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

Contents

Introduction

Este documento descreve como alterar os métodos e cifras usados com as configurações SSL (Secure Socket Layer) ou TLS (Transport Layer Security) no Cisco Email Security Appliance (ESA).

Altere os métodos e cifras usados com SSL/TLS

> **Note**: Os métodos e cifras SSL/TLS devem ser definidos com base nas políticas e preferências de segurança específicas da sua empresa. Para obter informações de terceiros sobre cifras, consulte o documento TLS Mozilla do lado servidor/segurança para obter as configurações recomendadas do servidor e informações detalhadas.

Com o Cisco AsyncOS for Email Security, um administrador pode usar o comando **sslconfig** para configurar os protocolos SSL ou TLS para os métodos e cifras usados para comunicação GUI, anunciados para conexões de entrada e solicitados para conexões de saída:

```
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 forem feitas alterações na configuração SSL, certifique-se de **confirmar** todas as alterações.

Métodos SSL

No AsyncOS para segurança de e-mail versões 9.6 e posteriores, o ESA está definido para usar o método *TLS v1/TLS v1.2* por padrão. Nesse caso, o TLSv1.2 tem precedência para a comunicação, se estiver em uso pelas partes de envio e de recebimento. Para estabelecer uma conexão TLS, ambos os lados devem ter pelo menos um método habilitado correspondente e pelo menos uma cifra habilitada correspondente.

> **Note**: No AsyncOS para versões de segurança de e-mail anteriores à versão 9.6, o padrão tem dois métodos: *SSL v3* e *TLS v1*. Alguns administradores podem querer desativar o SSL v3 devido a vulnerabilidades recentes (se o SSL v3 estiver ativado).

Cifras SSL

Quando você visualiza a cifra padrão listada no exemplo anterior, é importante entender o motivo pelo qual ela mostra duas cifras seguidas pela palavra *ALL*. Embora *TUDO* inclua as duas cifras que a precedem, a ordem das cifras na lista de cifras determina a preferência. Assim, quando uma conexão TLS é feita, o cliente escolhe a primeira cifra que ambos os lados suportam com base na ordem de apresentação na lista.

> **Nota**: as cifras RC4 são ativadas por padrão no ESA. No exemplo anterior, o **MÉDIO:ALTO** é baseado no documento Evitar Negociações para Ciphers Nulo ou Anônimos no ESA e no Cisco SMA. Para obter mais informações sobre RC4 especificamente, consulte o documento TLS Mozilla do lado servidor/segurança e também o documento On the Security of RC4 in TLS and WPA que é apresentado do *Simpósio de Segurança do USENIX 2013*. Para remover as cifras RC4 do uso, consulte os exemplos a seguir.

Por meio da manipulação da lista de cifras, você pode influenciar a cifra escolhida. Você pode listar cifras específicas ou intervalos de cifras e também reordená-los por força com a inclusão da opção **@STRENGTH** na string de cifra, como mostrado aqui:

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

Certifique-se de revisar todas as cifras e intervalos disponíveis no ESA. Para exibi-los, insira o comando **sslconfig**, seguido pelo subcomando **verify**. As opções para as categorias de cifras SSL são **LOW**, **MEDIUM**, **HIGH** e **ALL**:

```
[]> 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 também pode combiná-los para incluir intervalos:

```
[]> 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
```

Qualquer uma das cifras SSL que você não quer configuradas e disponíveis deve ser removida 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
```

As informações neste exemplo negariam os *NULL*, *EDH-RSA-DES-CBC3-SHA*, *EDH-DSS-DES-CBC3-SHA* e *DES-CBC3-SHA* cifras do anúncio e impediriam seu uso na comunicação SSL.

Você também pode fazer algo semelhante com a inclusão do "**!**" caractere em frente ao grupo de cifras ou string que você deseja tornar indisponível:

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

As informações neste exemplo removeriam todos os cifras RC4 do uso. Assim, os cifras *RC4-SHA* e *RC4-MD5* seriam negados e não anunciados na comunicação SSL.

Se forem feitas alterações na configuração SSL, certifique-se de **confirmar** todas as alterações.