ISE 통합으로 FlexVPN 구성

목차

소개

이 문서에서는 Cisco ISE(Identity Services Engine)를 사용하여 구성을 스포크에 동적으로 할당하도록 FlexVPN을 구성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco ISE(Identity Services Engine) 컨피그레이션
- RADIUS 프로토콜
- Flex Virtual Private Network(FlexVPN)

사용되는 구성 요소

이 문서는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco CSR1000V(VXE) - 버전 17.03.04a
- Cisco ISE(Identity Services Engine) - 3.1

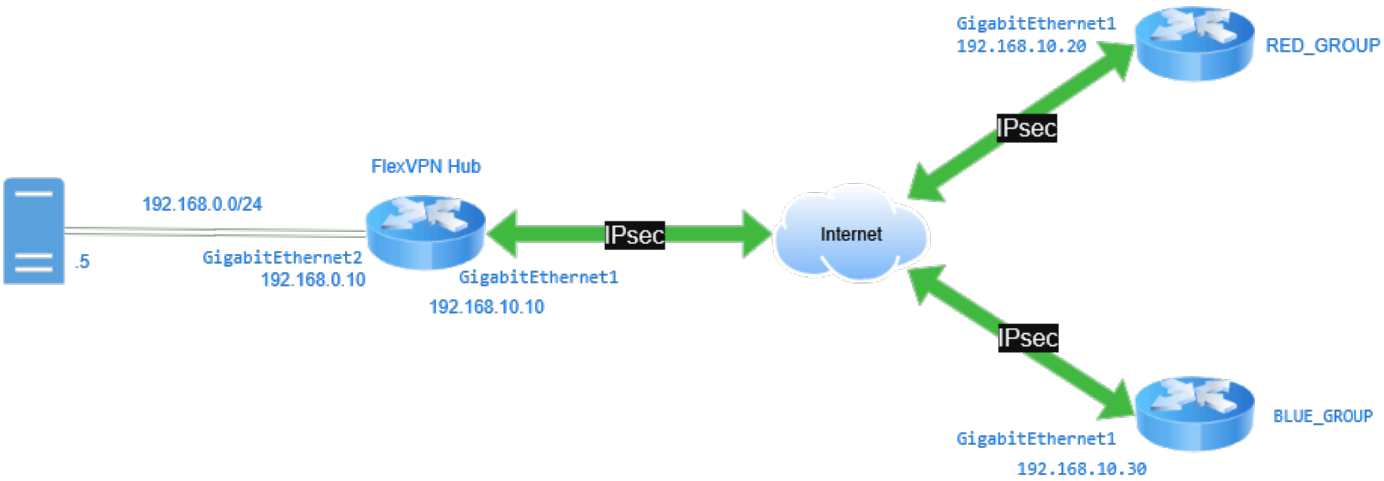
이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든

명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

구성

네트워크 다이어그램

FlexVPN은 스포크와 연결을 설정하고 통신 및 트래픽 관리를 지원하는 특정 컨피그레이션을 할당할 수 있습니다. 다이어그램에서 참조된 이 데모는 스포크가 HUB에 연결될 때 터널 소스 및 DHCP 풀의 매개변수가 스포크가 속한 그룹 또는 분기에 따라 지정되도록 FlexVPN이 ISE와 통합되는 방법을 보여 줍니다. 인증서를 사용하여 스포크를 인증한 다음 권한 부여 및 계정 관리 서버로 Radius를 사용하는 ISE를 인증합니다.



FlexVPN with ISE 통합

1단계: 허브 컨피그레이션

a. 라우터 인증서trustpoint를 저장하도록 를 구성합니다. 인증서는 스포크를 인증하는 데 사용됩니다.

```
crypto pki trustpoint FlexVPNCA
  enrollment url http://10.10.10.10:80
  subject-name cn=FlexvpnServer, o=Cisco, OU=IT_GROUP
  revocation-check crl
```

b. 를 **certificate map**구성합니다. 의 목적certificate map은 라우터에 여러 인증서가 설치된 경우 지정된 정보를 기반으로 인증서를 식별하고 매칭하는 것입니다.

```
crypto pki certificate map CERT_MAP 5
  issuer-name co ca-server.cisco.com
```

c. 디바이스에서RADIUS server권한 부여 및 어카운팅을 위해 를 구성합니다.

```
aaa new-model
!
aaa authorization network FLEX group ISE
aaa accounting network FLEX start-stop group ISE
```

d. RADIUS **RADIUS server group** 트래픽에 대한 IP 주소, 통신 포트, 공유 키 및 소스 인터페이스를 사용하여 를 정의합니다.

```
radius server ISE25
  address ipv4 192.168.0.5 auth-port 1645 acct-port 1646
  key cisco1234

aaa group server radius ISE
  server name ISE25
  ip radius source-interface g2
```

e. 를 **loopback interfaces**구성합니다. 는 loopback interfaces 터널의 소스 연결로 사용되며 연결된 그룹에 따라 동적으로 할당됩니다.

```
interface Loopback100
description RED TUNNEL SOURCE
ip address 10.100.100.1 255.255.255.255
!
interface Loopback200
description BLUE TUNNEL SOURCE
ip address 10.200.200.1 255.255.255.255
```

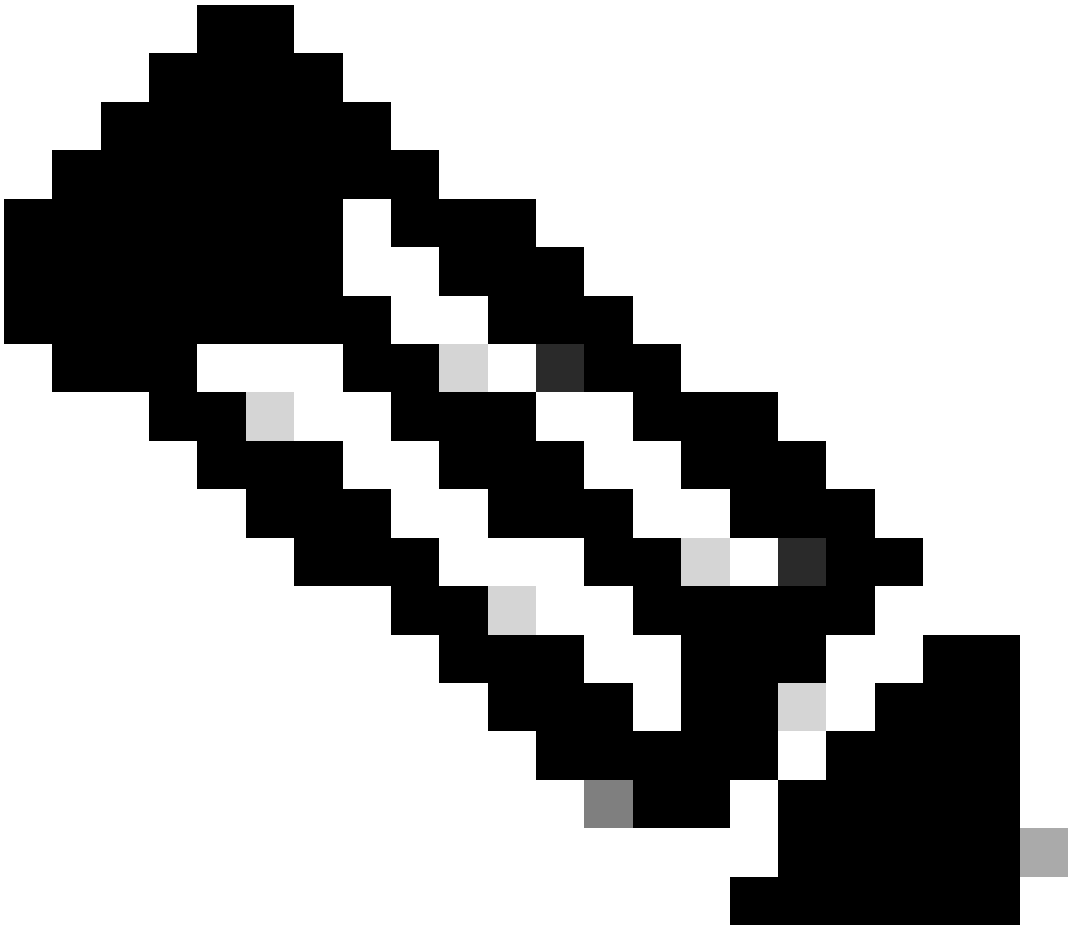
f. 각 그룹에 **IP local pool** 대한 을 정의합니다.

```
ip local pool RED_POOL 172.16.10.10 172.16.10.254
ip local pool BLUE_POOL 172.16.0.10 172.16.0.254
```

g. EIGRP를 구성하고 각 그룹의 네트워크를 광고합니다.

```
router eigrp Flexvpn
address-family ipv4 unicast autonomous-system 10
topology base
exit-af-topology
network 10.100.100.0 0.0.0.255
network 10.10.1.0 0.0.0.255
network 10.200.200.0 0.0.0.255
network 10.10.2.0 0.0.0.255
```

```
network 172.16.0.0
```



참고: FlexVPN은 OSPF, EIGRP, BGP over VPN 터널과 같은 동적 라우팅 프로토콜을 지원합니다. 이 가이드에서는 EIGRP가 사용되고 있습니다.

---

h. 를 **crypto ikev2 name mangler**구성합니다. 는 IKEv2 name mangler IKEv2 권한 부여를 위한 사용자 이름을 파생시키는 데 사용됩니다. 이 경우 스포크에 있는 인증서의 Organization-Unit 정보를 권한 부여를 위한 사용자 이름으로 사용하도록 구성됩니다.

```
crypto ikev2 name-mangler NM
dn organization-unit
```

i. 를 **IKEv2 profile**구성합니다. IKEv2 프로파일에서 certificate map, AAA server group 및 name mangler 이 참조됩니다.

이 특정 시나리오에서 로컬 및 원격 인증**RSA-SIG**은 다음과 같이 구성됩니다.

로컬 사용자 계정은 (아래 RADIUS server 컨피그레이션에 지정된 대로) 값 및 비밀번호와organization-unit일치하는Cisco1234사용자 이름으로에서 생성해야 합니다.

```
crypto ikev2 profile Flex_PROFILE
match certificate CERT_MAP
identity local dn
authentication remote rsa-sig
authentication local rsa-sig
pki trustpoint FlexVPNCA
dpd 10 2 periodic
aaa authorization group cert list FLEX name-mangler NM password Cisco1234
aaa accounting cert FLEX
virtual-template 1 mode auto
```

j. 를IPsec profile구성하고 를 IKEv2 profile참조합니다.

```
crypto ipsec profile IPSEC_FlexPROFILE
set ikev2-profile Flex_PROFILE
```

k. 를 virtual-template생성합니다. 를 생성하고 생성된 를 virtual-access interface 연결하는 데 IPsec profile 사용됩니다.

에서 **virtual-template** 할당한 대로 IP 주소가 없는 로 설정합니다RADIUS server.

```
interface Virtual-Template2 type tunnel
no ip address
tunnel source GigabitEthernet1
tunnel destination dynamic
tunnel protection ipsec profile IPSEC_FlexPROFILE
```

내부 네트워크를 시뮬레이션하도록 두loopbacks개를 구성합니다.

```
interface Loopback1010
ip address 10.10.1.10 255.255.255.255
!
interface Loopback1020
ip address 10.10.2.10 255.255.255.255
```

2단계: 스포크 컨피그레이션

a. 스포크trustpoint라우터의 인증서를 저장하도록 를 구성합니다.

```
crypto pki trustpoint FlexVPNSpoke
 enrollment url http://10.10.10.10:80
 subject-name cn=FlexVPNSpoke, o=Cisco, OU=RED_GROUP
 revocation-check crl
```

b. 를certificate map구성합니다. 의 목적certificate map은 라우터에 여러 인증서가 설치된 경우 지정된 정보를 기반으로 인증서를 식별하고 매칭하는 것입니다.

```
crypto pki certificate map CERT_MAP 5
issuer-name co ca-server.cisco.com
```

c. AAA 로컬 권한 부여 네트워크를 구성합니다.

aaa authorization network 명령은 네트워크 서비스와 관련된 액세스 요청을 인증하는 데 사용됩니다. 여기에는 사용자가 인증된 후 요청된 서비스에 액세스할 수 있는 권한이 있는지 확인하는 과정이 포함됩니다.

```
aaa new-model
aaa authorization network FLEX local
```

d. 를IKEv2 profile구성합니다. 및 certificate map AAA 권한 부여 로컬은에서 참조됩니다IKEv2 profile.

로컬 및 원격 인증은 **RSA-SIG**.

```
crypto ikev2 profile Flex_PROFILE
match certificate CERT_MAP
identity local dn
authentication local rsa-sig
authentication remote rsa-sig
pki trustpoint FlexVPNSpoke
dpd 10 2 on-demand
aaa authorization group cert list FLEX default
```

e. 를IPsec profile구성하고 IKEv2 profile.

```
crypto ipsec profile IPSEC_FlexPROFILE
set ikev2-profile Flex_PROFILE
```

f. 를tunnel interface구성합니다. 에서tunnel interface는 권한 부여 결과에 따라 허브로부터 터널 IP 주소를 수신하도록 구성됩니다.

```
interface Tunnel0
ip address negotiated
tunnel source GigabitEthernet1
tunnel destination 192.168.10.10
tunnel protection ipsec profile IPSEC_FlexPROFILE
```

g. EIGRP를 구성하여 스포크 및 의 로컬 네트워크를 tunnel interface알립니다.

```
router eigrp 10
network 10.20.1.0 0.0.0.255
network 172.16.0.0
```

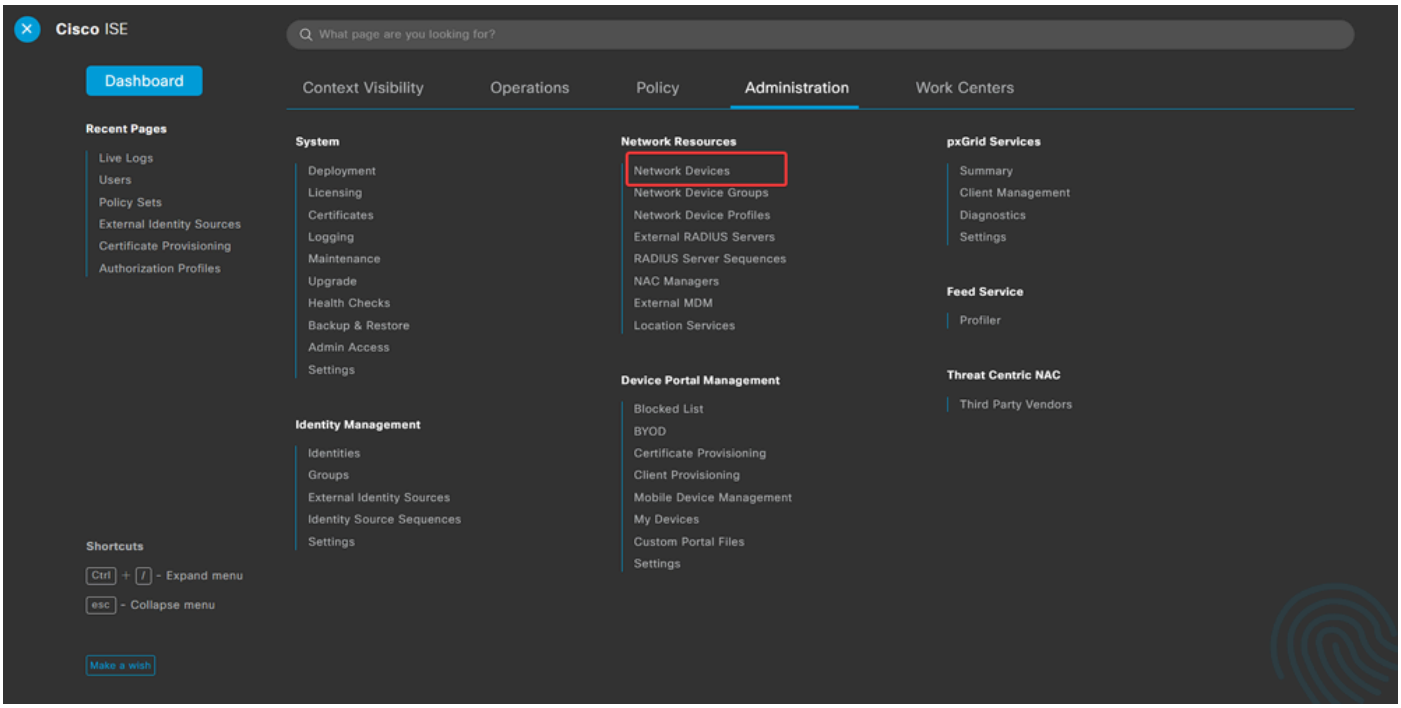
내부 네트워크를 시뮬레이션하도록 를loopback구성합니다.

```
interface Loopback2010
ip address 10.20.1.10 255.255.255.255
```

3단계: ISE 구성

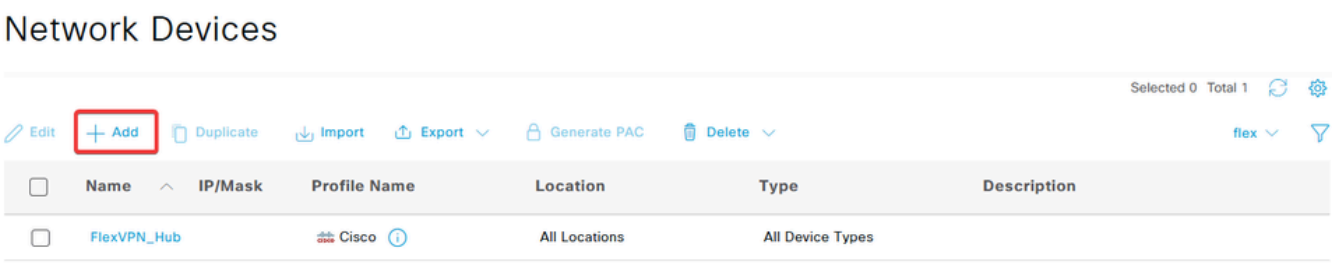
3.1단계: 사용자, 그룹 생성 및 네트워크 디바이스 추가

a. ISE 서버에 로그인하고 로 **Administration** > **Network Resources** > **Network Devices**이동합니다.



관리-네트워크 리소스-네트워크 디바이스

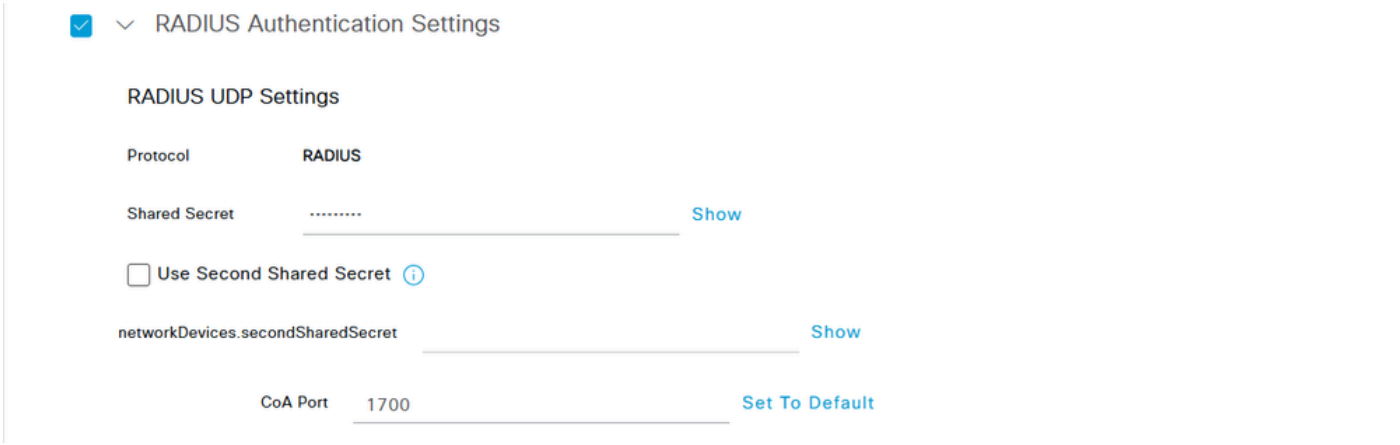
b. FlexVPN 허브**Add**를 AAA 클라이언트로 구성하려면 클릭합니다.



FlexVPN 라우터를 AAA 클라이언트로 추가

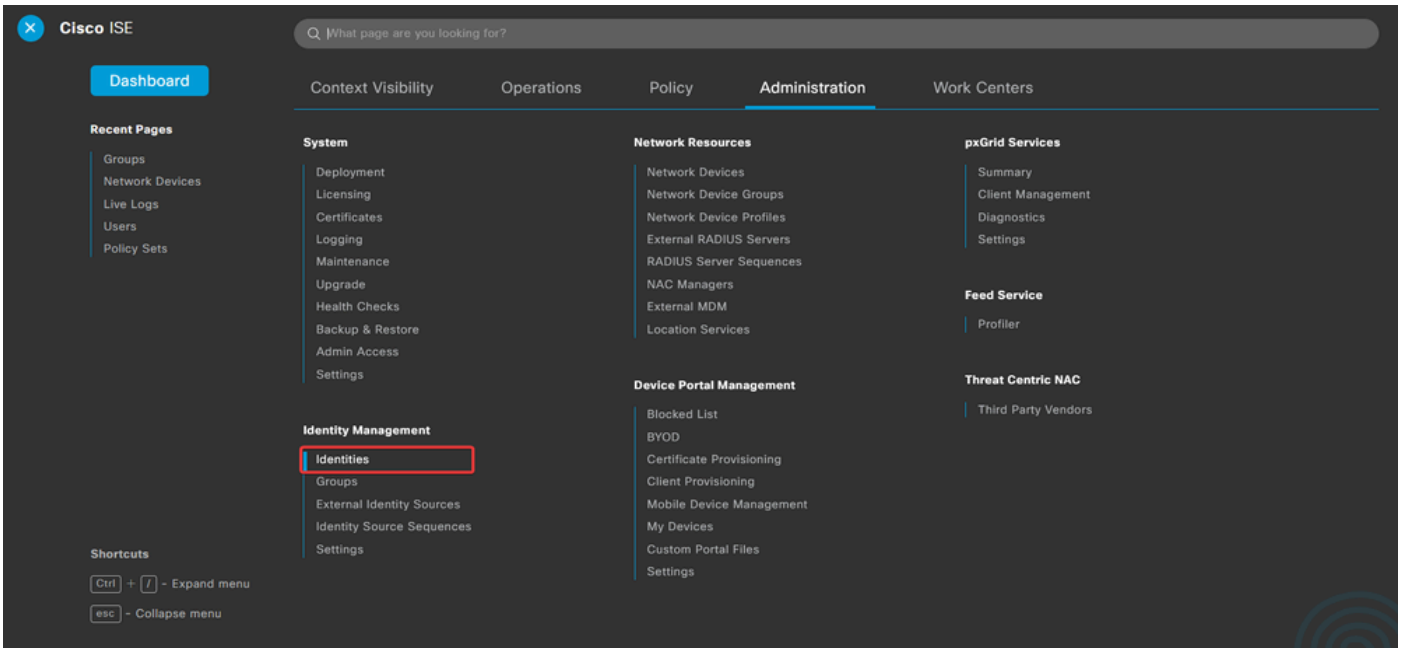
c. 네트워크 디바이스 이름 및 IP 주소 필드를 입력한 다음 확인란을 **RADIUS Authentication Settings** 선택하고 **Shared Secret**. 공유 암호 비밀번호는 RADIUS 서버 그룹이 FlexVPN 허브에 생성되었을 때 사용된 것과 동일해야 합니다. 을 클릭합니다.Save

네트워크 디바이스 IP 주소



네트워크 장치 공유 키

d. 로 이동합니다.**Administration > Identity Management > Identities**

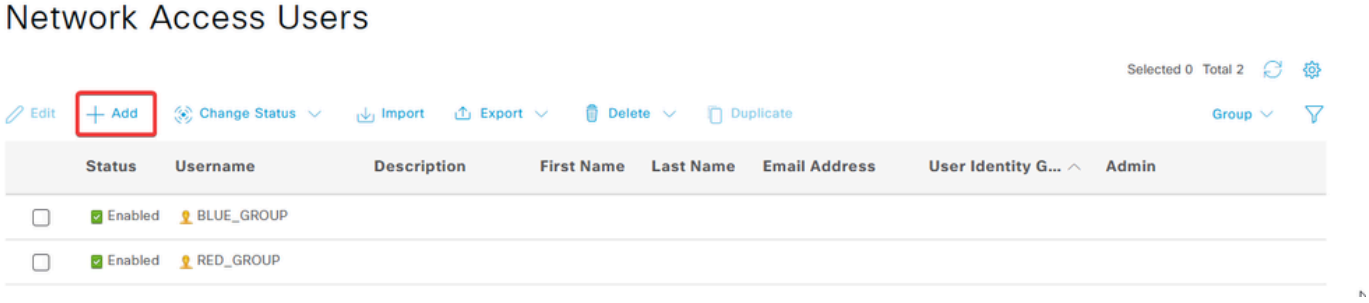


Administration-Identify 관리-Identifies

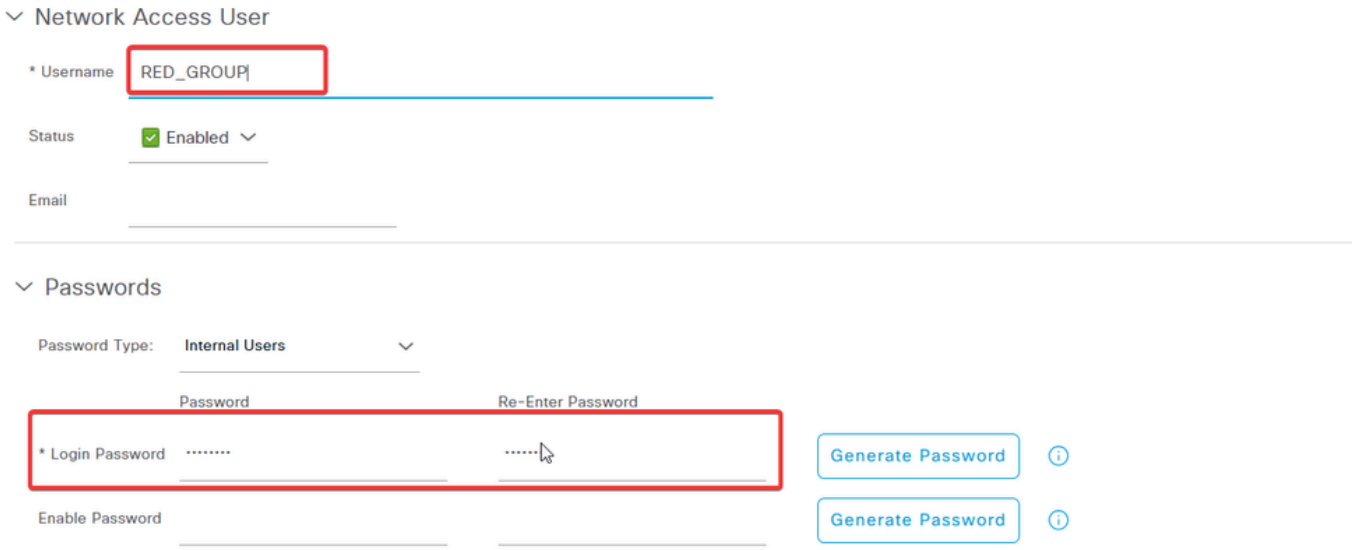
e. 서버 로컬 데이터베이스에 새 사용자를 만들려면 을 클릭합니다Add.

및Username를 **Login Password**입력합니다. 사용자 이름은 인증서의 조직 단위 값에 있는 인증서의 이름과 동일하며, 로그인 비밀번호는 IKev2 프로필에 지정된 것과 동일해야 합니다.

을 클릭합니다.**Save**



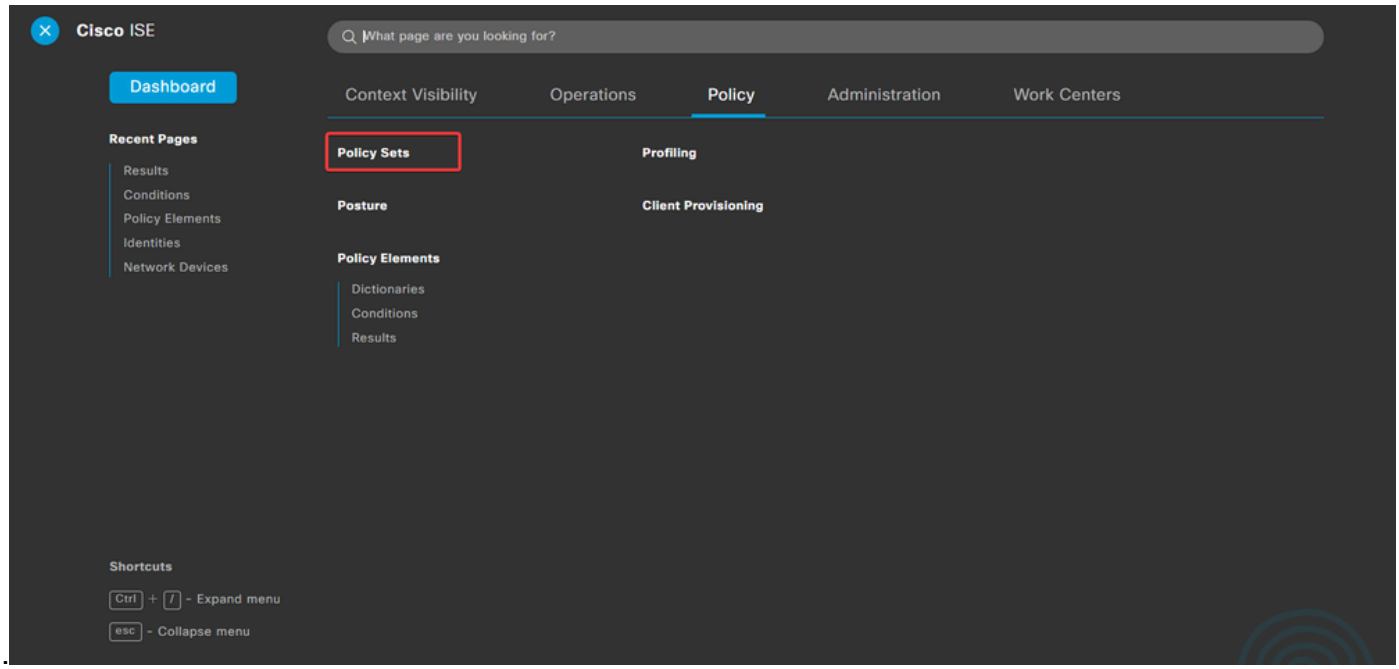
Administration-Identify 관리-Identifies



조직 단위 값과 동일하게 생성된 그룹

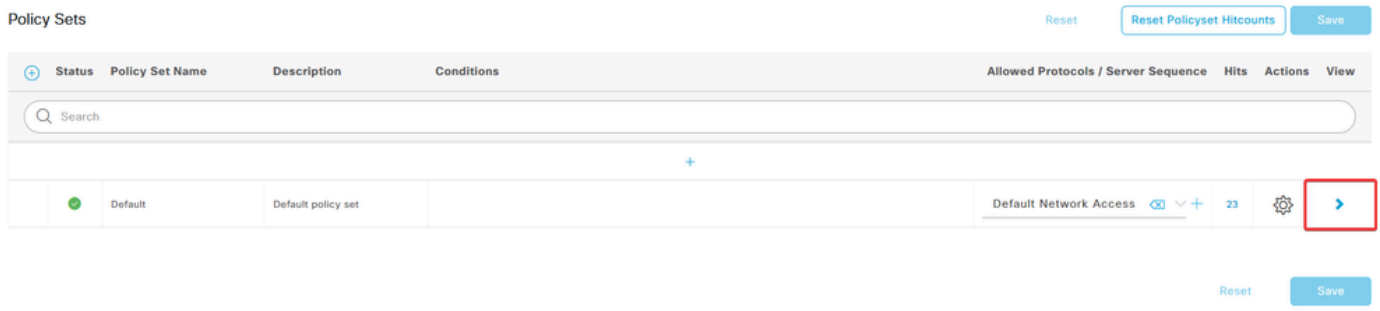
3.2단계: 정책 집합 구성

a. 로 이동합니다.**Policy > Policy Sets**



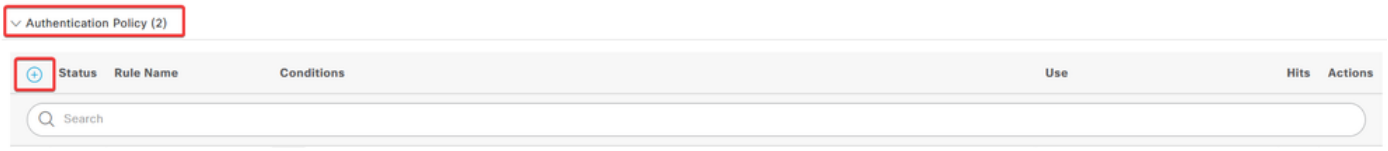
정책 설정

b. 화면 오른쪽의 화살표를 클릭하여 기본 권한 부여 정책을 선택합니다.



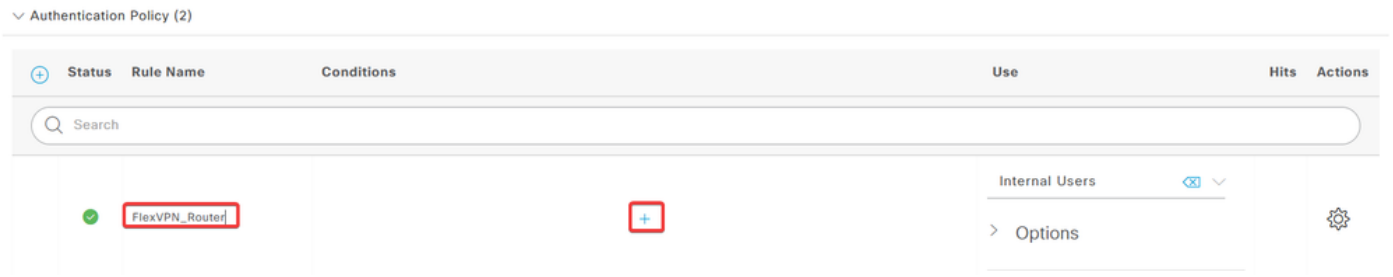
기본 정책 편집

c. 옆에 있는 드롭다운 메뉴 화살표를 클릭하여Authentication Policy확장합니다. 그런 다음 아이콘을 **add** (+) 클릭하여 새 규칙을 추가합니다.



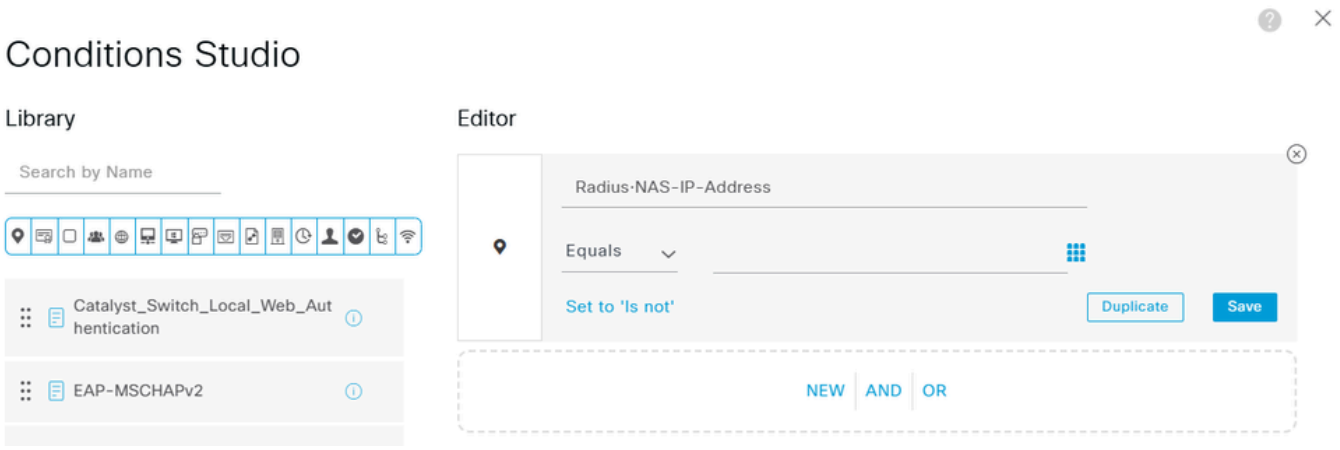
인증 정책 추가

d. 규칙의 이름을 입력하고 Conditions(조건) 열에서add (+)아이콘을 선택합니다.



인증 정책 생성

e. 속성 편집기 텍스트 상자를 클릭하고 아이콘을NAS-IP-Address클릭합니다. FlexVPN 허브의 IP 주소(192.168.0.10)를 입력합니다.

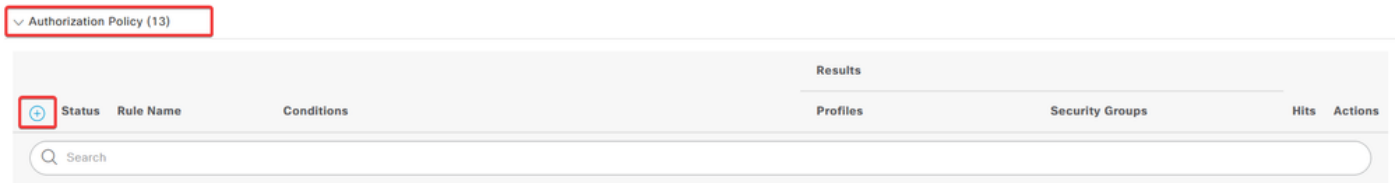


Authenticate FlexVPN Hub

인증 정책

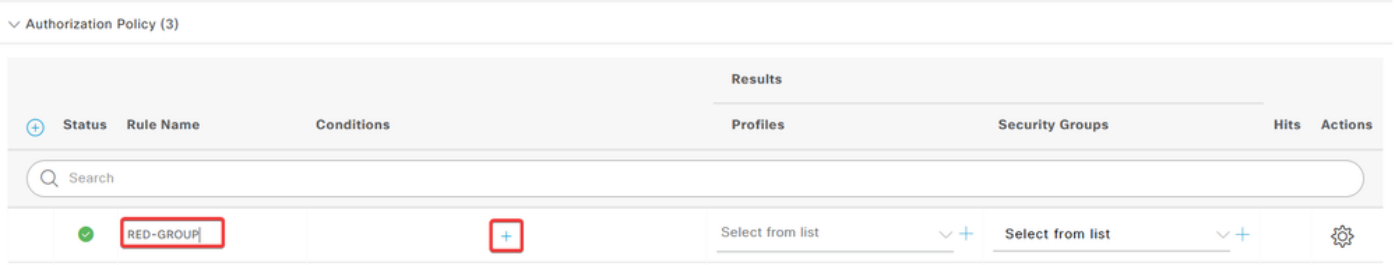
3.3단계: 권한 부여 정책 구성

a. 옆에 있는 드롭다운 메뉴 화살표를 클릭하여Authorization Policy확장합니다. 그런 다음 아이콘을 **add (+)** 클릭하여 새 규칙을 추가합니다.



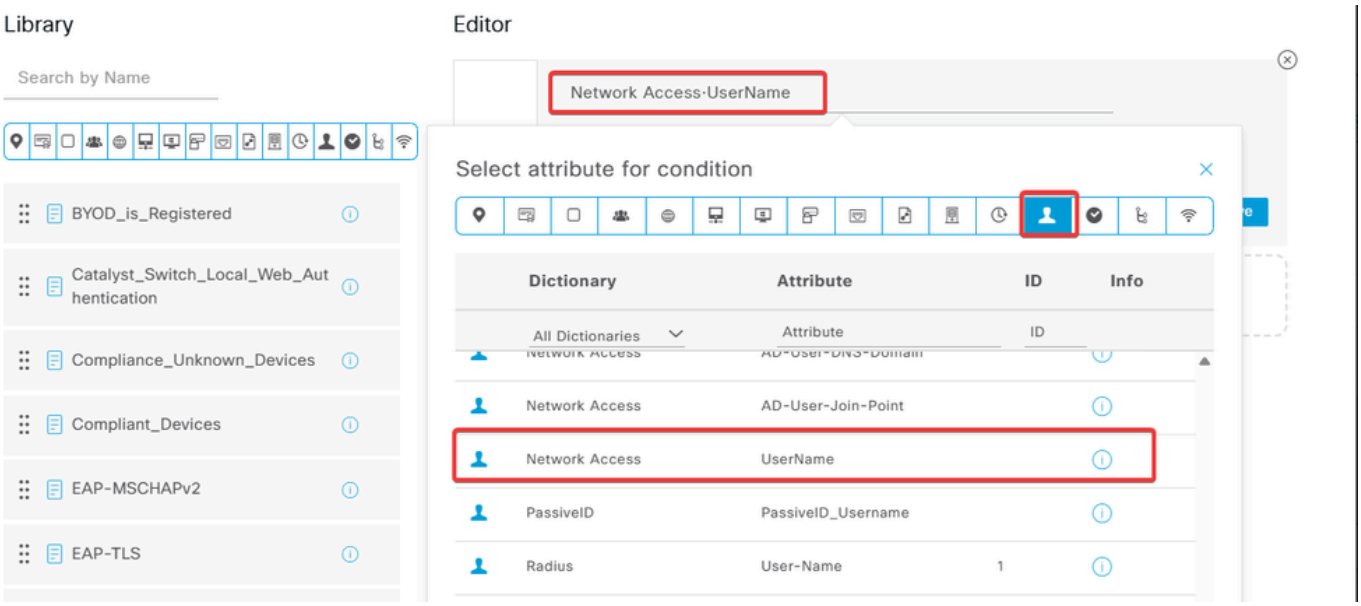
새 권한 부여 정책 생성

b. 규칙의 이름을 입력하고 Conditions(조건) 열에서 **add (+)** 아이콘을 선택합니다.



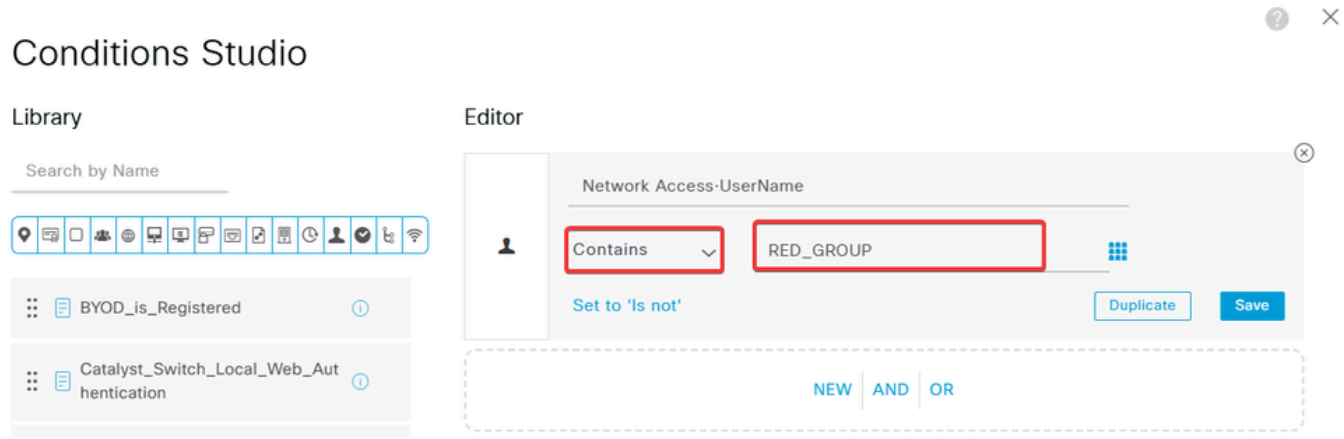
새 규칙 만들기

c. 속성 편집기 텍스트 상자를 클릭하고 아이콘을Subject클릭합니다. 특성을 **Network Access - UserName** 선택합니다.



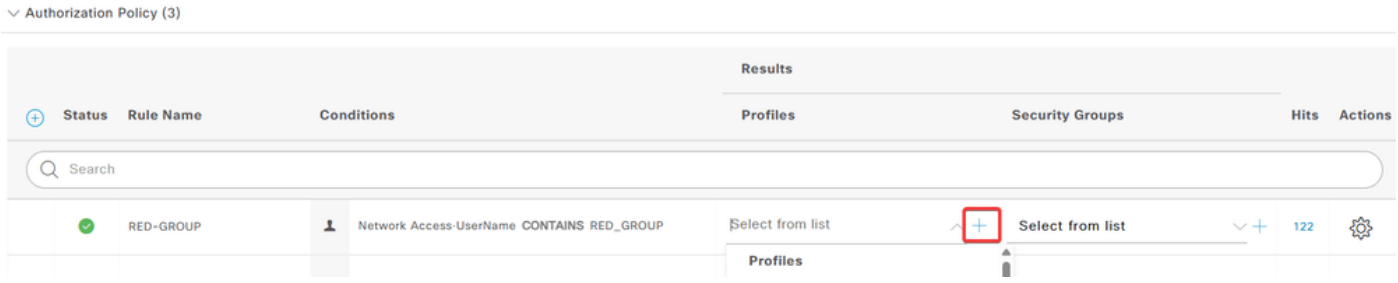
네트워크 액세스 - 사용자 이름 선택

d. 운영자로 선택한Contains다음 인증서의 Organization-Unit 값을 추가합니다.



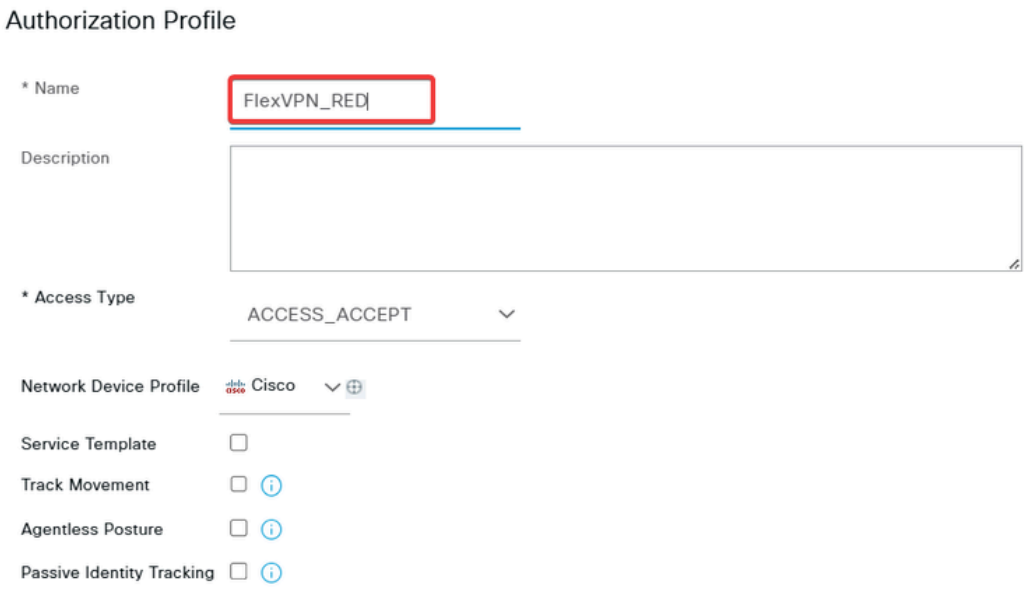
그룹 이름 추가

e. Profiles(프로필) 열에서 아이콘을add (+)클릭하고 **Create a New Authorization Profile**을 선택합니다.



새 권한 부여 프로파일 추가

f. 프로필을 입력합니다**Name.**



권한 부여 프로파일 이름 지정

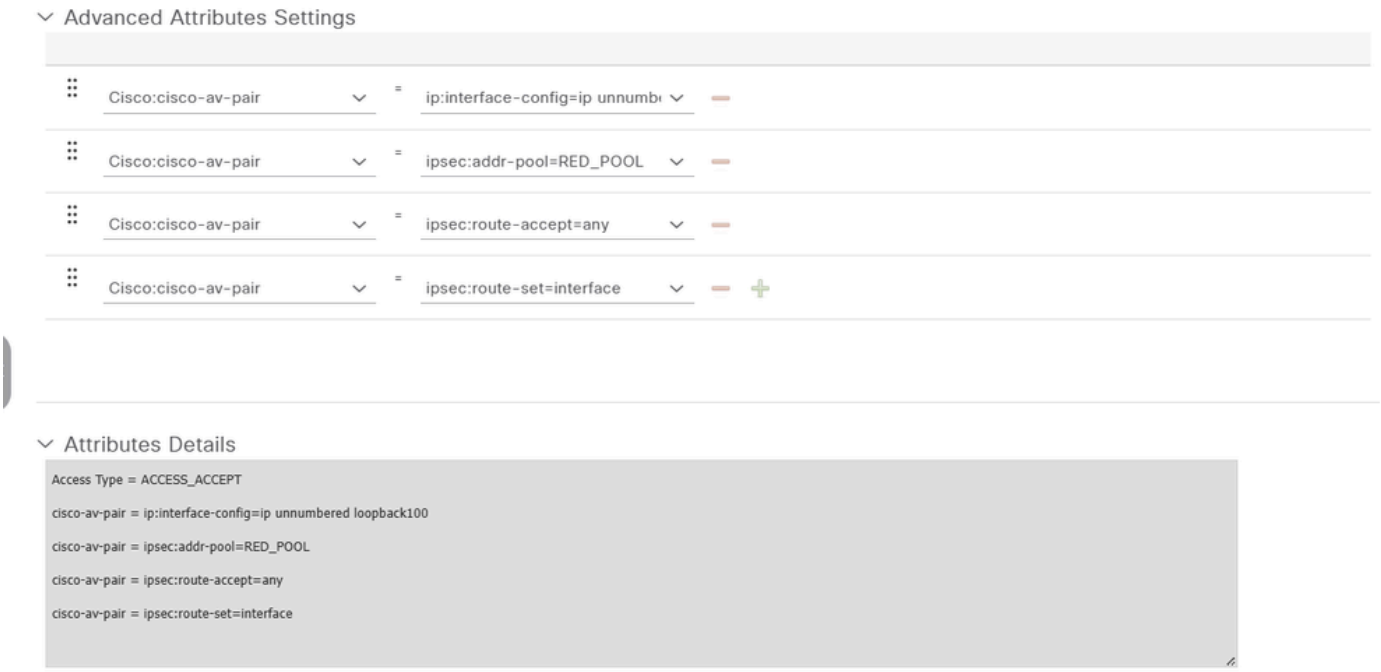
g. 로 이동합니다.**Advanced Attributes Settings** 그런 다음 왼쪽의 드롭다운 메뉴에서 cisco-av-pair특성을 선택하고 그룹에 따라 FlexVPN Spoke에 할당된 특성을 추가합니다.

이 예에 할당할 속성은 다음과 같습니다.

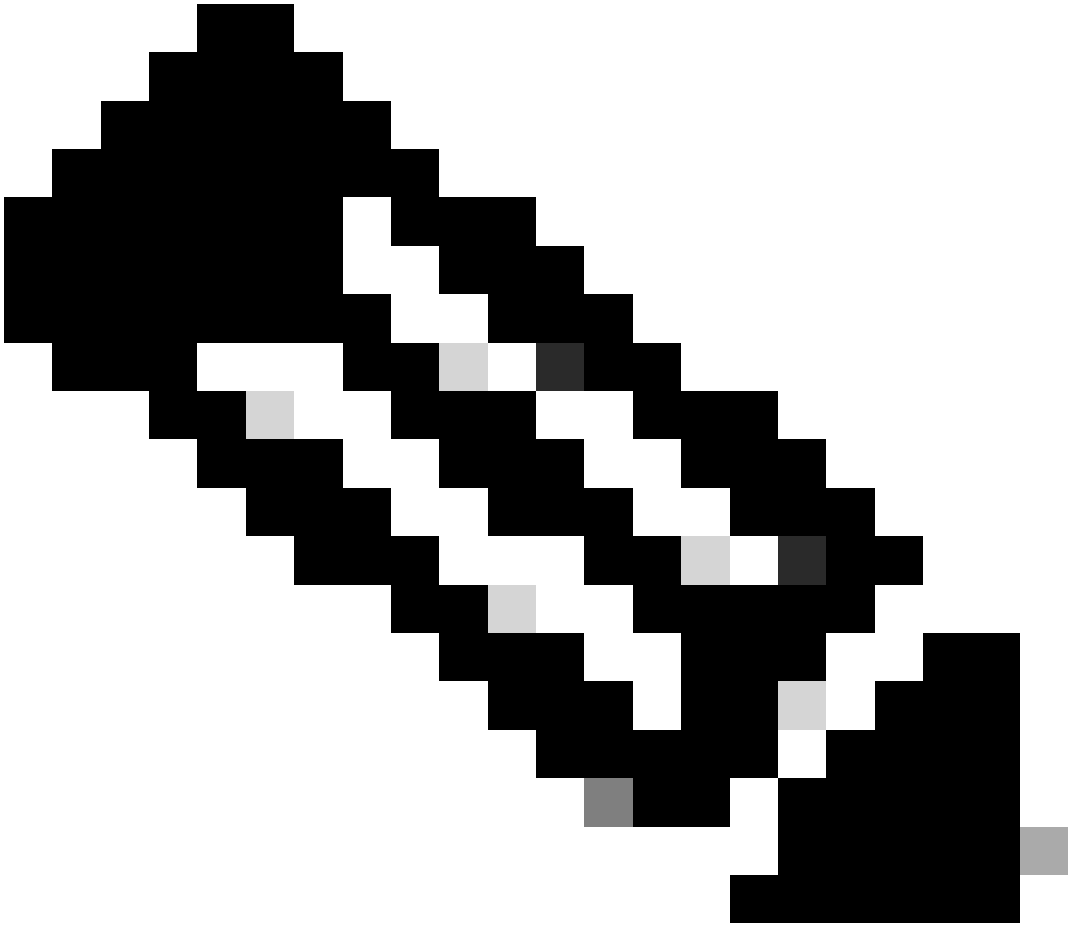
- 루프백 인터페이스를 소스로 할당합니다.
- 스포크가 IP 주소를 가져오는 풀 지정..

및 route accept any 특성은 route set interface 필요하지 않습니다. 이러한 특성이 없으면 경로가 스포크에 제대로 광고되지 않기 때문입니다.

```
Access Type = ACCESS_ACCEPT
cisco-av-pair = ip:interface-config=ip unnumbered loopback100
cisco-av-pair = ipsec:addr-pool=RED_POOL
cisco-av-pair = ipsec:route-accept=any
cisco-av-pair = ipsec:route-set=interface
```


Advanced Attributes Settings
Cisco:cisco-av-pair
ip:interface-config=ip unnumb
Cisco:cisco-av-pair
ipsec:addr-pool=RED_POOL
Cisco:cisco-av-pair
ipsec:route-accept=any
Cisco:cisco-av-pair
ipsec:route-set=interface
Attributes Details
Access Type = ACCESS_ACCEPT
cisco-av-pair = ip:interface-config=ip unnumbered loopback100
cisco-av-pair = ipsec:addr-pool=RED_POOL
cisco-av-pair = ipsec:route-accept=any
cisco-av-pair = ipsec:route-set=interface

고급 특성 설정

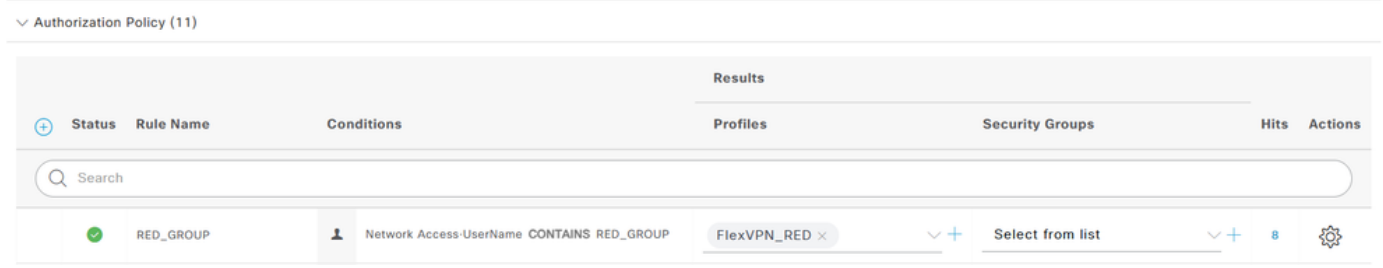


참고: 특성 사양(이름, 구문, 설명, 예 등)은 FlexVPN RADIUS 특성 컨피그레이션 가이드를 참조하십시오.

FlexVPN 및 Internet Key Exchange 버전 2 컨피그레이션 가이드, Cisco IOS XE Gibraltar 16.12.x

---

h. 프로파일 열**authorization profile**에서 를 할당합니다.



권한 부여 규칙

i. **Save**클릭합니다.

다음을 확인합니다.

- 이 명령을 **show ip interface brief** 사용하여 터널, 가상 템플릿 및 가상 액세스 상태를 검토할 수 있습니다.

허브에서 Virtual-Template의 up/down 상태는 정상이며, Virtual-Access는 허브와의 연결을 설정하고 up/up 상태를 표시하는 각 Spoke에 대해 생성됩니다.

<#root>

```
FlexVPN_HUB#show ip interface brief
Interface                  IP-Address      OK?  Method   Status          Protocol
GigabitEthernet1           192.168.10.10   YES  NVRAM    up              up
GigabitEthernet2           192.168.0.10    YES  manual   up              up
Loopback100                10.100.100.1    YES  manual   up              up
Loopback200                10.200.200.1    YES  manual   up              up
Loopback1010               10.10.1.10      YES  manual   up              up
Loopback1020               10.10.2.1       YES  manual   up              up

Virtual-Access1            10.100.100.1    YES  unset    up              up


Virtual-Template2          unassigned      YES  unset    up              dow
```

Spoke에서 터널 인터페이스가 그룹에 할당된 풀에서 IP 주소를 수신하고 up/up 상태를 표시합니다
.

<#root>

```
FlexVPN_RED_SPOKE#show ip interface brief
Interface                  IP-Address      OK?  Method   Status          Protocol
GigabitEthernet1           192.168.10.20    YES  NVRAM    up              up
Loopback2                  10.20.1.10      YES  manual   up              up

Tunnel0                    172.16.10.107   YES  manual   up              up
```

- 다음 명령을 사용하여.**show interfaces virtual-access**

  configuration

```
FlexVPN_HUB#show interfaces virtual-access 1 configuration
Virtual-Access1 is in use, but purpose is unknown
Derived configuration : 232 bytes
!
interface Virtual-Access1
 ip unnumbered Loopback100
 tunnel source GigabitEthernet1
```

```
 tunnel mode ipsec ipv4
 tunnel destination dynamic
 tunnel protection ipsec profile IPSEC_FlexPROFILE
 no tunnel protection ipsec initiate
end
```

- 이 명령**show crypto session** 을 사용하여 라우터 간의 보안 연결이 설정되었는지 확인합니다.

```
FlexVPN_HUB#show crypto session
Crypto session current status
Interface: Virtual-Access1
Profile: Flex_PROFILE
Session status: UP-ACTIVE
Peer: 192.168.10.20 port 500
  Session ID: 306
  IKEv2 SA: local 192.168.10.10/500 remote 192.168.10.20/500 Active
  IPSEC FLOW: permit ip 0.0.0.0/0.0.0.0 0.0.0.0/0.0.0.0
        Active SAs: 2, origin: crypto map
```

- 명령을 사용하여show ip eigrp neighborsEIGRP 인접성이 다른 사이트와 설정되었는지 확인합니다.

```
FlexVPN_HUB#show ip eigrp neighbors
EIGRP-IPv4 VR(Flexvpn) Address-Family Neighbors for AS(10)
H   Address                 Interface              Hold Uptime     SRTT   RTO   Q   Seq
                                                   (sec)           (ms)       Cnt  Num
0   172.16.10.107           Vi1                      10 00:14:00      8  1494   0   31
```

- 명령을 사용하여show ip route경로가 스포크에 푸시되었는지 확인합니다.
  - EIGRP가 스포크의 루프백 인터페이스인 10.20.1.10에 대한 경로를 허브에 학습했으며 가상 액세스를 통해 액세스할 수 있습니다

<#root>

```
FlexVPN_HUB#show ip route
<<<<< Output Ommitted >>>>>

Gateway of last resort is 192.168.10.1 to network 0.0.0.0

S*    0.0.0.0/0 [1/0] via 192.168.10.1
      10.0.0.0/32 is subnetted, 5 subnets
C        10.10.1.10 is directly connected, Loopback1010
C        10.10.2.10 is directly connected, Loopback1020

D        10.20.1.10 [90/79360000] via 172.16.10.107, 00:24:42, Virtual-Access1


C        10.100.100.1 is directly connected, Loopback100
C        10.200.200.1 is directly connected, Loopback200
      172.16.0.0/32 is subnetted, 1 subnets
```

```
S        172.16.10.107 is directly connected, Virtual-Access1
      192.168.0.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.0.0/24 is directly connected, GigabitEthernet2
L        192.168.0.10/32 is directly connected, GigabitEthernet2
C        192.168.10.0/24 is directly connected, GigabitEthernet1
L        192.168.10.10/32 is directly connected, GigabitEthernet1
```

- 10.10.1.10 및 10.10.2.10에 대한 경로는 EIGRP를 통해 학습되었으며 Tunnel0을 통해 액세스할 수 있는 RED_GROUP(10.100.100.1)의 소스 IP를 통해 연결할 수 있습니다.

<#root>

```
FlexVPN_RED_SPOKE#sh ip route
<<<<< Output Ommitted >>>>>

Gateway of last resort is 192.168.10.1 to network 0.0.0.0

S*    0.0.0.0/0 [1/0] via 192.168.10.1
      10.0.0.0/32 is subnetted, 5 subnets
D        10.10.1.10 [90/26880032] via 10.100.100.1, 00:00:00


D        10.10.2.10 [90/26880032] via 10.100.100.1, 00:00:00


C        10.20.1.10 is directly connected, Loopback2
S        10.100.100.1 is directly connected, Tunnel0


D        10.200.200.1 [90/26880032] via 10.100.100.1, 00:00:00


      172.16.0.0/32 is subnetted, 1 subnets
C        172.16.10.107 is directly connected, Tunnel0
      192.168.0.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.10.0/24 is directly connected, GigabitEthernet1
L        192.168.10.20/32 is directly connected, GigabitEthernet1
```

문제 해결

이 섹션에서는 이러한 유형의 구축 문제를 해결하는 데 사용할 수 있는 정보를 제공합니다. 다음 명령을 사용하여 터널 협상 프로세스를 디버깅할 수 있습니다.

debug crypto interface

debug crypto ikev2
debug crypto ikev2 client flexvpn
debug crypto ikev2 error
debug crypto ikev2 internal
debug crypto ikev2 packet

debug crypto ipsec
debug crypto ipsec error
debug crypto ipsec message
debug crypto ipsec states

AAA 및 RADIUS 디버그는 스포크 권한 부여의 트러블슈팅에 도움이 될 수 있습니다.

debug aaa authentication
debug aaa authorization
debug aaa protocol radius
debug radius authentication

Working Scenario

이 로그는 인증 프로세스 및 매개 변수의 할당을 보여줍니다.

```
     <#root>

RADIUS(000001A7): Received from id 1645/106
AAA/BIND(000001A8): Bind i/f
AAA/AUTHOR (0x1A8): Pick method list 'FLEX'
RADIUS/ENCODE(000001A8):Orig. component type = VPN IPSEC



RADIUS(000001A8): Config NAS IP: 192.168.0.10



vrfid: [65535]  ipv6 tableid : [0]
idb is NULL
RADIUS(000001A8): Config NAS IPv6: ::
RADIUS/ENCODE(000001A8): acct_session_id: 4414
RADIUS(000001A8): sending
RADIUS(000001A8): Send Access-Request to 192.168.0.5:1645 id 1645/107, len 138
RADIUS:  authenticator 7A B5 97 50 F2 6E F0 09 - 3D B0 54 B4 1A DB BA BA



RADIUS:  User-Name           [1]   11  "RED_GROUP"
```

```
RADIUS:  User-Password       [2]   18  *

RADIUS:  Calling-Station-Id  [31]  14  "192.168.10.20"

RADIUS:  Vendor, Cisco       [26]  63

RADIUS:   Cisco AVpair       [1]   57  "audit-session-id=L2L496130A2ZP2L496130A21ZI1F401F4ZM134"

RADIUS:  Service-Type        [6]   6   Outbound                 [5]

RADIUS:  NAS-IP-Address      [4]   6   192.168.0.10
```

```
RADIUS(000001A8): Sending a IPv4 Radius Packet



RADIUS(000001A8): Started 5 sec timeout



RADIUS: Received from id 1645/107 192.168.0.5:1645, Access-Accept, len 248



RADIUS:  authenticator BE F4 FC FF 7C 41 97 A7 - 3F 02 A7 A3 A1 96 91 38
RADIUS:  User-Name           [1]   11  "RED_GROUP"
RADIUS:  Class               [25]  69
RADIUS:   43 41 43 53 3A 4C 32 4C 34 39 36 31 33 30 41 32  [CACS:L2L496130A2]
RADIUS:   5A 50 32 4C 34 39 36 31 33 30 41 32 31 5A 49 31  [ZP2L496130A21ZI1]
RADIUS:   46 34 30 31 46 34 5A 4D 31 33 34 3A 49 53 45 42  [F401F4ZM134:ISEB]
RADIUS:   75 72 67 6F 73 2F 35 33 34 36 34 30 33 32 39 2F  [urgos/534640329/]
RADIUS:   32 39 31               [ 291]



RADIUS:  Vendor, Cisco       [26]  53









RADIUS:   Cisco AVpair       [1]   47  "ip:interface-config=ip unnumbered loopback100"









RADIUS:  Vendor, Cisco       [26]  32









RADIUS:   Cisco AVpair       [1]   26  "ipsec:addr-pool=RED_POOL"


```

```
RADIUS:  Vendor, Cisco       [26]  33

RADIUS:   Cisco AVpair       [1]   27  "ipsec:route-set=interface"

RADIUS:  Vendor, Cisco       [26]  30

RADIUS:   Cisco AVpair       [1]   24  "ipsec:route-accept=any"

RADIUS(000001A8): Received from id 1645/107
%LINEPROTO-5-UPDOWN: Line protocol on Interface Virtual-Access1, changed state to down
%SYS-5-CONFIG_P: Configured programmatically by process Crypto INT from console as console
AAA/BIND(000001A9): Bind i/f
INFO: AAA/AUTHOR: Processing PerUser AV interface-config
%SYS-5-CONFIG_P: Configured programmatically by process Crypto INT from console as console
AAA/BIND(000001AA): Bind i/f
INFO: AAA/AUTHOR: Processing PerUser AV interface-config
%SYS-5-CONFIG_P: Configured programmatically by process Crypto INT from console as console

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

AAA/BIND(000001AB): Bind i/f
RADIUS/ENCODE(000001AB):Orig. component type = VPN IPSEC
RADIUS(000001AB): Config NAS IP: 192.168.0.10
vrfid: [65535]  ipv6 tableid : [0]
```

```
idb is NULL
RADIUS(000001AB): Config NAS IPv6: ::
RADIUS(000001AB): Sending a IPv4 Radius Packet
RADIUS(000001AB): Started 5 sec timeout
RADIUS: Received from id 1646/23 192.168.0.5:1646, Accounting-response, len 20




%DUAL-5-NBRCHANGE: EIGRP-IPv4 10: Neighbor 172.16.10.109 (Virtual-Access1) is up: new adjacency
```

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.