Configurar vazamento de rota para encadeamento de serviço em SD-WAN

Contents

Introdução

Este documento descreve como configurar e verificar o encadeamento de serviços para inspecionar o tráfego em diferentes VRF.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Rede de longa distância definida por software da Cisco (SD-WAN)
- Políticas de controle.
- Modelos.

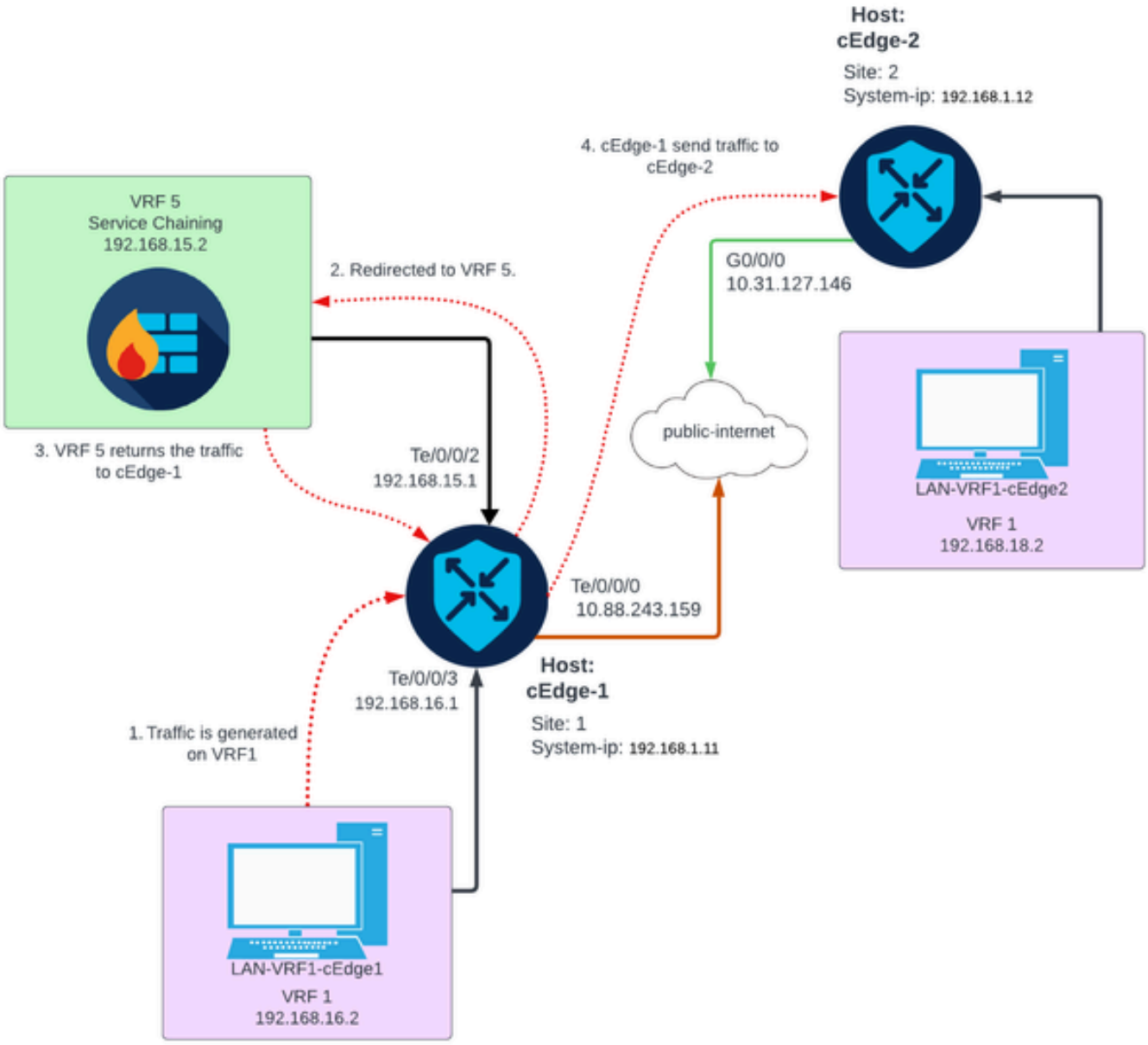
Componentes Utilizados

Este documento é baseado nestas versões de software e hardware:

- Controladores SD-WAN (20.9.4.1)
- Roteador Cisco Edge (17.09.04)

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Diagrama de Rede



Informações de Apoio

No diagrama da rede, o serviço de firewall está no Virtual Routing and Forwarding (VRF) 5,

enquanto os dispositivos de LAN estão localizados no VRF 1. As informações de rotas devem ser compartilhadas entre VRFs para que o encaminhamento e a inspeção do tráfego possam ser realizados. Para rotear o tráfego por meio de um serviço, é necessário configurar uma política de controle no controlador Cisco SD-WAN.

Configurar

Vazamento de rota

O vazamento de rota permite a propagação de informações de roteamento entre VRFs diferentes. Neste cenário, quando o Service Chaining (Firewall) e o LAN Service estão em VRFs diferentes, o vazamento de rota é necessário para a inspeção de tráfego.

Para garantir o roteamento entre o lado do serviço de LAN e o serviço de firewall, o vazamento de rotas é necessário em ambos os VRFs e aplica uma política nos locais onde o vazamento de rota é necessário.

Configuração via CLI

1. Configure as Listas no Controlador Cisco Catalyst SD-WAN.

A configuração permite que os sites sejam identificados por meio de uma lista.

```
<#root>
vSmart#
config
vSmart(config)#
 policy

vSmart(config-policy)#
lists

vSmart(config-lists)#
site-list cEdges-1

vSmart(config-site-list-cEdge-1)#
site-id 1

vSmart(config-site-list-cEdge-1)# exit
vSmart(config-lists)#
site-list cEdge-2

vSmart(config-site-list- cEdge-2)#
```

```
site-id 2


vSmart(config-site-list- cEdge-2)# exit
vSmart(config-site-list)#
vpn-list VRF-1


vSmart(config-vpn-list-VRF-1)#
vpn 1


vSmart(config-vpn-list-VRF-1)# exit
vSmart(config-site-list)#
vpn-list VRF-5


vSmart(config-vpn-list-VRF-5)#
 vpn 5
vSmart(config-vpn-list-VRF-5)#
 commit
```

2. Configure a Política no Controlador Cisco Catalyst SD-WAN.

A configuração permite a propagação de informações de roteamento entre o VRF 1 e o VRF 5, para garantir o roteamento entre eles, ambos os VRF devem compartilhar seus dados de roteamento.

A política permite que o tráfego de VRF 1 seja aceito e exportado para o VRF 5 e vice-versa.

```
<#root>
vSmart#
config


vSmart(config)#
 policy


vSmart(config-policy)#
control-policy Route-Leaking


vSmart(config-control-policy-Route-Leaking)#
sequence 1


vSmart(config-sequence-1)#
match route
```

```
vSmart(config-match-route)#
vpn 5

vSmart(config-match-route)# exit
vSmart(config-sequence-1)#
action accept

vSmart(config-action)#
export-to

vSmart(config-export-to)#
vpn-list VRF-1
vSmart(config-action)# exit


vSmart(config-sequence-1)# exit
vSmart(config-control-policy-Route-Leaking)#
sequence 10

vSmart(config-sequence-10)#
match route

vSmart(config-match-route)#
vpn 1

vSmart(config-match-route)# exit
vSmart(config-sequence-10)#
action accept

vSmart(config-action)#
export-to

vSmart(config-export-to)#
vpn-list VRF-5
vSmart(config-action)# exit


vSmart(config-sequence-10)# exit
vSmart(config-control-policy-Route-Leaking)#
default-action accept
vSmart(config-control-policy-Route-Leaking)#
commit
```

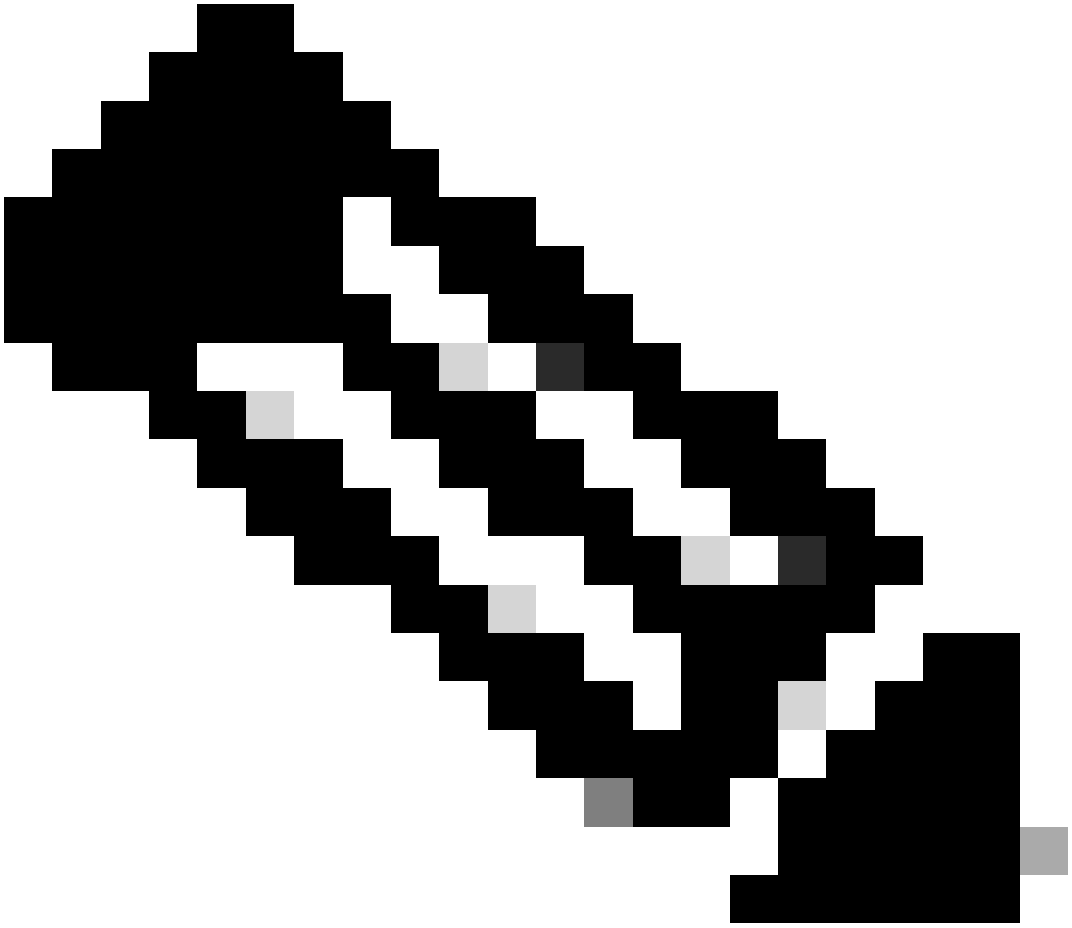
3. Aplique a Política no Controlador Cisco Catalyst SD-WAN.

A política é aplicada nos locais 1 e 2 para permitir o roteamento entre o VRF 1 situado nesses locais e no VRF 5.

A política é implementada na entrada, o que significa que ela é aplicada às atualizações OMP vindas dos Cisco Edge Routers para o Cisco Catalyst SD-WAN Controller.

```
<#root>
vSmart#
config

vSmart(config)#
apply-policy

vSmart(config-apply-policy)#
site-list cEdge-1
vSmart(config-site-list-cEdge-1)#
 control-policy Route-Leaking in

vSmart(config-site-list-cEdge-1)# exit

vSmart(config-apply-policy)#
site-list cEdge-2
vSmart(config-site-list-cEdge-2)#
 control-policy Route-Leaking in
vSmart(config-site-list-cEdge-2)#
 commit
```

Configuração via modelo

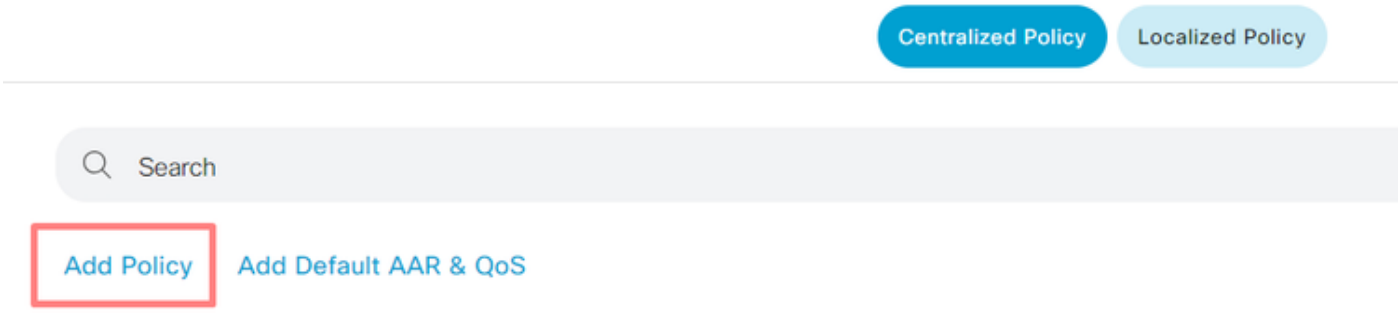


Observação: para ativar a política por meio da Interface Gráfica de Usuário (GUI) do Cisco Catalyst SD-WAN Manager, o Controlador Cisco Catalyst SD-WAN deve ter um modelo anexado.

1. Crie a política para permitir a propagação de informações de roteamento.

Crie uma política no Cisco Catalyst SD-WAN Manager, navegue paraConfiguration> Policies >Centralized Policy.

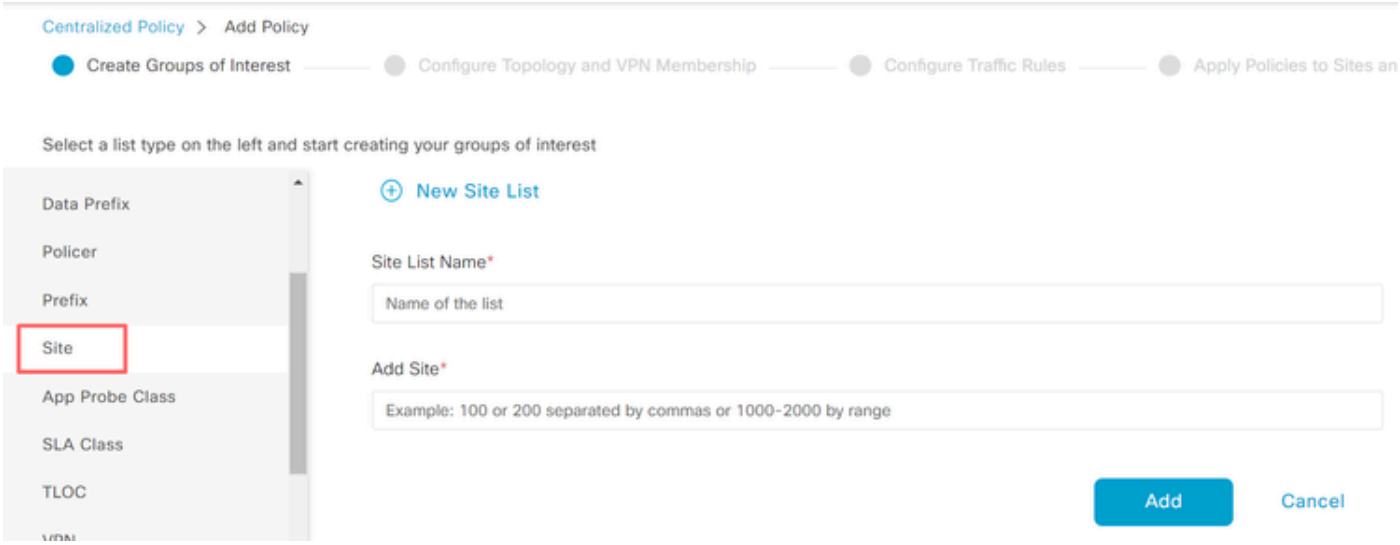
Na guia Centralized Policy, clique em Add Policy.



2. Crie listas no Cisco Catalyst SD-WAN Manager; a configuração permite que os sites sejam identificados através de uma lista.

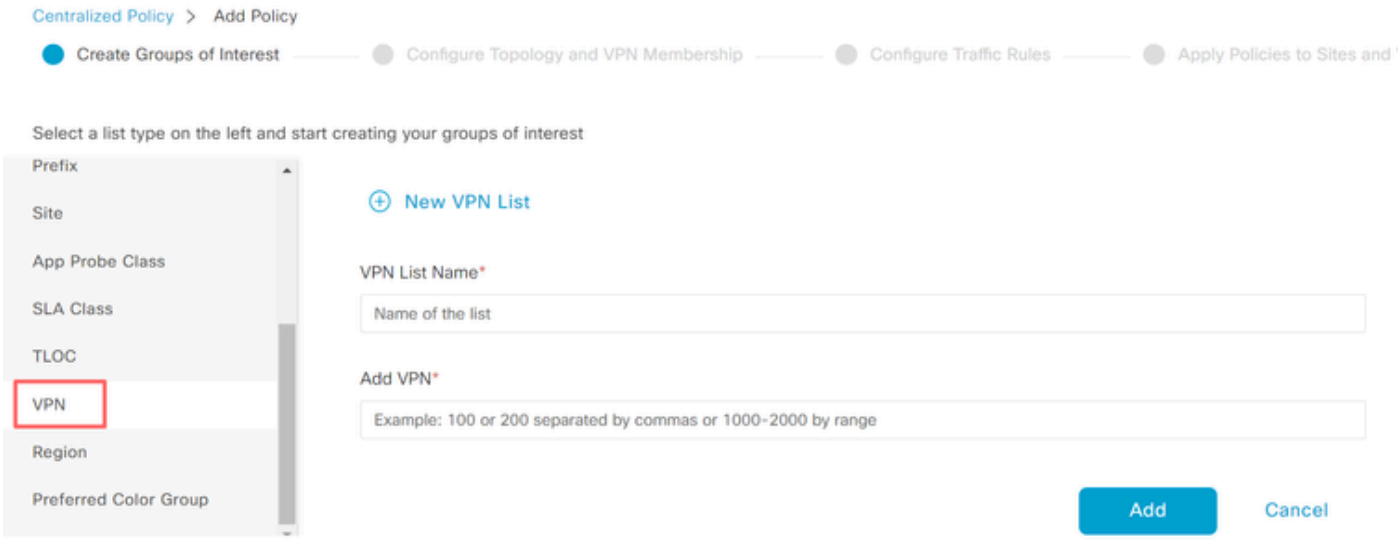
Navegue até Site > Nova lista de sites.

Crie a lista de sites onde o vazamento de rota é necessário e Adicione a lista.



Navegue para VPN > Nova lista de VPN.

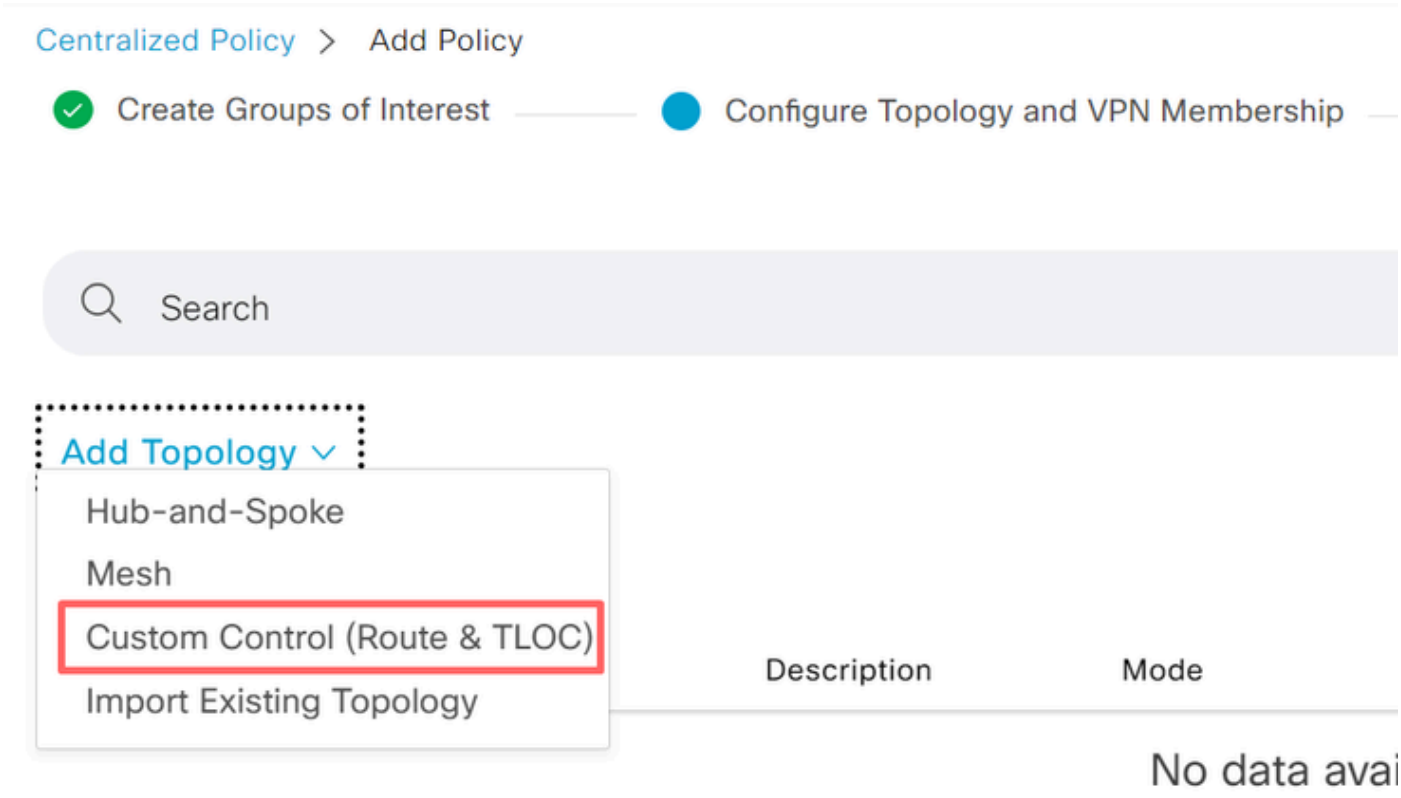
Crie a lista de VPN onde o vazamento de rota precisa ser aplicado, clique em Next.



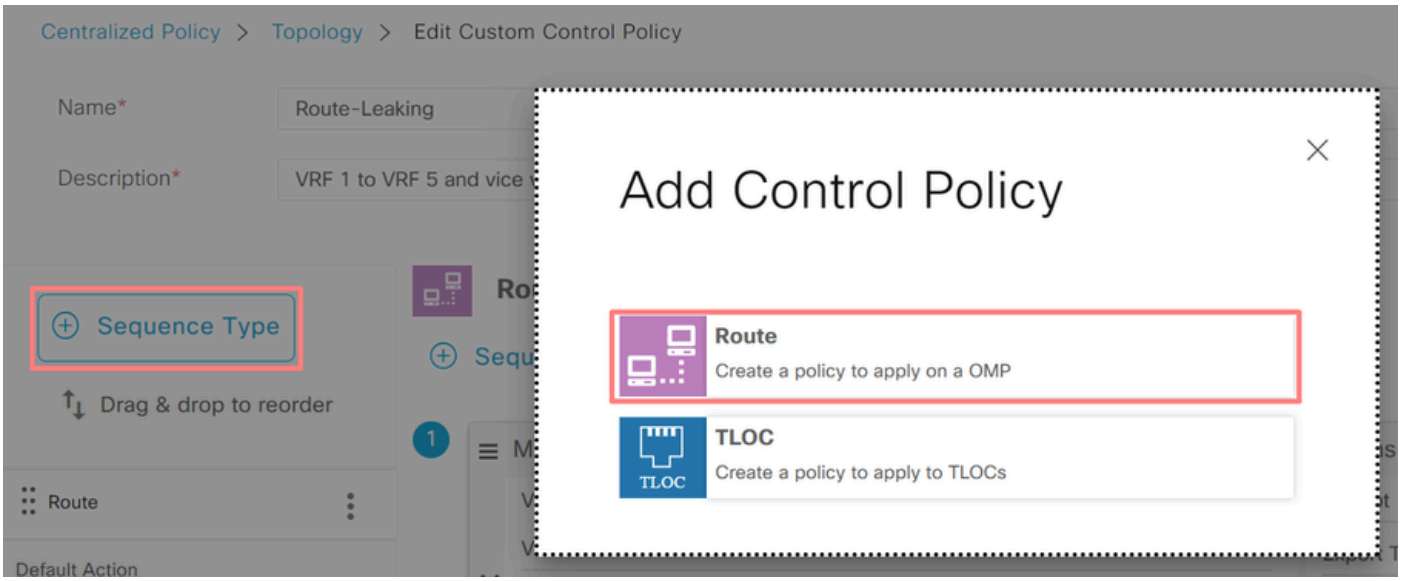
3. Configure a Política no Cisco Catalyst SD-WAN Manager.

Clique na guia Topologia e clique em Adicionar Topologia.

Crie um Controle Personalizado (Rota e TLOC).

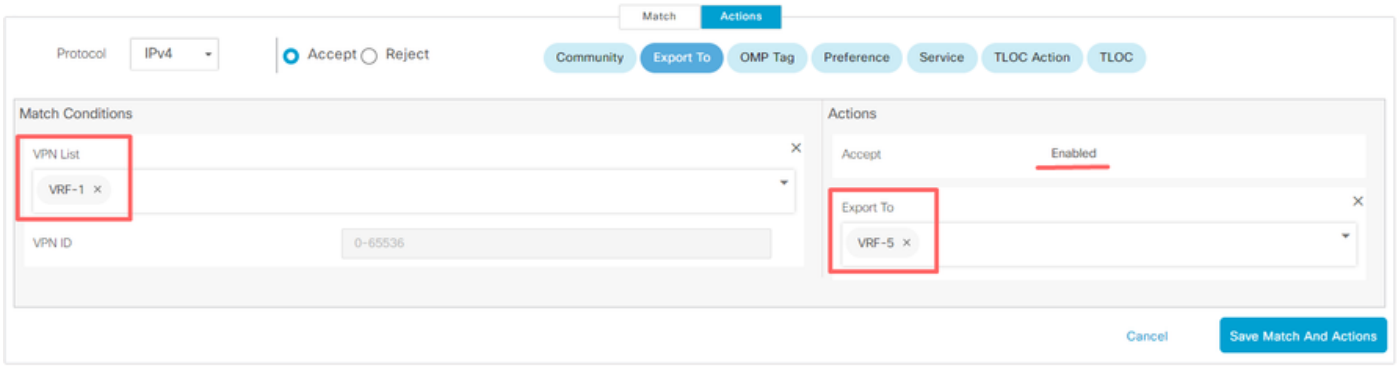


Clique em Sequence Type e selecione Route sequence.

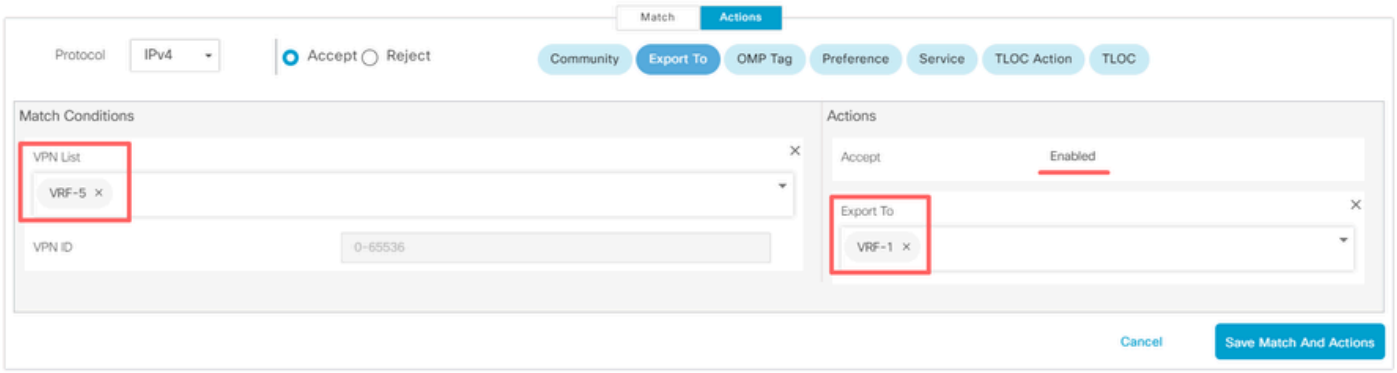


Adicione uma Regra de Sequência.

Condição 1: o tráfego do VRF 1 é aceito e exportado para o VRF 5.

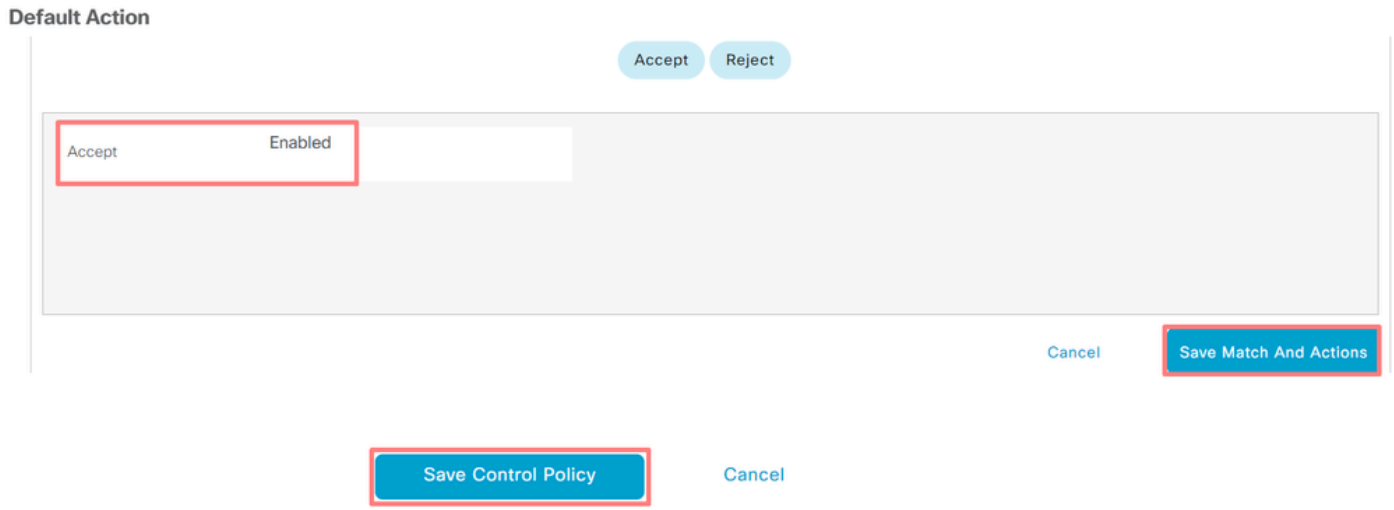


Condição 2: o tráfego do VRF 5 é aceito e exportado para o VRF 1.



Altere a ação padrão da política para Aceitar.

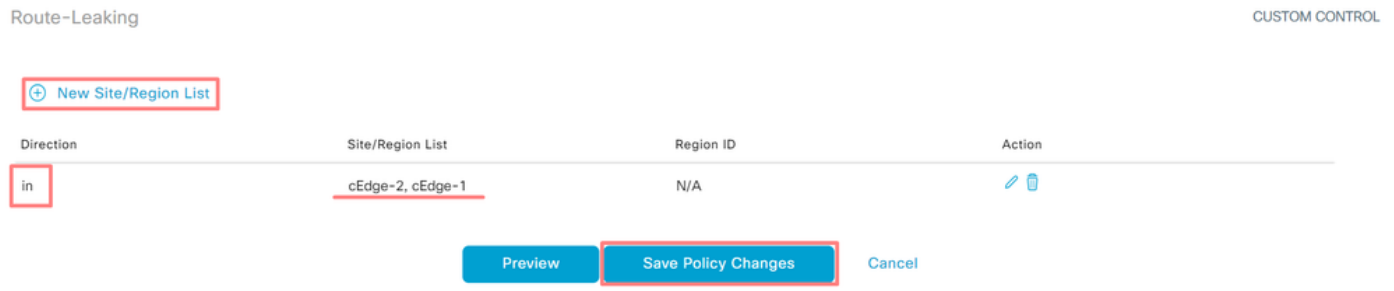
Clique em Salvar Correspondência e Ações e, em seguida, clique em Salvar Política de Controle.



4. Aplique a política nos locais onde o vazamento de rota é necessário.

Clique na guia Topology, na Route-Leaking Policy, selecione New Site/Region List em Inbound Site List. Selecione as listas de sites onde o vazamento de rota é necessário.

Para salvar as modificações, selecione Save Policy Changes.



Encadeamento de serviços

O encadeamento de serviços também é conhecido como inserção de serviços. Ela envolve a injeção de um serviço de rede; os serviços padrão incluem Firewall (FW), Sistema de Detecção de Intrusão (IDS) e Sistema de Prevenção de Intrusão (IPS). Nesse caso, um serviço de Firewall é inserido no caminho de dados.

Configuração via CLI

1. Configure as Listas no Controlador Cisco Catalyst SD-WAN.

A configuração permite que os sites sejam identificados por meio de uma lista.

Crie uma lista para os sites de onde cada VRF 1 está localizado.

Na lista Local de Transporte (TLOC), especifique o endereço onde o tráfego deve ser redirecionado para acessar o serviço.

<#root>

```
vSmart#
config

vSmart(config)#
 policy

vSmart(config-policy)#
lists

vSmart(config-lists)#
site-list cEdge-1

vSmart(config-site-list-cEdge-1)#
site-id 1

vSmart(config-site-list-cEdge-1)# exit
vSmart(config-lists)#
site-list cEdge-2

vSmart(config-site-list-cEdge-2)#
site-id 2

vSmart(config-site-list-cEdge-2)# exit
vSmart(config-lists)#
tloc-list cEdge-1-TLOC

vSmart(config-tloc-list-cEdge-1-TLOC)#
tloc 192.168.1.11 color public-internet encap ipsec

vSmart(config-tloc-list-cEdge-1-TLOC)#
commit
```

2. Configure a Política no Controlador Cisco Catalyst SD-WAN.

A sequência filtra o tráfego do VRF 1. O tráfego é permitido e inspecionado em um Firewall de serviço localizado no VRF 5.

```
<#root>
vSmart#
config
```

```
vSmart(config)#
 policy

vSmart(config-policy)#
control-policy Service-Chaining

vSmart(config-control-policy-Service-Chaining)#
sequence 1

vSmart(config-sequence-1)#
match route

vSmart(config-match-route)#
vpn 1

vSmart(config-match-route)#
action accept

vSmart(config-action)#
set

vSmart(config-set)#
 service FW vpn 5

vSmart(config-set)#
service tloc-list cEdge-1-TLOC

vSmart(config-set)# exit
vSmart(config-action)# exit
vSmart(config-sequence-1)# exit
vSmart(config-control-policy-Service-Chaining)#
default-action accept
vSmart(config-control-policy-Service-Chaining)#
commit
```

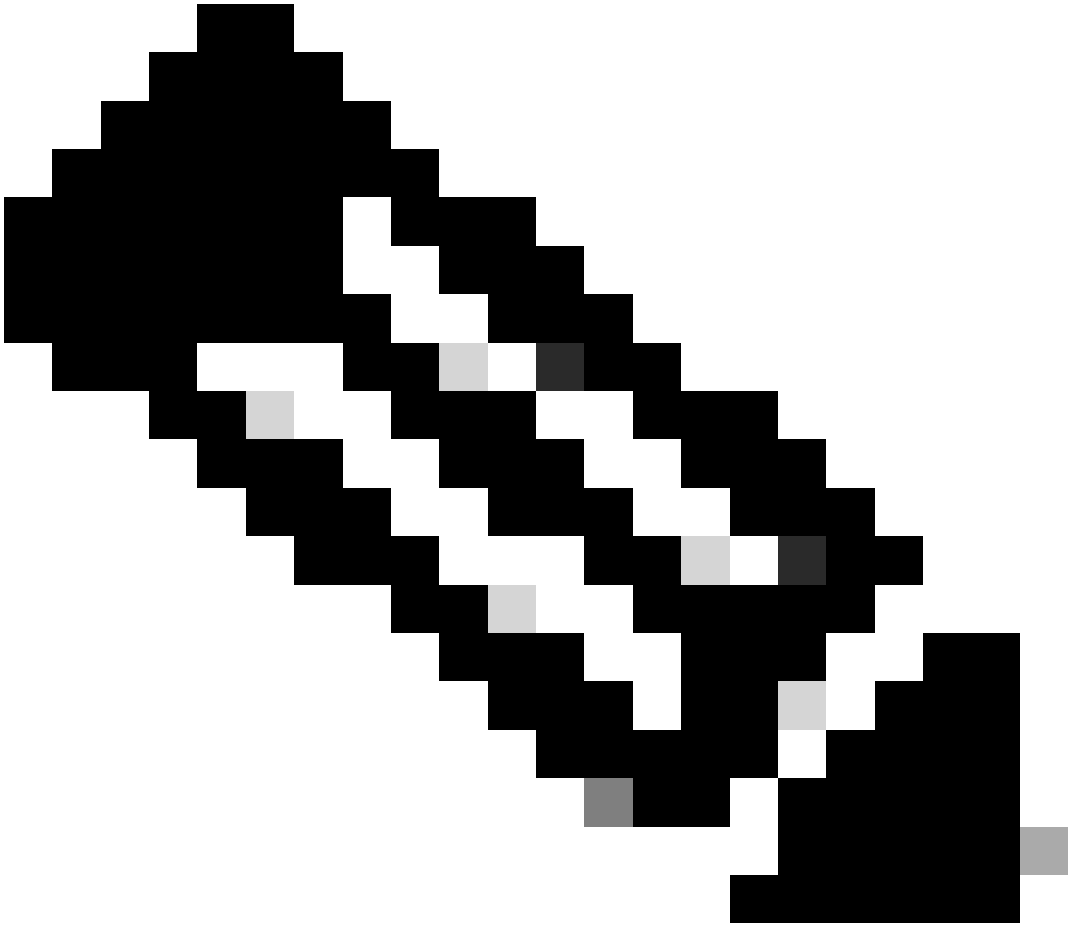
3. Aplique a Política no Controlador Cisco Catalyst SD-WAN.

A política é configurada nos locais 1 e 2 para permitir que o tráfego do VRF 1 seja inspecionado.

```
<#root>
vSmart#
```

```
config

vSmart(config)#
apply-policy

vSmart(config-apply-policy)#
site-list cEdge-1
vSmart(config-site-list-cEdge-1)#
 control-policy Service-Chaining out
vSmart(config-site-list-cEdge-1)# exit

vSmart(config-apply-policy)#
site-list cEdge-2
vSmart(config-site-list-cEdge-1)#
 control-policy Service-Chaining out
vSmart(config-site-list-cEdge-1)#
commit
```

Configuração via modelo

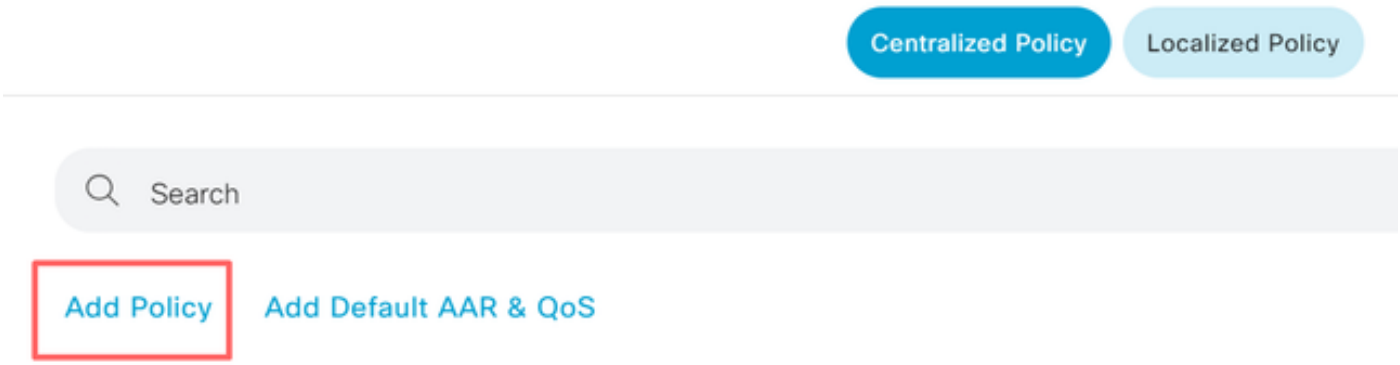


Observação: para ativar a política por meio da Interface Gráfica de Usuário (GUI) do Cisco Catalyst SD-WAN Manager, o Controlador Cisco Catalyst SD-WAN deve ter um modelo anexado.

1. Crie políticas no Cisco Catalyst SD-WAN Manager.

Navegue até Configuration > Policies >Centralized Policy.

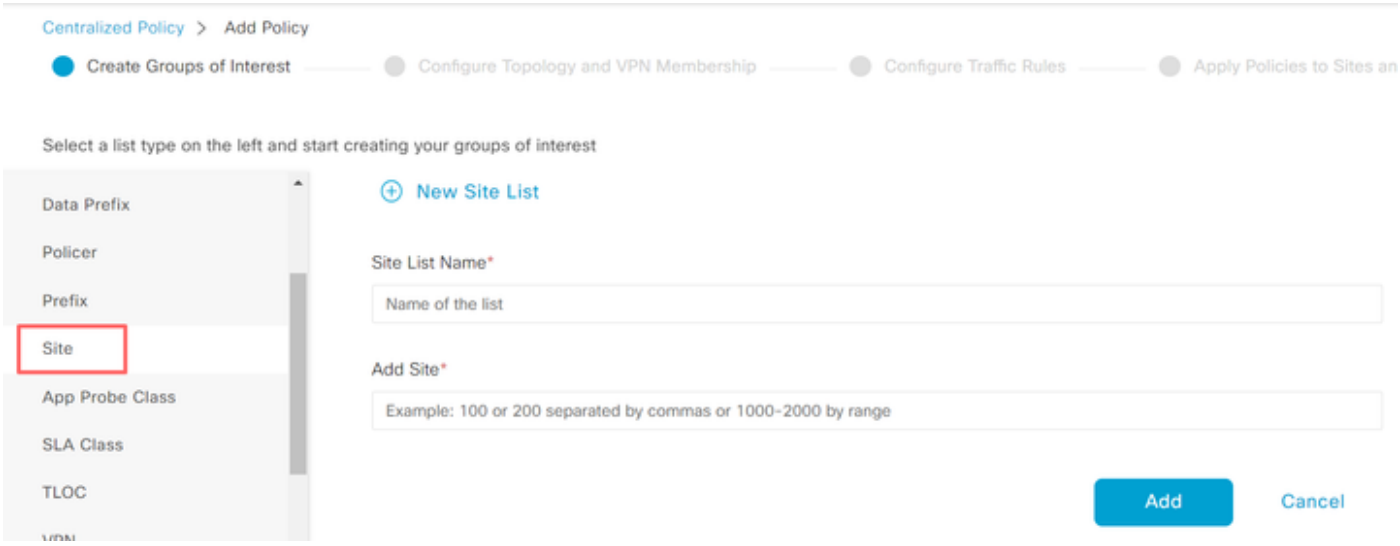
Na guia Centralized Policy, clique em Add Policy.



2. Crie listas no Cisco Catalyst SD-WAN Manager.

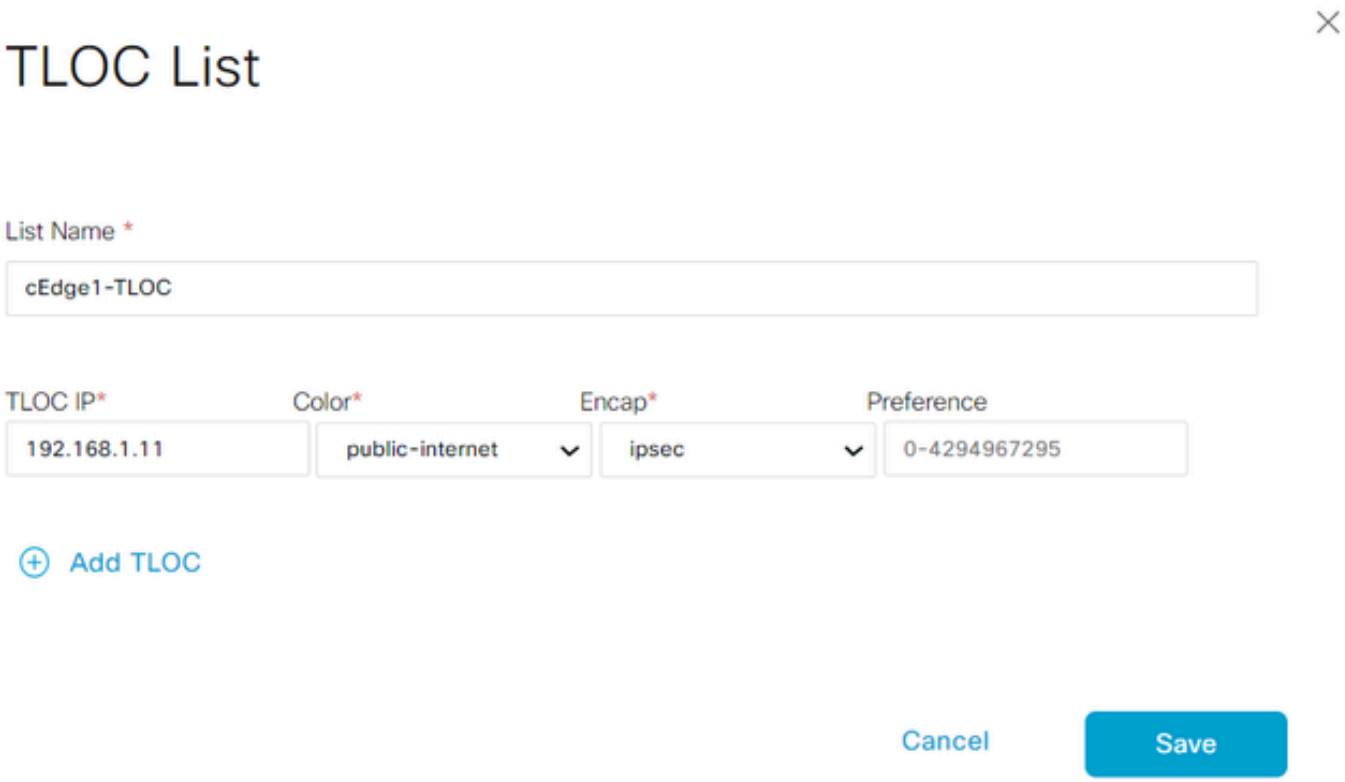
Navegue até Site > Nova lista de sites.

Crie a lista de sites dos sites em que o VRF 1 está localizado e selecione Add.



Navegue até TLOC > Nova lista TLOC.

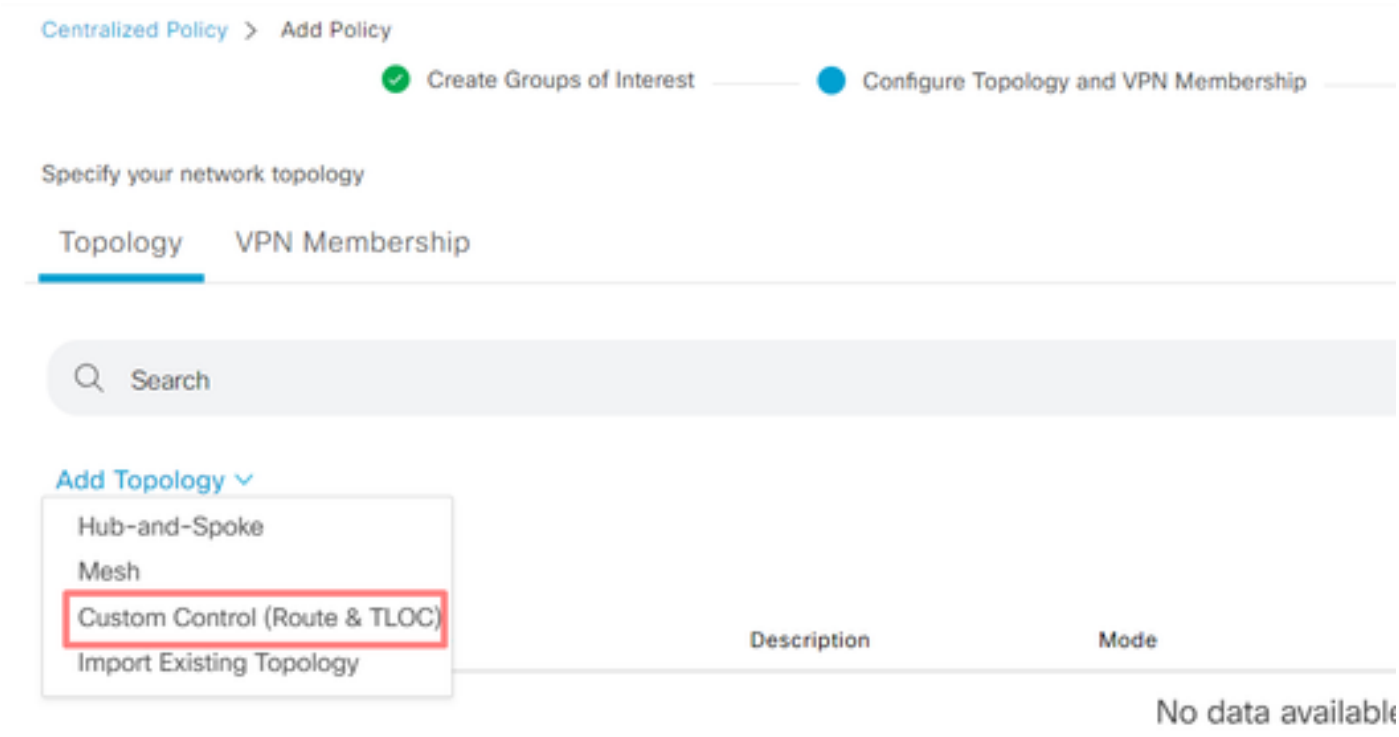
Crie a lista TLOC em que o encadeamento de serviços está localizado e selecione Salvar.



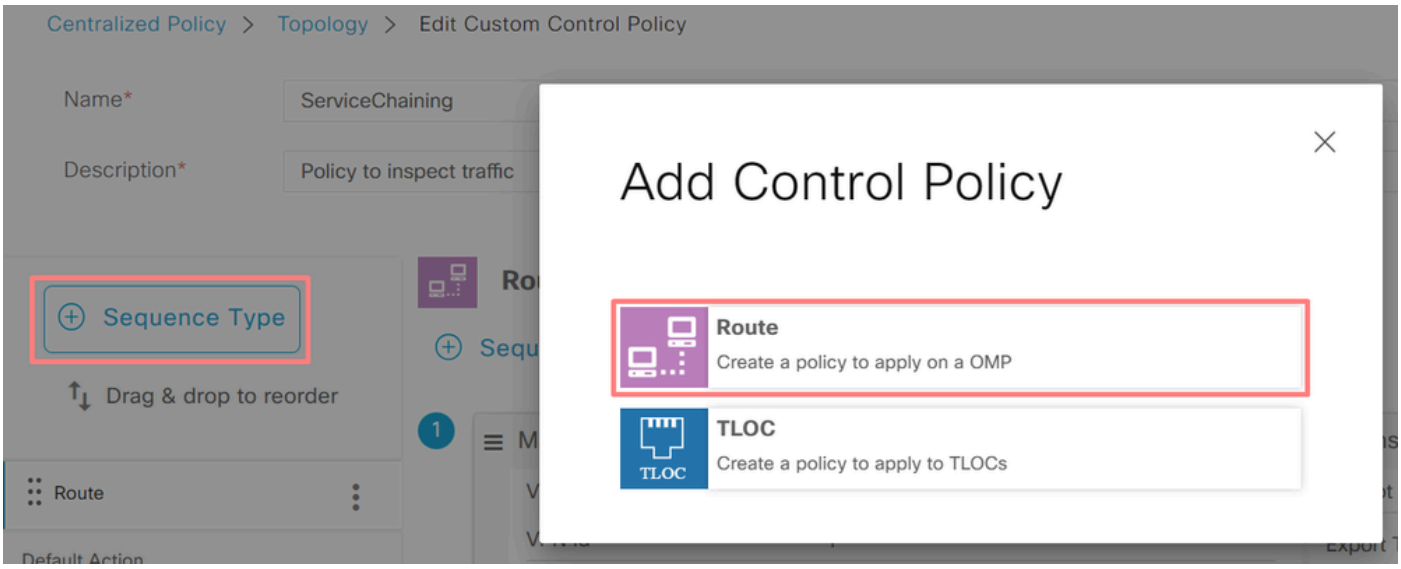
3. Adicione Regras de Sequência.

Clique na guia Topology e clique em Add Topology.

Crie um Controle Personalizado (Rota e TLOC).

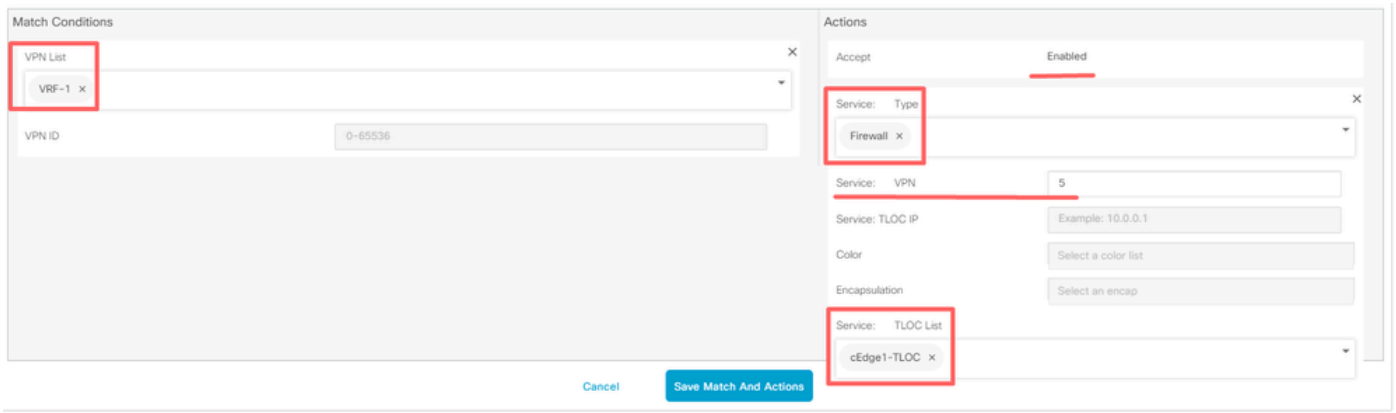


Clique em Sequence Type e selecione Route sequence.



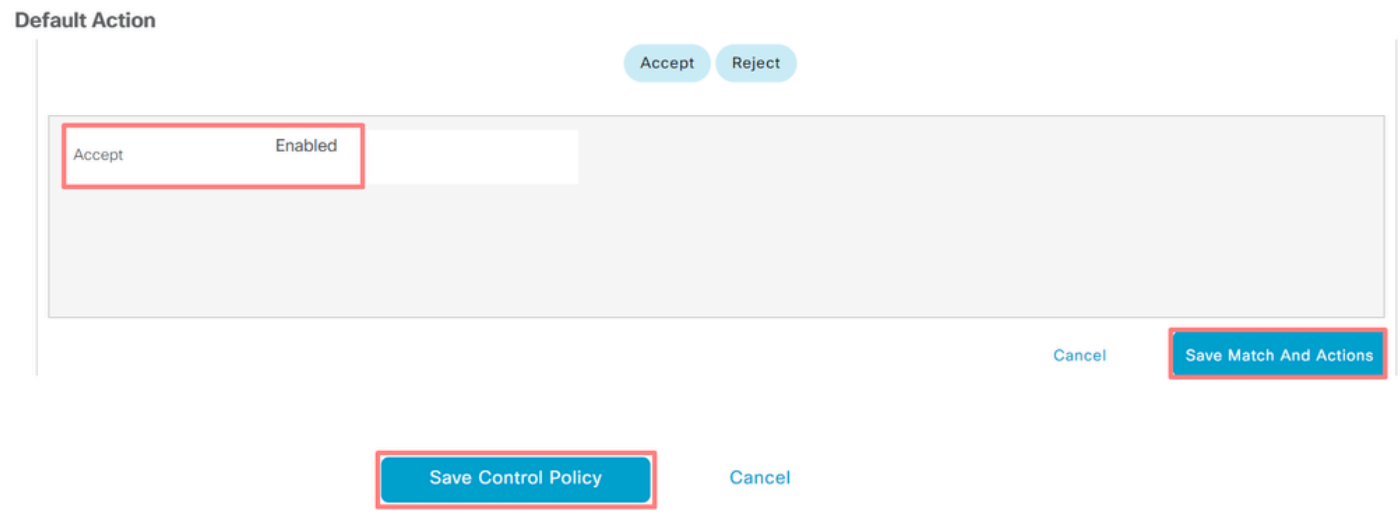
Adicione uma Regra de Sequência.

A sequência filtra o tráfego do VRF 1, permite-o e o redireciona para um serviço (Firewall) que existe no VRF 5. Isso pode ser obtido usando o TLOC no local 1, que é o local do serviço de firewall.



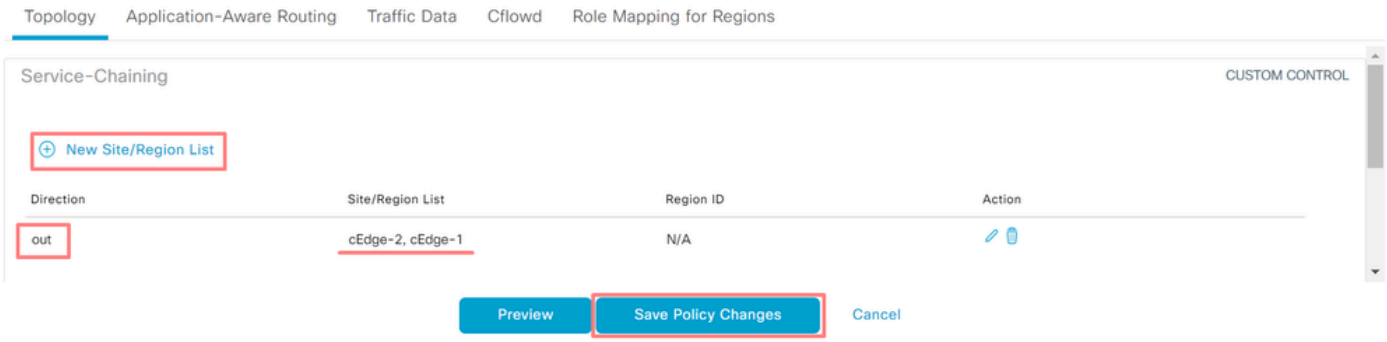
Altere a ação padrão da política para Aceitar.

Clique em Save Match and Actions e, em seguida, clique em Save Control Policy.



4. Aplique a política.

Clique na guia Topology, na Política de encadeamento de serviços, selecione New Site/Region List em Outbound Site List. Selecione os locais que o tráfego VRF 1 deve inspecionar e clique em Save Policy. Salve as modificações, clique em Save Policy Changes.



Anunciar Serviço de Firewall

Configuração via CLI

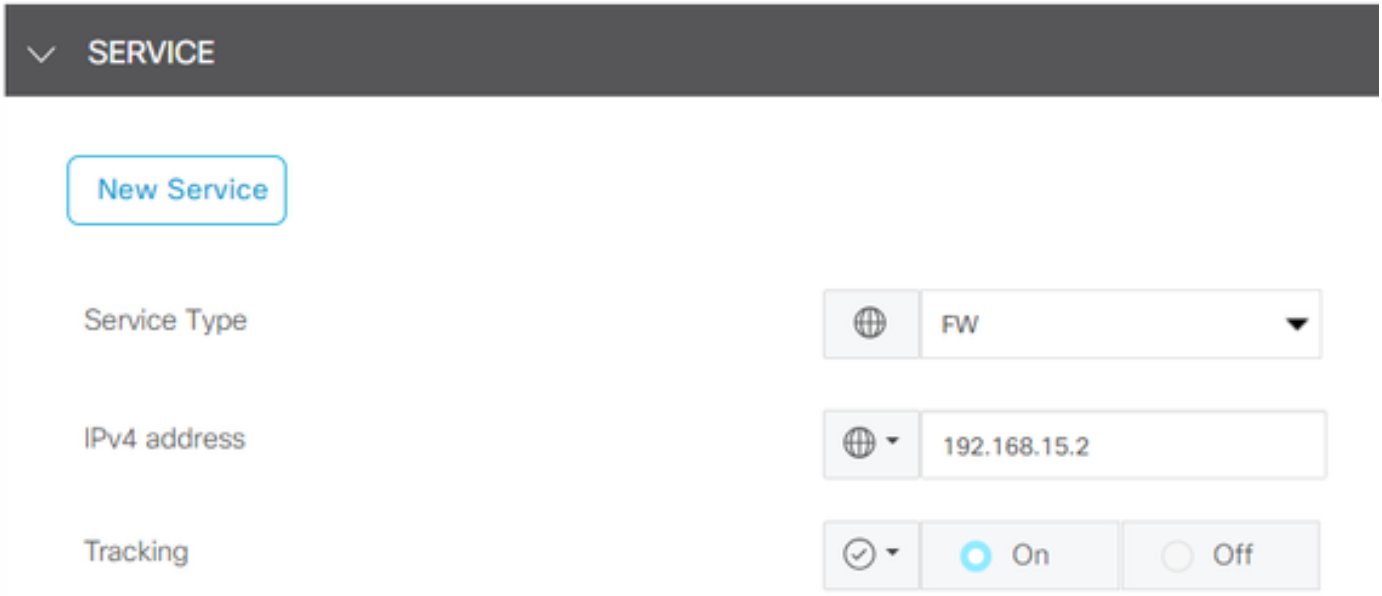
Para provisionar o serviço de Firewall, especifique o endereço IP do dispositivo de Firewall. O serviço é anunciado para o Cisco Catalyst SD-WAN Controller através de uma atualização OMP.

```
<#root>
cEdge-01#
config-transaction

cEdge-01(config)#
sdwan

cEdge-01(config-sdwan)#
service Firewall vrf 5

cEdge-01(config-vrf-5)#
ipv4 address 192.168.15.2
cEdge-01(config-vrf-5)#
 commit
```

Configuração via modelo

Navegue até o Modelo de recurso do VRF 5.
Continue em Configuration > Templates > Feature Template > Add Template > Cisco VPN.

Na seção Serviço, clique em Novo serviço. Insira os valores, Adicionar o serviço e Salvar o modelo.



Verificar

Vazamento de rota

Confirme se o controlador Cisco Catalyst SD-WAN está exportando rotas de VRF 1 para VRF 5 e vice-versa.

<#root>

```
vSmart# show omp routes vpn 1 | tab

                                                    PATH                                ATTRIBUTE
VPN     PREFIX                  FROM PEER           ID       LABEL      STATUS          TYPE          TLOC IP
-------------------------------------------------------------------------------------------------------------
1       192.168.15.0/24         192.168.3.16        92       1003       C,R,Ext         original      192.168.

                                                                                        installed     192.168.

1       192.168.16.0/24         192.168.3.16        69       1002       C,R             installed     192.168
1       192.168.18.0/24         192.168.3.15        69       1002       C,R             installed     192.168

vSmart# show omp routes vpn 5 | tab

                                                    PATH                                ATTRIBUTE
VPN     PREFIX                  FROM PEER           ID       LABEL      STATUS          TYPE          TLOC IP
-------------------------------------------------------------------------------------------------------------
5       192.168.15.0/24         192.168.3.16        69       1003       C,R             installed     192.168
5       192.168.16.0/24         192.168.3.16        92       1002       C,R,Ext         original      192.168.
```

```
                                                                    installed     192.168.
5      192.168.18.0/24     192.168.3.15           92       1002       C,R,Ext     original      192.168.
                                                                    installed     192.168.
```

Confirme se os Cisco Edge Routers receberam a rota vazada do VRF 1 para o VRF 5.

Confirme se os Cisco Edge Routers receberam a rota vazada do VRF 5 para o VRF 1.

<#root>

```
cEdge-1#
show ip route vrf 1

------- output omitted ------
m    192.168.15.0/24 [251/0] via 192.168.3.16 (5), 10:12:28, Sdwan-system-intf

     192.168.16.0/24 is variably subnetted, 2 subnets, 2 masks
C         192.168.16.0/24 is directly connected, TenGigabitEthernet0/0/3
L         192.168.16.1/32 is directly connected, TenGigabitEthernet0/0/3
m    192.168.18.0/24 [251/0] via 192.168.3.16, 10:12:28, Sdwan-system-intf

cEdge-1#
show ip route vrf 5

------- output omitted ------
192.168.15.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.168.15.0/24 is directly connected, TenGigabitEthernet0/0/2
L    192.168.15.1/32 is directly connected, TenGigabitEthernet0/0/2
m    192.168.16.0/24 [251/0] via 192.168.3.16 (1), 10:17:54, Sdwan-system-intf


m    192.168.18.0/24 [251/0] via 192.168.3.15, 10:17:52, Sdwan-system-intf


cEdge-2#
show ip route vrf 1

------- output omitted ------
m     192.168.15.0/24 [251/0] via 192.168.3.16, 01:35:15, Sdwan-system-intf

m     192.168.16.0/24 [251/0] via 192.168.3.16, 01:35:15, Sdwan-system-intf
      192.168.18.0/24 is variably subnetted, 2 subnets, 2 masks
```

```
C          192.168.18.0/24 is directly connected, GigabitEthernet0/0/1
L          192.168.18.1/32 is directly connected, GigabitEthernet0/0/1
```

Encadeamento de serviços

Verifique se o Cisco Edge Router anunciou o serviço de firewall para o controlador Cisco Catalyst SD-WAN via rota de serviço OMP.

<#root>

cEdge-01#

show sdwan omp services

```
ADDRESS                                                    PATH   REGION
FAMILY   TENANT    VPN    SERVICE  ORIGINATOR  FROM PEER       ID     ID        LABEL    STATUS    VRF
-------------------------------------------------------------------------------------------------------
ipv4     0         1      VPN      192.168.1.11    0.0.0.0          69     None      1002     C,Red,R
         0         5      VPN      192.168.1.11    0.0.0.0          69     None      1003     C,Red,R

0         5      FW       192.168.1.11    0.0.0.0          69     None      1005     C,Red,R   5
```

Confirme se o controlador Cisco Catalyst SD-WAN recebeu com êxito a rota de serviço.

<#root>

vSmart#

show omp services

```
ADDRESS                                          PATH   REGION
-----------------------------------------------------------------------------------
ipv4       1      VPN     192.168.1.12    192.168.1.12    69     None    1002     C,I,R
           1      VPN     192.168.1.11    192.168.1.11    69     None    1002     C,I,R
           5      VPN     192.168.1.11    192.168.1.11    69     None    1003     C,I,R

 5      FW      192.168.1.11    192.168.1.11    69     None    1005     C,I,R
```

Para verificar se o serviço de firewall inspeciona o tráfego do VRF 1, execute um traceroute.

<#root>

```
Service-Side-cEdge1#traceroute 192.168.18.2
Type escape sequence to abort.
```

```
Tracing the route to 192.168.18.2
VRF info: (vrf in name/id, vrf out name/id)
1 192.168.16.1 0 msec 0 msec 0 msec
2 192.168.16.1 1 msec 0 msec 0 msec
3 192.168.15.2 1 msec 0 msec 0 msec
4 192.168.15.1 0 msec 0 msec 0 msec
5 10.31.127.146 1 msec 1 msec 1 msec
6 192.168.18.2 2 msec 2 msec *

Service-Side-cEdge2#traceroute 192.168.16.2
Type escape sequence to abort.
Tracing the route to 192.168.16.2
VRF info: (vrf in name/id, vrf out name/id)
1 192.168.18.1 2 msec 1 msec 1 msec
2 10.88.243.159 2 msec 2 msec 2 msec
3 192.168.15.2 1 msec 1 msec 1 msec
4 192.168.15.1 2 msec 2 msec 1 msec
5 192.168.16.2 2 msec * 2 msec
```

Informações Relacionadas

- Encadeamento de serviços
- Vazamento de rota
- SD-WAN - Configurar vazamento de rota - YouTube

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.