

Testar controles de destino no ESA usando bombardeio de e-mail

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Problema](#)

[Solução](#)

[Script Python para bombardeio de e-mail](#)

[Detalhamento do Script](#)

[Teste de controles de destino](#)

[Informações Relacionadas](#)

Introdução

Este documento descreve o processo de testar controles de destino no dispositivo ESA usando o bombardeio de e-mail.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Cisco Secure Email Appliance
- Linguagem de programação Python

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Cisco Secure Email Appliance
- Python 3. X

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

Os controles de destino no dispositivo ESA regulam a entrega de e-mail para evitar a sobrecarga dos domínios de destinatário. O ESA permite definir o número de conexões que o dispositivo pode abrir e o número de mensagens enviadas a cada domínio de destino. A tabela de controles de destino fornece configurações para taxas de conexão e de mensagens ao entregar emails a destinos remotos, além de incluir opções para impor o uso de TLS.

Mais detalhes sobre controles de destino podem ser encontrados aqui: [Guia de práticas recomendadas para verificação de devolução e controles de destino.](#)

Uma bomba de correio é um tipo de ataque de negação de serviço (DoS) projetado para sobrecarregar uma caixa de entrada ou inibir um servidor, enviando um grande número de e-mails para um destinatário específico. Esse método tem como objetivo ocupar espaço em disco ou sobrecarregar o servidor, causando interrupções.

Problema

Testar a eficácia dos controles de destino na prevenção da inundação de e-mails é crucial. Sem a configuração adequada, tentativas excessivas de entrega de e-mail podem sobrecarregar o servidor, levando à degradação do desempenho ou interrupção do serviço.

Solução

Um script Python pode ser usado para simular uma bomba de e-mail e testar a eficácia dos controles de destino no dispositivo ESA.

Script Python para bombardeio de e-mail

```
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()
```



Observação: você pode substituir essas seções do código pelas informações necessárias:

- XXX.XXX.XXX.XXX - endereço IP do seu ESA.
- SENDER_ADDR - Endereço do remetente
- RECIPIENT_ADDR - Endereço do destinatário

Detalhamento do Script

- A biblioteca smtplib é importada para enviar emails usando o protocolo SMTP.
- O assunto e o corpo definem o conteúdo do email.
- A variável de servidor armazena os detalhes do servidor SMTP, com o IP do equipamento CES e a porta 25 para conexão.
- O loop while envia 99 emails usando os endereços de email do remetente e do destinatário fornecidos.
- A função server.quit() termina a conexão com o servidor SMTP.

Teste de controles de destino

1. Abra a GUI do equipamento CES/ESA e navegue para Mail Policies -> Destination Controls.
2. Clique em Default settings.

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.								

Tabela de controles de destino

3. Verifique o valor de Máximo de Mensagens por Conexão.

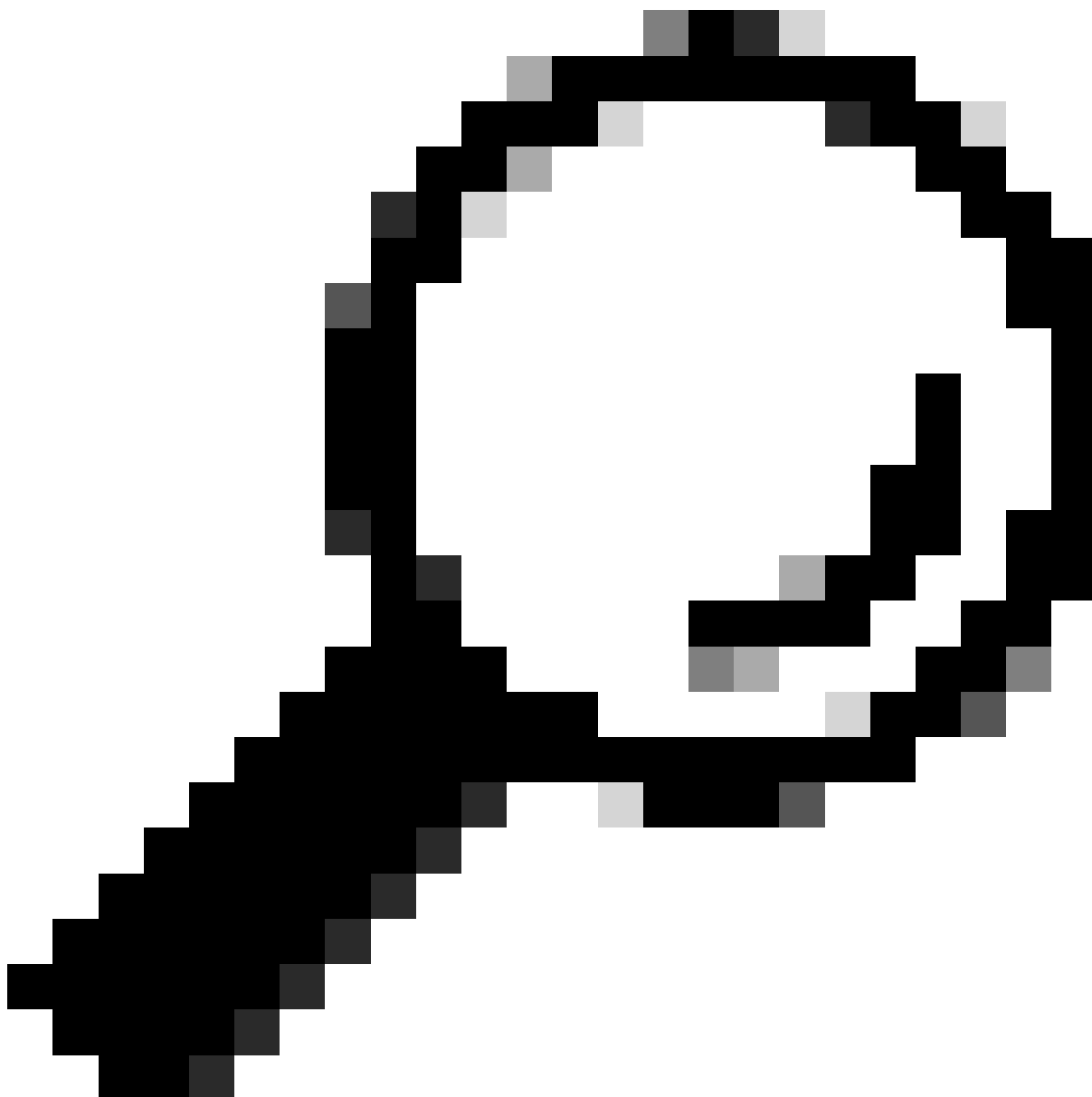
Default Destination Controls	
IP Address Preference:	IPv6 Preferred ▼
Limits:	Concurrent Connections: 500 (between 1 and 1,000) Maximum Messages Per Connection: 50 (between 1 and 1,000) Recipients: ☒ No Limit ☐ Maximum of 0 per 60 minutes Number of recipients between 0 and 1,000,000,000 per number of 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.	

Editar controles de destino padrão

4. Verifique se esse valor é inferior ao número de emails definido no script. Por exemplo, se o script estiver configurado para enviar 100 e-mails e o equipamento permitir apenas 50 mensagens por conexão, conexões excessivas serão bloqueadas.
5. Execute o script e observe os resultados em Rastreamento de Mensagem.
6. Se mais de 50 conexões forem tentadas, o sistema bloqueará o excesso de emails e registrará

a tentativa como muitas conexões.

7. Modifique o script para enviar menos de 50 emails e verifique se todos os emails foram entregues com êxito.



Tip: Para testes controlados, defina o valor de bombardeio de e-mail para menos de 10 e-mails. Até mesmo 50 e-mails podem ser considerados uma forma de bombardeio de e-mails. Ajuste o script conforme necessário para testar diferentes limites sem causar interrupções não intencionais.

Informações Relacionadas

- [Guia de controle de destino do Cisco ESA](#)
- [Suporte técnico e downloads da Cisco](#)

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.