# Cisco Eメールセキュリティアプライアンス(ESA)を使用してフィッシング詐欺プラットフォームキャンペーンをシミュレートする方法

## 内容



## 概要

このドキュメントでは、シミュレートされたフィッシングプラットフォームキャンペーンを正常に許可するためのCisco Eメールセキュリティアプライアンス(ESA)の設定手順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。

- ESAでのメッセージおよびコンテンツフィルタの作成。
- ホストアクセステーブル(HAT)の設定。
- Cisco ESAの受信Eメールパイプラインについて理解する。

### 使用するコンポーネント

このドキュメントの内容は、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

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。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

シミュレーションフィッシングプラットフォームを使用すると、管理者はサイクルの一部としてフィッシングキャンペーンを実行し、ソーシャルエンジニアリング攻撃のベクトルとして電子メ

ールシステムを使用する最大の脅威の1つを管理できます。

## 問題

このようなシミュレーションに対してESAが準備されていない場合、スキャンエンジンがフィッシング詐欺キャンペーンメッセージを停止することは珍しいことではなく、シミュレーションの効果が失敗または低下します。

## 解決方法

> **注意**：この設定例では、*TRUSTED*メールフローポリシーを選択して、ESAがスロットリングなしで大規模なシミュレートされたフィッシングキャンペーンを通過できるようにします。大量のフィッシングキャンペーンを継続的に実行すると、電子メール処理のパフォーマンスに影響を及ぼす可能性があります。

フィッシング詐欺キャンペーンメッセージがESA設定のどのセキュリティコンポーネントによっても停止されないようにするため、適切に設定する必要があります。

1. 新しい送信者グループの作成：**[GUI] > [Mail Policies] > [HAT Overview]を選択**して、それを*TRUSTED*メールフローポリシーにバインドします(または、**[GUI] > [Mail Policies] > [Mail Flow Policies]で同様のオプションを使用して新しいポリシーを作成**できます)。
2. シミュレートされたフィッシングプラットフォームの送信元ホストまたはIPをこの送信元グループに追加します。シミュレートされたフィッシングプラットフォームのIPの範囲が大きい場合は、ホスト名の一部を追加するか、IPの範囲を追加できます（該当する場合）。
3. *BLOCKLIST* Sender Groupの上にSender Groupを並べ替えて、*SBRSではなく静的*に照合されるようにします。
4. **[GUI] > [Mail Policies]** > [Mail Flow Policies] > [TRUSTED]（または新しく作成したメールフローポリシー）で*TRUSTED*メールフローポリシーのすべてのセキュリティ機能を無効にします。

| Security Features | |
|---|---|
| Spam Detection: | ○ Use Default (On) ○ On ◉ Off |
| AMP Detection | ○ Use Default (On) ○ On ◉ Off |
| Virus Protection: | ○ Use Default (On) ○ On ◉ Off |
| Sender Domain Reputation Verification: | ○ Use Default (On) ○ On ◉ Off |
| Virus Outbreak Filters: | ○ Use Default (On) ○ On ◉ Off |
| Advanced Phishing Protection: | ○ Use Default (On) ○ On ◉ Off |
| Graymail Detection: | ○ Use Default (On) ○ On ◉ Off |
| Content Filters: | ○ Use Default (On) ○ On ◉ Off |
| Message Filters: | ○ Use Default (On) ○ On ◉ Off |

5.これらの**変更を送信し、コミットします。**

**注意**：この設定例では、*TRUSTED*メールフローポリシーを選択して、ESAがスロットリングなしで大規模なシミュレートされたフィッシングキャンペーンを通過できるようにします。大量のフィッシングキャンペーンを継続的に実行すると、電子メール処理のパフォーマンスに影響を及ぼす可能性があります。

フィッシング詐欺キャンペーンメッセージがESA設定のどのセキュリティコンポーネントによっても停止されないようにするため、適切に設定する必要があります。

1. 新しい送信者グループの作成：**[GUI] > [Mail Policies] > [HAT Overview]の順に選択**し、信頼できるメールフローポリシーにバインドします。
2. シミュレートされたフィッシングプラットフォームの送信元ホストまたはIPをこの送信元グループに追加します。シミュレートされたフィッシングプラットフォームのIPの範囲が大きい場合は、ホスト名の一部を追加するか、IPの範囲を追加できます（該当する場合）。
3. *BLOCKLIST* Sender Groupの上にSender Groupを並べ替えて、*SBRSではなく静的*に照合されるようにします。
4. **これらの変更を送信し、確定します。**
5. CLIに移動し、新しいメッセージフィルタ、**[CLI] > [filters]を追加**し、構文をコピーして変更し、フィルタを追加します。
6. 
```
skip_engines_for_simulated_phishing:
if (sendergroup == "name_of_the_newly_created_sender_group")
{
insert-header("x-sp", "uniquevalue");
log-entry("Skipped scanning engines for simulated phishing");
skip-spamcheck();
skip-viruscheck();
skip-ampcheck();
skip-marketingcheck();
skip-socialcheck();
skip-bulkcheck();
skip-vofcheck();
skip-filters();
}
.
```
7. リスト内のメッセージフィルタを上に並べ替えて、リストの上の別のメッセージフィルタ（skip-filtersアクションを含む）によってスキップされないようにします。
8. Enterキーを押してAsyncOSのメインコマンドプロンプトに戻り、コマンド「**commit**」を発行して変更を確定します。（Ctrl+Cをクリックしないでください。すべての変更が消去されます）。
9. [GUI] > [メール**ポリシー] > [受信コンテンツフィルタ]に移動します**
10. 条件「***Other Header***」が設定された新しい受信コンテンツフィルタを作成し、メッセージフィルタに設定されているカスタムヘッダー**"x-sp"とその固有の値を探**し、アクション***Skip Remaining Content Filters (Final Action)を設定します***。
11. コンテンツフィルタを「1」に並べ替えて、他のフィルタがシミュレートされたフィッシングメッセージに対してアクションを実行しないようにします。
12. [GUI] > [メール**ポリシー] > [受信メールポリシー]に移動**し、コンテンツフィルタを必要なポリシーに割り当てます。
13. **変更を送信し、保存します。**
14. シミュレートされたフィッシングプラットフォームキャンペーンを実行し、

mail_logs/Message Trackingを監視して、フローとポリシールールの照合を確認します。