Põr um remetente malicioso ou do problema no ESA

Índice

Introdução

Este documento descreve como adicionar um endereço IP de Um ou Mais Servidores Cisco ICM NT ou um Domain Name malicioso a sua lista negra em uma ferramenta de segurança do email de Cisco (ESA).

Põr um remetente malicioso ou do problema

A maneira a mais fácil de põr um remetente é adicionar seu endereço IP de Um ou Mais Servidores Cisco ICM NT ou Domain Name ao grupo do remetente da LISTA NEGRA dentro da tabela do acesso host ESA (CHAPÉU). O grupo do remetente da LISTA NEGRA usa a política do fluxo de correio $BLOCKED, que tem uma regra do acesso de REJEIÇÃO.

> Nota: O endereço IP de Um ou Mais Servidores Cisco ICM NT ou o Domain Name são do mail server de emissão. O endereço IP de Um ou Mais Servidores Cisco ICM NT do mail server de emissão pode ser capturado do rastreamento de mensagem ou nos logs do correio, se não ser sabido.

Põr um remetente através do GUI

Termine estas etapas a fim põr um remetente através do GUI:

1. Clique **políticas do correio**.
2. Selecione a **vista geral do CHAPÉU**.
3. Se há ouvintes múltiplos configurados no ESA, assegure-se de que o ouvinte de *InboundMail* esteja selecionado atualmente.

4. Selecione a **LISTA NEGRA da** coluna do *grupo do remetente*.

5. O clique **adiciona o remetente….**

6. Incorpore o IP address ou o Domain Name que você deseja pôr. Estes formatos são permitidos:

   Endereços do IPv6, tais como *2001:420:80:1::5*Sub-redes do IPv6, tais como *2001:db8::/32*Endereços do IPv4, tais como *10.1.1.0*Sub-redes do IPv4, tais como *10.1.1.0/24* ou *10.2.3.1*Escalas de endereço do IPv4 e do IPv6, tais como *10.1.1.10-20*, *10.1.1-5*, ou *2001::2-2001::10*Nomes de host, tais como *example.com*Nomes de host parciais, tais como *.example.com*

7. O clique **submete-se** depois que você adicionou suas entradas.

8. O clique **compromete mudanças** a fim terminar as alterações de configuração.

Põr um remetente através do CLI

Está aqui um exemplo que mostre como pôr um remetente pelo Domain Name e o endereço IP de Um ou Mais Servidores Cisco ICM NT através do 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
```

Nota: Recorde comprometer alguns e todas as mudanças que forem feitas do CLI principal.