Verouderde SCEP met gebruik van het CLI-configuratievoorbeeld

Inhoud

Inleiding

Dit document beschrijft het gebruik van Verouderde Simple certificaatinschrijving Protocol (SCEP) op Cisco adaptieve security applicatie (ASA).

> **Voorzichtig:** Aangezien Cisco AnyConnect release 3.0 wordt gebruikt, mag deze methode niet worden gebruikt. Het was voorheen nodig omdat mobiele apparaten niet de 3.x-client hadden, maar zowel Android als iPhones hebben nu ondersteuning voor SCEP-proxy, die in plaats daarvan gebruikt zou moeten worden. Alleen in gevallen waarin deze niet vanwege de ASA wordt ondersteund, dient u Legacy SCEP te configureren. Maar zelfs in deze gevallen is een ASA-upgrade de aanbevolen optie.

Voorwaarden

Vereisten

Cisco raadt u aan kennis te hebben van Verouderde SCEP.

Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardware-versies.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Achtergrondinformatie

Het SCEP is een protocol dat is ontworpen om de distributie en herroeping van digitale certificaten zo schaalbaar mogelijk te maken. Het idee is dat elke standaardnetwerkgebruiker elektronisch een digitaal certificaat kan aanvragen met zeer weinig tussenkomst van netwerkbeheerders. Voor VPN-implementaties die certificatie van certificaten nodig hebben met de onderneming, certificaatautoriteit (CA) of een derde partij CA die SCEP ondersteunt, kunnen gebruikers nu om ondertekende certificaten van de clientmachines vragen zonder de betrokkenheid van de netwerkbeheerders.

> Opmerking: Als u de ASA als de CA server wilt configureren is SCEP niet de juiste protocolmethode. Raadpleeg in plaats daarvan het gedeelte Local CA van het **Cisco**-document dat **digitale certificaten** vormt.

Sinds ASA release 8.3 zijn er twee ondersteunde methoden voor SCEP:

- De oudere methode, genaamd Legacy SCEP, wordt in dit document besproken.
- De SCEP-proxymethode is de nieuwere van de twee methoden, waarbij de ASA het verzoek om inschrijving van certificaten namens de cliënt aanvult. Dit proces is schoner omdat het geen extra tunnelgroep nodig heeft en ook veiliger is. Maar de terugbetaling is dat de volmacht van SCEP slechts met Cisco AnyConnect release 3.x werkt. Dit betekent dat de huidige AnyConnect-clientversie voor mobiele apparaten geen SCEP-proxy ondersteunt.

Configureren

Deze sectie verschaft informatie die u kunt gebruiken om de bestaande SCEP-protocolmethode te configureren.

> Opmerking: Gebruik de Command Lookup Tool (alleen voor geregistreerde gebruikers) voor meer informatie over de opdrachten die in deze sectie worden gebruikt.

Hier zijn een paar belangrijke opmerkingen die in gedachten moeten worden gehouden wanneer het SCEP met de Legacy wordt gebruikt:

- Nadat de klant het ondertekende certificaat heeft ontvangen, moet de ASA de CA erkennen die het certificaat heeft ondertekend voordat deze de client kan authenticeren. Daarom moet u ervoor zorgen dat de ASA ook bij de CA server inschrijft. Het inschrijvingsproces voor de ASA moet de eerste stap zijn omdat het garandeert dat:

CA is correct ingesteld en kan certificaten via SCEP uitgeven als u de URL inschrijvingsmethode gebruikt.

De ASA kan communiceren met de CA. Als de cliënt dat niet kan, dan is er een probleem tussen de cliënt en de ASA.

- Wanneer de eerste verbindingspoging is gedaan, is er geen ondertekend certificaat. Er moet een andere optie zijn die kan worden gebruikt om de client voor authentiek te verklaren.

- In het inlogproces van certificaten speelt de ASA geen rol. Het dient alleen als VPN-aggregator zodat de client een tunnel kan bouwen om op een veilige manier het ondertekende certificaat te verkrijgen. Wanneer de tunnel wordt gevestigd, moet de cliënt de server van CA kunnen bereiken. Anders kan zij zich niet aanmelden.

ASA invoeren

Het ASA-inschrijvingsproces is relatief eenvoudig en vereist geen nieuwe informatie. Raadpleeg de Invoegen van Cisco ASA aan een CA Gebruik van SCEP document voor meer informatie over het inschrijven van de ASA aan een CA van derden.

Een tunneleffect instellen voor inschrijvingsgebruik

Zoals eerder vermeld, moet een beveiligde tunnel met de ASA worden aangelegd met behulp van een andere methode voor de echtheidscontrole, zodat de klant een certificaat kan verkrijgen. Om dit te doen, moet u één tunnel-groep vormen die slechts voor de eerste verbindingspoging wordt gebruikt wanneer een certificaatverzoek wordt gedaan. Hier is een momentopname van de configuratie die wordt gebruikt, die deze tunnelgroep definieert (de belangrijke lijnen worden weergegeven in ***vet-cursief***):

```
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
```

Hier is het clientprofiel dat in een Kladblok-bestand kan worden geplakt en naar de ASA kan worden geïmporteerd. Dit profiel kan ook worden ingesteld met de Adaptieve Security Devices Manager (ASDM):

```
<?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>
```

> Opmerking: Een groep-url wordt niet ingesteld voor deze tunnelgroep. Dit is belangrijk omdat Legacy SCEP niet werkt met de URL. Je moet de tunnelgroep selecteren met zijn alias. Dit komt door Cisco bug-ID CSCtq74054. Als u problemen ondervindt vanwege de groep-URL, moet u dit bug misschien opvolgen.

Een Tunnel configureren voor verificatie van gebruikerscertificaten

Wanneer het ondertekende ID-certificaat wordt ontvangen, is verbinding met certificatie mogelijk. De eigenlijke tunnelgroep die wordt gebruikt om verbinding te maken, is echter nog niet ingesteld. Deze configuratie is vergelijkbaar met de configuratie voor elk ander aansluitingsprofiel. Deze term

is synoniem met tunnelgroep en mag niet worden verward met clientprofiel, dat certificatie van certificaten gebruikt.

Hier volgt een momentopname van de configuratie die voor deze tunnel wordt gebruikt:

```
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
```

Verleng het gebruikerscertificaat

Wanneer het gebruikerscertificaat verloopt of wordt ingetrokken, voldoet Cisco AnyConnect niet aan de certificatie. De enige optie is om opnieuw aan te sluiten op de tunnelgroep van het certificaat om de SCEP inschrijving opnieuw te starten.

Verifiëren

Gebruik de informatie in dit gedeelte om te bevestigen dat uw configuratie correct werkt.

> Opmerking: Aangezien de verouderde SCEP-methode alleen met het gebruik van mobiele apparatuur mag worden toegepast, is deze paragraaf alleen van toepassing op mobiele klanten.

Volg deze stappen om de configuratie van uw computer te controleren:

1. Wanneer u voor het eerst probeert aan te sluiten, voer u het ASA hostname of IP adres in.

2. Selecteer **certenroll**, of de groepsalias die u in het Configureren van een Tunnel voor het vak Gebruik van dit document hebt ingesteld. U wordt dan gevraagd een gebruikersnaam en wachtwoord in te voeren, en de knop **verkrijgen certificaat** wordt weergegeven.

3. Klik op de knop **Certificaat verkrijgen**.

Als u uw clientbestanden controleert, dient deze uitvoer weer te geven:

```
[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]
```

Hoewel het laatste bericht een **fout** toont, is het alleen om de gebruiker op de hoogte te stellen dat deze stap nodig is om die client te kunnen gebruiken voor de volgende verbindingspoging. Dit is in het tweede verbindingsprofiel dat is ingesteld in het gedeelte Configuratie van een Tunnel voor de verificatie van het gebruikerscertificaat van dit document.

Gerelateerde informatie

- CSCtq74054 SCEP wordt niet geïnitieerd bij gebruik van een URL (als een IP/tunnelgroep alias)
- Technische ondersteuning en documentatie