Test dei controlli di destinazione nell'ESA mediante bombardamento via e-mail

Sommario

Introduzione

Questo documento descrive il processo di test dei controlli di destinazione nell'appliance ESA utilizzando Email Bombing.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Cisco Secure Email Appliance
- Linguaggio di programmazione Python

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco Secure Email Appliance
- Python 3.X

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

I controlli di destinazione sull'appliance ESA regolano la consegna delle e-mail per evitare il sovraccarico dei domini dei destinatari. L'ESA consente di definire il numero di connessioni che l'accessorio può aprire e il numero di messaggi inviati a ciascun dominio di destinazione. La tabella dei controlli di destinazione fornisce le impostazioni per la velocità di connessione e dei messaggi durante il recapito dei messaggi di posta elettronica a destinazioni remote e include inoltre le opzioni per l'applicazione dell'utilizzo di TLS.

Per ulteriori informazioni sui controlli di destinazione, consultare: Guida alle procedure ottimali per la verifica dei rimbalzi e i controlli di destinazione.

Una mail bombing è un tipo di attacco DoS (Denial-of-Service) progettato per sopraffare una casella di posta in arrivo o inibire un server inviando un numero enorme di e-mail a un destinatario specifico. Questo metodo ha lo scopo di riempire lo spazio su disco o sovraccaricare il server, causando interruzioni.

Problema

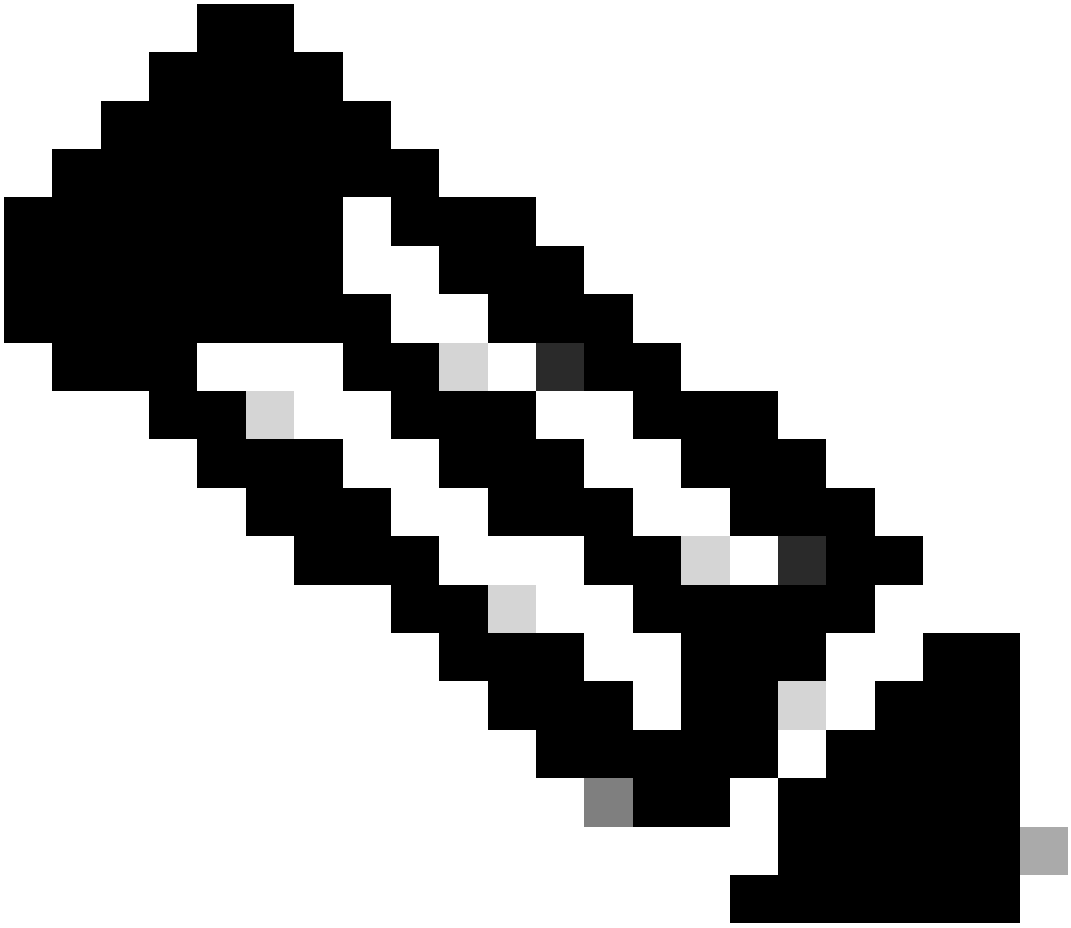
È fondamentale testare l'efficacia dei controlli di destinazione nel prevenire l'inondazione delle e-mail. Senza una corretta configurazione, un numero eccessivo di tentativi di consegna della posta elettronica può sovraccaricare il server, con conseguente riduzione delle prestazioni o interruzione del servizio.

Soluzione

Uno script Python può essere usato per simulare una bomba elettronica e testare l'efficacia dei controlli di destinazione sull'appliance ESA.

Script Python per e-mail bombing

```
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: è possibile sostituire queste sezioni del codice con le informazioni richieste:

- XXX.XXX.XXX.XXX - indirizzo IP dell'ESA.
- SENDER_ADDR - Indirizzo mittente
- RECIPIENT_ADDR - Indirizzo destinatario

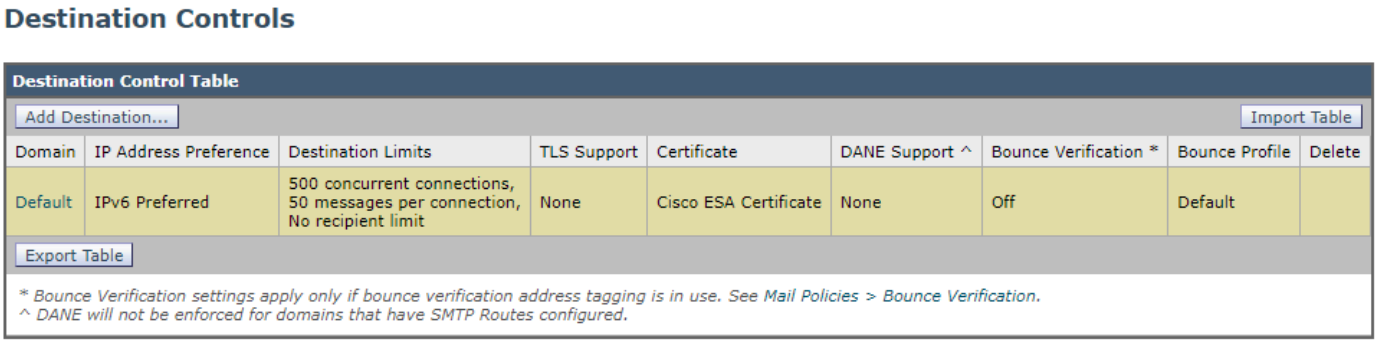
Analisi stratificata script

- La libreria smtplib viene importata per inviare e-mail utilizzando il protocollo SMTP.
- Oggetto e corpo definiscono il contenuto dell'e-mail.
- La variabile server memorizza i dettagli del server SMTP, con l'indirizzo IP dell'accessorio CES e la porta 25 per la connessione.
- Il ciclo while invia 99 messaggi di posta elettronica utilizzando gli indirizzi di posta elettronica del mittente e del destinatario specificati.
- La funzione server.quit() termina la connessione al server SMTP.

Verifica dei controlli di destinazione

1. Aprire la GUI dell'appliance CES/ESA e selezionare Mail Policies -> Destination Controls (Policy di posta -> Controlli destinazione).

2. Fare clic su Default settings (Impostazioni predefinite).



Destination Controls

Destination Control Table

Add Destination... | Import Table

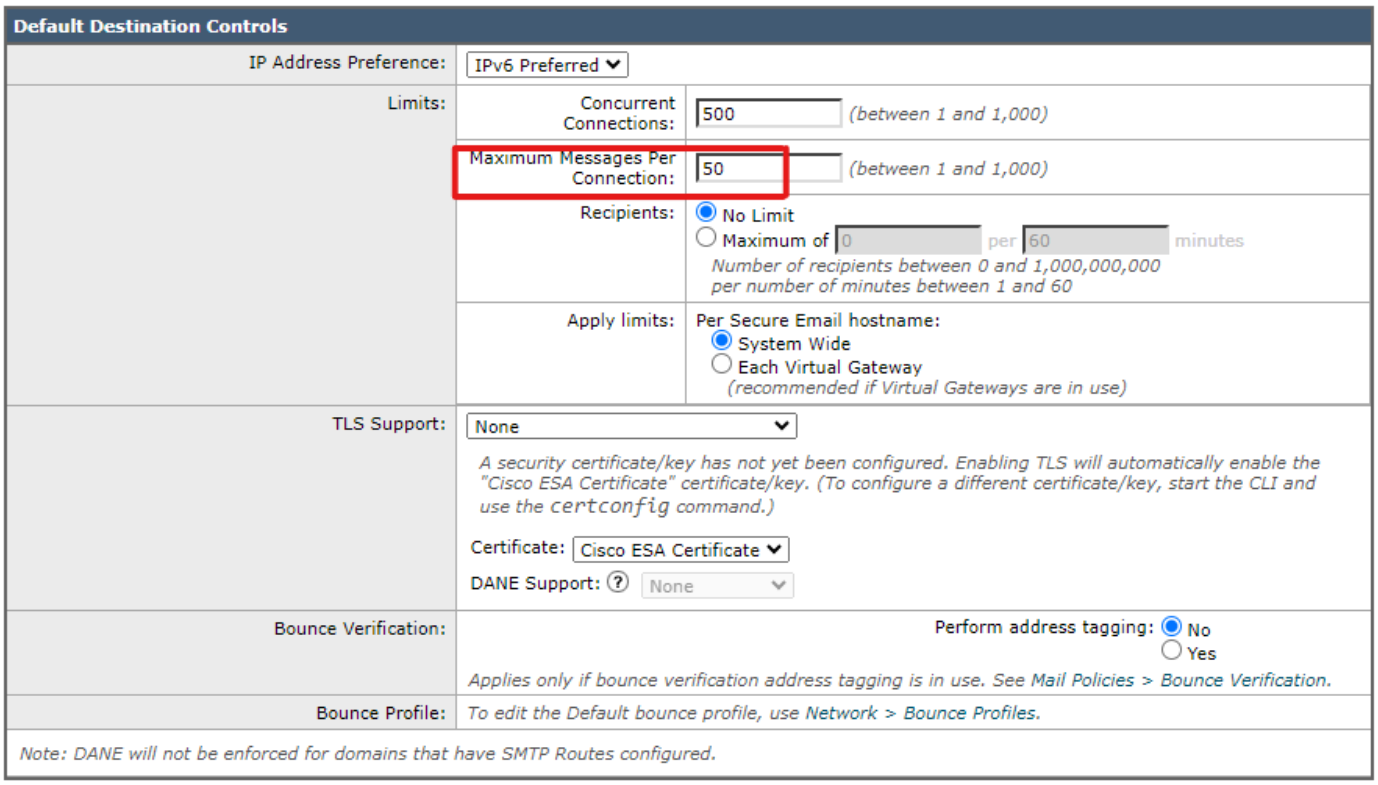
Domain	IP Address Preference	Destination Limits	TLS Support	Certificate	DANE Support ^	Bounce Verification *	Bounce Profile	Delete
Default	IPv6 Preferred	500 concurrent connections, 50 messages per connection, No recipient limit	None	Cisco ESA Certificate	None	Off	Default	

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.

Tabella Controlli destinazione

3. Controllare il valore Numero massimo di messaggi per connessione.



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.

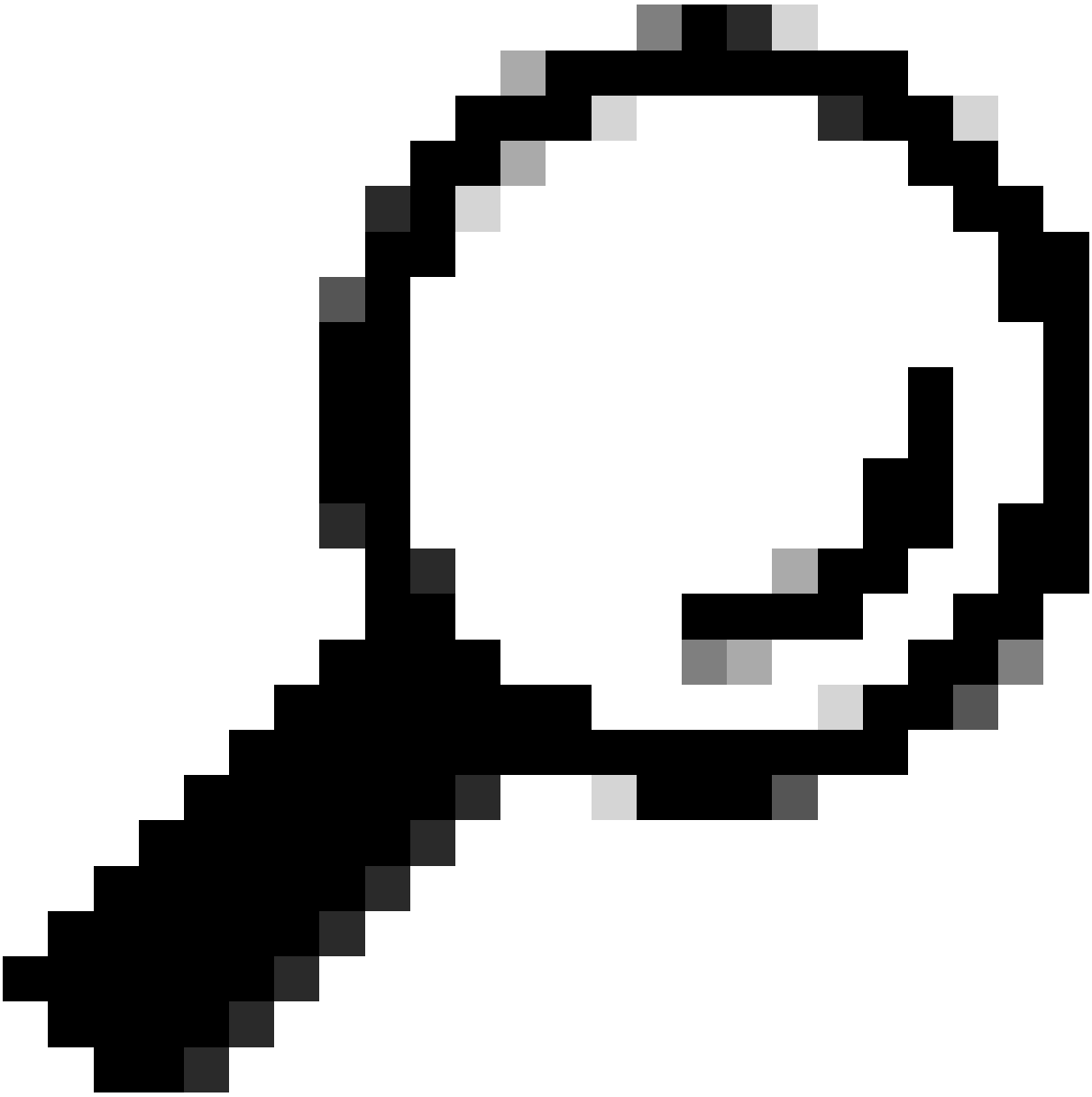
Modifica controlli di destinazione predefiniti

4. Verifica che questo valore sia inferiore al numero di messaggi di posta elettronica impostato nello script. Se ad esempio lo script è configurato per l'invio di 100 messaggi di posta elettronica e l'accessorio consente solo 50 messaggi per connessione, le connessioni eccessive verranno bloccate.

5. Eseguire lo script e osservare i risultati in Verifica messaggi.

6. Se vengono tentate più di 50 connessioni, il sistema blocca un numero eccessivo di e-mail e registra il tentativo come un numero eccessivo di connessioni.

7. Modifica lo script per inviare meno di 50 e-mail e verifica che tutti i messaggi siano stati recapitati correttamente.



Suggerimento: Per i test controllati, impostare il valore di email bombing su meno di 10 e-mail. Anche 50 email possono essere considerate una forma di email bombing. Regolare lo script in base alle esigenze per verificare soglie diverse senza causare interruzioni non intenzionali.

Informazioni correlate

- Cisco ESA Destination Control Guide
- Supporto tecnico Cisco e download

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).