Ändern der mit SSL/TLS auf der ESA verwendeten Methoden und Chiffren

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie Sie die Methoden und Chiffren ändern, die mit SSL- (Secure Socket Layer) oder TLS-Konfigurationen (Transport Layer Security) auf der Cisco E-Mail Security Appliance (ESA) verwendet werden.

Ändern der mit SSL/TLS verwendeten Methoden und Chiffren

> **Hinweis**: Die SSL/TLS-Methoden und -Verschlüsselungen sollten auf Basis der spezifischen Sicherheitsrichtlinien und -einstellungen Ihres Unternehmens festgelegt werden. Informationen zu Chiffren von Drittanbietern finden Sie im Dokument Security/Server Side TLS Mozilla, das empfohlene Serverkonfigurationen und detaillierte Informationen enthält.

Mit Cisco AsyncOS für Email Security kann ein Administrator mit dem Befehl **sslconfig** die SSL- oder TLS-Protokolle für die Methoden und Chiffren konfigurieren, die für die GUI-Kommunikation verwendet, für eingehende Verbindungen angekündigt und für ausgehende Verbindungen angefordert werden:

```
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.
[]>
```

Wenn Änderungen an der SSL-Konfiguration vorgenommen werden, stellen Sie sicher, dass Sie alle Änderungen **bestätigen**.

SSL-Methoden

In AsyncOS für E-Mail-Sicherheit Version 9.6 und höher ist die ESA so eingestellt, dass sie standardmäßig *die* TLS v1/TLS v1.2-Methode verwendet. In diesem Fall hat TLSv1.2 Vorrang bei der Kommunikation, wenn sowohl die sendenden als auch die empfangenden Parteien diese nutzen. Um eine TLS-Verbindung herzustellen, müssen beide Seiten über mindestens eine aktivierte Methode verfügen, die übereinstimmt, und mindestens einen aktivierten Code, der übereinstimmt.

> **Hinweis**: In AsyncOS für Email Security-Versionen vor Version 9.6 gibt der Standardwert zwei Methoden vor: *SSL v3* und *TLS v1*. Manche Administratoren möchten möglicherweise SSL v3 aufgrund aktueller Schwachstellen deaktivieren (wenn SSL v3 aktiviert ist).

SSL-Chiffren

Wenn Sie die im vorherigen Beispiel aufgeführte Standardchiffre anzeigen, ist es wichtig, den Grund zu verstehen, aus dem zwei Chiffren angezeigt werden, gefolgt vom Wort *ALL*. Obwohl *ALL* die beiden Chiffren enthält, die ihm vorangehen, bestimmt die Reihenfolge der Chiffren in der Verschlüsselungsliste die Präferenz. Wenn also eine TLS-Verbindung hergestellt wird, wählt der Client die erste Verschlüsselung aus, die von beiden Seiten je nach der Reihenfolge der Darstellung in der Liste unterstützt wird.

> **Hinweis**: Die RC4-Chiffren sind auf der ESA standardmäßig aktiviert. Im vorherigen Beispiel basiert das **MEDIUM:HIGH** auf Verhandlung gegen Null- oder Anonyme Chiffren im ESA- und SMA Cisco-Dokument. Weitere Informationen speziell zu RC4 finden Sie im Dokument Security/Server Side TLS Mozilla sowie im Dokument On the Security of RC4 in TLS and WPA im *USENIX Security Symposium 2013*. Um die RC4-Chiffren von der Verwendung zu entfernen, sehen Sie sich die folgenden Beispiele an.

Durch Manipulation der Verschlüsselungsliste können Sie die ausgewählte Chiffre beeinflussen. Sie können bestimmte Chiffren oder Verschlüsselungsbereiche auflisten und diese auch nach Stärke neu anordnen, indem Sie die **@STRENGTH-**Option in die Zeichenfolge einschließen, wie hier gezeigt:

```
Enter the inbound SMTP ssl cipher you want to use.
```

```
[RC4-SHA:RC4-MD5:ALL]> MEDIUM:HIGH:-SSLv2:-aNULL:@STRENGTH
```

Überprüfen Sie alle auf der ESA verfügbaren Chiffren und Bereiche. Um diese anzuzeigen, geben Sie den Befehl **sslconfig** gefolgt vom **Verifizieren**-Unterbefehl ein. Die Optionen für die SSL-Verschlüsselungskategorien sind **LOW**, **MEDIUM**, **HIGH** und **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
```

Sie können diese auch kombinieren, um Bereiche einzuschließen:

```
[]> 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
```

Alle SSL-Chiffren, die Sie nicht konfigurieren und verfügbar machen möchten, sollten mit der Option "**-**" entfernt werden, die den jeweiligen Chiffren vorangeht. Hier ein Beispiel:

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

Die Informationen in diesem Beispiel würden die *Chiffren NULL*, *EDH-RSA-DES-CBC3-SHA*,

EDH-DSS-DES-CBC3-SHA und *DES-CBC3-SHA* von der Werbung abhalten und ihre Verwendung in der SSL-Kommunikation verhindern.

Ähnlich kann man auch mit der Aufnahme des "**!**" Zeichen vor der Verschlüsselungsgruppe oder Zeichenfolge, die nicht verfügbar sein soll:

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

Die Informationen in diesem Beispiel würden alle RC4-Chiffren aus der Verwendung entfernen. So würden die *RC4-SHA*- und *RC4-MD5*-Chiffren verworfen und nicht in der SSL-Kommunikation angekündigt.

Wenn Änderungen an der SSL-Konfiguration vorgenommen werden, stellen Sie sicher, dass Sie alle Änderungen **bestätigen**.