FOIRE AUX QUESTIONS ESA : Quelle est une stratégie de flux de courrier ?

Contenu

Introduction

Ce document décrit ce qu'est une stratégie de flux de courrier sur l'appliance de sécurité du courrier électronique (ESA), et les actions qui sont associées à une stratégie de flux de courrier.

Quelle est une stratégie de flux de courrier ?

Une stratégie de flux de courrier te permet pour contrôler ou limiter l'écoulement des messages électroniques d'un expéditeur à l'auditeur pendant la conversation de SMTP. Vous contrôlez des conversations de SMTP en définissant les types suivants de paramètres dans la stratégie de flux de courrier :

- Paramètres de connexion, tels que le nombre maximal de messages par connexion.
- Paramètres de limitation de débit, tels que le nombre maximal de destinataires par heure.
- Modifiez les codes faits sur commande et les réponses de SMTP communiqués pendant la conversation de SMTP.
- Détection de Spam d'enable.
- Protection antivirus d'enable.
- Cryptage, tel qu'employer le TLS pour chiffrer la connexion de SMTP.
- Paramètres d'authentification, tels qu'employer DKIM pour vérifier la messagerie entrante.

Les stratégies de flux de courrier exécutent une des actions suivantes sur des connexions des serveurs distants :

- ACCEPT. La connexion est reçue, et l'acceptation d'email est alors davantage de restreinte par des configurations d'auditeur, y compris le Tableau réceptif d'Access (RAT) (pour les auditeurs publics).
- ANOMALIE. La connexion est au commencement reçue, mais le client tentant de se connecter obtient code d'état du SMTP 4XX ou 5XX. Aucun email n'est reçu.

  Note: Vous pouvez également configurer AsyncOS pour exécuter ce rejet au niveau de destinataire du message (RCPT À), plutôt qu'au début de la conversation de SMTP. Le rejet des messages de cette façon retarde le rejet de message et rebondit le message, permettant à AsyncOS pour retenir plus d'informations détaillées au sujet des messages

rejetés. Cette configuration est configurée du **listenerconfig > de la commande setup** CLI.

- TCPREFUSE. La connexion est refusée au niveau de TCP.
- RELAIS. La connexion est reçue. La réception pour n'importe quel destinataire est permise et n'est pas contrainte par le RAT.
- CONTINUEZ. Le mappage dans le Tableau d'accès au hôte (CHAPEAU) est ignoré, et traitement du CHAPEAU continue. Si la connexion entrante apparie une entrée postérieure qui n'est pas DE CONTINUER, cette entrée est utilisée à la place. La règle de CONTINUATION est utilisée de faciliter la retouche du CHAPEAU dans le GUI.

Maintenez dans l'esprit, les stratégies de flux de courrier sont au début du pipeline d'email, ainsi ces paramètres sont appliqués comme tentative de serveurs distants d'établir des connexions avec l'ESA.

Les stratégies de flux de courrier diffèrent des stratégies entrantes et de mail sortant, des lesquelles définissez l'anti-Spam, l'antivirus, l'attaque de virus, et les paramètres de filtre de contenu à appliquer pour envoyer par mail reçu ou destiné pour les domaines spécifiés, les groupes d'adresses e-mail ou les adresses e-mail de particularité.

Les stratégies par défaut de flux de courrier peuvent être modifiées et de nouvelles stratégies de flux de courrier peuvent être définies.

Il y a quatre stratégies par défaut de flux de courrier définies sur les auditeurs publics :

- REÇU
- BLOQUÉ
- ÉTRANGLÉ
- FAIT CONFIANCE

Les auditeurs privés utilisent les stratégies suivantes de flux de courrier :

- REÇU
- BLOQUÉ
- TRANSMIS PAR RELAIS

Informations connexes

- Appliance de sécurité du courrier électronique de Cisco - Guides d'utilisateur
- Support et documentation techniques - Cisco Systems