Contents

Introduction ..................................................................................................................................... 3
Target Audience ............................................................................................................................ 4
Prerequisites .................................................................................................................................. 4
Overview: Layer 2 Domains, Protected Subnets, and East-West Firewalls ..................................... 4
Overview: VRF Instances and Tenant-Edge Firewalls .................................................................... 8
East-West Firewall Deployment Scenarios ...................................................................................... 9
Basic Leaf Configuration for Protected Networks ......................................................................... 9
  Configuration 1a: IPVLAN-Based Leaf Switch Connecting to Hosts ................................................ 9
  Configuration 1b: IPBD-Based Leaf Switch Connecting to Hosts ..................................................... 10
Basic Leaf Configuration for Attaching the East-West Firewall ..................................................... 11
  Configuration 2a: IPVLAN-Based Leaf Switch Connecting to Firewall ........................................... 11
  Configuration 2b: IPBD-Based Leaf Switch Connecting to Firewall ............................................... 13
Routing Peering Configuration between the Standalone East-West Firewall and the Fabric ............. 15
  Static Routing Peering between the Fabric and the Standalone Firewall ...................................... 15
  Configuration 3a: IPVLAN-Based Leaf Switch Connecting to Firewall ......................................... 15
  Configuration 3b: IPBD-Based Leaf Switch Connecting to Firewall ............................................. 16
  Dynamic Routing Peering between the Fabric and the Standalone Firewall ................................ 17
  Configuration 4a: IPVLAN-Based Leaf Switch ............................................................................ 17
  Configuration 4b: IPBD-Based Leaf Switch .................................................................................. 17
  vPC Dual-Homed Active-Standby Firewall Connectivity in Routed Mode .................................. 18
  Single-Attached Active-Standby Firewall Connectivity in Routed Mode ........................................ 18
  Configuration 5a: IPVLAN-Based Leaf Switch ............................................................................ 19
  Configuration 5b: IPBD-Based Leaf Switch .................................................................................. 20
Clustered East-West Firewalls in Routed Mode ................................................................................ 20
  Configuration 6a: IPVLAN-Based Leaf Switch ............................................................................ 21
  Configuration 6b: IPBD-Based Leaf Switch .................................................................................. 23
Active-Standby Failover East-West Firewalls in Transparent Mode with vPC Connectivity ............ 25
  Configuration 7a: IPVLAN-Based Leaf Switch ............................................................................ 26
  Configuration 7b: IPBD-Based Leaf Switch .................................................................................. 28
Active-Standby Failover East-West Firewalls in Transparent Mode ................................................ 30
Clustered East-West Firewalls in Transparent Mode ....................................................................... 31
Tenant-Edge Firewall Deployment Scenarios .................................................................................. 31
  Active-Standby Failover: Single-Attached Tenant-Edge Firewalls in Routed Mode with Static Routing 34
    Configuration 8a: IPVLAN-Based Leaf Switch ............................................................................ 35
    Configuration 8b: IPBD-Based Leaf Switch ............................................................................... 38
  Active-Standby Failover: Single-Attached Tenant-Edge Firewalls in Routed Mode with Dynamic Routing 41
    Configuration 9a: IPVLAN-Based Leaf Switch ............................................................................ 42
    Configuration 9b: IPBD-Based Leaf Switch ............................................................................... 45
  Clustered Mode: vPC Dual-Attached Tenant-Edge Firewalls in Routed Mode with Static Routing .... 49
  Clustered Mode: Single-Attached Tenant-Edge Firewalls in Routed Mode with Dynamic Routing .... 49
    Configuration 10a: IPVLAN-Based Leaf Switch ............................................................................ 50
    Configuration 10b: IPBD-Based Leaf Switch ............................................................................... 53
Complex Deployment Scenarios ...................................................................................................... 56
  Active-Standby Failover: Single-Attached Tenant-Edge Firewalls in Routed Mode with Dynamic Routing and East-West Firewall Elements ................................................................. 57
    Configuration 11a: IPVLAN-Based Leaf Switch ............................................................................ 58
    Configuration 11b: IPBD-Based Leaf Switch ............................................................................... 59
  Clustered Mode: vPC Dual-Attached Tenant-Edge Firewalls in Routed Mode with Static Routing and East-West Firewall Elements ......................................................................................... 66
    Configuration 12a: IPVLAN-Based Leaf Switch ............................................................................ 67
    Configuration 12b: IPBD-Based Leaf Switch ............................................................................... 71
For More Information ..................................................................................................................... 74
Introduction

The primary goal of this document is to help readers gain basic- and advanced-level knowledge about how to implement some typical firewall deployments in the data center using the Cisco® programmable fabric.

This document presents examples and configuration details for network integration of firewalls in various deployment scenarios:

- East-west firewall in routed mode: active-standby deployment model (vPC and non-vPC)
- East-west firewall in routed mode: clustered firewalls deployment model (vPC only)
- East-west firewall in transparent mode: active-standby deployment model (vPC and non-vPC)
- East-west firewall in transparent mode: clustered firewalls deployment model (vPC only)
- Tenant-edge firewall in routed mode: active-standby deployment model (vPC and non-vPC)
- Tenant-edge firewall in routed mode: clustered firewalls deployment model (vPC and non-vPC)

The following scenarios are not covered in this document:

- Tenant-edge firewall in transparent mode: active-standby deployment model (vPC and non-vPC)
- Tenant-edge firewall in transparent mode: clustered firewalls deployment model (vPC only)

A Cisco Adaptive Security Appliance (ASA) firewall was used in the preparation of the document, but any firewall with a feature set similar to that of the ASA 5585-X (ASA Release 9.4) can be deployed.

This document does not provide firewall configurations.

When applicable, examples for both static routing and dynamic routing peering are shown.

This document assumes that heartbeat or cluster control links (CCLs) are connected outside the fabric using dedicated firewall interfaces. If in-band configuration is required, an additional Layer 2 segment must be provisioned (this configuration is outside the scope of this document).

This document discusses two of the most popular high-availability scenarios:

- Active-standby failover
- Clustered firewalls

The active-active failover scenario is not covered.

Note: Because of limitations of software and hardware support at the time of this writing, not all combinations of firewall types and deployment models are covered in this document.

This document describes two types of configurations for Cisco Nexus switches:

- IP bridge domain (IPBD)–based configuration
- IP VLAN (IPVLAN)–based configuration

In an IPBD-based configuration, the VLAN tag is mapped to the IPBD, which is mapped to the VxLAN network identifier (VNI). The encapsulation mapping is performed in a virtual switch instance (VSI) profile.
In an IPVLAN-based configuration, the downstream interfaces are used to map the receiving VLAN tag to the VNI. Please consult the configuration guides for the respective Cisco Nexus switches used to identify which configuration types are necessary in a specific case.

All vPC dual-homing scenarios are shown using regular server leaf nodes (dedicated services leaf nodes can also be used).

**Target Audience**
This document is written for network architects, designers, and planning and implementation teams and application services and maintenance teams.

**Prerequisites**
Readers should familiarize themselves with the document [Cisco Dynamic Fabric Automation](#) before proceeding to read the current document. The fabric automation document covers many of the fundamental notions and terms used in the current document.

Other configuration guides with useful additional information include [Cisco Nexus 7000 Series NX-OS VXLAN Configuration Guide](#) and [Cisco Nexus 9000 Series NX-OS VXLAN Configuration Guide, Release 7.0](#).

**Overview: Layer 2 Domains, Protected Subnets, and East-West Firewalls**

In Virtual Extensible LAN (VXLAN) Ethernet virtual private network (EVPN) fabric, the Layer 2 segment has at least two numerical values identifying it. This document uses both values in the figures:

- Fabric-significant Layer 2 VXLAN VNI
- Leaf-node-significant (or switch-port-significant) IEEE 802.1Q VLAN identifier

Traditionally, a given subnet is considered to be a distinct Layer 2 domain in which all workloads within a subnet receive all broadcast and unknown unicast frames that originate in the domain. The only route for the traffic to leave this domain traverses its default gateway (Figure 1).

**Figure 1.** Logical Diagram Showing Hosts in VLAN 101 and a Default Gateway for VLAN 101
When data needs to be forwarded between subnets within a given Virtual Routing and Forwarding (VRF) instance across the fabric, a transit Layer 3 VNI is used. Figure 2 shows a sample VXLAN EVPN network with two subnets (subnets B1 and B2), their respective SVIs and BDIs, and the Layer 3 VNI (50001) associated with their VRF instances.

**Figure 2.** Logical Diagram Showing Hosts in Nonprotected VLANs 111 and 112, their Respective Default Gateway SVIs and BDIs on Two Different Leaf Switches in the Fabric, and Their VRF Instances with the Layer 3 (Transit) VNI

When a given subnet needs to be protected by the firewall, its respective default gateway is no longer placed within the fabric, but instead is configured on the firewall. For such a protected subnet, VXLAN EVPN fabric acts only as a tunnel transport. Because multiple such subnets can terminate on the firewall, this type of firewall often is referred to as an east-west firewall. In this scenario, workloads within the protected subnet use the east-west firewall as the default gateway (Figure 3). The firewall enforces security policies for data passing between subnets and maintains adjacency tables for all workloads from protected subnets (Address Resolution Protocol [ARP] for IPv4 and Neighbor Discovery Protocol [NDP] for IPv6).

**Figure 3.** Logical Diagram Showing Hosts in VLANs 101 and 102 and a Firewall Terminating these VLANs as a Default Gateway for the Respective Subnets

Such a scenario also requires the east-west firewall to have an additional Layer 3 link, which is used to reach any other networks and connects back to the routed domain (Figure 4).
Cisco programmable fabric with VXLAN encapsulation and a BGP EVPN control plane provides multitenancy mechanisms and enhances traditional Layer 2 domain behavior by providing ARP suppression. This feature reduces the amount of flooded traffic in a given Layer 2 domain and lowers the load on the control plane of the firewall and on the CPU.

The following steps present a sample topology with the east-west firewall in routed mode. Figure 5 shows the packet movement for traffic from host 1 to host 5.

1. Traffic from host 1 enters the fabric in VLAN 101, where it is mapped to VNI 30101. The VXLAN Layer 2 tunnel with VNI 30101 traverses the fabric until it reaches the leaf node connecting to east-west firewall. The header of the frame is stripped and mapped back to VLAN 101. The firewall receives the traffic on the Layer 3 subinterface for VLAN 101.
2. Within the east-west firewall, the traffic is subjected to security firewall policies, and the routing process identifies that the destination subnet B1 is reachable through the Layer 3 subinterface for VLAN 200.
3. Data traffic is tagged with VLAN 200 and sent to the VXLAN EVPN fabric, where the VLAN 200 ID is mapped to VNI 30200.
4. The SVI and BDI logical interface for VLAN 200 and VNI 30200 receives the traffic and determines that the traffic needs to be routed to the destination network on a remote leaf node through the VXLAN EVPN fabric. All routing through the fabric within a given VRF instance is performed using the transit VNI, identified as the Layer 3 VRF VNI1: in this case, 50001.
5. The destination leaf node receives the traffic with VNI 50001 in the header and determines that the data traffic needs to be routed out of the locally configured SVI and BDI for VLAN 111 and VNI 30111.
6. The data traffic is then sent to host 5 with the VLAN 111 tag in the header.

---

In cases in which the firewall needs to be deployed in transparent mode, it no longer hosts the default gateway for the protected subnet, but acts as a transparent bridge, mapping the ingress VLAN to the respective egress VLAN. The VXLAN EVPN fabric itself hosts the SVI and BDI for the protected subnet (Figure 6).

Note that the VLAN ID and VNI (301 and 302) used for such termination is different from the VLAN ID and VNI (101 and 102) to which the actual hosts are attached.

**Figure 6.** Logical Diagram Showing Hosts in Protected (Subnets A1 and A2) and Nonprotected (Subnets B1 and B2) Subnets, and VXLAN Fabric and the East-West Firewall in Transparent Mode. Default Gateways for Protected Subnets A1 and A2 Reside in the Fabric, and the Firewall Acts as a Transparent Bridge
Overview: VRF Instances and Tenant-Edge Firewalls

In multitenant environments, you can deploy a tenant-edge firewall to apply filtering policies to data traffic moving between the VRF instances, or tenants. In such a scenario, each firewall interface resides in a particular VRF instance, or tenant. Figure 7 shows the deployment in mode.

A tenant-edge firewall can also be deployed in transparent mode in the programmable VXLAN EVPN fabric, as shown in Figure 8. However, this approach requires one firewall or one firewall context per protected VRF instance, which creates a large amount of overhead in multitenant environments and is a less popular deployment method. This document focuses only on tenant-edge firewall deployment in routed mode.

Figure 7. Logical Diagram Showing Hosts in Subnets that are Part of VRF A and VRF B, VXLAN Fabric, and the Tenant-Edge Firewall in Routed Mode. The Firewall Peers with the Fabric in VRF A and VRF B through IEEE 802.1Q Layer 3 Subinterfaces

Figure 8. Logical Diagram Showing Hosts in Subnets That Are Part of VRF A and VRF B, VXLAN Fabric, and the Tenant-Edge Firewall in Transparent Mode. The Interface in VRF A Peers with the Interface in VRF B through the Transparent Firewall, Which Acts as a Layer 2 Bridge between Two VRF Instances
East-West Firewall Deployment Scenarios

This section presents configurations for east-west firewall deployment scenarios.

**Basic Leaf Configuration for Protected Networks**

The protected network configuration is identical for any east-west firewall deployment. This set of commands is configured on the leaf node to which the workloads in a protected subnet are attached.

The Layer 2 network is configured as shown here, according to whether the Cisco Nexus switch is IPBD based or IPVLAN based. The configurations are used for the protected subnet VLAN 101 as shown in Figure 9.

**Figure 9.** Logical Diagram Showing Hosts in Subnets, VXLAN Fabric, and the East-West Firewall in Routed Mode. The Firewall Acts as a Default Gateway for Protected Subnets 10.10.101.0/24 and 10.10.102.0/24. Default Gateways for Nonprotected Subnets 10.10.111.0/24 and 10.10.112.0/24 Reside in the Fabric on Leaf Nodes

**Configuration 1a: IPVLAN-Based Leaf Switch Connecting to Hosts**

```plaintext
feature vn-segment-vlan-based
feature nv overlay

vlan 101
    vn-segment 30101  # mapping the vlan 101 to Layer-2 VNI 30101

interface Ethernet1/10
    switchport mode trunk
    switchport trunk allowed vlan add 101

router bgp 65000
    address-family l2vpn evpn  # enabling bgp evpn control plane for host reachability
    evpn
        vni 30101 12  # enabling bgp evpn control plane for host reachability for L2 VNI 30101
        rd auto
```

© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.
route-target import auto
route-target export auto

interface nve1  ## configuring VTEP (VXLAN tunnel endpoint) with parameters for L2 VNI 30101
    host-reachability protocol bgp
    member vni 30101
    suppress-arp
    mcast-group 239.1.1.101

Configuration 1b: IPBD-Based Leaf Switch Connecting to Hosts

install feature-set fabric
cdc leaf1 id 1
    allow feature-set fabric
feature-set fabric
feature nv overlay
feature vni
nv overlay evpn

vni 30101  ## creating VNI 30101 in the system
system bridge-domain 1500-2000  ## allocate bridge-domains

encapsulation profile vni VSI_101_to_30101 ## mapping vlan 101 to L2 VNI 30101
dot1q 101 vni 30101

bridge-domain 1500  ## mapping bridge-domain 1500 to L2 VNI 30101
    member vni 30101

interface Ethernet3/10
    service instance 1 vni
        encapsulation profile VSI_101_to_30101 ## config for port-significant VLAN to VNI mapping

interface nve1  ## VTEP configuration
    host-reachability protocol bgp
    member vni 30101
        suppress-arp
        mcast-group 239.1.1.101

router bgp 65000
    address-family l2vpn evpn
evpn
    vni 30101 12  ## configuring VNI 30101 to be L2 VNI
        rd auto
        route-target import auto
        route-target export auto
In cases in which workloads are vPC dual-attached, the relevant configuration needs to be added to the port channel.

**Basic Leaf Configuration for Attaching the East-West Firewall**

The following configurations are used on the leaf node attaching to the east-west firewall as shown in Figure 4. The east-west firewall uses at least two logical interfaces to attach to the fabric and prompts the respective configuration on the fabric leaf node:

- The Layer 3 subinterface of the firewall, in the case here, for VLANs 101 and 102, has to attach to the protected subnet. The leaf node should use the exact configuration used to attach workloads.
- The Layer 3 subinterface of the firewall, in the case here, for VLAN 200, has to attach to the network that is used to communicate with unprotected subnets in the rest of the fabric.

**Configuration 2a: IPVLAN-Based Leaf Switch Connecting to Firewall**

```
feature vn-segment-vlan-based
feature nv overlay

route-map FABRIC-RMAP-REDIST-SUBNET permit 10
    match tag 12345

vlan 200
    vn-segment 30200  ## mapping the vlan 200 to Layer-2 VNI 30200
vlan 101
    vn-segment 30101  ## mapping the vlan 101 to Layer-2 VNI 30101
vlan 2000
    vn-segment 50001  ## mapping the vlan 2000 to Layer-3 VRF VNI 50001

vrf context VRF-A
    vni 50001
    rd auto
    address-family ipv4 unicast
        route-target both auto
        route-target both auto evpn

interface Vlan200
    ## interface, used for Layer-3 peering with fabric.
    no shutdown
    vrf member VRF-A
    ip address 10.10.200.1/24  tag 12345  ## "tag 12345" is used by route-map to redistribute subnets into BGP

interface Vlan2000
    ## interface, used as an L3 VRF VNI interface
    no shutdown
    vrf member VRF-A
    no ip redirects
    ip forward
```

Please refer to Configuration 3a and Configuration 4a for more details.
ipv6 forward
no ipv6 redirects

interface Ethernet1/25  ## interface, used to attach to fabric and trunk protected subnet
    switchport mode trunk
    switchport trunk allowed vlan add 101

interface Ethernet1/26  ## interface, used to attach to peer with the Layer-3 “outside”
    switchport mode trunk
    switchport trunk allowed vlan add 200

interface nve1
    host-reachability protocol bgp
    member vni 30101  ## configuring VTEP (VXLAN tunnel endpoint) with parameters for L2 VNI 30101
        suppress-arp
        mcast-group 239.1.1.101
    member vni 30200  ## configuring VTEP with parameters for L2 VNI 30200
        suppress-arp
        mcast-group 239.1.1.200
    member vni 50001 associate-vrf  ## configuring VTEP with parameters for L3 VRF VNI 50001

router bgp 65000
    address-family l2vpn evpn  ## enabling bgp evpn control plane for host reachability
    vrf VRF-A
        address-family ipv4 unicast
        advertise l2vpn evpn
        redistribute direct route-map FABRIC-RMAP-REDIST-SUBNET
        maximum-paths ibgp 2

    evpn
    vni 30200 12  ## enabling bgp evpn control plane for host reachability for L2 VNI 30200
        rd auto
        route-target import auto
        route-target export auto
    vni 30101 12  ## enabling bgp evpn control plane for host reachability for L2 VNI 30101
        rd auto
        route-target import auto
        route-target export auto
Configuration 2b: IPBD-Based Leaf Switch Connecting to Firewall

```plaintext
install feature-set fabric
vdc leaf1 id 1
   allow feature-set fabric
feature-set fabric
feature nv overlay
feature vni	nv overlay evpn

vni 30101  ## creating VNI 30101 in the system
vni 30200  ## creating VNI 30200 in the system
vni 50001  ## creating VNI 50001 in the system

route-map FABRIC-RMAP-REDIST-SUBNET permit 10
   match tag 12345

system bridge-domain 1500-2500  ## bridge domains, which will tie VNI and VLANs together

encapsulation profile vni VSI_101_to_30101  ## mapping VLAN 101 to L2 VNI 30101
   dot1q 101 vni 30101
encapsulation profile vni VSI_200_to_30200  ## mapping VLAN 200 to L2 VNI 30200
   dot1q 200 vni 30200

bridge-domain 1500-1501  ## mapping bridge-domain 1500 to L2 VNI 30101, and 1500 to 30200
   member vni 30101, 30200

vrf context VRF-A
   vni 50001
   rd auto
   address-family ipv4 unicast
      route-target both auto
      route-target both evpn

interface Bdi15013
   vrf member VRF-A
   ip address 10.10.200.1/24 tag 12345
   no shutdown

interface nve1  ## VTEP configuration
   host-reachability protocol bgp
   member vni 30101  ## configuring VTEP (VXLAN tunnel endpoint) with parameters for L2 VNI 30101
      suppress-arp
      mcast-group 239.1.1.101
   member vni 30200  ## configuring VTEP with parameters for L2 VNI 30200

3 Please refer to Configuration 3b and Configuration 4b for more details.
```
suppress-arp
mcast-group 239.1.1.200
member vni 50001 associate-vrf

## configuring VTEP with parameters for L3 VRF VNI 50001

interface Ethernet3/10
  service instance 1 vni
    encapsulation profile VSI_101_to_30101

## config for port-significant VLAN to VNI mapping

interface Ethernet3/11
  service instance 1 vni
    encapsulation profile VSI_200_to_30200

## config for port-significant VLAN to VNI mapping

router bgp 65000
  address-family l2vpn evpn
  vrf VRF-A
    address-family ipv4 unicast
      advertise l2vpn evpn
      redistribute direct route-map FABRIC-RMAP-REDIST-SUBNET
      maximum-paths ibgp 2
  evpn
    vni 30200 12
      ## enabling bgp evpn control plane for host reachability for L2 VNI 30200
      rd auto
      route-target import auto
      route-target export auto
    vni 30101 12
      ## enabling bgp evpn control plane for host reachability for L2 VNI 30101
      rd auto
      route-target import auto
      route-target export auto
Routing Peering Configuration between the Standalone East-West Firewall and the Fabric

The firewall also can either run a dynamic routing protocol with the fabric or be configured with a set of static routes to facilitate network reachability. **Figure 10** shows the basic routing directions, which need to be present regardless of choice of static or dynamic routing.

**Figure 10.** Route 1 is Aimed at Protected Subnets and is Directed from the Fabric to the Outside Layer 3 Interface of the Firewall. Route 2 is a Default Route and is Directed from the Firewall to the Fabric. Route 3 is also a Default Route for the Entire Fabric and is Directed from the Border Leaf of the Fabric to the WAN or Edge Router

Static Routing Peering between the Fabric and the Standalone Firewall

The following configuration shows incremental changes to Configuration 2a and Configuration 2b, respectively, that are needed if you deploy static routing. Mainly these changes add static routes to protected subnets and redistribute them to the fabric Border Gateway Protocol (BGP), and they enable anycast-gateway forwarding mode for the SVI and BDI, which is used for peering with the firewall. This configuration is necessary to help ensure that the active-standby firewall high-availability models can use the same IP address as the next hop on both the active and standby firewall systems. These configurations need to be performed on the leaf switches to which the firewalls attach.

**Configuration 3a: IPVLAN-Based Leaf Switch Connecting to Firewall**

```
vrf context VRF-A
  ip route 0.0.0.0/0 10.77.1.1  # Default route to WAN/Edge router
  ip route 10.10.101.0/24 10.10.200.2  # static route to the firewall to reach subnet vlan 101
  ip route 10.10.102.0/24 10.10.200.2  # static route to the firewall to reach subnet vlan 102

  ip access-list PROTECTED_SUBNETS_LIST
  10 permit ip 10.10.101.0/24 any
```
Configuration 3b: IPBD-Based Leaf Switch Connecting to Firewall

```
vrf context VRF-A
  ip route 0.0.0.0/0 10.77.1.1  ## Default route to WAN/Edge router
  ip route 10.10.101.0/24 10.10.200.2  ## static route to the firewall to reach subnet vlan 101
  ip route 10.10.102.0/24 10.10.200.2  ## static route to the firewall to reach subnet vlan 102

  ip access-list PROTECTED_SUBNETS_LIST
  10 permit ip 10.10.101.0/24 any
  20 permit ip 10.10.102.0/24 any

  route-map REDIST_PROTECTED_SUBNETS permit 10
  match ip address PROTECTED_SUBNETS_LIST

interface Bdi1501  ## interface, used for Layer-3 peering with fabric.
  vrf member VRF-A
  ip address 10.10.200.1/24 tag 12345
  fabric forwarding mode anycast-gateway

interface Ethernet3/20.77  ## Layer-3 sub-interface, for peering with WAN/Edge router
  encapsulation dot1q 77
  vrf member VRF-A
  ip address 10.77.1.2/24

router bgp 65000
  vrf VRF-A
    address-family ipv4 unicast
      redistribute static route-map REDIST_PROTECTED_SUBNETS
```
Dynamic Routing Peering between the Fabric and the Standalone Firewall

When you run the dynamic routing protocol, the anycast-gateway fabric forwarding mode can not be used on the SVI and BDI for VLAN 200. The fabric will receive the routing reachability information for protected networks from the firewall through Open Shortest Path First (OSPF). Instead of redistributing static routes, you need to configure the new route map that redistributes dynamically learned routes. Incremental configurations needed to establish dynamic routing between the fabric and the firewall are shown here. Configuration 2a and Configuration 2b show the baseline configurations.

Configuration 4a: IPVLAN-Based Leaf Switch

```plaintext
router ospf FW-TO-FABRIC-OSPF  ## define OSPF routing process
vrf ORG1:PART1  ## specify a particular VRF, for which the routing peering is needed
    router-id 12.12.12.12

route-map ospfMap permit 10

interface Vlan200  ## interface, used for Layer-3 peering with fabric.
    vrf member VRF-A
    ip address 10.10.200.1/24  tag 12345
    ip router ospf FW-TO-FABRIC-OSPF area 0

router bgp 65000
    vrf VRF-A
        address-family ipv4 unicast
            redistribute ospf route-map ospfMap
```

Configuration 4b: IPBD-Based Leaf Switch

```plaintext
router ospf FW-TO-FABRIC-OSPF  ## define OSPF routing process
vrf ORG1:PART1  ## specify a particular VRF, for which the routing peering is needed
    router-id 12.12.12.12

route-map ospfMap permit 10

interface Bdi1501  ## interface, used for Layer-3 peering with fabric.
    vrf member VRF-A
    ip address 10.10.200.1/24  tag 12345
    ip router ospf FW-TO-FABRIC-OSPF area 0

router bgp 65000
    vrf VRF-A
        address-family ipv4 unicast
            redistribute ospf route-map ospfMap
```
Active-Standby Failover East-West Firewalls in Routed Mode

A pair of active-standby failover east-west firewalls can either individually connect to separate leaf nodes, as shown in Figure 11, or have their links dual-homed to a vPC pair of leaf switches, as shown in Figure 12. In general, border leaf nodes are not configured as vPC peers in programmable fabric, which limits the connectivity options to only the single-homed scenario. If dual-homed vPC is needed, the firewalls can be connected to regular or dedicated services leaf nodes.

Figure 11. Physical Connectivity Diagram Showing Active and Standby Firewall Units Single-Attached to Two Leaf Nodes, and Hosts in Protected Subnets

Figure 12. Physical Connectivity Diagram Showing Active and Standby Firewall Units, Each Dual-Homed to Leaf Nodes Using vPC

vPC Dual-Homed Active-Standby Firewall Connectivity in Routed Mode

With the current Cisco NX-OS Software, vPC dual-homed firewalls can be configured only with static routing. The configuration will be very similar to Configurations 2a, 2b, 3a, and 3b. The only difference is that the trunk ports to firewalls are now not individual interfaces, but vPCs connecting to both the active and standby units, as shown in Figure 12 with active 2 and standby 2 firewall units.
Single-Attached Active-Standby Firewall Connectivity in Routed Mode

Even though the standby firewall unit is dormant in normal operation mode, when you attach both active and standby firewall units to two individual leaf nodes, you must maintain route reachability to protected subnets on both leaf nodes. In other words, both leaf nodes will attract traffic directed to protected networks. When the leaf node with the standby firewall attached to it receives such data traffic, it will forward it to the active firewall unit through the fabric (Figure 13). Such suboptimal forwarding can be improved by using the clustered firewall deployment mode.

**Figure 13.** Border Leaf 2 Attracts Traffic for Protected Subnets, which Results in Suboptimal Routing in the Fabric

For the static routing scenario, configuration of both leaf nodes exactly matches Configurations 2a, 2b, 3a, and 3b.

For the dynamic routing scenario, configuration of both leaf nodes will be very similar to Configurations 2a, 2b, 3a, and 3b. The only difference is in the IP addresses of the SVI and BDI used for Layer 3 peering with the firewall. With dynamic routing, the anycast-gateway mode can’t be used, and different IP addresses must be used on respective leaf nodes. Configurations 5a and 5b show the configuration details.

**Configuration 5a: IPVLAN-Based Leaf Switch**

```
Border Leaf-1 configuration
interface Vlan200  ## interface, used for Layer-3 peering with fabric.
ip address 10.10.200.253/24
ip router ospf FW-TO-FABRIC-OSPF area 0

Border Leaf-2 configuration
interface Vlan200  ## interface, used for Layer-3 peering with fabric.
ip address 10.10.200.254/24
ip router ospf FW-TO-FABRIC-OSPF area 0
##It is assumed that the firewall's Layer-3 interface is in the same subnet as SVI above
```
Configuration 5b: IPBD-Based Leaf Switch

<table>
<thead>
<tr>
<th>Configuration</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Border Leaf-1 configuration</td>
<td>interface Bdi1501 ## interface, used for Layer-3 peering with fabric. ip address 10.10.200.253/24 ip router ospf FW-TO-FABRIC-OSPF area 0</td>
</tr>
<tr>
<td>Border Leaf-2 configuration</td>
<td>interface Bdi1501 ## interface, used for Layer-3 peering with fabric. ip address 10.10.200.254/24 ip router ospf FW-TO-FABRIC-OSPF area 0</td>
</tr>
</tbody>
</table>

Clustered East-West Firewalls in Routed Mode
ASA firewalls support clustered high-availability deployment models using a spanned Cisco EtherChannel. In combination with the vPC feature in the Cisco programmable fabric, they support multinode firewall clustering for greater scalability and throughput. This section describes some of the deployment considerations associated with deployment of an active-active cluster of ASA firewalls in programmable fabric (Figure 14).

Figure 14. Clustered Firewalls in Routed Mode with Spanned EtherChannel and vPC Connectivity to Leaf Nodes

As of this writing, Layer 3 over vPC is not supported in the current software, so the only available deployment scenario for vPC dual-homed routed mode firewalls uses static routing.

A cluster of east-west firewalls in routed mode completely mirrors running configurations between the firewall cluster members and synchronize all states to facilitate traffic policy enforcement. Their virtual IP and MAC addresses are also replicated in a way that makes the entire cluster look like a single device with multiple links in a port channel. With the vPC feature on the fabric leaf nodes, all links to firewall cluster members can be bundled in a single vPC. Multiple subinterfaces on both the leaf nodes as well as the firewall cluster members can be assigned to reflect, respectively, inside and outside logical interfaces.

The configuration on the leaf nodes will closely resemble Configurations 1a, 1b, 2a, 2b, 3a, and 3b.
Configuration 6a: IPVLAN-Based Leaf Switch

Border Leaf 1 and Border Leaf 2 Configuration

feature vn-segment-vlan-based
feature nv overlay

route-map FABRIC-RMAP-REDIST-SUBNET permit 10
   match tag 12345

vlan 200
   vn-segment 30200  ##mapping the vlan 200 to Layer-2 VNI 30200
vlan 101
   vn-segment 30101  ##mapping the vlan 101 to Layer-2 VNI 30101
vlan 102
   vn-segment 30102  ##mapping the vlan 102 to Layer-2 VNI 30102
vlan 2000
   vn-segment 50001  ##mapping the vlan 2000 to Layer-3 VRF VNI 50001

vrf context VRF-A
   vni 50001
   rd auto
   address-family ipv4 unicast
      route-target both auto
      route-target both auto evpn

interface Vlan200  ## interface, used for Layer-3 peering with fabric.
   no shutdown
   vrf member VRF-A
   ip address 10.10.200.1/24  tag 12345  ## "tag 12345" is used by route-map to redistribute
      subnets into BGP
   fabric forwarding mode anycast-gateway

interface Vlan2000  ## interface, used as an L3 VRF VNI interface
   no shutdown
   vrf member VRF-A
   no ip redirects
   ip forward
   ipv6 forward
   no ipv6 redirects

interface Ethernet1/25  ## interface, used to attach to fabric and trunk protected subnet
   channel-group 10 mode active

interface Ethernet1/26  ## interface, used to attach to peer with the Layer-3 "outside"
   interface
      channel-group 10 mode active
interface port-channel 10 ## configuring vPC port-channel to Firewall cluster
  switchport mode trunk
  switchport trunk allowed vlan add 101-102,200
  vpc 10

interface nve1
  host-reachability protocol bgp
  member vni 30101 ## configuring VTEP (VXLAN tunnel endpoint) with parameters for L2 VNI 30101
    suppress-arp
    mcast-group 239.1.1.101
  member vni 30200 ## configuring VTEP with parameters for L2 VNI 30200
    suppress-arp
    mcast-group 239.1.1.200
  member vni 50001 associate-vrf ## configuring VTEP with parameters for L3 VRF VNI 50001

router bgp 65000
  address-family l2vpn evpn ## enabling bgp evpn control plane for host reachability
  vrf VRF-A
    address-family ipv4 unicast
    advertise l2vpn evpn
    redistribute direct route-map FABRIC-RMAP-REDIST-SUBNET
    maximum-paths ibgp 2
  evpn
  vni 30200 12 ## enabling bgp evpn control plane for host reachability for L2 VNI 30200
    rd auto
    route-target import auto
    route-target export auto
  vni 30101 12 ## enabling bgp evpn control plane for host reachability for L2 VNI 30101
    rd auto
    route-target import auto
    route-target export auto
  vni 30102 12 ## enabling bgp evpn control plane for host reachability for L2 VNI 30102
    rd auto
    route-target import auto
    route-target export auto
Configuration 6b: IPBD-Based Leaf Switch

Border Leaf 1 and Border Leaf 2 Configuration

install feature-set fabric
vdc leaf1 id 1
  allow feature-set fabric
feature-set fabric
feature nv overlay
feature vni
nv overlay evpn

route-map FABRIC-RMAP-REDIST-SUBNET permit 10
  match tag 12345

vni 30101  ## creating VNI 30101 in the system
vni 30102  ## creating VNI 30102 in the system
vni 30200  ## creating VNI 30200 in the system
vni 50001  ## creating VNI 50001 in the system

system bridge-domain 1500-2500  ## bridge domains, which will tie VNIs and VLANs together

encapsulation profile vni VSI_to_VNI  ## mapping vlan 101 to L2 VNI 30101
  dot1q 101-102,200 vni 30101-30102,30200

bridge-domain 1500-1502  ## mapping bridge-domains 1500->30101, 1501->30102, 1502->30200
  member vni 30101-30102, 30200

vrf context VRF-A
  vni 50001
  rd auto
  address-family ipv4 unicast
    route-target both auto
    route-target both auto evpn

interface Bdi1502
  vrf member VRF-A
  ip address 10.10.200.1/24 tag 12345
  fabric forwarding mode anycast-gateway

interface nve1  ## VTEP configuration
  host-reachability protocol bgp
  member vni 30101  ## configuring VTEP (VXLAN tunnel endpoint) with parameters for L2 VNI 30101
    suppress-arp
    mcast-group 239.1.1.101
  member vni 30102  ## configuring VTEP (VXLAN tunnel endpoint) with parameters for L2 VNI 30102
    suppress-arp
mcast-group 239.1.1.102
member vni 30200
suppress-arp
mcast-group 239.1.1.200
member vni 50001 associate-vrf

interface Ethernet3/10
channel-group 10 mode active

interface Ethernet3/11
channel-group 10 mode active

interface Port-channel 10
vpc 10
service instance 1 vni
encapsulation profile VSI_to_VNI

router bgp 65000
address-family l2vpn evpn
vrf VRF-A
  address-family ipv4 unicast
  advertise l2vpn evpn
  redistribute direct route-map FABRIC-RMAP-REDIST-SUBNET
  maximum-paths ibgp 2
  evpn
vni 30200
rd auto
route-target import auto
route-target export auto

vni 30101
rd auto
route-target import auto
route-target export auto

vni 30102
rd auto
route-target import auto
route-target export auto
**Active-Standby Failover East-West Firewalls in Transparent Mode with vPC Connectivity**

Often firewalls are deployed in transparent mode. With this approach, the firewall acts as a transparent bridge between the inside and the outside interfaces. However, depending on the firewall vendor, the inside VLAN ID for the protected subnet may not match the outside VLAN ID, as shown in Figure 6. Figure 15 shows the physical connectivity.

**Figure 15.** Physical Connectivity Diagram Showing Active-Standby Failover East-West Firewalls in Transparent Mode with Dual-Homed vPC Connectivity to Leaf Nodes. VLANs 101 and 102 Are Protected Subnets. VLANs 111 and 112 Are Nonprotected Subnets

The vPC is configured as a trunk port carrying two VLANs for a given protected network. In the case here, VLAN 101 on the inside maps to VLAN 301 on the outside, and VLAN 102 similarly maps to VLAN 302, for a total of four VLANs trunked on port channels Po1 and Po2.

VLAN 301 maps to VNI 30301, and VLAN 302 maps to VNI 30302. Depending on the Cisco Nexus switch type used as leaf 1 and leaf 2, VLAN 301 and VNI 30301 and VLAN 302 and VNI 30302 are terminated either using an SVI or BDI (for VLAN or bridge-domain switches, respectively). These interfaces are configured in fabric forward anycast-gateway mode and serve as default gateways for the respective protected subnets:

- The SVI and BDI for VLAN 301 and VNI 30301 are default gateways for VLAN 101 and VNI 30101.
- The SVI and BDI for VLAN 302 and VNI 30302 are default gateways for VLAN 102 and VNI 30102.

Because the SVI and BDI are in anycast-gateway mode, you do not need to configure manual redistribution.

Note that no hosts in the fabric are directly attached to VLAN 301 and VNI 30301 or VLAN 302 and VNI 30302, and hosts are configured only on leaf nodes with attached east-west firewalls in transparent mode.

Configurations 7a and 7b show the required definitions and configurations needed to deploy the example in Figure 15. Note that only a single leaf configuration is provided; the second leaf has the exact same configuration. The VLAN and VNI and SVI and BDI configurations for nonprotected subnets VLAN 111 and VLAN 112 are not shown.
**Configuration 7a: IPVLAN-Based Leaf Switch**

```plaintext
feature vn-segment-vlan-based
feature nv overlay

route-map FABRIC-RMAP-REDIST-SUBNET permit 10
    match tag 12345

vlan 101
    vn-segment 30101  ## mapping the vlan 101 to Layer-2 VNI 30101
vlan 102
    vn-segment 30102  ## mapping the vlan 102 to Layer-2 VNI 30102

vlan 301
    vn-segment 30301  ## mapping the vlan 301 to Layer-2 VNI 30301
vlan 302
    vn-segment 30302  ## mapping the vlan 302 to Layer-2 VNI 30302

vlan 2000
    vn-segment 50001  ## mapping the vlan 2000 to Layer-3 VRF VNI 50001

vrf context VRF-A
    vni 50001
    rd auto
    address-family ipv4 unicast
        route-target both auto
        route-target both auto evpn

interface Vlan301 VLAN101/VNI30101.
    no shutdown
    vrf member VRF-A
    ip address 10.10.101.1/24  tag 12345
    fabric forwarding mode anycast-gateway

interface Vlan302 VLAN102/VNI30102.
    no shutdown
    vrf member VRF-A
    ip address 10.10.102.1/24 tag 12345
    fabric forwarding mode anycast-gateway

interface Vlan2000  ## interface, used as an L3 VRF VNI interface
    no shutdown
    vrf member VRF-A
    no ip redirects
    ip forward
    ipv6 forward
```

no ipv6 redirects

interface Ethernet1/25  ## configuring member of port-channel 1
  switchport mode trunk
  switchport trunk allowed vlan add 101-102, 301-302
  channel-group 1 mode active

interface Ethernet1/26  ## configuring member of port-channel 2
  switchport mode trunk
  switchport trunk allowed vlan add 101-102, 301-302
  channel-group 2 mode active

interface Port-channel 1  ## configuring port-channel 1/ vpc11 to active firewall node
  switchport mode trunk
  switchport trunk allowed vlan add 101-102, 301-302
  vpc 11

interface Port-channel 2  ## configuring port-channel 2/ vpc12 to standby firewall node
  switchport mode trunk
  switchport trunk allowed vlan add 101-102, 301-302
  vpc 12

interface nve1
  host-reachability protocol bgp
  member vni 30101  ## configuring VTEP parameters for L2 VNI 30101
    suppress-arp
    mcast-group 239.1.1.101
  member vni 30102  ## configuring VTEP parameters for L2 VNI 30102
    suppress-arp
    mcast-group 239.1.1.102
  member vni 30301  ## configuring VTEP parameters for L2 VNI 30301
    suppress-arp
    mcast-group 239.1.1.101
  member vni 30302  ## configuring VTEP parameters for L2 VNI 30302
    suppress-arp
    mcast-group 239.1.1.102
  member vni 50001 associate-vrf  ## configuring L3 VRF VNI 50001

router bgp 65000
  address-family l2vpn evpn  ## enabling bgp evpn control plane for host reachability
  vrf VRF-A
    address-family ipv4 unicast
    advertise l2vpn evpn
    redistribute direct route-map FABRIC-RMAP-REDIST-SUBNET
    maximum-paths ibgp 2
  evpn
    vni 30101 12  ## enabling bgp evpn control plane for host reachability for L2 VNI 30101
    rd auto
route-target import auto
route-target export auto
vni 30102 12  ## enabling bgp evpn control plane for host reachability for L2 VNI 30102
    rd auto
    route-target import auto
    route-target export auto
vni 30301 12  ## enabling bgp evpn control plane for host reachability for L2 VNI 30301
    rd auto
    route-target import auto
    route-target export auto
vni 30302 12  ## enabling bgp evpn control plane for host reachability for L2 VNI 30302
    rd auto
    route-target import auto
    route-target export auto

Configuration 7b: IPBD-Based Leaf Switch

install feature-set fabric
vdc leaf1 id 1
    allow feature-set fabric
feature-set fabric
feature nv overlay
feature vni
nv overlay evpn

route-map FABRIC-RMAP-REDIST-SUBNET permit 10
    match tag 12345

vni 30101  ## creating VNI 30101 in the system
vni 30102  ## creating VNI 30102 in the system
vni 30301  ## creating VNI 30301 in the system
vni 30302  ## creating VNI 30302 in the system
vni 50001  ## creating VNI 50001 in the system

system bridge-domain 1500-2500  ## bridge domains, which will tie VNIs and VLANs together

encapsulation profile vni VSI_to_VNI  ## mapping VLANs to respective VNIs
    dot1q 101-102,301-302 vni 30101-30102,30301-30302

bridge-domain 1500-1503  ## mapping bridge-domains: 1500->30101, 1501->30102, 1502->30301,
                        1503->30302
    member vni 30101-30102, 30301-30302

vrf context VRF-A
vni 50001
    rd auto
    address-family ipv4 unicast
    route-target both auto
    route-target both auto evpn
interface Bdi1502  ## interface, used as default gateway for protected subnet
   VLAN101/VNI30101
   vrf member VRF-A
   ip address 10.10.101.1/24 tag 12345
   fabric forwarding mode anycast-gateway

interface Bdi1503  ## interface, used as default gateway for protected subnet
   VLAN102/VNI30102
   vrf member VRF-A
   ip address 10.10.102.1/24 tag 12345
   fabric forwarding mode anycast-gateway

interface nve1   ## VTEP configuration
   host-reachability protocol bgp
   member vni 30101  ## configuring VTEP parameters for L2 VNI 30101
      suppress-arp
      mcast-group 239.1.1.101
   member vni 30102  ## configuring VTEP parameters for L2 VNI 30102
      suppress-arp
      mcast-group 239.1.1.102
   member vni 30301  ## configuring VTEP parameters for L2 VNI 30301
      suppress-arp
      mcast-group 239.1.1.101
   member vni 30302  ## configuring VTEP parameters for L2 VNI 30302
      suppress-arp
      mcast-group 239.1.1.102
   member vni 50001 associate-vrf  ## configuring L3 VRF VNI 50001

interface Ethernet3/10  ## configuring member of port-channel 1
   channel-group 11 mode active

interface Ethernet3/11  ## configuring member of port-channel 2
   channel-group 12 mode active

interface port-channel1  ## configuring port-channel 1/ vpc11 to active firewall node
   vpc 11
   service instance 1 vni
      encapsulation profile VSI_to_VNI  ## config for port-significant VLAN to VNI mapping

interface port-channel2  ## configuring port-channel 2/ vpc12 to standby firewall node
   vpc 11
   service instance 1 vni
      encapsulation profile VSI_to_VNI  ## config for port-significant VLAN to VNI mapping

router bgp 65000
   address-family l2vpn evpn
   vrf VRF-A
      address-family ipv4 unicast
      advertise l2vpn evpn
      redistribute direct route-map FABRIC-RMAP-REDIST-SUBNET
Active-Standby Failover East-West Firewalls in Transparent Mode

As with routed active-standby firewalls configured in routed mode (shown earlier in Figure 13), firewalls configured in single-attached mode will lead to suboptimal forwarding (Figure 16). Border leaf 2 is configured with the SVI and BDI in anycast-gateway mode and hence attracts traffic directed to protected subnets, but it is also attached to the standby firewall, which is dormant in the normal operational state. Upon receipt of traffic to protected subnets, border leaf 2 will route traffic to border leaf 1 through the fabric to reach protected subnets.

**Figure 16.** Suboptimal Forwarding in Scenario with Active-Standby Failover East-West Firewalls with Individual Port-Channel Connectivity to Leaf Nodes
The configuration is almost identical to Configurations 7a and 7b. The only difference is that the firewall-facing interfaces are no longer vPCs.

**Clustered East-West Firewalls in Transparent Mode**


The leaf configuration is identical to Configurations 7a and 7b. In addition, because both firewalls are actively forwarding traffic, this configuration eliminates suboptimal traffic routing (Figure 17).

**Figure 17.** Clustered Firewalls in Transparent Mode with Spanned EtherChannel and vPC Connectivity to Leaf Nodes

Tenant-Edge Firewall Deployment Scenarios

As discussed in the introduction to this document, tenant-edge firewalls are deployed when the data traffic between the VRF instances or tenants needs to be subjected to security policies. A tenant-edge firewall is often used as an ultimate gateway out of the VRF instance, which means that any traffic that needs to be sent outside the routing domain of a given VRF instance has to pass through the tenant-edge firewall. This section explores this case (Figure 18).
Figure 18. VRF A and VRF B Are Protected VRF Instances in the Fabric. VRF EXT Interfaces with the External World through the WAN or Edge Router. The Tenant-Edge Firewall in Routed Mode Is Connected to All Three VRF Instances and Enforces Security Policies for All Traffic Routed between These VRF Instances. The Tenant-Edge Firewall’s Default Route Points to VRF EXT to Reach External Networks

Figure 18 shows three connections between the tenant-edge firewall and the VRF instances in the fabric. These connections can be made using either separate interfaces or IEEE 802.1Q VLAN tags within a single interface.

The connection between the external VRF instance (VRF EXT) and the WAN or edge router is established using border leaf nodes and is outside the scope of this document. Note that this document assumes that the routing table for VRF EXT already has a default route (whether statically configured or dynamically learned) that points to the WAN or edge router.

A typical network connection location for the tenant-edge firewall is at the border leaf nodes. However, border leaf nodes often are not configured with vPC peering. If vPC dual-attached connection from firewalls is needed, the firewalls can be also connected to regular leaf nodes.

The firewall deployment scenario, where it is deployed as a default gateway for protected subnets in addition to protecting entire VRF is covered in the section “Complex Deployment Scenarios” later in this document.

This section discusses the tenant-edge firewall deployment scenarios shown in Figures 19, 20, and 21. These scenarios are derived from the logical diagram in Figure 18 and assume that the firewall is enforcing security policies between two or more VRF instances (tenants).
Figure 19. Single-Attached Tenant-Edge Firewalls in Routed Mode with Active-Standby Failover and Static or Dynamic Routing

Figure 20. vPC Dual-Attached Tenant-Edge Firewall in Routed Mode with Clustering and Static Routing

Figure 21. Single-Attached Tenant-Edge Firewalls in Transparent Mode with Clustering and Static or Dynamic Routing
Active-Standby Failover: Single-Attached Tenant-Edge Firewalls in Routed Mode with Static Routing

The physical topology for this deployment scenario is shown in Figure 19. The static routing deployment scenario is shown in Configurations 8a and 8b.

As shown in the logical topology in Figure 18, the port channel between each of the active and standby firewall nodes and the fabric carries three IEEE 802.1Q VLANs. Each of these VLANs is used to establish routing peering between the respective VRF instance in the fabric and the firewall.

In the example here, each leaf node is configured with the SVI and BDI in anycast-gateway mode for peering with the firewall. SVI and BDI 3001 is a member of VRF A, SVI and BDI 3002 is a member of VRF B, and SVI and BDI 3500 is a member of VRF EXT. Figure 22 shows the logical connections between leaf nodes and firewalls units.

Figure 22. One VLAN Is Used for Each VRF Instance for Routing Peering between the Leaf Nodes and Tenant-Edge Firewalls

The border leaf advertises a default route to each of the protected VRF instances: VRF A and VRF B. This behavior is achieved either by redistributing the statically configured default route to the fabric control plane (BGP) or by dynamically advertising the default route to BGP. The goal is to help ensure that all leaf nodes in a fabric forward any traffic traveling from the VRF instance to the border leaf (or whichever leaf is attracting the default route and is connected to a tenant-edge firewall).

After the traffic arrives at the border leaf, data is forwarded to the firewall for security policy enforcement. Because the firewall acts as a router and has local statically configured routes to each protected subnet across all attached VRF instances, it routes the traffic out of the appropriate logical interface. That is, if traffic from VRF A is destined for VRF B, the tenant-edge firewall will receive traffic in VLAN 3001 from the fabric and then forward it back to the fabric in VLAN 3002.

However, when traffic is destined for an unknown destination, it is sent using a statically configured default route that points to VRF EXT, and such traffic is tagged with IEEE 802.1Q tag 3500.

Both border leaf nodes are identically configured with anycast gateways, VRF instances, and static routes. In a normal operational state, border leaf 2 forwards all data traffic to the active tenant-edge firewall unit through border leaf 1. You can improve such suboptimal forwarding by implementing clustered firewalls.
Configuration 8a: IPVLAN-Based Leaf Switch

```plaintext
feature vn-segment-vlan-based
feature nv overlay

route-map FABRIC-RMAP-REDIST-SUBNET permit 10
    match tag 12345

ip access-list DEFAULT-ROUTE
    20 permit ip 0.0.0.0/0 any

ip access-list VRF-SUBNETS
    10 deny ip 0.0.0.0/0 any
    20 permit any any

route-map REDIST-DEF-ROUTE permit 10
    match ip address DEFAULT-ROUTE

route-map REDIST-VRF-SUBNETS permit 10
    match ip address VRF-SUBNETS

vlan 3001
    vn-segment 33001  # mapping the vlan 3001 to Layer-2 VNI 33001

vlan 3002
    vn-segment 33002  # mapping the vlan 3002 to Layer-2 VNI 33002

vlan 3500
    vn-segment 33500  # mapping the vlan 3500 to Layer-2 VNI 33500

vlan 2000
    vn-segment 50001  # mapping the vlan 2000 to Layer-3 VRF VNI 50001 of VRF-A

vlan 2001
    vn-segment 50002  # mapping the vlan 2001 to Layer-3 VRF VNI 50002 of VRF-B

vlan 2002
    vn-segment 50010  # mapping the vlan 2002 to Layer-3 VRF VNI 50010 of VRF-EXT

vrf context VRF-A
    vni 50001
    ip route 0.0.0.0/0 10.10.231.2  # static default route to attract all egress traffic out of the VRF-A. Next-hop is Firewall.
    rd auto
    address-family ipv4 unicast
    route-target both auto
    route-target both auto evpn

vrf context VRF-B
    vni 50002
    ip route 0.0.0.0/0 10.10.232.2  # static default route to attract all egress traffic out
```
of the VRF-B. Next-hop is Firewall.
rd auto
address-family ipv4 unicast
  route-target both auto
  route-target both auto evpn

vrf context VRF-EXT
  vni 50010
  ip route 0.0.0.0/0 10.77.1.2  ## static default route to WAN/Edge router
  ip route 10.10.101.0/24 10.10.235.5  ## static route to VLAN101 subnet in VRF-A. Next-hop is Firewall.
  ip route 10.11.121.0/24 10.10.235.5  ## static route to VLAN1121 subnet in VRF-B. Next-hop is Firewall.
rd auto
address-family ipv4 unicast
  route-target both auto
  route-target both auto evpn

interface Vlan3001  ## interface, used for Layer-3 peering with fabric.
  no shutdown
  vrf member VRF-A
  ip address 10.10.231.1/24  tag 12345
    fabric forwarding mode anycast-gateway  ## enabling anycast-gateway mode

interface Vlan3002  ## interface, used for Layer-3 peering with fabric.
  no shutdown
  vrf member VRF-B
  ip address 10.10.232.1/24  tag 12345
    fabric forwarding mode anycast-gateway  ## enabling anycast-gateway mode

interface Vlan3500  ## interface, used for Layer-3 peering with fabric.
  no shutdown
  vrf member VRF-EXT
  ip address 10.10.235.1/24  tag 12345
    fabric forwarding mode anycast-gateway  ## enabling anycast-gateway mode

interface Vlan2000  ## interface, used as an L3 VRF VNI interface
  no shutdown
  vrf member VRF-A
  no ip redirects
  ip forward
  ipv6 forward
  no ipv6 redirects

interface Vlan2001  ## interface, used as an L3 VRF VNI interface
  no shutdown
  vrf member VRF-B
no ip redirects
ip forward
ipv6 forward
no ipv6 redirects

interface Vlan2002  ## interface, used as an L3 VRF VNI interface
  no shutdown
  vrf member VRF-EXT
  no ip redirects
  ip forward
  ipv6 forward
  no ipv6 redirects

interface Ethernet1/25  ## port-channel 10 member interface
  channel-group 10 mode active

interface Ethernet1/26  ## port-channel 10 member interface
  channel-group 10 mode active

interface Port-channel 10
  switchport trunk allowed vlan add 3001-3002,3500

interface nve1
  host-reachability protocol bgp
  member vni 33001
    suppress-arp
    mcast-group 239.1.1.200
  member vni 33002
    suppress-arp
    mcast-group 239.1.1.201
  member vni 33500
    suppress-arp
    mcast-group 239.1.1.202
  member vni 50001 associate-vrf
  member vni 50002 associate-vrf
  member vni 50010 associate-vrf

router bgp 65000
  address-family l2vpn evpn
  vrf VRF-A
    address-family ipv4 unicast
    advertise l2vpn evpn
    redistribute direct route-map FABRIC-RMAP-REDIST-SUBNET
    redistribute static route-map REDIST-DEF-ROUTE ## redistributing default route into VRF-A
    maximum-paths ibgp 2
  vrf VRF-B
    address-family ipv4 unicast
advertise l2vpn evpn
redistribute direct route-map FABRIC-RMAP-REDIST-SUBNET

redistribute static route-map REDIST-DEF-ROUTE ## redistributing default route into VRF-B
maximum-paths ibgp 2
vrf VRF-EXT
address-family ipv4 unicast
advertise l2vpn evpn
redistribute direct route-map FABRIC-RMAP-REDIST-SUBNET
redistribute static route-map REDIST-VRF-SUBNETS ## redistributing routing reachability towards protected subnets in protected VRFs
maximum-paths ibgp 2
evpn
vni 33001 12
  rd auto
  route-target import auto
  route-target export auto
evni 33002 12
  rd auto
  route-target import auto
  route-target export auto
evni 33500 12
  rd auto
  route-target import auto
  route-target export auto

Configuration 8b: IPBD-Based Leaf Switch

install feature-set fabric
vdc leaf1 id 1
  allow feature-set fabric
feature-set fabric
feature nv overlay
feature vni
nv overlay evpn
route-map FABRIC-RMAP-REDIST-SUBNET permit 10
  match tag 12345

ip access-list DEFAULT-ROUTE
  20 permit ip 0.0.0.0/0 any

ip access-list VRF-SUBNETS
  10 deny ip 0.0.0.0/0 any
  20 permit any any

route-map REDIST-DEF-ROUTE permit 10
  match ip address DEFAULT-ROUTE
route-map REDIST-VRF-SUBNETS permit 10
   match ip address VRF-SUBNETS

vni 33001  ## creating VNI 33001 in the system
vni 33002  ## creating VNI 33002 in the system
vni 33500  ## creating VNI 33500 in the system
vni 50001  ## creating VNI 50001 in the system
vni 50002  ## creating VNI 50002 in the system
vni 50010  ## creating VNI 50010 in the system

system bridge-domain 1500-1502,2500-2502  ## bridge domains, which will tie VNIs and VLANs together

encapsulation profile vni VSI_to_VNI  ## mapping VLANs to respective VNIs
dot1q 3001-3002,3500 vni 33001-33002,33500

bridge-domain 1500-1502  ## mapping bridge-domains: 1500->33001, 1501->33002, 1502->33500
  member vni 33001-33002, 33500

vrf context VRF-A
  vni 50001
  ip route 0.0.0.0/0 10.10.231.2  ## static default route to attract all egress traffic out of the VRF-A. Next-hop is Firewall.
    rd auto
    address-family ipv4 unicast
      route-target both auto
      route-target both auto evpn

vrf context VRF-B
  vni 50002
  ip route 0.0.0.0/0 10.10.232.2  ## static default route to attract all egress traffic out of the VRF-B. Next-hop is Firewall.
    rd auto
    address-family ipv4 unicast
      route-target both auto
      route-target both auto evpn

vrf context VRF-EXT
  vni 50010
  ip route 0.0.0.0/0 10.77.1.2  ## static default route to WAN/Edge router
  ip route 10.10.101.0/24 10.10.235.5  ## static route to VLAN101 subnet in VRF-A. Next-hop is Firewall.
    rd auto
    address-family ipv4 unicast
      route-target both auto
      route-target both auto evpn

  ip route 10.11.121.0/24 10.10.235.5  ## static route to VLAN1121 subnet in VRF-B. Next-hop is Firewall.
    rd auto
    address-family ipv4 unicast
      route-target both auto
      route-target both auto evpn

interface Bdi1500
vrf member VRF-A
  ip address 10.10.231.1/24  tag 12345
  fabric forwarding mode anycast-gateway  ## enabling anycast-gateway mode

interface Bdi1501
  vrf member VRF-B
  ip address 10.10.232.1/24  tag 12345
  fabric forwarding mode anycast-gateway  ## enabling anycast-gateway mode

interface Bdi1501
  vrf member VRF-EXT
  ip address 10.10.235.1/24  tag 12345
  fabric forwarding mode anycast-gateway  ## enabling anycast-gateway mode

interface nve1  ## VTEP configuration
host-reachability protocol bgp
  member vni 33001
    suppress-arp
    mcast-group 239.1.1.200
  member vni 33002
    suppress-arp
    mcast-group 239.1.1.201
  member vni 33500
    suppress-arp
    mcast-group 239.1.1.202
  member vni 50001 associate-vrf
  member vni 50002 associate-vrf
  member vni 50010 associate-vrf

interface Ethernet3/10  ## configuring member of port-channel 10
  channel-group 10 mode active

interface Ethernet3/11  ## configuring member of port-channel 10
  channel-group 10 mode active

interface port-channel1  ## configuring port-channel 1/ vpc11 to active firewall node
  service instance 1 vni
    encapsulation profile VSI_to_VNI  ## config for port-significant VLAN to VNI mapping

router bgp 65000
  address-family l2vpn evpn
  vrf VRF-A
    address-family ipv4 unicast
    advertise l2vpn evpn
    redistribute direct route-map FABRIC-RMAP-REDIST-SUBNET
    redistribute static route-map REDIST-DEF-ROUTE  ## redistributing default route into VRF-A
      maximum-paths ibgp 2
Active-Standy Failover: Single-Attached Tenant-Edge Firewalls in Routed Mode with Dynamic Routing

When operational practices allow you to run a dynamic routing protocol between the fabric and the firewall, you can reduce the overhead related to the static configuration of routing reachability information on both the firewalls and the fabric. This scenario is based on the logical diagram shown in Figure 18.

The physical topology is precisely the same as shown in Figure 19, but some of the configuration is different. For example, anycast-gateway mode is no longer used for the SVI and BDI used to establish routing adjacency with the firewall. In addition, the IP addresses of the SVI and BDI for the respective VLANs must be different on each border leaf node, but the interfaces must be on the same subnet.

Also, the route maps used for route redistribution may need to change depending on the operating practices used. This document assumes that the firewall is sending the default route using OSPF.

```
vrf VRF-B
  address-family ipv4 unicast
  advertise l2vpn evpn
  redistribute direct route-map FABRIC-RMAP-REDIST-SUBNET

redistribute static route-map REDIST-DEF-ROUTE  ## redistributing default route into VRF-B
  maximum-paths ibgp 2
vrf VRF-EXT
  address-family ipv4 unicast
  advertise l2vpn evpn
  redistribute direct route-map FABRIC-RMAP-REDIST-SUBNET

redistribute static route-map REDIST-VRF-SUBNETS  ## redistributing routing reachability towards protected subnets in protected VRFs
  maximum-paths ibgp 2
evpn
  vni 33001 12
    rd auto
    route-target import auto
    route-target export auto
  vni 33002 12
    rd auto
    route-target import auto
    route-target export auto
  vni 33500 12
    rd auto
    route-target import auto
    route-target export auto
```
Configuration 9a: IPVLAN-Based Leaf Switch

feature vn-segment-vlan-based
feature nv overlay
feature ospf  ## enable feature ospf

route-map FABRIC-RMAP-REDIST-SUBNET permit 10
  match tag 12345

ip access-list DEFAULT-ROUTE
  20 permit ip 0.0.0.0/0 any

ip access-list DENY-DEFAULT
  10 deny ip 0.0.0.0/0 any
  20 permit any any

route-map REDIST-DEF-ROUTE permit 10
  match ip address DEFAULT-ROUTE

route-map REDIST-DENY-DEFAULT permit 10
  match ip address DENY-DEFAULT

route-map REDIST-BGP-OSPF permit 10

vlan 3001
  vn-segment 33001
vlan 3002
  vn-segment 33002
vlan 3500
  vn-segment 33500

vlan 2000
  vn-segment 50001
vlan 2001
  vn-segment 50002
vlan 2002
  vn-segment 50010

vrf context VRF-A  ## no static routes configured
  vni 50001
  rd auto
  address-family ipv4 unicast
    route-target both auto
    route-target both auto evpn

vrf context VRF-B  ## no static routes configured
  vni 50002
  rd auto
address-family ipv4 unicast
  route-target both auto
  route-target both auto evpn

vrf context VRF-EXT ## no static routes configured
  vni 50010
  rd auto
  address-family ipv4 unicast
  route-target both auto
  route-target both auto evpn

interface Vlan3001   ## regular (not anycast-gateway) SVI to establish routing adjacency with firewall
  no shutdown
  vrf member VRF-A
  ip address 10.10.231.1/24
  ip router ospf OSPF-10 area 0

interface Vlan3002   ## regular (not anycast-gateway) SVI to establish routing adjacency with firewall
  no shutdown
  vrf member VRF-B
  ip address 10.10.232.1/24
  ip router ospf OSPF-10 area 0

interface Vlan3500   ## regular (not anycast-gateway) SVI to establish routing adjacency with firewall
  no shutdown
  vrf member VRF-EXT
  ip address 10.10.235.1/24
  ip router ospf OSPF-10 area 0

interface Vlan2000
  no shutdown
  vrf member VRF-A
  no ip redirects
  ip forward
  ipv6 forward
  no ipv6 redirects

interface Vlan2001
  no shutdown
  vrf member VRF-B
  no ip redirects
  ip forward
  ipv6 forward
  no ipv6 redirects

interface Vlan2002
no shutdown
vrf member VRF-EXT
no ip redirects
ip forward
ipv6 forward
no ipv6 redirects

interface Ethernet1/25
  switchport mode trunk
  channel-group 10 mode active

interface Ethernet1/26
  switchport mode trunk
  channel-group 10 mode active

interface Port-channel 10
  switchport mode trunk
  switchport trunk allowed vlan add 3001-3002,3500

interface nve1
  host-reachability protocol bgp
  member vni 33001
    suppress-arp
    mcast-group 239.1.1.200
    member vni 33002
    suppress-arp
    mcast-group 239.1.1.201
  member vni 33500
    suppress-arp
    mcast-group 239.1.1.202
  member vni 50001 associate-vrf
  member vni 50002 associate-vrf
  member vni 50010 associate-vrf

router bgp 65000
  address-family l2vpn evpn
  vrf VRF-A
    address-family ipv4 unicast
    advertise l2vpn evpn
    redistribute direct route-map FABRIC-RMAP-REDIST-SUBNET
  redistribute ospf OSPF-10 route-map REDIST-DEF-ROUTE  ## redistribute default route from OSPF into VRF-A
    maximum-paths ibgp 2
  vrf VRF-B
    address-family ipv4 unicast
    advertise l2vpn evpn
    redistribute direct route-map FABRIC-RMAP-REDIST-SUBNET
    redistribute ospf OSPF-10 route-map REDIST-DEF-ROUTE  ## redistribute default route
from OSPF into VRF-B
maximum-paths ibgp 2
vrf VRF-EXT
address-family ipv4 unicast
advertise 12vpn evpn
redistribute direct route-map FABRIC-RMAP-REDIST-SUBNET
redistribute ospf OSPF-10 route-map REDIST-DENY-DEFAULT ## redistribute VRF-A and VRF-B protected subnet prefixes from OSPF into VRF-EXT
maximum-paths ibgp 2
evpn
vni 33001 12
  rd auto
  route-target import auto
  route-target export auto

vni 33002 12
  rd auto
  route-target import auto
  route-target export auto

vni 33500 12
  rd auto
  route-target import auto
  route-target export auto

router ospf OSPF-10 ## configuring per-VRF ospf routing protocol
vrf VRF-A
  redistribute bgp route-map REDIST-BGP-OSPF ## advertise VRF-A route prefixes to firewall
  router-id 10.10.10.10
vrf VRF-B
  redistribute bgp route-map REDIST-BGP-OSPF ## advertise VRF-A route prefixes to firewall
  router-id 10.10.10.10
vrf VRF-EXT
  redistribute bgp route-map REDIST-DEF-ROUTE ## advertise only default route to firewall
  router-id 10.10.10.10

Configuration 9b: IPBD-Based Leaf Switch
install feature-set fabric
vdc leaf1 id 1
  allow feature-set fabric
feature-set fabric
feature nv overlay
feature vni
feature ospf ## enable feature ospf
nv overlay evpn

route-map FABRIC-RMAP-REDIST-SUBNET permit 10
  match tag 12345

ip access-list DEFAULT-ROUTE
  20 permit ip 0.0.0.0/0 any

ip access-list DENY-DEFAULT
<table>
<thead>
<tr>
<th>Rule</th>
<th>Action</th>
<th>Source</th>
<th>Destination</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>deny</td>
<td>ip 0.0.0.0/0</td>
<td>any</td>
</tr>
<tr>
<td>20</td>
<td>permit</td>
<td>any</td>
<td>any</td>
</tr>
</tbody>
</table>

**Route Map**

```
route-map REDIST-DEF-ROUTE permit 10
match ip address DEFAULT-ROUTE
```

```
route-map REDIST-DENY-DEFAULT permit 10
match ip address DENY-DEFAULT
```

```
route-map REDIST-BGP-OSPF permit 10
```

**VNI Configuration**

- vni 33001
- vni 33002
- vni 33500
- vni 50001
- vni 50002
- vni 50010

**System Configuration**

```
system bridge-domain 1500-1502,2500-2502
```

```
encapsulation profile vni VSI_to_VNI
dot1q 3001-3002,3500 vni 33001-33002,33500
```

```
bridge-domain 1500-1502
member vni 33001-33002, 33500
```

**VRF Contexts**

**VRF-A**

```
vrf context VRF-A
vni 50001
ip route 0.0.0.0/0 10.10.231.2
rd auto
address-family ipv4 unicast
  route-target both auto
  route-target both auto evpn
```

**VRF-B**

```
vrf context VRF-B
vni 50002
ip route 0.0.0.0/0 10.10.232.2
rd auto
address-family ipv4 unicast
  route-target both auto
  route-target both auto evpn
```

**VRF-EXT**

```
vrf context VRF-EXT
vni 50010
ip route 0.0.0.0/0 10.77.1.2
ip route 10.10.101.0/24 10.10.235.5
ip route 10.11.121.0/24 10.10.235.5
rd auto
```
address-family ipv4 unicast
  route-target both auto
  route-target both auto evpn

interface Bdi1500
  vrf member VRF-A
  ip address 10.10.231.1/24  tag 12345
  fabric forwarding mode anycast-gateway

interface Bdi1501
  vrf member VRF-B
  ip address 10.10.232.1/24  tag 12345
  fabric forwarding mode anycast-gateway

interface Bdi1501
  vrf member VRF-EXT
  ip address 10.10.235.1/24  tag 12345
  fabric forwarding mode anycast-gateway

interface nve1
  host-reachability protocol bgp
  member vni 33001
    suppress-arp
    mcast-group 239.1.1.200
  member vni 33002
    suppress-arp
    mcast-group 239.1.1.201
  member vni 33500
    suppress-arp
    mcast-group 239.1.1.202
  member vni 50001 associate-vrf
  member vni 50002 associate-vrf
  member vni 50010 associate-vrf

interface Ethernet3/10
  channel-group 10 mode active

interface Ethernet3/11
  channel-group 10 mode active

interface port-channel1
  service instance 1 vni
    encapsulation profile VSI_to_VNI

router bgp 65000
  address-family l2vpn evpn
  vrf VRF-A
    address-family ipv4 unicast
advertise l2vpn evpn
redistribute direct route-map FABRIC-RMAP-REDIST-SUBNET
redistribute ospf OSPF-10 route-map REDIST-DEF-ROUTE ## redistribute default route
from OSPF into VRF-A
  maximum-paths ibgp 2
vrf VRF-B
  address-family ipv4 unicast
  advertise l2vpn evpn
  redistribute direct route-map FABRIC-RMAP-REDIST-SUBNET
redistribute ospf OSPF-10 route-map REDIST-DEF-ROUTE ## redistribute default route
from OSPF into VRF-B
  maximum-paths ibgp 2
vrf VRF-EXT
  address-family ipv4 unicast
  advertise l2vpn evpn
  redistribute direct route-map FABRIC-RMAP-REDIST-SUBNET
redistribute ospf OSPF-10 route-map REDIST-DENY-DEFAULT ## redistribute VRF-A and VRF-B protected subnet prefixes from OSPF into VRF-EXT
  maximum-paths ibgp 2
evpn
  vni 33001 12
    rd auto
    route-target import auto
    route-target export auto
  vni 33002 12
    rd auto
    route-target import auto
    route-target export auto
  vni 33500 12
    rd auto
    route-target import auto
    route-target export auto
router ospf OSPF-10 ## configuring per-VRF ospf routing protocol
vrf VRF-A
  redistribute bgp route-map REDIST-BGP-OSPF ## advertise VRF-A route prefixes to firewall
  router-id 10.10.10.10
vrf VRF-B
  redistribute bgp route-map REDIST-BGP-OSPF ## advertise VRF-A route prefixes to firewall
  router-id 10.10.10.10
vrf VRF-EXT
  redistribute bgp route-map REDIST-DEF-ROUTE ## advertise only default route to firewall
  router-id 10.10.10.10
Clustered Mode: vPC Dual-Attached Tenant-Edge Firewalls in Routed Mode with Static Routing

An active-active clustered firewall setup avoids suboptimal routing by presenting two firewall units as a single unit to the fabric. This approach requires vPC dual-attachment of both firewall cluster units to vPC leaf nodes, as shown in Figure 20. As mentioned earlier, border leaf nodes are rarely deployed in vPC pairs, limiting the applicability of this scenario to regular leaf nodes. In addition, only static routing is supported in the current software.

This deployment scenario assumes that the border leaf of the fabric is advertising a default route in VRF EXT.

The configuration for this deployment scenario is almost identical to Configurations 8a and 8b. The difference is that port channels are now configured as dual-homed vPCs.

The ASA firewalls used in this scenario use a spanned EtherChannel configuration. Please refer to the configuration guide for details: http://www.cisco.com/c/en/us/td/docs/security/asa/asa94/configuration/general/asa-general-cli/ha-cluster.html#pgfId-2551285.

Clustered Mode: Single-Attached Tenant-Edge Firewalls in Routed Mode with Dynamic Routing


This deployment scenario is shown in Figure 21 and is simpler than the others from a network configuration perspective. It provides active-active clustering and allows you to run either static routing or dynamic routing peering between the firewall and the fabric. Firewalls rely on Equal-Cost Multipath (ECMP) to distribute the load between the firewall cluster units. This document describes only the scenario with dynamic routing peering (Figure 23).

The respective routed interfaces of the firewall do not need to be in the same Layer 2 domain, which allows simpler Layer 3 subinterface-based configuration. SVIs and BDIs and VLANs and bridge domains are not needed here to establish routing adjacency.

Figure 23. One VLAN Is Used for Each VRF Instance for Routing Peering between the Leaf Nodes and Tenant-Edge Firewalls

The configurations on both switches are very similar except for the locally significant IP addresses on the Layer 3 subinterfaces used for OSPF peering.
Configuration 10a: IPVLAN-Based Leaf Switch

```plaintext
feature vn-segment-vlan-based
feature nv overlay
feature ospf  ## enable feature ospf

route-map FABRIC-RMAP-REDIST-SUBNET permit 10
   match tag 12345

ip access-list DEFAULT-ROUTE
   20 permit ip 0.0.0.0/0 any

ip access-list DENY-DEFAULT
   10 deny ip 0.0.0.0/0 any
   20 permit any any

route-map REDIST-DEF-ROUTE permit 10
   match ip address DEFAULT-ROUTE

route-map REDIST-DENY-DEFAULT permit 10
   match ip address DENY-DEFAULT

route-map REDIST-BGP-OSPF permit 10

vlan 2000
   vn-segment 50001
vlan 2001
   vn-segment 50002
vlan 2002
   vn-segment 50010

vrf context VRF-A  ## no static routes configured
   vni 50001
   rd auto
   address-family ipv4 unicast
      route-target both auto
      route-target both auto evpn

vrf context VRF-B  ## no static routes configured
   vni 50002
   rd auto
   address-family ipv4 unicast
      route-target both auto
      route-target both auto evpn

vrf context VRF-EXT  ## no static routes configured
   vni 50010
   rd auto
```
address-family ipv4 unicast
  route-target both auto
  route-target both auto evpn

interface Port-channel 10.101  ## Layer-3 sub-interface for peering with Firewall in VRF-A
  no shutdown
  encapsulation dot1q 101  ## link-significant dot1q vlan tag 101
  vrf member VRF-A
  ip address 10.10.231.1/24
  ip router ospf OSPF-10 area 0

interface Port-channel 10.102  ## Layer-3 sub-interface for peering with Firewall in VRF-B
  no shutdown
  encapsulation dot1q 102  ## link-significant dot1q vlan tag 102
  vrf member VRF-B
  ip address 10.10.232.1/24
  ip router ospf OSPF-10 area 0

interface Port-channel 10.110  ## Layer-3 sub-interface for peering with Firewall in VRF-EXT
  no shutdown
  encapsulation dot1q 110  ## link-significant dot1q vlan tag 110
  vrf member VRF-EXT
  ip address 10.10.235.1/24
  ip router ospf OSPF-10 area 0

interface Vlan2000
  no shutdown
  vrf member VRF-A
  no ip redirects
  ip forward
  ipv6 forward
  no ipv6 redirects

interface Vlan2001
  no shutdown
  vrf member VRF-B
  no ip redirects
  ip forward
  ipv6 forward
  no ipv6 redirects

interface Vlan2002
  no shutdown
  vrf member VRF-EXT
  no ip redirects
  ip forward
  ipv6 forward
  no ipv6 redirects
interface Ethernet1/25
  channel-group 10 mode active

interface Ethernet1/26
  channel-group 10 mode active

interface Port-channel 10
  no switchport

interface nve1
  host-reachability protocol bgp
  member vni 50001 associate-vrf
  member vni 50002 associate-vrf
  member vni 50010 associate-vrf

router bgp 65000
  address-family l2vpn evpn
  vrf VRF-A
    address-family ipv4 unicast
    advertise l2vpn evpn
    redistribute direct route-map FABRIC-RMAP-REDIST-SUBNET
    redistribute ospf OSPF-10 route-map REDIST-DEF-ROUTE  ## redistribute default route from OSPF into VRF-A
    maximum-paths ibgp 2
  vrf VRF-B
    address-family ipv4 unicast
    advertise l2vpn evpn
    redistribute direct route-map FABRIC-RMAP-REDIST-SUBNET
    redistribute ospf OSPF-10 route-map REDIST-DEF-ROUTE  ## redistribute default route from OSPF into VRF-B
    maximum-paths ibgp 2
  vrf VRF-EXT
    address-family ipv4 unicast
    advertise l2vpn evpn
    redistribute direct route-map FABRIC-RMAP-REDIST-SUBNET
    redistribute ospf OSPF-10 route-map REDIST-DENY-DEFAULT  ## redistribute VRF-A and VRF-B protected subnet prefixes from OSPF into VRF-EXT
    maximum-paths ibgp 2

router ospf OSPF-10  ## configuring per-VRF ospf routing protocol
  vrf VRF-A
    redistribute bgp route-map REDIST-BGP-OSPF  ## advertise VRF-A route prefixes to firewall router-id 10.10.10.10
  vrf VRF-B
    redistribute bgp route-map REDIST-BGP-OSPF  ## advertise VRF-A route prefixes to firewall router-id 10.10.10.10
  vrf VRF-EXT
    redistribute bgp route-map REDIST-DEF-ROUTE  ## advertise only default route to firewall router-id 10.10.10.10
Configuration 10b: IPBD-Based Leaf Switch

```
install feature-set fabric
vdc leaf1 id 1
  allow feature-set fabric
feature-set fabric
feature nv overlay
feature vni
feature ospf  ## enable feature ospf
nv overlay evpn

route-map FABRIC-RMAP-REDIST-SUBNET permit 10
  match tag 12345

ip access-list DEFAULT-ROUTE
  20 permit ip 0.0.0.0/0 any

ip access-list DENY-DEFAULT
  10 deny ip 0.0.0.0/0 any
  20 permit any any

route-map REDIST-DEF-ROUTE permit 10
  match ip address DEFAULT-ROUTE

route-map REDIST-DENY-DEFAULT permit 10
  match ip address DENY-DEFAULT

route-map REDIST-BGP-OSPF permit 10

vni 50001
vni 50002
vni 50010

system bridge-domain 2500-2502

vrf context VRF-A
  vni 50001
  rd auto
  address-family ipv4 unicast
    route-target both auto
    route-target both auto evpn

vrf context VRF-B
  vni 50002
  rd auto
  address-family ipv4 unicast
    route-target both auto
```
route-target both auto evpn

vrf context VRF-EXT
  vni 50010
  rd auto
  address-family ipv4 unicast
  route-target both auto
data
  route-target both auto evpn

interface Port-channel 10.101  ## Layer-3 sub-interface for peering with Firewall in VRF-A
  no shutdown
  encapsulation dot1q 101  ## link-significant dot1q vlan tag 101
  vrf member VRF-A
  ip address 10.10.231.1/24
  ip router ospf OSPF-10 area 0

interface Port-channel 10.102  ## Layer-3 sub-interface for peering with Firewall in VRF-B
  no shutdown
  encapsulation dot1q 102  ## link-significant dot1q vlan tag 102
  vrf member VRF-B
  ip address 10.10.232.1/24
  ip router ospf OSPF-10 area 0

interface Port-channel 10.110  ## Layer-3 sub-interface for peering with Firewall in VRF-EXT
  no shutdown
  encapsulation dot1q 110  ## link-significant dot1q vlan tag 110
  vrf member VRF-EXT
  ip address 10.10.235.1/24
  ip router ospf OSPF-10 area 0

interface nve1
  host-reachability protocol bgp
data
  member vni 50001 associate-vrf
  member vni 50002 associate-vrf
  member vni 50010 associate-vrf

interface Ethernet3/10
  channel-group 10 mode active

interface Ethernet3/11
  channel-group 10 mode active

interface port-channel1
  no switchport
  no shutdown
router bgp 65000
  address-family l2vpn evpn
vrf VRF-A
  address-family ipv4 unicast
  advertise l2vpn evpn
  redistribute direct route-map FABRIC-RMAP-REDIST-SUBNET
  redistribute ospf OSPF-10 route-map REDIST-DEF-ROUTE ## redistribute default route from OSPF into VRF-A
  maximum-paths ibgp 2
vrf VRF-B
  address-family ipv4 unicast
  advertise l2vpn evpn
  redistribute direct route-map FABRIC-RMAP-REDIST-SUBNET
  redistribute ospf OSPF-10 route-map REDIST-DEF-ROUTE ## redistribute default route from OSPF into VRF-B
  maximum-paths ibgp 2
vrf VRF-EXT
  address-family ipv4 unicast
  advertise l2vpn evpn
  redistribute direct route-map FABRIC-RMAP-REDIST-SUBNET
  redistribute ospf OSPF-10 route-map REDIST-DENY-DEFAULT ## redistribute VRF-A and VRF-B protected subnet prefixes from OSPF into VRF-EXT
  maximum-paths ibgp 2

router ospf OSPF-10 ## configuring per-VRF ospf routing protocol
vrf VRF-A
  redistribute bgp route-map REDIST-BGP-OSPF ## advertise VRF-A route prefixes to firewall
  router-id 10.10.10.10
vrf VRF-B
  redistribute bgp route-map REDIST-BGP-OSPF ## advertise VRF-A route prefixes to firewall
  router-id 10.10.10.10
vrf VRF-EXT
  redistribute bgp route-map REDIST-DEF-ROUTE ## advertise only default route to firewall
  router-id 10.10.10.10
Complex Deployment Scenarios

Often high-performance firewalls in routed mode combine two functions in one: tenant-edge firewall and east-west firewall. This approach allows the firewall both to present itself as a default gateway for a certain number of specific subnets and to enforce security policies for traffic forwarded between VRF instances, all in one firewall context (Figure 24).

**Figure 24.** Logical Diagram Showing a Single Tenant-Edge Firewall Acting as a Default Gateway for Subnets F1 and F2 as Well as Enforcing Security Policies between VRF A, VRF B, and VRF EXT
This section discusses the scenarios shown in Figures 25 and 26.

**Figure 25.** Single-Attached Tenant-Edge Firewalls in Routed Mode with Active-Standby Failover Dynamic Routing

![Diagram of Single-Attached Tenant-Edge Firewalls in Routed Mode with Dynamic Routing](image1)

**Figure 26.** vPC Dual-Attached Tenant-Edge Firewalls in Routed Mode with Clustering and Static Routing

![Diagram of vPC Dual-Attached Tenant-Edge Firewalls](image2)

**Active-Standby Failover: Single-Attached Tenant-Edge Firewalls in Routed Mode with Dynamic Routing and East-West Firewall Elements**

*Figure 27*, based on the logical diagram in *Figure 24*, shows the physical topology and the logical links between the border leaf nodes and the tenant-edge firewall units. Each firewall is connected to only one of the border leaf nodes using an IEEE 802.1Q trunk port channel. The arrows represent Layer 2 segments for respective subnets, and they reach all the way from the workloads to the firewalls.

Each active and standby firewall is connected with one logical link to each protected VRF instance. The green link shows Layer 3 OSPF routing protocol peering with VRF A, and the blue link shows Layer 3 OSPF routing protocol peering with VRF B. Depending on operating practices, the firewall may inject or relay a default route to VRF A and VRF B, making sure that it attracts any data traffic from the respective VRF instances destined for external networks.
Figure 27. Single-Attached Tenant-Edge Firewall Acting as a Default Gateway for Subnets F1 and F2 as Well as Enforcing Security Policies Among VRF A, VRF B, and VRF EXT. BORDER Leaf 1 and Border Leaf 2 Extend Layer 2 Segments for Subnets F1 and F2 to Both Firewalls

Configurations 11a and 11b apply to both border leaf nodes.

Note that anycast-gateway mode is not used for the SVI and BDI used to establish routing adjacency with the firewall. In addition, the IP addresses of the SVI and BDI for the respective VLANs must be different and on different border leaf nodes, but both interfaces must be in the same subnet.

Also, the route maps used for route redistribution may need to change, depending on the operating practices used. This document assumes that the firewall is sending the default route using OSPF.

Configuration 11a: IPVLAN-Based Leaf Switch

```plaintext
feature vn-segment-vlan-based
feature nv overlay
feature ospf  ## enable feature ospf

route-map FABRIC-RMAP-REDIST-SUBNET permit 10
    match tag 12345

ip access-list DEFAULT-ROUTE
    20 permit ip 0.0.0.0/0 any

ip access-list DENY-DEFAULT
    10 deny ip 0.0.0.0/0 any
    20 permit any any

route-map REDIST-DEF=ROUTE permit 10
    match ip address DEFAULT-ROUTE

route-map REDIST-DENY-DEFAULT permit 10
```
match ip address DENY-DEFAULT

route-map REDIST-BGP-OSPF permit 10

vlan 3001
  vn-segment 33001
vlan 3002
  vn-segment 33002
vlan 3500
  vn-segment 33500
vlan 201
  vn-segment 30201
vlan 202
  vn-segment 30202
vlan 2000
  vn-segment 50001
vlan 2001
  vn-segment 50002
vlan 2002
  vn-segment 50010

vrf context VRF-A  ## no static routes configured
  vni 50001
  rd auto
  address-family ipv4 unicast
    route-target both auto
    route-target both auto evpn

vrf context VRF-B  ## no static routes configured
  vni 50002
  rd auto
  address-family ipv4 unicast
    route-target both auto
    route-target both auto evpn

vrf context VRF-EXT  ## no static routes configured
  vni 50010
  rd auto
  address-family ipv4 unicast
    route-target both auto
    route-target both auto evpn

interface Vlan3001  ## regular (not anycast-gateway) SVI to establish routing adjacency with firewall
  no shutdown
  vrf member VRF-A
  ip address 10.10.231.1/24
    ip router ospf OSPF-10 area 0
interface Vlan3002  ## regular (not anycast-gateway) SVI to establish routing adjacency with firewall
    no shutdown
    vrf member VRF-B
    ip address 10.10.232.1/24
    ip router ospf OSPF-10 area 0

interface Vlan3500  ## regular (not anycast-gateway) SVI to establish routing adjacency with firewall
    no shutdown
    vrf member VRF-EXT
    ip address 10.10.235.1/24
    ip router ospf OSPF-10 area 0

interface Vlan2000
    no shutdown
    vrf member VRF-A
    no ip redirects
    ip forward
    ipv6 forward
    no ipv6 redirects

interface Vlan2001
    no shutdown
    vrf member VRF-B
    no ip redirects
    ip forward
    ipv6 forward
    no ipv6 redirects

interface Vlan2002
    no shutdown
    vrf member VRF-EXT
    no ip redirects
    ip forward
    ipv6 forward
    no ipv6 redirects

interface Ethernet1/25
    switchport mode trunk
    switchport trunk allowed vlan add 201-202,3001-3002,3500
    channel-group 10 mode active

interface Ethernet1/26
    switchport mode trunk
    switchport trunk allowed vlan add 201-202,3001-3002,3500
    channel-group 10 mode active
interface Port-channel 10
  switchport mode trunk
  switchport trunk allowed vlan add 201-202,3001-3002,3500

interface nve1
  host-reachability protocol bgp
  member vni 30201
    suppress-arp
    mcast-group 239.1.1.152
  member vni 30202
    suppress-arp
    mcast-group 239.1.1.152
  member vni 33001
    suppress-arp
    mcast-group 239.1.1.200
  member vni 33002
    suppress-arp
    mcast-group 239.1.1.201
  member vni 33500
    suppress-arp
    mcast-group 239.1.1.202
  member vni 50001 associate-vrf
  member vni 50002 associate-vrf
  member vni 50010 associate-vrf

router bgp 65000
  address-family l2vpn evpn
  vrf VRF-A
    address-family ipv4 unicast
    advertise l2vpn evpn
    redistribute direct route-map FABRIC-RMAP-REDIST-SUBNET
    redistribute ospf OSPF-10 route-map REDIST-DEF-ROUTE  ## redistribute default route from OSPF into VRF-A
      maximum-paths ibgp 2
  vrf VRF-B
    address-family ipv4 unicast
    advertise l2vpn evpn
    redistribute direct route-map FABRIC-RMAP-REDIST-SUBNET
    redistribute ospf OSPF-10 route-map REDIST-DEF-ROUTE  ## redistribute default route from OSPF into VRF-B
      maximum-paths ibgp 2
  vrf VRF-EXT
    address-family ipv4 unicast
    advertise l2vpn evpn
    redistribute direct route-map FABRIC-RMAP-REDIST-SUBNET
    redistribute ospf OSPF-10 route-map REDIST-DENY-DEFAULT  ## redistribute VRF-A and VRF-B protected subnet prefixes from OSPF into VRF-EXT
      maximum-paths ibgp 2
  evpn
    vni 30201 12
rd auto  
route-target import auto  
route-target export auto  
vni 30202 l2  
rd auto  
route-target import auto  
route-target export auto  
vni 33001 l2  
rd auto  
route-target import auto  
route-target export auto  
vni 33002 l2  
rd auto  
route-target import auto  
route-target export auto  
vni 33500 l2  
rd auto  
route-target import auto  
route-target export auto  

router ospf OSPF-10  
## configuring per-VRF ospf routing protocol  

<table>
<thead>
<tr>
<th>VRF</th>
<th>redistribute bgp route-map REDIST-BGP-OSPF</th>
<th>advertise VRF-A route prefixes to firewall</th>
</tr>
</thead>
<tbody>
<tr>
<td>VRF-A</td>
<td>router-id 10.10.10.10</td>
<td></td>
</tr>
<tr>
<td>VRF-B</td>
<td>router-id 10.10.10.10</td>
<td></td>
</tr>
<tr>
<td>VRF-EXT</td>
<td>router-id 10.10.10.10</td>
<td></td>
</tr>
</tbody>
</table>

Configuration 11b: IPBD-Based Leaf Switch

install feature-set fabric  
vdc leaf1 id 1  
allow feature-set fabric  
feature-set fabric  
feature nv overlay  
feature vni  
feature ospf  
## enable feature ospf  
nv overlay evpn  

route-map FABRIC-RMAP-REDIST-SUBNET permit 10  
match tag 12345  

ip access-list DEFAULT-ROUTE  
20 permit ip 0.0.0.0/0 any  

ip access-list DENY-DEFAULT  
10 deny ip 0.0.0.0/0 any  
20 permit any any
route-map REDIST-DEF-ROUTE permit 10
  match ip address DEFAULT-ROUTE

route-map REDIST-DENY-DEFAULT permit 10
  match ip address DENY-DEFAULT

route-map REDIST-BGP-OSPF permit 10

vni 30201
vni 30202
vni 33001
vni 33002
vni 33500
vni 50001
vni 50002
vni 50010

system bridge-domain 1500-1504,2500-2502

encapsulation profile vni VSI_to_VNI
  dotiq 3001=3002,201=202,3500 vni 33001=33002,30201=30202,33500

bridge-domain 1500-1504
  member vni 33001=33002,33500, 30201=30202

vrf context VRF-A
  vni 50001
  ip route 0.0.0.0/0 10.10.231.2
  rd auto
  address-family ipv4 unicast
    route-target both auto
    route-target both auto evpn

vrf context VRF-B
  vni 50002
  ip route 0.0.0.0/0 10.10.232.2
  rd auto
  address-family ipv4 unicast
    route-target both auto
    route-target both auto evpn

vrf context VRF-EXT
  vni 50010
  ip route 0.0.0.0/0 10.77.1.2
  ip route 10.10.101.0/24 10.10.235.5
  ip route 10.11.121.0/24 10.10.235.5
  rd auto
address-family ipv4 unicast
  route-target both auto
  route-target both auto evpn

interface Bdi1500
  vrf member VRF-A
  ip address 10.10.231.1/24  tag 12345

interface Bdi1501
  vrf member VRF-B
  ip address 10.10.232.1/24  tag 12345

interface Bdi1501
  vrf member VRF-EXT
  ip address 10.10.235.1/24  tag 12345

interface nve1
  host-reachability protocol bgp
  member vni 30201
    suppress-arp
    mcast-group 239.1.1.152
  member vni 30202
    suppress-arp
    mcast-group 239.1.1.152
  member vni 33001
    suppress-arp
    mcast-group 239.1.1.200
  member vni 33002
    suppress-arp
    mcast-group 239.1.1.201
  member vni 33500
    suppress-arp
    mcast-group 239.1.1.202
  member vni 50001 associate-vrf
  member vni 50002 associate-vrf
  member vni 50010 associate-vrf

interface Ethernet3/10
  channel-group 10 mode active

interface Ethernet3/11
  channel-group 10 mode active

interface port-channel1
  service instance 1 vni
  encapsulation profile VSI_to_VNI
router bgp 65000
  address-family l2vpn evpn
vrf VRF-A
  address-family ipv4 unicast
  advertise l2vpn evpn
  redistribute direct route-map FABRIC-RMAP-REDIST-SUBNET
  redistribute ospf OSPF-10 route-map REDIST-DEF-ROUTE  ## redistribute default route from OSPF into VRF-A
    maximum-paths ibgp 2
vrf VRF-B
  address-family ipv4 unicast
  advertise l2vpn evpn
  redistribute direct route-map FABRIC-RMAP-REDIST-SUBNET
  redistribute ospf OSPF-10 route-map REDIST-DEF-ROUTE  ## redistribute default route from OSPF into VRF-B
    maximum-paths ibgp 2
vrf VRF-EXT
  address-family ipv4 unicast
  advertise l2vpn evpn
  redistribute direct route-map FABRIC-RMAP-REDIST-SUBNET
  redistribute ospf OSPF-10 route-map REDIST-DENY-DEFAULT  ## redistribute VRF-A and VRF-B protected subnet prefixes from OSPF into VRF-EXT
    maximum-paths ibgp 2
evpn
  vni 30201 12
    rd auto
    route-target import auto
    route-target export auto
  vni 30202 12
    rd auto
    route-target import auto
    route-target export auto
  vni 33001 12
    rd auto
    route-target import auto
    route-target export auto
  vni 33002 12
    rd auto
    route-target import auto
    route-target export auto
  vni 33500 12
    rd auto
    route-target import auto
    route-target export auto

router ospf OSPF-10  ## configuring per-VRF ospf routing protocol
vrf VRF-A
  redistribute bgp route-map REDIST-BGP-OSPF  ## advertise VRF-A route prefixes to firewall
Clustered Mode: vPC Dual-Attached Tenant-Edge Firewalls in Routed Mode with Static Routing and East-West Firewall Elements

To increase their return on investment (ROI), many customers choose to deploy firewalls in clusters, in which each node actively forwards traffic, and all states are synchronized across cluster firewall members.

Such a scenario frequently requires dual-homed connection to two network switches, and in the case here, to two vPC leaf nodes. A general recommendation is to keep border leaf nodes deployed in standalone mode, so regular leaf nodes configured as vPC peers should be used for this scenario.

The physical diagram shown in Figure 26 closely resembles that of the previous scenario. However, now each firewall is vPC dual-attached to each of the leaf nodes. This scenario is based on the logical diagram shown in Figure 24.

In the current software, only static routing can be deployed with vPC dual-homed topology.

Just as in all previous cases with static routing, the SVIs and BDIs on the leaf nodes are configured in anycast-gateway mode.

This scenario assumes, that border leaf nodes are advertising default route (0.0.0.0/0) reachability in VRF EXT. This default route is then used by leaf 3 and leaf 4 to forward traffic to external networks outside VRF A and VRF B (Figure 28).

Figure 28. vPC Dual-Attached Cluster of Tenant-Edge Firewalls Acting as Default Gateways for Subnets F1 and F2 as Well as Enforcing Security Policies between VRF A, VRF B, and VRF EXT. Leaf 3 and Leaf 4 Are Extending Layer 2 Segments for Subnets F1 and F2 to Both Firewalls
Configuration 12a: IPVLAN-Based Leaf Switch

```plaintext
feature vn-segment-vlan-based
feature nv overlay

route-map FABRIC-RMAP-REDIST-SUBNET permit 10
  match tag 12345

ip access-list DEFAULT-ROUTE
  20 permit ip 0.0.0.0/0 any

ip access-list VRF-SUBNETS
  10 deny ip 0.0.0.0/0 any
  20 permit any any

route-map REDIST-DEF-ROUTE permit 10
  match ip address DEFAULT-ROUTE

route-map REDIST-VRF-SUBNETS permit 10
  match ip address VRF-SUBNETS

vlan 3001
  vn-segment 33001
vlan 3002
  vn-segment 33002
vlan 3500
  vn-segment 33500
vlan 201
  vn-segment 30201
vlan 202
  vn-segment 30202
vlan 2000
  vn-segment 50001
vlan 2001
  vn-segment 50002
vlan 2002
  vn-segment 50010

vrf context VRF-A
  vni 50001
  ip route 0.0.0.0/0 10.10.231.2
  rd auto
  address-family ipv4 unicast
    route-target both auto
    route-target both auto evpn

vrf context VRF-B
```

vrf context VRF-A
  vni 50001
  ip route 0.0.0.0/0 10.10.231.2
  rd auto
  address-family ipv4 unicast
    route-target both auto
    route-target both auto evpn

vrf context VRF-B
```
vni 50002
ip route 0.0.0.0/0 10.10.232.2 ## static default route to attract all egress traffic out of the VRF-B. Next-hop is Firewall.
rd auto
address-family ipv4 unicast
  route-target both auto
  route-target both auto evpn

vrf context VRF-EXT
vni 50010
ip route 10.10.101.0/24 10.10.235.5 ## static route to VLAN101 subnet in VRF-A. Next-hop is Firewall.
ip route 10.11.121.0/24 10.10.235.5 ## static route to VLAN1121 subnet in VRF-B. Next-hop is Firewall.
ip route 10.10.201.0/24 10.10.235.5 ## static route to VLAN201 subnet in VRF-B. Next-hop is Firewall.
ip route 10.10.202.0/24 10.10.235.5 ## static route to VLAN202 subnet in VRF-B. Next-hop is Firewall.
rd auto
address-family ipv4 unicast
  route-target both auto
  route-target both auto evpn

interface Vlan3001 ## interface, used for Layer-3 peering with fabric.
no shutdown
vrf member VRF-A
ip address 10.10.231.1/24  tag 12345
  fabric forwarding mode anycast-gateway ## enabling anycast-gateway mode

interface Vlan3002 ## interface, used for Layer-3 peering with fabric.
no shutdown
vrf member VRF-B
ip address 10.10.232.1/24  tag 12345
  fabric forwarding mode anycast-gateway ## enabling anycast-gateway mode

interface Vlan3500 ## interface, used for Layer-3 peering with fabric.
no shutdown
vrf member VRF-EXT
ip address 10.10.235.1/24  tag 12345
  fabric forwarding mode anycast-gateway ## enabling anycast-gateway mode

interface Vlan2000 ## interface, used as an L3 VRF VNI interface
no shutdown
vrf member VRF-A
no ip redirects
ip forward
ipv6 forward
no ipv6 redirects
interface Vlan2001  ## interface, used as an L3 VRF VNI interface
    no shutdown
    vrf member VRF-B
    no ip redirects
    ip forward
    ipv6 forward
    no ipv6 redirects

interface Vlan2002  ## interface, used as an L3 VRF VNI interface
    no shutdown
    vrf member VRF-EXT
    no ip redirects
    ip forward
    ipv6 forward
    no ipv6 redirects

interface Ethernet1/25  ## port-channel 10 member interface
    switchport mode trunk
    channel-group 10 mode active

interface Ethernet1/26  ## port-channel 10 member interface
    switchport mode trunk
    channel-group 10 mode active

interface Port-channel 10
    switchport mode trunk
    switchport trunk allowed vlan add 201-202,3001-3002,3500

interface nve1
    host-reachability protocol bgp
    member vni 30201
        suppress-arp
        mcast-group 239.1.1.211
    member vni 30202
        suppress-arp
        mcast-group 239.1.1.212
    member vni 33001
        suppress-arp
        mcast-group 239.1.1.200
    member vni 33002
        suppress-arp
        mcast-group 239.1.1.201
    member vni 33500
        suppress-arp
        mcast-group 239.1.1.202
    member vni 50001 associate-vrf
member vni 50002 associate-vrf
member vni 50010 associate-vrf

router bgp 65000
  address-family l2vpn evpn
  vrf VRF-A
    address-family ipv4 unicast
    advertise l2vpn evpn
    redistribute direct route-map FABRIC-RMAP-REDIST-SUBNET
    redistribute static route-map REDIST-DEF-ROUTE ## redistributing default route into VRF-A
    maximum-paths ibgp 2
  vrf VRF-B
    address-family ipv4 unicast
    advertise l2vpn evpn
    redistribute direct route-map FABRIC-RMAP-REDIST-SUBNET
    redistribute static route-map REDIST-DEF-ROUTE ## redistributing default route into VRF-B
    maximum-paths ibgp 2
  vrf VRF-EXT
    address-family ipv4 unicast
    advertise l2vpn evpn
    redistribute direct route-map FABRIC-RMAP-REDIST-SUBNET
    redistribute static route-map REDIST-DEF-ROUTE-SUBNETS ## redistributing routing reachability towards protected subnets in protected VRFs
    maximum-paths ibgp 2
  evpn
  vni 30201 12
    rd auto
    route-target import auto
    route-target export auto
  vni 30202 12
    rd auto
    route-target import auto
    route-target export auto
  vni 33001 12
    rd auto
    route-target import auto
    route-target export auto
  vni 33002 12
    rd auto
    route-target import auto
    route-target export auto
  vni 33500 12
    rd auto
    route-target import auto
    route-target export auto
Configuration 12b: IPBD-Based Leaf Switch

install feature-set fabric
vdc leaf1 id 1
  allow feature-set fabric
feature-set fabric
feature nv overlay
feature vni
nv overlay evpn

route-map FABRIC-RMAP-REDIST-SUBNET permit 10
  match tag 12345

ip access-list DEFAULT-ROUTE
  20 permit ip 0.0.0.0/0 any

ip access-list VRF-SUBNETS
  10 deny ip 0.0.0.0/0 any
  20 permit any any

route-map REDIST-DEF-ROUTE permit 10
  match ip address DEFAULT-ROUTE

route-map REDIST-VRF-SUBNETS permit 10
  match ip address VRF-SUBNETS

vni 30201
vni 30202
vni 33001
vni 33002
vni 33500
vni 50001
vni 50002
vni 50010

system bridge-domain 1500-1504,2500-2502  ## bridge domains, which will tie VNIs and VLANs together

encapsulation profile vni VSI_to_VNI  ## mapping VLANs to respective VNIs
  dot1q 3001-3002,201-202,3500 vni 33001-33002,30201-30202,33500

bridge-domain 1500-1504  ## mapping bridge-domains: 1500->33001, 1501->33002, 1502->33500
  member vni 33001-33002,30201-30202,33500

vrf context VRF-A
  vni 50001
  ip route 0.0.0.0/0 10.10.231.2  ## static default route to attract all egress traffic out of the VRF-A. Next-hop is Firewall.
rd auto
address-family ipv4 unicast
  route-target both auto
  route-target both auto evpn

vrf context VRF-B
  vni 50002
  ip route 0.0.0.0/0 10.10.232.2 ## static default route to attract all egress traffic out of the VRF-B. Next-hop is Firewall.
rd auto
address-family ipv4 unicast
  route-target both auto
  route-target both auto evpn

vrf context VRF-EXT
  vni 50010
  ip route 10.10.101.0/24 10.10.235.5 ## static route to VLAN101 subnet in VRF-A. Next-hop is Firewall.
ip route 10.11.121.0/24 10.10.235.5 ## static route to VLAN1121 subnet in VRF-A. Next-hop is Firewall.
ip route 10.10.201.0/24 10.10.235.5 ## static route to VLAN201 subnet in VRF-B. Next-hop is Firewall.
ip route 10.10.202.0/24 10.10.235.5 ## static route to VLAN202 subnet in VRF-B. Next-hop is Firewall.
rd auto
address-family ipv4 unicast
  route-target both auto
  route-target both auto evpn

interface Bdi1500
  vrf member VRF-A
  ip address 10.10.231.1/24  tag 12345
  fabric forwarding mode anycast-gateway ## enabling anycast-gateway mode

interface Bdi1501
  vrf member VRF-B
  ip address 10.10.232.1/24  tag 12345
  fabric forwarding mode anycast-gateway ## enabling anycast-gateway mode

interface Bdi1501
  vrf member VRF-EXT
  ip address 10.10.235.1/24  tag 12345
  fabric forwarding mode anycast-gateway ## enabling anycast-gateway mode

interface nve1 ## VTEP configuration
  host-reachability protocol bgp
  member vni 30201
  suppress-arp
  mcast-group 239.1.1.211
  member vni 30202
suppress-arp
mcast-group 239.1.1.212
member vni 33001
suppress-arp
mcast-group 239.1.1.200
member vni 33002
suppress-arp
mcast-group 239.1.1.201
member vni 33500
suppress-arp
mcast-group 239.1.1.202
member vni 50001 associate-vrf
member vni 50002 associate-vrf
member vni 50010 associate-vrf

interface Ethernet3/10  # configuring member of port-channel 10
channel-group 10 mode active

interface Ethernet3/11  # configuring member of port-channel 10
channel-group 10 mode active

interface port-channel1  # configuring port-channel 1/ vpc11 to active firewall node
service instance 1 vni
encapsulation profile VSI_to_VNI  # config for port-significant VLAN to VNI mapping

router bgp 65000
  address-family l2vpn evpn
  vrf VRF-A
    address-family ipv4 unicast
    advertise l2vpn evpn
    redistribute direct route-map FABRIC-RMAP-REDIST-SUBNET
    redistribute static route-map REDIST-DEF-ROUTE # redistributing default route into VRF-A
    maximum-paths ibgp 2
  vrf VRF-B
    address-family ipv4 unicast
    advertise l2vpn evpn
    redistribute direct route-map FABRIC-RMAP-REDIST-SUBNET
    redistribute static route-map REDIST-DEF-ROUTE # redistributing default route into VRF-B
    maximum-paths ibgp 2
  vrf VRF-EXT
    address-family ipv4 unicast
    advertise l2vpn evpn
    redistribute direct route-map FABRIC-RMAP-REDIST-SUBNET
    redistribute static route-map REDIST-DEF-ROUTE # redistributing routing reachability towards protected subnets in protected VRFs
maximum-paths ibgp 2
evpn
vni 30201 12
   rd auto
   route-target import auto
   route-target export auto
vni 30202 12
   rd auto
   route-target import auto
   route-target export auto
vni 33001 12
   rd auto
   route-target import auto
   route-target export auto
vni 33002 12
   rd auto
   route-target import auto
   route-target export auto
vni 33500 12
   rd auto
   route-target import auto
   route-target export auto

For More Information

- IETF Draft - BGP MPLS-based Ethernet VPN:
- IETF Draft - Network virtualization overlay solution with EVPN:
- IETF Draft - Integrated routing and bridging in EVPN:
- IETF Draft - IP prefix advertisement in EVPN:
- RFC 4271 - Border Gateway Protocol 4 (BGP-4):
- RFC 4760 - Multiprotocol extensions for BGP-4:
- RFC 4364 - BGP/MPLS IP VPNs:
- Cisco Nexus 9000 Series Switches: http://www.cisco.com/go/nexus9000
- Cisco Nexus 7000 Series Switches: http://www.cisco.com/go/nexus7000
- Cisco Nexus 5600 Series Switches: http://www.cisco.com/go/nexus5000