Configurez le TLS pour le cryptage de connexion entrante sur un auditeur ESA

Contenu

Introduction

Ce document décrit comment activer le Transport Layer Security (TLS) sur un auditeur sur l'appliance de sécurité du courrier électronique (ESA).

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

Les informations dans ce document sont basées sur l'ESA avec n'importe quelle version d'AsyncOS.

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Informations générales

Vous devez activer le TLS pour tous les auditeurs où vous avez besoin du cryptage pour des connexions entrantes. Vous pourriez vouloir activer le TLS sur les auditeurs qui font face à l'Internet (auditeurs publics), mais pas pour des auditeurs pour les systèmes internes (auditeurs privés). Ou, vous pourriez vouloir activer le cryptage pour tous les auditeurs. Par les auditeurs privés ni publics de par défaut, ni ne permettez les connexions de TLS. Vous devez permettre au TLS dans le Tableau de l'accès au hôte d'un auditeur (CHAPEAU) afin d'activer le TLS pour l'email (de envoi) d'arrivée (recevant) ou sortant. En outre, les paramètres de la stratégie de flux de courrier pour les auditeurs privés et publics ont "OFF" tourné par TLS par défaut.

Configurez

Vous pouvez spécifier trois configurations différentes pour le TLS sur un auditeur :

Établissement	Signification
Non	On ne permet pas le TLS pour les connexions entrantes. Les connexions à l'auditeur n'exig pas des conversations chiffrées de Protocole SMTP (Simple Mail Transfer Protocol). C'est valeur par défaut pour tous les auditeurs que vous configurez sur l'appliance.
Préféré	On permet le TLS pour les connexions entrantes à l'auditeur des messages transfer agent (MTA).
Requis	Le TLS est permis pour les connexions entrantes à l'auditeur des MTA, et jusqu'à STARTT une commande est reçue, l'ESA répond avec un message d'erreur à chaque commande a qu'aucune option (NOOP), EHLO, ou A QUITTÉ. Si le TLS « est exigé » il signifie que cet que l'expéditeur ne veut pas chiffré avec le TLS sera refusé par l'ESA avant qu'il dont soit envoyé, l'empêche de ce fait soit transmis en clair.

TLS d'enable sur une stratégie de flux de courrier de CHAPEAU pour un auditeur par l'intermédiaire du GUI

Procédez comme suit :

1. Du flux de courrier les stratégies paginent, choisissent un auditeur dont les stratégies vous voulez modifier et puis cliquez sur le lien pour le nom de la stratégie pour éditer. (Vous pouvez également éditer les paramètres de stratégie par défaut.) La page de stratégies de flux de courrier d'éditer est affichée.
2. Dans le « cryptage et l'authentification » section, pour le « TLS d'utilisation : le » champ, choisissent le niveau du TLS que vous voulez pour l'auditeur.
3. Cliquez sur **Submit**.
4. **Les modifications de validation de** clic, ajoutent un commentaire facultatif s'il y a lieu, et cliquent sur alors des **modifications de validation** afin de sauvegarder les modifications.

Note: Vous pouvez assigner un certificat spécifique pour des connexions de TLS à différents auditeurs publics quand vous créez un auditeur.

TLS d'enable sur une stratégie de flux de courrier de CHAPEAU pour un auditeur

par l'intermédiaire du CLI

1. Utilisez le **listenerconfig > éditent la** commande afin de choisir un auditeur que vous voulez configurer.
2. Utilisez les **hostaccess > la** commande de **par défaut** afin d'éditer les configurations par défaut du CHAPEAU de l'auditeur.
3. Écrivez un de ces choix afin de changer le TLS plaçant quand vous êtes incité :
```
Do you want to allow encrypted TLS connections?

   1. No
   2. Preferred
   3. Required
 [1]>3

You have chosen to enable TLS. Please use the 'certconfig' command to
ensure that there is a valid certificate configured.
```
Notez que cet exemple te demande d'employer la commande de **certconfig** afin de s'assurer qu'il y a un certificat valide qui peut être utilisé avec l'auditeur. Si vous n'avez créé aucun Certificats, l'auditeur utilise le certificat de démonstration qui est préinstallé sur l'appliance. Vous pouvez activer le TLS avec le certificat de démonstration afin de tester, mais il n'est pas sécurisé et n'est pas recommandé pour l'usage général. Utilisez le **listenerconfig > éditent >** commande de **certificat** afin d'assigner un certificat à l'auditeur.Une fois que vous avez configuré le TLS, la configuration est reflétée dans le résumé de l'auditeur dans le CLI :
```
Name: Inboundmail
Type: Public
Interface: PublicNet (192.168.2.1/24) TCP Port 25
Protocol: SMTP
Default Domain:
Max Concurrency: 1000 (TCP Queue: 50)
Domain map: disabled
TLS: Required
```
4. Sélectionnez la commande de **validation** afin d'activer la modification.

Vérifiez

Référez-vous à cette section pour vous assurer du bon fonctionnement de votre configuration.

- Utilisez le fichier journal de messagerie des textes et voyez le ce document : Déterminez si l'ESA utilise le TLS pour la livraison ou la réception
- Cheminement de message d'utilisation : GUI : Cheminement de moniteur > de message
- Signaler d'utilisation : GUI : Moniteur > connexions de TLS
- Utilisez un site Web de tiers tel que checktls.com

Dépannez

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

Vous pouvez spécifier si l'ESA envoie une alerte si la négociation de TLS échoue quand des messages sont fournis à un domaine qui exige une connexion de TLS. Le message d'alerte contient le nom du domaine de destination pour la négociation défectueuse de TLS. L'ESA envoie le message d'alerte à tous les destinataires réglés pour recevoir des alertes d'avertissement de

niveau d'importance pour des types d'alerte système. Vous pouvez gérer les destinataires vigilants par l'intermédiaire de la page d'administration système > d'alertes dans le GUI (ou par l'intermédiaire de la commande d'**alertconfig** dans le CLI).

Informations connexes

- L'utilisateur final guide AsyncOS pour l'email
- Support et documentation techniques - Cisco Systems