ESAでのスプーフィングされた電子メールメッセージの検出と例外の作成

内容

はじめに

このドキュメントでは、Cisco ESAで電子メールのスプーフィングを制御する方法と、スプーフィングされた電子メールの送信を許可するユーザの例外を作成する方法について説明します。

前提条件

要件

Eメールセキュリティアプライアンス(ESA)は受信メールと送信メールの両方を処理し、RELAYLISTの標準設定を使用してメッセージに発信フラグを設定する必要があります。

使用するコンポーネント

使用される具体的なコンポーネントは次のとおりです。

- ディクショナリ：すべての内部ドメインを格納するために使用されます。
- メッセージフィルタ：スプーフィングされた電子メールを検出し、コンテンツフィルタが動作できるヘッダーを挿入するロジックを処理するために使用されます。
- ポリシー隔離：スプーフィングされた電子メールの複製を一時的に保存するために使用され

ます。解放されたメッセージのIPアドレスをMY_TRUSTED_SPOOF_HOSTSに追加して、この送信者からの今後のメッセージがポリシー隔離に入らないようにすることを検討してください。
- MY_TRUSTED_SPOOF_HOSTS：信頼できる送信IPアドレスを参照するリスト。このリストに送信者のIPアドレスを追加すると、検疫がスキップされ、送信者がスプーフィングできるようになります。信頼できる送信者をMY_TRUSTED_SPOOF_HOSTS送信者グループに配置すると、これらの送信者からのスプーフィングされたメッセージが隔離されなくなります。
- RELAYLIST：リレーを許可されているIPアドレスを認証するリスト、または送信Eメールを送信するリスト。この送信者グループを介して電子メールが配信される場合、メッセージはスプーフィングされたメッセージではないと想定されます。

注：送信者グループがMY_TRUSTED_SPOOF_HOSTSまたはRELAYLIST以外の名前で呼び出されている場合は、対応する送信者グループ名でフィルタを変更する必要があります。また、複数のリスナーがある場合は、複数のMY_TRUSTED_SPOOF_HOSTSも存在します。

このドキュメントの情報は、すべてのAsyncOSバージョンのESA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、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

Cisco ESAでは、スプーフィングはデフォルトで有効になっています。自分の代わりに他のドメインからの送信を許可する理由はいくつかあります。 一般的な例として、ESA管理者は、スプーフィングされたメッセージが配信される前にそれらを隔離することで、スプーフィングされた電子メールを制御したいと考えています。

スプーフィングされた電子メールを隔離するなどの特定のアクションを実行するには、まずスプーフィングされた電子メールを検出する必要があります。

電子メールスプーフィングとは

電子メールのスプーフィングは、電子メールヘッダーの偽造であり、メッセージが実際の送信元とは別のユーザまたは場所から発信されたように見えます。電子メールのスプーフィングは、フィッシングキャンペーンやスパムキャンペーンで使用される手法です。これは、電子メールが正当な送信元から送信されたと思った場合に、その電子メールを開く可能性が高いためです。

スプーフィングされた電子メールの検出方法

エンベロープ送信者(Mail-From)ヘッダーとfriendly from(From)ヘッダーを持ち、電子メールアドレスに独自の着信ドメインが1つ含まれるメッセージをフィルタリングする。

特定の送信者のスプーフィングを許可する方法

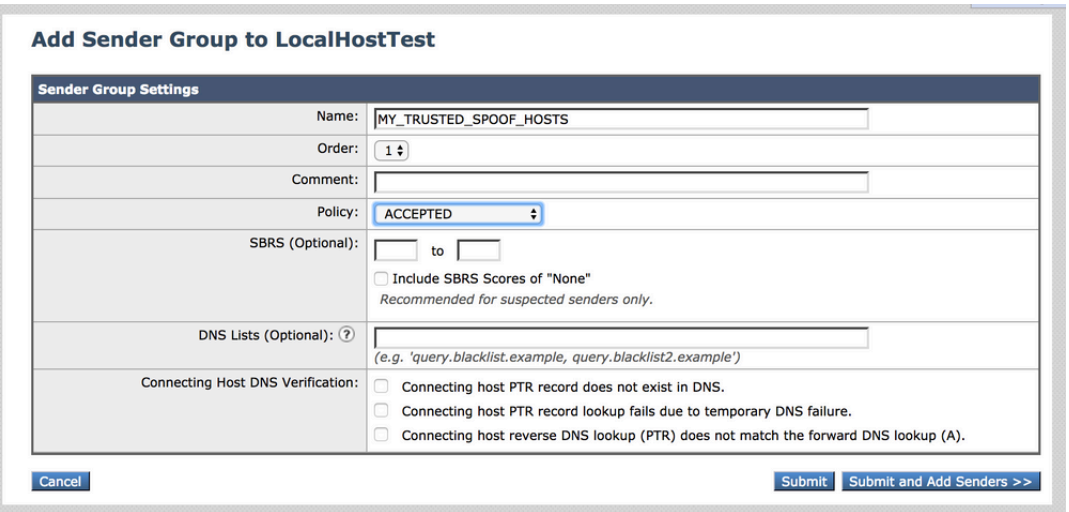
この記事に記載されているメッセージフィルタを実装すると、スプーフィングされたメッセージにはヘッダーのタグが付けられ、コンテンツフィルタを使用してヘッダーに対するアクションが実行されます。例外を追加するには、単に送信元IPをMY_TRUSTED_SPOOF_HOSTSに追加します。

設定

送信者グループの作成

1. ESA GUIから、Mail Policies > HAT Overviewの順に移動します。
2. クリック 追加.
3. NameフィールドにMY_TRUSTED_SPOOF_HOSTSと指定します。
4. Orderフィールドに1を指定します。
5. PolicyフィールドにACCEPTEDと指定します。
6. [Submit] をクリックして変更を保存します。
7. 最後に、Commit Changesをクリックして設定を保存します

以下に例を挙げます。

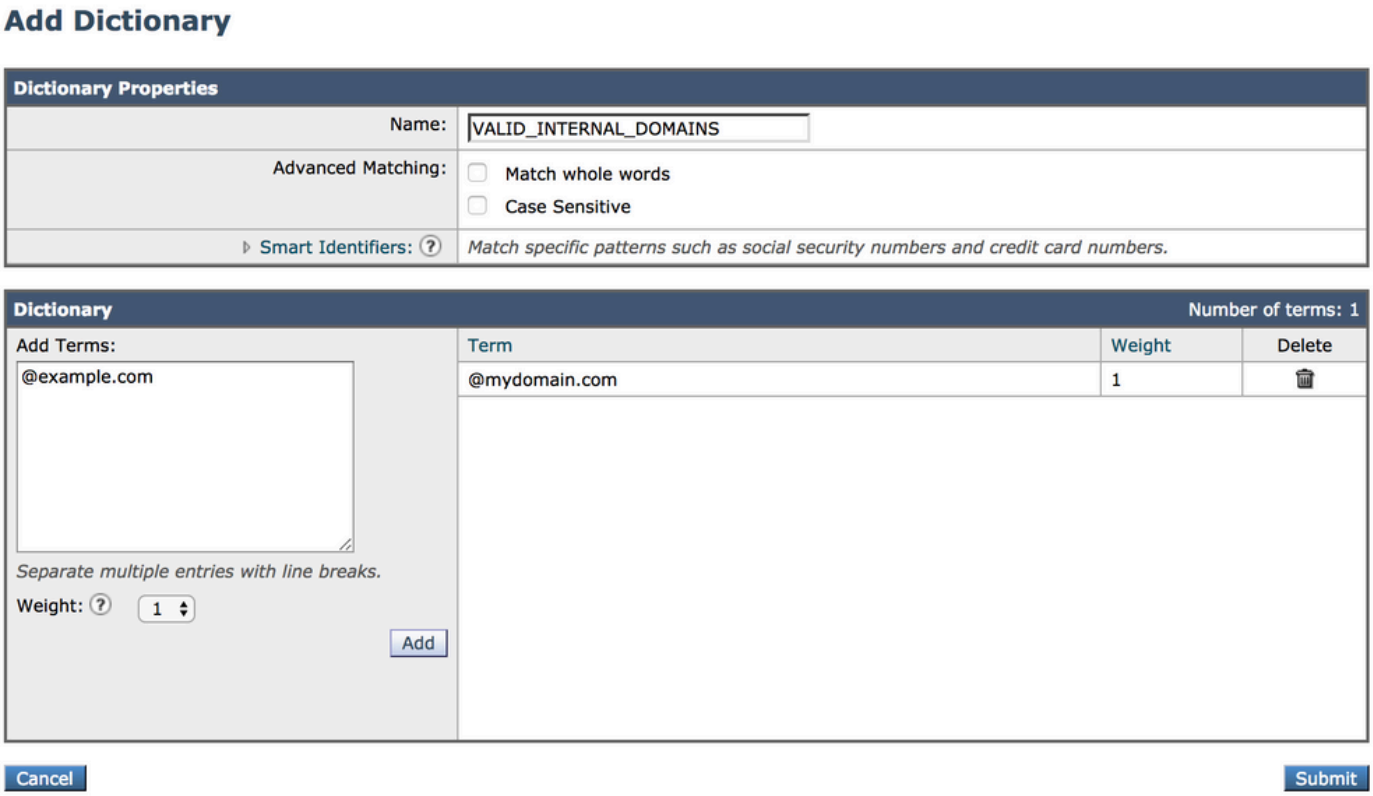


辞書の作成

ESAでスプーフィングを無効にするすべてのドメインのディクショナリを作成します。

1. ESAのGUIで、Mail Policies > Dictionariesの順に移動します。
2. クリック 辞書の追加
3. 「名前」フィールドに「VALID_INTERNAL_DOMAINS」を指定して、メッセージフィルタをコピーして貼り付けると、エラーが発生しなくなります。
4. [add terms]で、スプーフィングを検出するすべてのドメインを追加します。 ドメインの前に@記号(@)を付けてドメインを入力し、addをクリックします。
5. match whole wordsチェックボックスがオフになっていることを確認します。
6. Submitをクリックして、ディクショナリの変更を保存します。
7. 最後に、Commit Changesをクリックして設定を保存します。

以下に例を挙げます。



メッセージフィルタの作成

次に、作成したディクショナリ「VALID_INTERNAL_DOMAINS」を利用するために、メッセージフィルタを作成する必要があります。

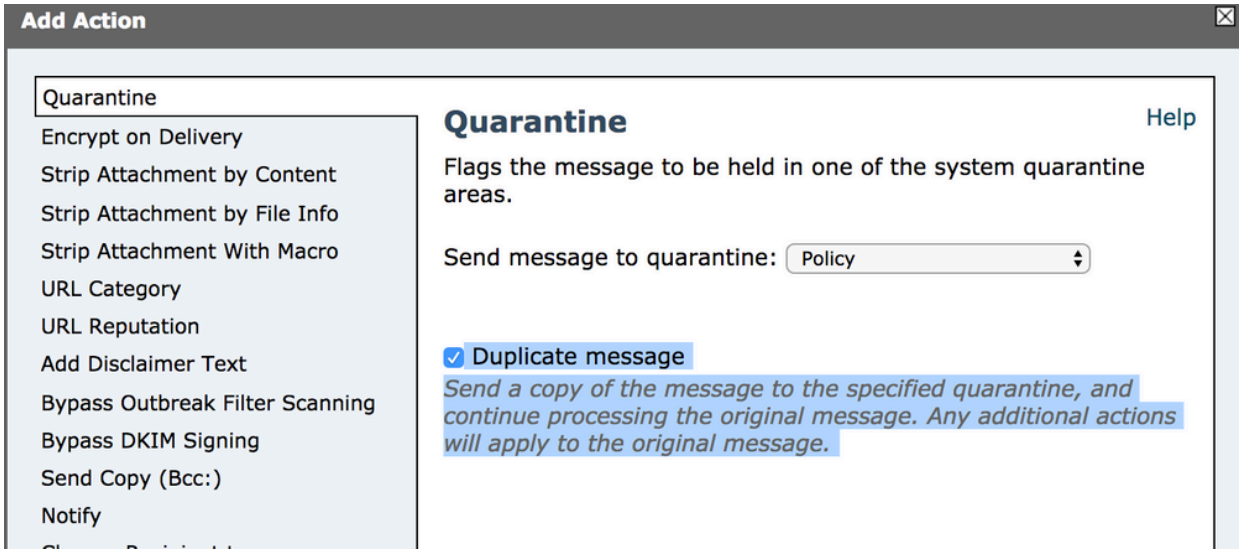
1. ESAのコマンドラインインターフェイス(CLI)に接続します。
2. Filtersコマンドを実行します。
3. Newコマンドを実行して、新しいメッセージフィルタを作成します。
4. このフィルタ例をコピーして貼り付け、必要に応じて実際の送信者グループ名を編集します。

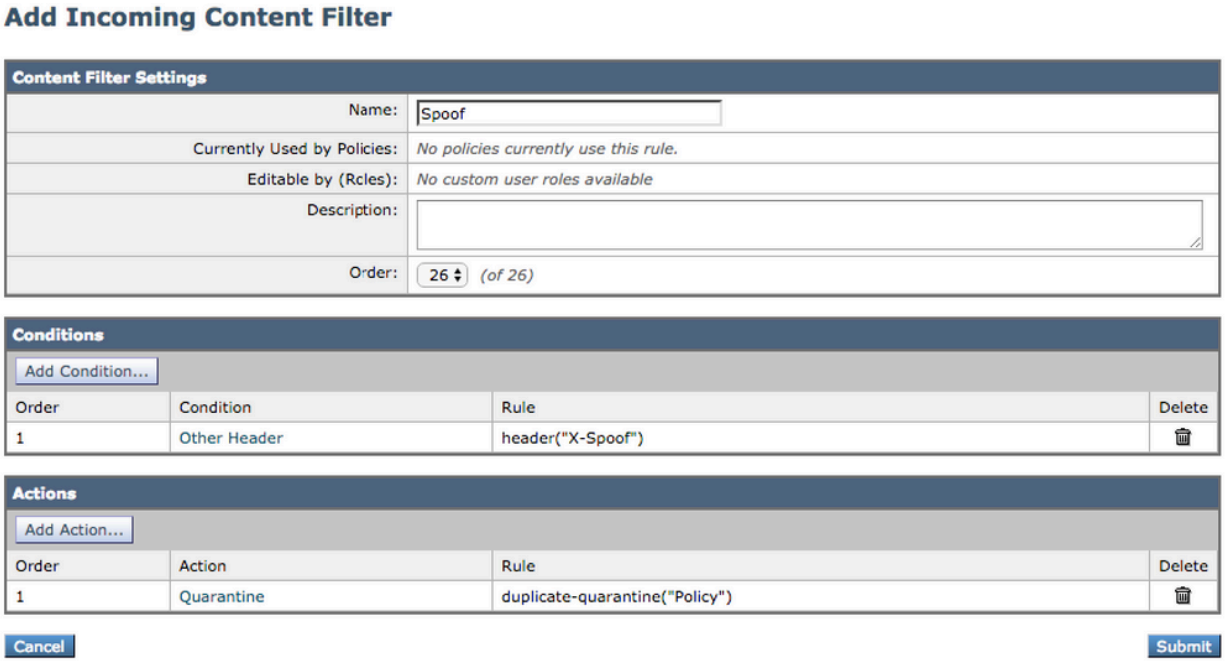
```
mark_spoofed_messages:
if(
     (mail-from-dictionary-match("VALID_INTERNAL_DOMAINS", 1))
 OR  (header-dictionary-match("VALID_INTERNAL_DOMAINS","From", 1)))
 AND ((sendergroup != "RELAYLIST")
 AND (sendergroup != "MY_TRUSTED_SPOOF_HOSTS")
  )
{
insert-header("X-Spoof", "");
}
```

5. メインCLIプロンプトに戻り、Commitを実行して設定を保存します。
6. GUI > Mail Policies > Incoming Content Filtersの順に移動します
7. スプーフィングヘッダーX-Spoofに対してアクションを実行する着信コンテンツフィルタを作成します。

1. その他のヘッダーの追加
2. ヘッダー名：X-Spoof
3. Header existsオプションボタン
4. アクションduplicate-quarantine(Policy)を追加します。

> 注：ここに示すメッセージの重複機能は、メッセージのコピーを保持し、受信者に元のメッセージを送信し続けます。





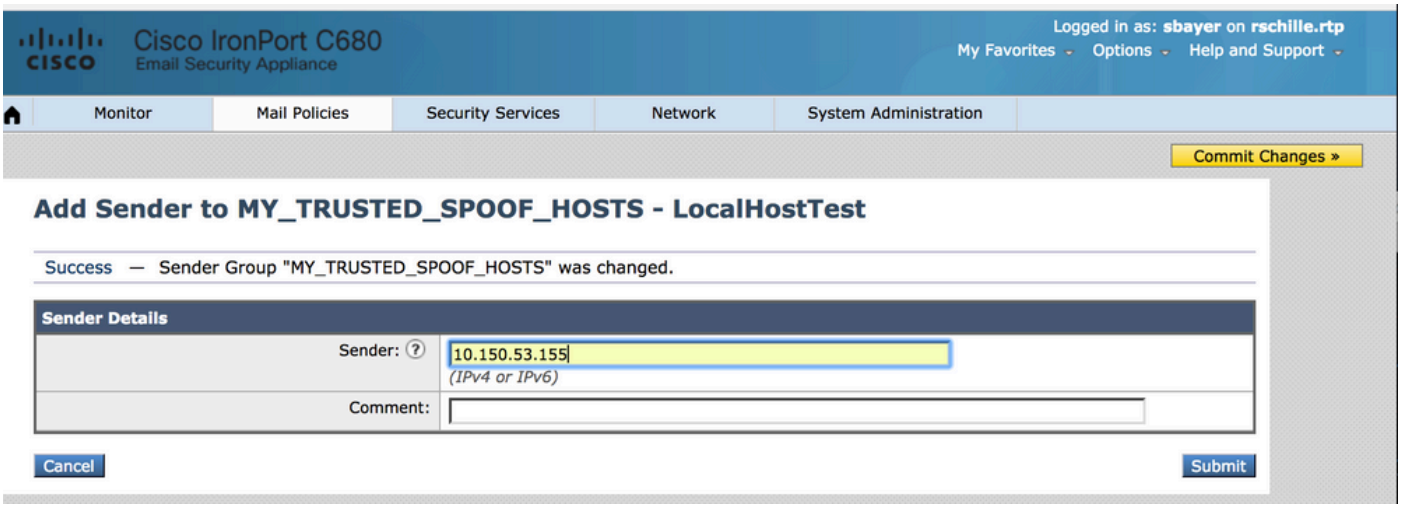
8. GUI > Mail Policies> Incoming Mail Policiesで、コンテンツフィルタを受信メールポリシーにリンクします。
9. 送信し、変更を確定します。

MY_TRUSTED_SPOOF_HOSTSにスプーフィング例外を追加する

最後に、スプーフィング例外（IPアドレスまたはホスト名）を
MY_TRUSTED_SPOOF_HOSTSセンダーグループに追加する必要があります。

1. Web GUIを使用して移動します：Mail Policies > HAT Overview
2. をクリックし、MY_TRUSTED_SPOOF_HOSTS送信者グループを開きます。
3. Add Sender...をクリックして、IPアドレス、範囲、ホスト名、またはホスト名の一部を追加します。
4. Submitをクリックして、送信者の変更を保存します。
5. 最後に、Commit Changesをクリックして設定を保存します。

以下に例を挙げます。



確認

スプーフィングされたメッセージが隔離されていることの確認

ドメインの1つをエンベロープ送信者として指定して、テストメッセージを送信します。メッセージに対してメッセージトラックを実行して、フィルタが期待どおりに機能することを確認します。期待される結果は、スプーフィングを許可された送信者に対してまだ例外が作成されていないため、メッセージが隔離されることです。

<#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_messag
```

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

スプーフィング例外メッセージが配信されていることの確認

Spoof-Exceptionの送信者は、上記のフィルタで参照されている送信者グループのIPアドレスです。

RELAYLISTは、ESAが送信メールの送信に使用するため、参照されます。通常、RELAYLISTによって送信されるメッセージは送信メールであり、これを含めないと誤検出が発生するか、上記のフィルタによって検疫される送信メッセージになります。

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追跡の例。予期されたアクションは配信であり、検疫ではありません。（このIPはスプーフィングが許可されます）。

<#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
```

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

シスコ内部情報

このプロセスを簡素化するために、RATをメッセージフィルタ/コンテンツフィルタに公開する機能の要求があります。

Cisco Bug ID CSCus49018:ENH：受信者アクセステーブル(RAT)をフィルタ処理に表示する

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。