Configurar o firewall baseado em zona SD-WAN (ZBFW) e vazamento de rota

Contents

Introduction

Este documento descreve como configurar, verificar e solucionar problemas do Zone-Based Firewall (ZBFW) com o Route-Leaking entre Virtual Private Networks (VPN).

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- A sobreposição SD-WAN da Cisco traz uma configuração inicial
- Configuração de ZBFW a partir da interface de usuário (UI) do vManage
- Configuração da política de controle de vazamento de rota da IU do vManage

Componentes Utilizados

Para os fins da demonstração, estes softwares foram usados:

- Controlador Cisco SD-WAN vSmart com versão de software 20.6.2
- Controlador Cisco SD-WAN vManage com versão de software 20.6.2
- Dois roteadores de plataforma de borda virtual Cisco IOS®-XE Catalyst 8000V com versão de

software 17.6.2 executados no modo de controlador
- Três roteadores de plataforma de borda virtual Cisco IOS-XE Catalyst 8000V com versão de software 17.6.2 executados em modo autônomo

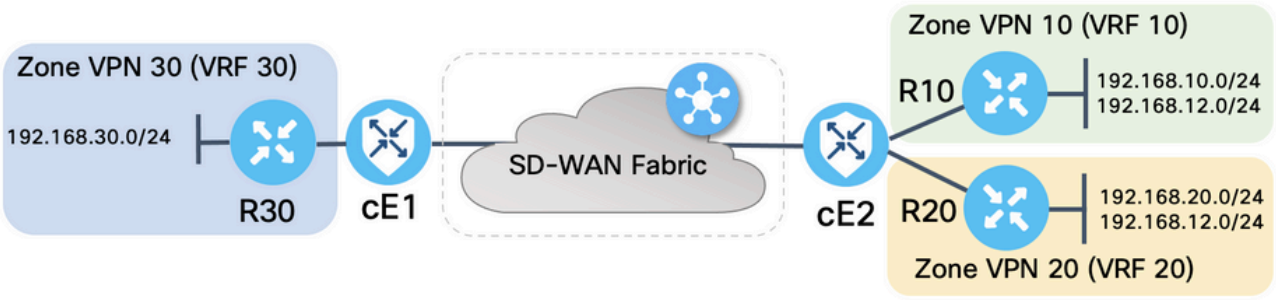
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

Este documento explica como o roteador determina o mapeamento de VPN de destino na sobreposição SD-WAN e como verificar e solucionar problemas de vazamento de rota entre VPNs. Ele também descreve as peculiaridades da seleção de caminho caso a mesma sub-rede seja anunciada de uma VPN diferente e que tipo de problemas podem surgir por causa disso.

Configurar

Diagrama de Rede



Ambos os roteadores SD-WAN foram configurados com parâmetros básicos para estabelecer conexões de controle com controladores SD-WAN e conexões de plano de dados entre eles. Os detalhes dessa configuração estão fora do escopo para o propósito deste documento. A tabela aqui resume as atribuições de VPN, ID do site e Zonas.

	CE1	CE2
ID do site	11	12
VPN	30	10,20
IP do sistema	169.254.206.11	169.254.206.12

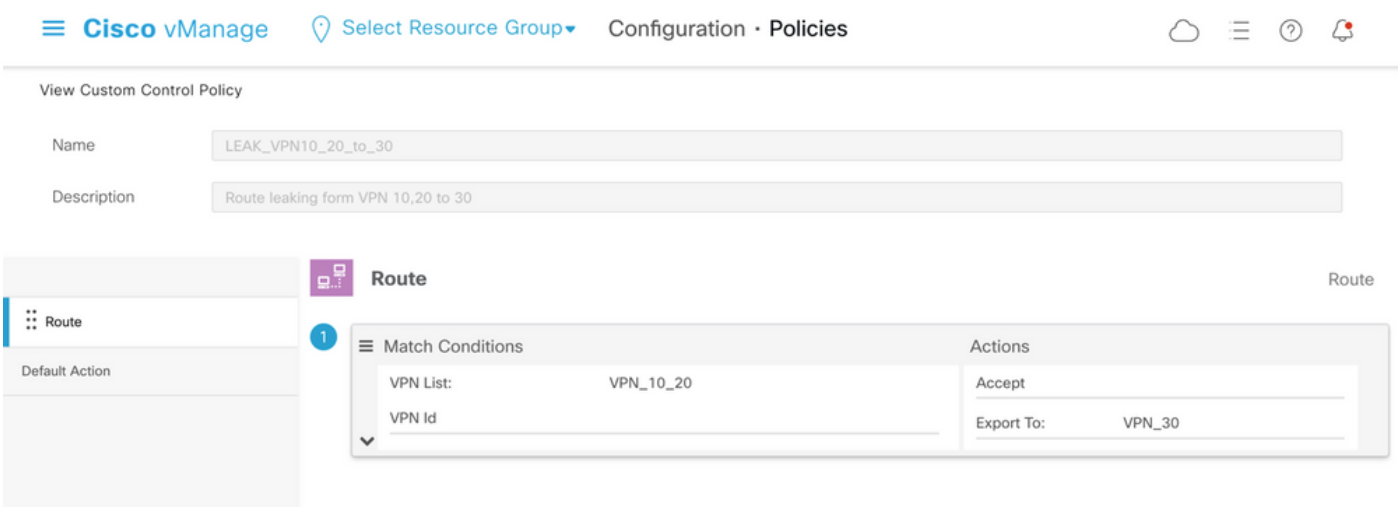
Os roteadores no lado do serviço foram configurados com rotas padrão estáticas em cada Virtual Routing and Forwarding (VRF) que aponta para o roteador SD-WAN correspondente. Da mesma forma, os roteadores SD-WAN Edge foram configurados com rotas estáticas que apontam para as sub-redes que correspondem. Observe que, para a demonstração dos possíveis problemas com vazamento de rota e ZBFW, os roteadores atrás do lado de serviço de cE2 têm a mesma sub-rede 192.168.12.0/24. Em ambos os roteadores atrás de cE2, há uma interface de Loopback configurada para emular um host com o mesmo endereço IP 192.168.12.12.

Éimportante observar que os roteadores Cisco IOS-XE R10, R20 e R30 são executados em modo autônomo nos lados de serviço das rotas de borda SD-WAN, que servem principalmente para emular hosts finais nesta demonstração. As interfaces de loopback em rotas SD-WAN Edge não

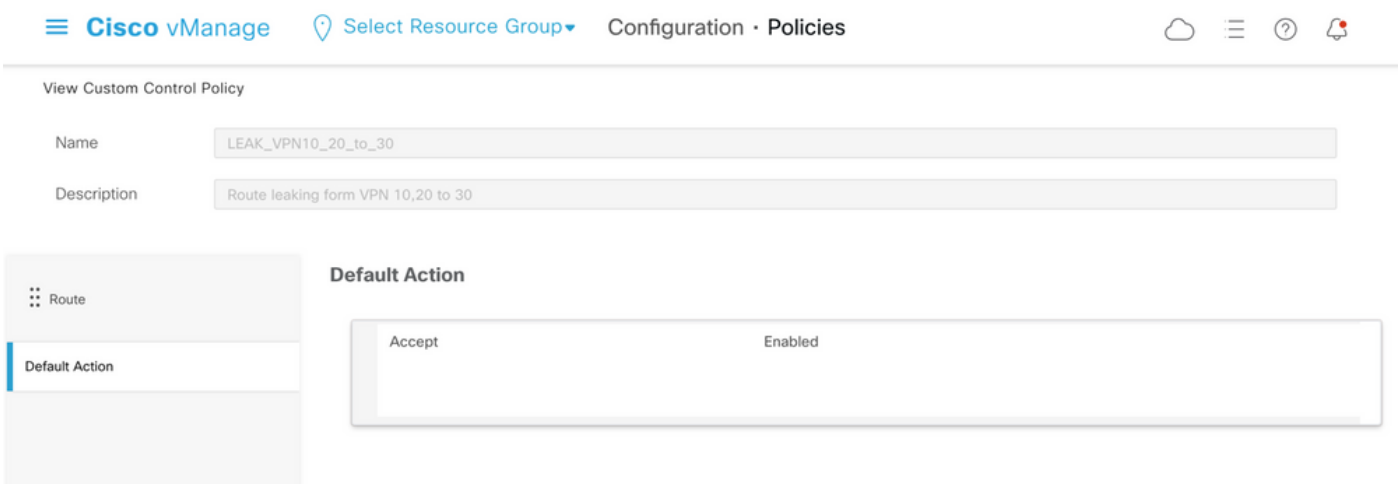
podem ser usadas para essa finalidade, em vez de hosts reais como roteadores de lado de serviço, porque o tráfego que se origina de uma interface em um VRF do roteador SD-WAN Edge não é considerado como tráfego originado na zona ZBFW que corresponde e, em vez disso, pertence à zona de auto especial de um roteador de borda. É por isso que a zona ZBFW não pode ser considerada como VRF. Uma discussão detalhada sobre a autozona está fora do escopo deste artigo.

Configuração de vazamento de rota

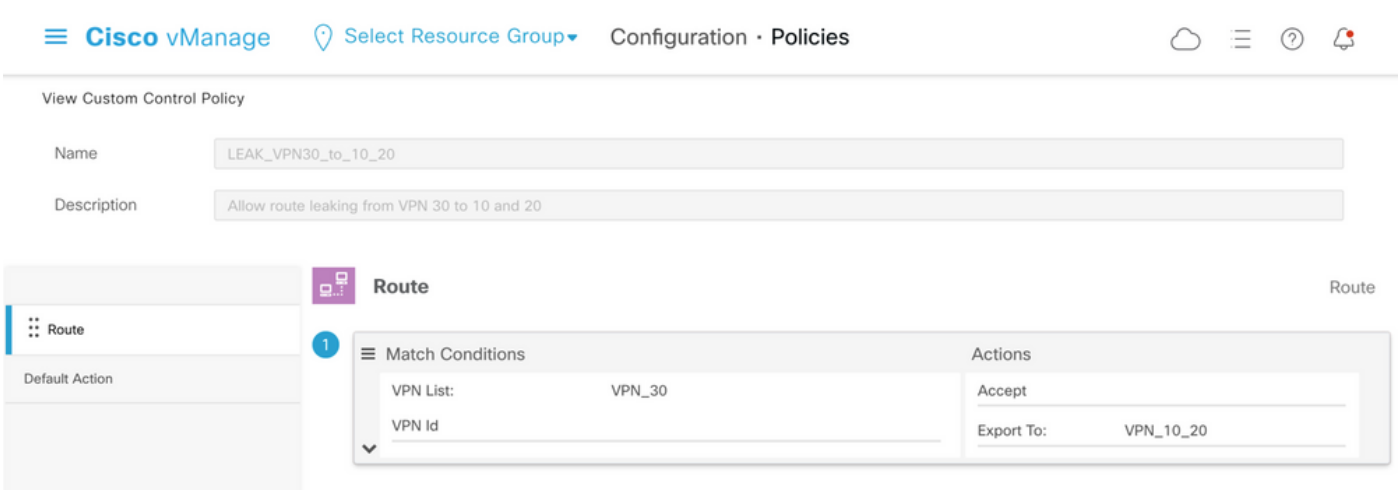
O principal objetivo de configuração da política de controle é permitir o vazamento de rotas de todas as rotas da VPN 10 e 20 para a VPN 30. O VRF 30 existe apenas no roteador cE1 e os VRFs 10 e 20 estão configurados somente no roteador cE2. Para isso, foram configuradas duas políticas de topologia (Controle personalizado). Aqui está a topologia para exportar todas as rotas da VPN 10 e 20 para a VPN 30.

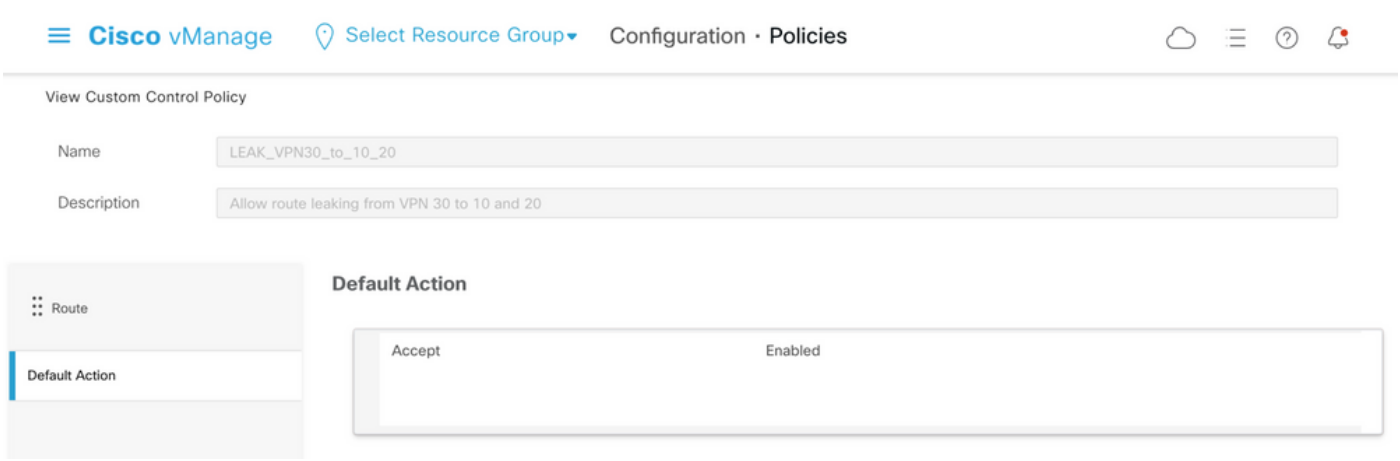


Observe que a Ação padrão está definida como **Permitir,** para evitar o bloqueio de anúncios de TLOC ou anúncios de rotas intrVPN normais acidentalmente.

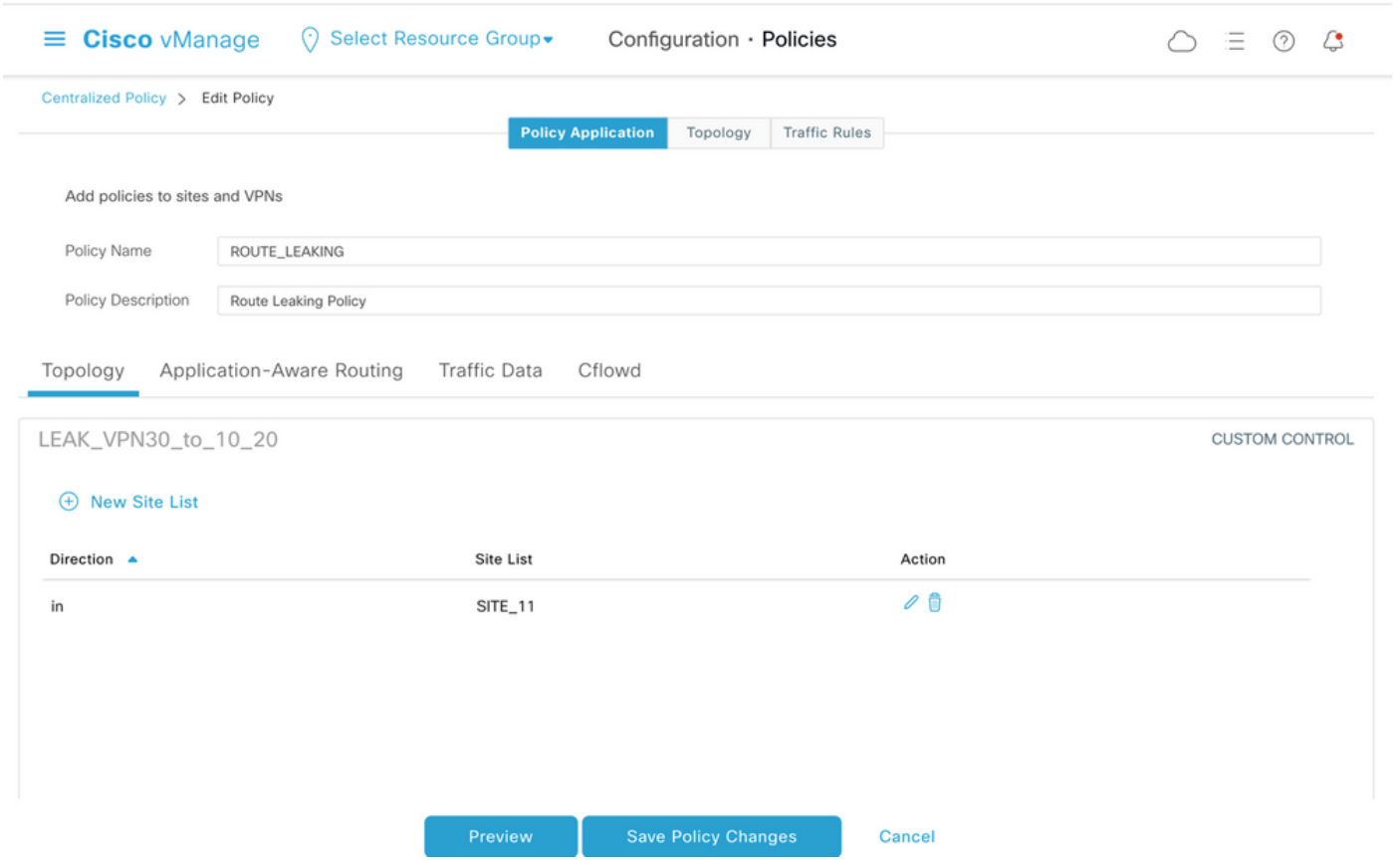


Da mesma forma, a política de topologia foi configurada para permitir o anúncio reverso de informações de roteamento da VPN 30 para a VPN 10 e 20.

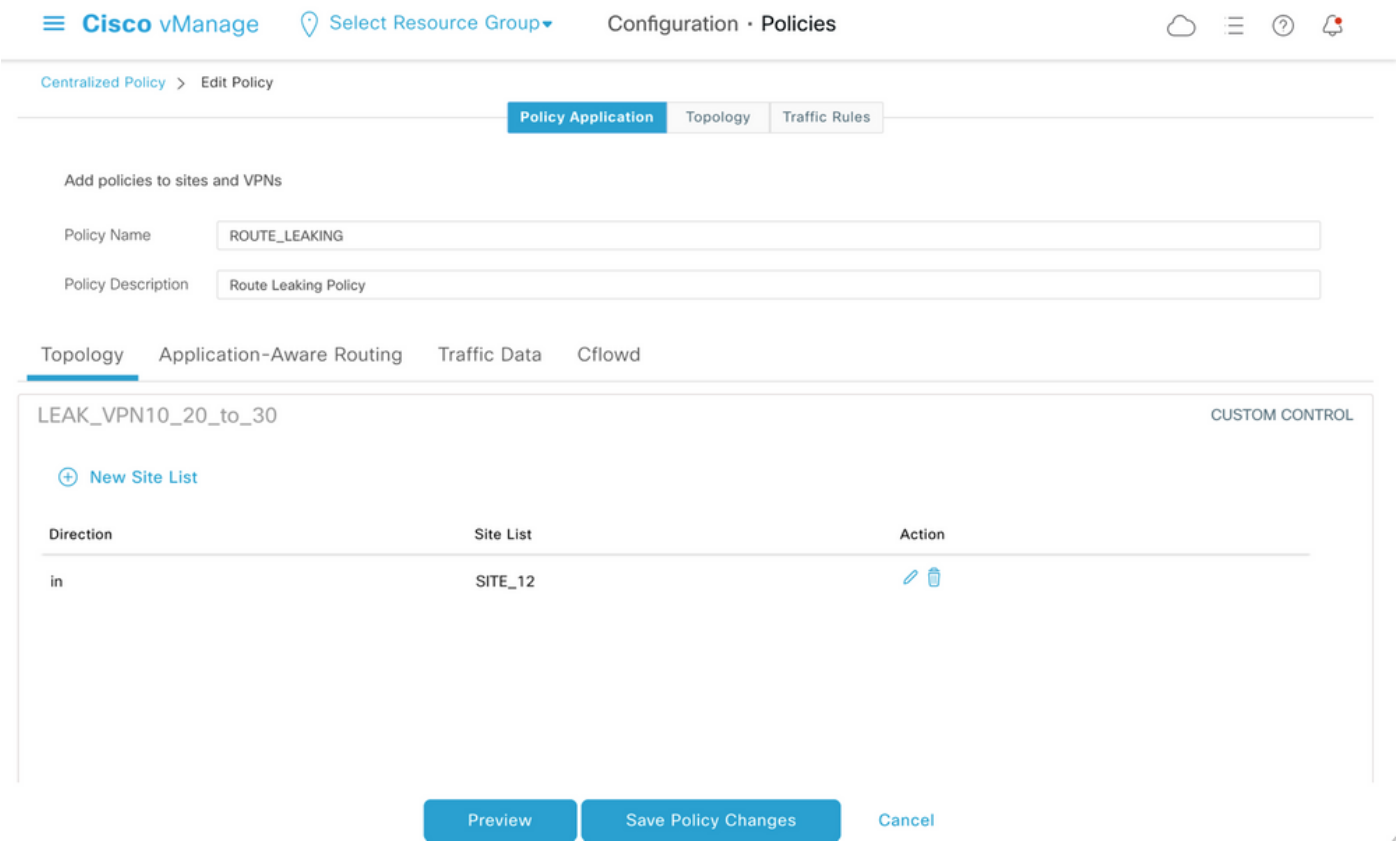




Em seguida, ambas as políticas de topologia são atribuídas às listas de sites que correspondem, na direção de entrada. As rotas da VPN 30 são exportadas pelo controlador vSmart para as tabelas do Protocolo de Gerenciamento de Sobreposição (OMP - Overlay Management Protocol) da VPN 10 e 20 quando recebidas do cE1 (site-id 11).



Da mesma forma, as rotas da VPN 10 e 20 são exportadas pelo vSmart para a tabela de roteamento da VPN 30 ao receberem as rotas VPN 10 e 20 do cE2 (id do site 12).



Aqui também está uma visualização completa da configuração da política de controle para referência.

```
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 ! !
```

A política deve ser ativada na **seção** vManage controller **Configuration > Policies** para ser efetiva no controlador vSmart.

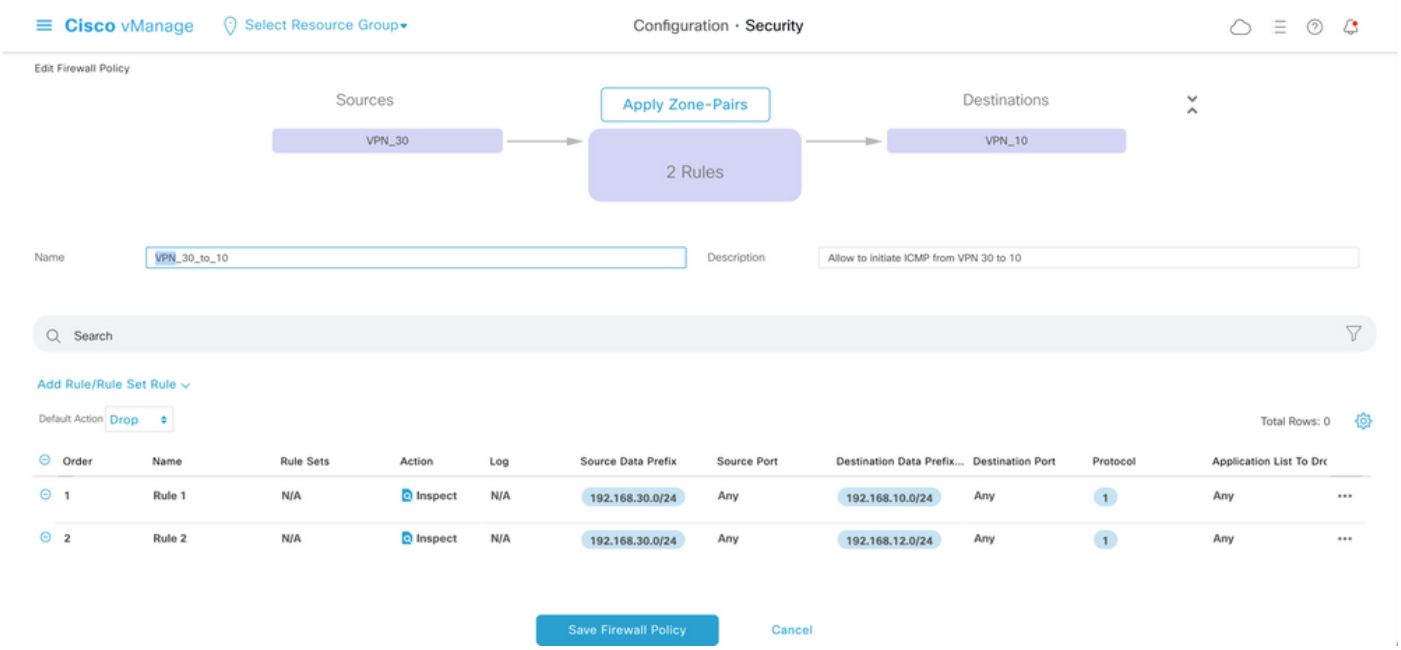
Configuração do ZBFW

Esta é uma tabela que resume o ZBFW para filtrar os requisitos para fins de demonstração neste artigo.

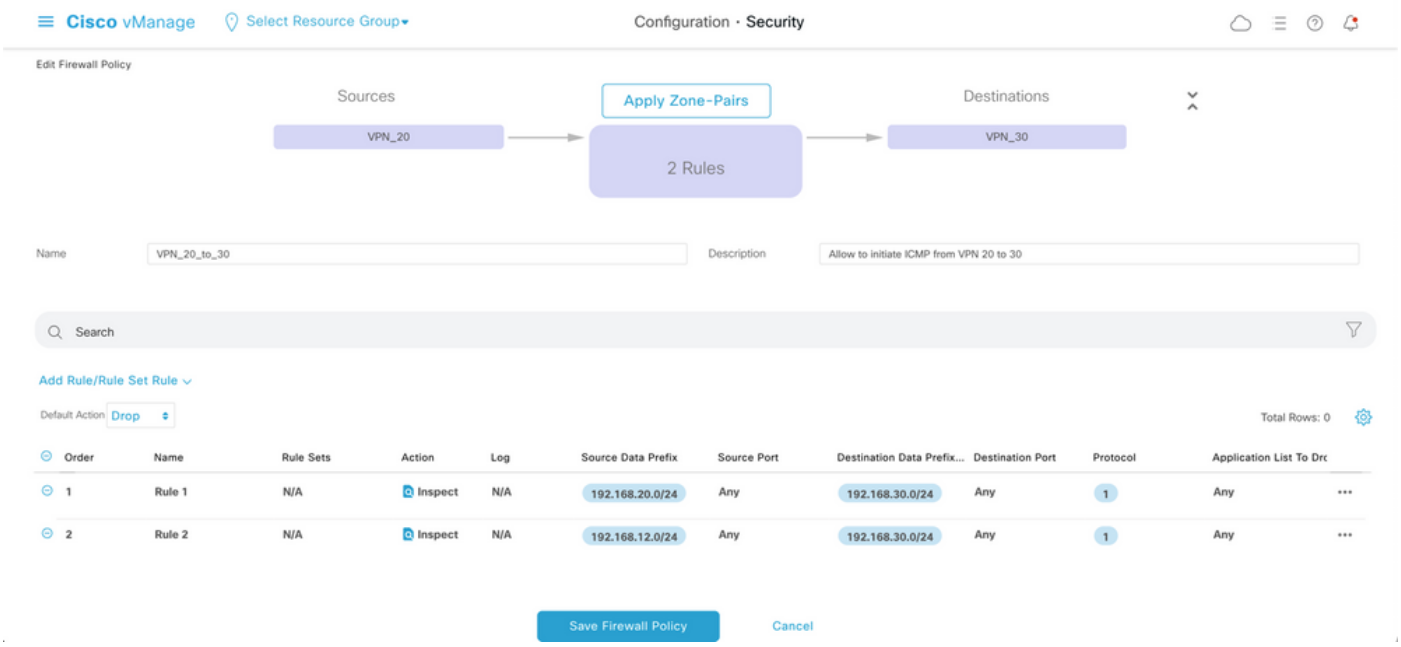
Zona de destino Zona de origem	VPN_10	VPN_20	VPN_30
VPN_10	intra-zone allow	Negar	Negar
VPN_20	Negar	intra-zone allow	Permissão
VPN_30	Permissão	Negar	intra-zone allow

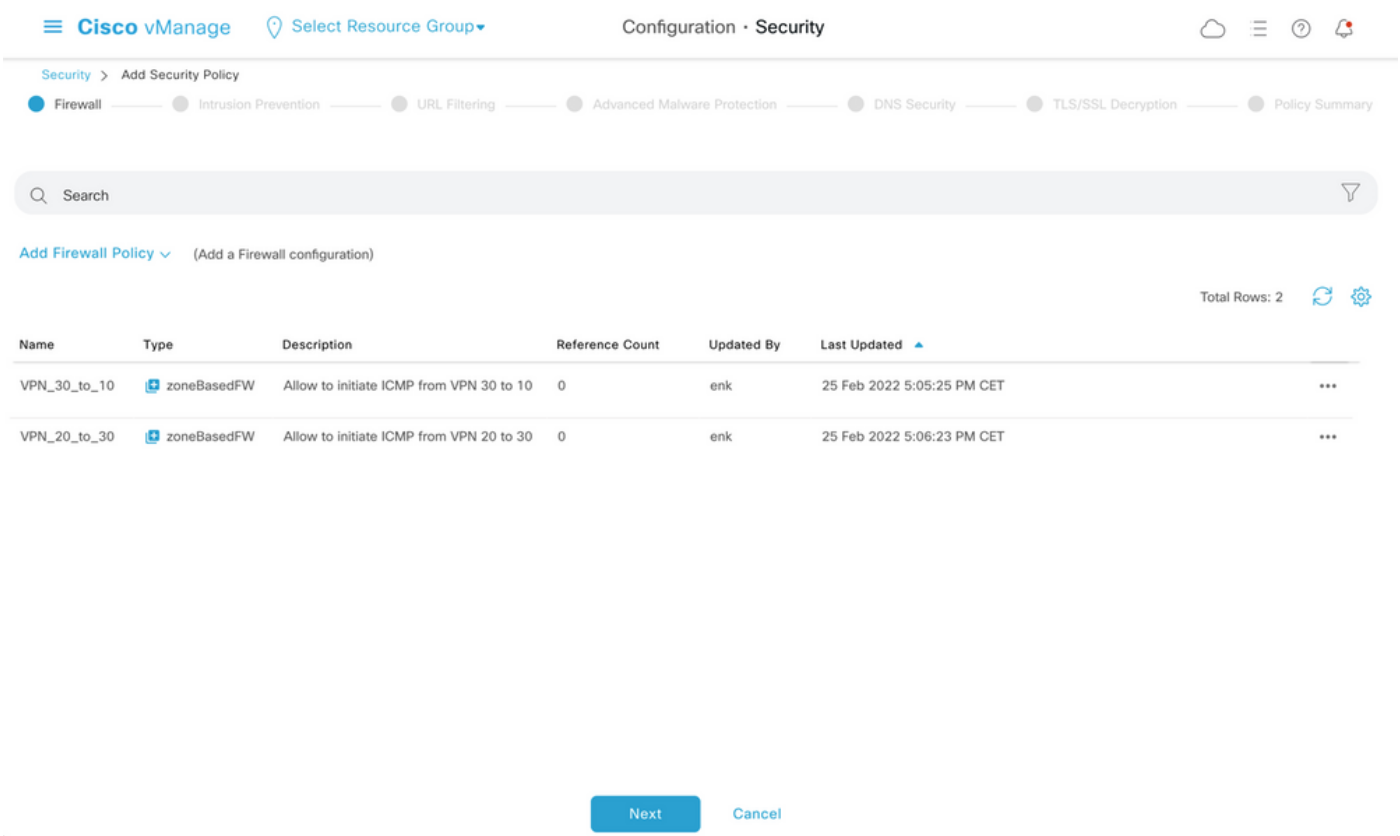
O principal objetivo é permitir qualquer tráfego ICMP (Internet Control Message Protocol)

originado do lado do serviço do roteador cE1 VPN 30 e destinado à VPN 10, mas não à VPN 20. O tráfego de retorno deve ser permitido automaticamente.



Além disso, qualquer tráfego ICMP do roteador cE2 VPN 20 do lado do serviço deve ter permissão para transitar para o lado do serviço VPN 30 do cE1, mas não do VPN 10. O tráfego de retorno da VPN 30 para a VPN 20 deve ser permitido automaticamente.

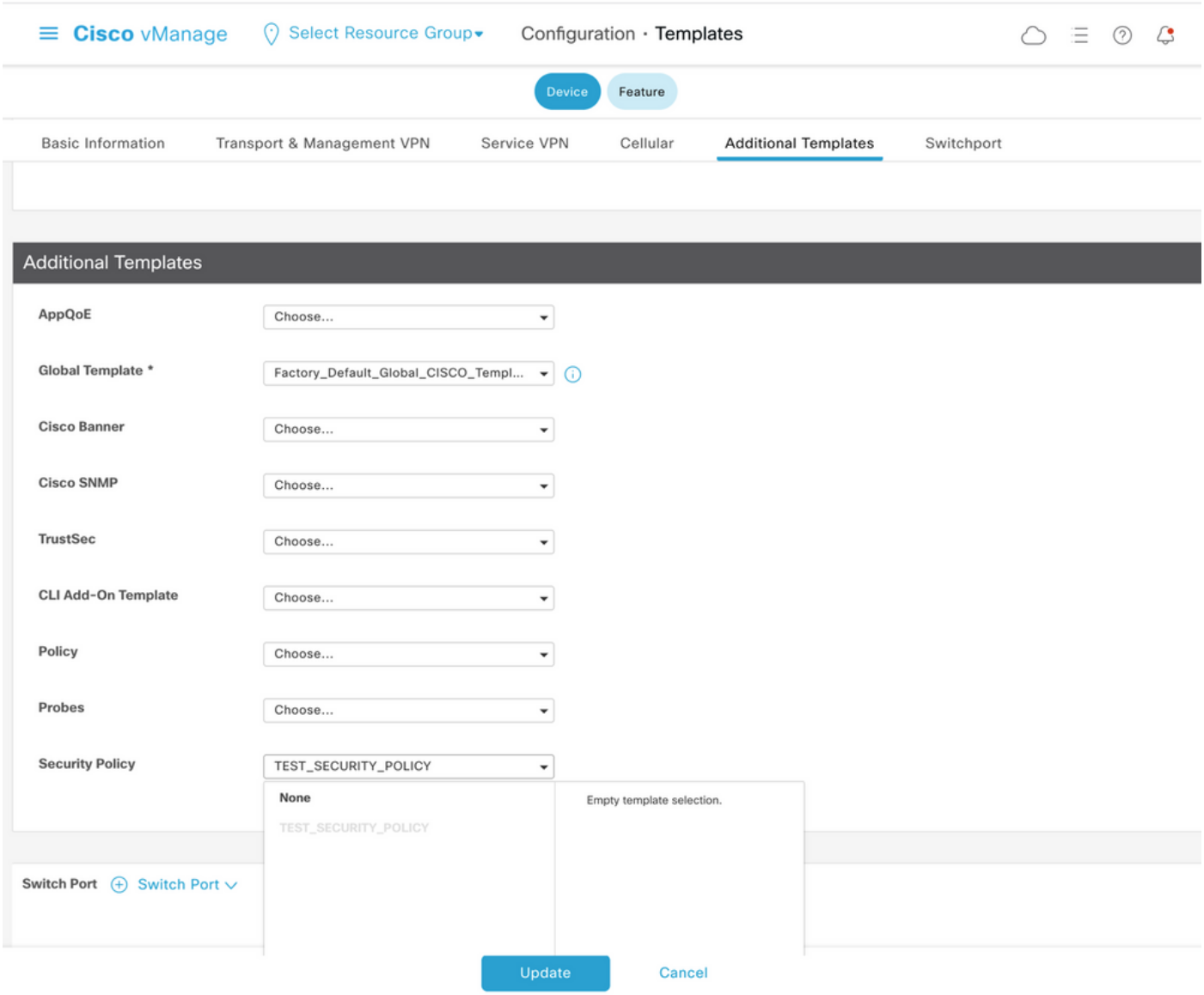




Aqui, você pode encontrar a visualização da política ZBFW para referência.

```
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 a política de segurança, ela deve ser atribuída na seção do menu suspenso **Política de segurança** da seção **Modelos adicionais** do modelo de dispositivo.



Quando o modelo do dispositivo é atualizado, a política de segurança torna-se ativa no dispositivo em que a política de segurança foi aplicada. Para a demonstração neste documento, foi suficiente habilitar a política de segurança somente no roteador cE1.

Verificar

Agora você precisa verificar se os objetivos da política de segurança (ZBFW) foram alcançados.

O teste com **ping** confirma que o tráfego da zona VPN 10 para VPN 30 é negado como esperado porque não há nenhum par de zonas configurado para o tráfego da VPN 10 para 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)
```

Da mesma forma, o tráfego da VPN 20 é permitido para a VPN 30 conforme esperado pela configuração da política de segurança.

```
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
```

O tráfego da VPN 30 para a sub-rede 192.168.10.0/24 na zona VPN 10 é permitido conforme esperado pela configuração de política.

```
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
```

O tráfego da VPN 30 para a sub-rede 192.168.20.0/24 na zona VPN 20 é negado porque não há nenhum par de zonas configurado para esse tráfego, o que é esperado.

```
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)
```

Resultados adicionais que podem interessar a você podem ser observados quando você tenta fazer ping no endereço IP 192.168.12.12 porque ele pode estar na zona VPN 10 ou VPN 20, e é impossível determinar a VPN de destino da perspectiva do roteador R30 situado no lado de serviço do roteador de borda 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)
```

O resultado é o mesmo para todas as fontes no VRF 30. Isso confirma que ele não depende dos resultados da função de hash de multi-caminho de custo igual (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)
```

Com base nos resultados do teste para o IP de destino 192.168.12.12, você pode apenas adivinhar que ele se localiza na VPN 20 porque não responde às solicitações de eco ICMP e é mais provavelmente bloqueado porque não há par de zonas configurado para permitir o tráfego da VPN 30 para a VPN 20 (conforme desejado). Se um destino com o mesmo endereço IP 192.168.12.12 estiver localizado na VPN 10 e supostamente responder à solicitação de eco ICMP, de acordo com a política de segurança ZBFW para tráfego ICMP da VPN 30 para a VPN 20, o tráfego deverá ser permitido. Você deve confirmar a VPN de destino.

Troubleshoot

Método 1. Para localizar a VPN de destino na tabela OMP

Uma simples verificação da tabela de roteamento em cE1 não ajuda a entender a VPN de destino real. A informação mais útil que você pode obter da saída é um system-IP do destino (169.254.206.12) e também que não há ECMP que aconteça.

```
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 descobrir a VPN de destino, primeiro, é necessário descobrir a etiqueta de serviço da tabela OMP em cE1 para o prefixo de 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 -
```

Podemos ver que o valor do rótulo é 1007. Finalmente, a VPN de destino pode ser encontrada se todos os serviços originados do roteador que possui o sistema IP 169.254.206.12 forem verificados no 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
```

Com base no rótulo de VPN 1007, pode-se confirmar que a VPN de destino é 20.

Método 2. Para localizar a VPN de destino com a ajuda dos comandos da plataforma

Para descobrir a VPN de destino com a ajuda dos comandos da plataforma, primeiro, você precisa obter um ID de VRF interno para VPN 30 no roteador cE1 com a ajuda dos comandos **show ip vrf detail 30** ou **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
```

Nesse caso, a ID 1 do VRF foi atribuída ao VRF com o nome 30. Os comandos da plataforma revelam a cadeia de objetos do Output Chain Element (OCE) no software SD-WAN que representam a lógica de encaminhamento interno que determina o caminho do pacote no 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)
```

O prefixo de pontos de interesse para o tipo de classe do objeto do Contrato de Nível de Serviço (SLA - Service Level Agreement) do próximo salto (OBJ_SDWAN_NH_SLA_CLASS) com ID 0xf800045f que pode ser verificado posteriormente é mostrado aqui:

```
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
```

Essa é uma saída longa, portanto as classes de SLA de 2 a 15 foram ignoradas porque não há classes de SLA de retorno configuradas e todas apontam para a mesma adjacência de DROP especial que o SLA 1. O principal interesse é o objeto do próximo salto do tipo indireto (SDWAN_NH_INDIRECT) do SLA 0. Também podemos observar que não há ECMP e todas as IDs são iguais (0xf800044f). Pode ser verificado ainda mais para encontrar a VPN de destino final e o rótulo de serviço.

```
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 localizar a VPN de destino com a ajuda da ferramenta Packet-Trace

Outra maneira de encontrar uma VPN de destino é uma ferramenta **de rastreamento de pacotes** que pode analisar pacotes reais que são executados pelo roteador em tempo real. A condição de depuração é definida para corresponder o tráfego somente de/para o endereço 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
```

Em seguida, se o tráfego foi iniciado do R30 com a ajuda do **ping**, você poderá ver os pacotes correspondentes no cE1 e verificar cada detalhe do pacote. Nesse caso, é o primeiro pacote número 0, por exemplo. As linhas mais importantes são destacadas com **<<<<<** sinais.

```
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 :
```

Um **rastreamento de pacote** informa que todos os cinco pacotes de eco ICMP enviados pelo **ping** foram descartados com o código de descarte 52 (FirewallL4Insp). **Recurso** da seção**: O SDWAN Forwarding** informa que a VPN de destino é 20 e o rótulo de serviço 1007 no cabeçalho interno do pacote encapsulado é usado para encaminhar a VPN de destino em cE2. **Recurso** da seção**: O ZBFW** confirma ainda que os pacotes foram descartados porque o par de zonas não foi configurado para tráfego da entrada VPN 20 destinado à zona VPN 30.

Possíveis problemas devido ao failover

O que acontece se a rota 192.168.12.0/24 for retirada pelo R20 ou não estiver mais acessível do cE2 no VRF 20? Embora da perspectiva do VRF 30 a sub-rede seja a mesma, porque a política de segurança ZBFW trata o tráfego da zona VPN 30 para as zonas VPN 20 e 10 de forma diferente, ela pode levar a resultados indesejados, como o tráfego permitido, enquanto não deve ser ou vice-versa.

Por exemplo, se você simular uma falha de um link entre os roteadores cE2 e R20. Isso leva à retirada da rota 192.168.12.0/24 da tabela de roteamento VPN 20 no controlador vSmart e, em vez disso, a rota VPN 10 vaza na tabela de roteamento VPN 30. A conectividade da VPN 30 para a VPN 10 é permitida de acordo com a política de segurança aplicada em cE1 (isso é esperado da perspectiva da política de segurança, mas não pode ser desejável para a sub-rede específica apresentada em ambas as VPNs).

```
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 o rótulo 1006 foi usado em vez de 1007 e o ID da VPN de saída é 10 em vez de 20 agora. Além disso, o pacote era permitido de acordo com a política de segurança ZBFW, e os correspondentes pares de zona, mapa de classe e nomes de política foram fornecidos.

Há um problema ainda maior que pode surgir devido ao fato de que a rota mais antiga é mantida na tabela de roteamento do VPN 30 e, nesse caso, é a rota VPN 10 que após a rota VPN 20 do aplicativo de controle inicial foi vazada na tabela VPN 30 OMP no vSmart. Imagine o cenário em que a ideia original era exatamente o oposto da lógica da política de segurança ZBFW descrita neste artigo. Por exemplo, o objetivo era permitir o tráfego da VPN 30 para a VPN 20 e não para a VPN 10. Se ele foi permitido após uma configuração de política inicial, depois da falha ou retirada da rota 192.168.12.0/24 da VPN 20, o tráfego permanece bloqueado para a sub-rede 192.168.12.0/24 mesmo após a recuperação porque a rota 192.168.12.0/24 ainda vaza da VPN 10.