Verander de methodes en CIFERS die met SSL/TLS op de ESA worden gebruikt

Inhoud

Inleiding

Dit document beschrijft hoe de methoden en symbolen moeten worden gewijzigd die worden gebruikt met Secure Socket Layer (SSL) of Transport Layer Security (TLS) configuraties op Cisco Email Security Appliance (ESA).

Verander de methodes en de CIFERS die met SSL/TLS worden gebruikt

> **Opmerking:** De SSL/TLS-methoden en -kaarten moeten worden ingesteld op basis van het specifieke beveiligingsbeleid en de voorkeuren van uw bedrijf. Raadpleeg voor informatie van derden over cifen het document Security/Server Side TLS Mozilla voor aanbevolen serverconfiguraties en gedetailleerde informatie.

Met Cisco AsyncOS voor e-mailbeveiliging kan een beheerder de **slineconfig** opdracht gebruiken om de SSL of TLS-protocollen te configureren voor de methoden en ciphers die voor GUI-communicatie worden gebruikt, voor inkomende verbindingen worden geadverteerd en om uitgaande verbindingen te vragen:

```
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.
[]>
```

Als de wijzigingen in de SSL-configuratie worden aangebracht, zorg er dan voor dat u alle wijzigingen **doorvoert**.

SSL-methodes

In AsyncOS voor e-mail security versies 9.6 en later, wordt de ESA ingesteld om standaard de methode *TLS v1/TLS v1.2* te gebruiken. In dit geval heeft TLSv1.2 een precedent voor communicatie, indien zij door zowel de verzendende als de ontvangende partijen wordt gebruikt. Om een TLS-verbinding op te bouwen moeten beide kanten minstens één enabled-methode hebben die aansluit, en minstens één enabled-algoritme die aansluit.

> **Opmerking:** In AsyncOS voor e-mail security versies vóór versie 9.6, heeft de standaard twee methoden: *SSL v3* en *TLS v1*. Sommige beheerders kunnen SSL v3 vanwege recente kwetsbaarheden willen uitschakelen (als SSL v3 is ingeschakeld).

SSL-cifen

Wanneer u het standaard algoritme bekijkt dat in het vorige voorbeeld is vermeld, is het belangrijk om de reden te begrijpen dat het twee ciphers toont gevolgd door het woord *ALL*. Hoewel *ALL* de twee ciphers bevat die eraan voorafgaan, bepaalt de volgorde van de ciphers in de lijst van het algoritme de voorkeur. Dus wanneer een TLS-verbinding wordt gemaakt, kiest de client het eerste algoritme dat beide kanten ondersteunen op basis van de volgorde van weergave in de lijst.

> **Opmerking**: De RC4-telefoons zijn standaard ingeschakeld op de ESA's. In het vorige voorbeeld is het **MEDIUM:HIGH** gebaseerd op de Prevent Negations for Null of Anonymous Ciphers in het ESA- en SMA-document. Raadpleeg voor meer informatie over RC4 in het bijzonder het Security/Server-document van TLS Mozilla en ook het On the Security of RC4 in TLS- en WAP-document dat wordt gepresenteerd vanaf het *USENIX-beveiligingssymposium 2013*. Om de RC4-cifen niet meer te gebruiken, raadpleegt u de volgende voorbeelden.

Door manipulatie van de lijst met algoritmen kunt u het gekozen algoritme beïnvloeden. U kunt een lijst maken van specifieke ciphers of algoritme bereik en ze ook met de optie@STRENGTH in de string herschikken, zoals hier wordt getoond:

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

Zorg ervoor dat u alle ciferen en bereik die beschikbaar zijn op de ESA's bekijkt. Om deze te bekijken, voer het **sslfig** bevel in, gevolgd door de **verify** sub-opdracht. De opties voor de SSL-programmacategorieën zijn **LOW**, **MEDIUM**, **HOOG** en **ALLE**:

```
[]> 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
```

U kunt deze ook combineren om bereik in te voegen:

```
[]> 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
```

Om het even welke SSL ciphers die u niet gevormd en beschikbaar wilt zouden met de "**-**"optie moeten worden verwijderd die de specifieke ciphers voorafgaat. Hier is een voorbeeld:

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

De informatie in dit voorbeeld zou de *NULL*, *EDH-RSA-DES-CBC3-SHA*, *EDH-DSS-DES-CBC3-*

SHA en *DES-CBC3-SHA*-schrijvers van advertenties uitsluiten en het gebruik ervan in de SSL-communicatie verhinderen.

U kunt ook hetzelfde bereiken met de opname van "**!**" karakter voor de algoritme of de string die u niet beschikbaar wilt worden:

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

De informatie in dit voorbeeld zou alle RC4-cifen uit het gebruik verwijderen. De *RC4-SHA*- en *RC4-MD5*-ciphers zouden dus verwaarloosd worden en niet geadverteerd worden in de SSL-communicatie.

Als de wijzigingen in de SSL-configuratie worden aangebracht, zorg er dan voor dat u alle wijzigingen doorvoert.