Wie Whitelist ein vertrauenswürdiger Absender?

Inhalt

Frage

Wie Whitelist ein vertrauenswürdiger Absender?

Antwort

Fügen Sie auf der Cisco E-Mail Security Appliance (ESA) der WHITELIST-Absendergruppe vertrauenswürdige Absender hinzu, da diese Absendergruppe die $TRUSTED Mail Flow-Richtlinie verwendet. Mitglieder der WHITELIST-Absendergruppe unterliegen keiner Ratenbeschränkung, und der Inhalt dieser Absender wird nicht von der Cisco IronPort AntiSpam-Engine gescannt, sondern wird weiterhin von der Sophos Anti-Virus-Software gescannt.

> **Hinweis**: In der Standardkonfiguration ist die Anti-Virus-Prüfung aktiviert, aber Anti-Spam ist deaktiviert.

Um einen Absender zu Whitelist hinzuzufügen, fügen Sie den Absender der WHITELIST-Absendergruppe in der Host Access Table (HAT) hinzu. Sie können die HAT über die GUI oder die CLI konfigurieren.

Über die Benutzeroberfläche

1. Klicken Sie auf die Registerkarte *Mail-Policys*.
2. Wählen Sie im Abschnitt "*Host Access Table*" die Option *HAT Overview (HAT-Übersicht) aus.*
3. Stellen Sie sicher, dass auf der rechten Seite Ihr *InboundMail*-Listener aktuell ausgewählt ist.
4. Klicken Sie in der Spalte *Absendergruppe* unten auf *WHITELIST,*
5. Klicken Sie auf die Schaltfläche *Absender hinzufügen* in der unteren Hälfte der Seite.
6. Geben Sie im ersten Feld die IP oder den Hostnamen ein, die bzw. der Sie Whitelist angeben möchten.

Wenn Sie alle Einträge hinzugefügt haben, klicken Sie auf die Schaltfläche *Senden*. Denken Sie

daran, auf die Schaltfläche *Änderungen bestätigen* zu klicken, um Ihre Änderungen zu speichern.

Über die 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
[]>
```

Denken Sie daran, `commit` um Ihre Änderungen zu speichern.

Zugehörige Informationen

- Cisco Email Security Appliance - Benutzerhandbücher
- Technischer Support und Dokumentation - Cisco Systems