Configurar o ESA para preferir PFS

Índice

[Introdução](#)
[Pré-requisitos](#)
[Requisitos](#)
[Componentes Utilizados](#)
[Informações de fundo](#)
[Configurar](#)
[DE ENTRADA - O ESA atua como o server TLS](#)
[Ajustes recomendados do sslconfig para DE ENTRADA](#)
[DE PARTIDA - O ESA atua como o cliente TLS](#)
[Ajustes recomendados do sslconfig para DE PARTIDA](#)
[Verificar](#)
[Troubleshooting](#)
[Informações Relacionadas](#)

Introdução

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

Pré-requisitos

Requisitos

Cisco recomenda que você tem o conhecimento do secure sockets layer (SSL) /TLS.

Componentes Utilizados

A informação neste documento é baseada em 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 usados neste original começaram com uma configuração cancelada (do padrão). Se sua rede está viva, certifique-se de que você compreende o impacto potencial do comando any.

Informações de fundo

O ESA oferece o secretismo dianteiro (PFS). O secretismo dianteiro significa que os dados estão transferidos através de um canal que use 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 com um problema matemático (problema do Diffie Hellman (DH)). O segredo não é armazenado em qualquer outro lugar do que a memória de acesso aleatório dos anfitriões (RAM) durante o intervalo da regeneração da sessão estabelecida ou da chave.

O ESA apoia o DH para trocas de chave.

Configurar

DE ENTRADA - O ESA atua como o server TLS

Estas séries da cifra estão disponíveis no ESA para o tráfego DE ENTRADA do Simple Mail Transfer Protocol (SMTP) que fornecem o secretismo dianteiro. Neste exemplo, a seleção da cifra permite somente séries da cifra considerou a ELEVAÇÃO ou o MEDIA e o uso o Diffie Hellman efêmero (EDH) 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 DH está usado a fim 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 PFS, você precisa de mudar seu **sslconfig** e de adicionar 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
```

> **Note**: O RC4 como uma cifra e um MD5 como um MAC é considerado fraco, legado e a fim evitar 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

Esta é uma opinião de prevalência e para permitir somente as cifras que são consideradas geralmente fortes e seguras.

Uma configuração recomendável para que remova o RC4 DE ENTRADA e o MD5 assim como o outros legado e opções fracas, a saber a exportação (EXP), baixo (BAIXO), a IDEIA (IDEIA), a SEMENTE (SEMENTE), (3DES) as cifras 3DES, os Certificados DSS (DSS), trocas de chave anônimas (aNULL), chaves pré-compartilhada (PSK), protocolo SRP (SRP), o Diffie Hellman elíptico da curva das inutilizações (ECDH) para trocas de chave e o Digital Signature Algorithm elíptico da curva (ECDSA) é os exemplos:

```
"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 corda inscrita 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
```

> **Note**: O ESA que atua como um server TLS (tráfego de entrada) atualmente não apoia o Diffie Hellman elíptico da curva para as trocas de chave (ECDHE) e os Certificados ECDSA.

DE PARTIDA - O ESA atua como o cliente TLS

Para o tráfego DE PARTIDA S TP, o ESA além do que os apoios DE ENTRADA ECDHE e Certificados ECDSA.

> **Note**: Os Certificados elípticos da criptografia da curva (ECC) com o ECDSA não são adotados extensamente.

Quando um email DE PARTIDA é entregado, 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) a fim fornecer um certificado de cliente ECDSA, o ESA pode continuar com uma sessão fixada ECDSA. Quando o ESA como o TLS-cliente é pedido ele é certificado, fornece o certificado configurado RSA para a direção externa.

> **Caution**: A loja confiada instalada do certificado de CA (lista do sistema) no ESA não inclui certificados de raiz ECC (ECDSA)! Você pôde precisar de adicionar manualmente os certificados de raiz ECC (que você confiança) à lista feita sob encomenda no orderto faz a corrente ECC da confiança passível de verificação.

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

Adicionar isto a sua seleção atual 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

Esta é uma 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
```

A corda inscrita 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
```

Verificar

Não há atualmente nenhum procedimento de verificação disponível para esta configuração.

Troubleshooting

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.

Informações Relacionadas

- Abra cifras SSL
- Criptografia da próxima geração de Cisco
- Suporte técnico & documentação - Cisco Systems