تكوين ESA لتفضيل PFS

المحتويات

المقدمة

يصف هذا وثيقة كيف أن يشكل التفضيل ل (Perfect Forward Secret (PFS في Transport Layer Security (TLS)) يشفر توصيل على جهاز أمان البريد الإلكتروني (ESA).

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة طبقة مآخذ التوصيل الآمنة (SSL/TLS).

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى AsyncOS لإصدار Email 9.6 والإصدارات الأحدث.

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.

معلومات أساسية

توفر ESA السرية لإعادة التوجيه (PFS). تعني إعادة توجيه السرية أن البيانات يتم نقلها عبر قناة تستخدم تشفير متماثل مع أسرار سريعة، وحتى إذا تم أختراق المفتاح الخاص (المفتاح طويل المدى) على أحد المضيفين أو كليهما، فمن غير الممكن فك تشفير جلسة سجلت مسبقا.

لا يتم نقل السر عبر القناة، بدلا من ذلك، يشتق السر المشترك مع مشكلة حسابية (Diffie Hellman (DH) مشكلة). لا يتم تخزين المفتاح في أي مكان آخر من المضيف ذاكرة الوصول العشوائي (RAM) أثناء الجلسة المحددة أو مهلة

إعادة إنشاء المفتاح.

يدعم ESA DH لتبادل المفاتيح.

التكوين

الوارد - يعمل ESA كخادم TLS

تتوفر مجموعات التشفير هذه على ESA لحركة مرور بروتوكول نقل البريد البسيط (SMTP) الواردة التي توفر سرية إعادة التوجيه. في هذا المثال، يسمح تحديد التشفير فقط لمجموعات التشفير التي تعتبر عالية أو متوسطة واستخدام Diffie Hellman (EDH) المؤقت لتبادل المفاتيح ويفضل TLSv1.2. تتبع صياغة تحديد التشفير صياغة OpenSSL.

تشفير مع سرية إعادة التوجيه على AsyncOS 9.6+:

```
"EDH+TLSv1.2:EDH+HIGH:EDH+MEDIUM:!LOW:!EXP:!aNULL:!RC4:!DSS:!SEED:!IDEA:!MD5:!PSK:!3DES:!SRP"

List:  DHE-RSA-AES256-GCM-SHA384 TLSv1.2 Kx=DH Au=RSA Enc=AESGCM(256) Mac=AEAD
       DHE-RSA-AES256-SHA256 TLSv1.2 Kx=DH Au=RSA Enc=AES(256) Mac=SHA256
       DHE-RSA-AES128-GCM-SHA256 TLSv1.2 Kx=DH Au=RSA Enc=AESGCM(128) Mac=AEAD
       DHE-RSA-AES128-SHA256 TLSv1.2 Kx=DH Au=RSA Enc=AES(128) Mac=SHA256
       DHE-RSA-AES256-SHA SSLv3 Kx=DH Au=RSA Enc=AES(256) Mac=SHA1
       DHE-RSA-CAMELLIA256-SHA SSLv3 Kx=DH Au=RSA Enc=Camellia(256) Mac=SHA1
       DHE-RSA-AES128-SHA SSLv3 Kx=DH Au=RSA Enc=AES(128) Mac=SHA1
       DHE-RSA-CAMELLIA128-SHA SSLv3 Kx=DH Au=RSA Enc=Camellia(128) Mac=SHA1
```

يوضح قسم kx (= مفتاح التبادل) أن DH يتم إستخدامه لاستخلاص السر.

يدعم ESA هذه التشفير باستخدام إعدادات **sslconfig** الافتراضية (:ALL)، ولكنه لا يفضلها. إذا كنت تريد تفضيل التشفير الذي يقدم PFS، تحتاج إلى تغيير **sslconfig** وإضافة EDH أو مجموعة **EDH+<cipher أو اسم مجموعة التشفير>** إلى تحديد التشفير الخاص بك.

التكوين الافتراضي:

```
ESA> sslconfig

:sslconfig settings
Inbound SMTP method:  tlsv1/tlsv1.2
:Inbound SMTP ciphers
        RC4-SHA
        RC4-MD5
            ALL
```

تكوين جديد:

```
ESA> sslconfig

Inbound SMTP method:  tlsv1/tlsv1.2
:Inbound SMTP ciphers
    EDH+TLSv1.2
       EDH+HIGH
     EDH+MEDIUM
        RC4-SHA
```

```
RC4-MD5
ALL
```

ملاحظة: يعتبر RC4 كتشفير و MD5 كعنوان MAC ضعيفا، متوارثا ولتجنب إستخدامه مع SSL/TLS، لا سيما عندما يتعلق الأمر بزيادة حجم البيانات دون إعادة إنشاء المفاتيح.

إعدادات sslconfig الموصى بها للداخل

وهو رأي سائد ولا يسمح إلا بالشفرات التي تعتبر عموما قوية وآمنة.

تكوين قابل للتوصية للداخل يزيل RC4 و MD5 بالإضافة إلى الخيارات القديمة والضعيفة الأخرى، مثل التصدير (EXP)، و LOW (LOW)، و IDEA (IDEA)، و SEED (SEED)، و 3DES (3DES) تشفير، و DSS Certificates (DSS))، و NULL (Anonymous Key Exchange)، و PSK (PreShared)، و SRP، وتعطيل المنحنى البيضاوي Diffie Hellman (ECDH) لخوارزمية التوقيع الرقمي للمفتاح والمنحنى البيضاوي (ECDSA (DSS) هي الأمثلة:

```
EDH+TLSv1.2:EDH+HIGH:EDH+MEDIUM:HIGH:MEDIUM:!ECDH:!ECDSA:!LOW:!EXP:!aNULL:!RC4:!DSS:!SEED:!IDEA:
!MD5:!PSK:!3DES:!SRP
```

ينتج عن السلسلة التي تم إدخالها في **sslconfig** هذه القائمة من التشفير المدعوم للداخل:

```
DHE-RSA-AES256-GCM-SHA384 TLSv1.2 Kx=DH Au=RSA Enc=AESGCM(256) Mac=AEAD
     DHE-RSA-AES256-SHA256 TLSv1.2 Kx=DH Au=RSA Enc=AES(256) Mac=SHA256
DHE-RSA-AES128-GCM-SHA256 TLSv1.2 Kx=DH Au=RSA Enc=AESGCM(128) Mac=AEAD
     DHE-RSA-AES128-SHA256 TLSv1.2 Kx=DH Au=RSA Enc=AES(128) Mac=SHA256
           DHE-RSA-AES256-SHA SSLv3 Kx=DH Au=RSA Enc=AES(256) Mac=SHA1
  DHE-RSA-CAMELLIA256-SHA SSLv3 Kx=DH Au=RSA Enc=Camellia(256) Mac=SHA1
           DHE-RSA-AES128-SHA SSLv3 Kx=DH Au=RSA Enc=AES(128) Mac=SHA1
  DHE-RSA-CAMELLIA128-SHA SSLv3 Kx=DH Au=RSA Enc=Camellia(128) Mac=SHA1
     AES256-GCM-SHA384 TLSv1.2 Kx=RSA Au=RSA Enc=AESGCM(256) Mac=AEAD
          AES256-SHA256 TLSv1.2 Kx=RSA Au=RSA Enc=AES(256) Mac=SHA256
                AES256-SHA SSLv3 Kx=RSA Au=RSA Enc=AES(256) Mac=SHA1
    CAMELLIA256-SHA SSLv3 Kx=RSA Au=RSA Enc=Camellia(256) Mac=SHA1
     AES128-GCM-SHA256 TLSv1.2 Kx=RSA Au=RSA Enc=AESGCM(128) Mac=AEAD
          AES128-SHA256 TLSv1.2 Kx=RSA Au=RSA Enc=AES(128) Mac=SHA256
                AES128-SHA SSLv3 Kx=RSA Au=RSA Enc=AES(128) Mac=SHA1
    CAMELLIA128-SHA SSLv3 Kx=RSA Au=RSA Enc=Camellia(128) Mac=SHA1
```

ملاحظة: لا تدعم ESA الذي يعمل كخادم TLS (حركة مرور البيانات الواردة) حاليا Diffie Hellman للمنحنى البيضاوي لتبادل المفاتيح (ECDHE) وشهادات ECDSA.

الصادر - تعمل ESA كعميل TLS

بالنسبة لحركة مرور SMTP الصادرة، يدعم ESA بالإضافة إلى الوارد شهادات ECDHE و ECDSA.

ملاحظة: شهادات تشفير المنحنى البيضاوي (ECC) مع ECDSA لا تعتمد على نطاق واسع.

عند تسليم بريد إلكتروني صادر، يكون ESA هو عميل TLS. شهادة عميل TLS إختيارية. إذا لم يفرض خادم TLS (يتطلب) ESA (كعميل TLS) لتوفير شهادة عميل ECDSA، يمكن ل ESA متابعة جلسة عمل مؤمنة ببروتوكول ECDSA. عندما يطلب من ESA كعميل TLS شهادته، فإنه يوفر شهادة RSA التي تم تكوينها للاتجاه الصادر.

تحذير: لا يتضمن مخزن شهادات CA (قائمة النظام) المثبت مسبقا في ESA شهادات جذر ECDSA) ECC)!

قد تحتاج إلى إضافة شهادات جذر نظام تصحيح الأخطاء (ECC) يدويا (والتي تثق بها) إلى القائمة المخصصة من أجل جعل سلسلة ثقة ECC قابلة للتحقق.

من أجل تفضيل شفرات DHE/ECDHE التي توفر سرية إعادة التوجيه، يمكنك تعديل تحديد تشفير **sslconfig** كما يلي.

أضف هذا إلى تحديد التشفير الحالي.

```
"EDH+TLSv1.2:ECDH+TLSv1.2:EDH+HIGH:EDH+MEDIUM:ECDH+HIGH:ECDH+MEDIUM"
```

إعدادات sslconfig الموصى بها ل OUTBOUND

وهو رأي سائد ولا يسمح إلا بالشفرات التي تعتبر عموما قوية وآمنة.

```
EDH+TLSv1.2:ECDH+TLSv1.2:EDH+HIGH:EDH+MEDIUM:ECDH+HIGH:ECDH+MEDIUM:HIGH:MEDIUM:!LOW:!EXP:!aNULL:
!RC4:!DSS:!SEED:!IDEA:!MD5:!PSK:!3DES:!SRP
```

ينتج عن السلسلة التي تم إدخالها في **sslconfig** هذه القائمة من التشفير المدعوم للصادر:

```
DHE-RSA-AES256-GCM-SHA384 TLSv1.2 Kx=DH Au=RSA Enc=AESGCM(256) Mac=AEAD
DHE-RSA-AES256-SHA256 TLSv1.2 Kx=DH Au=RSA Enc=AES(256) Mac=SHA256
DHE-RSA-AES128-GCM-SHA256 TLSv1.2 Kx=DH Au=RSA Enc=AESGCM(128) Mac=AEAD
DHE-RSA-AES128-SHA256 TLSv1.2 Kx=DH Au=RSA Enc=AES(128) Mac=SHA256
ECDHE-RSA-AES256-GCM-SHA384 TLSv1.2 Kx=ECDH Au=RSA Enc=AESGCM(256) Mac=AEAD
ECDHE-ECDSA-AES256-GCM-SHA384 TLSv1.2 Kx=ECDH Au=ECDSA Enc=AESGCM(256) Mac=AEAD
ECDHE-RSA-AES256-SHA384 TLSv1.2 Kx=ECDH Au=RSA Enc=AES(256) Mac=SHA384
ECDHE-ECDSA-AES256-SHA384 TLSv1.2 Kx=ECDH Au=ECDSA Enc=AES(256) Mac=SHA384
ECDHE-RSA-AES128-GCM-SHA256 TLSv1.2 Kx=ECDH Au=RSA Enc=AESGCM(128) Mac=AEAD
ECDHE-ECDSA-AES128-GCM-SHA256 TLSv1.2 Kx=ECDH Au=ECDSA Enc=AESGCM(128) Mac=AEAD
ECDHE-RSA-AES128-SHA256 TLSv1.2 Kx=ECDH Au=RSA Enc=AES(128) Mac=SHA256
ECDHE-ECDSA-AES128-SHA256 TLSv1.2 Kx=ECDH Au=ECDSA Enc=AES(128) Mac=SHA256
DHE-RSA-AES256-SHA SSLv3 Kx=DH Au=RSA Enc=AES(256) Mac=SHA1
DHE-RSA-CAMELLIA256-SHA SSLv3 Kx=DH Au=RSA Enc=Camellia(256) Mac=SHA1
DHE-RSA-AES128-SHA SSLv3 Kx=DH Au=RSA Enc=AES(128) Mac=SHA1
DHE-RSA-CAMELLIA128-SHA SSLv3 Kx=DH Au=RSA Enc=Camellia(128) Mac=SHA1
ECDHE-RSA-AES256-SHA SSLv3 Kx=ECDH Au=RSA Enc=AES(256) Mac=SHA1
ECDHE-ECDSA-AES256-SHA SSLv3 Kx=ECDH Au=ECDSA Enc=AES(256) Mac=SHA1
ECDHE-RSA-AES128-SHA SSLv3 Kx=ECDH Au=RSA Enc=AES(128) Mac=SHA1
ECDHE-ECDSA-AES128-SHA SSLv3 Kx=ECDH Au=ECDSA Enc=AES(128) Mac=SHA1
AES256-GCM-SHA384 TLSv1.2 Kx=RSA Au=RSA Enc=AESGCM(256) Mac=AEAD
AES256-SHA256 TLSv1.2 Kx=RSA Au=RSA Enc=AES(256) Mac=SHA256
AES256-SHA SSLv3 Kx=RSA Au=RSA Enc=AES(256) Mac=SHA1
CAMELLIA256-SHA SSLv3 Kx=RSA Au=RSA Enc=Camellia(256) Mac=SHA1
AES128-GCM-SHA256 TLSv1.2 Kx=RSA Au=RSA Enc=AESGCM(128) Mac=AEAD
AES128-SHA256 TLSv1.2 Kx=RSA Au=RSA Enc=AES(128) Mac=SHA256
AES128-SHA SSLv3 Kx=RSA Au=RSA Enc=AES(128) Mac=SHA1
CAMELLIA128-SHA SSLv3 Kx=RSA Au=RSA Enc=Camellia(128) Mac=SHA1
```

التحقق من الصحة

لا يوجد حاليًا إجراء للتحقق من صحة هذا التكوين.

استكشاف الأخطاء وإصلاحها

لا تتوفر حاليًا معلومات محددة لاستكشاف الأخطاء وإصلاحها لهذا التكوين.

معلومات ذات صلة

- فتح شفرات SSL
- تشفير الجيل التالي من Cisco
- 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).