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

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。 複数が、他のドメインが為を送出す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

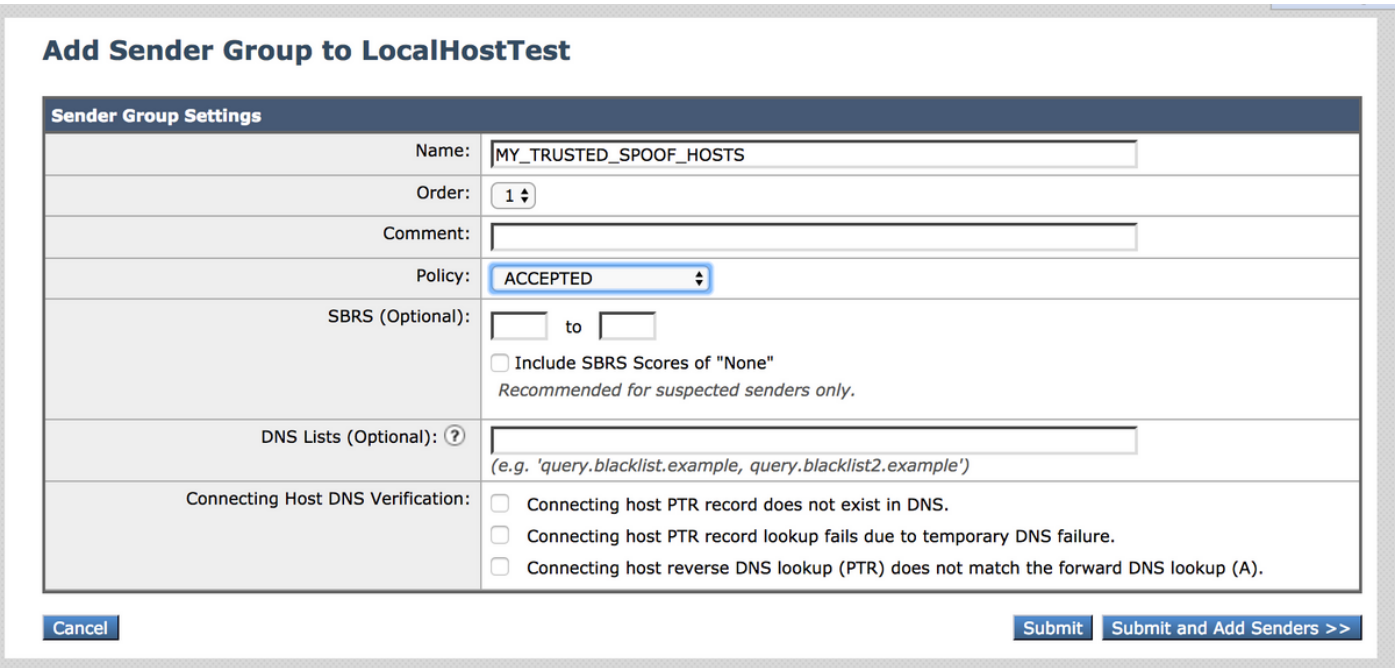
い。

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
:

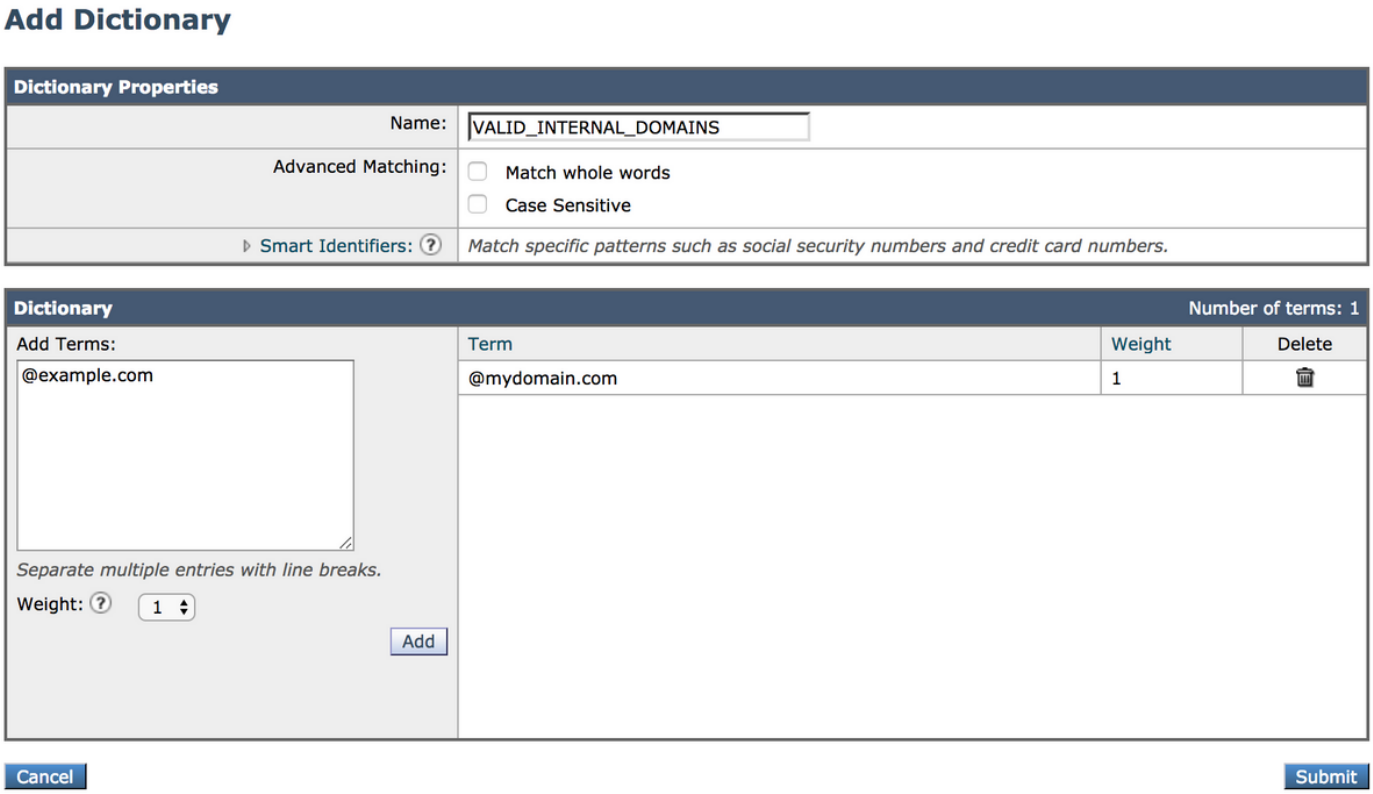


辞書を作成して下さい

ESA の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：



メッセージ フィルターを作成して下さい

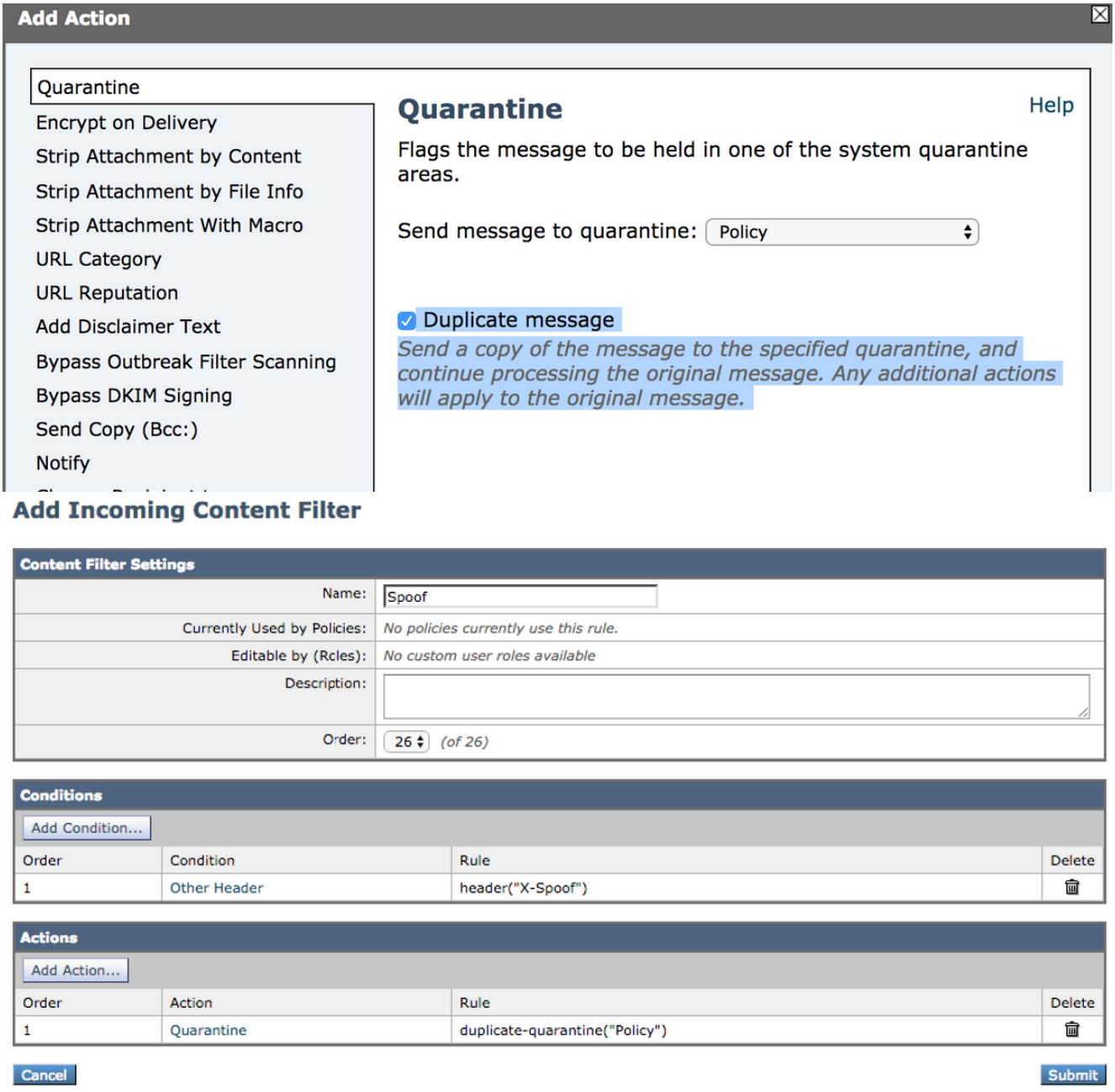
次に、「VALID_INTERNAL_DOMAINS」ちょうど作成された辞書にてこ入れするためにメッセージ フィルターを作成する必要があります:

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。



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。

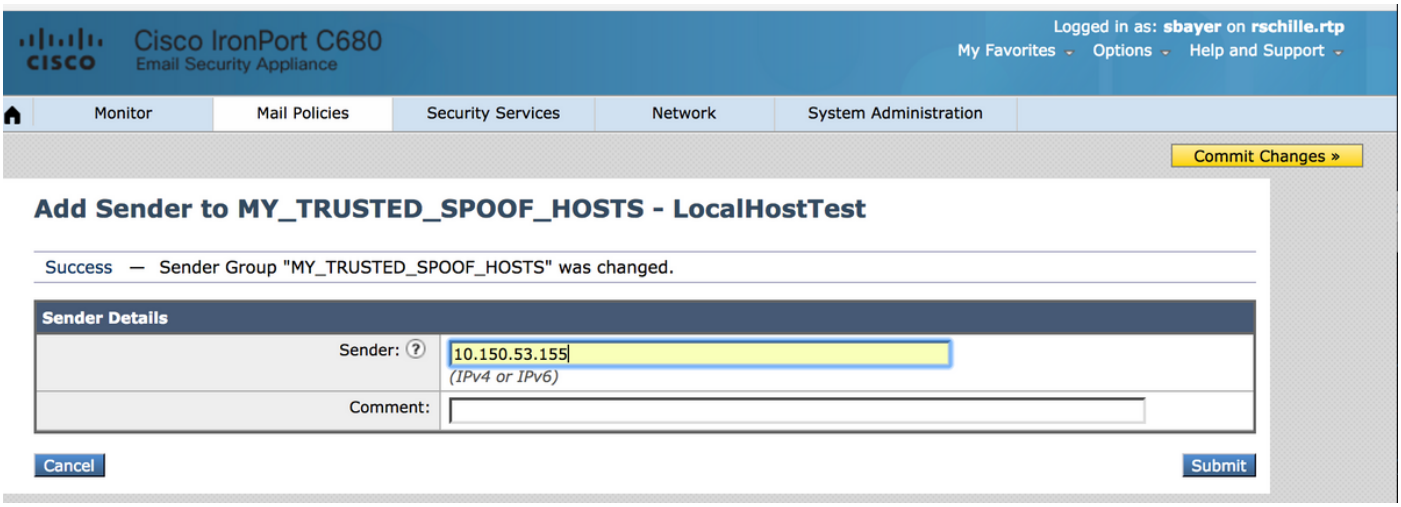
MY_TRUSTED_SPOOF_HOSTS にスプーフィング例外を追加して下さい

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：



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