

ESA のスプーフィングされた電子メール メッセージを検出し、スプーフィングすることができる送信側用の例外を作成して下さい

目次

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[メールは何をスプーフィングしていますか。](#)

[スプーフィングされたメールを検出する方法か。](#)

[特定の送信側用のスプーフィングすることを割り当てる方法か。](#)

[設定](#)

[メッセージ フィルターを作成して下さい](#)

[MY_TRUSTED_SPOOF_HOSTS にスプーフィング例外を追加して下さい](#)

[確認](#)

[スプーフィングされたメッセージが検疫されていることを確認して下さい](#)

[スプーフィング例外がメッセージ提供されていることを確認して下さい](#)

[関連情報](#)

概要

この資料に Cisco E メール セキュリティ アプライアンス (ESA) でスプーフィングするメールを制御する方法をおよびスプーフィングされたメールを送信 することができるユーザ向けの例外を作成する方法を記述されています。

前提条件

要件

ESA は両方の着信 および 発信メールを処理し発信ようにメッセージにフラグを付けるのに RELAYLIST の標準の設定を使用する必要があります。

使用するコンポーネント

この 文書に記載されている 情報は AsyncOS あらゆるバージョンの ESA に基づいています。本書の情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。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。稼働中のネットワークで作業を行う場合、コマンドの影響について十分に理解したうえで作業してください。

使用する特定のコンポーネントは下記のものを含んでいます:

- 辞書: 内部ドメインをすべて保存するのに使用しました。
- メッセージ フィルター: スプーフィングされたメールを検出し、コンテンツ フィルターが機能できるヘッダを挿入することのロジックを処理するのに使用しました。
- ポリシー検疫: スプーフィングされたメールの duplicartes を一時的に保存するのに使用しました。この送信側から未来のメッセージを防ぐためにポリシーの入力から MY_TRUSTED_SPOOF_HOSTS にリリースされたメッセージの IP アドレスを追加する Consider 検疫します。
- MY_TRUSTED_SPOOF_HOSTS: 信頼された送信 IP アドレスを参照するためのリスト。このリストへ送信側の IP アドレスを追加することは検疫をスキップし、送信側がスプーフィングすることを可能にします。これらの送信側からのスプーフィングされたメッセージが検疫されないように MY_TRUSTED_SPOOF_HOSTS 送信側グループに信頼された送信側を置いています。
- RELAYLIST: 中継で送ることができるリストして下さいまたは送信メールを送信して下さい 認証 IP アドレスのために。メールがこの送信側グループによって渡されれば想定はメッセージがスプーフィングされたメッセージではないことです。

注: 送信側グループが MY_TRUSTED_SPOOF_HOSTS か RELAYLIST と別の何かと呼出される場合対応する送信側グループ名を用いるフィルタを修正しなければなりません。また複数のリスナーがあれば、また複数の MY_TRUSTED_SPOOF_HOSTS があるかもしれません。

背景説明

スプーフィングは Cisco ESA でデフォルトでイネーブルになっています。複数の、他のドメインが為を送出するようにするための正当な理由あります。1つの一般的な例はスプーフィングされたメールの制御にスプーフィングされたメッセージの検疫によって、ESA 管理者提供される前にほしい場合もあります。

スプーフィングされたメールの検疫のような特定の処置をとるために、最初にスプーフィングされたメールを検出して下さい。

メールは何をスプーフィングしていますか。

スプーフィングするメールはメッセージが誰かからまたはどこかに実原始以外起きるために現れるようにメールヘッダの偽作です。スプーフィングするメールは phishing で使用される作戦であり、それを考えるときメールを開く個人が可能性が高いのでスパムキャンペーンは正規のソースによって送信されました。

スプーフィングされたメールを検出する方法か。

および (から) e メールアドレスであなた自身の着信ドメインの1つが含まれているヘッダ「から」友好的エンベロープ送信側 (Mail-From) があるメッセージをフィルタリングしたいと思います。

特定の送信側用のスプーフィングすることを割り当てる方法か。

この技術情報の中で提供されるメッセージ フィルターを実装するときスプーフィングされたメッセージはヘッダとタグ付けされ、コンテンツ フィルタがヘッダの処置をとるのに使用されています。例外を追加するために、MY_TRUSTED_SPOOF_HOSTS に送信側 IP を単に追加して下さい

い。

設定

Sendergroup を作成して下さい

1. ESA GUI から、ポリシー > 帽子概要を郵送するためにナビゲートして下さい
2. [Add] をクリックします。
3. "Name " フィールドで MY_TRUSTED_SPOOF_HOSTS を規定して下さい
4. 「順序」フィールドで 1 つを規定して下さい
5. 「ポリシー」フィールドに関しては、受け入れられる規定して下さい
6. 変更を保存するために『SUBMIT』 をクリックして下さい。
7. 最終的には、設定を保存するために保存します変更をクリックして下さい

例
:

Add Sender Group to LocalHostTest

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 >>

辞書を作成して下さい

ESA のためのスプーフィングを無効に してほしいすべてのドメインのための辞書を作成して下さい:

1. ESA GUI から、ポリシー > 辞書を郵送するためにナビゲートして下さい。
2. 辞書を『Add』 をクリックして下さい。
3. "Name " フィールドでは規定 しまメッセージ フィルターをエラーなしにコピー アンド ペーストします作るために「VALID_INTERNAL_DOMAINS」を。
4. の下で「用語」を、追加しますスプーフィングを検出してほしいすべてのドメインを追加して下さい。 ドメインを付加する@サインが付いているドメインを入力し、『Add』 をクリックして下さい。
5. 「全ワード」チェックボックスをチェックを外される一致確認して下さい。
6. 辞書変更を保存するために『SUBMIT』 をクリックして下さい。
7. 最終的には、設定を保存するために保存します変更をクリックして下さい

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

メッセージ フィルターを作成して下さい

次に、「VALID_INTERNAL_DOMAINS」ちょうど作成された辞書にてこ入れするためにメッセージ フィルターを作成する必要があります:

1. ESA の Command Line Interface (CLI) への接続応答。
2. コマンド フィルターを実行して下さい。
3. 新しい新しいメッセージ フィルターを作成するためにコマンドを実行して下さい。
4. 作るもし必要なら次のフィルタ例を編集します実際の送信側グループ名のためにコピーアンドペーストして下さい:

```
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. 主要な CLI プロンプトに戻れば設定を保存するために実行は託します。
6. へのナビゲート GUI > メール ポリシー > 着信コンテンツ フィルター
7. 着信コンテンツ フィルタを作成して下さいスプーフィング ヘッダ X スプーフィングの処置をとる: 操作を追加して下さい: 重複検疫 (「ポリシー」) 。

注: ここに示されている重複したメッセージ機能はメッセージのコピーを保存し、受信者に元のメッセージを送信し続けます。

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: Policy

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:	Spoof
Currently Used by Policies:	No policies currently use this rule.
Editable by (Roles):	No custom user roles available
Description:	
Order:	26 (of 26)

Conditions			
Add Condition...			
Order	Condition	Rule	Delete
1	Other Header	header("X-Spoof")	

Actions			
Add Action...			
Order	Action	Rule	Delete
1	Quarantine	duplicate-quarantine("Policy")	

Cancel

Submit

8. 着信メール ポリシーへのリンク内容フィルタの GUI > メール Policies > 着信メール ポリシー
9. 変更を送信して確定します。

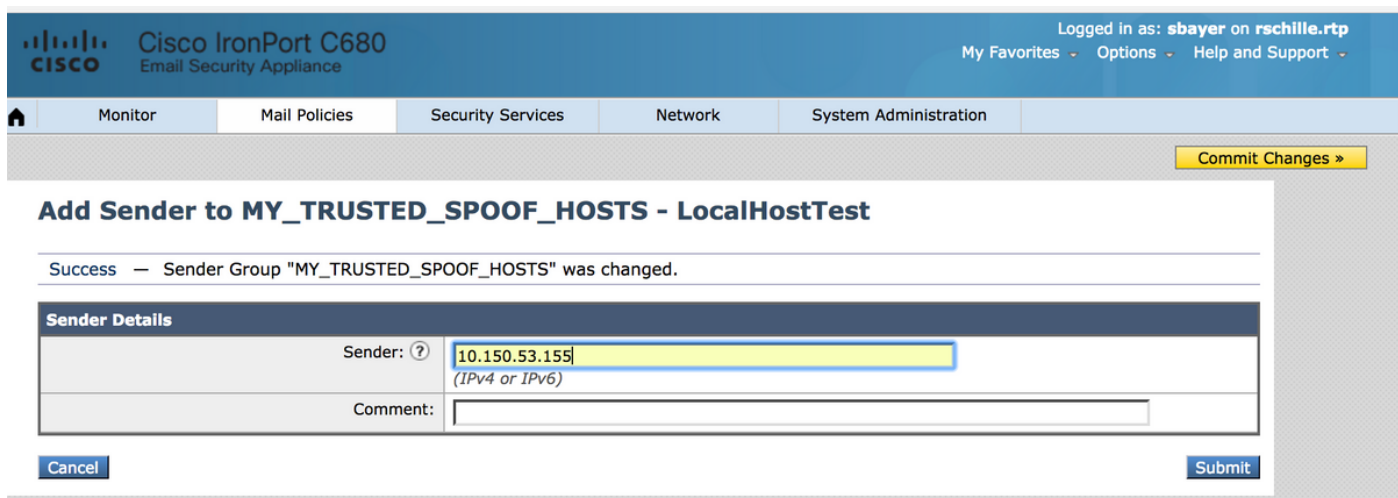
MY_TRUSTED_SPOOF_HOSTS にスプーフィング例外を追加して下さい

最終的には、MY_TRUSTED_SPOOF_HOSTS sendergroup にスプーフィング例外を (IP アドレスかホスト名) 追加する必要があります。

1. Web GUI でのナビゲート: [Mail Policies] > [HAT Overview]
2. MY_TRUSTED_SPOOF_HOSTS 送信側グループをクリックし、開いて下さい。
3. クリックして下さい「追加します送信側を...」 IP アドレス、範囲、ホスト名、または部分的なホスト名を追加するため。

4. 送信側変更を保存するために『SUBMIT』をクリックして下さい。
5. 最終的には、設定を保存するために**保存します変更**をクリックして下さい。

例：



Cisco IronPort C680
Email Security Appliance

Logged in as: sbayer on rschille.rtp
My Favorites - Options - Help and Support -

Monitor Mail Policies Security Services Network System Administration

Commit Changes >

Add Sender to MY_TRUSTED_SPOOF_HOSTS - LocalHostTest

Success - Sender Group "MY_TRUSTED_SPOOF_HOSTS" was changed.

Sender Details	
Sender: ?	10.150.53.155 <small>(IPv4 or IPv6)</small>
Comment:	

Cancel Submit

確認

スプーフィングされたメッセージが検疫されていることを確認して下さい

エンベロープ送信側としてドメインの1つを規定するテストメッセージを送信して下さい。フィルタを予想通りはたらいっていますそのメッセージのメッセージトラックの実行によって検証して下さい。期待された結果はスプーフィングすることができるそれらの送信側用の例外をけれども作成しなかったのでメッセージが検疫されて得ることです。

```
Thu Apr 23 07:09:53 2015 Info: MID 102 ICID 9 RID 0 To: <test_user@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 inbound table
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_messages)
Thu Apr 23 07:10:12 2015 Info: Message finished MID 102 done
```

スプーフィング例外がメッセージ提供されていることを確認して下さい

「スプーフィング例外」送信側は上でフィルタで参照される送信側グループのIPアドレスです。

RELAYLISTは送信メールを送信することをESAによって使用するので参照されます。RELAYLISTによって送信されるメッセージはこれを含む一般的に送信メール、ない作成します上でフィルタによって検疫されるfalse positive、か送信メッセージをであり。

MY_TRUSTED_SPOOF_HOSTSに追加された「スプーフィング例外」IPアドレスのメッセージトラッキング例。期待された操作は渡し、検疫しませんあります。(このIPはスプーフィングすることができます)。

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: <test_user@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 inbound table
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

関連情報

- [ESA のスプーフィングメールのフィルタリング](#)
- [送信者検証を使用したスプーフィング保護](#)