Configuración de TLSv1.3 para Secure Email Gateway

Contenido

Introducción

Este documento describe la configuración del protocolo TLS v1.3 para Cisco Secure Email Gateway (SEG).

Prerequisites

Se requiere un conocimiento general de los parámetros y la configuración de SEG.

Componentes Utilizados

- La información que contiene este documento se basa en las siguientes versiones de software y hardware.
  - Cisco Secure Email Gateway (SEG) AsyncOS 15.5.1 y versiones posteriores.
- Parámetros de configuración de SEG SSL.

"La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si su red está activa, asegúrese de comprender el impacto potencial de cualquier comando".

Overview

El SEG ha integrado el protocolo TLS v1.3 para cifrar las comunicaciones de los servicios relacionados con SMTP y HTTPS; interfaz de usuario clásica, NGUI y API de resto.

El protocolo TLS v1.3 presume de una comunicación más segura y una negociación más rápida a

medida que el sector trabaja para convertirlo en el estándar.

El SEG utiliza el método de configuración SSL existente dentro del SEG WebUI o CLI de SSL con algunas configuraciones notables para resaltar.

- Consejos de precaución al configurar los protocolos permitidos.
- Los cifrados no se pueden manipular.
- TLS v1.3 se puede configurar para HTTPS de GUI, correo entrante y correo saliente.
- Las opciones de selección de la casilla de verificación del protocolo TLS entre TLS v1.0 y TLS v1.3 utilizan un patrón ilustrado con más detalle en el artículo.

Configurar

El SEG integra el protocolo TLS v1.3 para HTTPS y SMTP dentro de AsycOS 15.5. Se recomienda precaución al seleccionar la configuración del protocolo para evitar HTTPS y los fallos de entrega/recepción de correo electrónico.

Las versiones anteriores de Cisco SEG admitían TLS v1.2 en la gama alta junto con otros proveedores de correo electrónico como MS O365 que admitían TLS v1.2 en el momento en que se escribió el artículo.

La implementación SEG de Cisco del protocolo TLS v1.3 admite 3 cifrados predeterminados que no se pueden cambiar ni excluir dentro de la configuración de cifrado SEG como lo permiten los otros protocolos.

Los parámetros de configuración SSL de SEG existentes todavía permiten la manipulación de TLS v1.0, v1.1, v1.2 en conjuntos de cifrado.

Cifrados TLS 1.3:

TLS_AES_256_GCM_SHA384

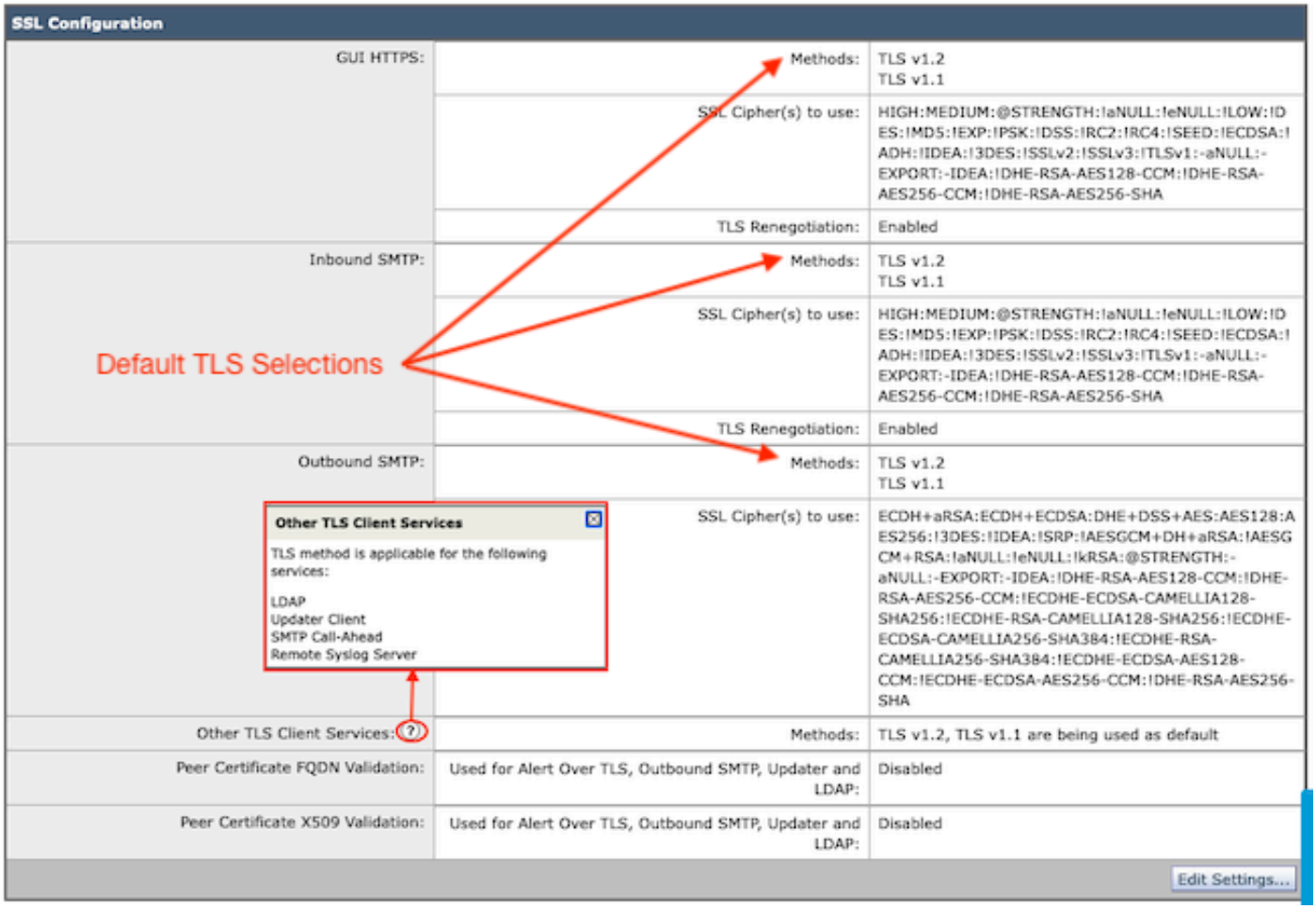
TLS_CHACHA20_POLY1305_SHA256

TLS_AES_128_GCM_SHA256

Configuración desde la interfaz de usuarioWeb

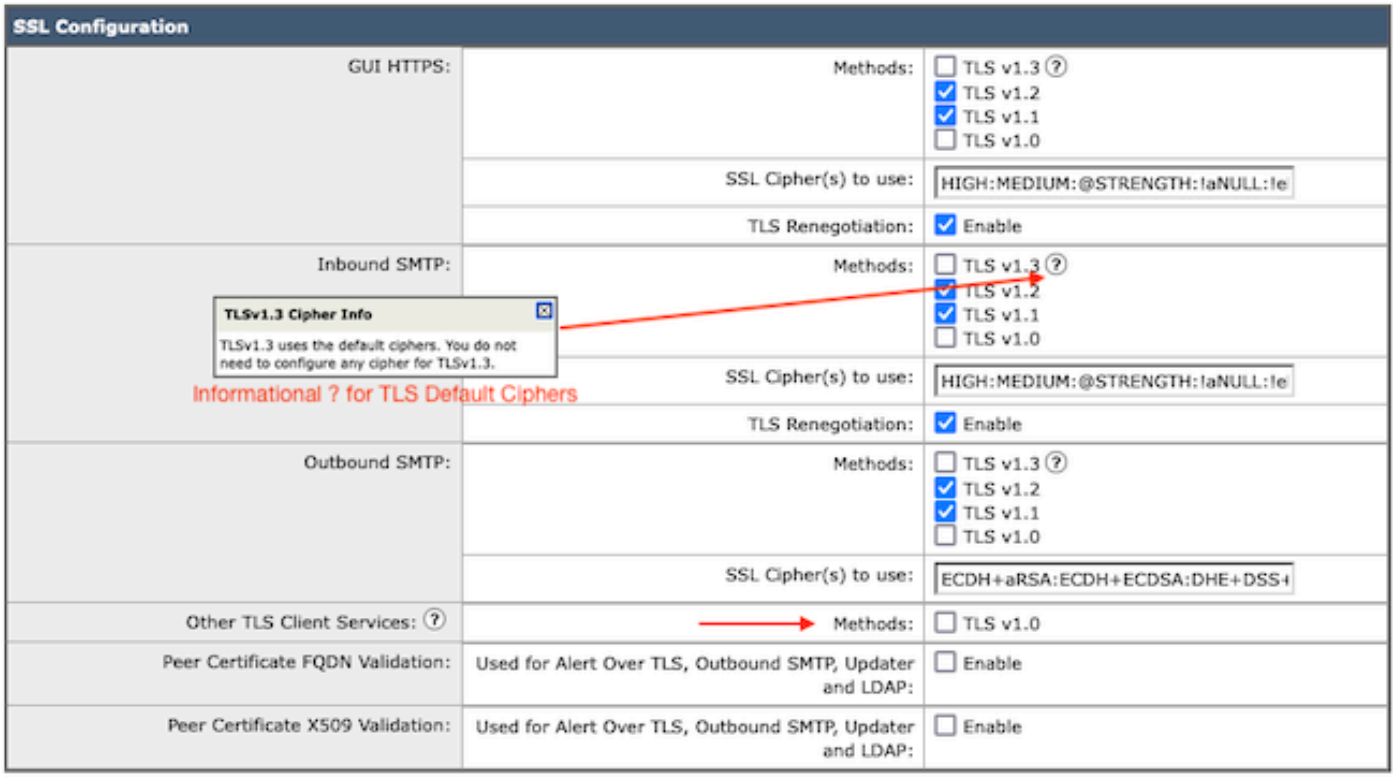
Vaya a > Administración del sistema > Configuración de SSL

- La selección predeterminada del protocolo TLS después de la actualización a 15.5 AsyncOS incluye TLS v1.1 y TLS v1.2 solamente.
- La configuración para "Otros servicios de cliente TLS" utiliza TLS v1.1 y TLS v1.2 con la opción de seleccionar, solo usar TLS v1.0.



Seleccione "Editar configuración" para presentar las opciones de configuración.

- TLS v1.1 y TLS v1.2 están marcados con casillas activas para seleccionar los otros protocolos.
- El signo ? situado junto a cada TLS v1.3 es una repetición de las opciones Cipher estáticas.
- "Otros servicios de cliente TLS:" ahora presenta la opción de utilizar TLS v1.0 solamente si se selecciona.



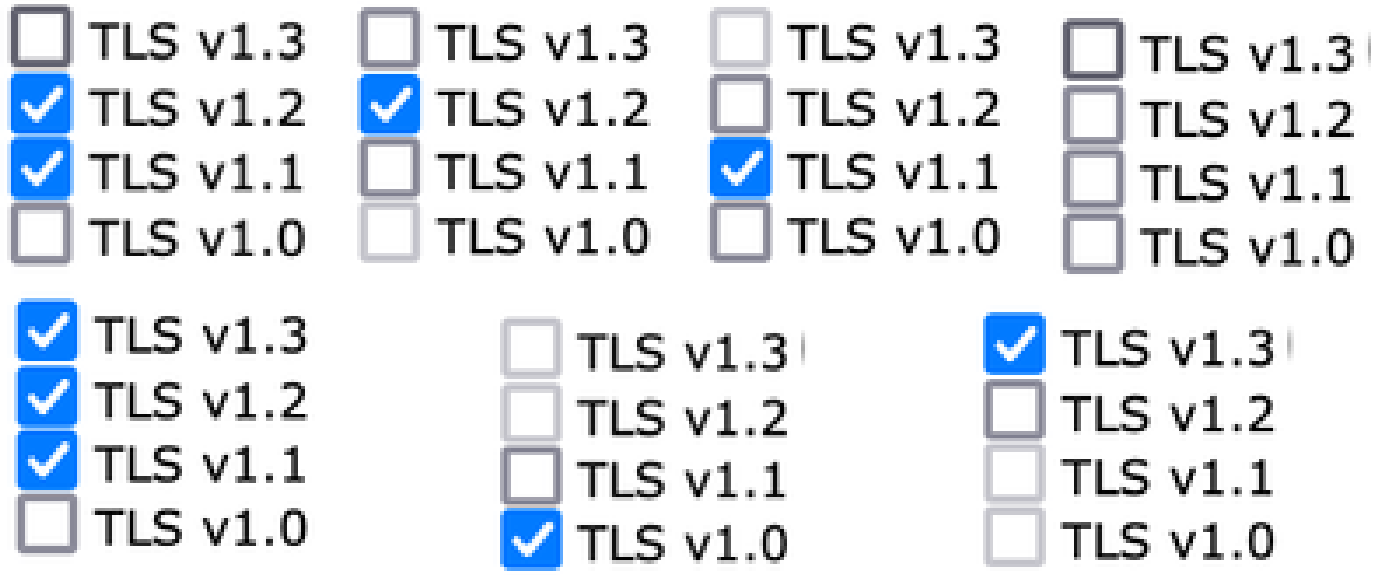
Note:
TLS protocols can be enabled only in sequence.
The configured SSL Cipher(s) do not apply to TLS 1.3. The TLS 1.3 protocol uses default ciphers.

Las opciones de selección del protocolo TLS incluyen TLS v1.0, TLS v1.1, TLS v1.2 y TLS v1.3.

- Tras la actualización a AsyncOS 15.5, solo los protocolos TLS v1.1 y TLS v1.2 están seleccionados de forma predeterminada.

Nota: TLS1.0 está obsoleto y, por lo tanto, está deshabilitado de forma predeterminada. TLS v1.0 sigue estando disponible si el propietario decide activarlo.

- Las opciones de la casilla de verificación se iluminan con cuadros en negrita que presentan los cuadros Protocolos disponibles y Atenuados para las opciones no compatibles.
- Las opciones de ejemplo de la imagen ilustran las opciones de la casilla de verificación.



Vista de ejemplo de confirmación posterior de los protocolos TLS seleccionados.

SSL Configuration

GUI HTTPS:	Methods:	TLS v1.3 TLS v1.2
	SSL Cipher(s) to use:	HIGH:MEDIUM:@STRENGTH:!aNULL:!eNULL:!LOW:!DES:!MD5:!EXP:!PSK:!DSS:!RC2:!RC4:!SEED:!ECDSA:!ADH:!IDEA:!3DES:!SSLv2:!SSLv3:!TLSv1:-aNULL:-EXPORT:-IDEA:!DHE-RSA-AES256-SHA:!DHE-RSA-AES128-CCM:!DHE-RSA-AES256-CCM
	TLS Renegotiation:	Enabled
Inbound SMTP:	Methods:	TLS v1.3 TLS v1.2 TLS v1.1 TLS v1.0
	SSL Cipher(s) to use:	HIGH:MEDIUM:@STRENGTH:!aNULL:!eNULL:!LOW:!DES:!MD5:!EXP:!PSK:!DSS:!RC2:!RC4:!SEED:!ECDSA:!ADH:!IDEA:!3DES:!SSLv2:!SSLv3:!TLSv1:-aNULL:-EXPORT:-IDEA:!DHE-RSA-AES256-SHA:!DHE-RSA-AES128-CCM:!DHE-RSA-AES256-CCM
	TLS Renegotiation:	Enabled
Outbound SMTP:	Methods:	TLS v1.3 TLS v1.2 TLS v1.1
	SSL Cipher(s) to use:	HIGH:MEDIUM:@STRENGTH:!aNULL:!eNULL:!LOW:!DES:!MD5:!EXP:!PSK:!DSS:!RC2:!RC4:!SEED:!ECDSA:!ADH:!IDEA:!3DES:!SSLv2:!SSLv3:!TLSv1:-aNULL:-EXPORT:-IDEA:!DHE-RSA-AES256-SHA:!DHE-RSA-AES128-CCM:!DHE-RSA-AES256-CCM:!ECDHE-ECDSA-CAMELLIA128-SHA256:!ECDHE-RSA-CAMELLIA128-SHA256:!ECDHE-ECDSA-CAMELLIA256-SHA384:!ECDHE-RSA-CAMELLIA256-SHA384:!ECDHE-ECDSA-AES128-CCM:!ECDHE-ECDSA-AES256-CCM
Other TLS Client Services:	Methods:	TLS v1.2, TLS v1.1 are being used as default
Peer Certificate FQDN Validation:	Used for Alert Over TLS, Outbound SMTP, Updater and LDAP:	Disabled
Peer Certificate X509 Validation:	Used for Alert Over TLS, Outbound SMTP, Updater and LDAP:	Disabled

Edit Settings...

Nota: Las modificaciones en el protocolo HTTPS TLS de la GUI provocan una desconexión breve de la interfaz de usuario web debido al restablecimiento del servicio https.

Configuración de CLI:

El SEG permite TLS v1.3 en 3 servicios:

- HTTPS GUI
- SMTP entrante
- SMTP saliente

Al ejecutar el comando **>** sslconfig, se generan los Protocolos y cifrados configurados actualmente para HTTPS GUI, SMTP entrante, SMTP saliente

- Método HTTPS de la GUI: tlsv1_0tlsv1_1tlsv1_2tlsv1_3
- Método SMTP entrante: tlsv1_0tlsv1_1tlsv1_2tlsv1_3
- Método SMTP saliente: tlsv1_1tlsv1_2tlsv1_3

Elija la operación que desea realizar:

- GUI - Editar GUI HTTPS ssl settings.
- INBOUND - Editar configuración de SSL SMTP entrante.
- OUTBOUND - Editar configuración de SSL SMTP saliente.

[]> entrante

Introduzca el método SSL de SMTP entrante que desea utilizar.

1. TLS v1.3
2. TLS v1.2
3. TLS v1.1
4. TLS v1.0

[2-4]> 1-3

 Nota: El proceso de selección SEG puede incluir un solo número de menú, como 2, un rango de números de menú, como 1-4, o números de menú separados por comas 1,2,3.

Los mensajes posteriores de CLI sslconfig aceptan el valor existente presionando ‘enter’ o modificando la configuración según lo desee.

Complete el cambio con el comando **>** commit **>>** ingrese un comentario opcional si lo desea **>** presione "Enter" para completar los cambios.

Verificación

Esta sección incluye algunos escenarios de prueba básicos y errores que pueden presentarse debido a versiones del Protocolo TLS no coincidentes o errores de sintaxis.

Entrada de registro de muestra de una negociación SMTP saliente SEG que genera un rechazo debido a un destino TLS v1.3 no admitido:

```
Wed Jan 17 20:41:18 2024 Info: DCID 485171 TLS deferring: (336151598, 'error:1409442E:SSL routines:ssl3
```

Entrada de registro de ejemplo de un SEG remitente que recibe una TLS v1.3 negociada correctamente:

```
Wed Jan 17 21:09:12 2024 Info: DCID 485206 TLS success protocol TLSv1.3 cipher TLS_AES_256_GCM_SHA384
```

Entrada de registro de muestra de un SEG receptor sin TLS v1.3 habilitado.

```
Wed Jan 17 20:11:06 2024 Info: ICID 1020004 TLS failed: (337678594, 'error:14209102:SSL routines:tls_ea
```

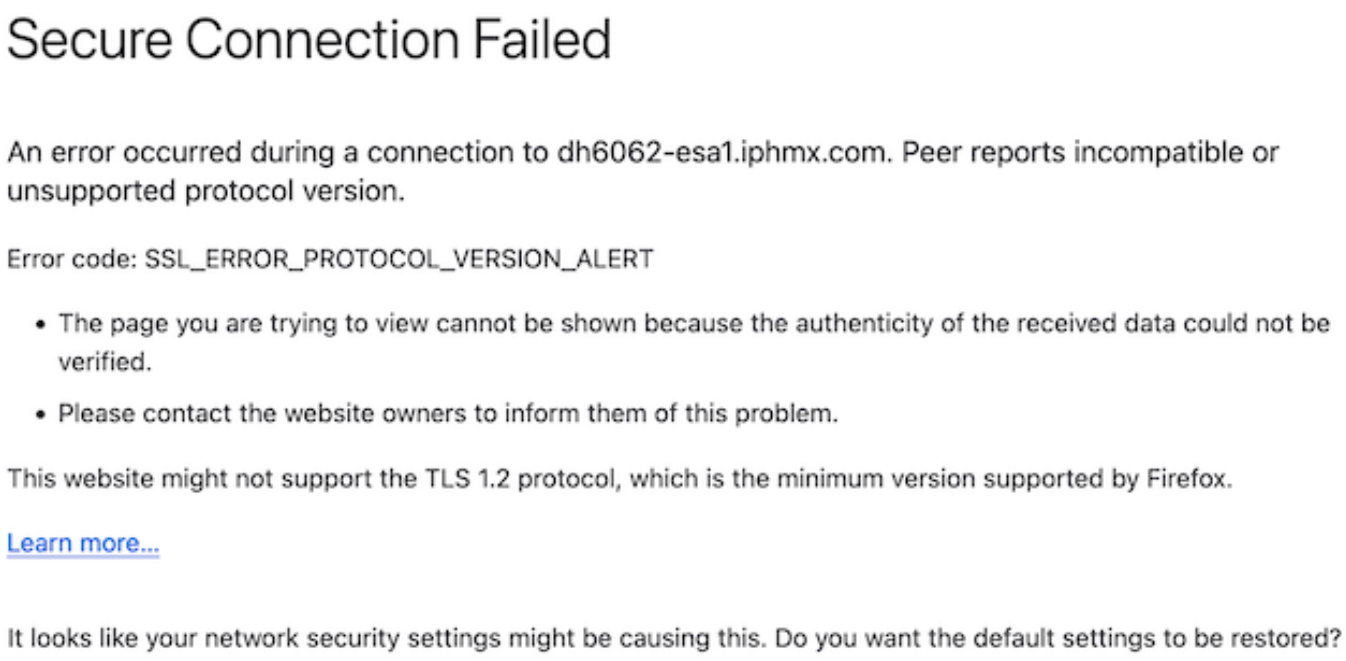
Recepción de TLS v1.3 compatible con SEG

```
Wed Jan 17 21:09:12 2024 Info: ICID 1020089 TLS success protocol TLSv1.3 cipher TLS_AES_256_GCM_SHA384
```

Para verificar la funcionalidad de su navegador, simplemente abra una sesión de navegador web a la interfaz de usuario web SEG o NGUI configurada con TLSv1.3.

Nota: todos los exploradores web que probamos ya están configurados para aceptar TLS v1.3.

- Prueba: configure la configuración del navegador en Firefox. Si se inhabilita la compatibilidad con TLS v1.3, se producirán errores tanto en la interfaz de usuario clásica como en la NGUI del dispositivo.
- Interfaz de usuario clásica con Firefox configurado para excluir TLS v1.3, como prueba.
- NGUI recibiría el mismo error con la única excepción del número de puerto 4431 (predeterminado) dentro de la URL.



- Para garantizar la comunicación, compruebe la configuración del explorador para asegurarse de que se incluye TLSv1.3. (Este ejemplo es de Firefox y utiliza números del 1 al 4

Información Relacionada

- Cisco Secure Email Gateway - Guía de configuración
- Página de inicio de Cisco Secure Email Gateway para las guías de asistencia
- Cisco Secure Email Gateway - Notas de la versión

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).