SSLVPN with IP Phones 컨피그레이션 예

목차

소개

이 문서에서는 WebVPN이라고도 하는 SSL VPN(Secure Sockets Layer VPN)을 통해 IP 전화기를 구성하는 방법에 대해 설명합니다.이 솔루션에서는 두 개의 Cisco Unified Communications Manager(CallManager) 및 세 가지 유형의 인증서를 사용합니다.통화 관리자는 다음과 같습니다.

- Cisco CUCM(Unified Communications Manager)
- Cisco Unified Communications Manager Express(Cisco Unified CME)

인증서 유형은 다음과 같습니다.

- 자체 서명 인증서
- Entrust, Thawte, GoDaddy 등의 서드파티 인증서
- Cisco IOS®/ASA(Adaptive Security Appliance) CA(Certificate Authority)

SSL VPN 게이트웨이 및 CallManager의 컨피그레이션이 완료되면 IP 전화를 로컬로 가입해야 합니다.이렇게 하면 전화기가 CUCM에 가입하고 올바른 VPN 정보 및 인증서를 사용할 수 있습니다.전화기가 로컬로 조인되지 않은 경우 SSL VPN 게이트웨이를 찾을 수 없으며 SSL VPN 핸드셰이크를 완료하기 위한 올바른 인증서가 없습니다.

가장 일반적인 컨피그레이션은 ASA 자체 서명 인증서 및 Cisco IOS 자체 서명 인증서가 포함된 CUCM/Unified CME입니다.따라서 구성이 가장 쉽습니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco Unified Communications Manager(CUCM) 또는 Cisco Unified Communications Manager Express(Cisco Unified CME)
- SSL VPN(WebVPN)
- Cisco ASA(Adaptive Security Appliance)
- 자체 서명, 서드파티, 인증 기관 등의 인증서 유형

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- ASA Premium 라이센스.
- AnyConnect VPN 전화 라이센스.
  - ASA 릴리스 8.0.x의 경우 라이센스는 Linksys Phone용 AnyConnect입니다.
  - ASA 릴리스 8.2.x 이상의 경우 라이센스는 Cisco VPN Phone용 AnyConnect입니다.
- SSL VPN 게이트웨이:ASA 8.0 이상(AnyConnect for Cisco VPN Phone 라이센스 포함) 또는 Cisco IOS Software 릴리스 12.4T 이상
  - Cisco IOS Software 릴리스 12.4T 이상은 SSL VPN 컨피그레이션 가이드에 설명된 대로 공식적으로 지원되지 않습니다.
  - Cisco IOS Software Release 15.0(1)M에서 SSL VPN 게이트웨이는 Cisco 880, Cisco 890, Cisco 1900, Cisco 2900 및 Cisco 3900 플랫폼의 사용자 수 기반 라이센스 기능입니다.성공적인 SSL VPN 세션에 유효한 라이센스가 필요합니다.
- 통화 관리자:CUCM 8.0.1 이상 또는 Unified CME 8.5 이상

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.

구성

> **참고:**
>
> 이 섹션에 사용된 명령에 대한 자세한 내용을 보려면 Command Lookup Tool(등록된 고객만 해당)을 사용합니다.
>
> Output Interpreter 도구(등록된 고객만 해당)는 특정 **show** 명령을 지원합니다.**show** 명령 출력의 분석을 보려면 [출력 인터프리터 도구]를 사용합니다.

기본 ASA SSL VPN 컨피그레이션

기본 ASA SSL VPN 컨피그레이션은 다음 문서에서 설명합니다.

- ASA 8.x:자체 서명 인증서 컨피그레이션을 사용하여 AnyConnect VPN 클라이언트를 통한 VPN 액세스 예
- AnyConnect VPN 클라이언트 연결 구성

이 컨피그레이션이 완료되면 원격 테스트 PC가 SSL VPN 게이트웨이에 연결하고 AnyConnect를 통해 연결한 다음 CUCM에 ping을 수행할 수 있어야 합니다.ASA에 Cisco IP Phone용 AnyConnect 라이센스가 있는지 확인합니다.(show ver 명령을 사용합니다.) 게이트웨이와 클라이언트 간에 TCP 및 UDP 포트 443이 모두 열려 있어야 합니다.

참고:부하 분산 SSL VPN은 VPN 전화에 대해 지원되지 않습니다.

CUCM:자체 서명 인증서 컨피그레이션이 있는 ASA SSL VPN

자세한 내용은 AnyConnect를 사용하여 IP Phone SSL VPN-ASA를 참조하십시오.

ASA에는 Cisco VPN Phone용 AnyConnect 라이센스가 있어야 합니다.SSL VPN을 구성한 다음 VPN에 대해 CUCM을 구성합니다.

1. ASA에서 자체 서명 인증서를 내보내려면 이 명령을 사용합니다.

```
ciscoasa(config)# crypto ca export trustpoint name identity-certificate
```

   이 명령은 터미널에 pem 인코딩 ID 인증서를 표시합니다.
2. 인증서를 복사하여 텍스트 편집기에 붙여넣고 .pem 파일로 저장합니다.BEGIN CERTIFICATE(시작 인증서) 및 END CERTIFICATE(종료 인증서) 행을 포함해야 합니다. 그렇지 않으면 인증서가 올바르게 임포트되지 않습니다.전화기가 ASA에 대한 인증을 시도할 때 문제가 발생하므로 인증서의 형식을 수정하지 마십시오.
3. CUCM의 **CERTIFICATE MANAGEMENT** 섹션에 인증서 파일을 로드하려면 Cisco Unified Operating System Administration(**Cisco Unified 운영 체제 관리) > Security(보안) > Certificate Management(인증서 관리) > Upload Certificate/Certificate Chain(인증서/인증서 체인 업로드**)으로 이동합니다.
4. ASA에서 자체 서명 인증서를 로드하는 데 사용되는 동일한 영역에서 CallManager.pem, CAPF.pem 및 Cisco_Manufacturing_CA.pem 인증서를 다운로드하고 데스크톱에 저장합니다(1단계 참조).
   1. 예를 들어 CallManager.pem을 ASA로 가져오려면 다음 명령을 사용합니다.

```
ciscoasa(config)# crypto ca trustpoint certificate-name
ciscoasa(config-ca-trustpoint)# enrollment terminal
ciscoasa(config)# crypto ca authenticate certificate-name
```

   2. 신뢰 지점에 해당하는 인증서를 복사하여 붙여넣으라는 메시지가 표시되면 CUCM에서 저장한 파일을 연 다음 Base64 인코딩 인증서를 복사하여 붙여넣습니다.BEGIN CERTIFICATE 및 END CERTIFICATE 줄(하이픈 포함)을 포함해야 합니다.
   3. end를 입력하고 Return을 **누릅니다**.
   4. 인증서를 수락하라는 메시지가 표시되면 **yes**를 입력하고 **Enter**를 누릅니다.
   5. CUCM의 다른 두 인증서(CAPF.pem, Cisco_Manufacturing_CA.pem)에 대해 1~4단계를 반복합니다.

5. CUCM IPphone VPN config.pdf에 설명된 대로 올바른 VPN 컨피그레이션에 대한 CUCM을 구성합니다.

   참고:CUCM에 구성된 VPN 게이트웨이는 VPN 게이트웨이에 구성된 URL과 일치해야 합니다.게이트웨이와 URL이 일치하지 않으면 전화기가 주소를 확인할 수 없으며 VPN 게이트웨이에 디버그가 표시되지 않습니다.

- CUCM에서 다음을 수행합니다.VPN 게이트웨이 URL은 https://192.168.1.1/VPNPhone입니다.
- ASA에서 다음 명령을 사용합니다.

```
ciscoasa# configure terminal
ciscoasa(config)# tunnel-group VPNPhones webvpn-attributes
ciscoasa(config-tunnel-webvpn)# group-url https://192.168.1.1/VPNPhone
enable
ciscoasa(config-tunnel-webvpn)# exit
```

- ASDM(Adaptive Security Device Manager) 또는 연결 프로파일에서 이 명령을 사용할 수 있습니다.

CUCM:서드파티 인증서 컨피그레이션이 포함된 ASA SSL VPN

이 컨피그레이션은 CUCM에 설명된 컨피그레이션과 매우 유사합니다.ASA SSLVPN with Self-Signed Certificates Configuration 섹션(서드파티 인증서를 사용 중임을 제외하고).ASA 8.x에 설명된 대로 서드파티 인증서로 ASA에서 SSL VPN을 구성합니다. WebVPN 컨피그레이션 예와 함께 사용할 타사 공급업체 인증서를 수동으로 설치합니다.

참고:ASA에서 CUCM으로 전체 인증서 체인을 복사하고 모든 중간 및 루트 인증서를 포함해야 합니다.CUCM에 전체 체인이 포함되지 않은 경우 전화기에 인증에 필요한 인증서가 없으며 SSL VPN 핸드셰이크에 실패합니다.

기본 IOS SSL VPN 컨피그레이션

참고:IP 전화는 IOS SSL VPN에서 지원되지 않는 것으로 지정됩니다.컨피그레이션은 최선의 노력일 뿐입니다.

기본 Cisco IOS SSL VPN 컨피그레이션은 다음 문서에서 설명합니다.

- SDM 컨피그레이션이 포함된 IOS의 SSL VPN 클라이언트(SVC) 예
- IOS Zone Based Policy Firewall을 사용하는 IOS 라우터의 AnyConnect VPN 클라이언트 컨피그레이션 예

이 컨피그레이션이 완료되면 원격 테스트 PC가 SSL VPN 게이트웨이에 연결하고 AnyConnect를 통해 연결한 다음 CUCM에 ping을 수행할 수 있어야 합니다.Cisco IOS 15.0 이상에서는 이 작업을 완료하려면 유효한 SSL VPN 라이센스가 있어야 합니다.게이트웨이와 클라이언트 간에 TCP 및 UDP 포트 443이 모두 열려 있어야 합니다.

CUCM:자체 서명 인증서 컨피그레이션이 있는 IOS SSL VPN

이 컨피그레이션은 CUCM에 설명된 컨피그레이션과 유사합니다.ASA SSLVPN with Third-Party Certificates Configuration 및 CUCM:ASA SSLVPN with Self-Signed Certificates Configuration 섹션.차이점은 다음과 같습니다.

1. 라우터에서 자체 서명 인증서를 내보내려면 이 명령을 사용합니다.

```
R1(config)# crypto pki export trustpoint-name pem terminal
```

2. CUCM 인증서를 가져오려면 다음 명령을 사용합니다.

```
R1(config)# crypto pki trustpoint certificate-name
R1(config-ca-trustpoint)# enrollment terminal
R1(config)# crypto ca authenticate certificate-name
```

WebVPN 컨텍스트 컨피그레이션에는 다음 텍스트가 표시되어야 합니다.

```
gateway webvpn_gateway domain VPNPhone
```

CUCM에 설명된 대로 CUCM을 구성합니다.ASA SSLVPN with Self-Signed Certificates Configuration 섹션.

CUCM:서드파티 인증서 컨피그레이션을 사용하는 IOS SSL VPN

이 컨피그레이션은 CUCM에 설명된 컨피그레이션과 유사합니다.ASA SSLVPN with Self-Signed Certificates Configuration 섹션.서드파티 인증서로 WebVPN을 구성합니다.

> **참고:**전체 WebVPN 인증서 체인을 CUCM에 복사하고 모든 중간 및 루트 인증서를 포함해야 합니다.CUCM에 전체 체인이 포함되지 않은 경우 전화기에 인증에 필요한 인증서가 없으며 SSL VPN 핸드셰이크에 실패합니다.

Unified CME:자체 서명 인증서/서드파티 인증서 컨피그레이션이 포함된 ASA/라우터 SSL VPN

Unified CME의 컨피그레이션은 CUCM의 컨피그레이션과 유사합니다.예를 들어 WebVPN 엔드포인트 컨피그레이션은 동일합니다.유일한 중요한 차이점은 Unified CME 통화 에이전트의 컨피그레이션입니다.Configuring SSL VPN Client for SCCP IP Phones(SCCP IP Phone용 SSL VPN 클라이언트 구성)에 설명된 대로 Unified CME에 대한 VPN 그룹 및 VPN 정책을 구성합니다.

> **참고:**Unified CME는 SCCP(Skinny Call Control Protocol)만 지원하며 VPN 전화에 대한 SIP(Session Initiation Protocol)를 지원하지 않습니다.

> **참고:**Unified CME에서 ASA 또는 라우터로 인증서를 내보낼 필요가 없습니다.ASA 또는 라우터 WebVPN 게이트웨이에서 Unified CME로 인증서를 내보내기만 하면 됩니다.

WebVPN 게이트웨이에서 인증서를 내보내려면 ASA/라우터 섹션을 참조하십시오.서드파티 인증서를 사용하는 경우 전체 인증서 체인을 포함해야 합니다.인증서를 Unified CME로 가져오려면 인증서를 라우터로 가져오는 데 사용되는 것과 동일한 방법을 사용합니다.

```
CME(config)# crypto pki trustpoint certificate-name
CME(config-ca-trustpoint)# enrollment terminal
CME(config)# crypto ca authenticate certificate-name
```

SSL VPN 구성을 사용하는 UC 520 IP Phone

Cisco Unified Communications 500 Series 모델 UC 520 IP 전화기는 CUCM 및 CME 구성과 매우 다릅니다.

- UC 520 IP 전화기는 CallManager 및 WebVPN 게이트웨이가 모두 되므로 두 전화기 간에 인증서를 구성할 필요가 없습니다.
- 일반적으로 자체 서명 인증서 또는 서드파티 인증서와 같이 라우터에서 WebVPN을 구성합니다.
- UC 520 IP 전화에는 WebVPN 클라이언트가 내장되어 있으며 일반적인 PC에서 WebVPN에 연결하는 것과 동일하게 구성할 수 있습니다.게이트웨이, 사용자 이름/비밀번호 조합을 입력합니다.
- UC 520 IP 전화는 Cisco Small Business IP Phone SPA 525G 전화와 호환됩니다.

다음을 확인합니다.

현재 이 구성에 대해 사용 가능한 확인 절차가 없습니다.

문제 해결

현재 이 컨피그레이션에 사용할 수 있는 특정 문제 해결 정보가 없습니다.