

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: One-arm Firewall, on page 16

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 Norie Interfece*				
Giga0/0				
Attached Fabric*				
SITE_A XV				
Attached Switch*				
es-leat3 ×				
Attached Switch Interface*				
Ethernet 1/3 × V				
Link Template* service_link_trunk ×				
General Parameters Advanced				
MTLP				
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	Enable spenning-tree bpduguard: true	en'enable', falsen'disable', non'return to default		
L	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**.

Step 3	Enter the Service Node Name and specify Firewall in the Service Node Type dropdown box.							
	The Ser	vice Node Name must be unique.						
Step 4	From the Form Factor drop-down list, select Virtual.							
Step 5	Choose 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.						
Step 6	Enter th	e interface name of the service node that connects to the service leaf.						
Step 7	Select th	ne attached switch that is the service leaf, and the respective interface on the service leaf.						
Step 8	Choose service_link_trunk template. NDFC supports trunk, port channel, and vPC link templates. Th available link templates in the Link Template drop-down list are filtered based on the selected Attach Switch Interface type.							
Step 9	Specify the defa	the General Parameters and Advanced parameters, if required. Some parameters are pre-filled with ult values.						
Step 10	Click Sa	ave to save the created service node.						

2. Create Route Peering

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

reening				
	Create Serv	Create Route Peering	Create Service Policy	
Detach Attach				
Rearing Namet				
peering Name				
Deployment*				
Intra-Tenant Firewall X				
Inside Network		Outside Network		
VRF*		VRF*		
MyVRF_51000 × ~		MyVRF_51000 X V		
Network Type*		Network Type*		
Inside Network X V		Outside Network X V		
Service Network*		Service Network*		
service_net_inside; 200.200.200 $\times \lor$		service_net_outside: 201.201.20 $\times \sim$		
MAN D*		M AN IDS		
3002		3003		
Propose		Propose		
Network ID*		Network ID*		
30002		30003		
Service Network Template*		Service Network Template*		
Service_NetWork_Oniversal A		Service_Network_Oniversal X		
General Parameters Advanced		General Parameters Advanced		
IPv4 Gateway/NetMask*		IPv4 Gateway/NetMask*		
200.200.200.1/24	example 192.0.2.1/24. (pv4	201.201.201.1/24	example 192.0.2.1/24. (pv4	
	or lpv6 gateway is mendatory.		or tpv6 gateway is mandatory.	
IPv6 Gateway/Prefix		IPv6 Gateway/Prefix		
	example		example	
NE AN Name	2001.3D8:1/06	VII AN Nome	and Labor 1. Sec. 17 DB	
Controlline	# > 32 chars	· La del montre	if > 32 chars	
	enable system vian long-name		enable:system vlan long-name	
Interface Description		Interface Description		
fw:inside:SITE_B:ASA1:Giga0/0:peering1		fw:outside:SITE_8: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
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	
D	etach Attach		
54	ervice Policy Name*		
	policy1		
P	eering Name*		
	peering1	××	
Se	ource VRF Name*		
	MyVRF_51000		
D	estination VRF Name*		
	MyVRF_51000	× v	
Se	ource Network*		
	VENN_10.10.110.1/24		
D	estination Network*		
	VLAN_11: 10.1.11.1/24	\times \sim	
	last Lion ID Addresst		
	200.200.200.200		
	Reverse Next Hop IP Address: 201.201.201.201		
	ink Template*		
se	ervice_pbr ×		
	General Parameters Advanced		
	Protocol*		
	ip ~	The protocol, example top.	
	Source Port*	Source port number, example any or 443. Value is ignored for 'lp'	
	any	and "icmp" protocol	
	Destination Port*	Destination port number, example any or 443. Value is ionored for	
	any	'p' and 'iomp' protocol	

- **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 in the Layer 4-Layer 7 Service configuration guide.

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.
- 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.
- 2. 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 Topology 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 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 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**.

eate New Service N	Node				?
		1 Create Service Node	2 Create Route Peering	Create Service Policy	
Service Noc	de Name*				
ASA2					
Service Noo	ie Type*				
Firewall	>				
Form Factor					
Physical	>				
External Fab	oric*				
SITE_B	>				
Service Noc	ie Interface*				
Giga1/1					
Attached Fa	bric*				
SITE_A					
Attached Sv es-leaf1 ~ e	witch* es-leaf2 ×				
Attached Sv	witch Interface*				
vPC1	>				
Link Templa service_link	_vpc ×				
			No Data in Template		

- **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 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 service_link_trunk template. NDFC 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.					
Step 9	If required, specify General Parameters, and Advanced. Some parameters are pre-filled with default values.					
Step 10	Click Sa	ve 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.

Create Route Peering			
	Create Service Node	2 3 Create Route Peering Create Service Policy	
Detach Attach Peoring Nama* peeringinterTenant Deployment*			
Inter-Tenant Firewall X V Peering Option* EBGP Dynamic Peering X V Inside Network		Outside Network	
V8F* MyV8F_51000 × ∞ Network Type*		VRF* MyVRF_51000 X V Network Type *	
Inside Network × ∨ Service Network* Inst_Inside_Inter_temant × ∨ VLAN ID*		Outside Network X V Service Network* net_outside_inter_tenant X V VI AN ID*	
3001 Network (D* 30010		3002 Network (D* 30011	
Service Network "Emplate" Service, Network Universal X		Service Network: Template* Service_Network_Universal × General Parameters Advanced	
IP-4 Gateway/HetMask* 192.163.22.1/24 IP-6 Gateway/Prefix	example 192.0.2.1/24. (pv8 or (pv6 gateway is monotatory) example 2001.db8:-1/64	IPv4 Gateway/NetMask* 32.32.32.1/24 IPv6 Gateway/Prefix	example 192.0.2.1/Q4. (pv6 or (pv6 gateway is mandatory) example 201:dbt:1/64
VLAN Name	If > 32 chars anable system vian long- name	VLAN Name Interface Description	\vec{x} is 32 chars analos agatem vian long- name
revision.arr.g.br.304.4.50p./forum		Volisious.51*2, 0.3-342, cigar (r), peering internetine Peering Template* service_ebgp_route ×	
Oninning Farameters Advanced Neighbor (FV4 address or subnet* 192.168.32.254	Neighbor IPvil address or address with netmask, ex 1.2.3.4 or 1.2.3.124. Neighbor IPvil or IPvil address is mandatore.	General Parameters Advanced	Neghor PvL solves or indives with newski, ex. (2.2.4 or (2.3.104) Neghor PvL or PvL address is mandation
Loopback (P* 60.1.1.60 VPC Peer's Loopback (P	IP address of the loopback Loopback IPvil or IPvil address is mandatory.	Loopback IP* 61.1.1.60 VPC Peer's Loopback IP	P address of the loopback. Loopback Pull or Pull address is manufatory.
60.1.1.61	IP address of the peer's loopback	61.1.1.61	IP address of the peer's loopback

	Procedure
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 .
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.
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.
1	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 shown. If this checkbox is not selected, the prefix routes will be shown.
	By default, the Enable Interface checkbox is selected.
	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.
	The default Peering Template for eBGP dynamic peering is service_ebgp_route.
	Under the General Parameters tab, Neighbor IPv4 address, Loopback IP address, and vPC Peer's Loopback IP address. The leaf switches are a vPC pair.
	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.
	Click Save 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 ibop 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.

_

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 Norle Name*						
LB1						
Service Node Type*						
Form Factor*						
T nyacai 🔨 🗸 🗸						
External Fabric*						
SITE_D X V						
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				
Touch Allowed Marcal						
none	Alone	d values: 'norve', 'all', or vian rances (e	er: 1-200.500-2000.3000)			
Enable BPDU Guard*	Enable	spanning-tree bpduguard: true="enab	ble', false='disable', no='return to default			
	settings	C				
Enable Port Type Fast*	Enable	spanning-tree edge port behavior				
Enable 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 the	From the Form Factor drop-down list, select Virtual.						
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 th	Enter the interface name of the service node that connects to the service leaf.						
Step 7	Select t	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. NDFC 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.							
Step 9	Specify General Parameters and Advanced parameters, if required. Some parameters are pre-filled with the 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 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 Service Network and specify Vlan ID . 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 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		? ×
c	Treate Service Node Create Route Peering Create Service Policy	
Detach e Attach Service Policy Name*		
policy1		
Peering Name*		
peering1.	XV	
Source VRF Name* MyVRF_51000		
Destination URE Mannet		
MyVRF_51000	××	
Source Network*		
VLAN_11: 10.1.11.1/24	×v	
Destination Network*		
VLAN_10: 10.1.10.1/24	××	
Reverse Next Hop IP 192.168.50.254		
Link Template* service_pbr \times		
General Parameters Advanced		
Protocol* tep	V Tra protecol, esample top.	
Source Port*		
any	Source port number, example any or 483. Value is ignored for "p" and "icmp" protocol	
Destination Port* 443	Destination por number, stample any or 443, Value is ignored for 'g' and 'sing' potential	

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
```

Use Case: One-arm Firewall

Starting from Cisco NDFC Release 12.1.1e, a new deployment One-arm firewall is added.

Refer to the figure for topology details. In this topology, BGW-VPC1 and BGW-VPC2 are vPC Border Gateway which is added as service switches. LEAF-7 and LEAF-8 are vPC leaf switches for which Source (S) network of the redirected flow is attached. LEAF-5 is attached to Destination (D) network of the redirected flow.



Now, let us see how to perform service redirection in NDFC. You can navigate to **Services** tab by one of the following mentioned paths:

LAN > Services

For selected Easy fabric, LAN > Fabrics > Fabric Overview > Services

For selected (leaf, border, and border gateway) switches, LAN > Switches > Switches Overview > 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 added to the steps in that use-case.

1. Create Service Node

Procedure

Cr

Step 1

Navigate to LAN > Fabrics > Fabric Overview > Services

Service Node				
	U	2	3	
	Create Service Node	Create Route Peering	Create Service Policy	
Service Node Name*				
ASA1				
Service Node Type*				
Firewall	$\times \sim$			
Form Factor*				
Virtual	$\times \sim$			
External Fabric*				
Ext2	××			
Service Node Interface*				
Giga0/0				
Attached Fabric*				
fab2				
Attached Switch* 93180YC-58 ×				
Attached Switch Interface*				
Ethernet1/51	\times \checkmark			
Link Template* service_link_trunk \times				
General Parameters Adva	anced			
MTU*				
jumbo	~	MTU for the interface		
SPEED*				
Auto	~	Interface Speed		
Trunk Allowed Vlans*				
none		Allowed values: 'none', 'all', or vian ranges (ex: 1-200,500-2000,3000))	
Enable BPDU Guard*		Enable spanning-tree bpdupuard: trues'enable', falses'disable',		
no	~	no='return to default settings'		
Enable Port Type Fast*		Enable spanning-tree edge port behavior		
Enable Interface*		Uncheck to disable the interface		

Step 2	Click the Add icon in the Service Nodes window.				
Step 3	Enter the node name and specify Firewall in the Type dropdown box. The Service Node Name must be unique.				
Step 4	From the Form Factor drop-down list, select Virtual.				
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.				
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. NDFC 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.				
Step 9	Specify the General Parameters and Advanced parameters, if required. Some parameters are pre-filled with the 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 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.

	\frown		
	 — 	2	
	Create Service Node	Create Route Peering	
Detach Attach			
Peering Name*			
Deployment*			
One-Arm Firewall			
Peering Option*			
Static Peering X			
Inside Network			
VRF*			
UIT_Service_OneArmLB ×	~		
Network Type*			
Inside Network $\qquad \qquad \qquad$	\sim		
Service Network*			
Select	\sim		
VI AN ID*			
3001			
Propose			
30203			
Service Network Template*			
Service_Network_Universal ×			
General Parameters Advanced			
General Parameters Advanced			
General Parameters Advanced	example		
General Parameters Advanced	example 192.0.2.1/24.10v4 or Lot gateway is		
General Parameters Advanced	example 192.0.2.1/24. by4 or by6 galeway is mancestry.		
General Parameters Advanced	example 192.0.2.1/24.lov4 or by/b galaxies is mandatory.		
General Parameters Advanced	example 192.0.2.174, tor4 or tor6 galaxies to manostory. example 2001 cdst:1/64		
General Parameters Advanced IPv4 Gateway/NetMask* IPv6 Gateway/Prefix* VLAN Name	example 192.0.2.124, toy4 or tyd gateway is maholawy, 2001.coli:1/64 r >2.2.char example z >2.char		
Ceneral Parameters Advanced Pv4 Gateway/NetMask* IPv6 Gateway/Prefix* VLAN Name	example 192.0.2.124 (by4 or physery) is manostory. example 201.038-1/64 f* 32.04m erable system vian torg-name		
Ceneral Parameters Advanced Prv4 Gateway/NetMask* IPv6 Gateway/Prefix* VLAN Name Interface Description	example 192.0.2.174.1974 or by daysway to mancatory. 201.008.1764 z201.008.1764 z2.2.204rs exatile system vian long name		
Cereral Parameters Advanced Pv4 Gateway/NetMask* Pv6 Gateway/Prefix* VLAN Name Interface Description	example 192.0.2.174.1094 or shuf galaway is manastory. 2003.code-1/64 2003.code-1/64 if % 522.chars anadexpytien vian long-name		
Cervice_rectwork_Universal × General Parameters Advanced IPv4 Gateway/NetMask* IPv6 Gateway/Prefix* VLAN Name Interface Description Peering Template* Peering Template*	example 192.0.2.174. loyd or by dynawy is mendstory. example 2001 doll-1/64 r > 22 chars enable system vian long-name		
Cervice_rectivors_utilizers Advanced Cervice_rectivors_data Pv6 Gateway/NetMask* Pv6 Gateway/Prefix* VLAN Name Interface Description Peering Template* service_static_route ×	example 192.0.2.194. loyd or sho ganewy is mandstory. example 2001 coll:1/64 If > 32.03mp enable system vian long name		
Cervice_rvctwork_Universal × Cervice_rvctwor	example 192.0.2.104, lov4 or bud gateway is malacitary. example 2001.colid=1/64 r > 32.colid or buds system vian long riteme		
Cerroral Parameters Advanced PV4 Gateway/NetMask* IPv6 Gateway/Prefix* VLAN Name Interface Description Peering Template* service_static_route × Static Routes	example 192.0.2.104 (byt4 or bid gateway is medicate) example 2011-08:11/64 or 52 coars or 52 coars or 52 coars or 52 coars or 52 coars or 54 coars or		
General Parameters Advanced IPv4 Gateway/NetMask* IPv6 Gateway/Prefix* VLAN Name Interface Description Interface Description Static Routes	example 192.0.2.1/24 (by4 or by3 party) is mandatory. example 201.0x8-1/64 if > 32.0x87 if >		
General Parameters Advanced IPv4 Gateway/NetMask* IPv6 Gateway/Prefix* VLAN Name Interface Description Interface Description Static Routes ▲	manple 192.0.2.1/34 (by4 or bydaway is manostory. 201.0bit-1/64 rf > 32 chars exatige anable system vian long name		
General Parameters Advanced IPv4 Gateway/NetMask* IPv6 Gateway/Prefix* VLAN Name Interface Description Interface Description Static Routes ▲	example 192.0.2.174. lov4 or by derivery is mandatory. 2001.codi.1/64 2001.codi.1/64 r/s 32.2.04/8 example autote system vian long name		
General Parameters Advanced IPv4 Gateway/NetMask* IPv6 Gateway/Prefix* VLAN Name Interface Description Interface Description Static Routes Static Routes Next Hop IP Address	example 192.0.2.1/34. (by4 or shulp always) is mandatory. 2001.codit.1/64 If > 322.chars enable system vian loop-name One Static House per line example 1.2.0.024, 1.2.2.2		
General Parameters Advanced IPv4 Gateway/NetMask* IPv6 Gateway/Prefix* VLAN Name Interface Description Interface Description Static Routes A Static Routes A Next Hop IP Address	example 192.0.2.174. lov4 or sho galaway is managatoy. 2001.cod-1764 If > 32 cMars anada aystem vian loop cante por fairs example 1.2.024, 1.2.2.2		
	example 192.0.2.174. loy4 or by danway is meanpatory. 2001.008-1764 47.52.04/s whole system vian long stante Dee Statis floode per loss example 1.2.0.04, 1.2.2.2		
General Parameters Advanced IPv4 Gateway/NetMask* IPv6 Gateway/Prefix* VLAN Name Interface Description Interface Description Static Routes A Static Routes A Next Hop IP Address Next Hop IPv6 Address	example 192.0.2.174. loyd or by danway is meanpatory. 2001.00811/04 47.92.0.009 or observed south system vian loog stante Doe Statis floote per line example 1.2.2.024, 1.2.2.2		

	Procedure				
Step 1	Enter the peering name and select One-Arm Firewall from the Deployment drop-down list. Also, from the Peering Option dropdown list, choose Static Peering .				
	Note You can also choose eBGP Peering option.				
Step 2	In Inside Network , specify the required values. From the VRF dropdown list, select a VRF that exists and select Inside Network under Network Type.				
Step 3	Enter the name of Service Network , specify Vlan ID , and Network ID . You can click Propose to allow NDFC to fetch the next available Vlan ID from the specified service network Vlan ID range and the next available Network ID from the specified Layer 2 VXLAN VNI range defined in the fabric settings. The defaul Service Network Template is Service_Network_Universal .				
	Under the General Parameters tab, specify the gateway address for the service network. Specify Hop IP Address . This next hop address has to be within the inside network's subnet. Under t tab, the default Routing Tag value is 12345.	ecify the Next he Advanced			
Step 4	The default Peering Template for static peering is service_static_route . Add routes, as require Routes field.	ed, in the Static			
Step 5	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.

4. Deploy Route Peering

Refer to 4. Deploy Route Peering, on page 6 in the Intra-tenant Firewall deployment use-case.

5. Deploy Service Policy

Refer to 5. Deploy Service Policy, on page 6 in the Intra-tenant Firewall deployment use-case.

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

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.