Hewlett Packard Enterprise

HPE IMC Orchestrator

Device Preprovisioning Guide

Document version: 5W100-20210426

Acknowledgments

Contents

Overview

The devices mentioned in this document refer to devices managed by the controller. To ensure the devices can correctly access the underlay network and the devices and the controller are reachable at Layer 3, you must preprovision the devices. This document describes how to preprovision devices in different scenarios. Then, you can manually preprovision devices by device type.

Depending on the carriers of devices, devices include the following types:

- Physical device—Devices carried on physical devices, for example, physical switches. Depending on the type of services provided, physical devices include physical access devices (L2VTEPs) and physical gateways. You must preprovision physical devices.
- Virtual device—Devices (for example, VNF devices and NGFW devices) virtualized on a physical server or physical network device (for example, M9000). Depending on the type of services provided, virtual devices include virtual gateway, virtual firewall, and virtual load balancer. Depending on how virtual devices are created, virtual devices include the following types:
  - **Manually added device**—Devices that are manually created and then manually added to the controller for management. You must preprovision this type of devices.
  - **Devices allocated by a resource pool**—Virtual devices allocated by the NGFW resource pool or VNF resource pool. When creating this type of devices, you must use the related template. Preprovisioned configuration is generated when the template is created. You do not need to preprovision this type of devices. You can learn the preprovisioned functions in the template through the configuration items described in "Configuration items." Also, you can modify the preprovisioned configuration in the template as needed.

Preprovisioning basic configuration

This chapter describes the configuration items and configuration tasks for devices of different types. The Configuration items section describes all possible functions for devices of different types. You can preprovision devices of the specified type according to the corresponding part in the Configuration tasks at a glance section. Also, you can learn which configuration items are preprovisioned in the templates for devices of different types.

Configuration tasks at a glance

Physical device configuration tasks at a glance

Task	Border devices
Enabling L2VPN	Y
Configuring local users and enabling the NETCONF service	Y
Configuring a routing protocol	Y
Configuring the management interface	Y
Configuring the interface where the VTEP IP address resides	Y
Configuring the interface where the DCI VTEP IP address resides on the border device	Y
Configuring an IBGP peer group for the border device	**Y**
Configuring the OVSDB VTEP function and site-facing interface	N
Reserving VLAN interface resources	Y
Assigning the physical interfaces connecting to the security devices to the same VLAN	Required only for border devices that are members of a service gateway group.
Configuring the IRF bridge MAC address to be permanent	Required only for border devices in IRF mode.

Manually added firewall configuration tasks at a glance

Task	Service-chain firewalls	Service gateway firewalls
Enabling L2VPN	N	N
Configuring local users and enabling the NETCONF service	Y	Y
Configuring a routing protocol	Y	Y
Configuring the management interface	Y	Y
Configuring the interface where the VTEP IP address resides	N	N
Configuring an IRF fabric	Required only for service-chain	Required only for service gateway

Task	Service-chain firewalls	Service gateway firewalls
Configuring track entries	firewalls in IRF mode.	firewalls in IRF mode.
Configuring redundancy groups		
Configuring stateful failover		
Configuring the IRF bridge MAC address to be permanent		
Configuring the firewall to permit traffic by default	Y	Y
Associating Track with NQA to monitor the primary and backup static routes	N	Required when multiple egresses are configured and SNAT is enabled.
Configuring the private line Reth interface	N	Y

Manually added load balancer configuration tasks at a glance

Task	Service-chain load balancers
Enabling L2VPN	N
Configuring local users and enabling the NETCONF service	Y
Configuring a routing protocol	Y
Configuring the management interface	Y
Configuring the interface where the VTEP IP address resides	N
Configuring an IRF fabric	Required only for service-chain load balancers in IRF mode.
Configuring track entries	
Configuring redundancy groups	
Configuring stateful failover	
Configuring the IRF bridge MAC address to be permanent	
Creating the interface where the vLB's virtual server IP resides	Y

Network cloud active/active gateway preconfiguration tasks at a glance

Task	Active/active EDs
Enabling L2VPN	Y
Configuring local users and enabling the NETCONF service	Y
Specifying the interface for BGP peer establishment	Y

Task	Active/active EDs
Configuring an fail-permit channel interface for active/active gateways	Y
Specifying the virtual VTEP address	Y
Configuring routing policies for active/active gateways	Y
Configuring asymmetric IRB	Y
Configuring the source IP address of BFD echo packets	Y
Configuring Router IDs	Y
Configuring OSPF	Y
Enabling packet statistics for VXLAN tunnels associated with L3 VXLAN IDs	Y
Enabling BGP to reset peer sessions gracefully	Y
Configuring optimal routes	Y
Configuring fail-permit for active/active gateways	Y
Configuring a virtual ED address	Y

Configuration items

Enabling L2VPN

Enable L2VPN on the device.

```
[Device] l2vpn enable
```

Configuring local users and enabling the NETCONF service

Create a local user named **sdn** and set the password to **123**.

To ensure security, the device needs to perform authentication and authorization for the connections initiated by the controller. Typically, local authentication and authorization are used in the current solution. Therefore, you need to create a local user and configure properties for the user.

```
[Device] local-user sdn
[Device-luser-manage-sdn] password simple 123
[Device-luser-manage-sdn] service-type ssh https
[Device-luser-manage-sdn] authorization-attribute user-role network-admin
```

Configure the device to communicate with the controller by using NETCONF over SSH channels.

```
[Device] ssh server enable
[Device] netconf ssh server enable
```

Configure the device to communicate with the controller by using NETCONF over HTTPS channels.

```
[Device] ip https enable
[Device] netconf soap https enable
```

Enable scheme authentication for VTY lines 0 through 63.

```
[Device] line vty 0 63
```

```
[Device-line-vty0-63] authentication-mode scheme
```

Configuring a routing protocol

IMPORTANT:

- You can select a routing protocol as needed. As a best practice, use OSPF.
- You must configure OSPF processes before enabling OSPF on an interface.
- When the device is a VNF device, IS-IS cannot be used.

Configure OSPF processes.

One process (for example, process 1) is used as the area for advertising the underlay network routes. The other process (for example, process 10) is used as the area for advertising the management network routes.

```
[Device] ospf 1
[Device] ospf 10
```

Configuring the management interface

IMPORTANT:

Reth 999 is reserved as the management interface of a device. Do not use this interface for any other purposes.

- For devices allocated by the resource pool (for example, VNF devices):
  - When the VNF operates in IRF mode: Create interface Reth 999 on the VNF in IRF mode. The IP address of the interface is allocated by the VNF manager. Add management interfaces on the two VNFs forming the IRF fabric (for example, GigabitEthernet 1/1/0 and GigabitEthernet 2/1/0) to Reth 999 as member interfaces. Add Reth 999 to the area for advertising the management network routes, for example, area 0 of OSPF process 10.

    ```
    [Device] interface Reth 999
    [Device-Reth999] member interface GigabitEthernet 1/1/0 priority 100
    [Device-Reth999] member interface GigabitEthernet 2/1/0 priority 80
    [Device-Reth999] ospf 10 area 0
    ```

  - When the VNF operates in standalone mode: The IP address of the management interface (for example, GigabitEthernet 1/1/0) is assigned by the VNF manager. Add the management interface to the area for advertising management network routes (for example, area 0 of OSPF process 10).

    ```
    [Device] interface GigabitEthernet 1/1/0
    [Device-GigabitEthernet1/1/0] ospf 10 area 0
    ```

- For physical devices and manually added virtual devices: Create the management interface (LoopBack 0 or another interface as needed) and configure an IP address for the interface. Add the interface to the area for advertising the management network routes (for example, area 0 of OSPF process 10).

  ```
  [Device] interface LoopBack 0
  [Device-LoopBack0] ip address 31.0.7.126 255.255.255.255
  [Device-LoopBack0] ospf 10 area 0
  ```

Configuring the interface where the VTEP IP address resides

IMPORTANT:

- Loopback 1 is reserved as the interface for configuring the VTEP IP address. Do not use this interface for any other purposes.
- The packets sent out of VMs are large and might be dropped because the MTU of an interface is too small during the forwarding process. As a practice, set a greater MTU size for the interface.

Perform this task to create the interface where the VTEP IP address resides. The VTEP IP address is deployed by the controller rather than manually configured. To ensure VTEP IPs are reachable at Layer 3, advertise the VTEP IP addresses and the addresses of underlay network interconnecting interfaces to the area for advertising underlay network routes.

Create Loopback 1 as the interface where the VTEP IP address resides. Add the interface to the area for advertising underlay network routes (for example, area 0 of OSPF process 1).

```
[Device] interface LoopBack 1
[Device-LoopBack1] ospf 1 area 0
```

Add all underlay network interconnecting interfaces (for example, Reth 2) to the area for advertising the underlay network routes (for example, area 0 of OSPF process 1). When the underlay network interconnecting interface is a physical interface, the configuration is similar.

On a device, the interface connected to the TOR switch or another device is an underlay network interconnecting interface. The IP addresses of the underlay network interconnecting interfaces are deployed by the VNF manager.

```
[Device] interface Reth 2
[Device-Reth2] member interface GigabitEthernet 1/4/0 priority 100
[Device-Reth2] member interface GigabitEthernet 2/4/0 priority 80
[Device-Reth2] mtu 9216
[Device-Reth2] ospf 1 area 0
```

Configuring the interface where the DCI VTEP IP address resides on the border device

IMPORTANT:

Perform this task before the border device comes online. After the border device comes online, the interface where the DCI VTEP IP addresses reside cannot be deleted or modified.

The DCI VTEP IP addresses are used for creating DCIs. You must manually create the interface where the DCI VTEP IP address resides and assign an IP address to the interface.

Create Loopback 2 as the interface where the DCI VTEP IP address resides, and assign an IP address to the interface.

```
[Device] interface LoopBack 2
[Device-LoopBack2] ip address 101.10.1.1 255.255.0.0
```

Configuring the external network VPN and the external network outgoing Reth interface

IMPORTANT:

- The VPN **external_vpn** is reserved as the external network VPN. Do not use this VPN for any other purposes.
- The interface Reth 1 is reserved as the external network egress interface or private line interface. Do not use this interface for any other purposes. If interface Reth 1 is already configured as the external network egress interface, you cannot configure cloud private line services on it.

(Applicable to VNF gateways and NGFW gateways.) The internal network traffic of the network managed by the controller is forwarded in a VPN. To make the internal network and external network communicate, you must create an external network VPN and add the external network egress interface to the VPN.

Create an external network VPN.

```
[Device] ip vpn-instance external_vpn
```

Configure the external network egress interface Reth1.

- When Reth1 connects to TOR switches through interfaces sending VLAN-tagged (for example, VLAN tag 2) packets, perform the following tasks:
  - Configure VLAN termination on the physical subinterfaces on the device.
  - Configure the physical subinterfaces (for example, GigabitEthernet 1/5/0.2 and GigabitEthernet 2/5/0.2) as the member interfaces of Reth1.

```
[Device] interface GigabitEthernet 1/5/0.2
[Device-GigabitEthernet1/5/0.2] vlan-type dot1q vid 2

[Device-GigabitEthernet1/5/0.2] interface GigabitEthernet 2/5/0.2
[Device-GigabitEthernet2/5/0.2] vlan-type dot1q vid 2

[Device-GigabitEthernet2/5/0.2] interface Reth 1
[Device-Reth1] member interface GigabitEthernet 1/5/0.2 priority 100
[Device-Reth1] member interface GigabitEthernet 2/5/0.2 priority 80
[Device-Reth1] ip binding vpn-instance external_vpn
```

- When Reth1 connects to a TOR switch through an interface sending untagged packets, configure the physical interfaces (for example, GigabitEthernet 1/5/0 and GigabitEthernet 2/5/0) as the member interfaces of Reth1.

```
[Device] interface Reth 1
[Device-Reth1] member interface GigabitEthernet 1/5/0 priority 100
[Device-Reth1] member interface GigabitEthernet 2/5/0 priority 80
[Device-Reth1] ip binding vpn-instance external_vpn
```

Specifying the interface for BGP peer establishment

BGP usually uses the interface configured with the VTEP IP for peer establishment. When two EDs are deployed and a virtual VTEP address is configured for the EDs, you must specify an independent interface for peer establishment.

```
[Device] interface LoopBack0
[Device-LoopBack0] ip address 1.1.1.1 255.255.255.255
[Device-LoopBack0] ospf 11 area 0.0.0.0
```

```
[Device] interface LoopBack0
[Device-LoopBack0] ip address 1.1.1.1 255.255.255.255
[Device-LoopBack0] ospfv3 11 area 0.0.0.0
[Device-LoopBack0] ipv6 address 1::1/128
```

Configuring an IBGP peer group for the border device

To use the vRouter link feature, add the other devices in the data center to IBGP peer group **evpn** when the firewall feature is disabled.

```
[Device] bgp 100
[Device-bgp-default] peer 195.0.0.241 group evpn
```

Configuring an fail-permit channel interface for active/active gateways

When two gateways are deployed in the network cloud scenario, you must configure an fail-permit channel interface to ensure continuous services when a single point of failure occurs.

- IPv4 network:

  ```
  [Device] interface Ten-GigabitEthernet2/0/19   (Enable MPLS and LDP on interface connecting GW1 and GW2.)
  [Device-Ten-GigabitEthernet2/0/19] port link-mode route
  [Device-Ten-GigabitEthernet2/0/19] ip address 22.0.0.1 255.255.255.0
  [Device-Ten-GigabitEthernet2/0/19] ospf 11 area 0.0.0.0
  [Device-Ten-GigabitEthernet2/0/19] mpls enable
  [Device-Ten-GigabitEthernet2/0/19] mpls ldp enable
  ```

- IPv6 network:

  ```
  [Device] interface Ten-GigabitEthernet2/0/19
  [Device-Ten-GigabitEthernet2/0/19] ospfv3 1 area 0.0.0.0
  [Device-Ten-GigabitEthernet2/0/19] ospfv3 network-type p2p
  [Device-Ten-GigabitEthernet2/0/19] mpls enable
  [Device-Ten-GigabitEthernet2/0/19] mpls ldp ipv6 enable
  [Device-Ten-GigabitEthernet2/0/19] mpls ldp transport-address 40:10::1
  [Device-Ten-GigabitEthernet2/0/19] ip forwarding
  [Device-Ten-GigabitEthernet2/0/19] ipv6 address 40:10::1/64
  ```

Specifying the virtual VTEP address

For high availability and load sharing, you can deploy two EDs at a data center. To virtualize the redundant EDs into one device, you must configure the same virtual VTEP address on them. The redundant EDs use the virtual VTEP address to establish tunnels with VTEPs and remote EDs.

As a best practice, configure the virtual VTEP address on the loopback interface.

- IPv4 network:

  ```
  [Device] interface LoopBack1
  [Device-LoopBack1] ip address 100.0.0.1 255.255.255.255
  [Device-LoopBack1] ospf 11 area 0.0.0.0
  ```

- IPv6 network:

  ```
  [Device] interface LoopBack1
  [Device-LoopBack1] ospfv3 11 area 0.0.0.0
  ```

```
[Device-LoopBack1] ipv6 address 11::11/128
```

Configuring an IRF fabric

(Applicable to VNF devices in IRF mode.) To improve availability for devices, you configure devices to operate in IRF mode.

Specify member IDs, priorities, and bind IRF ports to IRF physical interfaces for devices.

The data channel and the control channel must use different IRF physical interfaces.

```
[DeviceA] irf member 1
[DeviceA] irf member 1 priority 32
[DeviceA] irf-port 1
[DeviceA-irf-port1] port group interface GigabitEthernet1/2/0 type data
[DeviceA-irf-port1] port group interface GigabitEthernet1/3/0 type control

[DeviceB] irf member 2
[DeviceB] irf member 2 priority 31
[DeviceB] irf-port 2
[DeviceB-irf-port2] port group interface GigabitEthernet2/2/0 type data
[DeviceB-irf-port2] port group interface GigabitEthernet2/3/0 type control
```

Configuring track entries

Track entries are used for monitoring the status of the external network egress interfaces, downlink interfaces, and management interfaces.

NOTE:

You can modify interface names as needed. In this configuration example, GigabitEthernet 1/1/0 and GigabitEthernet 2/1/0 are used as the member interfaces of the management interface Reth 999, GigabitEthernet 1/4/0 and GigabitEthernet 2/4/0 are used as member interfaces of the downlink interface Reth2, and GigabitEthernet 1/5/0 and GigabitEthernet 2/5/0 are used as the member interfaces of the uplink interface Reth1.

(Applicable to VNF gateways and NGFW gateways.) Configure track entries to monitor the three types of interfaces on the virtual gateway.

The virtual gateway forwards internal network traffic at Layer 3 and implements communication between the internal network and external network.

```
[Device] track 1 interface GigabitEthernet 1/1/0
[Device] track 2 interface GigabitEthernet 1/4/0
[Device] track 3 interface GigabitEthernet 1/5/0
[Device] track 4 interface GigabitEthernet 2/1/0
[Device] track 5 interface GigabitEthernet 2/4/0
[Device] track 6 interface GigabitEthernet 2/5/0
```

(Applicable to service-chain vFWs and service-chain vLBs.) Configure track entries to monitor management interfaces and downlink interfaces.

The service-chain nodes forward traffic of the current service chain, and is not used for implementing communication between the internal network and external network. You do not need to monitor the external network egress interfaces.

```
[Device] track 1 interface GigabitEthernet 1/1/0
[Device] track 2 interface GigabitEthernet 1/5/0
```

```
[Device] track 3 interface GigabitEthernet 2/1/0
[Device] track 4 interface GigabitEthernet 2/5/0
```

Configuring redundancy groups

Redundancy groups are supported only in IRF mode. A redundancy group must contain two nodes, each of which is bound to an IRF member device. The two nodes implement device-level backup and ensure service packets are received, processed, and sent out on the same IRF member device.

NOTE:

The redundancy group names, interface names, and IRF member IDs can be modified as needed. For information about interfaces used in this example, see the note in "Configuring track entries."

(Applicable to VNF gateways and NGFW gateways.) Create node 1 as the primary node, bind the node to IRF member device 1, and associate it with track entries 1, 2, and 3. Create node 2 as the secondary node, bind the node to IRF member device 2, and associate it with track entries 4, 5, and 6.

When the uplink interface, downlink interface, or management interface of member device 1 fails or member device 1 fails, traffic is switched to member device 2. When the failure recovers, traffic is switched back to member device 1.

```
[Device] redundancy group reth
[Device-redundancy-group-reth] member interface Reth1
[Device-redundancy-group-reth] member interface Reth2
[Device-redundancy-group-reth] member interface Reth999

[Device-redundancy-group-reth] node 1
[Device-redundancy-group-right-node1] bind slot 1
[Device-redundancy-group-right-node1] priority 100
[Device-redundancy-group-right-node1] track 1 interface GigabitEthernet1/1/0
[Device-redundancy-group-right-node1] track 2 interface GigabitEthernet1/4/0
[Device-redundancy-group-right-node1] track 3 interface GigabitEthernet1/5/0
[Device-redundancy-group-right-node1] quit

[Device-redundancy-group-reth] node 2
[Device-redundancy-group-right-node2] bind slot 2
[Device-redundancy-group-right-node2] priority 80
[Device-redundancy-group-right-node2] track 4 interface GigabitEthernet2/1/0
[Device-redundancy-group-right-node2] track 5 interface GigabitEthernet2/4/0
[Device-redundancy-group-right-node2] track 6 interface GigabitEthernet2/5/0
```

(Applicable to service-chain vFWs and service-chain vLBs.) Create node 1 as the primary node, bind the node to IRF member device 1, and associate it with track entries 1 and 2. Create node 2 as the secondary node, bind the node to IRF member device 2, and associate it with track entries 3 and 4.

When the downlink interface or management interface of member device 1 fails or member device 1 fails, traffic is switched to member device 2. When the failure recovers, traffic is switched back to member device 1.

```
[Device] redundancy group reth
[Device-redundancy-group-reth] member interface Reth999
[Device-redundancy-group-reth] member interface Reth2
```

```
[Device-redundancy-group-reth] node 1
[Device-redundancy-group-right-node1] bind slot 1
[Device-redundancy-group-right-node1] priority 100
[Device-redundancy-group-right-node1] track 1 interface GigabitEthernet1/1/0
[Device-redundancy-group-right-node1] track 2 interface GigabitEthernet1/4/0
[Device-redundancy-group-right-node1] quit

[Device-redundancy-group-reth] node 2
[Device-redundancy-group-right-node2] bind slot 2
[Device-redundancy-group-right-node2] priority 80
[Device-redundancy-group-right-node2] track 3 interface GigabitEthernet2/1/0
[Device-redundancy-group-right-node2] track 4 interface GigabitEthernet2/4/0
```

Configuring stateful failover

When devices operate in IRF mode, you must configure stateful failover-related functions on the two virtual devices.

(Applicable to vFWs, vLBs, VNF gateways, and NGFW gateways.) Enable session synchronization.

```
[Device] session synchronization enable
```

(Applicable to VNF gateways and NGFW gateways.) Enable dynamic NAT444 service synchronization.

```
[Device] nat port-block synchronization enable
```

(Applicable to VNF gateways and NGFW gateways.) Enable IPsec redundancy.

```
[Device] ipsec redundancy enable
```

Creating the interface where the vLB's virtual server IP resides

IMPORTANT:

Loopback 127 is reserved as the interface where the virtual server IP resides. Do not use this interface for any other purposes.

The virtual server is a virtual carrier for user services on the load balancer. Only packets matching the virtual server can be processed by the load balancer.

(Applicable to vLBs.) Create interface Loopback 127, and use this interface to carry the virtual server IP address.

The virtual server IP address configured on the controller will be automatically deployed to the interface.

```
[Device] interface LoopBack 127
```

Configuring the firewall to permit traffic by default

IMPORTANT:

- The security zone **SDN_ZONE_DEFAULT** is reserved as the default SDN permit zone. Do not use this zone for any other purposes.
- The object policy **SDN_POLICY_DEFAULT** is reserved as the default SDN permit policy. Do not use this object policy for any other purposes.

Some firewalls (for example, vFWs created by the VNF manager or the vFWs virtualized on the M9K device) drop packets matching no security policies by default. As a result, the underlay network or management network might be unreachable.

Add the interfaces that permit traffic to the default SDN security zone, configure an object policy to permit traffic to pass through, and set the default action to **permit** for packets exchanged between interfaces in the same security zone.

Then, underlay data link packets and management packets are permitted, and the network is reachable.

```
[Device] security-zone name SDN_ZONE_DEFAULT
[Device-security-zone-SDN_ZONE_DEFAULT] import interface GigabitEthernet1/0
[Device-security-zone-SDN_ZONE_DEFAULT] import interface GigabitEthernet2/0
[Device-security-zone-SDN_ZONE_DEFAULT] import interface GigabitEthernet3/0
[Device-security-zone-SDN_ZONE_DEFAULT] import interface GigabitEthernet3/0.2
[Device-security-zone-SDN_ZONE_DEFAULT] quit

[Device] object-policy ip SDN_POLICY_DEFAULT
[Device-object-policy-ip-SDN_POLICY_DEFAULT] rule 0 pass
[Device-object-policy-ip-SDN_POLICY_DEFAULT] quit

[Device] security-zone intra-zone default permit

[Device] zone-pair security source any destination any
[Device-zone-pair-security-Any-Any] object-policy apply ip SDN_POLICY_DEFAULT
```

Configuring the OVSDB VTEP function and site-facing interface

Configure the OVSDB VTEP function on the physical access device (L2VTEP).

Then, the controller can automatically sense the online events of VMs or physical servers and learn ARP entries, so that the physical access device (L2VTEP) can run like a vSwitch.

```
[Device] ovsdb server ptcp port 6632
[Device] ovsdb server enable
[Device] vtep enable
```

Specify the site-facing interface as a VTEP access port.

The interface that connects the physical access device (L2VTEP) to a VM or physical server is a site-facing interface, for example, Ten-GigabitEthernet 2/0/5. To display and control the site-facing interface on the controller, you must specify the interface as a VTEP access port on the physical access device (L2VTEP).

```
[Device] interface Ten-GigabitEthernet2/0/5
[Device-Ten-GigabitEthernet2/0/5] vtep access port
```

Reserving VLAN interface resources

Because of the restrictions of the chips used in products (for example, the F series chips used in S12500-X switches), you must reserve VLAN interface resources before creating Layer 3 interfaces or subinterfaces other than VLAN interfaces or configuring features that use Layer 3 interface hardware resources.

Reserve global VLAN interface resources before creating VXLANs in VSI view when VXLAN tunnels operate in Layer 3 forwarding mode.

One global VLAN interface resource must be reserved for one VXLAN.

```
<Sysname> system-view
[Sysname] reserve-vlan-interface 3400 to 3500 global
```

Assigning the physical interfaces connecting to the security devices to the same VLAN

Perform this task when a service gateway group is used in the networking scheme,

Assign the physical interfaces (for example, GigabitEthernet 11/0/13) connecting service gateway group member devices to security devices (for example, firewalls and load balancers) to the same VLAN.

This configuration ensure the member devices and security devices can communicate at Layer 2.

```
[Device] interface GigabitEthernet 11/0/13
[Device-GigabitEthernet11/0/13] port link-mode bridge
[Device-GigabitEthernet11/0/13] port link-type trunk
[Device-GigabitEthernet11/0/13] port trunk permit vlan all
```

Activating the DPI feature on physical security devices

To deploy DPI services (for example, IPS, antivirus, and URL filtering) on firewall resources (contexts) virtualized from physical security devices, you must activate the DPI feature on these physical security devices. Otherwise, the controller cannot successfully deploy DPI service configurations to contexts on these devices.

Activate the DPI feature on physical security devices.

```
[Device] inspect activate
```

Configuring the IRF bridge MAC address to be permanent

Configure the IRF bridge MAC address to be permanent.

Perform this task when a device operates in IRF mode. The IRF bridge MAC address does not change after the address owner leaves the fabric.

```
[Device] irf mac-address persistent always
```

Associating Track with NQA to monitor the primary and backup static routes

Associate Track with NQA to monitor static routes and enable automatic switchover between the primary and backup static routes.

Create an NQA operation with administrator name **admin** and operation tag **test1**, and specify ICMP echo as the NQA operation type.

```
[Device] nqa entry admin test1
[Device-nqa-test-test] type icmp-echo
[Device-nqa-test-test-icmp-echo] destination ip 10.2.2.2
[Device-nqa-test-test-icmp-echo] frequency 1000
[Device-nqa-test-test-icmp-echo] reaction 1 checked-element probe-fail threshold-type consecutive 5 action-type trap-only
[Device-nqa-test-test-icmp-echo] vpn-instance external_vpn_22
[Device-nqa-test-test-icmp-echo] quit
[Device] nqa schedule test test start-time now lifetime forever
```

Create track entry 1 and associate it with reaction entry 1 of NQA operation admin-test.

```
[Device] track 1 nqa entry admin test reaction 1
```

Configuring the private line Reth interface

IMPORTANT:

The interface Reth 1 is reserved as the external network egress interface or private line interface. Do not use this interface for any other purposes. If interface Reth 1 is already configured as the private line interface, you cannot configure it as the external network egress interface.

(Applicable to service gateway firewalls.) Before configuring cloud private line services on IMC Orchestrator, you must manually configure the private line Reth interface on the firewall device.

VNF firewalls use interface Reth1 as the private line interface by default, and you cannot configure the private line interface for VNF firewalls through the VNFM resource template.

Create the default private line Reth interface.

```
[Device] interface Reth 1
```

Configuring routing policies for active/active gateways

1. Configure the community attribute to be advertised to vBGP.

   ```
   [Device] ip community-list 199 permit 2019:824
   ```

2. Advertise Type-2 and Type-3 EVPN routes that match the specified community attribute list.

   ```
   [Device] route-policy SDN_PREDEF_vbgp_suppress_policy permit node 0
   [Device-SDN_PREDEF_vbgp_suppress_policy-0] if-match community 199
   [Device-SDN_PREDEF_vbgp_suppress_policy-0] quit
   [Device] route-policy SDN_PREDEF_vbgp_suppress_policy permit node 1
   [Device-SDN_PREDEF_vbgp_suppress_policy-1] if-match route-type bgp-evpn-mac-ip
   [Device-SDN_PREDEF_vbgp_suppress_policy-1] quit
   [Device] route-policy SDN_PREFEF_vbgp_suppress_policy permit node 2
   [Device-SDN_PREDEF_vbgp_suppress_policy-2] if-match route-type bgp-evpn-imet
   [Device-SDN_PREDEF_vbgp_suppress_policy-2] quit
   ```

3. Advertise routes that match the routing policy to the BGP peer. This example uses IPv4 address 4.4.4.4 as example.

   ```
   [Device] bgp 100
   [Device-bgp-default] peer 4.4.4.4 as-number 100
   [Device-bgp-default] peer 4.4.4.4 connect-interface LoopBack1
   [Device-bgp-default] peer 4.4.4.4 graceful-restart timer restart extra no-limit
   ```

```
[Device-bgp-default] address-family l2vpn evpn
[Device-bgp-default-evpn] peer 4.4.4.4 route-policy SDN_PREDEF_vbgp_suppress_policy
export
[Device-bgp-default-evpn] peer 4.4.4.4 advertise-community
```

Configuring asymmetric IRB

In network cloud active/active gateway scenarios, configure asymmetric IRB on the gateways to enable the gateways to encapsulate VXLAN packets through L2VNI.

```
[Device] evpn irb asymmetric
```

Configuring the source IP address of BFD echo packets

As a best practice, do not configure the source IP address to be on the same network segment as any local interface's IP address. If you configure such a source IP address, a large number of ICMP redirect packets might be sent from the peer, resulting in link congestion.

As a best practice, configure different source IP addresses for the two gateways in network cloud active/active gateway scenarios.

- IPv4 network:

  ```
  [Device] bfd echo-source-ip 1.1.1.2
  ```

- IPv6 network:

  ```
  [Device] bfd echo-source-ipv6 1::2
  ```

Configuring Router IDs

In network cloud active/active gateway scenarios, you must manually specify different router IDs for the two gateways to avoid router ID conflict.

```
[Device] router id 1.1.1.1
[Device] bgp 100
[Device-bgp-default] router-id 1.1.1.1
```

Configuring OSPF

In network cloud active/active gateway scenarios, you must configure OSPF to implement underlay route failover.

- IPv4 network:

  ```
  [Device] ospf 11 router-id 1.1.1.1
  [Device-ospf-11] stub-router include-stub on-startup wait-for-bgp 1200
  [Device-ospf-11] fast-reroute lfa ecmp-shared
  [Device-ospf-11] area 0.0.0.0
  ```

- IPv6 network:

  ```
  [Device] ospfv3 11
  [Device-ospfv3-11] router-id 1.1.1.1
  [Device-ospfv3-11] non-stop-routing
  [Device-ospfv3-11] lsa-generation-interval 1 10 10
  [Device-ospfv3-11] spf-schedule-interval 1 10 10
  [Device-ospfv3-11] fast-reroute lfa
  [Device-ospfv3-11] stub-router r-bit on-startup wait-for-bgp 1200
  [Device-ospfv3-11] area 0.0.0.0
  ```

Enabling packet statistics for VXLAN tunnels associated with L3 VXLAN IDs

Enable packet statistics for VXLAN tunnels associated with L3 VXLAN IDs.

```
[Device] tunnel statistics vxlan auto
[Device] tunnel statistics vxlan l3-vni
[Device] l2vpn statistics interval 5
```

Enabling BGP to reset peer sessions gracefully

Enable BGP to reset peer sessions gracefully to ensure forwarding continuous when a routing protocol restarts or an active/standby switchover occurs.

```
[Device] bgp 100
[Device-bgp-default] graceful-restart
[Device-bgp-default] graceful-restart peer-reset all
```

Configuring optimal routes

Configure the BGP Additional Paths feature to enable BGP to advertise and receive multiple routes to perform load sharing.

```
[Device] bgp 100
[Device-bgp-default] address-family l2vpn evpn
[Device-bgp-default-evpn] additional-paths select-best 64
[Device-bgp-default-evpn] vpn-route cross multipath
[Device-bgp-default-evpn] peer 4.4.4.4 enable
[Device-bgp-default-evpn] peer 4.4.4.4 additional-paths receive send
[Device-bgp-default-evpn] peer 4.4.4.4 advertise additional-paths best 64
```

Configuring fail-permit for active/active gateways

1. Enable LDP for the gateways, and configure the gateways to advertise only VPNv4/VPNv6 next hop addresses to each other.
   - IPv4 network:

     ```
     [Device] ip prefix-list gw1-gw2 index 10 permit 1.1.1.1 32
     [Device] mpls lsr-id 1.1.1.1
     [Device] mpls ldp
     [Device-ldp] advertise-label prefix-list gw1-gw2
     ```
   - IPv6 network:

     ```
     [Device] ipv6 prefix-list gw1-gw2 index 20 permit 7::7 128
     [Device] mpls lsr-id 1.1.1.1
     [Device] mpls ldp
     [Device-ldp] ipv6 advertise-label prefix-list gw1-gw2
     ```
2. Configure routing policies to configure the gateways to not advertise default routes to each other to avoid routing loops.
   - IPv4 network:

     ```
     [Device] ip prefix-list SDN_PREFIXLIST_default index 10 permit 0.0.0.0 0
     [Device] route-policy SDN_PREDEF_dcgw_deny_IPv4_backup deny node 10
     ```

```
[Device-SDN_PREDEF_dcgw_deny_IPv4_backup-10] if-match ip address prefix-list
SDN_PREDEF_default
[Device-SDN_PREDEF_dcgw_deny_IPv4_backup-10] if-match tag 2019091122
[Device-SDN_PREDEF_dcgw_deny_IPv4_backup-10] quit
[Device] route-policy SDN_PREDEF_dcgw_deny_IPv4_backup permit node 20
```

- IPv6 network:

```
[Device] ipv6 prefix-list SDN_PREFIXLIST_default index 10 permit :: 0
[Device] route-policy SDN_PREDEF_dcgw_deny_IPv6_backup deny node 10
[Device-SDN_PREDEF_dcgw_deny_IPv6_backup-10] if-match ipv6 address prefix-list
SDN_PREDEF_default
[Device-SDN_PREDEF_dcgw_deny_IPv6_backup-10] if-match tag 2019091122
[Device-SDN_PREDEF_dcgw_deny_IPv6_backup-10] quit
[Device] route-policy SDN_PREDEF_dcgw_deny_IPv6_backup permit node 20
```

3. Configure the gateways to establish VPNv4 or VPNv6 peers with each other to implement route backup. This example uses IPv4 addresses as example.

```
[Device] bgp 100
[Device-bgp-default] flush suboptimal-route
[Device-bgp-default] labeled-route ignore-no-tunnel
[Device-bgp-default] peer 2.2.2.2 as-number 100
[Device-bgp-default] peer 2.2.2.2 connect-interface LoopBack0
[Device-bgp-default] address-family vpnv4
[Device-bgp-default-vpnv4] peer 2.2.2.2 enable
[Device-bgp-default-vpnv4] peer 2.2.2.2 route-policy
SDN_PREDEF_dcgw_deny_IPv4_backup export
[Device-bgp-default-vpnv4] address-family vpnv6
[Device-bgp-default-vpnv6] peer 2.2.2.2 enable
[Device-bgp-default-vpnv6] peer 2.2.2.2 route-policy
SDN_PREDEF_dcgw_deny_IPv6_backup export
```

Configuring a virtual ED address

For high availability and load sharing, you can deploy two EDs at a data center. To virtualize the redundant EDs into one device, you must configure the same virtual ED address on them. The redundant EDs use the virtual ED address to establish tunnels with VTEPs and remote EDs.

- IPv4 network:

```
[Device] evpn edge group 100.0.0.1
```

- IPv6 network:

```
[Device] evpn edge group 11::11
```

Configuration examples

Physical device preprovisioning

Border device

Local user and NETCONF configuration

```
[Device] local-user sdn
[Device-luser-manage-sdn] password simple 123
[Device-luser-manage-sdn] service-type ssh
[Device-luser-manage-sdn] authorization-attribute user-role network-admin

[Device] ssh server enable
[Device] netconf ssh server enable
[Device] ip https enable
[Device] netconf soap https enable

[Device] line vty 0 63
[Device-line-vty0-63] authentication-mode scheme
```

Underlay network configuration

```
[Device] l2vpn enable


[Device] ospf 1
[Device] ospf 10

[Device] interface LoopBack 0
[Device-LoopBack0] ip address 31.0.7.126 255.255.255.255
[Device-LoopBack0] ospf 10 area 0
[Device-LoopBack0] quit

[Device] interface GigabitEthernet 1/0/1
[Device-GigabitEthernet1/0/1] ip address 97.0.6.126 255.255.0.0
[Device-GigabitEthernet1/0/1] ospf 10 area 0
[Device-GigabitEthernet1/0/1] quit

[Device] interface LoopBack 1
[Device-LoopBack1] ospf 1 area 0
[Device-LoopBack1] quit

[Device] interface GigabitEthernet 2/0/1
[Device-GigabitEthernet2/0/1] ip address 111.0.9.126 255.255.0.0
[Device-GigabitEthernet2/0/1] mtu 9216
[Device-GigabitEthernet2/0/1] ospf 1 area 0
[Device-GigabitEthernet2/0/1] ospf cost 1
```

VNFM and NGFWM template configuration

When you use the VNF manager or NGFW manager to create devices of the specified type, the controller will deploy the preprovisioned configuration to devices according to the type of template used for creating the devices. This section describes the configuration deployed by the controller.

This section describes only the simplest configuration for devices to function. The deployed configuration might vary with the interfaces used for configuring templates.

VNFM 3.0 template

VNF gateway in standalone mode

```
ip vpn-instance external_vpn

interface GigabitEthernet 3/0.2
vlan-type dot1q vid 2

interface Reth 1
 member interface GigabitEthernet 3/0.2 priority 100
 ip binding vpn-instance external_vpn

ospf 1
ospf 10

interface LoopBack 0
 ospf 10 area 0

interface GigabitEthernet 1/0
 ospf 10 area 0

interface LoopBack 1
 ospf 1 area 0

interface GigabitEthernet 2/0
 mtu 9216
 ospf 1 area 0
```

VNF gateway in IRF mode

```
session synchronization enable
nat port-block synchronization enable
ipsec redundancy enable
ip vpn-instance external_vpn

interface GigabitEthernet 1/5/0.2
 vlan-type dot1q vid 2
interface GigabitEthernet 2/5/0.2
 vlan-type dot1q vid 2

interface Reth 1
```

```
 member interface GigabitEthernet 1/5/0.2 priority 100
 member interface GigabitEthernet 2/5/0.2 priority 80
 ip binding vpn-instance external_vpn

interface Reth2
 member interface GigabitEthernet 1/4/0 priority 100
 member interface GigabitEthernet 2/4/0 priority 80

track 1 interface GigabitEthernet 1/1/0
track 2 interface GigabitEthernet 1/4/0
track 3 interface GigabitEthernet 1/5/0
track 4 interface GigabitEthernet 2/1/0
track 5 interface GigabitEthernet 2/4/0
track 6 interface GigabitEthernet 2/5/0

redundancy group reth
 preempt-delay 0
 member interface Reth1
 member interface Reth2
 member interface Reth999

 node 1
  bind slot 1
  priority 100
  track 1 interface GigabitEthernet 1/1/0
  track 2 interface GigabitEthernet 1/4/0
  track 3 interface GigabitEthernet 1/5/0

node 2
  bind slot 2
  priority 80
  track 4 interface GigabitEthernet 2/1/0
  track 5 interface GigabitEthernet 2/4/0
  track 6 interface GigabitEthernet 2/5/0

ospf 1
 non-stop-routing

interface Reth2
 ospf 1 area 0
interface LoopBack 1
 ospf 1 area 0
interface LoopBack 127
interface Reth 2
 mtu 9216
```

Service-chain vFW in standalone mode

```
ospf 1
ospf 10
```

```
interface GigabitEthernet 1/0
 ospf 10 area 0

interface LoopBack 1
 ospf 1 area 0
interface GigabitEthernet 2/0
 mtu 9216
 ospf 1 area 0

security-zone name SDN_ZONE_DEFAULT
 import interface GigabitEthernet1/0
 import interface GigabitEthernet2/0
Object-policy ip SDN_POLICY_DEFAULT
 rule 0 pass

security-zone intra-zone default permit
zone-pair security source Any destination Any
 object-policy apply ip SDN_POLICY_DEFAULT
```

Service-chain vFW in IRF mode

```
session synchronization enable
interface Reth2
 member interface GigabitEthernet 1/4/0 priority 100
 member interface GigabitEthernet 2/4/0 priority 80

track 1 interface GigabitEthernet 1/1/0
track 2 interface GigabitEthernet 1/4/0
track 3 interface GigabitEthernet 2/1/0
track 4 interface GigabitEthernet 2/4/0

redundancy group reth
 preempt-delay 0
 member interface Reth2
 member interface Reth999

 node 1
  bind slot 1
  priority 100
  track 1 interface GigabitEthernet 1/1/0
  track 2 interface GigabitEthernet 1/4/0

 node 2
  bind slot 2
  priority 80
  track 3 interface GigabitEthernet 2/1/0
  track 4 interface GigabitEthernet 2/4/0

ospf 1
```

```
 non-stop-routing

interface Reth2
 ospf 1 area 0
interface LoopBack 1
 ospf 1 area 0
interface Reth2
 mtu 9216

security-zone name SDN_ZONE_DEFAULT
 import interface Reth2
 import interface Reth999
Object-policy ip SDN_POLICY_DEFAULT
 rule 0 pass
security-zone intra-zone default permit
zone-pair security source Any destination Any
 object-policy apply ip SDN_POLICY_DEFAULT
```

Service-chain vLB in IRF mode

```
session synchronization enable
interface Reth2
 member interface GigabitEthernet 1/4/0 priority 100
 member interface GigabitEthernet 2/4/0 priority 80
track 1 interface GigabitEthernet 1/1/0
track 2 interface GigabitEthernet 1/4/0
track 3 interface GigabitEthernet 2/1/0
track 4 interface GigabitEthernet 2/4/0
redundancy group reth
 preempt-delay 0
 member interface Reth2
 member interface Reth999

 node 1
  bind slot 1
  priority 100
  track 1 interface GigabitEthernet 1/1/0
  track 2 interface GigabitEthernet 1/4/0

 node 2
  bind slot 2
  priority 80
  track 3 interface GigabitEthernet 2/1/0
  track 4 interface GigabitEthernet 2/4/0

ospf 1
 non-stop-routing

interface Reth2
 ospf 1 area 0
```

```
interface LoopBack 1
 ospf 1 area 0
interface LoopBack 127
interface Reth2
  mtu 9216
```

Service-chain vLB in standalone mode

```
ospf 1
ospf 10

interface GigabitEthernet 1/0
 ospf 10 area 0

interface LoopBack 1
 ospf 1 area 0

interface GigabitEthernet 2/0
 mtu 9216
 ospf 1 area 0

interface LoopBack 127
```

NGFWM template

NGFW gateway

```
session synchronization enable
ip vpn-instance external_vpn
interface GigabitEthernet 3/0.2
 vlan-type dot1q vid 2
interface Reth 1
 member interface GigabitEthernet 3/0.2 priority 100
 ip binding vpn-instance external_vpn

ospf 1
ospf 10

interface GigabitEthernet 1/0
 ospf 10 area 0

interface LoopBack 1
 ospf 1 area 0

interface GigabitEthernet 2/0
 mtu 9216
 ospf 1 area 0
 ospf cost 1

security-zone name SDN_ZONE_DEFAULT
```

```
 import interface GigabitEthernet1/0
 import interface GigabitEthernet2/0
 import interface GigabitEthernet3/0
 import interface GigabitEthernet3/0.2

Object-policy ip SDN_POLICY_DEFAULT
 rule 0 pass

security-zone intra-zone default permit

zone-pair security source Any destination Any
 object-policy apply ip SDN_POLICY_DEFAULT
```

Service-chain vFW

```
session synchronization enable
nat port-block synchronization enable
ospf 1
ospf 10

interface GigabitEthernet 1/0
 ospf 10 area 0

interface LoopBack 1
 ospf 1 area 0
interface GigabitEthernet 2/0
 mtu 9216
 ospf 1 area 0

security-zone name SDN_ZONE_DEFAULT
 import interface GigabitEthernet1/0
 import interface GigabitEthernet2/0

Object-policy ip SDN_POLICY_DEFAULT
 rule 0 pass

security-zone intra-zone default permit

zone-pair security source Any destination Any
 object-policy apply ip SDN_POLICY_DEFAULT
```

Gateway service-type vFW

```
session synchronization enable
ipsec redundancy enable
nat port-block synchronization enable

ip vpn-instance external_vpn

ospf 1 vpn-instance external_vpn
 import-route direct
```

```
 import-route static
 area 0.0.0.0

interface LoopBack2
 ip binding vpn-instance external_vpn

interface Ten-GigabitEthernet2/0/4
 description internal

interface Ten-GigabitEthernet2/0/9
 description external
 ip binding vpn-instance external_vpn
 ospf 1 area 0.0.0.0

interface Ten-GigabitEthernet2/0/15
 description management

security-zone name SEC_ZONE_DEFAULT
 import interface Ten-GigabitEthernet2/0/15

object-policy ip SEC_POLICY_DEFAULT
 rule 0 pass

security-zone intra-zone default permit

zone-pair security source Any destination Any
 object-policy apply ip SEC_POLICY_DEFAULT

ip route-static 0.0.0.0 0 192.168.67.254
```

Service-chain vLB

```
session synchronization enable
nat port-block synchronization enable
session synchronization http
ospf 1
ospf 10

interface GigabitEthernet 1/0
 ospf 10 area 0

interface LoopBack 1
 ospf 1 area 0

interface GigabitEthernet 2/0
 mtu 9216
 ospf 1 area 0
 ospf cost 1

interface LoopBack 127
```

Gateway service-type vLB

```
session synchronization enable
nat port-block synchronization enable
session synchronization http

interface LoopBack127

interface GigabitEthernet1/0/1
 description management

interface Ten-GigabitEthernet1/0/26
 description internal

interface Ten-GigabitEthernet1/0/27
 description external

ip route-static 0.0.0.0 0 192.168.67.254
```

Preprovisioning manually added devices

Manually adding a firewall as a service chain node

Local user and NETCONF configuration

```
[Device] local-user sdn
[Device-luser-manage-sdn] password simple 123
[Device-luser-manage-sdn] service-type ssh
[Device-luser-manage-sdn] authorization-attribute user-role network-admin

[Device] ssh server enable
[Device] netconf ssh server enable

[Device] line vty 0 63
[Device-line-vty0-63] authentication-mode scheme
```

Underlay network configuration

```
[Device] l2vpn enable

[Device] ospf 1
[Device] ospf 10

[Device]interface LoopBack 0
[Device-LoopBack0] ip address 31.0.7.123 255.255.255.255
[Device-LoopBack0] ospf 10 area 0

[Device-LoopBack0] interface GigabitEthernet 1/0
[Device-GigabitEthernet1/0] ip address 97.0.6.126 255.255.0.0
[Device-GigabitEthernet1/0] ospf 10 area 0
```

```
[Device-GigabitEthernet1/0] interface LoopBack 1
[Device-LoopBack1] ip address 21.0.6.126 255.255.255.255
[Device-LoopBack1] ospf 1 area 0

[Device-LoopBack1] interface GigabitEthernet 2/0
[Device-GigabitEthernet2/0] ip address 111.0.9.125 255.255.0.0
[Device-GigabitEthernet2/0] mtu 9216
[Device-GigabitEthernet2/0] ospf 1 area 0
[Device-GigabitEthernet2/0] ospf cost 1
```

Security configuration

```
[Device] security-zone name SDN_ZONE_DEFAULT
[Device-security-zone-SDN_ZONE_DEFAULT] import interface GigabitEthernet1/0
[Device-security-zone-SDN_ZONE_DEFAULT] import interface GigabitEthernet2/0
[Device-security-zone-SDN_ZONE_DEFAULT] quit

[Device] Object-policy ip SDN_POLICY_DEFAULT
[Device-object-policy-ip-SDN_POLICY_DEFAULT] rule 0 pass
[Device-object-policy-ip-SDN_POLICY_DEFAULT] quit

[Device] security-zone intra-zone default permit

[Device] zone-pair security source any destination any
[Device-zone-pair-security-Any-Any] object-policy apply ip SDN_POLICY_DEFAULT
```

Manually adding a load balancer as a service chain node

Local user and NETCONF configuration

```
[Device] local-user sdn
[Device-luser-manage-sdn] password simple 123
[Device-luser-manage-sdn] service-type ssh
[Device-luser-manage-sdn] authorization-attribute user-role network-admin

[Device] ssh server enable
[Device] netconf ssh server enable

[Device] line vty 0 63
[Device-line-vty0-63] authentication-mode scheme
```

Underlay network configuration

```
[Device] l2vpn enable

[Device] ospf 1
[Device] ospf 10

[Device] interface LoopBack 0
[Device-LoopBack0] ip address 31.0.7.123 255.255.255.255
[Device-LoopBack0] ospf 10 area 0
```

```
[Device-LoopBack0] interface GigabitEthernet 1/0
[Device-GigabitEthernet1/0] ip address 97.0.6.126 255.255.0.0
[Device-GigabitEthernet1/0] ospf 10 area 0

[Device-GigabitEthernet1/0] interface LoopBack 1
[Device-LoopBack1] ospf 1 area 0

[Device-LoopBack1] interface GigabitEthernet 2/0
[Device-GigabitEthernet2/0] ip address 111.0.9.125 255.255.0.0
[Device-GigabitEthernet2/0] mtu 9216
[Device-GigabitEthernet2/0] ospf 1 area 0
[Device-GigabitEthernet2/0] ospf cost 1
```

Configuring the interface where the virtual server IP resides

```
[Device] interface LoopBack 127
```

Manually adding a VNF firewall as a VNF gateway

Local user and NETCONF configuration

```
[Device] local-user sdn
[Device-luser-manage-sdn] password simple 123
[Device-luser-manage-sdn] service-type ssh
[Device-luser-manage-sdn] authorization-attribute user-role network-admin

[Device] ssh server enable
[Device] netconf ssh server enable

[Device] line vty 0 63
[Device-line-vty0-63] authentication-mode scheme
```

Underlay network configuration

```
[Device] l2vpn enable

[Device] ip vpn-instance external_vpn
[Device] interface GigabitEthernet 3/0.2
[Device-GigabitEthernet3/0.2] vlan-type dot1q vid 2

[Device-GigabitEthernet3/0.2] interface Reth 1
[Device-Reth1] member interface GigabitEthernet 3/0.2 priority 100
[Device-Reth1] ip binding vpn-instance external_vpn
[Device-Reth1] quit

[Device] ospf 1
[Device] ospf 10
[Device] interface LoopBack 0
[Device-LoopBack0] ospf 10 area 0

[Device-LoopBack0] interface GigabitEthernet 1/0
```

```
[Device-GigabitEthernet1/0] ospf 10 area 0

[Device-GigabitEthernet1/0] interface LoopBack 1
[Device-LoopBack1] ospf 1 area 0

[Device-LoopBack1] interface GigabitEthernet 2/0
[Device-GigabitEthernet2/0] mtu 9216
[Device-GigabitEthernet2/0] ospf 1 area 0
[Device-GigabitEthernet2/0] ospf cost 1
```

Security configuration

```
[Device] security-zone name SDN_ZONE_DEFAULT
[Device-security-zone-SDN_ZONE_DEFAULT] import interface GigabitEthernet1/0
[Device-security-zone-SDN_ZONE_DEFAULT] import interface GigabitEthernet2/0
[Device-security-zone-SDN_ZONE_DEFAULT] import interface GigabitEthernet3/0
[Device-security-zone-SDN_ZONE_DEFAULT] import interface GigabitEthernet3/0.2
[Device-security-zone-SDN_ZONE_DEFAULT] quit

[Device] Object-policy ip SDN_POLICY_DEFAULT
[Device-object-policy-ip-SDN_POLICY_DEFAULT] rule 0 pass
[Device-object-policy-ip-SDN_POLICY_DEFAULT] quit

[Device] security-zone intra-zone default permit

[Device] zone-pair security source any destination any
[Device-zone-pair-security-Any-Any] object-policy apply ip SDN_POLICY_DEFAULT
```

Manually adding a VSR as a VNF gateway

Local user and NETCONF configuration

```
[Device] local-user sdn
[Device-luser-manage-sdn] password simple 123
[Device-luser-manage-sdn] service-type ssh
[Device-luser-manage-sdn] authorization-attribute user-role network-admin

[Device] ssh server enable
[Device] netconf ssh server enable

[Device] line vty 0 63
[Device-line-vty0-63] authentication-mode scheme
```

Underlay network configuration

```
[Device] l2vpn enable

[Device] ip vpn-instance external_vpn
[Device] interface GigabitEthernet 3/0.2
[Device-GigabitEthernet3/0.2] vlan-type dot1q vid 2
[Device-GigabitEthernet3/0.2] interface Reth 1
[Device-Reth1] member interface GigabitEthernet 3/0.2 priority 100
```

```
[Device-Reth1] ip binding vpn-instance external_vpn
[Device-Reth1] quit

[Device] ospf 1
[Device] ospf 10
[Device] interface LoopBack 0
[Device-LoopBack0] ospf 10 area 0

[Device-LoopBack0] interface GigabitEthernet 1/0
[Device-GigabitEthernet1/0] ospf 10 area 0

[Device-GigabitEthernet1/0] interface LoopBack 1
[Device-LoopBack1] ospf 1 area 0

[Device-LoopBack1] interface GigabitEthernet 2/0
[Device-GigabitEthernet2/0] mtu 9216
[Device-GigabitEthernet2/0] ospf 1 area 0
[Device-GigabitEthernet2/0] ospf cost 1
```

Manually adding bare-metal devices managed by NGFW manager

Local user and NETCONF configuration

```
[Device] local-user sdn
[Device-luser-manage-sdn] password simple 123
[Device-luser-manage-sdn] service-type ssh
[Device-luser-manage-sdn] authorization-attribute user-role network-admin

[Device] ssh server enable
[Device] netconf ssh server enable

[Device] line vty 0 63
[Device-line-vty0-63] authentication-mode scheme
```

Management interface and route configuration

Configure an IP address for the management interface, and configure a route to ensure the IP address and the controller IP address are reachable. (Details not shown.)