Altere los métodos y las cifras usados con el SSL/TLS en el ESA

Contenido

Introducción

Este documento describe cómo alterar los métodos y las cifras que se utilizan con las configuraciones del Secure Socket Layer (SSL) o de Transport Layer Security (TLS) en Cisco envían por correo electrónico el dispositivo de seguridad (ESA).

Altere los métodos y las cifras usados con el SSL/TLS

> Nota: Los métodos y las cifras SSL/TLS se deben fijar basadas en las políticas de seguridad y las preferencias específicas de su compañía. Para la información de tercera persona con respecto a las cifras, refiera documento del Mozilla a TLS de la Seguridad/del lado del servidor para las Configuraciones del servidor y la información detallada recomendadas.

Con Cisco AsyncOS para la Seguridad del correo electrónico, un administrador puede utilizar el comando del **sslconfig** para configurar el SSL o los protocolos TLS para los métodos y las cifras que se utilizan para la comunicación GUI, se hacen publicidad para las conexiones hacia adentro, y se piden para las 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 los cambios se realizan a la configuración de SSL, asegúrese de que usted **confíe** cualquiera y todos los cambios.

Métodos SSL

En AsyncOS para las versiones 9.6 de la Seguridad del correo electrónico y posterior, el ESA se fija para utilizar el método del *v1.2 de TLS v1/TLS* por abandono. En este caso, TLSv1.2 toma el precedente para la comunicación, si es funcionando por el envío y las partes receptoras. Para establecer una conexión TLS, los ambos lados deben tener por lo menos un método habilitado que haga juego, y por lo menos uno habilitó la cifra que hace juego.

> Nota: En AsyncOS para las versiones de la Seguridad del correo electrónico antes de la versión 9.6, el valor por defecto tiene dos métodos: *V3 SSL* y *v1 de TLS*. Algunos administradores pudieron querer inhabilitar el v3 SSL debido a las vulnerabilidades recientes (si se habilita el v3 SSL).

Cifras SSL

Cuando usted ve la cifra predeterminada que se enumera en el ejemplo anterior, es importante entender la razón que muestra dos cifras seguidas por la palabra *TODA*. Aunque *TODO* incluya las dos cifras que lo preceden, la orden de las cifras en la lista de la cifra determina la preferencia. Así, cuando se hace una conexión TLS, el cliente escoge la primera cifra que el soporte de los ambos lados basó por orden del aspecto en la lista.

> Nota: Las cifras RC4 se habilitan por abandono en el ESA. En el ejemplo anterior, el **MEDIA: El ALTO** se basa en las negociaciones de la prevención para las cifras nulas o anónimas en el documento de Cisco ESA y S A. Para más información con respecto al RC4 específicamente, refiera documento del Mozilla a TLS de la Seguridad/del lado del servidor, y también encendido la Seguridad del RC4 en el documento de TLS y WPA que se presenta del *simposio 2013 de la Seguridad USENIX*. Para quitar las cifras RC4 del uso, refiera a los ejemplos que siguen.

Con la manipulación de la lista de la cifra, usted puede influenciar la cifra se elige que. Usted puede enumerar las cifras o los rangos específicos de la cifra, y también los reordena por la fuerza con la inclusión de la opción **@STRENGTH** en la cadena de la cifra, 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 que usted revise todas las cifras y rangos que estén disponibles en el ESA. Para

ver éstos, ingrese el comando del **sslconfig**, seguido por el submandato del **verificar**. Las opciones para las categorías de la cifra SSL son **BAJAS**, **MEDIAS**, **ALTAS**, y **TODAS**:

```
[]> 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
```

Usted puede también combinar éstos para incluir los 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
```

Las cifras SSL que usted no quiere configurado y disponible uces de los se deben quitar con "**-**" la opción que precede las cifras específicas. 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 negaría las cifras de la *FALTA DE INFORMACIÓN*, *EDH-RSA-DES-CBC3-SHA*, *EDH-DSS-DES-CBC3-SHA*, y *DES-CBC3-SHA del* anuncio y prevendría su uso en la comunicación SSL.

Usted puede también lograr similar con la inclusión del "**!**" carácter delante del grupo de la cifra o

cadena que usted desea de hacer inasequible:

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

La información en este ejemplo quitaría todas las cifras RC4 del uso. Así, las cifras del *RC4-SHA* y del *RC4-MD5* serían negadas y no hechas publicidad en la comunicación SSL.

Si los cambios se realizan a la configuración de SSL, asegúrese de que usted confíe cualquiera y todos los cambios.