Toestaan dat een Trusted Sender anti-Spam omzeilt

Inhoud

Inleiding

In dit document worden de details beschreven van het toestaan dat een vertrouwde afzender anti-Spam scannen omzeilt en ook de verschillende methoden beschreven die u voor hetzelfde kunt kiezen in de Secure Email Gateway (voorheen bekend als de e-mail security applicatie).

Toevoeging van Sender Hostname/IP Adres in ALLOWED_LIST Sender Group

Voeg zenders toe die u vertrouwt op de ALLOWED_LIST sendergroep omdat deze sendergroep het beleid van de $TRUSTED mail flow gebruikt. Leden van de zendgroep ALLOWED_LIST zijn niet onderworpen aan snelheidsbeperking, en de inhoud van die zenders wordt niet gescand door de anti-Spam motor maar wordt nog steeds gescand door het anti-virus.

> **Opmerking:** Als de standaardinstelling is, wordt het scannen tegen het virus ingeschakeld, maar anti-spam is uitgeschakeld.

Om een zender te laten voorbijgaan aan het scannen van anti-Spam, voegt u de zender toe aan het vak ALLOWED_LIST in de Host Access Table (HAT). U kunt de HAT configureren via de GUI of de CLI.

Via de GUI

1. Selecteer het tabblad **Mail Policy**.
2. Selecteer onder het gedeelte **Host Access Tabel** de optie **HAT - Overzicht**.
3. Rechts moet u ervoor zorgen dat de **inkomendeMail** luisteraar is geselecteerd.
4. Selecteer in de kolom **Sender Group** de optie **ALLOWED_LIST**.
5. Selecteer de knop **Sender toevoegen** aan de onderkant van de pagina.
6. Voer de IP- of hostnaam in die u in het eerste veld wilt laten omzeilen.

Wanneer u klaar bent met het toevoegen van items, selecteert u de knop **Indienen**. Vergeet niet

de knop **Aanpassen** om de wijzigingen op te slaan.

Van de 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
[]>
```

Vergeet niet de **opdracht** aan te geven om de wijzigingen op te slaan.

Evalueer het scannen van antispam en antivirussen in het Trusted Mail Flow-beleid

Voor de Betrouwbare zender zal er een Mail Flow Policy zijn dat standaard wordt aangeduid als een Betrouwbaar cadeau. Het Trusted Mail Flow Policy zal een Connection-gedrag van accepteren (gelijk aan het gedrag voor andere Mail Flow-beleid voor inkomende e-mails).

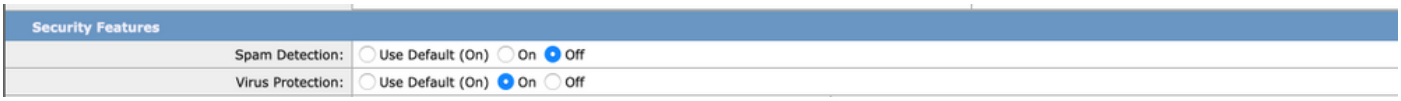
Als een afzender voor bedrijfsvereisten wordt vertrouwd, kunnen wij ervoor kiezen om de controles van het Antivirus en van het Antispam voor hen uit te schakelen. Dit vermindert de extra belasting voor de verwerking van zowel de scanmotoren als de e-mails die niet van vertrouwde bronnen afkomstig zijn.

> **Opmerking:** De anti-spam- en anti-virusmotoren uitgeschakeld zullen de scans van spam of virus voor de inkomende e-mail in het ESA overslaan. Dit moet gedaan worden, alleen als je er zeker van bent dat scans voor deze vertrouwde zenders geen risico lopen.

De optie waar u de motoren kunt uitschakelen is beschikbaar in het tabblad Security functies in het beleid voor e-mailstromen. Het pad voor hetzelfde is **GUI > Mail Policies > Mail Flow Policies**.

Klik op het **TRUSTEDM-stroombeleid** en scrollen naar **beveiligingsfuncties** op de volgende pagina.

Zorg ervoor dat u de wijzigingen doorvoert nadat u de gewenste aanpassingen hebt uitgevoerd.



Voeg een Trusted Sender toe aan Safelist

Eindgebruikersafselisten en -blokkers worden gecreëerd door eindgebruikers en opgeslagen in een database die wordt gecontroleerd voordat er wordt gescand met een anti-spam-scan. Elke eindgebruiker kan domeinen, subdomeinen of e-mailadressen identificeren die hij altijd als spam wil behandelen of nooit als spam wil behandelen. Als een senderadres deel uitmaakt van een safelist van de eindgebruiker, wordt het scannen van anti-spam overgeslagen

Deze opzet zal de eindgebruiker in staat stellen een zender veilig te stellen overeenkomstig zijn eis om de anti-spamscans vrij te stellen. Het scannen met een antivirus en andere scanners in de e-mailpijplijn worden niet aangeraakt door deze instelling. Bovendien wordt de configuratie in het Mail-beleid voortgezet. Deze instelling vermindert de betrokkenheid van de beheerder elke keer dat een eindgebruiker spam-scannen voor een zender moet vrijstellen.

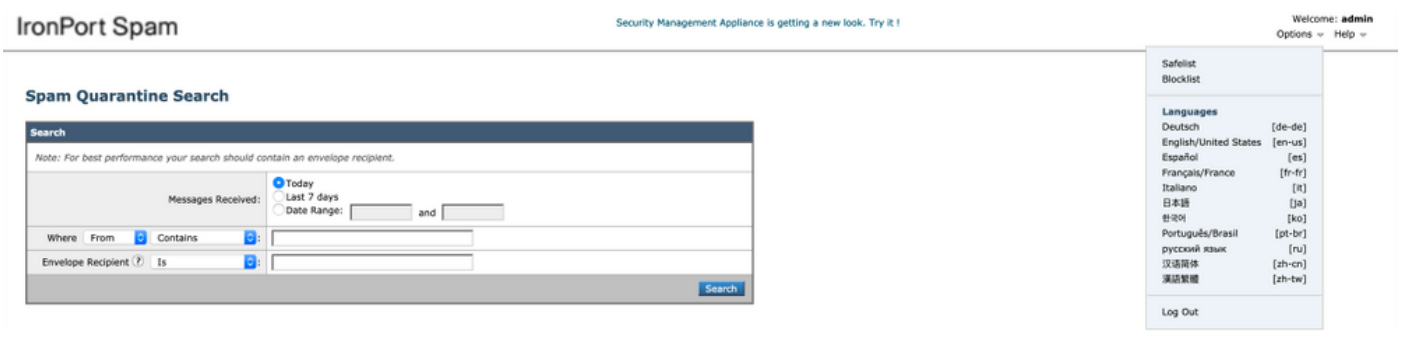
Voor de Safelist is het verplicht de eindgebruiker Quarantine-toegang beschikbaar te stellen voor de eindgebruikers en de eindgebruiker Safelist/Blocklist als ingeschakeld (zowel in ESA als SMA). Op die manier hebben ze toegang tot het Spam Quarantine-portaal en kunnen ze, naast **het** invullen**/verwijderen** van de in quarantaine geplaatste e-mails, ook zenders **toevoegen/verwijderen** in Safelist.

De toegang tot de **quarantaine** van de **eindgebruiker** kan als volgt worden ingeschakeld:

ESA: Navigeer naar **GUI > Monitor > Spam Quarantine**. Controleer de **radioknop** voor **eindgebruiker Quarantine Access**. Selecteer de verificatiemethode voor toegang volgens de vereisten (geen/LDAP/SAML/IMAP of POP). Schakel deze optie in als de eindgebruiker safelist/blocklist.

SMA: Navigeer naar **GUI > Gecentraliseerde services > Spam Quarantine**. Controleer de knop **Radio** voor **Eindgebruiker Quarantine Access**. Selecteer de verificatiemethode voor toegang volgens de vereisten (geen/LDAP/SAML/IMAP of POP). Schakel deze optie in als de eindgebruiker safelist/blocklist.

Als een eindgebruiker naar het Spam Quarantine-portaal navigeert, kunnen ze hun Safelist naar keuze **toevoegen of wijzigen** via uitrolopties rechts.



Trusted Senders met inkomend postbeleid

U kunt ook een Trusted Sender toevoegen in het inkomende e-mailbeleid en **Antivirus/Antispam-**scans uitschakelen volgens de vereisten. Een nieuw aangepast Mail-beleid kan worden gemaakt met een naam zoals **Trusted Senders/Safe Senders** enz. naar keuze en dan kunt u de afzender details zoals domeinnamen of e-mailadressen toevoegen aan dit aangepaste beleid.

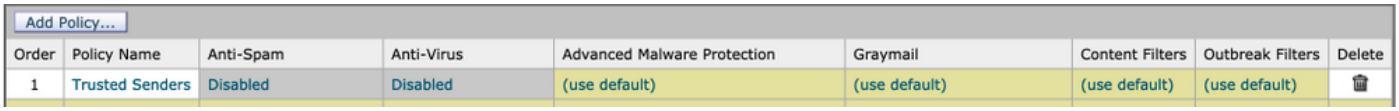
Nadat u het beleid na de gewenste toevoeging hebt ingediend, kunt u op de kolommen van **Antispam** of **Antivirus** klikken en op de volgende pagina **Uitschakelen**.

Bij deze instelling worden de vertrouwde verzenddomeinen of e-mailadressen die aan dit e-mailbeleid worden toegevoegd, vrijgesteld van Antispam- of Antivirusscans.

> **Opmerking:** De anti-spam- en anti-virusmotoren uitgeschakeld, overslaan de met Spam of Virus verband houdende scans voor het binnenkomende e-mailadres in het ESR dat via dit aangepast postbeleid wordt verwerkt. Dit moet gedaan worden, alleen als je er zeker van bent dat scans voor deze vertrouwde zenders geen risico lopen.

Het aangepast Mail-beleid kan worden gegenereerd door **ESA GUI > Mail-beleid > Inkomend Mail-beleid > Toevoegen**. Voer de beleidsnaam per keuze in en selecteer **Gebruiker toevoegen**. Controleer in het keuzerondje op **Volgende Senders.** Voeg het vereiste domein of e-mailadressen toe in het vak en klik op **OK**.

Post-mail beleidscreatie, kunt u selecteren om de Antivirus- en Antispamscans uit te schakelen volgens de zakelijke vereisten. Hier is een voorbeeld van een screenshot:



Gerelateerde informatie

- Cisco e-mail security applicatie – eindgebruikershandleiding
- Technische ondersteuning en documentatie – Cisco Systems