Blockieren eines Absenders mit schädlichen oder problematischen Inhalten auf der ESA

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie Sie Ihrer Sperrliste einer Cisco E-Mail Security Appliance (ESA) eine schädliche IP-Adresse oder einen schädlichen Domänennamen hinzufügen.

Blockieren eines Absenders mit schädlichen oder problematischen Inhalten

Die einfachste Möglichkeit, einen Absender zu blockieren, besteht darin, seine IP-Adresse oder seinen Domänennamen der Absendergruppe BLOCKED_LIST in der ESA Host Access Table (HAT) hinzuzufügen. Die Absendergruppe BLOCKED_LIST verwendet die $BLOCKED Mail Flow-Richtlinie, für die die Zugriffsregel REJECT gilt.

> **Hinweis**: Die IP-Adresse oder der Domänenname stammen vom sendenden Mailserver. Die IP-Adresse des sendenden Mail-Servers kann aus der Nachrichtenverfolgung oder in den Mail-Protokollen erfasst werden, wenn sie nicht bekannt ist.

Absender über die GUI blockieren

Gehen Sie wie folgt vor, um einen Absender über die GUI zu blockieren:

1. Klicken Sie auf **Mail-Policys**.
2. Wählen Sie **HAT Overview aus**.
3. Wenn auf der ESA mehrere Listener konfiguriert sind, stellen Sie sicher, dass der *InboundMail*-Listener aktuell ausgewählt ist.
4. Wählen Sie **BLOCKED_LIST** in der Spalte *Absendergruppe aus*.
5. Klicken Sie auf **Absender hinzufügen...**.
6. Geben Sie die IP-Adresse oder den Domänennamen ein, die bzw. den Sie blockieren möchten. Diese Formate sind zulässig:
   - IPv6-Adressen wie *2001:420:80:1::5*
   - IPv6-Subnetze wie *2001:db8::/32*
   - IPv4-Adressen wie *10.1.1.0*

- IPv4-Subnetze wie *10.1.1.0/24* oder *10.2.3.1*
- IPv4- und IPv6-Adressbereiche wie *10.1.1.10-20*, *10.1.1-5* oder *2001::2-2001::10*
- Hostnamen, z. B. *example.com*
- Partielle Hostnamen, z. B. *.example.com*

7. Klicken Sie nach dem Hinzufügen Ihrer Einträge auf **Senden**.

8. Klicken Sie auf **Änderungen bestätigen**, um die Konfigurationsänderungen abzuschließen.

Absender über die CLI blockieren

Das folgende Beispiel zeigt, wie ein Absender über die CLI nach Domänenname und IP-Adresse blockiert wird:

```
<#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

Hinweis: Denken Sie daran, alle über die Haupt-CLI vorgenommenen Änderungen zu **bestätigen**.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.