Konfigurieren der SD-WAN Zone-Based Firewall (ZBFW) und Route Leaking

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie zonenbasierte Firewall (ZBFW) mit Route Leaking zwischen Virtual Private Networks (VPN) konfiguriert, verifiziert und Fehler bei diesen behoben werden.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Erstkonfiguration durch Cisco SD-WAN-Overlay
- ZBFW-Konfiguration über die vManage-Benutzeroberfläche (UI)
- Konfiguration der Steuerelementrichtlinien über die vManage-Benutzeroberfläche

Verwendete Komponenten

Für die Demonstration wurden folgende Software verwendet:

- Cisco SD-WAN vSmart Controller mit Softwareversion 20.6.2
- Cisco SD-WAN vManage-Controller mit Softwareversion 20.6.2
- Zwei Cisco IOS®-XE Catalyst 8000V Virtual-Edge-Router mit Softwareversion 17.6.2, die im

Controller-Modus ausgeführt werden
- Drei Cisco IOS-XE Catalyst 8000V Virtual-Edge-Router mit Softwareversion 17.6.2, die im Autonomous-Mode ausgeführt werden

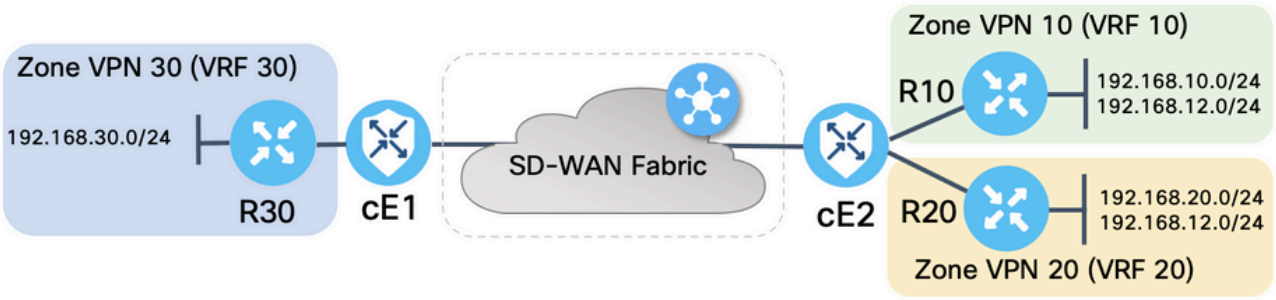
Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Hintergrundinformationen

In diesem Dokument wird erläutert, wie der Router die Ziel-VPN-Zuordnung im SD-WAN-Overlay festlegt und wie das Route Leaking zwischen VPNs überprüft und behoben wird. Außerdem werden die Besonderheiten der Pfadauswahl beschrieben, falls dasselbe Subnetz von einem anderen VPN angekündigt wird und welche Probleme dadurch entstehen können.

Konfigurieren

Netzwerkdiagramm



Beide SD-WAN-Router wurden mit Basisparametern konfiguriert, um Steuerungsverbindungen mit SD-WAN-Controllern und Datenebenenverbindungen zwischen ihnen herzustellen. Details dieser Konfiguration sind für dieses Dokument nicht relevant. In der Tabelle hier sind die Zuweisungen für VPN, Standort-ID und Zonen zusammengefasst.

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

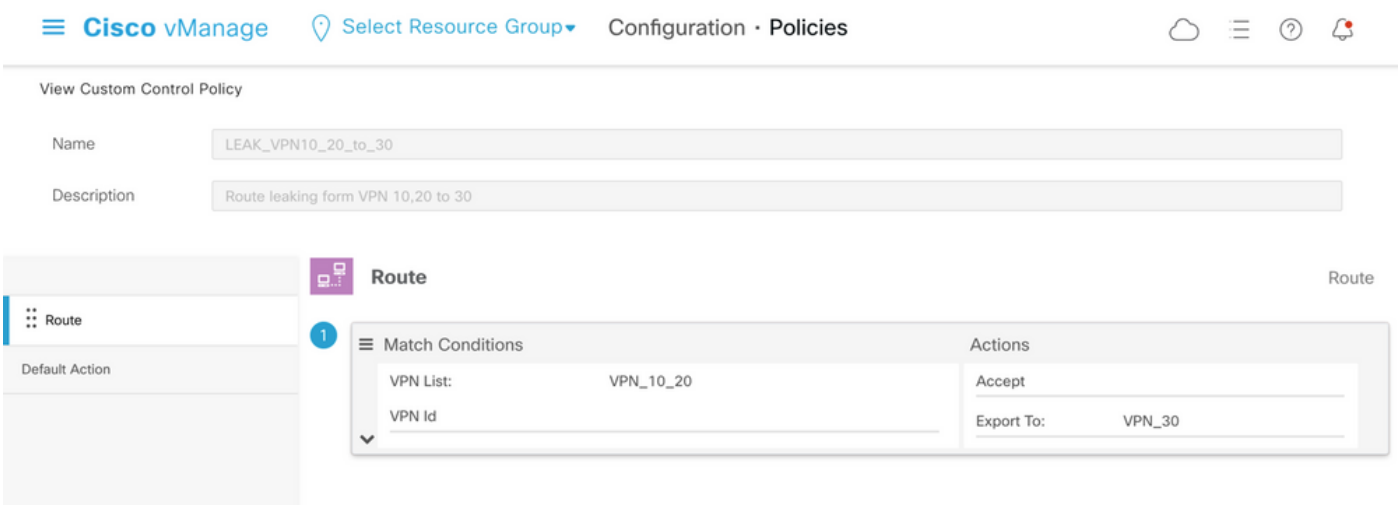
Die Router auf der Service-Seite wurden mit statischen Standardrouten in jeder Virtual Routing and Forwarding (VRF) konfiguriert, die auf den entsprechenden SD-WAN-Router zeigen. Ebenso wurden SD-WAN-Edge-Router mit statischen Routen konfiguriert, die auf die entsprechenden Subnetze zeigen. Beachten Sie, dass für die Demonstration der potenziellen Probleme mit Route Leaking und ZBFW die Router hinter der Service-Seite von cE2 dasselbe Subnetz 192.168.12.0/24 haben. Auf beiden Routern hinter cE2 ist eine Loopback-Schnittstelle konfiguriert, die einen Host mit der gleichen IP-Adresse 192.168.12.12 emuliert.

Es ist zu beachten, dass die Cisco IOS-XE-Router R10, R20 und R30 auf den Dienstseiten der SD-WAN-Edge-Routen im autonomen Modus ausgeführt werden, der hauptsächlich zur Emulation

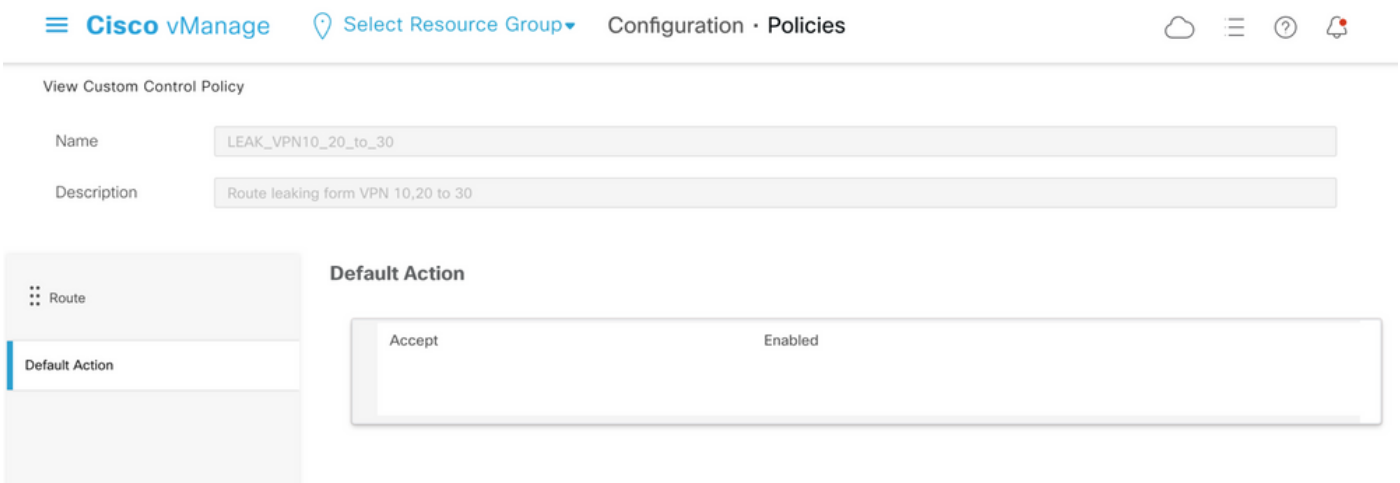
von End-Hosts in dieser Demonstration dient. Zu diesem Zweck können Loopback-Schnittstellen auf SD-WAN-Edge-Routen nicht anstelle von echten Hosts wie Service-Side-Routern verwendet werden, da Datenverkehr, der von einer Schnittstelle in einem VRF des SD-WAN-Edge-Routers stammt, nicht als Datenverkehr gilt, der von der ZBFW-Zone stammt, die der speziellen Kernzone eines Edge-Routers entspricht und eher gehört. Aus diesem Grund kann die ZBFW-Zone nicht mit der VRF-Instanz identisch sein. Eine detaillierte Erörterung der Selbstzone ist nicht Gegenstand dieses Artikels.

Route Leaking-Konfiguration

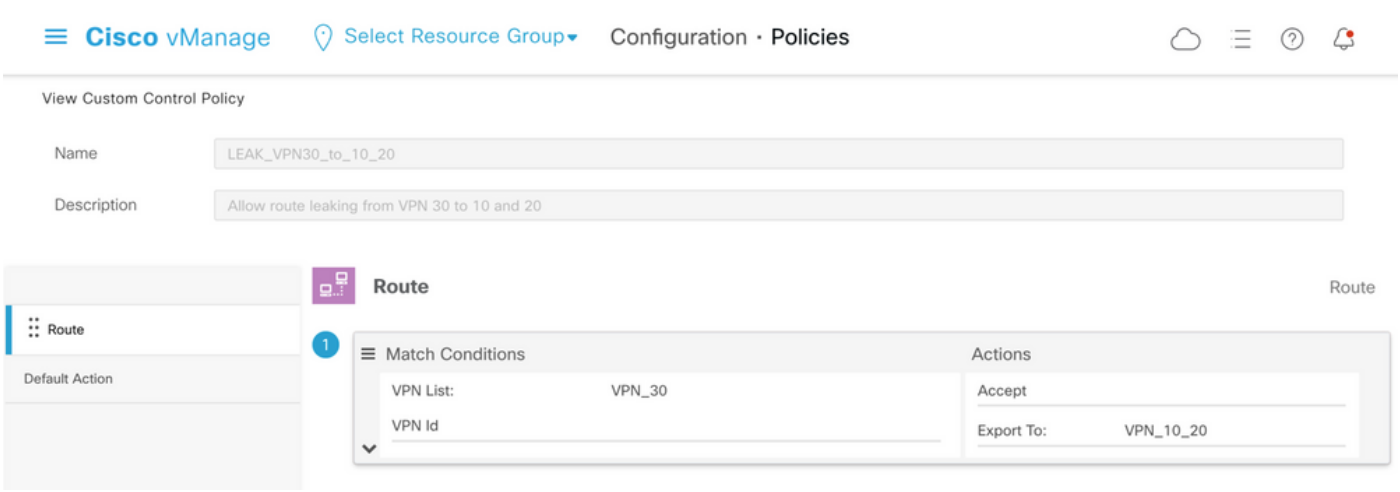
Das Hauptziel der Steuerungsrichtlinienkonfiguration besteht darin, das Route Leaking aller Routen von VPN 10 und 20 in VPN 30 zu ermöglichen. VRF 30 ist nur auf dem Router cE1 vorhanden, und die VRFs 10 und 20 sind nur auf dem Router cE2 konfiguriert. Zu diesem Zweck wurden zwei Topologie-Richtlinien (Custom Control) konfiguriert. Die folgende Topologie dient zum Exportieren aller Routen von VPN 10 und 20 in VPN 30.

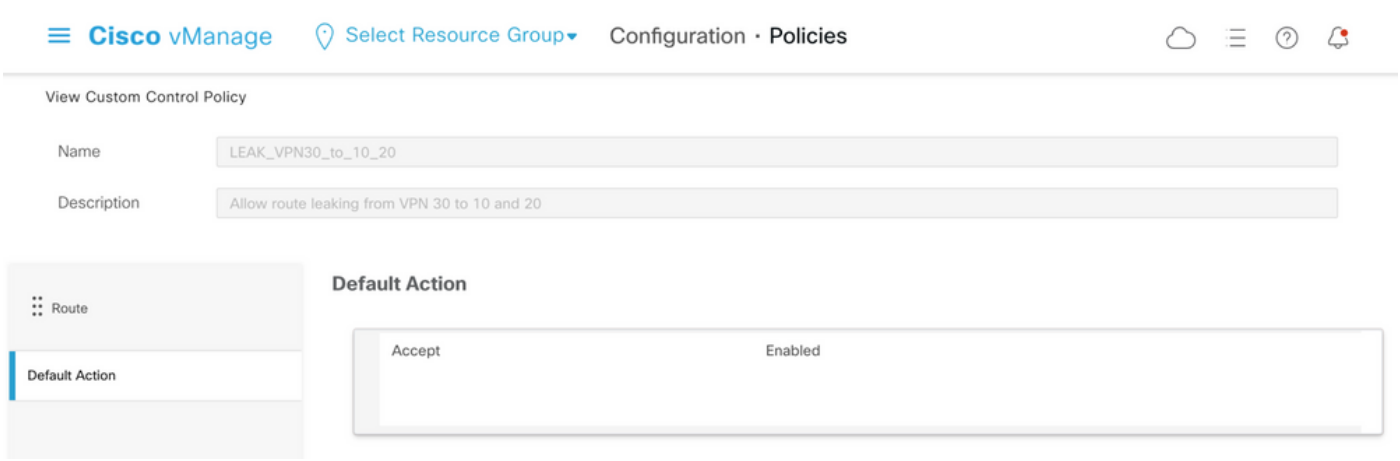


Beachten Sie, dass die Standardaktion auf **Zulassen** gesetzt ist, um den Block von TLOC-Meldungen oder normalen Intra-VPN-Routing-Meldungen versehentlich zu vermeiden.

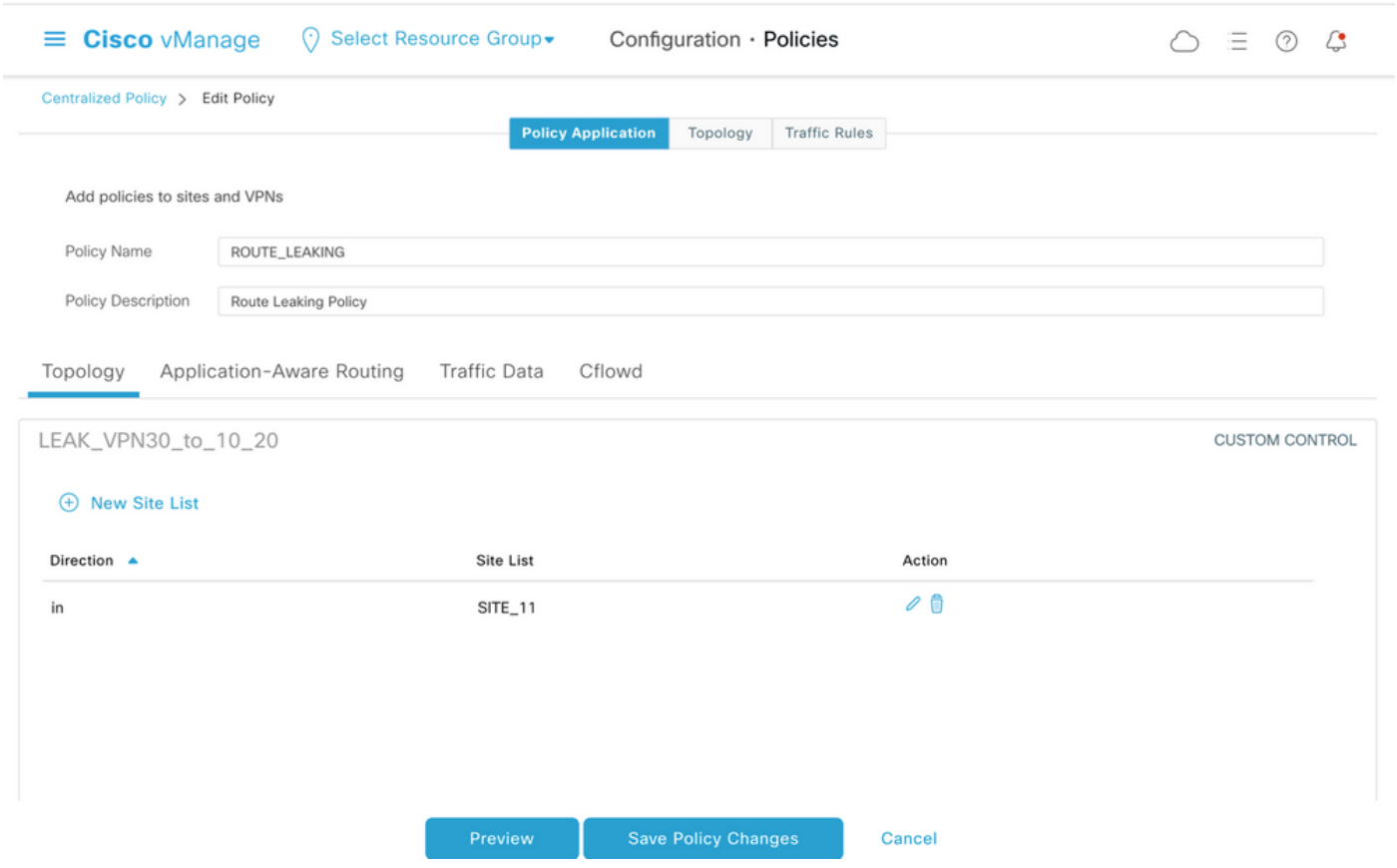


Ebenso wurde die Topologierichtlinie so konfiguriert, dass Routing-Informationen von VPN 30 zu VPN 10 und 20 umgekehrt angekündigt werden können.

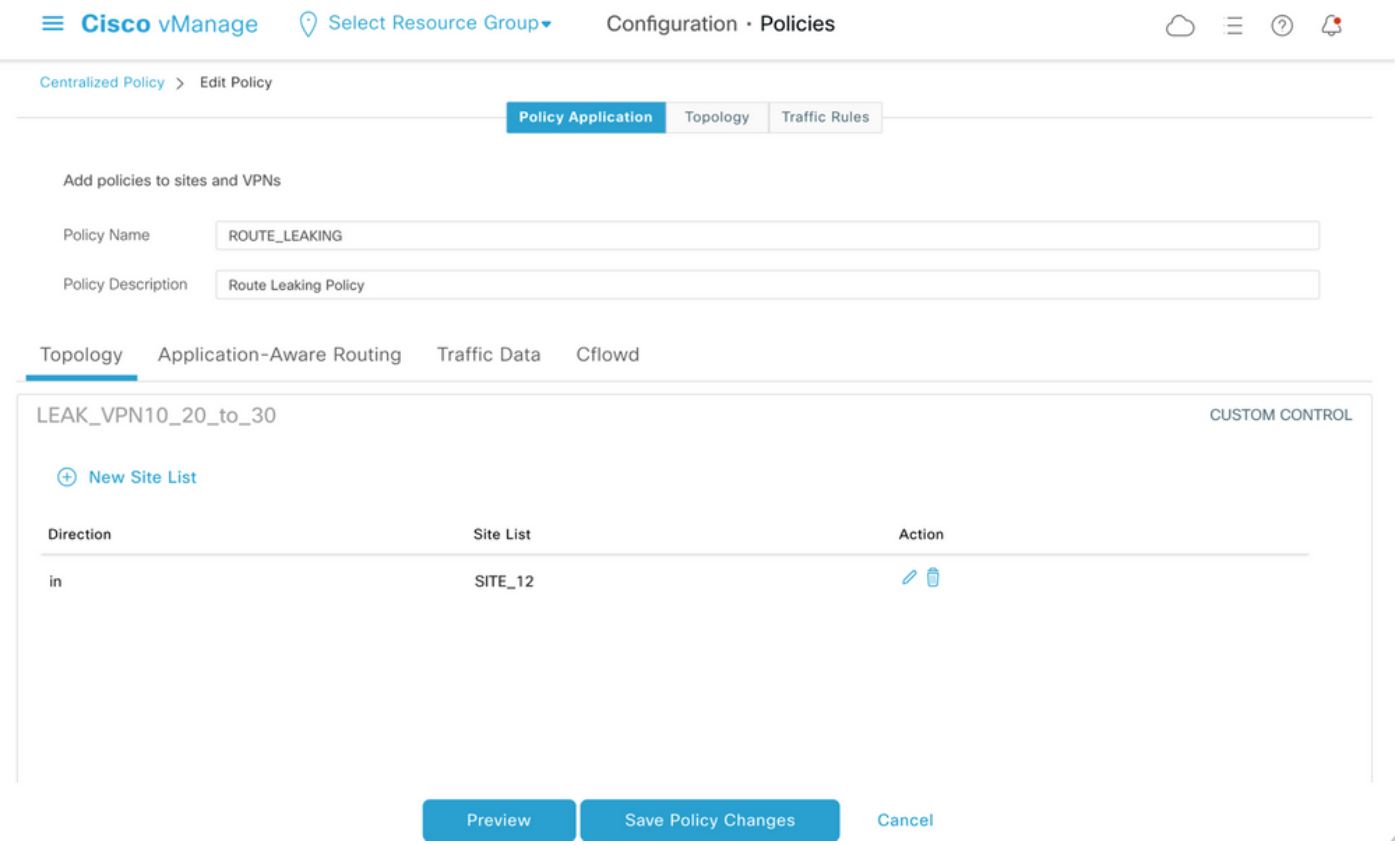




Anschließend werden beide Topologierichtlinien den Sitelisten zugewiesen, die in die Eingangs- (Eingehend-) Richtung entsprechen. Routen von VPN 30 werden vom vSmart Controller in OMP-Tabellen (Overlay Management Protocol) von VPN 10 und 20 exportiert, wenn sie von cE1 empfangen werden (Standort-ID 11).



Ebenso werden Routen von VPN 10 und 20 nach Erhalt von VPN 10- und 20-Routen von cE2 (Standort-ID 12) von vSmart in die VPN 30-Routing-Tabelle exportiert.



Hier finden Sie auch eine vollständige Vorschau der Konfiguration von Kontrollrichtlinien als Referenz.

```
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 ! !
```

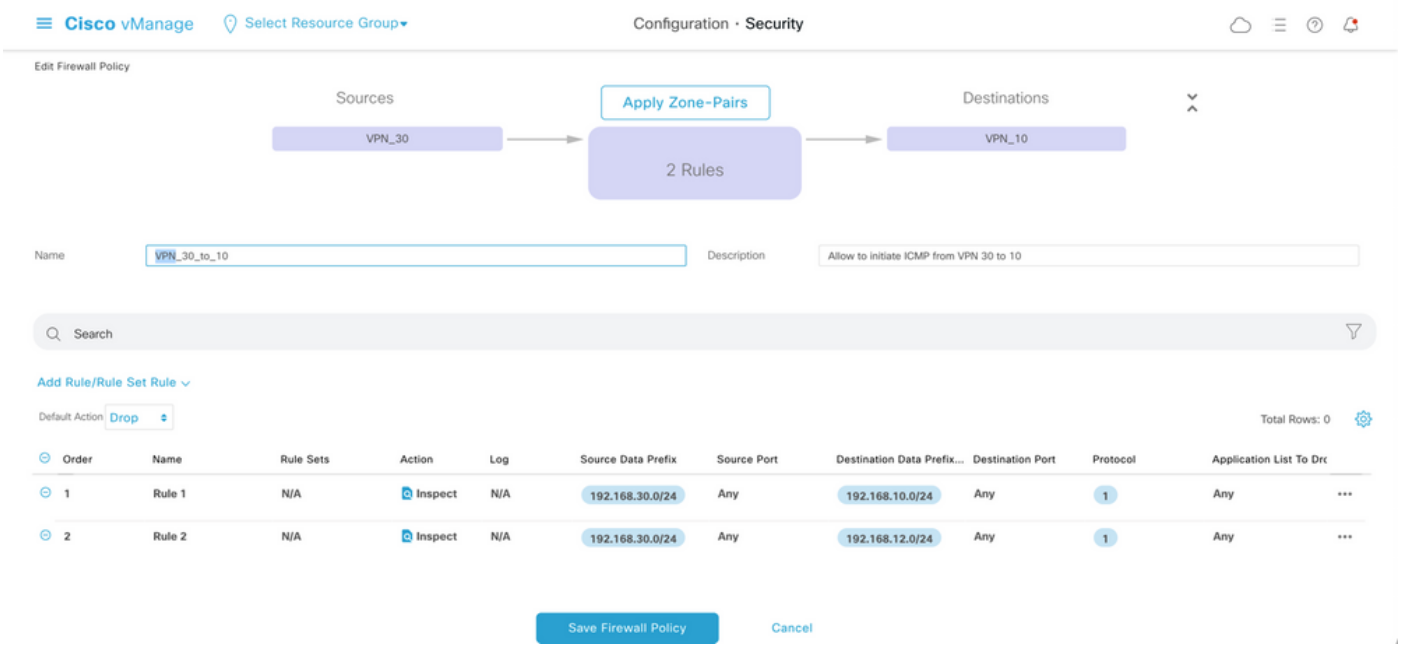
Die Richtlinie muss über den Abschnitt **Konfiguration > Richtlinien** des vManage-Controllers aktiviert werden, um für den vSmart-Controller wirksam zu sein.

ZBFW-Konfiguration

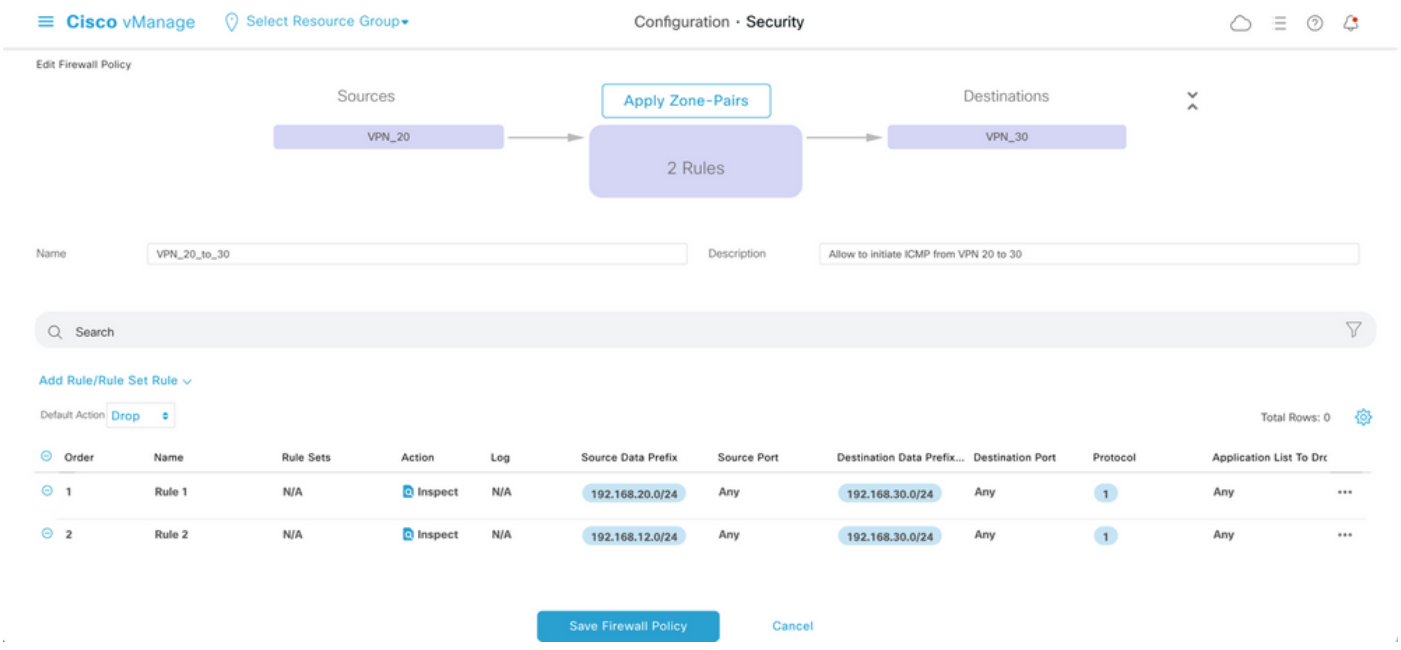
Hier ist eine Tabelle zusammengefasst ZBFW, um die Anforderungen für die Demonstration in diesem Artikel zu filtern.

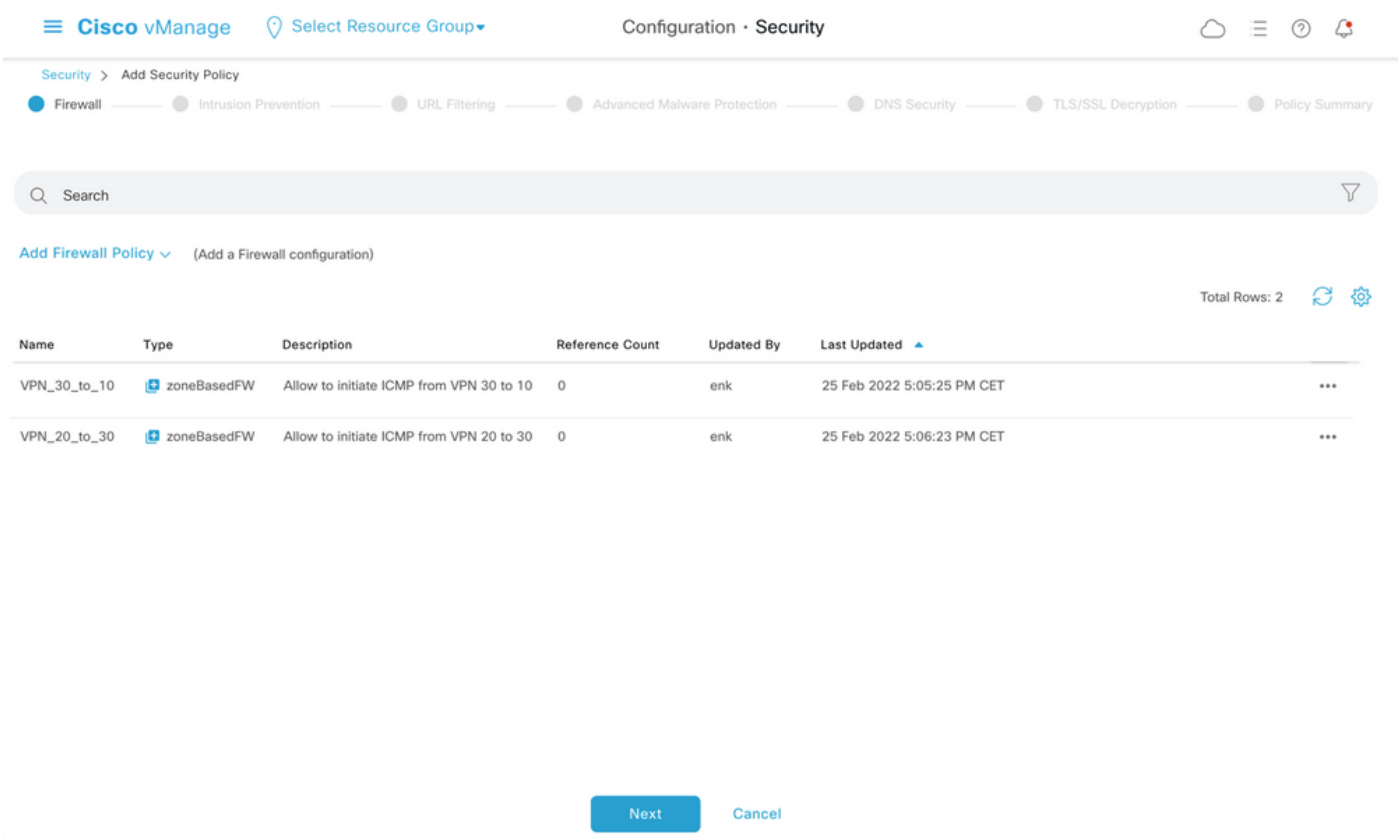
Zielzone Quellzone	VPN_10	VPN_20	VPN_30
VPN_10	zoneninterne Zulassung	Ablehnen	Ablehnen
VPN_20	Ablehnen	zoneninterne Zulassung	Zulassen
VPN_30	Zulassen	Ablehnen	zoneninterne Zulassung

Das Hauptziel besteht darin, jeden ICMP-Datenverkehr (Internet Control Message Protocol) zuzulassen, der von der Service-Seite des Router cE1 VPN 30 ausgeht und für VPN 10, aber nicht für VPN 20 bestimmt ist. Rücksendungen müssen automatisch zugelassen werden.



Außerdem muss jeder ICMP-Datenverkehr vom serviceseitigen VPN 20 des Routers in die VPN 30-Service-Seite von cE1, jedoch nicht von VPN 10 übertragen werden dürfen. Datenrückverkehr von VPN 30 zu VPN 20 muss automatisch zugelassen werden.

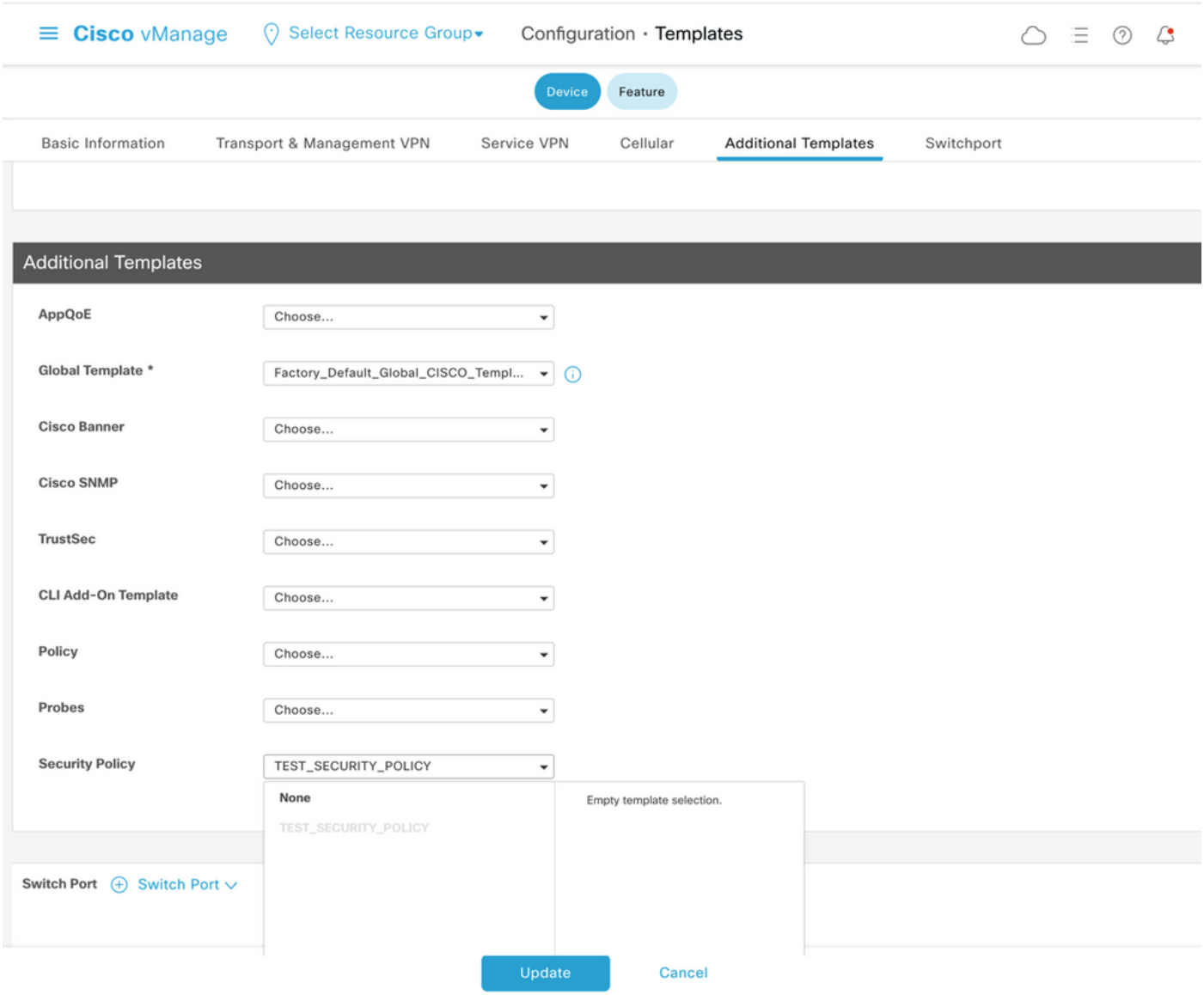




Hier finden Sie die ZBFW-Richtlinienvorschau als Referenz.

```
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 !
```

Um Sicherheitsrichtlinien anzuwenden, muss diese im Dropdown-Menü **Sicherheitsrichtlinie** im Bereich **Zusätzliche Vorlagen** der Gerätevorlage zugewiesen werden.



Nach der Aktualisierung der Gerätevorlage wird die Sicherheitsrichtlinie auf dem Gerät aktiviert, auf dem die Sicherheitsrichtlinie angewendet wurde. Zur Veranschaulichung in diesem Dokument reichte es aus, Sicherheitsrichtlinien nur auf dem cE1-Router zu aktivieren.

Überprüfung

Jetzt müssen Sie überprüfen, ob die erforderlichen Sicherheitsrichtlinien (ZBFW) erreicht wurden.

Der Test mit **Ping** bestätigt, dass der Datenverkehr von Zone VPN 10 zu VPN 30 wie erwartet abgelehnt wird, da für den Datenverkehr von VPN 10 zu VPN 30 kein Zonenpaar konfiguriert ist.

```
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)
```

Entsprechend ist der Datenverkehr von VPN 20 zu VPN 30 wie von der Konfiguration der Sicherheitsrichtlinien erwartet zulässig.

```
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
```

Datenverkehr von VPN 30 zu Subnetz 192.168.10.0/24 in Zone VPN 10 ist wie erwartet durch die Richtlinienkonfiguration zulässig.

```
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
```

Der Datenverkehr von VPN 30 zum Subnetz 192.168.20.0/24 in Zone VPN 20 wird abgelehnt, da für diesen Datenverkehr kein Zonenpaar konfiguriert ist, was erwartet wird.

```
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)
```

Zusätzliche Ergebnisse, die Sie interessieren können, können beim Pingen der IP-Adresse 192.168.12.12 beobachtet werden, da sie sich in der Zone VPN 10 oder VPN 20 befinden kann und es nicht möglich ist, das Ziel-VPN aus Sicht des Routers R30 auf der Service-Seite des SD-WAN Edge-Routers cE1 zu bestimmen.

```
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)
```

Das Ergebnis ist für alle Quellen in VRF 30 gleich. Dies bestätigt, dass die Hash-Funktion nicht von ECMP-Hashfunktionen (Equal-Cost Multi-Path) abhängt:

```
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)
```

Basierend auf den Testergebnissen für die Ziel-IP 192.168.12.12 können Sie nur vermuten, dass sie sich in VPN 20 befindet, da sie nicht auf die ICMP-Echo-Anfragen reagiert und höchstwahrscheinlich blockiert wird, da kein Zonenpaar konfiguriert ist, um Datenverkehr von VPN 30 zu VPN 20 zuzulassen (wie gewünscht). Wenn sich ein Ziel mit derselben IP-Adresse 192.168.12.12 im VPN 10 befindet und angenommen wird, dass es auf ICMP-Echoanfrage antwortet, muss Datenverkehr gemäß der ZBFW-Sicherheitsrichtlinie für ICMP-Datenverkehr vom VPN 30 zum VPN 20 zugelassen werden. Sie müssen das Ziel-VPN bestätigen.

Fehlerbehebung

Methode 1. So suchen Sie Ziel-VPN aus der OMP-Tabelle

Eine einfache Überprüfung der Routing-Tabelle auf cE1 hilft nicht, das tatsächliche Ziel-VPN zu ermitteln. Die hilfreichsten Informationen, die Sie von der Ausgabe erhalten können, sind eine System-IP-Adresse des Ziels (169.254.206.12) sowie die Tatsache, dass kein ECMP stattfindet.

```
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
```

Um das Ziel-VPN herauszufinden, muss zunächst das Service-Label aus der OMP-Tabelle auf cE1 für das gewünschte Präfix ermittelt werden.

```
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 -
```

Wir sehen, dass der Labelwert 1007 ist. Schließlich kann das Ziel-VPN gefunden werden, wenn alle Services, die vom Router mit dem System-IP 169.254.206.12 stammen, auf dem vSmart-Controller überprüft werden.

```
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
```

Basierend auf dem VPN-Label 1007 kann bestätigt werden, dass das Ziel-VPN 20 ist.

Methode 2. So suchen Sie Ziel-VPN mithilfe von Plattformbefehlen

Um mithilfe von Plattformbefehlen das Ziel-VPN zu ermitteln, müssen Sie zunächst eine interne VRF-ID für VPN 30 auf dem cE1-Router mithilfe von **show ip vrf detail 30** oder **show platform software ip f0 cef table * summary** Befehle **anzeigen**.

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

In diesem Fall wurde die VRF-ID 1 der VRF-Instanz mit dem Namen 30 zugewiesen. Plattformbefehle zeigen die OCE-Kette (Output Chain Element) von Objekten in SD-WAN-Software auf, die eine interne Weiterleitungslogik darstellt, die den Paketpfad in der Cisco IOS-XE-Software bestimmt:

```
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)
```

Das Präfix des Interesses zeigt auf das Next-Hop-Objekt des SLA-Klassentyps (OBJ_SDWAN_NH_SLA_CLASS) mit der ID 0xf80045f, das weiter verifiziert werden kann, wird hier angezeigt:

```
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
```

Dies ist eine lange Ausgabe, daher wurden SLA-Klassen von 2 bis 15 übersprungen, da keine Fallback-SLA-Klassen konfiguriert sind. Alle Klassen weisen auf dieselbe spezielle DROP-Adjacency wie SLA 1 hin. Das Hauptinteresse gilt dem Next-Hop-Objekt des indirekten Typs (SDWAN_NH_INDIRECT) von SLA 0. Es gibt kein ECMP und alle IDs sind identisch (0xf80044f). Sie kann genauer überprüft werden, um das ultimative Ziel-VPN und das Service-Label zu finden.

```
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: So suchen Sie mithilfe des Packet-Trace-Tools nach Ziel-VPN

Eine weitere Möglichkeit zum Auffinden eines Ziel-VPN ist ein **Paket-Trace-**Tool, das echte Pakete analysieren kann, die in Echtzeit über den Router laufen. Die Debug-Bedingung ist so festgelegt, dass der Datenverkehr nur mit der IP-Adresse 192.168.12.12 übereinstimmt.

```
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
```

Wenn anschließend der Datenverkehr von R30 mithilfe von **Ping** initiiert wurde, werden auf cE1 übereinstimmende Pakete angezeigt und die einzelnen Paketdetails überprüft. In diesem Fall ist es beispielsweise die erste Paketnummer 0. Die wichtigsten Zeilen werden mit **<<<<** Zeichen hervorgehoben.

```
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 :
```

Ein **Paket-Trace** gibt an, dass alle fünf per **Ping** gesendeten ICMP-Echopakete mit dem Drop-Code 52 verworfen wurden (FirewallL4Insp). Abschnitt**-Funktion: SDWAN Forwarding** gibt an, dass das Ziel-VPN 20 ist und das Service-Label 1007 im internen Header des getunnelten Pakets für die Weiterleitung verwendet wird, um das Ziel-VPN auf cE2 zu bestimmen. Abschnitt**-Funktion: Die ZBFW** bestätigt außerdem, dass Pakete verworfen wurden, da das Zonenpaar nicht für Datenverkehr vom Eingabe-VPN 20 an die VPN-30-Zone konfiguriert wurde.

Potenzielle Probleme durch Failover

Was passiert, wenn die Route 192.168.12.0/24 von R20 zurückgezogen wird oder nicht mehr von cE2 in VRF 20 erreichbar ist? Aus der Sicht von VRF 30 ist das Subnetz identisch, da die ZBFW-Sicherheitsrichtlinie Datenverkehr von Zone VPN 30 zu Zonen VPN 20 und 10 unterschiedlich behandelt, kann dies zu unerwünschten Ergebnissen führen, wie z. B. zum zulässigen Datenverkehr, aber nicht zum bzw. umgekehrt.

Wenn Sie beispielsweise einen Ausfall einer Verbindung zwischen cE2- und R20-Routern simulieren. Dies führt zu einer Route-Entnahme der 192.168.12.0/24 von der VPN 20-Routing-

Tabelle auf dem vSmart-Controller. Stattdessen wird die VPN 10-Route in die VPN 30-Routing-Tabelle übertragen. Verbindungen von VPN 30 zu VPN 10 sind gemäß den auf cE1 angewendeten Sicherheitsrichtlinien zulässig (dies ist aus Sicht der Sicherheitsrichtlinie zu erwarten, kann jedoch für das spezifische Subnetz in beiden VPNs nicht wünschenswert sein).

```
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 :
```

Beachten Sie, dass statt 1007 das Label 1006 verwendet wurde und die Ausgabe-VPN-ID jetzt 10 statt 20 lautet. Außerdem war das Paket gemäß der ZBFW-Sicherheitsrichtlinie zulässig, und es wurden entsprechende Zonenpaare, Klassenzuordnungen und Richtliniennamen angegeben.

Ein noch größeres Problem kann dadurch entstehen, dass die früheste Route in der Routing-Tabelle von VPN 30 gespeichert wird. In diesem Fall wird die VPN 10-Route durch die Übertragung der ursprünglich verwendeten VPN 20-Route in die VPN 30 OMP-Tabelle in vSmart übertragen. Stellen Sie sich das Szenario vor, in dem die ursprüngliche Idee genau das Gegenteil der in diesem Artikel beschriebenen Sicherheitsrichtlinienlogik der ZBFW war. So sollte beispielsweise der Datenverkehr von VPN 30 zu VPN 20 und nicht zu VPN 10 zugelassen werden. Wenn der Datenverkehr nach einer anfänglichen Richtlinienkonfiguration zugelassen wurde, bleibt der Datenverkehr nach dem Ausfall oder dem Rückzug der 192.168.12.0/24-Route aus VPN 20 auch nach der Wiederherstellung auf das Subnetz 192.168.12.0/24 blockiert, da die Route 192.168.12.0/24 immer noch aus VPN 10 ausläuft.