

Configuración de la Función Flexible Mail Policy Match en ESA y CES

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Configurar](#)

[Configuraciones](#)

[Desde la GUI:](#)

[Desde la CLI: \(versión 9.7.x - 11.0.x\)](#)

[Verificación](#)

[Opción 1](#)

[Opción 2](#)

[Troubleshoot](#)

[Información Relacionada](#)

Introducción

Este documento describe cómo configurar Flexible Mail Policy Match en Cisco Email Security Appliance (ESA) y Cloud Email Security (CES).

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Comprensión de las políticas de correo y su comportamiento en el ESA/CES.
- Uso de la CLI.
- Las diferencias entre un remitente de sobre y los encabezados: De, Responder a y Enviador.

Componentes Utilizados

La información de este documento se basa en Cisco ESA/CES en 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.

Antecedentes

Flexible Mail Policy Match se introdujo en los dispositivos Cisco ESA/CES en las versiones anteriores a la versión 11.1.x. Esto permite a los administradores adaptar los correos electrónicos a una política basada en:

- Remitente y cualquier destinatario.
- Cualquier remitente a destinatarios específicos.
- Remitente y destinatarios específicos.

La dirección del destinatario coincide con la dirección del destinatario del sobre.

La dirección del remitente coincide en este orden:

Nota: El orden correspondiente se **puede configurar en las versiones 11.1.x de AsyncOS.**

1. Remitente de sobre (dirección RFC821 MAIL FROM).
2. Dirección encontrada en RFC822 Desde: encabezado.
3. Dirección encontrada en el encabezado de respuesta RFC822.

Las coincidencias de usuario se evalúan de forma descendente, y las primeras ganan.

El orden de sus políticas es fundamental para garantizar que los mensajes se corresponden con una política según sus requisitos.

Si el correo electrónico contiene un remitente y varios destinatarios que coincidirían con más de una política, el mensaje se divide de una ID de mensaje (MID) a una MID adicional de la política coincidente.

Configurar

Configuraciones

Para configurar la coincidencia de política flexible en su ESA/CES:

Desde la GUI:

1. Vaya a **Políticas de correo**.
2. Haga clic en **Políticas de correo entrante** o **Políticas de correo saliente** para crear la política.
3. Haga clic en **Agregar política...**
4. Introduzca un nombre de directiva significativo, ordene según sus requisitos (teniendo en cuenta el comportamiento de la primera coincidencia descendente gana).
5. Haga clic en **Agregar usuario...**
6. Configure el remitente, el destinatario para que coincida con esta política.

7. En el lado del destinatario del panel, verifique si requiere el comportamiento **AND** o **OR** para esta política.

8. Haga clic en **Aceptar** para continuar, enviar y **confirmar** los cambios.

Nota: Los siguientes destinatarios no se utilizan para excluir destinatarios específicos del dominio definido en el campo **Destinatarios siguientes**.

Desde la CLI: (versión 9.7.x - 11.0.x)

1. Ejecute el comando **policy config**.
2. Ingrese **1** o **2** para configurar sus políticas de correo entrante o las políticas de correo saliente.
3. Ejecute el comando **"new"** para crear una nueva política de correo.
4. Siga las indicaciones para agregar usuarios que coincidan con esta política.
5. Siga las indicaciones para completar la configuración de los escáneres de seguridad de políticas.
6. Una vez completados, envíe y **confirme** los cambios.

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

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

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

**Nota:** El orden de coincidencia de remitentes se puede modificar en la versión AsyncOS 11.1.x GUI en la pestaña **Políticas de correo** o CLI.

Desde el comando CLI **policy config** introduce una opción adicional para que los administradores inicien el cambio.

De forma predeterminada, la prioridad es la que se proporciona anteriormente en **Información general**. Los valores editables de la versión 11.1.x son Remitente de sobre, encabezados: **Desde**,

## Responder a y Enviador.

Este es el ejemplo de Prioridad predeterminada:

```
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

## Verificación

Hay dos opciones disponibles para verificar el comportamiento de coincidencia de políticas en ESA/CES.

### Opción 1

1. Vaya a la GUI > Políticas de correo entrante/saliente.
2. En el cuadro **Buscar políticas**, introduzca la dirección de usuario y haga clic en el botón de opción correspondiente a la coincidencia de **remite**nte o destinatario correspondiente.
3. Haga clic en **Buscar políticas**.

La salida de ejemplo se muestra en la imagen:

The screenshot shows a web interface for finding policies. The 'Find Policies' section has an 'Email Address' field with 'matt@lee.com' and radio buttons for 'Recipient' and 'Sender' (selected). A 'Find Policies' button is present. Below, the 'Results' section states: 'Email Address "Sender: matt@lee.com" is defined in the following policies: matt\_two, Default Policy (all users)'. The second part of the screenshot shows 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 protection settings. The second row shows 'Default Policy' with more detailed settings.

| 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 ...<br>... | Not Available | envelope_copy_quaranty | Disabled         |        |

### Opción 2

1. Vaya a la GUI > Administración del sistema > Seguimiento.

2. Ingrese en los detalles de la herramienta Seguimiento, bajo **Información del sobre**, ingrese los detalles del remitente/destinatario para verificar la coincidencia.

3. Haga clic en **Iniciar seguimiento**.

4. Desplácese hacia abajo hasta **Mail Policy Processing** para verificar la política coincidente.

La salida de ejemplo se muestra en la imagen:

| Message Definition                                              |                                                                                                                                                          |
|-----------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------|
| Sender Information                                              |                                                                                                                                                          |
| Source IP Address:                                              | <input type="text" value="10.66.71.10"/>                                                                                                                 |
| Fully Qualified Domain Name:                                    | <input type="text"/><br><small>If left blank, a reverse DNS lookup will be performed on the source IP.</small>                                           |
| 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"/>                                |
| 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:<br><small>(If no file is uploaded.)</small> | <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:

## Troubleshoot

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.

## Información Relacionada

- [Dispositivo de seguridad Cisco Email Security Appliance - Guías de usuario final](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)
- [¿Qué es la fragmentación de mensajes?](#)