Prueba de controles de destino en ESA mediante bombardeo de correo electrónico

Contenido

Introducción

Prerequisites

- Requirements
- Componentes Utilizados

Antecedentes

Problema

Solución

- Guión en Python para bombardeos de correo electrónico
- Desglose de scripts

Probar controles de destino

Información Relacionada

Introducción

Este documento describe el proceso de prueba de los controles de destino en el dispositivo ESA mediante Email Bombing.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Dispositivo Cisco Secure Email
- Lenguaje de programación Python

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Dispositivo Cisco Secure Email
- Python 3.X

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

Los controles de destino del dispositivo ESA regulan la entrega de correo electrónico para evitar que los dominios de los destinatarios se vean abrumados. El ESA permite definir el número de conexiones que el dispositivo puede abrir y el número de mensajes enviados a cada dominio de destino. La tabla de controles de destino proporciona la configuración de las velocidades de conexión y de mensajes cuando se entregan correos electrónicos a destinos remotos, y también incluye opciones para aplicar el uso de TLS.

Puede encontrar más información sobre los controles de destino aquí: Guía de prácticas recomendadas para la verificación de rebotes y los controles de destino.

Una bomba de correo electrónico es un tipo de ataque de denegación de servicio (DoS) diseñado para saturar una bandeja de entrada o inhibir un servidor mediante el envío de una cantidad masiva de correos electrónicos a un destinatario específico. Este método tiene como objetivo llenar espacio en disco o sobrecargar el servidor, lo que provoca interrupciones.

Problema

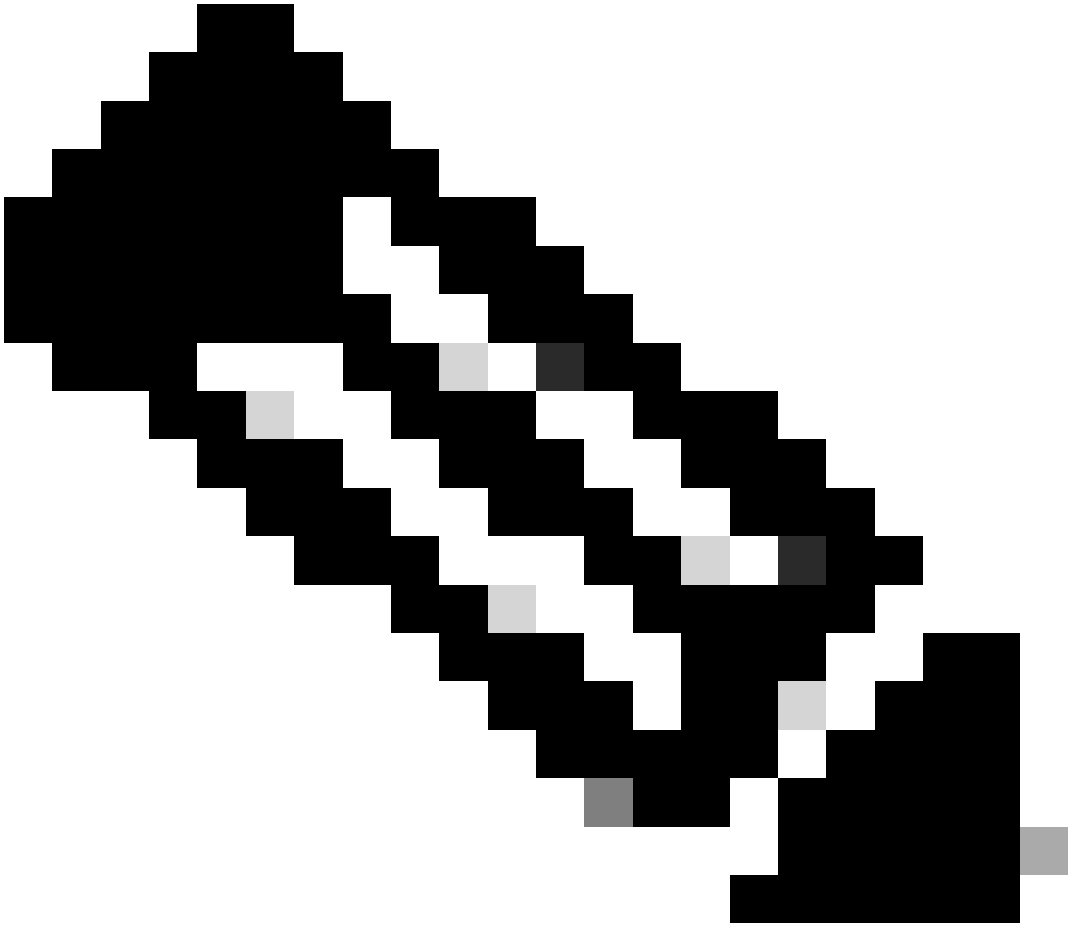
Es crucial probar la eficacia de los controles de destino para evitar la inundación de correos electrónicos. Sin una configuración adecuada, un número excesivo de intentos de entrega de correo electrónico puede saturar el servidor, lo que puede provocar una degradación del rendimiento o la interrupción del servicio.

Solución

Se puede utilizar un script Python para simular una bomba de correo electrónico y probar la eficacia de los controles de destino en el dispositivo ESA.

Guión en Python para bombardeos de correo electrónico

```
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()
```



Nota: Puede sustituir estas secciones del código por la información necesaria:

- XXX.XXX.XXX.XXX - Dirección IP de su ESA.
- SENDER_ADDR: Dirección del remitente
- RECIPIENT_ADDR: dirección del destinatario

Desglose de scripts

- La biblioteca smtplib se importa para enviar correos electrónicos mediante el protocolo SMTP.
- Asunto y cuerpo definen el contenido del correo electrónico.
- La variable de servidor almacena los detalles del servidor SMTP, con la IP del dispositivo CES y el puerto 25 para la conexión.
- El bucle while envía 99 mensajes de correo electrónico mediante las direcciones de correo electrónico de remitente y destinatario proporcionadas.
- La función server.quit() finaliza la conexión con el servidor SMTP.

Probar controles de destino

1. Abra la GUI del dispositivo CES/ESA y navegue hasta Políticas de correo -> Controles de destino.

2. Haga clic en 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.

Tabla de controles de destino

3. Compruebe el valor Máximo de mensajes por conexión.

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.

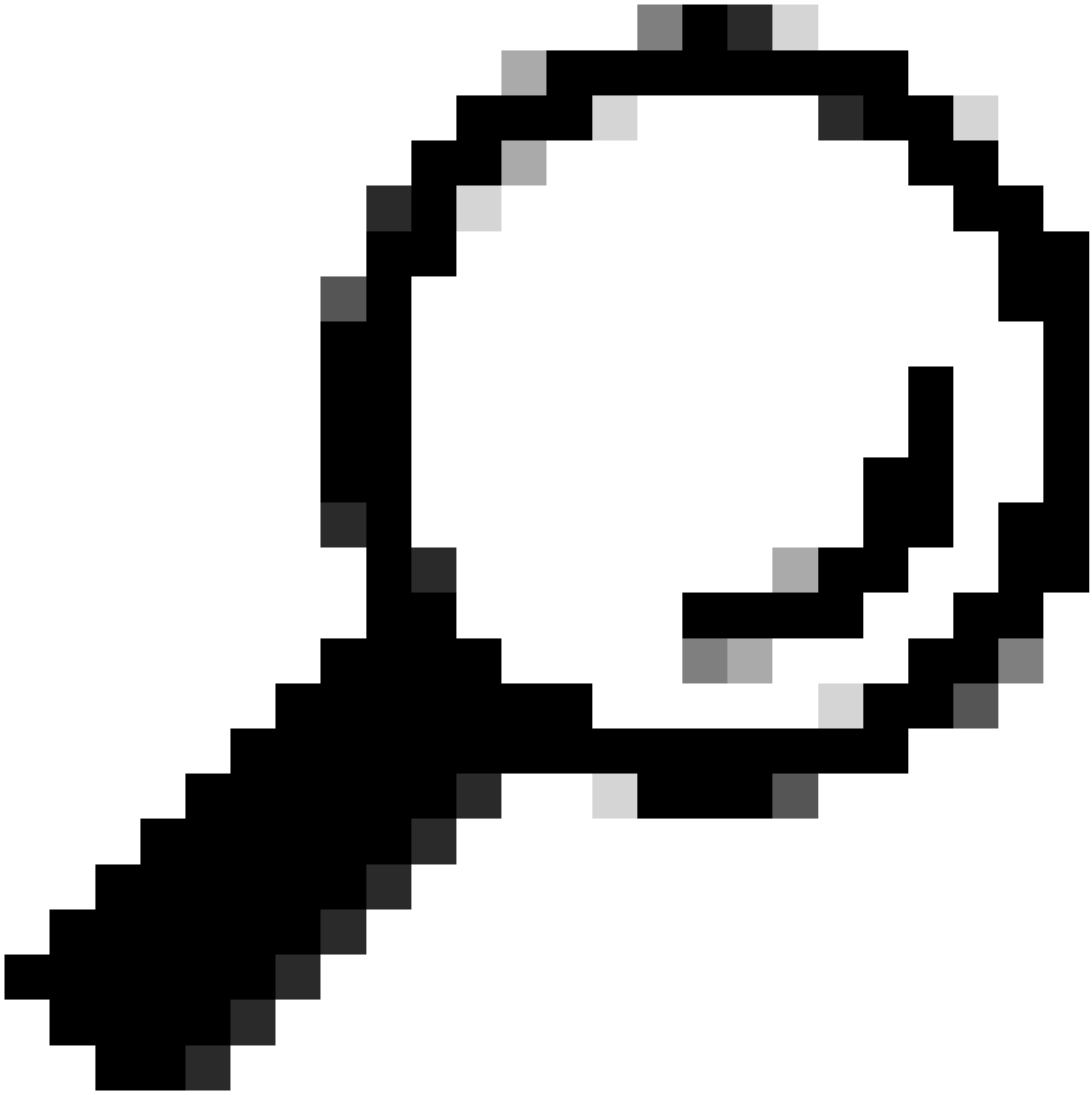
Editar controles de destino predeterminados

4. Asegúrese de que este valor sea inferior al número de correos electrónicos establecidos en el script. Por ejemplo, si el script se configura para enviar 100 correos electrónicos y el dispositivo solo permite 50 mensajes por conexión, se bloquearán conexiones excesivas.

5. Ejecute el script y observe los resultados en Rastreo de mensajes.

6. Si se intentan más de 50 conexiones, el sistema bloquea los correos electrónicos excesivos y registra el intento como demasiadas conexiones.

7. Modifique el guión para enviar menos de 50 correos electrónicos y compruebe que todos los correos electrónicos se han entregado correctamente.



Consejo: Para las pruebas controladas, establezca el valor de envío masivo de correos electrónicos en menos de 10 correos electrónicos. Incluso 50 correos electrónicos pueden ser considerados una forma de bombardeo de correo electrónico. Ajuste el script según sea necesario para probar diferentes umbrales sin causar interrupciones no deseadas.

Información Relacionada

- Guía de control de destino de Cisco ESA
- Soporte técnico y descargas de Cisco

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).