

ESAおよびCESでの柔軟なメールポリシー照合機能の設定

内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[設定](#)

[設定](#)

[GUI で次の手順を実行します。](#)

[CLI から、\(バージョン9.7.x ~ 11.0.x\)](#)

[確認](#)

[オプション 1](#)

[オプション 2](#)

[トラブルシューティング](#)

[関連情報](#)

概要

このドキュメントでは、Cisco Eメールセキュリティアプライアンス(ESA)およびクラウドEメールセキュリティ(CES)で柔軟なメールポリシーの一致を設定する方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- メールポリシーとそのESA/CESでの動作について理解する。
- CLIの使用。
- エンベロープ送信者とヘッダーの違い：送信者、返信先、送信者。

使用するコンポーネント

このドキュメントの情報は、AsyncOS上のCisco ESA/CESに基づくものです。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期(デフォルト)設定の状態から起動しています。対象のネットワークが稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

背景説明

Flexible Mail Policy Matchは、11.1.xリリースより前のバージョンのCisco ESA/CESデバイスに導入されました。これにより、管理者は次のいずれかに基づいて電子メールをポリシーに照合できます。

- 送信者およびすべての受信者。
- 特定の受信者に対するすべての送信者。
- 送信者と特定の受信者。

受信者のアドレスがエンベロープ受信者のアドレスと一致します。

送信者アドレスが次の順序で一致します。

注：AsyncOS 11.1.xリリースでは、照合順序を設定できます。

1. エンベロープ送信者 (RFC821 MAIL FROMアドレス)。
2. RFC822で見つかったアドレス：ヘッダーが含まれています。
3. RFC822 Reply-Toヘッダーで見つかったアドレス。

ユーザの一致はトップダウン方式として評価され、最初の一致が優先されます。

ポリシーの順序は、メッセージが要件に対するポリシーと照合されるようにするために重要です。

電子メールに複数のポリシーに一致する送信者と複数の受信者が含まれている場合、メッセージは1つのメッセージID(MID)から一致するポリシーの追加MIDに分割されます。

設定

設定

ESA/CESで柔軟なポリシー一致を設定するには、次の手順を実行します。

GUI で次の手順を実行します。

1. **に移動 メールポリシー。**
2. **[受信メールポリシー]または[送信メールポリシー]をクリックして、ポリシーを作成します。**
3. **クリック ポリシーの追加...**
4. **意味のあるポリシー名を入力し、要件に合わせて順序を付けます (トップダウンの最初の一致の動作に注意してください)。**
5. **[Add User...]をクリックします。**
6. **このポリシーに一致するように送信者と受信者を設定します。**

7. ペインの受信側で、このポリシーに対してANDまたはORの動作が必要かどうかを確認します。

8. [OK]をクリックして、変更を続行し、送信して**確定**してください。

注：次の受信者は[次の受信者]フィールドで定義されたドメインから特定の受信者を除外する場合は使用されません。

CLI から、(バージョン9.7.x ~ 11.0.x)

1. policyconfigコマンドを発行します。
2. 1または2を入力して、受信メールポリシーまたは送信メールポリシーを設定します。
3. コマンド「new」を発行して、新しいメールポリシーを作成します。
4. プロンプトに従って、このポリシーに一致するユーザを追加します。
5. 指示に従って、ポリシーセキュリティスキャナの設定を完了します。
6. 完了したら、変更を送信してコミットしてください。

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

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

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

**注：**バージョンAsyncOS 11.1.x GUIの[Mail Policies]タブまたはCLIでは、送信者一致の順序を変更できます。

CLIコマンドpolicyconfigでは、管理者が変更を開始するための追加オプションが導入されています。

デフォルトでは、優先順位は上記の「背景情報」の下に示されています。バージョン11.1.xの編集可能な値は次のとおりです エンベロープ送信者、ヘッダー：From、Reply-ToおよびSender。

次に、デフォルトのプライオリティの例を示します。

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

## 確認

ESA/CESのポリシー一致動作を確認するには、2つのオプションがあります。

### オプション 1

1. [GUI] > [Incoming/Outgoing Mail Policies]に移動します。
2. [ポリシーの検索]ボックスにユーザーアドレスを入力し、それぞれの送信者または受信者の一致に対応するラジオボタンをクリックします。
3. [ポリシーの検索]をクリックします。

出力例を次の図に示します。

Find Policies

Email Address:   Recipient  Sender

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

- matt\_two
- Default Policy (all users)

Policies matching "matt@lee.com"

| 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         |        |

### オプション 2

1. 次の場所に移動します。 [GUI] > [System Administration] > [Trace]を選択します。
2. トレースツールの詳細を入力し、[Envelope Information]の下に[Sender/Recipient]の詳細を入力して、一致を確認します。

3. [トレースの開始]をクリックします。

4. [メールポリシーの処理]まで下にスクロールし、一致するポリシーを確認します。出力例を次の図に示します。

| 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><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"/>                                |
| <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><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: matthew@cisco.com

## トラブルシューティング

現在、この設定に関する特定のトラブルシューティング情報はありません。

## 関連情報

- [Cisco E メール セキュリティ アプライアンス : エンドユーザ ガイド](#)
- [テクニカル サポートとドキュメント - Cisco Systems](#)

- メッセージ分割とは何ですか。