

在ESA和CES上配置灵活邮件策略匹配功能

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[背景信息](#)

[配置](#)

[配置](#)

[从 GUI :](#)

[从 CLI: \(版本9.7.x - 11.0.x \)](#)

[验证](#)

[第 1 项](#)

[第 2 项](#)

[故障排除](#)

[相关信息](#)

简介

本文档介绍如何在思科邮件安全设备(ESA)和云邮件安全(CES)上配置灵活邮件策略匹配。

先决条件

要求

Cisco 建议您了解以下主题：

- 了解邮件策略及其在ESA/CES上的行为。
- CLI的使用。
- 信封发件人和信头之间的区别：发件人、回复和发件人。

使用的组件

本文档中的信息基于AsyncOS上的思科ESA/CES。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

背景信息

在11.1.x版本之前的版本中，Cisco ESA/CES设备引入了灵活邮件策略匹配。这允许管理员根据以下任一项将电子邮件与策略相匹配：

- 发件人和任何收件人。
- 特定收件人的任何发件人。
- 发件人和特定收件人。

收件人地址与信封收件人地址匹配。

发件人地址按以下顺序匹配：

注意：匹配顺序在AsyncOS 11.1.x版本中可配置。

1. 信封发件人 (RFC821 MAIL FROM地址)。
2. 在RFC822中找到的地址：标题。
3. 在RFC822回复报头中找到的地址。

用户匹配按自上而下的方式计算，第一次匹配获胜。

策略的排序对于确保邮件与策略匹配符合您的要求至关重要。

如果电子邮件包含一个发件人和多个与多个策略匹配的收件人，则邮件会从一个邮件ID(MID)拆分到匹配策略的另一个MID。

配置

配置

要在ESA/CES上配置灵活的策略匹配，请执行以下操作：

从 GUI：

1. 导航至 **邮件策略**。
2. 单击“**传入邮件策略**”或“**传出邮件策略**”创建策略。
3. 单击 **添加策略.....**
4. 输入有意义的策略名称，根据您的要求对其进行排序（请记住自上而下的首次匹配获胜行为）。
5. 单击“**Add User... (添加用户.....)**”
6. 配置发件人和收件人以匹配此策略。
7. 在窗格的收件人端，验证是否需要此策略的**AND或OR**行为。
8. 单击**OK**继续，提交并**提交更改**。

注意：“以下收件人不是”用于从“以下收件人”字段中定义的域中排除特定收件人。

从CLI: (版本9.7.x - 11.0.x)

1. 发出命令**policyconfig**。
2. 输入**1**或**2**以配置传入邮件策略或传出邮件策略。
3. 发出命令“**new**”以创建新邮件策略。
4. 按照提示添加用户以匹配此策略。
5. 按照提示完成策略安全扫描程序配置。
6. 完成后，提交并**提交更改**。

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

Would you like to configure Incoming or Outgoing Mail Policies?

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

注意：在AsyncOS 11.1.x GUI版本的“邮件策略”(Mail Policies)选项卡或CLI中，可以修改发件人匹配顺序。

从CLI命令**policyconfig** 引入了管理员开始更改的附加选项。

默认情况下，优先级如上“背景信息”下所述。版本11.1.x中的可编辑值为 信封发件人，信头：**发件人、回复和发件人**。

以下是默认优先级的示例：

```
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

验证

两个可用选项可用于验证ESA/CES上的策略匹配行为。

第 1 项

1. 导航至GUI > Incoming/Outgoing Mail Policies。
2. 在“查找策略”框中，输入用户地址，然后单击相应发件人或收件人匹配项的单选按钮。
3. 单击“查找策略”。

示例输出如图所示：

The screenshot shows the 'Find Policies' interface. At the top, there is a search bar with 'Email Address: matt@lee.com' and radio buttons for 'Recipient' and 'Sender' (selected). A 'Find Policies' button is to the right. Below the search bar, the results are displayed: 'Results: 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. 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 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	

第 2 项

1. 导航至 GUI > System Administration > Trace。
2. 在“跟踪”工具的详细信息中，在“信封信息”(Envelope Information)下，输入“发件人/收件人”(Sender/Recipient)详细信息以验证匹配项。
3. 单击“Start Trace(开始跟踪)”。
4. 向下滚动到“邮件策略处理”，以验证策略是否匹配。

示例输出如图所示：

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

故障排除

目前没有针对此配置的故障排除信息。

相关信息

- [思科邮件安全设备 — 最终用户指南](#)
- [技术支持和文档 - Cisco Systems](#)
- [什么是消息拆分？](#)