Configuración del firewall basado en zonas SD-WAN (ZBFW) y la fuga de rutas

Contenido

Introducción

Este documento describe cómo configurar, verificar y resolver problemas de firewall basado en zonas (ZBFW) con filtrado de rutas entre redes privadas virtuales (VPN).

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- La superposición de Cisco SD-WAN ofrece una configuración inicial
- Configuración de ZBFW desde la interfaz de usuario vManage
- Configuración de la política de control de fuga de ruta desde la interfaz de usuario de vManage

Componentes Utilizados

A los efectos de la demostración, se utilizaron estos programas:

- Controlador vSmart SD-WAN de Cisco con versión de software 20.6.2
- Controlador Cisco SD-WAN vManage con versión de software 20.6.2

- Dos routers de plataforma de borde virtual Cisco IOS®-XE Catalyst 8000V con versión de software 17.6.2 que se ejecutan en modo controlador
- Tres routers de plataforma de borde virtual Cisco IOS-XE Catalyst 8000V con versión de software 17.6.2 que se ejecutan en modo autónomo

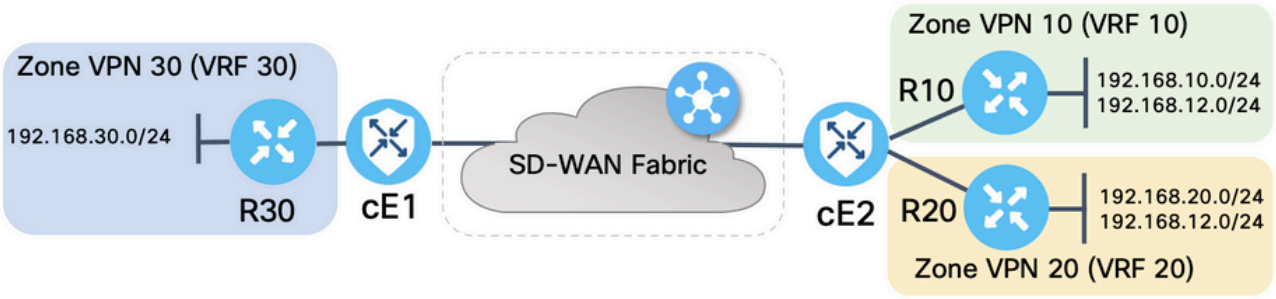
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

Este documento explica cómo el router determina el mapeo de VPN de destino en la superposición SD-WAN y cómo verificar y resolver la fuga de ruta entre las VPN. También describe las peculiaridades de la selección de trayectoria en caso de que la misma subred se anuncie desde una VPN diferente y qué tipo de problemas pueden surgir debido a esto.

Configurar

Diagrama de la red



Ambos routers SD-WAN se configuraron con parámetros básicos para establecer conexiones de control con controladores SD-WAN y conexiones de plano de datos entre ellos. Los detalles de esta configuración están fuera de alcance a los efectos de este documento. La tabla aquí resume las asignaciones de VPN, ID de sitio y Zonas.

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

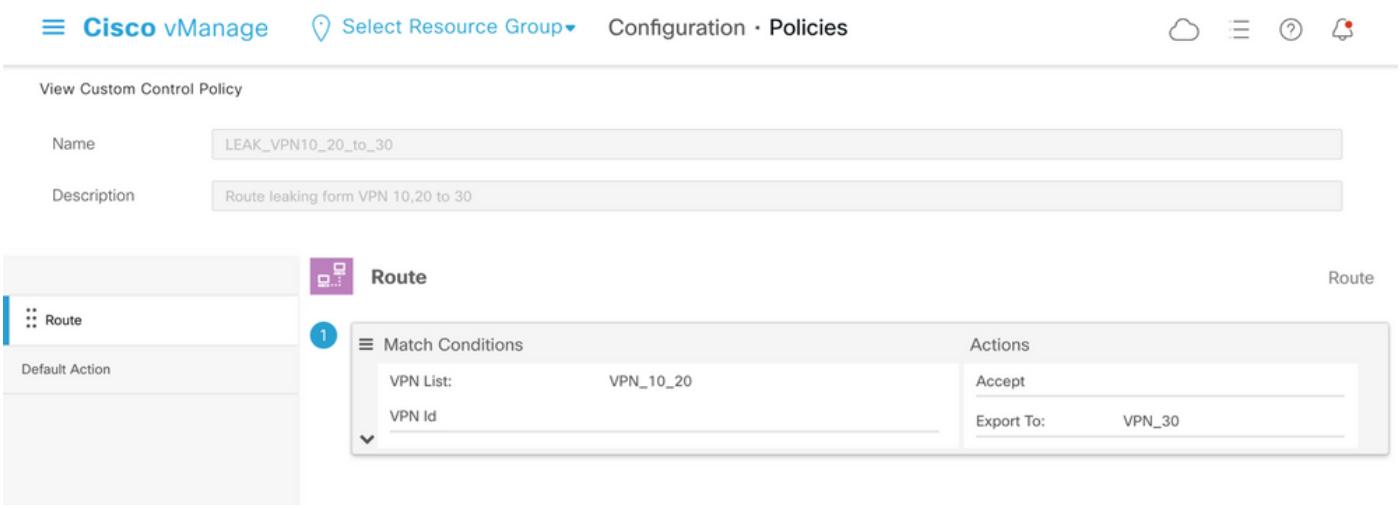
Los routers del lado del servicio se configuraron con rutas estáticas predeterminadas en cada Virtual Routing and Forwarding (VRF) que apunta al router SD-WAN correspondiente. Del mismo modo, los routers periféricos SD-WAN se configuraron con rutas estáticas que apuntan a las subredes que corresponden. Tenga en cuenta que, con el propósito de demostrar los problemas potenciales con la fuga de rutas y ZBFW, los routers detrás del lado de servicio de cE2 tienen la misma subred 192.168.12.0/24. En ambos routers detrás de cE2, hay una interfaz de loopback configurada para emular un host con la misma dirección IP 192.168.12.12.

Es importante tener en cuenta que los routers R10, R20 y R30 del IOS XE de Cisco se ejecutan en modo autónomo en los lados de servicio de las rutas del extremo SD-WAN que sirven

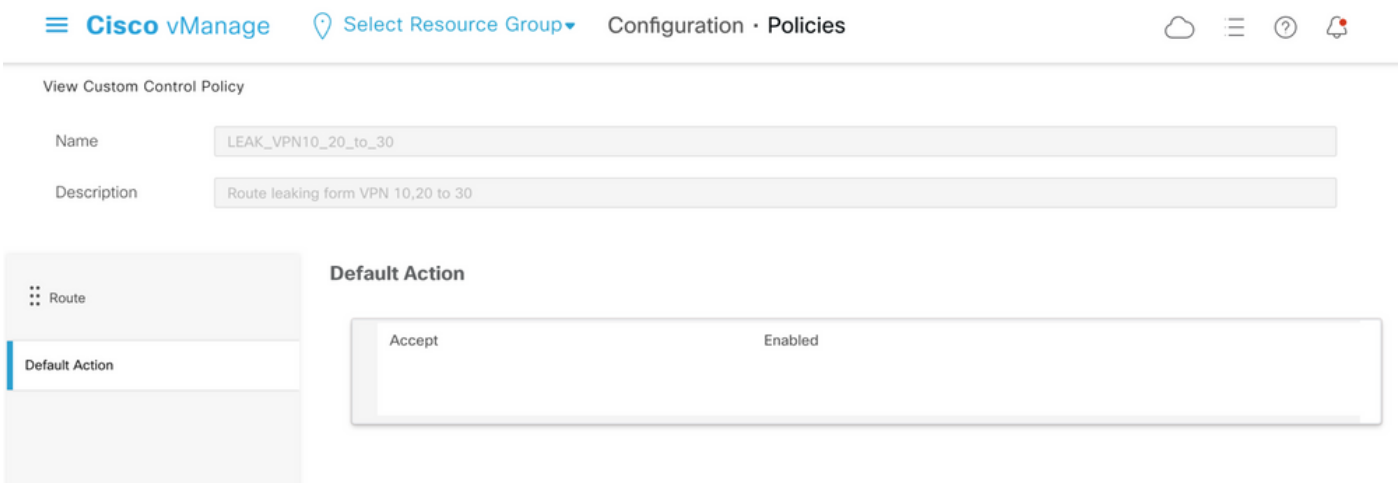
principalmente para emular los hosts finales en esta demostración. Las interfaces de loopback en las rutas del extremo SD-WAN no se pueden utilizar para este fin en lugar de hosts reales como los routers del lado del servicio, porque el tráfico que se origina desde una interfaz en un VRF de un router del extremo SD-WAN no se considera tráfico originado en la zona ZBFW que corresponde, y más bien pertenece a la zona automática especial de un router de borde. Por eso la zona ZBFW no puede considerarse igual que VRF. Una discusión detallada de la zona autónoma está fuera del alcance de este artículo.

Configuración de fuga de ruta

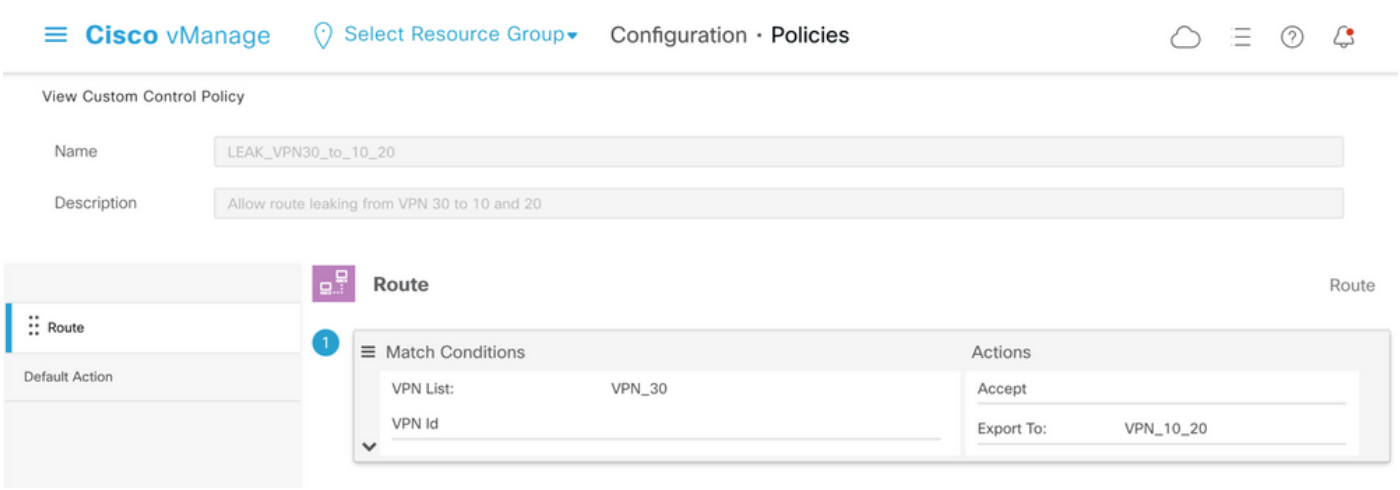
El objetivo principal de configuración de la política de control es permitir la fuga de rutas de todas las rutas desde VPN 10 y 20 a VPN 30. El VRF 30 existe solamente en el router cE1 y los VRF 10 y 20 se configuran solamente en el router cE2. Para lograrlo, se configuraron dos políticas de topología (Control personalizado). Esta es la topología para exportar todas las rutas desde VPN 10 y 20 a VPN 30.

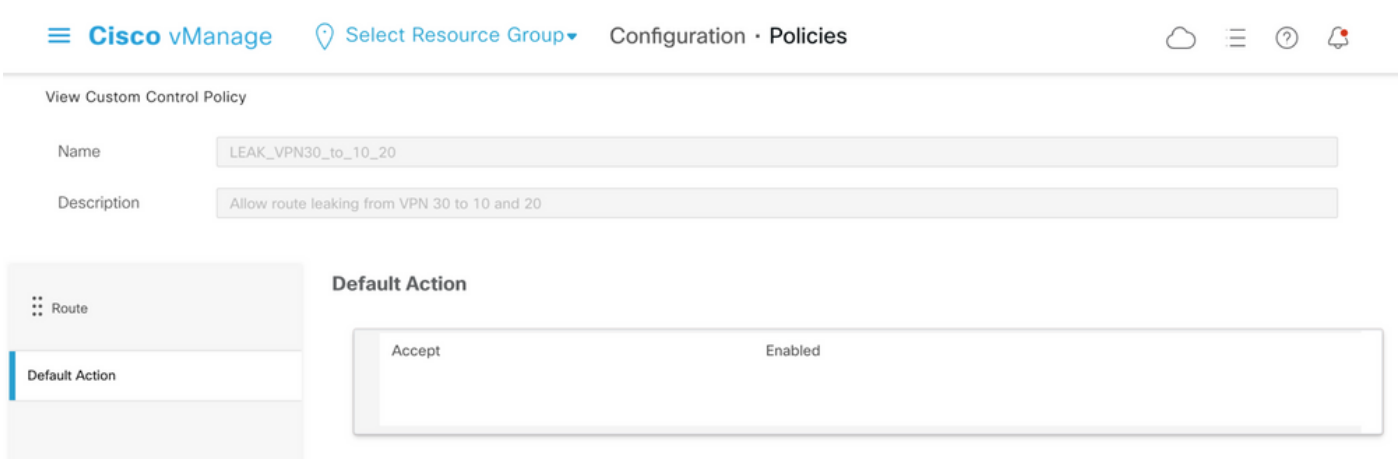


Tenga en cuenta que la Acción predeterminada se establece en **Permitir,** para evitar el bloqueo de anuncios TLOC o anuncios de rutas internas de VPN normales accidentalmente.

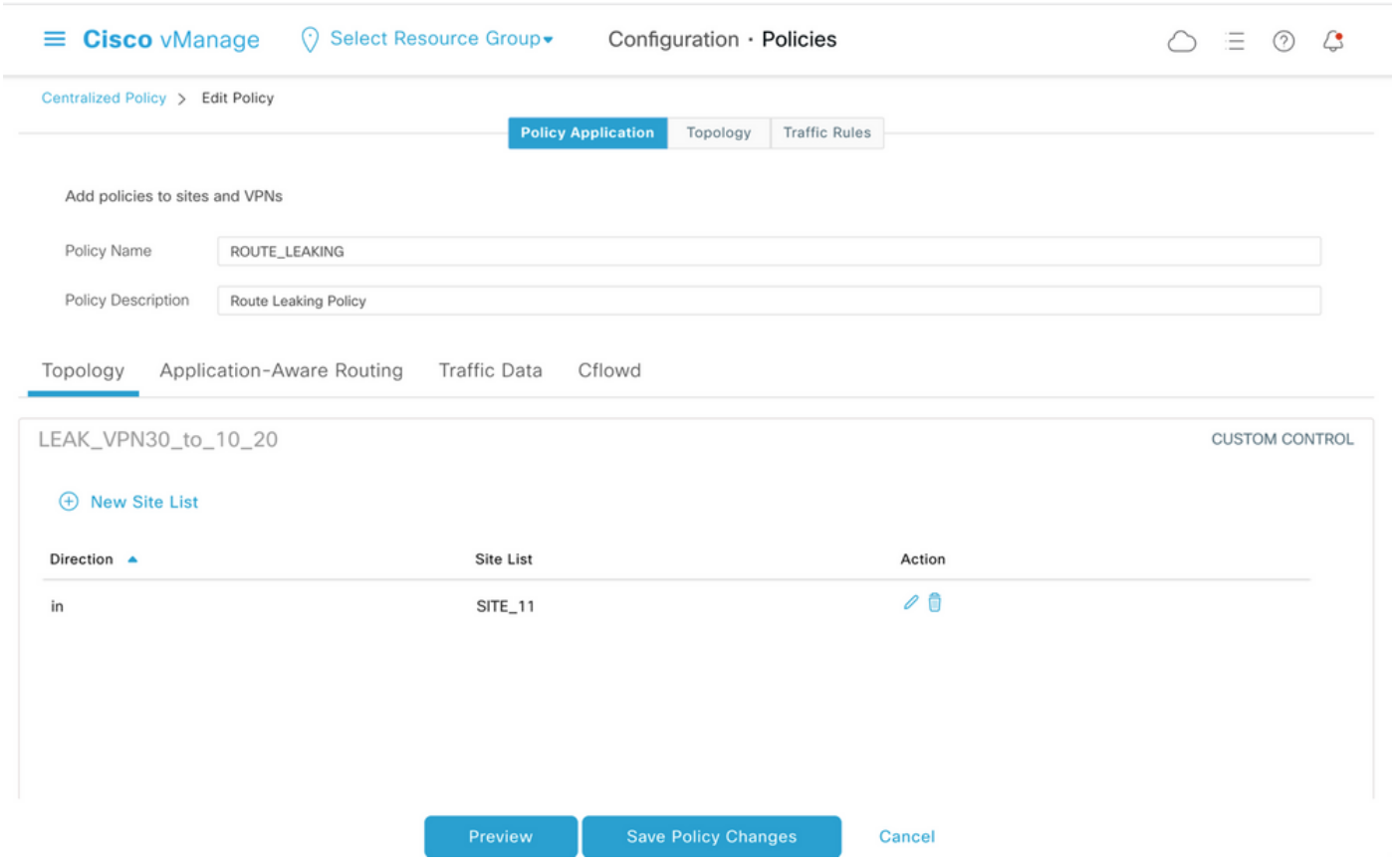


De manera similar, la política de topología se configuró para permitir el anuncio inverso de la información de ruteo de VPN 30 a VPN 10 y 20.

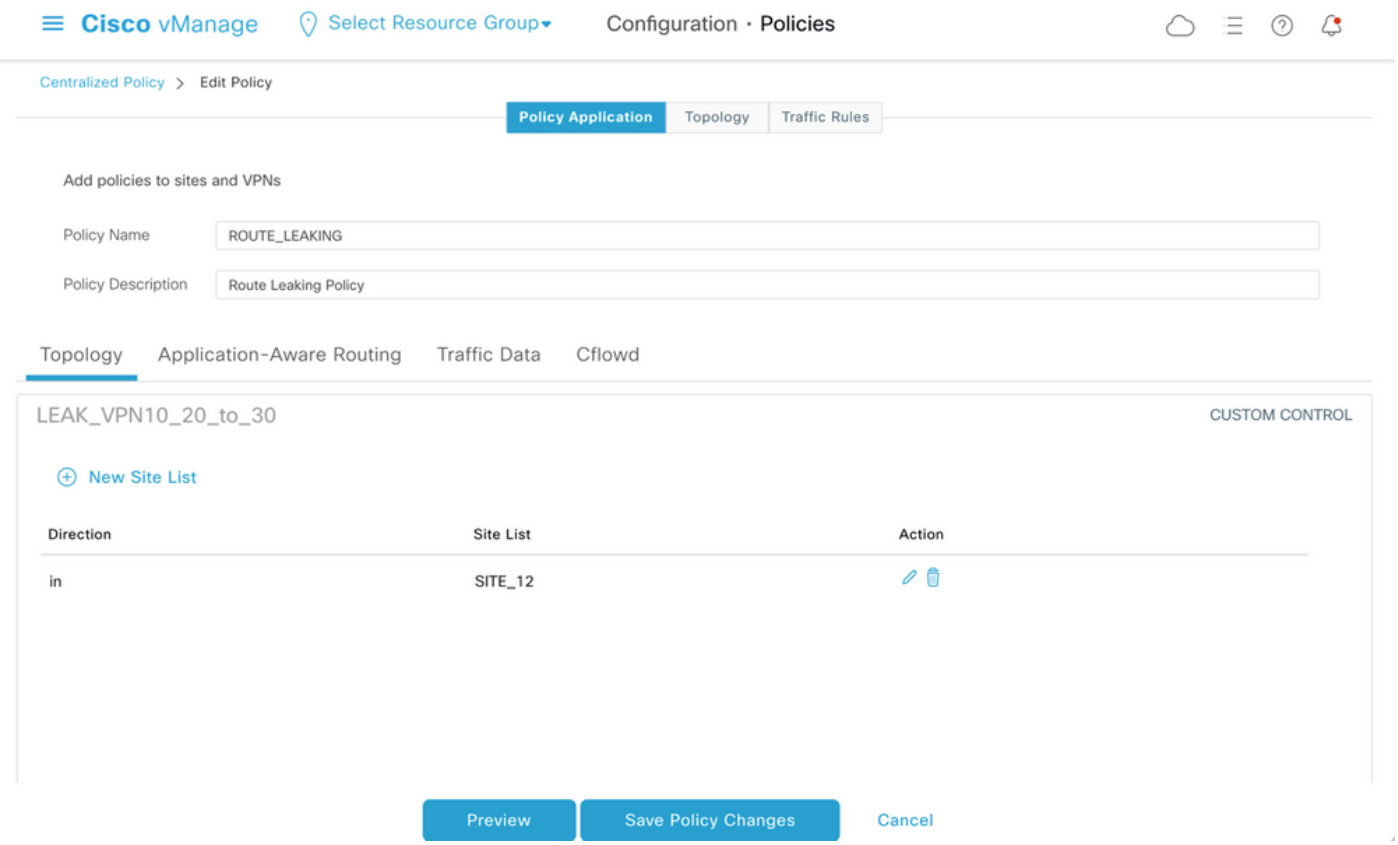




A continuación, ambas políticas de topología se asignan a las listas de sitios que corresponden, en la dirección de ingreso (entrante). Las rutas de VPN 30 son exportadas por el controlador vSmart a las tablas Overlay Management Protocol (OMP) de VPN 10 y 20 cuando se reciben desde cE1 (id del sitio 11).



De manera similar, las rutas de VPN 10 y 20 son exportadas por vSmart a la tabla de ruteo VPN 30 al recibir las rutas VPN 10 y 20 desde cE2 (id de sitio 12).



Aquí también se muestra una vista previa de la configuración de la política de control completa para referencia.

```
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 ! !
```

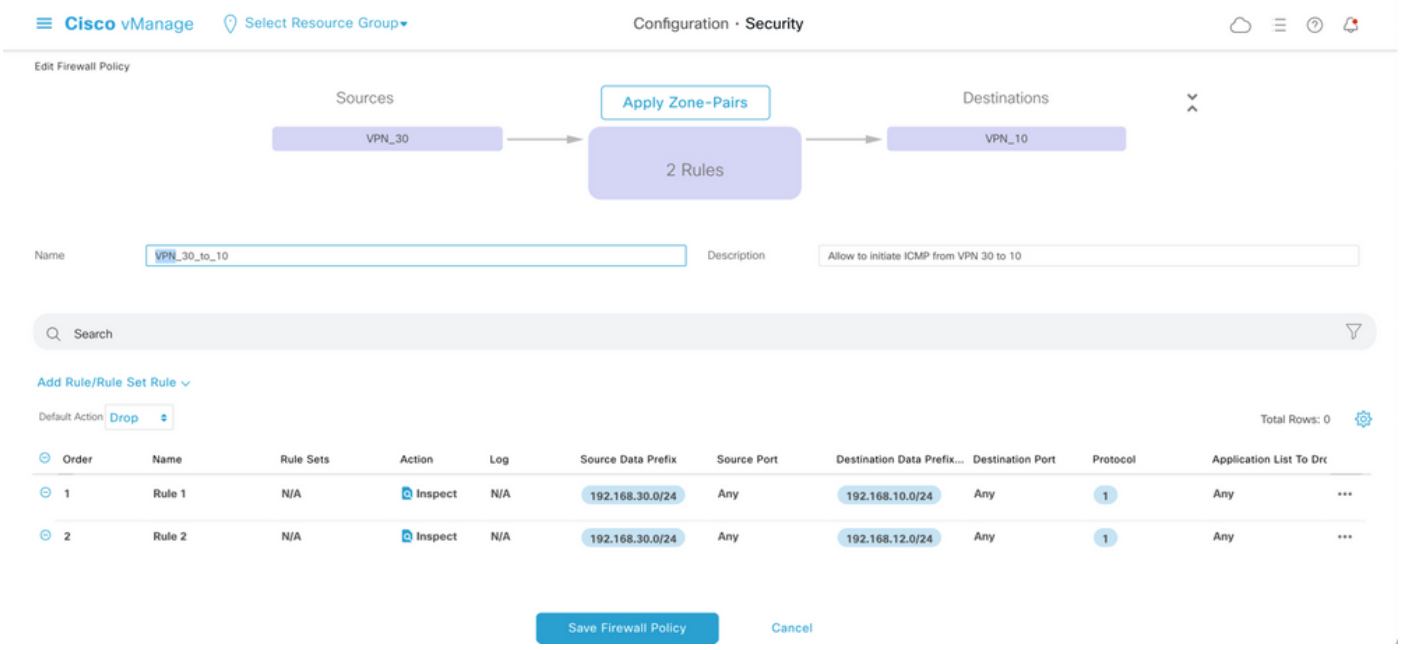
La política se debe activar desde la sección vManage controller **Configuration > Policies** para que sea efectiva en el controlador vSmart.

Configuración de ZBFW

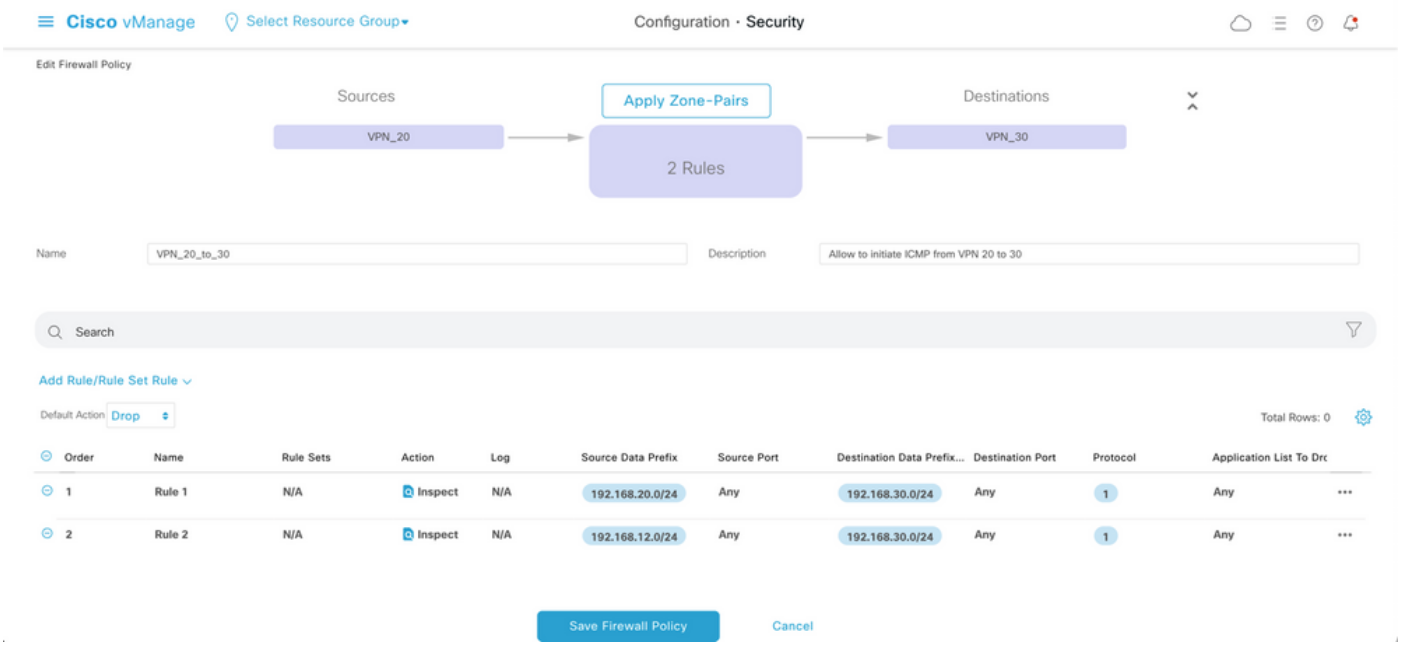
Esta es una tabla que resume ZBFW para filtrar los requisitos con el fin de demostrar en este artículo.

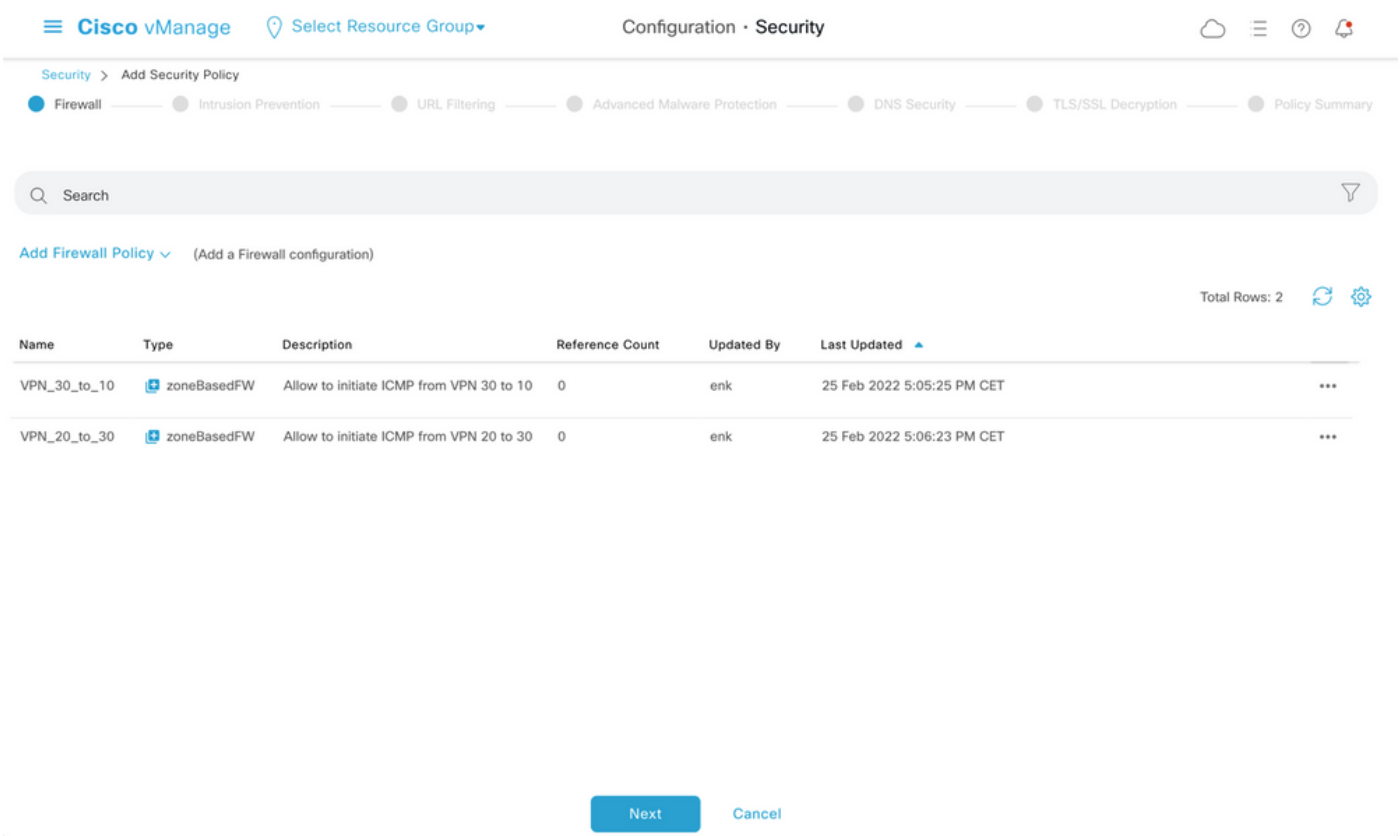
Zona de destino Zona de origen	VPN_10	VPN_20	VPN_30
VPN_10	permitir dentro de la zona	Denegar	Denegar
VPN_20	Denegar	permitir dentro de la zona	Permiso
VPN_30	Permiso	Denegar	permitir dentro de la zona

El objetivo principal es permitir cualquier tráfico de protocolo de mensajes de control de Internet (ICMP) que se originó en el lado de servicio del router cE1 VPN 30 y está destinado a VPN 10 pero no a VPN 20. El tráfico de retorno se debe permitir automáticamente.



También se debe permitir que cualquier tráfico ICMP del router cE2 service-side VPN 20 pase al lado de servicio VPN 30 de cE1, pero no desde VPN 10. El tráfico de retorno de VPN 30 a VPN 20 se debe permitir automáticamente.

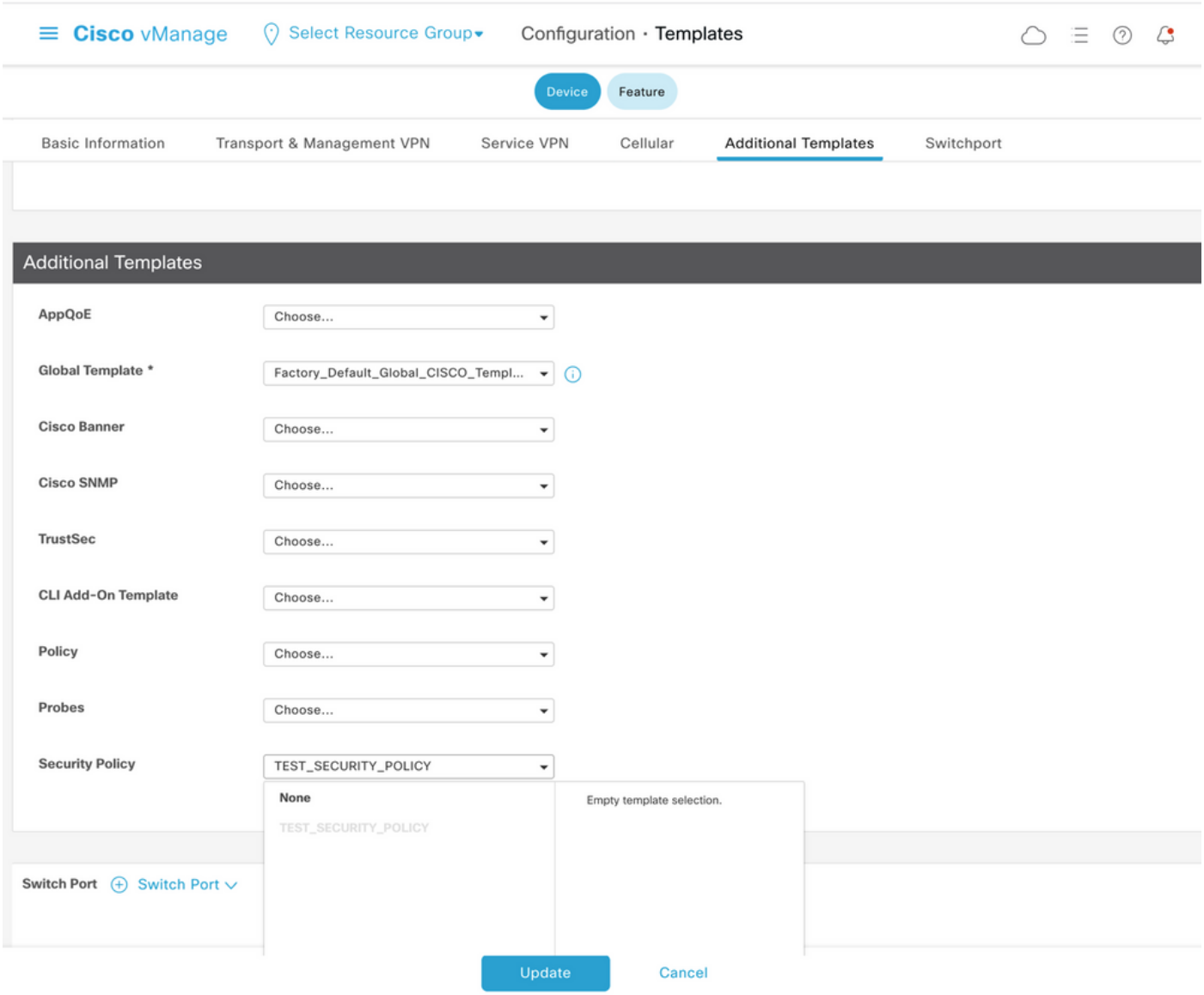




Aquí puede encontrar la vista previa de la política ZBFW como referencia.

```
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 !
```

Para aplicar la directiva de seguridad, se debe asignar en la sección del menú desplegable **Política de seguridad** de la sección **Plantillas adicionales** de la plantilla de dispositivo.



Una vez actualizada la plantilla de dispositivo, la política de seguridad se activa en el dispositivo en el que se aplicó la política de seguridad. Para el propósito de la demostración en este documento, fue suficiente habilitar la política de seguridad solamente en el router cE1.

Verificación

Ahora debe comprobar que se han alcanzado los objetivos de la política de seguridad necesaria (ZBFW).

La prueba con **ping** confirma que el tráfico de la zona VPN 10 a VPN 30 se niega como se esperaba porque no hay ningún par de zonas configurado para el tráfico de VPN 10 a 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)
```

De forma similar, el tráfico de VPN 20 se permite a VPN 30 como se espera en la configuración de la política de seguridad.

```
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
```

El tráfico de VPN 30 a subred 192.168.10.0/24 en la zona VPN 10 se permite como se espera en la configuración de políticas.

```
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
```

Se niega el tráfico de VPN 30 a subred 192.168.20.0/24 en la zona VPN 20 porque no hay ningún par de zonas configurado para este tráfico, lo que se espera.

```
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)
```

Se pueden observar resultados adicionales que pueden interesarle cuando intenta hacer ping a la dirección IP 192.168.12.12 porque puede estar en la zona VPN 10 o VPN 20, y es imposible determinar la VPN de destino desde la perspectiva del router R30 situado en el lado de servicio del router de borde 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)
```

El resultado es el mismo para todos los orígenes en el VRF 30. Esto confirma que no depende de los resultados de la función hash Equal-Cost Multi-Path (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)
```

Según los resultados de la prueba para la IP de destino 192.168.12.12, sólo puede suponer que se encuentra en VPN 20 porque no responde a las solicitudes de eco ICMP y es muy probable que esté bloqueado porque no hay ningún par de zonas configurado para permitir el tráfico de VPN 30 a VPN 20 (como se desea). Si un destino con la misma dirección IP 192.168.12.12 se ubicaría en VPN 10 y se supone que responde a la solicitud de eco ICMP, entonces según la política de seguridad ZBFW para el tráfico ICMP de VPN 30 a VPN 20, se debe permitir el tráfico. Debe confirmar la VPN de destino.

Troubleshoot

Método 1. Para encontrar la VPN de destino de la tabla OMP

Una simple verificación de la tabla de ruteo en cE1 no ayuda a entender la VPN de destino real. La información más útil que puede obtener de la salida es una IP del sistema del destino (169.254.206.12) y también que no hay ECMP que ocurra.

```
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
```

Para averiguar la VPN de destino, primero, es necesario encontrar la etiqueta de servicio de la tabla OMP en cE1 para el prefijo de interés.

```
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 -
```

Podemos ver que el valor de la etiqueta es 1007. Finalmente, se puede encontrar VPN de destino si todos los servicios que se originan desde el router que posee la IP del sistema 169.254.206.12 se verifican en el controlador 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
```

Según la etiqueta VPN 1007, se puede confirmar que la VPN de destino es 20.

Método 2. Para buscar VPN de destino con la ayuda de los comandos de la plataforma

Para averiguar el VPN de destino con la ayuda de los comandos de plataforma, primero debe obtener un VRF ID interno para VPN 30 en el router cE1 con la ayuda de los comandos **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
```

En este caso, el VRF ID 1 se asignó al VRF denominado 30. Los comandos de la plataforma revelan la cadena de objetos Output Chain Element (OCE) en el software SD-WAN que representa la lógica de reenvío interna que determina la ruta del paquete en el 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)
```

El prefijo de interés apunta al objeto de salto siguiente del tipo de clase de acuerdo de nivel de servicio (SLA) (OBJ_SDWAN_NH_SLA_CLASS) con ID 0xf800045f que se puede verificar más a fondo. Aquí se muestra:

```
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
```

Este es un resultado largo, por lo que se omitieron las clases SLA de 2 a 15 porque no hay clases SLA de reserva configuradas y todas ellas apuntan a la misma adyacencia DROP especial que SLA 1. El interés principal es el objeto de salto siguiente de tipo indirecto (SDWAN_NH_INDIRECT) de SLA 0. También podemos notar que no hay ECMP y todos los ID son iguales (0xf800044f). Se puede verificar más a fondo para encontrar la VPN de destino final y la etiqueta de servicio.

```
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
```

Método 3. Para encontrar VPN de destino con la ayuda de la herramienta Packet-Trace

Otra manera de encontrar una VPN de destino es una herramienta **packet-trace** que puede analizar los paquetes reales que se ejecutan a través del router en tiempo real. La condición de depuración se configura para que coincida con el tráfico solamente a/desde la dirección 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
```

A continuación, si el tráfico se inició desde R30 con ayuda de **ping**, puede ver los paquetes coincidentes en cE1 y verificar cada detalle de paquete. En este caso, es el primer número de paquete 0, por ejemplo. Las líneas más importantes se resaltan con **<<<<<** signos.

```
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 que los cinco paquetes de eco ICMP enviados por **ping** se descartaron con el código de descarte 52 (FirewallL4Insp). **Función** de sección**: El reenvío de SDWAN** indica que la VPN de destino es 20 y la etiqueta de servicio 1007 en el encabezado interno del paquete tunelizado se utiliza para reenviar para designar la VPN de destino en cE2. **Función** de sección**: ZBFW** confirma además que los paquetes fueron descartados porque el par de zonas no fue configurado para el tráfico de la VPN de entrada 20 destinada a la zona VPN 30.

Posibles problemas debido al failover

¿Qué sucede si la ruta 192.168.12.0/24 es retirada por R20 o ya no es accesible desde cE2 en el VRF 20? Aunque desde una perspectiva de VRF 30 la subred es la misma, porque la política de seguridad de ZBFW trata el tráfico de la zona VPN 30 a las zonas VPN 20 y 10 de forma diferente, puede producir resultados no deseados como el tráfico permitido, mientras que no debe ser o viceversa.

Por ejemplo, si simula una falla de un link entre los routers cE2 y R20. Esto lleva a la retirada de la ruta 192.168.12.0/24 de la tabla de ruteo VPN 20 en el controlador vSmart y, en su lugar, la ruta VPN 10 se filtra en la tabla de ruteo VPN 30. Se permite la conectividad de VPN 30 a VPN 10 según la política de seguridad aplicada en cE1 (esto se espera desde la perspectiva de la política de seguridad, pero no puede ser deseable para la subred específica presentada en ambas 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 :
```

Observe que se utilizó la etiqueta 1006 en lugar de 1007 y que el ID de VPN de salida es 10 en lugar de 20 ahora. Además, el paquete se permitía según la política de seguridad ZBFW, y se daban los nombres correspondientes de los pares de zonas, el mapa de clase y las políticas.

Hay un problema aún mayor que puede surgir debido al hecho de que la ruta más temprana se mantiene en la tabla de ruteo de VPN 30 y en este caso es la ruta VPN 10 la que después de la aplicación de política de control inicial la ruta VPN 20 se filtró en la tabla VPN 30 OMP en vSmart. Imaginemos el escenario en el que la idea original era exactamente lo contrario de la lógica de la política de seguridad de ZBFW descrita en este artículo. Por ejemplo, el objetivo era permitir el tráfico de VPN 30 a VPN 20 y no a VPN 10. Si se permitió después de una configuración de política inicial, después de la falla o la retirada de la ruta 192.168.12.0/24 de VPN 20, el tráfico permanece bloqueado a la subred 192.168.12.0/24 incluso después de la recuperación porque la ruta 192.168.12.0/24 sigue filtrándose de VPN 10.