Configuratie van Transport Layer Security versie 1.0 op Cisco ESA en CES

Inhoud

Inleiding

Dit document beschrijft hoe u transportlaag security versie 1.0 (TLSv1.0) kunt inschakelen voor de Cisco e-mail security applicatie (ESA) en Cisco Cloud Email Security (CES)-toewijzingen.

Hoe kunt u TLSv1.0 inschakelen op Cisco ESA en CES?

> Opmerking: De toewijzing van Cisco CES waarvoor voorzieningen zijn getroffen heeft TLSv1.0 standaard uitgeschakeld als gevolg van de beveiligingsvereisten als gevolg van kwetsbaarheidseffecten op het TLSv1.0-protocol. Dit omvat de string van het algoritme om al gebruik van de SSLv3 gedeelde algoritme te verwijderen.

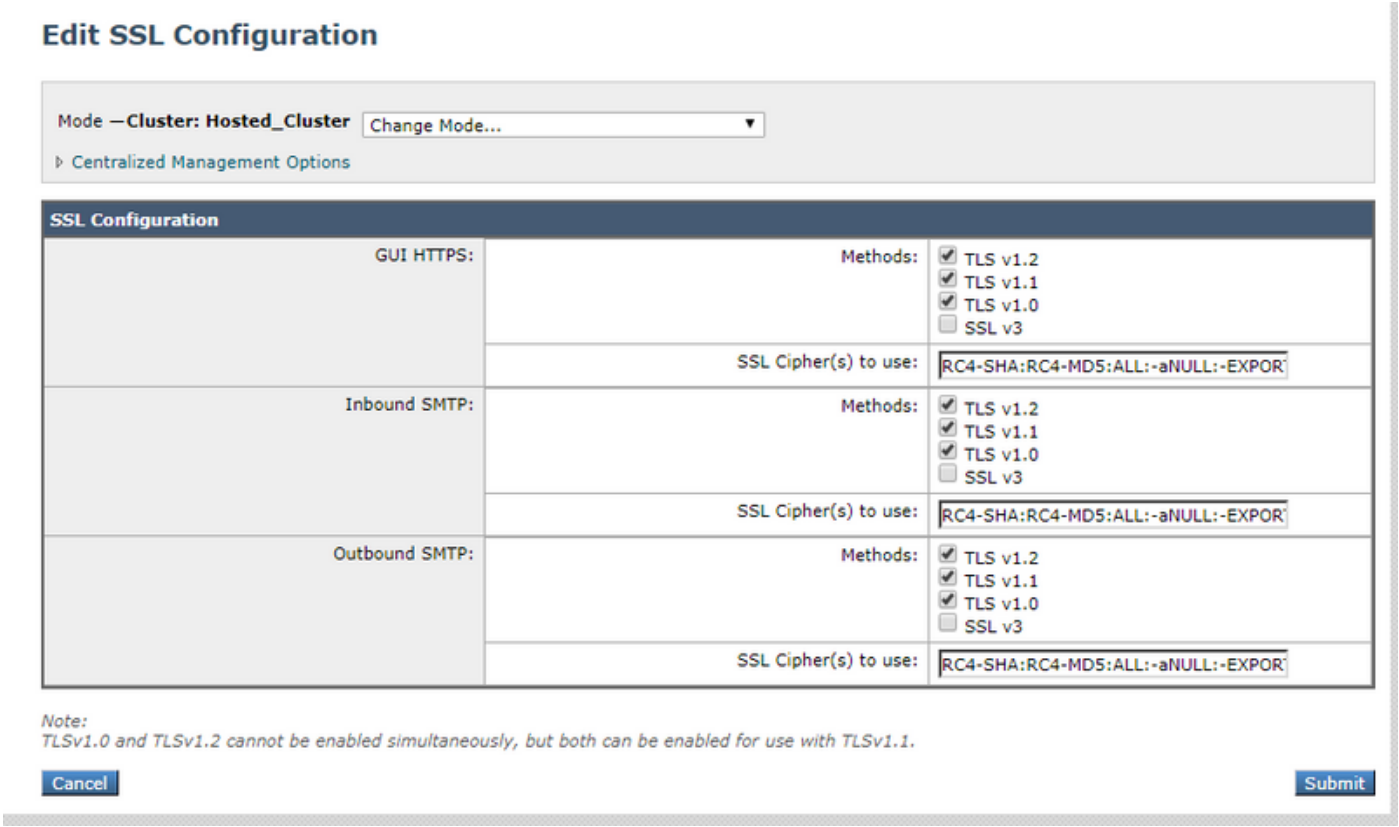
> **Voorzichtig:** De SSL/TLS-methoden en -kaarten worden ingesteld op basis van het specifieke beveiligingsbeleid en de voorkeuren van uw bedrijf. Raadpleeg voor informatie van derden over cifen het document Security/Server Side TLS Mozilla voor aanbevolen serverconfiguraties en gedetailleerde informatie.

Om TLSv1.0 op uw Cisco ESA of CES in te schakelen, kunt u dit doen via de Graphical User Interface (GUI) of de Opdracht Line Interface (CLI).

> Opmerking: Om toegang tot uw CES op de CLI te krijgen raadpleeg dan: **Toegang tot de Opdracht Line Interface (CLI) van Uw Cloud Email Security (CES)-oplossing**

grafische gebruikersinterface

1. Log in op de GUI.
2. Navigeer naar **systeembeheer > SSL-configuratie**.
3. Selecteer **Instellingen bewerken**.
4. Controleer het vakje **TLSv1.0**. Het is belangrijk op te merken dat TLSv1.2 en niet kunnen worden ingeschakeld in combinatie met TLSv1.0 tenzij het overbruggingsprotocol TLSv1.1 ook is ingeschakeld zoals in de afbeelding wordt getoond:



Opdrachtlijn-interface

1. Start de opdracht **slfig**.
2. Draai de opdracht **GUI**, **INBOUND** of **OUTBOUND**, afhankelijk van welk item u TLSv1.0 wilt inschakelen voor:

```
(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]>
```

CIFERS

ESA's en CES Toewijzingen kunnen worden geconfigureerd met strikte algoritmische formaten, het is belangrijk om ervoor te zorgen dat SSLv3-ciphers niet worden geblokkeerd wanneer u het TLSv1.0-protocol inschakelen. Het niet toestaan van de SSLv3-algoritme resulteert in TLS-onderhandelingmislukkingen of een abrupte sluiting van de TLS-verbinding.

Monster van het algoritme:

```
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
```

Dit algoritme voorkomt dat ESA/CES onderhandeling over SSLv3-telefoons zoals aangegeven op **!SSLv3:** dit betekent wanneer het protocol in de handdruk wordt aangevraagd, de SSL-handdruk mislukt omdat er geen gedeelde telefoons beschikbaar zijn voor onderhandeling.

Om ervoor te zorgen dat de string van het monsteralgoritme met TLSv1.0 werkt, moet het worden aangepast om **!SSLv3:!TLSv1:** zie in de vervangen algoritme:

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

> Opmerking: U kunt de formaten van het algoritme die op SSL-handdruk op de ESA/CES CLI worden gedeeld met de **VERIFY-**opdracht controleren.

Mogelijke fouten die in de mail_logs/Message Tracking zijn geregistreerd, maar niet beperkt tot:

```
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')
```

Gerelateerde informatie

- Verander de methodes en CIFERS die met SSL/TLS op de ESA worden gebruikt
- SSL-kaartgegevens Sterkte
- Comprehensive Setup Guide voor TLS op ESA
- Technische ondersteuning en documentatie – Cisco Systems