Configurazione di SD-WAN Zone-Based Firewall (ZBFW) e route Leaking

Sommario

Introduzione

Questo documento descrive come configurare, verificare e risolvere i problemi relativi a Zone-Based Firewall (ZBFW) con route-Leaking tra reti private virtuali (VPN).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- La sovrapposizione Cisco SD-WAN richiama una configurazione iniziale
- Configurazione ZBFW da interfaccia utente vManage
- Configurazione dei criteri di controllo della perdita di route dall'interfaccia utente di vManage

Componenti usati

Ai fini della dimostrazione, è stato utilizzato il software seguente:

- Controller Cisco SD-WAN vSmart con versione software 20.6.2
- Controller Cisco SD-WAN vManage con versione software 20.6.2
- Due router per piattaforma edge virtuale Cisco IOS®-XE Catalyst 8000V con versione

software 17.6.2 eseguibili in modalità controller
- Tre router per piattaforma edge virtuale Cisco IOS-XE Catalyst 8000V con versione software 17.6.2 eseguibili in modalità autonoma

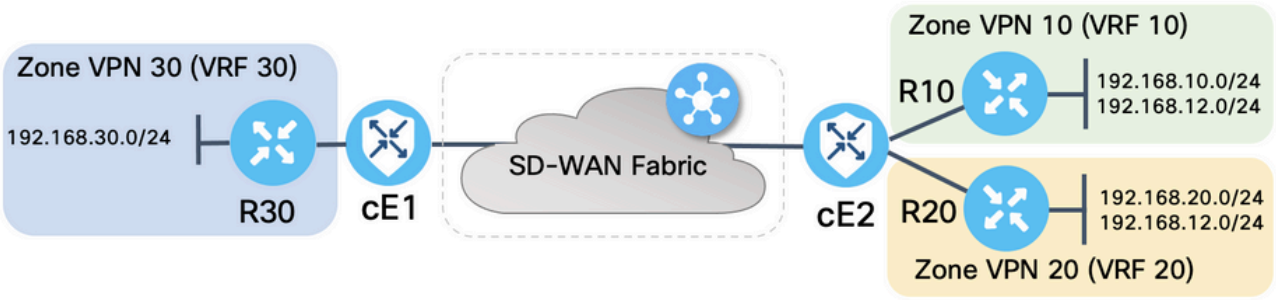
Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Questo documento spiega come il router determina il mapping della VPN di destinazione nella sovrapposizione SD-WAN e come verificare e risolvere i problemi di route che perdono tra VPN. Descrive inoltre le peculiarità della selezione del percorso nel caso in cui la stessa subnet venga annunciata da una VPN diversa e il tipo di problemi che possono sorgere a causa di ciò.

Configurazione

Esempio di rete



Entrambi i router SD-WAN sono stati configurati con parametri di base per stabilire connessioni di controllo con i controller SD-WAN e le connessioni del piano dati tra di essi. I dettagli di questa configurazione non sono compresi nell'ambito del presente documento. La tabella riepiloga le assegnazioni VPN, ID sito e zone.

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

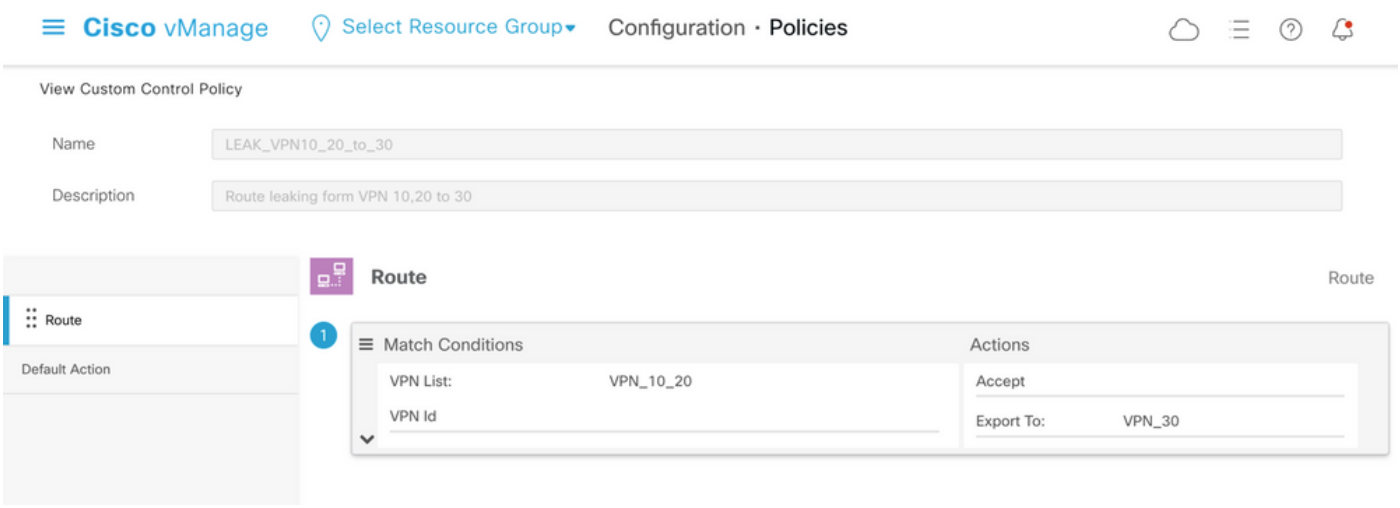
I router sul lato servizio sono stati configurati con route statiche predefinite in ciascun VRF (Virtual Routing and Forwarding) che punta al router SD-WAN corrispondente. Analogamente, i router SD-WAN Edge sono stati configurati con route statiche che puntano alle subnet corrispondenti. Notare che, per dimostrare i potenziali problemi di perdita di percorso e ZBFW, i router dietro il lato assistenza di cE2 hanno la stessa subnet 192.168.12.0/24. Su entrambi i router dietro cE2, è presente un'interfaccia di loopback configurata per emulare un host con lo stesso indirizzo IP 192.168.12.12.

Èimportante notare che i router Cisco IOS-XE R10, R20 e R30 vengono eseguiti in modalità autonoma sui lati dei servizi delle route SD-WAN Edge, che in questa dimostrazione servono

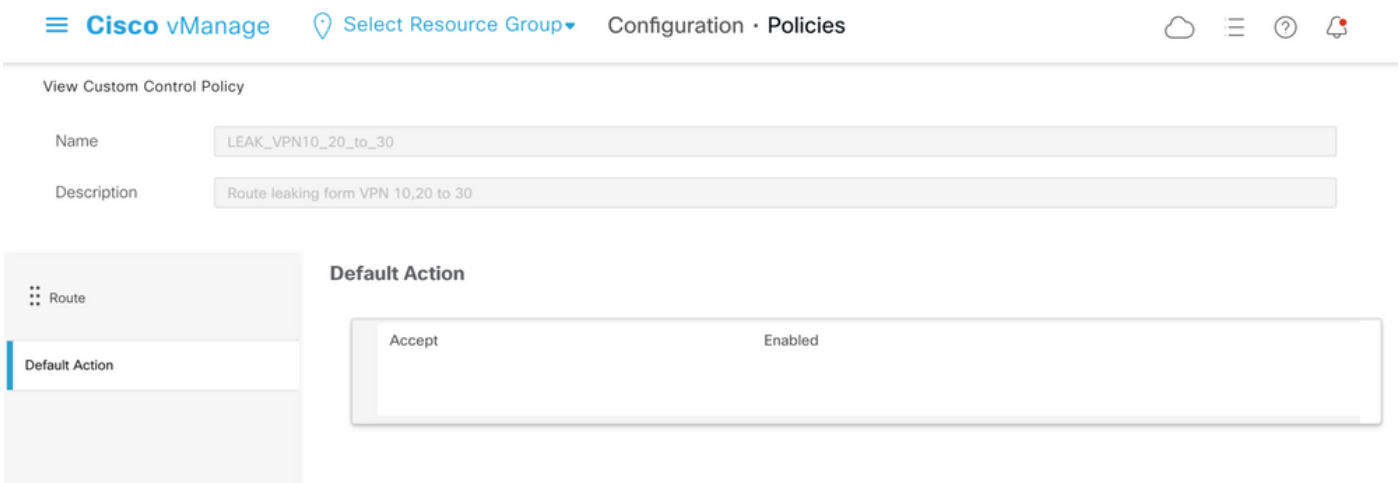
principalmente a emulare gli host finali. Le interfacce di loopback sulle route SD-WAN Edge non possono essere utilizzate per questo scopo anziché host reali come i router sul lato servizio, perché il traffico che proviene da un'interfaccia in un VRF di SD-WAN Edge router non è considerato come traffico originato nella zona ZBFW che corrisponde, ma appartiene alla zona autonoma speciale di un router edge. Per questo motivo la zona ZBFW non può essere considerata uguale alla zona VRF. Una discussione dettagliata sulla propria area esula dall'ambito di questo articolo.

Configurazione perdita route

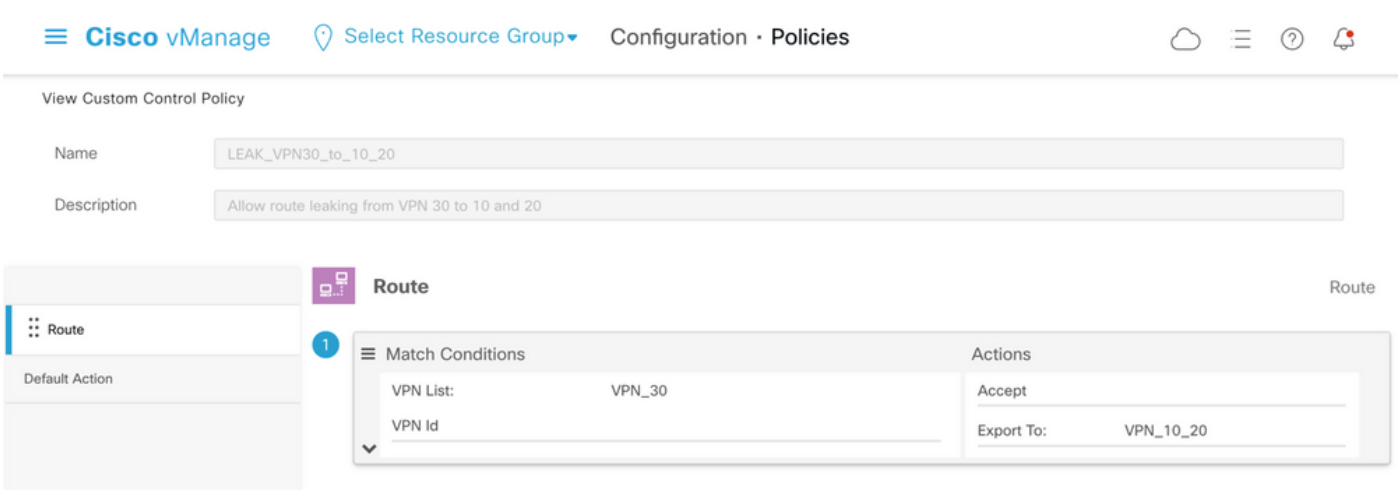
L'obiettivo principale della configurazione dei criteri di controllo è consentire la perdita di route da tutte le route dalla VPN 10 e 20 alla VPN 30. Il VRF 30 esiste solo sul router cE1 e i VRF 10 e 20 sono configurati solo sul router cE2. A tale scopo, sono stati configurati due criteri di topologia (controllo personalizzato). Di seguito è riportata la topologia per esportare tutte le route dalla VPN 10 e 20 alla VPN 30.

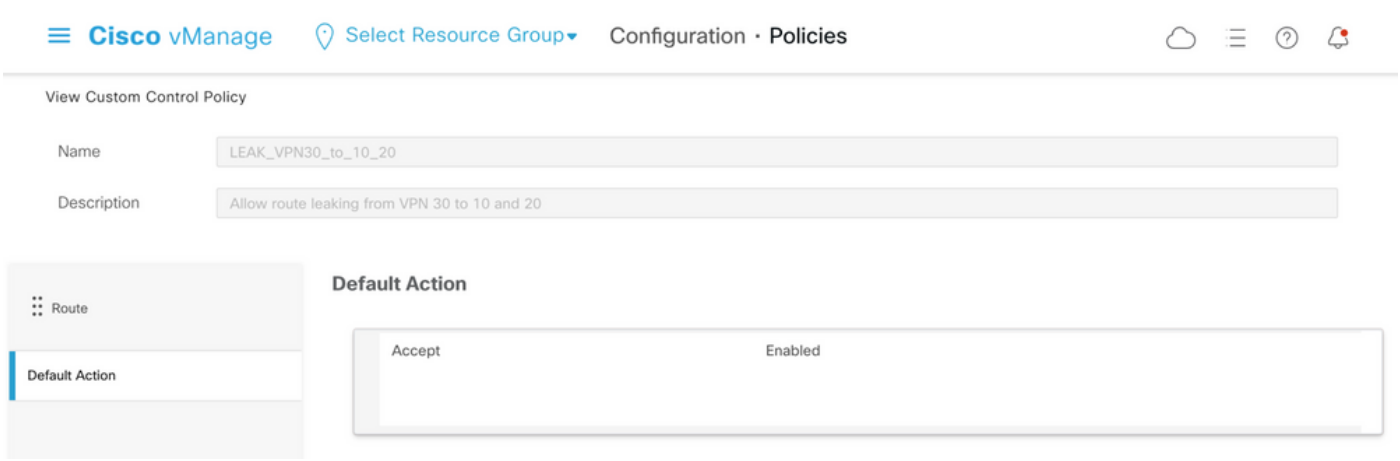


Notare che l'azione predefinita è impostata su **Consenti,** per evitare il blocco di annunci TLOC o di normali annunci di route intra-VPN accidentalmente.

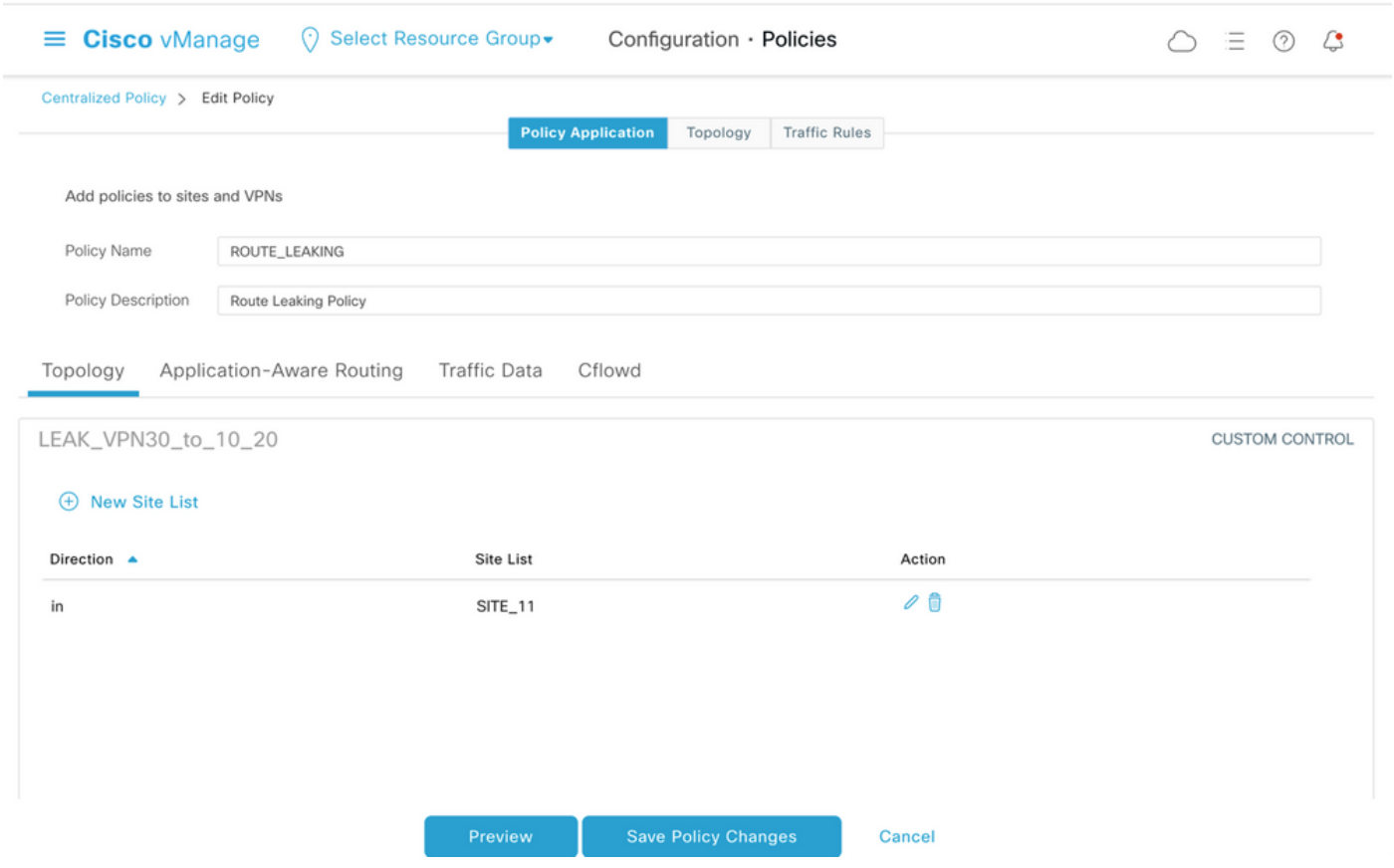


Analogamente, il criterio di topologia è stato configurato per consentire la pubblicità inversa delle informazioni di routing dalla VPN 30 alla VPN 10 e 20.

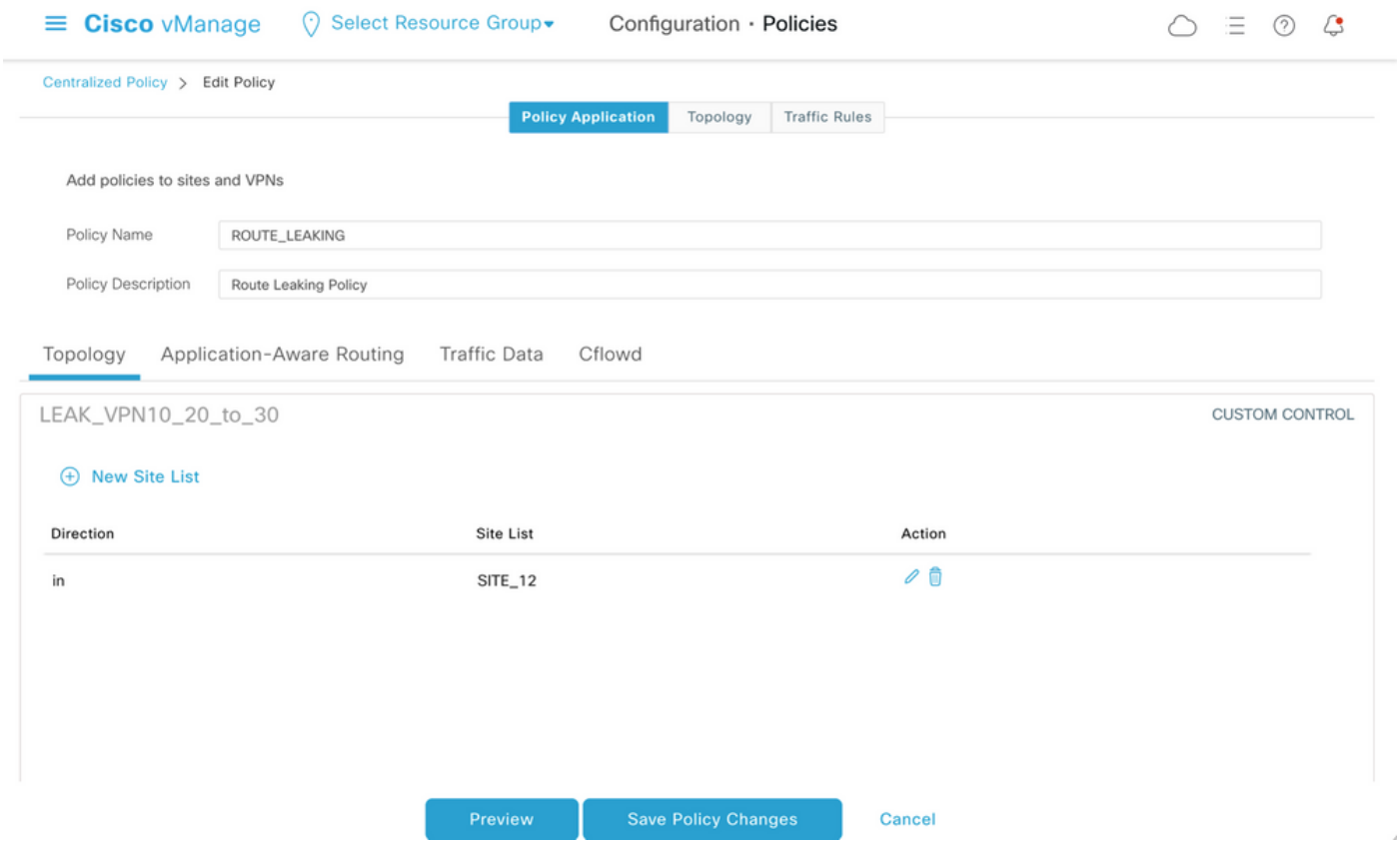




Entrambi i criteri di topologia vengono quindi assegnati agli elenchi di siti corrispondenti, nella direzione in ingresso (in ingresso). Le route della VPN 30 vengono esportate dal controller vSmart nelle tabelle OMP (Overlay Management Protocol) della VPN 10 e 20 quando vengono ricevute da cE1 (site-id 11).



Analogamente, le route da VPN 10 e 20 vengono esportate da vSmart nella tabella di routing VPN 30 alla ricezione delle route VPN 10 e 20 da cE2 (site-id 12).



Di seguito è riportata un'anteprima completa della configurazione dei criteri di controllo per riferimento.

```
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 ! !
```

Il criterio deve essere attivato dalla sezione **Configurazione** controller vManage **> Criteri** per essere valido sul controller vSmart.

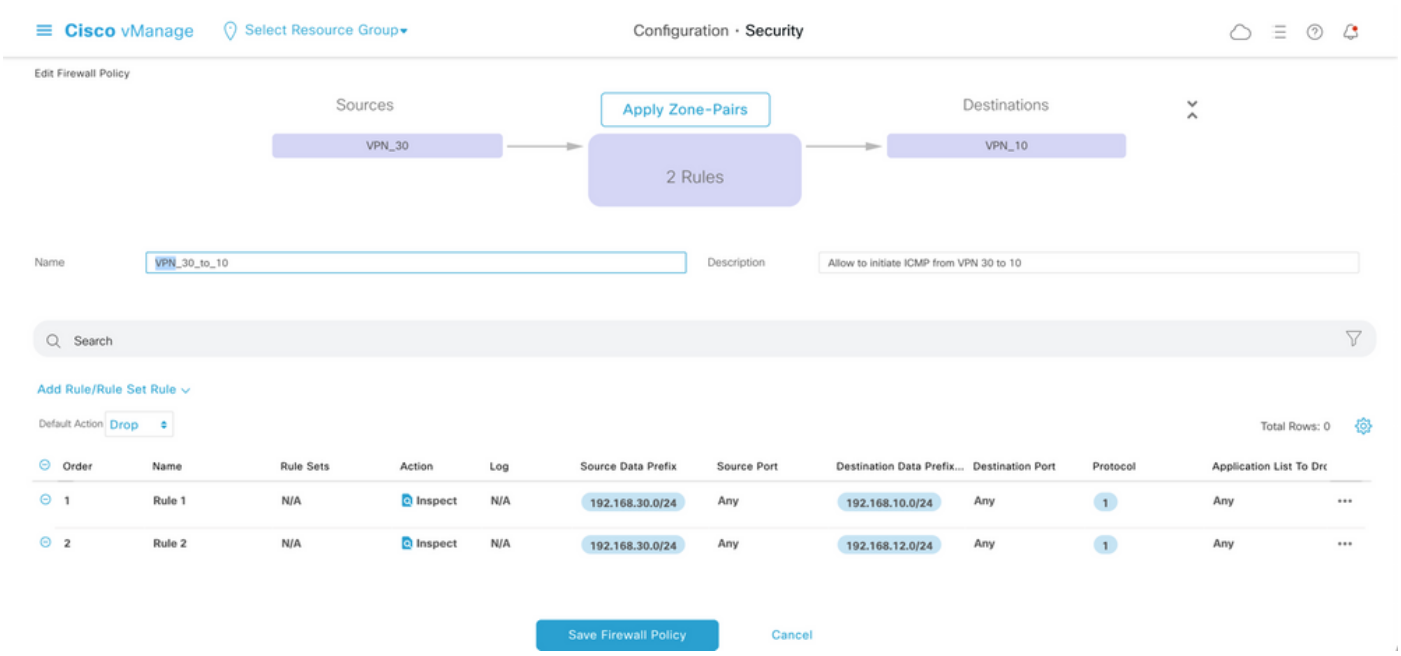
Configurazione ZBFW

Di seguito è riportata una tabella che riepiloga i requisiti ZBFW per filtrare i requisiti a scopo dimostrativo in questo articolo.

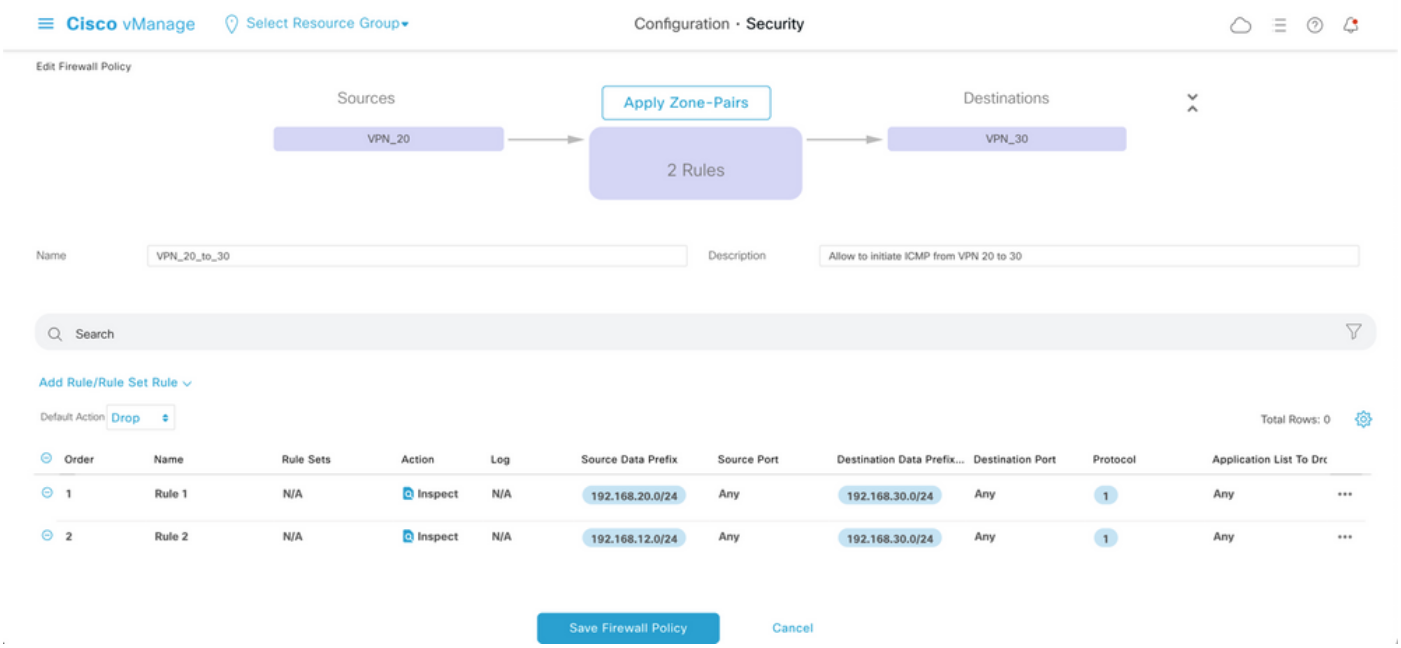
Zona di destinazione Zona di origine	VPN_10	VPN_20	VPN_30
VPN_10	consenti intra-zona	Nega	Nega
VPN_20	Nega	consenti intra-zona	Allow (Autorizza)
VPN_30	Allow (Autorizza)	Nega	consenti intra-zona

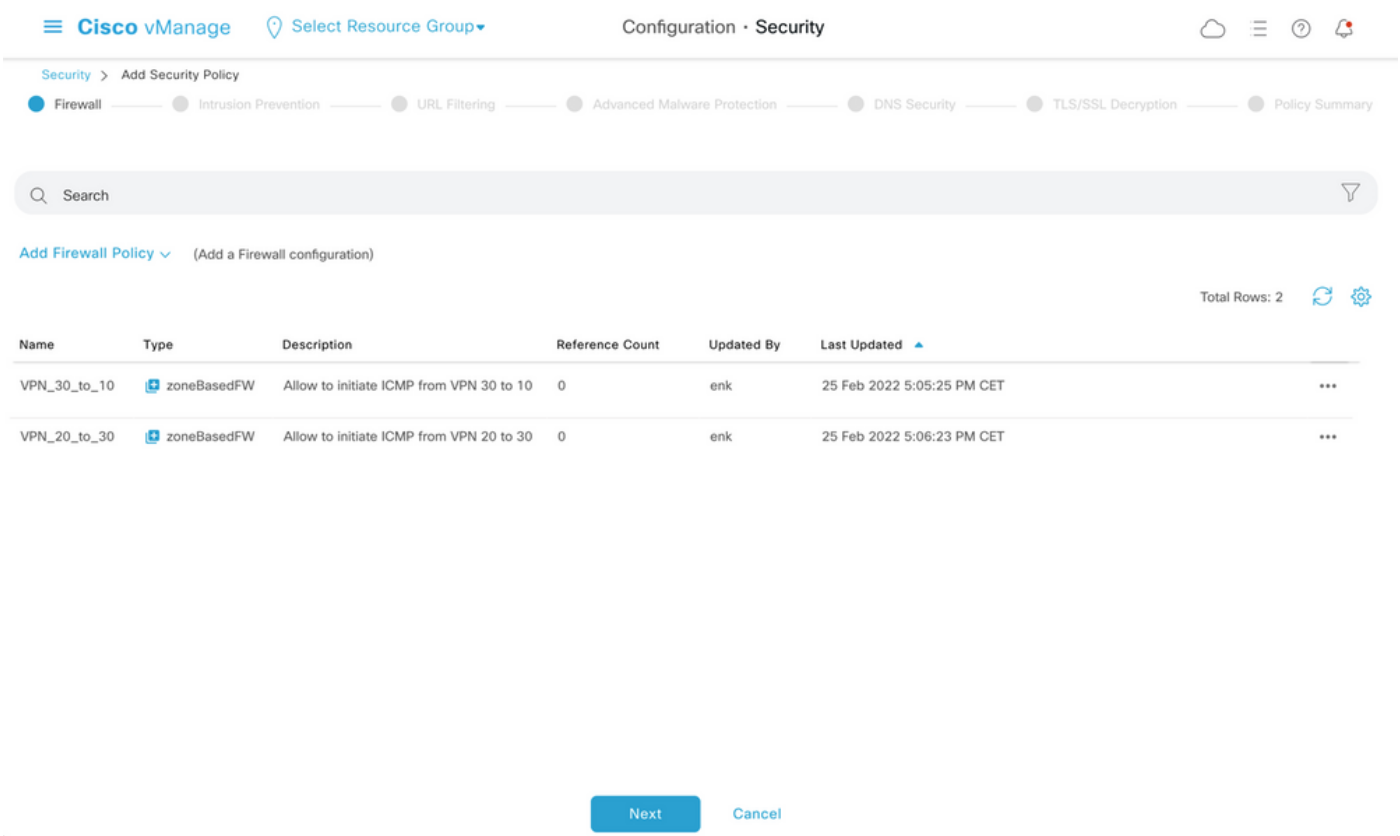
L'obiettivo principale è consentire tutto il traffico Internet Control Message Protocol (ICMP)

proveniente dal lato servizio del router cE1 VPN 30 e destinato alla VPN 10 ma non alla VPN 20. Il traffico di ritorno deve essere consentito automaticamente.



Anche il traffico ICMP proveniente dal router cE2 della VPN 20 sul lato servizio deve essere autorizzato al transito nella VPN 30 sul lato servizio di cE1, ma non dalla VPN 10. Il traffico di ritorno dalla VPN 30 alla VPN 20 deve essere autorizzato automaticamente.

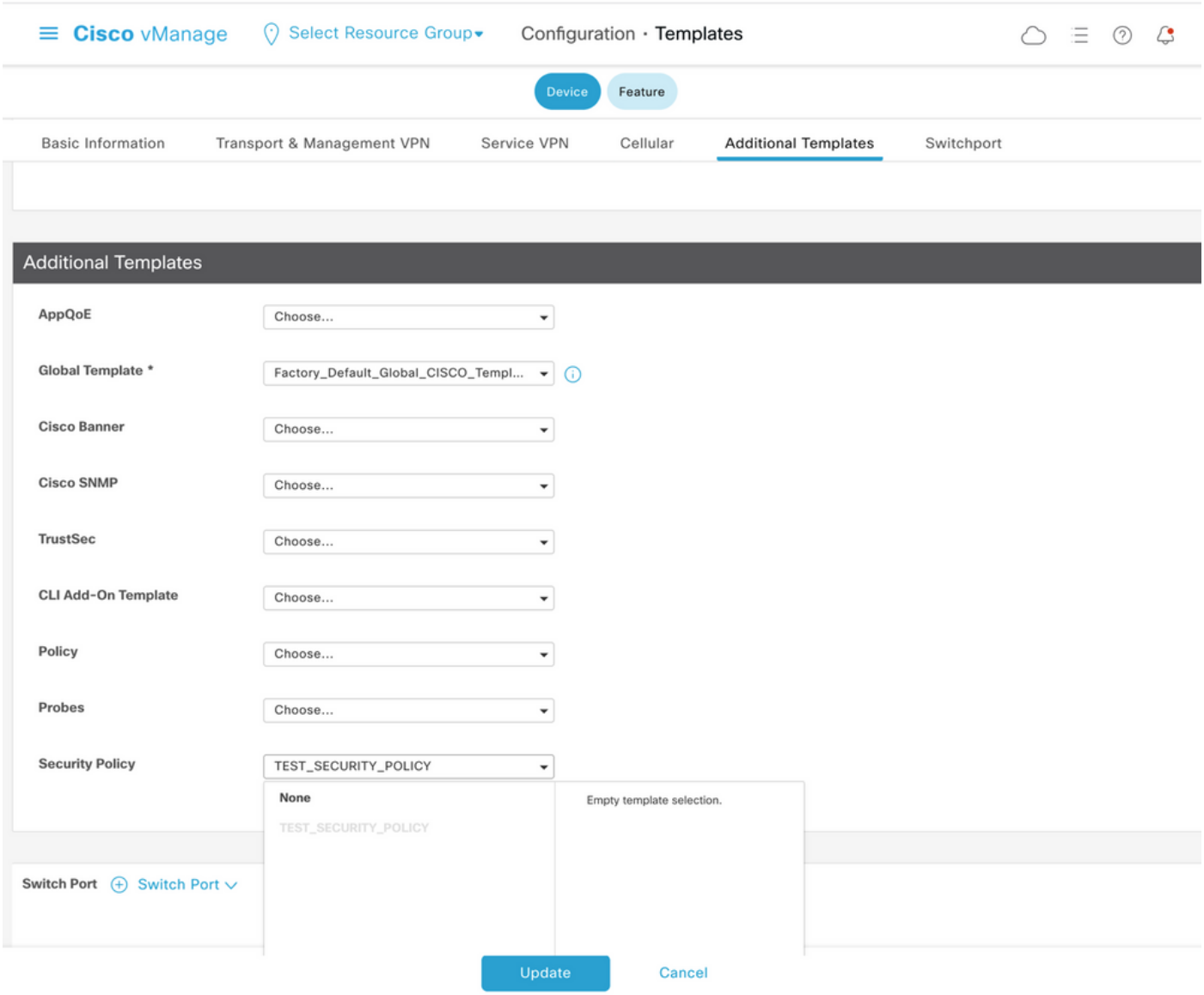




Qui è possibile trovare l'anteprima del criterio ZBFW per riferimento.

```
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 !
```

Per applicare il criterio di protezione, è necessario assegnarlo nella sezione del menu a discesa **Criterio di protezione** della sezione **Modelli aggiuntivi** del modello di dispositivo.



Una volta aggiornato il modello di dispositivo, il criterio di protezione diventa attivo nel dispositivo in cui è stato applicato. Ai fini della dimostrazione in questo documento, è stato sufficiente abilitare i criteri di sicurezza solo sul router cE1.

Verifica

A questo punto, è necessario verificare che gli obiettivi ZBFW richiesti siano stati raggiunti.

Il test con **ping** conferma che il traffico dalla zona VPN 10 alla VPN 30 viene rifiutato come previsto perché non è configurata una coppia di zone per il traffico dalla VPN 10 alla 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)
```

Analogamente, il traffico proveniente dalla VPN 20 è consentito alla VPN 30 come previsto dalla configurazione dei criteri di sicurezza.

```
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
```

Il traffico dalla VPN 30 alla subnet 192.168.10.0/24 nella zona VPN 10 è consentito come previsto dalla configurazione dei criteri.

```
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
```

Il traffico tra la VPN 30 e la subnet 192.168.20.0/24 nella zona VPN 20 è negato perché non è configurata alcuna coppia di zone per questo traffico, come previsto.

```
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)
```

Ulteriori risultati che possono essere interessanti possono essere osservati quando si cerca di eseguire il ping sull'indirizzo IP 192.168.12.12 perché può essere nella zona VPN 10 o VPN 20 e non è possibile determinare la VPN di destinazione dalla prospettiva del router R30 situato sul lato servizio del router edge SD-WAN 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)
```

Il risultato è lo stesso per tutte le origini in VRF 30. Ciò conferma che non dipende dai risultati della funzione hash ECMP (Equal-Cost Multi-Path):

```
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)
```

In base ai risultati dei test per l'indirizzo IP 192.168.12.12 di destinazione, è possibile prevedere solo che si trovi nella VPN 20 perché non risponde alle richieste echo ICMP e probabilmente è bloccato perché non è presente una coppia di zone configurata per consentire il traffico dalla VPN 30 alla VPN 20 (a seconda delle esigenze). Se una destinazione con lo stesso indirizzo IP 192.168.12.12 si trova nella VPN 10 e si presume che risponda alla richiesta echo ICMP, il traffico deve essere autorizzato in base ai criteri di sicurezza ZBFW per il traffico ICMP dalla VPN 30 alla VPN 20. È necessario confermare la VPN di destinazione.

Risoluzione dei problemi

Metodo 1. Per trovare la VPN di destinazione dalla tabella OMP

Una semplice verifica della tabella di routing su cE1 non aiuta a capire la VPN di destinazione effettiva. Le informazioni più utili che si possono ottenere dall'output sono un indirizzo IP del sistema di destinazione (169.254.206.12) e anche che non esiste alcun ECMP.

```
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
```

Per trovare la VPN di destinazione, è necessario innanzitutto trovare l'etichetta del servizio dalla tabella OMP su cE1 per il prefisso di interesse.

```
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 -
```

Vediamo che il valore dell'etichetta è 1007. Infine, la VPN di destinazione può essere trovata se tutti i servizi che provengono dal router che possiede l'IP 169.254.206.12 del sistema sono controllati sul controller vSmart.

```
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
```

In base all'etichetta VPN 1007, è possibile confermare che la VPN di destinazione sia 20.

Metodo 2. Per trovare la VPN di destinazione con l'aiuto dei comandi della piattaforma

Per individuare la VPN di destinazione con l'aiuto dei comandi della piattaforma, è necessario innanzitutto ottenere un ID VRF interno per la VPN 30 sul router cE1 con l'aiuto dei comandi **show ip vrf detail 30** o **show platform software ip f0 cef table * summary**.

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

In questo caso, l'ID VRF 1 è stato assegnato al VRF denominato 30. I comandi della piattaforma rivelano la catena OCE (Output Chain Element) di oggetti nel software SD-WAN che rappresentano la logica di inoltro interno che determina il percorso del pacchetto nel software Cisco IOS-XE:

```
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)
```

Di seguito è riportato il prefisso del riferimento all'oggetto dell'hop successivo del tipo di classe SLA (Service Level Agreement) (OBJ_SDWAN_NH_SLA_CLASS) con ID 0xf800045f che è possibile verificare ulteriormente:

```
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
```

Questo è un output lungo, quindi le classi SLA da 2 a 15 sono state ignorate perché non sono configurate classi SLA di fallback e tutte puntano alla stessa adiacenza DROP speciale di SLA 1. L'interesse principale è l'oggetto hop successivo di tipo indiretto (SDWAN_NH_INDIRECT) da SLA 0. È inoltre possibile notare che non esiste alcun ECMP e che tutti gli ID sono uguali (0xf800044f). È possibile eseguire ulteriori verifiche per trovare la VPN di destinazione finale e l'etichetta del servizio.

```
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
```

Metodo 3. Per trovare la VPN di destinazione con l'aiuto dello strumento Packet-Trace

Un altro modo per trovare una VPN di destinazione è uno strumento **di traccia dei pacchetti** che può analizzare i pacchetti reali che passano attraverso il router in tempo reale. La condizione di debug è impostata in modo da far corrispondere solo il traffico da/verso l'indirizzo IP 192.168.12.12.

```
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
```

Quindi, se il traffico è stato iniziato dalla R30 con l'aiuto del **ping**, è possibile vedere i pacchetti corrispondenti su cE1 e controllare i dettagli di ciascun pacchetto. In questo caso, è il primo numero di pacchetto, ad esempio 0. Le righe più importanti sono evidenziate con segni **<<<<**.

```
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 :
```

Un **packet-trace** indica che tutti e cinque i pacchetti echo ICMP inviati dal **ping** sono stati scartati con il codice di rilascio 52 (FirewallL4Insp). **Funzione** sezione**: SDWAN Forwarding** indica che la VPN di destinazione è 20 e che l'etichetta di servizio 1007 nell'intestazione interna del pacchetto tunneled viene utilizzata per inoltrare la VPN di destinazione su cE2. **Funzione della** sezione**: ZBFW** conferma inoltre che i pacchetti sono stati scartati perché la coppia di zone non era configurata per il traffico dall'input VPN 20 destinato alla zona VPN 30.

Problemi potenziali dovuti al failover

Cosa succede se la route 192.168.12.0/24 viene ritirata da R20 o non è più raggiungibile da cE2 in VRF 20? Anche se dal punto di vista del VRF 30 la subnet è la stessa, poiché i criteri di sicurezza ZBFW trattano il traffico dalla zona VPN 30 alle zone VPN 20 e 10 in modo diverso, può portare a risultati indesiderati come il traffico consentito, mentre non deve essere o viceversa.

Ad esempio, se si simula un errore di collegamento tra router cE2 e R20. Ciò porta al ritiro della route 192.168.12.0/24 dalla tabella di routing VPN 20 sul controller vSmart e, al contrario, alla perdita della route VPN 10 nella tabella di routing VPN 30. La connettività dalla VPN 30 alla VPN 10 è consentita in base ai criteri di sicurezza applicati alla VPN 1 (ciò è previsto dalla prospettiva dei criteri di sicurezza, ma non può essere auspicabile per la subnet specifica presentata in entrambe le VPN).

```
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 :
```

Si noti che è stata utilizzata l'etichetta 1006 anziché 1007 e che l'ID VPN di output è 10 anziché 20. Inoltre, il pacchetto è stato autorizzato in base ai criteri di sicurezza ZBFW e sono stati specificati i corrispondenti nomi di zone-pair, class-map e policy.

C'è un problema ancora più grande che può sorgere a causa del fatto che la route meno recente è conservata nella tabella di routing della VPN 30 e in questo caso è la route VPN 10 che dopo l'applicazione dei criteri di controllo iniziali la route VPN 20 è stata trapelata nella tabella VPN 30 OMP su vSmart. Immaginate lo scenario in cui l'idea originale era esattamente l'opposto della logica dei criteri di sicurezza di ZBFW descritta in questo articolo. Ad esempio, l'obiettivo era quello di consentire il traffico dalla VPN 30 alla VPN 20 e non alla VPN 10. Se fosse consentito dopo una configurazione iniziale dei criteri, dopo il guasto o il ritiro della route 192.168.12.0/24 dalla VPN 20, il traffico rimarrebbe bloccato alla subnet 192.168.12.0/24 anche dopo il ripristino, in quanto la route 192.168.12.0/24 continua a perdere dalla VPN 10.