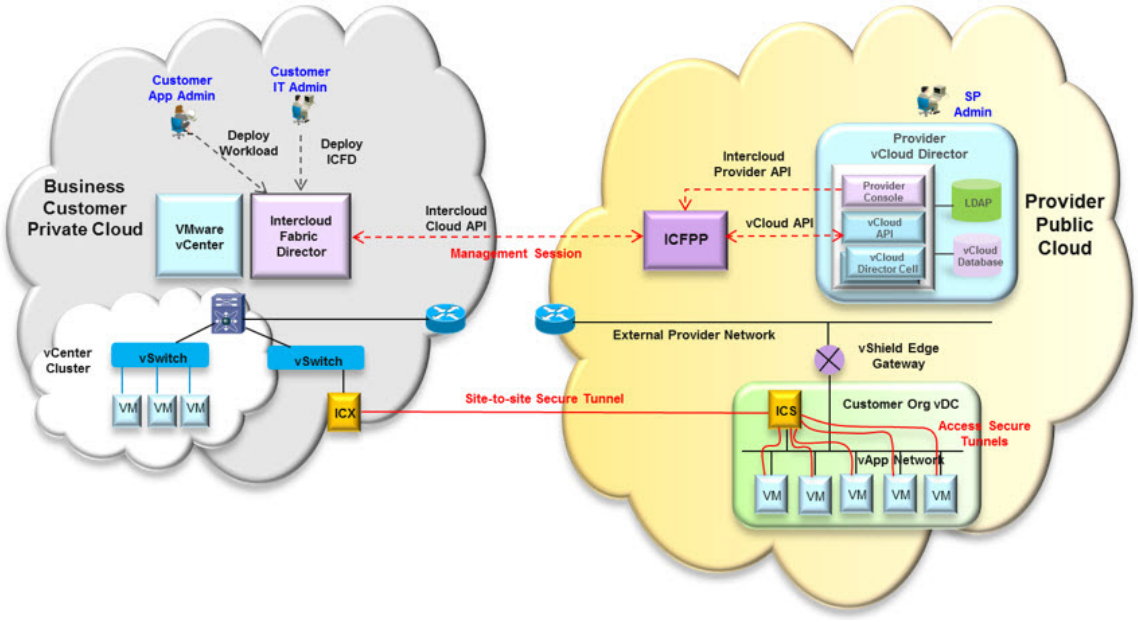
Configuring VMware vCloud Director for Cisco ICFPP

Configuring VMware vCloud Director

Installing Cisco ICFPP at a cloud provider site enables you to support a hybrid cloud environment with Cisco Intercloud Fabric for Business. For VMware vCloud Director (VCD) environments, Cisco ICFPP includes a built-in VCD adapter that enables Cisco ICFPP to integrate with the VCD platform. This VCD-Cisco ICFPP integration can be viewed as the infrastructure that binds the enterprise virtualization platform, such as VMware vCenter, to the provider cloud platform, VCD.

The following illustration depicts how Cisco Intercloud Fabric Director interfaces with the provider VCD platform through Cisco ICFPP.

Figure 1: VCD and Cisco Intercloud Fabric Integration Architecture



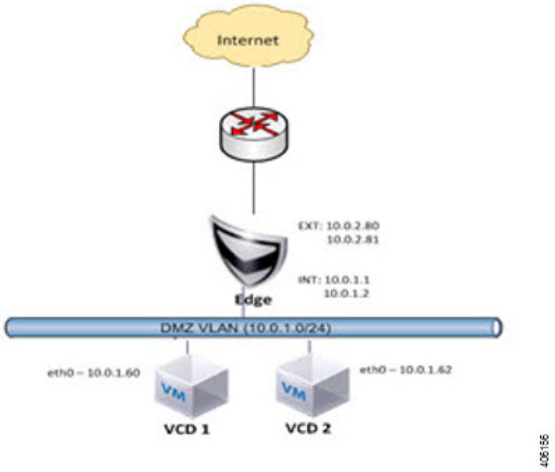
The secure site-to-site tunnel illustrated in the image is created between an Intercloud Fabric Switch (ICS) on the provider cloud and an Intercloud Fabric Extender (ICX) on the private cloud. In addition to providing secure communications between the private and provider clouds, this site-to-site tunnel enables Cisco Intercloud Fabric Secure Extender to integrate with VCD for each tenant network.

Before the ICS and ICX can communicate via the Internet, you must:

- Assign a public IP address to the ICS so that the ICX can reach the ICS.
- Ensure that the vShield Edge Gateway provides NAT functionality so that the ICS can connect to the Internet.

The following figure shows an example deployment:

Figure 2: vShield Edge Gateway Deployment Example

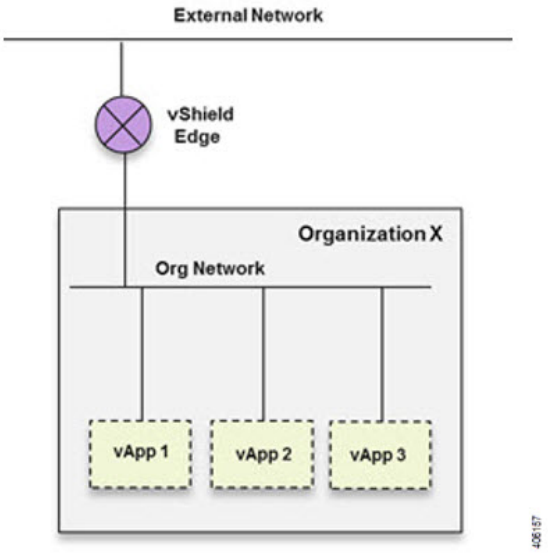


A vShield Edge Gateway is an interconnecting appliance which provides many edge network service features, including:

- NAT
- Firewall
- Load-balancer
- IPsec VPN
- DHCP
- Static route

The following figure shows how Organization X connects the Org Network to an external network through a vShield Edge Gateway and directly to vApp networks.

Figure 3: VCD Networking Model



Workflow for Integrating VCD with Cisco ICFPP

To integrate VCD with Cisco ICFPP, you must provision certain infrastructure resources in the target VCD platform. The following table identifies the tasks required to provision these resources:

Step	Task	Related Information
1.	Ensure that the following prerequisites are met: • VCD version 5.5 is installed. • You have access to the VCD system administrator account.	VMware VCD documentation
2.	Create an external network.	Creating an External Network, on page 5
3.	Deploy the vShield Edge Gateway.	Adding a vShield Edge Gateway on an Org VDC, on page 6
4.	Create an Org VDC network.	Creating an Org VDC Internal Network, on page 7
5.	Create a catalog.	Creating a Catalog, on page 9
6.	Ensure that NAT and firewall services are configured on the vShield Edge Gateway.	Verifying NAT and Firewall Service Configuration, on page 10

For additional information on any of these topics, see your VMware documentation.

Creating an External Network

This procedure describes how to create an external network in a virtual data center (VDC).

Procedure

Step 1 Log in to the VCD GUI as system administrator.

Step 2 Choose **System** > **Manage & Monitor** > **Cloud Resources** > **External Networks**.

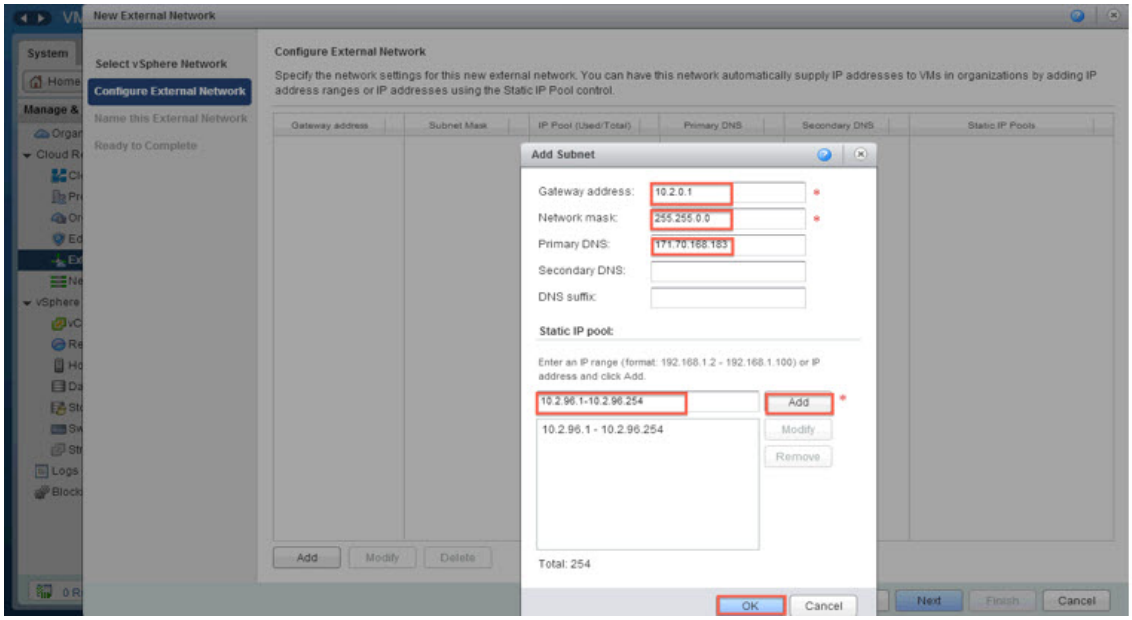
Step 3 In the **External Networks** pane, click **Add**.
The **New External Network** wizard opens, guiding you through the configuration process.

Step 4 In the **Select vSphere Network** screen, choose the VDC vCenter and the DVS port group created for the vSphere management network, and click **Next**.

Step 5 In the **Configure External Network** screen, click **Add**.

Step 6 In the **Add Subnet** dialog box, enter the following information for the external network:

- Gateway IP address
- Network mask
- DNS server IP address
- Static IP address or IP address range



Step 7 In the **Name this External Network** screen, enter a name for the external network, and click **Next**.

Step 8 In the **Ready to Complete** screen, review the content for accuracy and click **Finish**.
The newly created external network is displayed in the **External Networks** pane.

Adding a vShield Edge Gateway on an Org VDC

You must add a vShield Edge Gateway to integrate the Provider VDC and Org VDC with Cisco ICFPP.

Before You Begin

Confirm that the following have been configured:

- A Provider VDC
- An Org VDC
- An external network

Procedure

Step 1 In the VCD GUI, choose **System** > **Manage & Monitor** > **Cloud Resources** > **Organization VDCs**.

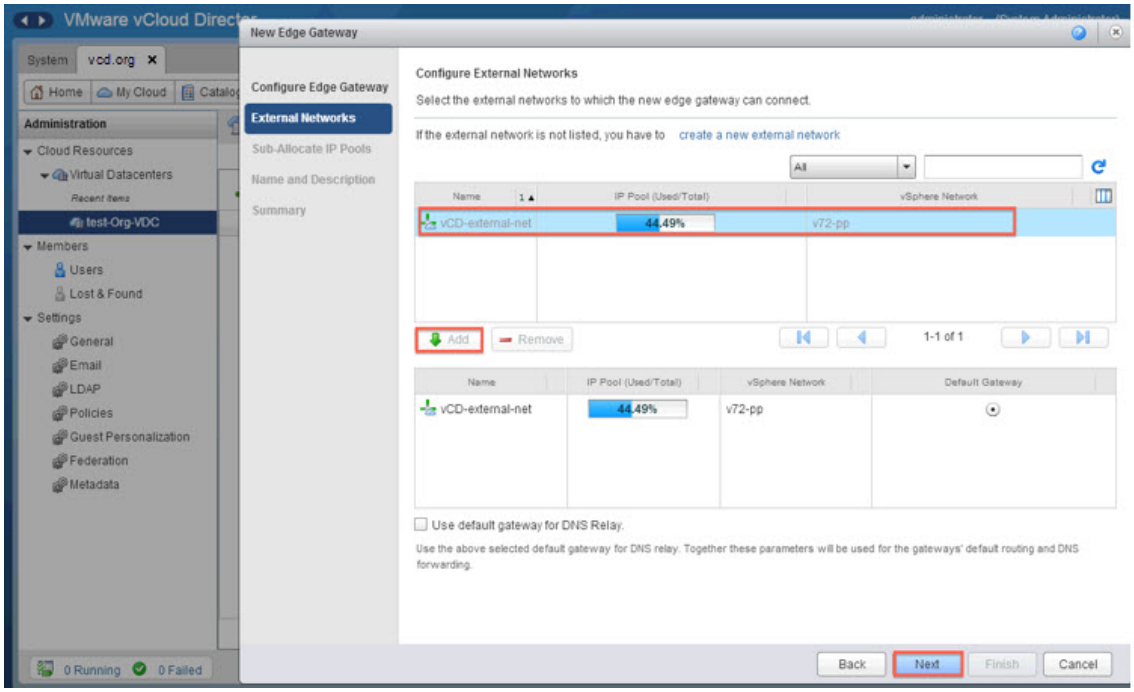
Step 2 In the **Organization VDCs** table, double-click the Org VDC where the vShield Edge Gateway is to be added.
The screen is refreshed with information about the selected VDC.

Step 3 Choose the **Edge Gateways** tab and click **Add**.
The **New Edge Gateway** wizard opens, guiding you through the configuration process.

Step 4 In the **Configure Edge Gateway** screen, configure the vShield Edge Gateway for connectivity with the external network as follows, and then click **Next**:

a) Choose the required edge gateway configuration: Compact, Full, or Full-4.
b) If the edge gateway is to be configured for HA, check the **Enable High Availability** check box.
c) In the **Advanced Options** section, check the **Sub-Allocate IP Pools** check box.

Step 5 In the **External Networks** screen, choose the external network that you created in Creating an External Network, on page 5 and click **Add**. If the external network is not listed, create a new external network.



Step 6 After the external network is added to the list of networks in the lower portion of the screen, click **Next**.

Step 7 In the **Sub-Allocate IP Pools** screen, identify the range of IP addresses allocated for each externally-connected interface on the external network, and click **Next**.

Step 8 In the **Name and Description** screen, enter the edge gateway name and description, and then click **Next**.

Step 9 In the **Summary** screen, review the information for accuracy and click **Finish**.

Creating an Org VDC Internal Network

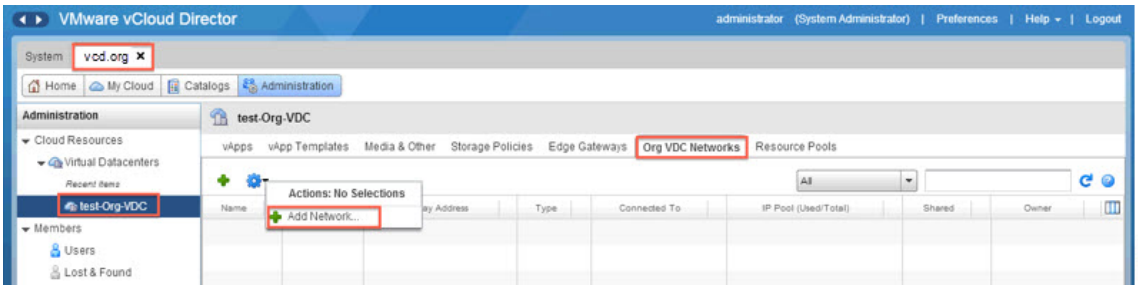
Use this procedure to create an internal network for the Org VDC.

Procedure

Step 1 In the VCD GUI, choose **System** > **Manage & Monitor** > **Cloud Resources** > **Organization VDCs**.

Step 2 In the **Organization VDCs** table, double-click the Org VDC where you want to create the internal network. The screen is refreshed with information about the selected VDC.

Step 3 In the **Org VDC Networks** tab, in the toolbar, choose **Actions** > **Add Network**.

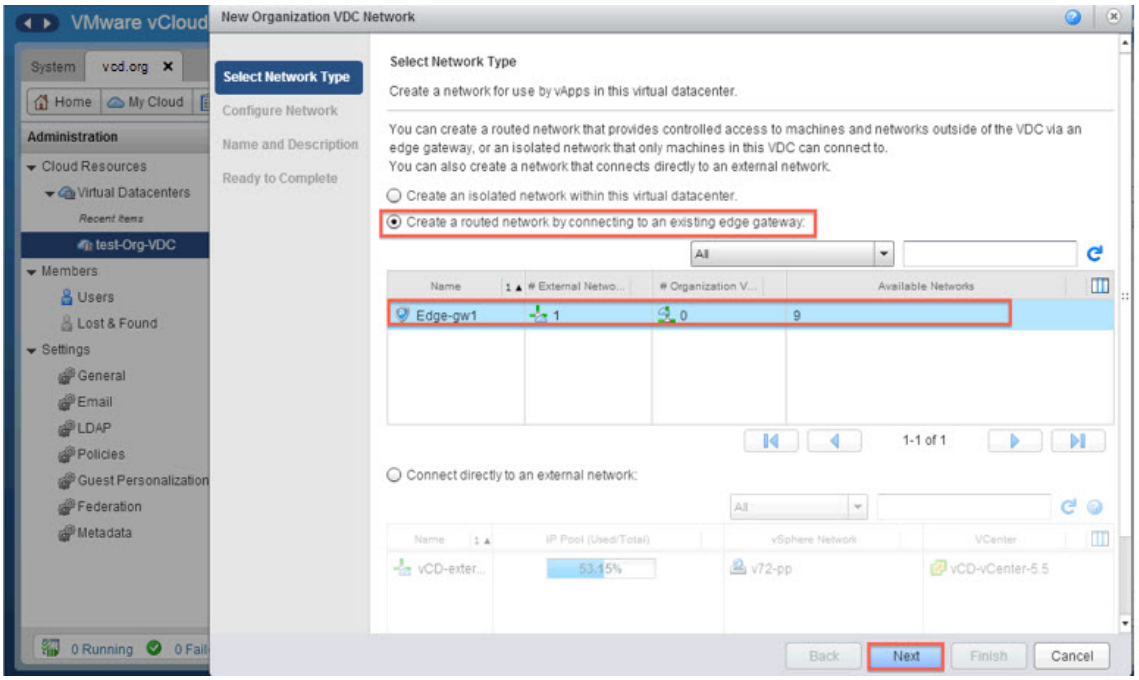


The **New Organization Network** wizard opens, guiding you through the configuration process.

Step 4 In the **Select Network Type** screen:

a) Choose **Create a routed network by connecting to an existing edge gateway**.

b) Choose the vShield Edge Gateway that you created in Adding a vShield Edge Gateway on an Org VDC, on page 6.



Step 5 In the **Configure Network** screen:

a) Enter the following information:

- Gateway IP address
- Network mask
- DNS server IP address

b) In the Static IP pool area, enter an IP address or an IP address range and click **Add**.

Step 6 In the **Name and Description** screen, enter a name and description (optional) for the Org VDC internal network.

Step 7 In the **Ready to Complete** screen, review the information for accuracy and click **Finish**.

Creating a Catalog

A catalog enables you to upload images from Cisco ICFPP to VCD.

For additional information about creating catalogs and selecting options, see your VMware vCloud Director documentation.

Before You Begin

Procedure

Step 1 In the VCD GUI, choose **System** > **Manage & Monitor** > **Cloud Resources** > **Organization VDCs**.

Step 2 In the **Organization VDCs** table, double-click the Org VDC in which to add the catalog.
The screen is refreshed with information about the selected VDC.

Step 3 Choose the **Catalogs** tab and, in the toolbar, choose **Actions** > **Add Catalog**.
A dialog box opens with multiple tabs so that you can configure the catalog and user access.

Step 4 In the **General** tab, enter a name and a description (optional) for the catalog.

Step 5 In the **Sharing** tab:

a) Click **Add Members**.

b) Choose the users or groups of users who can access the catalog.

c) In the **Access Level** field, choose the level of access for each user or group of users: Read-only, Read/Write, or Full Control.

Step 6 In the **Storage** tab, choose the type of storage.

Step 7 In the **Metadata** tab:

a) From the **Type** drop-down list, choose the metadata type.

b) In the **Name** field, enter a name for this metadata entry.

c) In the **User access of metadata** field, choose the level of access for the metadata: Read/Write, Read-only, or Hidden.

d) In the **Value** field, enter a text value for the metadata entry.

Step 8 After you have configured the catalog, click **OK**.

Verifying NAT and Firewall Service Configuration

When VCD is integrated with Cisco ICFPP, NAT and firewall services are configured automatically, enabling the vShield Edge Gateway to communicate with the external network. This procedure enables you to confirm that NAT and firewall services have been configured on the vShield Edge Gateway as expected.

Procedure

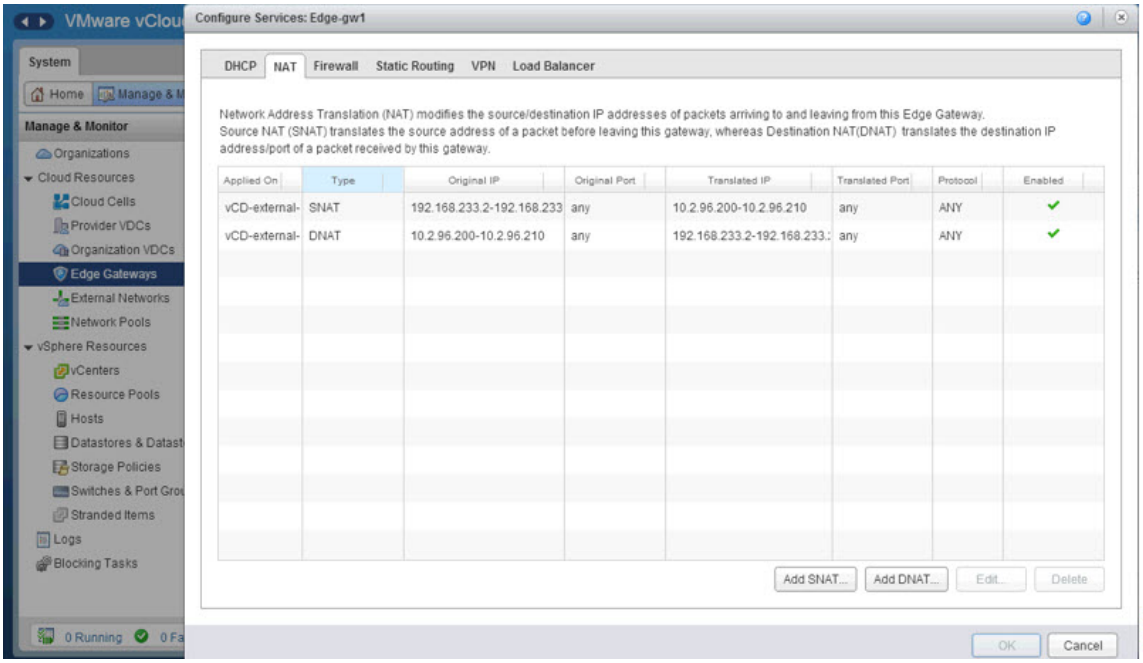
Step 1 In the VCD GUI, choose **System** > **Manage & Monitor** > **Cloud Resources** > **Organization VDCs**.

Step 2 In the **Organization VDCs** table, double-click the Org VDC where you created the vShield Edge Gateway (Adding a vShield Edge Gateway on an Org VDC, on page 6).
The screen is refreshed with information about the selected VDC.

Step 3 In the **Edge Gateways** tab, right-click the required edge gateway and choose **Edge Gateway Services**.

Step 4 In the Configure Services dialog box, confirm the following:

a) In the NAT tab, confirm that Source NAT and Destination NAT rules are displayed, as shown in the following example:



b) In the Firewall tab, confirm that inbound traffic is allowed for the following destination ports and protocols:

- 22—TCP
- 443—TCP
- 500—TCP, UDP
- 4500—TCP, UDP
- 6644—TCP, UDP

• 6646—TCP, UDP

The information should resemble the following example: