Vorhandenes SCEP mit Verwendung des CLI-Konfigurationsbeispiels

Inhalt

Einführung

Dieses Dokument beschreibt die Verwendung des Legacy Simple Certificate Enrollment Protocol (SCEP) auf der Cisco Adaptive Security Appliance (ASA).

> **Vorsicht**: Ab Cisco AnyConnect Release 3.0 sollte diese Methode nicht mehr verwendet werden. Das war zuvor nötig, weil Mobilgeräte nicht über den 3.x-Client verfügten, aber sowohl Android- als auch iPhones jetzt Unterstützung für den SCEP-Proxy haben, der stattdessen verwendet werden sollte. Nur in Fällen, in denen diese aufgrund der ASA nicht unterstützt wird, sollten Sie Legacy SCEP konfigurieren. Selbst in diesen Fällen wird jedoch ein ASA-Upgrade empfohlen.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse von Legacy SCEP verfügen.

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardwareversionen beschränkt.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Hintergrundinformationen

Das SCEP ist ein Protokoll, das entwickelt wurde, um die Verteilung und den Widerruf digitaler Zertifikate so skalierbar wie möglich zu machen. Die Idee ist, dass jeder Standard-Netzwerkbenutzer in der Lage sein sollte, ein digitales Zertifikat elektronisch anzufordern, wobei nur sehr wenig Eingriffe seitens der Netzwerkadministratoren erforderlich sind. Bei VPN-Bereitstellungen, die eine Zertifikatsauthentifizierung mit dem Unternehmen, der Zertifizierungsstelle (Certificate Authority, CA) oder einer Drittanbieter-Zertifizierungsstelle erfordern, die SCEP unterstützt, können Benutzer jetzt signierte Zertifikate von den Client-Computern anfordern, ohne dass die Netzwerkadministratoren involviert sind.

> **Hinweis**: Wenn Sie die ASA als CA-Server konfigurieren möchten, ist SCEP nicht die richtige Protokollmethode. Weitere Informationen finden Sie im Abschnitt Lokale Zertifizierungsstellen im Cisco Dokument **Konfigurieren digitaler Zertifikate**.

Ab ASA Version 8.3 gibt es zwei unterstützte Methoden für SCEP:

- Die ältere Methode, die Legacy SCEP genannt wird, wird in diesem Dokument behandelt.
- Die SCEP-Proxy-Methode ist die neuere der beiden Methoden, bei der die ASA die Zertifikatsanmeldungsanforderung im Namen des Clients anfordert. Dieser Prozess ist übersichtlicher, da er keine zusätzliche Tunnelgruppe erfordert und außerdem sicherer ist. Der Nachteil ist jedoch, dass der SCEP-Proxy nur mit Cisco AnyConnect Release 3.x funktioniert. Dies bedeutet, dass die aktuelle AnyConnect-Client-Version für Mobilgeräte keinen SCEP-Proxy unterstützt.

Konfigurieren

Dieser Abschnitt enthält Informationen, die Sie zum Konfigurieren der Legacy-SCEP-Protokollmethode verwenden können.

> **Hinweis**: Verwenden Sie das Command Lookup Tool (nur registrierte Kunden), um weitere Informationen zu den in diesem Abschnitt verwendeten Befehlen zu erhalten.

Bei Verwendung von Legacy-SCEP sind folgende wichtige Hinweise zu beachten:

- Nachdem der Client das signierte Zertifikat erhalten hat, sollte die ASA die Zertifizierungsstelle, die das Zertifikat signiert hat, erkennen, bevor der Client authentifiziert werden kann. Daher müssen Sie sicherstellen, dass die ASA auch beim CA-Server registriert wird. Der Registrierungsprozess für die ASA sollte der erste Schritt sein, da er Folgendes

gewährleistet:

Die CA ist korrekt konfiguriert und kann Zertifikate über SCEP ausgeben, wenn Sie die URL-Anmeldungsmethode verwenden.

Die ASA kann mit der CA kommunizieren. Wenn der Client das nicht kann, liegt daher ein Problem zwischen dem Client und der ASA vor.

- Beim ersten Verbindungsversuch wird kein signiertes Zertifikat ausgegeben. Es muss eine weitere Option zur Authentifizierung des Clients vorhanden sein.

- Bei der Zertifikatregistrierung übernimmt die ASA keine Rolle. Er dient lediglich als VPN-Aggregator, sodass der Client einen Tunnel erstellen kann, um das signierte Zertifikat sicher zu erhalten. Wenn der Tunnel eingerichtet ist, muss der Client in der Lage sein, den CA-Server zu erreichen. Andernfalls kann er sich nicht registrieren.

Registrieren Sie die ASA

Die ASA-Registrierung ist relativ einfach und erfordert keine neuen Informationen. Weitere Informationen zur Registrierung der Cisco ASA bei einer CA mithilfe von SCEP finden Sie im Dokument Enrolling the Cisco ASA to a CA.

Tunnel für die Verwendung bei der Registrierung konfigurieren

Wie bereits erwähnt, muss für den Client ein sicherer Tunnel mit der ASA mithilfe einer anderen Authentifizierungsmethode erstellt werden, damit er ein Zertifikat erhalten kann. Hierzu müssen Sie eine Tunnelgruppe konfigurieren, die nur für den ersten Verbindungsversuch verwendet wird, wenn eine Zertifikatsanforderung erstellt wird. Im Folgenden finden Sie einen Snapshot der verwendeten Konfiguration, die diese Tunnelgruppe definiert (die wichtigen Zeilen werden in ***Fettschrift kursiv*** angezeigt):

```
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
```

Das folgende Clientprofil kann entweder in eine Notepad-Datei eingefügt und in die ASA importiert werden oder direkt mit dem Adaptive Security Device Manager (ASDM) konfiguriert werden:

```
<?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>
```

Hinweis: Für diese Tunnelgruppe ist keine Gruppen-URL konfiguriert. Dies ist wichtig, da das Legacy-SCEP nicht mit der URL funktioniert. Sie müssen die Tunnelgruppe mit ihrem Alias auswählen. Grund hierfür ist die Cisco Bug-ID CSCtq74054. Wenn Sie Probleme aufgrund der group-url haben, müssen Sie möglicherweise diesen Fehler beheben.

Tunnel für Benutzerzertifikatauthentifizierung konfigurieren

Wenn das signierte ID-Zertifikat empfangen wird, ist eine Verbindung mit der

Zertifikatsauthentifizierung möglich. Die tatsächliche Tunnelgruppe, die für die Verbindung verwendet wird, wurde jedoch noch nicht konfiguriert. Diese Konfiguration ähnelt der Konfiguration für jedes andere Verbindungsprofil. Dieser Begriff ist gleichbedeutend mit Tunnelgruppe und darf nicht mit Clientprofil verwechselt werden, das die Zertifikatauthentifizierung verwendet.

Im Folgenden finden Sie einen Snapshot der Konfiguration, die für diesen Tunnel verwendet wird:

```
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
```

Verlängern des Benutzerzertifikats

Wenn das Benutzerzertifikat abläuft oder widerrufen wird, schlägt Cisco AnyConnect die Zertifikatauthentifizierung fehl. Die einzige Option besteht darin, erneut eine Verbindung zur Tunnelgruppe für die Zertifikatsregistrierung herzustellen, um die SCEP-Registrierung erneut auszulösen.

Überprüfen

Verwenden Sie die Informationen in diesem Abschnitt, um zu überprüfen, ob Ihre Konfiguration ordnungsgemäß funktioniert.

> **Hinweis**: Da die Legacy-SCEP-Methode nur mit mobilen Geräten implementiert werden sollte, werden in diesem Abschnitt nur mobile Clients behandelt.

Gehen Sie wie folgt vor, um Ihre Konfiguration zu überprüfen:

1. Wenn Sie zum ersten Mal versuchen, eine Verbindung herzustellen, geben Sie den ASA-Hostnamen oder die IP-Adresse ein.

2. Wählen Sie **certenroll** oder den Gruppen-Alias aus, den Sie im Abschnitt Tunnel für die

Nutzung der Registrierung konfigurieren konfiguriert haben. Sie werden dann zur Eingabe eines Benutzernamens und eines Kennworts aufgefordert, und die Schaltfläche **Zertifikat abrufen** wird angezeigt.

3. Klicken Sie auf die Schaltfläche **Zertifikat abrufen**.

Wenn Sie die Client-Protokolle überprüfen, sollte diese Ausgabe Folgendes anzeigen:

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

Obwohl die letzte Meldung einen **Fehler** anzeigt, muss der Benutzer lediglich darüber informiert werden, dass dieser Schritt erforderlich ist, damit dieser Client für den nächsten Verbindungsversuch verwendet wird. Dies ist im zweiten Verbindungsprofil enthalten, das im Abschnitt Konfiguration eines Tunnels für die Authentifizierung von Benutzerzertifikaten in diesem Dokument konfiguriert ist.

Zugehörige Informationen

- CSCtq74054 SCEP wird bei Verwendung einer URL (Alias für eine asa-IP/Tunnelgruppe) nicht initiiert
- Technischer Support und Dokumentation