로컬 인증으로 ISR4k에 대한 AnyConnect SSL VPN 구성

목차

소개

이 문서에서는 로컬 사용자 데이터베이스를 사용하여 AnyConnect SSL(Secure Sockets Layer) VPN용 ISR(Integrated Service Router) 4k Cisco IOS® XE 헤드엔드를 구성하는 방법의 샘플 컨피그레이션에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco IOS XE(ISR 4K)
- AnyConnect Secure Mobility 클라이언트
- 일반 SSL 작업
- PKI(Public Key Infrastructure)

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco ISR4451-X/K9 라우터(버전 17.9.2a)
- AnyConnect Secure Mobility Client 4.10.04065

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

배경 정보

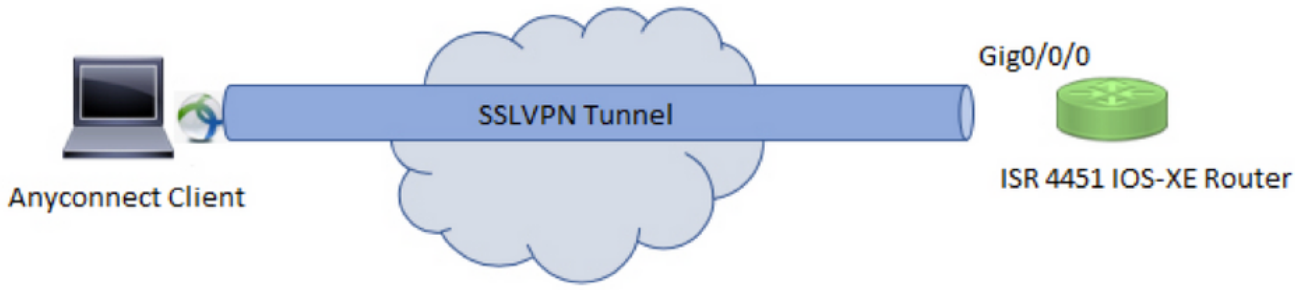
SSL Virtual Private Network(VPN) 기능은 Cisco IOS XE Software에서 원격 사용자가 인터넷의 어디에서나 엔터프라이즈 네트워크에 액세스할 수 있도록 지원합니다. 원격 액세스는 Secure Socket Layer-enabled(SSL-enabled) SSL VPN 게이트웨이를 통해 제공됩니다. SSL VPN 게이트웨이를 사용하면 원격 사용자가 보안 VPN 터널을 설정할 수 있습니다. Cisco IOS XE SSL VPN을 통해 최종 사용자는 집이나 무선 핫스팟과 같은 인터넷 사용 위치에서 안전하게 액세스할 수 있습니다. 또한 Cisco IOS XE SSL VPN을 통해 기업은 기업 데이터 보호를 위해 해외 파트너 및 컨설턴트에게 기업 네트워크 액세스를 확장할 수 있습니다.

이 기능은 지정된 플랫폼에서 지원됩니다.

플랫폼	지원되는 Cisco IOS XE 릴리스
Cisco Cloud Services Router 1000V 시리즈	Cisco IOS XE 릴리스 16.9
Cisco Catalyst 8000V	Cisco IOS XE Bengaluru 17.4.1
Cisco 4461 Integrated Services Router Cisco 4451 Integrated Services Router Cisco 4431 Integrated Services Router	Cisco IOS XE Cupertino 17.7.1a

구성

네트워크 다이어그램



설정

1. AAA(Authentication, Authorization, and Accounting)를 활성화하고, 인증, 권한 부여 목록을 구성하고, 로컬 데이터베이스에 사용자 이름을 추가합니다.

```
aaa new-model
!
aaa authentication login default local
aaa authorization exec default local
aaa authorization network default local
!
username test password cisco123
```

2. 로컬 인증을 위해 ID 인증서가 없으면 신뢰 지점을 만들어 ID 인증서를 설치합니다. 인증서 생성에 대한 자세한 내용은 PKI의 Certificate Enrollment(인증서 등록)를 참조하십시오.

```
crypto pki trustpoint SSL
enrollment mode ra
enrollment url http://x.x.x.x:80/certsrv/mscep/mscep.dll
subject-name cn=sslvpn.cisco.com
revocation-check crl
rsakeypair SSL-Keys
```

3. SSL 제안서를 구성합니다.

```
crypto ssl proposal SSL_Proposal
protection rsa-3des-ede-sha1 rsa-aes128-sha1
```

4. SSL 정책을 구성하고 SSL 제안 및 PKI 신뢰 지점을 호출합니다.

```
crypto ssl policy SSL_Policy
ssl proposal SSL_Proposal
pki trustpoint SSL sign
ip address local y.y.y.y port 443
```

y.y.y.y는 GigabitEthernet0/0/0의 IP 주소입니다.

5. (선택 사항) 스플릿 터널에 사용할 표준 액세스 목록을 구성합니다. 이 액세스 목록은 VPN 터널을 통해 액세스할 수 있는 대상 네트워크로 구성됩니다. 스플릿 터널이 구성되지 않은 경우 기본적으로 모든 트래픽이 VPN 터널(전체 터널)을 통과합니다.

```
ip access-list standard split_tunnel_acl
10 permit 192.168.10.0 0.0.0.255
```

6. IPv4 주소 풀을 생성합니다.

```
ip local pool SSLVPN_POOL 192.168.20.1 192.168.20.10
```

생성된 IP 주소 풀은 성공적인 AnyConnect 연결 중에 AnyConnect 클라이언트에 IPv4 주소를 할당합니다.

7. bootflash의 webvpn 디렉토리 아래에 AnyConnect 헤드엔드 이미지(**webdeploy**)를 업로드하고 라우터의 bootflash에 클라이언트 프로파일을 업로드합니다.

지정된 대로 AnyConnect 이미지 및 클라이언트 프로파일을 정의합니다.

```
crypto vpn anyconnect bootflash:/webvpn/anyconnect-win-4.10.04065-webdeploy-k9.pkg sequence 1
!
crypto vpn anyconnect profile sslvpn_client_profile bootflash:/sslvpn_client_profile.xml
```

8. 권한 부여 정책을 구성합니다.

```
crypto ssl authorization policy SSL_Author_Policy
rekey time 1110
client profile sslvpn_client_profile
mtu 1000
keepalive 500
dpd-interval client 1000
netmask 255.255.255.0
pool SSLVPN_POOL
dns 8.8.8.8
banner This is SSL VPN tunnel.
route set access-list split_tunnel_acl
```

IP 풀, DNS, 스플릿 터널 목록 등은 권한 부여 정책에 지정됩니다.

9. 가상 액세스 인터페이스를 복제할 가상 템플릿을 구성합니다.

```
interface Virtual-Template1 type vpn
ip unnumbered GigabitEthernet0/0/0
ip mtu 1400
ip tcp adjust-mss 1300
```

unnumbered 명령은 구성된 인터페이스(GigabitEthernet0/0/0)에서 IP 주소를 가져오고 해당 인터페이스에서 IPv4 라우팅이 활성화됩니다.

10. SSL 프로필을 구성하고 인증 및 권한 부여 매개변수 및 가상 템플릿과 함께 SSL 프로필에서 생성된 SSL 정책을 확인합니다.

```
crypto ssl profile SSL_Profile
match policy SSL_Policy
aaa authentication user-pass list default
aaa authorization group user-pass list default SSL_Author_Policy
authentication remote user-pass
virtual-template 1
```

AnyConnect 프로파일 편집기의 도움으로 AnyConnect 프로파일을 생성합니다. 참조를 위해 XML 프로파일의 스니펫이 제공됩니다. 전체 프로필이 이 이 문서에 첨부됩니다.

```
!
!
```

!

다음을 확인합니다.

구성이 올바르게 작동하는지 확인하려면 이 섹션을 활용하십시오.

1. Check the ssl connection parameters for your anyconnect connection

sslvpn# show crypto ssl session user test

```
Interface : Virtual-Access1
Session Type : Full Tunnel
Client User-Agent : AnyConnect Windows 4.10.04065

Username : test Num Connection : 1
Public IP : 10.106.52.195
Profile : SSL_Profile
Policy : SSL_Policy
Last-Used : 00:03:58 Created : *05:11:06.166 UTC Wed Feb 22 2023
Tunnel IP : 192.168.20.10 Netmask : 255.255.255.0
Rx IP Packets : 174 Tx IP Packets : 142
```

2. Verify the SSL session status

```
sslvpn# show crypto ssl session
SSL profile name: SSL_Profile
Client_Login_Name Client_IP_Address No_of_Connections Created Last_Used
test 10.106.52.195 1 00:03:32 00:03:32
```

3. Verify the tunnel statistics for the active connection

```
sslvpn# show crypto ssl stats tunnel
SSLVPN Profile name : SSL_Profile
Tunnel Statistics:
Active connections : 1
Peak connections : 1 Peak time : 5d12h
Connect succeed : 10 Connect failed : 0
Reconnect succeed : 38 Reconnect failed : 0
IP Addr Alloc Failed : 0 VA creation failed : 0
DPD timeout : 0
Client
in CSTP frames : 129 in CSTP control : 129
in CSTP data : 0 in CSTP bytes : 1516
out CSTP frames : 122 out CSTP control : 122
out CSTP data : 0 out CSTP bytes : 1057
cef in CSTP data frames : 0 cef in CSTP data bytes : 0
cef out CSTP data frames : 0 cef out CSTP data bytes : 0
Server
In IP pkts : 0 In IP bytes : 0
In IP6 pkts : 0 In IP6 bytes : 0
Out IP pkts : 0 Out IP bytes : 0
Out IP6 pkts : 0 Out IP6 bytes : 0
```

4. Check the actual configuration applied for the Virtual-Acces interface associated with client

```
sslvpn# show derived-config interface virtual-access 1
Building configuration...

Derived configuration : 171 bytes
!
interface Virtual-Access1
description ***Internally created by SSLVPN context profile1***
ip unnumbered GigabitEthernet0/0/0
ip mtu 1400
ip tcp adjust-mss 1300
```

문제 해결

이 섹션에서는 컨피그레이션 문제를 해결하는 데 사용할 수 있는 정보를 제공합니다.

1. 헤드엔드에서 수집할 SSL 디버깅

```
debug crypto ssl condition client username <username>
debug crypto ssl aaa
debug crypto ssl aggr-auth message
debug crypto ssl aggr-auth packets
debug crypto ssl tunnel errors
debug crypto ssl tunnel events
debug crypto ssl tunnel packets
debug crypto ssl package
```

2. SSL 연결 문제를 해결하기 위한 몇 가지 추가 명령:

```
# show crypto ssl authorization policy
# show crypto ssl diagnose error
# show crypto ssl policy
# show crypto ssl profile
# show crypto ssl proposal
# show crypto ssl session profile <profile_name>
# show crypto ssl session user <username> detail
# show crypto ssl session user <username> platform detail
```

3. AnyConnect 클라이언트의 DART

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.