تكوين الإصدار 1.0 من أمان طبقة النقل على Cisco ESA و CES

المحتويات

المقدمة

يصف هذا المستند كيفية تمكين الإصدار 1.0 (TLSv1.0) من أمان طبقة النقل في أجهزة أمان البريد الإلكتروني (ESA) من Cisco ومخصصات أمان البريد الإلكتروني للسحابة (CES) من Cisco.

كيف يمكنك تمكين TLSv1.0 على Cisco ESA و CES؟

ملاحظة: تم تعطيل TLSv1.0 لتخصيصات Cisco CES المقدمة بشكل افتراضي وفقا لمتطلبات الأمان بسبب تأثير الثغرات على بروتوكول TLSv1.0. ويتضمن ذلك سلسلة التشفير لإزالة جميع إستخدام مجموعة شفرة SSLv3 المشتركة.

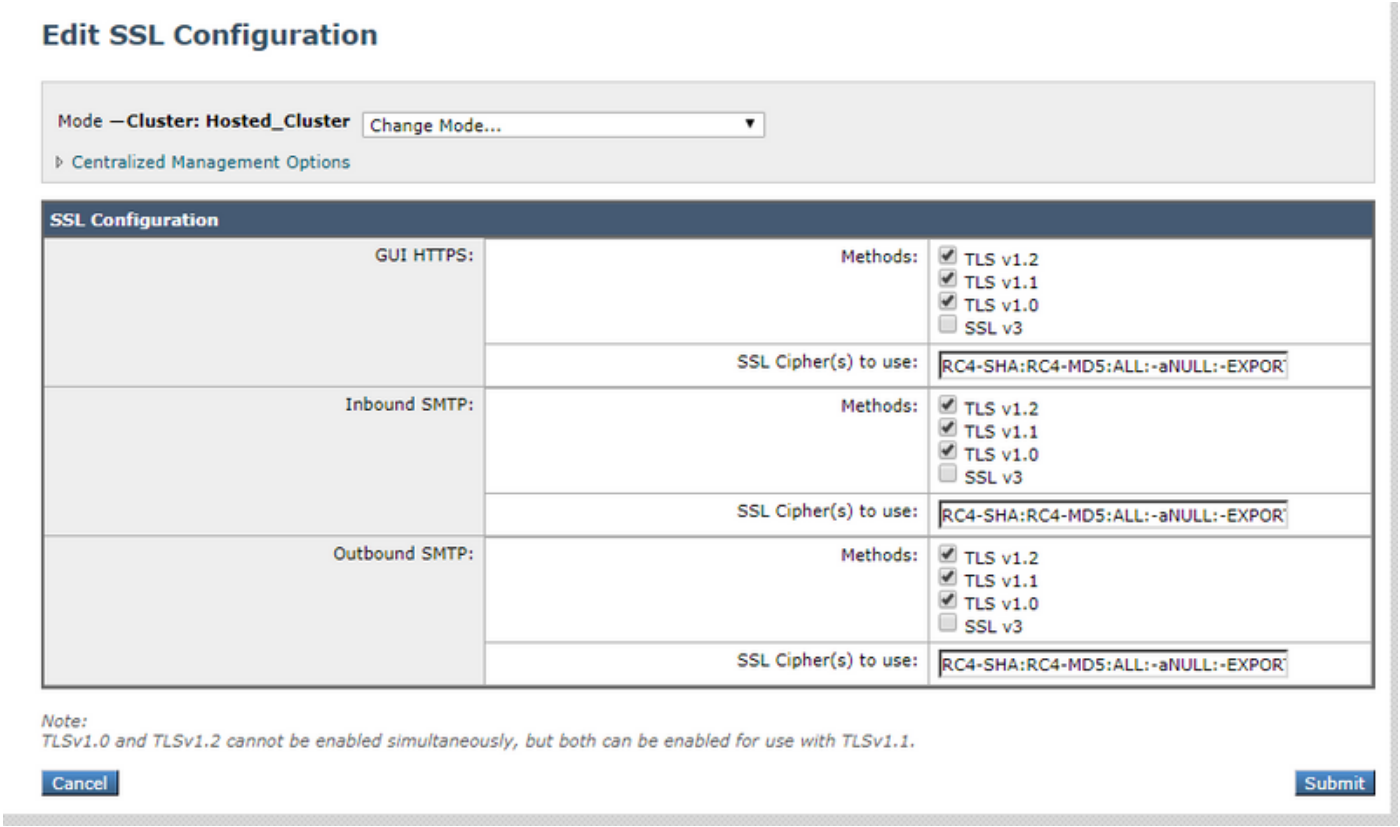
تحذير: يتم تعيين طرق وشفرات SSL/TLS بناء على سياسات الأمان وتفضيلات شركتك المحددة. للحصول على معلومات من طرف ثالث فيما يتعلق بالشفرات، ارجع إلى مستند Mozilla Security/Server Side TLS للحصول على تكوينات الخادم الموصى بها والمعلومات التفصيلية.

in order to مكنت TLSv1.0 على ك cisco ESA أو CES، أنت يستطيع فعلت ذلك من الرسوم مستعمل قارن (gui) أو أمر خط قارن (CLI).

ملاحظة: للحصول على وصول إلى CES الخاصة بك على واجهة سطر الأوامر، يرجى المراجعة: **الوصول إلى واجهة سطر الأوامر (CLI) الخاصة بحل أمان البريد الإلكتروني للسحابة (CES) الخاص بك**

واجهة المستخدم الرسومية

1. سجل الدخول إلى واجهة المستخدم الرسومية.
2. انتقل إلى **إدارة النظام > تكوين SSL**.
3. حدد **تحرير الإعدادات**.
4. حدد مربع **TLSv1.0**. من المهم ملاحظة أن TLSv1.2 ولا يمكن تمكينه بالاقتران مع TLSv1.0 ما لم يتم تمكين بروتوكول الجسر TLSv1.1 أيضا كما هو موضح في الصورة:



واجهة سطر الأوامر

1. قم بتشغيل الأمر **sslconfig**.
2. قم بتشغيل الأمر **gui** أو **inbound** أو **الصادر** حسب العنصر الذي تريد تمكين TLSv1.0 له:

```
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
TLS v1.0 .1
TLS v1.1 .2
TLS v1.2 .3
  SSL v2 .4
  SSL v3 .5
   1-3 <[3]

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

عمليات التشفير

يمكن تكوين عمليات تخصيص ESA و CES باستخدام مجموعات تشفير دقيقة، ومن المهم التأكد من عدم حظر شفرات SSLv3 عند تمكين بروتوكول TLSv1.0. يؤدي الفشل في السماح لمجموعات تشفير SSLv3 إلى فشل تفاوض TLS أو إغلاق اتصال TLS بشكل مفاجئ.

نموذج سلسلة تشفير:

```
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
```

تمنع سلسلة التشفير هذه ESA/CES من السماح بالتفاوض على شفرات SSLv3 كما هو موضح على **!SSLv3**، وهذا يعني أنه عند طلب البروتوكول في المصافحة، يفشل مصافحة SSL حيث لا توجد شفرات مشتركة متاحة للتفاوض.

لضمان عمل سلسلة التشفير العينة مع TLSv1.0، يلزم تعديلها لإزالة **!SSLv3:!TLSv1**يرى في سلسلة التشفير المستبدلة:

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

ملاحظة: يمكنك التحقق من مجموعات التشفير المشتركة على مصافحة SSL على واجهة سطر الأوامر (CLI) ل ESA/CES باستخدام الأمر **verify**.

الأخطاء المحتملة التي تم تسجيلها في MAIL_LOGS/Message Tracking ولكن لا تقتصر على:

```
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')
```

معلومات ذات صلة

- تبديل الطرق والشفرات المستخدمة مع SSL/TLS على ESA
- تفاصيل قوة تشفير SSL
- دليل الإعداد الشامل لقوائم التحكم في الوصول إلى النقل (TLS) على ESA
- الدعم التقني والمستندات - Cisco Systems

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).