تقوم TLS الخاصة بوحدة خدمات NGFW النمطية بإجهاض أخطاء بسبب فشل مصافحة اليدي أو خطأ في التحقق من صحة الشهادات

المحتويات

المقدمة

يصف هذا المستند كيفية استكشاف أخطاء عينة وإصلاحها مع الوصول إلى المواقع المستندة إلى HTTPS من خلال الوحدة النمطية لخدمات جدار الحماية (NGFW) من الجيل التالي من Cisco مع تمكين فك التشفير.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- إجراءات مصافحة طبقة مآخذ التوصيل الآمنة (SSL)
- شهادات SSL

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى الوحدة النمطية Cisco NGFW Services Module مع Cisco Prime Security Manager (PRSM)، الإصدار 9.2.1.2(52).

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.

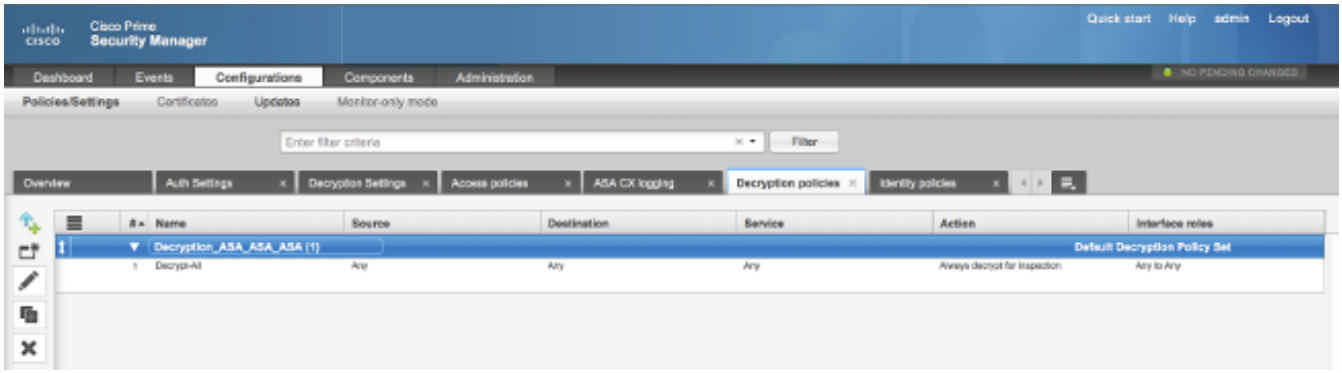
معلومات أساسية

فك التشفير وه ميزة تتيح لوحدة خدمات NGFW فك تشفير تدفقات SSL المشفرة (وفحص المحادثة التي يتم تشفيرها بخلاف ذلك) وفرض سياسات على حركة المرور. لتكوين هذه الميزة، يجب على المسؤولين تكوين شهادة فك تشفير على وحدة NGFW، والتي يتم تقديمها إلى مواقع ويب المستندة إلى HTTPS الخاصة بوصول العميل بدلا من شهادة الخادم الأصلية.

لكي يعمل فك التشفير، يجب أن تثق الوحدة النمطية NGFW في الشهادة المقدمة من الخادم. يشرح هذا المستند السيناريوهات التي يفشل فيها تأكيد اتصال SSL بين وحدة خدمات NGFW والخادم، مما يتسبب في فشل بعض مواقع الويب المستندة إلى HTTPS عند محاولة الوصول إليها.

لأغراض هذا المستند، يتم تحديد هذه السياسات على الوحدة النمطية لخدمات NGFW مع PRSM:

- **سياسات الهوية**: لا توجد سياسات هوية محددة.
- **سياسات فك التشفير**: يستخدم نهج **فك تشفير الكل** هذا التكوين:

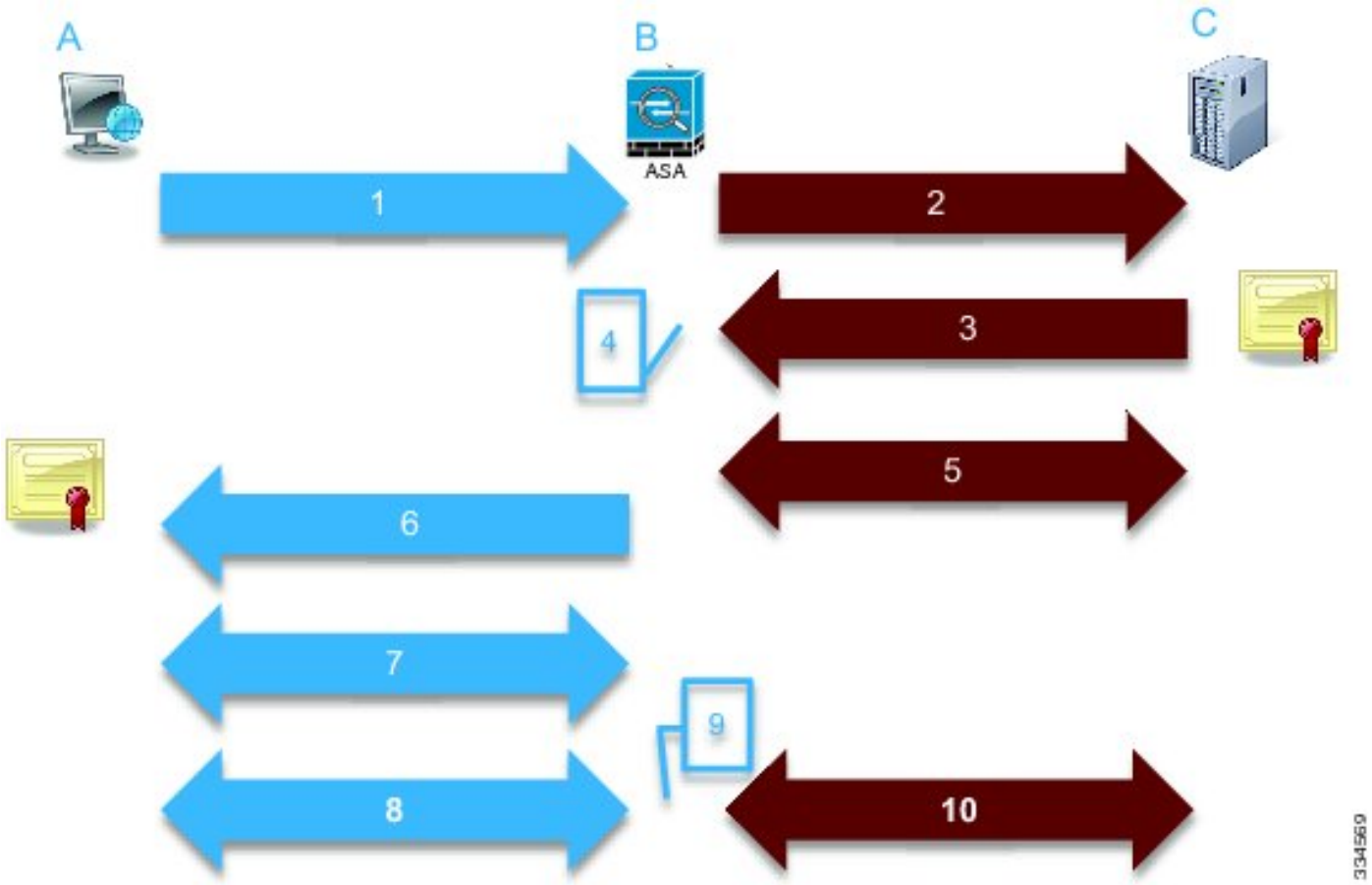


- **سياسات الوصول**: لا توجد سياسات وصول محددة.
- **إعدادات فك التشفير**: يفترض هذا المستند أن **شهادة فك التشفير** تم تكوينها على الوحدة النمطية لخدمات NGFW وأن العملاء يثقون بها.

عند تحديد سياسة فك تشفير على وحدة خدمات NGFW وتم تكوينها كما هو موضح مسبقا، تحاول الوحدة النمطية لخدمات NGFW اعتراض جميع حركة مرور بيانات SSL المشفرة من خلال الوحدة النمطية وفك التشفير.

> **ملاحظة**: يتوفر شرح خطوة بخطوة لهذه العملية في قسم [تدفق حركة المرور التي تم فك تشفيرها](#) في [دليل المستخدم لـ ASA CX و Cisco Prime Security Manager، الإصدار 9.2](#).

تصف هذه الصورة تسلسل الأحداث:



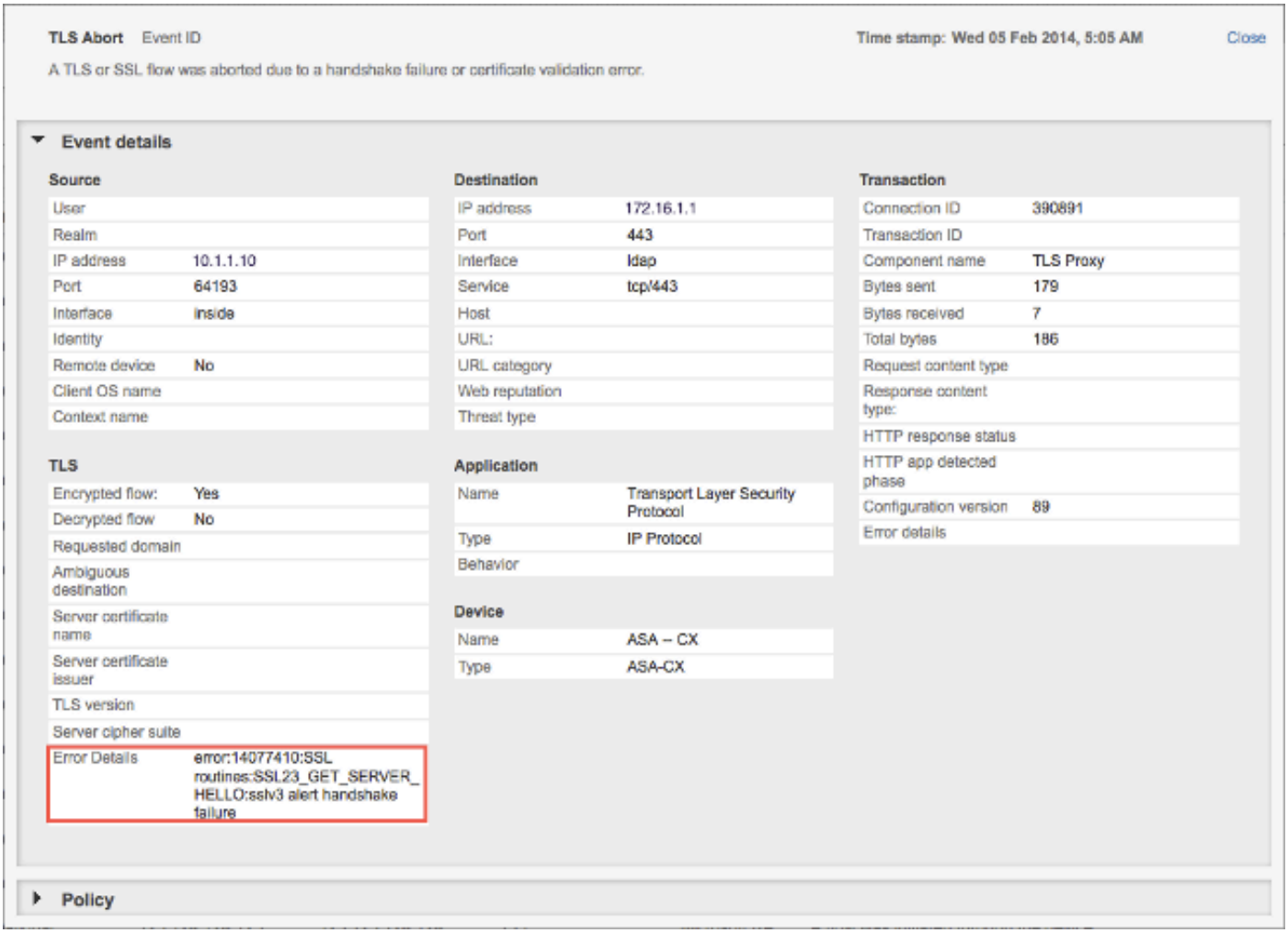
في هذه الصورة، يمثل **A** العميل و**B** وحدة خدمات NGFW و**C** هو خادم HTTPS. للأمثلة الواردة في هذا المستند، يعد الخادم المستند إلى HTTPS بمثابة مدير أجهزة الأمان المعدلة (ASDM) من Cisco على جهاز الأمان القابل للتكيف (ASA) من Cisco.

هناك عاملان مهمان في هذه العملية يتعين عليك أن تتأملهما:

- في الخطوة الثانية من العملية، يجب أن يقبل الخادم إحدى مجموعات شفرة SSL التي يتم تقديمها بواسطة وحدة خدمات NGFW.
- في الخطوة الرابعة من العملية، يجب أن تثق وحدة خدمات NGFW في الشهادة التي يقدمها الخادم.

المشكلة

إذا تعذر على الخادم قبول أي من شفرات SSL التي تم تقديمها بواسطة وحدة خدمات NFGW، فستتلقى رسالة خطأ مماثلة لما يلي:



من المهم أن تأخذ علما بمعلومات تفاصيل الخطأ (مبرزة)، والتي تظهر:

```
error:14077410:SSL routines:SSL23_GET_SERVER_HELLO:sslv3 alert handshake failure
```

عندما تقوم بعرض الملف /var/log/cisco/tls_proxy.log في أرشيف تشخيصات الوحدات النمطية، تظهر رسائل الخطأ التالية:

```
2014-02-05 05:21:42,189 INFO  TLS_Proxy   - SSL alert message received from
 server (0x228 = "fatal : handshake failure") in Session: x2fd1f6

2014-02-05 05:21:42,189 ERROR TLS_Proxy - TLS problem (error:14077410:
 SSL routines:SSL23_GET_SERVER_HELLO:sslv3 alert handshake failure) while
 connecting to server for Session: x2fd1f6
```

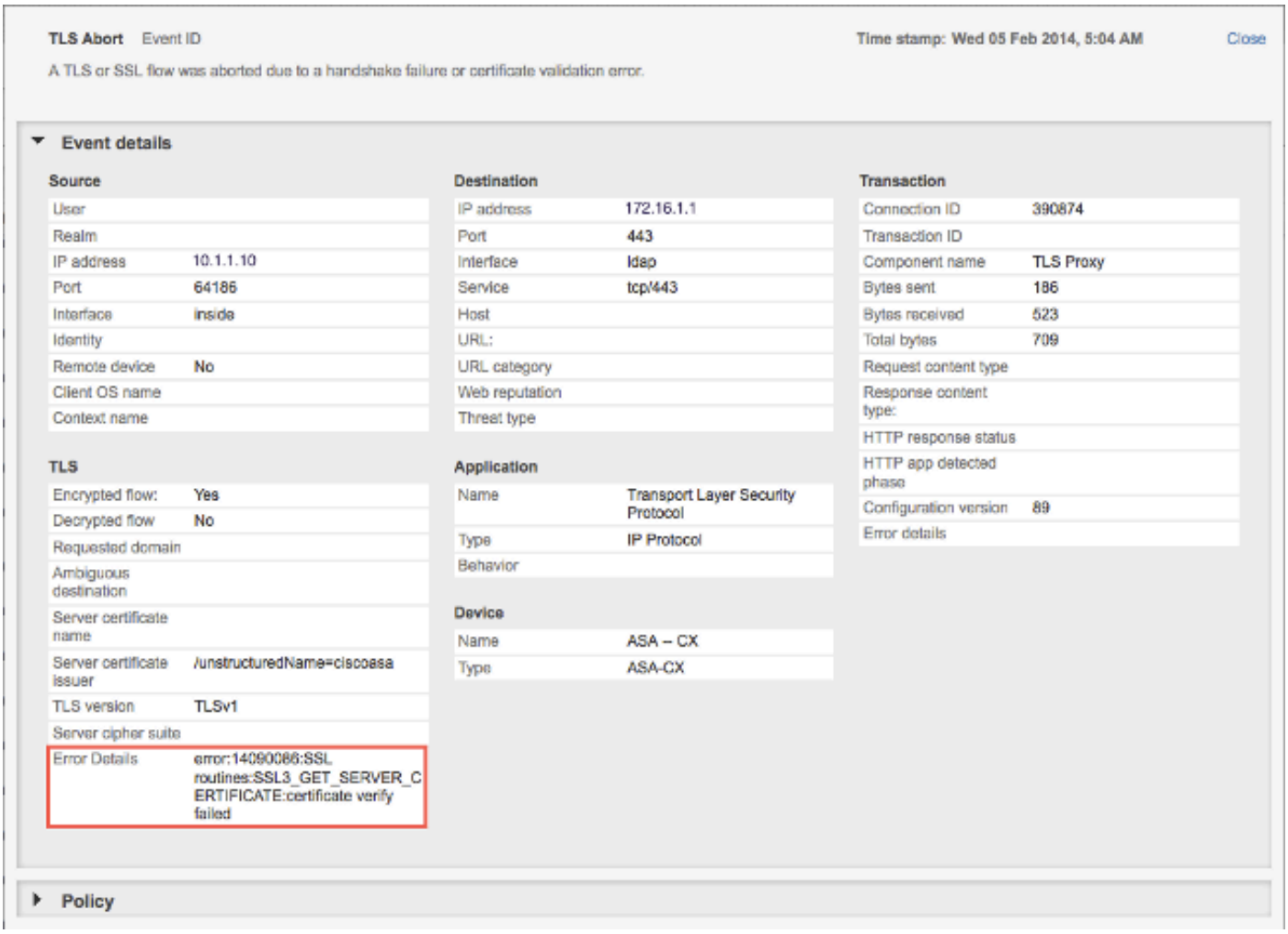
الحل

أحد الأسباب المحتملة لهذه المشكلة هو عدم تثبيت ترخيص معيار تشفير البيانات الثلاثي/معيار التشفير المتقدم (3DES/AES) (يشار إليه غالبا باسم K9) على الوحدة النمطية. يمكنك تنزيل ترخيص K9 للوحدة النمطية دون رسوم وتحميله عبر PRSM.

إذا إستمرت المشكلة بعد تثبيت ترخيص 3DES/AES، فعليك الحصول على صور الحزم لمصافحة SSL بين وحدة خدمات NGFW والخادم، والاتصال بمسؤول الخادم لتمكين تشفير SSL المناسب على الخادم.

المشكلة

إذا كانت الوحدة النمطية لخدمات NGFW ال تثق في الشهادة المقدمة من الخادم، فسوف تتلقى رسالة خطأ مماثلة لهذه:



من المهم أن تأخذ علما بمعلومات تفاصيل الخطأ (مبرزة)، والتي تظهر:

```
error:14090086:SSL routines:SSL3_GET_SERVER_CERTIFICATE:certificate verify failed
```

عندما تقوم بعرض الملف /var/log/cisco/tls_proxy.log في أرشيف تشخيصات الوحدات النمطية، تظهر رسائل الخطأ التالية:

```
2014-02-05 05:22:11,505 INFO  TLS_Proxy - Certificate verification failure:
 self signed certificate (code 18, depth 0)

2014-02-05 05:22:11,505 INFO TLS_Proxy - Subject: /unstructuredName=ciscoasa

2014-02-05 05:22:11,505 INFO TLS_Proxy - Issuer: /unstructuredName=ciscoasa

2014-02-05 05:22:11,505 INFO TLS_Proxy - SSL alert message received from
 server (0x230 = "fatal : unknown CA") in Session: x148a696e

2014-02-05 05:22:11,505 ERROR TLS_Proxy - TLS problem (error:14090086:
 SSL routines:SSL3_GET_SERVER_CERTIFICATE:certificate verify failed) while
 connecting to server for Session: x148a696e
```

الحل

إذا لم تتمكن الوحدة النمطية من الثقة في شهادة SSL للخادم، يجب إستيراد شهادة الخادم

إلى الوحدة النمطية باستخدام PRSM للتأكد من نجاح عملية مصافحة SSL.

أكمل الخطوات التالية لاستيراد شهادة الخادم:

1. تجاوز وحدة خدمات NGFW عند الوصول إلى الخادم لتنزيل الشهادة من خلال متصفح. تتمثل إحدى طرق تجاوز الوحدة النمطية في إنشاء سياسة فك تشفير الوقوم بفك تشفير حركة مرور البيانات إلى ذلك الخادم المعين. يوضح هذا الفيديو كيفية إنشاء النهج:

   هذه هي الخطوات التي تظهر في الفيديو:

   للوصول إلى PRSM على CX، انتقل إلى **https://<IP_ADDRESS_OF_PRSM>**. يستخدم هذا المثال **https://10.106.44.101**.

   انتقل إلى **التكوينات > السياسات/الإعدادات > سياسات فك التشفير** في PRSM.

   انقر فوق الرمز الموجود بالقرب من الركن العلوي الأيسر من الشاشة واختر خيار **إضافة النهج الأعلى** لإضافة نهج إلى أعلى القائمة.

   قم بتسمية النهج، واترك المصدر على أنه **Any**، ثم قم بإنشاء كائن **مجموعة شبكات CX**.
   ملاحظة: تذكر تضمين عنوان IP الخاص بالخادم المستند إلى HTTPS. في هذا المثال، يتم استخدام عنوان IP **172.16.1.1**. اختر **عدم فك التشفير** للإجراء.

   قم بحفظ النهج وتنفيذ التغييرات.
2. قم بتنزيل شهادة الخادم من خلال متصفح وتحميلها إلى وحدة خدمات NGFW عبر PRSM، كما هو موضح في هذا الفيديو:

   هذه هي الخطوات التي تظهر في الفيديو:

   بمجرد تحديد النهج المذكور مسبقا، أستخدم مستعرض للتنقل إلى الخادم المستند إلى HTTPS الذي يتم فتحه من خلال الوحدة النمطية للخدمات NGFW.
   ملاحظة: في هذا المثال، يتم استخدام Mozilla Firefox الإصدار 26.0 للتنقل إلى الخادم باستخدام عنوان URL **https://172.16.1.1**.قبل تجاوز الأمان في حالة ASA (ASDM على) ظهور استثناء أمان وإضافة استثناء أمان.

   انقر أيقونة القفل الصغيرة الموجودة على يسار شريط العنوان. يختلف موقع هذه الرمز باختلاف المستعرض المستخدم والإصدار.

   انقر فوق **عرض الشهادة** ثم فوق **تصدير** تحت علامة التبويب تفاصيل بعد أن تقوم بتحديد شهادة الخادم.

   احفظ الشهادة على جهازك الشخصي في المكان الذي تختاره.

قم بتسجيل الدخول إلى PRSM واستعرض إلى **التكوينات > الشهادات**.

انقر فوق **أريد أن ... > إستيراد الشهادة** واختر شهادة الخادم التي تم تنزيلها مسبقا (من الخطوة 4).

قم بحفظ التغييرات وتنفيذها. بمجرد اكتمال الوحدة النمطية لخدمات NGFW، يجب أن تثق في الشهادة التي يقدمها الخادم.

3. قم بإزالة النهج الذي تمت إضافته في الخطوة 1. أصبحت الوحدة النمطية لخدمات NGFW قادرة الآن على إكمال المصافحة بنجاح مع الخادم.

معلومات ذات صلة

- دليل المستخدم لـ ASA CX و Cisco Prime Security Manager، الإصدار 9.2
- 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).