Detectar mensagens de e-mail falsificadas no ESA e criar exceções

Contents

Introdução

Este documento descreve como controlar o spoofing de e-mail no Cisco ESA e como criar exceções para os usuários autorizados a enviar e-mails falsificados.

Pré-requisitos

Requisitos

Seu ESA (Email Security Appliance) deve processar e-mails de entrada e saída e usar uma configuração padrão de RELAYLIST para sinalizar mensagens como de saída.

Componentes Utilizados

Os componentes específicos usados incluem:

- Dicionário: usado para armazenar todos os seus domínios internos.
- Filtro de Mensagens : usado para manipular a lógica para detectar email falsificado e inserir um cabeçalho no qual os filtros de conteúdo possam agir.
- Quarentena de política: usada para armazenar duplicatas de emails falsificados temporariamente. Considere adicionar o endereço IP das mensagens liberadas a MY_TRUSTED_SPOOF_HOSTS para evitar que futuras mensagens desse remetente entrem na quarentena de política.
- MY_TRUSTED_SPOOF_HOSTS: lista para referenciar seus endereços IP de envio confiáveis. Adicionar um endereço IP de um remetente a essa lista ignora a quarentena e permite que o remetente falsifique. Você coloca os remetentes confiáveis em seu grupo de remetente MY_TRUSTED_SPOOF_HOSTS para que as mensagens falsificadas desses remetentes não sejam colocadas em quarentena.

- RELAYLIST: lista para autenticar endereços IP que podem retransmitir ou enviar e-mails de saída. Se o e-mail for entregue por meio desse grupo de remetente, presume-se que a mensagem não seja falsificada.

Observação: Se um grupo de remetente for chamado de algo diferente de MY_TRUSTED_SPOOF_HOSTS ou RELAYLIST, você terá que modificar o filtro com o nome do grupo de remetente correspondente. Além disso, se você tiver vários ouvintes, também terá mais de um MY_TRUSTED_SPOOF_HOSTS.

As informações neste documento são baseadas no ESA com qualquer versão do AsyncOS.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

O spoofing é ativado por padrão no Cisco ESA. Há várias razões válidas para permitir que outros domínios enviem em seu nome. Um exemplo comum, o administrador do ESA deseja controlar os e-mails falsificados colocando em quarentena as mensagens falsificadas antes que elas sejam entregues.

Para executar uma ação específica, como quarentena em e-mail falsificado, você deve primeiro detectar o e-mail falsificado.

O que é falsificação de email

Falsificação de e-mail é a falsificação de um cabeçalho de e-mail para que a mensagem pareça ter se originado de alguém ou em algum lugar que não seja a origem real. A falsificação de e-mail é uma tática usada em campanhas de phishing e spam, pois as pessoas têm maior probabilidade de abrir um e-mail quando acham que ele foi enviado por uma fonte legítima.

Como detectar e-mails falsificados

Você deseja filtrar todas as mensagens que tenham um remetente de envelope (Email-De) e um cabeçalho amigável de (De) que contenham um de seus próprios domínios de entrada no endereço de email.

Como permitir falsificação para remetentes específicos

Quando você implementa o filtro de mensagens fornecido neste artigo, as mensagens falsificadas são marcadas com um cabeçalho e o filtro de conteúdo é usado para executar uma ação no cabeçalho . Para adicionar uma exceção, basta adicionar o IP do remetente a MY_TRUSTED_SPOOF_HOSTS.

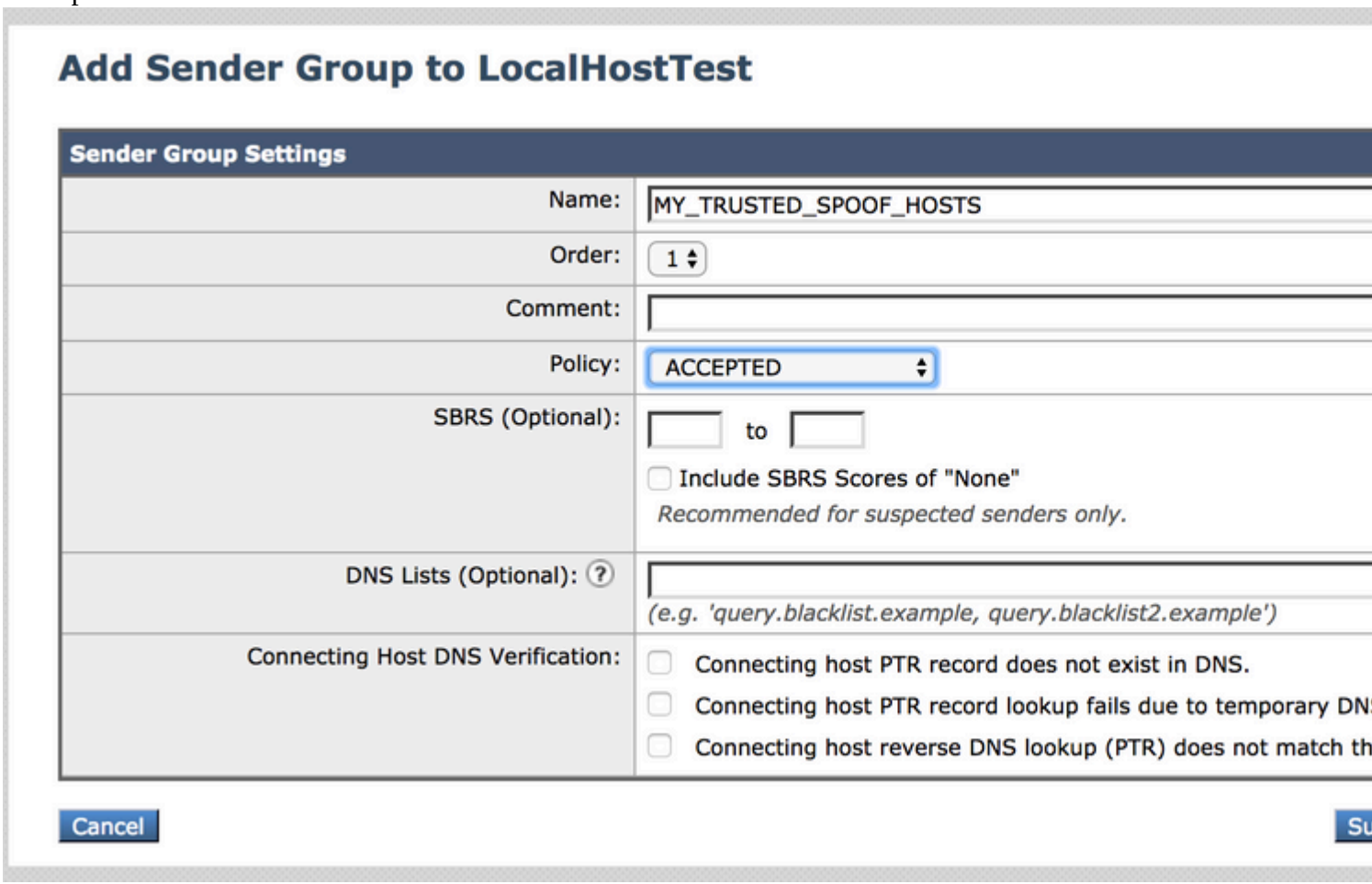
Configurar

Criar um grupo de remetente

1. Na GUI do ESA, navegue para **Políticas de e-mail > Visão geral do HAT**
2. Clique em **Adicionar.**
3. No campo Nome, especifique **MY_TRUSTED_SPOOF_HOSTS**.
4. No campo Pedido, especifique **1**.

5. Para o campo Política, especifique **ACEITO**.
6. Clique em **Enviar** para salvar as alterações.
7. Finalmente, clique em **Confirmar alterações** para salvar a configuração

Exemplo:

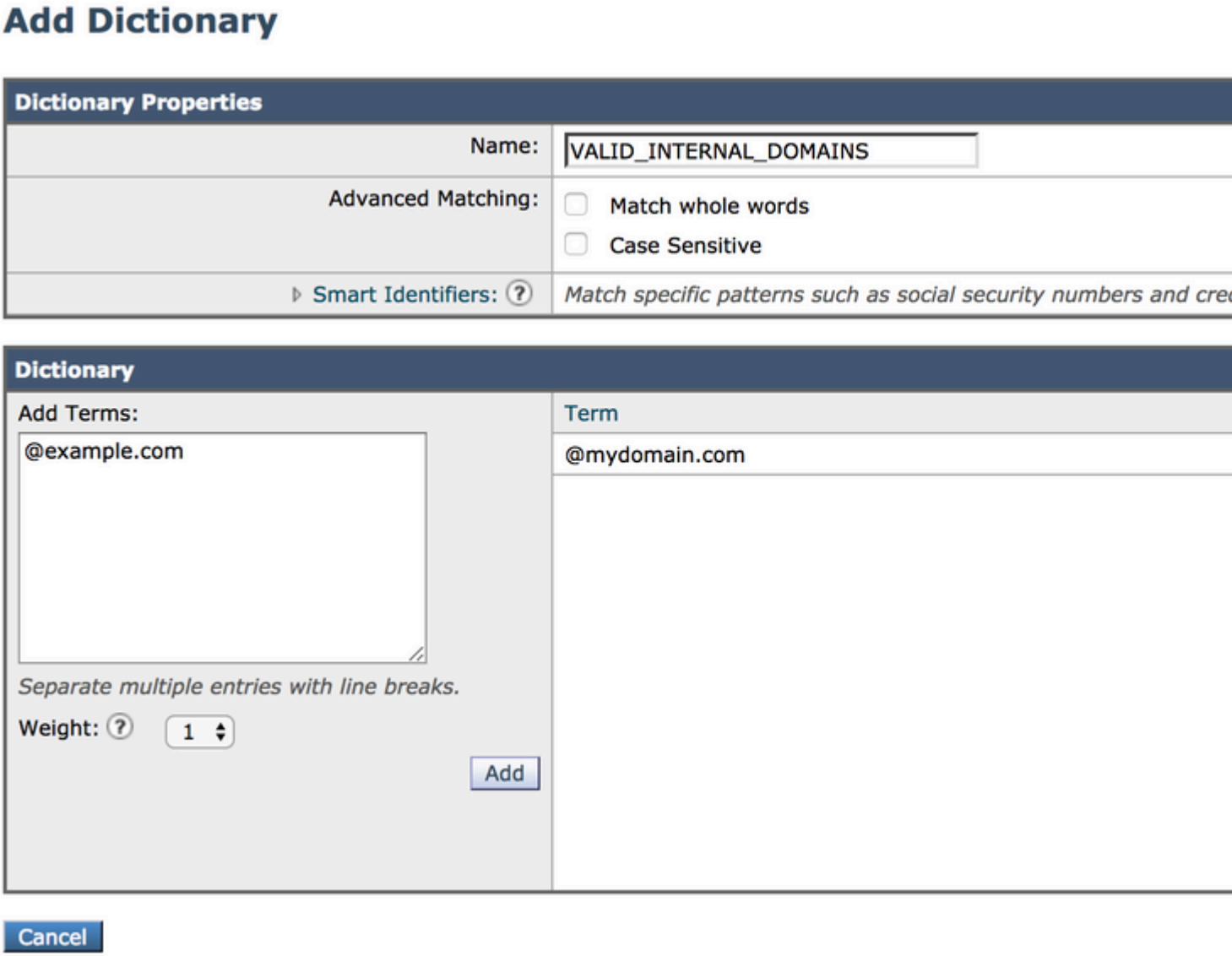


Criar um dicionário

Crie um dicionário para todos os domínios para os quais você deseja desativar o spoofing no ESA:

1. Na GUI do ESA, navegue para **Políticas de e-mail > Dicionários.**
2. Clique em **Adicionar dicionário.**
3. No campo Nome, especifique 'VALID_INTERNAL_DOMAINS' para que a cópia e a colagem do filtro de mensagens não apresentem erros.
4. Em adicionar termos, adicione todos os domínios nos quais deseja detectar falsificação. Insira o domínio com um sinal @ precedendo o domínio e clique em **adicionar**.
5. Certifique-se de que a caixa de seleção **combinar palavras inteiras** esteja desmarcada.
6. Clique em **Submeter** para salvar as alterações do dicionário.
7. Por fim, clique em **Confirmar alterações** para salvar a configuração.

Exemplo:



Criar um filtro de mensagens

Em seguida, você precisa criar um filtro de mensagem para aproveitar o dicionário recém-criado, "VALID_INTERNAL_DOMAINS"**:**

1. Conecte-se à interface de linha de comando (CLI) do ESA.
2. Execute o comando **Filters.**
3. Execute o comando **New** para criar um novo filtro de mensagens.
4. Copie e cole este exemplo de filtro, editando seus nomes de grupos de remetentes reais, se necessário:

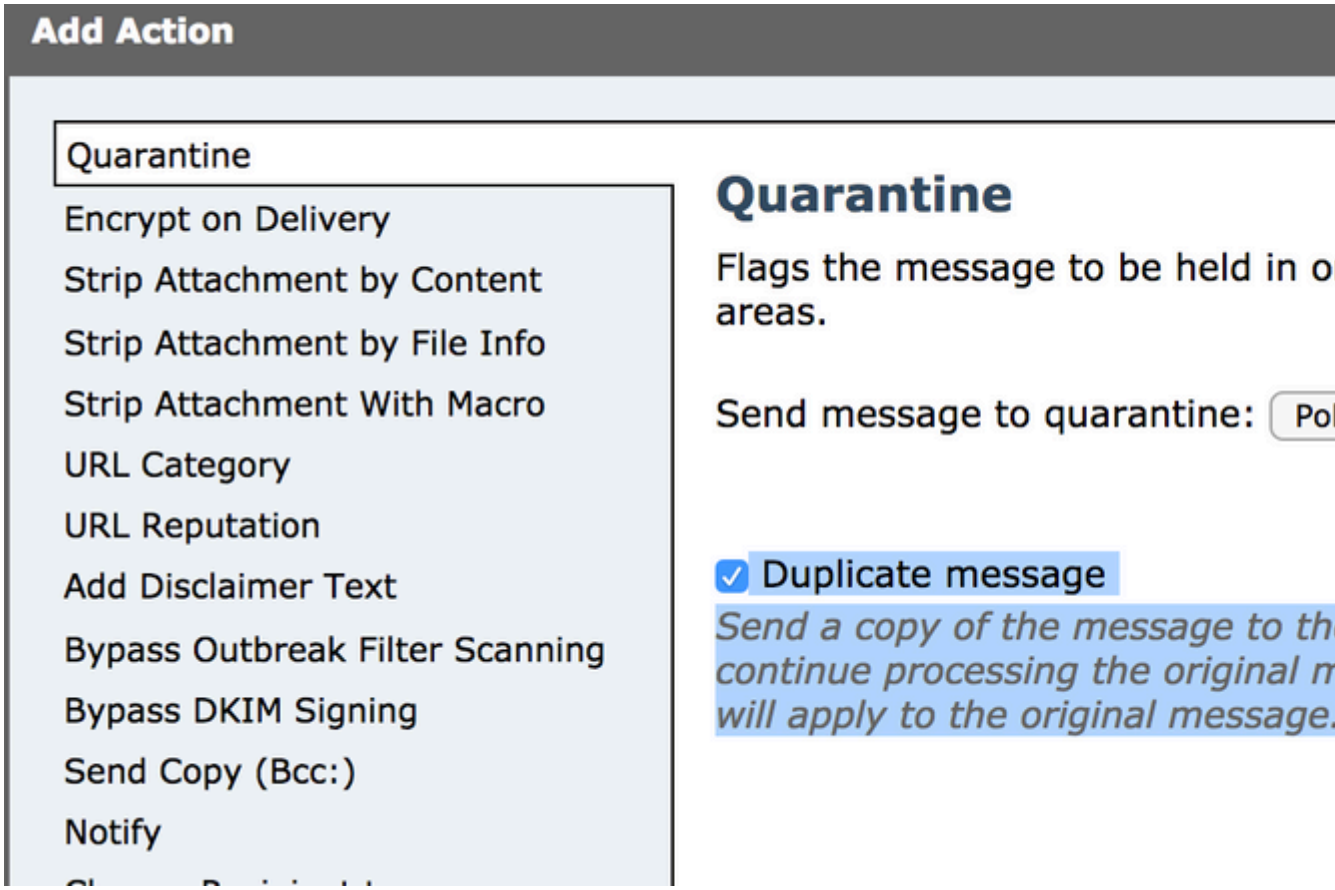
```
mark_spoofed_messages:
if(
     (mail-from-dictionary-match("VALID_INTERNAL_DOMAINS", 1))
 OR  (header-dictionary-match("VALID_INTERNAL_DOMAINS","From", 1)))
 AND ((sendergroup != "RELAYLIST")
 AND (sendergroup != "MY_TRUSTED_SPOOF_HOSTS")
  )
{
insert-header("X-Spoof", "");
```

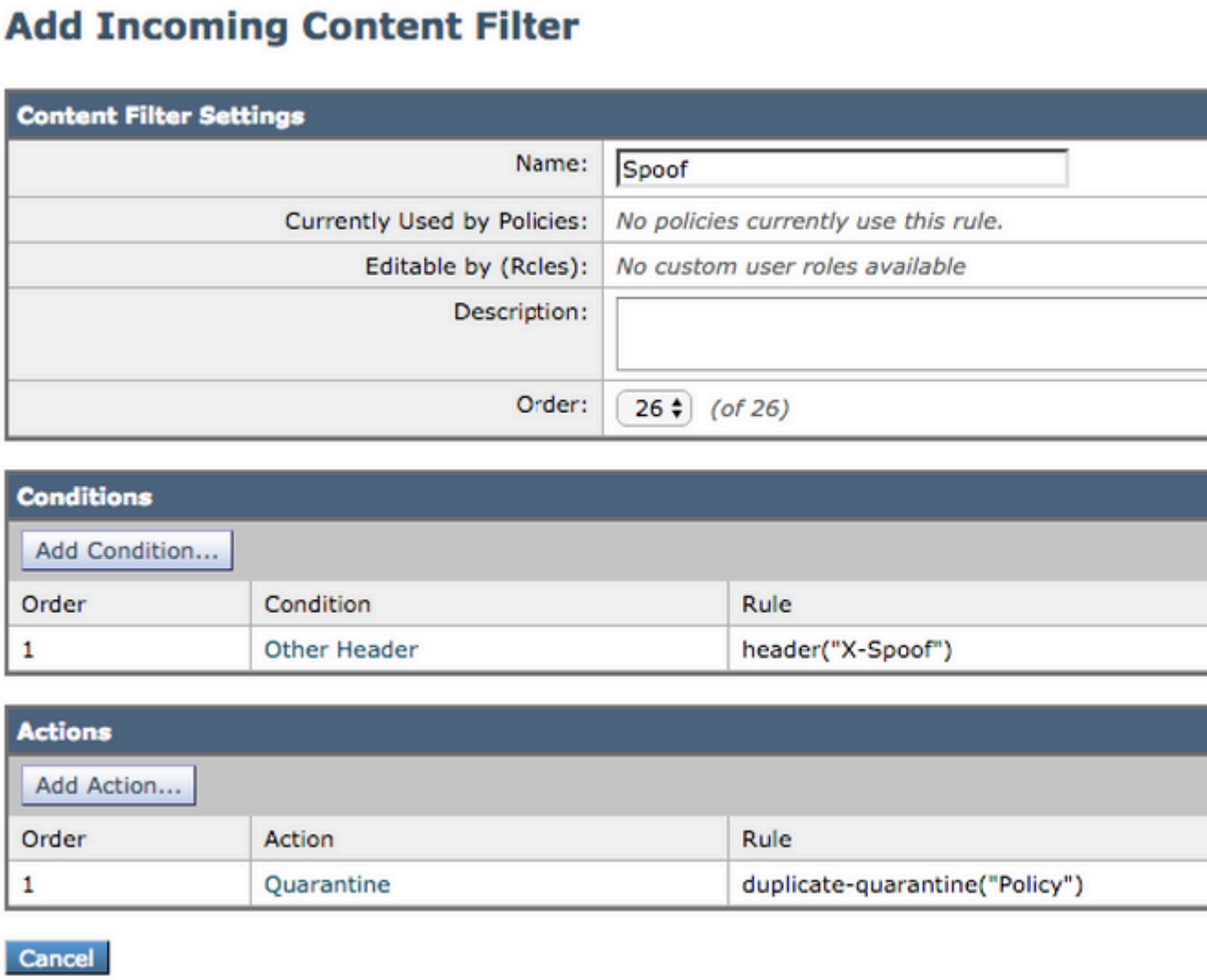
}

5. Retorne ao prompt principal da CLI e execute **Commit** para salvar a configuração.
6. Navegue até a **GUI > Políticas de e-mail > Filtros de conteúdo de entrada**
7. Criar filtro de conteúdo de entrada que age no X-Spoof do cabeçalho de spoof:

    1. Adicionar outro cabeçalho
    2. Nome do cabeçalho: X-Spoof
    3. Botão de opção Cabeçalho existe
    4. Adicionar ação: quarentena duplicada(Política).

> **Observação**: o recurso de mensagem duplicada mostrado aqui mantém uma cópia da mensagem e continua a enviar a mensagem original para o destinatário.





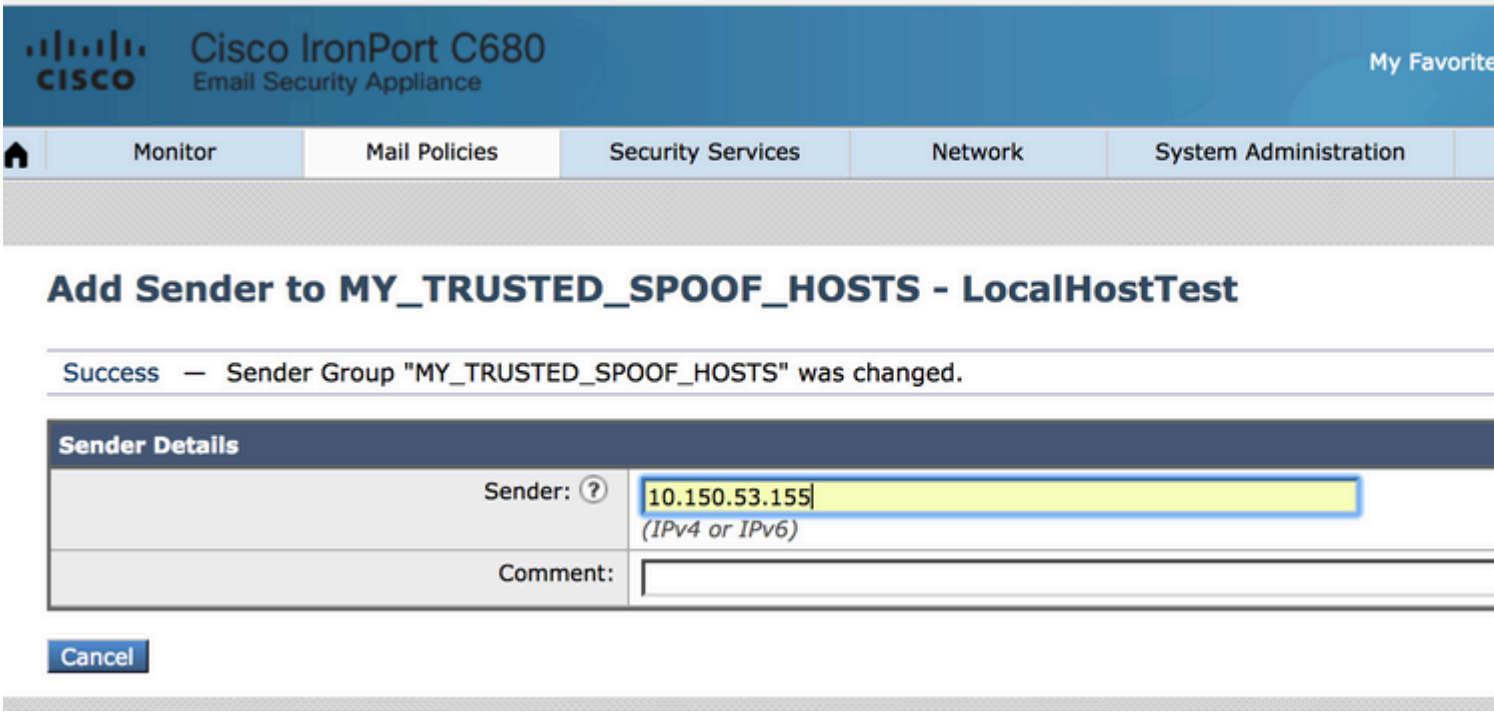
8. Vincule o filtro de conteúdo às políticas de recebimento de e-mail em **GUI > Políticas de e-mail> Políticas de Recebimento de e-mail**.
9. Enviar e confirmar alterações.

Adicionar Spoof-Exceptions a MY_TRUSTED_SPOOF_HOSTS

Finalmente, você precisa adicionar as exceções de falsificação (endereços IP ou nomes de host) ao grupo de remetente MY_TRUSTED_SPOOF_HOSTS.

1. Navegue pela GUI da Web: **Políticas de e-mail > Visão geral do HAT**
2. Clique e **abra** o grupo de remetente MY_TRUSTED_SPOOF_HOSTS.
3. Clique em **Adicionar remetente...** para adicionar um endereço IP, intervalo, nome de host ou nome de host parcial.
4. Clique em **Enviar** para salvar as alterações do remetente.
5. Por fim, clique em **Confirmar alterações** para salvar a configuração.

Exemplo:



Verificar

Verifique se as mensagens falsificadas estão em quarentena

Envie uma mensagem de teste especificando um de seus domínios como remetente de envelope. Valide se o filtro funciona conforme esperado executando um controle de mensagem nessa mensagem. O resultado esperado é que a mensagem seja colocada em quarentena porque você ainda não criou exceções para os remetentes que têm permissão para falsificar.

<#root>

```
Thu Apr 23 07:09:53 2015 Info: MID 102 ICID 9 RID 0 To: <xxxx_xxxx@domain.com>
Thu Apr 23 07:10:07 2015 Info: MID 102 Subject 'test1'
Thu Apr 23 07:10:07 2015 Info: MID 102 ready 177 bytes from <user_1@example.com>
Thu Apr 23 07:10:07 2015 Info: MID 102 matched all recipients for per-recipient policy DEFAULT in the in
Thu Apr 23 07:10:11 2015 Info: MID 102 interim verdict using engine: CASE spam negative
Thu Apr 23 07:10:11 2015 Info: MID 102 using engine: CASE spam negative
Thu Apr 23 07:10:11 2015 Info: MID 102 interim AV verdict using Sophos CLEAN
Thu Apr 23 07:10:11 2015 Info: MID 102 antivirus negative
```

Thu Apr 23 07:10:12 2015 Info: MID 102 quarantined to "Policy" (message filter:quarantine_spoofed_messag

```
Thu Apr 23 07:10:12 2015 Info: Message finished MID 102 done
```

Verifique se as mensagens de Spoof-Exception estão sendo entregues

Remetentes de Spoof-Exception são endereços IP em seus grupos de remetentes referenciados no filtro acima.

RELAYLIST é referenciado porque é usado pelo ESA para enviar e-mails de saída. As mensagens que estão sendo enviadas por RELAYLIST são geralmente e-mails de saída, e não incluir isso criaria falsos positivos

ou mensagens de saída que estão sendo colocadas em quarentena pelo filtro acima.

Exemplo de rastreamento de mensagem de um endereço IP de Spoof-Exception adicionado a MY_TRUSTED_SPOOF_HOSTS. A ação esperada é entregar e não quarentena. (Esse IP tem permissão para falsificar).

<#root>

```
Thu Apr 23 07:25:57 2015 Info: Start MID 108 ICID 11
Thu Apr 23 07:25:57 2015 Info: MID 108 ICID 11 From: <user_1@example.com>
Thu Apr 23 07:26:02 2015 Info: MID 108 ICID 11 RID 0 To: <user_xxxx@domain.com>
Thu Apr 23 07:26:10 2015 Info: MID 108 Subject 'test2'
Thu Apr 23 07:26:10 2015 Info: MID 108 ready 163 bytes from <user_1@example.com>
Thu Apr 23 07:26:10 2015 Info: MID 108 matched all recipients for per-recipient policy DEFAULT in the in
Thu Apr 23 07:26:10 2015 Info: MID 108 interim AV verdict using Sophos CLEAN
Thu Apr 23 07:26:10 2015 Info: MID 108 antivirus negative
Thu Apr 23 07:26:10 2015 Info: MID 108 queued for delivery
Thu Apr 23 07:26:10 2015 Info: Delivery start DCID 16 MID 108 to RID [0]
Thu Apr 23 07:26:11 2015 Info: Message done DCID 16 MID 108 to RID [0]
Thu Apr 23 07:26:11 2015 Info: MID 108 RID [0] Response '2.0.0 t58EVG9N031598
```

Message accepted for delivery'

```
Thu Apr 23 07:26:11 2015 Info: Message finished MID 108 done
```

Informações Relacionadas

- Filtragem de e-mail falsificada do ESA
- Proteger contra falsificação usando a verificação de remetente

Informações internas da Cisco

Há uma solicitação de recurso na exposição do RAT a filtros de mensagem/filtros de conteúdo para simplificar este processo:

ID de bug da Cisco CSCus49018 - ENH: Expose Recipient Access Table (RAT) to filter conditions

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.