تكوين شهادة فك التشفير في جهاز ويب الآمن

المحتويات

المقدمة

المتطلبات الأساسية

المتطلبات

المكونات المستخدمة

فك تشفير HTTPS

تكوين شهادة فك التشفير في SWA

تحميل شهادة ومفتاح رئيسي

إنشاء شهادة ومفتاح رئيسي HTTPS

استيراد الشهادة

استيراد شهادة وكيل تدفق البيانات إلى SWA

استيراد شهادة SWA إلى SWA أخرى

استيراد شهادة SWA في عميل Windows

استيراد شهادة SWA في عميل Mac

استيراد شهادة SWA في Ubuntu/Debian

استيراد شهادة SWA في CentOS 6

استيراد شهادة SWA في CentOS 5

استيراد شهادة SWA في Mozilla Firefox

استيراد شهادة SWA في Google Chrome

استيراد شهادة SWA في Microsoft Edge/Internet Explorer

استيراد شهادة SWA في Safari

استيراد شهادة SWA من الجهاز الموجود إلى العملاء

معلومات ذات صلة

المقدمة

يصف هذا المستند خطوات تكوين شهادات تشفير HTTPS في أجهزة ويب الآمنة (SWA) وعملاء الوكيل.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- الوصول الإداري إلى SWA
- الوصول إلى واجهة المستخدم الرسومية (GUI) ل SWA

المكونات المستخدمة

.لا يقتصر هذا المستند على إصدارات برامج ومكونات مادية معينة

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

فك تشفير HTTPS

يستخدم فك تشفير بروتوكول نقل النص التشعبي الآمن (HTTPS) ل SWA شهادات الجذر ومفاتيح الخاصة التي تقوم بتحميلها إلى الجهاز لتشفير حركة المرور. يجب أن تكون ملفات الشهادة الجذر والمفتاح الخاص التي تقوم بتحميلها إلى الجهاز بتنسيق PEM.

ملاحظة: تنسيق DER غير معتمد.

يمكنك أيضا تحميل شهادة وسيطة قام مرجع شهادة جذر بتوقيعها. عندما تنشئ SWA شهادة تمثل شهادة الخادم، فإنها ترسل الشهادة التي تم تحميلها مع الشهادة التي تم تقليدها إلى تطبيق العميل. بهذه الطريقة، طالما أن الشهادة الوسيطة موقعة من قبل المرجع المصدق الجذر (CA) الذي يثق به تطبيق العميل، فإن التطبيق يثق في شهادة الخادم التي تم تقليدها.

تكوين شهادة فك التشفير في SWA

يمكن أن تستخدم SWA شهادة موجودة ومفتاح خاص لفك تشفير HTTPS. على أي حال، يمكن أن يكون هناك إرتباك حول نوع الشهادة التي يجب إستخدامها، بما أن ليس كل شهادات X.509 تعمل.

هناك نوعان رئيسيان من الشهادات: شهادات الخادم والشهادات الجذر. تحتوي كافة شهادات

X.509 على حقل قيود أساسي، الذي يعرف نوع الشهادة:

- نوع الموضوع=وحدة النهاية - شهادة الخادم
- نوع الموضوع=CA - شهادة الجذر

تحميل شهادة ومفتاح جذر

الخطوة 1. من واجهة المستخدم الرسومية، انتقل إلى خدمات الأمان واختر وكيل HTTPS.
الخطوة 2. انقر فوق تحرير الإعدادات.
الخطوة 3. انقر فوق إستخدام الشهادة التي تم تحميلها والمفتاح.
الخطوة 4. انقر على إستعراض حقل الشهادة للتنقل إلى ملف الشهادة المخزن على الجهاز المحلي.

ملاحظة: إذا كان الملف الذي قمت بتحميله يحتوي على شهادات أو مفاتيح متعددة، فإن وكيل الويب يستخدم الشهادة أو المفتاح الأول في الملف.

الخطوة 5. انقر فوق إستعراض في حقل المفتاح للانتقال إلى ملف المفتاح الخاص.

ملاحظة: يجب أن يكون طول المفتاح 512 أو 1024 أو 2048 بت.

الخطوة 6. يتم تشفير المفتاح المحدد إذا تم تشفير المفتاح.
الخطوة 7. انقر فوق تحميل الملفات لنقل ملفات الشهادة والمفتاح إلى جهاز ويب الآمن.
يتم عرض معلومات الشهادة التي تم تحميلها في صفحة تحرير إعدادات وكيل HTTPS.
الخطوة 8. (إختياري) انقر فوق تنزيل الشهادة للنقل إلى تطبيقات العميل على الشبكة.

الخطوة 9. إرسال التغييرات وتنفيذها.

إنشاء شهادة ومفتاح لوكيل HTTPS

الخطوة 1. من واجهة المستخدم الرسومية، انتقل إلى خدمات الأمان واختر وكيل HTTPS.
الخطوة 2. انقر فوق تحرير الإعدادات.
الخطوة 3. أختر إستخدام الشهادة والمفاتح الذين تم إنشاؤهما.

.الخطوة 4. انقر فوق إنشاء شهادة ومفتاح جديدين
.الخطوة 5. في شاشة إنشاء شهادة ومفتاح، أدخل المعلومات لعرضها في الشهادة الجذر
.يمكنك إدخال أي حرف ASCII باستثناء شرطة مائلة للأمام (/) في حقل الاسم الشائع
.الخطوة 6. انقر فوق إنشاء
.الخطوة 7. يتم عرض معلومات الشهادة التي تم إنشاؤها في صفحة تحرير إعدادات وكيل HTTPS
.الخطوة 8. (إختياري) انقر على تنزيل الشهادة، حتى يمكنك نقلها إلى تطبيقات العميل على الشبكة
.الخطوة 9. (إختياري) انقر فوق إرتباط تنزيل طلب توقيع الشهادة، حتى يمكنك إرسال طلب توقيع الشهادة (CSR) إلى مرجع مصدق
.الخطوة 10. (إختياري) قم بتحميل الشهادة الموقعة إلى جهاز الويب الآمن بعد تلقيها من المرجع المصدق. يمكنك تنفيذ هذا الإجراء في أي وقت بعد إنشاء الشهادة على الجهاز
.الخطوة 11. إرسال التغييرات وتنفيذها

إستيراد الشهادة

إستيراد شهادة وكيل تدفق البيانات إلى SWA

إذا تم تكوين SWA لاستخدام وكيل للتحميل وتم تكوين وكيل الخادم لفك تشفير HTTPS، يجب إستيراد شهادة تشفير وكيل الخادم إلى SWA. يمكنك إدارة قائمة الشهادات الموثوق بها وإضافة شهادات إليها وإزالة الشهادات منها.

.الخطوة 1. من واجهة المستخدم الرسومية، أخترت شبكة واخترت شهادة إدارة
.الخطوة 2. انقر على إدارة شهادات الجذر الموثوق بها في صفحة إدارة الشهادات
.الخطوة 3. لإضافة شهادة جذر موثوق بها مخصصة لها مرجع توقيع، وليس في القائمة التي تعترف بها Cisco، انقر على إستيراد ثم أرسل ملف الشهادة

.الخطوة 4. إرسال التغييرات وتنفيذها

إستيراد شهادة SWA إلى SWA أخرى

إذا قمت بتحميل شهادة HTTPS ويمكن الوصول إلى HTTPS والمفاتح في SWA واحد لوكيل SWA آخر من ملف التكوين، فيمكنك إستيرادها إلى SWA الملفات الأصلية.

.الخطوة 1. من واجهة المستخدم الرسومية (GUI) لكل من SWAs، أختر إدارة النظام وانقر فوق ملف التكوين

.الخطوة 2. انقر فوق تنزيل الملف على الكمبيوتر المحلي لعرضه أو حفظه

الخطوة 3. أختر تشفير كلمات المرور في ملفات التكوين.

الخطوة 4. (إختياري) أختر إستخدام اسم ملف معرف من قبل المستخدم وإضافة الاسم المرغوب إلى ملف التكوين.

الخطوة 5. انقر فوق إرسال ضمن التكوين الحالي لتنزيل ملف .xml.

الخطوة 6. افتح الملفات التي تم تنزيلها باستخدام برامج تحرير النصوص أو برامج تحرير XML.

الخطوة 7. انسخ علامات التمييز هذه من SWA مع الترخيص، انسخ كل البيانات داخل علامات التمييز، واستبدلها في ملف تكوين SWA الأخرى:

```
<prox_config_signing_cert_name>....</prox_config_signing_cert_name>
<prox_config_uploaded_cert_name>....</prox_config_uploaded_cert_name>
<prox_config_uploaded_cert>....</prox_config_uploaded_key>
<prox_config_uploaded_key>....</prox_config_uploaded_key>
```

الخطوة 8. احفظ التغييرات في ملف .xml من الغاية SWA.

الخطوة 9. الاستيراد ملف التكوين الذي تم تحريره.xml مرة أخرى إلى SWA الوجهة، من واجهة المستخدم الرسومية، أختر إدارة النظام وانقر فوق ملف التكوين.

الخطوة 10. في قسم تكوين الحمل، انقر فوق تحميل ملف تكوين من كمبيوتر محلي.

الخطوة 11. انقر فوق إختيار ملف واختر ملف تكوين .xml الذي تم تحريره.

الخطوة 12. انقر فوق تحميل الاستيراد ملف التكوين الجديد باستخدام الشهادة والمفتاح.

الخطوة 13. قم بتنفيذ التغييرات إذا طلب منك النظام.

إستيراد شهادة SWA في عميل Windows

لعميل الكمبيوتر الذي يحتاج إلى الوثوق بها في شهادة HTTPS SWA لكي يستورد الشهادة، إتبع الخطوات التالية، باستخدام نظام التشغيل Microsoft Windows:

الخطوة 1. انقر على بدء من شريط المهام واكتب إدارة شهادات الكمبيوتر.
الخطوة 2. في صفحة الشهادات-الكمبيوتر المحلي، قم بتوسيع شهادة الجذر الموثوق بها وانقر بزر الماوس الأيمن على مجلد الشهادات.
الخطوة 3. انقر فوق جميع المهام واختر الاستيراد.
الخطوة 4. من صفحة معالج إستيراد الشهادات، انقر فوق التالي.
الخطوة 5. لاستيراد ملف شهادة SWA، انقر على إستعراض واختر الشهادة التي قمت بتنزيلها من SWA.

تلميح: لتنزيل شهادة SWA، ارجع إلى الخطوة 8 من القسم تحميل شهادة جذر ومفتاح HTTPS لوكيل SWA أو إنشاء شهادة ومفتاح.

الخطوة 6. انقر فوق وضع جميع الشهادات في خانة الاختيار التالية.
الخطوة 7. أختر مراجع مصادقة الجذر الموثوق بها وانقر فوق التالي.
الخطوة 8. انقر فوق إنهاء.

بدلا من ذلك، يمكنك تشغيل هذا الأمر لاستيراد الشهادة إلى مراجع التصديق الجذر الموثوق فيها.

```
certutil -addstore -f "ROOT" <Path to SWA Certificate/CertificateName.crt>
```

ملاحظة: يجب إستبدال <Path to SWA Certificate/CertificateName.crt> بمسار الشهادة والاسم الملف الحالي الذي تم تنزيله.

إستيراد شهادة SWA في عميل Mac

الخطوة 1. تنزيل شهادة وكيل HTTPS من SWA إلى عميل Mac OS.
الخطوة 2. أعد تسمية ملحق الملف إلى .crt.
الخطوة 3. قم بتشغيل هذا الأمر لاستيراد الشهادة كشهادة موثوق بها:

```
sudo security add-trusted-cert -d -r trustRoot -k /Library/Keychains/System.keychain <Path to SWA Certi
```

ملاحظة: يجب إستبدال بمسار الشهادة الذي تم تنزيله حاليا واسم الملف.

إستيراد شهادة SWA في Ubuntu/Debian

الخطوة 1. قم بتنزيل شهادة وكيل HTTPS من SWA.
الخطوة 2. افتح ملف الترخيص في محرر النص وانسخ كل المحتويات.
الخطوة 3. قم بإنشاء ملف جديد في /usr/local/share/ca-certificates/ مع a .crt كامتداد.
الخطوة 4. قم بتحرير الملف باستخدام محرر النص الذي تريده ولصق النص المنسوخ في الملف الجديد، ثم احفظ.
الخطوة 5. قم بتشغيل هذا الأمر لتحديث الشهادات في نظام التشغيل.

```
sudo update-ca-certificates
```

تلميح: إذا كان لديك الشهادة مخزنة محليا على العميل، يمكنك نسخ الشهادة إلى /usr/local/share/ca-certificates/ وتشغيل SUDO Update-ca-certificates.

ملاحظة: في بعض الإصدارات، يجب عليك تثبيت حزمة شهادات التصديق باستخدام هذا الأمر: تثبيت SUDO APT-Get - شهادات مرجع مصدق.

إستيراد شهادة SWA في CentOS 6

الخطوة 1. قم بتنزيل شهادة وكيل HTTPS من SWA.
الخطوة 2. افتح ملف الترخيص في محرر النص وانسخ كل المحتويات داخل الملف.
الخطوة 3. قم بإنشاء ملف جديد في /etc/pki/ca-trust/source/links/ باستخدام ملحق .crt.
الخطوة 4. قم بتحرير الملف باستخدام محرر النص الذي تريده والنص المنسوخ السابق في الملف الجديد، ثم احفظ.
الخطوة 5. قم بتثبيت حزمة شهادات التصديق:

```
yum install ca-certificates
```

الخطوة 6. قم بتشغيل هذا الأمر لتحديث الشهادات في نظام التشغيل:

```
update-ca-trust extract
```

تلميح: إذا كان لديك الشهادة مخزنة محليا على العميل، يمكنك نسخ الشهادة إلى /etc/pki/ca-trust/source/linkor/وتشغيل المستخرج update-ca-trust بعد تثبيت شهادات CA.

إستيراد شهادة SWA في CentOS 5

1. الخطوة قم بتنزيل شهادة وكيل HTTPS من SWA.
2. الخطوة افتح ملف الترخيص في محرر النص وانسخ كل المحتويات داخل الملف.
3. الخطوة قم بإنشاء ملف جديد في المجلد الحالي بامتداد .crt (على سبيل المثال، SWA.crt).
4. الخطوة قم بتحرير /etc/pki/tls/certs/ca-bundle.crt باستخدام محرر النص الذي تريده، قم بلصق النص المنسوخ في نهاية الملف، ثم احفظ.

تلميح: إذا كانت الشهادة مخزنة محليا على العميل (في هذا المثال، اسم الملف هو SWA.CRT)، فيمكنك إلحاق الشهادة بهذا الأمر: cat swa.crt>/etc/pki/tls/certs/ca-bundle.crt.

إستيراد شهادة SWA في Mozilla Firefox

1. الخطوة قم بتنزيل شهادة وكيل HTTPS من SWA.
2. الخطوة أعد تسمية ملحق الملف إلى .crt.
3. الخطوة افتح Firefox وانقر فوق القائمة (ثلاثة أشرطة في الزاوية العليا اليمنى).
4. الخطوة أختر الإعدادات (في بعض الإصدارات تكون خيارات).
5. الخطوة انقر فوق الخصوصية والأمان في القائمة اليسرى وانتقل إلى الشهادات.
6. الخطوة انقر فوق عرض الشهادات.
7. الخطوة انقر فوق علامة التبويب السلطات ثم الاستيراد.
8. الخطوة أختر ملف الترخيص وانقر فتح.
9. الخطوة انقر فوق OK.

إستيراد شهادة SWA في Google Chrome

1. الخطوة قم بتنزيل شهادة وكيل HTTPS من SWA.
2. الخطوة أعد تسمية ملحق الملف إلى .crt.
3. الخطوة افتح Google Chrome وانقر فوق خصائص Google Chrome والتحكم فيه (ثلاث نقاط في الزاوية العليا اليمنى).
4. الخطوة أختر الإعدادات.
5. الخطوة انقر فوق الخصوصية والأمان من القائمة اليسرى.
6. الخطوة أختر التأمين.

الخطوة 7. قم بالتمرير إلى إدارة الشهادات وانقر فوق الزر الموجود على اليمين.
الخطوة 8. أختر علامة التبويب مراجع التصديق الجذر الموثوق فيها وانقر فوق إستيراد.
الخطوة 9. أختر ملف الترخيص وانقر فتح.
الخطوة 10. انقر فوق OK.

ملاحظة: إذا قمت بتثبيت شهادة SWA في نظام التشغيل، فإن Google Chrome يثق في هذه الشهادة ولا توجد حاجة لاستيراد الشهادة بشكل منفصل إلى المستعرض الخاص بك.

إستيراد شهادة SWA في Microsoft Edge/Internet Explorer

يستخدم Microsoft Edge و Internet Explorer (IE) شهادات نظام التشغيل. إذا قمت بتثبيت شهادة SWA في نظام التشغيل، فلا حاجة لاستيراد الشهادة بشكل منفصل إلى المستعرض الخاص بك.

إستيراد شهادة SWA في Safari

الخطوة 1. قم بتنزيل شهادة وكيل HTTPS من SWA.
الخطوة 2. أعد تسمية ملحق الملف إلى .crt.
الخطوة 3. في لوحة التشغيل، حدد الوصول إلى سلسلة المفاتيح.
الخطوة 4. من القائمة ملف، انقر فوق إضافة سلسلة مفاتيح.
الخطوة 5. أختر ملف شهادة SWA وانقر إضافة.
الخطوة 6. أختر التأمين.
الخطوة 7. قم بالتمرير إلى إدارة الشهادات وانقر فوق الزر الموجود على اليمين.
الخطوة 8. أختر علامة التبويب مراجع التصديق الجذر الموثوق فيها وانقر فوق إستيراد.
الخطوة 9. أختر ملف الترخيص وانقر فتح.
الخطوة 10. انقر فوق OK.

إستيراد شهادة SWA من نهج المجموعة إلى العملاء

لتوزيع الشهادات على أجهزة كمبيوتر العميل بواسطة "نهج المجموعة" من Active Directory، استخدم الخطوات التالية:

الخطوة 1. قم بتنزيل شهادة وكيل HTTPS من SWA.
الخطوة 2. أعد تسمية ملحق الملف إلى .crt.
الخطوة 3. انسخ ملف الشهادة إلى وحدة التحكم بالمجال الخاصة بك.

الخطوة 4. في وحدة التحكم بالمجال، انقر فوق بدء وافتح الأداة الإضافية لإدارة نهج المجموعة.
الخطوة 5. ابحث عن كائن نهج المجموعة (GPO) المطلوب أو قم بإنشاء GPO جديد لاحتواء شهادة SWA لاستيرادها إلى العميل.
الخطوة 6. انقر بزر الماوس الأيمن فوق GPO، وانقر فوق تحرير.
الخطوة 7. من القائمة الموجودة على الجانب الأيسر، انتقل إلى تكوين الكمبيوتر > السياسات>إعدادات Windows > إعدادات الأمان>نهج المفاتيح العام.
الخطوة 8. انقر بزر الماوس الأيمن على مراجع التصديق الجذر الموثوق بها، وانقر على إستيراد.
الخطوة 9. انقر فوق التالي في صفحة الترحيب بمعالج إستيراد الشهادات.
الخطوة 10. أختر ملف شهادة SWA من أجل الاستيراد وانقر بعد ذلك.
الخطوة 11. انقر فوق وضع جميع الشهادات في المخزن التالي، ثم انقر فوق التالي.
الخطوة 12. تأكد من أن المعلومات المقدمة دقيقة، وانقر فوق إنهاء.

ملاحظة: في بعض الحالات، يجب إعادة تشغيل العميل أو تشغيل gpupdate /force لتطبيق التغييرات على جهاز عميل Active Directory.

المحتوى ذي الصلة

- دليل المستخدم لـ Cisco Secure Web Appliance - GD (نشر عام) لـ AsyncOS 14.5
- توزيع الشهادات على أجهزة الكمبيوتر العميلة باستخدام نهج المجموعة | Microsoft Learn
- 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).