منع التفاوض على التشفير الفارغ أو المجهول على ESA و SMA

المحتويات

المقدمة

يصف هذا المستند كيفية تغيير إعدادات تشفير جهاز أمان البريد الإلكتروني (ESA) من Cisco وأجهزة إدارة الأمان (SMA) لمنع المفاوضات حول التشفير الفارغ أو المجهول. ينطبق هذا المستند على كل من الأجهزة المستندة إلى الأجهزة والأجهزة الافتراضية.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- Cisco ESA
- Cisco SMA

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى جميع إصدارات Cisco ESA و Cisco SMA.

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

منع المفاوضات للشفرات الفارغة أو المجهولة

يوضح هذا القسم كيفية منع المفاوضات حول التشفير الفارغ أو المجهول على Cisco ESA الذي يشغل AsyncOS لإصدارات أمان البريد الإلكتروني 9.1 والإصدارات الأحدث، وعلى Cisco SMA أيضا.

ESAs التي تعمل بنظام التشغيل AsyncOS للإصدار 9.5 من أمان البريد الإلكتروني أو إصدار أحدث

مع إدخال AsyncOS للإصدار 9.5 من أمان البريد الإلكتروني، يتم الآن دعم TLS v1.2. لا تزال الأوامر الموضحة في القسم السابق تعمل، ومع ذلك، سترى تحديثات TLS v1.2 المضمنة في المخرجات.

هنا مثال إنتاج من ال CLI:

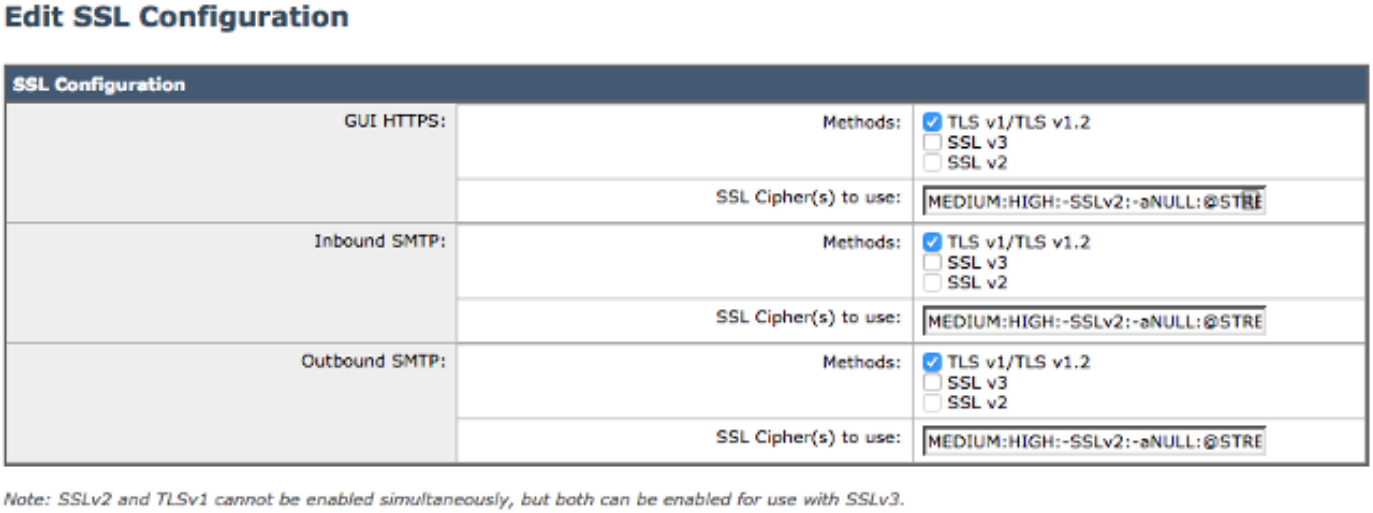
```
> sslconfig

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]>
```

للوصول إلى هذه الإعدادات من واجهة المستخدم الرسومية، انتقل إلى **إدارة النظام > تكوين SSL > تحرير الإعدادات...**:



تلميح: للحصول على معلومات كاملة، ارجع إلى دليل المستخدم النهائي ESA المناسب للإصدار 9.5 أو إصدار أحدث.

ESAs التي تعمل بنظام التشغيل AsyncOS للإصدار 9.1 لأمان البريد الإلكتروني أو الأقدم

أنت يستطيع عدلت الشفرة أن يكون استعملت على ال ESA مع ال **sslconfig** أمر. لمنع مفاوضات ESA الخاصة بالشفرات الفارغة أو المجهولة، أدخل الأمر **sslconfig** في واجهة سطر الأوامر (CLI) الخاصة ب ESA وقم بتطبيق الإعدادات التالية:

- أسلوب بروتوكول نقل البريد البسيط الوارد (SMTP): **sslv3tlsv1**
- شفرات SMTP الواردة: **متوسطة:عالية:-SSLv2:-aNULL:@Strength**
- أسلوب SMTP الصادر: **sslv3tlsv1**
- شفرات SMTP الصادرة: **متوسطة:عالية:-SSLv2:-aNULL:@Strength**

هنا مثال تشكيل للشفرات الواردة:

```
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
```

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

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

ملاحظة: قم بتعيين **واجهة المستخدم الرسومية (GUI)** و**الوارد** و**الصادر** حسب الحاجة لكل تشفير.

اعتبارا من AsyncOS لأمان البريد الإلكتروني الإصدار 8.5، يتوفر أمر **sslconfig** أيضا عبر واجهة المستخدم الرسومية (GUI). للوصول إلى هذه الإعدادات من واجهة المستخدم الرسومية، انتقل إلى **إدارة النظام > تكوينات SSL > إعدادات التحرير**:

SSL Configuration		
GUI HTTPS:	Methods:	TLS v1
	SSL Cipher(s) to use:	MEDIUM:HIGH:-SSLv2:-aNULL:@STRENGTH:!EXPORT
Inbound SMTP:	Methods:	TLS v1
	SSL Cipher(s) to use:	MEDIUM:HIGH:-SSLv2:-aNULL:@STRENGTH:!EXPORT
Outbound SMTP:	Methods:	TLS v1
	SSL Cipher(s) to use:	MEDIUM:HIGH:-SSLv2:-aNULL:@STRENGTH:!EXPORT
		Edit Settings...

تلميح: الإصدار 3.0 من مزود مآخذ التوصيل الآمنة (SSL) (RFC-6101) هو بروتوكول قديم وغير آمن. هناك ضعف في CVE-2014-3566 SSLv3 المعروف باسم *إضافة Oracle على هجوم التشفير القديم (PODLE) المخفض*، والذي يتم تتبعه بواسطة معرف تصحيح الأخطاء من cisco. CSCur27131 Cisco يوصي أن يعجز أنت SSLv3 بينما أنت تغير الشفرة، إستعمال طبقة النقل أمن (TLS) فقط، وحدد *خيار 3* (TLS v1). راجع معرف تصحيح الأخطاء من CSCur27131 Cisco للحصول على التفاصيل الكاملة.

SMAs التي تعمل بنظام التشغيل AsycnOS لإدارة أمان المحتوى 9.6 أو إصدار أحدث

وكما هو الحال مع ESA، قم بتشغيل الأمر **sslconfig** على واجهة سطر الأوامر.

SMAs التي تعمل بنظام التشغيل AsyncOS لإدارة أمان المحتوى 9.5 أو إصدار أحدث

لا يتوفر الأمر **sslconfig** للإصدارات القديمة من SMA.

ملاحظة: الإصدارات الأقدم من AsyncOS ل SMA تدعم TLS v1 فقط. يرجى الترقية إلى 9.6 أو إصدار أحدث من SMA للحصول على إدارة محدثة ل SSL.

يجب عليك إكمال هذه الخطوات من واجهة سطر الأوامر (CLI) ل SMA لتعديل شفرات SSL:

1. احفظ ملف تكوين SMA في الكمبيوتر المحلي.
2. افتح ملف XML.
3. ابحث عن قسم *<ssl>* في 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. قم بتعديل التشفير حسب الرغبة واحفظ XML:

```
<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. قم بتحميل ملف التكوين الجديد إلى SMA.

6. **إرسال** كافة التغييرات **وتنفيذها**.

معلومات ذات صلة

- Cisco ESA - ملاحظات الإصدار
- Cisco ESA - أدلة المستخدم
- Cisco SMA - ملاحظات الإصدار
- Cisco SMA - أدلة المستخدم
- 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).