Configure Route Leaking for Service Chaining in SD-WAN

Contents

Introduction

This document describes how to configure and verify Service Chaining to inspect traffic across different VRF.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco Software-defined Wide Area Network (SD-WAN)
- Control Policies.
- Templates.

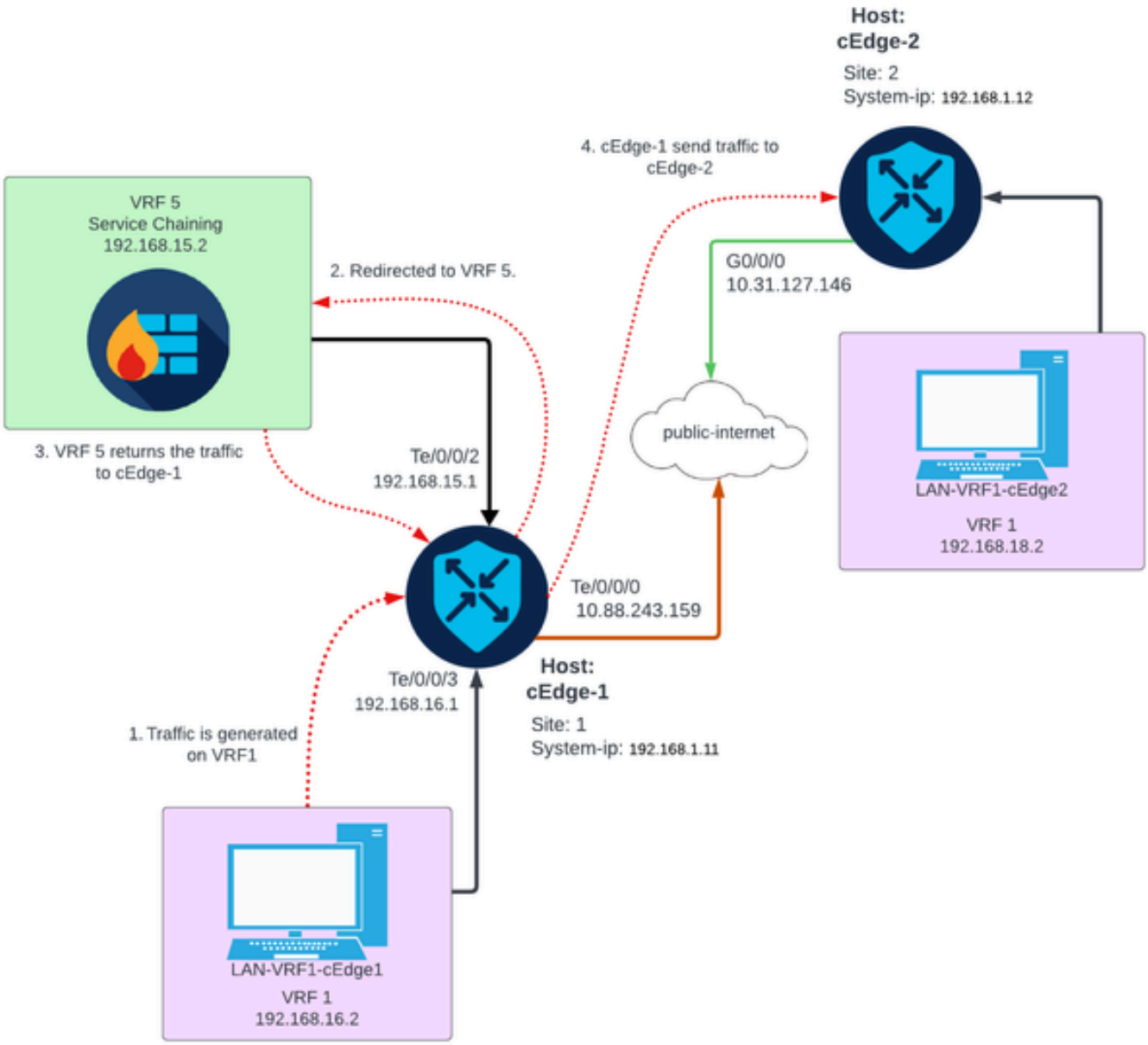
Components Used

This document is based on these software and hardware versions:

- SD-WAN Controllers (20.9.4.1)
- Cisco Edge Router (17.09.04)

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. If your network is live, ensure that you understand the potential impact of any command.

Network Diagram



Background Information

On the network diagram, Firewall service is in Virtual Routing and Forwarding (VRF) 5 while LAN devices are located on VRF 1. Information of routes must be shared between VRFs so that forward and inspection of the traffic can be achieved. To route traffic through a service a control policy on the Cisco SD-WAN Controller must be configured.

Configure

Route Leaking

Route leaking enables the propagation of routing information between different VRFs. In this scenario, when Service Chaining (Firewall) and LAN Service side are in different VRFs, route leaking is necessary for traffic inspection.

To ensure routing between LAN Service side and Firewall service, leak of routes is needed in both VRFs, and apply a policy in the sites where route leaking is required.

Configuration via CLI

1. Configure Lists on the Cisco Catalyst SD-WAN Controller.

The configuration allows sites to be identified through a list.

<#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 Policy on the Cisco Catalyst SD-WAN Controller.

The configuration allows propagation of routing information between VRF 1 and VRF 5, to ensure routing between them, both VRF must share their routing data.

Policy permit traffic of VRF 1 to be accepted and exported to the VRF 5 and 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. Apply the Policy on the Cisco Catalyst SD-WAN Controller.

Policy is applied in site 1 and site 2 to allow routing between the VRF 1 situated on those sites and on VRF 5.

Policy is implemented inbound, this means is applied to the OMP updates coming from Cisco Edge Routers to 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
```

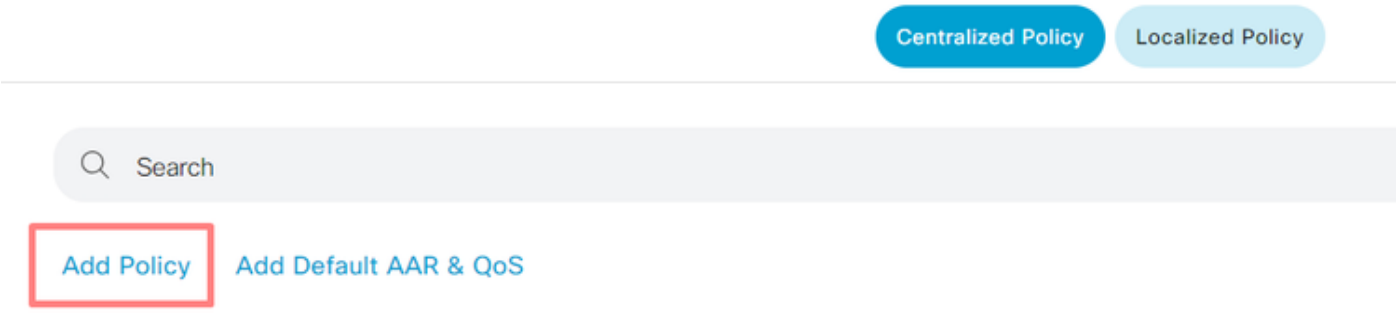
Configuration via Template

Note: To activate the policy through Cisco Catalyst SD-WAN Manager Graphic User Interface (GUI), Cisco Catalyst SD-WAN Controller must have a template attached.

1. Create the policy to allow propagation of routing information.

Create Policy on the Cisco Catalyst SD-WAN Manager, navigate to**Configuration**> **Policies** >**Centralized Policy**.

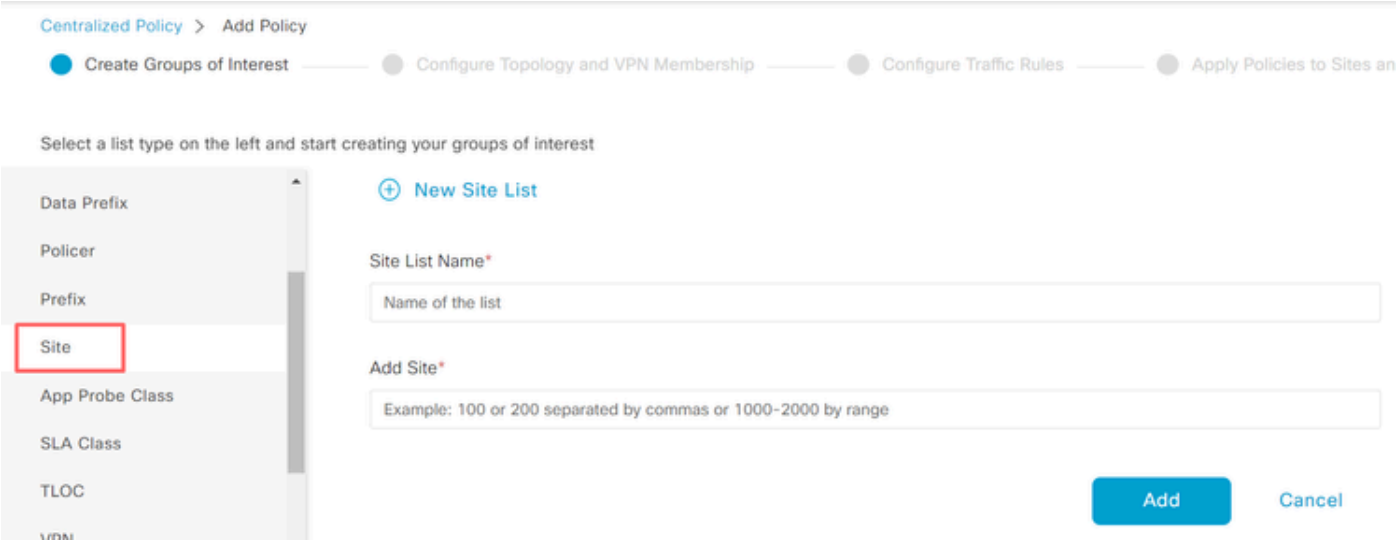
Under**Centralized Policy** tab click on**Add Policy**.



2. Create lists on the Cisco Catalyst SD-WAN Manager, the configuration allows sites to be identified through a list.

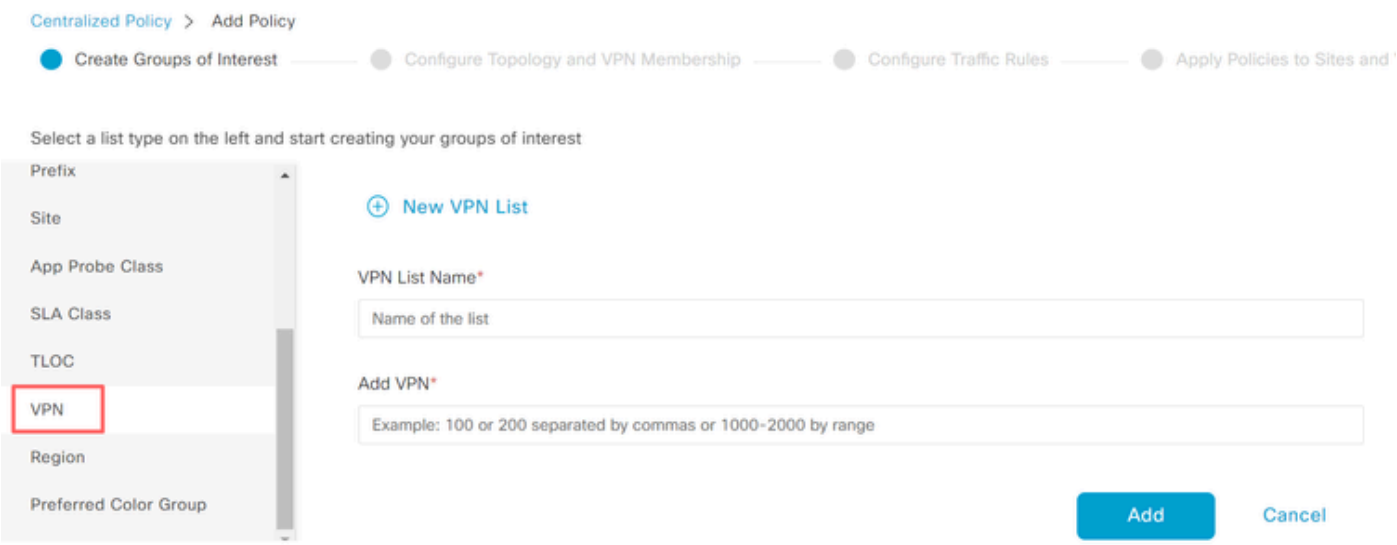
Navigate to **Site > New Site List**.

Create the list of sites where route leaking is needed and **Add** the list.



Navigate to **VPN > New VPN List**.

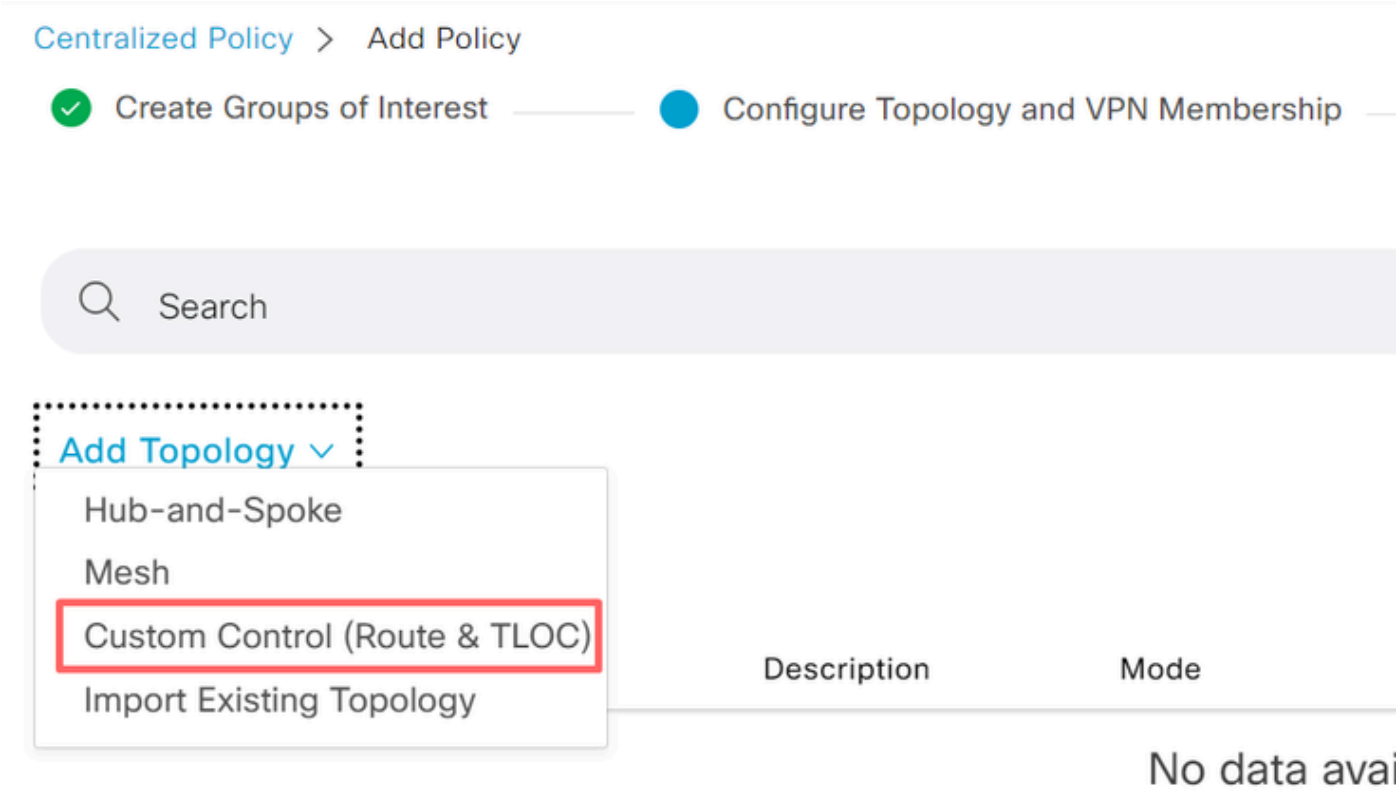
Create the **VPN** list where route leaking needs to be applied on, click on **Next**.



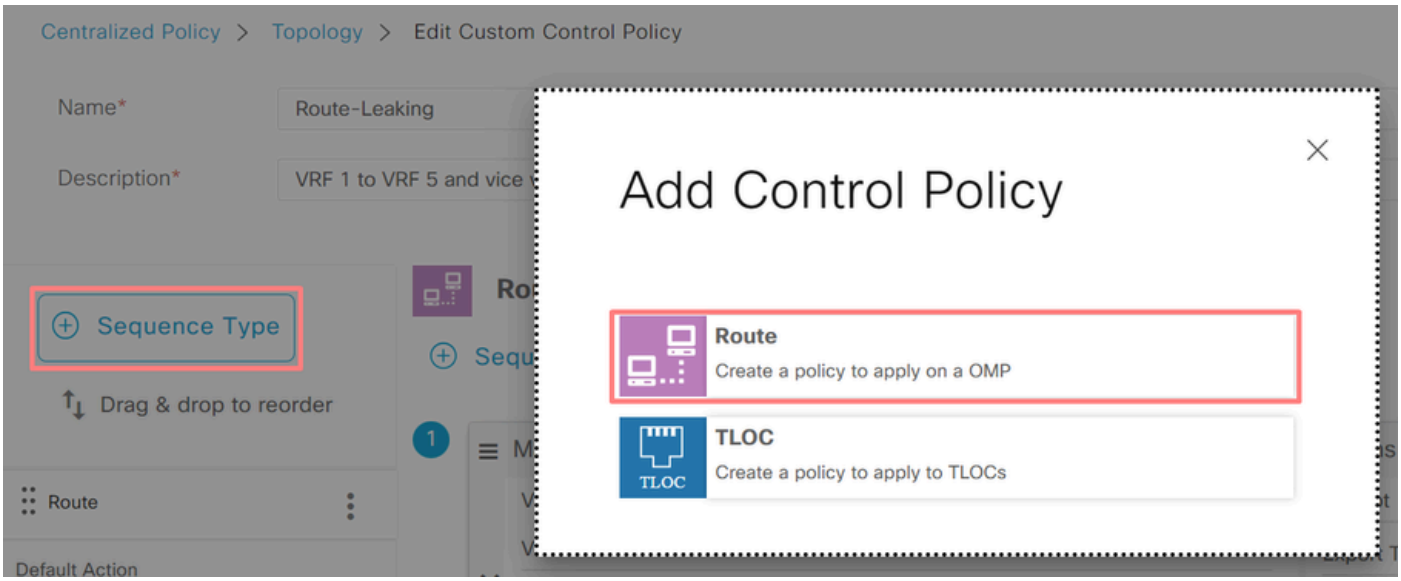
3. Configure Policy on the Cisco Catalyst SD-WAN Manager.

Click on the**Topology**tab and click on Add Topology.

Create a **Custom Control (Route & TLOC)**.

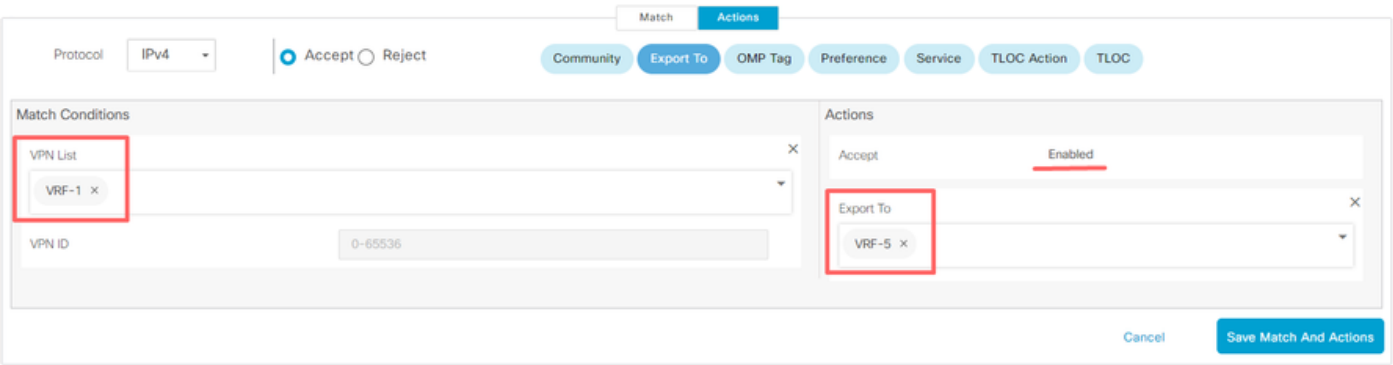


Click on **Sequence Type** and select **Route** sequence.

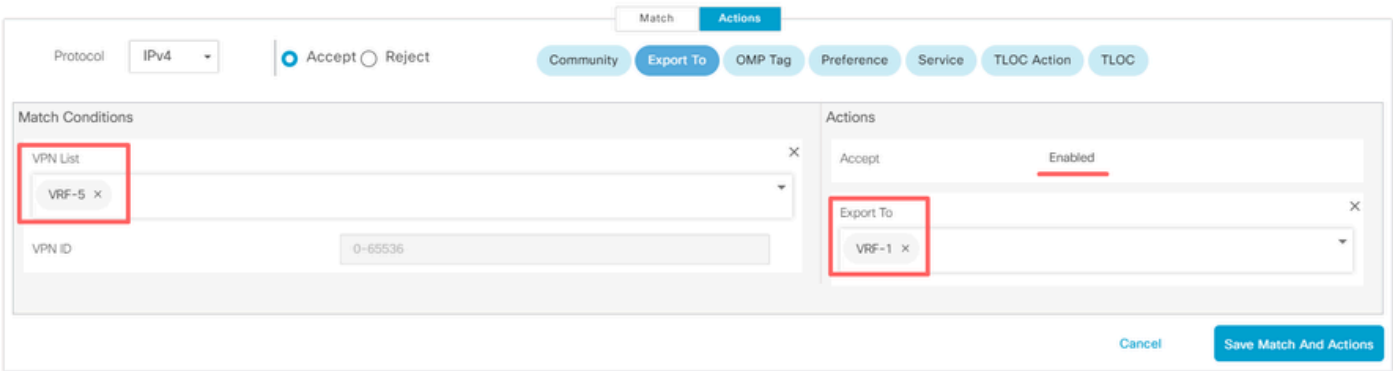


Add a **Sequence Rule**.

Condition 1: Traffic of VRF 1 is accepted and exported to the VRF 5.

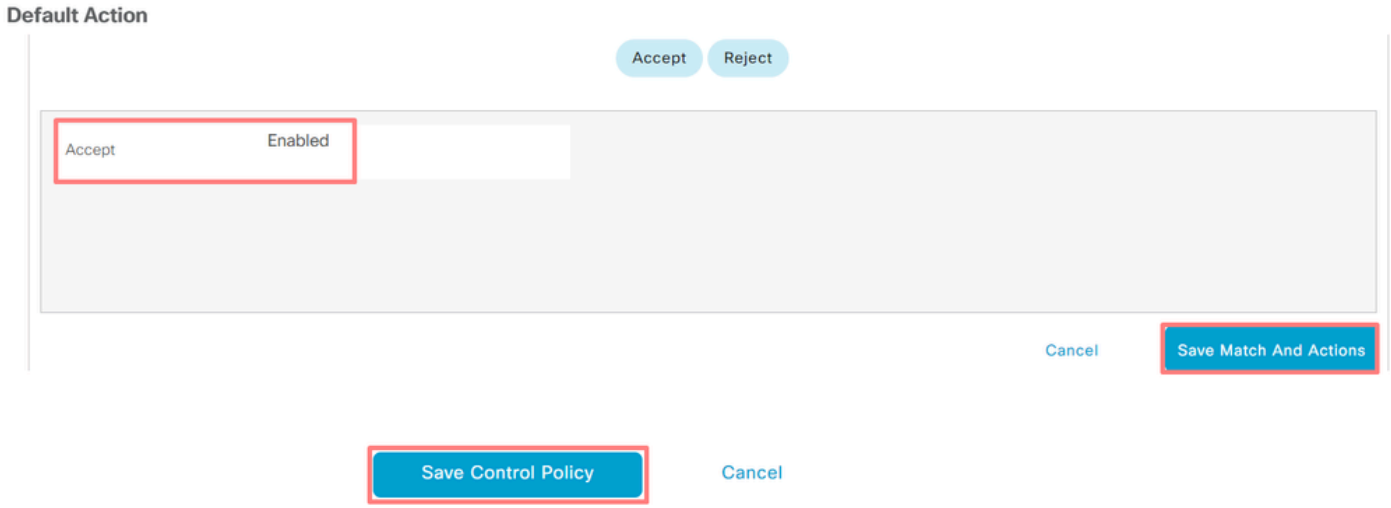


Condition 2: Traffic of VRF 5 is accepted and exported to the VRF 1.



Change the **Default Action** of the policy to **Accept**.

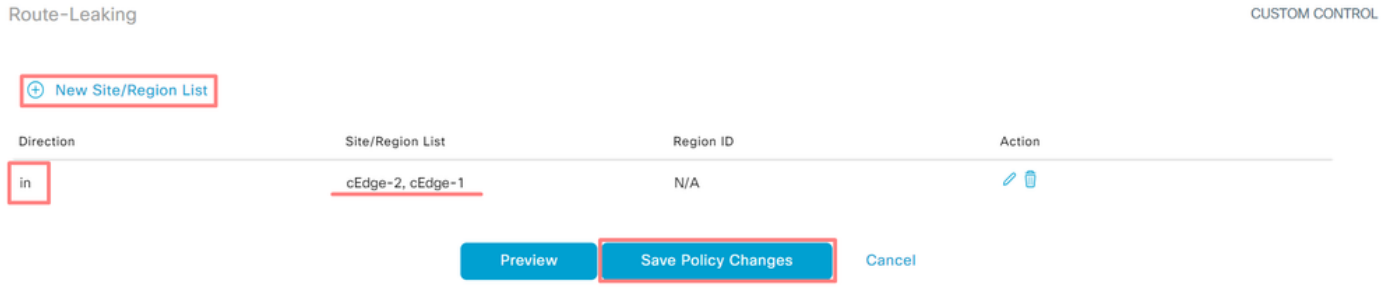
Click on **Save Match and Actions** and then click on **Save Control Policy**.



4. Apply the policy on the sites where route leaking is needed.

Click on the **Topology** tab, under the Route-Leaking Policy select **New Site/Region List** on **Inbound Site List**. Select the site lists where route leaking is needed.

To save the modifications select **Save Policy Changes**.



Service Chaining

Service Chaining is also known as service insertion. It involves the injection of a network service; the standard services include Firewall (FW), Intrusion Detection System (IDS), and Intrusion Prevention System (IPS). In this case, a Firewall service is inserted into the data path.

Configuration via CLI

1. Configure the Lists on the Cisco Catalyst SD-WAN Controller.

The configuration allows sites to be identified through a list.

Create a list for the sites of where each VRF 1 is located.

On the Transport Location (TLOC) list, specify the address where traffic must be redirected to reach the service.

<#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 Policy on the Cisco Catalyst SD-WAN Controller.

The sequence filters traffic from VRF 1. The traffic is permitted and inspected on a service Firewall located on 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
```

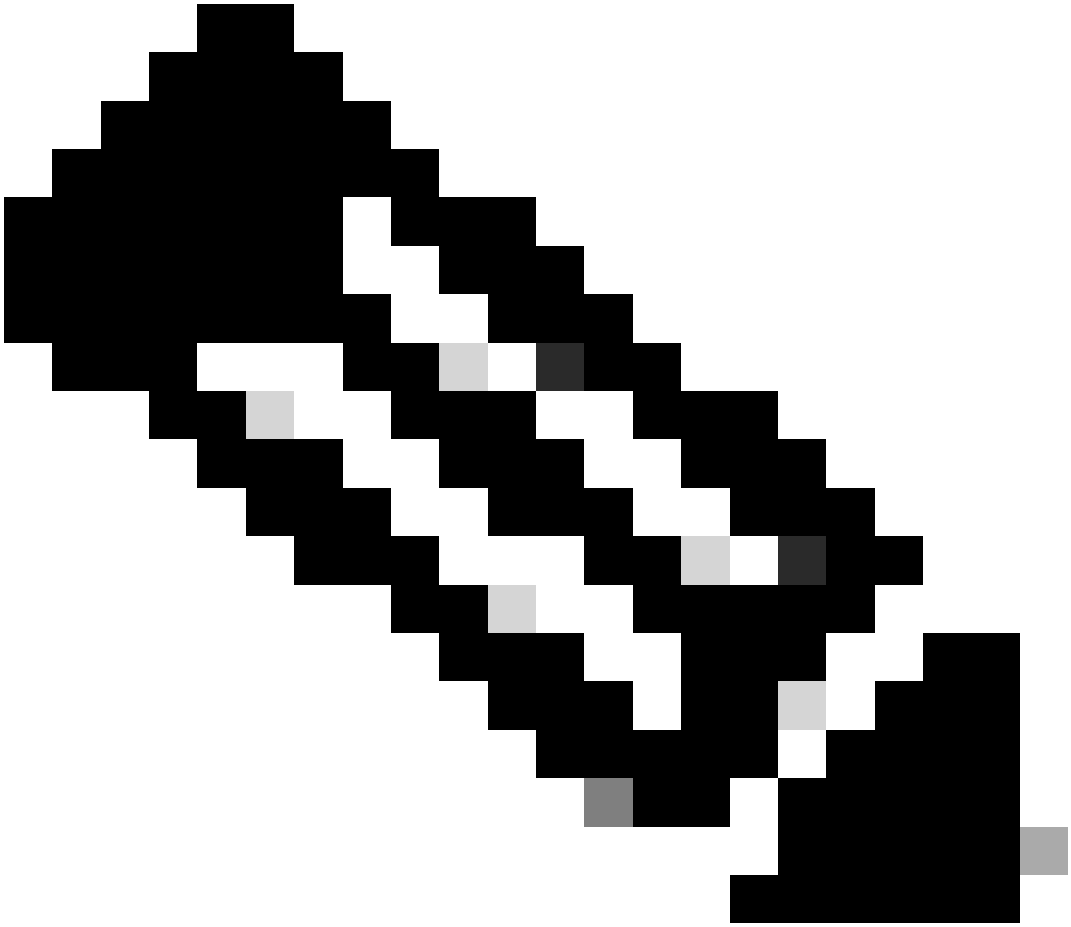
3. Apply the Policy on the Cisco Catalyst SD-WAN Controller.

The policy is configured in site 1 and 2 to permit traffic from VRF 1 to be inspected.

```
<#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
```

Configuration via Template

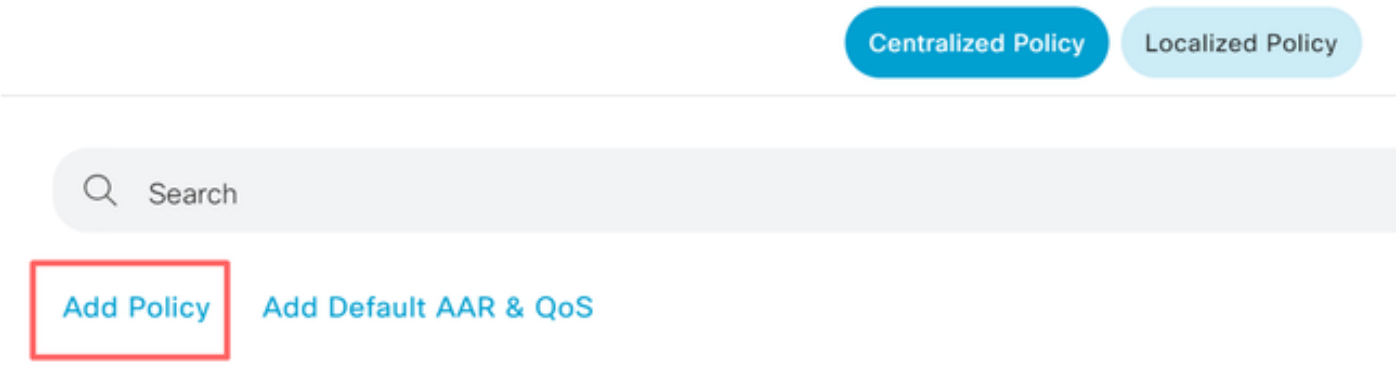


Note: To activate the policy through Cisco Catalyst SD-WAN Manager Graphic User Interface (GUI), Cisco Catalyst SD-WAN Controller must have a template attached.

1. Create Policy on the Cisco Catalyst SD-WAN Manager.

Navigate to **Configuration > Policies >Centralized Policy**.

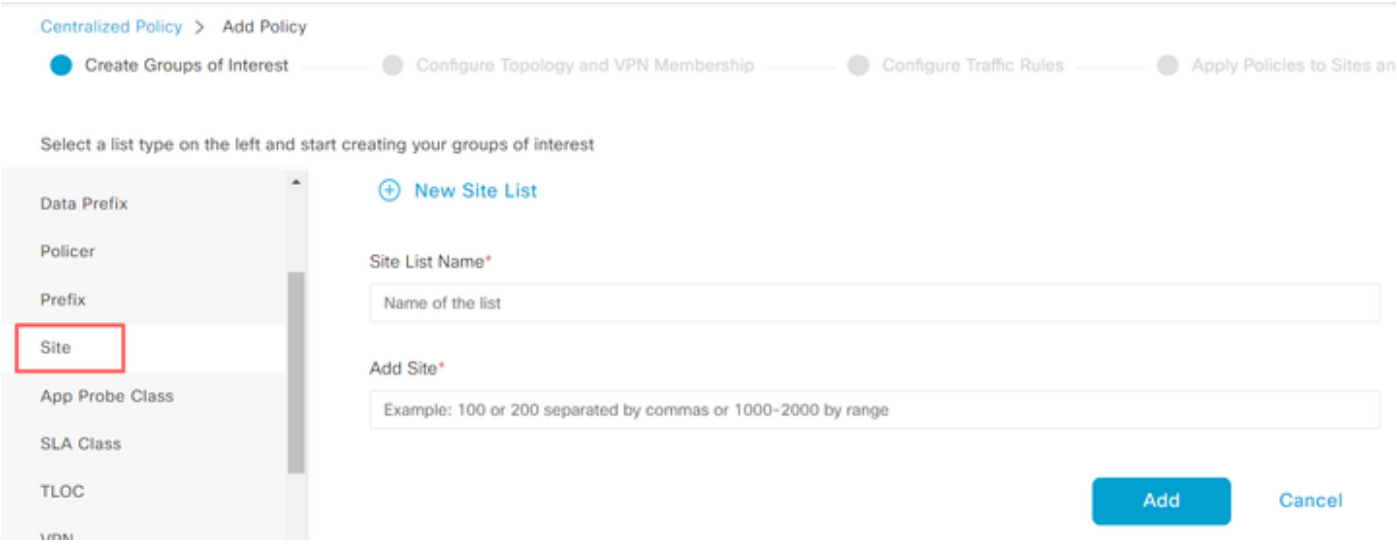
Under **Centralized Policy** tab click on **Add Policy**.



2. Create Lists on the Cisco Catalyst SD-WAN Manager.

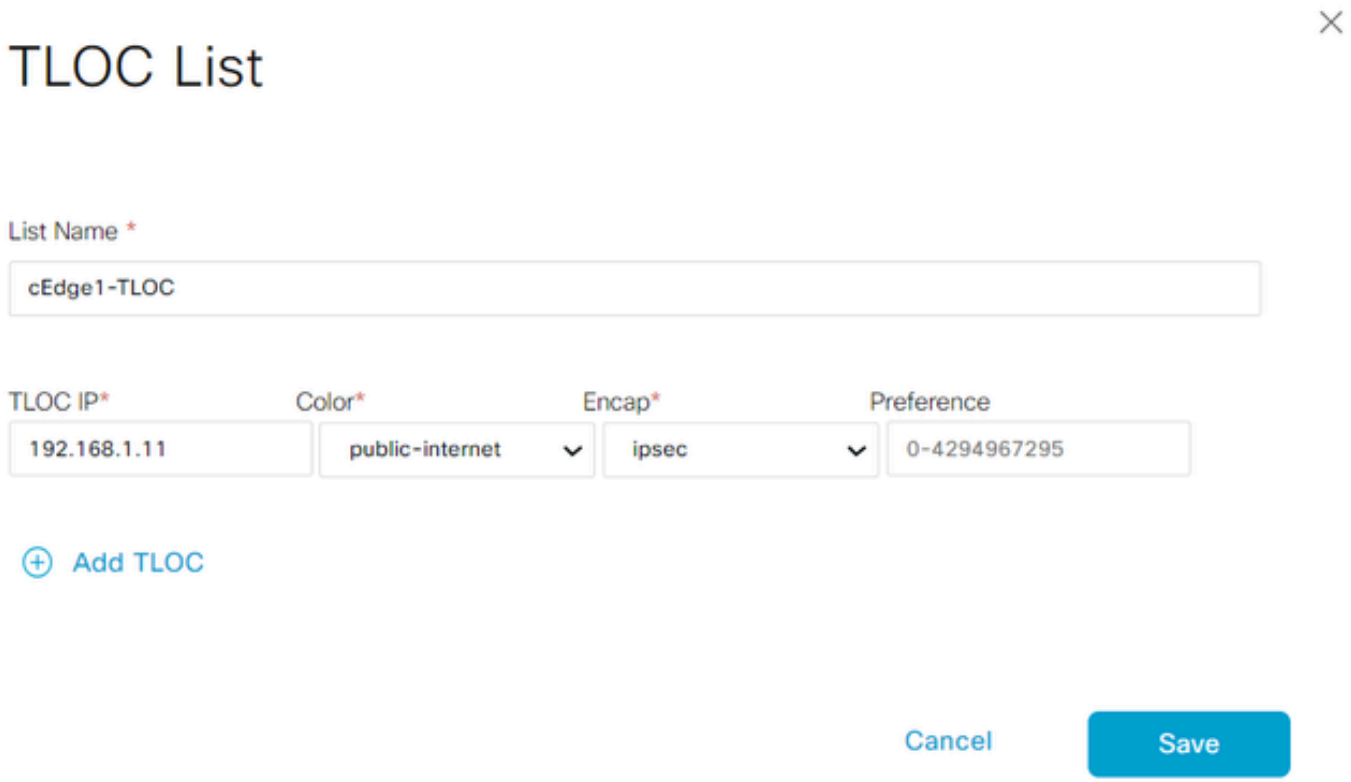
Navigate to **Site > New Site List**.

Create the site list of the sites where VRF 1 is located on and select **Add**.



Navigate to **TLOC > New TLOC List**.

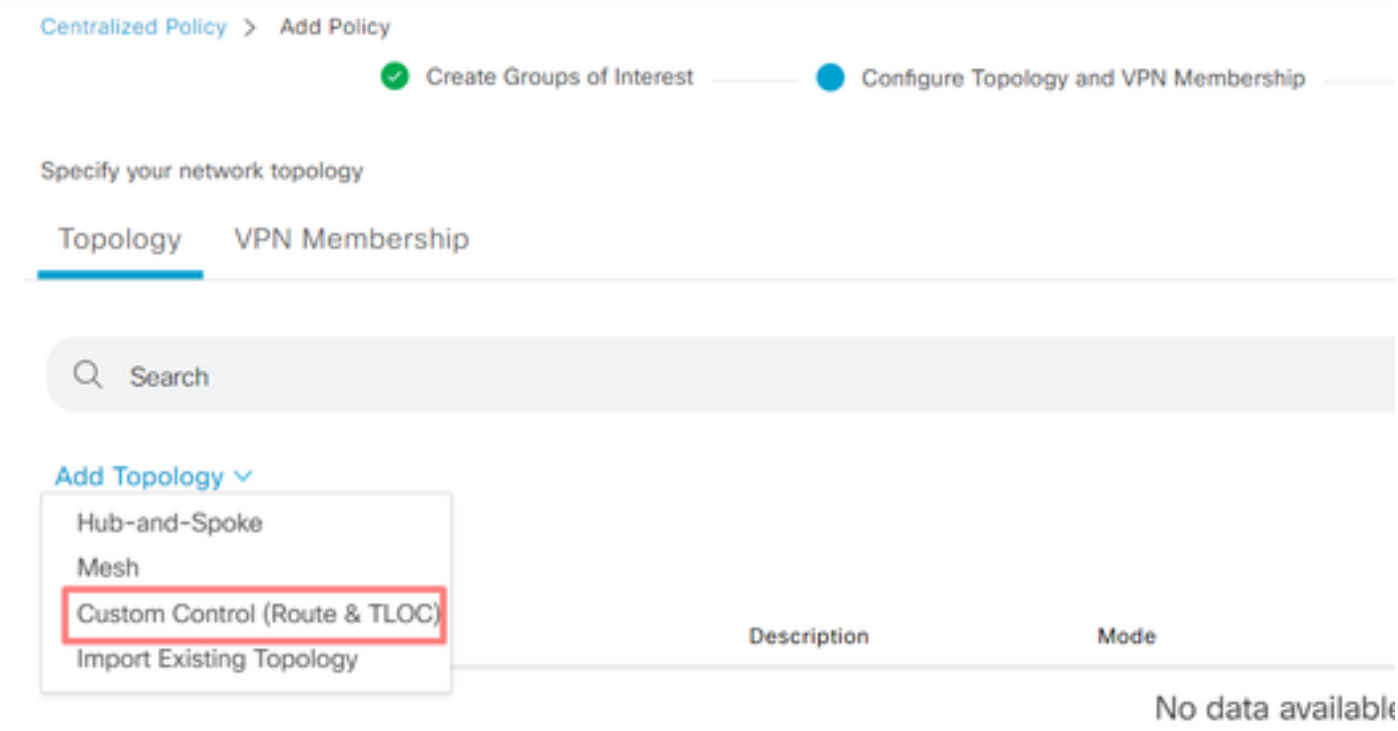
Create the TLOC list service chaining is located on and select **Save**.



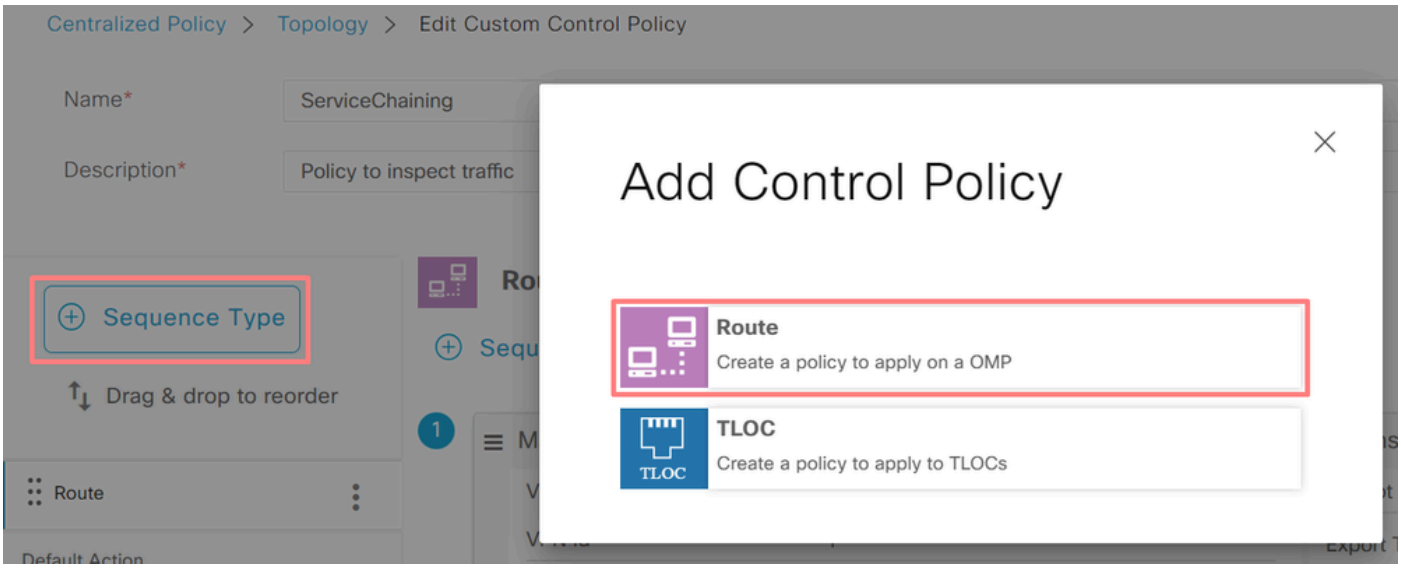
3. Add Sequence Rules.

Click on the **Topology** tab and click on **Add Topology**.

Create a **Custom Control (Route & TLOC)**.

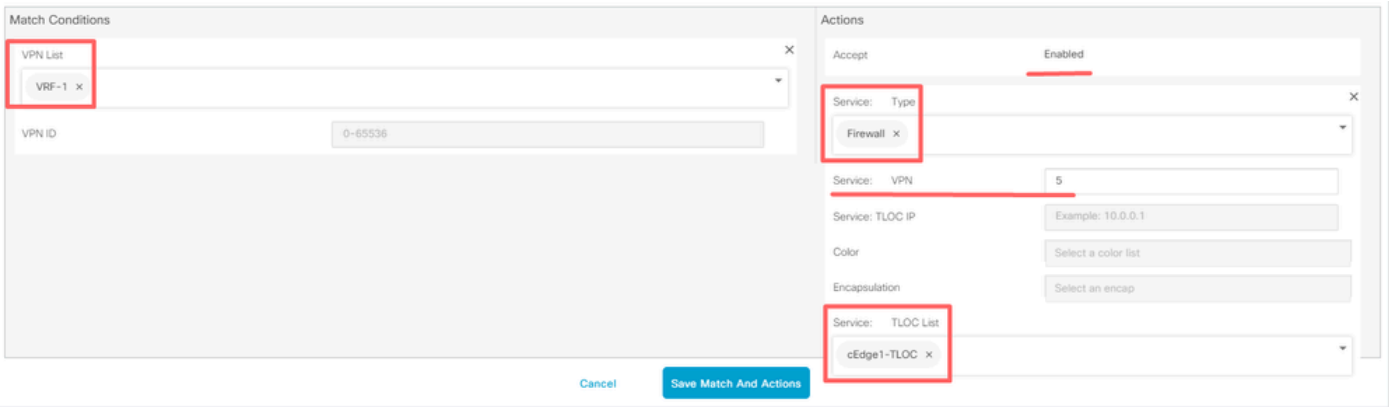


Click on **Sequence Type** and select **Route** sequence.



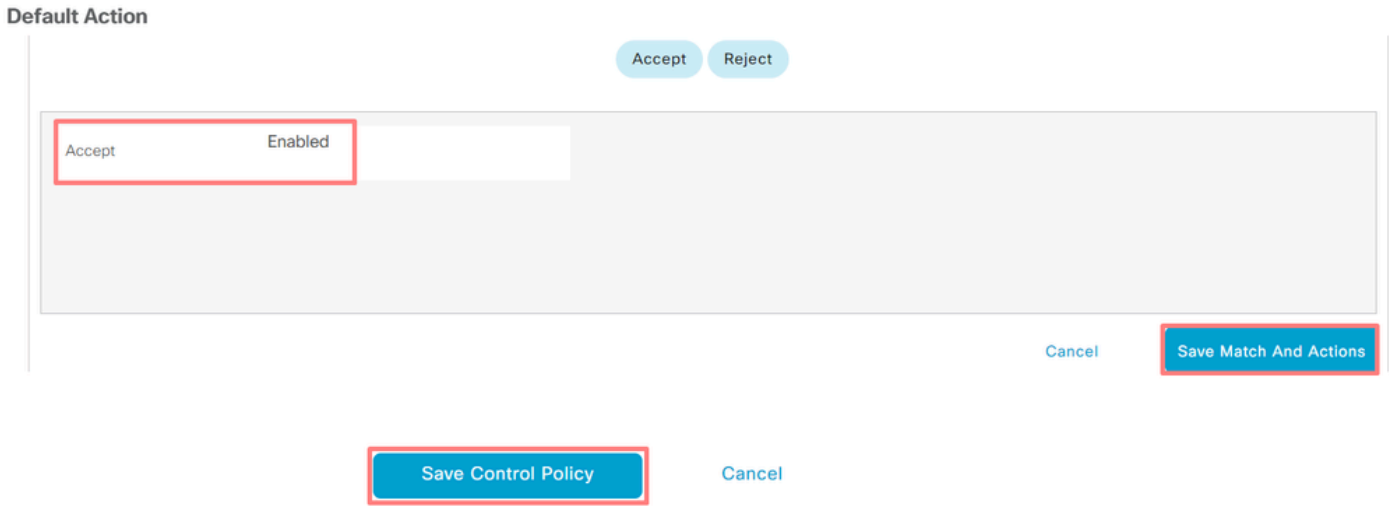
Add a **Sequence Rule**.

The sequence filters traffic from the VRF 1, allows it through, and then redirects it to a service (Firewall) that exists within VRF 5. This can be achieved by using the TLOC at site 1, which is the location of the Firewall service.



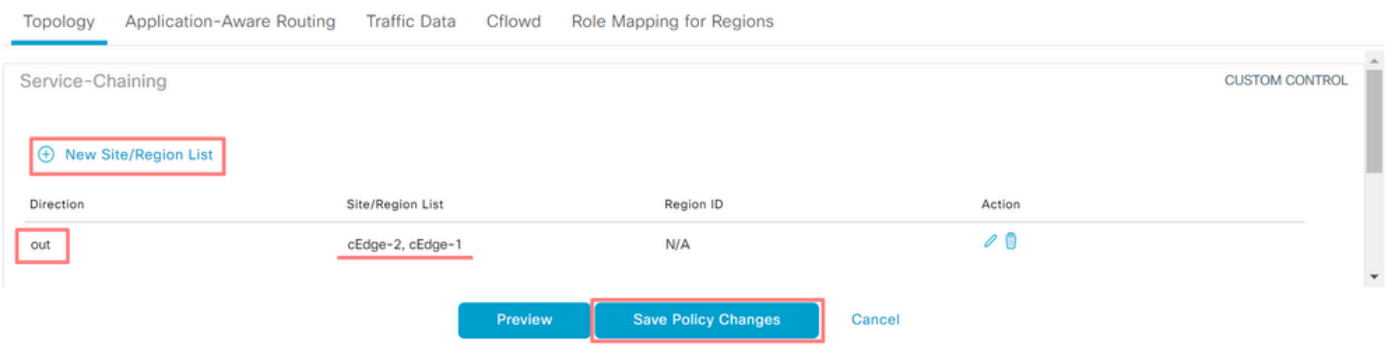
Change the **Default Action** of the policy to **Accept**.

Click on **Save Match and Actions** and then click **Save Control Policy**.



4. Apply the policy.

Click on the **Topology** tab, under the Service-Chaining Policy select **New Site/Region List** on **Outbound Site List**. Select the sites that the VRF 1 traffic must inspect and then click on **Save Policy**. Save the modifications, click on **Save Policy Changes**.



Advertise Firewall Service

Configuration via CLI

To provision the Firewall service, specify the IP address of the Firewall device. The service is announced to the Cisco Catalyst SD-WAN Controller through an OMP update.

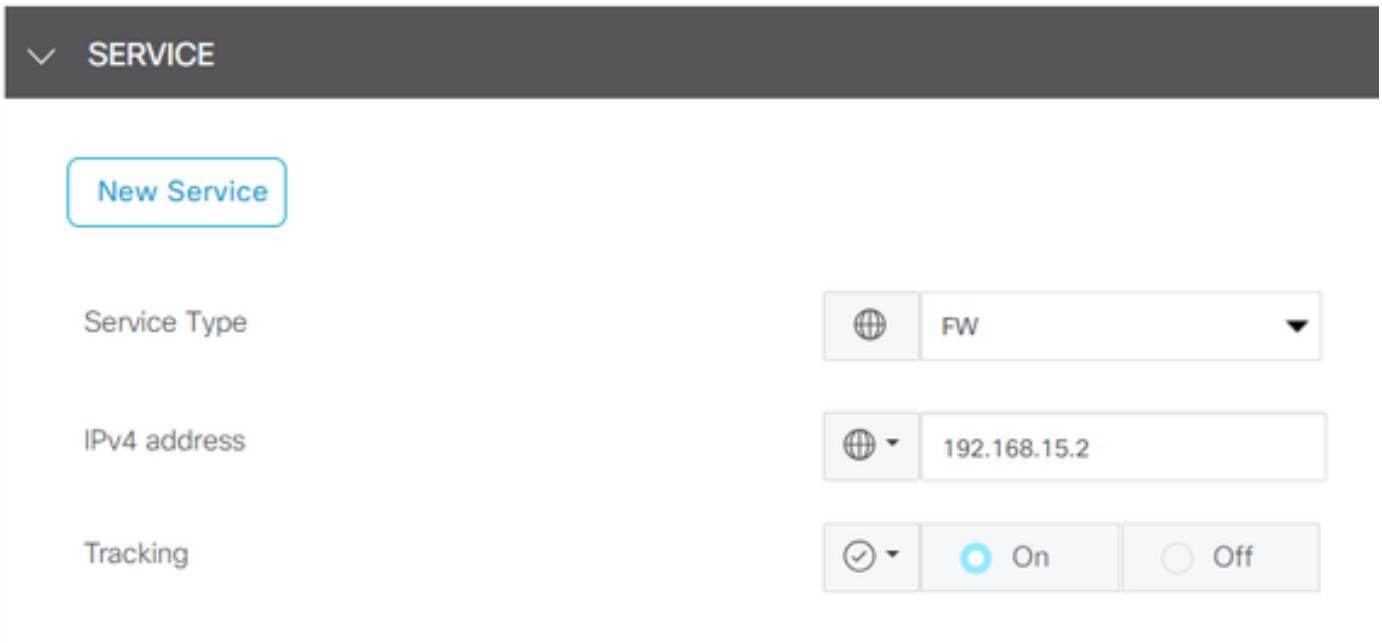
<#root>

```
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
```

Configuration via Template

Navigate to the **Feature template** of the VRF 5.
Proceed to **Configuration > Templates > Feature Template > Add Template > Cisco VPN**.

Under **Service** Section, click **New Service.** Enter the values, **Add the Service** and **Save** the template.



Verify

Route Leaking

Confirm Cisco Catalyst SD-WAN Controller is exporting routes from VRF 1 to VRF 5 and the other way around.

<#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.
```

Confirm Cisco Edge Routers received the leaked route from VRF 1 to VRF 5.

Confirm Cisco Edge Routers received the leaked route from VRF 5 to 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
```

Service Chaining

Verify Cisco Edge Router has advertised the Firewall service to the Cisco Catalyst SD-WAN Controller via OMP service route.

<#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
```

Confirm the Cisco Catalyst SD-WAN Controller has successfully received the service route.

<#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
```

To verify the Firewall service inspects the traffic from VRF 1; perform a 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
```

Related Information

- Service Chaining
- Route Leaking
- SD-WAN - Configure Route Leaking - YouTube