Tester les contrôles de destination dans ESA en utilisant le bombardement de messagerie

Table des matières

Introduction

Ce document décrit le processus de test des contrôles de destination dans l'appliance ESA à l'aide du bombardement par e-mail.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Appareil de messagerie électronique sécurisé Cisco
- Langage de programmation Python

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Appareil de messagerie électronique sécurisé Cisco
- Python 3.X

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Informations générales

Les contrôles de destination sur l'appliance ESA réglementent la remise des e-mails pour éviter de submerger les domaines de destinataires. L'ESA permet de définir le nombre de connexions que la solution matérielle-logicielle peut ouvrir et le nombre de messages envoyés à chaque domaine de destination. Le tableau des contrôles de destination fournit des paramètres pour les taux de connexion et de messages lors de la remise de courriers électroniques à des destinations distantes, et inclut également des options pour imposer l'utilisation de TLS.

Pour plus d'informations sur les contrôles de destination, cliquez ici : Guide des meilleures pratiques pour la vérification de renvoi et les contrôles de destination.

Une bombe de messagerie est un type d'attaque par déni de service (DoS) conçu pour submerger une boîte de réception ou inhiber un serveur en envoyant un nombre massif d'e-mails à un destinataire spécifique. Cette méthode vise à remplir l'espace disque ou à surcharger le serveur, ce qui entraîne des interruptions.

Problème

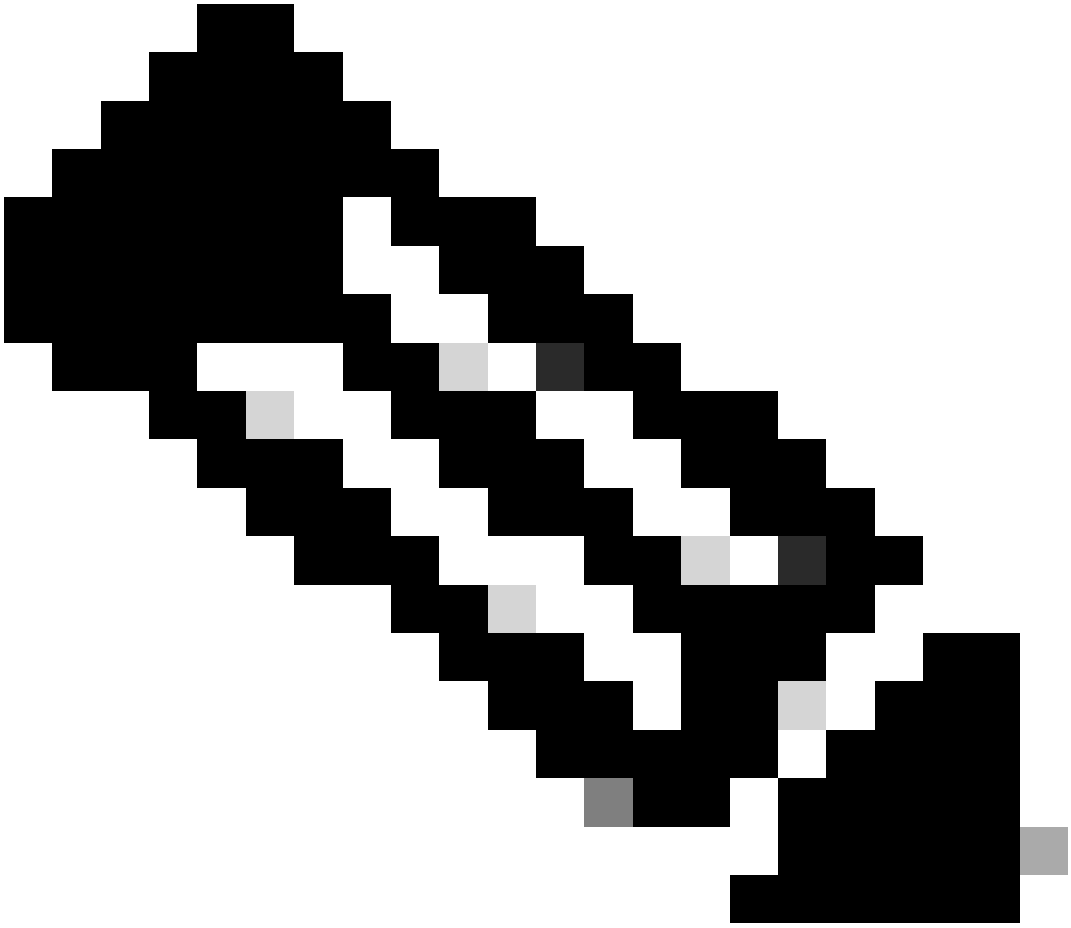
Il est essentiel de tester l'efficacité des contrôles de destination pour empêcher l'inondation des e-mails. Sans configuration appropriée, des tentatives excessives de remise d'e-mails peuvent submerger le serveur, entraînant une dégradation des performances ou une interruption du service.

Solution

Un script Python peut être utilisé pour simuler une bombe de messagerie et tester l'efficacité des contrôles de destination sur l'appliance ESA.

Script Python pour bombardement d'e-mails

```
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()
```



Remarque : vous pouvez remplacer ces sections du code par les informations requises :

- XXX.XXX.XXX.XXX - Adresse IP de votre ESA.
- SENDER_ADDR - Adresse de l'expéditeur
- RECIPIENT_ADDR - Adresse du destinataire

Ventilation du script

- La bibliothèque SMTP est importée pour envoyer des e-mails à l'aide du protocole SMTP.
- L'objet et le corps définissent le contenu du courrier électronique.
- La variable serveur stocke les détails du serveur SMTP, avec l'adresse IP de l'appliance CES et le port 25 pour la connexion.
- La boucle while envoie 99 e-mails en utilisant les adresses e-mail de l'expéditeur et du destinataire fournies.
- La fonction server.quit() met fin à la connexion au serveur SMTP.

Test des contrôles de destination

1. Ouvrez l'interface utilisateur graphique de l'appliance CES/ESA et accédez à Politiques de messagerie -> Contrôles de la destination.

2. Cliquez sur 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.

Tableau des contrôles de destination

3. Vérifiez la valeur Nombre maximal de messages par connexion.

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.

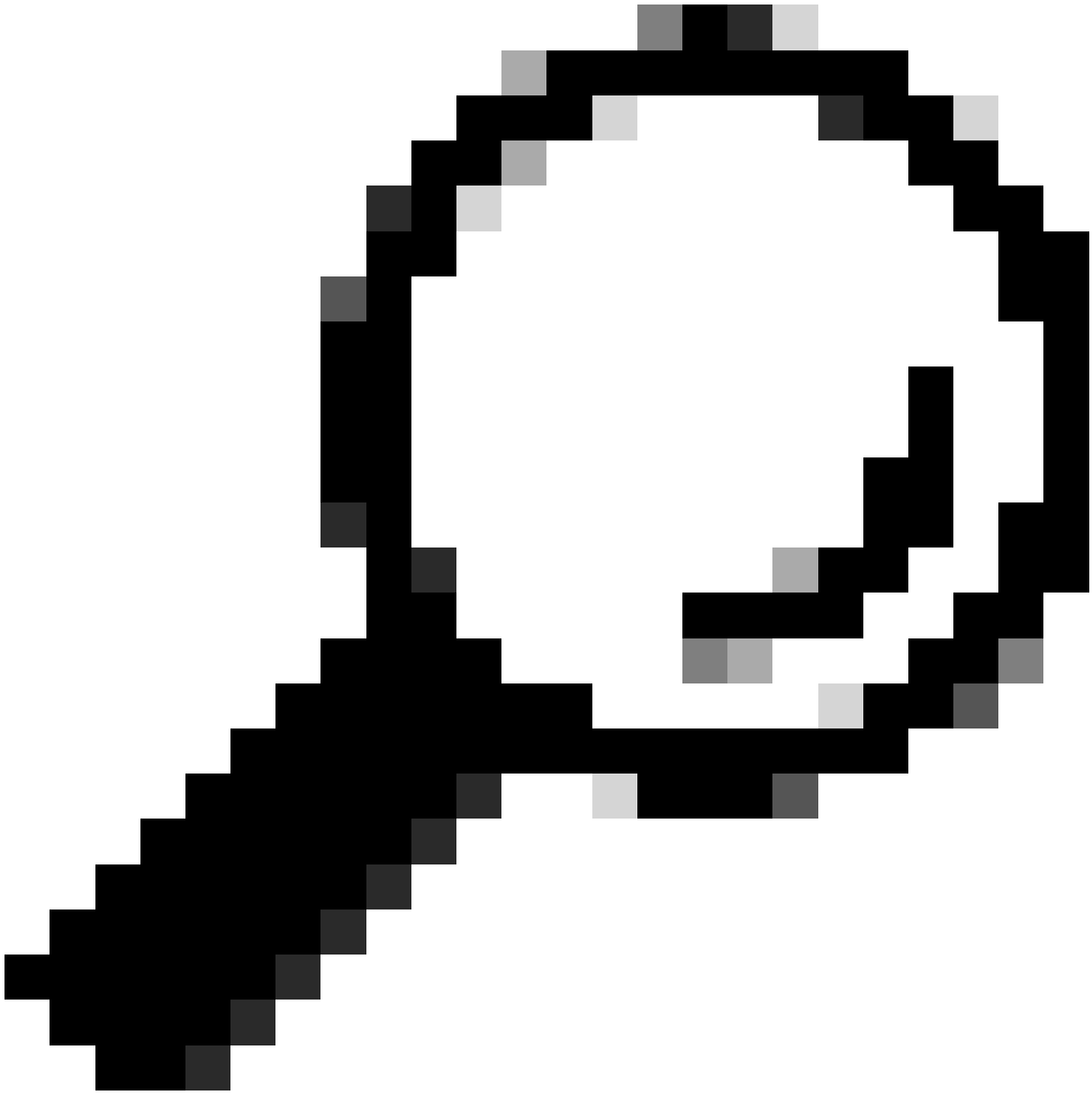
Modifier les contrôles de destination par défaut

4. Assurez-vous que cette valeur est inférieure au nombre d'e-mails défini dans le script. Par exemple, si le script est configuré pour envoyer 100 e-mails et que l'appliance n'autorise que 50 messages par connexion, les connexions excessives sont bloquées.

5. Exécutez le script et observez les résultats dans Suivi des messages.

6. Si plus de 50 connexions sont tentées, le système bloque les e-mails excessifs et consigne la tentative comme trop de connexions.

7. Modifiez le script pour envoyer moins de 50 e-mails et vérifiez que tous les e-mails ont bien été remis.



Conseil : Pour les tests contrôlés, définissez la valeur de bombardement des e-mails sur moins de 10 e-mails. Même 50 e-mails peuvent être considérés comme une forme de bombardement d'e-mails. Ajustez le script si nécessaire pour tester différents seuils sans provoquer d'interruptions involontaires.

Informations connexes

- Guide de contrôle de la destination Cisco ESA
- Assistance technique de Cisco et téléchargements

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.