Configurare Transport Layer Security versione 1.0 su Cisco ESA e CES

Sommario

[Introduzione](#)
[Come abilitare TLSv1.0 su Cisco ESA e CES?](#)
[Interfaccia grafica dell'utente](#)
[Interfaccia della riga di comando](#)
[Cifrature](#)
[Informazioni correlate](#)

Introduzione

In questo documento viene descritto come abilitare Transport Layer Security versione 1.0 (TLSv1.0) sulle allocazioni Cisco Email Security Appliance (ESA) e Cisco Cloud Email Security (CES).

Come abilitare TLSv1.0 su Cisco ESA e CES?

> **Nota:** Per impostazione predefinita, le allocazioni Cisco CES fornite dispongono di TLSv1.0 disabilitato in base ai requisiti di sicurezza a causa dell'impatto della vulnerabilità sul protocollo TLSv1.0. inclusa la stringa di crittografia per rimuovere tutti gli utilizzi della suite di cifratura condivisa SSLv3.

> **Attenzione:** I metodi e le cifrature SSL/TLS sono impostati in base ai criteri e alle preferenze di sicurezza specifici della società. Per informazioni di terze parti relative alle cifrature, consultare il documento Security/Server Side TLS Mozilla per le configurazioni server consigliate e informazioni dettagliate.

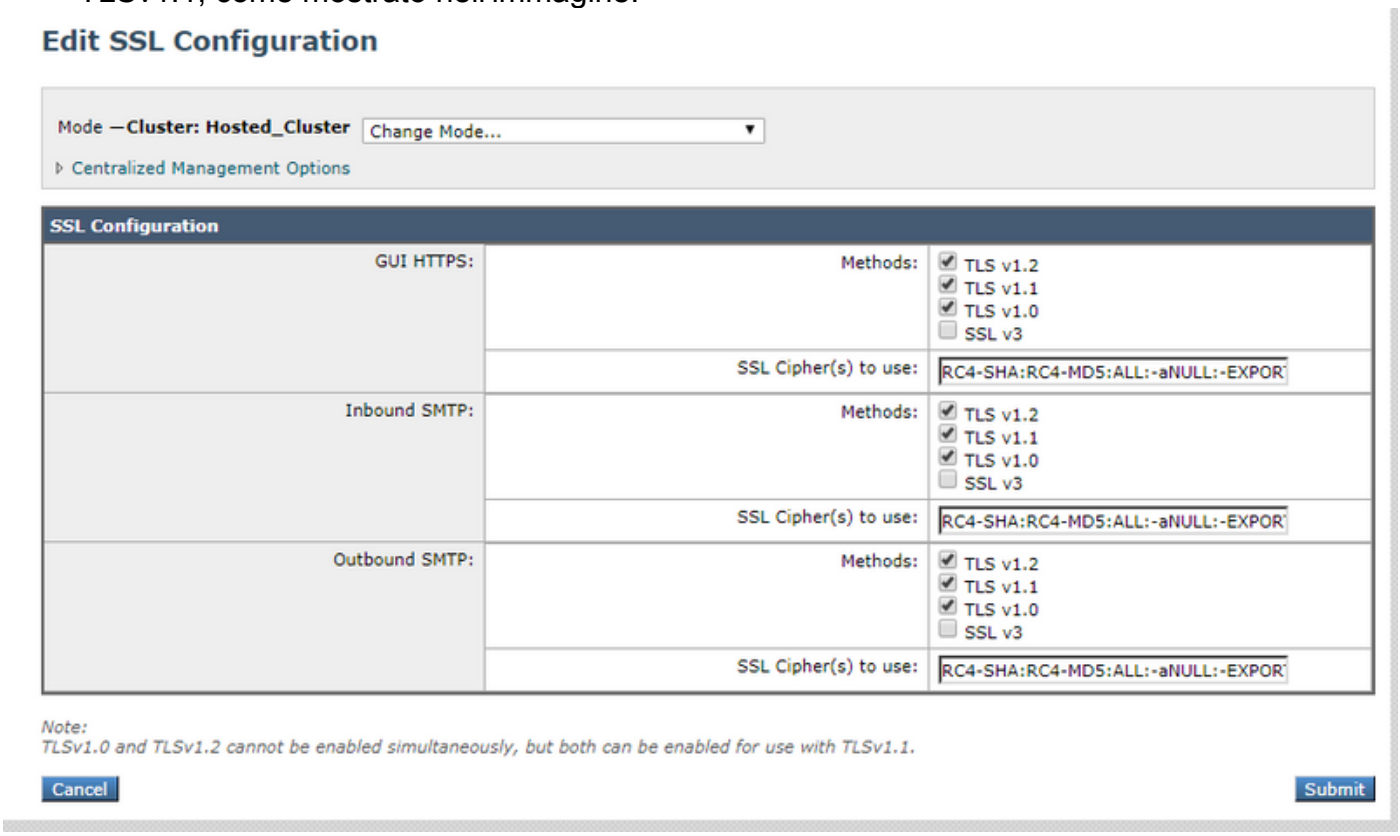
Per abilitare TLSv1.0 sull'ESA o sul CES Cisco, è possibile usare l'interfaccia grafica dell'utente (GUI) o l'interfaccia della riga di comando (CLI).

> **Nota:** Per ottenere l'accesso al CES dalla CLI, consultare: **Accesso all'interfaccia della riga di comando (CLI) della soluzione Cloud Email Security (CES)**

Interfaccia grafica dell'utente

1. Accedere alla GUI.
2. Selezionare **Amministrazione sistema > Configurazione SSL**.
3. Selezionare **Modifica impostazioni**.
4. Selezionare la casella **TLSv1.0**. È importante notare che TLSv1.2 e non possono essere abilitati insieme a TLSv1.0 a meno che non sia abilitato anche il protocollo di bridging

TLSv1.1, come mostrato nell'immagine:



Interfaccia della riga di comando

1. Eseguire il comando **sslconfig**.
2. Eseguire il comando **GUI** o **INBOUND** o **OUTBOUND** a seconda dell'elemento per cui si desidera abilitare 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]>
```

Cifrature

Le allocazioni ESA e CES possono essere configurate con suite di cifratura rigide. È importante assicurarsi che le cifrature SSLv3 non vengano bloccate quando si abilita il protocollo TLSv1.0. Se non si consentono le suite di cifratura SSLv3, si verificano errori di negoziazione TLS o interruzioni brusche delle connessioni TLS.

Stringa di esempio:

```
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
```

Questa stringa di cifratura impedisce all'ESA/CES di consentire la negoziazione sui cifrari SSLv3 come indicato in **!SSLv3:,** ciò significa che quando il protocollo viene richiesto nell'handshake, l'handshake SSL ha esito negativo perché non sono disponibili cifrature condivise per la negoziazione.

Per garantire che la stringa di crittografia di esempio funzioni con TLSv1.0, è necessario modificarla per rimuovere **!SSLv3:!TLSv1:** visualizzato nella stringa di crittografia sostituita:

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

> **Nota:** È possibile verificare le suite di cifratura condivise sull'handshake SSL sulla CLI ESA/CES con il comando **VERIFY**.

Possibili errori registrati in mail_logs/Message Tracking ma non limitati a:

```
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')
```

Informazioni correlate

- Modifica dei metodi e dei cifrari utilizzati con SSL/TLS sull'ESA

- Dettagli livello di crittografia SSL
- Guida completa alla configurazione di TLS su ESA
- Documentazione e supporto tecnico – Cisco Systems