تبديل الطرق والشفرات المستخدمة مع SSL/TLS على ESA

المحتويات

المقدمة

يصف هذا المستند كيفية تغيير الطرق والشفرات التي يتم إستخدامها مع تكوينات طبقة مأخذ التوصيل الآمنة (SSL) أو أمان طبقة النقل (TLS) على جهاز أمان البريد الإلكتروني من Cisco (ESA).

تبديل الطرق والشفرات المستخدمة مع SSL/TLS

ملاحظة: يجب تعيين أساليب وشفرات SSL/TLS استنادا إلى 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.

باستخدام Cisco AsyncOS لأمان البريد الإلكتروني، يمكن أن يستخدم المسؤول الأمر **sslconfig** لتكوين بروتوكولات SSL أو TLS للطرق والشفرات التي يتم إستخدامها لاتصالات واجهة المستخدم الرسومية (GUI)، والإعلان عنها للاتصالات الواردة، وطلب الاتصالات الصادرة:

```
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
                                                                SSL v2 .1
                                                                SSL v3 .2
                                                             TLS v1/TLS v1.2 .3
                                                               SSL v2 and v3 .4
                                                    SSL v3 and TLS v1/TLS v1.2 .5
                                                 SSL v2, v3 and TLS v1/TLS v1.2 .6
                                                                <[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 -
<[]
```

إذا تم إجراء تغييرات على تكوين SSL، فتأكد من **تنفيذ** أي تغييرات وكل التغييرات.

أساليب SSL

في AsyncOS لإصدارات أمان البريد الإلكتروني 9.6 والإصدارات الأحدث، يتم تعيين ESA على إستخدام طريقة *TLS v1.2 v1/TLS* بشكل افتراضي. وفي هذه الحالة، يتخذ TLSv1.2 سابقة للاتصال، إذا كان يستخدم من جانب كل من الأطراف المرسلة والمستقبلة. لإنشاء اتصال TLS، يجب أن يكون لكلا الجانبين طريقة تمكين واحدة على الأقل تتطابق، وشفرة واحدة على الأقل تم تمكينها وتطابق.

ملاحظة: في AsyncOS لإصدارات أمان البريد الإلكتروني قبل الإصدار 9.6، يحتوي الإعداد الافتراضي على طريقتين: *SSL v3* و*TLS v1*. قد يرغب بعض المسؤولين في تعطيل SSL v3 نظرا لنقاط الضعف الأخيرة (في حالة تمكين SSL v3).

شفرات SSL

عندما تعرض التشفير الافتراضي الذي تم سرده في المثال السابق، من المهم فهم سبب إظهاره شفرين متبوعين بكلمة *all*. على الرغم من أن *ALL* يتضمن الشفرين الذين يسبقونه، فإن ترتيب الشفرة في قائمة التشفير يحدد التفضيل. وهكذا، عند إجراء اتصال TLS، يختار العميل أول تشفير يدعمه كلا الجانبين استنادا إلى ترتيب الظهور في القائمة.

ملاحظة: يتم تمكين شفرات RC4 بشكل افتراضي على ESA. في المثال السابق، يستند **متوسط:high** إلى منع المفاوضات حول التشفير الفارغ أو المجهول على مستند Cisco الخاص ب ESA و SMA. لمزيد من المعلومات فيما يتعلق ب RC4 تحديدا، ارجع إلى وثيقة Mozilla Security/Server Side TLS، وأيضا وثيقة حول أمان RC4 في TLS و WPA المقدمة من *ندوة Usenix Security 2013*. لإزالة شفرات RC4 من الاستخدام، ارجع إلى الأمثلة التالية.

من خلال التلاعب بقائمة التشفير، يمكنك التأثير على التشفير الذي يتم إختياره. يمكنك سرد شفرة أو نطاقات تشفير معينة، وإعادة ترتيبها أيضا بالقوة باستخدام تضمين خيار **@STRENGTH** في سلسلة التشفير، كما هو موضح هنا:

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

تأكد من مراجعة كل التشفير والنطاقات المتوفرة على ESA. دخلت in order to شاهدت هذا، ال **sslconfig** أمر، يتبع ال **verify** أمر فرعي. تكون خيارات فئات تشفير SSL **منخفضة**، و**متوسطة**، و**عالية**، و**الكل**:

```
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
```

أنت يستطيع أيضا جمعت هذا in order to تضمنت نطاقات:

```
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
```

يجب إزالة أي من شفرات SSL التي لا تريد تكوينها وتوفرها باستخدام الخيار **-"** الذي يسبق الشفرات المحددة. فيما يلي مثال:

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

قد تؤدي المعلومات الواردة في هذا المثال إلى إلغاء تشفير *NULL* و*EDH-RSA-DES-CBC3-SHA* و*EDH-DSS-DES-CBC3-SHA* و*DES-CBC3-SHA* من الإعلان ومنع إستخدامها في اتصال SSL.

يمكنك أيضا إنجاز مماثل مع تضمين حرف **!"** أمام مجموعة التشفير أو السلسلة التي تريد أن تصبح غير متوفرة:

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

ستؤدي المعلومات الواردة في هذا المثال إلى إزالة جميع شفرات RC4 من الاستخدام. وبالتالي، سيتم إلغاء شفرات *RC4-SHA* و*RC4-MD5* ولن يتم الإعلان عنها في اتصال SSL.

إذا تم إجراء تغييرات على تكوين SSL، فتأكد من **تنفيذ** أي تغييرات وكل التغييرات.

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).