使用邮件轰炸测试ESA中的目标控制

目录

简介

本文档介绍使用邮件轰炸测试ESA设备中的目标控制的过程。

先决条件

要求

Cisco 建议您了解以下主题：

- 思科安全邮件设备
- Python编程语言

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 思科安全邮件设备
- Python 3.X

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

ESA设备上的目标控制功能可控制邮件传送，防止收件人域过大。ESA允许定义设备可以打开的连接数以及发送到每个目标域的邮件数。目标控制表提供了将电子邮件传送到远程目标时的连接和消

息速率的设置，并且还包含用于强制使用TLS的选项。

有关目标控制的更多详细信息，请访问此处：退回验证和目标控制的最佳实践指南。

邮件炸弹是一种拒绝服务(DoS)攻击，旨在通过向特定收件人发送大量电子邮件来淹没收件箱或阻止服务器。此方法旨在使磁盘空间耗尽或使服务器过载，从而造成中断。

问题

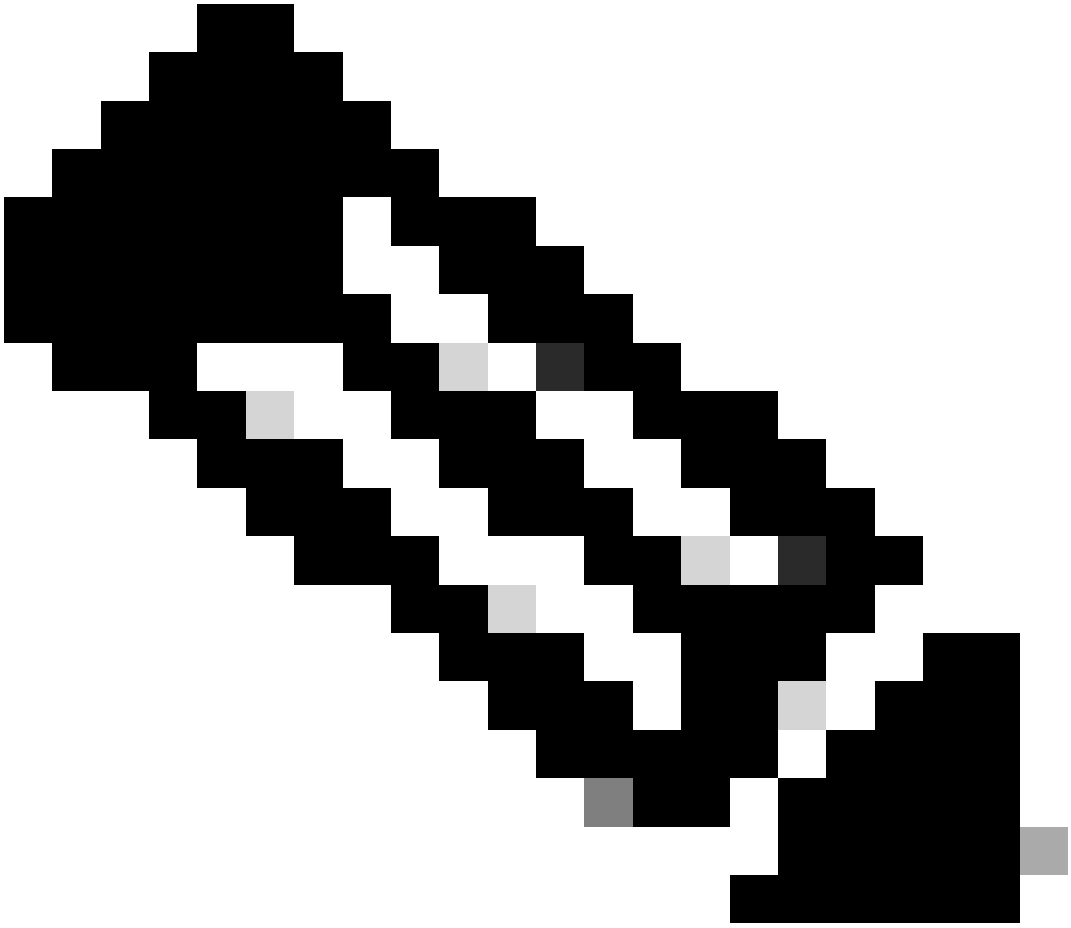
测试目标控制对防止邮件泛洪的有效性至关重要。如果没有正确的配置，过多的邮件传送尝试可能会使服务器不堪重负，导致性能下降或服务中断。

解决方案

Python脚本可用于模拟电子邮件炸弹并测试ESA设备上目标控制的效果。

邮件爆炸的Python脚本

```
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：您可以使用所需信息替换代码中的以下部分：

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

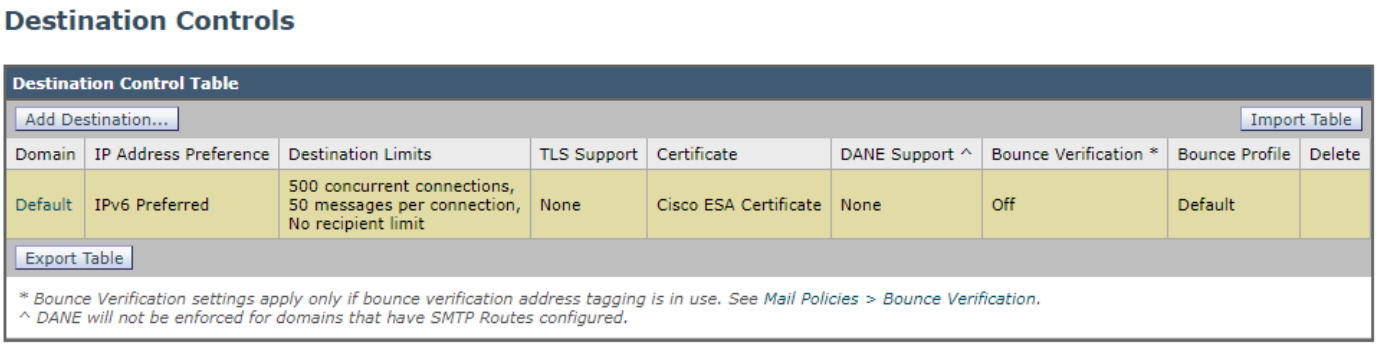
脚本细分

- 导入smtplib库以使用SMTP协议发送电子邮件。
- 主题和正文用于定义电子邮件内容。
- 服务器变量存储SMTP服务器详细信息，CES设备IP和端口25用于连接。
- while循环使用提供的发件人和收件人电子邮件地址发送99封电子邮件。
- server.quit()函数将终止与SMTP服务器的连接。

测试目标控制

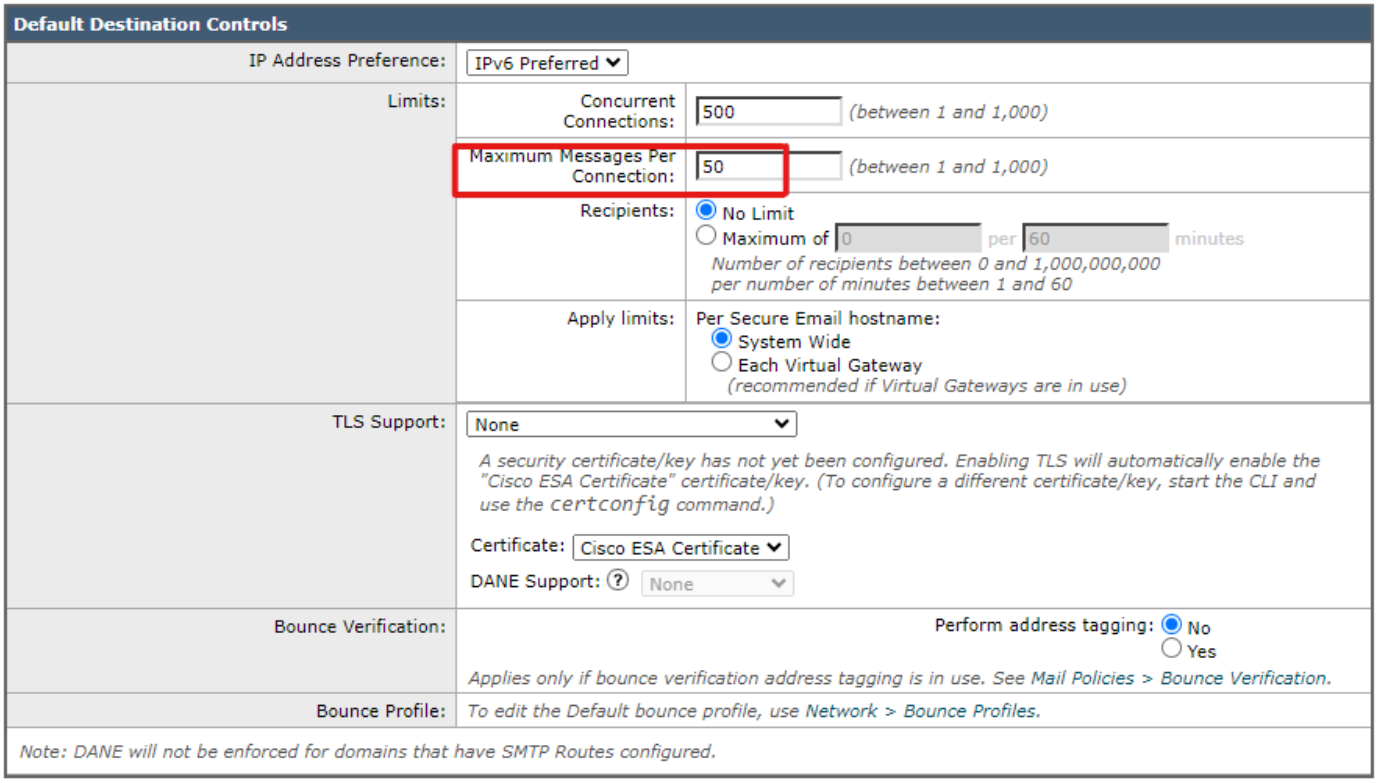
1.打开CES/ESA设备的GUI并导航至邮件策略 — >目标控制。

2.单击默认设置。



目标控制表

3.检查Maximum Messages Per Connection值。



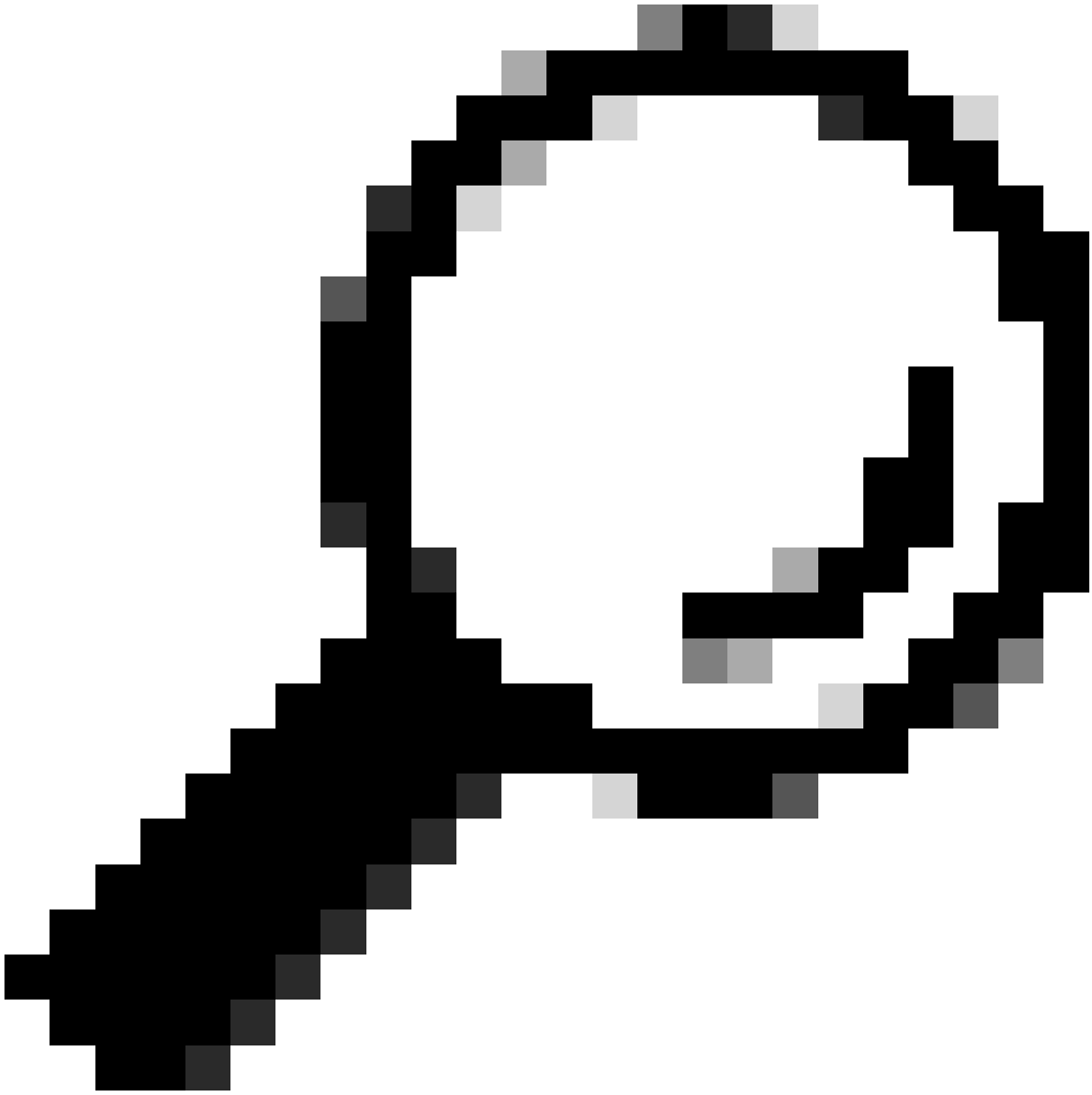
编辑默认目标控制

4.确保此值小于脚本中设置的电子邮件数量。例如，如果脚本配置为发送100封电子邮件，而设备只允许每个连接有50封邮件，则会阻止过多的连接。

5.执行脚本并观察邮件跟踪中的结果。

6.如果尝试的连接超过50个，系统会阻止过多的电子邮件，并将尝试记录为过多的连接。

7.修改脚本以发送少于50封电子邮件，并验证所有电子邮件是否已成功传送。



提示：对于受控测试，请将邮件爆炸值设置为少于10封邮件。甚至50封电邮也可能被视为一种电邮炸弹袭击形式。根据需要调整脚本，以测试不同的阈值，而不会造成意外中断。

相关信息

- 思科ESA目标控制指南
- 思科技术支持和下载

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。