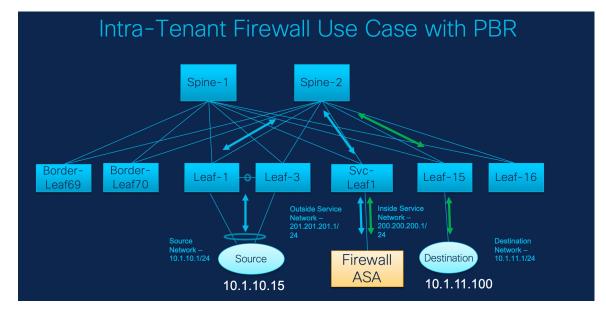


# L4-L7 Services Use Cases

- Use Case: Intra-tenant Firewall with Policy-based Routing, on page 1
- Use Case: Inter-tenant Firewall with eBGP Peering, on page 7
- Use Case: One-arm Load Balancer, on page 12

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



Refer the figure given below for topology details.

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 NDFC.



• This use-case does not cover how to provision the **Site\_A** VXLAN fabric. For information about this topic, refer to the Cisco Nexus Dashboard Fabric Controller for LAN Configuration Guide

• This use-case does not cover configurations on the service node (firewall or load balancer).

You can navigate to Services tab by one of the following below mentioned paths:

LAN > Services

LAN > Fabrics > Fabric Overview > Services

LAN > Switches > Switches Overview > Services

# **1. Create Service Node**

#### Procedure

**Step 1** Navigate LAN > Fabrics > Fabric Overview > Services.

v Service Node				
	0	2	3	
	Create Service Node	Create Route Peering	Create Service Policy	
Service Node Name*				
ASA1				
Service Node Type*				
Pilewaii × V				
Form Factor*				
Virtual × ~				
External Fabric*				
SITE_B × ~				
Service Node Interface*				
Giga0/0				
Attached Fabric*				
SITE_A X V				
Attached Switch* es-leaf3 ×				
Attached Switch Interface*				
Ethernet 1/3 × V				
Link Template* service_link_trunk ×				
General Parameters Advanced				
мти				
jumbo	MTU for the interface			
SPEED*				
Auto	V Interface Speed			
Trunk Allowed Vlans*				
none	Allowed values: 'none', 'all', or vian ran	anges (ex: 1-200,500-2000,3000)		
Enable BPDU Guard*				
no		en'enable', falsen'disable', non'return to default		
	settings'			
Enable Port Type Fast*	Enable spanning-tree edge port behav	avior		
Enable Interface*				
	Uncheck to disable the interface			

**Step 2** On **Services** tab, choose **Actions** > **Add**.

Enter the Service Node Name and specify Firewall in the Service Node Type dropdown box.						
The Ser	vice Node Name must be unique.					
From the	e Form Factor drop-down list, select Virtual.					
Choose appropriate external fabric from drop-down list, select the external fabric in which the service node (for example, ASA firewall) is located.						
Note	Ensure that the service nodes need to belong to the external fabric. This is a prerequisite before creating a service node.					
Enter the	e interface name of the service node that connects to the service leaf.					
Select th	e attached switch that is the service leaf, and the respective interface on the service leaf.					
Choose <b>service_link_trunk</b> template. NDFC supports trunk, port channel, and vPC link templates. The available link templates in the <b>Link Template</b> drop-down list are filtered based on the selected <b>Attache Switch Interface</b> type.						
1 2	the General Parameters and Advanced parameters, if required. Some parameters are pre-filled with ult values.					
Click Sa	we to save the created service node.					
	The Ser From the Choose a (for exar <b>Note</b> Enter the Select th Choose a available <b>Switch</b> I Specify the					

# 2. Create Route Peering

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

Peering					
	Create Serv	ice Node Create Route Peering	3 Create Service Polic	24	
Detach Attach					
Peering Name*					
peering tante					
Deployment*					
Intra-Tenant Firewall $ imes \sim$					
Inside Network		Outside Network			
VRF*		VRF*			
MyVRF_51000 X V		MyVRF_51000 × ~			
Network Type*		Network Type*			
Inside Network $\times \vee$		Outside Network X V			
Service Network*		Service Network*			
service_net_inside: 200.200.200 $\times \sim$		service_net_outside: 201.201.20 $\times\vee$			
VLAN ID*		VLAN ID*			
3002		3003			
Propose		Propose			
Network ID*		Network ID*			
30002		30003			
Service_Network_Template* Service_Network_Universal ×		Service_Network_Universal ×			
Service_NetWork_Oniversal X		Service_vetwork_oniversal ×			
General Parameters Advanced		General Parameters Advanced			
IPv4 Gateway/NetMask*		IPv4 Gateway/NetMask*			
200.200.200.1/24	example 192.0.2.1/24. (pu4	201.201.201.1/24	example 192.0.2.1/24. (pv4		
	or lpv6 gateway is mandatory		or tpv6 gateway is mandatory		
IPv6 Gateway/Prefix		IPv6 Gateway/Prefix			
	example 2001-db8=1/64		example 2001:db8:1/64		
VLAN Name	2001.0D0:1/06	VLAN Name	and case 1/06		
1.5 OK (40110	if > 32 chars	s a shi harne	if > 32 chars		
	enable system vlan long-name		enable:system vlan long-name		
Interface Description		Interface Description			
fw:inside:SITE_B:ASA1:Giga0/0:peering1		fw:outside:SITE_B:ASA1:Giga0/0:peering1			
At least one of the IP fields is mandatory*		At least one of the IP fields is mandatory*			
Next Hop IP Address		Next Hop IP Address for Reverse Traffic			
200.200.200.200		201.201.201.201			
Next Hop IPv6 Address		Next Hop IPv6 Address for Reverse Traffic			

#### Procedure

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

**Step 2** Under **Inside Network**, from the **VRF** drop-down list, select a VRF that 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 NDFC 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 3Specify the required parameters under Outside Network and specify the Next Hop IP Address for Reverse<br/>Traffic. This next hop address for reverse traffic needs to be within the 'outside service network' subnet.
- **Step 4** Click **Save** 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.

Create Service Policy		? ×
	Create Service Node Create Route Peering Create Service Policy	
	Detach Attach	
	Service Policy Name*	
	policy1	
	Peering Name*	
	pecing1 × V	
	Source VRF Name*	
	MyVR_51000 XV	
	Destination VRF Name*	
	MyVRF_51000 × v	
	Source Network* VLAN_10: 10.1.10.1/24 X V	
	Destination Network*	
	VLAN_11: 10.1.11.1/24 × V	
	Next Hop IP Address*	
	200.200.200.200 × ∨	
	Reverse Next Hop IP Address: 201.201.201.201	
	Link Template*	
	service_pbr ×	
	General Parameters Advanced	
	Protocol*	
	ip V The protocol example top.	
	Source Part*	
	Source port number, example any or 423. Value is ignored for 'lp'	
	and interp protocol	
	Destination Port* Destination Port* Destination port number; example any or 443, Value is ignored for	
	any 'grand temp protocol 'gran	

- **Step 2** Select the source and destination VRFs from **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.
- **Step 3** Select the source and destination networks from **Source Network** and **Destination Network** drop-down lists, or specify the source or destination network that is within the network subnets defined in **Fabric Overview** > **Services** window.
- **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 **Reverse Next Hop IP Address** field to enable policy enforcement on reverse traffic.
- Step 5 Under the General Parameters tab in the policy template, select ip from Protocol dropdown list, and specify any in Source Port and Destination Port fields.
  - **Note** For **ip** and **icmp** protocols, **any** source and destination port is used for ACL generation. You can also select a different protocol and specify the corresponding source and destination ports. NDFC converts well-known port numbers to match the format required by the switch. For example, you can convert port 80 to 'www'.

- Step 6 Under Advanced tab, by default permit is selected for Route Map Action and none is selected for 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* section in the Layer 4-Layer 7 Service chapter.
- **Step 7** Click **Save** to save the created service policy.

This completes procedures to perform and specify the flows for redirection.

# 5. Deploy Service Policy

- 1. On Services tab, on the Service Policy window choose the required peering.
- 2. Choose Actions > Deploy.

The Deploy Service Policy window appears.

**3.** Click **Deploy** to confirm deployment.

## 4. Deploy Route Peering

- 1. On Services tab, on the Route Peering window choose the required peering.
- Choose Actions > Deploy.
   The Deploy Route Peering window appears.
- 3. Click **Deploy** to confirm deployment.

## 6. View Stats

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

To visualize this scenario in NDFC, click the service policy, a slide-in pane appears.

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

Statistics are displayed for:

- Forwarding traffic on the source switch
- · Reversed traffic on the destination switch
- · 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 shown as a cloud icon in NDFC topology.

# Procedure Step 1 Click the service leaf, a slide-in pane appears and click Show more flows. You can see the flows that are redirected. Step 2 Click Details in the Service Flows window to display attachment details.

# 8. Visualize Redirected Flows to Destination in the Topology window

#### Procedure

Click <b>Topology</b> and click on leafs to visualize the redirected flows to destination.
Select Redirected Flows from the drop-down list.
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.
The switches, on which the source and destination network is attached and the flows are redirected and highlighted.
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.
The traffic from <b>Source</b> 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 to 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 NDFC.

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 added to the steps in that use-case.
  - Service policies are not applicable on Inter-tenant firewall deployments.

# **1. Create Service Node**

#### Procedure

- **Step 1** Navigate to LAN > Fabrics > Fabric Overview > Services.
- **Step 2** On **Services** tab, choose **Actions** > **Add**.

Create New	Service Node				? ×
		1 Create Service Node	2 Create Route Peering	Create Service Policy	
	Service Node Name*				
	ASAZ				
	Service Node Type*				
	Firewall × >				
	Form Factor*				
	Physical $\times \vee$				
	External Fabric*				
	SITE_B × V				
	Service Node Interface*				
	Giga1/1				
	Attached Fabric*				
	SITE_A 🗸				
	Attached Switch* es-leaf1 ~ es-leaf2 ×				
	Attached Switch Interface*				
	vPC1 × V				
	Link Template* service_link_vpc ×				
			No Data in Template		
					Cancel Save

- **Step 3** Enter service node name, choose Firewall in the Service Node Type dropdown box. The Service Node Name must be unique.
- **Step 4** From the **Form Factor** drop-down list, choose **Virtual**.
- **Step 5** From the **External Fabric** drop-down list, choose the external fabric in which the service node (for example, ASA firewall) is located.
  - **Note** Ensure that 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 connects to the service leaf.					
Step 7	Select the attached switch that is the service leaf, and the respective interface on the service leaf.					
Step 8	Select the <b>service_link_trunk</b> template. NDFC supports trunk, port channel, and vPC link templates. The available link templates in the <b>Link Template</b> drop-down list are filtered based on the selected <b>Attached Switch Interface</b> type.					
Step 9	If require	d, specify General Parameters, and Advanced. Some parameters are pre-filled with default values.				
Step 10	Click Save to save the created service node.					
	Note	For more sample screenshots, refer 1. Create Service Node, on page 2 section 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.

Peering	Create Service Node	2 3 Create Route Peering Create Service Policy	
Detach Attach			
Peering Name*			
peeringInterTenant			
Deployment*			
Inter-Tenant Firewall X V			
Peering Option*			
EBGP Dynamic Peering $\times \lor$			
Inside Network		Outside Network	
VRF* MyVRF_51000 X V		VRF* MyVRF_51000 × ~	
Network Type*		Network Type* Outside Network X V	
Inside Network X V		Outside Network X V	
Service Network*		Service Network*	
net_inside_inter_tenant X V		net_outside_inter_tenant X V	
VLAN ID*		VLAN ID*	
3001		3002	
Propose		Network ID*	
30010		30011	
Service Network Template* Service_Network_Universal ×		Service Network_Template* Service_Network_Universal ×	
General Parameters Advanced		General Parameters Advanced	
General Parameters Advanced		General Parameters Advanced	
IPv4 Gateway/NetMask*	example 192.0.2.1/24. Ipv4 or Ipv6	IPv4 Gateway/NetMask*	example 192.0.2.1/24. Ipu& or Ipv6
192.168.32.1/24	gateway is mandatory.	32.32.32.1/24	gateway is mandatory.
IPv6 Gateway/Preftx		IPv6 Gateway/Prefix	
	example 2001:db8::1/64		example 2001:db8::1/64
VLAN Name	if > 32 chars enable: system vian long-	VLAN Name	if > 32 chars enable:system vian long-
	same		name
Interface Description		Interface Description	
fw:inside:SITE_B:ASA2:Giga1/1:peeringInterTenant		fw:outside:SITE_B:ASA2:Giga1/1:peeringInterTenant	
Peering Template* service_ebgp_route ×		Peering Template* service_ebgp_route ×	
General Parameters Advanced		General Parameters Advanced	
Neighbor IPv4 address or subnet*	Neighbor IPv4 address or address with	Neighbor IPv4 address or subnet*	Neighbor IPe4 address or address with
192.168.32.254	neemask, ex 1.2.3.4 or 1.2.3.1/24. Neighbor IPv4 or IPv6 address is	32.32.32.254	nermask, ex 1.2.3.4 or 1.2.3.1/24. Neighbor IPv6 or IPv6 address is
	mandatory.		mandatory.
Loopback IP*	IP address of the loopback. Loopback	Loopback IP*	IP address of the loopback. Loopback
60.1.1.60	IPv6 or IPv6 address is mandatory.	61.1.1.60	IPel or IPv6 address is mandatory.
vPC Peer's Loopback IP		vPC Peer's Loopback IP	
60.1.1.61	IP address of the peer's loopback	61.1.1.61	IP address of the peer's loopback

#### 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 exists and select **Inside Network** under **Network Type**.

Enter the name of **Service Network**, specify **Vlan ID**. You can click **Propose** to allow NDFC to fetch the next available VLAN ID from specified service network VLAN ID range in the fabric settings. The default **Service Network Template** is **Service\_Network\_Universal**.

Under General Parameters tab, specify the gateway address for the service network. Specify 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.
	Under General Parameters tab, specify Neighbor IPv4 address, Loopback IP address, and vPC Peer's Loopback IP address. The border switches are a vPC pair.
Step 4	Under the <b>Advanced</b> tab, specify the <b>Local ASN</b> and select the <b>Advertise Host Routes</b> 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 shown. If this checkbox is not selected, the prefix routes will be shown.
	By default, the Enable Interface checkbox is selected.
Step 5	Specify the required parameters under <b>Outside Network</b> and specify the <b>Next Hop IP Address for Reverse Traffic</b> . 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 <b>service_ebgp_route</b> .
	Under the <b>General Parameters</b> tab, <b>Neighbor IPv4</b> address, <b>Loopback IP</b> address, and <b>vPC Peer's Loopback IP</b> address. The leaf switches are a vPC pair.
Step 7	Under the <b>Advanced</b> tab, specify the <b>Local ASN</b> and select the <b>Advertise Host Routes</b> checkbox. This local ASN value is used to override the system ASN on the switch and is required to avoid routing loops.
	If the <b>Advertise Host Routes</b> 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.
Step 8	Click <b>Save</b> to save the created route peering.

# **3. Deploy Route Peering**

Refer to 4. Deploy Route Peering, on page 6 in the Intra-Tenant Firewall deployment use-case. Ensure that the **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 12vpn evpn
 advertise-pip
neighbor 10.2.0.4
 remote-as 12345
 update-source loopback0
 address-family 12vpn evpn
  send-community
   send-community extended
vrf myvrf_50001
 address-family ipv4 unicast
  advertise 12vpn evpn
  redistribute direct route-map fabric-rmap-redist-subnet
  maximum-paths ibgp 2
 address-family ipv6 unicast
  advertise 12vpn 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 12vpn evpn
  redistribute direct route-map fabric-rmap-redist-subnet
 maximum-paths ibqp 2
 address-family ipv6 unicast
  advertise 12vpn 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 **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 figure given below for topology details.

L

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

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

You can navigate to Services tab by one of the following below mentioned paths:

LAN > Services

This use-case consists of the following steps:

10
v
_

Note

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

# **1. Create Service Node**

#### Procedure

Step 1

Navigate to LAN > Fabrics > Fabric Overview > Services

ervice Node						
	Creat	1 e Service Node	2 Create Route Peering	3 Create Service Po	licy	
Service Node Name*						
LB1						
Service Node Type*						
Form Factor* Physical X V						
External Fabric*						
Service Node Interface*						
G1/1						
Attached Fabric*						
SITE_A X V						
Attached Switch* es-leaf3 ×						
Attached Switch Interface*						
Ethernet1/50 $\times$ $\vee$						
Link Template* service_link_trunk ×						
General Parameters Advanced						
MTU*						
jumbo	V MTU fo	r the interface				
SPEED*						
Auto	✓ Interfac	e Speed				
Trunk Allowed Vlans*						
none	Alone	d values: 'none', 'all', or vian ranges (e	er: 1-200.500-2000.3000)			
Enable BPDU Guard*			ble', false='disable', no='return to default			
	settings	C				
Enable Port Type Fast*	Enable	spanning-tree edge port behavior				
Enable Interface*						
		k to disable the interface				

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

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

Step 4	From th	e Form Factor drop-down list, select Virtual.						
Step 5	In the <b>Switch Attachment</b> section, from the <b>External Fabric</b> 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 th	e interface name of the service node that connects to the service leaf.						
Step 7	Select th	Select the attached switch that is the service leaf, and the respective interface on the service leaf.						
Step 8	Select the <b>service_link_trunk</b> template. NDFC supports trunk, port channel, and vPC link templates. The available link templates in the <b>Link Template</b> drop-down list are filtered based on the selected <b>Attached Switch Interface</b> type.							
Step 9	Specify <b>General Parameters</b> and <b>Advanced</b> parameters, if required. Some parameters are pre-filled with the default values.							
Step 10	Click Sa	we 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**.

L

Step 2	Under First Arm, specify the required values. From the VRF dropdown list, select a VRF that exists and
	select First Arm under Network Type.
Step 3	Enter the name of <b>Service Network</b> and specify <b>Vlan ID</b> . Click <b>Propose</b> to allow NDFC 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.
- **Step 5** Specify **Next Hop IP Address** for Reverse Traffic.
- **Step 6** Click **Save** to save the created route peering.

# **3. Create Service Policy**

Refer to 3. Create Service Policy, on page 5 in the Intra-Tenant Firewall deployment use-case.

Create Service Policy		? >
	Create Service Node Create Route Peering	Create Service Policy
	efach e Attach anvice Policy Name*	
	policy1	
	eering Name* peering1, X V	
	ource VRF Name*	
	MyVRF_51000 $\times$ $\sim$	
	estination VRF Name*	
	ource Network*	
	VLAN_11: 10.1.11.1/24 × V	
	estination Network* VLAN_10: 10.1.10.1/24 X >>	
	evense Next Hop (P 92:168:50.254 Ni: Template*	
	General Parameters Advanced	
	Protoco)* tcp V The protocol, example top.	
	Source Port* Source Port* Source port number, example any or 433. Value is ground for "p" and "one" protocol	
	Destination Port* 443 Destination port number; example any or 443. Value is ignored for Value in ground for Value in ground for	

# 4. Deploy Route Peering

Refer to 4. Deploy Route Peering, on page 6 in the Intra-tenant Firewall deployment use-case. Note that **OneArmADC** is displayed under **Deployment**.

## 5. Deploy Service Policy

Refer to 5. Deploy Service Policy, on page 6 in the Intra-tenant Firewall deployment use-case. However, as there are two servers in this load balancer use-case, two service policies to be defined with each server network.

### 6. View Stats

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

# 7. View Traffic Flow in Fabric Builder

Refer to 7. View Traffic Flow in Fabric Builder, on page 6 in the Intra-Tenant Firewall deployment use-case.

# 8. Visualize Redirected Flows to Destination in the Topology window

Refer to 8. Visualize Redirected Flows to Destination in the Topology window, on page 7 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 12vpn 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 12vpn evpn
   redistribute direct route-map fabric-rmap-redist-subnet
   redistribute static route-map fabric-rmap-redist-static
   maximum-paths ibgp 2
```