# Ponga un remitente malévolo o del problema en el ESA

## Contenido



## Introducción

Este documento describe cómo agregar una dirección IP o un Domain Name malévola a su lista negra en un dispositivo de seguridad del correo electrónico de Cisco (ESA).

## Ponga un remitente malévolo o del problema

La manera más fácil de poner un remitente es agregar su dirección IP o Domain Name al grupo del remitente de la LISTA NEGRA dentro de la tabla del acceso del host ESA (SOMBRERO). El grupo del remitente de la LISTA NEGRA utiliza la directiva del flujo de correo $BLOCKED, que tiene una regla de acceso de RECHAZO.

> Nota: La dirección IP o el Domain Name es del mail server de envío. La dirección IP del mail server de envío puede ser capturada de Seguimiento de mensajes o en los registros del correo, si no ser sabida.

### Ponga un remitente vía el GUI

Complete estos pasos para poner un remitente vía el GUI:

1. Haga clic las **directivas del correo**.
2. Seleccione la **descripción del SOMBRERO**.
3. Si hay módulos de escucha múltiples configurados en el ESA, asegúrese de que seleccionen al módulo de escucha de *InboundMail* actualmente.
4. Seleccione la **LISTA NEGRA de la** columna del *grupo del remitente*.

5. El tecleo **agrega el remitente….**

6. Ingrese el IP address o el Domain Name que usted desea poner. Se permiten estos formatos:

   Direccionamientos del IPv6, tales como *2001:420:80:1::5*Subredes del IPv6, tales como *2001:db8::/32*Direccionamientos del IPv4, tales como *10.1.1.0*Subredes del IPv4, tales como *10.1.1.0/24* o *10.2.3.1*Intervalos de direcciones del IPv4 y del IPv6, tales como *10.1.1.10-20*, *10.1.1-5*, o *2001::2-2001::10*Nombres de host, tales como *example.com*Nombres de host parciales, tales como *.example.com*

7. El tecleo **somete** después de que usted haya agregado sus entradas.

8. **Cambios del cometer del** tecleo para completar los cambios de configuración.

## Ponga un remitente vía el CLI

Aquí está un ejemplo que muestra cómo poner un remitente por el Domain Name y la dirección IP vía el CLI:

```
myesa.local> listenerconfig

Currently configured listeners:
1. Bidirectional (on Management, 172.18.249.222) 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 (172.18.249.222/24) 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. BLACKLIST (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 blacklist query in the form dnslist[query.blacklist.example]
Separate multiple entries with commas.
[]> badhost.example.org, 10.1.1.10
```

Nota: Recuerde **confiar** cualquiera y todos los cambios que se realicen del CLI principal.