Blokkeer een kwaadaardige of probleemafzender op de ESA

Inhoud

Inleiding

Dit document beschrijft hoe u een kwaadaardig IP-adres of een domeinnaam aan uw blokkeringslijst kunt toevoegen op een Cisco Email Security Applicatie (ESA).

Blokkeer een kwaadaardige of probleemafzender

De gemakkelijkste manier om een afzender te blokkeren is hun IP-adres of domeinnaam toe te voegen aan de groep met afzenders van BLOCKED_LIST binnen de ESA Host Access Table (HAT). De afzendergroep BLOCKED_LIST gebruikt het beleid van $BLOCKED mail flow, dat een toegangsregel van REJECT heeft.

> **Opmerking**: Het IP-adres of de domeinnaam is afkomstig van de verzendende mailserver. Het IP-adres van de verzendende e-mailserver kan worden opgenomen bij het bijhouden van berichten of in de e-maillogbestanden, indien dit niet bekend is.

Een afzender blokkeren via de GUI

Voltooi deze stappen om een afzender via de GUI te blokkeren:

1. Klik op **E-mailbeleid**.
2. Selecteer **dat overzicht**.
3. Als meerdere luisteraars zijn geconfigureerd op de ESA, zorg er dan voor dat de *InboundMail* luisteraar is geselecteerd.
4. Selecteer **BLOCKED_LIST** in de kolom *Sender Group*.
5. Klik op **Verzender toevoegen...**.
6. Voer het IP-adres of de domeinnaam in dat u wilt blokkeren. Deze formaten zijn toegestaan:
    - IPv6-adressen, zoals *2001:420:80:1:5*
    - IPv6-subnetten, zoals *2001:db8::/32*
    - IPv4-adressen, zoals *10.1.1.0*
    - IPv4-subnetten, zoals *10.1.1.0/24* of *10.2.3.1*
    - IPv4- en IPv6-adresbereiken, zoals *10.1.10-20*, *10.1.1-5*, of *2001::2-2001::10*
    - Hostnames, zoals *example.com*

- Gedeeltelijke hostnamen, zoals *.example.com*

7. Klik op **Verzenden** nadat u uw gegevens hebt toegevoegd.
8. Klik op **Wijzigingen vastleggen** om de configuratiewijzigingen te voltooien.

Een afzender blokkeren via de CLI

Hier is een voorbeeld dat laat zien hoe u een afzender blokkeert op domeinnaam en IP-adres via de 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

Opmerking: Vergeet niet om alle wijzigingen te **begaan** die vanuit de belangrijkste CLI zijn aangebracht.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.