SD-WAN ZBFW(Zone-Based Firewall) 및 경로 유출 구성

목차

소개

이 문서에서는 VPN(Virtual Private Networks) 간 경로 누설(Route-Leasing)을 사용하여 ZBFW(Zone-Based Firewall)를 구성, 확인 및 트러블슈팅하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco SD-WAN 오버레이는 초기 컨피그레이션을 제공합니다.
- vManage 사용자 인터페이스(UI)의 ZBFW 컨피그레이션
- vManage UI에서 경로 유출 제어 정책 컨피그레이션

사용되는 구성 요소

이 데모에서는 다음과 같은 소프트웨어가 사용되었습니다.

- 20.6.2 소프트웨어 릴리스가 포함된 Cisco SD-WAN vSmart Controller
- 20.6.2 소프트웨어 릴리스가 포함된 Cisco SD-WAN vManage 컨트롤러
- 컨트롤러 모드에서 실행되는 17.6.2 소프트웨어 릴리스가 포함된 Cisco IOS®-XE Catalyst

8000V 가상 에지 플랫폼 라우터 2개
- 자동 모드에서 실행되는 17.6.2 소프트웨어 릴리스가 포함된 Cisco IOS-XE Catalyst 8000V 가상 에지 플랫폼 라우터 3개

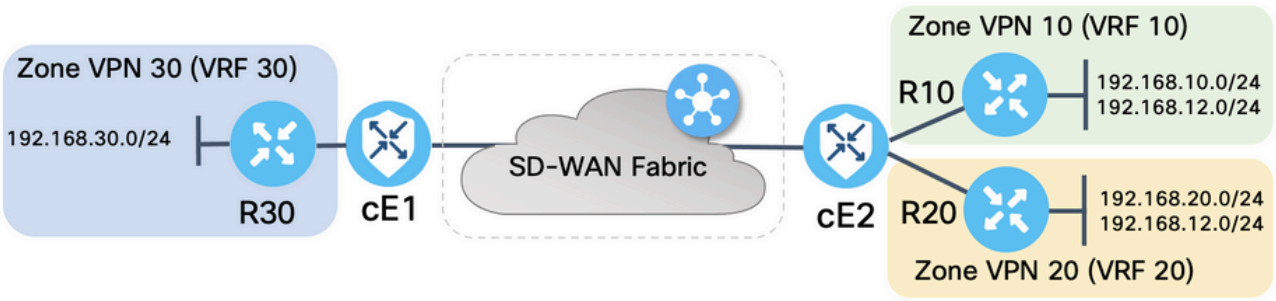
이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 이해해야 합니다.

배경 정보

이 문서에서는 라우터가 SD-WAN 오버레이에서 대상 VPN 매핑을 결정하는 방법과 VPN 간 경로 누설을 확인하고 문제를 해결하는 방법에 대해 설명합니다. 또한 다른 VPN에서 동일한 서브넷을 광고하는 경우 경로 선택의 특징과 이로 인해 발생할 수 있는 문제에 대해서도 설명합니다.

구성

네트워크 다이어그램



두 SD-WAN 라우터는 SD-WAN 컨트롤러와의 제어 연결 및 SD-WAN 컨트롤러 간의 데이터 플레인 연결을 설정하기 위한 기본 매개 변수로 구성되었습니다. 이 구성의 세부 정보는 이 문서의 목적에 맞지 않습니다. 이 표에는 VPN, 사이트 ID 및 영역 할당이 요약되어 있습니다.

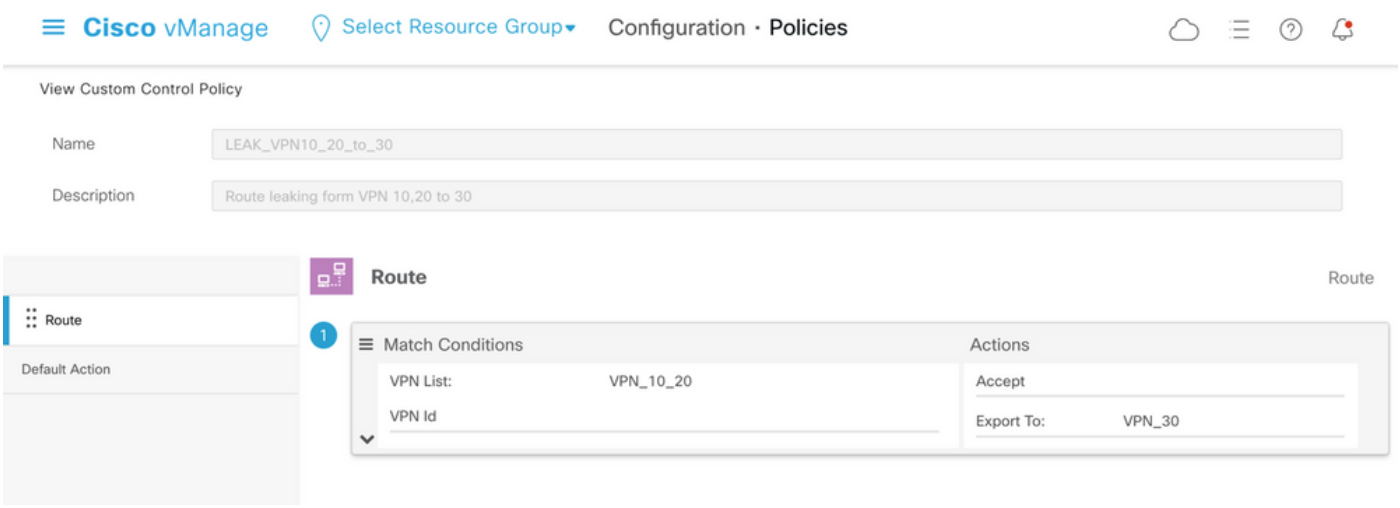
	cE1	cE2
사이트 ID	11	12
VPN	30	10,20
시스템-IP	169.254.206.11	169.254.206.12

서비스 측의 라우터는 각 VRF(Virtual Routing and Forwarding)에서 해당 SD-WAN 라우터를 가리키는 고정 기본 경로로 구성되었습니다. 마찬가지로, SD-WAN Edge 라우터는 해당하는 서브넷을 가리키는 고정 경로로 구성되었습니다. 경로 유출 및 ZBFW와 관련된 잠재적인 문제를 설명하기 위해 cE2 서비스 쪽 뒤에 있는 라우터는 동일한 서브넷 192.168.12.0/24을 가집니다. cE2 뒤의 두 라우터에는 동일한 IP 주소 192.168.12.12의 호스트를 에뮬레이션하도록 구성된 루프백 인터페이스가 있습니다.

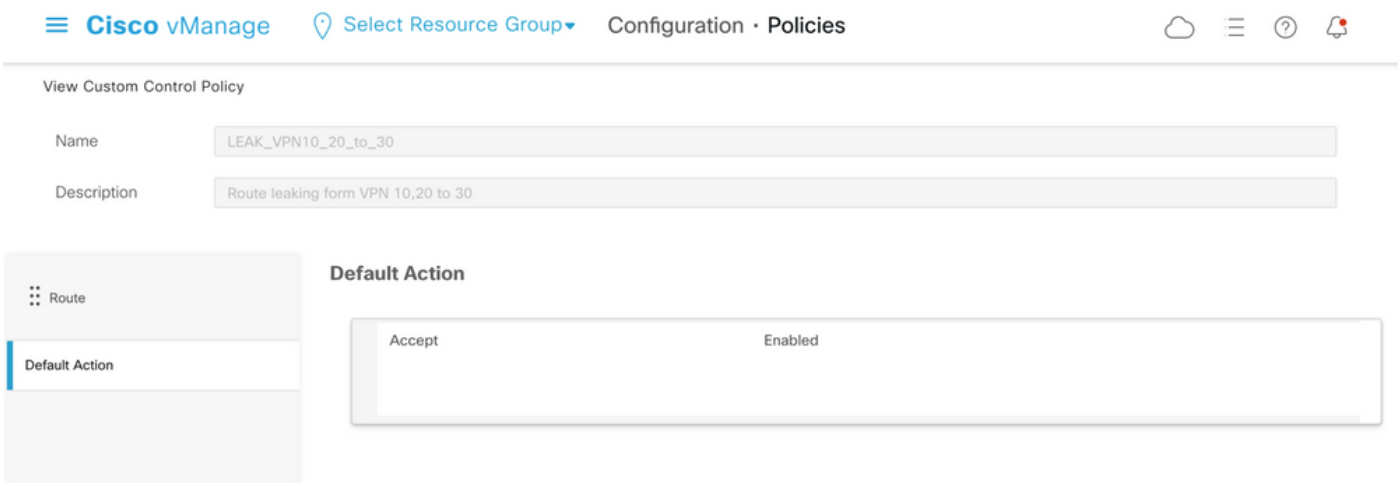
Cisco IOS-XE 라우터 R10, R20 및 R30은 이 데모에서 주로 엔드 호스트를 에뮬레이션하는 SD-WAN Edge 경로의 서비스 측에서 자동 모드로 실행됩니다. SD-WAN 에지 라우터의 VRF에서 시작된 트래픽은 이에 해당하는 ZBFW 영역에서 시작된 트래픽으로 간주되지 않으며 에지 라우터의 특수 자체 영역에 속하기 때문에 SD-WAN 에지 경로의 루프백 인터페이스를 서비스 측 라우터와 같은 실제 호스트 대신 이 용도로 사용할 수 없습니다. 따라서 ZBFW 영역은 VRF와 동일하게 간주할 수 없습니다. 자기구역에 대한 자세한 논의는 이 문서의 범위를 벗어난다.

경로 유출 컨피그레이션

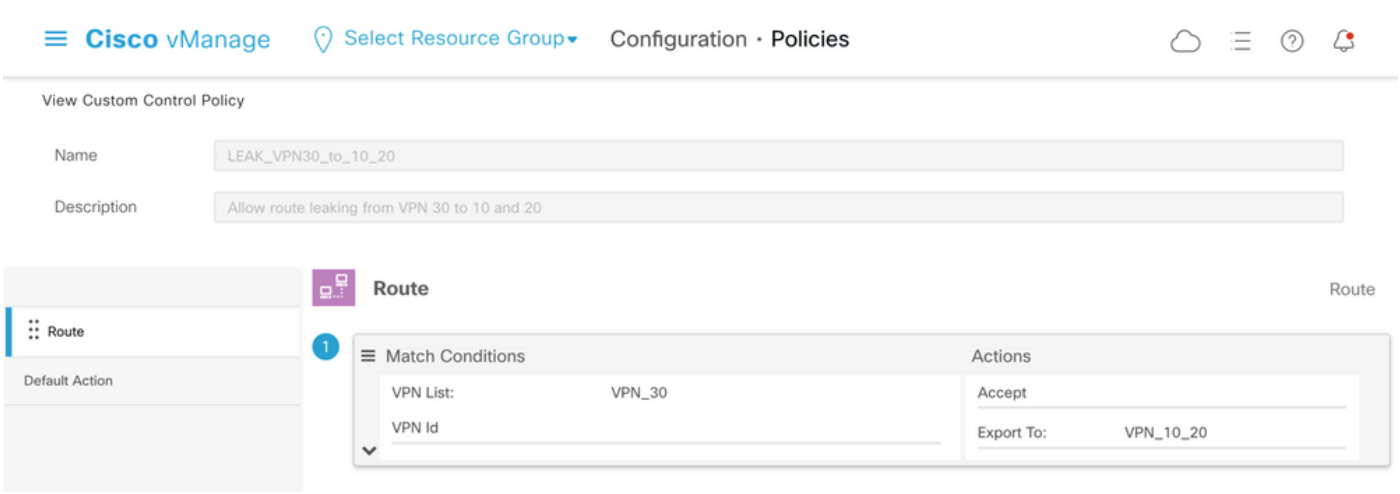
주요 제어 정책 구성 목표는 VPN 10 및 20에서 VPN 30으로 모든 경로의 경로 누수를 허용하는 것입니다. VRF 30은 라우터 cE1에만 있고 VRF 10 및 20은 라우터 cE2에서만 구성됩니다. 이를 위해 2개의 토폴로지(Custom Control) 정책이 구성되었습니다. 다음은 VPN 10 및 20에서 VPN 30으로 모든 경로를 내보내는 토폴로지입니다.

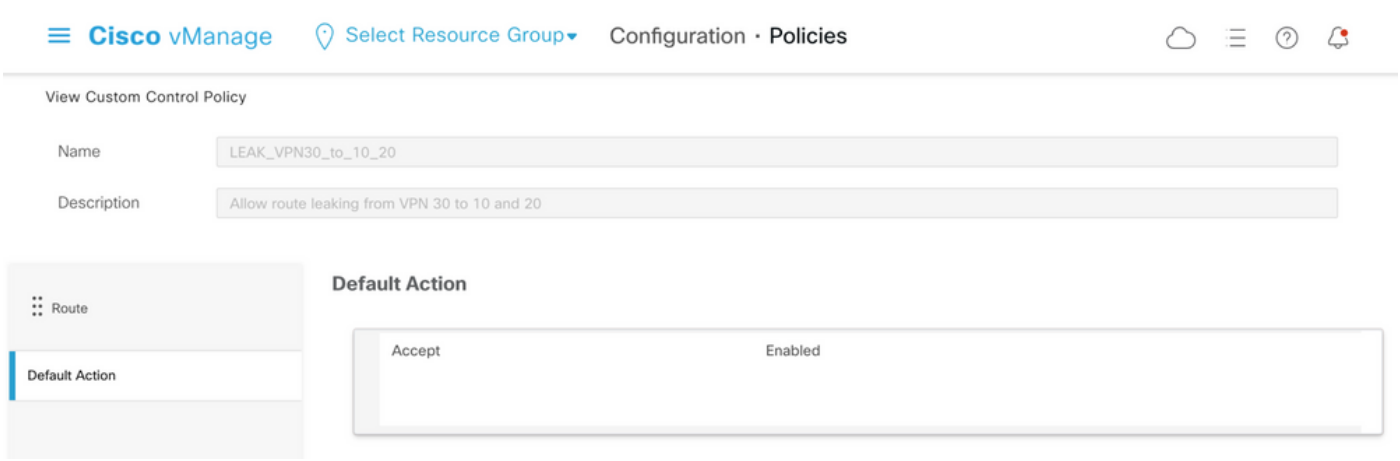


Default Action(기본 작업)은 Allow(허용)로 설정되어 실수로 TLOC 광고 또는 정상적인 intra-VPN 경로 광고 차단을 피합니다.

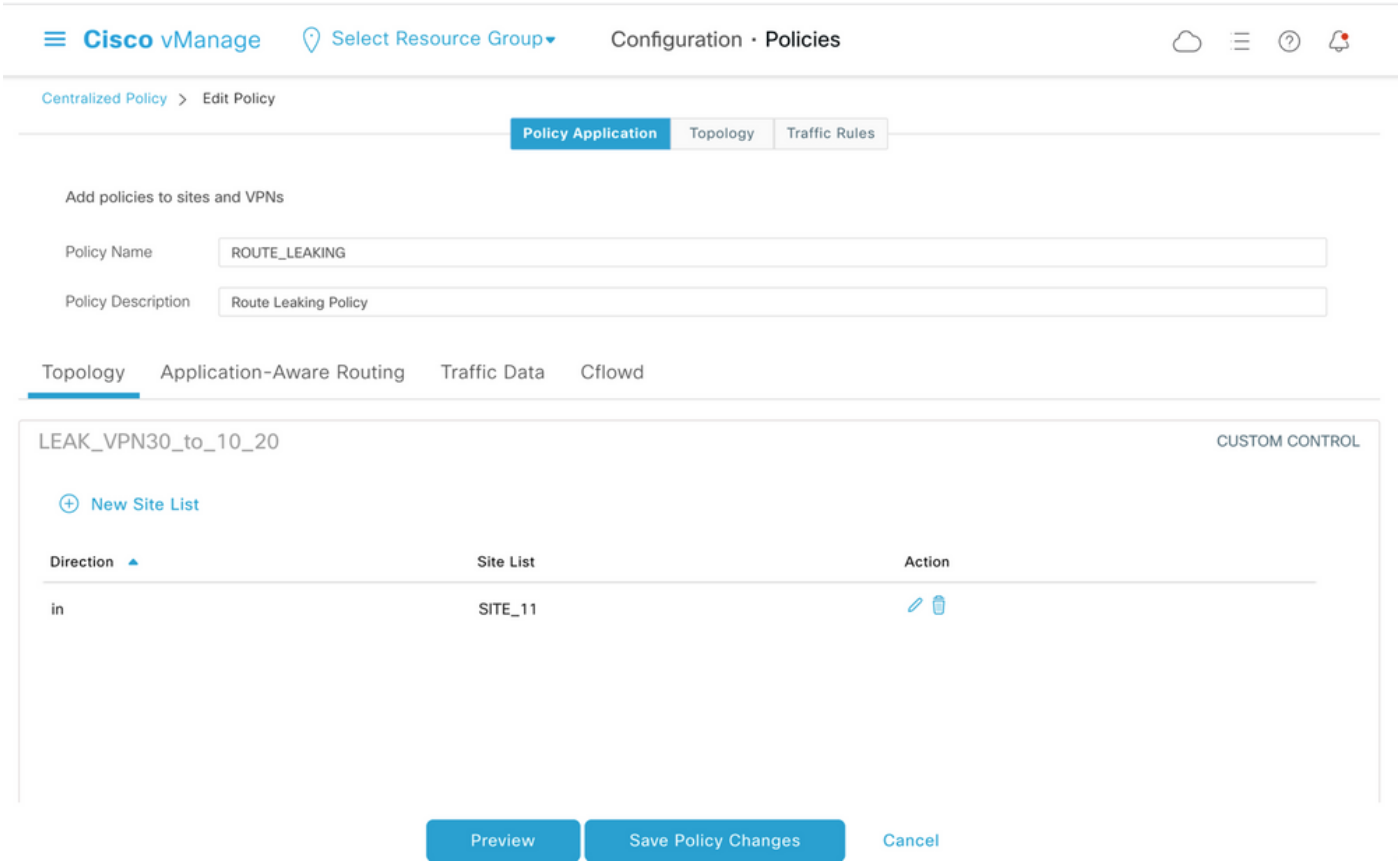


마찬가지로 토폴로지 정책은 VPN 30에서 VPN 10 및 20으로 라우팅 정보를 역방향 광고하도록 구성되었습니다.

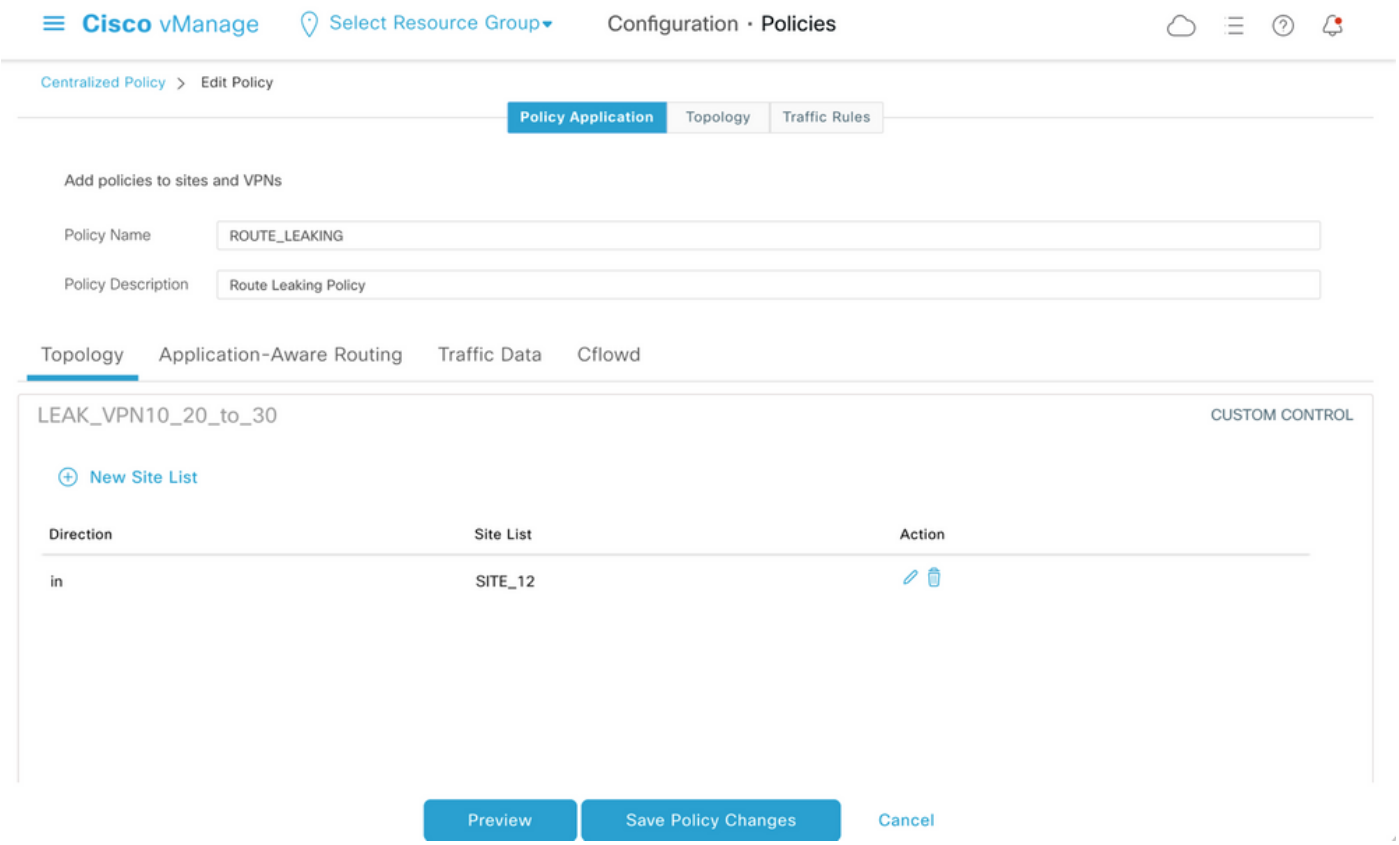




그런 다음 두 토폴로지 정책 모두 인그레스(수신) 방향에 해당하는 사이트 목록에 할당됩니다. VPN 30의 경로는 vSmart 컨트롤러에서 cE1(site-id 11)에서 수신될 때 VPN 10 및 20의 OMP(Overlay Management Protocol) 테이블로 내보냅니다.



마찬가지로, vSmart에서 VPN 10 및 20의 경로를 cE2에서 VPN 10 및 20개의 경로를 수신하면 VPN 30 라우팅 테이블로 내보냅니다(site-id 12).



또한 참조를 위한 완벽한 제어 정책 컨피그레이션 미리보기입니다.

```
viptela-policy:policy control-policy LEAK_VPN10_20_to_30 sequence 1 match route vpn-list
VPN_10_20 prefix-list _AnyIpv4PrefixList ! action accept export-to vpn-list VPN_30 ! ! default-
action accept ! control-policy LEAK_VPN30_to_10_20 sequence 1 match route vpn-list VPN_30
prefix-list _AnyIpv4PrefixList ! action accept export-to vpn-list VPN_10_20 ! ! default-action
accept ! lists site-list SITE_11 site-id 11 ! site-list SITE_12 site-id 12 ! vpn-list VPN_10_20
vpn 10 vpn 20 ! vpn-list VPN_30 vpn 30 ! prefix-list _AnyIpv4PrefixList ip-prefix 0.0.0.0/0 le
32 ! ! ! apply-policy site-list SITE_12 control-policy LEAK_VPN10_20_to_30 in ! site-list
SITE_11 control-policy LEAK_VPN30_to_10_20 in ! !
```

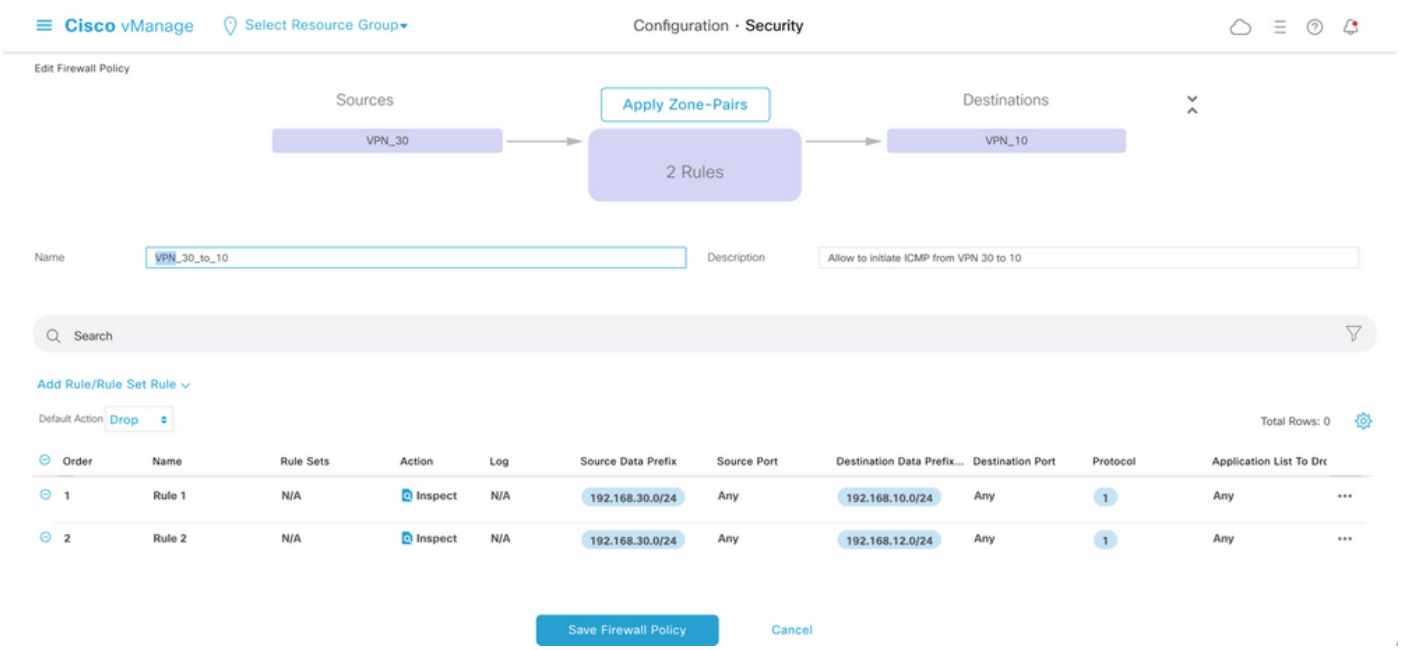
vSmart 컨트롤러에서 적용하려면 vManage 컨트롤러 Configuration(컨피그레이션) **> Policies(정책)** 섹션에서 정책을 활성화해야 합니다.

ZBFW 컨피그레이션

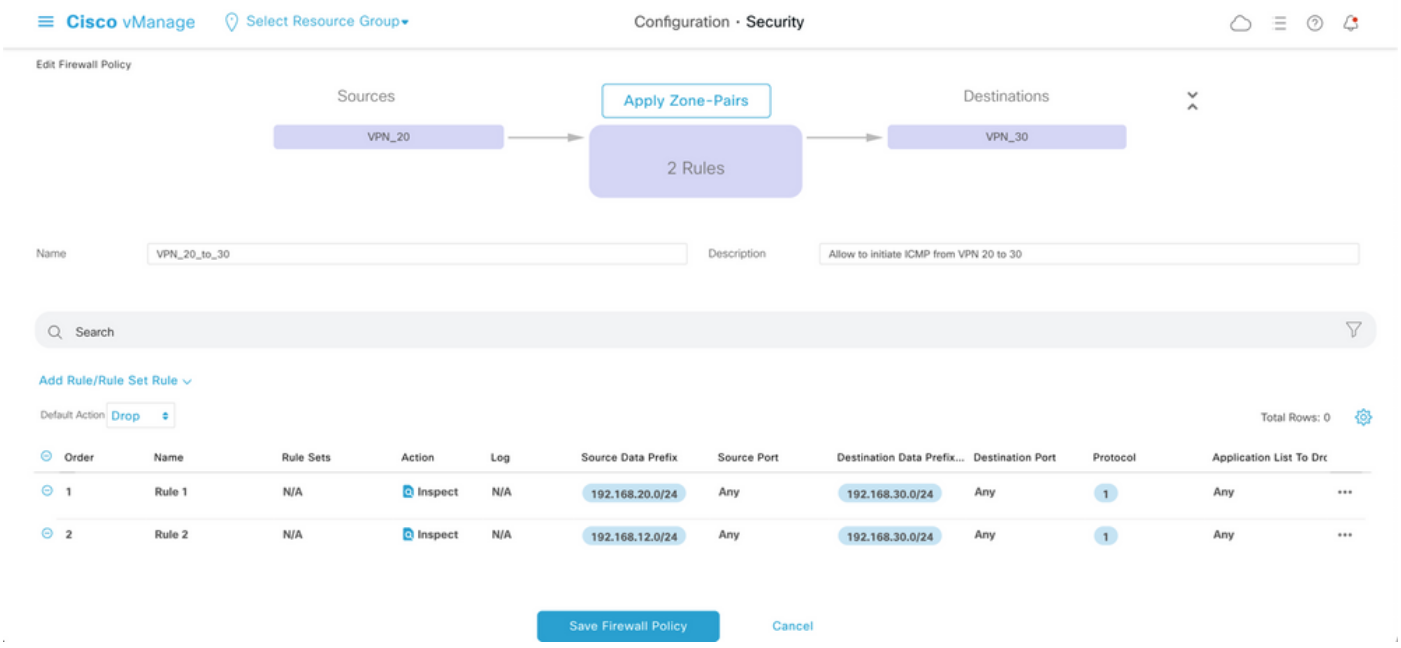
이 문서에서 데모를 위한 요건을 필터링하기 위해 ZBFW를 요약한 표가 있습니다.

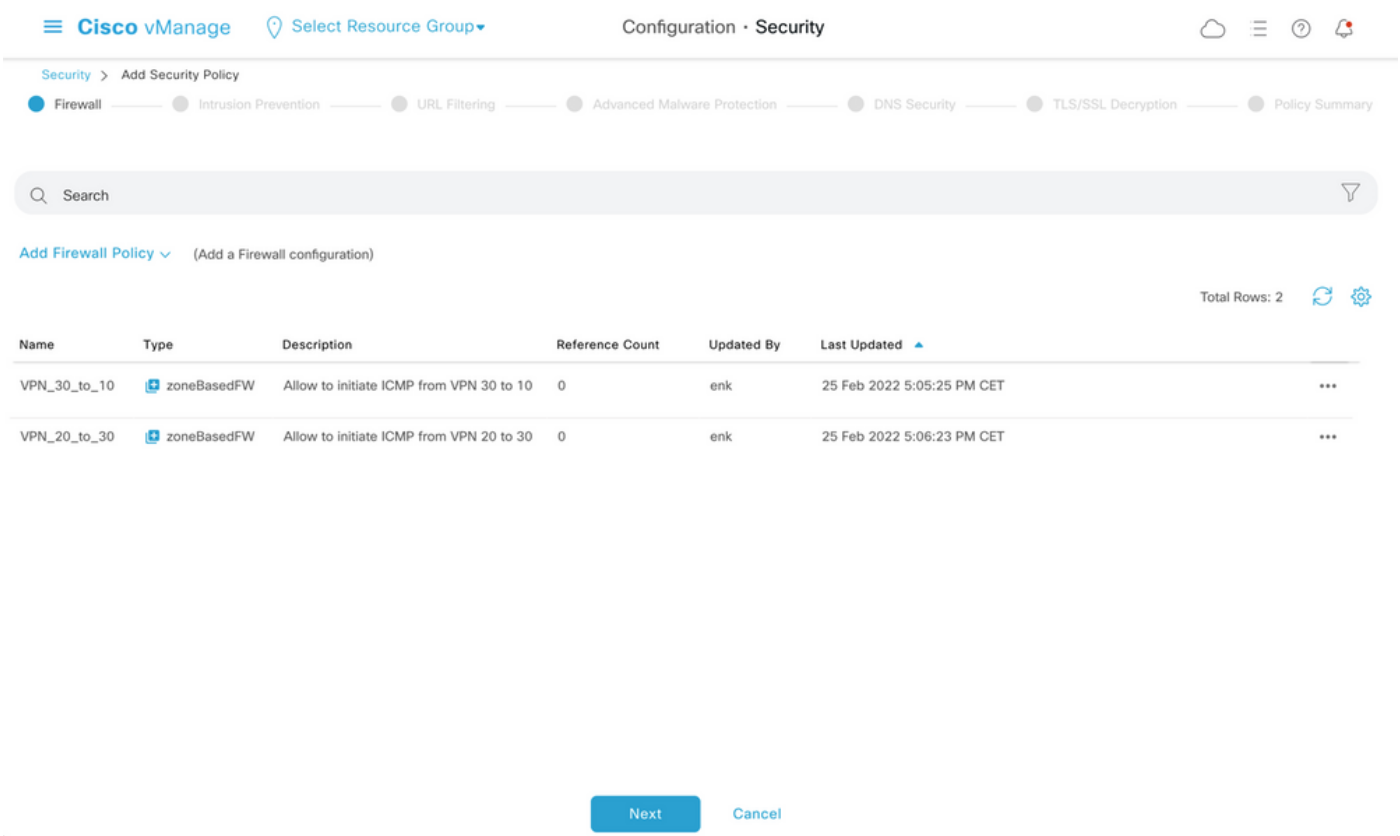
대상 영역 소스 영역	VPN_10	VPN_20	VPN_30
VPN_10	영역 내 허용	거부	거부
VPN_20	거부	영역 내 허용	허용
VPN_30	허용	거부	영역 내 허용

주요 목표는 라우터 cE1 VPN 30의 서비스 측면에서 시작되어 VPN 10으로 이동하지만 VPN 20으로 이동하지 않는 ICMP(Internet Control Message Protocol) 트래픽을 허용하는 것입니다. 반환 트래픽은 자동으로 허용되어야 합니다.



또한 라우터 cE2 서비스 측 VPN 20에서 오는 모든 ICMP 트래픽은 cE1의 VPN 30 서비스 쪽(VPN 10에서)으로 전송하도록 허용해야 합니다. VPN 30에서 VPN 20으로 반환 트래픽은 자동으로 허용되어야 합니다.

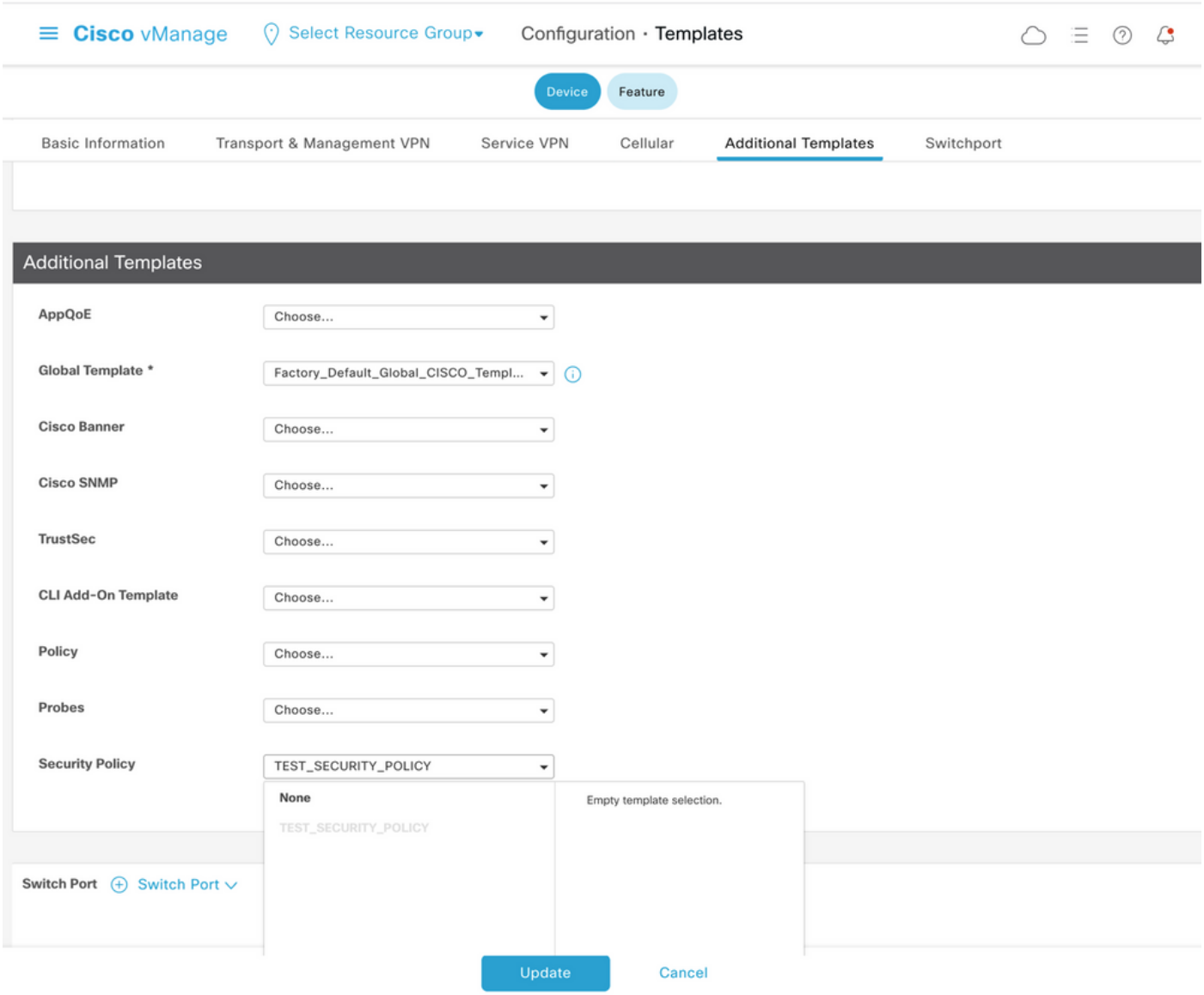




여기에서 참조할 ZBFW 정책 미리 보기를 찾을 수 있습니다.

```
policy zone-based-policy VPN_20_to_30 sequence 1 seq-name Rule_1 match source-ip 192.168.20.0/24
destination-ip 192.168.30.0/24 protocol 1 ! action inspect ! ! sequence 11 seq-name Rule_2 match
source-ip 192.168.12.0/24 destination-ip 192.168.30.0/24 protocol 1 ! action inspect ! !
default-action drop ! zone-based-policy VPN_30_to_10 sequence 1 seq-name Rule_1 match source-ip
192.168.30.0/24 destination-ip 192.168.10.0/24 protocol 1 ! action inspect ! ! sequence 11 seq-
name Rule_2 match protocol 1 source-ip 192.168.30.0/24 destination-ip 192.168.12.0/24 ! action
inspect ! ! default-action drop ! zone VPN_10 vpn 10 ! zone VPN_20 vpn 20 ! zone VPN_30 vpn 30 !
zone-pair ZP_VPN_20_VPN_30_VPN_20_to_30 source-zone VPN_20 destination-zone VPN_30 zone-policy
VPN_20_to_30 ! zone-pair ZP_VPN_30_VPN_10_VPN_30_to_10 source-zone VPN_30 destination-zone
VPN_10 zone-policy VPN_30_to_10 ! zone-to-nozone-internet deny !
```

보안 정책을 적용하려면 디바이스 템플릿의 **Additional Templates** 섹션의 **Security Policy(보안 정책)** 드롭다운 메뉴 섹션에 보안 정책을 할당해야 합니다.



디바이스 템플릿이 업데이트되면 보안 정책이 적용된 디바이스에서 보안 정책이 활성화됩니다. 이 문서의 데모에서는 cE1 라우터에서만 보안 정책을 활성화할 수 있었습니다.

다음을 확인합니다.

이제 필수 ZBFW(보안 정책) 목표가 달성되었는지 확인해야 합니다.

ping을 **사용하여** 테스트하면 VPN 10에서 VPN 30까지의 트래픽에 대해 구성된 zone-pair가 없으므로 zone VPN 10에서 VPN 30까지의 트래픽이 예상대로 거부되는지 확인합니다.

```
R10#ping 192.168.30.30 source 192.168.10.10 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 192.168.30.30, timeout is 2 seconds: Packet sent with a source address of 192.168.10.10 ..... Success rate is 0 percent (0/5) R10#ping 192.168.30.30 source 192.168.12.12 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 192.168.30.30, timeout is 2 seconds: Packet sent with a source address of 192.168.12.12 ..... Success rate is 0 percent (0/5)
```

마찬가지로, 보안 정책 컨피그레이션에서 예상한 대로 VPN 20의 트래픽이 VPN 30에 허용됩니다.

```
R20#ping 192.168.30.30 source 192.168.20.20 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 192.168.30.30, timeout is 2 seconds: Packet sent with a source address of
```

```
192.168.20.20 !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
R20#ping 192.168.30.30 source 192.168.12.12 Type escape sequence to abort. Sending 5, 100-byte
ICMP Echos to 192.168.30.30, timeout is 2 seconds: Packet sent with a source address of
192.168.12.12 !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

영역 VPN 10의 VPN 30에서 서브넷 192.168.10.0/24으로 이동하는 트래픽은 정책 컨피그레이션에서 예상한 대로 허용됩니다.

```
R30#ping 192.168.10.10 source 192.168.30.30 Type escape sequence to abort. Sending 5, 100-byte
ICMP Echos to 192.168.10.10, timeout is 2 seconds: Packet sent with a source address of
192.168.30.30 !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

이 트래픽에 대해 구성된 영역 쌍이 없기 때문에 영역 VPN 20의 VPN 30에서 서브넷 192.168.20.0/24으로 향하는 트래픽이 거부됩니다. 이는 예상됩니다.

```
R30#ping 192.168.20.20 source 192.168.30.30 Type escape sequence to abort. Sending 5, 100-byte
ICMP Echos to 192.168.20.20, timeout is 2 seconds: Packet sent with a source address of
192.168.30.30 ..... Success rate is 0 percent (0/5)
```

IP 주소 192.168.12.12은 영역 VPN 10 또는 VPN 20에 있을 수 있으므로 ping을 시도할 때 관심 있는 추가 결과를 확인할 수 있으며, SD-WAN 에지 라우터 cE1의 서비스 쪽에 있는 라우터 R30의 관점에서 대상 VPN을 확인할 수 없습니다.

```
R30#ping 192.168.12.12 source 192.168.30.30 Type escape sequence to abort. Sending 5, 100-byte
ICMP Echos to 192.168.12.12, timeout is 2 seconds: Packet sent with a source address of
192.168.30.30 ..... Success rate is 0 percent (0/5)
```

결과는 VRF 30의 모든 소스에 대해 동일합니다. 따라서 ECMP(Equal-Cost Multi-Path) 해시 함수 결과에 종속되지 않습니다.

```
R30#ping 192.168.12.12 source 192.168.30.31 Type escape sequence to abort. Sending 5, 100-byte
ICMP Echos to 192.168.12.12, timeout is 2 seconds: Packet sent with a source address of
192.168.30.31 ..... Success rate is 0 percent (0/5) R30#ping 192.168.12.12 source 192.168.30.32
Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 192.168.12.12, timeout is 2
seconds: Packet sent with a source address of 192.168.30.32 ..... Success rate is 0 percent
(0/5)
```

목적지 IP 192.168.12.12의 테스트 결과를 기반으로, VPN 20에서는 ICMP 에코 요청에 응답하지 않으며 VPN 30에서 VPN 20으로의 트래픽을 허용하도록 구성된 zone-pair가 없기 때문에(원하는 경우)만 찾을 수 있습니다. IP 주소가 192.168.12.12인 대상이 VPN 10에 있고 ICMP 에코 요청에 응답한다고 가정할 경우, VPN 30에서 VPN 20으로의 ICMP 트래픽에 대한 ZBFW 보안 정책에 따라 트래픽이 허용되어야 합니다. 대상 VPN을 확인해야 합니다.

문제 해결

방법 1. OMP 테이블에서 대상 VPN을 찾으려면

cE1에서 라우팅 테이블을 간단히 확인해도 실제 대상 VPN을 이해하는 데 도움이 되지 않습니다. 출력에서 얻을 수 있는 가장 유용한 정보는 대상(169.254.206.12)의 시스템 IP이며, ECMP가 없다는 것입니다.

```
cE1# show ip route vrf 30 192.168.12.0 255.255.255.0 Routing Table: 30 Routing entry for
192.168.12.0/24 Known via "omp", distance 251, metric 0, type omp Last update from
169.254.206.12 on Sdwan-system-intf, 01:34:24 ago Routing Descriptor Blocks: * 169.254.206.12
(default), from 169.254.206.12, 01:34:24 ago, via Sdwan-system-intf Route metric is 0, traffic
```

```
share count is 1
```

대상 VPN을 찾으려면 먼저 cE1의 OMP 테이블에서 해당 접두사에 대한 서비스 레이블을 찾아야 합니다.

```
cE1#show sdwan omp routes vpn 30 192.168.12.0/24 Generating output, this might take time, please
wait ... Code: C -> chosen I -> installed Red -> redistributed Rej -> rejected L -> looped R ->
resolved S -> stale Ext -> extranet Inv -> invalid Stg -> staged IA -> On-demand inactive U ->
TLOC unresolved PATH ATTRIBUTE FROM PEER ID LABEL STATUS TYPE TLOC IP COLOR ENCAP PREFERENCE ---
-------------------------------------------------------------------------------------------
-------- 169.254.206.4 12 1007 C,I,R installed 169.254.206.12 private2 ipsec -
```

레이블 값이 1007임을 확인할 수 있습니다. 마지막으로, 시스템-IP 169.254.206.12을 보유한 라우터에서 시작되는 모든 서비스가 vSmart 컨트롤러에서 선택된 경우 대상 VPN을 찾을 수 있습니다.

```
vsmart1# show omp services family ipv4 service VPN originator 169.254.206.12 C -> chosen I ->
installed Red -> redistributed Rej -> rejected L -> looped R -> resolved S -> stale Ext ->
extranet Inv -> invalid Stg -> staged IA -> On-demand inactive U -> TLOC unresolved PATH VPN
SERVICE ORIGINATOR FROM PEER ID LABEL STATUS ----------------------------------------------------
----------------------- 1 VPN 169.254.206.12 169.254.206.12 82 1003 C,I,R 2 VPN 169.254.206.12
169.254.206.12 82 1004 C,I,R 10 VPN 169.254.206.12 169.254.206.12 82 1006 C,I,R 17 VPN
169.254.206.12 169.254.206.12 82 1005 C,I,R 20 VPN 169.254.206.12 169.254.206.12 82 1007 C,I,R
```

VPN 레이블 1007에 따라 대상 VPN이 20인지 확인할 수 있습니다.

방법 2. 플랫폼 명령의 도움말을 사용하여 대상 VPN을 찾는 방법

플랫폼 명령의 도움말로 대상 VPN을 확인하려면 먼저 **show ip vrf detail 30** 또는 **show platform software ip f0 cef table * summary** 명령의 도움을 받아 cE1 라우터에서 VPN 30에 대한 내부 VRF ID를 받아야 합니다.

```
cE1#show ip vrf detail 30 | i Id VRF 30 (VRF Id = 1); default RD 1:30; default VPNID
```

이 경우 VRF ID 1은 30이라는 VRF에 할당되었습니다. platform 명령은 SD-WAN 소프트웨어에서 Cisco IOS-XE 소프트웨어에서 패킷 경로를 결정하는 내부 포워딩 논리를 나타내는 OCE(Output Chain Element) 개체 체인을 표시합니다.

```
cE1#show platform software ip F0 cef table index 1 prefix 192.168.12.0/24 oce === Prefix OCE ===
Prefix/Len: 192.168.12.0/24 Next Obj Type: OBJ_SDWAN_NH_SLA_CLASS Next Obj Handle: 0xf800045f,
urpf: 0 Prefix Flags: unknown aom id: 1717, HW handle: 0x561b60eeba20 (created)
```

관심 접두사는 ID가 0xf800045f인 OBJ_SDWAN_NH_SLA_CLASS(Service Level Agreement)의 next-hop object를 가리키며, 이 클래스 유형은 다음과 같습니다.

```
cE1#show platform software sdwan F0 next-hop sla id 0xf800045f SDWAN Nexthop OCE SLA: num_class
16, client_handle 0x561b610c3f10, ppe addr 0xdbce6c10 SLA_0: num_nhops 1, Fallback_sla_flag
TDL_FALSE, nhobj_type SDWAN_NH_INDIRECT ECMP: 0xf800044f 0xf800044f 0xf800044f 0xf800044f
0xf800044f 0xf800044f 0xf800044f 0xf800044f 0xf800044f 0xf800044f 0xf800044f 0xf800044f
0xf800044f 0xf800044f 0xf800044f 0xf800044f SLA_1: num_nhops 0, Fallback_sla_flag TDL_FALSE,
nhobj_type ADJ_DROP ECMP: 0xf800000f 0xf800000f 0xf800000f 0xf800000f 0xf800000f 0xf800000f
0xf800000f 0xf800000f 0xf800000f 0xf800000f 0xf800000f 0xf800000f 0xf800000f 0xf800000f
0xf800000f 0xf800000f
```

이것은 긴 출력이므로 폴백 SLA 클래스가 구성되지 않아 2에서 15까지의 SLA 클래스를 건너뛰었습니다. 모두 SLA 1과 동일한 특수 DROP 인접성을 가리킵니다. 주된 관심사는 SLA 0의 간접 유형(SDWAN_NH_INDIRECT)의 next-hop 객체입니다. ECMP가 없고 모든 ID가 동일하다는 점도 알 수 있습니다(0xf8004f). ...을 클릭합니다. 최종 목적지 VPN 및 서비스 레이블을 찾는 방법을 더 자세히

확인할 수 있습니다.

```
cE1#show platform software sdwan F0 next-hop indirect id 0xf800044f SDWAN Nexthop OCE Indirect:
client_handle 0x561b610f8140, ppe addr 0xd86b4cf0 nhobj_type: SDWAN_NH_LOCAL_SLA_CLASS,
nhobj_handle: 0xf808037f label: 1007, vpn: 20, sys-ip: 169.254.206.12, vrf_id: 1, sla_class: 1
```

방법 3. 패킷 추적 도구의 도움을 받아 대상 VPN을 찾는 방법

대상 VPN을 찾는 또 다른 방법은 실시간 라우터를 통해 실행되는 실제 패킷을 분석할 수 있는 **패킷 추적** 툴입니다. 디버그 조건은 IP 주소 192.168.12.12과 주고받는 트래픽만 매칭하도록 설정됩니다
.

```
cE1#debug platform condition ipv4 192.168.12.12/32 both cE1#debug platform packet-trace packet
10 Please remember to turn on 'debug platform condition start' for packet-trace to work
cE1#debug platform condition start
```

다음으로, R30에서 **ping**을 통해 트래픽이 시작된 경우 cE1에서 일치하는 패킷을 확인하고 각 패킷 세부 정보를 확인할 수 있습니다. 이 경우, 첫 번째 패킷 번호 0입니다. 가장 중요한 줄은 **<<<<<**기호로 강조 표시됩니다.

```
cE1#show platform packet-trace summary Pkt Input Output State Reason 0 Gi6 Tu3 DROP 52
(FirewallL4Insp) 1 Gi6 Tu3 DROP 52 (FirewallL4Insp) 2 Gi6 Tu3 DROP 52 (FirewallL4Insp) 3 Gi6 Tu3
DROP 52 (FirewallL4Insp) 4 Gi6 Tu3 DROP 52 (FirewallL4Insp) 5 Gi6 Tu3 DROP 52 (FirewallL4Insp)
cE1#show platform packet-trace packet 0 Packet: 0 CBUG ID: 0 Summary Input : GigabitEthernet6
Output : Tunnel3 State : DROP 52 (FirewallL4Insp) <<<<<<<<<<<<<<<<<<<<<<<< Timestamp Start :
161062920614751 ns (03/24/2022 16:19:31.754050 UTC) Stop : 161062920679374 ns (03/24/2022
16:19:31.754114 UTC) Path Trace Feature: IPV4(Input) Input : GigabitEthernet6 Output :
```

packet-trace는 ping을 통해 전송되는 다섯 개의 ICMP 에코 패킷이 모두 삭제 코드 52(FirewallL4Insp)와 함께 삭제되었음을 나타냅니다. 섹션 **기능: SDWAN 포워딩**은 대상 VPN이 20이고 터널링된 패킷의 내부 헤더에 있는 서비스 레이블 1007이 cE2에서 목적지 VPN을 지정하기 위해 전달되도록 합니다. 섹션 **기능: ZBFW**는 영역 쌍이 Input VPN 20에서 VPN 30 영역으로 향하는 트래픽에 대해 구성되지 않았으므로 패킷이 삭제되었음을 추가로 확인합니다.

장애 조치로 인한 잠재적 문제

경로 192.168.12.0/24이 R20에 의해 철회되거나 VRF 20의 cE2에서 더 이상 연결할 수 없는 경우 어떻게 됩니까? VRF 30의 관점에서 보면 서브넷은 동일하지만, ZBFW 보안 정책은 VPN 30 영역에서 VPN 20 및 10 영역으로 트래픽을 다르게 처리하기 때문에 트래픽이 허용되는 것과 같은 원치 않는 결과를 초래할 수 있지만, 트래픽은 허용되거나 그 반대의 경우도 마찬가지입니다.

예를 들어 cE2와 R20 라우터 간의 링크 장애를 시뮬레이션하는 경우 이를 통해 vSmart 컨트롤러의 VPN 20 라우팅 테이블에서 192.168.12.0/24 경로 철수가 이루어지며 대신 VPN 10 경로가 VPN 30 라우팅 테이블로 유출됩니다. cE1에 적용된 보안 정책에 따라 VPN 30에서 VPN 10으로의 연결이 허용됩니다(보안 정책의 관점에서 예상되지만 두 VPN에 모두 표시되는 특정 서브넷에는 바람직하지 않음).

```
cE1#show platform packet-trace packet 0 Packet: 0 CBUG ID: 644 Summary Input : GigabitEthernet6
Output : GigabitEthernet3 State : FWD Timestamp Start : 160658983624344 ns (03/24/2022
16:12:47.817059 UTC) Stop : 160658983677282 ns (03/24/2022 16:12:47.817112 UTC) Path Trace
Feature: IPV4(Input) Input : GigabitEthernet6 Output :
```

1006 레이블이 1007 대신 사용되었으며 출력 VPN ID는 현재 20이 아닌 10입니다. 또한 ZBFW 보안 정책에 따라 패킷이 허용되었으며 해당 zone-pair, class-map 및 policy 이름이 지정되었습니다.

가장 빠른 경로가 VPN 30의 라우팅 테이블에 보관되고 이 경우 초기 제어 정책 애플리케이션 VPN 20 경로가 vSmart의 VPN 30 OMP 테이블에 유출된 후 VPN 10 경로가 VPN 10 라우트이기 때문에 더 큰 문제가 발생할 수 있습니다. 이 문서에서 설명한 ZBFW 보안 정책 로직과 정확히 반대의 개념이었던 시나리오를 상상해 보십시오. 예를 들어, VPN 30에서 VPN 20으로 이동하는 트래픽을 허용하고 VPN 10으로 이동하는 것을 목표로 했습니다. 초기 정책 구성 이후에 허용되었던 경우, 장애 또는 VPN 20에서 192.168.12.0/24 경로 철회 후 192.168.12.0/24 서브넷으로 트래픽이 차단된 상태로 남아 있습니다. 192.168.12.0/24 경로는 여전히 VPN 10에서 유출되기 때문입니다.