Verhindern von Verhandlungen für Null- oder Anonyme Chiffren auf der ESA und SMA

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie Sie die Verschlüsselungseinstellungen der Cisco E-Mail Security Appliance (ESA) und Cisco Security Management Appliance (SMA) ändern, um Verhandlungen für NULL- oder anonyme Verschlüsselungen zu verhindern. Dieses Dokument gilt sowohl für hardwarebasierte als auch für virtuelle Appliances.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- Cisco ESA
- Cisco SMA

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf allen Versionen der Cisco ESA und Cisco SMA.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Verhandlung für Null- oder anonyme Chiffren verhindern

In diesem Abschnitt wird beschrieben, wie Sie Verhandlungen für Null- oder anonyme Chiffren auf der Cisco ESA, auf der AsyncOS für E-Mail-Sicherheit Version 9.1 und höher ausgeführt wird, sowie auf der Cisco SMA verhindern.

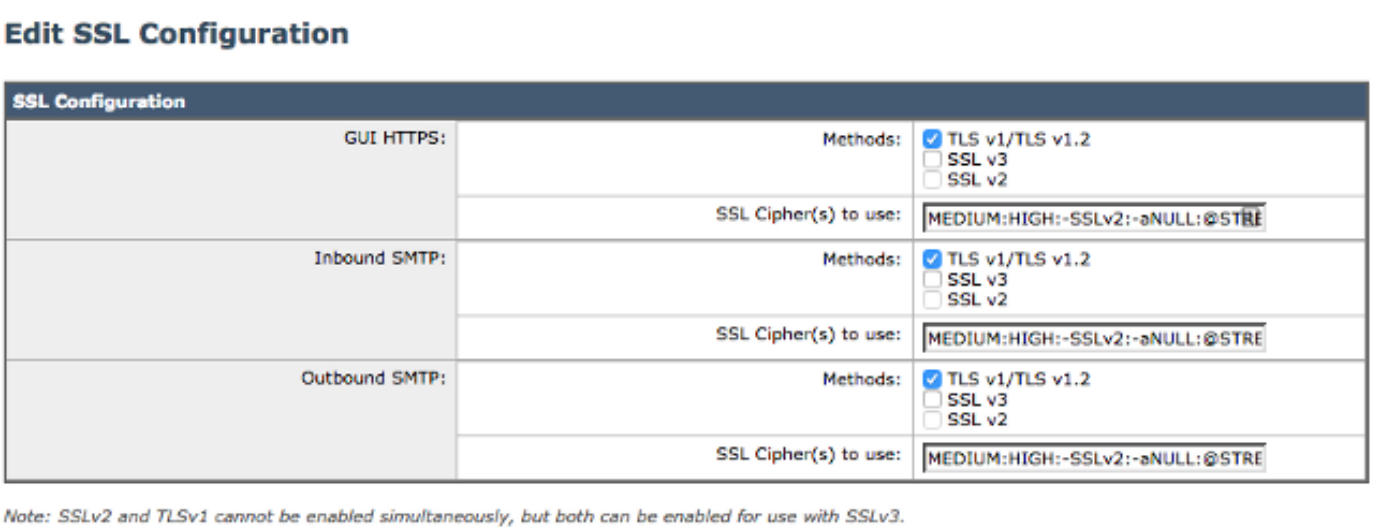
ESAs, die AsyncOS für E-Mail-Sicherheit ab Version 9.5 ausführen

Mit der Einführung von AsyncOS für Email Security Version 9.5 wird TLS v1.2 nun unterstützt. Die Befehle, die im vorherigen Abschnitt beschrieben wurden, funktionieren weiterhin. Die Aktualisierungen für TLS v1.2 werden jedoch in den Ausgaben enthalten sein.

Im Folgenden finden Sie ein Beispiel für eine Ausgabe aus der 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]>
```

Um diese Einstellungen über die Benutzeroberfläche zu erreichen, navigieren Sie zu **Systemverwaltung > SSL-Konfiguration > Einstellungen bearbeiten..**:



Tipp: Vollständige Informationen finden Sie im entsprechenden ESA-Endbenutzerhandbuch für Version 9.5 oder höher.

ESAs, die AsyncOS für E-Mail-Sicherheit Version 9.1 oder älter ausführen

Sie können die auf der ESA verwendeten Chiffren mit dem Befehl **sslconfig** ändern. Um die ESA-Verhandlungen für NULL- oder anonyme Verschlüsselungen zu verhindern, geben Sie den **Befehl sslconfig** in die ESA-CLI ein, und wenden Sie die folgenden Einstellungen an:

- SMTP-Methode (Inbound Simple Mail Transfer Protocol): **sslv3tlsv1**
- Eingehende SMTP-Chiffren: **MITTEL:HOCH:-SSLv2:-aNULL:@STRENGTH**
- SMTP-Methode für ausgehenden Datenverkehr: **sslv3tlsv1**
- Ausgehende SMTP-Chiffren: **MITTEL:HOCH:-SSLv2:-aNULL:@STRENGTH**

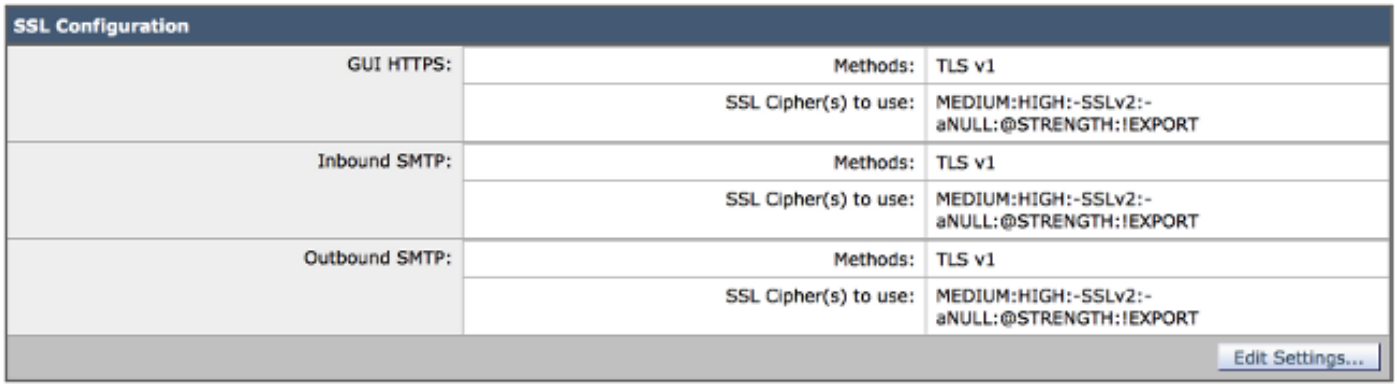
Hier eine Beispielkonfiguration für eingehende Chiffren:

```
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
```

> **Hinweis**: Legen Sie die **GUI**, **INBOUND** und **OUTBOUND** je nach Bedarf für die einzelnen Chiffren fest.

Ab AsyncOS für Email Security Version 8.5 ist der Befehl **sslconfig** auch über die GUI verfügbar. Um diese Einstellungen über die Benutzeroberfläche zu erreichen, navigieren Sie zu **Systemverwaltung > SSL-Konfigurationen > Einstellungen bearbeiten**:



> **Tipp**: Secure Sockets Laver (SSL) Version 3.0 (RFC-6101) ist ein veraltetes und unsicheres Protokoll. Eine Schwachstelle in SSLv3 CVE-2014-3566, bekannt als *Padding Oracle On Downgraded Legacy Encryption (POODLE)-Angriff*, der von der Cisco Bug-ID CSCur27131 nachverfolgt wird. Cisco empfiehlt, SSLv3 zu deaktivieren, während Sie die Chiffren ändern, nur Transport Layer Security (TLS) verwenden und *Option 3* (TLS v1) auswählen. Ausführliche Informationen finden Sie unter Cisco Bug ID CSCur27131.

SMAs, die AsycnOS für Content Security Management 9.6 oder höher ausführen

Führen Sie ähnlich wie die ESA den Befehl **sslconfig** in der CLI aus.

SMAs, die AsyncOS für Content Security Management 9.5 oder höher ausführen

Der Befehl **sslconfig** ist für ältere Versionen von SMA nicht verfügbar.

> **Hinweis**: Ältere Versionen von AsyncOS für SMA unterstützten nur TLS v1. Bitte aktualisieren Sie auf 9.6 oder neuere Version Ihres SMA, um eine aktuelle SSL-Verwaltung zu erhalten.

Führen Sie die folgenden Schritte in der SMA-CLI aus, um die SSL-Verschlüsselung zu ändern:

1. Speichern Sie die SMA-Konfigurationsdatei auf Ihrem lokalen Computer.
2. Öffnen Sie die XML-Datei.

3. Suchen Sie im XML nach dem Abschnitt *<ssl>*:

```
<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. Ändern Sie die Chiffren nach Bedarf, und speichern Sie die XML-Datei:

```
<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. Laden Sie die neue Konfigurationsdatei auf die SMA.

6. **Senden** und **bestätigen Sie** alle Änderungen.

Zugehörige Informationen

- Cisco ESA - Versionshinweise
- Cisco ESA - Benutzerhandbücher
- Cisco SMA - Versionshinweise
- Cisco SMA - Benutzerhandbücher
- Technischer Support und Dokumentation - Cisco Systems