Bloquear un remitente malintencionado o con problemas en el ESA

Contenido

Introducción

Este documento describe cómo agregar una dirección IP maliciosa o un nombre de dominio a su lista de bloqueo en un dispositivo de seguridad Cisco Email Security Appliance (ESA).

Bloquear un remitente malintencionado o con problemas

La forma más sencilla de bloquear a un remitente es agregar su dirección IP o nombre de dominio al grupo de remitentes BLOCKED_LIST dentro de la Tabla de acceso de host (HAT) ESA. El grupo de remitentes BLOCKED_LIST utiliza la política de flujo de correo $BLOCKED, que tiene una regla de acceso de RECHAZO.

> **Nota**: La dirección IP o el nombre de dominio proviene del servidor de correo remitente. La dirección IP del servidor de correo de envío se puede capturar en el seguimiento de mensajes o en los registros de correo, si no se conoce.

Bloquear un remitente mediante la GUI

Complete estos pasos para bloquear un remitente a través de la GUI:

1. Haga clic en **Políticas de correo**.
2. Seleccione **HAT Overview**.
3. Si se configuran varios receptores en el ESA, asegúrese de que el receptor *InboundMail* esté seleccionado actualmente.
4. Seleccione **BLOCKED_LIST** en la columna *Grupo de Remitentes*.
5. Haga clic en **Agregar remitente...**.
6. Introduzca la dirección IP o el nombre de dominio que desea bloquear. Se permiten estos formatos:
   - Direcciones IPv6, como *2001:420:80:1::5*
   - Subredes IPv6, como *2001:db8::/32*
   - Direcciones IPv4, como *10.1.1.0*
   - Subredes IPv4, como *10.1.1.0/24* o *10.2.3.1*
   - Intervalos de direcciones IPv4 e IPv6, como *10.1.1.10-20*, *10.1.1-5* o *2001::2-2001::10*

- Nombres de host, como *example.com*
- Nombres de host parciales, como *.example.com*

7. Haga clic en **Submit** después de agregar las entradas.

8. Haga clic en **Commit Changes** para completar los cambios de configuración.

Bloquear un remitente mediante la CLI

Este es un ejemplo que muestra cómo bloquear a un remitente por nombre de dominio y dirección IP a través de la CLI:

<#root>

```
myesa.local>
```

listenerconfig

```
Currently configured listeners:
1. Bidirectional (on Management, 192.168.1.x) SMTP TCP Port 25 Public

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: Bidirectional
Type: Public
Interface: Management (192.168.1.x/24) TCP Port 25
Protocol: SMTP
Default Domain: example.com
Max Concurrent Connections: 50 (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
Heading: None
SMTP Call-Ahead: Disabled
LDAP: Off

Choose the operation you want to perform:
- NAME - Change the name of the listener.
```

```
- INTERFACE - Change the interface.
- CERTIFICATE - Choose the certificate.
- 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.
- LDAPACCEPT - Configure an LDAP query to determine whether a recipient address
  should be accepted or bounced/dropped.
- LDAPGROUP - Configure an LDAP query to determine whether a sender or recipient
  is in a specified group.
[]>
```

hostaccess

```
Default Policy Parameters
==========================
Maximum Message Size: 10M
Maximum Number Of Concurrent Connections From A Single IP: 10
Maximum Number Of Messages Per Connection: 10
Maximum Number Of Recipients Per Message: 50
Directory Harvest Attack Prevention: Enabled
Maximum Number Of Invalid Recipients Per Hour: 25
Maximum Number Of Recipients Per Hour: Disabled
Maximum Number of Recipients per Envelope Sender: Disabled
Use SenderBase for Flow Control: Yes
Allow TLS Connections: No
Allow SMTP Authentication: No
Require TLS To Offer SMTP authentication: No
DKIM/DomainKeys Signing Enabled: No
DKIM Verification Enabled: No
S/MIME Public Key Harvesting Enabled: Yes
S/MIME Decryption/Verification Enabled: Yes
SPF/SIDF Verification Enabled: Yes
 Conformance Level: SIDF compatible
 Downgrade PRA verification: No
 Do HELO test: Yes
 SMTP actions:
 For HELO Identity: Accept
 For MAIL FROM Identity: Accept
 For PRA Identity: Accept
 Verification timeout: 40
DMARC Verification Enabled: No
Envelope Sender DNS Verification Enabled: No
Domain Exception Table Enabled: Yes

There are currently 6 policies defined.
There are currently 7 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.
```

```
- RESET - Remove senders and set policies to system default.
[]>
```

edit

```
1. Edit Sender Group
2. Edit Policy
[1]>
```

1

```
Currently configured HAT sender groups:
1. ALLOWSPOOF
2. MY_INBOUND_RELAY
3. WHITELIST (My trusted senders have no anti-spam scanning or rate limiting)
4. BLOCKED_LIST (Spammers are rejected)
5. SUSPECTLIST (Suspicious senders are throttled)
6. UNKNOWNLIST (Reviewed but undecided, continue normal acceptance)
7. (no name, first host = ALL) (Everyone else)
Enter the sender group number or name you wish to edit.
[]>
```

4

```
Choose the operation you want to perform:
- NEW - Add a new host.
- DELETE - Remove a host.
- POLICY - Change the policy settings and options.
- PRINT - Display the current definition.
- RENAME - Rename this sender group.
[]>
```

new

```
Enter the senders to add to this sender group. A sender group entry can be
any of the following:
- an IP address
- a CIDR address such as 10.1.1.0/24 or 2001::0/64
- an IP range such as 10.1.1.10-20, 10.1.1-5 or 2001:db8::1-2001:db8::10.
- an IP subnet such as 10.2.3.
- a hostname such as crm.example.com
- a partial hostname such as .example.com
- a range of SenderBase Reputation Scores in the form SBRS[7.5:10.0]
- a SenderBase Network Owner ID in the form SBO:12345
- a remote blocklist query in the form dnslist[query.blocklist.example]
Separate multiple entries with commas.
[]>
```

badhost.example.org, 10.1.1.10

Nota: Recuerde **realizar** todos y cada uno de los cambios que se realicen desde la CLI principal.

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).