Cisco Unified Fabric Innovations: Deploy a Layer 3 Firewall and a Tenant-Edge Firewall

White Paper

Last Updated: 1/9/2015
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>3</td>
</tr>
<tr>
<td>Target Audience</td>
<td>3</td>
</tr>
<tr>
<td>Prerequisites</td>
<td>3</td>
</tr>
<tr>
<td><strong>Overview of Design and Connectivity in Cisco Unified Fabric Networks with Integrated Firewalls</strong></td>
<td>3</td>
</tr>
<tr>
<td>Typical Firewall Deployments in the Data Center</td>
<td>3</td>
</tr>
<tr>
<td>Introduction to Optimized Networking in Cisco Unified Fabric</td>
<td>4</td>
</tr>
<tr>
<td><strong>Overview of Firewall and Cisco Unified Fabric Network Integration</strong></td>
<td>5</td>
</tr>
<tr>
<td>Service Node Integration</td>
<td>5</td>
</tr>
<tr>
<td>Service Node Deployment</td>
<td>5</td>
</tr>
<tr>
<td>Service Policy Creation</td>
<td>6</td>
</tr>
<tr>
<td>Cisco Unified Fabric Network Integration</td>
<td>6</td>
</tr>
<tr>
<td><strong>Planning and Configuring Network Autoconfiguration Profiles</strong></td>
<td>6</td>
</tr>
<tr>
<td>Service Network Autoconfiguration Profiles Overview</td>
<td>7</td>
</tr>
<tr>
<td>Planning and Configuring a Service Network Autoconfiguration Profile</td>
<td>11</td>
</tr>
<tr>
<td>Case 1a: Unified Fabric with Tenant-Edge Firewall and Dynamic Routing Protocol (OSPF)</td>
<td>13</td>
</tr>
<tr>
<td>Case 1b: Unified Fabric with Tenant-Edge Firewall and Static Routing</td>
<td>16</td>
</tr>
<tr>
<td>Case 1c: Unified Fabric with Tenant-Edge Firewall, Redundant Connectivity, and Dynamic Routing</td>
<td>18</td>
</tr>
<tr>
<td>Case 2a: Unified Fabric with East-West Layer 3 Firewall and Dynamic Routing Protocol (OSPF)</td>
<td>20</td>
</tr>
<tr>
<td>Case 2b: Unified Fabric with East-West Layer 3 Firewall and Static Routing</td>
<td>21</td>
</tr>
<tr>
<td>Autoconfiguration Profiles for Typical Deployment Use Cases</td>
<td>22</td>
</tr>
<tr>
<td><strong>Tenant-Edge Firewall Deployment Example with Cisco Unified Fabric</strong></td>
<td>25</td>
</tr>
<tr>
<td>Sample Scenario</td>
<td>25</td>
</tr>
<tr>
<td>vPC+ Configuration Details</td>
<td>28</td>
</tr>
<tr>
<td>Cisco Prime DCNM Configuration</td>
<td>29</td>
</tr>
<tr>
<td><strong>Appendix: Configuration Profiles (CLI Configurations)</strong></td>
<td>36</td>
</tr>
</tbody>
</table>
Introduction

It’s hard to imagine a modern data center without applications and Layer 4 to 7 services, which among other benefits help address various security, scalability, and high-availability requirements. This document provides both an overview and detailed information about how to integrate physical and virtual firewalls with the Cisco® Unified Fabric with automation.

The primary goal of this document is to help readers gain a basic and advanced level of knowledge of how to implement some typical firewall deployments in the data center using Cisco Unified Fabric with automation.

This document is structured to help readers gain knowledge as they progress through the sections, building from the basic terms and concepts to advanced topics for planning the deployment.

Readers will learn about typical firewall deployments and network designs and get a brief introduction to optimized networking in the Cisco Unified Fabric. Readers also will learn about how to integrate a firewall into the network and the tool set that the Cisco Unified Fabric provides to simplify error-prone and routine tasks. Equipped with this knowledge, readers will be presented with several examples that illustrate how to integrate firewalls into Cisco Unified Fabric using optimized networking and automation.

Target Audience

This document is written for network architects; network design, planning, and implementation teams; and application services and maintenance teams.

Prerequisites

Readers should be familiar with the fundamental concepts and terms Cisco Unified Fabric with automation before proceeding with this document.

A professional (Cisco CCNP®) or higher level of knowledge of routing and switching protocols and network deployment best practices is highly recommended.

Overview of Design and Connectivity in Cisco Unified Fabric Networks with Integrated Firewalls

Typical Firewall Deployments in the Data Center

The history of networking and service appliances development reveals growth from simple single-server applications to clusters of multiple front-end and back-end servers and a shift from simple logic-based rules to more advanced URL- and context-based filtering and load balancing. These changes guided the evolution of network designs, resulting in many niche and specialized network designs that nevertheless share the same fundamental requirements: physical and virtual service appliances must be attached to the network and be reachable through static or dynamic routing. Depending on the deployment case, these service appliances may also need to attach to one or more Layer 2 domains and connect to a separate management network.
Table 1 summarizes some typical firewall deployment scenarios in traditional data centers.

<table>
<thead>
<tr>
<th>Deployment Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tenant-edge firewall</td>
<td>The firewall acts as an ultimate gateway for a particular tenant (Virtual Routing and Forwarding [VRF] instance). All traffic that needs to leave a particular VRF instance must traverse this firewall and be subjected to its policies and filtering. In this scenario, the tenant can consist of one or more subnets. The inside interface of the tenant-edge firewall is attached to a subnet within a given tenant (VRF instance), and the external interface connects to an external VRF instance. This scenario is sometimes referred to as VRF stitching.</td>
</tr>
<tr>
<td>East-west Layer 3 firewall</td>
<td>The firewall acts as a default gateway for one of more protected subnets and has one or more internal interfaces attached to these subnets. The outside interface connects to an external unprotected subnet.</td>
</tr>
<tr>
<td>Layer 2 transparent firewall</td>
<td>The firewall acts as a bridge and is inserted between protected and external network segments. The Layer 2 transparent firewall performs VLAN stitching and applies policies to all data traffic that passes through. This deployment scenario is not covered in this document.</td>
</tr>
<tr>
<td>Layer 3 transparent firewall</td>
<td>The firewall acts as a router, attracting traffic for one or more protected subnets, either through routed prefix metrics manipulation or connection between the Layer 2 and 3 aggregation router and the core router. This deployment scenario is not covered in this document.</td>
</tr>
<tr>
<td>Host-based firewall</td>
<td>The firewall can be deployed on a host-by-host basis and is used to protect a given host. This deployment scenario is not covered in this document.</td>
</tr>
</tbody>
</table>

Today, Cisco Nexus® switching platforms, including Cisco Nexus 2000 Series Fabric Extenders, Cisco Nexus 5600 platform switches, and Cisco Nexus 6000 and 7000 Series Switches, can all be deployed in Cisco Unified Fabric with the firewall scenarios listed in Table 1 in the traditional, manual way. In the traditional approach, the firewall connectivity and integration, planning, and implementation are delivered using traditional Layer 2 switching and Layer 3 routing mechanisms, such as Spanning Tree Protocol (STP), Multiple Spanning Tree Protocol (MST), and various First-Hop Redundancy Protocols (FHRPs) such as Hot Standby Router Protocol (HSRP), Virtual Router Redundancy Protocol (VRRP), and Gateway Load Balancing Protocol (GLBP). These are well known and widely deployed protocols with a large number of associated best practices. However, stability or scalability issues may arise when these traditional mechanisms are used for building large Layer 2 fabrics.

Cisco Unified Fabric with optimized networking helps eliminate risks associated with large Layer 2 fabrics by deploying distributed gateways and other mechanisms. To further reduce the risks associated with integration and implementation steps, Cisco Unified Fabric with optimized networking can take advantage of automation and orchestration tools. Workload automation simplifies routine tasks, and optimized networking dramatically improves overall network stability and scalability.

**Introduction to Optimized Networking in Cisco Unified Fabric**

Building a data center fabric has traditionally involved a trade-off between the flexibility of forwarding Ethernet frames at Layer 2 (switching), and the stability and small failure domains of forwarding IP packets at Layer 3 (routing). Optimized networking allows Cisco Unified Fabric to offer the best attributes of Layer 2 switching and Layer 3 routing concurrently. The difficult trade-off decisions no longer need to be made. Cisco Unified Fabric with optimized networking results in small failure domains, with any IP subnet supported anywhere on the fabric concurrently through the use of a simple distributed default gateway mechanism. Redundant switching models for spine and leaf elements also provide N+ redundancy across the entire fabric. Other properties of optimized networking include the Clos topology with high bisectional bandwidth and uniform reachability and deterministic latency.

Optimized networking uses Cisco FabricPath frame encapsulation for efficient forwarding based on a Shortest Path First (SPF) algorithm for unicast and multicast IP traffic. Host and subnet route distribution across the fabric is accomplished using a scalable Multiprotocol Border Gateway Protocol (MP-BGP) control plane.
Cisco Unified Fabric enhances the traditional frame and packet forwarding by improving the Ethernet flood-and-learn concept. By using Cisco FabricPath frame encapsulation and its conversational learning for Layer 2 traffic, Cisco Dynamic Fabric Automation (DFA) uses the forwarding methodology of frame routing to overcome logical single-tree topologies. By adding a control plane for host and subnet reachability, unnecessary flooding can be reduced by using proactive learning. In addition to the enhanced control plane and data plane for unicast and multicast forwarding, Cisco DFA reduces the Layer 2 failure domain by having the Layer 2 and Layer 3 demarcation on the host-connected leaf switch, terminating the host-originated discovery protocols at this layer.

The use of the distributed proxy or anycast gateway technology on all leaf switches for a given VLAN also improves resilience and allows the fabric to scale to a larger number of hosts.

A major difference between the distributed gateway technology in Cisco Unified Fabric and anycast HSRP and other traditional FHRPs such as HSRP, VRRP, and GLBP is the absence of a hello exchange between the various leaf nodes participating and serving the same virtual IP address. Each Cisco Unified Fabric leaf provides the same gateway-pervasive MAC address and IP address for a given subnet without using any additional anycast of hello control-plane protocol.

Overview of Firewall and Cisco Unified Fabric Network Integration

Typically, network and application teams work together to deploy Firewalls. This process can be divided into three main tasks: network service node integration, service node deployment, and service policy creation. The manual steps for accomplishing each main task are presented here.

Service Node Integration

Service node integration includes the following steps:

- Set a relevant Layer 2 configuration on port of the network access device (leaf node): trunk or access port, VLAN membership, mapping of the bridge domain and VLAN to the segment ID, selection of a forwarding mode (Enhanced Forwarding, Traditional Forwarding, or Layer 2 mode), etc.
- Set a relevant Layer 3 configuration on the network access device (leaf node): switch virtual interface (SVI) IP address and mask, VRF membership, static routing or dynamic routing protocol (when applicable), redistribution of service-node-originated route prefixes, etc.
- Attach the service node’s network interfaces to network access devices. This step could also be part of service node deployment.
- Set a relevant Layer 2 and Layer 3 configuration on the port of the service node: VLAN access and trunk, Layer 3 interface and subinterfaces, static or dynamic routing, etc. This step could also be part of service node deployment.

Service Node Deployment

The details of service node deployment are typically vendor specific and may differ depending on scale, high-availability, and performance requirements. Following are general tasks commonly performed when deploying a service node:

- Create a service node: a physical node, virtual machine, or virtual context.
- Create logical inside and outside links: an untagged physical or tagged IEEE 892.1Q subinterface or some other kind of interface, according to the appliances’ capabilities.
- Create a forwarding context: either a single context or multiple contexts, binding inside and outside logical interfaces.
- Create a virtual IP address. This address is used by load balancers to attract traffic to a virtual server farm. This step can also be a part of policy creation.
Service Policy Creation

After a service node is deployed and integrated into the network, you can configure specific policies that control filtering or policing (in the case of a firewall), service redirection and load balancing, application server farms, and other parameters. You can perform this task in a wide variety of ways. Most frequently, application administrators use a web GUI or a command-line interface (CLI) to specify the necessary configurations. As the demand for more efficient and automated orchestration tools arise, GUI and CLI may be replaced by APIs, integrated into orchestrators.

Cisco Unified Fabric Network Integration

With Cisco Unified Fabric, you can manually integrate Firewalls. In addition, you can use the tools built into the fabric to automate many of the steps for service node integration. In the latter case, the network administrator needs to provision all relevant network autoconfiguration profiles in Cisco Prime™ Data Center Network Manager (DCNM), and the Cisco Unified Fabric will automatically configure an appropriate network profile when the service node is attached to fabric. The details of planning and deploying of such networking profiles and configurations are provided in the next section.

Service node integration and service policy creation tasks can be performed manually through the service appliances GUI, but they can also be automated and orchestrated. Cisco Prime Network Services Controller (NSC) together with orchestrators such as Cisco UCS® Director and OpenStack allow automated deployment of the virtual service nodes and service policies.

Planning and Configuring Network Autoconfiguration Profiles

This section discusses how to plan, manually create, and deploy network autoconfiguration profiles to integrate firewall nodes into Cisco Unified Fabric.

Keep in mind as you plan and configure profiles to integrate firewalls into your data center that unlike traditional in Layer 2 and Layer 3 networks, in Cisco Unified Fabric with optimized networking, hosted workloads gain significant benefits due to the changes in the forwarding behavior. Following are some of the differences:

- When Enhanced Forwarding (EF) mode is configured, Address Resolution Protocol (ARP), Generic Attribute Registration Protocol (GARP), and Neighbor Discovery Protocol (NDP) traffic are contained at the leaf layer. As a benefit, flood and fault domains are reduced to a single switch port on the leaf node. (Typically a top-of-rack [ToR] switch is a leaf node.)
- With Enhanced and Traditional Forwarding modes, Cisco Unified Fabric uses control-plane-based learning, instead of the data-plane-based learning used in traditional Layer 2 networks. BGP is used to distribute end-host reachability information.
- With Enhanced and Traditional Forwarding modes, the default gateway is configured and instantiated on any of the leaf nodes, where the appropriate workload is connected. That is, the same default gateway virtual IP address can exist simultaneously on multiple leaf nodes if end hosts using the same network are attached to multiple leaf nodes.

The Cisco Unified Fabric takes full advantage of common firewall deployment profiles to significantly simplify deployment of security solutions:

- Identify the kind of deployment that is required. Following are some sample deployment scenarios:
  - No firewall, load balancer, or any other Layer 4 to 7 service appliance is deployed. Simple network connectivity for end hosts needs to be provided.
A tenant-edge firewall is deployed, in which all subnets within a given VRF instance must pass through the firewall. Dynamic or static routing needs to be selected for the inside and outside interfaces of the firewall.

An east-west Layer 3 firewall is deployed, in which the firewall is a default gateway for a protected subnet. Dynamic or static routing needs to be selected to connect the outside interface of the firewall.

- Depending on the kind of deployment you prefer, select and configure relevant autoconfiguration profiles in Cisco Prime™ Data Center Network Manager (DCNM) from a prepackaged list.
- Attach end hosts, firewall, and other required appliances to the fabric.
- When static routing is used, manually add static routes on fabric devices.
- Begin using your solution.

Deployment scenarios are not limited to ones listed here. However, Cisco Prime DCNM conveniently comes with prepackaged autoconfiguration profiles for these scenarios because they are the most popular ones. If you are working with atypical deployment cases, you will find relevant information later in this document.

**Service Network Autoconfiguration Profiles Overview**

The autoconfiguration profile is a powerful feature that helps provision the related configuration. It consists of a set of configuration commands, which are grouped together to achieve certain goals and provision a specific function. Provisioning is performed on demand within the Cisco Unified Fabric infrastructure and is directly related to service node integration.

Two types of profiles exist: partition autoconfiguration profiles and network autoconfiguration profiles.

Cisco Unified Fabric with automation stores a predefined set of network autoconfiguration profiles in the OpenLDAP directory service accessible through the Lightweight Directory Access Protocol (LDAP). OpenLDAP runs in Cisco Prime DCNM and stores all the relevant data.

Partition autoconfiguration profiles are included and stored as part of the default leaf configurations and are included as part of the PowerOn Auto Provisioning (POAP) process. The relevant partition profile is populated during instantiation with the parameters received from LDAP.

Network autoconfiguration profiles typically include only the host-side configuration details, such as switch port access and trunk mode, VLAN and bridge domain ID membership, switched virtual interface (SVI) and VRF membership information, the forwarding mode (Enhanced Forwarding, Traditional Forwarding, or plain Layer 2 mode), etc.

Note that a network autoconfiguration profile can specify only its particular VRF membership, but not the VRF definition and VRF configuration itself. The VRF definition and all relevant configurations are defined as part of the partition autoconfiguration. To correlate the two types of autoconfiguration profiles, network profiles are configured with an `include` statement, like this:

```
cfg-profile sampleNetworkProfile
  vlan $vlanId
  vn-segment $segmentId
  --omitted for brevity --
  include profile samplePartitionProfile
end
```
Network profiles are further subdivided into categories (Figure 1):

- **defaultNetwork**: Typically used to connect end hosts
- **serviceNetwork**: Typically used to connect service appliances
- **externalNetwork**: Used to connect outside interfaces of the tenant-edge firewall

**Figure 1.** Subsection of a List of Network Autoconfiguration Profiles Available in Cisco Prime DCNM

This subdivision helps provide a clear logical and functional separation of the profiles.

The network autoconfiguration profile template for attaching an IPv4 host to the fabric and enabling Enhanced Forwarding mode looks like this:

```plaintext
config profile defaultNetworkIpv4EfProfile
  vlan $vlanId  ## VLAN ID, used between the switchport and the host
  vn-segment $segmentId  ## Segment ID, which uniquely identifies this particular L2 domain in the fabric
  mode fabricpath  ## configuring a VLAN to be a FabricPath mode VLAN.
  interface vlan $vlanId  ## SVI for a VLAN ID, used between the switchport and the host
    vrf member $vrfName  ## VRF membership of the SVI for this particular VLAN.
    ip address $gatewayIpAddress/$netMaskLength tag 12345  ## IP and subnet mask of an SVI
```
ip dhcp relay address $dhcpServerAddr use-vrf management ## IP address of DHCP server, where all DHCP requests are redirected
fabric forwarding mode proxy-gateway  ## enabling Enhanced Forwarding mode for this VLAN
no ip redirects
no shutdown
include profile vrf-common  ## including additional “partition” configuration profile
end

Note the variables within the profile. These variables within a particular template are replaced with an actual value, stored in the OpenLDAP directory service. These values are specified during profile creation in Cisco Prime DCNM, as shown in Figure 2.

**Figure 2.** Configuring a Network Autoconfiguration Profile in Cisco Prime DCNM

As you can see, the `defaultNetworkIpv4EfProfile` profile configuration specifies the VLAN ID and segment ID for a given network, the SVI IP address, and VRF membership, as well as fabric forwarding mode, which in this case is Enhanced Forwarding.

Also, the `include profile vrf-common` configuration means that the following autoconfiguration profile will be used as well:

```
configure profile vrf-common
  vrf context $vrfName  ## defining a VRF context
  vni $include_vrfSegmentId  ## configuring a Virtual Network Identifier for VRF-specific Layer 3 fabric communications.
  rd auto  ## configuring route distinguisher with “router-id:vrf-id” format, where router-id is an identifier for a backbone VLAN and source interface of the BGP configuration.
  address-family ipv4 unicast  ## configuring ipv4 address family specific
```
route-target import %BORDER_LEAF_RT  ## importing all prefixes originated by border leaf and its’ route-target
route-target both auto
address-family ipv6 unicast  ## configuring ipv6 address family specific details.
route-target import %BORDER_LEAF_RT  ## importing all prefixes originated by border leaf and its’ route-target
route-target both auto
router bgp $asn  ## configuring MP-BGP autonomous system as per PoAP config.
vrf $vrfName  ## configuring a VRF context
address-family ipv4 unicast
  redistribute hmm route-map FABRIC-RMAP-REDIST-HOST  ## redistributing ARP entries converted to /32 prefixes by HMM
  redistribute direct route-map FABRIC-RMAP-REDIST-SUBNET  ## redistributing all prefixes, matching “tag 12345”, like the end-host VLAN/SVI
  maximum-paths ibgp 2  ## allowing 2 paths for iBGP multipathing.
  address-family ipv6 unicast
    redistribute hmm route-map FABRIC-RMAP-REDIST-V6HOST  ## redistributing ARP entries converted to /128 prefixes by HMM
    redistribute direct route-map FABRIC-RMAP-REDIST-SUBNET  ## redistributing all prefixes, matching “tag 12345”, like the end-host VLAN/SVI
    maximum-paths ibgp 2  ## allowing 2 paths for iBGP multipathing
end

Now compare this profile to a service network autoconfiguration profile specifically created to attach an outside interface of the Layer 3 east-west firewall. This profile was created with the assumption that the Layer 3 east-west firewall uses Open Shortest Path First (OSPF) as the routing protocol to exchange the protected network’s reachability information with the fabric.

config profile serviceNetworkIpv4DynamicRoutingFWProfile
  vlan $vlanId  ## same as in previous example
  vn-segment $segmentId  ## same as in previous example
  mode fabricpath  ## same as in previous example
  interface vlan $vlanId  ## same as in previous example
    vrf member $vrfName  ## same as in previous example
    ip address $gatewayIpAddress/$netMaskLength tag 12345  ## same as in previous example
  ip router ospf 5 area 0.0.0.0  ## establishing OSPF adjacency with the appliance
    no shutdown
  router ospf 5  ## defining OSPF routing process on Leaf node.
    vrf $vrfName  ## defining VRF-specific OSPF configuration details
    router-id $gatewayIpAddress  ## configuring router-id as matching with the SVI’s IP
    include profile vrf-common-FW  ## including additional "partition" configuration profile.
End
The first obvious difference is the presence of **service** keyword in the name of the profile. Also, notice that unlike in the profile in the previous example, there is no Dynamic Host Configuration Protocol (DHCP) relay configuration because this profile assumes that the IP address of the appliance will be statically defined. There is also no forwarding mode specified, because the interfaces defined with this profile will be configured as normal switch ports, and subsequently the SVI for such a VLAN is used for route peering with the attached appliance. No end hosts or workloads should be attached to network segment defined by this profile. In addition, the included partition profile is different: **include profile vrf-common-FW**.

```plaintext
configure profile vrf-common-FW
  vrf context $vrfName  ## same as in previous example unless otherwise specified
    vni $include_vrfSegmentId
    rd auto
      address-family ipv4 unicast
      route-target import %BORDER_LEAF_RT
      route-target both auto
    address-family ipv6 unicast
    route-target import %BORDER_LEAF_RT
    route-target both auto
  router bgp $asn
    vrf $vrfName
      address-family ipv4 unicast
        redistribute hmm route-map FABRIC-RMAP-REDIST-HOST
        redistribute direct route-map FABRIC-RMAP-REDIST-SUBNET
        maximum-paths ibgp 2
        redistribute ospf 5 route-map ospfMap  ## redistribute all dynamically learned OSPF prefixes into BGP.
        address-family ipv6 unicast
        redistribute hmm route-map FABRIC-RMAP-REDIST-HOST
        redistribute direct route-map FABRIC-RMAP-REDIST-SUBNET
        maximum-paths ibgp 2
    exit
```

Now that you know some of the basic concepts of network and partition autoconfiguration profiles, you can begin to plan and configure network service integration.

### Planning and Configuring a Service Network Autoconfiguration Profile

This section presents several typical deployment scenarios and autoconfiguration profiles to use to implement them. Table 2 at the end of this section summarizes all mandatory and optional configurable options for the autoconfiguration profiles discussed here. Full command-line interface (CLI) configurations for these autoconfiguration profiles are presented in the appendix.

For a step-by-step deployment example, refer to the next section.

The information in this section is provided in the following format:

- Graphical representation of a sample deployment case and respective autoconfiguration profile
- Expected configuration parameters on connected devices
The decision tree that follows should help you identify necessary autoconfiguration profiles to deploy inside and outside interfaces, depending on respective requirements.

**Figure 3.** Decision Tree for Use in Selecting the Necessary Network Autoconfiguration Profile
Case 1a: Unified Fabric with Tenant-Edge Firewall and Dynamic Routing Protocol (OSPF)

Figure 4. Tenant-Edge Firewall with Dynamic Routing Between the Appliance and the Fabric

In the deployment scenario in Figure 4, the Layer 3 tenant-edge firewall acts as an ultimate gateway for a given VRF instance: that is, any traffic destined for or coming from the protected VRF instance has to pass through the Layer 3 tenant-edge firewall. Dynamic routing adjacency between the fabric and the firewall is expected on both the inside and outside interfaces using the OSPF routing protocol. Protected VRF instances can include one or more networks configured with the network autoconfiguration profiles that include the suffix ESProfile in their names, where ES stands for edge service.

Following are some of the configuration parameters for the components:

- Hosts A1 and B1 reside in their respective networks; both networks are part of the VRF instance protected by the tenant edge firewall.
- Cisco Prime DCNM is prepackaged with a variety of autoconfiguration profiles that can be used in this scenario. When configuring networks for the workloads protected by the tenant-edge firewall, make sure that the network autoconfiguration profile name includes the keyword ESProfile. All network autoconfiguration profiles with this keyword are listed in Table 2 at the end of this section.
- The network profiles with the required keyword include a special partition profile: vrf-common-ES. This profile includes a static default route in which the next-hop IP address is the inside interface of the tenant-edge firewall. This routing helps ensure that any traffic originating from hosts in a configured VRF instance pass through the tenant-edge firewall, which serves as the ultimate gateway for all incoming and outgoing data flows.
- The VRF-specific default route in the partition profile is defined by the command ip route 0.0.0.0/0 $include_serviceNodeIpAddress, where the $include_serviceNodeIpAddress variable is defined during creation of the partition in Cisco Prime DCNM (creation of the VRF instance), as shown in Figure 5.
Workloads and hosts must be configured with IP address and default gateway information, either statically or using the DHCP relay function on leaf nodes similar to the configuration described in Case 1a.

- The inside interface of the tenant-edge firewall needs to be configured using the profile serviceNetworkipv4DynamicRoutingESProfile. Note that this profile should be configured as part of the protected VRF instance: that is, the inside VRF instance. This profile promotes the following configurations:
  - The vrf-common-ES partition profile mentioned previously is included and configured.
  - Dynamic routing adjacency between the fabric leaf and the tenant-edge firewall is configured. The fabric leaf expects to establish adjacency using OSPF process 2, area 0.
  - All internal BGP prefixes from the protected VRF instance are shared with the tenant-edge firewall using dynamic OSPF routing adjacency.
  - The OSPF router ID is configured to match the interface VLAN defined with the profile. In other words, all host prefixes that exist in a particular protected VRF instance will be shared with the firewall through the OSPF routing protocol.

- The outside interface of the tenant-edge firewall needs to be configured using the profile externalNetworkipv4DynamicRoutingESProfile. Note that this profile should be configured as part of the external VRF instance. This profile promotes the following configurations:
  - Dynamic routing adjacency between the fabric leaf and the tenant-edge firewall is configured. The fabric leaf expects to establish adjacency using OSPF process 4, area 0. That is, because the OSPF routing protocol process IDs are different, both the inside and the outside interfaces of the tenant-edge firewall can be connected to the same leaf node.
  - The vrf-common-External-Dynamic partition profile (described next) is included and configured.
  - All IP address prefixes dynamically learned from tenant-edge firewall through the OSPF routing protocol are redistributed to the BGP routing protocol of the fabric. If necessary, the tenant-edge firewall performs IP address route summarization before sharing these prefixes with the fabric.
  - The OSPF router ID is configured to match the interface VLAN defined with the profile.
All IP address prefixes from the protected internal VRF instance, or their summarized equivalents, are learned through the tenant-edge firewall and are received in the external VRF through the OSPF routing protocol. OSPF routing adjacency from the leaf node is established with the outside interface of the tenant-edge firewall and then distributed through the fabric BGP. This configuration helps ensure that the only path to the protected internal VRF instance is through the tenant-edge firewall (Figure 6).

**Figure 6.** Logical Network Connectivity Flow for Tenant-Edge, Firewall-Integrated, Unified Fabric Network

- It is expected that the tenant-edge firewall is configured with a static IP address on both the inside and outside interfaces.
- The tenant-edge firewall should configure the default route, where the next-hop IP address is `gatewayIpAddress`, specified in the autoconfiguration profile (`externalNetworkIpv4DynamicRoutingESProfile`) defined for the outside interface.
- In most cases, active-standby tenant-edge firewall redundancy is required. When the active firewall fails, the standby firewall detects this failure through a designated mechanism (in-band or out-of-band keepalive), and in response, starts advertising the network reachability information for a protected VRF instance through the outside interface. Note that in such a node-redundancy deployment case, both the active and standby firewalls use the same kind of network autoconfiguration profiles, with differences in their respective IP addresses (dependent on the firewall vendor); see Figure 7.

**Figure 7.** Active-Standby Tenant-Edge Firewall Redundant Deployment.
Case 1b: Unified Fabric with Tenant-Edge Firewall and Static Routing

Figure 8. Tenant-Edge Firewall with Static Routing Between the Appliance and the Fabric

In the deployment scenario in Figure 8, just as in the previous scenario, the Layer 3 tenant-edge firewall acts as the ultimate gateway for a given VRF instance. However, in the deployment scenario in Figure 8, the tenant-edge firewall does not have any dynamic routing protocol running, but rather has static routes to promote protected network reachability. This difference also dictates a choice of different profiles. Nevertheless, any traffic destined for or coming from the protected VRF instance has to pass through the Layer 3 tenant-edge firewall. The protected VRF instance can include one or more networks configured with network autoconfiguration profiles that include the **ESPProfile** suffix in their names.

Here are some of the configuration parameters for the components:

- Hosts A1 and B1 reside in their respective networks, where both networks are part of the VRF instance protected by the tenant-edge firewall.

- Cisco Prime DCNM is prepackaged with a variety of autoconfiguration profiles that can be used in this scenario. When configuring networks for the workloads protected by the tenant-edge firewall, make sure that the network autoconfiguration profile includes the keyword **ESPProfile**. All network autoconfiguration profiles with this keyword are listed in Table 2 at the end of this section.

- The network profiles with the required keyword include a special partition profile: **vrf-common-ES**. This profile includes a static default route in which the next-hop IP address is the inside interface of the tenant-edge firewall. This routing helps ensure that any traffic that originates from a configured VRF instance uses the tenant-edge firewall, which serves as the ultimate gateway for all incoming and outgoing data flows.

- The VRF-specific default route in the partition profile is defined by the command **ip route 0.0.0.0/0 $include_serviceNodeIpAddress**, where the **$include_serviceNodeIpAddress** variable is defined during creation of the partition in Cisco Prime DCNM (creation of the VRF instance) as shown in the Figure 5.

- Workloads and hosts must be configured with IP address and default gateway information, either statically or by using the DHCP relay function on leaf nodes, similar to the configuration described in Case 1a.
The inside interface of the tenant-edge firewall needs to be configured using the profile `serviceNetworkipv4TfStaticRoutingESPProfile`. Note that this profile is configured as part of the protected VRF instance: that is, the inside VRF instance. This profile promotes the following configurations:

- The `vrf-common-ES` partition profile mentioned previously is configured. This partition profile already includes a default route that points to the IP address of the inside interface of the tenant-edge firewall.
- The inside interface of the tenant-edge firewall requires a set of static routes to every subnet within the protected VRF instance that needs to be reachable through the tenant-edge firewall. The next-hop IP address needs to be equal to `gatewayIpAddress` specified in the `serviceNetworkipv4TfStaticRoutingESPProfile` network autoconfiguration profile.
- The inside interface of the tenant-edge firewall must be statically configured with the IP address.

The outside interface of the tenant-edge firewall needs to be configured using the profile `externalNetworkipv4TfStaticRoutingESPProfile`. Note that this profile is configured as part of the external VRF instance. This profile promotes the following configurations:

- The outside interface of the tenant-edge firewall requires a set of VRF-specific static routes. The default route should point to `gatewayIpAddress` specified in `externalNetworkipv4TfStaticRoutingESPProfile`.
- The leaf node to which the outside interface of the tenant-edge firewall is connected requires a set of VRF-specific static routes to every subnet within the protected VRF instance that needs to be reachable through the tenant-edge firewall. The next-hop IP address needs to be equal to the IP address of the outside interface of the tenant-edge firewall.
- The `vrf-common-Static` partition-profile is included. This partition profile helps ensure that all configured static routes are redistributed in the fabric BGP in the external VRF instance.

Here’s a summary:

- For traffic in the outgoing direction, all networks within the protected VRF instance use the inside IP address of the tenant-edge firewall as the ultimate gateway. The tenant-edge firewall itself uses a default route through the outside interface to the external VRF instance.
- All traffic to networks of the protected VRF instance has to go the tenant-edge firewall. For traffic in the incoming direction, all protected networks are reachable through BGP through the leaf to which the outside interface of the tenant-edge firewall is connected. This leaf is configured with the static routes for all networks in the protected VRF instance, where the next hop is the outside interface of the tenant-edge firewall.
- The firewall is also configured with static routes to reach all the protected networks. The next-hop IP address is the IP address of the gateway to which the inside interface of the tenant-edge firewall is connected.
- The leaf node to which the inside interface of the tenant-edge firewall is attached has full IP reachability to all networks within the protected VRF instance using the fabric BGP.
Case 1c: Unified Fabric with Tenant-Edge Firewall, Redundant Connectivity, and Dynamic Routing

All the preceding scenarios used nonredundant, single-attached appliances. When appliances are attached redundantly to a fabric, additional configuration may be required, depending on the appliance vendor.

When dual-attachment of an appliance is required, the recommended approach is to use enhanced virtual PortChannel (vPC+) technology with the Link Aggregation Control Protocol (LACP) to maintain the working condition of the PortChannel.

Figure 9 shows a firewall with a two-member PortChannel for each inside and outside interface. Depending on the firewall vendor, this setup may not be possible. In those cases in which only two physical ports are available on the firewall, you can use one VLAN to represent the inside network and the second VLAN to represent the outside network. In either case, autoconfiguration profiles will be deployed in the same way.

Figure 9. Attaching the Tenant-Edge Firewall with Redundant Dynamic Routing Using vPC+

Figure 9 shows the tenant-edge firewall with dynamic routing redundantly attached using vPC+. The deployment case is similar to the scenarios described earlier. However, several differences and additional considerations need to be noted:

- Configure vPC+ in the POAP templates of the leaf nodes to which the dual-homed firewall is attached.
- Verify that the `vpc peer-gateway` command is specified as part of the vPC+ domain configuration. This command is required to support dynamic routing over vPC+.
- The Secondary Gateway IPv4 Address field in the network autoconfiguration profiles for both the inside and outside interfaces must be specified. This field is needed to help ensure that SVIs on both vPC+ peers have unique IP addresses, to establish routing adjacency with the tenant-edge firewall.
- The IP address in the Secondary Gateway IPv4 Address field needs to be in the same subnet as `gatewayIpAddress`, as shown in Figure 10.
The tenant-edge firewall will have to establish two OSPF routing adjacencies on each inside and outside interface: that is, the OSPF adjacencies from SVIs on each vPC+ peer.

If dual-node firewall redundancy is implemented in a high-availability cluster, you need to ensure that both firewalls have reliably established OSPF routing adjacency with the fabric. It is especially important that you ensure reliable behavior for failover events.

Dual-node or multinode clusters with multiple identical appliances can be attached to the fabric to facilitate load sharing or hot-standby failover. Depending on the cluster implementation, additional configuration of the network autoconfiguration profiles may be necessary:

- In-band Layer 2 adjacency over a dedicated VLAN
- Out-of-band Layer 2 or Layer 3 connectivity
Case 2a: Unified Fabric with East-West Layer 3 Firewall and Dynamic Routing Protocol (OSPF)

Figure 11. East-West Layer 3 Firewall with Dynamic Routing Between the Appliance and the Fabric

In the deployment scenario in Figure 11, the Layer 3 east-west firewall acts as a default gateway for the protected networks.

Following are some of the configuration parameters for the components:

- Hosts A1 and B1 reside in their respective networks, protected by the firewall. All host networks and outside interface networks in this example belong to the same VRF instance.
- Both workloads residing in the networks and the inside interface of the Layer 3 east-west firewall are defined by the same network autoconfiguration profile: defaultNetworkL2Profile.
- Hosts must be configured with IP address and default gateway information either statically or using a third-party in-band DHCP server. Another option is to configure DHCP relay on the firewall.
- Depending on the firewall capabilities, the inside interfaces can either be configured as separate physical interfaces carrying a single IEEE 802.1Q VLAN each, or as one IEEE 802.1Q trunk carrying multiple VLANs for each of the protected networks.
- The network, to which the outside interface of the firewall is attached, should be configured with the networking autoconfiguration profile serviceNetworkIpv4DynamicRoutingFWProfile.\(^1\)
- The Layer 3 east-west firewall is expected to use OSPF with area 0 as a routing protocol to establish routing adjacency on its outside interface. The firewall also has to advertise all protected networks (inside networks) in area 0 using the OSPF routing protocol.
- The fabric expects to establish OSPF routing adjacency with the firewall on its outside interface and to receive all route prefixes for protected networks through OSPF from the firewall.
- The configuration of the profile serviceNetworkIpv4DynamicRoutingFWProfile for the outside network includes the configuration of the vrf-common-FW partition profile. This partition profile promotes the redistribution of the dynamically learned prefixes from OSPF to the fabric MP-BGP.

\(^1\) The serviceNetworkIpv4DynamicRoutingFWProfile and serviceNetworkIpv4DynamicRoutingLBProfile profiles are equivalent.
Case 2b: Unified Fabric with East-West Layer 3 Firewall and Static Routing

Figure 12. East-West Layer 3 Firewall with Static Routing Between the Appliance and the Fabric

In the deployment scenario in Figure 12, the Layer 3 east-west firewall resides in the same Layer-2 domain(s) as the protected workloads and also acts as a default gateway for the protected networks. Unlike in the previous case, there is no dynamic routing adjacency between with the fabric and the firewall, but instead the static routes are configured on both the firewall and the leaf to which the firewall is attached.

Following are some of the configuration parameters for the components:

- Hosts A1 and B1 reside in their respective networks, protected by the firewall. All host networks and outside interface networks in this example belong to the same VRF instance.

- Both workloads residing in the networks and the inside interface of the Layer 3 east-west firewall are defined by the same network autoconfiguration profile: `defaultNetworkL2Profile`.

- Workloads and hosts have to be configured with IP address and default gateway information either statically or using a third-party in-band DHCP server. Another option is to configure DHCP relay on the firewall.

- Depending on the firewall capabilities, the inside interfaces can be either configured as separate physical interfaces carrying a single IEEE 802.1Q VLAN each, or as one IEEE 802.1Q trunk carrying multiple VLANs for each of the protected networks.

- The network to which the outside interface of the firewall is attached should be configured with the networking autoconfiguration profile `serviceNetworkIpv4TfStaticRoutingFWProfile`. The choice of this Traditional Forwarding mode profile is dictated by the fact that some of the available firewalls on the market show signs of silent-host behavior.

- The Layer 3 east-west firewall is expected to be configured with a static IP address on the outside interface with the default route pointed toward the leaf node to which it is attached. The static route’s next-hop IP address is `gatewayIpAddress`, specified in the autoconfiguration profile.

---

2 The `serviceNetworkIpv4TfStaticRoutingFWProfile` and `serviceNetworkIpv4TfStaticRoutingLBProfile` profiles are equivalent.
On the leaf node for each protected network you need to configure static routes pointed toward the firewall’s outside interface IP address.

The configuration of the Traditional Forwarding mode or Enhanced Forwarding mode of the profile `serviceNetworkipv4TfStaticRoutingFWProfile` for the outside network also includes the configuration of the `vrf-common-Static` partition profile. This partition profile promotes the redistribution of the static IP address routes into the fabric’s MP-BGP.

### Autoconfiguration Profiles for Typical Deployment Use Cases

Table 2 summarizes the autoconfiguration profiles for common deployment scenarios.

**Table 2. Autoconfiguration Profiles for Typical Deployment Scenarios**

<table>
<thead>
<tr>
<th>Network Autoconfiguration Profile Name and Configurable Options</th>
<th>Use Case</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>defaultNetworkIPv4EFProfile</strong></td>
<td>This profile is used to attach regular IPv4-only hosts, appliances, and virtual machines to the fabric with enhanced forwarding and a distributed gateway. All learned ARP entries are converted to/32 prefixes by the host mobility manager (HMM) and distributed throughout the BGP fabric. ARP and GARP broadcast is suppressed at the leaf layer.</td>
</tr>
<tr>
<td>Configurable options:</td>
<td></td>
</tr>
<tr>
<td>• <strong>VLAN ID</strong>: The locally significant VLAN ID between the leaf node and the host</td>
<td></td>
</tr>
<tr>
<td>• <strong>Segment ID</strong>: The globally significant segment ID that uniquely identifies a given bridge domain</td>
<td></td>
</tr>
<tr>
<td>• <strong>VRF membership</strong>: Assigns a given network to a particular VRF instance</td>
<td></td>
</tr>
<tr>
<td>• <strong>Gateway IP address</strong>: IP address for the SVI that will serve as the default gateway for this VLAN</td>
<td></td>
</tr>
<tr>
<td>• <strong>DHCP server address</strong>: The address of the DHCP server from which the DHCP relay will forward DHCP packets, if necessary</td>
<td></td>
</tr>
<tr>
<td>• <strong>Mobility domain</strong>: A value configured in the POAP template that enables identification of the Layer 2 segment ID based on the VLAN and mobility-domain information</td>
<td></td>
</tr>
<tr>
<td>Configurable options also include the partition profile <code>vrf-common</code>.</td>
<td></td>
</tr>
<tr>
<td><strong>defaultNetworkIPv4TfTProfile</strong></td>
<td>This profile is used to attach regular IPv4-only hosts, appliances, and virtual machines to the fabric with Traditional Forwarding and a distributed gateway. All learned ARP entries are converted to/32 prefixes by HMM and distributed throughout the BGP fabric. ARP, GARP, and NDP broadcasts are forwarded throughout the fabric with the intention of finding silent hosts.</td>
</tr>
<tr>
<td>Configurable options:</td>
<td></td>
</tr>
<tr>
<td>• <strong>VLAN ID</strong>: The locally significant VLAN ID between the leaf node and the host</td>
<td></td>
</tr>
<tr>
<td>• <strong>Segment ID</strong>: The globally significant segment ID that uniquely identifies a given bridge domain</td>
<td></td>
</tr>
<tr>
<td>• <strong>VRF membership</strong>: Assigns a given network to a particular VRF instance</td>
<td></td>
</tr>
<tr>
<td>• <strong>Gateway IP address</strong>: IP address for the SVI that will serve as the default gateway for this VLAN</td>
<td></td>
</tr>
<tr>
<td>• <strong>DHCP server address</strong>: The address of the DHCP server from which the DHCP relay will forward DHCP packets, if necessary</td>
<td></td>
</tr>
<tr>
<td>• <strong>Mobility domain</strong>: A value configured in the POAP template that enables identification of the Layer 2 segment ID based on the VLAN and mobility-domain information</td>
<td></td>
</tr>
<tr>
<td>Configurable options also include the partition profile <code>vrf-common</code>.</td>
<td></td>
</tr>
<tr>
<td><strong>defaultNetworkL2Profile</strong></td>
<td>This profile is used to create a single Layer 2 flood domain. That is, all broadcast frames are flooded throughout the domain. In contrast to plain Cisco FabricPath, this Layer 2 profile allows more than 4000 VLANs in the fabric, and each VLAN maps to a segment ID. This profile is used in conjunction with an east-west firewall, where the firewall acts as a default gateway for a protected VLAN. All hosts and inside interfaces of the firewall connect to this VLAN.</td>
</tr>
<tr>
<td>Configurable options:</td>
<td></td>
</tr>
<tr>
<td>• <strong>VLAN ID</strong>: The locally significant VLAN ID between the leaf node and the host</td>
<td></td>
</tr>
<tr>
<td>• <strong>Segment ID</strong>: The globally significant segment ID that uniquely identifies a given bridge domain</td>
<td></td>
</tr>
<tr>
<td>• <strong>Mobility domain</strong>: A value configured in the POAP template that enables identification of the Layer 2 segment ID based on the VLAN and mobility-domain information</td>
<td></td>
</tr>
<tr>
<td>This profile does not include any VRF-specific partition profile.</td>
<td></td>
</tr>
</tbody>
</table>
### Network Autoconfiguration Profile Name and Configurable Options

<table>
<thead>
<tr>
<th>Profile Name</th>
<th>Unimplemented</th>
<th>Use Case</th>
</tr>
</thead>
<tbody>
<tr>
<td>serviceNetworkipv4DynamicRoutingFWProfile</td>
<td>Configurable options:</td>
<td>This profile is used to connect an outside interface of the east-west firewall and establish dynamic routing adjacency between the fabric and the firewall. OSPF routing protocol is used to exchange routing information between the firewall and the fabric. In addition, the included partition profile helps ensure that the learned prefixes for protected networks are redistributed to BGP and shared within a given VRF instance across the fabric.</td>
</tr>
<tr>
<td>serviceNetworkipv44TStaticRoutingFWProfile</td>
<td>Configurable options:</td>
<td>This profile is used to attach an outside interface of the east-west firewall when only static routing between the fabric and the firewall is possible (because of licensing, software capabilities, etc.). On the fabric side, all configured static routes are redistributed in BGP and shared with the rest of the VRF members.</td>
</tr>
<tr>
<td>serviceNetworkipv4DynamicRoutingESProfile</td>
<td>Configurable options:</td>
<td>This profile is used to attach an internal interface of the tenant-edge firewall, which establishes a dynamic routing peer adjacency between the firewall and the fabric using OSPF. The tenant-edge firewall is used as an ultimate exit point from the VRF instance, so all prefixes (BGP and directly connected) from the VRF instance are shared with the firewall through a routing protocol.</td>
</tr>
<tr>
<td>externalNetworkipv4DynamicRoutingESProfile</td>
<td>Configurable options:</td>
<td>This profile is used to connect an external (outside) interface of the tenant-edge firewall and establish dynamic routing peering between the firewall and the fabric using OSPF. All prefixes dynamically learned from the firewall through OSPF are redistributed to BGP to facilitate end-to-end reachability between the external world and the networks within the protected VRF instance.</td>
</tr>
</tbody>
</table>

- **VLAN ID**: The locally significant VLAN ID between the leaf node and the host
- **Segment ID**: The globally significant segment ID that uniquely identifies a given bridge domain
- **VRF membership**: Assigns a given network to a particular VRF instance
- **Gateway IP address**: IP address for the SVI that will serve as the default gateway for this VLAN
- **Mobility domain**: A value configured in the POAP template that enables identification of the Layer 2 segment ID based on the VLAN and mobility-domain information

Configurable options also include partition profile `vrft-common-FW`, which promotes VRF-specific redistribution of all dynamically learned prefixes from OSPF to the fabric MP-BGP.

- **VLAN ID**: The locally significant VLAN ID between the leaf node and the host
- **Segment ID**: The globally significant segment ID that uniquely identifies a given bridge domain
- **VRF membership**: Assigns a given network to a particular VRF instance
- **Gateway IP address**: IP address for the SVI that will serve as the default gateway for this VLAN
- **Mobility domain**: A value configured in the POAP template that enables identification of the Layer 2 segment ID based on the VLAN and mobility-domain information

Configurable options also include partition profile `vrft-common-static`, which promotes VRF-specific redistribution of all locally defined static routes to the fabric MP-BGP.

- **VLAN ID**: The locally significant VLAN ID between the leaf node and the host
- **Segment ID**: The globally significant segment ID that uniquely identifies a given bridge domain
- **VRF membership**: Assigns a given network to a particular VRF instance
- **Gateway IP address**: IP address of the SVI that is the ultimate gateway for the entire protected VRF instance; must be identical to the service node IP address, as shown in Figure 5
- **Autonomous system number (ASN)**: The fabric’s MP-BGP autonomous system number
- **Mobility domain**: A value configured in the POAP template that enables identification of the Layer 2 segment ID based on the VLAN and mobility-domain information

Configurable options also include partition profile `vrft-common-ES`, which promotes injection of the static default route with the next-hop IP address equal to the gateway IP address described above. 

```
$ include_serviceNodeIpAddress
$ include_vrfIngressExitExitId
$ include_vrfEgressExitExitId
$ include_vrfIngressExitExitId
$ include_vrfEgressExitExitId
```

- **VLAN ID**: The locally significant VLAN ID between the leaf node and the host
- **Segment ID**: The globally significant segment ID that uniquely identifies a given bridge domain
- **VRF membership**: Assigns a given network to a particular VRF instance
- **Gateway IP address**: IP address for the SVI that will serve as the default gateway for this VLAN
- **Autonomous system number (ASN)**: The fabric’s MP-BGP autonomous system number
- **Mobility domain**: A value configured in the POAP template that enables identification of the Layer 2 segment ID based on the VLAN and mobility-domain information

```
$ include_serviceNodeIpAddress
$ include_vrfIngressExitExitId
$ include_vrfEgressExitExitId
$ include_vrfIngressExitExitId
$ include_vrfEgressExitExitId
```
### Network Autoconfiguration Profile Name and Configurable Options

<table>
<thead>
<tr>
<th>Profile Name</th>
<th>Configurable Options</th>
<th>Use Case</th>
</tr>
</thead>
</table>
| serviceNetworkIPv4TIStaticRoutingESProfile | Configurable options:  
- **VLAN ID**: The locally significant VLAN ID between the leaf node and the host  
- **Segment ID**: The globally significant segment ID that uniquely identifies a given bridge domain  
- **VRF membership**: Assigns a given network to a particular VRF instance  
- **Gateway IP address**: IP address for the SVI that will serve as the default gateway for this VLAN  
- **Mobility domain**: A value configured in the POAP template that enables identification of the Layer 2 segment ID based on the VLAN and mobility-domain information  
  - Configurable options also include partition profile vrf-common-ES, which promotes injection of the static default route with the next-hop IP address equal to the gateway IP address defined during creation of the parent partition as shown in Figure 5: `ip route 0.0.0.0/0 `\|include_serviceNodelpAddress. | This profile is used to attach the internal interface of the tenant-edge firewall when static routing is used between the firewall and the fabric. This profile can be used when the firewall can't run the routing protocol, or when enabling such a routing protocol would incur additional licensing costs for the customer. The whole fabric will use the attached firewall as an ultimate exit point for a specific VRF instance, but because no dynamic routing protocol is running between the fabric and the firewall, the firewall needs a set of static routes that provide reachability from the outside world to protected VRF instances. |
| externalNetworkIPv4TIStaticRoutingESProfile | Configurable options:  
- **VLAN ID**: The locally significant VLAN ID between the leaf node and the host  
- **Segment ID**: The globally significant segment ID that uniquely identifies a given bridge domain  
- **VRF membership**: Assigns a given network to a particular VRF instance  
- **Gateway IP address**: IP address for the SVI that will serve as the default gateway for this VLAN  
- **Mobility domain**: A value configured in the POAP template that enables identification of the Layer 2 segment ID based on the VLAN and mobility-domain information  
  - Configurable options also include partition profile vrf-common-ES, which promotes injection of the static default route equal to the gateway IP address defined during creation of the parent partition as shown in Figure 5: `ip route 0.0.0.0/0 `\|include_serviceNodelpAddress. | This profile is used to attach an external interface of the tenant-edge firewall in the external VRF instance. A VLAN configured with this profile operates in Traditional Forwarding mode. The included partition profile vrf-common-Static is similar to vrf-common, but also redistributes static routes matched by the route map StaticMap. On the firewall side, an interface needs to be configured with either an IEEE 802.1Q VLAN or a subinterface with a particular VLAN. The static default route is also configured on the firewall. |
| defaultNetworkIPv4EIFProfile | Configurable options:  
- **VLAN ID**: The locally significant VLAN ID between the leaf node and the host  
- **Segment ID**: The globally significant segment ID that uniquely identifies a given bridge domain  
- **VRF membership**: Assigns a given network to a particular VRF instance  
- **Gateway IP address**: IP address for the SVI that will serve as the default gateway for this VLAN  
- **Mobility domain**: A value configured in the POAP template that enables identification of the Layer 2 segment ID based on the VLAN and mobility-domain information  
  - Configurable options also include partition profile vrf-common-ES, which promotes injection of the static default route with the next-hop IP address equal to the gateway IP address defined during creation of the parent partition as shown in Figure 5: `ip route 0.0.0.0/0 `\|include_serviceNodelpAddress. That is, all data traffic that needs to leave from the current VRF will have to be tunneled through the tenant-edge firewall. | This profile is used to attach hosts, virtual machines, and other end-host devices to the tenant-edge firewall protected network. Workloads connected to this network can take advantage of the Enhanced Forwarding mode of Cisco Unified Fabric. You should use this network profile for those protected networks, because all traffic from hosts in such networks go through the edge service device (tenant-edge firewall). Only network autoconfiguration profiles that include vrf-common-ES should be used within the VRF instance protected by the tenant-edge firewall because the vrf-common-ES partition profile has a globally defined static route that directs any outgoing traffic through the tenant-edge firewall. |
| defaultNetworkIPv4TIProfile | Configurable options:  
- **VLAN ID**: The locally significant VLAN ID between the leaf node and the host  
- **Segment ID**: The globally significant segment ID that uniquely identifies a given bridge domain  
- **VRF membership**: Assigns a given network to a particular VRF instance  
- **Gateway IP address**: IP address for the SVI that will serve as the default gateway for this VLAN  
- **Mobility domain**: A value configured in the POAP template that enables identification of the Layer 2 segment ID based on the VLAN and mobility-domain information  
  - Configurable options also include partition profile vrf-common-ES, which promotes injection of the static default route equal to the gateway IP address defined during creation of the parent partition as shown in Figure 5: `ip route 0.0.0.0/0 `\|include_serviceNodelpAddress. | This profile is almost identical to the previous one (defaultNetworkIPv4EIFProfile), except that this profile uses Traditional Forwarding mode in the Cisco Unified Fabric. |

© 2015 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.
<table>
<thead>
<tr>
<th>Network Autoconfiguration Profile Name and Configurable Options</th>
<th>Use Case</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configurable options also include partition profile <strong>vrf-common-ES</strong>, which promotes injection of the static default route with the next-hop IP address equal to the gateway IP address defined during creation of the parent partition as shown in Figure 5: <code>ip route 0.0.0.0 0 $include_serviceNodeIpAddress</code>. That is, all data traffic that needs to leave from the current VRF will have to be tunneled through the tenant-edge firewall.</td>
<td></td>
</tr>
</tbody>
</table>

**Tenant-Edge Firewall Deployment Example with Cisco Unified Fabric**

**Sample Scenario**

The sample scenario presented here builds a multitenant spine-and-leaf data center for a technology company named ABC that has the following departments:

- Sales
- Finance
- Research and development (R&D)

The core business of this company is a knowledge technology, so business requirements dictate the use of a dedicated firewall that filters any ingress and egress traffic from workloads in the R&D department.

Translating the business requirements into lower-level technical details, Company ABC can represent an organization construct in the Cisco Prime DCNM LDAP database, and each department can be represented by a partition construct. Each of the partitions constitutes a VRF instance in the fabric for the subsequently included member networks.

The tenant-edge firewall deployment model is well suited to the customer's requirements.

During the network security design process, the customer determined that the R&D department should be secured using two physical firewalls configured in an active-standby pair: that is, both firewalls would be up and running, but only one of them at a time would be actively engaged in enforcing network security.

Depending on the available features and capabilities of the firewall, the standby unit can maintain routing adjacencies, but start advertising network reachability information only in an event that the active unit fails. For example, Cisco Adaptive Security Appliances (ASA) with Cisco ASA Software Release 9.3 or later support such a configuration and are used as a reference in this deployment example ([http://www.cisco.com/c/en/us/td/docs/security/asa/asa93/configuration/general/asa-general-cli/ha-failover.html#pgfId-1495028](http://www.cisco.com/c/en/us/td/docs/security/asa/asa93/configuration/general/asa-general-cli/ha-failover.html#pgfId-1495028)).

Each firewall has four 10-Gbps links, for a total of 40 Gbps of forwarding capacity.

The customer decided to dedicate two 10-Gbps links of a given firewall for ingress and two 10-Gbps links for the egress direction, with each of the port pairs bundled into IEEE 802.3ad LACP. These firewalls also support dynamic OSPF routing protocol, and each firewall will have a total of six adjacencies:

- Two OSPF adjacencies with each of the SVI interfaces reachable through the inside vPC+ interface
- Two OSPF adjacencies with each of the SVI interfaces reachable through the outside vPC+ interface
- Additional optional adjacencies between respective inside interfaces and respective outside interfaces of the active and standby firewalls (may be needed if the firewall vendor requires such configuration)
Figure 13 shows this scenario.

**Figure 13.** Tenant-Edge Firewall Enforcing Security Policies for All Member Networks of the RnD VRF Instance

A pair of leaf nodes constitutes a vPC+ pair. This pair will establish OSPF dynamic routing adjacencies between the SVIs for the VLANs to which the inside and outside interfaces of the firewalls are attached. This step is an important operational nuance, necessary to provide a consistent and stable environment for the dynamic exchange of IP prefixes using a routing protocol. As a result, the active and standby nodes must both be attached to the same pair of vPC+ leaf nodes.

Translating the customer’s requirements into technical details, the following low-level design needs to be configured (Figure 14):

- The ABC organization consists of three partitions:
  - Sales
  - Finance
  - RnD
- The RnD VRF instance is the partition that needs to be secured by the tenant-edge firewall.
- Only the IPv4 protocol is used in the network.
- Several networks are included in the RnD VRF instance:
  - HW-ENG (hardware engineering): 172.24.8.0/24
  - SW-ENG (software engineering): 172.24.10.0/24
  - FW-INSIDE (network segment to which the inside interface of the tenant-edge firewall is connected): 172.24.6.40/29
- Data forwarding between HW-ENG, SW-ENG, IP-STRG, and FW-INSIDE networks within the fabric is not restricted because they are all part of the same VRF: RnD.
- Data traffic originating from any of the networks in the RnD VRF toward any other network outside this VRF will be sent to the firewall for filtering and policy enforcement.
- Host and workload networks should be configured using one of these two profiles: `defaultNetworkipv4EfESProfile` for Enhanced Forwarding mode, and `defaultNetworkipv4TfESProfile` for Traditional Forwarding mode.
- The FW-INSIDE network should be configured using the following profile: `serviceNetworkipv4DynamicRoutingESProfile`. The firewall will establish dynamic OSPF routing adjacency with the fabric through the inside interface.
- OSPF dynamic routing adjacency from the leaf side is established using OSPF area 0 with process ID 2.
- The design does not require enforcement of OSPF Designated Router (DR) and Backup Designated Router (BDR) roles in the network. However, if such requirements existed, `ospf priority 0` should be configured on the firewalls to prevent them from assuming one of these roles in a given network segment.

**Figure 14.** IP Addresses and OSPF Dynamic Routing Adjacencies Between Inside and Outside Interfaces of the Tenant-Edge Firewall

- The RnD-EXT VRF is the external partition used as a transit VRF for all traffic originating from the RnD VRF and destined for the outside world.
  - The FW-OUTSIDE network is used to connect the outside interface of the tenant-edge firewall: 192.168.14.40/29.
  - The FW-OUTSIDE network should be configured using the following profile: `externalNetworkipv4DynamicRoutingESProfile`. The firewall will establish dynamic OSPF routing adjacency with the fabric through the outside interface.
  - The design does not require enforcement of the OSPF DR and BDR roles in the network. However, if such requirements existed, `ospf priority 0` should be configured on the firewalls to prevent them from assuming one of these roles in a given network segment.
OSPF dynamic routing adjacency from the leaf side is established using OSPF area 0 and process ID 4: that is, OSPF processes are different for the inside and outside interfaces to help ensure process-level separation.

Both active and standby firewalls need to configure a default route with the next-hop IP address simultaneously set to both 192.168.14.41 and 192.168.14.42 (FW-OUTSIDE segment):

- `ciscoasa(config)# route outside 0 0 192.168.14.41`
- `ciscoasa(config)# route outside 0 0 192.168.14.42`


**vPC+ Configuration Details**

As discussed earlier, firewalls need to connect to leaf nodes using vPC+. This section shows the required POAP configuration in Cisco Prime DCNM. The example in Figure 15 shows the POAP settings for only one of the vPC+ peer switches.

**Figure 15.** Enabling the vPC+ Feature and All Other Configurations

![vPC+ Configuration Menu](image)

The vPC+ hosts should be provisioned using the menu shown in Figure 16.
Additionally, make sure that the `vpc peer-gateway` configuration is present on both vPC+ leaf peers.

Cisco Prime DCNM Configuration
The flowchart in Figure 17 shows the configuration steps that need to be performed to deploy tenant-edge firewalls. Depending on the customer’s operational model, step 4 may be moved to the end of this flowchart.

Figure 17. Configuration Steps in Cisco Prime DCNM and Border Leaf Nodes

The steps are shown in more detail here.

**Step 1.** Create an organization in the Cisco Prime DCNM GUI (Figures 18 and 19).

Figure 18. Choose Organization from the Config > Auto-Configuration Menu
Figure 19. Specify a Name for the Created Organization

Step 2. Create a secure partition in the Cisco Prime DCNM GUI (Figure 20).

Figure 20. Specify a Name for the Secure Partition and the Service Node IP Address

As determined earlier (Figure 14), the service node IP address will be the IP address of the inside interface of the tenant-edge firewall: 172.24.6.43. Note that if the active unit fails, the standby unit will assume this IP address with negligible service disruption. The Cisco ASA firewall with Cisco ASA Software Release 9.3 allows the use of a single inside IP address that is up and running on the active firewall unit; in the event of failover, the secondary firewall unit assumes this same IP address (subject to the failover capabilities of the third-party firewalls).

The result of the first two steps is the creation of the ABC organization with the RnD partition in it (Figure 21).

Figure 21. ABC Organization with RnD Partition as Configured in Cisco Prime DCNM

Step 3. Create a service subnet for the inside interface.

As discussed earlier, the serviceNetworkIPv4DynamicRoutingESPProfile profile will be used to define a network segment for the inside interface of the tenant-edge firewall (Figure 22).
Figure 22. FW-INSIDE Network Provisioning in Cisco Prime DCNM GUI Using the serviceNetworkIpV4DynamicRoutingESProfile Profile

IP addresses for both primary and secondary vPC+ peers are specified as discussed previously in this section and shown in Figure 14.

The number in the ASN field should match the ASN of the backbone BGP fabric. This ASN is used in route redistribution to enable end-to-end routing information consistency.

**Step 4.** Create protected subnets with either Enhanced Forwarding or Traditional Forwarding mode (Figures 23, 24, and 25).

In a real-world production environment, it is not always possible to know all the client networks at the beginning, and thus this step can be moved elsewhere in the process, but not earlier than step 2.
Figure 23. HW-ENG Network Provisioning in the Cisco Prime DCNM GUI Using the defaultNetworkipv4EfIESProfile Profile

Figure 24. SW-ENG Network Provisioning in the Cisco Prime DCNM GUI Using the defaultNetworkipv4EfIESProfile Profile
Figure 25. IP-STRG Network Provisioning in the Cisco Prime DCNM GUI Using the defaultNetworkipv4TIESProfile Profile

Figure 26 shows the results of the first four steps.

Figure 26. RnD Protected Partitions for HW-ENG, SW-ENG, IP-STRG, and FW-INSIDE Networks for the Inside Interface of the Tenant-Edge Firewall
Step 5. Create the external VRF instance in the Cisco Prime DCNM GUI (Figure 27).

**Figure 27.** RnD-EXT External Transit Partition Provisioning in the Cisco Prime DCNM GUI

Note that you don’t need to specify the service node IP address in the external transit partition.

Step 6. Create a service subnet for the outside interface.

As in the autoconfiguration profile for the inside interface, you need to configure SVI IP addresses for both the primary and secondary vPC+ peers (Figure 28).

**Figure 28.** FW-OUTSIDE Network Provisioning in the Cisco Prime DCNM GUI Using the externalNetworkIpv4DynamicRoutingESProfile Profile
Figure 29 shows the overall progress in the first six steps. Note that the external transit VRF, RnD-EXT, was autoconfigured with the Layer 3 segment ID (Visual Networking Index [VNI]) set to 50009. You will use this ID in the next steps.

**Figure 29.** Summary of Configured VRF Instances and Networks

<table>
<thead>
<tr>
<th>Organizations (5 rows)</th>
<th>Company ABC</th>
<th>ABC</th>
<th>RnD</th>
<th>VRF protected by the Tenant-Edge Firewall</th>
<th>50008</th>
<th>172.24.6.43</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>RnD-EXT</td>
<td></td>
<td>External transit partition for secured partition “RnD”</td>
<td>50009</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Networks (5 rows)</th>
<th>Segment ID</th>
<th>VLAN ID</th>
<th>Mobility Domain</th>
<th>Profile Name</th>
<th>Subnet:</th>
</tr>
</thead>
<tbody>
<tr>
<td>FW-INSIDE</td>
<td>30010</td>
<td>240</td>
<td>MD-1</td>
<td>servcelnetworkipv4DynamicRoutingESProfile</td>
<td></td>
</tr>
<tr>
<td>HV-ENG</td>
<td>30011</td>
<td>101</td>
<td>MD-1</td>
<td>defaulnetworkipv4EBGPProfile</td>
<td></td>
</tr>
<tr>
<td>SW-ENG</td>
<td>30012</td>
<td>102</td>
<td>MD-1</td>
<td>defaulnetworkipv4EBGPProfile</td>
<td></td>
</tr>
<tr>
<td>IP-STRG</td>
<td>30013</td>
<td>103</td>
<td>MD-1</td>
<td>defaulnetworkipv4EBGPProfile</td>
<td></td>
</tr>
<tr>
<td>FW-OUTSIDE</td>
<td>30014</td>
<td>1301</td>
<td></td>
<td>externaNetworkipv4DynamicRoutingESProfile</td>
<td></td>
</tr>
</tbody>
</table>

**Steps 7 and 8.** Perform additional configuration of border leaf nodes. Define the external VRF and import route target for the external VRF.

The network administrator needs to verify that the border leaf nodes are indeed configured as such in POAP (Figure 30).

**Figure 30.** POAP Configuration to Activate Border Leaf Function

Border leaf functions already include fabric MP-BGP configuration, including injection of the default route to the fabric. However, to pass the IP prefixes of the protected networks to an external service provider edge router, you need to manually add a few commands to the border leaf nodes.

As mentioned in a previous step, the Layer 3 segment ID (VNI) needs to be set to 50009 because it was automatically configured through the Cisco Prime DCNM for the tenant RnD-EXT.

Note that the output shown here is only an incremental addition to the configured MP-BGP.

```
vrf context ABC:RnD-EXT
vni 50009
rd auto
address-family ipv4 unicast
  route-target both auto
address-family ipv6 unicast
  route-target both auto
```
In addition to the preceding configuration, you need to configure peering with the external service provider edge router. In the example here, the customer decided to use the IEEE 802.1Q subinterface with VRF-lite between the border leaf and service provider edge router.

```
router bgp 65500
  vrf ABC:RnD-EXT
  address-family ipv4 unicast
  maximum-paths ibgp 2
  address-family ipv6 unicast
  maximum-paths ibgp 2
```

```
interface E1/32
  no switchport
  no shutdown

interface E1/32.100
  encapsulation dot1q 100
  vrf member ABC:RnD-EXT
  ip address 10.20.10.1/30
  no shutdown

router bgp 65500
  vrf ABC:RnD-EXT
  address-family ipv4 unicast
    maximum-paths 2
    maximum-paths ibgp 2
  neighbor 10.20.10.2 remote-as 350
    peer-type fabric-external
    address-family ipv4 unicast
    send-community both
```

### Appendix: Configuration Profiles (CLI Configurations)

<table>
<thead>
<tr>
<th>Network Autoconfiguration Profile Name and Included Partition Profile</th>
</tr>
</thead>
<tbody>
<tr>
<td>defaultNetworkIpv4EfProfile</td>
</tr>
</tbody>
</table>

```
config profile defaultNetworkIpv4EfProfile
  vlan $vlanId
  vn-segment $segmentId
  mode fabricpath
  interface vlan $vlanId
  vrf member $vrfName
  ip address $gatewayIpAddress/$netMaskLength tag 12345
  ip dhcp relay address $dhcpServerAddr use-vrf management
  fabric forwarding address mode proxy-gateway
```
no ip redirects
no shutdown
include profile vrf-common
end

configure profile vrf-common
  vrf context $vrfName
    vni $include_vrfSegmentId
    rd auto
    address-family ipv4 unicast
      route-target import %BORDER_LEAF_RT
      route-target both auto
    address-family ipv6 unicast
      route-target import %BORDER_LEAF_RT
      route-target both auto
  router bgp $asn
    vrf $vrfName
      address-family ipv4 unicast
        redistribute hmm route-map FABRIC-RMAP-REDIST-HOST
        redistribute direct route-map FABRIC-RMAP-REDIST-SUBNET
        maximum-paths ibgp 2
      address-family ipv6 unicast
        redistribute hmm route-map FABRIC-RMAP-REDIST-V6HOST
        redistribute direct route-map FABRIC-RMAP-REDIST-SUBNET
        maximum-paths ibgp 2
end

defaultNetworkIpv4TfProfile

config profile defaultNetworkIpv4TfProfile
  vlan $vlanId
    vn-segment $segmentId
    mode fabricpath
    interface vlan $vlanId
      vrf member $vrfName
      ip address $gatewayIpAddress/$netMaskLength tag 12345
      ip dhcp relay address $dhcpServerAddr use-vrf management
      fabric forwarding mode anycast-gateway
    no shutdown
    include profile vrf-common
end

configure profile vrf-common
  vrf context $vrfName
    vni $include_vrfSegmentId
rd auto
address-family ipv4 unicast
  route-target import %BORDER_LEAF_RT
  route-target both auto
address-family ipv6 unicast
  route-target import %BORDER_LEAF_RT
  route-target both auto
router bgp $asn
  vrf $vrfName
    address-family ipv4 unicast
      redistribute hmm route-map FABRIC-RMAP-REDIST-HOST
      redistribute direct route-map FABRIC-RMAP-REDIST-SUBNET
      maximum-paths ibgp 2
    address-family ipv6 unicast
      redistribute hmm route-map FABRIC-RMAP-REDIST-V6HOST
      redistribute direct route-map FABRIC-RMAP-REDIST-SUBNET
      maximum-paths ibgp 2
end

**defaultNetworkL2Profile**

config profile defaultNetworkL2Profile
  vlan $vlanId
    vn-segment $segmentId
    mode fabricpath
end

**serviceNetworkIpv4DynamicRoutingFWProfile**

config profile serviceNetworkIpv4DynamicRoutingLBProfile
  vlan $vlanId
    vn-segment $segmentId
    mode fabricpath
  interface vlan $vlanId
    vrf member $vrfName
      ip address $gatewayIpAddress/$netMaskLength tag 12345
      ip router ospf 5 area 0.0.0.0
      no shutdown
    router ospf 5
      vrf $vrfName
        router-id $gatewayIpAddress
      include profile vrf-common-LB
end

configure profile vrf-common-LB
  vrf context $vrfName
vni $include_vrfSegmentId
rd auto
   address-family ipv4 unicast
   route-target import %BORDER_LEAF_RT
   route-target both auto
   address-family ipv6 unicast
   route-target import %BORDER_LEAF_RT
   route-target both auto
router bgp $asn
vrf $vrfName
   address-family ipv4 unicast
       redistribute hmm route-map FABRIC-RMAP-REDIST-HOST
       redistribute direct route-map FABRIC-RMAP-REDIST-SUBNET
       maximum-paths ibgp 2
       redistribute ospf 5 route-map ospfMap
   address-family ipv6 unicast
       redistribute hmm route-map FABRIC-RMAP-REDIST-HOST
       redistribute direct route-map FABRIC-RMAP-REDIST-SUBNET
       maximum-paths ibgp 2
exit

serviceNetworkIpv4TfStaticRoutingFWProfile

config profile serviceNetworkIpv4TfStaticRoutingLBProfile
   vlan $vlanId
   vn-segment $segmentId
   mode fabricpath
   interface vlan $vlanId
       vrf member $vrfName
       ip address $gatewayIpAddress/$netMaskLength tag 12345
       fabric forwarding mode anycast-gateway
       no shutdown
   include profile vrf-common-Static
end

configure profile vrf-common-Static
   vrf context $vrfName
   vni $include_vrfSegmentId
   rd auto
   address-family ipv4 unicast
       route-target import %BORDER_LEAF_RT
       route-target both auto
   address-family ipv6 unicast
       route-target import %BORDER_LEAF_RT
       route-target both auto
router bgp $asn
vrf $vrfName
  address-family ipv4 unicast
    redistribute hmm route-map FABRIC-RMAP-REDIST-HOST
    redistribute direct route-map FABRIC-RMAP-REDIST-SUBNET
    maximum-paths ibgp 2
    redistribute static route-map staticMap
    address-family ipv6 unicast
    redistribute hmm route-map FABRIC-RMAP-REDIST-HOST
    redistribute direct route-map FABRIC-RMAP-REDIST-SUBNET
    maximum-paths ibgp 2
exit

serviceNetworkIpv4DynamicRoutingESProfile

config profile serviceNetworkIpv4DynamicRoutingESProfile
  vlan $vlanId
    vn-segment $segmentId
    mode fabricpath
  interface vlan $vlanId
    vrf member $vrfName
    ip address $gatewayIpAddress/$netMaskLength tag 12345
    ip router ospf 2 area 0.0.0.0
    no shutdown
  router ospf 2
    vrf $vrfName
      router-id $gatewayIpAddress
      redistribute direct route-map directMap
      redistribute bgp $asn route-map bgpMap
  include profile vrf-common-ES
end

configure profile vrf-common-ES
  vrf context $vrfName
    vni $include_vrfSegmentId
    rd auto
    ip route 0.0.0.0/0 $include_serviceNodeIpAddress
    address-family ipv4 unicast
      route-target import %BORDER_LEAF_RT
      route-target both auto
    address-family ipv6 unicast
      route-target import %BORDER_LEAF_RT
      route-target both auto
  router bgp $asn
  vrf $vrfName
address-family ipv4 unicast
  redistribute hmm route-map FABRIC-RMAP-REDIST-HOST
  redistribute direct route-map FABRIC-RMAP-REDIST-SUBNET
  maximum-paths ibgp 2
address-family ipv6 unicast
  redistribute hmm route-map FABRIC-RMAP-REDIST-HOST
  redistribute direct route-map FABRIC-RMAP-REDIST-SUBNET
  maximum-paths ibgp 2
exit

externalNetworkIpv4DynamicRoutingESProfile

cfg profile externalNetworkIpv4DynamicRoutingESProfile
  vlan $vlanId
    vn-segment $segmentId
    mode fabricpath
  interface vlan $vlanId
    vrf member $vrfName
    ip address $gatewayIpAddress/$netMaskLength tag 12345
    ip router ospf 4 area 0.0.0.0
    no shutdown
  router ospf 4
    vrf $vrfName
      router-id $gatewayIpAddress
      include profile vrf-common-External-Dynamic
end

configure profile vrf-common-External-Dynamic
  vrf context $vrfName
    vni $include_vrfSegmentId
    rd auto
    address-family ipv4 unicast
      route-target import %BORDER_LEAF_RT
      route-target both auto
    address-family ipv6 unicast
      route-target import %BORDER_LEAF_RT
      route-target both auto
  router bgp $asn
    vrf $vrfName
    address-family ipv4 unicast
      redistribute hmm route-map FABRIC-RMAP-REDIST-HOST
      redistribute direct route-map FABRIC-RMAP-REDIST-SUBNET
      maximum-paths ibgp 2
      redistribute ospf 4 route-map ospfMap
    address-family ipv6 unicast
redistribute hmm route-map FABRIC-RMAP-REDIST-HOST
redistribute direct route-map FABRIC-RMAP-REDIST-SUBNET
maximum-paths ibgp 2
exit

**serviceNetworkIpv4TfStaticRoutingESProfile**

```bash
cfg profile serviceNetworkIpv4TfStaticRoutingESProfile
  vlan $vlanId
  vn-segment $segmentId
  mode fabricpath
  interface vlan $vlanId
  vrf member $vrfName
  ip address $gatewayIpAddress/$netMaskLength tag 12345
  fabric forwarding mode anycast-gateway
  no shutdown
  include profile vrf-common-ES
end
```

```bash
configure profile vrf-common-ES
  vrf context $vrfName
  vni $include_vrfSegmentId
  rd auto
  ip route 0.0.0.0/0 $include_serviceNodeIpAddress
  address-family ipv4 unicast
    route-target import %BORDER_LEAF_RT
    route-target both auto
  address-family ipv6 unicast
    route-target import %BORDER_LEAF_RT
    route-target both auto
  router bgp $asn
  vrf $vrfName
    address-family ipv4 unicast
      redistribute hmm route-map FABRIC-RMAP-REDIST-HOST
      redistribute direct route-map FABRIC-RMAP-REDIST-SUBNET
      maximum-paths ibgp 2
    address-family ipv6 unicast
      redistribute hmm route-map FABRIC-RMAP-REDIST-HOST
      redistribute direct route-map FABRIC-RMAP-REDIST-SUBNET
      maximum-paths ibgp 2
exit
```
**externalNetworkIpv4TfStaticRoutingESProfile**

```text
config profile externalNetworkIpv4TfStaticRoutingESProfile
  vlan $vlanId
  vn-segment $segmentId
  mode fabricpath
  interface vlan $vlanId
  vrf member $vrfName
  ip address $gatewayIpAddress/$netMaskLength tag 12345
  fabric forwarding mode anycast-gateway
  no shutdown
  include profile vrf-common-Static
End
```

```text
configure profile vrf-common-Static
  vrf context $vrfName
  vni $include_vrfSegmentId
  rd auto
  address-family ipv4 unicast
    route-target import %BORDER_LEAF_RT
    route-target both auto
  address-family ipv6 unicast
    route-target import %BORDER_LEAF_RT
    route-target both auto
  router bgp $asn
    vrf $vrfName
    address-family ipv4 unicast
      redistribute hmm route-map FABRIC-RMAP-REDIST-HOST
      redistribute direct route-map FABRIC-RMAP-REDIST-SUBNET
      maximum-paths ibgp 2
    redistribute static route-map staticMap
    address-family ipv6 unicast
      redistribute hmm route-map FABRIC-RMAP-REDIST-HOST
      redistribute direct route-map FABRIC-RMAP-REDIST-SUBNET
      maximum-paths ibgp 2
  exit
```

**defaultNetworkIpv4EfESProfile**

```text
config profile defaultNetworkIpv4EfESProfile
  vlan $vlanId
  vn-segment $segmentId
  mode fabricpath
  interface vlan $vlanId
  vrf member $vrfName
```
configuration for border leaf (leaf-1):

```
ip address $gatewayIpAddress/$netMaskLength tag 12345
fabric forwarding mode proxy-gateway
no ip redirect
no shutdown
include profile vrf-common-ES
end

configure profile vrf-common-ES
vrf context $vrfName
  vni $include_vrfSegmentId
  rd auto
  ip route 0.0.0.0/0 $include_serviceNodeIpAddress
  address-family ipv4 unicast
    route-target import %BORDER_LEAF_RT
  route-target both auto
  address-family ipv6 unicast
    route-target import %BORDER_LEAF_RT
  route-target both auto
router bgp $asn
  vrf $vrfName
    address-family ipv4 unicast
      redistribute hmm route-map FABRIC-RMAP-REDIST-HOST
      redistribute direct route-map FABRIC-RMAP-REDIST-SUBNET
      maximum-paths ibgp 2
  address-family ipv6 unicast
    redistribute hmm route-map FABRIC-RMAP-REDIST-HOST
    redistribute direct route-map FABRIC-RMAP-REDIST-SUBNET
    maximum-paths ibgp 2
exit
```

defaultNetworkIpv4TfESProfile

```
config profile defaultNetworkIpv4TfESProfile
  vlan $vlanId
  vn-segment $segmentId
  mode fabricpath
interface vlan $vlanId
  vrf member $vrfName
  ip address $gatewayIpAddress/$netMaskLength tag 12345
  fabric forwarding mode anycast-gateway
  no shutdown
  include profile vrf-common-ES
end

configure profile vrf-common-ES
```
vrf context $vrfName
  vni $include_vrfSegmentId
  rd auto
  ip route 0.0.0.0/0 $include_serviceNodeIpAddress
    address-family ipv4 unicast
      route-target import %BORDER_LEAF_RT
      route-target both auto
  address-family ipv6 unicast
    route-target import %BORDER_LEAF_RT
    route-target both auto
router bgp $asn
  vrf $vrfName
    address-family ipv4 unicast
      redistribute hmm route-map FABRIC-RMAP-REDIST-HOST
      redistribute direct route-map FABRIC-RMAP-REDIST-SUBNET
      maximum-paths ibgp 2
    address-family ipv6 unicast
      redistribute hmm route-map FABRIC-RMAP-REDIST-HOST
      redistribute direct route-map FABRIC-RMAP-REDIST-SUBNET
      maximum-paths ibgp 2
exit