o administrador de um domínio está autorizando determinados MTAs a enviar e-mails em nome deste domínio. O objetivo é evitar que terceiros enviem mensagem indevidamente em nome de seu domínio, e que mensagens de erro (bounces) causadas por spam com envelope falso sejam enviadas para o seu servidor.

Estas políticas são publicadas através de registros TXT do DNS, em formato ASCII. Um exemplo desse registro é:

Exemplo:

```
example.com.    IN    TXT    "v=spf1 a mx ip4:192.0.2.32/27 -all"
```

Neste caso a política estabelece que pode enviar mensagens em nome do domínio example.com uma máquina que satisfaça um dos seguintes critérios:

seu endereço IP deve ser um RR tipo A do domínio example.com (a);
seja designada como MX do domínio example.com (mx); ou
pertença ao bloco de endereços IP 192.0.2.32/27 (ip4).

A cláusula "-all" diz que devem ser recusados ("-", prefixo Fail) e-mails partindo de qualquer outro endereço IP (all).

Todas as opções de prefixos são:

"+" Pass
"-" Fail
"~" SoftFail
"?" Neutral

O prefixo é opcional, e se omitido o valor utilizado é o "+" (Pass).

A cláusula "all" deve ser sempre a cláusula mais à direita. Ela define qual resposta será retornada em uma consulta SPF, caso nenhuma das outras cláusulas se aplique.

O administrador de um MTA que consulte a política SPF do domínio do remetente de um e-mail, como definido no envelope, poderá rejeitar ou marcar como suspeita uma mensagem que não satisfaça à política SPF daquele domínio.

A especificação completa de como expressar uma política SPF pode ser encontrada no site de referência do SPF (http://www.openspf.org/) e na RFC 4408: "Sender Policy Framework (SPF) for Authorizing Use of Domains in E-Mail, Version 1" (http://tools.ietf.org/html/rfc4408).

Caso tenha dificuldades em criar SPF, é possível fazer busca na internet de geradores de SPF, tais como https://spfwizard.net

DKIM / Domain Key

Use esta página para exibir ou editar configurações do DKIM / Domain Key.

Configurações **/ Anti Spoofing / DKIM/Domain Key**

Visão geral do DKIM / Domain Key

DKIM (DomainKey Identified Mail) é uma especificação do IETF **RFC 6376** que define um mecanismo para autenticação de e-mail baseado em criptografia de chaves públicas.

Através do uso do DKIM, uma organização assina digitalmente as mensagens que envia, permitindo ao receptor confirmar a autenticidade da mensagem. Para verificar a assinatura digital, a chave pública é obtida por meio de consulta ao DNS do domínio do assinante.

Ao contrário do SPF, que verifica somente o envelope, o DKIM verifica o cabeçalho da mensagem. Esta técnica acarreta um custo computacional adicional por mensagem, tanto para o MTA remetente quanto para o receptor.

Estas são as principais vantagens dessa tecnologia:

- O destinatário poderá confiar na origem do e-mail e no conteúdo da mensagem se a análise do DKIM for concluída.
- Aumento na eficiência das listas negras e brancas de domínios.
- Controle antispam mais eficaz, além de opções de ações automatizadas que podem ser executadas nos resultados da análise do DKIM.
- Agora, os proprietários de domínios abusivos podem ser rastreados.
- O DKIM é inteiramente compatível com todos os servidores baseados em SMTP e DNS.

Para maiores informações sobre o DKIM visite o website http://dkim.org/.
Para testar seu DKIM, acesse http://dkimcore.org/c/keycheck.

Definições de Opções - DKIM / Domain Key

Estas informações descrevem as opções disponíveis nesta página.

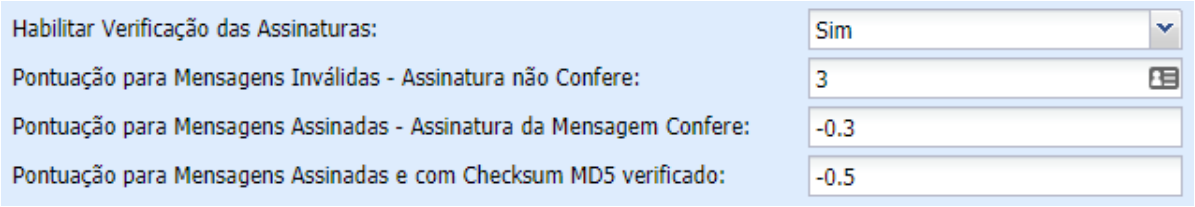
Opções	Definição
Salvar	Quando clicado, grava as configurações realizadas.

Definições de Opções - Verificação

Estas informações descrevem as opções disponíveis nesta página.

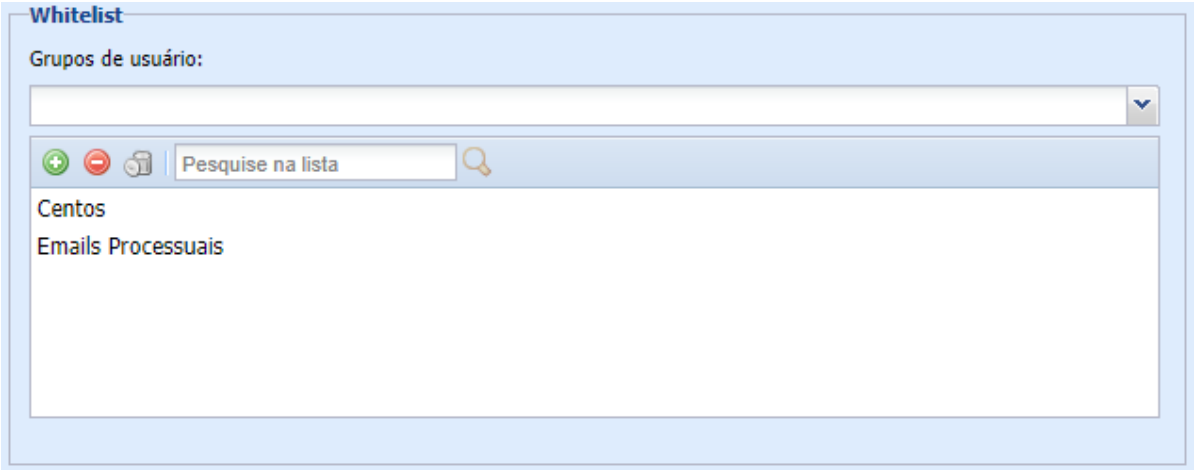
Opções	Definição
Habilitar Verificação de Assinaturas	Escolha entre: • **Sim** - Indica que a verificação de DKIM está ativa. • **Não** - Indica que a verificação de DKIM está desativada.

Pontuação para Mensagens Inválidas - Assinatura não Confere	Informe o valor da pontuação atribuída as mensagens consideradas inválidas.
Pontuação para Mensagens Assinadas - Assinatura da Mensagem Confere	Informe o valor da pontuação atribuída as mensagens que foram assinadas com DKIM.
Pontuação para Mensagens Assinadas e com Checksum MD5 verificado	Informe o valor da pontuação atribuída as mensagens que foram assinadas com DKIM e certificadas como válidas.



Definições de Opções - Whitelist

Adicione aqui os grupos de usuários "Endereços, IPs, Ranges, Domínios, etc" que não deverão ser validados pelo sistema DKIM.



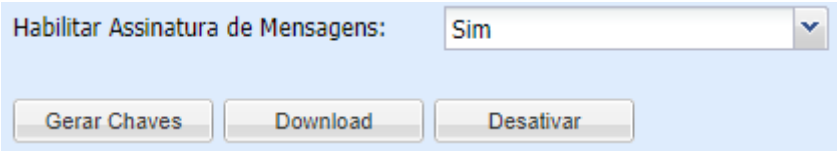
Definições de Opções - Assinatura

A função da aba Assinatura é ativar/desativar o DKIM para e-mails de saída e gerenciar chaves de criptografia de DKIM.

Ao ativar uma assinatura DKIM para um determinado domínio, é gerada uma chave e ela é atrelada aos e-mails de saída do domínio selecionado. Importante salientar que a chave é por domínio e selector, permitindo que tenha mais de uma chave DKIM por domínio, mudando somente o selector.

Após ativado o DKIM para o domínio selecionado, a etapa seguinte é mandar gerar a chave (bastando clicar no botão Gerar Chaves) e depois, fazer download da indicação de entrada no DNS do domínio selecionado. Uma vez baixado a string, basta incluí-la no seu DNS. Após a publicação do DNS, o DKIM estará ativo e funcional.

Opções	Definição
Habilitar Assinatura de Mensagens	Escolha entre: • **Sim** - Indica que a assinatura de mensagens através do DKIM está ativa. • **Não** - Indica que a assinatura de mensagens através do DKIM está desativada.
Gerar Chaves	Permite ativar a assinatura de mensagens para o domínio selecionado, através da geração de chave única de criptografia.
Download	Permite baixar a chave pública de criptografia do domínio selecionado, que deve ser adicionada ao registro DNS do domínio.
Desativar	Permite desativar a assinatura de mensagens para o domínio selecionado.



Ao efetuar o DOWNLOAD da chave gerada (chave pública), o sistema disponibilizará o arquivo para download em arquivo padrão TXT.

O arquivo já vem no padrão a ser incrementado no DNS da empresa. Segue exemplo:

default._domainkey IN TXT "v=DKIM1; k=rsa; p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDMKXWJrMWm4lOGlWi7v6CD08GcPmd7vj98Yh6u4sK1zNDudhNWwoEEmFl4BoRjLsT7if85M0GwTKX0MrzDEyi04FCEFYtHTtSqmS4Wds2QapGdWdVJjcEzG55j23Q04HGfxNRHZJOvr+lm8hTCBH0Y123DKjFk1pqoFcroNWfBaQIDAQAB" ;

DMARC

DMARC é um sistema de validação de e-mail criado pelo PayPal junto com o Google, Microsoft e Yahoo.

Com o DMARC, uma organização obtém insights e controle sobre quem está mandado e-mail usando o seu domínio como origem do e-mail. As organizações podem usar o DMARC para proteger suas marcas contra o abuso em ataques de phishing ou Spoofing de terceiros.

Configurações **/ Anti Spoofing / DMARC**

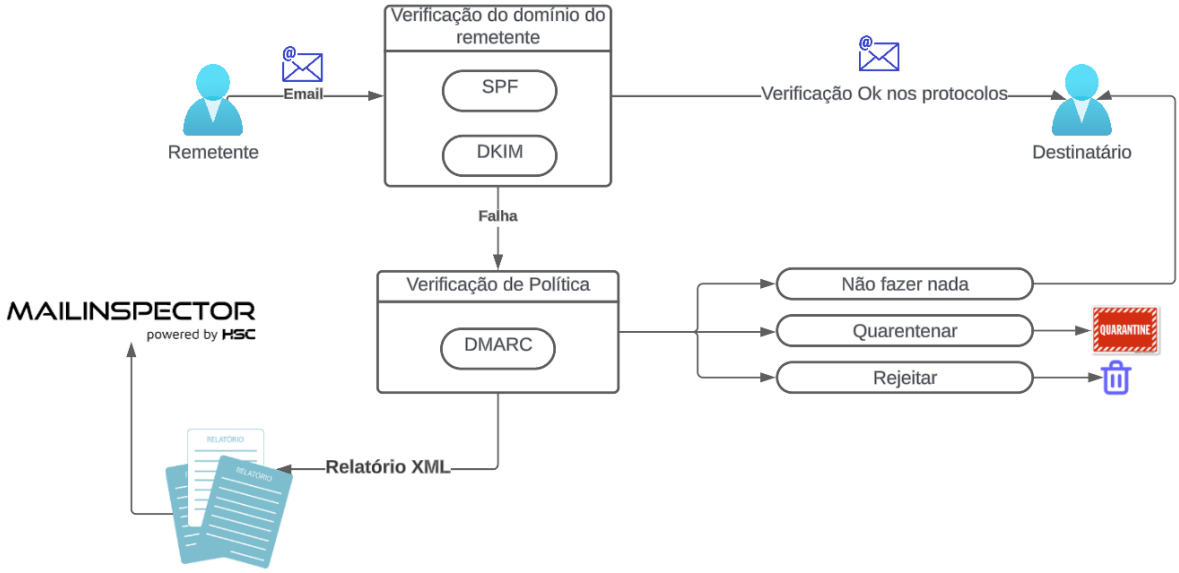
Visão geral do DMARC

DMARC (Domain-based Message Authentication, Reporting, and Conformance) é uma especificação do IETF **RFC 7489.**

Este novo padrão baseia-se nos protocolos SPF e DKIM adicionando ligação ao nome de domínio do autor ("De:"), políticas publicadas para tratamento de falhas de autenticação e relatórios de receptores para remetentes, para melhorar e monitorar a proteção do domínio de e-mail fraudulento.

O DMARC é um mecanismo de autenticação de mensagens eletrônicas que permite ao remetente garantir aos seus destinatários que as mensagens que irão receber partiram da organização de origem (valida as mensagens). Em outras palavras, DMARC é um conjunto de regras que permite aos remetentes e destinatários trabalharem em conjunto detectando e tratando os e-mails fraudulentos. O DMARC é basicamente um novo padrão que visa unificar as validações atuais.

A grande diferença entre o DMARC e outros sistemas, é que com o DMARC será possível o administrador do domínio receber alertas (reports) de servidores que estão tentando mandar e-mail usando o seu domínio, dessa forma, o aviso é preventivo, ou seja, o administrador poderá tomar ação de proteção “antes” de algum usuário cair em golpes.



Desenho do funcionamento do DMARC.
Para todas as entradas de e-mails, são registrados os dados e enviados diariamente em um relatório no formato XML para um endereço de e-mail estipulada pela entrada no DNS (registro DMARC)

O MailInspector permite o envio de relatórios agregados (RUA - Reporting URI(s) for aggregate data) e forenses/falhas (RUF - Reporting URI(s) for failure data) para endereços configurados pelo administrador.

Para maiores informações sobre o DMARC visite o website https://dmarc.org

DMARC – Verificação

Nesta aba é possível verificar toda a configuração referente ao DMARC, para ativação de uso de DMARC, bem como envio de relatórios padrão RUF ou RUA e a ação a ser tomada quando ocorrer algum erro de DMARC nos e-mails recebidos.

Definições de Opções - DMARC

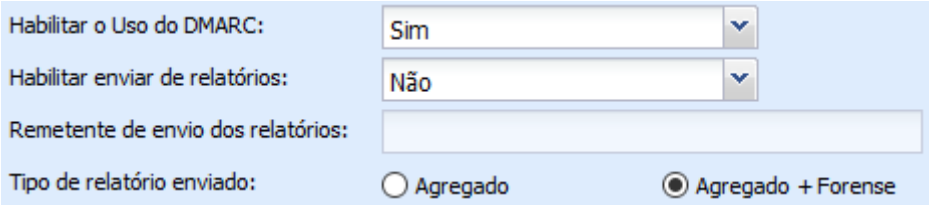
Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição
Salvar	Quando clicado, grava as configurações realizadas.

Definições de Opções - Verificação

Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição
Habilitar o Uso do DMARC	Escolha entre: • **Sim** - Indica que o DMARC estará ativo. • **Não** - Indica que o DMARC estará desativado.
Habilitar enviar relatórios	Escolha entre: • **Sim** - Indica que o envio de relatórios estará ativo • **Não** - Indica que o envio de relatório estará desativado.
Remetente de envio dos relatórios	Define o endereço do remetente dos relatórios.
Tipo de relatório enviado	**Agregado:** É o relatório que contabiliza o total diário. **Agregado + Forense:** É o relatório agregado mais o relatório específico com os dados de ataque (falhas) verificado pelo DMARC.



É enviado um relatório diário (dos acumulados do dia), dessa forma não sobrecarregando o sistema de envio de e-mails.

Definições para Ações FAIL do DMARC

Estas informações descrevem as opções disponíveis nesta página.

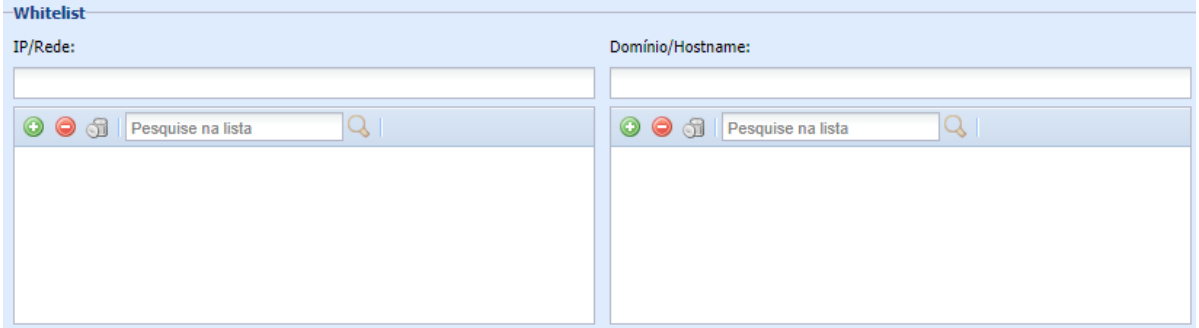
Opções	Definições Possíveis
Bloquear	Bloqueia a msg não entregando ao destinatário colocando em quarentena.
Ignorar	Não realiza ação na mensagem recebida.
Pontuar	Adiciona uma pontuação para contabilizar no sistema de antispam HSC.

Definições de Opções - Whitelist

É possível criar whitelist para o DMARC, ao qual não serão verificados os registros indicados quanto a esse protocolo de segurança.

Aceita-se as entradas em:

- Endereços de IP;
- Range de IP;
- Classe de IP;
- Rede;
- Domínios;
- Hostnames



Indicação de preenchimento de Whitelist do DMARC

DMARC – Análise de Relatórios

Nesta aba é verificada a configuração de coleta das informações dos relatórios XML, onde podemos configurar as contas de e-mails utilizados para a coleta dos XMLs utilizados pelo Analisador de DMARC.

Definições para Análise de Relatórios

Estas informações descrevem as opções disponíveis nesta página.

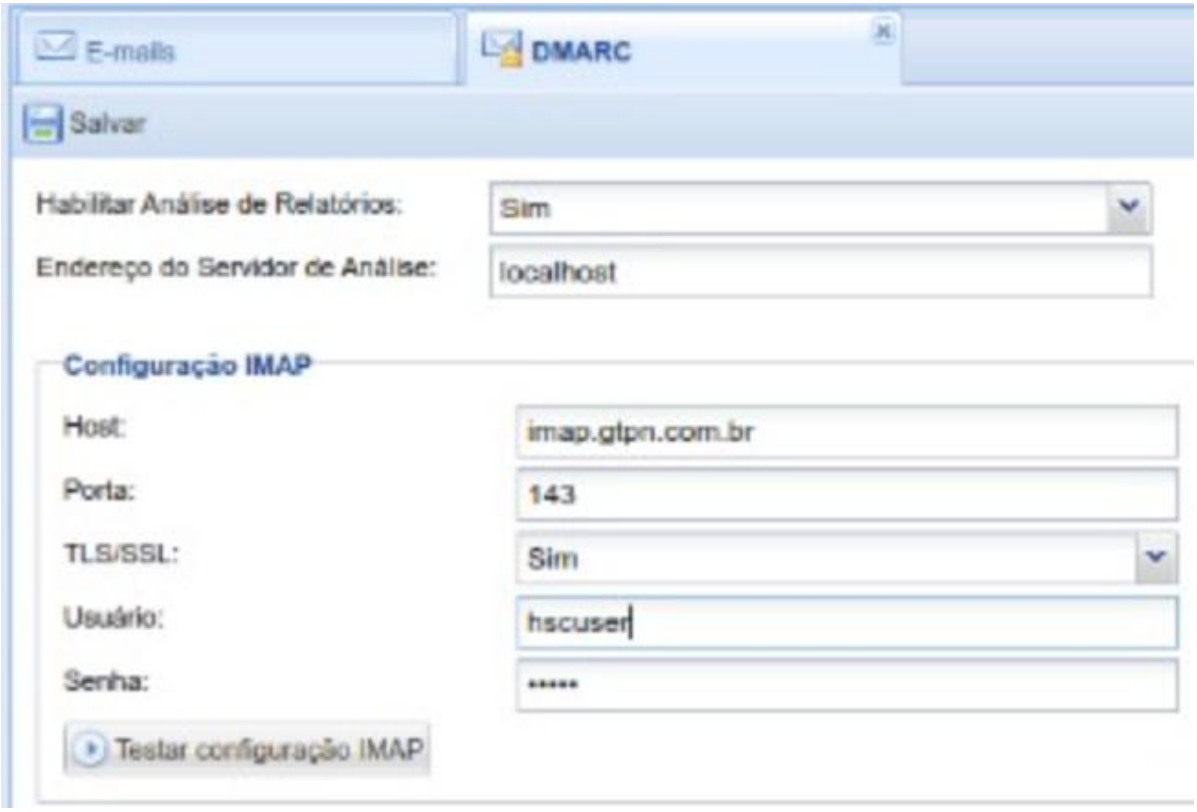
Opções	Definição
Salvar	Quando clicado, grava as configurações realizadas.

Habilitar Análise de Relatórios	Sim – Habilita o Analisador de Relatórios Não – Desabilita o Analisador de Relatórios
Endereço do Servidor de Análise	Endereço do servidor de análise

Configuração IMAP

Dados do IMAP a ser utilizado para a coleta dos XMLs

Opções	Definição
Host	Servidor de e-mail que hospeda XMLs enviados pelos ISPs
Porta	Porta utilizada pelo protocolo IMAP
TLS/SSL	Sim – Habilita o uso de TLS/SSL para o IMAP Não – Dedativa o protocolo TLS/SSL para o IMAP
Usuário	Usuário utilizado para a autenticação do IMAP
Senha	Senha utilizada para a autenticação do IMAP
Testar configuração IMAP	Testa as credenciais, bem como a conexão com o servidor IMAP



Tela de configuração da conta IMAP utilizada para a coleta de relatórios RUF /RUA padrão XML

Definições de Analisador de DMARC

Os relatórios agregados e forenses do DMARC contêm muitas informações úteis, mas o feedback XML precisa ser processado, rearranjado e visualizado para dar aos humanos uma chance de entender o que esse relatório significa. Sem esse processamento, você provavelmente terá dificuldade em entender seus Relatórios DMARC. Pensando nisso, o MailInspector coleta esses relatórios padrão XML e os transforma em dados elegíveis.

O que os relatórios DMARC indicam?

- Quais servidores ou remetentes de terceiros estão enviando e-mails usando o seu domínio;
- Qual a porcentagem de mensagens de seu domínio que passam no DMARC;
- Quais servidores ou serviços estão enviando mensagens que falham no DMARC;
- Quais ações DMARC o servidor receptor realiza em mensagens não autenticadas de seu domínio:
    - None;
    - Quarantine;
    - Reject;

Por que usar o Analisador de DMARC do MailInspector?

- Os relatórios XML DMARC são muito difíceis de ler;
- É praticamente impossível interpretar as informações em XML puro, dessa forma não é possível resolver problemas de entrega de e-mail (Spoofing de criminosos usando o seu domínio como origem);

Uma vez ativado o DMARC, com o endereço RUA e/ou RUF devidamente configurado, os endereços indicados receberão múltiplos relatórios XML de diversas fontes (tais como Google, Yahoo, Amazon, etc), dessa forma é praticamente impossível analisar os dados de arquivo em arquivo. O MailInspector permite combinar todos os relatórios DMARC recebidos, dessa forma é obtida uma visão completa de todos os e-mails enviados em nome de seu domínio, detectando possíveis e-mails fraudulentos oriundos de IP's que não possuem permissão de envio "usando o seu domínio".

O MailInspector possui sistema de análise de relatórios enviados a uma determinada conta de e-mail, indicado pelo registro DNS do DMARC. Existem dois tipos de análise:

- Analítico;
- Forense;

Para o uso da coleta de e-mails pelo sistema de análise de DMARC do MailInspector, o administrador deverá configurar no seu DNS o RUF e RUA do DMARC para o mesmo e-mail.

O MailInspector diferencia os relatórios XML analítico do XML forense pelo formato do relatório XML emitido. Dessa forma, não há a necessidade de cadastrar duas contas de e-mail diferentes, sendo um só para o relatório analítico e outro para o forense. O MailInspector consegue diferenciar de forma inteligente e automática esses relatórios, analisando ambos os relatórios e agrupando os dados relevantes, bem como gerando os gráficos para análise do administrador.

Relatórios de análise forense

Os relatórios de análise forense são criados apenas quando o ISP recebe uma mensagem que falha na autenticação DMARC. Os relatórios forenses contêm dados de amostra que indicam que há um problema com uma determinada fonte, fluxo de correio ou IP de envio. Os relatórios forenses contêm dados no nível da mensagem, endereços de e-mail "Para" e "De" e os endereços IP do remetente. Também é possível ver o corpo de uma mensagem.

Os relatórios forenses podem conter as seguintes informações:

- Linha de assunto
- Horário em que a mensagem foi recebida
- Informações de IP;
- Resultados de autenticação
    - Resultado de SPF;
    - Resultado de DKIM;
    - Resultado de DMARC;
- Informações de domínio de:
    - Endereço DE
    - Endereço de correio
    - Endereço de DKIM DE
- Mensagem ID;
- URLs;
- Resultado da entrega;
- Qual foi a política aplicada, a mensagem pode ser rejeitada se houver uma política de rejeição em vigor, ou colocada em quarentena ou entregue devido a nenhuma política;
- Informações do ISP;

Relatórios de agregado

Os relatórios agregados DMARC (Domain-based Message Authentication, Reporting and Conformance) contém informações sobre o status de autenticação de mensagens enviadas em nome de um domínio. Com os relatórios, uma organização pode ver quais e-mails estão sendo autenticados no DKIM (DomainKeys Identified Mail) e SPF (Sender Policy Framework). Também é visível quais e-mails não estão sendo autenticados.

Um relatório agregado não contém nenhuma informação sobre os próprios e-mails. Os relatórios agregados DMARC contêm informações sobre a origem que enviou a mensagem, o domínio que foi usado para enviar essas mensagens, o IP de envio, a quantidade de mensagens enviadas em uma data específica, o domínio de envio DKIM / SPF, a autenticação DKIM / SPF resultado e o resultado DMARC. Todas essas informações são muito úteis para uma organização determinar quem está enviando e-mail em seu nome, se um remetente tem permissão para enviar e-mail em seu nome e se as mensagens são autenticadas corretamente. Além disso, uma organização pode ver quem está enviando e-mails maliciosos em seu nome.

O que está incluído no relatório agregado do DMARC?

1. Informações do ISP

- Número de identificação do relatório;
- Nome da organização relatora;
- Organização relatora de envio de endereço de e-mail e informações de contato adicionais;
- Intervalo de dados inicial e final em segundos;

2. Descrição do registro DMARC

- Domínio do cabeçalho / do domínio;
- Configurações de alinhamento para DKIM e SPF;
- Política de domínio (rejeitar);
- Política de subdomínio (rejeitar);
- Porcentagem de mensagens às quais a política DMARC deve ser aplicada;

3. Resumo dos resultados de autenticação

- IP identificado no e-mail;
- Total de endereços IP identificados;
- Disposição da mensagem, para mostrar se a política foi aplicada;

- Resultado da autenticação DKIM, o domínio e o resultado;
- Resultado da autenticação SPF, o domínio e o resultado;

O MailInspector coleta ambos os relatórios emitidos e os converte em dados relevantes para uma análise mais precisa e de fácil compreensão.

Por padrão usamos o IMAP para comunicação e coleta dos relatórios enviados à conta de e-mail configurado no registro DMARC (RUF e RUA). Seguem informações de configuração de Analisador de DMARC:

Opções	Definição
Salvar	Quando clicado, grava as configurações realizadas.
Servidor	IP do Servidor de E-mail
Porta IMAP	Indicação da Porta utilizada para coleta dos e-mails através do protocolo IMAP
Login	Login do SERVIDOR
Senha	Senha para acesso a conta IMAP
Usa SSL/TLS	Indique o protocolo de criptografia utilizado no IMAP configurado no servidor de e-mail, podendo ser: • Nenhum; • SSL/TLS; • STARTTLS;

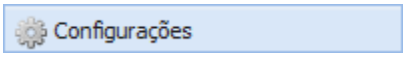
Os relatórios gerados a partir dos XMLs coletados pela conta de e-mail acima configurado, poderão ser visualizados em RealTime > DMARC.

O módulo Analisador de DMARC é um módulo do HSC MailInspector licenciado à parte, para o uso do mesmo é necessário aquisição da licença específica para este fim.

Notificações

Configurações Gerais

Use esta página para exibir, adicionar, editar ou excluir configurações gerais das Notificações (bounces).



/ Notificações / Configurações Gerais

Visão geral das configurações gerais de Notificações

Permite configurar e administrar o **sistema de notificações do MailInspector**, possibilitando o envio de alertas relacionados a mensagens bloqueadas, eventos de segurança e demais ocorrências identificadas pelo sistema.

Para as mensagens bloqueadas pelo sistema (**bounce**), é possível configurar notificações destinadas tanto ao **remetente quanto ao destinatário**, conforme as políticas definidas pelo administrador. Os perfis de retorno de mensagem podem ser personalizados de acordo com as necessidades da organização, permitindo definir o conteúdo e as informações apresentadas nas notificações.

O sistema também permite configurar **alertas por e-mail baseados em eventos de segurança**, possibilitando ao administrador selecionar quais tipos de eventos deverão gerar notificações, bem como definir os **destinatários responsáveis pelo recebimento dos alertas**. Dessa forma, diferentes equipes ou responsáveis podem ser notificados de acordo com a natureza do evento identificado.

As notificações podem ainda ser associadas a **níveis de severidade, criticidade ou classificação equivalente**, permitindo diferenciar eventos de acordo com seu grau de risco e priorizar a atuação dos responsáveis. Essa classificação possibilita, por exemplo, estabelecer tratamentos distintos para eventos informativos, de baixa, média, alta ou crítica severidade.

O sistema permite, portanto, configurar de forma granular **quais eventos serão monitorados, quais condições deverão gerar alertas, quem deverá recebê-los e qual nível de criticidade deverá ser atribuído**, proporcionando maior controle sobre o processo de monitoramento e resposta a incidentes de segurança.

Quando necessário, o MailInspector também permite encaminhar determinadas mensagens ou notificações a **terceiros ou destinatários adicionais**, conforme as políticas de segurança, compliance e DLP estabelecidas pela organização.

> A leitura das regras segue o padrão de firewall, ao qual lê de cima para baixo e ao encontrar uma regra que case com a condição, a mesma será executada e finalizado o processo, ou seja, não será processada nenhuma outra regra subsequente.

Definições de Opções - Configurações Gerais

Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição
Salvar	Quando clicado, grava as configurações realizadas.

Definições de Opções - Notificação de E-mails

Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição
Ativar Notificação ao Remetente/Destinatário das Mensagens que Forem Bloqueadas	Escolha entre: • **Sim** - Indica que a notificação de remetente/destinatário está ativa. Esta funcionalidade envia uma mensagem de notificação para o remetente/destinatário caso a mensagem seja bloqueada pelo sistema de filtragem. • **Não** - Indica que a notificação de remetente/destinatário está desativada.
Adicionar	Cadastra uma nova regra de notificação de mensagem bloqueada. Quando clicado, abre a caixa de diálogo **Cadastro do Controle Personalizado**.
Editar	Edita as configurações de um registro existente. Quando clicado, abre a caixa de diálogo **Cadastro do Controle Personalizado**.
Remover	Quando clicado, exclui o registro selecionado.

Definições de Opções - Notificação de E-mail com Vírus

Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição
Notificar em caso de Vírus	Escolha entre: • **Sim** - Indica que a notificação de mensagem com vírus está ativa. Esta funcionalidade envia uma mensagem de notificação para o remetente/destinatário caso a mensagem seja bloqueada pelo sistema de filtragem por conter vírus ou outra ameaça, informando os detalhes do bloqueio, tais como: Data/hora, Origem/Destino, Nome da ameaça e ID da mensagem. • **Não** - Indica que a notificação de mensagem com vírus está desativada. Nesta tela é possível selecionar se serão notificados o remetente, destinatário ou ambos
Adicionar	Cadastra uma nova regra de notificação de mensagem com vírus. Quando clicado, abre a caixa de diálogo **Cadastro do Controle Personalizado**.
Editar	Edita as configurações de um registro existente. Quando clicado, abre a caixa de diálogo **Cadastro do Controle Personalizado**.
Remover	Quando clicado, exclui o registro selecionado.

Definições de Opções - Notificação de Anexos Bloqueados

Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição

Notificar em caso de Extensão ou Mime-type bloqueado	Escolha entre: • **Sim** - Indica que a notificação de mensagem com anexo bloqueada está ativa. Esta funcionalidade envia uma mensagem de notificação para o remetente/destinatário caso a mensagem seja bloqueada pelo sistema de filtragem por conter um anexo que possua uma extensão ou tipo de arquivo não permitido. • **Não** - Indica que a notificação de mensagem com anexo bloqueada está desativada.
Adicionar	Cadastra uma nova regra de notificação de mensagem com anexo bloqueado. Quando clicado, abre a caixa de diálogo **Cadastro do Controle Personalizado**.
Editar	Edita as configurações de um registro existente. Quando clicado, abre a caixa de diálogo **Cadastro do Controle Personalizado**.
Remover	Quando clicado, exclui o registro selecionado.

Definições de Opções - Notificação de Tamanho Excedido

Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição
Notificar em caso de Tamanho Excedido	Escolha entre: • **Sim** - Indica que a notificação de mensagem com tamanho excedido está ativa. Esta funcionalidade envia uma mensagem de notificação para o remetente/destinatário caso a mensagem seja bloqueada pelo sistema de filtragem por ter excedido o tamanho máximo permitido. • **Não** - Indica que a notificação de mensagem com tamanho excedido está desativada.
Adicionar	Cadastra uma nova regra de notificação de mensagem com tamanho excedido. Quando clicado, abre a caixa de diálogo **Cadastro do Controle Personalizado**.
Editar	Edita as configurações de um registro existente. Quando clicado, abre a caixa de diálogo **Cadastro do Controle Personalizado**.
Remover	Quando clicado, exclui o registro selecionado.

Definições de Opções - Notificação de Web Attacks

Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição
Notificar em caso de Web Attacks	Escolha entre: • **Sim** - Indica que a notificação de mensagem com web attack está ativa. Esta funcionalidade envia uma mensagem de notificação para o remetente/destinatário caso a mensagem seja bloqueada pelo sistema de filtragem por conter algum tipo de web attack. • **Não** - Indica que a notificação de mensagem com web attack está desativada.
Adicionar	Cadastra uma nova regra de notificação de mensagem com web attack. Quando clicado, abre a caixa de diálogo **Cadastro do Controle Personalizado**.

Editar	Edita as configurações de um registro existente. Quando clicado, abre a caixa de diálogo **Cadastro do Controle Personalizado**.
Remover	Quando clicado, exclui o registro selecionado.

Definições de Opções - Notificação do Administrador

Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição
Notificar o Administrador em caso de mensagens bloqueadas	Escolha entre: • **Sim** - Indica que a notificação para o administrador no caso de mensagem bloqueada está ativa. Esta funcionalidade envia uma mensagem de notificação para o administrador caso a mensagem seja bloqueada pelo sistema de filtragem. • **Não** - Indica que a notificação para o administrador no caso de mensagem bloqueada está desativada.
E-mail do Administrador	Informe o endereço de e-mail do administrador que receberá as mensagens de notificação. Ex.: administrador@empresa.com.br
Adicionar	Cadastra uma nova regra de notificação para o administrador no caso de mensagem bloqueada. Quando clicado, abre a caixa de diálogo **Cadastro do Controle Personalizado**.
Editar	Edita as configurações de um registro existente. Quando clicado, abre a caixa de diálogo **Cadastro do Controle Personalizado**.
Remover	Quando clicado, exclui o registro selecionado.

Definições de Opções - Cadastro do Controle Personalizado

Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição
Adicionar	Quando clicado, adiciona o controle personalizado.
Cancelar	Quando clicado, cancela a ação.
De	Selecione o grupo pré-cadastrado de remetentes.
Para	Selecione o grupo pré-cadastrado de destinatários.
Ação	Escolha entre: • **Sim** - Indica que a regra será aplicada, quando os remetentes e os destinatários pertencerem aos grupos selecionados. • **Não** - Indica que a regra não será aplicada, quando os remetentes e os destinatários pertencerem aos grupos selecionados.

Padronização

Use esta página para exibir ou modificar o padrão das respostas de notificação enviadas aos usuários.

Configurações **/ Notificações / Padronização**

Visão geral da padronização dos e-mails de notificação

O item Padronização permite personalizar as mensagens enviadas pelo sistema de notificação, quando as mensagens são bloqueadas pelo sistema de filtragem de conteúdo. As notificações podem ser configuradas para serem enviadas ao remetente, destinatário ou a terceiros, de acordo com a configuração efetuada pelo administrador da solução.

É obrigatório nas mensagens de padronização possuir os seguintes campos no início da mensagem customizada:
From: $to
To: $from
Subject: <Título do E-mail>
Caso não tenha os campos acima citados, o e-mail de notificação não será disparado!

```
From: "$postmastername" <$localpostmaster>
To: $from
Subject: Aviso: Sistema de Filtragem de E-MAIL - HSC MAILINSPECTOR
X-%org-name%-HSC_MailInspector: generated

Nossos filtros de conte►do de E-Mail foram ativados por uma mensagem
que voce enviou :
  Para: $to
  Assunto: $subject
  Data: $date

Um ou mais dos anexos encontra-se na lista de tipos de arquivo
proibidos pelo sistema e nao podera ser entregue.
```

Exemplo de Padronização de Notificação com os campos obrigatórios presentes na mensagem

Todo o conteúdo pode ser customizado conforme a necessidade do administrador. Abaixo segue uma lista de macros para ser utilizadas para substituição em tempo real pela ferramenta a fim de melhor personalizar as repostas:

Variáveis	Representação no e-mail
$from	Remetente
$to	Destinatário
$date_year	Ano do recebimento do e-mail
$date_month	Mês do recebimento do e-mail
$date_day	Dia do recebimento do e-mail
$date_hour	Hora do recebimento do e-mail
$date_minute	Minuto do recebimento do e-mail
$date_second	Segundo do recebimento do e-mail

$subject	Assunto da mensgaem
$proto	Protocolo utilizado na varredura
$report	Report dado pela ferramenta de antivírus Ex: Nome do Arquivo infectado, Nome do Vírus que infectou, grupo de ameaça (trojan, ransomware, worm, etc) entre outras informações apresentadas pelo sistema de detecção de vírus.
$action	Ação tomada sobre o arquivo infectado
$messagesize	Tamanho da mensagem
$maxmessagesize	Tamanho máximo configurado da mensagem
$quarantine	Quarentena
$postmastername	Display Name do DaemonMail
$localpostmaster	E-mail do DaemonMail
$notification	Link de solicitação de notificação de quarentena
\n	Quebra de linha

Definições de Opções - Padronização

Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição
Salvar	Quando clicado, grava as configurações realizadas.

Definições de Opções - Resposta Conteúdo Bloqueado

Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição
Resposta para os Remetentes	Personalize a mensagem que será enviada ao remetente, caso o sistema de filtragem bloqueie uma mensagem pelo seu tipo de conteúdo.
Resposta para os Destinatários	Personalize a mensagem que será enviada ao destinatário, caso o sistema de filtragem bloqueie uma mensagem pelo seu tipo de conteúdo.

Definições de Opções - Resposta Anexo Bloqueado por Tipo

Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição
Resposta para os Remetentes	Personalize a mensagem que será enviada ao remetente, caso o sistema de filtragem bloqueie uma mensagem por conter em anexo um tipo de arquivo com extensão não permitida.
Resposta para os Destinatários	Personalize a mensagem que será enviada ao destinatário, caso o sistema de filtragem bloqueie uma mensagem por conter em anexo um tipo de arquivo com extensão não permitida.

Definições de Opções - Resposta Anexo Bloqueado por Tamanho

Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição

Resposta para os Remetentes	Personalize a mensagem que será enviada ao remetente, caso o sistema de filtragem bloqueie uma mensagem por conter em anexo um tipo de arquivo com o tamanho maior que o permitido.
Resposta para os Destinatários	Personalize a mensagem que será enviada ao destinatário, caso o sistema de filtragem bloqueie uma mensagem por conter em anexo um tipo de arquivo com o tamanho maior que o permitido.

Definições de Opções - Resposta Bloqueio por Ameaça

Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição
Resposta para os Remetentes	Personalize a mensagem que será enviada ao remetente, caso o sistema de filtragem bloqueie uma mensagem por conter em anexo malicioso.
Resposta para os Destinatários	Personalize a mensagem que será enviada ao destinatário, caso o sistema de filtragem bloqueie uma mensagem por conter em anexo malicioso.

Definições de Opções - Criptografia

Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição
Resposta para os Remetentes	Personalize a mensagem que será enviada ao destino do e-mail criptografado. Essa notificação indicará ao recebedor do e-mail a data do envio do e-mail criptografado, remetente do e-mail criptografado e o assunto. Também dará instruções para o destinatário sobre como deve proceder para a leitura do e-mail criptografado. **Obs:** Este template é em formato HTML, permitindo ao administrador customizar do jeito que achar necessário, até mesmo com a troca da logomarca.

Definições de Opções - Resposta Mensagens Rejeitadas

Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição
Resposta para os Remetentes	Personalize a mensagem que será enviada ao remetente, caso o sistema de filtragem rejeite o recebimento de uma mensagem.
Resposta para os Destinatários	Personalize a mensagem que será enviada ao destinatário, caso o sistema de filtragem rejeite o recebimento de uma mensagem.

Definições de Opções - Resposta Mensagens DLP

Personalização da mensagem quando ativada regra de DLP.

Opções	Definição
Resposta para os Remetentes	Personalize a mensagem que será enviada ao remetente, caso o sistema de filtragem notifique o recebimento de uma mensagem que se casou com uma regra de DLP.

Resposta para os Destinatários	Personalize a mensagem que será enviada ao destinatário, caso o sistema de filtragem notifique o recebimento de uma mensagem que se casou com uma regra de DLP.

Definições de Opções - Resposta Mensagens Criptografadas

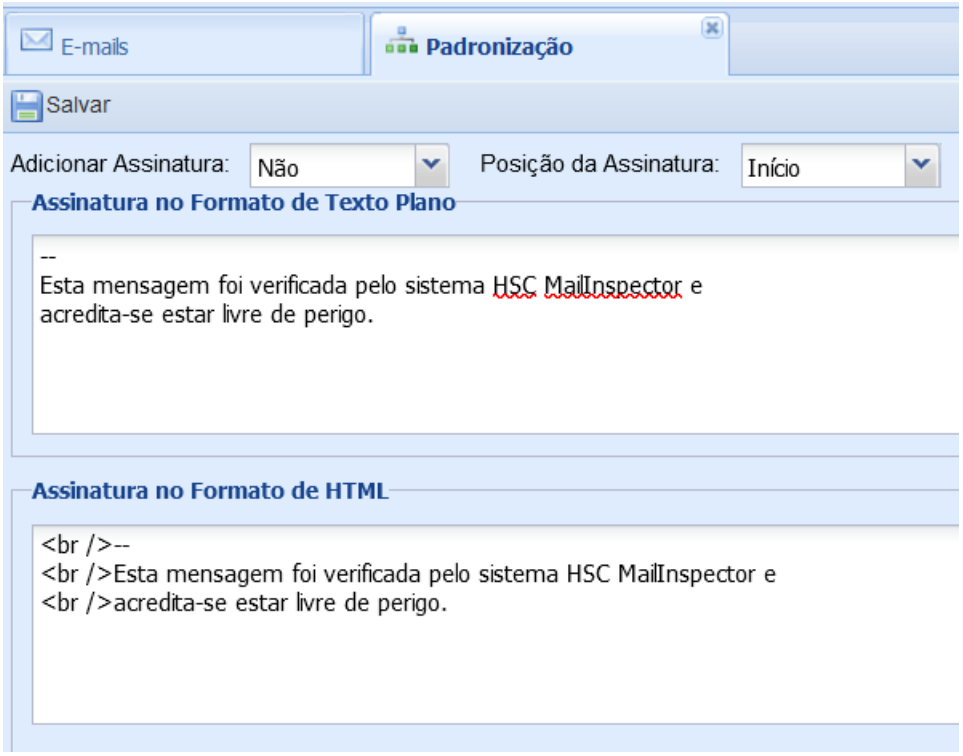
Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição
Resposta para os Destinatários	Personalize a mensagem que será enviada ao destinatário, caso o sistema de filtragem criptografe o envio de uma mensagem.

Definições de Opções - Assinatura de E-mails

É possível customizar um Disclaimer ou alteração no corpo da mensagem, incluindo/alterando textos no seu conteúdo, conforme a necessidade da empresa.

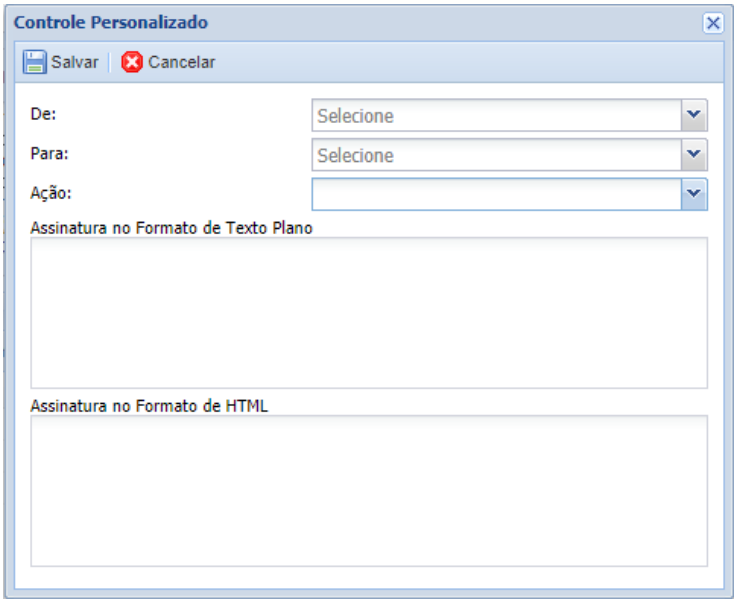
Opções	Definição
Adicionar Assinatura	Ativa ou desativa a assinatura nas mensagens deixando como padrão a seleção marcada. Escolha entre: • **Sim** - Indica que a inclusão automática da assinatura personalizada por domínio está ativada. Esta funcionalidade permite adicionar automaticamente no final da mensagem uma assinatura personalizada. • **Não** - Indica que a inclusão automática da assinatura personalizada está desativada.
Posição da Assinatura	**Início:** Insere a assinatura indicada no início do e-mail. **Final:** Insere a assinatura indicada no final do e-mail.
Assinatura no Formato de Texto Plano	Informe uma assinatura padronizada a ser personalizada que será adicionada ao final das mensagens que forem enviadas no formato de texto plano.
Assinatura no Formato de HTML	Informe uma assinatura padronizada a ser personalizada que será adicionada ao final das mensagens que forem enviadas no formato HTML.
Adicionar	Cadastra uma nova regra de assinatura personalizada. Quando clicado, abre a caixa de diálogo **Cadastro do Controle Personalizado**.
Editar	Edita as configurações de um registro existente. Quando clicado, abre a caixa de diálogo **Cadastro do Controle Personalizado**.
Remover	Quando clicado, exclui o registro selecionado.



Definições de Opções - Cadastro do Controle Personalizado

Configura múltiplos disclaimers/textos alterados ou incluídos de acordo com grupos de origem e grupos de destino, cada qual com um disclaimer/textos alterados ou incluídos, conforme necessidade da empresa. Dessa forma é possível controlar quando será ativado o disclaimer (customizado) e para qual situação, ex: ativar disclaimer de alerta de e-mail externo somente para quando o e-mail vier de fora para o setor financeira da empresa, para todo o resto da empresa, usar-se o disclaimer padrão, ou ainda, ativar o disclaimer para determinados domínios de origem ou destino.

Opções	Definição
Adicionar	Quando clicado, adiciona o controle personalizado.
Cancelar	Quando clicado, cancela a ação.
De	Selecione o grupo pré-cadastrado de remetentes.
Para	Selecione o grupo pré-cadastrado de destinatários.
Assinatura no Formato de Texto Plano	Informe uma assinatura personalizada que será adicionada ao final das mensagens que forem enviadas no formato de texto plano.
Assinatura no Formato de HTML	Informe uma assinatura personalizada que será adicionada ao final das mensagens que forem enviadas no formato HTML.
Ação	Escolha entre: • **Sim** - Indica que a regra será aplicada, quando os remetentes e os destinatários pertencerem aos grupos selecionados. • **Não** - Indica que a regra não será aplicada, quando os remetentes e os destinatários pertencerem aos grupos selecionados.



Definições de Opções – Data Loss Prevention

Configuração de mensagem em caso de detecção de regras de DLP.

Opções	Definição
Resposta para os Remetentes	Configuração da mensagem de retorno para o(s) remetente(s) do e-mail em caso de ter sido ativado a regra de DLP.
Resposta para os Destinatários	Configuração da mensagem para o(s) destinatário(s) do e-mail em caso de ter sido ativado a regra de DLP.

Definições de Opções – Outros Bloqueios

Configuração de mensagem em caso de detecção de regras em outros tipos de bloqueios (além dos que já foram mencionados anteriormente).

Opções	Definição
Resposta para os Destinatários	Configuração da mensagem para o(s) destinatário(s) do e-mail em caso de ter sido barrado por algum outro motivo (bloqueio de anexo).

Modificação do Assunto

Use esta página para exibir, adicionar, editar ou excluir modificações no assunto da mensagem.

Configurações **/ Notificações / Modificação do Assunto**

Visão geral da modificação do assunto

O item Modificação do Assunto permite personalizar o assunto das mensagens classificadas pelo sistema de filtragem de conteúdo e filtragem de SPAM. Esta personalização é adicionada no início do assunto, permitindo que o usuário crie regras de filtragem diretamente no software cliente de e-mail.

Definições de Opções - Modificação do Assunto

Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição
Salvar	Quando clicado, grava as configurações realizadas.

Definições de Opções - Provável SPAM

Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição
Modificar o Assunto das Mensagens Categorizadas como Provável SPAM	Escolha entre: • **Sim** - Indica que a modificação de assunto para mensagens categorizadas como provável SPAM está ativa. Esta funcionalidade adiciona um texto personalizado no início do assunto para mensagens que foram classificadas como provável SPAM. • **Não** - Indica que a modificação de assunto para mensagens categorizadas como provável SPAM está desativada.
Texto Inserido no Assunto das Mensagens	Permite personalizar o texto que será inserido no início do assunto da mensagem.
Adicionar	Cadastra uma nova regra de modificação do assunto de mensagens classificadas como provável SPAM. Quando clicado, abre a caixa de diálogo **Cadastro do Controle Personalizado**.
Editar	Edita as configurações de um registro existente. Quando clicado, abre a caixa de diálogo **Cadastro do Controle Personalizado**.
Remover	Quando clicado, exclui o registro selecionado.

Definições de Opções - SPAM

Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição
Modificar o Assunto das Mensagens Categorizadas como SPAM	Escolha entre: • **Sim** - Indica que a modificação de assunto para mensagens categorizadas como SPAM está ativa. Esta funcionalidade adiciona um texto personalizado no início do assunto para mensagens que foram classificadas como SPAM. • **Não** - Indica que a modificação de assunto para mensagens categorizadas como SPAM está desativada.
Texto Inserido no Assunto das Mensagens	Permite personalizar o texto que será inserido no início do assunto da mensagem.
Adicionar	Cadastra uma nova regra de modificação do assunto de mensagens classificadas como SPAM. Quando clicado, abre a caixa de diálogo **Cadastro do Controle Personalizado**.
Editar	Edita as configurações de um registro existente. Quando clicado, abre a caixa de diálogo **Cadastro do Controle Personalizado**.
Remover	Quando clicado, exclui o registro selecionado.

Definições de Opções - Conteúdo Perigoso

Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição
Modificar o Assunto das Mensagens Categorizadas como Conteúdo Perigoso	Escolha entre: • **Sim** - Indica que a modificação de assunto para mensagens categorizadas como conteúdo perigoso está ativa. Esta funcionalidade adiciona um texto personalizado no início do assunto para mensagens que foram classificadas como conteúdo perigoso. • **Não** - Indica que a modificação de assunto para mensagens categorizadas como conteúdo perigoso está desativada.
Texto Inserido no Assunto das Mensagens	Permite personalizar o texto que será inserido no início do assunto da mensagem.
Adicionar	Cadastra uma nova regra de modificação do assunto de mensagens classificadas como conteúdo perigoso. Quando clicado, abre a caixa de diálogo **Cadastro do Controle Personalizado**.
Editar	Edita as configurações de um registro existente. Quando clicado, abre a caixa de diálogo **Cadastro do Controle Personalizado**.
Remover	Quando clicado, exclui o registro selecionado.

Definições de Opções - Web Attacks

Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição
Modificar o Assunto das Mensagens Categorizadas como Web Attacks	Escolha entre: • **Sim** - Indica que a modificação de assunto para mensagens categorizadas como fonte de web attack está ativa. Esta funcionalidade adiciona um texto personalizado no início do assunto para mensagens que foram classificadas como fonte de web attack. • **Não** - Indica que a modificação de assunto para mensagens categorizadas como fonte de web attack está desativada.
Texto Inserido no Assunto das Mensagens	Permite personalizar o texto que será inserido no início do assunto da mensagem.
Adicionar	Cadastra uma nova regra de modificação do assunto de mensagens classificadas como fonte de web attack. Quando clicado, abre a caixa de diálogo **Cadastro do Controle Personalizado**.
Editar	Edita as configurações de um registro existente. Quando clicado, abre a caixa de diálogo **Cadastro do Controle Personalizado**.
Remover	Quando clicado, exclui o registro selecionado.

Definições de Opções - Ameaças

Estas informações descrevem as opções disponíveis nesta página. Vírus, Phishing e demais ameaças.

Opções	Definição
Modificar o Assunto das Mensagens Categorizadas como Ameaças	Escolha entre: • **Sim** - Indica que a modificação de assunto para mensagens categorizadas como ameaças está ativa. Esta funcionalidade adiciona um texto personalizado no início do assunto para mensagens que foram classificadas como Ameaças. • **Não** - Indica que a modificação de assunto para mensagens categorizadas como Ameaças está desativada.
Texto Inserido no Assunto das Mensagens	Permite personalizar o texto que será inserido no início do assunto da mensagem.
Adicionar	Cadastra uma nova regra de modificação do assunto de mensagens classificadas como ameaças. Quando clicado, abre a caixa de diálogo **Cadastro do Controle Personalizado**.
Editar	Edita as configurações de um registro existente. Quando clicado, abre a caixa de diálogo **Cadastro do Controle Personalizado**.
Remover	Quando clicado, exclui o registro selecionado.

Definições de Opções - Cadastro do Controle Personalizado

Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição
Adicionar	Quando clicado, adiciona o controle personalizado.
Cancelar	Quando clicado, cancela a ação.
De	Selecione o grupo pré-cadastrado de remetentes.
Para	Selecione o grupo pré-cadastrado de destinatários.
Ação	Escolha entre: • **Sim** - Indica que a regra será aplicada, quando os remetentes e os destinatários pertencerem aos grupos selecionados. • **Não** - Indica que a regra não será aplicada, quando os remetentes e os destinatários pertencerem aos grupos selecionados.

E-mail Compliance

A parte de Compliance de E-mail compreende o sistema de:

- Criptografia de E-mails;
- Data Loss Prevention;
- Quarentena Customizada;

Gerenciar Fingerprint

Use esta página para exibir, adicionar, editar ou excluir grupos de fingerprint.

Configurações **/ E-mail Compliance / Gerenciar Fingerprint**

Visão geral do cadastro de fingerprint

Os grupos de fingerprint são utilizados para agrupar arquivos com até cinco megabytes que serão submetidos a alguma regra de Compliance.

Permite que o administrador faça um Upload de um arquivo para que o HSC MailInspector crie uma assinatura específica deste arquivo.

A impressão digital de arquivos, também conhecida como impressão digital de dados ou impressão digital de documentos, é uma técnica empregada por muitas soluções de prevenção de perda de dados de rede para identificar e rastrear dados em uma rede, mas no caso do MailInspector é utilizado para rastrear e-mails com o documento indicado pelo fingerprint.

Na função de DLP, ao possuir regra de detecção de vazamento de dados casando com Fingerprint, o mesmo possibilita detectar variantes dos arquivos enviados ao Fingerprint, ou seja, mesmo se o arquivo "vazado" tiver sofrido alguma alteração, o sistema de DLP continuará detectando e tomando as medidas cabíveis (configuradas pelo administrador).

Definições de Opções - Gerenciamento de Fingerprint

Estas informações descrevem as opções disponíveis nesta página.

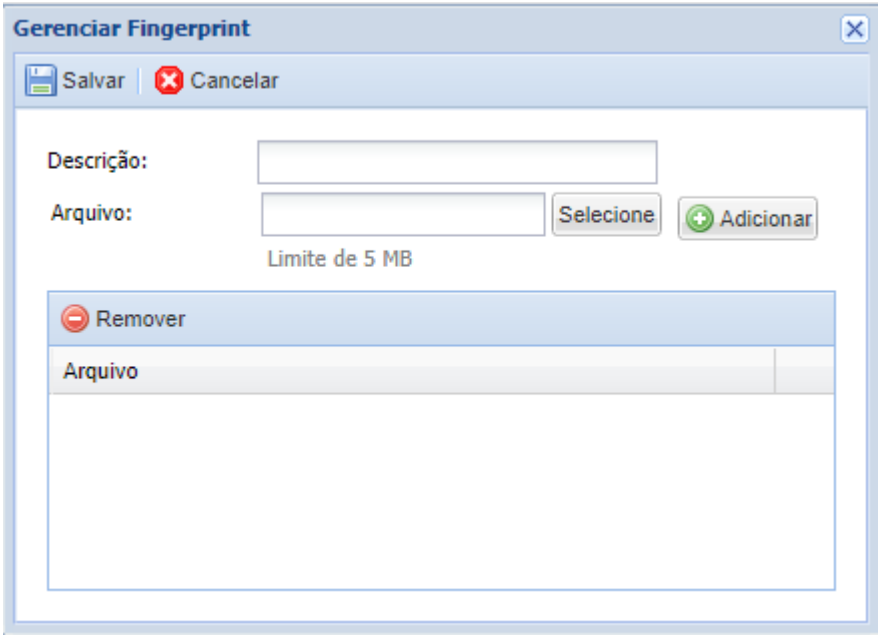
Opções	Definição
Adicionar	Cadastra um novo registro de grupo. Quando clicado, abre a caixa de diálogo **Gerenciar Fingerprint**.
Editar	Edita as configurações de um registro existente. Quando clicado, abre a caixa de diálogo **Gerenciar Fingerprint**.
Remover	Quando clicado, exclui o registro selecionado.

	⚠ Ao remover um grupo, todas as regras em que este grupo foi utilizado serão removidas do sistema.

Definições de Opções - Gerenciar Fingerprint

Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição
Salvar	Quando clicado, grava as configurações realizadas.
Cancelar	Quando clicado, cancela a ação.
Descrição	Informe a descrição de identificação do grupo. Ex.: Contratos, Orçamentos.
Remover	Quando clicado, exclui o arquivo selecionado na listagem.
Selecione	Quando clicado, permite selecionar um arquivo para ser incluído no grupo de fingerprint.
Adicionar	Quando clicado, adiciona o arquivo ao grupo de fingerprint.



Regras de Compliance

Use esta página para exibir, adicionar, editar ou excluir regras de Compliance.

Configurações **/ E-mail Compliance / Regras de Compliance**

Visão geral das regras de compliance

As regras de compliance são divididas em três tipos de controles: DLP, Criptografia e Quarentena Customizada.

DLP - O **DLP (Data Loss Prevention)** permite a criação e aplicação de regras de **compliance, prevenção contra vazamento de informações e controle de conteúdo**, por meio da composição e combinação de diferentes critérios de análise das mensagens.

O sistema permite analisar **qualquer parte do cabeçalho (header) da mensagem**, o conteúdo do corpo da mensagem (body), a mensagem em seu formato original (raw), os arquivos anexados e as URLs presentes no conteúdo da mensagem.

A análise de anexos contempla diversos formatos de arquivos, incluindo **DOC, XLS, PDF, DOCX, XLSX, PPS, PPSX, ODF, ODT, ODS, ODP, PPT, HTML**, entre outros, inclusive quando esses arquivos estiverem armazenados dentro de **arquivos compactados**.

O sistema permite a criação de **dicionários de palavras, termos e padrões**, utilizando expressões regulares que podem ser aplicadas a qualquer campo da mensagem ou ao conteúdo dos arquivos anexados, inclusive arquivos contidos em estruturas compactadas. Também é possível definir a **quantidade mínima de ocorrências** de determinado termo ou padrão para que uma regra seja considerada atendida.
As regras podem ser combinadas por meio de **operações booleanas**, como AND, OR e NOT, permitindo a criação de condições simples ou complexas para determinar quando uma mensagem deverá ser considerada em desacordo com as políticas estabelecidas.

A partir dessas condições, o administrador pode definir **ações específicas para cada conjunto de regras**, permitindo, por exemplo, bloquear, rejeitar, colocar em quarentena, encaminhar para análise ou permitir a entrega da mensagem, conforme as políticas de segurança e compliance estabelecidas pela organização.
O sistema permite ainda a criação de **múltiplas regras de filtragem**, possibilitando combinar uma ou mais condições e associar ações distintas a cada regra, proporcionando maior granularidade no controle e na aplicação das políticas de DLP.

O MailInspector permite criar e utilizar **dicionários de dados e padrões de informações sensíveis**, possibilitando a implementação de políticas alinhadas às principais normas e regulamentações de mercado, como **SOX, GLBA, HIPAA**, entre outras.

O mecanismo de DLP permite realizar consultas e análises abrangentes sobre diferentes elementos da mensagem, desde informações presentes no **cabeçalho do e-mail**, passando pelo conteúdo do corpo da mensagem e pelo conteúdo textual dos arquivos anexados, até mecanismos de **comparação por hash de arquivos** e outras condições que podem ser combinadas na construção das regras.

Dessa forma, o DLP do MailInspector proporciona um mecanismo flexível e granular para **identificação, classificação e aplicação de políticas sobre informações sensíveis**, permitindo à organização controlar o fluxo

de mensagens e reduzir os riscos de **vazamento, exposição ou envio indevido de informações** por meio do correio eletrônico.

O HSC MailInspector já vem com alguns dicionários de palavras consideradas sensíveis pela LGPD, tais como:

- CPF;
- RG;
- CNH;
- CNPJ;
- Placa de Carro padrão Mercosul;
- Número de Passaporte brasileiro;
- E-mails/Lista de e-mails;
- TLP;
- Número de Cartão de crédito e outros dicionários;

Criptografia - Criptografe automaticamente os e-mails sem a necessidade da interação dos usuários, garantindo a Confidencialidade na troca de mensagens. O Administrador pode configurar quais e-mails deverão ser criptografados baseados em regras por: Cabeçalho (se tem algum cabeçalho customizado, ou se em algum cabeçalho está com um valor específico nele, FROM do Envelope, FROM do Header, Return Path, entre diversos outros campos do cabeçalho do e-mail, etc), origem (IP, e-mail ou domínio), destino (IP, e-mail ou domínio), assunto, anexos (Tamanho, nome do anexo, nome parcial do anexo, se o anexo está compactado, se o anexos está compactado com senha, palavras/texto específico contido dentro de anexos, etc), conteúdo (texto no corpo do e-mail, etc), etc.

As mensagens que forem criptografadas serão armazenadas na ferramenta usando o algoritmo de criptografia configurado na quarentena, usando uma chave única e exclusiva por mensagem.

Por padrão os acessos a estas mensagens são efetuados através de uma console Web HTTPS customizável e compatível com qualquer Browser de forma segura e com bloqueio de uso do cache via Cookies. É possível modificar esta configuração, para que seja liberado o uso do Cache (na parte de inserção da senha do leitor do e-mail), dessa forma, caso o leitor do e-mail já tenha se cadastrado e efetuada a leitura do e-mail pelo menos uma vez, não será necessária nova entrada de senha, desde que a senha já esteja registrada no cache da máquina utilizada.

Os métodos de Criptografia de E-mails aceitos utilizados pelo MailInspector são Push e Pull, cabendo ao administrador a seleção do método a ser utilizado.

O módulo de Criptografia é totalmente responsivo, de modo de que o usuário poderá abrir os e-mails criptografados pelo browser do seu celular/tablet e trabalhar com o e-mail criptografado, sem necessidade de configurar tamanho de tela ou outro parâmetro.

Tela responsiva de avido de recebimento de e-mail criptografado

Todas as ações executadas nos e-mails criptografados são registrados em logs, por exemplo: leitura, resposta do e-mail, encaminhamento do e-mail, etc.

É possível efetuar o controle de chaves por e-mail criptografado, isto é, o administrador pode revogar a chave de criptografia individualmente por e-mail criptografado. Dessa forma fica impedido a leitura e operação do e-mail, mesmo que ainda não tenha sido expirado o tempo de "vida útil" do e-mail criptografado.

O módulo de criptografia de e-mails do MailInspector, não utiliza JavaScript para leitura e operação dos e-mails criptografados, dessa forma não fica na dependência da necessidade de instalação de Java na máquina destino e/ou origem do e-mail criptografado.

Quarentena Personalizada - Permite que o administrador possa definir quais tipos de mensagens serão adicionadas a uma quarentena personalizada. O Administrador pode criar filtros através de qualquer parte do e-mail, tais como: Cabeçalho (com inspeção profunda), Origem, Destino, Conteúdo no e-mail, Anexos (Tamanho, nome do anexo, nome parcial do anexo, se o anexo está compactado, se o anexos está compactado com senha, etc), Vírus ou Outras Ameaças, Conteúdo dentro de anexos e etc.

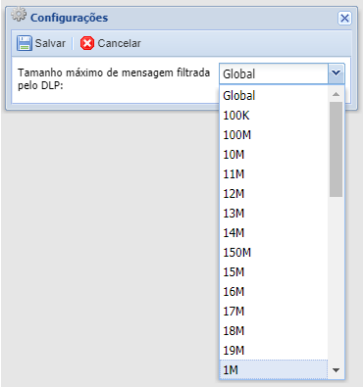
Todas as regras criadas nesta sessão podem ser concatenadas e combinadas com os operadores booleanos tais como: AND, OR, NOT, NEAR, OCCUR, (,), [,], etc.

Desta forma o administrador pode criar uma vasta gama de combinações casando por exemplo: Quando um e-mail vir do remetente X, com destino a um grupo de LDAP Y contendo o grupo de anexos Z!

É possível cruzar informações do módulo de E-mail Compliance para obter um resultado de acordo com a necessidade do administrador, por exemplo: Criptografar um e-mail de acordo com uma regra de DLP. Por exemplo criptografar (ativar o módulo de criptografia) e-mails que contenham números de cartão de crédito no corpo do e-mail (que será detectado pelo módulo DLP).

Definições de Opções - Regras de Compliance

Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição
Adicionar	Cadastra um novo registro de regra de compliance. Quando clicado, abre a caixa de diálogo **Adicionar/Editar Regras de Compliance**.
Editar	Edita as configurações de um registro existente. Quando clicado, abre a caixa de diálogo **Adicionar/Editar Regras de Compliance**.
Remover	Quando clicado, exclui o registro selecionado.
Conectar	Permite combinar duas regras de compliance previamente cadastradas. Quando clicado, abre a caixa de diálogo **Conectar**.
Desconectar	Permite desconectar duas regras previamente conectadas.
Configurações	Indica o tamanho máximo do anexo a ser analisado pela regra de DLP.  Ao selecionar Global (default), indica que não tem limite de tamanho.
Ativar	Ativa a regra selecionada
Desativar	Desativa a regra selecionada

Definições de Opções – Adicionar/Editar Regras de Compliance - Seleção do Controle

Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição
Cabeçalho	Permite verificar qualquer parte do cabeçalho da mensagem.
Corpo	Permite realizar a análise do conteúdo da mensagem.

Conteúdo Original	Permite verifica a mensagem no formato original que foi recebida.
Anexos	Verifica conteúdo dos anexos e nome / extensão. Também permite identificar anexos por Mime-Type e Criptografia. Permite identificar Dicionário de Palavras no conteúdo de anexos como: DOC, XLS, PDF, DOCX, XLSX, PPT, HTML entre outros. Permite identificar Conteúdos nocivos "Executáveis" dentro documentos "DOC, DOCX, XLS, XLSX", entre outros.
URL	Permite verifica URLs incluídas no corpo da mensagem.
Localização	Permite a aplicação de regras baseadas na linguagem da mensagem ou no páis de origem.
Controle de Assinaturas	Possibilita a combinação de regras com ações realizadas em outros filtros da ferramenta.
Avançar	Quando clicado, prossegue para a configuração do tipo de controle selecionado.

Definições de Opções – Adicionar/Editar Regras de Compliance - Cabeçalho

Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição
Define o cabeçalho a ser utilizado	Selecione um cabeçalho para ser pesquisado na mensagem.
Cabeçalho Customizado	Quando definido o cabeçalho a ser utilizado como **CUSTOMIZADO**. Informe o nome do cabeçalho presente na mensagem para combinar com a regra.
Grupos	Quando definido o cabeçalho a ser utilizado como **From**, **To**, **CC** ou **Bcc**. Selecione o grupo de usuários que contém os endereços presentes na mensagem para combinar com a regra.
Dicionário de Palavras	Quando definido o cabeçalho a ser utilizado como diferente de **From**, **To**, **CC** ou **Bcc**. Selecione o dicionário de palavras que contém os termos presentes no cabeçalho da mensagem para combinar com a regra.
Número Mínimo de Ocorrências	Informe o número de ocorrências que devem ser encontradas de grupo de usuários ou dicionário de palavras no cabeçalho da mensagem para combinar com a regra.
Voltar	Quando clicado, retorna a seleção de controle.
Avançar	Quando clicado, prossegue para a configuração das informações e pontuação.

Definições de Opções – Adicionar/Editar Regras de Compliance - Corpo

Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição
Dicionário de Palavras	Selecione o dicionário de palavras que contém os termos presentes no corpo da mensagem para combinar com a regra.
Número Mínimo de Ocorrências	Informe o número de ocorrências que devem ser encontradas no dicionário de palavras para combinar com a regra.

Voltar	Quando clicado, retorna a seleção de controle.
Avançar	Quando clicado, prossegue para a configuração das informações e pontuação.

Definições de Opções – Adicionar/Editar Regras de Compliance - Conteúdo Original

Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição
Dicionário de Palavras	Selecione o dicionário de palavras que contém os termos presentes no corpo da mensagem, em seu formato original, para combinar com a regra.
Número Mínimo de Ocorrências	Informe o número de ocorrências que devem ser encontradas no dicionário de palavras para combinar com a regra.
Voltar	Quando clicado, retorna a seleção de controle.
Avançar	Quando clicado, prossegue para a configuração das informações e pontuação.

Definições de Opções – Adicionar/Editar Regras de Compliance - Anexos

Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição

Tipo de Anexo	Escolha entre:
	• **Grupo de Anexos** - Cria uma regra de controle compliance realizando a busca por um determinado grupo de anexos, buscando por nome, extensão ou expressão regular no nome do arquivo em anexo.
	• **Mime-type** - Cria uma regra de controle compliance realizando a busca por um determinado tipo MIME no arquivo em anexo.
	• **Fingerprint** - Cria uma regra de controle compliance realizando a busca por uma determinada assinatura de fingerprint no arquivo em anexo.
	• **Dicionário de Palavras** - Cria uma regra de controle avançado realizando a busca por um determinado dicionário de palavras, buscando por expressões no conteúdo do arquivo em anexo.
	• **Criptografia** - Permite identificar anexos Criptografados nas mensagens. É utilizado para detectar arquivos **não compactados** que foram inseridas senhas. Os tipos de anexo detectado são:
	  o Heurística: Detecta automaticamente o arquivo com senha, podendo ser qualquer tipo de arquivo com senha, por exemplo PDF com senha, DOC com senha, XLS com senha, etc.
	  o MimeType: Detecta através do tipo de arquivo, via mime type.
	  o Extensão: Detecta especificamente por extensões.

Grupo de Anexos	Selecione o grupo de anexo que contém os nomes, extensões ou expressões regulares presentes no nome do arquivo anexo da mensagem para combinar com a regra.
Mime-Type	Selecione o grupo de Mime-Types que contém os tipos MIME presentes no arquivo anexo da mensagem para combinar com a regra.
Fingerprint	Selecione o grupo de fingerprint que contém a assinatura do arquivo anexo da mensagem para combinar com a regra.

Dicionário de Palavras	Quando definido o tipo de anexo como **Dicionário de Palavras**. Selecione o dicionário de palavras que contém os termos presentes no conteúdo do anexo para combinar com a regra.
Número Mínimo de Ocorrências	Quando definido o tipo de anexo como **Dicionário de Palavras**. Informe o número de ocorrências que devem ser encontradas no dicionário de palavras para combinar com a regra.
Criptografia	Selecione quais são os identificadores desejados: • Heurística; • MimeType; • Extensão;
Voltar	Quando clicado, retorna a seleção de controle.
Avançar	Quando clicado, prossegue para a configuração das informações e pontuação.

Definições de Opções – Adicionar/Editar Regras de Compliance - URL

Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição
Dicionário de Palavras	Selecione o dicionário de palavras que contém os termos das URLs presentes no corpo da mensagem para combinar com a regra.
Número Mínimo de Ocorrências	Informe o número de ocorrências que devem ser encontradas no dicionário de palavras para combinar com a regra.
Voltar	Quando clicado, retorna a seleção de controle.
Avançar	Quando clicado, prossegue para a configuração das informações e pontuação.

Definições de Opções – Adicionar/Editar Controle Avançado - Localização

Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição
Tipo de controle	Selecione por controle de Linguagem ou por País de origem.
Linguagem ou País de Origem	De acordo com a opção anterior, selecione ou a linguagem ou o País para o filtro.
Voltar	Quando clicado, retorna a seleção de controle.
Avançar	Quando clicado, prossegue para a configuração das informações e pontuação.

Definições de Opções – Adicionar/Editar Controle Avançado - Controle de Assinaturas

Indicações de operadores lógicos para trabalho com regras de compliance (DLP, Criptografia e Quarentena Customizada).

Opções	Definição
Regras	Select box que possibilita a combinação de regras com ações realizadas em outros filtros da ferramenta.

Operador Lógico	Escolha entre: • **E** - A pontuação será atribuída as mensagens que combinarem com as duas regras selecionadas. • **OU** - A pontuação será atribuída as mensagens que combinarem com qualquer uma das regras selecionadas.
Voltar	Quando clicado, retorna à seleção de controle.
Avançar	Quando clicado, prossegue para a configuração das informações e pontuação.

Definições de Opções - Adicionar/Editar Regras de Compliance - Informações e Ações

Indicação das ações possíveis para as regras de compliance (DLP, Criptografia e Quarentena Customizada).

Opções	Definição
Nome	Informe um nome descritivo para a regra.
Descrição	Campo livre para comentários.
Tipo	Tipo da Regra que está sendo criada. Pode ser: • DLP; • Criptografia; • Quarentena Customizada;
Ações DLP	Permite selecionar as ações para mensagens que combinarem com os parâmetros definidos na regra. • **Armazenar em Log** - Registra o processamento da mensagem no banco de dados. • **Remover Anexo** - Remove anexo da Mensagem. • **Auditoria** - Armazena a mensagem na quarentena. • **Deletar** - Exclui a mensagem. • **Entregar** - Entrega a mensagem para o destinatário. • **Notificar Destinatário** - Envia um e-mail de notificação ao destinatário da mensagem. • **Notificar Remetente** - Envia um e-mail de notificação ao remetente da mensagem. • **Rejeitar** - Rejeita o recebimento da mensagem. • **Encaminhar para** - Encaminha uma cópia da mensagem para outro destinatário. • **Alterar Assunto** - Adiciona uma TAG no assunto do e-mail para identificação • **Alterar Cabeçalho** - Adiciona um cabeçalho na mensagem para ideintificação
Ações Criptografia	Permite selecionar as ações para mensagens que combinarem com os parâmetros definidos na regra de criptografia. • **Tempo de Expiração** - Define o tempo em que a mensagem ficará disponível para consulta no console de criptografia. • **Permitir Responder** - Permite que o usuário responda o e-mail na console de criptografia

	• **Permitir Encaminhar** - Permite que o usuário encaminhe o e-mail na console de criptografia
Ações Quarentena	Permite selecionar em qual quarentena customizada a regra será armazenada
Voltar	Quando clicado, retorna para a configuração do controle selecionado.
Avançar	Quando clicado, prossegue para a conferência dos itens configuradas na regra.

Definições de Opções - Adicionar/Editar Regras de Compliance - Conclusão do Processo

Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição
Voltar	Quando clicado, retorna para a configuração das informações e pontuação.
Salvar	Quando clicado, grava as configurações realizadas.

Definições de Opções - Conectar

Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição
Salvar	Quando clicado, grava as configurações realizadas.
Cancelar	Quando clicado, cancela a ação.
Regra	Escolha entre: • **Casar** - A pontuação será atribuída as mensagens que combinarem com a regra selecionada. • **Não Casar** - A pontuação será atribuída as mensagens que não combinarem com a regra selecionada.
Operação Lógica	Escolha entre: • **E** - A pontuação será atribuída as mensagens que combinarem com as duas regras selecionadas. • **OU** - A pontuação será atribuída as mensagens que combinarem com qualquer uma das regras selecionadas.
Regra	Escolha entre: • **Casar** - A pontuação será atribuída as mensagens que combinarem com a regra selecionada. • **Não Casar** - A pontuação será atribuída as mensagens que não combinarem com a regra selecionada.
Ações DLP	Permite selecionar as ações para mensagens que combinarem com os parâmetros definidos na regra. • **Armazenar em Log** - Registra o processamento da mensagem no banco de dados. • **Remover Anexo** - Remove anexo da Mensagem. • **Auditoria** - Armazena a mensagem na quarentena. • **Deletar** - Exclui a mensagem.

	• **Entregar** - Entrega a mensagem para o destinatário. • **Notificar Destinatário** - Envia um e-mail de notificação ao destinatário da mensagem. • **Notificar Remetente** - Envia um e-mail de notificação ao remetente da mensagem. • **Rejeitar** - Rejeita o recebimento da mensagem. • **Encaminhar para** - Encaminha uma cópia da mensagem para outro destinatário. • **Alterar Assunto** - Adiciona uma TAG no assunto do e-mail para identificação • **Alterar Cabeçalho** - Adiciona um cabeçalho na mensagem para ideintificação
Ações Criptografia	Permite selecionar as ações para mensagens que combinarem com os parâmetros definidos na regra. • **Tempo de Expiração** - Define o tempo em que a mensagem ficará disponível para consulta na console de criptografia. • **Permitir Responder** - Permite que o usuário responda o e-mail na console de criptografia • **Permitir Encaminhar** - Permite que o usuário encaminhe o e-mail na console de criptografia
Ações Quarentena	Permite selecionar em qual quarentena customizada a regra será armazenada

Definições de Opções

Indica as colunas apresentadas nas regras, apresentando o que cada uma delsa representa.

Opções	Definição
Regra	Número da regra
Nome	Indica o nome da regra
Controle	Apresenta a regra em si, ou a concatenação entre múltiplas regras (dependendo do que foi feito com a regra)
Ação	Ação executada quando a regra é ativada
Ordem	Muda a sequência de execução. Quanto mais acima maior a prioridade. O MailInspector executa como se fosse fireall, ou seja, ao casar uma regra, as outras automaticamente serão ignoradas
Ativo	Indica se a regra está ativa ou desativada ☑ Indica que a regra está ativa ☐ Indica que a regra está inativa

M-SOAR / Deep Integration

M-SOAR ou Modified Security Orchestration, Automation and Response é um conjunto de tecnologias que coleta dados e traz alertas de segurança de e-mail para o MailInspector, com isso, é possível gerenciar ameaças e vulnerabilidades, automatizando processos operacionais de segurança, tais como:

- Remoção de Anexos nos e-mails já entregues;
- Remoção de links em e-mails já entregues ao servidor de e-mail;
- Mover o e-mail entregue para a lixeira eletrônica;
- Bloqueio de conteúdo de mensagem entregue;
- Apagar na caixa de correio eletrônico uma ou mais mensagens já entregadas;

Esses serviços são somente disponibilizados caso você utilize serviço da Microsoft Office 365, G-Suite e Zimbra.

É possível automatizar o processo ações a serem tomadas para e-mails considerados campanhas e/ou ameaças que foram entregues, incluindo processo para aprovação prévia de ações a serem executadas.

Office 365

Para acessar o módulo M-SOAR referente ao Office 365, vá em:

Configurações **/ M-SOAR**

Visão geral de M-SOAR para Office 365

Com o módulo M-SOAR integrado a Microsoft Office 365, é possível ao administrador:

- Remoção de Anexos nos e-mails já entregues;
- Remoção de links em e-mails já entregues ao servidor de e-mail;
- Mover o e-mail entregue para a lixeira eletrônica;
- Bloqueio de conteúdo de mensagem entregue;
- Apagar na caixa de correio eletrônico uma ou mais mensagens já entregues;

Definições de Opções

Estas informações descrevem as opções disponíveis na adição/edição/remoção de domínios a serem gerenciados com M-SOAR.

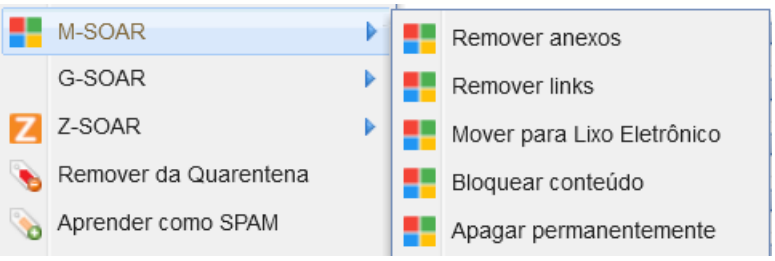
Opções	Definição
Adicionar	Cadastra um novo registro de regra de M-SOAR. Quando clicado, abre a caixa de diálogo **Adicionar Domínio.**

Editar	Edita as configurações de um registro existente. Quando clicado, abre a caixa de diálogo **Adicionar Domínio.**
Remover	Remove uma regra M-SOAR anteriormente adicionada.
Ativar	Ativa uma regra M-SOAR já criada, caso a mesma esteja desativada.
Desativar	Desativa a regra ativa de M-SOAR selecionada.

Definições de Opções – Adicionar Domínio

Estas informações descrevem as opções que serão disponibilizadas ao operador/administrador da solução, quando o e-mail for do domínio selecionado.

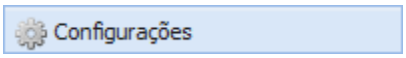
Opções	Definição
Domínio	Selecione o domínio ao qual o módulo M-SOAR estará atuando.
Autenticar conta Microsoft Office 365	Autentica a conta na Microsoft, ao qual o administrador poderá verificar a chave de autenticação utilizada para sincronização do serviço M-SOAR junto ao Office 365.
Ações – Remover Anexos	Modificar Assunto • **Não:** Não modifica o assunto do e-mail com indicação de anexo removido; • **Sim:** Modifica o asssunto do e-mail indicando ao usuário que o anexo foi removido **[Anexos removidos]**;
Ações – Remover Links	Modificar Assunto • **Não:** Não modifica o assunto no e-mail com indicação de link removido; • **Sim:** Modifica o assunto do e-mail indicando ao usuário que o link contido no e-mail foi removido **[Links removidos]**; Modificar tag do link • **Não:** Não modifica o link no corpo e-mail com indicação de link removido, somente remove o link em si, sem indicação alguma; • **Sim:** Modifica o link, trocando-o por uma indicação de que o mesmo foi removido **[Link removido]**;
Ações – Mover para Lixo Eletônico	Modificar Assunto • **Não:** Não modifica o assunto no e-mail com indicação de que o e-mail foi enviado ao lixo eletrônico; • **Sim:** Modifica o assunto do e-mail indicando ao usuário que o e-mail foi enviado ao lixo eletrônico **[Mensagem removida]**;
Ações – Bloquear Conteúdo da Mensagem	Modificar Assunto • **Não:** Não modifica o assunto no e-mail com indicação de que o e-mail possui conteúdo bloqueado; • **Sim:** Modifica o assunto do e-mail indicando ao usuário que o e-mail possui conteúdo bloqueado **[Mensagem bloqueada]**; Conteúdo Permite ao administrador incluir um texto específico no lugar do conteúdo do e-mail.
Ações – Apagar Mensagem	Apaga o e-mail, removendo-o completamente da caixa postal do usuário.
Ativo	Indica se a regra M-SOAR está ativa ou inativa.



Tela indicativa das ações presentes no M-SOAR integrado ao Office 365

G-Suite

Para acessar o módulo M-SOAR referente ao G-Suite, vá em:

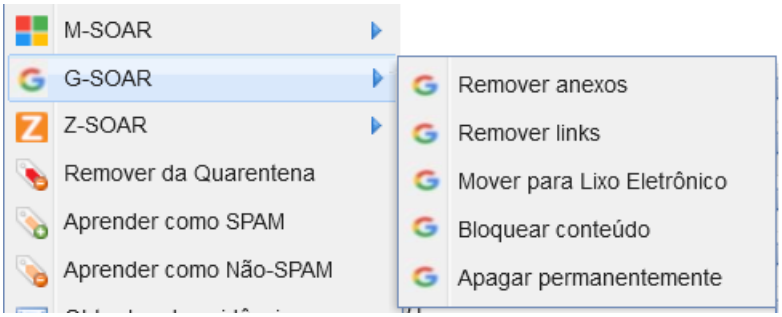


/ G-SOAR

Visão geral de M-SOAR para G-Suite

Com o módulo M-SOAR integrado ao G-Suite, é possível ao administrador:

- Remoção de Anexos nos e-mails já entregues;
- Remoção de links em e-mails já entregues ao servidor de e-mail;
- Mover o e-mail entregue para a lixeira eletrônica;
- Bloqueio de conteúdo de mensagem entregue;
- Apagar na caixa de correio eletrônico uma ou mais mensagens já entregues;



Tela indicativa das ações presentes no M-SOAR integrado ao G-Suite

Definições de Opções

Estas informações descrevem as opções disponíveis na adição/edição/remoção de domínios a serem gerenciados com M-SOAR.

Opções	Definição
Adicionar	Cadastra um novo registro de regra de M-SOAR. Quando clicado, abre a caixa de diálogo **Adicionar Domínio.**

Editar	Edita as configurações de um registro existente. Quando clicado, abre a caixa de diálogo **Adicionar Domínio.**
Remover	Remove uma regra M-SOAR anteriormente adicionada.
Ativar	Ativa uma regra M-SOAR já criada, caso a mesma esteja desativada.
Desativar	Desativa a regra ativa de M-SOAR selecionada.

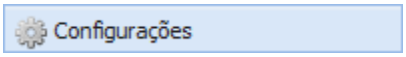
Definições de Opções – Adicionar Domínio

Estas informações descrevem as opções que serão disponibilizadas ao operador/administrador da solução, quando o e-mail for do domínio selecionado.

Opções	Definição
Domínio	Selecione o domínio ao qual o módulo M-SOAR estará atuando.
Autenticar conta Microsoft Office 365	Autentica a conta na Microsoft, ao qual o administrador poderá verificar a chave de autenticação utilizada para sincronização do serviço M-SOAR junto ao Office 365.
Ações – Remover Anexos	Modificar Assunto • **Não:** Não modifica o assunto do e-mail com indicação de anexo removido; • **Sim:** Modifica o asssunto do e-mail indicando ao usuário que o anexo foi removido **[Anexos removidos]**;
Ações – Remover Links	Modificar Assunto • **Não:** Não modifica o assunto no e-mail com indicação de link removido; • **Sim:** Modifica o assunto do e-mail indicando ao usuário que o link contido no e-mail foi removido **[Links removidos]**; Modificar tag do link • **Não:** Não modifica o link no corpo e-mail com indicação de link removido, somente remove o link em si, sem indicação alguma; • **Sim:** Modifica o link, trocando-o por uma indicação de que o mesmo foi removido **[Link removido]**;
Ações – Mover para Lixo Eletônico	Modificar Assunto • **Não:** Não modifica o assunto no e-mail com indicação de que o e-mail foi enviado ao lixo eletrônico; • **Sim:** Modifica o assunto do e-mail indicando ao usuário que o e-mail foi enviado ao lixo eletrônico **[Mensagem removida]**;
Ações – Bloquear Conteúdo da Mensagem	Modificar Assunto • **Não:** Não modifica o assunto no e-mail com indicação de que o e-mail possui conteúdo bloqueado; • **Sim:** Modifica o assunto do e-mail indicando ao usuário que o e-mail possui conteúdo bloqueado **[Mensagem bloqueada]**; Conteúdo Permite ao administrador incluir um texto específico no lugar do conteúdo do e-mail.
Ações – Apagar Mensagem	Apaga o e-mail, removendo-o completamente da caixa postal do usuário.
Ativo	Indica se a regra M-SOAR está ativa ou inativa.

Zimbra

Para acessar o módulo M-SOAR referente ao Zimbra, vá em:

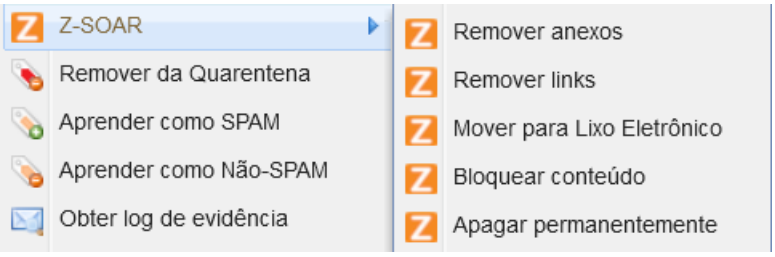


/ Z-SOAR

Visão geral de M-SOAR para Zimbra

Com o módulo M-SOAR integrado ao Zimbra, é possível ao administrador:

- Remoção de Anexos nos e-mails já entregues;
- Remoção de links em e-mails já entregues ao servidor de e-mail;
- Mover o e-mail entregue para a lixeira eletrônica;
- Bloqueio de conteúdo de mensagem entregue;
- Apagar na caixa de correio eletrônico uma ou mais mensagens já entregues;



Tela indicativa das ações presentes no M-SOAR integrado ao Zimbra

Definições de Opções

Estas informações descrevem as opções disponíveis na adição/edição/remoção de domínios a serem gerenciados com M-SOAR.

Opções	Definição
Adicionar	Cadastra um novo registro de regra de M-SOAR. Quando clicado, abre a caixa de diálogo **Adicionar Domínio.**
Editar	Edita as configurações de um registro existente. Quando clicado, abre a caixa de diálogo **Adicionar Domínio.**
Remover	Remove uma regra M-SOAR anteriormente adicionada.
Ativar	Ativa uma regra M-SOAR já criada, caso a mesma esteja desativada.
Desativar	Desativa a regra ativa de M-SOAR selecionada.

Definições de Opções – Adicionar Domínio

Estas informações descrevem as opções que serão disponibilizadas ao operador/administrador da solução, quando o e-mail for do domínio selecionado.

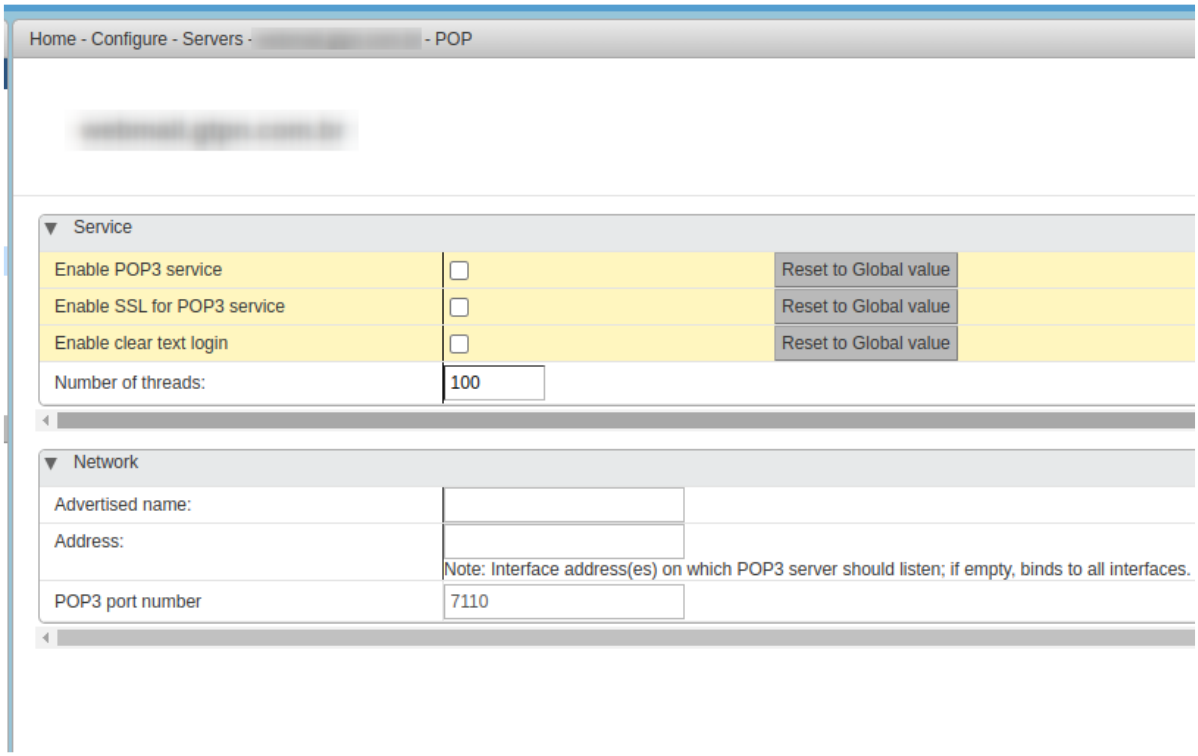
Opções	Definição

Domínio	Selecione o domínio ao qual o módulo M-SOAR estará atuando.
Autenticar conta Microsoft Office 365	Autentica a conta na Microsoft, ao qual o administrador poderá verificar a chave de autenticação utilizada para sincronização do serviço M-SOAR junto ao Office 365.
Ações – Remover Anexos	Modificar Assunto • **Não:** Não modifica o assunto do e-mail com indicação de anexo removido; • **Sim:** Modifica o asssunto do e-mail indicando ao usuário que o anexo foi removido **[Anexos removidos]**;
Ações – Remover Links	Modificar Assunto • **Não:** Não modifica o assunto no e-mail com indicação de link removido; • **Sim:** Modifica o assunto do e-mail indicando ao usuário que o link contido no e-mail foi removido **[Links removidos]**; Modificar tag do link • **Não:** Não modifica o link no corpo e-mail com indicação de link removido, somente remove o link em si, sem indicação alguma; • **Sim:** Modifica o link, trocando-o por uma indicação de que o mesmo foi removido **[Link removido]**;
Ações – Mover para Lixo Eletônico	Modificar Assunto • **Não:** Não modifica o assunto no e-mail com indicação de que o e-mail foi enviado ao lixo eletrônico; • **Sim:** Modifica o assunto do e-mail indicando ao usuário que o e-mail foi enviado ao lixo eletrônico **[Mensagem removida]**;
Ações – Bloquear Conteúdo da Mensagem	Modificar Assunto • **Não:** Não modifica o assunto no e-mail com indicação de que o e-mail possui conteúdo bloqueado; • **Sim:** Modifica o assunto do e-mail indicando ao usuário que o e-mail possui conteúdo bloqueado **[Mensagem bloqueada]**; Conteúdo Permite ao administrador incluir um texto específico no lugar do conteúdo do e-mail.
Ações – Apagar Mensagem	Apaga o e-mail, removendo-o completamente da caixa postal do usuário.
Ativo	Indica se a regra M-SOAR está ativa ou inativa.

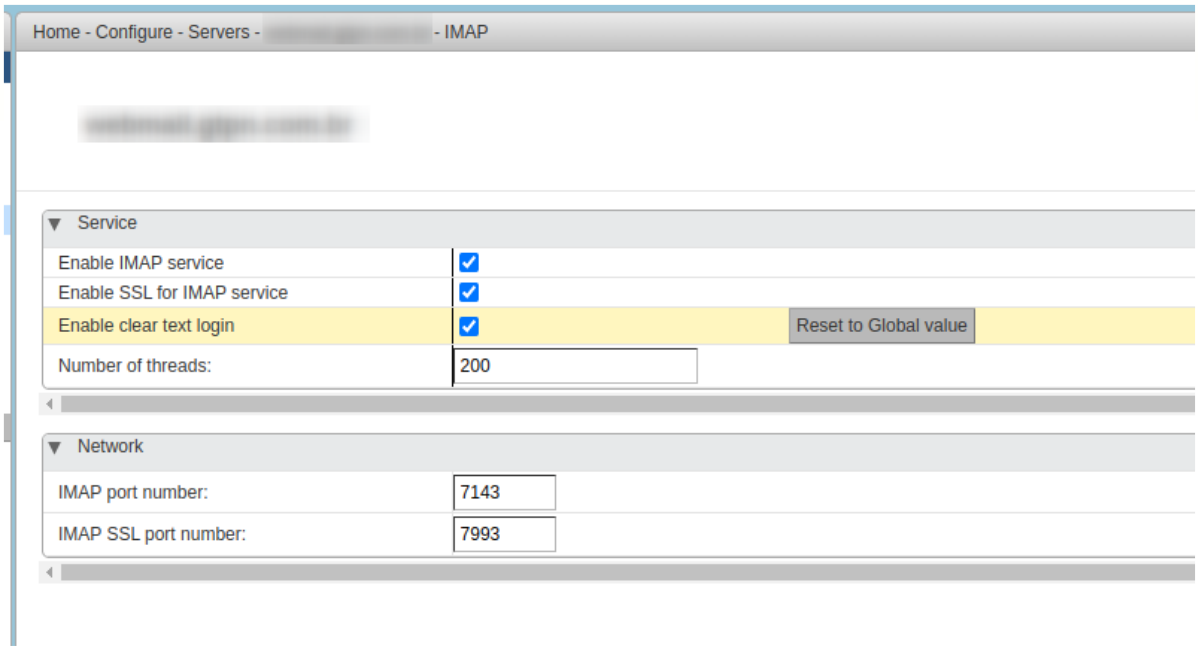
HSC Extended Mailbox Integration

Integração POP e IMAP para Gerenciamento de Quarentenas

Este módulo tem como objetivo facilitar o acesso dos usuários aos e-mails em quarentena criando uma experiência completa e simplificada facilitando o seu uso através de ferramentas de cliente de e-mail. Os protocolos utilizados para comunicação podem ser POP3 (com ou sem SSL/TLS) e IMAP (com ou sem SSL/TLS), com suporte completo para ambos.



Configuração POP



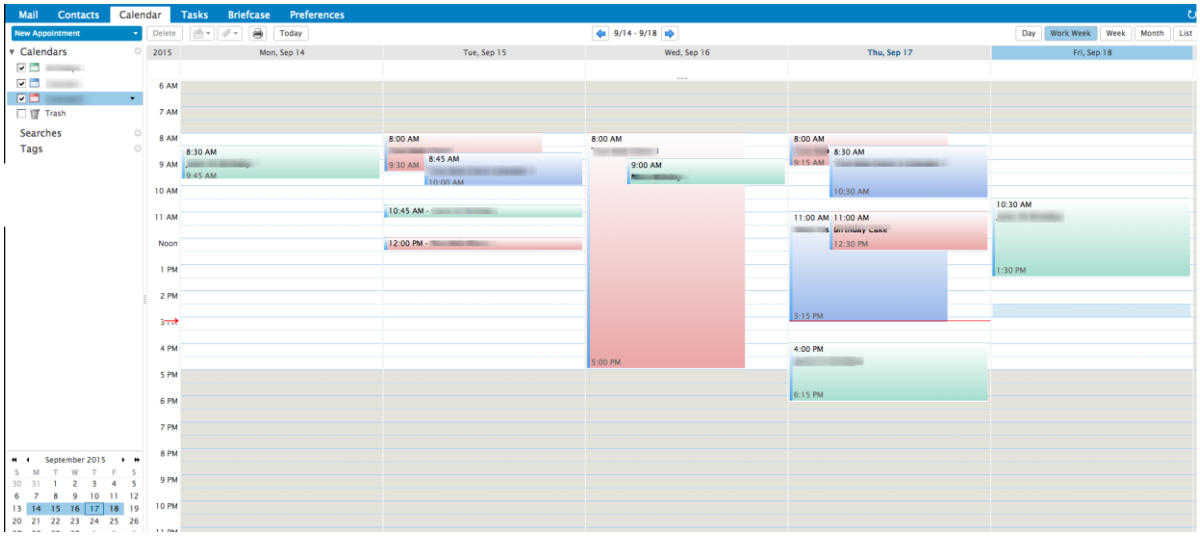
Configuração IMAP

Sincronização Bidirecional de Agendas

A plataforma oferece recursos de sincronização de contatos e calendários de forma bidirecional, permitindo seu gerenciamento completo:

- Adicionar;
- Editar;
- Excluir;

Através de padrões como CalDAV, CardDAV, WebDAV, entre outros. Este tipo de funcionalidade possibilita unificar os recursos em um só lugar, simplificando a gestão e manutenção, e facilitando os processos de auditorias.

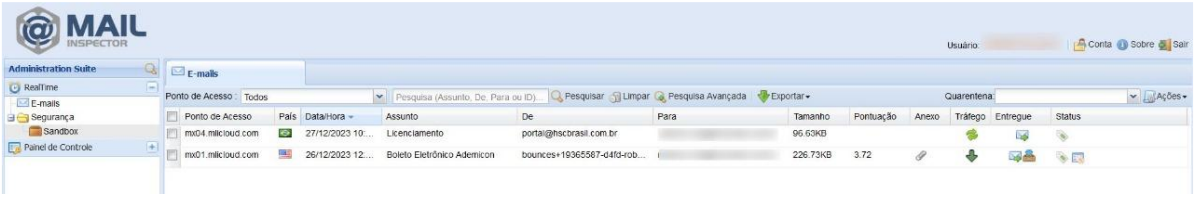


Configuração CalDav

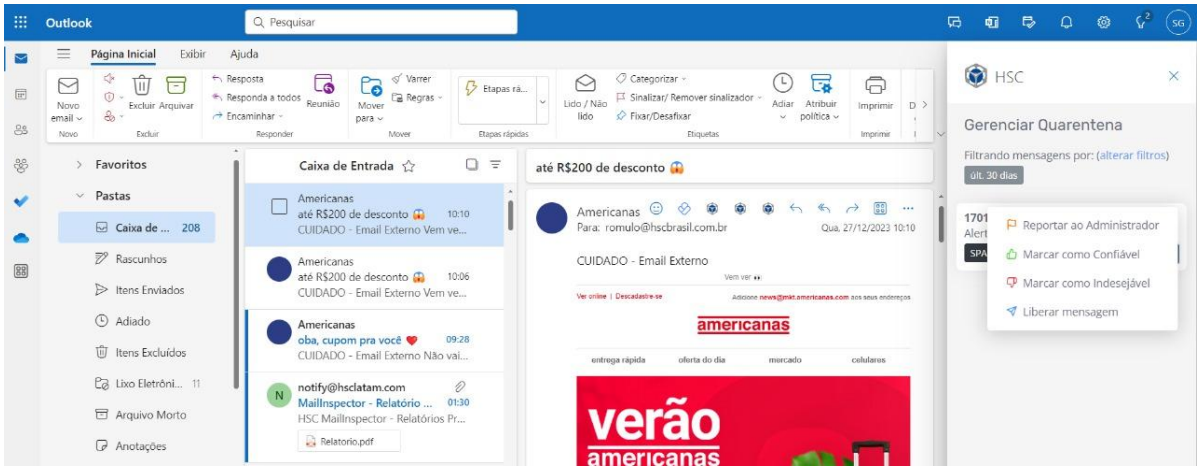
Continuidade de Acesso

Além disso, a solução garante disponibilidade contínua do serviço de e-mail reduzindo o risco de inatividade e perda de produtividade. Permite que os usuários enviem e recebam e-mails em caso de interrupção, sem a necessidade de qualquer ação adicional deles ou da equipe de TI.

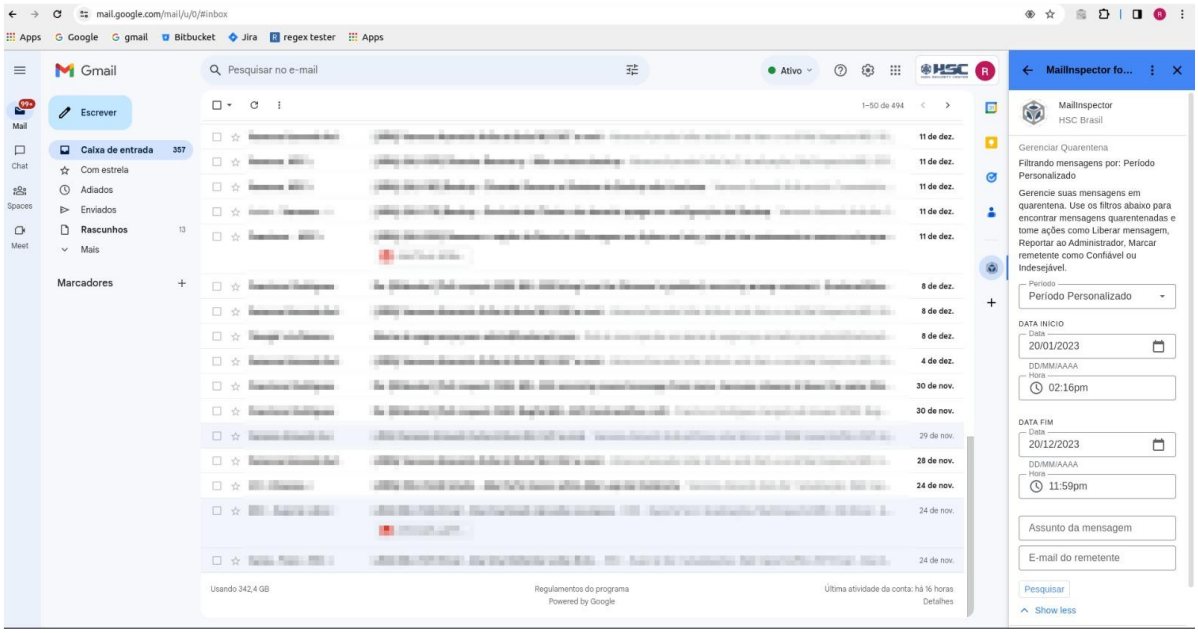
O módulo HSC Extended Mailbox Integration não requer manutenção e fornece uma espécie de seguro sempre ativo para manter suas comunicações importantes fluindo.



Continuidade de Acesso - Quarentena do Usuário



Continuidade de Acesso - Quarentena do Usuário - Microsoft 365 – Ações sobre os e-mails quarentenados

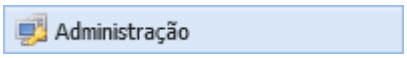


Continuidade de Acesso - Quarentena do Usuário - Gmail

Menu - Administração

Ponto de Acesso

Use esta página para exibir, adicionar, editar ou excluir os pontos de filtragem do HSC MailInspector.



/ Administração / Ponto de Acesso

Visão geral do ponto de acesso

Ponto de acesso é a designação dada a todos os servidores que possuem o HSC MailInspector instalado. Cada ponto de filtragem tem configurações e características próprias, podem ser máquinas virtuais, físicas ou clusters com diferentes recursos. A console permite gerenciar múltiplos ponto de acesso e clusters de forma centralizada. Os pontos de acesso podem ser criados e administrado conforme a necessidade do administrador, podendo gerenciar Sub-organizações "Filiais" a partir de um ponto de acesso virtual, desta forma pode-se repassar a administração deste ponto de acesso para outros administradores específicos.

Junto ao sistema de configuração do ponto de acesso, podemos configurar o sistema de depuração de problemas. Com o SYSLOG, onde o administrador poderá selecionar o envio do SYSLOG do ponto de acesso ou de um Cluster e o nível de depuração, tais como:

- Emergency;
- Alert;
- Critical;
- Error;
- Warning;
- Notice;
- Informational;
- Debug;

No syslog do MailInspector, é possível verificar logs que indicam o processo das etapas efetuadas na mensagem, tais como:

- Comandos do antispam (varredura e ação/pontuação);
- Comandos de sistema;
- Debug;
- Antivírus (varredura e detecção do Antivírus HSC SmartDefender antivírus, Antivírus ESET, AntiPhishing);
- Erros;
- Status: Início da conexão, origem, destino, IP de origem e dados de DNS, Resultado do SPF, Resultado DKIM, Resultado DMARC, País de Origem do IP, from, to, assunto, tamanho da mensagem;
- Muitas outras informações relevantes na varredura do e-mail;

Definições de Opções - Ponto de Acesso

Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição

Adicionar	Cadastra um novo ponto de acesso. Quando clicado, abre a caixa de diálogo **Adicionar/Editar Ponto de Acesso**.
Editar	Edita as configurações de um registro existente. Quando clicado, abre a caixa de diálogo **Adicionar/Editar Ponto de Acesso**.
Remover	Quando clicado, exclui o registro selecionado.
Coleta de Dados	Configura a coleta dos registros das mensagens filtradas e dos arquivos das mensagens armazenados na quarentena. Quando clicado, abre a caixa de diálogo **Coleta de Dados**.
Syslog	Permite enviar logs para um servidor Externo de Logs via protocolo "SYSLOG" para sistemas de análise e relatórios externos. Ex: Sistemas SIEM Pode ser selecionado o nível de log que será enviado e o período de envio destes logs.

Coleta de dados é o termo utilizado para o processo que centraliza os registros das mensagens filtradas no banco de dados da interface de administração e os arquivos das mensagens armazenados na quarentena.

No caso do Syslog, também são enviados os dados de auditoria do sistema, no formato:

Jun 7 10:51:53 mli-admin httpd: MailInspector-Audit:: User: admin , IP_Address: 192.168.4.25 , **Action: Efetuou login no sistema.**

Jun 7 10:57:00 mli-admin httpd: MailInspector-Audit:: User: admin , IP_Address: 192.168.4.25 , **Action: Aplicou novas configurações no ponto de acesso ID 3 dos módulos ['AntiSPAM/Filtro de Conteúdo/Controle de Ameaças', Block List/Allow List Personalizadas', 'Controle de Conexão', 'Data Loss Prevention'].**

Jun 7 10:57:00 mli-admin httpd: MailInspector-Audit:: User: admin , IP_Address: 192.168.4.25 , **Action: Aplicou novas configurações no ponto de acesso ID 3 dos módulos ['AntiSPAM/Filtro de Conteúdo/Controle de Ameaças', Block List/Allow List Personalizadas', 'Controle de Conexão', 'Data Loss Prevention'].**

Definições de Opções - Adicionar/Editar Ponto de Acesso

Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição
Salvar	Quando clicado, grava as configurações realizadas.
Cancelar	Quando clicado, cancela a ação.
Nome do Servidor	Informe um nome exclusivo para este servidor. Pode-se utilizar o padrão de nome de máquina da empresa, criar um nome padrão com o local, unidade ou cidade onde o equipamento será instalado. Ex.: mx01.empresa.com.br.
E-mail do Administrador	Informe um endereço de e-mail ou lista de distribuição dos responsáveis pela administração do servidor.

Endereço IP	Informe o endereço IP do servidor no formato IPv4.
Habilitar Consultas SNMPv2/SNMPv3	Escolha entre: • **Sim** - Indica que a consulta SNMP está ativa, permitindo que sistemas de monitoramento, com suporte a SNMP v2 ou v3, realizem o monitoramento do sistema operacional e da aplicação. • **Não** - Indica que a consulta SNMP está desativada.
Comunidade SNMP	Personalize o nome da community de consulta SNMP.
Ativar Coleta de Dados	Escolha entre: • **Sim** - Indica que a coleta de dados será executada no ponto de acesso. • **Não** - Indica que a coleta de dados não será executada no ponto de acesso.
Comentário	Campo livre para comentários.
O Servidor está Ativo	Escolha entre: • **Sim** - Indica que o servidor está ativo, pode ser configurado e utilizado. • **Não** - Indica que o servidor está inativo. Não é possível realizar nenhum tipo de configuração ou consulta.

Definições de Opções - Syslog

Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição
Salvar	Quando clicado, grava as configurações realizadas.
Cancelar	Quando clicado, cancela a ação.
Nome do Servidor	Informe Nome ou IP do Servidor de Destino
Nível do LOG	Marque quais níveis de Logs serão enviados: • Emergency; • Alert; • Critical; • Error; • Warning; • Notice; • Informational; • Debug;
Período de Armazenamento	Informe o úmero de dias que serão armazenados os logs. Os arquivos de logs que ultrapassarem o período indicado, automaticamente serão removidos. A quantidade de registro de logs é ilimitada, bastando a ter capacidade de armazenamento alocada conforme a necessidade do administrador.
Período de Envio	Informe o intervalo (hora) que pode ser enviado os logs ao servidor externo de log.
Tipo	• FTP: Envio pelo protocolo FTP • SFTP: Envio usando o protocolo SFTP

	• Autenticar: Utiliza sistema autenticado de usuário e senha para o protocolo selecionado anteriormente. • Anônimo: Não utiliza sistema de autenticação para uso com o protocolo selecionado anteriormente.
Host	IP / Nome do host para qual será enviado os logs. O campo após o host é a porta utilizada para o protocolo de envio dos logs.
Username	Nome do usuário que está apto a autenticar no protocolo anteriormente selecionado.
Senha	Senha para uso do envio dos logs.

Os dados apresentados nos logs são (com variações de acordo com o nível de log selecionado):

- Endereço de IP de Origem;
- Endereço de IP de Destino;
- Endereço de IP do ponto de filtragem utilizado;
- Qual ponto de filtragem utilizado;
- E-mail de Origem;
- E-mail de Destino;
- Assunto do e-mail;
- Composição da pontuação;
- Pontuação final atribuída ao e-mail;
- Status;
- Tamanho do e-mail;
- Pontuação sobre a reputação da Origem, por IP, Domínio, País, linguagem utilizada, códigos UTF-8 e UTF-16;
- Se o e-mail possui anexo ou não;
- Nome e tipo do anexo;
- Data e hora de entrada do e-mail;
- Data e hora da saída do e-mail no MailInspector;
- Resultados de análise de DKIM;
- Resultados de análise de SPF;
- Resultados de análise de DMARC;
- Resultado de controle de fluxo;
- Informações e análise sobre CDR's;
- Análise de ameaças e ações tomadas;
- Reputação da Origem;
- Políticas Aplicadas no e-mail;
- Regras ativadas sobre o e-mail;
- Regras customizadas aplicadas no e-mail;
- Comandos executados sobre o e-mail;
- Resultado de análise sobre imagens (inclusive sobre imagens pornográficas);
- Tempo de escaneamento para cada módulo do MailInspector;
- Pontuação do e-mail em relação a Mail Marketing;
- Pontuação do e-mail em relação a Redes Sociais;
- Pontuação do e-mail em relação a Conteúdo Adulto;
- Alertas (warnings), erros e outros alertas;
- Entre outros dados...

Os dados enviados por Syslog segue o padrão abaixo:
Jul 12 04:05:59 mli01 mta/smtpd[11351]: info: connect from localhost. localdomain [127.0.0.1]
DATA/HORA SERVIDOR PROCESSO NÍVEL_SYSLOG MENSAGEM

O campo Mensagem informa o que está sendo processado e possui diversos detalhes sobre o processamento de cada mensagem. O HSC MailInspector possui interface Web Gráfica de Análise de Logs de E-mails de forma muito mais simplificada e de fácil administração.
Exemplo de Alguns dados enviados por Syslog:
ID da mensagem
Data e Hora, Time zone
Informativo de inicialização/parada/reinício de cada serviço
Registro de fila de e-mail
Detalhes de envio e recebimento completo: Início da conexão, origem, destino, IP de origem e dados de DNS, Resultado do SPF, Resultado DKIM, Resultado DMARC, País de Origem do IP, from, to, tamanho da mensagem, etc.
Etapa que está analisando o e-mail: Antivírus HSC SmartDefender antivírus, Antivírus ESET, AntiSpam, AntiPhishing, SmartDefender, Criptografia, DLP, Controle de Fluxo, etc.
Detalhes do Escaneamento: Informações sobre Vírus, Informações sobre classificação de SPAM "Pontuação e Regra Ativadas", Pontuação dos sistemas de: "E-mail Marketing, Redes Sociais e Conteúdo Adulto", Regra que casou, status final do escaneamento, tempo de escaneamento, status final do sistema de quarentena com detalhes sobre qual quarentena foi arquivada, etc.
Log dos comandos executados na interface CLI.
Erros e Warning dos serviços.
E muito mais ...

Em relação aos logs, o MailInspector trabalha de forma ativa com o envio de logs (via FTP, SFTP, SCP) ou de forma passiva, com compartilhamento dos logs através de acesso remoto (disponibilização de acesso aos logs por SCP, sendo o usuário e senha o mesmo do utilizado pelo sistema de SSH), dessa forma cobrindo todas as necessidades do administrador.

É possível compartilhar os LOGs através de uma cópia remota usando o protocolo SFTP/SCP com as mesmas credenciais utilizadas para o acesso via SSH, sendo assim, é possível que o administrador copie os LOGs para um servidor externo e/ou a partir de um servidor Externo.

/var/log/messages - Contém dados referentes a Informações, Falhas, Debug e Avisos dos seguintes componentes: Sistema Operacional, Hardware, Processos, etc

/var/log/secure - Contém dados referentes a Informações, Falhas, Debug e Avisos dos seguintes componentes: Segurança e Autenticação

/var/log/maillog - Contém dados referentes a Informações, Falhas, Debug e Avisos dos seguintes componentes: E-mails

Aqui todos dados referentes aos Registro de entrada e saída de e-mails estão contidos neste arquivo.

O LOG é completo e detalhado, mantendo informações completas de todo tráfego de entrada e saída dos e-mails.

OBS: Este LOG serve para possível integração com sistemas Externos de SIEM, lembramos que todos os dados de LOGs e informações também são registrados na Base de Dados relacional onde se pode usar a interface web para as mais variadas formas de consultas, sendo este LOG uma forma adicional de registro.

Exemplo de Alguns itens contidos neste arquivo:

ID da mensagem
Data e Hora, Time zone
Informativo de inicialização/parada/reinicio de cada serviço
Registro de fila de e-mail
Detalhes de envio e recebimento completo: Inicio da conexão, origem, destino, IP de origem e dados de DNS, Resultado do SPF, Resultado DKIM, Resultado DMARC, País de Origem do IP, from, to, tamanho da mensagem, etc.
Etapa que está analisando o e-mail: Antivírus HSC SmartDefender antivírus, Antivírus ESET, AntiSpam, AntiPhishing, SmartDefender, Criptografia, DLP, Controle de Fluxo, etc.
Detalhes do Escaneamento: Informações sobre Vírus, Informações sobre classificação de SPAM "Pontuação e Regra Ativadas", Pontuação dos sistemas de: "E-mail Marketing, Redes Sociais e Conteúdo Adulto", Regra que casou, status final do escaneamento, tempo de escaneamento, status final do sistema de quarentena com detalhes sobre qual quarentena foi arquivada, etc.
Log dos comandos executados na interface CLI.
Erros e Warning dos serviços
E muito mais ...

Definições de Opções - Coleta de Dados

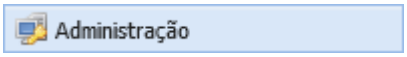
Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição
Salvar	Quando clicado, grava as configurações realizadas.
Cancelar	Quando clicado, cancela a ação.
Ativar Coleta	Escolha entre: • **Sim** - Indica que a coleta está ativa. Os registros das mensagens filtradas e os arquivos das mensagens armazenados na quarentena serão coletados dos pontos de acesso ativos, e os mesmos serão inseridos no ponto de acesso "Histórico". • **Não** - Indica que a coleta está desativada.
Tempo de Armazenamento de Quarentena no Histórico	Informe o tempo, em dias, que os registros das mensagens filtradas permanecerão armazenados no banco de dados do ponto de acesso "Histórico".
Tempo de Armazenamento dos Logs no Histórico	Informe o tempo, em dias, que os arquivos das mensagens da quarentena permanecerão armazenados no ponto de acesso "Histórico".
Horário de Execução da Coleta	Selecione o horário em que o processo de coleta será executado.
Ativar Envio de Notificação	Escolha entre:

	• **Sim** - Indica que o envio de notificação da coleta está ativo. Este recurso envia uma mensagem com o resumo do processamento da coleta para o endereço de e-mail informado. • **Não** - Indica que o envio de notificação da coleta está desativado.
Endereço de E-mail	Informe um endereço de e-mail ou lista de distribuição que receberá uma mensagem com o estado da coleta.
Selecione os tipos de e-mail que não serão coletados para a quarentena	Permite definir tipos de os arquivos das mensagens da quarentena que não serão coletados. • **Provável SPAM** - Mensagens processadas que foram classificadas como proveniente de provável fonte de SPAM ou ameaças. • **SPAM** - Mensagens processadas que foram classificadas como proveniente de fonte confirmada de SPAM ou ameaças. • **Conteúdo Bloqueado** - Mensagens processadas quer foram classificadas como contendo arquivos anexos com o mime-types ou extensões proibidas. • **Outros Bloqueios** - Mensagens processadas quer foram classificadas em qualquer outro tipo de bloqueio. • **Tamanho Excedido** - Mensagens processadas quer foram classificadas como tendo o tamanho maior que o permitido. • **Block List** - Mensagens que foram processadas e estavam cadastradas na block list. • **Vírus e Outras Ameaças** - Mensagens processadas que foram classificadas como contendo vírus ou que tenham fontes para vírus ou outras ameaças.

Configurações de Rede

Permite configurar as interfaces de redes do Pontos de Filtragem.



/ Administração / Configurações de Rede

Visão geral de Configurações de Rede

Permite ao administrador configurar os detalhes das interfaces de rede dos Pontos de Filtragem não importando se são Appliances Físicos ou Appliances Virtuais.

Definições da Aba Rede

Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição
Nome do Host	Hostname deste servidor
Domínio	Domínio do servidor.
Interfaces	Selecione uma das interfaces que serão configuradas
Criar Alias	Permite criar alias de IP "Virtual IP" para interface. Este alias pode ser utilizado para definir novas rotas de entrada ou saída de e-mails. Ex: Forçar que um determinado domínio saia por um determinado endereço IP. Com a criação de alias de IP, o MailInspector fornece a opção de segmentar o fluxo de e-mail por diferentes IP's virtuais e domínios (combinando com a configuração de Configurações > Controle de Conexão > Configurações do MTA > Rotas). Como exemplo, podemos citar o uso para e-mails de saída para casos de mailmarketing, dessa forma, se o IP de saída utilizado na campanha de marketing cair em blacklist (RBL), não ocorrerá problema do IP de saída de e-mails cair na mesma blacklist (RBL), pois são IP's distintos.
Habilitar interface de rede	Esta interface estará habilitada sim ou não.
Endereço IPV4	Endereço IPV4 deste servidor. Permite adicionar alias de IP a fim de configurar múltiplos endereços IPs
Máscara de Rede	Máscara de rede IPV4 deste servidor
Habilitar IPV6	Permite habilitar o Suporte a IPV6 no MailInspector, permitindo que o MailInspector receba e processe na sua totalidade as conexões via protocolo IPV6
Endereço IPV6	Endereço IPV6 deste servidor
Gateway Endereço IPV4	Endereço do Default Gateway IPV4 deste servidor
Gateway Endereço IPV6	Endereço do Default Gateway IPV6 deste servidor

Habilitar Horário	**Automático:** Habilita as configurações via Servidor NTP (IPv4 ou FQDN), com uso de TimeZone **Manual:** Habilita a entrada de horário manual, no formato HH:MM:SS
NTP SERVER Endereço IPV4 ou FQDN	Informe o endereço do NTP server para sincronismo de Data e Hora.
Fuso Horário	Informe o fuso horário.
Horário	Inserção de horário manual.

Definições da Aba Rotas

Aqui é possível adicionar rotas estáticas para redes IPV4

Opções	Definição
Destino IPV4:	Informe a rede ou host de destino para esta rota
Máscara de Rede:	Informe a máscara de rede para esta rota.
Gateway	Informe o Gateway para esta rota
Botão Adicionar	Adiciona a rota

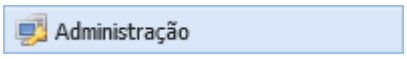
Definições do DNS

Aqui é possível configurar a resolução de nomes DNS

Opções	Definição
Servidor Primário	Informe qual é o servidor primário de consultas DNS
Servidor Secundário	Informe qual é o servidor secundário de consultas DNS. "Opcional"
Servidor Terciário	Informe qual é o servidor terciário de consultas DNS. "Opcional"
Mapeamento de Hostnames	Permite definir entradas manuais estáticas "Arquivo hosts”. Formato de inserção Ex: Formato: [IP] [HOSTNAME]

Usuários do Sistema

Use esta página para exibir, adicionar, editar ou excluir usuários da interface administrativa do HSC MailInspector.



/ Administração / Usuários do Sistema

Visão geral dos usuários do sistema

Usuário do sistema é qualquer indivíduo que utiliza os recursos da interface de administração do HSC MailInspector.

As ações do usuário são limitadas através de um perfil de acesso, que lhe é atribuído no momento do seu cadastro. Os usuários importados através de conectores externos serão automaticamente cadastrados como perfil Usuário (a não ser que seja efetuado o filtro e selecionado a função dele), e poderá acessar a console de administração conforme a definição do perfil de acesso.

O sistema pode ser configurado para limitar o número de tentativas de autenticação a fim de bloquear tentativas de coleta de senhas.

É possível efetuar cadastro de múltiplos administradores, cada um com um perfil customizado, para que cada administrador do sistema acesse somente a parte referente a sua área, dessa forma pode-se criar administradores setorizados, por exemplo: administradores para administração geral da solução, outro administrador somente com permissão de leitura (para auditar as políticas customizadas no sistema), outro administrador somente com acesso as configurações de compliance, etc.

No MailInspector é possível atrelar múltiplos e-mails e/ou domínios/subdomínios a um único usuário do sistema (este usuário pode ser de qualquer perfil, desde simples usuário até administrador), dessa forma permitindo que o mesmo faça manutenção/controle a múltiplos domínios e/ou múltiplos e-mails.

O MailInspector também permite que o mesmo administrador efetue múltiplos logins simultâneos, mas sempre registrando a origem da conexão, bem como todas as ações tomadas pela pessoa que entrou no sistema, independente do perfil utilizado.

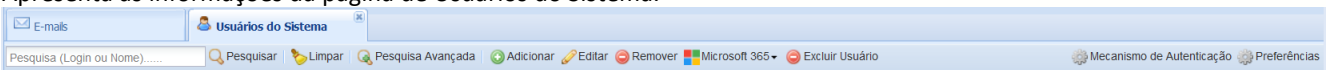
Por padrão os perfis pré-configurados no MailInspector são:

Perfis Disponíveis

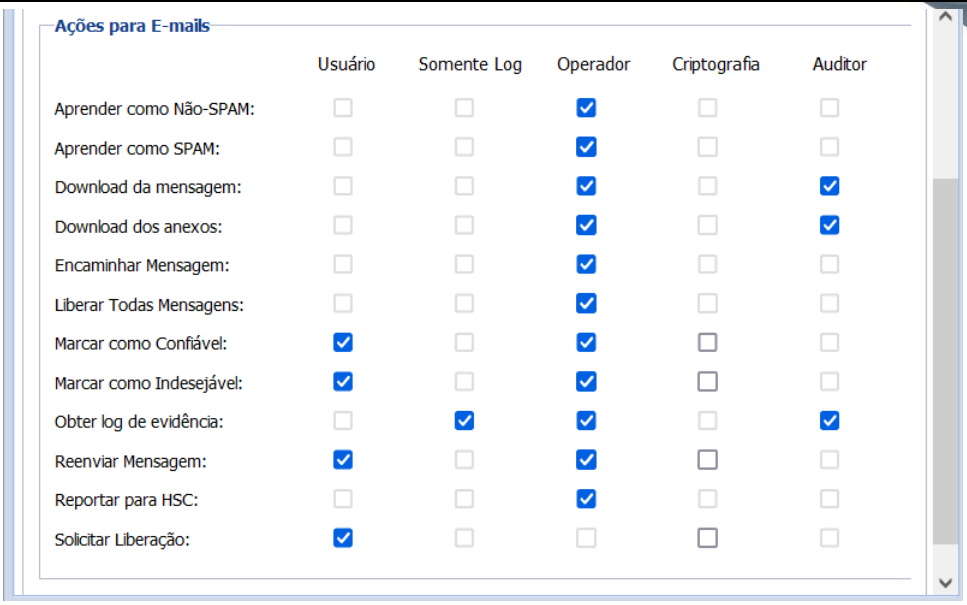
- Administrador;
- Administrador Customizado;
- Usuário;
- Auditor;
- Operador;
- Somente Log;
- Criptografia;
- API;

Definições de Opções - Usuários do Sistema

Apresenta as informações da página de Usuários do Sistema.



Opções	Definição
Pesquisar	Quando clicado, aplica o filtro informado na caixa de pesquisa rápida a listagem de usuários.
Limpar	Quando clicado, remove os filtros informados da caixa de pesquisa rápida e recarrega toda a listagem de usuários.
Adicionar	Cadastra um novo usuário que utilizará a interface de administração. Quando clicado, abre a caixa de diálogo **Adicionar/Editar Usuário do Sistema**.
Editar	Edita as configurações de um registro existente. Quando clicado, abre a caixa de diálogo **Adicionar/Editar Usuário do Sistema**.
Remover	Quando clicado, exclui o registro selecionado.
Mecanismo de Autenticação	Configura o mecanismo de autenticação dos usuários do sistema. Quando clicado, abre a caixa de diálogo **Mecanismo de Autenticação**.
Pesquisa Avançada	Filtra por diversos itens um determinado usuário ou conjunto de usuários
Microsoft 365	• **Bloqueio de Usuário:** Bloqueia o usuário no Office 365, utilizando o conector via API.
Excluir Usuário	Permite criar um filtro no conector Externo (LDAP/Zimbra/AD) para que o usuário não seja mais importado, dessa forma, ao sincronizar o conector externo, o usuário não será mais "puxado" para o MailInspector.
Preferências	



Permite customizar a solução para apresentação e uso de configuração no módulo RealTime > E-mails

Administradores

Período de busca por e-mail: Configuração exclusiva a administradores da solução, ao qual poderão efetuar buscas rápidas em um período customizado, em vez de usar o padrão de 24 horas.

Usuários

Período de busca por e-mails: Configuração exclusiva a usuários da solução, ao qual poderão efetuar buscas rápidas em um período customizado, em vez de usar o padrão de 24 horas.

Mensagem Entregue: Permite configurar a apresentação de acordo com o status de entrega:

- **Todos:** Apresenta todos os e-mails sem filtro ativo;
- **Somente Sim:** Apresenta somente os e-mails entregues;
- **Somente Não:** Apresenta somente os e-mails que foram barrados;

Ações para E-mails: Limita as ações possíveis aos usuários, podendo ser:

- **Aprender como Não-SPAM:** Ensina o MailInspector (local) como sendo este e-mail não SPAM;
- **Aprender com SPAM:** Ensina o MailInspector (local) como sendo este e-mail SPAM;
- **Download da Mensagem:** Permite o download da mensagem toda;
- **Download dos anexos:** Permite que seja baixado os anexos contidos no e-mail;
- **Encaminhar Mensagem:** Encaminha o e-mail a um terceiro, sem que o remetente, nem o destinatário sejam alertados;
- **Liberar Todas Mensagens:** Libera todas as mensagens apresentadas na tela;
- **Marcar como Confiável:** Marca o remetente do e-mail como confiável (whitelist);
- **Marcar como Indesejável:** Marca o remetente como indesejável (block list);
- **Obter log de evidência:** Apresenta todos os logs de filtragem da mensagem, desde a entrada até a saída/quarentena;

	• **Reenviar a mensagem:** Libera a mensagem da quarentena e prossegue com a entrega, ignorando qualquer filtragem que a tenha bloqueado; • **Remover da Quarentena:** Exclui a mensagem (não é apagado os logs, somente a mensagem); • **Reportar para HSC:** Envia a mensagem para HSC como amostra, ao qual será analisado primeiramente pelo sistema de Machine Learning e posteriormente por especialistas para averiguação confirmatória; • **Solicitar liberação:** Solicita ao administrador da solução a liberação da mensagem;

Definições de Opções – Colunas Indicatórias

Indica as informações que compõem cada uma das colunas.

Opções	Definição
Login	Login do usuário
Nome	Nome do usuário
Perfil	Qual perfil está atrelado ao usuário, podendo ser: • Administrador; • Administrador Customizado; • Usuário; • Auditor; • Operador; • Somente Log; • Criptografia; • API;
Tipo	Como foi inserido no MailInspector: Importado através de conector externo; Inserido manualmente no MailInspector (Usuário local);
Status	Bloqueado Ativo

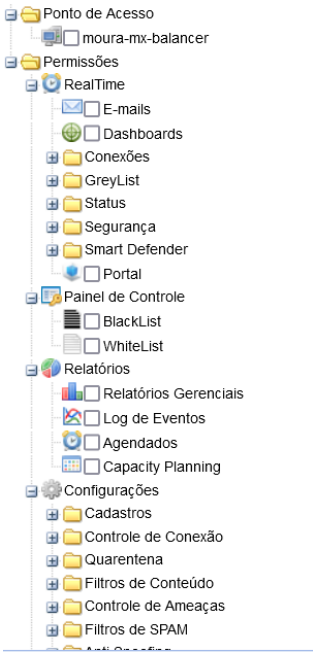
Definições de Opções – Adicionar / Editar Usuários do Sistema

Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição
Salvar	Quando clicado, grava as configurações realizadas.
Cancelar	Quando clicado, cancela a ação.
Login	Informe um nome de login exclusivo para este usuário.
Nome	Informe um nome de exibição para este usuário.
Perfil	Defina o perfil com as permissões de acesso deste usuário.

	• **Administrador** - Permite executar qualquer ação nos domínios ou endereços de e-mail atribuídos, podendo ser configurado para visualizar o conteúdo das mensagens, exclusão de mensagens, liberar e-mails de quarentena, chegando até a excluir e-mails armazenados, ou ainda efetuar configurações customizadas na solução, tais como alterar a pontuação de e-mails, atribuir exceções em análises de e-mail, redefinir senhas de usuários, excluir usuários, etc.
	• **Administrador Customizado** - Permite definir a permissão que um administrador terá na ferramenta, podendo configurar quais menus ou Áreas da ferramenta ele terá permissão de acesso e quais domínios e/ou grupos de usuários, ou e-mails e/ou Ponto de Acesso ele poderá gerenciar. Este tipo de usuário permite segregar a administração por Sub-organizações e/ou Matriz/Filial de sua empresa.
	Alguns exemplos de criação de Perfil para Administrador Customizado:
	  ○ Perfil para para tratamento de Filas de e-mail;
	  ○ Perfil para tratamento de Bounces de e-mail;
	  ○ Perfil para tratamento de malwares;
	  ○ Perfil para customização de regras de compliance;
	  ○ Perfil para backup e restore;
	  ○ Perfil para configuração e criação de regras contra fraudes de e-mail;
	• **Usuário** - Permite executar ações restritas nos domínios ou endereços de e-mail atribuídos tais como: liberar e-mails bloqueados por SPAM, visualizar seus próprios e-mails quarentenados, solicitar uma liberação pelo administrador, notificar ao administrador e gerenciar a sua block list e allow list.
	• **Auditor** - Permite visualizar as mensagens e o seu conteúdo nos domínios ou endereços de e-mail atribuídos, visualizar e imprimir relatórios, e visualizar o log de eventos.
	• **Operador** - Permite executar ações restritas nos domínios, grupos de usuários ou endereços de e-mail atribuídos, podendo ser configurado para visualizar o conteúdo das mensagens, bem como os registros do MTA, tais como retorno de bounce, negação de e-mails por excesso de tamanho, negação de e-mails por DNS reverso inexistente, block list e allow list, etc.
	• **Somente Log** - Permite visualizar as mensagens e os registros do MTA (retorno de bounce, negação de e-mails por excesso de tamanho, negação de e-mails por DNS reverso inexistente, etc.) nos domínios ou endereços de e-mail atribuídos.
	• **Criptografia** - Este usuário pode ser criado manualmente ou através da interface de acesso a área de acesso aos e-mails criptografados. Estes serão os usuários externos que poderão acessar a console a fim de ler os e-mails que foram enviados para ele e foram criptografados.
	• **API** - Permite criar um usuário para fazer consultas de integração com outros sistemas via API REST (Representational State Transfer API), também podendo usar o método GET e POST.
	
	O administrador customizado também pode ser selecionado para uso com quarentenas específicas, por exemplo liberar o acesso a quarentena de vírus.

Permissão de Acesso	Essa permissão somente é visível ao selecionar o Perfil Administrador Customizado.

	Permite selecionar que telas do sistema estará disponível para visualização do usuário. Para definir a permissão basta selecionar e marcar no Checkbox quais telas estarão disponíveis. Para usuários do tipo API as permissões podem ser: Pesquisa de Quarentena, Listar Políticas de SPAM, Criar/Editar/Remover/Pesquisar Usuários Finais. Disponível apenas para usuários do sistema com o perfil de Administrador Customizado. 
Senha	Informe uma senha para autenticação local deste usuário.
Repetir senha	Informe a senha novamente para confirmação.
Notificação de Quarentena	Escolha entre: • **Sim** - Habilita o envio da notificação do resumo das mensagens retidas na quarentena. As pastas de quarentena que serão apresentadas têm que ser selecionadas pelo administrador no módulo Notificação de Quarentena. • **Não** - Desabilita o envio da notificação do resumo da quarentena. Disponível apenas para usuários do sistema com o perfil de usuário.
Permitir notificação vazia	Escolha entre: • **Sim** – Permite envio de notificação de quarentena vazia ao usuário (mesmo queando ele não tenha nenhum e-mail quarentenado). • **Não** – Desativa o envio de notificação de quarentena, quando o usuário não possui e-mails na quarentena.

Sensibilidade do AntiSpam	Define qual a sensibilidade do sistema de antispam está configurada para o usuário. Por padrão a sensibilidade vem como Normal. Os níveis de sensibilidades disponíveis são: **Normal:** Age de acordo com a configuração efetuada na solução; **Permissivo:** Partindo da configuração aplicada na solução como base, é reduzida a sensibilidade da solução quanto a definição de pontuação de SPAM, deixando mais flexível quanto a entrada de e-mails; **Restritivo:** Partindo da configuração aplicada na solução como base, é aumentada a sensibilidade da solução quanto a definição de pontuação de SPAM, deixando mais restritiva quanto a entrada de e-mails;
Métodos	Se for um usuário com perfil API, é possível selecionar os métodos do API: • Gerenciar Quarentenas; • Gerenciar Usuários; • Políticas de SPAM; Disponível apenas para usuários do sistema com o perfil de API.
Idioma	Seleciona a linguagem utilizada na interface para o usuário. Quando alterada afeta a interface, o disgest e demais componentes de interação com o usuário. Linguagens disponíveis: • Português Brasil; • Inglês; • Espanhol; • Espanhol do Paraguai; • Finlandês (Suomi);
Grupos de Usuários	Se estiver marcado com o perfil de administrador customizado, é possível indicar quais grupos de usuários o administrador customizado poderá acessar.
Filtros de Quarentena	Se estiver marcado com o perfil de administrador customizado, é possível indicar quais quarentenas ele terá acesso.
Ações para E-mail	Se for definido como Administrador Customizado e o mesmo for liberado o acesso a RealTime > E-mails, é possível limitar as ações do que este administrador pode fazer sobre os e-mails.

Segundo fator de autenticação	Escolha entre:
	• **Nenhum** – Indica que o usuário não habilitou o uso do segundo fator de autenticação.
	• **OTP Authenticator** – Ativado o segundo fator de autenticação utilizando quaisquer um dos sistemas de autenticação abaixo indicado:
	  ○ Google Authenticator;
	  ○ Microsoft Authenticator;
	  ○ Entre outros sistemas de autenticação de duplo fator.
	• **API MFA Externa** - Ativa Segundo Fator de Autenticação com API extena de soluções de terceiros.
	• **Somente Autenticação Simples** – Uso sem o segundo fator de autenticação, ou seja, é simples autenticação de senha única.

Permitir visualização do conteúdo de e-mail	Escolha entre: • **Sim** - Habilita a visualização do conteúdo das mensagens. • **Não** - Desabilita a visualização do conteúdo das mensagens. Disponível apenas para usuários do sistema com o perfil de administrador ou operador.
Somente Leitura	Escolha entre: • **Sim** - Habilita ambiente em somente leitura (visualização das configurações estabelecidas), não permitindo alteração nas configurações • **Não** - Permite alterações nas configurações do MailInspector Disponível apenas para usuários do sistema com o perfil de administrador, administrador customizado ou operador.
Bloqueado	Quando marcado torna o usuário bloqueado para uso do sistema.
Permitir aplicar configurações	Habilita o botão de Aplicar Configurações ao perfil.
E-mails/Domínios	Informe os endereços de e-mail, alias, grupos ou domínios associados a conta do usuário. Os e-mails informados podem ser alias ou mascaramento de e-mails, grupos, e-mails reais ou até mesmo lista de distribuição. A administração de domínios está disponível apenas para usuários do sistema com o perfil de administrador, auditor ou operador.
IP's/Rede com permissão de acesso	Indica qual o IP/Rede que o usuário em questão deve estar para poder acessar a ferramenta. Caso este campo esteja em branco, o MailInspector irá assumir que este usuário pode acessar o MailInspector de qualquer ip/rede.

Definições de Opções - Mecanismo de Autenticação

Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição
Salvar	Quando clicado, grava as configurações realizadas.
Cancelar	Quando clicado, cancela a ação.
Forçar uso de Autenticação de dois fatores	Ativa ou desativa GLOBALMENTE o uso de autenticação de dois fatores. Escolha entre: • **Sim** - Habilita o uso de autenticação de dois fatores. • **Não** - Não habilita o uso de sistema de dois fatores.
Ativar sincronismo automático de usuários com servidores LDAP	Quando selecionado a opção de **Autenticação LDAP**, permite sincronizar os usuários de bases LDAP com a base de usuários do sistema.

Intervalo de Sincronismo	Indica qual o intervalo de sincronismo, podendo ser em: • 1 hora; • 9 horas; • 17 horas; • 2 horas; • 10 horas; • 18 horas; • 3 horas; • 11 horas; • 19 horas; • 4 horas; • 12 horas; • 20 horas; • 5 horas; • 13 horas; • 21 horas; • 6 horas; • 14 horas; • 22 horas; • 7 horas; • 15 horas; • 23 horas; • 8 horas; • 16 horas; • 24 horas;
Número Máximo de Tentativas de Login	Limita o número máximo de tentativas de autenticação com falhas.
Autenticação Local	Permite a criação e autenticação local de contas de usuário do sistema.
Autenticação LDAP	Permite a integração da autenticação dos usuários da interface administrativa com uma base de diretório Microsoft Active Directory ou base de diretórios LDAP.

Definições de Opções - Definição das Pesquisas

Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição
Login	Login do usuário
Nome	Nome do usuário
Perfil	Escolha entre: • **Administrador** • **Usuário** • **Auditor** • **Operador** • **Somente Log** • **Criptografia** • **Customizado**
Tipo	Usuário Local ou LDAP
Notificação de Quarentena	Se está habilitado ou não o recebimento
Bloqueado	Usuários bloqueados
Alias	Pesquisa por alias
E-mail/Domínio	Pesquisar por domínio ou e-mail

Política de senhas

No MailInspector é possível criar políticas de senhas, as quais são diferentes das senhas utilizadas pelos usuários da rede (senhas do domínio).

Para esse procedimento, é necessário ativar o procedimento.

Definições de Opções - Definição de Política de Senhas

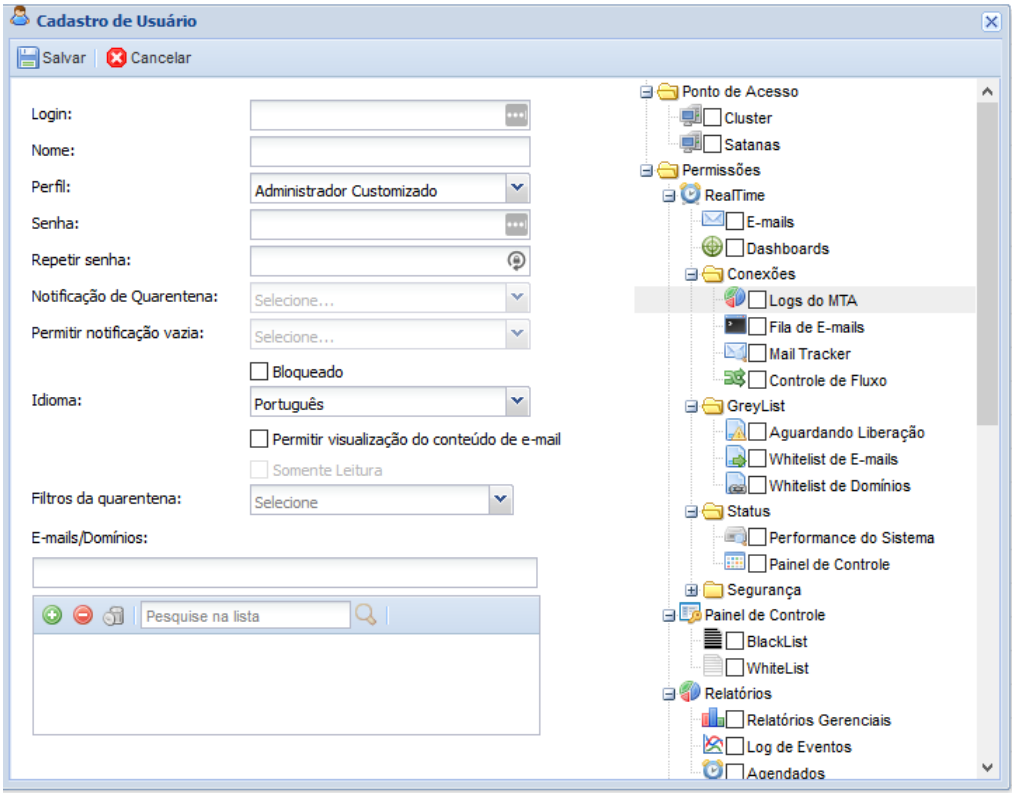
Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição
Habilitar Política de Senhas	**Sim:** Política de senha está ativada e vigente. Esta política se sobrepõe à política de Single Sign-On. **Não:** Política de senha está inativa, dessa forma, caso tenha um conector externo configurado com autenticação por Sigle Sign-On, a senha do seu domínio estará vigente, deixando este módulo (politica de senha) inativa.
Número mínimo de caracteres	Indica o número mínimo de caracteres para a composição da senha.
Número máximo de caracteres	Indica o número máximo de caracteres para a composição da senha.
Obrigatoriedade de letra maiúscula	**Sim:** Obrigatoriedade de existir pelo menos uma letra maiúscula na composição da senha. **Não:** Não é necessário ter uma letra maiúscula na composição da senha.
Obrigatoriedade de número	**Sim:** Deve possuir um ou mais algarismo numérico na composição da senha. **Não:** Não é necessário possuir um ou mais algarismo numérico na composição da senha.
Obrigatoriedade de caracter especial na senha (símbolo)	**Sim:** Deve possuir um ou mais caracter especial na composição da senha. **Não:** Não é necessário possuir um ou mais caracter especial na composição da senha. São considerados símbolos/caracteres especiais os seguintes caracteres: **! @ # $ % & * ( ) _ + - = [ ] { } ? < >**
Tempo de validade	Indicar quantos dias o prazo máximo de validade da senha (contados a partir da criação da mesma para o usuário). **Obs:** 0 (zero) dias indica que a senha nunca irá expirar

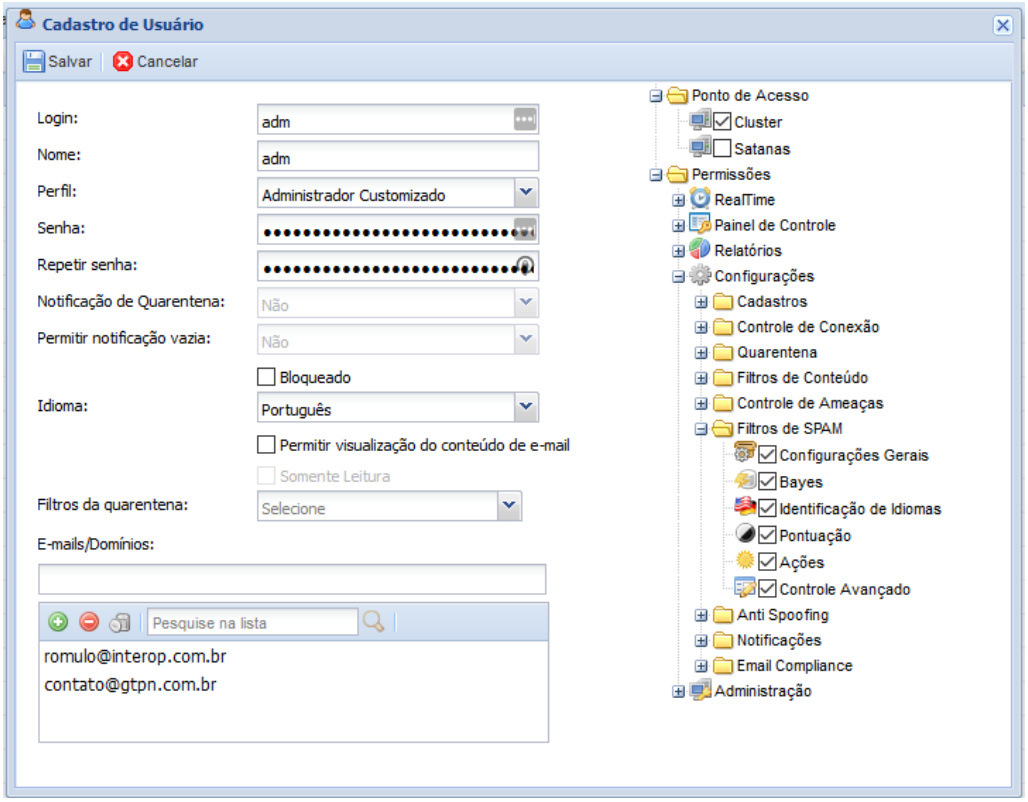
Administrador Customizado

No MailInspector é possível criar usuário administrador customizado, para que o mesmo possa acessar áreas/menus específicos, de acordo com a necessidade da empresa.

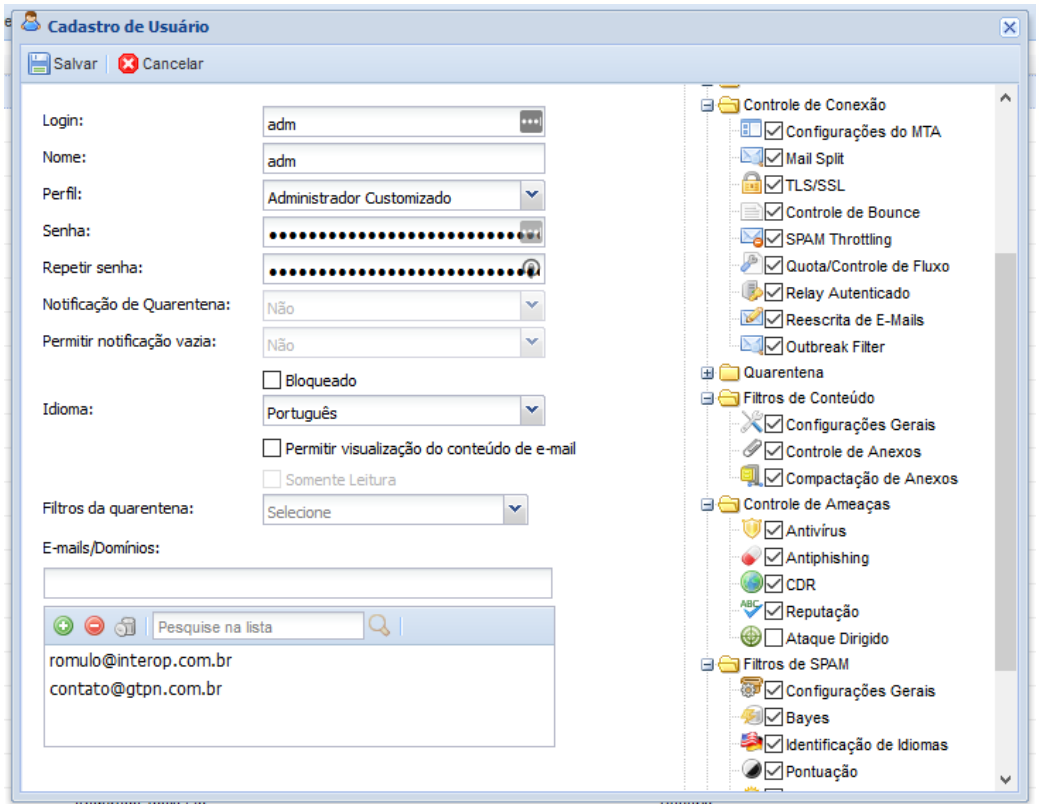
Basta o administrador selecionar quais menus ele quer permitir que o administrador customizado acesse, dessa forma é possível criar QUALQUER perfil desejado, limitando o acesso a módulos ou níveis de permissionamento.



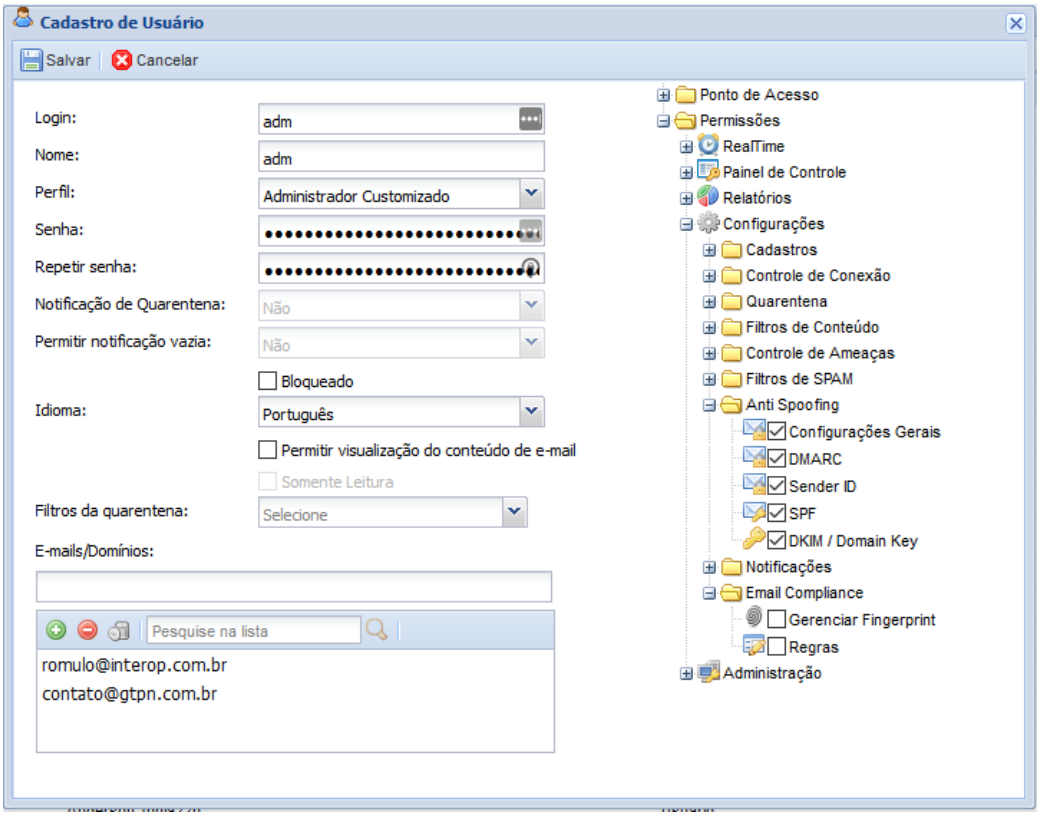
Tela de configuração do administrador customizado



Tela de configuração do administrador customizado



Tela de configuração do administrador customizado



Tela de configuração do administrador customizado

Permissões dos Perfis de Usuários do Sistema

O MailInspector utiliza gerenciamento de perfis de acesso tanto por RBAC (Controle Baseado em Função), quanto por ABAC (Controle baseado em Atributo). Por RBAC, o MailInspector possui perfis já pré-configurados, como:

- Usuário;
- Auditor;
- Operador;
- Somente Log;
- API;
- Criptografia;
- Entre outros perfis pré-configurados;

Os perfis são baseados em funcionalidades:

- Acessos;
- Visualização de Logs;
- Visualização de status;
- Emissão de relatórios;
- Entre outras funcionalidades específicas;

Quanto a compatibilidade com ABAC, o MailInspector possui capacidade de personalização do perfil (Administrador Customizado), por atributo, acesso a telas, permissões de gravação/leitura, entre outros atributos, tais como acesso a dados específicos (por exemplo: administrador customizado que somente terá acesso a determinados e-mails ou e-mails atribuídos a um domínio/tenet), acesso a determinada parte do sistema, ações específicas, tais como liberação de e-mail em quarentena, exclusão de determinado e-mail da quarentena, integração com o módulo SOAR no G-Suite ou Office365 ou Zimbra, etc.

Perfil Usuário

Perfil de usuário padrão do sistema.

- RealTime
  - E-mails
    - Visualizar mensagens dos seus endereços de e-mail
    - Visualizar conteúdo dos seus endereços de e-mail
    - Liberar Mensagem retidas na quarentena dos seus endereços de e-mail
    - Marcar Domínios como Confiáveis dos seus endereços de e-mail
    - Marcar Endereços como Confiáveis dos seus endereços de e-mail
    - Marcar Domínios como Indesejáveis dos seus endereços de e-mail
    - Marcar Endereços como Indesejáveis dos seus endereços de e-mail
    - Solicitar Liberação
- Painel de Controle
  - Block List
    - Visualizar a lista de block list
    - Adicionar, editar e remover seus registros da block list
  - Allow List

        - Visualizar a lista de allow list
        - Adicionar, editar e remover seus registros da allow list

Perfil Auditor

Perfil utilizado exclusivamente para emissão de relatórios e verificação de quem fez o quê e quando.

- RealTime
    - E-mails
        - Obter Log de Evidência do E-mail (Log de filtragem da mensagem)
- Relatórios
    - Relatórios Gerenciais
        - Visualizar relatórios dos domínios ou endereços de e-mail atrelados ao auditor
    - Log de Eventos
        - Visualizar logs de eventos associado ao domínio ou endereços de e-mail atrelado ao auditor

Perfil Operador

Perfil destinado a revisão e aprovação de emails retidos na quarentena.

- RealTime
    - E-mails
        - Visualizar mensagens dos domínios ou endereços de e-mail atribuídos ao operador
        - Visualizar conteúdo dos domínios ou endereços de e-mail atribuídos ao operador
        - Liberar Mensagem dos domínios ou endereços de e-mail atribuídos ao operador
        - Marcar Domínios como Confiáveis dos domínios ou endereços de e-mail atribuídos ao operador
        - Marcar Endereços como Confiáveis dos domínios ou endereços de e-mail atribuídos ao operador
        - Marcar Domínios como Indesejáveis dos domínios ou endereços de e-mail atribuídos ao operador
        - Marcar Endereços como Indesejáveis dos domínios ou endereços de e-mail atribuídos ao operador
        - Encaminhar Mensagem dos domínios ou endereços de e-mail atribuídos ao operador
        - Aprender como Não-SPAM dos domínios ou endereços de e-mail atribuídos ao operador
        - Aprender como SPAM dos domínios ou endereços de e-mail atribuídos ao operador
        - Obter Log de Evidência do E-mail (Log de filtragem do e-mail)
        - Download da mensagem e anexos
        - Liberar todas as mensagens
    - Logs do MTA
        - Visualizar logs do MTA atrelado ao domínio/e-mail atrelado a ele
    - Fila de E-mails
        - Visualizar Fila de E-mails atrelado ao domínio/e-mail atrelado a ele
    - GreyList
        - Aguardando Liberação
            - Visualizar todos
- Painel de Controle
    - Block List
        - Visualizar os registros de block list atrelados ao Operador

        - Adicionar, editar e remover dos domínios ou endereços de e-mail atribuídos ao Operador
    - Allow List
        - Visualizar os registros de allow list atrelados ao Operador
        - Adicionar, editar e remover dos domínios ou endereços de e-mail atribuídos ao Operador

Perfil Somente Log

Perfil focado em obtenção de logs, muito utilizado em sistemas de SIEM.

- RealTime
    - E-mails
        - Obter log de evidência (log de filtragem) de e-mails atribuídos a ele
    - Logs do MTA
        - Visualizar registros dos domínios ou endereços de e-mail atribuídos ao usuário de log

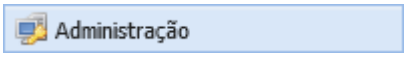
Além dos perfis padrão já apresentados, também temos outros perfis específicos, tais como:

- Perfil para API: Perfil específico para trabalho com as API's do MLI
- Perfil para Criptografia: Perfil para uso com mensagens criptografadas. Esse perfil permite que seja cadastrado um leitor de mensagens criptografadas.
- Perfil Customizado: Com este perfil, é possível liberar acesso a qualquer área de acordo com a necessidade da empresa, dessa forma, criando qualquer tipo de usuário, não ficando preso aos perfis pré-estabelecidos.

Uma vez que você tiver alterado o perfil do usuário, por exemplo: mudar do perfil usuário para o perfil operador, mesmo com o sistema de Conector Externo sincronizado, o perfil alterado **NÃO SERÁ SOBREPOSTO**, ou seja, no exemplo citado, o perfil permaneceria como operador, pois o sistema considera a alteração manual de perfil como prioritária.

Conectores Externos

Use esta página para exibir, adicionar, editar ou excluir servidores LDAP.



/ Administração / Conectores Externos

Visão geral do cadastro de servidores LDAP

Este recurso permite que o HSC MailInspector utilize informações de diretórios LDAP para obter lista de usuários, administradores, operadores, endereços de e-mail e grupos, utilizados para autenticação e realização de diversas configurações dentro do sistema.

Os conectores podem ser utilizados para conectar com serviços LDAPs tais como:

- Microsoft Active Directory:
  - Windows 2000 Server;
  - Windows Server 2003 RTM, Windows 2003 Service Pack 1, Windows 2003 Service Pack 2;
  - Windows Server 2003 R2;
  - Windows Server 2008 RTM, Windows 2008 Service Pack 1, Windows 2008 Service Pack 2;
  - Windows Server 2008 R2, Windows Server 2008 R2 Service Pack 1;
  - Windows Server 2012;
  - Windows Server 2012 R2;
  - Windows Server 2016;
  - Windows Server 2019;
  - Versões superiores;
- Zimbra:
  - Zimbra 7.2.x;
  - Zimbra 8.0.x;
  - Zimbra 8.5.x;
  - Zimbra 8.6.x;
  - Zimbra 8.7.x;
  - Zimbra 8.8.x;
  - Versões superiores;
- IBM Lotus Domino:
  - IBM Lotus Domino 6.0.x;
  - IBM Lotus Domino 6.5.x;
  - IBM Lotus Domino 7.0.x;
  - IBM Lotus Domino 8.0.x;
  - IBM Lotus Domino 8.5.x;
  - IBM Lotus Domino 9.0.x;
  - IBM Lotus Domino 10.0.x;
  - Versões superiores;
- IBM Lotus Notes:
  - IBM Lotus Notes 8.5.x;
  - IBM Lotus Notes 9.x;
  - IBM Lotus Notes 11.x (HCL Notes);
  - Versões superiores;
- Open LDAP:
  - Open LDAP 1.x;
  - Open LDAP 2.0.x;

- Open LDAP 2.1.x;
- Open LDAP 2.2.x;
- Open LDAP 2.3.x;
- Open LDAP 2.4.x;
- Versões superiores;

- Microsoft Exchange:
  - Exchange 2000 Server;
  - Exchange 2003;
  - Exchange 2007;
  - Exchange 2010;
  - Exchange 2013;
  - Exchange 2016;
  - Exchange 2019;
  - Versões superiores;
- Diversos outros sistemas:
  - SAML - Secure Assertion Markup Language;
  - Federation Services;
  - RSA SecureID;
  - CAS - Central Authentication System;
  - Entre outros;

É possível criar múltiplos conectores para diversas plataformas, por exemplo, ter configurado no mesmo appliance conectores para Microsoft AD, outro para Exchange e ainda outro para Zimbra, todos trabalhando de forma harmônica.

Os sistemas, plataformas e versões anteriormente mencionados são apresentados **como referência**, não constituindo uma relação restritiva de compatibilidade. Os conectores utilizados pela **HSCBRASIL no MailInspector** são desenvolvidos para oferecer compatibilidade com as versões inicialmente disponibilizadas pelos respectivos fabricantes, bem como com as versões atualmente suportadas e utilizadas em seus ambientes.

A **HSCBRASIL mantém continuamente atualizadas as configurações e os mecanismos de integração e conexão do MailInspector**, acompanhando as especificações técnicas, requisitos de interoperabilidade e recomendações de configuração estabelecidas pelos fabricantes.
Entre as principais plataformas, diretórios e mecanismos de autenticação contemplados, destacam-se:

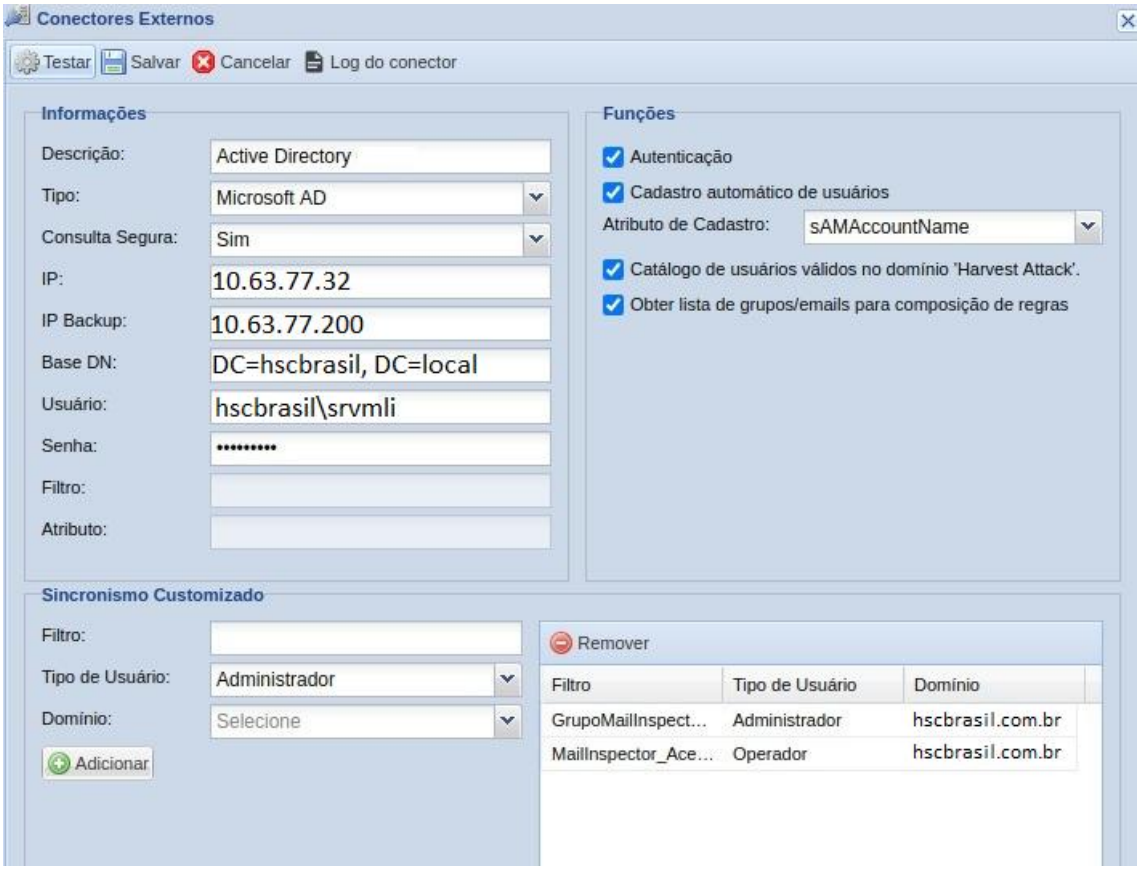
- Zimbra;
- Microsoft;
- IBM Lotus Domino / IBM Lotus Notes;
- Novell GroupWise;
- OpenLDAP;
- SUN iPlanet;
- Novell eDirectory;
- SUN ONE;
- Red Hat Directory Server;
- Sistemas baseados em NTLM;
- Microsoft Active Directory com Kerberos;
- RSA SecurID;
- CAS (Central Authentication Service);
- SAML (Security Assertion Markup Language);

- Federation Services;
- Azure SAML;
- Entre outros sistemas, diretórios, serviços de autenticação e protocolos de integração compatíveis.

Os conectores utilizados pela HSCBRASIL, seguem as normativas de LDAP, dessa forma o servidor sendo padrão LDAP, seguindo RFC's normativas do mesmo, ocorrerá comunicação total e irrestrita com MailInspector. Segue abaixo as RFC's de LDAP atendidas pelo MailInspector.

- RFC 3296: Named Subordinate References in Lightweight Directory Access Protocol (LDAP) Directories
- RFC 3671: Collective Attributes in the Lightweight Directory Access Protocol (LDAP)
- RFC 3672: Subentries in the Lightweight Directory Access Protocol (LDAP)
- RFC 3673: Lightweight Directory Access Protocol version 3 (LDAPv3): All Operational Attributes
- RFC 3866: Language Tags and Ranges in the Lightweight Directory Access Protocol (LDAP) – Antigo: RFC 2596
- RFC 4511: Lightweight Directory Access Protocol (LDAP): The Protocol – Antigo: RFC 2251, RFC 2830, RFC 3771
- RFC 4512: Lightweight Directory Access Protocol (LDAP): Directory Information Models – Antigo: RFC 2251, RFC 2252, RFC 2256, RFC 3674
- RFC 4513: Lightweight Directory Access Protocol (LDAP): Authentication Methods and Security Mechanisms – Antigo: RFC 2251, RFC 2829, RFC 2830
- RFC 4514: Lightweight Directory Access Protocol (LDAP): String Representation of Distinguished Names – Antigo: RFC 2253
- RFC 4515: Lightweight Directory Access Protocol (LDAP): String Representation of Search Filters – Antigo: RFC 2254
- RFC 4516: Lightweight Directory Access Protocol (LDAP): Uniform Resource Locator – Antigo: RFC 2255
- RFC 4518: Lightweight Directory Access Protocol (LDAP): Internationalized String Preparation
- RFC 4522: Lightweight Directory Access Protocol (LDAP): The Binary Encoding Option
- RFC 4525: Lightweight Directory Access Protocol (LDAP) Modify-Increment Extension
- RFC 4526: Lightweight Directory Access Protocol (LDAP) Absolute True and False Filters

Existe a possibilidade de em um único conector importar múltiplos tipos de usuários, por exemplo no mesmo conector diferenciar quais usuários são administradores, quais são operadores e o restante como Usuário normal, conforme imagem a seguir.



Tala de Conector Externo indicando importação de múltiplos tipos de usuários a serem importados

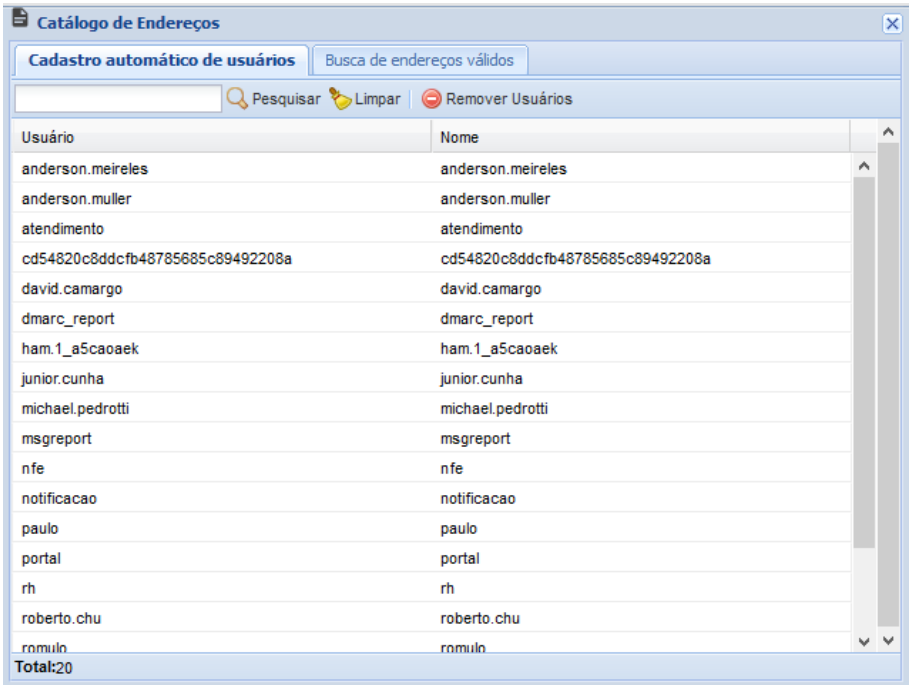
O filtro utilizado no campo de Sincronismo Customizado, deve ser padrão LDAP/AD, por exemplo, separando os grupos distintos, conforme exemplo abaixo:
memberOf= CN=MailInspector_Acesso_Admin, OU=Operadores, OU=Grupos Seguranca, DC=hscbrasil, DC=local

Outro exemplo de Sincronismo Customizado (Filtro aplicado):
memberOf=CN=admin-mail,OU=Rede,OU=Grupos de Servico,OU=Servicos,DC=teste,DC=com,DC=br

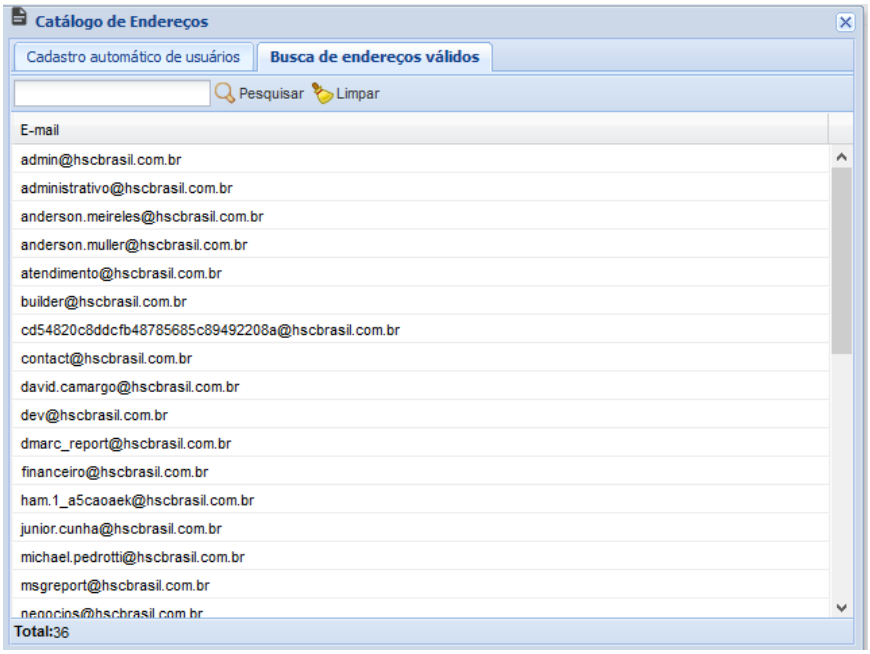
Definições do menu Conectores Externos

As ações possíveis em relação a conectores externos podem ser:

Opções	Definição
Adicionar	Adiciona novo conector externo
Editar	Edita um conector previamente selecionado
Remover	Remove o conector selecionado
Executar	Roda todos os conectores cadastrados
Log Geral	Apresenta os logs dos conectores
Catálogo de Endereços	Indica o que foi importado pelo conector em específico (é necessário selecionar o conector antes de clicar nesta opção), incluindo grupos e listas. Este indicador é separado por: • **Cadastro automático de usuários**: Indica todo os usuários importados para cadastro no MailInspector, caso tenha sido marcada a opção de cadastro automático de usuários no conector; • **Busca de Endereços Válidos:** Indica todos os e-mails válidos importados pelo conector, incluindo listas e alias.



Tala de Catálogo de Endereços > Cadastro automático de usuários



Tala de Catálogo de Endereços > Busca de Endereços Válidos

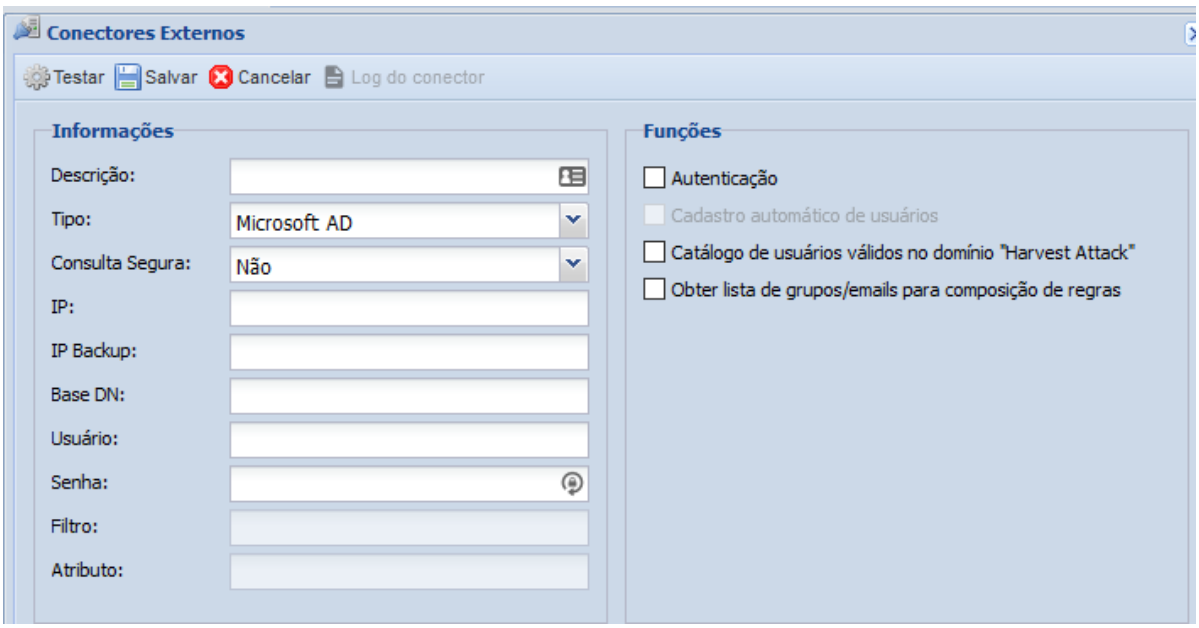
Definições de Opções - Cadastro de Conector Externo

Indique as informações necessárias para que o MailInspector possa conectar e sincronizar com o seu serviço de diretório (LDAP ou similar).

Opções	Definição
Salvar	Quando clicado, grava as configurações realizadas.
Cancelar	Quando clicado, cancela a ação.
Testar	Quando clicado, testa as configurações inseridas.
Log do conector	Quando utilizado, gera log do conector para debug.
Descrição	Informe o nome de identificação do conector LDAP. Ex.: MSAD - srvad.empresa.local.
Tipo de Conector	Escolha entre: • **Microsoft AD** - Sincroniza os usuários existentes em um servidor Microsoft Active Directory. • **Zimbra** - Sincroniza os usuários existentes em um servidor Zimbra. • **LDAP** - Sincroniza os usuários existentes em um servidor que possua uma base LDAP. Compatível com OpenLDAP, IBM Lotus Domino/IBM Lotus Notes, e outros serviços LDAP • **Plesk** - Sincroniza os usuários existentes em um servidor que possua Plesk.
IP	Quando selecionado o conector do tipo **Microsoft Active Directory**, **Zimbra** ou **LDAP**, informe o endereço IP do servidor.
IP Backup	Quando selecionado o conector do tipo **Microsoft Active Directory**, **Zimbra** ou **LDAP**, informe, opcionalmente, o endereço IP de um servidor secundário.

Base DN	Quando selecionado o conector do tipo **Microsoft Active Directory** ou **LDAP**, informe a base DN do domínio. **Obs: SEMPRE é o domínio da empresa, conforme indicação abaixo.** A base DN deve ser informada de maneira completa, no seguinte formato: dc=empresa, dc=com, dc=br Também é aceito domínio local. Segue exemplo: dc=empresa, dc=local
Usuário	Quando selecionado o conector do tipo **Microsoft Active Directory**, informe o nome de um usuário para consulta no formato: usuario@dominio_da_empresa. Quando selecionado o conector do tipo **Zimbra** ou **LDAP**, informe o nome de um usuário para consulta no formato: uid=zimbra, cn=admins, cn=zimbra. Caso o campo fique em branco, será considerado autenticação sem senha (de forma anônima).
Senha	Quando selecionado o conector do tipo **Microsoft Active Directory**, **Zimbra** ou **LDAP**, informe a senha do usuário. Caso o campo fique em branco, será considerado autenticação sem senha (de forma anônima).
Filtro de Pesquisa	Quando selecionado o conector do tipo **LDAP**, informe o filtro de pesquisa do usuário. Um exemplo de filtro de pesquisa por usuário LDAP é (uid=%u).
Atributo	Quando selecionado o conector do tipo **LDAP**, informe o atributo de pesquisa do usuário. Um exemplo de valor de atributo é (uid).
Consulta Segura	Habilita Consulta via protocolo LDAPS "LDAP Seguro". Ao selecionar consulta segura, o MailInspector torna o tráfego LDAP confidencial e seguro usando a tecnologia SSL/TLS (Secure Sockets Layer/Transport Layer Security). Para uso com a consulta segura, é necessária a liberação das portas TCP 636 e TCP 3269, bem como eventual NAT para o servidor LDAP.
Funções	Permite definir funções específicas do servidor LDAP: • **Autenticação** - Quando selecionado, o servidor LDAP é utilizado para realização de autenticação do acesso a interface administrativa, dessa forma, ativando o sistema de **Single Sign-On (SSO)**. Para que o sincronismo dos usuários da base LDAP seja realizado com os **Usuários do Sistema**, a opção de **Autenticação** deve estar marcada. • **Cadastro automático de usuários** - Quando selecionado, faz com que o HSC MailInspector automaticamente cadastre os usuários dentro da console de administração sem a necessidade de interação do administrador. • **Catálogo de usuários válidos no domínio "Harvest Attack"** - Quando selecionado, permite que os usuários sejam sincronizados com o controle de

	Harvest Attack. Este sistema valida na camada de MTA a existência de um usuário válido no sistema interno de e-mails. • **Obter lista de grupos/e-mails para composição de regras** - Quando selecionado, permite a utilização de grupos de usuário, listas de distribuições e alias na composição de **Grupos de Usuários** do sistema.



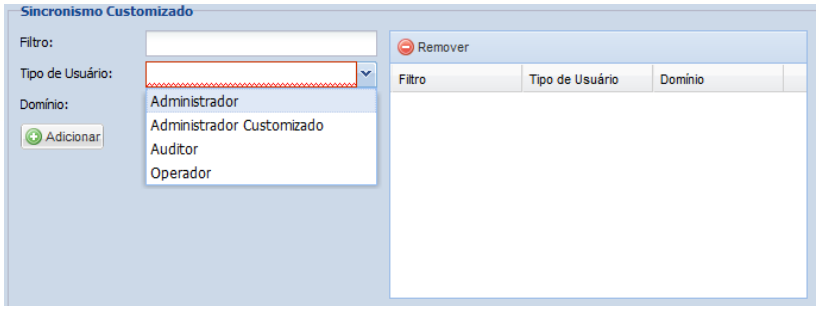
Tala de Configuração de Conector Externo

Definições de Opções - Cadastro de Conector Externo – Sincronismo Customizado

A opção sincronismo customizado somente é habilitada, se for selecionada a opção **Cadastro automático de usuários** no Conector Externo.

A opção de sincronismo Customizado, permite ao administrador do MailInspector inserir automaticamente pessoas usando outros perfis que não sejam somente de usuário, dessa forma permitindo a importação através de sincronização com LDAP/AD de "usuários" do tipo administradores, administradores customizados, operadores ou auditores.

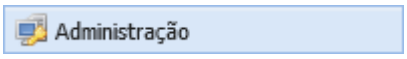
Opções	Definição
Filtro	É necessário incluir um filtro para seleção dos usuários que serão atribuídos os perfis diferenciados (Tipo de Usuário)
Tipo de Usuário	Perfil a ser atribuído ao usuário importado pelo conector. Perfis disponíveis para esse tipo de importação: • Administrador • *Administrador Customizado* • Auditor • Operador
Domínio	Qual(is) domínio(s) que o(s) indivíduo(s) importado(s) irá atuar



Tala de Seleção de Tipo de usuário a ser importado no Conector Externo

Configuração do Cluster

Use esta página para exibir, adicionar, editar ou excluir os pontos em cluster de alta disponibilidade do HSC MailInspector.



/ Administração / Configuração do Cluster

Visão geral da configuração do ambiente de cluster

A configuração de cluster permite que o dois ou mais pontos de acesso funcionem em modo de alta disponibilidade "Tolerância a Falhas" e loadbalancing com sincronização automática dos registros de banco de dados, configurações e dos arquivos armazenados na quarentena dos usuários. Caso ocorra a queda de um dos servidores/link/node/ponto de filtragem, os outros servidores/link/node/ponto de filtragem assumem a carga do processamento, sem ocorrer a sobrecarga do sistema.

Um cluster do MailInspector pode conter dois ou mais servidores podendo ser eles Appliances Virtuais ou Físicos. Um cluster também pode ser configurado para ambientes onde haja necessidade de uma arquitetura como Site Backup onde um dos servidores ficará em outro datacenter. Novos nodos podem ser adicionados de forma simples e sem impacto na infraestrutura atual, aumentando a capacidade de processamento paralelo e disponibilidade da solução.

No MailInspector a inclusão de novos nodes para a montagem de cluster, ou criação de clusters novos, ou ainda edição de cluster já montado, é todo efetuado pela interface gráfica. Não há a necessidade de rodar linha de comando ou acessar o appliance pelo Secure Shell (SSH).

No MailInspector ainda é possível receber os e-mails de forma centralizada em um único IP (VIP – Virtual IP), em vez de encaminhar os e-mails diretamente para pontos de acesso (pontos de filtragem). Uma das vantagens de utilizar este endereço VIP, é que o mesmo distribui os e-mails entre os pontos de filtragem de forma inteligente. O IP do endereço VIP é um IP “flutuante”, ao qual não é atrelado a um único ponto de filtragem, ou seja, o IP sempre ficará em funcionamento, desde que tenha pelo menos um nodo de filtragem ativo. Dessa forma basta o administrador apontar os e-mails para este endereço VIP, que o mesmo se encarrega de manter a alta disponibilidade quanto ao funcionamento do cluster, bem como o redirecionamento dos e-mails ao nodo de melhor performance (loadbalance).

Modos de Balanceamento de Carga entre os Nodes do Cluster

Balanceamento por registro DNS MX: Neste modo as conexões são divididas conforme a resposta do DNS do domínio, isto é, caso ocorra a queda de um link ou indisponibilidade de um node, todo o tráfego automaticamente é direcionado aos outros MX’s/nodes/links, dessa forma em caso de indisponibilidade de um MX, o processo de redirecionamento é efetuado de forma automático e transparente, sem necessidade de intervenção humana.

Balanceamento pelo HSC Smart Balancer: Quando ativado, permite que os e-mails sejam balanceados entre todos os nodes do cluster de forma automática e igualitária diferente do que ocorre quando usando o balanceamento por registro DNS "MX". Esse balanceamento é efetuado de forma automática e transparente, sem necessidade de intervenção humana, mesmo em caso de queda de um dos nodes, o tráfego dos e-mails continua sendo balanceado entre os nodes restantes.

Definições de Opções - Configuração do Cluster

Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição
Adicionar	Cadastra um novo cluster. Quando clicado, abre a caixa de diálogo **Cluster**.
Editar	Edita as configurações de um registro existente. Quando clicado, abre a caixa de diálogo **Cluster**.
Remover	Quando clicado, exclui o cluster selecionado.

Definições de Opções - Cluster - Informações Gerais

Indica a configuração da montagem do Cluster. Basta preencher os dados e seguir o Wizard para criação de fromma simples e fácil de Cluster no MailInspector. É possível criar agrupamentos de Cluster e sub-Clusters, para maior facilidade de uso.

Opções	Definição
Nome	Informe um nome exclusivo para este cluster.
VIP - Virtual IP	Informe o endereço IP virtual do cluster no formato IPv4.
Modo de Balanceamento	Pode ser por "MX" ou pela tecnologia "HSC Smart Balancer" **MX:** O balanceamento das mensagens é feito através da configuração do MX no DNS do cliente. **HSC Smart Balancer:** O balanceamento das mensagens ocorre de forma transparente e não necessita de configurações externas. A carga é divida igualmente entre os nós do cluster garantindo alta performance e escalabilidade. O **HSC Smart Balancer** é o balancer recomendado pela HSCBRASIL, uma vez que ele trabalha melhor que o balancer por MX.
Quarentena Local/Remota	**Local:** O sistema de quarentena é no próprio equipamento. **Remota:** O sistema de quarentena será em outro local. Se for selecionada a opção quarentena remota, é necessário informar o IP do servidor de quarentena. Essa opção somente é liberada se for marcado Quarentena Remota.
Data Center Distribuído	**Sim:** Indica que os dados não serão centralizados na console de gerenciamento; **Não:** Indica que os dados serão centralizados no sistema de gerenciamento;
Pontos de Acesso	Selecione os pontos de acesso que farão parte do cluster em alta disponibilidade. Pode ser selecionado um Cluster anteriormente criado e com isso, agrupar Cluster “dentro” de Cluster.
Avançar	Quando clicado, prossegue para a configuração das informações dos nodos.

Definições de Opções - Cluster - Configuração de Nodos

Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição

Nome do Host	Informe o hostname do ponto de acesso selecionado. Será configurado pelo sistema de instalação do cluster e não poderá ser modificado.
Senha Usuário Root	Informe a senha do usuário root do ponto de acesso.
IP Interface do Cluster	Informe o endereço IP da interface de rede exclusiva para o cluster.
Interface do Cluster	Selecione a interface de rede exclusiva no ponto de acesso para comunicação e replicação dos dados do cluster. Normalmente, a interface configurada para o cluster é a eth1.
Voltar	Quando clicado, retorna a informações gerais.
Avançar	Quando clicado, prossegue para a configuração das informações e pontuação.

Definições de Opções - Cluster - Confirmação das Informações

Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição
Voltar	Quando clicado, retorna a configuração dos nodos.
Avançar	Quando clicado, prossegue para a configuração das informações e pontuação.

Confira todas as informações fornecidas para a criação do cluster de alta disponibilidade, após a criação do cluster não é possível alterar as configurações informadas.

Definições de Opções - Cluster - Conclusão

Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição
Voltar	Quando clicado, retorna a confirmação das informações.
Salvar	Quando clicado, salva as configurações informadas e cria o ambiente de cluster.

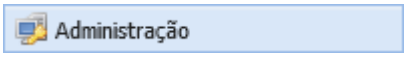
Para o funcionamento do cluster é necessário que tenha sido ativado IPv6, tanto na interface de gerenciamento, quanto nos agentes.

Se a versão do Mailinspector for 4.x ou anterior, após configurado o Cluster, é OBRIGATÓRIA a execução do script na interface de gerenciamento (através de linha de comando).
 # /opt/hsc/mailinspector/admsuite/scripts/mConfigMta.sh

Caso o MailInspector seja 5.x ou superior, não há a necessidade desse procedimento.

Notificação de Quarentena

Use esta página para efetuar as atualizações do sistema HSC MailInspector.



/ Administração / Notificação de Quarentena

Visão geral da Notificação de Quarentena

A notificação de Quarentena ou "Digest" é um sistema que automaticamente envia um resumo da quarentena ara usuário através de um e-mail contendo os detalhes do porquê a mensagem ficou retida.

Deste e-mail o usuário pode executar ações como: Visualizar de forma segura a mensagem, Liberar mensagem, Reportar Bloqueio Indevido, Excluir da Quarentena, Aprender como SPAM, aprender como NÃO SPAM, colocar na Allow List e Block List. Estas ações permitem que o usuário administre sua quarentena sem precisar acessar a interface do sistema, nem solicitar a um administrador ou operador a liberação da mensagem quarentenada.

O e-mail é compatível com todos os clientes de e-mail que suportam e-mails no formato HTML, completamente compatível com sistemas portáteis do tipo Android e iOS, usados em tablets, celulares, etc, sendo totalmente de forma responsiva.

A linguem padrão da Notificação é em Português Brasil, mas pode ser modificada conforme a configuração dos usuários através do botão do canto direito superior "Conta" ou através da tela de gestão dos usuários, estão disponíveis mais de 30 linguagens, dentre eles o Português do Brasil, espanhol, francês, inglês, alemão, italiano, entre outros.

Por padrão (boas práticas recomendadas pela HSCBRASIL), a notificação apresenta somente os e-mails considerados SPAM, PROVÁVEL SPAM e BULK Mail, mas é possível o administrador do sistema liberar qualquer pasta/quarentena para ser apresentado nas notificações de quarentena e dessa forma permitir que o usuário faça liberação de e-mails que tenha sido classificado e bloqueado por outros motivos, por exemplo: a pasta que contenha os e-mails que foram bloqueados por conterem anexos compactados com senha.

Também é permitido ao administrador configurar a periodicidade de envio desse e-mail de quarentena individual, dessa forma pode-se configurar disparos em períodos diferentes para setores diferentes da empresa, como por exemplo a diretoria recebe duas vezes ao dia, enquanto o resto da empresa recebe uma vez por dia a notificação.

A Notificação de Quarentena enviado ao usuário, é totalmente customizável padrão HTML e já planejado para funcionar em tablets, celulares e sistemas afins (por exemplo Android e iOS), trabalhando de forma responsiva, dessa forma, é possível modificar a notificação de quarentena de acordo com a necessidade do administrador, podendo ser alterado e/ou inserido qualquer informação na notificação, desde:

- E-mail de Origem (Tanto na forma de Envelope, quanto na forma de FROM do Cabeçalho);
- E-mail de Destino;
- Assunto;
- Links customizados;
- Imagens diversas;
- Logomarcas da empresa;
- ID do E-mail;
- Telefones;

- Dados da empresa;
- Formatação (Cores, tamanho da fonte, tabulação, etc);
- Motivo da quarentena ou para qual pasta de quarentena o e-mail foi armazenado;
- Entre outras informações e formatos;

No e-mail enviado ainda é possível editar ações:

- **Liberar:** Libera a mensagem correspondente
- **Confiável:** Marca na Allow List do usuário o remetente como confiável
- **Não Confiável:** Marca na Block List do usuário o remetente como Não Confiável
- **Reportar:** Reporta ao administrador um bloqueio indevido, solicitando ao administrador a liberação do e-mail (para caso não tenha a opção de liberação do e-mail por motivo de ser classificado na quarentena de alta periculosidade – tais como vírus, malware, atp, etc). Nesse processo, o email reportado também é analisado pelo administrador e utilizado no autoaprendizado do Machine Learning, de acordo com o que foi reportado e analisado.
- **Excluir:** Exclui o e-mail da quarentena, apagando-o permanentemente do sistema.
- **Solicitar um novo resumo da quarentena:** Faz com que o sistema envie um novo digest ao usuário que solicitou.
- **Enviar informações de Block List/Allow List:** Envia ao usuário o resumo de Sua Block List e Allow List permitindo que o usuário remova entradas.
- **Acessar a quarentena:** Acessa a interface de quarentena individual via HTTPS, permitindo que o usuário possa administrar as suas mensagens retidas na quarentena, mudar a linguagem da interface, controlar block list e allow list, entre outras ações.

Importante salientar que é possível incluir outras ações no e-mail, tais como:

- Visualizar e-mail;
- Marcar como confiável e liberar o e-mail (duas ações em um único link);
- Marcar como indesejável e excluir o e-mail (duas ações em um único link);
- Remoção de todas as ações (transformando a notificação individual em aviso do que está em quarentena) e inclusão do campo ID do e-mail;
- Reportar falso positivo de spam. Uma vez reportado, será enviada a mensagem para averiguação do administrador da ferramenta;
- Reportar falso negativo de spam. Uma vez reportado, será enviada a mensagem para averiguação do administrador da ferramenta;
- Reportar phishing. Uma vez reportado, será enviada a mensagem para averiguação do administrador da ferramenta;
- Reportar falso positivo de phishing. Uma vez reportado, será enviada a mensagem para averiguação do administrador da ferramenta;
- Entre outras ações possíveis, uma vez que o administrador tem acesso as variáveis de notificação, portanto pode ser criado um template próprio;

Nesta tela é possível configurar o envio automático do resumo da quarentena para cada usuário configurando regras por:

- Usuários, Domínio;
- Grupo LDAP;
- Grupo do Microsoft Active Directory;
- Horários;
- Dia da semana;
- Classificação dos e-mails (quais pastas de quarentena serão apresentadas nas notificações)

Ainda é possível customizar os textos (formato, tipo, cor, tamanho, etc) e logotipos do e-mail que é disparado automaticamente pelo sistema, bem como as ações a serem efetuadas, por exemplo: É possível criar uma notificação de quarentena, onde não possui ações a serem tomadas, somente a listagem dos e-mails bloqueados, para que o usuário acione o sistema de suporte da empresa, solicitando a liberação, ou ainda um link externo apontando para algum serviço utilizado pela empresa.

As modificações nas notificações de quarentena, customização de Allow List/Block List, customização da página de resultado, são baseadas em HTML, portanto pode ser feito qualquer tipo de alteração, desde que atenda aos requisitos do código HTML. As customizações podem ser desde mudança de cor ou fonte, até mesmo código de programação específico de acordo com a necessidade da empresa.

É possível ativar o sistema de aprendizado do Digest , dessa forma ele detecta o comportamento do usuário e após o período de aprendizagem, pode-se habilitar a ação automática para o Digest, dessa forma o sistema simula as ações comumente efetuado pelo usuário, tais como:

- Liberar os e-mails sempre oriundos de um determinado remente
- Liberar e-mails sempre que tenha determinado assunto;
- Sempre reportar determinado tipo de mensagem;

As regras são processadas conforme a ordem de inserção.

As regras são processadas conforme a ordem de inserção. Sendo assim caso queira priorizar uma determinada regra você deve movê-la para cima das demais regras.

A leitura das regras segue o padrão de firewall, ao qual lê de cima para baixo e ao encontrar uma regra que case com a condição, a mesma será executada e finalizado o processo, ou seja, não será processada nenhuma outra regra subsequente.

A regra "**Padrão**" sempre será a última e casará com todos usuários do sistema que ainda não casaram com alguma regra acima.

Importante salientar que o conteúdo apresentado do Digest varia de acordo com o que foi configurado no prazo de repetição dele. Por exemplo, se for feita uma regra de Digest a cada 2 horas, o relatório apresentado no Digest, será somente do que for quarentenado nas últimas 2 horas.

Definições de Opções e botões de ações

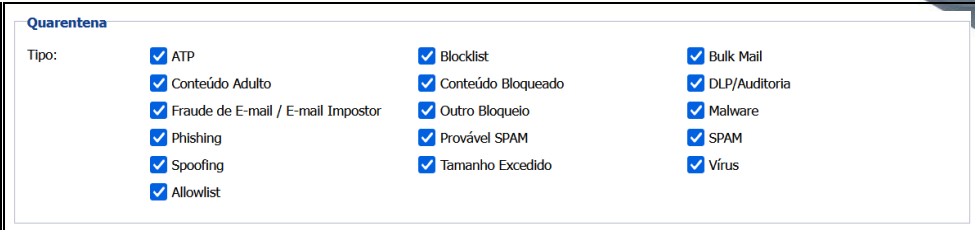
Estas informações descrevem as opções disponíveis nesta página.

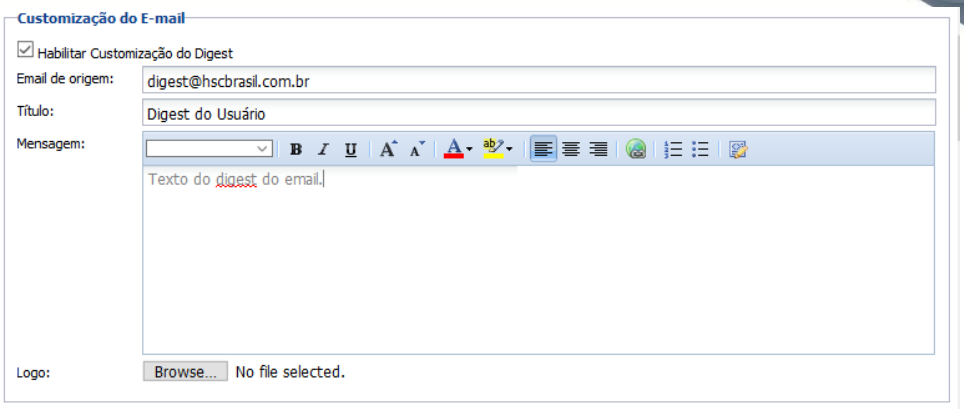
Opções	Definição
Adicionar	Adiciona uma nova regra
Remover	Remove a regra selecionada
Usuários Afetados	Permite ver quais usuários casam com a regra selecionada
Enviar Notificação	Permite o envio de notificação para os usuários que compõem a regra selecionada

Definições de Opções - Adicionar

Estas informações descrevem as opções disponíveis para o agendamento de Notificação de Quarentena por usuário.

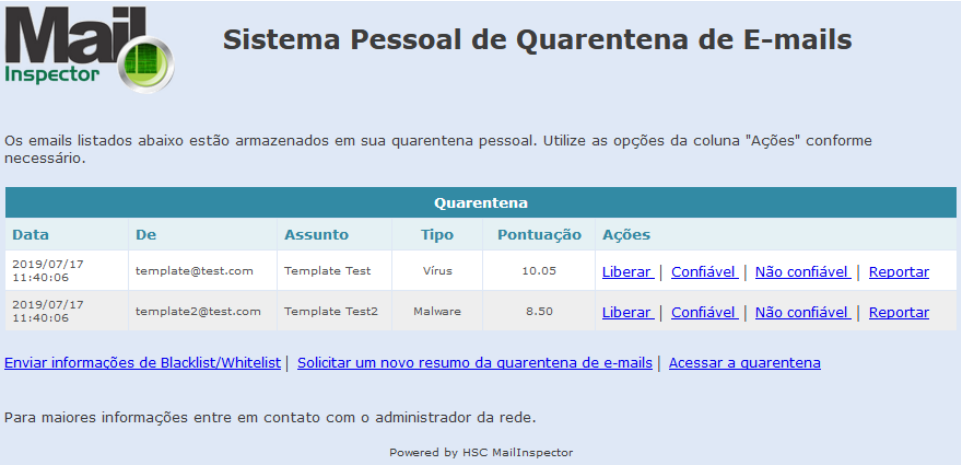
Opções	Definição
Nome	Nome da regra
Permitir Notificação Vazia	Envia a notificação para o usuário mesmo que não existam e-mails retidos na sua quarentena
Tráfego de mensagens que serão analisadas	**Somente Entrada:** É o padrão da notificação. O MailInspector por padrão gera a notificação de quarentena somente para os e-mails de entrada. **Somente Saída:** Ao selecionar esta opção, no Digest gerado, será somente apresentado os e-mails de saída. **Todos:** Cria o Digest apresentando os e-mails quarentenados tanto na saída, quanto na entrada.
Domínios	Selecione quais domínios irão casar com esta regra
Grupos LDAP	Selecione os Grupos LDAP que irão casar com esta regra
Grupos Usuários	Selecione os Grupo de Usuários criados (Configurações > Cadastros > Grupos Usuários) que irão casar com esta regra
Usuários	Selecione os Usuários que irão casar com esta regra
Período de Execução - Dias da Semana	Selecione em que dias da semana o agendamento automático irá ocorrer: • Domingo • Segunda • Terça • Quarta • Quinta • Sexta • Sábado Periodo de Execução - Dias da Semana Dias da Semana: ☐ Domingo ☐ Segunda ☐ Terça ☐ Quarta ☐ Quinta ☐ Sexta ☐ Sábado
Período de Execução - Horário	Selecione em qual(ais) horário(s) o agendamento automático irá disparar a notificação: 00h 01h 02h 03h 04h 05h 06h 07h 08h 09h 10h 11h 12h 13h 14h 15h 16h 17h 18h 19h 20h 21h 22h 23h Periodo de Execução - Horário Horário: ☐ 00h ☐ 01h ☐ 02h ☐ 03h ☐ 04h ☐ 05h ☐ 06h ☐ 07h ☐ 08h ☐ 09h ☐ 10h ☐ 11h ☐ 12h ☐ 13h ☐ 14h ☐ 15h ☐ 16h ☐ 17h ☐ 18h ☐ 19h ☐ 20h ☐ 21h ☐ 22h ☐ 23h
Quarentena	Selecione quais quarentenas serão disponibilizados na notificação (imagem abaixo indica as quarentenas padrão, caso tenha criado uma quarentena customizada, ela também será listada): ATP | Block List | Bulk Mail Conteúdo Adulto | Conteúdo Bloqueado | DLP/Auditoria Frande de E-mail / E-mail Impostor | Outro Bloqueio | Malware Phishing | Provável SPAM | SPAM Spoofing | Tamanho Excedido | Vírus Allow List As quarentenas personalizadas também poderão ser selecionadas nesta opção.

	
Idioma	Selecione o idioma que será utilizado por padrão. Se não for selecionado nenhum idioma o sistema utilizará o idioma configurado na conta do usuário. Os idiomas disponíveis são os mesmos disponíveis no cadastro do usuário. Por padrão além do idioma configurado na conta do usuário, para seleção também são disponibilizados: • Definição do Usuário (ao qual usa o idioma configurado na conta do usuário); • Português; • Inglês; • Espanhol; • Espanhol Paraguaio; • Finlandês
Tempo Máximo Para Liberação	Define tempo máximo em que um usuário poderá liberar uma mensagem retina em sua quarentena (em dias).
Processos Simultâneos	Coloca uma opção no Digest permitindo o usuário selecionar duas ou mais ações simultâneas
Solicitar confirmação do usuário para executar ação	Antes de aplicar a ação clicada, solicita ao usuário a confirmação
Habilitar Auto Aprendizado	Quando selecionado, as ações dos usuários feitas através do Digest serão automaticamente aprendidas no sistema de Blocklist e Allowlist do usuário
Habilitar múltiplo processamento de ações	Permite o múltiplo processamento de ações, sendo compatível somente com quem usa versões mais antigas do leitor de e-mail Outlook. ⚠ Está opção **NÃO é compatível** com Microsoft Outlook 2003 ou superior!
Customização do E-mail	Permite customizar: • E-mail de Origem; • Título: Assunto do E-mail; • Mensagem: Texto do e-mail; • Logo: Logotipo da empresa;



Customização Avançada do Template

Permite customizar o texto e o logotipo do e-mail que será enviado ao usuário de modo avançado, ou seja, permite que seja inserido textos com variáveis de composição do e-mail, imagens, bem como alteração de cores, estilo de fonte, tipo de fonte, tamanho de fonte, inserções de outros links, qualquer elemento externo ou ainda qualquer outro elemento no formato HTML.
Na parte de ações permite ao administrador configurar, incluir e remover links de ações, até mesmo adicionar ação de visualização (preview) do e-mail.
É possível efetuar Preview da página e também carregar de um template padrão.
Segue o template padrão:



Customização de Mensagem de Block List e Allow List

Permite customizar o texto e o logotipo do e-mail que será enviado ao usuário, bem como a disponibilidade das variáveis desejadas, ou seja, permite que seja inserido textos com variáveis de composição do e-mail, imagens, bem como alteração de cores, estilo de fonte, tipo de fonte, tamanho de fonte, inserções de outros links, qualquer elemento externo ou ainda qualquer outro elemento no formato HTML.
Quando o usuário clicar em **Enviar Informações de Block List/Allow List**, ele receberá esta customização no texto da sua lista.
É possível efetuar Preview da página e também carregar de um template padrão.
Segue o template padrão:

<table>
<tr><td></td><td>

</td></tr>
<tr><td>Customização da Página de Resultado</td><td>
Template de retorno de êxito no envio e processamento da mensagem.
É possível customizar o texto e o logotipo do e-mail que será enviado ao usuário, bem como a disponibilidade das variáveis desejadas, ou seja, permite que seja inserido textos com variáveis de composição do e-mail, imagens, bem como alteração de cores, estilo de fonte, tipo de fonte, tamanho de fonte, inserções de outros links, qualquer elemento externo ou ainda qualquer outro elemento no formato HTML.
Segue o template padrão:

</td></tr>
</table>

Mail Inspector

Sistema Pessoal de Quarentena de E-mails

Os emails listados abaixo estão armazenados em sua quarentena pessoal. Utilize as opções da coluna "Ações" conforme necessário.

Quarentena

Data	De	Assunto	Tipo	Pontuação	Ações
14/01/2019 00:39	salete-freitas-9330810-atendimento=hscbrasil.com.br@maildre.com.br	Amil Saude - Condi??es especiais para voc? e para sua familia!	Spam	13.73	Liberar | Confiável | Não Confiável | Reportar
14/01/2019 02:33	renato-passos-11151432-atendimento=hscbrasil.com.br@quartasdefinal.com.br	? s? hoje - Toda linha Ray-Ban com 50% OFF!	Spam	10.12	Liberar | Confiável | Não Confiável | Reportar
14/01/2019 03:18	return-atendimento=hscbrasil.com.br@app.crowmod.com.br	? exclusividade que voc? quer? Aqui voc? tem NOVIDADE!	Spam	19.74	Liberar | Confiável | Não Confiável | Reportar
14/01/2019 06:48	return-atendimento=hscbrasil.com.br@lupadedescontos.com.br	Diversas c?psulas com 30% OFF! Aproveite!	Spam	24.90	Liberar | Confiável | Não Confiável | Reportar
14/01/2019 06:48	return-atendimento=hscbrasil.com.br@lupadedescontos.com.br	? exclusividade que voc? quer? Aqui voc? tem NOVIDADE!	Spam	18.76	Liberar | Confiável | Não Confiável | Reportar

Enviar informações de Blacklist/Whitelist | Solicitar um novo resumo da quarentena de e-mails | Acessar a quarentena

Para maiores informações entre em contato com o administrador da rede.

Powered by HSC MailInspector

Exemplo do E-mail de Notificação de Quarentena

Nome : [Nome do Digest a ser configurado]

Permitir notificação vazia: Não

Dominios: Pesquise na lista

Grupos LDAP: Pesquise na lista

Grupos Usuários: Pesquise na lista

Usuários: Selecione

Pesquise na lista

Periodo de Execução - Dias da Semana

Dias da Semana: ☐ Domingo ☐ Segunda ☐ Terça ☐ Quarta ☐ Quinta ☐ Sexta ☐ Sábado

Periodo de Execução - Horário

Horário: ☐ 00h ☐ 01h ☐ 02h ☐ 03h ☐ 04h ☐ 05h ☐ 06h ☐ 07h ☐ 08h ☐ 09h ☐ 10h ☐ 11h ☐ 12h ☐ 13h ☐ 14h ☐ 15h ☐ 16h ☐ 17h ☐ 18h ☐ 19h ☐ 20h ☐ 21h ☐ 22h ☐ 23h

Quarentena

Tipo:
- ☑ ATP
- ☑ Conteúdo Adulto
- ☑ DLP/Auditoria
- ☑ Malware
- ☑ SPAM
- ☑ Vírus
- ☑ Blacklist
- ☑ Conteúdo Bloqueado
- ☑ Fraude de E-mail / E-mail Impostor
- ☑ Phishing
- ☑ Spoofing
- ☑ Whitelist
- ☑ Bulk Mail
- ☑ Controle de Surto/Comportamento Anômalo
- ☑ Outro Bloqueio
- ☑ Provável SPAM
- ☑ Tamanho Excedido

Idioma

Selecione idioma: Português

Configuração de Regra

Tempo Máximo Para Liberação:

Processos Simultâneos: 5

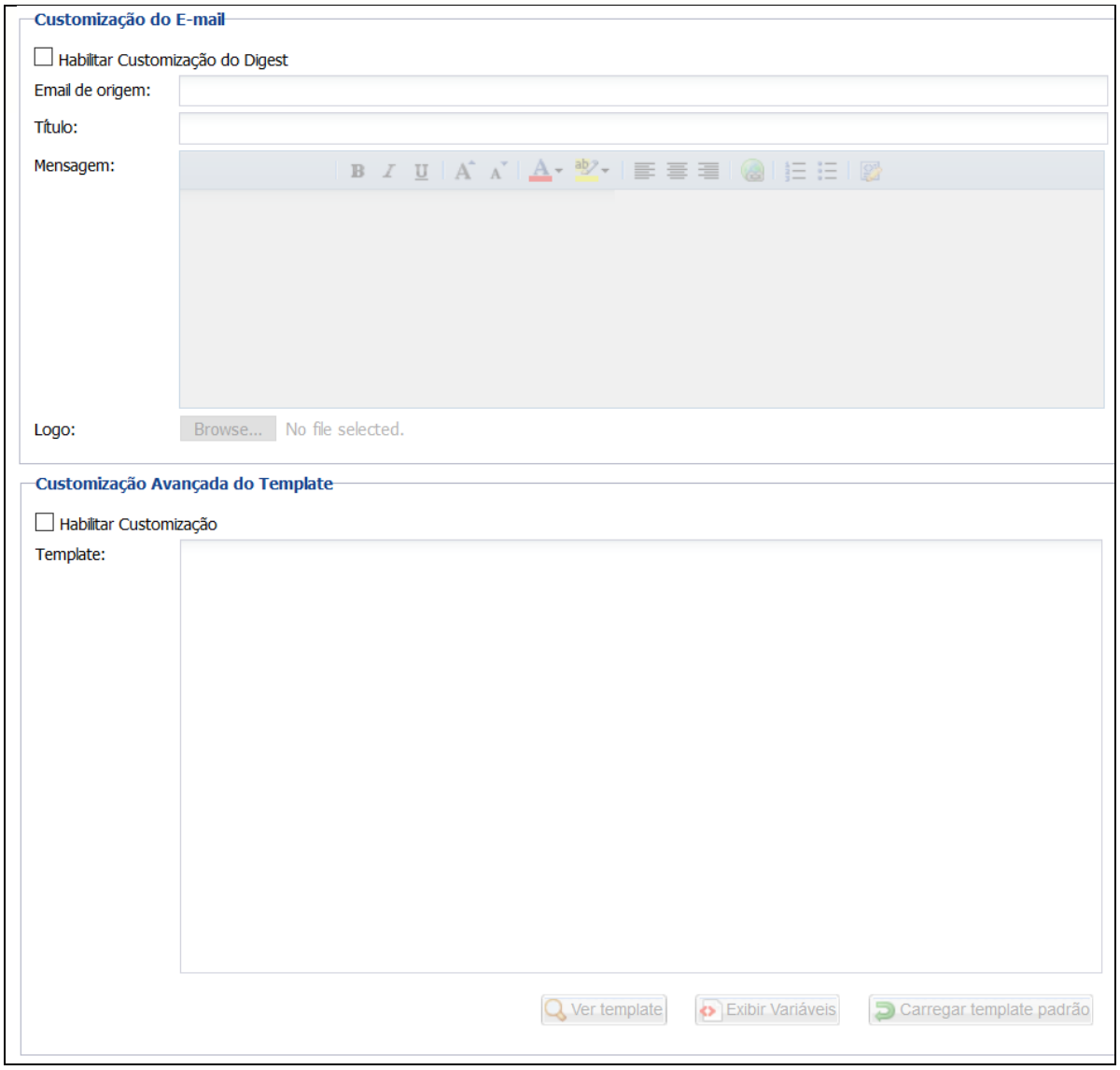
Auto Aprendizado

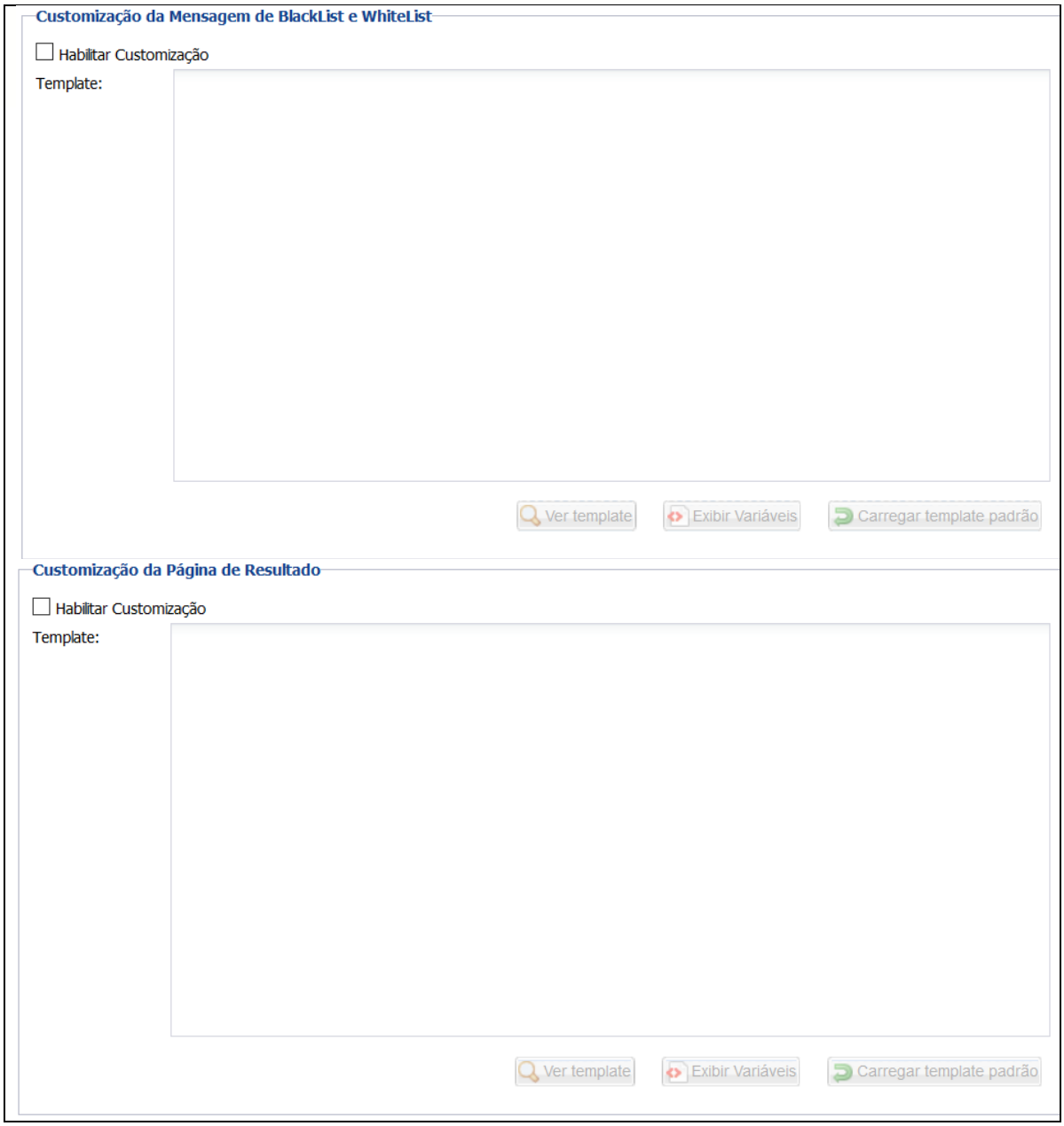
Habilitar Auto Aprendizado: Não

Processamento de ações

Habilitar múltiplo processamento de ações: Não

Está opção NÃO é compatível com Microsoft Outlook 2003 ou superior


Customização do E-mail
Habilitar Customização do Digest
Email de origem:
Título:
Mensagem:
Logo:
Browse...
No file selected.
Customização Avançada do Template
Habilitar Customização
Template:
Ver template
Exibir Variáveis
Carregar template padrão



Tela de Configuração do E-mail de Notificação de Quarentena

Na notificação recebida pelo usuário é possível executar as seguintes **ações sobre a quarentena.**

- **Liberar:** Liberar a mensagem quarentenada.
- **Confiável:** Marcar o remetente da mensagem como confiável (irá incluir remetente na allow list individual).
- **Não Confiável:** Marcar o remetente da mensagem como não confiável (irá incluir remetente na block list individual).
- **Reportar:** Enviar para o fabricante (HSCBRASIL) o e-mail como falso positivo. Uma vez enviada a mensagem, ela será analisada primeiramente pelo sistema de Machine Learning e posteriormente por especialistas para averiguação confirmatória. Uma vez confirmado será gerada a devida assinatura de NÃO SPAM.

- **Excluir:** Exclui o e-mail da quarentena, apagando-o permanentemente do sistema.

Na notificação recebida pelo usuário ainda é possível executar as seguintes ações:

- **Enviar informações de Block List/Allow List:** Envia por e-mail ao usuário o que está marcado como whitelist e blacklist individual dele.
- **Solicitar um novo resumo de quarentena de e-mails:** Envia um novo Digest ao usuário. Esta função é muito utilizada quando se tem um Digest já "vencido" e o usuário precisa solicitar um novo Digest, para conseguir liberar e-mails quarentenados.
- **Acessar a quarentena:** Acessa o portal web do usuário pelo browser. É necessário que o usuário insira seu login e senha. Ao acessar o portal, o usuário além de ter acesso a toda a quarentena, ele poderá efetuar várias configurações, dentre eles:
    - Conta:
        - Alterar a sua senha de acesso ao portal;
        - Bloquear ou liberar envio de notificação de quarentena;
        - Permitir ou não envio de notificação vazia;
        - Mudar o idioma da notificação (Português do Brasil, Inglês, Espanhol, Finlandês);
    - Acesso a Blacklist e Whitelist do usuário;
    - Visualizar os filtros aplicados nos e-mails quarentenados, indicando a pontuação recebida do e-mail, quais filtros aplicados (vírus, filtros de spam, rede social, e-mail marketing, possível ameaça, e-mail suspeito, etc).
    - Visualizar o cabeçalho do e-mail bloqueado;
    - Análise em tempo real dos links contidos no e-mail, pelo SmartDefender;

Ações possíveis em relação as quarentenas no Digest

Quarentena	Liberar	Marcar como Confiável	Marcar como Não Confiável	Reportar
ATP	Não	Não	Não	Sim
DLP/Auditoria	Não	Não	Não	Sim
Vírus	Não	Não	Não	Sim
Tamanho Excedido	Não	Não	Não	Sim
Conteúdo Bloqueado	Não	Não	Não	Sim
Outro Bloqueio	Não	Não	Não	Sim
Block List	Sim	Sim	Não	Sim
Allow List	Sim	Não	Sim	Sim
Provável SPAM	Sim	Sim	Sim	Sim
SPAM	Sim	Sim	Sim	Sim
Bulk Mail	Sim	Sim	Sim	Sim
Conteúdo Adulto	Não	Não	Não	Sim
Controle de Surto/Comportamento Anômalo	Não	Não	Não	Sim
Fraude de E-mail/E-mail Impostor	Não	Não	Não	Sim
Malware	Não	Não	Não	Sim
Phishing	Não	Não	Não	Sim
Spoofing	Não	Não	Não	Sim

Variáveis disponibilizadas para customização de notificações

Template (variáveis) de Notificação de E-mails

VARIÁVEL	DESCRIÇÃO
img1	Logo padrão HSC
customContent	Contém o texto do campo “Mensagem” na opção “Customização do E-mail”.
customLogo	"Contém a imagem do logo personalizado na opção “Customização do E-mail”. No template padrão, esta variável, quando não está vazia, é usada no lugar da variável img1.
multiActions	Indica a configuração da opção "Habilitar múltiplo processamento de ações".
ip	IP ou URL do console de administração, usada no template padrão como parte de alguns links de Ações.
username	Login do usuário.
user_e-mail	E-mail do usuário.

userID	Código do usuário.
rule	Código da regra de notificação de quarentena.
totalMSGS	Total de mensagens nesta notificação.
data	Contém as informações das mensagens em formato array. As informações da primeira mensagem estarão em **data.0**, a segunda mensagem em **data.1** e assim sucessivamente.

Abaixo estão todas as variáveis possíveis de uso em uma mensagem de notificação de quarentena:

VARIÁVEL	**DESCRIÇÃO**
data.0.size	Tamanho da mensagem.
data.0.timestamp	Data e hora da mensagem.
data.0.from_address	Remetente da mensagem.
data.0.subject	Título da mensagem.
data.0.id	Código da mensagem.
data.0.sascore	Pontuação da mensagem.
data.0.release	Indica que se selecionada essa opção, a mensagem será liberada.
data.0.white	Indica que se selecionada essa opção, a mensagem será marcada como Confiável/Allow List.
data.0.black	Indica que se selecionada essa opção, a mensagem será marcada como Não Confiável/Block List.
data.0.report	Indica que se selecionada essa opção, a mensagem será Reportada para avaliação da HSC.
data.0.wlrelease	Indica que se selecionada essa opção, a mensagem será liberada e marcada como Confiável/Allow List (duas ações em “uma”, sem necessidade de marcar como confiável e DEPOIS liberar a mensagem).
data.0.view	Indica que se selecionada essa ação, o conteúdo da mensagem será visualizado.
data.0.delete	Indica que se selecionada essa opção, a mensagem será apagada.
data.0.deleteall	Indica a ação de apagar TODAS as mensagens listadas pela notificação.

Template (variáveis) de Notificaçõa de Whitelist / Blacklist

VARIÁVEL	**DESCRIÇÃO**
ip	IP ou URL do console de administração, usada no template padrão como parte de alguns links de Ações.
img	Imagem usada no botão Apagar.
username	Login do usuário.
rule	Código da regra de notificação de quarentena.
lists	"Contém as informações de Allow List e Block List em formato array.

	As informações da Allow List estão em lists.wl e da Block List em lists.bl."
lists.wl	"Contém as informações de Allow List em formato array. As informações da primeira Allow List estão em **lists.wl.0**, a segunda Whitelist em **lists.wl.1** e assim sucessivamente.

Abaixo estão todas as propriedades de uma Allow List:

VARIÁVEL	DESCRIÇÃO
lists.wl.0.date	Data da criação da Allow List.
lists.wl.0.from_address	Remetente.
lists.wl.0.to_address	Destinatário.
lists.wl.0.token	Token que será verificado ao executar a ação de Apagar.
lists.wl.0.id	Código da Allow List.
lists.bl	"Contém as informações de Block List em formato array. As informações da primeira Block List estão em **lists.bl.0**, a segunda Whitelist em **lists.bl.1** e assim sucessivamente.

Abaixo estão todas as propriedades de uma Block List:

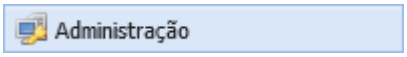
VARIÁVEL	DESCRIÇÃO
lists.bl.0.date	Data da criação da Block List.
lists.bl.0.from_address	Remetente.
lists.bl.0.to_address	Destinatário.
lists.bl.0.token	Token que será verificado ao executar a ação de Apagar.
lists.bl.0.id	Código da Block List.

Template (variáveis) de Notificação de Allow List / Block List

VARIÁVEL	DESCRIÇÃO
logo	Contém a imagem do logo personalizado na opção “Customização do E-mail”, se estiver vazio usará o logo padrão da HSC.
msg_title	Título da página de resultado.
msg_content	Texto da página de resultado.
msg_color	Cor usada para msg_title e msg_content. Em caso de falha será “red” em caso de sucesso “green”.

Ferramentas

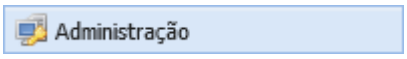
Encontre aqui ferramentas para de administração do MailInspector



/ Administração /Ferramentas

Central de Atualizações

Use esta página para efetuar as atualizações do sistema HSC MailInspector.



/ Administração / Ferramentas / Central de Atualizações

Visão geral da Central de Atualizações

A Central de atualização de software permite visualizar a versão instalada, bem como verificar a disponibilidade de atualizações e novos updates (atualizações), sendo possível disparar a atualização tanto dos pontos de filtragem como da console de administração e nodos do cluster de forma automática ou manual.

Nesta tela também é possível configurar o sistema de Extreme Update, que é responsável por atualizar as assinaturas de segurança (por padrão são aplicadas automaticamente) como:

- Antivírus, Anti-Malware;
- Anti-Phishing;
- Anti-Spam;
- Lista de Mime-Types;
- Sistema de reputação de URLs (websites);
- Sistemas de reputação de IPs (confiáveis e bloqueados);
- Assinaturas de websites;
- Aplicativos Web;
- Imagens de SPAM;
- Imagens pornográficas;
- Acesso ao sistema de inteligência global (SmartDefender);
- Regras e políticas em modo automático (em caso de epidemia, se o administrador tiver ativado o modo de políticas automáticas durante surtos e epidemias);
- E todos os demais mecanismos de filtragem;

Além das assinaturas, a atualização também contempla:

- Download de correção de bugs (aplicação manual);
- Download de novas funcionalidades/features (aplicação manual);

As atualizações são efetuadas na frequência definida pelo administrador, de forma incremental, sendo assim, não é necessária a atualização de toda a base, baixando somente as novas assinaturas. A atualização pode ser feita passando por proxy, bastando configurar as suas definições:

- URL/IP:Porta;
- Usuário;
- Senha;

É possível configurar envio de alertas por SMTP, para:

- Caso ocorra de falha em update de assinatura;
- Caso não ocorra atualização por um determinado período;
- Novas atualizações disponíveis;

Dessa forma o administrador ficará sempre ciente de eventos ocorridos na atualização, sendo tanto como falhas em update de assinatura de antivírus, assinaturas de spams, URL's mal-intencionados, assinaturas de anti-phishing, etc, bem como status de novas atualizações. Também é possível gerar notificação via SMTP para quando a atualização for bem-sucedida, assim, o administrador sempre ficará ciente do processo de atualização.

Na Central de Atualizações também apresenta a opção de Upload de Módulo Customizado, isto é, importação de módulos customizados pela HSCBRASIL especificamente para uso da empresa.

Antes de atualizar qualquer componente do sistema você deve realizar uma cópia de segurança "Backup" através do menu Administração > Backup.

O Processo de atualização das assinaturas de segurança realizadas pelo Extreme Update, **NÃO** irão indisponibilizar o sistema.

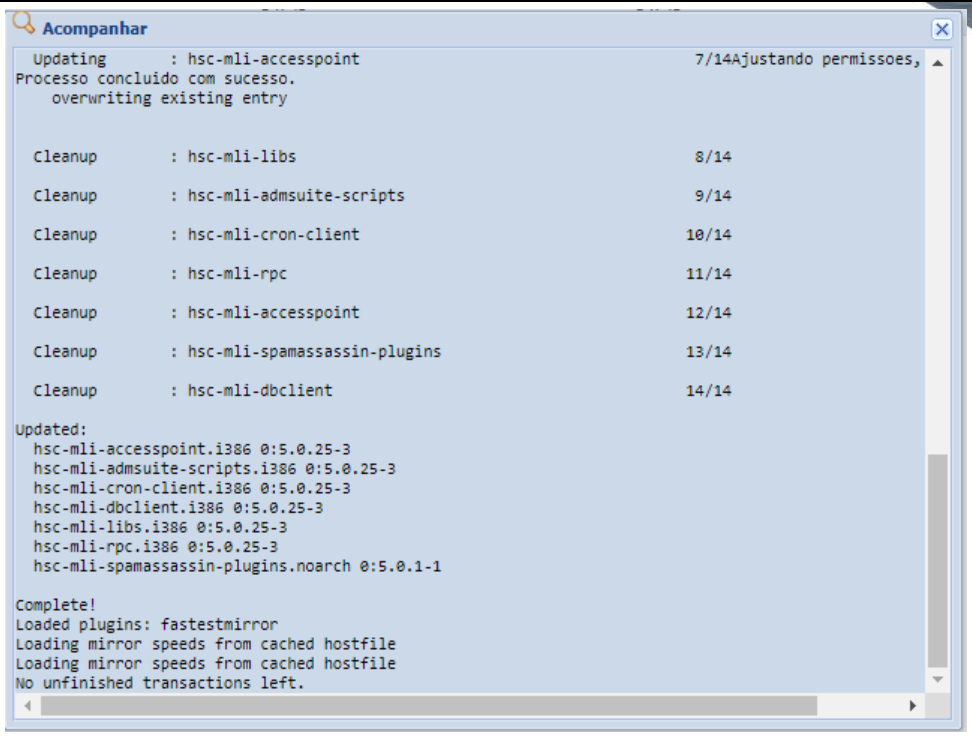
As assinaturas de vírus, malwares, phishing, spam, mime-type, reputação de URL's e IP's, imagens de spam e todos os demais mecanismos, por padrão são efetuados automaticamente.

As atualizações são efetuadas de forma automática enquanto estiver vigente o contrato do uso do MailInspector junto a HSCBRASIL. Após o fim do contrato, elas são desabilitadas automaticamente.

Definições de Opções e botões de ações

Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição
Recarregar	Este botão irá forçar o sistema a checar se há atualizações de software disponíveis. Caso exista os mesmos serão listados no Grid abaixo.
Atualizar	Este botão irá forçar a Atualização do item da Grid selecionado. No Grid será listado todos os pontos de acesso de filtragem bem como a console de administração e os nodos de um cluster.
Acompanhar	Permite o acompanhamento da instalação da atualização que foi marcado para execução. É possível verificar quais pacotes estão sendo baixados e instalados em tempo real.



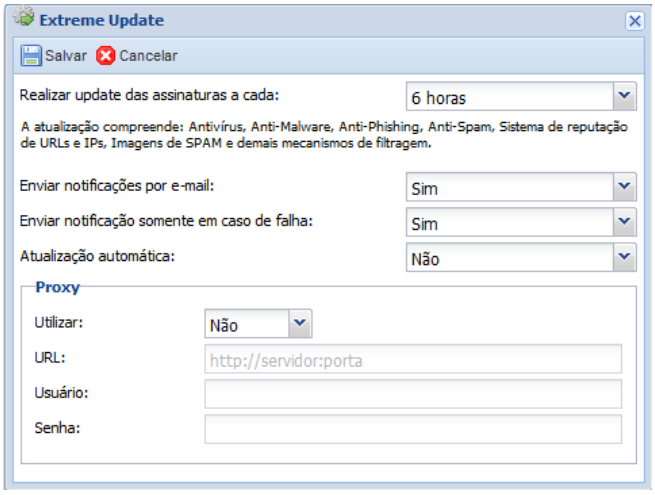
Configuração do extreme update	Este botão irá abrir uma tela para configuração de agendamento do Extreme Update.
Pacote Personalizado	Importa o pacote personalizado criado pela HSCBRASIL para a empresa. Neste mesmo campo é feita a importação manual de assinaturas, bem como importação manual de pacotes de vacinas e outras informações que por padrão seriam transmitidas automaticamente pelo Extreme Update

Definições de Opções - Botão Configuração do extreme update

Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição
Realizar update das assinaturas a cada:	Permite definir de quanto em quanto tempo o Extreme update irá verificar e atualizar as novas assinaturas. Os períodos disponíveis para a customização são: • A cada 5 minutos; • A cada 15 minutos; • A cada 30 minutos; • A cada 1 hora; • A cada 3 horas; • A cada 6 horas; • A cada 12 horas; • A cada 24 horas;

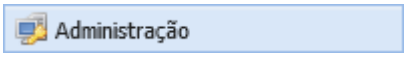
	As atualizações serão realizadas automaticamente sem parar os serviços de e-mail e sem necessidade de reinício dos mesmos. Quando rodando em modo cluster o update ocorre em todos os nodos do cluster automaticamente. Caso haja muito tempo sem atualização, um e-mail de alerta será emitido ao administrador da solução, conforme e-mail configurado no Ponto de Acesso, em Administração > Ponto de Acesso.
Enviar notificações por e-mail:	Define se será enviado um e-mail de notificação ao administrador sobre as atualizações realizadas. Essas atualizações vão desde novas vacinas, novas assinaturas de spams, novas URL's incorporadas no banco de dados, etc.
Enviar notificação somente em caso de falha	Caso seja marcado como Sim, é enviado e-mail somente no caso de falha de alguma atualização automática, como por exemplo, falha em update de vacinas ou falha em update de assinaturas de spam.
Atualização Automática	Configura se o sistema se atualizará de forma automática ou não as correções do sistema e correções de segurança.
Configuração do Proxy	Permite a configuração de um Proxy HTTP para acesso a atualização do sistema. • Servidor • Porta • Usuário • Senha



Configuração de Extreme Update

Backup

Use esta página para exibir e manipular as cópias de segurança do HSC MailInspector



/ Administração / Ferramentas / Backup

Visão geral do backup

Backup significa cópia de segurança.

No HSC MailInspector existem três tipos de cópias de segurança que podem ser geradas:

- **Completo (Tudo):** Faz backup de todo o sistema, bem como o backup da quarentena, portanto tem que tomar cuidado para não extrapolar a capacidade de armazenamento que foi configurado para o MailInspector;
- **Somente Configurações:** Permite executar o backup de todas as configurações/políticas efetuadas pelos administradores e usuários. No caso do ambiente estar em cluster, todas as configurações do cluster serão feitos backup de forma centralizada, permitindo um restore de forma rápida e fácil;
- **Somente Logs/Quarentena:** Backup do sistema de quarentena e logs da ferramenta, isto é, de todas as mensagens armazenadas nas quarentenas do sistema, quarentenas personalizadas, DLP e auditoria, bem como todos os registros de logs das mensagens e relatórios da solução.

A cópia de segurança do tipo *Completo* é composta pelas *Configurações* (banco de dados de configurações da interface de administração) e pelos *Logs/Quarentena*.

Nesta tela é possível também recuperar as últimas 30 alterações efetuadas na ferramenta usando o "Snapshot de Configurações", neste contêiner serão listadas as últimas 30 alterações onde o administrador poderá efetuar a restauração sem impactar no funcionamento da ferramenta.

O backup sempre é feito a “quente”, isto é, sem parada do sistema.

Definições de Opções - Backup

Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição
Mostar registros excluídos?	**Não:** Mostra as rotinas de backup ativos, bem como os backups efetuados pela rotina. **Sim:** Mostra somente as rotinas de backup removidos, bem como os backups efetuados pela rotina.
Adicionar	Cadastra um novo agendamento de criação das cópias de segurança. Quando clicado, abre a caixa de diálogo **Adicionar/Editar Backup**.
Editar	Edita as configurações de um registro existente. Quando clicado, abre a caixa de diálogo **Adicionar/Editar Backup**.
Remover	Quando clicado, exclui o registro selecionado.
Executar	Executa manualmente o processo de criação de uma cópia de segurança, a partir de uma configuração de agendamento previamente cadastrada.

	Todas as configurações serão sobrescritas, somente será possível restaurar as modificações a partir de uma cópia de segurança realizada anteriormente.
Disaster Recovery	Serve para executar uma restauração completa do ambiente em caso de perda total. Para isso basta selecionar o arquivo de backup e enviar para recuperação no MailInspector. Todas as configurações serão sobrescritas, somente será possível restaurar as modificações a partir de uma cópia de segurança realizada anteriormente.
Configurações	Ativar Backup automático quando aplicar uma nova configuração: **Sim:** Faz o snapshot automático das configurações antes de aplicar uma configuração, **Não:** Não ativa snapshot automático das configurações antes de aplicar uma nova configuração.

Menu de controle de backup

Definições de Opções - Adicionar/Editar Backup

Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição
Salvar	Quando clicado, grava as configurações realizadas.
Cancelar	Quando clicado, cancela a ação.
Tipo de Backup	Escolha entre: • **Completo (Tudo):** Faz backup de todo o sistema, bem como o backup da quarentena, portanto tem que tomar cuidado para não extrapolar a capacidade de armazenamento que foi configurado para o MailInspector; • **Somente Configurações:** Permite executar o backup de todas as configurações /políticas efetuadas pelos administradores e usuários. No caso do ambiente estar em cluster, todas as configurações do cluster serão feitos backup de forma centralizada, permitindo um restore de forma rápida e fácil; • **Somente Logs/Quarentena:** Backup do sistema de quarentena e logs da ferramenta, isto é, de todas as mensagens armazenadas nas quarentenas do sistema, quarentenas personalizadas, DLP e auditoria, bem como todos os registros de logs das mensagens e relatórios da solução.
Dia da Semana	Defina a periodicidade com que a cópia de segurança será gerada automaticamente pelo sistema.
Hora	Defina o horário em que a cópia de segurança será criada.

Definições de Opções – Enviar para Servidor Remoto

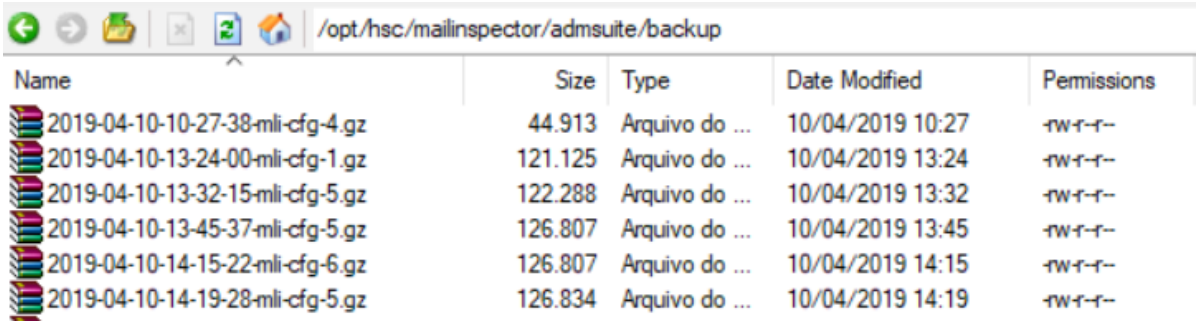
Esta opção permite criar agendamentos/automatização de envio de backup para um sistema externo de armazenamento.

Opções	Definição
Ativar	• **Sim:** Ativa envio do Backup para um servidor Remoto • **Não:** Mantém inativo a opção de envio do backup para servidor remoto
Tipo	• **FTP:** Envio pelo protocolo FTP • **SFTP:** Envio usando o protocolo SFTP • **Autenticar:** Utiliza sistema autenticado de usuário e senha para o protocolo selecionado anteriormente. • **Anônimo:** Não utiliza sistema de autenticação para uso com o protocolo selecionado anteriormente.
Host	IP / Nome do host para qual será enviado o backup. O campo após o host é a porta utilizada para o protocolo de envio do backup.
Username	Nome do usuário que está apto a autenticar no protocolo anteriormente selecionado.
Senha	Senha para uso do envio do backup.

É possível efetuar a exportação dos arquivos do backup utilizando outras ferramentas além do FTP. A localização dos arquivos a serem puxados ficam na máquina de Interface de Gerenciamento em: **./opt/hsc/mailinspector/admsuite/backup/**

Estes arquivos podem ser acessados através de acesso via protocolo SSH ou mesmo copiado através do protocolo SFTP/SCP.

Desta forma também é possível a instalação de agentes de backup dentro da solução a fim de integrar com soluções de backups de terceiros.



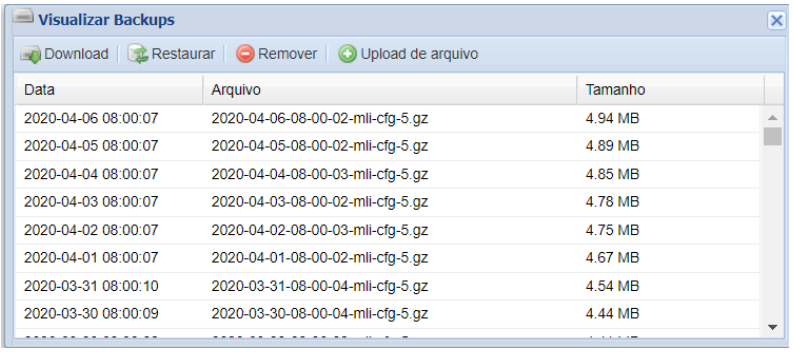
Tela de backup disponíveis (ao dar duplo clique sobre a rotina de backup)

Definições de Opções – Visualizar Backups

Ao efetuar duplo clique em job de backup é possível visualizar todos os backups efetuados na solução, permitindo as seguintes ações:

Opções	Definição
Download	Realiza o download da cópia de segurança selecionada para a estação do usuário, desta forma permite ao administrador exportar um backup já realizado.
Restaurar	Restaura a cópia de segurança selecionada, sobrescrevendo todo o conteúdo do banco de dados.

	Este procedimento não irá gerar parada do sistema ou indisponibilidade de serviços.
Remover	Quando clicado, exclui a cópia de segurança selecionada.



Restore

Para efetuar a restauração, basta dar duplo clique sobre a rotina de backup (conforme orientado na opção anterior), que apresentará todos os backups efetuados pela rotina selecionada. Selecione o backup a ser restaurado e clique no botão Restaurar.

Obs: Caso seja efetuado a restauração do MailInspector em outra máquina, é necessário alterar os dados de rede e outras configurações diferentes do backup original.

Disaster Recovery

É a forma mais rápida de efetuar uma restauração de backup previamente efetuado.

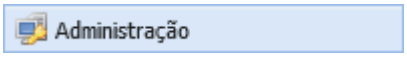
Ao clicar no botão de Disaster Recovery, é aberta uma tela ao qual o administrador poderá indicar o arquivo de restauração e após seleção, o recovery tem início, restaurando as configurações/logs/quarentena, de acordo com o arquivo indicado. A restauração é automatizada, sem necessidade de intervenção ou necessidade de configuração do administrador.

Banco de Dados

O MailInspector utiliza Banco de Dados relacional, indexado, de forma a agilizar as consultas, para maior confiabilidade e estabilidade do sistema. Os dados são encriptados, dessa forma garantindo maior segurança e o licenciamento do mesmo já está incluso.

Dentre as vantagens do Banco de Dados usado pelo MailInspector, podemos citar:

- Escalabilidade: Lida com mais transações e faz ajuste de escala deixando mais eficiente;
- Desempenho: Utiliza tecnologia XtraDB, que garante maior rapidez em relação a outros Banco de Dados relacionais;
- Confiabilidade: Resiliência a corrupção de dados, replicação com segurança contra quebra;
- Gerenciamento: Capacidade de Backup on-line, importação/exportação de tabela on-line;
- Diagnóstico: Perfil e instrumentação avançados;
- Portabilidade: Possibilidade de exportação de diversas tabelas;
- Flexibilidade: Tamanho de página variável, gerenciamento de buffer pool melhorado em relação aos Bancos de Dados normais;
- Licenciamento ilimitado: O Banco de Dados já vem completo para uso, sem eventuais limitações, nem necessidade de aquisição de módulos e/ou licenças extras;



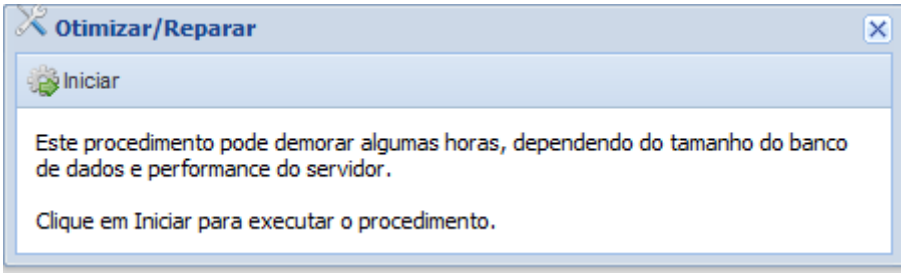
/ Ferramentas /Banco de Dados

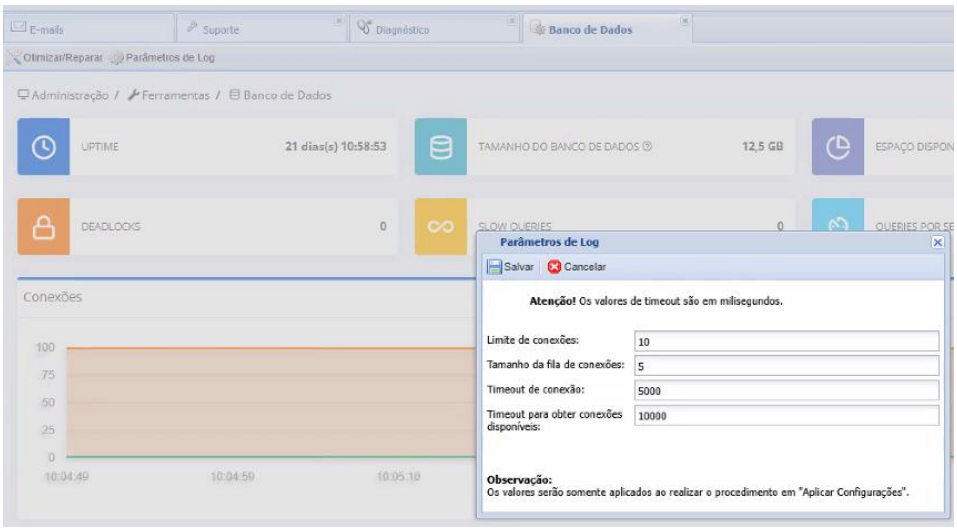
Visão geral do Banco de Dados

O Dashboard de análise da saúdo do Banco de dados dos Logs, Relatórios e Quarentena da solução MailInspector. Através desta tela é possível verificar a situação do DB bem como efetuar reparos, otimização e compactação. Essas atividades podem ser agendadas para execução automática, de acordo com a necessidade do administrador da solução.

Definições de Opções - Botões

Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição
Otimizar/Reparar	Quando clicado, inicia o processo de análise, reparação do Banco de Dados, reindexação e compactação do Banco de Dados. Neste processo todo sistema de dados e índices serão reparados, reindexados e compactados automaticamente. 

Agendamento	Agenda quando será executado a otimização, reparo e compactação do Banco de Dados. Periodo de Execução - Dias da Semana Dias da Semana: Domingo, Segunda, Terça, Quarta, Quinta, Sexta, Sábado Periodo de Execução - Horário Horário: 00h, 01h, 02h, 03h, 04h, 05h, 06h, 07h, 08h, 09h, 10h, 11h, 12h, 13h, 14h, 15h, 16h, 17h, 18h, 19h, 20h, 21h, 22h, 23h
Parâmetros de Log	Apresenta valores em milissegundos em relação a conexões do Banco de Dados **Limite de Conexão:** Limita o número de conexões do Banco de Dados **Tamanho da fila de conexões:** Número de conexões em fila **Timeout de conexão:** Tempo para ser considerado um timeout na conexão **Timeout para obter conexões disponíveis:** Tempo de espera para obter uma conexão no Banco de Dados 

Definições das Sessões de Informações e Gráficos

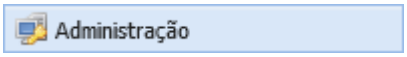
Estas informações descrevem as informações disponíveis nesta sessão.

Item	Definição
Uptime	Tempo de execução da daemon do DB
Tamanho do DB	Tamanho utilizado pelo DB atualmente
Espaço disponível	Espaço disponível na Partição do Disco do DB
Tabelas	Número de tabelas da solução
Gráfico de Conexões	Gráfico que apresenta histórico de número de conexões por segundo no DB
Deadlocks	Número de processos em DeadLock no DB
Slow Queries	Número de Queries lentas que foram executadas
Queries P/ Segundo	Média de Queries por segundo

Saúde do Banco	Status da saúde das tabelas.

Diagnóstico

Use esta página para realizar diagnósticos de: Rede, DNS, Serviços e Conectividade.



/ Ferramentas / Diagnostico

Visão geral do Diagnóstico

Nesta tela o administrador poderá efetuar teste na infraestrutura do HSC MailInspector, a fim de identificar possíveis problemas, consolidando as informações de diagnóstico necessárias para o suporte.

Os seguintes testes podem ser possíveis:

- **Conectividade TCP:** Testa Conectividade com alguma porta TCP;
- **Conectividade ICMP:** Testa o protocolo PING;
- **DNS:** Faz consulta DNS sobre um domínio;
- **Conectividade HSC:** Testa conectividade com servidores da HSC;
- **DNS – Reverso:** Testa DNS Reverso de um determinado IP;
- **SPF:** Lista a configuração SPF de um determinado domínio. Apresenta a entrada TXT referente ao protocolo de segurança SPF;
- **DKIM:** Lista a configuração DKIM de um determinado domínio. Apresenta a entrada TXT referente ao protocolo de segurança DKIM;
- **DMARC:** Lista a configuração DMARC de um determinado domínio. Apresenta a entrada TXT referente ao protocolo de segurança DMARC;
- **Portas de Saída do MailInspector:** Testa todas as portas de conectividade dos MailInspector. Estas portas devem estar abertas no Firewall sentido MailInspector para Internet;
- **Envia E-mail:** Permite o envio de e-mail à partir de um ponto de acesso selecionado;
- **Trace Route:** Testa a rota até o destino indicado, apresentando todos os saltos;
- **Performance do Servidor:** Executa um teste completo do servidor em relação a atendimento dos requisitos para o bom funcionamento do MailInspector;
- **Conectividade Microsoft 365:** Testa a conectividade com os Serviços da Microsoft Office 365, para teste de uso do M-SOAR;
- **Análise de Conteúdo:** Permite realizar a análise de assinaturas e de regras DLP em um e-mail em formato .EML ou .TXT;

Definições de Opções - Botões

Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição
Selecione o Ponto de Acesso	Selecione o Ponto de Acesso no qual deseja fazer o diagnóstico
Executar	Executa o Diagnóstico selecionado

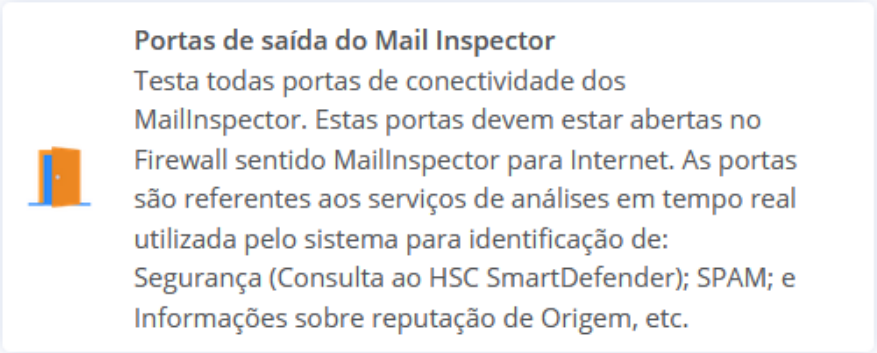
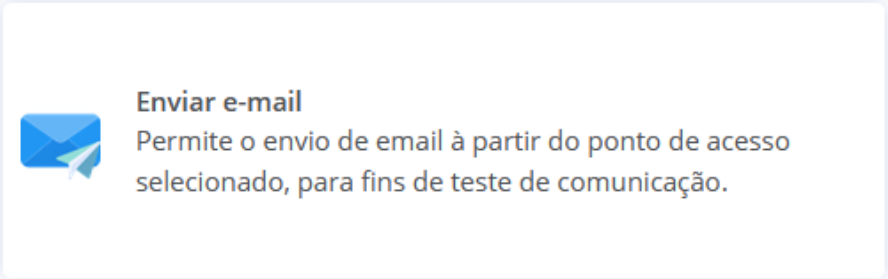
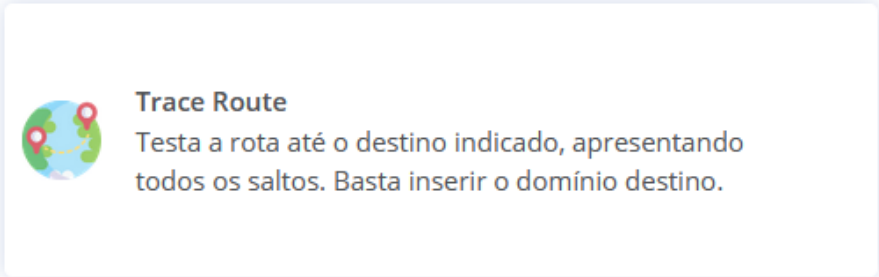
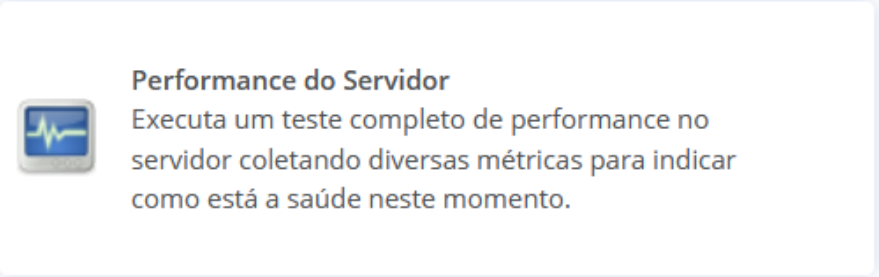
Definições dos Testes de Diagnósticos disponíveis

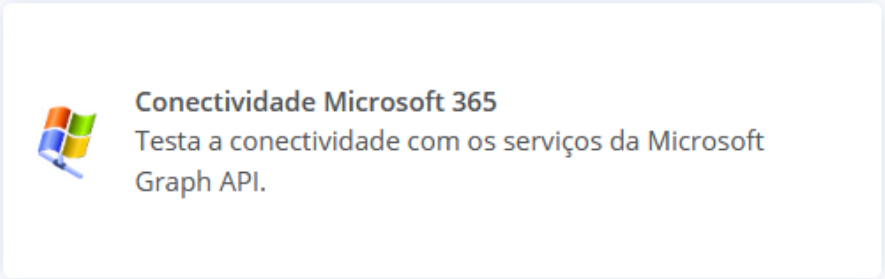
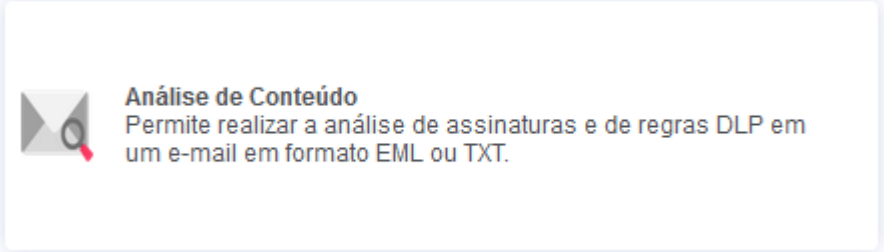
Estas informações descrevem as informações disponíveis nesta sessão.

Item	Definição

Conectividade TCP	Testa Conectividade com alguma porta TCP. Informe o IP destino e a porta de teste. **Conectividade TCP** Testa Conectividade com alguma porta TCP. Informe o IP destino e a porta de teste.
Conectividade ICMP	Testa Conectividade ICMP. Informe o IP destino. **Conectividade ICMP** Testa Conectividade ICMP. Informe o IP destino.
DNS	Faz consulta DNS sobre um domínio. Informe o domínio e o servidor DNS que será utilizado para o teste. **DNS** Faz consulta DNS sobre um domínio. Informe o domínio e o servidor DNS que será utilizado para o teste.
Conectividade HSC	Testa conectividade com servidores da HSC. Servidores de Atualização e Cloud Security, dessa forma é verificado se consegue alcançar os servidores dos serviços de atualização de assinaturas da HSCBRASIL. **Conectividade HSC** Testa conectividade com servidores da HSC. Servidores de Atualização e Cloud Security, dessa forma é verificado se consegue alcançar os servidores dos serviços de atualização de assinaturas da HSCBRASIL. Retorna como resultado os endereços testados e se houve perda de pacotes ou erro na comunicação entre o MailInspector e os repositórios da HSCBRASIL.
DNS - Reverso	Testa DNS Reverso de um determinado IP. É possível efetuar o teste sobre o servidor de DNS indicado, dando maior flexibilidade quanto a averiguação do DNS Reverso.

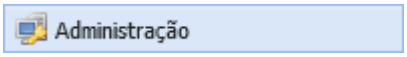
	DNS Reverso Testa DNS Reverso de um determinado IP. É possível efetuar o teste sobre o servidor de DNS indicado, dando maior flexibilidade quanto a averiguação do DNS Reverso.
SPF	Lista a configuração SPF de um determinado domínio. Apresenta a entrada TXT referente ao protocolo de segurança SPF. **SPF** Lista a configuração SPF de um determinado domínio. Apresenta a entrada TXT referente ao protocolo de segurança SPF.
DKIM	Lista a configuração DKIM de um determinado domínio. Apresenta a entrada TXT referente ao protocolo de segurança DKIM (por padrão é utilizado o SELECTOR **default**, mas é possível indicar outro SELECTOR). **DKIM** Lista a configuração DKIM de um determinado domínio. Apresenta a entrada TXT referente ao protocolo de segurança DKIM (por padrão é utilizado o SELECTOR default).
DMARC	Lista a configuração DMARC de um determinado domínio. Apresenta a entrada TXT referente ao protocolo de segurança DMARC. Dessa forma é possível verificar o RUF e RUA, bem como a ação definida no DMARC. **DMARC** Lista a configuração DMARC de um determinado domínio. Apresenta a entrada TXT referente ao protocolo de segurança DMARC. Assim, é possível verificar o RUF e RUA, bem como a ação definida no DMARC.
Portas de Saída do MailInspector	Testa todas as portas de conectividade dos MailInspector. Estas portas devem estar abertas no Firewall sentido MailInspector para Internet. As portas são referentes aos serviços de análises em tempo real utilizada pelo sistema para identificação de: • Segurança (Consulta ao HSC SmartDefender);

	• SPAM; • Informações sobre reputação de Origem, etc. 
Enviar E-mail	Permite o envio de e-mail à partir do ponto de acesso selecionado, para fins de teste de comunicação. 
Trace Route	Testa a rota até o destino indicado, apresentando todos os saltos. Basta inserir o domínio destino. 
Performance do Servidor	Executa um teste completo do servidor em relação a atendimento dos requisitos para o bom funcionamento do MailInspector. 
Conectividade Microsoft 365	Testa a conectividade com os Serviços da Microsoft Office 365, para teste de uso do M-SOAR.

	
Análise de Conteúdo	Faz a análise de e-mails previamente salvos no formato .EML ou .TXT, analisando assinaturas e regras de DLP. 

Suporte

Use esta página para features de monitoria e suporte com o fabricante

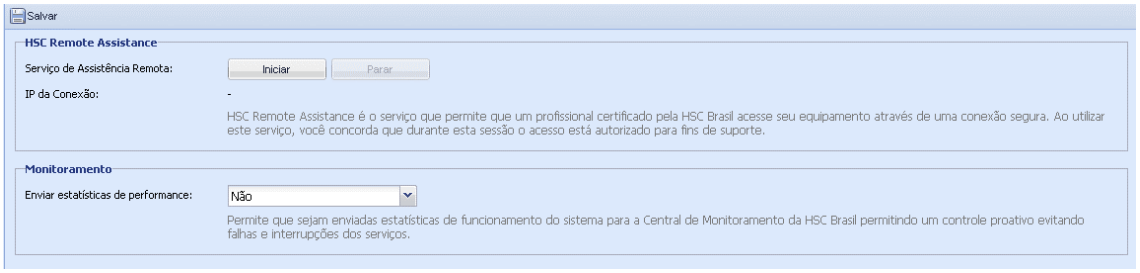


/ Administração / Ferramentas / Suporte

Visão geral do Suporte

HSC Remote Assistance

HSC Remote Assistance é o serviço que permite que um profissional certificado pela HSCBRASIL acesse seu equipamento através de uma conexão segura (VPN) criptografada. Ao utilizar este serviço, você concorda que durante esta sessão o acesso está autorizado para fins de suporte. O acionamento da VPN somente poderá ser efetuado pelo administrador da solução.

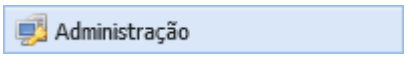


Monitoramento

Ao ativar esta função, o sistema envia as informações de consumo e desempenho dos appliances para HSCBRASIL, para controle de falhas e prevenção de sobrecarga no sistema, disparando alertas quando ocorrem sobrecargas nos appliances, como uso excessivo do disco, CPU, memória. Com essas informações, é possível a prevenção de falha no sistema por problemas de consumo e/ou falta de recursos.

Tunning

É possível efetuar um ajuste fino nos pontos de acesso individualmente, para que o MailInspector tenha uma melhor performance.



/ Administração / Ferramentas / Tunning

Visão geral do Tunning

O uso do Tunning é indicado para administradores experientes, pois esse processo pode tanto melhorar a performance do sistema, quanto a sua degradação e até mesmo colapso do sistema. O administrador poderá indicar a quantidade de memória reservada para uso do sistema, bem como alterar controles de cache e opções de kernel do sistema.

Definições de Opções - Botões

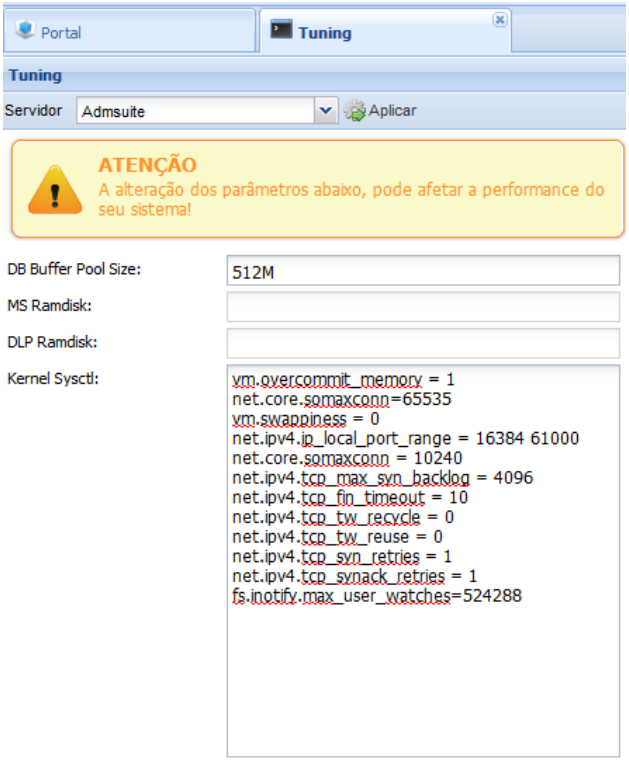
Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição
Selecione o Ponto de Acesso	Selecione o Ponto de Acesso no qual deseja fazer o ajuste fino
Aplicar	Executa o Tunning configurado

Definições de Opções

Estas informações descrevem as opções disponíveis nesta página.

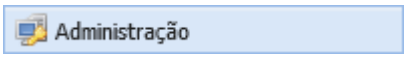
Opções	Definição
DB Buffer Pool Size	Tamanho de Cache em Memoria do Banco de Dados. Quando usando cluster alterar este valor somente no Admsuite deixando um valor de no máximo 80% da memoria total. O valor deve ser colocado seguindo o Prefixo **M** para Mega e **G** para Giga.
MS Ramdisk	Área reservada em memoria RAM para Escaneamento de mensagens
DLP Ramdisk	Área reservada em memoria RAM para Escaneamento de mensagens DLP
Kernel Sysctl	Este campo mexe com múltiplos parâmetros do Kernel do sistema, devendo ser mexido somente por profissionais certificados pela HSCBRASIL



Tela de Tunning do Sistema MailInspector

Certificado SSL

É possível criar um certificado autoassinado ou importar um certificado customizado para o sistema do MailInspector.



/ Administração / Ferramentas / Certificado SSL

Visão geral do Certificado SSL

O SSL (Secure Sockets Layer) é um protocolo de segurança criado pela Netscape que se tornou padrão internacional para troca de informações sigilosas na Internet.

A tecnologia SSL foi incorporada em todos os browsers populares e funciona automaticamente quando um usuário se conecta a um servidor habilitado para o protocolo, que é o caso do MailInspector. É fácil saber quando um servidor o usa, pois sua URL iniciará com https. O “s” vem de “Secure”

O browser utilizado ao se conectar, automaticamente pedirá ao MailInspector um certificado digital da Autoridade Certificadora (CA), esse certificado poderá ser autoassinado ou importado. Ela autentica a identidade do servidor para garantir que não seja enviado dados sigilos para um hacker ou um site falso.

Uma vez com a comunicação esteja estabelecida com SSL entre o browser e o servidor do MailInspector, o browser irá automaticamente criptografar todas as informações enviadas para o sistema, assegurando a comunicação segura entre o browser e o servidor do MailInspector. Quando as informações chegam ao MailInspector, são decifradas usando uma chave secreta. Se o MailInspector envia informações de volta, essas informações também são criptografadas antes de serem enviadas. O navegador irá decifrá-las automaticamente no momento da chegada.

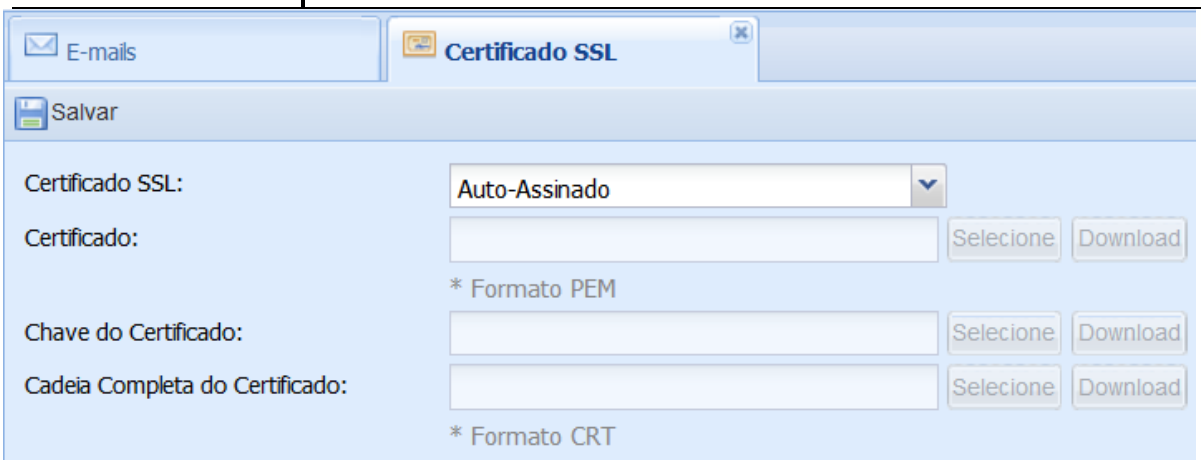
Outra característica da tecnologia SSL é a capacidade de autenticar os dados de modo que um intercessor não possa substituir por outros falsos sem serem detectados.

Definições de Opções

Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição
Salvar	Salva as configurações do Certificado SSL
Certificado SSL	Escolha entre: • **Auto-assinado:** O próprio MailInspector gera o certificado SSL, sem necessidade de importação ou configuração. • **Customizado:** Permite a importação de certificado gerado por unidade certificadora.
Certificado	Somente é liberada esta opção, quando for escolhido o Certificado SSL como sendo Customizado. Selecione o local do Certificado com extensão padrão .PEM
Chave do Certificado	Somente é liberada esta opção, quando for escolhido o Certificado SSL como sendo Customizado. Selecione o local da chave do certificado, com o formato padrão .KEY

Cadeia Completa do Certificado	Selecione o local da cadeia do certificado, no formato padrão .CRT



Tela de Importação de Certificado Válido para o MailInspector

Caso o certificado esteja em outro formato, é possível efetuar a conversão dele para os formatos PEM e CRT.

Devemos lembrar que os certificados são por padrão de acordo com o sistema operacional que o gerou ou que o opera, seguindo os formatos:

- Microsoft Windows: Arquivos formato .PFX
- Linux Apache: Arquivos formato .CRT, .CER

Além dos formatos acima descritos (os mais comuns), ainda temos outros. Segue a descrição completa dos formatos, bem como a finalidade de cada um deles:

Formato PEM

O formato PEM é o formato mais comum em que as Autoridades de Certificação emitem certificados. Os certificados PEM geralmente têm extensões como .pem, .crt, .cer e .key . Eles são arquivos ASCII codificados em Base64 e contêm instruções "----- BEGIN CERTIFICATE -----" e "----- END CERTIFICATE -----". Certificados de servidor, certificados intermediários e chaves privadas podem ser colocados no formato PEM.

O Apache e outros servidores semelhantes usam certificados de formato PEM. Vários certificados PEM, e até mesmo a chave privada, podem ser incluídos em um arquivo, um abaixo do outro, mas a maioria das plataformas, como o Apache, espera que os certificados e a chave privada estejam em arquivos separados.

Formato DER

O formato DER é simplesmente uma forma binária de um certificado em vez do formato ASCII PEM. Às vezes, ele tem uma extensão de arquivo .der, mas geralmente tem uma extensão de arquivo .cer, portanto, a única maneira de diferenciar um arquivo DER .cer de um arquivo PEM .cer é abri-lo em um editor de texto e procurar as instruções BEGIN / END. Todos os tipos de certificados e chaves privadas podem ser codificados no formato DER. O DER é normalmente usado com plataformas Java. O Conversor SSL só pode converter certificados para o formato DER. Se você precisar converter uma chave privada em DER , use os comandos OpenSSL citados a seguir.

Formato PKCS # 7 / P7B

O formato PKCS # 7 ou P7B é normalmente armazenado no formato Base64 ASCII e possui uma extensão de arquivo de .p7b ou .p7c . Os certificados P7B contêm instruções "----- BEGIN PKCS7 -----" e "----- END PKCS7 -----". Um arquivo P7B contém apenas certificados e certificados de cadeia, não a chave privada. Várias plataformas suportam arquivos P7B, incluindo Microsoft Windows e Java Tomcat.

Formato PKCS # 12 / PFX

O formato PKCS # 12 ou PFX é um formato binário para armazenar o certificado do servidor, quaisquer certificados intermediários e a chave privada em um arquivo criptografável. Os arquivos PFX geralmente possuem extensões como .pfx e .p12 . Os arquivos PFX são normalmente usados em máquinas Windows para importar e exportar certificados e chaves privadas.

Ao converter um arquivo PFX para o formato PEM, o OpenSSL colocará todos os certificados e a chave privada em um único arquivo. Você precisará abrir o arquivo em um editor de texto e copiar cada certificado e chave privada (incluindo as instruções BEGIN / END) em seu próprio arquivo de texto individual e salvá-los como certificate.cer, CACert.cer e privateKey.key, respectivamente.

Convertendo manualmente o certificado

É altamente recomendável que você converta para e de arquivos .pfx em sua própria máquina usando o OpenSSL para que você possa manter a chave privada lá. Use os seguintes comandos **OpenSSL** para converter o certificado em diferentes formatos em sua própria máquina:

Converter PEM para DER

openssl x509 -outform der -in certificate.pem -out certificate.der

Converta PEM para P7B

openssl crl2pkcs7 -nocrl -certfile certificate.cer -out certificate.p7b -certfile CACert.cer

Converter PEM para PFX

openssl pkcs12 -export -out certificate.pfx -inkey privateKey.key -in certificate.crt -certfile CACert.crt

Converter DER para PEM

openssl x509 -inform der -in certificate.cer -out certificate.pem

Converter P7B para PEM

openssl pkcs7 -print_certs -in certificate.p7b -out certificate.cer

Converter P7B para PFX

openssl pkcs7 -print_certs -in certificate.p7b -out certificate.cer

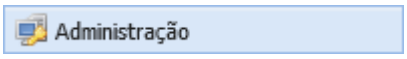
openssl pkcs12 -export -in certificate.cer -inkey privateKey.key -out certificate.pfx -certfile CACert.cer

Converter PFX para PEM

openssl pkcs12 -in certificate.pfx -out certificate.cer -nodes

Restrição de Acesso

É possível criar regras de acesso a interface gráfica do MailInspector, baseados em perfis de usuários, atrelados a IP`s e redes.



/ Administração / Ferramentas / Restrição de Acesso

Visão geral de Restrição de Acesso

Para garantia de maior segurança, o MailInspector permite ao administrador atrelar usuários/perfis de usuários a redes/IP's, dessa forma restringindo o acesso somente a redes e máquinas autorizadas.

Definições de Opções - Botões

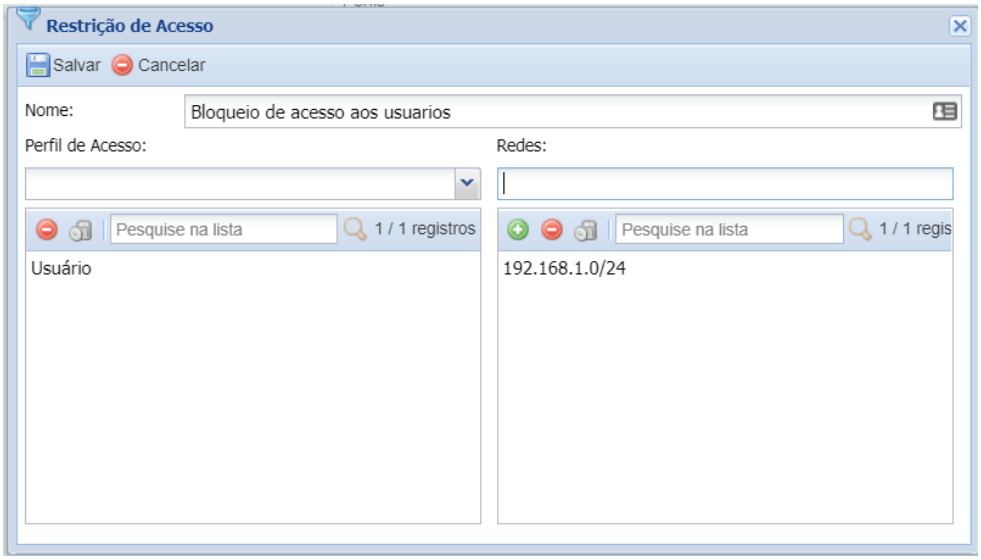
Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição
Adicionar	Adiciona nova regra de restrição de acesso
Editar	Edita a regra de restrição de acesso
Remover	Exclui regra de restrição de acesso

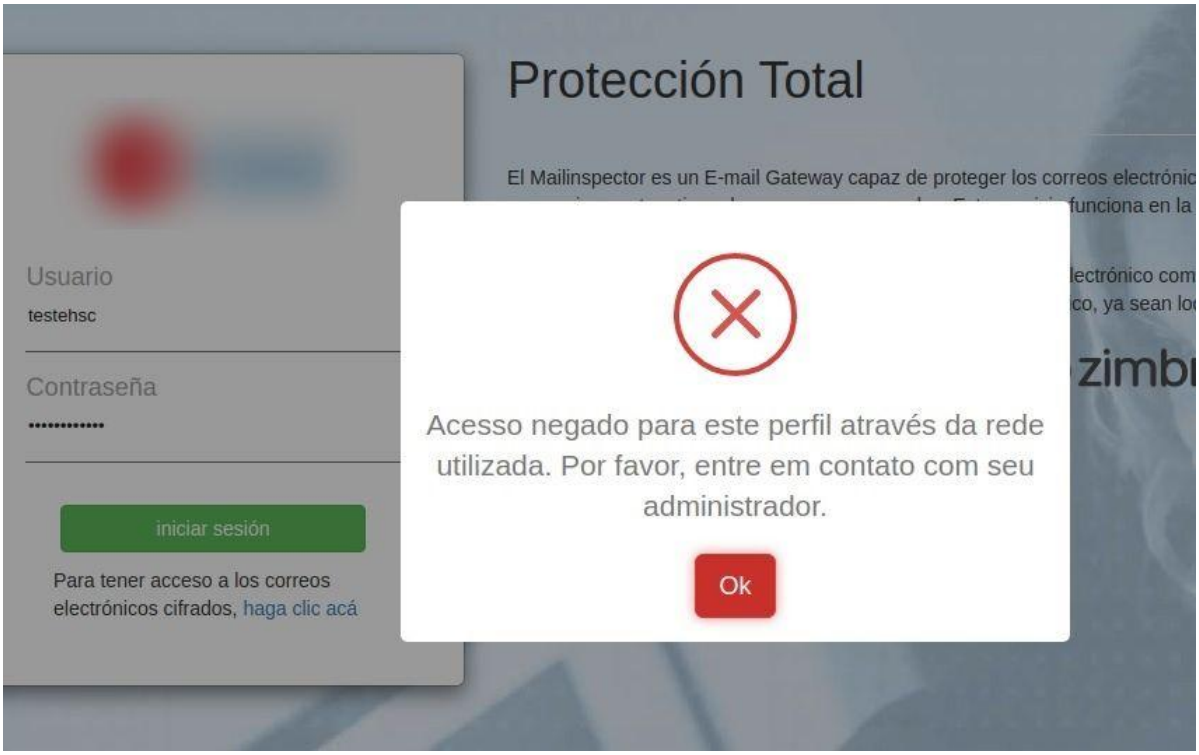
Definições de Opções

Estas informações descrevem as opções disponíveis nesta página.

Opções	Definição
Salvar	Salva a regra criada/editada
Cancelar	Ignora a criação/edição da regra de restrição de acesso
Perfil de Acesso	Selecione o perfil desejado para adição/edição da regra de restrição de acesso
Redes	Indique o Ip ou rede que possui permissão de acesso ao MailInspector



Tela de Configuração de Restrição de Acesso – No exemplo está somente os usuários que fazem parte da rede 192.168.1.0/24 que terão acesso ao MLI com perfil de Usuário.



Tela de Bloqueio por Restrição de Acesso

Branding

É possível trocar a logomarca do MailInspector para uso da logomarca da empresa desejada, bastando substituir as logomarcas do MailInspector por outra.

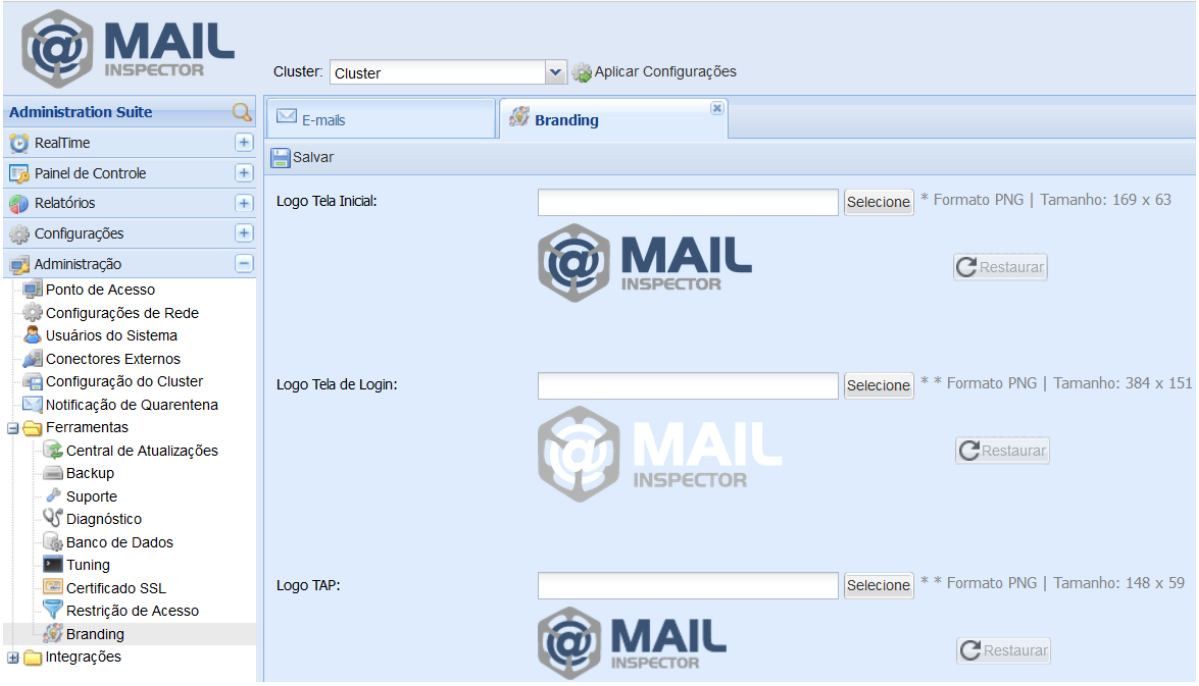
Administração **/ Administração / Ferramentas / Branding**

Visão geral de Restrição de Acesso

Caso o administrador deseje, é possível trocar a logomarca do MailInspector por outro, dessa forma, dando maior fidelidade do produto à sua empresa.

Para a troca da logomarca, basta ir em Administração > Ferramentas > Branding e trocar as logomarcas de:

- Tela Inicial
- Tela de Login
- Logomarca do modulo de Ataque Dirigido (TAP)



Tela de troca de Logomarca

Integrações

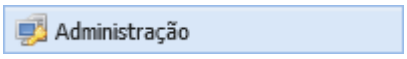
O MailInspector possui integração com alguns sistemas através de plug-ins e APIs.

Os sistemas que o MailInspector possui integração são:

- Zimbra
- Microsoft 365 (Office 365)
- G-Suite

Para maiores informações sobre integração e funcionalidades do Add-On, bem como o funcionamento do IA Cyber Assistant: https://hsclabs.com/wp-content/uploads/2025/10/Datasheet-MailInspector-integracao-providers.pdf

Visão geral de Integração com Zimbra



/ Administração / Integrações / Zimbra

A integração com o Zimbra é através de Add-On do MailInspector.

Esse Add-On é feito através de APIs, serve para que clientes de correio eletrônico como Zimbra que possam interagir com o mecanismo de aprendizagem do MailInspector diretamente da interface do Cliente de E-mail.

Nesta tela é possível efetuar o download do Add-On para ser instalado no Zimbra a fim de permitir a interação dos usuários do Zimbra com o HSC MailInspector.

O Add-On é compatível com Zimbra Versão 7.2.5 ou superior.

O Add-On irá substituir os Botões "SPAM" e "Não SPAM" tradicionais do Zimbra, tendo as mesmas funcionalidades, porém interagindo com o Servidor HSC MailInspector e adicionando o remetente automaticamente na Allow List e Block List do usuário conectado no Zimbra.

Para o funcionamento correto do Add-On o sistema de integração com LDAP deve estar ativado o modo "Cadastro Automático de usuários"

Para um melhor funcionamento do Add-On o MailInspector pode ser configurado para marcar as mensagens que forem classificadas como SPAM através da adição de um cabeçalho customizável ("X-Spam-Status: Yes").

Processo de Instalação do Add-On da HSC no Servidor Zimbra Passo a Passo:

1) Efetue o download do Zimlet da HSC através do botão "Download"

2) Acesse a interface de administração do seu servidor Zimbra.
Ex: https://ip_seu_servidor:7071

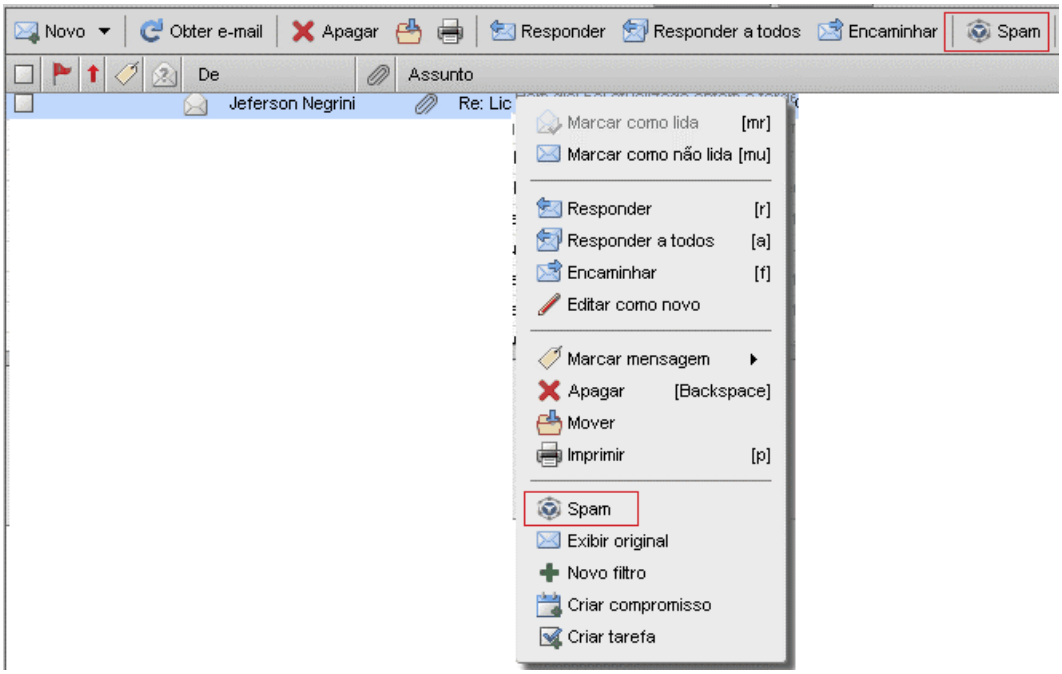
3) Acesse as configurações na opção "Zimlet".

4) Clique no botão "Distribuir". Esta opção irá instalar o Ad-On no Zimbra, para isto selecione o arquivo que você faça download e clique em "Distribuir".

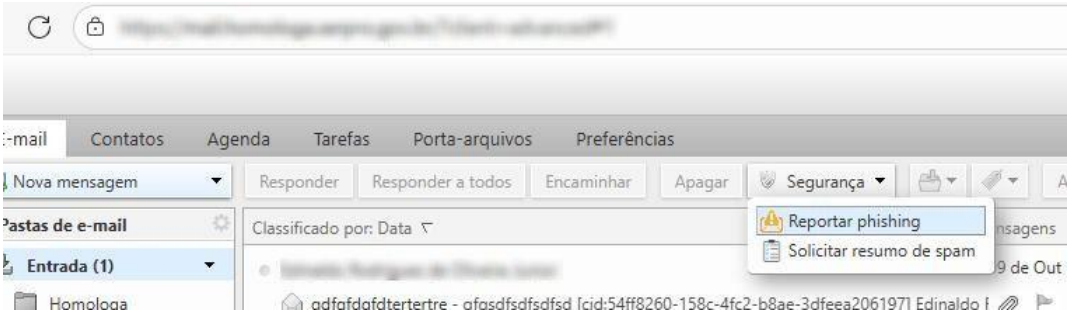
5) Certifique-se que o Zimlet está ativado para todas as "Classes de Serviço" que você deseja disponibilizar no Zimbra.

6) Reinicie o serviço do Zimbra através da console de administração Shell via SSH.
Ex: zmcontrol restart

7) Pronto. Agora o Zimlet já está disponível para os usuários e irá aparecer na interface de e-mails substituindo os botões "SPAM" e "Não Spam", por botões customizados da HSC, conforme as imagens abaixo.

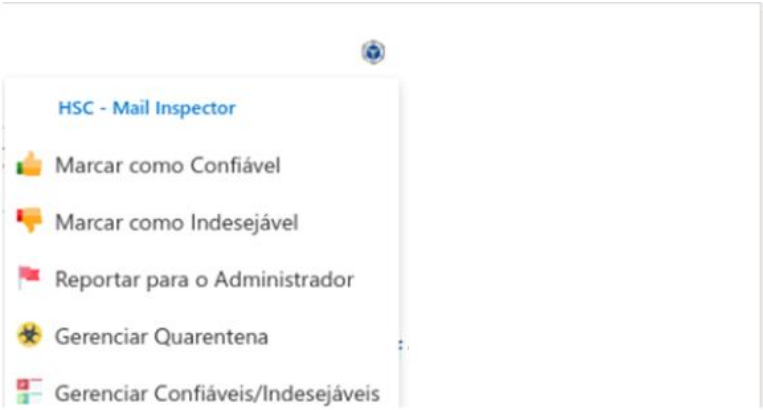


Tela do AddOn Zimbra



Solicitação de Novo Resumo de Spam e Reportar Phishing pelo Add-On Zimbra

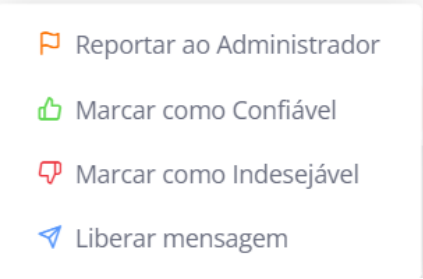
Além das funções acima descritos, ao clicar no ícone da HSCBRASIL, presente após a integração do Add-On com o Zimbra, aparecerá o menu, com as seguintes ações:



- **Marcar como Confiável:** Marca o remetente como confiável (allow list pessoal).
- **Marcar como Indesejável:** Marca o remetente como não confiável (block list pessoal).
- **Reportar para o Administrador:** Reporta o e-mail como phishing, enviando automaticamente o e-mail como amostra ao administrador e para a HSCBRASIL.
- **Gerenciar Quarentena:** Abre toda a quarentena do usuário, para ele gerenciar os e-mails quarentenados (liberar/excluir/visualizar/reportar/marcar como confiável/marcar como não confiável).
- **Gerenciar Confiáveis/Indesejáveis:** Habilita ao usuário gerenciar a lista dos que estão marcados como remetente confiável e remetente não confiável, permitindo ao usuário remover/incluir qualquer entrada nessa lista.

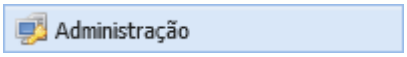
Ao selecionar a opção de **Gerenciar Quarentena**, o usuário terá acesso ao gerenciamento dos e-mails na quarentena dele, ao qual poderá efetuar as seguintes ações (por padrão):

- **Reportar ao Administrador:** Reporta ao administrador como phishing;
- **Marcar como Confiável:** Marca o remetente do e-mail como confiável, para os próximos e-mails não serem quarentenados por pontuação de SPAM;
- **Marcar como Indesejável:** Marca o remetente do e-mail como indesejável, para os próximos e-mails do remetente serem quarentenados automaticamente;
- **Liberar Mensagem:** Libera a mensagem quarentenada;



Dessa forma o MailInspector permite total integração com o Zimbra através de Add-On, permitindo ao usuário final efetuar as tomadas de decisão sobre os e-mails quarentenados e também ao administrador gerenciar quais quarentenas serão apresentadas ao usuário, bem como quais ações serão permitidas a ele.

Visão geral de Integração com Microsoft 365 (Office 365)



/ Administração / Integrações / Microsoft 365

A integração é feita por EntraID do Office365, com isso, é possível utilizar sistema de SSO (Single Sign-On) do Office365 para efetuar login no MailInspector, integrado com funcionalidade de MFA (Autenticação Multifator) do MailInspector e utilizar as políticas de senha da Microsoft como base.

A integração com Office 365 é através de API. Com a instalação da API efetuada, o administrador pode atuar diretamente no Exchange do Office 365, ou seja, o administrador atua diretamente na caixa postal do usuário, chegando até a remover um ou mais e-mails já entregues. Essa integração com o Office 365, também é conhecida como Deep Integration.

Além de integração através de ações de Deep Integration, a integração do MailInspector com Office365, permite que seja feita a autenticação no MailInspector pelas credenciais do Office365, possibilitando a autenticação através do mesmo usuário utilizado no Office365.

Uma vez integrado, é possível a importação das contas de e-mails, alias e grupos, bem como o cadastro automático dos usuários.

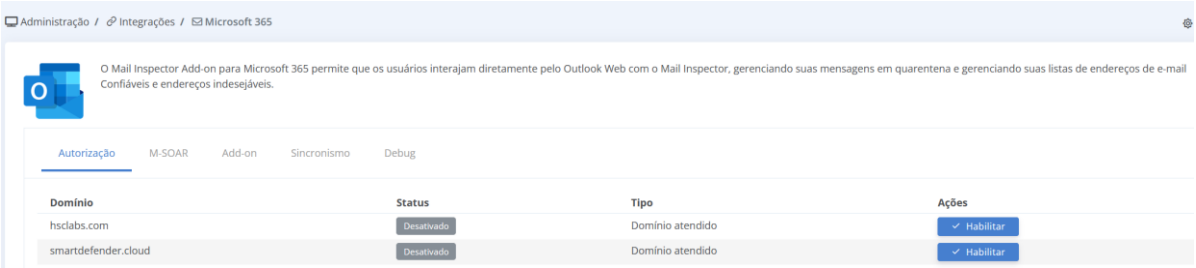
Com a Integração efetuada, será ativada a função Deep Integration, com M-SOAR. Maiores informações: *M-SOAR*

As ações de orquestração possíveis sobre o e-mail são:

- **Remover Anexo:** Remove o anexo do e-mail que já foi entregue ao Office365;
- **Remover links:** Remove todos os links contidos no corpo do e-mail;
- **Mover para o lixo eletrônico:** Move o e-mail da caixa atual, para a liceira eletrônica;
- **Bloquear Conteúdo:** Bloqueia todo o conteúdo do e-mail, impedindo que o mesmo seja visualizado pelo usuário;
- **Apagar permanentemente:** Deleta o e-mail da caixa postal do usuário;

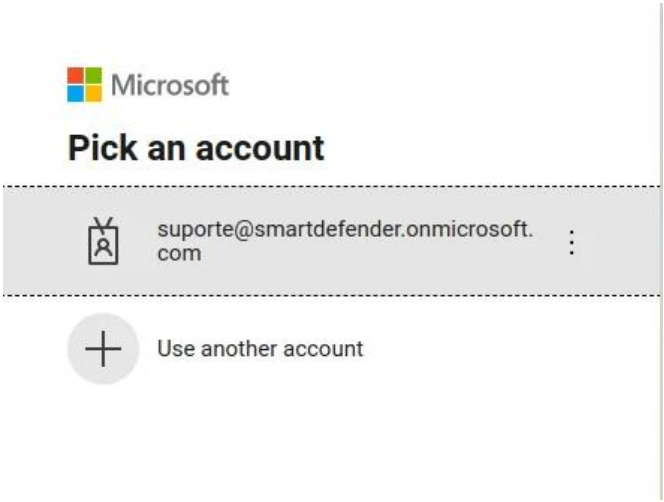
Etapas para integração com Office365

Em Integrações > Microsoft 365 clique na opção Habilitar



Aparecerá um aviso de autorização. Clique no botão Prosseguir.

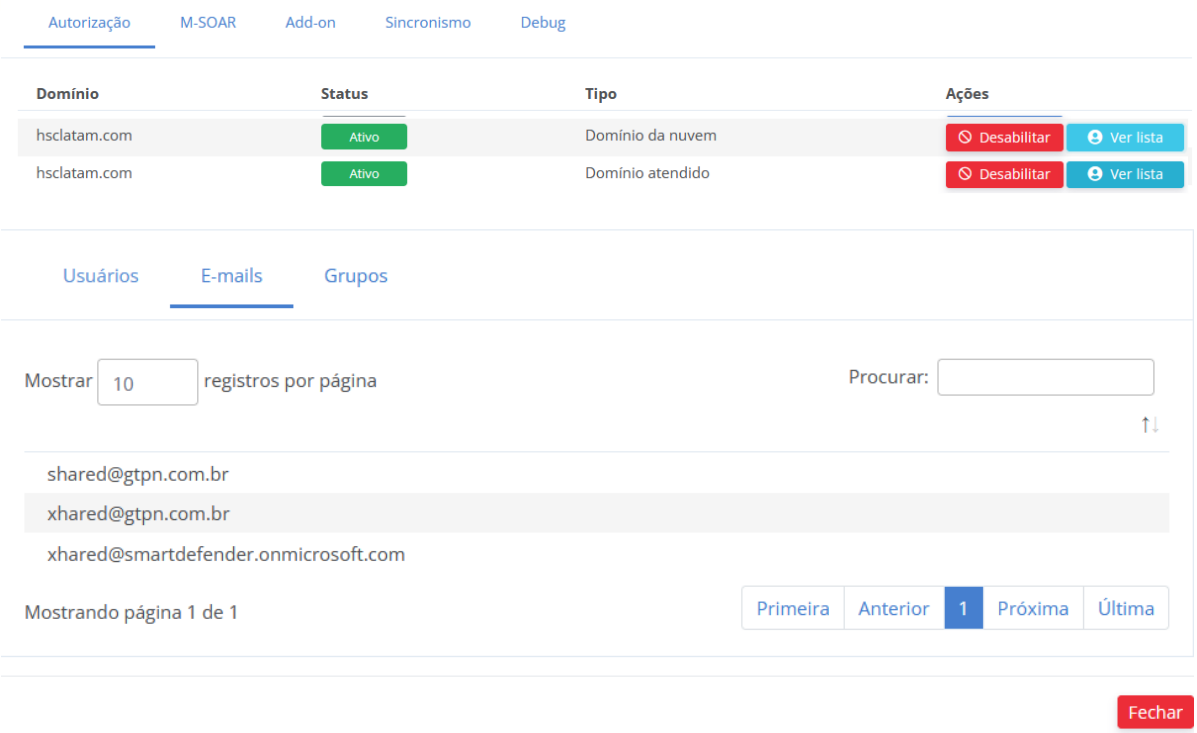
Será necessário efetuar o login com conta de usuário com permissão de administrador.



Após efetuado o login, selecione a aba Sincronismo e deixe marcado a opção Cadastro automático de usuários e Cadastro de usuários válidos no domínio. Opcionalmente é possível selecionar o item Ambiente Híbrido, caso seja necessário (geralmente é).

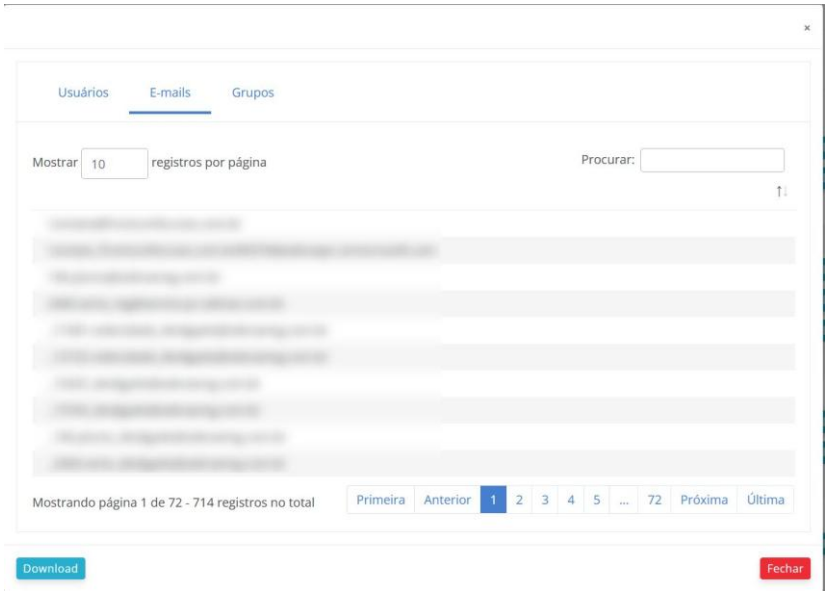
Clique no primeiro botão de sincronizar e aguarde um tempo. Depois clique no outro botão de sincronizar.

Em caso de sucesso, você poderá verificar as contas, grupos e usuários importadas, clicando em **Ver Listas (**na primeira aba - **Autorização)**.



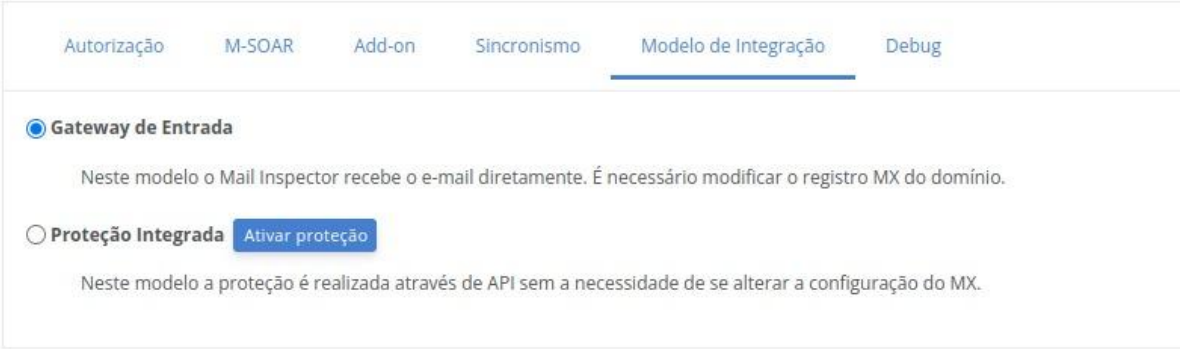
Após aberto a janela de Ver Listas, é possível visualizar os Usuários importados (na aba Usuários), lista dos e-mails importados (na aba E-mails) e grupos importados (aba Grupos).

Em todas as abas acima citados, tem o botão download, para que possa ser efetuado o download em arquivo **.CSV** das respectivas informações (Usuários importados, lista de e-mails importados ou lista de grupos importados).



A opção seguinte ao sincronismo é a escolha da forma de integração (Modelo de Integração):

- **Por Gateway de Entrada:** É o processo em que é feito o apontamento dos e-mails para o MailInspector. Esse apontamento é através de mudança do MX no DNS da empresa.
- **Proteção Integrada:** Não há a necessidade de apontar o MX no DNS da empresa, basta configurar o Office365/G-Suite para que ao receberem os e-mails, eles sejam redirecionados ao MailInspector, que os filtrarão e os devolverá ao servidor Office365/G-Suite.
  Essa configuração poderá ser de forma automática, sem necessidade de intervenção ou criação de regras por parte do administrador, somente será necessária a intervenção manual em determinados casos, como por exemplo falta de permissão do administrador para acesso automático do MailInspector sobre o Office365/G-Suite, ou falha de comunicação.



Implementação da API do Office 365

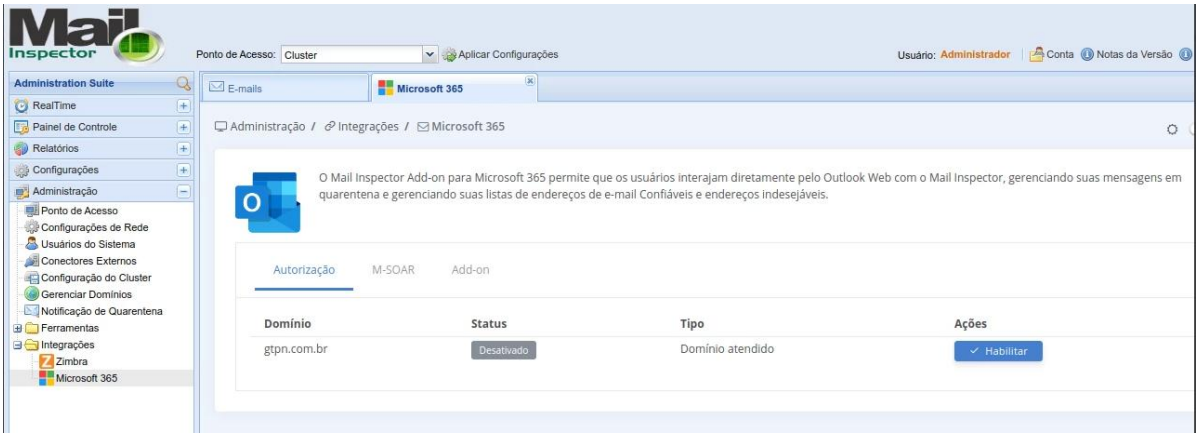
Requisitos:

1. Possuir Conta ativa no serviço Microsoft 365 em qualquer versão;
2. Possuir acesso administrativo ao Mail Inspector Enterprise Cloud;
3. Versão Mail Inspector 5.2 On Premisses ou Enterprise Cloud;
4. Possuir uma URL pública do Mail Inspector configurada com certificado SSL Válido;

Primeira Etapa

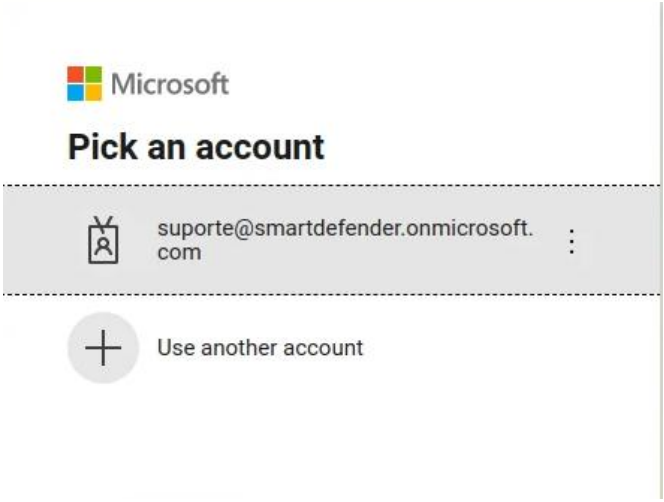
Autorização da Integração do MailInspector com seu domínio no serviço Microsoft 365

1. Acesse o MailInspector com privilégio de administrador e vá em Administração > Integrações > Microsoft 365
2. Escolha o domínio que você deseja integrar
3. Clique na opção Habilitar

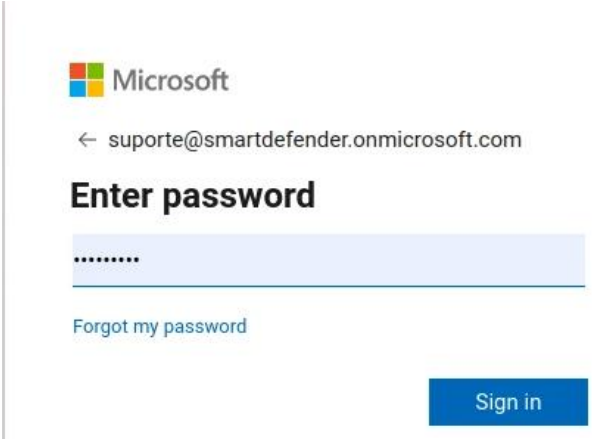


4. Será exibido uma janela para autorizar, para isso, clique em Prosseguir.

5. Na nova janela, informe as credenciais do administrador do serviço Microsoft 365.

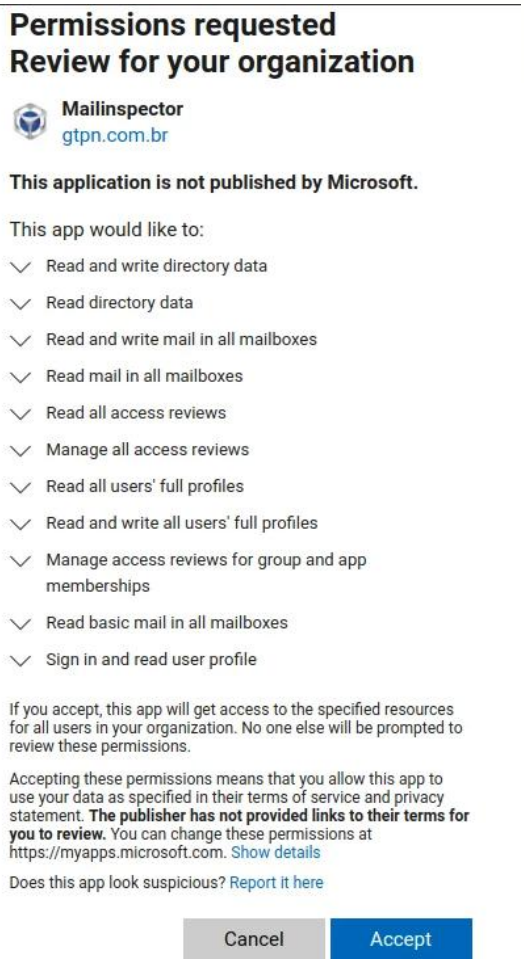


6. Informe a senha.

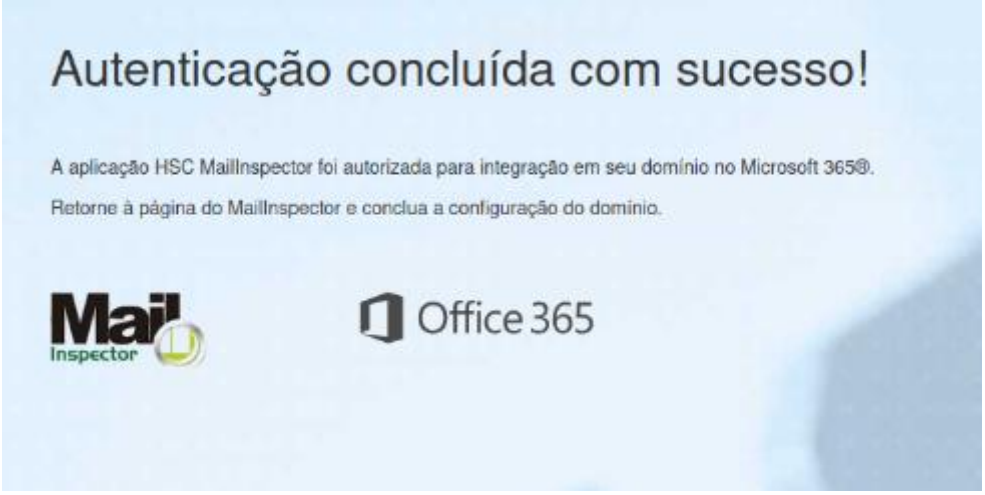


7. Na janela que abrirá, informe as credenciais do Administrador da conta Microsoft 365.

8. Confirme as permissões solicitadas



9. Em caso de sucesso será apresentada a mensagem a seguir (algo parecido):



10. Em caso de falha no acesso das credenciais fornecidas, será apresentada a mensagem: Neste caso contate o administrador da conta Microsoft 365

Segunda Etapa

Configuração do M-SOAR: corresponde a configuração das ações que o administrador poderá efetuar em tempo real na caixa de e-mail do usuário em tempo real.

1. Com suas credenciais aprovadas, clique em Sim, Configurar

2. Configure as ações permitidas aos administradores do Mail Inspector e personalize os rótulos para as ações que serão registrados nas mensagens afetadas na caixa do usuário do Microsoft 365. Ao final clique em Salvar alterações

Configurar domínio

Remoção de anexos da mensagem

Adicionar rótulo no assunto das mensagens afetadas

Texto do rótulo no assunto [Anexos removidos]

Remoção de links da mensagem

Adicionar rótulo no assunto da mensagem afetada

Texto do rótulo no assunto [Links removidos]

Adicionar rótulo no conteúdo da mensagem afetada

Texto do rótulo no assunto [Link removido]

Movimentação de mensagem para a pasta Lixo Eletrônico

Adicionar rótulo no assunto das mensagens afetadas

Texto do rótulo no assunto [Mensagem movida

Remoção permanente da mensagem

Bloqueio de conteúdo da mensagem

Adicionar rótulo no assunto das mensagens afetadas

Texto do rótulo no assunto [Conteúdo bloqueado]

Substituir o conteúdo original da mensagem por:

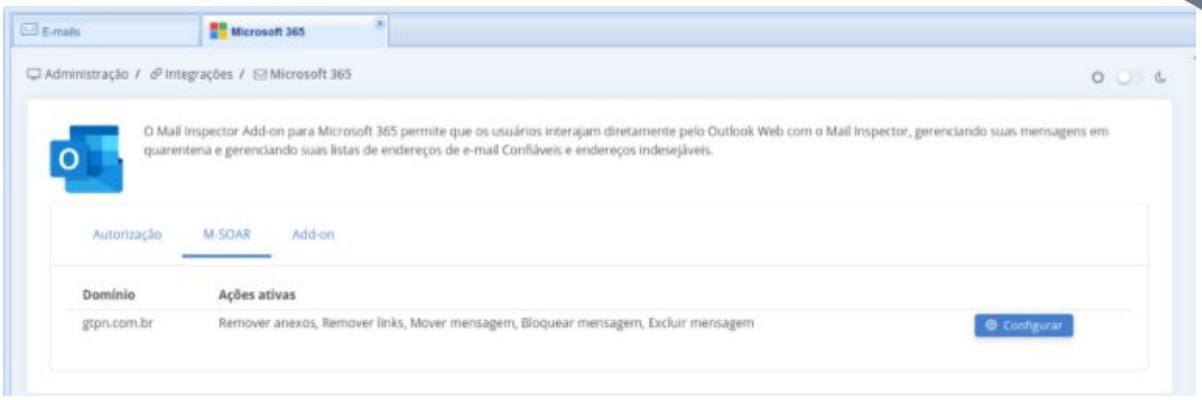
System Font 12pt

O conteúdo desta mensagem foi bloqueado pelo administrador.

P 8 WORDS

Cancelar Salvar alterações

3. Será exibido o resumo das ações ativas.



4. Pressione SALVAR e clique aba Aba Add-on, para avançar para próxima etapa.

Terceira Etapa

Configuração do Add-on: Corresponde à implementação do Add-on nas configurações do domínio no ambiente de administração do Office 365 (https://admin.microsoft.com/), o que permite ao administrador do Microsoft 365 implementar apenas para alguns usuários, grupos ou todos.

Essas funcionalidades liberadas aos usuários com o Add-On ativo, permitem ao usuário as seguintes ações sobre os e-mails (através de um botão presente no leitor de e-mail – Outlook e Outlookweb):

Nos e-mails Entregues:

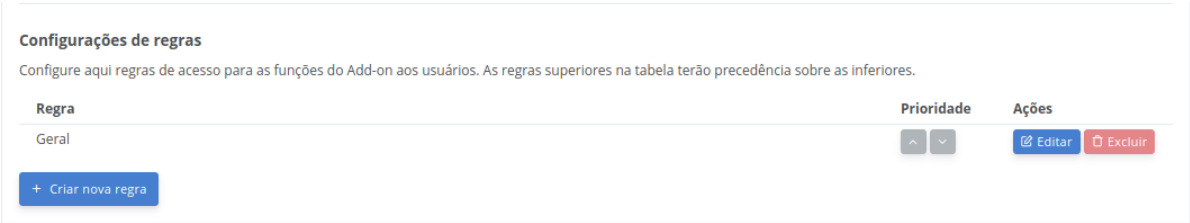
- Incluir o remetente do e-mail na sua whitelist (remetente confiável);
- Enviar ao administrador o e-mail como amostra de:
    - Phishing;
    - Vírus;
- Usar o e-mail como amostra de NÃO SPAM, para que o MailInspector possa aprimorar a sua aprendizagem nas características de e-mail limpo;

Nos e-mails Quarentenados:

- Liberar e-mail quarentenado (por ser um falso positivo);
- Permite ao usuário efetuar pesquisa e filtro dos e-mails quarentenados, através de campos específicos, como:
    - Assunto;
    - E-mail do Remetente;
- Usar o e-mail como amostra de SPAM, para que o MailInspector possa aprimorar a sua aprendizagem nas características de SPAM;
- Solicitar ao administrador a liberação de um e-mail quarentenado, cujo tipo de quarentena não permite ao usuário normal que o mesmo seja liberado (ex: quarentena de vírus);

1. Ative o Add-on no botão deslizante e informe o FDQN do seu Mail Inspector clique em salvar e em seguida em Download. Salve o aquivo XML para a Quarta etapa.

2. Configure as ações o usuario poderá executar em sua caixa de e-mail do Microsoft 365



3. Edite a regra Geral ou crie uma nova regra personalizada. Será permitido aplicar regras para um domínio ou mais dominios, Grupos LDAP, Grupos de Usuários ou Usuário.

4. Determine as ações e quarentenas que serão disponibilizadas na interface do usuário do Office 365

Ações disponíveis no menu do Add-on

- [x] Marcar como Confiável
- [x] Gerenciar Quarentena
- [x] Marcar como Indesejável
- [x] Gerenciar listas Confiáveis/Indesejáveis
- [x] Reportar ao Administrador

Quarentenas acessíveis aos usuários

Quarentenas do sistema

- [x] Todas
- [x] ATP
- [x] Blacklist
- [x] Bulk Mail
- [x] Conteúdo Adulto
- [x] Conteúdo Bloqueado
- [x] Controle de Surto/Comportamento Anômalo
- [x] DLP/Auditoria
- [x] Fraude de E-mail / E-mail Impostor
- [x] Malware
- [x] Outro Bloqueio
- [x] Phishing
- [x] Provável SPAM
- [x] SPAM
- [x] Spoofing
- [x] Tamanho Excedido
- [x] Vírus
- [x] Whitelist

Quarentenas customizadas

- [x] Todas
- [x] URL MALICIOSAS

5. Determine as ações permitidas paras mensagens em quarentena. É possível personalizar o rodapé.

Ações disponíveis aos usuários para mensagens em quarentena

- [x] Liberar mensagem
- [x] Marcar como Confiável
- [x] Reportar ao Administrador
- [x] Marcar como Indesejável

Rodapé personalizado do Add-on

Insira o código HTML para o rodapé do Add-on. Considere que o código será inserido dentro de uma DIV HTML. A largura do mesmo é de 320 pixels e sua altura máxima é de 60 pixels.

Dica: Para editar margens e padding, utilize o editor de código fonte clicando no ícone <>.

Powered by HSC HIGH SECURITY CENTER

P 2 WORDS

Simulação da área ocupada pelo rodapé

Clique em atualizar visualizaçao

Atualizar pré-visualização

Cancelar | Salvar alterações

Somente é permitido ao usuario liberar mensagens em quarentena do tipo SPAM e Provável SPAM. Não é possível liberar ameaças como vírus, malware e phishing.

Quarta Etapa (Última Etapa)

Deploy do Add-on: corresponde à implementação do Add-on nas configurações do domínio no ambiente de administração do Microsoft 365 (https://admin.microsoft.com/). Permite ao administrador do Microsoft 365 implementar apenas para alguns usuários ou grupos, conforme sua preferência.

1. Acesse o Portal de Administração do Microsoft 365 como Administrador.
2. Acesse https://admin.microsoft.com/ e navegue em Configurações > Aplicativos Integrados
   Clique em Add-ins (https://admin.microsoft.com/Adminportal/Home#/Settings/AddIns)

HSC Modo escuro

Aplicativos integrados

Descubra, adquira, gerencie e implante os aplicativos Microsoft 365 desenvolvido por parceiros da Microsoft.
Os aplicativos de linha de negócios desenvolvidos em sua própria organização não serão exibidos aqui. Para gerenciar esses aplicativos, acesse as respectivas centrais de administração ou página : Azure Active Directory | SharePoint | Teams | Add-ins

3. Em Add-ins, clique em + Implantar Suplemento

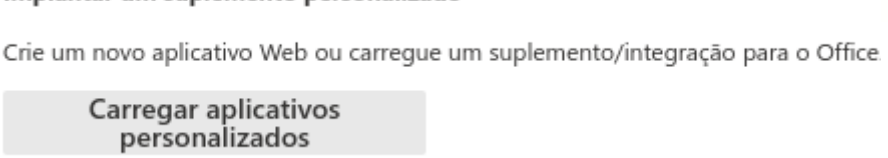
HSC

Add-ins

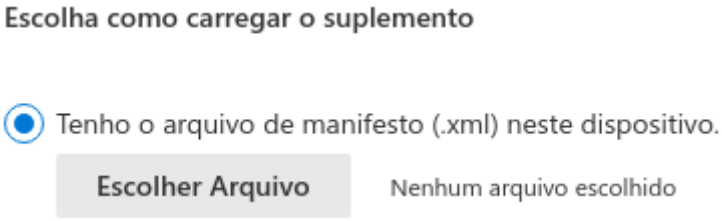
Implantar Suplemento Pesquisar

Nome ↑ Descrição

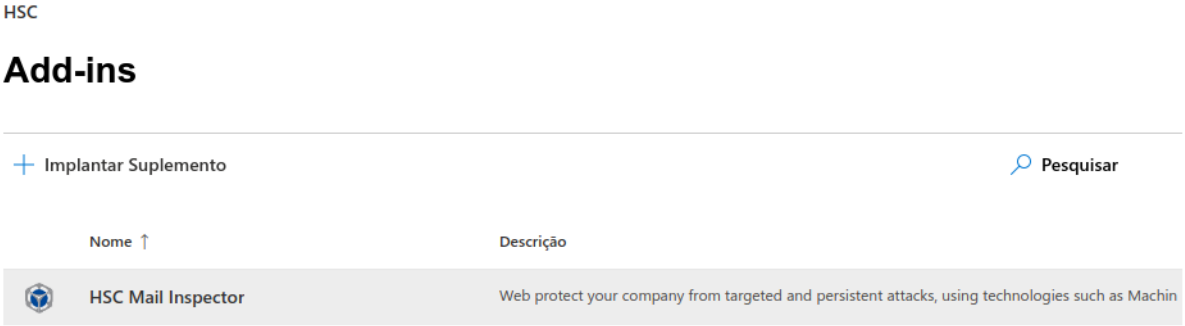
4. Na janela lateral que será apresentada, clique em PRÓXIMO e selecione Implantar um Suplemento Personalizado



5. Clique em Escolher Arquivo e selecione o arquivo .XML obtido na Terceira Etapa. Clique em CARREGAR.



Deverá exibir o Add-in conforme a seguir:



6. Selecione as opções da Implementação e IMPLANTAR

Recomendação

Para minimizar impactos aos usuários finais, recomenda-se realizar a implementação para um usuário ou grupo de usuários, e então implementar para toda a corporação.

Configurar suplemento

HSC Mail Inspector
Versão 1.0.0.0

Aplicativos de Host: Outlook

Política de Privacidade
Termos de Uso
Obter Ajuda

Web protect your company from targeted and persistent attacks, using technologies such as Machine Learningn and Behaviour Analysis

Atribuir Usuários

Escolha quais usuários terão acesso ao HSC Mail Inspector

- ○ **Todos**
- ◉ **Usuários/grupos específicos**

Procurar por usuários ou grupos específicos para adicionar ou remover

Comece a digitar um nome para pesquisar usu

s suporte ×

7. É possível permitir ao usuario gerenciar a ativação e utilização ou não. Recomenda o método Fixo (Padrão)

Método de Implantação

- ◉ **Fixo (Padrão)**

  O suplemento será implantado automaticamente para os usuários atribuídos e não será possível removê-lo da faixa de opções deles.

- ○ **Disponível**

  Os usuários podem instalar este suplemento clicando no botão obter mais suplementos na faixa de introdução inicial no Outlook e indo gerenciado pelo administrador.

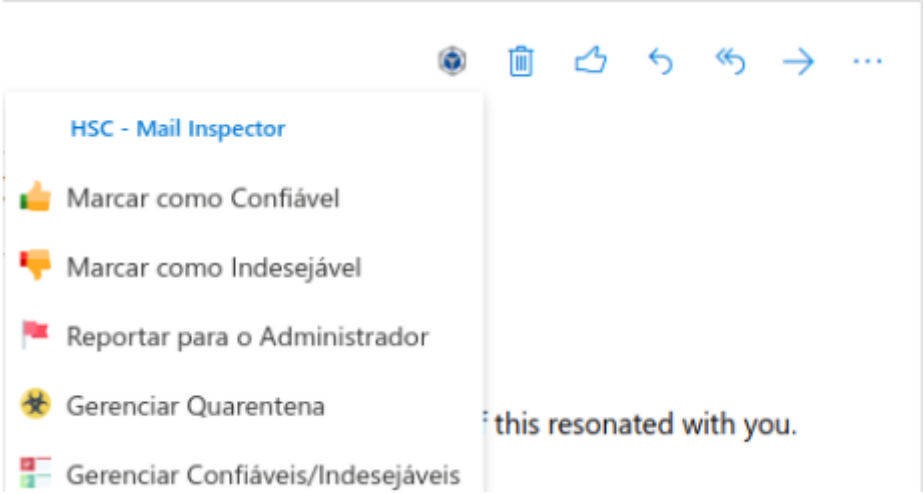
- ○ **Opcional**

  O suplemento será implantado automaticamente para os usuários atribuídos, mas eles podem optar por removê-lo da faixa de opções deles.

Atenção

É necessário aguardar 24h para disponibilizar o Add-on após sua ativação para os usuários ou grupos determinados

8. Após o período de 24h, faça logoff e login, vá ao painel de e-mails e clique no Ícone da HSC. Serão exibidas as ações a seguir:



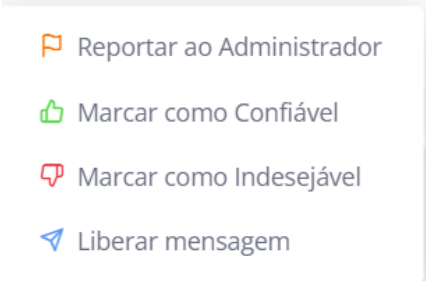
- **Marcar como Confiável:** Marca o remetente como confiável (allow list pessoal).
- **Marcar como Indesejável:** Marca o remetente como não confiável (block list pessoal).
- **Reportar para o Administrador:** Reporta o e-mail como phishing, enviando automaticamente o e-mail como amostra ao administrador e para a HSCBRASIL.
- **Gerenciar Quarentena:** Abre toda a quarentena do usuário, para ele gerenciar os e-mails quarentenados (liberar/excluir/visualizar/reportar/marcar como confiável/marcar como não confiável).
- **Gerenciar Confiáveis/Indesejáveis:** Habilita ao usuário gerenciar a lista dos que estão marcados como remetente confiável e remetente não confiável, permitindo ao usuário remover/incluir qualquer entrada nessa lista.

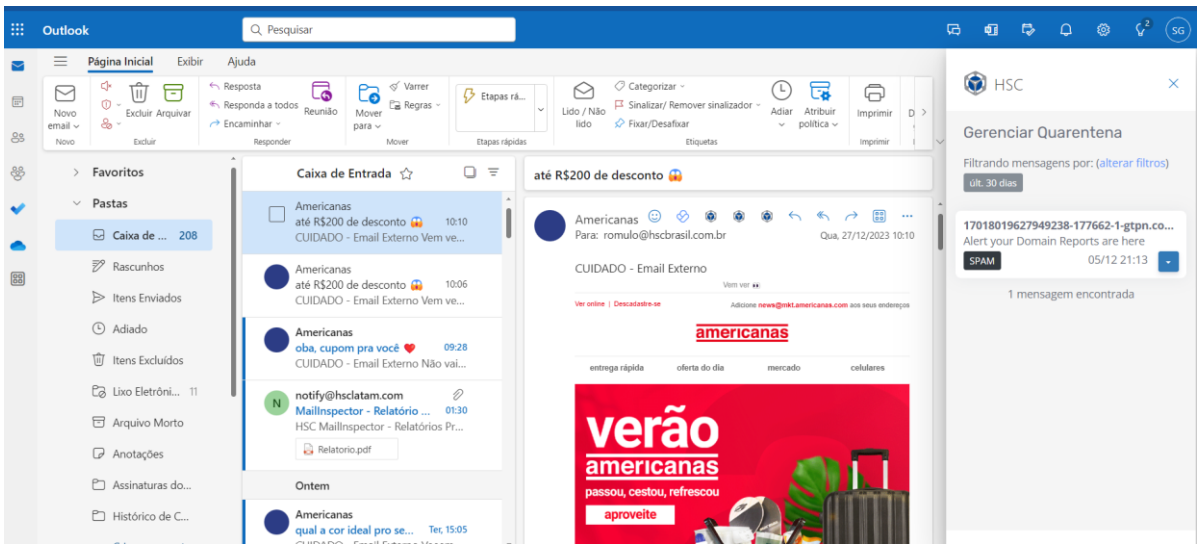
O processo de implementação descrito instala o Add-On automaticamente nos clientes de e-mail Microsoft Office 2016/2019.

Após o decorrer de 24 h, é recomendado realizar logoff e logon em suas contas para forçar o carregamento do Add-on.

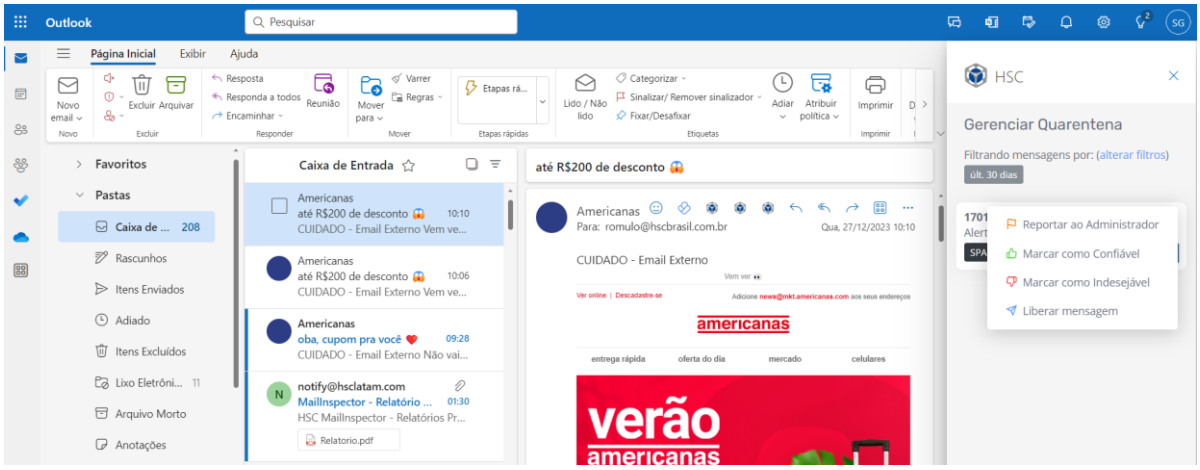
Após incluído o Add-On no Office 365, o usuário terá acesso as ações sobre os e-mails quarentenados, tais como (ao solicitar a ação de Gerenciar Quarentena):

- **Reportar ao Administrador:** Reporta ao administrador como phishing;
- **Marcar como Confiável:** Marca o remetente do e-mail como confiável, para os próximos e-mails não serem quarentenados por pontuação de SPAM;
- **Marcar como Indesejável:** Marca o remetente do e-mail como indesejável, para os próximos e-mails do remetente serem quarentenados automaticamente;
- **Liberar Mensagem:** Libera a mensagem quarentenada;



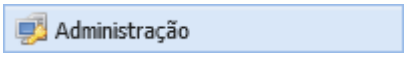


Tela de uso de Add-On no Outlook para gerenciamento de Quarentena Individual



Ações disponíveis para os e-mails quarentenados

Visão geral de Integração com Crowd Strike

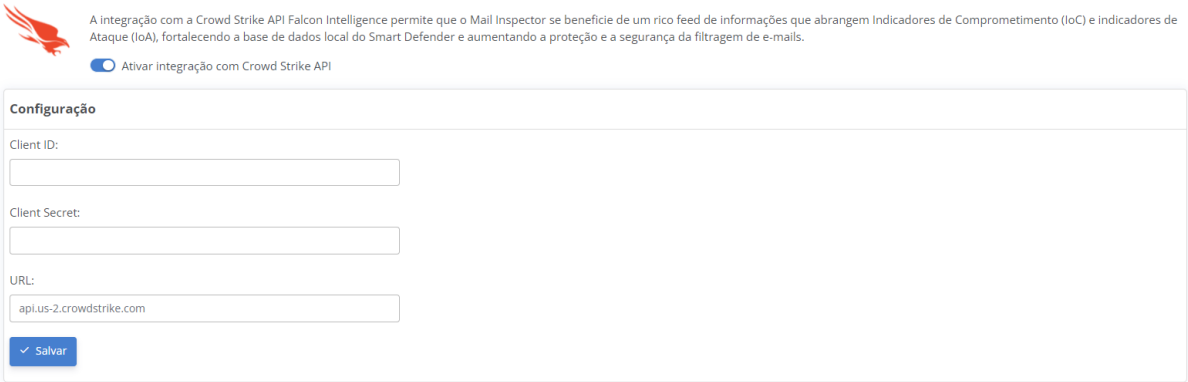


/ Administração / Integrações / Crowd Strike

A integração com a Crowd Strike API Falcon Intelligence permite que o Mail Inspector se beneficie de um rico feed de informações que abrangem Indicadores de Comprometimento (IoC) e indicadores de Ataque (IoA), fortalecendo a base de dados local do Smart Defender e aumentando a proteção e a segurança da filtragem de e-mails.

É necessário que tenha no mínimo o pacote Crowd Strike Falcon Intelligence

Ao selecionar Ativar integração com Crowd Strike API, o MailInspector libera as ações de inclusão das configurações de API Crowd Strike.

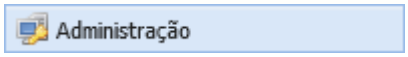


Configurações

Client ID	ID único do cliente fornecido pela Crowd Strike
Client Secret	Chave secreta da API
URL	Já vem previamente preenchida com a URL da API do Crowd Strike, mas é possível efetuar a sua edição

Após preenchido todos os campos, basta clicar em Salvar, para que as configurações sejam salvas. Após salvo, é necessário aplicar as configurações, para que as mesmas passem a ser vigente nos pontos de filtragem.

Visão geral de Integração com Google Workspace



/ Administração / Integrações / Google Workspace

A integração com Google Workspace é através de API. Com a instalação da API efetuada, o administrador pode atuar diretamente no servidor de e-mail do Google, ou seja, o administrador atua diretamente na caixa postal do usuário, chegando até a remover um ou mais e-mails já entregues.

Essa integração com o Google, também é conhecida como Deep Integration.

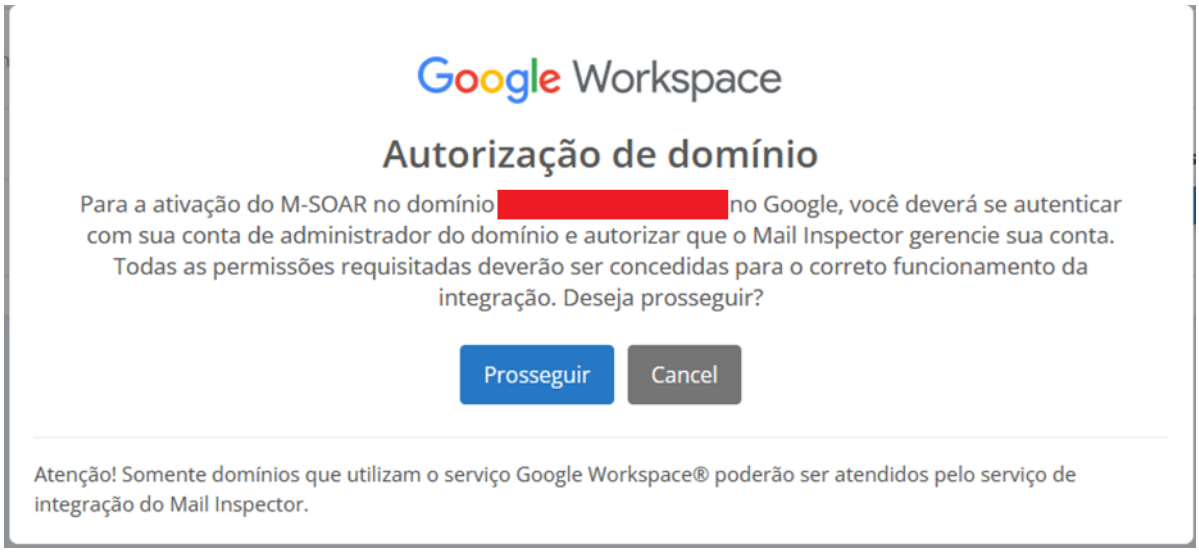
Além de integração através de ações de Deep Integration, a integração do MailInspector com Google Workspace, permite que seja feita a autenticação no MailInspector pelas credenciais do Google, possibilitando a autenticação através do mesmo usuário utilizado no Google.

Uma vez integrado, é possível a importação das contas de e-mails, alias e grupos, bem como o cadastro automático dos usuários.

Com a Integração efetuada, será ativada a função Deep Integration, com M-SOAR.

As ações de orquestração possíveis sobre o e-mail são:

- **Remover Anexo:** Remove o anexo do e-mail que já foi entregue ao servidor Google;
- **Remover links:** Remove todos os links contidos no corpo do e-mail;
- **Mover para o lixo eletrônico:** Move o e-mail da caixa atual, para a lixeira eletrônica;
- **Bloquear Conteúdo:** Bloqueia todo o conteúdo do e-mail, impedindo que o mesmo seja visualizado pelo usuário;
- **Apagar permanentemente:** Deleta o e-mail da caixa postal do usuário;



Gmail

O Mail Inspector Add-on para Google Workspace® permite que os usuários interajam diretamente pelo gMail com o Mail Inspector, gerenciando suas mensagens em quarentena e gerenciando suas listas de endereços de e-mail Confiáveis e endereços indesejáveis.

Autorização | M-SOAR | Add-on | Sincronismo | Debug

Domínio	Status	Tipo	Ações
defensoria.go.def.br	Desativado	Domínio atendido	✓ Habilitar

Visão geral de Integração com Serviços Externos STIX/TAXII

Administração / Administração / Integrações / STIX/TAXII

O HSC MailInspector oferece suporte nativo à integração com plataformas de inteligência de ameaças (Threat Intelligence) que utilizam os padrões STIX (Structured Threat Information eXpression) e TAXII (Trusted Automated eXchange of Indicator Information). Esses padrões permitem o compartilhamento estruturado, automatizado e padronizado de indicadores de comprometimento (IOCs), como endereços IP, domínios maliciosos, URLs de phishing, hashes de arquivos, entre outros. A versão compatível com serviços externos é TAXII 1.1 e STIX 1.1.1/1.2.

Como funciona a integração STIX/TAXII no MailInspector

1. Conexão ao Servidor TAXII
   O MailInspector se conecta periodicamente a um ou mais servidores TAXII externos, utilizando autenticação simples ou baseada em token, conforme configuração do provedor de Threat Intelligence. Nessa etapa, o MailInspector negocia os endpoints disponíveis, coleções e parâmetros de acesso.
2. Coleta de coleções STIX
   Uma vez estabelecida a conexão, o MailInspector consulta as **coleções STIX** disponibilizadas (collections, feeds ou channels) e identifica quais são relevantes para segurança de e-mail — como coleções de phishing, malware, botnets, command-and-control (C2), domínios recém-criados, URLs suspeitas ou campanhas direcionadas.
3. Download incremental de IOCs
   O mecanismo de ingestão realiza consultas periódicas (polling) utilizando **Timestamps** ou **versionamento TAXII**, garantindo:
   a. Ingestão incremental (somente registros novos ou atualizados);
   b. Otimização do volume de dados transferidos;
   c. Sincronização contínua com o provedor de Threat Intelligence.
4. Normalização e conversão
   Os objetos STIX 2.x recebidos (como indicator, observed-data, malware, attack-pattern, etc.) são processados e convertidos pelo MailInspector para um formato interno otimizado para decisão em tempo real.
   São extraídos apenas atributos relevantes para segurança de e-mail, incluindo:
   a. IPs maliciosos
   b. Domínios e subdomínios
   c. URLs de phishing ou C2
   d. Hashes de anexos maliciosos
   e. Padrões comportamentais
5. Atualização da base interna de reputação
   Após o processamento, todos os indicadores são integrados à base interna de reputação do MailInspector, que passa a utilizá-los imediatamente como parte do pipeline de verificação das mensagens recebidas. Isso inclui:
   a. Reputação de URLs e domínios
   b. Reputação de IPs de origem

   c. Bloqueio de anexos conhecidos maliciosos
   d. Detecção de campanhas ativas de phishing
   e. Identificação de ameaças emergentes (zero-day intelligence)

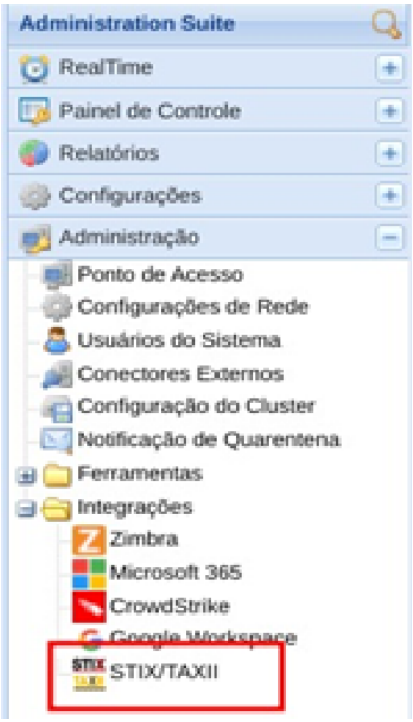
6. Aplicação em tempo real
   A cada e-mail analisado, o motor de segurança consulta sua base interna, enriquecida pelas coleções STIX/TAXII, permitindo decisões mais precisas e atualizadas:
   a. Quarentena automática
   b. Bloqueio imediato
   c. Penalização de reputação (scoring)

Benefícios da integração STIX/TAXII

- Atualização automática e contínua de indicadores de ameaça
- Redução significativa de exposição a campanhas recentes de phishing
- Aumenta a acurácia no bloqueio de ataques direcionados
- Suporte a múltiplas fontes simultâneas de Threat Intelligence
- Conformidade com padrões internacionais de cibersegurança
- Melhora o tempo de resposta e a capacidade de defesa da organização

Requisitos para habilitação

- Servidor TAXII compatível com STIX 2.0+
- Credenciais de acesso (quando exigidas)
- Configuração do endpoint no painel administrativo do MailInspector
- Agendamento da periodicidade das sincronizações



Tela de Configuração de Integrações do MailInspector – STIX/TAXII

Post-delivery Action

Realiza a reanálise contínua de e-mails já entregues, identificando ameaças, IOCs e comportamentos suspeitos que possam ter passado despercebidos pelos mecanismos tradicionais de proteção. A solução atua diretamente nos mailboxes, permitindo automatizar a resposta e a remediação, como remover, mover, isolar ou neutralizar mensagens maliciosas.

Além disso, possibilita correlação de indicadores, classificação de ameaças, aplicação de políticas de resposta e rastreabilidade das ações executadas, reduzindo o tempo entre a detecção e a contenção do incidente. Dessa forma, o Post-Delivery Action amplia a proteção do ambiente de e-mail mesmo após a mensagem ter sido entregue ao usuário.

A reanálise dos e-mails identifica ameaças com o SmartDefender e sistemas de terceiros (STIX/TAXII Servers, VirusTotal, Alien Vault, entre outros) e age diretamente nos mailboxes — removendo, movendo ou neutralizando mensagens maliciosas que passaram despercebidas.

É possível efetuar essa ação de post-delivery action de forma automatizada ou manual, de acordo com a necessidade do administrador.

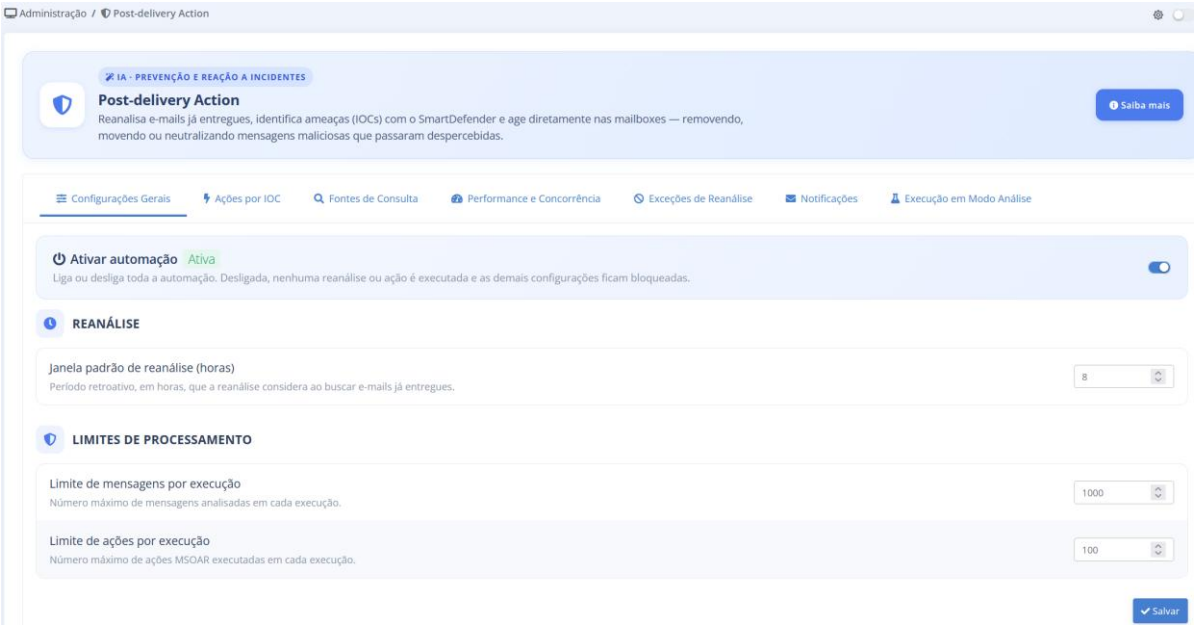
O **Post-Delivery Action** trabalha de forma integrada ao módulo **M-SOAR**, utilizando recursos de **Inteligência Artificial (IA)** para identificar ameaças e automatizar a ativação das ações de resposta e remediação. A solução permite que o M-SOAR **orquestre e execute ações diretamente sobre os e-mails já entregues**, possibilitando sua remoção, movimentação, isolamento ou neutralização de forma rápida e automatizada.

Essa integração amplia a capacidade de resposta do ambiente de segurança, reduzindo o tempo entre a **detecção, análise e contenção** de uma ameaça, inclusive quando o e-mail já chegou à caixa postal do usuário.

POR QUE ATIVAR

- Reduz o tempo de exposição a mensagens maliciosas que passaram na primeira análise.
- Reage a incidentes automaticamente, sem intervenção manual e em escala.
- Aproveita a inteligência atualizada do SmartDefender para reavaliar ameaças recentes.
- Atua diretamente na caixa do usuário (Microsoft 365, Google Workspace, Zimbra) via MSOAR.

Faz parte do mecanismo de IA de automação, prevenção e reação a incidentes do MailInspector.



Configurações Gerais

Ativação Automática: Liga ou desliga toda a automação. Desligada, nenhuma reanálise ou ação é executada e as demais configurações ficam bloqueadas.

Reanálise: Período retroativo, em horas, que a reanálise considera ao buscar e-mails já entregues.

Limites de Processamento

Limite de mensagens por execução: Número máximo de mensagens analisadas em cada execução.

Limite de ações por execução: Número máximo de ações MSOAR executadas em cada execução.

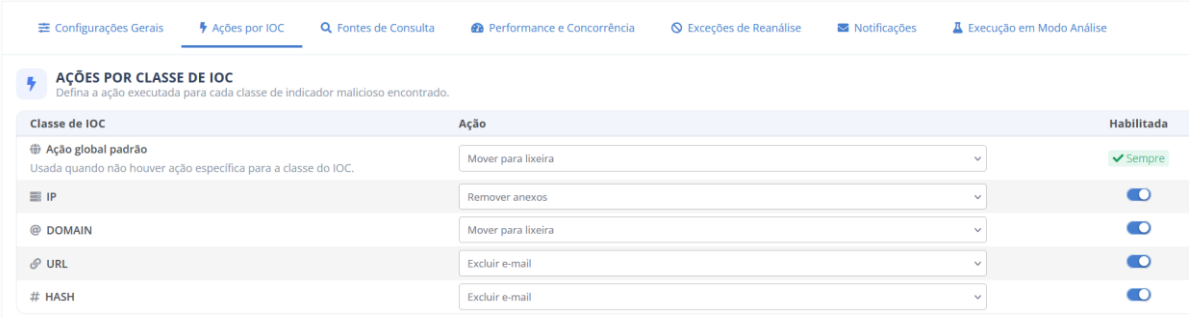
Ações por IOC

Ações por Classe de IOC: Define a ação executada para cada classe de indicador malicioso encontrado.

Opções de Ações de classe de IOC:

Classe de IOC	Ação possível	Habilitada
Ação global padrão Usada quando não houver ação específica para a classe do IOC.	• Nenhuma ação (apenas registrar) • Mover para lixeira • Excluir e-mail • Desabilitar links • Remover anexos • Bloquear conteúdo	SEMPRE
IP	• Nenhuma ação (apenas registrar) • Mover para lixeira • Excluir e-mail • Desabilitar links • Remover anexos • Bloquear conteúdo	SIM NÃO
DOMAIN	• Nenhuma ação (apenas registrar) • Mover para lixeira • Excluir e-mail • Desabilitar links • Remover anexos • Bloquear conteúdo	SIM NÃO
URL	• Nenhuma ação (apenas registrar) • Mover para lixeira • Excluir e-mail • Desabilitar links • Remover anexos • Bloquear conteúdo	SIM NÃO
HASH	• Nenhuma ação (apenas registrar) • Mover para lixeira • Excluir e-mail • Desabilitar links • Remover anexos • Bloquear conteúdo	SIM NÃO

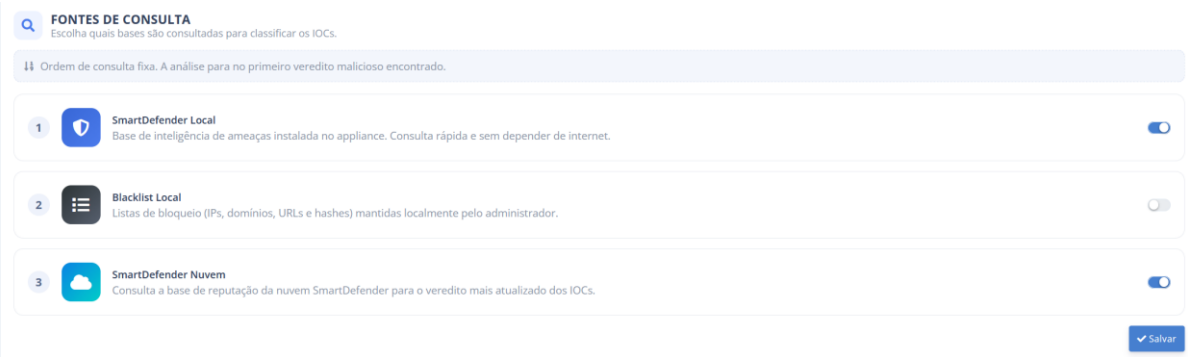
IMPACTO DAS AÇÕES DISPONÍVEIS	
Nenhuma ação (apenas registrar)	Apenas registra, sem executar ação no mailbox.
Mover para lixeira	Move a mensagem para a lixeira do usuário.
Excluir e-mail	Remove definitivamente a mensagem do mailbox.
Desabilitar links	Neutraliza/remove os links da mensagem.
Remover anexos	Remove os anexos da mensagem.
Bloquear conteúdo	Bloqueia o conteúdo da mensagem.



Fontes de Consulta

É possível escolher quais bases são consultados para a classificação das ameaças (IOCs)

1. **Smart Defender Local:** Base de inteligência de ameaças instalada no appliance. Consulta rápida e sem depender de internet.
2. **Blacklist Local:** Listas de bloqueio (IPs, domínios, URLs e hashes) mantidas localmente pelo administrador.
3. **SmartDefender Nuvem:** Consulta a base de reputação da nuvem SmartDefender para o veredito mais atualizado dos IOCs.



Performance e Concorrência

Parâmetros usados pelo script. Respeite os limites para não sobrecarregar as APIs.

Consultas Cloud

Consultas simultâneas (nuvem): Consultas simultâneas ao SmartDefender Nuvem (1 a 100).

Tempo limite por consulta (nuvem): Tempo máximo por consulta à nuvem, em segundos (1 a 300).

Novas tentativas (nuvem): Tentativas extras em caso de falha (0 a 5).

Ações M-SOAR

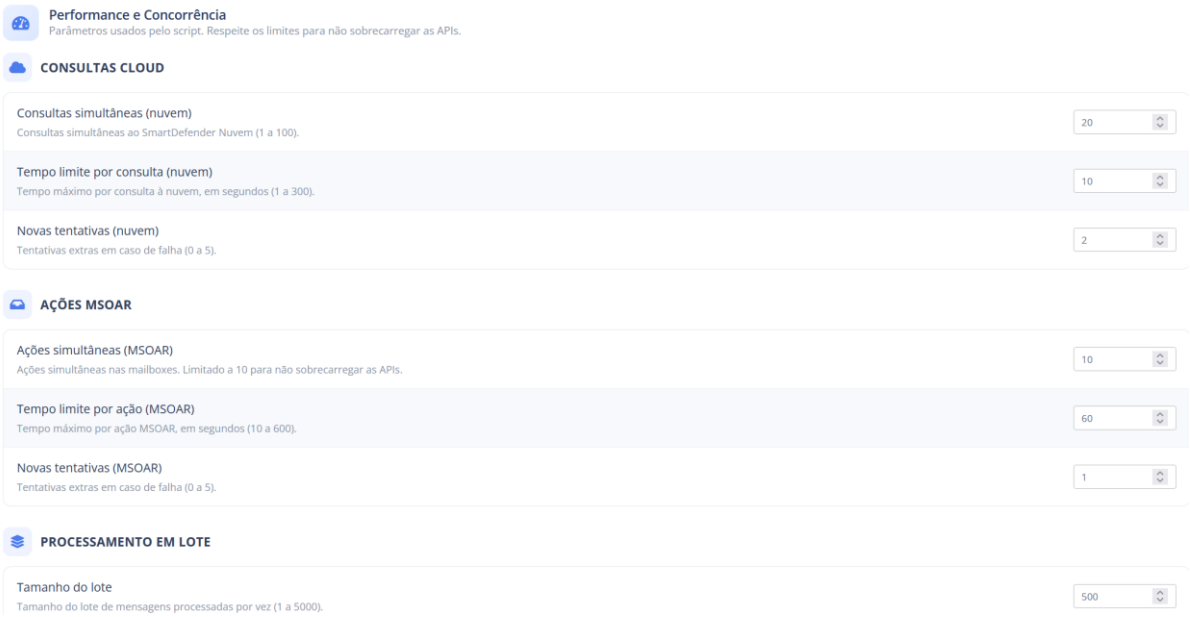
Ações simultâneas (MSOAR): Ações simultâneas nos mailboxes. Limitado a 10 para não sobrecarregar as APIs.

Tempo limite por ação (MSOAR): Tempo máximo por ação MSOAR, em segundos (10 a 600).

Novas tentativas (MSOAR): Tentativas extras em caso de falha (0 a 5).

Processamento em lote

Tamanho do lote: Tamanho do lote de mensagens processadas por vez (1 a 5000).

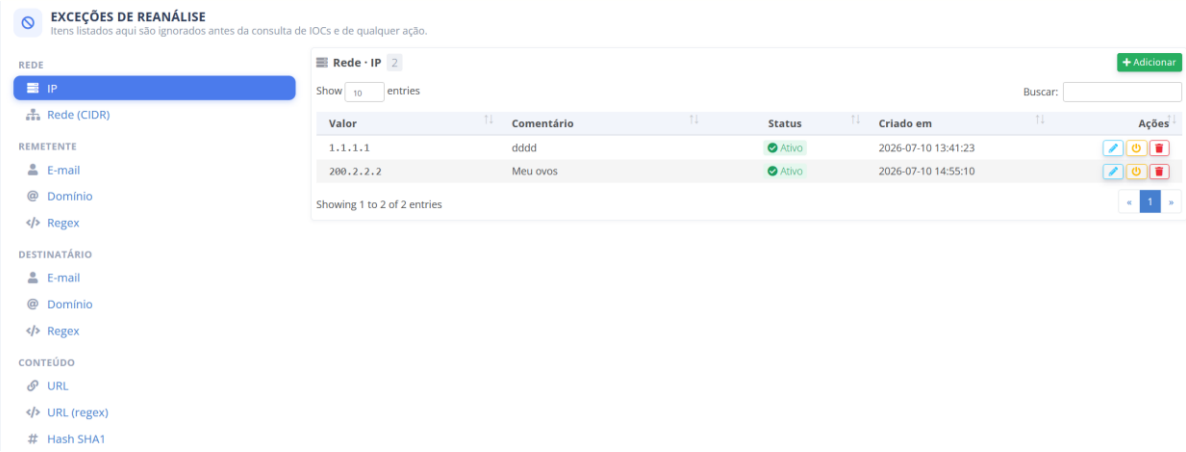


Exceções de Reanálise

Itens ignorados antes da consulta de IOCs e de qualquer ação. É possível criar exceções de reanálise para os seguintes itens:

- IP;
- Rede;
- E-mail do remetente;
- Domínio do remetente;
- RegEx do remetente;
- E-mail do destinatário;
- Domínio do destinatário;
- RegEx do destinatário;
- URL no conteúdo do e-mail;

- RegEx no conteúdo do e-mail (incluindo URLs);
- HASH (padrão SHA-1)



Notificações

Envia um resumo/alerta ao administrador após as execuções.

Quando notificar: Define em quais situações o e-mail de notificação é enviado.

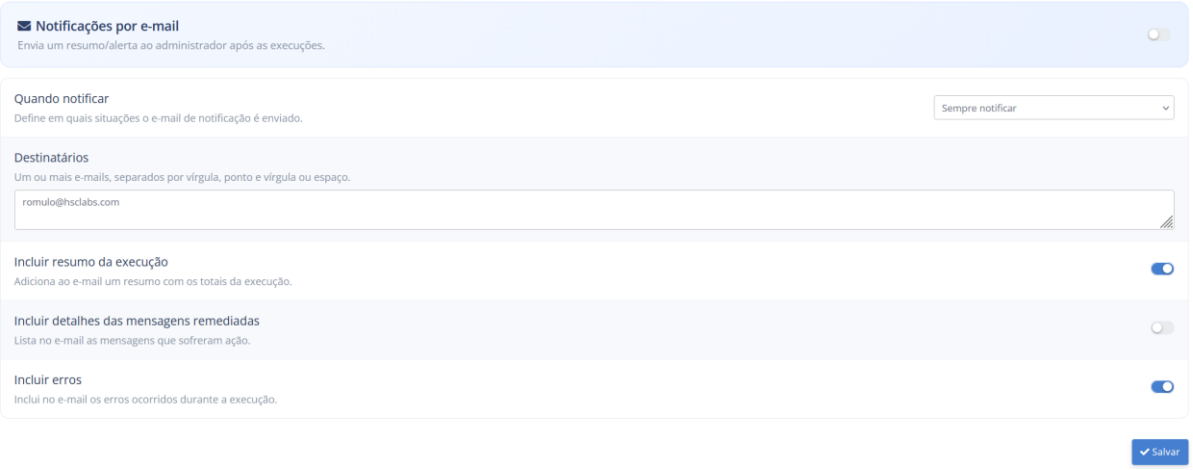
- Nunca;
- Sempre notificar;
- Apenas quando houver remediação;
- Apenas em caso de erro;
- Somente eventos críticos;

Destinatários: Um ou mais e-mails, separados por vírgula, ponto e vírgula ou espaço.

Incluir resumo da execução: Adiciona ao e-mail um resumo com os totais da execução.

Incluir detalhes das mensagens remediadas: Lista no e-mail as mensagens que sofreram ação.

Incluir erros: Inclui no e-mail os erros ocorridos durante a execução.



Execução em modo Análise

Identifica o que seria afetado, sem executar nenhuma ação real. Nenhuma ação real é executada: não move, não exclui, não altera links/anexos e não altera maillog.

Administração por Linha de Comando

Comandos via SSH (Secure Shell)

O HSC MailInspector conta com uma interface de administração por linha de comando que permite a execução de algumas tarefas administrativas diretamente em todos os appliances da solução.

O acesso é feito pelo protocolo SSH, ou seja, de forma criptografada e segura.

O superusuário (root) é de uso liberado ao cliente administrador do sistema. A sua senha é gerada durante a instalação e informada ao final do processo de instalação.

Conheça a seguir todas as opções disponíveis no menu.

A console de administração por linha de comando pode ser utilizada para suporte remotos permitindo ao administrador gerenciar o produto, criar scripts de automatização, transferência de arquivos "SCP", instalar agentes como: sistema de backup e monitoramento.

Os scripts podem ser escritos nas linguagens: Bash, Perl e PHP.

O Acesso é efetuado através do protocolo seguro SSH que pode ser ativado ou desativado conforme a necessidade do administrador através dos comandos:

Iniciar: *service sshd start*
Parar: *service sshd stop*

Configurações

O menu Configurações permite que sejam realizadas as seguintes tarefas:

Alterar configurações de rede

Altera as configurações da interface de rede do servidor, tal como: endereço IP, máscara de rede, gateway, nome do servidor e servidores DNS.

Alterar configurações DATA/HORA

Ajusta a data e hora do sistema operacional.

Serviços

O menu Serviços permite executar as seguintes ações: verificar o estado, iniciar, parar, reiniciar e recarregar as configurações do serviço selecionado. Os serviços que podem ser gerenciados são: MailInspector, Antivírus, Policyd, Greylist, MTA LOGD, Reputation, LDAP Conector.

Ferramentas

O menu Ferramentas permite que sejam realizadas as seguintes tarefas:

PING

Se você estiver com problemas de conectividade, será possível usar a opção ping para verificar o endereço IP de destino a ser alcançado. A opção ping exibe se o destino respondeu e quanto tempo demorou para receber uma resposta. Se houver um erro na remessa ao destino, será exibida uma mensagem de erro.
Você pode utilizar a opção ping para:

- Efetuar ping do seu servidor (por endereço e não por nome do host) para determinar se o TCP/IP está funcionando. (Ping do servidor não verifica se a placa de rede está funcionando.)
- Efetuar ping do roteador local para determinar se o roteador está em execução.
- Efetuar ping além de seu roteador local.

TRACEROUTE

Se você estiver com problemas de conectividade, pode utilizar a opção traceroute para verificar o caminho até o endereço IP de destino a ser alcançado. A opção tracerourte exibe a série de roteadores IP que são utilizados para entregar pacotes do seu computador no destino e quanto tempo demorou cada salto. Se os pacotes não puderem ser entregues no destino, será exibido o último roteador que encaminhou seus pacotes com sucesso.

DIG

Caso você esteja com problemas de acesso através de nomes, é possível efetuar a verificação de consulta de nome/URL's/hosts pelo comando DIG na console. Este comando é o equivalente ao NSLOOKUP da Microsoft.

Para isso, basta indicar o comando DIG, seguido da URL e por último (opcionalmente), o DNS utilizado para resolver o nome. Por exemplo:

```
# DIG www.hscbrasil.com.br 2999
hscbrasil.com.br. 2999     IN     A     68.66.216.19
```

Status

O menu Status permite que sejam realizadas as seguintes tarefas:

Uso de Memória

Exibe informações sobre a memória livre e a memória utilizada pelo sistema.

Uso CPU

Exibe informações sobre a carga da CPU no último minuto, nos últimos dez minutos e nos últimos quinze minutos.

Uso Disco

Exibe informações sobre o uso das partições do servidor. São elas: espaço total, espaço utilizado, espaço disponível, percentual de utilizado e ponto de montagem.

Estatísticas de Rede

O menu Estatísticas de Rede permite monitorar a largura de banda utilizada em todas as interfaces do servidor. Este item exibe o envio ou upload (Rx), o recebimento ou download (Tx) e o total.

Rastrear E-mail

O menu Rastrear E-mail permite acompanhar o recebimento ou envio de uma mensagem através do HSC MailInspector. Pode ser utilizado como filtro: o endereço IP do servidor remetente, o endereço de e-mail do remetente, o domínio do remetente, o endereço de e-mail do destinatário ou domínio do destinatário.

Forçar Reenvio da Fila de E-mails

O menu Forçar Reenvio da Fila de E-mails tenta entregar, novamente, todas as mensagens que ainda estão na fila do servidor.

Reiniciar/Desligar

O menu Reiniciar/Desligar permite que sejam realizadas as seguintes tarefas:

Reiniciar

Reinicia o servidor.

Desligar

Desliga o servidor.

Acesso ao Terminal

O menu Acesso ao Terminal permite ao administrador acessar o terminal do servidor para uso de comandos administrativos, todos os comandos executados são registrados no sistema.

O Acesso é completo ao Shell podendo ser utilizado pelo administrador para gerenciar e automatizar serviços. O sistema também permite instalação de softwares de terceiros para Monitoramento e agentes de Backup.

Estrutura de Diretório da Console de Administração

/opt/hsc

Serviços de Banco de Dados e Cache

/opt/hsc/common

Log do sistema de Banco de Dados

--common/log/mysqld.log

Configuração Serviço DB LOGS e Quarentena

--common/etc/my-log.cnf

Configuração Serviço DB Configurações

--common/etc/my-central.cnf

Sistema de Arquivos Banco de Dados de Configurações (existe somente em instalações da Console de Administração)

--common/db/central/

Sistema de Arquivos Banco de Dados de Quarentena, Criptografia e Logs de E-mails (existe em instalações da Console de Administração e Agentes de Filtragem)

--common/db/logs/

Sistema de Cache

--common/ssdb

Localização do MailInspector e arquivos referentes ao seu funcionamento

/opt/hsc/mailinspector

Sistema de Arquivo de armazenamento do DB da Quarentena de e-mails.

-- mailinspector/quarantine/db/mailinspector/mailfile.ibd

Localização do sistema HSC MailInspector e scripts

--mailinspector/admsuite

Localização dos Backup executados ou agendados pela interface de administração

--mailinspector/admsuite/backup

Logs de Aplicações referentes a console de administração

--mailinspector/admsuite/logs

/etc

Serviços Gerais

Sistema de Agendamento de Tarefas

/etc/crontab

Arquivos de LOG dos agentes e Console de Administração

/var/log

Arquivo de Logs de Envio, Recebimento e Filtragens de E-mails em tempo real

/var/log/maillog

Arquivo de Logs do sistema operacional HSC OS

/var/log/messages

Arquivo de Logs de Segurança do Sistema Operacional HSC OS

/var/log/secure

Arquivo de Logs do sistema de análise de segurança em tempo real da HSC SmartDefender

/var/log/hsc-smart-defender.log

Arquivo de Logs do sistema de Divisão de e-mails, para analise individual de e-mails, quando habilitada

/var/log/hscmailsplit.log

Arquivo de Logs do sistema de Logs de E-mails e Quarentena

/var/log/hsclogger.log

MIBS de Controles

Controle de Fila - Total de E-mail

OID: .1.3.6.1.4.1.41932.1.2.3.4.1
postfix_queue /opt/hsc/mailinspector/admsuite/scripts/mailqueue.sh total

Controle de Fila - Entrada de E-mail

OID: .1.3.6.1.4.1.41932.1.2.3.4.2
postfix_queue /opt/hsc/mailinspector/admsuite/scripts/mailqueue.sh incoming

Controle de Fila – Tamanho da fila de e-mails pendentes

OID: .1.3.6.1.4.1.49699.1.7

Split de E-mail

OID: .1.3.6.1.4.1.41932.1.2.3.4.3
postfix_queue /opt/hsc/mailinspector/admsuite/scripts/mailqueue.sh split

Processamento de E-mail

OID: .1.3.6.1.4.1.41932.1.2.3.4.4
postfix_queue /opt/hsc/mailinspector/admsuite/scripts/mailqueue.sh proc

E-mails Deferidos

OID: .1.3.6.1.4.1.41932.1.2.3.4.5
postfix_queue /opt/hsc/mailinspector/admsuite/scripts/mailqueue.sh deferred

E-mails classificados como SPAM

OID: .1.3.6.1.4.1.49699.1.2

E-mails com vírus detectado

OID: .1.3.6.1.4.1.49699.1.3

E-mails com phishing detectado

OID: .1.3.6.1.4.1.49699.1.4

Controle de Conexões

OID: .1.3.6.1.4.1.41932.1.2.3.4.8
postfix_connections /opt/hsc/mailinspector/admsuite/scripts/mailqueue.sh connections

Controle de Fluxo

OID: .1.3.6.1.4.1.41932.1.2.3.4.6
fluxcontrol /opt/hsc/mailinspector/admsuite/scripts/snmpd_extenal_oid.sh fluxcontrol

Limite de Cota

OID: .1.3.6.1.4.1.41932.1.2.3.4.7
fluxcontrol /opt/hsc/mailinspector/admsuite/scripts/snmpd_extenal_oid.sh quotalimit

MIBS de Hardware

Tempo de Uptime do Sistema

OID: .1.3.6.1.2.1.1.3.0

Estatísticas da Placa de Rede

List NIC names

OID: .1.3.6.1.2.1.2.2.1.2

Get Bytes IN

OID: .1.3.6.1.2.1.2.2.1.10

Get Bytes IN for NIC 4

OID: .1.3.6.1.2.1.2.2.1.10.4

Get Bytes OUT

OID: .1.3.6.1.2.1.2.2.1.16

Get Bytes OUT for NIC 4

OID: .1.3.6.1.2.1.2.2.1.16.4

Estatísticas da CPU

1 minute Load

OID: .1.3.6.1.4.1.2021.10.1.3.1

5 minute Load

OID: .1.3.6.1.4.1.2021.10.1.3.2

15 minute Load

OID: .1.3.6.1.4.1.2021.10.1.3.3

Consumo da CPU

percentage of user CPU time

OID: .1.3.6.1.4.1.49699.1.5

raw user cpu time

OID: .1.3.6.1.4.1.2021.11.50.0

percentages of system CPU time

OID: .1.3.6.1.4.1.2021.11.10.0

raw system cpu time

OID: .1.3.6.1.4.1.2021.11.52.0

percentages of idle CPU time

OID: .1.3.6.1.4.1.2021.11.11.0

raw idle cpu time

OID: .1.3.6.1.4.1.2021.11.53.0

raw nice cpu time
OID: .1.3.6.1.4.1.2021.11.51.0

Estatísticas de Memória

Total Swap Size
OID: .1.3.6.1.4.1.2021.4.3.0

Available Swap Space
OID: .1.3.6.1.4.1.2021.4.4.0

Total RAM in machine
OID: .1.3.6.1.4.1.2021.4.5.0

Total RAM used
OID: .1.3.6.1.4.1.49699.1.6

Total RAM free
OID: .1.3.6.1.4.1.2021.4.11.0

Total RAM shared
OID: .1.3.6.1.4.1.2021.4.13.0

Total RAM Buffered
OID: .1.3.6.1.4.1.2021.4.14.0

Total Cached Memory
OID: .1.3.6.1.4.1.2021.4.15.0

Estatísticas de Disco

Para habilitar as MIBs para disco, adicione a seguinte linha ao snmpd.conf (tanto nos agentes, quanto no gerenciador) e reinicie individualmente as máquinas (recomendamos não reiniciar todas ao mesmo tempo, para não haver queda do sistema de filtragem de e-mail)

includeAllDisks 10% para todas as partições e discos

Path where the disk is mounted
OID: .1.3.6.1.4.1.2021.9.1.2.1

Path of the device for the partition
OID: .1.3.6.1.4.1.2021.9.1.3.1

Total size of the disk/partion (kBytes)
OID: .1.3.6.1.4.1.2021.9.1.6.1

Available space on the disk
OID: .1.3.6.1.4.1.2021.9.1.7.1

Used space on the disk
OID: .1.3.6.1.4.1.2021.9.1.8.1

Percentage of space used on disk
OID: .1.3.6.1.4.1.2021.9.1.9.1

Percentage of inodes used on disk
OID: .1.3.6.1.4.1.2021.9.1.10.1

Scripts e Comandos

Responsável por disparar a limpeza dos Logs e Quarentena de E-mails

/opt/hsc/mailinspector/admsuite/scripts/newMliQuarentineManager.php

Responsável por disparar a limpeza da Quarentena de E-mails

/opt/hsc/mailinspector/admsuite/scripts/cleanQuarantineDB.php

Sistema de disparo de notificação de quarentena "DIGEST"

/opt/hsc/mailinspector/admsuite/scripts/mliQuarantineUserNotificationScheduler.php

Envio automatizado dos relatórios agendados pela console de Adminstração

/opt/hsc/mailinspector/admsuite/scripts/mliScheduledReports.php

Sistema de sincronização e cadastro de Usuários dos conectores Externos cadastrados na console de administração

/opt/hsc/mailinspector/admsuite/scripts/mliLdapUserSync.pl

Sistema de sincronização e cadastro de E-mails Válidos dos conectores Externos cadastrados na console de administração

/opt/hsc/mailinspector/admsuite/scripts/mliLdapUserSnapshot.pl

Scripts de Automatização de Serviços - Agentes

Executa Update das assinaturas junto a Nuvem da HSC

/opt/hsc/mailinspector/admsuite/scripts/exupdate

Sistema de Monitoramento dos Serviços de Filtragem e Recebimento de e-mails

/opt/hsc/mailinspector/admsuite/scripts/watchDog.sh

Comando para visualizar os Logs de E-mails e Filtragens em Tempo Real

/usr/sbin/tm

Monitoramento de filas com Zabbix (através dos parâmetros do usuário)

Importante lembrar que se for utilizar os MIBs do MailInspector, não utilizar o monitoramento do Zabbix simultaneamente, para não ter informações duplicadas.

O MailInspector utiliza a porta UDP 13371 para envio de informações de SNMP.

Vamos usar o recurso: “user parameter” no Zabbix para monitorar nossas filas de e-mail.

Este recurso é para quando não existe algum tipo de checagem nos templates da ferramenta, normalmente o utilizamos para executar algum comando no ponto de filtragem pelo agente do Zabbix e a resposta deste comando é enviada para o monitoramento.

Um parâmetro de usuário tem a seguinte sintaxe:

UserParameter=<chave>,<comando>

Para este exemplo, o comando que iremos executar no ponto de filtragem, e passar para o Zabbix, é o que exibe a fila de mensagens total do agente:

 # /opt/hsc/mailinspector/admsuite/scripts/mailqueue.sh total

151

Vamos editar o arquivo de configuração do Zabbix:

 # vim /etc/zabbix/zabbix_agentd.conf

No final do arquivo iremos acrescentar as informações de UserParamenter, responsáveis pelo monitoramento da fila, são elas:

UserParameter=mli.qtotal,/opt/hsc/mailinspector/admsuite/scripts/mailqueue.sh total
UserParameter=mli.qincoming,/opt/hsc/mailinspector/admsuite/scripts/mailqueue.sh incoming
UserParameter=mli.split,/opt/hsc/mailinspector/admsuite/scripts/mailqueue.sh split
UserParameter=mli.proc,/opt/hsc/mailinspector/admsuite/scripts/mailqueue.sh proc
UserParameter=mli.smtpconnections,/opt/hsc/mailinspector/admsuite/scripts/mailqueue.sh connections
UserParameter=mli.fluxcontrol,/opt/hsc/mailinspector/admsuite/scripts/snmpd_extenal_oid.sh fluxcontrol
UserParameter=mli.quotalimit,/opt/hsc/mailinspector/admsuite/scripts/snmpd_extenal_oid.sh quotalimit

Vamos pegar a primeira linha para explicar, em linhas gerais o comando:

"UserParameter=" - Indica ao agente que você vai usar um parâmetro de usuário.

"mli.qtotal=" - Nome da chave. A chave será necessária ao configurar um item. Digite uma chave de sua escolha que ser fácil de referenciar (deve ser único dentro de um host).

"/opt/hsc/mailinspector/admsuite/scripts/mailqueue.sh total" - Comando a ser executado no ponto de acesso que retornará a informação com o total da fila.

Após as devidas inserções, iremos reiniciar o agente:

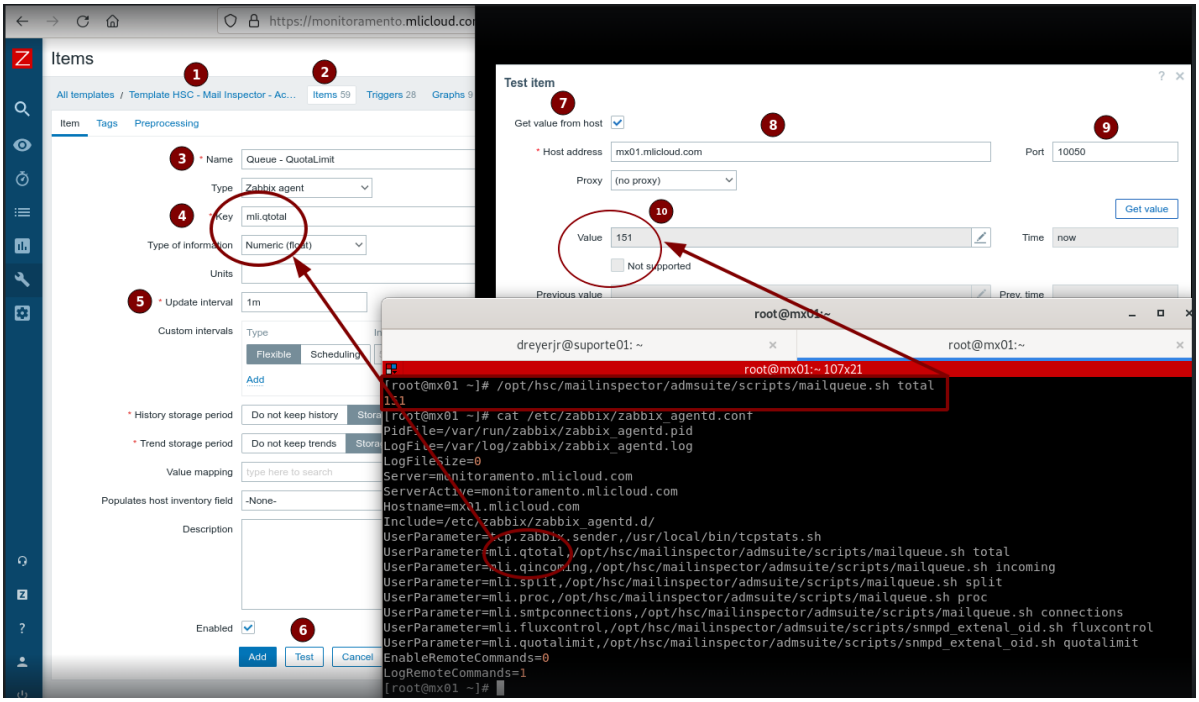
 # /etc/init.d/zabbix-agent restart

Para saber se a configuração está ok, vá até o servidor na linha de comando e digite:

root@Zabbix:~# zabbix_get -s <IPDOAGENTE> -p 10050 -k "mli.qtotal"

151

Abaixo um print com todas as configurações e, logo em seguida, sua explicação:



01 - Abrimos um template ou criamos um novo.
02 - Criamos um novo item.
03 - Nome do Item
04 - Chave, exatamente como informado no arquivo /etc/zabbix/zabbix.conf
05 - Intervalo, normalmente cinco minutos.
06 - Testando o novo item.
07 - Selecionar o campo para obtenção do dado.
08 - Informar o nome ou IP do host.

09 - Informar a porta, normalmente 10050.
10 - Clicar em "Get value", será exibido o número total de mensagens na fila.

Se vier a deparar com o erro:

Value of type "string" is not suitable for value type "Numeric (unsigned)". Value "sudo: no tty present and no askpass program specified"

Ao executar o teste, habilite, no **zabbix.conf** o parâmetro **AllowRoot=1**

Alguns monitoramentos disponíveis para o Zabbix:

- Disponibilidade e Performance da Instância do DOCKER;
- Serviço responsável pelo sistema de Filtros da Camada MTA;
- Serviço responsável pelo sistema de Controle de Fluxo e Anti DOS/DDOS;
- Serviço responsável pelo sistema de filtragem de Vírus e demais ameaças;
- Serviço responsável pelo sistema de Bounce Address Tag Verification;
- Serviço responsável pelo sistema de Cache de consultas;
- Serviço responsável pelo sistema de Armazenamento dos dados "Banco de Dados" de Logs, Relatórios e Quarentena;
- Serviço responsável pelo sistema de Data Loss Prevention;
- Serviço responsável pelo sistema de DKIM;
- Serviço responsável pelo sistema de DMARC;
- Serviço responsável pelo sistema de Console de Administração da ferramenta, Interface de Gestão para Usuário, Interface de gestão de Criptografia, Interface de Gestão de Relatórios, Interface de Gestão da Quarentena e Interface de Gestão de Pesquisas;
- Serviço responsável pelo sistema de Log;
- Serviço responsável pelo sistema de Filtragem de E-mails e seus módulos, tais como:
    - Filtro de Conteúdo;
    - Criptografia;
    - AntiSpam;
    - Anti Phishing;
- Serviço de Targeted Attack Protection;
- Sistema de MailSplit (Serviço responsável pelo sistema de Divisão de Destinatários de E-mail);
- Serviço responsável pelo sistema de Análise de Reputação de Mensagens;
- Serviço responsável pelo sistema de monitoramento SNMP;
- Serviço responsável pelo sistema de Análise de ameaças em tempo real;
- Serviço de SSH;
- Uso de CPU;
- Uso de memória;
- Uso de disco (espaço em disco);
- Status de fonte de alimentação (quando for em instalação com appliance);
- Serviço de MTA (Serviço responsável pelo sistema de Envio e Recebimento de e-mails "SMTP" e filas);
- Processamento de e-mails:
    - Número total de mensagens na fila de entrada;
    - Número total de mensagens na fila de saída;
    - Número de mensagens com erro na entrega;
    - Taxa de processamento de mensagens (mensagens/hora);
    - Número de conexões SMTP simultâneas;
- Status das atualizações de assinaturas (antivírus, antispam, sandbox);
- Data/hora da última atualização de assinaturas;
- Alertas de falha de atualização;
- Eventos de quarentena (volume utilizado, volume máximo, variação, erros);
- Ocorrências de bloqueio por listas RBL;
- Estado do cluster (ativo-ativo / ativo-passivo);
- Status da replicação de políticas entre instâncias;
- Estado do link de sincronização entre instâncias;

- Grande quantidade de erros na entrega de e-mails (erros de SMTP) ou em um determinado e-mail;

Consulte o suporte para ativação dos monitoramentos acima citados com o Zabbix.
Importante lembrar que o monitoramento pelo Zabbix, pode ser feito tanto com agente do Zabbix instalado no MailInspector, quanto com SNMP (Simple Network Management Protocol).

Alguns comandos úteis para o MailInspector

É importante ressaltar que os comandos a seguir somente podem ser efetuados pelo administrador da solução.

Visualizar log do MTA:

cat /var/log/maillog

Visualizar fila em tempo real:

tm

Limpeza de cache e restart de update:

yum clean all && yum clean metadata && yum clean dbcache && yum makecache && yum update hsc-mli*

Atualização do MailInspector via linha de comando:

yum clean all
yum update hsc-mli-*

Caso tenha alguma falha na atualização executar:

yum install yum-utils
yum-complete-transaction

Teste de conectividade com servidores HSCBRASIL:

cdcc info

Deve retornar algo parecido com:

```
dcc.hscbrasil.com.br,-      RTT-1000 ms  32768 HSC@2019lookup
#  167.114.98.132,-                                        hsc ID 1368
#     100% of  2 requests ok  168.39-1000 ms RTT         0 ms queue wait
# *167.114.128.56,-                                       hsc ID 1370
#     100% of  2 requests ok  168.32-1000 ms RTT         0 ms queue wait
```

Obs: Esse comando deve ser efetuado nos agentes.

Visualiza número de serviços rodando protocolo SMTP:

ps -eaux | grep smtp | wc –l

Para ver o IP externo da máquina:

curl ifconfig.me

```
[root@mli-admin ~]# curl ifconfig.me
200.175.93.135[root@mli-admin ~]#
```

Se não tiver instalado o comando curl, basta instalar usando o comando # yum install curl

Para ver quantos e-mails estão na fila para serem processados:

mailq

Deve retornar algo parecido com:

```
[root@srv-hsc ~]# mailq
-Queue ID- --Size-- ----Arrival Time---- -Sender/Recipient-------
1984170BCC!   49912 Mon Oct 29 10:24:19  mailbenner@gascom.com.br
                                         xml-nfe@altamogiana.com.br

0535270A46!   12961 Mon Oct 29 10:24:19  newsletter@vsmtp1.com
                                         tarcisio-zanquetta@altamogiana.com.br

-- 63 Kbytes in 2 Requests.
```

Caso queira visualizar a fila de um e-mail em específico:
mailq | grep 'monitoramento@hscbrasil.com.br' | awk '{ print $1 }' | tr -d "\!"
Onde:
monitoramento@hscbrasil.com.br é o e-mail a ser rastreado.

Inicializar VPN de suporte HSCBRASIL:

service openvpn restart

Use o comando:
ifconfig
Para ver IP estabelecido do túnel. Deve ser algo parecido com: 192.168.176.X

Para ver o arquivo de log para confirmar se a conexão com o servidor LDAP foi concluída com sucesso:

tail -f /var/log/mildapconnector.log

```
root@mail:/var/log
[root@mail log]# tail -f /var/log/mildapconnector.log
Usuario para Conexão:          uid=zimbra,cn=admins,cn=zimbra
---------------------------------------------

---------------------------------------------
Coletando Informações dos Servidores LDAP
---------------------------------------------

20/08/2015 11:59:43 Processando Servidor: 94.23.111.192
Mapa de usuarios criados com sucesso.
---------------------------------------------
```

Script de sincronização:

/opt/hsc/mailinspector/admsuite/scripts/mliLdapUserSync.pl –d
/opt/hsc/mailinspector/admsuite/scripts/mliLdapUserSnapshot.pl

Obs: Para uso do script acima, é obrigatório que tenha sido configurado o conector LDAP/AD.

Para verificar a velocidade do disco utilizado pelo MailInspector:

sudo hdparm -I /dev/sda | grep -i speed

Deve retornar algo similar a:

```
*    Gen1 signaling speed (1.5Gb/s)
*    Gen2 signaling speed (3.0Gb/s)
```

Onde a velocidade acima (na primeira linha) indica discos SATA, no caso do MLI, que na maioria das vezes é instalado em disco SAS, a valocidade deve ficar sempre em torno de 3.0 G/s (segunda linha).

ou execute o seguinte comando, que também apresenta a velocidade utilizada pelo HD:
time dd if=/dev/zero of=/opt/output conv=fdatasync bs=384k count=1k; rm -f /opt/output

Lista de Comandos Individuais

man - Mostra informações sobre um comando (exemplo: man wget)

wget - Faz o download de um arquivo (exemplo: wget http://dominio.com/arquivo.zip)

chmod - Altera as permissões de arquivos ou diretórios (exemplo: chmod 0777 pasta)

chown - Altera o dono de arquivos ou diretórios (exemplo: chown usuario:grupo pasta)

mkdir - Cria uma nova pasta

rm - Remove uma pasta ou arquivo (caso pasta, se estiver vazio)

rm -rf - Remove uma pasta e todo o seu conteúdo

cp - Copia um arquivo (exemplo: cp /pasta/arquivo.txt /pasta2/arquivo.txt)

mv - Move um arquivo (exemplo: mv/pasta/arquivo.txt /pasta2/arquivo.txt)

cd - Entra em uma pasta (exemplo: cd /home)

cd - Vai para a pasta do usuário (exemplo: /home/usuario)

cd .. - Volta 1 pasta

cd ../.. - Volta 2 pastas

pwd - Exibe o caminha ate a pasta que você esta

ls - Listar o conteúdo do diretório

ls -alh - Mostra o conteúdo detalhado do diretório

df -h - Mostra o uso de espaço em disco do sistema

du -h - Mostra a listagem dos arquivos e seu tamanho

cat - Imprime o conteudo do arquivo na shell (exemplo: cat arquivo.txt)

touch - Cria um arquivo vazio (exemplo: touch arquivo.txt);

useradd - Adiciona um usuário no sistema (exemplo: useradd usuario)

userdel - Remove um usuário do sistema (exemplo: userdel usuario)

passwd - Altera a senha do usuário (exemplo: passwd usuario)

su - Altera para outro usuário (exemplo: su usuario)

traceroute - Mostra a rota de rede ate o destino (exemplo: traceroute 192.168.1.1)

ps -aux - Mostra todos os processos no sistema

kill - Mata um processo (exemplo: kill 111)

killall - Mata vários processos (exemplo: killall nome)

top - Mostra o gerenciador de processos

vi - Editor de texto em linha de comando (Exemplo: vi arquivo.txt)

vim - Editor de texto em linha de comando (Exemplo: vim arquivo.txt)

tcpdump - Captura pacotes de rede. Usado para análise de tráfego de rede. (Exemplo: tcpdump -i eth0)

ping - Envia pacotes icmp para o destino (Exemplo: ping 8.8.8.8)

hostname – Muda o nome da máquina

Alterar Senha de Acesso

O menu Alterar Senha de Acesso permite ao administrador alterar a senha atual do usuário admin.

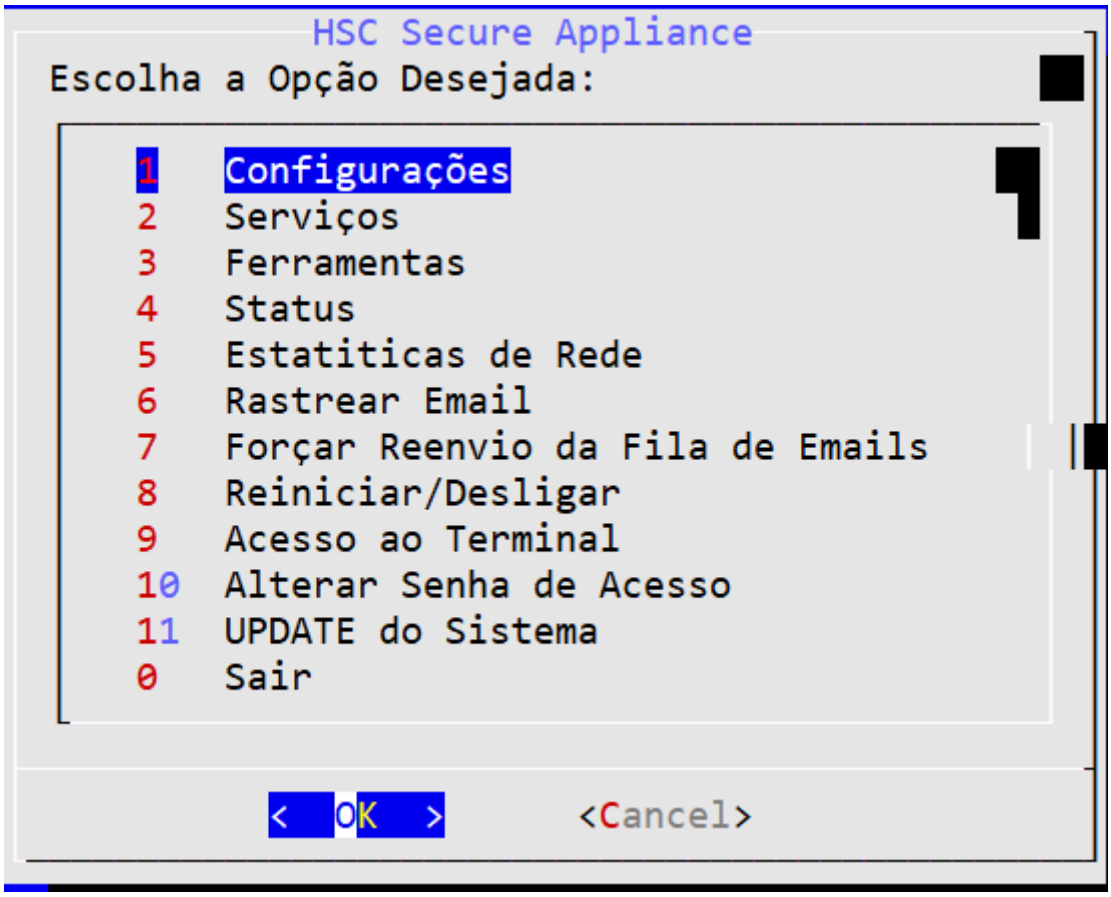
Sair

O menu Sair sai da interface de administração por linha de comando.

Acessando MLI pelo menu de configuração no SSH

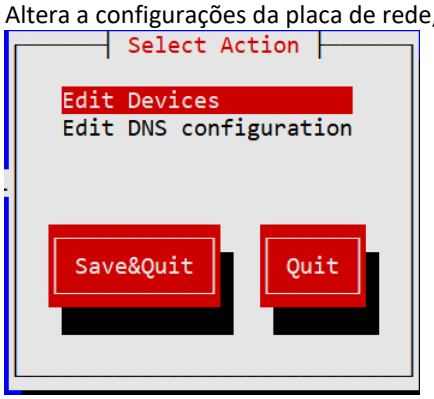
É possível acessar o MailInspector pelo menu de configuração, através do SSH, que em vez de entrar diretamente em linha de comando, ele irá abrir um menu com as principais opções de configuração do MailInspector.

Usuário de acesso: **admin**
Senha: **<Consulte a HSC para fornecimento da senha>**

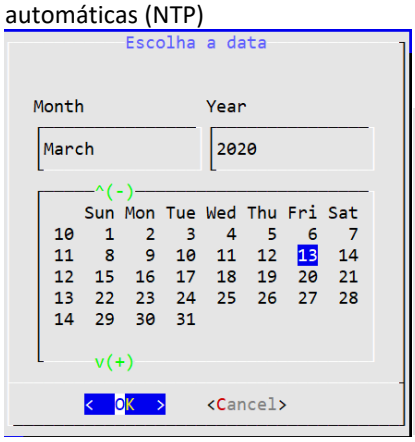


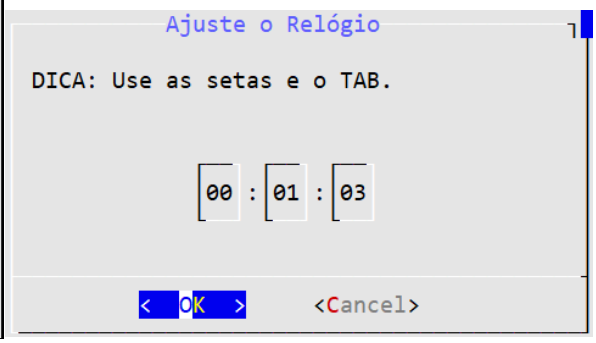
As opções disponíveis para configuração são:

1. Configurações
   a. Alterar configurações de rede
      Altera a configurações da placa de rede, tais como IP, DNS, gateway, etc.

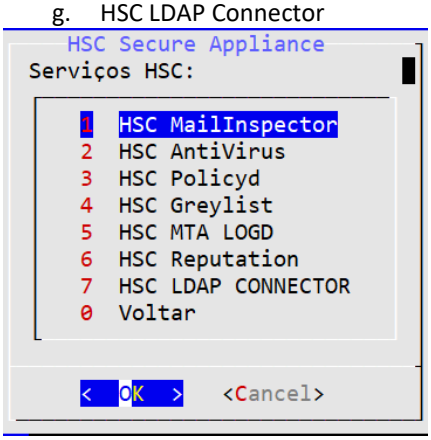


   b. Alterar configurações DATA/HORA
      Altera as configurações de data e hora manualmente, sobrepondo as configurações automáticas (NTP)

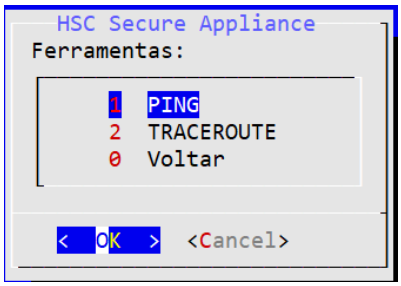




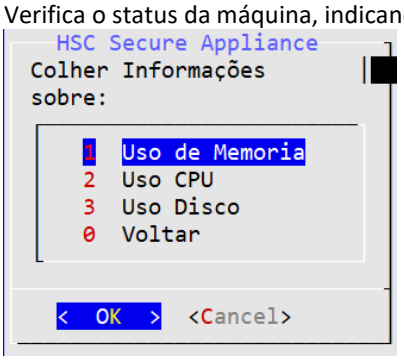
2. Serviços
   Permite a parada, reinício e verificação dos status dos serviços no MailInspector
   a. HSC MailInspector
   b. HSC Antivirus
   c. HSC Policyd
   d. HSC Greylist
   e. HSC MTA LOGD
   f. HSC Reputation
   g. HSC LDAP Connector



3. Ferramentas
   Permite o uso das principais ferramentas de rastreamento.
   a. Ping
   b. Traceroute



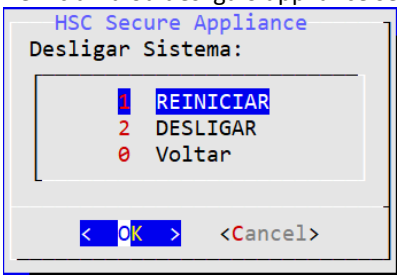
4. Status
   Verifica o status da máquina, indicando o uso de memória, uso de CPU, uso de espaço em disco.



5. Estatísticas de rede
   Indica em tempo real a quantidade de tráfego de rede

```
bwm-ng v0.5 (probing every 0.500s), press 'h' for help
input: /proc/net/dev type: rate
|       iface                   Rx                   Tx                Total
==============================================================================
          lo:           0.00 KB/s            0.00 KB/s            0.00 KB/s
        eth0:           0.23 KB/s            0.36 KB/s            0.60 KB/s
------------------------------------------------------------------------------
       total:           0.23 KB/s            0.36 KB/s            0.60 KB/s
```

6. Rastrear e-mail
   Faz a filragem dos e-mails em tempo real, bucando por um e-mail específico.
7. Forçar Reenvio da Fila de E-mail
   Reprocessa toda a fila de e-mails
8. Reiniciar/Desligar
   Reinicializa ou desliga o appliance selecionado

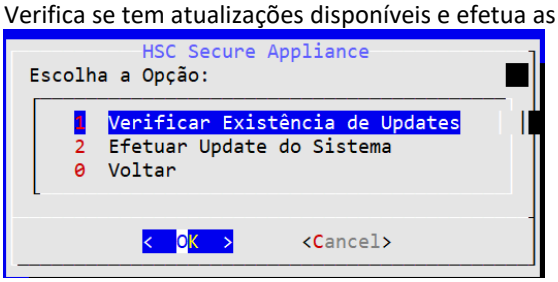


9. Acesso ao Terminal

Abre o prompt de comando do MLI, para o administrador

```
[admin@mli-admin ~]$
```

10. Alterar senha de acesso
    Altera a senha do usuário **admin**
11. Update do sistema
    Verifica se tem atualizações disponíveis e efetua as devidas atualizações



12. Sair
    Encerra a comunicação do acesso do menu de configuração

Requisitos Mínimos de Hardware

Requisitos Mínimos para Pontos de Acesso

Mensagens por Dia	Requisito mínimo de Hardware
Até 2.500	Processador: 6 VCPUs (Equivalente a Processador Intel I3) Memória: 16GB RAM Disco: 160GB
De 2.501 a 5.000	Processador: 8 VCPUs (Equivalente a Processador Intel I3) Memória: 16GB RAM Disco: 160GB
De 5.001 a 10.000	Processador: 10 VCPUs (Equivalente a Processador Intel I5) Memória: 16GB RAM Disco: 250GB
De 10.001 a 20.000	Processador: 12 VCPUs (Equivalente a Processador Intel I7) Memória: 16GB RAM Disco: 250GB
De 20.001 a 50.000	Processador: 16 VPUs (Equivalente a Processador Intel Xeon Six Core) Memória: 16GB RAM Disco: 250GB
De 50.001 a 100.000	Processador: 20 VCPUs (Equivalente a Processador Intel Xeon Octa Core) Memória: 20GB RAM Disco: 250GB
Acima de 100.001	Sob Consulta

Considerando que será somente **1 (um) ponto de acesso assumindo toda a carga**.

Em caso de cluster ativo-ativo, pode-se reduzir a configuração recomendada por ponto de acesso, de acordo com a distribuição de fluxo de e-mail (necessária consulta junto ao pessoal da engenharia da HSCBRASIL, de acordo com o desenho da solução a ser implementada).

Requisitos Mínimos para Interface de Administração

Mensagens por Dia	Requisito mínimo de Hardware
Até 2.500	Processador: 6 VCPUs (Equivalente a Processador Intel I3) Memória: 16GB RAM Disco: 250GB
De 2.501 a 5.000	Processador: 8 VCPUs (Equivalente a Processador Intel I3) Memória: 16GB RAM Disco: 360GB
De 5.001 a 10.000	Processador: 12 VCPUs (Equivalente a Processador Intel I5) Memória: 16GB RAM Disco: 360GB
De 10.001 a 20.000	Processador: 16 VCPUs (Equivalente a Processador Intel I7) Memória: 16GB RAM Disco: 500GB
De 20.001 a 50.000	Processador: 20 VPUs (Equivalente a Processador Intel Xeon Six Core) Memória: 20GB RAM Disco: 640GB
De 50.001 a 100.000	Processador: 32 VCPUs (Equivalente a Processador Intel Xeon Octa Core) Memória: 24GB RAM Disco: 1TB
Acima de 100.001	Sob Consulta

O espaço em disco sugerido suporta até 90 dias de armazenamento de quarentena, caso seja necessário o armazenamento por um período maior, é necessário adicionar espaço em disco.

Também é considerado o uso de filtragem em e-mails de ENTRADA E SAÍDA, sem ter sido considerado o uso do sistema de filtragem para e-mails INTERNOS.

Processo de Instalação em VM's

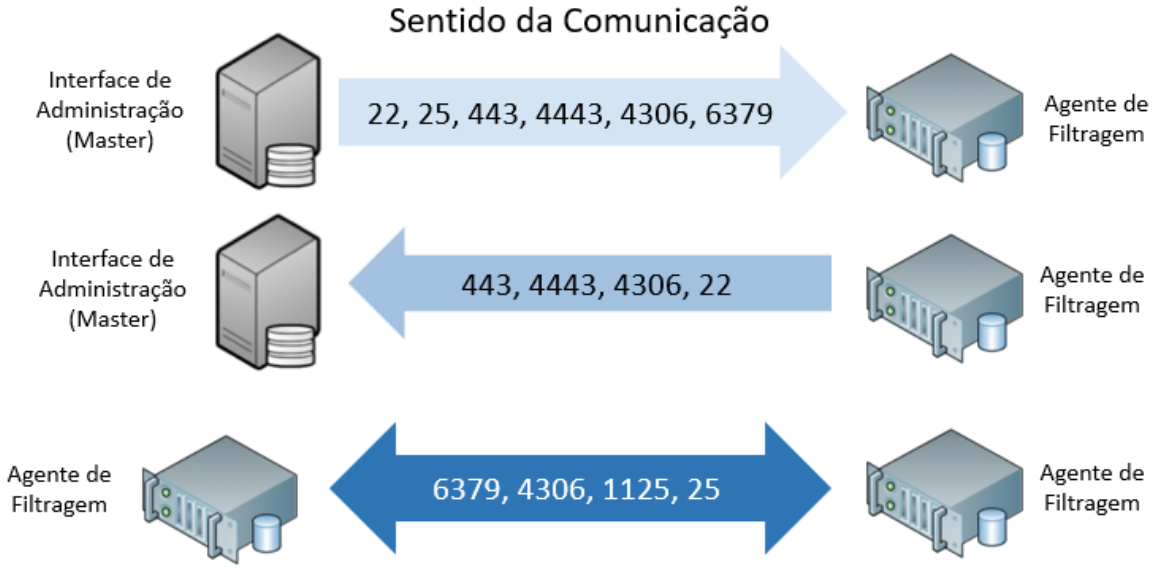
A instalação do MilInspector é extremamente simples, com Wizard auxiliando no processo, desde a configuração do IP utilizado até a atualização automática da engine e updates.

Se for utilizado o VMWare, utilize o template de Other Linux 64 bits, tanto para os agentes (agente de filtragem), quanto para o Master (Interface de Administração).

Premissas na instalação

Durante a instalação o sistema deve possuir acesso a internet nas portas **80 e 443**

Liberação de portas necessárias para o bom funcionamento da solução



Para a comunicação de entrega de e-mails do MailInspector para seu MTA (Exchange, Zimbra, SendMail, etc), é necessário deixar livre a comunicação dos agentes de filtragem e da interface de administração para porta SMTP 25/TCP.

No firewall devem ser liberados as seguintes portas e serviços de saída:

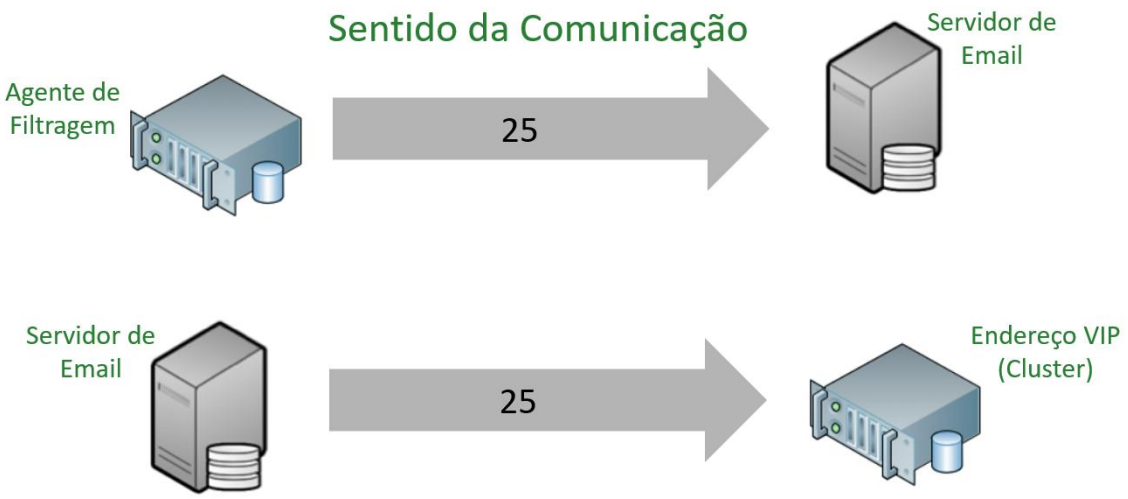
- Ponto de Acesso (Gateway de Filtragem):
  - Portas de Saída
    - 80 TCP – HTTP
    - 443 TCP – HTTPS
    - 25 TCP – SMTP
    - 465 TCP – SMTPS
    - port 6277 UDP
    - port 4306 TCP
    - port 53 TCP/UDP - DNS
  - Portas de Entrada
    - 25 TCP – SMTP

- Console de Administração:
  - Portas de Saída
    - 80 TCP – HTTP
    - 443 TCP – HTTPS
  - Porta de Entrada (se utilizar reescrita de link)
    - 80 TCP – HTTP

IMPORTANTE: É indicado que o DNS esteja corretamente configurado na empresa.

IMPORTANTE: É necessário que o DNS esteja corretamente configurado na empresa.

Comunicação entre Agentes de Filtragem ao Servidor de e-mail e Servidores de E-mail ao Cluster



Liberação de IP's e portas de comunicação

Dos agentes/ponto de acesso

Serviço: HSC SmartDefender		
TCP 80 / 443		
Hosts: app.smartdefender.cloud smartdefender.mlicloud.com smartdefender01.mlicloud.com smartdefender02.mlicloud.com smartdefender03.mlicloud.com smartdefender04.mlicloud.com smartdefender05.mlicloud.com smartdefender06.mlicloud.com smartdefender07.mlicloud.com smartdefender08.mlicloud.com support.smartdefender.cloud		
IP/Rede		**IP/Rede**
187.108.196.0/24		187.108.197.0/24
187.108.198.0/24		

Serviço: WHOIS
TCP/UDP 43
Acesso ao WHOIS, para verificação de dados de IP e domínio: **https://registro.br/tecnologia/ferramentas/whois/** **https://www.whois.com/whois/** **https://whois-2.verisign-grs.com** **O mais indicado é liberar o acesso da porta 43 sem limitação de URL, uma vez que é feita consulta a várias URLs de whois (em tabela de URL de consulta dinâmica). As URLs acima citadas são as principais.**

Serviço: HSC Message Reputation - Distributed Checksum Clearinghouses		
TCP/UDP 6277		
Hosts: dcc.hscbrasil.com.br dcc1.hscbrasil.com.br dcc2.hscbrasil.com.br		
IP/Rede		**IP/Rede**
187.108.197.76/32		187.108.197.145/32
54.156.255.136/32		192.184.137.21/32
209.168.14.29/32		209.168.14.26/32
192.135.10.194/32		69.171.29.33/32
34.102.136.180/32		212.223.15.198/32
74.92.232.243/32		209.169.14.30/32

204.90.71.235/32		136.199.199.160/32
212.223.15.198/32		209.169.14.26/32
157.131.0.46/32		

Serviço: HSC Updates		
TCP 80 / 443		
Hosts: sigs.hscbrasil.com.br portal.hscbrasil.com.br exupdate.hscbrasil.com.br exup.hscbrasil.com.br pkg.hscbrasil.com.br mirrors.hscbrasil.com.br repo.hscbrasil.com.br		
IP/Rede		**IP/Rede**
51.255.200.200/32		200.175.93.135/32
162.243.29.184/32		187.53.219.224/28
187.108.196.0/24		187.108.197.0/24
187.108.198.0/24		

Serviço: Antivírus ESET		
TCP 80 / 443		
Hosts: update.eset.com um01.eset.com um02.eset.com um03.eset.com um04.eset.com um05.eset.com um06.eset.com um07.eset.com um08.eset.com um09.eset.com um10.eset.com um11.eset.com um12.eset.com um13.eset.com um21.eset.com um23.eset.com um01.ru.eset.com um01.cn.eset.com		
IP/Rede		**IP/Rede**
91.228.166.13/32		91.228.166.14/32
91.228.166.15/32		91.228.166.16/32
91.228.167.132/32		91.228.167.133/32

38.90.226.36/32		38.90.226.37/32
38.90.226.38/32		38.90.226.39/32
91.228.166.88/32		91.228.167.170/32
38.90.226.40/32		91.228.167.26/32
91.228.167.21/32		188.225.81.21/32
119.29.72.159/32		

Da Interface de Gerenciamento E dos agentes/ponto de acesso

Outros Serviços				
Porta	**Finalidade**		**Porta**	**Finalidade**
25 TCP	SMTP (Simple Mail Transfer Protocol - Protocolo simples de envio de e-mail) - usada para envio e recebimento de e-mails.		443 TCP	HTTPS - HTTP Protocol over TLS/SSL (transmissão segura - Camada de transporte seguro). Usada para consulta de sistemas de segurança – Liberar sem restrição de IP destino e origem
53 TCP/UDP	Consulta de DNS (Domain Name System - Sistema de nome de domínio) – Sem restrição de IP de destino		80 TCP	HTTP (HyperText Transfer Protocol - Procolo de transferência de HiperTexto) - usada para updates de pacotes – Liberar sem restrição de IP destino e origem

ENTRE os agentes/ponto de acesso

Outros Serviços	
Protocolo	**Finalidade**
Protocolo **VRRP**	O **Virtual Router Redundancy Protocol (VRRP)** é um protocolo de rede de computadores que fornece atribuição automática de roteadores de Protocolo de Internet (IP) disponíveis para hosts participantes. Isso aumenta a disponibilidade e a confiabilidade dos caminhos de roteamento por meio de seleções automáticas de gateway padrão em uma sub-rede IP. No MailInspector esse protocolo é utilizado para HeartBeat entre os agentes, para verificar onde deve ficar instalado o IP VIP (no agente que estiver em funcionamento). **O número do protocolo na categoria no firewall é 112**

Da Interface de Gerenciamento

Serviço: Consulta ao SmartDefender

TCP 80 / 443		
Hosts: app.smartdefender.cloud smartdefender.mlicloud.com support.smartdefender.cloud		
IP/Rede		**IP/Rede**
187.108.196.0/24		187.108.197.0/24
187.108.198.0/24		

Monitoramento via SNMP

Caso resolva monitorar os serviços SNMP, será necessário liberar a comunicação dos agentes e console de gerenciamento com o sistema utilizado de monitoramento (por exemplo Zabbix)
UDP 13371

Da Interface de Gerenciamento ao AD/LDAP

Consulta do Conector do MailInspector ao AD/LDAP da Empresa
TCP 389, 3268, 3269, 636

Serviço: Consulta ao Microsoft Office 365		
TCP 443		
Hosts: endpoints.office.com		
IP/Rede		**IP/Rede**
23.101.16.146/32		

Obs: Importante lembrar que os IP's podem ser alterados, uma vez que muitos deles são de datacenters de fornecedores de serviços de HSCBRASIL, tais como sistemas de antivírus.

Em caso de integração com sistemas de diretório Microsoft Active Directory (AD)/Exchange/LDAP, será necessária liberação de comunicação nas portas:

- **Global Catalog: 3268 (TCP);**
- **Global Catalog por SSL/TLS: 3269 (TCP);**
- **Comunicação LDAP: 389 (TCP);**
- **Comunicação LDAP por SSL/TLS: 636 (TCP);**

Todas as portas de comunicação são oriundas da Interface de Gerenciamento ao seu servidor de diretório (AD/LDAP).

Caso utilize integração com sistemas de diretório LDAP do tipo OpenLDAP, Lotus Domino/Lotus Notes, SUN iPlanet, Sun ONE Directory Server e demais serviços de diretórios compatíveis com LDAP, será necessária

liberação de comunicação na porta 389 (TCP), comunicação oriunda da Interface de Gerenciamento ao seu servidor de diretório.

Instalação

O MailInspector possui um sistema de fácil instalação e configuração, sendo orientado passo a passo, através de Wizard, na língua portuguesa. Abaixo é indicado todo o processo de instalação.

Dicas importantes de Instalação

1. Baixe o arquivo .ISO – O endereço de download é fornecido pelo HSCBRASIL;
2. Dica: Se for utilizar máquina virtual (VMWare), não esqueça de mudar o padrão NAT de rede para bridge;
3. No caso de VMWare, utilize o template Other Linux 64 bits ou CentOS 5x 64 bits e **SEMPRE** utilizar a placa de rede **E1000;**
4. Tenha acesso ao DNS (para poder alterar o MX se necessário);
5. É preciso disco mínimo de 80GB;
6. Tenha acesso ao firewall, para liberação das portas necessárias para comunicação e também para redirecionamento da porta 25;
7. Acesso ao servidor de e-mail, para eventual criação de regra de aceite de conexão do MLI/criação de conector;
8. Na hora de configurar a rede, ative o IPv6. Não é necessário preencher o IPv6, mas para o bom funcionamento, é necessária a ativação.

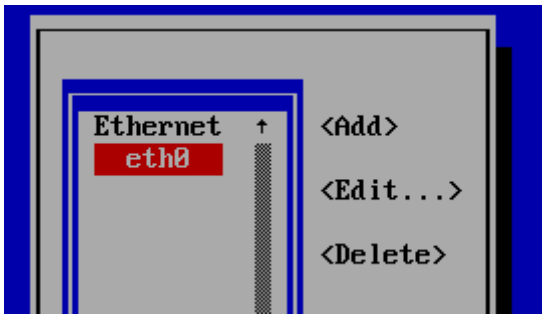
   Obs Importante: O appliance deve ter acesso a internet para poder baixar as atualizações!
   O Template utilizado deve ser:
   - **CentOS 7 64 bits ou superior;**
   - **Alma Linux 64 bits;**
   - **Rocky Linux 64 bits;**

Dê <ENTER> para inicializar o processo de instalação

```
Starting installer, one moment...
anaconda 34.25.2.10-1.el9_2.rocky.0.3 for HSC OS 6.0 started.
 * installation log files are stored in /tmp during the installation
 * shell is available on TTY2
 * if the graphical installation interface fails to start, try again with the
   inst.text bootoption to start text installation
 * when reporting a bug add logs from /tmp as separate text/plain attachments
10:20:39 Not asking for VNC because of an automated install
10:20:39 Not asking for VNC because text mode was explicitly asked for in kickstart
10:20:39 Not asking for VNC because we don't have a network
Starting automated install..Saving storage configuration...
.Checking storage configuration...
.
...
================================================================================
================================================================================
Installation

1) [x] Language settings                 2) [x] Time settings
       (English (United States))                (America/Sao_Paulo timezone)
3) [x] Installation source               4) [x] Software selection
       (Local media)                            (Minimal Install)
5) [x] Installation Destination          6) [x] Kdump
       (Custom partitioning selected)           (Kdump is disabled)
7) [x] Network configuration             8) [ ] User creation
       (Unknown)                                (No user will be created)

================================================================================
================================================================================
Progress

.
Setting up the installation environment
Configuring storage
Creating disklabel on /dev/nvme0n1
Creating lvmpv on /dev/nvme0n1p5
Creating xfs on /dev/mapper/vg02-opt
Creating lvmpv on /dev/nvme0n1p3
```

```
 _ _ _      _      ___                  _ _          ___        _
| || (_)__ _| |_   / __| ___ __ _  _ _ _(_) |_ _  _  / __|___ _ _| |_ ___ _ _
| __ | / _` | ' \  \__ \/ -_) _| || | '_| |  _| || | | (__/ -_) ' \  _/ -_) '_|
|_||_|_\__, |_||_| |___/\___\__|\_,_|_| |_|\__|\_, |  \___\___|_||_\__\___|_|
       |___/                                   |__/

To get started, please log in with the following credentials:

Username: ******
Password: ******

Once logged in, you'll be guided through the configuration process step by step.
If you encounter any issues or have questions, feel free to reach out for assistance.

hsc login: _
```

```
STEP 1) NETWORK CONFIGURATION

The first step is to configure the network settings.
Please ensure you have the necessary information at hand.

Press <ENTER> to continue... _
```



Configure o IP da máquina (na opção <Edit...>, não esqueça de incluir o Gateway e o DNS

```
                    Edit Connection

        Profile name eth0
              Device eth0 (00:0C:29:4D:66:B0)

= ETHERNET                                                  <Show>
= 802.1X SECURITY                                           <Show>

= IPv4 CONFIGURATION <Manual>                               <Show>
= IPv6 CONFIGURATION <Automatic>                            <Show>

[ ] Automatically connect
[X] Available to all users

                                                  <Cancel> <OK>
```

Mude a opção para <Manual> e clique em <Show> para editar as opções de IP

```
                    Edit Connection

        Profile name eth0
              Device eth0 (00:0C:29:4D:66:B0)

= ETHERNET                                                  <Show>
= 802.1X SECURITY                                           <Show>

v IPv4 CONFIGURATION <Manual>                               <Hide>
          Addresses 192.168.1.100          <Remove>
                    <Add...>
            Gateway 192.168.1.254
        DNS servers 8.8.8.8                <Remove>
                    <Add...>
     Search domains <Add...>

            Routing (No custom routes) <Edit...>
  [ ] Never use this network for default route
  [ ] Ignore automatically obtained routes
  [ ] Ignore automatically obtained DNS parameters

  [X] Require IPv4 addressing for this connection

= IPv6 CONFIGURATION <Automatic>                            <Show>

[X] Automatically connect
[X] Available to all users

                                                  <Cancel> <OK>
```

Configure o IP conforme o endereço disponível para o MailInspector, no exemplo foi configurado o IP como 192.168.1.100, com o Gateway 192.168.1.254 e DNS 8.8.8.8

Não esqueça de marcar as seguintes configurações:

- **Require IPv4 addressing for this connection**
- **Automatically connect**

Também é possível renomear o hostname

Ao prosseguir com a instalação, o MailInspector fará a verificação de comunicação com a internet

```
STEP 3) REPOSITORY CONFIGURATION AND PACKAGE INSTALLATION

The next step is to configure repositories and install necessary packages.

Press <ENTER> to continue...
```

A seguir o MailInspector passará a baixar os pacotes do repositório

```
Upgrade  1 Package

Total download size: 40 k
Downloading Packages:
(1/3): hsc-repos-9.5-1.7.el9.noarch.rpm                                    35 kB/s | 9.0 kB     00:00
(2/3): hsc-release-9.5-1.7.el9.noarch.rpm                                  78 kB/s |  21 kB     00:00
(3/3): rocky-gpg-keys-9.5-1.7.el9.noarch.rpm                               34 kB/s |  10 kB     00:00
--------------------------------------------------------------------------------------------------------
Total                                                                     129 kB/s |  40 kB     00:00
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction
  Preparing        :                                                                                1/1
  Upgrading        : rocky-gpg-keys-9.5-1.7.el9.noarch                                              1/6
  Installing       : hsc-repos-9.5-1.7.el9.noarch                                                   2/6
warning: /etc/yum.repos.d/hsc.repo saved as /etc/yum.repos.d/hsc.repo.rpmorig

  Installing       : hsc-release-9.5-1.7.el9.noarch                                                 3/6
  Obsoleting       : rocky-release-9.2-1.4.el9.noarch                                               4/6
  Obsoleting       : rocky-repos-9.2-1.4.el9.noarch                                                 5/6
  Cleanup          : rocky-gpg-keys-9.2-1.4.el9.noarch                                              6/6
  Running scriptlet: rocky-gpg-keys-9.2-1.4.el9.noarch                                              6/6
[ 1288.614515] systemd-rc-local-generator[8941]: /etc/rc.d/rc.local is not marked executable, skipping.
  Verifying        : hsc-release-9.5-1.7.el9.noarch                                                 1/6
  Verifying        : rocky-release-9.2-1.4.el9.noarch                                               2/6
  Verifying        : hsc-repos-9.5-1.7.el9.noarch                                                   3/6
  Verifying        : rocky-repos-9.2-1.4.el9.noarch                                                 4/6
  Verifying        : rocky-gpg-keys-9.5-1.7.el9.noarch                                              5/6
  Verifying        : rocky-gpg-keys-9.2-1.4.el9.noarch                                              6/6

Upgraded:
  rocky-gpg-keys-9.5-1.7.el9.noarch
Installed:
  hsc-release-9.5-1.7.el9.noarch                                    hsc-repos-9.5-1.7.el9.noarch
```

Instalação de pacotes do repositório

```
  vim-enhanced-2:8.2.2637-20.el9_1.x86_64                    vim-filesystem-2:8.2.2637-20.el9_1.noarch
  webkit2gtk3-jsc-2.46.1-2.el9_4.x86_64                      webrtc-audio-processing-0.3.1-8.el9.x86_64
  wget-1.21.1-8.el9_4.x86_64                                 wireplumber-0.4.14-1.el9.0.1.x86_64
  wireplumber-libs-0.4.14-1.el9.0.1.x86_64                   xdg-desktop-portal-1.12.6-1.el9.x86_64
  xdg-desktop-portal-gtk-1.12.0-3.el9.x86_64                 xkeyboard-config-2.33-2.el9.noarch
  xml-common-0.6.3-58.el9.noarch                             xorg-x11-fonts-ISO8859-1-100dpi-7.5-33.el9.noarch
  xorg-x11-server-utils-7.7-44.el9.x86_64                    yum-utils-4.3.0-13.el9.noarch
  yyjson-0.10.0-1.el9.x86_64

Complete!
 Press <ENTER> to continue...
```

Ao finalizar essa etapa, será solicitado o <ENTER> para continuar

```
STEP 4) PRODUCT SELECTION

Choose the product you want to install:

> 1. MailInspector (Administration Suite)
> 2. MailInspector (Access Point)
> 3. MailInspector (Administration Suite + Access Point)
> 4. None - Install only the HSC OS without any product

Enter the number corresponding to your choice and press Enter [1-4]:
```

Após finalizada a etapa de instalação dos pacotes iniciais, será solicitado a escolha das opções de qual produto a ser instalado:

1. Console de Administração;
2. Ponto de Acesso;
3. Console de Administração com o ponto de acesso em um único ambiente;
4. Instalação somente do HSC OS

```
STEP 4) PRODUCT SELECTION

Choose the product you want to install:

> 1. MailInspector (Administration Suite)
> 2. MailInspector (Access Point)
> 3. MailInspector (Administration Suite + Access Point)
> 4. None - Install only the HSC OS without any product

Enter the number corresponding to your choice and press Enter [1-4]: 1
Last metadata expiration check: 0:03:09 ago on Tue 22 Apr 2025 11:12:21 AM -03.
hsc-mli-docker-stack-master-5.3.0-14.noarch.rpm                65 kB/s | 9.2 kB     00:00
Verifying...                    ################################# [100%]
Preparing...                    ################################# [100%]
Updating / installing...
   1:hsc-mli-docker-stack-master-5.3.0################################# [100%]
[+] Pulling 9/16
 ▪ mailinspector-admsuite [■■■■■■■■■■■■■■■■■■■■■■■] Pulling                    14.5s
 ▪ mailbox [■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■] Pulling   14.5s
 ▪ mailbox-ui [■■■■■■■■■■■■■■■■■■] Pulling                                    14.5s
 ▪ dmarc-analyzer [■■■■■■] Pulling                                              14.5s
 ▪ dmarc-imap [■■■■■■■■■■■] Pulling                                             14.5s
 ▪ dmarc-db [■■■■■■■■■] 319.6MB / 350.3MB Pulling                               14.5s
 ▪ mailbox-dav [■■■■] Pulling                                                   14.5s
```

Após escolhido o que será instalado, terá início ao download dos pacotes necessários

```
STEP 5) POST-INSTALLATION TASKS

Executing post-installation tasks...

Press <ENTER> to continue...

Generating grub configuration file ...
Adding boot menu entry for UEFI Firmware Settings ...
done
removed '/root/anaconda-ks.cfg'
removed '/root/original-ks.cfg'

Changing password for user root.
New password:
```

Insira uma nova senha para acesso como root (por SSH)

```
STEP 5) POST-INSTALLATION TASKS

Executing post-installation tasks...

Press <ENTER> to continue...

Generating grub configuration file ...
Adding boot menu entry for UEFI Firmware Settings ...
done
removed '/root/anaconda-ks.cfg'
removed '/root/original-ks.cfg'

Changing password for user root.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.

Press <ENTER> to continue...
```

Uma vez que tenha sido inserida a nova senha, o sistema pedirá para dar <ENTER> para prosseguir

```
STEP 6) SERVER RESTART

Your configuration is now complete.
The final step is to restart the server for changes to take effect.

Press <ENTER> to continue... _
```

Como última etapa, será reinicializado o sistema

```
OS: HSC OS 6.0 x86_64
Host: VMware Virtual Platform
Kernel: Linux 5.14.0-284.11.1.el9_2.x86_64
CPU: 11th Gen Intel(R) Core(TM) i7-11800H (4) @ 2.30 GHz
Local IP (eth0): 192.168.1.100/24

hsc-console login:
```

Após o reboot, será apresentada a tela indicando o IP a ser utilizada para acesso a interface gráfica do MailInspector

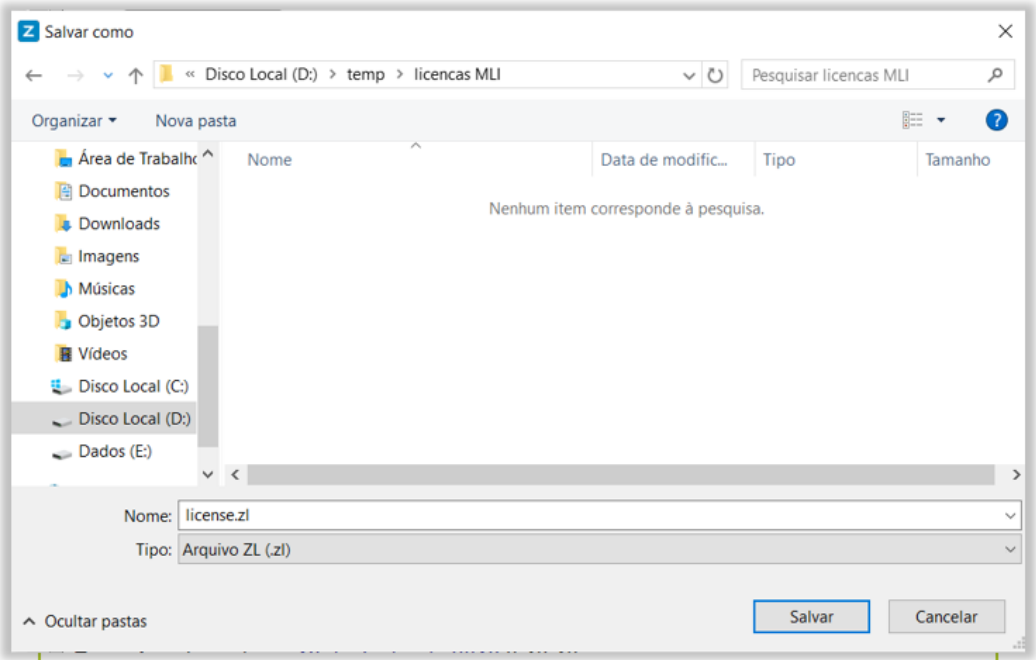
Ao finalizar a instalação, será ativada a interface gráfica (após o reboot).

Ao acessar pela primeira vez a console de administração, será apresentada a tela com o código para criação do licenciamento do MailInspector.

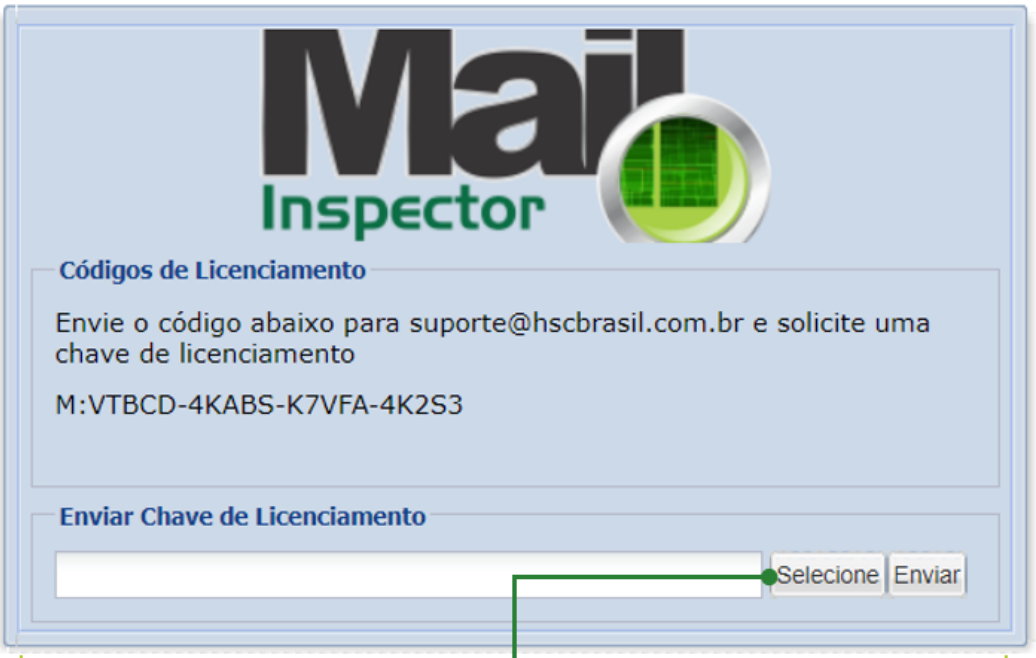
Para receber a sua licença, mande a chave (começa com M:) indicada para: suporte@hscbrasil.com.br com os seguintes dados:

1. IP externo utilizado pelo sistema para consulta a internet;
2. Nome da Empresa;
3. Dados de contato;

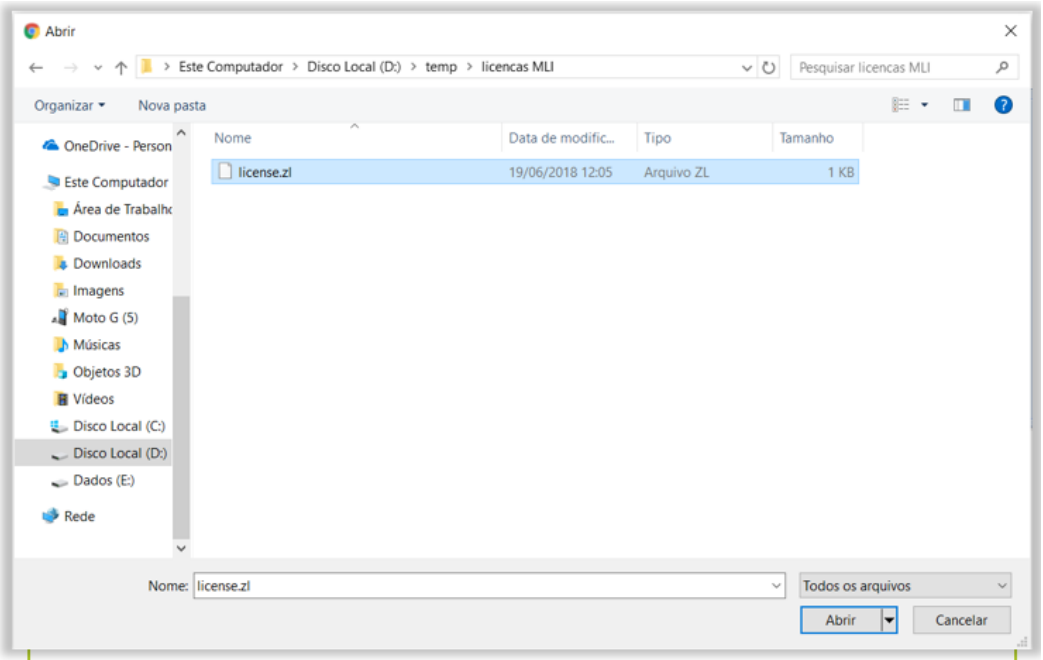
Mande o código da chave (para suporte@hscbrasil.com.br) que será enviada a licença de uso na sequência.



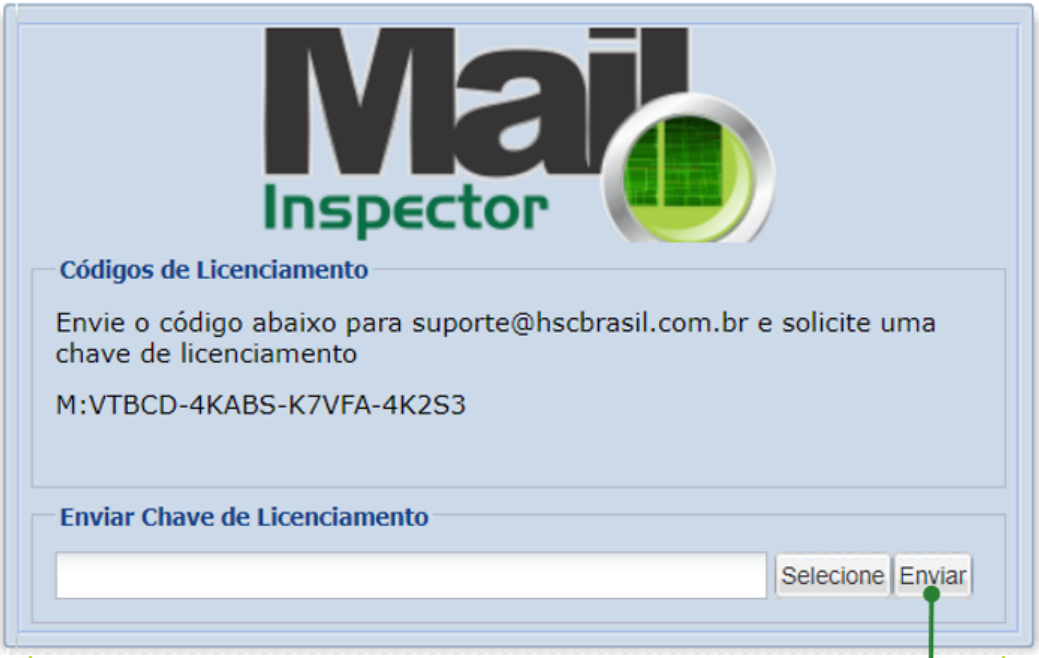
O pessoal do suporte encaminhará para o seu email o arquivo de licença, conforme acima indicado. Salve o arquivo.



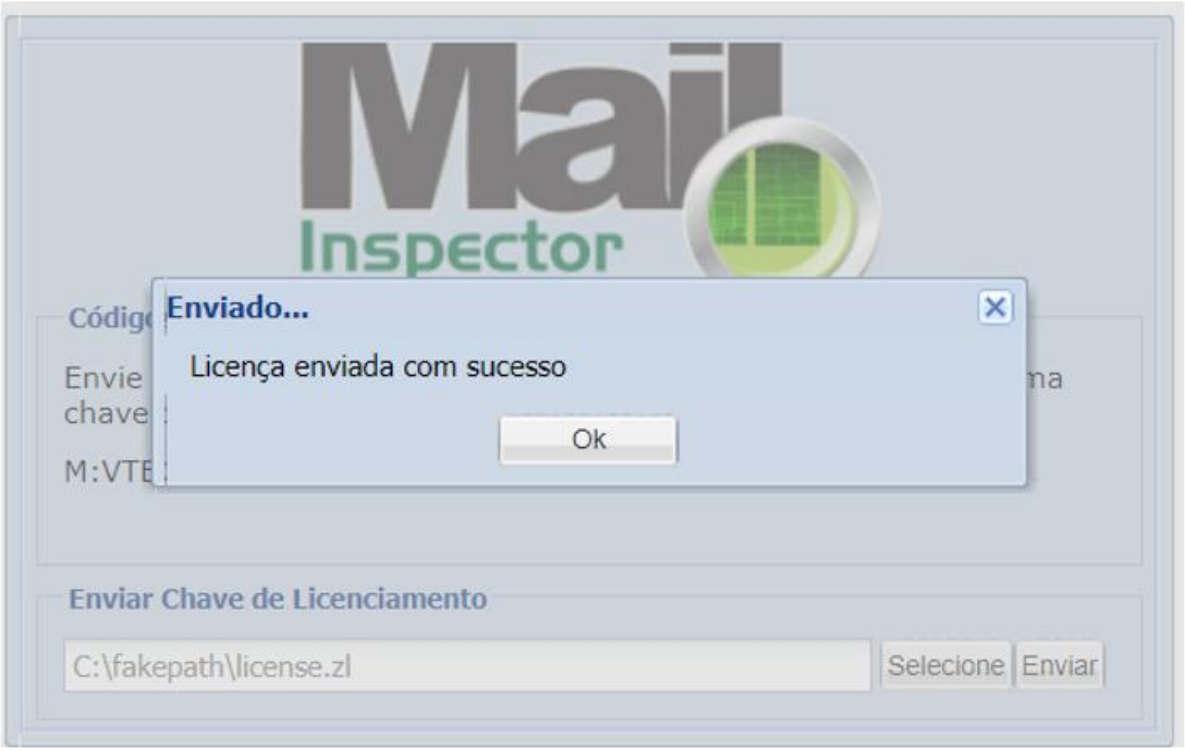
Clique no botão **Selecione**, para indicar o local do arquivo de licença que foi salvo.

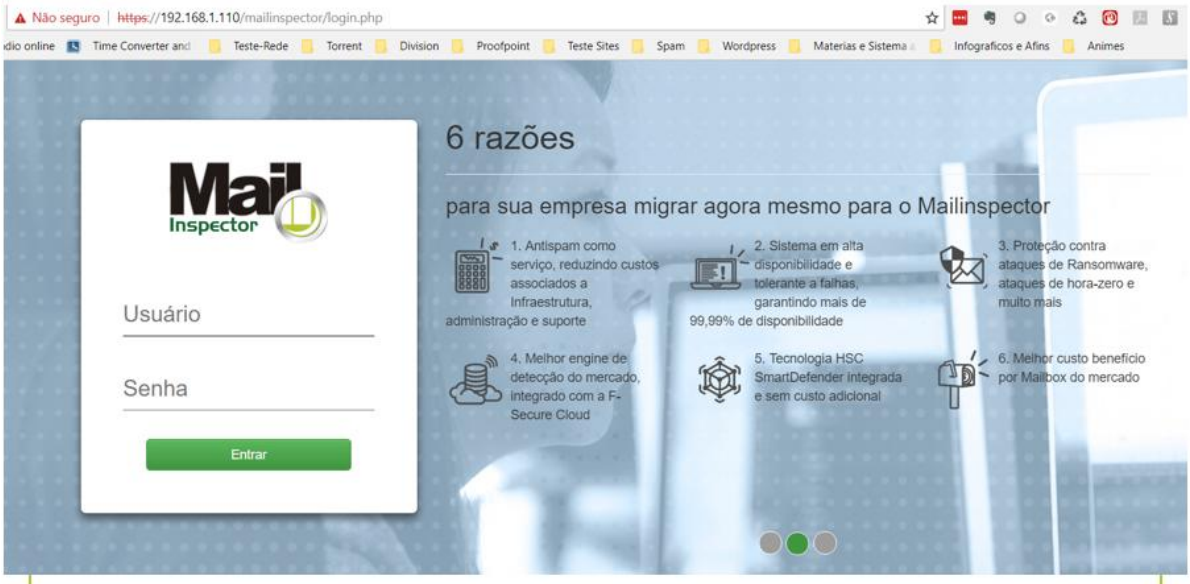


Indique o local onde está o arquivo de licença, anterior mente salvo.



Clique no botão **Enviar**.





Como resultado, é liberado o acesso a interface de gerenciamento.

Para acessar a interface web do MLI

Porta 80/443.

Usando protocolo HTTP/HTTPS

Navegadores suportados:

- Firefox 23 ou mais atual no Windows e Linux.
- Internet Explorer 7 ou mais recente no Windows.
- Chrome 29 ou mais recente Windows e Linux.
- Safari 5.1 ou mais recente no Windows e Mac.
- Microsoft Edge 86 ou mais recente no Windows.

Outros navegadores suportados:

- Chromium;
- Opera;
- Comodo Dragon;
- Vivaldi;
- Maxthon;
- Outros navegadores;

Usuários padrão e senha

A senha de acesso é apresentada ao final da instalação.

API de integração com outras aplicações

O MailInspector possui uma API que permite integração com aplicativos externos que utilizando o protocolo HTTP/HTTPS e possuem envio de requisições no formato FORM-DATA/REST API (Representational State Transfer API) por método POST ou GET, a API retorna no formato JSON. Dessa forma, com o uso de API's, é possível integrar o MailInspector com outros sistemas inerentes a empresa, tais como ferramentas medidoras de BI. O uso de API's é somente uma das formas de integração, existem outras formas, além das API's, tais como SYSLOG, acesso direto das informações via Banco de Dados, exportações de tabelas, integração via Dashboards ou até mesmo instalação de agentes na plataforma MailInspector.

Formatos aceitos na comunicação por API:

- YAML (Yet Another Markup Language ou YAML Ain't Markup Language);
- REST (Representational State Transfer API);
- XML (Extensible Markup Language);
- JSON (JavaScript Object Notation);
- SYSLOG;

Para um aplicativo externo efetuar o login da API é necessário ter o username e senha de um usuário, cadastrado pelo admsuite, que tenha o perfil API. Este ao efetuar o login essa aplicação pode interagir com as principais funcionalidades administrativas do Mailinspector.

Para efetuar os exemplos desse documento as requisições por protocolo HTTP serão simuladas pelo programa Postman, onde podemos efetuar o login. Essa requisição de login retorna um TOKEN, que possui exatos 96 caracteres alfanuméricos, e deve sempre ser adicionado nos cabeçalhos das próximas requisições. Este possui um tempo de 60 minutos de inatividade entre requisições, caso ultrapasse esse tempo um novo login deverá ser efetuado.

O MailInspector permite que outros sistemas utilizem a sua API, para aproveitar toda a inteligência do sistema SmartDefender, por exemplo, integração do EDR contido na empresa atualizado em tempo real com bloqueio automático de arquivos que foram utilizados em campanhas de ataques via e-mail. O MailInspector "avisa" ao antivírus da empresa que um anexo foi utilizado em uma campanha de ataque (no exemplo, o ataque foi dirigido a outro cliente ou detectado por outra plataforma como o ESET) e o antivírus já fica ciente de que o anexo é uma ameaça e já efetua bloqueio automático do mesmo, sem necessidade de análise do anexo, nem processamento desnecessário. Cria-se dessa forma uma rede GLOBAL de inteligência utilizando a inteligência múltiplos fabricantes em um único produto.

> É possível efetuar o rastreamento de todas as ações efetuadas através de usuário de API pelo módulo *Log de Eventos*.

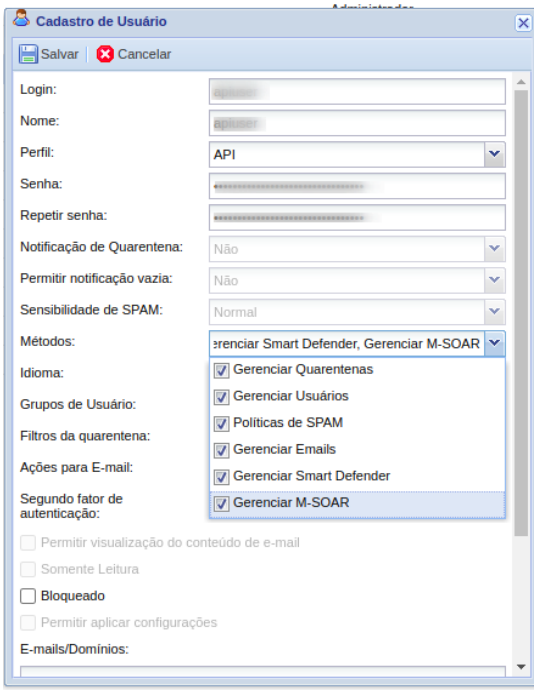
Algumas das ações possíveis com API (Cadastro/Criação, Exclusão, Consulta/Leitura, Atualização):

- Operação sobre lista de Usuários: Sincronização com sistemas de LDAP/AD/Zimbra e atuação sobre cadastro de usuários, permitindo as ações, até mesmo a nível de bloqueio em importação/sincronização de determinado usuário. Também atua sobre grupos de usuários,

podendo ser: domínios, subdomínios, regex, LDAP, grupos LDAP, grupos AD, IPs, range de IP, etc. Atua na camada de processamento;

- Operação sobre e-mails limpos (camada de processamento);
- Operação sobre e-mails quarentenados (camada de processamento);
- Operação de Controle de lista de Quarentena (camada de processamento);
- Operação sobre RBL's (camada de conexão – MTA);
- Operação sobre Allow List (camada de processamento);
- Operação sobre Block List (camada de processamento);
- Operação sobre filtros MTA: Todos os filtros que atuam na mensagem, podendo ser dede verificação de cabeçalho, até classificação de URL's, atuação sobre domínios, subdomínios, e-mails ou até por hostnames/IPs, range de IP, regex, filtros de condicionamento de mensagem (tamanho máximo, número de anexos, número de compactação, extensões bloqueadas/permitidas, etc). A operação sobre filtros é feita tanto na camada de conexão – MTA;
- Operação sobre filtros: Atua sobre filtros de filtragem do e-mail, podendo ser URL's, cabeçalho do e-mail, IPs, dicionários de palavras, domínios, subdomínios, etc. Esse processo é na camada de processamento;
- Operação sobre o módulo SmartDefender: Filtragem ativada no módulo SmartDefender, desde análise em SandBox local e em nuvem, até listas de DUL, ETL, etc. Esse processamento é feito na camada de processamento e camada de conexão – MTA;
- Operação sobre o módulo M-SOAR: Integração com sistema de orquestração, atuando sobre integração com Office 365, Zimbra e G-Suite. Esse processo é na camada de processamento;

Para o uso da API, primeiramente é necessário criar um usuário para a API do MailInspector.



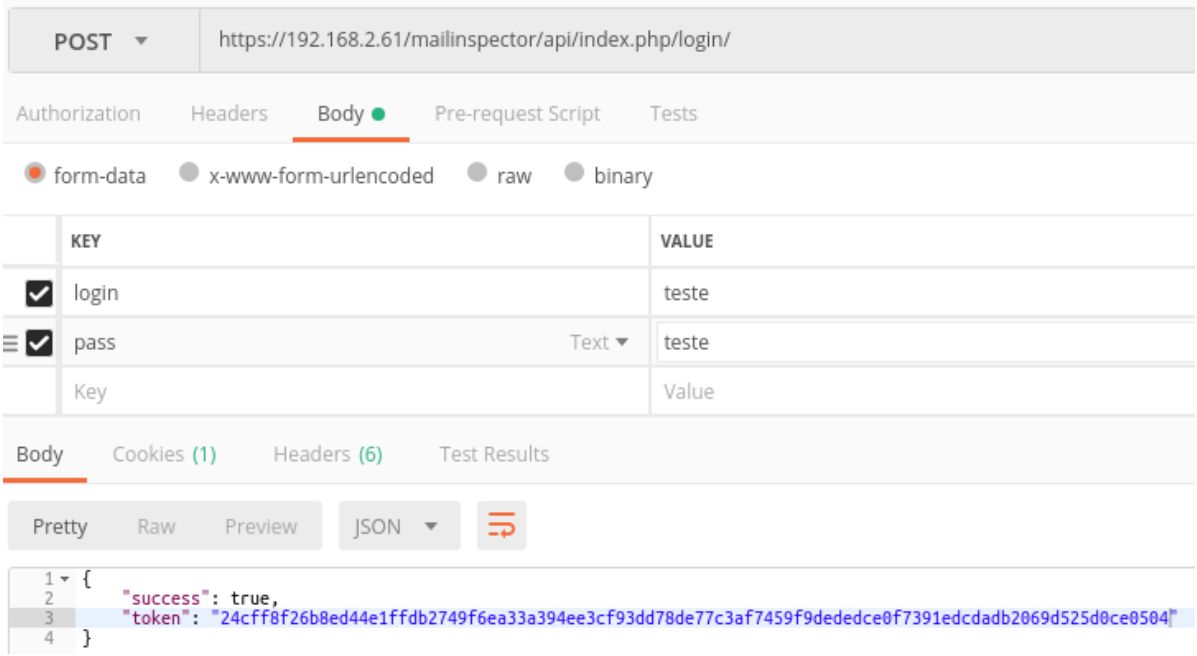
Autenticação

Executar o método login e retorna um JSON com o atributo token, quando inativo expira em uma hora, será adicionado no header das demais requisições com o nome de **token_auth**.

Localizar o hostname onde o Mailinspector está instalado. E efetuar uma requisição HTTP por método POST para o endereço:

```
https://{hostname}/mailinspector/api/index.php/login/
```

No corpo devem constar dois atributos **user** e **pass** com seus respectivos valores cadastrados no Admsuite.



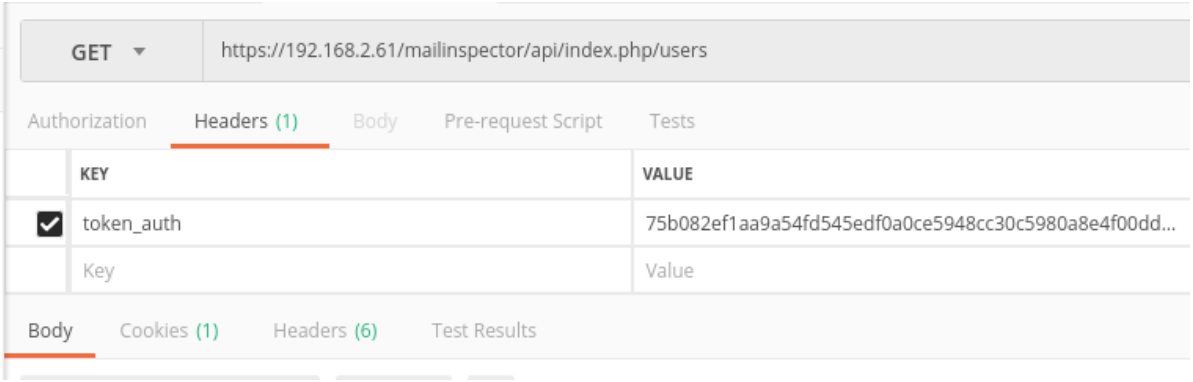
Ao enviar a requisição, em caso de sucesso, o atributo **success** retorna um Boolean true, junto com um atributo **token** que contém o token de sessão.

```
#!json

{

  "success": true,

  "token":
"a2a2d194f58348fc701dcfe58d635623d45dbf7853c4f9e2b9b33b4db6d5c3ea24eaeff
19c134fb22f9268264c94c540"

}
```

Em caso de falha, o atributo **success** retorna um Boolean false, junto com um novo atributo **msg** contendo a mensagem de erro.

```
#!json
{
  "success": false,
  "msg": "Senha incorreta."
}
```

Uma vez que você tenha o token deve usá-lo nos cabeçalhos das próximas requisições. Atribuindo o token no header com o nome do atributo **token_auth**.



Requisições

Vamos fazer uma nova requisição por HTTP por método GET para:

```
https://{hostname}/mailinspector/api/index.php/users
```

Retorna um JSON com a lista de usuários cadastrados no sistema.


```
{
  "success": true,
  "total": "1",
  "rows": [
    {
      "id": "54474",
      "username": "loureiro.silva",
      "name": "José Loureiro da Silva",
      "type": "1",
      "first_login": "1",
      "enable": "1",
      "sync": "1",
      "readOnly": "N",
      "language": "pt_BR"
    },
    {...},
    {...},
    {...},
    {...}
  ]
}
```


Porém se houver algum erro no token pode retorna a seguinte JSON:


```
{"success":false,"code":403,"msg":"Acesso negado"}
```

Lista de rotas

Rota	Método	Paramêtros	Utiliza Token
/login	POST	user[1], pass[1]	Não
/logout	GET		Sim
/point	GET		Sim
/users	GET		Sim
/users/add	POST	name[1], user[1], pass[1], e-mail[1], locale[2]	Sim
/users/show/{user_id}	GET		Sim
/users/update/{user_id}	POST	name[1], user[1], pass[1], e-mail[1], locale[2]	Sim
/users/delete/{user_id}	GET		Sim
/spam/filters	GET		Sim
/spam/rbls	GET		Sim
/spam/controls	GET		Sim
/spam/scorepoints	GET		Sim
/point	GET		Sim
/probable-spam/scorepoints	GET		Sim
/quarantine/system	GET	point	Sim
/quarantine/custom	GET	point	Sim
/quarantine/mails	GET	point[1], date_start[3], date_end[3], size[5] , score[5] , delivered[4]	Sim
/blacklist	POST	point[1], to_address[2], from_address[2]	Sim
/blacklist/add	POST	point[1], to_address[1], from_address[1]	Sim
/blacklist/update/	POST	point[1], to_address[1], from_address[1]	Sim
/blacklist/delete/	GET		Sim

/whitelist	POST	point[1], to_address[2], from_address[2]	Sim
/whitelist/add	POST	point[1], to_address[1], from_address[1]	Sim
/whitelist/update/	POST	point[1], to_address[1], from_address[1]	Sim
/whitelist/delete/	GET		Sim
/e-mail/search	POST	point[1], id[2], from[2], to[2], subject[2], date_start[2], date_end[2], operator_from_address[2], operator_to_address[2]	Sim
/e-mail/details	POST	point[1], id[1]	Sim
/e-mail/evidencelog	POST	point[1], id[1]	Sim
/smartDefender/search	POST	point[1], type[1](url, file or ip), value[1]	Sim
/smartDefender/whitelist	POST	point[1], type[1](url, file or ip), value[1]	Sim
/smartDefender/blacklist	POST	point[1], type[1](url, file or ip), value[1]	Sim
/office365/attach	POST	point[1], selected[1](Array)	Sim
/office365/links	POST	point[1], selected[1](Array)	Sim
/office365/move	POST	point[1], selected[1](Array)	Sim
/office365/block	POST	point[1], selected[1](Array)	Sim
/office365/delete	POST	point[1], selected[1](Array)	Sim

Leganda:

1 – Campo Obrigatório

2 – Campo Opcional

3 – Campo Opcional Datetime (YYYY-MM-DD)

4 – Campo opcional Boolean (0-1)

5 – Campo opcional inteiro

Login da API

POST {{url}}/mailinspector/api/index.php/login

➔ Request Body

```
login VALUE [nome  do usuário]

pass  VALUE [senha do usuário]
```

➔ Retorno


```
{

    "success": true,

    "token":
"9asd6777asd0fbesdf0cf3913a4da2b854177b2dd7fbc3e2e4d0fec98a9bd38881eee8841
4c868adb8"

}
```


Pontos de Acesso

GET {{url}}/mailinspector/api/index.php/point

➔ Request Header

```
token_auth VALUE [token]
```

➔ Request Body

```
none
```

➔ Retorno


```
{

    "success": true,

    "rows": [

        {

            "id": "1",

            "name": "Ponto 1",
```

```
            "ip": "192.168.0.10"
        }
    ]
}
```


E-mails

GET {{url}}/mailinspector/api/index.php/e-mail/search

➔ Request Header

token_auth VALUE [token]

➔ Request Body

start VALUE 0 (offset da requisição)

limit VALUE [10,30,50,70,100] (limite de dados retornados)

sort VALUE [datetime, ...]

dir VALUE [DESC]

➔ Retorno


```
{
    "success": true,
    "total": "36",
    "rows": [
        {
            "id": "138CA9B59B5.ABD09",
            "datetime": "29/08/2023 10:18:41",
            "from": "",
            "to": "app@mindaware.com.br",
            "subject": "Aviso de erro de entrega e-mail",
            "headers": "... ... ... ",
```

"size": "12590",

"delivered": true,

"report": " (msg-5210-2.msg) MimeType: text/plain ",

"quarantined": 1,

"userReleased": "0",

"spamreport": "Nao e SPAM, HSC MailInspector (cached, Pontuacao=6.325, requerido 9, BAYES_99 6.00, BAYES_999 0.20, HSC_ENVELOPE_EMPTY_SENDER 0.10, HSC_THREAT_PHISHING 0.00, HSC_THREAT_ZERO_DAY 0.00, HSC_UNCATEGORIZED_SENDER 0.01, HSC_UNCATEGORIZED_URL 0.01, HTML_MESSAGE 0.00, RCVD_IN_DNSWL_BLOCKED 0.00, SPF_HELO_NONE 0.00)",

"clientip": "187.108.197.228",

"status": "",

"point_id": "1",

"has_attachment": 1,

"score": "6.33",

"isspam": false,

"ishighspam": false,

"spamwhitelisted": false,

"spamblacklisted": false,

"virusinfected": false,

"nameinfected": false,

"otherinfected": false,

"partition": "2023-08-29 10:18:41",

"mcpreport": null,

"isUTF8": true,

"country": "Brazil\n",

"cdr": 0,

"url": 0,

```
        "threat": true,
        "custom_quarantined": 0,
        "dlp": 0,
        "advancedcontrolrule": 0,
        "isphishing": 1,
        "suspect_mail": 0,
        "suspect_file": 0,
        "suspect_domains": 0,
        "another_lock": false,
        "dmarc": 0,
        "dkim": 0,
        "spf": 0,
        "social_networking": 0,
        "antispoofing": 0,
        "e-mail_marketing": false,
        "mail_bulk": 0,
        "mail_fake": 0,
        "atp": true,
        "malware": 0,
        "mail_adult": 0,
        "header_diff_domains": 0,
        "free-mail_fake": 0,
        "free-mail_from": 0,
        "oversize": 0,
        "ok": false,
        "encrypt_messages": 0,
        "passvault": 0
    },
```

```
            { . . . }

        ]

    }
```

Informações da Mensagem

ID:		
Assunto:		
Domínio de Origem:		
Domínio de Destino:		
Hostname:		
Campos de filtragem com as cláusulas Parcial ou Header podem tornar a pesquisa lenta.		
E-mail de Origem:		Exata
E-mail de Destino:		Exata
Corpo:		
URL:		
Nome do Anexo:		
IP de Origem:		
Tamanho (MB):		
Mensagem Entregue:	Selecione...	
Assinatura:		
Regra de Controle Avançado:	Selecione...	
Regra de DLP:	Selecione...	
Ameaça:		
Cabeçalho:		
Pontuação:	Igual	
Tráfego:	Todos	
País de origem:	Selecione...	

ID ⇒ **filter[id]**

Assunto ⇒ **filter[subject]**

Domínio de Origem ⇒ **filter[from_domain]**

Domínio de Destino ⇒ **filter[to_domain]**

Hostname ⇒ **filter[from_hostname]**

E-mail de Origem ⇒ **filter[from_address]** ♦ **operator[from_address]** VALUES [**EQUAL**|**RLIKE**|**HEADER**]

E-mail de Destino ⇒ **filter[to_address]** ♦ **operator[to_address]** VALUES [**EQUAL**|**RLIKE**|**HEADER**]

Corpo ⇒ **filter[body]**

URL ⇒ **filter[url]**

Nome do Anexo ⇒ **filter[attachment]**

IP de Origem ⇒ **filter[clientip]**

Tamanho (MB) ⇒ **filter[size]**

Mensagem Entregue ⇒ **filter[delivered]** VALUES [Todos=**T** | Somente Sim = **1** | Somente Não = **0**]

Assinatura ⇒ **filter[spamRule]**

Regra de Controle Avançado ⇒ **filter[advancedControlRule]**

Regra de DLP ⇒ **filter[ldapRule]**

Ameaça ⇒ **filter[threat]**

Cabeçalho ⇒ **filter[header]**

Pontuação ⇒ **filter[score_operator]** VALUES [“>” | “>=” | “=” | “<=” | “<”] ♦ **filter[score]**

Tráfego ⇒ **filter[traffic]** VALUES [Todos = **null** | Entrada = **INPUT** | Saída = **OUTPUT** | Interno = **INTERNAL**]

País de origem ⇒ **filter[country]** VALUES [Brazil = **Brazil** | …]

Período de Tempo

Data Inicial: 29/08/2023 00:00

Data Final: 29/08/2023 23:59

Status

Operador lógico: E

- [ ] Arquivos suspeitos
- [ ] BlackList
- [ ] CDR
- [ ] Conteúdo Bloqueado
- [ ] Domínios Diferentes no Cabeçalho
- [ ] Domínios Recentes / Suspeitos
- [ ] E-mail Marketing
- [ ] Free Mail
- [ ] Limpa/Auditoria
- [ ] Outro Bloqueio
- [ ] Phishing
- [ ] Redes Sociais
- [ ] Regras de Controle Avançado
- [ ] Spoofing de domínio
- [ ] Vírus
- [ ] ATP
- [ ] Bulk Mail
- [ ] Conteúdo Adulto
- [ ] Criptografada
- [ ] Domínios Forjados com Free Mail
- [ ] Liberados
- [ ] Malware
- [ ] Password Vault
- [ ] Provável Spam
- [ ] Regras de Compliance
- [ ] Spam
- [ ] Tamanho Excedido
- [ ] WhiteList

Data Inicial ⇒ **filter[date_start]**

Data Final ⇒ **filter[date_end]**

Operador lógico ⇒ **filter[statusCondition]** VALUES [E = **AND** | OU = **OR**]

Arquivos suspeitos ⇒ **filter[status][suspect_file]** VALUE [**1**]

BlackList ⇒ **filter[status][spamblacklisted]**

CDR ⇒ **filter[status][cdr]**

Conteúdo Bloqueado ⇒ **filter[status][nameinfected]**

Domínios Diferentes no Cabeçalho ⇒ **filter[status][suspect_domains]**

Domínios Recentes / Suspeitos ⇒ **filter[status][suspect_domains]**

E-mail Marketing ⇒ **filter[status][email_marketing]**

Free Mail ⇒ **filter[status][freemail_from]**

Limpa/Auditoria ⇒ **filter[status][ok]**

Outro Bloqueio ⇒ **filter[status][otherinfected]**

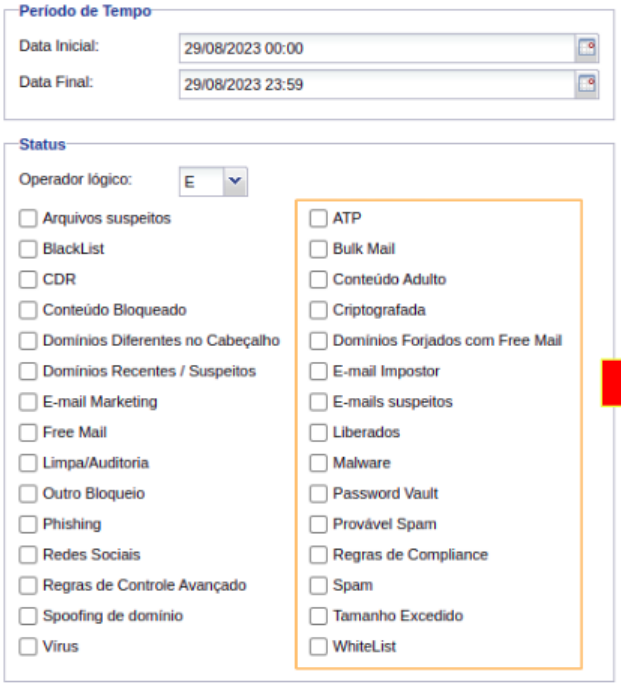
Phishing ⇒ **filter[status][isphishing]**

Redes Sociais ⇒ **filter[status][social_networking]**

Regras de Controle Avançado ⇒ **filter[status][advancedcontrolrule]**

Spoofing de domínio ⇒ **filter[status][antispoofing]**

Vírus ⇒ **filter[status][virusinfected]**




```
ATP ⇒ filter[status][atp]
Bulk Mail ⇒ filter[status][mail_bulk]
Conteúdo Adulto ⇒ filter[status][mail_adult]
Criptografada ⇒ filter[status][encrypt_messages]
Domínios Forjados com Free Mail ⇒ filter[status][freemail_fake]
E-mail Impostor ⇒ filter[status][mail_fake]
E-mails suspeitos ⇒ filter[status][suspect_mail]
Liberados ⇒ filter[status][released]
Malware ⇒ filter[status][malware]
Password Vault ⇒ filter[status][passvault]
Provável Spam ⇒ filter[status][isspam]
Regras de Compliance ⇒ filter[status][dlp]
Spam ⇒ filter[status][ishighspam]
Tamanho Excedido ⇒ filter[status][oversize]
WhiteList ⇒ filter[status][spamwhitelisted]
```

M-SOAR

Remover Anexos

Executa ação M_SOAR - Remover Anexos

```
{{url}}/mailinspector/api/index.php/office365/attach
```

➔ Request Header

token_auth VALUE [token]

➔ Request Body

point VALUE [id do ponto]

selected VALUE [array com id de mensagens]

ex.: ["B23D89B59BA.A4C8D","A71EB9B59B2.A49EE"]

[id do ponto] obtido pelo request /point (ver lista de rotas)

Remover Links

Executa ação M_SOAR - Remover Links

```
{{url}}/mailinspector/api/index.php/office365/links
```

➔ Request Header

token_auth VALUE [token]

➔ Request Body

point VALUE [id do ponto]

selected VALUE [array com id de mensagens]

ex.: ["B23D89B59BA.A4C8D","A71EB9B59B2.A49EE"]

[id do ponto] obtido pelo request /point (ver lista de rotas)

Mover para Lixo Eletrônico

Executa ação M_SOAR - Mover para Lixo Eletrônico

```
{{url}}/mailinspector/api/index.php/office365/move
```

➔ Request Header

token_auth VALUE [token]

➔ Request Body

point VALUE [id do ponto]

selected VALUE [array com id de mensagens]

ex.: ["B23D89B59BA.A4C8D","A71EB9B59B2.A49EE"]

[id do ponto] obtido pelo request /point (ver lista de rotas)

Bloquear Conteúdo

Executa ação M_SOAR - Bloquear conteúdo

```
{{url}}/mailinspector/api/index.php/office365/block
```

➔ Request Header

token_auth VALUE [token]

➔ Request Body

point VALUE [id do ponto]

selected VALUE [array com id de mensagens]

ex.: ["B23D89B59BA.A4C8D","A71EB9B59B2.A49EE"]

[id do ponto] obtido pelo request /point (ver lista de rotas)

Apagar Permanentemente

Executa ação M_SOAR - Apagar permanentemente

```
{{url}}/mailinspector/api/index.php/office365/delete
```

➔ Request Header

token_auth VALUE [token]

➔ Request Body

point VALUE [id do ponto]

selected VALUE [array com id de mensagens]

ex.: ["B23D89B59BA.A4C8D","A71EB9B59B2.A49EE"]

[id do ponto] obtido pelo request /point (ver lista de rotas)

Modo Rewrite

Para ativar o rewrite, é necessário configurar a rota para o arquivo index. A rota é processada pelo framework SlimPHP que fica no diretório /api. Com este processo de rota processada, o rewrite é ativado.

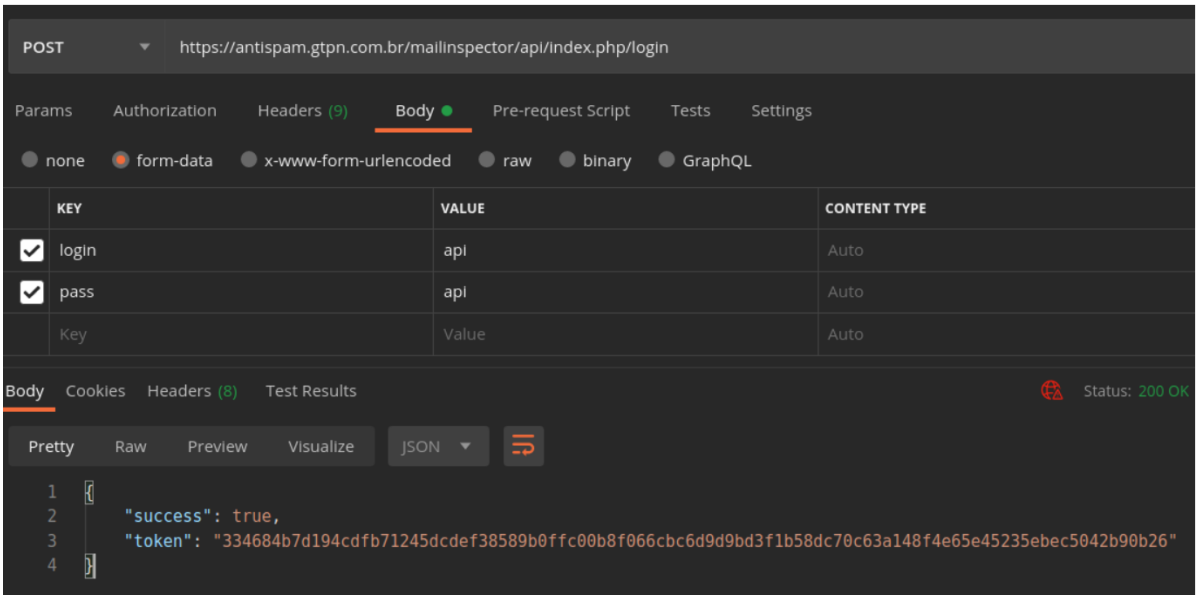
Com o modo write:

```
#!
https://{hostname}/mailinspector/api/index.php/users
```

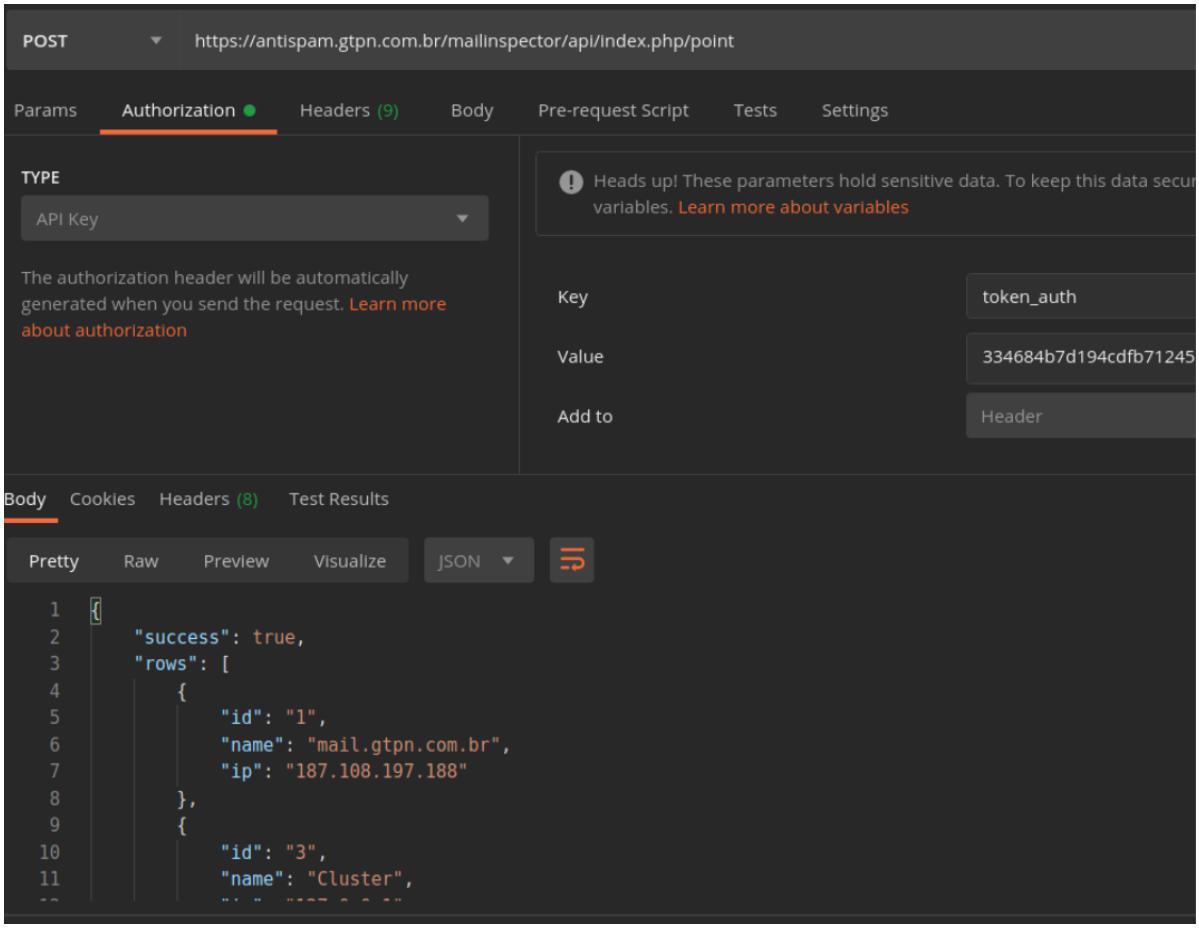
Sem modo write:

```
#!
https://{hostname}/mailinspector/api/index.php/login/
```

Efetuando login:



Autenticando por token



Integração com outros produtos da HSCBRASIL

O HSC MailInspector® possui capacidade de integração com outros produtos da HSCBRASIL, tais como:

- MindAware: Sistema de Conscientização, treinamento e campanhas de simulação de ataques de phishing e afins. Com a integração com o MailInspector, contamos como:
    - Interface de admin ganha um dashboard com dados sobre as ações do usuário em e-mails reais, para comparar com as simulações.
    - O grau de maturidade do usuário (inseguro, vulnerável, prevenido e conscientizado) passa a levar em conta também os dados do Mailinspector.
    - Através de integração por API, o sistema de IA sugere aos usuários cursos com base no seu comportamento com e-mails reais, indo além das sugestões baseadas nas simulações. Isso garante uma abordagem personalizada e efetiva.

MindAware

1. MailInspector detecta ações positivas e negativas dos usuários em e-mails reais.
2. Com a API, o MailInspector Identifica e reporta ao MindAware o comportamento do usuário ao lidar com e-mails reais.
    a. Os dados são enviados ao MindAware, que ajusta os treinamentos e a pontuação de maturidade dos usuários, bem como ajuste da sua posição nos quadrantes:
        i. Inseguro;
        ii. Vulnerável;
        iii. Prevenido;
        iv. Conscientizado;
3. Contabiliza tanto comportamentos de risco (como cliques numa URL maliciosa) quanto ações positivas (como reportar um phishing ou link malicioso).
4. De acordo com a maturidade indicada do usuário no MindAware, o sistema de IA no MailInspector ajusta a sensibilidade de detecção para aquele usuário em específico, sendo mais rígido ou não, de acordo com o perfil e comportamento do usuário, junto com a indicação dos treinamentos efetuados no MindAware.
5. Se o usuário do MailInspector clicar em um link malicioso de um e-mail real, esse clique é computado no sistema e o registro do clique é enviado ao MindAware. O mesmo acontece quando ele reporta um e-mail como sendo malicioso, dessa forma, a indicação do usuário no quadrante é constantemente atualizada de acordo com a sua ação tomada nos e-mails verdadeiros.
6. No MindAware, de acordo com a localização do usuário no quadrante e comportamento, o sistema de IA personaliza a sugestão de cursos, emite alertas e mitiga comportamentos de risco em tempo real.

Apêndice 1 - Glossário

Adware

É qualquer programa de computador que executa automaticamente e exibe uma grande quantidade de anúncios sem a permissão do usuário.

As funções do adware servem para analisar os locais de Internet que o usuário visita e lhe apresentar publicidade pertinente aos tipos de bens ou serviços apresentados lá.

O MailInspector utiliza HSC SmartDefender antivírus e ESET para detectar esse tipo de ameaça, entre outros.

Alertas

São disparados, quando atinge algum parâmetro pré-programado atinge o nível indicado. O sistema dispara aviso ao administrador. Os alertas no MailInspector podem ser enviados por E-mail, sistema de comunicação instantânea (Telegram), SNMP (utilizados por múltiplos sistemas de monitoramento, tal como CACTI), syslog apontado para servidor específico e até mesmo através de agentes de monitoramento de terceiros instalados (como Zabbix, Nagios, etc). O MailInspector é totalmente compatível com sistemas do tipo SIEM.

Os alertas enviados pelo MailInspector podem ser dos mais variados tipos, seguindo alguns exemplos:

- Consumo de CPU;
- Consumo de disco;
- Consumo de memória;
- Fila excessiva de e-mails (tanto na fila de entrada, como na fila de saída), com indicação de quantidade e e-mails parados na fila;
- Excessivo número de conexões oriundos de um único ponto;
- Agentes de filtragem com problema de comunicação;
- Atualizações do sistema (vacinas, assinaturas de spam, novas URL's, novas categorizações de URL's, etc);
- Problemas de consulta de reputação de IP, URL's, domínios, etc;
- Erros de sincronização dos conectores externos (LDAP, AD, Zimbra, etc);
- Problemas de comunicação com portas necessárias para o bom funcionamento do sistema;
- Surtos de vírus;
- Surtos de ataques de dicionário;
- Falha de componentes da solução (que não estão respondendo ou não estão ativados);
- Muitos outros alertas;

Ameaças Persistentes Avançadas (APT)

É o ataque ao qual o criminoso realiza o reconhecimento do seu alvo com planejamento, estudando possíveis falhas ou até ambientes de terceiros que podem facilitar o acesso a uma rede corporativa, por exemplo. Ele também pode utilizar engenharia social e explorar ambientes com pouca ou nenhuma monitoração.

Após obter o acesso à rede, o golpista procura elevar os seus privilégios e aumentar o seu controle sobre os servidores e sistemas. Depois da invasão, irá explorar as falhas, de forma contínua, até obter as informações

definidas como alvo. Se não for pego, ele possui tempo suficiente para extrair uma grande quantidade de dados e até mesmo selecioná-los.

Na APT, o atacante pode utilizar aplicativos que não são maliciosos, que possuem assinatura digital e que nenhuma solução de segurança seja capaz de detectar tal ação. O que exige atenção são os aplicativos e ferramentas que fazem parte dos whitelisted das soluções de segurança, pois muitas vezes são estes que o golpista acaba usando para a APT.

No MailInspector, quem detecta o APT é o SmartDefender, que consulta BigData para verificar ameaças crescentes de forma dinâmica e bloqueando as novas campanhas maliciosas. O Sistema BigData do MailInspector é alimentado pelos mais variados indicadores de IOCs, desde outro fabricante (de antivírus como ESET), outras bases instaladas de MailInspector entre outras fontes globais.

Anti-phishing

Sistema que bloqueia e-mails que contêm links no corpo da mensagem que direcionam para sites de phishing conhecidos ou se eles contiverem palavras-chave de phishing conhecidas. Phishing é uma técnica de engenharia social baseado em e-mail que tem como objetivo fazer com que usuários de e-mails divulguem informações pessoais a remetentes de spam. Um e-mail de phishing é provavelmente criado para que seja semelhante a um e-mail oficial de uma empresa respeitável, por exemplo, um banco. Os e-mails de phishing geralmente contêm instruções que exigem que os usuários reconfirmem informações confidenciais, como dados de acesso a serviços bancários on-line ou dados de cartão de crédito. E-mails de phishing geralmente incluem um Uniform Resource Identifier (URI) de phishing que o usuário deverá seguir para inserir informações confidenciais em um site de phishing. O site acessado pelo URI de phishing pode ser uma réplica de um site oficial, mas, na verdade, é controlado por quem enviou os e-mails de phishing. Quando o usuário digita as informações confidenciais no site de phishing, os dados são coletados e usados, por exemplo, para retirar dinheiro de contas bancárias.

No MailInspector possui várias camadas de detecção de phishing, utilizando as mais variadas técnicas de proteção e bloqueio de phishing. A seguir, seguem as camadas que detectam e bloqueiam phishing:

- HSC SmartDefender;
- Global Sender Reputation & Threat Response;
- Message Reputation;
- URL Categorization & Reputation;
- Sandbox File & URL;
- HSC Targeted Attack;

Anti-Spam

É um sistema de bloqueio de mensagens indesejadas na caixa de e-mail do usuário.

O sistema MailInspector da HSCBRASIL, faz a proteção contra spams a nível de entrada E saída, tanto em solução implementada localmente, quanto na solução em nuvem, dessa forma possibilitando a proteção completa na empresa. No MailInspector, o sistema de anti-spam, trabalha de forma com assinaturas atualizadas constantemente através de updates e também utiliza sistema inteligente de análise contextual do corpo do e-mail (Machine Learning, análise bayesiana e heurística), verificação de e-mail sem conteúdo (e-mail vazio), análise léxica, bem como detecção de spam em imagens (tanto no corpo do e-mail, quanto em

anexos – detectando vários modelos de imagens, tais como: BMP, JPEG, JPG, GIF, PNG, TIFF, etc), spam em documentos do tipo Office, dentre eles: PDF's, DOC's, XML's, entre outros tipos de anexos. Além de análise do e-mail em si, também é efetuada a análise da reputação do IP de origem, entre outras técnicas, tais como proteção a domínios recém adquiridos mandando e-mails em massa, ou até mesmo detecção e proteção a ataques de e-mails usando domínios similares de domínios válidos.

Antivírus

É um programa de proteção do computador que detecta e elimina os vírus (certos programas danosos) nele existentes, assim como impede sua instalação e propagação.

No MailInspector, podemos encontrar dois sistemas de antivírus trabalhando simultaneamente (ESET e nativamente o HSC SmartDefender antivírus), sendo ambos já licenciados. Além disso, contamos com sistema Zero Hour, para maior segurança do sistema. Uma vez ativada na configuração, o sistema de Zero Hour atua de forma automática, sem a necessidade de intervenção do administrador ou do usuário.

Já a nível de SandBox, contamos também temos o ESET (além do antivírus nativo HSC SmartDefender antivírus) para a varredura e detecção das ameaças.

API

A sigla API corresponde às palavras em inglês "Application Programming Interface". No português "Interface de Programação de Aplicações". Elas são uma forma de integrar sistemas, possibilitando benefícios como a segurança dos dados, facilidade no intercâmbio entre informações com diferentes linguagens de programação.

O MailInspector possui API's para uso. Para isso, basta cadastrar um usuário como API, ao qual é gerada a credencial de API, liberando dessa forma a conexão com outros aplicativos.

Para usuários do tipo API as permissões podem ser:

- Pesquisa de Quarentena,
- Listar Políticas de SPAM,
- Criar/Editar/Remover/Pesquisar Usuários Finais

Um exemplo de uso de API é a integração do MailInspector com SIEM (Security Information and Event Management).

Appliance

É um dispositivo de hardware separado e dedicado com software integrado, especificamente projetado para fornecer um recurso de computação específico.

Estes dispositivos se tornaram conhecidos como "aparelhos" (appliance) devido a sua similaridade com os aparelhos domésticos, que geralmente são "fechados e selados". O hardware e o software são pré-integrados e pré-configurados antes de ser entregue ao cliente.

O hardware utilizado no appliance sempre é homologado pelo fabricante para o uso do sistema em específico, oferecendo uma maior confiabilidade e reduzindo o risco de eventual incompatibilidade engtre software e hardware.

O MailInspector pode ser trabalhado de forma appliance (software sobre o hardware homologado e otimizado para o sistema), instalado em VMWares e/ou em nuvem (sem o custo de manter hardware e hospedagem do sistema). O uso do MailInspector também pode ser de forma mista, appliances virtuais em conjunto com appliances físicos.

Ataque Dirigido

Ver Spear Phishing

APT (Advanced Persistent Attack) ou Ameaça Persistente Avançada

É geralmente usada para se referir a ameaças cibernéticas, em particular a prática de espionagem via internet por intermédio de uma variedade de técnicas de coleta de informações que são consideradas valiosas o suficiente para que o agente espião despenda tempo e recursos para obtê-las.

Ataques APT são direcionados (targeted attacks). Esses ataques utilizam uma grande variedade de técnicas, inclusive drive-by download, injeção de SQL (SQL injection), malwares, spywares, phishing e spam, etc. Esses ataques podem simultaneamente usar (e frequentemente usam) mais de uma técnica. Embora ataques APT sejam sempre direcionados, nem todo ataque dirigido é do tipo APT.

O MailInspector detecta o ataque do tipo ATP através de múltiplos processos de proteção, tendo uma quarentena específica para esse processo, bem como técnicas específicas de detecção. A quarente a de ATP tem a maior prioridade sobre todas as outras, dessa forma qualquer e-mail considerado ATP, por padrão, será quarentenado na pasta de quarentena ATP, mesmo que ela tenha outros status classificatórios, como por exemplo malware ou spam.

ARC (Authenticated Received Chain)

É um protocolo de autenticação de e-mail que permite aos servidores de correio de destino verificar os resultados de autenticação de um e-mail quando este é reencaminhado ou transmitido por um servidor intermediário.

ARC é uma extensão dos padrões de autenticação de e-mail existentes, como SPF (Sender Policy Framework), DKIM (DomainKeys Identified Mail) e DMARC (Domain-based Message Authentication, Reporting, and Conformance).

Muitos serviços de e-mail já estão usando este sistema de autenticação de cadeia, para ter garantia de que não houve violação sobre os dados de SPF, DKIM e DMARC.

Como funciona o ARC?

1. Quando um e-mail é enviado, cada servidor na cadeia de entrega adiciona o seu resultado de autenticação ao cabeçalho ARC do e-mail.
2. O ARC gera uma cadeia de autenticação confiável, garantindo que nenhumas alterações ou cabeçalhos adicionais por parte de servidores intermediários causem o e-mail a falhar os verificadores de autenticação SPF, DKIM e DMARC.
3. O ARC Seal header contém um tag chamado chain validation “cv=”, que contém o resultado da avaliação da cadeia ARC existente. O valor pode ser “none”, “fail” ou “pass”.

O MailInspector é totalmente compatível com o protocolo ARC, uma vez que ele mantém intacto os cabeçalhos originais do e-mail, dessa forma, preservando os resultados da autenticação dos e-mails, respeitando a cadeia ARC, incluindo a resposta do chain validation, bem como o resultado da autenticação dos outros protocolos (SPF, DKIM e DMARC).

BEC

O BEC (Business E-mail Compromise), também conhecido como fraude de e-mail, é um ataque na qual o invasor obtém acesso a uma conta de e-mail corporativa e falsifica a identidade do proprietário (ou de algum funcionário) para fraudar a empresa ou seus funcionários, clientes ou parceiros para golpes financeiros. Em alguns casos, um invasor simplesmente cria uma conta com um endereço de e-mail muito semelhante a um na rede corporativa.

O MailInspector detecta este tipo de ataque usando métodos proteção de controle contra Look-Alike Domains, análise com SPF, DKIM e DMARC, bem como verificação de eventual ataque de dicionário (que muitas vezes antecede este tipo de fraude). Além disso tudo, o MailInspector conta com o sistema de SmartDefender que sincroniza as ameaças crescentes em tempo real com consultas no BigData do ESET antivírus.

BitDefender

BitDefender é uma empresa de segurança na Internet que produz software antivírus e outros serviços fundada na Romênia em 2001.

Com até 1.600 funcionários, além de uma equipe de mais de 800 engenheiros e pesquisadores, a Bitdefender é uma das empresas de software de segurança de TI mais inovadoras do mundo atualmente.

Possui mais de 100 patentes registradas para tecnologias de núcleo apenas nos últimos três anos. Mais 230 estão atualmente aguardando exame, sendo que 10% das patentes são referentes a algoritmos de aprendizagem de máquina para a detecção de malware e outras ameaças online, aprendizagem profunda e técnicas de detecção baseadas em anomalias que têm um papel crítico na luta proativa contra ameaças novas e desconhecidas.

O BitDefender antivírus tem cerca de 500 milhões de usuários em todo o mundo, dessa forma a base de conhecimento é enorme e à disposição para consultas do MailInspector.

O MailInspector utiliza o BitDefender em segundo plano dentro do módulo HSC SmartDefender Cloud (roda em primeiro plano o antivírus nativo HSC SmartDefender antivírus), integrando todas as funcionalidades dele para análise e segurança dos e-mails.

Bounce Mail

O termo "bounce" é uma mensagem de erro enviada pelos servidores e que nos indica o número de pessoas que não receberam o seu e-mail e os motivos.

A customização das mensagens de bounce no MailInspector é efetuado na parte de *Notificações*, permitindo ao administrador alterar as mensagens retorno de erro, com possibilidade de ativação por política de ORIGEM (DE:) e/ou DESTINO (PARA:).

Similarmente ao Bounce-mail é o Non-Delivery Report, que é parecido, mas com outra tecnologia de aviso.

Botnet

Botnet (abreviação de rede de bots ou robôs) é uma rede de computadores zumbis controlados remotamente por um hacker. O hacker pode usar a rede para enviar spam e iniciar ataques de DoS (Denial of Service - Negação de Serviço), além de poder alugar a rede a outros criminosos.

BulkMail

O Bulkmail refere-se aquelas correspondências (cartas) enviadas com valores reduzidos, devido a ser considerado envio massivo de correspondência. No MailInspector o conteúdo do e-mail é verificado para que se caracterize a devida pontuação como BulkMail, dessa forma é verificado o contexto do e-mail e se casando com conteúdo de propaganda ou newsletter, passa a ser pontuado o BulkMail.

A título de sistema de proteção a e-mail, eles são similares a GrayMail, ou seja, e-mails em massa que não são considerados SPAMS, podendo ser propagandas que em algum momento foi autorizado pelo usuário, mas que com o passar do tempo, perdeu-se o interesse, mas o usuário manteve-se cadastrado na lista.

CATCH-ALL

É uma função que serve exclusivamente para pegar todas as mensagens enviadas (caso o destinatário não exista no domínio) e encaminhá-las para um e-mail definido pelo administrador do sistema.

A vantagem desse processo é que não há perda de mensagem, mesmo que o remetente tenha digitado errado o destinatário da mensagem, como por exemplo: No lugar do e-mail **pedro@empresa.com.br** o remetente tenha digitado **pedr@empresa.com.br** que por padrão seria rejeitado, por não existir o e-mail **pedr@empresa.com.br** na empresa. Com o catch-all, o e-mail "errado" passaria a ser entregue a uma outra caixa postal, ao qual o administrador posteriormente poderia verificar que foi digitação errada da caixa postal e fazer o encaminhamento correto do e-mail.

Vantagens e desvantagens do catch-all:

- Vantagem:
  - Não há perda de e-mails;
- Desvantagem:
  - Lota rapidamente a capacidade de disco, uma vez que todos os e-mails são encaminhados a caixa postal configurado para catch-all;
  - É desabilitada a proteção de ataque por dicionário (DHA – Dictionary Harvest Attack), uma vez que o sistema tem que receber e-mails de usuários inexistentes e entregue para a caixa configurado para catch-all;
  - Vulnerabilidade a recebimento de campanhas de spam/phishing (uma vez que o criminoso verifica que você recebeu todos os spams/phishing enviados, a sua empresa passa a ser considerada por ele como empresa recebedora de spam/phishing e com isso, o criminoso passa a mandar campanhas constantes de spam/phishing);

No MailInspector é possível ativar o catch-all por dois métodos:

1. Através das ações sobre os e-mails, ao qual você poderá encaminhar todas as mensagens para uma determinada caixa postal, independente se o e-mail foi entregue ou não;
2. Através do DLP, ao qual é possível configurar a ação de encaminhamento dos e-mails para uma caixa postal configurado para o catch-all;

CLI

Interface de linha de comandos (ILC), em inglês comand-line interface (CLI), é um meio de interagir com um programa de computador, onde o utilizador (ou cliente) emite comandos para o programa sob a forma de sucessivas linhas de texto (linhas de comando).

No MailInspector é possível utilizar este tipo de interface para efetuar configurações, execução de scripts próprios ou até mesmo instalar agentes de outras ferramentas, tais como Zabbix, Nagios, etc.

Para acessar a linha de comando é necessário utilizar protocolo SSH.

Cluster

Em um sistema computacional, um cluster é um grupo de servidores e outros recursos que agem como um único sistema e permite a alta disponibilidade e balanceamento de carga, com processamento paralelo.

No MailInspector, é possível formar múltiplos clusters no mesmo sistema, bem como incluir nodes em datacenters distintos, com a forma de trabalho ativo/ativo ou ativo/passivo. Todo o cluster pode ser gerenciado em uma única interface centralizada, sem necessidade de carga de múltiplas janelas de gerenciamento. É possível efetuar o aumento do cluster adicionando novo node a estrutura, sem necessidade de aquisição de novas licenças ou novos módulos.

Os dados acumulados pelos nodes são enviados e armazenados no sistema de gerenciamento centralizado, com uso de banco de dados com tabelas criptografadas, dessa forma assegurando a integridade e segurança dos dados, bem como excelente performance.

Código Malicioso

Termo usado para se referir a programas desenvolvidos para ações danosas e atividades maliciosas em um computador ou dispositivo móvel. Normalmente são projetados para interromper sistemas, ganhar acesso não autorizado ou coletar informações sobre o sistema ou usuário sob ataque.

O MailInspector possui várias camadas de detecção de código malicioso, indo desde o sistema duplo de antivírus (ESET e o antivírus nativo HSC SmartDefender antivírus - dois fabricantes distintos, para maior segurança e abrangência), além de consulta a BigData e SandBox (opcionalmente este conta também com ESET como antivírus em segundo plano).

Criptografia de E-mail

Trata-se de um conjunto de regras que visa codificar a informação de forma que só o emissor e o receptor consigam decifrá-la.

Os dois tipos de criptografis de e-mails mais utilizados são:

Método Push

No método push, o MailInspector envia um e-mail ao destinatário para que ele faça o cadastro no appliance através de uma página HTTPS do Browser (sem uso de cache). Após o cadastro, é envido um e-mail ao destinatário contendo um anexo criptografado nele. Junto nesse e-mail, tem um link que leva o usuário a fazer um cadastro no appliance através de uma página HTTPS do Browser (sem uso de cache). Após efetuado o cadastro (caso ele ainda não tenha sido cadastrado anteriormente),

ele acessa o appliance, onde é apresentado a senha de descriptografia do anexo. Ao abrir o anexo, o usuário tem acesso ao e-mail.

Esse método contém uma grande falha de segurança, uma vez que o usuário está abrindo o e-mail localmente, sendo passível de captura das informações por keylogger, entre outras formas de vulnerabilidade, por isso, sempre recomendamos uso do método Pull.

Método Pull

No método pull, o MailInspector envia um e-mail ao destinatário para que ele faça o cadastro no appliance através de uma página HTTPS do Browser (sem uso de cache). Após esse cadastro, o destinatário consegue acessar o e-mail pelo browser (HTTPS) e efetuar a leitura, ou seja, o e-mail na verdade nunca saiu do appliance, todo o acesso e leitura é pelo browser como se fosse um webmail.

As ações sobre o e-mail (responder, encaminhar, até mesmo a validade do e-mail criptografado), são definidas pelo administrador do appliance.

O MailInspector possui criptografia embutida no próprio sistema, sem necessidade de aquisição de equipamento separado, nem instalação de aplicativos e/ou plugins para este fim. A criptografia utilizada no MailInspector segue de acordo com as principais normas de conformidade, tais como HIPAA, PIPEDA (Personal Information Protection and Electronic Documents Act), PCI-DSS, SOX e GLB.

DBCS (Double Byte Character Set)

O DBCS (Conjunto de caracteres de byte duplo) é uma codificação de caracteres na qual os caracteres (incluindo caracteres de controle) são codificados em dois bytes.

O DBCS suporta idiomas nacionais que contêm um grande número de caracteres ou símbolos exclusivos (o número máximo de caracteres que podem ser representados com um byte é de 256 caracteres, enquanto dois bytes podem representar até 65.536 caracteres). Exemplos de tais idiomas incluem japonês, coreano e chinês.

O MailInspector possui suporta tanto a DBCS, quanto a UTF-16 e UTF-8.

DHA (Directory Harvest Attack – Ataque de Dicionário)/DHAP (Directory Harvesting Attack Prevention)

Ataque de dicionário de nomes, consiste em formar endereços de e-mail a partir de listas de nomes de pessoas, de palavras presentes em dicionários e/ou da combinação de caracteres alfanuméricos. O hacker manda um ataque em massa para uma determinada empresa com múltiplos e-mails com os nomes desse dicionário criado. Se não retornar e-mail de erro de usuário inexistente, é porque o usuário existe e com isso ele vai validando uma lista de e-mails.

O MailInspector possui um sistema de proteção específico contra este tipo de ataque, ao qual é possível indicar a quantidade de ocorrência de usuário desconhecido oriundos de uma única origem por um determinado tempo. Se o limite for ultrapassado, a origem é bloqueada automaticamente por uma hora.

Digest (Notificação de Quarentena)

Notificação de Quarentena é uma lista de todos os e-mails que foram identificados como spam ou bloqueador por outra forma, como por exemplo com anexos contaminados por malware, etc. Esses e-mails são colocados em quarentena pelos módulos de segurança do MailInspector.

O appliance enviará o resumo da quarentena como um e-mail a todos os usuários em um determinado horário agendado pelo administrador, e os usuários poderão classificar o remetente do e-mail em quarentena como válido ou inválido e liberá-los em suas caixas de entrada pessoais, se necessário.

No MailInspector é possível criar diversos agendamentos de envio da notificação de quarentena, de acordo com o administrador, podendo ser separados por grupos, usuários específicos, range de IP, etc. O administrador também pode customizar toda a mensagem do e-mail enviado, mudar a logomarca e cores. Também pode configurar quais pastas de quarentena serão liberadas aos usuários, por exemplo: Liberar no digest o conteúdo da pasta de quarentena VIRUS para o gerente de TI, com isso, no digest do gerente de TI também aparecerão os e-mails bloqueados como VÍRUS junto aos outros e-mails quarentenados (spams).

DKIM

DKIM é uma especificação do IETF que define um mecanismo para autenticação de e-mail baseado em criptografia de chaves públicas. Através do uso do DKIM, uma organização assina digitalmente as mensagens que envia, permitindo ao receptor confirmar a autenticidade da mensagem. Para verificar a assinatura digital, a chave pública é obtida por meio de consulta ao DNS do domínio do assinante.

Ao contrário do SPF, que verifica somente o envelope, o DKIM verifica o cabeçalho da mensagem. Esta técnica acarreta um custo computacional adicional por mensagem, tanto para o MTA remetente quanto para o receptor.

Para habilitar DKIM é necessário:

- Criar um par de chaves pública e privada (o OpenSSL pode ser usado para isso);
- Deixar a chave pública disponível via DNS, de forma semelhante à publicação da política do SPF;
- Colocar a chave privada no MTA responsável pelo envio das mensagens;

Para utilizar DKIM no envio de mensagens basta assinar cada mensagem enviada com a chave privada colocada no MTA. Esta assinatura é enviada como um campo adicional do cabeçalho.

Para verificar a autenticidade de uma mensagem recebida é necessário:

- Obter a chave pública do domínio do From:, via DNS,
- Verificar a assinatura da mensagem;

O resultado da verificação da assinatura pode chegar a uma das três conclusões:

- A assinatura é válida, a mensagem vem realmente do domínio indicado no campo From: e pode então ser avaliada por outras técnicas anti-spam;
- A assinatura não é válida, a mensagem pode ser marcada como suspeita ou ser recusada;
- O domínio do remetente não possui um registro DKIM, não sendo possível usar a informação de DKIM como critério de decisão.

O MailInspector possui suporte a DKIM, podendo tomar as seguintes ações após a análise: Pontuar, Bloquear ou Ignorar. É possível também configurar o MailInspector para efetuar a assinatura de DKIM nos e-mails de saída.

DLP (Data Loss Prevention)

O Data Loss Prevention (Prevenção de Perda de Dados) é um sistema utilizado pelas empresas para garantir que dados confidenciais não sejam perdidos, acessados por pessoas não autorizadas, roubados, mal utilizados ou vazados por usuários mal-intencionados. Esse sistema consiste em um conjunto de políticas de segurança e regras que podem ser aplicadas com a ajuda de softwares especializados para reforçar o bloqueio contra possíveis invasores.

No MailInspector, o DLP permite criar regras de compliance, através da composição e combinação de regras por: qualquer parte do cabeçalho (header) da mensagem, pela análise do conteúdo da mensagem (body), pela análise da mensagem no seu formato original (raw), pela avaliação do conteúdo dos arquivos anexados a mensagem (DOC, XLS, PDF, DOCX, XLSX, PPS, PPSX, ODF, ODT, ODS, ODP, PPT, HTML e outros) e pela verificação das URL's contidas no corpo da mensagem. Podendo criar dicionários de palavras, através de expressões regulares que combinem com qualquer campo da mensagem ou conteúdo do anexo. Permitindo definir o número de repetições de um mesmo dicionário de palavras, para considerar que a regra combina com a mensagem, através da concatenação das regras por operações booleanas. Desta forma é possível determinar a ação que será tomada para cada conjunto de regras. O Sistema permite criar múltiplas regras de filtragem combinando uma ou mais regras e determinado as ações que serão tomadas por cada regra.

O sistema permite que sejam criados Dicionários de dados compatíveis com as principais normas de regulamentação do mercado, tais como: SOX, GLBA, HIPPA e outros.

DMARC

DMARC é uma sigla em inglês para "Mensagem Baseada em Domínio de Autenticação, Relatório e Conformidade", é uma proposta de normatização para garantia de autenticidade de um e-mail, e tem sido muito bem aceita e largamente adotada, inclusive por grandes players como Google e Microsoft.

Para o bom funcionamento do DMARC, é preciso que o SPF e DKIM estejam devidamente configurados e em funcionamento. O DMARC é basicamente um novo padrão que visa unificar as validações atuais.

Com o DMARC devidamente configurado, é possível detectar origens de fraudes de e-mail que usam o domínio da empresa.

O Mail Inspector é compatível com uso de DMARC, podendo gerar os relatórios para envio nos sistemas com DMARC e também configurar o DMARC para as ações com falha ou sucesso de verificação de DMARC, ao qual poderá: Bloquear, Ignorar ou Pontuar no cálculo de spam.

DNS

Do inglês Domain Name System, o sistema de nomes de domínios, responsável pela tradução, entre outros tipos, de nome de máquinas/domínios para o endereço IP correspondente e vice-versa.

Para o sistema de e-mails, as duas principais funções do DNS é apontamento de entregados e-mails e protocolos de segurança inclusos no sistema de DNS, tais como SPF, DKIM e DMARC.

Domain-Wide

Domain-Wide ou Delegação em todo o domínio é um recurso que permite que você conceda aos aplicativos permissão para acessar os dados dos usuários sem exigir o consentimento deles, ou seja, habilita que um aplicativo via API envie e receba e-mails direto, como se fosse um usuário.

O MailInspector possui filtros customizáveis para esse tipo de conta, para isso, basta criar um grupo para esses e-mails e criar regras customizadas sobre eles, tais como pontuação diferente para detecção de spam ou atuação do filtro de anti-vírus de forma distinta, ou ainda autorização para recebimento de anexos compactados com senha, entre outras ações.

DoS (Negação de Serviço)

É um ataque que tenta saturar um servidor ou a rede com um volume de tráfego (malicioso ou não) tão grande que faz com que o recurso não consiga realizar suas funções. Este tipo de ataque geralmente usa redes contaminados (BOTNET) para essa finalidade.

Quando uma série de BOTNETS atacam um único indivíduo ou um único sistema ele passa de DoS para DDoS (Distributed Denial of Service).

Para prevenir este tipo de ataque, o MailInspector possui controle de conexões, ao qual é possível limitar a quantidade de conexão de um único ponto, bem como controle de limite de tempo de conexão, dessa forma se uma conexão "demorar" para encerrar, o mesmo pode ser descartado. Essa proteção funciona tanto a nível de sistema operacional, quanto a nível de MTA.

E-mail Bomb

É uma forma de ataque que consiste em enviar grandes volumes de e-mail para um determinado endereço, na tentativa de sobrecarregar a caixa de correio, dessa forma sobrecarregando o servidor em que o endereço de e-mail está hospedado.

Para prevenir este tipo de ataque, o MailInspector possui controle de conexões, incluindo módulo para verificação de surtos e-mails dirigidos a endereços inválidos, bloqueando o IP de origem do atacante.

Engenharia Social

A engenharia social, no contexto de segurança da informação, refere-se à manipulação psicológica de pessoas para a execução de ações ou divulgar informações confidenciais. Este é um termo que descreve um tipo psicotécnico de intrusão que depende fortemente de interação humana e envolve enganar outras pessoas para quebrar procedimentos de segurança. Um ataque clássico na engenharia social é quando uma pessoa se passa por um alto nível profissional dentro das organizações e diz que o mesmo possui problemas urgentes de acesso ao sistema, conseguindo assim o acesso a locais restritos.

A maioria das técnicas de engenharia social consiste em obter informações privilegiadas enganando os usuários de um determinado sistema através de identificações falsas, aquisição de carisma e confiança da vítima. Um ataque de engenharia social pode se dar através de qualquer meio de comunicação. Tendo-se destaque para telefonemas, conversas diretas com a vítima, e-mails e páginas web.

Expressão Regular / RegEx

Expressões regulares são escritas numa linguagem formal que pode ser interpretada por um processador de expressão regular, um programa que serve um gerador de analisador sintático ou examina o texto e identifica as partes que casam com a especificação dada.

No MailInspector é possível utilizar expressão regular para quase tudo, isto é, desde a parte de criação de Grupos de Usuários, até mesmo em dicionários para bloqueio inteligente de expressões, tais como exitar vazamento de número de cartão de crédito ou bloqueio de um e-mail com a palavra TABELA DE PREÇO no corpo do e-mail, mas detectado as variações tanto em maiúsculo e minúsculo. Para maiores informações vá em Apêndice 3 – Expressões Regulares.

Falso Positivo

É quando um e-mail é barrado como spam ou com conteúdo malicioso e ele na verdade não é spam, nem ameaça. Isso ocorre quando o e-mail possui muitos atributos que o caracteriza como spam ou anexo com características de malware, dessa forma "enganando" o sistema de proteção a e-mail. O contrário também pode ocorrer, gerando incidência de falso negativo.

No MailInspector o usuário pode reportar um falso positivo. Na notificação de quarentena individual, o próprio usuário pode reportar através de um link o e-mail quarentenado como falso positivo, dessa forma a HSCBRASIL analisará o e-mail reportado através de Inteligência Artificial e sequencialmente também analisará através de um especialista e uma vez confirmado o Falso Positivo, será criada uma assinatura específica referente ao e-mail.

Falso Negativo

É quando o sistema de proteção a e-mail deixa passar um spam ou e-mail com conteúdo malicioso. O contrário também pode ocorrer, gerando incidência de falso positivo.

File Fingerprint

A impressão digital de arquivos, também conhecida como impressão digital de dados ou impressão digital de documentos, é uma técnica empregada por muitas soluções de prevenção de perda de dados (DLP) para identificar e rastrear dados em uma rede/e-mail.

A impressão digital de documentos é realizada por algoritmos que mapeiam dados como documentos e arquivos para seqüências de texto mais curtas, também conhecidas como impressões digitais. Essas impressões digitais são identificadoras exclusivos para seus dados e arquivos correspondentes, assim como as impressões digitais humanas identificam exclusivamente pessoas individuais.

A impressão digital do documento é usada para identificar informações confidenciais, para que possam ser rastreadas e protegidas adequadamente. À medida que os funcionários continuam produzindo e manipulando vários tipos de dados e informações sensíveis em quantidades cada vez maiores, a impressão digital de dados fornece uma técnica escalável para identificar, monitorar e aplicar controles de proteção aos dados à medida que eles se movem pela rede corporativa ou entram/saem por e-mails.

No caso do MailInspector, o File Fingerprint é utilizado para rastrear e-mails contendo o(s) arquivo(s) previamente enviado(s) e processado(s) pelo sistema de proteção a e-mails.

FIPS 140-2

Uma das normas publicadas pelo NIST (National Institute of Standards and Technology) é o Federal Information Processing Standard Security Requirements for Cryptographic Modules, chamado de FIPS 140-2.

O FIPS 140-2 fornece uma norma que pode ser requerida pelas agências federais dos EUA que especificam que os sistemas de segurança baseados em criptografia devem ser usados para fornecer proteção para dados sensíveis ou importantes.

O MailInspector por padrão trabalha tanto com FIPS 140-2 quanto com NIST SP800-131a (que requer comprimentos de chaves maiores e criptografia mais forte.do que a FIPS 140-2).

Fuzzy Hashing

Fuzzy Hash é similar ao hash, só que em vez de ser feito sobre um único hash, no elemento analisado, é gerado uma série de "mini-hashes" e efetuada a comparação desses "mini-hashes". Dessa forma é possível indicar em percentual a semelhança entre elementos.

Por exemplo:

Em uma lista de frutas (lista1): **Maçã, banana, melão, mamão e melancia**

Em comapação de outra lista (lista2): **maca, banana, melão, mamão e melancia**

Repare que a diferença da lista1, para lista2 é a maçã, que na lista 1 está com **M** (**maiúsculo** e tem **Ç**)

Se fosse comparado só com hash, como retorno, teria dado diferença entre os hashes e não "casaria" os arquivos.

Já no caso de Fuzzy Hash, ele daria semelhança de 71%.

Nessa mesma linha de pensamento com o processo de Fuzzy Hash, é possível detectar VARIANTES de malwares antes mesmo de ter sido criada uma vacina.

O MailInspector utiliza o Fuzzy Hash para análise de dados no BigData e detecção de vírus e malwares.

É importante lembrar que o hash e Fuzzy hash são metadados, ou seja, são registros únicos criados a partir do arquivo analisado, sem vínculo algum com o arquivo original e não são identificáveis. Esses metadados são utilizados para comparação com os dados do BigData, dessa forma atendendo a Lei Geral de Proteção de Dados Pessoais, uma vez que é dado sensível para **prevenção à fraude e à segurança da pessoa**.

> Conforme o Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses:
>
> > g) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.

GUI (Graphical User Interface)

Interface gráfica do utilizador ou usuário, abreviadamente, o acrônimo GUI, do inglês Graphical User Interface é um tipo de interface do utilizador que permite a interação com dispositivos digitais por meio de elementos gráficos como ícones e outros indicadores visuais, em contraste a interface de linha de comando.

No MailInspector é utilizada este tipo de interface para criação de políticas e outras configurações/customizações do sistema, sem necessidade do administrador utilizar linha de comando. Esta interface é única ao qual gerencia TODOS os pontos do cluster, sem necessidade de abrir novas interfaces e/ou acessar outros sistemas. É utilizado o protocolo HTTP/HTTPS para o acesso a interface GUI (Interface Gráfica).

Greylist

Greylisting é um recurso que ajuda a verificar se um servidor de envio de e-mail é um servidor de e-mail real, em vez de um spammer.

Quando um e-mail é recebido de um domínio que não enviou recentemente um e-mail para o seu domínio, a função Greylisting solicitará o reenvio do servidor de envio de e-mail.

As regras SMTP determinam que todos os servidores de e-mail são obrigados a reenviar a mensagem (o padrão para o Microsoft Exchange é de 5 minutos). Os spammers não usam servidores de e-mail e não reenviam a mensagem.

Servidores de e-mail legítimos reenviarão a mensagem. A greylist evitará que muitos e-mails de spam sejam baixados pelo servidor, reduzindo quantidade de e-mails que precisam ser processados pelo MailInspector.

Hash

Hash é uma sequência de bits geradas por um algoritmo de dispersão, em geral representada em base hexadecimal, que permite a visualização em letras e números (0 a 9 e A a F), representando um nibble cada.

O conceito teórico diz que "hash é a transformação de uma grande quantidade de dados em uma pequena quantidade de informações".

Essa sequência busca identificar um arquivo ou informação unicamente. Por exemplo, uma mensagem de correio eletrônico, uma senha, uma chave criptográfica ou mesmo um arquivo.

O MailInspector utiliza o hash para busca no BigData de forma sigilosa, uma vez que hash e Fuzzy hash são metadados (não são os arquivos dos anexos), ou seja, o hash do elemento analisado não tem identificação, dessa forma atendendo a Lei Geral de Proteção de Dados Pessoais, uma vez que é dado sensível para **prevenção à fraude e à segurança da pessoa**.

> Conforme o Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses:
>
> > g) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.

HTTP/HTTPS

Protocolos de transferência de hipertexto seguros e não seguros (HTTP / HTTPS), embora não estritamente transporte de e-mail, são frequentemente usados por aplicativos de webmail para exibir e-mails que são armazenados remotamente.

As comunicações HTTP geralmente ocorrem no número da porta TCP 80; Comunicações HTTPS normalmente ocorrem no número da porta TCP 443.

O MailInspector por padrão usa o protocolo HTTPS (Porta 443) para acesso da sua Interface de Gerenciamento. É possível substituir o certificado digital autoassinado, por um de uso exclusivo da empresa.

Imagens Pornográficas

Para o contexto de pornografia no e-mail, devemos considerar para tal finalidade, detecção de nudes, imagens de relacionamento sexual com ênfase a órgãos sexuais.

O MailInspector utiliza o módulo de SmartDefender para análise de imagens pornográficas com técnicas de redes neurais e sistema de Machine Learning. Em primeira instância, já é verificada se a imagem está cadastrada em uma rede neural de imagens pornográficas. Após essa etapa é acionado o modelo de Machine Learning, ao qual o sistema verifica vários parâmetros da imagem (incluindo o contexto da mensagem) e a pontua.

Para a análise da imagem são considerados vários parâmetros, dentre eles:

- Cor da pele;
- Tamanho da imagem analisada (cobertura) em relação ao tamanho total;
- Curvatura do corpo;
- Comparação da imagem com o fundo;

IMAP

O IMAP (Internet Message Access Protocol) é um protocolo padrão usado por clientes de e-mail para recuperar e-mail que foi entregue e armazenado em um servidor de e-mail.

Geralmente, as comunicações IMAP ocorrem no número da porta TCP 143.

A menos que configurado para disponibilidade offline, os clientes IMAP normalmente baixam apenas cabeçalho da mensagem. Eles baixam o corpo da mensagem e os anexos apenas quando o usuário do e-mail seleciona para ler o e-mail.

Ao contrário do POP3, quando um cliente IMAP baixa um e-mail para o computador do usuário de e-mail, uma cópia do o e-mail permanece no disco rígido do servidor de e-mail. A vantagem disso é que habilita o e-mail usuários visualizem e-mails de mais de um computador. Isso é especialmente útil em situações em que mais de uma pessoa pode precisar visualizar uma caixa de entrada, onde todos os membros de um departamento monitorar uma caixa de entrada coletiva. A desvantagem disso é que, a menos que os usuários de e-mail excluam o e-mail, O IMAP pode consumir mais rapidamente o espaço em disco do servidor.

O MailInspector permite escanear e-mails de servidores POP3/IMAP externos. O HSC Mailinspector permite configurar contas de servidores POP3/IMAP externo e baixar elas para que sejam filtradas contra Vírus, SPAMs e demais ameaças.

IOC

IOC's são eventos mal-intencionados conhecidos individualmente que indicam que uma rede ou um computador já foram violados. Ao contrário de definições de alerta, esses indicadores são considerados como evidência de uma violação. Muitas vezes, eles são vistos depois que um ataque já foi executado e o objetivo foi atingido, como roubar os dados. Monitorar os IOC's também é importante durante as investigações forenses. Embora ele não possa fornecer a capacidade de intervir em uma cadeia de ataque, coletar esses indicadores pode ser útil na criação de defesas melhores para possíveis ataques futuros.

O MailInspector utiliza o SmartDefender para consulta dos IOC's, dessa forma detectando campanhas maliciosas já realizadas anteriormente e prevenindo que as empresas sofram de um ataque que já tenha sido registrado anteriormente.

Keylogger

É um tipo específico de spyware. Programa capaz de capturar e armazenar as teclas digitadas pelo usuário no teclado do computador, os modelos mais avançados chegam a captuar a tela quando o usuário clica no mouse.

Normalmente os keyloggers capturam e armazenam todas as atividades do teclado, permitindo que alguém ou outro aplicativo examine os registros das teclas para obter informações valiosas como credenciais de logon e números de cartão de crédito, por exemplo. No entanto, existem programas legítimos de registro do uso do teclado, utilizados por empresas para monitorar funcionários e por pais que desejam controlar seus filhos.

O MailInspector utiliza ESET e HSC SmartDefender para detectar esse tipo de ameaça, entre outros.

LOG / LOG de EVIDÊNCIA

É o processo de registro de eventos relevantes num sistema computacional. Esse registro pode ser utilizado para restabelecer o estado original de um sistema ou para que um administrador conheça o seu comportamento no passado.

No MailInspector, através do Log de Eventos, é possível visualizar e filtrar os registros das ações realizadas pelos usuários e administradores através da interface de administração do HSC MailInspector. Permitindo auditar todas as ações tomadas pelos usuários a fim de identificar quaisquer abusos ou ações indevidas.

Além do log de Eventos (logs das ações tomadas no MailInspector), é possível verificar os logs do MTA, onde pode visualizar, filtrar e aplicar ações nos registros das mensagens processadas pelo MTA do HSC MailInspector. Este recurso nos permite diagnosticar problemas no recebimento de mensagens tais como: servidor de origem não tem endereço reverso cadastrado (reverse DNS LookUp - rDNS), destinatário inválido, servidor de origem listado em RBL entre outros motivos.

O MailInspector também possui logs referentes a cada e-mail recebido, isto é, o nível de log gerado é desde a conexão MTA (de entrada), passando pelo log de processamento da mensagem (log de análise de filtros spam, log de antivírus e outros) e por último log de Evidência na entrega (SAÍDA do e-mail do sistema de e-mail gateway ao servidor destino). Se necessário, é possível configurar o envio desses logs diretamente por Syslog ou por consulta direta via RealTime > E-mails, que mostra de forma gráfica a interpretação desse log (por tags de status do e-mail ou até mesmo indicação de entrega ou quarentena de forma gráfica).

Malware

Malware (abreviatura para “software malicioso”) é considerado um tipo de software irritante ou malígno que pretende acessar secretamente um dispositivo sem o conhecimento do usuário. Os tipos de malware incluem spyware, adware, phishing, vírus, Cavalos de Tróia, worms, rootkits, ransoware e sequestradores de navegador.

O MailInspector utiliza ESET e HSC SmartDefender para detectar esse tipo de ameaça, entre outros.

Mass Mailing Worm (Worm de Mala Direta)

Um worm de mala direta é um programa de computador corrompido que tem a capacidade de se copiar e criar links para sites infectados e distribuir as cópias por e-mail. Esses e-mails podem ser espalhados automaticamente, usando endereços de e-mail coletados dos seus contatos de e-mail ou manualmente pelo hacker.

O MailInspector utiliza ESET e HSC SmartDefender para detectar esse tipo de ameaça, com verificação dos links nos e-mails, conteúdos maliciosos e detecção de e-mails fraudulentos, entre outras técnicas.

Mime-Type

MIME é a abreviação de Multipurpose Internet Mail Extensions. É um padrão originalmente desenvolvido para estender e-mails para suportar mais formatos como texto não-ASCII e anexos em formato de imagem, áudio, vídeo ou arquivos executáveis. O tipo MIME é parte do cabeçalho do MIME e especifica o tipo de mídia contido em um e-mail.

Os servidores da Web e os navegadores contêm uma lista de tais Tipos MIME que os ajudam a identificar e, assim, interpretar todos os tipos de arquivos, independentemente do sistema operacional e do hardware utilizados pelo usuário.

Tipos MIME são estruturados de uma certa maneira, contendo um tipo e um subtipo. Por exemplo, o Tipo MIME de uma imagem .jpg é image / jpeg com “image” sendo o tipo e “jpeg” sendo o subtipo. Uma barra (/) é usada para separar o tipo do subtipo.

O MailInspector já vem com vários tipos de mime-types cadastrados, sendo atualizados constantemente nas assinaturas. Também é posspivel incluir novos tipos de Mime-Type, cadastrando-os e utilizando em regras específicas.

MTA

Um agente de transporte de e-mail ou MTA, acrônimo para Mail Transfer Agent é um programa de computador responsável por transferências de mensagens de correio eletrônico entre um computador e outro, utilizando a arquitetura de aplicações cliente-servidor. Um MTA implementa as porções cliente (envio) e servidor (receptor) do Simple Mail Transfer Protocol (SMTP).

O HSC MailInspector® é um Gateway de E-mails "MTA" padrão protocolo SMTP/SMTPS e POP3 que foi desenvolvido para prover segurança e performance no fluxo de entrada e saída de e-mails de sua empresa, oferecendo proteção em tempo real através da utilização de 28 camadas de filtragem.

MUA

Mail User Agent (MUA), ou cliente de e-mail, é um software (como o Microsoft Outlook/Mozilla Thunderbird, Windows Live Mail, IncrediMail, Zimbra DeskTop, etc) que permite usuários para enviar e receber e-mail.

Non-Delivery Report Attack

O Non-Delivery Report (NDR) é relatório de falha na entrega e é gerado automaticamente por um servidor de e-mail para informar ao remetente que a mensagem de e-mail não foi entregue com êxito. O NDR ao contrário do Bounce-mail (que é o retorno de e-mail gerado pelo servidor de destino), é um relatório do próprio servidor de origem, enviando ao remetente, indicando que o e-mail não teve sucesso na entrega. Esse relatório é muito comum com a Microsoft, Yahoo e outros servidores de e-mail de grande porte e para gerar esse relatório, o sistema baseia-se no Bounce Mail, uma vez recebido o e-mail de Bounce Mail (que é "ruim" para o usuário final interpretar o erro, o servidor, gera um e-mail de Non-Delivery Report, que é um e-mail mais fácil de interpretar).

Para o ataque, o criminoso cria um e-mail falso com a mesma "cara" do e-mail de Non-Delivery Report e manda para a vítima, geralmente com link malicioso (phishing), que dá para uma página parecida com o do fabricante, onde terá formulário e/ou arquivos maliciosos para download automático.

O MailInspector detecta este tipo de ataque e faz a prevenção pelo Bounce TAG Verification (caso ele tenha feito um e-mail falso de Bounce Mail), além de verificar todos os links contidos no falso e-mail de Non-Delivery-Report, desabilitando por completo esse ataque.

NTP

NTP (Network Time Protocol), é protocolo que permite a sincronização dos relógios dos dispositivos de uma rede, como servidores, estações de trabalho, roteadores e outros equipamentos, a partir de referências de tempo confiáveis. No Brasil o mais utilizado é o ntp.br.

No MailInspector esta configuração pode ser efetuada na parte de Administração > Configuração de Rede, ao qual é configurado um NTP para cada placa de rede utilizada pelo appliance.

PCI/DSS

A Norma de Segurança de Dados da Indústria de Cartões de Pagamento (PCI DSS) é uma norma internacional que visa ajudar a prevenir a fraude nos cartões de crédito, aumentando o controle em torno dos dados dos titulares de cartões.

O MailInspector já inclui expressões regulares (RegEx em dicionário de palavras) que podem ser usadas para identificar dados sensíveis de cartões de crédito que estão sujeitos à proteção sob o PCI DSS. Esses dicionários podem ser utilizados em regras de DLP:

- Números de Cartões de Crédito
  - Visa
  - American Express
  - MasterCard
  - Discover
- Código CVV de 3 dígitos (usados em cartões de crédito padrão Visa, MasterCard, Discover)
- Código CID de 4 dígitos (usado para cartão de crédito American Express)

- Data de expiração do cartão de crédito

Além disso, o PCI DSS protege todos os dados do titular do cartão, não apenas aqueles que podem ser facilmente identificados por expressões regulares. A conformidade efetiva com o PCI DSS requer uma abordagem abrangente à segurança da informação que vai além da simples identificação de dados do titular do cartão. Isso pode incluir medidas como criptografia de dados em repouso e em trânsito, controles de acesso rigorosos, auditoria e monitoramento de acessos e muito mais.

PGP

Pretty Good Privacy. Programa que implementa criptografia de chave simétrica, de chaves assimétricas e assinatura digital. Possui versões comerciais e gratuitas.

No MailInspector é possível a configuração de exceção de reescrita de URL's em caso de as mensagens estarem assinadas com: PGP, S/MIME e DKIM.

Phishing

É uma forma de roubo de identidade em que o fraudador utiliza um e-mail que parece autêntico de uma empresa legítima, para induzir destinatários a fornecer informações pessoais confidenciais, como números de cartão de crédito, conta bancária, seguro social ou outras informações pessoais confidenciais. A mensagem do e-mail falso convida o destinatário a clicar em um link para atualizar seu perfil pessoal ou realizar alguma transação, levando a vítima a um site falso em que todas as informações inseridas são encaminhadas diretamente ao fraudador.

POP3

Post Office Protocol versão 3 (POP3) é um protocolo padrão usado por clientes de e-mail para recuperar e-mail que foi entregue e armazenado em um servidor de e-mail.

Geralmente, as comunicações POP3 ocorrem no número de porta TCP 110.

Ao contrário do IMAP, depois que um cliente POP3 faz o download de um e-mail para o computador do usuário de e-mail, uma cópia do e-mail geralmente não permanece no disco rígido do servidor de e-mail.

A vantagem disso é que libera espaço no disco rígido no servidor. A desvantagem disso é que o e-mail baixado geralmente reside em apenas um computador pessoal, com isso, se o usuário tiver múltiplos dispositivos, somente conseguirá receber e ver o e-mail no primeiro dispositivo que tiver baixado o conteúdo.

A menos que todos os seus clientes POP3 estejam sempre configurados para deixar cópias de e-mail no servidor, usuários de e-mail que usam vários computadores para visualizar e-mails, como um desktop e laptop, não será capaz de ver de um computador qualquer um dos e-mails anteriormente baixado para outro computador.

O MailInspector permite escanear e-mails de servidores POP3/IMAP externos. O HSC Mailinspector permite configurar contas de servidores POP3/IMAP externo e baixar elas para que sejam filtradas contra Vírus, SPAMs e demais ameaças.

Quarentena de E-mail

Quarentena de e-mail é o local onde são armazenados os e-mails considerados spam/possível spam ou e-mails considerados ameaças ao usuário final.

A quarentena de e-mail oferece uma forma mais conveniente de gerenciar os e-mails “rejeitados”, ou com anexos infectados contendo malware ou mensagens de phishing.

Existem motivos diferentes pelos quais as mensagens de e-mail são colocadas na quarentena de e-mail, dependendo de qual a classificação da ameaça.

No MailInspector é possível que o próprio usuário possa gerenciar a quarentena de POSSÍVEL SPAM e SPAM, sendo que para as outras quarentenas são bloqueadas o acesso. O administrador por outro lado, possui total autonomia sobre as quarentenas, sendo de livre acesso e liberação das mensagens quarentenadas.

Existem ainda quarentenas temporárias no sistema ao qual podem ser configuradas o prazo de quarentena. Alguns exemplos de quarentena temporária são:

- Quarentena de Zero Hour: Aguarda até que uma determinada assinatura do antivírus seja lançada. Após isso, o e-mail é novamente reanalisado e liberado ou bloqueado em definitivo;
- Quarentena de assinatura de SPAM: Aguarda até que determinada assinatura de e-mail spam seja detectada e lançada. Após isso, o e-mail é novamente reanalisado e liberado ou bloqueado em definitivo;

No MailInspector ainda é possível criar quarentena customizada, isto é, o MailInspector permite que o administrador crie novas pastas de quarentena. Em E-mail Compliance utilize esta quarentena customizada, através de políticas corporativas próprias.

Ransomware

É um tipo de malware que restringe o acesso ao sistema infectado e cobra um valor de "resgate" para que o acesso possa ser reestabelecido.

O ransomware pode se propagar de diversas formas, embora as mais comuns são:

- Através de e-mails com o código malicioso em anexo ou que induzam o usuário a seguir um link;
- Explorando vulnerabilidades em sistemas que não tenham recebido as devidas atualizações de segurança.

Basicamente existem dois tipos de ransomware:

- Ransomware Locker: impede que você acesse o equipamento infectado.
- Ransomware Crypto: impede que você acesse aos dados armazenados no equipamento infectado, geralmente usando criptografia.

O MailInspector utiliza BitDefender e HSC SmartDefender para detectar esse tipo de ameaça, entre outros.

RBL

Também conhecidas como DNSBL ou Blacklists, RBL (Blackhole Lists) são listas de endereços IP, domínios ou endereços eletrônicos que possuem histórico como fonte de spams.

Essas listas são criadas por centros de inteligências automatizadas que usam técnicas para identificação deste tipo de atividade, por exemplo, a criação de “listas de e-mails” para recebimento de spam (honeypot), fontes de códigos maliciosos. Esses endereços são usados apenas para o recebimento de spams e são divulgados estrategicamente em fóruns e chats usados por spammers. Os spammers ao enviar spams para essas listas, eles ficam registrados nas listas de RBL.

O MailInspector já vem com as principais listas de RBL habilitadas e funcionando:

- HSCBRASIL;
- Spamhaus;
- SpamCop;

Mas também permite que o administrador cadastre novas listas ou até mesmo edite as listas para remoção de algum RBL que ele não deseje utilizar.

Outro ponto importante a ressaltar é que o MailInspector permite que o administrador indique em qual camada a RBL será ativada, ou seja, ela pode ser ativada “antes” da entrada do e-mail no appliance (já barrando a nível de conexão) ou “depois” (na etapa de processamento de cálculo de spam).

Também é possível ao administrador indicar a incidência de vezes nas listas até que o e-mail seja bloqueado, isto é, se um e-mail chega ao MailInspector, o administrador por exemplo pode indicar que esse e-mail obrigatoriamente para que seja bloqueado a nível de RBL, deva constar em pelo menos 5 RBL’s diferentes.

Reputação do Remetente

A grande maioria dos sistemas de proteção a e-mail, utiliza o sistema de verificação de reputação do remetente. Essa análise da reputação do remetente, pode ser de terceiros ou do próprio fabricante e auxilia na detecção de spammers, uma vez que muitos spams são enviados dos mesmos IP’s.

No MailInspector, a reputação é principalmente determinada pela própria HSCBRASIL, através de indicadores de histórico do remetente, bem como histórico do próprio e-mail (verificando se o mesmo já não foi enviado em massa para outros equipamentos ou registros do e-mail em outros fabricantes de segurança). Os outros parceiros de segurança que fornecem informações de ameaças são: ESET e CrowdStrike. Dessa forma cruzam-se as informações em um único BigData, reduzindo dessa forma possíveis falsos positivos. Na consulta da reputação é retornado os seguintes dados do remetente:

- Infraestrutura de rede;
- Registro em blacklists mundiais;
- Configuração de serviço de notificação de envio e autenticidade de mensagens de mensagens como SPF e DKIM.

Return-oriented Programming (R.O.P.)

Return-oriented programming, cuja sigla é R.O.P, em Língua portuguesa programação orientada ao retorno é uma técnica que se incorpora ao retorno de uma função, alterando a saída da instrução RET (return). O ROP pode ser aplicado sem que haja nenhuma injeção de código, na verdade, ele subscreve um trecho de código já existente.

A programação orientada ao retorno age gerando um algoritmo que ao ser injetado numa máquina vulnerável constitui um código binário, ou gadget, que se acopla a partes já existentes de qualquer tipo de programa, como por exemplo .XLS, .DOC, .PPT ou mesmo funcionalidades do próprio sistema operacional. O worm se posiciona junto a uma instrução RET duma função e é colocado dentro da área de execução.

Tarefas bem definidas são realizadas quando um binário malicioso é inserido na pilha e utiliza os ponteiros para sequenciar as instruções RET. O atacante pode realizar qualquer comportamento que desejar, uma vez que posiciona o worm na pilha de execução.

No MailInspector, tanto o sistema de antivírus proprietário (HSC SmartDefender antivírus), quanto o ESET detectam esse tipo de ameaça nativamente, sem necessidade de módulo adicional.

S/MIME

S/MIME para assinatura e criptografia de mensagens. S/MIME (Secure/Multipurpose Internet Mail Extensions) é um método amplamente aceito, ou mais precisamente um protocolo, para o envio de mensagens assinadas e criptografadas digitalmente. S/MIME permite que você criptografe e-mail e os assine digitalmente.

No MailInspector é possível a configuração de exceção de reescrita de URL's em caso de as mensagens estarem assinadas com: PGP, S/MIME e DKIM.

SaaS (Software as Service)

SaaS (Software as a Service) é um modelo de distribuição de software em que aplicativos são disponibilizados pela internet como serviços. Isso significa que os usuários não precisam instalar o software em seus computadores, mas acessam as funcionalidades através da web.

O MailInspector pode ser comercializado como SaaS em Datacenter padrão LGPD, bem como certificações ISO 27001, ISO 22301 e ISAE 3402, ou seja, atende os quesitos da legislação brasileira de proteção a dados, com sistemas de proteção a acesso físico, proteção a incêndio, tier layer 3, sistemas de redundância de alimentação de energia e de fibra ótica para tráfego de dados. O MailInspector utiliza dois datacenters distintos, fisicamente separadas e ambos os datacenters em território nacional, permitindo total auditoria em seus ambientes. atendendo a normativa da Lei Geral de Proteção a Dados.

Maiores informação sobre estrutura utilizada para o SaaS da HSCBRASIL: *MailInspector e seus módulos em Datacenter brasileiro*

SandBox File

Sandbox é um mecanismo de segurança para separar programas em execução, geralmente em um esforço para mitigar falhas de sistema ou vulnerabilidades de software contra propagação. É frequentemente usado para executar programas ou códigos não testados ou não confiáveis, possivelmente de terceiros e não verificados ou que náo estão em conformidade da empresa.

O SandBox File trabalha de duas formas, SandBox Estático e SandBox Dinâmico (com opção de análise local ou envio para nuvem da HSCBRASIL).

Forma Estática de trabalho do SandBox

A forma estática consiste em fazer engenharia reversa do binário, carregando o executável em um desmontador, para obter o código-fonte da linguagem de montagem a partir do código do programa original. Depois disso é feita a análise para saber o que o programa faz.

Algumas das técnicas utilizadas na análise estática são a determinação do tipo de arquivo, cadeias codificadas no arquivo binário, a verificação de ofuscações de arquivos para determinar se o arquivo foi compactado ou determinar se eles usaram criptografia, hash e comparação, verificação de hash em relação a assinatura de vírus.

Forma Dinâmica de trabalho do SandBox

A técnica de análise dinâmica envolve a execução do arquivo e a observação de seu comportamento no sistema, em que o sistema é configurado em um ambiente isolado.

A análise dinâmica nos ajuda a remover a infecção, produzir assinaturas efetivas ou ambas. O ambiente é totalmente isolado e se o arquivo estiver enviando solicitações de rede ou estiver esperando uma resposta, a resposta geralmente é simulada.

A análise dinâmica geralmente se concentra nas seguintes atividades:

- Sistema de arquivos;
- Registro;
- Processo;
- Acesso a Rede;
- Chamadas do sistema;

O MailInspector possui duas formas de utilização do SandBox dinâmico:

1. Localmente (todo o processo de SandBox dinâmico é efetuado em um appliance local, indicado pelo administrador da solução, sem envio de dado algum para a nuvem da HSCBRASIL);
2. Na nuvem da HSCBRASIL (que poupa processamento do equipamento utilizado para de análise do arquivo);

Se for optado pelo uso da nuvem da HSCBRASIL, o envio do arquivo é de forma anônima, ao qual não é rastreável, nem detectável, dessa forma atendendo a Lei Geral de Proteção de Dados Pessoais, uma vez que é dado sensível para **prevenção à fraude e à segurança da pessoa**.

> Conforme o Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses:
>
> > g) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.

Sender ID

Sender ID (definido na RFC 4406) é um protocolo da Microsoft derivado do SPF (de sintaxe idêntica), que valida o campo do endereço da mensagem no cabeçalho, de acordo com RFC 2822. A validação segue um algoritmo chamado PRA (Purported Responsible Address, RFC 4407).

O algoritmo certifica se o campo do cabeçalho com o endereço do e-mail é responsável por enviar a mensagem. Como ele deriva do SPF, pode também validar o MAIL FROM, mas ele irá definir uma nova

identidade e PRA e novos campos de política de envio, substituindo o MAIL FROM (MFROM by Sender ID), PRA, ou os dois.

Sender ID é licenciado pela Microsoft, a despeito de projetos de licença pública e precisa da especificação para PRA na entrada TXT do DNS. Como isso pode causar erros de sintaxe no padrão SPF, que é mais usado, tornou-se uma política pouco implementada.

No MailInspector é possível configurar a pontuação para ser incluída na contagem de spam quanto a mensagem for válida/inválida em relação a Sender ID.

Scareware

Aviso que promete aos usuários de computador uma atualização para cuidar de um problema de segurança urgente quando, na verdade, é o próprio scareware que é a ameaça de segurança maliciosa. Gera receio e "medo" ao usuário de que ele possa estar utilizando um equipamento com programa desatualizado em relação a sua segurança, mas na verdade a própria "atualização" é uma ameaça ao usuário.

É uma técnica muito utilizada em engenharia social. O MailInspector detecta esse tipo de perigo, através de contexto do e-mail, bem como análise dos links onde serão baixadas as "atualizações".

SOX

A Lei Sarbanes-Oxley (SOX) é uma lei dos EUA que estabelece requisitos de relatórios financeiros para empresas de capital aberto. Ela não especifica necessariamente tipos específicos de Informações Pessoais Identificáveis (PII) que devem ser protegidas, como a LGPD. No entanto, ela exige controles internos adequados sobre todas as informações financeiras, que poderiam incluir PII.

O MailInspector possui dicionários relativos a SOX, contendo termos específicos bancários, cartões de crédito e detecção de outros termos financeiros.

Entre os dicionários já contidos no MailInspector para questão financeira/SOX podemos destacar:

- Números de Cartões de Crédito
  - Visa
  - American Express
  - MasterCard
  - Discover
- Número de Seguro Social dos EUA
- Número de PIS/PASEP do Brasil
- Número de Carteira de Trabalho do Brasil
- Número de conta bancária dos EUA
- Data no formato MM/DD/AAA, comumente utilizado em instituições financeiras dos EUA
- Endereços de e-mail

SMTP

Simple Mail Transfer Protocol (abreviado SMTP. Traduzido do inglês, significa "Protocolo de transferência de correio simples") é o protocolo padrão para envio de e-mails através da Internet, definido na RFC 821.

O HSC MailInspector® é um Gateway de E-mails "MTA" padrão protocolo SMTP/SMTPS e POP3 que foi desenvolvido para prover segurança e performance no fluxo de entrada e saída de e-mails de sua empresa, oferecendo proteção em tempo real através da utilização de 28 camadas de filtragem.

Spear Phishing

Spear phishing é um ataque de falsificação de e-mail que tem como alvo uma organização ou indivíduo específico, buscando acesso não autorizado a informações confidenciais. As tentativas de spear phishing geralmente não são iniciadas por hackers aleatórios, são mais propensas a serem conduzidas por criminosos em busca de ganhos financeiros, segredos comerciais ou informações militares.

O MailInspector possui um sistema de proteção específico contra Spear Phishing, chamado de TAP (Targeted Attack Protection). Também conhecido como Proteção a Ataques Dirigidos, esta função faz a reescrita de todo e qualquer link contido no e-mail, para quando o usuário ao clicar no link, é feita nova análise do link para verificação de conteúdo malicioso, tais como vírus, malwares, ransomwares, ou até mesmo formulários indevidos. Essa análise é feita OnClick, simulando um usuário acessando a página e clicando e/ou preenchendo formulários e verificando a ação tomada pela página web, dessa forma detectando falsas páginas web, como páginas falsas de bancos/cartões de crédito ou falsas páginas de órgãos do governo e bloqueando o acesso a essa página.

Quando há anexos no e-mail, se o mesmo não tiver já sido analisado anteriormente e combinado com o sistema de BigData da HSCBRASIL/ESET, o arquivo será executado em uma área de memória reservada e isolada (SandBox) e verificada a ação do arquivo. Uma vez que tenha sido analisada e eventualmente verificado ameaça, é o resultado alimenta a base de dados da HSC/ESET a nível GLOBAL, gerando dessa forma uma base gigantesca de conhecimento de ameaças sem assinaturas (somente análise comportamental), que trabalha em conjunto com sistema de assinatura. Após esse processo, o arquivo é bloqueado e o usuário/administrador alertado (caso o administrador do MailInspector tenha configurado para esse processo).

SPF

SPF é uma tecnologia para combater a falsificação de endereços de retorno dos e-mails (return-path). O mecanismo permite:

- Ao administrador de um domínio: definir e publicar uma política SPF, onde são designados os endereços das máquinas autorizadas a enviar mensagens em nome deste domínio; e
- Ao administrador de um serviço de e-mail: estabelecer critérios de aceitação de mensagens em função da checagem das políticas SPF publicadas para cada domínio.

O HSC Mailinspector pode ser configurado para identificar a autenticidade de mensagens através da verificação do SPF.

O processo de publicação de uma política SPF é independente da implantação de checagem de SPF por parte do MTA, estes podem ou não ser feitos em conjunto.

Após a análise de segurança do SPF, no MailInspector é possível a configuração das ações: Pontuar, Bloquear ou Ignorar.

Spyware

São programas que monitoram e coletam informações pessoais e as enviam a terceiros, sem permissão ou conhecimento do usuário. Muitos usuários instalam spywares de forma não intencional, como por exemplo, quando aceitam o contrato de licença para usuário final (EULA) de certos softwares gratuitos. Um dos spywares mais conhecidos e utilizados pelos hackers são os Keyloggers.

O MailInspector utiliza ESET e HSC SmartDefender antivírus para detectar esse tipo de ameaça, entre outros.

SSH (Secure SHell)

O SSH (Secure SHell) é um protocolo que permite a você acessar virtualmente o servidor como se você estivesse em um terminal (no prompt do DOS, por exemplo). Se você preferir, considere como o SSH como um computador controlando outro computador.

A diferença entre o telnet e o SSH está na segurança. Toda a transmissão de dados no SSH é criptografada. Assim, os riscos de alguém "bisbilhotar" o que você está fazendo no servidor (às vezes você precisa transmitir senhas para acessar outros sistemas ou programas) é virtualmente zero. Fora isso, tudo o que você faz no telnet pode ser feito pelo SSH.

Quando você conecta via terminal remoto com seu servidor, você está controlando aquele servidor a partir de seu sistema operacional. Qualquer comando que você digitar é executado no servidor (e não no seu computador) e você opera de acordo com os paramêtros de comandos do servidor.

No MailInspector o administrador quando utiliza o acesso por SSH, pode por exemplo instalar e/ou configurar agentes de monitoramento, tais como Zabbix, Nagios, entre outros. Também é possível alterar serviços e outras configurações, desde que tenha permissão para isso.

SSL (Secure Sockets Layer)

O protocolo SSL é o protocolo originário de segurança de comunicação utilizado entre duas pontas de servidores. Ele foi substituído pelo TLS. Vide TLS para maiores informações.

TAP (Targeted Attack Protection)

Um ataque dirigido (Targeted Attack) usa um tipo de crimeware ou programa de malware projetado para atacar a entidade de destino. Primeiro, os perpetradores de ataques de alvo tipicamente analisam a empresa/sistema/usuário alvo, seus mecanismos de segurança subjacentes e possíveis ramificações pós-ataque.

Por exemplo, iniciar um ataque de destino em um banco requer um entendimento de sua arquitetura de segurança e possíveis brechas. Quando um ataque é bem-sucedido, o invasor pode interromper as operações bancárias de rotina, transferir fundos ilegalmente e extrair informações financeiras do cliente.

O MailInspector possui um sistema de proteção contra esse tipo específico de ataque, ao qual analisa as mensagens de e-mails, URL's e Anexos em busca de de malwares, vírus e informações maliciosas para proteção a ataques dirigidos, com utilização de Sandbox.

O Modulo de Proteção contra ataque dirigido atua em diversas camadas do produto garantindo uma maior segurança aos usuários finais.

TLP (Traffic Light Protocol)

O TLP é um conjunto de quatro marcações (labels) usadas para indicar os limites de compartilhamento a serem aplicados pelos destinatários. Somente as marcações listadas neste padrão são consideradas válidas pelo FIRST.

As quatro marcações do TLP são: TLP:RED, TLP:AMBER, TLP:GREEN e TLP:CLEAR. Em sua forma escrita elas NUNCA DEVEM conter espaços e DEVEM ser em letras maiúsculas. O TLP provê um esquema simples e intuitivo para indicar com quem informações potencialmente sensíveis podem ser compartilhadas.

Como usar TLP em mensagens como o e-mail?
Mensagens com marcação TLP DEVEM OBRIGATORIAMENTE indicar a marcação TLP da informação, bem como quaisquer restrições adicionais, imediatamente antes da informação em si. A marcação TLP DEVE estar na linha de assunto (subject) do e-mail.

O MailInspector possui capacidade de trabalhar com TLP, bastando usar o dicionário de palavras e fazendo a devida verificação pelo DLP tanto no assunto, quanto no corpo do e-mail, quanto em anexos.

TLS (Transport Layer Security)

O protocolo TLS provê a privacidade e a integridade de dados entre duas aplicações que comuniquem pela internet. Isso ocorre por intermédio da autenticação das partes envolvidas e da cifragem dos dados transmitidos entre as partes. Ainda, esse protocolo ajuda a prevenir que intermediários entre as duas extremidades das comunicações obtenham acesso indevido ou falsifiquem os dados que estão sendo transmitidos. Portanto em muitas vezes a comunicação entre dois servidores de e-mail possui a camada de TLS habilitada, para garantia de segurança na comunicação entre as duas pontas.

No MailInspecto é possível confugurar o TLS/SSL como inativo, permissivo e obrigatório. Também é possível obrigar o uso de TLS/SSL para domínios específicos.

Obs: No MailInspector pode-se trabalhar tanto com TLS, como com SSL.

UTF-8 e UTF-16

UTF-8 (8-bit Unicode Transformation Format- informática avançada) é um tipo de codificação binária (Unicode) de comprimento variável criado por Ken Thompson e Rob Pike. Pode representar qualquer caracter universal padrão do Unicode, sendo também compatível com o ASCII. Por esta razão, está lentamente a ser adaptado como tipo de codificação padrão para e-mail, páginas web, e outros locais onde os caracteres são armazenados.

UTF-8 usa de um a quatro bytes (estritamente, octetos) por carácter, dependendo do símbolo Unicode que representa. É necessário apenas um byte para codificar os 128 caracteres ASCII (Unicode U+0000 a U+007F). São necessários dois bytes para caracteres Latinos com diacríticos. São também usados dois bytes para representar caracteres dos alfabetos Grego, Cirílico, Armênio, Hebraico, Sírio e Thaana (Unicode U+0080 a U+07FF). São necessários três bytes para o resto do Plano Multilingual Básico (que contém praticamente todos os caracteres comuns utilizados). Existem ainda outros caracteres que necessitam de quatro bytes.

Quatro bytes pode parecer muito para um caracter ("code point"), mas muito raramente são utilizados. Além disso, UTF-16 (a principal alternativa ao UTF-8) necessita também de quatro bytes para estes "code points". A definição de qual dos dois é mais eficiente (UTF-8 ou UTF-16) depende da variedade de "code points" usados.

Contudo, as diferenças entre os vários tipos de codificação tornam-se irrelevantes com o uso de sistemas de compressão como o DEFLATE. Para textos curtos nos quais os tradicionais algoritmos não funcionam bem e se faz necessário ter o tamanho em consideração, é geralmente usado o Esquema Padrão de Compressão para Unicode (Standard Compression Scheme for Unicode).

UTF-16 é um "Formato de Transformação Unicode" de 16-bits. Um formato de transformação Unicode é uma codificação de caracteres que provê uma maneira de representar os diversos caracteres abstratos, presentes no Unicode e no ISO/IEC 10646, como uma série de palavras (neste caso, de 16-bits), para então poder ser armazenados ou transmitidos por uma rede. A codificação UTF-16 é oficialmente definida no Anexo Q do padrão ISO/IEC 10646-1. É também descrita em "The Unicode Standard", versões 3.0 e superiores.

O MailInspector possui suporte a codificação de caracteres DBCS, UTF-8 e UTF-16.

Vírus

É um software malicioso que é desenvolvido por programadores geralmente inescrupulosos. Tal como um vírus biológico, o programa infecta o sistema, faz cópias de si e tenta se espalhar para outros computadores e dispositivos de informática.

A maioria das contaminações ocorre por ação do usuário. Um exemplo muito comum se dá por meio do download de arquivos infectados que são recebidos em anexos de e-mail's. A contaminação também pode ocorrer de outras formas: acessando sites de procedência duvidosa ou ainda por meio de arquivos infectados em pendrives, CD's, DVD's ou qualquer outro tipo dispositivo de armazenamento de dados. Uma outra maneira de ter um dispositivo contaminado, seria por meio de um Sistema Operacional desatualizado, sem as devidas correções de segurança que visam barrar o acesso indevido destes softwares maliciosos que tentam entrar nas máquinas via Internet.

No MailInspector, podemos encontrar dois sistemas de antivírus trabalhando simultaneamente (ESET e HSC SmartDefender antivírus), sendo ambos já licenciados. Além disso, contamos com sistema Zero Hour, para maior segurança do sistema.

Já a nível de SandBox, também contamos com ESET em segundo plano (além do antivírus nativo HSC SmartDefender antivírus, que é executado em primeiro plano).

Vírus Polimórfico

É uma ameaça que muda a sua forma com cada ficheiro que infeta. Como não têm um padrão binário consistente, essas ameaças são difíceis de identificar.

O MailInspector em conjunto com BitDefender e ESET é capaz de identificar esse tipo de ameaça, uma vez que o sistema verifica tanto assinaturas, quanto o comportamento através de SandBox, detectando qualquer anomalia, mesmo sendo disfarçado de solicitações válidas do Windows. Um exemplo de vírus polimórfico é o Sality, que apesar de ser “antigo”, ainda possui grande espectro de atuação. A ESET possui código específico para detecção e extermínio dele.

Zero-Day Exploits

Zero-day Exploits ou explorações em zero dias, se referem a vulnerabilidades de software encontradas, antes que pesquisadores de segurança e desenvolvedores de software tomem conhecimento da ameaça. Por isso, representam um risco maior para os usuários do que outras vulnerabilidades.

O MailInspector permite identificar novos focos de ataques e proliferações de Virus e outras ameaças sem que haja uma assinatura de detecção disponível.

Localmente o MailInspector analisa o comportamento do arquivo e se ele tiver comportamento suspeito, é feita a consulta Online no BigData da ESET (comparando as características do comportamento apresentado localmente, com o registro de comportamentos de outros programas já analisados pela ESET), dessa forma, ele consegue detectar se o programa está tentando explorar falhas de segurança, ou outra anomalia. A identificação da ameaça é efetuada sem a necessidade de que o sistema do usuário esteja atualizado.

Apêndice 2 - RFC's Suportadas

RFC's de SMTP

- RFC 1213: Management Information Base for Network Management of TCP/IP-based internets: MIB-II) - Antigo: 1158
- RFC 1918: Address Allocation for Private Internets - Antigo: RFC 1627, RFC 1597
- RFC 1985: SMTP Service Extension for Remote Message Queue Starting
- RFC 2034: SMTP Service Extension for Returning Enhanced Error Codes
- RFC 2045: Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies - Antigo: RFC 1590, RFC 1522, RFC 1521, RFC 1342, RFC1341
- RFC 2505: Anti-Spam Recommendations for SMTP MTAs
- RFC 2634: Enhanced Security Services for S/MIME
- RFC 2920: SMTP Service Extension for Command Pipelining - Antigo: RFC 2197, RFC 1854
- RFC 3207: SMTP Service Extension for Secure SMTP over TLS - Antigo: RFC 2487
- RFC 3461: Simple Mail Transfer Protocol (SMTP) Service Extension for Delivery Status Notifications (DSNs) - Antigo: RFC 1891
- RFC 3463: Enhanced Mail System Status Codes – Antigo: RFC 1893
- RFC 3464: Extensible Message Format for Delivery Status Notifications – Antigo: RFC 1894
- RFC 3635: Definitions of Managed Objects for the Ethernet-like Interface Types – Antigo: RFC 2665, RFC 2358, RFC 1650
- RFC 4954: SMTP Service Extension for Authentication – Antigo: RFC 2554
- RFC 5321: Simple Mail Transfer Protocol – Antigo: RFC 2821, RFC 1869, RFC 1651, RFC 1425, RFC 974, RFC 821
- RFC 5322: Internet Message Format – Antigo: RFC 2822, RFC 822
- RFC 6376: DomainKeys Identified Mail (DKIM) Signatures – Antigo: RFC 5672, RFC 4871, RFC 4870
- RFC 6522: Multipart/Report Content Type for the Reporting of Mail System Administrative Messages – Antigo: RFC 3462, RFC 1892
- RFC 6409: Message Submission – Antigo: RFC 4409, RFC 2476
- RFC 7208: Sender Policy Framework (SPF) for Authorizing Use of Domains in E-Mail – Antigo: RFC 4408
- RFC 6531: SMTP Extension for Internationalized E-mail – Antigo: RFC 5336
- RFC 7504: SMTP 521 and 556 Reply Codes

RFC's de IMAP

- RFC 2088: IMAP4 Non-synchronizing Literals
- RFC 2177: IMAP4 Idle Command
- RFC 2221: Login Referrals
- RFC 2342: IMAP4 Namespace
- RFC 2683: IMAP4 Implementation Recommendations
- RFC 2971: IMAP4 ID Extension
- RFC 3348: IMAP4 Child Mailbox Extension
- RFC 3501: IMAP4 rev1 - Antigo: RFC 2060, RFC 1730
- RFC 3502: IMAP Multiappend Extension
- RFC 3516: IMAP4 Binary Content Extension
- RFC 3691: Unselect Command
- RFC 4315: UIDPLUS Extension - Antigo: RFC 2359
- RFC 4469: Catenate Extension
- RFC 4731: Extension to SEARCH Command for Controlling What Kind of Information Is Returned
- RFC 4959: Extension for Simple Authentication and Security Layer (SASL) Initial Client Response
- RFC 5032: WITHIN Search Extension
- RFC 5161: Enable Extension
- RFC 5182: Extension for Referencing the Last SEARCH Result
- RFC 5255: IMAP Internationalization
- RFC 5256: Sort and Thread Extensions
- RFC 5258: List Command Extensions - Antigo: RFC 3348
- RFC 5267: Contexts for IMAP4
- RFC 5819: Extension for Returning STATUS Information in Extended LIST
- RFC 6154: LIST Extension for Special-Use Mailboxes
- RFC 6851: MOVE extension
- RFC 7162: IMAP Extensions: Quick Flag Changes Resynchronization (CONDSTOR) and Quick Mailbox Resynchronization (QRESYNC) - Antigo: RFC 5162, RFC 4551

RFC's de POP3

- RFC 1939: POP3 - Antigo: RFC 1725, RFC 1460, RFC 1225, RFC 1081
- RFC 2449: POP3 Extension Mechanism

RFC's IDN (Internationalized Domain Names)

- RFC 5891: Internationalized Domain Names in Applications (IDNA): Protocol
- RFC 5892: The Unicode Code Points and Internationalized Domain Names for Applications (IDNA)
- RFC 5893: Right-to-Left Scripts for Internationalized Domain Names for Applications (IDNA)
- RFC 5894: Internationalized Domain Names for Applications (IDNA): Background, Explanation, and Rationale
- RFC 3454: Preparation of Internationalized Strings ("stringprep")
- RFC 3490: Internationalizing Domain Names in Applications (IDNA)
- RFC 3491: Nameprep: A Stringprep Profile for Internationalized Domain Names (IDN)
- RFC 3492: Punycode: A Bootstring encoding of Unicode for Internationalized Domain Names in Applications (IDNA)

Outros RFC's

- RFC 1155: Structure and Identification of Management Information for TCP/IP-based Interface - Antigo: RFC 1065
- RFC 1157: SNMP v1 - Antigo: RFC 1098, RFC 1067
- RFC 1213: MIB 2 - Antigo: RFC 1158
- RFC 2578: Structure of Management Information Version 2 - Antigo: RFC 1902, RFC 1442
- RFC 2579: Textual Conventions for SMIv2 - Antigo: RFC 1903, RFC 1443
- RFC 2595: Using TLS with IMAP, POP3 and ACAP
- RFC 3410: SNMP v3 - Antigo: RFC 2570
- RFC 3416: SNMP v2 - Antigo: RFC 1905, RFC 1448
- RFC 2849: The LDAP Data Interchange Format (LDIF) – Technical Specification
- RFC 3296: Named Subordinate References in Lightweight Directory Access Protocol (LDAP) Directories
- RFC 3671: Collective Attributes in the Lightweight Directory Access Protocol (LDAP)
- RFC 3672: Subentries in the Lightweight Directory Access Protocol (LDAP)
- RFC 3673: Lightweight Directory Access Protocol version 3 (LDAPv3): All Operational Attributes
- RFC 3866: Language Tags and Ranges in the Lightweight Directory Access Protocol (LDAP) – Antigo: RFC 2596
- RFC 4511: Lightweight Directory Access Protocol (LDAP): The Protocol – Antigo: RFC 2251, RFC 2830, RFC 3771
- RFC 4512: Lightweight Directory Access Protocol (LDAP): Directory Information Models – Antigo: RFC 2251, RFC 2252, RFC 2256, RFC 3674
- RFC 4513: Lightweight Directory Access Protocol (LDAP): Authentication Methods and Security Mechanisms – Antigo: RFC 2251, RFC 2829, RFC 2830
- RFC 4514: Lightweight Directory Access Protocol (LDAP): String Representation of Distinguished Names – Antigo: RFC 2253
- RFC 4515: Lightweight Directory Access Protocol (LDAP): String Representation of Search Filters – Antigo: RFC 2254
- RFC 4516: Lightweight Directory Access Protocol (LDAP): Uniform Resource Locator – Antigo: RFC 2255
- RFC 4518: Lightweight Directory Access Protocol (LDAP): Internationalized String Preparation
- RFC 4522: Lightweight Directory Access Protocol (LDAP): The Binary Encoding Option
- RFC 4525: Lightweight Directory Access Protocol (LDAP) Modify-Increment Extension
- RFC 4526: Lightweight Directory Access Protocol (LDAP) Absolute True and False Filters
- RFC 4529: Requesting Attributes by Object Class in the Lightweight Directory Access Protocol
- RFC 2781: UTF-16, an encoding of ISO 10646
- RFC 2279: UTF-8, a transformation format of ISO 10646 – Antigo 3629
- RFC 6376: DomainKeys Identified Mail (DKIM) Signatures
- RFC 7489: Domain-based Message Authentication, Reporting, and Conformance (DMARC)
- RFC 7553: The Uniform Resource Identifier (URI) DNS Resource Record
- RFC 5751: Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2 – Antigo: RFC 3851

Apêndice 3 – Expressões Regulares

O MailInspector segue o padrão utilizado pelo Google para formação de Expressões Regulares.

Grande parte das Expressões Regulares podem ser usados para:

- Criação de Grupos de Usuários;
- Dicionários de Palavras;
- Anexos;

Alguns Exemplos:

Expressão regular para casar com a frase "TESTE hscbrasil"

No exemplo, vamos dar 4 opções para a "mesma" coisa:

Exemplo 1	(\W|^)TESTE\shscbrasil(\W|$)
Exemplo 2	(\W|^)TESTE\s{0,3}hscbrasil(\W|$)
Exemplo 3	(\W|^)TESTE(s){0,1}\s{0,3}hscbrasil(\W|$)
Exemplo 4	(?i)(\W|^)teste(s){0,1}\s{0,3}HSCbRaSIL(\W|$)

No Exemplo 1:

Pega exatamente como está escrito **TESTE hscbrasil**.

Onde:

\W Corresponde a qualquer caractere que não seja uma letra, um dígito ou sublinhado. Impede que a regex corresponda a caracteres antes (indicado pelo caracter **^**) ou depois da frase (indicado pelo caracter **$**).

\s Indica espaço.

No Exemplo 2:

Pega exatamente como está escrito TESTE hscbrasil

Onde:

O {0,3} depois do \s indica que de 0 a 3 espaços podem ocorrer entre as palavras **TESTE** e **hscbrasil**.

No Exemplo 3:

(s) corresponde à letra s, e **{0,1}** indica que a letra pode ocorrer 0 vezes ou 1 vez depois da palavra "**TESTE**". Portanto, a regex corresponde a **TESTE hscbrasil** e **TESTES hscbrasil**. Você também pode usar o caractere **?** em vez de **{0,1}**.

No Exemplo 4:

(?i) Faz com que a expressão não diferencie maísculas ou minúsculas (Case INSENSITIVE).

Expressão regular para detecção de qualquer palavra ou frase em lista

No exemplo, iremos utilizar uma lista com os seguintes itens:

- limão;
- laranja;
- tomate;
- melancia;
- banana;
- batata doce

Expressão Regular:

(?i)(\W|^)(limão|laranja|tomate|melancia|banana|batata\sdoce)(\W|$)

Onde:

(...) agrupa todas as palavras, de forma que a classe de caractere \W seja aplicável a todas as palavras entre parênteses.

(?i) faz com que a correspondência de conteúdo não diferencie maiúsculas de minúsculas.

\W corresponde a qualquer caractere que não seja uma letra, um dígito ou sublinhado. Impede que a regex corresponda a caracteres antes ou depois de palavras ou frases na lista.

^ corresponde ao início de uma nova linha. Permite que a regex corresponda à palavra se ela aparecer no início de uma linha, sem caracteres antes dela.

$ corresponde ao fim de uma linha. Permite que a regex corresponda à palavra se ela aparecer no fim de uma linha, sem caracteres depois dela.

| indica um "ou" para que a regex corresponda a qualquer uma das palavras na lista.

\s corresponde a um caractere de espaço. Use esse caractere para separar palavras em uma frase.

Expressão regular que corresponde à palavra com variantes.

No exemplo, iremos utilizar a palavra "viagra" e a alguns dos disfarces que remetentes de spam usam, como:

- vi@gra
- v1agra
- v1@gra
- v!@gr@

Expressão Regular:

(?i)v[i!1][a@]gr[a@]

Onde:

(?i) Case INSENSITIVE

[i!1] corresponde aos caracteres i, ! ou 1 na posição do segundo caractere da palavra.

Obs:

\W não é incluído, para que outros caracteres possam aparecer antes ou depois de qualquer uma das variantes de viagra. Por exemplo, a regex ainda corresponde a viagra no texto a seguir:

viagra!! ou ***viagra***

Expressão Regular para Corresponder a e-mail de um domínio específico

Vamos usar como exemplo e-mails de qualquer de um dos seguintes domínios:

- yahoo.com;
- hotmail.com;
- gmail.com

Expressão Regular:

(?i)(\b|^)[\w.\-]{0,25}@(yahoo|hotmail|gmail)\.com(\W|$)\b

Onde:

(?i) Case insensitive

\b corresponde a qualquer caractere que não seja uma letra, um dígito ou sublinhado. Ele impede que a regex corresponda a caracteres antes ou depois do endereço de e-mail.

^ corresponde ao início de uma nova linha. Ele permite que a regex corresponda ao endereço se ele aparecer no início de uma linha, sem caracteres antes dele.

$ corresponde ao fim de uma linha. Permite que a regex corresponda ao endereço quando ele aparece no fim de uma linha, sem caracteres depois dele.

[\w.\-] corresponde a qualquer caractere de palavra **(a-z, A-Z, 0-9, ou sublinhado)**, ponto final ou hífen. Esses são os caracteres válidos usados mais frequentemente na primeira parte de um endereço de e-mail. Observe que o **\-** (indica um hífen) precisa ocorrer por último na lista de caracteres dentro dos colchetes.

A **** antes do travessão e do ponto fazem o "escape" desses caracteres. Isso indica que o travessão e o ponto não são caracteres especiais da regex. Observe que não é necessário realizar o escape do ponto dentro dos colchetes.

{0,25} indica que de 0 a 25 caracteres no conjunto de caracteres precedente podem ocorrer antes do símbolo @. A configuração de e-mail "Compliance do conteúdo" é compatível com a correspondência de até 25 caracteres para cada conjunto de caracteres em uma expressão regular.

A formatação **(...)** agrupa os domínios, e o caractere **|** que os separa indica um "ou".

Expressão Regular para Corresponder início de uma URL

Vamos supor que você esteja recebendo uma ameaça vinda do seguinte domínio (para baixar um arquivo contaminado):

http://utxre81ua4m.restricoesveiculos.com.de/2V3GR0ZDMIV/JC0090790G3Q8068D2NAPVUKY9IUH/americanas.loja3022 **e de outro domínio ao qual também faz download de conteúdo malicioaso** ***http://storage.googleapis.com/update-delta/hfnkpimlhhgieaddgfemjhofmfblmnib/5825/5824/dbdf4a228dad5b04a8d71374649666276391e789d87fbf26da81b98d0f25ddc1.crxd***

Expressão Regular:

(?i)(^|\b)(http:\/\/|https:\/\/)([\w.\-]{0,200})+(\.restricoesveiculos\.com\.de|\.googleapis\.com)\b

Vamos detectar a string, ignorando todo o resto: http://utxre81ua4m.restricoesveiculos.com.de

Onde:

(?i) Case insensitive

^ corresponde ao início de uma nova linha. Ele permite que a regex corresponda ao endereço se ele aparecer no início de uma linha, sem caracteres antes dele.

(http:\/\/|https:\/\/) Indica a string http:// OU https://

[\w.\-] corresponde a qualquer caractere de palavra **(a-z, A-Z, 0-9, ou sublinhado)**, ponto final ou hífen. Esses são os caracteres válidos usados mais frequentemente na primeira parte de um endereço de e-mail. Observe que o **\-** (indica um hífen) precisa ocorrer por último na lista de caracteres dentro dos colchetes.

A **** antes do travessão e do ponto fazem o "escape" desses caracteres. Isso indica que o travessão e o ponto não são caracteres especiais da regex. Observe que não é necessário realizar o escape do ponto dentro dos colchetes.

{0,200} indica que de 0 a 200 caracteres no conjunto de caracteres precedente podem ocorrer antes do símbolo da parte final que seria **.restricoesveiculos.com.de** OU **.googleapis.com**

(\.restricoesveiculos\.com\.de|\.googleapis\.com) Indica o condicionador OU para qualquer um dos domínios apresentados: .restricoesveiculos.com.de OU .googleapis.com

Expressão Regular para Corresponder ao meio de um e-mail

Vamos supor que você esteja recebendo uma ameaça fingindo ser bounce de e-mail, ao qual como característica:

bounce-600235-5027-741686-cleverson.silva**=hscbrasil.pr.gov.br@**d80.asa.acemsd1.com

A string =hscbrasil.pr.gov.br é sempre em comum nos e-mails de ataque do bouce indicado.

Expressão Regular:

^(?i)(bounces|bounce)+([\w.\-\+]{0,200})+(\=hscbrasil\.pr\.gov\.br\@)+([\w.\-\+]{0,200})

Onde:

^ corresponde ao início de uma nova linha. Ele permite que a regex corresponda ao endereço se ele aparecer no início de uma linha, sem caracteres antes dele.

(?i) Case insensitive

(bounces|bounce) Corresponde a palavra bounce no início da string. Foi verificado que em muitos ataques eles utilizam como bounce de e-mail, sendo obrigatório a palavra **bounces ou bounce** no início da string.

[\w.\-\+] corresponde a qualquer caractere de palavra **(a-z, A-Z, 0-9, ou sublinhado, ou +)**, ponto final ou hífen. Esses são os caracteres válidos usados mais frequentemente na primeira parte de um endereço de e-mail. Observe que o **\-** (indica um hífen) precisa ocorrer por último na lista de caracteres dentro dos colchetes.

{0,200} indica que de 0 a 200 caracteres no conjunto de caracteres precedente podem ocorrer antes do **=hscbrasil.com.br@**

(\=hscbrasil\.pr\.gov\.br\@) Indica a expressão =hscbrasil.pr.gov.br@

[\w.\-\+] corresponde a qualquer caractere de palavra **(a-z, A-Z, 0-9, ou sublinhado, ou +)**, ponto final ou hífen. Esses são os caracteres válidos usados mais frequentemente na primeira parte de um endereço de e-mail. Observe que o **\-** (indica um hífen) precisa ocorrer por último na lista de caracteres dentro dos colchetes.

{0,200} indica que de 0 a 200 caracteres no conjunto de caracteres precedente podem ocorrer após a expressão **=hscbrasil.pr.gov.br@**

Expressão regular para detecção de extensões de arquivos

No exemplo, iremos utilizar uma lista prévia de extensões bloqueadas por padrão pelo Google e Outlook.

Expressão Regular:

((?i)((\.ade|\.adp|\.app|\.asp|\.bas|\.bat|\.cab|\.cer|\.chm|\.cmd|\.cnt|\.com|\.cpl|\.crt|\.csh|\.der|\.dll|\.dmg|\.diagcab|\.exe|\.fxp|\.gadget|\.grp|\.hlp|\.hpj|\.hta|\.inf|\.ins|\.isp|\.its|\.jar|\.jsr|\.jnlp|\.js|\.jse|\.ksh|\.lib|\.lnk|\.mad|\.maf|\.mag|\.mam|\.maq|\.mar|\.mas|\.mat|\.mau|\.mav|\.maw|\.mcf|\.mda|\.mdb|\.mde|\.mdt|\.mdw|\.mdz|\.msc|\.msh|\.msh1|\.msh2|\.mshxml|\.msh1xml|\.msh2xml|\.msi|\.msp|\.mst|\.msu|\.nsh|\.ops|\.osd|\.pcd|\.pif|\.pl|\.plg|\.prf|\.prg|\.printerexport|\.ps1|\.ps1xml|\.ps2|\.ps2xml|\.psc1|\.psc2|\.psd1|\.psdm1|\.pst|\.reg|\.scf|\.scr|\.sct|\.shb|\.shs|\.sys|\.theme|\.tmp|\.url|\.vb|\.vbe|\.vbp|\.vbs|\.vsmacros|\.vsw|\.vxd|\.webpnp|\.website|\.ws|\.wsc|\.wsf|\.wsh|\.xbap|\.xll|\.xnk)$))

Onde:

(...) agrupa todas as palavras, de forma que a classe de caractere \W seja aplicável a todas as palavras entre parênteses.

(?i) faz com que a correspondência de conteúdo não diferencie maiúsculas de minúsculas.

\. Indica **ponto** (como caracter)

$ Indica final do nome do arquivo

| Indica operador lógico **OU**

Expressão Regular para Corresponder a qualquer endereço IP em um intervalo

Vamos usar como exemplo qualquer endereço IP com a variação de 192.168.1.0 a 192.168.1.255.

Iremos efetuar de duas formas:

Exemplo 1	192\.168\.1\.
Exemplo 2	192\.168\.1\.\d{1,3}
Exemplo 3	(((1[0-9] | [1-9]?) [0-9] | 2 ([0-4][0-9] | 5[0-5])) \.) {3} ((1[0-9] | [1-9]?) [0-9] | 2 ([0-4][0-9] | 5[0-5]))

A **** antes de cada ponto realiza o "escape" do ponto. Isso indica que o ponto não é um caractere especial da regex.

No Exemplo 1, como nenhum caractere aparece depois do último ponto, a regex corresponde a qualquer endereço IP iniciado por **192.168.1.**, com qualquer número em seguida.

No Exemplo 2, **\d** corresponde a qualquer dígito de 0 a 9 depois do último ponto, e **{1,3}** indica que de 1 a 3 dígitos podem aparecer depois do último ponto. Nesse caso, a regex corresponde a qualquer endereço IP completo iniciado por 192.168.1.. Essa regex também corresponde a endereços IP inválidos, como 192.168.1.999.

Explicação do Exemplo 3

Em análise mais profunda teremos uma expressão regular que irá cobrir 1.1.1.1 a 255.255.255.255

(((1[0-9] | [1-9]?) [0-9] | 2 ([0-4][0-9] | 5[0-5])) \.) {3} ((1[0-9] | [1-9]?) [0-9] | 2 ([0-4][0-9] | 5[0-5]))

Segue abaixo a explicação da Expressão Regular válida de Range de IP 1.1.1.1 a 255.255.255.255

Primeiro precisamos de uma ER para casar o intervalo de números inteiros entre 0 a 255. Como o intervalo [0-255] não é valido em ERs, visto que só podemos representar intervalos entre dois caracteres, fica complicado (mas não impossível) representar este intervalo com construções regulares.

Uma primeira expressão que poderia ser alcançada poderia ser uma comprida, porém fácil de entender:

```
ER   : ([0-9]|[1-9][0-9]|1[0-9][0-9]|2([0-4][0-9]|5[0-5]))
casa:   0-9 |   10-99  |  100-199  |   200-249  |250-255
```

Funciona, mas é pouco eficiente. E lembre-se a melhor parte de ERs é passar horas para diminuí-la um caractere que seja. Como nos dois primeiros intervalos, de 0-9 e 10-99, temos o [0-9] comum a ambos, tendo num o [1-9] e no outro não, podemos torná-lo opcional:

```
ER   : ([1-9]?[0-9]|1[0-9][0-9]|2([0-4][0-9]|5[0-5]))
casa:   0-9,10-99 |  100-199  |   200-249  |250-255
```

Novamente, percebemos um [0-9] repetido no final dos intervalos 0-9,10-99 e 100-199. Vamos isolá-lo. SIM! É igual a matemática lá no primário! xa+xb = x(a+b)

```
ER   : ((1[0-9]|[1-9]?)[0-9]|2([0-4][0-9]|5[0-5]))
casa:   0-9,10-99,100-199  |   200-249  |250-255
```

Chegamos a seguinte expressão regular:

((1[0-9] | [1-9]?) [0-9] | 2 ([0-4][0-9] | 5[0-5]))

Como um ip seria quatro vezes este intervalo, separado por pontos, algo como "0-255.0-255.0-255.0-255", teríamos, no final da brincadeira o monstro que casa um IP válido:

((1[0-9]|[1-9]?)[0-9]|2([0-4][0-9]|5[0-5]))\.((1[0-9]|[1-9]?)[0-9]|2([0-4][0-9]|5[0-5]))\.((1[0-9]|[1-9]?)[0-9]|2([0-4][0-9]|5[0-5]))\.((1[0-9]|[1-9]?)[0-9]|2([0-4][0-9]|5[0-5]))

É claro, que ao programar e precisar validar um número IP com expressões regulares, estruturas e funções da linguagem de programação ajudarão nessa tarefa, como o laço e o "split", ou seja, basta chegar uma mente aberta e sugerir outra abordagem: "(0-255.){3}0-255"

Chegando a abordagem final com a seguinte expressão:

(((1[0-9] | [1-9]?) [0-9] | 2 ([0-4][0-9] | 5[0-5])) \.) {3} ((1[0-9] | [1-9]?) [0-9] | 2 ([0-4][0-9] | 5[0-5]))

Fonte:

https://aurelio.net/regex/casar-ip.html

Também é possível criar uma expressão regular de Range de IP no link a seguir:

http://www.analyticsmarket.com/freetools/ipregex

Outras expressões regulares úteis

Regex para CEP

\d{5}-\d{3}

Onde:

\d É um metacaractere, um curinga que casa com um dígito (0 a 9)

{5} Indica repetição de 5 vezes

- Hífen

{3} Indica repetição de 3 vezes

Regex para Placa de Carro

[A-Z]{3}-\d{4}

Onde:

[A-Z] Indica caractere de A a Z

{3} Indica repetição de 3 vezes

- Hífen

\d É um metacaractere, um curinga que casa com um dígito (0 a 9)

{4} Indica repetição de 4 vezes

Regex para Placa de Carro Mercosul

[A-Z]{3}[0-9][0-9A-Z][0-9]{2}

Onde:

[A-Z] Indica caractere alfabético de A a Z

{3} Indica repetição de 3 vezes

[0-9] Indica caractere numérico de 0 a 9

[0-9A-Z] Indica caractere alfanumérico A a Z e 0 a 9

[0-9] Indica caractere numérico de 0 a 9

{2} Indica repetição de 2 vezes

Regex de Horas no formata hh:mm padrão 24h

[012]\d:[0-5]\d

Semelhante ao formato de horas e minutos, como 03:10 ou 23:59.

Onde:

[012] Define um conjunto. Neste caso, o conjunto especifica que primeiro caractere deve ser 0, 1 ou 2.

[0-5] Forma abreviada para o conjunto [012345];

\d O conjunto que representa todos os dígitos de 0 a 9.

Regex para "vazio"/sem conteúdo (em branco)

(^$|^.@.\..*$)

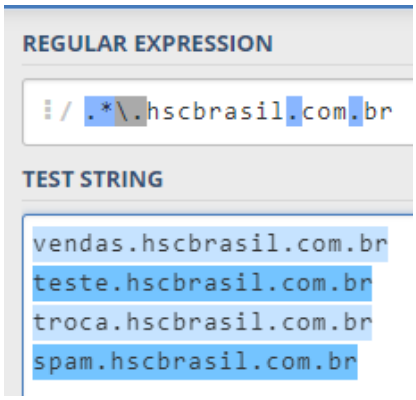
Com a expressão acima, é possível criar regras para por exemplo e-mails sem remetente, ou e-mail sem Assunto, e-mails sem o conteúdo no corpo da mensagem, ou cabeçalho "RETURN-PATH" sem conteúdo no seu interior.

Regex para qualquer conjunto de caracter

.*

Muito útil para aceitar qualquer CONJUNTO de caracter, para usar em montagem de expressões.

Ex: Quero aceitar subdomínios para o hscbrasil.com.br



O RegEx de qualquer CONJUNTO de caracter é considerado RegEx coringa, portanto não deve ser utilizado com várias repetições, correndo risco de ficar extremamente lento o processamento por causa disso.

Regex para contagem de e-mails

\@

Muito útil para detectar quantidade de e-mails em cópia e efetuar alguma regra quando ultrapassar a quantidade desejada.

Regex para casar com uma ou mais palavras contidas em uma frase

/(?=.*\bOferta\b)(?=.*\bCaixa\b)(?=.*\bSeguridade\b).*$/si

No exemplo acima verfica a presença ocorrência de uma ou mais palavras na mesma frase,independente da ordem (com case INsensitive), contidas na expressão regular. As palavras do exemplo verificado são: oferta, caixa e seguridade.

Exemplo de RegEx para CPF

(\s|^|.*)([0-9]{3}.[0-9]{3}.[0-9]{3}-[0-9]{2})|([0-9]{11})|([0-9]{9}\-[0-9]{2})|([0-9]{3}.[0-9]{3}[0-9]{3}-[0-9]{2})|([0-9]{3}[0-9]{3}.[0-9]{3}-[0-9]{2})(\s|$|.*)

Sabendo que CPF são onze números, sendo os dois últimos dígitos verificadores, foi criado regex que casa com qualquer formato de CPF (com ponto, sem ponto, com traço, sem traço, etc), bem como considera-se que o CPF esteja "colado" a uma palavra antes ou depois.

Segue teste com o CPF: 100.744.640-43

TEST STRING

```
fgfgfg100.744.640-43 10074464043-0vbbv
```

MATCH INFORMATION

Match 1	0-40	fgfgfg100.744.640-43 10074464043-0vbbv
Group 1	0-22	fgfgfg100.744.640-43
Group 2	22-33	10074464043
Group 4	22-33	10074464043
Group 8	33-40	-0vbbv

Caso o seu ambiente possa vir a ter muitos "falsos positivos de CPF", tais como onze números em sequência, sugerimos colocar a seguinte expressão, sendo múltiplas linhas de entrada:

[0-9]{3}\.[0-9]{3}\.[0-9]{3}\-[0-9]{2}

[0-9]{9}\-[0-9]{2}

[0-9]{3}\.[0-9]{6}\-[0-9]{2}

[0-9]{6}\.[0-9]{3}\-[0-9]{2}

No processo, foi removida a expressão que detecta onze números sequenciais.

Exemplo de RegEx para RG

(^\d{1,2}).?(\d{3}).?(\d{3})-?(\d{1}|X|x$)

RegEx consegue detectar expressão com ponto, sem ponto e com letra no final (alguns estados colocam letra X no final).

REGULAR EXPRESSION

```
/ (^\d{1,2}).?(\d{3}).?(\d{3})-?(\d{1}|X|x$)
```

TEST STRING

```
6.099.339-X
0222333-2
```

MATCH INFORMATION

Match 1	0-11	6.099.339-X
Group 1	0-1	6
Group 2	2-5	099
Group 3	6-9	339
Group 4	10-11	X
Match 2	12-21	0222333-2

Exemplo de RegEx para detecção de qualquer e-mail

Seguindo RFC 5322, para validação de e-mails:

(?:[a-z0-9!#$%&'*+=?^_`{|}~-]+(?:\.[a-z0-9!#$%&'*+=?^_`{|}~-]+)*|"(?:[\x01-\x08\x0b\x0c\x0e-\x1f\x21\x23-\x5b\x5d-\x7f]|\\[\x01-\x09\x0b\x0c\x0e-\x7f])*")@(?:(?:[a-z0-9](?:[a-z0-9-]*[a-z0-9])?\.)+[a-z0-9](?:[a-z0-9-]*[a-z0-9])?|\[(?:(?:25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)\.){3}(?:25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?|[a-z0-9-]*[a-z0-9]:(?:[\x01-\x08\x0b\x0c\x0e-\x1f\x21-\x5a\x53-\x7f]|\\[\x01-\x09\x0b\x0c\x0e-\x7f])+)\])

RegEx de Número de Passaporte brasileiro

\b[\wñáéíóúü]{2}\d{6}((\d{1}|[\wñáéíóúü]{1}){1}(\d{1}|[\wñáéíóúü]{1}){1}(\d{1}|[\wñáéíóúü]{1}){1})?\b

Expressão Regular para block list/allow list casando com subdomínios

Como exemplo vamos pegar um spammer, ao qual utiliza dois subdomínios para envio de spam:

<xxx>subdominio01.subdominio02.vmdecor.com.br

Onde:

<xxx> é o "remetente"

Subdominio01 é a indicação de subdomínio utilizado, podendo ser qualquer coisa, por exemplo **olimpio04**

Subdomínio02 é a indicação de subdomínio utilizado, podendo ser qualquer coisa, por exemplo **atenas**

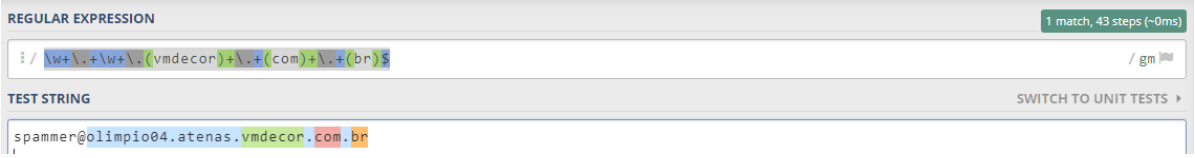
Portanto, por exemplo vamos considerar o seguinte e-mail de origem:

spammer@olimpio04.atenas.vmdecor.com.br

O RegEx para detecção será:

(?i)\@+\w+\.+\w+\.(vmdecor)+\.+(com)+\.+(br)$

Testando o RegEx



Explicando a lógica:

(?i) Case insensitive

\@ Indica o caracter @

\w Indica palavra completa (qualquer palavra)

+ Indica incluir mais expressões (operador concatenador)

\. Indica o caracter ponto .

\w Indica palavra completa (qualquer palavra)

+ Indica incluir mais expressões

\. Indica o caracter ponto .

Por último a expressão entre parênteses, indica que o que tem dentro, não é afetado por variáveis, isto é, são palavras "fixas". Ele está entre parênteses, para indicar que é para considerar toda a expressão, caso contrário o RegEx interpretará cada caracter individualmente como possível componente do RegEx.

$ Indica que é para analisar a expressão do Fim para o começo, ou seja, da direita para esquerda.

Segue abaixo explicação do testador do RegEx:

\w+\.+\w+\.(vmdecor)+\.+(com)+\.+(br)$

\w+ matches any word character (equal to [a-zA-Z0-9_])
+ **Quantifier** — Matches between **one** and **unlimited** times, as many times as possible, giving back as needed (greedy)
\.+ matches the character . literally (case sensitive)
+ **Quantifier** — Matches between **one** and **unlimited** times, as many times as possible, giving back as needed (greedy)
\w+ matches any word character (equal to [a-zA-Z0-9_])
+ **Quantifier** — Matches between **one** and **unlimited** times, as many times as possible, giving back as needed (greedy)
\. matches the character . literally (case sensitive)

1st Capturing Group
(vmdecor)+
+ **Quantifier** — Matches between **one** and **unlimited** times, as many times as possible, giving back as needed (greedy)
A repeated capturing group will only capture the last iteration. Put a capturing group around the repeated group to capture all iterations or use a non-capturing group instead if you're not interested in the data
vmdecor matches the characters vmdecor literally (case sensitive)
\.+ matches the character . literally (case sensitive)
+ **Quantifier** — Matches between **one** and **unlimited** times, as many times as possible, giving back as needed (greedy)

2nd Capturing Group
(com)+
+ **Quantifier** — Matches between **one** and **unlimited** times, as many times as possible, giving back as needed (greedy)
A repeated capturing group will only capture the last iteration. Put a capturing group around the repeated group to capture all iterations or use a non-capturing group instead if you're not interested in the data
com matches the characters com literally (case sensitive)
\.+ matches the character . literally (case sensitive)
+ **Quantifier** — Matches between **one** and **unlimited** times, as many times as possible, giving back as needed (greedy)

3rd Capturing Group
(br)
br matches the characters br literally (case sensitive)
$ asserts position at the end of a line

MATCH INFORMATION

Match 1

Full match	8-39	olimpio04.atenas.vmdecor.com.br
Group 1.	25-32	vmdecor
Group 2.	33-36	com
Group 3.	37-39	br

Expressão Regular para detectar repetição de mesmo caractere em e-mail

Como exemplo vamos considerar o e-mail aaa123bbb345@gmail.com como e-mail falso criado por spammer.

Partindo desse princípio teremo que detectar repetição de pelo menos 3 letras consecutivamente, vindo do domínio gmail.com

O RegEx para detecção será:

(?i)((a{3,}|b{3,}|c{3,}|d{3,}|e{3,}|f{3,}|g{3,}|h{3,}|i{3,}|j{3,}|k{3,}|l{3,}|m{3,}|n{3,}|o{3,}|p{3,}|q{3,}|r{3,}|s{3,}|t{3,}|u{3,}|v{3,}|x{3,}|y{3,}|w{3,}|z{3,})(.+(\@gmail\.com)|\@gmail\.com))

Testando o RegEx

(?i)((a{3,}|b{3,}|c{3,}|d{3,}|e{3,}|f{3,}|g{3,}|h{3,}|i{3,}|j{3,}|k{3,}|l{3,}|m{3,}|n{3,}|o{3,}|p{3,}|q{3,}|r{3,}|s{3,}|t{3,}|u{3,}|v{3,}|x{3,}|y{3,}|w{3,}|z{3,})(.+(\@gmail\.com)|\@gmail\.com))

i modifier: insensitive. Case insensitive match (ignores case of [a-zA-Z])

(a{3,}|b{3,}|c{3,}|d{3,}|e{3,}|f{3,}|g{3,}|h{3,}|i{3,}|j{3,}|k{3,}|l{3,}|m{3,}|n{3,}|o{3,}|p{3,}|q{3,}|r{3,}|s{3,}|t{3,}|u{3,}|v{3,}|x{3,}|y{3,}|w{3,}|z{3,})

Verifica a repetição de no mínimo 3 vezes qualquer caracter, sequencialmente, por exemplo: yyy, bbb, ddd, kkk, ggg, etc.

Variação de dois termos:

Primeiro termo:

> **.** matches any character (except for line terminators)
>
> **+** matches the previous token between one and unlimited times, as many times as possible, giving back as needed (greedy)

Segundo termo:

Não usa o **.+** pois dá margem a necessidade de no mínimo um caracter. Caso o e-mail seja finalizado com repetição de três caracteres, o RegeX não casará com a idéia. Para evitar isso, faz-se o uso do operador lógico OU, fazendo que seja utilizada a expressão @gmail.com sem ter o usio do **.+**

2nd Capturing Group (\@gmail\.com)

\@ matches the character @ with index 6410 (4016 or 1008) literally (case insensitive)

gmail matches the characters gmail literally (case insensitive)

\. matches the character . with index 4610 (2E16 or 568) literally (case insensitive)

com matches the characters com literally (case insensitive)

TEST STRING

```
meuemailaaa7576@gmail.com
bbb76kkk98@gmail.com
meuemailxxx@gmail.com
```

Estrutura de Data e hora

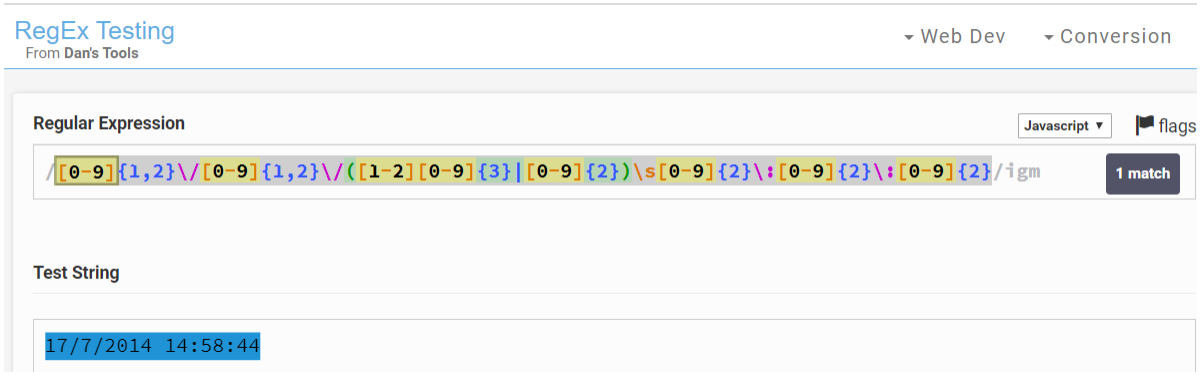
Como exemplo vamos verificar uma expressão para detectar data e hora no seguinte formato:

Ex: 17/7/2014 14:58:44

O RegEx para detecção será:

[0-9]{1,2}\/[0-9]{1,2}\/([1-2][0-9]{3}|[0-9]{2})\s[0-9]{2}\:[0-9]{2}\:[0-9]{2}

Testando o RegEx



Explicando a lógica:

[0-9]{1,2} Indica caracter numérico de 0 a 9, podendo ser aceito com uma ou duas casas numéricas. Este campo pretende detectar o dia da string apresentada.

\/ Indica o caracter barra (/)

[0-9]{1,2} Indica caracter numérico de 0 a 9, podendo ser aceito com uma ou duas casas numéricas. Este campo pretende detectar o mês da string apresentada.

\/ Indica o caracter barra (/)

(Indica início de expressão a ser analisada.

[1-2] Um caracter, sendo o número 1 ou 2 (estamos fechando isso para o milênio do ano na string).

[0-9]{3} Qualquer caracter numérico entre 0 a 9, sendo aceito 3 caracteres

| Operador lógico OU

[0-9]{2} Qualquer número entre 0 a 9, sendo dois caracteres

) Indica fim de expressão a ser analisada.

\s Indica espaço em branco

[0-9]{2} Qualquer número de 0 a 9 com dois caracteres (para considerar a hora da string).

\: Indica o caracter :

[0-9]{2} Qualquer número de 0 a 9 com dois caracteres (para considerar os minutos da string).

\: Indica o caracter :

[0-9]{2} Qualquer número de 0 a 9 com dois caracteres (para considerar os segundos da string).

Dicionário de Palavrões – Evitando que palavra seja detectada no meio de outras palavras

Um erro muito comum é criar um dicionário sem verificação de composição da palavra no meio de eventuais outras palavras, um exemplo é a palavra "**PUTA**", que pode vir dentro da palavra DE**PUTA**DO, ou IM**PUTA**DA.

Para solução desse problema, é necessário criar o dicionário com eventual verificação de dentro de outras palavras e/ou início de frase e/ou final de frase.

((?i)\Wputa\W|^puta\W|\Wputa$)

Explicando a lógica:

1st Capturing Group
((?i)\Wputa\W|^puta\W|\Wputa$)

1st Alternative
(?i)\Wputa\W

i modifier: insensitive. Case insensitive match (ignores case of [a-zA-Z])
\W matches any non-word character (equal to [^a-zA-Z0-9_])
puta matches the characters puta literally (case insensitive)
\W matches any non-word character (equal to [^a-zA-Z0-9_])

2nd Alternative
^puta\W
^ asserts position at start of a line
puta matches the characters puta literally (case insensitive)
\W matches any non-word character (equal to [^a-zA-Z0-9_])

3rd Alternative
\Wputa$
\W matches any non-word character (equal to [^a-zA-Z0-9_])
puta matches the characters puta literally (case insensitive)
$ asserts position at the end of a line

Segue abaixo tabela de palavrões, com as devidas expressões regulares:

Palavrão	RegEx
Bicha	((?i)\Wbicha\W|^bicha\W|\Wbicha$)
Bichona	((?i)\Wbichona\W|^bichona\W|\Wbichona$)
Biscate	((?i)\Wbiscate\W|^biscate\W|\Wbiscate$)
Biscatona	((?i)\Wbiscatona\W|^biscatona\W|\Wbiscatona$)
Boiola	((?i)\Wboiola\W|^boiola\W|\Wboiola$)
Boquete	((?i)\Wboquete\W|^boquete\W|\Wboquete$)
Boceta/Buceta	((?i)\Wb(o|u)ceta\W|^b(o|u)ceta\W|\Wb(o|u)ceta$)
Bocetuda/Bucetuda	((?i)\Wb(o|u)cetuda\W|^b(o|u)cetuda\W|\Wb(o|u)cetuda$)
Caceta/Cacete	((?i)\Wcacet(a|e)\W|^cacet(a|e)\W|\Wcacet(a|e)$)

Caralho	((?i)\Wcaralho\W|^caralho\W|\Wcaralho$)
Chupa meu pau	((?i)\Wchupa\smeu\spau\W|^chupa\smeu\spau\W|\Wchupa\smeu\spau$)
Corno(a)	((?i)\Wcorn(o|a)\W|^corn(o|a)\W|\Wcorn(o|a)$)
Corno(a) manso(a)	((?i)\Wcorn(o|a)\smans(o|a)\W|^corn(o|a)\smans(o|a)\W|\Wcorn(o|a)\sman s(o|a)$)
Cornão	((?i)\Wcorn\Wo\W|^corn\Wo\W|\Wcorn\Wo$)
Currado(a)	((?i)\Wcurrad(o|a)\W|^currad(o|a)\W|\Wcurrad(o|a)$)
Cuzão/Cuzona	((?i)\Wcuz(ão|ona)\W|^cuz(ão|ona)\W|\Wcuz(ão|ona)$)
Do caralho	((?i)\Wdo\scaralho\W|^do\scaralho\W|\Wdo\scaralho$)
Enrabado(a)	((?i)\Wenrabad(a|o)\W|^enrabad(a|o)\W|\Wenrabad(a|o)$)
Escroto(a)	((?i)\Wescrot(a|o)\W|^escrot(a|o)\W|\Wescrot(a|o)$)
Filho(a) do(a) Puto(a)	((?i)\Wfilh(a|o)\sd(a|o)\sput(a |o)\W|^filh(a|o)\sd(a|o)\sput (a|o)\W|\Wfilh(a|o)\sd(a|o)\s put(a|o)$)
Foda/Fodi/Fudi	((?i)\Wf(o|u)d(a|i)\W|^f(o|u)d(a|i)\W|\Wf(o|u)d(a|i)$)
Foda-se	((?i)\Wfoda-se\W|^foda-se\W|\Wfoda-se$)
Foder/Fuder	((?i)\Wf(o|u)der\W|^f(o|u)der\W|\Wf(o|u)der$)
Fodido(a)/Fudido(a)	((?i)\Wf(o|u)did(a|o)\W|^f(o|u)did(a|o)\W|\Wf(o|u)did(a|o)$)
Grelhuda	((?i)\Wgrelhuda\W|^grelhuda\W|\Wgrelhuda$)
Nem fodendo/fudendo	((?i)\Wnem\sf(o|u)dendo\W|^nem\sf(o|u)dendo\W|\Wnem\sf(o|u)dendo$)
Pica	((?i)\Wpica\W|^pica\W|\Wpica$)
Porra	((?i)\Wporra\W|^porra\W|\Wporra$)
Porra nenhuma	((?i)\Wporra\snenhuma\W|^porra\snenhuma\W|\Wporra\snenhuma$)
Punheta	((?i)\Wpunheta\W|^punheta\W|\Wpunheta$)
Puto(a)	((?i)\Wput(o|a)\W|^put(o|a)\W|\Wput(o|a)$)
Siririca	((?i)\Wsiririca\W|^siririca\W|\Wsiririca$)
Transar	((?i)\Wtransar\W|^transar\W|\Wtransar$)
Vadio(a)	((?i)\Wvadi(o|a)\W|^vadi(o|a)\W|\Wvadi(o|a)$)
Vagabundo(a)	((?i)\Wvagabund(a|o)\W|^vagabund(a|o)\W|\Wvagabund(a|o)$)
Vai pro Caralho	((?i)\Wvai\spro\scaralho\W|^vai\spro\scaralho\W|\Wvai\spro\scaralho$)
Vai tomar no Cú	((?i)\Wvai\stomar\sno\sc(ú|u)\W|^vai\stomar\sno\sc(ú|u)\W|\Wvai\stomar\s no\sc(ú|u)$)
Vou te foder/fuder	((?i)\Wvou\ste\sf(o|u)der\W|^vou\ste\sf(o|u)der\W|\Wvou\ste\sf(o|u)der$)
Xana	((?i)\Wxana\W|^xana\W|\Wxana$)
Xoxota	((?i)\Wxoxota\W|^xoxota\W|\Wxoxota$)

Metacaracteres do RegEx

metacaractere	conhecido como	significado
`.`	Único curinga	qualquer caractere, exceto a quebra de linha `\n`
`.*`	Expressão Curinga	qualquer caractere, exceto a quebra de linha `\n` (só que com conjunto total de caracteres, comportando strings inteiras, ou até mesmo frases). Por exemplo: .*hscbrasil\.com\.br = Qualquer caracter antes do hscbrasil.com.br. Ex: abc**hscbrasil.com.br** Outro exemplo: hscbrasil.*\.com\.br casaria com **hscbrasil**xxxyyyzzz123abc098**.com.br**

`[...]`
 	
`[^...]`
	conjunto
	
	conjunto negado
		qualquer caractere incluido no conjunto
		
		qualquer caractere não incluido no conjunto

`\d`	dígito	o mesmo que `[0-9]`
`\D`	não-digíto	o mesmo que `[^0-9]`
`\s`	branco	espaço, quebra de linha, tabs etc.; o mesmo que `[ \t\n\r\f\v]`
`\S`	não-branco	o mesmo que `[^ \t\n\r\f\v]`
`\w`	alfanumérico	o mesmo que `[a-zA-Z0-9_]` (mas pode incluir caracteres Unicode; ver *flag_unicode*)
`\W`	não-alfanumérico	o complemento de `\w`
`\`	escape	anula o significado especial do metacaractere seguinte; por exemplo, `\.` representa apenas um ponto, e não o curinga

metacaractere	significado
`{n}`	exatamente *n* ocorrências
`{n,m}`	no mínimo *n* ocorrências e no máximo *m*

metacaractere	significado
`{n,}`	no mínimo *n* ocorrências
`{,n}`	no máximo *n* ocorrências
`?`	0 ou 1 ocorrência; o mesmo que `{,1}`
`+`	1 ou mais ocorrência; o mesmo que `{1,}`
`*`	0 ou mais ocorrência
`«q»?`	modera qualquer um dos quantificadores acima (ver *Gula × moderação*)

`[^0-9]`	representa todos os caracteres da tabela ASCII menos os numéricos
	`!"#$%&'()*+,-./0123456789:;<=>?`
	`@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`
	`` `abcdefghijklmnopqrstuvwxyz{|}~¡ ``
	`¢£¤¥¦§¨©ª«¬®¯°±²³´µ¶·¸¹º»¼½¾¿ÀÁÂ`
	`ÃÄÅÆÇÈÉÊÈÌÍÎÏÐÑÒÓÔÕÖ×ØÙÚÛÜÝÞßàáâ`
	`ãäåæçèéêëìíîïðñòóôõö÷øùúûüýþÿ`

`[A-Za-z0-9]`	casa com os símbolos **alfa numéricos** (números, letras maiúsculas e minúsculas) porém todas sem acento.
	`!"#$%&'()*+,-./0123456789:;<=>?`
	`@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`
	`` `abcdefghijklmnopqrstuvwxyz{|}~¡ ``
	`¢£¤¥¦§¨©ª«¬®¯°±²³´µ¶·¸¹º»¼½¾¿ÀÁÂ`
	`ÃÄÅÆÇÈÉÊÈÌÍÎÏÐÑÒÓÔÕÖ×ØÙÚÛÜÝÞßàáâ`
	`ãäåæçèéêëìíîïðñòóôõö÷øùúûüýþÿ`

`[A-Za-z]`	casa apenas com letras maiúscula e minúsculas.
	`!"#$%&'()*+,-./0123456789:;<=>?`
	`@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`
	`` `abcdefghijklmnopqrstuvwxyz{|}~¡ ``
	`¢£¤¥¦§¨©ª«¬®¯°±²³´µ¶·¸¹º»¼½¾¿ÀÁÂ`
	`ÃÄÅÆÇÈÉÊÈÌÍÎÏÐÑÒÓÔÕÖ×ØÙÚÛÜÝÞßàáâ`
	`ãäåæçèéêëìíîïðñòóôõö÷øùúûüýþÿ`

`[A-z]`	alcançará todas as letras, incluindo as maiúsculas e minúsculas, mas ela vai pegar algo a mais além das letras do alfabeto.
	`!"#$%&'()*+,-./0123456789:;<=>?`
	`@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`
	`` `abcdefghijklmnopqrstuvwxyz{|}~¡ ``
	`¢£¤¥¦§¨©ª«¬®¯°±²³´µ¶·¸¹º»¼½¾¿ÀÁÂ`
	`ÃÄÅÆÇÈÉÊÈÌÍÎÏÐÑÒÓÔÕÖ×ØÙÚÛÜÝÞßàáâ`
	`ãäåæçèéêëìíîïðñòóôõö÷øùúûüýþÿ`

metacaractere	significado

`[A-Z]`	casa com a letras maiúsculas (também sem acentos).
	`!"#$%&'()*+,-./0123456789:;<=>?`
	`@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`
	`` `abcdefghijklmnopqrstuvwxyz{|}~¡ ``
	`¢£¤¥¦§¨©ª«¬®¯°±²³´µ¶·¸¹º»¼½¾¿ÀÁÂ`
	`ÃÄÅÆÇÈÉÊËÌÍÎÏÐÑÒÓÔÕÖ×ØÙÚÛÜÝÞßàáâ`
	`ãäåæçèéêëìíîïðñòóôõö÷øùúûüýþÿ`

`[a-z]`	casa com todas as minúsculas sem acentos.
	`!"#$%&'()*+,-./0123456789:;<=>?`
	`@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`
	`` `abcdefghijklmnopqrstuvwxyz{|}~¡ ``
	`¢£¤¥¦§¨©ª«¬®¯°±²³´µ¶·¸¹º»¼½¾¿ÀÁÂ`
	`ÃÄÅÆÇÈÉÊËÌÍÎÏÐÑÒÓÔÕÖ×ØÙÚÛÜÝÞßàáâ`
	`ãäåæçèéêëìíîïðñòóôõö÷øùúûüýþÿ`

`[aeiou]`	casa com as vogais.

metacaractere	significado
`^`	início do texto, ou de uma linha com o flag `re.MULTILINE`
`\A`	início do texto
`$`	fim do texto, ou de uma linha com o flag `re.MULTILINE`; não captura o `\n` no fim do texto ou da linha

`\Z`
 	
`\b`
	fim do texto
	
	posição de borda, logo antes do início de uma palavra, ou logo depois do seu término;
	
	o mesmo que a posição entre `\W` e `\w` ou vice-versa
	
	Exemplo de borda:
	
	REGULAR EXPRESSION
	`/ \bcomercial@sauk.com.br\b`
	TEST STRING
	`vcomercial@sauk.com.br`
	`comercial@sauk.com.br`
	`xxxcomercial@sauk.com.br`
	
	Repare que com a borda (boundarie), ele detecta somente o comercial@sauk.com.br

metacaractere	significado
	Já sem isso, ele pega qualquer expressão que contenha comercial@sauk.com.br. Segue abaixo expressão sem borda configurada. REGULAR EXPRESSION / comercial@sauk.com.br TEST STRING vcomercial@sauk.com.br comercial@sauk.com.br xxxcomercial@sauk.com.br Repare que ele casa com qualquer expressão que contenha comercial@sauk.com.br
`\B`	posição de não-borda (Exatamente ao contrário da borda, ou seja, força a expressão a não possuir borda para limitação da string)

metacaractere	significado
`(...)`	define um *grupo*, para efeito de aplicação de quantificador, alternativa ou de posterior extração ou re-uso
`...|...`	alternativa; casa a regex à direita ou à esquerda
`\«n»`	recupera o texto casado no n-ésimo grupo

Apêndice 4 – DLP

Modelos de DLP

O MailInspector já possui diversos dicionários de palavras constituído junto com a solução, bem como permite que o administrador crie suas próprias expressões/dicionário de palavras para ser utilizado em regras de DLP, dessa forma permitindo mais de 500 modelos para criação de regras de DLP, casando tanto dicionários de palavras (já pré-cadastrados e dicionários que podem ser criados e/ou importados), quanto Finger Print de arquivos.

É ainda possível casar regras de DLP, junto com grupos de usuários, padrão de anexos, mime-types, etc.

Exemplo de DLP – Cartão de Crédito

Objetivo da regra do DLP:

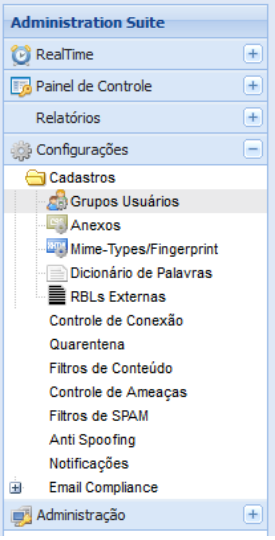
Detectar, bloquear (evitar que o e-mail siga adiante para entrega), registrar log e mandar alerta para monitoramento@hscbrasil.com.br, os e-mails que saem do domínio hscbrasil.com.br que contenham números de cartão de crédito nele.

Planejamento das ações:

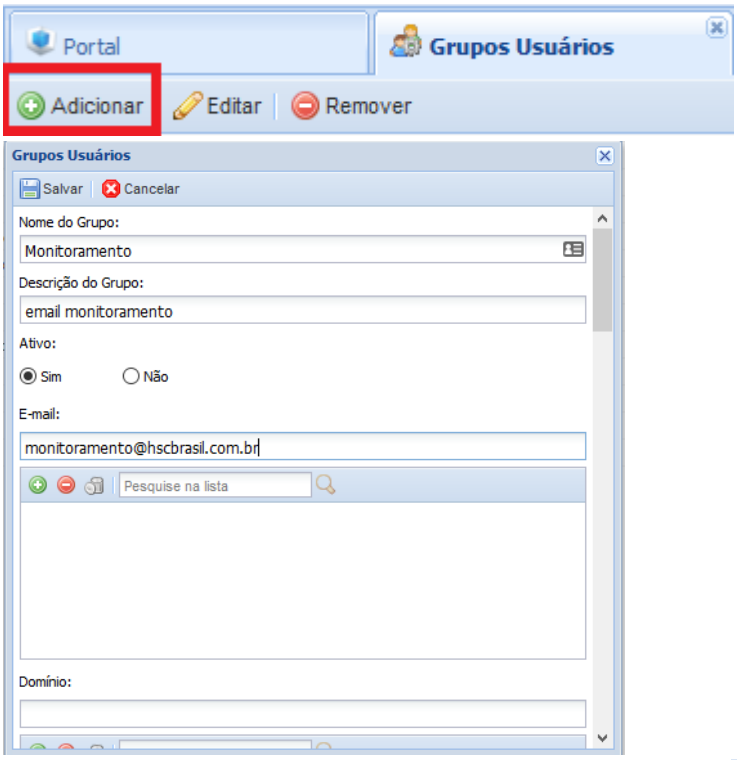
a) Criar um Grupo de Usuários chamado **Monitoramento** contendo o e-mail monitoramento@hscbrasil.com.br
b) Criar um Grupo de Usuários chamado **Dominio HSC** contendo o domínio hscbrasil.com.br
c) Criar uma regra de DLP para o Grupo de Usuários **Dominio HSC**
d) Criar uma regra de DLP para a ação de detecção de Cartão de Crédito
e) Concatenar as duas regras de DLP previamente criadas, configurando a ação desejada, que no caso é bloquear, registar log e disparar um aviso ao Monitoramento

Executando as ações anteriormente planejadas:

1. Criar um Grupo de Usuários chamado **Monitoramento** contendo o e-mail monitoramento@hscbrasil.com.br
   Crie um Grupo de Usuários com o e-mail monitoramento@hscbrasil.com.br
   Configurações > Cadastro > Grupo de Usuários

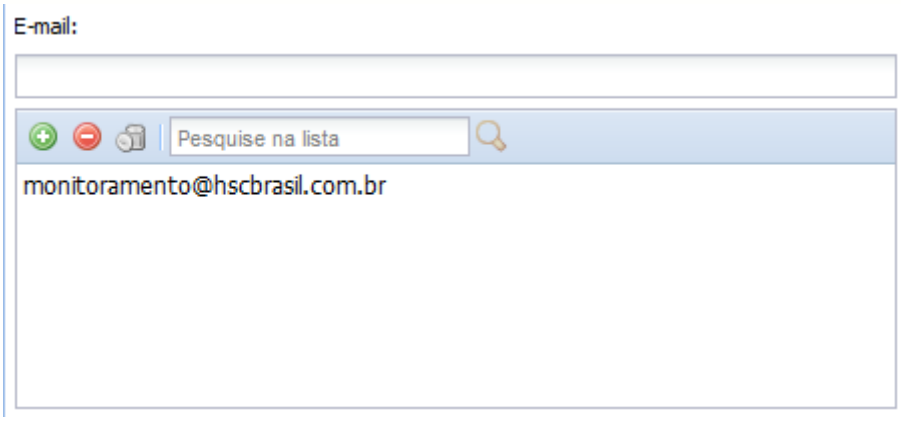


Clique em Adicionar



Preencha os campos solicitados. Não esqueça de clicar no sinal de ( ) para adicionar o domínio na

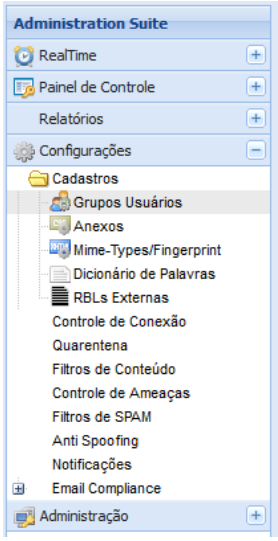
regra.



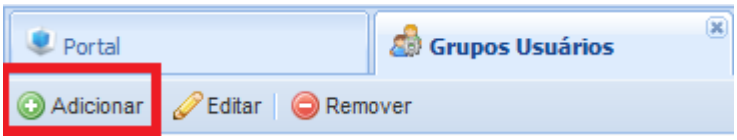
Clique em Salvar

Monitoramento	email monitoramento	Sim

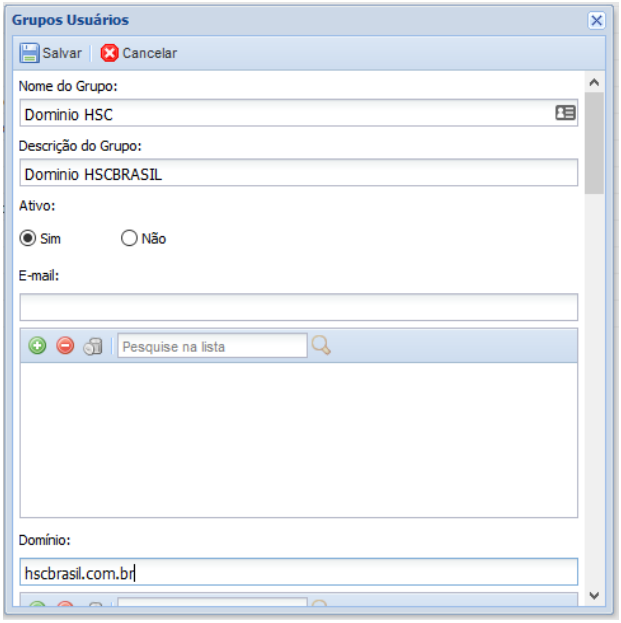
2. Criar um Grupo de Usuários chamado **Dominio HSC** contendo o domínio hscbrasil.com.br
   Crie um Grupo de Usuários com o domínio hscbrasil.com.br.
   Configurações > Cadastro > Grupo de Usuários

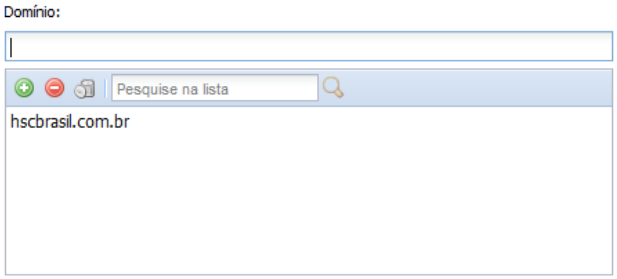


Clique em Adicionar



Preencha os campos solicitados. Não esqueça de clicar no sinal de ( ) para adicionar o domínio na regra.

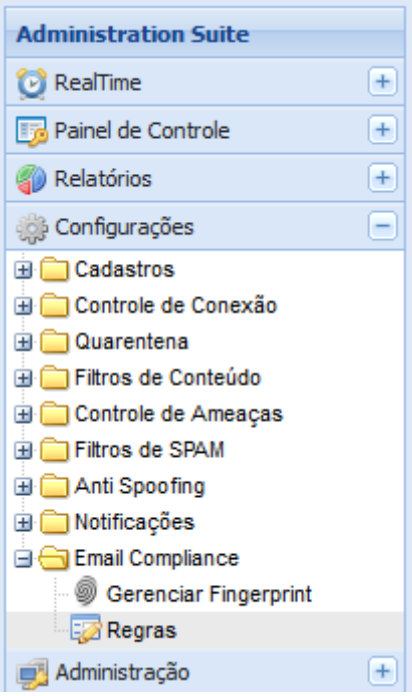




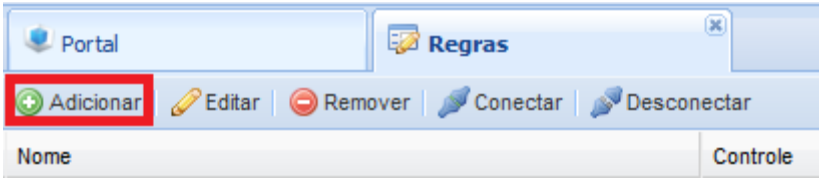
Clique em Salvar

Dominio HSC	Dominio HSCBRASIL	Sim

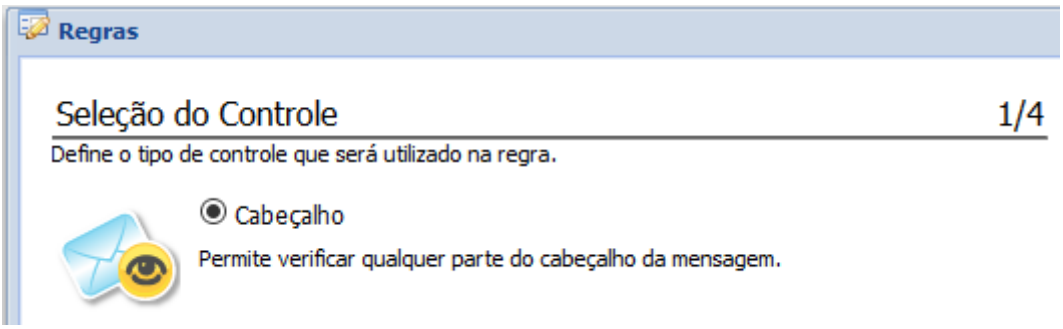
3. Criar uma regra de DLP para o Grupo de Usuários **Dominio HSC**
   Configurações > E-mail Compliance > Regras



Clique em Adicionar



Selecione a opção Cabeçalho

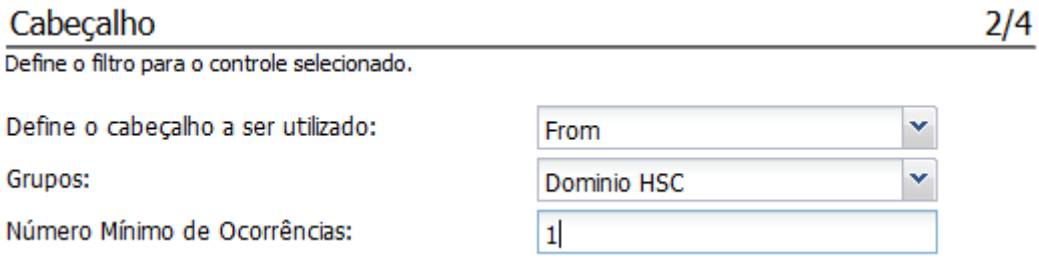


Clique em Avançar

No campo **Define o cabeçalho a ser utilizado: From**

No campo **Grupos: Dominio HSC**

No campo **Número Mínimo de Ocorrências: 1**



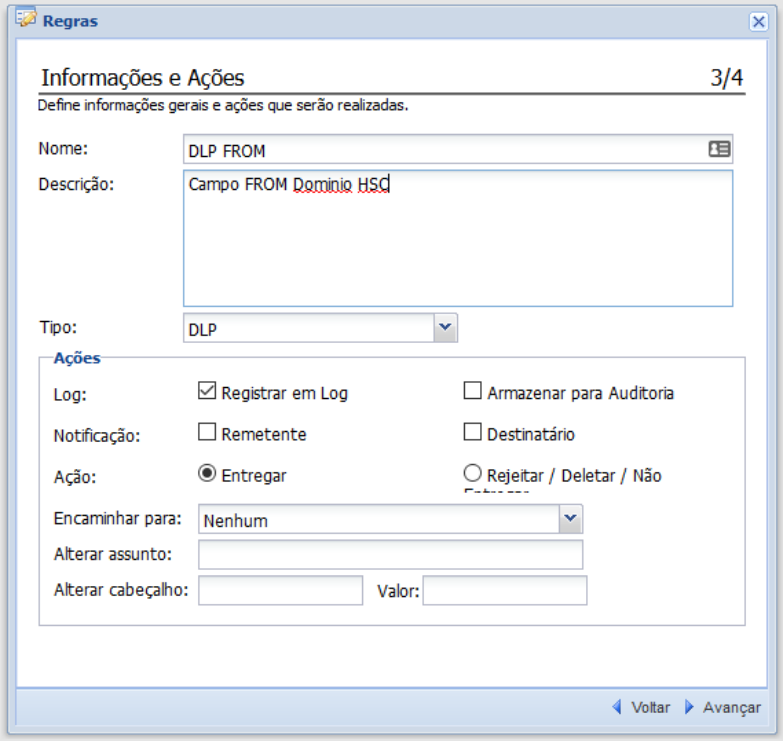
Clique em Avançar

No campo **Nome: DLP FROM**

No campo **Descrição: Campo FROM Dominio HSC**

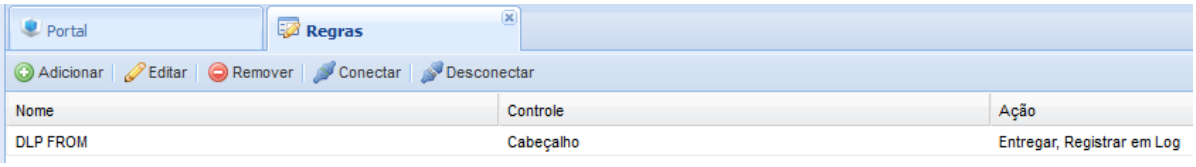
No campo **Tipo: DLP**

No campo **Ações: Pode deixar como está, nesse momento não é necessário definir ação.**



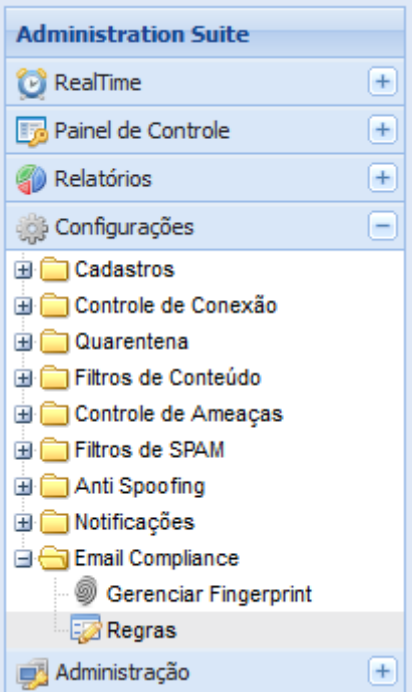
Clique em Avançar

Clique em Salvar

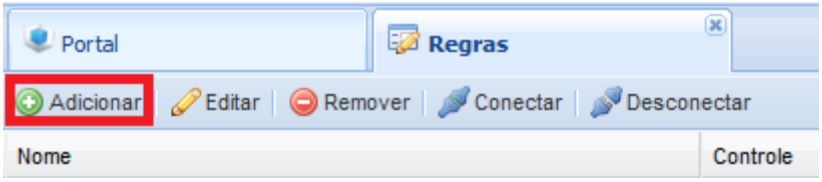


4. Criar uma regra de DLP para a ação de detecção de Cartão de Crédito

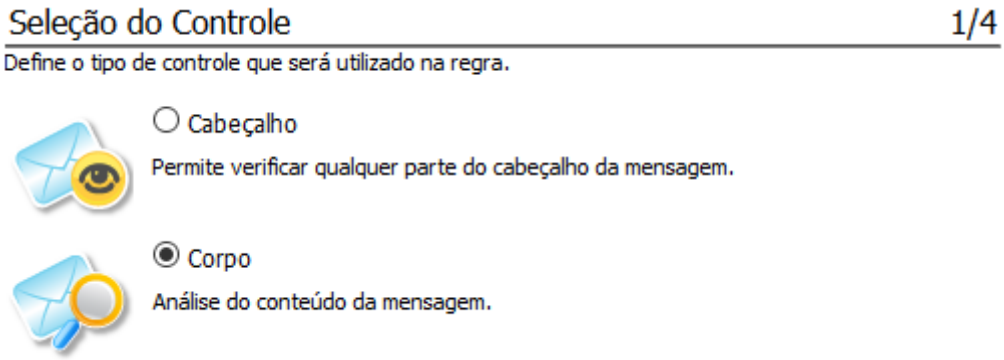
   Configurações > E-mail Compliance > Regras



Clique em Adicionar



Selecione a opção Corpo

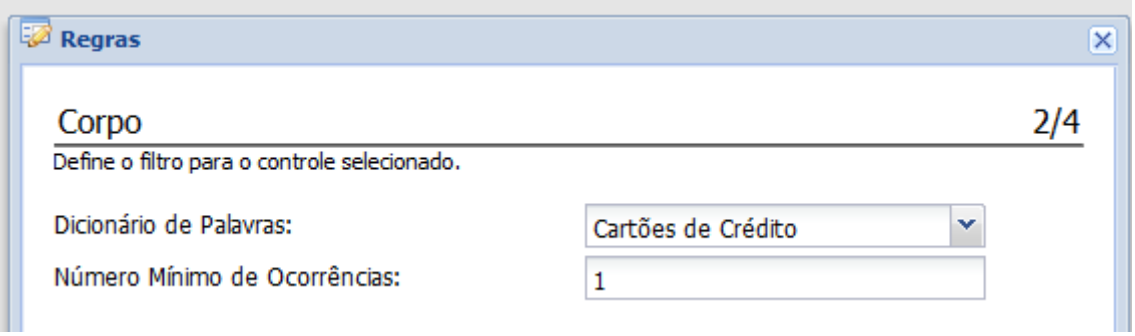


Clique em Avançar

No campo **Dicionário de Palavras: Cartões de Crédito**

No campo **Número de Ocorrências: 1**

Como já tínhamos o dicionário de palavras Cartões de Crédito já criado, não houve a necessidade de criar isso, mas caso você não tenha um dicionário de palavras previamente criado, é necessário cria-lo. Para isso, vá em Cadastro > Grupos de Usuário e crie o grupo, de acordo com a condição mais apropriada para o DLP.



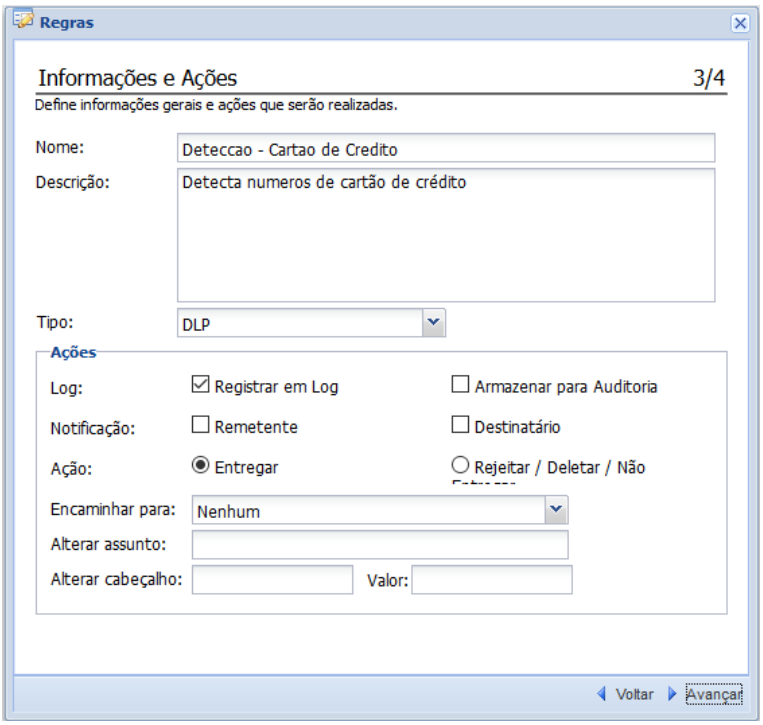
Clique em Avançar

No campo **Nome: Deteccao – Cartao de Credito**

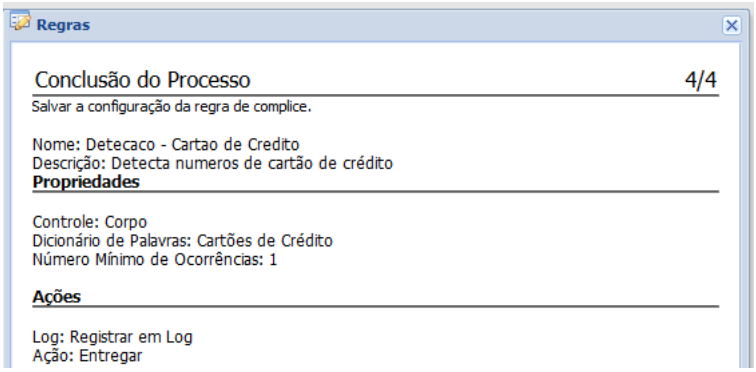
No campo **Descrição: Detecta números de cartão de crédito**

No campo **Tipo: DLP**

No campo **Ações: Pode deixar como está, nesse momento não é necessário definir ação.**



Clique em Avançar



Clique em Salvar

Detecaco - Cartao de Credito	Corpo	Entregar, Registrar em Log

5. Concatenar as duas regras, configurando a ação desejada, que no caso é bloquear, registar log e disparar um aviso ao Monitoramento.

Selecione as duas regras de DLP

Clique no botão Conectar

No campo **DLP FROM: Casar**

No campo **Operador Lógico: E**

No campo **Deteccao – Cartao de Credito: Casar**

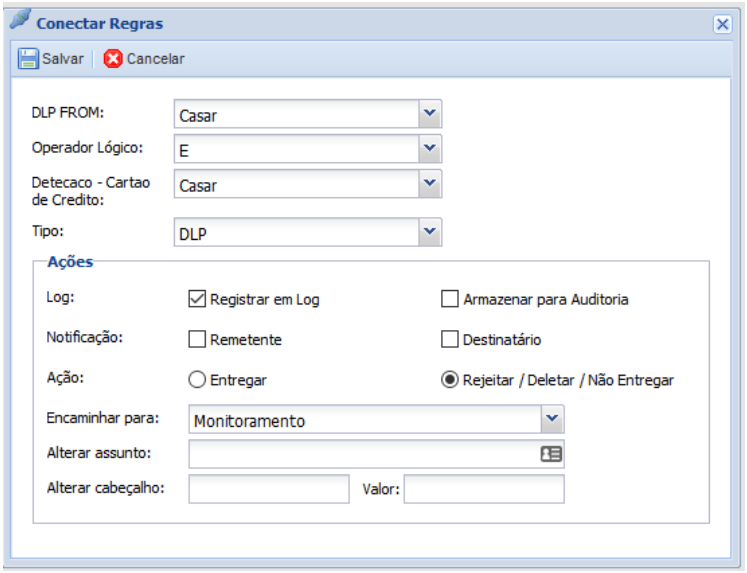
No campo **Tipo: DLP**

No campo **Log: Registrar em Log**

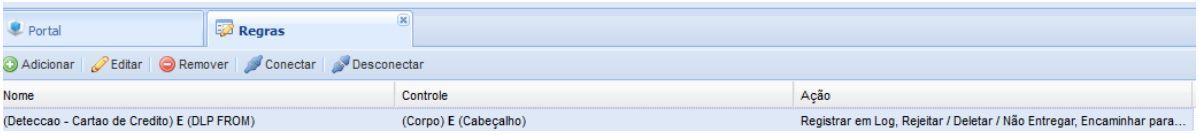
No campo **Notificação: Não marque nada** (para não gerar aviso nem ao remetente, nem ao destinartário)

No campo **Ação: Rejeitar/Deletar/Não Entregar**

No campo **Encaminhar para: Monitoramento**



Clique em Salvar



Pronto! A regra de DLP está salva.

Agora basta clicar em **Aplicar Configurações**, para que a regra seja aplicada em TODO o sistema!

Apêndice 5 – FAQ's e HowTo's

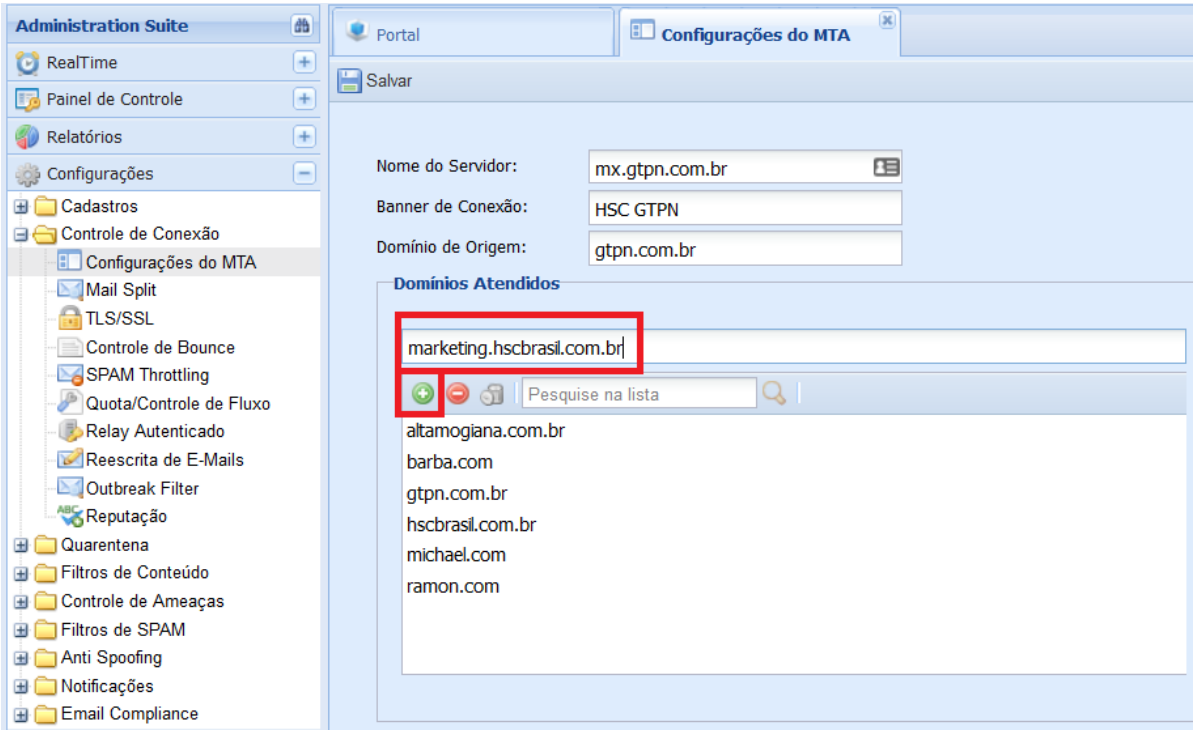
Adicionando subdomínios

Em muitos casos é necessário adicionar subdomínios à solução, tais como subdomínios de marketing, por exemplo **marketing.hscbrasil.com.br**, onde o domínio principal é **hscbrasil.com.br**

Para esses casos, basta ir em Configurações > Controle de Conexão > Configurações do MTA

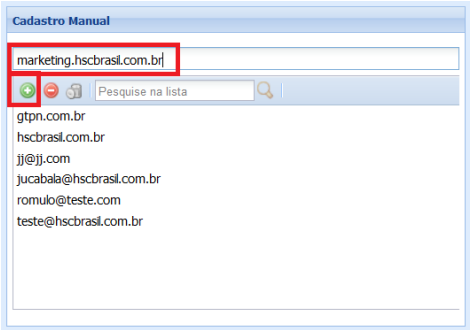
Vá na aba Configurações Gerais > Domínios Atendidos

Insira o sub-domínio desejado a lista.



Clique em (+) para adicionar o subdomínio na lista e clique no botão Salvar

Após isso, vá para a aba Catálogo de Endereços e na parte de Cadastro Manual, acrescente o subdomínio.



Clique em (+) e depois em Salvar

Clique no botão Aplicar Configurações para que as configurações salvas anteriormente sejam aplicadas no cluster.

Obs: Importante lembrar que é possível efetuar saída de e-mails por um IP específico.

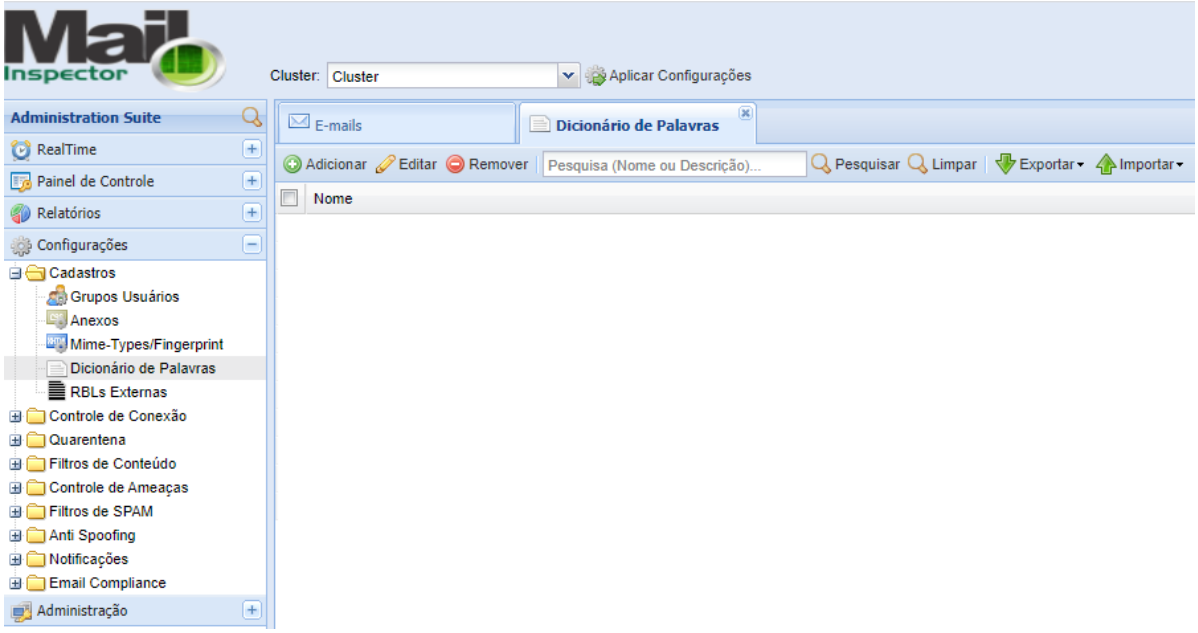
Criptografando e-mails quando começa com o assunto [CRIPTOGRAFADO]

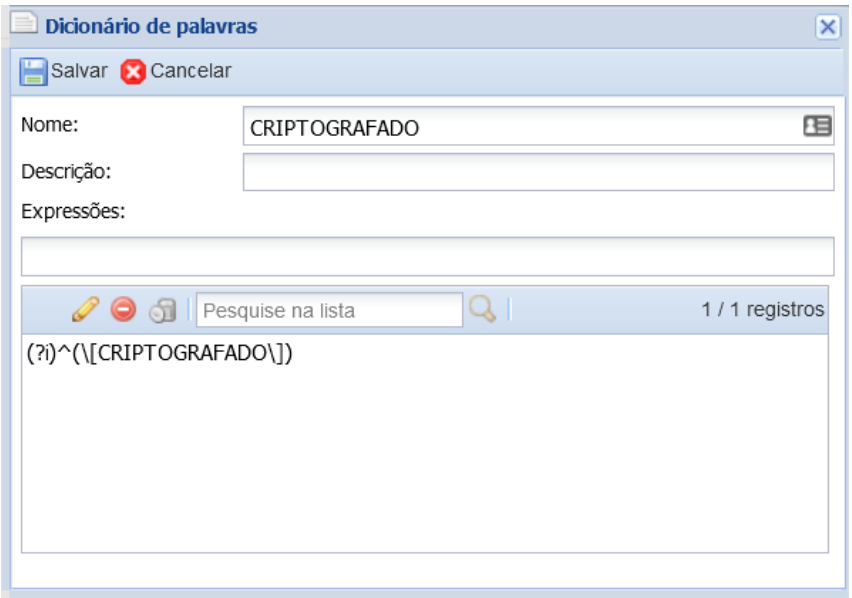
Vamos supor que quero enviar e-mails criptografados quando o assunto estiver **começando** com a palavra **[CRIPTOGRAFADO]**, sendo esta palavra CASE SENSITIVE.

Para isso, devo primeiramente criar um dicionário de palavra onde identifico a palavra [CRIPTOGRAFADO] no início do assunto.

Vá na aba Configurações > Cadastros > Dicionário de Palavras.

Selecione a opção Adicionar.





Explicando a string utilizada:

^(\[CRIPTOGRAFADO\])

Onde:

^ Indica início da frase

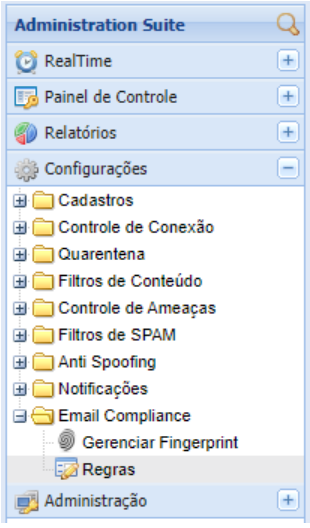
() Indica toda string que estiver entre os parênteses

\ Indica que o caracter seguinte a ser utilizado deve ser literalmente o caracter, ou seja colchete, tanto para aberura de colchete, quanto para fechamento do colchete.

Não esqueça de clicar em (+) e depois no botão Salvar.

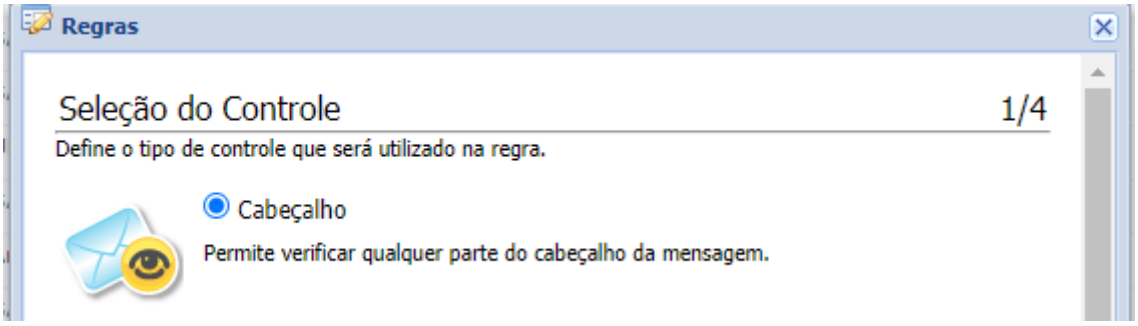
Agora vamos para a parte de E-mail Compliance, em:

Configurações > E-mail Compliance > Regras



Clique em Adicionar.

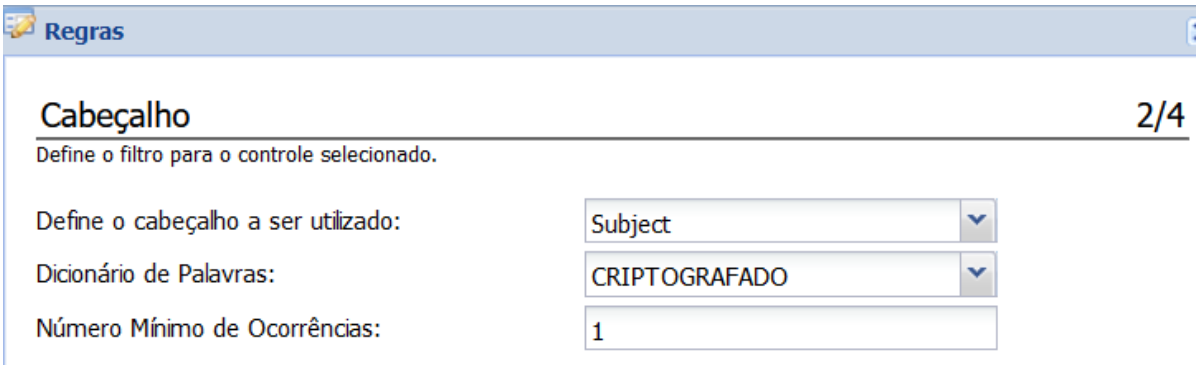
Selecione o Controle Cabeçalho e clique em Avançar



Define o cabeçalho a ser utilizado: Subject

Dicionário de Palavras: Selecione o dicionário que você cricou. No nosso exemplo é CRIPTOGRAFADO

Número Mínimo de Ocorrências: 1



Clique em Avançar

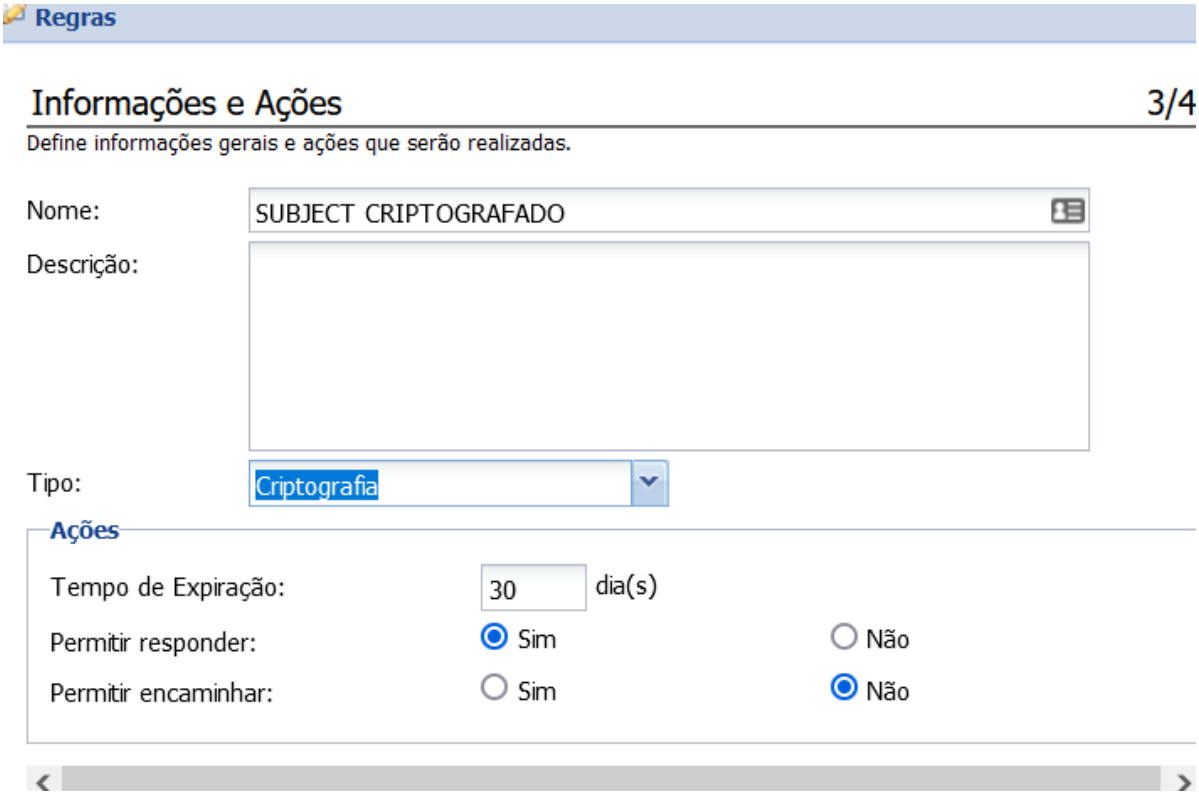
Crie um nome para a regra

Mude o Tipo para Criptografia

Determite o Tempo de Expiração em dias

Determine se pode permitir responder e se pode permitir encaminhar

Clique em Avançar



Por último, clique em Salvar.

Não esqueça de clicar em Aplicar Configurações.

Agora quando mandar um e-mail com a palavra [CRIPTOGRAFADO] no início do assunto, o e-mail será criptografado.

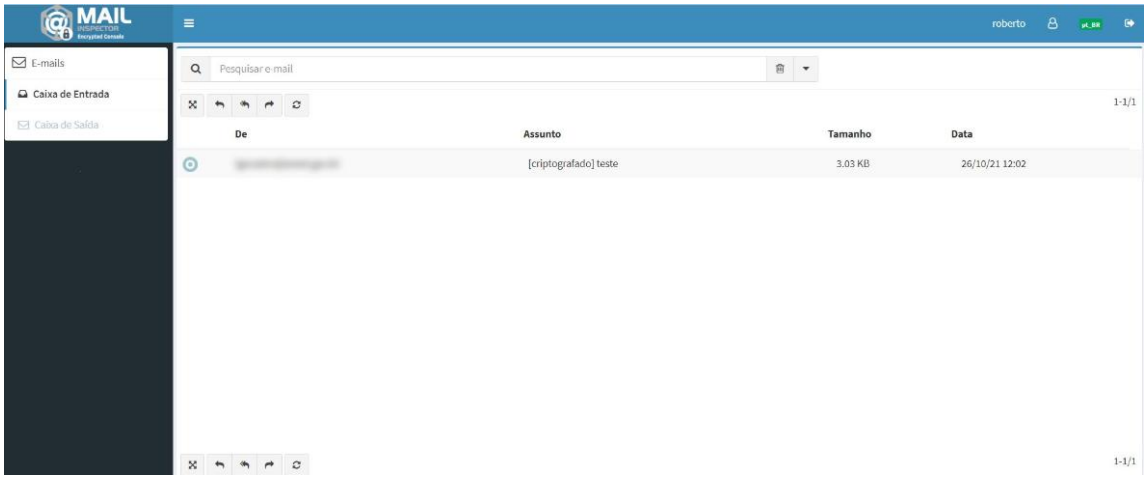
Na verdade, o sistema manda um e-mail para o destino informando que ele recebeu um e-mail criptografado e nesse mesmo e-mail, tem um link (que ao clicar, abre o browser em https) para o destinatário efetuar o cadastro (se não tiver cadastrado) ou se já tiver cadastrado, ele efetuar o login para a leitura do e-mail.

Dessa forma o e-mail em si, não sai do MailInspector, fica no MailInspector, onde é permitida a leitura do mesmo via browser.

A seguir, indicação de aplicação da regra criada. Ao mandar e-mail com a palavra [CRIPTOGRAFADO] no começo do assunto, ele irá disparar um e-mail ao destinatário com a seguinte informação:

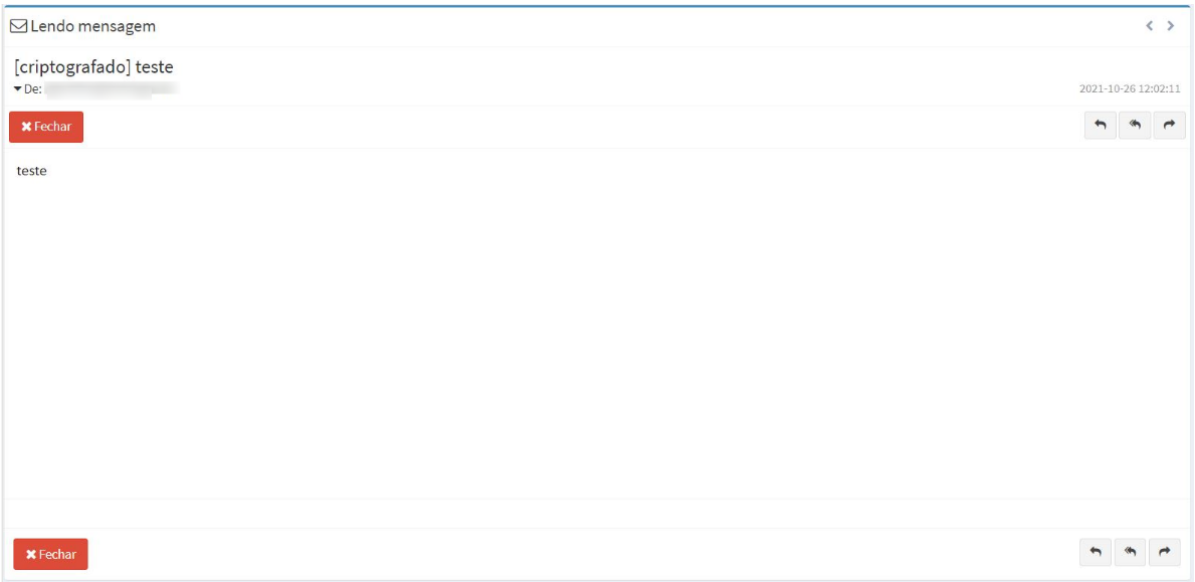
Exemplo de indicação de e-mail criptografado que o destinatário recebe

Depois que o destinatário tiver efetuado o cadastro e acessado o sistema de criptografia, ele acessa uma área específica dele para a leitura de e-mails.



Exemplo de indicação tela de acesso aos e-mails criptografados enviados ao destinatário

Basta selecionar o e-mail a ser lido, que o conteúdo será liberado ao destinatário.



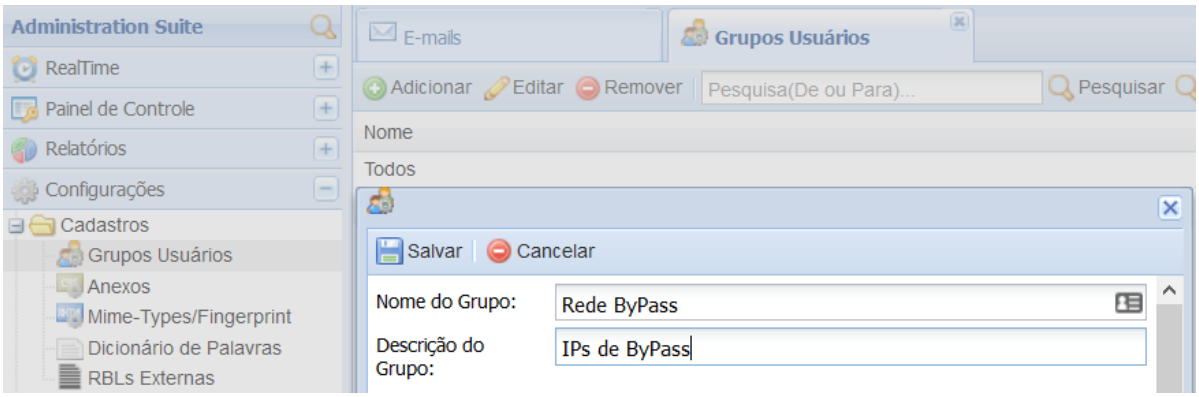
Exemplo de tela de leitura de e-mail criptografado

ByPass total no MailInspector

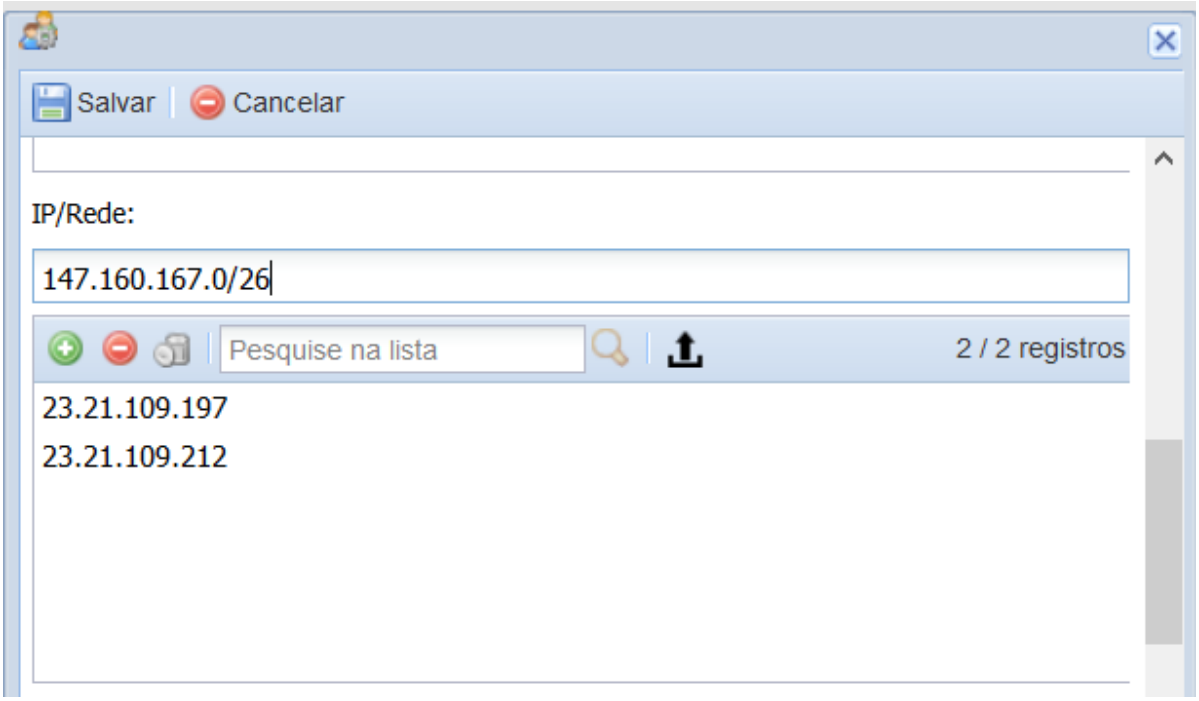
Vamos supor que o administrador tenha que efetuar um ByPass total no MailInspector (nem chegar a verificar a camada de conexão, isto é, se o e-mail tem o mínimo necessário para conectar no protocolo SMTP,como por exemplo verificar se o cabeçalho do e-mail está íntegro).

Vamos supor que queremos fazer ByPass dos e-mails oriundos dos seguintes Redes e IP's:
147.160.167.0/26
23.21.109.212
23.21.109.197

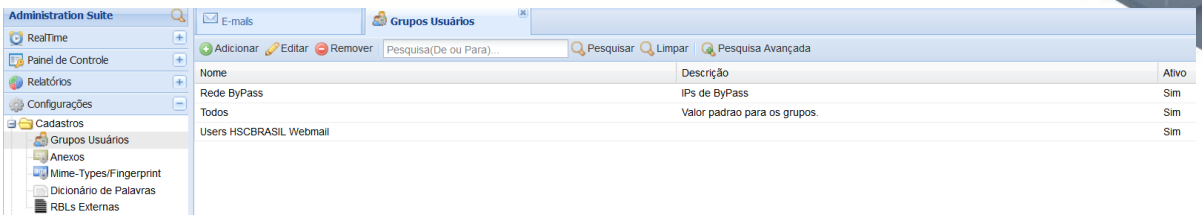
1. Primeiramente vamos griar um grupo para esses IP's e Redes:
   Vá em Configurações > Cadastros > Grupos Usuários
   Clique em Adicionar
   Insira o nome do Grupo e uma breve descrição.



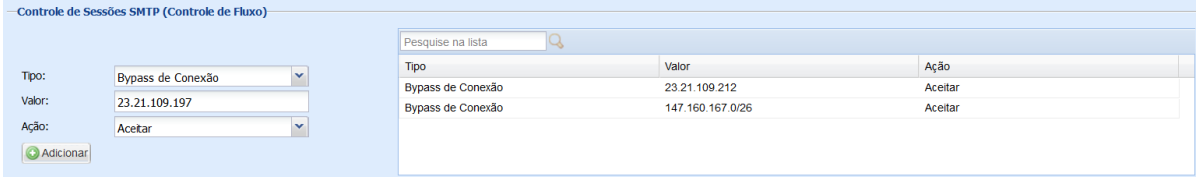
   Desça até onde indica IP/Rede e insira os IP's e a rede indicada:



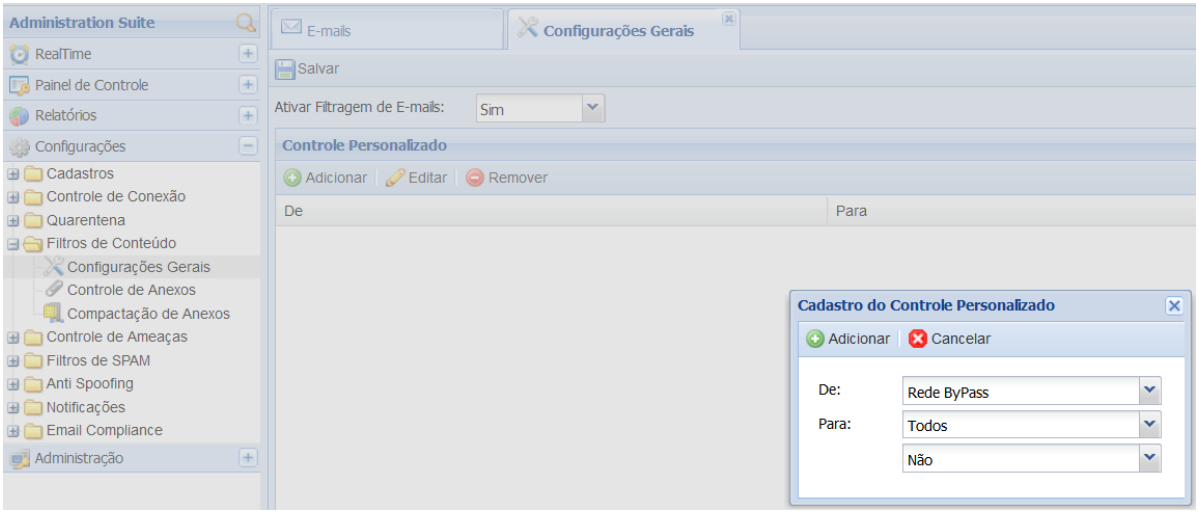
   Resultará em algo parecido com:



2. Vamos dar **ByPass** a nível de **Conexão**.
   Vá em Configurações > Controle de Conexão > Cnfigurações do MTA > Filtragem
   Na parte de **Controle de Sessões SMTP (Controle de Fluxo)** selecione:
   Tipo: ByPass de Conexão
   Valor: Insira os IPs e a rede
   Ação: Aceitar

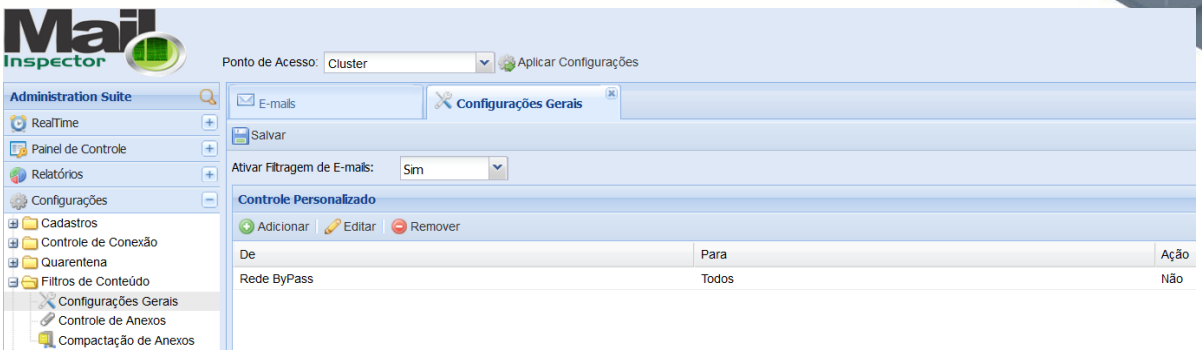


3. Agora vamos dar **ByPass** a nível de **Processamento**.
   Vá em Configurações > Filtro de Conteúdo > Configurações Gerais > Filtragem de E-mails
   Clique em Adicionar
   Selecione no campo:
   DE: O grupo que você criou anteriormente. No exemplo foi chamado de Rede ByPass
   PARA: Selecione a opção TODOS
   E por último selecione **NÃO**

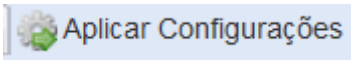


4. Clique em Adicionar e Clique em Salvar

   Deve ficar algo parecido com



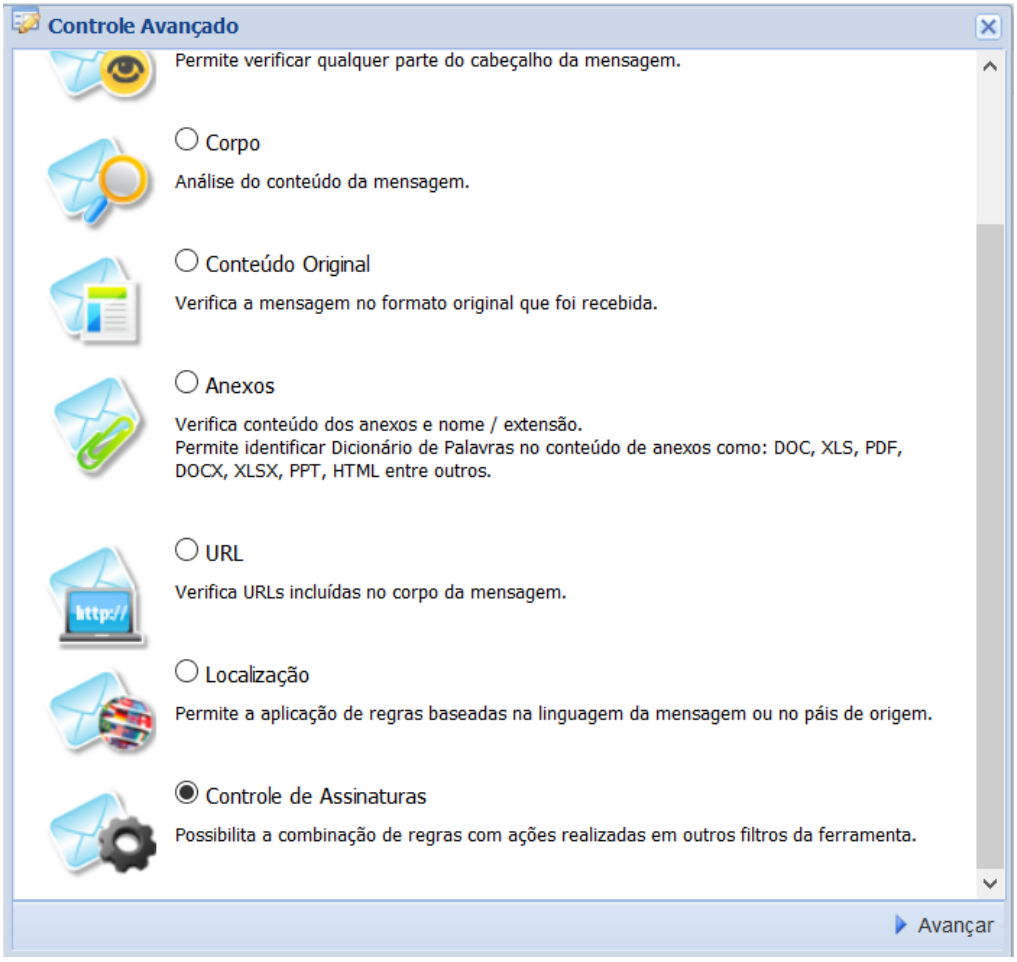
5. Clique em Aplicar Configurações

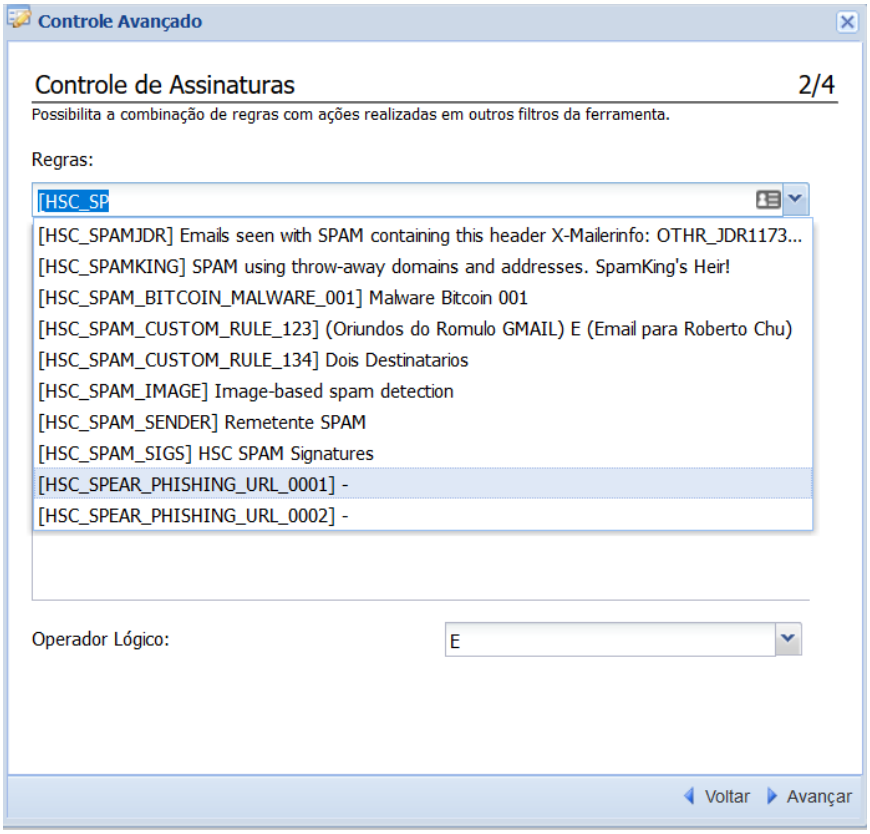


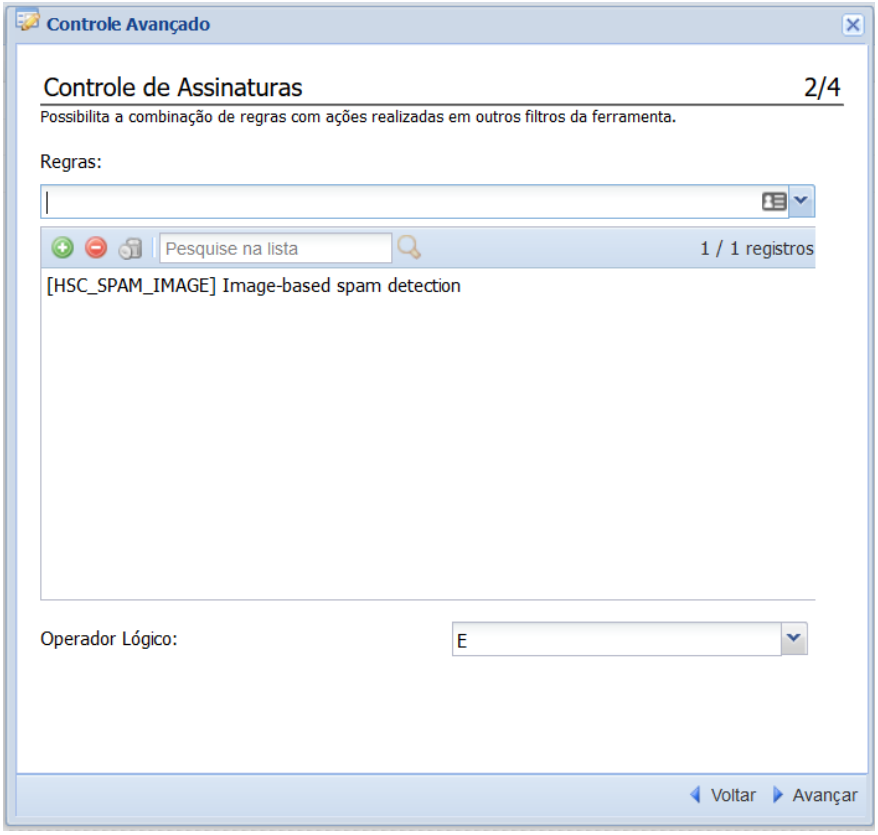
Aumento de pontuação de SPAM em Imagens diretamente por assinatura

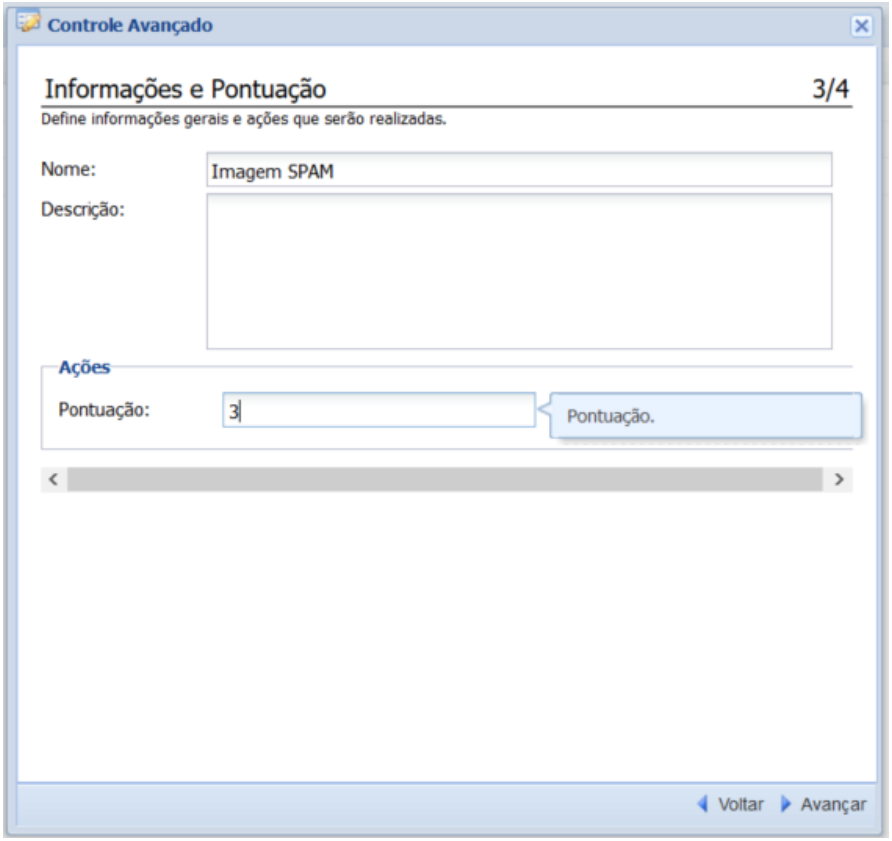
O MailInspector permite ao administrador criar/alterar as assinaturas utilizados, dessa forma ele já vem com uma série de assinaturas ao qual permite ao administrador modificar a pontuação deles na hora de computar se o e-mail é ou não spam.

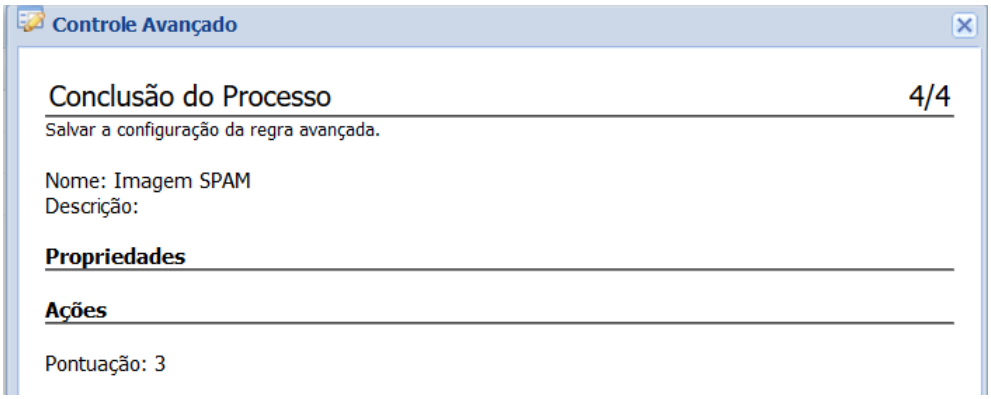
Por exemplo segue regra de aumento de pontuação, quando é detectado o SPAM em IMAGEM:




Controle Avançado
Controle de Assinaturas
2/4
Possibilita a combinação de regras com ações realizadas em outros filtros da ferramenta.
Regras:
[HSC_SP
[HSC_SPAMJDR] Emails seen with SPAM containing this header X-Mailerinfo: OTHR_JDR1173...
[HSC_SPAMKING] SPAM using throw-away domains and addresses. SpamKing's Heir!
[HSC_SPAM_BITCOIN_MALWARE_001] Malware Bitcoin 001
[HSC_SPAM_CUSTOM_RULE_123] (Oriundos do Romulo GMAIL) E (Email para Roberto Chu)
[HSC_SPAM_CUSTOM_RULE_134] Dois Destinatarios
[HSC_SPAM_IMAGE] Image-based spam detection
[HSC_SPAM_SENDER] Remetente SPAM
[HSC_SPAM_SIGS] HSC SPAM Signatures
[HSC_SPEAR_PHISHING_URL_0001] -
[HSC_SPEAR_PHISHING_URL_0002] -
Operador Lógico:
E
Voltar
Avançar


Controle Avançado
Controle de Assinaturas
2/4
Possibilita a combinação de regras com ações realizadas em outros filtros da ferramenta.
Regras:
Pesquise na lista
1 / 1 registros
[HSC_SPAM_IMAGE] Image-based spam detection
Operador Lógico:
E
Voltar
Avançar





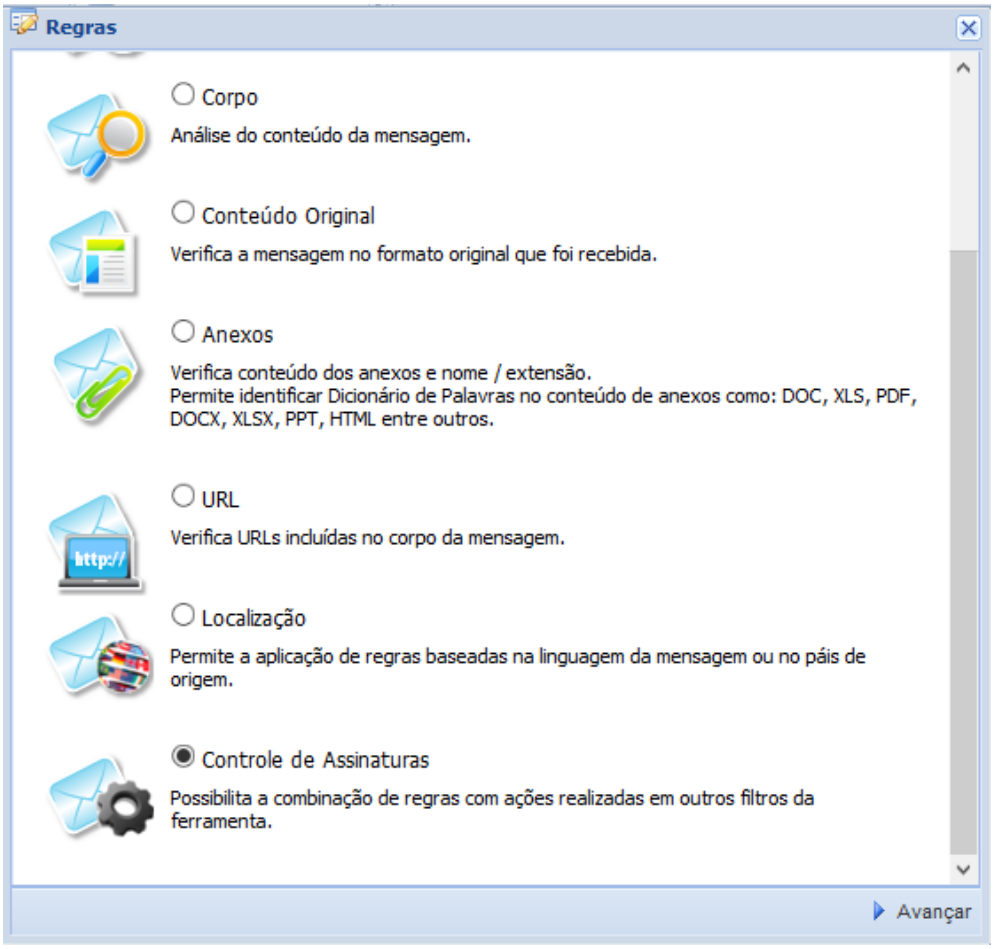
135	Imagem SPAM	SA_RULES	Pontuação: 3

Bloqueio de SPAM em Imagens diretamente por assinatura

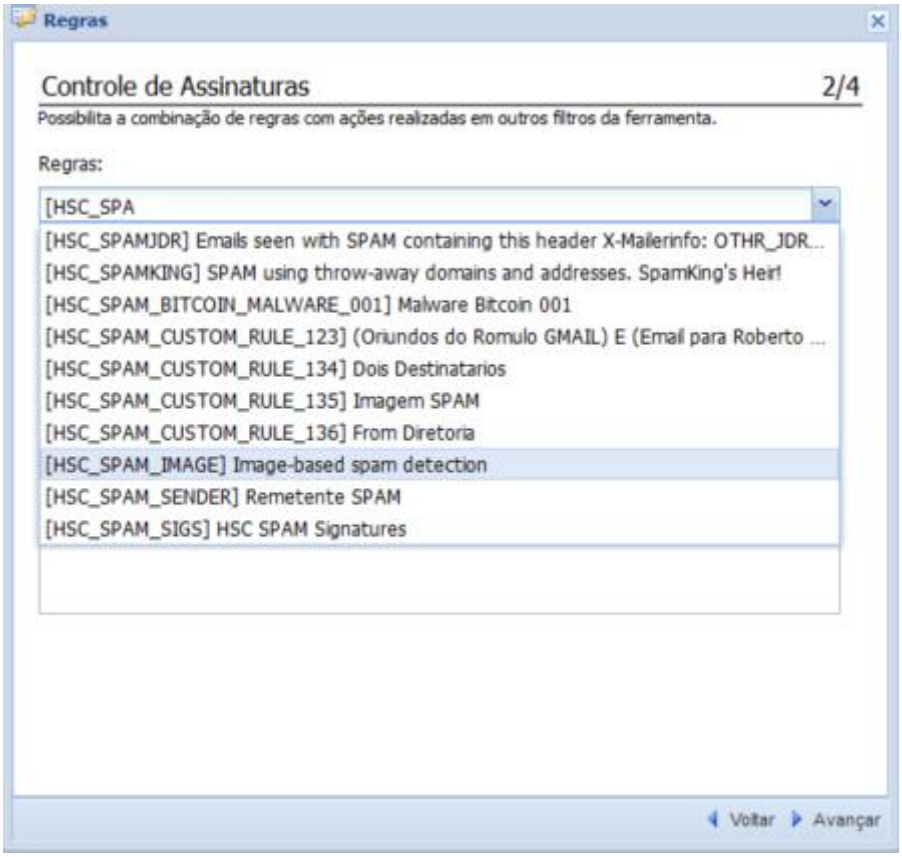
O MailInspector permite ao administrador criar/alterar as assinaturas utilizados, dessa forma ele já vem com uma série de assinaturas ao qual permite ao administrador modificar a pontuação deles na hora de computar se o e-mail é ou não spam.

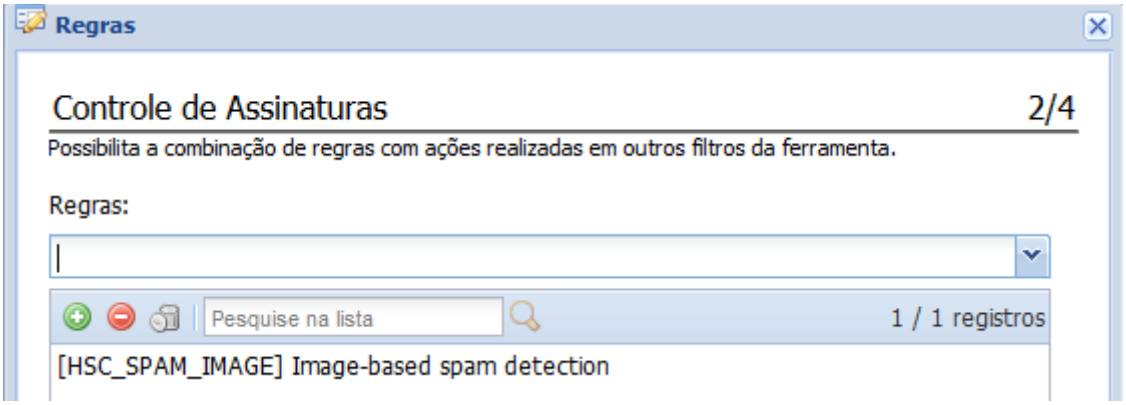
É possível efetuar o bloqueio de SPAM em IMAGEM por E-mail Compliance:

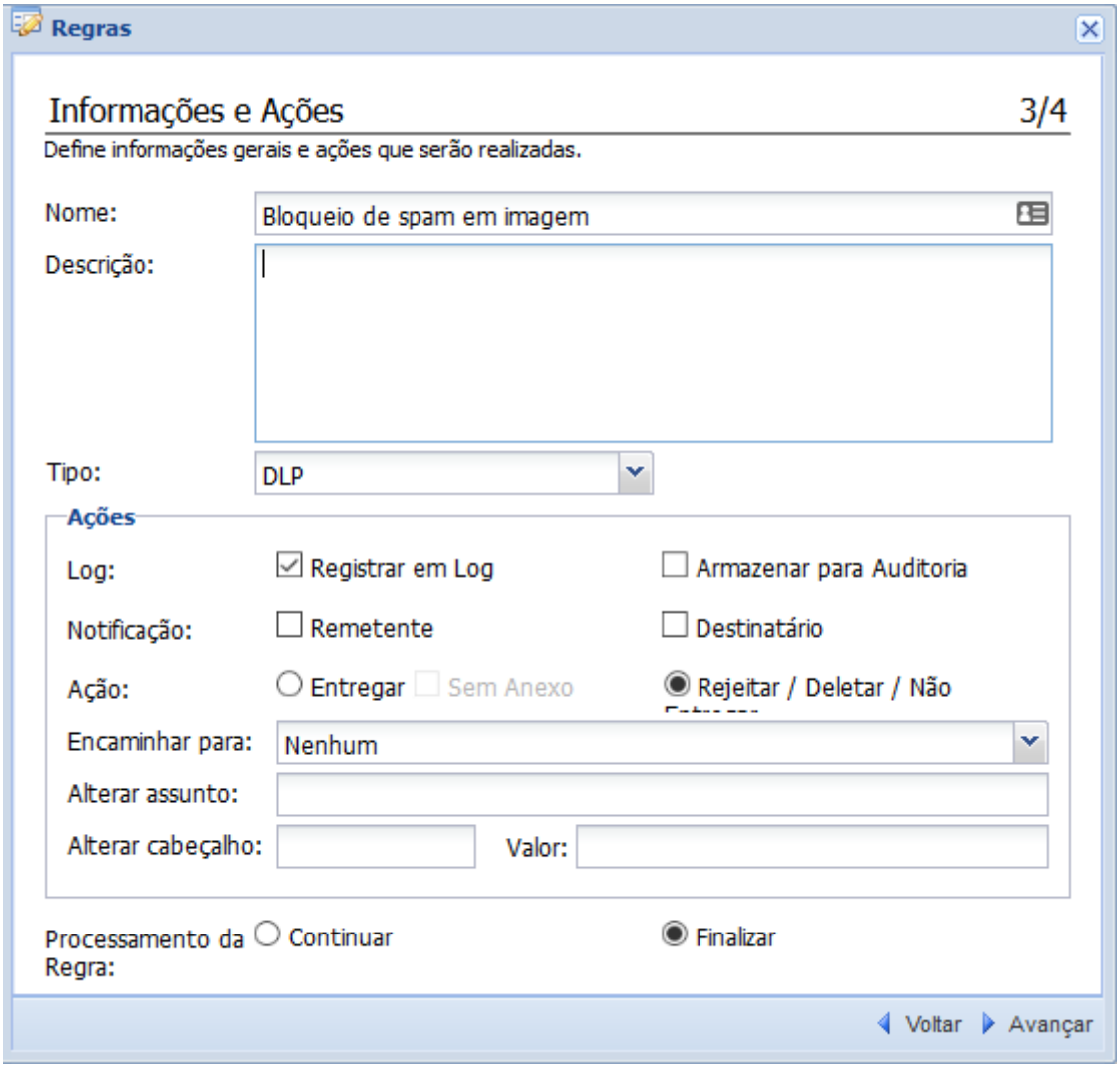
Adicione uma nova regra de E-mail Compliance, usando como filtro o Controle de Assinaturas

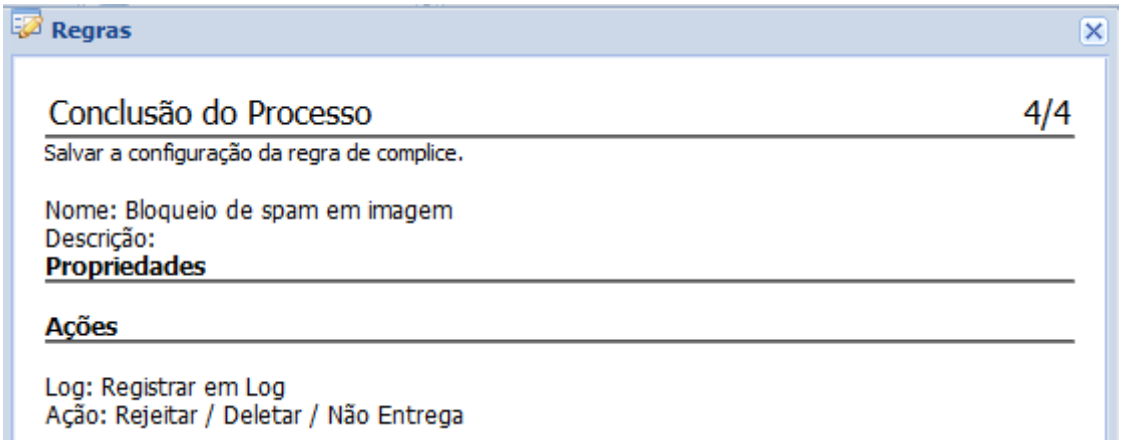


Selecione a assinatura [HSC_SPAM_IMAGE]







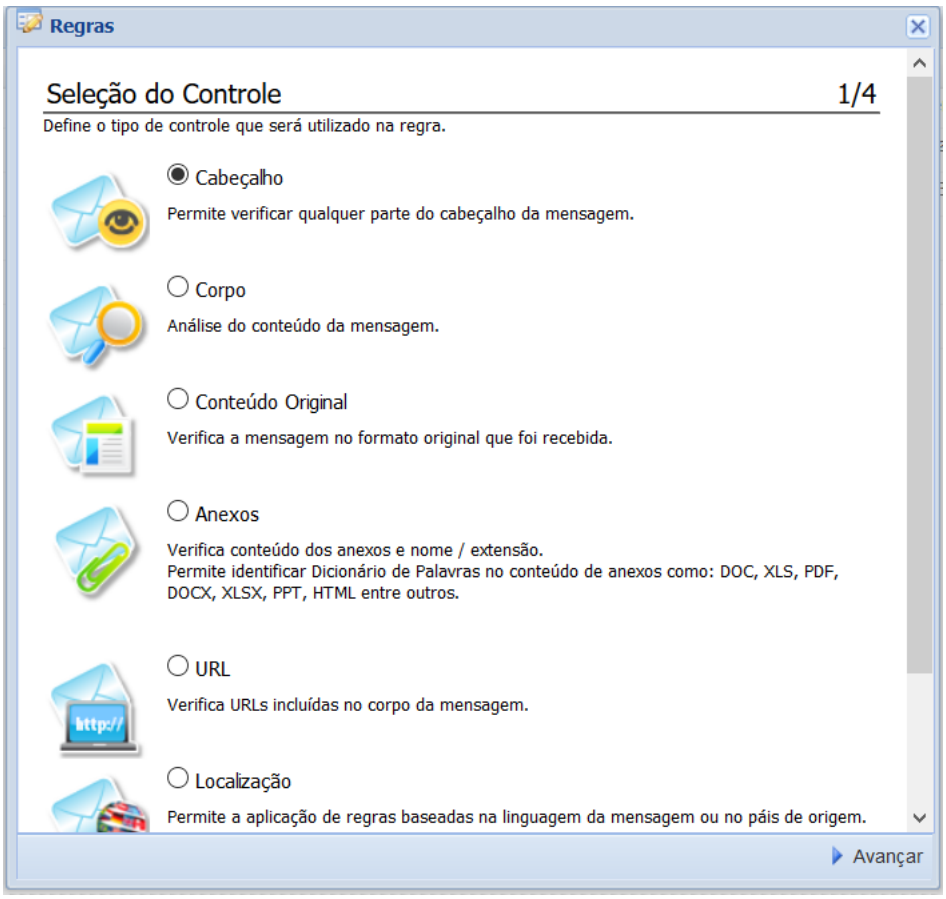


Agora basta Salvar a regra e Aplicar as Configurações.

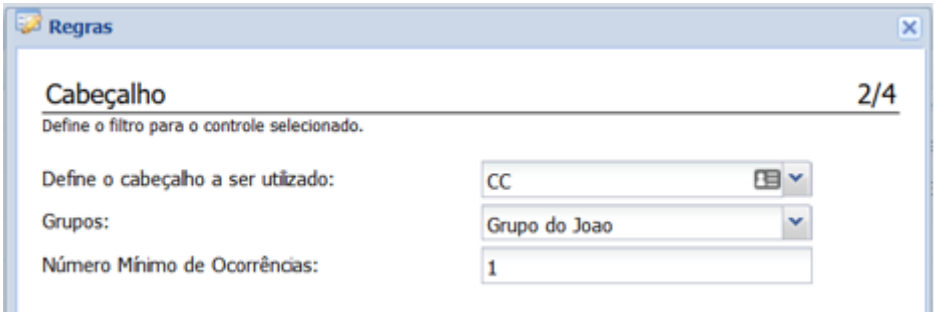
Bloqueio de E-mails pelo módulo E-mail Compliance

É possível utilizar o módulo de DLP no E-mail Complicane, para que seja efetuado o bloqueio direto do e-mail (independete da pontuação). Vamos citar como exemplo bloqueio de e-mails que tenham com cópia para um e-mail já previamento cadastrado em Cadastro>Grupos Usuários (com o Grupo chamado **Grupo do Joao**)

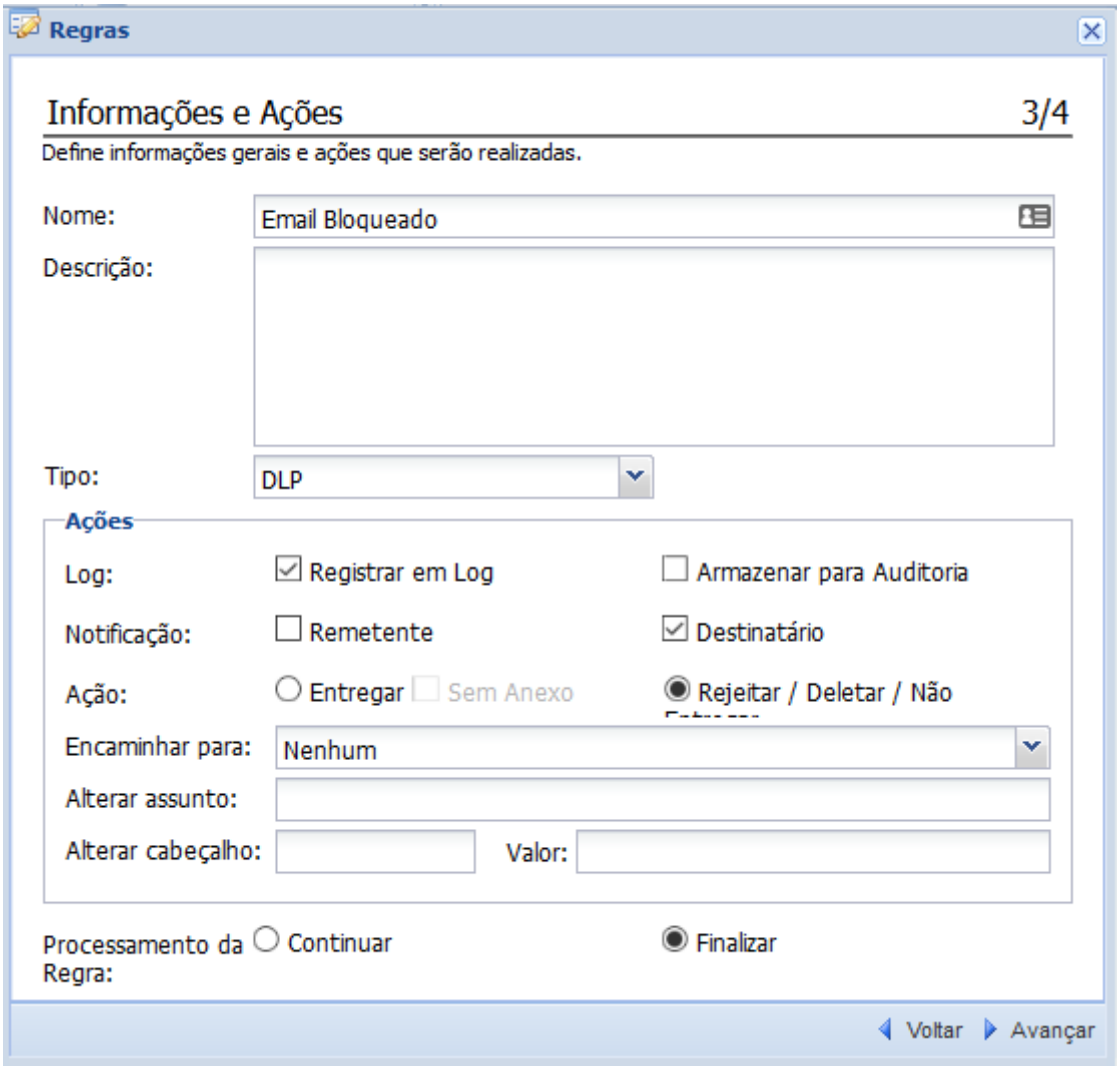
Em Configurações > E-mail Compliance > Regras, selecione Cabeçalho:

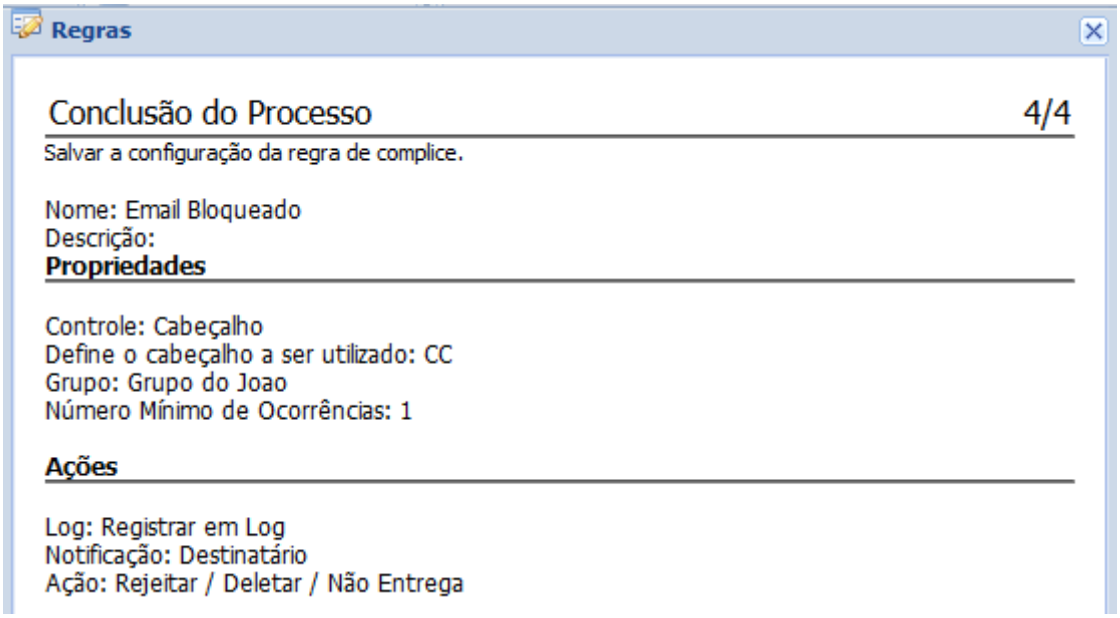


Considerando caso o e-mail seja em Cópia para alguém do Grupo do Joao, então no campo da definição de cabeçalho a ser usado será CC (com cópia) para o Grupo do Joao, com mínimo de 1 ocorrência, ou seja, se o e-mail for para cópia de um dos integrantes cadastrados como parte do Grupo do Joao, já acionará a regra de Compliance.



Nas ações, defina-se o nome da regra e o Tipo como DLP, ao qual vamos bloquear o e-mail colocando-o em quarentena e além do bloqueio, vamos registar isso nos logs e ainda mandar uma notificação ao destinatário do e-mail, avisando que o e-mail foi bloqueado.



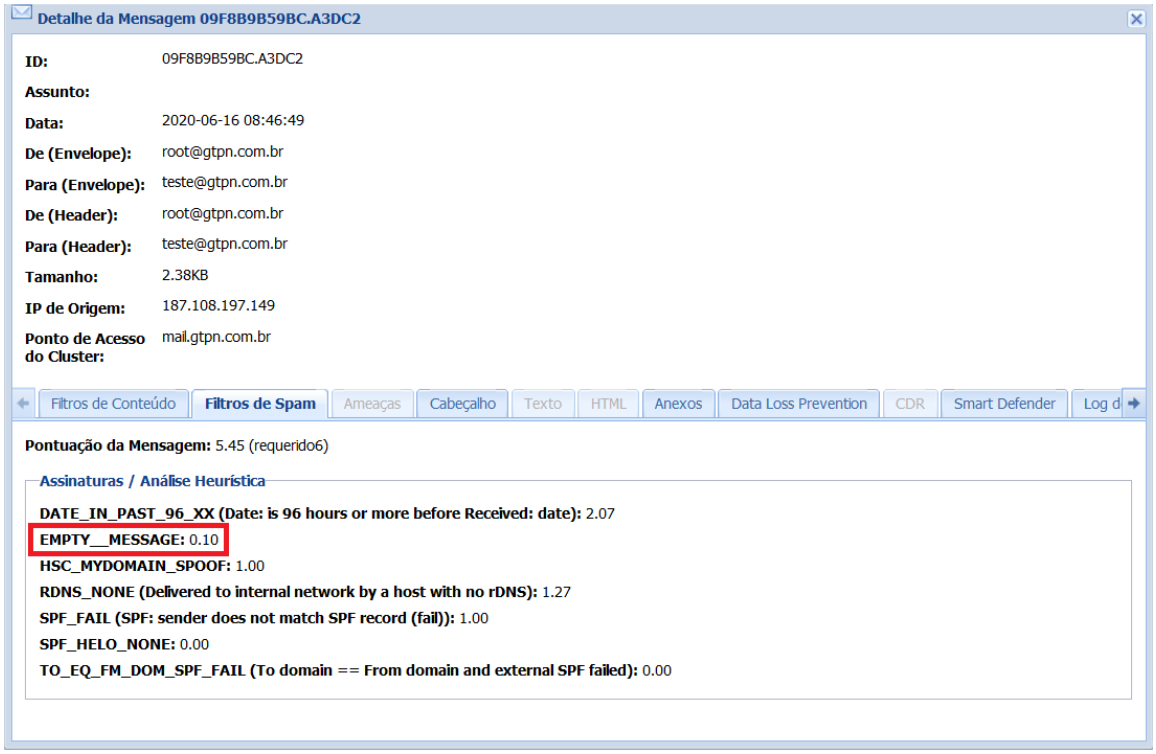


Agora é só Salvar e Aplicar as Configurações, dessa forma a regra criada já passrá a entrar em vigor.

Bloqueio de E-mails Vazios

O MailInspector possui uma assinatura específica para detecção sobre e-mails sem conteúdo e/ou assunto vazio.

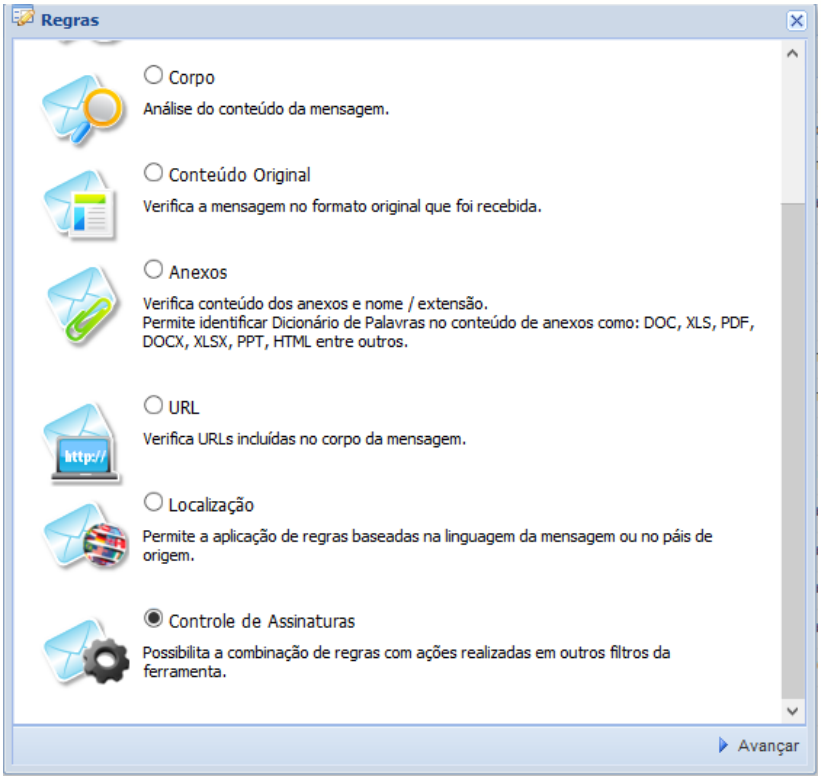
Primeiramente segue abaixo a tela indicando a assinatura que detecta e-mails sem conteúdo:

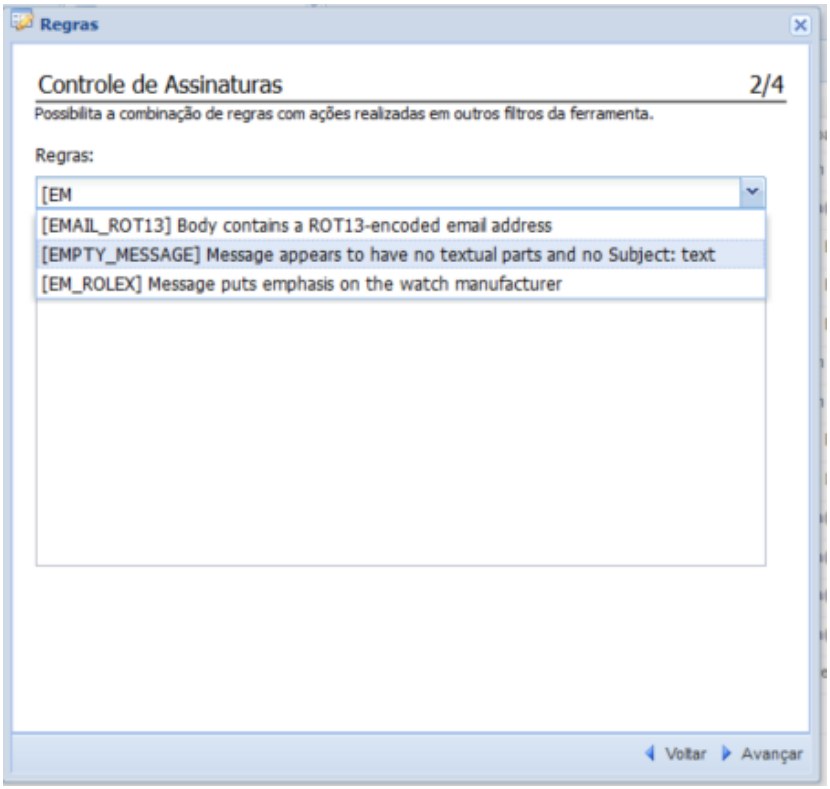


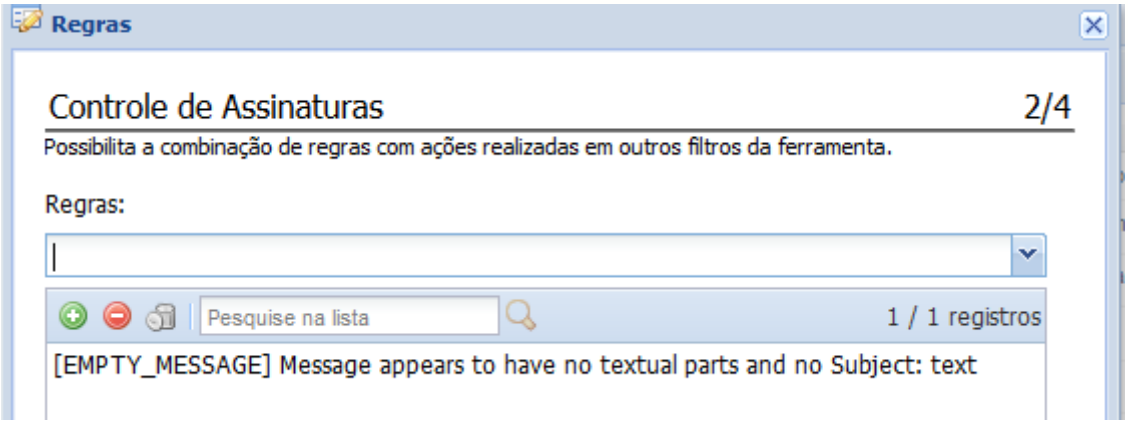
Para criarmos uma regra de bloqueio, temos que fazê-la no E-mail Compliance. Vá em:

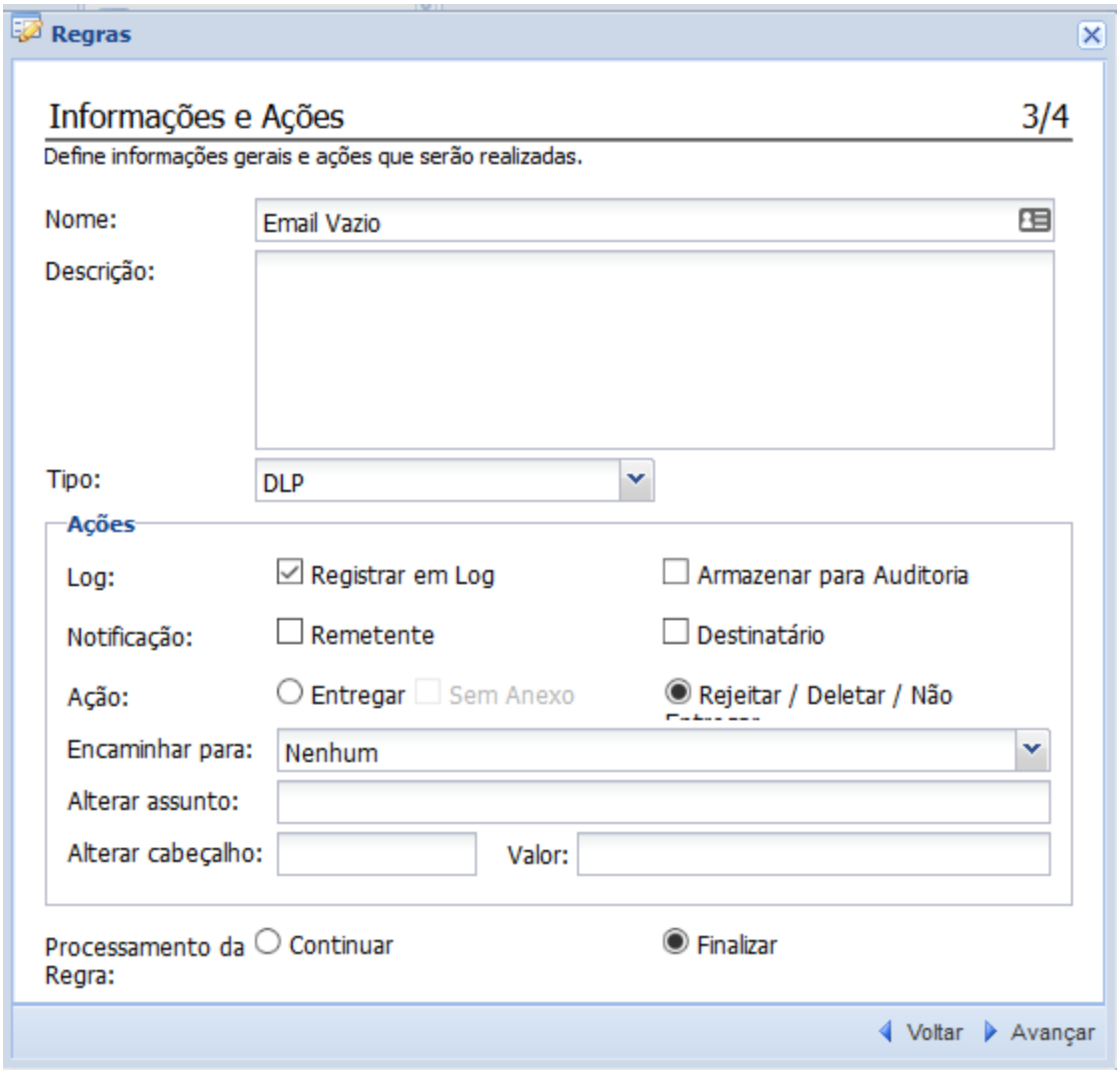
Configurações > E-mail Compliance > Regras

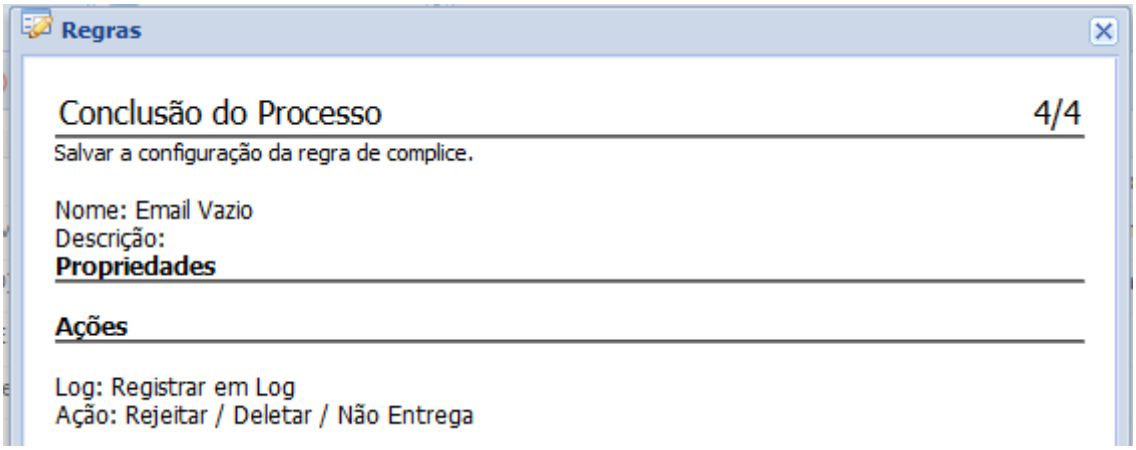
Adicione uma nova regra, conforme tela a seguir:


Regras
Corpo
Análise do conteúdo da mensagem.
Conteúdo Original
Verifica a mensagem no formato original que foi recebida.
Anexos
Verifica conteúdo dos anexos e nome / extensão.
Permite identificar Dicionário de Palavras no conteúdo de anexos como: DOC, XLS, PDF, DOCX, XLSX, PPT, HTML entre outros.
URL
Verifica URLs incluídas no corpo da mensagem.
Localização
Permite a aplicação de regras baseadas na linguagem da mensagem ou no páis de origem.
Controle de Assinaturas
Possibilita a combinação de regras com ações realizadas em outros filtros da ferramenta.
Avançar


Regras
Controle de Assinaturas
2/4
Possibilita a combinação de regras com ações realizadas em outros filtros da ferramenta.
Regras:
[EM
[EMAIL_ROT13] Body contains a ROT13-encoded email address
[EMPTY_MESSAGE] Message appears to have no textual parts and no Subject: text
[EM_ROLEX] Message puts emphasis on the watch manufacturer
Voltar
Avançar


Regras
Controle de Assinaturas
2/4
Possibilita a combinação de regras com ações realizadas em outros filtros da ferramenta.
Regras:
Pesquise na lista
1 / 1 registros
[EMPTY_MESSAGE] Message appears to have no textual parts and no Subject: text


Regras
Informações e Ações
3/4
Define informações gerais e ações que serão realizadas.
Nome:
Email Vazio
Descrição:
Tipo:
DLP
Ações
Log:
Registrar em Log
Armazenar para Auditoria
Notificação:
Remetente
Destinatário
Ação:
Entregar
Sem Anexo
Rejeitar / Deletar / Não
Encaminhar para:
Nenhum
Alterar assunto:
Alterar cabeçalho:
Valor:
Processamento da Regra:
Continuar
Finalizar
Voltar
Avançar



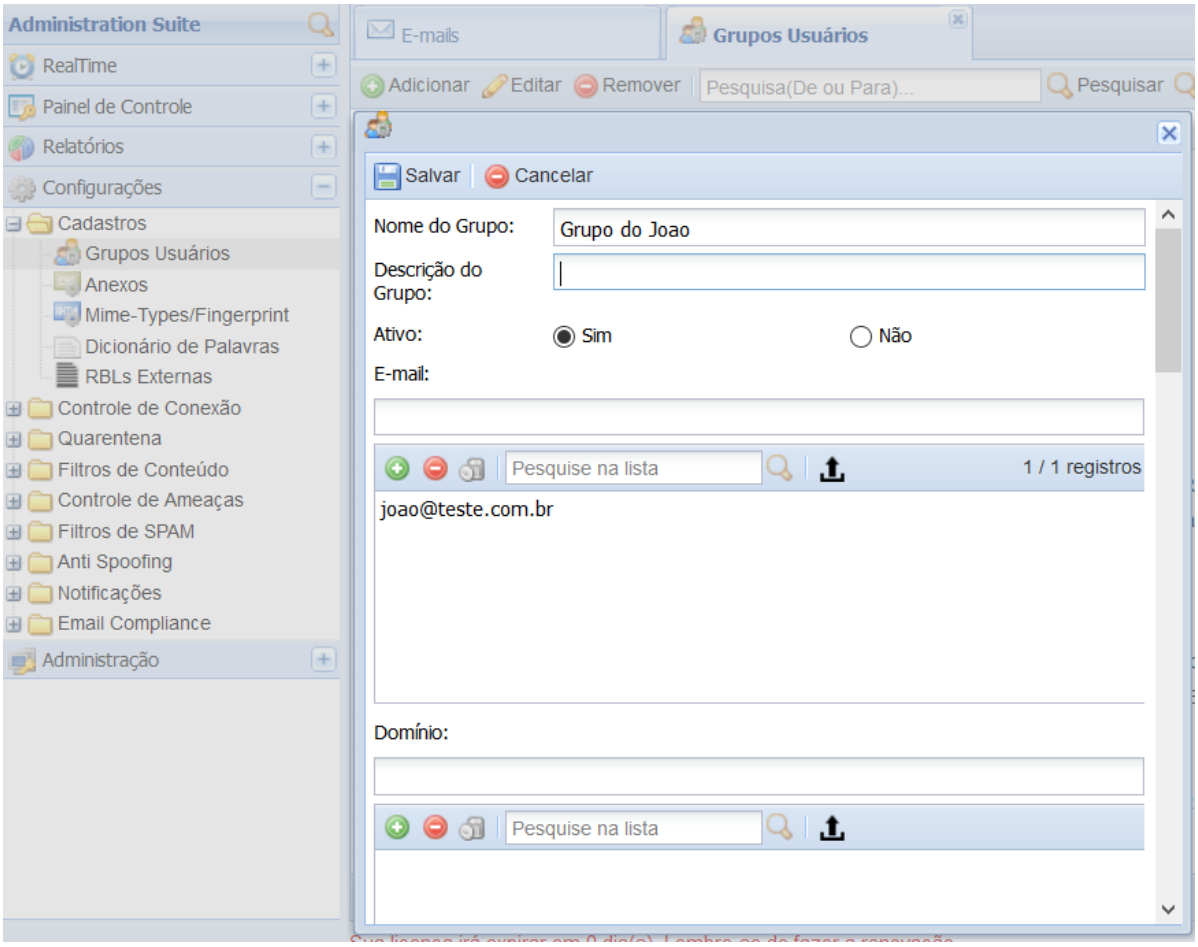
Agora é só Salvar a regra e clicar em Aplicar Configurações

Colocar e-mail em uma quarentena específica

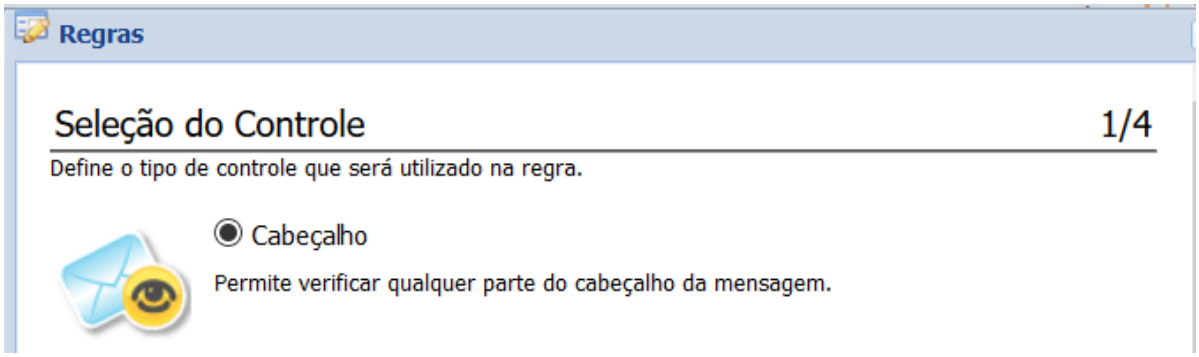
Em E-mail Compliance, é possível criar qualquer tipo de regra. Primeiramente cadastra-se o grupo de e-mails ao qual as regras farão atuação. Vamos citar como exemplo TODOS os e-mails com destino ao **joao@teste.com.br**, serão colocados em uma quarentena chamada Quarentena do Joao.

Para isso vá em Cadastros > Grupos de Usuários e adicione um novo grupo de usuário, onde o e-mail será **joao@teste.com.br**

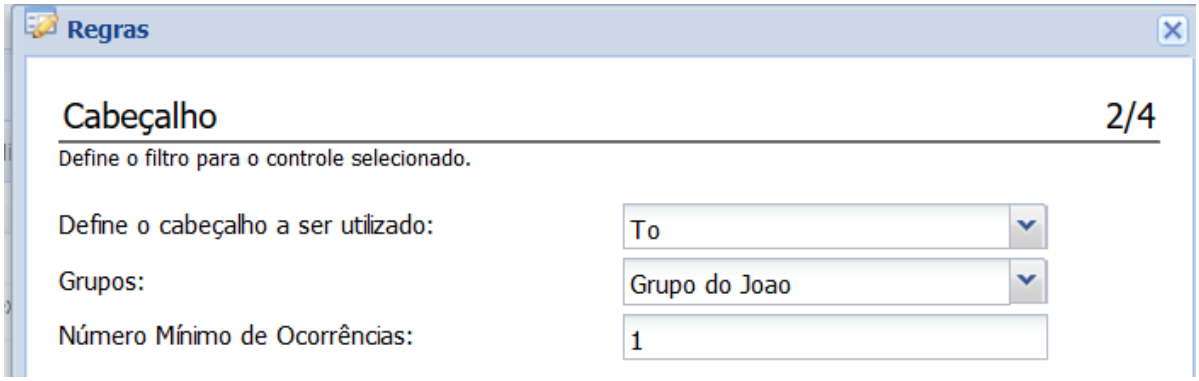
Chamarei o nome deste grupo de **Grupo do Joao**



Agora vamos para Configurações > E-mail Complicane > Regras, para adicionar nova regra

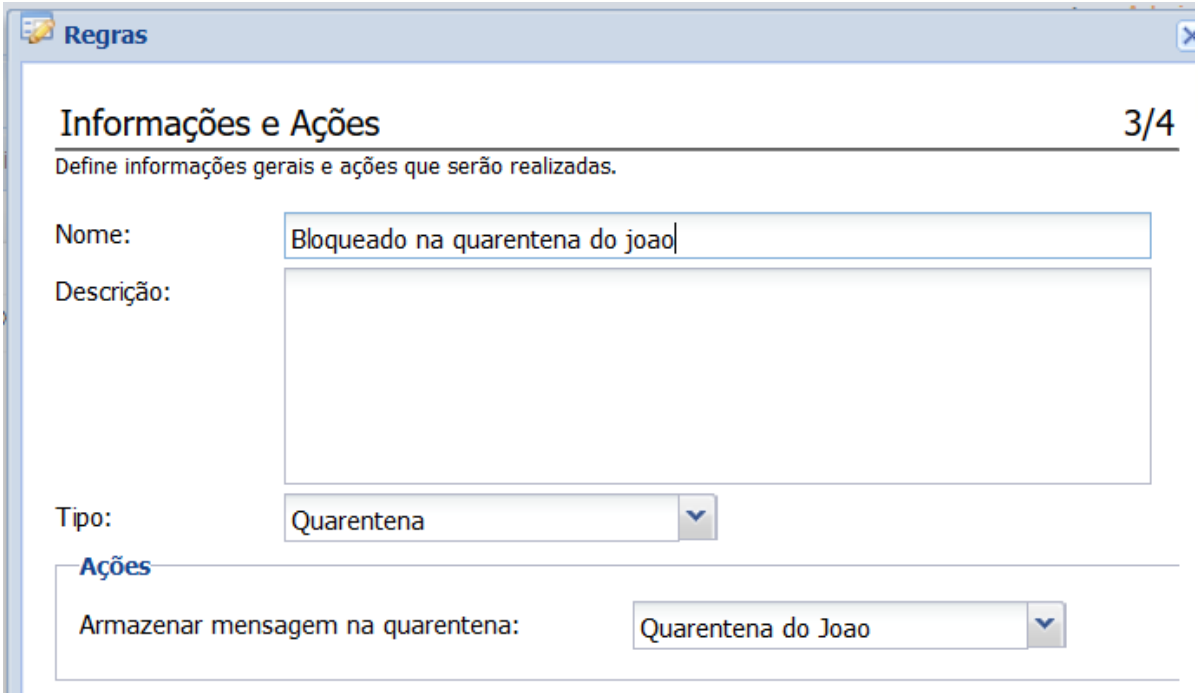


Sendo o cabeçalho utilizado será o TO (a ideia da regra é se for para o joao@teste.com.br). No Grupo agora deve-se marcar o Grupo do Joao (anteriormente criado) e mínimo de 1 ocorrência.

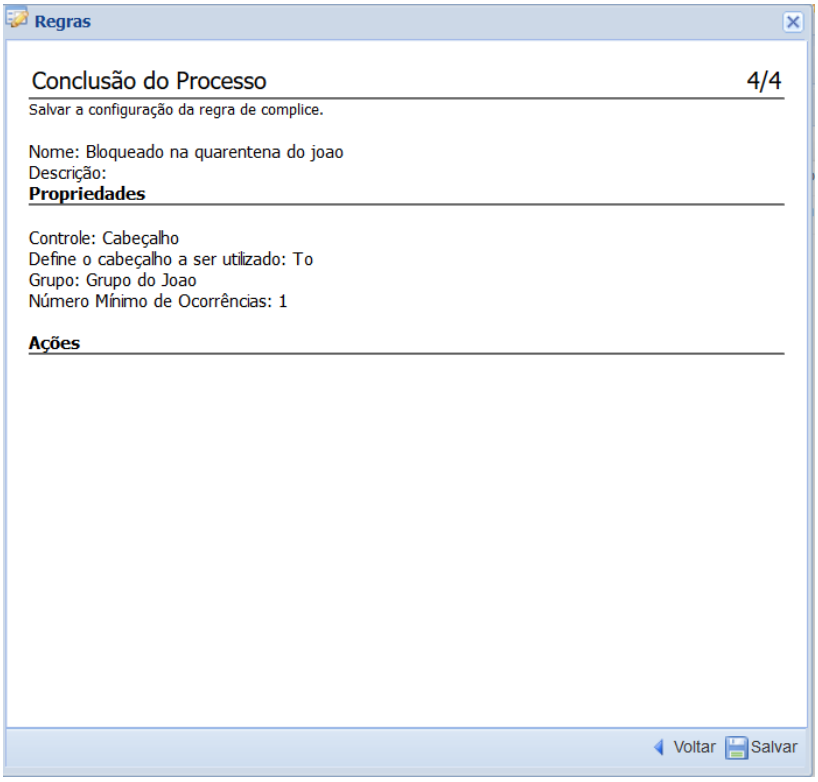


Por último a ação a ser tomada é Quarentena do e-mail na “Quarentena no Joao”

Obs: A quarentena chamada “Quarentena do Joao” tem que já ter sido criada antecipadamente. Para isso veja criação em *Customizada*



É apresentado o resumo da regra, aí é só clicar em Salvar e Aplicar Configurações.



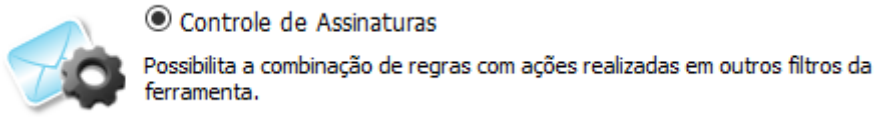
Modificando a pontuação de e-mail devido a reputação de origem do IP

O MailInspector permite que o administrador mude a pontuação de um e-mail baseado na reputação do mesmo.

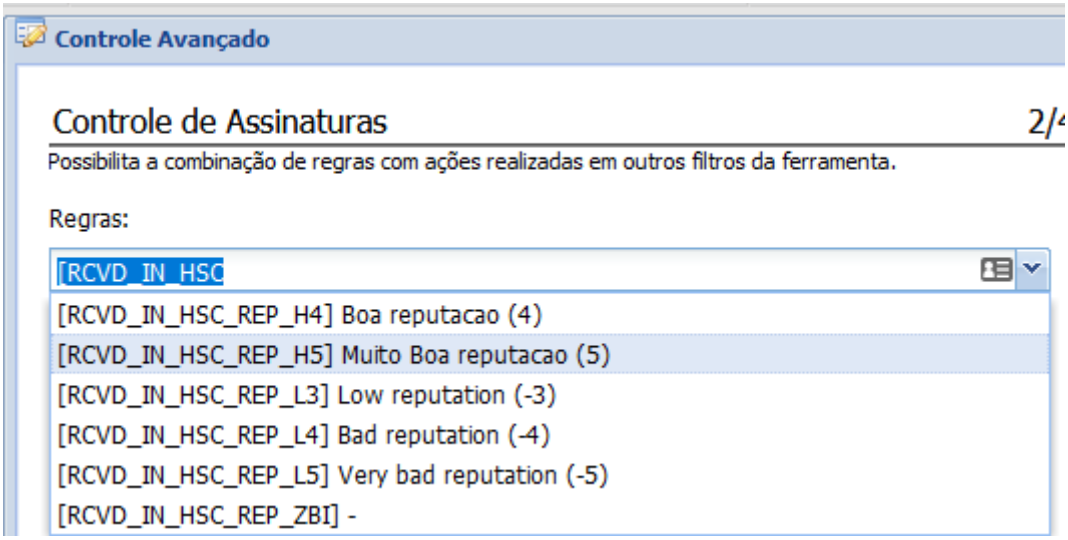
Para esse processo, vá em Configurações > Filtros de SPAM > Controle Avançado

Clique em Adicionar

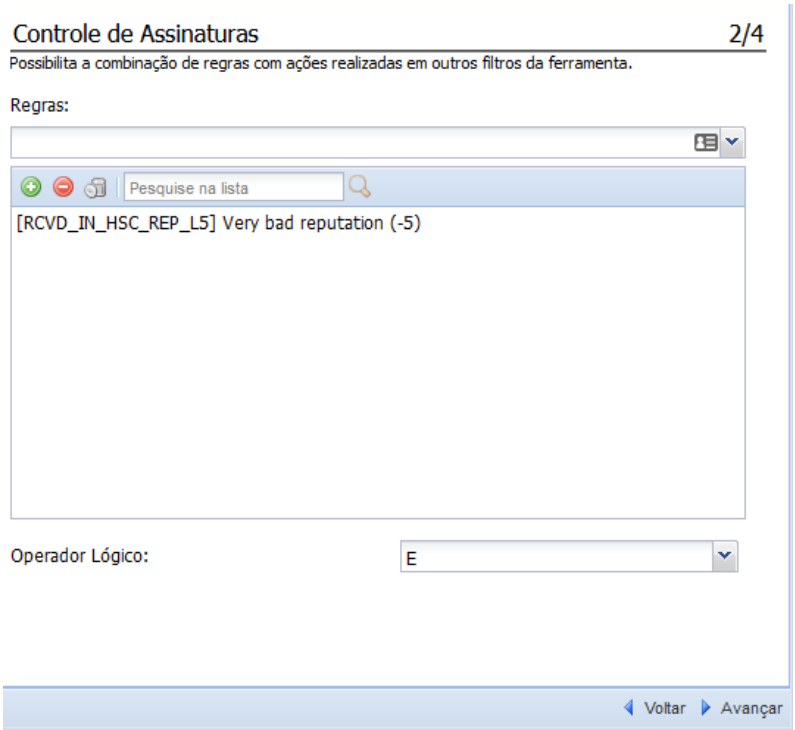
Selecione a opção Controle de Assinaturas



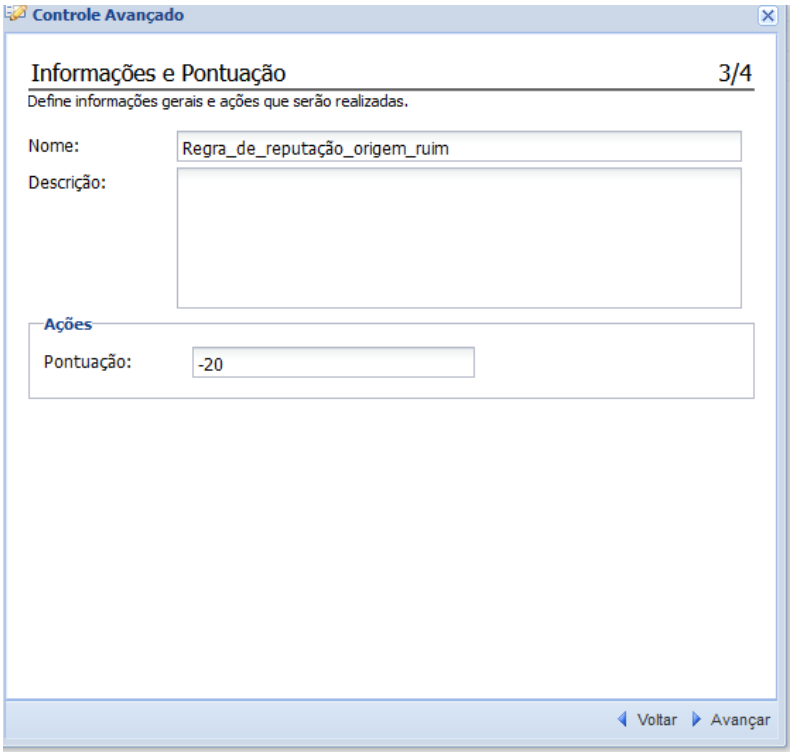
Selecione a assinatura de reputação, conforme as reputações indicadas abaixo.



Para a título de exemplo selecionaremos a reputação [RCVD_IN_HSC_REP_L5]

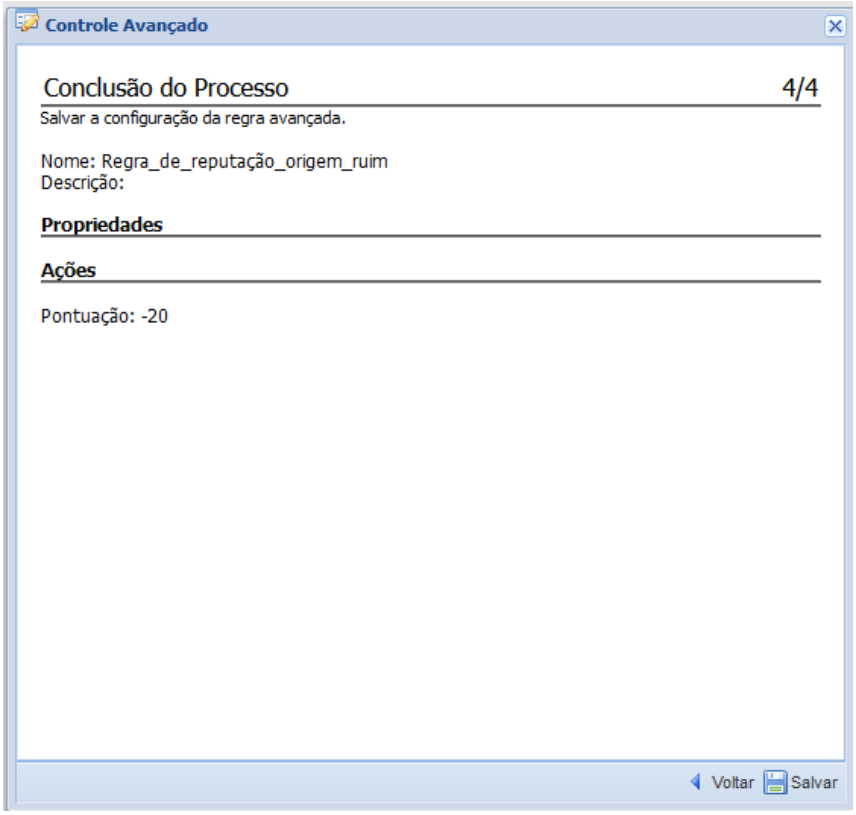


Clique em avançar e preencha os campos de acordo com a sua necessidade (lembrando que quanto MAIOR a pontuação, maior a ameaça do e-mail, isto é, ele será "mais" considerado SPAM). No exemplo, ao colocar a pontuação -20, o e-mail não será considerado SPAM, pois ficará com pontuação negativa (o sistema considerará que será reduzido de vinte pontos o cálculo total de SPAM).



Clique em avançar

Clique em Salvar e depois em Aplicar Configurações



120	Regra_de_reputação_origem_ruim	SA_RULES	Pontuação: -20

É possível efetuar regras similares usando como base outros parâmetros de pontuação, tais como:

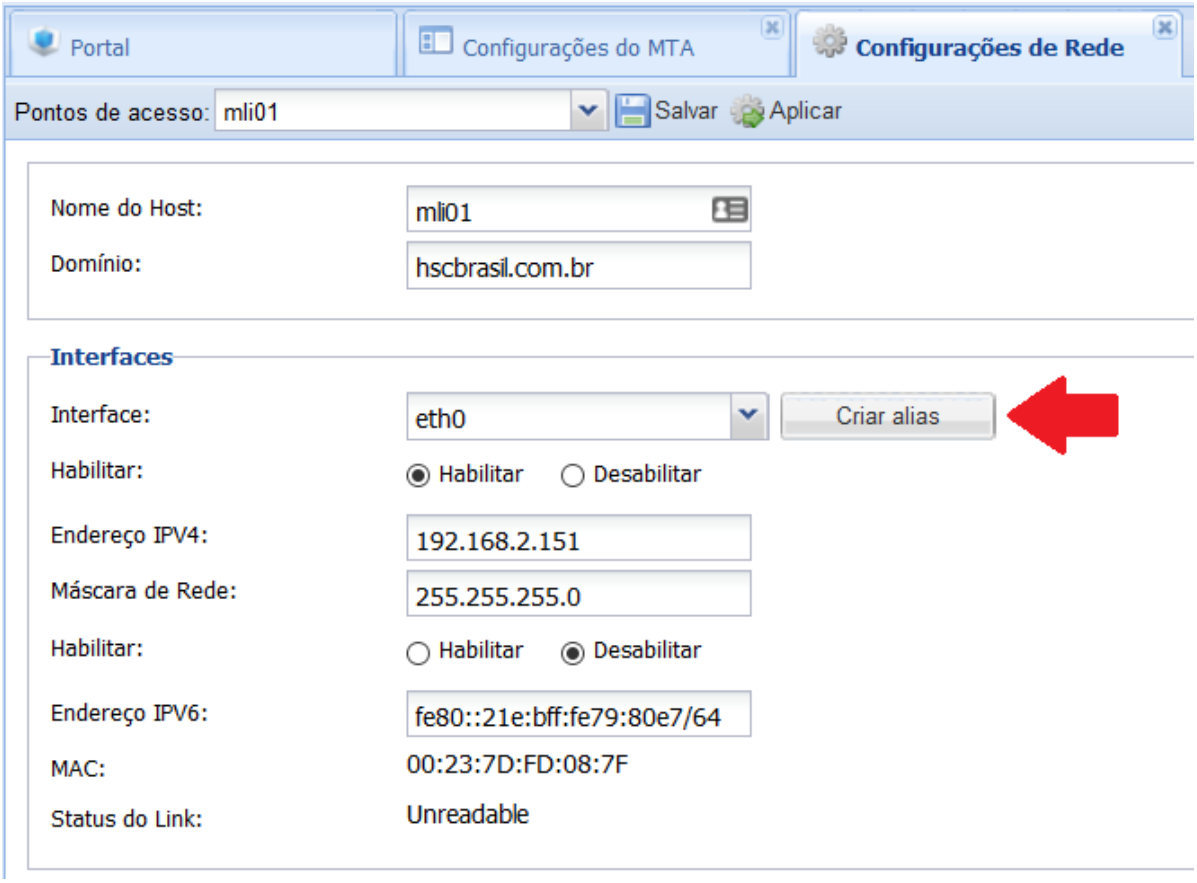
- Assinaturas de vírus;
- Assinaturas de SPAM;
- Análise Bayesiana;
- Reputação de URL's;
- Entre outros pontos;

Saída de e-mail por IP específico

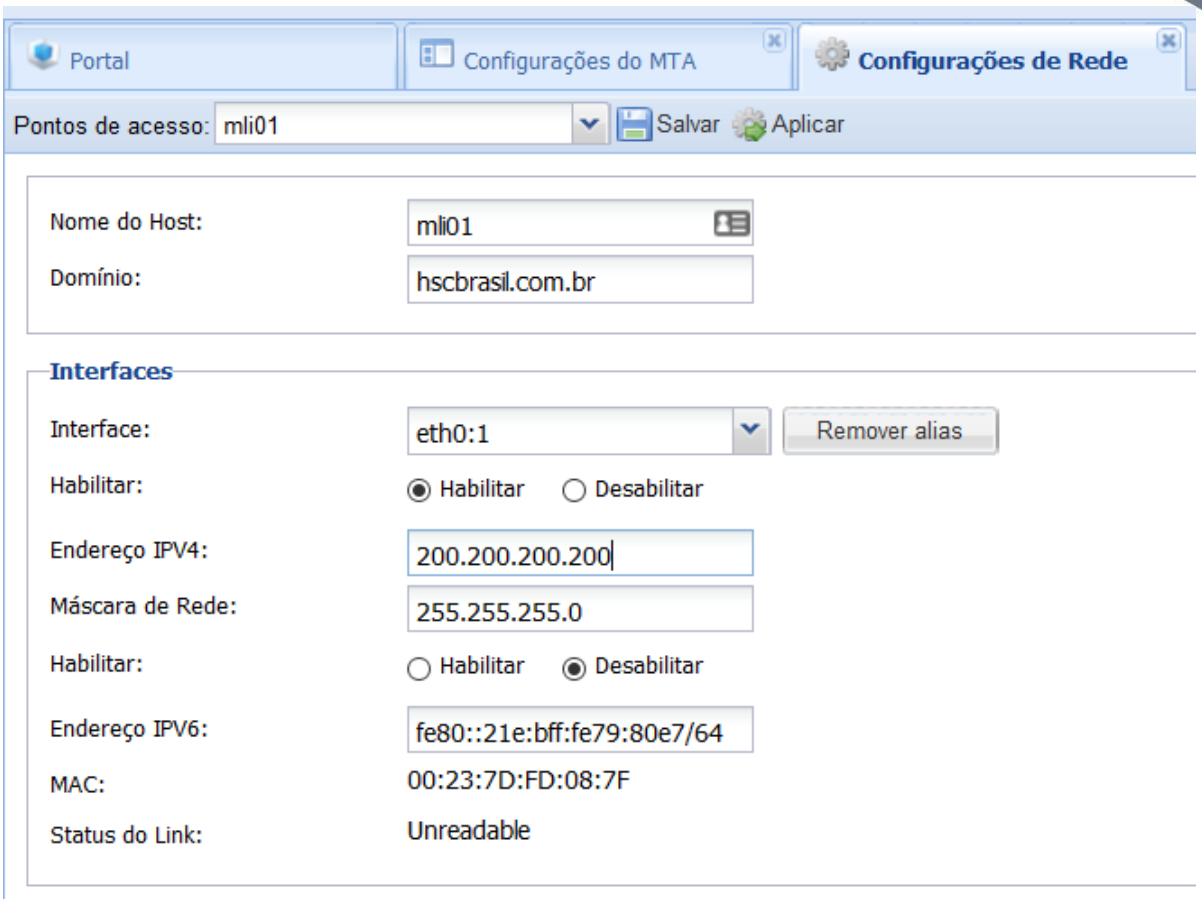
No MailInspector é possível configurar a saída de e-mails por um IP específico.

Por exemplo no domínio hscbrasil.com.br tem o subdomínio marketing.hscbrasil.com.br e este subdomínio envia várias campanhas de mail marketing. Para evitar que o IP caia em blacklist (RBL's), vamos efetuar a saída dos e-mails de marketing.hscbrasil.com.br no IP 200.200.200.200

1. Vá em Adminstração > Configurações de Rede
2. Configure um Alias na placa de rede desejada. Para isso, clique no botão Criar Alias.



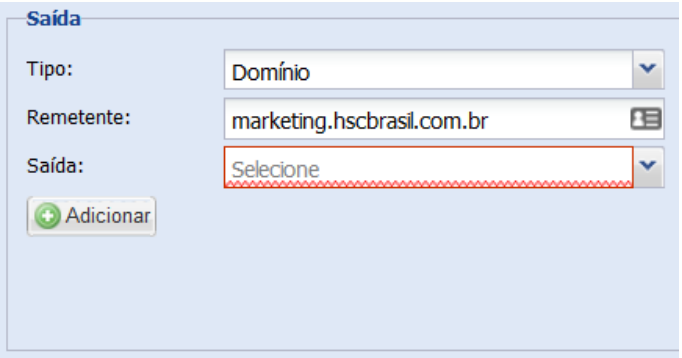
3. Configure o IP no novo alias criado: ETH0:1



Se houver mais de um ponto de acesso, formando um cluster, é necessário fazer este procedimento para TODOS os pontos que compõem o Cluster.

4. Clique em Salvar a depois em Aplicar
5. Vá em Configurações > Configurações do MTA
   Selecione a aba Rotas
6. Na parte Saída
   No campo Tipo selecione a opção Domínio
   No campo remetente insira o remetente a ser filtrado na saída. No nosso exemplo é marketing.hscbrasil.com.br

No campo saída indique a interface, que no caso é eth0:1

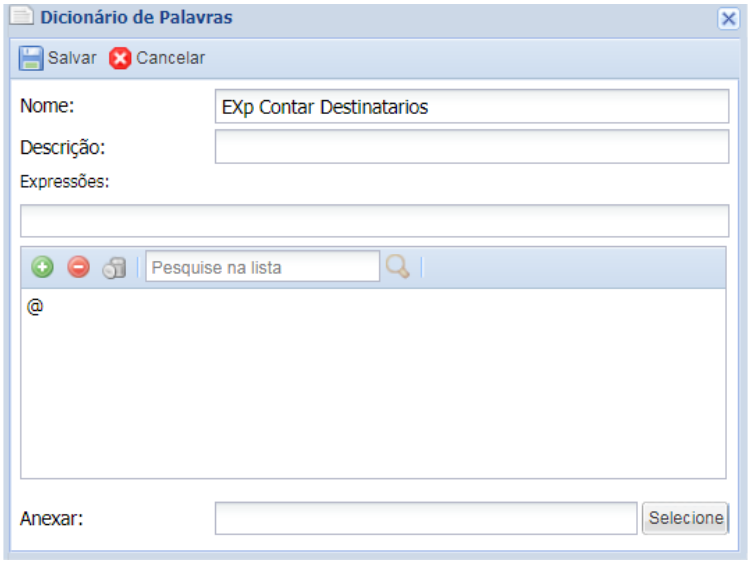


7. Clique no botão Salvar e Aplicar Configurações

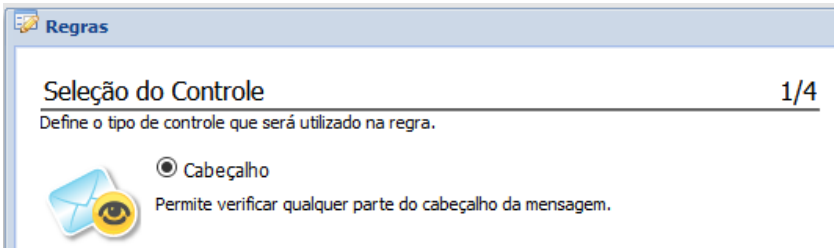
Criando contador de número de destinatários de um e-mail

No MailInspector é possível criar um contador para ser utilizado em conjuntunto com regras, isto é, por exemplo queremos bloquear e-mails que contenham mais de 15 destinatários.

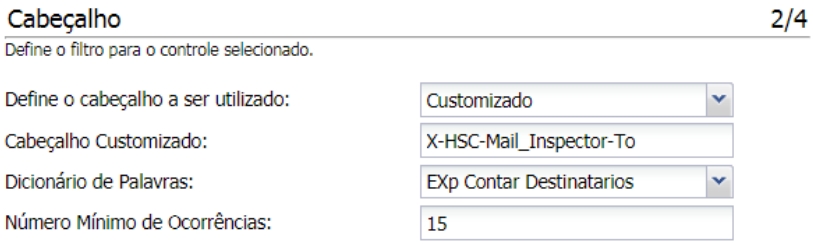
1. Crie o objeto no dicionario de palavras (Contador).
   Vá em Configurações > Cadastros > Dicionário de Palavras
2. Clique no botão Adicionar
3. Crie o objeto, conforme a imagem abaixo



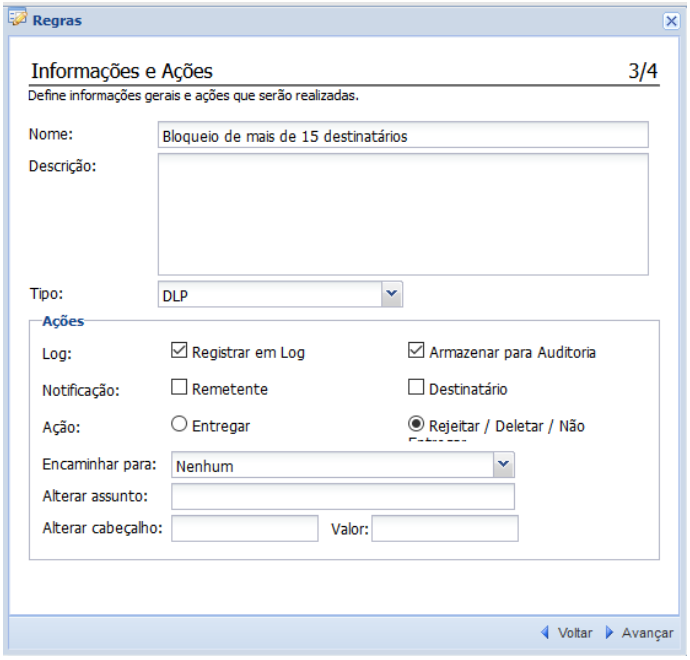
4. Clique em Salvar
5. Agora vá em Configurações > E-mail Compliance > Regras
6. Clique no botão Adicionar
7. Selecione a opção Cabeçalho



8. Clique em Avançar
9. Preencha os campos conforme imagem a seguir



10. Indique a ação a ser tomada quando esta regra for acionada



11. Clique em Avançar
12. Em seguida, clique em Salvar
13. Não esqueça de clicar em Aplicar Configurações

Obs: Lembrando que sempre é possível “CASAR” múltiplas regras, por exemplo na regra anteriormente indicada, que é para 15 destinatários, é possível casar essa condição em e-mails oriundos de um determinado grupo, dessa forma a contagem de 15 destinatários somente afetaria esse grupo.

Redirecionamento de e-mails para outro servidor de e-mail (que não é o padrão de entrega para o mesmo domínio) em regra de DLP

Estes procedimentos tem o propósito de orientar de forma clara o processo de como fazer roteamento de e-mails que não seja para o(s) servidor(es) padrão(ões). Vamos citar por exemplo, que a sua empresa tem o IP 192.168.1.100 como o servidor principal de e-mail, onde tem os e-mails gerais da empresa, mas quando vem um determinado e-mail específico, você precisa mandar para outro servidor (192.168.1.101), por exemplo, servidor de e-mails marketing, que dispara vários e-mails e aguarda a resposta de uma campanha.

a. Crie os objetos referentes às condições para o redirecionamento.

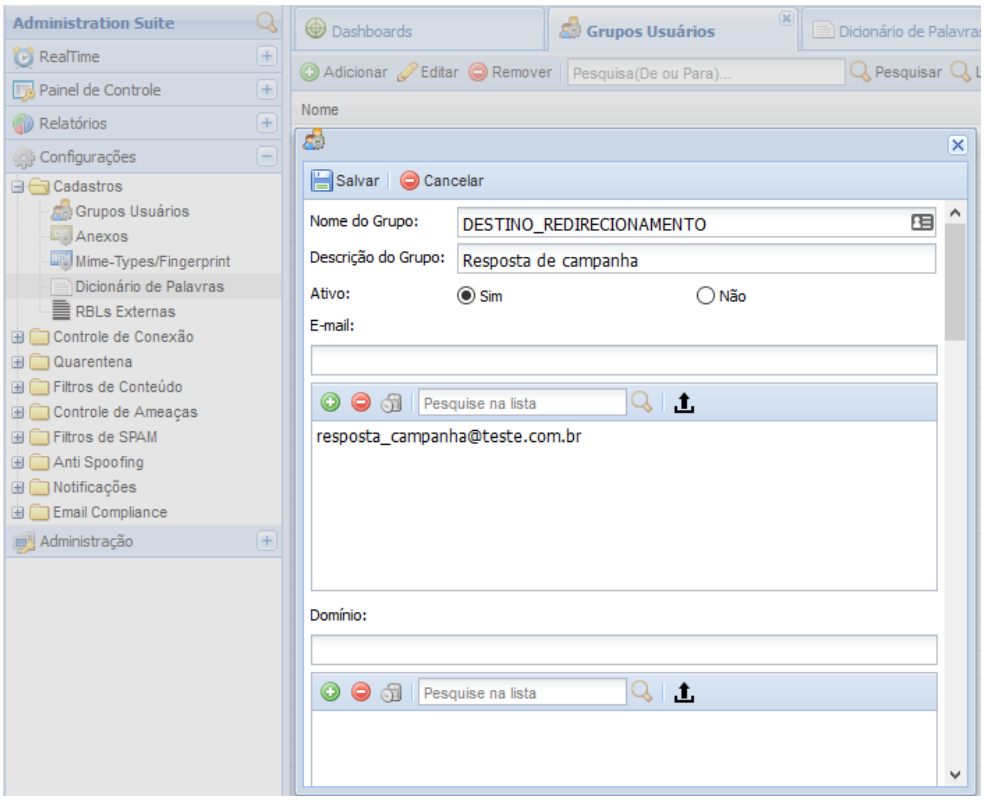
Por exemplo:

Quero redirecionar para outros servidor os e-mails que **forem para** (destino) resposta_campanha@teste.com.br e que no campo assunto tenha a palavra **[** RESPOSTA **]** no **inicio** do assunto do e-mail.

Crie os objetos necessários

b. Em Cadastros > Grupos Usuários

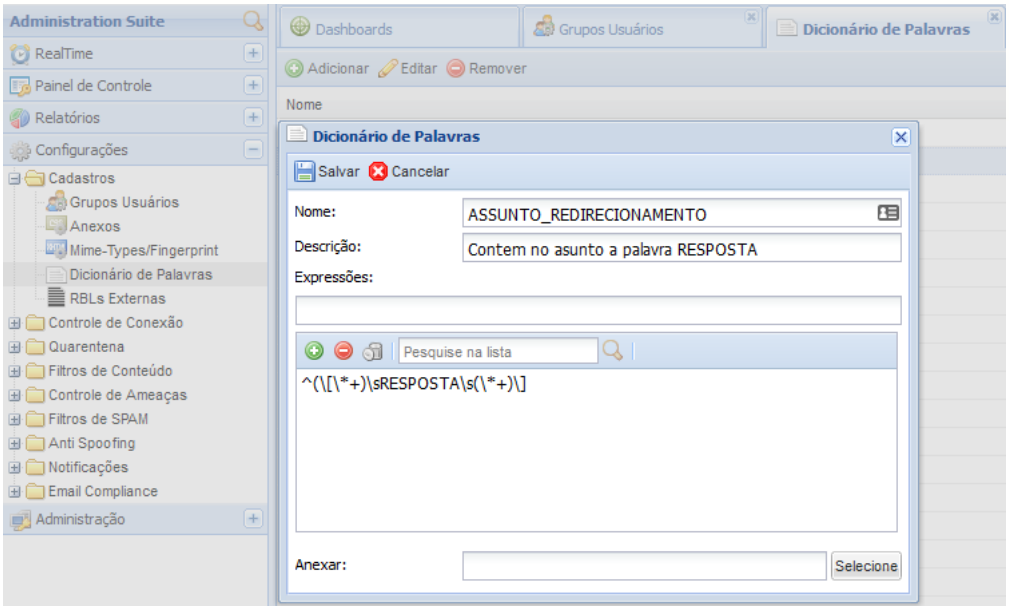
Adicione um novo grupo e inclua o e-mail resposta_campanha@teste.com.br. No exemplo vamos chamar o grupo de **DESTINO_REDIRECIONAMENTO**



c. Salve o grupo criado (Salvar);

d. Também de acordo com a condição citada, precisaremos de um objeto para o assunto [** RESPOSTA **].

Para isso, vamos em Cadastros > Dicionário de Palavras. Vamos criar um "dicionário" cuja expressão será a Expressão Regular para a string **[**RESPOSTA **]** em maiúsculo, no ínicio do campo assunto e colocaremos como nome da regra da expressão **ASSUNTO_REDIRECIONAMENTO**



Observe que a expressão regular para indicar o assunto no INÍCIO do campo assunto e a palavra RESPOSTA em maiúsculo. Tudo isso, entre colchetes e com dois asteriscos, conforme a string a seguir: [** RESPOSTA **]

Para poder attender a todas essas regras, da expressão do campo assunto, a expressão regular ficará:

^(\[*+)\sRESPOSTA\s(*+)\]

e. Salve o dicionário criado (Salvar);

f. Agora vamos criar a regra de DLP, que fará o redirecionamento para o outro servidor de e-mail. Vá em configurações > E-mail Compliance > Regras

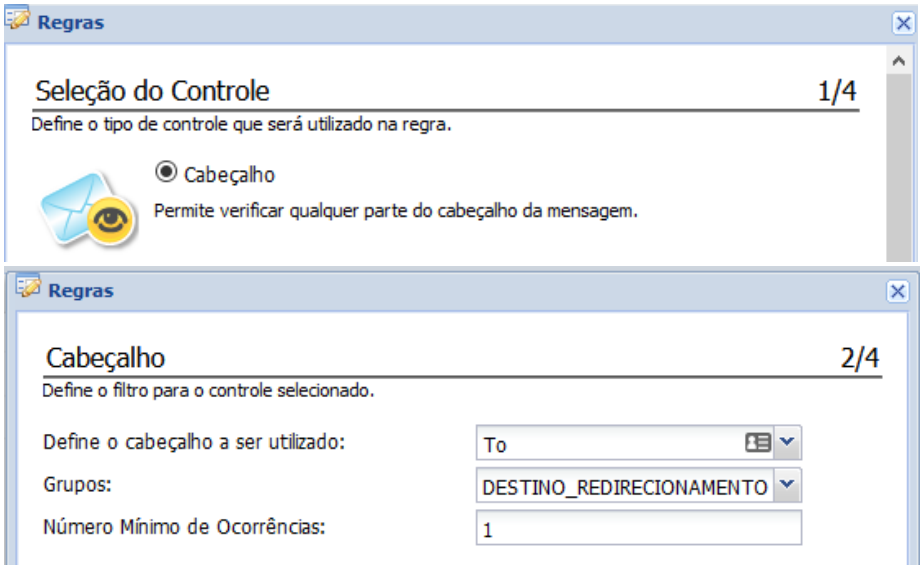
g. Adicione uma nova regra com as seguintes características:

   a. Cabeçalho

      Define o Cabeçalho a ser Utilizado: To

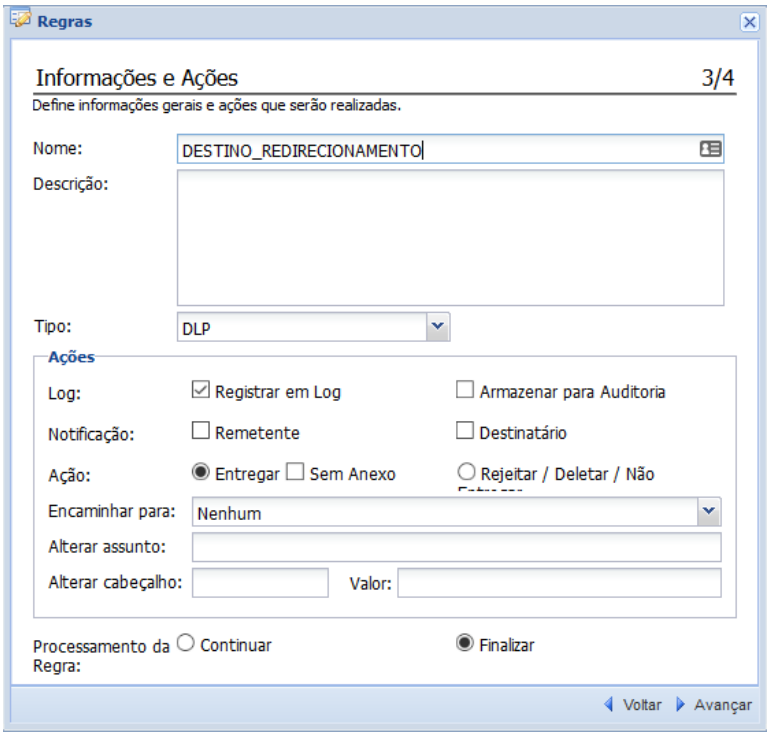
      Grupos: DESTINO_REDIRECIONAMENTO

      Número de Ocorrências: 1



Nome: DESTINO_REDIRECIONAMENTO

Nos outros campos, pode deixar inalterado.



b. Salve a primeira regra criada;

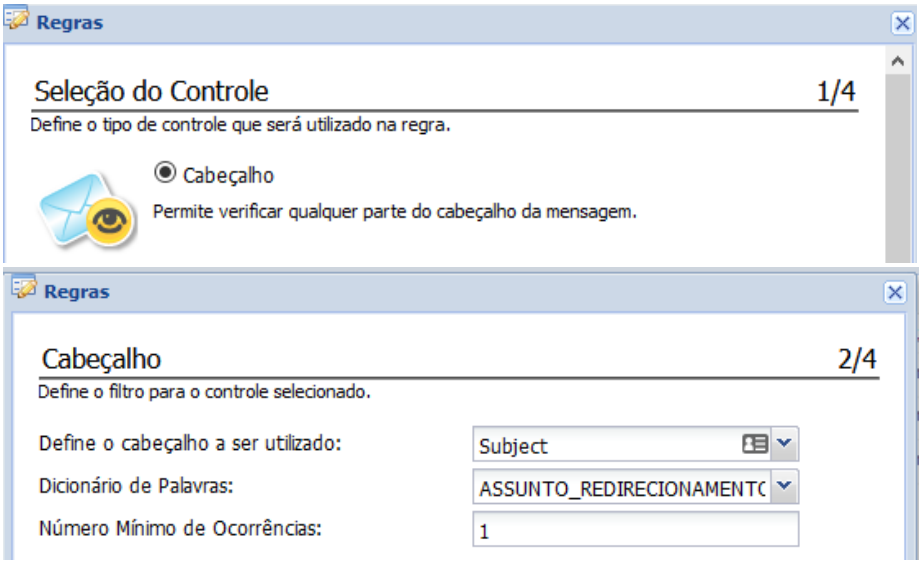
h. Novamente adicione uma nova regra com as seguintes características:

a. Cabeçalho

Define o Cabeçalho a ser Utilizado: Subject

Dicionário de Palavras: ASSUNTO_REDIRECIONAMENTO

Número de Ocorrências: 1

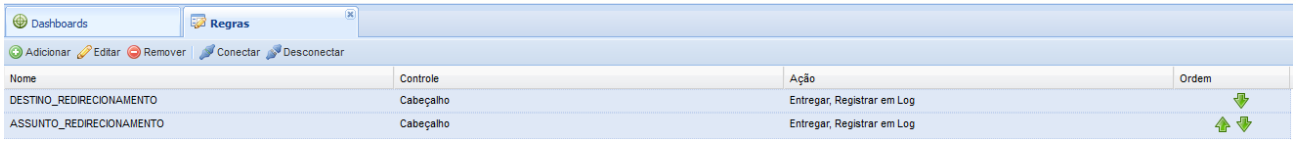


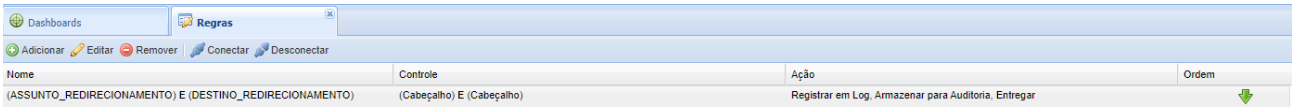
Nome: ASSUNTO_REDIRECIONAMENTO

Nos outros campos, pode deixar inalterado.

b. Salve a segunda regra criada;

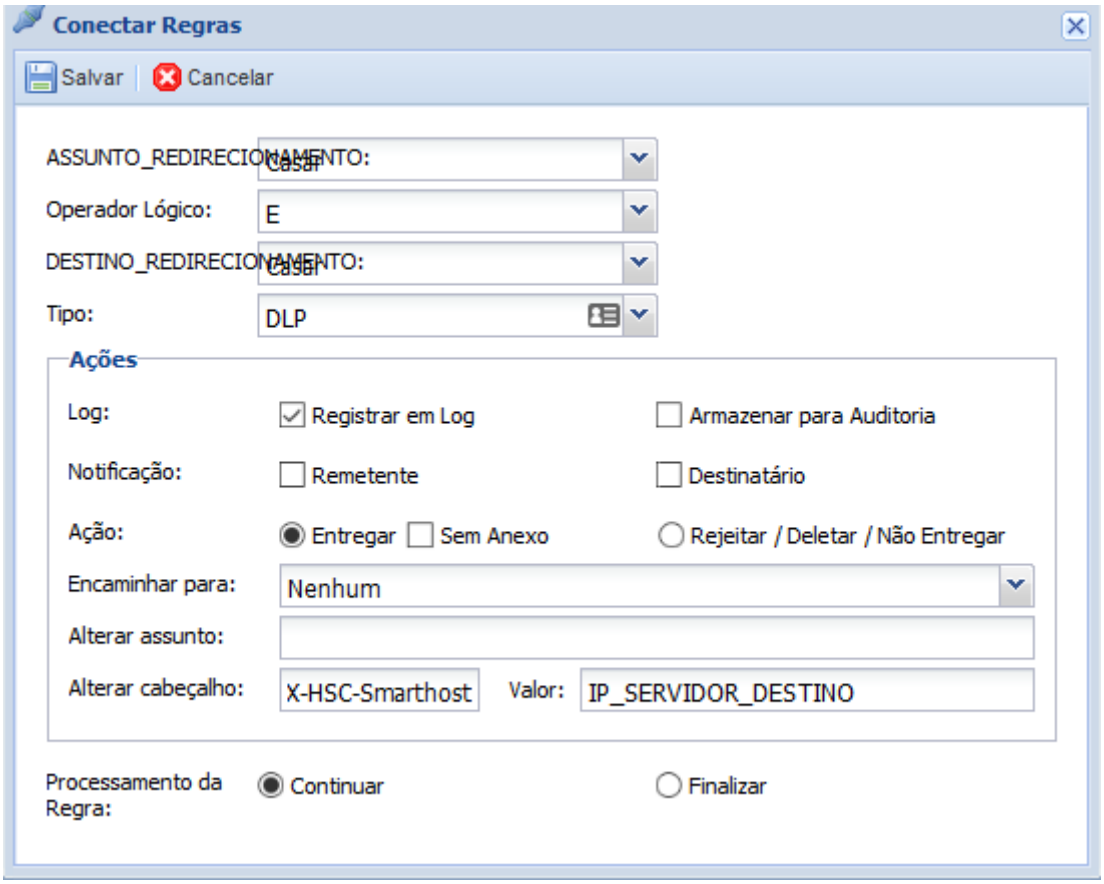
c. Selecione as duas regras criadas e clique em Conectar





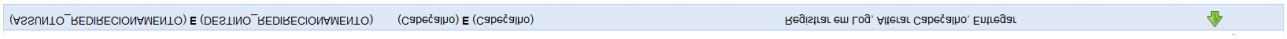
No campo Alterar cabeçalho coloque a variável **X-HSC-Smarthost**

Essa variável indica para o módulo DLP que ele deve ativar o redirecionamento de e-mail para o IP designado no campo **Valor**.



Onde o IP_SERVIDOR_DESTINO no nosso exemplo será 192.168.1.101

d. Clique em Salvar

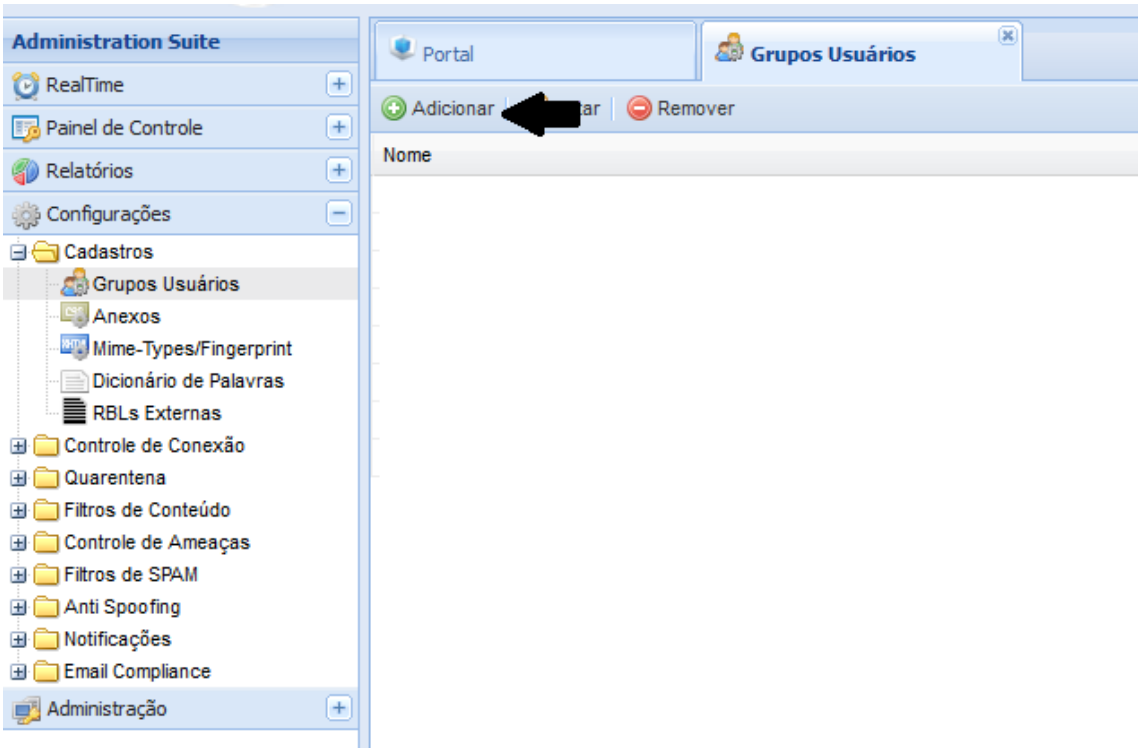


e. Clique em Aplicar Configurações

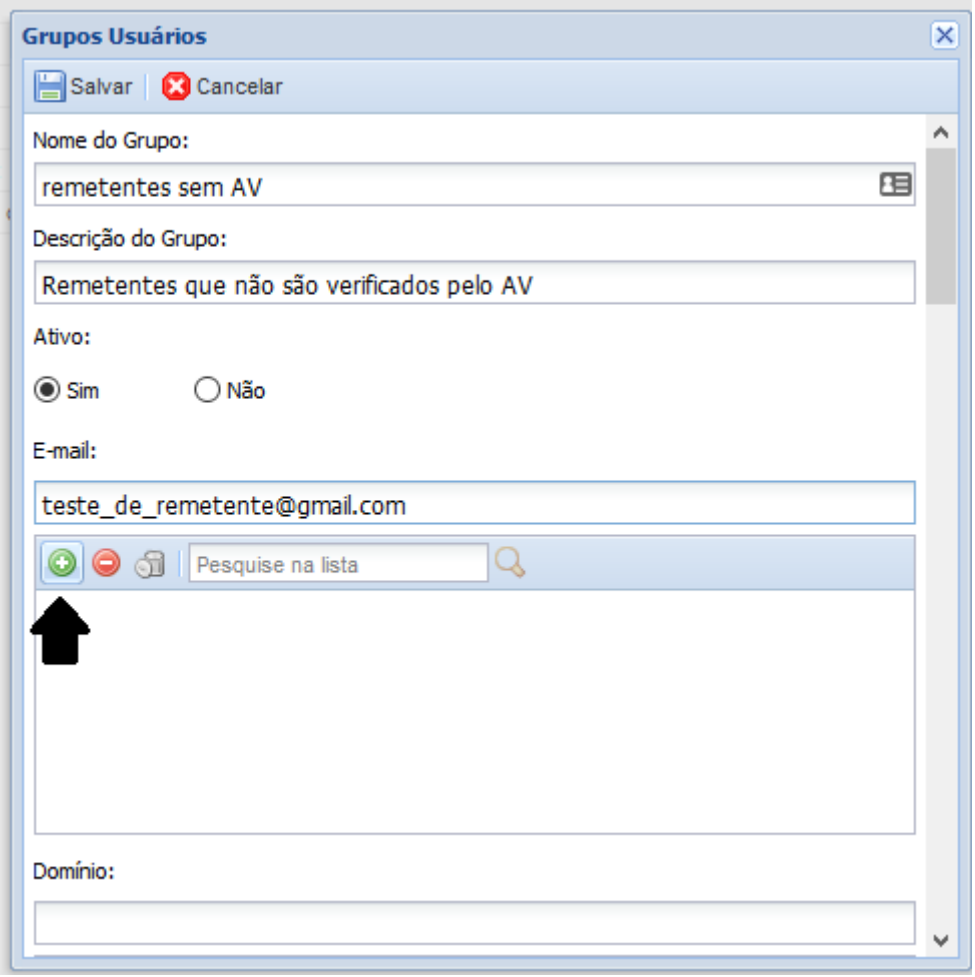
Exceção para Arquivos Compactados com Senha

Estes procedimentos tem o propósito de orientar de forma clara o processo de criar uma exceção (por e-mail do remetente), para arquivos compactados com senha não serem verificados pelo antivírus e eventualmente bloqueados.

a. No MLI, vá em:
   Configurações > Cadastro > Grupo de Usuários
b. Clique em Adicionar

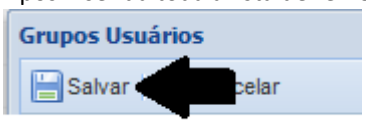


c. Insira no nome do Grupo, descrição e os e-mails dos remetentes que não serão verificados pelo módulo de anti-vírus.



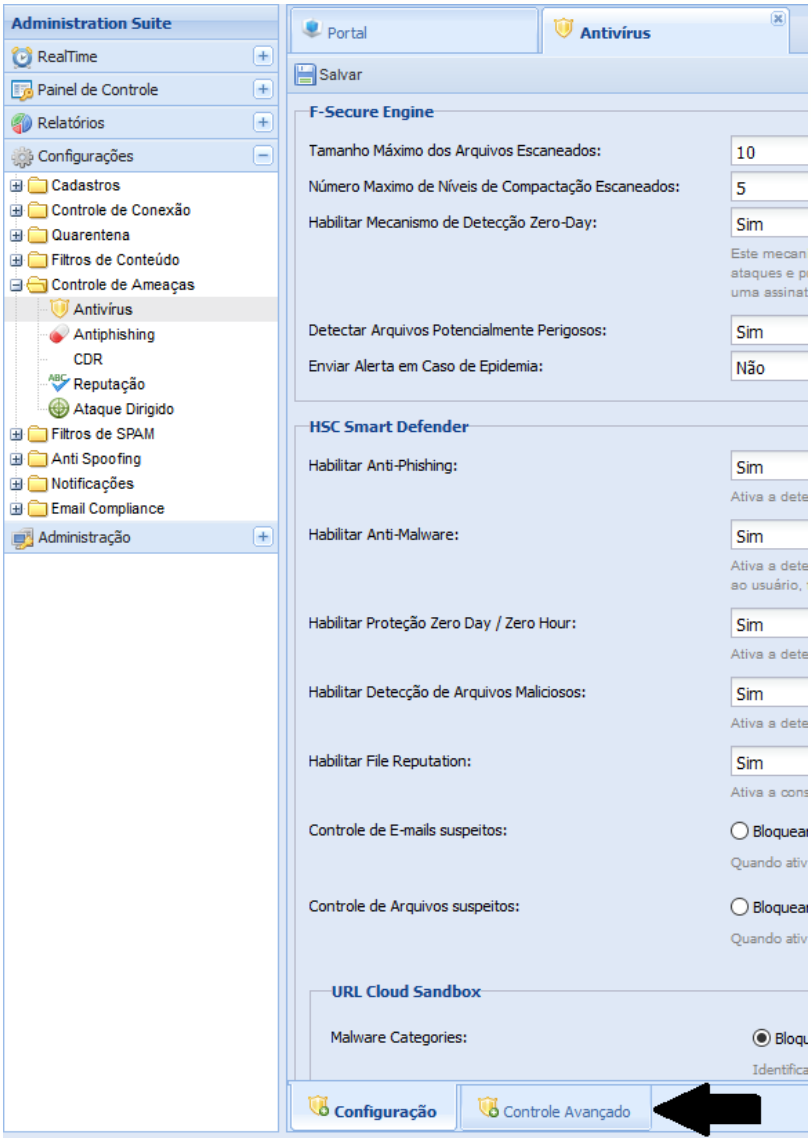
Obs: Não esqueça de clicar em (+) para incluir o e-mail na lista.

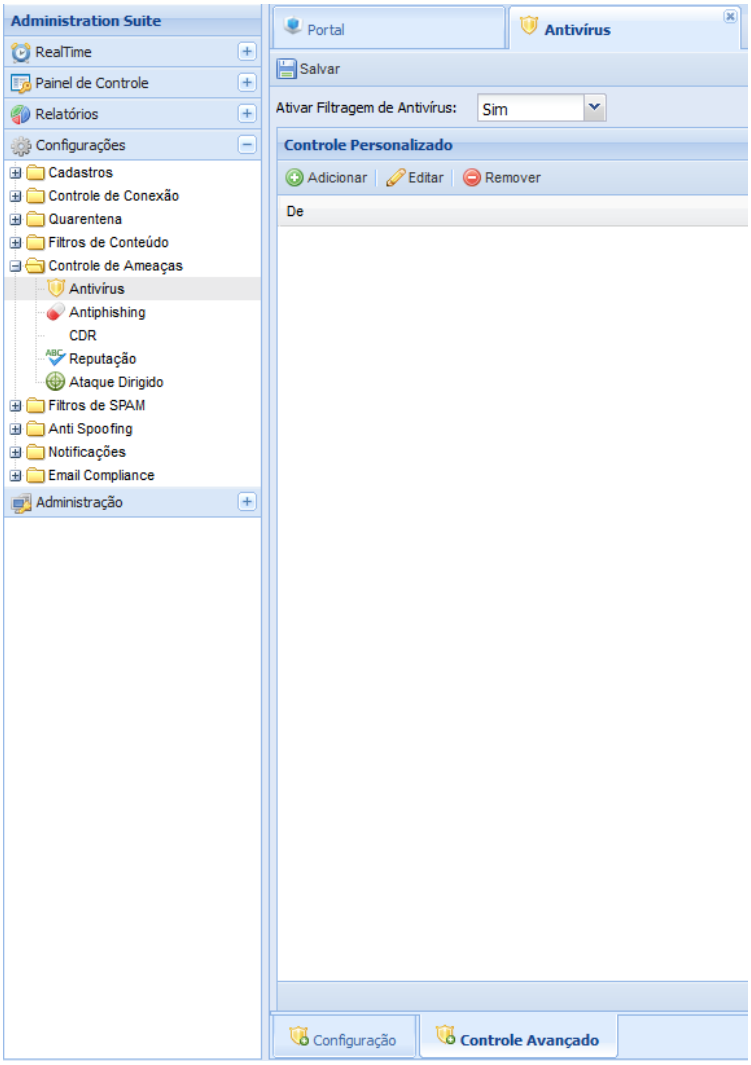
d. Após inserida toda a lista de remetentes, clique em Salvar.



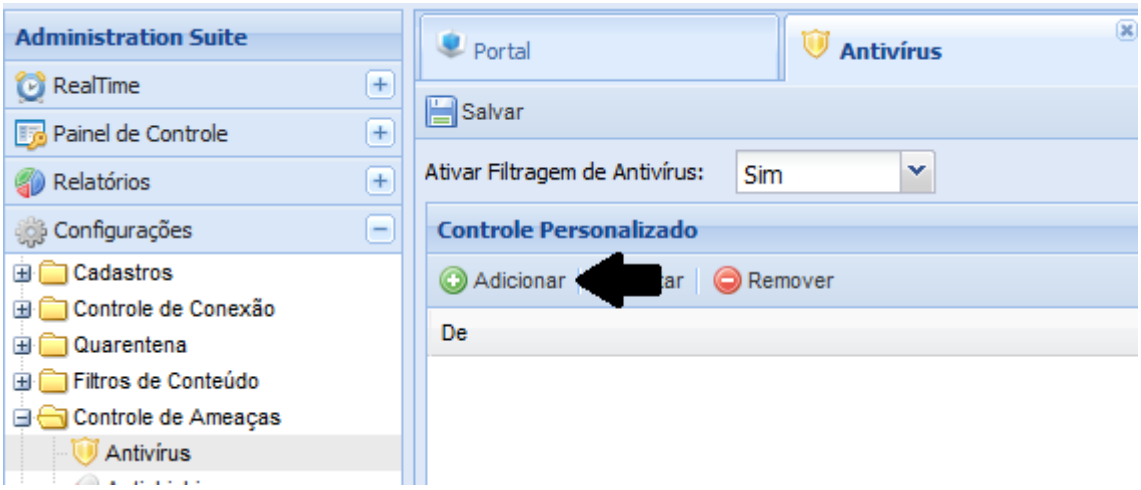
e. Será fechada a janela de Grupos de Usuários e aparecerá na lista o grupo que você acabou de criar.

f. Vá em:
Configurações > Controle de Ameaças > Antivírus
Clique na aba Controle Avançado


Administration Suite
RealTime
Painel de Controle
Relatórios
Configurações
Cadastros
Controle de Conexão
Quarentena
Filtros de Conteúdo
Controle de Ameaças
Antivírus
Antiphishing
CDR
Reputação
Ataque Dirigido
Filtros de SPAM
Anti Spoofing
Notificações
Email Compliance
Administração
Portal
Antivírus
Salvar
F-Secure Engine
Tamanho Máximo dos Arquivos Escaneados:
10
Número Maximo de Níveis de Compactação Escaneados:
5
Habilitar Mecanismo de Detecção Zero-Day:
Sim
Detectar Arquivos Potencialmente Perigosos:
Sim
Enviar Alerta em Caso de Epidemia:
Não
HSC Smart Defender
Habilitar Anti-Phishing:
Sim
Habilitar Anti-Malware:
Sim
Habilitar Proteção Zero Day / Zero Hour:
Sim
Habilitar Detecção de Arquivos Maliciosos:
Sim
Habilitar File Reputation:
Sim
Controle de E-mails suspeitos:
Controle de Arquivos suspeitos:
URL Cloud Sandbox
Malware Categories:
Configuração
Controle Avançado



g. Clique no Botão Adicionar

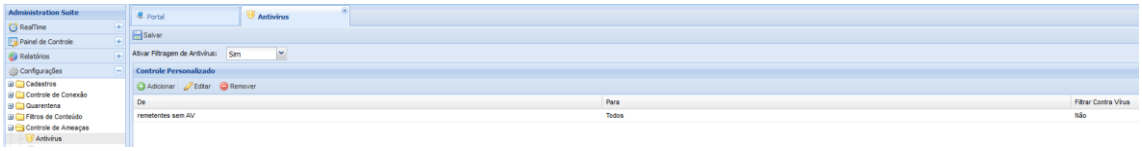


h. Agora é só criar a regra de exceção.

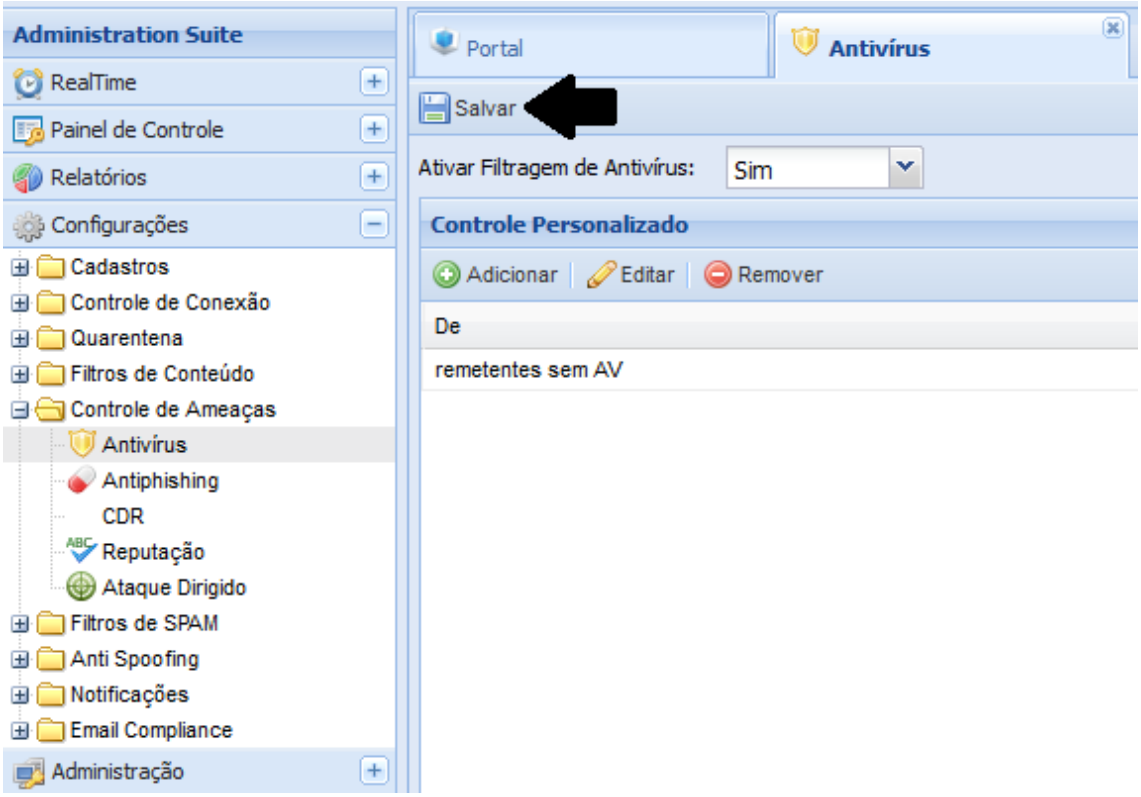
No campo De: Selecione o grupo que você criou. No nosso exemplo é o grupo chamado remetentes sem AV

No campo Para: Selecione Todos, caso você queira "fechar" mais ainda, é possível criar um grupo de e-mails de DESTINATÁRIOS e aplicar a regra aí, mas para título de tutorial, vamos usar o grupo Todos
No campo Filtrar Vírus: Não

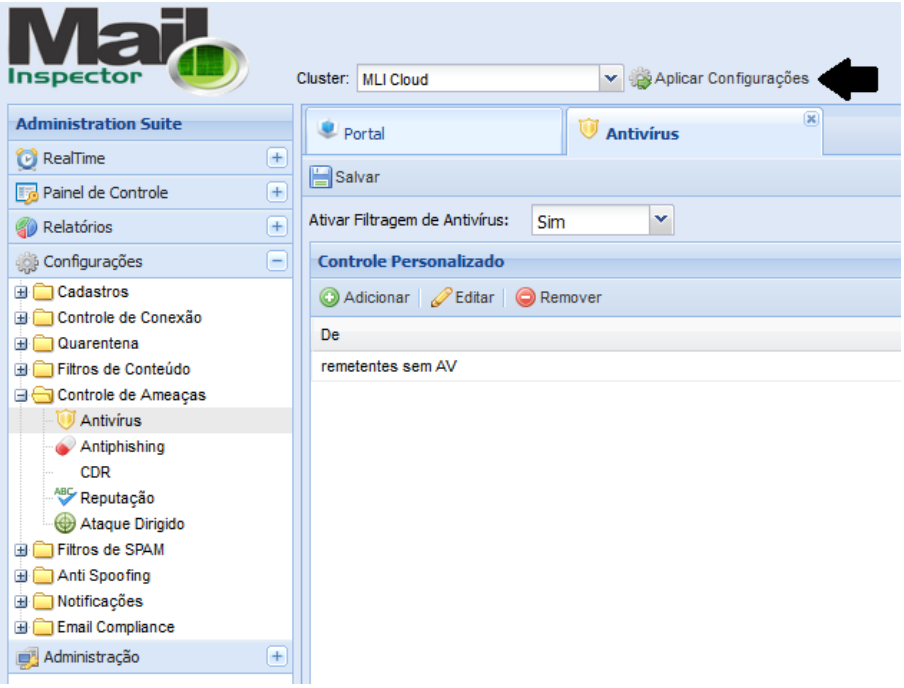
i. Clique no botão Adicionar



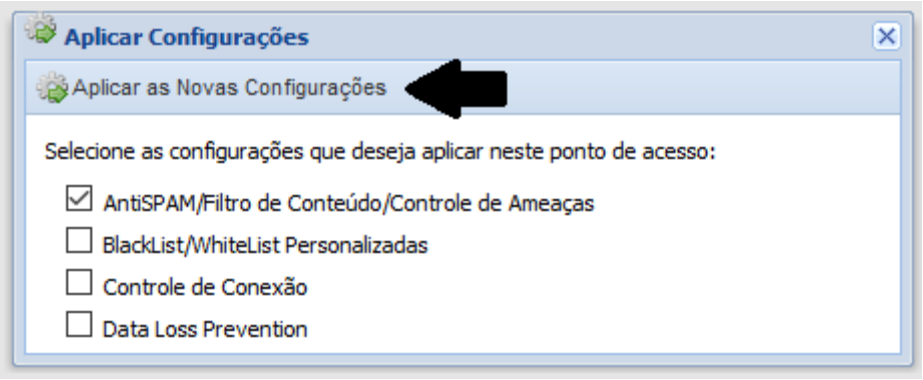
j. Clique no Botão Salvar



k. Clique no Botão Aplicar Configurações



l. Na janela Aplicar configurações, só deixe marcada a opção Aplicar as Novas Configurações e clique em Aplicar as Novas Configurações.



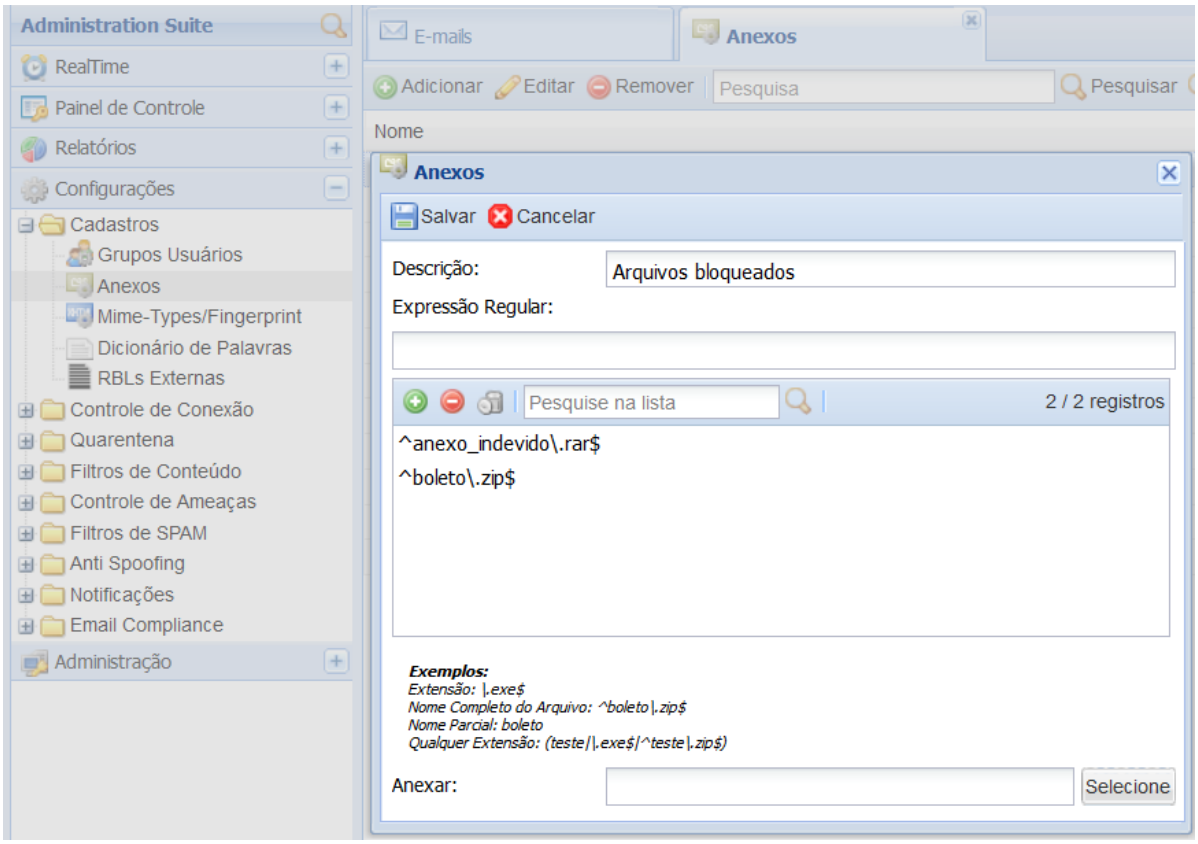
m. Aguarde ele finalizar aplicação das novas configurações. Uma vez finalizada, já está pronto para uso.

Remoção de Anexos

No MailInspector existem duas formas de remover anexos. Primeira é diretamente em Configurações > Filtro de Conteúdo > Controle de Anexos e o Segunda é através de E-mail Compliance.

Basta você criar um grupo de anexos a ser removido.

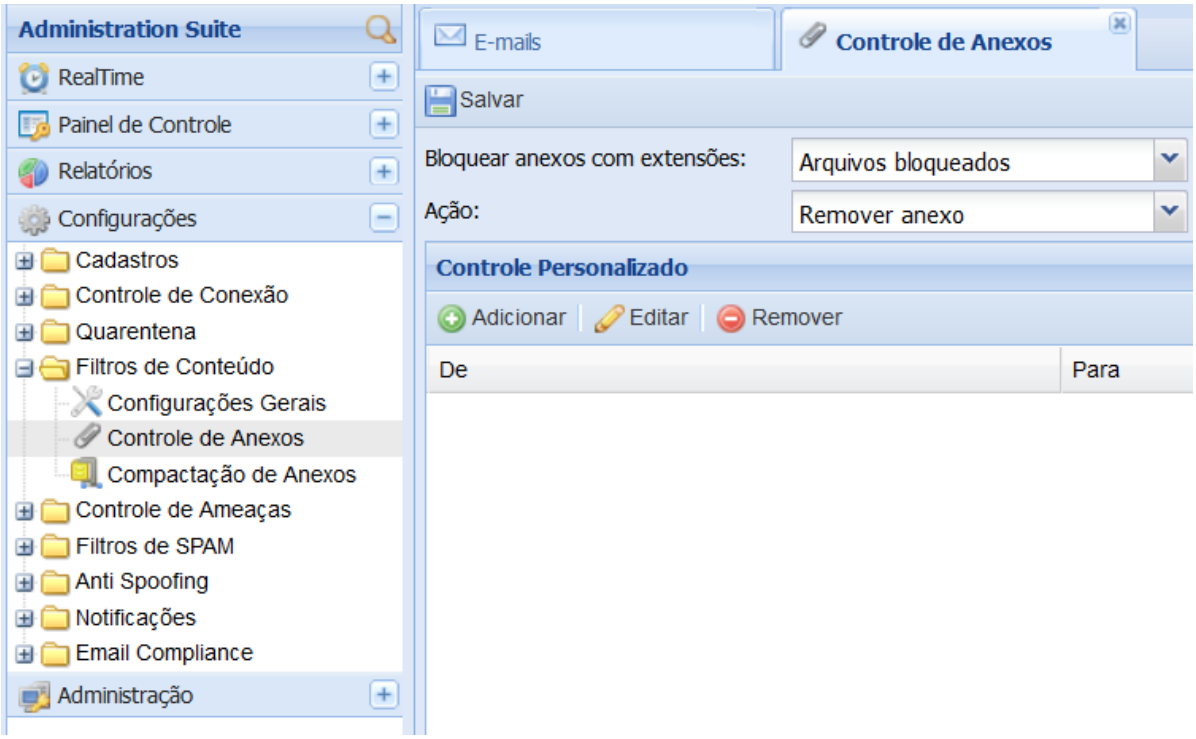
Segue abaixo a tela de exemplo da criação do grupo de anexos a serem removidos:



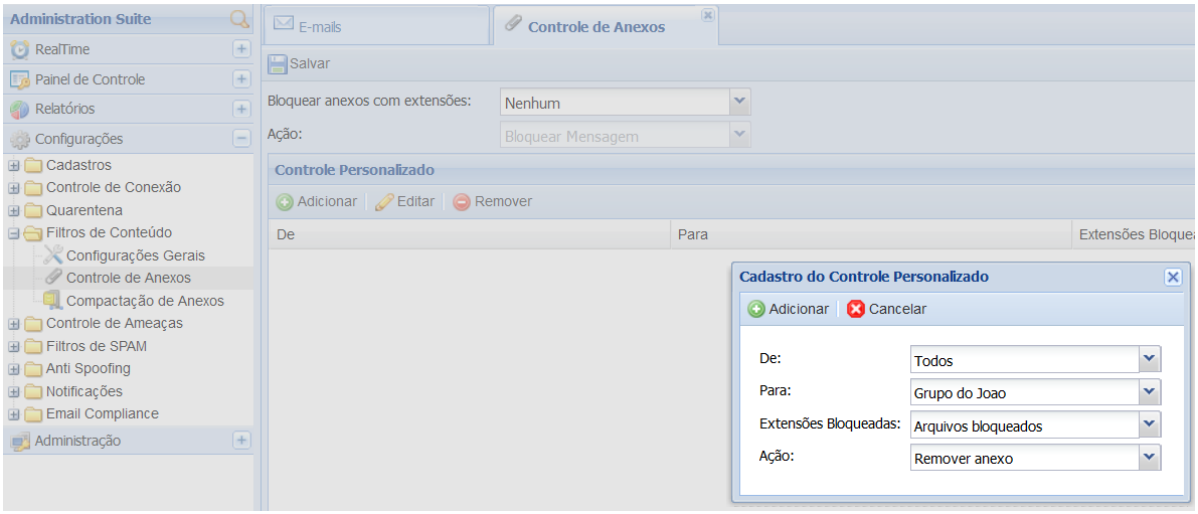
No exemplo serão removidos os anexos indicados.

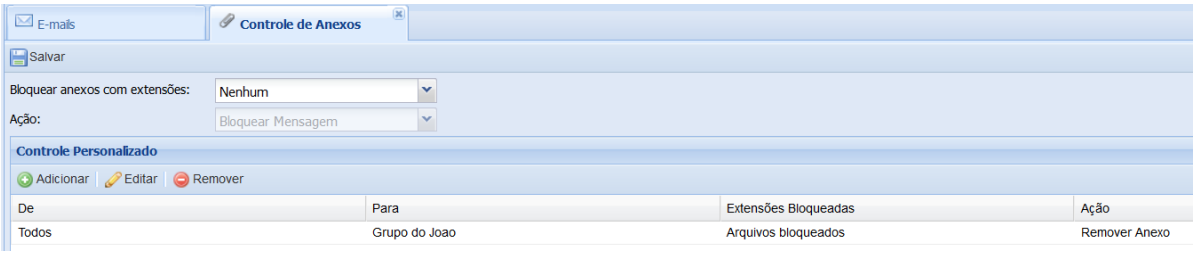
Após criado o grupo, basta ir para a parte de Controle de Anexo > Exten.Bloqueadas e selecionar o Grupo de anexos a serem removidos.

Selecione como ação Remover Anexo.



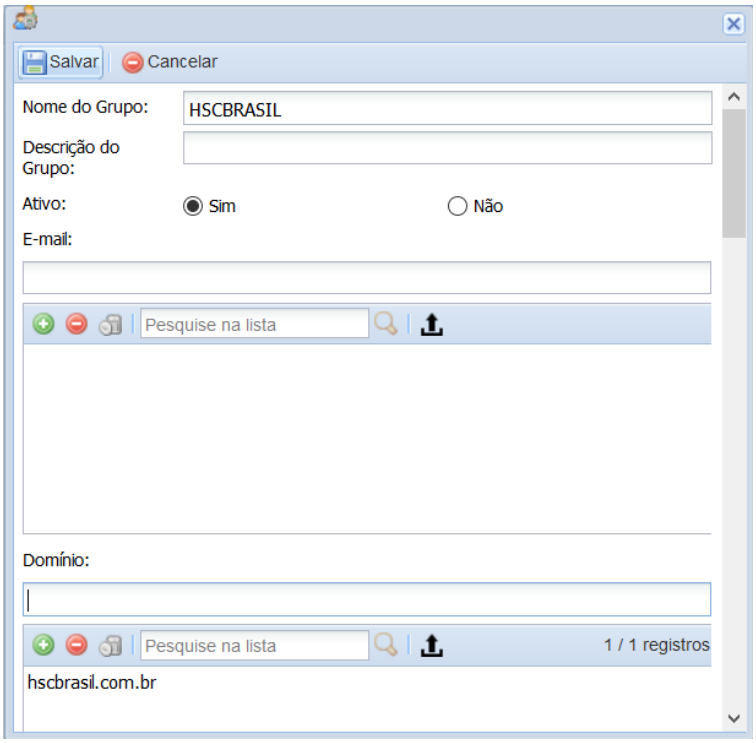
Importante salientar que a regra pode ser aplicada por grupos, ou seja, abaixo segue exemplo da mesma regra aplicada para os e-mails destinados por exemplo Grupo do Joao (é necessário que já tenha sido criado o grupo anteriormente, em Cadasttos > Grupos Usuários)



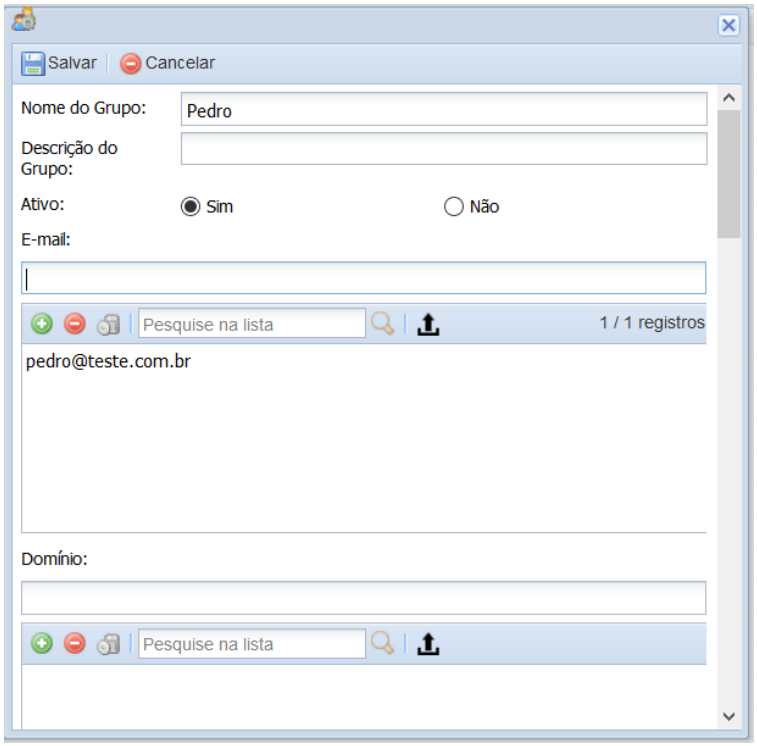


Assim como usando o De: Todos para o Grupo do Joao, é possível cruzar outras referências, como por exemplo o que vier do domínio hscbrasil.com.br (coloquei nome do grupo para pedro@teste.com.br efetuar o procedimento de Remover anexo, para arquivos bloqueados (anexos específicos). Para isso, basta criar o grupo e depois aplicar a regra de remoção de anexo.

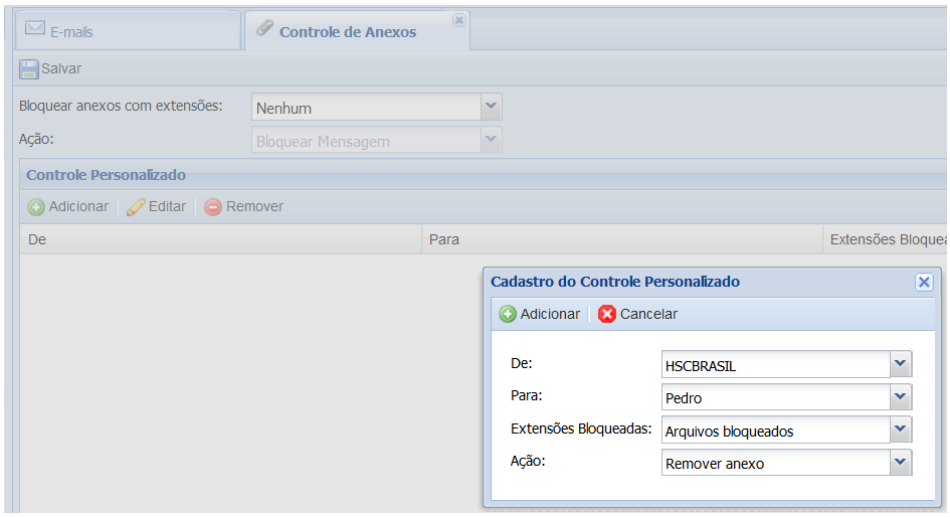
Criando o grupo HSCBRASIL, onde o grupo terá o domínio da hscbrasil.com.br:



E também criando o Grupo chamado Pedro, onde este grupo terá somente o e-mail pedro@teste.com.br



Criando a regra de remoção de anexo:



Onde:

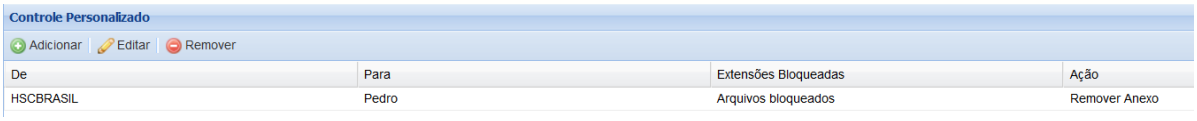
DE: HSCBRASIL, indica que todo e-mail que vier do domínio hscbrasil.com.br (conforme grupo criado anteriormente)

PARA: Pedro (e-mail para pedro@teste.com.br)

Extensões Bloqueadas (Arquivos bloqueados)

Ação: Remover Anexo

Deve ficar:



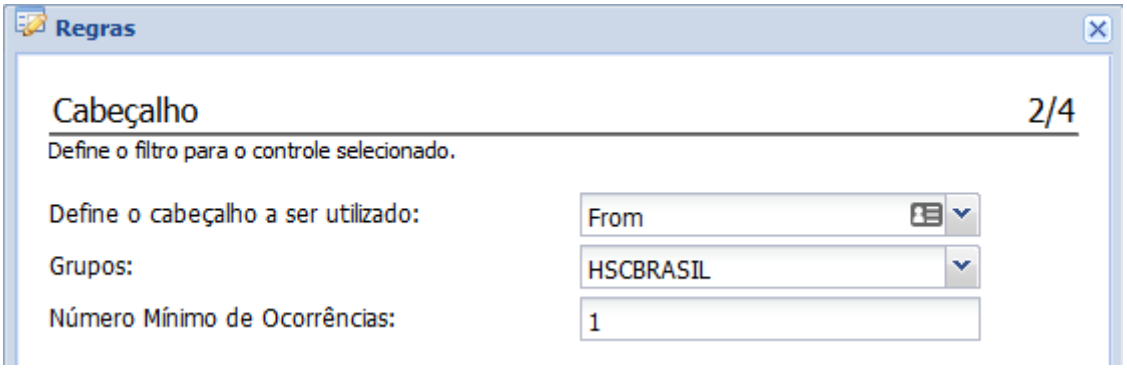
Controle Personalizado

Adicionar | Editar | Remover

De	Para	Extensões Bloqueadas	Ação
HSCBRASIL	Pedro	Arquivos bloqueados	Remover Anexo

A Segunda forma de remoção de anexo é pelo E-mail Compliance:

No E-mail Compliance, faça a regra FROM



Regras

Cabeçalho 2/4

Define o filtro para o controle selecionado.

Define o cabeçalho a ser utilizado: From

Grupos: HSCBRASIL

Número Mínimo de Ocorrências: 1

Regras

Informações e Ações 3/4

Define informações gerais e ações que serão realizadas.

Nome: FROM HSCBRASIL

Descrição:

Tipo: DLP

Ações

Log: ☑ Registrar em Log ☐ Armazenar para Auditoria

Notificação: ☐ Remetente ☐ Destinatário

Ação: ◉ Entregar ☐ Sem Anexo ○ Rejeitar / Deletar / Não Entregar

Encaminhar para: Nenhum

Alterar assunto:

Alterar cabeçalho: Valor:

Processamento da Regra: ◉ Continuar ○ Finalizar

Voltar Avançar

Regras

Conclusão do Processo 4/4

Salvar a configuração da regra de complice.

Nome: FROM HSCBRASIL
Descrição:

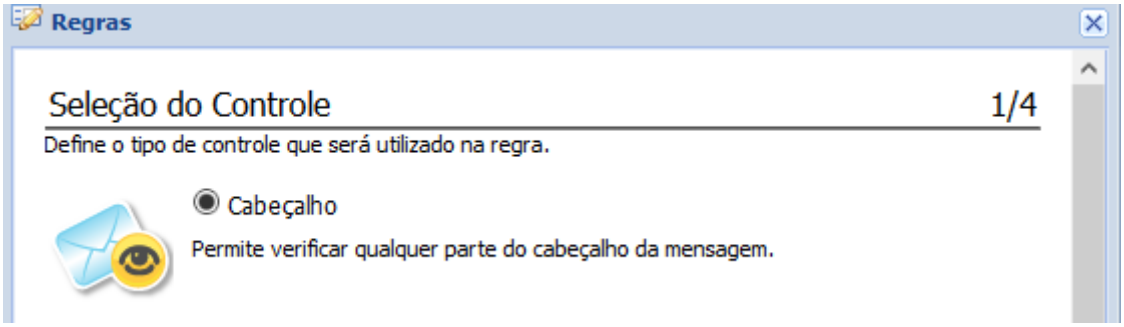
Propriedades

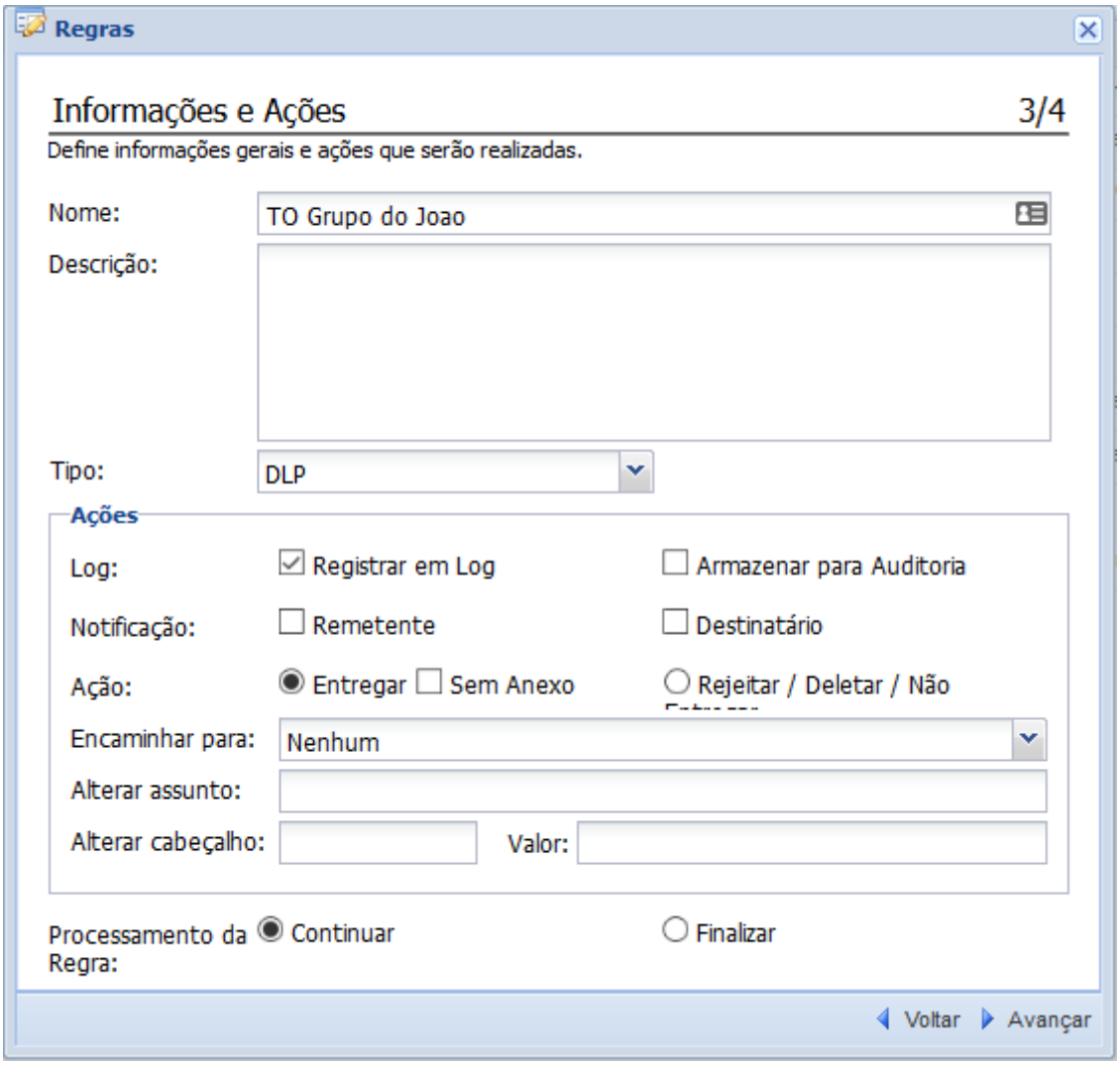
Controle: Cabeçalho
Define o cabeçalho a ser utilizado: From
Grupo: HSCBRASIL
Número Mínimo de Ocorrências: 1

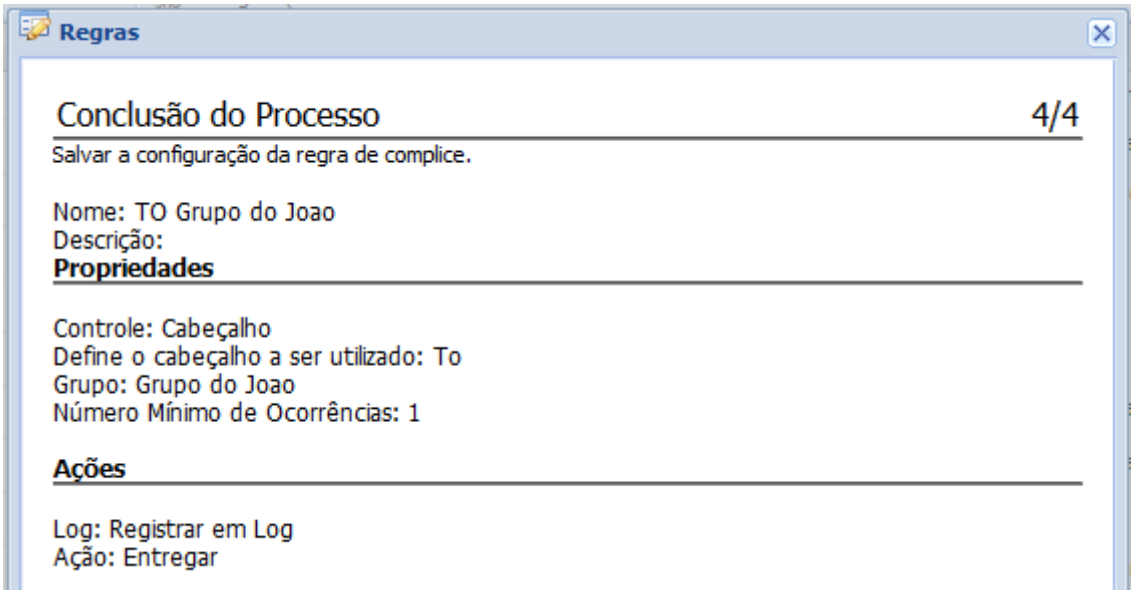
Ações

Log: Registrar em Log
Ação: Entregar

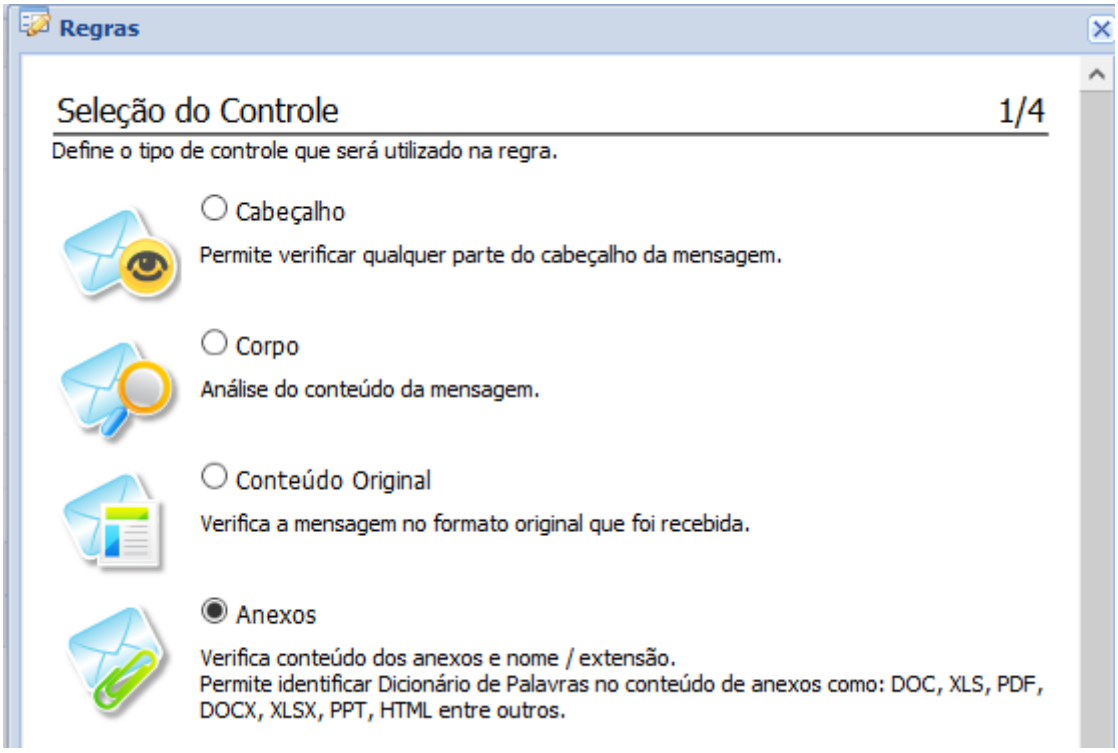
Faça outra regra de Compliance, agora considerando o TO







Vamos agora criar a regra de compliance, onde detectará os ARQUIVOS BLOQUEADOS



Regras

Anexo 2/4

Define o filtro para o controle selecionado.

Tipo de Anexo: Grupo de Anexos

Grupo de Anexos: Arquivos bloqueados

Regras

Informações e Ações 3/4

Define informações gerais e ações que serão realizadas.

Nome: Arquivos Bloqueados

Descrição:

Tipo: DLP

Ações

Log: ☑ Registrar em Log ☐ Armazenar para Auditoria

Notificação: ☐ Remetente ☐ Destinatário

Ação: ◉ Entregar ☐ Sem Anexo ○ Rejeitar / Deletar / Não Entregar

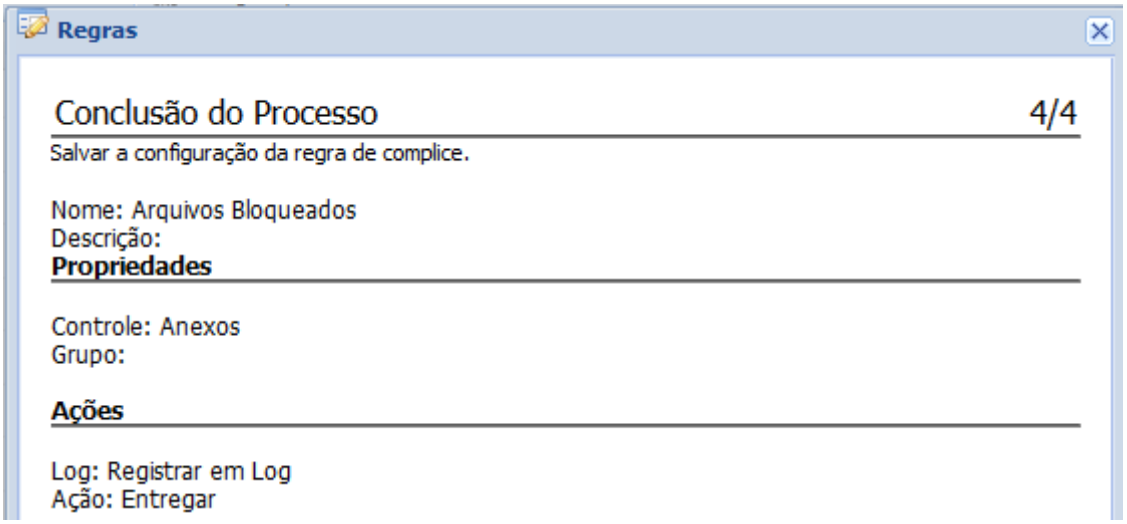
Encaminhar para: Nenhum

Alterar assunto:

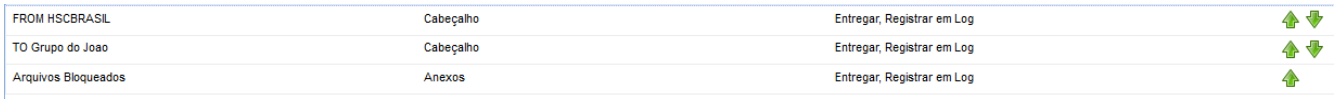
Alterar cabeçalho: Valor:

Processamento da Regra: ◉ Continuar ○ Finalizar

Voltar Avançar

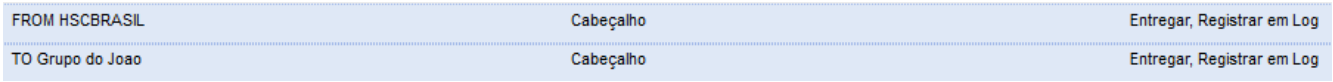


Repare que tem três novas regras criadas no E-mail Compliance:

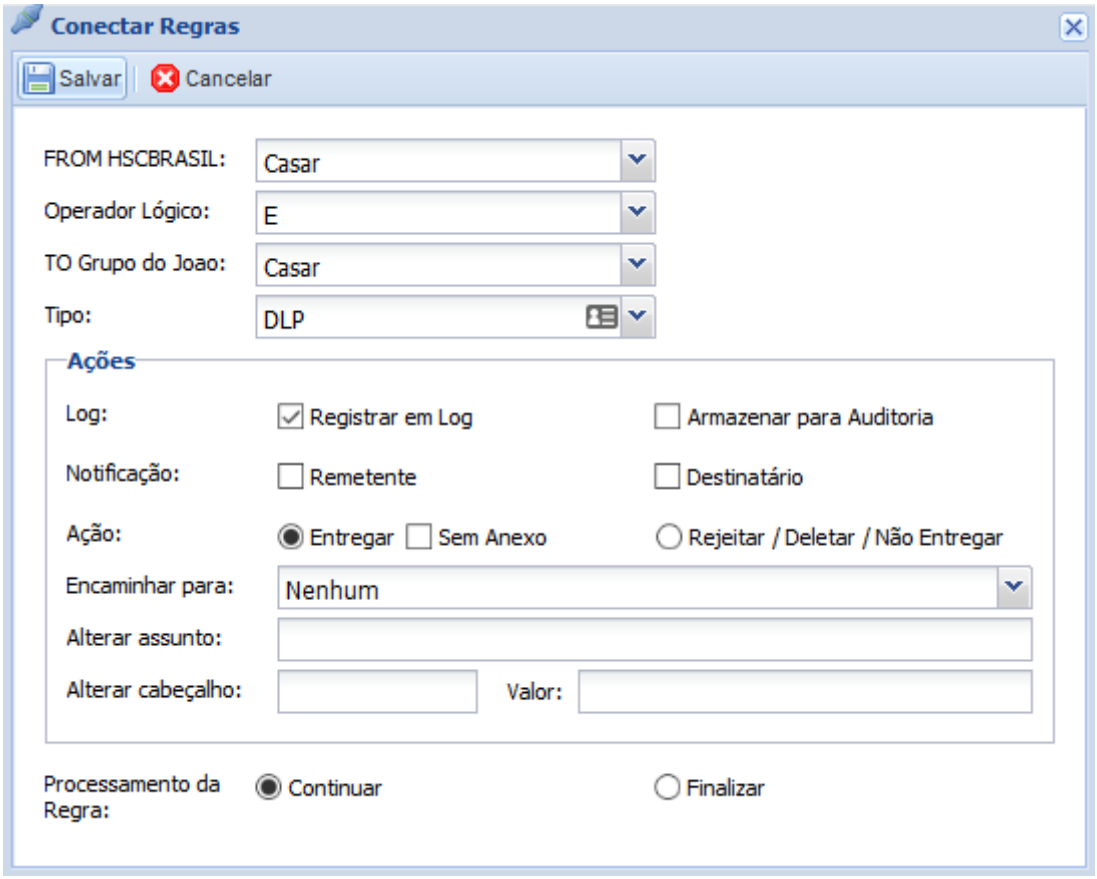


FROM HSCBRASIL	Cabeçalho	Entregar, Registrar em Log	
TO Grupo do Joao	Cabeçalho	Entregar, Registrar em Log	
Arquivos Bloqueados	Anexos	Entregar, Registrar em Log	

Selecione as regras de FROM e TO e clique em Conectar



FROM HSCBRASIL	Cabeçalho	Entregar, Registrar em Log
TO Grupo do Joao	Cabeçalho	Entregar, Registrar em Log



Após salvar a regra, pode-se verificar que no E-mail Compliance, aparecerá a regra agrupada:

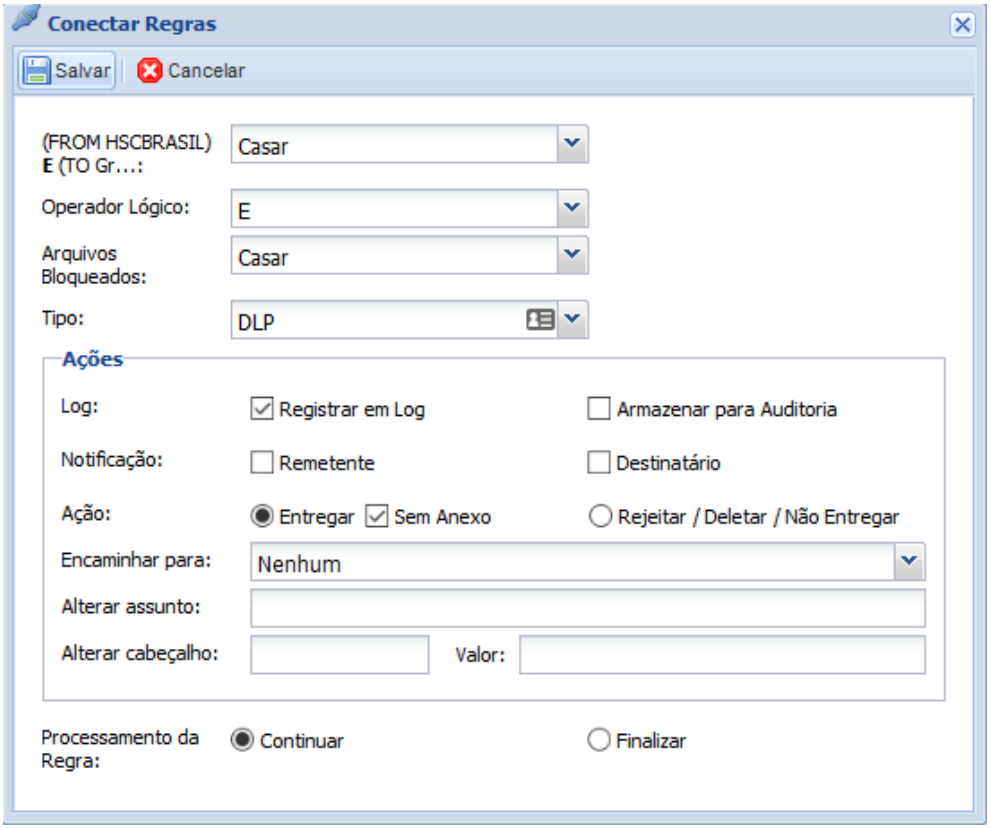
(FROM HSCBRASIL) E (TO Grupo do Joao)	(Cabeçalho) E (Cabeçalho)	Registrar em Log, Entregar

Marca-se a “nova” regra agrupada e a regra de Arquivos Bloqueados

Arquivos Bloqueados	Anexos	Entregar, Registrar em Log
(FROM HSCBRASIL) E (TO Grupo do Joao)	(Cabeçalho) E (Cabeçalho)	Registrar em Log, Entregar

Clica-se em Conectar, para agrupar as duas regras.

Nas ações seleciona-se Entregar, mas marca-se a opção Sem Anexo.



Agora é só Salvar a Aplicar as Configurações

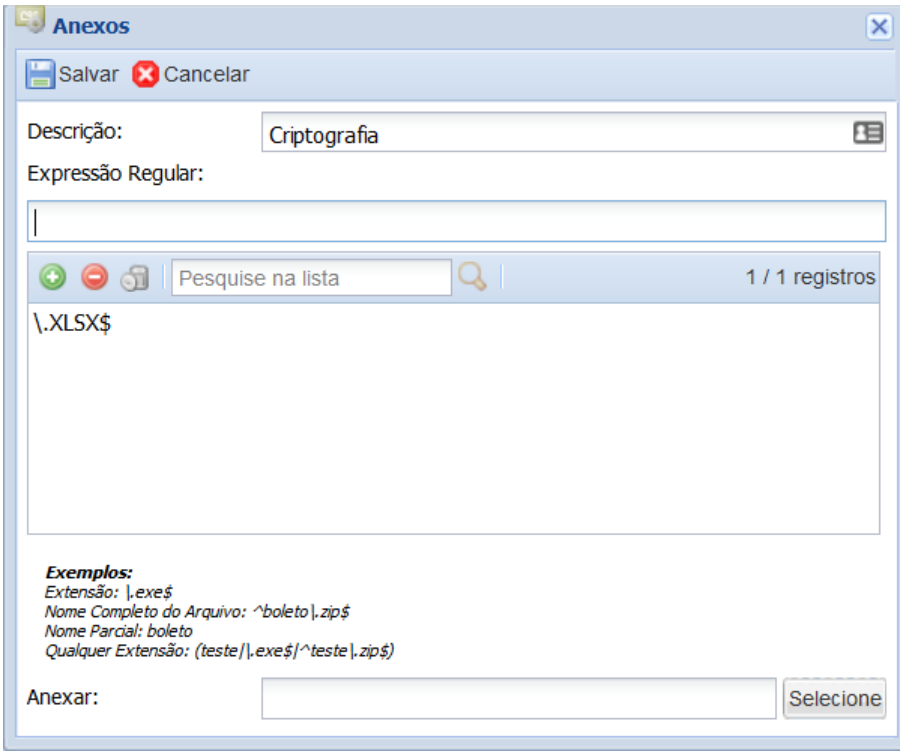
Remoção de Anexo Cifrado, mas sem Compactação

Exemplo de bloqueio de anexo com senha, do tipo XLSX.

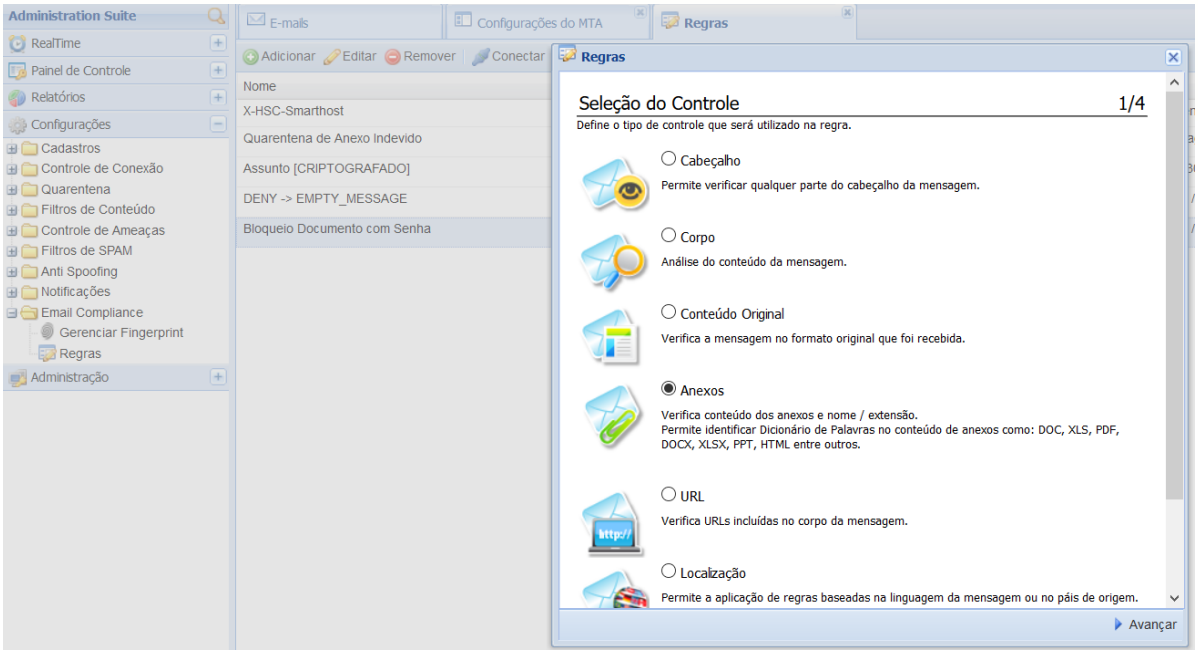
Criando regra de bloqueio de arquivo cifrado, mas sem compactação:

Em Configurações > Cadastros > Anexos

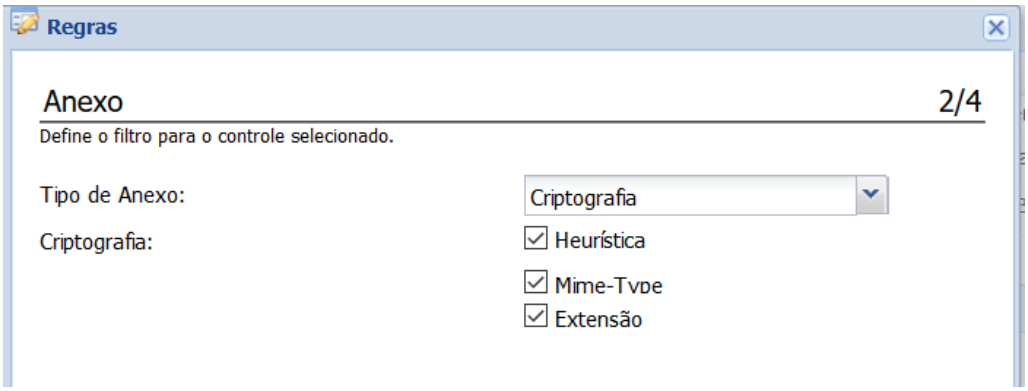
Cria-se o grupo de anexo do tipo XLSX, ao qual chamei de Criptografia:



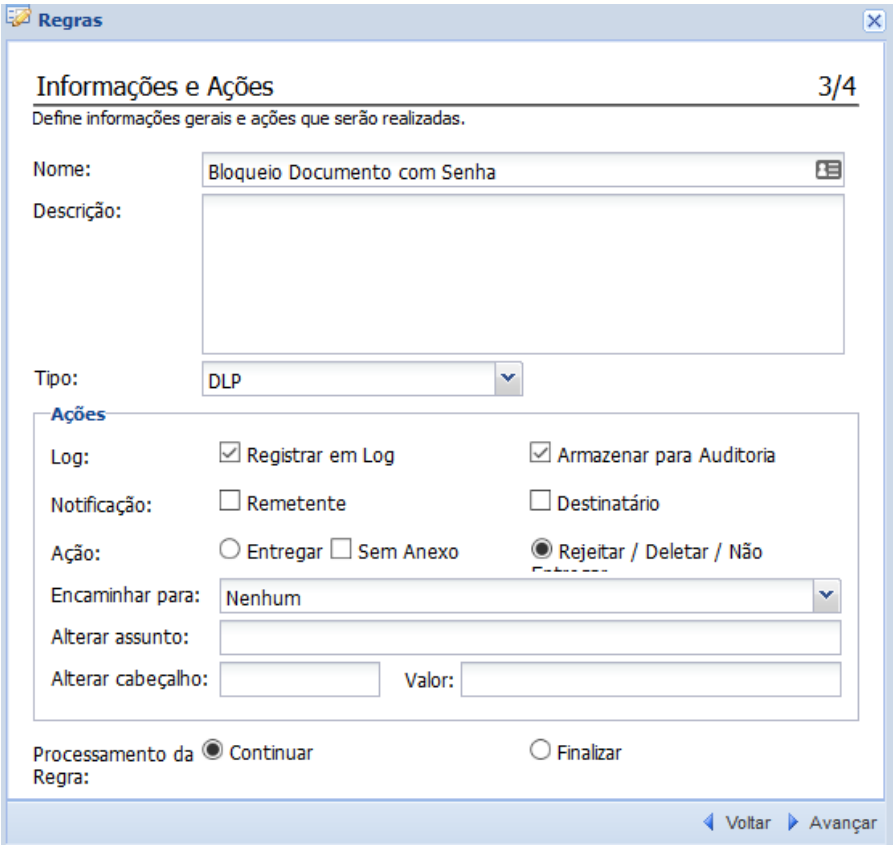
Vá em Configurações > E-mail Compliance > Regras



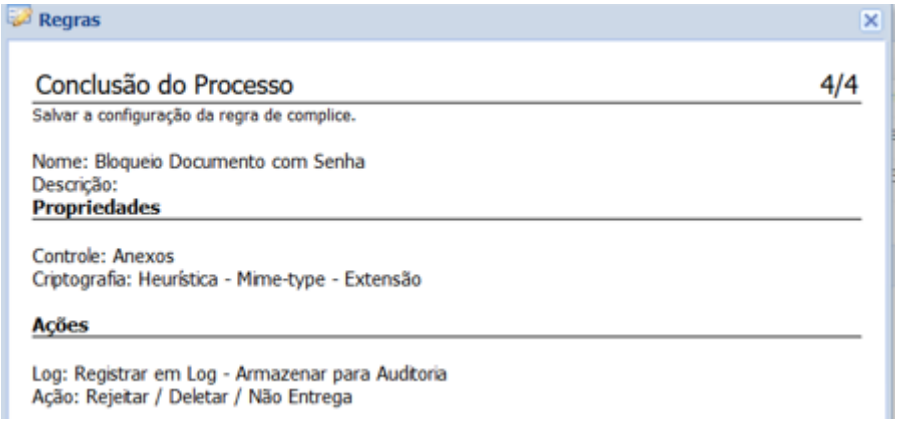
No Tipo de Anexo, selecione o Grupo anteriormente criado (que são referentes a XLSX)



No tipo de criptografia, selecione todas as opções



Selecione a ação de Rejeiar/Deletar/Não Entregar. Caso você queira que o e-mail seja entregue, mas sem o anexo, bastaria selecionar a ação de Entregar sem Anexo, no lugar ada ação de Rejeitar/Deletar/Não Entregar.



É só Salvar e Aplicar Configurações, para que a regra comece a ser considerada.

Segue abaixo o resultado do bloqueio:

E-mails | Configurações do MTA | Regras

Ponto de Acesso: Todos | 14C049B59BB.A415E | Pesquisar | Limpar | Pesquisa Avançada | Exportar | Quarentena: | Ações

Ponto de Acesso	Data/Hora	Assunto	De	Para	Tamanho	Pontuação	Anexo	Tráfego	Entregue	Status
mail.gtpn.com.br	16/06/20 14:26:47	Teste XLS Com Senha	root@gtpn.com.br	romulo@hscbrasil.com.br	317.49KB	4.28				

Regras de Compliance

Detalhe da Mensagem 14C049B59BB.A415E

ID: 14C049B59BB.A415E
Assunto: Teste XLS Com Senha
Data: 2020-06-16 14:26:47
De (Envelope): root@gtpn.com.br
Para (Envelope): romulo@hscbrasil.com.br
De (Header): root@hscbrasil.com.br
Para (Header): romulo <romulo@hscbrasil.com.br>
Tamanho: 317.49KB
IP de Origem: 187.108.197.149
Ponto de Acesso do Cluster: mail.gtpn.com.br

Filtros de Conteúdo | Filtros de Spam | Ameaças | Cabeçalho | Texto | HTML | Anexos | **Data Loss Prevention** | CDR | Smart Defender | Log de

Regras de Compliance

Nome: Bloqueio Documento com Senha
Ação: Rejeitar / Deletar / Não Entrega, Armazenar para Auditoria, Registrar em Log

Detalhe da Mensagem 14C049B59BB.A415E

ID: 14C049B59BB.A415E
Assunto: Teste XLS Com Senha
Data: 2020-06-16 14:26:47
De (Envelope): root@gtpn.com.br
Para (Envelope): romulo@hscbrasil.com.br
De (Header): root@hscbrasil.com.br
Para (Header): romulo <romulo@hscbrasil.com.br>
Tamanho: 317.49KB
IP de Origem: 187.108.197.149
Ponto de Acesso do Cluster: mail.gtpn.com.br

Filtros de Conteúdo | Filtros de Spam | Ameaças | Cabeçalho | Texto | HTML | **Anexos** | Data Loss Prevention | CDR | Smart Defender | Log de

Anexos

Fluxo HSC 2020 (14).xlsx

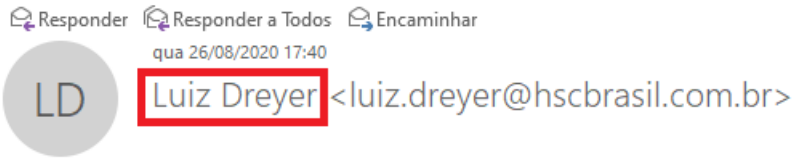
Código Fonte

Mensagem Completa

Proteção de Display Names (Usuários VIPs) Verificação no FROM do Header

Um dos ataques mais comuns é o criminoso enviar e-mail fingindo ser um diretor da empresa, mas o que ele acaba não se atentando é o Display Name apresentado no e-mail.

No exemplo abaixo o display name é Luiz Dreyer

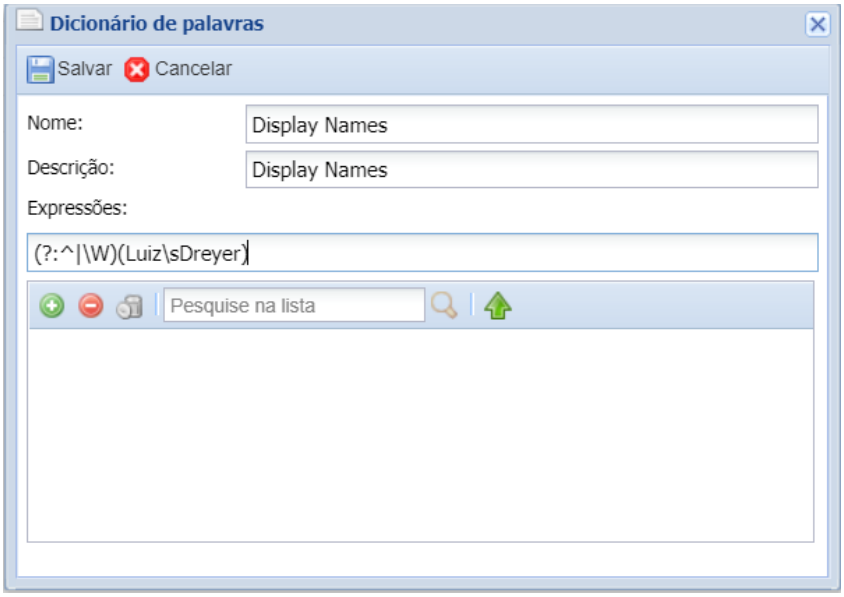


Lógica a ser aplicada:

1. Cria-se um Cadastro de Dicionário de Palavras chamado Display Names.
2. Cria-se um outro grupo de usuários chamado ALVO, onde serão incluídos os e-mails dos diretores e outras pessoas que podem ser alvos dos criminosos.
3. Na parte de E-mail compliance, faz-se uma regra para quando o TO for para o grupo ALVO, quando você desejar a proteção com os VIP's como ALVO, mas é possível também fazer a proteção sendo alguém tentando se passar por um VIP (típico BEC - Business E-mail Compromise), aí a regra em vez de ser TO, será FROM.
4. Na parte de E-mail compliance, faz-se outra regra para quando o e-mails no campo to tiver um membro do Grupo Display Names.
5. Concatena-se as regras do item 3 e 4, mas desta vez, **casando** a regra 3 com **não casando** regra 4. Na concatenação, ativa-se o DLP, para bloqueio.

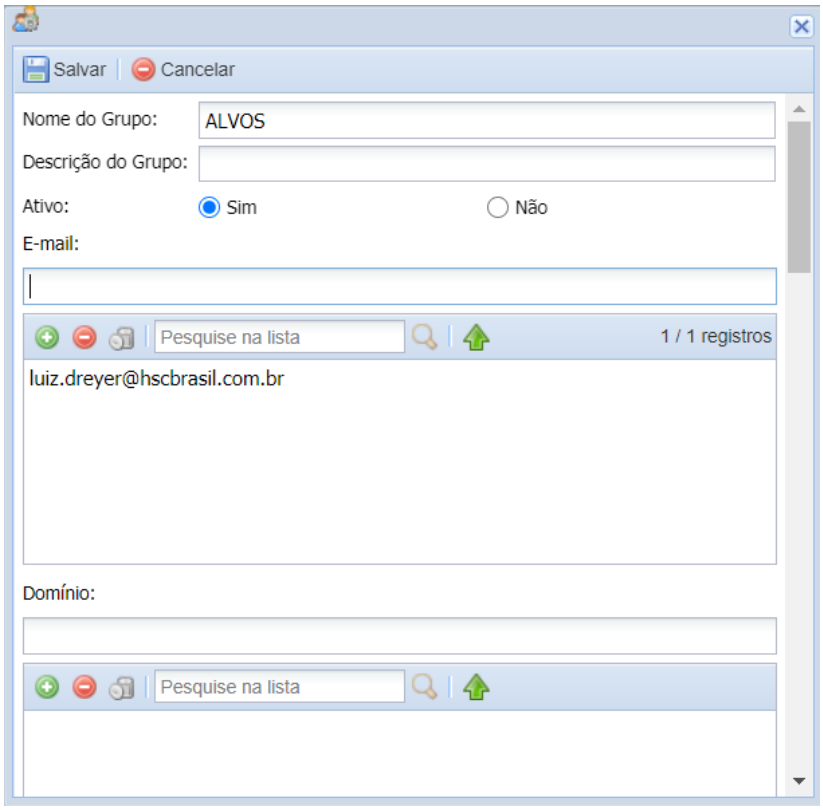
Em Configurações > Cadastros > Dicionário de Palavras

É criado o cadastro dos Display Names.



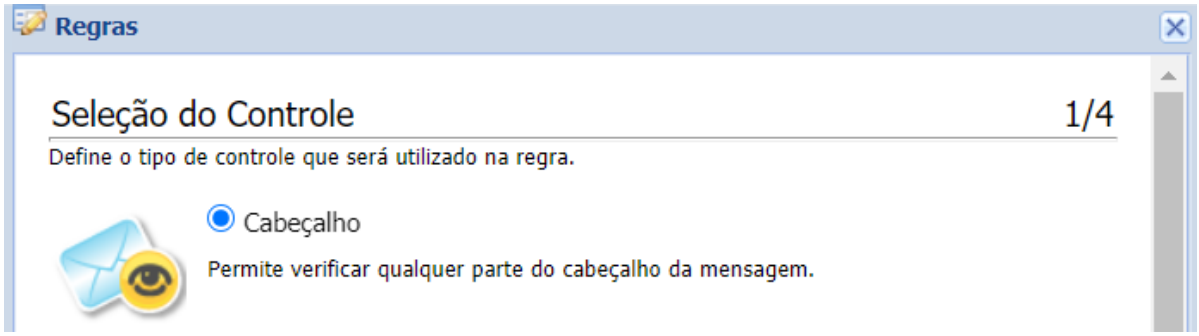
Em Configurações > Cadastro > Grupo Usuários

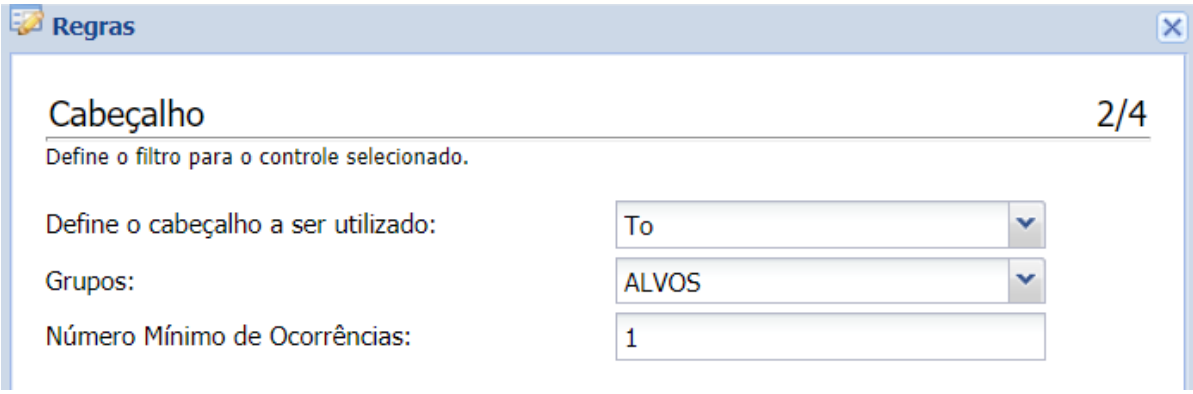
É criado os e-mails ALVOS

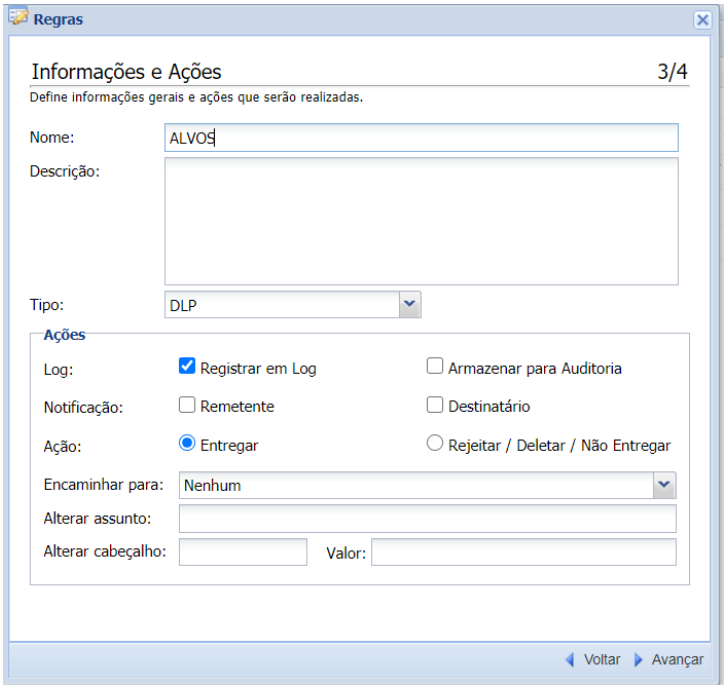


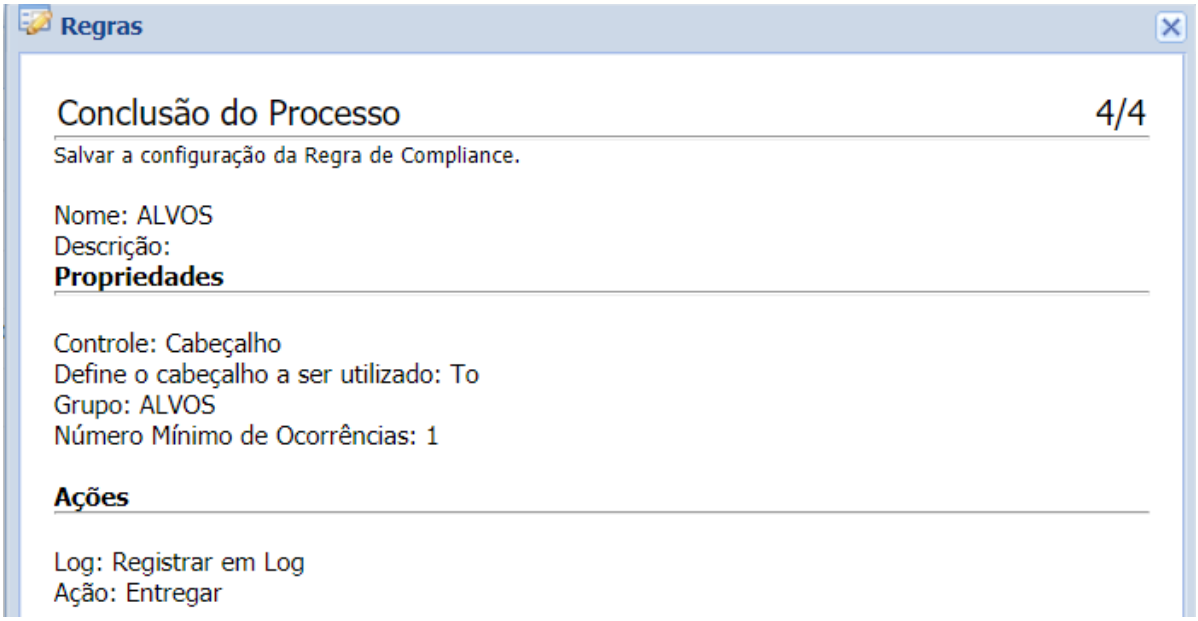
Em Configurações > E-mail Compliance > Regras

Crio a primeira regra, que é todos os e-mails para o destino ALVOS.



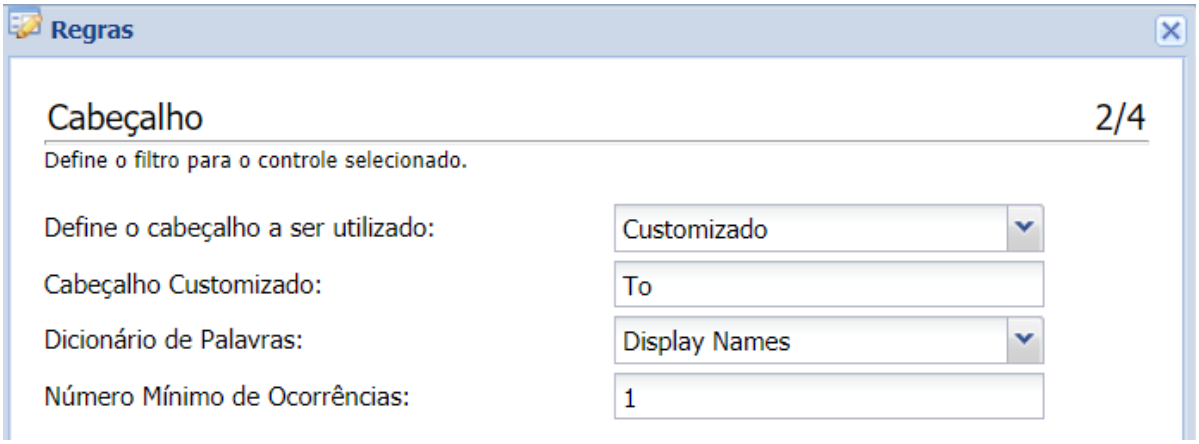

Regras
Cabeçalho
2/4
Define o filtro para o controle selecionado.
Define o cabeçalho a ser utilizado:
To
Grupos:
ALVOS
Número Mínimo de Ocorrências:
1

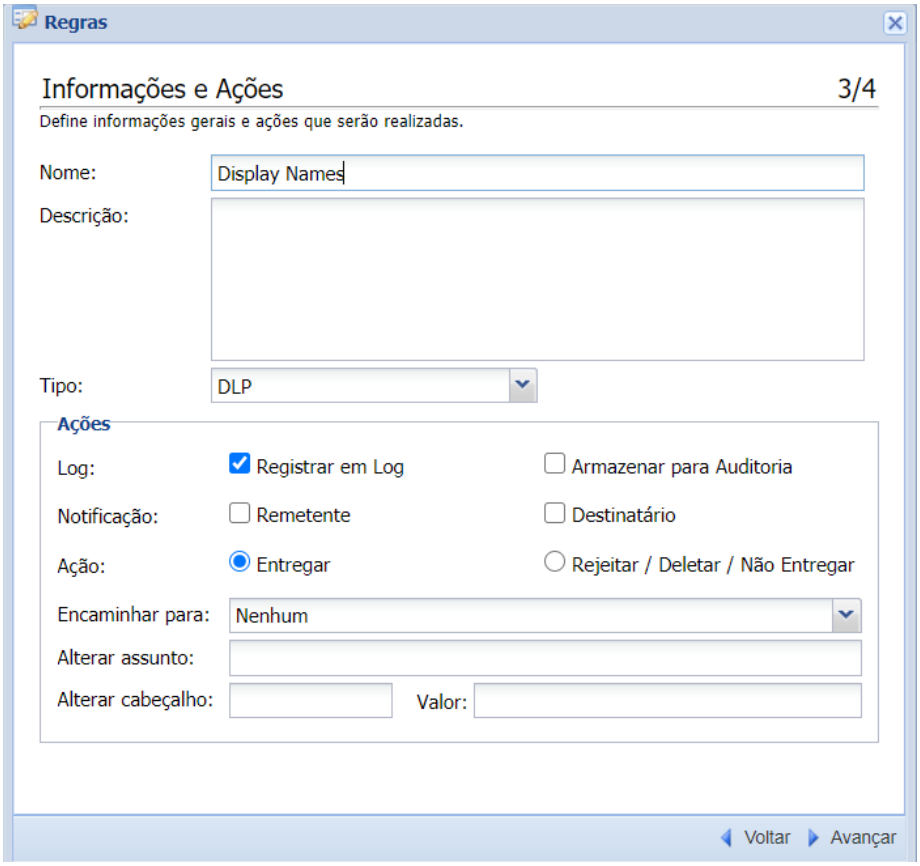

Regras
Informações e Ações
3/4
Define informações gerais e ações que serão realizadas.
Nome:
ALVOS
Descrição:
Tipo:
DLP
Ações
Log:
Registrar em Log
Armazenar para Auditoria
Notificação:
Remetente
Destinatário
Ação:
Entregar
Rejeitar / Deletar / Não Entregar
Encaminhar para:
Nenhum
Alterar assunto:
Alterar cabeçalho:
Valor:
Voltar
Avançar

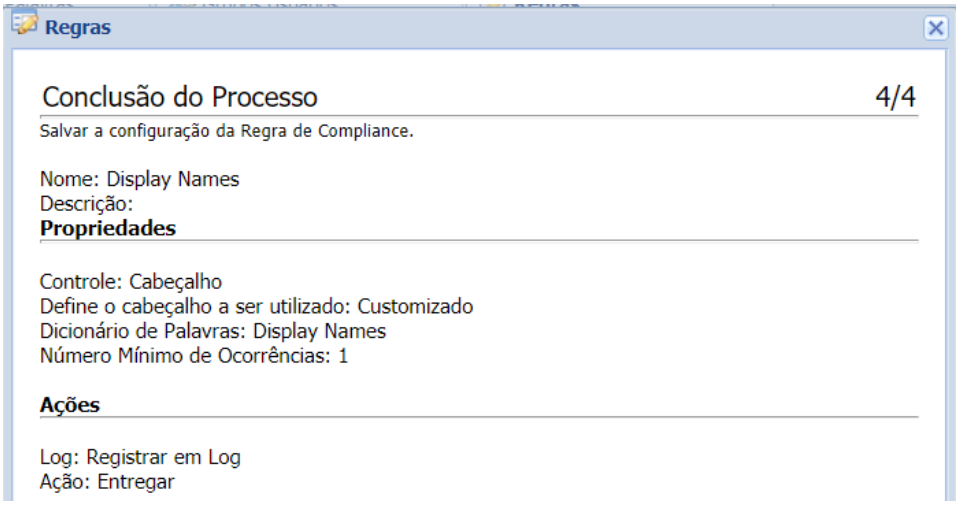


9	ALVOS	Cabeçalho	Entregar, Registrar em Log	

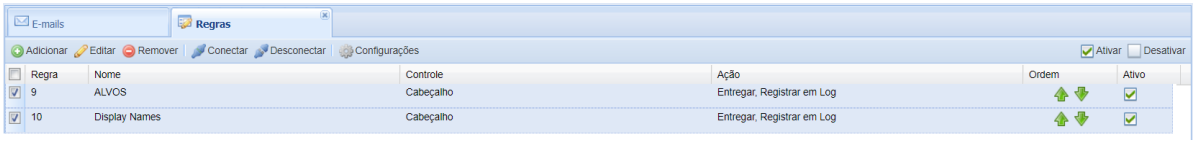
Agora faremos similarmente coisa para o Display Name, ou seja, adiciona-se nova regra chamada Display Names.







Selecione as duas regras.



Clique em Conectar.

Nos campos:

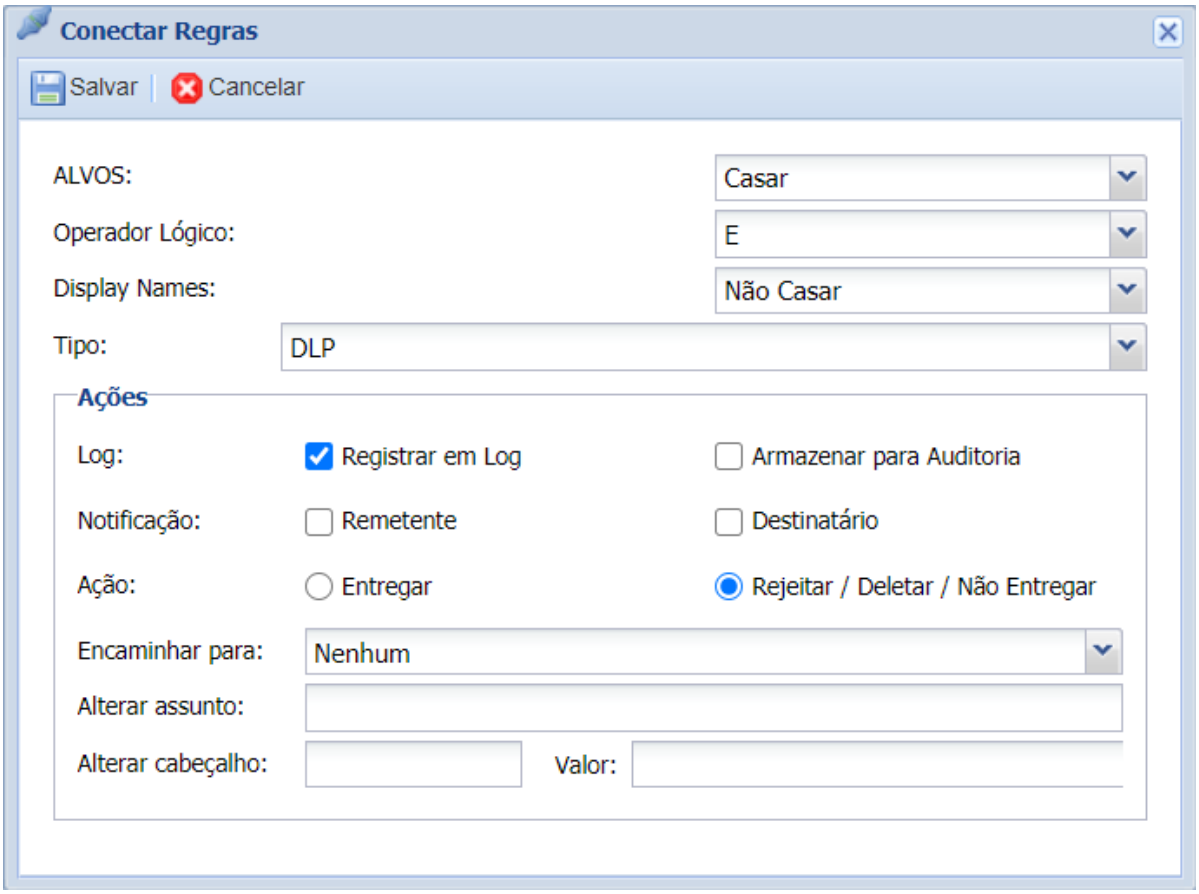
ALVOS selecione CASAR

Display Names selecione NÃO CASAR

Tipo: DLP

Ação: Rejeitar/Deletar/Não Entregar

Se você quiser, é possível encamonhar o e-mail a um terceiro, mas no caso, vamos deixar sem esse encaminhamento.



Clique em Salvar.

Clique em Aplicar Configurações.

Obs: Foi feita a regra no módulo E-mail Compliance, mas é possível fazer essa mesma regra para o módulo SPAM, ou seja, em vez de efetuar o bloqueio direto pelo DLP, pode-se optar por aumentar a pontuação do e-mail e com isso ele vir a ser bloqueado pela pontuação.

Obs: Fzemos a proteção à partir do DESTINO (no caso ALVO), é possível fazer baseado em ORIGEM, ou seja pelo FROM do HEADER, verificando o Display Name no FROM em vez de verificar no campo TO, dessa forma é

possível fazer a proteção com cadastro de display names de e-mails particulares, como por exemplo de um diretor da empresa que use o Gmail, aí pode ser feito o cadastro do display name do Gmail dele e a verificação pelo FROM do HEADER. Maiores informações, favor acione o nosso suporte.

O MailInspector fornece total proteção a usuários do tipo VIP, detectando fraudes de e-mail, fraudes de Display Names, evitando dessa forma o ataque do tipo BEC (Business E-mail Compromise).

Aumentando segurança com detecção de phishing por FakeBounce (Boas Práticas)

Sabendo que por padrão os e-mails de Bounce Mail, vem com o Remetente (no Envelope do E-mail) em branco, muitos hackers fazem ataques simulando fakebounce deixando o FROM do ENVELOPE em branco.

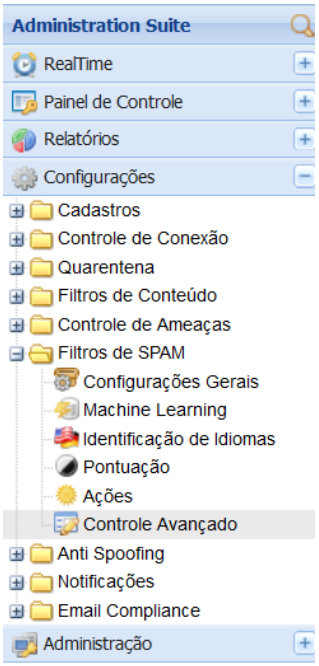
Para prevenir esse tipo de ataque, podemos fazer uma regra casando duas assinaturas do MailInspector:

- Detecção de SENDER DO ENVELOPE em branco;
- Detecção de palavras chaves e/ou texto padrão de phishing no corpo da mensagem;

Casando essas duas regras, aumentaremos a pontuação em 10.

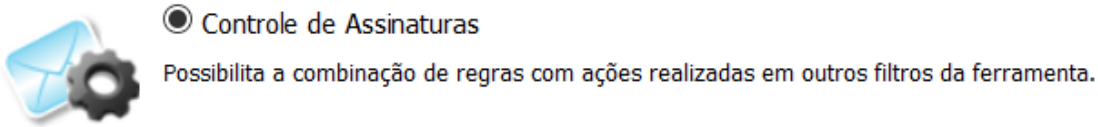
Primeiramente vamos para a parte onde criaremos as regras:

Configurações > Filtro de SPAM > Controle Avançado



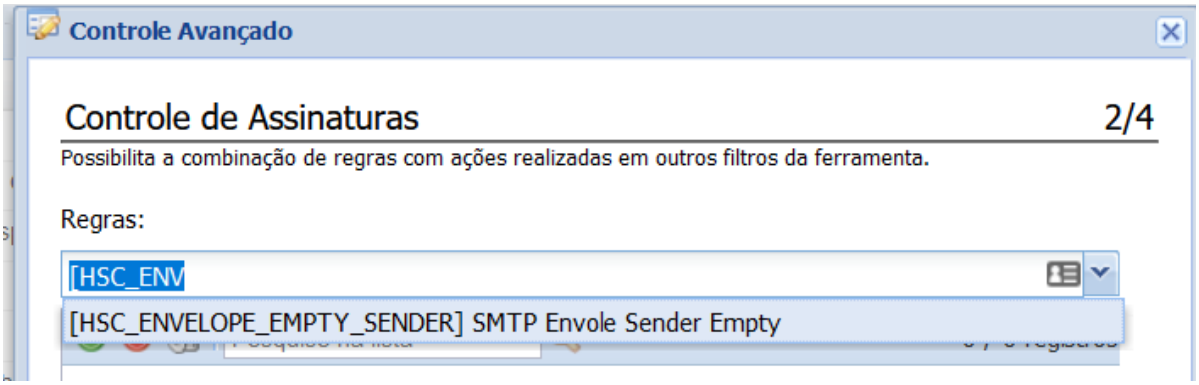
1. Clique em Adicionar (+)

Selecione a Regra por Controle de Assinaturas



A primeira regra que vamos fazer é para detectar o SENDER do ENVELOPE VAZIO

Indicado pela regra: [HSC_ENVELOPE_EMPTY_SENDER]



Selecione a regra indicada e clique em Avançar

Dê um nome a regra e coloque qualquer pontuação (já que essa pontuação será suprimida ao casar com outra regra – regra de texto com características de phishing)

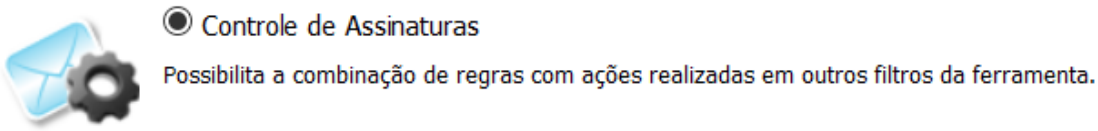
Clique em Avançar e na próxima tela clique em Salvar

Será criada uma linha parecida com essa abaixo:

SENDER ENVELOPE EMPTY	SA_RULES	Pontuação: 1

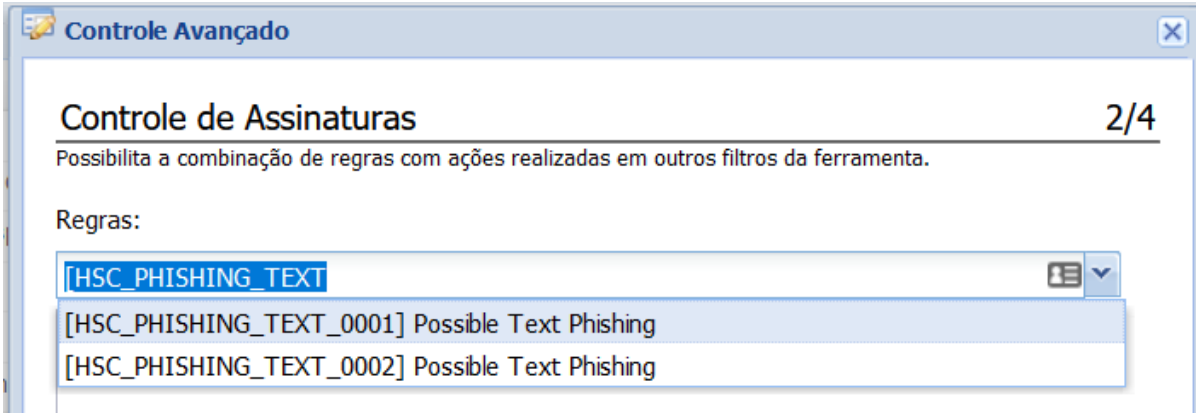
2. Clique em Adicionar (+)

Selecione a Regra por Controle de Assinaturas



A segunda regra que vamos fazer é para detectar o texto phishing no corpo da mensagem

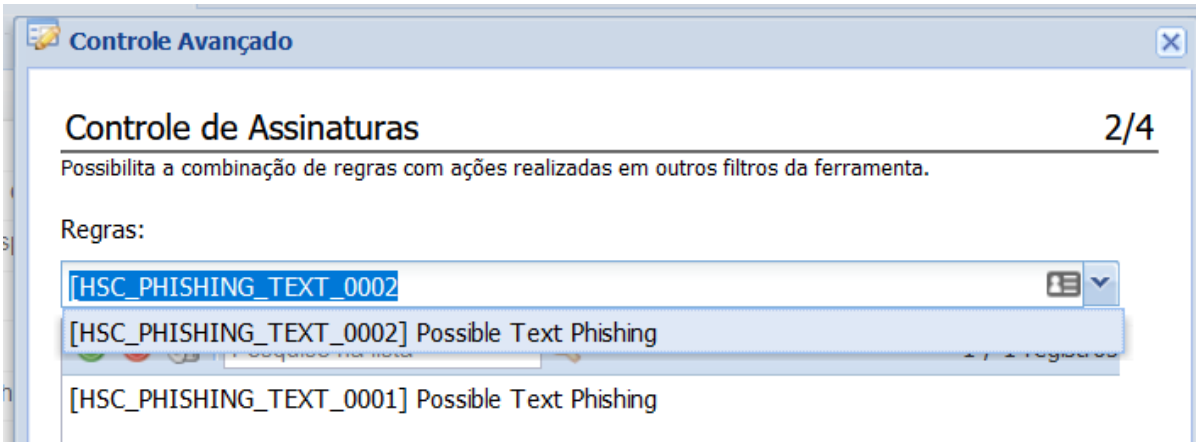
Indicado pela regra: [HSC_PHISHING_TEXT_0001] e [HSC_PHISHING_TEXT_0002]



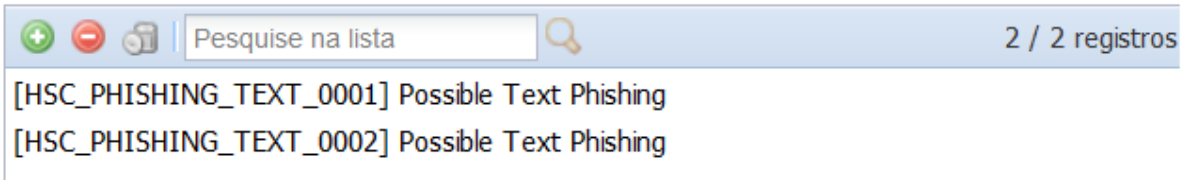
Selecione o primeiro [HSC_PHISHING_TEXT_0001]

No campo Operador Lógico, mude para **OU**

Agora inclua a outra assinatura de texto phishing [HSC_PHISHING_TEXT_0002]

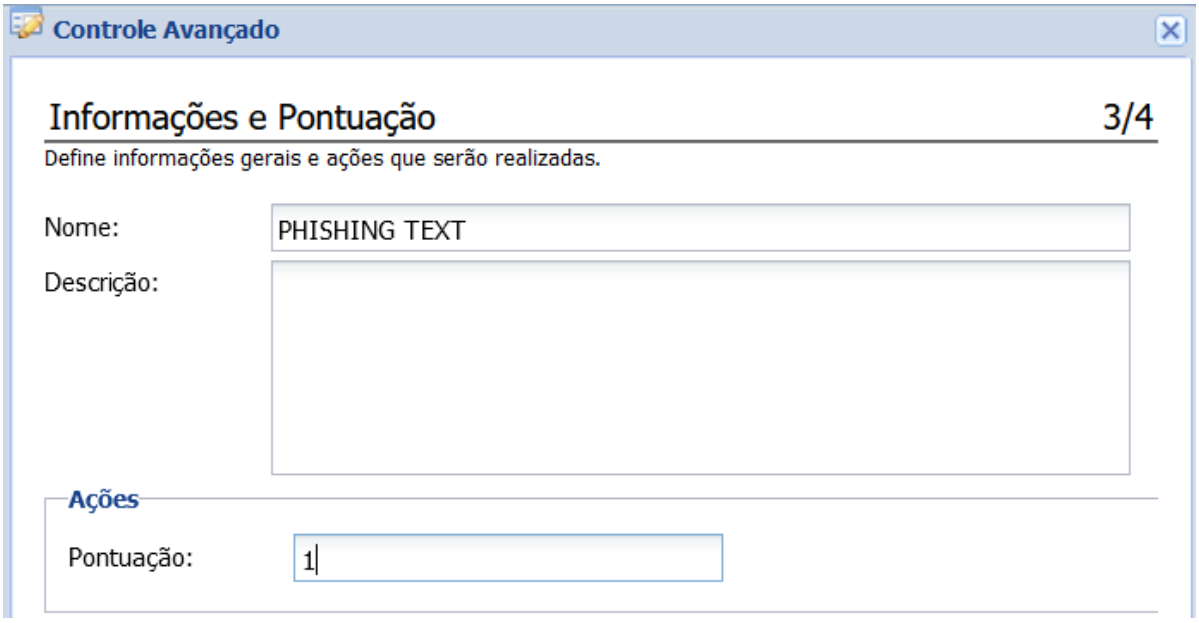


Ao incluir a segunda assinatura, deve ficar algo parecido com:



Clique em Avançar

Dê um nome para a regra e uma pontuação qualquer



Clique em Avançar e na próxima tela Clique em Salvar

Será criada uma nova linha no Controle Avançado parecido com:

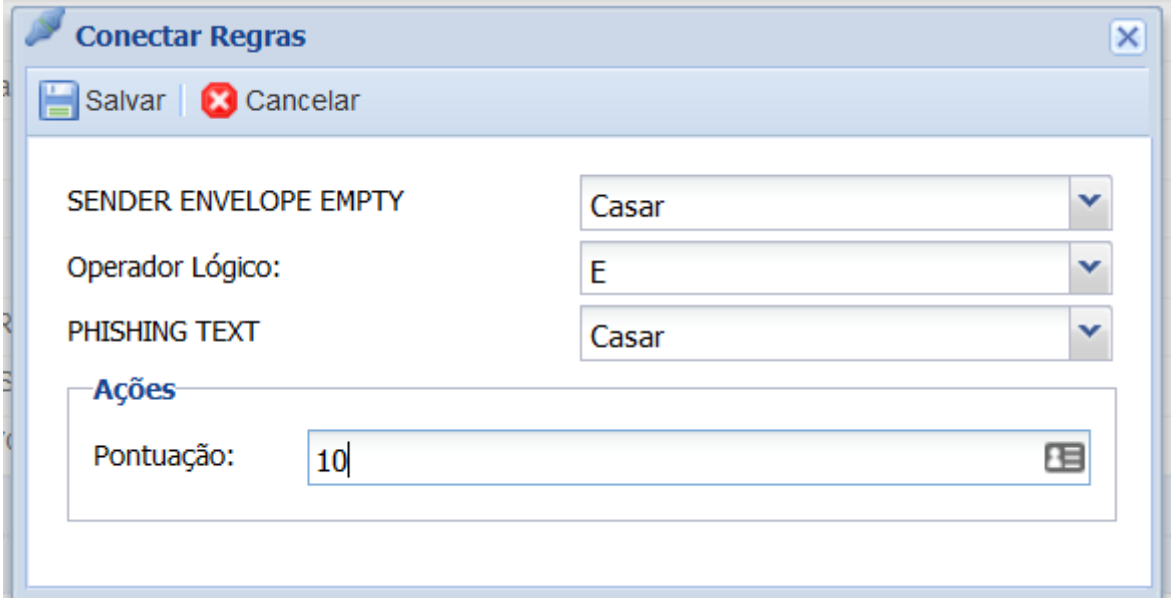
PHISHING TEXT	SA_RULES	Pontuação: 1

3. Selecione as duas regras criadas

☑	39	SENDER ENVELOPE EMPTY	SA_RULES	Pontuação: 1
☑	40	PHISHING TEXT	SA_RULES	Pontuação: 1

Clique no botão Conectar

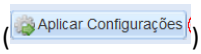
Aponte a pontuação desejada, que no nosso exemplo é 10



Clique em Salvar

Deve aparecer as duas regras casadas em uma única linha, parecida com:

(SENDER ENVELOPE EMPTY) **E** (PHISHING TEXT) (SA_RULES) **E** (SA_RULES) Pontuação: 10

Clique no botão em Aplicar Configurações (

) na parte superior do MailInspector e aplique as regras, para que esse controle avançado (aumenta a pontuação em 10), seja válido.

Regra para contar número de remetentes

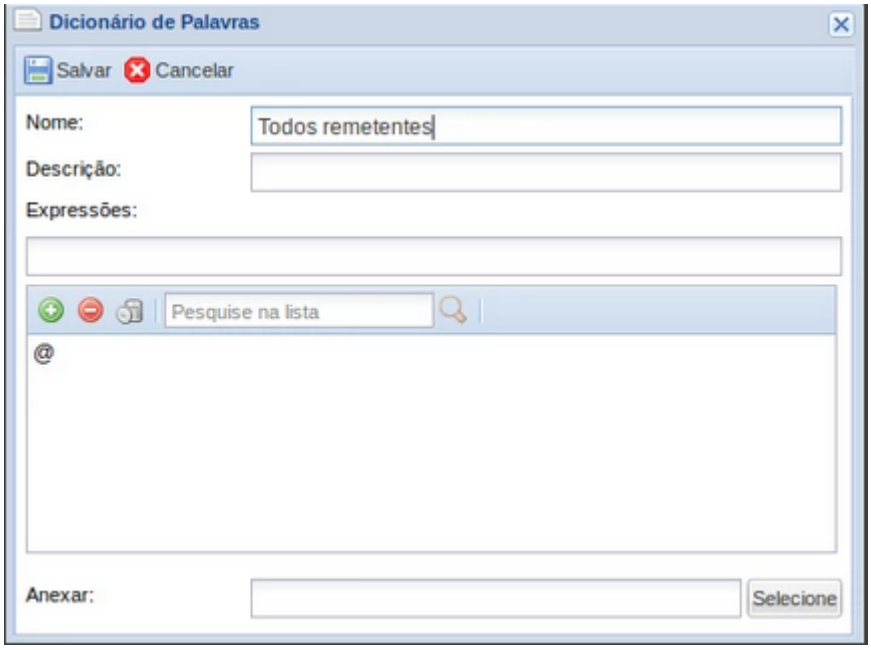
Lógica aplicada:

1. Criar um dicionário de palavras com caracter contador (no caso será o **@** já que é um caracter comum presente nos e-mails).

2. Fazer a regra de contagem de e-mails.

Criando a regra:

Primeiramente, temos que criar um Dicionário de palavras conforme o passo abaixo. Clique em Configurações > Dicionário de palavras > Adicionar.



Clique em salvar. Pronto, criado o dicionário de palavras.

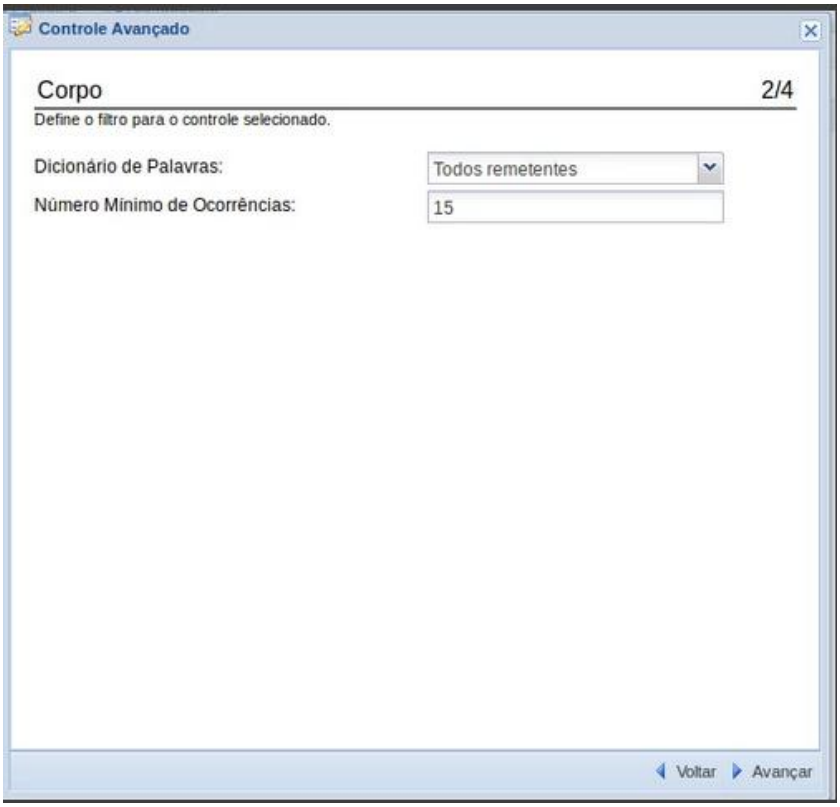
Agora vmos fazer a regra no E-mail Compliance.

Clique em Configurações > E-mail compliance > Regras > Adicionar.

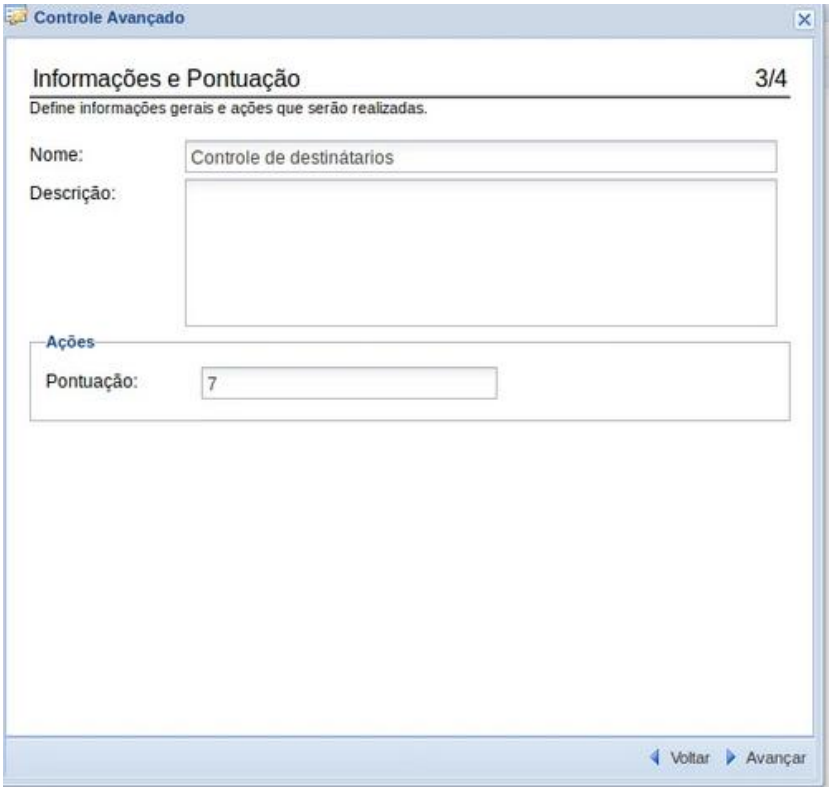
Siga os passos a seguir:

1- Escolha controle avançado de CORPO;

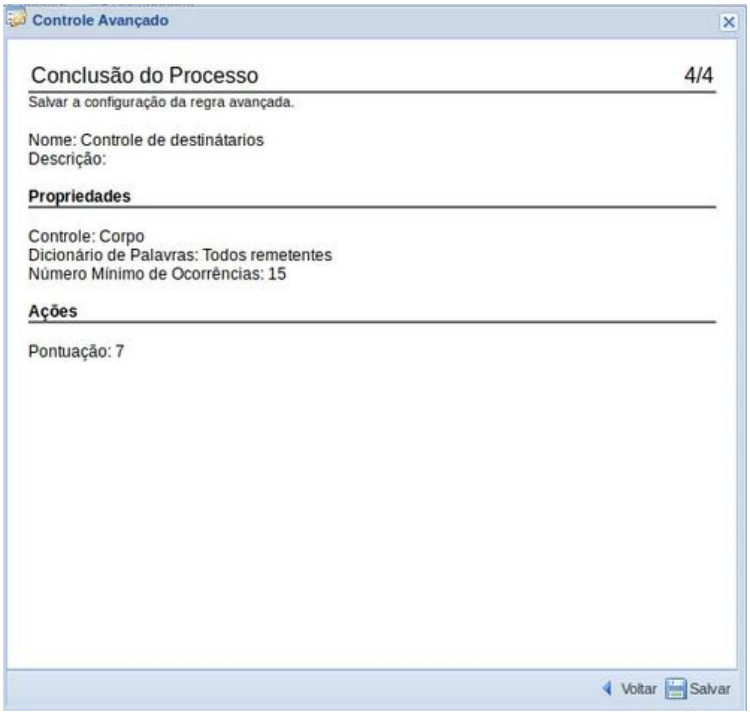
2- Como exemplo, o filtro a seguir irá buscar 15 destinatários:



Quando tiver 15 ou mais destinatários, irá pontuar em 7 pontos:



Confirmando a regra:



Clique em Salvar

Por último, na parte superior do MailInspector, clique no botão em Aplicar Configurações

Aumentar a pontuação dos e-mails que possuem palavras de conotação de BitCoin no corpo

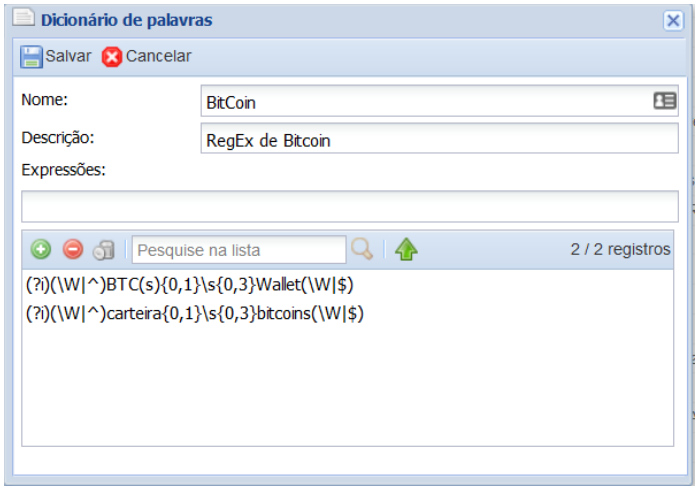
Muitos e-mails que chegam com ameaças, possuem conotação de bitcoin no corpo do e-mail. Neste HowTo faremos a criação de dicionário de palavras, ao qual detectará no corpo do e-mail palavras referentes a bitcoin.

Para esse processo, primeiramente, vá em Configurações > Cadastros > Dicionário de Palavras

Clique em Adicionar e crie o dicionário com as seguintes expressões:

(?i)(\W|^)BTC(s){0,1}\s{0,3}Wallet(\W|$)

(?i)(\W|^)carteira{0,1}\s{0,3}bitcoins(\W|$)



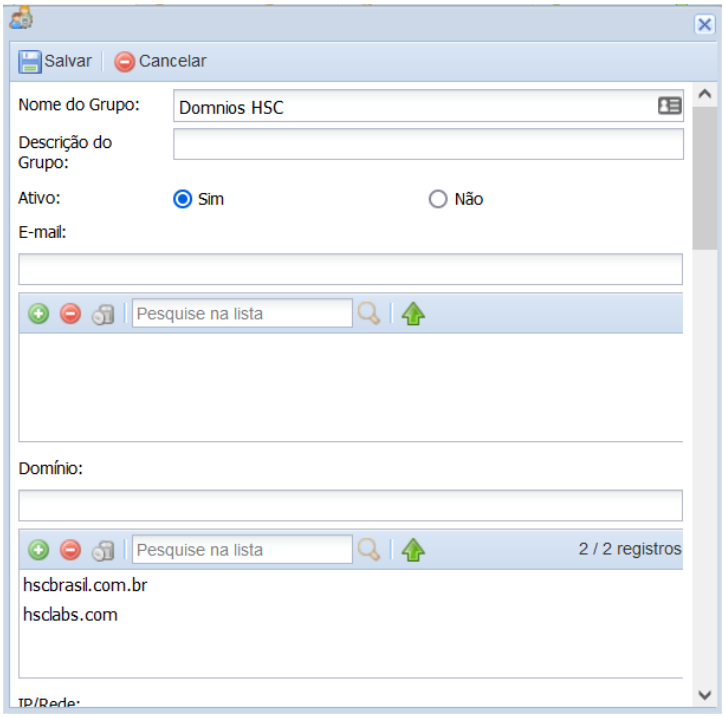
Clique em Salvar

Agora iremos criar um grupo de domínios que você deseja proteger destas palavras. Vá em Configurações > Cadastros > Grupos de Usuários

Clique em Adicionar

Agora coloque um nome para o grupo e na parte de domínios, basta você adicionar os domínios que você quer que sejam protegidas com a verificação de conotação de bitcoins no corpo do e-mail.

No exemplo, vamos criar um grupo chamado Domínios HSC e colocar nos domínios os domínios a serem protegidos.



Clique em Salvar.

Vamos criar duas regras e depois casar as duas regras:

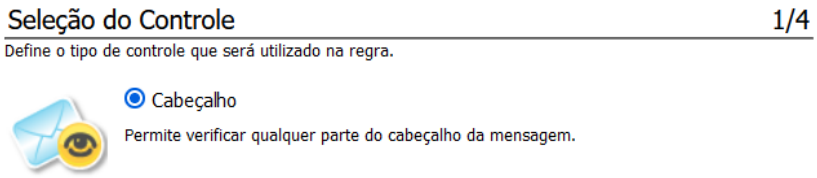
1. Regra de cabeçalho, onde irá verificar o destino para aquele grupo de domínios a serem protegidos;
2. Regra de verificação do corpo da mensagem contendo referência a bitcoin;

Depois das duas regras criadas, vamos casá-las e colocar para aumentar a pontuação em 4 pontos.

Vá em Configurações > Filtros de SPAM > Controle Avançado

Clique em Adicionar

Selecione a opção cabeçalho



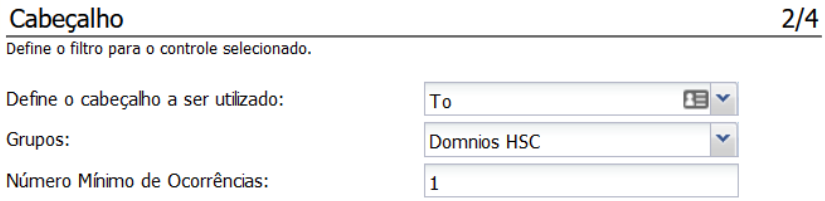
Clique em Avançar

Preencha conforme imagem a seguir.

O cabeçalho é o **To**

Nos grupos, selecione o grupo que você criou anteriormente. No nosso exemplo é o grupo Domínios HSC.

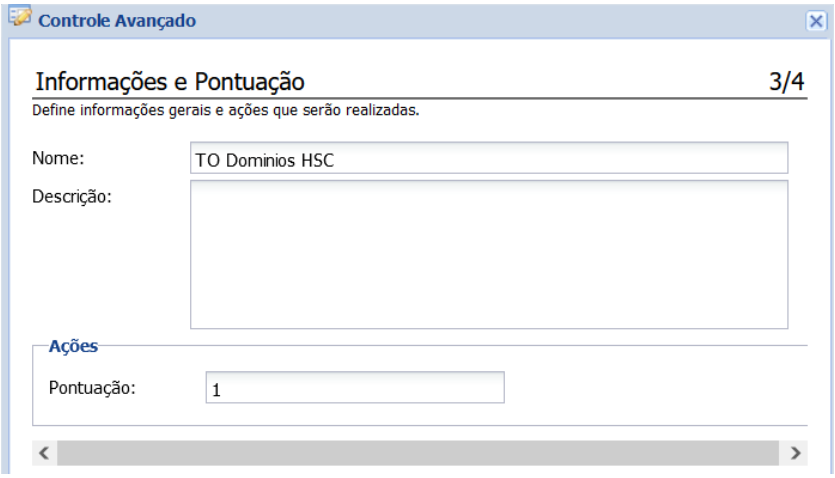
Em número de ocorrências, preencha com **1**



Clique em Avançar

No nome, coloque um nome de fácil correlação com a regra que você está criando. No exemplo, vou colocar o nome de: TO Domínios HSC

Na pontuação, pode colocar 1

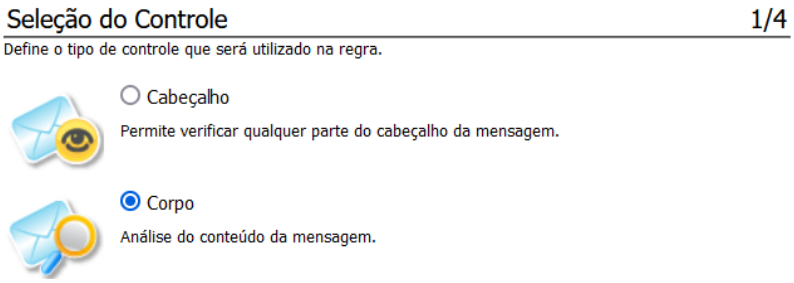


Clique em Avançar e depois em Salvar

Agora vamos fazer a segunda parte, que é a segunda regra, para que depois possamos casar as duas regras.

Novamente em Configurações > Filtros de SPAM > Controle Avançado, clique em Adicionar

Dessa vez, será uma regra para o Corpo da mensagem.



Clique em Avançar (depois de selecionado Corpo)

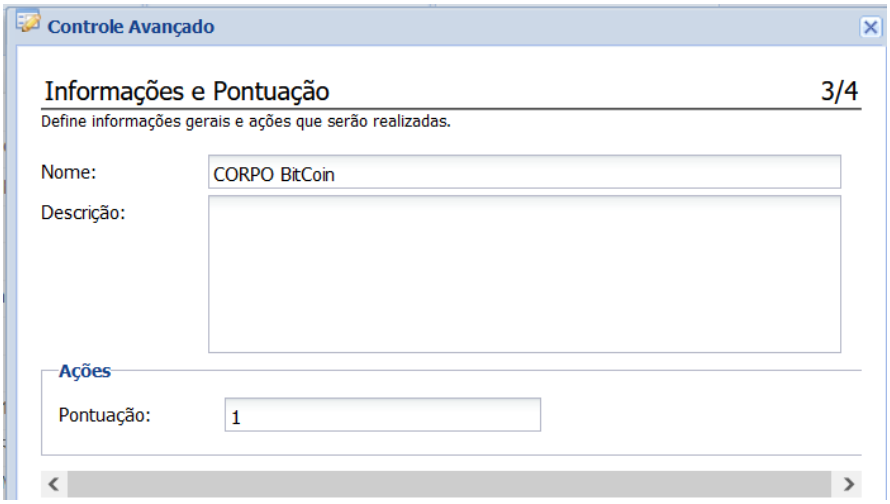
No dicionário de palavras, selecione o dicionário que você criou com referência a bitcoin.

Em número de ocorrências, coloque 1

Clique em Avançar

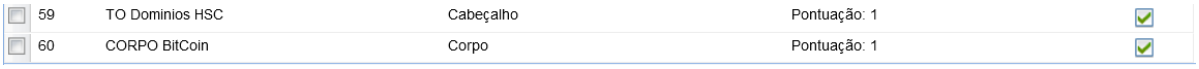
No nome, coloque um nome de fácil referência. No exemplo, colocarei CORPO BitCoin

Em Pontuação, coloque 1



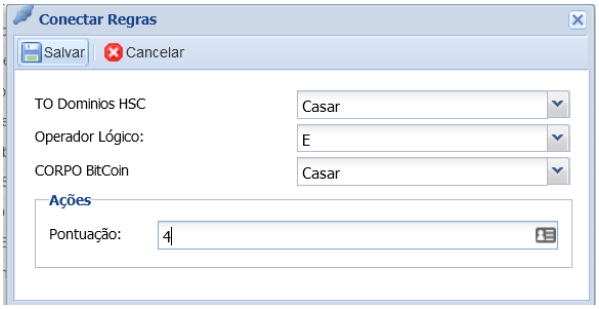
Clique em Avançar e depois em Salvar

Observando as regras de Controle Avançado, você deve verificar que tem as duas regras criadas



Selecione as duas regas e clique em Conectar

Deve abrir uma janela parecida com a imagem a seguir



Mude a pontuação para 4 e verifique que estejam em Casar E Casar

Clique em Salvar

Deve aparecer algo parecido com:

(TO Dominios HSC) **E** (CORPO BitCoin)	(Cabeçalho) **E** (Corpo)	Pontuação: 4

Por último clique em Aplicar Configurações (para que a regra entre em ação)

Proteção a VIP (Very Important Person) e Look-aLike Domains

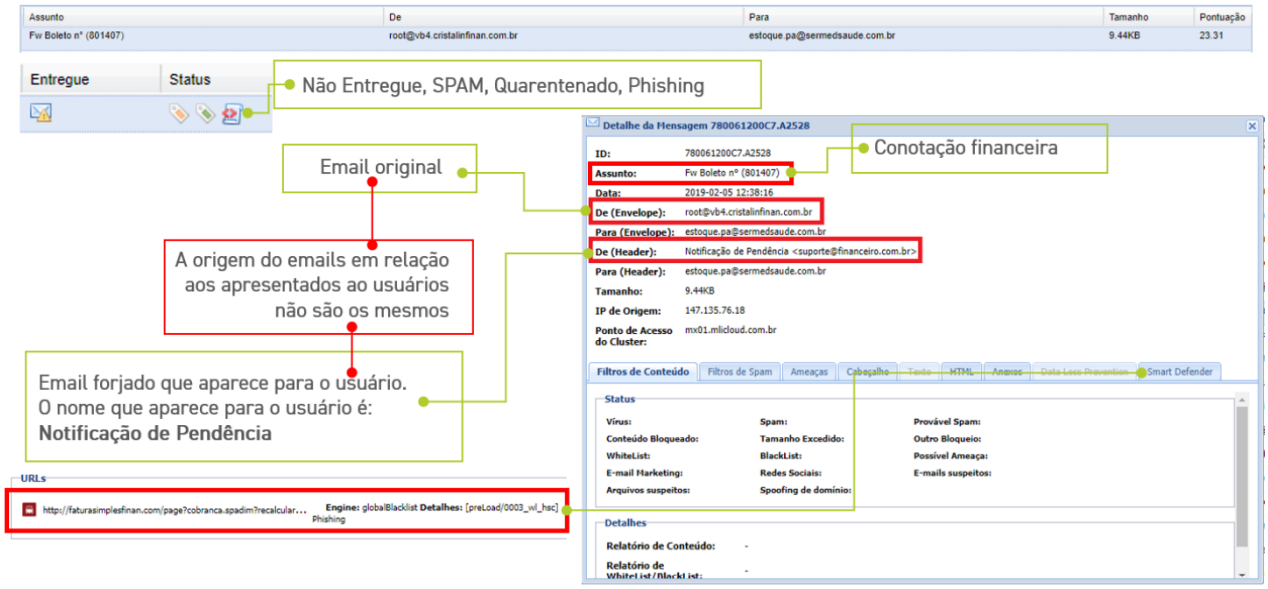
Configuração de uso com proteção a VIP (Very Important Person)

Essa proteção se dá a nível de Display Name, uma vez que o criminoso não tem acesso ao Display Name correto utilizado pela empresa e com isso, acaba colocando um Display Name **similar ao original**.

Passo-a-passo

1. Criar um dicionário de palavras chamado Display Name e incluir o Display Name dos Diretores nesta lista.
2. Criar um grupo de usuários chamado Diretoria e incluir os e-mails deles nesta lista.
3. Crie regra de SPAM.
4. Crie regra de Display Name.
5. Case as regras e ajuste a pontuação necessária

Características de Fraude de E-mail



1. Criação de Display Name customizados

Configurações > Cadastro > Dicionário de Palavras

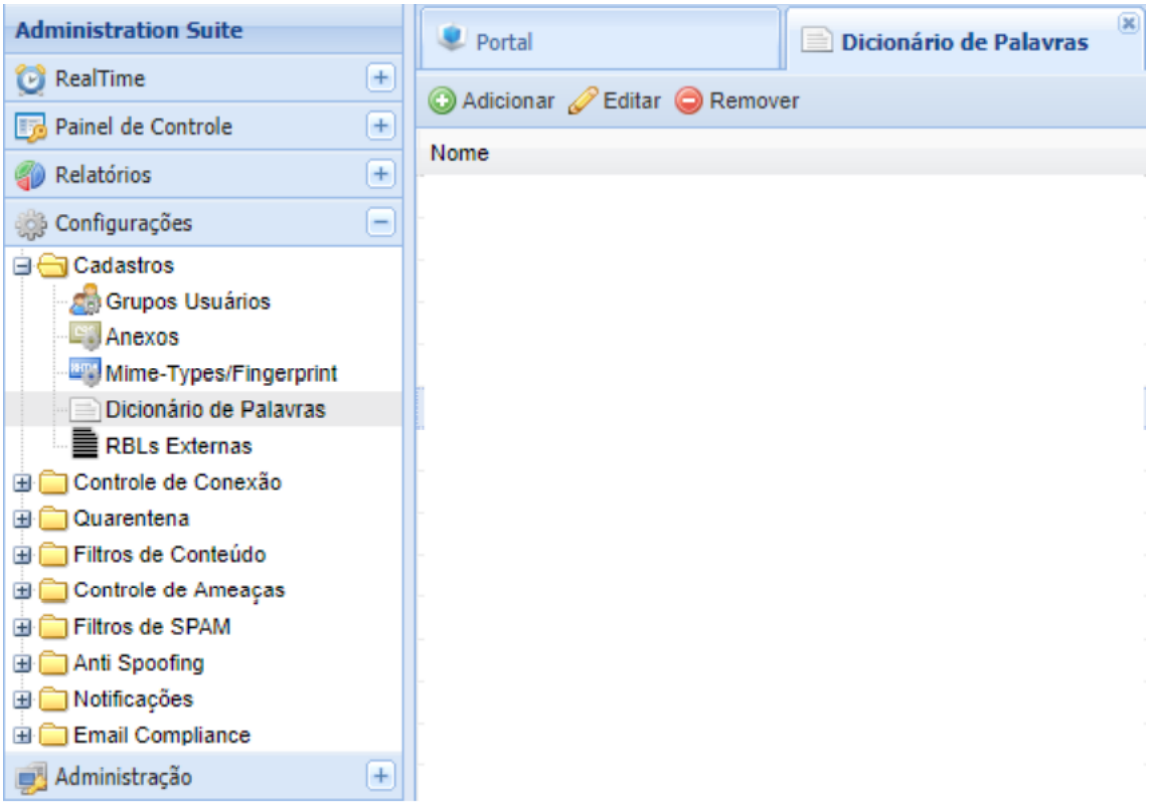
Clique em Adicionar

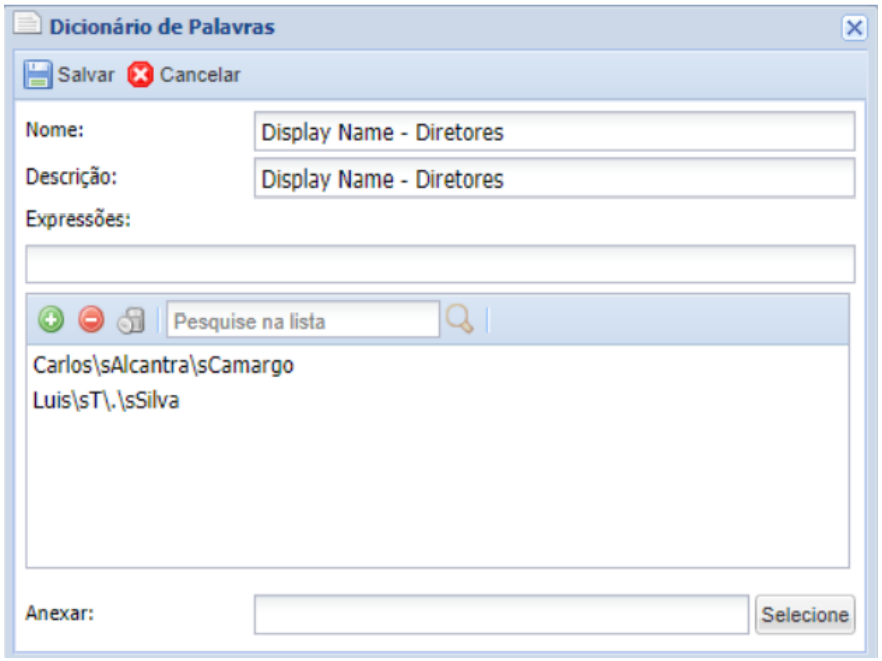
Insira no nome do Dicionário (no exemplo foi **Display Name - Diretores**), descrição as expressões regulares que comporiam o Display Name.

Obs: Não esqueça de clicar em + para incluir a Expressão na lista.

No exemplo, vamos considerar 2 diretores:

- Carlos Alcantra Camargo
- Luis T. Silva





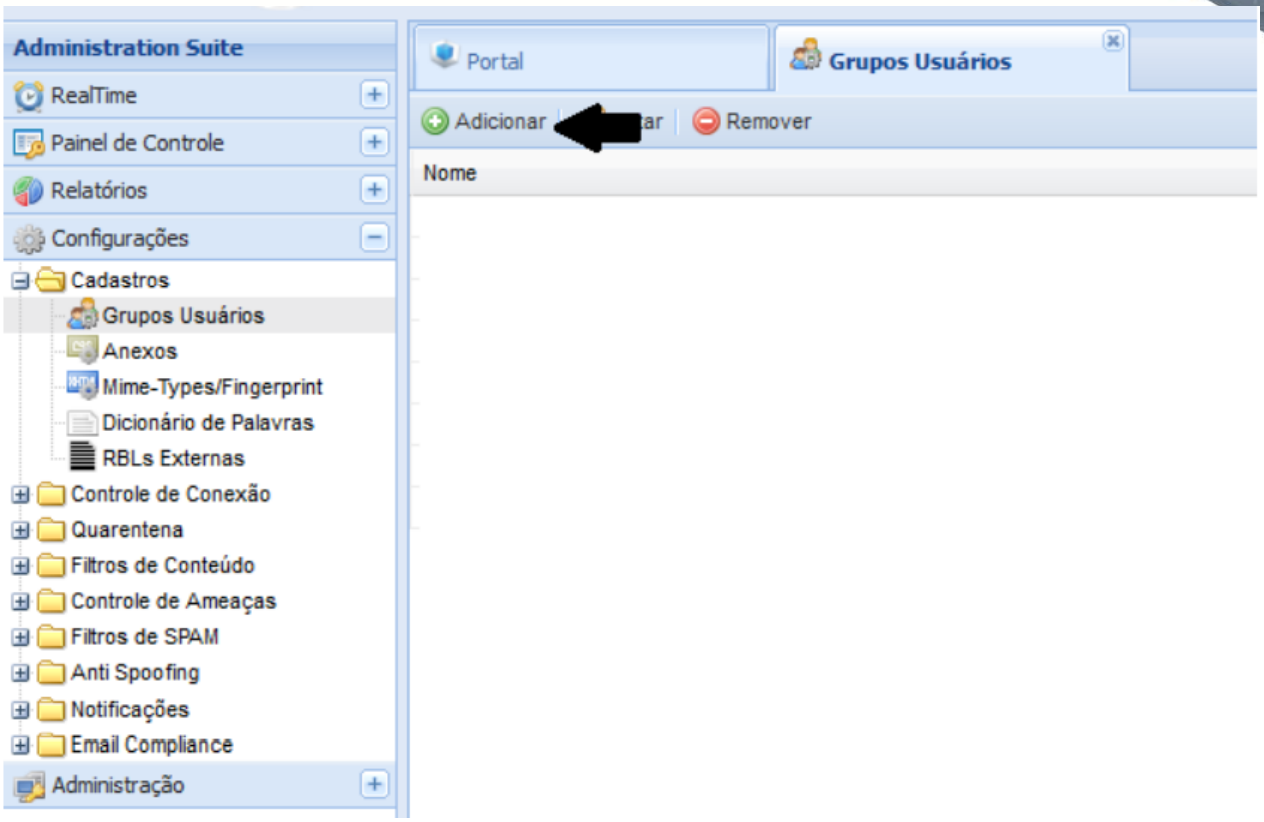
Após inserida toda as **expressões regulares**, clique em Salvar.

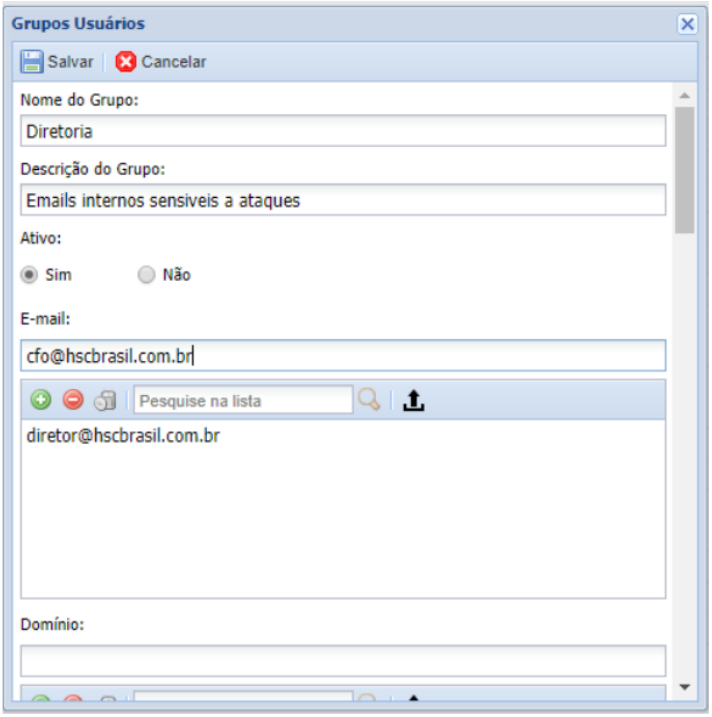
2. Criação de Grupo de E-mails dos Diretores

Configurações > Cadastro > Grupo de Usuários

Clique em Adicionar Insira no nome do Grupo (no exemplo foi Diretoria), descrição e inclua neste grupo os e-mails dos diretores/e-mails sensíveis a ataques.

Obs: Não esqueça de clicar em + para incluir o e-mail na lista.


Administration Suite
RealTime
Painel de Controle
Relatórios
Configurações
Cadastros
Grupos Usuários
Anexos
Mime-Types/Fingerprint
Dicionário de Palavras
RBLs Externas
Controle de Conexão
Quarentena
Filtros de Conteúdo
Controle de Ameaças
Filtros de SPAM
Anti Spoofing
Notificações
Email Compliance
Administração
Portal
Grupos Usuários
Adicionar
Remover
Nome


Grupos Usuários
Salvar
Cancelar
Nome do Grupo:
Diretoria
Descrição do Grupo:
Emails internos sensiveis a ataques
Ativo:
Sim
Não
E-mail:
cfo@hscbrasil.com.br
Pesquise na lista
diretor@hscbrasil.com.br
Domínio:

Após inserida toda a lista de e-mail diretoria, clique em Salvar.

Regra de DLP - Diretoria

Configurações > E-mail Compliance > Regras

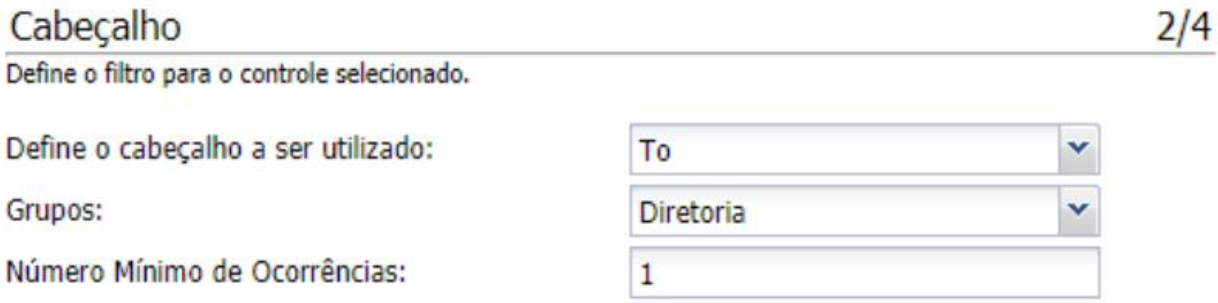
Clique em Adicionar

Seleção de Controle: Cabeçalho

Define o cabeçalho a ser utilizado: To

Grupos: Diretoria

Número Mínimo de Ocorrências: 1



Na etapa de informações e ação

Nome: Diretoria

Descrição: E-mails da diretoria e/ou sensíveis a ataques

Tipo: DLP

Ações:

- Log: Marque a opção Registrar em Log
- Notificação: Não marque nada
- Ação: Rejeitar / Deletar / Não Entregar
- Encaminhar para: Nenhum

Informações e Ações 3/4

Define informações gerais e ações que serão realizadas.

Nome: Diretoria

Descrição: Emails da diretoria e/ou sensíveis a ataques

Tipo: DLP

Ações

Log: ☑ Registrar em Log ☐ Armazenar para Auditoria

Notificação: ☐ Remetente ☐ Destinatário

Ação: ○ Entregar ◉ Rejeitar / Deletar / Não Entregar

Encaminhar para: Nenhum

Alterar assunto:

Alterar cabeçalho: Valor:

Clique em Avançar e depois de apresentado o resumo, clique em Salvar

Regra	Nome	Controle	Ação
306	Diretoria	Cabeçalho	Rejeitar / Deletar / Não Entrega, Registrar em Log

Regra de DLP – Display Name

Configurações > E-mail Compliance > Regras

Clique em Adicionar

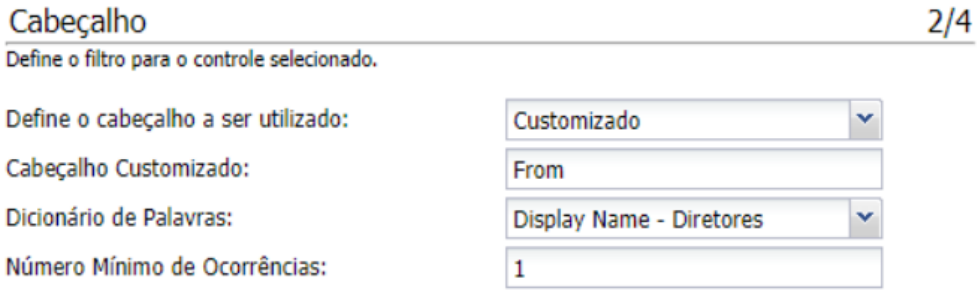
Seleção de Controle: Cabeçalho

Define o cabeçalho a ser utilizado: Customized

Cabeçalho Customizado: From

Dicionário de Palavras: Display Name - Diretores

Número Mínimo de Ocorrências: 1



Clique em Avançar

Na etapa de Informações e Ações

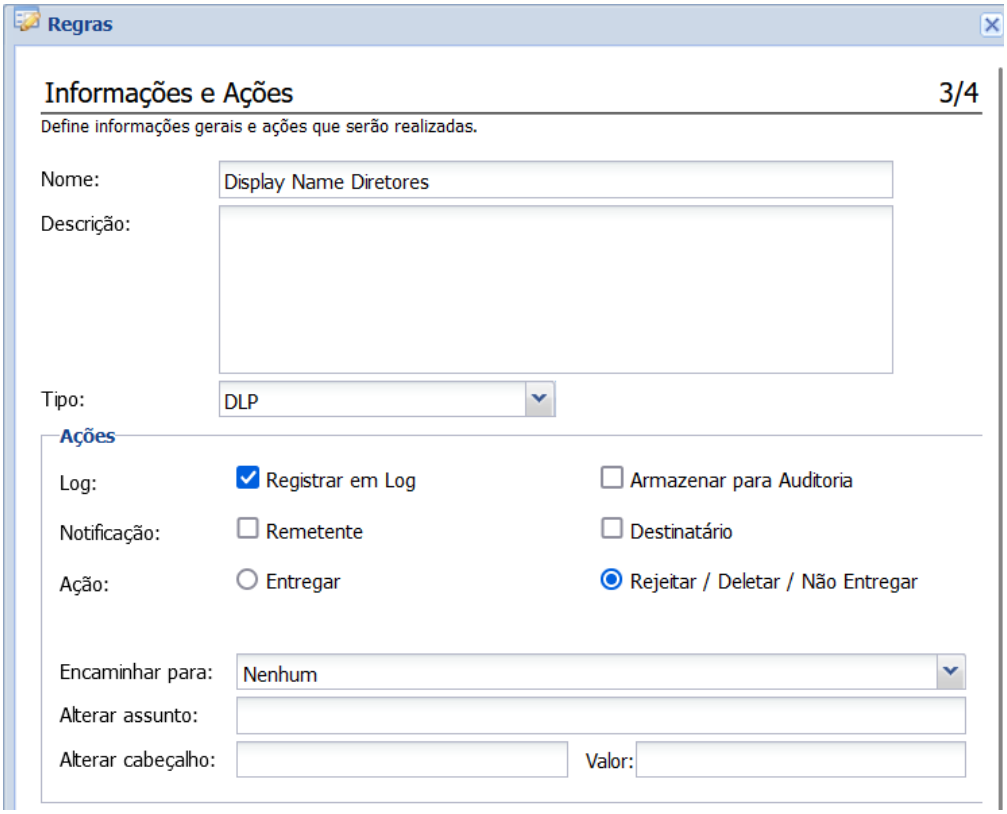
Nome: Display Name Diretores

Descrição: Nomes de Apresentação utilizados pelos diretores em Seus E-mails Profissionais

Tipo: DLP

Ações:

- Log: Marque a opção Registrar em Log
- Notificação: Não marque nada
- Ação: Rejeitar / Deletar / Não Entregar
- Encaminhar para: Nenhum



Clique em Avançar e depois de apresentado o resumo, clique em Salvar.

307	Display Name Diretores	Cabeçalho	Rejeitar / Deletar / Não Entrega, Registrar em Log

Casando as Regras

Selecione as duas regras que você criou e clique em Conectar

Regra	Nome	Controle	Ação
306	Diretoria	Cabeçalho	Rejeitar / Deletar / Não Entrega, Registrar em Log
307	Display Name Diretores	Cabeçalho	Rejeitar / Deletar / Não Entrega, Registrar em Log

Conectar

A ideia é para quando os e-mails foram para os diretores, mas o Display Name não se casar, é porque foi alguém que colocou um Display Name diferente do que é usado na empresa para aquele diretor, portanto, é e-mail forjado.

Conectar Regras:

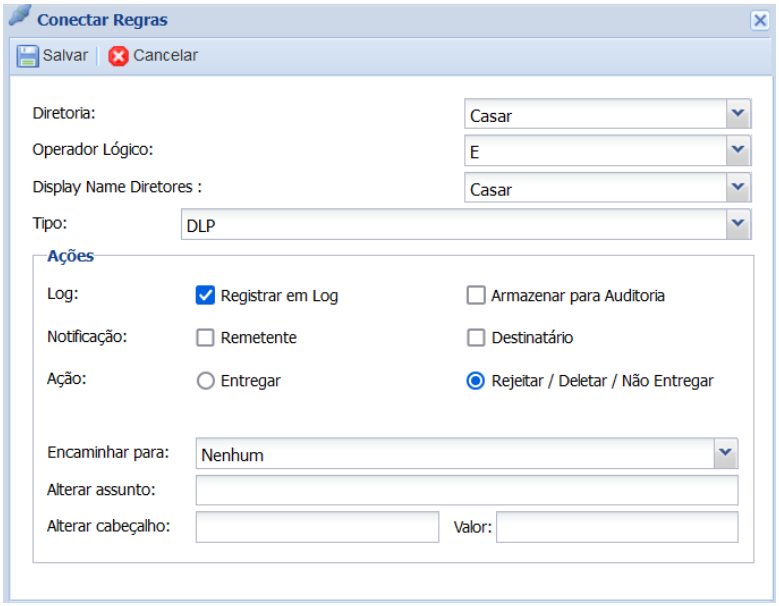
- Diretoria: Casar

- Operador Lógico: E
- Display Name Diretores: Casar
- Tipo: DLP

Ações:

- Log: Marque a opção Registrar em Log
- Notificação: Não marque nada
- Ação: Rejeitar / Deletar / Não Entregar
- Encaminhar para: Nenhum

Clique em Salvar



Regra	Nome	Controle	Ação
308	(Diretoria) **E** (Display Name Diretores)	(Cabeçalho) **E** (Cabeçalho)	Registrar em Log, Rejeitar / Deletar / Não Entregar, DLP, Encaminhar para:

Resumo da regra: O que vier destinado a Diretoria, será verificado o Display Name e caso o Display Name não case com nenhum dos nomes cadastrados pelas expressões regulares cadastradas, o sistema bloqueará o e-mail pelo DLP.

Configuração de uso com proteção a Look-alike Domains/Cousin Domains

Look-aLike Domains ou Cousin Domains é Uma técnica de ataques muito utilizada por hackers, ao qual consistem em compra de domínios “parecidos/similares” em relação ao domínio alvo.

O MailInspector consegue verificar se a origem do e-mail é similar ao domínio aplicado no remetente e ainda compara com eventual problema de SPF em relação ao domínio.

Top Violações de SPF por Domínio

DOMÍNIO	SPF HELO SOFTFAIL	SPF FAIL	SPF SOFTFAIL	TOTAL
hscbrasil.com.br	861	5.346	-	6.207

Além da proteção já mencionada, podemos utilizar o sistema de DNSTwister para verificar domínios parecidos com o domínio original.

O cousin domain ou domínios primos, também chamado de look-alike domain (também conhecidos como domínios similares), é um domínio DNS (sistema de nome de domínio) semelhante a outro nome quando processado por um agente de usuário de e-mail (MUA).

Por exemplo, **americanas1.com** ou **americamas.com** são domínios primo de **americanas.com**.

Outros exemplos incluem erros de ortografia de um domínio, como americamas.com e americanas.com

Os domínios primos geralmente são criados como uma ferramenta de phishing para falsificar sua marca e seu nome de domínio.

No MLI existem **3 (três) formas de bloqueio** a domínios similares:

1. Bloqueio a nível de conexão;
2. Bloqueio a nível de pontuação de SPAM;
3. Bloqueio em quarentena customizada;

Em qualquer uma das formas de bloqueio, primeiramente o administrador deverá acessar o DNSTwister e verificar as variações do domínio já registradas.

No exemplo, vamos considerar o domínio HSCBRASIL.COM.BR

https://dnstwister.report/

dnstwister report

dnstwister

hscbrasil.com.br

new search

SHOW UNRESOLVED DOMAINS

export: json csv

Tweak	Type	IP	Tools
hscbrasil.com.br	Original*	68.66.216.19	analyse
iscbrasil.com.br	Bitsquatting	165.160.15.20	analyse
hsecbrasil.com.br	Insertion	177.11.54.112	analyse
scbrasil.com.br	Omission	108.167.132.144	analyse
hsbrasil.com.br	Omission	67.23.238.82	analyse
hcbrasil.com.br	Omission	45.79.161.146	analyse
hdcbrasil.com.br	Replacement	177.67.118.70	analyse
bscbrasil.com.br	Replacement	177.185.194.97	analyse

Então temos os domínios variantes:

- icsbrasil.com.br
- hsebrasil.com.br
- hdcbrasil.com.br
- scbrasil.com.br
- scbrasil.com.br
- hscbrasil.com.br

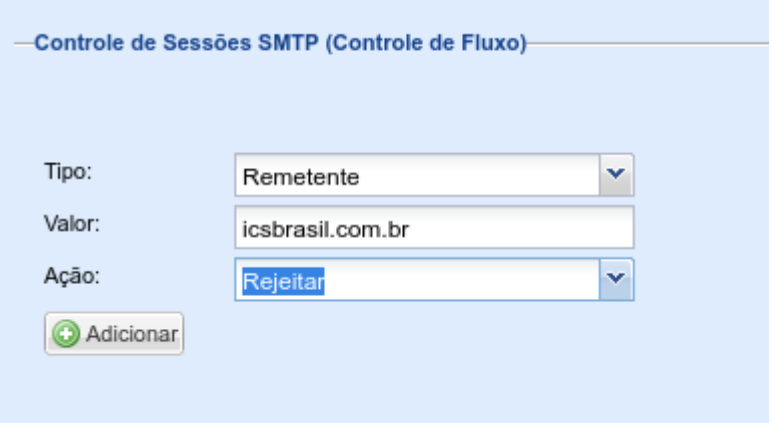
É possível também verificar os domínios que ainda não foram registrados (possíveis domínios similares), para isso, basta clicar no botão SHOW UNRESOLVED DOMAINS.

Com as variações dos domínios em mãos, é possível bloquear os domínios similares pelas três formas anteriormente citados.

1. Bloqueando na camada de conexão

Em Configurações > Cadastros > Configurações do MTA > Filtragem

Inclua toda a lista apresentada no DNSTwister, como exemplo a seguir:



Repita o processo acima até finalizar com todos os domínios similares.

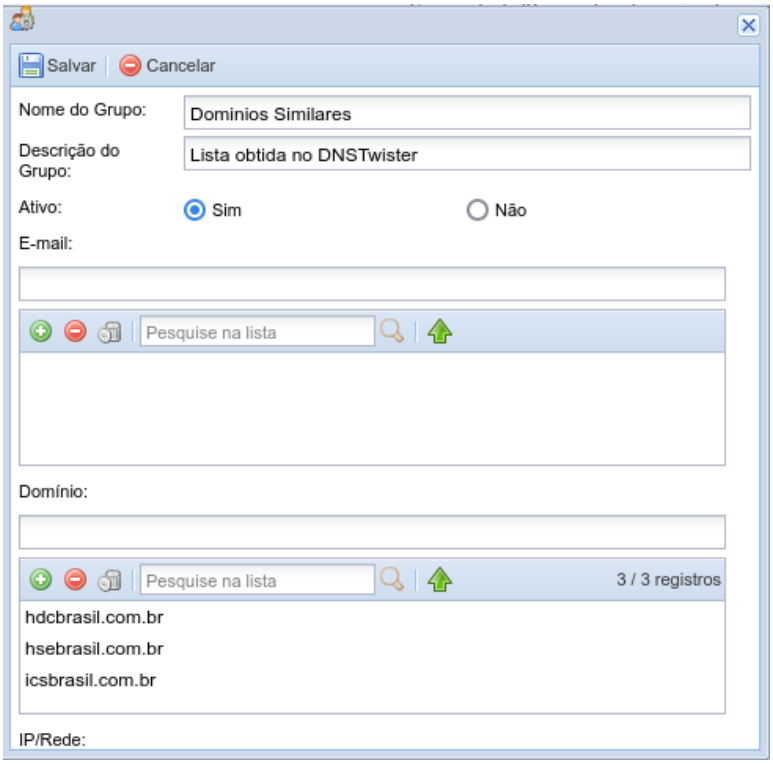
Clique em Salvar.

Clique em Aplicar Configurações.

2. Bloqueando na camada de SPAM

Em Configurações > Cadastros > Grupos de Usuários

Crie um Grupo de usuários (domínios), com toda a lista dos domínios similares indicados pelo DNSTwister, conforme imagem a seguir:



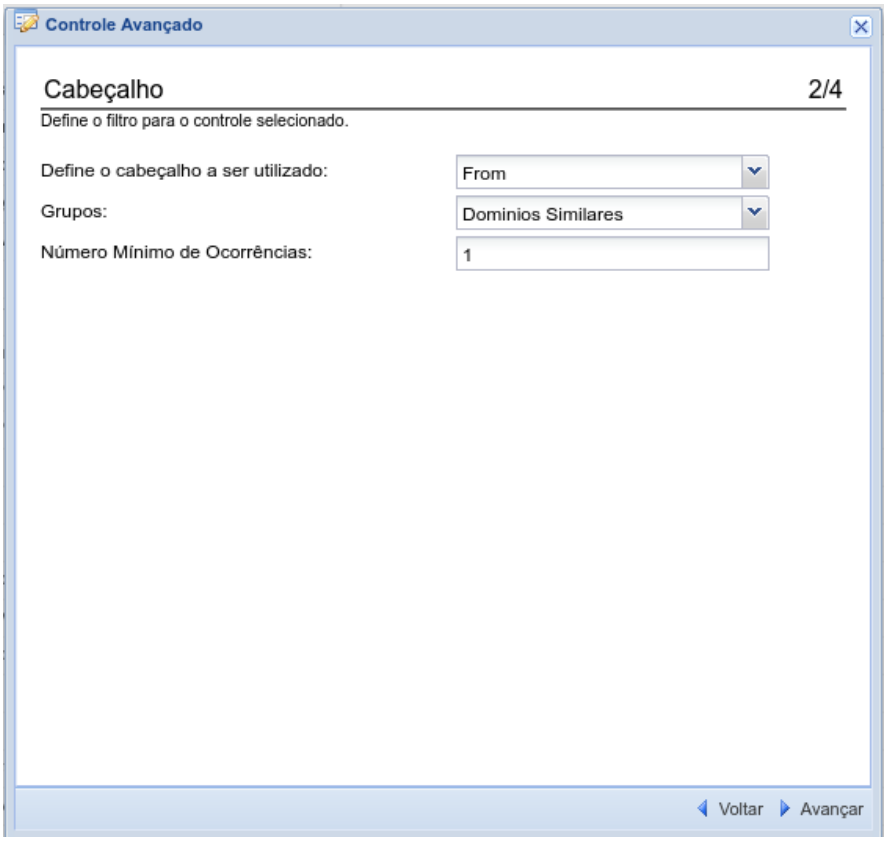
Clique em Salvar

Depois vá em: Configurações > Filtros de SPAM > Controle Avançado

Clique em Adicionar

Regras do Controle Avançado:

- Seleção de Controle: Cabeçalho
- Clique em Avançar
- Define o Cabeçalho a Ser Utilizado: From
- Grupos: Domínios Similares
- Número Mínimo de Ocorrências: 1



Clique em Avançar

Nome: Domínios Similares

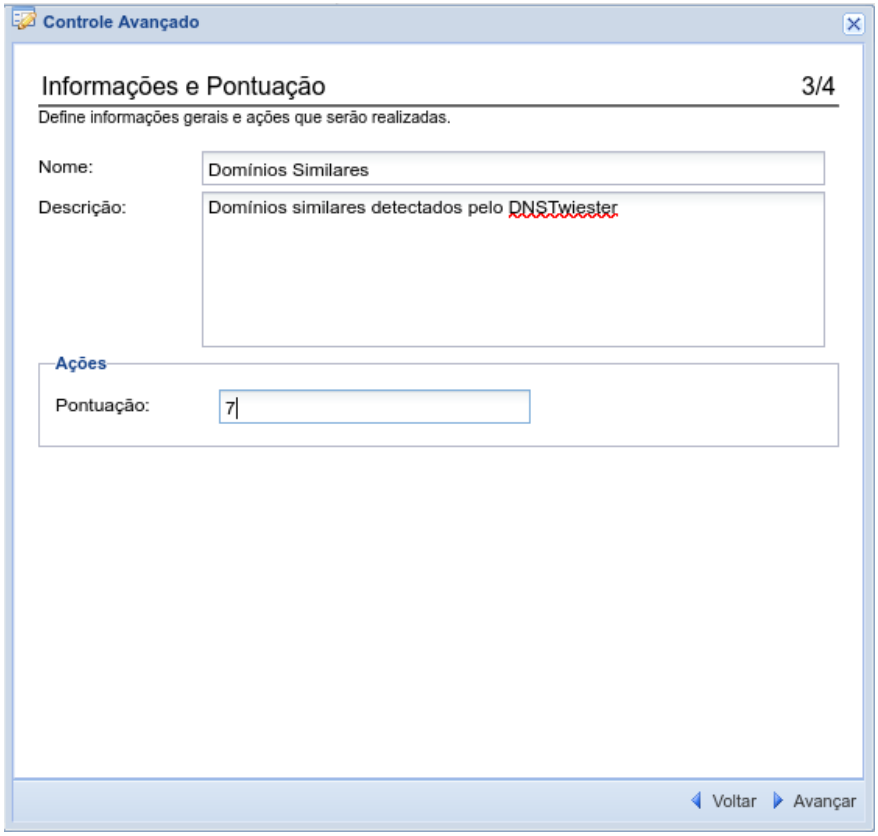
Descrição: Domínios similares detectados pelo DNSTwiester

Pontuação: 7

Clique em Avançar

Clique em Salvar

Clique em Aplicar Configurações



3. Quarentena Customizada

Em Configurações > Quarentena > Customizada

Clique em Adicionar

Nome: Domínio similar

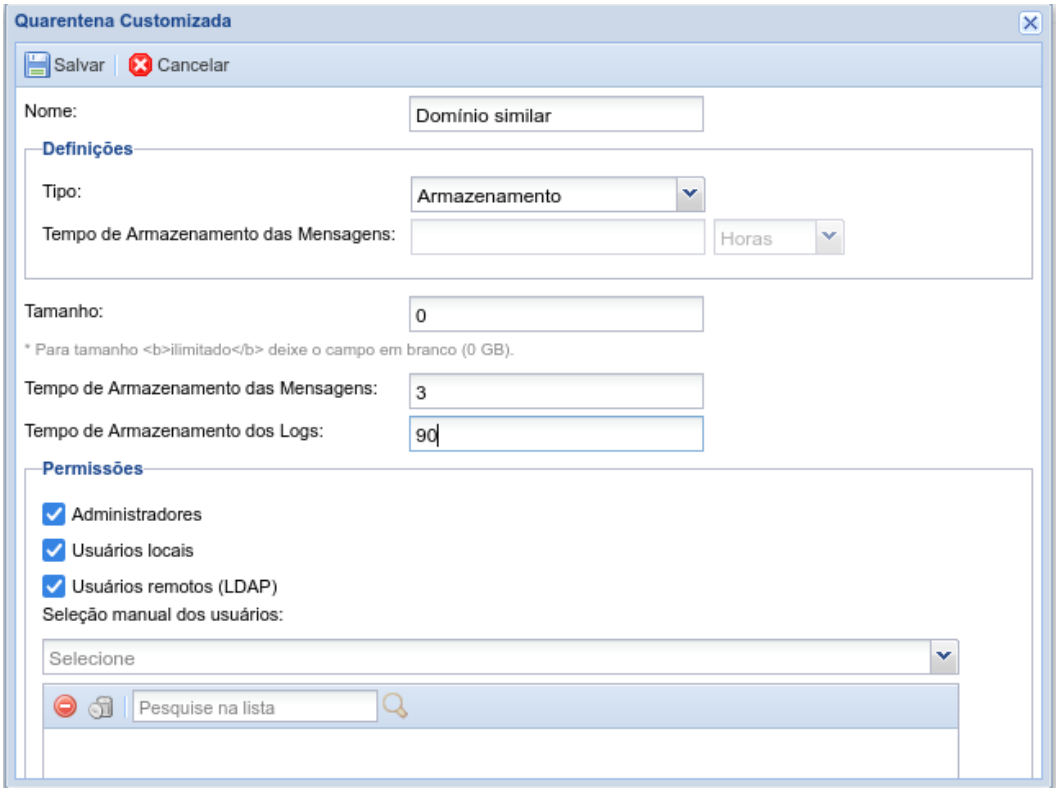
Tipo: Armazenamento

Tamanho: 0

Tempo de Armazenamento de Mensagens: 3

Tempo de Armazenamento dos Logs: 90

Clique em Salvar



Em Configurações > E-mail Compliance > Regras

Clique em Adicionar

Seleção de Controle: Cabeçalho

Define o cabeçalho a ser utilizado: From

Grupos: Domínio Similar

Número Mínimo de Ocorrências: 1

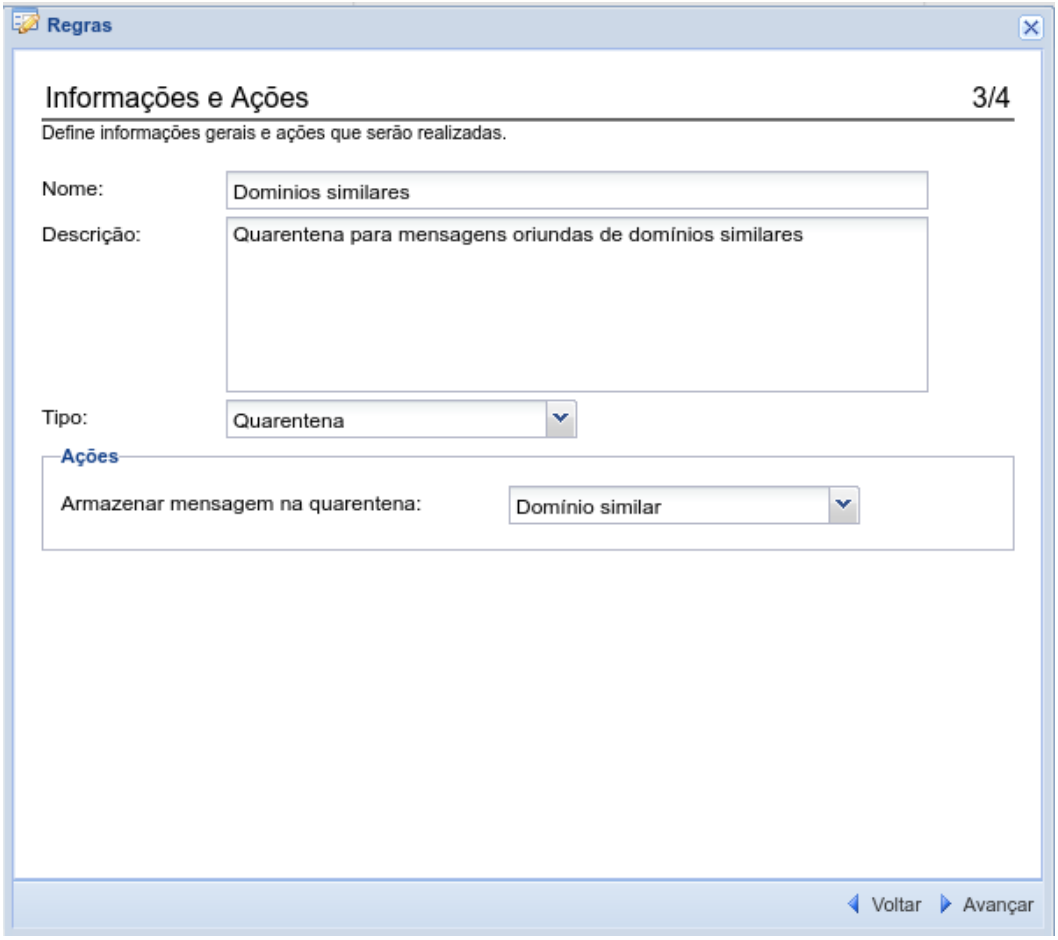
Clique em Avançar

Nome: Domínios similares

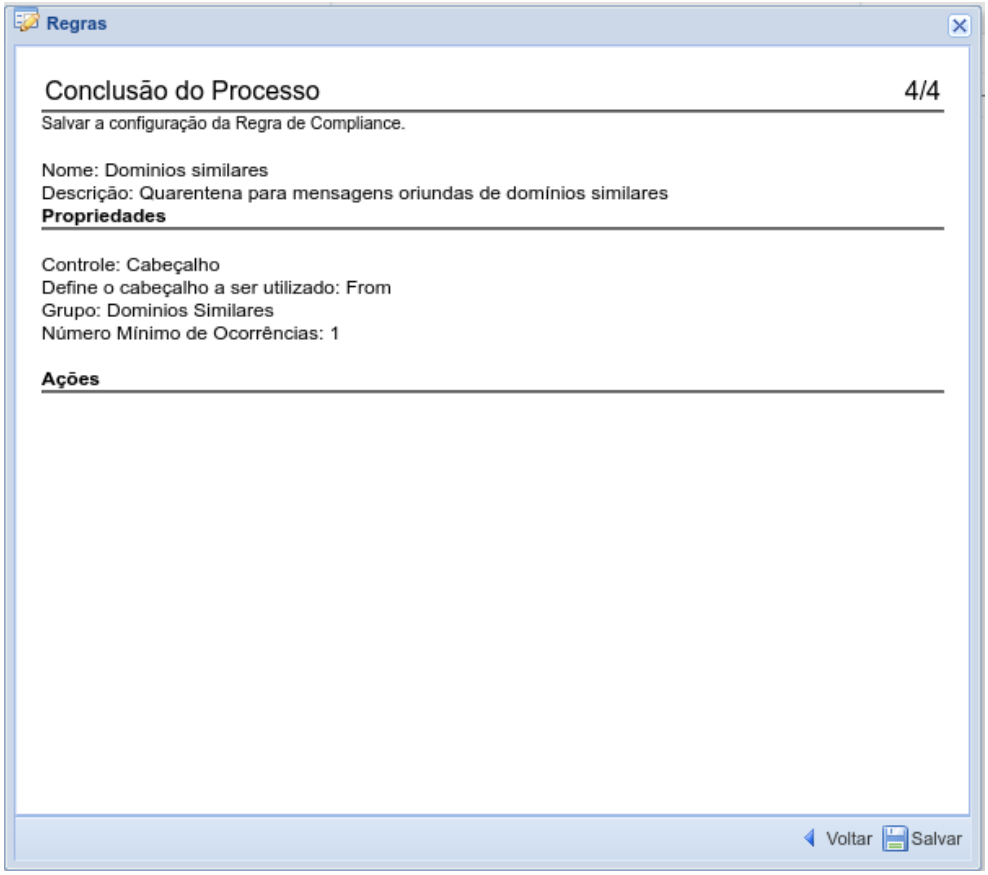
Descrição: Domínios similares

Tipo: Quarentena

Armazenar na Quarentena: Domínio similar



Clique em Avançar



Por último, clique em Salvar e depois em Aplicar Configurações.

Ativação de Sincronismo com Azure e do M-SOAR para Office 365

O modulo do Mail Inspector chamado de M-SOAR permite que os Administradores interajam nas mensagens entregues para o ambiente da Microsoft 365, permitindo assim, ações de Take Down na mensagem, links, conteúdo e anexos, posterior a entrega da mensagem.

O procedimento a seguir ensina como ativar o Modulo M-SOARD do Mail Inspector no Microsoft 365.

Requisitos

- Possuir Conta ativa no serviço Microsoft 365 em qualquer versão
- Possuir acesso administrativo ao MailInspector Enterprise
- Versão MailInspector 5.2 On Premisses ou Enterprise Cloud
- Possuir conector de saída e entrada configurado para trabalhar com MailInspector (verificar com pessoal do suporte, caso ainda não tenha configurado)

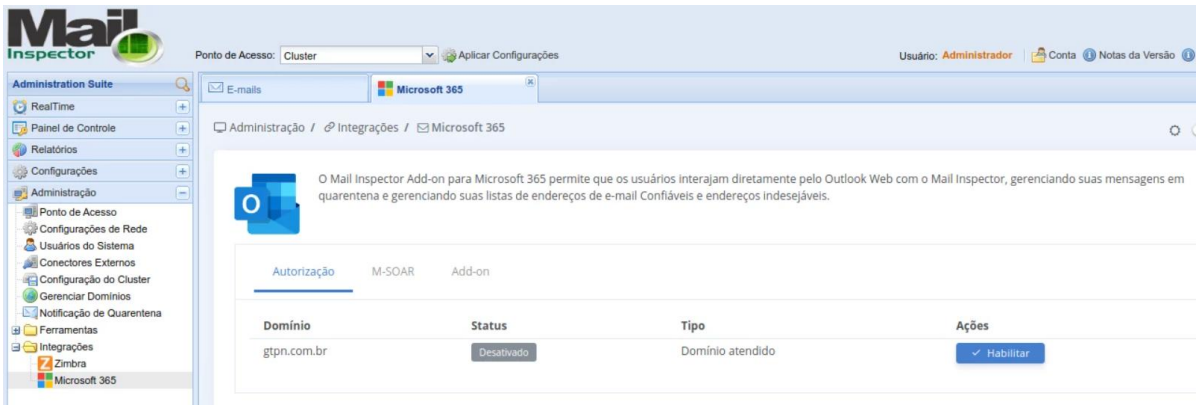
Guia Passo-a-Passo

Este guia é dividido em 2 etapas que são executadas em sequência: Autorização da Integração e Configuração das Ações de Administração do M-SOAR.

Primeira Etapa

Autorização da Integração do M-SOAR com seu domínio no serviço Microsoft 365 irá permitir ao Administrador do Mail Inspector interagir com as mensagens entregues nos serviços da Microsoft 365.

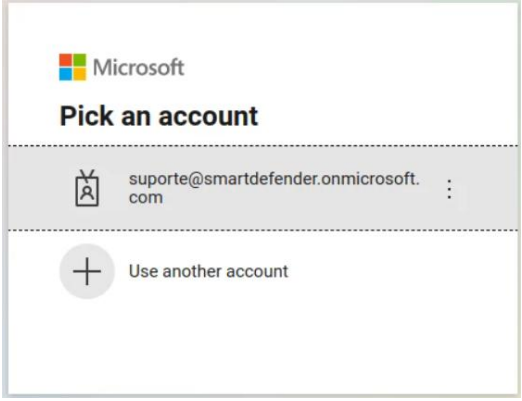
1. Acesse o Mail Inspector com privilégios administrativos e vá em Administração > Integrações > Microsoft 365



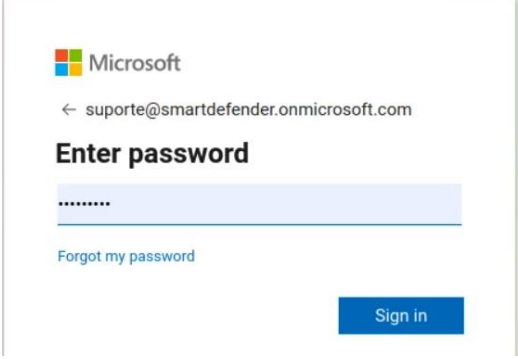
2. Serão exibidos todos os domínios protegidos pelo Mail Inspector. Escolha o domínio que deseja ativar a integração e clique em **Habilitar**.

3. Será exibido uma janela para autorizar, para isso, clique em Prosseguir

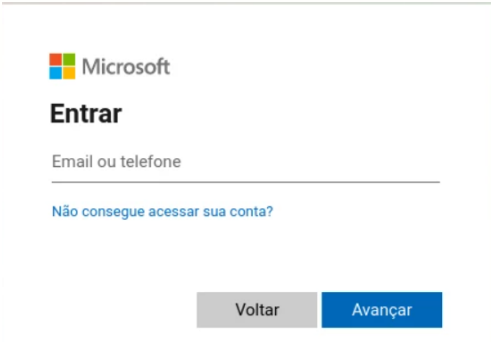
4. Na nova janela, informe as credenciais do administrador do serviço Microsoft 365



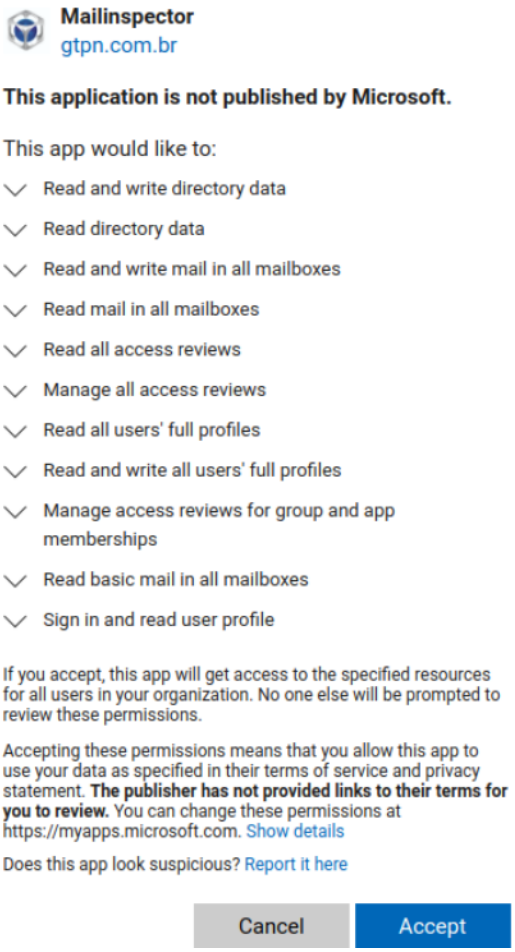
5. Informe a senha



6. Na janela que abrirá, informe as credenciais do Administrador da conta Microsoft 365



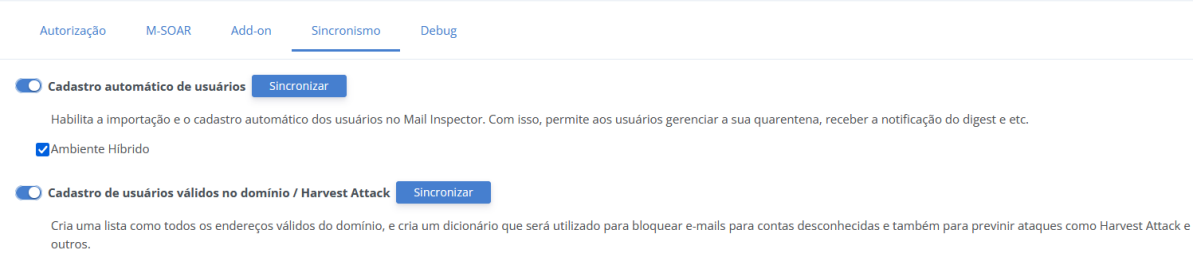
7. Confirme as permissões solicitadas



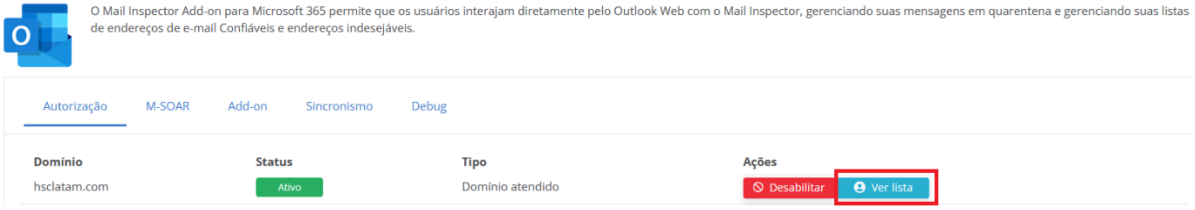
8. Em caso de sucesso será apresentada a mensagem a seguir:

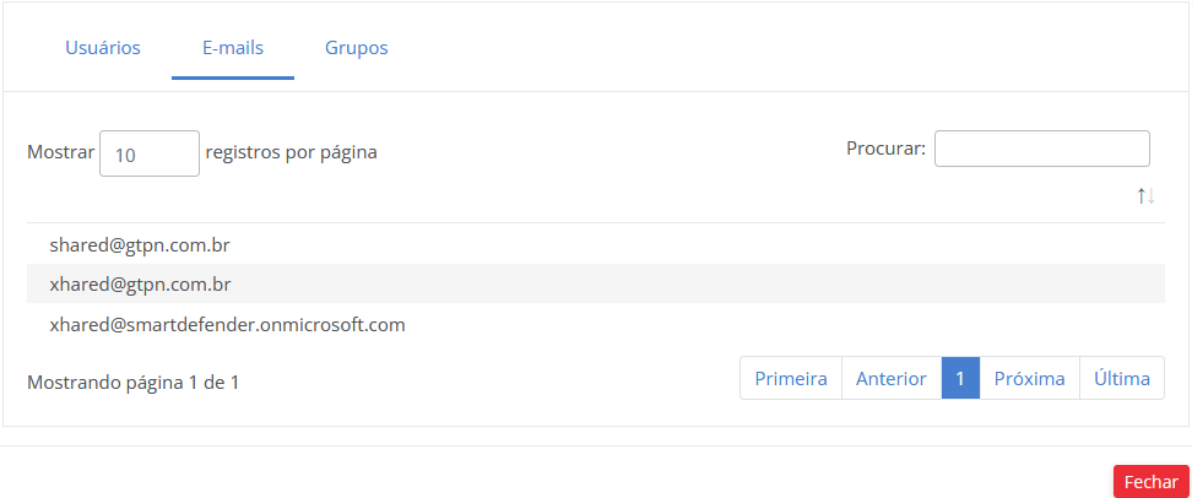
9. Em caso de falha no acesso das credenciais fornecidas, será apresentada a mensagem:
Neste caso contate o administrador da conta Microsoft 365

10. Para importar os usuários, Grupos e Lista de E-mails, clçique na aba Sincronismo
Clique em Sincronizar, tanto para Cadastro automático de usuários, quanto para Cadastro de usuários válidos no domínio/Harvest Attack



11. Para visualizar os usuários, e-mails e Grupos importados para autenticação por SSO (Single Sign-On), vá na aba Autorização e no domínio que você habilitou, clique no botão Ver Lista





Caso você queira ativar outro domínio e importar os usuários, repita o processo desde o item 1

Segunda Etapa

Configuração do M-SOAR:

Permite personalizar quais ações o Administrador do Mail Inspector poderá efetuar em tempo real na caixa de e-mail do usuário do Microsoft 365.

1. No MailInspector vá em Integrações > Microsoft 365 → M-SOAR e clique em Configurar. Logo com suas credenciais aprovadas na primeira etapa, clique em Sim, Configurar

2. Configure as ações permitidas aos administradores do Mail Inspector e personalize os rótulos para as ações que serão registrados nas mensagens afetadas na caixa do usuário do Microsoft 365. Ao final clique em Salvar alterações

Configurar domínio

Remoção de anexos da mensagem

Adicionar rótulo no assunto das mensagens afetadas

Texto do rótulo no assunto [Anexos removidos]

Remoção de links da mensagem

Adicionar rótulo no assunto da mensagem afetada

Texto do rótulo no assunto [Links removidos]

Adicionar rótulo no conteúdo da mensagem afetada

Texto do rótulo no assunto [Link removido]

Movimentação de mensagem para a pasta Lixo Eletrônico

Adicionar rótulo no assunto das mensagens afetadas

Texto do rótulo no assunto [Mensagem movida

Remoção permanente da mensagem

Bloqueio de conteúdo da mensagem

Adicionar rótulo no assunto das mensagens afetadas

Texto do rótulo no assunto [Conteúdo bloqueado]

Substituir o conteúdo original da mensagem por:

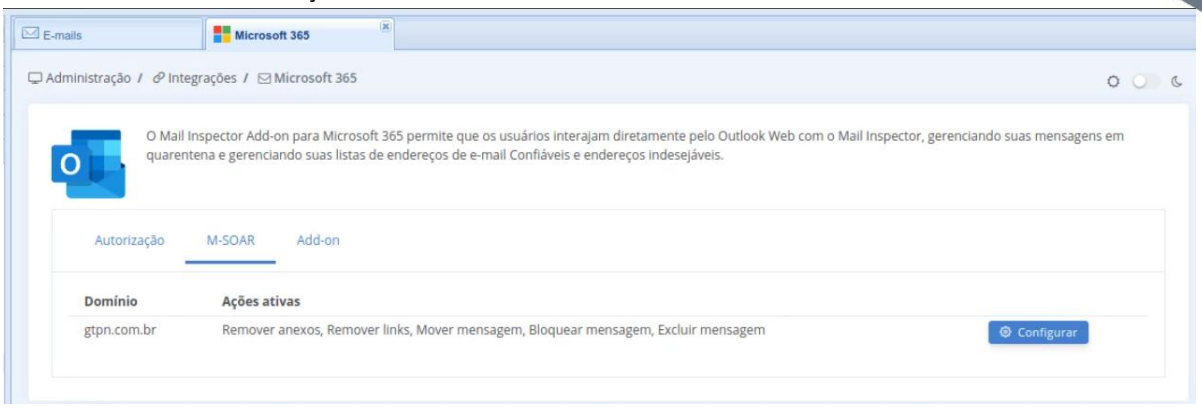
System Font 12pt

O conteúdo desta mensagem foi bloqueado pelo administrador.

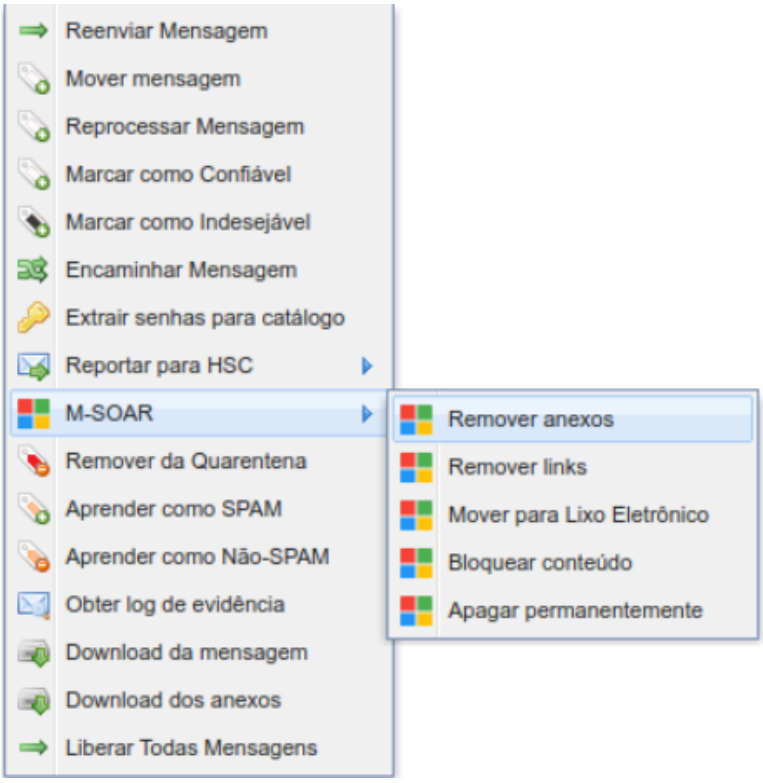
P 8 WORDS

Cancelar Salvar alterações

3. Será exibido o resumo das ações ativas.



4. Pressione SALVAR
5. A partir deste momento o Administrador do MailInspector pode executar ações sobre as mensagens já entregues na caixa do usuário do Microsoft 365.
   Para executar as ações acima, basta localizar a mensagem desejada no Painel Real Time → E-mail e clicar com o botão direito sobre a mensagem e escolher a ação desejada:



Ações do M-SOAR

Remover anexos da mensagem - remove os anexos do e-mail selecionado no Office 365 do usuário final
Remover links da mensagem - remove os links contidos no -mail selecionado no Office 365 do usuário final

Mover para Lixo Eletrônico - move a mensagem para a pasta Lixo Eletrônico no Office 365 do usuário final
Bloquear Conteúdo - impede a visualização da mensagem no Office 365 do usuário final
Apagar a mensagem - apaga a mensagem no Office 365 do usuário final

Requisito para ações

O Administrador do Mail Inspector deve levar em consideração que as ações do M-SOAR são disponibilizadas exclusivamente para as mensagens já entregues no Tennant da Microsoft 365

Ativação de Add-On do MLI no Office 365

O Add-on para Microsoft 365 permite que os usuários dos serviços da Microsoft interagirem a partir de seu MS Outlook Web, MS Outlook 2016 e MS Outlook 2019 com o Mail Inspector. O usuário pode visualizar as suas mensagens em quarentena e liberar alguns tipos de quarentena além de adicionar ou remover registros de sua lista de endereços Confiáveis e Indesejáveis.

O procedimento a seguir descreve a ativação do Add-on do Mail Inspector no Microsoft 365.

Requisitos

- Ativação do M-SOAR
- Possuir acesso administrativo ao Mail Inspector 5.2 (On Premisses ou Enterprise Cloud)
- Possuir uma URL pública do MailInspector configurada com certificado SSL Válido (não pode ser auto-assinado)
- Acesso Administrativo ao Exchange Admin Center (https://admin.exchange.microsoft.com/)

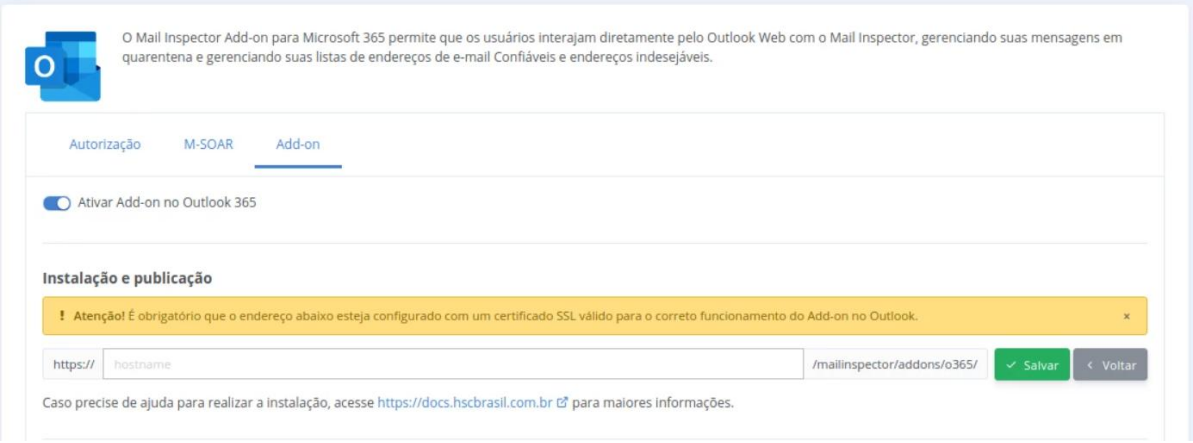
Guia Passo-a-Passo

Este guia é dividido em 2 etapas que são executadas em sequência: Configuração das Ações do Usuário no Add-On e Deploy para os usuários do Microsoft 365.

Primeira Etapa

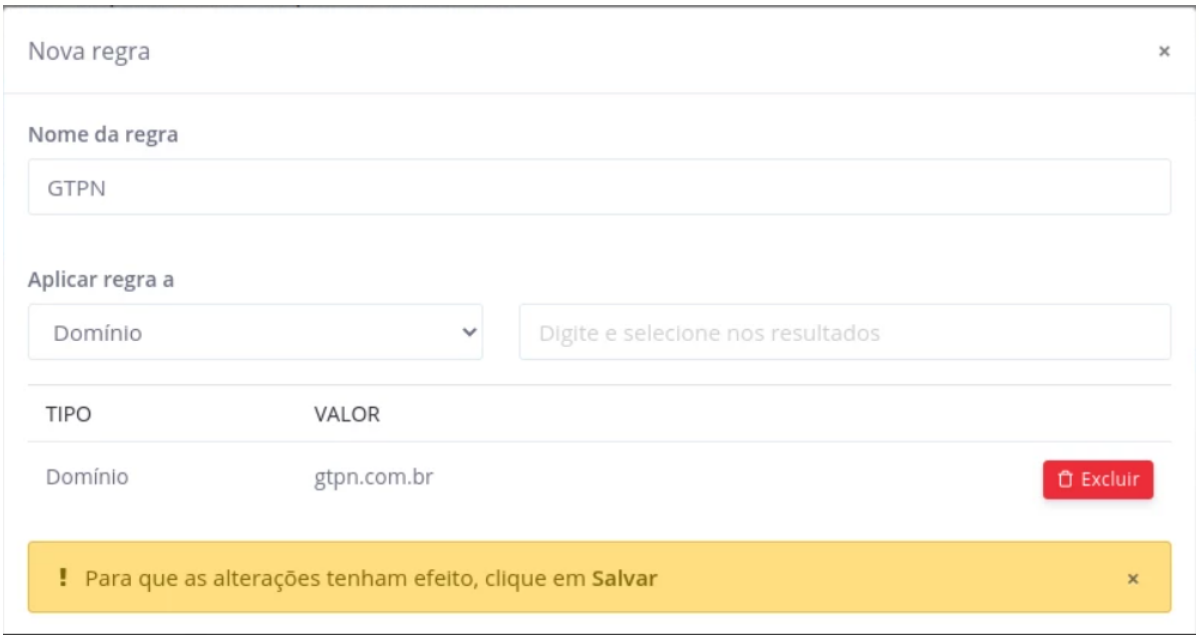
Configuração do Add-on: corresponde à personalização das ações que o usuário do Add-on terá em seu cliente de e-mail Web ou instalação local do MS Outlook 2016 / 2019

1. Ative o Add-on no botão deslizante e informe o FDQN do seu Mail Inspector, clique em salvar e em seguida em Download. Salve o arquivo XML para a Segunda Etapa.



2. Configure as ações o usuário poderá executar em sua caixa de e-mail do Microsoft 365

3. Edite a regra Geral ou crie uma nova regra personalizada. Será permitido aplicar regras diferentes por domínio, Grupos LDAP, Grupos de Usuários ou Usuário.



4. Determine as ações e quarentenas que serão disponibilizadas na interface do usuário do Office 365

Ações disponíveis no menu do Add-on

- [x] Marcar como Confiável
- [x] Gerenciar Quarentena
- [x] Marcar como Indesejável
- [x] Gerenciar listas Confiáveis/Indesejáveis
- [x] Reportar ao Administrador

Quarentenas acessíveis aos usuários

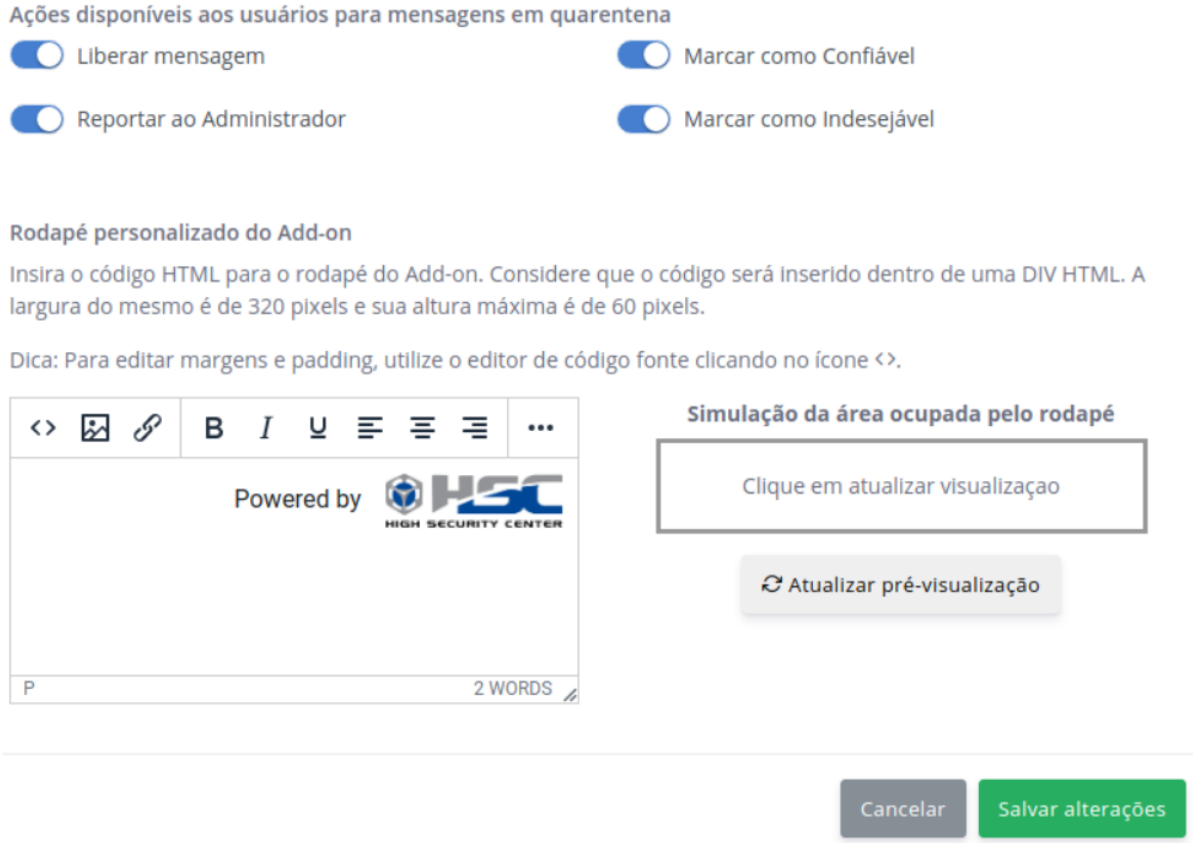
Quarentenas do sistema

- [x] Todas
- [x] ATP
- [x] Blacklist
- [x] Bulk Mail
- [x] Conteúdo Adulto
- [x] Conteúdo Bloqueado
- [x] Controle de Surto/Comportamento Anômalo
- [x] DLP/Auditoria
- [x] Fraude de E-mail / E-mail Impostor
- [x] Malware
- [x] Outro Bloqueio
- [x] Phishing
- [x] Provável SPAM
- [x] SPAM
- [x] Spoofing
- [x] Tamanho Excedido
- [x] Vírus
- [x] Whitelist

Quarentenas customizadas

- [x] Todas
- [x] URL MALICIOSAS

5. Determine as ações permitidas paras mensagens em quarentena. É possível personalizar o rodapé.

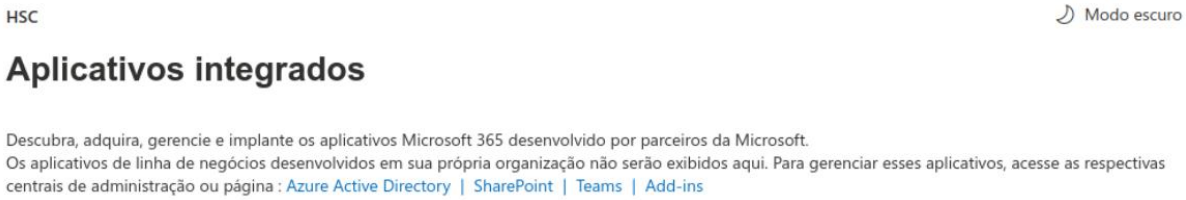


Somente é permitido ao usuário liberar mensagens em quarentena do tipo SPAM, Provável SPAM e Bulk Mail.
Não é possível liberar ameaças como vírus, malware e phishing.

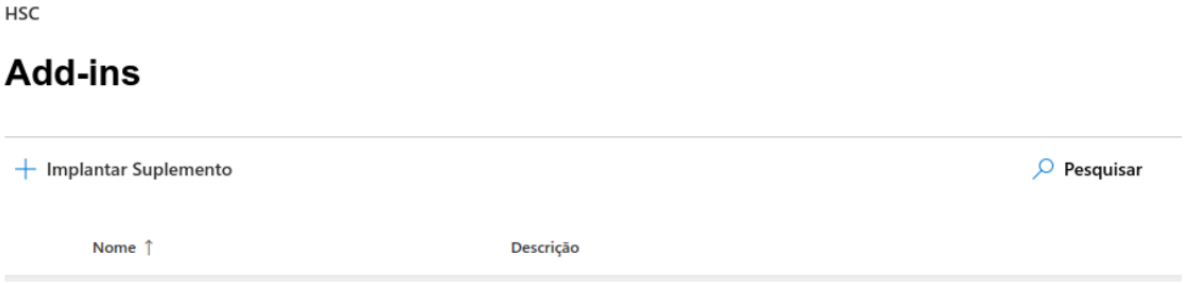
Segunda Etapa

Deploy do Add-on: corresponde à implementação do Add-on nas configurações do domínio no ambiente de administração do Microsoft 365 (https://admin.microsoft.com/). Permite ao administrador do Microsoft 365 implementar apenas para alguns usuários ou grupos, conforme sua preferência.

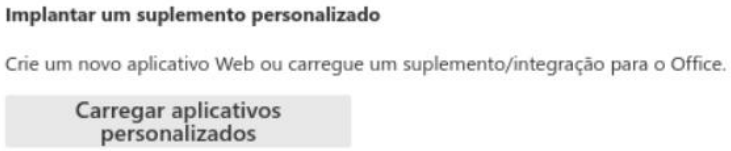
1. Acesse o Portal de Administração do Microsoft 365 como Administrador.
2. Acesse https://admin.microsoft.com/ e navegue em Configurações > Aplicativos Integrados
   Clique em Add-ins (https://admin.microsoft.com/Adminportal/Home#/Settings/AddIns)



3. Em Add-ins, clique em + Implantar Suplemento

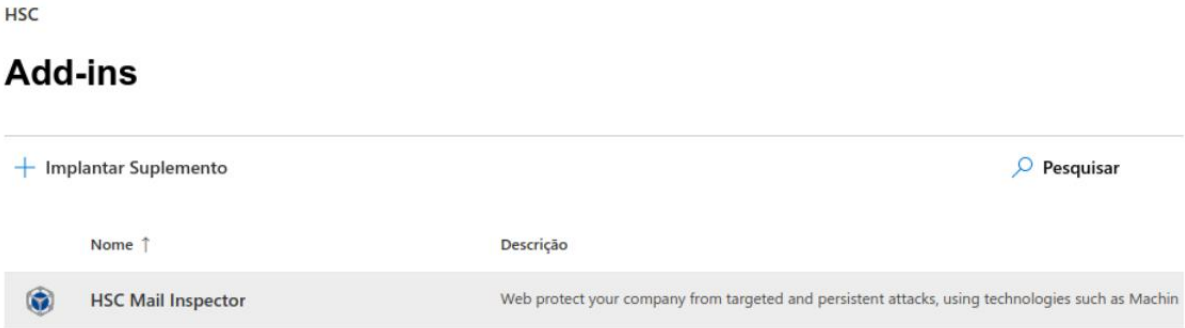


4. Na janela lateral que será apresentada, clique em PRÓXIMO e selecione Implantar um Suplemento Personalizado



5. Clique em Escolher Arquivo e selecione o arquivo .XML obtido na Terceira Etapa. Clique em CARREGAR

Deverá exibir o Add-in conforme abaixo:

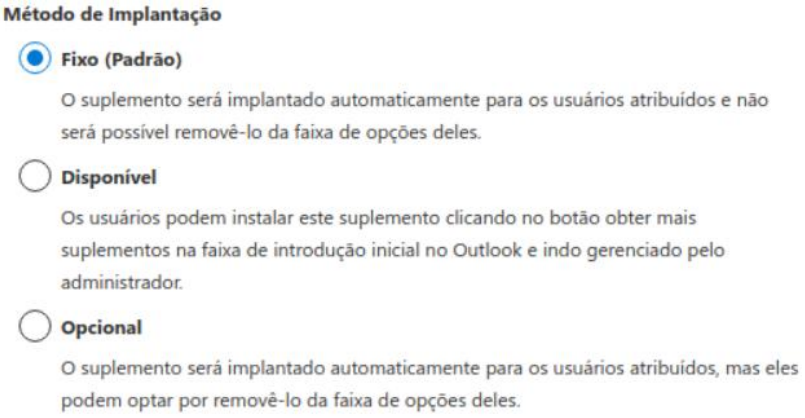


Recomendação

Para minimizar impactos aos usuários finais, recomenda-se realizar a implementação para um usuário ou grupo de usuários, e então implementar para toda a corporação.

6. Selecione as opções da Implementação e IMPLANTAR

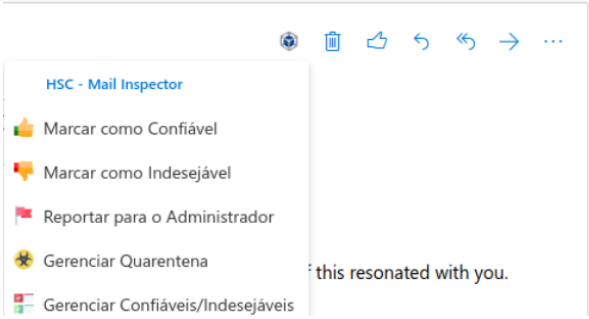
7. É possível permitir ao usuario gerenciar a ativação e utilização ou não. Recomenda o método Fixo (Padrão)



Atenção

É necessário aguardar 24h para disponibilizar o Add-on após sua ativação para os usuários ou grupos determinados

8. Após o período de 24h, faça logoff e login, vá ao painel de e-mails e clique no Ícone da HSC. Serão exibidas as ações a seguir:



Ações do M-SOAR

Marcar como Confiável - Adiciona o remetente da mensagem na lista Confiável do usuário no Mail Inspector (Whitelist)

Marcar como Indesejável - Adiciona o remetente da mensagem na lista Indesejável do usuário no Mail Inspector (Blacklist)

Reportar para o Administrador - remete uma cópia da mensagem para o Administrador do Mail Inspector

Gerenciar Quarentena - Permite ao usuarios visualizar as mensagens que estão retidas na sua quarentena pessoal, podendo liberar as mensagens do tipo Provável SPAM, SPAM e Bulk Mail

Gerenciar Confiáveis / Indesejáveis - Permite ao usuario adicionar ou remover registros de sua lista de remetentes Confiável ou Indesejável

Aviso

O processo de implementação descrito instala o Add-On automaticamente nos clientes de e-mail Microsoft Office 2016/2019.

Atenção

Após o decorrer de 24 h, é recomendado realizar logoff e logon em suas contas para forçar o carregamento do Add-on.

Bloqueio de e-mails com liberação pelo supervisor de e-mails

Em algumas empresas temos o papel do supervisor de e-mails, ao qual passa por ele os e-mails de uma determinada conta ou determinadas contas ficam "paradas" em uma quarentena aguardando a liberação do supervisor.

Premissas

É necessário que o tenha acesso ao MailInspector com privilégio de administrador.

Lógica empregada

Criar uma quarentena customiza, com permissão de acesso ao administrador e aos supervisores. Todos os e-mails de origem e/ou destino para os e-mails monitorados são redirecionados a esta quarentena, aguardando a liberação dos mesmos pelo supervisor.

Obs: É possível trabalhar de duas formas distintas de quarentena supervisionada.

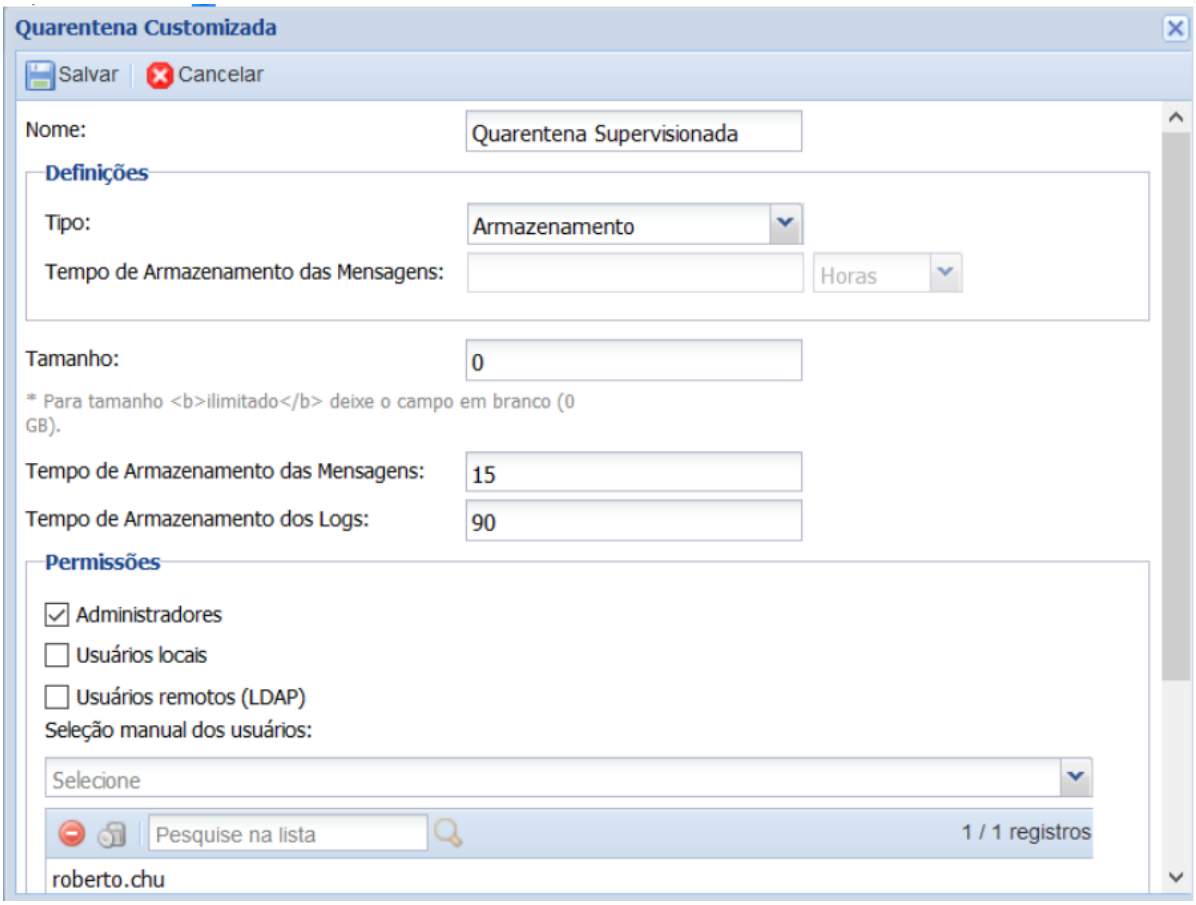
1. Usando quarentena temporária: Os e-mails ficam parados nesta quarentena por um período definido pelo administrador e ao ultrapassar esse tempo, o e-mail segue o seu caminho de entrada ou saída. Quando o supervisor libera o e-mail desta quarentena, ela já sai da caixa e segue o seu caminho (sem ter que aguardar o tempo limite para a liberação automática).
2. Usando quarentena permanente: Os e-mails ficam retidos permanentemente na quarentena customizada, aguardando a liberação do supervisor, se o mesmo não ocorrer, até o tempo estipulado de rotate da quarentena (pelo administrador), o e-mail é automaticamente apagado do sistema.

Criar regra de E-mail Compliance, onde jogará para a quarentena customizada os e-mails que atenderem a condição e o acesso a pasta de E-mail Compliance somente será os que o administrador configurar (que no caso será o supervisor de e-mails e os administradores da caixa).

Guia Passo a Passo

1. Vá em Configurações > Quarentena > Customizada

2. Clique em Adicionar



Selecione o nome da quarentena

Selecione o Tipo:

- Quarentena fixa (as mensagens ficarem retidas até que o supervisor libere ou até ocorrer a exclusão automática da mesma)
- Quarentena por tempo de Armazenamento (Atrasar a Entrega). Essa quarentena é para caso você queira que a aprovação do e-mail seja "automática", ao qual se o supervisor não tomar a medida de excluir o e-mail retido, o mesmo prosseguirá com a entrega após o tempo expirar.

Tamanho: 0;

Tempo de Armazenamento das Mensagens: 15 (em dias). Indica por quanto tempo ficarão as mensagens disponíveis ao supervisor. Após esse período, a mensagem é excluída automaticamente.

Tempo de Armazenamento dos Logs: 90 (em dias). Indica tempo de permanência no sistema dos logs referentes a mensagem.

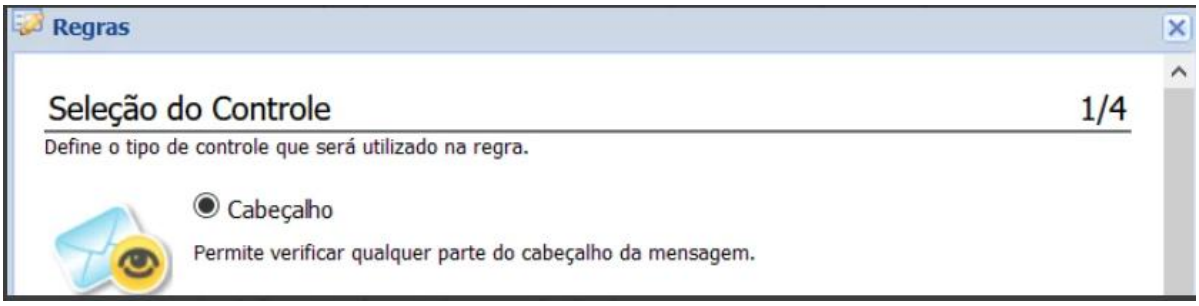
Permissões: Quem você deseja possuir permissão de acesso a essa pasta. Geralmente é o supervisor com permissão de aprovação do e-mail. Como exemplo, vamos colocar o usuário roberto.chu e administradores como supervisor da pasta.

3. Clique em Salvar
4. Vá em Configurações > E-mail Compliance > Regras e Crie e Regra de Bloqueio na Quarentena Customizada (baseado nos e-mails com origem ou destino ao grupo de E-mails Supervisionados).

Como exemplo, vamos supor que todos os e-mails com DESTINO ao Grupo de E-mails Supervisionados, devam cair na caixa de quarentena Supervisionada e somente seja liberado pelo Supervisor da pasta (no exemplo usamos roberto.chu)

Clique em Adicionar

Selecione Cabeçalho



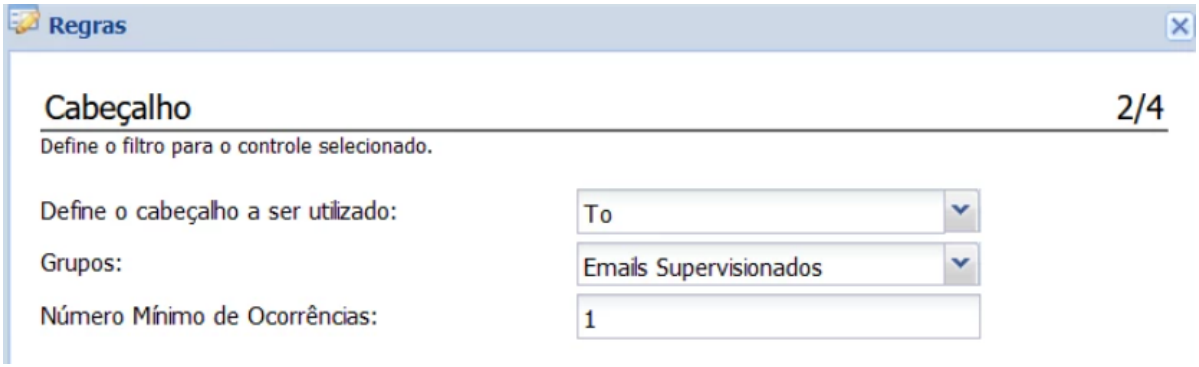
Clique em Avançar

Na tela a seguir (Regra) selecione:

Define o cabeçalho a ser utilizado: To

Grupo: E-mails Supervisionados

Número Mínimo de Ocorrências: 1

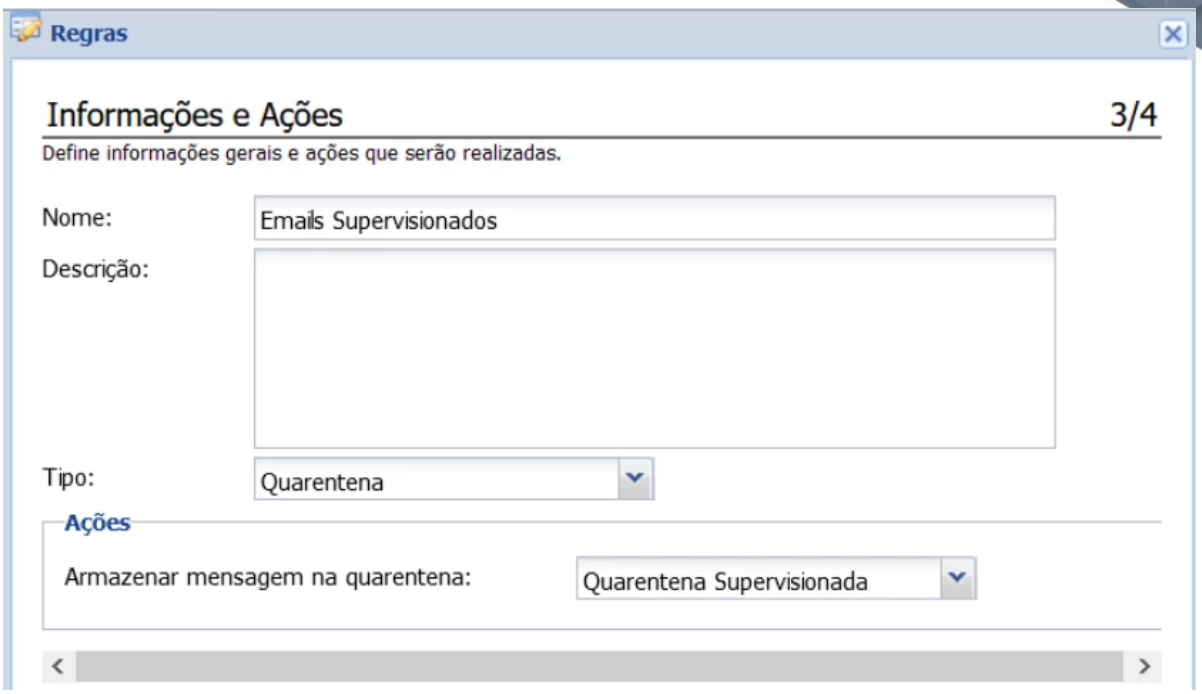


Clique em Avançar

Na próxima tela indique o nome da regra (no exemplo colocamos E-mails Supervisionados)

Mude o Tipo para: Quarentena

Em Ações (Armazenar mensagens na quarentena) selecione a pasta Quarentena Supervisionada

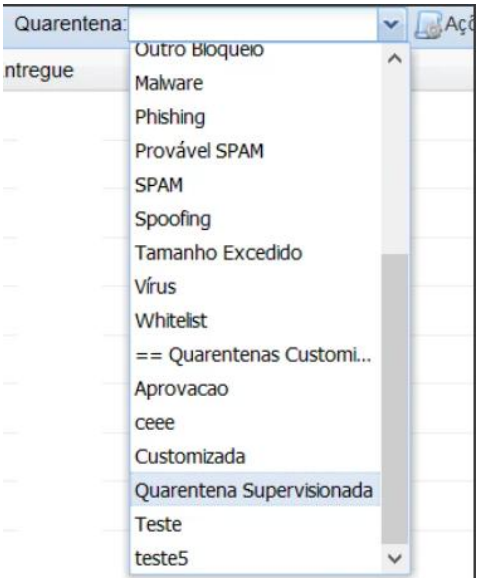


Clique em Avançar

Clique em Salvar

Clique em Aplicar Configurações e Aplicar

5. Na tela de RealTime > E-mails > Quarentena, verifique que agora tem a pasta Quarentena Supervisionada para seleção, ao qual mostrará somente os e-mails que caírem na condição de E-mail supervisionado, permitindo dessa forma que o supervisor e o administrador possam tomar as ações de liberação ou exclusão dos e-mails dessa quarentena.



Regras com base nos Cabeçalhos de TO do Header ou TO do Envelope e ambos

O Mail Inspector permite utilizar todos os campos do Cabeçalho para a composição de Regras de Controle Avançado e DLP.

Aqui iremos detalhar as formas para utilizar o campo de Destinatário da Mensagem para compor nossas Regras de Controle avançada e de DLP.

O campo Para existe em 2 locais. No Para do Envelope (1), usado para transporte da mensagem e o Para do Header (2), que é exibido para o usuário final ao ler a mensagem

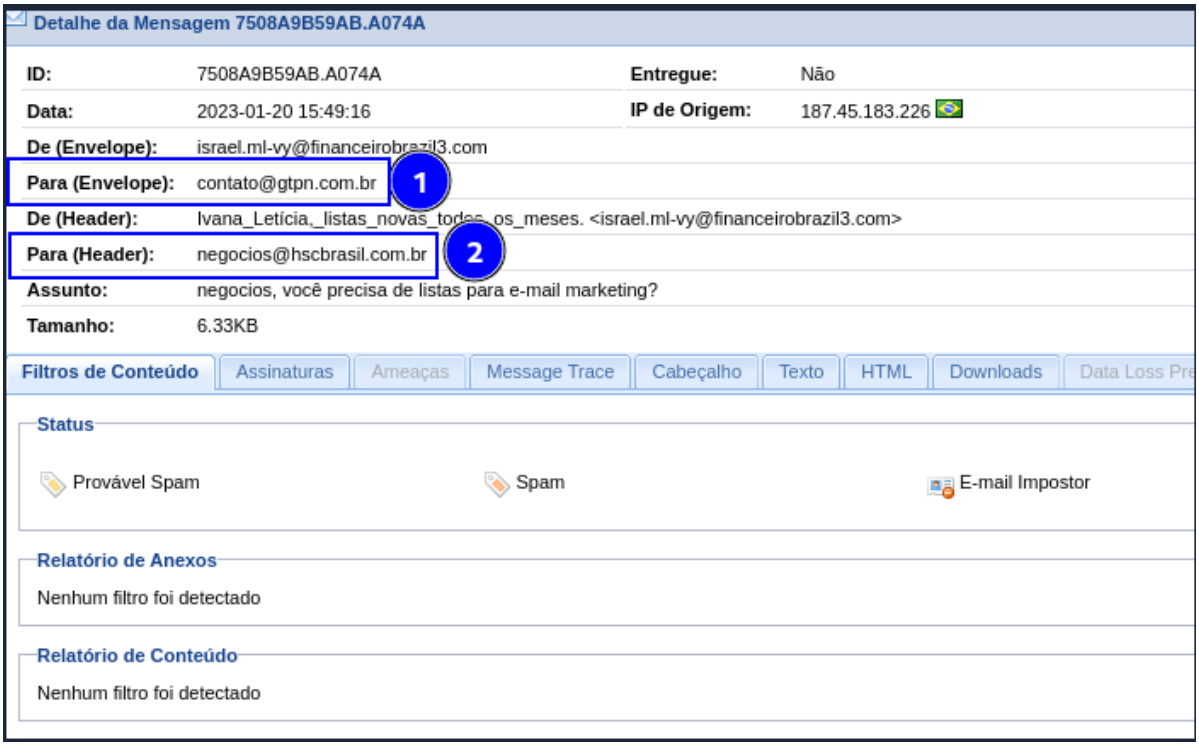
Em muitos cenários, é necessário utilizar apenas um, ou outro para tomar ações específicas e granulares.

Sendo assim, segue abaixo as diferenças e um exemplo de cada tipo de configuração

Premissas

É necessário que o tenha acesso ao MailInspector com privilégio de administrador.

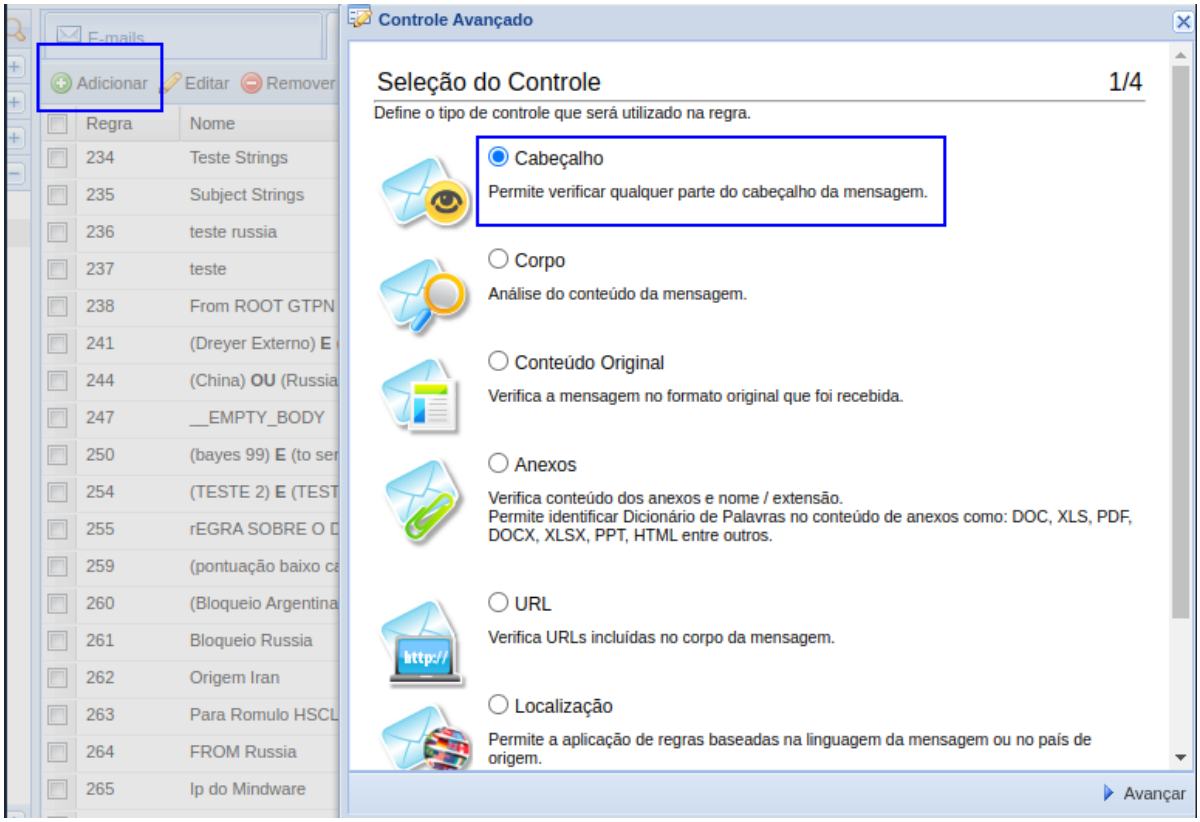
Exemplo de uma mensagem qualquer:



Caso 1

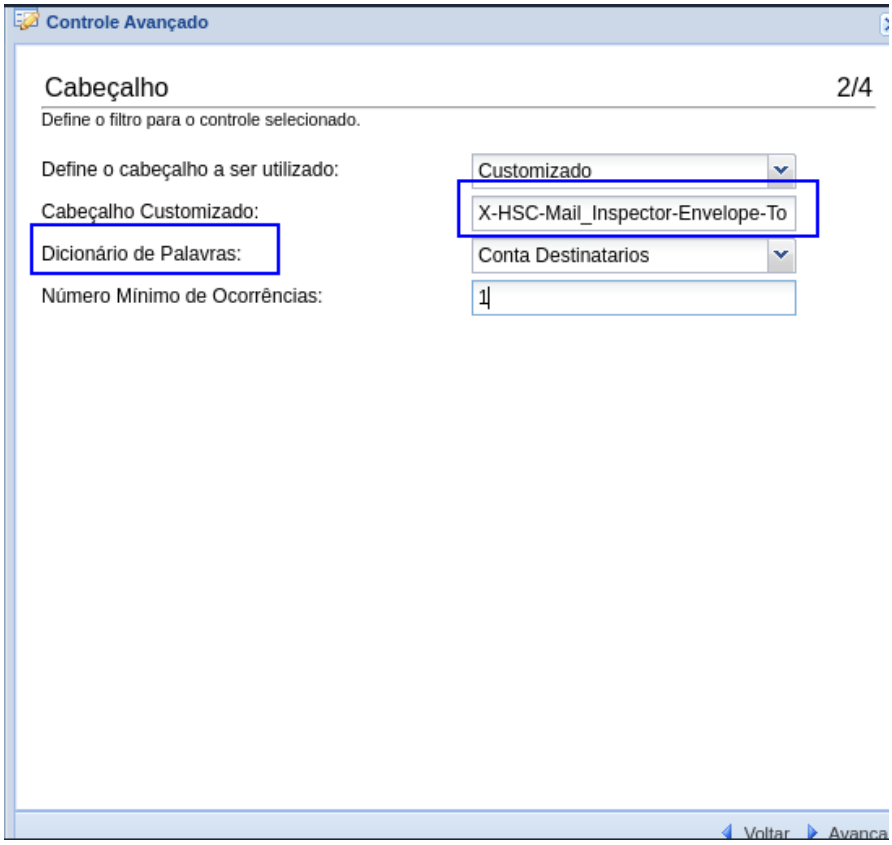
Criando uma regra de Controle Avançado que diminui a pontuação para um Grupo de Destinatários

Vá em Configurações → Filtros de Spam → Controle Avançado e Adicione uma Regra de Cabeçalho e avance



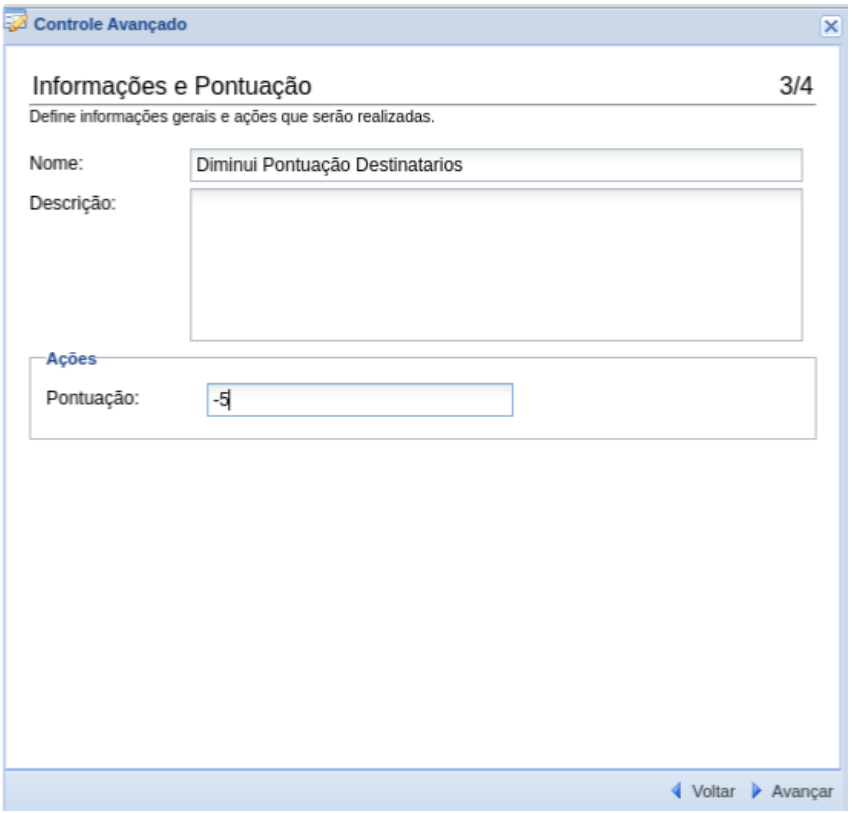
Selecione o Cabeçalho Customizado e digite **X-HSC-Mail_Inspector-Envelope-To** para usar o **TO do Envelope** ou **X-HSC-Mail_Inspector-To** para usar o **TO do Header**. Caso deseje **mapear ambos,** utilize o Customizado e digite **TO**.

Selecione o Dicionário de Palavras, o qual deve conter os e-mails dos destinatários alvos desta regra.

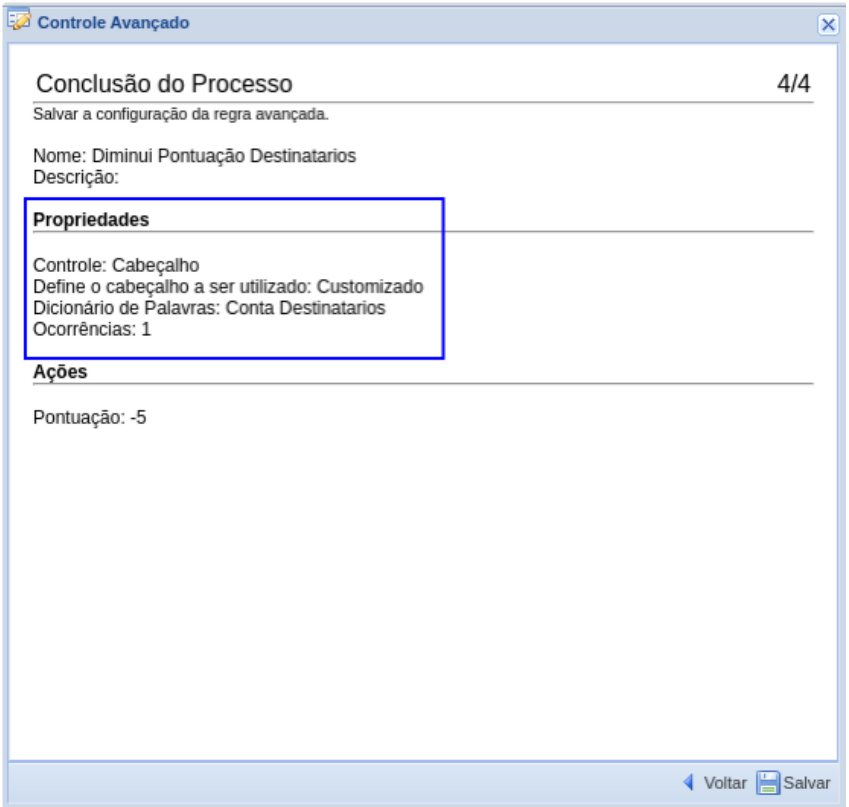


O dicionário de palavras deve ser criado considerando as regras de Expressão Regular (RegEx):

Obs: utilize o caracter **** antecedendo o **@** e **pontos**



Revise o resumo e salve



Resumo da Regra:

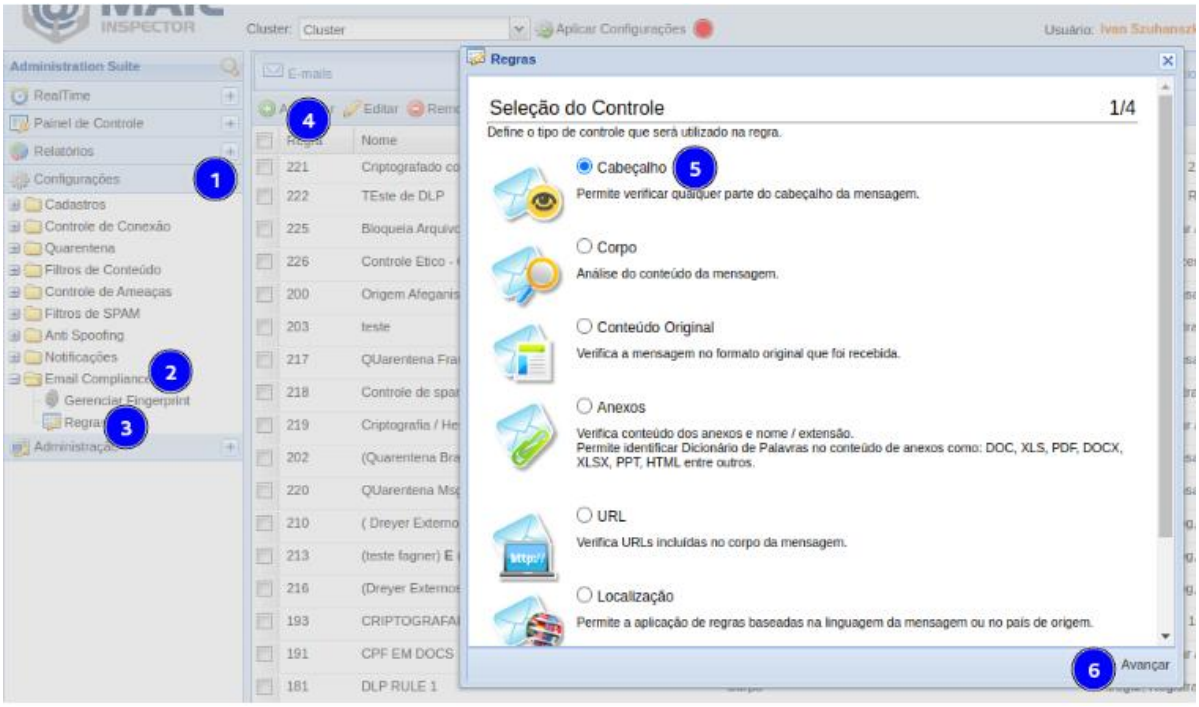
O Mail Inspector ao filtrar uma mensagem irá identificar os destinatários no To do Envelope e irá subtrair 5 pontos, facilitando assim a entrega deste e-mail

Caso 2

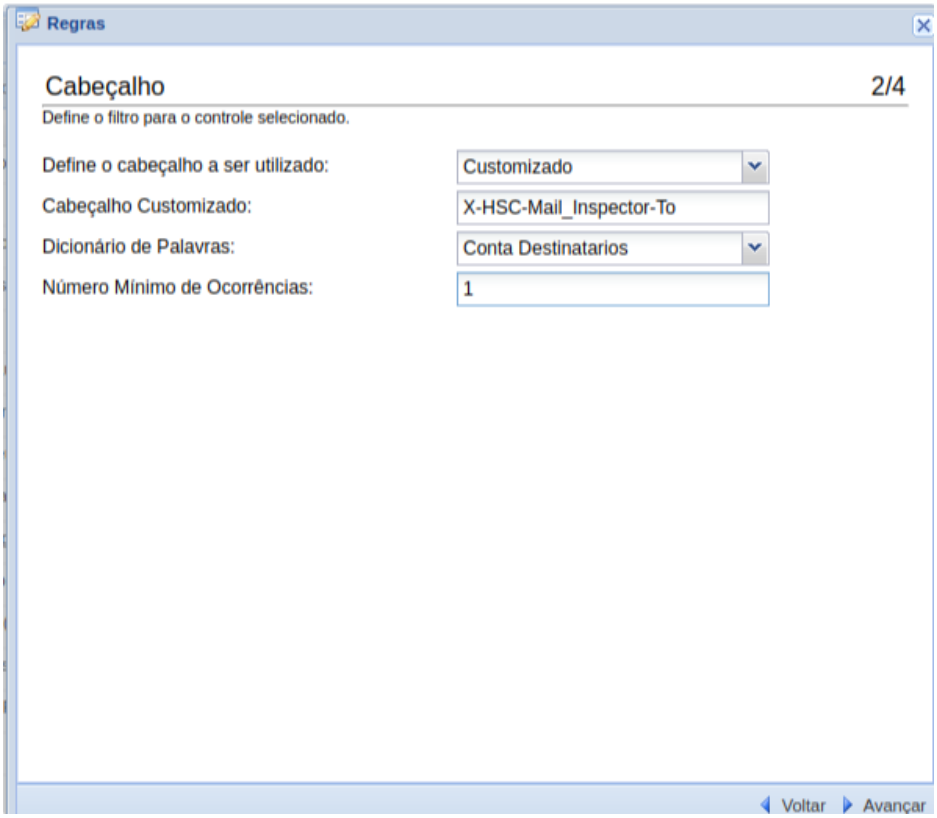
Criando uma regra de DLP para Encaminhar as mensagens de um grupo de destinatários para um grupo.

Nesta regra iremos usar o assistente de DLP para mapear o campo **TO do Header**

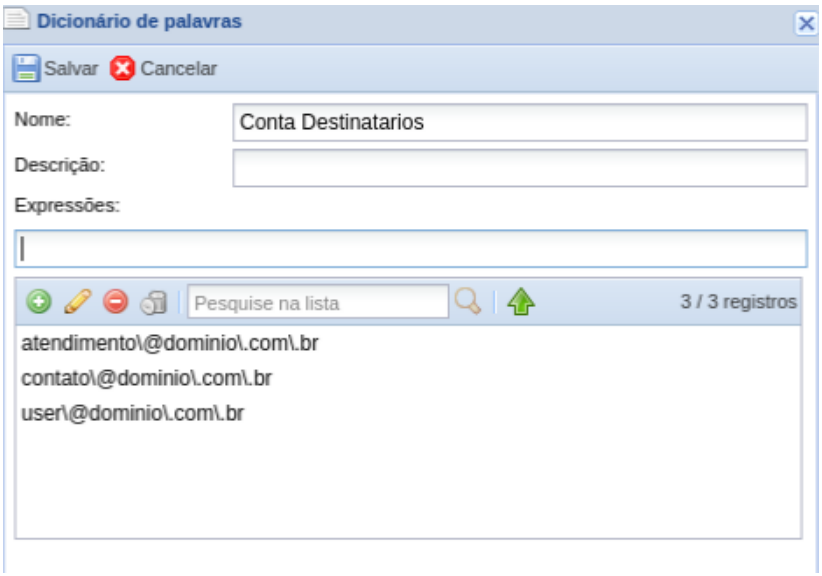
Vá em Configurações → E-mail Compliance → Regras e Adicione uma Regra de DLP.



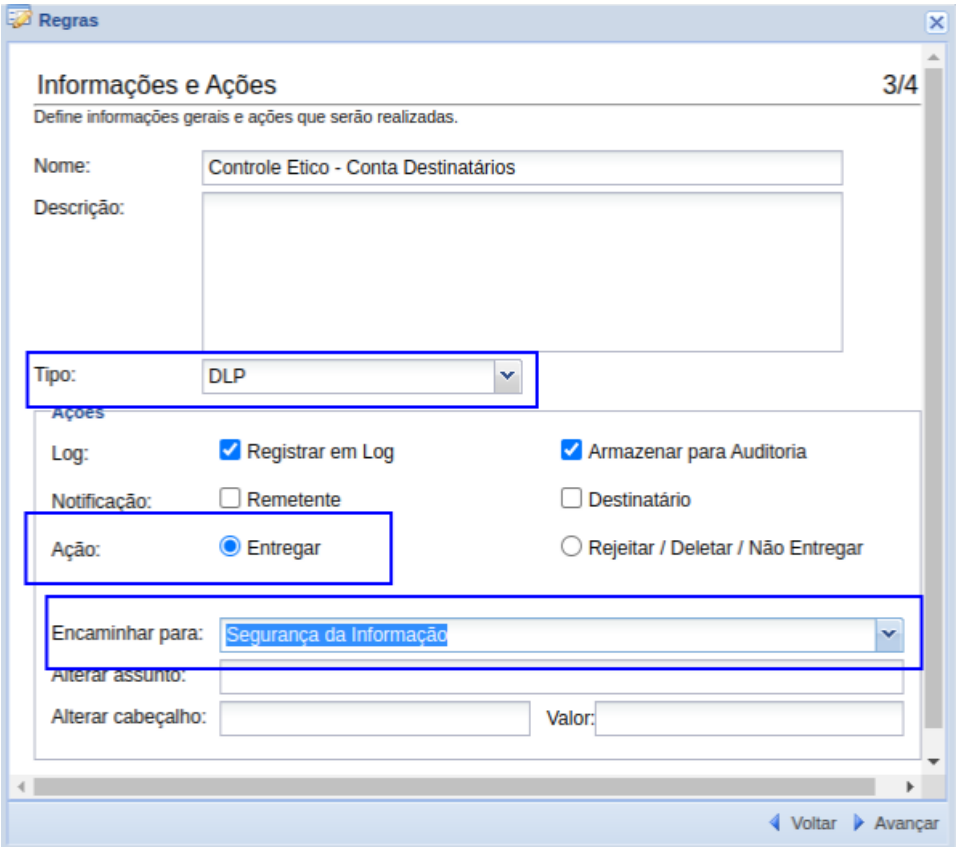
Selecione o Cabeçalho Customizado e digite **X-HSC-Mail_Inspector-To** para usar o **TO do Header** ou **X-HSC-Mail_Inspector-Envelope-To** para usar o **TO do Envelope**. Caso deseje **mapear ambos** Utilize o Customizado e Digite **TO**.



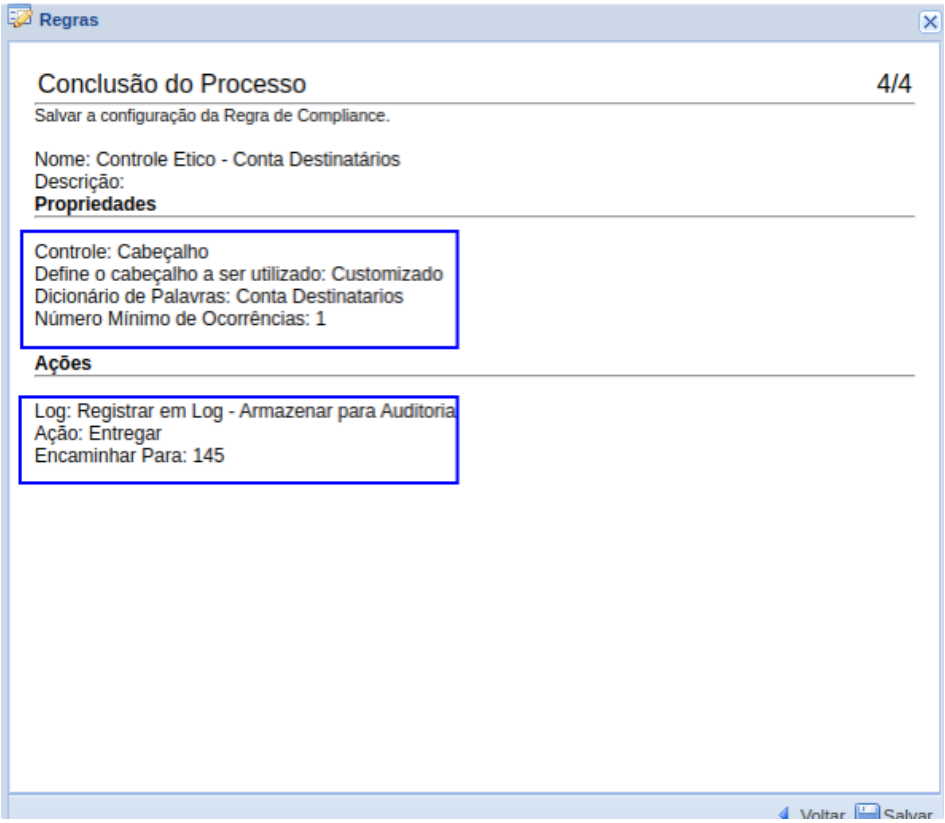
Selecione o Dicionário de Palavras, o qual deve conter os e-mails dos destinatários Alvos desta regra



Após avançar, configuramos as Políticas da Regra de DLP, as quais permite bloquear a mensagem ou entregá-la, notificar ao remetente ou destinatário ou reencaminhar para outros destinatários, podendo alterá-las conforme a necessidade do seu negócio. É possível alterar o assunto e incluir cabeçalhos especiais.



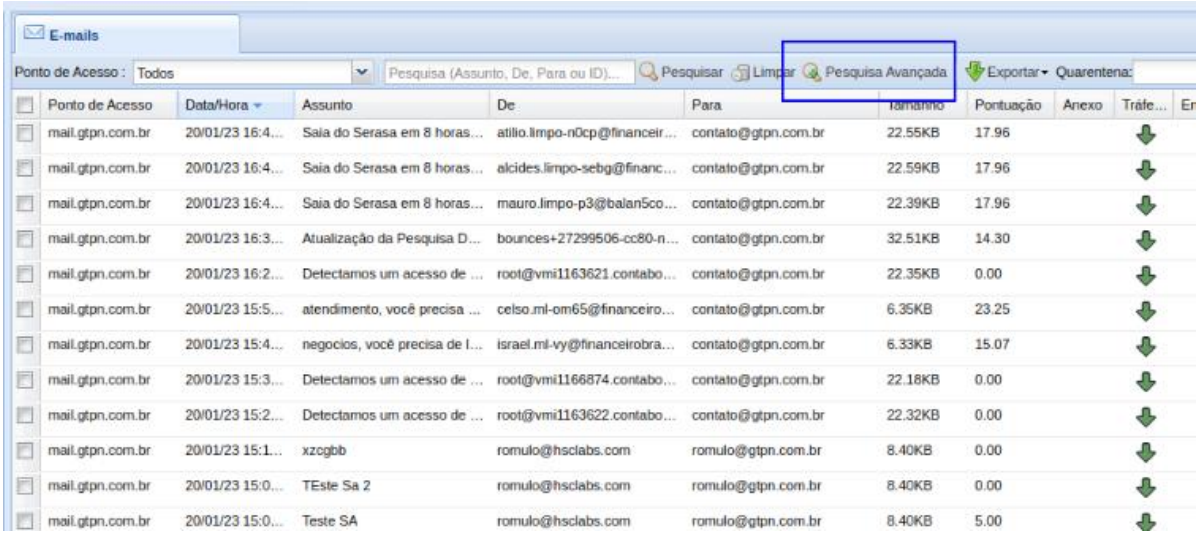
Revise o resumo e salve

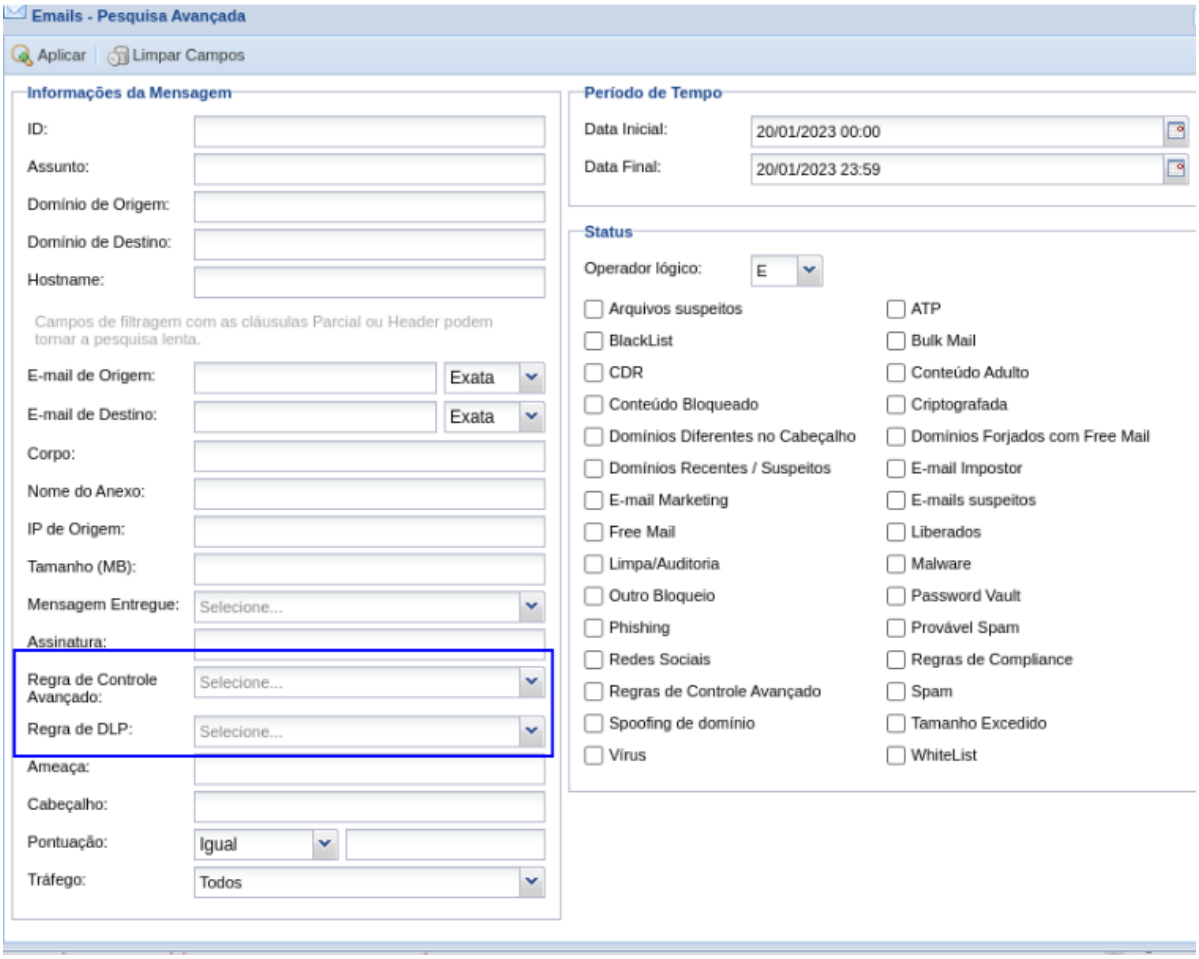


Resumo da Regra de DLP

O Mail Inspector ao filtrar uma mensagem irá identificar os Destinários do Grupo no campo **TO do Header** e irá Entregar a mensagem normalmente. Adicionalmente enviará uma cópia da mesma para um Grupo de Segurança da Informação.

Utilize a Pesquisa Avançada para verificar o comportamento da regra criada.



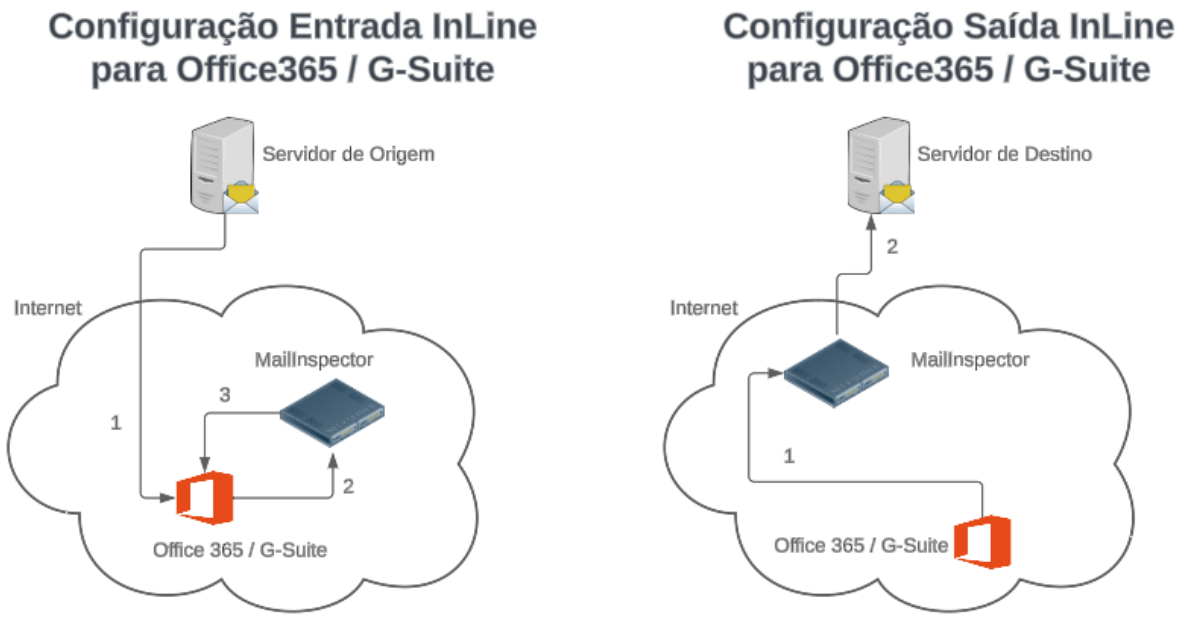


Obs: Somente será possível pesquisar por mensagens filtradas posteriormente a criação das Regras.

Apêndice 6 - Integração do MailInspector com Microsoft Office365 sem alteração no apontamento MX/DNS

Entrada de E-mails Office365 sem alteração de MX

Exibe documento tem por finalidade mostrar a integração do MailInspector com Offi365, sem necessidade de mudança de MX e integração e importação de contas via API.



Modelo de Configuração de Entrada e Saída de E-mails sem alteração de MX

Configuração Entrada InLine (sem mudança no MX) para Office365 / G-Suite

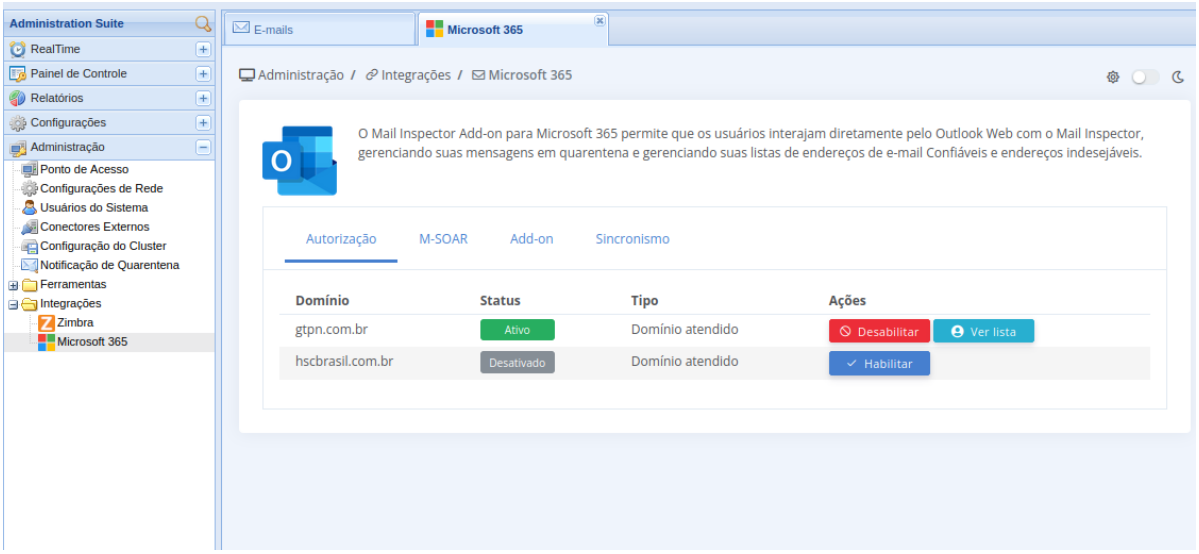
1. Os e-mails são direcionados ao Office365/G-Suite (que é o padrão quando se usa Office365 ou G-Suite), portanto, não há necessidade de mexer no MX/DNS;
2. Ao receber o e-mail, o Office365/G-Suite efetua a filtragem e encaminha para o MailInspector;
3. Após a filtragem por parte da Microsoft/Google, as mensagens são escaneadas novamente pelo MailInspector e os devolve ao Office365/G-Suite;

Configuração Saída InLine (sem mudança no MX) para Office365 / G-Suite

1. E-mail sai do Office365 / G-Suite e é entregue ao MailInspector;
2. É feita a filtragem do e-mail no MailInspector e entregue a Internet (servidor destino);

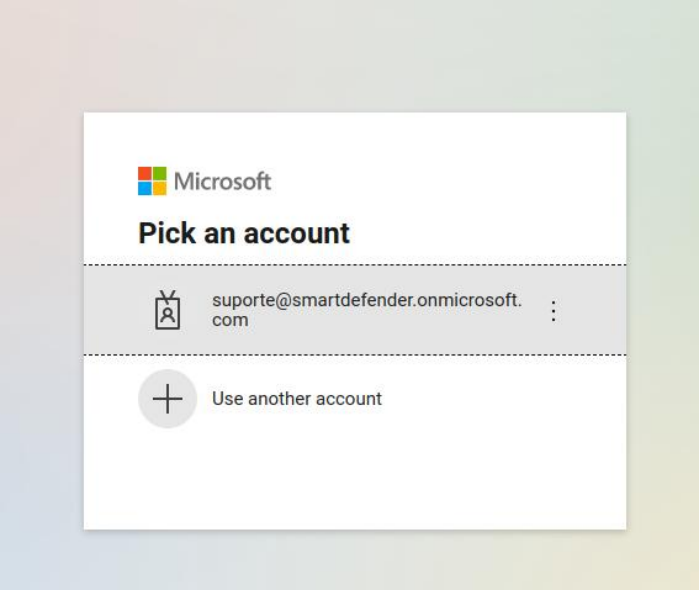
Configuração de conexão com Office365 via API

Primeiramente temos que configurar a conexão do MailInspector com o Office365. Para isso, vá em: Administração > Integrações > Microsoft 365

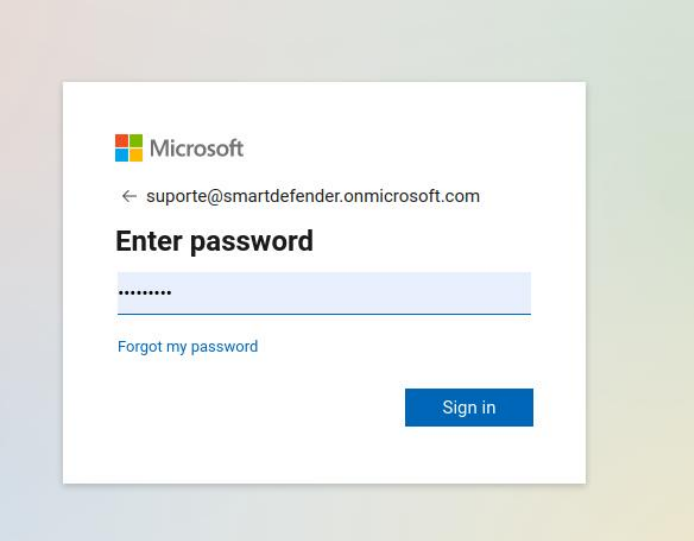


1. Serão exibidos todos os domínios protegidos pelo Mail Inspector. Escolha o domínio que deseja ativar a integração e clique em Habilitar.

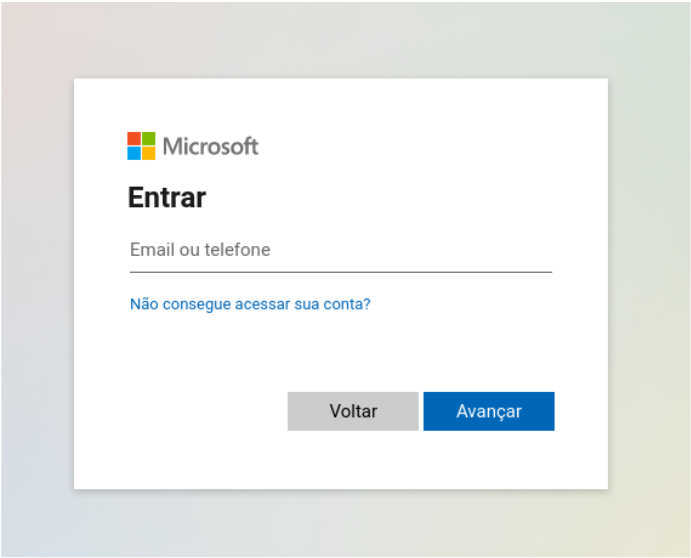
2. Na nova janela, informe as credenciais do administrador do serviço Microsoft 365



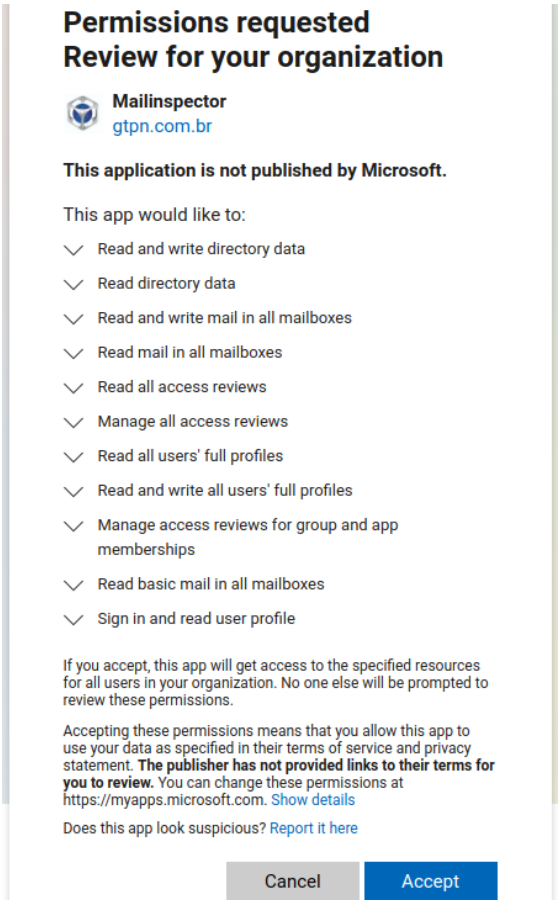
3. Informe a senha



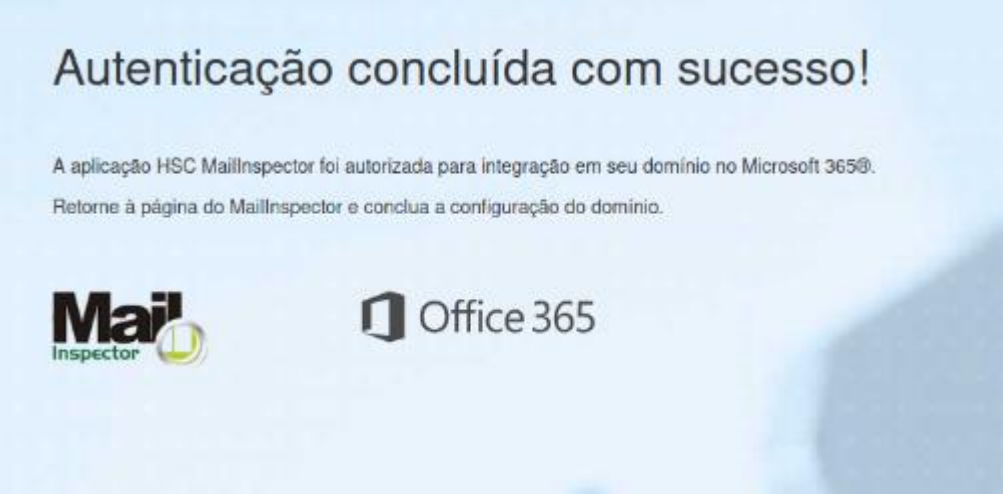
4. Na janela que abrirá, informe as credenciais do Administrador da conta Microsoft 365



5. Confirme as permissões solicitadas



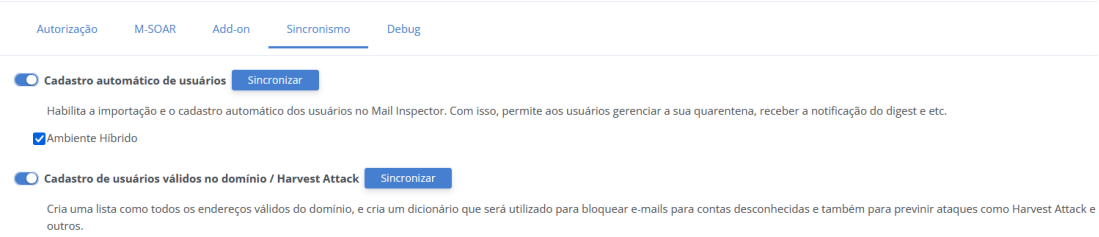
6. Em caso de sucesso será apresentada a mensagem a seguir:



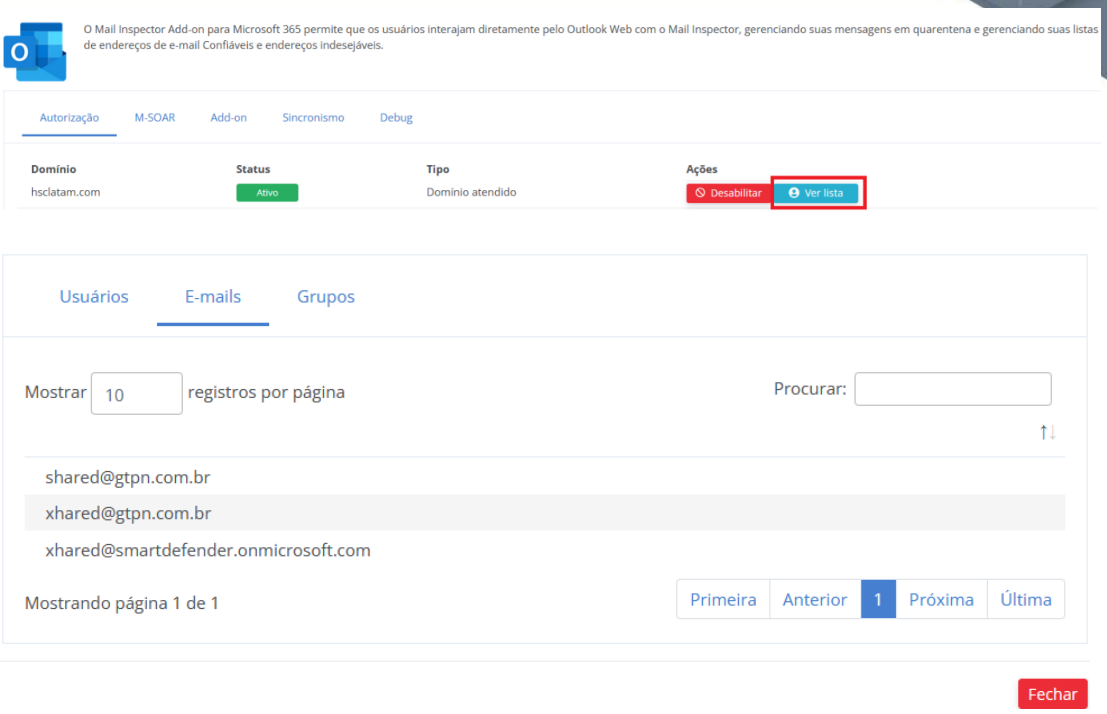
7. Em caso de falha no acesso das credenciais fornecidas, será apresentada a mensagem:

Neste caso contate o administrador da conta Microsoft 365

8. Para importar os usuários, Grupos e Lista de E-mails, clique na aba Sincronismo Clique em Sincronizar, tanto para Cadastro automático de usuários, quanto para Cadastro de usuários válidos no domínio/Harvest Attack



Para visualizar os usuários, e-mails e Grupos importados para autenticação por SSO (Single Sign-On), vá na aba Autorização e no domínio que você habilitou, clique no botão **Ver Lista**

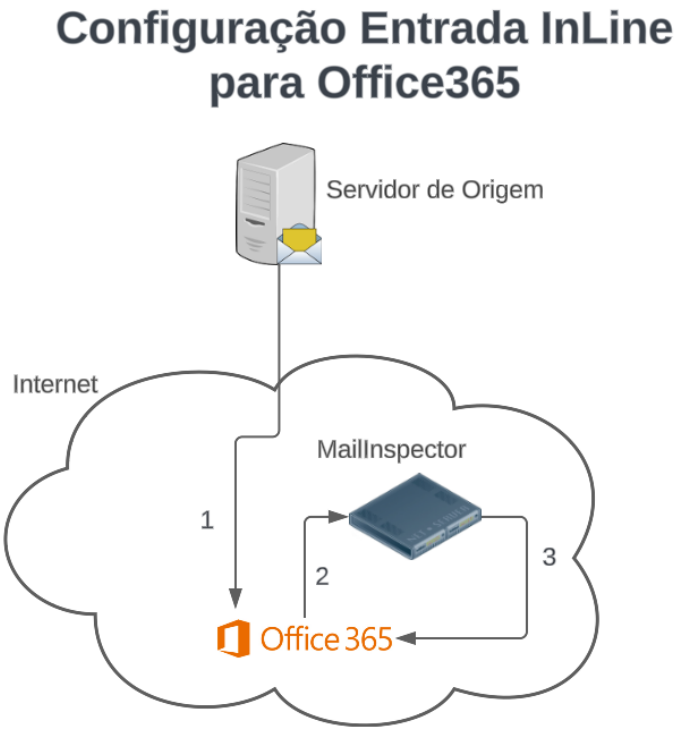


Nessas abas você poderá visualizar:

- Usuários importados;
- E-mails importados;
- Grupos importados;

Caso você queira ativar outro domínio e importar os usuários, repita o processo.

Configuração Entrada de E-mails para Office365 Inline (sem alteração de MX)



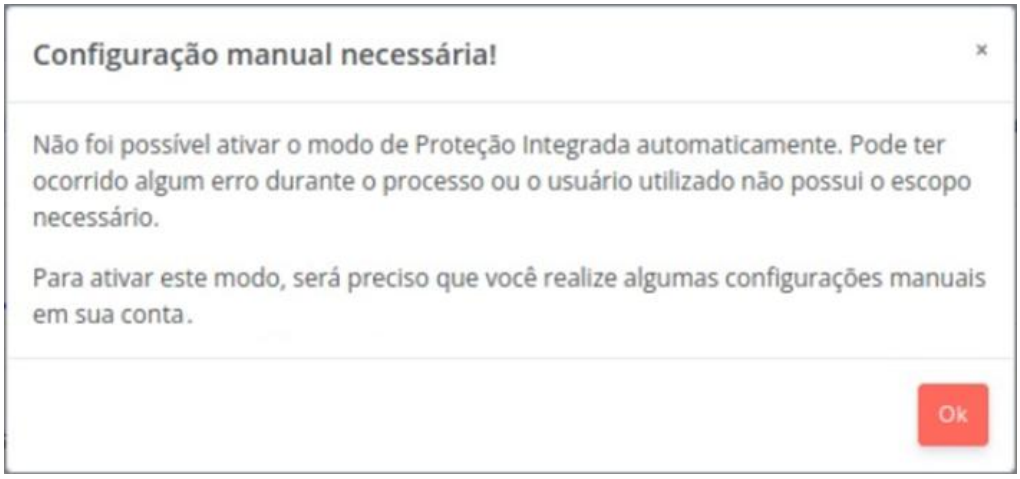
1. O e-mail é entregue ao Office365;
2. Através de criação de conector de entrada, atrelada a rota no Fluxo de e-mail, o Office365 redireciona o e-mail de entrada direto ao MailInspector;
3. O MailInspector faz a filtragem e devolve ao Office365 o e-mail limpo.
   Para evitar o loop, é criado um conector com os IPs do MailInspector indicando que quando o e-mail vier dos IPs do MailInspector, esses devem ser entregues ao Office365;

Por padrão o MailInspector permite que as configurações InLine sejam automáticas, bastando selecionar a opção Proteção Integrada.

- **Por Gateway de Entrada:** É o processo em que é feito o apontamento dos e-mails para o MailInspector. Esse apontamento é através de mudança do MX no DNS da empresa.
- **Proteção Integrada:** Não há a necessidade de apontar o MX no DNS da empresa, basta configurar o Office365/G-Suite para que ao receberem os e-mails, eles sejam redirecionados ao MailInspector, que os filtrarão e os devolverá ao servidor Office365/G-Suite.

Essa configuração poderá ser de forma automática, sem necessidade de intervenção ou criação de regras por parte do administrador, somente será necessária a intervenção manual em determinados casos, como por exemplo falta de permissão do administrador para acesso automático do MailInspector sobre o Office365/G-Suite, ou falha de comunicação, etc.

Caso ocorra alguma falha de configuração automática, será necessária a configuração manual, para isso, basta seguir as etapas indicadas a seguir, de acordo com o tipo de servidor de e-mail utilizado (G-Suite ou Office365).



Vamos criar algumas etapas para o redirecionamento de e-mail para o MailInspector, quando o e-mail vier de fora. Para isso, vamos seguir a seguintes etapas:

1. Criar um Conector de Saída ao MailInspector
2. Criar regra de redirecionamento atrelado ao conector de saída
3. Criar Conector de Entrada InLine

1. Criando um Conector de Saída ao MailInspector

1. Acesse o seu Office365 como administrador;
2. Acesse o módulo de administração do Exchange;
3. Vá em Fluxo de e-mail > Conectores
4. Clique em Adicionar um conector
5. **Novo conector**
   Conexão de: Office365
   Conexão com: Organização parceira
   Clique em Próxima
6. **Nome do conector**
   Nome: Saída InLine MLI

Deixe marcada a caixa Ativar
Clique em Próxima

7. **Uso de conector**
   Marque a opção:
   Somente quando houver uma configuração de regra de transporte que redirecione mensagens para este conector
   Clique em Próxima
8. **Roteamento**
   Selecione a opção:
   Rotear e-mail através desses hosts inteligentes
   Insira os IPs dos nodes do MailInspector
   Clique em Próxima
9. **Restrições de Segurança**
   Deixe marcada a opção Sempre usar o protocolo TLS para proteger a conexão (recomendado)
   Selecione a opção Qualquer certificado digital, inclusive certificados autoassinados
   Clique em Próxima
10. E-mail de validação
    Insira qualquer e-mail, para validação
    Clique em Próxima
11. Clique em Criar conector

2. Criando regra de redirecionamento atrelado ao conector de saída

1. Acesse o seu Office365 como administrador;
2. Acesse o módulo de administração do Exchange;
3. Vá em Fluxo de e-mail > Regras;
4. Clique em Adicionar uma regra;
   Criar uma nova regra;
5. **Definir condições de regra**
   Nome: Roteamento Inbound InLine MLI
   Aplicar esta regra se: O remetente
   é externo/interno: Outside the organization
   selecionar local do remetente

   Faça do seguinte:
   Redirecionar a mensagem para: o seguinte conector > Saída InLine MLI
   Exceto se:
   O remetente > o endereço IP está em qualquer um desses intervalos ou correspondências exatas
   Clique em Enter words
   especificar intervalos de endereços IP
   Insira todos os IPs do MailInspector disponibilizado para a sua empresa (fornecido pelo pessoal de suporte)
   Clique em Salvar
   Clique em Avançar

6. **Definir configurações de regra**
   Deixe a opção Modo de regra em Impor
   Mude a severidade para: Alto
   Clique em Avançar
7. **Revisar e concluir**
   Clique em Concluir
8. **Regras**
   Mude a ordem de preferência da regra criada para o primeiro do grupo usando o botão ^Mover para cima, com isso, essa regra fará com que todos os e-mails de entrada sejam redirecionados para o MailInspector, quando não vierem dos IPs do MailInspector. Caso vierem de algum IP do MailInspector, o e-mail será processado normalmente.

3. Criando um Conector de Entrada InLine

1. Acesse o seu Office365 como administrador;
2. Acesse o módulo de administração do Exchange;
3. Vá em Fluxo de e-mail > Conectores
4. Clique em Adicionar um Conector
5. **Novo conector**
   Conexão de: Organização parceira
6. **Nome do conector**
   Nome: Entrada InLine MLI
   Deixe marcada a opção Ativar
   Clique em Próxima
7. **Autenticando e-mail enviado**
   Selecione a opção:
   Ao verificar se o endereço IP do servidor de envio corresponde a um destes endereços IP que pertencem à sua organização
   Insira todos os IPs do MailInspector (fornecidos pelo suporte da HSCBRASIL)
   Clique em Próxima
8. **Restrições de segurança**
   Verifique que esteja marcada a seguinte opção:
   Rejeitar mensagens de e-mail que não forem enviadas por TLS
   Desmarque a opção E exigir que o nome da entidade no certificado usado pelo parceiro para autenticar o Office 365 corresponda a este nome de domínio
   Clique em Próxima
9. Clique em Criar conector

Configuração Saída de E-mails para Office365 Inline

Vamos criar algumas etapas para o redirecionamento de e-mail para o MailInspector, quando o e-mail vier de fora. Para isso, vamos seguir a seguintes etapas:

1. Criar um Conector de Saída ao MailInspector
2. Criação de regra de saída atrelado ao conector de Saída ao MailInspector

Caso você **já tenha criado um conector de saída** indicado na parte de **Configuração Entrada de E-mails para Office365 Inline (sem alteração de MX)**, **pule para o item 2** que é **Criação de regra de saída** atrelado ao conector de Saída ao MailInspector.

1. Criando um Conector de Saída ao MailInspector

1. Acesse o seu Office365 como administrador;
2. Acesse o módulo de administração do Exchange;
3. Vá em Fluxo de e-mail > Conectores
4. Clique em Adicionar um conector
5. **Novo conector**
   Conexão de: Office365
   Conexão com: Organização parceira
   Clique em Próxima
6. **Nome do conector**
   Nome: Saída InLine MLI
   Deixe marcada a caixa Ativar
   Clique em Próxima
7. **Uso de conector**
   Marque a opção:
   Somente quando houver uma configuração de regra de transporte que redirecione mensagens para este conector
   Clique em Próxima
8. **Roteamento**
   Selecione a opção:
   Rotear e-mail através desses hosts inteligentes
   Insira os IPs dos nodes do MailInspector
   Clique em Próxima
9. **Restrições de Segurança**
   Deixe marcada a opção Sempre usar o protocolo TLS para proteger a conexão (recomendado)
   Selecione a opção Qualquer certificado digital, inclusive certificados autoassinados
   Clique em Próxima
10. **E-mail de validação**
    Insira qualquer e-mail, para validação
    Clique em Próxima
11. Clique em Criar conector

2. Criando regra de saída atrelado ao conector de Saída ao MailInspector

1. Acesse o seu Office365 como administrador;
2. Acesse o módulo de administração do Exchange;
3. Vá em Fluxo de e-mail > Regras
4. Clique em Adicionar uma regra
5. **Definir condições de regra**
   Nome: Saída InLine MLI
   Aplicar esta regra se: O remetente
   Selecionar local do remetente: Inside the organization
   Faça do seguinte:
   Redirecionar a mensagem para: o seguinte conector > Saída InLine MLI
   Exceto se:
   As propriedades da mensagem: incluir o tipo de mensagem > Calendaring
   Clique em Salvar
   Clique em Avançar
6. **Definir configurações de regra**
   Modo de regra: Impor
   Severidade: Alta
   Clique em Avançar
7. **Revisar e Concluir**
   Clique em Concluir

Comunicação segura entre MailInspector e Microsoft 365 / G-Suite

Verifique se está ativado o protocolo TLS no MailInspector.

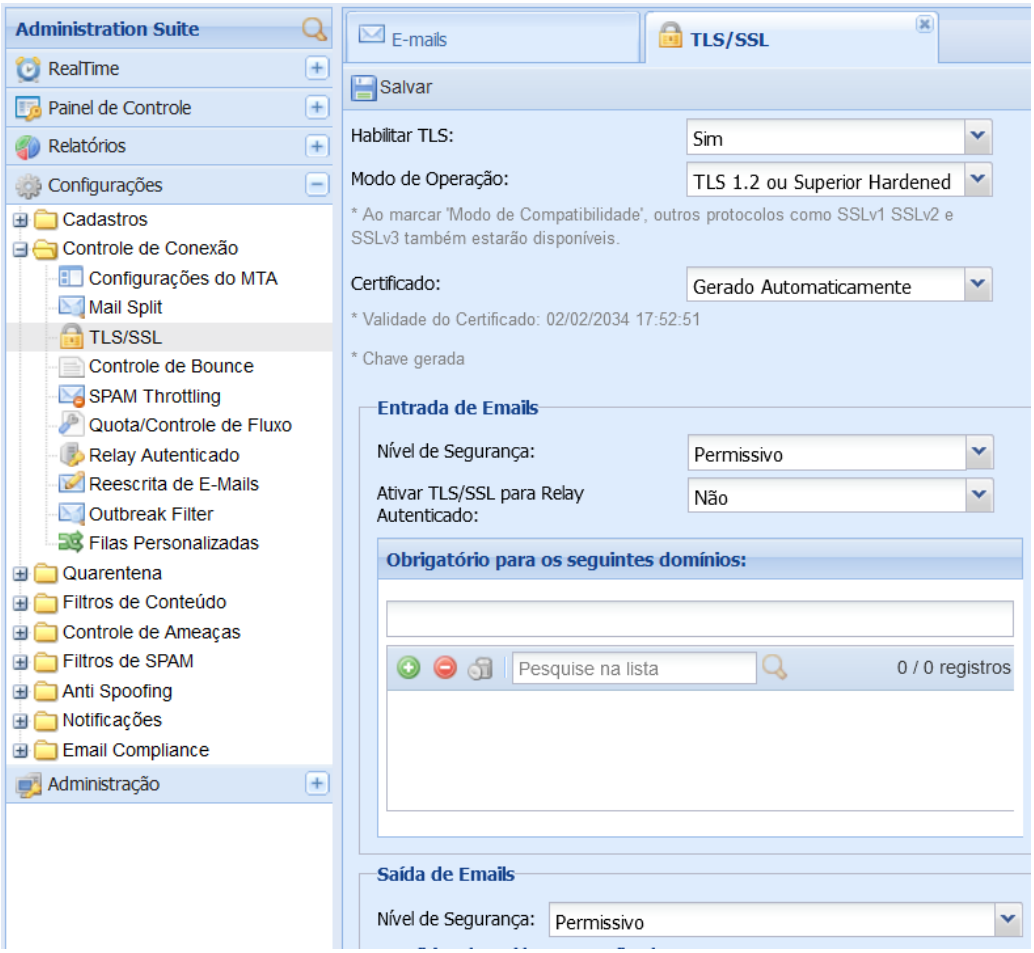
É necessário que esteja habilitado e configurado no modo de operação TLS 1.2 ou Superior Hardened. As outras versões foram mantidas por questão de compatibilidade, mas oferecem menor segurança, não sendo recomendado o uso delas.

Para esse processo, vá em:

Configurações > Controle de Conexão > TLS/SSL

Marque as seguintes opções:

1. Habilitar TLS: Sim
2. Modo de Operação: TLS1.2 ou Superior Hardened
3. Entrada de E-mails > Nível de Segurança: Permissivo
4. Saída de E-mails > Nível de Segurança: Permissivo



Com essas configurações você está indicando a comunicação com TLS ativado entre Microsoft e MailInspector, dessa forma a comunicação de e-mails (tanto envio, quanto recebimento) é completamente segura.

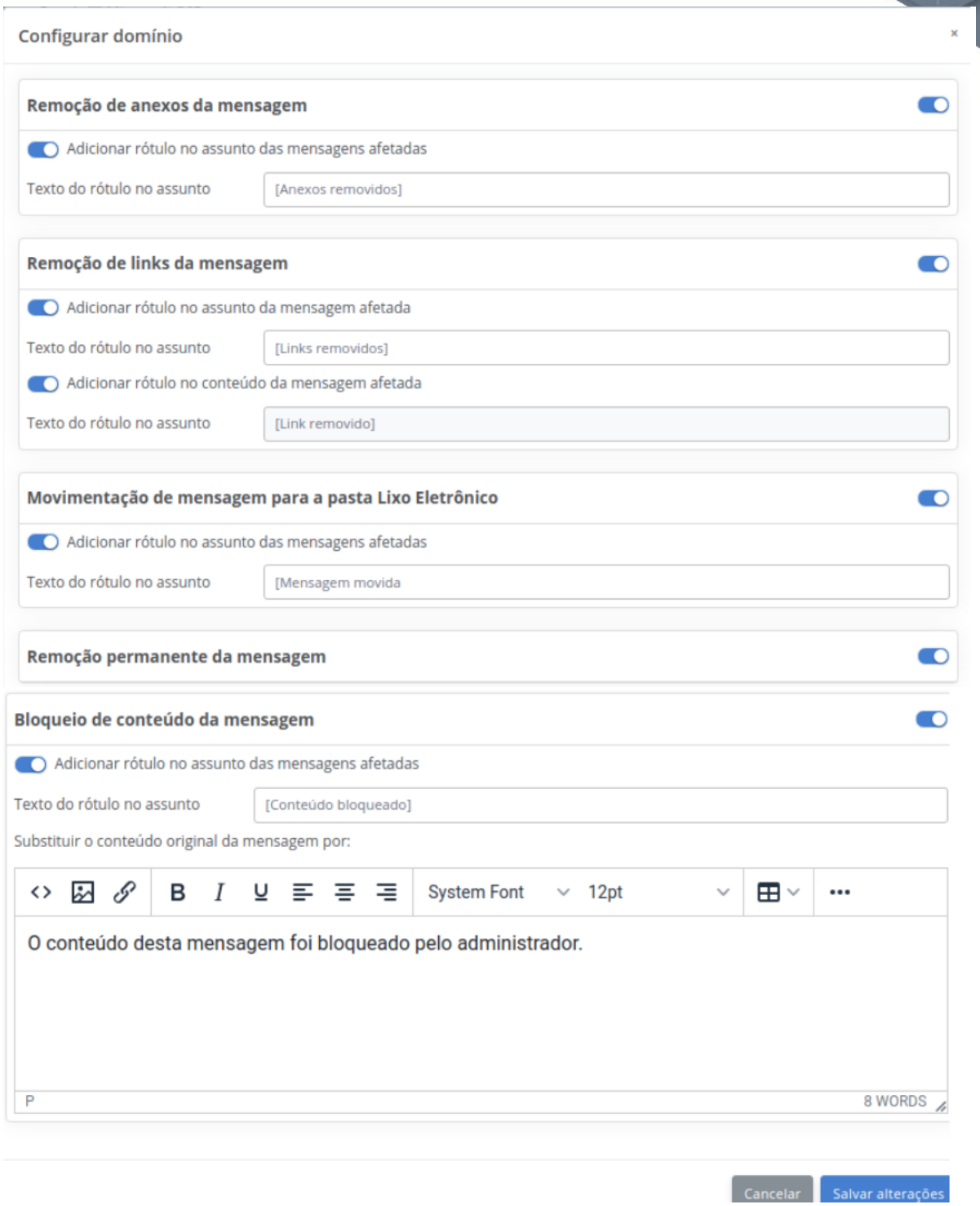
TLS v1.2	Cifra		Order	Strengh
TLS 1.2 ou Superior Hardened	xc030	ECDHE-RSA-AES256-GCM-SHA384	ECDH	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
	x9f	DHE-RSA-AES256-GCM-SHA384	DH	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384

Configuração de Orquestração (M-SOAR)

Configuração do M-SOAR permite personalizar quais ações o Administrador do MailInspector poderá efetuar em tempo real na caixa de e-mail do usuário do Microsoft 365 (diretamente na caixa no Exchange).

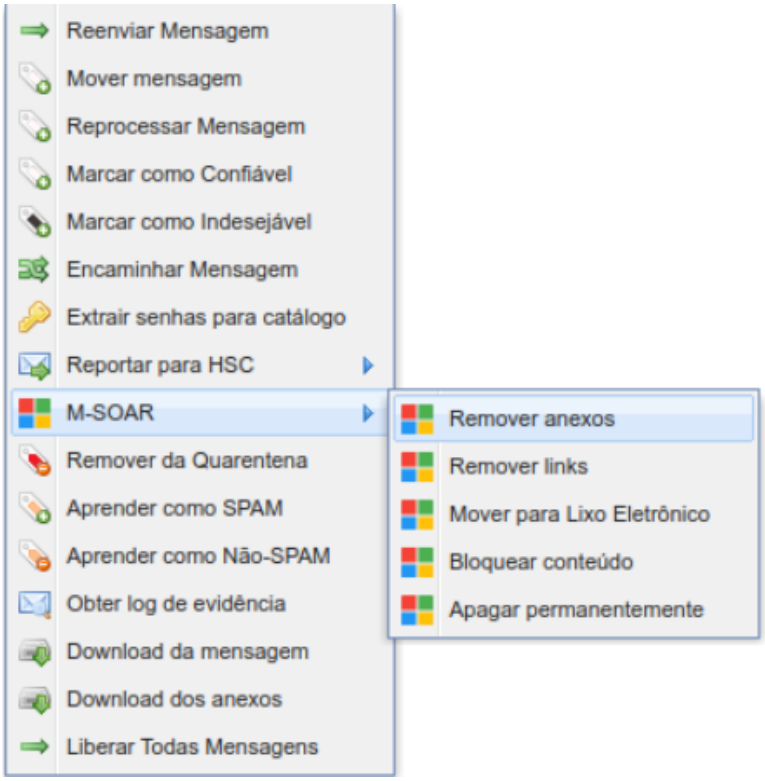
3. No MailInspector vá em Integrações > Microsoft 365 → M-SOAR e clique em Configurar. Logo com suas credenciais aprovadas na primeira etapa, clique em Sim, Configurar

4. Selecione Sim, configurar e configure as ações permitidas aos administradores do MailInspector e personalize os rótulos para as ações que serão registrados nas mensagens afetadas na caixa do usuário do Microsoft 365.



5. Ao final clique em Salvar alterações.
6. Clique no botão SALVAR
7. A partir deste momento o Administrador do MailInspector pode executar ações sobre as mensagens já entregues na caixa do usuário do Microsoft 365
   Para executar as ações acima, basta localizar a mensagem desejada no Painel Real Time → E-mail

e clicar com o botão direito sobre a mensagem e escolher a ação desejada:



Ações do M-SOAR

Remover anexos da mensagem - remove os anexos do e-mail selecionado no Office 365 do usuário final

Remover links da mensagem - remove os links contidos no -mail selecionado no Office 365 do usuário final

Mover para Lixo Eletrônico - move a mensagem para a pasta Lixo Eletrônico no Office 365 do usuário final

Bloquear Conteúdo - impede a visualização da mensagem no Office 365 do usuário final

Apagar a mensagem - apaga a mensagem no Office 365 do usuário final

Requisito para ações

O Administrador do MailInspector deve levar em consideração que as ações do M-SOAR são disponibilizadas exclusivamente para as mensagens já entregues no Tennant da Microsoft 365

Ativação de Add-On do MLI no Office 365

O Add-on para Microsoft 365 permite que os usuários dos serviços da Microsoft interagirem a partir de seu MS Outlook Web, MS Outlook 2016 e MS Outlook 2019 com o Mail Inspector. O usuário pode visualizar as suas mensagens em quarentena e liberar alguns tipos de quarentena além de adicionar ou remover registros de sua lista de endereços Confiáveis e Indesejáveis.

O procedimento a seguir descreve a ativação do Add-on do Mail Inspector no Microsoft 365.

Requisitos

- Ter ativado o M-SOAR (Orquestração)
- Possuir acesso administrativo ao MailInspector 5.2
- Já ter configurado o certificado digital no MailInspector (não pode ser o auto-assinado)
- Acesso Administrativo ao Exchange Admin Center (https://admin.exchange.microsoft.com/)

Guia Passo-a-Passo

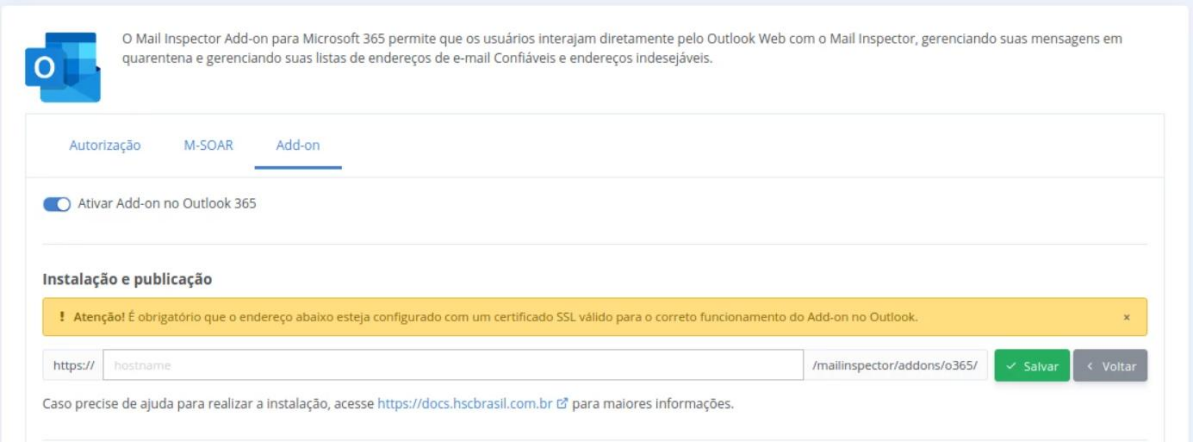
Este guia é dividido em 2 etapas que são executadas em sequência:

1. Configuração das Ações do Usuário no Add-On e
2. Deploy para os usuários do Microsoft 365.

Primeira Etapa

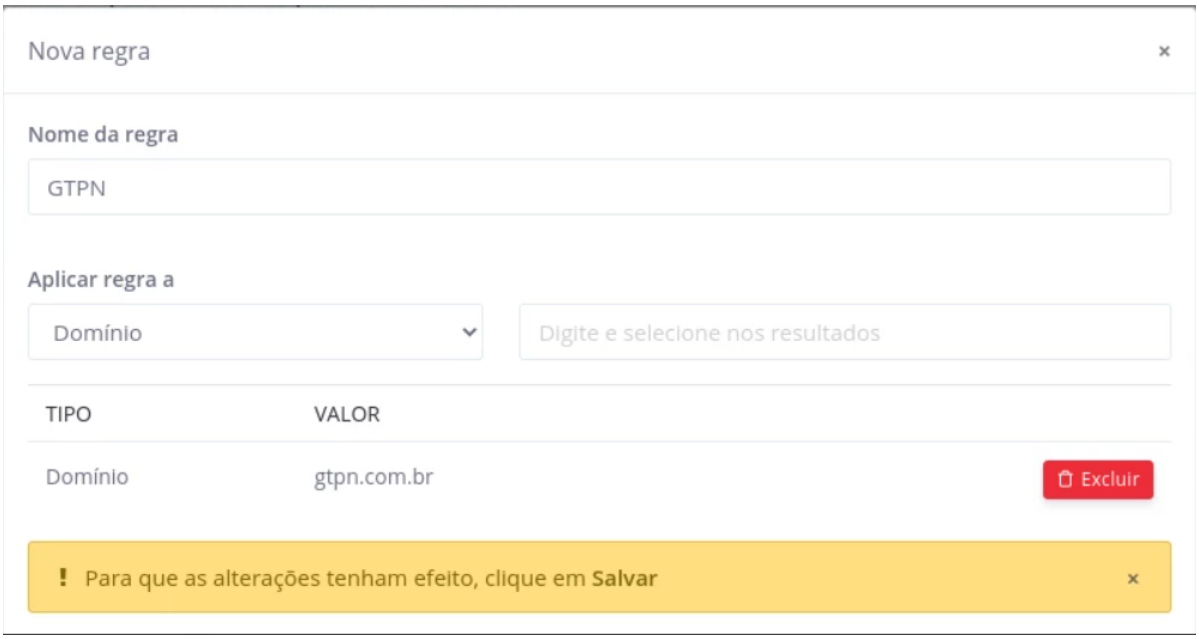
Configuração do Add-on: Corresponde à personalização das ações que o usuário do Add-on terá em seu cliente de e-mail Web ou instalação local do MS Outlook 2016 / 2019

1. Ative o Add-on no botão deslizante e informe o FDQN do seu Mail Inspector, clique em salvar e em seguida em Download. Salve o arquivo XML para a Segunda Etapa.



2. Configure as ações o usuário poderá executar em sua caixa de e-mail do Microsoft 365

3. Edite a regra Geral ou crie uma nova regra personalizada. Será permitido aplicar regras diferentes por domínio, Grupos LDAP, Grupos de Usuários ou Usuário.



4. Determine as ações e quarentenas que serão disponibilizadas na interface do usuário do Office 365

Ações disponíveis no menu do Add-on

- [x] Marcar como Confiável
- [x] Gerenciar Quarentena
- [x] Marcar como Indesejável
- [x] Gerenciar listas Confiáveis/Indesejáveis
- [x] Reportar ao Administrador

Quarentenas acessíveis aos usuários

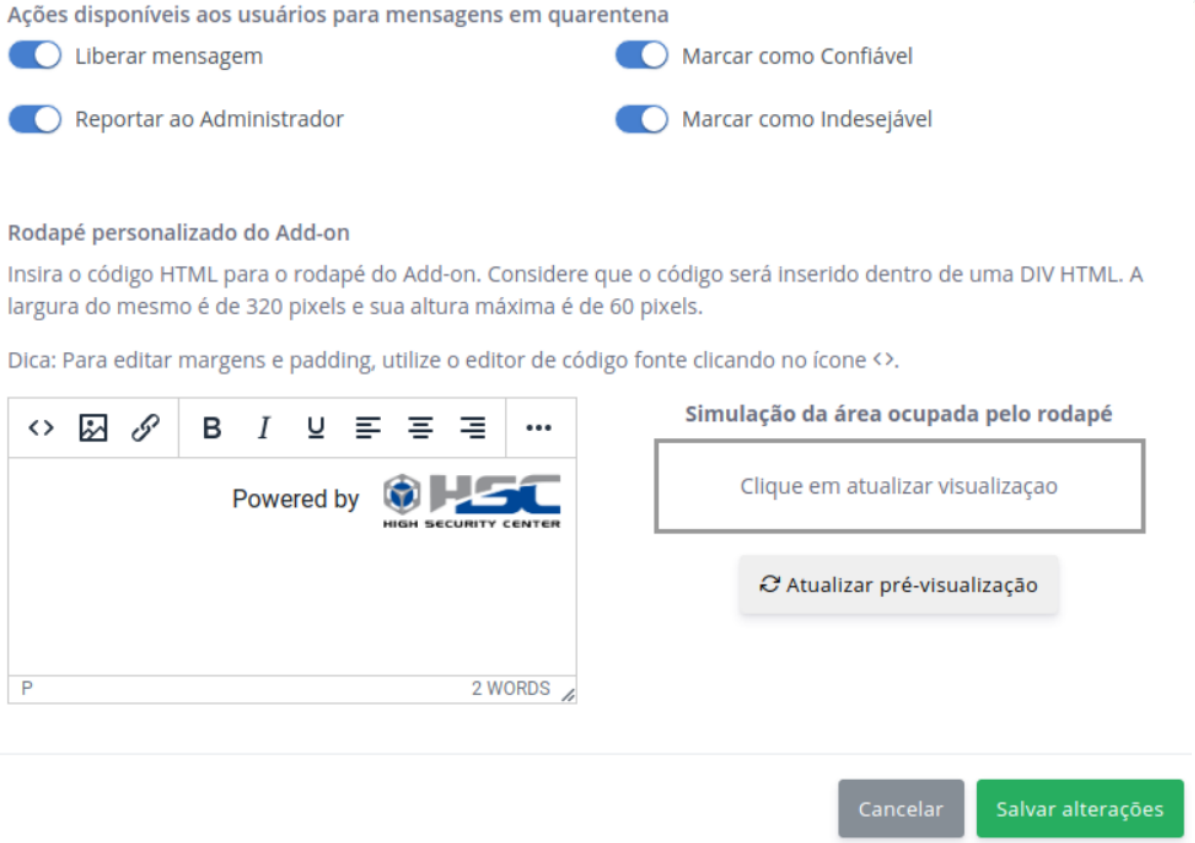
Quarentenas do sistema

- [x] Todas
- [x] ATP
- [x] Blacklist
- [x] Bulk Mail
- [x] Conteúdo Adulto
- [x] Conteúdo Bloqueado
- [x] Controle de Surto/Comportamento Anômalo
- [x] DLP/Auditoria
- [x] Fraude de E-mail / E-mail Impostor
- [x] Malware
- [x] Outro Bloqueio
- [x] Phishing
- [x] Provável SPAM
- [x] SPAM
- [x] Spoofing
- [x] Tamanho Excedido
- [x] Vírus
- [x] Whitelist

Quarentenas customizadas

- [x] Todas
- [x] URL MALICIOSAS

5. Determine as ações permitidas paras mensagens em quarentena. É possível personalizar o rodapé.



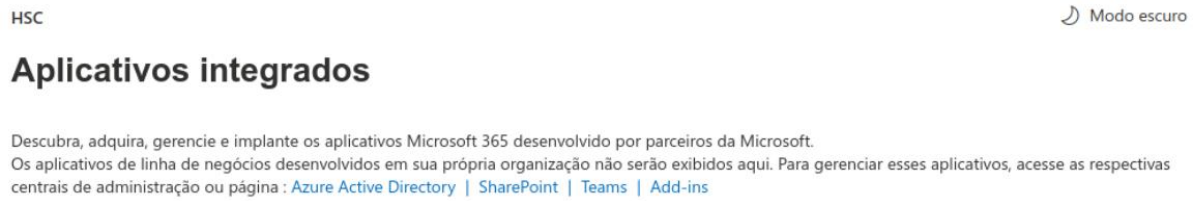
Somente é permitido ao usuário liberar mensagens em quarentena do tipo SPAM, Provável SPAM e Bulk Mail.

Não é possível liberar ameaças como vírus, malware e phishing.

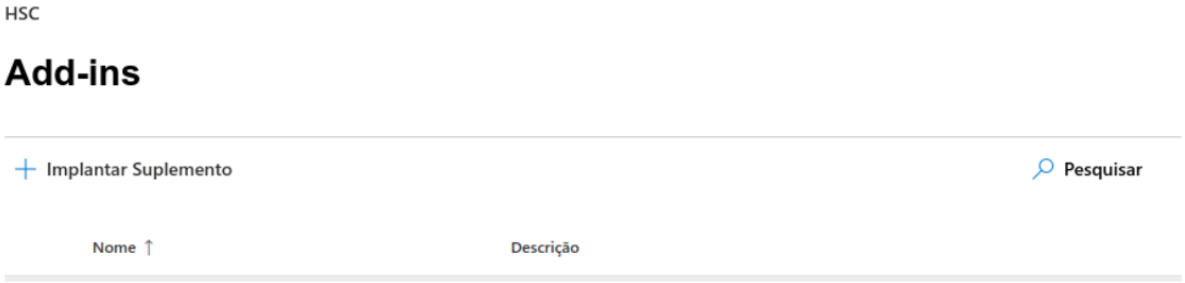
Segunda Etapa

Deploy do Add-on: Corresponde à implementação do Add-on nas configurações do domínio no ambiente de administração do Microsoft 365 (https://admin.microsoft.com/). Permite ao administrador do Microsoft 365 implementar apenas para alguns usuários ou grupos, conforme sua preferência.

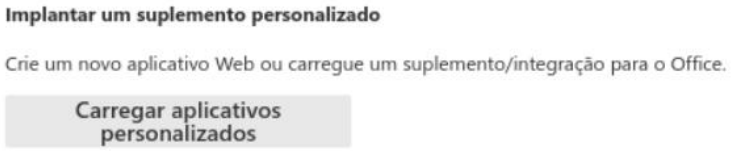
1. Acesse o Portal de Administração do Microsoft 365 como Administrador.
2. Acesse https://admin.microsoft.com/ e navegue em Configurações > Aplicativos Integrados
   Clique em Add-ins (https://admin.microsoft.com/Adminportal/Home#/Settings/AddIns)



3. Em Add-ins, clique em + Implantar Suplemento.

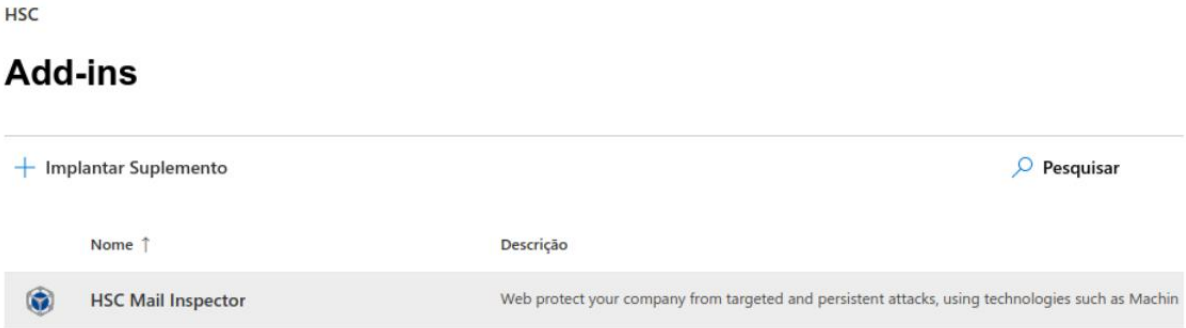


4. Na janela lateral que será apresentada, clique em PRÓXIMO e selecione Implantar um Suplemento Personalizado



5. Clique em Escolher Arquivo e selecione o arquivo .XML obtido na Terceira Etapa. Clique em CARREGAR

Deve abrir o Add-On, conforme imagem a seguir:

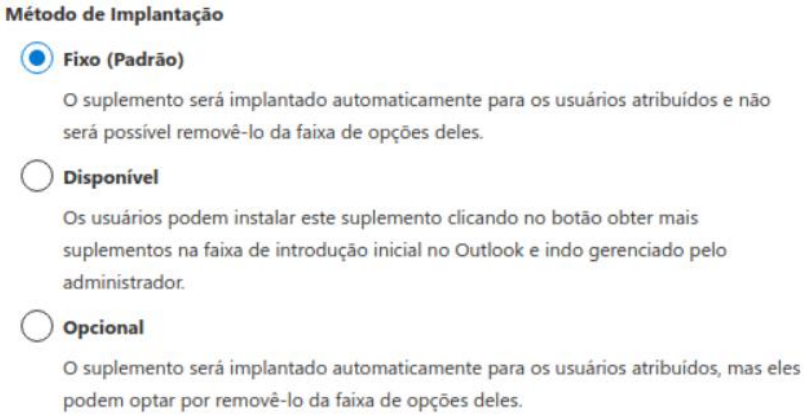


Recomendação

Para minimizar impactos aos usuários finais, recomenda-se realizar a implementação para um usuário ou grupo de usuários, e então implementar para toda a corporação.

6. Selecione as opções da Implementação e IMPLANTAR

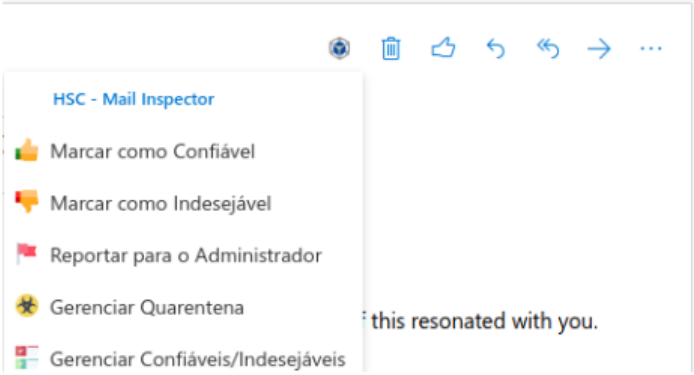
7. É possível permitir ao usuário gerenciar a ativação e utilização ou não. Recomenda o método Fixo (Padrão)



Atenção

É necessário aguardar 24h para disponibilizar o Add-on após sua ativação para os usuários ou grupos determinados.

8. Após o período de 24h, faça logoff e login, vá ao painel de e-mails e clique no Ícone da HSC. Serão exibidas as ações a seguir:



Ações do Add-On	
Marcar como Confiável	Adiciona o remetente da mensagem na lista Confiável do usuário no MailInspector (Allow List)
Marcar como Indesejável	Adiciona o remetente da mensagem na lista Indesejável do usuário no MailInspector (Block List)
Reportar para o Administrador	Remete uma cópia da mensagem para o Administrador do MailInspector • Como SPAM; • Como PHISHING; • Como AMEAÇA (Virus/Malware); Uma vez reportado, o sistema de Inteligência Artificial atua sobre o e-mail, validando se é realmente o tipo de e-mail informado pelo usuário, ao mesmo tempo em que é enviada uma cópia do e-mail ao administrador do sistema, permitindo análise manual e ações manuais sobre ele. O sistema de Inteligência Artificial além de validar o e-mail, faz a aprendizagem automática de acordo com a classificação do e-mail, analisando vários pontos dele, desde conteúdo, até origem/destino, frequência de envio/recebimento, características do anexo contido no e-mail, etc. Ainda na opção de Reportar para o Administrador, o usuário pode indicar a razão da notificação e selecionar a opção de Remover a mensagem automaticamente, dessa forma, ao enviar o e-mail como amostra para o administrador, ele será removido automaticamente da caixa postal do usuário.
Gerenciar Quarentena	Permite aos usuários visualizarem as mensagens que estão retidas na sua quarentena pessoal, podendo liberar as mensagens do tipo Provável SPAM, SPAM e Bulk Mail. Ao selecionar esta opção, abre o menu de seleção de opções de: • Período; • Assunto;

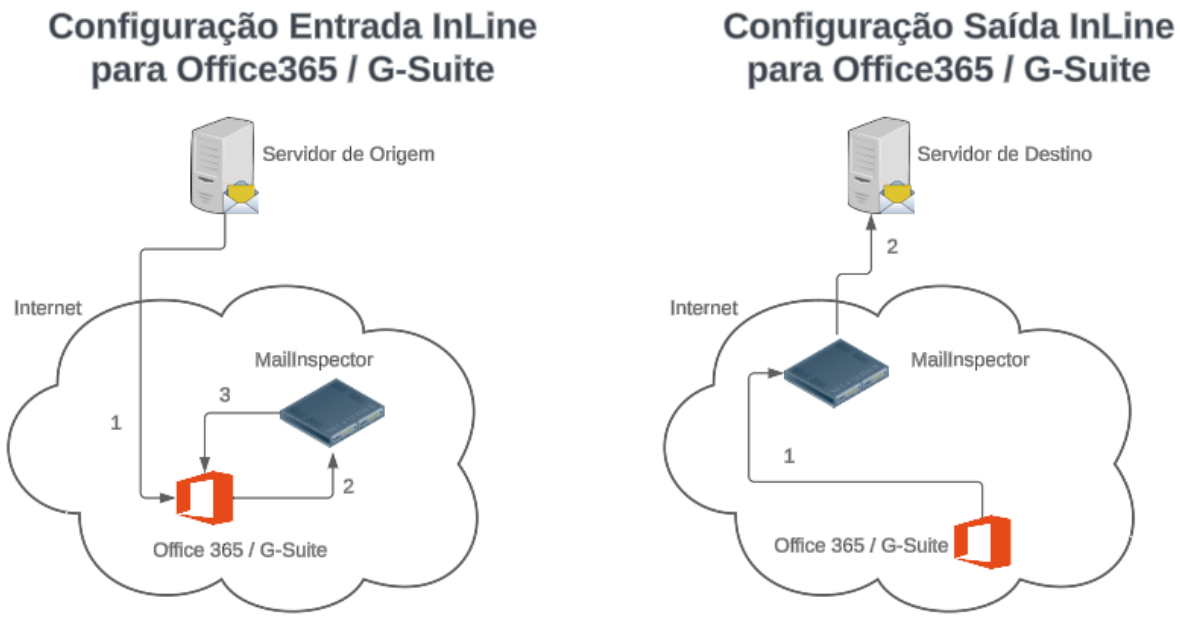
	• E-mail do remetente.
Gerenciar Confiáveis / Indesejáveis	Permite ao usuário adicionar ou remover registros de sua lista de remetentes: • Confiáveis; • Indesejados; Ao selecionar uma das opções, apresenta-se a lista de usuários já registrados no MailInspector como Confiáveis e/ou Indesejados;

Todo o processo de Importação dos Usuários, importação de e-mails, importação de grupos, ativação de Add-On, ativação de M-SOAR, é feito através de API's, mas de modo a ficar o mais transparente possível ao administrador e aos usuários da solução.

Apêndice 7 - Integração do MailInspector com G-Suite sem alteração no apontamento MX/DNS

Entrada de E-mails G-Suite sem alteração de MX

Exibe documento tem por finalidade mostrar a integração do MailInspector com Offi365, sem necessidade de mudança de MX e integração e importação de contas via API.



Modelo de Configuração de Entrada e Saída de E-mails sem alteração de MX

Configuração Entrada InLine (sem mudança no MX) para Office365 / G-Suite

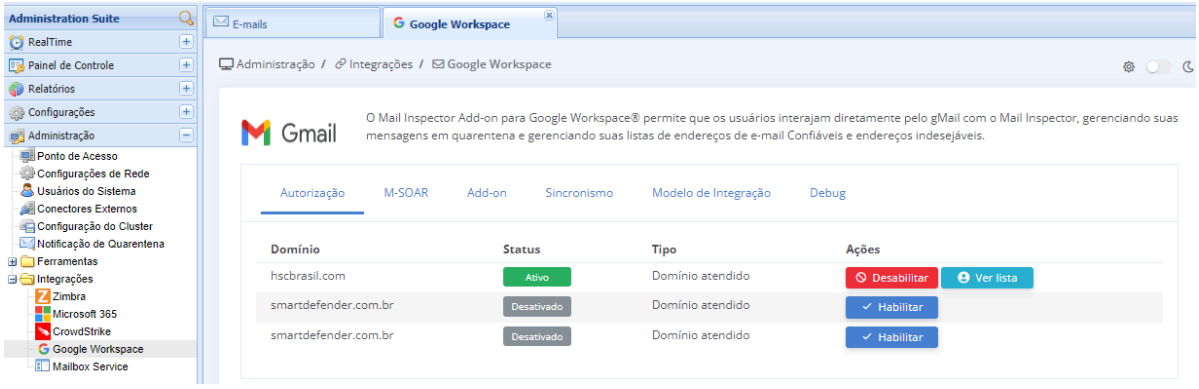
1. Os e-mails são direcionados ao Office365/G-Suite (que é o padrão quando se usa Office365 ou G-Suite), portanto, não há necessidade de mexer no MX/DNS;
2. Ao receber o e-mail, o Office365/G-Suite efetua a filtragem e encaminha para o MailInspector;
3. Após a filtragem por parte da Microsoft/Google, as mensagens são escaneadas novamente pelo MailInspector e os devolve ao Office365/G-Suite;

Configuração Saída InLine (sem mudança no MX) para Office365 / G-Suite

1. E-mail sai do Office365 / G-Suite e é entregue ao MailInspector;
2. É feita a filtragem do e-mail no MailInspector e entregue a Internet (servidor destino);

Configuração de conexão com G-Suite via API e configuração de M-SOAR

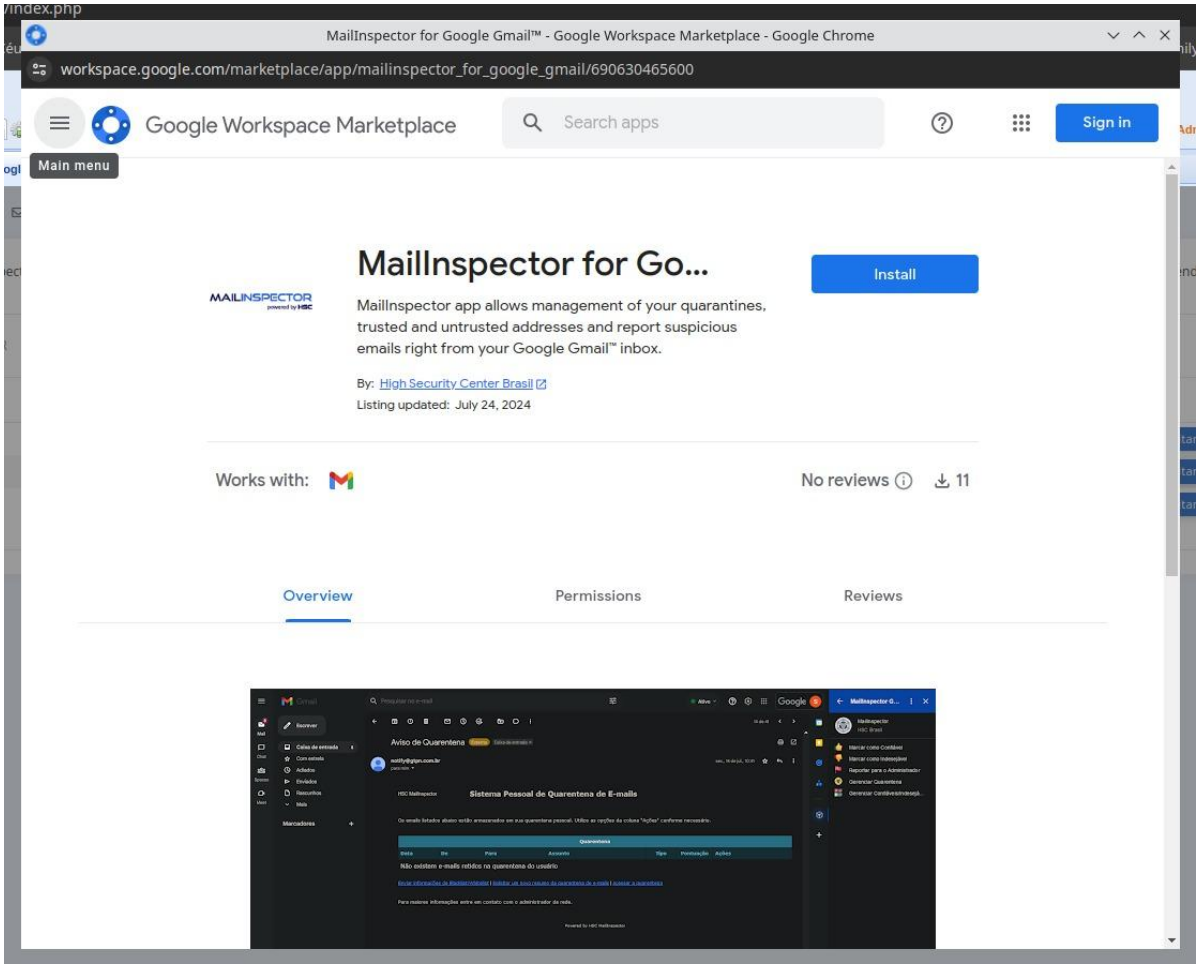
Primeiramente temos que configurar a conexão do MailInspector com o G-Suite. Para isso, vá em: Administração > Integrações > Google Workspace



1. Serão exibidos todos os domínios protegidos pelo Mail Inspector. Escolha o domínio que deseja ativar a integração e clique em Habilitar.

2. Na nova janela, informe a conta do administrador do serviço G-Suite

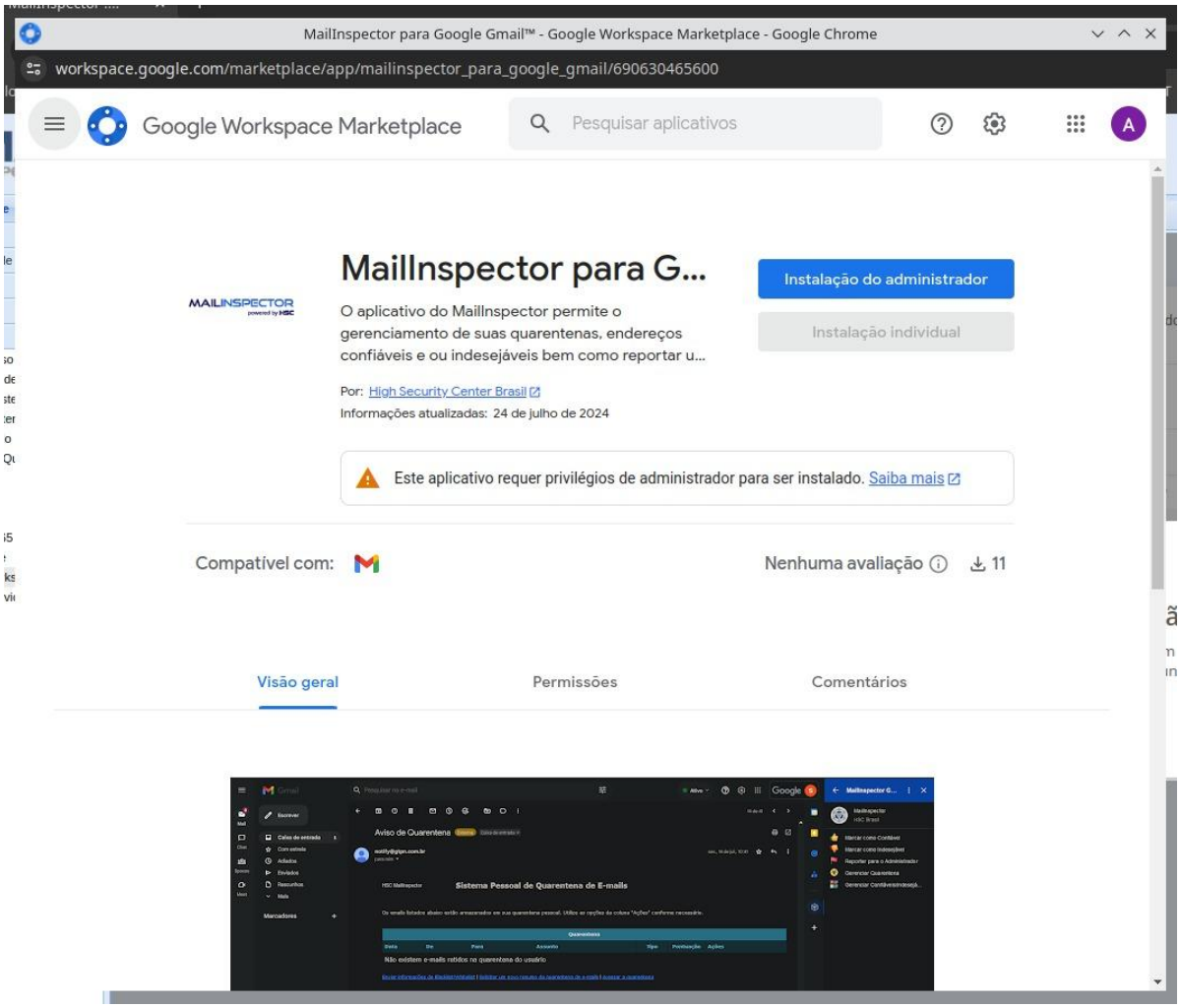
3. Ao fer isso, será aberta a tela de login (canto superior direito).



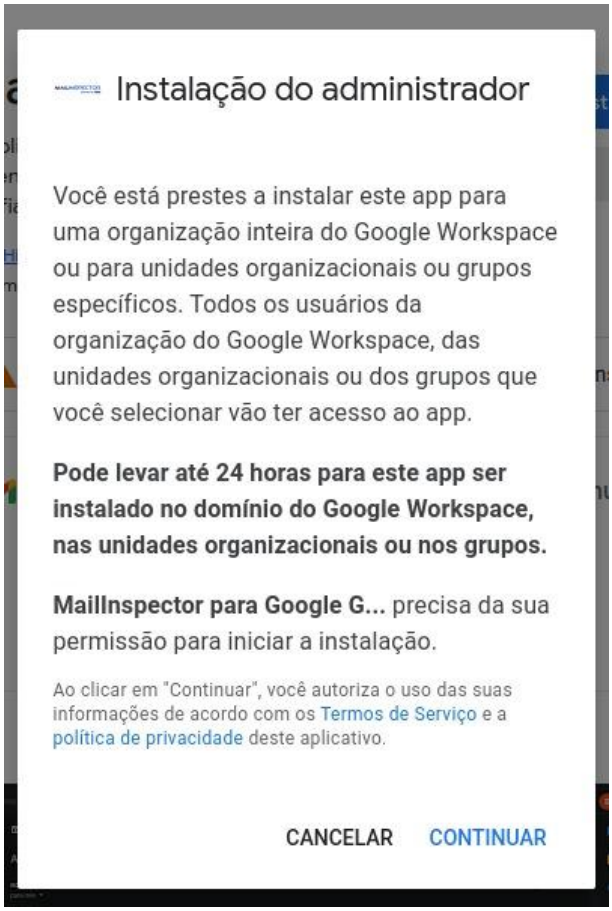
Ao mesmo tempo aparecerá uma tela de Autorização de integração com contador em segundos,

para você autenticar a sua senha.

4. Uma vez autenticado, clique em Instalação do Administrador

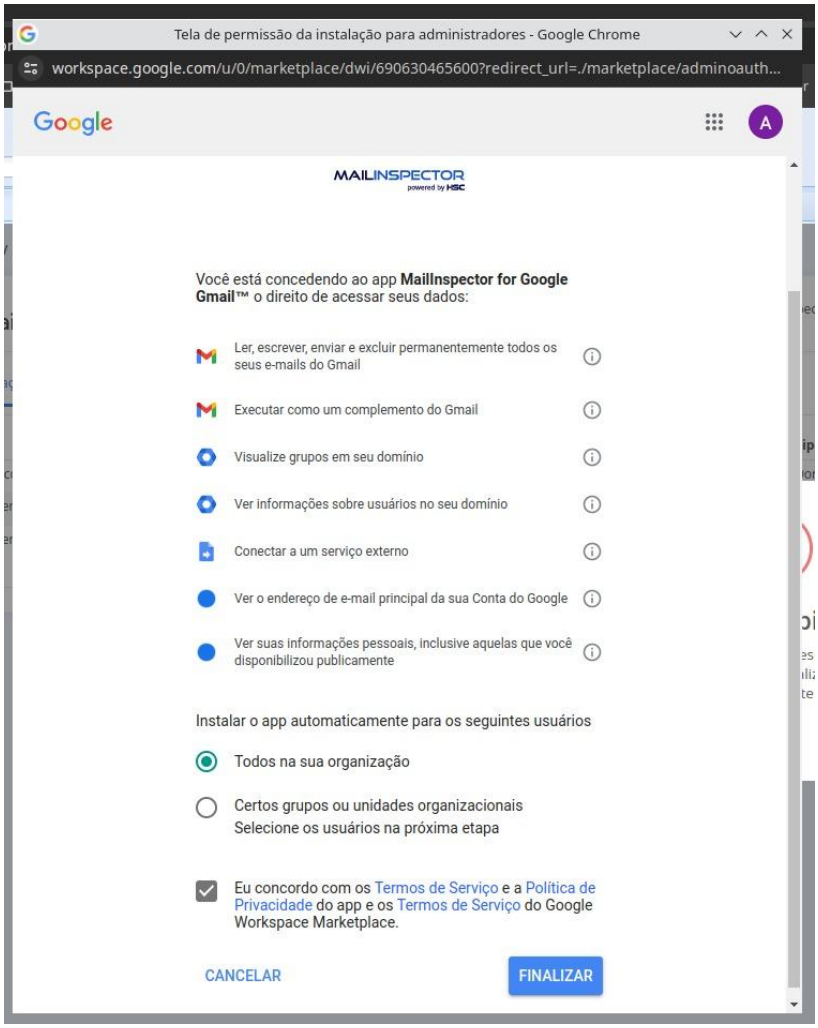


5. Depois de clicar em Instalação do administrador, será aberta janela de aviso. Clique em continuar.



6. Será apresentada a tela de concordância com os termos de uso, bem como indicação das permissões necessárias para a integração do MailInspector com o G-Suite. Marque o box de Eu concordo com os Termos de Serviço e Política de Privacidade do app e os Termos de Serviço do Google Workspace Marketplace.

Depois marcado o box, clique em FINALIZAR

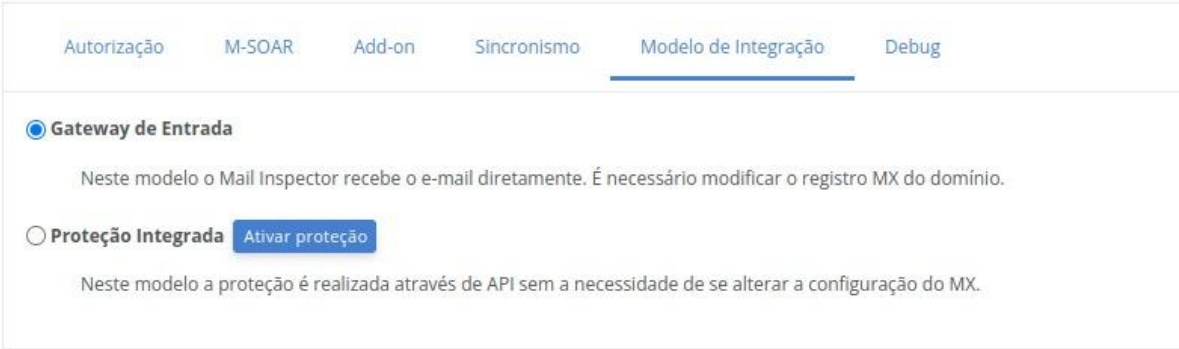


7. Será indicado que o MailInspector foi instalado no G-Suite. clique em CONCLUÍDO.

8. Após clicado em CONCLUÍDO, você pode configurar as ações de M-SOAR, ou deixar parta depois. Sugerimos que seja - **Não, manter o padrão** - Ao qual serão mantidas as ações padrão do M-SOAR, sem necessidade de alteração.

Configuração Entrada e Saída de E-mails para G-Suite Inline (sem alteração de MX)

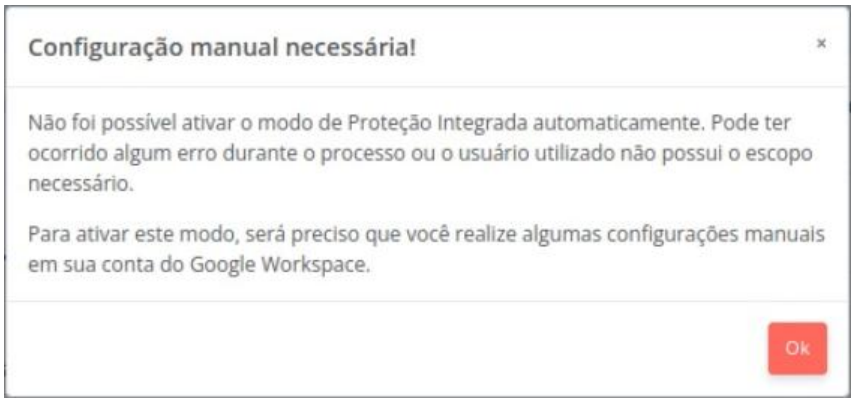
Por padrão o MailInspector permite que as configurações InLine sejam automáticas, bastando selecionar a opção Proteção Integrada.



Caso ocorra alguma falha de configuração automática, será necessária a configuração manual, para isso, basta seguir as etapas indicadas a seguir, de acordo com o tipo de servidor de e-mail utilizado (G-Suite ou Office365).

- **Por Gateway de Entrada:** É o processo em que é feito o apontamento dos e-mails para o MailInspector. Esse apontamento é através de mudança do MX no DNS da empresa.
- **Proteção Integrada:** Não há a necessidade de apontar o MX no DNS da empresa, basta configurar o Office365/G-Suite para que ao receberem os e-mails, eles sejam redirecionados ao MailInspector, que os filtrarão e os devolverá ao servidor Office365/G-Suite.
  Essa configuração poderá ser de forma automática, sem necessidade de intervenção ou criação de regras por parte do administrador, somente será necessária a intervenção manual em determinados casos, como por exemplo falta de permissão do administrador para acesso automático do MailInspector sobre o Office365/G-Suite, ou falha de comunicação, etc.

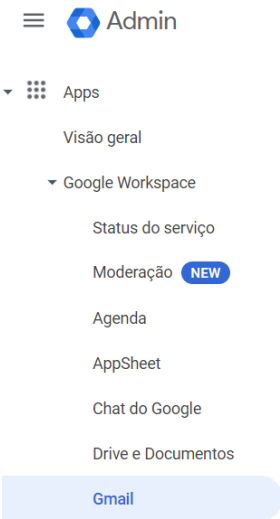
Caso ocorra alguma falha de configuração automática, será necessária a configuração manual, para isso, basta seguir as etapas indicadas a seguir, de acordo com o tipo de servidor de e-mail utilizado (G-Suite ou Office365).



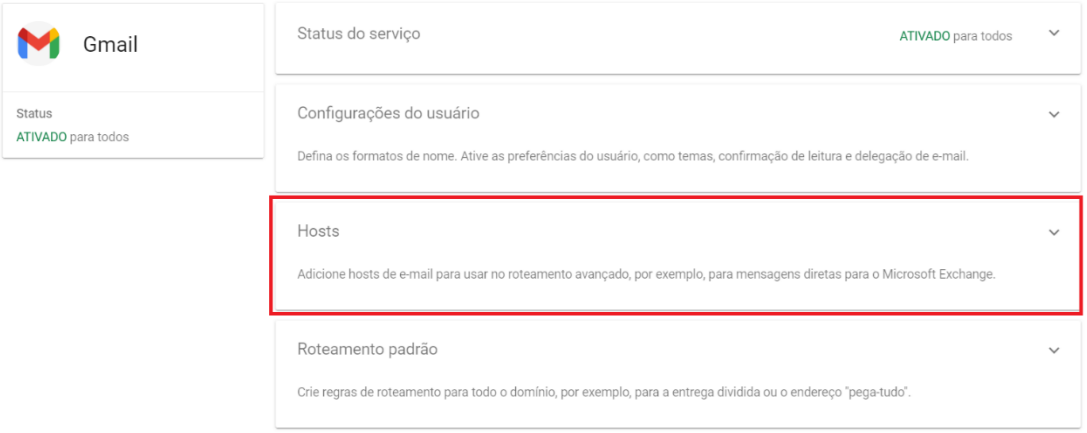
Acesse a sua conta de G-Suite pelo Google Admin Console.

Etapa 1: Adicionar os nodes de filtragem

1. Entre no Google Admin Console. (admin.google.com)
2. No painel de navegação esquerdo, clique em Apps > Google Workspace > Gmail.

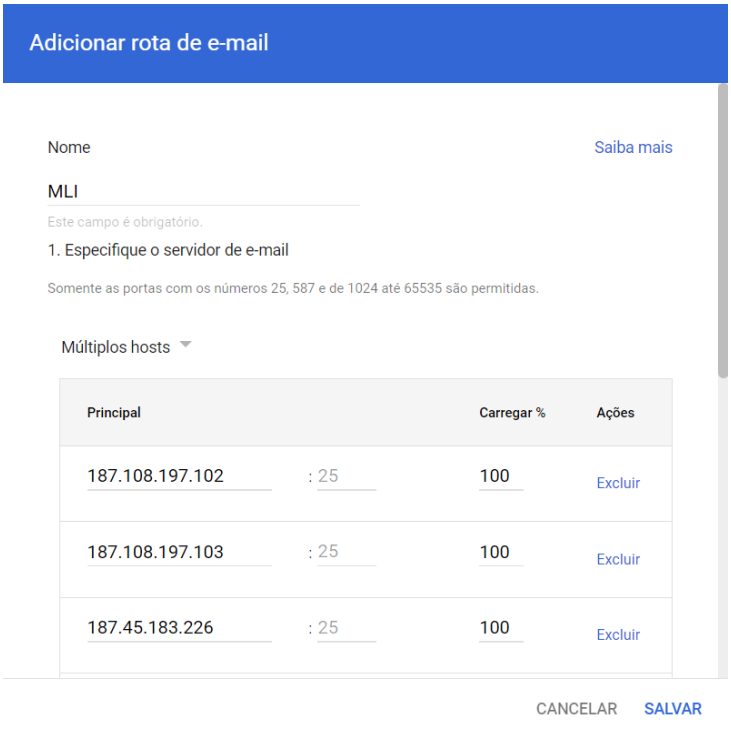


3. Clique em Hosts.



4. Clique em ADICIONAR ROTA.
5. Em Nome do rupo de NODES que você irá cadastrar. Para saber quais são os hostnames destes node, entre em contato com o suporte da HSCBRASIL. Como exemplo, vamos criar os nodes da nuvem MLICLOUD, através dos IPs.
6. Você pode adicionar uma única máquina ou múltiplas máquinas. No exemplo, vamos colocar múltiplas máquinas, ao qual o próprio Google irá gerenciar a alta disponibilidade e preferência de

entrega.



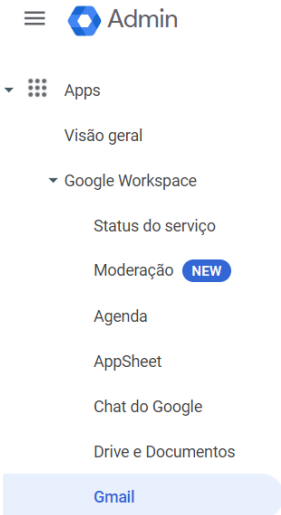
Repare que adicionei vários principais, não usamos os secundários.

Obs: Também é possível usar HOSTNAME por exemplo: **mx-balancer.mlicloud.com** em vez de IP.

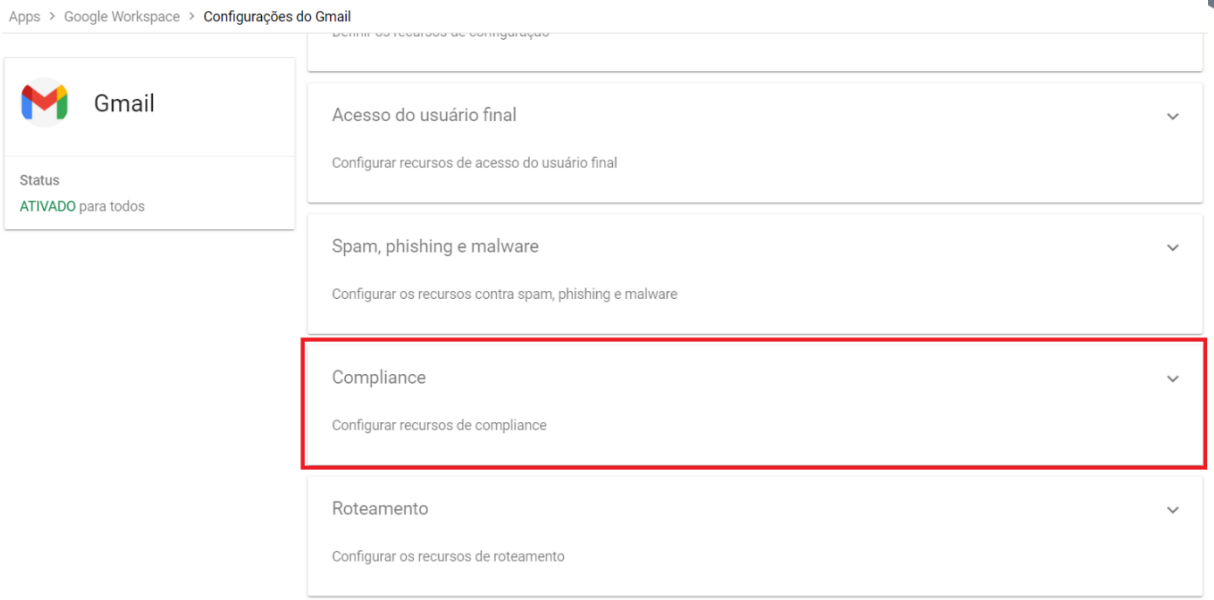
7. Digite o número das portas como 25 e 100% em carregar, para todas os nodes incluídos.
8. Em Opções, **desmarque** a caixa de seleção - Exigir um certificado assinado pela autoridade de certificação (recomendado).
9. Clique em Salvar.

Etapa 2: Criar regra de Entrada de E-mails e redirecionamento se necessário

1. No painel de navegação esquerdo, clique em Apps > Google Workspace > Gmail



2. Role para baixo e clique em Compliance

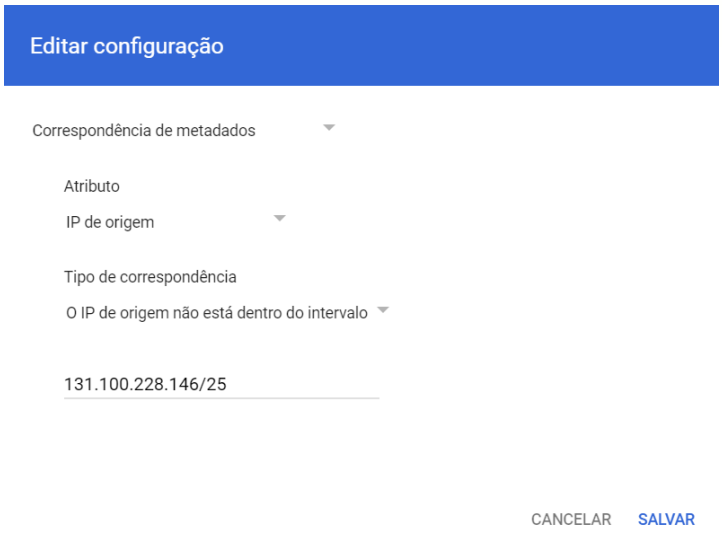


3. Clique em Compliance de conteúdo.
4. Essa opção nos permite criar regra de redirecionamento perante determinadas condições.
5. Vamos criar três regras de compliance:
    a. Inbound (E-mails de Entrada);
    b. Interno (E-mails Internos);
    c. Outbound (E-mails de Saída);

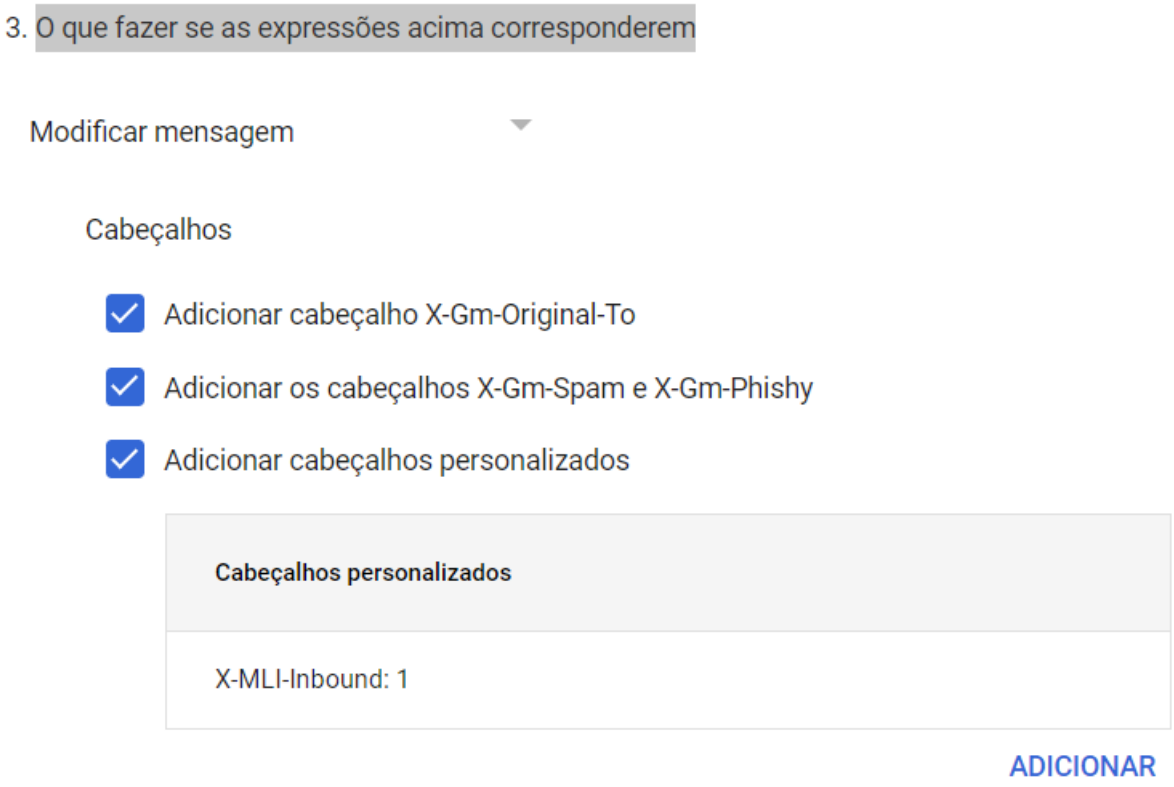
Regra Inbound

6. Clique em ADICIONAR REGRA
7. Na regra Inbound indique em Compliance do conteúdo o nome da regra (Inbound)
    a. Mensagens de e-mails afetadas: Recebidas
    b. Adicionar as expressões que descrevem o conteúdo que você quer pesquisar em cada mensagem: Se QUALQUER UMA das seguintes opções coincidirem com a mensagem
    c. Correspondência de Metadados
    d. Atributo: IP de origem
    e. Tipo de correspondência: O IP de origem não está dentro do intervalo

f. Repetir a entrada dos IP's, caso tenha mais de um IP a ser acrescentado, clicando em adicionar e repetir a ação de inserir IP.



8. O que fazer se as expressões acima corresponderem: Modificar mensagem



Assunto

☐ Adicionar assunto personalizado

Rota

☑ Alterar rota

☑ Também redirecionar spam

☐ Suprimir rejeições deste destinatário

MLI (mail.smartdefender.com.br)

Roteamento normal

MLI (mail.smartdefender.com.br)

Destin

☐ Alterar destinatário do envelope

Spam

☐ Ignorar o filtro de spam para esta mensagem

Em ROTA, marque a opção Alterar rota e marque Também redirecionar spam e escolha a opção MLI

Role a tela até SPAM e escolha a opção Ignorar o filtro de spam para esta mensagem

Destinatário do envelope

☐ Alterar destinatário do envelope

Spam

☑ Ignorar o filtro de spam para esta mensagem

Anexos

☐ Remover anexos da mensagem

Entregar também a

☐ Adicionar mais destinatários

Criptografia (apenas para a entrega de agora em diante)

☐ Exigir transporte seguro (TLS)

Regra Interno

1. Clique em ADICIONAR OUTRA REGRA
2. Na regra Interno indique em Compliance do conteúdo o nome da regra (Interno)
3. Selecione Interno – enviando
   Adicionar as expressões que descrevem o conteúdo que você quer pesquisar em cada mensagem
   Se QUALQUER UMA das seguintes opções coincidir com a mensagem
   Expressões
   Local: Cabeçalhos completos
   Não contém texto: X-MLI-Internal

1. Mensagens de e-mail afetadas

- [ ] Recebidas
- [ ] Enviadas
- [x] Interno - enviando
- [ ] Interno - recebendo

2. Adicionar as expressões que descrevem o conteúdo que você quer pesquisar em cada mensagem

Se QUALQUER UMA das seguintes opções coincidir com a mensagem

Expressões
Local: Cabeçalhos completos Não contém texto: X-MLI-Internal

ADICIONAR

Correspondência de conteúdo avançado

Local

Cabeçalhos completos

Tipo de correspondência

Não contém texto

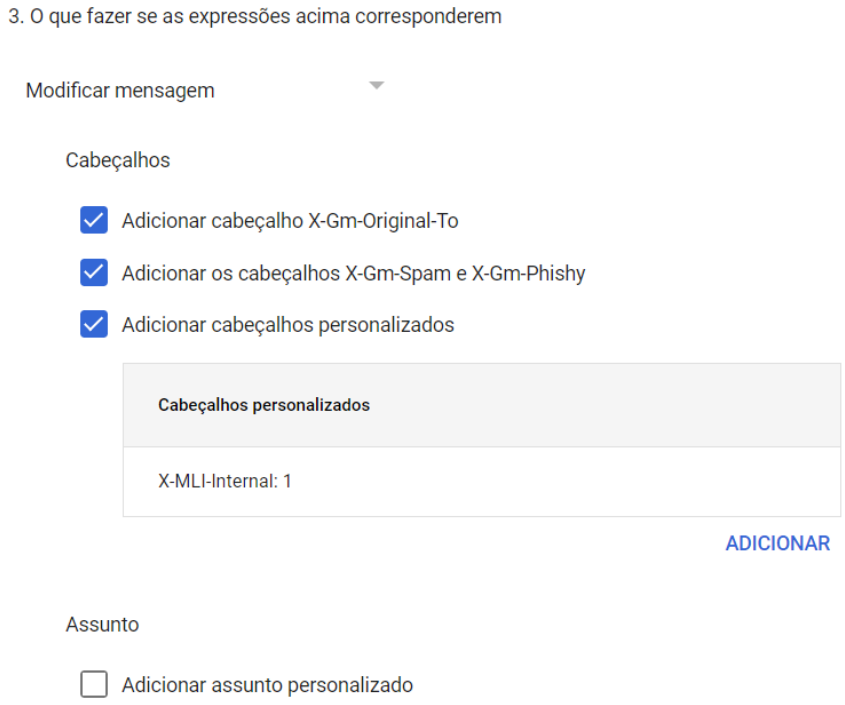
Conteúdo

X-MLI-Internal

Marque as opções Cabeçalhos:

a. Adicionar cabeçalho X-Gm-Original-To
b. Adicionar os cabeçalhos X-Gm-Spam e X-Gm-Phishy

c. Adicionar cabeçalhos personalizados: X-MLI-Internal: 1



Regra Oubound

1. Clique em ADICIONAR OUTRA REGRA

Na regra Outbound indique em Compliance do conteúdo o nome da regra (Outbound)

2. Selecione Enviadas

Adicionar as expressões que descrevem o conteúdo que você quer pesquisar em cada mensagem

Se QUALQUER UMA das seguintes opções coincidir com a mensagem

Expressões

Local: Cabeçalhos completos

Não contém texto: X-MLI-Outbound

Compliance do conteúdo Saiba mais

Outbound

1. Mensagens de e-mail afetadas

- [ ] Recebidas
- [x] Enviadas
- [ ] Interno - enviando
- [ ] Interno - recebendo

2. Adicionar as expressões que descrevem o conteúdo que você quer pesquisar em cada mensagem

Se QUALQUER UMA das seguintes opções coincidir com a mensagem

Expressões
Local: Cabeçalhos completos Não contém texto: X-MLI-Outbound

3. Marque as opções Cabeçalhos:

a. Adicionar cabeçalho X-Gm-Original-To

b. Adicionar os cabeçalhos X-Gm-Spam e X-Gm-Phishy

c. Adicionar cabeçalhos personalizados: X-MLI-Outbound: 1

3. O que fazer se as expressões acima corresponderem

Modificar mensagem

Cabeçalhos

- [x] Adicionar cabeçalho X-Gm-Original-To
- [x] Adicionar os cabeçalhos X-Gm-Spam e X-Gm-Phishy
- [x] Adicionar cabeçalhos personalizados

Cabeçalhos personalizados
X-MLI-Outbound: 1

ADICIONAR

Assunto

- [ ] Adicionar assunto personalizado

4. Em ROTA, marque a opção Alterar rota e indique a opção de rota MLI

Rota

- [x] Alterar rota
  - [ ] Também redirecionar spam
  - [ ] Suprimir rejeições deste destinatário

MLI (mail.smartdefender.com.br)

Destinatário do envelope

- [ ] Alterar destinatário do envelope

Spam

- [ ] Ignorar o filtro de spam para esta mensagem

Anexos

- [ ] Remover anexos da mensagem

5. Clique em Salvar

Comunicação segura entre MailInspector e Microsoft 365 / G-Suite

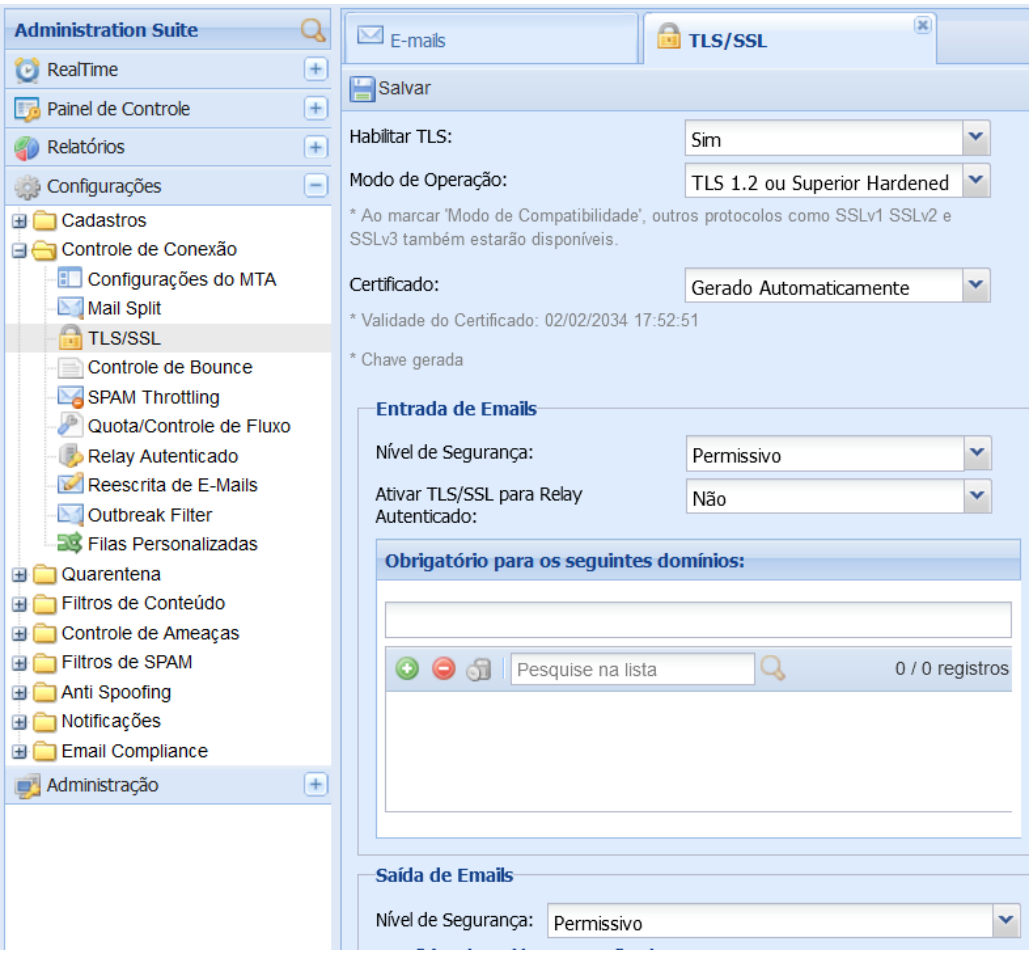
Verifique se está ativado o protocolo TLS no MailInspector.

É necessário que esteja habilitado e configurado no modo de operação TLS 1.2 ou Superior Hardened. As outras versões foram mantidas por questão de compatibilidade, mas oferecem menor segurança, não sendo recomendado o uso delas.

Para esse processo, vá em:
Configurações > Controle de Conexão > TLS/SSL

Marque as seguintes opções:

1. Habilitar TLS: Sim
2. Modo de Operação: TLS1.2 ou Superior Hardened
3. Entrada de E-mails > Nível de Segurança: Permissivo
4. Saída de E-mails > Nível de Segurança: Permissivo



Com essas configurações você está indicando a comunicação com TLS ativado entre G-Suite e MailInspector, dessa forma a comunicação de e-mails (tanto envio, quanto recebimento) é completamente segura.

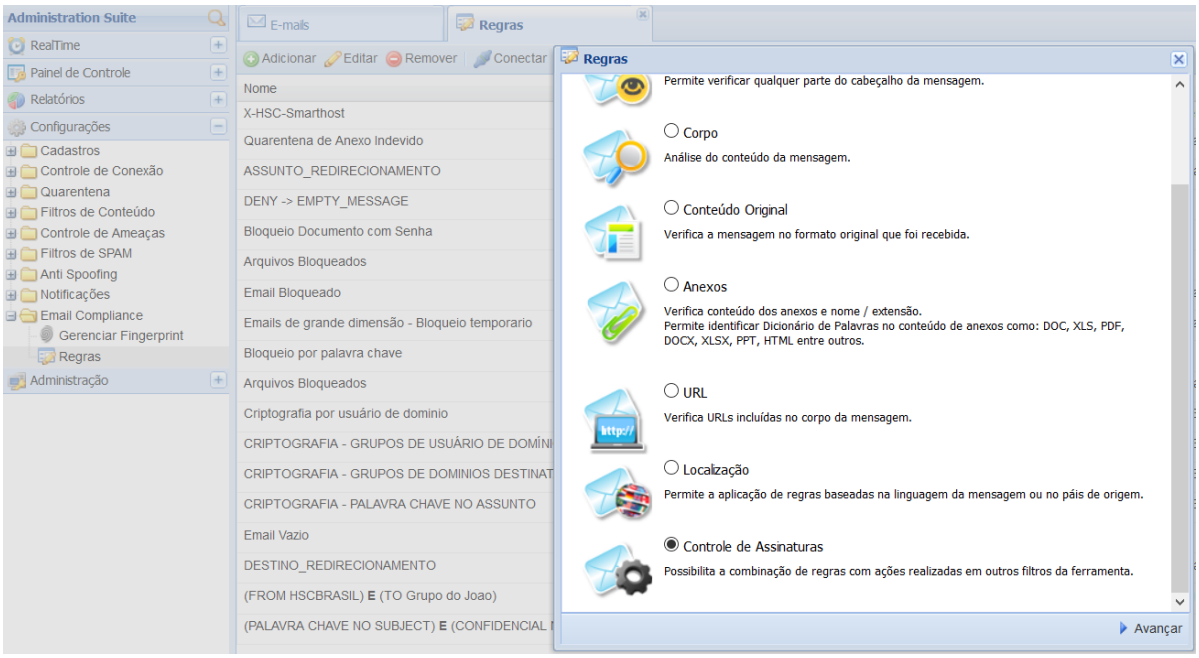
TLS v1.2	Cifra		Order	Strengh
TLS 1.2 ou Superior Hardened	xc030	ECDHE-RSA-AES256-GCM-SHA384	ECDH	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
	x9f	DHE-RSA-AES256-GCM-SHA384	DH	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384

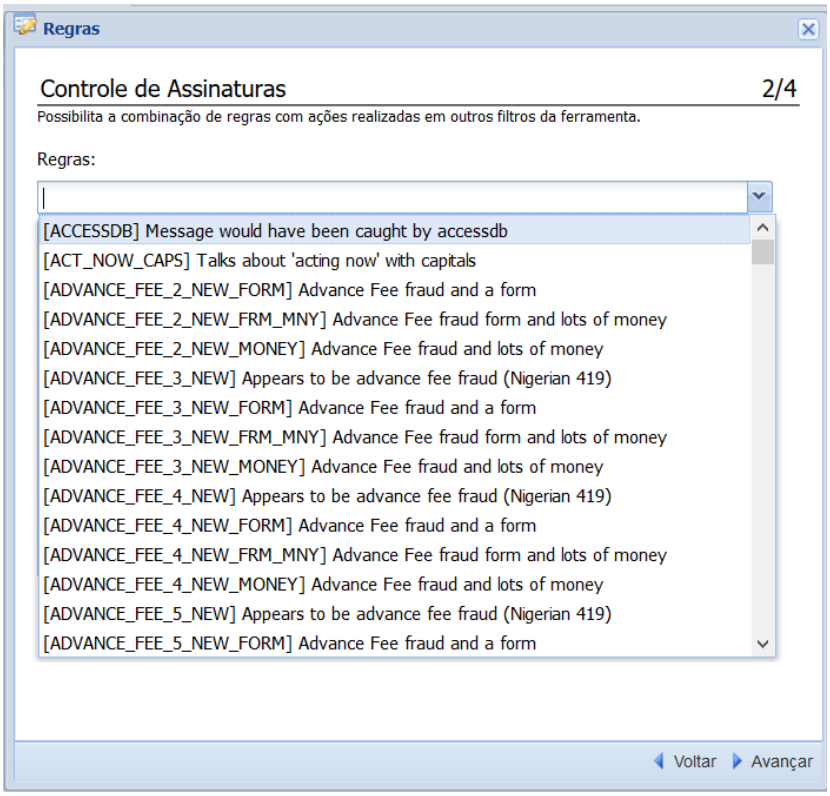
Apêndice 8 – Assinaturas

Existem duas formas de uso de assinaturas em regras/políticas de entrada ou saída dos e-mails no MailInspector:

1. E-mail Compliance;
2. Filtros de SPAM no módulo de Controle Avançado

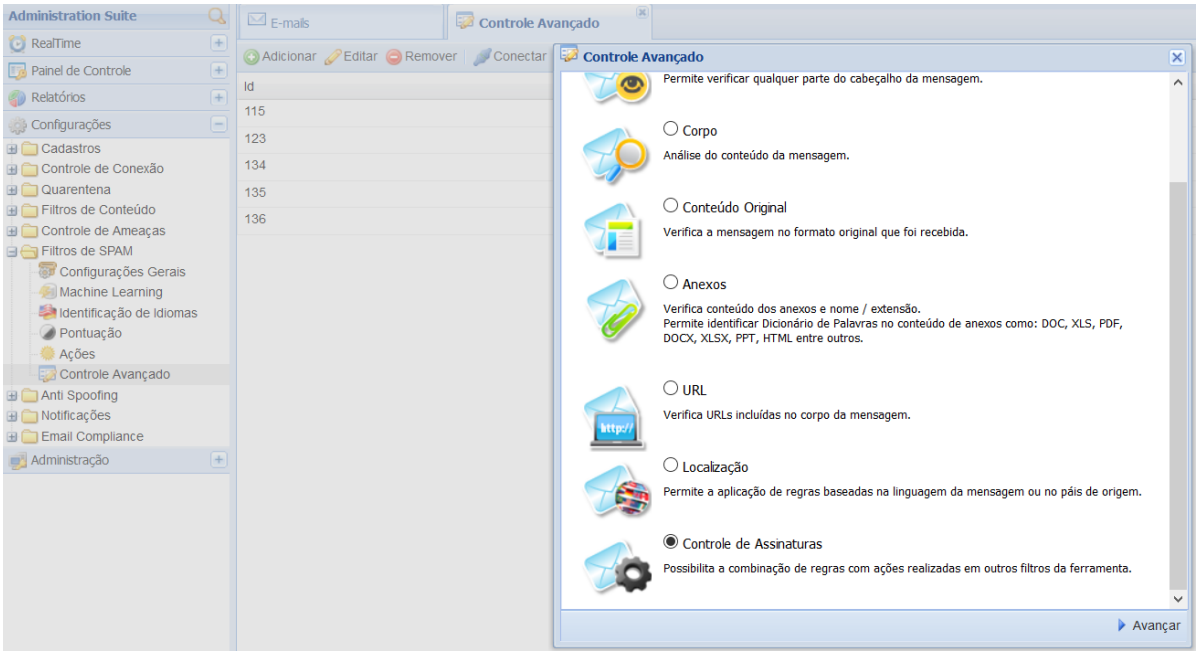
No E-mail Compliance:

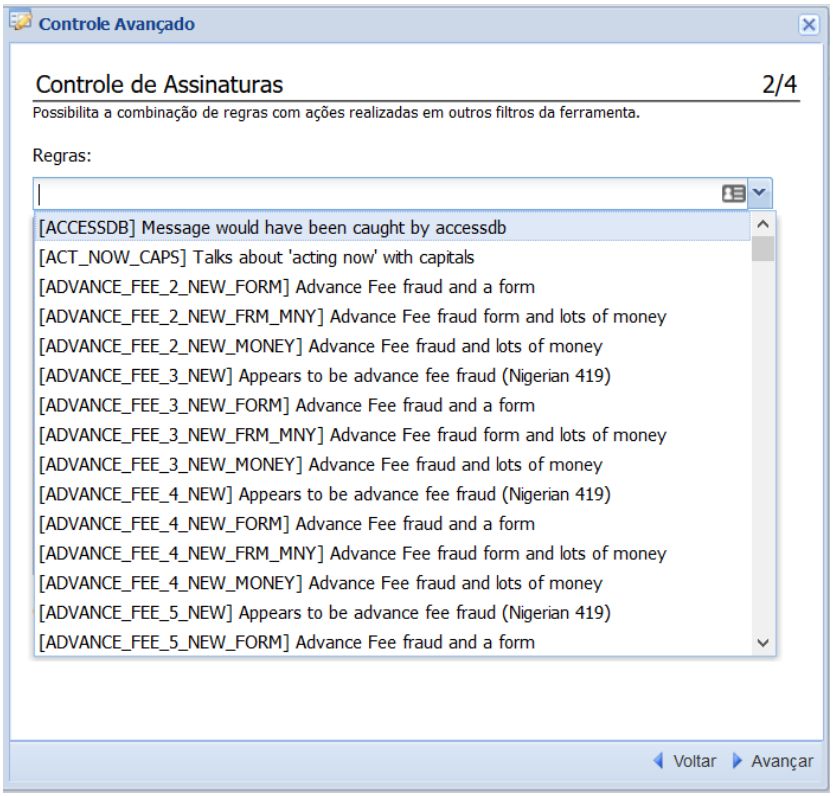




Após selecionada a regra que deseja utilizar, basta dar continuidade dela, selecionando a pontuação a ser atribuída. Após isso, basta salvar a Aplicar Configurações.

Em Filtros de SPAM > Controle Avançado





Após selecionada a regra que irá atuar, basta continuar e escolher a ação a ser tomada. Após isso, basta salvar a política e Aplicar Configurações, para que a regra passe a valer.

Importante salientar que toda e qualquer regra/política criada em E-mail Compliance, pode ser concatenada com outras regras, usando operadores lógicos, dessa forma será possível criar uma vastidão de políticas customizadas de acordo com a necessidade da empresa.

Seguem as principais assinaturas (mais utilizadas), com as devidas explicações para que o administrador possa usar tanto em E-mail Compliance, quanto em regras de SPAM, dessa forma possibilitando a criação das mais diversas regras/políticas de bloqueio/liberação/controle sobre os e-mails.

É possível criar regras até sobre reputação de origem do domínio/IP do e-mail, influenciando na sua pontuação ou bloqueando o e-mail, ou simplesmente removendo eventual anexo e prosseguindo com a entrega.

Principais assinaturas do MailInspector

Assinatura	Descrição Ingles	Descrição
AC_DIV_BONANZA	Too many divs in a row... spammy template	
AC_FROM_MANY_DOTS	Multiple periods in From user name	
AC_HTML_NONSENSE_TAGS	Many consecutive multi-letter HTML tags- likely nonsense/spam	
ACCT_PHISHING_MANY	Phishing for account information	Conta de phishing
ACT_NOW_CAPS	Talks about 'acting now' with capitals	
ADVANCE_FEE_3_NEW_MONEY	Advance Fee fraud and lots of money	
ALIBABA_IMG_NOT_RCVD_ALI	Alibaba hosted image but message not from Alibaba	
ALL_TRUSTED	Passed through trusted hosts only via SMTP	O email passou por servidores de confiança
AXB_XMAILER_MIMEOLE_OL_024C2	Yet another X header trait	
BAD_ENC_HEADER	Message has bad MIME encoding in the header	
BASE64_LENGTH_78_79	-	
BASE64_LENGTH_79_INF	base64 encoded email part uses line length greater than 79 characters	
BIGNUM_EMAILS_MANY	Lots of email addresses/leads- over and over	
BITCOIN_EXTORT_01	Extortion spam- pay via BitCoin	Combinações de palavras chaves com bitcoin utilizadas para SexTortion
BITCOIN_EXTORT_02		
BITCOIN_MALF_HTML	Bitcoin + malformed HTML	
BITCOIN_MALWARE	BitCoin + malware bragging	
BITCOIN_ONAN	BitCoin + [censored]	
BITCOIN_PAY_ME		
BITCOIN_SPAM_01	BitCoin spam pattern 01	
BITCOIN_SPAM_03	BitCoin spam pattern 03	
BITCOIN_SPAM_05	BitCoin spam pattern 05	
BITCOIN_XPRIO	Bitcoin + priority	
BODY_URI_ONLY	Message body is only a URI in one line of text or for an image	
BOGUS_MIME_VERSION	Mime version header is bogus	
CHARSET_FARAWAY_HEADER	A foreign language charset used in headers	
CN_B2B_SPAMMER	Chinese company introducing itself	
CTE_8BIT_MISMATCH	Header says 7bits but body disagrees	

DATE_IN_FUTURE_03_06	Date: is 3 to 6 hours after Received: date	
DATE_IN_FUTURE_06_12	Date: is 6 to 12 hours after Received: date	
DATE_IN_FUTURE_12_24	Date: is 12 to 24 hours after Received: date	
DATE_IN_PAST_03_06	Date: is 3 to 6 hours before Received: date	
DATE_IN_PAST_06_12	Date: is 6 to 12 hours before Received: date	
DATE_IN_PAST_12_24	Date: is 12 to 24 hours before Received: date	
DATE_IN_PAST_24_48	Date: is 24 to 48 hours before Received: date	
DATE_IN_PAST_96_XX	Date: is 96 hours or more before Received: date	
DC_GIF_UNO_LARGO	Message contains a single large gif image	
DC_PNG_UNO_LARGO	Message contains a single large png image	O email possui um único arquivo PNG
DEAR_EMAIL	Message contains Dear email address	
DEAR_FRIEND	Dear Friend? That's not very dear!	
DEAR_SOMETHING	Contains 'Dear (something)'	
DIET_1	Lose Weight Spam	
DIRECT_LOW_CONTRAST	Direct-to-MX + hidden text	
DKIM_ADSP_ALL	No valid author signature- domain signs all mail	
DKIM_ADSP_CUSTOM_MED	No valid author signature- adsp_override is CUSTOM_MED	
DKIM_ADSP_DISCARD	No valid author signature- domain signs all mail and suggests discarding the rest	
DKIM_ADSP_NXDOMAIN	No valid author signature and domain not in DNS	
DKIM_INVALID	DKIM or DK signature exists- but is not valid	
DKIM_SIGNED	Message has a DKIM or DK signature- not necessarily valid	
DKIM_VALID	Message has at least one valid DKIM or DK signature	
DKIM_VALID_AU	Message has a valid DKIM or DK signature from author's domain	
DOS_BODY_HIGH_NO_MID	High bit body and no message ID header	

DOS_OUTLOOK_TO_MX	Delivered direct to MX with Outlook headers	
DRUGS_ANXIETY	Refers to an anxiety control drug	
DRUGS_ERECTILE	Refers to an erectile drug	Referentes a medicamentos de ereção
DRUGS_ERECTILE_OBFU	Obfuscated reference to an erectile drug	Utilizado sistema de ofuscação, associado a termos de medicamento para ereção
DYN_RDNS_AND_INLINE_IMAGE	Contains image- and was sent by dynamic rDNS	
DYN_RDNS_SHORT_HELO_HTML	Sent by dynamic rDNS- short HELO- and HTML	
DYN_RDNS_SHORT_HELO_IMAGE	Short HELO string- dynamic rDNS- inline image	
DYNAMIC_IMGUR	dynamic IP + hosted image	
EMPTY_MESSAGE	Message appears to have no textual parts and no Subject text	Indica que a mensagem não tem conteúdo de texto- nem Título de e-mail
FAKE_REPLY_C	-	
FILL_THIS_FORM	Fill in a form with personal information	
FONT_INVIS_DIRECT	Invisible text + direct-to-MX	
FONT_INVIS_LONG_LINE	Invisible text + long lines	
FONT_INVIS_MSGID	Invisible text + suspicious message ID	
FORGED_HOTMAIL_RCVD2	hotmail.com 'From' address- but no 'Received:'	
FORGED_MUA_MOZILLA	Forged mail pretending to be from Mozilla	
FORGED_MUA_OUTLOOK	Forged mail pretending to be from MS Outlook	
FORGED_OUTLOOK_HTML	Outlook can't send HTML message only	
FORGED_OUTLOOK_TAGS	Outlook can't send HTML in this format	
FORGED_SPF_HELO	-	
FORGED_TELESP_RCVD	Contains forged hostname for a DSL IP in Brazil	
FORGED_YAHOO_RCVD	'From' yahoo.com does not match 'Received' headers	
FREEMAIL_ENVFROM_END_DIGIT	Envelope-from freemail username ends in digit	
FREEMAIL_FORGED_FROMDOMAIN	2nd level domains in From and EnvelopeFrom freemail headers are different	
FREEMAIL_FORGED_REPLYTO	Freemail in Reply-To- but not From	

FREEMAIL_FROM	Sender email is commonly abused enduser mail provider	
FREEMAIL_REPLY	From and body contain different freemails	
FREEMAIL_REPLYTO	Reply-To/From or Reply-To/body contain different freemails	
FREEMAIL_REPLYTO_END_DIGIT	Reply-To freemail username ends in digit	
FROM_ADDR_WS	Malformed From address	
FROM_DOMAIN_NOVOWEL	From: domain has series of non-vowel letters	
FROM_EXCESS_BASE64	From: base64 encoded unnecessarily	
FROM_LOCAL_DIGITS	From: localpart has long digit sequence	
FROM_LOCAL_HEX	From: localpart has long hexadecimal sequence	
FROM_LOCAL_NOVOWEL	From: localpart has series of non-vowel letters	
FROM_LONG_DOM	Absurdly long From domain name	
FROM_LONG_DOM_MINFP	Absurdly long From domain name-suspicious relays	
FROM_MISSP_EH_MATCH	From misspaced- matches envelope	
FROM_MISSP_SPF_FAIL	-	
FROM_MISSP_XPRIO	Misspaced FROM + X-Priority	
FROM_NO_USER	From: has no local-part before @ sign	No FROM não tem letras antes do @
FROM_OFFERS	From address is "at something-offers"	
FROM_STARTS_WITH_NUMS	From: starts with several numbers	
FROM_UNBAL2	From with unbalanced angle brackets-'<' missing	
FSL_CTYPE_WIN1251	Content-Type only seen in 419 spam	
FSL_HAS_TINYURL	-	
FSL_HELO_BARE_IP_1	-	
FSL_HELO_NON_FQDN_1	-	
FSL_NEW_HELO_USER	Spam's using Helo and User	
FUZZY_CREDIT	Attempt to obfuscate words in spam	
FUZZY_MONERO	Obfuscated "Monero"	
FUZZY_WALLET	Obfuscated "Wallet"	
FUZZY_XPILL	Attempt to obfuscate words in spam	
GAPPY_SUBJECT	Subject: contains G.a.p.p.y-T.e.x.t	
GB_BITCOIN_CP	Localized Bitcoin scam	

GB_FREEMAIL_DISPTO	Disposition-Notification-To/From or Disposition-Notification-To/body contain different freemails	
GOOG_STO_IMG_NOHTML	Apparently using google content hosting to avoid URIBL	
GOOG_STO_NOIMG_HTML	Apparently using google content hosting to avoid URIBL	
HDRS_MISSP	Misspaced headers	
HEADER_FROM_DIFFERENT_DOMAINS	From and EnvelopeFrom 2nd level mail domains are different	
HELO_DYNAMIC_DHCP	Relay HELO'd using suspicious hostname (DHCP)	
HELO_DYNAMIC_IPADDR	Relay HELO'd using suspicious hostname (IP addr 1)	
HELO_DYNAMIC_IPADDR2	Relay HELO'd using suspicious hostname (IP addr 2)	
HELO_MISC_IP	Looking for more Dynamic IP Relays	
HELO_NO_DOMAIN	Relay reports its domain incorrectly	No Helo não possui o domínio
HELO_STATIC_HOST	Relay HELO'd using static hostname	
HK_RANDOM_ENVFROM	Envelope sender username looks random	
HK_RANDOM_FROM	From username looks random	
HK_RANDOM_REPLYTO	Reply-To username looks random	
HOSTED_IMG_FREEM	Image hosted at large ecomm- CDN or hosting site or redirected- freemail from or reply-to	
HOSTED_IMG_MULTI_PUB_01	Multiple hosted images at public site	
HREF_EMPTY_XANTIABUSE	Empty href + X-AntiAbuse	
HREF_EMPTY_XAUTHED	Empty href + X-Authenticated-Sender	
HSC_1000148_OTRS_02	-	
HSC_ADV_EMAIL	Marks adv@<domain.com> Addresses as likely SPAM	
HSC_ADVERT2	This is probably an unwanted commercial email...	
HSC_AI_GOV_SPOOFING	HSC Artificial Intelligence - Identification of messages attempting to impersonate government communications	
HSC_AI_SUSPICIOUS_001	HSC AI - Suspicious News Domains	
HSC_AI_SUSPICIOUS_002	HSC AI - Suspicious Countries	
HSC_AI_SUSPICIOUS_003	Detect Bitcoin	Detecta textos relacionados com bitcoin
HSC_AI_SUSPICIOUS_004	HSC AI - Unsolicited Bitcon	
HSC_AUTO_WHITELIST	HSC Auto Whitelist	HSC Auto Whitelist

HSC_BADIPHTTP	Due to the Storm Bot Network- IPs in e-mails is bad	Rede de BOTNET
HSC_BADSWF	SWF embedded links in E-mail Scams	Links de Flash com ataques
HSC_BATV_INVALID	Bounced Message don't have a valid TAG	A Mesagem não Possui Bounce TAG Valida
HSC_BATV_VALID	Bounced Message has a valid TAG	A Mensagem Possui Bounce TAG Valida
HSC_BLACKFRIDAY_SUB_001	Combinations of BLACK FRIDAY in the Subject	Combinações da palavra Black Friday no assunto
HSC_BLACKFRIDAY_SUB_UPPER	Subject BLACK FRIDAY (Upper case)	Contendo a palavra BLACK FRIDAY em maiúsculo no assunto do e-mail
HSC_BOUNCE_MESSAGE	An MTA-generated bounce	MTA que gera e-mails de bounce
HSC_BR_HPG_URI		Link para sites no HPG
HSC_BR_KITNET_URI		Link para sites no kit.net
HSC_BR_KNOWN_MAILER	X-Mailer conhecido	
HSC_BR_LACADOR_01	-	
HSC_BR_LACADOR_03	-	
HSC_BR_MALADIRETA	Inclui 'Mala Direta'	
HSC_BR_MENOSPRECO_01	-	
HSC_BR_MENOSPRECO_03	-	
HSC_BR_ML_URI		Link para produtos no Mercado Livre
HSC_BR_REMOVER_QUOTE	Inclui texto para remover email (quote)	
HSC_BR_SPAMMER_URI		Texto suspeito
HSC_BR_TELEMARKETING	Fala sobre 'Telemarketing'	
HSC_BR_WWW_SUAEMPRESA	www.suaempresa.com.br (e similares)	
HSC_BR_WWW_SUAEMPRESA_URI		www.suaempresa.com.br (e similares)
HSC_BR_WWW_SUAEMPRESA_URI	www.suaempresa.com.br (e similares)	
HSC_COBRANCA_10	Emails Text De cobranca . 1 HIT	
HSC_COBRANCA_20	Emails Text De cobranca . 2 HITS	
HSC_DANGEROUS_URL_EXTENSIONS	URL contains executable content	URL encaminha a um executável
HSC_DANGEROUS_URL_EXTENSIONS2	URL contains .com to download	URL possui .COM para download de conteúdo
HSC_DISABLE_RELAY_NET_02	-	
HSC_DISABLE_RELAY_NET_03	-	
HSC_E-MAIL_ADULT	Adult Content Sender	Remetentes E-mail Conteúdo Adulto ou com conteúdo adulto (podendo ser URL)- sendo categorizados como

		pornography- sex_erotic-nudity ou dating_relationships
HSC_EMAIL_MARKETING	Remetente Email Marketing	Remetente de Email Marketing
HSC_E-MAIL_MARKETING	MailMarketing Sender	Remetente E-mail Marketing
HSC_EMPTY_BODY	Message is empty - No Body	Sem conteúdo no corpo da mensagem. Detectado quando NÃO É SMIME.
HSC_EMPTY_MESSAGE	Message is empty - No Body	Sem conteúdo no corpo da mensagem. Detectado somente com SMIME.
HSC_EMPTY_SENDER	Header From - Sender Empty	Campo FROM (do Header) em branco
HSC_EMPTY_SUBJECT	Massage has Empty Subject	Sem assunto no e-mail
HSC_ENVELOPE_EMPTY_SENDER	SMTP Envelop Sender Empty	Campo FROM (do Envelope) em branco
HSC_FACE	Facebook bogus phishing e-mails	E-mails de phishing originários do facebook
HSC_FAKEPDF	Fake PDF Reader / Writer	Falso arquivo de PDF
HSC_FLASH	Fake Flash Player Phishing Scam	Phishing em Flash
HSC_FREE_WEB_HOSTING	URL free web hosting	URL hospedada em servidores web gratuitos- podendo ser formulários
HSC_FROM_SUSPICIOUS_TLD	TLD's used in common attacks	TLD's comumente usado em ataques
HSC_GOOGLE_STRING	Use of Google redir appearing in spam July 2006	Usa o Google para redirecionamento de SPAM
HSC_GRAY_MAIL		Conjunto de indicadores fortes de graymail
HSC_GRAYMAIL_LIKELY	-	
HSC_GRAYMAIL_STRONG	Multiple GrayMail indicators	Múltiplos indicadores de GrayMail
HSC_HAS_ATTACHMENT	The message has attachments	A mensagem possui anexo(s)
HSC_HAS_ATTACHMENT	The message has attachments	
HSC_HEADER_FROM_DOMAIN_TEST	Header sender has no MX or A DNS records	
HSC_HIDDEN_URI	URI obfuscation techniques	Possui técnicas de ofuscação URI/URL
HSC_LIST	Mailing List Database SPAM	Está listado como SPAMMER
HSC_LIST_UNSUBSCRIBE	Mailing List UNSUBSCRIBE	Removido da lista de SPAMMER
HSC_LIVE	blogspot.com & livejournal.com likely spam (Apr 2010)	

HSC_LOOK_ALIKE_BANK_SENDER	Suspicius Sender using Look-Alike Bank Domain	
HSC_LOOK_ALIKE_BANK_URI	Message contains Look-Alike Bank Domain URL^	
HSC_MAIL_REPUTATION	Listado Sistema de Reputacao de Emails HSC SmartDefender	
HSC_MKT_EMAIL_001	Mail Marketing From:	
HSC_MKT_EMAIL_002	Mail Marketing From Suspect Domains	
HSC_MLI_SPAM_ENGINE	This message has been scanned by HSC MailInspector - Spam Engine	
HSC_MULTIPLE_HEADER_FROM	Message with more than One Header From	
HSC_MX3	Odd prevalence of MX records for non-identified Spammers	
HSC_MX4	MX Record and dot info domains associated with COMPANY3 Spammers	
HSC_MYDOMAIN_SPOOF	-	
HSC_PHISHING_DOMAIN	Phishing Source Domains	Domínio usado para phishing
HSC_PHISHING_TEXT_0001	Possible Text Phishing	Texto padrão utilizado em phishing
HSC_PHISHING_TEXT_0002	Possible Text Phishing	Texto padrão utilizado em phishing
HSC_POSSIBLE_GOV_SPOOFING	Possible gov.br Spoofing	Spoofing de domínios do governo. Compara os dois headers e se tiver diferença-verifica se está tentando se passar pelos principais domínios do governo brasileiro
HSC_POSSIBLE_HTML_EXEC	Possible Hiden Executable into HTML Attach	Eecutável Escondido dentro de código HTML
HSC_POSSIBLE_PHISHING_COMBO_005	Anti-Phishing filters were triggered more than 1 time (T_DKIM_INVALID)	
HSC_POSSIBLE_PHISHING_COMBO_006	Anti-Phishing filters were triggered more than 1 time (HSC_MYDOMAIN_SPOOF)	
HSC_POSSIBLE_PHISHING_COMBO_007	Anti-Phishing filters were triggered more than 1 time (HSC_HEADER_FROM_DOMAIN_TEST)	
HSC_POSSIBLE_PHISHING_COMBO_008	Anti-Phishing filters were triggered more than 1 time (SPF_FAIL)	
HSC_POSSIBLE_PHISHING_COMBO_01	Combo Rules where detect Phishing	Combo Rules where detect Phishing
HSC_POSSIBLE_PHISHING_COMBO_010	Anti-Phishing filters were triggered more than 1 time (ALL > 3)	

HSC_POSSIBLE_PHISHING_COMBO_02	Anti-Phishing filters were triggered more than 1 time (HSC_SUSPECT_MAIL_RULE)	Combo Rules where detect Phishing
HSC_POSSIBLE_PHISHING_COMBO_03	Anti-Phishing filters were triggered more than 1 time (FREEMAIL_FORGED_FROMDOMAIN)	Combo Rules where detect Phishing
HSC_POSSIBLE_PHISHING_COMBO_04	Anti-Phishing filters were triggered more than 1 time (HSC_SUSPICIOUS_NEW_DOMAINS)	Combo Rules where detect Phishing
HSC_POSSIBLE_PHISHING_COMBO_05	Combo Rules where detect Phishing	Combo Rules where detect Phishing
HSC_POSSIBLE_PHISHING_COMBO_06	Combo Rules where detect Phishing	Combo Rules where detect Phishing
HSC_POSSIBLE_PHISHING_COMBO_07	Combo Rules where detect Phishing	Combo Rules where detect Phishing
HSC_POSSIBLE_PHISHING_COMBO_08	Combo Rules where detect Phishing	Combo Rules where detect Phishing
HSC_POSSIBLE_PHISHING_COMBO_09	Combo Rules where detect Phishing	Combo Rules where detect Phishing
HSC_POSSIBLE_PHISHING_COMBO_10	Combo Rules where detect Phishing	Combo Rules where detect Phishing
HSC_POSSIBLE_PHISHING_COMBO_11	Combo Rules where detect Phishing	Combo Rules where detect Phishing
HSC_RAT	Variable Replacements Indicative of RatWare/Mass Mailing	Detectado uso de Sistema Ratware para disparo de e-mail em massa
HSC_RETURNPATH_EMPTY	Header Return-Path Empty	Campo Return-Path no Cabeçalho está em branco
HSC_RETURNPATH_SPAM	Possible Mailling List Spam - No ReturnPath	O campo Return-Path no cabeçalho é de spammer
HSC_RULE_20130923_02	-	
HSC_RULE_URI_0132	-	
HSC_RULE_URI_0133		
HSC_RULE_URI_0133	-	
HSC_SD_URL_BAD_CAT	HSC SmartDefender - URL Reputation - Malware Categories	Reputação de URL – Categoria: Malware
HSC_SD_URL_BASEGUARD	HSC SmartDefender - URL Reputation	Reputação de URL – Listado
HSC_SD_URL_BLACKLIST	HSC SmartDefender - URL Reputation - dbCheck engine	Reputação de URL – Listado em Blacklist no Banco de Dados
HSC_SD_URL_LOOKUP	HSC SmartDefender - URL Reputation - URL Lookup engine	Reputação de URL – Detectado em ferramenta de Lookup
HSC_SD_URL_SMARTBLACKLIST	HSC Smart Blacklist- Local Blacklist	Reputação de URL – Listado em Blacklist local

HSC_SD_URL_SMARTCRAWLER	HSC Smart Defender - URL Reputation - SmartCrawler URL SandBox	
HSC_SD_URL_SMARTCRAWLER	HSC SmartDefender - URL Reputation - SmartCrawler URL SandBox	Reputação de URL – Detectada ameaça em URL pela análise de URL no SandBox
HSC_SENDERID_INVALID	SenderID not authorized or invalid	O Servidor de Origem da mensagem não e autorizado. SENDER ID.
HSC_SENDERID_VALID	SenderID valid	O Servidor de Origem da mensagem e autorizado. SENDER ID.
HSC_SEX	Sexually Explicit SPAM / Penis Enlargement Scam	
HSC_SEXTORTION	-	
HSC_SEXTORTION_COMBO	-	
HSC_SOC_001	-	
HSC_SOC_004	-	
HSC_SOC_005	-	
HSC_SOC_006	-	
HSC_SOC_007	-	
HSC_SOC_008	-	
HSC_SOC_010	-	
HSC_SOCIAL_NETWORKING	Sender from Social Networks	Remetentes Redes Sociais
HSC_SPAM_CUSTOM_RULE_107	(EMPTY ENVELOPE) E (PHISHING TEXT02)	
HSC_SPAM_CUSTOM_RULE_143	URL SPAM	
HSC_SPAM_CUSTOM_RULE_169	(Origen TI) E (Macros)	
HSC_SPAM_CUSTOM_RULE_198	(ToTubosIpiranga) E (MailMarketing)	
HSC_SPAM_CUSTOM_RULE_229	regra saida excessão frigol (2)	
HSC_SPAM_CUSTOM_RULE_236	(From 3 Coroas) E (HSC_EMAIL_MARKETING)	
HSC_SPAM_CUSTOM_RULE_260	(To - Dominios Sermed) E (HSC_EMPTY_SUBJECT)	
HSC_SPAM_CUSTOM_RULE_261	TLD Suspeito e Dominios Diferentes	
HSC_SPAM_CUSTOM_RULE_278	(Uncatorized Sender ou URL) E ((India) OU ((((Iraq) OU ((((Russia) OU (China)) OU (Malasia)) OU (Tchecoslovaquia))) OU (Iran)) OU (Belarus)))	
HSC_SPAM_CUSTOM_RULE_279	Disable - RCVD_IN_DNSWL_MED	
HSC_SPAM_CUSTOM_RULE_284	(Dominios Novos) E (TO Sermed)	
HSC_SPAM_CUSTOM_RULE_292	(From Igrejinha) E (HSC_SUSPECT_MAIL_RULE)	
HSC_SPAM_CUSTOM_RULE_293	NEW_DOMAINS + SUSPECT_TLD	

HSC_SPAM_CUSTOM_RULE_296	(UNCATEGORIZED (SENDER + URL)) E (! IP Relay Autorizado)	
HSC_SPAM_CUSTOM_RULE_303	(Assunto em Branco) E (! RFC3834)	
HSC_SPAM_CUSTOM_RULE_326	MISSING HEADERS	
HSC_SPAM_CUSTOM_RULE_327	DNS DINÂMICO ou IP MALICIOSO	
HSC_SPAM_CUSTOM_RULE_340	(! GOV.BR) E (GUIAS)	
HSC_SPAM_CUSTOM_RULE_344	DOC_Fiscal	
HSC_SPAM_CUSTOM_RULE_65	(From - Servidores do Google) E (From HEADER HSC)	
HSC_SPAM_CUSTOM_RULE_84	(Assinaturas suspeitas) E (TO HSC)	
HSC_SPAM_CUSTOM_RULE_87	(Fake Bounce) E (Fake Dominio)	
HSC_SPAM_IMAGE	Message has Spam Image	E-mail com imagem de SPAM
HSC_SPAM_SENDER	Sender SPAMMER	Remetente SPAM
HSC_SPAM_SIGS	HSC SPAM Signatures	
HSC_SPEAR_PHISHING_URL_0001	-	
HSC_SRC_REP_HIGH_RISK	Domain/IP Very bad reputation- High Risk	Domínio/IP com reputação ruim: Alto Risco
HSC_SRC_REP_MEDIUM_RISK	Domain/IP Medium reputation- Medium Risk	Domínio/IP com reputação mediana: Médio Risco
HSC_SRC_REP_NO_KNOW_RISK	Domain/IP Good reputation- No Know Risk	Domínio/IP com reputação boa: Sem Risco conhecido
HSC_SRC_REP_POSSIBLE_RISK	Domain/IP Low reputation- Possible Risk	Domínio/IP com baixa reputação: Possível risco
HSC_SUSPECT_FILE_RULE	-	
HSC_SUSPECT_MAIL_RULE	-	
HSC_SUSPECT_TLD	Message contains know suspects TLDs domains	Mensagem contém domínios suspeitos TLD's (Top Level Domain / Sufixo de domínio).
HSC_SUSPICIOUS_NEW_DOMAINS	Detect recently registered domains	Domínios recém adquiridos
HSC_THREAT_MALICIOUS_FILE	HSC THREAT MALICIOUS FILE Signatures	Assinaturas de arquivos maliciosos cadastrados pela HSCBRASIL
HSC_THREAT_MALWARE	HSC THREAT MALWARE Signatures	Assinaturas de malwares cadastrados pela HSCBRASIL
HSC_THREAT_PHISHING	HSC THREAT PHISHING Signatures	Assinaturas de phishing cadastrados pela HSCBRASIL
HSC_THREAT_ZERO_DAY	HSC THREAT ZERO DAY/HOUR Signatures	Assinaturas de ataques Zero Day/Zero Hour cadastrados pela HSCBRASIL
HSC_TIME	Pssss. Hey Buddy- wanna buy a watch?	Possui o texto: Quer comprar um relógio?
HSC_TMP_SENDER	Temporary Sender mail using for spam/phishing attack	Remetente temporário usado para ataques. Essa lista de e-mails é atualizada a cada 3h.

HSC_UNCATEGORIZED_SENDER		Remetente ainda não categorizado
HSC_UNCATEGORIZED_URL		URL hospedada em servidores ainda não categorizados
HSC_URGENT_SUBJECT_001	Urgent Subject Upper Case	Assuntos de e-mail com indicação de urgência
HSC_URGENT_SUBJECT_002	Urgent Subject Upper Case % OFF	Assuntos de e-mail com indicação de urgência
HSC_URL_MAIL_MARKETING	HSC URL E-Mail Marketing & GrayMail	URL de Mail Marketing/Bulk Mail e Graymail
HSC_URL_MEDIUM_SPAM	HSC URL MEDIUM SPAM	URL de SPAM de nível médio
HSC_URL_POSSIBLE_SPAM	-	
HSC_URL_REP_HIGH_RISK	Contains an URL listed in the HSC URL Reputation HIGH RISK - Anti-Malware & Anti-Phishing List	URL listado no Sistema da HSCBRASIL- como reputação de alto risco
HSC_URL_REP_MEDIUM_RISK	Contains an URL listed in the HSC Reputation MEDIUM RISK	URL listado no Sistema da HSCBRASIL- como reputação de médio risco
HSC_URL_REP_POSSIBLE_RISK	Contains an URL listed in the HSC Reputation POSSIBLE RISK or SPAM URLS	URL listado no Sistema da HSCBRASIL- como reputação de possível risco
HSC_URL_SPAM	URL listed by HSCBRASIL as SPAMMER	URL listado no Sistema da HSCBRASIL- como SPAMMER
HSC_URL_WHITELISTED	-	
HSC_URLCAT_ABORTION	Abortion URL Found	URL de Aborto
HSC_URLCAT_ADS	ADS URL Found	URL de ADWARE
HSC_URLCAT_AGRICULTURE	Agriculture URL Found	URL agrícolas
HSC_URLCAT_ANONYMIZER	Anonymizer URL Found	Detectado uso de anonimizador de URL
HSC_URLCAT_ARCHITECTURE	Architecture Construction URL Found	URL de arquitetura
HSC_URLCAT_AUDIO	Streaming Audio URL Found	URL de streaming de áudio
HSC_URLCAT_BANK	Bank URL Found	URL de Bancos
HSC_URLCAT_BLOG	Blogs URL Found	URL de Blogs
HSC_URLCAT_BOTNET	Botnet URL Found	URL de Botnet
HSC_URLCAT_CDN	CDN URL Found	URL CDN (Centro de distribuição de conteúdo)
HSC_URLCAT_CHAT	Chat URL Found	URL de chats
HSC_URLCAT_CHILD_ABUSE	Child Abuse Images URL Found	URL de abuso infantil
HSC_URLCAT_COMMAND_CONTROL	Command Control Center URL Found	URL de Centro de Controle
HSC_URLCAT_COMPROMISED	Websites Compromised URL Found	URL de sites comprometidos
HSC_URLCAT_CRIMINAL_SKILLS	Criminal Skills URL Found	URL de atividades/habilidades criminais
HSC_URLCAT_DATING	Dating URL Found	URL de encontros

HSC_URLCAT_EDUCATIONAL	Educational Institutions URL Found	URL de instituições educacionais
HSC_URLCAT_ENTERTAINMENT	Entertainment URL Found	URL de entretenimento
HSC_URLCAT_EROTIC	Sex Erotic URL Found	URL de conteúdo erótico/sexo
HSC_URLCAT_FASHION	Fashion Beauty URL Found	URL de moda
HSC_URLCAT_FINANCE	Finance URL Found	URL financeiro
HSC_URLCAT_GOV	Government URL Found	URL governamental
HSC_URLCAT_HACKING	Hacking URL Found	URL de hacking
HSC_URLCAT_HEALTH	Health Medical URL Found	URL médico e saúde
HSC_URLCAT_HUMOR	Humor URL Found	URL de humor
HSC_URLCAT_INSURENCE	Insurance URL Found	URL de seguradora
HSC_URLCAT_IT_SECURITY	Information Security URL Found	URL de segurança de informação
HSC_URLCAT_JOB_SEARCH	Job Search URL Found	URL de empregos e busca de empregos
HSC_URLCAT_MALWARES	Malwares URL Found	URL de malwares
HSC_URLCAT_MANUFACTURING	Manufacturing URL Found	URL de fabricação/manufatura
HSC_URLCAT_MILITARY	Military URL Found	URL militar
HSC_URLCAT_MOTOR	Motorized Vehicles URL Found	URL de veículos automotores
HSC_URLCAT_NEWS	News URL Found	URL de notícias
HSC_URLCAT_NUTRITION	Nutrition URL Found	URL de nutrição
HSC_URLCAT_P2P	P2P URL Found	URL de conteúdo Peer-to-Peer
HSC_URLCAT_PARKED	Parked URL Found	URL parado
HSC_URLCAT_PAY_TO_SURF	Pay to Surf URL Found	URL pague para navegar
HSC_URLCAT_PERSONAL_STORAGE	Personal Storage URL Found	URL de armazenamento pessoal
HSC_URLCAT_PHARMACY	PHARMACY URL Found	URL de farmácia
HSC_URLCAT_PHISING	Phishing URL Found	URL de phishing
HSC_URLCAT_PIRACY	Piracy Copyright Theft URL Found	URL de conteúdo pirata
HSC_URLCAT_PORN	Porn URL Found	URL de conteúdo pornográfico
HSC_URLCAT_PRICE_COMPARISONS	Product Reviews Price Comparisons URL Found	URL de comparação de preços
HSC_URLCAT_PROFESSIONAL	Professional Networking URL Found	URL de rede de profissionais
HSC_URLCAT_RACISM	Rasicm URL Found	URL com conteúdo racista
HSC_URLCAT_REAL_ESTATE	Real Estate URL Found	URL de imobiliárias
HSC_URLCAT_REMOTE_ACCESS	Remote Access URL Found	URL de acesso remoto
HSC_URLCAT_RESTAURANTS	Food Restaurants URL Found	URL de restaurantes e comida
HSC_URLCAT_SHOPPING	Online Shopping URL Found	URL de compras online
HSC_URLCAT_SOCIAL	Social Affiliation Organizations URL Found	URL de organizações sociais/ongs
HSC_URLCAT_SOCIAL_NETWORKING	Social Networking URL Found	URL de redes sociais
HSC_URLCAT_SPAM	Spam URL Found	URL de conteúdo SPAM
HSC_URLCAT_SPORTS	Sports URL Found	URL de conteúdo esportivo

HSC_URLCAT_SPYWARES	Spywares & Keyloggers URL Found	URL de spywares e Keyloggers
HSC_URLCAT_SUPPLEMENTS	Supplements Compounds URL Found	URL de suplementos e compostos
HSC_URLCAT_TECNOLOGY	Tecnology URL Found	URL de tecnologia
HSC_URLCAT_TRAVEL	Travel URL Found	URL de viagens
HSC_URLCAT_TV	TV & Movies URL Found	URL de TV- filmes e seriados
HSC_URLCAT_UNREACHABLE	Unreachable URL Found	URL inalcançável/fora do ar
HSC_URLCAT_VIDEO	Video URL Found	URL de vídeos
HSC_URLCAT_VIOLENCE	Violence URL Found	URL de conteúdo violento
HSC_URLCAT_WIKIS	Wikis URL Found	URL de enciclopédia rápida- de consultas rápidas
HSC_VIAGRA3	Common Viagra and Medicinal Table Trick	
HSC_VIAGRA6	Viagra Obfuscation Technique SPAM	Técnica de ofuscação para palavra VIAGRA
HTML_COMMENT_SAVED_URL	HTML message is a saved web page	
HTML_ENTITY_ASCII_TINY	Obfuscated ASCII + tiny fonts	Código ASCII ofuscado ou letras muito pequenas
HTML_EXTRA_CLOSE	HTML contains far too many close tags	
HTML_FONT_FACE_BAD	HTML font face is not a word	
HTML_FONT_LOW_CONTRAST	HTML font color similar or identical to background	
HTML_FONT_SIZE_HUGE	HTML font size is huge	
HTML_FONT_SIZE_LARGE	HTML font size is large	
HTML_FONT_TINY_NORDNS	Font too small to read- no rDNS	Fonte muito pequena para leitura e também não possui DNS reverso.
HTML_IMAGE_ONLY_04	HTML: images with 0-400 bytes of words	
HTML_IMAGE_ONLY_08	HTML: images with 400-800 bytes of words	
HTML_IMAGE_ONLY_12	HTML: images with 800-1200 bytes of words	
HTML_IMAGE_ONLY_16	HTML: images with 1200-1600 bytes of words	
HTML_IMAGE_ONLY_20	HTML: images with 1600-2000 bytes of words	
HTML_IMAGE_ONLY_24	HTML: images with 2000-2400 bytes of words	
HTML_IMAGE_ONLY_28	HTML: images with 2400-2800 bytes of words	
HTML_IMAGE_ONLY_32	HTML: images with 2800-3200 bytes of words	
HTML_IMAGE_RATIO_02	HTML has a low ratio of text to image area	

HTML_IMAGE_RATIO_04	HTML has a low ratio of text to image area	
HTML_IMAGE_RATIO_06	HTML has a low ratio of text to image area	
HTML_IMAGE_RATIO_08	HTML has a low ratio of text to image area	
HTML_MESSAGE	HTML included in message	
HTML_MIME_NO_HTML_TAG	HTML-only message- but there is no HTML tag	Mensagem HTML- mas sem TAG de HTML
HTML_OBFUSCATE_05_10	Message is 5% to 10% HTML obfuscation	
HTML_OBFUSCATE_10_20	Message is 10% to 20% HTML obfuscation	
HTML_OBFUSCATE_20_30	Message is 20% to 30% HTML obfuscation	
HTML_OFF_PAGE	HTML element rendered well off the displayed page	
HTML_SHORT_LINK_IMG_2	HTML is very short with a linked image	
HTML_SHORT_LINK_IMG_3	HTML is very short with a linked image	
HTML_SINGLET_MANY	Many single-letter HTML format blocks	
HTML_TAG_BALANCE_BODY	HTML has unbalanced "body" tags	
HTML_TAG_BALANCE_CENTER	Malformatted HTML	
HTML_TAG_BALANCE_HEAD	HTML has unbalanced "head" tags	
HTML_TEXT_INVISIBLE_FONT	HTML hidden text - word obfuscation?	
HTML_TEXT_INVISIBLE_STYLE	HTML hidden text + other spam signs	
HTML_TITLE_SUBJ_DIFF	-	
HTTP_ESCAPED_HOST	Uses %-escapes inside a URL's hostname	Usa a tecla ESC em URL's
HTTP_EXCESSIVE_ESCAPES	Completely unnecessary %-escapes inside a URL	Tecla ESC desnecessária dentro de URL's
HTTPS_HTTP_MISMATCH	-	
IMG_DIRECT_TO_MX	-	
INVALID_DATE	Invalid Date: header (not RFC 2822)	
INVALID_MSGID	Message-Id is not valid- according to RFC 2822	
INVESTMENT_ADVICE	Message mentions investment advice	
IP_LINK_PLUS	Dotted-decimal IP address followed by CGI	Ponto em endereços seguidos de código CGI
KHOP_HELO_FCRDNS	Relay HELO differs from its IP's reverse DNS	
LOCALPART_IN_SUBJECT	Local part of To: address appears in Subject	
LONG_HEX_URI	Very long purely hexadecimal URI	
LONG_INVISIBLE_TEXT	Long block of hidden text - bayes poison?	Longo bloco de texto escondido

LONGLN_LOW_CONTRAST	Excessively long line + hidden text	
LOTS_OF_MONEY	Huge... sums of money	Indicação de muito dinheiro no contexto do email
MAILING_LIST_MULTI	Multiple indicators imply a widely-seen list manager	Múltiplos destinatários- indicando lista de envio massivo de email
MALFORMED_FREEMAIL	Bad headers on message from free email service	
MALWARE_NORDNS	Malware bragging + no rDNS	
MALWARE_PASSWORD		
MANY_SPAN_IN_TEXT	Many <SPAN> tags embedded within text	
MANY_SUBDOM	Lots and lots of subdomain parts in a URI	
MIME_BASE64_TEXT	Message text disguised using base64 encoding	
MIME_CHARSET_FARAWAY	MIME character set indicates foreign language	
MIME_HEADER_CTYPE_ONLY	'Content-Type' found without required MIME headers	Content-Type sem o MIME do header
MIME_HTML_MOSTLY	Multipart message mostly text/html MIME	
MIME_HTML_ONLY	Message only has text/html MIME parts	
MIME_HTML_ONLY_MULTI	Multipart message only has text/html MIME parts	
MIME_QP_LONG_LINE	Quoted-printable line longer than 76 chars	
MISSING_DATE	Missing Date: header	
MISSING_FROM	Missing From: header	
MISSING_HEADERS	Missing To: header	
MISSING_MID	Missing Message-Id: header	Sem ID da mensagem no cabeçalho do email
MISSING_MIMEOLE	Message has X-MSMail-Priority- but no X-MimeOLE	
MISSING_SUBJECT	Missing Subject: header	
MIXED_CENTER_CASE	Has center tag in mixed case	
MIXED_ES	Too many es are not es	
MIXED_HREF_CASE	Has href in mixed case	
MONEY_FORM	Lots of money if you fill out a form	
MONEY_FORM_SHORT	Lots of money if you fill out a short form	
MONEY_FREEMAIL_REPTO	Lots of money from someone using free email?	
MONEY_NOHTML	Lots of money in plain text	

MPART_ALT_DIFF	HTML and text parts are different	
MSGID_FROM_MTA_HEADER	Message-Id was added by a relay	ID da mensagem adicionado ao relay
MSGID_HDR_MALF	Has invalid message ID header	
MSGID_MULTIPLE_AT	Message-ID contains multiple '@' characters	
MSGID_SHORT	Message-ID is unusually short	
MXG_EMAIL_FRAG	URI with email in fragment	
MXG_SPOOFED_DOCUSIGN	Docusign spoofing	
NA_DOLLARS	Talks about a million North American dollars	
NEW_PRODUCTS	-	
NICE_REPLY_A	Looks like a legit reply (A)	
NML_ADSP_CUSTOM_MED	ADSP custom_med hit- and not from a mailing list	
NO_FM_NAME_IP_HOSTN	No From name + hostname using IP address	
NO_PRESCRIPTION	No prescription needed	
NORMAL_HTTP_TO_IP	Uses a dotted-decimal IP address in URL	Usa o PONTO (decimal) em endereços de URL
NSL_RCVD_FROM_USER	Received from User	
NUMERIC_HTTP_ADDR	Uses a numeric IP address in URL	Usa IP em URL
OBFU_HTML_ATTACH	HTML attachment with non-text MIME type	
OBFU_TEXT_ATTACH	Text attachment with non-text MIME type	
OBFUSCATING_COMMENT	HTML comments which obfuscate text	
PDS_BTC_ID	FP reduced Bitcoin ID	
PDS_FRNOM_TODOM_NAKED_TO	Naked to From name equals to Domain	
PDS_FROM_NAME_TO_DOMAIN	From:name looks like To:domain	
PHISH_ATTACH	Attachment filename suspicious-probable phishing	
PHONE_983_NOVEL	Body contains phone number in unassigned NANP area code 983	
PHP_SCRIPT	Sent by PHP script	
PLING_QUERY	Subject has exclamation mark and question mark	
POSSIBLE_GMAIL_PHISHER	Apparent phishing email sent from a gmail account	
RATWARE_EFROM	Bulk email fingerprint (envfrom) found	
RCVD_DOUBLE_IP_LOOSE	Received: by and from look like IP addresses	
RCVD_DOUBLE_IP_SPAM	Bulk email fingerprint (double IP) found	

RCVD_HELO_IP_MISMATCH	Received: HELO and IP do not match-but should	
RCVD_IN_BL_SPAMCOP_NET	Received via a relay in bl.spamcop.net	
RCVD_IN_DNSWL_BLOCKED	ADMINISTRATOR NOTICE: The query to DNSWL was blocked. See http://wiki.apache.org/spamassassin/DnsBlocklists\#DnsBlocklists-dnsbl-block for more information.	
RCVD_IN_DNSWL_LOW	Sender listed at https://www.dnswl.org/- low trust	
RCVD_IN_DNSWL_MED	Sender listed at https://www.dnswl.org/- medium trust	
RCVD_IN_DNSWL_NONE	Sender listed at https://www.dnswl.org/- no trust	
RCVD_IN_HSC_REP_L3	Low reputation (-3)	
RCVD_IN_HSC_REP_L4	Bad reputation (-4)	
RCVD_IN_HSC_REP_L5	Very bad reputation (-5)	
RCVD_IN_HSC_REP_ZBI	-	
RCVD_IN_IADB_DK	IADB: Sender publishes Domain Keys record	
RCVD_IN_IADB_DMARC	IADB: Sender has DMARC record	
RCVD_IN_IADB_DOPTIN_LT50	IADB: Confirmed opt-in used less than 50% of the time	
RCVD_IN_IADB_ESP	IADB: Email Service Provider (ESP)	
RCVD_IN_IADB_LISTED	Participates in the IADB system	
RCVD_IN_IADB_OPTIN	IADB: All mailing list mail is opt-in	
RCVD_IN_IADB_OPTIN_GT50	IADB: Opt-in used more than 50% of the time	
RCVD_IN_IADB_RDNS	IADB: Sender has reverse DNS record	
RCVD_IN_IADB_SENDERID	IADB: Sender publishes Sender ID record	
RCVD_IN_IADB_SPF	IADB: Sender publishes SPF record	
RCVD_IN_IADB_VOUCHED	ISIPP IADB lists as vouched-for sender	
RCVD_IN_PBL	Received via a relay in Spamhaus PBL	
RCVD_IN_PSBL	Received via a relay in PSBL	
RCVD_IN_SBL	Received via a relay in Spamhaus SBL	
RCVD_IN_SBL_CSS	Received via a relay in Spamhaus SBL-CSS	
RCVD_IN_VALIDITY_RPBL_BLOCKED	ADMINISTRATOR NOTICE: The query to Validity was blocked. See https://knowledge.validity.com/hc/en-us/articles/20961730681243 for more information.	

RCVD_IN_VALIDITY_SAFE_BLOCKED	ADMINISTRATOR NOTICE: The query to Validity was blocked. See https://knowledge.validity.com/hc/en-us/articles/20961730681243 for more information.	
RCVD_IN_XBL	Received via a relay in Spamhaus XBL	
RDNS_DYNAMIC	Delivered to internal network by host with dynamic-looking rDNS	
REPLYTO_WITHOUT_TO_CC	-	
SB_GIF_AND_NO_URIS	-	
SHORT_HELO_AND_INLINE_IMAGE	Short HELO string- with inline image	
SORTED_RECIPS	Recipient list is sorted by address	
SPF_FAIL	SPF: sender does not match SPF record (fail)	
SPF_HELO_FAIL	SPF: HELO does not match SPF record (fail)	
SPF_HELO_NEUTRAL	SPF: HELO does not match SPF record (neutral)	
SPF_HELO_NONE	SPF: HELO does not publish an SPF Record	Servidor de e-mail que envia sua mensagem não possui um registro SPF no DNS configurado para o nome que ele usa para se identificar (HELO/EHLO)
SPF_HELO_PASS	SPF: HELO matches SPF record	
SPF_HELO_SOFTFAIL	SPF: HELO does not match SPF record (softfail)	
SPF_NONE	SPF: sender does not publish an SPF Record	
SPF_PASS	SPF: sender matches SPF record	
SPF_SOFTFAIL	SPF: sender does not match SPF record (softfail)	
SPOOF_COM2OTH	URI contains ".com" in middle	Contém o .COM no meio do remetente
SPOOF_GMAIL_MID	From Gmail but it doesn't seem to be...	
SPOOFED_FREEM_REPTO	Forged freemail sender with freemail reply-to	
SPOOFED_FREEMAIL	-	
SPOOFED_FREEMAIL_NO_RDNS	From SPOOFED_FREEMAIL and no rDNS	
STATIC_XPRIO_OLE	Static RDNS + X-Priority + MIMEOLE	
STOCK_IMG_CTYPE	Stock spam image part- with distinctive Content-Type header	

STOCK_IMG_OUTLOOK	Stock spam image part- with Outlook-like features	
STY_INVIS_DIRECT	HTML hidden text + direct-to-MX	
SUBJ_ALL_CAPS	Subject is all capitals	O assunto do email com letras maiúsculas
SUBJ_ALL_CAPS	Subject is all capitals	
SUBJ_DOLLARS	Subject starts with dollar amount	
SUBJECT_DIET	Subject talks about losing pounds	
SUSPICIOUS_RECIPS	Similar addresses in recipient list	
T_ANY_PILL_PRICE	Prices for pills	
T_DKIM_INVALID	Message has a DKIM or DK signature invalid	DKIM Inválido
T_DOC_ATTACH_NO_EXT	Document attachment with suspicious name	Documento anexo com nome suspeito
T_DOS_OUTLOOK_TO_MX_IMAGE	Direct to MX with Outlook headers and an image	
T_FILL_THIS_FORM_FRAUD_PHISH	Answer suspicious question(s)	
T_FILL_THIS_FORM_LONG	-	
T_FILL_THIS_FORM_SHORT	Fill in a short form with personal information	Formulário pré-preenchido com informações pessoais
T_FREEMAIL_DOC_PDF	MS document or PDF attachment- from freemail	Documento DOC ou PDF- mas oriundo de freemail
T_FREEMAIL_DOC_PDF_BCC	MS document or PDF attachment- from freemail- all recipients hidden	Documento DOC ou PDF- mas oriundo de freemail e em cópia oculta
T_FREEMAIL_RVW_ATTCH	Please review attached document- from freemail	Anexos oriundos de freemail
T_FUZZY_SPRM	-	
T_HK_SPAMMY_FILENAME		Nome de arquivo usado em anexos de spam
T_HTML_ATTACH	HTML attachment to bypass scanning?	
T_MONEY_PERCENT	X% of a lot of money for you	X% de dinheiro para você
T_MXG_LOWER_HDR_SPAM	Lower case header spam	Spam com palavras minúsculas
T_OBFU_ATTACH_MISSP	Obfuscated attachment type and misspaced From	Ofuscação de anexos e mudança no campo from
T_OBFU_JPG_ATTACH	JPG attachment with generic MIME type	
T_OBFU_PDF_ATTACH	PDF attachment with generic MIME type	
T_REMOTE_IMAGE	Message contains an external image	Contém imagens externas
T_TVD_FUZZY_SECTOR	-	
T_TVD_MIME_EPI	-	
T_TVD_MIME_NO_HEADERS	-	

TEQF_USR_POLITE	To and from user nearly same + polite greeting	
TO_EQ_FM_DIRECT_MX	To == From and direct-to-MX	
TO_EQ_FM_DOM_HTML_ONLY	To domain == From domain and HTML only	
TO_EQ_FM_DOM_SPF_FAIL	To domain == From domain and external SPF failed	
TO_EQ_FM_HTML_DIRECT	To == From and HTML only- direct-to-MX	
TO_EQ_FM_HTML_ONLY	To == From and HTML only	
TO_EQ_FM_SPF_FAIL	To == From and external SPF failed	
TO_IN_SUBJ	To address is in Subject	
TO_MALFORMED	TO: Has a malformed Address	Formação errada do e-mail no campo TO
TO_NO_BRKTS_HTML_IMG	To: lacks brackets and HTML and one image	
TO_NO_BRKTS_MSFT	To: lacks brackets and supposed Microsoft tool	
TRACKER_ID	Incorporates a tracking ID number	
TVD_PH_BODY_ACCOUNTS_PRE	The body matches phrases such as "accounts suspended"- "account credited"- "account verification"	
TVD_PH_SEC	Message includes a phrase commonly used in phishing mails	
TVD_RCVD_IP	Message was received from an IP address	
TVD_RCVD_IP4	Message was received from an IPv4 address	
TVD_SPACE_RATIO	-	
TVD_SPACE_RATIO_MINFP	Space ratio (vertical text obfuscation?)	
TVD_SUBJ_ACC_NUM	Subject has spammy looking monetary reference	
TVD_SUBJ_NUM_OBFU_MINFP	-	
UNDISC_MONEY	Undisclosed recipients + money/fraud signs	Destinatários com cópia oculta + indicação de fraude/dinheiro
UNICODE_OBFU_ZW	Obfuscating text with hidden characters	Texto com técnicas de ofuscação
UNICODE_OBFU_ZW_MANY	Heavily obfuscating text with hidden characters	Técnica avançada de ofuscação de texto
UNPARSEABLE_RELAY	Informational: message has unparseable relay lines	Informação: Não foi possível interpretar corretamente as informações de rota do email

UPPERCASE_50_75	message body is 50-75% uppercase	Corpo da mensagem com 50 a 75% de letras maiúsculas
UPPERCASE_75_100	message body is 75-100% uppercase	Corpo da mensagem com 75 a 100% de letras maiúsculas
UPPERCASE_URI	Link protocol has unexpected mixed case	
URG_BIZ	Contains urgent matter	Contém indicação de urgência
URI_DATA	"data:" URI - possible malware or phish	
URI_GOOGLE_PROXY	Accessing a blacklisted URI or obscuring source of phish via Google proxy?	
URI_HEX	URI hostname has long hexadecimal sequence	Possui sequencia hexadecimal
URI_IMG_CWINDOWSNET	Non-MSFT image hosted by Microsoft Azure infra- possible phishing	
URI_IPFS	References Interplanetary File System PtP content- probable phishing	
URI_IPFSIO	References Interplanetary File System PtP content via ipfs.io- likely phishing	
URI_NO_WWW_BIZ_CGI	CGI in .biz TLD other than third-level "www"	Código CGI em extensão .BIZ
URI_NO_WWW_INFO_CGI	CGI in .info TLD other than third-level "www"	Código CGI em extensão de TLD
URI_NOVOWEL	URI hostname has long non-vowel sequence	Sequência inválida
URI_PHISH	Phishing using web form	
URI_TRUNCATED	Message contained a URI which was truncated	
URI_TRY_3LD	"Try it" URI- suspicious hostname	
URI_WP_DIRINDEX	URI for compromised WordPress site- possible malware	
URI_WP_HACKED	URI for compromised WordPress site- possible malware	
URI_WP_HACKED_2	URI for compromised WordPress site- possible malware	
URI_WPADMIN	WordPress login/admin URI- possible phishing	
URIBL_ABUSE_SURBL	Contains an URL listed in the ABUSE SURBL blocklist	
URIBL_BLACK	Contains an URL listed in the URIBL blacklist	
URIBL_CSS	Contains an URL's NS IP listed in the Spamhaus CSS blocklist	

URIBL_CT_SURBL	Contains an URL listed in the CT SURBL blocklist	
URIBL_DBL_ABUSE_REDIR	Contains an abused redirector URL listed in the Spamhaus DBL blocklist	
URIBL_DBL_MALWARE	Contains a malware URL listed in the Spamhaus DBL blocklist	
URIBL_DBL_PHISH	Contains a Phishing URL listed in the Spamhaus DBL blocklist	
URIBL_DBL_SPAM	Contains a spam URL listed in the Spamhaus DBL blocklist	
URIBL_DM_SURBL	Contains an URL listed in the DM SURBL blocklist	
URIBL_GREY	Contains an URL listed in the URIBL greylist	
URIBL_JP_SURBL	Has URI in JP at http://www.surbl.org/lists.html	
URIBL_PH_SURBL	Contains an URL listed in the PH SURBL blocklist	
URIBL_RED	Contains an URL listed in the URIBL redlist	
URIBL_SBL	Contains an URL's NS IP listed in the Spamhaus SBL blocklist	
URIBL_SBLXBL	Contains a URL listed in the SBL/XBL blocklist	
USER_IN_DEF_DKIM_WL	From: address is in the default DKIM welcome-list	
VFY_ACCT_NORDNS	Verify your account to a poorly-configured MTA - probable phishing	
WEIRD_PORT	Uses non-standard port number for HTTP	Usa porta de HTTP não padrão
WEIRD_QUOTING	Weird repeated double-quotation marks	
WIKI_IMG	Image from wikipedia	
WORD_INVIS	A hidden word	
WORD_INVIS_MANY	Multiple individual hidden words	
XFER_LOTSA_MONEY	Transfer a lot of money	
XPRIO	Has X-Priority header	

Assinatura de IA	Descrição em Inglês	Descrição em Português
HSC_MAIL_REPUTATION	HSC Artificial Intelligence - Analysis of e-mail sending behavior to identify an unusual number of messages or the presence of threats	Analisa o comportamento de envio de e-mails, para identificar envio de números de e-mails fora do padrão, perante presença de ameaça.
HSC_AI_BANK_PHISHING	HSC Artificial Intelligence - Identification of textual elements indicating banking fraud	Elementos no texto do e-mail, que indicam possível fraude bancária
HSC_AI_GOV_SPOOFING	HSC Artificial Intelligence - Identification of messages attempting to impersonate government communications	Indicação de contexto do e-mail indicando fraude de e-mails do governo
BAYES_00	HSC Artificial Intelligence - Identification of a 0% possibility of SPAM based on Machine Learning models	Indicação de 0% de ser spam, baseado em modelos de Aprendizagem em Máquina
BAYES_05	Identification of SPAM probability from 1% to 5% based on Machine Learning models	Indicação de 0% a 5% de ser spam, baseado em modelos de Aprendizagem em Máquina
BAYES_20	Identification of SPAM probability from 5% to 20% based on Machine Learning models	Indicação de 5% a 20% de ser spam, baseado em modelos de Aprendizagem em Máquina
BAYES_40	Identification of SPAM probability from 20% to 40% based on Machine Learning models	Indicação de 20% a 40% de ser spam, baseado em modelos de Aprendizagem em Máquina
BAYES_50	Identification of SPAM probability from 40% to 60% based on Machine Learning models	Indicação de 40% a 60% de ser spam, baseado em modelos de Aprendizagem em Máquina
BAYES_60	Identification of SPAM probability from 60% to 80% based on Machine Learning models	Indicação de 60% a 80% de ser spam, baseado em modelos de Aprendizagem em Máquina
BAYES_80	Identification of SPAM probability from 80% to 95% based on Machine Learning models	Indicação de 80% a 95% de ser spam, baseado em modelos de Aprendizagem em Máquina
BAYES_95	Identification of SPAM probability from 95% to 99% based on Machine Learning models	Indicação de 95% a 99% de ser spam, baseado em modelos de Aprendizagem em Máquina
BAYES_99	Identification of SPAM probability from 99% to 99.98% based on Machine Learning models	Indicação de 99% a 99.98% de ser spam, baseado em modelos de Aprendizagem em Máquina
BAYES_999	Identification of SPAM probability from 99.9% to 100% based on Machine Learning models	Indicação de 99.9% a 100% de ser spam, baseado em modelos de Aprendizagem em Máquina

Apêndice 9 – Notas de Versão

Release 5.4.2-3 (01/06/2026)

Ajustes:

- [MLI-1202] - Melhoria na Listagem de Integração Microsoft 365
- [MLI-1294] - Alteração Integração Google
- [MLI-1240] - Regra composta SPAM

Features:

- [MLI-1119] - Permitir exportar e importar a lista de Controle de Sessões SMTP
- [MLI-1037] - AllowList / BlockList - Adicionar validação de regex
- [MLI-510] - Implementar log rotate nas tabelas

Correções:

- [MLI-1238] - Execução script postBuilder única
- [MLI-1239] - Persistência script
- [MLI-706] - Restart do SmartDefender interrompe a filtragem da mensagem
- [MLI-708] - Mensagem processada no agente não é exibida na console
- [MLI-935] - Remoção emails de grupos
- [MLI-1036] - DMARC - Dashboards não estão respeitando o nível de visualização do usuário
- [MLI-1120] - Não aparecem as URLs no SmartDefender
- [MLI-1178] - Autenticação Integrada MLI x Microsoft - Possível vetor de enumeração de usuários
- [MLI-1187] - Termo "Whitelist" não substituído por "Allow list" na tela de SPF
- [MLI-1213] - Bug no usuário Administrador Customizado - Perde permissões em "Ações para E-mail"
- [MLI-1237] - Importação de regras de allow e block list em migração de ambientes
- [MLI-1244] - Informação exibida incorretamente em relatórios do MLI
- [MLI-1249] - Notificação de Quarentena - Subdominios
- [MLI-1261] - Update Sistema - Deslogar usuário no término
- [MLI-1273] - Backup - Snapshot - Console MLI - Versão 5.3
- [MLI-1289] - Regras de controle de fluxo não respeitam prioridade
- [MLI-1293] - Mail Inspector > Sandbox / TAP
- [MLI-1298] - Connection bug Smart Defender

Release 5.4.1 (08/05/2026)

Ajustes:

- [MLI-1228] - Core Manager detach ao executar comandos
- [MLI-1229] - Adicionar Volume de certificados apache
- [MLI-1247] - Atualização script Watchdog

Features:

- [MLI-1218] - Habilitar/Desabilitar do ESET deve ser exibida como primeiro item da listagem

- [MLI-1223] - Relatório Licenças
- [MLI-1224] - Habilitar/Desabilitar Notificação de Quarentena por ponto
- [MLI-1265] - Implementação Nova identidade visual de alguns módulos
    - [MLI-1267] - Implementação nova identidade visual do módulo de Aplicar Regras
    - [MLI-1268] - Implementação nova identidade visual do módulo de Relatórios
    - [MLI-1272] - Implementação scripts de interação com APIs Microsoft / Google Workspace

Correções:

- [MLI-1210] - Falha no envio de notificação em e-mails quarentenados por regra DLP
- [MLI-1221] - Correção de vulnerabilidades
- [MLI-1230] - Configuração Ponto no builder incorreta
- [MLI-1231] - Regra LDAP sem usuários
- [MLI-1233] - Configuração Mailhub errada
- [MLI-1241] -Problema na ordenação de Regras DLP
- [MLI-1252] - Falha na tentativa de validação da integração Google ao habilitar domínio
- [MLI-1254] - Notificações de Quarentena - Criação de nova regra apaga dados da regra padrão
- [MLI-1270] - Relatório Licenças formato csv incompleto

Release 5.4

Ajustes:

- [MLI-827]- Especificar quantidade de conexões o serviço SMTP irá abrir
- [MLI-962] - Digest - Melhorias na configuração das regras
- [MLI-1034] - Inclusão de script e disponibilização na tela de Diagnóstico
- [MLI-1107] - Padronização de Termos: WhiteList > Allow List / BlackList > Block List
- [MLI-1127] – Consolidação do Minerador de Relatórios
- [MLI-1157] - Configurações - Tempo máximo de cache de escaneamento
- [MLI-1162] - Ajuste de Macro do OpenDMARC e Inclusão de Assinatura DMARC_PASS
- [MLI-1212] - Builder relay_recipients considerar mais tabelas
- [MLI-1201] - Alteração de label da tabela de volume para tamanho

Features:

- [MLI-1035] - DMARC Analyzer - Configurar stack para funcionamento automático
- [MLI-1094] - Patch - Permitir persistir pacotes por versão
- [MLI-1146] - Integração com TAXII Server
    - [MLI-1167] - Tela de integração com TAXII Server - Backend
- [MLI-1147] – Possibilidade de Ativar ou Desativar o antivírus “ESET Scan Engine”
- [MLI-1148] - Ativar função de converter DOC malicioso em PDF com imagem
    - [MLI-1149] - Ativar função de converter doc malicioso em PDF com imagem – Backend
- [MLI-1150] - Relatórios - Sumário de conexões TLS
- [MLI-1151] - Relatórios - Quantidade de conexões vindas por país
- [MLI-1153] - Relatórios - Top categorias URL e quantidade SPAM URL
- [MLI-1158] - Relatórios - Ranking de Domínios Analisados por DMARC
- [MLI-1154] - Mensagens afetadas - Consulta Smart Defender

- [MLI-1155] - Filtros de SPAM - Adicionar o controle “GrayMail”
- [MLI-1156] - Filtros de SPAM - Adicionar o controle “GrayMail” - Definição do builder
- [MLI-1196] - Implementar logs de debug Microsoft 365 Addon

Correções:

- [MLI-1194] – Correção de vulnerabilidade identificada no MLI na versão 5.3.2-3
- [MLI-882] - Sincronização de Usuários LDAP - Microsoft365 365
- [MLI-975] - Relatório de Quarentena Indisponível
- [MLI-1022] - Reprocessamento de mensagem não reprocessa assinaturas
- [MLI-1050] - Correção Login Social
- [MLI-1053] - Tempo de Execução dos Scripts
- [MLI-1063] - Busca rápida em Administração > Usuários do Sistema retorna registros errados
- [MLI-1067] - Integrações > Ver Lista não respeita paginação
- [MLI-1088] - Erro "Class 'App_Mail_UpdateNotify' not found"
- [MLI-1118] - Erro ao analisar RegExp em anexos
- [MLI-1121] - O Log de Evento não aparecem todas as ações
- [MLI-1128] - Correção Redirect Login Externo Microsoft
- [MLI-1138] - Impossibilidade de liberar/reenviar mensagens quarentenadas
- [MLI-1140] - Não aceita determinados caracteres na senha
- [MLI-1171] - Problema no botão "Usuários Afetados" Notificações de Quarentena
- [MLI-1179] - Snapshots e-mails válidos
- [MLI-1181] - Ativar função de converter DOC malicioso em PDF com imagem
    - [MLI-1185] - Ativar função de converter doc malicioso em PDF com imagem – Backend
- [MLI-1195] - Snap de Configuração Não está sendo realizado
- [MLI-1198] - Tem vezes que o Plugin do Office365 dá erro ao acessar a Quarentena
- [MLI-1200] - MSOAR na Microsoft
- [MLI-1205] - Erro ao executar exupdate em hmg - Fix MLI-1088
- [MLI-1211] - Problema no Sincronismo LDAP
- [MLI-1209] - Fix lista de emails não retornando dados

Release 5.3.3 (17/11/2025)

Ajustes:

- [MLI-1055] - Sincronismo - Modificar o mecanismo de snapshot para somente adicionar/atualizar registros e nunca apagar

Features:

- [MLI-901] - Incluída opção de Ativar Relay Automático para G-Suite
- [MLI-1084] - Criação de Debug na Integração Google

Correções:

- [MLI-643] - Anti Spoofing – SPF
- [MLI-744] - Caracter % em link de redirecionamento "bypass" a análise do SmartDefender

- [MLI-798] - Correção de a cada 5 minutos o MLI fazia backup sozinho
- [MLI-884] - Erro de remetente no envio de e-mail de teste em ferramenta de diagnóstico do MLI
- [MLI-896] - Remoção indevida de Anexos
- [MLI-923] - Microsoft 365 - Erro no funcionamento do addon quando login != e-mail
- [MLI-944] - Integrações - após desativar não era mais possível reativar
- [MLI-963] - Central de Atualizações – Acompanhar não estava funcionando devidamente
- [MLI-965] - Redirecionamento do Fluxo de Saída
- [MLI-974] - Configuração do usuário customizado está mostrando desabilitado Integração do Workspace
- [MLI-985] - Admin Customizado não consegue incluir e-mail em Blacklist/Whitelist mesmo com controle sobre todo o domínio
- [MLI-986]- Smart Defender - By Pass de links
- [MLI-1011] - LDAP - Ajustar script mliLdapUserSync para suportar caixas corporativas
- [MLI-1025] - Filtragem de data do Log de Eventos
- [MLI-1026] - Atualização do IP do ponto de acesso
- [MLI-1027] - Diferença de tamanho do arquivo baixado - Acaba baixando arquivo texto com o código
- [MLI-1046] - Digest - Erro ao solicitar WhiteList/BlackList via Digest – versão nova do MLI
- [MLI-1047] - Erro ação Digest
- [MLI-1049] - Erro no link de notificação de usuário - Notificação solicitando confirmação de usuário para MLI administrar e-mail
- [MLI-1054] - DIGEST - Resumo Blacklist/Whitelist
- [MLI-1058] - Ativado a integração do google Workspace, mas não habilitou
- [MLI-1059] - Não aceita senha nova
- [MLI-1060] - Erro ao aplicar as configurações
- [MLI-1073] - Relatório Gerencial - Dados inconsistentes
- [MLI-1078] - Erro ao Aplicar as Configurações
- [MLI-1085] - Erro ao baixar arquivo anexo
- [MLI-1086] - Integração Google - Remoção E-mail Notificação Dev \(report\)
- [MLI-1089] - GoogleSync - ERRO no processo de sincronização de Usuários

Release 5.3.2 (04/09/2025)

Ajustes:

- [MLI-885] – Ajuste - Diagnóstico - Indicar o real erro em teste (indicava somente que deu erro de CURL)
- [MLI-886] - Configurar rede ao criar Ponto de Acesso
- [MLI-966] - Adicionado o novo script no MLI

Features:

- [MLI-901] - Incluída opção de Ativar Relay Automático para G-Suite

Correções:

- [MLI-842] - Backup - Erro ao mandar apagar arquivos de backup

- [MLI-845] - Filtro E-mails - Não acha direito a URL na Pesquisa Avançada
- [MLI-878] - E-mail - O MailInspector estava permitindo execução automática de scipt (direto em código HTML) mesmo em perfil de usuário
- [MLI-880] - Não apresenta os e-mails importados em Administração > Integrações > Microsoft 365 > Ver Lista
- [MLI-883] - Ponto/Cluster não encontrado
- [MLI-892] - Usuários do Sistema - Perfil Administrador
- [MLI-914] - E-mail Compliance - Quando é criada regra, o nome de Grupos aparecia quebrado
- [MLI-956] - Digest problema na identificação do Token
- [MLI-969] - Smart Defender - Exibição URLs da Base Local
- [MLI-1010] - Builder – Correção de alteração de Expressão em palavra reservada
- [MLI-1018] - Configuração do SNMP do ponto de acesso estava aplicando a configuração do cluster
- [MLI-1019] – Correção de limpeza automática de backups
- [MLI-1020] - Ajustes no script de verificação de permissão
- [MLI-1021] - Integração Zimbra - Não estava permitindo realizar ações de MSOAR

Release 5.3.1 (17/07/2025)

Ajustes:

- [MLI-781] - Ajuste - Healthcheck para serviço Core Manager
- [MLI-879] - Ajuste - Docker - Implementar suporte para script pre/post no entrypoint
- [MLI-919] - Ajuste - Captcha - Melhorias na função de autenticação do Captcha

Correções:

- [MLI-661] - Correção - Expiração de Sessão Ativa
- [MLI-669] - Correção - LDAP Consulta Segura
- [MLI-670] - Correção - Apache - Cadeia Completa
- [MLI-671] - Correção - E-mails - Problemas de filtragem ao ordernar tela
- [MLI-672] - Correção - E-mails - Problema no Download de Anexos
- [MLI-677] - Correção - Log de Eventos - Erro ao realizar a pesquisa
- [MLI-685] - Correção - Perfil Administrador Customizado - Não está respeitando a ACL de ações liberadas
- [MLI-687] - Correção - Diagnóstico - Erro no Teste de Conectividade Office 365
- [MLI-728] - Correção - Usuários do Sistema - Erro na inserção de nova caixa com string parcial
- [MLI-731] - Correção - Digest - Mensagem de Erro conforme período de liberação
- [MLI-749] - Correção - Tela de Diagnóstico - Administrador Customizado
- [MLI-790] - Correção - E-mails - Detalhes da Mensagem - Ao clicar no icone VirusTotal apareceu erro de arquivo não encontrado
- [MLI-823] - Correção - Administração - Notificação de Quarentena
- [MLI-839] - Correção - Login - Usuário não autentica ao realizar acesso via SSO
- [MLI-841] - Correção - Notificação de Quarentena expira em 1 dia com qualquer periodo configurado.
- [MLI-844] - Correção - Agendamento de Relatórios - Erro ao executar o scheduler
- [MLI-851] - Correção - Central de Atualizações - Erro ao aplicar pacote manual

- [MLI-854] - Correção - Microsoft 365 - Erro no funcionamento do addon após remoção do suporte a token
- [MLI-865] - Correção - Builder - Erro ao Aplicar as configurações: DMARC
- [MLI-867] - Correção - Erro ao Aplicar Configurações: Cluster
- [MLI-869] - Correção - Download Pesquisas e Cabeçalhos de Mensagens
- [MLI-889] - Correção - Digest - Botão Pré Visualizar
- [MLI-900] - Correção - RBLs Externas - Seleção da interface não é aplicada no arquivo final
- [MLI-903] - Correção - Builder - Não aplica as configurações do Outbreak no ponto
- [MLI-912] - Correção - Integrações da MS 365 - M-SOAR em domínio está mostrando \[object Object\]
- [MLI-913] - Correção - Configurações - E-mail Compliance - Tipo Quarentena não está mostrando a lista
- [MLI-915] - Correção - Configuração do Digest - Período de execução
- [MLI-921] - Correção - Integrações Google - M-SOAR em domínio está mostrando \[object Object\]
- [MLI-922] - Correção - Erro ao usar o MSOAR no Gmail
- [MLI-930] - Correção - Logs de auditoria do msoar
- [MLI-933] - Correção - Microsoft 365 - Erro ao realizar ações de remover via M-SOAR
- [MLI-934] - Correção - Pesquisas Log de Eventos

Features:

- [MLI-787] - Feature - Integrações - Melhorar a experiencia de configuração Microsoft 365 e Google
- [MLI-931] - Feature - Implementar MSOAR no Zimbra
- [MLI-932] - Feature - Captcha - reload invisivel (melhoria)

Release 5.2.20-5 (16/11/2024)

Ajustes:

- MLI-485 - Ajuste - Impedir o usuário continuar no sistema durante a restauração do backup
- MLI-511 - Ajuste - Backup não faz backup do Auditlog e dos próprios jobs de Backup
- MLI-690 - Ajuste - Merge, correções e teste versão 5.3
- MLI-713 - Ajuste - MLI - Relatório de Vulnerabilidades v1. 07/2024 - Implementar as melhorias identificadas no relatório anexo Alta
- MLI-721 - Ajuste - MLI - Relatório de Vulnerabilidades v2. 07/2024 - Implementar as melhorias identificadas no relatório anexo Média
- MLI-722 - Ajuste - MLI - Relatório de Vulnerabilidades v3. 07/2024 - Implementar as melhorias identificadas no relatório anexo
- MLI-737 - Ajuste - Adicionar Script
- MLI-740 - Ajuste - Esconder temporariamente Mailbox Service
- MLI-766 - Ajuste - MailScanner - Implementar controle de fila por Redis
- MLI-795 - Ajuste - Remover Entradas WhiteList de Domínios do Policyd-SPF

Correções:

- MLI-186 - Correção - DLP - Implementar contador de expressões por HTML ou Texto
- MLI-354 - Correção - Alerta de Monitoramento do Logger na Console

- MLI-506 - Correção - DoS na consulta Smart Defender
- MLI-512 - Correção - Corrigir backup corrompido (Remover MYSQL force)
- MLI-548 - Correção - Admin Customizado visualiza Logs de MTA de domínio que não gerencia
- MLI-568 - Correção - Não restaurou configurações presentes no backup
- MLI-574 - Correção - Não apresenta o conteúdo da mensagem
- MLI-600 - Correção - Vulnerabilidades encontradas - Pentest Blackbox
- MLI-607 - Correção - Não apresenta o e-mail como texto
- MLI-619 - Correção - Adicionar Log do Docbleach no Logrotate
- MLI-639 - Correção - Digest - Implementar confirmação do usuário para execução das ações
- MLI-646 - Correção - Não indica o país, quando pausa o mouse sobre o ícone do país
- MLI-649 - Correção - Ativar Relay Automático para Office 365
- MLI-650 - Correção - Configurações do MTA
- MLI-696 - Correção - Digest - Caracteres Especiais
- MLI-711 - Correção - Mensagens com anexo dão erro ao tentar abrir os detalhes de um e-mail
- MLI-712 - Correção - Erro ao tentar abrir detalhes de um e-mail
- MLI-748 - Correção - Homologação da 5.3 - Falhas de permissões
- MLI-750 - Correção - Tela Relatórios - Capacity Planning
- MLI-751 - Correção - Corrigir restart do hscpolicyd no script de watchdog
- MLI-767 - Correção - Correções pontuais e melhorias de estabilidade

Features:

- MLI-34 - Feature - Integrações - G-Suite
- MLI-187 - Feature - Disaster Recovery - Permitir acessar a tela de Backup sem agente configurado
- MLI-256 - Feature - Configurar Identity Platform e Multi-Tenancy no Google Workspace
- MLI-288 - Feature - Docker - Otimizar stack e container
- MLI-367 - Feature - MS365 - Criar Mecanismo de Post Delivery Action Automatizada via API
- MLI-368 - Feature - DMARC Analyzer - Melhoria em Dashboards e Relatórios
- MLI-383 - Feature - E-mails - Criar Aba Anexos em Detalhes da Mensagem
- MLI-405 - Feature - Ajuste Configuração do Logger
- MLI-406 - Feature - Utilitário - Consulta de mensagens e ações do M-SOAR
- MLI-423 - Feature - DKIM - Sempre vem como default / Incluir coluna SELECTOR
- MLI-464 - Feature - Backup - Notificação Sucesso / Falha
- MLI-487 - Feature - Upload de logo das empresas em diversas telas, relatórios e mudança de cor do layout
- MLI-552 - Feature - Builder Rsyslog
- MLI-557 - Feature - Relatórios Gerenciais - Sumário por Domínio
- MLI-598 - Feature - Criar campo hostname na tabela mliPoint
- MLI-602 - Feature - Aumentar limite máximo de upload de arquivo Média
- MLI-605 - Feature - TLS/SSL - Alterar Parametros de Troca de Chave
- MLI-651 - Feature - Implementar Consulta das URLs e Hashs no site do AlienVault e Virustotal
- MLI-682 - Feature - Expressão Black/WhiteList
- MLI-734 - Feature - Integrações - Controle de domínios já integrados e unificação do M-SOAR
- MLI-735 - Feature - HSC Remote Assistance - Suporte para funcionamento em ambiente Docker

- MLI-98 - Feature - Docker - Implementar serviço de comunicação Host x Container

Release 5.2.20-3 (30/10/2024)

Inclusão de informações no manual:

- Inclusão de termos no Glossário e correções ortográficas
- Inclusão de tela de indicação da funcionalidade de HSC AI Cyber Assistant

Release 5.2.20 (08/07/2024)

Correções:

- [MLI-693] - Ajuste TLS Cifer Hard MLI
  Obs: Aumento das cifras disponíveis no modo Hardening
- [MLI-700] - Erro ao Reprocessar Mensagem - Correção de Backport
- [MLI-709] - Falha de Execução do MailScanner - Melhorias de estabilidade do processo e do log

Release 5.2.19 (18/04/2024)

Melhorias (novas funcionalidades e/ou ajustes de funcionalidades):

- [MLI-581] - TLS/SSL - Alteração da ordem das cifras fortes para atendimento a compliance;

Correções:

- [MLI-603] - Configuração do Modo de Operação TLS não persiste - Em toda atualização de versão do sistema, a configuração de TLS voltava a operar em Modo de Compatibilidade
- [MLI-606] - QRCode Google - O Gerador de QRCode não estava gerando corretamente a imagem
- [MLI-656] - Pontuação zerada - Em alguns momentos, o mecanismo de filtragem retorna zerado impedindo o correto funcionamento da filtragem;

Release 5.2.18 (11/01/2024)

Melhorias (novas funcionalidades e/ou ajustes de funcionalidades):

- [MLI-382] - Permitir Filtragem de E-mails por HASH e tipo de arquivo
- [MLI-392] - E-mails - Executar Ações em Lote
- [MLI-429] - Implementar e documentar utilização da busca de e-mail utilizando API do MLI
- [MLI-555] - Remover a opção de Reenviar Mensagem em Ações em lote, pois ele faz exatamente a mesma coisa que Liberar Todas Mensagens
- [MLI-587] - SMTP Smuggling - Implementar proteção na camada de MTA

Correções:

- [MLI-178] - Backup - Exclusão de Cluster não deveria apagar as configurações de Backup
- [MLI-182] - Backup - Disaster Recover e Restore do Backup não funciona
- [MLI-184] - 2FA - Exigir que seja salva configuração para entrar em vigor
- [MLI-243] - Administrador Customizável - Melhorar a capacidade de controle
- [MLI-247] - E-mails- Adicionar para WL/BL não oferece From do Header

- [MLI-364] - Campo Grupo de Usuarios > Domínios não casa realmente como domínio, mas casa como string
- [MLI-379] - E-mails - Aba Smartdefender não sanfornar os Hash dos anexos
- [MLI-422] - Problema em restauração de backup
- [MLI-426] - Problema de envio de e-mail da console de adm quando o cluster é tipo MX
- [MLI-449] - SmartDefender - Limpar cache não funciona
- [MLI-460] - Limpeza de arquivos temporários
- [MLI-461] - Regras Avançadas \(SPAM e DLP\) - Listar todas assinaturas
- [MLI-477] - MS365 - Erro no Assunto no Reporte de mensagem
- [MLI-480] - Formatação de RegExp
- [MLI-482] - Status do agente na Central de atualizações
- [MLI-483] - Fila de E-mails - Admin da nuvem enxerga fila de outros clientes
- [MLI-498] - TAP URL - Falha na reescrita de URLs com autenticação basic
- [MLI-504] - TAP URL - Mensagem de erro indevida
- [MLI-517] - Aba Smart Defender - Exibe Sanfona para anexos
- [MLI-519] - Digest - Mensagens Indevidas
- [MLI-523] - Exibição da BL/WL
- [MLI-524] - Backup - Não exibe nenhuma rotina de execução
- [MLI-526] - SandBox - URLS estão com erro
- [MLI-531] - TAP - Adequar a consulta
- [MLI-532] - Smartdefender - Consulta manual
- [MLI-533] - E-mails - Aba Smartdefender com erro na consulta de URL
- [MLI-535] - E-mail - Aba Filtros de Conteúdo exibe NULL
- [MLI-536] - E-mail - Aba Downloads não exibe os anexos
- [MLI-537] - E-mail - Aba SmartDefender exibe NULL
- [MLI-540] - E-mails - Smartdefender Phishign Detection
- [MLI-541] - Microsoft 365 - Bug no parse do Message-ID
- [MLI-546] - Envio de Logs para a console
- [MLI-551] - Alterar Horários \(exupdate e rules_description_populate\)
- [MLI-565] - E-mails - Não abre os detalhes de mensagens removidas pela limpeza de quarentena
- [MLI-567] - Backup - Erro no download do arquivo de Logs
- [MLI-569] - E-mails - Ações Liberar mensagem perde dados do header
- [MLI-576] - E-mails - Message ID fica em branco na aba Cabeçalho
- [MLI-582] - WL/BL - Registros criados pelo usuário não são exibidos para ele
- [MLI-587] - SMTP Smuggling - Implementar proteção na camada de MTA
- [MLI-589] - WL/BL - Falha com o botão Limpar pesquisa

Release 5.2.17 (24/10/2023)

Melhorias (novas funcionalidades e/ou ajustes de funcionalidades):

- [MLI-71] DLP - Identificar qual palavra que casou com o dicionário no corpo/assunto/anexos
- [MLI-76] Criar Exceção de E-mails e Domínios que não devem ser feito MailSplit
- [MLI-289] Padronização - Implementar Tabela UTF-8 automaticamente nos templates
- [MLI-363] API - Suporte para ações de MSOAR

- [MLI-401] TLS / SSL - Alinhar componentes da tela - v.2
- [MLI-435] Limpeza do cache no redis - Melhoria de desempenho
- [MLI-494] CDR - Ativação de scan em Documentos .ZIP
- [MLI-318] Painel de Controle - Alertas para agentes Inativos

Correções:

- [MLI-101] E-mails - Faltam filtros em Pesquisa Avançada > Regras de Controle Avançado
- [MLI-111] E-mails - Não apresenta alguns anexos para download
- [MLI-160] SmartDefender - Preview incompleto de URLs se sobrepoem a novas consultas
- [MLI-167] Conectores Externos - Remover da tela de Debug a senha
- [MLI-202] SmartDefender - Reclassificação de Arquivo - Dados errados
- [MLI-253] SmartDefender - Termo Indesejável no Wizard
- [MLI-265] Reescrita de URL - Caracteres cirilicos não funcionam corretamente
- [MLI-322] Smart Defender - Erro na consulta de URLs com caracteres cirilicos
- [MLI-333] Integrações - Erro na regra padrão Add-on MS 365
- [MLI-339] Notificação de Quarentena - Problema na pesquisa de Usuários Afetados
- [MLI-340] TAP - Tratar URLs que contém @
- [MLI-418] Falha ao visualizar a aba Smartdefender nos detalhes da mensagem
- [MLI-484] E-mails - Aba Smart Defender não exibe a categoria correta no status Atual
- [MLI-489] TAP URL - Falha na proteção de URLs com carateres especiais
- [MLI-497] Tratamento de Codificação no "TO" do "Header"

Release 5.2.16 (15/08/2023)

Melhorias (novas funcionalidades e/ou ajustes de funcionalidades):

- TLS / SSL - Alinhar componentes da tela
- Painel de Controle - Incluir controles para o serviço de atualização do AV
- Backup - Implementar campo para determinar diretório no FTP
- Notificação de Solicitação de Liberação - Adicionar campos
- E-mails - Remoção de campos da Pesquisa Avançada para perfil de usuários
- Notificação – Melhoria no reporte de Ameaças
- Compliance – Ajuste da regra de notificação no DLP
- Notificação – Ajuste no reporte de Outro Bloqueios
- Monitoramento – Adição de Monitoramento do Apache nos watchdogs
- Filtragem - Melhorias na Filtragem do AV
- Whitelist / Blacklist - Melhoria no builder e processo de filtragem
- Remover a ação "Adicionar ao Grupo " da tela de realtime e-mail do perfil usuário

Correções:

- E-mails - Pesquisa de quarentena retornava com e-mails indevidos
- E-mail - Smart Defender - Ajustada a consulta do cabeçalho from
- Aplicar Configurações - Ponto de Acesso com Status Inativo
- Performance do Sistema - Ponto de Acesso com Status Inativo

- Painel de Controle - Ponto de Acesso com Status Inativo
- E-mails - Falha de segurança na busca dos dados
- Ponto de Acesso - Alertas de monitoramento para serviços desativados
- Digest - Reportar Mensagem
- E-mails - Indicação de tamanho dos anexos contidos no e-mail
- E-mails - Ação Reprocessar gera erro relacionado ao M-SOAR
- E-mails - Ação Reportar gera erro relacionado ao M-SOAR
- E-mails - Ação Remover da quarentena gera erro relacionado ao M-SOAR
- Criação de Regras Avançadas (SPAM e DLP) - Listar todas as assinaturas
- Erro ao visualizar detalhes da mensagem
- Ataque Dirigido - Erro em regras de reescrita de URL
- Não adiciona usuários ao domínio
- Correção do estado do BD - Transaction DeadLock na criação de usuários
- Usuario - Não salva
- Erro ao salvar Regras de Compliance
- Problema permanece em ambiente que possua cluster e ponto
- E-mails - Ação Liberar Mensagem com Erro
- E-mails - Erro ao visualizar aba Texto
- E-mails - Permitir ações administrativas quando M-SOAR estiver habilitado
- E-mails - Aba Smartdefender não exibe o Hash dos anexos
- Bug ao ver message trace nos detalhes da mensagem na tela de realtime e-mails
- E-mails - Ajustes na ação Marcar como Confiável/Indesejável

Release 5.2.13-1 (27/03/2023)

- Feature – Seleção pela interface do posicionamento da assinatura de e-mails
- Feature - Remover usuários importados pelo LDAP
- Feature – Inclusão de novos dicionários pré-instalados:
    - CNH;
    - Placa de Carro padrão Mercosul;
    - Número de passaporte brasileiro;
    - E-mail (seguindo padrão RFC 5322)
- Feature - Inclusão de observação ao aplicar configuração, dessa forma permitindo indicar a justificativa das alterações de parâmetros efetuado pelo administrador
- Feature – Permite solicitação de mudança de categorização de URL (recategorização) direto pelo Smart Defender
- Feature – Inclusão de bandeira do país de origem do e-mail em uma coluna de Realtime > E-mails;
- Feature – Permite clonar pontos de filtragem
- Fix – Checkbox de TLS/SSL carregava sempre desmarcada. Efetuada a correção
- Feature – Realização da consulta de WHOIS de forma assíncrona
- Feature – Apresentação da última atualização do sistema
- Fix – Correção de API onde apresentava erro 404
- Fix – Correção de RegEx inválida
- Fix – Correção de acentuação no assunto do e-mail
- Fix – Correção no contador de número de ocorrências

- Fix – Correção na ação de recrita de URL, onde estava reescrevendo link de telefones nos e-mails
- Fix – Correção em fila de e-mails que estavam com data futura
- Fix – E-mail de teste (em diagnóstico) agora utiliza o remetente configurado
- Fix – Fila de e-mails estava apresentado data errada em pesquisas de mensagens de outros anos
- Fix – Pesquisa de e-mails na fila de e-mails estava retornando resultado errado
- Fix – Em RealTime > E-mails a coluna data e hora não informava a hora

Release 5.2.12-1 (27/01/2023)

- Feature – Criada na interface gráfica a integração com API Crowd Strike Falcon Intelligence

Release 5.2.11-1 (07/11/2022)

- Feature – Adicionada na tela de detalhes do e-mail a pontuação indicando que foi utilizado o cache
- Fix – Redução de interação para casamento de whitelist e blacklist no SmartDefender
- Fix – Melhora no desempenho na coleta de informações dos logs dos agentes
- Fix – Correção na falha de reescrita de URL
- Fix – Remoção de dependência de memcached
- Fix – Adicionado verificação de destinatário em regras de DLP
- Fix - Correção de Conector Zimbra – UserSync
- Fix – Correção de erro na importação de CSV
- Feature – Inclusão de opção TODOS no relatório de Sumário por Domínio
- Fix – Correção de vulnerabilidade de token com uso do digest

Release 5.2.10-1 (18/08/2022)

- Fix - E-mail - Ajuste de performance
- Fix - E-Mail - Consulta unica para os registros da aba SmartDefender
- Fix - Relatorios - Volume de Mensagens exibe linha do tempo invertida
- Fix - MTA - Relay Recipients
- Fix - E-mails - Mensagens não quarentenadas estão apresentando como quarentena NULL
- Fix - Relatórios - Incluir opção TODOS no Sumário por Domínio
- Fix - Usuário padrão com opção de liberação de e-mail quarentenado como E-mail Impostor
- Fix - Correção de atualização no antivírus ESET
- Fix - Atualização do protocolo TLS utilizado na comunicação com Office 365

Release 5.2.7-1 (05/04/2022)

- Fix - RPC Client - Modificar porta de destino se localhost
- Fix - Microsoft 365 – Correção de compatibilidade de Add-on com IE11
- Fix - Fraude de E-mail - Principais Alvos não retorna os e-mails afetados
- Fix - E-mails – Correção de divergência de dados exportados divergem do Nome da Coluna
- Fix - E-mails – Correção de alteração indevida de mensagem ao liberar mensagem
- Fix - E-mails - Erro no reenvio de mensagens sem o campo To no Header
- Fix - E-mails - Erro ao reprocessar múltiplas mensagens
- Fix - Smart Defender – Removida a permissão de usuário comum para recategorização de URLs
- Fix - SmartDefender - Erro na reclassificação de Host
- Fix - E-mails - Aba SmartDefender exibe URLs com false, null e mailto

- Fix - Notificações - Padronização - Outros Bloqueios
- Fix - Fila de E-mails - Falha ao excluir e-mails em massa
- Fix - Perfil de Usuário - Falha ao alterar senha de admisnistrador customizado
- Fix - TAP - Conversão de URL
- Fix - Logs do MTA - Apresenta dados de outros clusters
- Fix - E-mails - Ajuste na Label para alguns casos de Fraude de E-mail
- Fix - Relatórios - Erro na consulta e problema nos filtros
- Fix - Problemas ao adicionar "Expressão Regular (Nomes parciais)"
- Fix - Configurações de MTA - Cadastro manual volta, mesmo depois de removido e aplicado
- Fix - Administrador Customizado - Ações Indisponíveis
- Fix - MTA - Dominio inativo continua filtrando os e-mails
- Fix - Log de Eventos - Falha ao registrar ação
- Fix - Snapshot de Usuários - Tabela corrompe e impede o funcionamento do sistema
- Fix - Controle de Fluxo - Não carrega a tela com muitos pontos de acesso
- Fix - Cadastro de Usuário - Sensibilidade de SPAM
- Fix - SmartDefender - Erro ao configurar lista Confiável / Indesejável
- Feature - E-mails - Ícone para aprender como SPAM e Não SPAM
- Fix - Builder - Corrigir a busca dos endereços da whitelist do Bayes
- Fix - Microsoft 365 - Serviço de validação do token não funciona com SSLv3
- Fix - Admin da Nuvem - Visualiza usuários inativos

Release 5.2.6-2 (27/01/2021)

- Feature – Inclusão do módulo DMARC Analyzer na solução
- Feature – Verificação do campo FROM dos e-mails pelo SmartDefender. Agora além de verificar links, é também verificado o domínio do campo FROM
- Feature – Verificação de arquivos compactados com senha, onde é verificada a extensão dos anexos contidos no arquivo compactado e se os mesmos violarem a política da empresa (conforme configurado pelo administrador), ocorre o bloqueio do e-mail

Release 5.2.6-1 (07/12/2021)

- Fix – Correção de erro ao adicionar novas regras com Mime Type
- Fix – Corrreção de criação de regra no módulo DLP
- Fix - Microsoft 365 – Compatibilidade do Add-on com Internet Explorer 11
- Feature – Implantação de cache DNS named
- Fix – Correção da falha ao recategorizar URL's

Release 5.2.0-18 (27/08/2020)

- Feature - Relatórios - Modificar backend
- Feature - Tela de Login - Novo layout
- Feature - Microsoft 365 - Conector de Usuários, Grupos e E-mail Válidos
- Feature - Login - Suporte para 2FA
- Feature - MTA - Possibilidade de exportação e importação da tabela de entrega de e-mails.
- Feature - Detalhes da Mensagem - Novo layout
- Feature - Tela detalhes de E-mail - Criar nova aba Performance

- Feature - E-mails - Criar aba Message Trace
- Feature - Relatórios - Modificar coleta de keys para scan
- Feature - Relatórios - DataSource
- Feature - Relatórios - Minerar dados da nuvem
- Feature - Relatórios - Adicionar botão para "Rebuild do Cache"
- Feature - Relatórios - Limpeza dos dados históricos
- Feature - Relatórios - Criar mecanismo de cache dos dados
- Feature - Relatórios - Filtros
- Feature - Relatórios - Debuging cache
- Feature - Minerador – Melhorias
- Feature - Relatórios - Formatters
- Feature - Relatórios - Versão em PDF com formato landscape
- Feature - Admin Customizado - Suporte para aplicar configurações
- Feature - Relatório - Mensagens SPAM Por Regras por Redis
- Feature - Controle de Anexos - Banco de Senhas e #696: Banco de Senhas - Builder das configurações
- Feature - E-mails - Mudar o termo na pesquisa avançada de Regra de SPAM para Assinatura
- Feature - Relatório - Sumário por Domínio por Redis
- Feature - Dashboards - Minerar dados
- Feature - Relatórios - Ajustar label de coleta
- Feature - Relatório - Top E-mail Relays por Redis
- Feature - Relatório - Estatísticas da Quarentena
- Feature - TAP - Permitir ordenamento de regras
- Feature - Console de Administração - Apache + PHP Hardening
- Feature - E-mails - Download do cabeçalho
- Feature - Empacotamento - Não substituir o LogRotate
- Feature - M-SOAR Office 365 - Add-on Outlook
- Feature - Adicionar opções ao ativar um novo dominio na nuvem
- Feature - Relatório - Volume de Mensagens por Data por Redis
- Feature - BlackList / Whitelist - Modificar builder para suporte ao Redis
- Feature - Backup / Disaster Recovery
- Feature - M-SOAR Office 365 - Log de atividades
- Feature - Diagnóstico - Saúde do Servidor
- Feature - Microsoft 365 - Licenciar módulo
- Feature - Relatórios - Status do minerador
- Feature - Smart Defender - Algoritmo para detectar instabilidade
- Feature - TAP - Novo layout
- Feature - Digest - Configuração do tráfego por regra
- Feature - Dashboard - Migração de Admin LTE para Spain
- Feature - Dashboards - Layout
- Feature - E-mails - Incluir nos Detalhes da mensagem o Hostname de Origem do E-mail
- Feature - Smart Defender - Reescrever tela utilizando o Spain
- Feature - Interface - Migração de Admin LTE para Spain
- Feature - DLP - Criar serviço doc2text
- Feature - Microsoft 365 - Ações de controle do usuário

- Feature - E-mails - Melhorar usabilidade e feedback ao usuário
- Feature - Pesquisa Avançada - Já vir preenchido com data inicial e final no campo período de tempo
- Feature - Log de Eventos - Serializar ação
- Feature - M-SOAR Office 365 - Interface de Configuração
- Feature - Configurações do MTA - Importar Domínios
- Feature - E-mails - Granularizar as ações por tipo de usuário
- Feature - M-SOAR Office 365 - Mecanismo de comunicação com plataforma externa
- Feature - M-SOAR: ajustar o comportamento das ações
- Feature - M-SOAR Office 365 - Estudo de viabilidade Add-on
- Feature - M-SOAR Office 365 - Ações na tela de E-mails
- Feature - Controle de Bounce - Criar serviços separados sign e verify
- Feature - E-mails - Melhorar a visualização dos anexos
- Feature - Configuração do Cluster - Tipo Distribuído
- Feature - E-mails - Adicionar coluna Status na exportação
- Feature - E-mails - Extrair senhas do corpo da mensagem
- Feature - BlackList/Whitelist - Adicionar campo de comentário
- Feature - MTA - Validar IP ao adicionar um Relay
- Feature - Smart Defender - Ajustes na tela e usabilidade
- Feature - Tela Fila de E-mails- Aumentar Janela de Detalhes de e-mail na fila
- Feature - Dicionário - Permitir editar expressões do dicionário
- Feature - Smart Defender - Limpar o cache das entradas similares
- Feature - SmartDefender - Adicionar Wizard para configuração de confiável/indesejável
- Fix - E-mails - Function is not defined
- Fix - Logs do MTA - Exportação só retorna a primeira página
- Fix - Quarentenas - Não está salvando Tempo de Armazenamento
- Fix - Fila de E-mails - Problema nos filtros da Pesquisa avançada
- Fix - Sendmail – Redundância
- Fix - Criptografia - Corrigido formato da notificação
- Fix - Dashboard - "Some" ao mudar para o modo claro/escuro
- Fix - Notificações - Tela não salva corretamente opção para E-mail com Vírus
- Fix - E-mails - Aba CDR com problemas de layout
- Fix - E-mails - Informação na tela de Incluir em Não Confiável (Blacklist) está invertida
- Fix - E-mail - Pesquisa Avançada Ignora Filtro de Quarentena
- Fix - TAP - Preview das telas não funciona corretamente
- Fix - Smart Defender - Consulta não retorna dados do WHOIS
- Fix - Agendamento de backup - Não respeita o horário
- Fix - E-mails - Ajustes na tradução do Wizard para adição de Black/WhiteLists
- Fix - Fila de E-mails - Adicionar fila do mailsplit
- Fix - E-mail - Registrar na aba Assinaturas Blacklist da HSC
- Fix - Conectores Externos - Logs Geral da sincronização não são exibidos por mais tempo
- Fix - DKIM - Erro na chave ao adicionar um novo dominio nas configurações do MTA
- Fix - Relatórios Programados - Não anexa o relatório em PDF
- Fix - Interface - Abas em uso permanecem abertas apos a troca de usuario
- Fix - Ataque Dirigido - Erro ao aplicar Configurações após ativar CDR de Documento

- Fix - Diagnóstico - Portas de saída
- Fix - Filtros de SPAM / Configurações Gerais - Não altera a pontuação
- Fix - Regras de Compliance - Regra de Criptografia (CONECTADA) não indica a ação
- Fix - Digest - Não lista todos os Grupos ao criar uma regra de Digest
- Fix - Ponto de Acesso - Erro ao remover ponto de acesso
- Fix - Cluster - Erro ao criar um cluster
- Fix - CDR – Correção de CDR, que estava causando problemas o MLI Cloud ao ser ativado
- Fix - E-mails - Contabilizar pontuação atribuida a arquivos maliciosos na Aba Filtros de Conteúdo
- Fix - Template - Redundância
- Fix - Digest - Modificar forma de buscar as mensagens se Mailsplit ativado
- Fix - E-mails - Falha na exibição dos Links contidos na mensagem
- Fix - Controle de Surto/Comportamento Anômalo – Remover quarentena
- Fix - E-mails - Seletor do Ponto de Acesso
- Fix - E-mails - Não é possível carregar os detalhes da mensagem
- Fix - Conta - Usuário consegue remover os próprios e-mails

Release 5.2.0-10 (22/06/2020)

- Feature - M-SOAR Office 365 - Log de atividades
- Feature - Relatórios - Modificar backend
- Feature - Interface - Migração de Admin LTE para Spain
- Fix - Falha ao exportar Whitelist
- Feature - M-SOAR Office 365 - Add-on Outlook
- Feature - Adicionar opções ao ativar um novo dominio na nuvem
- Fix - E-mail - Detalhes na Aba Filtros de Conteúdo não grifa em Vermelho o arquivo ou ameaça encontrada
- Feature - Relatórios - Versão em PDF com formato landscape
- Feature - E-mails - Ajustes na tradução do Wizard para adição de Black/WhiteLists
- Fix - Digest - Disparo manual dispara para destinatários incorretos
- Fix - Gerenciar Dominios - Erro ao atualizar dados do dominio da nuvem gerenciado
- Fix - E-mails - Alteração tradução do Menu de Ações
- Fix - Regras de Compliance - Regra de Criptografia (CONECTADA) não indica a ação
- Fix - Smart Defender - Consulta não retorna dados do WHOIS
- Fix - Digest - Erro ao configurar a regra
- Feature - Tela de Login - Novo layout
- Feature - Detalhes da Mensagem - Novo layout
- Fix - Não tem todas informações de filtragem em relatório
- Fix - Editar regra de SPAM customizado, não apresenta os dados da regra
- Fix - E-mails - Erro ao reprocessar mensagem
- Fix - Pesquisa Avançada -> Horário
- Feature - TAP - Alteração no Tipo de Controle
- Feature - TAP - Novo layout
- Fix - Filtros de SPAM / Configurações Gerais - Não altera a pontuação
- Fix - Digest - Não lista todos os Grupos ao criar uma regra de Digest
- Fix - E-mails - Visualização do conteúdo da mensagem

- Fix - Realtório de Quarentena - Filtro de domínio não funciona
- Fix - MLI Cloud - Pesquisa Avançada não retorna o resultado
- Feature - Diagnóstico - Saúde do Servidor
- Fix - E-mails - Falha ao mover mensagem para quarentena personalizada
- Fix - Falha ao exportar Whitelist
- Feature - E-mails - Detalhes na Aba Filtros de Conteúdo grifa em Vermelho o arquivo ou ameaça encontrada
- Fix – Reprocessamento de Mensagem
- Fix – Correção de indicação de icone de anexo
- Fix - MTA - Erro ao salvar após filtro + edição de grid
- Fix - Digest - Disparo manual dispara para destinatários incorretos
- Feature - E-mails - Alteração tradução do Menu de Ações
- Fix - Digest - Erro ao configurar a regra
- Fix - Não tem todas informações de filtragem em relatório
- Fix - Editar regra de SPAM customizado, não apresentava os dados da regra
- Fix - Banco de Senhas - Insert default
- Fix - Pesquisa Avançada -> Horário – Antes não estava permitindo alteração
- Feature - TAP - Alteração no Tipo de Controle
- Fix - TAP - Ataque Dirigido só é possível fazer ativação de 1 domínio por vez. Agora é possível ativar para múltiplos domínios simultâneos
- Fix - E-mails – Visualização do conteúdo da mensagem
- Fix - Realtório de Quarentena - Filtro de domínio não funciona
- Fix - E-mails – Correção de falha ao mover mensagem para quarentena personalizada
- Fix - E-mails - Tamanho excedido estava sendo classificado como DLP/Auditoria
- Feature - Interface - Removida a funcionalidade de cache das abas, para melhor desempenho
- Fix - Ponto de Acesso - Erro ao alterar parametros do ponto de acesso
- Fix - E-mails - Filtro de Pesquisa Avançada não retornava dados corretos
- Fix - Whitelist - Pesquisa não funcionava corretamente
- Fix - E-mails - Pesquisa avançada de Regras de Controle Avançado traz caracteres HTML
- Fix - Digest - Erro ao buscar e-mails de um usuário

Release 5.1.9-1 (23/12/2020)

- Fix – Corrigida consulta quando é inserido o campo E-mail de Origem sem preencher o campo Domínio de Origem
- Fix – Corrigida atualização dos dados no RealTime>Portal
- Fix – Corrigido bug que permitia entrada duplicada de registros em RealTime > SmartDefender > Consulta
- Fix – Corrigido erro de RPC na execução do Digest
- Fix – Permissão de visualização de e-mails para o usuário final
- Fix – Correção de Digest duplicado, quando tem mais de um cluster no mesmo gerenciador

Release 5.1.8-1 (11/12/2020)

- Fix - MLI Cloud – Correção em pesquisa rápida, que não apresentava o retorno da pesquisa corretamente

- Fix – Corrigida a estética da caixa de ação em DLP
- Fix – Reapresentado resultados de bloqueio de malwares (nas versões anteriores apresentavam esse resultado), indicando toda a informação sobre eventual malware detectado
- Feature - Exibição reduzida dos Grupos de Usuários ao Adicionar Cadastro de Controle Personalizado
- Fix – Corrigido erros de ortografia
- Fix – Correção de Pesquisa Avançada no campo Domínios Diferentes no Cabeçalho
- Fix – Correção em dicionário de palavras (Possivelmente Perigosos)
- Fix – Correção a indicação de país de origem do e-mail
- Feature – Incluídas novas informações de $data como variáveis para uso na composição de personalização de notificação
- Fix – Corrreção ao qual permitia entrada de registro duplicado (URL's) em SmartDefender

Release 5.1.16 (24/11/2020)

- Manual do Administrador - Correção de errata no manual
- Manual do Administrador - Incluídas informações na tabela de Erros SMTP

Release 5.1 (15/10/2020)

- Feature – Incluído novos dicionários de palavras com definições mais precisas de variantes de Cartões de Crédito e Dicionário de Palavrões em RegEx
- Manual do Administrador – Inclída tabela de Erros de SMTP para consulta facilitando o entendimento dos motivos de bloqueio do Log de MTA
- Feature - E-mails - Adicionado novos campos de busca e Pesquisa avançada. Melhorias de Performance na pesquisa
- Feature - E-mails - Permitir Busca do From e To do e-mail no Header
- Feature - E-mails - Colocar Ícone de Identificação de Item Removido da Quarentena
- Feature - E-Mails - Pesquisa e identificação do Sentido do Tráfego das mensagens
- Feature - E-Mails - Melhorias visuais nos detalhes do e-mails
- Feature - E-Mails - Detalhes do E-mail - Adicionar Bandeira do País no IP de Origem
- Feature - E-mails - Ações devem ser executadas em background
- Feature - E-mails - Nos detalhes da mensagem adicionado indicação de qual quarentena a mensagem foi armazenada
- Feature - Relatórios - Volume de Mensagens por Domínios Atendidos
- Feature - Relatórios - Sumário por Domínio
- Feature - Relatórios - Melhorias de Performance e usabilidade
- Feature - Relatórios - Permitir agrupar por Hora, Dia e Mês
- Feature - MTA - Permitir controle de Ativar Restrição do Envelope RFC 821
- Feature - MTA - Suporte a RelayHost
- Feature - MTA - Permitir Seleccionar Protocolo de Entrega IPV4/IPV6
- Feature - MTA - Liberar Relay - Permitir cadastro de hostnames
- Feature - Logs do MTA - incluindo pesquisa avançada por: Data, Hora, Hostname e status
- Feature - Logs do MTA - Exportar
- Feature - Login - Melhorar mecanismos de autenticação e validação de usuários
- Feature - Login - Link para acesso a interface de criptografia
- Feature - Reescrita de E-Mails - Adicionada pesquisa rápida

- Feature - Tela de Configuração de Cluster - Ajustes visuais e informativos
- Feature - Perfil de Usuário - Restrição de Acesso. Permite definir permissões de acesso por rede e tipo de usuário
- Feature – Módulo exclusivo para análise de Imagem de Pornográfica
- Feature - Seletor Ponto de Acesso / Cluster - Regras de exibição e auto seletor. Permite automatizar e auto selecionar o Ponto de Acesso ou Cluster através: /mailinspector/login.php?pointId=3
- Feature - MLI Cloud - Cadastro Manual do MTA
- Feature - Padronizados telas de cadastros incluindo: Pesquisa Rápida, Importar/Exportar, Multi Seleção e Multiação
- Feature - Filas de E-mail - Melhorias na visualização, ordenação e pesquisas
- Feature - Controle de Fluxo - Melhorias na visualização, ordenação e pesquisas
- Feature - Dashboad - Acompanhamento das Filas
- Feature - Capacity Plainning - Ajustes e Melhorias
- Feature - Nova Interface para usuários de criptografia, com interface Responsiva
- Feature - Grupos de usuários - Remover validação do domínio, permitindo os novos tipos de registros
- Feature - Black&White Lists - Pesquisas Avançadas, novos campos de busca
- Feature - Certificado SSL- Permitir Adição da Cadeia do Certificado
- Feature - Certificado SSL - Validar antes de aplicar
- Feature - Permitir Desabilitar Regras de DLP e Regras de SPAM Avançadas
- Feature - Usuários - Preferências, permite configurar diretivas de visualização das quarentenas do usuário pela interface web
- Feature - Licenciamento - Aviso de Licença próxima de expirar
- Feature - MailSplit - Melhorias de Performance e Disponibilidade
- Feature - MailSplit - Adicionar cabeçalho indicando o destinatário real para ser usado nas regras de Compliance: X-HSC-Mail_Inspector-Envelope-To
- Feature - Filtro de Conteúdo - Remetente de Notificações, permite configurar o remetente das mensagens de Bounce
- Feature - Criptografia - Customizar templates via WEB
- Feature - Portal - Cache para acesso rápido
- Feature - Quota/Controle de Fluxo - Permitir definir o Tracker por Regra
- Feature - Notificação de Quarentena - Melhorias de Performance e processamento
- Feature - Notificação de Quarentena - Customização Avançada do Template
- Feature - Smartdefender Consulta - Adicionada pesquisa rápida
- Feature - Ataque Dirigido - Definir Url/Hostname e Protocolo de Reescrita no TAP
- Feature - Quota/Controle de Fluxo - Combobox com auto-complete
- Feature - Script de Importação Users LDAP - Desabilitar users por conector
- Feature - Usuários do Sistema - Selecionar mais de um registro e multiação
- Feature - Log de eventos - Formatação ao ler
- Feature - Diagnostico - Incluído teste de TRACEROUTE
- Feature - Interface Web - Tradução para Espanhol e inglês
- Feature - Ataque Dirigido - Melhorias visuais
- Feature - Ataque Dirigido - Novas configurações de File Sandbox
- Feature - Ataque Dirigido - Novas configurações de CDR e Sandbox de Documentos

- Feature - MailTracker: Melhorias visuais, nova aba para pesquisar dados mais antigos
- Feature - BACKUP - Permitir Configurar Sistema de SnapShot Automático
- Feature - DLP / Regras Avançadas de SPAM - Melhorar visualização ao editar regras
- Feature - DLP - Adicionar boundaries nas regex
- Feature - CDR - Nova interface e maior granularidade nas ações
- Feature - Hardening MailInspector Security: TLS1.2, Firewall, etc
- Fix - MLI Cloud - Usuário (admin nuvem), ajustes de permissão de visualização
- Fix - E-mails - Problema na visualização com múltiplos clusters
- Fix - DLP / Compliance - Não indica o nome da regra ao remover
- Fix - AntiVirus - Bug Tela de Conf Antivírus
- Fix - Painel de Controle - MailSplit mostra como desabilitado
- Fix - Notificação de Quarentena - Erro na execução manual
- Fix - E-mails - Bloquear a tela enquanto estiver carregando a aba Log de Evidências
- Fix - Banco de Dados - Bug na indicação de dias uptime
- Fix - Limpeza de Quarentena - Ajuste para DB Remoto
- Fix - Configurações de Rede - Erro ao aplicar
- Fix - Controle Avançado & Regras De Compliance -Erro ao Remover regras conectadas
- Fix - Pontuação: Na classificação de possível spam e spam na pontuação não permite números fracionados
- Fix - E-mails - Detalhes da mensagem exibe quarentena de forma errada
- Fix - Gerenciar Domínios - Usuários Bloqueados após importar TXT
- Fix - Regras de SPAM Avançado - Bug ao editar conexão
- Fix - Usuários - Reset de senha ao editar
- Fix - Gerenciar Domínios - Contador de Contas importadas por TXT subtraindo 1 conta
- Fix - DLP - Erro no builder para ação de Quarentena Customizada
- Fix - Controle Avançado de SPAM - Erro no wizard
- Fix - Diagnóstico - Erro ao testar portas de saída do MLI

Release 5.0.30-7 (29/07/2020)

- Fix – Atualização da Engine de antivírus
- Manual – Inserido novos HowTo’s
- Feature – Mudança de layout do módulo de Ataque Dirigido

Release 5.0.30-6 (08/07/2020)

- Documentação – Inclusão de novos HowTo’s no manual
- Fix - Ajustes na tela de Configuração do Cluster
- Fix - Aumento no timeout da comunicação XML/RPC
- Fix - Correção na busca da Whitelist / Blacklist
- Fix - Correção no tratamento de mensagens encodadas como Quoted Printable
- Fix- Correção no script de envio de notificação de quarentena
- Fix - Correção na Pesquisa Rápida da Reescrita de E-mails
- Fix - Correção na exibição dos e-mails quando existem múltiplos clusters
- Fix - Correção para executar restart ao invés de reload no serviço MailInspector
- Fix - Correção na aplicação das listas confiáveis e não confiáveis do SmartDefender

- Feature - Melhorias no visual dos relatórios e adicionada tela de carregamento
- Feature - Adicionada regra de YARA para detecção de HTML maliciosa e permitindo integração com regras de detecção de ameaças
- Feature - Melhorias na busca avançada dos Logs do MTA
- Fix - Correção no tratamento da sessão para melhorar a performance das requisições simultâneas
- Fix - Correção na tela do DKIM
- Fix - Correção para utilizar o IP de backup no script mliUserSnapshot
- Feature - Melhorias na utilização do Administrador da Nuvem
- Fix - Correção para evitar DOS ao requisitar um novo Digest

Release 5.0.30-5 (24/06/2020)

- Feature – Incluído na busca de Logs do MTA o campo Status, possibilitando filtrar os logs por: Bloqueado, Temporariamente Bloqueado ou Todos
- Feature – Desabilitar o recurso de reescrita de URL por política, isto é, possibilitar que o e-mail seja entregue sem a reescrita de URL para determinados grupos (tanto para origem, quanto para destino), definido pelo administrador
- Documentação – Inclusão de novos HowTo's no manual
- Documentação – Inclusão de Apêndice 6 (Lista das principais Assinaturas)
- Feature – Exportação de RBL's externas cadastradas no formato XML ou CSV

Release 5.0.30-4 (21/06/2020)

- Feature – Histórico de Mail Tracker. Permite visualizar o histórico de registro de logs dos e-mails

Release 5.0.30-3 (06/05/2020)

- Fix – Correção de execução de notificação de quarentena em modo manual
- Modificação - Alteração dos IP's utilizados pelo serviço de antivírus
- Remoção de porta utilizada por serviço substituído na nova versão do MailInspector
- Fix – Limpeza do banco de dados na parte de Logs. Corrigida a periodicidade da limpeza
- Feature – Controle de redes/IP's e usuários que podem ter acesso ao MailInspector
- Feature – Novos widgets para Dashboards (Acompanhamento de Filas)
- Feature – Interface de acesso exclusivo para usuários (destinatários) com e-mails criptografados
- Feature – Aprimoramento no sistema de detecção de imagem pornográfica, bem como permissão ao administrador ativar a funcionalidade para determinados grupos de usuários
- Feature – Quando o MailInspector estiver próximo do vencimento da licença, aparecerá um pop-up no logon do administrador avisando da proximidade da data de vencimento
- Feature – Certificado SSL será verificado antes de ser aceito a sua adição no MailInspector

Release 5.0.30-1 (23/03/2020)

- Fix – Correção de configuração de ativação de configuração de antivirus
- Feature - Permitir Busca do From e To do e-mail no Header
- Fix - Certificado SSL - Permitir Adição da Cadeia do Certificado
- Feature - Criptografia - Customizar templates via WEB
- Fix - Limpeza de Quarentena - Ajuste para DB Remoto
- Fix - Segurança - Problema Digest + Token + Sessão

- Fix - Configurações de Rede - Erro ao aplicar
- Fix - E-mails - Ações devem ser executadas em background
- Fix - Cluster com DB Remoto - Não Aplica
- Feature - Usuários - Preferências
- Feature - Black&White Lists - Pesquisas Avançadas
- Fix - Alteração de Senha do Administrador Nuvem (Solução Cloud)
- Feature - Criptografia – Suporte celular em modo responsivo
- Fix - Limpeza de Quarentena - Não está realizando a limpeza em modo cluster com muitos nodes
- Feature - Permitir Desabilitar Regras de DLP e Regras de SPAM Avançadas
- Fix - Tela Detalhes de E-mail - Bloquear a tela enquanto estiver carregando a aba Log de Evidencias
- Fix - Grupos de usuários - Removida validação do dominio
- Feature - Tela de E-mail - Permitir Busca do From e To do e-mail no Header
- Fix - Painel de Controle - MailSplit mostra como desabilitado
- Feature - Interface para usuários de cryptografia
- Fix - Builder Antivirus - Enviar Template do /etc/clamd-dlp.conf
- Feature - Portal - Cache para acesso rápido
- Feature - Filtro de Conteúdo - Remetente de Notificações
- Feature - MailSplit - Verificar a necessidade de split via postcat
- Feature - MTA - Não verificar header sem regras de X-HSC-Smarthost
- Feature - Melhorias de performance de navegação
- Feature - PopUp de alerta quando a licença estiver próxima de expirar
- Feature - Certificado SSL - Validar antes de aplicar
- Fix - Banco de Dados - Bug na indicação de dias uptime

Release 5.0.27-4 (09/12/2019)

- Feature - Melhoria nos logs no mecanismo supervisor de serviços
- Feature - Melhoria na visualização dos cabeçalhos nos detalhes da mensagem
- Feature - Criado novo mecanismo para proteção e segurança na comunicação externa e entre pontos de acesso
- Feature - Melhoria no mecanismo de assinatura de mensagens com DKIM
- Feature - Otimização na declaração de regras de DLP
- Feature - Maior granularidade nos mecanismos de controle de ameaças
- Feature - Otimização do mecanismo de aplicação de configurações
- Feature - Suporte para limpeza do cache do SmartDefender
- Feature - Suporte para controle de filas de saída personzalidos
- Feature - Suporte para armazenar a quarentena em servidor externo
- Feature - Novo relatório Mensagens por Domínios Atendidos
- Feature - Melhorias na interface de criptografia
- Feature - Suporte para configuração manual do horário
- Feature - Suporte para download da mensagem original e anexos em lote na tela de E-mails
- Feature - Capacidade de visualizar os detalhes do módulo de CDR na tela de E-mails
- Feature - Suporte para exportar em CSV/PDF os Logs de eventos
- Feature - Melhorias no módulo de CDR com maior granularidade nos controles
- Feature - Suporte para mover a fila de mensagens entre os pontos de acesso

- Feature - Novo relatório Volume de Mensagens por Domínios Atendidos
- Feature - Otimização do mecanismo de atualização
- Fix - Correção no download de anexos com problemas na codificação
- Fix - Correção de erros na busca rápida para usuários comuns
- Fix - Correção no mecanismo de reboot do ponto de acesso
- Fix - Correção na visualização da reputação de arquivos na aba SmartDefender nos detalhes da mensagem
- Fix - Correção na visualização de mensagens para usuários Adminitradores da Nuvem
- Fix - Correção no reload dos serviços após atualização de vacinas
- Fix - Correção no download do arquivo original de algumas mensagens
- Fix - Correção na performance do relatório Top Remetentes por Quantidade
- Fix - Correção no carregamento de alguns componentes do Dashboard
- Fix - Correção na exibição do status da consulta das URLS na aba SmartDefender
- Fix - Correção no mecanismo de whitelist/blacklist para verificar regras De/Para 'Todos'
- Fix - Correção para exibir corretamente a versão do database do antivirus na tela de Performance do Sistema

Release 5.0.26-1 (13/11/2019)

- Fix - Correção no parse de URLs e Arquivos na aba SmartDefender nos detalhes da mensagem
- Fix - Correção na validação do tipo de permissão de usuário no mecanismo que adiciona elementos na lista de Confiáveis e Não Confiáveis
- Fix - Ajuste no timeout para download de anexos grandes
- Fix - Ajuste no mecanismo de atualização via Extreme Update
- Fix - Correção para consulta de quarentenas customizadas
- Fix - Correção no módulo de criptografia
- Fix - Correção no parse dos logs de evidência

Release 5.0.25-3 (01/11/2019)

- Feature - Melhoria no sistema de detecção de ameaças de documentos via sandbox local
- Versão do manual baseado sobre a versão de release.

Release 5.0.24-1 (29/10/2019)

- Feature - Melhoria que permite visualizar com mais detalhes a análise do SmartDefender nos detalhes da mensagem
- Feature - Melhoria de performance no processamento da Blacklist/Whitelist
- Feature - Melhoria de performance no mecanismo de Mail Split
- Feature - Melhoria de performance no mecanismo de análise local do SmartDefender
- Feature - Melhoria para melhor identificar/acompanhar o processo de atualização
- Feature - Adicionado mecanismo de para validação do From do Header se o dominio do From existe e se ele possui um endereço A e MX válido
- Fix - Correção no mecanismo de criação de regras de DLP
- Fix - Correção na exibição do mecanismo de Controle de novos Domínos
- Fix - Correção para visualizar corretamente o processo de Aplicar Configurações
- Fix - Correção para não aplicar o módulo de Extreme Update via linha de comando

- Fix - Adicionado suporte para filtrar e-mails que tenham sido liberados
- Fix - Correção que permite tratar melhor as mensagens quando a fila de e-mails estiver alta
- Fix - Ajustes na tradução para Ingles e Espanhol

Release 5.0.23-1 (16/10/2019)

- Fix - Correção ao apagar mensagens da Fila de E-mails
- Fix - Correção no mecanismo de sincronização de usuários LDAP
- Feature - Melhorias no processo de Filtros de Conteúdo
- Feature - Adicionado suporte para expressões regulares estendidas

Release 5.0.22-1 (14/10/2019)

- Fix - Correção para melhoria na performance no processamento das mensagens

Release 5.0.21-2 (14/10/2019)

- Fix - Correção para aplicar regras de controle corretamente para clientes ISP
- Fix - Correção para prevenir a troca de perfil dos usuários no mecanismo de sincronização
- Feature - Melhorias no mecanismo interno do MTA para tratamento de cabeçalhos customizados
- Fix - Ajustes no mecanismo de prevenção de Spoofing de Domínio

Release 5.0.20-1 (09/10/2019)

- Fix - Correção no mecanismo de antispoofing
- Fix - Correção para melhoria na execução dos mecanismos agendados do sistema
- Fix - Correção no mecanismo de logs do sistema

Release 5.0.19-1 (08/10/2019)

- Fix - Correção na limpeza de arquivos temporários do módulo de CDR
- Fix - Correção de erro na configuração de múltiplos servidores nas rotas de entrada de mensagens
- Fix - Correção de erro na configuração do Extreme Update

Release 5.0.18-1 (07/10/2019)

- Fix - Correção que previne a exibição de Grupos LDAP e Listas Distribuição duplicados

Release 5.0.17-1 (24/09/2019)

- Fix - Correção na permissão de visualização de e-mails e filas para usuario Operador
- Fix - Correção no mecanismo de prevenção de spoofing de saída de e-mails
- Fix - Correção na visualização do catálogo de endereços dos conectores externos
- Fix - Correção para alterar corretamente a campo From no Envelope SMTP da notificação de quarentena

Release 5

- Disponível para atualização para clientes da versão 4.5.17 em 07/10/2019 (26/05/2019)