Permitir que un remitente de confianza omita el Anti-Spam

Contenido

Introducción

Este documento describe los detalles de permitir que un remitente de confianza omita el escaneo Anti-Spam y también los diferentes métodos que puede elegir para el mismo en el gateway de correo electrónico seguro (anteriormente conocido como dispositivo de seguridad de correo electrónico).

Adición de Nombre de Host de Remitente/Dirección IP en Grupo de Remitentes ALLOWED_LIST

Agregue remitentes en los que confía al grupo de remitentes ALLOWED_LIST porque este grupo de remitentes utiliza la política de flujo de correo de $TRUSTED. Los miembros del grupo de remitentes ALLOWED_LIST no están sujetos a limitación de velocidad, y el contenido de esos remitentes no es analizado por el motor Anti-Spam, pero aún es escaneado por Anti-Virus.

> **Nota:** Con la configuración predeterminada, el análisis antivirus está habilitado pero Anti-Spam está desactivado.

Para permitir que un remitente omita el escaneo antispam, agregue el remitente al grupo de remitentes ALLOWED_LIST en la Tabla de acceso de host (HAT). Puede configurar HAT a través de la GUI o la CLI.

Desde la GUI

1. Seleccione la pestaña **Políticas de correo**.
2. En la sección **Tabla de Acceso de Host**, seleccione **Descripción General de HAT**.
3. A la derecha, asegúrese de que el receptor **InboundMail** esté seleccionado actualmente.
4. En la columna **Grupo de Enviadores**, seleccione **ALLOWED_LIST**.
5. Seleccione el botón **Agregar remitente** cerca de la mitad inferior de la página.
6. Introduzca la dirección IP o el nombre de host que desea permitir que se desvíe en el primer

campo.

Cuando termine de agregar entradas, seleccione el botón **Enviar**. Recuerde seleccionar el botón **Registrar cambios** para guardar los cambios.

Desde la 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
[]>
```

Recuerde ejecutar el comando **commit** para guardar los cambios.

Revisar el análisis antivirus y antispam en la política de flujo de correo de confianza

Para el remitente de confianza, habrá una política de flujo de correo denominada como un presente de confianza de forma predeterminada. La política de flujo de correo de confianza tendrá un comportamiento de conexión de Aceptar (similar al comportamiento de otras políticas de flujo de correo para los correos entrantes).

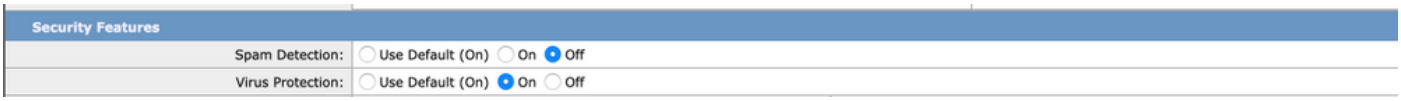
Cuando se confía en un remitente para cumplir los requisitos empresariales, podemos optar por desactivar las comprobaciones antivirus y antispam para ellos. Esto ayudará a reducir la carga de procesamiento adicional en ambos motores de escaneo mientras se escanean los correos electrónicos que no provienen de fuentes de confianza.

> **Nota:** Los motores antivirus y antispam desactivados omitirán los análisis de spam o virus para el correo electrónico entrante en ESA. Esto debe hacerse, sólo si está totalmente seguro de que saltar los escaneos de estos remitentes de confianza no conlleva ningún

riesgo.

La opción desde la que puede inhabilitar los motores está disponible en la pestaña Funciones de seguridad en Políticas de flujo de correo. La trayectoria para lo mismo es **GUI > Políticas de correo > Políticas de flujo de correo**. Haga clic en la **política de flujo de TRUSTEDMail** y desplácese hacia abajo hasta **Funciones de seguridad** en la página siguiente.

Asegúrese de registrar los cambios después de realizar los ajustes que desee.



Agregar un remitente de confianza a la lista de seguridad

Los usuarios finales crean listas de seguridad y listas de bloqueo de usuarios finales y se almacenan en una base de datos que se comprueba antes del análisis antispam. Cada usuario final puede identificar dominios, subdominios o direcciones de correo electrónico que desea tratar siempre como spam o que nunca como spam. Si una dirección de remitente forma parte de una lista de seguridad de usuarios finales, se omite el análisis antispam

Esta configuración permitirá al usuario final poner en la lista de seguridad a un remitente según su requisito de eximir a los análisis antispam. El análisis antivirus y otros análisis de la canalización de correo electrónico no se modificarán con esta configuración y continuarán según la configuración de las políticas de correo. Esta configuración reducirá el compromiso del administrador, cada vez que un usuario final tenga que eximir el escaneo de spam para un remitente.

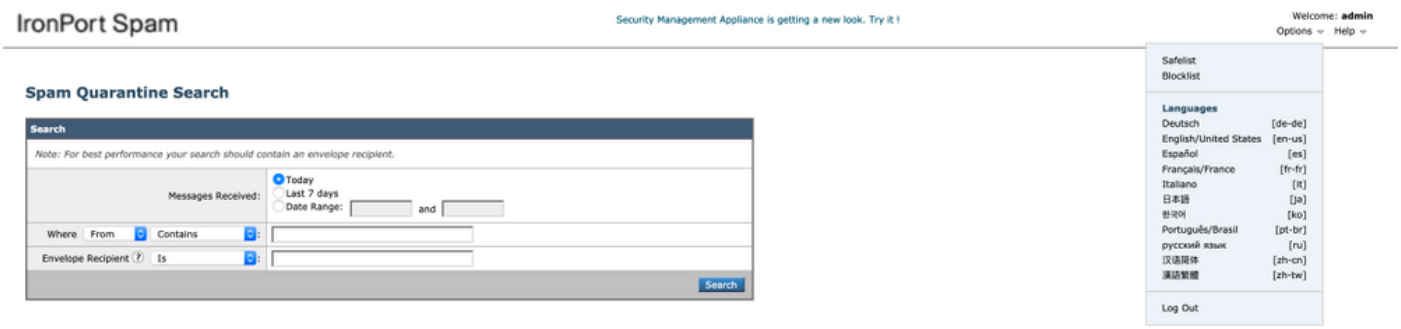
Para la lista de seguridad, es obligatorio que el acceso a la cuarentena de usuario final esté habilitado para los usuarios finales y la lista de seguridad/lista de bloqueo de usuario final como habilitado (tanto en ESA como en SMA). De esa manera, pueden acceder al portal de Spam Quarantine y, junto con **Release/Delete** de los correos electrónicos en cuarentena, también pueden **Agregar/Eliminar** remitentes en la lista de seguridad.

El acceso **a la cuarentena de usuario final** se puede habilitar como se muestra a continuación:

ESA: Vaya a **GUI > Monitor > Spam Quarantine**. Proteja el botón **Radio** para **acceso a cuarentena de usuario final**. Seleccione el método de autenticación para el acceso según los requisitos (Ninguno/LDAP/SAML/IMAP o POP). Publica esto, habilita la lista de seguridad/lista de bloqueo del usuario final.

SMA: Vaya a **GUI > Servicios centralizados > Spam Quarantine**. Proteja el botón **Radio** para **acceso a cuarentena de usuario final**. Seleccione el método de autenticación para el acceso según los requisitos (Ninguno/LDAP/SAML/IMAP o POP). Publica esto, habilita la lista de seguridad/lista de bloqueo del usuario final.

Una vez habilitada, cuando un usuario final navega al portal Spam Quarantine podrá **agregar/modificar** su lista de seguridad según las opciones del menú desplegable de la parte superior derecha.



Remitentes de confianza con políticas de correo entrante

También puede agregar un remitente de confianza en la política de correo entrante y desactivar los análisis **antivirus/antispam** según el requisito. Se puede crear una nueva política de correo personalizada con un nombre como **Remitentes de confianza/Remitentes seguros** etc. según las opciones y, a continuación, puede agregar los detalles del remitente, como nombres de dominio o direcciones de correo electrónico del remitente, a esta política personalizada.

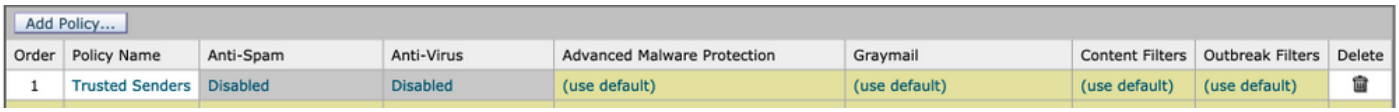
Una vez que envíe la política después de la adición requerida, puede hacer clic en las columnas **Antispam** o **Antivirus,** y en la página siguiente, seleccione **Desactivar**.

Con esta configuración, los dominios de remitentes de confianza o las direcciones de correo electrónico agregadas a esta política de correo quedarán exentos de los análisis antispam o antivirus.

> **Nota:** Los motores antivirus y antispam desactivados omitirán los análisis relacionados con spam o virus para el correo entrante en ESA procesados a través de esta política de correo personalizada. Esto debe hacerse, sólo si está totalmente seguro de que saltar los escaneos de estos remitentes de confianza no conlleva ningún riesgo.

La política de correo personalizada se puede crear desde **ESA GUI > Políticas de correo > Políticas de correo entrante > Agregar política**. Introduzca el nombre de la política según la opción y, a continuación, seleccione **Agregar usuario**. Marque el botón de opción para **Siguientes Remitentes.** Agregue el dominio o las direcciones de correo electrónico necesarias en el cuadro y haga clic en **Aceptar**.

La creación de la política de correo postal permite desactivar los análisis antivirus y antispam según los requisitos empresariales. A continuación se muestra un ejemplo de captura de pantalla:



Información Relacionada

- Dispositivo de seguridad Cisco Email Security Appliance - Guías de usuario final
- Soporte Técnico y Documentación - Cisco Systems