Mettez un expéditeur sur la liste noire malveillant ou de problème sur l'ESA

Contenu

Introduction

Ce document décrit comment ajouter une adresse IP ou un nom de domaine malveillante à votre liste noire sur une appliance de sécurité du courrier électronique de Cisco (ESA).

Mettez un expéditeur sur la liste noire malveillant ou de problème

Le moyen le plus simple de mettre un expéditeur sur la liste noire est d'ajouter leur adresse IP ou nom de domaine au groupe d'expéditeur de LISTE NOIRE dans le Tableau d'accès au hôte ESA (CHAPEAU). Le groupe d'expéditeur de LISTE NOIRE utilise la stratégie de flux de courrier $BLOCKED, qui a une règle d'accès d'ANOMALIE.

> Remarque: L'adresse IP ou le nom de domaine est du serveur de messagerie de envoi. L'adresse IP du serveur de messagerie de envoi peut être capturée du message dépistant ou dans la messagerie se connecte, sinon connu.

Mettez un expéditeur sur la liste noire par l'intermédiaire du GUI

Terminez-vous ces étapes afin de mettre un expéditeur sur la liste noire par l'intermédiaire du GUI :

1. **Stratégies de messagerie de** clic.
2. **Aperçu** choisi de **CHAPEAU**.
3. S'il y a de plusieurs auditeurs configurés sur l'ESA, assurez-vous que l'auditeur d'*InboundMail* est actuellement sélectionné.
4. Sélectionnez la **LISTE NOIRE de la** colonne de *groupe d'expéditeur*.

5. Cliquez sur Add l'**expéditeur….**

6. Écrivez l'IP address ou le Domain Name que vous souhaitez mettre sur la liste noire. On permet ces formats :

   Adresses d'IPv6, telles que *2001:420:80:1::5*Sous-réseaux d'IPv6, tels que *2001:db8::/32*Adresses d'ipv4, telles que *10.1.1.0*Sous-réseaux d'ipv4, tels que *10.1.1.0/24* ou *10.2.3.1*Chaînes d'ipv4 et d'ipv6 addres, telles que *10.1.1.10-20*, *10.1.1-5*, ou *2001::2-2001::10*Adresses Internet, telles qu'*example.com*Adresses Internet partielles, telles que *.example.com*

7. Cliquez sur Submit **après que vous ayez ajouté vos entrées.**

8. **La validation de** clic **change** afin de se terminer les modifications de configuration.

Mettez un expéditeur sur la liste noire par l'intermédiaire du CLI

Voici un exemple qui affiche comment mettre un expéditeur sur la liste noire par le nom de domaine et l'adresse IP par l'intermédiaire du 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
```

Remarque: Souvenez-vous **pour commettre** l'intégralité de modifications qui sont apportées à partir du CLI principal.