Bloquer un expéditeur malveillant ou problématique sur l'ESA

Table des matières

Introduction

Ce document décrit comment ajouter une adresse IP ou un nom de domaine malveillant à votre liste de blocage sur un appareil de sécurité de la messagerie Cisco (ESA).

Bloquer un expéditeur malveillant ou problématique

Le moyen le plus simple de bloquer un expéditeur consiste à ajouter son adresse IP ou son nom de domaine au groupe d'expéditeurs BLOCKED_LIST dans la table d'accès aux hôtes ESA (HAT). Le groupe d'expéditeurs BLOCKED_LIST utilise la stratégie de flux de messages $BLOCKED, dont la règle d'accès est REJECT.

Remarque : l'adresse IP ou le nom de domaine provient du serveur de messagerie expéditeur. L'adresse IP du serveur de messagerie expéditeur peut être capturée à partir du suivi des messages ou dans les journaux de messagerie, si elle n'est pas connue.

Bloquer un expéditeur via l'interface utilisateur graphique

Complétez ces étapes afin de bloquer un expéditeur via l'interface utilisateur graphique :

1. Cliquez sur Politiques de messagerie.
2. Sélectionnez HAT Overview.
3. Si plusieurs écouteurs sont configurés sur l'ESA, assurez-vous que l'écouteur InboundMail est actuellement sélectionné.
4. Sélectionnez BLOCKED_LIST dans la colonne Sender Group.
5. Cliquez sur Ajouter un expéditeur...
6. Saisissez l'adresse IP ou le nom de domaine que vous souhaitez bloquer. Ces formats sont

autorisés :

- Adresses IPv6, telles que 2001:420:80:1::5
- Sous-réseaux IPv6, tels que 2001:db8::/32
- Adresses IPv4, telles que 10.1.1.0
- Sous-réseaux IPv4, tels que 10.1.1.0/24 ou 10.2.3.1
- Plages d'adresses IPv4 et IPv6, telles que 10.1.1.10-20, 10.1.1-5 ou 2001::2-2001::10
- Noms d'hôte, tels que example.com
- Noms d'hôte partiels, tels que .example.com

7. Cliquez sur Submit après avoir ajouté vos entrées.

8. Cliquez sur Commit Changes afin de compléter les modifications de configuration.

Bloquer un expéditeur via la CLI

Voici un exemple qui montre comment bloquer un expéditeur par nom de domaine et adresse IP via l'interface de ligne de commande :

```
<#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

 Remarque : n'oubliez pas de valider toutes les modifications apportées à partir de l'interface de ligne de commande principale.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.