Eメールボンビングを使用したESAでの宛先制御のテスト

内容

[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](#)

[問題](#)

[解決方法](#)

- [電子メール爆破用のPythonスクリプト](#)
- [スクリプトの内訳](#)

[宛先制御のテスト](#)

[関連情報](#)

はじめに

このドキュメントでは、Eメールボンビングを使用してESAアプライアンスの宛先制御をテストするプロセス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。

- CiscoセキュアEメールアプライアンス
- Pythonプログラミング言語

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- CiscoセキュアEメールアプライアンス
- Python 3.X

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

ESAアプライアンスの宛先制御は、受信者ドメインが過多にならないように電子メール配信を制御します。ESAでは、アプライアンスが開くことができる接続の数と、各宛先ドメインに送信されるメッセージの数を定義できます。宛先制御テーブルには、リモート接続先に電子メールを配信するときの接続速度とメッセージ速度の設定が含まれ、TLSの使用を強制するためのオプションも含まれています。

宛先制御の詳細については、『バウンス検証および宛先制御のベストプラクティスガイド』を参照してください。

メールボムは、特定の受信者に大量の電子メールを送信することによって、受信トレイを圧倒したり、サーバを妨害したりすることを目的としたDoS攻撃の一種です。この方法の目的は、ディスクスペースを使い果たすか、サーバを過負荷にして中断させることです。

問題

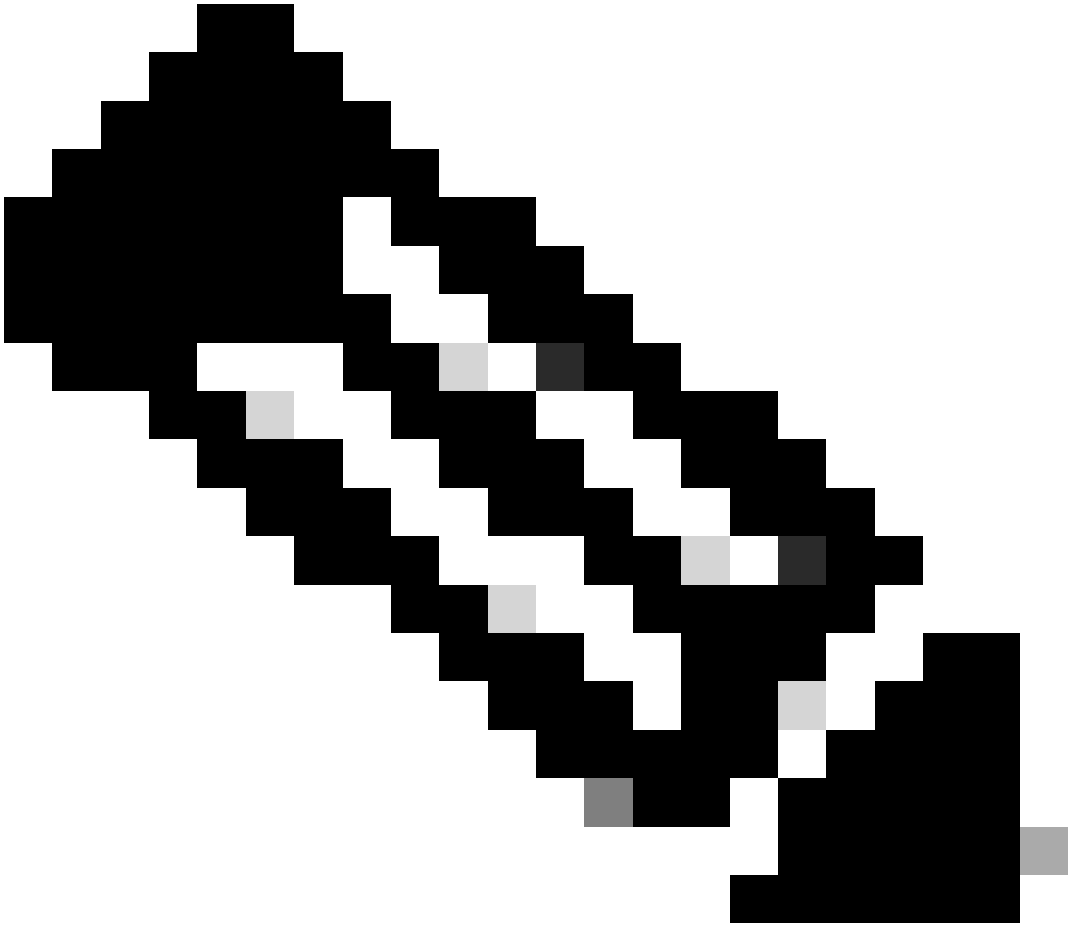
電子メールのフラッディングを防止する宛先制御の効果をテストすることは非常に重要です。適切に設定しないと、過剰なEメール配信によってサーバに過大な負荷がかかり、パフォーマンスの低下やサービスの中断を招く可能性があります。

解決方法

Pythonスクリプトを使用して、電子メールボムをシミュレートし、ESAアプライアンスでの宛先制御の有効性をテストできます。

電子メール爆破用のPythonスクリプト

```
import smtplib subject = 'EMAIL BOMBER' body = 'I am bombing you!' message = f'Subject: {subject}\n\n{body}' server = smtplib.SMTP("XXX.XXX.XXX.XXX", 25) i = 1 while i < 100: server.sendmail("SENDER_ADDR", "RECIPIENT_ADDR", message) i += 1 server.quit()
```



注：コードの次のセクションを、必要な情報に置き換えることができます。

- XXX.XXX.XXX.XXX:ESAのIPアドレス。
- SENDER_ADDR – 送信者アドレス
- RECIPIENT_ADDR – 受信者アドレス

スクリプトの内訳

- smtplibライブラリは、SMTPプロトコルを使用して電子メールを送信するためにインポートされます。
- 件名と本文で電子メールの内容を定義します。
- サーバ変数には、CESアプライアンスのIPと接続用のポート25を含むSMTPサーバの詳細が保存されます。
- whileループは、指定された送信者と受信者の電子メールアドレスを使用して、99通の電子メールを送信します。
- server.quit()関数は、SMTPサーバへの接続を終了します。

宛先制御のテスト

1. CES/ESAアプライアンスのGUIを開き、Mail Policies -> Destination Controlsの順に移動します。

2. Default設定をクリックします。

Destination Controls

Destination Control Table

Add Destination... | Import Table

Domain	IP Address Preference	Destination Limits	TLS Support	Certificate	DANE Support ^	Bounce Verification *	Bounce Profile	Delete
Default	IPv6 Preferred	500 concurrent connections, 50 messages per connection, No recipient limit	None	Cisco ESA Certificate	None	Off	Default	

Export Table

** Bounce Verification settings apply only if bounce verification address tagging is in use. See Mail Policies > Bounce Verification.*
^ DANE will not be enforced for domains that have SMTP Routes configured.

宛先制御テーブル

3. 「Maximum Messages Per Connection」の値を確認します。

Default Destination Controls

IP Address Preference: IPv6 Preferred

Limits:
- Concurrent Connections: 500 *(between 1 and 1,000)*
- Maximum Messages Per Connection: 50 *(between 1 and 1,000)*
- Recipients: (•) No Limit ( ) Maximum of 0 per 60 minutes
  Number of recipients between 0 and 1,000,000,000 per number of minutes between 1 and 60
- Apply limits: Per Secure Email hostname: (•) System Wide ( ) Each Virtual Gateway *(recommended if Virtual Gateways are in use)*

TLS Support: None

A security certificate/key has not yet been configured. Enabling TLS will automatically enable the "Cisco ESA Certificate" certificate/key. (To configure a different certificate/key, start the CLI and use the `certconfig` command.)

Certificate: Cisco ESA Certificate

DANE Support: None

Bounce Verification: Perform address tagging: (•) No ( ) Yes

Applies only if bounce verification address tagging is in use. See Mail Policies > Bounce Verification.

Bounce Profile: *To edit the Default bounce profile, use Network > Bounce Profiles.*

Note: DANE will not be enforced for domains that have SMTP Routes configured.

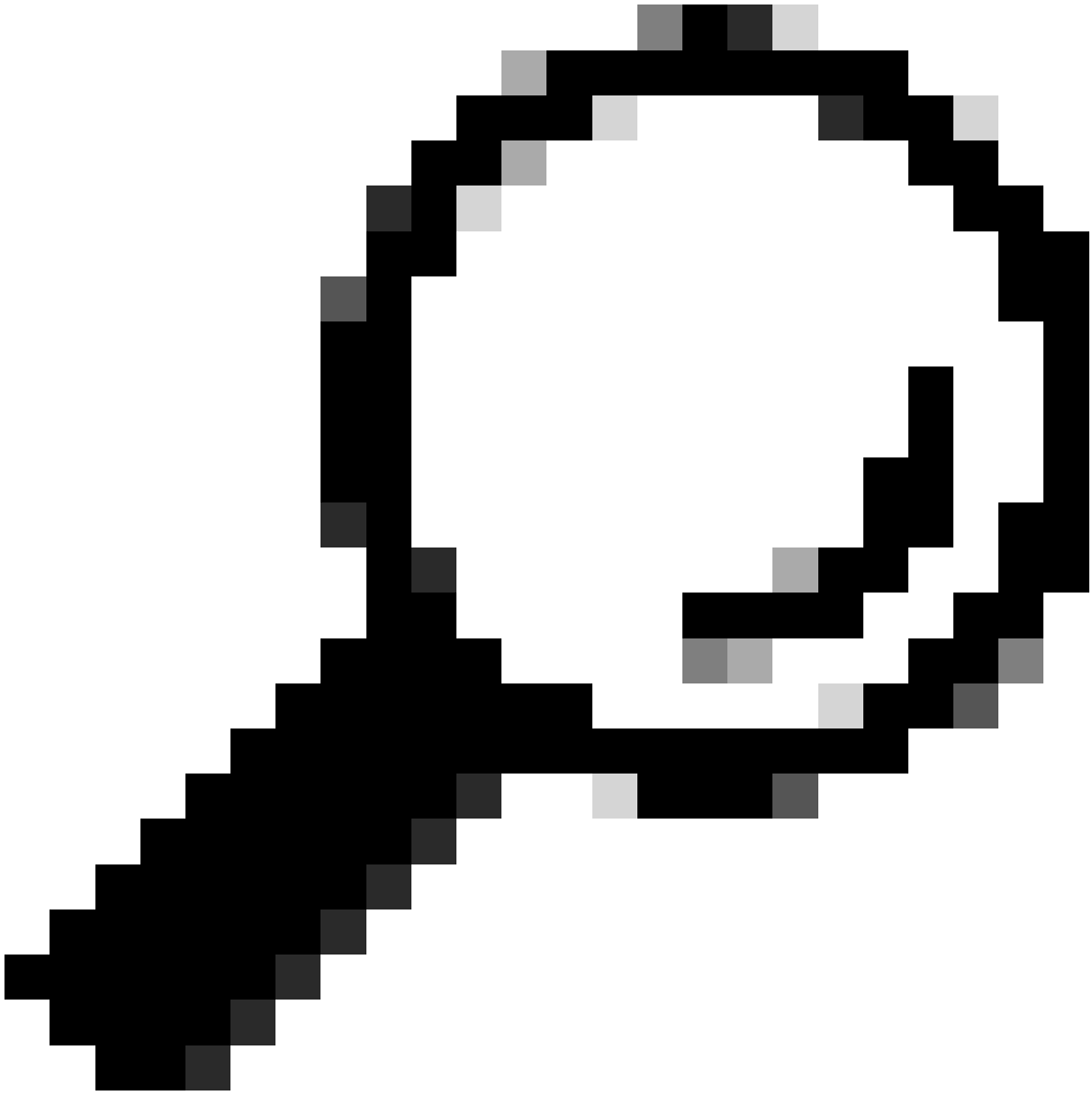
既定の通知先コントロールの編集

4. この値が、スクリプトで設定されている電子メールの数より小さいことを確認します。たとえば、スクリプトが100通の電子メールを送信するように設定されていて、アプライアンスが1接続あたり50通のメッセージしか許可していない場合、過剰な接続がブロックされます。

5. スクリプトを実行し、メッセージトラッキングの結果を確認します。

6. 50を超える接続を試みると、過剰な電子メールがブロックされ、接続が多すぎるとしてログに記録されます。

7. 送信する電子メールが50未満になるようにスクリプトを変更し、すべての電子メールが正常に配信されることを確認します。



ヒント：制御されたテストでは、Eメールボンビング値を10電子メール未満に設定します。50通の電子メールでさえ、電子メール攻撃の一形態と考えることができます。必要に応じてスクリプトを調整し、意図しない中断を引き起こさずに異なるしきい値をテストします。

関連情報

- Cisco ESA宛先制御ガイド
- シスコのテクニカルサポートとダウンロード

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。