Umgehung von Anti-Spam durch einen vertrauenswürdigen Absender zulassen

Inhalt

Einführung

In diesem Dokument werden die Details beschrieben, wie ein vertrauenswürdiger Absender die Anti-Spam-Prüfung umgehen kann, sowie die verschiedenen Methoden, die Sie auf dem sicheren E-Mail-Gateway (früher E-Mail Security Appliance genannt) verwenden können.

Hinzufügen von Absenderhostname/IP-Adresse in ALLOWED_LIST-Absendergruppe

Fügen Sie der Absendergruppe ALLOWED_LIST vertrauenswürdige Absender hinzu, da diese Absendergruppe die $TRUSTED Mail Flow-Richtlinie verwendet. Mitglieder der Absendergruppe ALLOWED_LIST unterliegen keiner Ratenbeschränkung, und der Inhalt dieser Absender wird nicht von der Anti-Spam-Engine gescannt, sondern wird weiterhin von Anti-Virus gescannt.

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

Um einem Absender die Umgehung des Anti-Spam-Scans zu ermöglichen, fügen Sie den Absender der Absendergruppe ALLOWED_LIST in der Host Access Table (HAT) hinzu. Sie können die HAT über die GUI oder die CLI konfigurieren.

Über die GUI

1. Wählen Sie die Registerkarte **Mail-Policys aus**.
2. Wählen Sie im Abschnitt **Host Access Table** (**Hostzugriffstabelle**) die Option **HAT Overview (HAT-Übersicht)**.
3. Vergewissern Sie sich, dass der **InboundMail-**Listener aktuell ausgewählt ist.
4. Wählen Sie in der Spalte **"Absendergruppe"** die Option **ALLOWED_LIST**.
5. Wählen Sie die Schaltfläche **Absender hinzufügen** in der unteren Hälfte der Seite aus.
6. Geben Sie die IP- oder Hostname ein, die im ersten Feld umgangen werden soll.

Wenn Sie alle Einträge hinzugefügt haben, wählen Sie die Schaltfläche **Senden**. Denken Sie daran, die Schaltfläche **Änderungen bestätigen** auszuwählen, 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. ALLOWED_LIST (My trusted senders have no anti-spam scanning or rate limiting)
2. BLOCKED_LIST (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 blocklist queries such as dnslist[query.blocklist.example] are allowed.
Separate multiple hosts with commas
[]>
```

Denken Sie daran, den **Commit-**Befehl auszugeben, um Ihre Änderungen zu speichern.

Überprüfen Sie die Anti-Spam- und Anti-Virus-Prüfung in der Trusted Mail Flow Policy.

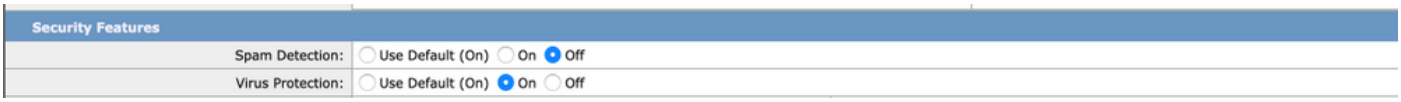
Für den vertrauenswürdigen Absender gibt es standardmäßig eine Mail Flow Policy, die als vertrauenswürdige Vorlage bezeichnet wird. Die Trusted Mail Flow Policy hat ein Connection-Verhalten von Accept (ähnlich dem Verhalten für andere Mail Flow-Richtlinien für eingehende E-Mails).

Wenn ein Absender für geschäftliche Anforderungen vertrauenswürdig ist, können wir die Anti-Spam- und Antivirus-Prüfungen für ihn deaktivieren. Dadurch wird die zusätzliche Verarbeitungslast beider Scan-Engines verringert, während sie E-Mails scannen, die nicht von vertrauenswürdigen Quellen stammen.

> **Hinweis:** Die Anti-Spam- und Anti-Virus-Engines sind deaktiviert und überspringen alle Spam- oder Virenscans für eingehende E-Mails in der ESA. Dies ist nur dann zu tun, wenn Sie absolut sicher sind, dass das Überspringen von Scans für diese vertrauenswürdigen Absender kein Risiko darstellt.

Die Option, von der aus Sie die Engines deaktivieren können, finden Sie auf der Registerkarte Sicherheitsfunktionen in Mail Flow Policies (Mail-Fluss-Richtlinien). Der Pfad für dasselbe ist **GUI > Mail Policies > Mail Flow Policies**. Klicken Sie auf die **TRUSTEDMail-Datenflussrichtlinie**, und scrollen Sie auf der nachfolgenden Seite nach unten zu **Sicherheitsfunktionen**.

Vergewissern Sie sich, dass Sie die Änderungen bestätigen, nachdem Sie die Änderungen nach Bedarf vorgenommen haben.



Hinzufügen eines vertrauenswürdigen Absenders zur Liste sicherer Absender

Endbenutzer-Sicherheitslisten und Sperrlisten werden von Endbenutzern erstellt und in einer Datenbank gespeichert, die vor dem Anti-Spam-Scannen überprüft wird. Jeder Endbenutzer kann Domänen, Subdomänen oder E-Mail-Adressen identifizieren, die er immer als Spam behandeln oder niemals als Spam behandeln möchte. Wenn eine Absenderadresse Teil einer Liste sicherer Absender ist, wird der Anti-Spam-Scan übersprungen.

Diese Konfiguration ermöglicht es dem Endbenutzer, einen Absender gemäß der Anforderung zur Freistellung der Anti-Spam-Scans zu verschlüsseln. Die Virenschutz-Prüfung und andere Scans in der E-Mail-Pipeline bleiben mit dieser Konfiguration unberührt und werden entsprechend der Konfiguration in den Mail-Policys fortgesetzt. Durch diese Konfiguration wird das Engagement des Administrators verringert, jedes Mal, wenn ein Endbenutzer Spam-Scans für einen Absender ausschließen muss.

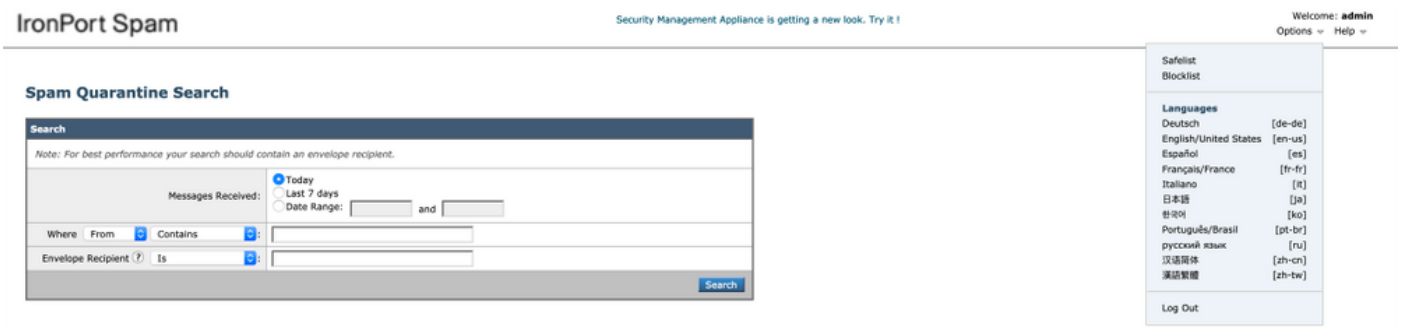
Für die Liste sicherer Absender muss der Endbenutzer-Quarantänezugriff für die Endbenutzer aktiviert sein, und die Liste sicherer Absender/Sperrliste für Endbenutzer muss aktiviert sein (sowohl in der ESA als auch in SMA). Auf diese Weise können sie auf das Spam-Quarantäne-Portal zugreifen und neben **der** Löschung/**Löschung** der unter Quarantäne stehenden E-Mails auch Absender in der Liste sicherer Absender **hinzufügen/löschen**.

Der Quarantänezugriff für Endbenutzer kann wie folgt aktiviert werden:

ESA: Navigieren Sie zu **GUI > Monitor > Spam Quarantine**. Aktivieren Sie die **Optionsschaltfläche** für den **Endbenutzer-Quarantänezugriff**. Wählen Sie die Authentifizierungsmethode für den Zugriff gemäß Anforderung aus (Keine/LDAP/SAML/IMAP oder POP). Posten Sie diese, und aktivieren Sie die Liste sicherer Absender/Sperrliste für Endbenutzer.

SMA: Navigieren Sie zu **GUI > Centralized Services > Spam Quarantine**. Aktivieren Sie die **Optionsschaltfläche** für den **Endbenutzer-Quarantänezugriff**. Wählen Sie die Authentifizierungsmethode für den Zugriff gemäß Anforderung aus (Keine/LDAP/SAML/IMAP oder POP). Posten Sie diese, und aktivieren Sie die Liste sicherer Absender/Sperrliste für Endbenutzer.

Wenn ein Endbenutzer nach der Aktivierung zum Spam Quarantine-Portal navigiert, kann er seine Liste sicherer Absender **hinzufügen/ändern**, je nach Auswahl der Dropdown-Optionen oben rechts.



Vertrauenswürdige Absender mit Richtlinien für eingehende E-Mails

Sie können in der Richtlinie für eingehende E-Mails auch einen vertrauenswürdigen Absender hinzufügen und Scans für **Antivirus/Antispam** entsprechend der Anforderungen deaktivieren. Eine neue benutzerdefinierte Mail-Richtlinie kann mit einem Namen wie **vertrauenswürdige Absender/sichere Absender** usw. erstellt werden. Anschließend können Sie dieser benutzerdefinierten Richtlinie die Absenderdetails wie Domänennamen oder Absender-E-Mail-Adressen hinzufügen.

Wenn Sie die Richtlinie nach dem erforderlichen Hinzufügen gesendet haben, können Sie auf die Spalten von **Antispam** oder **Antivirus** klicken**,** und auf der nachfolgenden Seite die Option **Disable (Deaktivieren)** auswählen.

Bei dieser Konfiguration werden die vertrauenswürdigen Absender-Domänen oder E-Mail-Adressen, die dieser Mail-Richtlinie hinzugefügt werden, von Antispam- oder Antivirus-Scans ausgenommen.

> **Hinweis:** Die Anti-Spam- und Anti-Virus-Engines sind deaktiviert und überspringen alle Spam- oder Virenscans für eingehende E-Mails in der ESA, die über diese benutzerdefinierte Mail-Richtlinie verarbeitet werden. Dies ist nur dann zu tun, wenn Sie absolut sicher sind, dass das Überspringen von Scans für diese vertrauenswürdigen Absender kein Risiko darstellt.

Die benutzerdefinierte Mail-Richtlinie kann über die **ESA-GUI > Mail-Policys > Mail-Policys für eingehende E-Mails > Richtlinie hinzufügen** erstellt werden. Geben Sie als Auswahl den Namen der Richtlinie ein, und wählen Sie dann **Benutzer hinzufügen aus**. Aktivieren Sie das Optionsfeld **Absender folgen.** Fügen Sie die erforderliche Domäne oder E-Mail-Adressen in das Feld ein, und klicken Sie auf **OK**.

Sie können die AntiSpam- und AntiSpam-Prüfung nach der Erstellung von Mail-Richtlinien deaktivieren, wenn diese den geschäftlichen Anforderungen entsprechen. Hier ein Beispiel-Screenshot:

Zugehörige Informationen

- [Cisco Email Security Appliance - Benutzerhandbücher]

- Technischer Support und Dokumentation für Cisco Systeme