이메일 폭격을 사용하여 ESA의 대상 제어 테스트

목차

[소개](#)

[사전 요구 사항](#)

- [요구 사항](#)
- [사용되는 구성 요소](#)

[배경 정보](#)

[문제](#)

[솔루션](#)

- [이메일 폭격을 위한 Python 스크립트](#)
- [스크립트 분류](#)

[대상 컨트롤 테스트](#)

[관련 정보](#)

소개

이 문서에서는 이메일 폭격을 사용하여 ESA 어플라이언스에서 대상 제어를 테스트하는 프로세스에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco Secure Email Appliance
- Python 프로그래밍 언어

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco Secure Email Appliance
- 파이썬 3.X

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

ESA 어플라이언스의 대상 컨트롤은 수신자 도메인이 너무 많아지지 않도록 이메일 전달을 제어합니다. ESA에서는 어플라이언스가 열 수 있는 연결 수 및 각 대상 도메인으로 전송되는 메시지 수를 정의할 수 있습니다. 대상 제어 테이블은 원격 대상에 전자 메일을 전달할 때 연결 및 메시지 속도 설정을 제공하며 TLS 사용을 적용하는 옵션도 포함합니다.

대상 제어에 대한 자세한 내용은 여기를 참조하십시오. 바운스 확인 및 대상 제어에 대한 모범 사례 가이드.

메일 폭탄은 특정 수신자에게 대량의 이메일을 전송하여 받은 편지함을 마비시키거나 서버를 억제하도록 설계된 일종의 DoS(서비스 거부) 공격입니다. 이 방법은 디스크 공간을 채우거나 서버를 과부하 시켜 중단을 일으키는 것을 목적으로 합니다.

문제

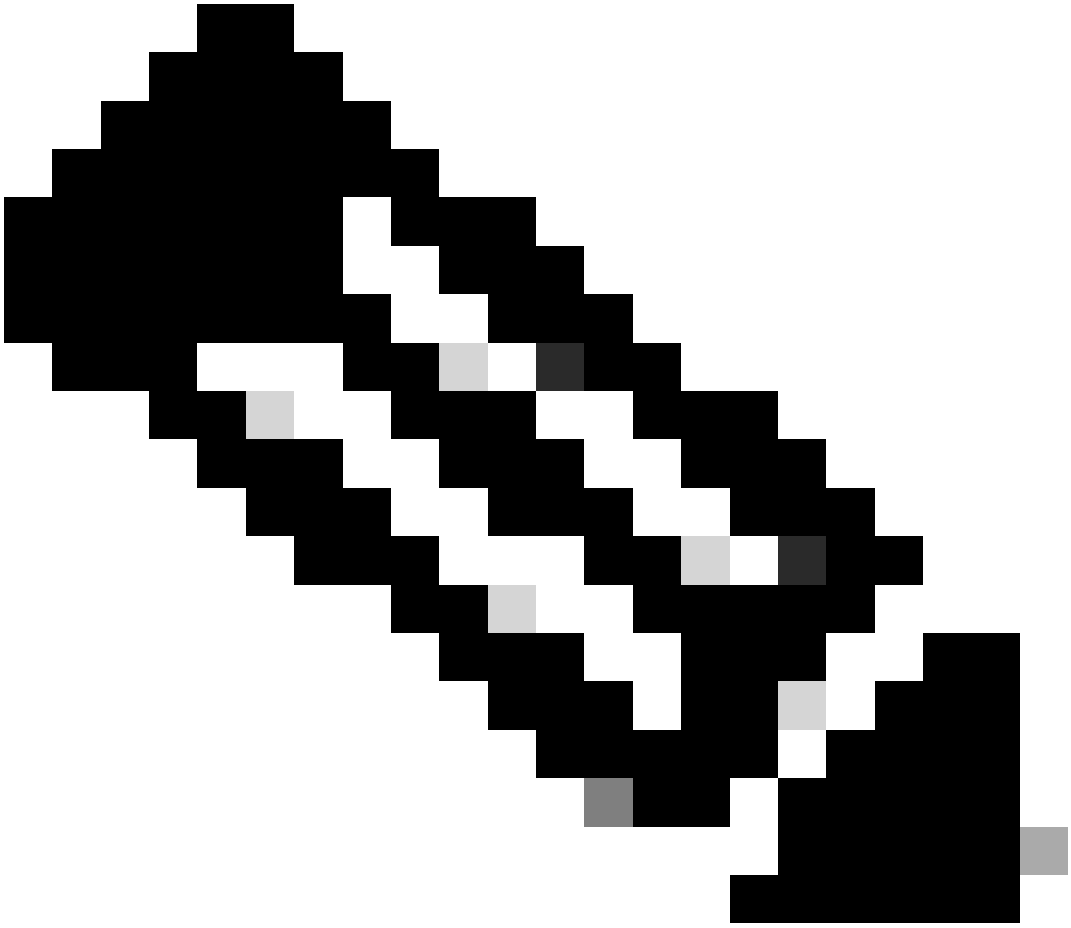
이메일 홍수를 방지하는 데 있어서 대상 제어의 효과를 테스트하는 것이 중요합니다. 적절한 구성이 없으면 과도한 이메일 전달 시도로 인해 서버가 마비되어 성능이 저하되거나 서비스가 중단될 수 있습니다.

솔루션

Python 스크립트를 사용하여 이메일 폭탄을 시뮬레이션하고 ESA 어플라이언스에서 대상 컨트롤의 유효성을 테스트할 수 있습니다.

이메일 폭격을 위한 Python 스크립트

```
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()
```



주: 코드의 다음 섹션을 필수 정보로 대체할 수 있습니다.

- XXX.XXX.XXX.XXX - ESA의 IP 주소입니다.
- SENDER_ADDR - 발신자 주소
- RECIPIENT_ADDR - 수신자 주소

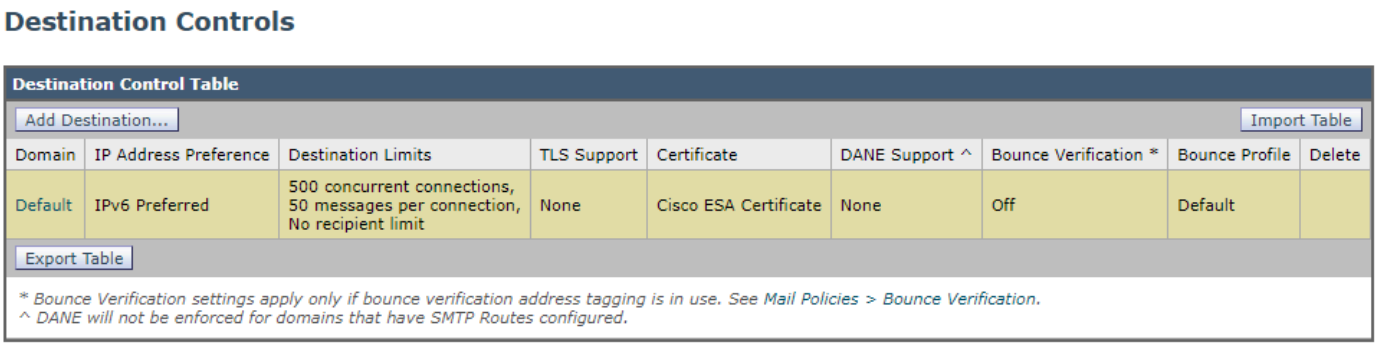
스크립트 분류

- SMTP 프로토콜을 사용하여 이메일을 보내기 위해 smtplib 라이브러리를 가져옵니다.
- 제목과 본문이 이메일 콘텐츠를 정의합니다.
- 서버 변수는 CES 어플라이언스 IP 및 연결용 포트 25와 함께 SMTP 서버 세부사항을 저장합니다.
- while 루프는 제공된 발신자 및 수신자 이메일 주소를 사용하여 99개의 이메일을 전송합니다.
- server.quit() 함수는 SMTP 서버와의 연결을 종료합니다.

대상 컨트롤 테스트

1. CES/ESA 어플라이언스의 GUI를 열고 Mail Policies(메일 정책) -> Destination Controls(대상 제어)로 이동합니다.

2. 기본 설정을 클릭합니다.



Destination Controls

Destination Control Table

Add Destination... | Import Table

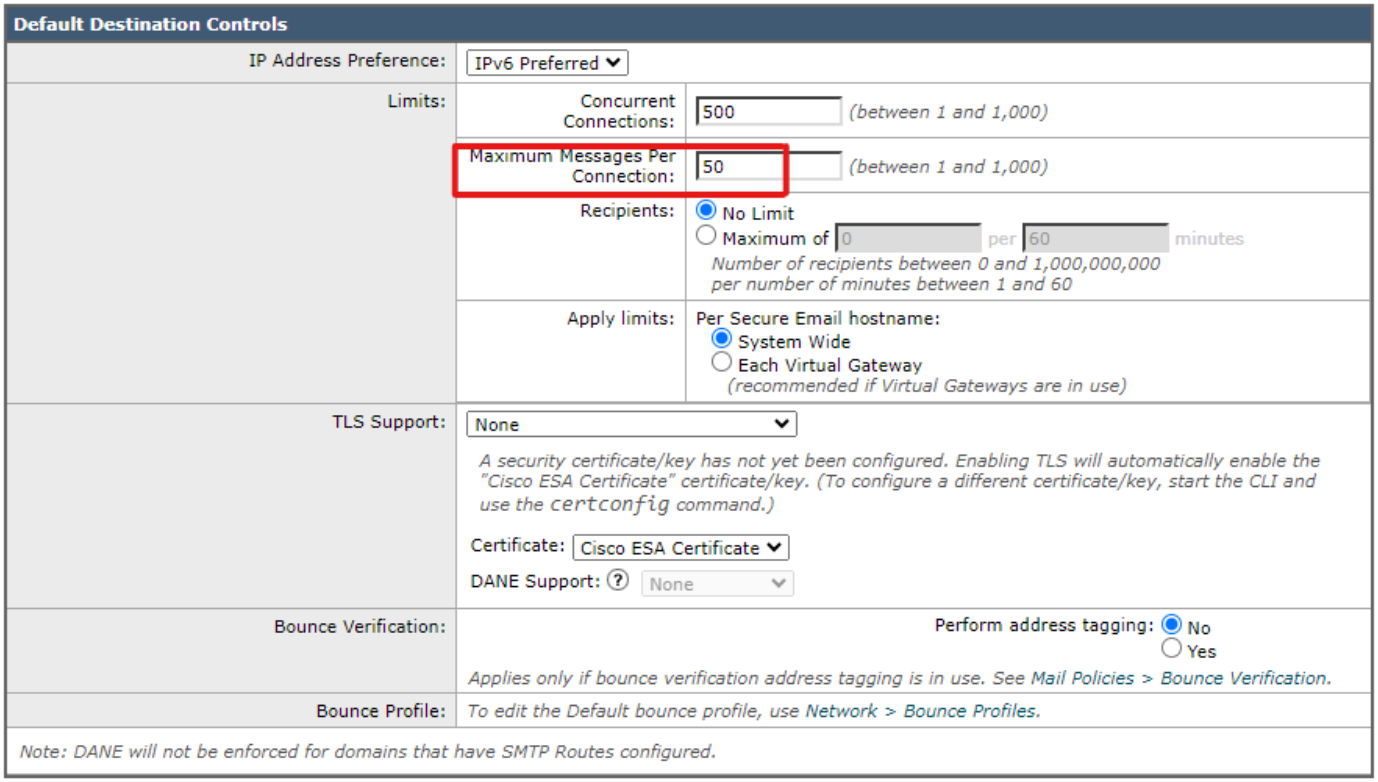
Domain	IP Address Preference	Destination Limits	TLS Support	Certificate	DANE Support ^	Bounce Verification *	Bounce Profile	Delete
Default	IPv6 Preferred	500 concurrent connections, 50 messages per connection, No recipient limit	None	Cisco ESA Certificate	None	Off	Default	

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.

대상 제어 테이블

3. Maximum Messages Per Connection 값을 확인합니다.



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.

기본 대상 컨트롤 편집

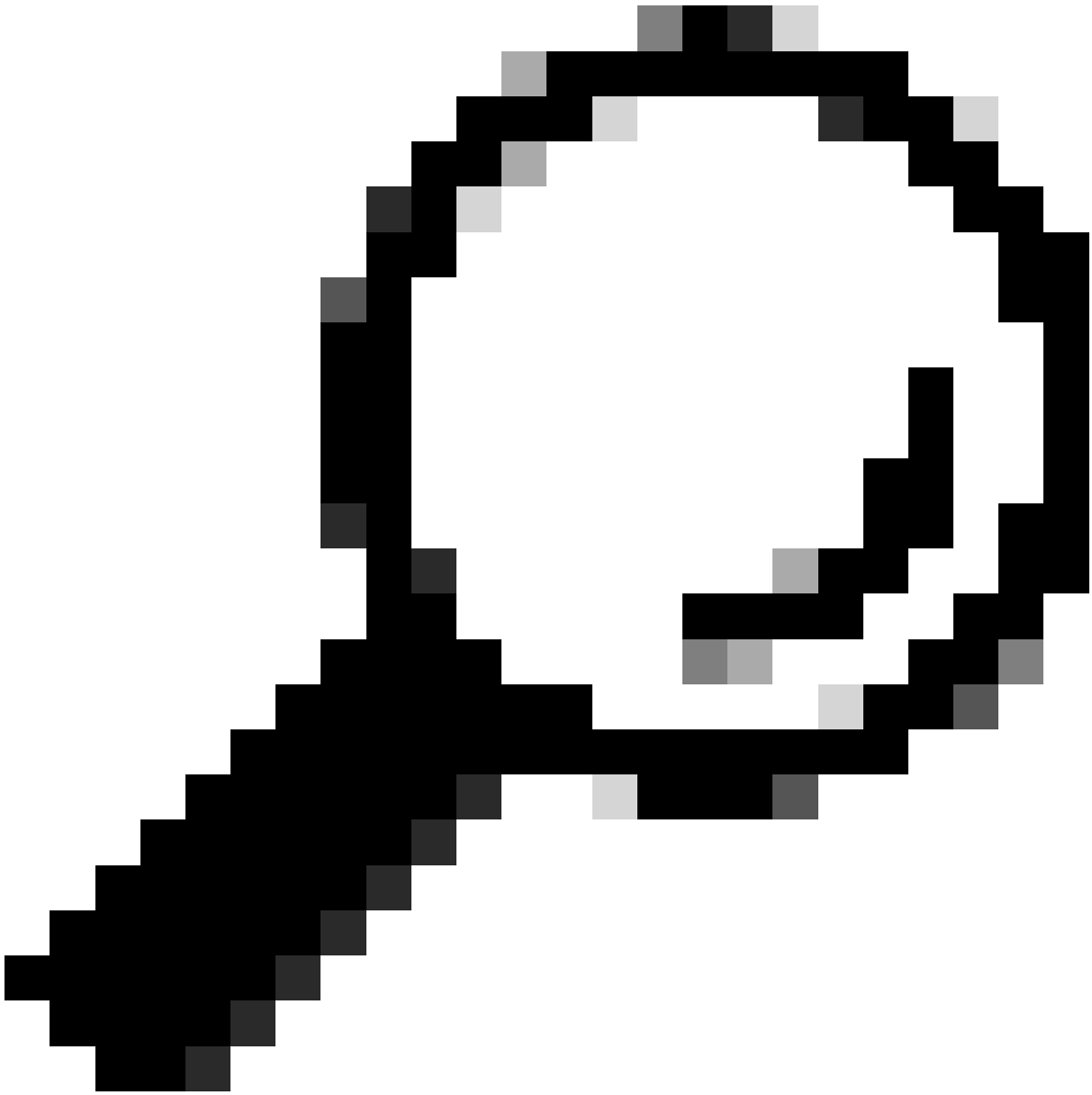
4. 이 값이 스크립트에 설정된 전자 메일 수보다 작은지 확인합니다. 예를 들어, 스크립트가 100개의 이메일을 전송하도록 구성되어 있고 어플라이언스에서 연결당 50개의 메시지만 허용할 경우 과도한 연결이 차단됩니다.

5. 스크립트를 실행하고 메시지 추적 결과를 확인합니다.

6. 50개 이상의 연결이 시도되면 과도한 이메일이 차단되고 너무 많은 연결로 기록됩니다.

7. 50개 미만의 전자 메일을 보내도록 스크립트를 수정하고 모든 전자 메일이 성공적으로 배달되었

는지 확인합니다.



팁: 제어된 테스트의 경우 이메일 폭격 값을 이메일 10개 미만으로 설정합니다. 심지어 50통의 이메일조차도 이메일 폭파의 한 형태로 간주될 수 있다. 필요에 따라 스크립트를 조정하여 의도하지 않은 중단을 유발하지 않고 서로 다른 임계값을 테스트합니다.

관련 정보

- Cisco ESA 대상 제어 가이드
- Cisco 기술 지원 및 다운로드

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.