使用郵件轟炸測試ESA中的目標控制

目錄

簡介

本文檔介紹使用Email Booting測試ESA裝置中的目標控制的過程。

必要條件

需求

思科建議您瞭解以下主題：

- 思科安全電子郵件裝置
- Python程式語言

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 思科安全電子郵件裝置
- Python 3.X

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

ESA裝置上的目標控制可控制郵件傳送，防止收件人域過多。ESA允許定義裝置可以開啟的連線數以及傳送到每個目標域的郵件數。「目標控制」表提供了將電子郵件傳送到遠端目標時的連線和郵

件速率設定，並且還包含用於強制使用TLS的選項。

有關目標控制元件的更多詳細資訊，請訪問以下網站：退回驗證和目的地控制的最佳實踐指南。

郵件炸彈是一種拒絕服務(DoS)攻擊，旨在通過向特定收件人傳送大量電子郵件來壓垮收件箱或阻止伺服器。此方法旨在使磁碟空間耗盡或使伺服器過載，從而造成中斷。

問題

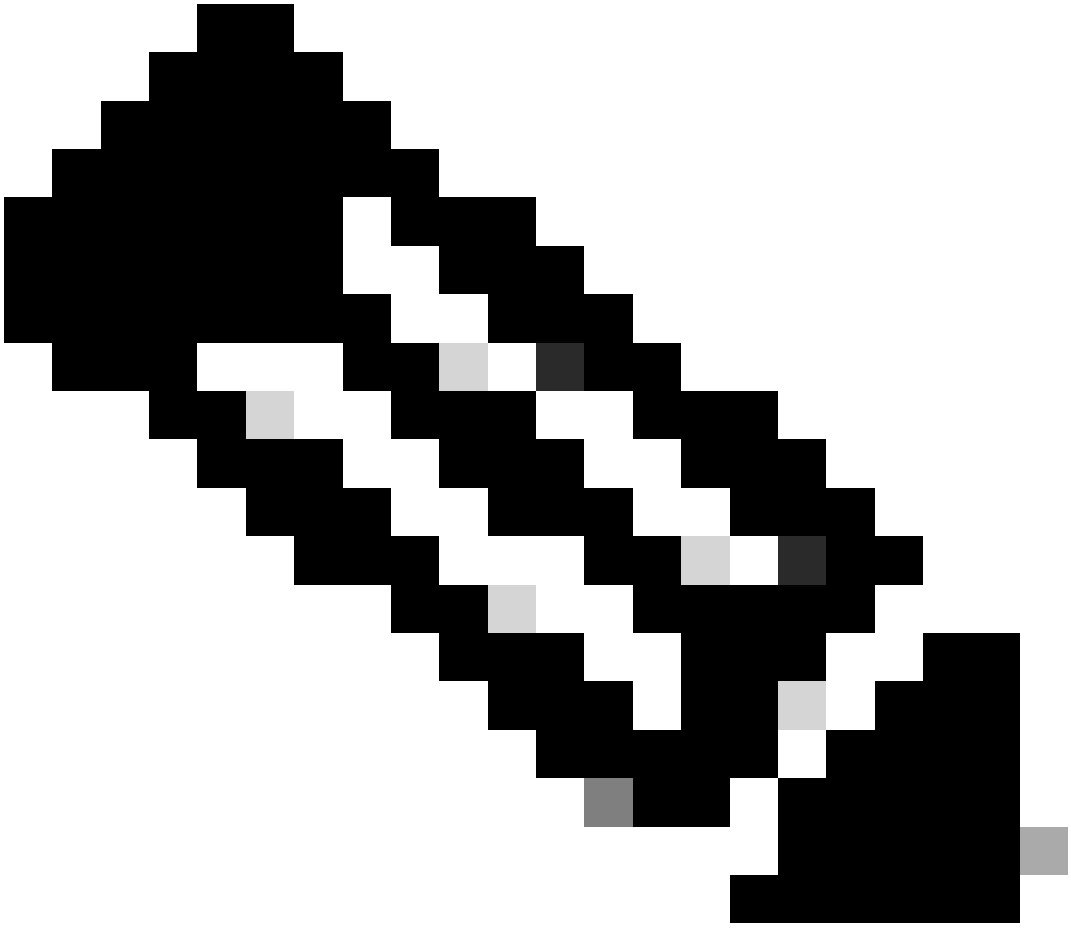
測試目的地控制對防止電子郵件泛濫的效果至關重要。如果沒有正確的配置，過多的電子郵件傳送嘗試可能會使伺服器不堪重負，導致效能下降或服務中斷。

解決方案

Python指令碼可用於類比電子郵件炸彈並測試ESA裝置上目標控制的效果。

電子郵件爆炸的Python指令碼

```
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()
```



註：您可以使用所需資訊替換代碼的以下部分：

- XXX.XXX.XXX.XXX - ESA的IP地址。
- SENDER_ADDR — 發件人地址
- RECIPIENT_ADDR — 收件人地址

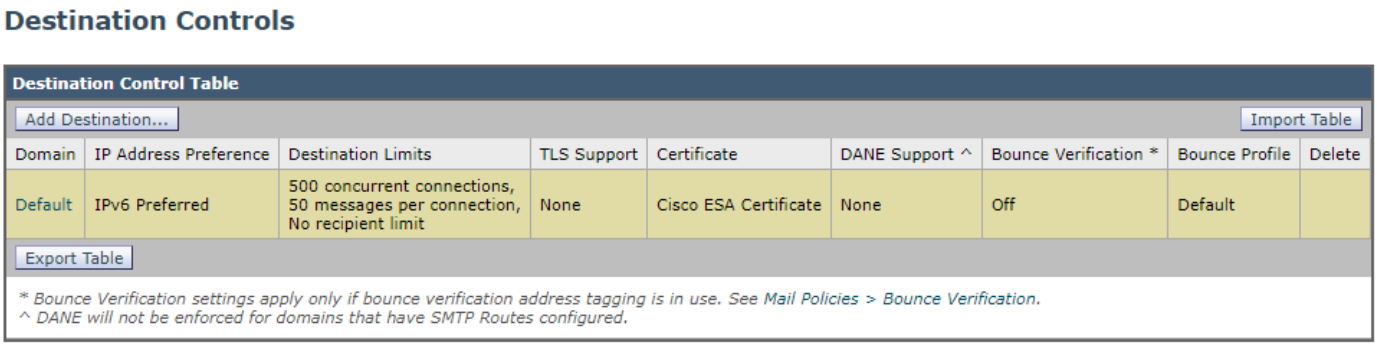
指令碼細分

- 匯入smtplib庫以使用SMTP協定傳送電子郵件。
- 主題和正文用於定義電子郵件內容。
- 伺服器變數儲存SMTP伺服器詳細資訊，並使用CES裝置IP和埠25進行連線。
- while循環使用提供的發件人和收件人電子郵件地址傳送99封電子郵件。
- server.quit()函式將終止與SMTP伺服器的連線。

測試目標控制元件

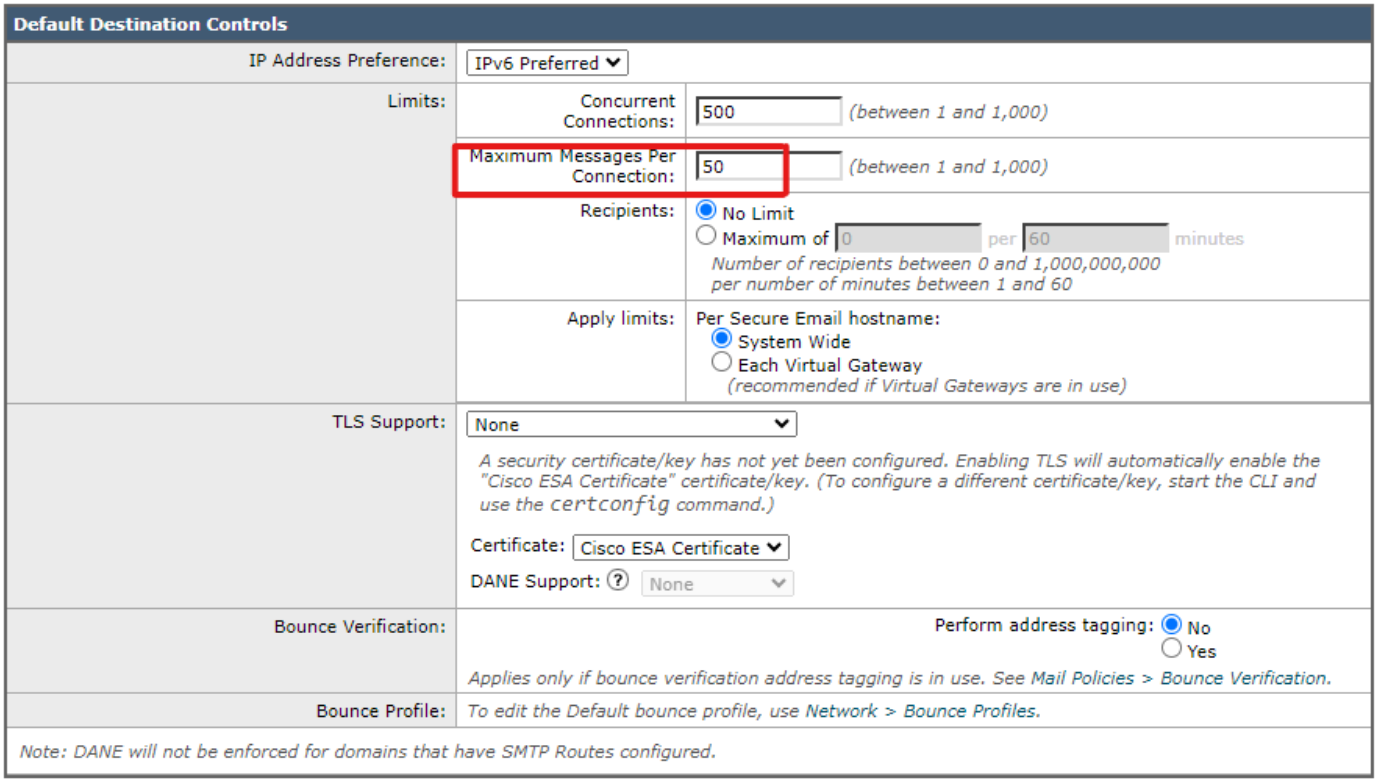
1.開啟CES/ESA裝置的GUI並導航至Mail Policies -> Destination Controls。

2.按一下Default settings。



目標控制表

3.檢查Maximum Messages Per Connection值。



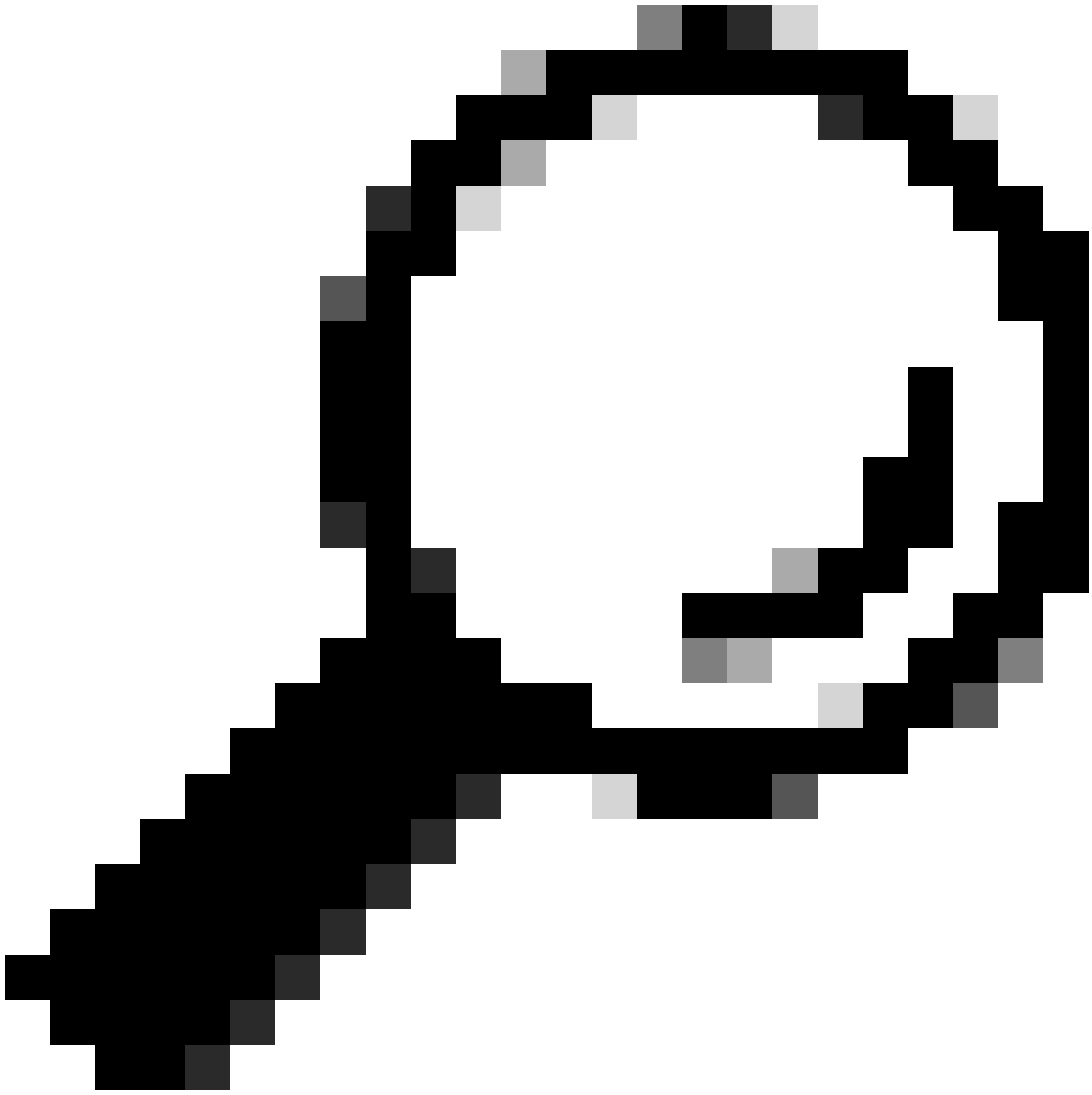
編輯預設目標控制元件

4.確保此值小於指令碼中設定的電子郵件數。例如，如果指令碼配置為傳送100封電子郵件，而裝置只允許每個連線傳送50封郵件，則會阻止過度連線。

5.執行指令碼並觀察消息跟蹤中的結果。

6.如果嘗試的連線超過50個，系統會阻止過多的電子郵件，並將嘗試記錄為過多的連線。

7.修改指令碼以傳送少於50封電子郵件，並驗證所有電子郵件是否已成功傳送。



提示：對於受控測試，請將郵件爆炸值設定為少於10封郵件。甚至50封電子郵件都可能被視為一種電子郵件爆炸形式。根據需要調整指令碼，以便測試不同的閾值，而不會造成意外中斷。

相關資訊

- 思科ESA目標控制指南
- 思科技術支援與下載

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。