دليل ترقية AsyncOS الأحدث لأمان البريد الإلكتروني 9.5 مع فشل الشهادات القديمة TLSv1.2 اتصال (MD5)

المحتويات

المقدمة

يصف هذا المستند الخطوات الضرورية التي يجب تطبيقها في حالة مواجهة مشكلة باتصال TLS، أو الوصول إلى واجهة الويب، بعد الترقية إلى AsyncOS لإصدار أمان البريد الإلكتروني 9.5 أو إصدار أحدث على أجهزة أمان البريد الإلكتروني (ESA) من Cisco.

تتسبب الشهادات القديمة (MD5) في فشل اتصال TLSv1.2 على 9.5 AsyncOS لترقيات أمان البريد الإلكتروني والإصدارات الأحدث

ملاحظة: فيما يلي حل بديل مدرج لشهادات العرض التوضيحي الحالية المطبقة على الجهاز. ومع ذلك، قد تنطبق الخطوات التالية أيضا على أي شهادات MD5 موقعة.

عند إجراء ترقية إلى AsyncOS للإصدار 9.5 وأحدث من أمان البريد الإلكتروني، قد تواجه أي من الشهادات التوضيحية القديمة ل IronPort التي لا تزال قيد الاستخدام ومطبقة للتسليم أو الاستلام أو LDAP أخطاء أثناء محاولة الاتصال عبر TLSv1/TLSv1.2 ببعض المجالات. سيؤدي خطأ TLS إلى فشل جميع جلسات العمل الواردة أو الصادرة.

إذا تم تطبيق الشهادات على واجهة HTTPS، ستفشل مستعرضات الويب الحديثة في الوصول إلى واجهة الويب الخاصة بالجهاز.

يجب أن تبدو سجلات البريد مماثلة للمثال التالي:

```
,Tue Jun 30 15:27:59 2015 Info: ICID 4420993 TLS failed: (336109761
('error:1408A0C1:SSL routines:SSL3_GET_CLIENT_HELLO:no shared cipher'
```

يحدث هذا الخطأ بسبب خوارزمية التوقيع المطبقة على الشهادة الأقدم وهي MD5، ومع ذلك، فإن الشهادات المرتبطة بجهاز التوصيل/المستعرض تدعم الخوارزميات المستندة إلى توقيع SHA فقط. على الرغم من ذلك، فإن شهادات العرض التوضيحي الأقدم التي تحتوي على توقيع MD5 تظهر على الجهاز في نفس الوقت الذي تظهر فيه شهادة العرض التوضيحية الجديدة المستندة إلى SHA الخطأ أعلاه إلا إذا تم تطبيق الشهادة المستندة إلى توقيع MD5 على الأقسام المحددة (مثل الاستلام والتسليم وما إلى ذلك).

فيما يلي مثال مأخوذ من واجهة سطر الأوامر الخاصة بجهاز مزود بشهادات MD5 القديمة بالإضافة إلى شهادة العرض

التوضيحي الجديدة (ملاحظة: يجب أن تكون الشهادة الأحدث (النسخة التجريبية) هي خوارزمية SHA الأحدث وأن يكون لها تاريخ انتهاء صلاحية أطول من شهادات العرض التوضيحي القديمة).:

```
                                                    List of Certificates
Name       Common Name           Issued By             Status         Remaining
---------  ------------  --------------------  --------------------  ---------
delivery_  IronPort Appliance D  IronPort Appliance D  Active          303 days
https_cer  IronPort Appliance D  IronPort Appliance D  Active          303 days
ldaps_cer  IronPort Appliance D  IronPort Appliance D  Active          303 days
receiving  IronPort Appliance D  IronPort Appliance D  Valid           303 days
Demo       Cisco Appliance Demo  Cisco Appliance Demo  Active         3218 days
```

إجراءات تصحيحية

1. انتقل إلى الويب (UI): **الشبكة > الشهادات**
2. تحقق من أن لديك حاليا الشهادات القديمة المثبتة لديك أيضا شهادة SHA التجريبية الجديدة.
3. بناء على أين يتم تطبيق شهادات العرض التوضيحي القديمة، استبدل هذا بشهادة عرض توضيحي جديدة.

بشكل نموذجي، يمكن العثور على تلك الشهادات التي يتم تطبيقها في الأقسام التالية:

- **شبكة > مستمعين > اسم المستمع > ترخيص**
- **سياسات البريد > تحكمات الوجهة > تحرير الإعدادات العامة > الترخيص**
- **شبكة > واجهة IP > إختيار الواجهة المرتبطة بالوصول إلى واجهة المستخدم الرسومية (GUI) > شهادة HTTPS**
- **إدارة النظام > LDAP > تحرير الإعدادات > الترخيص**

4. بمجرد إستبدال جميع الشهادات، تحقق من سطر الأوامر من نجاح اتصال TLS الآن.

مثال على اتصال TLS العامل الذي يتم التفاوض عليه باستخدام TLSv1.2:

```
(Thu Jul  2 16:38:30 2015 Info: New SMTP ICID 4435675 interface Data1 (10.0.10.1
address 209.85.213.182 reverse dns host mail-ig0-f182.google.com verified yes Thu Jul 2 16:38:30
2015 Info: ICID 4435675 ACCEPT SG UNKNOWNLIST match sbrs[0.0:10.0] SBRS 4.8 Thu Jul 2 16:38:30
2015 Info: ICID 4435675 TLS success protocol TLSv1.2 cipher AES128-GCM-SHA256
```

إجراءات CLI التصحيحية (إذا تعذر الوصول إلى واجهة المستخدم الرسومية)

قد يلزم تعديل الشهادة على كل واجهة IP تحتوي على شهادة تم تمكينها لخدمة HTTPS. لتعديل الشهادة المستخدمة للواجهات، يرجى تشغيل الأوامر التالية على CLI (واجهة سطر الأوامر):

1. اكتب **interfaceConfig**.
2. حدد **تحرير**.
3. أدخل رقم الواجهة التي تريد تحريرها.
4. أستخدم مفتاح الإرجاع لقبول الإعدادات الحالية لكل سؤال معروض. عندما يكون خيار الشهادة أن تطبق معروض، حدد شهادة العرض التوضيحي:
   1.

```
Ironport Demo Certificate .1
Demo .2
Please choose the certificate to apply:
[1]> 2

You may use "Demo", but this will not be secure.
Do you really wish to use the "Demo" certificate? [N]> Y
```

5. قم بإنهاء المرور خلال مطالبات الإعدادات حتى يتم إكمال جميع أسئلة التكوين.
6. أستخدم مفتاح الإرجاع للخروج إلى موجه أوامر واجهة سطر الأوامر (CLI) الرئيسية.

7. **تستخدم** حفظ التغييرات التي أجريتها على التكوين.

ملاحظة: يرجى تذكر **إجراء** التغييرات بعد تغيير الشهادة المستخدمة على الواجهة.

معلومات ذات صلة

- دليل الإعداد الشامل لقوائم التحكم في الوصول إلى النقل (TLS) على ESA
- جهاز أمان البريد الإلكتروني من Cisco - أدلة المستخدم النهائي
- جهاز إدارة الأمان من Cisco - أدلة المستخدم النهائي
- 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).