Testen der Zielsteuerelemente in der ESA mithilfe von E-Mail-Bombardierung

Inhalt

Einleitung

In diesem Dokument wird der Prozess beschrieben, bei dem die Zielsteuerelemente in der ESA-Appliance mithilfe von E-Mail-Bombardierung getestet werden.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Cisco Secure E-Mail Appliance
- Python-Programmiersprache

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Cisco Secure E-Mail Appliance
- Python 3.X

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

Die Zielsteuerelemente auf der ESA-Appliance regeln die E-Mail-Zustellung, um eine Überlastung der Empfängerdomänen zu verhindern. Die ESA ermöglicht die Definition der Anzahl von Verbindungen, die die Appliance öffnen kann, und der Anzahl von Nachrichten, die an jede Zieldomäne gesendet werden. Die Zielsteuerelementtabelle enthält Einstellungen für die Verbindungs- und Nachrichtenraten bei der Zustellung von E-Mails an Remote-Ziele sowie Optionen zum Erzwingen der Verwendung von TLS.

Weitere Einzelheiten zu den Bestimmungskontrollen finden Sie hier: Best Practice-Leitfaden für Bounce-Verifizierung und Zielsteuerelemente.

Eine Mail-Attacke ist eine Art Denial-of-Service (DoS)-Angriff, der entwickelt wurde, um einen Posteingang zu überlasten oder einen Server zu blockieren, indem eine enorme Anzahl von E-Mails an einen bestimmten Empfänger gesendet wurde. Diese Methode soll entweder Speicherplatz belegen oder den Server überlasten, wodurch es zu Unterbrechungen kommt.

Problem

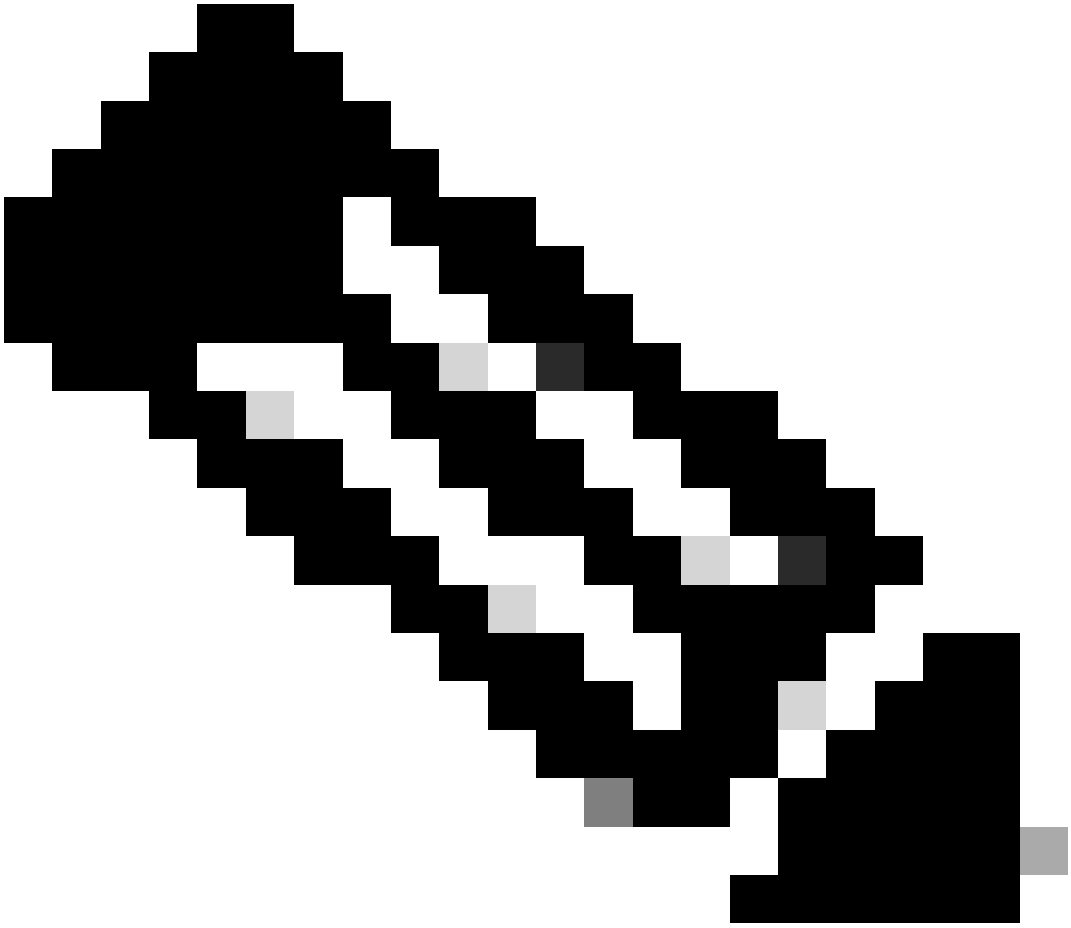
Die Wirksamkeit der Zielkontrollen zur Verhinderung von E-Mail-Überflutungen muss getestet werden. Ohne ordnungsgemäße Konfiguration kann die übermäßige E-Mail-Zustellung den Server überlasten und zu Leistungseinbußen oder Serviceunterbrechungen führen.

Lösung

Ein Python-Skript kann verwendet werden, um eine E-Mail-Bombe zu simulieren und die Wirksamkeit der Zielsteuerelemente auf der ESA-Appliance zu testen.

Python-Skript für E-Mail-Bombardierung

```
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()
```



Hinweis: Sie können die folgenden Abschnitte des Codes durch die erforderlichen Informationen ersetzen:

- XXX.XXX.XXX.XXX - IP-Adresse Ihrer ESA.
- SENDER_ADDR - Absenderadresse
- RECIPIENT_ADDR - Empfängeradresse

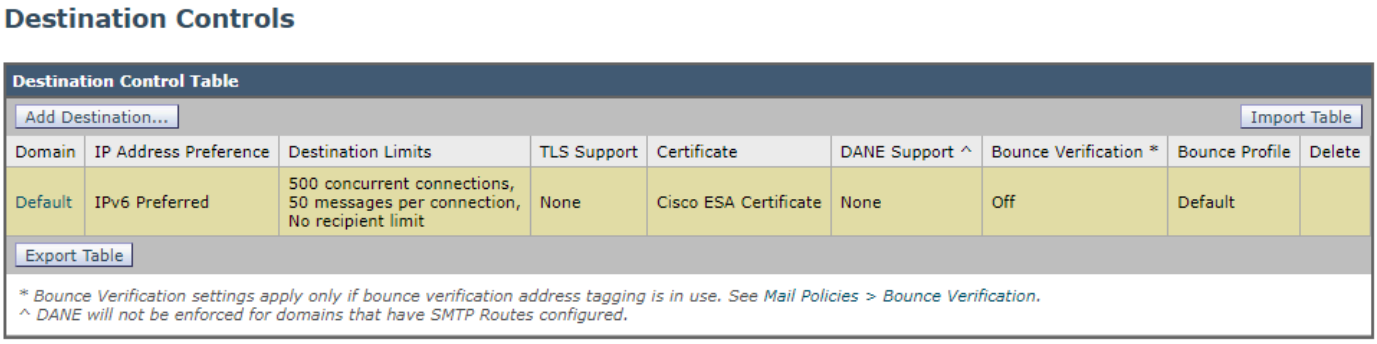
Skript-Aufschlüsselung

- Die smtplib-Bibliothek wird zum Senden von E-Mails mithilfe des SMTP-Protokolls importiert.
- Betreff und Text definieren den E-Mail-Inhalt.
- Die Servervariable speichert die SMTP-Serverdetails mit der CES-Appliance-IP und dem Port 25 für die Verbindung.
- Der while-Loop sendet 99 E-Mails unter Verwendung der angegebenen Absender- und Empfänger-E-Mail-Adressen.
- Die Funktion server.quit() beendet die Verbindung zum SMTP-Server.

Testen von Zielsteuerelementen

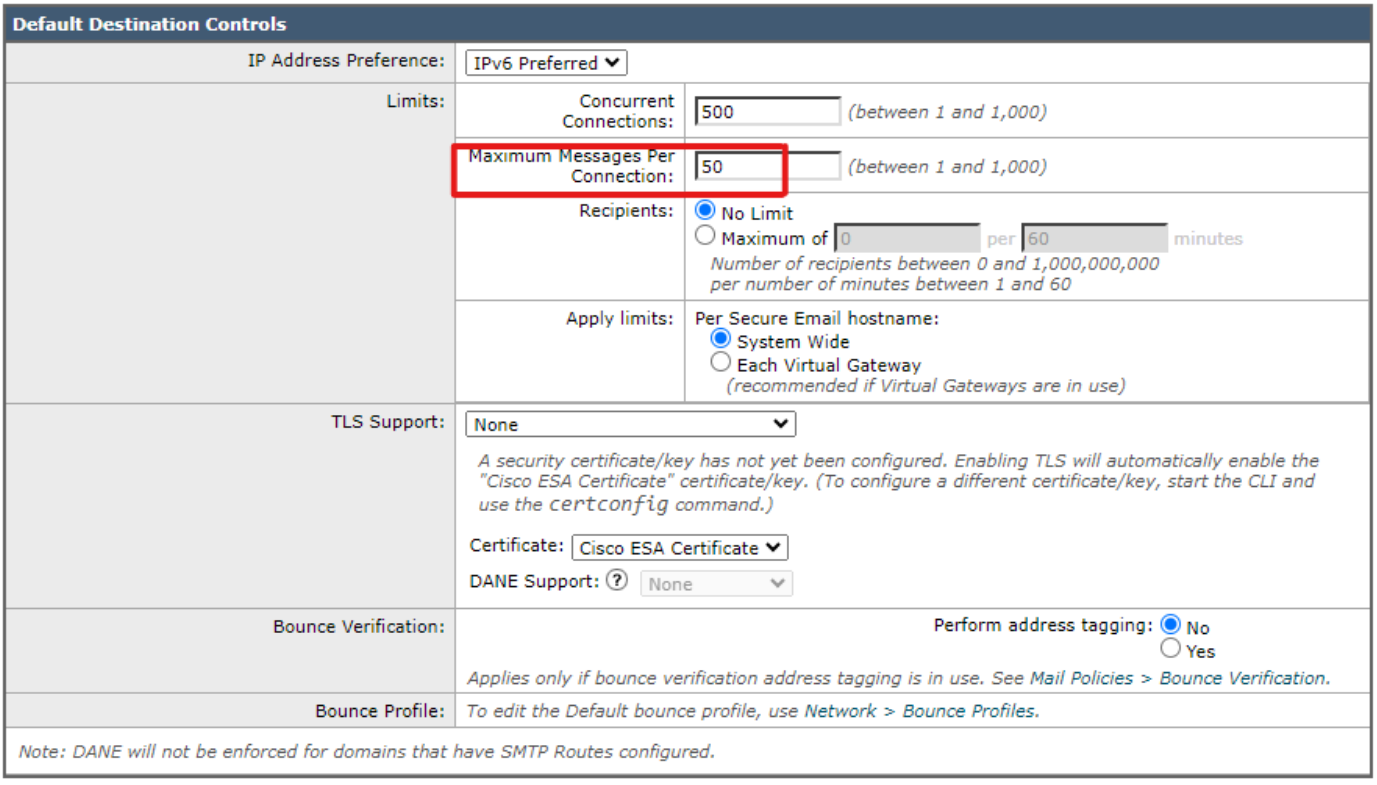
1. Öffnen Sie die GUI der CES/ESA-Appliance und navigieren Sie zu Mail Policies -> Destination Controls.

2. Klicken Sie auf Default settings.



Zielsteuerelementtabelle

3. Überprüfen Sie den Wert Maximum Messages Per Connection (Maximale Anzahl Nachrichten pro Verbindung).



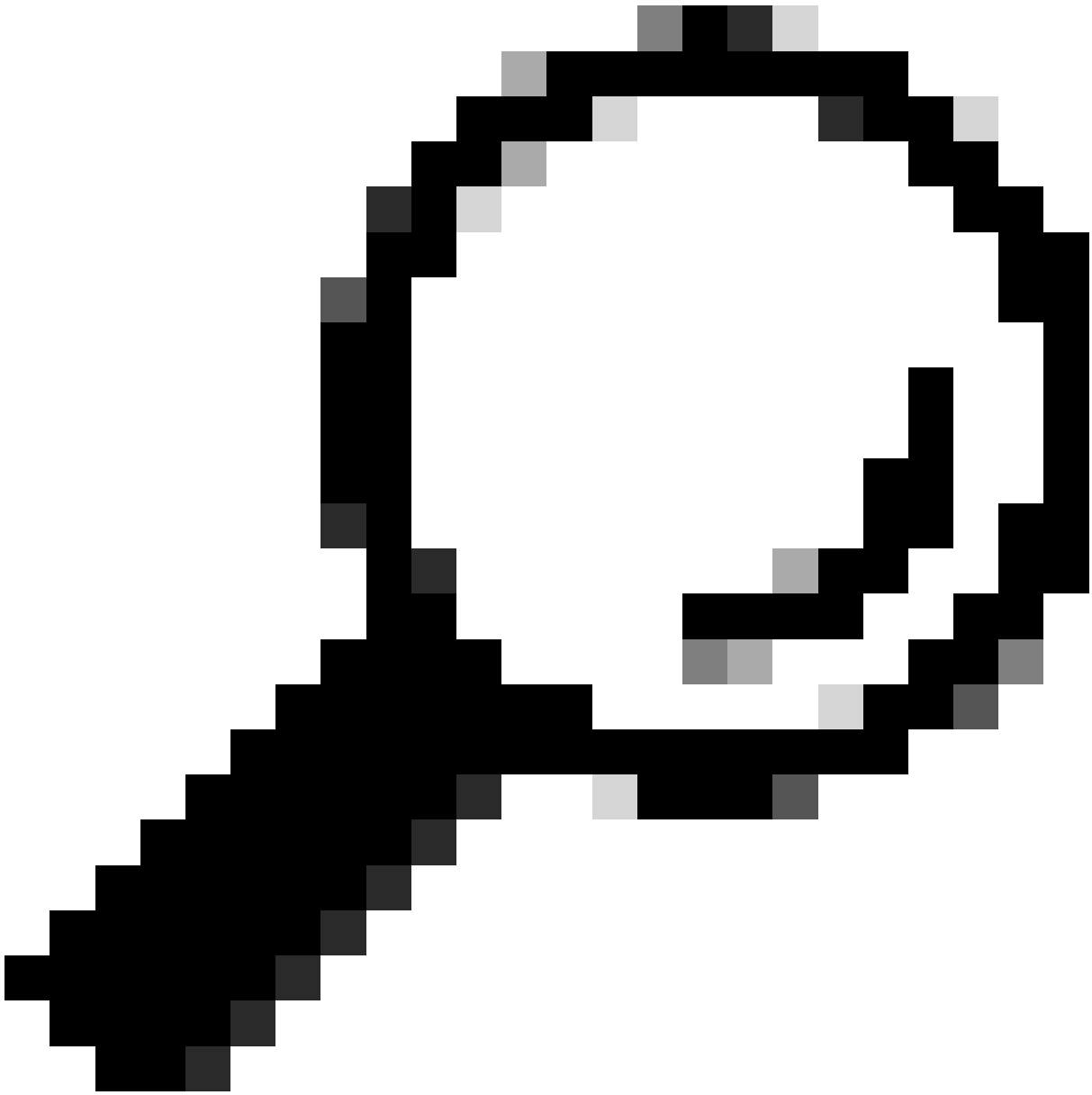
Standardzielsteuerelemente bearbeiten

4. Stellen Sie sicher, dass dieser Wert unter der Anzahl der im Skript festgelegten E-Mails liegt. Wenn das Skript beispielsweise so konfiguriert ist, dass 100 E-Mails gesendet werden, und die Appliance nur 50 Nachrichten pro Verbindung zulässt, werden übermäßige Verbindungen blockiert.

5. Führen Sie das Skript aus und beobachten Sie die Ergebnisse in Nachrichtenverfolgung.

6. Wenn mehr als 50 Verbindungen versucht werden, blockiert das System übermäßige E-Mails und protokolliert den Versuch als zu viele Verbindungen.

7. Ändern Sie das Skript, um weniger als 50 E-Mails zu senden, und stellen Sie sicher, dass alle E-Mails erfolgreich zugestellt wurden.



Tipp: Legen Sie für kontrollierte Tests den Bombingwert für E-Mails auf weniger als 10 fest. Selbst 50 E-Mails können als eine Art E-Mail-Bombenangriff angesehen werden. Passen Sie das Skript nach Bedarf an, um verschiedene Grenzwerte zu testen, ohne unbeabsichtigte Unterbrechungen zu verursachen.

Zugehörige Informationen

- Leitfaden zur Zielsteuerung der Cisco ESA
- Technischer Support und Downloads von Cisco

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.