Personalizar la configuración de cifrado SSL de Expressway

Contenido

Introducción

Este documento describe los pasos para personalizar las cadenas de cifrado preconfiguradas en Expressway.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Cisco Expressway o Cisco VCS.
- Protocolo TLS.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Cisco Expressway versión X15.0.2.

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 tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

La configuración predeterminada de Expressway incluye cadenas de cifrado preconfiguradas, que por razones de compatibilidad, permiten el soporte de algunos cifrados que se pueden considerar débiles en algunas políticas de seguridad de la empresa. Es posible personalizar las cadenas de cifrado para ajustarlas a las políticas específicas de cada entorno.

En Expressway, es posible configurar una cadena de cifrado independiente para cada uno de estos protocolos:

- HTTPS
- LDAP
- Proxy inverso
- SIP
- SMTP
- aprovisionamiento de TMS
- detección de servidores de UC
- XMPP

Las cadenas de cifrado obedecen al formato de OpenSSL descrito en la página de comando man OpenSSL Ciphers. La versión actual de Expressway X15.0.2 incluye la cadena predeterminada EECDH:EDH:HIGH:-AES256+SHA:!MEDIUM:!LOW:!3DES:!MD5:!PSK:!eNULL:!aNULL:!aDH preconfigurada para todos los protocolos por igual. Desde la página de administración web, en Mantenimiento > Seguridad > Cifras, puede modificar la cadena de cifrado asignada a cada protocolo, para agregar o quitar cifrados específicos o grupos de cifrados usando un algoritmo común.

Inspeccionar la cadena de cifrado

Mediante el comando openssl ciphers -V "<cipher string>", puede generar una lista con todos los cifrados que permite una cadena determinada, lo que resulta útil para inspeccionar visualmente los cifrados. Este ejemplo muestra el resultado al inspeccionar la cadena de cifrado predeterminada de Expressway:

<#root>

```
~ #
openssl ciphers -V "EECDH:EDH:HIGH:-AES256+SHA:!MEDIUM:!LOW:!3DES:!MD5:!PSK:!eNULL:!aNULL:!aDH"

0x13,0x02 - TLS_AES_256_GCM_SHA384 TLSv1.3 Kx=any Au=any Enc=AESGCM(256) Mac=AEAD
0x13,0x03 - TLS_CHACHA20_POLY1305_SHA256 TLSv1.3 Kx=any Au=any Enc=CHACHA20/POLY1305(256) Mac=AEAD
0x13,0x01 - TLS_AES_128_GCM_SHA256 TLSv1.3 Kx=any Au=any Enc=AESGCM(128) Mac=AEAD
```

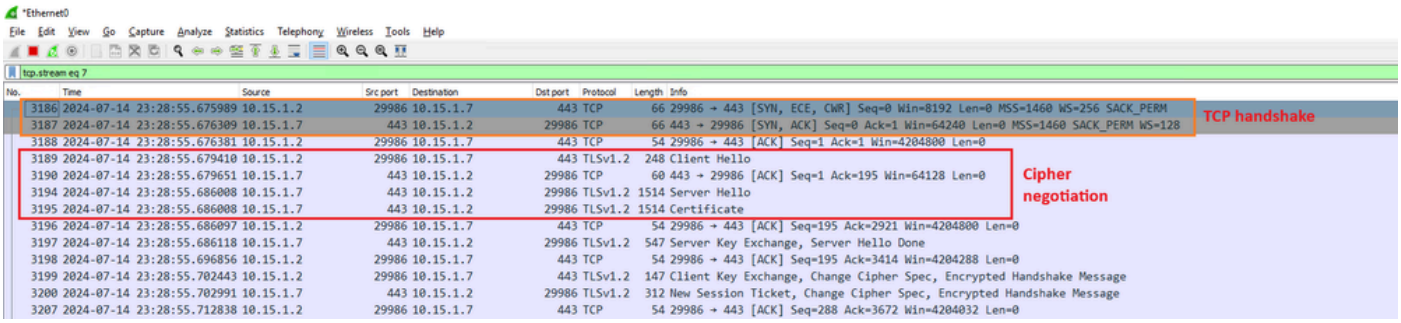
```
0xC0,0x2C - ECDHE-ECDSA-AES256-GCM-SHA384 TLSv1.2 Kx=ECDH Au=ECDSA Enc=AESGCM(256) Mac=AEAD
0xC0,0x30 - ECDHE-RSA-AES256-GCM-SHA384 TLSv1.2 Kx=ECDH Au=RSA Enc=AESGCM(256) Mac=AEAD
0xCC,0xA9 - ECDHE-ECDSA-CHACHA20-POLY1305 TLSv1.2 Kx=ECDH Au=ECDSA Enc=CHACHA20/POLY1305(256) Mac=AEAD
0xCC,0xA8 - ECDHE-RSA-CHACHA20-POLY1305 TLSv1.2 Kx=ECDH Au=RSA Enc=CHACHA20/POLY1305(256) Mac=AEAD
0xC0,0xAD - ECDHE-ECDSA-AES256-CCM TLSv1.2 Kx=ECDH Au=ECDSA Enc=AESCCM(256) Mac=AEAD
0xC0,0x2B - ECDHE-ECDSA-AES128-GCM-SHA256 TLSv1.2 Kx=ECDH Au=ECDSA Enc=AESGCM(128) Mac=AEAD
0xC0,0x2F - ECDHE-RSA-AES128-GCM-SHA256 TLSv1.2 Kx=ECDH Au=RSA Enc=AESGCM(128) Mac=AEAD
0xC0,0xAC - ECDHE-ECDSA-AES128-CCM TLSv1.2 Kx=ECDH Au=ECDSA Enc=AESCCM(128) Mac=AEAD
0xC0,0x24 - ECDHE-ECDSA-AES256-SHA384 TLSv1.2 Kx=ECDH Au=ECDSA Enc=AES(256) Mac=SHA384
0xC0,0x28 - ECDHE-RSA-AES256-SHA384 TLSv1.2 Kx=ECDH Au=RSA Enc=AES(256) Mac=SHA384
0xC0,0x23 - ECDHE-ECDSA-AES128-SHA256 TLSv1.2 Kx=ECDH Au=ECDSA Enc=AES(128) Mac=SHA256
0xC0,0x27 - ECDHE-RSA-AES128-SHA256 TLSv1.2 Kx=ECDH Au=RSA Enc=AES(128) Mac=SHA256
0xC0,0x09 - ECDHE-ECDSA-AES128-SHA TLSv1 Kx=ECDH Au=ECDSA Enc=AES(128) Mac=SHA1
0xC0,0x13 - ECDHE-RSA-AES128-SHA TLSv1 Kx=ECDH Au=RSA Enc=AES(128) Mac=SHA1
0x00,0xA3 - DHE-DSS-AES256-GCM-SHA384 TLSv1.2 Kx=DH Au=DSS Enc=AESGCM(256) Mac=AEAD
0x00,0x9F - DHE-RSA-AES256-GCM-SHA384 TLSv1.2 Kx=DH Au=RSA Enc=AESGCM(256) Mac=AEAD
0xCC,0xAA - DHE-RSA-CHACHA20-POLY1305 TLSv1.2 Kx=DH Au=RSA Enc=CHACHA20/POLY1305(256) Mac=AEAD
0xC0,0x9F - DHE-RSA-AES256-CCM TLSv1.2 Kx=DH Au=RSA Enc=AESCCM(256) Mac=AEAD
0x00,0xA2 - DHE-DSS-AES128-GCM-SHA256 TLSv1.2 Kx=DH Au=DSS Enc=AESGCM(128) Mac=AEAD
0x00,0x9E - DHE-RSA-AES128-GCM-SHA256 TLSv1.2 Kx=DH Au=RSA Enc=AESGCM(128) Mac=AEAD
0xC0,0x9E - DHE-RSA-AES128-CCM TLSv1.2 Kx=DH Au=RSA Enc=AESCCM(128) Mac=AEAD
0x00,0x6B - DHE-RSA-AES256-SHA256 TLSv1.2 Kx=DH Au=RSA Enc=AES(256) Mac=SHA256
0x00,0x6A - DHE-DSS-AES256-SHA256 TLSv1.2 Kx=DH Au=DSS Enc=AES(256) Mac=SHA256
0x00,0x67 - DHE-RSA-AES128-SHA256 TLSv1.2 Kx=DH Au=RSA Enc=AES(128) Mac=SHA256
0x00,0x40 - DHE-DSS-AES128-SHA256 TLSv1.2 Kx=DH Au=DSS Enc=AES(128) Mac=SHA256
0x00,0x33 - DHE-RSA-AES128-SHA SSLv3 Kx=DH Au=RSA Enc=AES(128) Mac=SHA1
0x00,0x32 - DHE-DSS-AES128-SHA SSLv3 Kx=DH Au=DSS Enc=AES(128) Mac=SHA1
0x00,0x9D - AES256-GCM-SHA384 TLSv1.2 Kx=RSA Au=RSA Enc=AESGCM(256) Mac=AEAD
0xC0,0x9D - AES256-CCM TLSv1.2 Kx=RSA Au=RSA Enc=AESCCM(256) Mac=AEAD
0x00,0x9C - AES128-GCM-SHA256 TLSv1.2 Kx=RSA Au=RSA Enc=AESGCM(128) Mac=AEAD
0xC0,0x9C - AES128-CCM TLSv1.2 Kx=RSA Au=RSA Enc=AESCCM(128) Mac=AEAD
0x00,0x3D - AES256-SHA256 TLSv1.2 Kx=RSA Au=RSA Enc=AES(256) Mac=SHA256
0x00,0x3C - AES128-SHA256 TLSv1.2 Kx=RSA Au=RSA Enc=AES(128) Mac=SHA256
0x00,0x2F - AES128-SHA SSLv3 Kx=RSA Au=RSA Enc=AES(128) Mac=SHA1
~ #
```

Inspeccione la negociación de cifrado en el intercambio de señales de TLS con una captura de paquetes

Al capturar una negociación TLS en una captura de paquetes, puede inspeccionar los detalles de la negociación de cifrado mediante Wireshark.

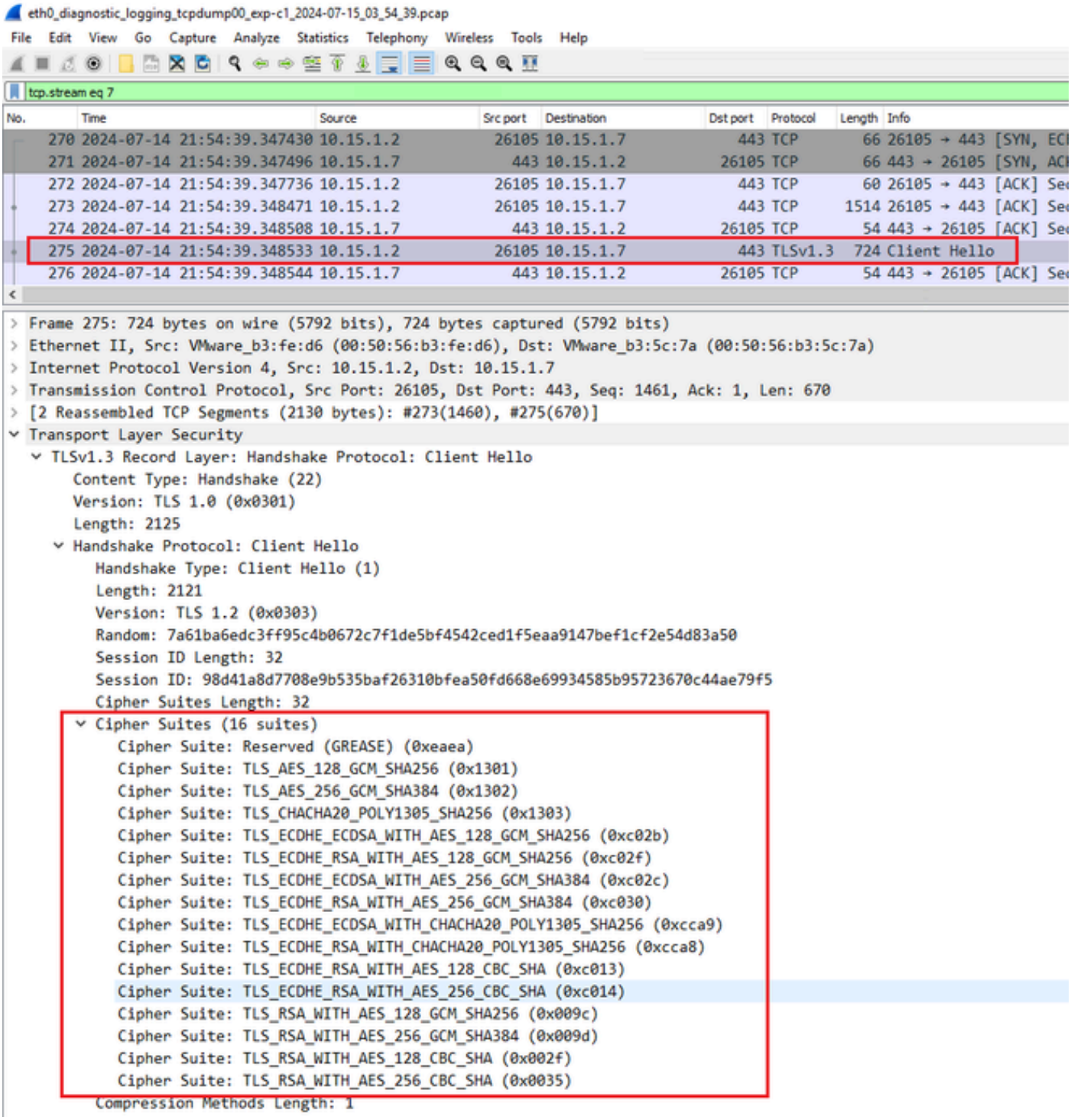
El proceso de intercambio de señales TLS incluye un paquete ClientHello enviado por el dispositivo cliente, que proporciona la lista de los cifrados que admite de acuerdo con su cadena de cifrado configurada para el protocolo de conexión. El servidor revisa la lista, la compara con su propia lista de cifrados permitidos (determinada por su propia cadena de cifrado) y elige un cifrado compatible con ambos sistemas para utilizarlo en la sesión cifrada. A continuación, responde con un paquete ServerHello que indica el cifrado elegido. Existen diferencias importantes entre los diálogos de entrada en contacto de TLS 1.2 y 1.3, sin embargo el mecanismo de negociación de cifrado utiliza este mismo principio en ambas versiones.

Este es un ejemplo de una negociación de cifrado TLS 1.3 entre un navegador web y Expressway en el puerto 443, como se ve en Wireshark:



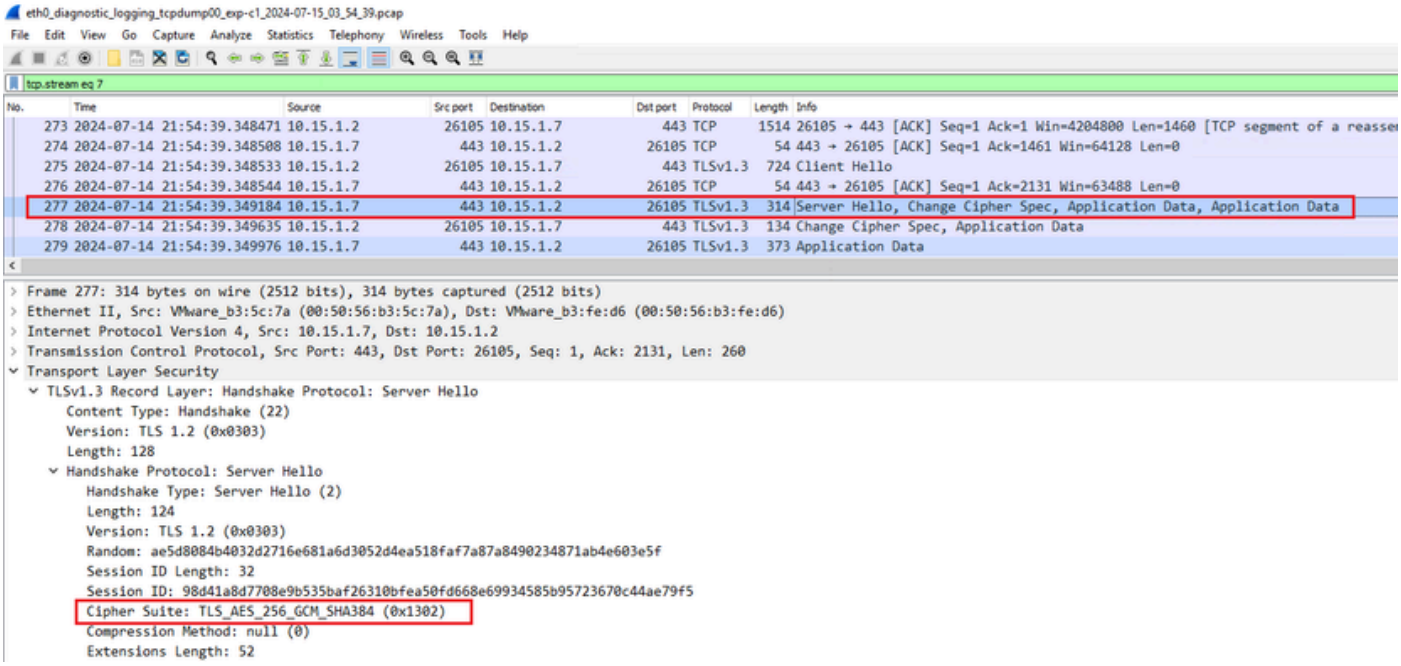
Ejemplo de un intercambio de señales TLS en Wireshark

En primer lugar, el navegador envía un paquete ClientHello con la lista de cifrados que admite:



Ejemplo de un paquete ClientHello en Wireshark

Expressway comprueba su cadena de cifrado configurada para el protocolo HTTPS y encuentra un cifrado que admite tanto él mismo como el cliente. En este ejemplo se selecciona el cifrado ECDHE-RSA-AES256-GCM-SHA384. Expressway responde con su paquete ServerHello indicando el cifrado seleccionado:



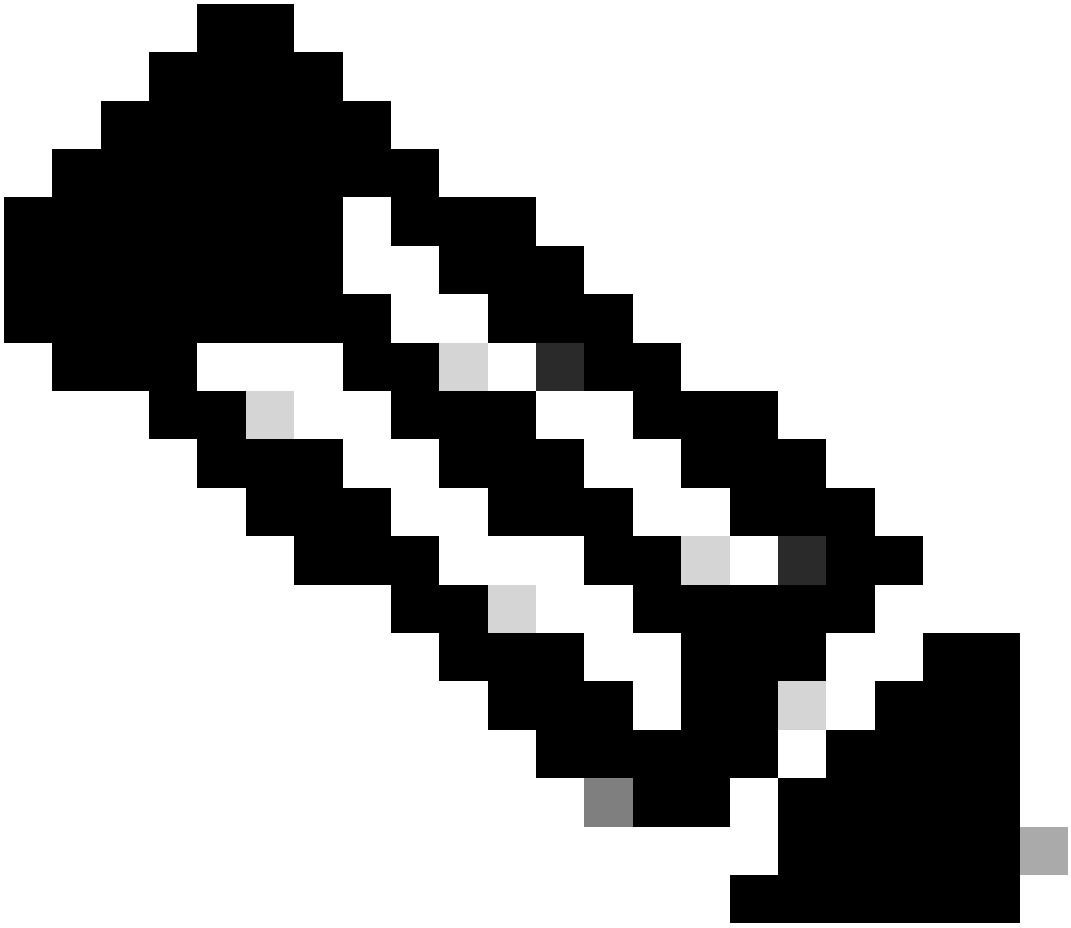
Ejemplo de un paquete ServerHello en Wireshark

Configurar

El formato de cadena de cifrado OpenSSL incluye varios caracteres especiales para realizar operaciones en la cadena, como quitar un cifrado específico o un grupo de cifrados que comparten un componente común. Dado que el objetivo de estas personalizaciones suele ser la eliminación de cifrados, los caracteres utilizados en estos ejemplos son:

- El carácter -, que se utiliza para quitar los cifrados de la lista. Algunas o todas las cifras eliminadas se pueden permitir de nuevo mediante opciones que aparecen más adelante en la cadena.
- El carácter !, también se utiliza para quitar cifrados de la lista. Cuando se utiliza, los cifrados eliminados no se pueden permitir de nuevo por ninguna otra opción que aparezca más adelante en la cadena.
- El carácter :, que actúa como separador entre los elementos de la lista.

Ambos se pueden utilizar para quitar un código de la cadena, sin embargo se prefiere !. Para obtener una lista completa de caracteres especiales, revise la página OpenSSL Ciphers Manpage.



Nota: El sitio OpenSSL indica que cuando se utiliza el carácter !, "los cifrados eliminados nunca pueden volver a aparecer en la lista aunque se hayan indicado explícitamente". Esto no significa que los cifrados se eliminen permanentemente del sistema, sino que se refiere al alcance de la interpretación de la cadena de cifrado.

Deshabilitar un cifrado específico

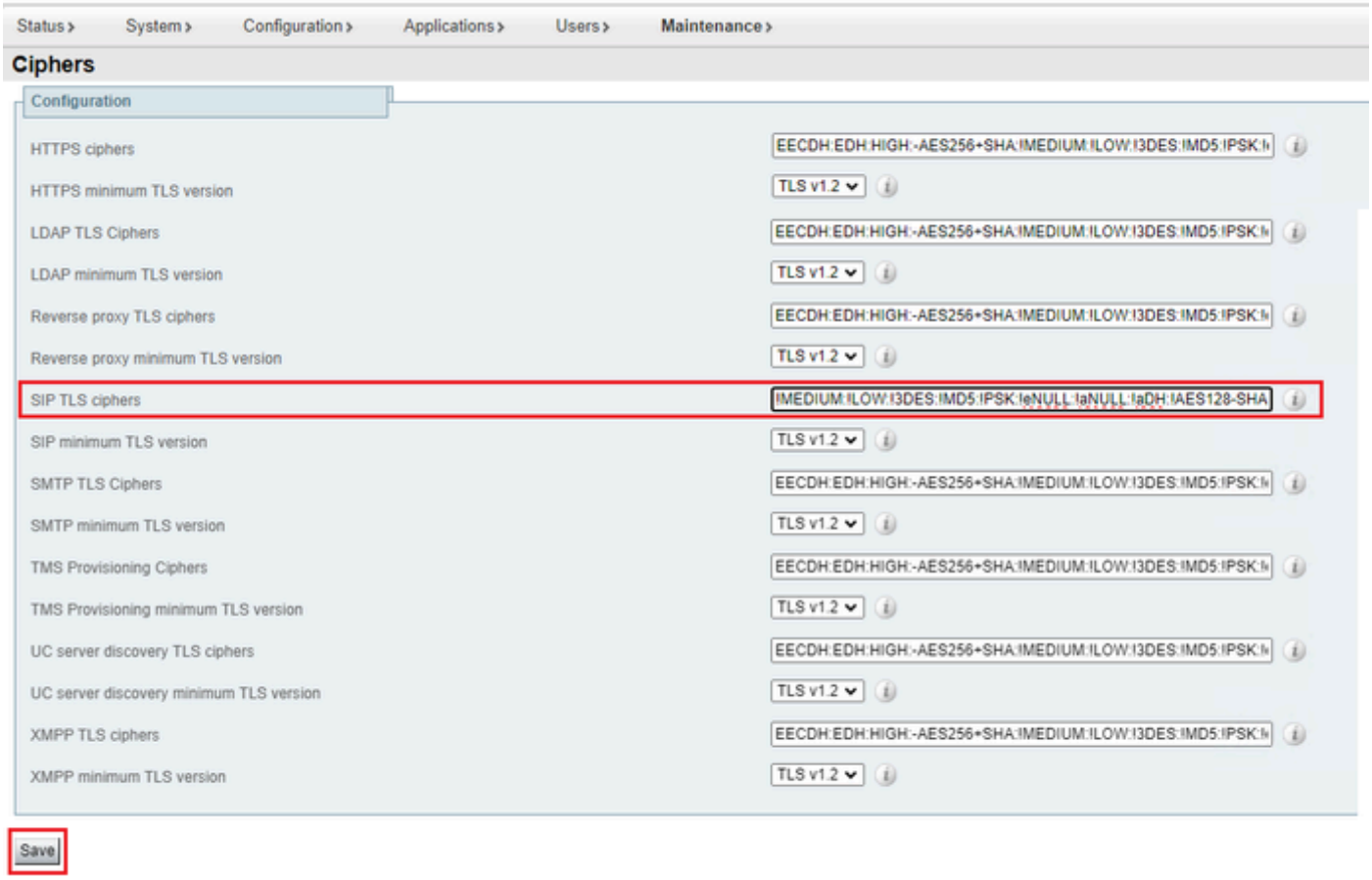
Para inhabilitar un cifrado específico, anexe a la cadena predeterminada el separador :, el signo ! o - y el nombre del cifrado que se va a inhabilitar. El nombre de cifrado debe obedecer al formato de nomenclatura OpenSSL, disponible en la página de comando man OpenSSL Ciphers. Por ejemplo, si necesita inhabilitar el cifrado AES128-SHA para las conexiones SIP, configure una cadena de cifrado como esta:

<#root>

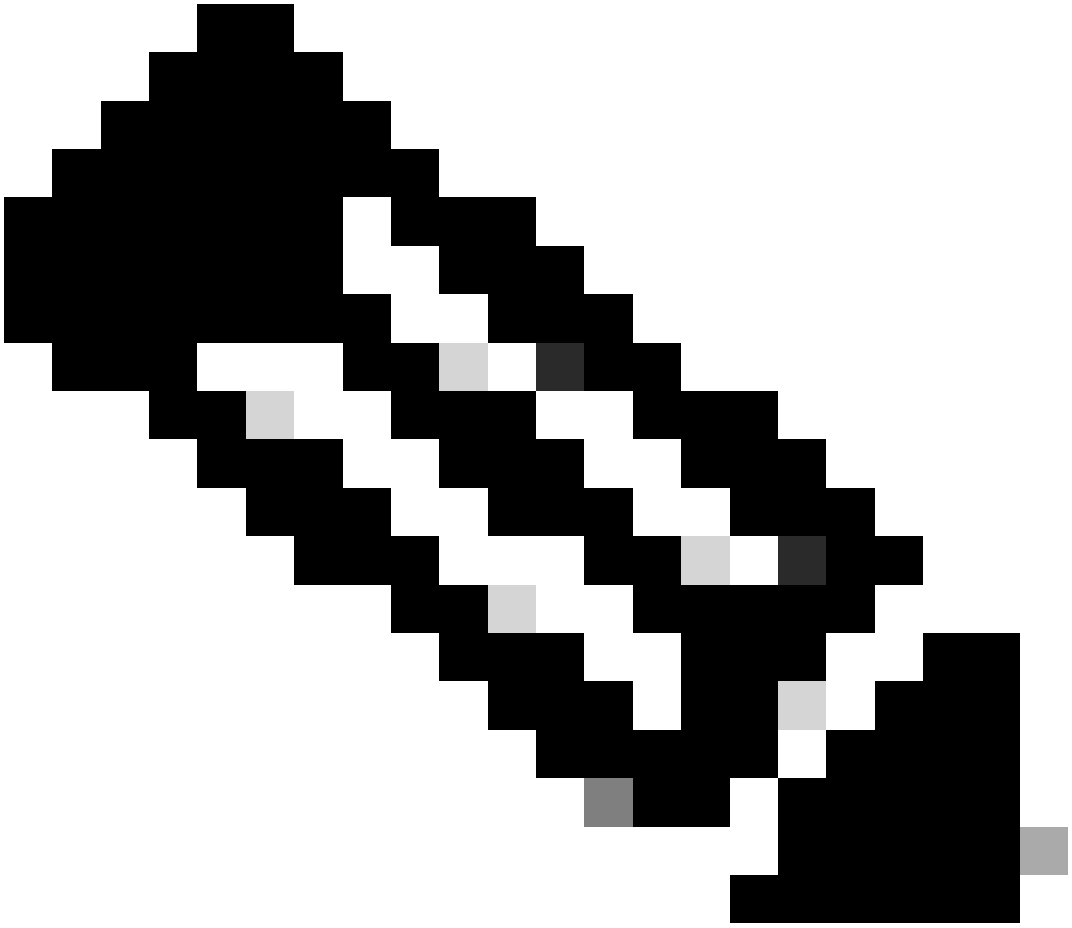
EECDH:EDH:HIGH:-AES256+SHA:!MEDIUM:!LOW:!3DES:!MD5:!PSK:!eNULL:!aNULL:!aDH

:!AES128-SHA

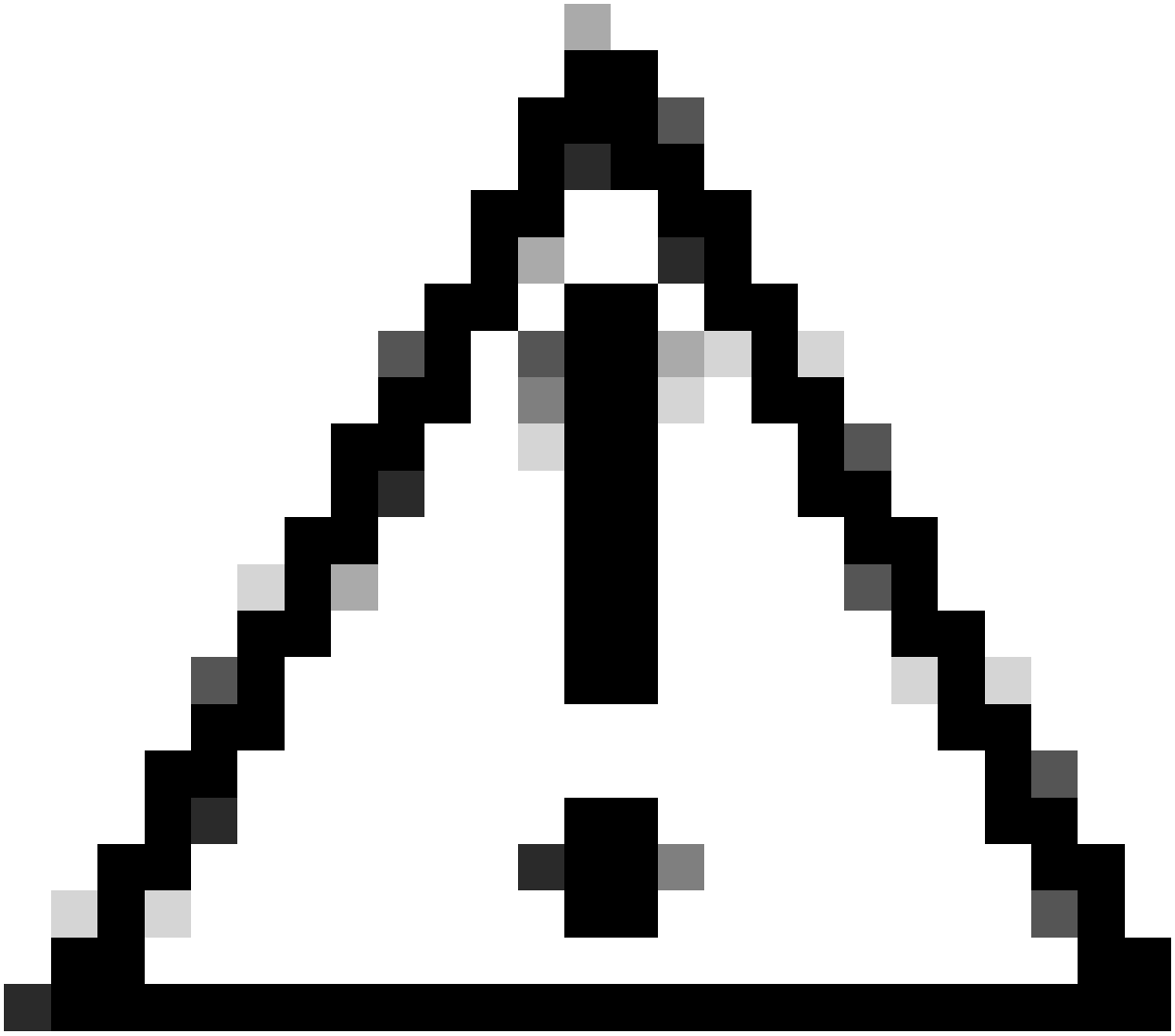
A continuación, vaya a la página de administración web de Expressway, vaya a Mantenimiento > Seguridad > Cifras, asigne la cadena personalizada a los protocolos requeridos y haga clic en Guardar. Para aplicar la nueva configuración, es necesario reiniciar el sistema. En este ejemplo, la cadena personalizada se asigna al protocolo SIP en Cifrados SIP TLS:



Página Cipher Settings (Configuración de cifrado) en el portal de administración web de Expressway



Nota: en el caso de un clúster de Expressway, realice los cambios solo en el servidor principal. La nueva configuración se replica en el resto de los miembros del clúster.



Precaución: utilice la secuencia de reinicio del clúster recomendada en la Guía de implementación de creación y mantenimiento de clústeres de Cisco Expressway. Comience reiniciando el servidor primario, espere a que sea accesible a través de la interfaz web, luego haga lo mismo con cada par en orden según la lista configurada en System > Clustering.

Deshabilitar un grupo de cifrados mediante un algoritmo común

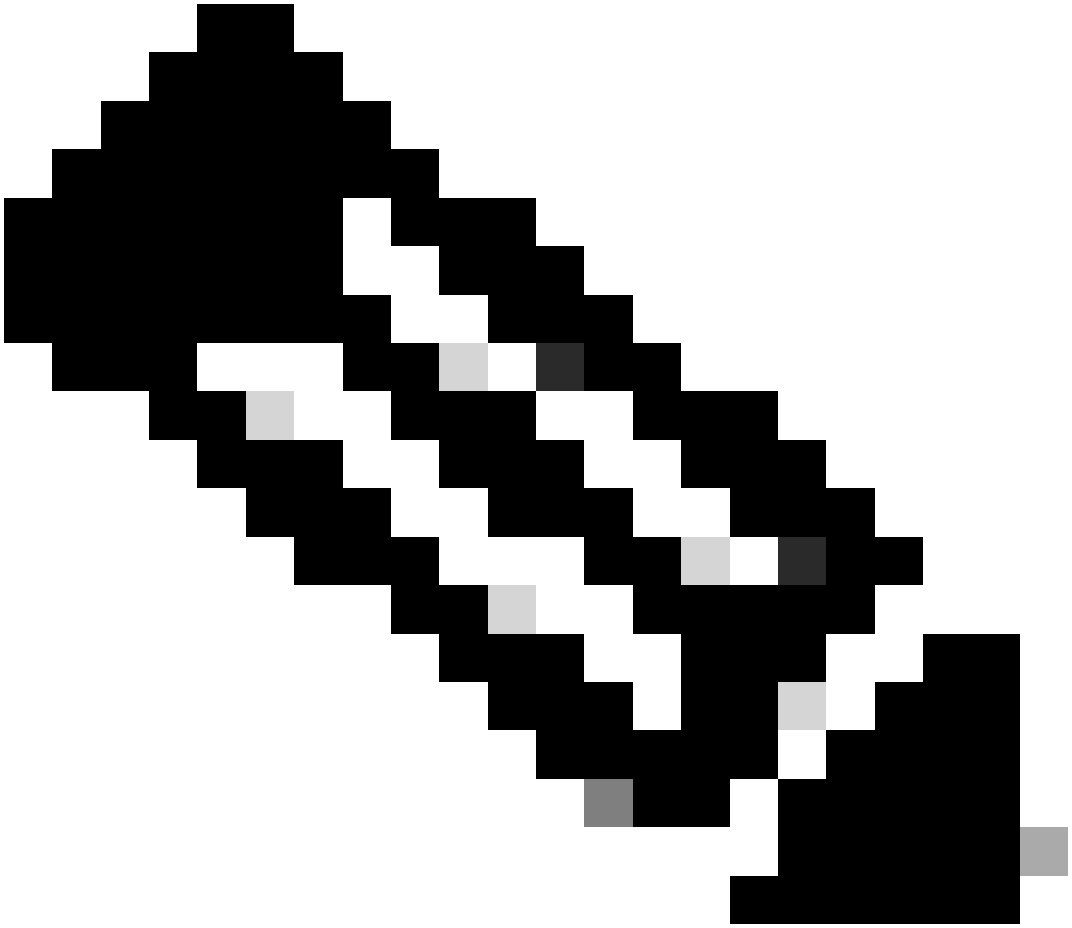
Para inhabilitar un grupo de cifrados usando un algoritmo común, anexe a la cadena predeterminada el separador :, el signo ! o - y el nombre del algoritmo que se inhabilitará. Los nombres de los algoritmos admitidos están disponibles en la página OpenSSL Ciphers Manpage. Por ejemplo, si necesita inhabilitar todos los cifrados que utilizan el algoritmo DHE, configure una cadena de cifrado como esta:

<#root>

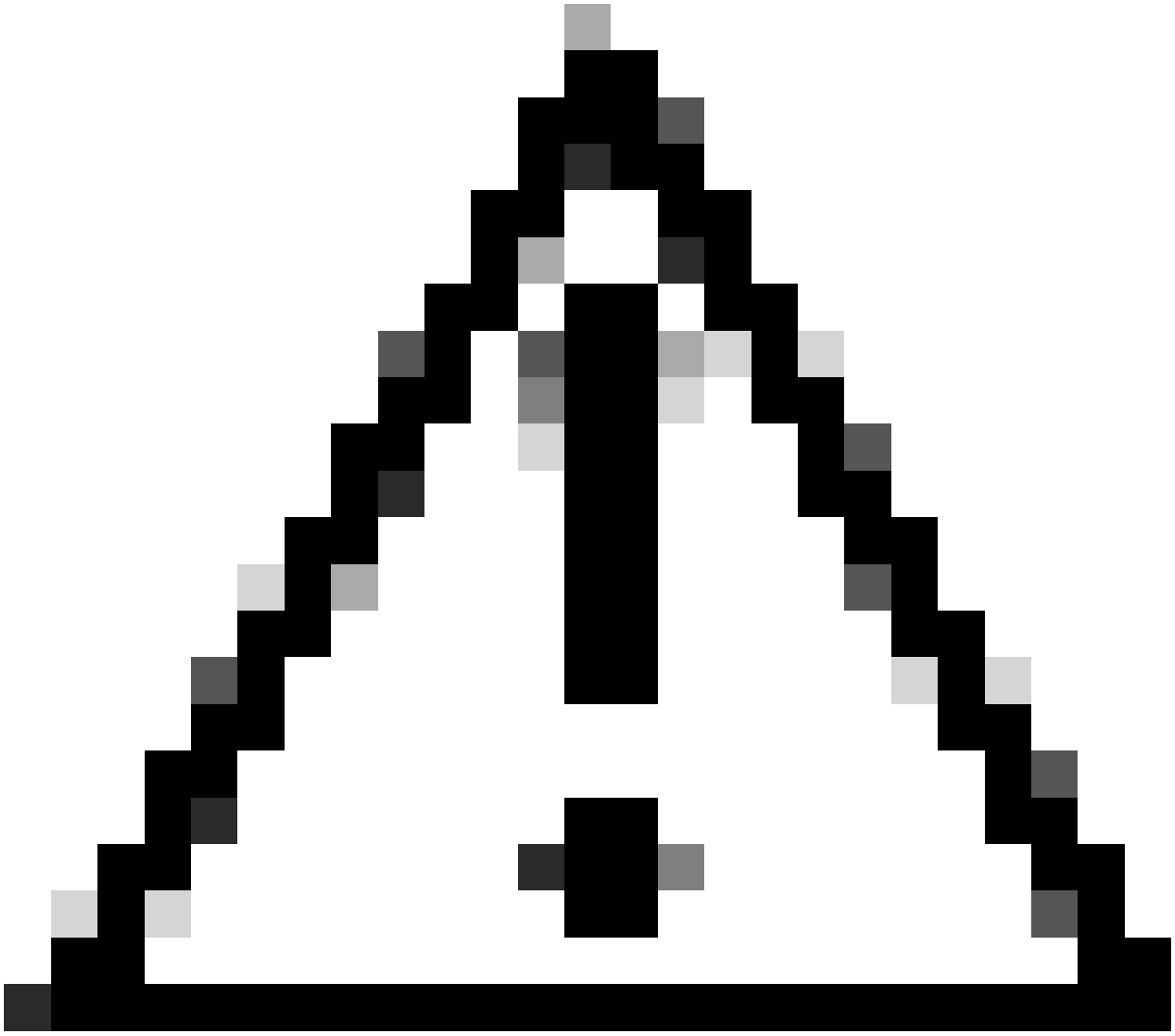
```
EECDH:EDH:HIGH:-AES256+SHA:!MEDIUM:!LOW:!3DES:!MD5:!PSK:!eNULL:!aNULL:!aDH
```

:!DHE

Navegue hasta la página de administración web de Expressway, navegue hasta Mantenimiento > Seguridad > Cifrados, asigne la cadena personalizada a los protocolos requeridos y haga clic en Guardar. Para aplicar la nueva configuración, es necesario reiniciar el sistema.



Nota: en el caso de un clúster de Expressway, realice los cambios solo en el servidor principal. La nueva configuración se replica en el resto de los miembros del clúster.



Precaución: utilice la secuencia de reinicio del clúster recomendada en la Guía de implementación de creación y mantenimiento de clústeres de Cisco Expressway. Comience reiniciando el servidor primario, espere a que sea accesible a través de la interfaz web, luego haga lo mismo con cada par en orden según la lista configurada en System > Clustering.

Verificación

Inspeccionar la lista de cifrados permitidos por la cadena de cifrado

Puede inspeccionar la cadena de cifrado personalizada mediante el comando openssl ciphers -V "<cadena de cifrado>". Revise el resultado para confirmar que los cifrados no deseados ya no aparecen después de los cambios. En este ejemplo, se inspecciona la cadena de cifrado EECDH:EDH:HIGH:-AES256+SHA:!MEDIUM:!LOW:!3DES:!MD5:!PSK:!eNULL:!aNULL:!aDH:!DHE. El resultado del comando confirma que la cadena no permite ninguno de los cifrados que utilizan el algoritmo

DHE:

<#root>

```
    ~ # openssl ciphers -V "EECDH:EDH:HIGH:-AES256+SHA:!MEDIUM:!LOW:!3DES:!MD5:!PSK:!eNULL:!aNULL:!aDH
:!DHE
"
0x13,0x02 - TLS_AES_256_GCM_SHA384 TLSv1.3 Kx=any Au=any Enc=AESGCM(256) Mac=AEAD
0x13,0x03 - TLS_CHACHA20_POLY1305_SHA256 TLSv1.3 Kx=any Au=any Enc=CHACHA20/POLY1305(256) Mac=AEAD
0x13,0x01 - TLS_AES_128_GCM_SHA256 TLSv1.3 Kx=any Au=any Enc=AESGCM(128) Mac=AEAD
0xC0,0x2C - ECDHE-ECDSA-AES256-GCM-SHA384 TLSv1.2 Kx=ECDH Au=ECDSA Enc=AESGCM(256) Mac=AEAD
0xC0,0x30 - ECDHE-RSA-AES256-GCM-SHA384 TLSv1.2 Kx=ECDH Au=RSA Enc=AESGCM(256) Mac=AEAD
0xCC,0xA9 - ECDHE-ECDSA-CHACHA20-POLY1305 TLSv1.2 Kx=ECDH Au=ECDSA Enc=CHACHA20/POLY1305(256) Mac=AEAD
0xCC,0xA8 - ECDHE-RSA-CHACHA20-POLY1305 TLSv1.2 Kx=ECDH Au=RSA Enc=CHACHA20/POLY1305(256) Mac=AEAD
0xC0,0xAD - ECDHE-ECDSA-AES256-CCM TLSv1.2 Kx=ECDH Au=ECDSA Enc=AESCCM(256) Mac=AEAD
0xC0,0x2B - ECDHE-ECDSA-AES128-GCM-SHA256 TLSv1.2 Kx=ECDH Au=ECDSA Enc=AESGCM(128) Mac=AEAD
0xC0,0x2F - ECDHE-RSA-AES128-GCM-SHA256 TLSv1.2 Kx=ECDH Au=RSA Enc=AESGCM(128) Mac=AEAD
0xC0,0xAC - ECDHE-ECDSA-AES128-CCM TLSv1.2 Kx=ECDH Au=ECDSA Enc=AESCCM(128) Mac=AEAD
0xC0,0x24 - ECDHE-ECDSA-AES256-SHA384 TLSv1.2 Kx=ECDH Au=ECDSA Enc=AES(256) Mac=SHA384
0xC0,0x28 - ECDHE-RSA-AES256-SHA384 TLSv1.2 Kx=ECDH Au=RSA Enc=AES(256) Mac=SHA384
0xC0,0x23 - ECDHE-ECDSA-AES128-SHA256 TLSv1.2 Kx=ECDH Au=ECDSA Enc=AES(128) Mac=SHA256
0xC0,0x27 - ECDHE-RSA-AES128-SHA256 TLSv1.2 Kx=ECDH Au=RSA Enc=AES(128) Mac=SHA256
0xC0,0x09 - ECDHE-ECDSA-AES128-SHA TLSv1 Kx=ECDH Au=ECDSA Enc=AES(128) Mac=SHA1
0xC0,0x13 - ECDHE-RSA-AES128-SHA TLSv1 Kx=ECDH Au=RSA Enc=AES(128) Mac=SHA1
0x00,0x9D - AES256-GCM-SHA384 TLSv1.2 Kx=RSA Au=RSA Enc=AESGCM(256) Mac=AEAD
0xC0,0x9D - AES256-CCM TLSv1.2 Kx=RSA Au=RSA Enc=AESCCM(256) Mac=AEAD
0x00,0x9C - AES128-GCM-SHA256 TLSv1.2 Kx=RSA Au=RSA Enc=AESGCM(128) Mac=AEAD
0xC0,0x9C - AES128-CCM TLSv1.2 Kx=RSA Au=RSA Enc=AESCCM(128) Mac=AEAD
0x00,0x3D - AES256-SHA256 TLSv1.2 Kx=RSA Au=RSA Enc=AES(256) Mac=SHA256
0x00,0x3C - AES128-SHA256 TLSv1.2 Kx=RSA Au=RSA Enc=AES(128) Mac=SHA256
0x00,0x2F - AES128-SHA SSLv3 Kx=RSA Au=RSA Enc=AES(128) Mac=SHA1
~ #
```

Probar una conexión TLS mediante la negociación de un cifrado deshabilitado

Puede utilizar el comando openssl s_client para verificar que se rechaza un intento de conexión que utiliza un cifrado deshabilitado. Utilice la opción -connect para especificar la dirección y el puerto de Expressway, y utilice la opción -cipher para especificar el cifrado único que negociará el cliente durante el intercambio de señales de TLS:

openssl s_client -connect <address>:<port> -cipher <cipher> -no_tls1_3

En este ejemplo, se intenta una conexión TLS con Expressway desde un equipo con Windows con openssl instalado. La PC, como cliente, negocia solamente el cifrado DHE-RSA-AES256-CCM no deseado, que utiliza el algoritmo DHE:

<#root>

```
C:\Users\Administrator>

openssl s_client -connect exp.example.com:443 -cipher DHE-RSA-AES256-CCM -no_tls1_3
```

```
Connecting to 10.15.1.7
CONNECTED(00000154)
D0130000:error:0A000410:SSL routines:ssl3_read_bytes:
```

ssl/tls alert handshake failure

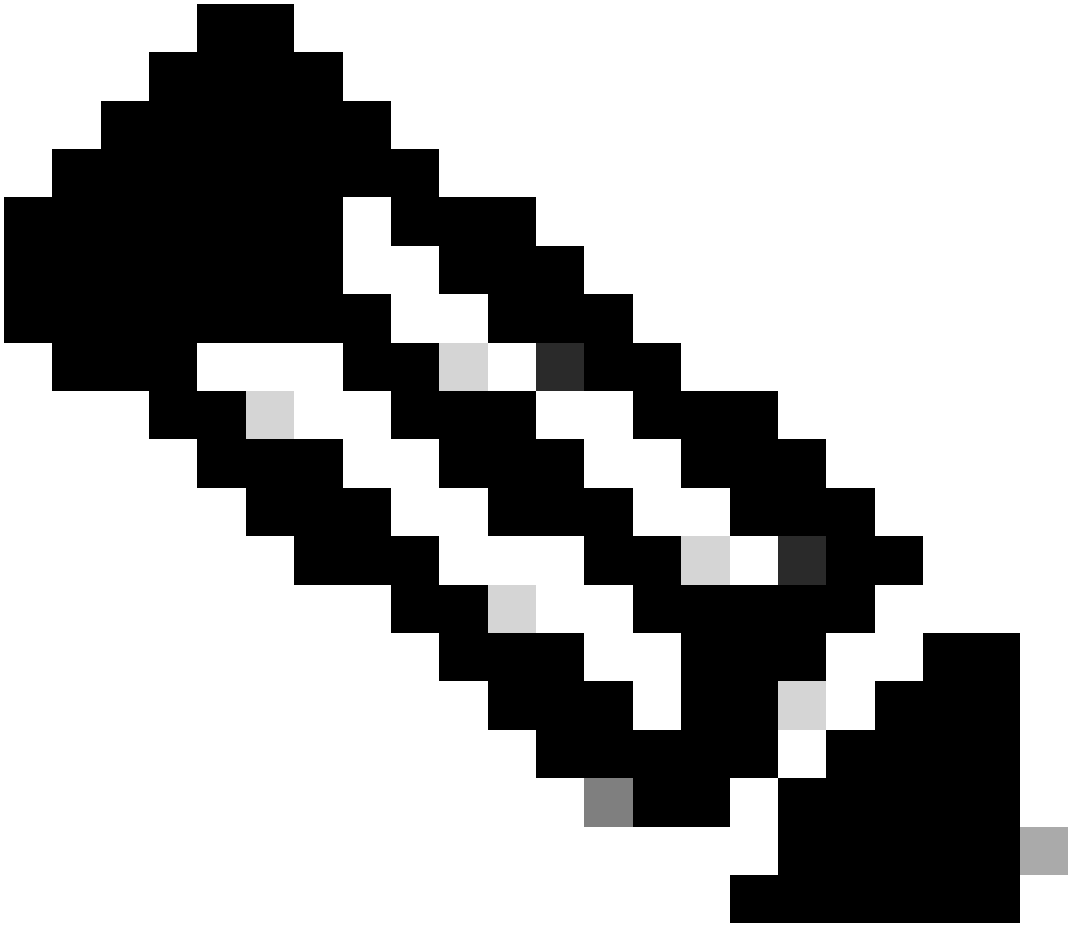
```
:..\ssl\record\rec_layer_s3.c:865:
```

SSL alert number 40

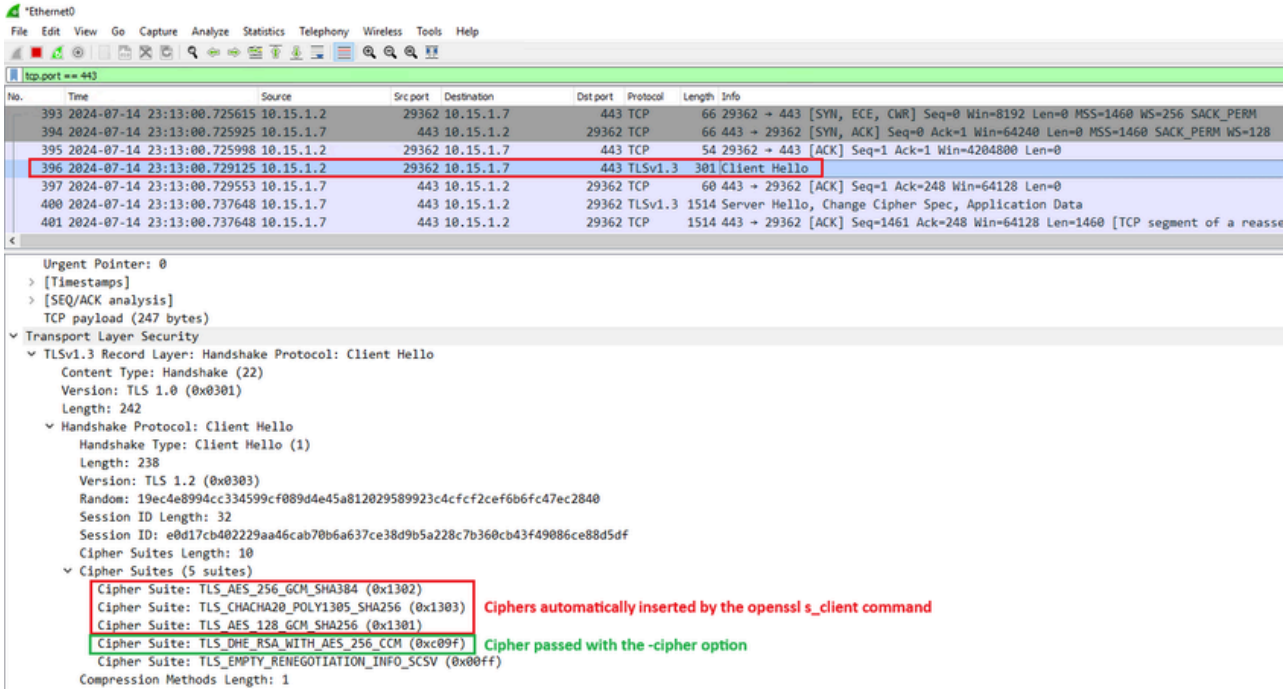
```
---
no peer certificate available
---
No client certificate CA names sent
---
SSL handshake has read 7 bytes and written 118 bytes
Verification: OK
---
New, (NONE), Cipher is (NONE)
Secure Renegotiation IS NOT supported
No ALPN negotiated
SSL-Session:
Protocol : TLSv1.2
Cipher : 0000
Session-ID:
Session-ID-ctx:
Master-Key:
PSK identity: None
PSK identity hint: None
SRP username: None
Start Time: 1721019437
Timeout : 7200 (sec)
Verify return code: 0 (ok)
Extended master secret: no
---

C:\Users\Administrator>
```

El resultado del comando muestra un error en el intento de conexión con un mensaje de error "ssl/tls alert handshake failure:..\ssl\record\rec_layer_s3.c:865:SSL alert number 40", porque Expressway está configurado para utilizar la cadena de cifrado EECDH:EDH:HIGH:-AES256+SHA:!MEDIUM:!LOW:!3DES:!MD5:!PSK:!eNULL:!aNULL:!aDH:!DHE para conexiones HTTPS, lo que deshabilita los cifrados que utilizan el algoritmo DHE.



Nota: Para que las pruebas con el comando openssl s_client funcionen como se explicó, la opción -no_tls1_3 debe pasarse al comando. Si no se incluye, el cliente inserta automáticamente los cifrados TLS 1.3 en el paquete ClientHello:



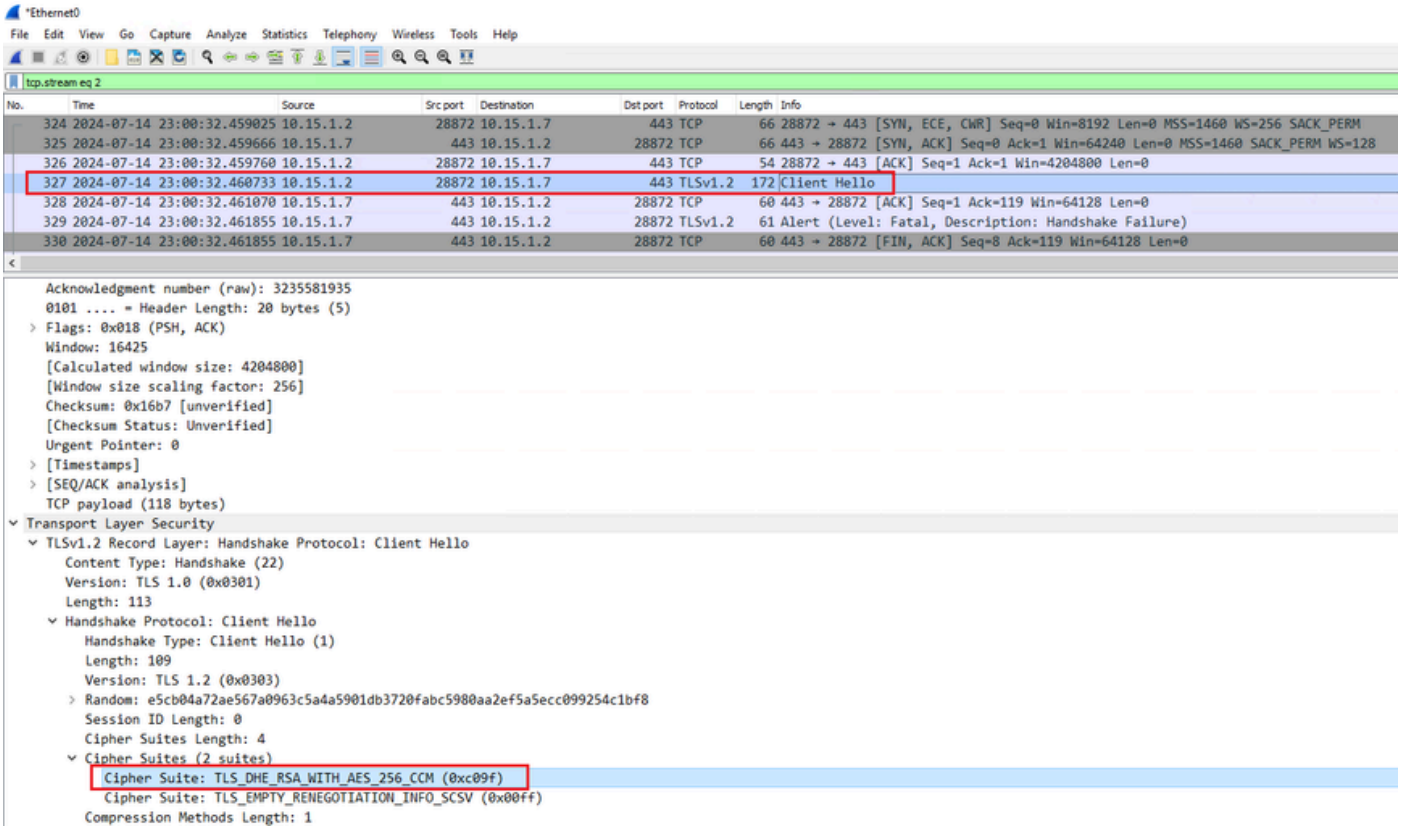
Paquete ClientHello Con Cifrados Agregados Automáticamente

Si Expressway de destino admite esos cifrados, se puede elegir uno de ellos en lugar del cifrado específico que necesita probar. La conexión es exitosa, lo que puede llevarlo a creer que una conexión era posible usando el cifrado inhabilitado pasado al comando con la opción -cipher.

Inspeccionar una captura de paquetes de un intercambio de señales TLS mediante un cifrado deshabilitado

Puede recopilar una captura de paquetes, desde el dispositivo de prueba o desde Expressway, mientras realiza una prueba de conexión mediante uno de los cifrados deshabilitados. A continuación, puede inspeccionarlo con Wireshark para analizar más a fondo los eventos de entrada en contacto.

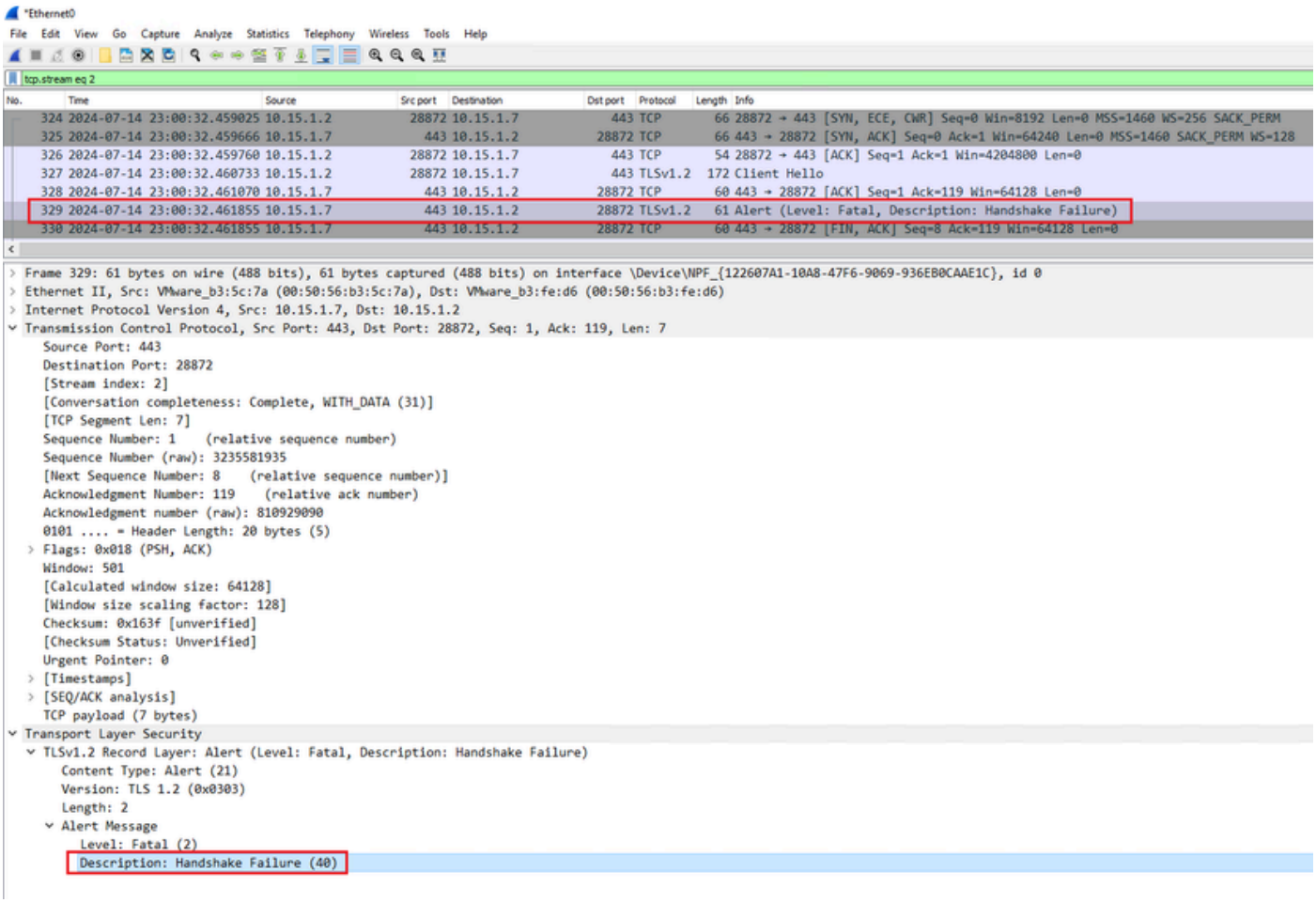
Busque ClientHello enviado por el dispositivo de prueba. Confirme que negocia solamente el cifrado de prueba no deseado, en este ejemplo un cifrado que utiliza el algoritmo DHE:



Ejemplo de un paquete ClientHello en Wireshark

:

Confirme que Expressway responde con un paquete de alerta TLS irrecuperable y rechace la conexión. En este ejemplo, dado que Expressway no admite cifrados DHE por su cadena de cifrado configurada para el protocolo HTTPS, responde con un paquete de alerta TLS fatal que contiene el código de error 40.



Un paquete de alerta de TLS fatal en Wireshark

Información Relacionada

- Página de comando man OpenSSL Ciphers
- Guía del administrador de Cisco Expressway (X15.0) - Capítulo: Administración de la seguridad - Configuración de la versión mínima de TLS y conjuntos de cifrado

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).