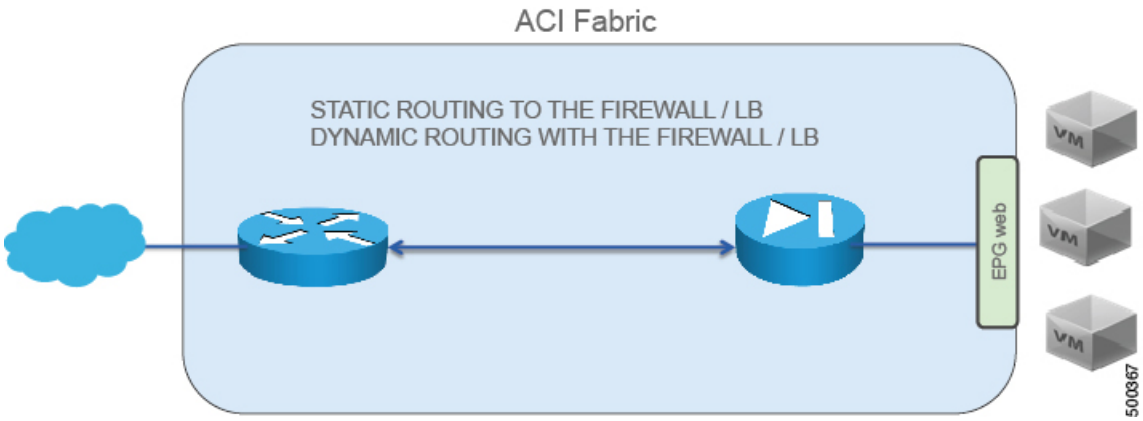
Route Peering

About Route Peering

Route peering is a special case of the more generic Cisco Application Centric Infrastructure (ACI) fabric as a transit use case, in which route peering enables the ACI fabric to serve as a transit domain for Open Shortest Path First (OSPF) or Border Gateway Protocol (BGP) protocols. A common use case for route peering is route health injection, in which the server load balancing virtual IP is advertised over OSPF or internal BGP (iBGP) to clients that are outside of the ACI fabric. You can use route peering to configure OSPF or BGP peering on a service device so that the device can peer and exchange routes with the ACI leaf node to which it is connected.

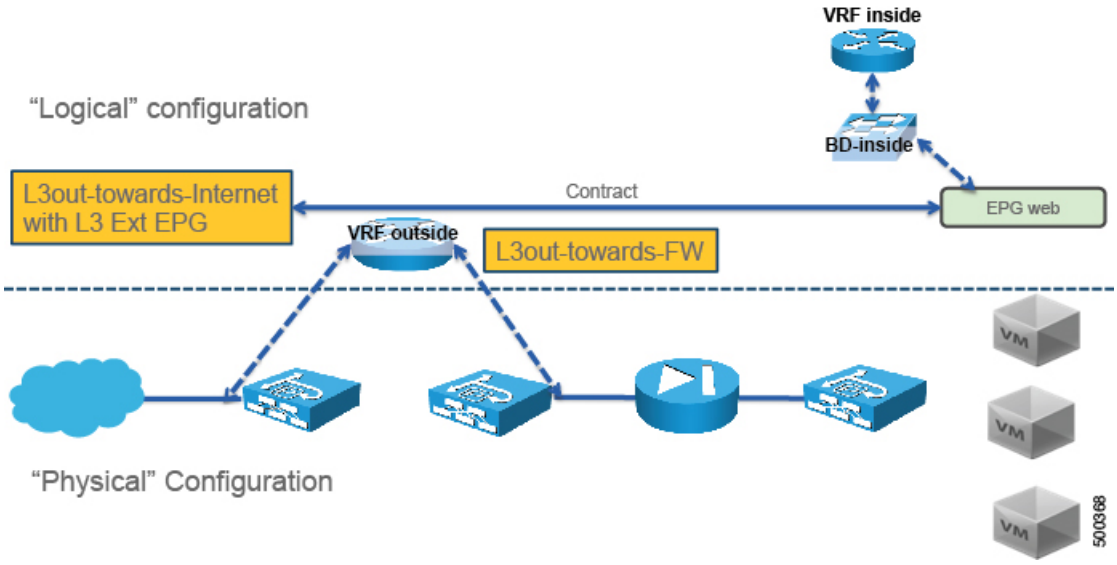
The goal for using route peering is to configure static routing to the firewall or load balancer and to use dynamic routing with the firewall or load balancer, as shown in the following figure:

Figure 1: Route Peering



Route peering requires 2 L3Outs, as shown in the following figure:

Figure 2: The 2 L3Outs Required by Route Peering



If you deploy route peering with a virtual appliance, you must specify the exact physical interface to which the virtual appliance is connected.

For more information about route peering, see *Cisco APIC Layer 4 to Layer 7 Services Deployment Guide* .

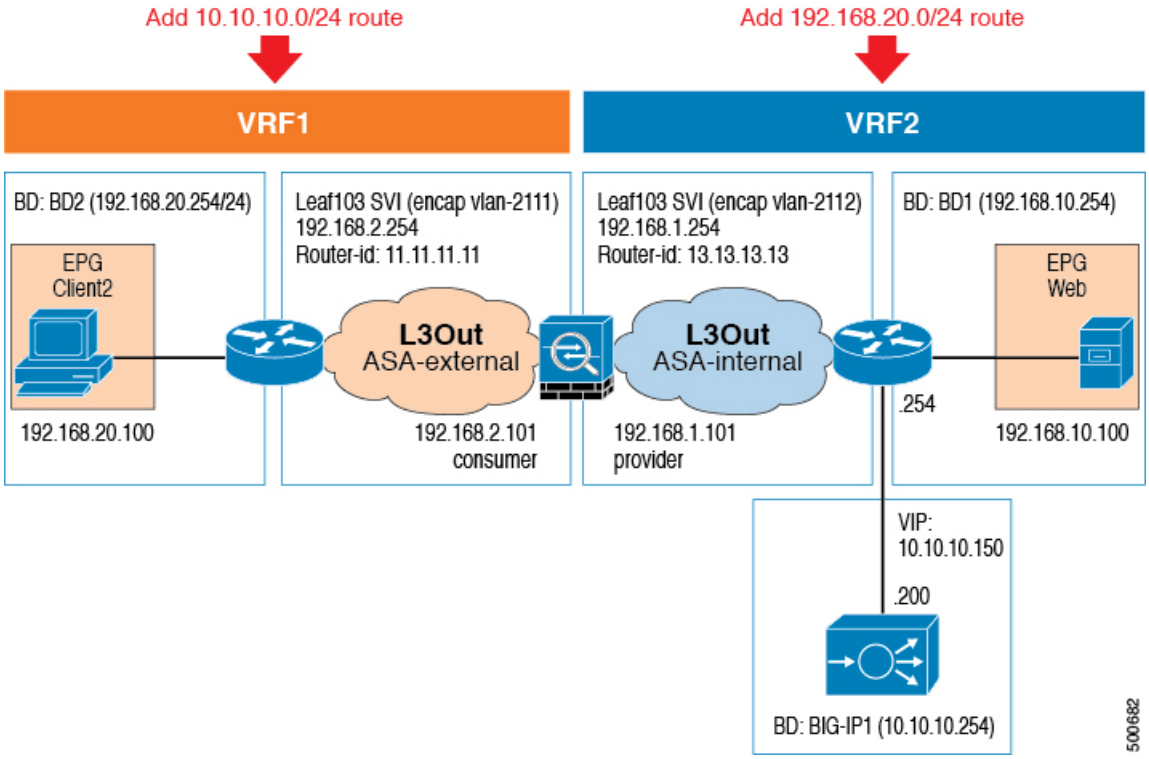
Configuring Route Peering Using the GUI

The following procedure provides an example on how to configure route peering using an ASA device that is part of a two-node service graph. The other service device in the service graph is an F5 BIG-IP device.

This example provides values for most of the fields; the values for your setup will vary. You must fill out mandatory fields even if no example values are given in this procedure. This example uses `T1` as the name of the Tenant.

The following figure illustrates the components that you must configure to use route peering.

Figure 3: Configurng Route Peering



Procedure

Step 1 Create three bridge domains and two VRFs. This procedure uses `BD1`, `BD2`, and `BIG-IP1` as the bridge domains, and `VRF1` and `VRF2` as the VRFs.
See Creating Bridge Domains and VRFs Using the GUI.

1. For `BD1`, in the **VRF** drop-down list, choose **Create VRF** to create `VRF2`.
2. For `BD2`, in the **VRF** drop-down list, choose **Create VRF** to create `VRF1`.
3. For `BIG-IP1`, in the **VRF** drop-down list, choose **VRF2**.

Step 2 On the menu bar, choose **Tenants** > **All Tenants**.

Step 3 In the Work pane, double click the tenant's name.

Step 4 In the Navigation pane, choose **Tenant** ***tenant_name*** > **Security Policies** > **Contracts** > ***contract_name***.
Choose the contract that you will associate with `VRF2`.

Step 5 In the Work pane, choose the **Policy** tab.

Step 6 In the **Scope** drop-down list, if the provider endpoint group and consumer endpoint group are in different tenants, choose **Global**. Otherwise, choose **Tenant**.

Step 7 Click **Submit**.

Step 8 Create an L3Out domain for ASA. On the menu bar, choose **Fabric** > **Access Policies**.

Step 9 In the Navigation pane, choose **Physical and External Domains** > **External Routed Domains**.

Step 10 In the Work pane, choose **Actions** > **Create Layer 3 Domain**.

Step 11 In the **Create Layer 3 Domain** dialog box, fill in the fields as required, except as specified below:

a) In the **Name** field, enter `L3_ASA`.

b) In the **VLAN Pool** drop-down list, choose **Create VLAN Pool**.

Step 12 In the **Create VLAN Pool** dialog box, fill in the fields as required, except as specified below:

a) In the **Name** field, enter `L3out-L4L7`.

b) In the **Encap Blocks** section, add a block with a **VLAN Range** of `2101-2199` and an **Allocation Mode** of **Static Allocation**.

Step 13 Click **Submit**.

Step 14 In the **Create Layer 3 Domain** dialog box, click **Submit**.

Step 15 In the Work pane, verify that `L3_ASA` was created.

Step 16 Create an external routed network with either a static route or OSPF.
To create an external routed network with a static route, see Configuring an External Routed Network for Route Peering with a Static Route Using the GUI, on page 9.

To create an external routed network with OSPF, see Configuring an External Routed Network for Route Peering with OSPF Using the GUI, on page 11.

In either case, use the values for the first external routed network.

Step 17 Create a second external routed network using the same protocol as the previous step.
To create an external routed network with a static route, see Configuring an External Routed Network for Route Peering with a Static Route Using the GUI, on page 9.

To create an external routed network with OSPF, see Configuring an External Routed Network for Route Peering with OSPF Using the GUI, on page 11.

In either case, use the values for the second external routed network.

Step 18 Create an ASA function profile in the `Common` tenant.
See Creating a Function Profile Using the GUI.

The following differences in the steps are specific to route peering.

In the **Create Routed Outside** dialog box:

1. In the **Name** field, enter `ASA-routed`.
2. In the **Profile Group** drop-down list, choose **ASA-FP**.
3. In the **Copy Existing Profile Parameters** check box, put a check in the box.
4. In the **Profile** drop-down list, choose **CISCO-ASA-1.2/WebPolicyForRoutedMode**.
5. In the **Basic Parameters** section, configure the parameters as necessary. In the example setup, set the following parameters:

L4-L7 Parameter or Folder	Usage and Notes
Device Config > Interface Related Configuration - externalIf > Interface Specific Configuration - externalIfCfg > IPv4 Address Configuration > IPv4 Address parameter.	Set the value to 192.168.2.101/255.255.255.0.
Device Config > Interface Related Configuration - externalIf > Static Routes List > IPv4 Route > Gateway parameter	Set the value to 192.168.2.254.
Device Config > Interface Related Configuration - externalIf > Static Routes List > IPv4 Route > Netmask parameter	Set the value to 255.255.255.0.
Device Config > Interface Related Configuration - externalIf > Static Routes List > IPv4 Route > Network parameter	Set the value to 192.168.20.0.
Device Config > Interface Related Configuration - internalIf > Interface Specific Configuration - internalIfCfg > IPv4 Address Configuration > IPv4 Address parameter	Set the value to 192.168.1.101/255.255.255.0.
Device Config > Interface Related Configuration - internalIf > Static Routes List > IPv4 Route > Gateway folder	Set the value to 192.168.1.254.
Device Config > Interface Related Configuration - internalIf > Static Routes List > IPv4 Route > Netmask parameter	Set the value to 255.255.255.0.
Device Config > Interface Related Configuration - internalIf > Static Routes List > IPv4 Route > Network	Set the value to 10.10.10.0.

6 Click **Submit**.

Step 19 Create a BIG-IP function profile in the Common tenant.
See Creating a Function Profile Using the GUI.

The following differences in the steps are specific to this scenario.

1. In the **Name** field, enter `BIGIP-routed`.
2. In the **Profile Group** drop-down list, choose **BIGIP-FP**.
3. In the **Copy Existing Profile Parameters** check box, put a check in the box.
4. In the **Profile** drop-down list, choose **CISCO-BIGIP-1.2/WebPolicyForRoutedMode**.
5. In the **Basic Parameters** section, configure the parameters as necessary. In the example setup, set the following parameters:

L4-L7 Parameter or Folder	Usage and Notes
`Device Config > LocalTraffic` folder	Define as `LocalTraffic-HTTP`.
`Device Config > LocalTraffic > Monitor` folder	Define as `Monitor`.
`Device Config > LocalTraffic > Monitor > Number of Monitor Failures to Trigger Service Down` parameter	Define as `FailByAttempts` with a value of `3`.
`Device Config > LocalTraffic > Monitor > Monitor Frequency` parameter	Define as `FrequencySeconds` with a value of `3`.
`Device Config > LocalTraffic > Monitor > Monitor Protocol` parameter	Define as `Type` with a value of `TCP`.
`Device Config > LocalTraffic > Pool` folder	Define as `Pool`.
`Device Config > LocalTraffic > Pool > Load Balancing Method` parameter	Define as `LBMethod` with a value of `ROUND_ROBIN`.
`Device Config > LocalTraffic > Pool > Pool Type` parameter	Define as `PoolType` with a value of `DYNAMIC`.
`Device Config > LocalTraffic > Pool > Pool Monitor` folder	Define as `PoolMonitor`.
`Device Config > LocalTraffic > Pool > Pool Monitor > Select Pool Monitor` parameter	Define as `PoolMonitorRel` with a value of `LocalTraffic-HTTP/Monitor`.
`Device Config > Network` folder	Define as `Network`.
`Device Config > Network > InternalSelfIP` folder	Define as `InternalSelfIP`.
`Device Config > Network > InternalSelfIP > Internal Self IP Address` parameter	Define as `SelfIPAddress` with a value of `10.10.10.200`.

L4-L7 Parameter or Folder	Usage and Notes
Device Config > Network > InternalSelfIP > Internal Self IP Netmask parameter	Define as SelfIPNetmask with a value of 255.255.255.0.
Device Config > Network > InternalSelfIP > Port Lockdown parameter	Define as PortLockdown with a value of NONE.
Device Config > Network > Route folder	Define as Route.
Device Config > Network > Route > Destination IP Address parameter	Define as DestinationIPAddress with a value of 0.0.0.0.
Device Config > Network > Route > Destination Netmask parameter	Define as DestinationNetmask with a value of 0.0.0.0.
Device Config > Network > Route > Next Hop Router IP Address parameter	Define as NextHopIPAddress with a value of 10.10.10.254.
Function Config > Listener folder	Define as Listener-HTTP.
Function Config > Listener > Protocol parameter	Define as Protocol with a value of TCP.
Function Config > Listener > Virtual Server IP Address parameter	Define as DestinationIPAddress with a value of 10.10.10.150.
Function Config > Listener > Virtual Server Netmask parameter	Define as DestinationIPAddress with a value of 255.255.255.255.
Function Config > Listener > Virtual Server Port parameter	Define as DestinationPort with a value of 80.
Function Config > Pool folder	Define as Pool.
Function Config > Pool > EPG Destination Port parameter	Define as EPGDestinationPort with a value of 80.
Function Config > Pool > Select Pool parameter	Define as PoolRel with a value of LocalTraffic-HTTP/Pool.

6 Click **Submit**.

Step 20 Create a service graph template.
See Creating a Layer 4 to Layer 7 Service Graph Template Using the GUI.

The following differences in the steps are specific to route peering.

In the **Create L4-L7 Service Graph Template** dialog box:

1. In the **Graph Name** field, enter `FW-ADC-Graph-Peering`.
2. Drag the ASA device from the **Device Clusters** section and drop it between the consumer endpoint group and provider endpoint group to create a service node.
3. Drag the BIGIP device from the **Device Clusters** section and drop it between the consumer endpoint group and provider endpoint group, next to the ASA device, to create a service node.
4. In the **ASA-5525X-L3 Information** section, for the **Firewall** radio buttons choose **Routed** and for the **Profile** drop-down list choose **common/ASA-FP/ASA-routed**.
5. In the **BIGIP-LTM Information** section, for the **ADC** radio buttons choose **One-Arm** and for the **Profile** drop-down list choose **common/BIGIP-FP/BIGIP-oneARM-FP**.
6. Click **Submit**.

Step 21 (Optional) In the Navigation pane, choose **Tenant** *tenant_name* > **L4-L7 Services** > **L4-L7 Service Graph Templates** > *template_name* > **Function Node -** *node_name* > **provider**.
Choose the service graph template that you just created and the load balancer function node.

a) In the **Attachment Notification** drop-down list, choose **Yes** if you want to use dynamic endpoint attach.

Step 22 Apply the service graph template.
See Applying a Service Graph Template to Endpoint Groups Using the GUI.

The following differences in the steps are specific to route peering.

In the **Apply L4-L7 Service Graph Template to EPGs** dialog box:

1. In the **Consumer EPG / External Network** drop-down list, choose **T1/test/epg-client2**.
2. In the **Provider EPG / External Network** drop-down list, choose **T1/test/epg-web**.
3. In the **Contract Information** section, fill out the fields as required.
4. Click **Next**.
5. In the **BIGIP-LTM Information** section, in the **BD** drop-down list, choose `T1/BIG-IP1`, and in the **Cluster Interface** drop-down list, choose `provider`.
6. In the **ASA-5525X-L3 Information** section, if you choose **Create Router Configuration**, then in the **Create Router Configuration** dialog box, in the **Name** field enter `ASA-RouterID`, and in the **Router ID** field enter `10.10.10.1`.
7. Click **Submit**.
8. In the **Apply L4-L7 Service Graph Template to EPGs** dialog box, in the **ASA-5525X-L3 Information** section, in the **Router Config** drop-down list, choose **T1/ASA-RouterID**.
9. In the **Consumer Connector** section, for the **Type** radio buttons, choose **Route Peering**.
10. In the **L3 Ext Network** drop-down list, choose **T1/ASA-external/ASA-external**.
11. In the **Cluster Interface** drop-down list, choose **consumer**.
12. In the **Provider Connector** section, for the **Type** radio buttons, choose **Route Peering**.
13. In the **L3 Ext Network** drop-down list, choose **T1/ASA-internal/ASA-internal**.
14. In the **Cluster Interface** drop-down list, choose **provider**.
15. Click **Next**.

16 Modify the parameter values if needed.

17 Click **Finish**.

Configuring an External Routed Network for Route Peering with a Static Route Using the GUI

You can configure an external routed network for use with route peering by using a static route. The external routed network specifies the routing configuration in the Cisco Application Centric Infrastructure (ACI) fabric.

You must configure two external routed networks, and as such the following procedure provides two different sets of values—one for each of the networks—where necessary.

Procedure

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_name*** > **Networking** > **External Routed Networks**.

Step 4 In the Work pane, choose **Actions** > **Create Routed Outside**.

Step 5 In the **Create Routed Outside** dialog box, fill in the fields as required, except as specified below:

a) In the **Name** field, enter `ASA-external` for the first external routed network, or `ASA-internal` for the second external routed network.

b) In the **VRF** drop-down list, choose **T1/VRF1** for the first external routed network, or **T1/VRF2** for the second external routed network.

c) Do not put a check in either the **BGP** or **OSPF** check box.

d) In the **External Routed Domain** drop-down list, choose **L3_ASA**.

e) In the **Nodes and Interfaces Protocol Profiles** section, click +.

Step 6 In the **Create Node Profile** dialog box, fill in the fields as required, except as specified below:

a) In the **Name** field, enter `Leaf3-NP`.

b) In the **Nodes** section, click +.

Step 7 In the **Select Node** dialog box, fill in the fields as required, except as specified below:

a) In the **Node ID** drop-down list, choose **topology/pod-1/node-103**.

b) In the **Router ID** field, enter `11.11.11.11` for the first external routed network, or `13.13.13.13` for the second external routed network.

c) In the **Static Routes** section click +.

Step 8 In the **Create Static Route** dialog box, fill in the fields as required, except as specified below:

a) In the **IP Address** field, enter `10.10.10.0/24` for the first external routed network, or `192.168.20.0/24` for the second external routed network.

b) In the **Prefix** section, enter a prefix for the static route.

c) In the **Next Hop Addresses** section, click +.

d) In the **Next Hop IP** column, enter `192.168.2.101` for the first external routed network, or `192.168.1.101` for the second external routed network.
e) Click **Update**.

Step 9 Click **OK**.

Step 10 In the **Select Node** dialog box, click **OK**.

Step 11 In the **Interface Profiles** section, click +.

Step 12 In the **Create Interface Profile** dialog box, fill in the fields as required, except as specified below:
a) In the **Name** field, enter `Leaf3-IP`.
b) In the **Interface** section, choose the **SVI** tab.

Step 13 In the **Interface** section, click +.

Step 14 In the **Select SVI Interface** dialog box, fill in the fields as required, except as specified below:
a) For the **Path Type** buttons, click **Direct Port Channel**.
b) In the **Path** drop-down list, choose **topology/pod-1/paths-103/pathep-[1G-PC-ASA]**.
c) In the **Encap** field, enter `vlan-2111` for the first external routed network, or `vlan-2112` for the second external routed network.
d) In the **IPv4 Primary / IPv6 Preferred Address** field, enter `192.168.2.254` for the first external routed network, or `192.168.1.254` for the second external routed network.
e) (Optional) In the **MTU (bytes)** field, change the value if necessary. This is the maximum transmission unit size, in bytes.
The default value is "inherit", which uses a default value of "9000" on the ACI and typically a default value of "1500" on the remote device. Having different MTU values can cause issues when peering between the ACI and the remote device. If the remote device's MTU value is set to "1500", then set the MTU value on the remote device's `L3Out` object to "9000" to match the ACI's MTU value.

Step 15 Click **OK**.

Step 16 In the **Create Interface Profile** dialog box, click **OK**.

Step 17 In the **Create Node Profile** dialog box, click **OK**.

Step 18 In the **Create Routed Outside** dialog box, click **Next**.

Step 19 In the **External EPG Networks** section, click +.

Step 20 In the **Create External Network** dialog box, fill in the fields as required, except as specified below:
a) In the **Name** field, enter `ASA-external` for the first external routed network, or `ASA-internal` for the second external routed network.
b) In the **Subnet** section, click +.

Step 21 In the **Create Subnet** dialog box, fill in the fields as required, except as specified below:
a) In the **IP Address** field, enter `10.10.10.0/24` for the first external routed network, or `192.168.20.0/24` for the second external routed network.
b) In the **Scope** section, put a check in the **External Subnets for the External EPG** check box.

Step 22 Click **OK**.

Step 23 (Optional) Create additional subnets as needed.

Step 24 In the **Create External Network** dialog box, click **OK**.

Step 25 In the **Create Routed Outside** dialog box, click **Finish**.

Configuring an External Routed Network for Route Peering with OSPF Using the GUI

You can configure an external routed network for use with route peering by using OSPF. The external routed network specifies the routing configuration in the Cisco Application Centric Infrastructure (ACI) fabric.

You must configure two external routed networks, and as such the following procedure provides two different sets of values—one for each of the networks—where necessary.

Procedure

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_name*** > **Networking** > **External Routed Networks**.

Step 4 In the Work pane, choose **Actions** > **Create Routed Outside**.

Step 5 In the **Create Routed Outside** dialog box, fill in the fields as required, except as specified below:

a) In the **Name** field, enter `ASA-external` for the first external routed network, or `ASA-internal` for the second external routed network.

b) In the **VRF** drop-down list, choose **T1/VRF1** for the first external routed network, or **T1/VRF2** for the second external routed network.

c) Put a check in the **OSPF** check box.

d) In the **OSPF Area ID** field, enter `0.0.0.1`.

e) For the **OSPF Area Type** buttons, click **Regular area**.

f) In the **External Routed Domain** drop-down list, choose **L3_ASA**.

g) In the **Nodes and Interfaces Protocol Profiles** section, click +.

Step 6 In the **Create Node Profile** dialog box, fill in the fields as required, except as specified below:

a) In the **Name** field, enter `Leaf3-NP`.

b) In the **Nodes** section, click +.

Step 7 In the **Select Node** dialog box, fill in the fields as required, except as specified below:

a) In the **Node ID** drop-down list, choose **topology/pod-1/node-103**.

b) In the **Router ID** field, enter `11.11.11.11` for the first external routed network, or `13.13.13.13` for the second external routed network.

c) In the **Static Routes** section click +.

Step 8 Click **OK**.

Step 9 In the **Select Node** dialog box, click **OK**.

Step 10 In the **Interface Profiles** section, click +.

Step 11 In the **Create Interface Profile** dialog box, fill in the fields as required, except as specified below:

a) In the **Name** field, enter `Leaf3-IP`.

b) In the **Interface** section, choose the **SVI** tab.

Step 12 In the **Interface** section, click +.

Step 13 In the **Select SVI Interface** dialog box, fill in the fields as required, except as specified below:

a) For the **Path Type** buttons, click **Direct Port Channel**.

b) In the **Path** drop-down list, choose **topology/pod-1/paths-103/pathep-[1G-PC-ASA]**.
c) In the **Encap** field, enter `vlan-2111` for the first external routed network, or `vlan-2112` for the second external routed network.
d) In the **IPv4 Primary / IPv6 Preferred Address** field, enter `192.168.2.254` for the first external routed network, or `192.168.1.254` for the second external routed network.
e) (Optional) In the **MTU (bytes)** field, change the value if necessary. This is the maximum transmission unit size, in bytes.
The default value is "inherit", which uses a default value of "9000" on the ACI and typically a default value of "1500" on the remote device. Having different MTU values can cause issues when peering between the ACI and the remote device. If the remote device's MTU value is set to "1500", then set the MTU value on the remote device's `L3Out` object to "9000" to match the ACI's MTU value.

Step 14 Click **OK**.
Step 15 In the **Create Interface Profile** dialog box, click **OK**.
Step 16 In the **Create Node Profile** dialog box, click **OK**.
Step 17 In the **Create Routed Outside** dialog box, click **Next**.
Step 18 In the **External EPG Networks** section, click **+**.
Step 19 In the **Create External Network** dialog box, fill in the fields as required, except as specified below:
a) In the **Name** field, enter `ASA-external` for the first external routed network, or `ASA-internal` for the second external routed network.
b) In the **Subnet** section, click **+**.
Step 20 In the **Create Subnet** dialog box, fill in the fields as required, except as specified below:
a) In the **IP Address** field, enter `192.168.20.0/24` for the first external routed network (`ASA-external`), or `10.10.10.0/24` for the second external routed network (`ASA-internal`).
b) In the **Scope** field, choose **Export Route Control Subnet**.
Step 21 Click **OK**.
Step 22 (Optional) Create additional subnets as needed.
Step 23 In the **Create External Network** dialog box, click **OK**.
Step 24 In the **Create Routed Outside** dialog box, click **Finish**.
Step 25 In the Navigation pane, choose ***tenant_name*** > **Networking** > **VRFs** > **VRF1** for the first external routed network, or ***tenant_name*** > **Networking** > **VRFs** > **VRF2** for the second external routed network..
Step 26 In the Work pane, in the **Route Tag Policy** drop-down list, choose **Create Route Tag Policy**.
Step 27 In the **Create Route Tag Policy** dialog box, fill in the fields as required, except as specified below:
a) In the **Name** field, enter `Tag-100` for the first external routed network, or `Tag-200` for the second external routed network.
b) In the **Tag** drop-down list, choose **100** for the first external routed network, or `200` for the second external routed network.
c) Click **Submit**.
Step 28 Click **Submit**.

Verifying a Route Peering With a Static Route Configuration Using the GUI

After configuring a setup to use route peering with a static route, you can verify the configuration with the following procedure.

Procedure

Step 1 Verify the service graph deployment.
See Verifying a Service Graph Deployment Using the GUI

For the deployed devices, you should see `ASA-5525X-L3-none` and `BIGIP-LTM-VRF2`.

For the ASA-5525X-L3 cluster interfaces, you should see `ASA-5525X-L3_consumer` and `ASA-5525X-L3_provider`[

Step 2 Using the CLI on the leaf switch, verify that the IP routing table for `VRF1` is correct.

```
Leaf3# show ip route vrf T1:VRF1
...
10.10.10.0/24, ubest/mbest: 1/0
    *via 192.168.2.101, vlan15, [1/0], 17:29:50, static
11.11.11.11/32, ubest/mbest: 2/0, attached, direct
    *via 11.11.11.11, lo3, [1/0], 4d23h, local, local
    *via 11.11.11.11, lo3, [1/0], 4d23h, direct
192.168.2.0/24, ubest/mbest: 1/0, attached, direct
    *via 192.168.2.254, vlan15, [1/0], 17:29:50, direct
192.168.2.254/32, ubest/mbest: 1/0, attached
    *via 192.168.2.254, vlan15, [1/0], 17:29:50, local, local
192.168.20.0/24, ubest/mbest: 1/0, attached, direct, pervasive
    *via 10.0.80.64%overlay-1, [1/0], 01:53:21, static
```

The route peering IP route is shown in bold.

Step 3 Verify that the IP routing table for `VRF2` is correct.

```
Leaf3# show ip route vrf T1:VRF2
...
10.10.10.0/24, ubest/mbest: 1/0, attached, direct, pervasive
    *via 10.0.80.64%overlay-1, [1/0], 01:54:10, static
10.10.10.254/32, ubest/mbest: 1/0, attached
    *via 10.10.10.254, vlan17, [1/0], 01:54:10, local, local
192.168.1.0/24, ubest/mbest: 1/0, attached, direct
    *via 192.168.1.254, vlan16, [1/0], 02:08:12, direct
192.168.1.254/32, ubest/mbest: 1/0, attached
    *via 192.168.1.254, vlan16, [1/0], 02:08:12, local, local
192.168.10.0/24, ubest/mbest: 1/0, attached, direct, pervasive
    *via 10.0.80.64%overlay-1, [1/0], 01:54:10, static
192.168.20.0/24, ubest/mbest: 1/0
    *via 192.168.1.101, vlan16, [1/0], 02:08:12, static
```

The route peering IP route is shown in bold.

Step 4 Verify that the routing table is correct.

```
ASA5525X/T1# show route
...
S*    0.0.0.0 0.0.0.0 [1/0] via 172.16.255.254, management
S        10.10.10.0 255.255.255.0 [1/0] via 192.168.1.254, internalIf
C        172.16.0.0 255.255.0.0 is directly connected, management
L        172.16.0.101 255.255.255.255 is directly connected, management
C        192.168.1.0 255.255.255.0 is directly connected, internalIf
L        192.168.1.101 255.255.255.255 is directly connected, internalIf
C        192.168.2.0 255.255.255.0 is directly connected, externalIf
L        192.168.2.101 255.255.255.255 is directly connected, externalIf
S     192.168.20.0 255.255.255.0 [1/0] via 192.168.2.254, externalIf
```

The route peering routes are shown in bold.

Verifying a Route Peering With OSPF Configuration Using the GUI

After configuring a setup to use route peering with OSPF, you can verify the configuration with the following procedure.

Procedure

Step 1 Verify the service graph deployment.
See Verifying a Service Graph Deployment Using the GUI

For the deployed devices, you should see `ASA-5525X-L3-none` and `BIGIP-LTM-VRF2`.

For the ASA-5525X-L3 cluster interfaces, you should see `ASA-5525X-L3_consumer` and `ASA-5525X-L3_provider`[

Step 2 Using the CLI on the leaf switch, verify that the IP routing table for `VRF1` is correct.

```
Leaf3# show ip route vrf T1:VRF1
...
10.10.10.0/24, ubest/mbest: 1/0
    *via 192.168.2.101, vlan20, [110/20], 00:00:27, ospf-default, type-2, tag 200
11.11.11.11/32, ubest/mbest: 2/0, attached, direct
    *via 11.11.11.11, lo3, [1/0], 5d02h, local, local
    *via 11.11.11.11, lo3, [1/0], 5d02h, direct
192.168.1.0/24, ubest/mbest: 1/0
    *via 192.168.2.101, vlan20, [110/14], 00:15:51, ospf-default, intra
192.168.2.0/24, ubest/mbest: 1/0, attached, direct
    *via 192.168.2.254, vlan20, [1/0], 00:30:04, direct
192.168.2.254/32, ubest/mbest: 1/0, attached
    *via 192.168.2.254, vlan20, [1/0], 00:30:04, local, local
192.168.20.0/24, ubest/mbest: 1/0, attached, direct, pervasive
    *via 10.0.80.64%overlay-1, [1/0], 00:16:02, static
```

The route peering IP route is shown in bold.

Step 3 Verify that the IP routing table for VRF2 is correct.

```
Leaf3# show ip route vrf T1:VRF2
...
10.10.10.0/24, ubest/mbest: 1/0, attached, direct, pervasive
    *via 10.0.80.64%overlay-1, [1/0], 00:16:05, static
10.10.10.254/32, ubest/mbest: 1/0, attached
    *via 10.10.10.254, vlan13, [1/0], 00:16:05, local, local
192.168.1.0/24, ubest/mbest: 1/0, attached, direct
    *via 192.168.1.254, vlan16, [1/0], 04:48:44, direct
192.168.1.254/32, ubest/mbest: 1/0, attached
    *via 192.168.1.254, vlan16, [1/0], 04:48:44, local, local
192.168.2.0/24, ubest/mbest: 1/0
    *via 192.168.1.101, vlan16, [110/14], 00:15:53, ospf-default, intra
192.168.10.0/24, ubest/mbest: 1/0, attached, direct, pervasive
    *via 10.0.80.64%overlay-1, [1/0], 00:01:52, static
192.168.20.0/24, ubest/mbest: 1/0
    *via 192.168.1.101, vlan16, [110/20], 00:01:48, ospf-default, type-2, tag 100
```

The route peering IP route is shown in bold.

Step 4 Verify that the routing table is correct.

```
ASA5525X/T1# show route
...
S*    0.0.0.0 0.0.0.0 [1/0] via 172.16.255.254, management
O E2     10.10.10.0 255.255.255.0
           [110/20] via 192.168.1.254, 00:00:32, internalIf
C        172.16.0.0 255.255.0.0 is directly connected, management
L        172.16.0.101 255.255.255.255 is directly connected, management
C        192.168.1.0 255.255.255.0 is directly connected, internalIf
L        192.168.1.101 255.255.255.255 is directly connected, internalIf
C        192.168.2.0 255.255.255.0 is directly connected, externalIf
L        192.168.2.101 255.255.255.255 is directly connected, externalIf
O E2     192.168.20.0 255.255.255.0
           [110/20] via 192.168.2.254, 00:00:32, externalIf
```

The route peering routes are shown in bold.