Permitir que um remetente confiável ignore o antisspam

Contents

Introduction

Este documento descreve os detalhes de permitir que um remetente confiável ignore a verificação antisspam e também os diferentes métodos que você pode optar pelo mesmo no Secure Email Gateway (anteriormente conhecido como Email Security Appliance).

Adição de nome de host/endereço IP do remetente no grupo de remetente ALLOWED_LIST

Adicione os remetentes confiáveis ao grupo de remetentes ALLOWED_LIST porque esse grupo de remetentes usa a política de fluxo de e-mail $TRUSTED. Os membros do grupo de remetentes ALLOWED_LIST não estão sujeitos a limitação de taxa, e o conteúdo desses remetentes não é analisado pelo mecanismo Anti-Spam, mas ainda é verificado pelo antivírus.

> **Note**: Com a configuração padrão, a verificação de antivírus está ativada, mas o antisspam está desativado.

Para permitir que um remetente ignore a verificação antisspam, adicione o remetente ao grupo de remetente ALLOWED_LIST na HAT (Host Access Table). Você pode configurar o HAT por meio da GUI ou da CLI.

Na GUI

1. Selecione a guia **Políticas de e-mail**.
2. Na seção **Host Access Table**, selecione **HAT Overview**.
3. Àdireita, certifique-se de que o ouvinte **InboundMail** está selecionado no momento.
4. Na coluna **Grupo de Remetentes**, selecione **ALLOWED_LIST**.
5. Selecione o botão **Adicionar remetente** próximo à metade inferior da página.
6. Insira o IP ou o nome de host que deseja permitir ignorar no primeiro campo.

Quando terminar de adicionar entradas, selecione o botão **Submit**. Lembre-se de selecionar o

botão **Confirmar alterações** para salvar suas alterações.

Da CLI

```
example.com> listenerconfig
Currently configured listeners:
1. InboundMail (on PublicNet, 172.19.1.80) SMTP TCP Port 25 Public
2. OutboundMail (on PrivateNet, 172.19.2.80) SMTP TCP Port 25 Private
Choose the operation you want to perform:
- NEW - Create a new listener.
- EDIT - Modify a listener.
- DELETE - Remove a listener.
- SETUP - Change global settings.
[]> edit
Enter the name or number of the listener you wish to edit.
[]> 1
Name: InboundMail
Type: Public
Interface: PublicNet (172.19.1.80/24) TCP Port 25
Protocol: SMTP
Default Domain:
Max Concurrency: 1000 (TCP Queue: 50)
Domain Map: Disabled
TLS: No
SMTP Authentication: Disabled
Bounce Profile: Default
Use SenderBase For Reputation Filters and IP Profiling: Yes
Footer: None
LDAP: Off

Choose the operation you want to perform:
- NAME - Change the name of the listener.
- INTERFACE - Change the interface.
- LIMITS - Change the injection limits.
- SETUP - Configure general options.
- HOSTACCESS - Modify the Host Access Table.
- RCPTACCESS - Modify the Recipient Access Table.
- BOUNCECONFIG - Choose the bounce profile to use for messages injected on this
listener.
- MASQUERADE - Configure the Domain Masquerading Table.
- DOMAINMAP - Configure domain mappings.
[]> hostaccess
Default Policy Parameters
=========================
Allow TLS Connections: No
Allow SMTP Authentication: No
Require TLS To Offer SMTP authentication: No
Maximum Concurrency Per IP: 1,000
Maximum Message Size: 100M
Maximum Messages Per Connection: 1,000
Maximum Recipients Per Message: 1,000
Maximum Recipients Per Hour: Disabled
Use SenderBase For Flow Control: Yes
Spam Detection Enabled: Yes
Virus Detection Enabled: Yes
There are currently 4 policies defined.
There are currently 5 sender groups.
Choose the operation you want to perform:
- NEW - Create a new entry.
- EDIT - Modify an entry.
- DELETE - Remove an entry.
```

```
- MOVE - Move an entry.
- DEFAULT - Set the defaults.
- PRINT - Display the table.
- IMPORT - Import a table from a file.
- EXPORT - Export the table to a file.
- CLEAR - Remove all entries.
[]> edit
1. Edit Sender Group
2. Edit Policy
[1]> 1
Currently configured HAT sender groups:
1. ALLOWED_LIST (My trusted senders have no anti-spam scanning or rate limiting)
2. BLOCKED_LIST (Spammers are rejected)
3. SUSPECTLIST (Suspicious senders are throttled)
4. UNKNOWNLIST (Reviewed but undecided, continue normal acceptance)
5. (no name, first host = ALL) (Everyone else)
Enter the sender group number or name you wish to edit.
[]> 1

Choose the operation you want to perform:
- NEW - Add a new host.
- DELETE - Remove a host.
- MOVE - Reorder the hosts.
- POLICY - Change the policy settings and options.
- PRINT - Display the current definition.
- RENAME - Rename this sender group.
[]> new
Enter the hosts to add. CIDR addresses such as 10.1.1.0/24 are allowed. IP
address ranges such as 10.1.1.10-20 are allowed. IP subnets such as 10.2.3. are
allowed. Hostnames such as crm.example.com are allowed. Partial hostnames such
as .example.com are allowed.
Ranges of SenderBase Reputation scores such as SBRS[7.5:10.0] are allowed.
SenderBase Network Owner IDs such as SBO:12345 are allowed.
Remote blocklist queries such as dnslist[query.blocklist.example] are allowed.
Separate multiple hosts with commas
[]>
```

Lembre-se de emitir o comando **commit** para salvar suas alterações.

Revise a verificação antisspam e antivírus na política de fluxo de e-mail confiável

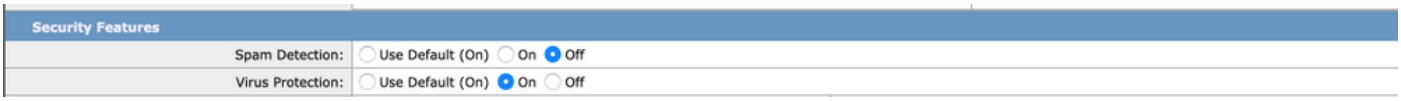
Para o remetente confiável, haverá uma política de fluxo de e-mail nomeada como confiável presente por padrão. A Política de fluxo de e-mail confiável terá um comportamento de conexão Aceitar (semelhante ao comportamento de outras políticas de fluxo de e-mail para emails de entrada).

Quando um remetente é confiável para requisitos comerciais, podemos optar por desabilitar as verificações de antivírus e antisspam para eles. Isso ajudará a reduzir a carga de processamento extra em ambos os mecanismos de verificação enquanto eles verificam os emails que não são de fontes confiáveis.

> **Note**: Os mecanismos antisspam e antivírus desativados ignorarão qualquer verificação relacionada a spam ou vírus para o e-mail recebido no ESA. Isso tem que ser feito, apenas se você tiver certeza absoluta de que não há risco de ignorar verificações para esses remetentes confiáveis.

A opção de onde você pode desabilitar os mecanismos está disponível na guia Recursos de segurança em Políticas de fluxo de e-mail. O caminho para o mesmo é **GUI > Políticas de e-mail > Políticas de fluxo de e-mail**. Clique na **política de fluxo TRUSTEDMail** e role para baixo até **Recursos de segurança** na página subsequente.

Certifique-se de confirmar as alterações depois de fazer ajustes conforme desejado.



Adicionar um remetente confiável à lista de permissão

As listas de permissão e bloqueio do usuário final são criadas por usuários finais e armazenadas em um banco de dados verificado antes da verificação antisspam. Cada usuário final pode identificar domínios, subdomínios ou endereços de e-mail que deseja sempre tratar como spam ou nunca tratar como spam. Se um endereço de remetente fizer parte de uma lista segura de usuários finais, a verificação antisspam será ignorada

Essa configuração permitirá que o usuário final proteja um remetente de acordo com a exigência de isenção das verificações antisspam. A verificação do antivírus e outras verificações no pipeline de e-mails não serão tocadas com essa configuração e continuarão conforme a configuração nas Políticas de e-mail. Essa configuração reduzirá o envolvimento do administrador, sempre que um usuário final tiver que isentar a verificação de spam de um remetente.

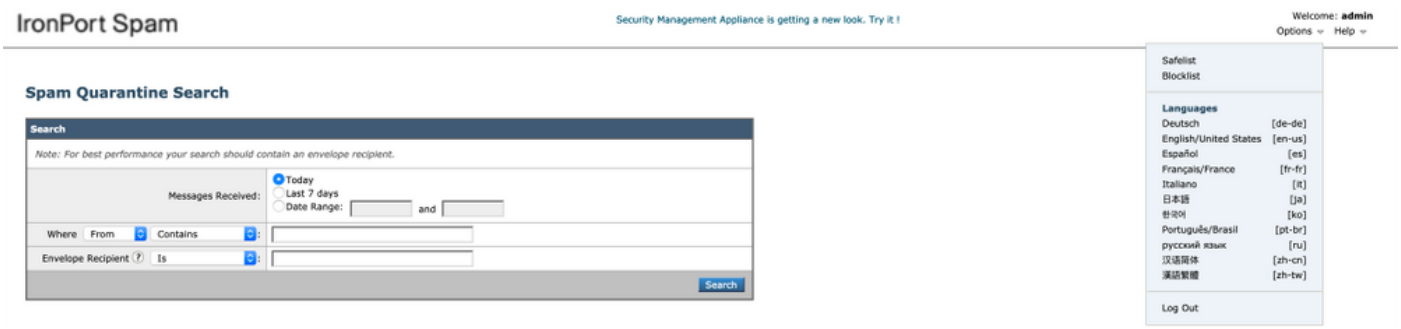
Para a Lista de permissão, é obrigatório ter o acesso à Quarentena de usuário final habilitado para Usuários finais e Lista de permissão/bloqueio do usuário final como Ativado (ambos no ESA ou SMA). Dessa forma, eles podem acessar o portal Quarentena de spam e, ao lado de **Liberar/Excluir** dos emails em quarentena, também podem **Adicionar/Excluir** remetentes na Lista de permissão.

O acesso à **Quarentena de usuário final** pode ser ativado como abaixo:

ESA: Navegue até **GUI > Monitor > Quarentena de spam**. Verifique o botão **de opção Acesso à quarentena do usuário final**. Selecione o método de autenticação para acesso conforme o requisito (None/LDAP/SAML/IMAP ou POP). Publique isso, ative a lista de permissão/bloqueio do usuário final.

SMA: Navegue até **GUI > Serviços centralizados > Quarentena de spam**. Verifique o botão **de opção Acesso à quarentena do usuário final**. Selecione o método de autenticação para acesso conforme o requisito (None/LDAP/SAML/IMAP ou POP). Publique isso, ative a lista de permissão/bloqueio do usuário final.

Depois de habilitado, quando um usuário final navega para o portal Quarentena de spam, ele poderá **adicionar/modificar** sua Lista de permissão conforme a escolha nas opções suspensas do canto superior direito.



Remetentes confiáveis com políticas de e-mail de entrada

Você também pode adicionar um remetente confiável na Política de recebimento de e-mail e desabilitar as verificações **antivírus/antispam** de acordo com o requisito. Uma nova Política de Correio Personalizada pode ser criada com um nome como **Remetentes Confiáveis/Remetentes Seguros**, etc., como preferir, e depois pode adicionar os detalhes do remetente, como nomes de domínio ou endereços de correio eletrônico do remetente, a esta política personalizada.

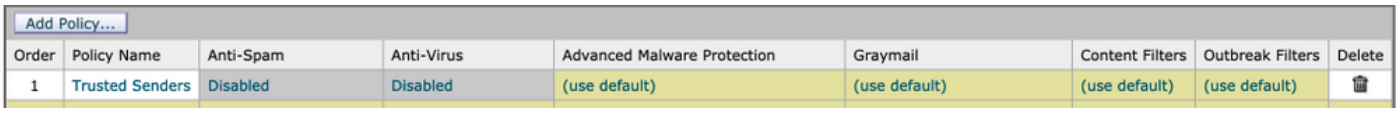
Depois de submeter a política após a adição necessária, pode clicar nas colunas de **Antispam** ou **Antivírus** e, na página subsequente, selecionar **Desativar**.

Com essa configuração, os domínios de remetente confiável ou os endereços de e-mail adicionados a essa política de e-mail serão isentos das verificações do Antispam ou Antivírus.

> **Note**: Os mecanismos antisspam e antivírus desativados ignorarão qualquer verificação relacionada a spam ou vírus para o e-mail de entrada no ESA processado por meio dessa política de e-mail personalizada. Isso tem que ser feito, apenas se você tiver certeza absoluta de que não há risco de ignorar verificações para esses remetentes confiáveis.

A política de e-mail personalizada pode ser criada a partir da **GUI do ESA > Políticas de e-mail > Políticas de e-mail de entrada > Adicionar política**. Insira o nome da diretiva conforme a escolha e selecione **Adicionar usuário**. Verifique o botão de opção **Seguindo remetentes.** Adicione o domínio ou os endereços de e-mail necessários na caixa e clique em **Ok**.

Após a criação da política de correio eletrônico, pode optar por desativar as pesquisas Antivírus e Antispam de acordo com os requisitos da empresa. Aqui está um exemplo de captura de tela:



Informações Relacionadas

- [Cisco Email Security Appliance – Guias do usuário final]
- [Suporte Técnico e Documentação - Cisco Systems]