Configuración de ESA para preferir PFS

Contenido

Introducción

Este documento describe cómo configurar la preferencia de Confidencialidad directa perfecta (PFS) en conexiones cifradas de Seguridad de la capa de transporte (TLS) en el dispositivo de seguridad de correo electrónico (ESA).

Prerequisites

Requirements

Cisco recomienda que conozca Secure Sockets Layer (SSL)/TLS.

Componentes Utilizados

La información de este documento se basa en AsyncOS para Email versión 9.6 y posterior.

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). If your network is live, make sure that you understand the potential impact of any command.

Antecedentes

El ESA no ofrece Confidencialidad directa (PFS). La confidencialidad directa significa que los datos se transfieren a través de un canal que utiliza cifrado simétrico con secretos efímeros e

incluso si la clave privada (clave a largo plazo) de uno o ambos hosts se ha visto comprometida, no es posible descifrar una sesión previamente grabada.

El secreto no se transfiere a través del canal, en lugar del secreto compartido se deriva con un problema matemático (Diffie Hellman (DH) Problema). El secreto no se almacena en ningún otro lugar que la memoria de acceso aleatorio (RAM) de los hosts durante la sesión establecida o el tiempo de espera de regeneración de claves.

El ESA admite DH para el intercambio de claves.

Configurar

ENTRANTE: ESA actúa como servidor TLS

Estos conjuntos de cifrado están disponibles en el ESA para el tráfico SMTP (protocolo simple de transferencia de correo) entrante que proporciona Confidencialidad directa. En este ejemplo, la selección de cifrado solo permite conjuntos de cifrado considerados ALTOS o MEDIOS y utiliza Diffie Hellman (EDH) efímero para el intercambio de claves y prefiere TLSv1.2. La sintaxis de selección de cifrado sigue la sintaxis de OpenSSL.

Cifrados con Confidencialidad directa en AsyncOS 9.6+:

<#root>

"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 (= Key Exchange) muestra que DH se utiliza para derivar el secreto.

El ESA soporta estos cifrados con la configuración predeterminada sslconfig (:ALL), pero no lo prefiere. Si desea preferir los cifrados que ofrecen PFS, debe cambiar su sslconfig y agregar EDH o una combinación de EDH+<cipher or cipher group name> a su selección de cifrado.

Configuración predeterminada:

```
ESA> sslconfig

sslconfig settings:
  Inbound SMTP method:  tlsv1/tlsv1.2
  Inbound SMTP ciphers:
        RC4-SHA
        RC4-MD5
        ALL
```

Nueva configuración:

```
ESA> sslconfig

Inbound SMTP method:  tlsv1/tlsv1.2
  Inbound SMTP ciphers:
        EDH+TLSv1.2
        EDH+HIGH
        EDH+MEDIUM
        RC4-SHA
        RC4-MD5
        ALL
```

Nota: RC4 como cifrado y MD5 como MAC se considera débil, heredado y para evitar el uso con SSL/TLS, especialmente cuando se trata de un mayor volumen de datos sin regeneración de claves.

Configuración de sslconfig recomendada para INBOUND

Esta es una opinión predominante y sólo permite cifrados que generalmente se consideran fuertes y seguros.

Los ejemplos son una configuración recomendada para INBOUND que elimina RC4 y MD5, así como otras opciones antiguas y débiles, como Exportar (EXP), Bajo (LOW), IDEA (IDEA), SEED (SEED), cifrados 3DES (3DES), certificados DSS (DSS), Intercambio de claves anónimas (aNULL), Claves previamente compartidas (PSK), protocolo SRP (SRP), deshabilita Elliptic Curve Diffie Hellman (ECDH) para intercambio de claves y Elliptic Curve Digital Signature Algorithm (ECDSA):

```
EDH+TLSv1.2:EDH+HIGH:EDH+MEDIUM:HIGH:MEDIUM:!ECDH:!ECDSA:!LOW:!EXP:!aNULL:!RC4:!DSS:!SEED:!IDEA:!MD5:!P
```

La cadena ingresada en sslconfig da como resultado esta lista de cifrados soportados para INBOUND:

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

Nota: El ESA que actúa como servidor TLS (tráfico ENTRANTE) actualmente no admite Elliptic Curve Diffie Hellman for Key Exchange (ECDHE) y certificados ECDSA.

SALIENTE: ESA actúa como cliente TLS

Para el tráfico SMTP SALIENTE, el ESA, además de INBOUND, admite certificados ECDHE y ECDSA.

Nota: los certificados de criptografía de curva elíptica (ECC) con ECDSA no se han

adoptado de forma generalizada.

Cuando se envía un correo electrónico SALIENTE, el ESA es el cliente TLS. Un certificado de cliente TLS es opcional. Si el servidor TLS no fuerza (requiere) el ESA (como cliente TLS) para proporcionar un certificado de cliente ECDSA, el ESA puede continuar con una sesión segura ECDSA. Cuando se solicita el certificado del ESA como cliente de TLS, éste proporciona el certificado RSA configurado para la dirección SALIENTE.

Precaución: el almacén de certificados de CA de confianza (lista de sistemas) preinstalado en el ESA no incluye certificados raíz ECC (ECDSA). Es posible que tenga que agregar manualmente certificados raíz ECC (en los que confía) a la lista personalizada para que la cadena de confianza ECC sea verificable.

Para preferir los cifrados DHE/ECDHE que ofrecen Confidencialidad directa, puede modificar la selección del cifrado sslconfig de la siguiente manera.

Añada esto a su selección de cifrado actual.

```
"EDH+TLSv1.2:ECDH+TLSv1.2:EDH+HIGH:EDH+MEDIUM:ECDH+HIGH:ECDH+MEDIUM"
```

Valores de configuración de sslconfig recomendados para SALIENTES

Esta es una opinión predominante y sólo permite cifrados que generalmente se consideran fuertes y seguros.

```
EDH+TLSv1.2:ECDH+TLSv1.2:EDH+HIGH:EDH+MEDIUM:ECDH+HIGH:ECDH+MEDIUM:HIGH:MEDIUM:!LOW:!EXP:!aNULL:!RC4:!D
```

La cadena ingresada en sslconfig da como resultado esta lista de cifrados soportados para OUTBOUND:

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

Verificación

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

Troubleshoot

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.

Información Relacionada

- Cifrados SSL abiertos
- Cifrado Cisco Next Generation
- Soporte Técnico y Documentación - Cisco Systems

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).