Beletten dat er over de ESA en de SMA onderhandelingen worden gevoerd met betrekking tot volledige of anonieme burgers

Inhoud

Inleiding

Dit document beschrijft hoe de instellingen van het Cisco Email Security Appliance (ESA) en Cisco Security Management Appliance (SMA) worden gewijzigd om onderhandelingen voor ongeldige en anonieme tekens te voorkomen. Dit document is van toepassing op zowel op hardware gebaseerde als virtuele apparaten.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco ESA
- Cisco SMA

Gebruikte componenten

De informatie in dit document is gebaseerd op alle versies van Cisco ESA en Cisco SMA.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Beletten dat er wordt onderhandeld over volledige of anonieme

tekens

In deze sectie wordt beschreven hoe u onderhandelingen voor ongeldige of anonieme telefoons kunt voorkomen op Cisco ESA dat AsyncOS voor e-mail security versies 9.1 en later, en ook op Cisco SMA draait.

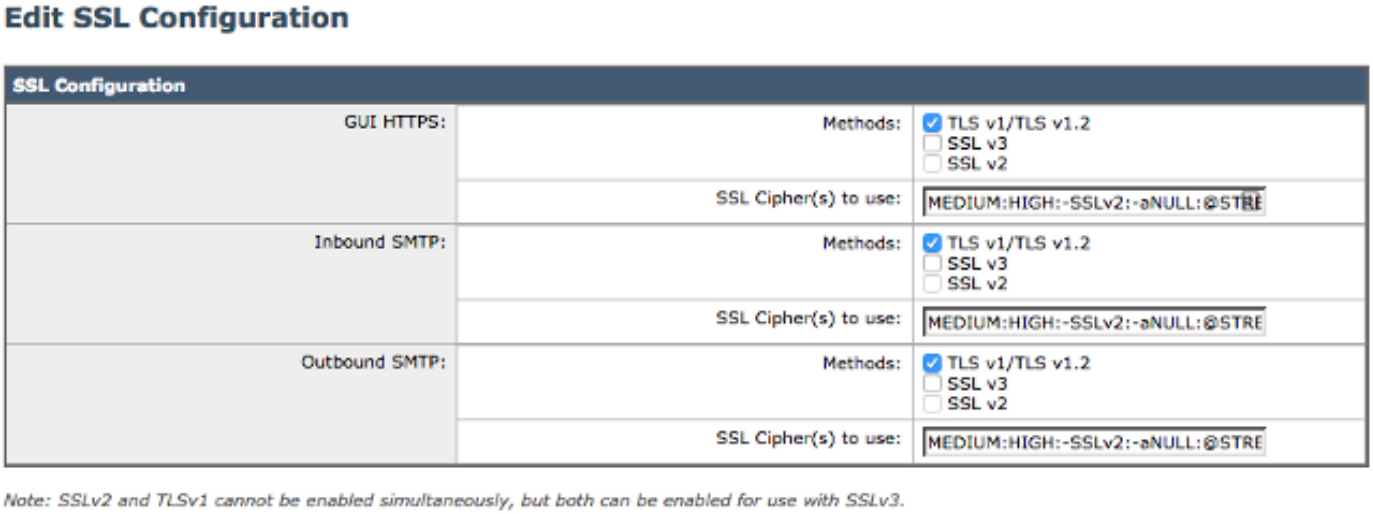
ESA's die AsyncOS uitvoeren voor e-mail security versie 9.5 of nieuwer

Dankzij de introductie van AsyncOS voor e-mail security versie 9.5 wordt TLS v1.2 nu ondersteund. De opdrachten die in de vorige sectie worden beschreven, werken nog steeds. de updates voor TLS v1.2 zijn echter opgenomen in de uitgangen.

Hier is een voorbeeldoutput van CLI:

```
> sslconfig

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

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]>
```

Als u deze instellingen vanuit de GUI wilt bereiken, navigeer dan naar **systeembeheer > SSL-configuratie > Instellingen bewerken...**:



Tip: Raadpleeg voor volledige informatie de betreffende ESA-eindgebruikershandleiding voor versie 9.5 of hoger.

ESA's die AsyncOS uitvoeren voor e-mail security versie 9.1 of hoger

U kunt de ciphers wijzigen die op ESA met het **slfig** bevel gebruikt worden. Om te voorkomen dat de ESA-onderhandelingen voor ongeldige of anonieme schrijvers verlopen, voert u het **slanken-**commando in in de ESA CLI en past u deze instellingen toe:

- Inbound Simple Mail Transfer Protocol (MTP) - methode: **sslv3tlsv1**
- Binnenkomende MTP-cifen: **MEDIUM:HOOG:-SSLv2:-ANULL:@STRENGTH**
- Uitgaande MTP-methode: **sslv3tlsv1**
- Uitgaande MTP-ciphers: **MEDIUM:HOOG:-SSLv2:-ANULL:@STRENGTH**

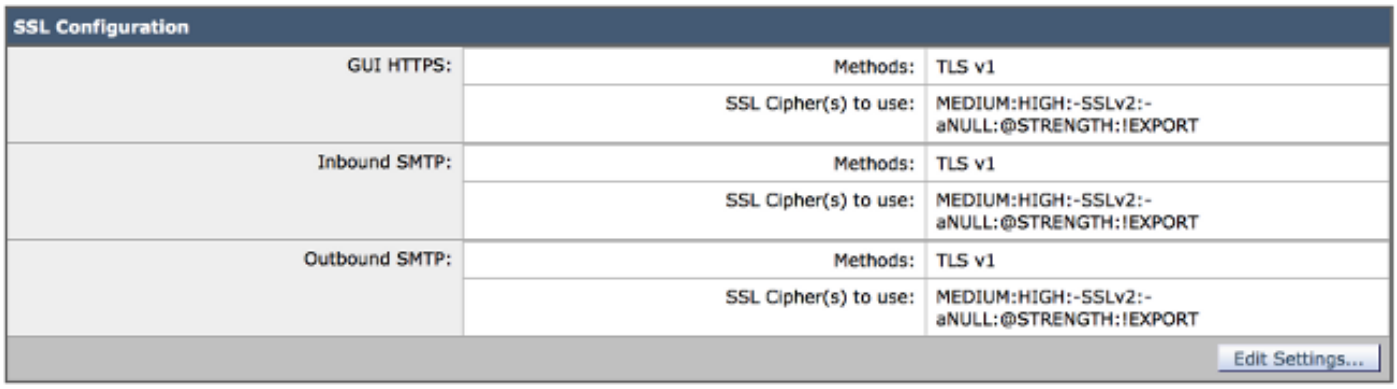
Hier is een voorbeeldconfiguratie voor inkomende ciphers:

```
CLI: > sslconfig

sslconfig settings:
  GUI HTTPS method:  sslv3tlsv1
  GUI HTTPS ciphers: RC4-SHA:RC4-MD5:ALL
  Inbound SMTP method:  sslv3tlsv1
  Inbound SMTP ciphers: RC4-SHA:RC4-MD5:ALL
  Outbound SMTP method:  sslv3tlsv1
  Outbound SMTP ciphers: RC4-SHA:RC4-MD5:ALL

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
4. SSL v2 and v3
5. SSL v3 and TLS v1
6. SSL v2, v3 and TLS v1
[5]> 3

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

Opmerking: Stel de **GUI**, **INBOUND** en **OUTBOUND** indien nodig in voor elk algoritme.

Aangezien AsyncOS voor e-mail security versie 8.5, is de **slinkende** opdracht ook beschikbaar via de GUI. Om deze instellingen vanuit de GUI te bereiken, navigeer dan naar **System Administration > SSL Configuraties > Instellingen bewerken**:



Tip: Secure Socket Laver (SSL) versie 3.0 (RFC-6101) is een verouderd en onveilig protocol. Er is een kwetsbaarheid in SSLv3 CVE-2014-3566 bekend als *Padding Oracle On Downgraded Legacy Encryption (POODLE) aanval*, die wordt gevolgd door Cisco bug ID CSCur27131. Cisco raadt u aan SSLv3 uit te schakelen terwijl u de client wijzigt phers, gebruik uitsluitend Transport Layer Security (TLS) en selecteer *optie 3* (TLS v1). Raadpleeg Cisco bug-ID CSCur27131 voor volledige informatie.

SMA's die ABBYY FineReader uitvoeren voor Content Security Management 9.6 of nieuwer

Net als het ESA, voer het **slfig** bevel op de CLI uit.

SMA's die AsyncOS uitvoeren voor Content Security Management 9.5 of hoger

Het **slfig** opdracht is niet beschikbaar voor oude versies van SMA.

Opmerking: Oudere versies van AsyncOS voor alleen SMA ondersteunde TLS v1. upgrade naar 9.6 of nieuwer op uw SMA voor up-to-date SSL-beheer.

U moet deze stappen van de SMA CLI voltooien om de SSL-tekens te wijzigen:

1. Sla het SMA-configuratiebestand op de lokale computer op.
2. Open het XML-bestand.

3. Zoeken naar de sectie *<ssl>* in XML:

```
<ssl>
   <ssl_inbound_method>sslv3tlsv1</ssl_inbound_method>
   <ssl_inbound_ciphers>RC4-SHA:RC4-MD5:ALL</ssl_inbound_ciphers>
   <ssl_outbound_method>sslv3tlsv1</ssl_outbound_method>
   <ssl_outbound_ciphers>RC4-SHA:RC4-MD5:ALL</ssl_outbound_ciphers>
   <ssl_gui_method>sslv3tlsv1</ssl_gui_method>
   <ssl_gui_ciphers>RC4-SHA:RC4-MD5:ALL</ssl_gui_ciphers>
 </ssl>
```

4. Wijzig de tekens naar wens en slaat XML op:

```
<ssl>
<ssl_inbound_method>tlsv1</ssl_inbound_method>
<ssl_inbound_ciphers>MEDIUM:HIGH:-SSLv2:-aNULL:@STRENGTH</ssl_inbound_ciphers>
<ssl_outbound_method>tlsv1</ssl_outbound_method>
<ssl_outbound_ciphers>MEDIUM:HIGH:-SSLv2:-aNULL:@STRENGTH</ssl_outbound_ciphers>
<ssl_gui_method>tlsv1</ssl_gui_method>
<ssl_gui_ciphers>MEDIUM:HIGH:-SSLv2:-aNULL:@STRENGTH</ssl_gui_ciphers>
</ssl>
```

5. Laad het nieuwe configuratiebestand op het SMA.

6. Alle wijzigingen **indienen** en **doorgeven**.

Gerelateerde informatie

- Cisco ESA - release Notes
- Cisco ESA - gebruikershandleidingen
- Cisco SMA - Releaseopmerkingen
- Cisco SMA - gebruikershandleidingen
- Technische ondersteuning en documentatie – Cisco Systems