Phishing 教育テスト用の Cisco ESA のホワイトリスト ポリシーの作成

目次

[はじめに](#)
[前提条件](#)
[要件](#)
[背景説明](#)
[設定](#)
[送信側 グループの作成](#)
[メッセージ フィルターの作成](#)
[確認](#)

概要

この資料に教育テスト/キャンペーンを phishing 割り当てるように Cisco E メール セキュリティ アプライアンス（ESA）またはクラウド E メール セキュリティ（CES）例のホワイトリスト ポリシーを作成する方法を記述されています。

前提条件

要件

次の項目に関する知識が推奨されます。

- ナビゲート し、WebUI の Cisco ESA/CES のルールを設定します。
- Command Line Interface （CLI）の Cisco ESA/CES のメッセージ フィルターの作成。
- phishing キャンペーン/テストに使用するリソースのナレッジ。

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。 対象のネットワークが実稼働中である場合には、どのような作業についても、その潜在的な影響について確実に理解しておく必要があります。

背景説明

phishing 教育テストかキャンペーンを実行している管理者はメールを反スパムや発生フィルタ規則セットの Talos 現在のルールと一致する情報と生成します。 そのようなイベントでは、phishing キャンペーン メールはエンドユーザに達しなかったりし、こうして停止にテストを引き起こす Cisco により ESA/CES 自体によって actioned。 管理者はキャンペーン/テストを遂行するためにこれらのメールを通して ESA/CES 割り当てを確認する必要があります。

設定

警告： whitelisting phishing シミュレーション及び教育ベンダーの Cisco のスタンスはグローバルに許可されません。 管理者に phishing シミュレーター サービスを使用するように助言します *(たとえば:* IP を得る *PhishMe は)* ホワイトリストにそれからそれらをローカルで追加します。 Cisco はそれらの IP からハンドを変更するか、または実際に脅威になればESA/CES 顧客を保護する必要があります。

注意： 管理者はホワイトリストでしかこれらの IP を保存するはずではないです、ホワイトリストに外部 IP を残すテストしている間長時間にわたってテストを非要請を持って来るかもしれないです掲示すればこれらの IP エンドユーザへの悪意のあるメールは妥協されるようになります。

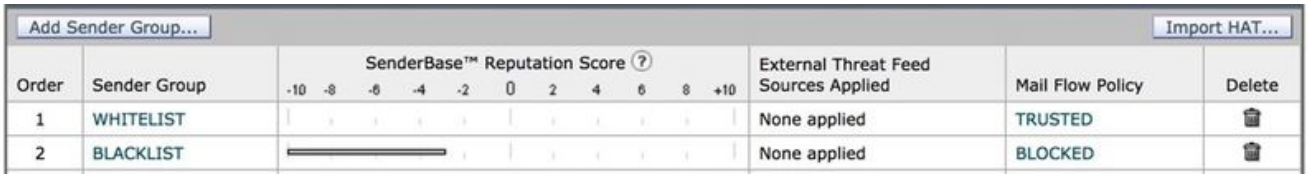
Cisco E メール セキュリティ アプライアンス (ESA) で、phishing シミュレーションのための新しい送信側 グループを作成し、$TRUSTED メール フロー ポリシーにそれを割り当てて下さい。これはすべての phishing シミュレーション メールがエンドユーザに渡されるようにします。 この新しい送信側 グループのメンバーは制限する比率に応じてないしそれらの送信側からのコンテンツは Cisco IronPort 反スパム エンジンによってスキャンされませんが、まだアンチウィルス ソフトウェアによってスキャンされます。

注: デフォルトで、$TRUSTED メール フロー ポリシーに消えるアンチウィルス イネーブルになった反スパムがあります。

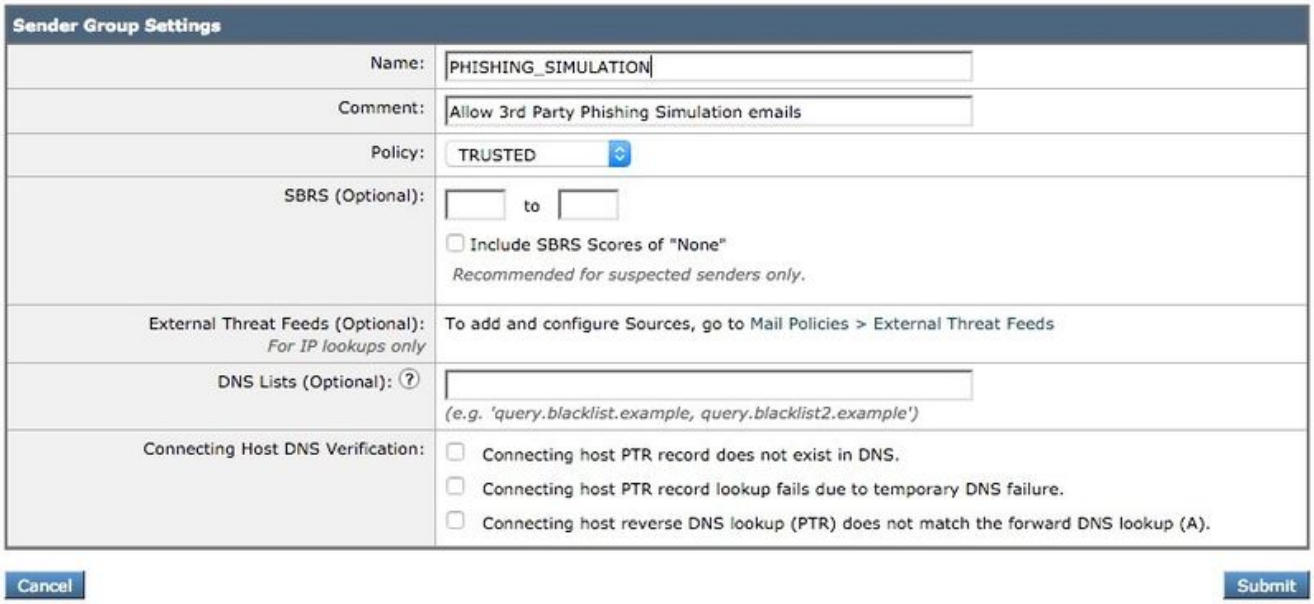
送信側 グループの作成

1. [Mail Policies] タブをクリックします。
2. ***ホスト アクセス 表 セクションの下で、帽子概要を選択して下さい***

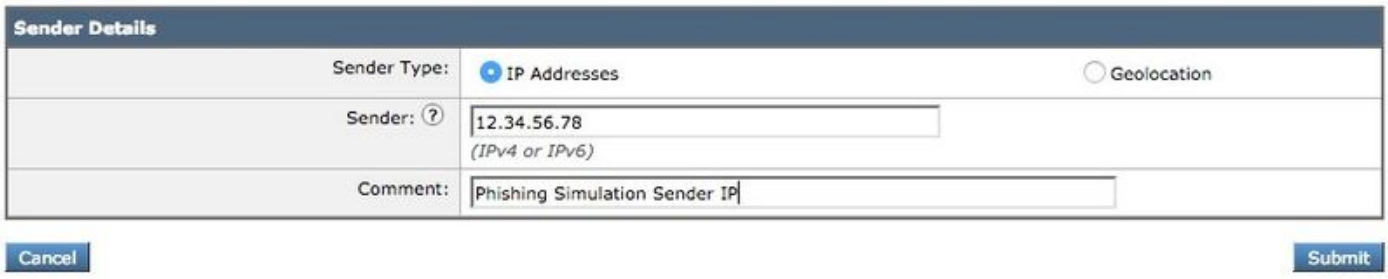
3. 右側の [InboundMail] リスナーが現在選択されていることを確認します。
4. 下記の***送信側 Group カラム***から***送信側 グループを...*** 『Add』 をクリック して下さい、



5. ***名前およびコメント 欄を記入して下さい。 次にドロップダウンなポリシーの下で「$TRUSTED」を選択し、送信側を >> 『SUBMIT』 をクリック し、追加して下さい。***



6. ホワイトリストに追加する IP またはホスト名を最初のフィールドに入力します。 Phishing シミュレーション パートナーは送信側 IP情報を与えます。



エントリの追加を終了したら、[Submit] ボタンをクリックします。 必ず [Commit Changes] ボタンをクリックして変更を保存してください。

メッセージ フィルターの作成

反スパムのバイパスを許可するために送信側 グループを作成した後アンチウィルス Phishing キャンペーン/テストを一致するかもしれない他のセキュリティ エンジンをスキップするために、メッセージ フィルターが必要となり。

1. ESA の 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:

```
skip_amp_graymail_vof_for_phishing_campaigns:
if(sendergroup == "PHISHING_SIMULATION")
{
skip-ampcheck();
skip-marketingcheck();
skip-socialcheck();
skip-bulkcheck();
skip-vofcheck();
}
```

5. 主要な CLI プロンプトに戻り、『Enter』 を押して下さい。
6. 設定を保存するために***託します***実行して下さい。

確認

Phishing キャンペーン/テストを送信 するのにサード パーティ リソースを使用すればメッセージ トラッキング ログの結果をすべてのエンジンを確認するために確認するためにスキップされ、メールは渡されました。