ISE를 사용하여 AnyConnect FlexVPN에 대해 스플릿 제외 구성

목차

소개

이 문서에서는 Cisco IOS® XE 라우터에 대한 IKEv2 AnyConnect 연결을 위해 ISE를 사용하여 스플릿 제외를 구성하는 절차에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- 라우터의 AnyConnect IPsec 구성 경험
- Cisco ISE(Identity Services Engine) 컨피그레이션
- CSC(Cisco Secure Client)
- RADIUS 프로토콜

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco Catalyst 8000V(C8000V) - 17.12.04
- Cisco Secure Client - 5.0.02075
- Cisco ISE - 3.2.0
- Windows 10

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.

구성

네트워크 다이어그램

네트워크 다이어그램

설정

구성을 완료하려면 다음 섹션을 고려하십시오.

라우터 컨피그레이션

1. 디바이스에서 인증 및 로컬 권한 부여를 위해 RADIUS 서버를 구성합니다.

```
radius server ISE
 address ipv4 10.127.197.105 auth-port 1812 acct-port 1813
 timeout 120
 key cisco123

aaa new-model
aaa group server radius FlexVPN_auth_server
 server name ISE

aaa authentication login FlexVPN_auth group FlexVPN_auth_server
aaa authorization network a-eap-author-grp local
```

2. 라우터 인증서를 설치할 신뢰 지점을 구성합니다. 라우터의 로컬 인증 유형이 RSA이므로 디바이스에서 인증서를 사용하여 서버를 인증해야 합니다. 인증서 생성에 대한 자세한 내용은 PKI -1의 인증서 등록 및 PKI -2의 인증서 등록을 참조하십시오.

```
crypto pki trustpoint flex
 enrollment terminal
 ip-address none
 subject-name CN=flexserver.cisco.com
 revocation-check none
```

```
 rsakeypair flex1
 hash sha256
```

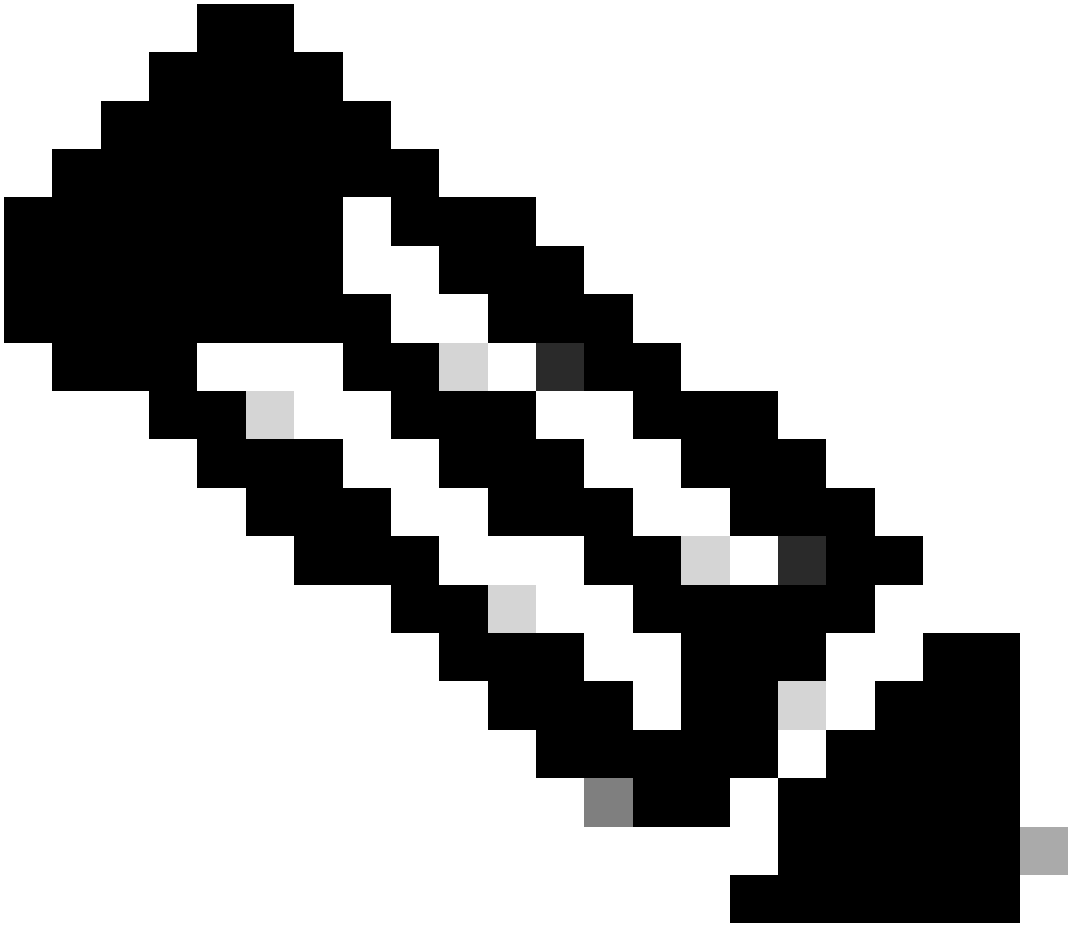
3. AnyConnect 연결이 성공하면 AnyConnect VPN 클라이언트에 주소를 할당하도록 IP 로컬 풀을 정의합니다.

```
ip local pool ACPOOL 172.16.10.5 172.16.10.30
```

4. IKEv2 로컬 권한 부여 정책을 생성합니다.

Radius 서버에서 푸시된 특성과 함께 이 정책에 정의된 특성이 사용자에게 적용됩니다

```
crypto ikev2 authorization policy ikev2-auth-policy
 pool ACPOOL
 dns 8.8.8.8
```



참고: 사용자 지정 IKEv2 권한 부여 정책이 구성되지 않은 경우 기본 권한 부여 정책인 default가 권한 부여에 사용됩니다. IKEv2 권한 부여 정책에 지정된 특성은 RADIUS 서버를 통해 푸시될 수도 있습니다. RADIUS 서버에서 split-exclude 특성을 푸시해야 합니다.

5(선택 사항). IKEv2 제안서 및 정책을 생성합니다(구성되지 않은 경우 스마트 기본값이 사용됨).

```
crypto ikev2 proposal IKEv2-prop1
 encryption aes-cbc-256
 integrity sha256
 group 19

crypto ikev2 policy IKEv2-pol
 proposal IKEv2-prop1
```

6(선택 사항). 변형 집합을 구성합니다(구성되지 않은 경우 스마트 기본값이 사용됨).

```
crypto ipsec transform-set TS esp-aes 256 esp-sha256-hmac
mode tunnel
```

7. 일부 더미 IP 주소로 루프백 인터페이스를 구성합니다. Virtual-Access 인터페이스는 다음과 같이 IP 주소를 차용합니다.

```
interface Loopback100
 ip address 10.0.0.1 255.255.255.255
```

8. 가상 액세스 인터페이스를 복제할 가상 템플릿을 구성합니다.

```
interface Virtual-Template100 type tunnel
 ip unnumbered Loopback100
 ip mtu 1400
```

9. AnyConnect 클라이언트 프로파일을 라우터의 부트플래시에 업로드하고 지정된 대로 프로파일을 정의합니다.

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

10. 모든 연결 관련 정보를 포함하는 IKEv2 프로필을 구성합니다.

```
crypto ikev2 profile prof1
 match identity remote key-id *$AnyConnectClient$*
 authentication local rsa-sig
 authentication remote eap query-identity
 pki trustpoint flex
 aaa authentication eap FlexVPN_auth
 aaa authorization group eap list a-eap-author-grp ikev2-auth-policy
 aaa authorization user eap cached
 virtual-template 100
 anyconnect profile acvpn
```

IKEv2 프로파일에서 사용됩니다.

- match identity remote key-id *$AnyConnectClient$* - 클라이언트의 ID를 나타냅니다. AnyConnect는 *$AnyConnectClient$*를 key-id 유형의 기본 IKE ID로 사용합니다. 그러나 AnyConnect 프로파일에서 이 ID를 수동으로 변경하여 배포 요구 사항을 일치시킬 수 있습니다.

- authentication remote - 클라이언트 인증에 EAP 프로토콜을 사용해야 함을 나타냅니다.
- authentication local - 로컬 인증에 인증서를 사용해야 함을 나타냅니다.
- aaa authentication eap - EAP 인증 중에 RADIUS serverFlexVPN_auth가 사용됩니다.
- aaa authorization group eap list - 권한 부여 중에 네트워크 목록 a-eap-author-grp가 권한 부여 policyikev2-auth-policy와 함께 사용됩니다.
- aaa authorization user eap cached - 암시적 사용자 권한 부여를 활성화합니다.
- virtual-template 100 - 복제할 가상 템플릿을 정의합니다.
- anyconnect 프로파일 acvpn - 9단계에 정의된 클라이언트 프로파일이 여기에 이 IKEv2 프로파일에 적용됩니다.

11. IPsec 프로필을 구성합니다.

```
crypto ipsec profile AnyConnect-EAP
 set transform-set TS
 set ikev2-profile prof1
```

12. 가상 템플릿에 IPsec 프로필을 추가합니다.

```
interface Virtual-Template100 type tunnel
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile AnyConnect-EAP
```

13. 라우터에서 HTTP-URL 기반 인증서 조회 및 HTTP 서버를 비활성화합니다.

```
no crypto ikev2 http-url cert
no ip http server
no ip http secure-server
```

14. SSL 정책을 구성하고 라우터의 WAN IP를 프로파일 다운로드를 위한 로컬 주소로 지정합니다.

```
crypto ssl policy ssl-server
 pki trustpoint flex sign
 ip address local 10.106.67.33 port 443

crypto ssl profile ssl_prof
 match policy ssl-server
```

AnyConnect 클라이언트 프로파일(XML 프로파일)의 코드 조각:

Cisco IOS XE 16.9.1 이전에는 헤드엔드에서 자동 프로파일 다운로드를 사용할 수 없습니다.

16.9.1을 게시하면 헤드엔드에서 프로필을 다운로드할 수 있습니다.

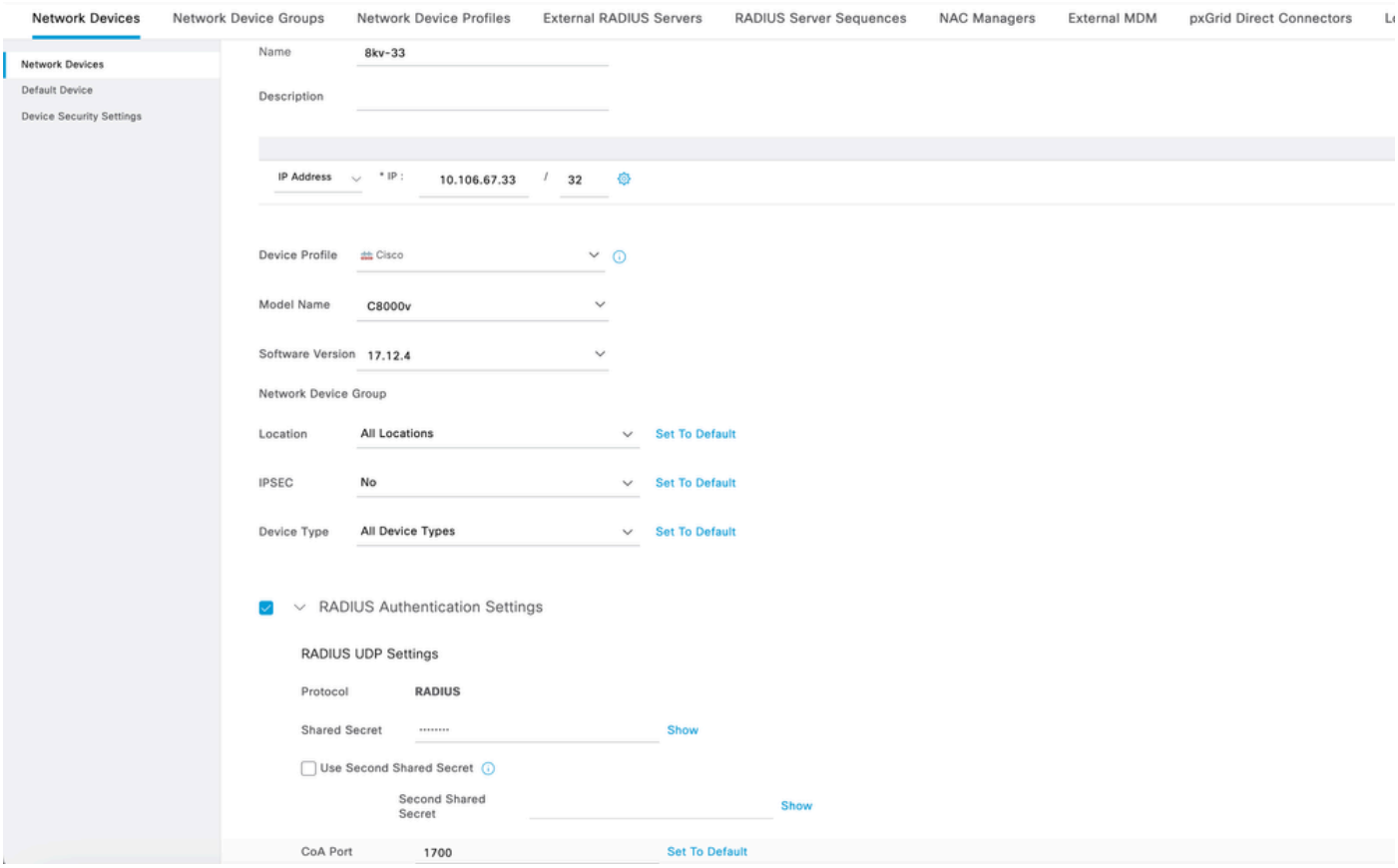
<#root>

```
<?xml version="1.0" encoding="UTF-8"?>
<AnyConnectProfile xmlns="http://schemas.xmlsoap/encoding/" xmlns:xsi="http://www.w3.org/2001/XMLSchema
<ClientInitialization>
<UseStartBeforeLogon UserControllable="true">false</UseStartBeforeLogon>
<AutomaticCertSelection UserControllable="true">false</AutomaticCertSelection>
<ShowPreConnectMessage>false</ShowPreConnectMessage>
<CertificateStore>All</CertificateStore>
<CertificateStoreMac>All</CertificateStoreMac>
<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>
<DisableCaptivePortalDetection UserControllable="true">false</DisableCaptivePortalDetection>
<ClearSmartcardPin UserControllable="true">true</ClearSmartcardPin>
<IPProtocolSupport>IPv4,IPv6</IPProtocolSupport>
<AutoReconnect UserControllable="false">true
<AutoReconnectBehavior UserControllable="false">ReconnectAfterResume</AutoReconnectBehavior>
</AutoReconnect>
<AutoUpdate UserControllable="false">true</AutoUpdate>
<RSASecurIDIntegration UserControllable="false">Automatic</RSASecurIDIntegration>
<WindowsLogonEnforcement>SingleLocalLogon</WindowsLogonEnforcement>
<WindowsVPNEstablishment>AllowRemoteUsers</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>
<AllowManualHostInput>true</AllowManualHostInput>
</ClientInitialization>
<ServerList>
<HostEntry>

<HostName>

Flex

</HostName>
<HostAddress>

flexserver.cisco.com

</HostAddress>
<PrimaryProtocol>IPsec
<StandardAuthenticationOnly>true
<AuthMethodDuringIKENegotiation>

EAP-MD5

</AuthMethodDuringIKENegotiation>
```

```
</StandardAuthenticationOnly>
</PrimaryProtocol>
</HostEntry>
</ServerList>
</AnyConnectProfile>
```

ISE(Identity Services Engine) 컨피그레이션

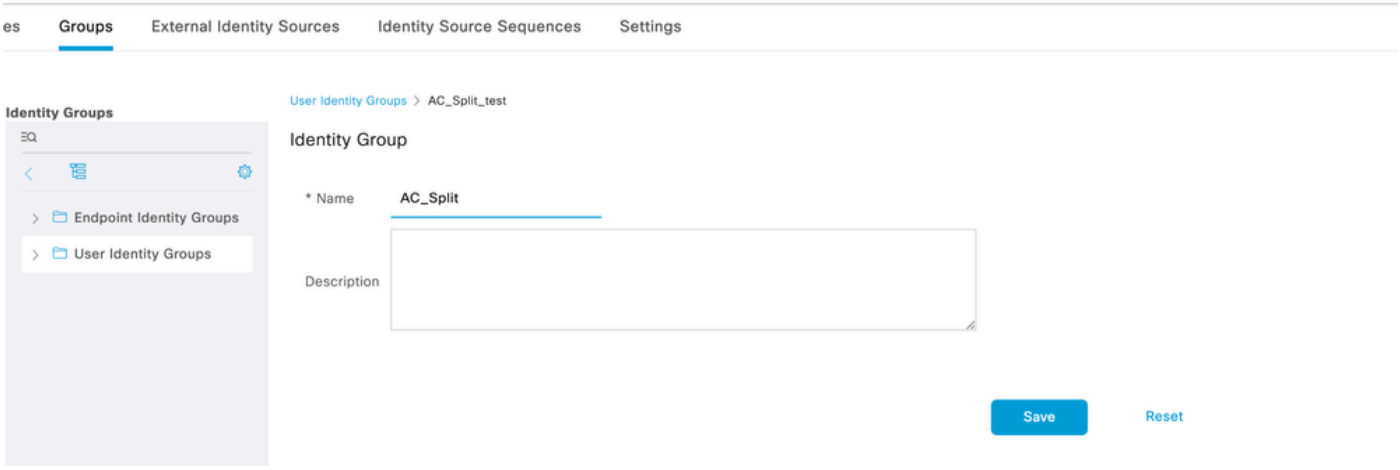
1. 라우터를 ISE의 유효한 네트워크 디바이스로 등록하고 RADIUS에 대한 공유 비밀 키를 구성합니다. 이를 위해 Administration(관리) > Network Resources(네트워크 리소스) > Network Devices(네트워크 디바이스)로 이동합니다. Add(추가)를 클릭하여 라우터를 AAA 클라이언트로 구성합니다.



네트워크 디바이스 추가

2. ID 그룹을 생성합니다.

비슷한 특성을 가진 사용자와 비슷한 권한을 공유하는 사용자를 연결하도록 ID 그룹을 정의합니다. 다음 단계에서 사용됩니다. Administration(관리) > Identity Management(ID 관리) > Groups(그룹) > User Identity Groups(사용자 ID 그룹)로 이동한 다음 Add(추가)를 클릭합니다.



ID 그룹 생성

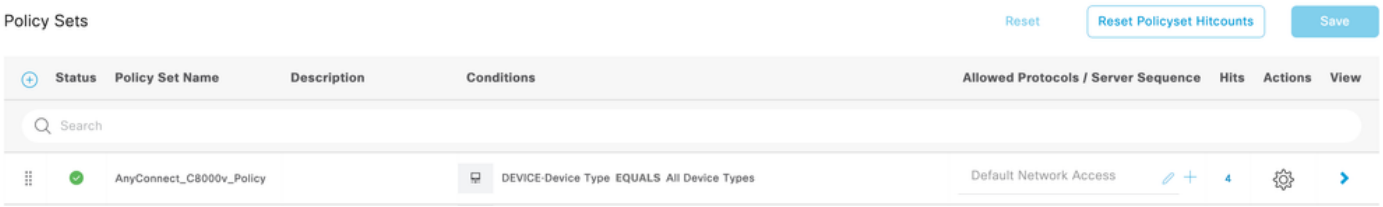
3. 사용자를 ID 그룹에 연결:

사용자를 올바른 ID 그룹에 연결합니다. Administration(관리) > Identity Management(ID 관리) > Identities(ID) > Users(사용자)로 이동합니다.

ID 그룹에 사용자 추가

4. 정책 집합 만들기:

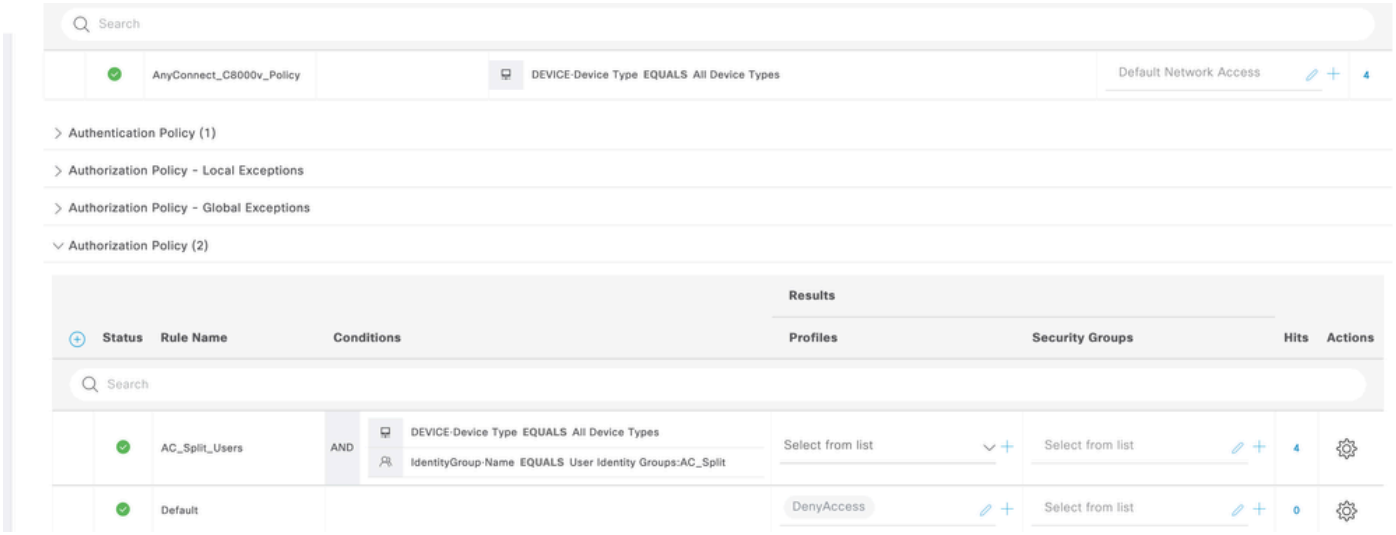
새 정책 집합을 정의하고 정책과 일치하는 조건을 정의합니다. 이 예에서는 모든 디바이스 유형이 조건에서 허용됩니다. 이렇게 하려면 Policy>Policy sets로 이동합니다.



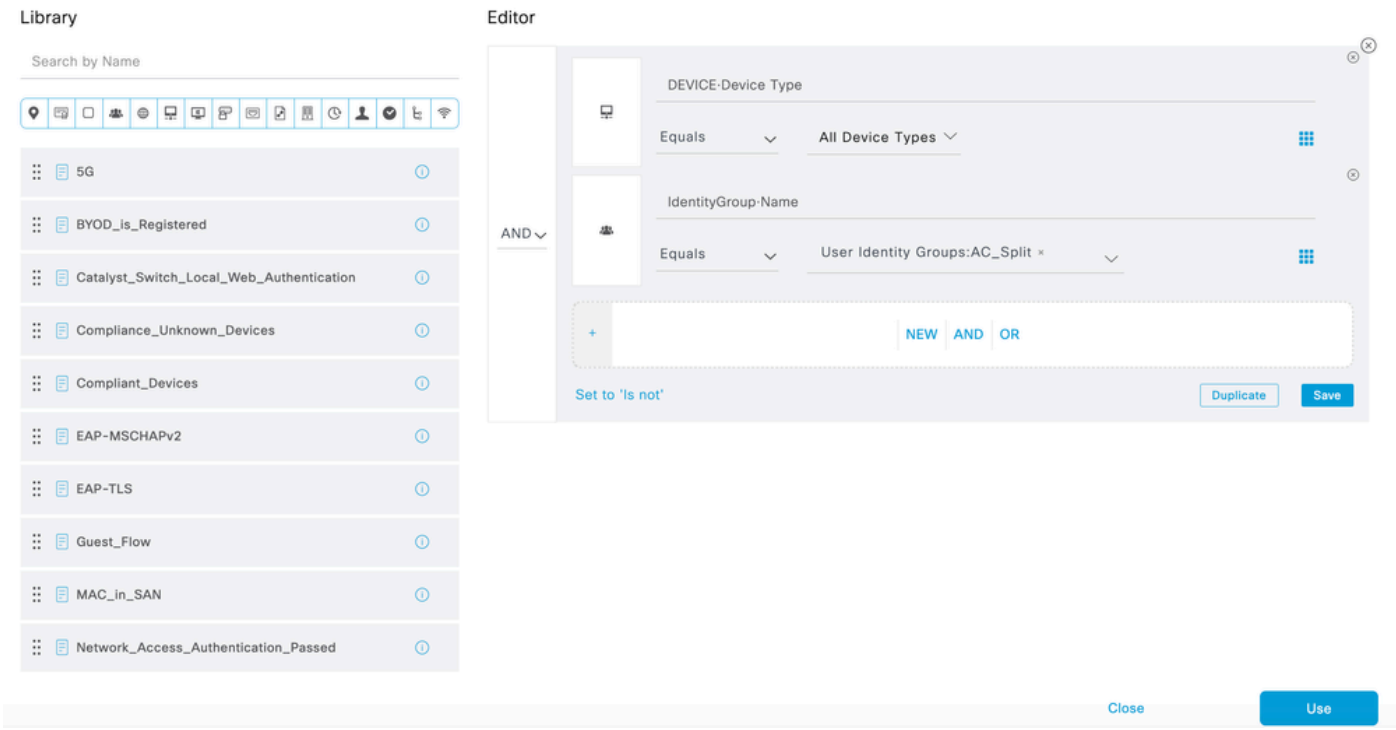
정책 집합 생성

5. 권한 부여 정책을 생성합니다.

정책과 일치하는 필수 조건으로 새 권한 부여 정책을 정의합니다. 2단계에서 생성한 ID 그룹을 조건으로 포함해야 합니다.



권한 부여 정책 생성

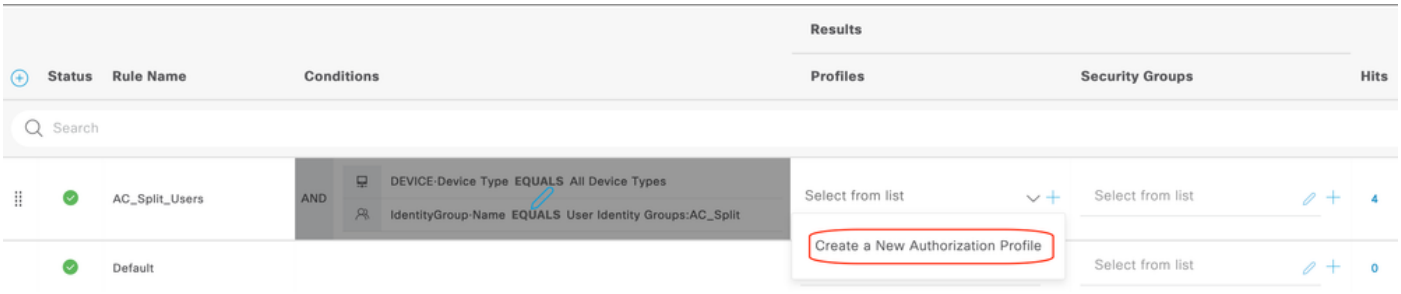


권한 부여 정책에서 조건 선택

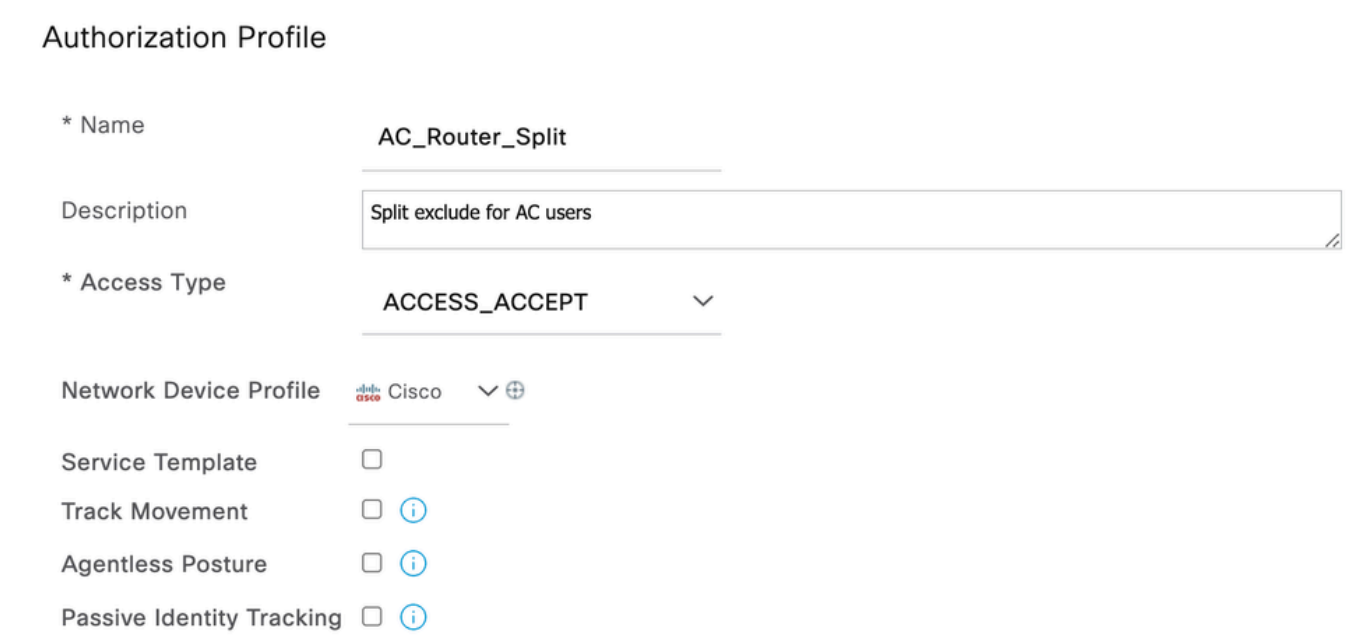
6. 권한 부여 프로파일을 생성합니다.

권한 부여 프로파일에는 권한 부여 정책이 일치할 때 수행되는 작업이 포함됩니다. 다음 특성을 포함하는 새 권한 부여 프로파일을 만듭니다.

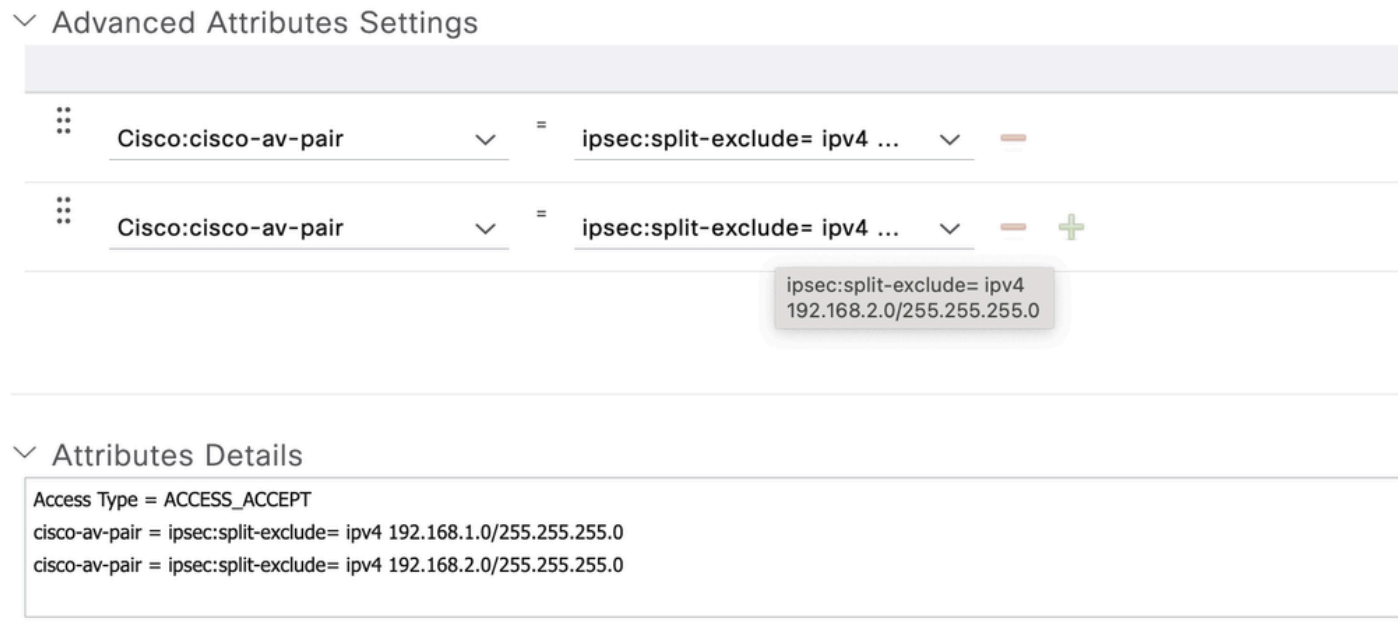
액세스 유형 = ACCESS_ACCEPT
cisco av 쌍 = ipsec: split-exclude= ipv4 <ip_network>/<subnet_mask>



새 권한 부여 프로파일 생성

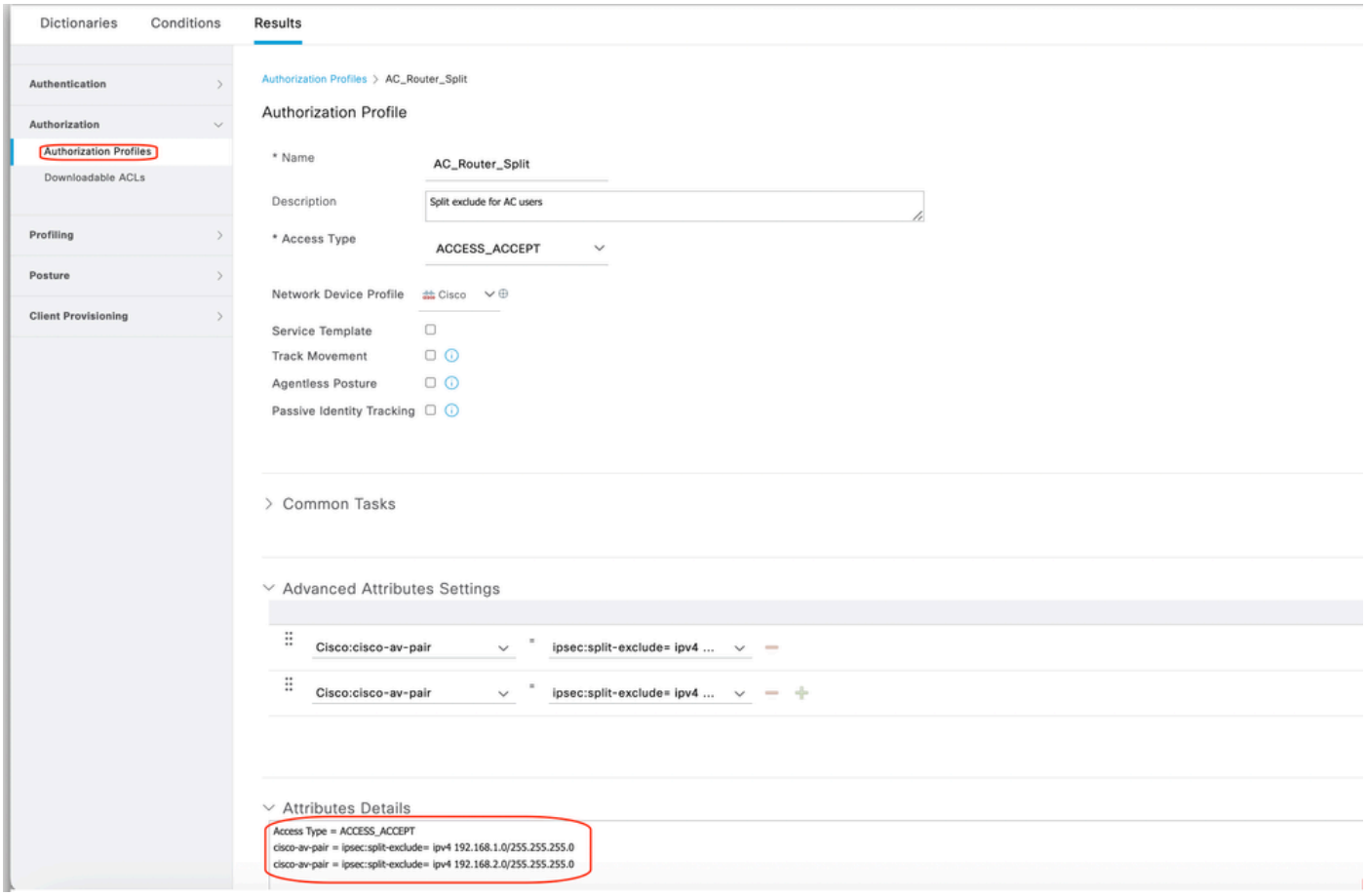


권한 부여 프로파일 구성



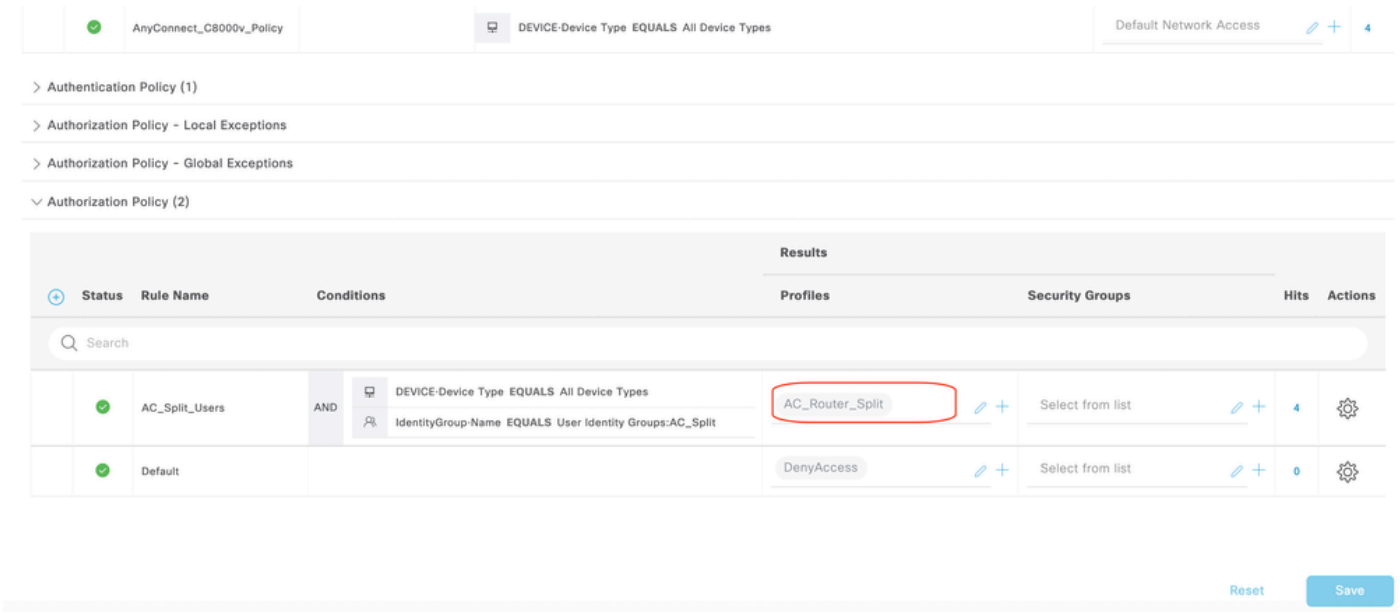
권한 부여 프로파일의 특성 구성

7. 권한 부여 프로파일 구성을 검토합니다.



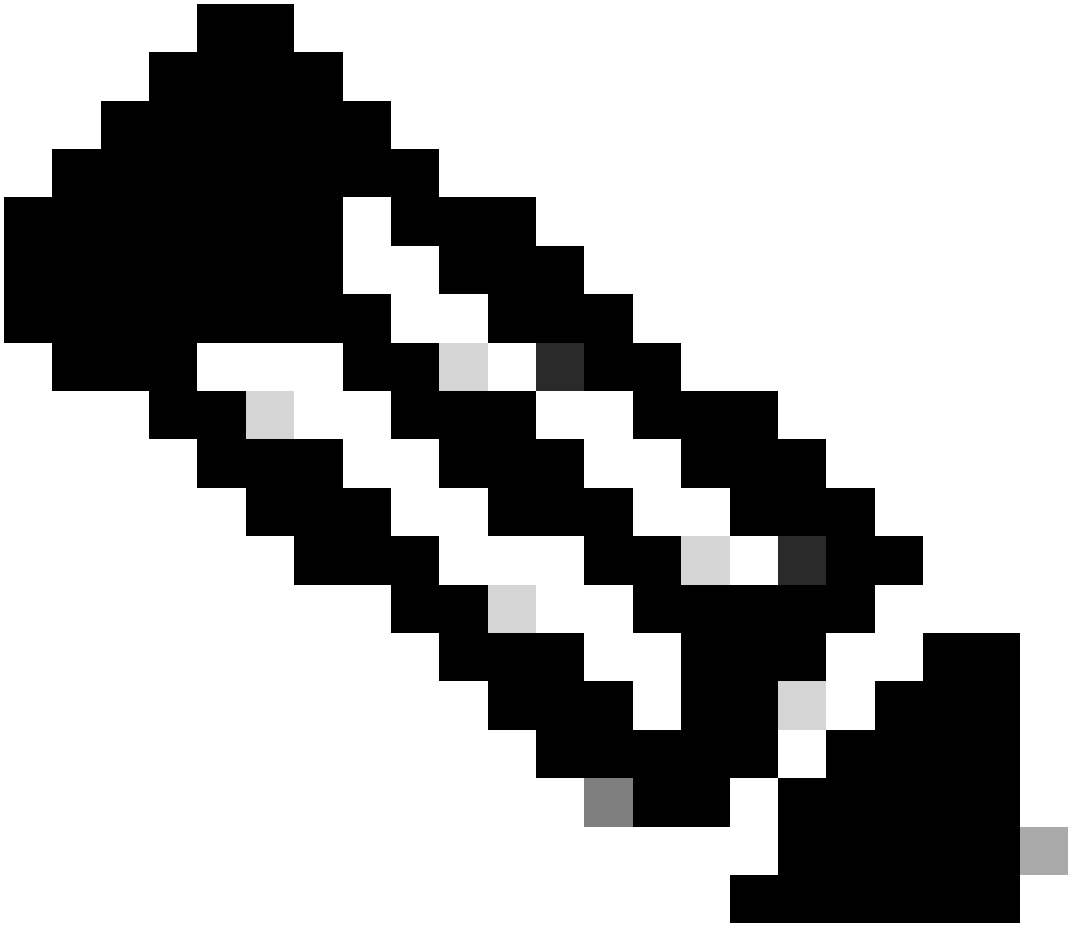
인증 프로파일 구성 검토

8. 이것은 필수 프로파일을 선택 한 후 정책 집합 구성의 권한 부여 정책 입니다.



최종 권한 부여 정책 구성

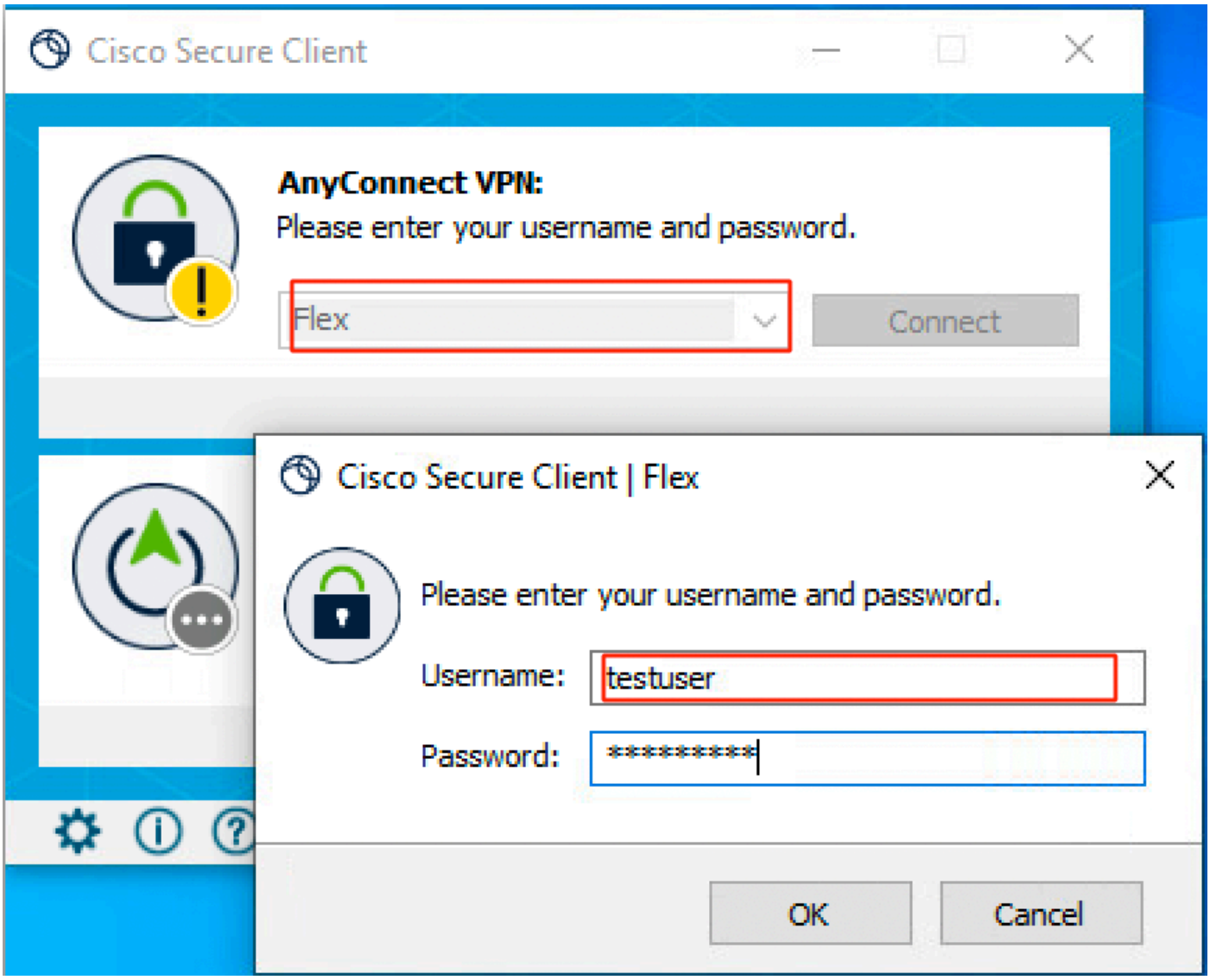
이 컨피그레이션 예에서는 사용자가 속한 ID 그룹을 기반으로 ISE 컨피그레이션을 통해 VPN을 통과하는 네트워크에서 제외할 수 있습니다.



참고: RA VPN 연결에 Cisco IOS XE 헤드엔드를 사용할 경우 스플릿 제외 서브넷을 클라이언트 PC에 하나만 푸시할 수 있습니다. 이 문제는 Cisco 버그 ID CSCwj38106에서 해결되었으며 여러 스플릿 제외 서브넷을 17.12.4에서 푸시할 수 있습니다. 고정 버전에 대한 자세한 내용은 버그를 참조하십시오.

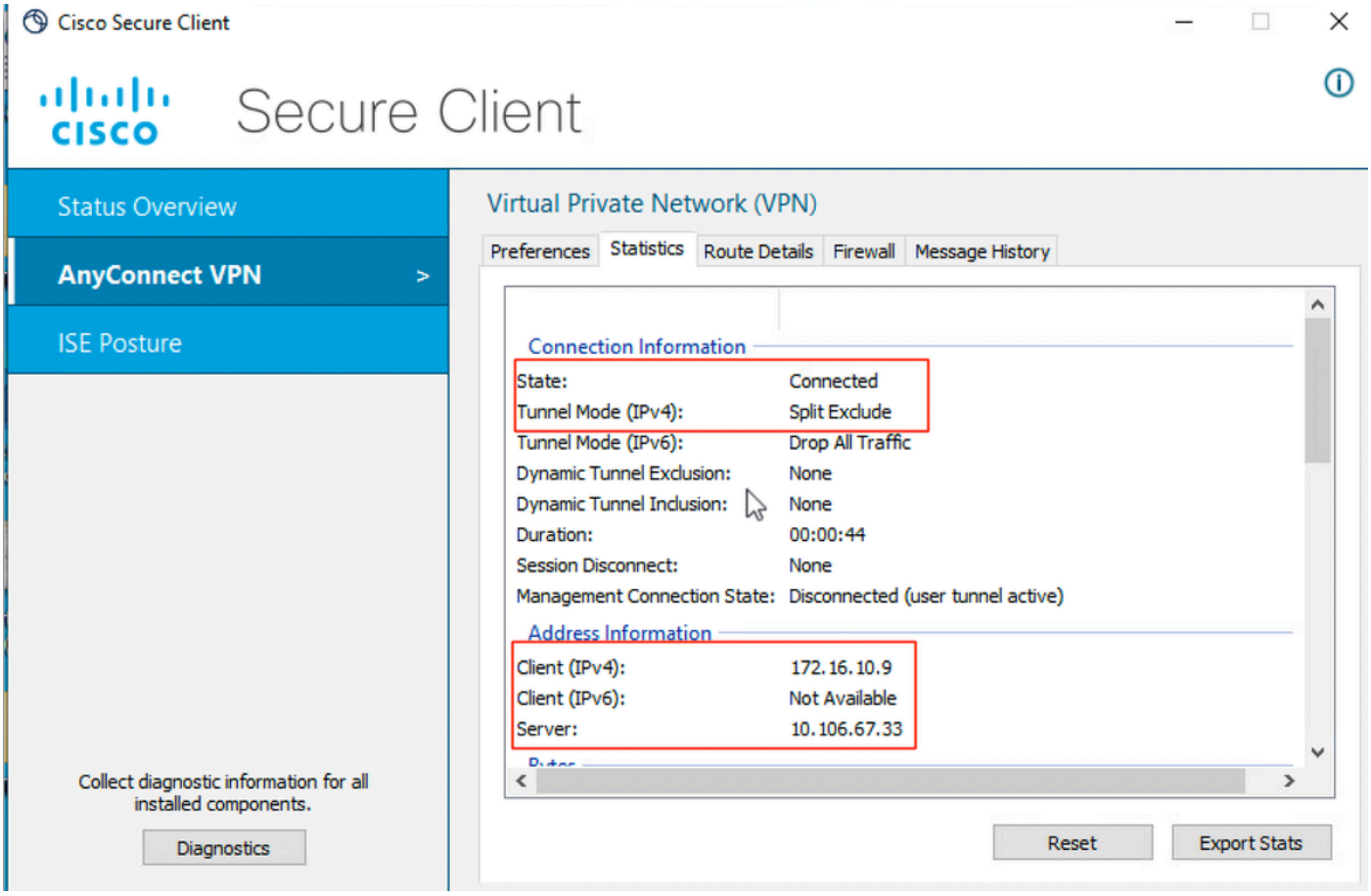
다음을 확인합니다.

1. 인증을 테스트하려면 AnyConnect를 통해 사용자의 PC에서 C8000V에 연결하고 자격 증명을 입력합니다.



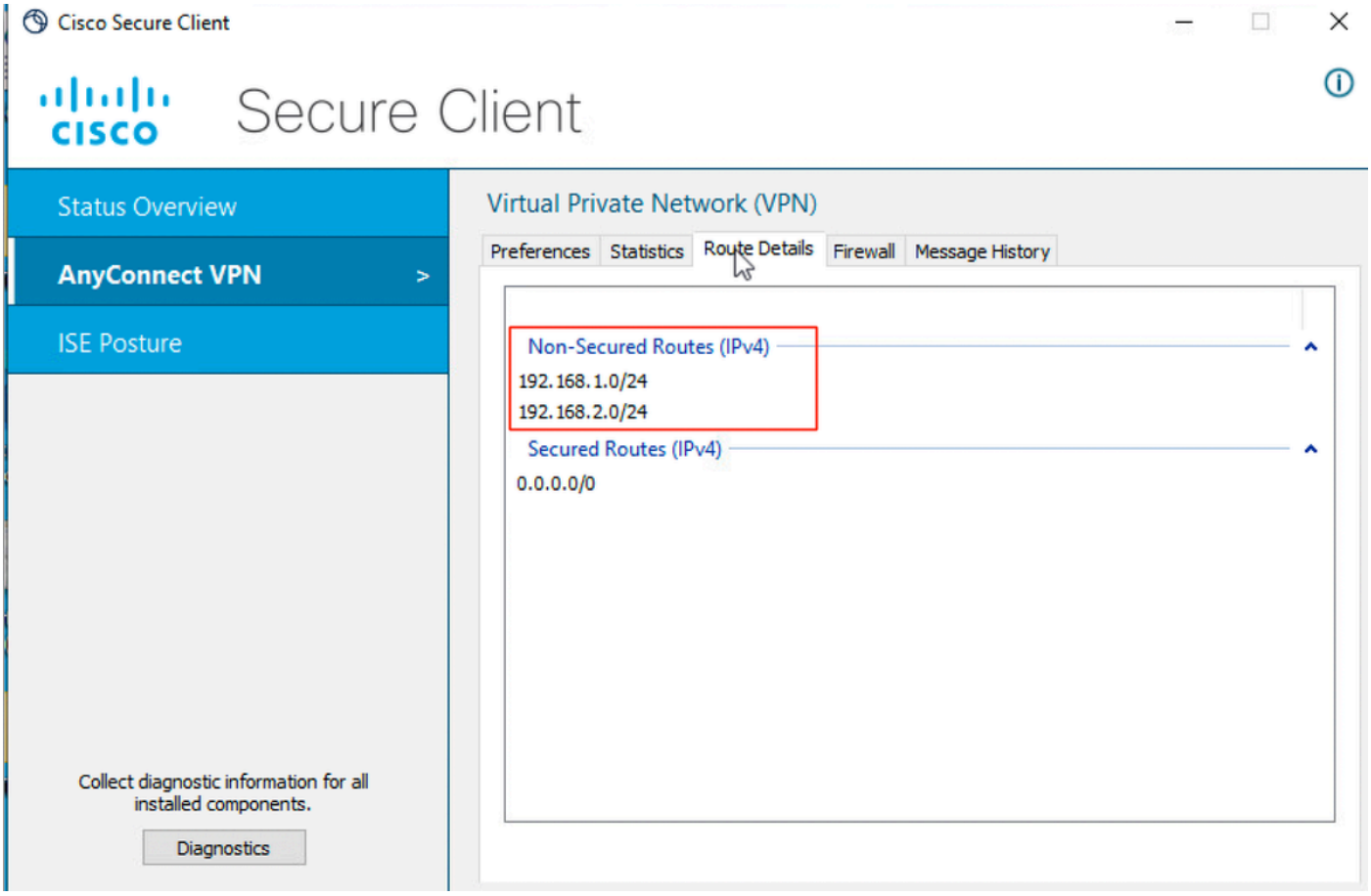
AnyConnect에 로그인

2. 연결이 설정되면 기어 아이콘(왼쪽 하단 모서리)을 클릭하고 AnyConnectVPN(AnyConnectVPN) > Statistics(통계)로 이동합니다. 스플릿 제외할 터널 모드를 확인합니다.



통계 검증

AnyConnectVPN > Route details(경로 세부사항)로 이동하고 표시되는 정보가 보안 경로 및 비보안 경로에 해당하는지 확인합니다.



경로 세부사항 확인

VPN 헤드엔드에서 연결 세부사항을 확인할 수도 있습니다.

1. IKEv2 parameters

<#root>

8kv#

show crypto ikev2 sa detail

IPv4 Crypto IKEv2 SA

Tunnel-id Local Remote fvrf/ivrf Status

1 10.106.67.33/4500 10.106.50.91/55811 none/none READY

Encr: AES-CBC, keysize: 256, PRF: SHA256, Hash: SHA256, DH Grp:19, Auth sign: RSA, Auth verify: EAP

Life/Active Time: 86400/22 sec

CE id: 1012, Session-id: 6

Local spi: E8C6C5EEF0F0EF72 Remote spi: 7827644A7CA8F1A5

Status Description: Negotiation done

Local id: 10.106.67.33

Remote id: *$AnyConnectClient$*

Remote EAP id: testuser

Local req msg id: 0 Remote req msg id: 6

Local next msg id: 0 Remote next msg id: 6

Local req queued: 0 Remote req queued: 6

Local window: 5 Remote window: 1

DPD configured for 0 seconds, retry 0

Fragmentation not configured.

Dynamic Route Update: disabled

Extended Authentication configured.

NAT-T is detected outside

Cisco Trust Security SGT is disabled

Assigned host addr: 172.16.10.10

Initiator of SA : No

Post NATed Address : 10.106.67.33

PEER TYPE: Other

IPv6 Crypto IKEv2 SA

2 .This is the crypto session detail for the VPN session:

<#root>

8kv#

show crypto session detail

Crypto session current status

Code: C - IKE Configuration mode, D - Dead Peer Detection

K - Keepalives, N - NAT-traversal, T - cTCP encapsulation

X - IKE Extended Authentication, F - IKE Fragmentation

R - IKE Auto Reconnect, U - IKE Dynamic Route Update

S - SIP VPN

Interface: Virtual-Access1

Profile: prof1

Uptime: 00:00:44

Session status: UP-ACTIVE

Peer: 10.106.50.91 port 55811 fvrf: (none) ivrf: (none)

```
Phase1_id: *$AnyConnectClient$*

Desc: (none)

Session ID: 16

IKEv2 SA: local 10.106.67.33/4500 remote 10.106.50.91/55811 Active

Capabilities:NX connid:1 lifetime:23:59:16

IPSEC FLOW: permit ip 0.0.0.0/0.0.0.0 host 172.16.10.10

Active SAs: 2, origin: crypto map

Inbound: #pkts dec'ed 114 drop 0 life (KB/Sec) 4607987/3556

Outbound: #pkts enc'ed 96 drop 0 life (KB/Sec) 4608000/3556
```

3. Verify on ISE live logs.

문제 해결

Cisco 라우터:

1. IKEv2 및 IPsec 디버그를 사용하여 헤드엔드와 클라이언트 간의 협상을 확인합니다.

```
debug crypto condition peer ipv4 <public_ip>
debug crypto ikev2
debug crypto ikev2 packet
debug crypto ikev2 error
debug crypto ikev2 internal
debug crypto ipsec
debug crypto ipsec error
```

2. 로컬 및/또는 원격 특성의 할당을 확인하려면 AAA 디버그를 사용합니다.

```
debug aaa authorization
```

```
debug aaa authentication
debug radius authentication
```

ISE의 경우:

Operations(운영) > Live logs(라이브 로그)로 이동하여 RADIUS 라이브 로그를 사용합니다.

작업 시나리오

성공적인 연결의 디버그:

<#root>

```
*Oct 13 10:01:25.928: RADIUS/ENCODE(0000012D):Orig. component type = VPN IPSEC
*Oct 13 10:01:25.929: RADIUS/ENCODE(0000012D): dropping service type, "radius-server attribute 6 on-for
*Oct 13 10:01:25.929: RADIUS(0000012D): Config NAS IP: 0.0.0.0
*Oct 13 10:01:25.929: vrfid: [65535] ipv6 tableid : [0]
*Oct 13 10:01:25.929: idb is NULL
*Oct 13 10:01:25.929: RADIUS(0000012D): Config NAS IPv6: ::
*Oct 13 10:01:25.929: RADIUS/ENCODE(0000012D): acct_session_id: 4291
*Oct 13 10:01:25.929: RADIUS(0000012D): sending
*Oct 13 10:01:25.929: RADIUS/ENCODE: Best Local IP-Address 10.106.67.33 for Radius-Server 10.127.197.10
*Oct 13 10:01:25.929: RADIUS: Message Authenticator encoded
*Oct 13 10:01:25.929: RADIUS(0000012D): Send Access-Request to 10.127.197.105:1812 id 1645/24, len 344
RADIUS: authenticator 85 AC BF 77 BF 42 0B C7 - DE 85 A3 9A AF 40 E5 DC
*Oct 13 10:01:25.929: RADIUS: Service-Type [6] 6 Login [1]
*Oct 13 10:01:25.929: RADIUS: Vendor, Cisco [26] 26
*Oct 13 10:01:25.929: RADIUS: Cisco AVpair [1] 20 "service-type=Login"
*Oct 13 10:01:25.929: RADIUS: Vendor, Cisco [26] 45
*Oct 13 10:01:25.929: RADIUS: Cisco AVpair [1] 39 "isakmp-phase1-id=*$AnyConnectClient$*"
*Oct 13 10:01:25.929: RADIUS: Calling-Station-Id [31] 14 "10.106.50.91"
*Oct 13 10:01:25.929: RADIUS: Vendor, Cisco [26] 64
*Oct 13 10:01:25.929: RADIUS: Cisco AVpair [1] 58 "audit-session-id=L2L40A6A4321ZO2L40A6A325BZH1194CC58
*Oct 13 10:01:25.929: RADIUS: User-Name [1] 10 "testuser"
*Oct 13 10:01:25.929: RADIUS: Vendor, Cisco [26] 21
*Oct 13 10:01:25.929: RADIUS: Cisco AVpair [1] 15 "coa-push=true"
*Oct 13 10:01:25.929: RADIUS: EAP-Message [79] 24
RADIUS: 02 8E 00 16 04 10 8A 09 BB 0D 4B A9 D6 2B 59 1C C8 FE 1C 90 56 F5 [ K+YV]
*Oct 13 10:01:25.929: RADIUS: Message-Authenticato[80] 18
RADIUS: 54 85 1B AC BE A8 DA EF 24 AE 4D 28 46 32 8C 48 [ T$M(F2H]
*Oct 13 10:01:25.929: RADIUS: State [24] 90
RADIUS: 35 32 43 50 4D 53 65 73 73 69 6F 6E 49 44 3D 4C [52CPMSessionID=L]
RADIUS: 32 4C 34 30 41 36 41 34 33 32 31 5A 4F 32 4C 34 [2L40A6A4321ZO2L4]
RADIUS: 30 41 36 41 33 32 35 42 5A 48 31 31 39 34 43 43 [0A6A325BZH1194CC]
RADIUS: 35 38 5A 4E 31 32 3B 33 30 53 65 73 73 69 6F 6E [58ZN12;30Session]
RADIUS: 49 44 3D 69 73 65 2D 70 73 6E 2F 35 31 37 31 33 [ID=ise-psn/51713]
RADIUS: 35 39 30 30 2F 33 38 3B [ 5900/38;]
*Oct 13 10:01:25.929: RADIUS: NAS-IP-Address [4] 6 10.106.67.33
*Oct 13 10:01:25.929: RADIUS(0000012D): Sending a IPv4 Radius Packet
*Oct 13 10:01:25.929: RADIUS(0000012D): Started 120 sec timeout
*Oct 13 10:01:25.998: RADIUS: Received from id 1645/24 10.127.197.105:1812, Access-Accept, len 239
RADIUS: authenticator BC 19 F2 EE 10 67 80 C5 - 9F D9 30 9A EA 7E 5E D3
```

```
*Oct 13 10:01:25.998: RADIUS: User-Name [1] 10 "testuser"
*Oct 13 10:01:25.998: RADIUS: Class [25] 67
RADIUS: 43 41 43 53 3A 4C 32 4C 34 30 41 36 41 34 33 32 [CACS:L2L40A6A432]
RADIUS: 31 5A 4F 32 4C 34 30 41 36 41 33 32 35 42 5A 48 [1ZO2L40A6A325BZH]
RADIUS: 31 31 39 34 43 43 35 38 5A 4E 31 32 3A 69 73 65 [1194CC58ZN12:ise]
RADIUS: 2D 70 73 6E 2F 35 31 37 31 33 35 39 30 30 2F 33 [-psn/517135900/3]
RADIUS: 38 [ 8]
*Oct 13 10:01:25.998: RADIUS: EAP-Message [79] 6
RADIUS: 03 8E 00 04
*Oct 13 10:01:25.998: RADIUS: Message-Authenticato[80] 18
RADIUS: F9 61 C1 FD 6D 26 31 A2 89 04 72 BC DD 32 A9 29 [ am&1r2)]
*Oct 13 10:01:25.998: RADIUS: Vendor, Cisco [26] 59
*Oct 13 10:01:25.998: RADIUS: Cisco AVpair [1] 53 "ipsec:split-exclude= ipv4 192.168.1.0/255.255.255.0"

*Oct 13 10:01:25.998: RADIUS: Vendor, Cisco [26] 59
*Oct 13 10:01:25.998: RADIUS: Cisco AVpair [1] 53 "ipsec:split-exclude= ipv4 192.168.2.0/255.255.255.0"

*Oct 13 10:01:25.998: RADIUS(00000012D): Received from id 1645/24
RADIUS/DECODE: EAP-Message fragments, 4, total 4 bytes
8kv#
```

참조

- 로컬 사용자 데이터베이스를 사용하여 IKEv2 원격 액세스를 위한 FlexVPN Headend 구성
- EAP 및 DUO 인증을 사용하여 AnyConnect Flexvpn 구성
- EAP-MD5로 AnyConnect IKEv2 원격 액세스 구성

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.