

Bestemmingscontroles in ESE testen met e-mailbombardementen

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Probleem](#)

[Oplossing](#)

[Python Script voor e-mailbombardementen](#)

[Script-uitsplitsing](#)

[Bestemmingscontroles testen](#)

[Gerelateerde informatie](#)

Inleiding

In dit document wordt beschreven hoe de doelbesturingselementen in het ESA-apparaat worden getest met behulp van e-mail bombarderen.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco beveiligde e-mail applicatie
- Python-programmeertaal

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco beveiligde e-mail applicatie
- Python 3.X

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

Bestemmingscontroles op het ESA-apparaat regelen de e-maillevering om overweldigende ontvangerdomeinen te voorkomen. Met de ESA kunt u het aantal verbindingen definiëren dat door het apparaat kan worden geopend en het aantal berichten dat naar elk doeldomein wordt verzonden. De doelcontrolelijst biedt instellingen voor verbinding en berichtssnelheden bij het leveren van e-mails naar externe bestemmingen, en omvat ook opties voor het afdwingen van het gebruik van TLS.

Meer details over de controles op de bestemming vindt u hier: [Best Practice Guide voor Bounce Verification en Bestemmingscontroles](#).

Een mailbom is een type denial-of-service (DoS)-aanval die is ontworpen om een inbox te overweldigen of een server te remmen door een enorm aantal e-mails naar een specifieke ontvanger te sturen. Deze methode is bedoeld om schijfruimte te vullen of de server te overladen, wat verstoringen veroorzaakt.

Probleem

Het testen van de effectiviteit van bestemmingscontroles om overstromingen van e-mail te voorkomen is cruciaal. Zonder de juiste configuratie kunnen buitensporige pogingen om e-mail te bezorgen de server overweldigen, wat leidt tot verslechtering van de prestaties of onderbreking van de service.

Oplossing

Een Python-script kan worden gebruikt om een e-mailbom te simuleren en de effectiviteit van doelcontroles op het ESA apparaat te testen.

Python Script voor e-mailbombardementen

```
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()
```



Opmerking: U kunt deze secties van de code vervangen door de gewenste informatie:

- XXX.XXX.XXX.XXX - IP-adres van uw ESA.
- SENDER_ADDR - Adres afzender
- ONTVANGER_ADR. - Adres ontvanger

Script-uitsplitsing

- De smtplib-bibliotheek wordt geïmporteerd om e-mails te verzenden met behulp van het SMTP-protocol.
- Onderwerp en lichaam definiëren de e-mail content.
- De servervariabele slaat de SMTP-servergegevens op, met het CES-apparaat IP en poort 25 voor verbinding.
- De while loop verstuurt 99 e-mails met behulp van de opgegeven afzender en ontvangende e-mailadressen.
- De server.quit() functie beëindigt de verbinding met de SMTP server.

Bestemmingscontroles testen

1. Open de GUI van het CES/ESA apparaat en navigeer naar Mail Policies -> Bestemmingscontroles.

2. Klik op Standaardinstellingen.

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.								

Tabel Bestemmingscontroles

3. Controleer de waarde Maximum aantal berichten per verbinding.

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.	

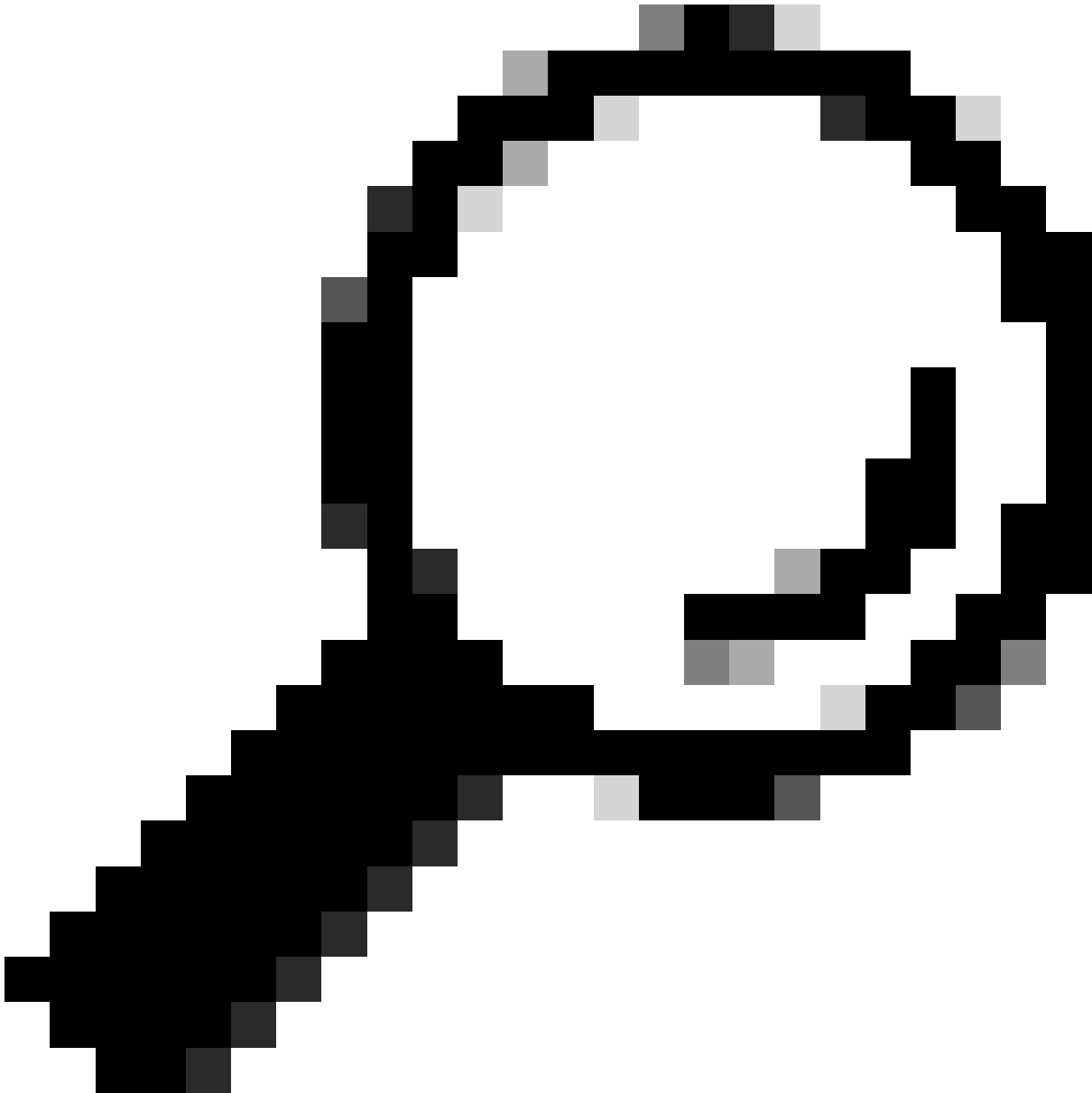
Standaarddoelbesturingselementen bewerken

4. Zorg ervoor dat deze waarde lager is dan het aantal e-mails dat in het script is ingesteld. Als het script bijvoorbeeld is ingesteld om 100 e-mails te verzenden en het apparaat slechts 50 berichten per verbinding toestaat, worden buitensporige verbindingen geblokkeerd.

5. Voer het script uit en bekijk de resultaten in Message Tracking.

6. Als meer dan 50 verbindingen worden geprobeerd, blokkeert het systeem overmatige e-mails en registreert de poging als teveel verbindingen.

7. Wijzig het script om minder dan 50 e-mails te verzenden en controleer of alle e-mails succesvol zijn afgeleverd.



Tip: Stel voor gecontroleerd testen de waarde van e-mailbombardementen in op minder dan 10 e-mails. Zelfs 50 e-mails kunnen worden beschouwd als een vorm van e-mailbombardementen. Pas het script naar behoefte aan om verschillende drempels te testen zonder onbedoelde onderbrekingen te veroorzaken.

Gerelateerde informatie

- [Cisco ESA-besturingshandleiding](#)
- [Cisco Technical Support en downloads](#)

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.