Configurez la version 1.0 de Transport Layer Security sur Cisco ESA et CES

Contenu

Introduction

Ce document décrit comment activer la version 1.0 (TLSv1.0) de Transport Layer Security sur l'appliance de sécurité du courrier électronique de Cisco (ESA) et Cisco opacifient des allocations de sécurité du courrier électronique (CES).

Comment pouvez-vous activer TLSv1.0 sur Cisco ESA et CES ?

> Remarque: Les allocations de CES de Cisco provisioned ont TLSv1.0 désactivé par défaut selon des exigences de sécurité dues aux incidences de vulnérabilité sur le protocole TLSv1.0. Ceci inclut la chaîne de chiffrement pour enlever toute l'utilisation de la suite de chiffrement partagée par SSLv3.

> **Attention** : Les méthodes et les chiffrements SSL/TLS sont réglés basés sur les stratégies de sécurité et les préférences spécifiques de votre société. Pour les tiers informations en vue de des chiffrements, document de Mozilla référez-vous de Sécurité/côté serveur à TLS pour des configurations du serveur et des informations détaillées recommandées.

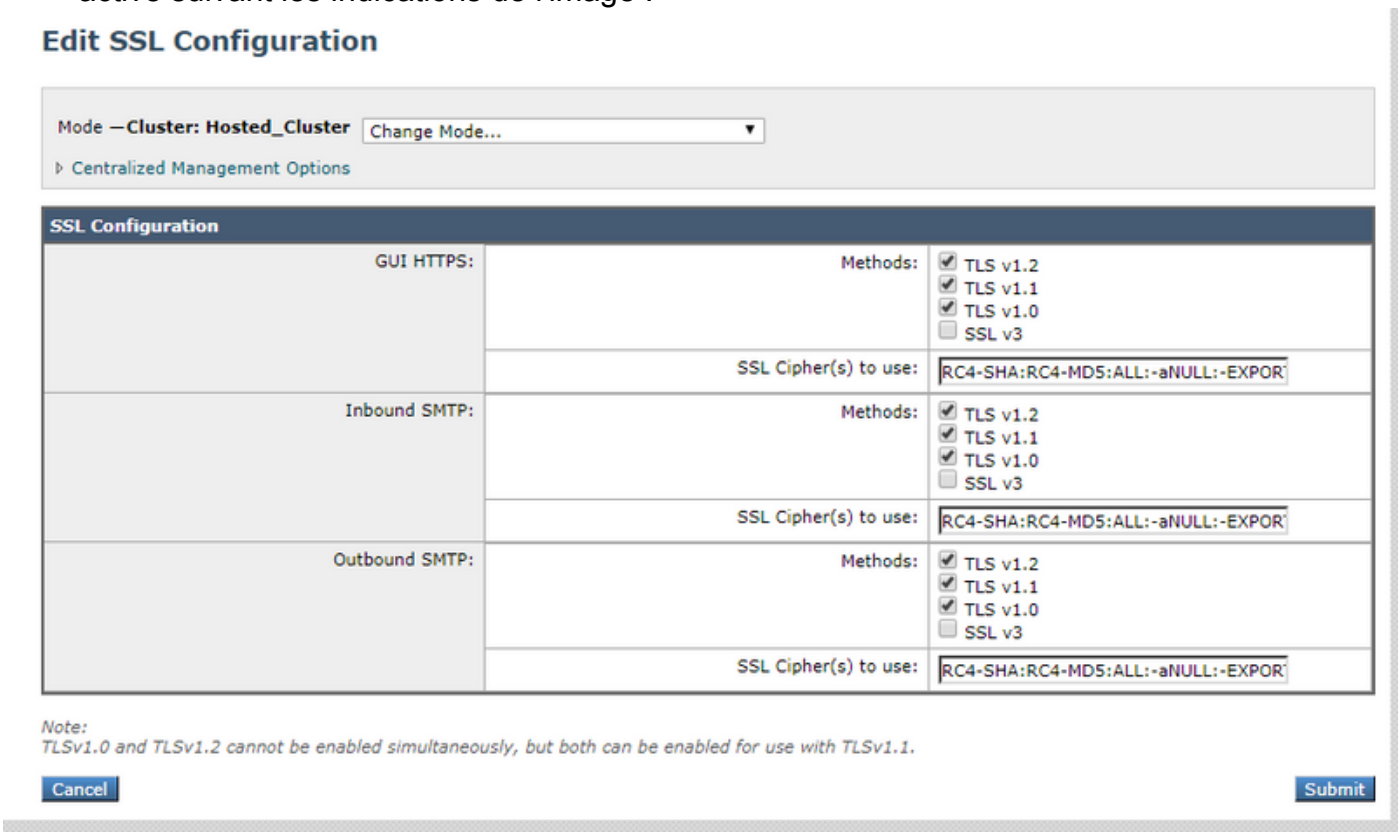
Afin d'activer TLSv1.0 sur votre Cisco ESA ou CES, vous pouvez faire ainsi de l'interface utilisateur graphique (GUI) ou de l'interface de ligne de commande (CLI).

> Remarque: Afin d'obtenir l'accès à votre CES sur le CLI passez en revue s'il vous plaît : Accéder à l'interface de ligne de commande (CLI) de votre solution de sécurité du courrier électronique de nuage (CES)

Interface utilisateur graphique

1. Connectez-vous dans le GUI.
2. Naviguez vers l'**administration système > la configuration SSL**.
3. Choisi **éditez les configurations**.
4. Cochez la case **TLSv1.0**. Il est important de noter que TLSv1.2 et ne peut pas être activé en

même temps que TLSv1.0 à moins que le protocole de pontage TLSv1.1 soit également activé suivant les indications de l'image :



Interface de ligne de commande

1. Exécutez le **sslconfig de** commande.
2. Exécutez le **GUI de** commande ou **D'ARRIVÉE** ou **SORTANT** selon pour quel élément vous voulez activer TLSv1.0 :

```
(Cluster Hosted_Cluster)> sslconfig

sslconfig settings:
GUI HTTPS method: tlsv1_2
GUI HTTPS ciphers:
RC4-SHA
RC4-MD5
ALL
-aNULL
-EXPORT
Inbound SMTP method: tlsv1_2
Inbound SMTP ciphers:
RC4-SHA
RC4-MD5
ALL
-aNULL
-EXPORT
Outbound SMTP method: tlsv1_2
Outbound SMTP ciphers:
RC4-SHA
RC4-MD5
ALL
-aNULL
-EXPORT
```

```
Choose the operation you want to perform:
- GUI - Edit GUI HTTPS ssl settings.
- INBOUND - Edit Inbound SMTP ssl settings.
- OUTBOUND - Edit Outbound SMTP ssl settings.
- VERIFY - Verify and show ssl cipher list.
- CLUSTERSET - Set how ssl settings are configured in a cluster.
- CLUSTERSHOW - Display how ssl settings are configured in a cluster.
[]> INBOUND

Enter the inbound SMTP ssl method you want to use.
1. TLS v1.0
2. TLS v1.1
3. TLS v1.2
4. SSL v2
5. SSL v3
[3]> 1-3

Enter the inbound SMTP ssl cipher you want to use.
[RC4-SHA:RC4-MD5:ALL:-aNULL:-EXPORT]>
```

Chiffrements

Il peut être configuré avec les suites strictes de chiffrement, il est importante assurer des allocations d'ESAs et de CES que les chiffrements SSLv3 ne sont pas bloqués quand vous activez le protocole TLSv1.0. Le manque de permettre les suites du chiffrement SSLv3 ont comme conséquence des pannes de négociation de TLS ou des fermetures brusques de connexion de TLS.

Chaîne de chiffrement d'échantillon :

```
HIGH:MEDIUM:@STRENGTH:!aNULL:!eNULL:!LOW:!DES:!MD5:!EXP:!PSK:!DSS:!RC2:!RC4:!SEED:!ECDSA:!ADH:!I
DEA:!3DES:!SSLv2:!SSLv3:!TLSv1:-aNULL:-EXPORT:-IDEA
```

Cette chaîne de chiffrement arrête l'ESA/CES de permettre la négociation sur les chiffrements SSLv3 comme indiqué en fonction **! SSLv3 : ,** ceci signifie quand le protocole est demandé dans la prise de contact, la prise de contact SSL échoue car il n'y a aucun chiffrement partagé disponible pour la négociation.

Afin d'assurer les fonctions de chaîne de chiffrement d'échantillon avec TLSv1.0, il doit être modifié pour retirer **! SSLv3:!TLSv1 :** vu dans la chaîne remplacée de chiffrement :

```
HIGH:MEDIUM:@STRENGTH:!aNULL:!eNULL:!LOW:!DES:!MD5:!EXP:!PSK:!DSS:!RC2:!RC4:!SEED:!ECDSA:!ADH:!I
DEA:!3DES:!SSLv2:-aNULL:-EXPORT:-IDEA
```

> Remarque: Vous pouvez vérifier les suites de chiffrement partagées sur la prise de contact SSL sur l'ESA/CES CLI avec la commande de **VÉRIFIER**.

Les erreurs possibles ont ouvert une session les mail_logs/message dépistant mais non limité à :

```
Sun Feb 23 10:07:07 2020 Info: DCID 1407038 TLS failed: (336032784, 'error:14077410:SSL
routines:SSL23_GET_SERVER_HELLO:sslv3 alert handshake failure')
Sun Feb 23 10:38:56 2020 Info: DCID 1407763 TLS failed: (336032002, 'error:14077102:SSL
routines:SSL23_GET_SERVER_HELLO:unsupported protocol')
```

Informations connexes

- Modifiez les méthodes et les chiffrements utilisés avec SSL/TLS sur l'ESA
- Détails de point fort de chiffrement SSL
- Guide complet d'installation pour le TLS sur l'ESA
- Support et documentation techniques - Cisco Systems