

Flexibele Mail Policy matching en functies voor ESR en CES configureren

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Configureren](#)

[Configuraties](#)

[Via de GUI:](#)

[Van de CLI: \(versie 9.7.x - 11.0.x\)](#)

[Verifiëren](#)

[Optie 1](#)

[Optie 2](#)

[Problemen oplossen](#)

[Gerelateerde informatie](#)

Inleiding

Dit document beschrijft hoe u Flexibel Mail Policy matching kunt configureren op Cisco e-mail security applicatie (ESA) en Cloud Email Security (CES).

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Begrijpen van het postbeleid en het gedrag van de ESA/CES.
- Gebruik van de CLI.
- De verschillen tussen een zender en de Koppen: Van, antwoorden en sturen.

Gebruikte componenten

De informatie in dit document is gebaseerd op Cisco ESA/CES op AsyncOS.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Achtergrondinformatie

Flexibel Mail Policy Match is in Cisco ESA/CES-apparaten geïntroduceerd op versies voorafgaand aan 11.1.x releases. Hiermee kunnen beheerders e-mails aan een beleid aanpassen dat is gebaseerd op:

- Zender en alle ontvangers.
- Elke zender naar de specifieke ontvanger(s).
- Zender en specifieke ontvanger(s).

Ontvankelijk adres is gelijk aan het adres van de ontvanger.

Overeenkomsten voor verzendadres in deze volgorde:

Opmerking: De matchingsvolgorde kan worden **ingesteld in de versies AsyncOS 11.1.x**.

1. Envelope Sender (RFC821 MAIL VAN adres).
2. Adres in RFC8222: kopbal.
3. Adres in de RFC822 Reply-To header.

Gebruikerspatronen worden beoordeeld als een top-down mode, eerste match-wins.

Het bepalen van uw beleid is van cruciaal belang om ervoor te zorgen dat de boodschappen worden afgestemd op een beleid dat aan uw vereisten voldoet.

Als de e-mail een afzender en meerdere ontvangers bevat die meer dan één beleid zouden passen, wordt het bericht verdeeld van één Bericht ID (MID) in een extra MID van het overeenkomende beleid.

Configureren

Configuraties

U kunt als volgt een flexibele beleidsmatch op uw ESA/CES configureren:

Via de GUI:

1. Navigeren in om **Mail-beleid**.
2. Klik op **inkomende e-mailbeleid** of **uitgaand postbeleid** om het beleid te maken.
3. Klik op **Beleid toevoegen....**
4. Voer een betekenisvolle beleidsnaam in en beveel deze aan uw vereisten (houd rekening met het top-down first match wins gedrag).
5. Klik op **Gebruiker toevoegen...**
6. Configureer de zender, de ontvanger om dit beleid te matchen.

7. Aan de ontvangende kant van het venster, controleer of u voor dit beleid **EN** of **OF** gedrag vereist.

8. Klik op **OK** om uw wijzigingen voort te zetten, in te sturen en **aan te geven**.

Opmerking: **De volgende ontvangers** worden **niet** gebruikt om specifieke ontvangers uit te sluiten van het domein dat in het veld **volgende ontvangers** is gedefinieerd.

Add User

Any Sender

Following Senders

Following Senders are Not

Email Address:

matthew@abc.com

(e.g. user@example.com, user@, @example.com, @.example.com)

LDAP Group:

There are no LDAP group queries defined.

Any Recipient

Following Recipients

externaluser@xyz.com, externaluser@gmail.com

(e.g. user@example.com, user@, @example.com, @.example.com)

LDAP Group:

There are no LDAP group queries defined.

Following Recipients are Not

Email Address:

Van de CLI: (versie 9.7.x - 11.0.x)

1. Geef de opdracht **beleidsconfiguratie** uit.
2. Voer **1** of **2** in om uw inkomende e-mailbeleid of een uitgaand postbeleid te configureren.
3. Geef de opdracht **"nieuw"** uit om een nieuw e-mailbeleid te maken.
4. Volg de aanwijzingen om gebruikers toe te voegen om dit beleid aan te passen.
5. Volg de aanwijzingen om de configuratie van de beveiligingsscanners te voltooien.
6. Nadat dit is voltooid, **kunt u** uw wijzigingen indienen en **doorgeven**.

```
C680.esa.lab> policyconfig
```

```
Would you like to configure Incoming or Outgoing Mail Policies?
```

```
1. Incoming
2. Outgoing
[1]> 1
```

Opmerking: De volgorde voor verzenden kan worden gewijzigd in versie AsyncOS 11.1.x GUI in het tabblad **Mail** of in CLI.

Van CLI opdracht **beleidsconfiguratie** introduceert een extra optie voor beheerders om de wijziging te starten.

Standaard wordt de prioriteit gegeven aan de **achtergrondinformatie**. De bewerkbare waarden in versie 11.1.x zijn Kop-zender, kop: **Van**, **antwoord op** en **zender**.

Dit is het voorbeeld van Default prioriteit:

```
vesa2.lab> policyconfig
```

Would you like to configure Incoming Mail Policy or Outgoing Mail Policies or Match Headers Priority?

1. Incoming Mail Policies
 2. Outgoing Mail Policies
 3. Match Headers Priority
- ```
[1]> 3
```

Match Headers Priority Configuration

Priority: Headers:

-----

P1 Envelope Sender

Choose the operation you want to perform:

- ADD - Add match priority for headers
- EDIT - Edit an existing match priority for headers
- REMOVE - Remove an existing match priority for headers

## Verifiëren

Er zijn twee beschikbare opties beschikbaar om het beleid van de ESA/CES te toetsen.

### Optie 1

1. Navigeer naar de **GUI > Inkomend/uitgaand postbeleid**.
2. In het **vakje Beleid zoeken**, voer het gebruikersadres in en klik op de radioknop voor de respectieve **Afzender** of de **Ontvanger** partij.
3. Klik op **Beleid zoeken**.

De voorbeelduitvoer wordt in de afbeelding weergegeven:

The screenshot shows a 'Find Policies' search interface. The 'Email Address' field contains 'matt@lee.com'. The 'Recipient' radio button is selected. The 'Find Policies' button is visible. The results section shows: 'Email Address "Sender: matt@lee.com" is defined in the following policies: matt\_two, Default Policy (all users)'. Below this is a table titled 'Policies matching "matt@lee.com"'. The table has columns for Order, Policy Name, Anti-Spam, Anti-Virus, Advanced Malware Protection, Graymail, Content Filters, Outbreak Filters, and Delete. The first row shows 'matt\_two' with various settings like '(use default)'. The second row shows 'Default Policy' with more detailed settings like 'IronPort Anti-Spam Positive: Deliver'.

| Order | Policy Name    | Anti-Spam                                                     | Anti-Virus                                                                   | Advanced Malware Protection                                                                                                                                                          | Graymail      | Content Filters        | Outbreak Filters | Delete |
|-------|----------------|---------------------------------------------------------------|------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------|------------------------|------------------|--------|
| 2     | matt_two       | (use default)                                                 | (use default)                                                                | (use default)                                                                                                                                                                        | (use default) | (use default)          | (use default)    |        |
|       | Default Policy | IronPort Anti-Spam<br>Positive: Deliver<br>Suspected: Deliver | Sophos<br>Encrypted: Deliver<br>Unscannable: Deliver<br>Virus Positive: Drop | File Reputation<br>Malware File: Drop<br>Pending Analysis: Deliver<br>Unscannable - Message Error: Deliver<br>Unscannable - Rate Limit: Deliver<br>Unscannable - AMP Service Not ... | Not Available | envelope_copy_quaranty | Disabled         |        |

### Optie 2

1. Navigeren in naar de **GUI > Systeembeheer > Overtrekken**.
2. Voer in de informatie op het gereedschap Trace in onder de **Informatie over de omtrek**, de gegevens van de afzender/ontvanger in om de overeenkomst te controleren.

3. Klik op **Start tracering**.

4. Scrollt naar **Mail Policy Processing** om het overeenkomende beleid te controleren. De voorbeelduitvoer wordt in de afbeelding weergegeven:

| Message Definition                                      |                                                                                                                                                          |
|---------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Sender Information</b>                               |                                                                                                                                                          |
| Source IP Address:                                      | <input type="text" value="10.66.71.10"/>                                                                                                                 |
| Fully Qualified Domain Name:                            | <input type="text"/><br><i>If left blank, a reverse DNS lookup will be performed on the source IP.</i>                                                   |
| Trace Behavior on:                                      | <input type="text" value="InOutListener"/>                                                                                                               |
| Domain Name to be passed to HELO/EHLO (optional):       | <input type="text" value="EHLO"/>                                                                                                                        |
| SMTP Authentication Username (optional):                | <input type="text"/>                                                                                                                                     |
| SenderBase Network Owner ID:                            | <input checked="" type="radio"/> Lookup network owner ID associated with source IP<br><input type="radio"/> Use: <input type="text"/>                    |
| SenderBase Reputation Score (SBRs):                     | <input checked="" type="radio"/> Lookup SBRs associated with source IP<br><input type="radio"/> Use: <input type="text"/>                                |
| <b>Envelope Information</b>                             |                                                                                                                                                          |
| Envelope Sender:                                        | <input type="text" value="matt@lee.com"/>                                                                                                                |
| Envelope Recipients (separated by commas):              | <input type="text" value="matthew@cisco.com"/>                                                                                                           |
| <b>Message Body</b>                                     |                                                                                                                                                          |
| Upload Message Body:                                    | <input type="button" value="Browse..."/> No file selected.                                                                                               |
| Paste Message Body:<br><i>(If no file is uploaded.)</i> | <pre>From: matt@lee.com To: matthew@cisco.com Subject: Body is required for Trace to show X-Headers: Inserted at the top  This is the body portion</pre> |

|                                                                     |                   |
|---------------------------------------------------------------------|-------------------|
| <b>Mail Policy Processing: Inbound (matched on policy matt_two)</b> |                   |
| Message going to:                                                   | matthew@cisco.com |

## Problemen oplossen

Er is momenteel geen specifieke troubleshooting-informatie beschikbaar voor deze configuratie.

## Gerelateerde informatie

- [Cisco e-mail security applicatie - eindgebruikershandleidingen](#)
- [Technische ondersteuning en documentatie – Cisco Systems](#)

- Wat is de spreiding van berichten?