CLI 컨피그레이션 사용이 가능한 레거시 SCEP 예

목차

[소개](#)
[사전 요구 사항](#)
[요구 사항](#)
[사용되는 구성 요소](#)
[배경 정보](#)
[구성](#)
[ASA 등록](#)
[등록 용도로 터널 구성](#)
[사용자 인증서 인증을 위한 터널 구성](#)
[사용자 인증서 갱신](#)
[다음을 확인합니다.](#)
[관련 정보](#)

소개

이 문서에서는 Cisco ASA(Adaptive Security Appliance)에서 레거시 SCEP(Simple Certificate Enrollment Protocol)를 사용하는 방법에 대해 설명합니다.

> **주의:**Cisco AnyConnect 릴리스 3.0부터 이 방법을 사용하면 안 됩니다.이전에는 모바일 디바이스에 3.x 클라이언트가 없지만 Android와 iPhone 모두 이제 SCEP 프록시를 지원하므로 대신 사용해야 했습니다.ASA로 인해 지원되지 않는 경우에만 레거시 SCEP를 구성해야 합니다.그러나 이러한 경우에도 ASA 업그레이드가 권장됩니다.

사전 요구 사항

요구 사항

레거시 SCEP에 대한 지식이 있는 것이 좋습니다.

사용되는 구성 요소

이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

SCEP는 디지털 인증서의 배포 및 취소를 가능한 한 확장 가능하도록 설계된 프로토콜입니다.표준 네트워크 사용자는 네트워크 관리자의 개입이 거의 없는 상태에서 디지털 인증서를 전자적으로 요청할 수 있어야 합니다.엔터프라이즈, CA(Certificate Authority) 또는 SCEP를 지원하는 서드파티 CA와의 인증서 인증이 필요한 VPN 구축의 경우 사용자는 이제 네트워크 관리자의 개입 없이 클라이언트 시스템에서 서명된 인증서를 요청할 수 있습니다.

> **참고:**ASA를 CA 서버로 구성하려면 SCEP가 올바른 프로토콜 방법이 아닙니다.대신 디지털 인증서 구성 Cisco 문서의 로컬 CA 섹션을 참조하십시오.

ASA 릴리스 8.3부터는 SCEP에 대해 다음 두 가지 방법이 지원됩니다.

- 이 문서에서는 레거시 SCEP라는 이전 방법에 대해 설명합니다.
- SCEP 프록시 방법은 두 가지 방법 중 최신 방법입니다. 여기서 ASA는 클라이언트를 대신하여 인증서 등록 요청을 프록시합니다.이 프로세스는 추가 터널 그룹이 필요하지 않으며 더 안전하기 때문에 더 간단합니다.그러나 단점은 SCEP 프록시가 Cisco AnyConnect 릴리스 3.x에서만 작동한다는 것입니다.즉, 모바일 디바이스용 현재 AnyConnect 클라이언트 버전이 SCEP 프록시를 지원하지 않습니다.

구성

이 섹션에서는 레거시 SCEP 프로토콜 방법을 구성하는 데 사용할 수 있는 정보를 제공합니다.

> **참고:**이 섹션에 사용된 명령에 대한 자세한 내용을 보려면 Command Lookup Tool(등록된 고객만 해당)을 사용합니다.

다음은 레거시 SCEP를 사용할 때 기억해야 할 몇 가지 중요한 참고 사항입니다.

- 클라이언트가 서명된 인증서를 수신한 후 ASA는 클라이언트를 인증하기 전에 인증서를 서명한 CA를 인식해야 합니다.따라서 ASA가 CA 서버와 함께 등록되도록 해야 합니다.ASA의 등록 프로세스는 다음 사항을 보장하므로 첫 번째 단계가 되어야 합니다.

  URL 등록 방법을 사용하는 경우 CA가 올바르게 구성되어 SCEP를 통해 인증서를 발급할 수 있습니다.

  ASA는 CA와 통신할 수 있습니다.따라서 클라이언트가 할 수 없는 경우 클라이언트와 ASA 사이에 문제가 있습니다.
- 첫 번째 연결을 시도하면 서명된 인증서가 없습니다.클라이언트를 인증하려면 다른 옵션을 사용할 수 있어야 합니다.

- 인증서 등록 프로세스에서 ASA는 역할을 수행하지 않습니다.클라이언트가 서명된 인증서를 안전하게 얻기 위해 터널을 구축할 수 있도록 VPN 집선자 역할만 합니다.터널이 설정되면 클라이언트가 CA 서버에 연결할 수 있어야 합니다.그렇지 않으면 등록할 수 없습니다.

ASA 등록

ASA 등록 프로세스는 비교적 간단하며 새 정보가 필요하지 않습니다. ASA를 타사 CA에 등록하는 방법에 대한 자세한 내용은 Cisco ASA를 SCEP를 사용하여 CA에 등록 문서를 참조하십시오.

등록 용도로 터널 구성

앞서 언급한 대로 클라이언트가 인증서를 얻으려면 다른 인증 방법을 통해 ASA를 사용하여 보안 터널을 구축해야 합니다.이렇게 하려면 인증서 요청이 있을 때 첫 번째 연결 시도에만 사용되는 하나의 터널 그룹을 구성해야 합니다.다음은 이 터널 그룹을 정의하는 데 사용되는 컨피그레이션의 스냅샷입니다(중요한 줄은 ***굵은 기울임꼴***로 표시됨).

```
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
```

다음은 메모장 파일에 붙여넣어 ASA로 가져오거나 ASDM(Adaptive Security Device Manager)을 사용하여 직접 구성할 수 있는 클라이언트 프로파일입니다.

```
<?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>
```

> **참고:**이 터널 그룹에 대해 group-url이 구성되지 않았습니다.레거시 SCEP가 URL에서 작동하지 않기 때문에 이는 중요합니다.별칭이 있는 터널 그룹을 선택해야 합니다.이는 Cisco 버그 ID CSCtq74054로 인해 발생합니다. group-url로 인해 문제가 발생하는 경우 이 버그에 대한 후속 조치가 필요할 수 있습니다.

사용자 인증서 인증을 위한 터널 구성

서명된 ID 인증서를 받으면 인증서 인증과 연결할 수 있습니다. 그러나 연결에 사용되는 실제 터널 그룹은 아직 구성되지 않았습니다.이 컨피그레이션은 다른 연결 프로파일에 대한 컨피그레이션과 유사합니다.이 용어는 터널 그룹과 동의하며 인증서 인증을 사용하는 클라이언트 프로파일과 혼동되지 않습니다.

다음은 이 터널에 사용되는 컨피그레이션의 스냅샷입니다.

```
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
```

사용자 인증서 갱신

사용자 인증서가 만료되거나 취소되면 Cisco AnyConnect에서 인증서 인증에 실패합니다.유일한 옵션은 SCEP 등록을 다시 트리거하기 위해 인증서 등록 터널 그룹에 다시 연결하는 것입니다.

다음을 확인합니다.

이 섹션에 제공된 정보를 사용하여 컨피그레이션이 제대로 작동하는지 확인합니다.

> **참고:**레거시 SCEP 방법은 모바일 디바이스를 사용하는 경우에만 구현해야 하므로 이 섹션에서는 모바일 클라이언트만 다룹니다.

구성을 확인하려면 다음 단계를 완료하십시오.

1. 처음 연결을 시도할 때 ASA 호스트 이름 또는 IP 주소를 입력합니다.
2. **certenroll** 또는 이 문서의 Configure a Tunnel for Enrollment Use 섹션에서 구성한 그룹 별칭을 선택합니다.그러면 사용자 이름과 비밀번호를 입력하라는 프롬프트가 표시되고 **인증서 가져오기** 버튼이 표시됩니다.
3. **인증서 가져오기** 버튼을 클릭합니다.

클라이언트 로그를 확인하는 경우 이 출력에 다음이 표시됩니다.

```
[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]
```

마지막 메시지에 **오류**가 표시되더라도 이 단계는 이 문서의 사용자 인증서 인증을 위한 터널 구성 섹션에 구성된 두 번째 연결 프로파일에 있는 다음 연결 시도에 해당 클라이언트를 사용하려면 이 단계가 필요하다는 것을 사용자에게 알리는 것입니다.

관련 정보

- URL을 사용할 때 CSCtq74054 SCEP가 시작되지 않음(asa-IP/tunnel-group 별칭)
- 기술 지원 및 문서