Detección de mensajes de correo electrónico falsos en el ESA y creación de excepciones

Contenido

Introducción

Este documento describe cómo controlar la suplantación de correo electrónico en Cisco ESA y cómo crear excepciones para los usuarios a los que se les permite enviar correos electrónicos suplantados.

Prerequisites

Requirements

El dispositivo de seguridad Email Security Appliance (ESA) debe procesar tanto el correo entrante como el saliente, y utilizar una configuración estándar de RELAYLIST para marcar los mensajes como salientes.

Componentes Utilizados

Entre los componentes específicos utilizados se incluyen:

- Diccionario: se utiliza para almacenar todos sus dominios internos.
- Filtro de mensajes: se utiliza para controlar la lógica de detección de correos electrónicos falsificados e insertar un encabezado sobre el que pueden actuar los filtros de contenido.
- Cuarentena de políticas: se utiliza para almacenar temporalmente duplicados de correos electrónicos falsificados. Considere agregar la dirección IP de los mensajes liberados a MY_TRUSTED_SPOOF_HOSTS para evitar que futuros mensajes de este remitente entren en la cuarentena de políticas.
- MY_TRUSTED_SPOOF_HOSTS: lista para hacer referencia a sus direcciones IP remitentes de confianza. Agregar una dirección IP de un remitente a esta lista salta la cuarentena y permite al remitente falsificar. Los remitentes de confianza se colocan en el grupo de remitentes MY_TRUSTED_SPOOF_HOSTS para que los mensajes suplantados de estos remitentes no se

pongan en cuarentena.
- RELAYLIST: lista para autenticar las direcciones IP que pueden retransmitir o enviar correo electrónico saliente. Si el correo electrónico se envía a través de este grupo de remitentes, se supone que el mensaje no es un mensaje falsificado.

Nota: Si se llama a cualquiera de los grupos de remitentes de forma diferente a MY_TRUSTED_SPOOF_HOSTS o RELAYLIST, debe modificar el filtro con el nombre del grupo de remitentes correspondiente. Además, si tiene varios receptores, también tiene más de un MY_TRUSTED_SPOOF_HOSTS.

La información de este documento se basa en el ESA con cualquier versión de AsyncOS.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

La suplantación está activada de forma predeterminada en Cisco ESA. Hay varias razones válidas para permitir que otros dominios envíen en su nombre. Un ejemplo común es que el administrador de ESA desea controlar los correos electrónicos falsos poniendo en cuarentena los mensajes falsos antes de que se entreguen.

Para realizar una acción específica, como poner en cuarentena un correo electrónico falso, primero debe detectar el correo electrónico falso.

Qué es la suplantación de correo electrónico

La suplantación de correo electrónico es la falsificación de un encabezado de correo electrónico para que parezca que el mensaje se ha originado en alguien o en algún lugar que no sea el origen real. La suplantación de correo electrónico es una táctica utilizada en las campañas de phishing y spam, ya que las personas tienen más probabilidades de abrir un correo electrónico cuando creen que lo ha enviado una fuente legítima.

Cómo detectar correo electrónico falso

Desea filtrar todos los mensajes que tengan un remitente de sobre (De correo) y un encabezado de remitente de mensaje descriptivo (De) que contengan uno de sus propios dominios entrantes en la dirección de correo electrónico.

Cómo permitir la suplantación para remitentes específicos

Al implementar el filtro de mensajes proporcionado en este artículo, los mensajes suplantados se etiquetan con un encabezado y el filtro de contenido se utiliza para realizar acciones en el encabezado . Para agregar una excepción, simplemente agregue la IP del remitente a MY_TRUSTED_SPOOF_HOSTS.

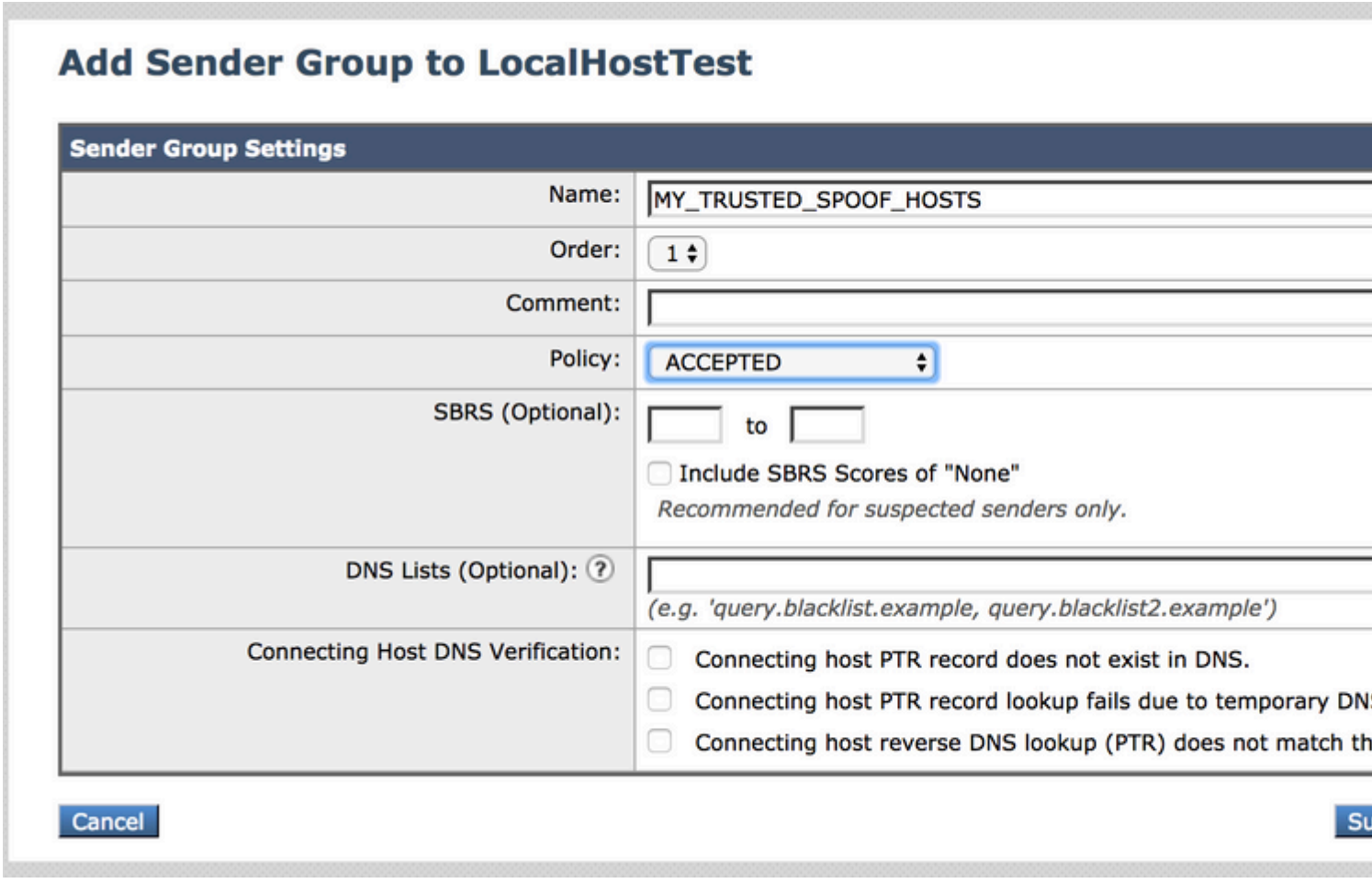
Configurar

Crear un grupo de remitentes

1. Desde la GUI de ESA, navegue hasta **Políticas de correo > Descripción general de HAT**

2. Haga clic en **Agregar.**
3. En el campo Nombre, especifique **MY_TRUSTED_SPOOF_HOSTS**.
4. En el campo Orden, especifique **1**.
5. Para el campo Política, especifique **ACCEPTED**.
6. Haga clic en **Enviar** para guardar los cambios.
7. Por último, haga clic en **Commit Changes** para guardar la configuración

Ejemplo:

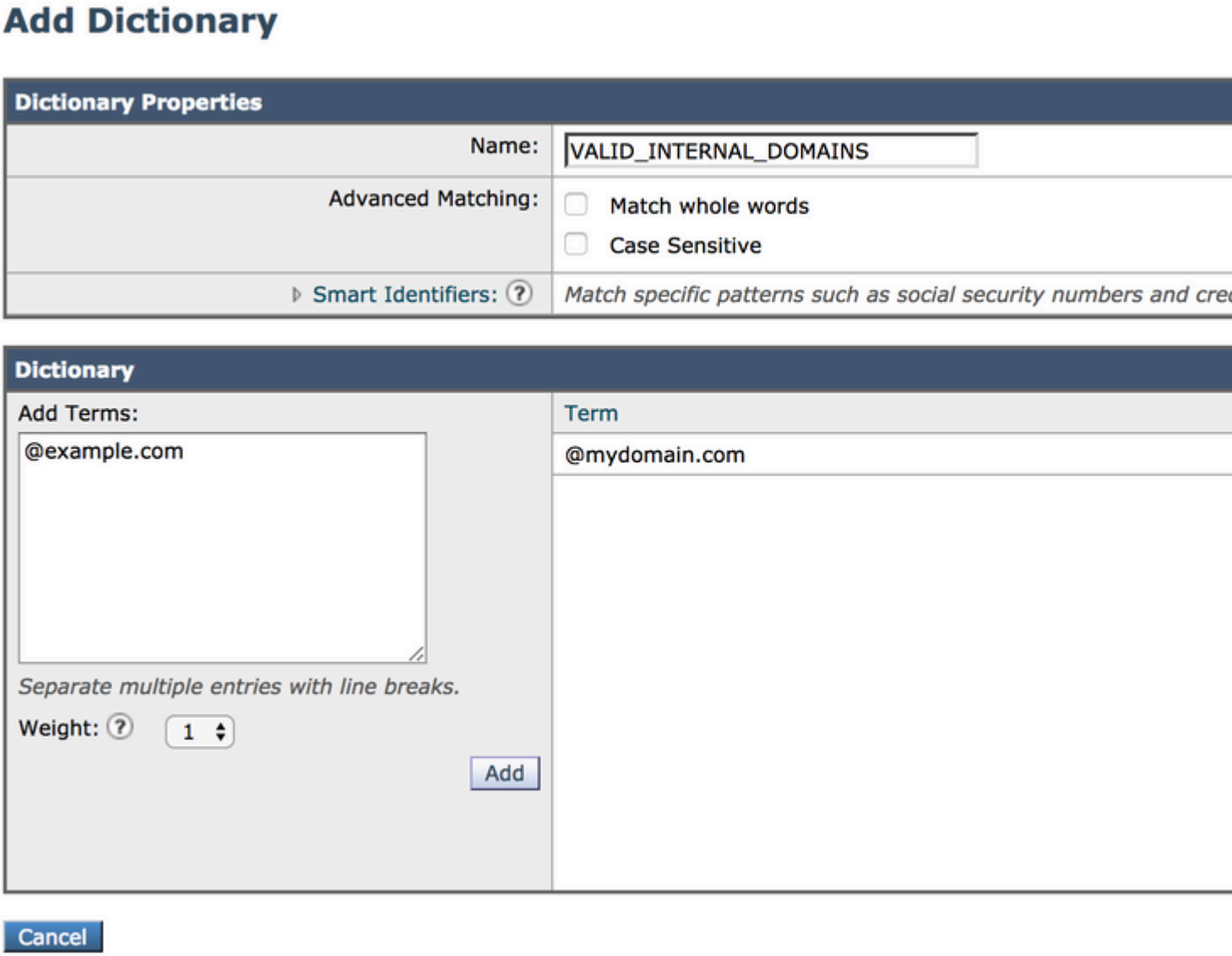


Crear un diccionario

Cree un diccionario para todos los dominios para los que desee inhabilitar la suplantación en el ESA:

1. Desde la GUI de ESA, navegue hasta **Políticas de correo > Diccionarios.**
2. Haga clic en **Agregar Diccionario.**
3. En el campo Nombre, especifique 'VALID_INTERNAL_DOMAINS' para que la copia y el pegado del filtro de mensajes no tengan errores.
4. En Agregar términos, agregue todos los dominios que desee que detecten suplantación. Ingrese el dominio con un signo @ precediendo al dominio y haga clic en **add**.
5. Asegúrese de que la casilla de verificación **coincidencia de palabras enteras** no esté marcada.
6. Haga clic en **Submit** para guardar los cambios del diccionario.
7. Por último, haga clic en **Commit Changes** para guardar la configuración.

Ejemplo:



Crear un filtro de mensajes

A continuación, debe crear un filtro de mensajes para aprovechar el diccionario recién creado, "VALID_INTERNAL_DOMAINS"**:**

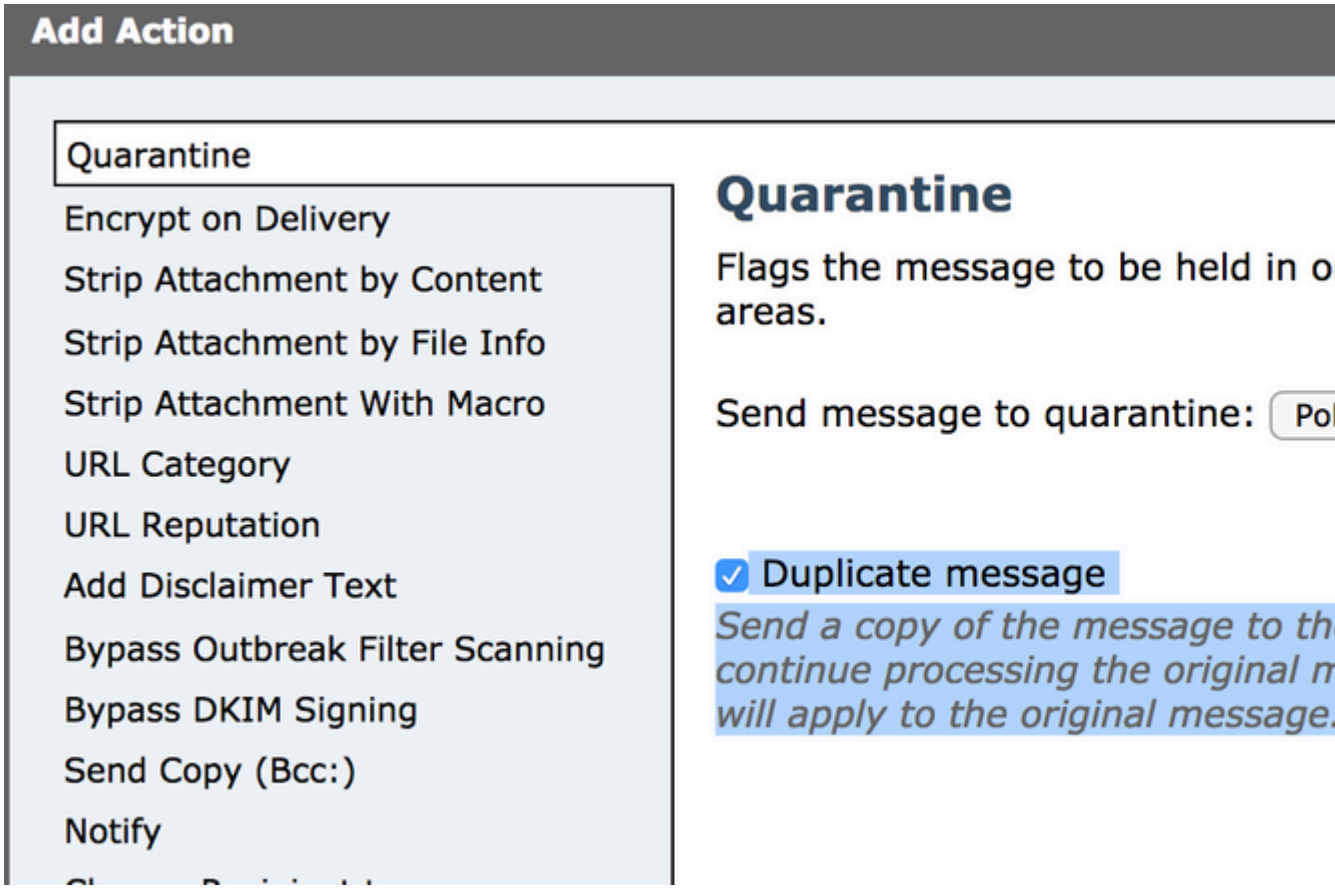
1. Conectar con la interfaz de línea de comandos (CLI) del ESA.
2. Ejecute el comando **Filters.**
3. Ejecute el comando **New** para crear un nuevo filtro de mensajes.
4. Copie y pegue este ejemplo de filtro y edite los nombres reales de los grupos de remitentes si es necesario:

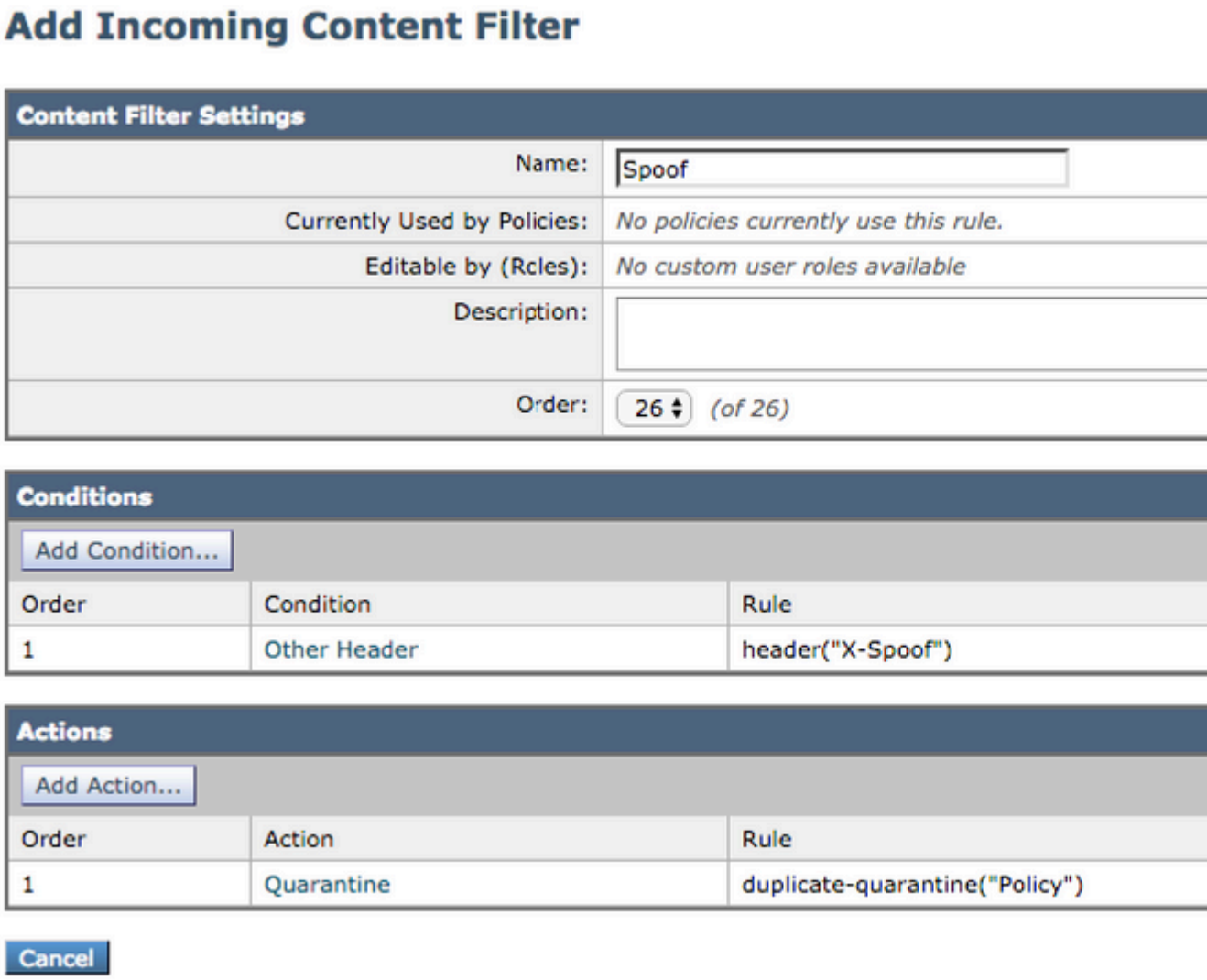
```
mark_spoofed_messages:
if(
     (mail-from-dictionary-match("VALID_INTERNAL_DOMAINS", 1))
 OR  (header-dictionary-match("VALID_INTERNAL_DOMAINS","From", 1)))
 AND ((sendergroup != "RELAYLIST")
 AND (sendergroup != "MY_TRUSTED_SPOOF_HOSTS")
  )
{
```

```
insert-header("X-Spoof", "");
}
```

5. Vuelva al prompt principal de CLI y ejecute **Commit** para guardar la configuración.
6. Vaya a **GUI > Políticas de correo > Filtros de contenido entrante**
7. Cree un filtro de contenido entrante que realice una acción sobre el encabezado de simulación X-Spoof:
    1. Agregar otro encabezado
    2. Nombre del encabezado: X-Spoof
    3. Botón de opción El encabezado existe
    4. Agregar acción: duplicate-quarantine(Policy).

Nota: La función Duplicar mensaje que se muestra aquí mantiene una copia del mensaje y continúa enviando el mensaje original al destinatario.





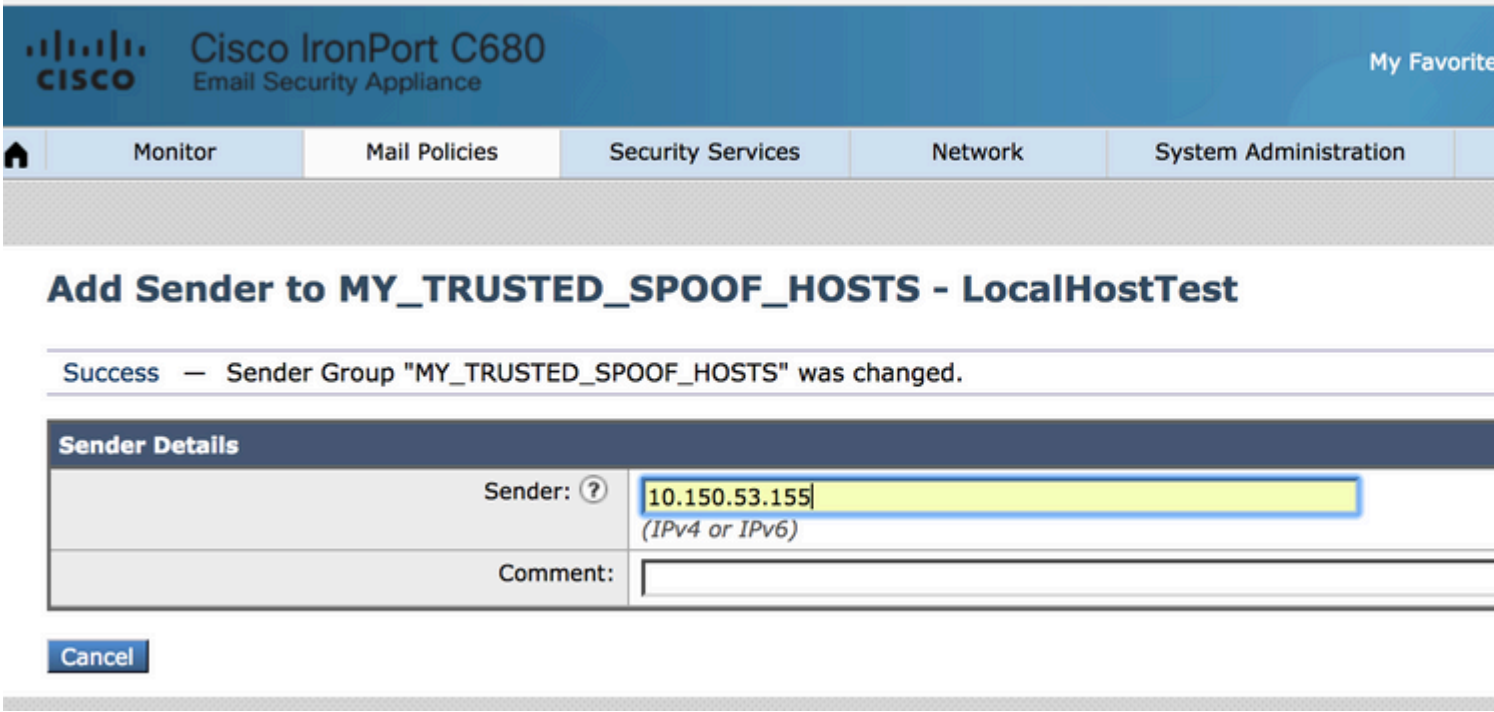
8. Enlace el filtro de contenido a las políticas de correo entrante en **GUI > Políticas de correo> Políticas de correo entrante**.
9. Enviar y registrar cambios.

Agregar excepciones de simulación a MY_TRUSTED_SPOOF_HOSTS

Por último, debe agregar excepciones simuladas (direcciones IP o nombres de host) al grupo de remitentes MY_TRUSTED_SPOOF_HOSTS.

1. Navegue a través de la GUI web: **Políticas de correo > Descripción general de HAT**
2. Haga clic y **abra** el grupo de remitentes MY_TRUSTED_SPOOF_HOSTS.
3. Haga clic en **Agregar remitente...** para agregar una dirección IP, intervalo, nombre de host o nombre de host parcial.
4. Haga clic en **Enviar** para guardar los cambios del remitente.
5. Por último, haga clic en **Commit Changes** para guardar la configuración.

Ejemplo:



Verificación

Verificar que los Mensajes Falsificados estén en Cuarentenas

Envíe un mensaje de prueba especificando uno de sus dominios como remitente del sobre. Valide que el filtro funciona según lo esperado realizando un seguimiento del mensaje en ese mensaje. El resultado esperado es que el mensaje se ponga en cuarentena porque aún no ha creado ninguna excepción para los remitentes a los que se les permite suplantar.

<#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
```

Verificar que se Entregan Mensajes de Falsificación-Excepción

Los remitentes de excepción de simulación son direcciones IP de los grupos de remitentes a los que se hace referencia en el filtro anterior.

Se hace referencia a RELAYLIST porque ESA la utiliza para enviar correo saliente. Los mensajes enviados por RELAYLIST son generalmente correo saliente, y no incluirlos crearía falsos positivos, o mensajes

salientes puestos en cuarentena por el filtro anterior.

Ejemplo de seguimiento de mensajes de una dirección IP de excepción falsa que se agregó a MY_TRUSTED_SPOOF_HOSTS. La acción esperada es entregar y no poner en cuarentena. (Esta IP puede falsificarse).

<#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
```

Información Relacionada

- ESA Spoofed Mail Filtering
- Protección contra falsificación mediante verificación de remitente

Información interna de Cisco

Hay una solicitud de función sobre la exposición de la RAT a filtros de mensaje/filtros de contenido para simplificar este proceso:

ID de bug de Cisco CSCus49018 - ENH: Exponer la Tabla de Acceso de Destinatarios (RAT) para filtrar condiciones

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).