SD-WAN의 C8000V를 사용하여 서비스측 IPSec 터널 구성

목차

소개

이 문서에서는 SD-WAN Cisco Edge Router와 서비스 VRF를 사용하는 VPN 엔드포인트 간에 IPSec 터널을 구성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco SD-WAN(Software-defined Wide Area Network)
- IPSec(인터넷 프로토콜 보안)

구성 요소

이 문서는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco Edge Router 버전 17.6.1
- SD-WAN vManage 20.9.3.2

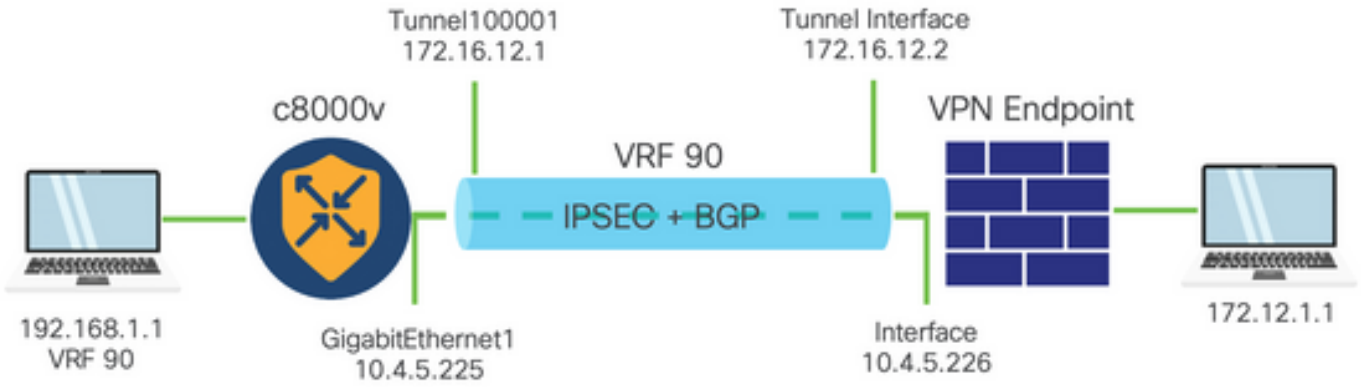
이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서의 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

배경 정보에는 이 문서의 범위, 사용 편의성 및 SD-WAN에 C8000v를 사용하여 서비스측 IPSec 터널 구축의 혜택이 포함되어 있습니다.

- 컨트롤러 관리 모드의 Cisco IOS® XE 라우터와 VPN(Virtual Private Network) 엔드포인트 간의 서비스 VRF(Virtual Routing and Forwarding)에서 IPSec 터널을 구축하려면 퍼블릭 WAN(Wide Area Network)을 통해 데이터 기밀성과 무결성을 보장합니다. 또한 회사 사설 네트워크의 보안 확장을 용이하게 하고 인터넷을 통한 원격 연결을 허용하면서 높은 수준의 보안을 유지합니다.
- 서비스 VRF는 트래픽을 격리합니다. 이는 다중 클라이언트 환경에서 또는 네트워크의 서로 다른 부분 간의 세그멘테이션을 유지하는 데 특히 유용합니다. 요약하면, 이 컨피그레이션은 보안 및 연결을 향상시킵니다.
- 이 문서에서는 BGP(Border Gateway Protocol)가 SD-WAN 서비스 VRF에서 VPN 엔드포인트 뒤의 네트워크로 또는 그 반대로 네트워크를 통신하는 데 사용되는 라우팅 프로토콜이라고 간주합니다.
- BGP 컨피그레이션은 이 문서의 범위를 벗어납니다.
- 이 VPN 엔드포인트는 방화벽, 라우터 또는 IPSec 기능이 있는 모든 유형의 네트워크 디바이스일 수 있습니다. VPN 엔드포인트의 컨피그레이션은 이 문서의 범위에 속하지 않습니다.
- 이 문서에서는 라우터가 활성 제어 연결 및 서비스 VRF로 이미 온보딩되었다고 가정합니다.

IPSEC 컨피그레이션의 구성 요소



1단계 IKE(Internet Key Exchange)

IPSec 컨피그레이션 프로세스의 1단계에는 터널 엔드포인트 간의 보안 매개변수 및 인증 협상이 포함됩니다. 이러한 단계는 다음과 같습니다.

IKE 컨피그레이션

- 암호화 제안(알고리즘 및 키 길이)을 정의합니다.
- 암호화 제안, TTL(Time to Live) 및 인증을 포함하는 IKE 정책을 구성합니다.

원격 엔드 피어 구성

- 원격 단의 IP 주소를 정의합니다.
- 인증을 위해 공유 키(사전 공유 키)를 구성합니다.

2단계(IPSec) 컨피그레이션

2단계에는 터널을 통과하는 트래픽 흐름에 대한 보안 변환 및 액세스 규칙에 대한 협상이 포함됩니다. 이러한 단계는 다음과 같습니다.

IPSec 변환 세트 구성

- 암호화 알고리즘 및 인증을 포함하는 제안된 변형 집합을 정의합니다.

IPSec 정책 구성

- 변형 집합을 IPSec 정책과 연결합니다.

터널 인터페이스 구성

IPSec 터널의 양쪽 끝에 터널 인터페이스를 구성합니다.

- 터널 인터페이스를 IPSec 정책과 연결합니다.

구성

CLI의 컨피그레이션

1단계. 암호화 제안을 정의합니다.

```
<#root>
cEdge(config)#
crypto ikev2 proposal p1-global

cEdge(config-ikev2-proposal)#
encryption aes-cbc-128 aes-cbc-256

cEdge(config-ikev2-proposal)#
integrity sha1 sha256 sha384 sha512

cEdge(config-ikev2-proposal)#
group 14 15 16
```

2단계. 제안 정보를 포함하는 IKE 정책을 구성합니다.

<#root>

```
cEdge(config)#
crypto ikev2 policy policy1-global

cEdge(config-ikev2-policy)#
proposal p1-global
```

3단계. 원격 단의 IP 주소를 정의합니다.

<#root>

```
cEdge(config)#
crypto ikev2 keyring if-ipsec1-ikev2-keyring

cEdge(config-ikev2-keyring)#
peer if-ipsec1-ikev2-keyring-peer

cEdge(config-ikev2-keyring-peer)#
address 10.4.5.226

cEdge(config-ikev2-keyring-peer)#
pre-shared-key Cisco
```

4단계. 인증을 위해 공유 키(사전 공유 키)를 구성합니다.

<#root>

```
cEdge(config)#
crypto ikev2 profile if-ipsec1-ikev2-profile

cEdge(config-ikev2-profile)#
match identity remote address
10.4.5.226 255.255.255.0

cEdge(config-ikev2-profile)#
authentication remote
```

```
cEdge(config-ikev2-profile)#
authentication remote pre-share

cEdge(config-ikev2-profile)#
authentication local pre-share

cEdge(config-ikev2-profile)#
keyring local if-ipsec1-ikev2-keyring

cEdge(config-ikev2-profile)#
dpd 10 3 on-demand

cEdge(config-ikev2-profile)#
no config-exchange request

cEdge(config-ikev2-profile)#
```

5단계. 암호화 알고리즘 및 인증을 포함하는 제안된 transform-set을 정의합니다.

<#root>

```
cEdge(config)#
crypto ipsec transform-set if-ipsec1-ikev2-transform esp-gcm 256

cEdge(cfg-crypto-trans)#
mode tunnel
```

6단계. transform-set을 IPSec 정책과 연결합니다.

<#root>

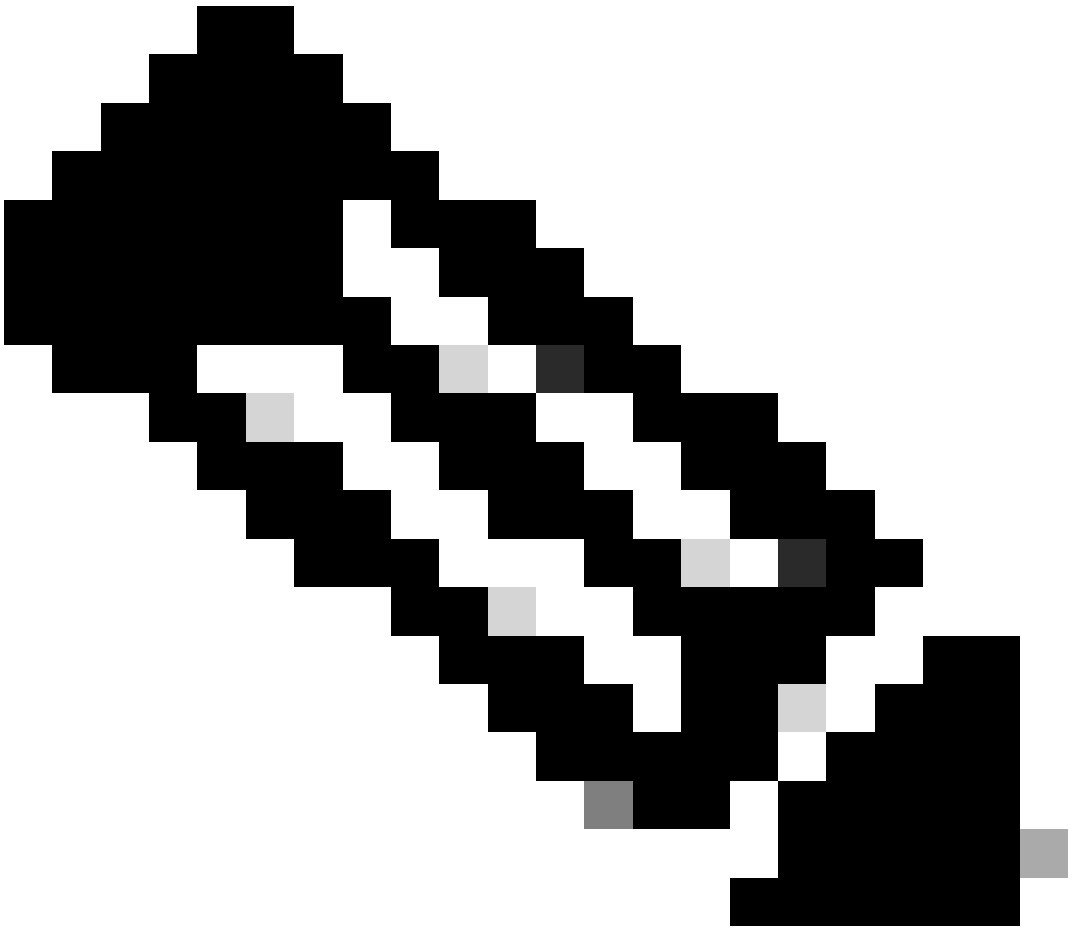
```
cEdge(config)#
crypto ipsec profile if-ipsec1-ipsec-profile

cEdge(ipsec-profile)#
set security-association lifetime kilobytes disable

cEdge(ipsec-profile)#
set security-association replay window-size 512
```

```
cEdge(ipsec-profile)#
set transform-set if-ipsec1-ikev2-transform

cEdge(ipsec-profile)#
set ikev2-profile if-ipsec1-ikev2-profile
```

7단계. 인터페이스 터널을 생성하고 IPSec 정책과 연결합니다.

```
<#root>
cEdge(config)#
interface Tunnel100001

cEdge(config-if)#
vrf forwarding 90

cEdge(config-if)#
ip address 172.16.12.1 255.255.255.252

cEdge(config-if)#
ip mtu 1500

cEdge(config-if)#
tunnel source GigabitEthernet1

cEdge(config-if)#
tunnel mode ipsec ipv4

cEdge(config-if)#
tunnel destination 10.4.5.226

cEdge(config-if)#
tunnel path-mtu-discovery

cEdge(config-if)#
tunnel protection ipsec profile if-ipsec1-ipsec-profile
```

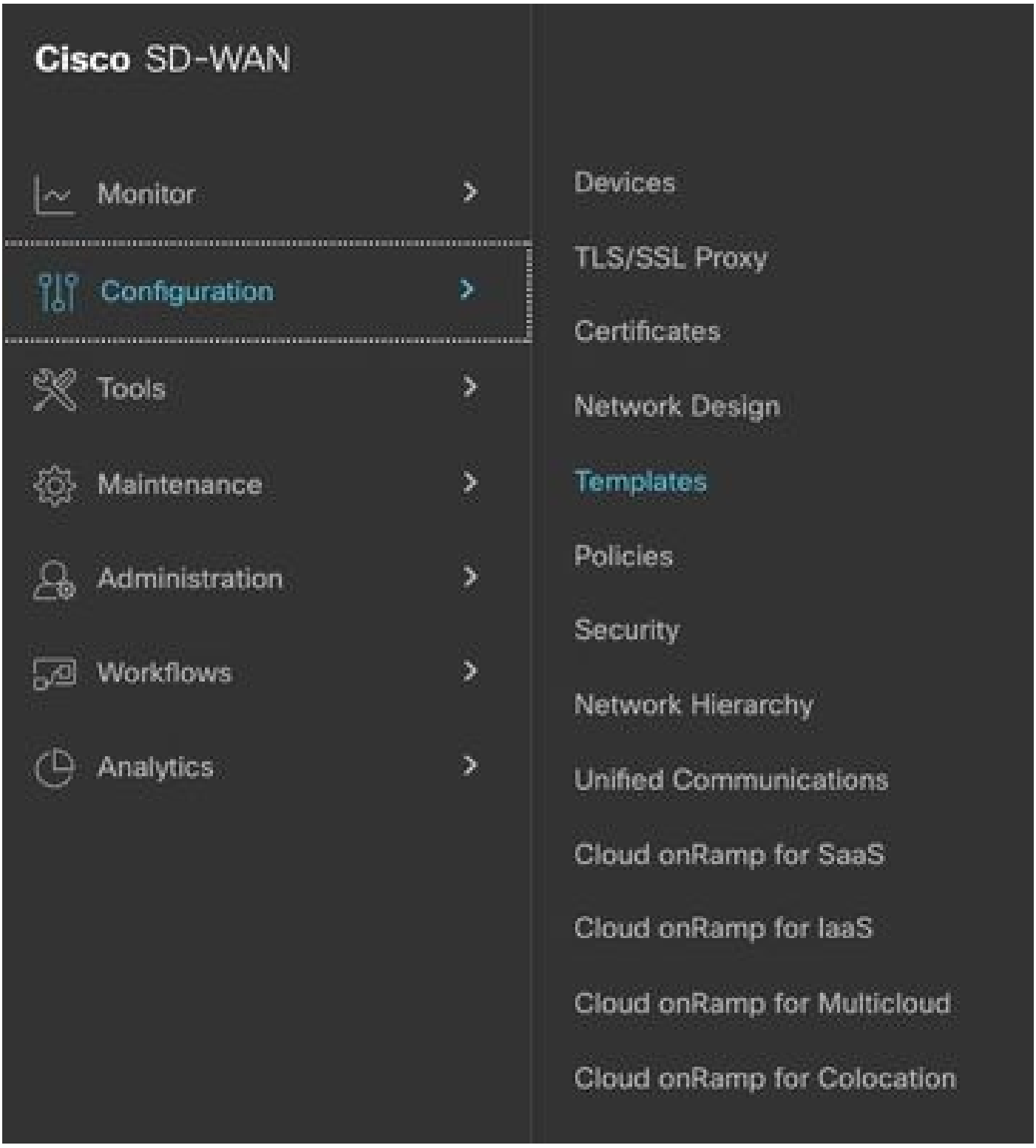
vManage의 CLI 애드온 템플릿에 대한 컨피그레이션



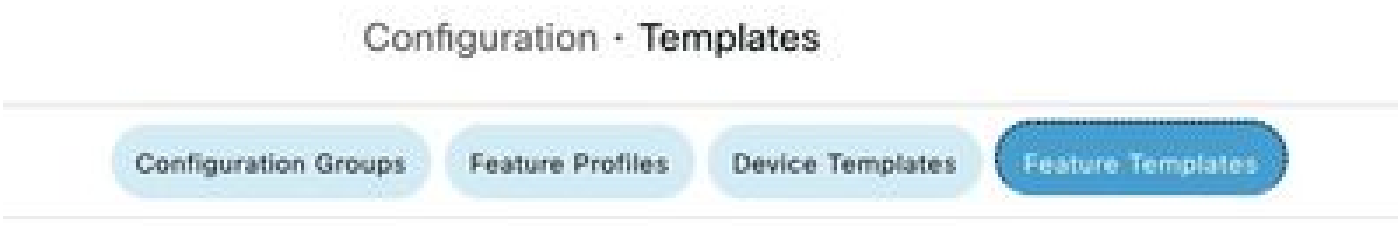
참고: 이 컨피그레이션 유형은 CLI 애드온 템플릿을 통해서만 추가할 수 있습니다.

1단계. Cisco vManage로 이동하여 로그인합니다.

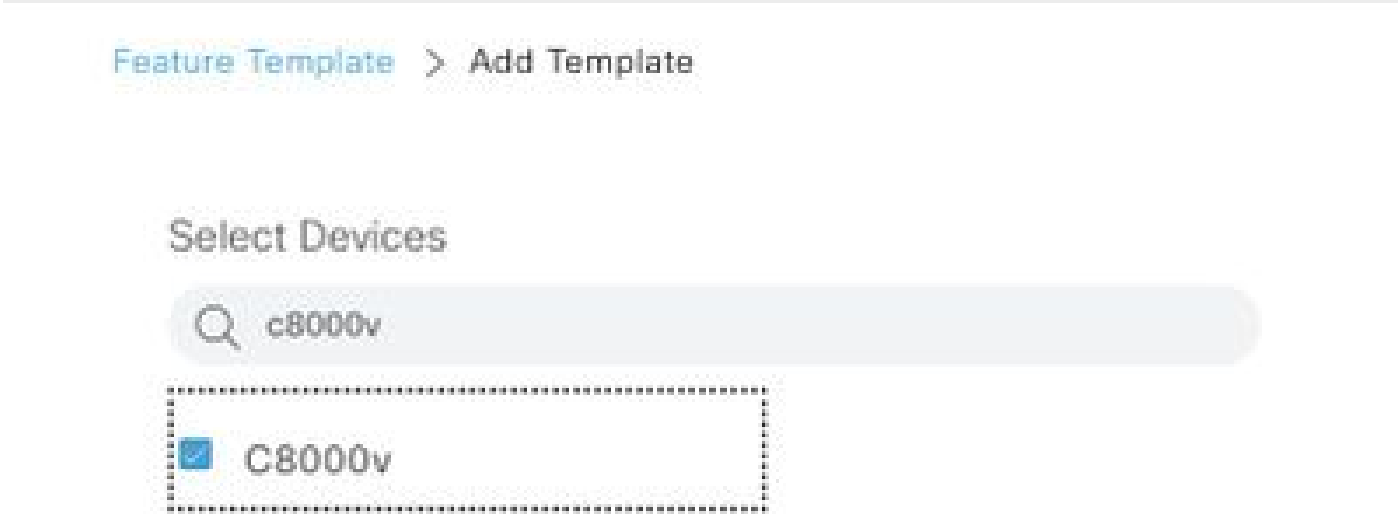
2단계. Configuration(컨피그레이션) > Templates(템플릿)로 이동합니다.



3단계. Feature Templates(기능 템플릿) > Add Template(템플릿 추가)으로 이동합니다.

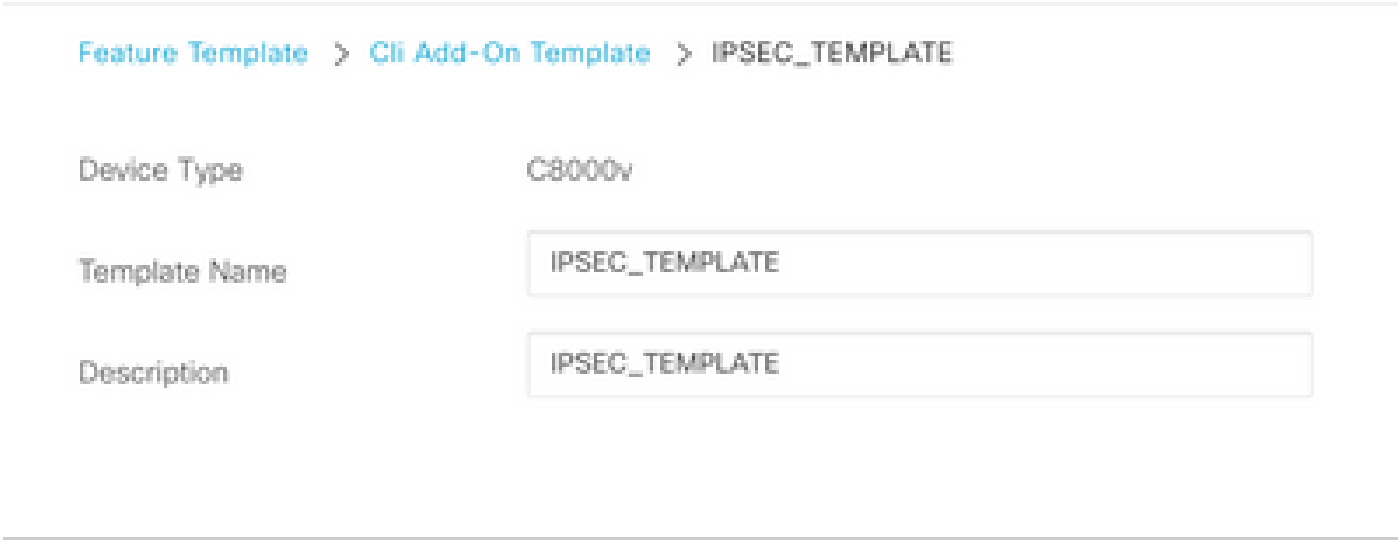


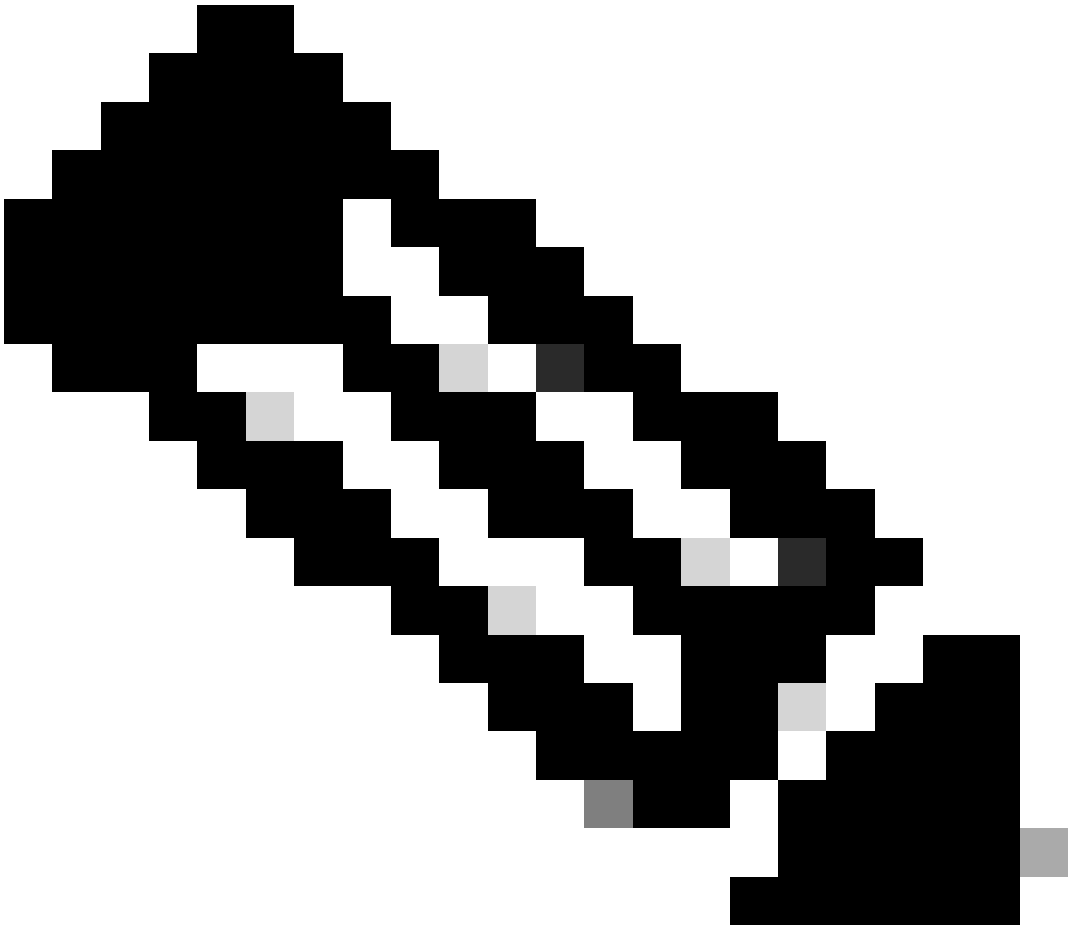
4단계. 모델을 필터링하고 c8000v 라우터를 선택합니다.



5단계. Other Templates(기타 템플릿)로 이동하고 Cli Add-On Template(Cli 애드온 템플릿)을 클릭합니다.

6단계. 템플릿 이름 및 설명을 추가합니다.





참고: CLI 애드온 템플릿에서 변수를 생성하는 방법에 대한 자세한 내용은 CLI 애드온 기능 템플릿을 참조하십시오.

7단계. 명령을 추가합니다.

CLI CONFIGURATION

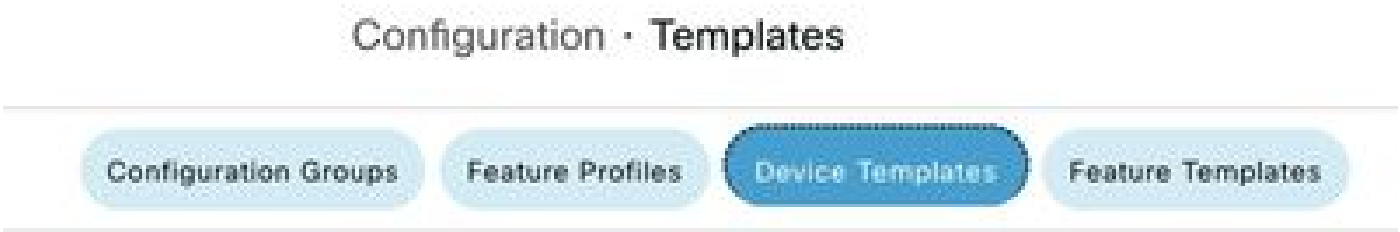
```
crypto ikev2 proposal p1-global
 encryption aes-cbc-128 aes-cbc-256
 integrity sha1 sha256 sha384 sha512
 group 14 15 16
!
crypto ikev2 policy policy1-global
 proposal p1-global
!
crypto ikev2 keyring if-ipsec1-ikev2-keyring
 peer if-ipsec1-ikev2-keyring-peer
  address 10.4.5.226
  pre-shared-key Cisco
 !
!
!
crypto ikev2 profile if-ipsec1-ikev2-profile
 match identity remote address 10.4.5.226 255.255.255.0
 authentication remote pre-share
 authentication local pre-share
 keyring local if-ipsec1-ikev2-keyring
 dpd 10 3 on-demand
 no config-exchange request

crypto ipsec transform-set if-ipsec1-ikev2-transform esp-gcm 256
 mode tunnel
!
!
crypto ipsec profile if-ipsec1-ipsec-profile
 set security-association lifetime kilobytes disable
 set security-association replay window-size 512
 set transform-set if-ipsec1-ikev2-transform
 set ikev2-profile if-ipsec1-ikev2-profile
!
!
!
```

CLI CONFIGURATION

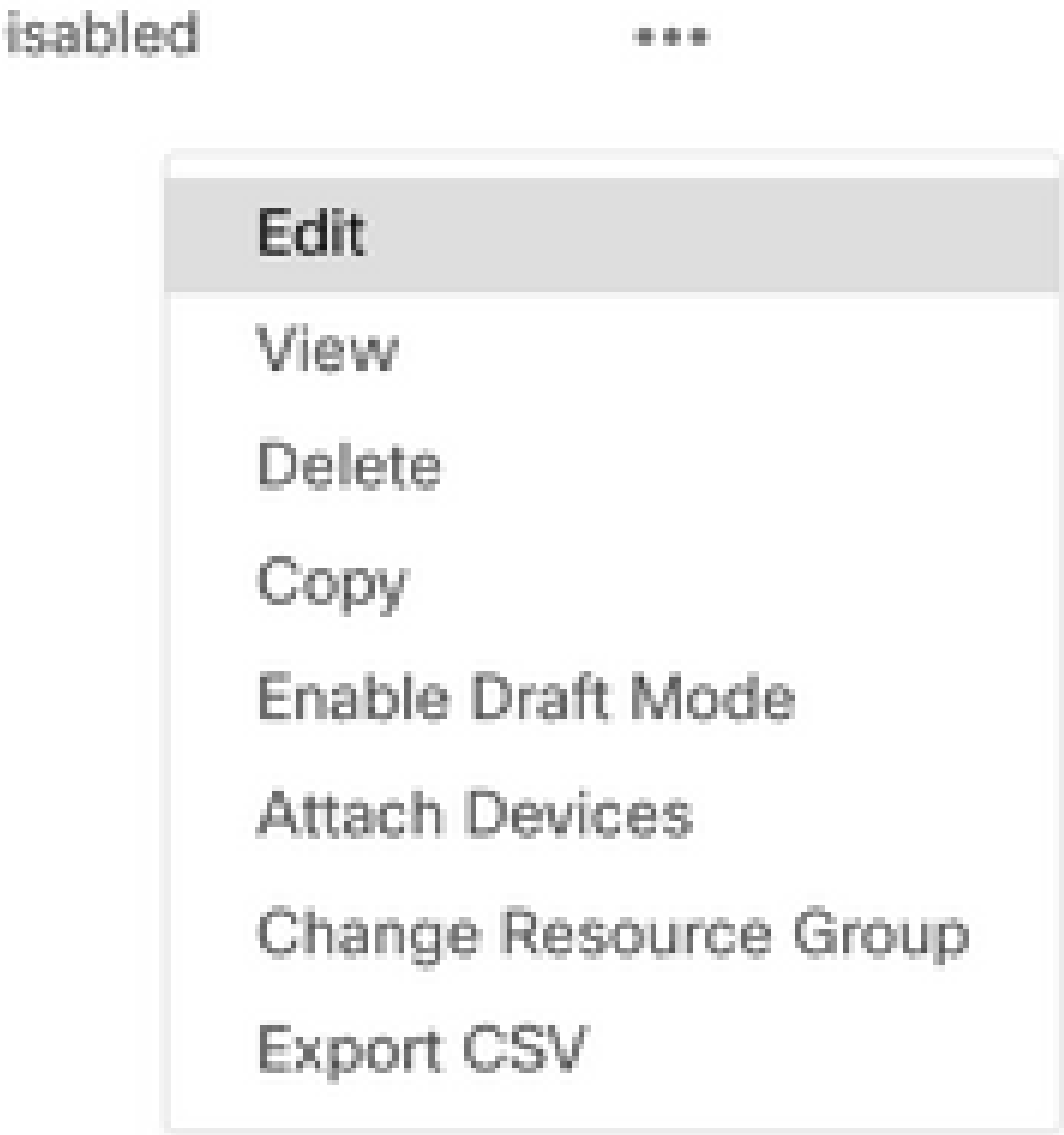
```
 authentication remote pre-share
 authentication local pre-share
 keyring local if-ipsec1-ikev2-keyring
 dpd 10 3 on-demand
 no config-exchange request

crypto ipsec transform-set if-ipsec1-ikev2-transform esp-gcm 256
 mode tunnel
!
!
crypto ipsec profile if-ipsec1-ipsec-profile
 set security-association lifetime kilobytes disable
 set security-association replay window-size 512
 set transform-set if-ipsec1-ikev2-transform
 set ikev2-profile if-ipsec1-ikev2-profile
!
!
!
!
!
!
!
!
interface Tunnel100001
 description Tunnel 1 - Ipsec BGP vWAN Azure
 vrf forwarding 90
 ip address 20.20.20.1 255.255.255.252
 ip mtu 1500
 tunnel source GigabitEthernet1
 tunnel mode ipsec ipv4
 tunnel destination 10.4.5.226
 tunnel path-mtu-discovery
 tunnel protection ipsec profile if-ipsec1-ipsec-profile
!
```

8단계. Save(저장)를 클릭합니다.

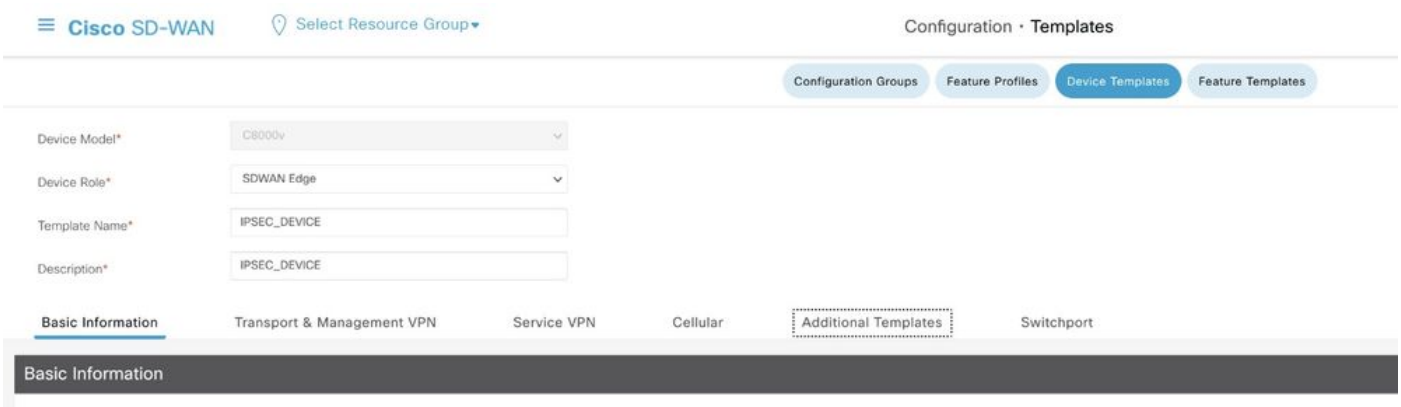
9단계. Device Templates(디바이스 템플릿)로 이동합니다.



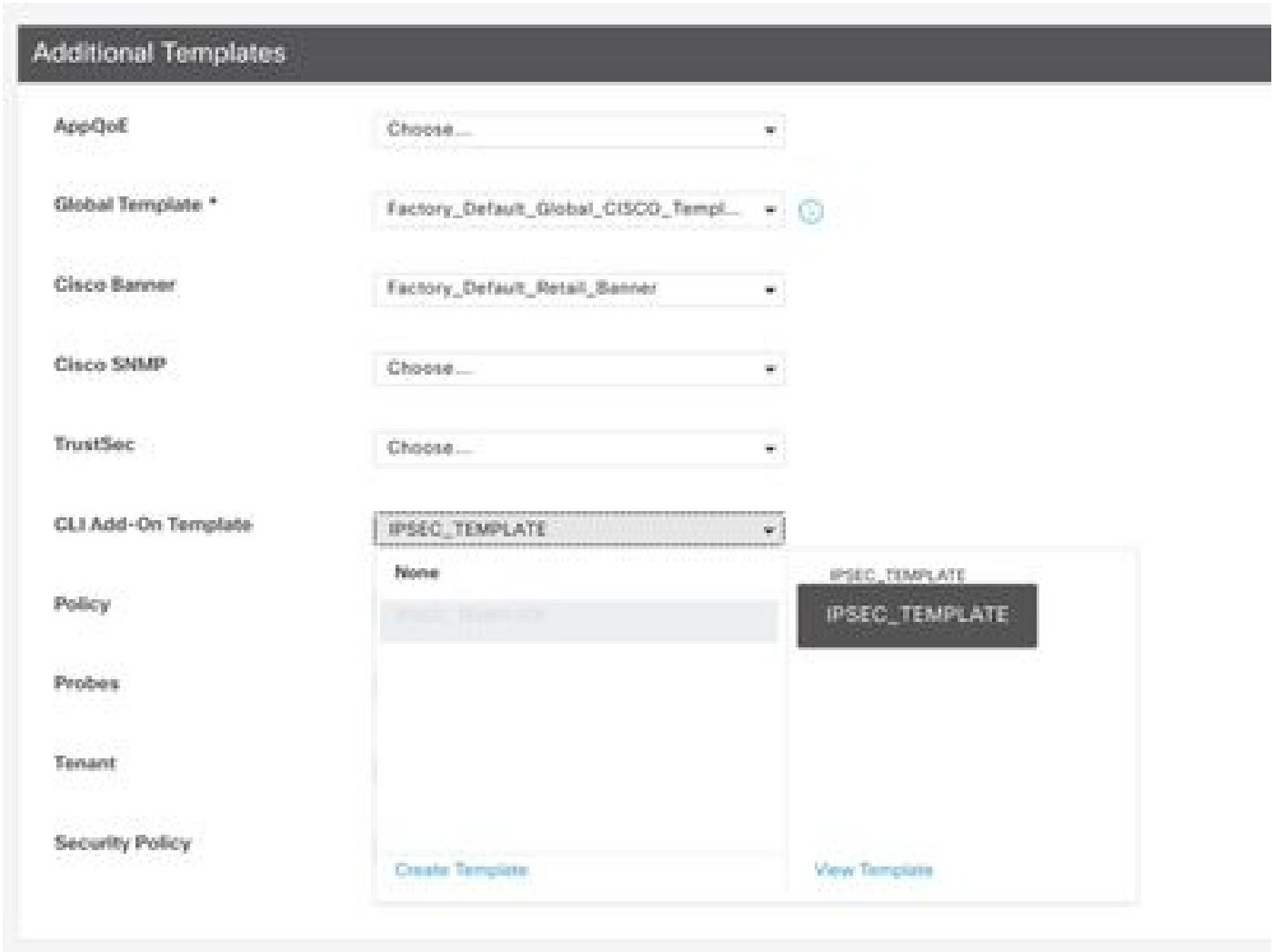
10단계. 올바른 디바이스 템플릿을 선택하고 3개의 점에서 수정합니다.



11단계. Additional Templates(추가 템플릿)로 이동합니다.

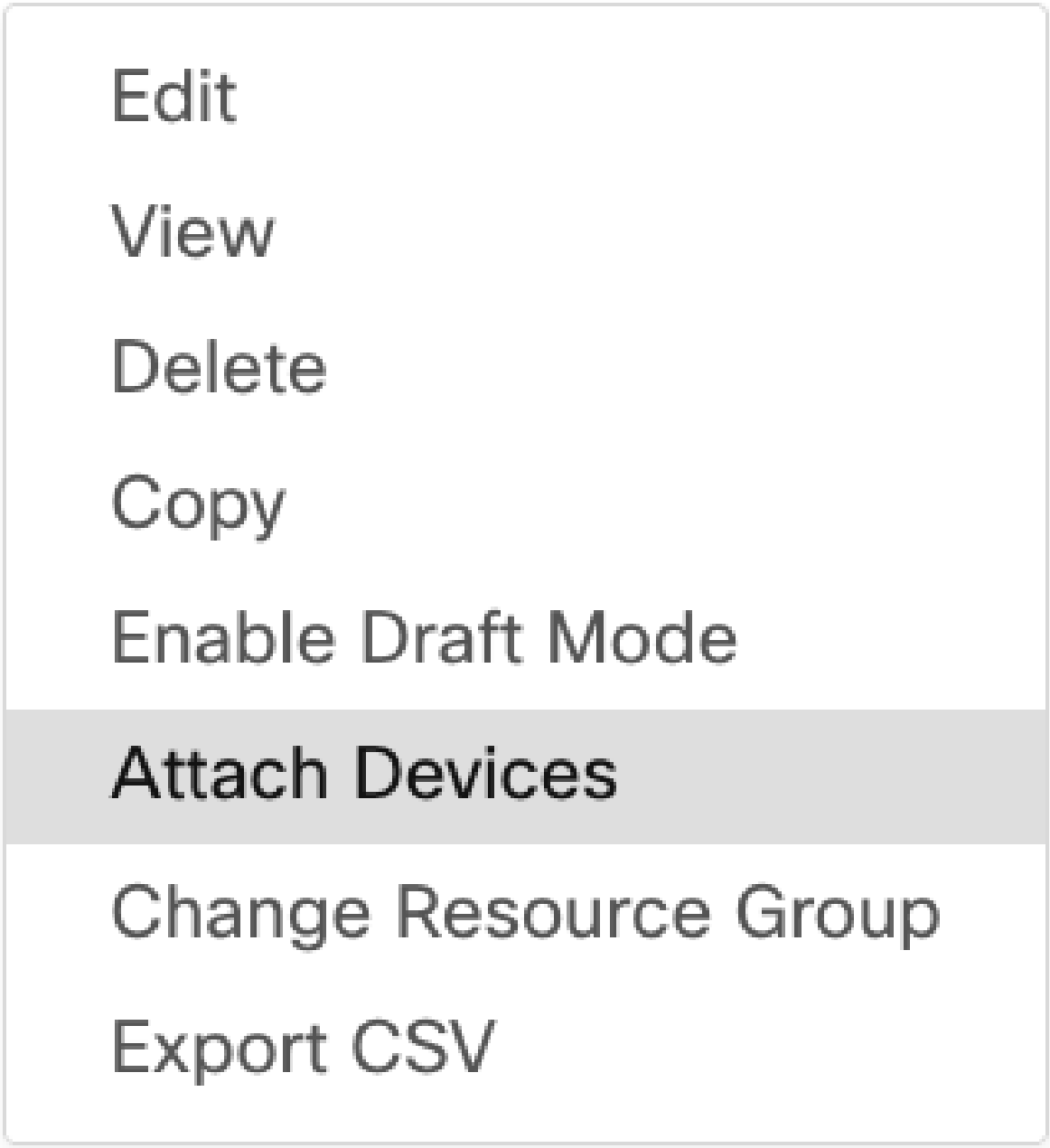


12단계. CLI Add-On Template(CLI 애드온 템플릿)에서 이전에 생성한 Feature Template(기능 템플릿)을 선택합니다.



13단계. Update(업데이트)를 클릭합니다.

14단계. Attach Devices from 3 dots(3개의 점에서 디바이스 연결)를 클릭하고 템플릿을 푸시할 올바른 라우터를 선택합니다.



다음을 확인합니다.

설정이 올바르게 작동하는지 확인하려면 이 섹션을 활용하십시오.

show ip interface brief 명령을 실행하여 IPSec 터널의 상태를 확인합니다.

```
<#root>
cEdge#
show ip interface brief
```

```
Interface IP-Address OK? Method Status Protocol
GigabitEthernet1 10.4.5.224 YES other up up

--- output omitted ---


Tunnel100001 172.16.12.1 YES other up up


cEdge#
```

문제 해결

디바이스에 설정된 IKEv2 세션에 대한 자세한 정보를 표시하려면 show crypto ikev2 session 명령을 실행합니다.

```
<#root>

cEdge#

show crypto ikev2 session


IPv4 Crypto IKEv2 Session

Session-id:1, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id Local Remote fvrf/ivrf Status
1 10.4.5.224/500 10.4.5.225/500 none/90 READY
Encr: AES-CBC, keysize: 128, PRF: SHA1, Hash: SHA96, DH Grp:14, Auth sign: PSK, Auth verify: PSK
Life/Active Time: 86400/207 sec
Child sa: local selector 0.0.0.0/0 - 255.255.255.255/65535
remote selector 0.0.0.0/0 - 255.255.255.255/65535
ESP spi in/out: 0xFC13A6B7/0x1A2AC4A0

IPv6 Crypto IKEv2 Session

cEdge#
```

show crypto ipsec sa interface Tunnel10001 명령을 실행하여 IPSec SA(Security Association)에 대한 정보를 표시합니다.

```
<#root>

cEdge#

show crypto ipsec sa interface Tunnel100001


interface: Tunnel100001
Crypto map tag: Tunnel100001-head-0, local addr 10.4.5.224
```

```
protected vrf: 90
local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
current_peer 10.4.5.225 port 500
PERMIT, flags={origin_is_acl,}
#pkts encaps: 38, #pkts encrypt: 38, #pkts digest: 38
#pkts decaps: 39, #pkts decrypt: 39, #pkts verify: 39
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0

local crypto endpt.: 10.4.5.224, remote crypto endpt.: 10.4.5.225
plaintext mtu 1446, path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet1
current outbound spi: 0x1A2AC4A0(439010464)
PFS (Y/N): N, DH group: none

inbound esp sas:
spi: 0xFC13A6B7(4229146295)
transform: esp-gcm 256 ,
in use settings ={Tunnel, }
conn id: 2001, flow_id: CSR:1, sibling_flags FFFFFFFF80000048, crypto map: Tunnel100001-head-0
sa timing: remaining key lifetime (sec): 2745
Kilobyte Volume Rekey has been disabled
IV size: 8 bytes
replay detection support: Y replay window size: 512
Status: ACTIVE(ACTIVE)

inbound ah sas:

inbound pcp sas:

outbound esp sas:
spi: 0x1A2AC4A0(439010464)
transform: esp-gcm 256 ,
in use settings ={Tunnel, }
conn id: 2002, flow_id: CSR:2, sibling_flags FFFFFFFF80000048, crypto map: Tunnel100001-head-0
sa timing: remaining key lifetime (sec): 2745
Kilobyte Volume Rekey has been disabled
IV size: 8 bytes
replay detection support: Y replay window size: 512
Status: ACTIVE(ACTIVE)

outbound ah sas:

outbound pcp sas:
cEdge#
```

show crypto ikev2 statistics 명령을 실행하여 IKEv2 세션과 관련된 통계 및 카운터를 표시합니다.

<#root>

```
cEdge#
```

show crypto ikev2 statistics

```
------------------------------------------------------------------------------
Crypto IKEv2 SA Statistics
```

```
------------------------------------------------------------------------------
System Resource Limit: 0 Max IKEv2 SAs: 0 Max in nego(in/out): 40/400
Total incoming IKEv2 SA Count: 0 active: 0 negotiating: 0
Total outgoing IKEv2 SA Count: 1 active: 1 negotiating: 0
Incoming IKEv2 Requests: 0 accepted: 0 rejected: 0
Outgoing IKEv2 Requests: 1 accepted: 1 rejected: 0
Rejected IKEv2 Requests: 0 rsrc low: 0 SA limit: 0
IKEv2 packets dropped at dispatch: 0
Incoming Requests dropped as LOW Q limit reached : 0
Incoming IKEV2 Cookie Challenged Requests: 0
accepted: 0 rejected: 0 rejected no cookie: 0
Total Deleted sessions of Cert Revoked Peers: 0

cEdge#
```

디바이스의 활성 보안 세션에 대한 정보를 표시하려면 show crypto session 명령을 실행합니다.

<#root>

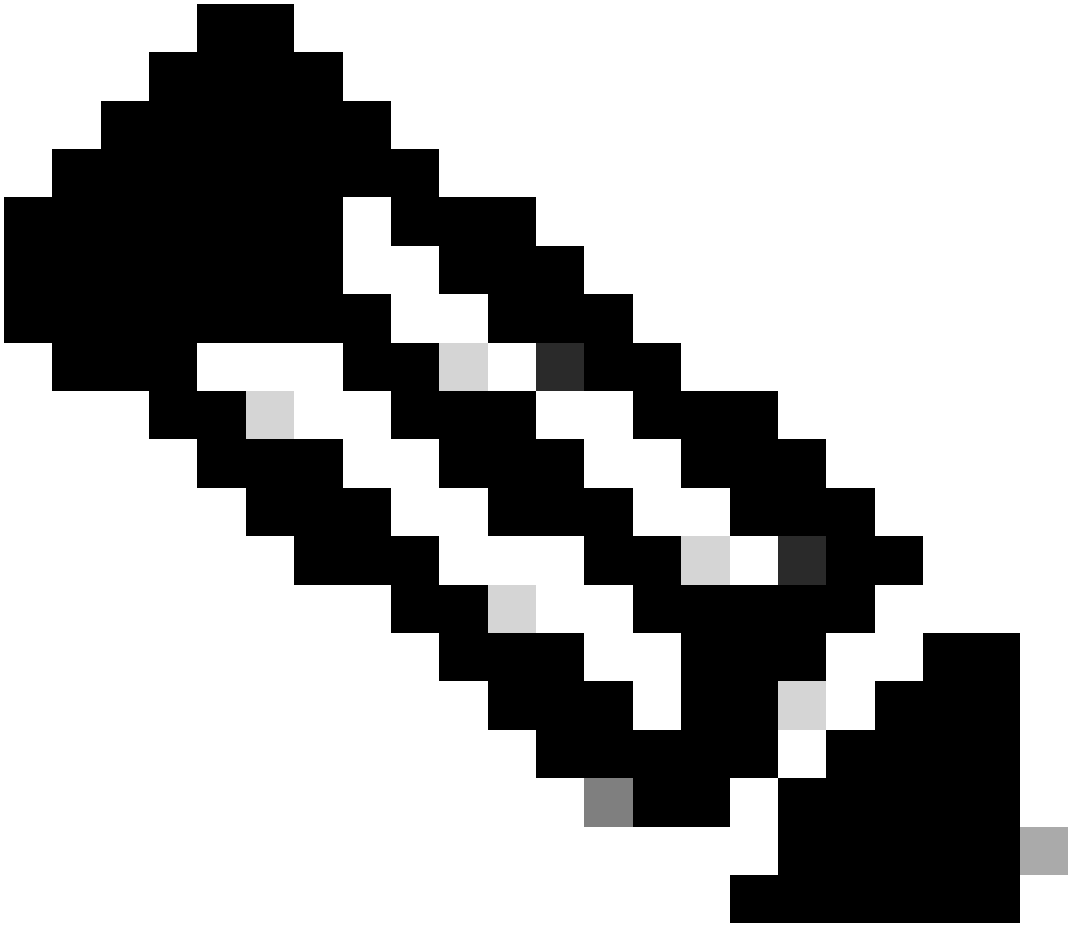
```
cEdge#

show crypto session


Crypto session current status

Interface: Tunnel100001
Profile: if-ipsec1-ikev2-profile
Session status: UP-ACTIVE
Peer: 10.4.5.225 port 500
Session ID: 1
IKEv2 SA: local 10.4.5.224/500 remote 10.4.5.225/500 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
```

디바이스 패킷 프로세서에서 IPSec 관련 패킷 삭제에 대한 정보를 얻으려면 다음을 실행할 수 있습니다.

show platform hardware qfp active feature ipsec datapath drops clear

show platform hardware qfp active statistics 삭제

이러한 명령은 터널 인터페이스를 종료하기 전에 완료하고 종료하지 않아야 카운터와 통계를 지울 수 있습니다. 이렇게 하면 디바이스 패킷 프로세서 데이터 경로에 있는 IPsec 관련 패킷 삭제에 대한 정보를 얻을 수 있습니다.



참고: 이러한 명령은 clear 옵션을 사용하지 않고 실행할 수 있습니다. 드롭 카운터가 기록 카운터임을 강조하는 것이 중요합니다.

<#root>

```
cEdge#

show platform hardware qfp active feature ipsec datapath drops clear


----------------------------------------------------------------------
Drop Type Name Packets
----------------------------------------------------------------------



IPSEC detailed dp drop counters cleared after display.

cEdge#
```

<#root>

cEdge#

show platform hardware qfp active statistics drop clear

Last clearing of QFP drops statistics : Thu Sep 28 01:35:11 2023

Global Drop Stats Packets Octets

Ipv4NoRoute 17 3213
UnconfiguredIpv6Fia 18 2016

cEdge#

터널 인터페이스를 종료하고 종료하지 않은 후 다음 명령을 실행하여 새 통계 또는 카운터가 등록되었는지 확인할 수 있습니다.

show ip interface brief | 터널 포함100001

show platform hardware qfp active statistics drop(플랫폼 하드웨어 qfp 활성 통계 표시)

플랫폼 하드웨어 qfp 활성 기능 ipsec 데이터 경로 삭제 표시

<#root>

cEdge#

show ip interface brief | include Tunnel100001

Tunnel100001 169.254.21.1 YES other up up
cEdge#
cEdge#sh pl hard qfp act feature ipsec datapath drops

Drop Type Name Packets

<#root>

cEdge#

show platform hardware qfp active statistics drop

Last clearing of QFP drops statistics : Thu Sep 28 01:35:11 2023
(5m 23s ago)

Global Drop Stats Packets Octets

Ipv4NoRoute 321 60669
UnconfiguredIpv6Fia 390 42552

```
cEdge#
```

<#root>

```
cEdge#
```

show platform hardware qfp active feature ipsec datapath drops

```
----------------------------------------------------------------------
Drop Type Name Packets
----------------------------------------------------------------------

cEdge#
```

유용한 명령

<#root>

show crypto ipsec sa peer <peer_address> detail

show crypto ipsec sa peer <peer_address> platform

show crypto ikev2 session

show crypto ikev2 profile

show crypto isakmp policy

show crypto map

show ip static route vrf NUMBER

show crypto isakmp sa

debug crypto isakmp

debug crypto ipsec

관련 정보

IPsec Pairwise 키

Cisco Catalyst SD-WAN 보안 컨피그레이션 가이드, Cisco IOS® XE Catalyst SD-WAN 릴리스 17.x

Cisco IPsec 기술 소개

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.