Alterar los métodos y los cifradores utilizados con SSL/TLS en el ESA

Contenido

Introducción

Este documento describe cómo modificar los métodos y los códigos que se utilizan con las configuraciones Secure Socket Layer (SSL) o Transport Layer Security (TLS) en Cisco Email Security Appliance (ESA).

Alterar los métodos y los cifradores utilizados con SSL/TLS

> **Nota:** Los métodos SSL/TLS y los códigos deben establecerse en función de las políticas de seguridad y preferencias específicas de su empresa. Para obtener información de terceros con respecto a los cifrados, refiérase al documento Security/Server Side TLS Mozilla para ver las configuraciones recomendadas del servidor y la información detallada.

Con Cisco AsyncOS para Email Security, un administrador puede utilizar el comando **sslconfig** para configurar los protocolos SSL o TLS para los métodos y cifrados que se utilizan para la comunicación GUI, anunciados para conexiones entrantes y solicitados para conexiones salientes:

```
esa.local> sslconfig

sslconfig settings:
GUI HTTPS method: tlsv1/tlsv1.2
GUI HTTPS ciphers:
MEDIUM
HIGH
-SSLv2
-aNULL
!RC4
@STRENGTH
-EXPORT
Inbound SMTP method: tlsv1/tlsv1.2
Inbound SMTP ciphers:
```

```
MEDIUM
HIGH
-SSLv2
-aNULL
!RC4
@STRENGTH
-EXPORT
Outbound SMTP method: tlsv1/tlsv1.2
Outbound SMTP ciphers:
MEDIUM
HIGH
-SSLv2
-aNULL
!RC4
@STRENGTH
-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.
[]> inbound

Enter the inbound SMTP ssl method you want to use.
1. SSL v2
2. SSL v3
3. TLS v1/TLS v1.2
4. SSL v2 and v3
5. SSL v3 and TLS v1/TLS v1.2
6. SSL v2, v3 and TLS v1/TLS v1.2
[3]>

Enter the inbound SMTP ssl cipher you want to use.
[MEDIUM:HIGH:-SSLv2:-aNULL:!RC4:@STRENGTH:-EXPORT]>

sslconfig settings:
GUI HTTPS method: tlsv1/tlsv1.2
GUI HTTPS ciphers:
MEDIUM
HIGH
-SSLv2
-aNULL
!RC4
@STRENGTH
-EXPORT
Inbound SMTP method: tlsv1/tlsv1.2
Inbound SMTP ciphers:
MEDIUM
HIGH
-SSLv2
-aNULL
!RC4
@STRENGTH
-EXPORT
Outbound SMTP method: tlsv1/tlsv1.2
Outbound SMTP ciphers:
MEDIUM
HIGH
-SSLv2
-aNULL
!RC4
@STRENGTH
-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.
[]>
```

Si se realizan cambios en la configuración SSL, asegúrese de que **confirma** todos los cambios.

Métodos SSL

En AsyncOS para Email Security Versiones 9.6 y posteriores, el ESA está configurado para utilizar el método *TLS v1/TLS v1.2* de forma predeterminada. En este caso, TLSv1.2 tiene un precedente para la comunicación, si está siendo utilizado por las partes de envío y recepción. Para establecer una conexión TLS, ambos lados deben tener al menos un método habilitado que coincida y al menos un dígito habilitado que coincida.

> **Nota:** En AsyncOS para las versiones de Email Security anteriores a la versión 9.6, el valor predeterminado tiene dos métodos: *SSL v3* y *TLS v1*. Es posible que algunos administradores deseen desactivar SSL v3 debido a vulnerabilidades recientes (si SSL v3 está activado).

Cifrados SSL

Cuando ve el cifrado predeterminado que se muestra en el ejemplo anterior, es importante comprender la razón por la que muestra dos cifras seguidas de la palabra *ALL*. Aunque *ALL* incluye las dos cifras que lo preceden, el orden de las cifras en la lista de cifras determina la preferencia. Por lo tanto, cuando se realiza una conexión TLS, el cliente elige el primer cifrado que ambos lados admiten en función del orden de aparición en la lista.

> **Nota**: Los cifrados RC4 se habilitan de forma predeterminada en el ESA. En el ejemplo anterior, el **MEDIUM:HIGH** se basa en el documento Evitar Negociaciones para Cifres Nulos o Anónimos en el ESA y SMA de Cisco. Para obtener más información sobre RC4 específicamente, refiérase al documento Security/Server Side TLS Mozilla y también al documento Sobre la seguridad de RC4 en TLS y WPA que se presenta desde el *Simposio de Seguridad USENIX 2013*. Para quitar los cifrados RC4 del uso, consulte los ejemplos siguientes.

A través de la manipulación de la lista de cifras, puede influir en el cifrado elegido. Puede enumerar cifras específicas o rangos de cifras, y también reordenarlos por fuerza con la inclusión de la opción **@STRENGTH** en la cadena de cifrado, como se muestra aquí:

```
Enter the inbound SMTP ssl cipher you want to use.
[RC4-SHA:RC4-MD5:ALL]> MEDIUM:HIGH:-SSLv2:-aNULL:@STRENGTH
```

Asegúrese de revisar todos los códigos e intervalos disponibles en el ESA. Para verlos, ingrese el

comando **sslconfig**, seguido del subcomando **verify**. Las opciones para las categorías de cifrado SSL son **BAJO**, **MEDIO**, **ALTO** y **TODO**:

```
[]> verify

Enter the ssl cipher you want to verify.
[]> MEDIUM

ADH-RC4-MD5 SSLv3 Kx=DH Au=None Enc=RC4(128) Mac=MD5
IDEA-CBC-SHA SSLv3 Kx=RSA Au=RSA Enc=IDEA(128) Mac=SHA1
RC4-SHA SSLv3 Kx=RSA Au=RSA Enc=RC4(128) Mac=SHA1
RC4-MD5 SSLv3 Kx=RSA Au=RSA Enc=RC4(128) Mac=MD5
IDEA-CBC-MD5 SSLv2 Kx=RSA Au=RSA Enc=IDEA(128) Mac=MD5
RC2-CBC-MD5 SSLv2 Kx=RSA Au=RSA Enc=RC2(128) Mac=MD5
RC4-MD5 SSLv2 Kx=RSA Au=RSA Enc=RC4(128) Mac=MD5
```

También puede combinarlos para incluir rangos:

```
[]> verify

Enter the ssl cipher you want to verify.
[]> MEDIUM:HIGH

ADH-RC4-MD5 SSLv3 Kx=DH Au=None Enc=RC4(128) Mac=MD5
IDEA-CBC-SHA SSLv3 Kx=RSA Au=RSA Enc=IDEA(128) Mac=SHA1
RC4-SHA SSLv3 Kx=RSA Au=RSA Enc=RC4(128) Mac=SHA1
RC4-MD5 SSLv3 Kx=RSA Au=RSA Enc=RC4(128) Mac=MD5
IDEA-CBC-MD5 SSLv2 Kx=RSA Au=RSA Enc=IDEA(128) Mac=MD5
RC2-CBC-MD5 SSLv2 Kx=RSA Au=RSA Enc=RC2(128) Mac=MD5
RC4-MD5 SSLv2 Kx=RSA Au=RSA Enc=RC4(128) Mac=MD5
ADH-CAMELLIA256-SHA SSLv3 Kx=DH Au=None Enc=Camellia(256) Mac=SHA1
DHE-RSA-CAMELLIA256-SHA SSLv3 Kx=DH Au=RSA Enc=Camellia(256) Mac=SHA1
DHE-DSS-CAMELLIA256-SHA SSLv3 Kx=DH Au=DSS Enc=Camellia(256) Mac=SHA1
CAMELLIA256-SHA SSLv3 Kx=RSA Au=RSA Enc=Camellia(256) Mac=SHA1
ADH-CAMELLIA128-SHA SSLv3 Kx=DH Au=None Enc=Camellia(128) Mac=SHA1
DHE-RSA-CAMELLIA128-SHA SSLv3 Kx=DH Au=RSA Enc=Camellia(128) Mac=SHA1
DHE-DSS-CAMELLIA128-SHA SSLv3 Kx=DH Au=DSS Enc=Camellia(128) Mac=SHA1
CAMELLIA128-SHA SSLv3 Kx=RSA Au=RSA Enc=Camellia(128) Mac=SHA1
ADH-AES256-SHA SSLv3 Kx=DH Au=None Enc=AES(256) Mac=SHA1
DHE-RSA-AES256-SHA SSLv3 Kx=DH Au=RSA Enc=AES(256) Mac=SHA1
DHE-DSS-AES256-SHA SSLv3 Kx=DH Au=DSS Enc=AES(256) Mac=SHA1
AES256-SHA SSLv3 Kx=RSA Au=RSA Enc=AES(256) Mac=SHA1
ADH-AES128-SHA SSLv3 Kx=DH Au=None Enc=AES(128) Mac=SHA1
DHE-RSA-AES128-SHA SSLv3 Kx=DH Au=RSA Enc=AES(128) Mac=SHA1
DHE-DSS-AES128-SHA SSLv3 Kx=DH Au=DSS Enc=AES(128) Mac=SHA1
AES128-SHA SSLv3 Kx=RSA Au=RSA Enc=AES(128) Mac=SHA1
ADH-DES-CBC3-SHA SSLv3 Kx=DH Au=None Enc=3DES(168) Mac=SHA1
EDH-RSA-DES-CBC3-SHA SSLv3 Kx=DH Au=RSA Enc=3DES(168) Mac=SHA1
EDH-DSS-DES-CBC3-SHA SSLv3 Kx=DH Au=DSS Enc=3DES(168) Mac=SHA1
DES-CBC3-SHA SSLv3 Kx=RSA Au=RSA Enc=3DES(168) Mac=SHA1
DES-CBC3-MD5 SSLv2 Kx=RSA Au=RSA Enc=3DES(168) Mac=MD5
```

Cualquiera de los cifrados SSL que no desea configurar y disponible debe eliminarse con la opción "**-**" que precede a los cifrados específicos. Aquí tiene un ejemplo:

```
[]> MEDIUM:HIGH:-SSLv2:-aNULL:@STRENGTH:-EDH-RSA-DES-CBC3-SHA:
-EDH-DSS-DES-CBC3-SHA:-DES-CBC3-SHA
```

La información en este ejemplo anularía los *códigos NULL*, *EDH-RSA-DES-CBC3-SHA*, *EDH-DSS-DES-CBC3-SHA* y *DES-CBC3-SHA* del anuncio y evitaría su uso en la comunicación SSL.

También puede lograr lo mismo con la inclusión del "**!**" delante del grupo o cadena de cifrado que desea que no esté disponible:

```
[]> MEDIUM:HIGH:-SSLv2:-aNULL:!RC4:@STRENGTH
```

La información de este ejemplo quitaría el uso de todos los elementos RC4. Por lo tanto, los cifrados *RC4-SHA* y *RC4-MD5* se negarían y no se anunciarían en la comunicación SSL.

Si se realizan cambios en la configuración SSL, asegúrese de que **confirma** todos los cambios.