Konfigurieren von Transport Layer Security Version 1.0 auf der Cisco ESA und CES

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie die Transport Layer Security Version 1.0 (TLSv1.0) für die Cisco E-Mail Security Appliance (ESA)- und Cisco Cloud E-Mail Security (CES)-Zuweisungen aktiviert wird.

Wie können Sie TLSv1.0 auf der Cisco ESA und CES aktivieren?

> **Hinweis**: Bei den bereitgestellten Cisco CES-Zuweisungen ist TLSv1.0 aufgrund von Schwachstellenauswirkungen auf das TLSv1.0-Protokoll standardmäßig gemäß den Sicherheitsanforderungen deaktiviert. Dazu gehört auch die Verschlüsselungszeichenfolge zum Entfernen der gesamten Verwendung der SSLv3-Verschlüsselungs-Suite.

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

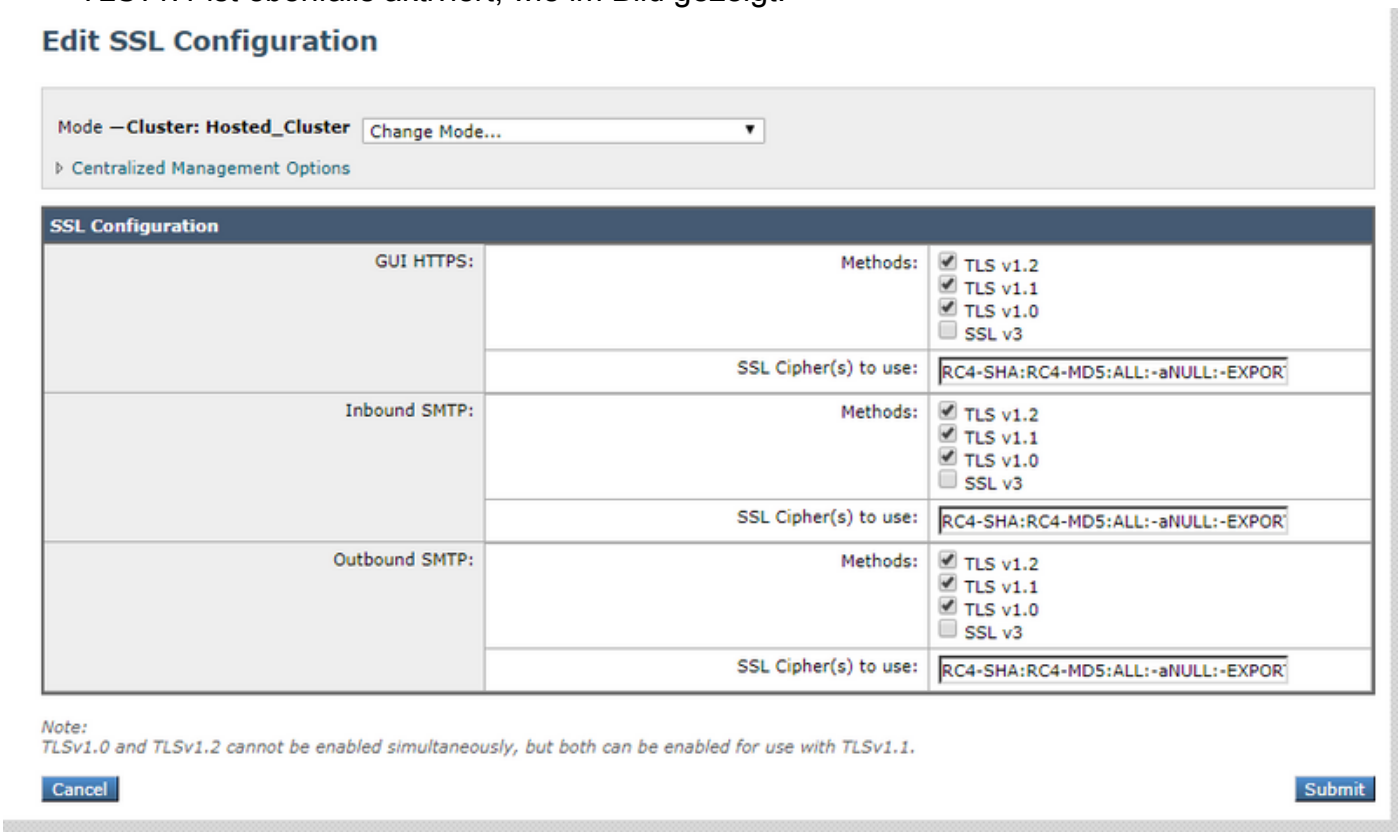
Um TLSv1.0 auf Ihrer Cisco ESA oder CES zu aktivieren, können Sie dies über die grafische Benutzeroberfläche (GUI) oder die Befehlszeilenschnittstelle (CLI) tun.

> **Hinweis**: Um auf Ihre CES über die CLI zugreifen zu können, lesen Sie bitte: **Zugriff auf die Kommandozeile (CLI) Ihrer Cloud Email Security (CES)-Lösung**

Grafische Benutzeroberfläche

1. Melden Sie sich bei der GUI an.
2. Navigieren Sie zu **Systemverwaltung > SSL-Konfiguration**.
3. Wählen Sie **Einstellungen bearbeiten aus**.
4. Aktivieren Sie das Kontrollkästchen **TLSv1.0**. Beachten Sie, dass TLSv1.2 und nicht in

Verbindung mit TLSv1.0 aktiviert werden können, es sei denn, das Bridging-Protokoll TLSv1.1 ist ebenfalls aktiviert, wie im Bild gezeigt:



Befehlszeilenschnittstelle

1. Führen Sie den Befehl **sslconfig aus**.
2. Führen Sie den Befehl **GUI** oder **INBOUND** oder **OUTBOUND aus**, je nachdem, für welches Element Sie TLSv1.0 aktivieren möchten:

```
(Cluster Hosted_Cluster)> sslconfig

sslconfig settings:
GUI HTTPS method: tlsv1_2
GUI HTTPS ciphers:
RC4-SHA
RC4-MD5
ALL
-aNULL
-EXPORT
Inbound SMTP method: tlsv1_2
Inbound SMTP ciphers:
RC4-SHA
RC4-MD5
ALL
-aNULL
-EXPORT
Outbound SMTP method: tlsv1_2
Outbound SMTP ciphers:
RC4-SHA
RC4-MD5
ALL
-aNULL
-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.
- CLUSTERSET - Set how ssl settings are configured in a cluster.
- CLUSTERSHOW - Display how ssl settings are configured in a cluster.
[]> INBOUND

Enter the inbound SMTP ssl method you want to use.
1. TLS v1.0
2. TLS v1.1
3. TLS v1.2
4. SSL v2
5. SSL v3
[3]> 1-3

Enter the inbound SMTP ssl cipher you want to use.
[RC4-SHA:RC4-MD5:ALL:-aNULL:-EXPORT]>
```

Chiffren

ESAs und CES-Zuweisungen können mit strikten Verschlüsselungssuiten konfiguriert werden. Es ist wichtig, sicherzustellen, dass SSLv3-Verschlüsselungen nicht blockiert werden, wenn Sie das TLSv1.0-Protokoll aktivieren. Wenn die SSLv3-Verschlüsselungssuiten nicht zugelassen werden, werden Fehler bei der TLS-Aushandlung oder abrupte TLS-Verbindungsschließungen verursacht.

Beispiel für eine Chiffrierzeichenfolge:

```
HIGH:MEDIUM:@STRENGTH:!aNULL:!eNULL:!LOW:!DES:!MD5:!EXP:!PSK:!DSS:!RC2:!RC4:!SEED:!ECDSA:!ADH:!I
DEA:!3DES:!SSLv2:!SSLv3:!TLSv1:-aNULL:-EXPORT:-IDEA
```

Diese Verschlüsselungszeichenfolge verhindert, dass die ESA/CES die Aushandlung auf SSLv3-Verschlüsselungen wie in **!SSLv3:** angegeben zulassen**.** Das bedeutet, wenn das Protokoll im Handshake angefordert wird, schlägt der SSL-Handshake fehl, da keine freigegebenen Verschlüsselungen für die Aushandlung verfügbar sind.

Um sicherzustellen, dass die Beispielzeichenfolge mit TLSv1.0 funktioniert, muss sie geändert werden, um **!SSLv3:!TLSv1:** in der ersetzten Verschlüsselungszeichenfolge zu entfernen:

```
HIGH:MEDIUM:@STRENGTH:!aNULL:!eNULL:!LOW:!DES:!MD5:!EXP:!PSK:!DSS:!RC2:!RC4:!SEED:!ECDSA:!ADH:!I
DEA:!3DES:!SSLv2:-aNULL:-EXPORT:-IDEA
```

> **Hinweis**: Sie können die auf SSL-Handshake gemeinsam genutzten Verschlüsselungssuiten auf der ESA/CES-CLI mit dem Befehl **VERIFY** überprüfen.

Mögliche Fehler, die im mail_logs/Message Tracking protokolliert wurden, jedoch nicht beschränkt auf:

```
Sun Feb 23 10:07:07 2020 Info: DCID 1407038 TLS failed: (336032784, 'error:14077410:SSL
routines:SSL23_GET_SERVER_HELLO:sslv3 alert handshake failure')
Sun Feb 23 10:38:56 2020 Info: DCID 1407763 TLS failed: (336032002, 'error:14077102:SSL
routines:SSL23_GET_SERVER_HELLO:unsupported protocol')
```

Zugehörige Informationen

- Ändern der mit SSL/TLS auf der ESA verwendeten Methoden und Chiffren
- Strength-Details für SSL-Chips
- Umfassender Einrichtungsleitfaden für TLS auf ESA
- Technischer Support und Dokumentation - Cisco Systems