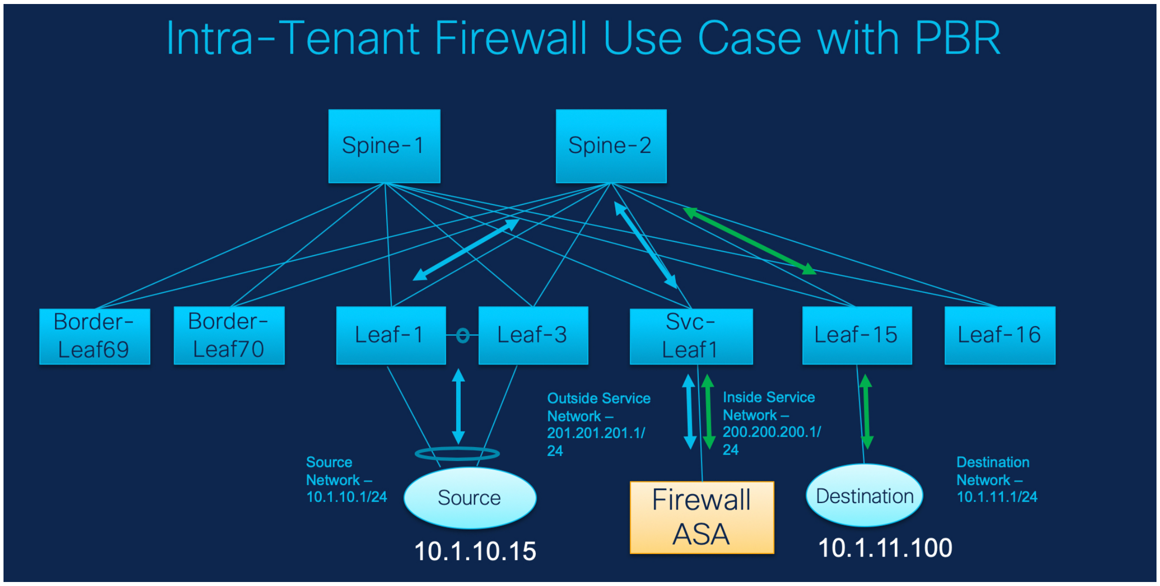
L4-L7 Service Use Cases

Use Case: Intra-tenant Firewall with Policy-based Routing

Refer the figure given below for topology details.



Intra-Tenant Firewall Use Case with PBR
Spine-1
Spine-2
Border-Leaf69
Border-Leaf70
Leaf-1
Leaf-3
Svc-Leaf1
Leaf-15
Leaf-16
Outside Service Network – 201.201.201.1/24
Inside Service Network – 200.200.200.1/24
Source Network – 10.1.10.1/24
Source
10.1.10.15
Firewall ASA
Destination
10.1.11.100
Destination Network – 10.1.11.1/24

In this topology, Leaf1 and Leaf3 are a vPC pair and they are connected to **Source** (10.1.10.15) with the **Source Network** (10.1.10.1/24). The service leaf is connected to the virtual **Firewall ASA** and Leaf-15 is connected to **Destination** (10.1.11.100). In this use case, the source network refers to 'client' and the destination refers to 'server'.

Any traffic that is traversing from **Source** to **Destination** must go to the outside service network, and the firewall performs its function by allowing or denying traffic. This traffic is then routed to the inside service network and on to the Destination network. Since the topology is stateful, the traffic coming back from the destination to the source follows the same path.

Now, let us see how to perform service redirection in DCNM.

Note

- This use-case does not cover how to provision the **Site_A** VXLAN fabric. For information about this topic, refer to the Cisco DCNM LAN Fabric Configuration Guide.
- This use-case does not cover configurations on the service node (firewall or load balancer).

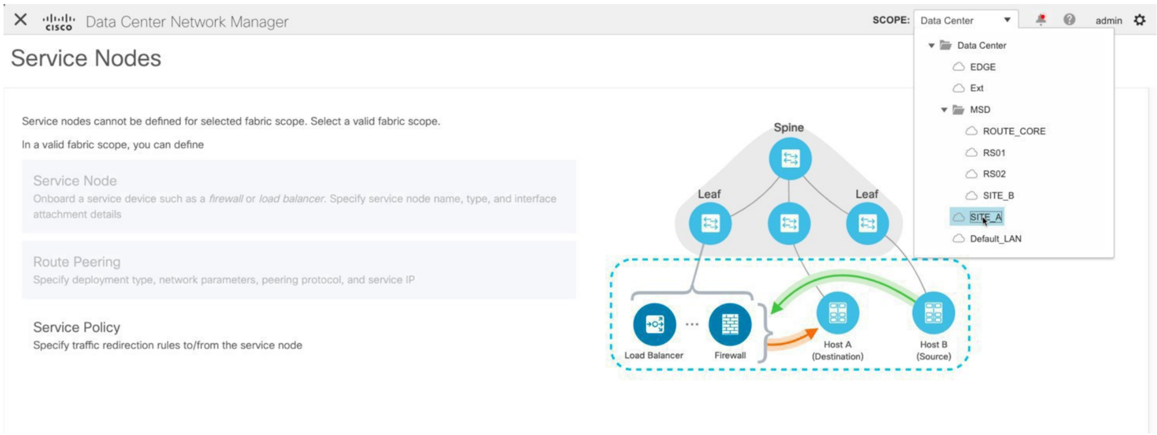
Select **Control** > **Fabrics** > **Services**.

This use-case consists of the following steps:

1. Create Service Node

Procedure

Step 1 From the **Scope** drop-down list, select **Site_A**.



Service Nodes

Service nodes cannot be defined for selected fabric scope. Select a valid fabric scope.

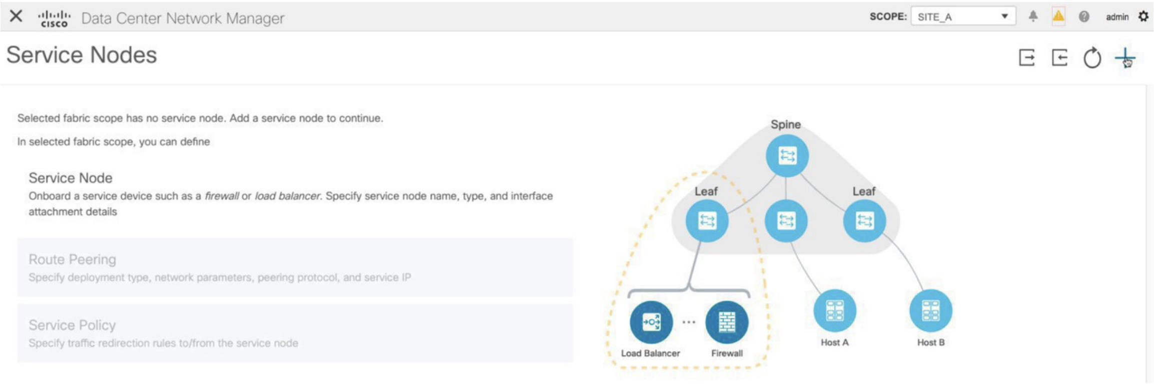
In a valid fabric scope, you can define

Service Node
Onboard a service device such as a *firewall* or *load balancer*. Specify service node name, type, and interface attachment details

Route Peering
Specify deployment type, network parameters, peering protocol, and service IP

Service Policy
Specify traffic redirection rules to/from the service node

Step 2 Click the **Add** icon in the **Service Nodes** window.



Service Nodes

Selected fabric scope has no service node. Add a service node to continue.

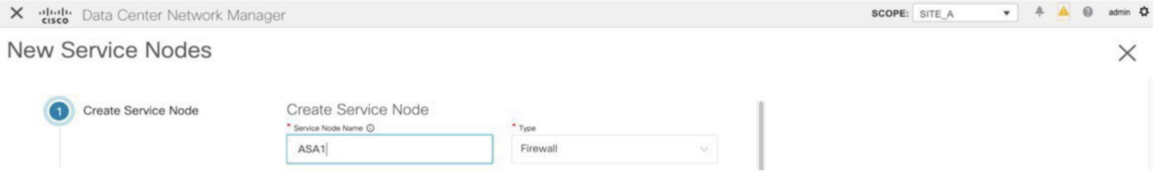
In selected fabric scope, you can define

Service Node
Onboard a service device such as a *firewall* or *load balancer*. Specify service node name, type, and interface attachment details

Route Peering
Specify deployment type, network parameters, peering protocol, and service IP

Service Policy
Specify traffic redirection rules to/from the service node

Step 3 Enter the node name and specify **Firewall** in the **Type** dropdown box. The **Service Node Name** has to be unique.

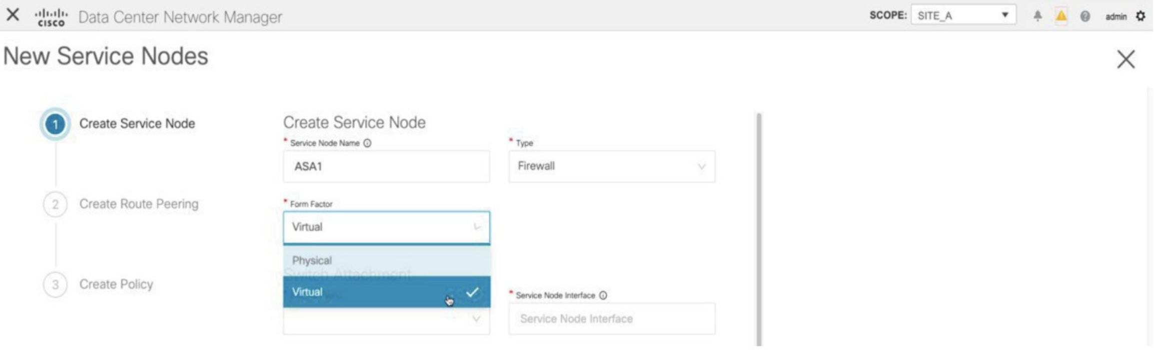


Create Service Node

* Service Node Name: ASA1

* Type: Firewall

Step 4 From the **Form Factor** drop-down list, select **Virtual**.



Create Service Node

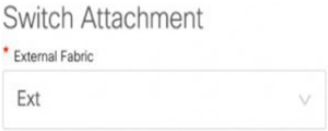
* Service Node Name: ASA1

* Type: Firewall

* Form Factor: Virtual

* Service Node Interface: Service Node Interface

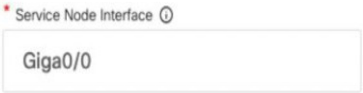
Step 5 In the **Switch Attachment** section, from the **External Fabric** drop-down list, select the external fabric in which the service node (for example, ASA firewall) is located. Note that the service nodes need to belong to the external fabric. This is a prerequisite before creating a service node.



Switch Attachment

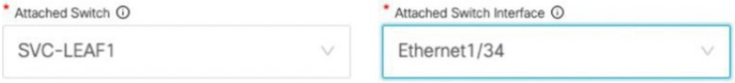
* External Fabric: Ext

Step 6 Enter the interface name of the service node that will be connected to the service leaf.



* Service Node Interface: Giga0/0

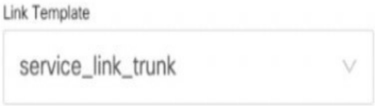
Step 7 Select the attached switch that is the service leaf, and the respective interface on the service leaf.



* Attached Switch: SVC-LEAF1

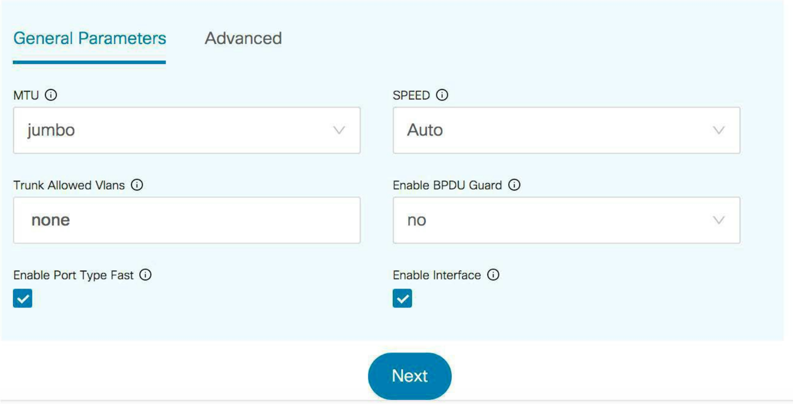
* Attached Switch Interface: Ethernet1/34

Step 8 Select the **service_link_trunk** template. DCNM supports trunk, port channel, and vPC link templates. The available link templates in the **Link Template** drop-down list are filtered based on the selected **Attached Switch Interface** type.



Link Template: service_link_trunk

Step 9 Specify the **General Parameters** and **Advanced** parameters, if required. Some parameters are pre-filled with the default values.



MTU: jumbo

SPEED: Auto

Trunk Allowed Vlans: none

Enable BPDU Guard: no

Enable Port Type Fast ☑

Enable Interface ☑

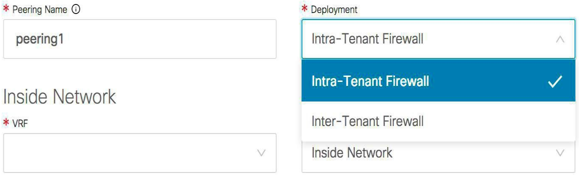
Step 10 Click **Next** to save the created service node.

2. Create Route Peering

Let us now configure the peering between a service leaf and a service node.

Procedure

Step 1 Enter the peering name and select **Intra-Tenant Firewall** from the **Deployment** drop-down list.



* Peering Name: peering1

* Deployment: Intra-Tenant Firewall

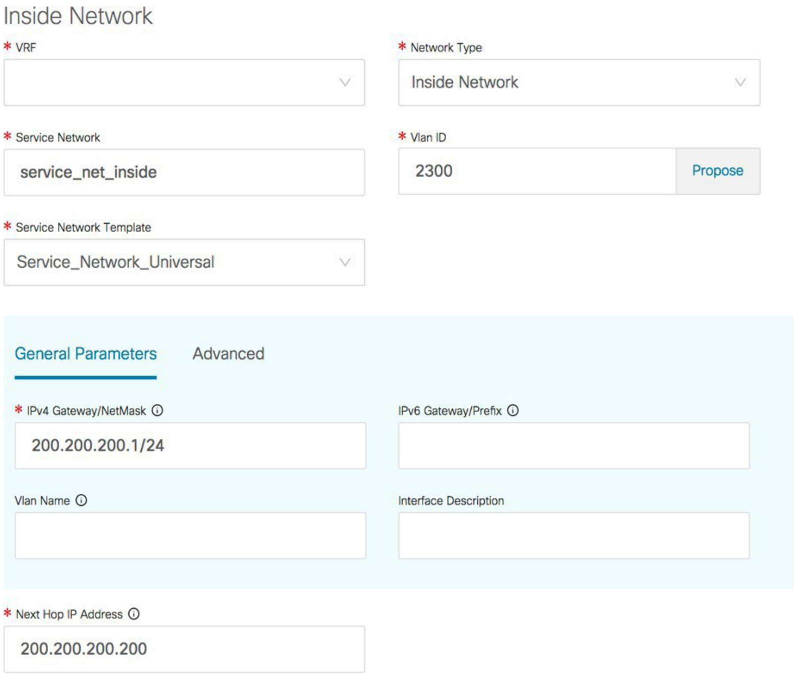
Inside Network

* VRF:

Step 2 Under **Inside Network**, from the **VRF** drop-down list, select a VRF that already exists and select **Inside Network** under **Network Type**.

Enter the name of the **Service Network** and specify the **Vlan ID**. You can also click **Propose** to allow DCNM to fetch the next available VLAN ID from the specified service network VLAN ID range in the fabric settings. The default **Service Network Template** is **Service_Network_Universal**.

Under the **General Parameters** tab, specify the gateway address for the service network. Specify the **Next Hop IP Address**. This next hop address has to be within the ‘inside service network’ subnet. Under the **Advanced** tab, the default **Routing Tag** value is 12345.



Inside Network

* VRF:

* Network Type: Inside Network

* Service Network: service_net_inside

* Vlan ID: 2300

* Service Network Template: Service_Network_Universal

General Parameters

* IPv4 Gateway/NetMask: 200.200.200.1/24

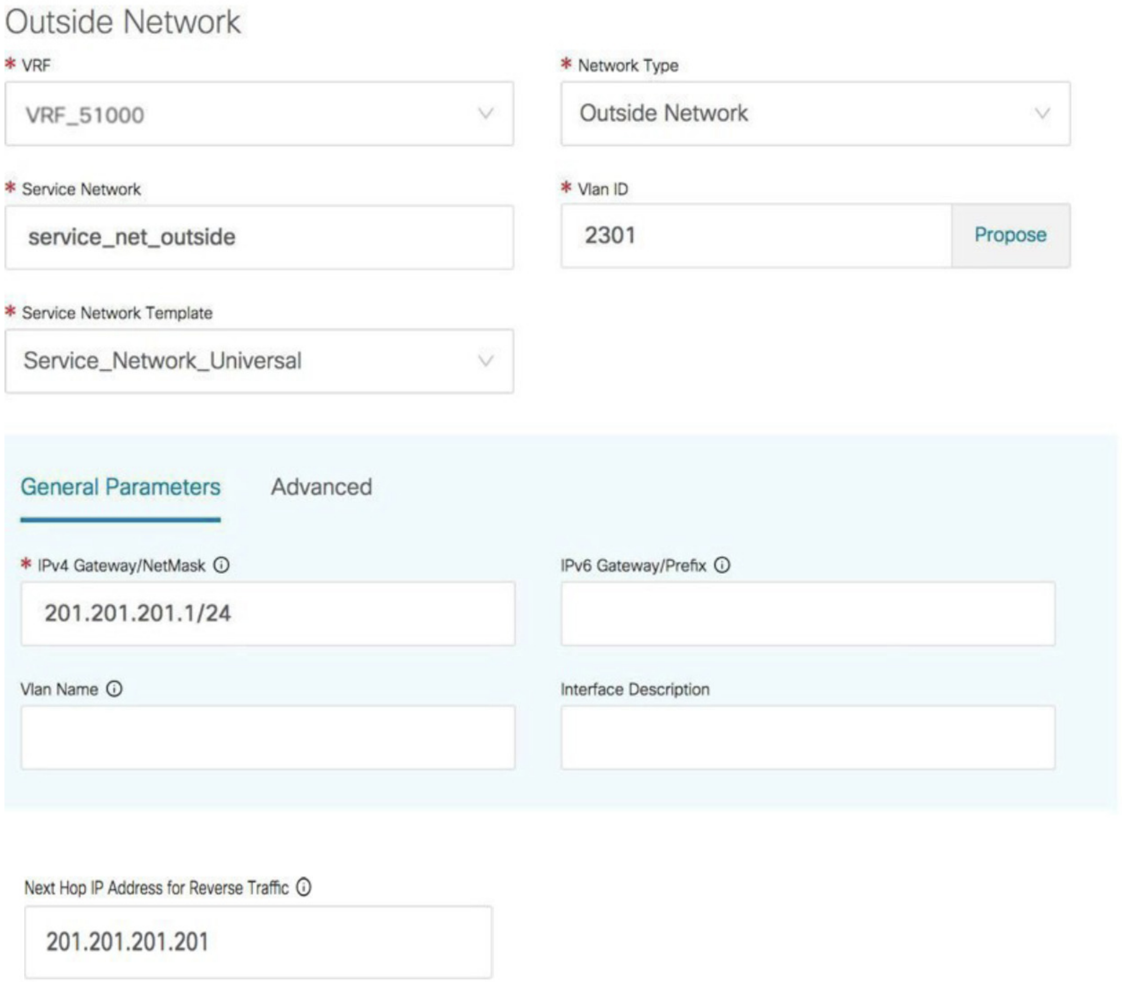
IPv6 Gateway/Prefix:

Vlan Name:

Interface Description:

* Next Hop IP Address: 200.200.200.200

Step 3 Specify the required parameters under **Outside Network** and specify the **Next Hop IP Address for Reverse Traffic**. This next hop address for reverse traffic needs to be within the ‘outside service network’ subnet.



Outside Network

* VRF: VRF_51000

* Network Type: Outside Network

* Service Network: service_net_outside

* Vlan ID: 2301

* Service Network Template: Service_Network_Universal

* IPv4 Gateway/NetMask ⓘ: 201.201.201.1/24

IPv6 Gateway/Prefix ⓘ:

Vlan Name ⓘ:

Interface Description:

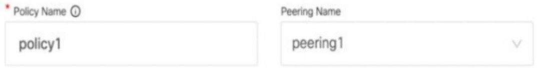
Next Hop IP Address for Reverse Traffic ⓘ: 201.201.201.201

Step 4 Click **Next** to save the created route peering.

3. Create Service Policy

Procedure

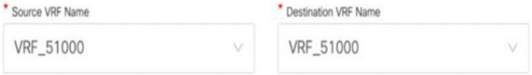
Step 1 Specify a name for the policy and select the route peering from the **Peering Name** drop-down list.



* Policy Name ⓘ: policy1

Peering Name: peering1

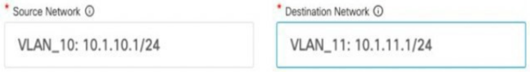
Step 2 Select the source and destination VRFs from the **Source VRF Name** and **Destination VRF Name** drop-down lists. The source and destination VRFs for an intra-tenant firewall deployment have to be the same.



* Source VRF Name: VRF_51000

* Destination VRF Name: VRF_51000

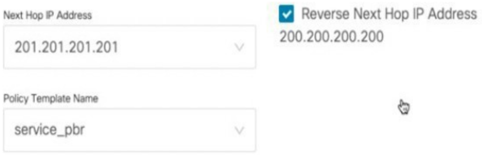
Step 3 Select the source and destination networks from the **Source Network** and **Destination Network** drop-down lists, or specify the source or destination network that is within the network subnets defined in the **Control > Fabrics > Networks** window.



* Source Network: VLAN_10: 10.1.10.1/24

* Destination Network: VLAN_11: 10.1.11.1/24

Step 4 The next hop and reverse next hop fields are populated based on the values entered while creating the route peering. Select the check box next to the **Reverse Next Hop IP Address** field to enable policy enforcement on reverse traffic.



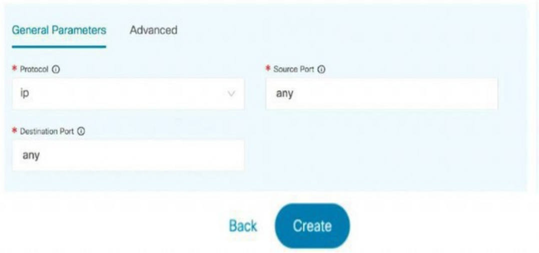
Next Hop IP Address: 201.201.201.201

☑ Reverse Next Hop IP Address: 200.200.200.200

Policy Template Name: service_pbr

Step 5 Under the **General Parameters** tab in the policy template, select **ip** from the **Protocol** dropdown list, and specify **any** in the **Source Port** and the **Destination Port** fields.

Note For **ip** and **icmp** protocols, the **any** source and destination port is always used for ACL generation. You can also select a different protocol and specify the corresponding source and destination ports. DCNM will convert well-known port numbers to match the format required by the switch. For example, you can convert port 80 to ‘www’.

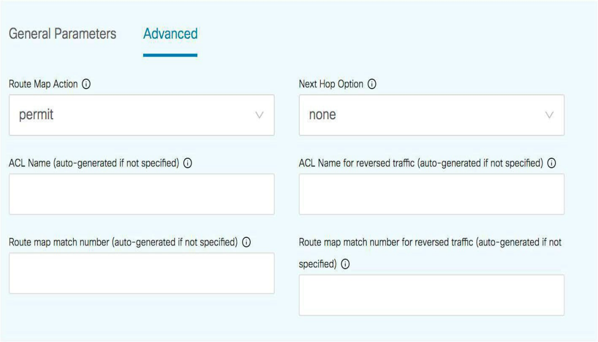


* Protocol: ip

* Source Port: any

* Destination Port: any

Step 6 Under the **Advanced** tab, by default, **permit** is selected for **Route Map Action** and **none** is selected for the **Next Hop Option**. You can change these values, and customize the ACL name and route map match sequence number, if required. For more information, refer Templates in the Layer 4-Layer 7 Service configuration guide.



General Parameters | Advanced

Route Map Action: permit

Next Hop Option: none

ACL Name (auto-generated if not specified):

ACL Name for reversed traffic (auto-generated if not specified):

Route map match number (auto-generated if not specified):

Route map match number for reversed traffic (auto-generated if not specified):

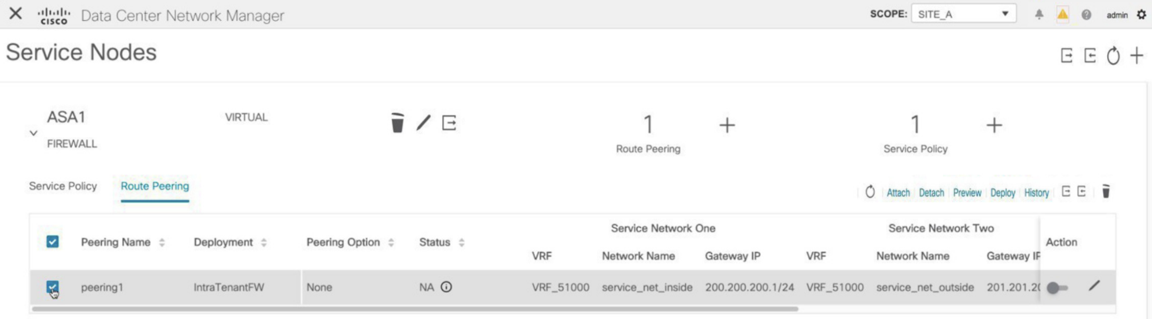
Step 7 Click **Create** to save the created service policy.

This completes the procedures that have to be performed to specify the flows for redirection.

4. Deploy Route Peering

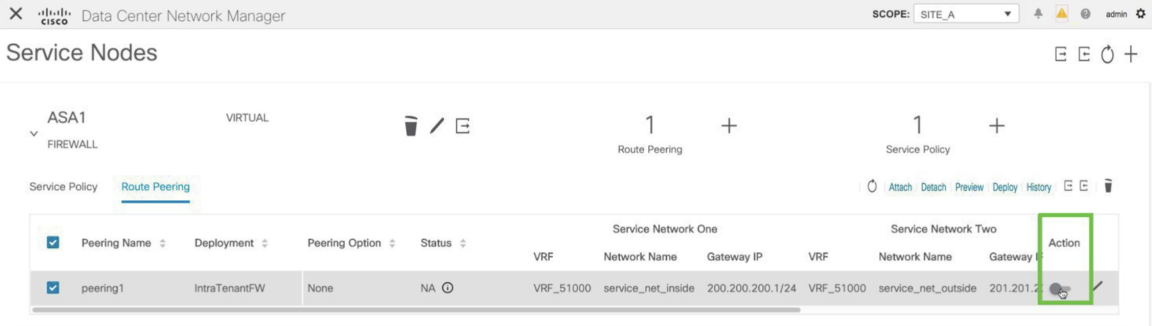
Procedure

Step 1 In the **Service Nodes** window, select the required peering under the **Route Peering** tab.



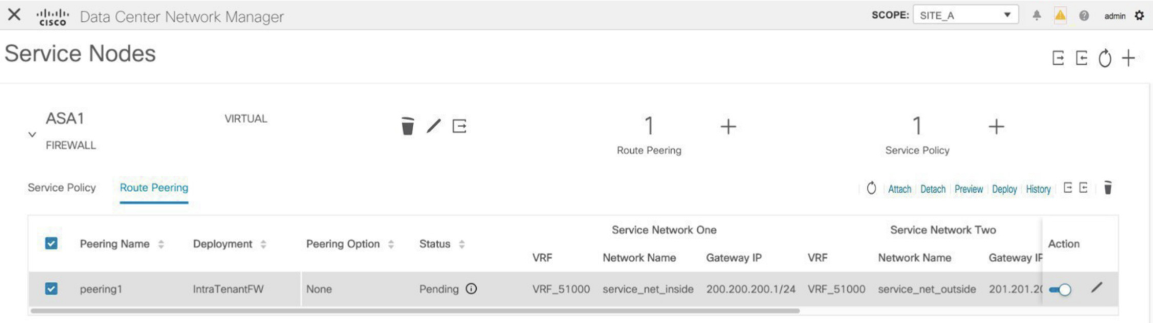
☑	Peering Name	Deployment	Peering Option	Status	Service Network One			Service Network Two			Action
					VRF	Network Name	Gateway IP	VRF	Network Name	Gateway IP	
☑	peering1	IntraTenantFW	None	NA ⓘ	VRF_51000	service_net_inside	200.200.200.1/24	VRF_51000	service_net_outside	201.201.2	

Step 2 Click the toggle button under **Action** to attach service networks to the service leafs.



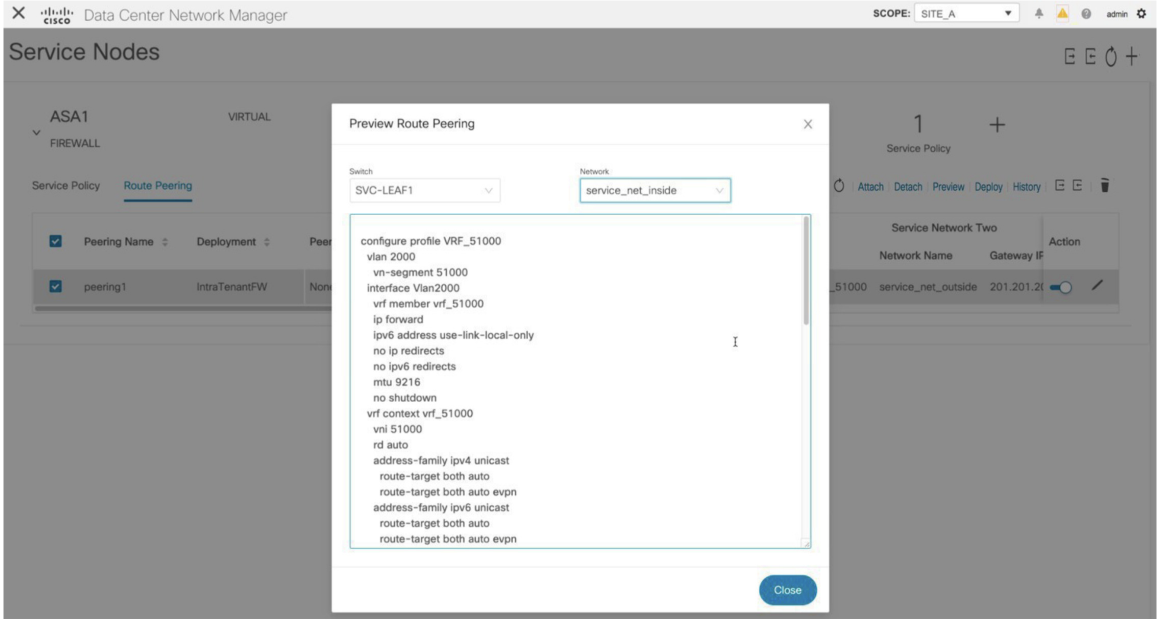
☑	Peering Name	Deployment	Peering Option	Status	Service Network One			Service Network Two			Action
					VRF	Network Name	Gateway IP	VRF	Network Name	Gateway I	
☑	peering1	IntraTenantFW	None	NA ⓘ	VRF_51000	service_net_inside	200.200.200.1/24	VRF_51000	service_net_outside	201.201.2	

Step 3 Click **Preview** to view the configurations that will be pushed to the service leaf.



				Service Network One			Service Network Two			
☑ Peering Name	Deployment	Peering Option	Status	VRF	Network Name	Gateway IP	VRF	Network Name	Gateway IP	Action
☑ peering1	IntraTenantFW	None	Pending ⓘ	VRF_51000	service_net_inside	200.200.200.1/24	VRF_51000	service_net_outside	201.201.2	

Previously, we had created inside and outside service networks. You can view these network configurations that will be pushed to the service leaf.



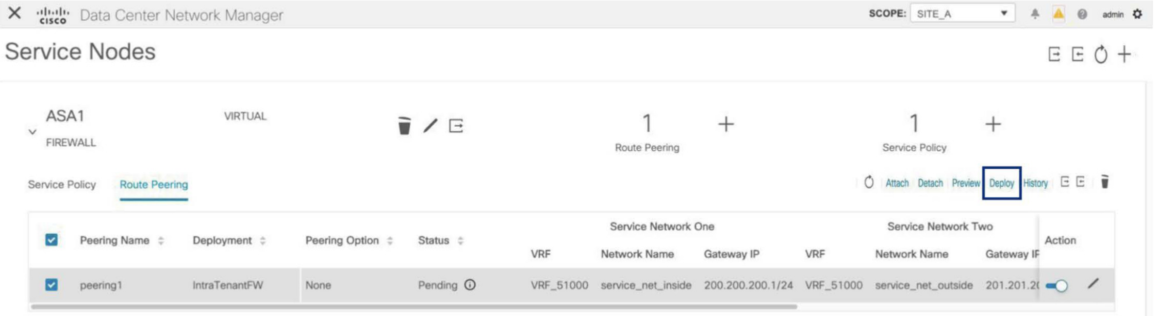
Switch: SVC-LEAF1

Network: service_net_inside

```
configure profile VRF_51000
  vlan 2000
    vn-segment 51000
  interface Vlan2000
    vrf member vrf_51000
    ip forward
    ipv6 address use-link-local-only
    no ip redirects
    no ipv6 redirects
    mtu 9216
    no shutdown
  vrf context vrf_51000
    vni 51000
    rd auto
    address-family ipv4 unicast
      route-target both auto
      route-target both auto evpn
    address-family ipv6 unicast
      route-target both auto
      route-target both auto evpn
```

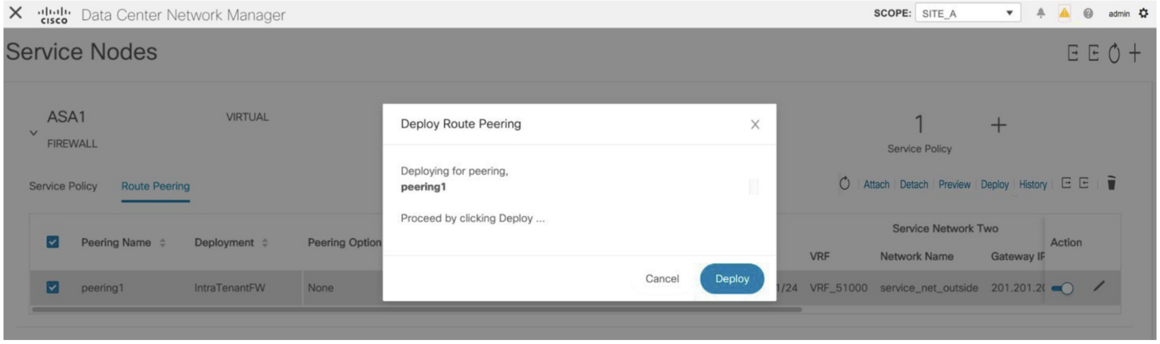
Step 4 Click **Close** to close the **Preview Route Peering** window.

Step 5 Click **Deploy** in the **Service Nodes** window to deploy the configuration to the attached switches (service leaf(s)) for route peering.



				Service Network One			Service Network Two			
☑ Peering Name	Deployment	Peering Option	Status	VRF	Network Name	Gateway IP	VRF	Network Name	Gateway IP	Action
☑ peering1	IntraTenantFW	None	Pending ⓘ	VRF_51000	service_net_inside	200.200.200.1/24	VRF_51000	service_net_outside	201.201.2	

Click the **Deploy** button in the pop-up window to confirm deployment.



Deploy Route Peering

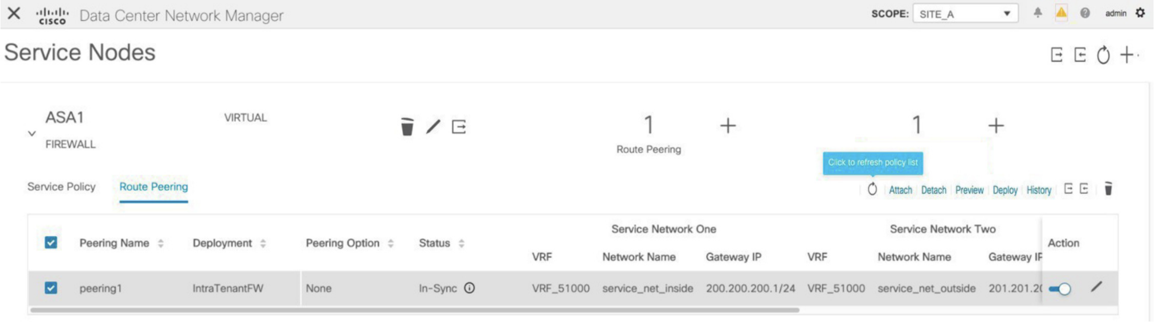
Deploying for peering,
peering1

Proceed by clicking Deploy ...

Cancel | Deploy

☑	Peering Name	Deployment	Peering Option			Service Network Two		Action
					VRF	Network Name	Gateway IP	
☑	peering1	IntraTenantFW	None	1/24	VRF_51000	service_net_outside	201.201.2(	

Step 6 Click the **Refresh** icon for the latest peering configuration attachment and deployment status.



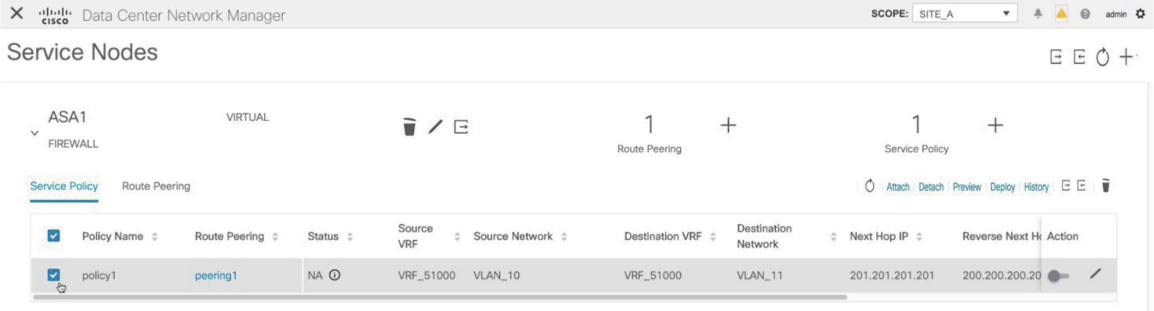
☑	Peering Name	Deployment	Peering Option	Status	Service Network One			Service Network Two			Action
					VRF	Network Name	Gateway IP	VRF	Network Name	Gateway IP	
☑	peering1	IntraTenantFW	None	In-Sync ⓘ	VRF_51000	service_net_inside	200.200.200.1/24	VRF_51000	service_net_outside	201.201.2(	

5. Deploy Service Policy

Perform the following procedure to deploy the service policy. This policy's corresponding configuration will be deployed to the switches that the source and destination network are attached to, and to the service leaf(s).

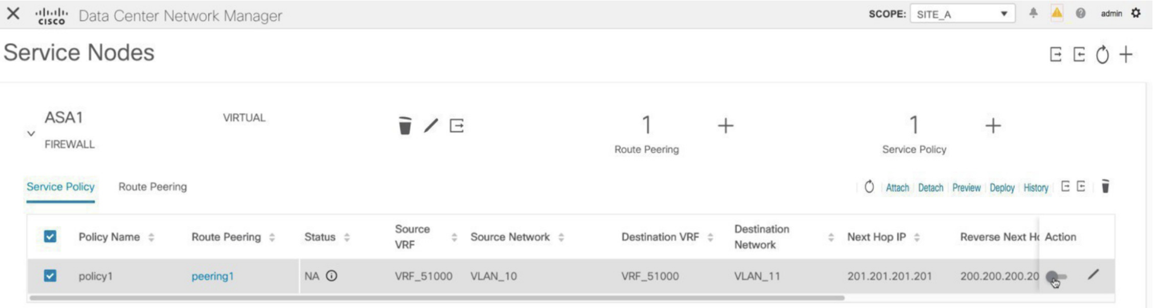
Procedure

Step 1 Select the checkbox next to the required policy under the **Service Policy** tab.



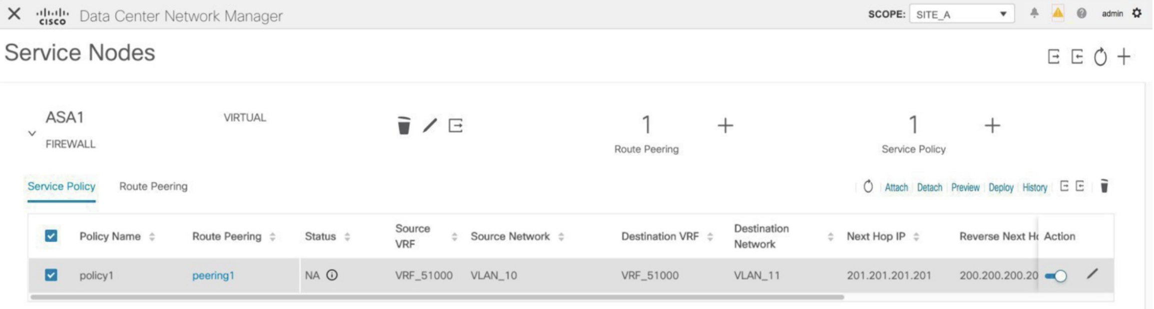
☑	Policy Name	Route Peering	Status	Source VRF	Source Network	Destination VRF	Destination Network	Next Hop IP	Reverse Next H	Action
☑	policy1	peering1	NA ⓘ	VRF_51000	VLAN_10	VRF_51000	VLAN_11	201.201.201.201	200.200.200.20	

Step 2 Click the toggle button under **Action** to enable this policy.



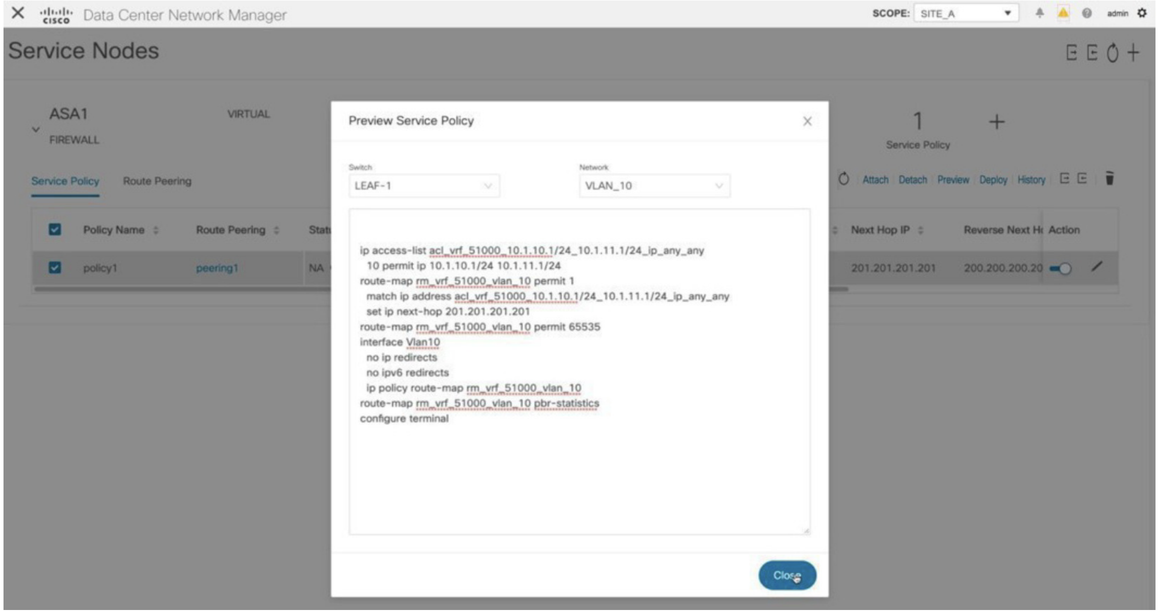
☑	Policy Name	Route Peering	Status	Source VRF	Source Network	Destination VRF	Destination Network	Next Hop IP	Reverse Next H	Action
☑	policy1	peering1	NA	VRF_51000	VLAN_10	VRF_51000	VLAN_11	201.201.201.201	200.200.200.20	

Step 3 Click **Preview** to view the configuration of the selected network.



☑	Policy Name	Route Peering	Status	Source VRF	Source Network	Destination VRF	Destination Network	Next Hop IP	Reverse Next H	Action
☑	policy1	peering1	NA	VRF_51000	VLAN_10	VRF_51000	VLAN_11	201.201.201.201	200.200.200.20	

Step 4 Select a switch and a source, destination, or service network, from the drop-down lists to view the intended configuration of a specific source, destination, or service network, on the selected switch. In this window, you can see that there is an access list that will be created with a route map. This configuration will be pushed to the SVI.



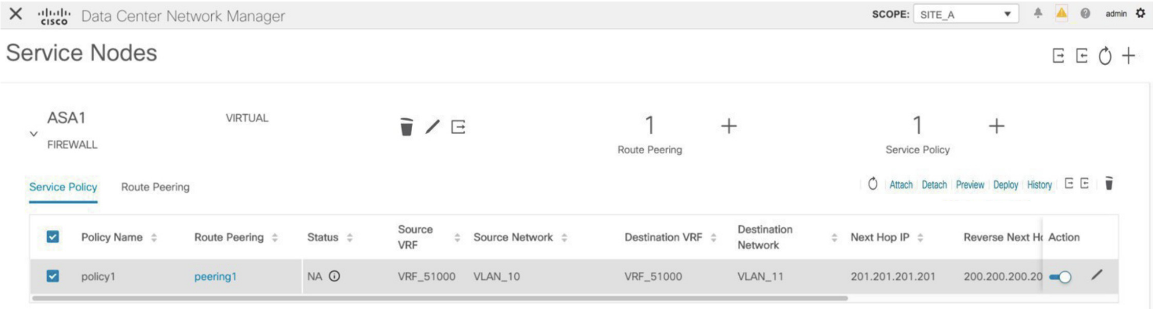
Switch: LEAF-1

Network: VLAN_10

```
ip access-list acl_vrf_51000_10.1.10.1/24_10.1.11.1/24_ip_any_any
  10 permit ip 10.1.10.1/24 10.1.11.1/24
route-map rm_vrf_51000_vlan_10 permit 1
  match ip address acl_vrf_51000_10.1.10.1/24_10.1.11.1/24_ip_any_any
  set ip next-hop 201.201.201.201
route-map rm_vrf_51000_vlan_10 permit 65535
interface Vlan10
  no ip redirects
  no ipv6 redirects
  ip policy route-map rm_vrf_51000_vlan_10
route-map rm_vrf_51000_vlan_10 pbr-statistics
configure terminal
```

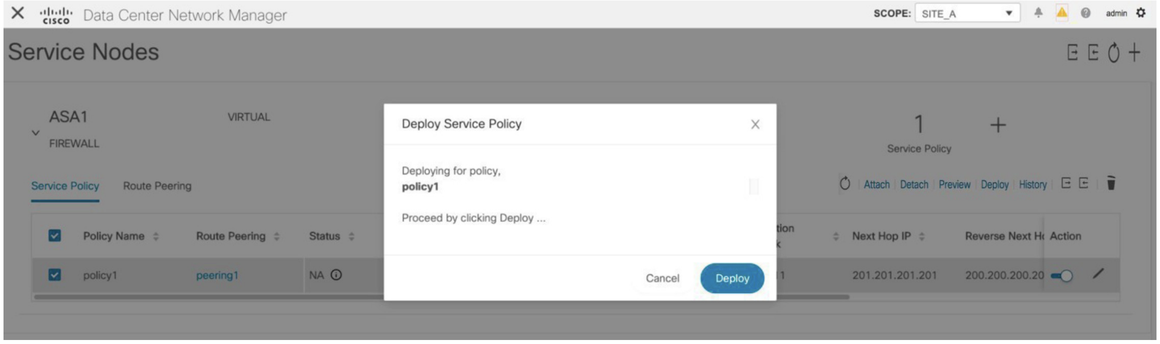
Click **Close** to close the Preview Service Policy window.

Step 5 Click **Deploy** in the **Service Nodes** window to deploy the configuration to the attached switches (service leaf(s)).



Policy Name	Route Peering	Status	Source VRF	Source Network	Destination VRF	Destination Network	Next Hop IP	Reverse Next H	Action
policy1	peering1	NA	VRF_51000	VLAN_10	VRF_51000	VLAN_11	201.201.201.201	200.200.200.20	

Click the **Deploy** button in the pop-up window to confirm deployment.



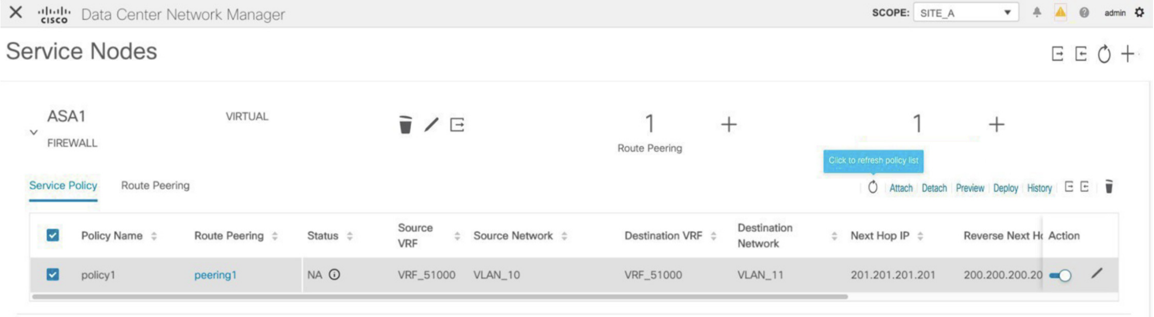
Deploy Service Policy

Deploying for policy,
policy1

Proceed by clicking Deploy ...

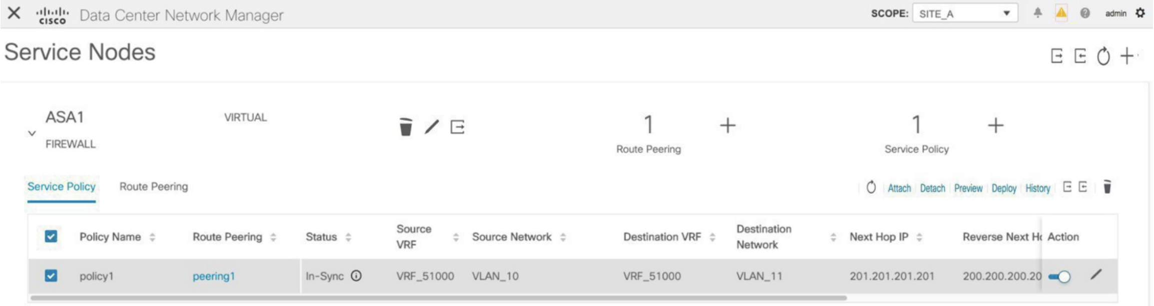
Policy Name	Route Peering	Status	tion	Next Hop IP	Reverse Next H	Action
policy1	peering1	NA		201.201.201.201	200.200.200.20	

Step 6 Click the **Refresh** icon for the latest policy attachment and deployment status.



Policy Name	Route Peering	Status	Source VRF	Source Network	Destination VRF	Destination Network	Next Hop IP	Reverse Next H	Action
policy1	peering1	NA	VRF_51000	VLAN_10	VRF_51000	VLAN_11	201.201.201.201	200.200.200.20	

This policy will be pushed to the switches that the source and destination networks are attached to, as well as the service leaf(s). After pushing the policy, the status column shows **In-Sync**.

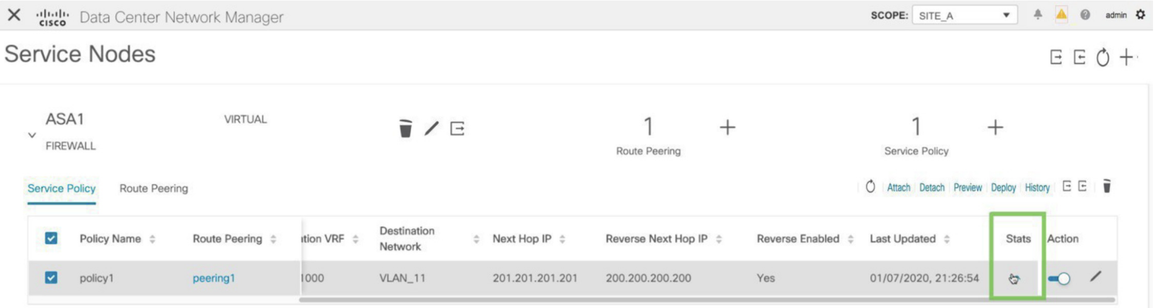


Policy Name	Route Peering	Status	Source VRF	Source Network	Destination VRF	Destination Network	Next Hop IP	Reverse Next H	Action
policy1	peering1	In-Sync	VRF_51000	VLAN_10	VRF_51000	VLAN_11	201.201.201.201	200.200.200.20	

6. View Stats

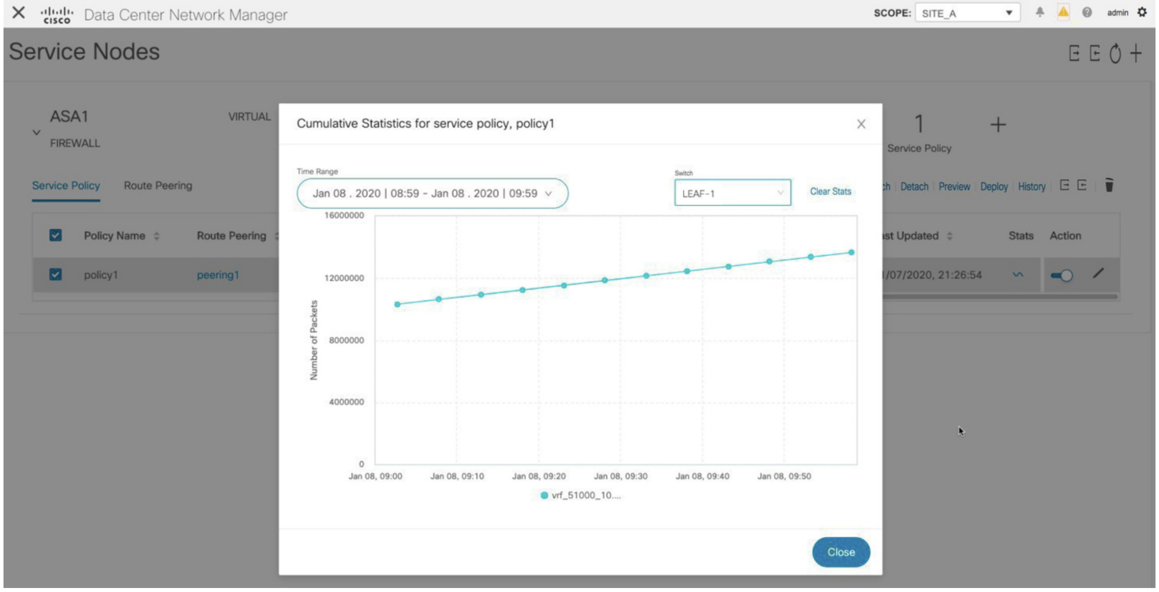
Now that the respective redirection policies are deployed, ping traffic will be redirected to the firewall.

To visualize this scenario in DCNM, click the icon under the **Stats** column.



Policy Name	Route Peering	tion VRF	Destination Network	Next Hop IP	Reverse Next Hop IP	Reverse Enabled	Last Updated	Stats	Action
policy1	peering1	l000	VLAN_11	201.201.201.201	200.200.200.200	Yes	01/07/2020, 21:26:54		

You can view the cumulative statistics for a policy in a specified time range.



Cumulative Statistics for service policy, policy1

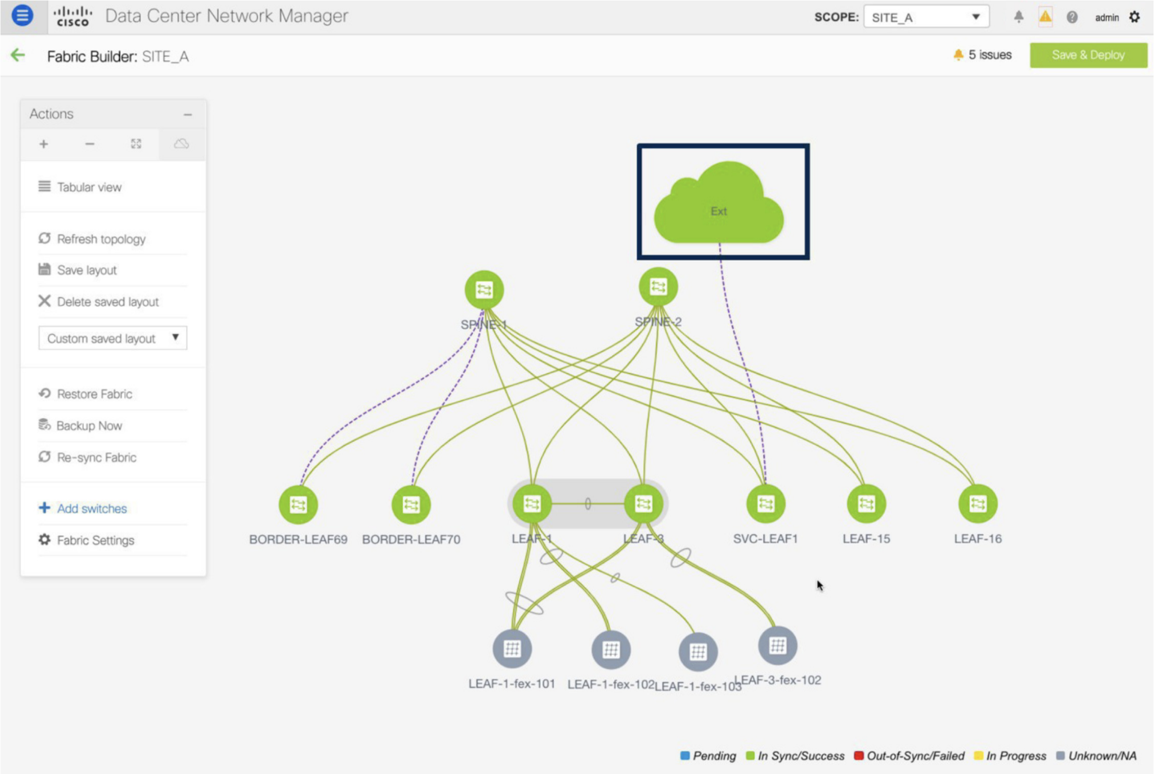
Time Range: Jan 08 . 2020 | 08:59 - Jan 08 . 2020 | 09:59

Switch: LEAF-1

Statistics are displayed for forwarding traffic on the source switch, for reversed traffic on the destination switch, and for traffic in both directions on the service switch.

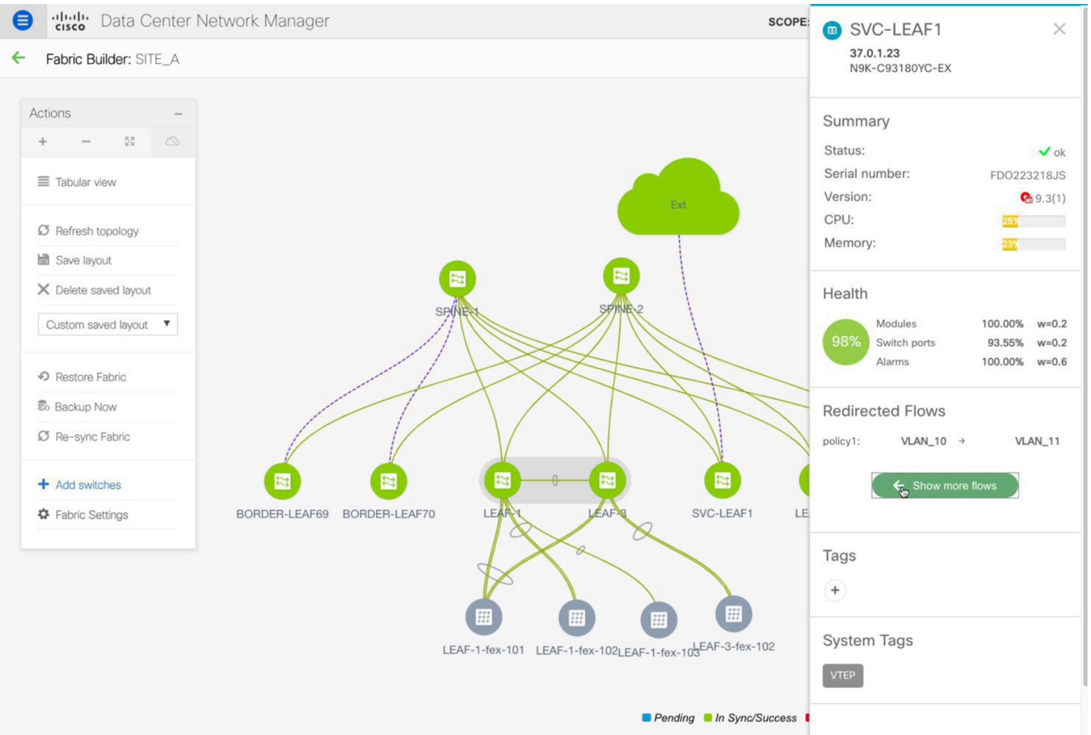
7. View Traffic Flow in Fabric Builder

The service node in the external fabric is attached to the service leaf, and this external fabric is shown as a cloud icon in the DCNM topology in the fabric builder.



Procedure

Step 1 Click the service leaf and click **Show more flows**. You can see the flows that have been redirected.



SVC-LEAF1

37.0.1.23

N9K-C93180YC-EX

Summary

Status: ✓ ok

Serial number: FDO223218JS

Version: 9.3(1)

CPU: 25%

Memory: 23%

Health

98%

Modules	100.00%	w=0.2
Switch ports	93.55%	w=0.2
Alarms	100.00%	w=0.6

Redirected Flows

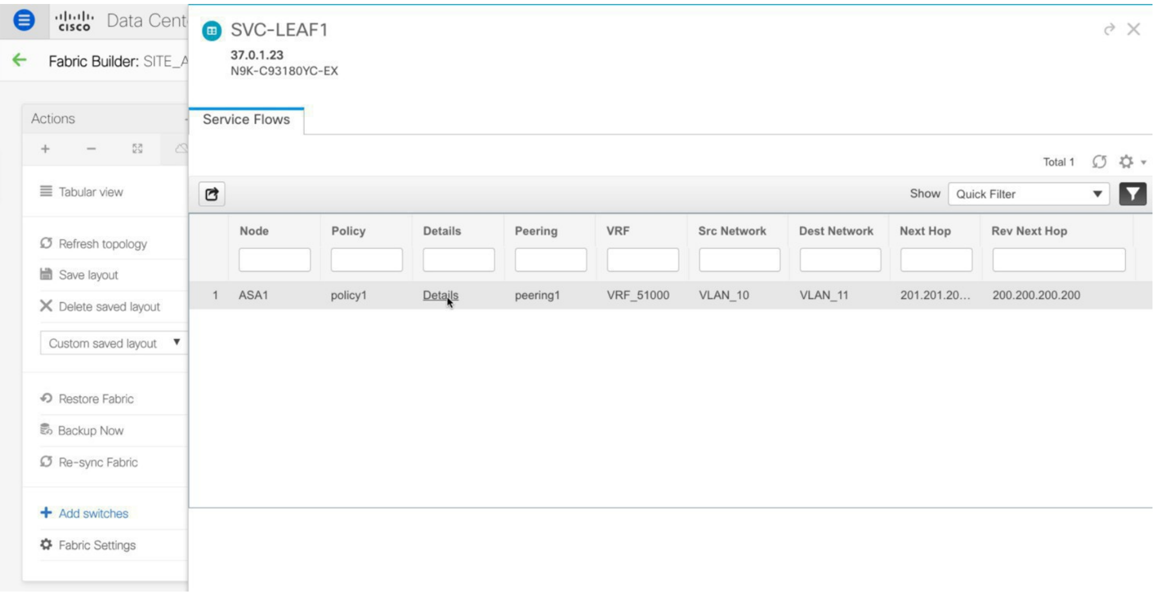
policy1: VLAN_10 → VLAN_11

Tags

System Tags

VTEP

Step 2 Click **Details** in the **Service Flows** window to display attachment details.



SVC-LEAF1

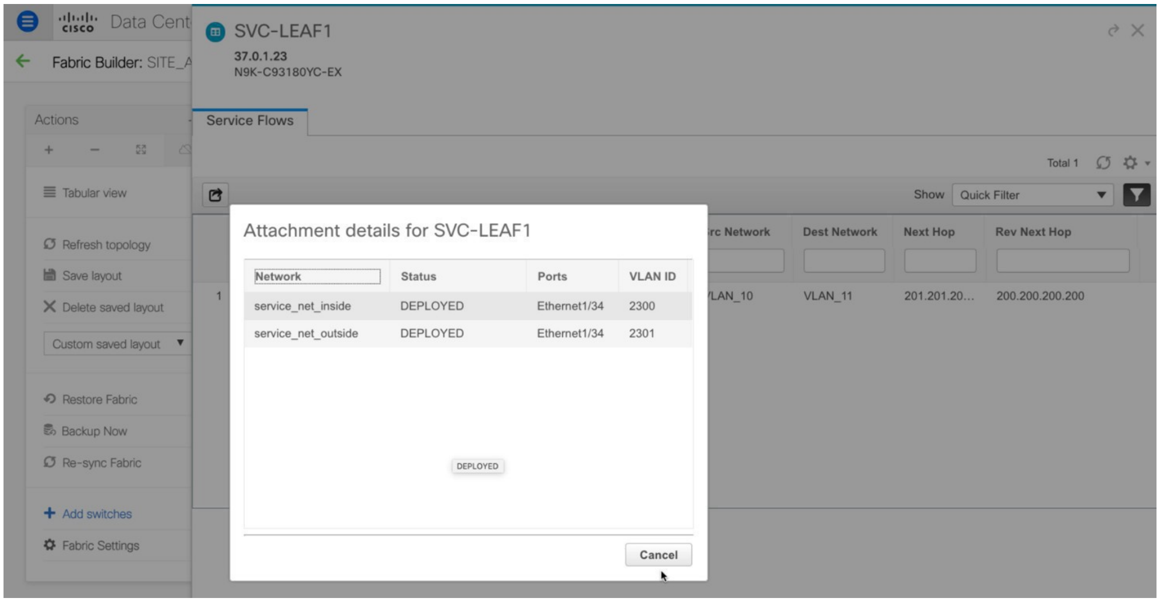
37.0.1.23

N9K-C93180YC-EX

Service Flows

Total 1

	Node	Policy	Details	Peering	VRF	Src Network	Dest Network	Next Hop	Rev Next Hop
1	ASA1	policy1	Details	peering1	VRF_51000	VLAN_10	VLAN_11	201.201.20...	200.200.200.200



	rc Network	Dest Network	Next Hop	Rev Next Hop
1	/LAN_10	VLAN_11	201.201.20...	200.200.200.200

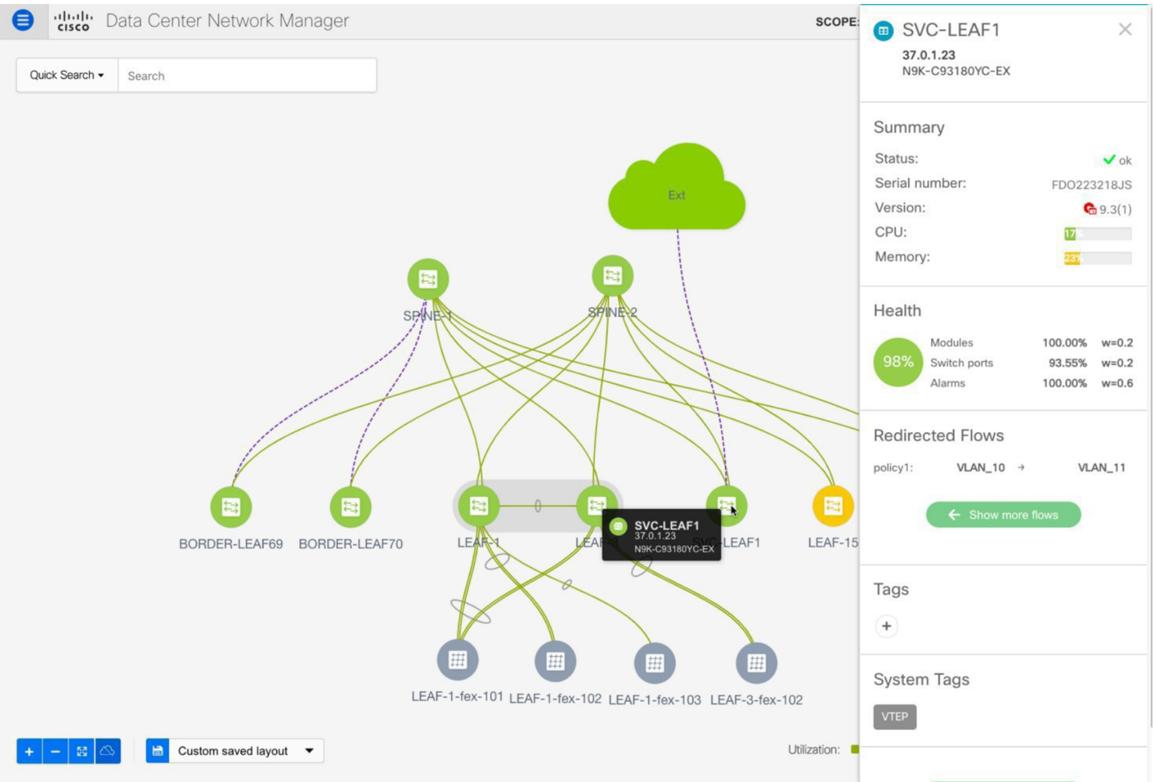
Attachment details for SVC-LEAF1

Network	Status	Ports	VLAN ID
service_net_inside	DEPLOYED	Ethernet1/34	2300
service_net_outside	DEPLOYED	Ethernet1/34	2301

8. Visualize Redirected Flows to Destination in the Topology window

Procedure

Step 1 Click **Topology** and click on leafs to visualize the redirected flows to destination.



SVC-LEAF1

37.0.1.23

N9K-C93180YC-EX

Summary

Status: ✓ ok

Serial number: FDO223218JS

Version: 9.3(1)

CPU: 17%

Memory: 23%

Health

98%

Modules	100.00%	w=0.2
Switch ports	93.55%	w=0.2
Alarms	100.00%	w=0.6

Redirected Flows

policy1: VLAN_10 → VLAN_11

Show more flows

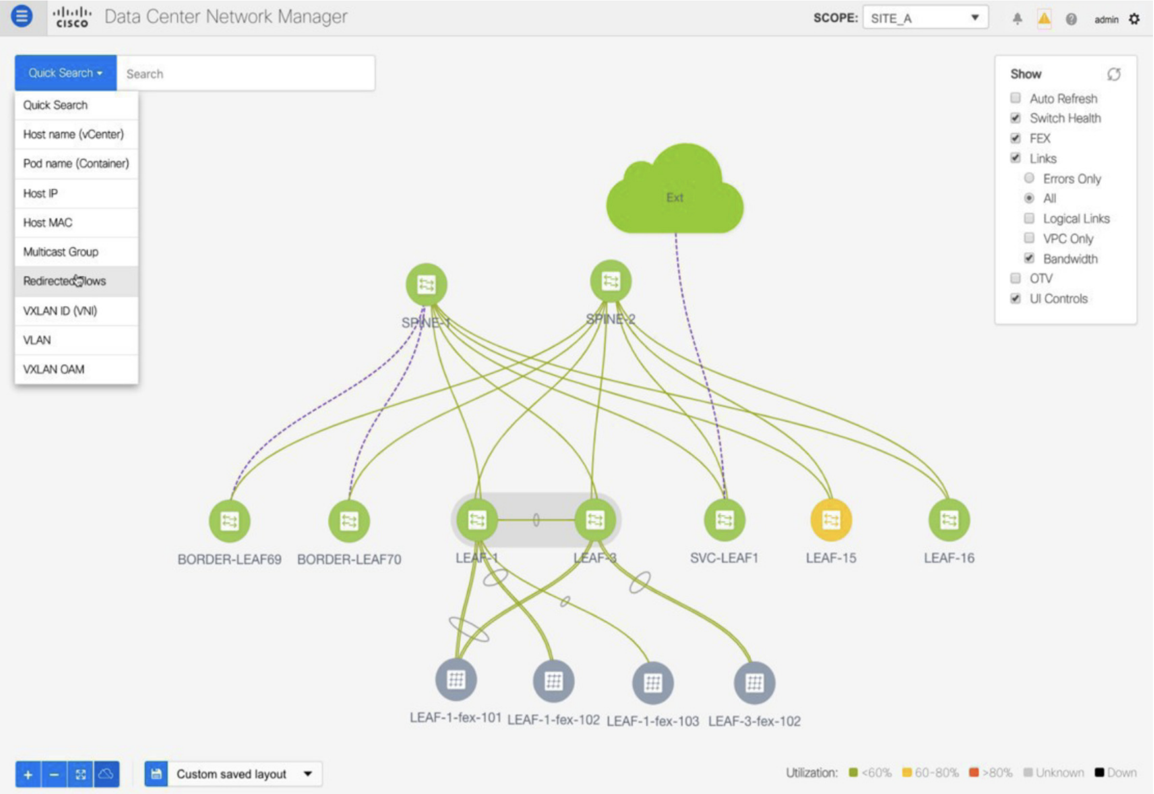
Tags

+

System Tags

VTEP

Step 2 Select **Redirected Flows** from the drop-down list.

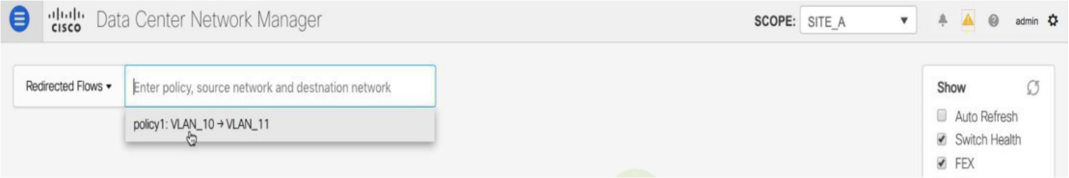


Show

- ☐ Auto Refresh
- ☑ Switch Health
- ☑ FEX
- ☑ Links
  - ○ Errors Only
  - ● All
  - ☐ Logical Links
  - ☐ VPC Only
  - ☑ Bandwidth
- ☐ OTV
- ☑ UI Controls

Utilization: 🟩 <60% 🟨 60-80% 🟥 >80% ▨ Unknown ■ Down

Step 3 Select a policy from the drop-down list or initiate a search by entering a policy name, source network and destination network in the search field. The search field is autopopulated based on your input.

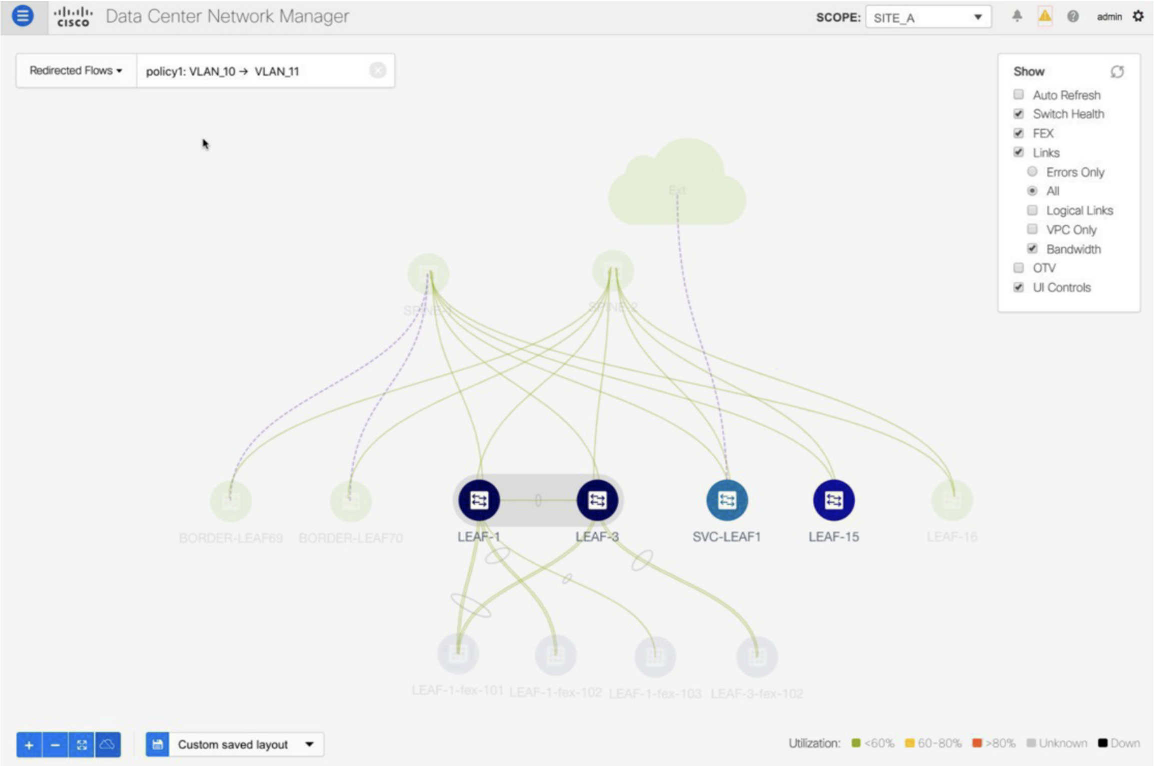


Enter policy, source network and destnation network

policy1: VLAN_10 → VLAN_11

Show
- □ Auto Refresh
- ☑ Switch Health
- ☑ FEX

The switches, on which the source and destination network have been attached and the flows have been redirected, are highlighted.

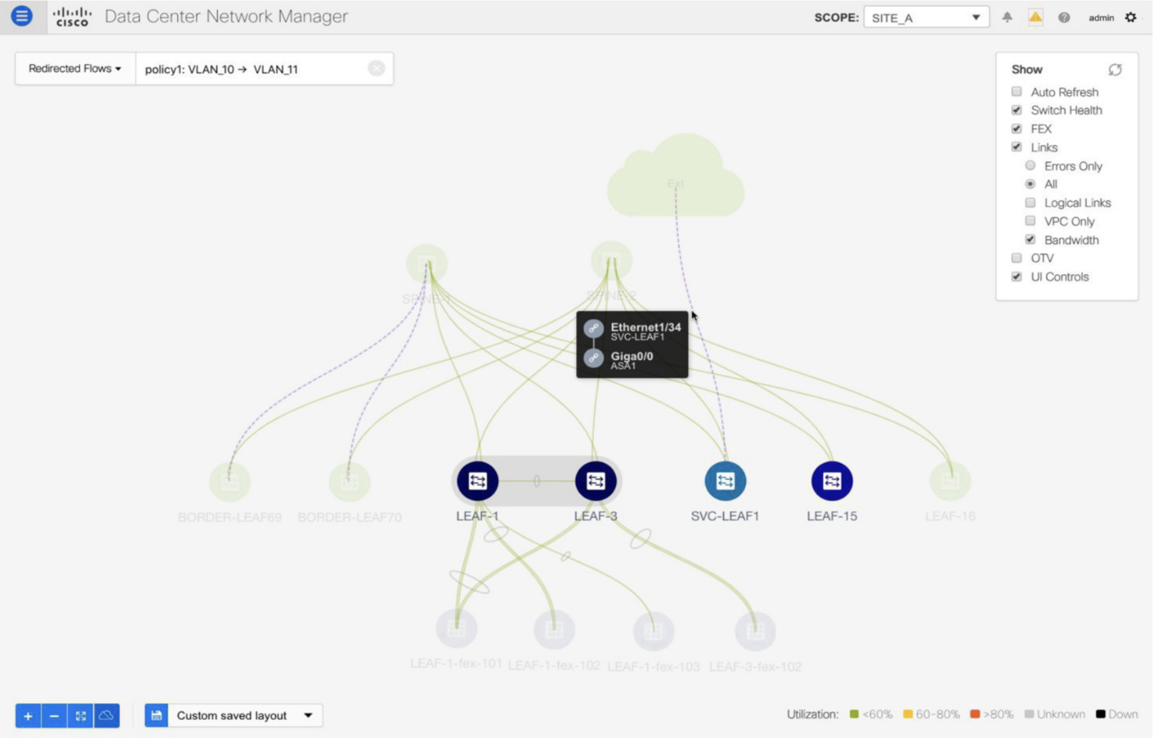


policy1: VLAN_10 → VLAN_11

Show
- □ Auto Refresh
- ☑ Switch Health
- ☑ FEX
- ☑ Links
  - ○ Errors Only
  - ● All
  - □ Logical Links
  - □ VPC Only
  - ☑ Bandwidth
- □ OTV
- ☑ UI Controls

Utilization: 🟩 <60% 🟨 60-80% 🟥 >80% ▨ Unknown ■ Down

Step 4 The service node is shown as connected by a dotted line to the leaf switch on the topology window. Hover over the dotted line to get more information about the interface.



Show

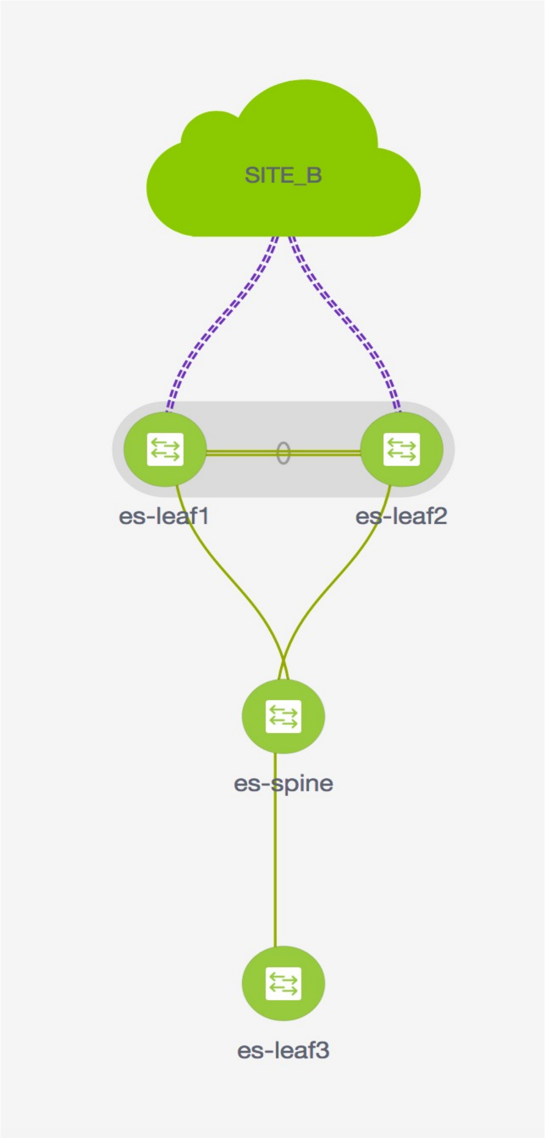
- ☐ Auto Refresh
- ☑ Switch Health
- ☑ FEX
- ☑ Links
  - ○ Errors Only
  - ● All
  - ☐ Logical Links
  - ☐ VPC Only
  - ☑ Bandwidth
- ☐ OTV
- ☑ UI Controls

The traffic from **Source** traverses to the service leaf where the firewall is configured.

Based on firewall rules, traffic is allowed to reach the destination, Leaf 15.

Use Case: Inter-tenant Firewall with eBGP Peering

Refer the figure given below for topology details.



In this topology, es-leaf1 and es-leaf2 are vPC border leaf switches.

Now, let us see how to perform service redirection in DCNM.

Select **Control** > **Fabrics** > **Services**.

This use-case consists of the following steps:

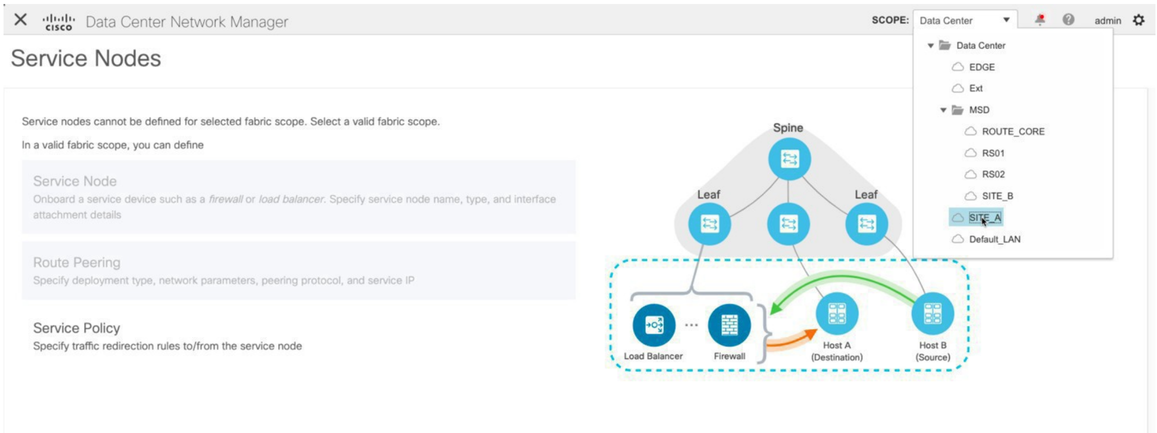
Note

- As some steps are similar to the steps given in the Intra-tenant Firewall deployment use- case, reference links have been provided to the steps in that use-case.
- Service policies are not applicable on Inter-tenant firewall deployments.

1. Create Service Node

Procedure

Step 1 From the **Scope** drop-down list, select **Site_A**.



Service nodes cannot be defined for selected fabric scope. Select a valid fabric scope.

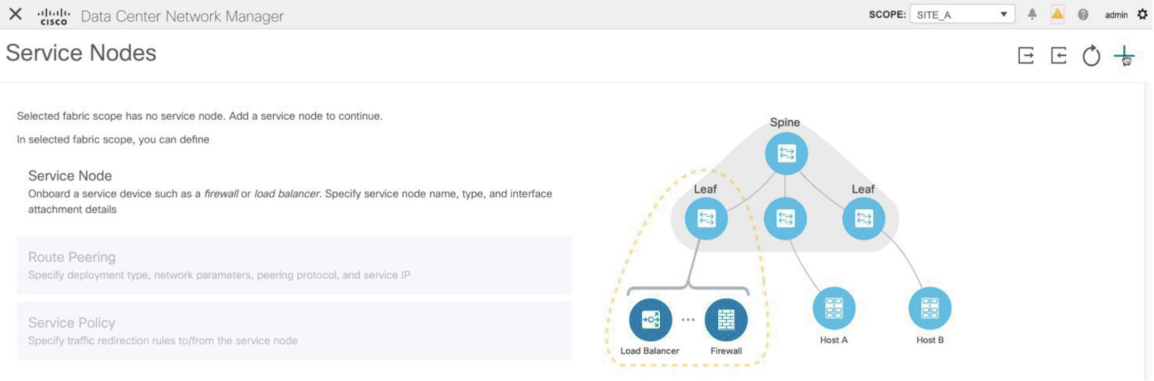
In a valid fabric scope, you can define

Service Node
Onboard a service device such as a *firewall* or *load balancer*. Specify service node name, type, and interface attachment details

Route Peering
Specify deployment type, network parameters, peering protocol, and service IP

Service Policy
Specify traffic redirection rules to/from the service node

Step 2 Click the **Add** icon in the **Service Nodes** window.



Selected fabric scope has no service node. Add a service node to continue.

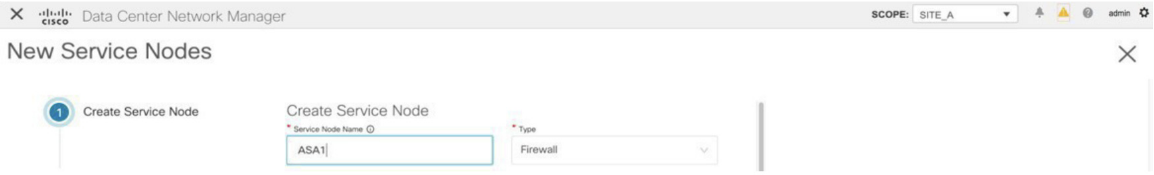
In selected fabric scope, you can define

Service Node
Onboard a service device such as a *firewall* or *load balancer*. Specify service node name, type, and interface attachment details

Route Peering
Specify deployment type, network parameters, peering protocol, and service IP

Service Policy
Specify traffic redirection rules to/from the service node

Step 3 Enter the node name and specify **Firewall** in the **Type** dropdown box. The **Service Node Name** has to be unique.

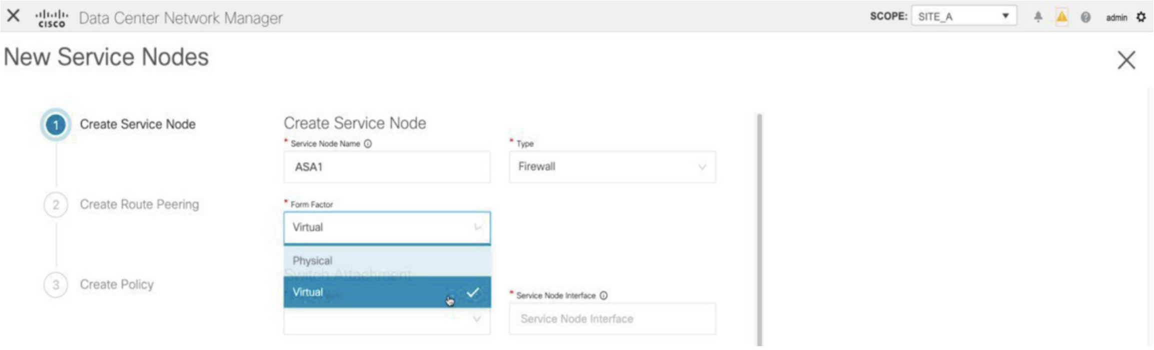


Create Service Node

* Service Node Name: ASA1

* Type: Firewall

Step 4 From the **Form Factor** drop-down list, select **Virtual**.



New Service Nodes

1 Create Service Node
2 Create Route Peering
3 Create Policy

Create Service Node

* Service Node Name: ASA1

* Type: Firewall

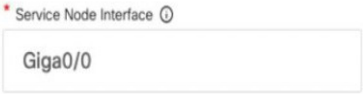
* Form Factor: Virtual

Physical
Virtual ✓

* Service Node Interface: Service Node Interface

Step 5 In the **Switch Attachment** section, from the **External Fabric** drop-down list, select the external fabric in which the service node (for example, ASA firewall) is located. Note that the service nodes need to belong to the external fabric. This is a prerequisite before creating a service node.

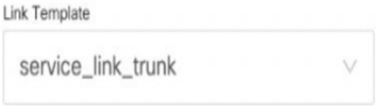
Step 6 Enter the interface name of the service node that will be connected to the service leaf.



* Service Node Interface: Giga0/0

Step 7 Select the attached switch that is the service leaf, and the respective interface on the service leaf.

Step 8 Select the **service_link_trunk** template. DCNM supports trunk, port channel, and vPC link templates. The available link templates in the **Link Template** drop-down list are filtered based on the selected **Attached Switch Interface** type.



Link Template: service_link_trunk

Step 9 Specify the **General Parameters** and **Advanced** parameters, if required. Some parameters are pre-filled with the default values.

Step 10 Click **Next** to save the created service node.

Note For more sample screenshots, refer 1. Create Service Node, on page 2 in the Intra-tenant firewall with policy-based routing use case.

2. Create Route Peering

Let us now configure the peering between a service leaf and a service node.

Procedure

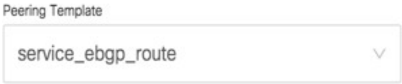
Step 1 Enter the peering name and select **Inter-Tenant Firewall** from the **Deployment** drop-down list. From the **Peering Option** drop-down list, select **eBGP Dynamic Peering**.

Step 2 Under **Inside Network**, from the **VRF** drop-down list, select a VRF that already exists and select **Inside Network** under **Network Type**.

Enter the name of the **Service Network** and specify the **Vlan ID**. You can also click **Propose** to allow DCNM to fetch the next available VLAN ID from the specified service network VLAN ID range in the fabric settings. The default **Service Network Template** is **Service_Network_Universal**.

Under the **General Parameters** tab, specify the gateway address for the service network. Specify the **Next Hop IP Address**. This next hop address has to be within the 'inside service network' subnet. Under the **Advanced** tab, the default **Routing Tag** value is 12345.

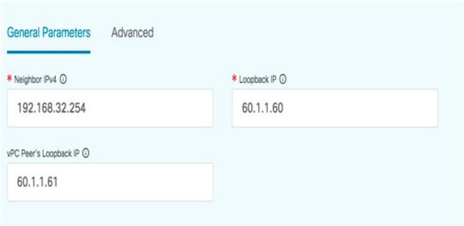
Step 3 The default Peering Template for eBGP dynamic peering is **service_ebgp_route**.



Peering Template

service_ebgp_route

Under the **General Parameters** tab, specify the **Neighbor IPv4** address, **Loopback IP** address, and the **vPC Peer's Loopback IP** address. The border switches are a vPC pair.



General Parameters | Advanced

* Neighbor IPv4: 192.168.32.254

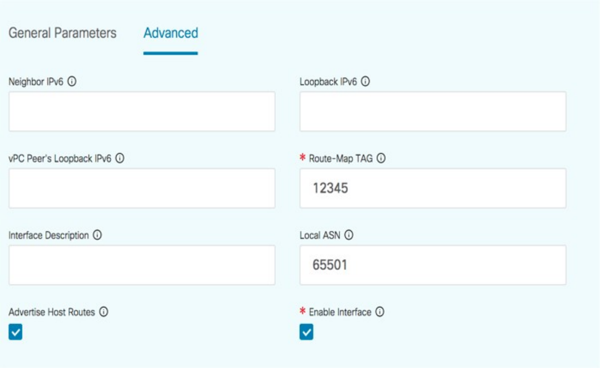
* Loopback IP: 60.1.1.60

vPC Peer's Loopback IP: 60.1.1.61

Step 4 Under the **Advanced** tab, specify the **Local ASN** and select the **Advertise Host Routes** checkbox. This local ASN value is used to override the system ASN on the switch and is required to avoid routing loops.

If the **Advertise Host Routes** checkbox is selected, the /32 and /128 routes are advertised. If this checkbox is not selected, the prefix routes will be advertised.

By default, the **Enable Interface** checkbox is selected.



General Parameters | Advanced

Neighbor IPv6:

Loopback IPv6:

vPC Peer's Loopback IPv6:

* Route-Map TAG: 12345

Interface Description:

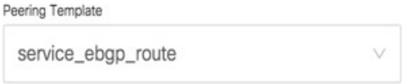
Local ASN: 65501

Advertise Host Routes ☑

* Enable Interface ☑

Step 5 Specify the required parameters under **Outside Network** and specify the **Next Hop IP Address for Reverse Traffic**. This next hop address for reverse traffic needs to be within the 'outside service network' subnet.

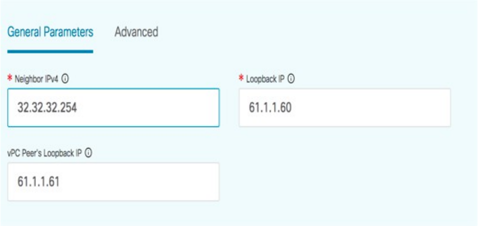
Step 6 The default Peering Template for eBGP dynamic peering is **service_ebgp_route**.



Peering Template

service_ebgp_route

Under the **General Parameters** tab, **Neighbor IPv4** address, **Loopback IP** address, and the **vPC Peer's Loopback IP** address. The leaf switches are a vPC pair.



* Neighbor IPv4: 32.32.32.254

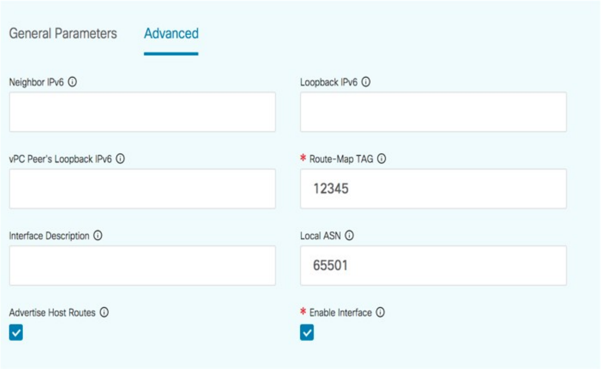
* Loopback IP: 61.1.1.60

vPC Peer's Loopback IP: 61.1.1.61

Step 7 Under the **Advanced** tab, specify the **Local ASN** and select the **Advertise Host Routes** checkbox. This local ASN value is used to override the system ASN on the switch and is required to avoid routing loops.

If the **Advertise Host Routes** checkbox is selected, the /32 and /128 routes are advertised. If this checkbox is not selected, the prefix routes will be advertised.

By default, the **Enable Interface** checkbox is selected.



Neighbor IPv6:

Loopback IPv6:

vPC Peer's Loopback IPv6:

* Route-Map TAG: 12345

Interface Description:

Local ASN: 65501

Advertise Host Routes: ☑

* Enable Interface: ☑

Step 8 Click **Next** to save the created route peering.

3. Deploy Route Peering

Refer 4. Deploy Route Peering, on page 8 of the Intra-Tenant Firewall deployment use-case. Note that **InterTenantFW** is displayed under **Deployment**.

The BGP configuration on the vPC border leaf for this use-case is given below.

```
router bgp 12345
 router-id 10.2.0.1
 address-family l2vpn evpn
  advertise-pip
 neighbor 10.2.0.4
  remote-as 12345
  update-source loopback0
  address-family l2vpn evpn
   send-community
    send-community extended
 vrf myvrf_50001
  address-family ipv4 unicast
   advertise l2vpn evpn
   redistribute direct route-map fabric-rmap-redist-subnet
   maximum-paths ibgp 2
  address-family ipv6 unicast
   advertise l2vpn evpn
   redistribute direct route-map fabric-rmap-redist-subnet
   maximum-paths ibgp 2
  neighbor 192.168.32.254
   remote-as 9876
  local-as 65501 no-prepend replace-as // Note: This configuration corresponds to the Local
 ASN template parameter value of the service_ebgp_route template of the inside network with
 VRF myvrf_50001. The no-prepend replace-as keyword is generated along with the local-as
command.
  update-source loopback2
  ebgp-multihop 5
  address-family ipv4 unicast
   send-community
   send-community extended
   route-map extcon-rmap-filter-allow-host out
vrf myvrf_50002
 address-family ipv4 unicast
  advertise l2vpn evpn
  redistribute direct route-map fabric-rmap-redist-subnet
  maximum-paths ibgp 2
 address-family ipv6 unicast
  advertise l2vpn evpn
  redistribute direct route-map fabric-rmap-redist-subnet
  maximum-paths ibgp 2
 neighbor 32.32.32.254
  remote-as 9876
  local-as 65502 no-prepend replace-as // Note: This configuration corresponds to the Local
 ASN template parameter value of the service_ebgp_route template of the outside network
with VRF myvrf_50002. The no-prepend replace-as keyword is generated along with the local-as
 command.
  update-source loopback3
  ebgp-multihop 5
  address-family ipv4 unicast
   send-community
   send-community extended
   route-map extcon-rmap-filter-allow-host out
```

The loopback interface configuration on the vPC switch es-leaf1 for this use-case is given below. The loopback interfaces in the configuration correspond to the 'Loopback IP' parameter of the **service_ebgp_route** template. Two loopback interfaces are created automatically on each vPC switch for two separate VRF instances using the **Loopback IP** parameter values that are specified in the **service_ebgp_route** template.

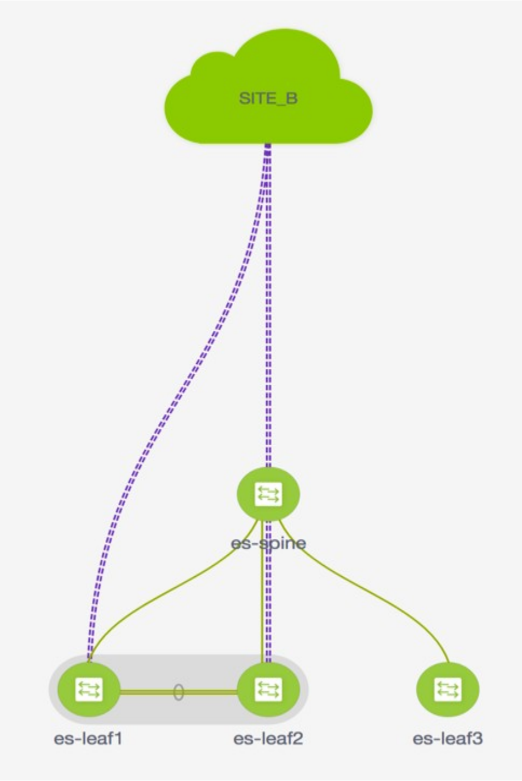
```
interface loopback2
 vrf member myvrf_50001
 ip address 60.1.1.60/32 tag 12345
interface loopback3
 vrf member myvrf_50002
 ip address 61.1.1.60/32 tag 12345
```

The loopback interface config on vPC peer switch es-leaf2:

```
interface loopback2
 vrf member myvrf_50001
 ip address 60.1.1.61/32 tag 12345
interface loopback3
 vrf member myvrf_50002
 ip address 61.1.1.61/32 tag 12345
```

Use Case: One-arm Load Balancer

Refer the figure given below for topology details.



In this topology, es-leaf1 and es-leaf2 are vPC leafs.

Now, let us see how to perform service redirection in DCNM.

Select **Control** > **Fabrics** > **Services**.

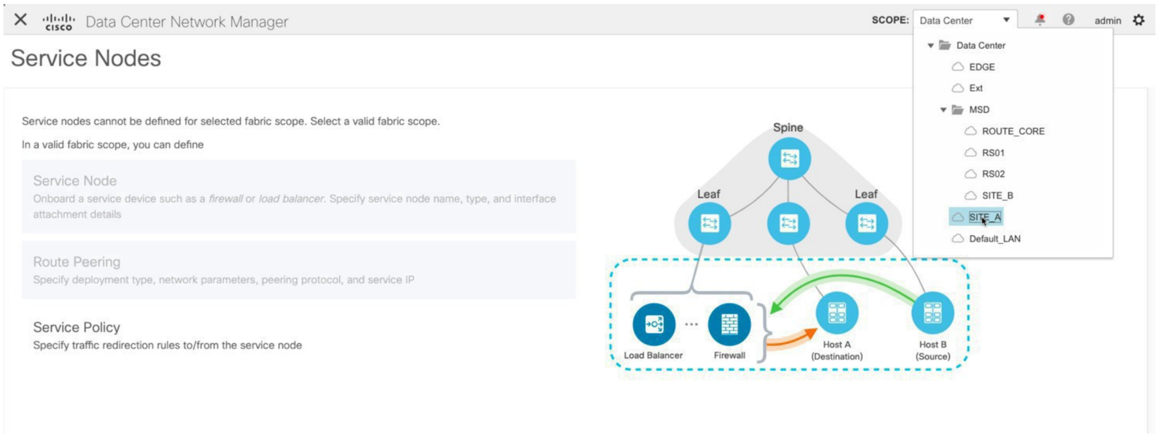
This use-case consists of the following steps:

Note As some steps are similar to the steps given in the Intra-tenant Firewall deployment usecase, reference links have been provided to the steps in that use-case.

1. Create Service Node

Procedure

Step 1 From the **Scope** drop-down list, select **Site_A**.



Data Center Network Manager

SCOPE: Data Center

admin

Service Nodes

Service nodes cannot be defined for selected fabric scope. Select a valid fabric scope.

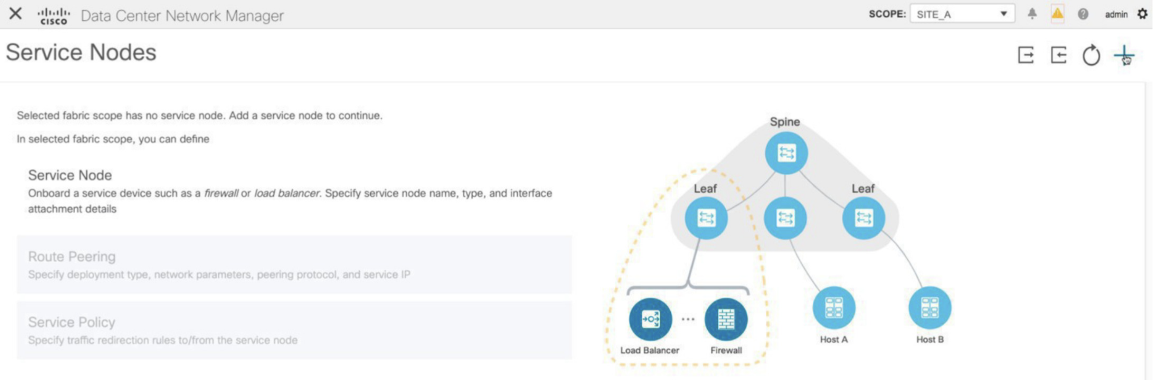
In a valid fabric scope, you can define

Service Node
Onboard a service device such as a *firewall* or *load balancer*. Specify service node name, type, and interface attachment details

Route Peering
Specify deployment type, network parameters, peering protocol, and service IP

Service Policy
Specify traffic redirection rules to/from the service node

Step 2 Click the **Add** icon in the **Service Nodes** window.



Data Center Network Manager

SCOPE: SITE_A

admin

Service Nodes

Selected fabric scope has no service node. Add a service node to continue.

In selected fabric scope, you can define

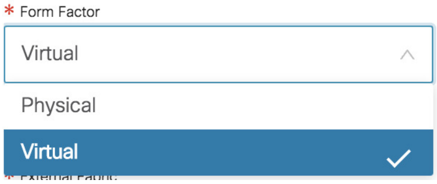
Service Node
Onboard a service device such as a *firewall* or *load balancer*. Specify service node name, type, and interface attachment details

Route Peering
Specify deployment type, network parameters, peering protocol, and service IP

Service Policy
Specify traffic redirection rules to/from the service node

Step 3 Enter the node name and specify **Load Balancer** in the **Type** dropdown box. The **Service Node Name** has to be unique.

Step 4 From the **Form Factor** drop-down list, select **Virtual**.



* Form Factor

Virtual

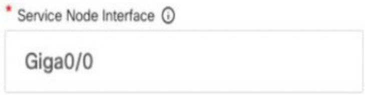
Physical

Virtual ✓

* External Fabric

Step 5 In the **Switch Attachment** section, from the **External Fabric** drop-down list, select the external fabric in which the service node (for example, ASA firewall) is located. Note that the service nodes need to belong to the external fabric. This is a prerequisite before creating a service node.

Step 6 Enter the interface name of the service node that will be connected to the service leaf.

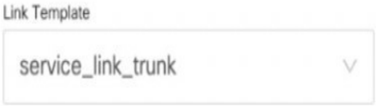


* Service Node Interface

Giga0/0

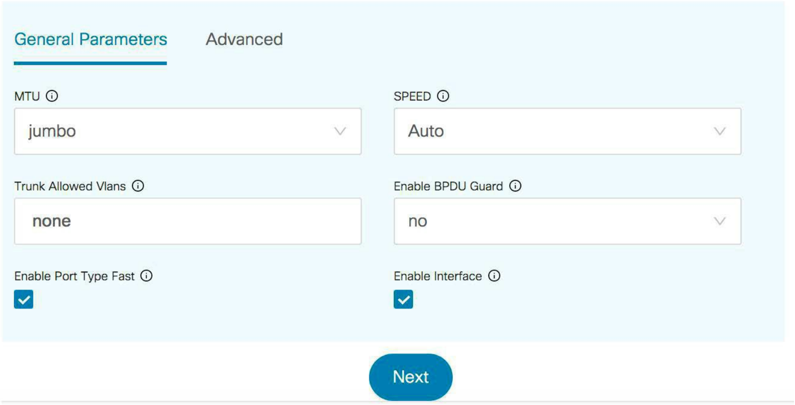
Step 7 Select the attached switch that is the service leaf, and the respective interface on the service leaf.

Step 8 Select the **service_link_trunk** template. DCNM supports trunk, port channel, and vPC link templates. The available link templates in the **Link Template** drop-down list are filtered based on the selected **Attached Switch Interface** type.



Link Template: service_link_trunk

Step 9 Specify the **General Parameters** and **Advanced** parameters, if required. Some parameters are pre-filled with the default values.



MTU: jumbo

SPEED: Auto

Trunk Allowed Vlans: none

Enable BPDU Guard: no

Enable Port Type Fast: ☑

Enable Interface: ☑

Step 10 Click **Next** to save the created service node.

Note For more sample screenshots, refer 1. Create Service Node, on page 2 in the Intra-tenant firewall with policy-based routing use case.

2. Create Route Peering

Let us now configure peering between a service leaf and a service node. In this use-case, we configure static route peering.

Procedure

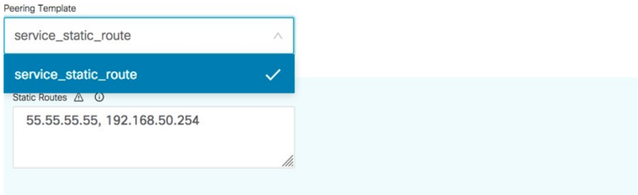
Step 1 Enter the peering name and select **One-Arm Mode** from the **Deployment** drop-down list. Also, from the **Peering Option** dropdown list, select **Static Peering**.

Step 2 Under **First Arm**, specify the required values. From the **VRF** dropdown list, select a VRF that already exists and select **First Arm** under **Network Type**.

Step 3 Enter the name of the **Service Network** and specify the **Vlan ID**. You can also click Propose to allow DCNM to fetch the next available VLAN ID from the specified service network VLAN ID range in the fabric settings. The default **Service Network Template** is **Service_Network_Universal**.

Under the **General Parameters** tab, specify the gateway address for the service network. Specify the **Next Hop IP Address**. This next hop address has to be within the first arm's subnet. Under the **Advanced** tab, the default **Routing Tag** value is 12345.

Step 4 The default **Peering Template** is **service_static_route**. Add routes, as required, in the **Static Routes** field.

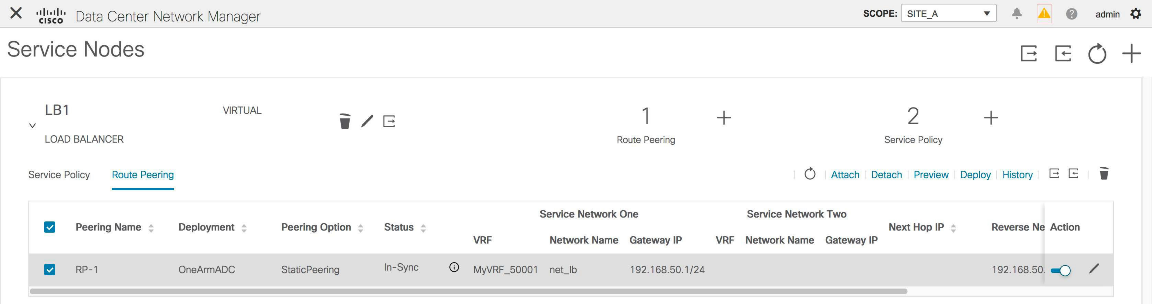


Peering Template: service_static_route

Static Routes: 55.55.55.55, 192.168.50.254

Step 5 Specify the **Next Hop IP Address** for Reverse Traffic.

Step 6 Click **Next** to save the created route peering.



Data Center Network Manager
SCOPE: SITE_A
admin
Service Nodes
Attach | Detach | Preview | Deploy | History

LB1 VIRTUAL
LOAD BALANCER
1 Route Peering
2 Service Policy

Service Policy | Route Peering

☑	Peering Name	Deployment	Peering Option	Status		Service Network One			Service Network Two			Next Hop IP	Reverse Ne	Action
						VRF	Network Name	Gateway IP	VRF	Network Name	Gateway IP			
☑	RP-1	OneArmADC	StaticPeering	In-Sync	ⓘ	MyVRF_50001	net_lb	192.168.50.1/24					192.168.50.	✎

3. Create Service Policy

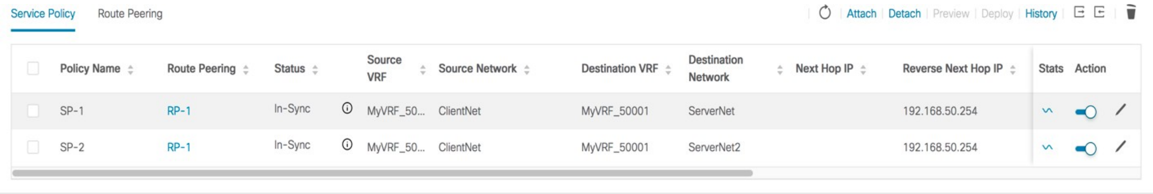
Refer 3. Create Service Policy, on page 6 in the Intra-Tenant Firewall deployment use-case.

4. Deploy Route Peering

Refer 4. Deploy Route Peering, on page 8 in the Intra-tenant Firewall deployment use-case. Note that **OneArmADC** is displayed under **Deployment**.

5. Deploy Service Policy

Refer 5. Deploy Service Policy, on page 10 in the Intra-tenant Firewall deployment use-case. However, as there are two servers in this load balancer use-case, two service policies have to be defined with each server network.



□	Policy Name	Route Peering	Status		Source VRF	Source Network	Destination VRF	Destination Network	Next Hop IP	Reverse Next Hop IP	Stats	Action
□	SP-1	RP-1	In-Sync	ⓘ	MyVRF_50...	ClientNet	MyVRF_50001	ServerNet		192.168.50.254		✎
□	SP-2	RP-1	In-Sync	ⓘ	MyVRF_50...	ClientNet	MyVRF_50001	ServerNet2		192.168.50.254		✎

6. View Stats

Refer 6. View Stats, on page 13 in the Intra-Tenant Firewall deployment use-case.

7. View Traffic Flow in Fabric Builder

Refer 7. View Traffic Flow in Fabric Builder, on page 13 in the Intra-Tenant Firewall deployment use-case.

8. Visualize Redirected Flows to Destination in the Topology window

Refer 8. Visualize Redirected Flows to Destination in the Topology window, on page 16 in the Intra-Tenant Firewall deployment use-case.

The VRF configuration on the service leaf is as given below.

```
interface Vlan2000
 vrf member myvrf_50001
 ip policy route-map rm_myvrf_50001

interface Vlan2306
 vrf member myvrf_50001
vrf context myvrf_50001
vni 50001
 ip route 55.55.55.55/32 192.168.50.254 // Note: This is the static route
 rd auto
 address-family ipv4 unicast
  route-target both auto
  route-target both auto evpn
 address-family ipv6 unicast
  route-target both auto
  route-target both auto evpn
router bgp 12345
 vrf myvrf_50001
  address-family ipv4 unicast
   advertise l2vpn evpn
   redistribute direct route-map fabric-rmap-redist-subnet
   redistribute static route-map fabric-rmap-redist-static
   maximum-paths ibgp 2
  address-family ipv6 unicast
   advertise l2vpn evpn
   redistribute direct route-map fabric-rmap-redist-subnet
   redistribute static route-map fabric-rmap-redist-static
   maximum-paths ibgp 2
```