

檢測ESA上的欺騙性電子郵件並建立例外

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[什麼是電子郵件欺騙](#)

[如何檢測偽裝電子郵件](#)

[如何允許特定發件人的欺騙](#)

[設定](#)

[建立字典](#)

[建立郵件篩選器](#)

[向MY_TRUSTED_SPOOF_HOSTS新增欺騙異常](#)

[驗證](#)

[驗證偽裝郵件是否已隔離](#)

[驗證是否正在傳送欺騙異常消息](#)

[相關資訊](#)

簡介

本文檔介紹如何控制思科ESA上的電子郵件欺騙，以及如何為允許傳送欺詐電子郵件的使用者建立例外。

必要條件

需求

您的郵件安全裝置(ESA)必須處理傳入和傳出郵件，並使用RELAYLIST的標準配置將郵件標籤為傳出。


採用元件

使用的特定元件包括：

- 字典：用於儲存所有內部域。
- 郵件過濾器：用於處理檢測偽裝電子郵件的邏輯並插入內容過濾器可以操作的標頭。
- 策略隔離：用於臨時儲存偽造電子郵件的副本。考慮將已釋放郵件的IP地址新增到MY_TRUSTED_SPOOF_HOSTS，以防止來自此發件人的未來郵件進入策略隔離區。
- MY_TRUSTED_SPOOF_HOSTS：引用您的受信任傳送IP地址的清單。將發件人的IP地址新增到此清單中會跳過隔離區並允許發件人進行欺騙。您可以將受信任的發件人放在

MY_TRUSTED_SPOOF_HOSTS發件人組中，以便不會隔離來自這些發件人的假郵件。

- RELAYLIST：對允許中繼或傳送出站郵件的IP地址進行身份驗證的清單。如果通過此發件人組傳送電子郵件，則假設郵件不是偽裝郵件。

 註：如果呼叫某個發件人組的對象與MY_TRUSTED_SPOOF_HOSTS或RELAYLIST不同，則必須使用相應的發件人組名稱修改篩選器。此外，如果您有多個監聽程式，則您還有多個MY_TRUSTED_SPOOF_HOSTS。

本文檔中的資訊基於任何AsyncOS版本的ESA。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

Cisco ESA上預設啟用欺騙。允許其他域代表您傳送郵件有幾個正當的理由。一個常見的示例是，ESA管理員想要通過在傳送欺騙郵件之前隔離這些郵件來控制欺騙郵件。

要採取特定操作，如隔離偽造的電子郵件，您必須首先檢測偽造的電子郵件。

什麼是電子郵件欺騙

郵件欺騙是指偽造郵件頭以使郵件看起來來自某人或其他實際來源。電子郵件欺騙是網路釣魚和垃圾郵件活動中使用的一項策略，因為人們更可能在認為電子郵件是由合法來源傳送時開啟該電子郵件。

如何檢測偽裝電子郵件

您想要篩選具有信封發件人(Mail-From)和友好發件人(From)信頭的郵件，該信封發件人在電子郵件地址中包含您自己的某個傳入域。

如何允許特定發件人的欺騙

實施本文中提供的郵件過濾器時，偽裝郵件會使用標頭進行標籤，內容過濾器則用於對標頭執行操作。要新增例外，只需將發件人IP新增到MY_TRUSTED_SPOOF_HOSTS中。

設定

建立發件人組

1. 從ESA GUI導航至Mail Policies > HAT Overview
2. 按一下 新增。
3. 在「名稱」欄位中，指定MY_TRUSTED_SPOOF_HOSTS。
4. 在「訂單」欄位中，指定1。
5. 對於Policy欄位，指定ACCEPTED。
6. 按一下Submit儲存更改。

7. 最後，按一下Commit Changes以儲存配置

Sender Group Settings	
Name:	MY_TRUSTED_SPOOF_HOSTS
Order:	1
Comment:	
Policy:	ACCEPTED
SBRS (Optional):	<input type="checkbox"/> to <input type="checkbox"/> <input type="checkbox"/> Include SBRS Scores of "None" <i>Recommended for suspected senders only.</i>
DNS Lists (Optional): ?	<input type="text"/> <i>(e.g. 'query.blacklist.example, query.blacklist2.example')</i>
Connecting Host DNS Verification:	<input type="checkbox"/> Connecting host PTR record does not exist in DNS. <input type="checkbox"/> Connecting host PTR record lookup fails due to temporary DNS failure. <input type="checkbox"/> Connecting host reverse DNS lookup (PTR) does not match the forward DNS lookup (A).

Buttons: Cancel, Submit, Submit and Add Senders >>

範例：

建立字典

為要在ESA上禁用欺騙的所有域建立詞典：

1. 從ESA GUI導航到Mail Policies > Dictionaries。
2. 按一下 新增字典。
3. 在「名稱」欄位中，指定「VALID_INTERNAL_DOMAINS」，以使複製和貼上消息過濾器不會出錯。
4. 在add terms下，新增要檢測欺騙的所有域。 在域前輸入帶有@符號的域，然後按一下add。
5. 確保未選中匹配整字覈取方塊。
6. 按一下Submit儲存字典更改。
7. 最後，按一下Commit Changes以儲存配置。

範例：

Add Dictionary

Dictionary Properties	
Name:	<input type="text" value="VALID_INTERNAL_DOMAINS"/>
Advanced Matching:	<input type="checkbox"/> Match whole words <input type="checkbox"/> Case Sensitive
Smart Identifiers: ?	Match specific patterns such as social security numbers and credit card numbers.

Dictionary		Number of terms: 1	
Add Terms:	Term	Weight	Delete
<input type="text" value="@example.com"/> <small>Separate multiple entries with line breaks.</small> Weight: ? <input type="text" value="1"/> <input type="button" value="Add"/>	@mydomain.com	1	<input type="button" value="Delete"/>

建立郵件篩選器

接下來，您需要建立郵件過濾器，以便利用剛建立的詞典「VALID_INTERNAL_DOMAINS」：


1. 連線到ESA的命令列介面(CLI)。
2. 運行命令Filters。
3. 運行命令New以建立新的消息過濾器。
4. 複製並貼上此過濾器示例，根據需要編輯實際的發件人組名稱：

```
mark_spoofed_messages:
if(
    (mail-from-dictionary-match("VALID_INTERNAL_DOMAINS", 1))
    OR (header-dictionary-match("VALID_INTERNAL_DOMAINS","From", 1)))
AND ((sendergroup != "RELAYLIST")
AND (sendergroup != "MY_TRUSTED_SPOOF_HOSTS"))
)
{
insert-header("X-Spoof", "");
}
```

5. 返回主CLI提示符並運行Commit以儲存配置。
6. 導航到GUI > Mail Policies > Incoming Content Filters
7. 建立對欺騙標頭X-Spoof執行操作的傳入內容過濾器：

1. 新增其他標頭

2. 報頭名稱：X-Spoof
3. 標頭存在單選按鈕
4. 新增操作：duplicate-quarantine(Policy)。

 注意：此處顯示的「重複郵件」功能會保留郵件的副本，並繼續向收件人傳送原始郵件。

Add Action

Quarantine

Encrypt on Delivery

Strip Attachment by Content

Strip Attachment by File Info

Strip Attachment With Macro

URL Category

URL Reputation

Add Disclaimer Text

Bypass Outbreak Filter Scanning

Bypass DKIM Signing

Send Copy (Bcc:)

Notify

Quarantine Help

Flags the message to be held in one of the system quarantine areas.

Send message to quarantine:

Duplicate message

Send a copy of the message to the specified quarantine, and continue processing the original message. Any additional actions will apply to the original message.

Add Incoming Content Filter

Content Filter Settings

Name:	<input type="text" value="Spoof"/>
Currently Used by Policies:	No policies currently use this rule.
Editable by (Rcles):	No custom user roles available
Description:	<input style="width: 100%; height: 20px;" type="text"/>
Order:	<input type="text" value="26"/> (of 26)

Conditions

<input type="button" value="Add Condition..."/>			
Order	Condition	Rule	Delete
1	Other Header	header("X-Spoof")	<input type="button" value="Delete"/>

Actions

<input type="button" value="Add Action..."/>			
Order	Action	Rule	Delete
1	Quarantine	duplicate-quarantine("Policy")	<input type="button" value="Delete"/>

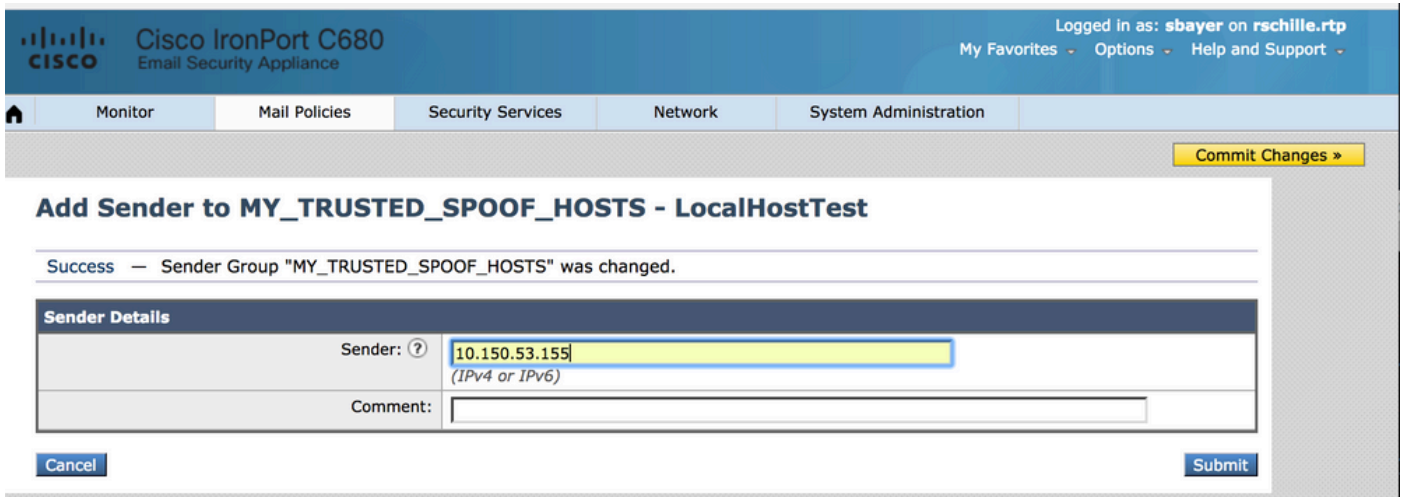
8. 在GUI > Mail Policies > Incoming Mail Policies處，將內容過濾器連結到傳入郵件策略。
9. 提交和提交更改。

向MY_TRUSTED_SPOOF_HOSTS新增欺騙異常

最後，您需要將欺騙異常（IP地址或主機名）新增到MY_TRUSTED_SPOOF_HOSTS發件人組。

1. 通過Web GUI導航：郵件策略> HAT概述
2. 按一下並開啟MY_TRUSTED_SPOOF_HOSTS發件人組。
3. 按一下Add Sender..以新增IP地址、範圍、主機名或部分主機名。
4. 按一下Submit儲存發件人更改。
5. 最後，按一下Commit Changes以儲存配置。

範例：



驗證

驗證偽裝郵件是否已隔離

傳送測試消息，指定其中一個域作為信封發件人。通過對郵件執行郵件跟蹤來驗證過濾器是否按預期工作。預期的結果是郵件被隔離，因為您尚未為允許欺騙的發件人建立任何例外。

<#root>

```
Thu Apr 23 07:09:53 2015 Info: MID 102 ICID 9 RID 0 To: <xxxx_xxxx@domain.com>
Thu Apr 23 07:10:07 2015 Info: MID 102 Subject 'test1'
Thu Apr 23 07:10:07 2015 Info: MID 102 ready 177 bytes from <user_1@example.com>
Thu Apr 23 07:10:07 2015 Info: MID 102 matched all recipients for per-recipient policy DEFAULT in the i
Thu Apr 23 07:10:11 2015 Info: MID 102 interim verdict using engine: CASE spam negative
Thu Apr 23 07:10:11 2015 Info: MID 102 using engine: CASE spam negative
Thu Apr 23 07:10:11 2015 Info: MID 102 interim AV verdict using Sophos CLEAN
Thu Apr 23 07:10:11 2015 Info: MID 102 antivirus negative

Thu Apr 23 07:10:12 2015 Info: MID 102 quarantined to "Policy" (message filter:quarantine_spoofed_messa

Thu Apr 23 07:10:12 2015 Info: Message finished MID 102 done
```

驗證是否正在傳送欺騙異常消息

欺騙例外發件人是上面過濾器中引用的發件人組中的IP地址。

之所以引用RELAYLIST，是因為它被ESA用於傳送出站郵件。由RELAYLIST傳送的郵件通常是出站郵件，如果不包括此項，則會產生誤報，或者由上面的過濾器隔離出站郵件。

新增到MY_TRUSTED_SPOOF_HOSTS的欺騙異常IP地址的郵件跟蹤示例。預期的操作是傳送，而不是隔離。（此IP允許偽裝）。

<#root>

```
Thu Apr 23 07:25:57 2015 Info: Start MID 108 ICID 11
Thu Apr 23 07:25:57 2015 Info: MID 108 ICID 11 From: <user_1@example.com>
Thu Apr 23 07:26:02 2015 Info: MID 108 ICID 11 RID 0 To: <user_xxxx@domain.com>
Thu Apr 23 07:26:10 2015 Info: MID 108 Subject 'test2'
Thu Apr 23 07:26:10 2015 Info: MID 108 ready 163 bytes from <user_1@example.com>
Thu Apr 23 07:26:10 2015 Info: MID 108 matched all recipients for per-recipient policy DEFAULT in the i
Thu Apr 23 07:26:10 2015 Info: MID 108 interim AV verdict using Sophos CLEAN
Thu Apr 23 07:26:10 2015 Info: MID 108 antivirus negative
Thu Apr 23 07:26:10 2015 Info: MID 108 queued for delivery
Thu Apr 23 07:26:10 2015 Info: Delivery start DCID 16 MID 108 to RID [0]
Thu Apr 23 07:26:11 2015 Info: Message done DCID 16 MID 108 to RID [0]
Thu Apr 23 07:26:11 2015 Info: MID 108 RID [0] Response '2.0.0 t58EVG9N031598
```

Message accepted for delivery'

Thu Apr 23 07:26:11 2015 Info: Message finished MID 108 done

相關資訊

- [ESA詐騙郵件過濾](#)
- [使用發件人驗證進行欺騙保護](#)

思科內部資訊

有一個功能請求，要求將RAT公開到郵件過濾器/內容過濾器，以簡化此過程：

思科錯誤ID [CSCus49018](#) — 增強型：將收件人訪問表(RAT)暴露到過濾條件

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。