Blocca un mittente dannoso o con problemi sull'ESA

Sommario

Introduzione

In questo documento viene descritto come aggiungere un indirizzo IP o un nome di dominio dannoso all'elenco di indirizzi bloccati su Cisco Email Security Appliance (ESA).

Blocca un mittente dannoso o con problemi

Il modo più semplice per bloccare un mittente è quello di aggiungere il suo indirizzo IP o nome di dominio al gruppo di mittenti BLOCKED_LIST all'interno della tabella HAT (Host Access Table) dell'ESA. Il gruppo mittente BLOCKED_LIST utilizza il criterio di flusso di posta $BLOCKED, che dispone di una regola di accesso REJECT.

> **Nota**: l'indirizzo IP o il nome di dominio proviene dal server di posta elettronica di invio. L'indirizzo IP del server di posta elettronica di invio può essere acquisito da verifica messaggi o nei log di posta, se non è noto.

Blocca un mittente tramite la GUI

Per bloccare un mittente tramite la GUI, completare la procedura seguente:

1. Fare clic su **Criteri di posta**.
2. Selezionare **Panoramica HAT**.
3. Se sull'ESA sono configurati più listener, verificare che il listener *InboundMail* sia selezionato.
4. Selezionare **BLOCKED_LIST** dalla colonna *Gruppo mittenti*.
5. Scegliere **Aggiungi mittente...**.
6. Immettere l'indirizzo IP o il nome di dominio che si desidera bloccare. Sono consentiti i seguenti formati:
   - indirizzi IPv6, ad esempio *2001:420:80:1::5*
   - Subnet IPv6, ad esempio *2001:db8::/32*
   - indirizzi IPv4, ad esempio *10.1.1.0*
   - Subnet IPv4, ad esempio *10.1.1.0/24* o *10.2.3.1*
   - Intervalli di indirizzi IPv4 e IPv6, ad esempio *10.1.1.10-20*, *10.1.1-5* o *2001::2-2001::10*

- nomi host, ad esempio *example.com*
- nomi host parziali, ad esempio *.example.com*

7. Fare clic su **Submit** (Invia)dopo aver aggiunto i dati.

8. Per completare le modifiche alla configurazione, fare clic su **Commit delle modifiche**.

Blocca un mittente tramite la CLI

Di seguito è riportato un esempio che mostra come bloccare un mittente per nome di dominio e indirizzo IP tramite la 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

Nota: ricordarsi di eseguire il **commit** su qualsiasi modifica apportata dalla CLI principale.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).