Como faz você Whitelist um remetente confiado?

Índice

Pergunta

Como faz você Whitelist um remetente confiado?

Resposta

Na ferramenta de segurança do email de Cisco (ESA), adicionar remetentes que você confia ao grupo do remetente WHITELIST porque este grupo do remetente usa a política do fluxo de correio $TRUSTED. Os membros do grupo do remetente WHITELIST não são sujeitos avaliar a limitação, e o índice daqueles remetentes não é feito a varredura pelo motor de Cisco IronPort AntiSpam, mas é feito a varredura ainda pelo software anti-vírus de Sophos.

> Nota: À revelia a configuração, exploração anti-vírus é permitida mas o Anti-Spam é desligado.

Ao whitelist um remetente, adiciona o remetente ao grupo do remetente WHITELIST na tabela do acesso host (CHAPÉU). Você pode configurar o CHAPÉU através do GUI ou do CLI.

Do GUI

1. Clique a aba das *políticas do correio*.
2. Sob a seção da *tabela do acesso host*, selecione a *vista geral do CHAPÉU,*
3. Àdireita, certifique-se que seu ouvinte de *InboundMail* está selecionado atualmente,
4. Da coluna do *grupo do remetente* abaixo, clique o *WHITELIST,*
5. Clique o botão do *remetente adicionar* perto da metade inferior da página.
6. Entre no IP ou no hostname que você quer ao whitelist no primeiro campo.

Quando você termina adicionar entradas, clique o *botão Submit Button*. Recorde clicar as *mudanças comprometer* abotoam-se para salvar suas mudanças.

Do CLI

```
example.com> listenerconfig
Currently configured listeners:
1. InboundMail (on PublicNet, 172.19.1.80) SMTP TCP Port 25 Public
2. OutboundMail (on PrivateNet, 172.19.2.80) SMTP TCP Port 25 Private
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: InboundMail
Type: Public
Interface: PublicNet (172.19.1.80/24) TCP Port 25
Protocol: SMTP
Default Domain:
Max Concurrency: 1000 (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
LDAP: Off

Choose the operation you want to perform:
- NAME - Change the name of the listener.
- INTERFACE - Change the interface.
- 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.
[]> hostaccess
Default Policy Parameters
=========================
Allow TLS Connections: No
Allow SMTP Authentication: No
Require TLS To Offer SMTP authentication: No
Maximum Concurrency Per IP: 1,000
Maximum Message Size: 100M
Maximum Messages Per Connection: 1,000
Maximum Recipients Per Message: 1,000
Maximum Recipients Per Hour: Disabled
Use SenderBase For Flow Control: Yes
Spam Detection Enabled: Yes
Virus Detection Enabled: Yes
There are currently 4 policies defined.
There are currently 5 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.
- CLEAR - Remove all entries.
[]> edit
1. Edit Sender Group
2. Edit Policy
[1]> 1
Currently configured HAT sender groups:
1. WHITELIST (My trusted senders have no Brightmail or rate limiting)
2. BLACKLIST (Spammers are rejected)
3. SUSPECTLIST (Suspicious senders are throttled)
4. UNKNOWNLIST (Reviewed but undecided, continue normal acceptance)
5. (no name, first host = ALL) (Everyone else)
Enter the sender group number or name you wish to edit.
[]> 1

Choose the operation you want to perform:
- NEW - Add a new host.
- DELETE - Remove a host.
- MOVE - Reorder the hosts.
- POLICY - Change the policy settings and options.
- PRINT - Display the current definition.
- RENAME - Rename this sender group.
[]> new
Enter the hosts to add. CIDR addresses such as 10.1.1.0/24 are allowed. IP
address ranges such as 10.1.1.10-20 are allowed. IP subnets such as 10.2.3. are
allowed. Hostnames such as crm.example.com are allowed. Partial hostnames such
as .example.com are allowed.
Ranges of SenderBase Reputation scores such as SBRS[7.5:10.0] are allowed.
SenderBase Network Owner IDs such as SBO:12345 are allowed.
Remote blacklist queries such as dnslist[query.blacklist.example] are allowed.
Separate multiple hosts with commas
[]>
```

Recorde emitir o `comando commit` salvar suas mudanças.

Informações Relacionadas

- Cisco envia por correio eletrónico a ferramenta de segurança - Guias do utilizador final
- Suporte Técnico e Documentação - Cisco Systems