

Configuration de la fonction de correspondance de stratégie de messagerie flexible sur ESA et CES

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Informations générales](#)

[Configuration](#)

[Configurations](#)

[À partir de la GUI :](#)

[À partir de l'interface de ligne de commande : \(version 9.7.x - 11.0.x\)](#)

[Vérification](#)

[Option 1](#)

[Option 2](#)

[Dépannage](#)

[Informations connexes](#)

Introduction

Ce document décrit comment configurer la correspondance de stratégie de messagerie flexible sur l'apppliance de sécurité de la messagerie Cisco (ESA) et la sécurité de la messagerie cloud (CES).

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Compréhension des politiques de messagerie et de son comportement sur l'ESA/CES.
- Utilisation de l'interface de ligne de commande.
- Différences entre un expéditeur d'enveloppe et les en-têtes : De, Réponse et Expéditeur.

Components Used

Les informations de ce document sont basées sur Cisco ESA/CES sur AsyncOS.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is

live, make sure that you understand the potential impact of any command.

Informations générales

La fonctionnalité Flexible Mail Policy Match a été introduite dans les périphériques Cisco ESA/CES sur les versions antérieures à la version 11.1.x. Cela permet aux administrateurs de faire correspondre les e-mails à une stratégie basée sur :

- Expéditeur et tous les destinataires.
- Tout expéditeur vers un ou plusieurs destinataires spécifiques.
- Expéditeur et destinataire(s) spécifique(s).

L'adresse du destinataire correspond à l'adresse du destinataire du message.

L'adresse de l'expéditeur correspond dans cet ordre :

Note: L'ordre correspondant est **configurable dans les versions d'AsyncOS 11.1.x.**

1. Enveloppe Sender (RFC821 MAIL FROM adresse).
2. Adresse trouvée dans le document RFC822 De : Header (En-tête) .
3. Adresse trouvée dans l'en-tête de réponse RFC822.

Les correspondances utilisateur sont évaluées de manière descendante, la première correspondance gagne.

L'ordre de vos stratégies est essentiel pour s'assurer que les messages correspondent à une stratégie en fonction de vos besoins.

Si l'e-mail contient un expéditeur et plusieurs destinataires qui correspondent à plusieurs stratégies, le message est fractionné d'un ID de message (MID) à un MID supplémentaire de la stratégie correspondante.

Configuration

Configurations

Pour configurer une correspondance de stratégie flexible sur votre ESA/CES :

À partir de la GUI :

1. Accéder à **Politiques de messagerie**.
2. Cliquez sur **Stratégies de messagerie entrante** ou **Stratégies de messagerie sortante** pour créer la stratégie.
3. Cliquez sur **Ajouter une stratégie...**
4. Entrez un nom de stratégie significatif, ordonnez-le à vos besoins (en gardant à l'esprit le comportement de la première correspondance descendante gagnant).

5. Cliquez sur **Ajouter un utilisateur...**
6. Configurez l'expéditeur et le destinataire pour qu'ils correspondent à cette stratégie.
7. Du côté destinataire du volet, vérifiez si vous avez besoin du comportement **AND** ou **OR** pour cette stratégie.
8. Cliquez sur **OK** pour continuer, envoyer et **valider** vos modifications.

Note: Les destinataires suivants ne sont pas utilisés pour exclure des destinataires spécifiques du domaine défini dans le champ **Destinataires suivants**.

À partir de l'interface de ligne de commande : (version 9.7.x - 11.0.x)

1. Émettez la commande **policy config**.
2. Entrez **1** ou **2** pour configurer vos stratégies de messagerie entrante ou sortante.
3. Exécutez la commande « **new** » pour créer une nouvelle stratégie de messagerie.
4. Suivez les invites pour ajouter des utilisateurs correspondant à cette stratégie.
5. Suivez les instructions pour terminer la configuration des analyseurs de sécurité des stratégies.
6. Une fois terminé, envoyez et **confirmez** vos modifications.

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

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

```
1. Incoming
```

```
2. Outgoing
```

```
[1]> 1
```

Remarque : l'ordre de correspondance de l'expéditeur peut être modifié dans la version de l'interface utilisateur graphique AsyncOS 11.1.x dans l'onglet **Politiques de messagerie** ou CLI.

À partir de la commande CLI **policy config** introduit une option supplémentaire permettant aux administrateurs de commencer la modification.

Par défaut, la priorité est celle qui est indiquée ci-dessus dans **Informations générales**. Les valeurs modifiables dans la version 11.1.x sont Expéditeur du message, En-têtes : **De, Réponse et Expéditeur**.

Voici l'exemple de priorité par défaut :

```
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

Vérification

Deux options sont disponibles pour vérifier le comportement de correspondance de stratégie sur le ESA/CES.

Option 1

1. Accédez à l'**interface utilisateur graphique > Politiques de messagerie entrante/sortante**.
2. Dans la **zone Rechercher des stratégies**, entrez l'adresse de l'utilisateur et cliquez sur la case d'option correspondant à l'**expéditeur** ou au **destinataire** correspondant.
3. Cliquez sur **Rechercher des stratégies**.

L'exemple de résultat est affiché dans l'image :

Find Policies

Email Address: Recipient Sender [Find Policies](#)

Results: Email Address "Sender: matt@lee.com" is defined in the following policies:

- matt_two
- Default Policy (all users)

Policies matching "matt@lee.com"

[Add Policy...](#) [Show All Policies](#)

| 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 Positive: Deliver Suspected: Deliver | Sophos Encrypted: Deliver Unscannable: Deliver Virus Positive: Drop | File Reputation Malware File: Drop Pending Analysis: Deliver Unscannable - Message Error: Deliver Unscannable - Rate Limit: Deliver Unscannable - AMP Service Not | Not Available | envelope_copy_quaranty | Disabled | |

Option 2

1. Accédez à la **GUI > Administration système > Trace**.
2. Entrez dans les détails de l'outil Trace, sous **Informations sur l'enveloppe**, les détails de l'expéditeur/du destinataire pour vérifier la correspondance.
3. Cliquez sur **Démarrer la trace**.
4. Faites défiler jusqu'à **Traitement de la stratégie de messagerie** pour vérifier la stratégie correspondante.

L'exemple de résultat est affiché dans l'image :

| Message Definition | |
|---|--|
| Sender Information | |
| Source IP Address: | <input type="text" value="10.66.71.10"/> |
| Fully Qualified Domain Name: | <input type="text"/> <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 <input type="radio"/> Use: <input type="text"/> |
| SenderBase Reputation Score (SBRs): | <input checked="" type="radio"/> Lookup SBRs associated with source IP <input type="radio"/> Use: <input type="text"/> |
| Envelope Information | |
| Envelope Sender: | <input type="text" value="matt@lee.com"/> |
| Envelope Recipients (separated by commas): | <input type="text" value="matthew@cisco.com"/> |
| Message Body | |
| Upload Message Body: | <input type="button" value="Browse..."/> No file selected. |
| Paste Message Body: <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> |

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

Dépannage

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.

Informations connexes

- [Cisco Email Security Appliance - Guides de l'utilisateur final](#)
- [Support et documentation techniques - Cisco Systems](#)
- [Qu'est-ce que la division des messages ?](#)