Configuratie van SD-WAN Zone-Based Firewall (ZBFW) en routeslekken

Inhoud

Inleiding

Dit document beschrijft hoe u zone-gebaseerde firewall (ZBFW) kunt configureren, controleren en problemen oplossen met routeblokkering tussen Virtual Private Networks (VPN's).

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco SD-WAN overlay maakt een eerste configuratie
- ZBFW-configuratie van vManager User Interface (UI)
- Routerblokkering beleidsconfiguratie van vManager UI-beheer

Gebruikte componenten

Voor de demonstratie werden deze software gebruikt:

- Cisco SD-WAN vSmart-controller met 20.6.2 softwarerelease
- Cisco SD-WAN v Manager controller met 20.6.2 softwarerelease
- Twee Cisco IOS®-XE Catalyst 8000V virtuele-scherpste platformrouters met 17.6.2

softwarerelease die in de controller-modus werken
- Drie Cisco IOS-XE Catalyst 8000V virtuele-scherpste routers met 17.6.2 softwarerelease die in autonome modus werken

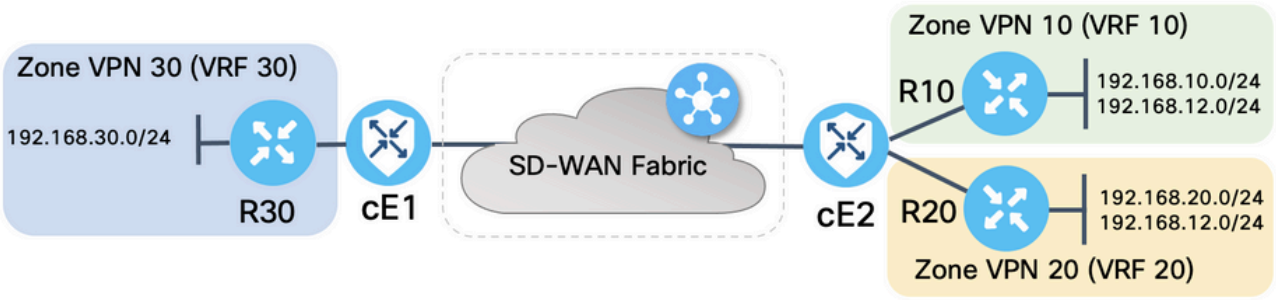
De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk levend is, zorg er dan voor dat u de mogelijke impact van om het even welke opdracht begrijpt.

Achtergrondinformatie

Dit document legt uit hoe de router de bestemming VPN-omzetting in SD-WAN overlay bepaalt en hoe u de route voor het lekken van VPN's kunt controleren en oplossen. Het beschrijft ook de eigenaardigheden van pad selectie in het geval dat hetzelfde net vanaf een ander VPN wordt geadverteerd en welk soort problemen hierdoor kunnen ontstaan.

Configureren

Netwerkdiagram



Beide SD-WAN routers waren geconfigureerd met fundamentele parameters om bedieningsverbindingen tot stand te brengen met SD-WAN controllers en datalevaste verbindingen tussen deze controllers. Details van deze configuratie zijn in het kader van dit document niet toegestaan. De tabel hier vat de opdrachten VPN, Site ID en Zones samen.

	cE1	cE2
Site-ID	11	12
VPN	30	10,20
System-IP	169.254.206.11	169.254.206.12

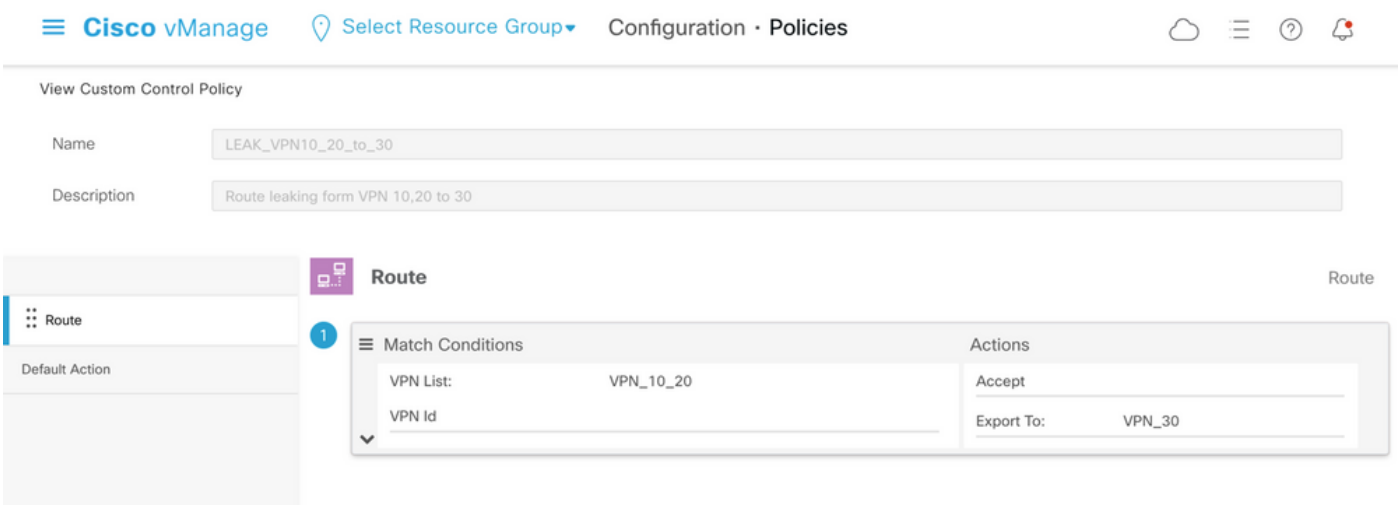
De routers aan de servicekant werden geconfigureerd met statische standaardroutes in elke Virtual Routing en Forwarding (VRF), die wijzen naar de SD-WAN router die overeenkomt. Op dezelfde manier werden SD-WAN Edge routers geconfigureerd met statische routes die wijzen naar de bijbehorende subnetten. Merk op dat, voor de demonstratie van de mogelijke problemen met route-lekken en ZBFW, routers achter de serviceskant van cE2 hetzelfde subtype 192.168.12.0/24 hebben. Op beide routers achter cE2 is er een Loopback-interface die is geconfigureerd om een host te evenaren met hetzelfde IP-adres 192.168.12.12.

Het is belangrijk om op te merken dat de Cisco IOS-XE routers R10, R20 en R30 in autonome modus op de servicekant van SD-WAN Edge-routes lopen die voornamelijk dienen om eindhosts

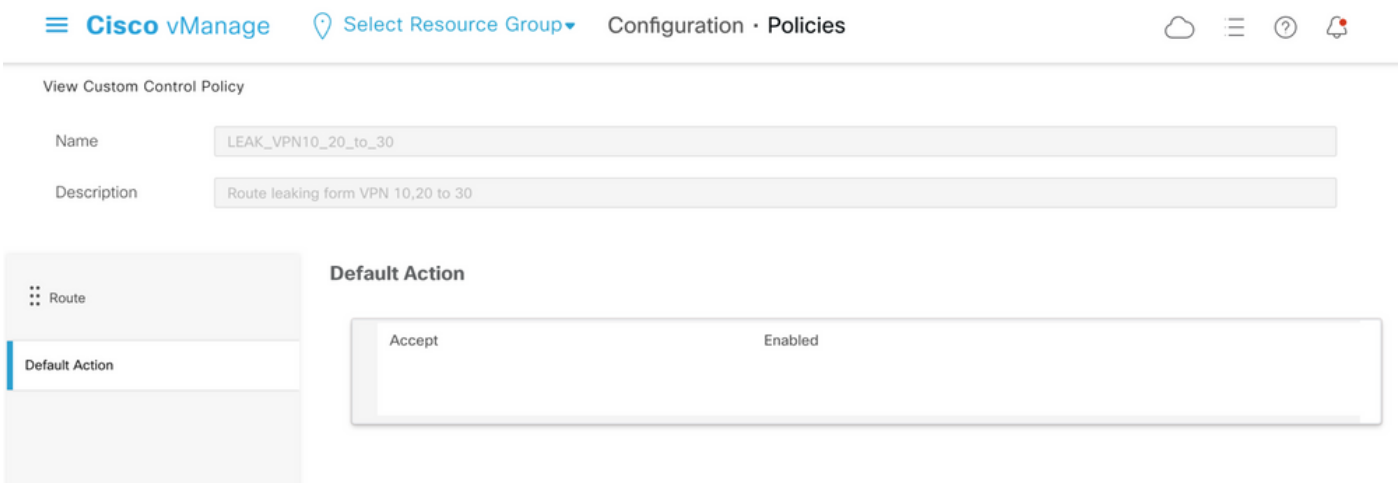
in deze demonstratie te nabootsen. Loopback interfaces op SD-WAN Edge-routes kunnen voor dit doel niet worden gebruikt in plaats van echte hosts zoals routers aan de serviczijde, omdat verkeer dat afkomstig is van een interface in een VRF van SD-WAN Edge-router niet wordt beschouwd als verkeer dat is ontstaan in de ZBFW-zone die correspondeert, en eerder tot de speciale zelfzone van een randrouter behoort. Dat is de reden dat de ZBFW-zone niet als dezelfde VRF kan worden beschouwd. Een gedetailleerde discussie over de eigen zone valt buiten de werkingssfeer van dit artikel.

Configuratie van routeswitches

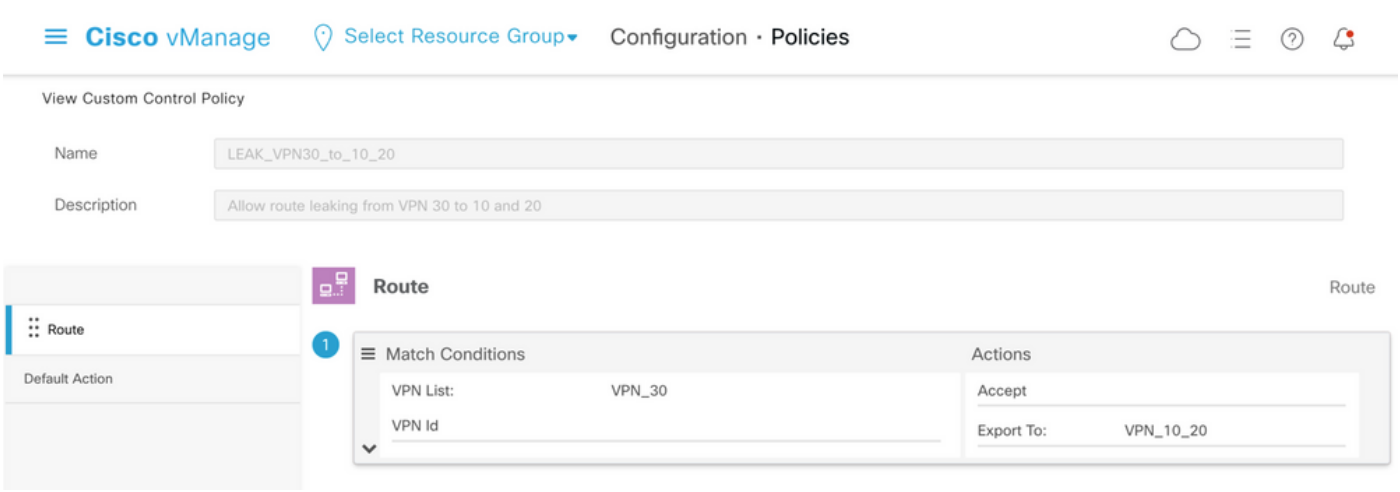
De belangrijkste configuratiedoelstelling van het controlebeleid is om route die van alle routes van VPN 10 en 20 in VPN 30 toe te staan. VRF 30 bestaat slechts op de router cE1 en VRFs 10 en 20 worden gevormd op de router cE2 slechts. Om dit te bereiken, werden twee topologie (Aangepaste Controle) beleid gevormd. Hier is de topologie om alle routes van VPN 10 en 20 in VPN 30 te exporteren.

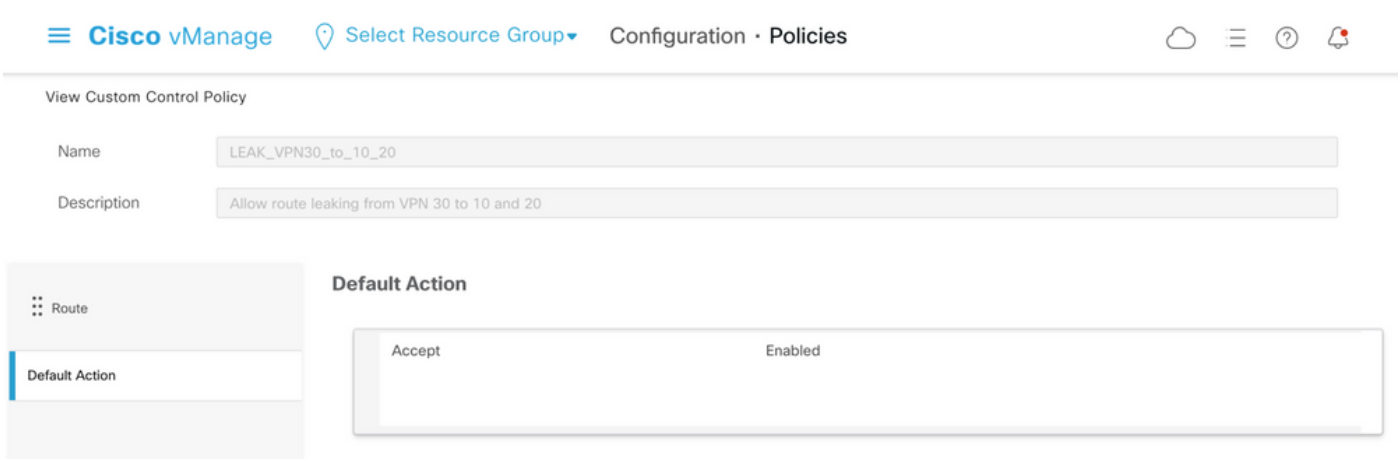


Merk op dat de Default Action is ingesteld op **Sta toe,** om het blokkeren van TLOC-advertenties of normale intra-VPN-routeadvertenties per ongeluk te voorkomen.

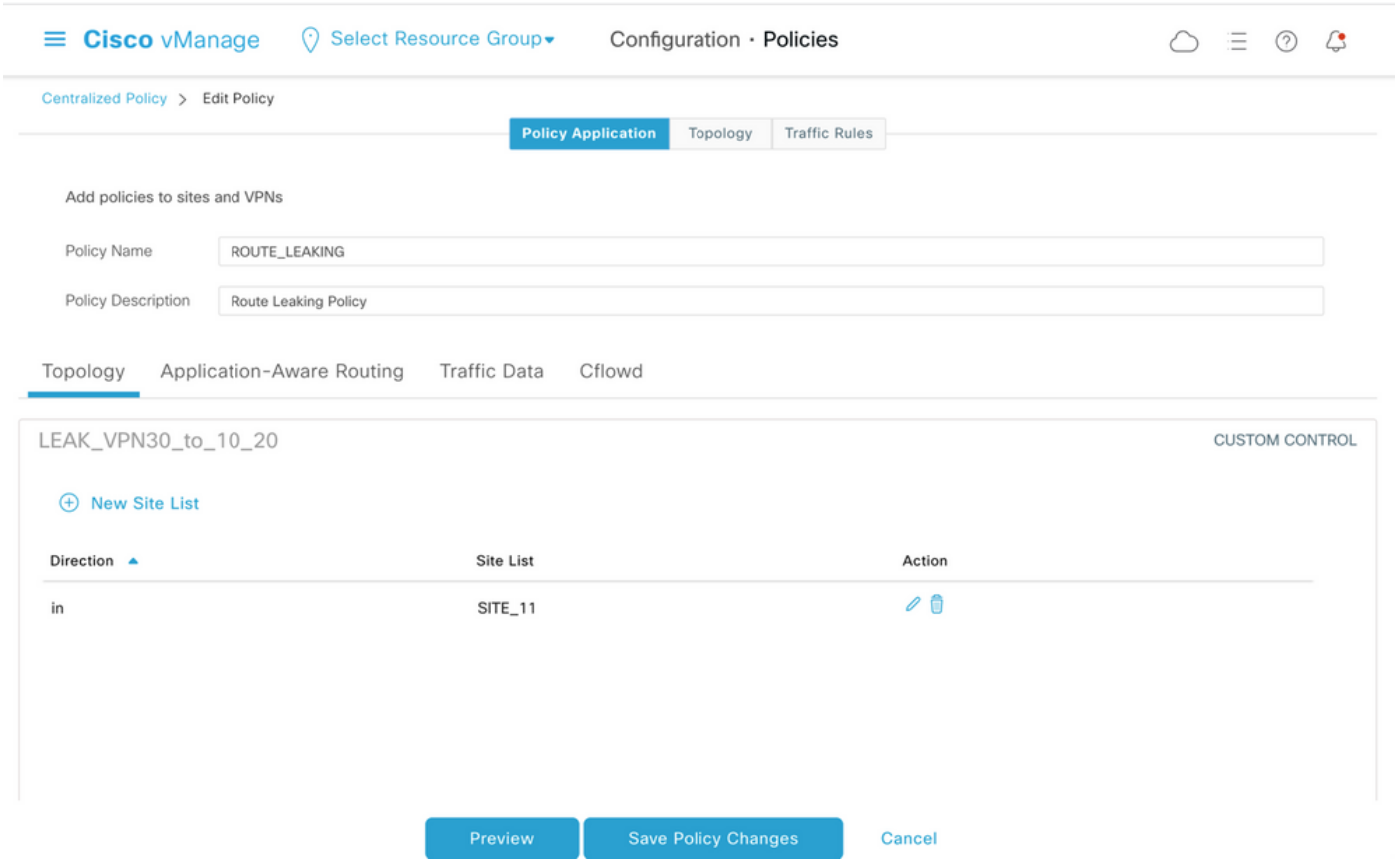


Op dezelfde manier werd het topologiebeleid geconfigureerd om omgekeerde advertenties toe te staan voor het verzenden van informatie van VPN 30 naar VPN 10 en 20.

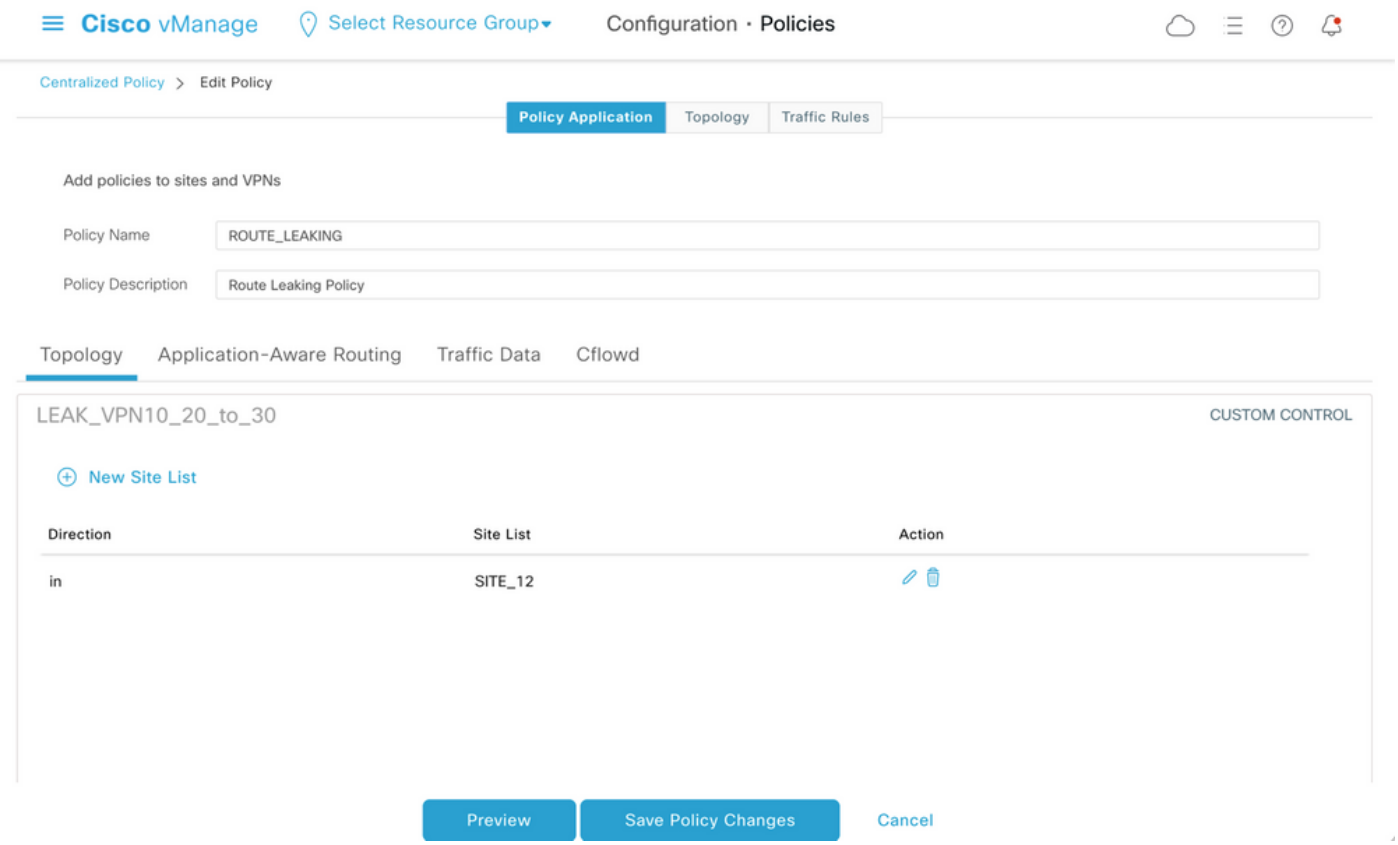




Vervolgens wordt beide topologiebeleid toegewezen aan de site lijstjes die corresponderen, in de ingress (inkomende) richting. Routes van VPN 30 worden door de vSmart-controller geëxporteerd naar OMP-tabellen (Overlay Management Protocol) van VPN 10 en 20 wanneer ontvangen van cE1 (site-id 11).



Op dezelfde manier worden de routes van VPN 10 en 20 door vSmart geëxporteerd naar VPN 30 routingtabel na ontvangst van VPN 10 en 20 routes van cE2 (site-id 12).



Hier is ook een compleet voorbeeld van de configuratie van het controlebeleid ter referentie.

```
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 ! !
```

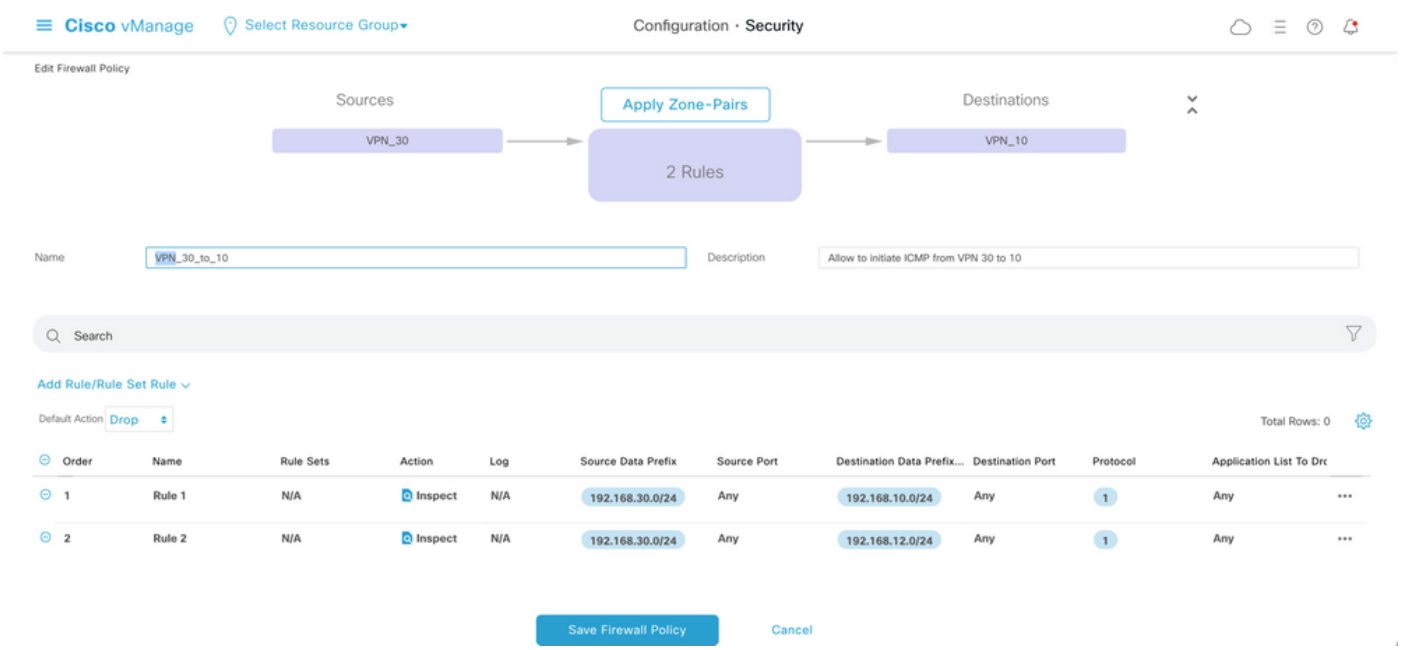
Het beleid moet worden geactiveerd vanuit het gedeelte **Configuratie** vManager **> Beleid** om effectief te zijn op de vSmart-controller.

ZBFW-configuratie

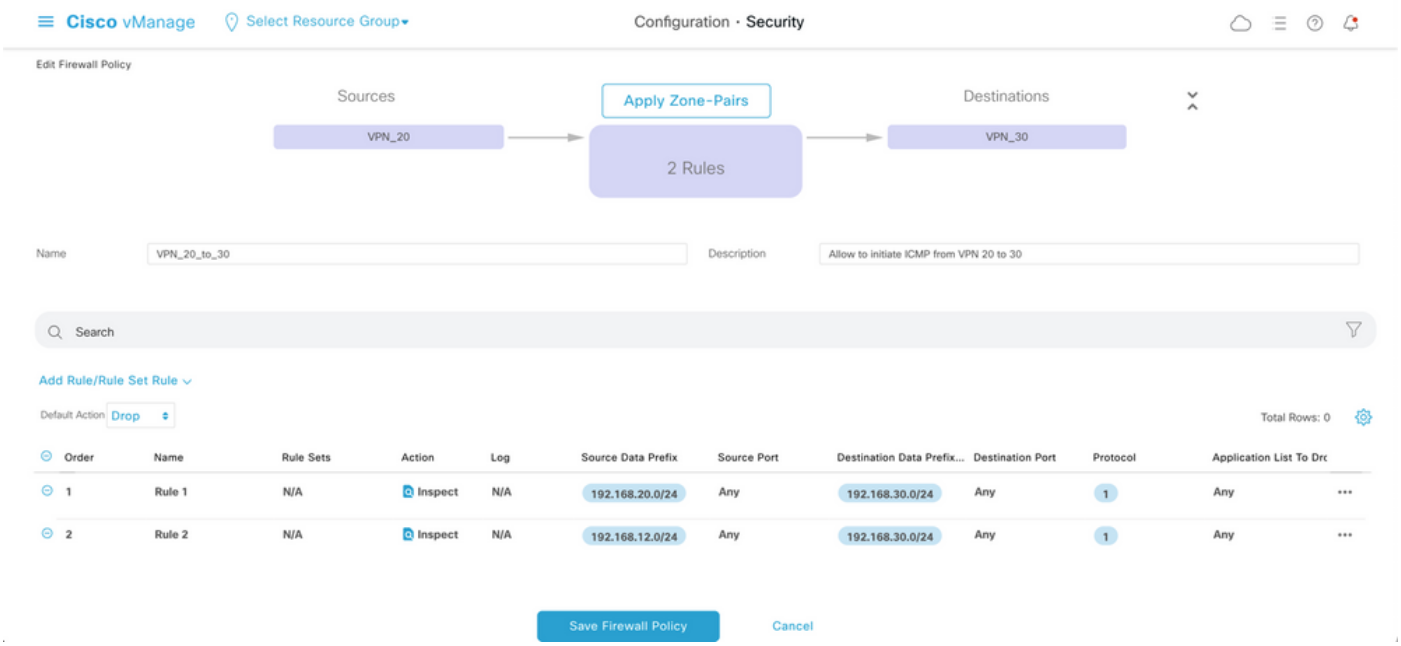
Hier is een tabel die ZBFW samenvat om de vereisten voor demonstratie in dit artikel te filteren.

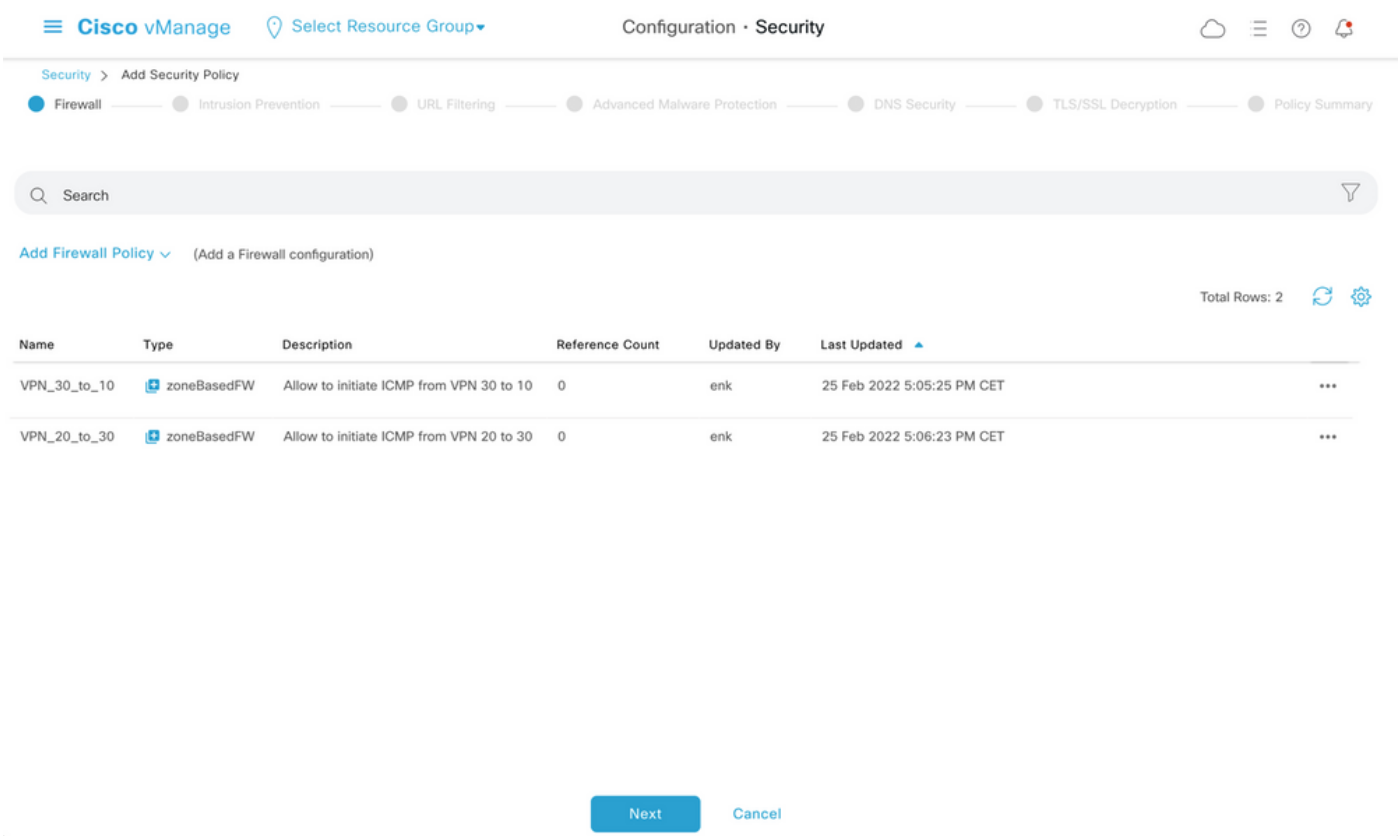
Doelzone bronzone	VPN_10	VPN_20	VPN_30
VPN_10	binnen de zone	ontkennen	ontkennen
VPN_20	ontkennen	binnen de zone	toestaan
VPN_30	toestaan	ontkennen	binnen de zone

Het belangrijkste doel is om elk verkeer van het Internet Control Message Protocol (ICMP) toe te staan dat van de servicetzij van router cE1 VPN 30 is afkomstig en bestemd is voor VPN 10 maar niet voor VPN 20. Het retourverkeer moet automatisch worden toegestaan.



Ook moet elk ICMP-verkeer van de router cE2 service-side VPN 20 toegestaan zijn om naar VPN 30 servicekant van cE1 te gaan, maar niet van VPN 10. Terugkeren van VPN 30 naar VPN 20 moet automatisch toegestaan zijn.

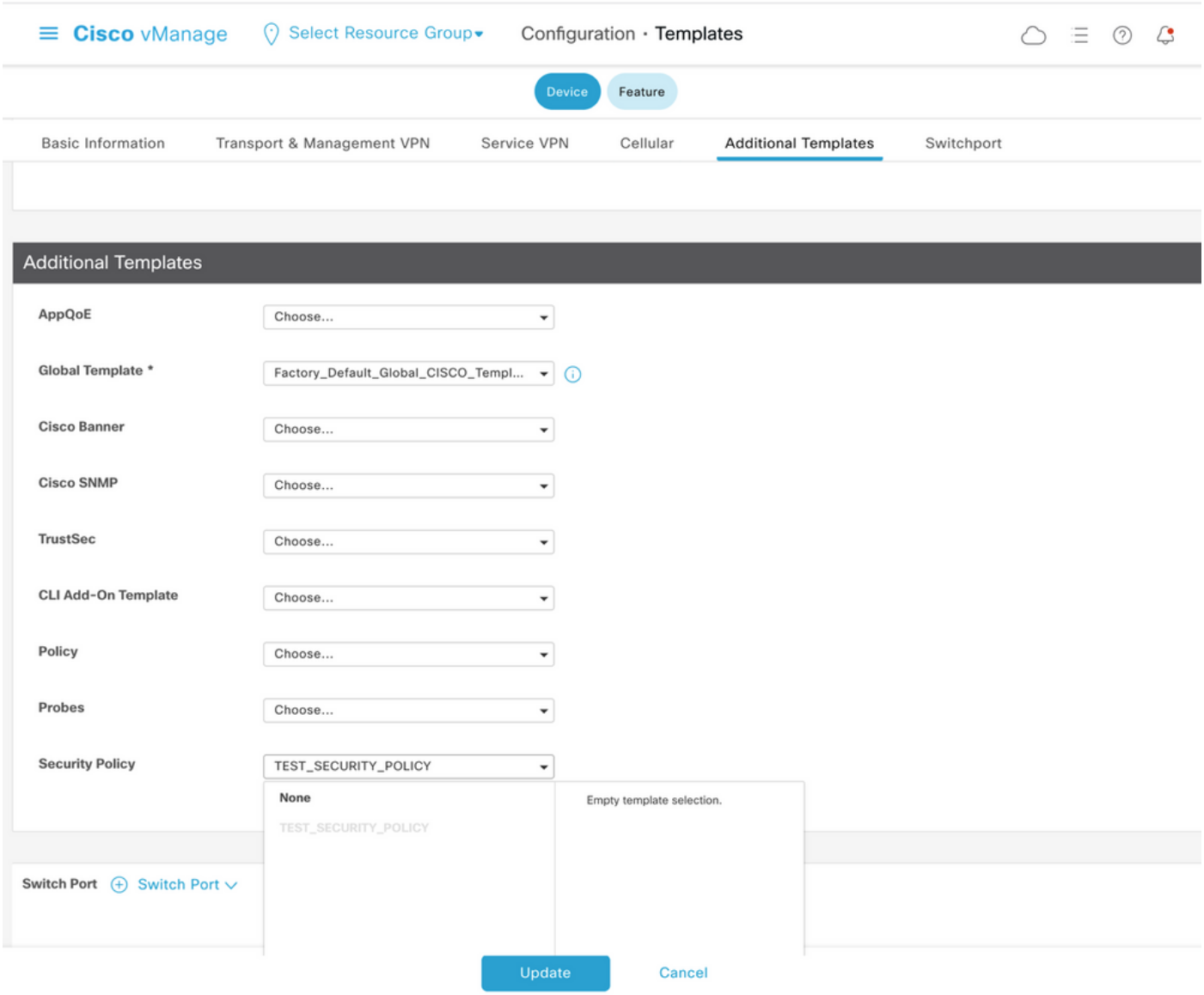




Hier vindt u het ZBFW-beleidsvoorbeeld ter referentie.

```
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 !
```

Om veiligheidsbeleid toe te passen, moet het onder het vervolgkeuzemenu van het **Veiligheidsbeleid** van de **Extra** gedeelte van de apparatentemplate worden toegewezen.



Zodra de apparaatsjabloon is bijgewerkt, wordt het beveiligingsbeleid actief op het apparaat waar het beveiligingsbeleid is toegepast. Voor de demonstratie in dit document was het genoeg om het veiligheidsbeleid op de cE1 router toe te staan.

Verifiëren

U moet nu controleren of de ZBFW-doelstellingen (het vereiste beveiligingsbeleid) zijn bereikt.

Test met **ping** bevestigt dat het verkeer van zone VPN 10 naar VPN 30 wordt ontkend zoals verwacht omdat er geen zone-paar is ingesteld voor verkeer van VPN 10 naar VPN 30.

```
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)
```

Op dezelfde manier is verkeer van VPN 20 naar VPN 30 toegestaan zoals verwacht door de configuratie van het beveiligingsbeleid.

```
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
```

Verkeer van VPN 30 tot 192.168.10.0/24 in zone VPN 10 is toegestaan zoals verwacht door beleidsconfiguratie.

```
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
```

Het verkeer van VPN 30 tot Subnet 192.168.20.0/24 in zone VPN 20 wordt ontkend omdat er geen zone paar is ingesteld voor dit verkeer dat verwacht wordt.

```
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)
```

Aanvullende resultaten die u kunnen interesseren kunnen worden waargenomen wanneer u probeert het IP-adres 192.168.12.12 te pingelen omdat dit in zone VPN 10 of VPN 20 kan zijn, en het is onmogelijk om de bestemming VPN te bepalen vanuit het perspectief van de router R30 op de servicekant van SD-WAN Edge-router cE1.

```
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)
```

Het resultaat is hetzelfde voor alle bronnen in VRF 30. Dit bevestigt dat het niet afhangt van de resultaten van de opslagfunctie van Gelijk pad (ECMP):

```
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)
```

Gebaseerd op testresultaten voor de bestemming IP 192.168.12.12, kunt u alleen maar raden dat deze zich in VPN 20 vestigt omdat deze niet reageert op de echo-verzoeken van ICMP en is waarschijnlijk geblokkeerd omdat er geen zone-paar is ingesteld om verkeer van VPN 30 naar VPN 20 toe te staan (zoals gewenst). Als een bestemming met hetzelfde IP-adres 192.168.12.12 in VPN 10 zou staan en naar verwachting op een ICMP-echo-verzoek zal reageren, dan moet volgens het ZBFW-beveiligingsbeleid voor ICMP-verkeer van VPN 30 naar VPN 20, verkeer worden toegestaan. U moet de bestemming VPN bevestigen.

Problemen oplossen

Methode 1. Om lot VPN te vinden uit OMP-tabel

Een simpele controle van de routeringstabel op cE1 helpt niet om de echte bestemming VPN te begrijpen. De meest nuttige informatie die je kunt krijgen van de output is een systeem-IP van de bestemming (169.254.206.12) en ook dat er geen ECMP is dat gebeurt.

```
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
```

Wilt u te weten komen wat de bestemming VPN is, dan moet u eerst het servicetabel uit de OMP-tabel op cE1 zoeken voor de kengetal van belang.

```
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 -
```

We kunnen zien dat de waarde van het etiket 1007 is. Ten slotte kan er VPN op de bestemming worden gevonden als alle services die afkomstig zijn van de router die het systeem-IP 169.254.206.12 heeft, zijn gecontroleerd op de vSmart-controller.

```
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
```

Op basis van VPN-label 1007 kan worden bevestigd dat de bestemming VPN 20 is.

Methode 2. Om lot VPN te vinden met Help van platform opdrachten

Om te weten te komen wat de bestemming VPN is met hulp van platformopdrachten, moet u eerst een interne VRF-id verkrijgen voor VPN 30 op de cE1-router met behulp van **ip vrf-details 30** of **platformsoftware ip f0 cef tabel * summiere** opdrachten tonen.

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

In dit geval werd VRF ID 1 toegewezen aan VRF met de naam 30. Opdrachten van het platform onthullen de keten van het element van de keten (OCE) van voorwerpen in SD-WAN software die de interne verzendlogica vertegenwoordigen die pakketpad in Cisco IOS-XE software bepaalt:

```
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)
```

Het voorvoegsel van interesses van het klasse type van het volgende-hopobject van Service Level Agreement (SLA) (OBJ_SDWAN_NH_SLA_CLASS) met ID 0xf80045f die nader kan worden geverifieerd, wordt hier weergegeven:

```
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
```

Dit is een lange productie, dus werden SLA-klassen van 2 tot 15 overgeslagen omdat er geen back-up SLA-klassen zijn geconfigureerd, en al deze punten wijzen op dezelfde speciale DROP-nabijheid als SLA 1. Het belangrijkste belang is het volgende-hopobject van indirect type (SDWAN_NH_INDIRECT) van SLA 0. We kunnen ook opmerken dat er geen ECMP is en alle ID's hetzelfde zijn (0xf) 800044f). Er kan verder worden geverifieerd of de uiteindelijke bestemming VPN- en servicelabel is gevonden.

```
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
```

Methode 3. Om lot VPN te vinden met Help van Packet-Trace Tool

Een andere manier om een bestemming VPN te vinden is een **pakket-spoor** gereedschap dat echte pakketten kan analyseren die door de router in real-time kunnen worden uitgevoerd. Debug is ingesteld om alleen verkeer aan/van het IP-adres 192.168.12.12 aan te passen.

```
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
```

Als het verkeer vervolgens vanaf R30 is gestart **met** behulp van **ping**, kunt u aangepaste pakketten op cE1 zien en elk pakketdetail controleren. In dit geval is het bijvoorbeeld het allereerste pakketnummer 0. De belangrijkste lijnen worden gemarkeerd met **<<<<<** tekens.

```
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 :
```

Een **pakketspoor** vertelt dat alle vijf ICMP echo-pakketten die door **ping** werden verzonden, met drop-code 52 (FirewallL4Insp) werden gedropt. **Functie** sectie**: SDWAN Forwarding** vertelt dat de bestemming VPN 20 is en Service-label 1007 in de interne header van het getunnelde pakket wordt gebruikt om bestemming VPN aan te wijzen op cE2. Sectie **Functie: ZBFW** bevestigt verder dat pakketten werden gevallen omdat het zone-paar niet was ingesteld voor verkeer van Input VPN 20 dat bestemd was voor VPN 30-zone.

Potentiële problemen door failover

Wat gebeurt er als route 192.168.12.0/24 wordt ingetrokken door R20 of niet meer bereikbaar is vanaf cE2 in VRF 20? Hoewel vanuit het perspectief van VRF 30 is het subnetwerk het zelfde, omdat het ZBFW veiligheidsbeleid verkeer van zone VPN 30 tot zones VPN 20 en 10 verschillend behandelt kan het tot ongewenste resultaten zoals verkeer toegelaten leiden, terwijl het niet moet zijn of omgekeerd.

Bijvoorbeeld, als u een mislukking van een verbinding tussen cE2 en R20 routers simuleert. Dit leidt tot 192.168.12.0/24 routeintrekking van VPN 20 routingtabel op vSmart controller en in plaats daarvan wordt VPN 10-route uitgelekt naar VPN 30 routingtabel. Connectiviteit van VPN 30 aan VPN 10 is toegestaan volgens het beveiligingsbeleid dat op cE1 wordt toegepast (dit wordt

verwacht vanuit het perspectief van beveiligingsbeleid, maar kan niet wenselijk zijn voor het specifieke subtype dat in beide VPN's wordt aangeboden).

```
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 :
```

Merk op dat etiket 1006 werd gebruikt in plaats van 1007 en dat de uitvoer VPN-id nu 10 is in plaats van 20. Bovendien was het pakket toegestaan volgens het ZBFW-beveiligingsbeleid en zijn er bijbehorende zone-paar, class-map- en beleidsnamen gegeven.

Er is een zelfs nog groter probleem dat kan ontstaan door het feit dat de vroegste route in de routingtabel van VPN 30 wordt gehouden en in dit geval is het de VPN 10 route die na de aanvankelijke toepassing van het controlebeleid VPN 20 route op vSmart in VPN 30 OMP-tabel is uitgelekt. Stel je het scenario voor dat het oorspronkelijke idee precies het tegenovergestelde was van de ZBFW security beleidslogica die in dit artikel wordt beschreven. Bijvoorbeeld, het doel was om verkeer van VPN 30 naar VPN 20 toe te staan en niet naar VPN 10. Als het toegestaan was na een eerste beleidsconfiguratie, dan na de mislukking of 192.168.12.0/24 route terugtrekking van VPN 20, blijft het verkeer geblokkeerd naar 192.168.12.0/24 zelfs na herstel omdat de 192.168.12.0/24 route nog steeds lekt van VPN 10.