Configurar o ESA para preferir o discrição perfeita adiante (PFS)

Índice

Introdução

Este documento descreve como configurar a preferência para o discrição perfeita adiante (PFS) em conexões encrpyted do Transport Layer Security (TLS) na ferramenta de segurança do email (ESA).

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- SSL/TLS

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- AsyncOS para a versão 9.6 e mais recente do email

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Informações de Apoio

O ESA oferece o secretismo dianteiro (discrição perfeita adiante). O secretismo dianteiro significa que os dados estão transferidos através de um canal que esteja usando a criptografia simétrica com segredos efêmeros, e mesmo se a chave privada (chave a longo prazo) em um ou em ambos os anfitriões foi comprometida, não é possível decifrar uma sessão previamente gravada.

O segredo não é transferido através do canal, em lugar do segredo compartilhado é derivado usando um *problema matemático (problema do Diffie Hellman)*. O segredo não é armazenado em qualquer outro lugar do que a memória de acesso aleatório dos anfitriões (RAM) durante a sessão estabelecida (ou o intervalo da regeneração da chave).

O ESA apoia o **Diffie Hellman (DH) para trocas de chave**.

Configurar

DE ENTRADA - ESA que atua como o server TLS

Abaixo da cifra as séries estão disponíveis no ESA para o tráfego de entrada S TP que fornecem o secretismo dianteiro. A seleção abaixo da cifra do *exemplo* permite somente séries da cifra considerou a *ELEVAÇÃO* ou o *MEDIA* e o uso DH efêmero para trocas de chave e prefere TLSv1.2. A sintaxe da seleção da cifra segue a sintaxe do OpenSSL.

Cifras com secretismo dianteiro em 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
```

A seção **Kx** (= trocas de chave) mostra que o Diffie Hellman está usado para derivar o segredo.

O ESA apoia estas cifras com os ajustes do sslconfig do padrão (: TUDO), mas não o prefere. Se você quer preferir as cifras que oferecem o PFS, você precisaria de mudar seu **sslconfig** e de adicionar o Diffie Hellman efêmero (EDH*)* ou uma combinação "*EDH+<cipher ou name> do grupo da cifra*" a sua seleção da cifra.

Configuração padrão:

```
"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
```

Configuração nova:

```
"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: O RC4 como uma cifra e um MD5 como um MAC é considerado fraco, legado e para evitar para o uso com SSL/TLS, especialmente quando se trata de um volume mais alto dos dados sem regeneração chave.

Ajustes recomendados do sslconfig para DE ENTRADA

O seguinte é opinião de prevalência e para permitir somente as cifras que são consideradas geralmente fortes e seguras

Uma configuração recomendável para DE ENTRADA que removesse o RC4 e o MD5 assim como o outros legado e opções fracas, a saber a exportação (EXP), baixo (BAIXO), o IDEA (IDEA), a SEMENTE (SEMENTE), (3DES) as cifras 3DES, os Certificados DSS (DSS) e trocas de chave anônimas (aNULL) e chaves pré-compartilhada (PSK) e protocolo SRP (SRP) e desabilitasse ECDH e ECDSA seria por exemplo:

```
"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
```

O acima da corda inscrito no **sslconfig** conduz a esta lista de cifras apoiadas para DE ENTRADA:

```
"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: O ESA que atua como o server TLS (tráfego de entrada) atualmente não apoia o Diffie Hellman elíptico da curva para as trocas de chave (*ECDHE*) e Certificados elípticos do

Digital Signature Algorithm da curva (*ECDSA*).

DE PARTIDA - ESA que atua como o cliente TLS

Para o tráfego de partida S TP o ESA **além do que** trocas de chave efêmeras do Diffie Hellman elíptico **DE ENTRADA da** curva dos apoios (*ECDHE*) e Certificados elípticos do Digital Signature Algorithm da curva (*ECDSA*).

> Nota: Os Certificados elípticos da criptografia da curva (ECC) com o algoritmo elíptico da assinatura de Digitial da curva, (ECDSA) não são adotados extensamente.

Ao entregar o email (de partida), o ESA é o cliente TLS. Um certificado do TLS-cliente é opcional. Se o TLS-server não força (para exigir) o ESA (como um TLS-cliente) para fornecer um certificado de cliente ECDSA, o ESA pode continuar com uma sessão fixada ECDSA. Quando o ESA como o TLS-cliente é pedido seu certificado, fornece o certificado configurado ***RSA*** para a direção externa.

> Cuidado: *A loja confiada* instalada do *certificado de CA* (*lista do sistema*) no ESA não inclui certificados de raiz ECC (ECDSA)! Pode-se exigir adicionar manualmente os certificados de raiz ECC (que você confiança) à *lista feita sob encomenda* para fazer a corrente ECC da confiança passível de verificação.

Para preferir as cifras DHE/ECDHE que oferecem o secretismo dianteiro, você pode alterar a seleção da cifra do **sslconfig** como segue.

Adicionar o abaixo a sua seleção existente da 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
```

Ajustes recomendados do sslconfig para DE PARTIDA

O seguinte é opinião de prevalência e para permitir somente as cifras que são consideradas geralmente fortes e 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
```

O acima da corda inscrito no **sslconfig** conduz a esta lista de cifras apoiadas para DE PARTIDA:

```
"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
```

Informações Relacionadas

- Abra cifras SSL
- Criptografia da próxima geração de Cisco