Configuración ESA para preferir el Confidencialidad directa perfecta (PFS)

Contenido

Introducción

Este documento describe cómo configurar la preferencia por el Confidencialidad directa perfecta (PFS) en las conexiones encrpyted de Transport Layer Security (TLS) en el dispositivo de seguridad del correo electrónico (ESA).

Prerrequisitos

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- SSL/TLS

Componentes Utilizados

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

- AsyncOS para la versión 9.6 y posterior del correo electrónico

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 la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Antecedentes

El ESA ofrece el secreto delantero (perfecta reserva hacia adelante). El secreto delantero significa que los datos están transferidos vía un canal que esté utilizando el cifrado simétrico con los secretos efímeros, e incluso si la clave privada (clave a largo plazo) en uno o ambos host fue comprometida, no es posible desencriptar una sesión previamente registrada.

El secreto no se transfiere a través del canal, en lugar el secreto compartido se deriva usando un *problema matemático (problema del Diffie Hellman).* El secreto no se salva en cualquier parte que memoria de acceso aleatorio de los host (RAM) durante la sesión establecida (o el descanso de la regeneración de la clave).

El ESA soporta el **Diffie Hellman (DH) para el intercambio de claves**.

Configurar

ENTRANTE - ESA que actúa como servidor de TLS

Debajo de la cifra las habitaciones están disponibles en el ESA para el tráfico entrante S TP que proporcionan el secreto delantero. La selección abajo de la cifra del *ejemplo* permite solamente las habitaciones de la cifra consideraba el *ALTO* o *MEDIA* y uso DH efímero para el intercambio de claves y prefiere TLSv1.2. El sintaxis de la selección de la cifra sigue el sintaxis del OpenSSL.

Cifras con el secreto delantero en AsyncOS 9.6+

```
"EDH+TLSv1.2:EDH+HIGH:EDH+MEDIUM:!LOW:!EXP:!aNULL:!RC4:!DSS:!SEED:!IDEA:!MD5:!PSK:!3DES:!SRP"

List:  DHE-RSA-AES256-GCM-SHA384 TLSv1.2 Kx=DH Au=RSA Enc=AESGCM(256) Mac=AEAD
DHE-RSA-AES256-SHA256 TLSv1.2 Kx=DH Au=RSA Enc=AES(256) Mac=SHA256
DHE-RSA-AES128-GCM-SHA256 TLSv1.2 Kx=DH Au=RSA Enc=AESGCM(128) Mac=AEAD
DHE-RSA-AES128-SHA256 TLSv1.2 Kx=DH Au=RSA Enc=AES(128) Mac=SHA256
DHE-RSA-AES256-SHA SSLv3 Kx=DH Au=RSA Enc=AES(256) Mac=SHA1
DHE-RSA-CAMELLIA256-SHA SSLv3 Kx=DH Au=RSA Enc=Camellia(256) Mac=SHA1
DHE-RSA-AES128-SHA SSLv3 Kx=DH Au=RSA Enc=AES(128) Mac=SHA1
DHE-RSA-CAMELLIA128-SHA SSLv3 Kx=DH Au=RSA Enc=Camellia(128) Mac=SHA1
```

La sección **KX** (= intercambio de claves) muestra que el Diffie Hellman está utilizado para derivar el secreto.

El ESA soporta estas cifras con las configuraciones predeterminadas del sslconfig (: TODO), pero no lo prefiere. Si usted quiere preferir las cifras que ofrecen el PFS, usted necesitaría cambiar su **sslconfig** y agregar el Diffie Hellman efímero (EDH*)* o una combinación "*name> del grupo EDH+<cipher o de la cifra*" a su selección de la cifra.

Configuración predeterminada:

```
"EDH+TLSv1.2:EDH+HIGH:EDH+MEDIUM:!LOW:!EXP:!aNULL:!RC4:!DSS:!SEED:!IDEA:!MD5:!PSK:!3DES:!SRP"

List:  DHE-RSA-AES256-GCM-SHA384 TLSv1.2 Kx=DH Au=RSA Enc=AESGCM(256) Mac=AEAD
DHE-RSA-AES256-SHA256 TLSv1.2 Kx=DH Au=RSA Enc=AES(256) Mac=SHA256
DHE-RSA-AES128-GCM-SHA256 TLSv1.2 Kx=DH Au=RSA Enc=AESGCM(128) Mac=AEAD
DHE-RSA-AES128-SHA256 TLSv1.2 Kx=DH Au=RSA Enc=AES(128) Mac=SHA256
DHE-RSA-AES256-SHA SSLv3 Kx=DH Au=RSA Enc=AES(256) Mac=SHA1
DHE-RSA-CAMELLIA256-SHA SSLv3 Kx=DH Au=RSA Enc=Camellia(256) Mac=SHA1
DHE-RSA-AES128-SHA SSLv3 Kx=DH Au=RSA Enc=AES(128) Mac=SHA1
```

```
DHE-RSA-CAMELLIA128-SHA SSLv3 Kx=DH Au=RSA Enc=Camellia(128) Mac=SHA1
```

Nueva configuración:

```
"EDH+TLSv1.2:EDH+HIGH:EDH+MEDIUM:!LOW:!EXP:!aNULL:!RC4:!DSS:!SEED:!IDEA:!MD5:!PSK:!3DES:!SRP"

List:  DHE-RSA-AES256-GCM-SHA384 TLSv1.2 Kx=DH Au=RSA Enc=AESGCM(256) Mac=AEAD
DHE-RSA-AES256-SHA256 TLSv1.2 Kx=DH Au=RSA Enc=AES(256) Mac=SHA256
DHE-RSA-AES128-GCM-SHA256 TLSv1.2 Kx=DH Au=RSA Enc=AESGCM(128) Mac=AEAD
DHE-RSA-AES128-SHA256 TLSv1.2 Kx=DH Au=RSA Enc=AES(128) Mac=SHA256
DHE-RSA-AES256-SHA SSLv3 Kx=DH Au=RSA Enc=AES(256) Mac=SHA1
DHE-RSA-CAMELLIA256-SHA SSLv3 Kx=DH Au=RSA Enc=Camellia(256) Mac=SHA1
DHE-RSA-AES128-SHA SSLv3 Kx=DH Au=RSA Enc=AES(128) Mac=SHA1
DHE-RSA-CAMELLIA128-SHA SSLv3 Kx=DH Au=RSA Enc=Camellia(128) Mac=SHA1
```

> Nota: El RC4 como una cifra y MD5 como MAC se considera débil, herencia y evitar para el uso con el SSL/TLS, especialmente cuando se trata de un volumen más alto de los datos sin la regeneración dominante.

Configuraciones recomendadas del sslconfig para ENTRANTE

Lo que sigue es opinión que prevalece y permitir solamente las cifras que generalmente se consideran fuertes y seguras

Una configuración recomendable para ENTRANTE que quita el RC4 y MD5 así como otra herencia y opciones débiles, a saber la exportación (EXP), bajo (BAJO), IDEA (IDEA), GERMEN (GERMEN), las cifras 3DES (3DES), los Certificados DSS (DSS) y intercambio de claves anónimo (aNULL) y las claves previamente compartidas (PSK) y el protocolo SRP (SRP) y inhabilita ECDH y ECDSA estaría por ejemplo:

```
"EDH+TLSv1.2:EDH+HIGH:EDH+MEDIUM:!LOW:!EXP:!aNULL:!RC4:!DSS:!SEED:!IDEA:!MD5:!PSK:!3DES:!SRP"

List:  DHE-RSA-AES256-GCM-SHA384 TLSv1.2 Kx=DH Au=RSA Enc=AESGCM(256) Mac=AEAD
DHE-RSA-AES256-SHA256 TLSv1.2 Kx=DH Au=RSA Enc=AES(256) Mac=SHA256
DHE-RSA-AES128-GCM-SHA256 TLSv1.2 Kx=DH Au=RSA Enc=AESGCM(128) Mac=AEAD
DHE-RSA-AES128-SHA256 TLSv1.2 Kx=DH Au=RSA Enc=AES(128) Mac=SHA256
DHE-RSA-AES256-SHA SSLv3 Kx=DH Au=RSA Enc=AES(256) Mac=SHA1
DHE-RSA-CAMELLIA256-SHA SSLv3 Kx=DH Au=RSA Enc=Camellia(256) Mac=SHA1
DHE-RSA-AES128-SHA SSLv3 Kx=DH Au=RSA Enc=AES(128) Mac=SHA1
DHE-RSA-CAMELLIA128-SHA SSLv3 Kx=DH Au=RSA Enc=Camellia(128) Mac=SHA1
```

El antedicho de la cadena ingresado en el **sslconfig** da lugar a esta lista de cifras soportadas para ENTRANTE:

```
"EDH+TLSv1.2:EDH+HIGH:EDH+MEDIUM:!LOW:!EXP:!aNULL:!RC4:!DSS:!SEED:!IDEA:!MD5:!PSK:!3DES:!SRP"

List:  DHE-RSA-AES256-GCM-SHA384 TLSv1.2 Kx=DH Au=RSA Enc=AESGCM(256) Mac=AEAD
DHE-RSA-AES256-SHA256 TLSv1.2 Kx=DH Au=RSA Enc=AES(256) Mac=SHA256
DHE-RSA-AES128-GCM-SHA256 TLSv1.2 Kx=DH Au=RSA Enc=AESGCM(128) Mac=AEAD
DHE-RSA-AES128-SHA256 TLSv1.2 Kx=DH Au=RSA Enc=AES(128) Mac=SHA256
DHE-RSA-AES256-SHA SSLv3 Kx=DH Au=RSA Enc=AES(256) Mac=SHA1
DHE-RSA-CAMELLIA256-SHA SSLv3 Kx=DH Au=RSA Enc=Camellia(256) Mac=SHA1
DHE-RSA-AES128-SHA SSLv3 Kx=DH Au=RSA Enc=AES(128) Mac=SHA1
DHE-RSA-CAMELLIA128-SHA SSLv3 Kx=DH Au=RSA Enc=Camellia(128) Mac=SHA1
```

Nota: El ESA que actúa como servidor de TLS (tráfico entrante) no soporta actualmente el Diffie Hellman elíptico de la curva para el intercambio de claves (*ECDHE*) y los Certificados elípticos del Digital Signature Algorithm de la curva (*ECDSA*).

SALIENTE - ESA que actúa como cliente de TLS

Para el tráfico saliente S TP el ESA **además del** intercambio de claves efímero de los soportes del Diffie Hellman elíptico **ENTRANTE de la** curva (*ECDHE*) y de los Certificados elípticos del Digital Signature Algorithm de la curva (*ECDSA*).

Nota: Los Certificados elípticos de la criptografía de la curva (ECC) con el algoritmo elíptico de la firma de Digitial de la curva, (ECDSA) no se adoptan extensamente.

Al entregar el correo electrónico (saliente), el ESA es el cliente de TLS. Un certificado del TLS-cliente es opcional. Si el TLS-servidor no fuerza (requerir) el ESA (como TLS-cliente) para proporcionar un certificado del cliente ECDSA, el ESA puede continuar con una sesión asegurada ECDSA. Cuando el ESA como el TLS-cliente se pide su certificado, proporciona el certificado configurado ***RSA*** para la dirección saliente.

Precaución: ¡*El almacén de confianza* instalado previamente del *certificado de CA* (*lista del sistema*) en el ESA no incluye los certificados raíz ECC (ECDSA)! Puede ser requerido agregar manualmente los certificados raíz ECC (que usted confianza) a la *lista de encargo* para hacer el encadenamiento ECC de la confianza comprobable.

Para preferir las cifras DHE/ECDHE que ofrecen el secreto delantero, usted puede modificar la selección de la cifra del **sslconfig** como sigue.

Agregue el abajo a su selección existente de la cifra.

```
"EDH+TLSv1.2:EDH+HIGH:EDH+MEDIUM:!LOW:!EXP:!aNULL:!RC4:!DSS:!SEED:!IDEA:!MD5:!PSK:!3DES:!SRP"

List:  DHE-RSA-AES256-GCM-SHA384 TLSv1.2 Kx=DH Au=RSA Enc=AESGCM(256) Mac=AEAD
DHE-RSA-AES256-SHA256 TLSv1.2 Kx=DH Au=RSA Enc=AES(256) Mac=SHA256
DHE-RSA-AES128-GCM-SHA256 TLSv1.2 Kx=DH Au=RSA Enc=AESGCM(128) Mac=AEAD
DHE-RSA-AES128-SHA256 TLSv1.2 Kx=DH Au=RSA Enc=AES(128) Mac=SHA256
DHE-RSA-AES256-SHA SSLv3 Kx=DH Au=RSA Enc=AES(256) Mac=SHA1
DHE-RSA-CAMELLIA256-SHA SSLv3 Kx=DH Au=RSA Enc=Camellia(256) Mac=SHA1
DHE-RSA-AES128-SHA SSLv3 Kx=DH Au=RSA Enc=AES(128) Mac=SHA1
DHE-RSA-CAMELLIA128-SHA SSLv3 Kx=DH Au=RSA Enc=Camellia(128) Mac=SHA1
```

Configuraciones recomendadas del sslconfig para SALIENTE

Lo que sigue es opinión que prevalece y permitir solamente las cifras que generalmente se consideran fuertes y seguras

```
"EDH+TLSv1.2:EDH+HIGH:EDH+MEDIUM:!LOW:!EXP:!aNULL:!RC4:!DSS:!SEED:!IDEA:!MD5:!PSK:!3DES:!SRP"

List:  DHE-RSA-AES256-GCM-SHA384 TLSv1.2 Kx=DH Au=RSA Enc=AESGCM(256) Mac=AEAD
DHE-RSA-AES256-SHA256 TLSv1.2 Kx=DH Au=RSA Enc=AES(256) Mac=SHA256
DHE-RSA-AES128-GCM-SHA256 TLSv1.2 Kx=DH Au=RSA Enc=AESGCM(128) Mac=AEAD
DHE-RSA-AES128-SHA256 TLSv1.2 Kx=DH Au=RSA Enc=AES(128) Mac=SHA256
DHE-RSA-AES256-SHA SSLv3 Kx=DH Au=RSA Enc=AES(256) Mac=SHA1
DHE-RSA-CAMELLIA256-SHA SSLv3 Kx=DH Au=RSA Enc=Camellia(256) Mac=SHA1
```

```
DHE-RSA-AES128-SHA SSLv3 Kx=DH Au=RSA Enc=AES(128) Mac=SHA1
DHE-RSA-CAMELLIA128-SHA SSLv3 Kx=DH Au=RSA Enc=Camellia(128) Mac=SHA1
```

El antedicho de la cadena ingresado en el **sslconfig** da lugar a esta lista de cifras soportadas para SALIENTE:

```
"EDH+TLSv1.2:EDH+HIGH:EDH+MEDIUM:!LOW:!EXP:!aNULL:!RC4:!DSS:!SEED:!IDEA:!MD5:!PSK:!3DES:!SRP"

List:  DHE-RSA-AES256-GCM-SHA384 TLSv1.2 Kx=DH Au=RSA Enc=AESGCM(256) Mac=AEAD
DHE-RSA-AES256-SHA256 TLSv1.2 Kx=DH Au=RSA Enc=AES(256) Mac=SHA256
DHE-RSA-AES128-GCM-SHA256 TLSv1.2 Kx=DH Au=RSA Enc=AESGCM(128) Mac=AEAD
DHE-RSA-AES128-SHA256 TLSv1.2 Kx=DH Au=RSA Enc=AES(128) Mac=SHA256
DHE-RSA-AES256-SHA SSLv3 Kx=DH Au=RSA Enc=AES(256) Mac=SHA1
DHE-RSA-CAMELLIA256-SHA SSLv3 Kx=DH Au=RSA Enc=Camellia(256) Mac=SHA1
DHE-RSA-AES128-SHA SSLv3 Kx=DH Au=RSA Enc=AES(128) Mac=SHA1
DHE-RSA-CAMELLIA128-SHA SSLv3 Kx=DH Au=RSA Enc=Camellia(128) Mac=SHA1
```

Información Relacionada

- Abra las cifras SSL
- Cifrado de la última generación de Cisco