CLI تكوين لمثال تكوين إستخدام مع القديم SCEP

المحتويات

المقدمة

يصف هذا المستند إستخدام بروتوكول تسجيل الشهادة البسيط القديم (SCEP) على جهاز الأمان القابل للتكيف (ASA) من Cisco.

تحذير: اعتبارا من Cisco AnyConnect، الإصدار 3.0، يجب عدم إستخدام هذه الطريقة. كان ذلك ضروريا في السابق لأن الأجهزة المحمولة لم تكن تحتوي على عميل x.3، ولكن يتوفر الآن لكل من Android و iPhone دعم لوكيل SCEP، والذي يجب إستخدامه بدلا من ذلك. يجب تكوين SCEP القديمة فقط في الحالات التي لا يتم فيها دعم ASA. ومع ذلك، حتى في هذه الحالات، تكون ترقية ASA هي الخيار الموصى به.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة ب SCEP القديمة.

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. بدأت جميع الأجهزة المستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي

أمر.

معلومات أساسية

SCEP هو بروتوكول تم تصميمه لجعل توزيع وإلغاء الشهادات الرقمية قابلة للتوسع قدر الإمكان. والفكرة هي أن أي مستخدم شبكة قياسي ينبغي أن يكون قادرا على طلب شهادة رقمية إلكترونيا بتدخل قليل جدا من مسؤولي الشبكة. بالنسبة لعمليات نشر الشبكات الخاصة الظاهرية (VPN) التي تتطلب مصادقة الشهادة مع المؤسسة أو المرجع المصدق (CA) أو أي مرجع مصدق من جهة خارجية يدعم SCEP، يمكن للمستخدمين الآن طلب الشهادات الموقعة من الأجهزة العميلة دون إشراك مسؤولي الشبكة.

ملاحظة: إذا كنت ترغب في تكوين ASA كخادم CA، فإن SCEP ليس طريقة البروتوكول المناسبة. أحلت المحلي ca قسم من **يشكل شهادات رقمية** cisco وثيقة بدلا من ذلك.

في الإصدار 8.3 من ASA، هناك طريقتان مدعومتان ل SCEP:

- تتم مناقشة الطريقة الأقدم، والتي تسمى SCEP القديمة، في هذا المستند.

- أسلوب وكيل SCEP هو الأسلوب الأحدث من الطريقتين، حيث يقوم وكيل ASA بتوكيل طلب تسجيل الشهادة نيابة عن العميل. هذه العملية أكثر نظافة لأنها لا تتطلب مجموعة نفق إضافية وهي أيضا أكثر أمانا. ومع ذلك، فإن العائق هو أن وكيل SCEP يعمل فقط مع الإصدار x.3 من Cisco AnyConnect. وهذا يعني أن إصدار عميل AnyConnect الحالي للأجهزة المحمولة لا يدعم وكيل SCEP.

التكوين

يوفر هذا القسم معلومات يمكنك إستخدامها لتكوين أسلوب بروتوكول SCEP القديم.

ملاحظة: أستخدم أداة بحث الأوامر (للعملاء المسجلين فقط) للحصول على مزيد من المعلومات حول الأوامر المستخدمة في هذا القسم.

فيما يلي بعض الملاحظات الهامة التي يجب وضعها في الاعتبار عند إستخدام SCEP القديمة:

- بعد أن يستلم العميل الشهادة الموقعة، يجب أن يتعرف ASA على المرجع المصدق الذي وقع الشهادة قبل أن يتمكن من مصادقة العميل. لذلك، يجب التأكد من أن ASA مرتبط أيضا بخادم CA. يجب أن تكون عملية التسجيل ل ASA الخطوة الأولى لأنها تضمن:

  يتم تكوين CA بشكل صحيح ويمكن إصدار الشهادات عبر SCEP إذا كنت تستخدم طريقة تسجيل URL.

  يمكن أن يتصل ASA مع CA. لذلك، إذا تعذر على العميل، فهذا يعني وجود مشكلة بين العميل و ASA.
- عند إجراء أول محاولة اتصال، لن تكون هناك شهادة موقعة. يجب أن يكون هناك خيار آخر يمكن إستخدامه لمصادقة العميل.

- في عملية تسجيل الشهادة، لا يخدم ASA أي دور. وهو يعمل فقط كمجمع الشبكة الخاصة الظاهرية (VPN) حتى يتمكن العميل من إنشاء نفق للحصول بشكل آمن على الشهادة الموقعة. عند إنشاء النفق، يجب أن يكون العميل قادرا على الوصول إلى خادم CA. وإلا، فلن تتمكن من التسجيل.

تسجيل ASA

عملية تسجيل ASA سهلة نسبيا ولا تتطلب أية معلومات جديدة. ارجع إلى تسجيل Cisco ASA إلى CA باستخدام مستند SCEP للحصول على مزيد من المعلومات حول كيفية تسجيل ASA إلى CA لجهة خارجية.

تكوين نفق لاستخدام التسجيل

وكما ذكر سابقا، لكي يتمكن العميل من الحصول على شهادة، يجب بناء نفق آمن مع ASA من خلال طريقة مختلفة للمصادقة. للقيام بذلك، يجب تكوين مجموعة نفق واحدة يتم إستخدامها فقط لمحاولة الاتصال الأولى عند إجراء طلب شهادة. فيما يلي لقطة للتكوين المستخدم، الذي يحدد مجموعة الأنفاق هذه (تظهر الخطوط المهمة ***بالخط*** المائل ***الغامق***):

```
rtpvpnoutbound6(config)# show run user
username cisco password ffIRPGpDSOJh9YLq encrypted privilege 0

rtpvpnoutbound6# show run group-policy gp_certenroll
group-policy gp_certenroll internal
group-policy gp_certenroll attributes
wins-server none
<dns-server value <dns-server-ip-address

vpn-tunnel-protocol ikev2 ssl-client ssl-clientless
group-lock value certenroll
split-tunnel-policy tunnelspecified
split-tunnel-network-list value acl_certenroll
default-domain value cisco.com
webvpn
anyconnect profiles value pro-sceplegacy type user

rtpvpnoutbound6# show run access-l acl_certenroll
access-list acl_certenroll remark to allow access to the CA server
access-list acl_certenroll standard permit host

rtpvpnoutbound6# show run all tun certenroll
tunnel-group certenroll type remote-access
tunnel-group certenroll general-attributes
address-pool ap_fw-policy
authentication-server-group LOCAL
secondary-authentication-server-group none
default-group-policy gp_certenroll
tunnel-group certenroll webvpn-attributes
authentication aaa
group-alias certenroll enable
```

وفيما يلي ملف تعريف العميل الذي يمكن لصقه في ملف Notepad واستيراده إلى ASA، أو يمكن تكوينه باستخدام Adaptive Security Device Manager (ASDM) مباشرة:

```
<?"xml version="1.0" encoding="UTF-8?>
"/AnyConnectProfile xmlns="http://schemas.xmlsoap.org/encoding>
"xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance
<"xsi:schemaLocation="http://schemas.xmlsoap.org/encoding/ AnyConnectProfile.xsd
<ClientInitialization>
<UseStartBeforeLogon UserControllable="true">false</UseStartBeforeLogon>
<AutomaticCertSelection UserControllable="true">false</AutomaticCertSelection>
<ShowPreConnectMessage>false</ShowPreConnectMessage>
<CertificateStore>All</CertificateStore>
```

<CertificateStoreOverride>false</CertificateStoreOverride>
<ProxySettings>Native</ProxySettings>
<AllowLocalProxyConnections>true</AllowLocalProxyConnections>
<AuthenticationTimeout>12</AuthenticationTimeout>
<AutoConnectOnStart UserControllable="true">false</AutoConnectOnStart>
<MinimizeOnConnect UserControllable="true">true</MinimizeOnConnect>
<LocalLanAccess UserControllable="true">false</LocalLanAccess>
<ClearSmartcardPin UserControllable="true">true</ClearSmartcardPin>
AutoReconnect UserControllable="false">true>
AutoReconnectBehavior UserControllable="false">ReconnectAfterResume>
<AutoReconnectBehavior/>
<AutoReconnect/>
<AutoUpdate UserControllable="false">true</AutoUpdate>
<RSASecurIDIntegration UserControllable="false">Automatic</RSASecurIDIntegration>
<WindowsLogonEnforcement>SingleLocalLogon</WindowsLogonEnforcement>
<WindowsVPNEstablishment>LocalUsersOnly</WindowsVPNEstablishment>
<AutomaticVPNPolicy>false</AutomaticVPNPolicy>
PPPExclusion UserControllable="false">Disable>
<PPPExclusionServerIP UserControllable="false"></PPPExclusionServerIP>
<PPPExclusion/>
<EnableScripting UserControllable="false">false</EnableScripting>

EnableAutomaticServerSelection UserControllable="false">false>
<AutoServerSelectionImprovement>20</AutoServerSelectionImprovement>
<AutoServerSelectionSuspendTime>4</AutoServerSelectionSuspendTime>
<EnableAutomaticServerSelection/>
<RetainVpnOnLogoff>false</RetainVpnOnLogoff>

```
<ClientInitialization/>
```

```
<AnyConnectProfile/>
```

ملاحظة: لم يتم تكوين عنوان URL لمجموعة النفق هذه. هذا مهم لأن SCEP القديم لا يعمل مع عنوان الربط. يجب تحديد مجموعة النفق مع الاسم المستعار الخاص بها. هذا بسبب cisco بق CSCtq74054 id. إذا واجهت مشاكل بسبب URL المجموعة، فقد تحتاج إلى متابعة هذا الخطأ.

تكوين نفق لمصادقة شهادة المستخدم

عند إستلام شهادة المعرف الموقع، يمكن الاتصال بمصادقة الشهادة. ومع ذلك، لم يتم تكوين مجموعة النفق الفعلية التي يتم إستخدامها للاتصال بعد. ويكون هذا التكوين مماثلا للتكوين الخاص بأي ملف تعريف اتصال آخر. هذا المصطلح مرادف لمجموعة النفق ولا يجب الخلط بينه وبين ملف تعريف العميل الذي يستخدم مصادقة الشهادة.

فيما يلي لقطة للتكوين المستخدم لهذا النفق:

```
rtpvpnoutbound6(config)# show run access-l acl_fw-policy

access-list acl_fw-policy standard permit 192.168.1.0 255.255.255.0

rtpvpnoutbound6(config)# show run group-p gp_legacyscep
group-policy gp_legacyscep internal
group-policy gp_legacyscep attributes
vpn-tunnel-protocol ssl-client
split-tunnel-policy tunnelspecified
split-tunnel-network-list value acl_fw-policy
default-domain value cisco.com
webvpn
anyconnect modules value dart

rtpvpnoutbound6(config)# show run tunnel tg_legacyscep
tunnel-group tg_legacyscep type remote-access
tunnel-group tg_legacyscep general-attributes
address-pool ap_fw-policy
default-group-policy gp_legacyscep
tunnel-group tg_legacyscep webvpn-attributes
authentication certificate
```

```
group-alias legacyscep enable
group-url https://rtpvpnoutbound6.cisco.com/legacyscep enable
```

تجديد شهادة المستخدم

عند انتهاء صلاحية شهادة المستخدم أو إبطالها، يفشل Cisco AnyConnect في مصادقة الشهادة. الخيار الوحيد هو إعادة الاتصال بمجموعة نفق تسجيل الشهادة لتشغيل تسجيل SCEP مرة أخرى.

التحقق من الصحة

أستخدم المعلومات المقدمة في هذا القسم للتأكد من أن التكوين لديك يعمل بشكل صحيح.

ملاحظة: نظرا لأنه يجب تنفيذ طريقة SCEP القديمة فقط باستخدام الأجهزة المحمولة، فإن هذا القسم يتعامل فقط مع العملاء كثيري التنقل.

أتمت هذا steps in order to دققت تشكيلك:

1. عند محاولة الاتصال لأول مرة، أدخل اسم مضيف ASA أو عنوان IP.

2. حدد **certenroll**، أو الاسم المستعار للمجموعة الذي قمت بتكوينه في قسم تكوين نفق لاستخدام التسجيل في هذا المستند. أنت بعد ذلك حضضت على username وكلمة، **وال get شهادة** زر يعرض.

3. انقر على زر **الحصول على شهادة**.

إذا قمت بفحص سجلات العميل، فيجب أن يعرض هذا الإخراج:

```
.Information> - Contacting https://rtpvpnoutbound6.cisco.com> [11:23:45:121 06-22-12]
.Warning> - No valid certificates available for authentication> [11:23:45:324 06-22-12]
...Information> - Establishing VPN session> [11:23:51:767 06-22-12]
...Information> - Establishing VPN session> [11:23:51:879 06-22-12]
...Information> - Establishing VPN - Initiating connection> [11:23:51:884 06-22-12]
...Information> - Establishing VPN - Examining system> [11:23:52:066 06-22-12]
...Information> - Establishing VPN - Activating VPN adapter> [11:23:52:069 06-22-12]
...Information> - Establishing VPN - Configuring system> [11:23:52:594 06-22-12]
...Information> - Establishing VPN> [11:23:52:627 06-22-12]
[11:23:52:734 06-22-12]

[11:23:52:764 06-22-12]

[11:23:52:771 06-22-12]

[11:23:55:642 06-22-12]
```

```
[11:24:02:756 06-22-12]
```

وعلى الرغم من أن الرسالة الأخيرة تظهر **خطأ**، إلا أنها تعلم المستخدم بأن هذه الخطوة ضرورية لاستخدام ذلك العميل في محاولة التوصيل التالية، والتي تكون في ملف تعريف الاتصال الثاني الذي تم تكوينه في قسم تكوين نفق لمصادقة شهادة المستخدم في هذا المستند.

معلومات ذات صلة

- لم يتم بدء تشغيل CSCtq74054 SCEP عند إستخدام URL (الاسم المستعار لمجموعة النفق/asa-IP)
- الدعم التقني والمستندات

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).