Configure el ESA para preferir PFS

Contenido

Introducción

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

Prerequisites

Requisitos

Cisco recomienda que usted tiene conocimiento de Secure Sockets Layer (SSL) /TLS.

Componentes usados

La información en este documento se basa en 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 (PFS). El secreto delantero significa que los datos están transferidos vía un canal que utilice 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 con un problema matemático problema (de Diffie Hellman (ADO)). El secreto no se salva en cualquier parte que memoria de acceso aleatorio de los host (RAM) durante el descanso de la regeneración de la sesión establecida o de la clave.

El ESA utiliza el ADO para el intercambio dominante.

Configurar

ENTRANTE - El ESA actúa como servidor de TLS

Estas habitaciones de la cifra están disponibles en el ESA para el tráfico ENTRANTE del Simple Mail Transfer Protocol (SMTP) que proporcionan al secreto delantero. En este ejemplo, la selección de la cifra permite solamente las habitaciones de la cifra consideraba el ALTO o MEDIA y uso Diffie efímero Hellman (EDH) para el intercambio dominante y prefiere TLSv1.2. El sintaxis de la selección de la cifra sigue el sintaxis de 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 la clave) muestra que el ADO está utilizado para derivar el secreto.

El ESA utiliza estas cifras con las configuraciones del **sslconfig del** valor por defecto (: TODO), pero no lo prefiere. Si usted quiere preferir las cifras que ofrecen PFS, usted necesita cambiar su **sslconfig** y agregar EDH o una combinación **EDH+<cipher o name> del grupo de la cifra a** su selección de la cifra.

Configuración de valor por defecto:

```
"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
```

Note: El RC4 como una cifra y MD5 como MAC se considera débil, herencia y para evitar 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

Esto es una opinión que prevalece y permitir solamente las cifras que generalmente se consideran fuertes y seguras.

Una configuración recomendable para que quita el RC4 ENTRANTE 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), intercambio dominante anónimo (aNULL), las claves previamente compartidas (PSK), el protocolo SRP (SRP), la curva elíptica Diffie Hellman (ECDH) de las neutralizaciones para el intercambio dominante y el algoritmo elíptico de la firma digital de la curva (ECDSA) es los ejemplos:

```
"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 cadena ingresada en el **sslconfig** da lugar a esta lista de cifras utilizadas 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
```

Note: El ESA que actúa como servidor de TLS (tráfico entrante) actualmente no utiliza la curva elíptica Diffie Hellman para el intercambio dominante (ECDHE) y los Certificados ECDSA.

SALIENTE - El ESA actúa como cliente de TLS

Para el tráfico SALIENTE SMTP, el ESA además de las ayudas ENTRANTES ECDHE y los Certificados ECDSA.

> **Note**: Los Certificados elípticos de la criptografía de la curva (ECC) con el ECDSA no se adoptan extensamente.

Cuando se entrega un 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 a un certificado del cliente ECDSA, el ESA puede continuar con una sesión asegurada ECDSA. Cuando el ESA como el TLS-cliente se pide él es certificado, proporciona al certificado configurado RSA para la dirección saliente.

> **Caution**: ¡El almacén de certificados de confianza instalado previamente CA (lista del sistema) en el ESA no incluye los certificados raíz ECC (ECDSA)! Usted puede ser que necesite agregar manualmente al ECC que los certificados raíz (que usted confianza) a la lista de encargo en el orderto hacen 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 esto a su selección actual 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

Esto es una 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
```

La cadena ingresada en el **sslconfig** da lugar a esta lista de cifras utilizadas 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
```

Verifique

Actualmente, no hay un procedimiento de verificación disponible para esta configuración.

Troubleshooting

No hay actualmente información disponible específica del troubleshooting para esta configuración.

Información Relacionada

- Abra las cifras SSL
- Cifrado de la última generación de Cisco
- Soporte técnico y documentación - Cisco Systems