

로컬 인증을 사용하여 C8000v에서 AnyConnect SSL VPN 구성

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[배경 정보](#)

[구성](#)

[네트워크 다이어그램](#)

[설정](#)

[연결 흐름](#)

[Cisco Secure Client\(AnyConnect\) - C8000v 하이 레벨 연결 흐름](#)

[다음을 확인합니다.](#)

[문제 해결](#)

[관련 정보](#)

소개

이 문서에서는 로컬 사용자 데이터베이스를 사용하여 AnyConnect SSL VPN용 Cisco IOS XE Headend C8000v를 구성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco IOS XE
- CSC(Cisco Secure Client)
- 일반 SSL 작업
- PKI(Public Key Infrastructure)

사용되는 구성 요소

목이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- 버전 17.16.01a를 실행하는 Cisco Catalyst 8000V(C8000V)
- Cisco Secure Client 버전 5.1.8.105
- Cisco Secure Client가 설치된 클라이언트 PC

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

Cisco IOS XE SSL(Secure Socket Layer) VPN은 통합된 데이터, 음성 및 무선 플랫폼에서 업계 최고의 보안 및 라우팅 기능과 통합된 SSL VPN 원격 액세스 연결을 제공하는 라우터 기반 솔루션입니다. 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 네트워크 액세스를 해외 파트너 및 컨설턴트에게 확장하여 기업 데이터를 항상 보호할 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

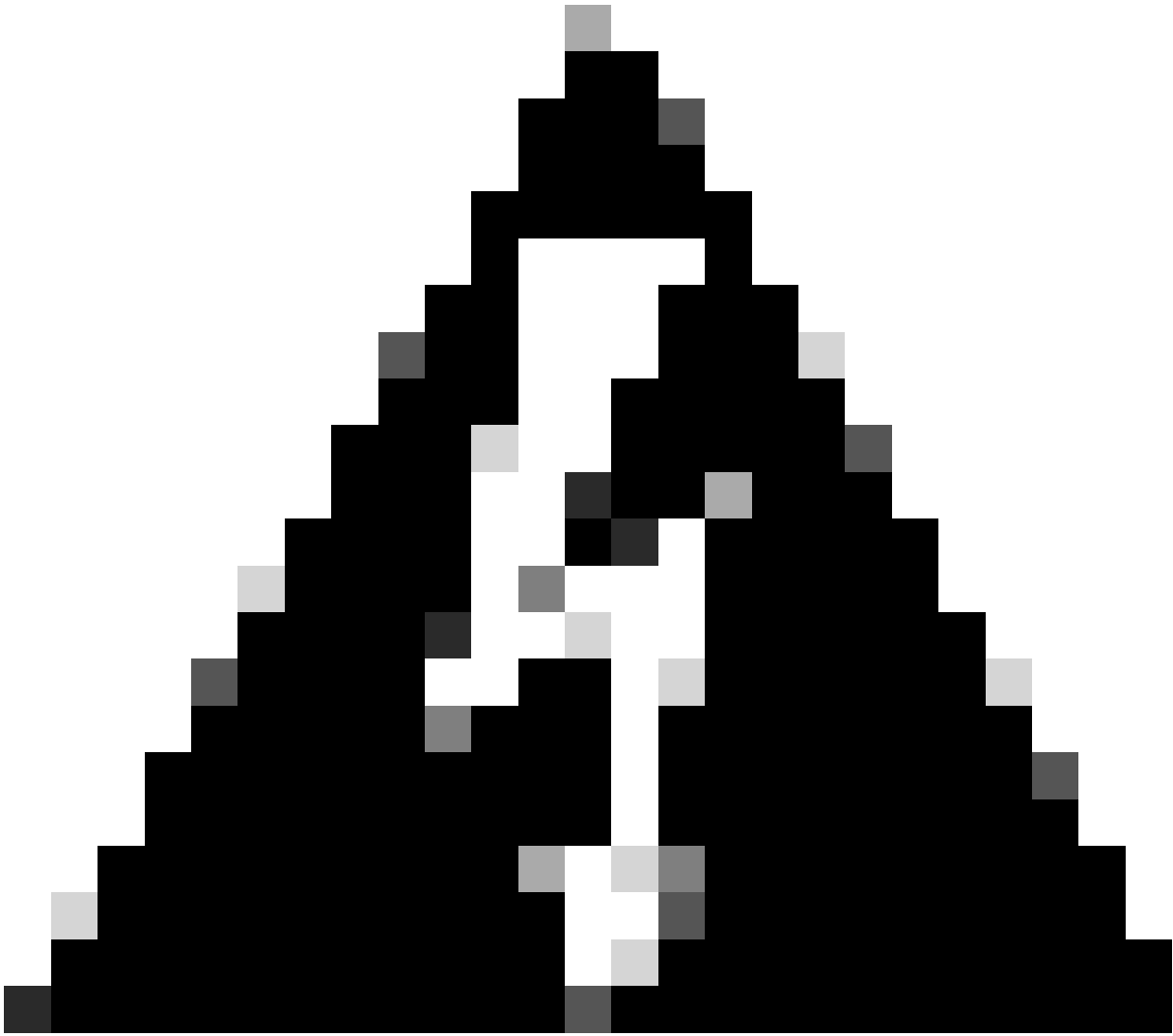


기본 네트워크 다이어그램

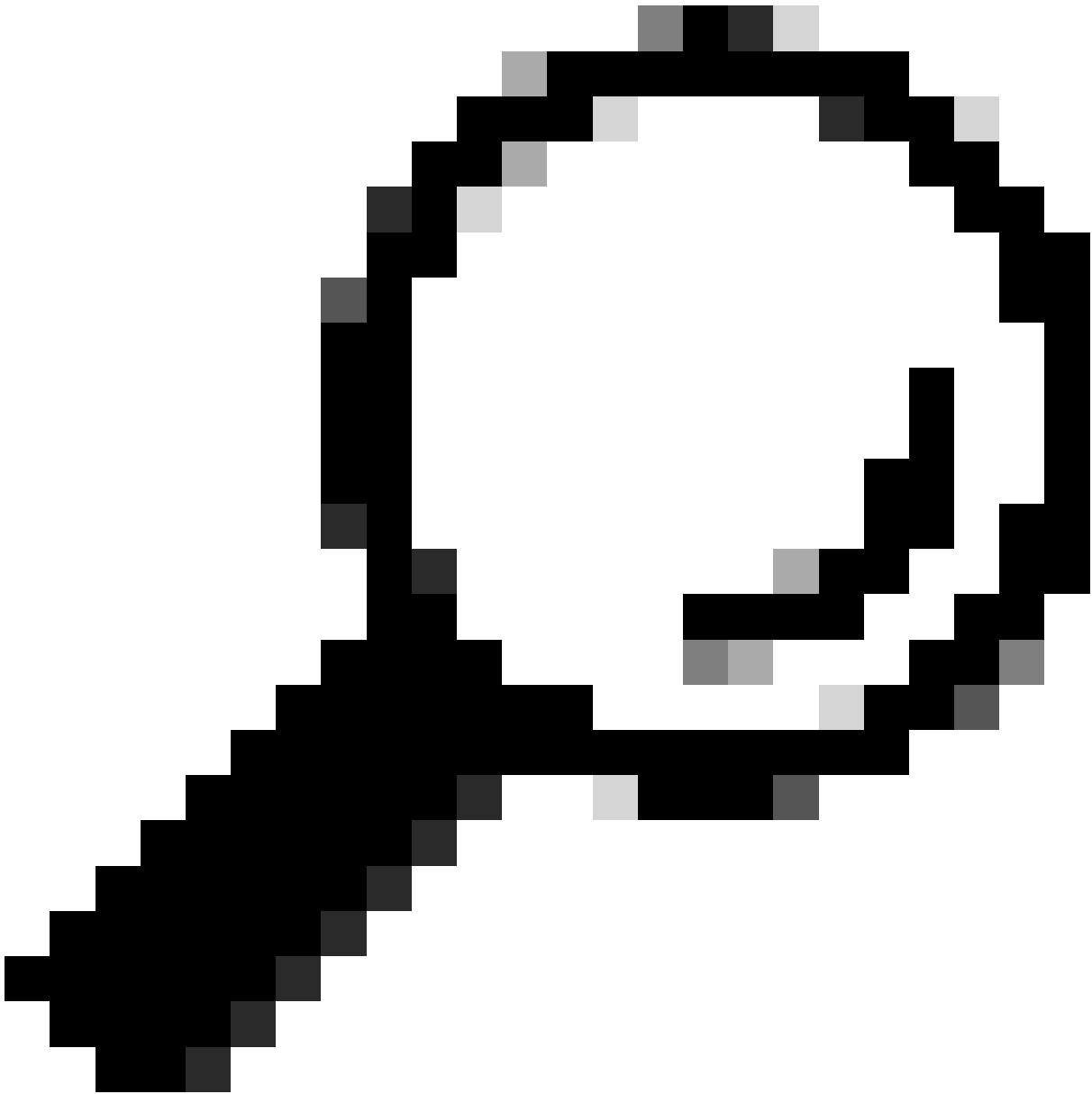
설정

1. AAA를 활성화하고, 인증, 권한 부여 목록을 구성하고, 로컬 데이터베이스에 사용자 이름을 추가합니다.

```
aaa new-model
!
aaa authentication login SSLVPN_AUTHEN local
aaa authorization network SSLVPN_AUTHOR local
!
username test password cisco123
```



경고: aaa new-model 명령은 모든 회선 및 인터페이스에 로컬 인증을 즉시 적용합니다(콘솔 회선 con 0 제외). 이 명령이 활성화된 후 텔넷 세션이 라우터에 열리면(또는 연결 시간이 초과되어 다시 연결해야 하는 경우) 사용자는 라우터의 로컬 데이터베이스를 사용하여 인증해야 합니다. AAA 컨피그레이션을 시작하기 전에 라우터에서 사용자 이름과 비밀번호를 정의하는 것이 좋습니다. 그러면 라우터에서 잠기지 않습니다.



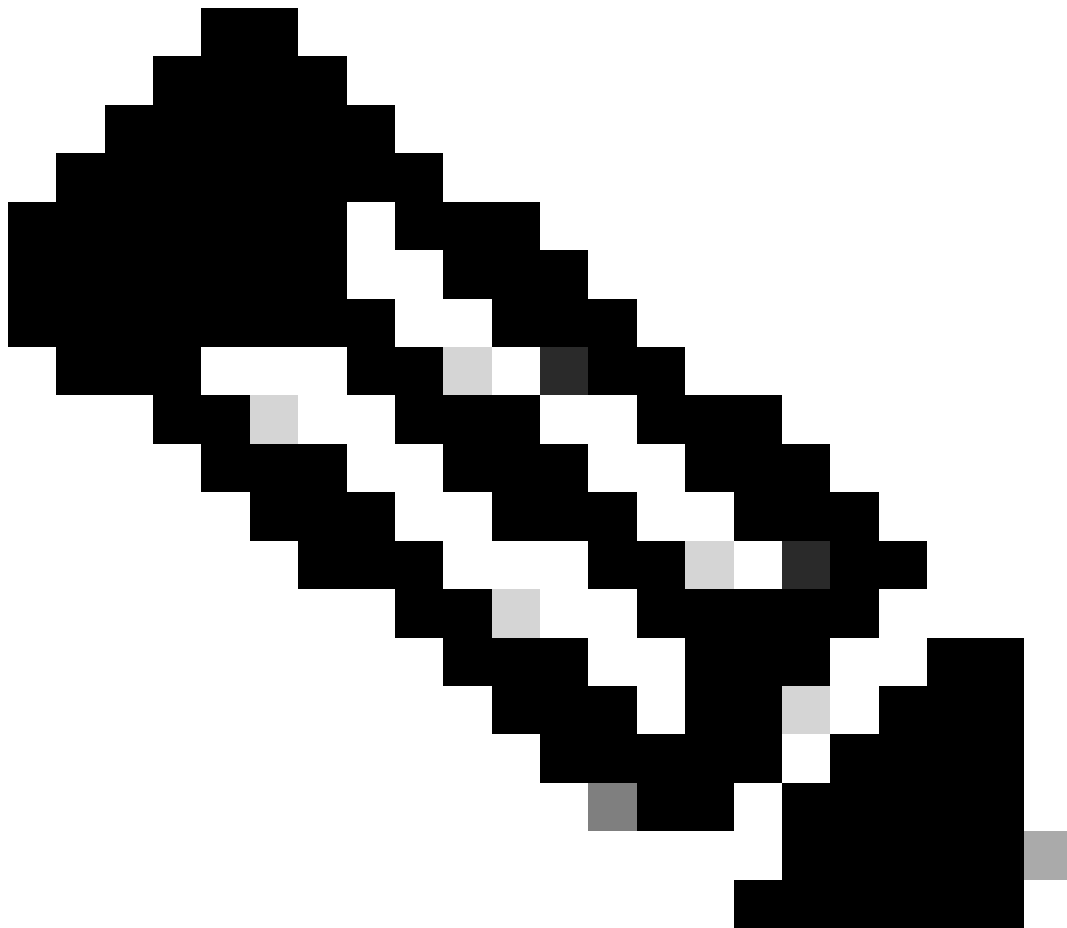
팁: AAA 명령을 구성하기 전에 컨피그레이션을 저장합니다. AAA 컨피그레이션을 완료하고 올바르게 작동한 후에만 컨피그레이션을 다시 저장할 수 있습니다. 이렇게 하면 라우터를 다시 로드하여 변경 사항을 롤백할 수 있으므로 예기치 않은 잠금이 발생하는 경우에도 복구할 수 있습니다.

2. RSA(Rivest-Shamir-Adleman) 키 쌍을 생성합니다.

```
crypto key generate rsa label AnyConnect modulus 2048 exportable
```

3. 라우터의 ID 인증서를 설치할 신뢰 지점을 만듭니다. 인증서 생성에 대한 자세한 [내용은 PKI에 대한 인증서 등록](#) 구성 방법을 참조할 수 있습니다.

```
crypto pki trustpoint TP_AnyConnect
enrollment terminal
fqdn sslvpn-c8kv.example.com
subject-name cn=sslvpn-c8kv.example.com
subject-alt-name sslvpn-c8kv.example.com
revocation-check none
rsakeypair AnyConnect
```



참고: 주체 이름의 CN(Common Name)은 사용자가 보안 게이트웨이(C8000V)에 연결하는 데 사용하는 IP 주소 또는 FQDN(Fully Qualified Domain Name)으로 구성해야 합니다. 필수 사항은 아니지만 CN을 올바르게 입력하면 사용자가 로그인할 때 발생하는 인증서 오류의 수를 줄일 수 있습니다.

4. Cisco Secure Client에 주소를 할당하기 위한 IP 로컬 풀을 정의합니다.

```
ip local pool SSLVPN_POOL 192.168.13.1 192.168.13.10
```

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 192.168.11.0 0.0.0.255
20 permit 192.168.12.0 0.0.0.255
```

6.HTTP 보안 서버를 비활성화합니다.

```
no ip http secure-server
```

7. SSL 제안을 구성합니다.

```
crypto ssl proposal ssl_proposal
protection rsa-aes128-sha1 rsa-aes256-sha1
```

8. SSL 정책을 구성하고 SSL 제안서 및 PKI 신뢰 지점을 호출합니다.

```
crypto ssl policy ssl_policy
ssl proposal ssl_proposal
pki trustpoint TP_AnyConnect sign
ip interface GigabitEthernet1 port 443
```

SSL 정책은 SSL 협상 중에 사용할 제안 및 신뢰 지점을 정의합니다. SSL 협상에 포함된 모든 매개변수의 컨테이너 역할을 합니다. 정책 선택은 정책 아래에 구성된 세션 매개변수에 대해 세션 매개

변수를 일치시켜 수행됩니다.

9 . (선택 사항) Cisco Secure Client Profile Editor Cisco Secure Client Profile Editor의 도움을 받아 AnyConnect [프로파일을 생성합니다](#). 프로필에 해당하는 XML 코드 조각이 참조용으로 제공됩니다.

<#root>

true

true

false

A11

A11

A11

false

Native

true

30

false

true

false

false

true

IPv4, IPv6

true

ReconnectAfterResume

false

true

Automatic

SingleLocalLogon

SingleLocalLogon

AllowRemoteUsers

LocalUsersOnly

false

Disable

false

false

20

4

false

false

true

SSL_C8KV

sslvpn-c8kv.example.com

10. 생성된 XML 프로파일을 라우터의 플래시 메모리에 업로드하고 프로파일을 정의합니다.

```
crypto vpn anyconnect profile acvpn bootflash:/acvpn.xml
```

11.HTTP 보안 서버를 비활성화합니다.

```
no ip http secure-server
```

12. SSL 권한 부여 정책을 구성합니다.

```
crypto ssl authorization policy ssl_author_policy
client profile acvpn
pool SSLVPN_POOL
dns 192.168.11.100
banner Welcome to C8kv SSLVPN
def-domain example.com
route set access-list split-tunnel-ac1
```

SSL 권한 부여 정책은 원격 클라이언트에 푸시되는 권한 부여 매개변수의 컨테이너입니다. 권한 부여 정책은 SSL 프로파일에서 참조됩니다.

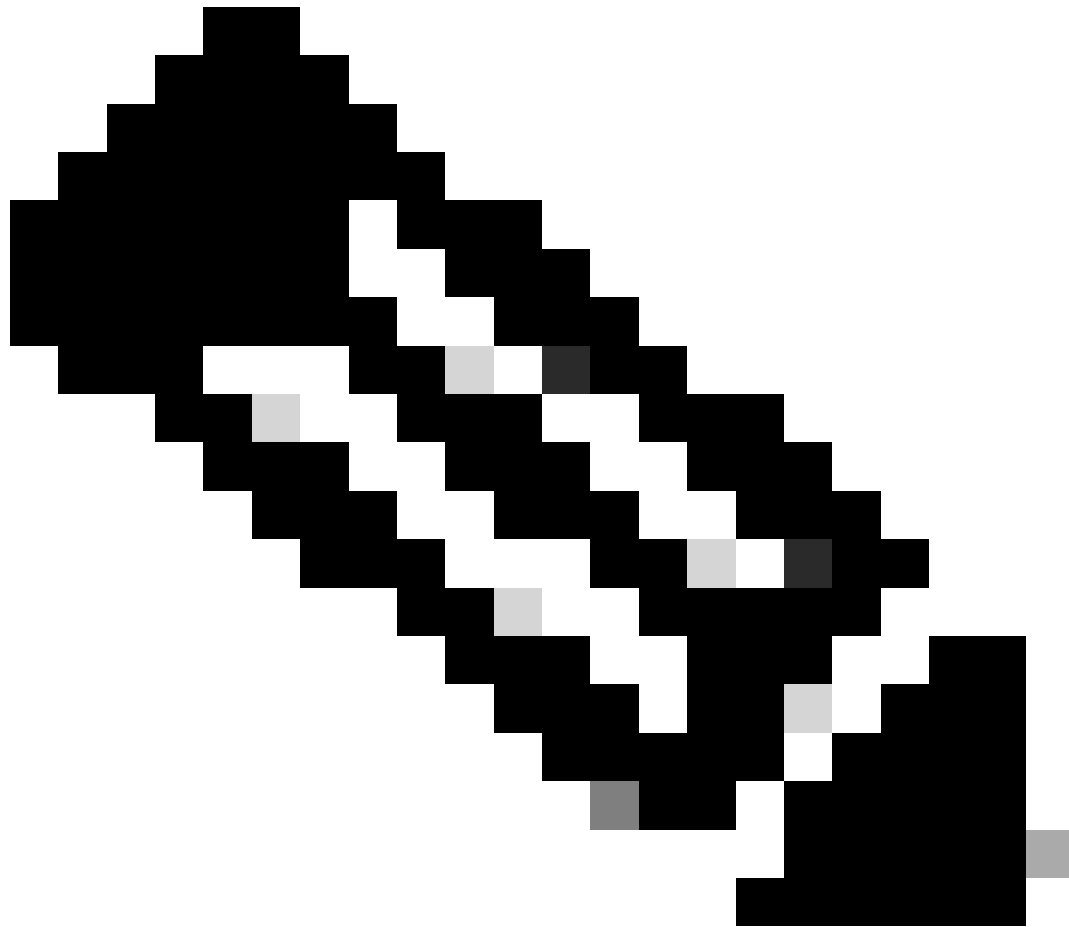
13. 가상 액세스 인터페이스를 복제할 가상 템플릿을 구성합니다.

```
interface Virtual-Template2 type vpn
ip unnumbered GigabitEthernet1
ip mtu 1400
ip tcp adjust-mss 1300
```

14. SSL 프로필을 구성하고 인증, 계정 목록 및 가상 템플릿을 정의합니다.

```
crypto ssl profile ssl_prof
match policy ssl_policy
match url https://sslvpn-c8kv.example.com
aaa authentication user-pass list SSLVPN_AUTHEN
aaa authorization group user-pass list SSLVPN_AUTHOR ssl_author_policy
authentication remote user-pass
virtual-template 2
```

프로필 선택은 정책 및 URL 값에 따라 달라집니다.



참고: 정책 및 URL은 SSL VPN 프로필에 대해 고유해야 하며 세션을 실행하려면 하나 이상의 권한 부여 방법을 지정해야 합니다.

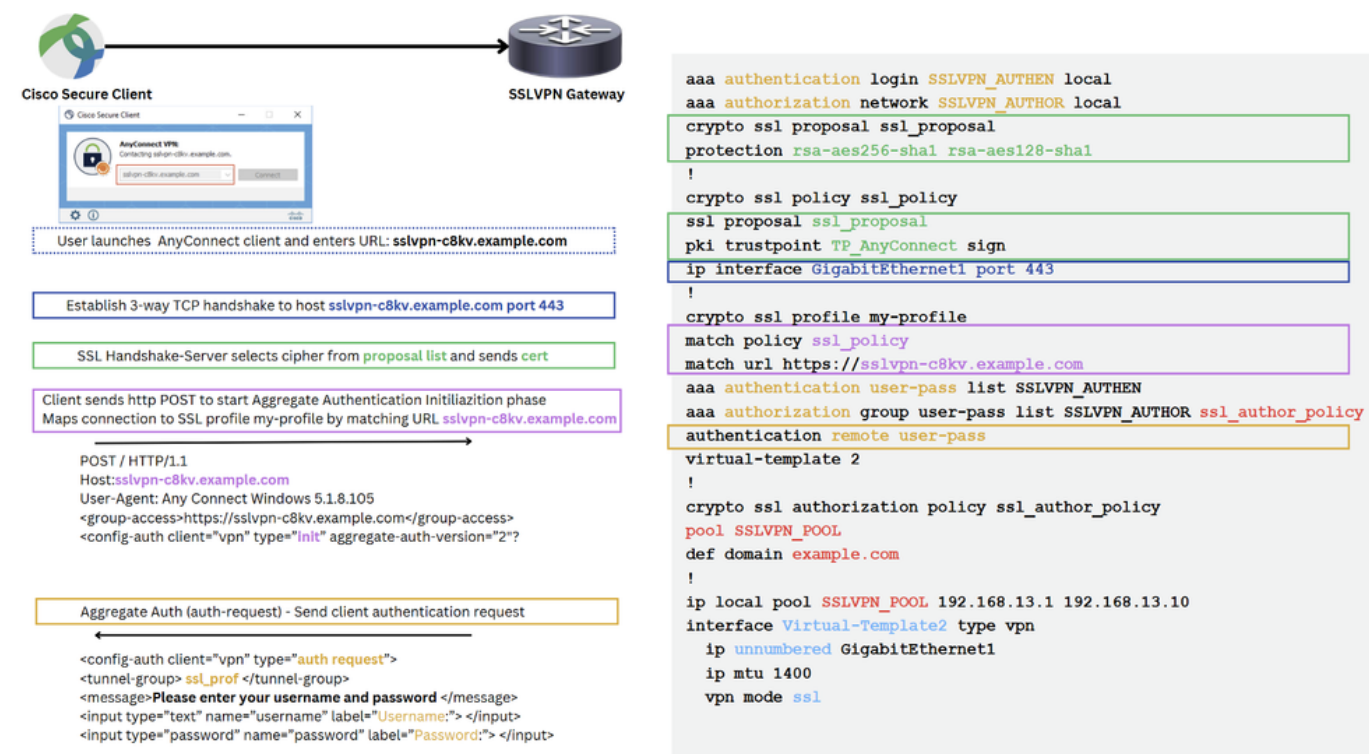
이러한 항목은 SSL 프로필에서 사용됩니다.

- match policy - match 명령문을 사용하여 SSL 정책 이름 ssl_policy에서 클라이언트에 대한 SSL 프로필 ssl_prof를 선택합니다.
- match url - URL sslvpn-c8kv.example.com 디렉토리에서 클라이언트에 대한 SSL 프로파일 ssl_prof를 선택하기 위해 명령문을 일치시킵니다.
- aaa authentication user-pass list - 인증 중에 SSLVPN_AUTHEN 목록이 사용됩니다.
- aaa authorization group user-pass list - 권한 부여 중에 네트워크 목록 SSLVPN_AUTHOR가 권한 부여 정책 ssl_author_policy와 함께 사용됩니다.
- authentication remote user-pass - 사용자 이름/비밀번호를 기반으로 하는 원격 클라이언트의 인증 모드를 정의합니다.
- virtual-template 2 - 복제할 가상 템플릿을 정의합니다.

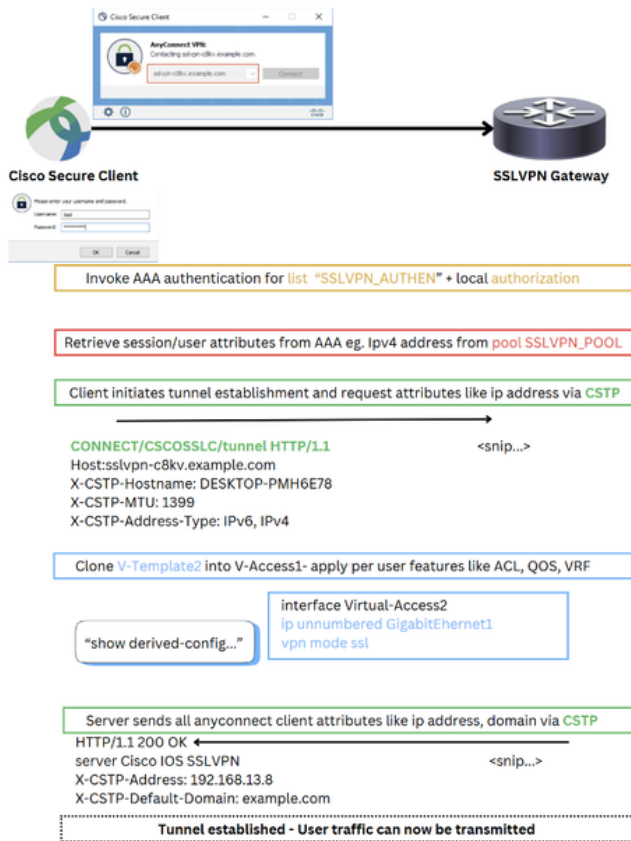
연결 흐름

SSL VPN 연결 설정 중에 Cisco Secure Client와 Secure Gateway 간에 발생하는 이벤트에 대한 자세한 내용은 AnyConnect [SSL VPN 연결 흐름 이해 문서를 참조하십시오](#)

Cisco Secure Client(AnyConnect) - C8000v 하이 레벨 연결 흐름



상위 레벨 연결 흐름 1

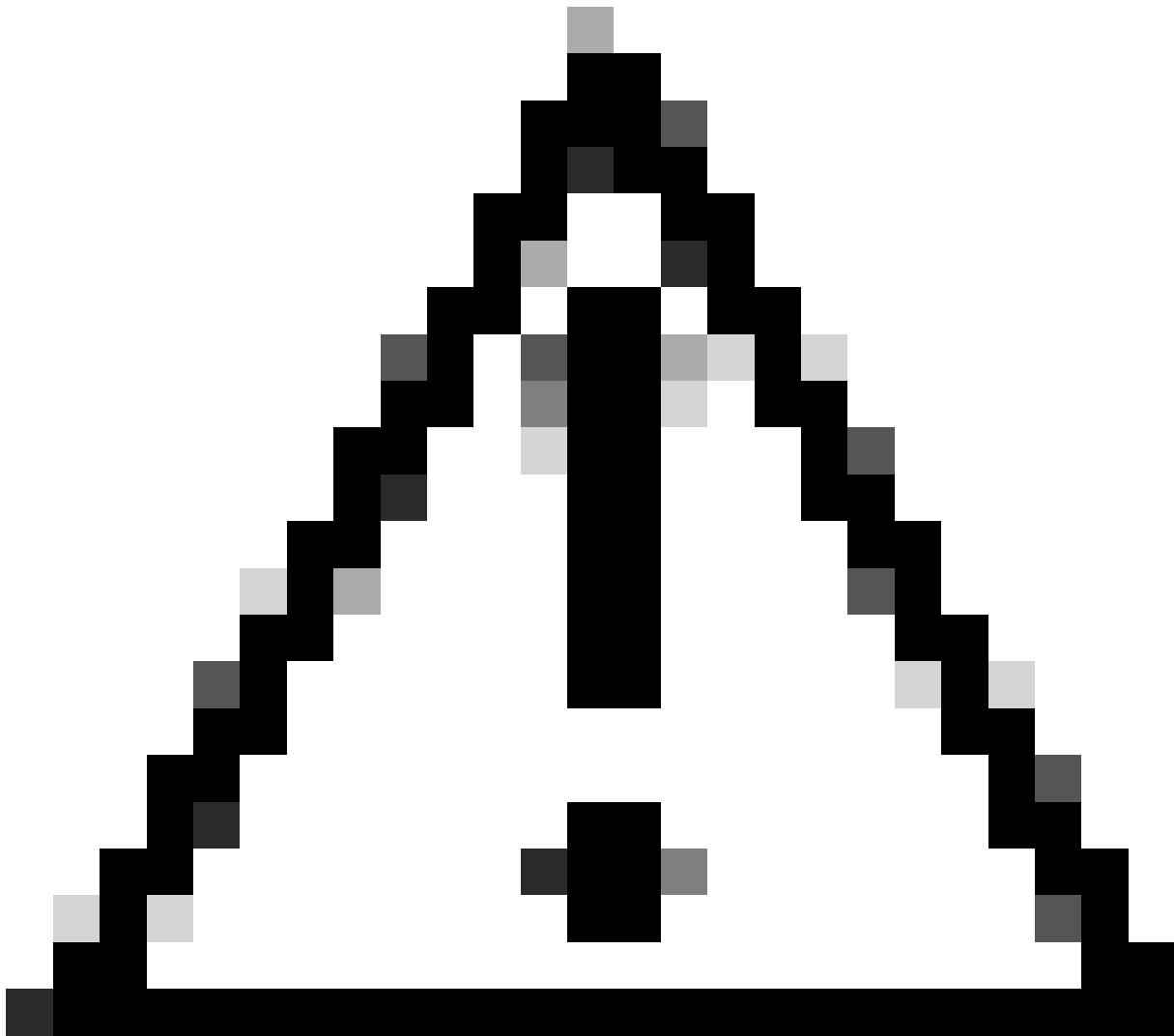


```
aaa authentication login SSLVPN_AUTHEN local
aaa authorization network SSLVPN_AUTHOR local
crypto ssl proposal ssl_proposal
protection rsa-aes256-sha1 rsa-aes128-sha1
!
crypto ssl policy ssl_policy
ssl proposal ssl_proposal
pki trustpoint TP_AnyConnect sign
ip interface GigabitEthernet1 port 443
!
crypto ssl profile my-profile
match policy ssl_policy
match url https://sslvpn-c8kv.example.com
aaa authentication user-pass list SSLVPN_AUTHEN
aaa authorization group user-pass list SSLVPN_AUTHOR ssl_author_policy
authentication remote user-pass
virtual-template 2
!
crypto ssl authorization policy ssl_author_policy
pool SSLVPN_POOL
def domain example.com
!
ip local pool SSLVPN_POOL 192.168.13.1 192.168.13.10
interface Virtual-Template2 type vpn
ip unnumbered GigabitEthernet1
ip mtu 1400
vpn mode ssl
```

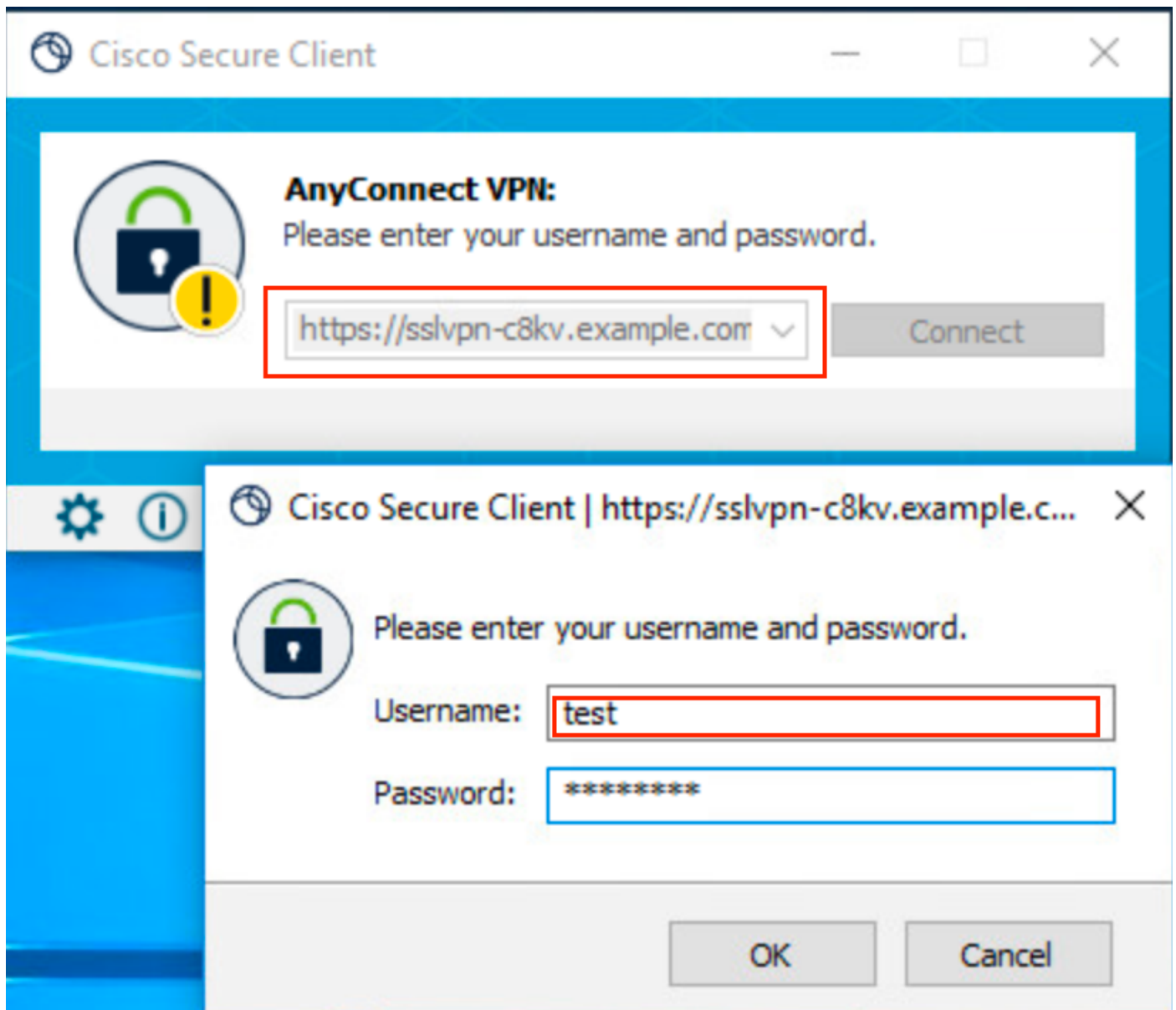
상위 레벨 연결 흐름 2

다음을 확인합니다.

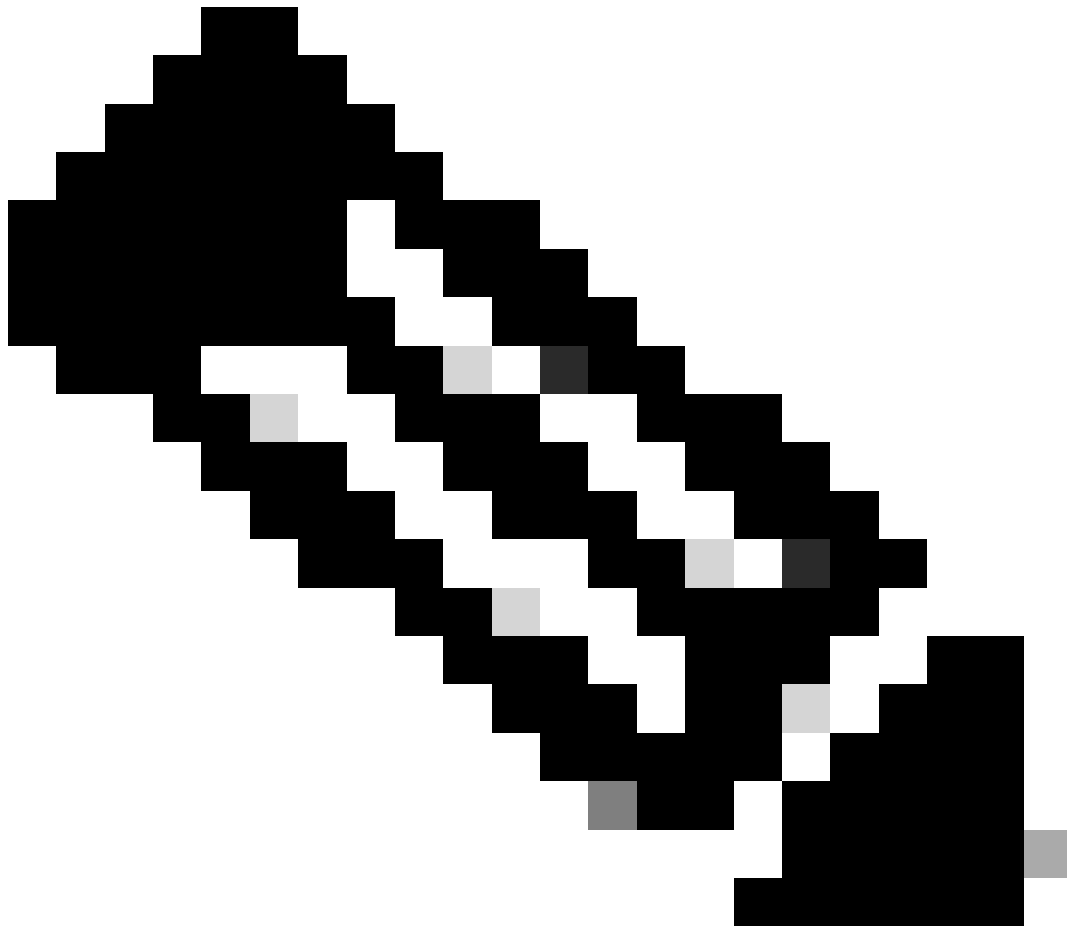
1. 인증을 테스트하려면 Cisco Secure Client에서 FQDN(Fully Qualified Domain Name) 또는 IP 주소 C8000v로 연결한 다음 자격 증명을 입력합니다.



주의: C8000v는 헤드엔드에서 클라이언트 소프트웨어 다운로드를 지원하지 않습니다.
Cisco Secure Client가 PC에 미리 설치되어 있어야 합니다.

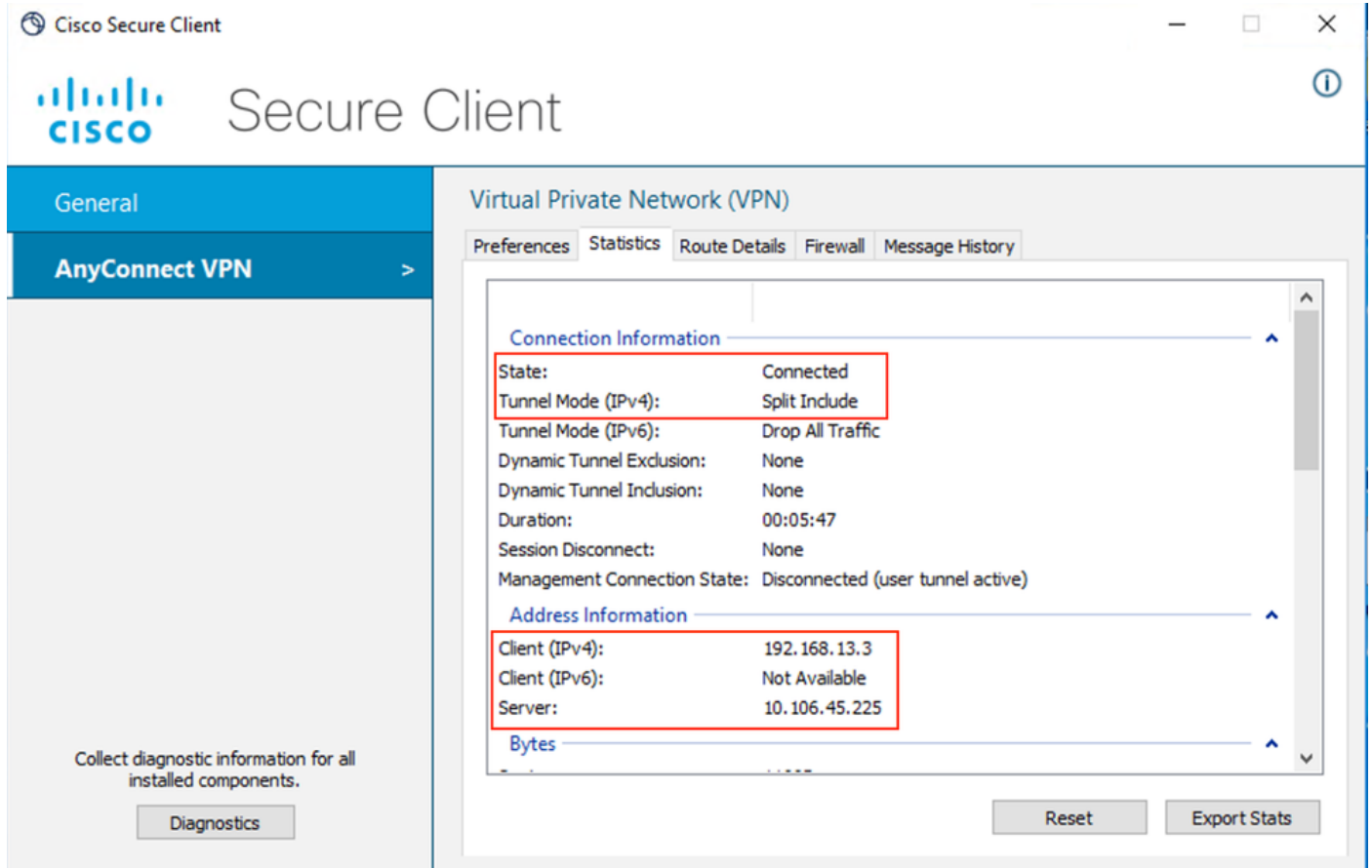


Cisco 보안 클라이언트 연결 시도



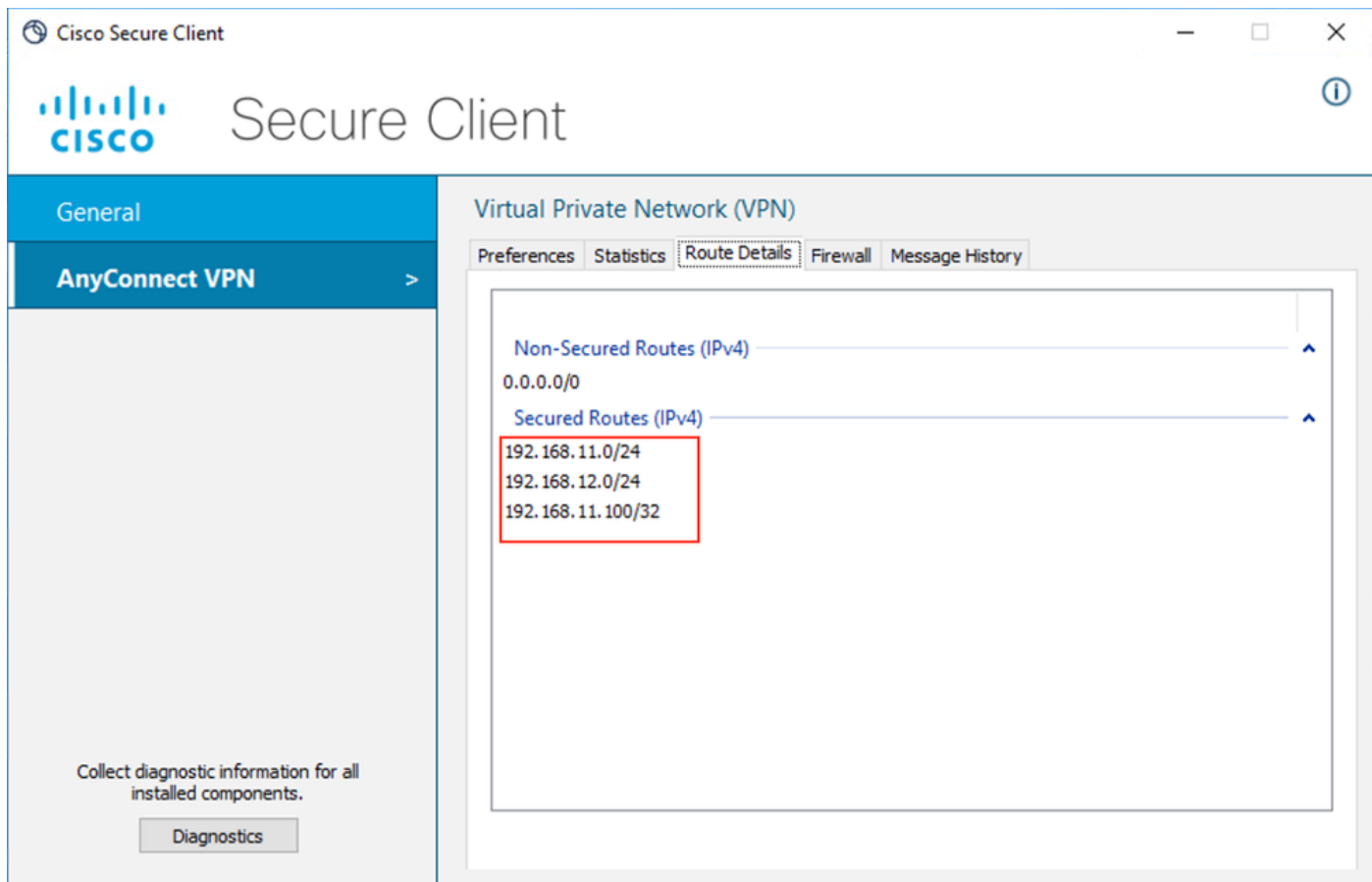
참고: Cisco Secure Client를 새로 설치하면(XML 프로파일이 추가되지 않음) Cisco Secure Client 주소 표시줄에 VPN 게이트웨이의 FQDN을 수동으로 입력할 수 있습니다. 로그인에 성공하면 Cisco Secure Client는 기본적으로 XML 프로파일 다운로드를 시도합니다. 그러나 프로필이 GUI에 나타나려면 Cisco Secure Client를 다시 시작해야 합니다. Cisco Secure Client 창을 닫는 것만으로는 충분하지 않습니다. 프로세스를 다시 시작하려면 Windows 트레이에서 Cisco Secure Client 아이콘을 마우스 오른쪽 단추로 클릭하고 Quit 옵션을 선택합니다.

2. 연결이 설정되면 왼쪽 하단 모서리에 있는 기어 아이콘을 클릭하고 AnyConnect VPN > 통계로 이동합니다. 표시된 정보가 연결 및 주소 정보와 일치하는지 확인합니다.



Cisco Secure Client(AnyConnect) 통계

3. 다음으로 이동 AnyConnectVPN > 경로 세부 정보 표시된 정보가 보안 경로와 비보안 경로에 해당하는지 확인합니다.



Cisco Secure Client(AnyConnect) 경로 세부 정보

C8000v에서 컨피그레이션이 제대로 작동하는지 확인하려면 이 섹션을 사용합니다.

1. ssl 세션 정보를 표시하려면 - 암호화 ssl session{user user-name |profile profile-name}

<#root>

```
sal_c8kv#show crypto ssl session user test
```

Interface :

Virtual-Access1

Session Type : Full Tunnel

Client User-Agent : AnyConnect Windows 5.1.8.105

Username : test

Num Connection : 1

Public IP : 10.106.69.69

Profile :

ssl_prof

Policy :

ssl_policy

Last-Used : 00:41:40
Tunnel IP : 192.168.13.3
Rx IP Packets : 542

Created : *15:25:47.618 UTC Mon Mar 3 2025
Netmask : 0.0.0.0
Tx IP Packets : 410

sal_c8kv#show crypto ssl session profile ssl_prof

SSL profile name: ssl_prof

Client_Login_Name	Client_IP_Address	No_of_Connections	Created	Last_Used
cisco	10.106.69.69	1	00:49:41	00:49:41

2. ssl vpn 통계를 표시하려면 show crypto ssl stats [profile profile-name] [tunnel] [¶ detail]

<#root>

sal_c8kv#show crypto ssl stats tunnel profile ssl_prof

SSLVPN Profile name : ssl_prof

Tunnel Statistics:

Active connections	: 1		
Peak connections	: 1	Peak time	: 1d23h
Connect succeed	: 13	Connect failed	: 0
Reconnect succeed	: 0	Reconnect failed	: 0
IP Addr Alloc Failed	: 0	VA creation failed	: 0
DPD timeout	: 0		

Client

in CSTD frames	: 23	in CSTD control	: 23
in CSTD data	: 0	in CSTD bytes	: 872
out CSTD frames	: 11	out CSTD control	: 11
out CSTD data	: 0	out CSTD bytes	: 88
cef in CSTD data frames	: 0	cef in CSTD data bytes	: 0
cef out CSTD data frames	: 0	cef out CSTD 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

3. 클라이언트와 연결된 Virtual-Access 인터페이스에 적용된 실제 구성을 확인합니다.

```
<#root>
```

```
sal_c8kv#show derived-config interface Virtual-Access1
```

Building configuration...

Derived configuration : 143 bytes

!

```
interface Virtual-Access1
```

```
description ***Internally created by SSLVPN context ssl_prof***
```

```
ip unnumbered GigabitEthernet1
```

```
ip mtu 1400
```

```
end
```

문제 해결

이 섹션에서는 설정 문제 해결에 사용할 수 있는 정보를 제공합니다.

1. 헤드엔드와 클라이언트 간의 협상을 확인하기 위한 SSL 디버깅

```
<#root>
```

```
debug crypto ssl condition client 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 컨피그레이션을 확인하기 위한 몇 가지 추가 명령입니다.

```
# 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. Cisco Secure Client용 진단 및 보고 툴(DART)

DART 번들을 수집하려면 Run DART to Collect Data for Troubleshooting에 설명된 [단계를 수행합니다](#)

성공적인 연결의 샘플 디버깅:

```
debug crypto ssl
debug crypto ssl tunnel events
debug crypto ssl tunnel errors
```

<#root>

```
*Mar 3 16:47:11.141: CRYPTO-SSL: sslvpn process rcvd context queue event
*Mar 3 16:47:14.149: CRYPTO-SSL: Chunk data written..
buffer=0x726BCA8891B8 total_len=621 bytes=621 tcb=0x0
*Mar 3 16:47:15.948: %SSLVPN-5-LOGIN_AUTH_PASSED: vw_ctx: ssl_prof vw_gw: ssl_policy remote_ip: 10.106.
*Mar 3 16:47:15.948: %SEC_LOGIN-5-LOGIN_SUCCESS: Login Success [user: cisco] [Source: LOCAL] [localport
*Mar 3 16:47:15.949: CRYPTO-SSL: Chunk data written..
buffer=0x726BCA8891E0 total_len=912 bytes=912 tcb=0x0
*Mar 3 16:47:17.698: CRYPTO-SSL: sslvpn process rcvd context queue event
*Mar 3 16:47:20.755: [CRYPTO-SSL-TUNL-EVT]:[726BCA848AB0] CSTP Version recd , using 1
*Mar 3 16:47:20.755: [CRYPTO-SSL-TUNL-ERR]: IPv6 local addr pool not found
*Mar 3 16:47:20.755: [CRYPTO-SSL-TUNL-EVT]:[726BCA848AB0] No free IPv6 available, disabling IPv6
*Mar 3 16:47:20.755: [CRYPTO-SSL-TUNL-EVT]:[726BCA848AB0]
SSLVPN requesting a VA creation
*Mar 3 16:47:20.755: [CRYPTO-SSL-TUNL-EVT]:[726BCA848AB0] Per Tunnel Vaccess cloning 2 request sent
*Mar 3 16:47:20.760: %SYS-5-CONFIG_P: Configured programmatically by process VTEMPLATE Background Mgr f
*Mar 3 16:47:20.760: [CRYPTO-SSL-TUNL-EVT]:[0] VACCESS: Received VACCESS PER TUNL EVENT response.
*Mar 3 16:47:20.760: [CRYPTO-SSL-TUNL-EVT]:[726BCA848AB0] VACCESS: Received vaccess Virtual-Access1 from
*Mar 3 16:47:20.760: [CRYPTO-SSL-TUNL-EVT]:[726BCA848AB0] VACCESS: Cloning Per Tunnel Vaccess
*Mar 3 16:47:20.760: [CRYPTO-SSL-TUNL-EVT]:[726BCA848AB0] VACCESS: Interface Vi1 assigned to Session Us
*Mar 3 16:47:20.761: [CRYPTO-SSL-TUNL-EVT]:[726BCA848AB0] Allocating IP 192.168.13.4 from address-pool
*Mar 3 16:47:20.761: [CRYPTO-SSL-TUNL-EVT]:[726BCA848AB0] Using new allocated IP 192.168.13.4 0.0.0.0
*Mar 3 16:47:20.761: %LINK-3-UPDOWN: Interface Virtual-Access1, changed state to up
*Mar 3 16:47:20.763: [CRYPTO-SSL-TUNL-EVT]:[726BCA848AB0] Full Tunnel CONNECT request processed, HTTP r
*Mar 3 16:47:20.763: HTTP/1.1 200 OK
*Mar 3 16:47:20.763: Server: Cisco IOS SSLVPN
*Mar 3 16:47:20.763: X-CSTP-Version: 1
*Mar 3 16:47:20.763: X-CSTP-Address: 192.168.13.4
*Mar 3 16:47:20.763: X-CSTP-Netmask: 0.0.0.0
*Mar 3 16:47:20.763: X-CSTP-DNS: 192.168.11.100
*Mar 3 16:47:20.764: X-CSTP-Lease-Duration: 43200
*Mar 3 16:47:20.764: X-CSTP-MTU: 1406
*Mar 3 16:47:20.764: X-CSTP-Default-Domain: example.com
*Mar 3 16:47:20.764: X-CSTP-Split-Include: 192.168.11.0/255.255.255.0
*Mar 3 16:47:20.764: X-CSTP-Split-Include: 192.168.12.0/255.255.255.0
*Mar 3 16:47:20.764: X-CSTP-Split-Include: 192.168.11.0/255.255.255.0
*Mar 3 16:47:20.764: X-CSTP-Split-Include: 192.168.12.0/255.255.255.0
*Mar 3 16:47:20.765: X-CSTP-Rekey-Time: 3600
*Mar 3 16:47:20.765: X-CSTP-Rekey-Method: new-tunnel
*Mar 3 16:47:20.765: X-CSTP-DPD: 300
*Mar 3 16:47:20.765: X-CSTP-Disconnected-Timeout: 0
*Mar 3 16:47:20.765: X-CSTP-Idle-Timeout: 1800
*Mar 3 16:47:20.765: X-CSTP-Session-Timeout: 43200
*Mar 3 16:47:20.765: X-CSTP-Keepalive: 30
```

```
*Mar 3 16:47:20.765: X-CSTP-Smartcard-Removal-Disconnect: false
*Mar 3 16:47:20.766: X-CSTP-Include-Local_LAN: false
*Mar 3 16:47:20.766: [CRYPTO-SSL-TUNL-EVT]:[726BCA848AB0] For User cisco, DPD timer started for 300 sec
*Mar 3 16:47:20.766: CRYPTO-SSL: Chunk data written..
buffer=0x726BCA8891E0 total_len=693 bytes=693 tcb=0x0
*Mar 3 16:47:21.762:
```

%LINEPROTO-5-UPDOWN: Line protocol on Interface Virtual-Access1, changed state to up

관련 정보

- [Cisco 기술 지원 및 다운로드](#)

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.