AnyConnect 기능으로 Phone VPN용 CUCM의 ASA 인증서 업데이트

목차

소개

이 문서에서는 전화 서비스 중단을 방지하기 위해 AnyConnect 기능을 사용하여 Cisco VPN(Unified Communications Manager)에서 CUCM(Adaptive Security Appliance) 인증서를 AnyConnect 기능으로 업데이트하는 올바른 프로세스에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- AnyConnect 기능이 있는 전화 VPN.
- ASA 및 CUCM 인증서.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco Unified Communications Manager 10.5.2.15900-8.
- Cisco Adaptive Security Appliance Software 버전 9.8(2)20.
- Cisco IP Phone CP-8841.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 이해해야 합니다.

배경 정보

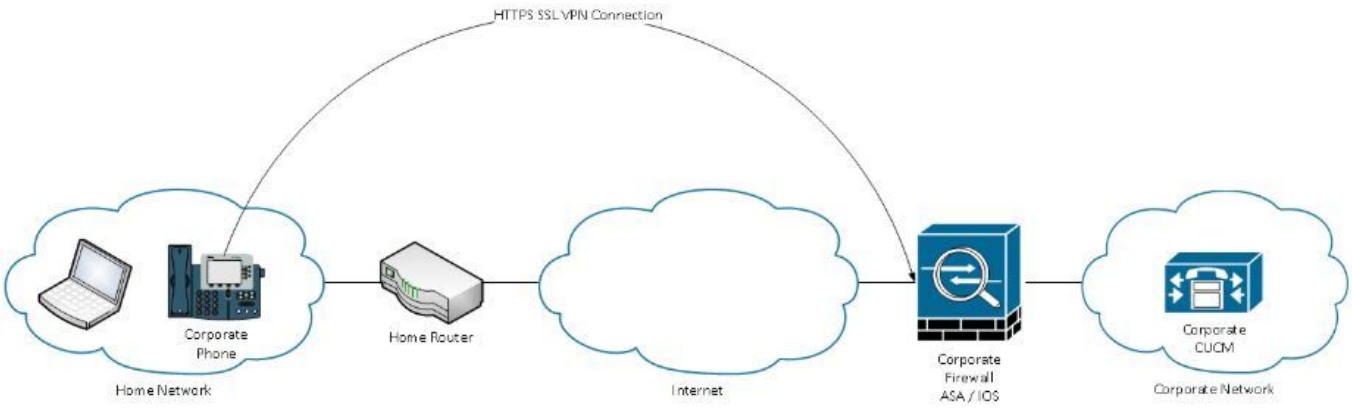
AnyConnect가 포함된 Phone VPN 기능을 사용하면 VPN 연결을 통해 전화 서비스를 프로비저닝할 수 있습니다.

전화기가 VPN을 위해 준비되기 전에 먼저 내부 네트워크에서 프로비저닝되어야 합니다.이렇게 하려면 CUCM TFTP(Trivial file transfer Protocol) 서버에 직접 액세스해야 합니다.

ASA가 완전히 구성된 후 첫 번째 단계는 ASA HTTPS(Hypertext Transfer Protocol Secure) 인증서를 가져와 CUCM 서버에 Phone-VPN-trust로 업로드한 다음 CUCM의 올바른 VPN 게이트웨이에 할당하는 것입니다. 이렇게 하면 CUCM 서버에서 ASA에 연결하는 방법을 알려주는 IP 전화 구성 파일을 작성할 수 있습니다.

네트워크 외부로 이동하여 VPN 기능을 사용하려면 먼저 네트워크 내에서 전화기를 프로비저닝해야 합니다. 전화기가 내부적으로 프로비저닝되면 VPN 액세스를 위해 외부 네트워크로 이동할 수 있습니다.

전화기가 HTTPS를 통해 TCP 포트 443에서 ASA에 연결됩니다.ASA는 구성된 인증서로 다시 응답하고 제공된 인증서를 확인합니다.



VPN Phones 서비스 중단 없이 ASA 인증서를 업데이트하는 방법

예를 들어 ASA 인증서를 변경해야 하는 경우도 있습니다.

인증서가 곧 만료됩니다.

인증서는 서드파티 서명 및 CA(Certificate Authority) 변경 등

VPN with AnyConnect를 통해 CUCM에 연결된 전화기의 서비스 중단을 방지하기 위해 몇 가지 단계를 수행해야 합니다.

> **주의:**단계를 수행하지 않으면 외부 네트워크에 구축하기 전에 내부 네트워크에서 전화기를 다시 프로비저닝해야 합니다.

1단계. 새 ASA 인증서를 생성하지만 아직 인터페이스에 적용하지 않습니다.

인증서는 자체 서명 또는 CA 서명 될 수 있습니다.

> **참고:**ASA 인증서에 대한 자세한 내용은 디지털 인증서 구성을 참조하십시오.

2단계. CUCM의 해당 인증서를 CUCM 게시자의 전화 VPN 트러스트로 업로드합니다.

Call Manager에 로그인하여 Unified **OS Administration(Unified OS 관리) > Security(보안) > Certificate Management(인증서 관리) > Upload Certificate(인증서 업로드) > Select Phone-VPN-trust(Phone-VPN-trust 선택)로 이동합니다.**

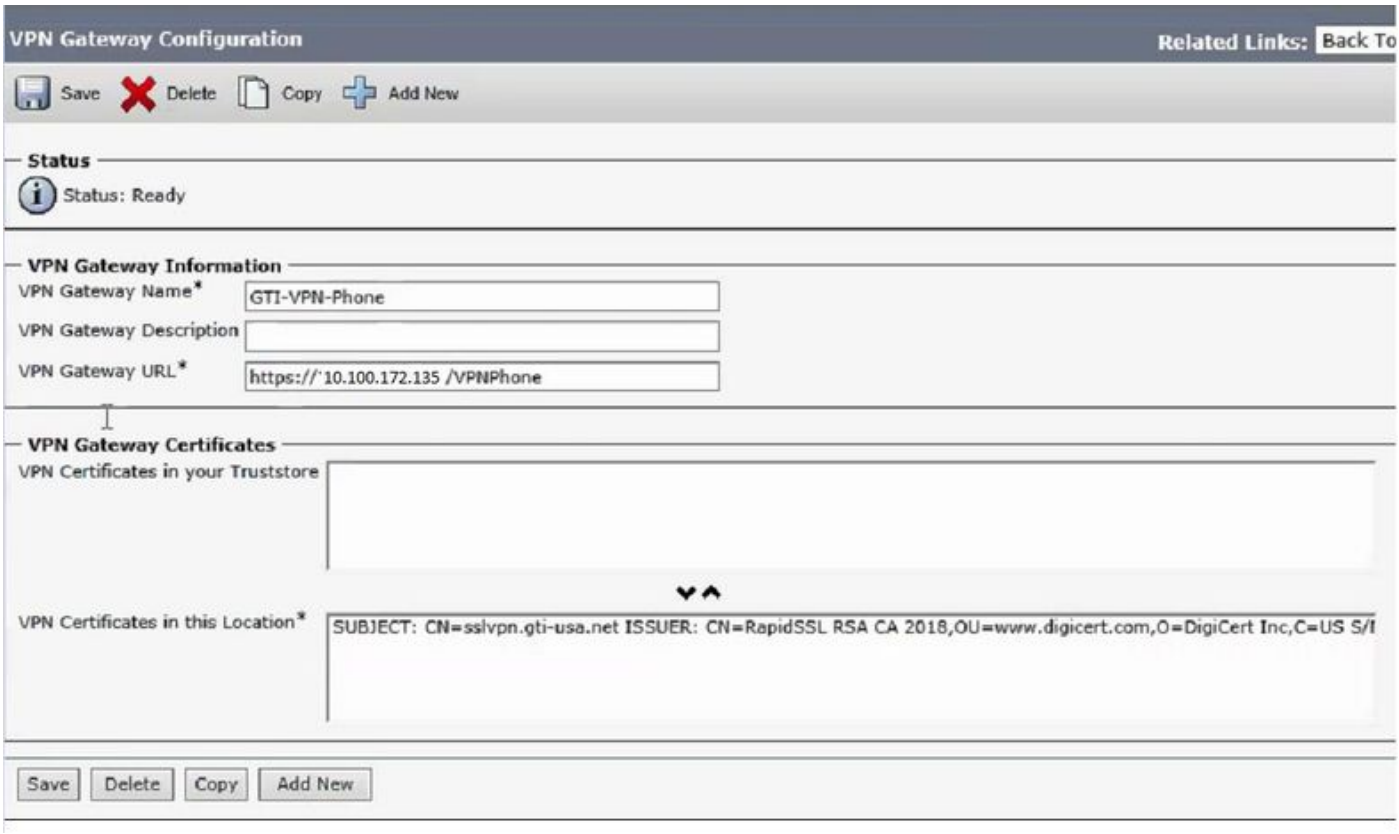
루트 및 중간 인증서가 이미 CUCM에 업로드된 경우 권장 사항으로 전체 인증서 체인을 업로드합니다. 다음 단계로 이동합니다.

> **주의:**이전 ID 인증서와 새 CN이 동일한 경우 새 인증서가 이전 인증서를 덮어쓰지 않도록 버그 CSCuh19734에 대한 해결 방법을 따라야 합니다.이렇게 하면 새 인증서가 Phone VPN Gateway 컨피그레이션의 데이터베이스에 있지만 기존 인증서를 덮어쓰지 않습니다.

3단계. VPN 게이트웨이에서 두 인증서(이전 인증서 및 새 인증서)를 모두 선택합니다.

Cisco Unified **CM Administration(Cisco Unified CM 관리) > Advanced Features(고급 기능) > VPN > VPN Gateway(VPN 게이트웨이)로 이동합니다.**

이 Location(위치) 필드의 VPN Certificates(VPN 인증서)에 두 인증서가 모두 있는지 확인합니다.



4단계. VPN 그룹, 프로파일 및 일반 전화기 프로파일이 올바르게 설정되었는지 확인합니다.

5단계. 전화기를 재설정합니다.

이 단계에서는 전화기가 새 컨피그레이션 설정을 다운로드하고 전화기에 두 인증서 해시가 모두 있으므로 이전 인증서와 새 인증서를 신뢰할 수 있습니다.

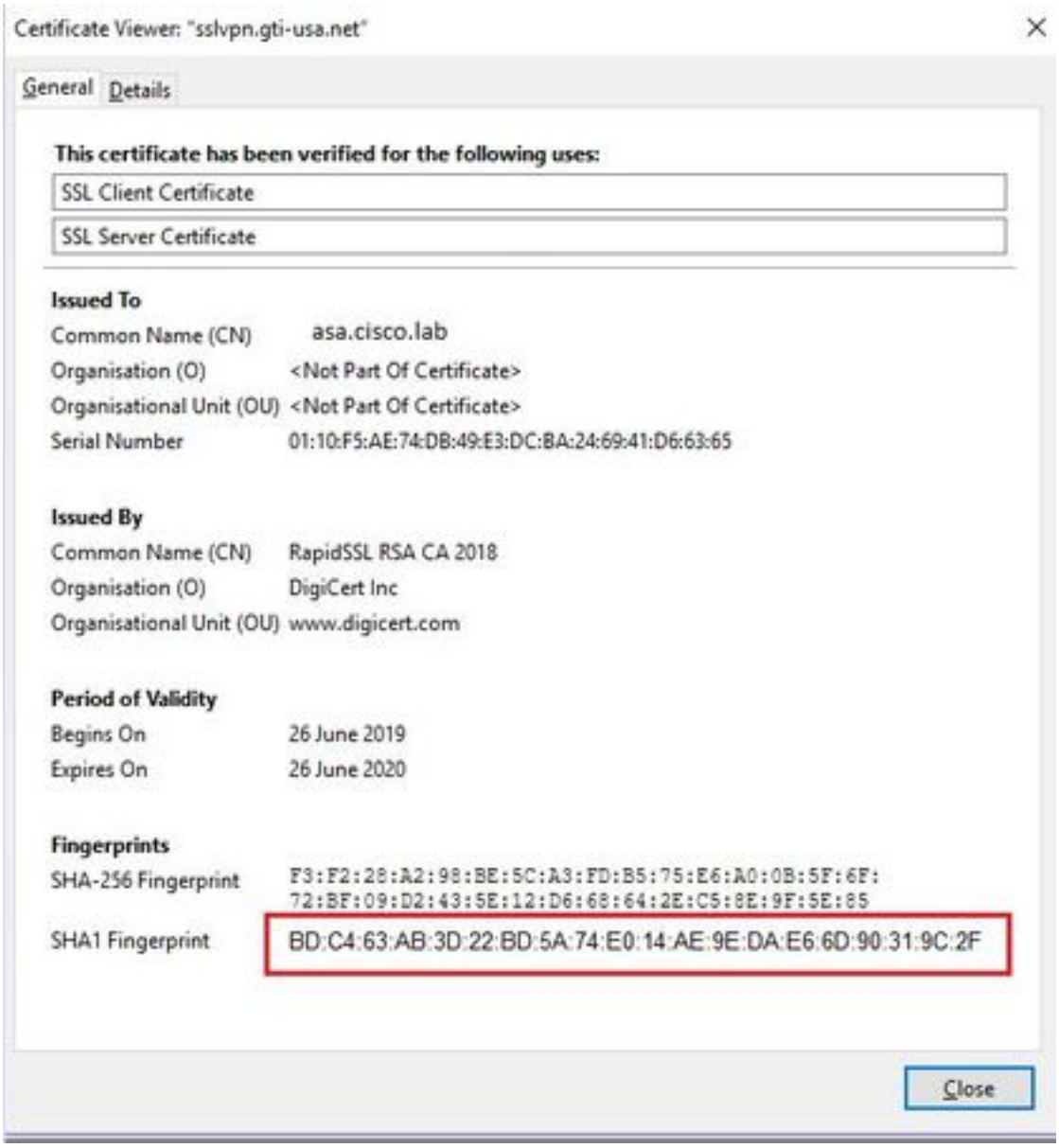
6단계. ASA 인터페이스에 새 인증서를 적용합니다.

인증서가 ASA 인터페이스에 적용되면 이전 단계의 두 인증서 해시가 모두 있으므로 전화기는 해당 새 인증서를 신뢰해야 합니다.

다음을 확인합니다.

이 섹션을 사용하여 단계를 올바르게 수행했는지 확인합니다.

1단계. 이전 및 새 ASA 인증서를 열고 SHA-1 핑거프린트를 기록합니다.



2단계. VPN을 통해 연결해야 하는 전화기를 선택하고 해당 컨피그레이션 파일을 수집합니다.

> **참고:**전화 컨피그레이션 파일을 수집하는 방법에 대한 자세한 내용은 CUCM에서 전화기의 컨피그레이션 파일을 얻는 두 가지 방법을 참조하십시오.

3단계. 컨피그레이션 파일이 있으면 다음 섹션을 찾습니다.

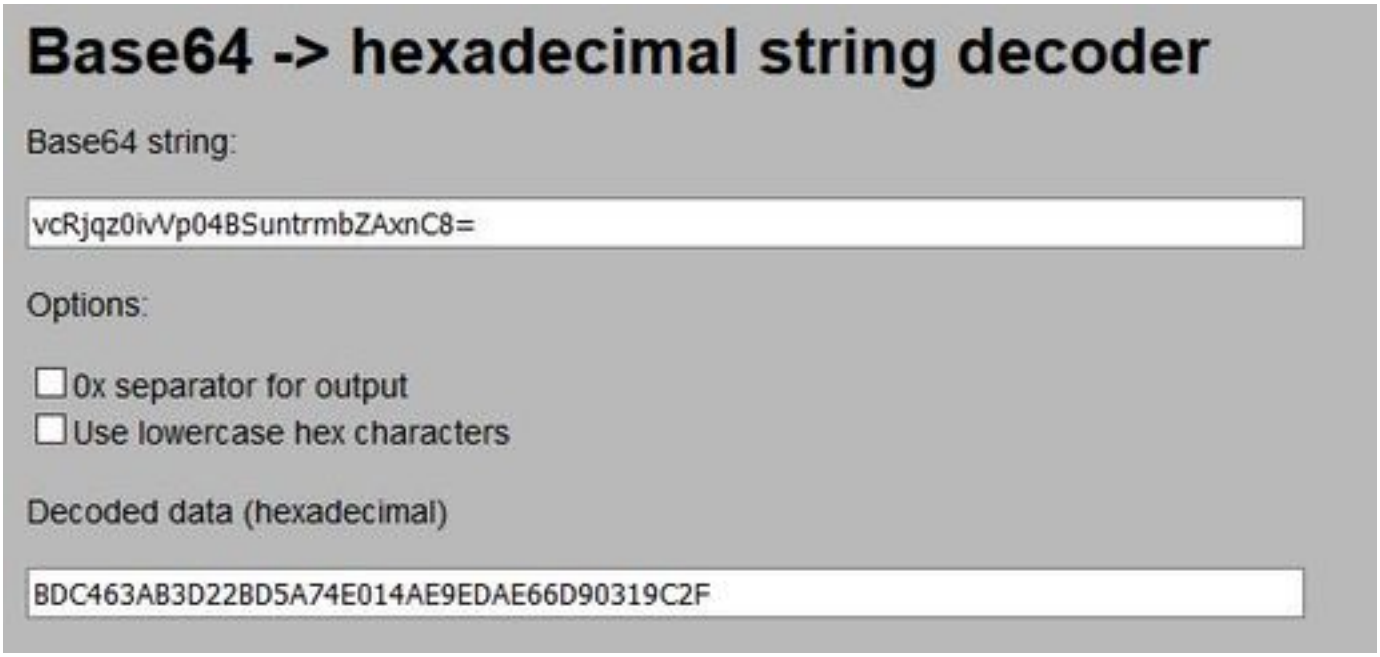
```
<vpnGroup>
<mtu>1290</mtu>
<failConnectTime>30</failConnectTime>
<authMethod>2</authMethod>
<pswdPersistent>0</pswdPersistent>
<autoNetDetect>1</autoNetDetect>
```

```
<enableHostIDCheck>0</enableHostIDCheck>
<addresses>
<url1> https://radc.cgsinc.com/Cisco_VOIP_VPN</url1>;
</addresses>
<credentials>
<hashAlg>0</hashAlg>




        </credentials>
</vpnGroup>
```

4단계. 컨피그레이션 파일의 해시는 Base 64 형식으로 인쇄되고 ASA 인증서는 16진수 형식으로 인쇄되므로 Base 64에서 16진수로 디코더를 사용하여 해시된(전화 및 ASA) 모두 일치하는지 확인할 수 있습니다.



관련 정보

AnyConnect VPN Phone 기능에 대한 자세한 내용은 다음을 참조하십시오.

- **ASA에서 인증서 인증을 사용하여 AnyConnect VPN Phone을 구성합니다.**

https://www.cisco.com/c/en/us/support/docs/unified-communications/unified-communications-manager-callmanager/115785-anyconnect-vpn-00.html