Configuración de Transport Layer Security Version 1.0 en ESA y CES

Contenido

Introducción

Este documento describe cómo habilitar Transport Layer Security versión 1.0 (TLSv1.0) en las asignaciones de Cisco Email Security Appliance (ESA) y Cisco Cloud Email Security (CES).

¿Cómo puede habilitar TLSv1.0 en Cisco ESA y CES?

Nota: las asignaciones de Cisco CES aprovisionadas tienen TLSv1.0 deshabilitado de forma predeterminada según los requisitos de seguridad debido a los impactos de vulnerabilidad en el protocolo TLSv1.0. Esto incluye la cadena de cifrado para eliminar todo el uso de la suite de cifrado compartido SSLv3.

Precaución: Los métodos SSL/TLS y los cifrados se establecen en función de las políticas y preferencias de seguridad específicas de su empresa. Para obtener información de terceros con respecto a los cifrados, consulte el documento Seguridad/Lado del servidor TLS Mozilla para obtener configuraciones de servidor recomendadas e información detallada.

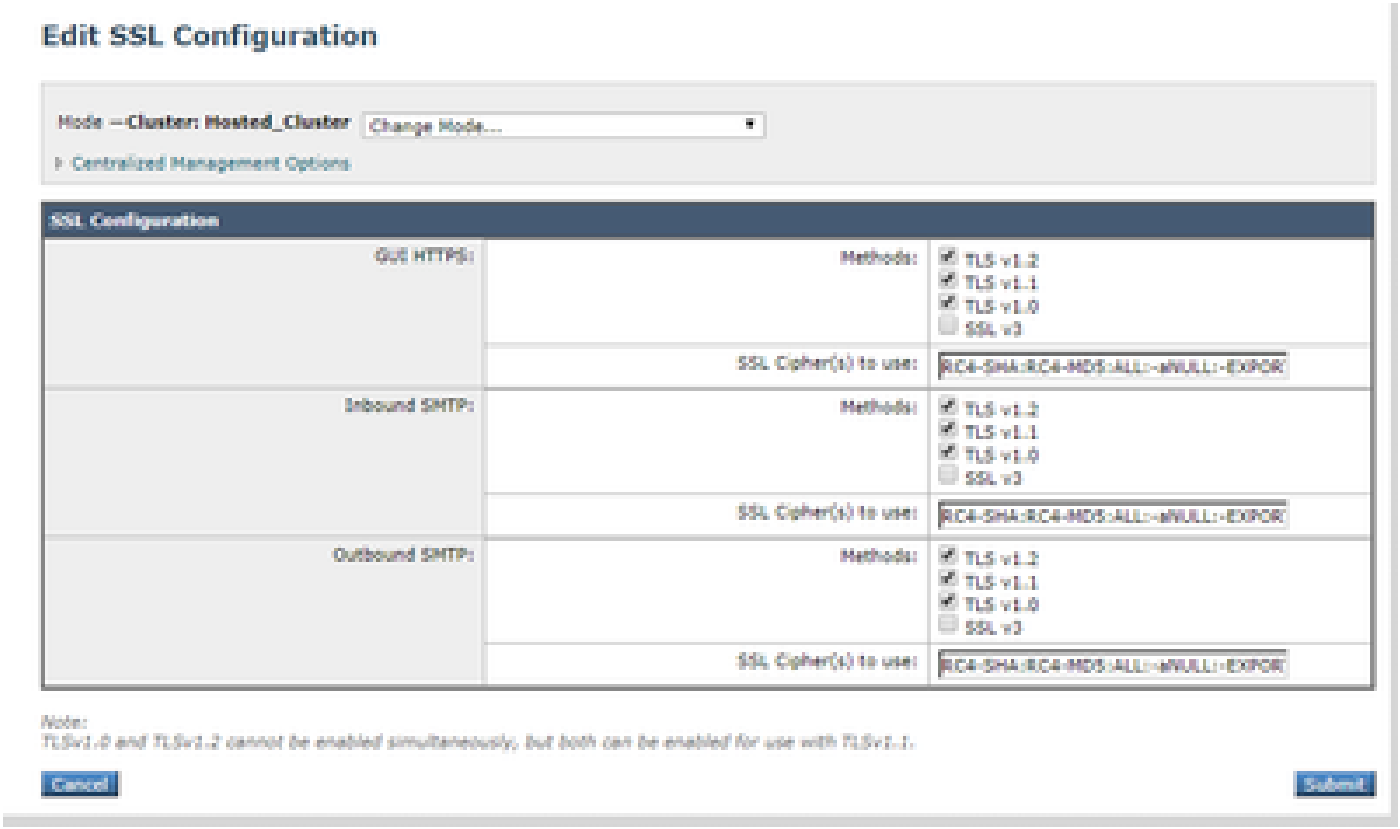
Para habilitar TLSv1.0 en Cisco ESA o CES, puede hacerlo desde la interfaz gráfica de usuario (GUI) o la interfaz de línea de comandos (CLI).

Nota: para obtener acceso a CES en la CLI, revise: Acceso a la interfaz de línea de comandos (CLI) de la solución Cloud Email Security (CES)

Interfaz gráfica del usuario

1. Inicie sesión en la GUI.
2. Vaya a Administración del sistema > Configuración SSL.
3. Seleccione Editar configuración.

4. Marque la casilla TLSv1.0. Es importante tener en cuenta que TLSv1.2 y no se pueden habilitar junto con TLSv1.0 a menos que el protocolo de puente TLSv1.1 también esté habilitado como se muestra en la imagen:



Interfaz de la línea de comandos

1. Ejecute el comando sslconfig.
2. Ejecute el comando GUI o INBOUND o OUTBOUND en función del elemento para el que desee habilitar TLSv1.0:

<#root>

(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]>
```

Cifras

Las asignaciones de ESA y CES se pueden configurar con conjuntos de cifrado estrictos. Es importante asegurarse de que los cifrados SSLv3 no se bloqueen cuando habilite el protocolo TLSv1.0. Si no se permiten los conjuntos de cifrado SSLv3, se producen errores de negociación de TLS o cierres abruptos de la conexión TLS.

Cadena de cifrado de ejemplo:

<#root>

```
HIGH:MEDIUM:@STRENGTH:!aNULL:!eNULL:!LOW:!DES:!MD5:!EXP:!PSK:!DSS:!RC2:!RC4:!SEED:!ECDSA:!ADH:!IDEA:!3D
```

!SSLv3:!TLSv1

```
:-aNULL:-EXPORT:-IDEA
```

Esta cadena de cifrado impide que el ESA/CES permita la negociación en cifrados SSLv3 como se indica en !SSLv3:, esto significa que cuando se solicita el protocolo en el protocolo de enlace, el protocolo de enlace SSL falla ya que no hay cifrados compartidos disponibles para la negociación.

Para asegurarse de que la cadena de cifrado de ejemplo funciona con TLSv1.0, es necesario modificarla para quitar !SSLv3:!TLSv1: visto en la cadena de cifrado reemplazada:

```
HIGH:MEDIUM:@STRENGTH:!aNULL:!eNULL:!LOW:!DES:!MD5:!EXP:!PSK:!DSS:!RC2:!RC4:!SEED:!ECDSA:!ADH:!IDEA:!3D
```

Nota: Puede verificar los conjuntos de cifrado compartidos en el protocolo de enlace SSL en la CLI de ESA/CES con el comando VERIFY.

Posibles errores registrados en mail_logs/Rastreo de mensajes, pero no limitados a:

```
Sun Feb 23 10:07:07 2020 Info: DCID 1407038 TLS failed: (336032784, 'error:14077410:SSL routines:SSL23_
Sun Feb 23 10:38:56 2020 Info: DCID 1407763 TLS failed: (336032002, 'error:14077102:SSL routines:SSL23_
```

Información Relacionada

- Modificar los métodos y cifrados utilizados con SSL/TLS en el ESA
- Detalles de fortaleza de cifrado SSL
- Completa guía de configuración para TLS en ESA
- Soporte Técnico y Documentación - Cisco Systems

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).