About Policy-Based Routing

Cisco Application Centric Infrastructure (ACI) policy-based routing (PBR) enables provisioning service appliances, such as firewalls or load balancers, as managed or unmanaged nodes without needing a Layer 4 to Layer 7 package. Typical use cases include provisioning service appliances that can be pooled, tailored to application profiles, scaled easily, and have reduced exposure to service outages. PBR simplifies the deployment of service appliances by enabling the provisioning consumer and provider endpoint groups all in the same virtual routing and forwarding (VRF) instance. PBR deployment consists of configuring a route redirect policy, a cluster redirect policy, and creating a service graph template that uses route and cluster redirect policies. After the service graph template is deployed, use the service appliance by enabling endpoint groups to consume the service graph provider endpoint group. This can be further simplified and automated by using vzAny. While performance requirements may dictate provisioning dedicated service appliances, virtual service appliances can also be deployed easily using PBR.
The following figure illustrates the use case of redirecting specific traffic to the firewall:

**Figure 1: Use Case: Redirecting Specific Traffic to the Firewall**

In this use case, you must create two subjects. The first subject permits HTTP traffic, which then gets redirected to the firewall. After the traffic passes through the firewall, it goes to the Web endpoint. The second subject permits all traffic, which captures traffic that is not redirected by the first subject. This traffic goes directly to the Web endpoint.

The following figure illustrates a sample ACI PBR physical topology:

**Figure 2: Sample ACI PBR Physical Topology**
The following figure illustrates a sample ACI PBR logical topology:

*Figure 3: Sample ACI PBR Logical Topology*

While these examples illustrate simple deployments, ACI PBR enables scaling up mixtures of both physical and virtual service appliances for multiple services, such as firewalls and server load balancers.

Observe the following guidelines and limitations when planning PBR service nodes:

- For high availability active/standby deployment, configure the service nodes with their actual MAC address.
- The next-hop service node IP address and virtual MAC address must be provided.
- The service node bridge domain must have the learning of the source VTEP on remote leaf switches disabled and GARP learning enabled.
- Provision service appliances in a separate bridge domain.
- The service appliance, source, and bridge domain can be in the same VRF.
- For N9K-93128TX, N9K-9396PX, and N9K-9396TX switches, the service appliance must not be in the same leaf switch as either the source or destination endpoint group. For N9K-C93180YC-EX and N9K-93108TC-EX switches, the service appliance can be in the same leaf switch as either the source or destination endpoint group.
- The service appliance can only be in a regular bridge domain.
- The contract offered by the service appliance provider endpoint group cannot be configured to allow-all. Also, it must specify IP as the contract filter.
- Multicast and broadcast traffic redirection is not supported.
- Redirection to transparent services is not supported.
- Supported PBR configurations in the same VRF instance include the following:

**Figure 4: Supported PBR Configurations in the Same VRF Instance**
• Supported PBR configurations in a different VRF instance include the following:

Figure 5: Supported PBR Configurations in a Different VRF Instance
• Unsupported PBR configurations include the following:

_Figure 6: Unsupported PBR Configurations_
Configuring Policy-Based Routing

About Policy-Based Routing
About Symmetric Policy-Based Routing

Symmetric policy-based routing (PBR) configurations enable provisioning a pool of service appliances so that the consumer and provider endpoint groups traffic is policy-based. The traffic is redirected to one of the service nodes in the pool, depending on the source and destination IP equal-cost multi-path routing (ECMP) prefix hashing.

Note

Symmetric PBR configurations require 9300-EX hardware.

Sample symmetric PBR REST posts are listed below:

Under fvTenant svcCont

```xml
<vnsSvcRedirectPol name="LoadBalancer_pool">
  <vnsRedirectDest name="lb1" ip="1.1.1.1" mac="00:00:11:22:33:44"/>
  <vnsRedirectDest name="lb2" ip="2.2.2.2" mac="00:de:ad:be:ef:01"/>
  <vnsRedirectDest name="lb3" ip="3.3.3.3" mac="00:de:ad:be:ef:02"/>
</vnsSvcRedirectPol>
<vnsLIFCtx name="external">
  <vnsRsSvcRedirectPol tnVnsSvcRedirectPolName="LoadBalancer_pool"/>
  <vnsRsLIFCtxToBD tDn="uni/tn-solar/bd-fwBD"/>
</vnsLIFCtx>
<vnsAbsNode name="FW" routingMode="redirect">
</vnsAbsNode>
```

Sample symmetric PBR NX-OS-style CLI commands are listed below.

The following commands under the tenant scope create a service redirect policy:

```
apicl(config-tenant)# svcredir-pol fw-external
apicl(config-svcredir-pol)# redir-dest 2.2.2.2 00:11:22:33:44:56
```

The following commands enable PBR:

```
apicl(config-tenant)# l4l7 graph FWOnly contract default
apicl(config-graph)# service FW svcredir enable
```

The following commands set the redirect policy under the device selection policy connector:

```
apicl(config-service)# connector external
apicl(config-connector)# svcredir-pol tenant solar name fw-external
```

Configuring Policy-Based Routing Using the GUI

The following procedure configures policy-based routing using the GUI.

**Step 1**
On the menu bar, choose Tenants > All Tenants.

**Step 2**
In the Work pane, double click the tenant's name.

**Step 3**
In the Navigation pane, choose Tenant tenant_name > L4-L7 Services > L4-L7 Devices.

**Step 4**
In the Work pane, choose Actions > Create L4-L7 Devices.

**Step 5**
In the Create L4-L7 Devices dialog box, complete the fields as required. In the General section, the Service Type can be Firewall or ADC.
Step 6 In the Navigation pane, choose Tenant tenant_name > L4-L7 Services > L4-L7 Service Graph Templates.

Step 7 In the Work pane, choose Action > Create L4-L7 Service Graph Template.

Step 8 In the Create L4-L7 Service Graph Template dialog box, perform the following actions:
   a) In the Graph Name field, enter a name for the service graph template.
   b) For the Graph Type radio buttons, click Create A New One.
   c) Drag and drop the device that you created from the Device Clusters pane to between the consumer endpoint group and provider endpoint group. This creates the service node.
   d) For the Firewall radio buttons, click Routed.
   e) Put a check in the Routed Redirect check box.
   f) Click Submit.

Step 9 In the Navigation pane, choose Tenant tenant_name > Networking > Protocol Policies > L4-L7 Policy Based Routing.

Step 10 In the Work pane, choose Action > Create L4-L7 Policy Based Routing.

Step 11 In the Create L4-L7 Policy Based Routing dialog box, complete the fields as required. This policy-based routing policy is for the consumer connector.

Step 12 Create another policy-based routing policy for the provider connector.

Step 13 In the Navigation pane, choose Tenant tenant_name > L4-L7 Services > L4-L7 Service Graph Templates > service_graph_template_name. Choose the service graph template that you just created.

Step 14 Right click the service graph template and choose Apply L4-L7 Service Graph Template.

Step 15 In the Apply L4-L7 Service Graph Template to EPGs dialog box, perform the following actions:
   a) In the Consumer EPG/External Network drop-down list, choose the consumer endpoint group.
   b) In the Provider EPG/External Network drop-down list, choose the provider endpoint group.
   c) For the Contract radio buttons, click Create A New Contract.
   d) In the Contract Name field, enter a name for the contract.
   e) Do not put a check in the No Filter (Allow All Traffic) check box.
   f) On the Filter Entries table, click + to add an entry.
   g) For the new filter entry, enter "IP" for the name, choose IP for the Ether Type, and click Update.
   h) Click Next.
   i) For the Consumer Connector BD drop-down list, choose the external bridge domain that connects to the consumer endpoint group. The bridge domain must have the Enable the Learning of the Source VTEP on Remote Leafs check box unchecked.
   j) For the Consumer Connector Redirect Policy drop-down list, choose the redirect policy that you created for the consumer connector.
   k) For the Consumer Connector Cluster Interface drop-down list, choose the consumer cluster interface.
   l) For the Provider Connector BD drop-down list, choose the internal bridge domain that connects to the provider endpoint group. The bridge domain must have IP learning disabled.
   m) For the Provider Connector Redirect Policy drop-down list, choose the redirect policy that you created for the provider connector.
   n) For the Provider Connector Cluster Interface drop-down list, choose the provider cluster interface.
   o) Click Next.
   p) Configure the parameters as necessary for the device.
   q) Click Finish.
Configuring Policy-Based Routing Using the NX-OS-Style CLI

The example commands in this procedure include the route redirect, the cluster redirect, and the graph deployment. The device is created under tenant T1. The device is a Cisco ASA virtual device in managed mode; only unmanaged mode devices can be configured using the CLI.

**Step 1** Create the device cluster.

**Example:**
```
1417 cluster name ifav-asa-vm-ha type virtual vlan-domain ACIVswitch service FW function go-to
cluster-device Device2 vcenter ifav108-vcenter vm "ASAv_HA1"
cluster-device Device1 vcenter ifav108-vcenter vm "ASAv_HA"
cluster-interface provider
  member device Device1 device-interface GigabitEthernet0/1
  interface ethernet 1/45 leaf 102
  vnic "Network adapter 3"
  exit
member device Device2 device-interface GigabitEthernet0/1
  interface ethernet 1/45 leaf 102
  vnic "Network adapter 3"
  exit
exit
cluster-interface failover_link
member device Device1 device-interface GigabitEthernet0/8
  interface ethernet 1/45 leaf 102
  vnic "Network adapter 10"
  exit
member device Device2 device-interface GigabitEthernet0/8
  interface ethernet 1/45 leaf 102
  vnic "Network adapter 10"
  exit
exit
cluster-interface consumer
member device Device1 device-interface GigabitEthernet0/0
  interface ethernet 1/45 leaf 102
  vnic "Network adapter 2"
  exit
member device Device2 device-interface GigabitEthernet0/0
  interface ethernet 1/45 leaf 102
  vnic "Network adapter 2"
  exit
exit
```

**Step 2** Under tenant PBRv6_ASA_HA_Mode, deploy the PBR service graph instance.

**Example:**
```
tenant PBRv6_ASA_HA_Mode
  access-list Contract_PBRv6_ASA_HA_Mode_Filter
    match ip
    exit
```

**Step 3** Create a contract for PBR with the filter match IP protocol. Under the subject, specify the Layer 4 to Layer 7 service graph name.
The contract offered by the service appliance provider endpoint group cannot be configured with the allow-all setting.
Example:
contract Contract_PBRv6_ASA_HA_Mode
  scope tenant
  subject Subject
  access-group Contract_PBRv6_ASA_HA_Mode_Filter both
  l4l7 graph PBRv6_ASA_HA_Mode_Graph
  exit
exit
vrf context CTX1
exit
vrf context CTX2
exit

Step 4  Create a bridge domain for the client and server endpoint group. Both the client and server are in the same VRF instance.

Example:
  bridge-domain BD1
  arp flooding
  l2-unknown-unicast flood
  vrf member CTX1
  exit
  bridge-domain BD2
  arp flooding
  l2-unknown-unicast flood
  vrf member CTX1
  exit

Step 5  Create a separate bridge domain for the external and internal leg of the firewall. 
PBR requires the learning of the source VTEP on remote leaf switches to be disabled, which is done using the no ip learning command.

Example:
  bridge-domain External-BD3
  arp flooding
  no-ip learning
  l2-unknown-unicast flood
  vrf member CTX1
  exit
  bridge-domain Internal-BD4
  arp flooding
  no ip learning
  l2-unknown-unicast flood
  vrf member CTX1
  exit

Step 6  Create the application profile and specify the endpoint groups.

Example:
  application AP1
  epg ClientEPG
    bridge-domain member BD1
    contract consumer Contract_PBRv6_ASA_HA_Mode
    exit
  epg ServerEPG
    bridge-domain member BD2
    contract provider Contract_PBRv6_ASA_HA_Mode
    exit
  exit

Step 7  Specify the default gateway for the bridge domains.
Example:

interface bridge-domain BD1
  ipv6 address 89:1:1:1::64/64
  exit
interface bridge-domain BD2
  ipv6 address 99:1:1:1::64/64
  exit

interface bridge-domain External-BD3
  ipv6 address 10:1:1:1::64/64
  exit
interface bridge-domain Internal-BD4
  ipv6 address 20:1:1:1::64/64
  exit

Step 8
Import the device from tenant T1.

Example:

l4l7 cluster import-from T1 device-cluster ifav-asa-vm-ha

Step 9
Create the service graph using the service redirect policy.

Example:

l4l7 graph PBRv6_ASA_HA_Mode_Graph contract Contract_PBRv6_ASA_HA_Mode
  service N2 device-cluster-tenant T1 device-cluster ifav-asa-vm-ha mode FW_ROUTED svcredir
  enable
    connector consumer cluster-interface consumer_PBRv6
    bridge-domain tenant PBRv6_ASA_HA_Mode name External-BD3
    svcredir-pol tenant PBRv6_ASA_HA_Mode name External_leg
    exit
    connector provider cluster-interface provider_PBRv6
    bridge-domain tenant PBRv6_ASA_HA_Mode name Internal-BD4
    svcredir-pol tenant PBRv6_ASA_HA_Mode name Internal_leg
    exit
  exit
connection C1 terminal consumer service N2 connector consumer
connection C2 terminal provider service N2 connector provider
exit

Step 10
Create the service redirect policy for the external and internal legs. IPv6 addresses are used in this example; you can also specify IPv4 addresses using the same command.

Example:

svcredir-pol Internal_leg
  redir-dest 20:1:1:1::1 00:00:AB:CD:00:11
  exit
svcredir-pol External_leg
  redir-dest 10:1:1:1::1 00:00:AB:CD:00:09
  exit
exit
Verifying a Policy-Based Routing Configuration Using the NX-OS-Style CLI

After you have configured policy-based routing, you can verify the configuration using the NX-OS-style CLI.

**Step 1**
Show the running configuration of the tenant.

**Example:**
```
apic1# show running-config tenant PBRv6_ASA_HA_Mode svcredir-pol
# Command: show running-config tenant PBRv6_ASA_HA_Mode svcredir-pol
# Time: Wed May 25 00:57:22 2016
tenant PBRv6_ASA_HA_Mode
  redir-dest 20:1:1:1:1/32 00:00:AB:CD:00:11
  exit
svcredir-pol Internal_leg
  redir-dest 20:1:1:1:1/32 00:00:AB:CD:00:11
  exit
exit
```

**Step 2**
Show the running configuration of the tenant and its service graph.

**Example:**
```
apic1# show running-config tenant PBRv6_ASA_HA_Mode l4l7 graph PBRv6_ASA_HA_Mode_Graph
# Command: show running-config tenant PBRv6_ASA_HA_Mode l4l7 graph PBRv6_ASA_HA_Mode_Graph
tenant PBRv6_ASA_HA_Mode
  l4l7 graph PBRv6_ASA_HA_Mode_Graph contract Contract_PBRv6_ASA_HA_Mode enable
  connector consumer cluster-interface consumer_PBRv6
    bridge-domain tenant PBRv6_ASA_HA_Mode name External-BD3
    svcredir-pol tenant PBRv6_ASA_HA_Mode name External_leg
    exit
  connector provider cluster-interface provider_PBRv6
    bridge-domain tenant PBRv6_ASA_HA_Mode name Internal-BD4
    svcredir-pol tenant PBRv6_ASA_HA_Mode name Internal_leg
    exit
connection C1 terminal consumer service N2 connector consumer connection C2 terminal provider service N2 connector provider
exit
```

**Step 3**
Show the service graph configuration.

**Example:**
```
apic1# show l4l7-graph graph PBRv6_ASA_HA_Mode_Graph
Graph : PBRv6_ASA_HA_Mode-PBRv6_ASA_HA_Mode_Graph
Graph Instances : 1
Consumer EPG : PBRv6_ASA_HA_Mode-ClientEPG
Provider EPG : PBRv6_ASA_HA_Mode-ServerEPG
Contract Name : PBRv6_ASA_HA_Mode-Contract_PBRv6_ASA_HA_Mode
Config status : applied
```
Service Redirect: enabled

<table>
<thead>
<tr>
<th>Connector</th>
<th>Encap</th>
<th>Bridge-Domain</th>
<th>Device Interface</th>
<th>Service Redirect Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>consumer</td>
<td>vlan-241</td>
<td>FBRv6 ASA_HA_</td>
<td>consumer_PBRv6</td>
<td>External_leg</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Mode=External-BD3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>provider</td>
<td>vlan-105</td>
<td>FBRv6 ASA_HA_</td>
<td>provider_PBRv6</td>
<td>Internal_leg</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Mode=Internal-BD4</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>