Altere os métodos e as cifras usados com o SSL/TLS no ESA

Índice

Introdução

Este documento descreve como alterar os métodos e as cifras que são usadas com configurações do Secure Socket Layer (SSL) ou do Transport Layer Security (TLS) em Cisco enviam por correio eletrónico a ferramenta de segurança (ESA).

Altere os métodos e as cifras usados com SSL/TLS

> Nota: Os métodos e as cifras SSL/TLS devem ser ajustados baseadas nas políticas de segurança e nas preferências específicas de sua empresa. Para a informação da terceira com respeito às cifras, refira o documento da Segurança/lado de servidor TLS Mozilla para configurações do servidor e a informação detalhada recomendadas.

Com Cisco AsyncOS para a Segurança do email, um administrador pode usar o comando do **sslconfig** a fim configurar o SSL ou os protocolos TLS para os métodos e as cifras que são usados para uma comunicação GUI, anunciados para conexões de entrada, e pedidos para conexões externas:

```
esa.local> sslconfig

sslconfig settings:
GUI HTTPS method: tlsv1/tlsv1.2
GUI HTTPS ciphers:
MEDIUM
HIGH
-SSLv2
-aNULL
!RC4
@STRENGTH
-EXPORT
Inbound SMTP method: tlsv1/tlsv1.2
Inbound SMTP ciphers:
MEDIUM
```

```
HIGH
-SSLv2
-aNULL
!RC4
@STRENGTH
-EXPORT
Outbound SMTP method: tlsv1/tlsv1.2
Outbound SMTP ciphers:
MEDIUM
HIGH
-SSLv2
-aNULL
!RC4
@STRENGTH
-EXPORT

Choose the operation you want to perform:
- GUI - Edit GUI HTTPS ssl settings.
- INBOUND - Edit Inbound SMTP ssl settings.
- OUTBOUND - Edit Outbound SMTP ssl settings.
- VERIFY - Verify and show ssl cipher list.
[]> inbound

Enter the inbound SMTP ssl method you want to use.
1. SSL v2
2. SSL v3
3. TLS v1/TLS v1.2
4. SSL v2 and v3
5. SSL v3 and TLS v1/TLS v1.2
6. SSL v2, v3 and TLS v1/TLS v1.2
[3]>

Enter the inbound SMTP ssl cipher you want to use.
[MEDIUM:HIGH:-SSLv2:-aNULL:!RC4:@STRENGTH:-EXPORT]>

sslconfig settings:
GUI HTTPS method: tlsv1/tlsv1.2
GUI HTTPS ciphers:
MEDIUM
HIGH
-SSLv2
-aNULL
!RC4
@STRENGTH
-EXPORT
Inbound SMTP method: tlsv1/tlsv1.2
Inbound SMTP ciphers:
MEDIUM
HIGH
-SSLv2
-aNULL
!RC4
@STRENGTH
-EXPORT
Outbound SMTP method: tlsv1/tlsv1.2
Outbound SMTP ciphers:
MEDIUM
HIGH
-SSLv2
-aNULL
!RC4
@STRENGTH
-EXPORT
```

```
Choose the operation you want to perform:
- GUI - Edit GUI HTTPS ssl settings.
- INBOUND - Edit Inbound SMTP ssl settings.
- OUTBOUND - Edit Outbound SMTP ssl settings.
- VERIFY - Verify and show ssl cipher list.
[]>
```

Se as mudanças são feitas à configuração de SSL, assegure-se de que você **comprometa** alguns e tudo mude.

Métodos SSL

Em AsyncOS para versões 9.6 e mais recente da Segurança do email, o ESA é ajustado para usar à revelia o método do *v1.2 TLS v1/TLS*. Neste caso, TLSv1.2 toma o precedente para uma comunicação, se no uso pela emissão e por partes de recebimento. A fim estabelecer uma conexão TLS, os ambos os lados devem ter pelo menos um método permitido que combina, e pelo menos um permitiu a cifra que combina.

> Nota: Em AsyncOS para versões da Segurança do email antes da versão 9.6, o padrão tem dois métodos: *SSL v3* e *TLS v1*. Alguns administradores puderam querer desabilitar SSL v3 devido às vulnerabilidades recentes (se o SSL v3 é permitido).

Cifras SSL

Quando você vê a cifra do padrão que está alistada no exemplo anterior, é importante compreender a razão que mostra duas cifras seguidas *TODA pela* palavra. Embora *TUDO* inclua as duas cifras que o precedem, a ordem das cifras na lista da cifra determina a preferência. Assim, quando uma conexão TLS é feita, o cliente escolhe a primeira cifra que o apoio dos ambos os lados baseou na ordem da aparência na lista.

> Nota: As cifras RC4 são permitidas à revelia no ESA. No exemplo anterior, o **MEDIA: A ELEVAÇÃO** é baseada nas negociações do impedimento para cifras nulas ou anônimas no documento Cisco ESA e S A. Para mais informações com respeito ao RC4 especificamente, refira o documento da Segurança/lado de servidor TLS Mozilla, e igualmente sobre a Segurança do RC4 no documento TLS e WPA que é apresentado do *simpósio 2013 da Segurança USENIX*. A fim remover as cifras RC4 do uso, refira os exemplos que seguem.

Com a manipulação da lista da cifra, você pode influenciar a cifra que é escolhida. Você pode alistar cifras ou escalas específicas da cifra, e igualmente requisita-os novamente pela força com a inclusão da opção **@STRENGTH na** corda da cifra, como mostrado aqui:

```
Enter the inbound SMTP ssl cipher you want to use.
[RC4-SHA:RC4-MD5:ALL]> MEDIUM:HIGH:-SSLv2:-aNULL:@STRENGTH
```

Assegure-se de que você rever todas as cifras e escalas que estão disponíveis no ESA. A fim ver estes, incorpore o comando do **sslconfig**, seguido pelo secundário-comando da **verificação**. As opções para as categorias da cifra SSL são **BAIXAS**, **MÉDIAS**, **ALTAS**, e **TODAS**:

```
[]> verify

Enter the ssl cipher you want to verify.
[]> MEDIUM

ADH-RC4-MD5 SSLv3 Kx=DH Au=None Enc=RC4(128) Mac=MD5
IDEA-CBC-SHA SSLv3 Kx=RSA Au=RSA Enc=IDEA(128) Mac=SHA1
RC4-SHA SSLv3 Kx=RSA Au=RSA Enc=RC4(128) Mac=SHA1
RC4-MD5 SSLv3 Kx=RSA Au=RSA Enc=RC4(128) Mac=MD5
IDEA-CBC-MD5 SSLv2 Kx=RSA Au=RSA Enc=IDEA(128) Mac=MD5
RC2-CBC-MD5 SSLv2 Kx=RSA Au=RSA Enc=RC2(128) Mac=MD5
RC4-MD5 SSLv2 Kx=RSA Au=RSA Enc=RC4(128) Mac=MD5
```

Você pode igualmente combinar estes a fim incluir escalas:

```
[]> verify

Enter the ssl cipher you want to verify.
[]> MEDIUM:HIGH

ADH-RC4-MD5 SSLv3 Kx=DH Au=None Enc=RC4(128) Mac=MD5
IDEA-CBC-SHA SSLv3 Kx=RSA Au=RSA Enc=IDEA(128) Mac=SHA1
RC4-SHA SSLv3 Kx=RSA Au=RSA Enc=RC4(128) Mac=SHA1
RC4-MD5 SSLv3 Kx=RSA Au=RSA Enc=RC4(128) Mac=MD5
IDEA-CBC-MD5 SSLv2 Kx=RSA Au=RSA Enc=IDEA(128) Mac=MD5
RC2-CBC-MD5 SSLv2 Kx=RSA Au=RSA Enc=RC2(128) Mac=MD5
RC4-MD5 SSLv2 Kx=RSA Au=RSA Enc=RC4(128) Mac=MD5
ADH-CAMELLIA256-SHA SSLv3 Kx=DH Au=None Enc=Camellia(256) Mac=SHA1
DHE-RSA-CAMELLIA256-SHA SSLv3 Kx=DH Au=RSA Enc=Camellia(256) Mac=SHA1
DHE-DSS-CAMELLIA256-SHA SSLv3 Kx=DH Au=DSS Enc=Camellia(256) Mac=SHA1
CAMELLIA256-SHA SSLv3 Kx=RSA Au=RSA Enc=Camellia(256) Mac=SHA1
ADH-CAMELLIA128-SHA SSLv3 Kx=DH Au=None Enc=Camellia(128) Mac=SHA1
DHE-RSA-CAMELLIA128-SHA SSLv3 Kx=DH Au=RSA Enc=Camellia(128) Mac=SHA1
DHE-DSS-CAMELLIA128-SHA SSLv3 Kx=DH Au=DSS Enc=Camellia(128) Mac=SHA1
CAMELLIA128-SHA SSLv3 Kx=RSA Au=RSA Enc=Camellia(128) Mac=SHA1
ADH-AES256-SHA SSLv3 Kx=DH Au=None Enc=AES(256) Mac=SHA1
DHE-RSA-AES256-SHA SSLv3 Kx=DH Au=RSA Enc=AES(256) Mac=SHA1
DHE-DSS-AES256-SHA SSLv3 Kx=DH Au=DSS Enc=AES(256) Mac=SHA1
AES256-SHA SSLv3 Kx=RSA Au=RSA Enc=AES(256) Mac=SHA1
ADH-AES128-SHA SSLv3 Kx=DH Au=None Enc=AES(128) Mac=SHA1
DHE-RSA-AES128-SHA SSLv3 Kx=DH Au=RSA Enc=AES(128) Mac=SHA1
DHE-DSS-AES128-SHA SSLv3 Kx=DH Au=DSS Enc=AES(128) Mac=SHA1
AES128-SHA SSLv3 Kx=RSA Au=RSA Enc=AES(128) Mac=SHA1
ADH-DES-CBC3-SHA SSLv3 Kx=DH Au=None Enc=3DES(168) Mac=SHA1
EDH-RSA-DES-CBC3-SHA SSLv3 Kx=DH Au=RSA Enc=3DES(168) Mac=SHA1
EDH-DSS-DES-CBC3-SHA SSLv3 Kx=DH Au=DSS Enc=3DES(168) Mac=SHA1
DES-CBC3-SHA SSLv3 Kx=RSA Au=RSA Enc=3DES(168) Mac=SHA1
DES-CBC3-MD5 SSLv2 Kx=RSA Au=RSA Enc=3DES(168) Mac=MD5
```

Algumas das cifras SSL que você não quer configurado e disponível devem ser removidas com "**-**" a opção que precede as cifras específicas. Aqui está um exemplo:

```
[]> MEDIUM:HIGH:-SSLv2:-aNULL:@STRENGTH:-EDH-RSA-DES-CBC3-SHA:
-EDH-DSS-DES-CBC3-SHA:-DES-CBC3-SHA
```

A informação neste exemplo negaria as cifras do *ZERO*, *EDH-RSA-DES-CBC3-SHA*, *EDH-DSS-DES-CBC3-SHA*, e *DES-CBC3-SHA da* propaganda e impediria seu uso na comunicação SSL.

Você pode igualmente realizar similar com a inclusão do "**!**" caráter na frente do grupo da cifra ou corda que você deseja se tornar não disponível:

```
[]> MEDIUM:HIGH:-SSLv2:-aNULL:!RC4:@STRENGTH
```

A informação neste exemplo removeria todas as cifras RC4 do uso. Assim, as cifras do *RC4-SHA* e do *RC4-MD5* seriam negadas e não anunciadas na comunicação SSL.

Se as mudanças são feitas à configuração de SSL, assegure-se de que você comprometa alguns e tudo mude.