This document supports the version of each product listed and supports all subsequent versions until the document is replaced by a new edition. To check for more recent editions of this document, see http://www.vmware.com/support/pubs.
You can find the most up-to-date technical documentation on the VMware Web site at:
http://www.vmware.com/support/
The VMware Web site also provides the latest product updates.
If you have comments about this documentation, submit your feedback to:
docfeedback@vmware.com
Contents

About this Networking Guide 5

1 Overview of Gateways and Networks 7
   Network Virtualization in Virtual Private Cloud OnDemand 7
   Default Setup for Gateways and Networks 8
   Allocation of IP Addresses 11
   About Networking Services for Gateways 12
   Network Address Translation (NAT) 13
   DHCP 14
   Load Balancer 15
   DNS 16
   Static Routing 17

2 About Managing Gateways and Networks 19
   View Networks in a Virtual Data Center 19
   Add a Network to a Virtual Data Center 20
   View and Edit Gateway Details 21
   Add a Network to a Gateway 22
   Delete a Network 22
   Add a NAT Rule 23
   Allocate Public IP Addresses 25

3 Network Security and Secure Access 27
   About Network Security 27
   About Firewall Rules 29
   Add a Firewall Rule 29
   VPN and Remote Networks 30
   About IPsec VPN 31
   About Setting up an IPsec VPN Connection 31
   Set up an IPsec VPN Connection to a Remote Site 33
   SSL VPN for Data Center Extension 34

4 Network Connectivity for Virtual Machines 37
   Connect a Virtual Machine to a Network 38
   Change Network Assignments for a Virtual Machine 38
   Connect a Virtual Machine to the Internet 39

Index 41
About this Networking Guide

The vCloud Air – Virtual Private Cloud OnDemand Networking Guide provides information about configuring networking and gateways for VMware® vCloud Air – Virtual Private Cloud OnDemand, including how to add networks to gateways, set up network security by using the gateway’s networking services, and configure networking for virtual machines.

Additionally, this guide describes how to set up secure access to Virtual Private Cloud OnDemand from remote sites.

Intended Audience

This guide is intended for network administrators and virtual administrators who will be configuring networking in Virtual Private Cloud OnDemand. The information is written for experienced administrators who are familiar with virtual machine technology and networking concepts.

Related Documentation

See the following related documentation as part of understanding network configuration for Virtual Private Cloud OnDemand:


- See vCloud Director Administrator’s Guide for information about performing tasks affecting Virtual Private Cloud OnDemand by using vCloud Director.

Additionally, this guide provides in context cross-references to related information for the topics.

VMware Technical Publications Glossary

VMware Technical Publications provides a glossary of terms that might be unfamiliar to you. For definitions of terms as they are used in VMware technical documentation, go to http://www.vmware.com/support/pubs.
Overview of Gateways and Networks

Virtual Private Cloud OnDemand networking replicates traditional network technologies and design. Virtual Private Cloud OnDemand utilizes the software-defined networking (SDN) technologies used by VMware products, including VMware vSphere, VXLAN, vCloud Networking and Security, and vCloud Director.

This chapter includes the following topics:

- “Network Virtualization in Virtual Private Cloud OnDemand,” on page 7
- “Default Setup for Gateways and Networks,” on page 8
- “Allocation of IP Addresses,” on page 11
- “About Networking Services for Gateways,” on page 12
- “Network Address Translation (NAT),” on page 13
- “DHCP,” on page 14
- “Load Balancer,” on page 15
- “DNS,” on page 16
- “Static Routing,” on page 17

Network Virtualization in Virtual Private Cloud OnDemand

Network virtualization in Virtual Private Cloud OnDemand provides the ability to extend your virtual machines in your private cloud to the VMware public cloud.

The following VMware products and solutions work together to provide the network virtualization and features in Virtual Private Cloud OnDemand.

Figure 1-1. VMware Products and Solutions Providing Networking Functions in Virtual Private Cloud OnDemand
vSphere is the foundation on which Virtual Private Cloud OnDemand is built. On top of vSphere, Virtual eXtensible Local Area Network (VXLAN), part of VMware vCloud Networking and Security, provides the functions necessary to implement a flexible virtual network in the data center. VXLAN—dynamic and encapsulated—provides the ability to deploy networks in Virtual Private Cloud OnDemand rather than requiring complex VLAN architectures. VXLAN technology allows compute resources to be pooled across non-contiguous clusters and segmented into logical networks attached to applications. VXLAN allows for full encapsulation at Layer 2, providing network security. Also part of vCloud Networking and Security, the gateway virtual appliance enables networking services, such as the firewall, NAT, load balancer, and a VPN endpoint.

The Virtual Private Cloud OnDemand Web UI is the primary portal for managing gateways and networks. Additionally, you can use vCloud Director to manage your gateways and networks at a more detailed level. The Virtual Private Cloud OnDemand Web UI provides single sign-on access to vCloud Director.

**Capacity for Gateways and Networks**

Gateways and networks in Virtual Private Cloud OnDemand are subject to the following capacity limitations:

<table>
<thead>
<tr>
<th>Resource</th>
<th>Limit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum gateways/Virtual Data Center</td>
<td>1</td>
</tr>
<tr>
<td>Routed Networks/Gateway</td>
<td>9</td>
</tr>
<tr>
<td>Isolated Networks/Gateway</td>
<td>Unlimited</td>
</tr>
<tr>
<td>Networks/Virtual Data Center</td>
<td>20</td>
</tr>
<tr>
<td>Virtual NICs/Virtual Data Center</td>
<td>100</td>
</tr>
<tr>
<td>Network Objects/Virtual Data Center</td>
<td>100</td>
</tr>
<tr>
<td>Public IP Addresses/Virtual Data Center</td>
<td>5</td>
</tr>
<tr>
<td>Public IP Addresses/Customer</td>
<td>20</td>
</tr>
</tbody>
</table>

When you reach your capacity and resource limits, file a support request. Log into My VMware to file support requests for Virtual Private Cloud OnDemand.

See **Account Support** in *vCloud Air – Virtual Private Cloud OnDemand Getting Started* for information.

See also the My VMware Help (href) for information.

**Default Setup for Gateways and Networks**

Virtual data centers use the VMware vCloud Networking and Security Edge Gateway (called “the gateway” in this guide) to provide external network connectivity.

The following components comprise the default setup for networks and gateways in Virtual Private Cloud OnDemand. VMware manages the external network for connectivity to the Intranet. In Virtual Private Cloud OnDemand, customers create and manage networks (utilizing the embedded VXLAN technology).
Gateways

When you create an account for the Virtual Private Cloud OnDemand service, VMware creates your first virtual data center (named VDC1 by default) for you, and adds a default gateway and routed network to that virtual data center. You can log in to the Virtual Private Cloud OnDemand Web UI and create more virtual data centers; thereby adding additional gateways to your public cloud.


When you create an account for the Virtual Private Cloud OnDemand, you are not allocated any public IP addresses. You can purchase public IP addresses at any time through the Virtual Private Cloud OnDemand Web UI by using the Public IPs tab for a gateway. See “Allocation of IP Addresses,” on page 11 for information.

By default, a gateway has the following properties:

- Compact configuration
- High availability disabled
- Multi-interface mode enabled

A gateway supports 10 interfaces, but one interface is reserved for access to the external network. To configure networking for a gateway using routed networks, use the remaining nine interfaces. You can configure unlimited isolated networks for a gateway.

Networks

When you create a virtual data center, it contains a routed network by default. You can add additional networks as needed. See “Add a Network to a Virtual Data Center,” on page 20 and “Add a Network to a Gateway,” on page 22 for information.

When creating a network, you create the network as one of the following types:

- Routed: virtual machines on this network can connect to the Internet.
  
  To allow virtual machines on a routed network to connect to the Internet, you must also add NAT and firewall rules for external network connectivity. See “Connect a Virtual Machine to the Internet,” on page 39 for information.

- Isolated: an internal network; virtual machines on an isolated network are not reachable through the Internet.
Default Settings for Routed Networks

By default, Virtual Private Cloud OnDemand creates a routed network when you create a virtual data center. Virtual Private Cloud OnDemand configures this auto-generated routed network with the following properties:

- Connects to the gateway through the public IP address
- Has the default gateway IP address 192.168.12.1
- Has the subnet mask 255.255.252.0
- Has an IP address pool in the range 192.168.12.100–192.168.12.200
- Has the following networking services enabled or disabled by default:
  - Firewall: enabled; deny all traffic
  - DHCP: disabled
  - NAT: disabled
  - Static routing: disabled
  - VPN: disabled
  - Load balancing: disabled

When you add routed networks to a virtual data center, you must specify the default gateway IP address and the IP address range for virtual machines attached to the network.

**IMPORTANT** When you initially add a routed network in Virtual Private Cloud OnDemand, virtual machines added to that network will not be accessible through or able to connect to the Internet. By default, gateways are deployed with firewall rules configured to deny all network traffic to and from the virtual machines on the gateway networks. Also, NAT is disabled by default so that gateways are unable to translate the IP addresses of the incoming and outgoing traffic. You must configure firewall and NAT rules on a gateway for the virtual machines on its gateway network to be accessible. See “Add a Firewall Rule,” on page 29 and “Add a NAT Rule,” on page 23 for information.

Default Settings for Isolated Networks

An isolated network has an internal IP address and subnet. Virtual machines attached to an isolated network communicate only with each other.

Most often, you connect your virtual machines to a routed network; however, you might connect virtual machines to an isolated network as shown in the following examples:

- To isolate your log servers or database server from direct Internet traffic
- To run internal only applications or virtual machines such as applications under development

When you add an isolated network to a virtual data center, you must specify all network settings. DHCP is disabled by default. (NAT, VPN, firewall rules, static routing, and DNS services are not applicable to isolated networks.)

Summary of Default Settings for Gateways and Networks

The following table summarizes the default configuration for gateways and networks.
### Table 1-1. Summary of Default Settings for Gateways and Networks in Virtual Private Cloud OnDemand

<table>
<thead>
<tr>
<th>FEATURE</th>
<th>DEFAULT SETTINGS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Networking Resources</td>
<td>Logically separated</td>
</tr>
<tr>
<td>Gateways</td>
<td>1 per virtual data center</td>
</tr>
<tr>
<td>Available Gateway Interfaces</td>
<td>9 per gateway</td>
</tr>
<tr>
<td>Bandwidth</td>
<td>10 Mbps allocated and 50 Mbps burstable</td>
</tr>
<tr>
<td>Public IP Addresses</td>
<td>None</td>
</tr>
<tr>
<td>Available Networks on First Log in</td>
<td>Routed</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ROUTED NETWORK</th>
<th>ISOLATED NETWORK</th>
</tr>
</thead>
<tbody>
<tr>
<td>Available Networking Services</td>
<td>Firewall: enabled; deny all traffic</td>
</tr>
<tr>
<td></td>
<td>DHCP: disabled</td>
</tr>
<tr>
<td></td>
<td>Static routing: disabled</td>
</tr>
<tr>
<td></td>
<td>Load balancing: disabled</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Internet Access</th>
<th>Yes—through the gateway public IP address</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address for the Default Gateway</td>
<td>192.168.12.1</td>
<td>—</td>
</tr>
<tr>
<td>Subnet</td>
<td>192.168.12.0/24</td>
<td>—</td>
</tr>
</tbody>
</table>

### Allocation of IP Addresses

When you sign up for Virtual Private Cloud OnDemand and log in for the first time, selecting the service tile on the Home page creates your first virtual data center and a routed network by default. The default, routed network includes a gateway. A public IP address is not assigned to the gateway until you allocate one.

Allocate public IP addresses to a gateway when you have virtual machines that need to be accessible through the Internet. When you allocate public IP addresses, they are reserved for the gateway.

In Virtual Private Cloud OnDemand, you have three ways to assign an IP address to a virtual machine:

- **IP Range**: whenever you attach a virtual machine to a network, the virtual machine gets an IP address from the IP Range created for that network.

- Virtual Private Cloud OnDemand creates pools of IP addresses by default on the auto-generated routed networks.

- Virtual machines attached to the routed networks get an IP address from the default range.

- To change the IP address range for an auto-generated routed network, select the **Networks** tab > default network > Network menu drop-down arrow (→) > **Edit Network**. For information about the network fields, see “Add a Network to a Virtual Data Center,” on page 20.

  When you add a network in Virtual Private Cloud OnDemand, you configure the IP Range for that network.

  See “Add a Network to a Virtual Data Center,” on page 20 and “Add a Network to a Gateway,” on page 22 in this guide for information.

**Note** Gateways in Virtual Private Cloud OnDemand allow for suballocation of IP addresses from multiple subnets that are configured for a gateway’s external interface. Therefore, when you assign IP addresses to a virtual data center or a virtual machine, the IP addresses can belong to different subnets. For example, if you have assigned all the IP addresses from one subnet, while a second subnet is only 50% allocated, you can use IP addresses from the second subnet.
Static IP Address: configure a static IP address for a virtual machine when you create it or change its network settings.

- Provides a fixed IP address for a virtual machine.
- Set a static IP address for a virtual machine in vCloud Director.

DHCP: provides basic DHCP service for a gateway.

- Part of the networking services for a gateway.
- Disabled by default.
- Change the configuration in vCloud Director.

You can view the public IP addresses you have allocated to a gateway by clicking the Gateways tab in the Virtual Private Cloud OnDemand, clicking the gateway for which to view public IP addresses, and then clicking the Public IPs tab. The list of Public IP addresses allocated to that gateway appears.

You can view the IP Range configured for a network by clicking the virtual data center in the Virtual Data Center pane > Networks tab.

### About Networking Services for Gateways

Isolated and routed networks provide the following services.

Configuring networking services for a gateway is accomplished by using a combination of the Virtual Private Cloud OnDemand Web UI and by using vCloud Director:

- NAT: Virtual Private Cloud OnDemand or vCloud Director
- DHCP: vCloud Director
- Load Balancer: vCloud Director
- DNS: vCloud Director
- Firewall Rules: Virtual Private Cloud OnDemand or vCloud Director
- IPSec VPN: vCloud Director
- Static Routing: vCloud Director

You can find information about how these services are implemented in Virtual Private Cloud OnDemand from the following sources.

<table>
<thead>
<tr>
<th>Networking Service</th>
<th>See this related information...</th>
</tr>
</thead>
<tbody>
<tr>
<td>NAT</td>
<td>&quot;Network Address Translation (NAT),” on page 13 in this guide</td>
</tr>
<tr>
<td></td>
<td>&quot;Add a NAT Rule,” on page 23 in this guide</td>
</tr>
<tr>
<td></td>
<td>Add a Source NAT rule to an Edge Gateway in vCloud Director Administrator’s Guide</td>
</tr>
<tr>
<td></td>
<td>Add a Destination NAT rule to an Edge Gateway in vCloud Director Administrator’s Guide</td>
</tr>
<tr>
<td>DHCP</td>
<td>&quot;DHCP,&quot; on page 14 in this guide</td>
</tr>
<tr>
<td></td>
<td>Configure DHCP for an Edge Gateway in vCloud Director Administrator’s Guide</td>
</tr>
<tr>
<td>Load Balancer</td>
<td>&quot;Load Balancer,&quot; on page 15 in this guide</td>
</tr>
<tr>
<td></td>
<td>Managing Load Balancer Service on an Edge Gateway in vCloud Director Administrator’s Guide</td>
</tr>
<tr>
<td>DNS</td>
<td>&quot;DNS,&quot; on page 16 in this guide</td>
</tr>
<tr>
<td></td>
<td>Modify an Organization Virtual Datacenter Network DNS Settings in vCloud Director Administrator’s Guide</td>
</tr>
<tr>
<td></td>
<td>&quot;Deploy Directory and DNS Services” in VMware vCloud Air Solution Brief</td>
</tr>
</tbody>
</table>

VMware, Inc.
### Network Address Translation (NAT)

Gateways in Virtual Private Cloud OnDemand support NAT for the virtual machines connected to routed networks. Create a NAT rule to translate a public IPv4 address to and from the private IPv4 address of a virtual machine on your isolated network in Virtual Private Cloud OnDemand.

Virtual Private Cloud OnDemand supports source NAT (SNAT) and destination NAT (DNAT) rules. When you configure an SNAT or a DNAT rule, you always configure the rule from the perspective of Virtual Private Cloud OnDemand. You configure the rules in the following ways:

- **SNAT**: the traffic is traveling from a virtual machine on an isolated network in Virtual Private Cloud OnDemand (the source) through the Internet to the external network (the destination).
- **DNAT**: the traffic is traveling from the Internet (the source) to a virtual machine inside Virtual Private Cloud OnDemand (the destination).

**Figure 1-3. Example for Network Address Translation**

![Network Address Translation Diagram]

Given the example in Figure 1-3, you can add the following NAT rules for VM1 to communicate with the Web server (IP address 209.165.200.225):

- **SNAT**
  - Original (Internal) Source: 10.0.0.2
  - Translated (External) Source: 209.165.200.1

- **DNAT**
  - Original (External) IP: 209.165.200.1
This NAT example shows the translation of IP addresses on the private network on the inside of the gateway. When the virtual machine at 10.0.0.2 sends a packet to the Web server at 209.165.200.225, the virtual machine’s real address (10.0.0.2) is translated to 209.165.200.1. When the Web server responds, it sends the response to IP address 209.165.200.1, and the gateway translates 209.165.200.1 back to the real address 10.0.0.2 before sending it to the virtual machine.

You can configure NAT rules to create a private IP address space inside Virtual Private Cloud OnDemand to port your private IP address space from your enterprise into the cloud. Configuring NAT rules in Virtual Private Cloud OnDemand allows you to use the same private IP addresses for your virtual machines in Virtual Private Cloud OnDemand that are used in your local data center.

NAT rules in Virtual Private Cloud OnDemand include the following support:

- Creating subnets within the private IP address space
- Creating multiple private IP address spaces for a gateway
- Configuring multiple NAT rules on multiple gateway interfaces

**IMPORTANT** By default, gateways are deployed with firewall rules configured to deny all network traffic to and from the virtual machines on the routed networks. Also, NAT is disabled by default so that gateways are unable to translate the IP addresses of the incoming and outgoing traffic. You must configure both firewall and NAT rules on a gateway for the virtual machines on a routed network to be accessible. Attempting to ping a virtual machine on a network after configuring a NAT rule will fail without adding a firewall rule to allow the corresponding traffic.

**Related Information**

- See “Add a NAT Rule,” on page 23 in this guide for the steps to create a SNAT or DNAT rule
- See “Add a Firewall Rule,” on page 29 in this guide for the steps to create a firewall rule.

**DHCP**

To change the default behavior for DHCP in Virtual Private Cloud OnDemand networks, you edit the DHCP service settings in vCloud Director.

When you create a network in Virtual Private Cloud OnDemand, DHCP is configured for Virtual Private Cloud OnDemand in the following ways.

**Routed Network**

DHCP is configured for routed networks in the following ways:

- Disabled by default.

  When you create a virtual machine and add it to a routed network, you must explicitly set its IP address unless you have enabled DHCP for that network.

Configure DHCP for a routed network by navigating from Virtual Private Cloud OnDemand to the networking services for the gateway in vCloud Director:

Virtual Private Cloud OnDemand Web UI > Gateway tab > Manage in vCloud Director > vCloud Director Administration page > Edge Gateways tab > select the gateway, right-click and choose Edge Gateway Services > DHCP tab

Enable and configure DHCP for a routed network to automatically assign an IP address to a virtual machine when it is added to a routed network. The virtual machine gets assigned an IP address based on the DHCP parameters configured.
See Configure DHCP for an Edge Gateway in vCloud Director Administrator’s Guide for more information.

**Note** Before you enable DHCP for a routed network and add an IP address pool, you must determine a valid range for the IP addresses assigned by DHCP.

You can view the public IP addresses you have allocated to a gateway by clicking the Gateways tab from the Virtual Private Cloud OnDemand Web UI, clicking the gateway for which to view public IP addresses, and clicking the Public IPs tab. The list of Public IP addresses allocated to that gateway appears.

**Isolated Network**

DHCP is disabled by default for isolated networks.

Configure DHCP for an isolated network by navigating from Virtual Private Cloud OnDemand to the Org VDC Networks tab for the virtual data center in vCloud Director:

Virtual Private Cloud OnDemand Web UI > Networks tab > Manage in vCloud Director > vCloud Director Administration page > Org VDC Networks tab > select the isolated network, right-click and choose Configure Services > DHCP tab.

**Load Balancer**

Gateways in Virtual Private Cloud OnDemand support load balancing for the virtual machines connected to routed networks.

In Virtual Private Cloud OnDemand, a load balancer for a gateway has a virtual server and corresponding server pool. The virtual server and server pool have the following characteristics:

- The virtual server has a public IP address and services all incoming client requests.
- The server pool assigned to the virtual server is responsible for all load balancing.

Because a gateway supports up to nine interfaces, the load balancer service supports multiple server pools and separate load balancing methods for each server pool (as shown in the following graphic).

**Figure 1-4. Load Balancing Components in Virtual Private Cloud OnDemand**

See Add a Pool Server to an Edge Gateway in vCloud Director Administrator’s Guide for a description of each load balancing method.

To configure load balancing for a gateway, do the following tasks:

1. Determine which public IP address is allocated to the gateway before you configure load balancing for it by clicking the Gateway tab from the Virtual Private Cloud OnDemand Web UI > gateway name > Public IPs tab. The list of public IP addresses allocated to the gateway appears.
To view the public IP address allocation for the gateway by using vCloud Director, see View IP Use for an Edge Gateway in vCloud Director Administrator’s Guide for information.

Additionally, view the Sub-allocated IP Range configured for the gateway. (A gateway uses the Sub-allocated IP Range for NAT configuration. A Sub-allocated IP Range contains a subset of IP addresses from the IP Range that is already assigned to the gateway’s external network.)

Navigate from Virtual Private Cloud OnDemand to the following area of vCloud Director:

Virtual Private Cloud OnDemand Web UI > Gateway tab > Manage in vCloud Director > vCloud Director Administration page > Edge Gateway tab > select the gateway, right-click and choose Properties > Sub-Allocate IP Pools tab


1 Configure load balancing for the gateway by using vCloud Director.

Load balancing for a gateway is configured on the external interface because the gateway load balances incoming traffic from the external network. When configuring the virtual server for load balancing, specify one of the available IP addresses that you determined from task 1.

Navigate from Virtual Private Cloud OnDemand to the following area of vCloud Director:

Virtual Private Cloud OnDemand Web UI > Gateways tab > Manage in vCloud Director > vCloud Director Administration page > Edge Gateway tab > select the gateway, right-click and choose Edge Gateway Services > Load Balancer tab

See Managing Load Balancer Service on an Edge Gateway in vCloud Director Administrator’s Guide for the steps to configure the virtual server and server pool.

3 Create a firewall rule to permit traffic to the new virtual server (the destination IP address).

See “Add a Firewall Rule,” on page 29 in this guide for information.

Traffic to this routed network is now load balanced between the servers in the server pool.

DNS

The gateway provides a Domain Name System (DNS) server to networks within Virtual Private Cloud OnDemand. You can choose to use the DNS services provided by the gateway or you can specify an alternative DNS server. If you choose to use the gateway DNS service, DNS relay must be preconfigured on the gateway.

You can configure external DNS servers to which the gateway can relay name resolution requests from clients. When an external DNS server is configured, the gateway relays client application requests to the DNS servers to fully resolve a network name and cache the response from the servers.

To configure DNS for your virtual machines in Virtual Private Cloud OnDemand, update the default DNS settings in vCloud Director. Access the DNS settings in vCloud Director by navigating from Virtual Private Cloud OnDemand to the following area of vCloud Director:

Virtual Private Cloud OnDemand Web UI > Networks tab > Manage in vCloud Director > vCloud Director Administration tab > Org VDC Networks tab > select the network, right-click and choose Properties > Network Specification tab
See Modify an Organization Virtual Datacenter Network DNS Settings in vCloud Director Administrator’s Guide for information.

**Note** If the DNS settings on a DHCP-enabled gateway are changed, the gateway no longer provides DHCP services. To correct this issue, disable and re-enable DHCP on the gateway. For information about enabling DHCP, see the following documentation:

- “DHCP,” on page 14 in this guide
- Configure DHCP for an Edge Gateway in vCloud Director Administrator’s Guide

### Related Information


### Static Routing

In Virtual Private Cloud OnDemand, the gateway supports configuring static routing between the interfaces in the gateway. By default, static routing is disabled for a gateway. (On an isolated network, which does not connect to a gateway, static routing is not applicable).

On a routed network, network traffic goes to the gateway’s default interface, which connects to the Internet. When you configure a static route between interfaces, traffic bypasses the default interface to the Internet.

**Figure 1-5.** Example of Static Routing in Virtual Private Cloud OnDemand

![Static Routing Diagram](image)

You might want to enable static routing on a gateway for the following use cases:

- So that all the traffic from the external network traverses the antivirus appliance first before accessing your virtual machines
- When you want a Web server on one routed network to connect to an application server on another routed network without having the traffic traverse the Internet

Configure static routing for a routed network by navigating from Virtual Private Cloud OnDemand to the networking services for the gateway in vCloud Director:

Virtual Private Cloud OnDemand Web UI > **Gateway** tab > **Manage in vCloud Director** > vCloud Director Administration page > **Edge Gateways** tab > select the gateway, right-click and choose **Edge Gateway Services** > **Static Routing** tab
For the steps to configure static routing by using vCloud Director, see the following topics in *vCloud Director Administrator’s Guide*:

- Enable Static Routing on an Edge Gateway
- Add Static Routes Between vApp Networks Routed to the Same Organization Virtual Datacenter Network
About Managing Gateways and Networks

The Virtual Private Cloud OnDemand Web UI is the primary portal for managing gateways and networks. Additionally, you can use vCloud Director to manage your gateways and networks at a more detailed level. The Virtual Private Cloud OnDemand Web UI provides single sign-on access to vCloud Director.

To do the following tasks to manage gateways and networks in Virtual Private Cloud OnDemand, verify that you have network administrator or virtual infrastructure administrator privileges in the Virtual Private Cloud OnDemand services where you plan to manage your networking resources. (Configuring more permissions in vCloud Director is not required.)

This chapter includes the following topics:

- “View Networks in a Virtual Data Center,” on page 19
- “Add a Network to a Virtual Data Center,” on page 20
- “View and Edit Gateway Details,” on page 21
- “Add a Network to a Gateway,” on page 22
- “Delete a Network,” on page 22
- “Add a NAT Rule,” on page 23
- “Allocate Public IP Addresses,” on page 25

**View Networks in a Virtual Data Center**

You can view a list of the networks in your virtual data center. For each network, you can view the type of network, default gateway IP address, IP range, and the number of virtual machines attached to it. For routed networks, you can also view the gateway and the number of public IP addresses allocated to it.

**Prerequisites**

Verify that you have network administrator privileges.

**Procedure**

1. If necessary, click the expand icon ( ) to display the Virtual Data Centers pane.
2. Select the virtual data center to which the network belongs.
3. Click the Networks tab.

Details about the networks configured for the virtual data center appear, including the gateway IP address, and any public IP addresses allocated to the network.
What to do next

See “Default Setup for Gateways and Networks,” on page 8 in this guide for information about the settings for routed and isolated networks.

Add a Network to a Virtual Data Center

You can add more isolated or routed networks to virtual data centers. Routed networks can be added only to virtual data centers that have a gateway.

This topic provides the steps to add a network for a virtual data center by using vCloud Air. For information about adding networks by using vCloud Director, see the following topics in vCloud Director Administrator’s Guide:

- Managing Organization vDC Networks
- Adding Networks to an Organization vDC

Prerequisites

Verify that you have network administrator privileges.

Procedure

1. If necessary, click the expand icon ( ) to display the Virtual Data Centers pane.
2. Select the virtual data center to which the network belongs.
3. Click the Networks tab.
4. Click Add One. The Add Network dialog appears.
5. Complete the following settings for the network:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network name</td>
<td>Enter a name for the gateway.</td>
</tr>
<tr>
<td>Description</td>
<td>(Optional) Enter a description for the network.</td>
</tr>
<tr>
<td>Routed through VDC gateway</td>
<td>(Optional) Select this option to create a routed network; create a routed network when the virtual machines on the network need access to the Internet. If you do not select this option, an isolated network is added to the virtual data center.</td>
</tr>
<tr>
<td>VDC gateway</td>
<td>After selecting Routed through VDC gateway, select the gateway from the drop-down list. The drop-down list contains the gateways available for the virtual data center.</td>
</tr>
<tr>
<td>Network Gateway</td>
<td>Enter the gateway IP address for the network.</td>
</tr>
<tr>
<td>Subnet mask</td>
<td>Enter the subnet mask for the IP Range for this network.</td>
</tr>
<tr>
<td>IP Range</td>
<td>Enter the IP address range for this network.</td>
</tr>
</tbody>
</table>

NOTE This option is only available when the virtual data center has at least one gateway.

NOTE Entering a gateway IP address is required even when adding an isolated network because isolated networks are dependent on a gateway for DHCP networking services. If you are adding an isolated network, entering a gateway address in this field does not affect the network’s isolated status.

NOTE Entering a gateway IP address is required even when adding an isolated network because isolated networks are dependent on a gateway for DHCP networking services. If you are adding an isolated network, entering a gateway address in this field does not affect the network’s isolated status.

See “Allocation of IP Addresses,” on page 11 for more information.
6 Click Add Network.

**View and Edit Gateway Details**

You can view a list of the gateways in your Virtual Private Cloud OnDemand service. You can configure details to make workloads available on the Internet.

**Prerequisites**

Verify that you have network administrator privileges.

Verify that you are familiar with gateway configuration. See *Managing Edge Gateways* in the *vCloud Director Administrator’s Guide*.

**Procedure**

1. If necessary, click the expand icon (expand icon) to display the Virtual Data Centers pane.
2. Select the virtual data center to which the gateway belongs.
3. Click the **Gateways** tab.

   Details about the gateway appear, including the gateway IP address, configuration, VMware High Availability settings, number of networks configured for the gateway, and any public IP addresses allocated to the gateway.

4. To view and adjust the gateway configuration, click the gateway tile.

   The gateway details appear.

5. View and configure the gateway:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NAT Rules tab</td>
<td>View SNAT or DNAT details. Disable, enable, or delete rules. Click Add One to add an SNAT or DNAT rule. For SNAT, configure source and enabled status. For DNAT, configure external IP, protocol and range details, and enabled status.</td>
</tr>
<tr>
<td>Firewall Rules tab</td>
<td>View or add firewall rules to allow or deny types of incoming traffic.</td>
</tr>
<tr>
<td>Networks tab</td>
<td>View details about the gateway’s network, such as name, type, default IP address, number of connected virtual machines, public IP addresses, and IP range.</td>
</tr>
<tr>
<td>Public IPs tab</td>
<td>View whether IP addresses are available or allocated.</td>
</tr>
</tbody>
</table>

6. To configure gateway services or edit gateway details, click **Manage Gateway in vCloud Director**.

   Using vCloud Director, you can configure DHCP, load balancing, DNS, and static routing for the gateway, or manage settings such as compact configuration, high availability, and rate limits.

**What to do next**

See “About Networking Services for Gateways,” on page 12 for a list of gateway configuration adjustments you can make using the Virtual Private Cloud OnDemand Web UI or vCloud Director.
Add a Network to a Gateway

You can view a list of the networks added to a gateway. For each network, you can view the default gateway IP address, IP range, and the number of virtual machines attached to it and the number of public IP addresses allocated to the gateway.

Prerequisites

Verify that you have network administrator privileges.

Procedure

1. If necessary, click the expand icon ( ) to display the Virtual Data Centers pane.
2. Select the virtual data center to which the gateway belongs.
3. Click the Gateways tab.
   A tile displaying details about the gateway appears.
4. Click the gateway tile.
5. Click the Networks tab.
   All networks in the gateway are listed.
6. Click Add One.
   The Add Network dialog appears.
7. Complete the following settings for the network:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network name</td>
<td>Enter a name for the gateway.</td>
</tr>
<tr>
<td>Description</td>
<td>(Optional) Enter a description for the gateway.</td>
</tr>
<tr>
<td>Network Gateway</td>
<td>Enter the gateway IP address for the network.</td>
</tr>
<tr>
<td>Subnet mask</td>
<td>Enter the subnet mask for the IP Range for this network. When you attach a virtual machine to a network, the virtual machine gets an IP address from the IP Range created for that network. See “Allocation of IP Addresses,” on page 11 for more information.</td>
</tr>
<tr>
<td>IP Range</td>
<td>Enter the IP address range for this network. Click the plus to add additional IP address ranges.</td>
</tr>
</tbody>
</table>

*NOTE* The Routed through VDC gateway and VDC gateway fields are completed for you automatically.

Delete a Network

You can delete isolated or routed networks from a virtual data center. Before you delete a network, disconnect all virtual machines from it.

Prerequisites

Verify that you have network administrator privileges.

Procedure

1. If necessary, click the expand icon ( ) to display the Virtual Data Centers pane.
2. Select the virtual data center to which the network belongs.
3 Click the Networks tab.

4 For the network you want to delete, click the drop-down arrow (▼) and select Delete Network.
   A dialog appears reminding you to disconnect all the virtual machines from the network before deleting it.

5 Click Yes.
   The network is deleted and a confirmation message appears at the top of the Virtual Private Cloud OnDemand page.

Add a NAT Rule

In Virtual Private Cloud OnDemand, you can create a NAT rule to direct traffic between an external network and your virtual machines on an inside network. When you configure a SNAT or DNAT rule, you always configure the rule from the perspective of Virtual Private Cloud OnDemand.

You configure NAT rules in the following ways:

- **SNAT**: the traffic is traveling from a virtual machine on an internal network in Virtual Private Cloud OnDemand (the source) through the Internet to the external network (the destination).
- **DNAT**: the traffic is traveling from the Internet (the source) to a virtual machine inside Virtual Private Cloud OnDemand (the destination).

See “Network Address Translation (NAT),” on page 13 in this guide for more information.

This procedure provides the steps to create a NAT rule by using Virtual Private Cloud OnDemand. For information about creating or editing NAT rules by using vCloud Director, see the following topics in vCloud Director Administrator’s Guide:

- Add a Source NAT rule to an Edge Gateway
- Add a Destination NAT rule to an Edge Gateway

Prerequisites

Before creating a NAT rule, complete the following items:

- Verify that you have network administrator privileges.
- Obtain the IP addresses for the virtual machines that you are creating the NAT rules.

Procedure

1 If necessary, click the expand icon (▼) to display the Virtual Data Centers pane.

2 Select the virtual data center to which the gateway belongs.

3 Click the Gateways tab.

4 Click the gateway tile.

5 Click the NAT Rules tab.

6 Click the Add button.
   The Add NAT Rule dialog appears.
7 Depending on which type of NAT rule you want to create, click one of the following options:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SNAT</td>
<td>A source NAT rule changes the source IP address and, optionally, port of outgoing packets. When you create an SNAT rule in Virtual Private Cloud OnDemand, by default the port and protocol are set to “any.” To change the default port and protocol settings for an SNAT rule, edit the settings in vCloud Director.</td>
</tr>
<tr>
<td>DNAT</td>
<td>A destination NAT rule changes the destination IP address and, optionally, port of inbound packets.</td>
</tr>
</tbody>
</table>

Depending on which option you chose, the dialog refreshes with the required fields.

8 Depending on which type of NAT rule you are creating, complete the following settings:

**Source NAT (SNAT) (inside -> outside)**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Original (Internal) Source</td>
<td>Enter the original IP address or range of IP addresses to apply to this rule. The original addresses are the IP addresses of the virtual machine (or machines) for which you are configuring SNAT so that they can send traffic to the external network.</td>
</tr>
<tr>
<td>Translated (External) Source</td>
<td>Specifies the IP address to which source addresses (the virtual machines) on outbound packets are translated to when they send traffic to the external network. The translated address is always the public IP address of the gateway for which you are configuring the SNAT rule. Select the required IP address from the drop-down menu.</td>
</tr>
</tbody>
</table>

**Destination NAT (DNAT) (outside -> inside)**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Original (External) IP</td>
<td>Specifies the destination IP address to which the rule applies; the address is always the public IP address of the gateway for which you are configuring the DNAT rule. Select the required IP address from the drop-down menu.</td>
</tr>
<tr>
<td>Protocol</td>
<td>Select the protocol to which the rule applies—any, TCP, UDP, TCP/UDP, and ICMP. By default, the protocol is set to “any.”</td>
</tr>
<tr>
<td>Original Port/Range</td>
<td>(Optional) Enter the port or port range that the incoming traffic uses on the gateway to connect to the internal network on which the virtual machines are connected.</td>
</tr>
<tr>
<td>ICMP type</td>
<td>If you selected ICMP (an error reporting and diagnostic utility used between devices to communicate error information) in the Protocol field, select the ICMP type from the drop-down menu. ICMP messages are identified by the “type” field. By default, the ICMP type is set to “any.”</td>
</tr>
<tr>
<td>Translated (Internal) IP/Range</td>
<td>Enter the IP address or a range of IP addresses to which destination addresses on inbound packets will be translated. The translated addresses are the IP addresses of the virtual machine (or machines) for which you are configuring DNAT so that they can receive traffic from the external network.</td>
</tr>
<tr>
<td>Translated Port/Range</td>
<td>(Optional) Enter the port or port range that traffic connects to on the virtual machines on the isolated network.</td>
</tr>
</tbody>
</table>

9 Select **Enable this rule** and click **Save**.

The NAT Rules dialog appears.

10 Click **Add** to add additional rules or click **Finish** to commit the rules to the gateway.
Allocate Public IP Addresses

Allocate public IP addresses to a gateway only when you create virtual machines that need to be accessible through the Internet; for example, you want to assign a public IP address to Web server. When you allocate public IP addresses, they are reserved for that gateway.

Virtual Private Cloud OnDemand offers resource pool-based pay-as-you-go service, which includes charges for public IP addresses allocated for your gateways. Virtual Private Cloud OnDemand monitors your gateways to determine when you allocate or de-allocate public IP addresses to them. You are charged for those public IP addresses only while they are in use.

You can allocate up to 5 public IP addresses per gateway and up to 20 public IP addresses across all gateways in your Virtual Private Cloud OnDemand environment.

If you require more than 20 public IP addresses, file a support request. Log into My VMware to file support requests for Virtual Private Cloud OnDemand. See the My VMware Help (?) for information.

Prerequisites

Verify that you have network administrator privileges.

Procedure

1. If necessary, click the expand icon ( ) to display the Virtual Data Centers pane.

2. Select the virtual data center that contains the gateway to which you want to allocate the public IP address.

3. Click the Gateways tab.

   Details about the gateway appear, including any public IP addresses allocated to the gateway.

4. Click Add IP Address.

   A dialog box appears indicating charges apply when adding a public IP address to a gateway.

5. Click Add.

   A notification appears at the top of the page indicating the public IP address is allocated to the gateway.

What to do next

See “Change Network Assignments for a Virtual Machine,” on page 38 for information about assigning a public IP address to a virtual machine.
Network Security and Secure Access

Virtual Private Cloud OnDemand provides features and functions to ensure network security and secure access to your resources in the cloud.

This chapter includes the following topics:

- “About Network Security,” on page 27
- “About Firewall Rules,” on page 29
- “Add a Firewall Rule,” on page 29
- “VPN and Remote Networks,” on page 30
- “About IPsec VPN,” on page 31
- “About Setting up an IPsec VPN Connection,” on page 31
- “Set up an IPsec VPN Connection to a Remote Site,” on page 33
- “SSL VPN for Data Center Extension,” on page 34

About Network Security

Your configuration decisions within Virtual Private Cloud OnDemand have network security implications. The type of networks you add to Virtual Private Cloud OnDemand and how you connect your virtual machines to those networks have security considerations as well. Connect your virtual machines to the appropriate networks based on their security needs.

<table>
<thead>
<tr>
<th>Table 3-1. Security Differences Between Network Types</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Routed Network</strong></td>
</tr>
<tr>
<td><strong>REQUIRED FOR</strong></td>
</tr>
<tr>
<td>- Virtual machines that need access to external networks.</td>
</tr>
<tr>
<td>- Workloads subject to specific security policies; for example, compliance rules that a particular application cannot be connected directly to the Internet.</td>
</tr>
<tr>
<td><strong>BENEFITS</strong></td>
</tr>
<tr>
<td>- Connecting virtual machines to routed networks gives those virtual machines access to the networking services provided by a gateway—firewall, NAT, and load balancing.</td>
</tr>
<tr>
<td>- Isolated networks are not connected to gateways; therefore, they are ideal for running internal applications.</td>
</tr>
<tr>
<td><strong>Note</strong> You can have an instance of a dual NIC on a virtual machine and can connect one interface of the virtual machine to the routed network and the other interface to the isolated network.</td>
</tr>
<tr>
<td>- Virtual machines running applications you want to isolate from direct Internet traffic, such as your log servers, tracking servers, and database servers.</td>
</tr>
</tbody>
</table>

VMware, Inc.  27
The following products and solutions are supported with Virtual Private Cloud OnDemand and work together to provide network security for Virtual Private Cloud OnDemand.

**Figure 3-1. Product Interactions to Provide Security in Virtual Private Cloud OnDemand**

![Diagram showing interactions between gateway, threat mitigation, and third-party appliance]

The following security functions are available in Virtual Private Cloud OnDemand:

- **Gateway:** firewall, IP address management, and routing
- **Threat mitigation:** third-party antivirus, traffic analysis, and threat mitigation appliances
- **Third-party appliances:** virtual appliances of your choice allowing you to deploy your own security policies
- **VXLAN:** the foundation for elastic portable virtual data centers

### Third-party Virtual Appliances

Virtual Private Cloud OnDemand supports threat mitigation by allowing you to deploy your own antivirus solution (such as, MacAfee antivirus) and configure static routing between the gateway interfaces so that all traffic traverses the antivirus first, then travels to your virtual machines.

Virtual Private Cloud OnDemand supports the deployment of third-party virtual appliances in the cloud. For example, if you are using policies based on a Palo Alto security appliance, or appliances deployed onsite at your data center, you can deploy that same third-party virtual appliance in Virtual Private Cloud OnDemand and run network traffic to your virtual machines through the appliance. Using the same virtual appliance in Virtual Private Cloud OnDemand that you used onsite in your data center, Virtual Private Cloud OnDemand can become an extension of your onsite cloud.

Virtual Private Cloud OnDemand supports the deployment of all third-party virtual appliances supported by VMware vSphere; such as, F5, RSA (for secure ID), and Riverbed (caching).

Additionally, you can use a third-party appliance with your isolated networks in Virtual Private Cloud OnDemand. Isolated networks (which are not connected to the gateway) can connect to a third-party appliance; the third-party virtual appliance can have access to the gateway.
About Firewall Rules

You configure all networking security policies on the gateway by creating firewall rules. Virtual Private Cloud OnDemand does not require configuring security groups like other cloud providers. You configure firewall rules to manage the traffic flowing in and out of your Virtual Private Cloud OnDemand cloud. Additionally, you can configure firewall rules to secure network traffic between interfaces on a gateway.

Firewall rules in Virtual Private Cloud OnDemand have the following characteristics:

- Consist of 5 tuple policies (protocol, source/destination IP address, source/destination port)
- Can have multiple policies across multiple networks
- Are ideal for enterprise-grade application deployment

**IMPORTANT** By default, gateways are deployed with firewall rules configured to deny all network traffic to and from the virtual machines on the routed networks. Attempting to ping a virtual machine on a network after configuring a NAT rule will fail without adding a firewall rule to allow the corresponding traffic.

See “Add a Firewall Rule,” on page 29 in this guide for the steps to create a firewall rule.

Related Information

- Configure the Firewall for an Edge Gateway in *vCloud Director Administrator’s Guide*
- Add a Firewall Rule for an Edge Gateway in *vCloud Director Administrator’s Guide*

Add a Firewall Rule

Configure a firewall rule to allow traffic through a gateway to reach the virtual machines on your isolated network and so that your virtual machines can reach the Internet.

This procedure provides the steps to create a firewall rule by using Virtual Private Cloud OnDemand. For information about creating or editing firewall rules by using vCloud Director, see the following topics in the *vCloud Director Administrator’s Guide*:

- Configure the Firewall for an Edge Gateway
- Add a Firewall Rule for an Edge Gateway

Prerequisites

- Verify that you have network administrator privileges.
- Obtain the IP address for the virtual machine for which you are creating the firewall rule.

Procedure

1. If necessary, click the expand icon to display the Virtual Data Centers pane.
2. Select the virtual data center to which the gateway belongs.
3. Click the Gateways tab.
   - Details about the gateway appear.
4. Click Firewall Rules tab.
5. Click the Add button.
   - The Add a Firewall “Allow” Exception dialog appears.
Complete the following settings to configure the rule:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a name for the rule.</td>
</tr>
<tr>
<td>Settings</td>
<td>(Optional) Select <strong>Enable this</strong> to enable the rule for the gateway.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong>: Selecting the <strong>Log network traffic for this exception</strong> option is</td>
</tr>
<tr>
<td></td>
<td>unnecessary because you cannot access firewall logging data in Virtual</td>
</tr>
<tr>
<td></td>
<td>Private Cloud OnDemand at this time.</td>
</tr>
<tr>
<td>Protocol</td>
<td>Choose a protocol to which the rule applies from the drop-down menu:</td>
</tr>
<tr>
<td></td>
<td>any, TCP, UDP, TCP/UDP, or ICMP.</td>
</tr>
<tr>
<td></td>
<td>By default, the protocol is set to “any” so that network traffic from all</td>
</tr>
<tr>
<td></td>
<td>protocols traverses the firewall.</td>
</tr>
<tr>
<td>Source</td>
<td>Choose an option from the drop-down menu:</td>
</tr>
<tr>
<td></td>
<td>Any: allows traffic from any source on the external network to reach</td>
</tr>
<tr>
<td></td>
<td>the virtual machines.</td>
</tr>
<tr>
<td></td>
<td>Internal: apply this rule to all internal traffic.</td>
</tr>
<tr>
<td></td>
<td>External: apply this rule to all external traffic.</td>
</tr>
<tr>
<td></td>
<td>Specific CIDR, IP, or IP Range: type the CIDR notation of traffic to</td>
</tr>
<tr>
<td></td>
<td>apply this rule on.</td>
</tr>
<tr>
<td>Source Port</td>
<td>(Optional) Enter a port or port range to allow traffic from those ports to</td>
</tr>
<tr>
<td></td>
<td>reach your virtual machines on your isolated network.</td>
</tr>
<tr>
<td>Destination</td>
<td>Choose an option from the drop-down menu:</td>
</tr>
<tr>
<td></td>
<td>Any: allows traffic from any virtual machine on your isolated network to</td>
</tr>
<tr>
<td></td>
<td>access the external network.</td>
</tr>
<tr>
<td></td>
<td>Internal: apply this rule to all internal traffic.</td>
</tr>
<tr>
<td></td>
<td>External: apply this rule to all external traffic.</td>
</tr>
<tr>
<td></td>
<td>Specific CIDR, IP, or IP Range: type the CIDR notation of traffic to</td>
</tr>
<tr>
<td></td>
<td>apply this rule on.</td>
</tr>
<tr>
<td>Destination Port</td>
<td>(Optional) Enter a port or port range to allow traffic from those ports on</td>
</tr>
<tr>
<td></td>
<td>your virtual machines to reach the external network.</td>
</tr>
</tbody>
</table>

Click **Save**.

VPN and Remote Networks

Another aspect of network security is the connectivity you establish between your on premise data center and the Virtual Private Cloud OnDemand cloud. Based on the workload, a virtual machine can have various connectivity needs.

Virtual Private Cloud OnDemand supports the following types of secure connections between your remote site and the Virtual Private Cloud OnDemand cloud.

Each type of connection has different security features:

- Secure Internet connectivity with firewall rules (a gateway service)
  See “About Firewall Rules,” on page 29 in this guide for information.
- Secure VPN
  - IPsec VPN—secure site-to-site VPN
    See “About Setting up an IPsec VPN Connection,” on page 31 and “Set up an IPsec VPN Connection to a Remote Site,” on page 33 in this guide for information.
  - SSL VPN (Data Center Extension)—extension of your existing IP address range from your on-premise data center into the cloud with Layer 2 extension
    See “SSL VPN for Data Center Extension,” on page 34 in this guide for information.
Create an IPsec VPN connection by using Virtual Private Cloud OnDemand and vCloud Director. Create an SSL VPN (Data Center Extension) connection by using vCloud Connector.

**Related Information**
- See [Create a VPN Tunnel to a Remote Network](#) in vCloud Director Administrator’s Guide for information.
- See the VMware Blog article [How To Use VPN to Connect Multiple vCloud Air Clouds](#) for more information.

**About IPsec VPN**

Internet Protocol Security (IPsec) is a protocol suite for securing the IP packets of a communication session. vCloud Air – Virtual Private Cloud OnDemand supports using IPsec to create a secure VPN connection between your Virtual Private Cloud OnDemand public cloud and a remote site, such as your on-premises data center.

The gateway supports the following IPsec functionality for IPsec VPN connections between sites:
- Certificate authentication using pre-shared key mode
- IP unicast traffic (but not dynamic routing) between the gateway and remote VPN routers
- The ability to configure multiple subnets per remote VPN router to connect an IPsec VPN to a gateway network on the gateway’s inside interface

**Note**: The VPN router subnets and the gateway network cannot have overlapping IP address ranges. They must use different subnets because the IPsec VPN connection requires they have different local endpoint IP addresses.

- A maximum of 64 IPsec VPN connections across a maximum of 10 sites
- Deploying a gateway behind a NAT device to translate the gateway’s VPN IP address to a public IP address accessible from the Internet
  - Remote VPN routers use the public IP address to access the gateway.
- Deploying remote VPN routers behind a NAT device
  - When deploying a remote VPN router behind a NAT device, configure the IPsec VPN connection using the VPN native IP address and the VPN Gateway ID. On both sides of the connection, configure static one-to-one NAT for the VPN IP address.

**Related Information**

See “Set up an IPsec VPN Connection to a Remote Site,” on page 33 in this guide for the steps to set up an IPsec VPN connection in vCloud Air.

See also [Create a VPN Tunnel to a Remote Network](#) in vCloud Director Administrator’s Guide

See also [Enable VPN for an Organization Virtual Datacenter Network](#) in vCloud Director Administrator’s Guide

**About Setting up an IPsec VPN Connection**

You can configure an IPsec VPN connection between networks within Virtual Private Cloud OnDemand and between a remote site and Virtual Private Cloud OnDemand. Setting up an IPsec VPN connection from a remote network to Virtual Private Cloud OnDemand is the most common scenario.
Using vCloud Director, you configure an IPsec VPN connection for Virtual Private Cloud OnDemand as part of configuring gateway services. When you configure an IPsec VPN connection between sites, you configure the connection from the point of view of your current location. Setting up the connection requires that you understand how to configure the following values so that you configure the VPN connection correctly:

- **Peer Networks**: specifies the remote networks to which the VPN connects. When you configure this setting, enter a network range and not a specific IP address. Enter the IP address using CIDR format; for example, 192.168.99.0/24.

- **Local Endpoint (LEP)**: specifies the network in Virtual Private Cloud OnDemand on which the gateway transmits. Typically, the external network is the local endpoint.

- **Peer ID**: specifies the public IP address of the remote device terminating the VPN connection. If the peer IP address is from another organization VDC network, you enter the peer’s native IP address. If NAT is configured for the peer, you enter the private peer IP address.

- **Peer IP**: specifies the public IP address of the remote device to which you are connecting. If NAT is configured for the peer, you enter the public IP address that the devices uses for NAT.

- **Local ID**: specifies the public IP address of the gateway. You can enter an IP address or hostname in conjunction with the gateway firewall.

**Example: Configuring IPsec VPN Connection between VM1 and VM2**

The following diagram shows an example for how to specify the VPN connection settings correctly:

**Figure 3-2. Architecture: IPsec VPN between Virtual Private Cloud OnDemand and a Remote Site**

Specifying the peer IDs and peer IPs configure how network traffic travels from one side of the connection to the other side. In the example, the peer ID and peer IP for the Virtual Private Cloud OnDemand side of the connection are different values because in the on-premises side of the connection, the on-premises gateway is not directly accessible from the Internet (it connects to the Internet through an external router). In the on-premises side of the connection, the peer ID and peer IP are the same value because the gateway in Virtual Private Cloud OnDemand is directly accessible from the Internet (it does not sit behind another device).
Set up an IPsec VPN Connection to a Remote Site

This procedure provides the steps to create an IPsec VPN connection between Virtual Private Cloud OnDemand and a remote site. In this procedure, you configure the Virtual Private Cloud OnDemand side of the connection.

You use vCloud Director to configure the IPsec VPN connection. You configure an IPsec VPN connection as part of configuring gateway services in vCloud Director.

Prerequisites

Verify that you have networking administration privileges in Virtual Private Cloud OnDemand.

If a firewall is between the connection endpoints, you must configure it to allow the following IP protocols and UDP ports:

- IP Protocol ID 50 (ESP)
- IP Protocol ID 50 (ESP)
- IP Protocol ID 51 (AH)
- UDP Port 500 (IKE)
- UDP Port 4500

Procedure

1. If necessary, click the expand icon ( ) to display the Virtual Data Centers pane.
2. Select the virtual data center that contains the gateway for which you want to add a VPN connection.
3. Click the Gateways tab.
   The complete list of gateways configured for Virtual Private Cloud OnDemand appears. The virtual data center to which each gateway belongs is displayed next to the gateway name.
4. Click the gateway for which you want to set up an IPsec VPN connection.
5. Click Manage Gateway in vCloud Director.
   The vCloud Director Administration page > Edge Gateway tab appears.
6. Select the gateway name, right-click and choose Edge Gateway Services > VPN tab.
7. Check Enable VPN to enable the VPN networking service for the gateway.
8. Click Add.
   The Add a Site-to-Site VPN configuration dialog appears.
9. Complete the following settings for the IPsec VPN connection:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a name for the connection.</td>
</tr>
<tr>
<td>Description</td>
<td>(Optional) Enter a description for the connection.</td>
</tr>
<tr>
<td>Enable this VPN Configuration</td>
<td>Select the checkbox to enable the connection between the two VPN endpoints.</td>
</tr>
<tr>
<td>Establish VPN to</td>
<td>From the drop-down menu, select a remote network.</td>
</tr>
<tr>
<td>Local Networks</td>
<td>In the text field, select the local network to which the connection applies.</td>
</tr>
<tr>
<td>Peer Networks</td>
<td>Enter the remote network to which the VPN connects.</td>
</tr>
<tr>
<td></td>
<td>Note: Enter a network range (not a specific IP address) by entering the IP address using CIDR format; for example, 192.168.99.0/24.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Local Endpoint</td>
<td>From the drop-down list, select the network that is the local endpoint for the connection. The local endpoint specifies the network in Virtual Private Cloud OnDemand on which the gateway transmits. Typically, the external network is the local endpoint.</td>
</tr>
<tr>
<td>Local ID</td>
<td>Enter the local ID, which is the public IP address of the gateway.</td>
</tr>
<tr>
<td>Peer ID</td>
<td>Enter the peer ID, which is the public IP address of the remote device terminating the VPN connection.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> If the peer IP address is from another organization VDC network, enter the peer’s native IP address. If NAT is configured for the peer, enter the private peer IP address.</td>
</tr>
<tr>
<td>Peer IP</td>
<td>Enter the peer IP, which is the public IP address of the remote device to which you are connecting.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> If NAT is configured for the peer, enter the public IP address that the device uses for NAT.</td>
</tr>
<tr>
<td>Encryption protocol</td>
<td>Select the encryption type from the drop-down list.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> The encryption type you select must match the encryption type configured on the remote site VPN device.</td>
</tr>
<tr>
<td>Shared Key</td>
<td>Enter an alphanumeric string between 32 and 128 characters, which includes at least one uppercase letter, one lowercase letter, and one number.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> The shared key must match the key that is configured on the remote site VPN device.</td>
</tr>
<tr>
<td>MTU</td>
<td>Enter the the maximum transmission units (MTU) for the VPN connection. The MTU is the maximum amount of data that can be transmitted in one packet before it is divided into smaller packets.</td>
</tr>
</tbody>
</table>

For additional information on how to determine the correct values for the VPN connection settings, see “About Setting up an IPsec VPN Connection,” on page 31.

10 Click OK.

The VPN configuration appears in the table.

**What to do next**

You must configure the IPsec VPN connection from both sides of the connection—Virtual Private Cloud OnDemand and your on-premises facility. This procedure details how to configure the connection for Virtual Private Cloud OnDemand. Configure the connection for your on-premises facility.

**SSL VPN for Data Center Extension**

Using Data Center Extension, you can extend your enterprise network to the public cloud (vSphere or vCloud Director), allowing you to move virtual machines from your private cloud to Virtual Private Cloud OnDemand while retaining the same IP addresses and MAC addresses. Data Center Extension is a Layer 2 extension from your existing enterprise network to Virtual Private Cloud OnDemand over a secure SSL VPN connection. Once you are done, you can consume and manage your moved virtual machines by using their same IP addresses and MAC addresses.

**Note** To use Data Center Extension with Virtual Private Cloud OnDemand, you must purchase a VMware vCloud Connector Advanced Edition license.

With Data Center Extension, you can extend your existing IP address range from your on-premise data center into Virtual Private Cloud OnDemand without the need to change your applications. Data Center Extension uses an SSL VPN between two gateways thus bridging the two sites; you are not running VXLAN over a WAN.
See the following use cases for using Data Center Extension with Virtual Private Cloud OnDemand:

- When you have licenses tied to MAC addresses
- Your virtual machine applications have dependencies on IP addresses or MAC addresses
- You lack DNS control, which prevents DNS updates
- To avoid invalidating existing security rules or the need to re-configure access control lists

Data Center Extension has the following requirements.

- Extended Network Considerations:
  - Extended virtual machines use the on premise gateway.
  - All network traffic traverses the SSL VPN connection.
- Microsoft Active Directory Sites and Services:
  - The extended network is part of the on premise site in Active Directory.
  - DNS and Active Directory communication with vCloud servers traverses the SSL VPN connection.
  - You cannot split a network between sites.
- vApp Limitations:
  - An extended network supports 128 virtual machines per vApp.
  - An extended network supports power operations for one vApp.
    You can perform power operations simultaneously on all virtual machines contained in a vApp.

Related Information

See Stretch Deploy a VM from a Private vCloud Director Cloud to a Public vCloud in Using vCloud Connector for the tasks required to set up Data Center Extension for Virtual Private Cloud OnDemand.

See Data Center Extension to VMware vCloud Air, a VMware technical whitepaper for more information.
Network Connectivity for Virtual Machines

When deploying a virtual machine from Virtual Private Cloud OnDemand, the virtual machine is created without a network. A virtual machine without a network is isolated from communicating with other virtual machines and servers both in and outside of the service.

When you create a virtual machine, you have the choice of assigning the virtual machine to a routed network or to an isolated network. An isolated network does not have Internet connectivity. Isolated networks have an internal subnet assigned and an IP Range from which virtual machines can obtain IP addresses.

When you create a virtual machine, you have the following choices for how the virtual machine obtains an IP address:

- **DHCP**: if you use DHCP to get an IP address from the DHCP pool, the gateway functions as a DHCP router.
- **Static IP Pool**: by choosing to obtain an IP address from the Static IP Pool, the virtual machine gets an IP address from the range configured for the network.
- **Static Manual**: you enter the IP address manually when creating the virtual machine and specifying the networking configuration.

**NOTE** To use the Static IP Pool or Static Manual networking options, VMware Tools must be installed on the virtual machine you are creating. You can use DHCP to provide an IP address regardless of whether VMware Tools are installed on a virtual machine.

See “Allocation of IP Addresses,” on page 11 for more information about how you allocate IP addresses to virtual machines.

For information about VMware Tools, see the following documentation:

- **Installing VMware Tools** in vCloud Director User’s Guide
- **Installing and Configuring VMware Tools** in the VMware Tools Installation and Configuration Guide

This chapter includes the following topics:

- “Connect a Virtual Machine to a Network,” on page 38
- “Change Network Assignments for a Virtual Machine,” on page 38
- “Connect a Virtual Machine to the Internet,” on page 39
Connect a Virtual Machine to a Network

You can connect virtual machines to isolated networks or routed networks in your virtual data center. To get connectivity to the Internet and to use networking services such as NAT, firewall, or load balancing, connect virtual machines to a routed network.

When you connect a virtual machine to a network, it is assigned an IP address from the network’s predefined private IP address range.

Prerequisites

You have the required permission to manage the virtual machine. Administrators can connect all virtual machines in their Virtual Private Cloud OnDemand environment to networks; while an end user can connect only the virtual machines that the user owns to networks. The owner of the virtual machine is the user who created the virtual machine or who was transferred ownership of the virtual machine.

Procedure

1. Select the virtual machine to be connected to a network.
2. If the virtual machine is powered on, select it and click Power Off.
3. From the virtual machines list, click the virtual machine name.
4. Click the Networks tab.
5. Click Add a Network.
6. Select a network from the list of networks.
7. When selecting more than one network for the virtual machine, specify the virtual machine’s primary network by clicking the Primary NIC option for that network. By default, the primary network is set to the first network you selected for the virtual machine.
8. Click Save.

Change Network Assignments for a Virtual Machine

You can change the network assignment of a virtual machine or connect it to more networks.

Prerequisites

You have the required permission to manage the virtual machine. Administrators can change network assignments of all virtual machines in their Virtual Private Cloud OnDemand environment; while an end user can change network assignments of only the virtual machines that the user owns. The owner of the virtual machine is the user who created the virtual machine or who was transferred ownership of the virtual machine.

Procedure

1. Select the virtual machine for which you want to change the network assignment.
2. If the virtual machine is powered on, select it and click Power Off.
3. Click the virtual machine name.
4. Click the Networks tab.
5. Click Edit Network Assignment.
   The Edit Networks dialog appears.
6 Set the new network assignments:
   - Select a new network for the virtual machine.
   - Deselect a network to disconnect the virtual machine from it.

7 When selecting more than one network for the virtual machine, specify the virtual machine’s primary network by clicking the Primary NIC option for that network. By default, the primary network is set to the first network you selected for the virtual machine.

8 Click Save.

Connect a Virtual Machine to the Internet

You can connect virtual machines to routed networks in your virtual data center so that the virtual machines have access to the Internet.

When you connect a virtual machine to a network, it is assigned an IP address from the network’s predefined private IP address range.

**Important** By default, gateways are deployed with firewall rules configured to deny all network traffic to and from the virtual machines on the routed networks. Also, NAT is disabled by default so that gateways are unable to translate the IP addresses of the incoming and outgoing traffic. You must configure both firewall and NAT rules on a gateway for the virtual machines on a routed network to be accessible. Attempting to ping a virtual machine on a network after configuring a NAT rule will fail without adding a firewall rule to allow the corresponding traffic.

**Prerequisites**
Verify that you have network administrator privileges.

**Procedure**
1 Select the virtual machine for which you want Internet access.
2 If the virtual machine is powered on, select it and click Power Off.
3 Click the virtual machine name.
4 Click the Networks tab.
5 If the virtual machine is not connect to a network, click Add a Network. Otherwise, click Edit Network Assignments.
6 Select a routed network from the list of networks.

    **Note** You can select more than one network to which to connect the virtual machine.

7 When selecting more than one network for the virtual machine, specify the virtual machine’s primary network by click the Primary NIC option for that network. By default, the primary network is set to the first network you selected for the virtual machine.
8 Click Save.
9 Create a NAT rule to translate the external network address and isolated network address of the virtual machine so that it can receive network traffic from the Internet.

    See “Add a NAT Rule” in the vCloud Air – Virtual Private Cloud OnDemand Networking Guide for the steps to create a NAT rule for the virtual machine.
10 Create a firewall rule to allow the gateway to send and receive Internet traffic for the virtual machine.

    See “Add a Firewall Rule” in the vCloud Air – Virtual Private Cloud OnDemand Networking Guide for the steps to create a firewall rule allowing Internet access for the virtual machine.
Index

A
add networks 20
allocation, public IP addresses 25
antivirus appliances 17

B
bandwidth 8

C
CIDR, firewall rules 29

D
Data Center Extension 34
default firewall setup 29
isolated network 8
routed network 8
setup 8
destination NAT 13
DHCP
changing DNS settings 16
IP addresses 11
IP pools 14
overview 14
virtual machines 37
DMZ 17
DNS
external servers 16
overview 16
dynamic routing 31

E
encryption 33
external network
NAT 13, 23
static routing 17

F
firewall
adding rules 21, 29
default setup 29
IPsec 33
overview 29

gateways
adding networks 22
allocating public IP addresses 25
compact configuration 8
default IP address 8
default setup 8
DNS servers 16
high availability 8
interfaces 8
IP addresses 15
links to advanced management 21
load balancer 15
local ID 31
networking services 12
viewing 21
VPN connections 31
glossary 5

H
high availability 8

I
ICMP type 23
intended audience 5
interfaces, primary NIC 39
internal networks, default setup 8
Internet
connectivity 8
secure connectivity 30
virtual machine access 39
IP addresses
allocating public 25
DHCP 14
free or allocated 21
overlapping 31
peer 31
public 11
static 11
static pool 37
suballocation from multiple subnets 11
Virtual Private Cloud OnDemand 11
IP pools 8
IP ranges
suballocated 15
<table>
<thead>
<tr>
<th><strong>virtual machines</strong></th>
<th>37</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>virtual machines using</strong></td>
<td>38</td>
</tr>
<tr>
<td><strong>IP range,</strong> See IP Ranges</td>
<td></td>
</tr>
<tr>
<td><strong>IP Ranges</strong></td>
<td>11</td>
</tr>
<tr>
<td><strong>IPsec</strong></td>
<td></td>
</tr>
<tr>
<td>encryption</td>
<td>33</td>
</tr>
<tr>
<td>overview</td>
<td>31</td>
</tr>
<tr>
<td>setup</td>
<td>33</td>
</tr>
<tr>
<td>setup overview</td>
<td>31</td>
</tr>
<tr>
<td><strong>IPsec VPN,</strong> overview</td>
<td>30</td>
</tr>
<tr>
<td>isolated networks</td>
<td></td>
</tr>
<tr>
<td>DHCP</td>
<td>14</td>
</tr>
<tr>
<td>security</td>
<td>27</td>
</tr>
</tbody>
</table>

**L**

<table>
<thead>
<tr>
<th><strong>layer 2 networking</strong></th>
<th>34</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>load balancer</strong></td>
<td>15</td>
</tr>
<tr>
<td><strong>local endpoints</strong></td>
<td>31</td>
</tr>
<tr>
<td><strong>local ID</strong></td>
<td>31</td>
</tr>
</tbody>
</table>

**M**

| **multi-interface mode** | 8 |

**N**

<table>
<thead>
<tr>
<th><strong>NAT</strong></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>adding rules</td>
<td>21, 23</td>
</tr>
<tr>
<td>example</td>
<td>13</td>
</tr>
<tr>
<td><strong>IPsec</strong></td>
<td>31</td>
</tr>
<tr>
<td>networking</td>
<td></td>
</tr>
<tr>
<td>components</td>
<td>8</td>
</tr>
<tr>
<td>infrastructure</td>
<td>7</td>
</tr>
<tr>
<td><strong>layer 2</strong></td>
<td>34</td>
</tr>
<tr>
<td>managing</td>
<td>19</td>
</tr>
<tr>
<td>overview</td>
<td>7</td>
</tr>
<tr>
<td>privileges</td>
<td>19</td>
</tr>
<tr>
<td>security</td>
<td>27</td>
</tr>
<tr>
<td>segmentation</td>
<td>27</td>
</tr>
<tr>
<td>software defined data center</td>
<td>7</td>
</tr>
<tr>
<td>software stack</td>
<td>7</td>
</tr>
<tr>
<td>subnets</td>
<td>31</td>
</tr>
<tr>
<td>virtualization</td>
<td>7</td>
</tr>
<tr>
<td>networks</td>
<td></td>
</tr>
<tr>
<td>adding to gateway</td>
<td>22</td>
</tr>
<tr>
<td>changing assignments</td>
<td>38</td>
</tr>
<tr>
<td>deleting</td>
<td>22</td>
</tr>
<tr>
<td><strong>peer</strong></td>
<td>31</td>
</tr>
<tr>
<td><strong>remote</strong></td>
<td>30</td>
</tr>
<tr>
<td>stretched</td>
<td>34</td>
</tr>
<tr>
<td>viewing</td>
<td>19</td>
</tr>
</tbody>
</table>

**O**

| **on-premises,** IPsec configuration | 31 |
| Org VDC networks | |
| DHCP | 14 |
| DNS | 16 |

**P**

| **peer networks** | 31 |
| **peer IP addresses** | 31 |
| **pool servers** | 15 |
| **ports** | |
| firewall rules | 29 |
| NAT | 23 |
| UDP | 33 |
| primary NIC | 39 |
| public IP addresses | |
| allocating | 11 |
| limits | 25 |
| public IP addresses, allocating | 25 |

**R**

| **related documentation** | 12 |
| **remote site,** connectivity | 33 |
| **routed networks** | |
| DHCP | 14 |
| security | 27 |

**S**

| **security,** benefits | 27 |
| **server pools** | 15 |
| software defined data center | 7 |
| source NAT | 13 |
| SSL VPN | 34 |
| static routing | 17 |
| suballocate IP ranges | 15 |

**T**

| **third-party appliances** | 17, 27 |
| **threat mitigation** | 27 |

**U**

| **unicast traffic** | 31 |

**V**

| **vApps** | 34 |
| **vCloud Director** | |
| configuring network services | 12 |
| IPsec configuration | 31 |
| static routing | 17 |
| vCloud Networking and Security Edge Gateway | 8 |
| virtual machines | |
| connecting to networks | 38 |
DHCP 37
editing networks 38
virtual servers 15
virtual data centers
  deleting networks 22
  viewing networks 19
Virtual Private Cloud OnDemand service,
  security 27
virtualization 7
VMware Tools 37
VPN
  enabling 33
  overview 30
  setup 33
vSphere 7

X
XVLAN 7, 8