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.
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 Public IP Addresses 12
   About Networking Services for Gateways 13
   Network Address Translation (NAT) 14
   DHCP 16
   Load Balancer 16
   DNS 17
   Static Routing 18

2 About Managing Gateways and Networks 21
   View and Edit Gateway Details 21
   Add a Gateway to a Virtual Data Center 22
   Delete a Gateway 23
   View Networks in a Virtual Data Center 23
   Add a Network to a Virtual Data Center 23
   View Networks for a Gateway 24
   Add a Network to a Gateway 25
   Delete a Network 25
   Add a NAT Rule 26

3 Network Security and Secure Access 29
   About Network Security 29
   About Firewall Rules 31
   Add a Firewall Rule 31
   VPN and Remote Networks 32
   About IPsec VPN 33
   About Setting up an IPsec VPN Connection 33
   Set up an IPsec VPN Connection to a Remote Site 35
   SSL VPN for Data Center Extension 36

4 Network Connectivity for Virtual Machines 39
   Connect a Virtual Machine to a Network 40
   Change Network Assignments for a Virtual Machine 40
   Connect a Virtual Machine to the Internet 41

5 Direct Connect for vCloud Air 43
   Features of Direct Connect 43
About this Networking Guide

The vCloud Air Networking Guide provides information about configuring networking and gateways for VMware® vCloud Air (formerly known as vCloud Hybrid Service), including how to add gateways to virtual data centers, add networks to gateways, and set up network security by using the gateway's networking services.

Additionally, this guide describes how to set up secure access to vCloud Air from remote sites.

Intended Audience

This guide is intended for network administrators and virtual administrators who will be configuring networking in vCloud Air. 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 vCloud Air:

- See vCloud Air User’s Guide for information about using the vCloud Air console for all managing virtual machines in your cloud service.
- See vCloud Director Administrator’s Guide for information about performing tasks affecting vCloud Air by using vCloud Director.
- See the vCloud Air Tutorials for information about using many of the vCloud Air features.

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.
vCloud Air networking replicates traditional network technologies and design. Networking in vCloud Air is based on 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 Public IP Addresses,” on page 12
- “About Networking Services for Gateways,” on page 13
- “Network Address Translation (NAT),” on page 14
- “DHCP,” on page 16
- “Load Balancer,” on page 16
- “DNS,” on page 17
- “Static Routing,” on page 18

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 also the My VMware Help (8) for information.

**Default Setup for Gateways and Networks**

The default setup for gateways and networks varies in vCloud Air depending on which service you purchased—Dedicated Cloud service or Virtual Private Cloud service.


With both services, you configure networks for each virtual data center. Virtual data centers use the VMware vCloud Networking and Securityy Edge Gateway (referred to as “the gateway” in this guide) to provide external network connectivity. The following components comprise the default setup for networks and gateways in vCloud Air.

VMware manages the external network for connectivity to the Intranet. In vCloud Air, customers create and manage networks (utilizing the embedded VXLAN technology).
Gateways

When you subscribe to a Virtual Private Cloud service, VMware creates your virtual data center for you and adds a gateway to that virtual data center. When you subscribe to a Dedicated Cloud service, you log into the vCloud Air console and create your first virtual data center. When you allocate a public IP address to your virtual data center, vCloud Air creates a gateway in that virtual data center.

By default, a gateway has the following properties:

- Compact configuration
- High availability enabled
- Multi-interface mode enabled
- An internal network with an internal IP address and subnet

When you subscribe to the Dedicated Cloud service, you can deploy additional gateways in a virtual data center. When you subscribe to the Virtual Private Cloud service, your virtual data center can have only one gateway.

A gateway supports 10 interfaces, but one interface is reserved for access to the external network. You configure networking for a gateway by using the remaining nine interfaces. If a virtual data center requires additional interfaces for its networking configuration, add additional gateways (only possible for the Dedicated Cloud service).

Networks

When you subscribe to the Dedicated Cloud service, you are allocated three public IP addresses to configure access to the Internet. When you subscribe to the Virtual Private Cloud service, you are allocated two public IP addresses. You can purchase additional public IP addresses at any time through your Subscription Services in My VMware.

When VMware creates the virtual data center for your Virtual Private Cloud service or you allocate a public IP address to a virtual data center that you create for your Dedicated Cloud service, the virtual data center has the following networks by default:

- **DATACENTER_NAME-DEFAULT-ROUTED**: a gateway network because it is connected to a gateway and virtual machines on this network can connect to the Internet.
- **DATACENTER_NAME-DEFAULT-ISOLATED**: an internal network that is not connect to a gateway; virtual machines on this network are not reachable through the Internet.

A private IP address pool is assigned to each network.
Default Settings for Gateway Networks

By default, vCloud Air creates a gateway network when you assign a public IP address to a virtual data center or gateway and configures it with the following properties:

- Named `DATACENTER_NAME-DEFAULT-ROUTED`
- Connects to the gateway through the public IP address
- Created on the 192.168.109.0 subnet
- Has the default gateway IP address 192.168.109.1
- 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

**IMPORTANT** When you initially add a gateway and gateway network in vCloud Air, you will not be able to connect to any virtual machines added to that network and those virtual machines will not be 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 31 and “Add a NAT Rule,” on page 26 in this guide for information.
Default Settings for Internal Networks

An internal network is not connected to a gateway. An internal network has an internal IP address and subnet. Virtual machines attached to an internal network can communicate only with each other.

DHCP is the only service that can be enabled on an internal network. You use DHCP to get IP addresses for your virtual machines. By default, internal networks are created with the following DHCP settings:

- Enabled for the internal network
- A private IP address range of 192.168.0.101 through 192.168.0.254
- A default lease of 1 hour (3600 seconds)
- A maximum lease of 2 hour (7200 seconds)

Most often, you will connect your virtual machines to a gateway network; however, you might need to 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

Summary of Default Settings for Gateways and Networks

The following table summarizes the default configuration for gateways and networks in vCloud Air.

Table 1-1. Summary of Default Settings for Gateways and Networks in vCloud Air

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Networking Resources</td>
<td>DEDICATED CLOUD</td>
</tr>
<tr>
<td>Gateways</td>
<td>Multiple; created by customer</td>
</tr>
<tr>
<td>Available Gateway Interfaces</td>
<td>9 per gateway; multiple gateways supported</td>
</tr>
<tr>
<td>Bandwidth</td>
<td>50 Mbps allocated 1 Gbps burstable</td>
</tr>
<tr>
<td>Public IP Addresses</td>
<td>3 (can purchase more)</td>
</tr>
<tr>
<td>Available Networks on First Log in</td>
<td>None; created by customer (creating your first gateway adds the default networks)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>GATEWAY NETWORK</th>
<th>INTERNAL NETWORK</th>
</tr>
</thead>
<tbody>
<tr>
<td>Available Networking Services</td>
<td>Firewall: enabled; deny all traffic</td>
</tr>
<tr>
<td>Internet Access</td>
<td>Yes—through the connection to gateway public IP address</td>
</tr>
<tr>
<td>IP Address for the Default Gateway</td>
<td>192.168.109.1</td>
</tr>
<tr>
<td>Subnet</td>
<td>192.168.109.0/24</td>
</tr>
</tbody>
</table>
Allocation of Public IP Addresses

When you subscribe to vCloud Air, you are given public IP addresses as part of the subscription service with both offerings. You can purchase additional public IP addresses at any time through your Subscription Services in My VMware.

- Dedicated Cloud service—3 public IP addresses
- Virtual Private Cloud service—2 public IP addresses

Allocate public IP addresses to a virtual data center only when you want to create virtual machines that need access to the Internet. When you allocate public IP addresses, they are reserved for the virtual data center.

In vCloud Air, you have three ways to assign an IP address to a virtual machine:

- IP Pool: whenever you attach a virtual machine to a network, the virtual machine gets an IP address from the IP Pool created for that network.
  - vCloud Air creates pools of IP addresses by default on the auto-generated internal and gateway networks.
  - Virtual machines attached to those networks get an IP address from the default pool.
  - To change the IP pool for a default network, you must use vCloud Director.

**Note** Gateways in vCloud Air 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.
  - Change the configuration in vCloud Director.

You can view the public IP addresses you have allocated to a gateway by clicking the Gateways tab from the vCloud Air Dashboard, clicking the gateway for which you want 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 Pool configured for a network by clicking the virtual data center in the Dashboard > Networks tab, as shown in the following screenshot:
When you add a network in vCloud Air, you configure the IP Pool for that network, as shown in the following screenshot:

Add Network

VPC cloud: bmw-dc-124744
Virtual data center: AMAR_VDC_D1D
Network name:
Description:

Routed through VDC gateway

Select VDC gateway: Select VDC Gateway
Default gateway IP:
Subnet mask:
P Range

Add Network

See “Add a Network to a Virtual Data Center,” on page 23 and “Add a Network to a Gateway,” on page 25 in this guide for information.

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
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
  - Translated (Internal) IP/Range: 10.0.0.2

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 in to 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 [GUID-B97D00F7-1E61-4FDD-B8FB-78FDEC59F506#GUID-B97D00F7-1E61-4FDD-B8FB-78FDEC59F506](#) in this guide for the steps to create a SNAT or DNAT rule
See GUID-4A9EF77F-0E90-428C-8C4E-DA1E72AAE934 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 vCloud Air support load balancing for the virtual machines connected to gateway networks.

In vCloud Air, 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).

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, perform 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 vCloud Air Dashboard > gateway name > Public IP 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 Pool configured for the gateway. (A gateway uses the Sub-allocated IP Pool for NAT configuration. A Sub-allocated IP Pool contains a sub-set of IP addresses from the IP Pool that is already assigned to the gateway’s external network.)

Navigate from vCloud Air to the following area of vCloud Director:

vCloud Air Dashboard > Gateway tab > gateway name > Manage Advanced Gateway Settings > vCloud Director Administration page > Edge Gateway tab > select the gateway, right-click and choose Properties > Sub-Allocate IP Pools tab


2. 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 above.

Navigate from vCloud Air to the following area of vCloud Director:

vCloud Air Dashboard > Gateways tab > Manage Advanced Gateway Settings > 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 31 in this guide for information.

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

Related Information

See also Introduction to Gateway Services: Load Balancing in the vCloud Air Tutorials for the steps to set up load balancing for a gateway in vCloud Air.

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


**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 16 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 1-4. Example of Static Routing in Virtual Private Cloud OnDemand**

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

**Note** You cannot register static routes with duplicate networks; for example, you cannot add static routes using the longest prefix matching protocol.

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
The vCloud Air console is the primary portal for managing gateways and networks. Additionally, you can use vCloud Director to manage your gateways and networks at a more granular level. The vCloud Air console provides single sign-on access to vCloud Director.

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

This chapter includes the following topics:

- “View and Edit Gateway Details,” on page 21
- “Add a Gateway to a Virtual Data Center,” on page 22
- “Delete a Gateway,” on page 23
- “View Networks in a Virtual Data Center,” on page 23
- “Add a Network to a Virtual Data Center,” on page 23
- “View Networks for a Gateway,” on page 24
- “Add a Network to a Gateway,” on page 25
- “Delete a Network,” on page 25
- “Add a NAT Rule,” on page 26

View and Edit Gateway Details

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

For each gateway, you can view the virtual data center, gateway IP address, compact or full configuration, VMware vSphere High Availability settings, the number of networks connected to it, and the number of used and free public IP addresses.

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. Click the Gateways tab.
   
   All gateways are listed. The virtual data center to which each gateway belongs is displayed next to the gateway name.

2. Click a gateway to access its details.

3. In the upper right of the pane, view the gateway IP, configuration, VMware High Availability settings, and the activity status.

4. View and configure gateway details.

<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 free or allocated.</td>
</tr>
</tbody>
</table>

5. Use links for advanced management of gateways.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Edit Name &amp; Description</td>
<td>Modify the name and description of the gateway.</td>
</tr>
<tr>
<td>Delete Gateway</td>
<td>Deletes the gateway from vCloud Air and removes all configured networking services for the gateway, such as NAT rules, firewall rules, load balancing, and the networks added for that gateway.</td>
</tr>
<tr>
<td>Manage Gateway in vCloud Director</td>
<td>Click Manage Advanced Gateway Settings to go to vCloud Director to manage settings such as changing from compact configuration, disabling High Availability, or configuring rate limits.</td>
</tr>
</tbody>
</table>

Add a Gateway to a Virtual Data Center

You can add additional gateways to a virtual data center after you create the virtual data center. A gateway provides connectivity to the Internet and also provides networking services such as NAT, firewall protection, load balancing, and IPsec VPN. Virtual machines connect to the gateway through a gateway network.

You can add gateways to virtual data centers in the Dedicated Cloud service only. You cannot add gateways in the Virtual Private Cloud service.

Gateways are created with a compact configuration and have High Availability enabled.

Prerequisites

Verify that you have network administrator privileges.

Procedure

1. In the Dashboard tab, click the virtual data center.

2. Click the Gateways tab.

3. Click Add a Gateway or, if the virtual data center already has a gateway, click Add One.

4. Type a name and description for the gateway.
5 Specify the number of IP addresses that you want to allocate to the gateway.

6 Click Add Gateway.

The gateway is created. You can click on the gateway to view its details.

Delete a Gateway

You can delete gateways from virtual data centers in the Dedicated Cloud service. When you delete a gateway, all gateway networks associated with it are deleted. Networking services such as NAT rules, firewall settings, and load balancing settings are also deleted.

You delete gateways from the vCloud Director console.

Prerequisites
Verify that you have network administrator privileges.

Procedure
1 In the Dashboard tab, click the virtual data center that contains the gateway.
2 Click the Gateways tab.
3 Click Manage in vCloud Director.
4 Click the Edge Gateways tab if it is not already selected.
5 Right-click the gateway name and select Delete.

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 gateway 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 In the Dashboard tab, click the virtual data center.
2 Click the Networks tab.
   All networks in the virtual data center are listed.

Add a Network to a Virtual Data Center

You can add additional internal or gateway networks to virtual data centers. Gateway networks can only be added to virtual data centers that have a gateway.

Prerequisites
Verify that you have network administrator privileges.

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
Procedure

1 In the **Dashboard** tab, click the virtual data center to which you want to add a network.
2 Click the **Networks** tab.
3 Click **Add One**.
   
   The Add Network dialog box appears.
4 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>
</tbody>
</table>
| **Routed through VDC gateway** | (Optional) Select this option to create a gateway network; create a gateway network when the virtual machines on the network need access to the Internet. If you do not select this option, an internal network is added to the virtual data center.  
   **NOTE** This option is only available when the virtual data center has at least one gateway. |
| VDC gateway             | 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. |
| Network Gateway         | Enter the gateway IP address for the network.                             |
|                         | **NOTE** Entering a gateway IP address is required even when adding an internal (isolated) network because internal networks are dependent on a gateway for DHCP networking services. If you are adding an internal network, entering a gateway address in this field does not affect the network's isolated status. |
| Subnet mask             | Enter the subnet mask for the IP Pool for this network. When you attach a virtual machine to a network, the virtual machine gets an IP address from the IP Pool created for that network.  
   **See “Allocation of Public IP Addresses,” on page 12 for more information.** |
| IP Range                | Enter the IP address range for the IP Pool for this network.               |

5 Click **Add Network**.

**View Networks for a Gateway**

You can view all the networks that are attached to a gateway.

**Prerequisites**

Verify that you have network administrator privileges.

**Procedure**

1 Click the **Gateways** tab.
2 Click the gateway whose networks you want to view.
3 Click the **Networks** tab.
   
   All gateway networks attached to the gateway are listed.
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. From the Dashboard tab, click the Gateways tab.
2. Click the gateway for which you want to add a network.
3. Click the Networks tab.
   - All networks in the gateway are listed.
4. Click Add One.
   - The Add Network dialog box 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 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 Pool for this network. When you attach a virtual machine to a network, the virtual machine gets an IP address from the IP Pool created for that network. See “Allocation of Public IP Addresses,” on page 12 for more information.</td>
</tr>
<tr>
<td>IP Range</td>
<td>Enter the IP address range for the IP Pool for this network.</td>
</tr>
</tbody>
</table>

**Note** The Routed through VDC gateway and VDC gateway fields are completed for you automatically.
6. Click Add Network.

Delete a Network

You can delete internal or gateway 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. In the **Dashboard** tab, click the virtual data center from which you want to delete a network.

   Alternatively, if you are deleting a gateway network, you can navigate to the gateway and delete the network there. Click the **Gateway** tab > select the gateway that contains the network you want to delete > click the **Network** tab.

2. Click the **Network** tab.

   The list of networks appears.

3. For the network you want to delete, click the drop-down arrow and select **Delete Network**.

   A dialog box appears reminding you to disconnect all the virtual machines from the network before deleting it.

4. Click **Yes**.

   The network is deleted and a confirmation message appears at the top of the vCloud Air console.

**Add a NAT Rule**

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

You configure NAT rules in the following ways:

- **SNAT**: the traffic is traveling from a virtual machine on an internal network in vCloud Air (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 vCloud Air (the destination).

See “**Network Address Translation (NAT)**” on page 14 in this guide for more information.

This procedure provides the steps to create a NAT rule by using vCloud Air. 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. In the **Dashboard** tab, click the **Gateways** tab.

2. Click the gateway for which you want to add a NAT rule.

3. Click the **NAT Rules** tab.
4 Click the **Add** button and from the drop-down menu, choose one of the following options:

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

5 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><strong>Original (Internal) Source</strong></td>
<td>Enter the original IP address or range of IP addresses to apply to this rule. These 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><strong>Translated (External) Source</strong></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. This 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 list.</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Original (External) IP</strong></td>
<td>Specifies the destination IP address to which the rule applies; this 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 list.</td>
</tr>
<tr>
<td><strong>Protocol</strong></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><strong>Original Port/Range</strong></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><strong>ICMP type</strong></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><strong>Translated (Internal) IP/Range</strong></td>
<td>Enter the IP address or a range of IP addresses to which destination addresses on inbound packets will be translated. These 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><strong>Translated Port/Range</strong></td>
<td>(Optional) Enter the port or port range that traffic connects to on the virtual machines on the internal network.</td>
</tr>
</tbody>
</table>

6 Select **Enable this rule** and click **Save**.
vCloud Air provides features and functionality to ensure network security and secure access to your resources in the cloud.

This chapter includes the following topics:

- “About Network Security,” on page 29
- “About Firewall Rules,” on page 31
- “Add a Firewall Rule,” on page 31
- “VPN and Remote Networks,” on page 32
- “About IPsec VPN,” on page 33
- “About Setting up an IPsec VPN Connection,” on page 33
- “Set up an IPsec VPN Connection to a Remote Site,” on page 35
- “SSL VPN for Data Center Extension,” on page 36

### 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>REQUIRED FOR</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>BENEFITS</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>- 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>

**NOTE** You can have an instance of a dual NIC on a virtual machine and connect one interface of the virtual machine to the routed network and the other interface to the isolated network.
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**

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 to 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. (vCloud Air does not require configuring security groups like some of the other cloud providers.) You configure firewall rules to manage the traffic flowing in and out of your vCloud Air cloud. Additionally, you can configure firewall rules to secure network traffic between any and all interfaces on a gateway.

Firewall rules in vCloud Air 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 gateway 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 31 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
- Introduction to Gateway Services: Firewall in the vCloud Air Tutorials
- “Configure Firewall and NAT Rules” in VMware vCloud Air Solution Brief

Add a Firewall Rule

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

This procedure provides the steps to create a firewall rule by using vCloud Air. 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 addresses for the virtual machines that you are creating the firewall rule.

Procedure

1. In the **Dashboard** tab, click the **Gateways** tab.
2. Click the gateway for which you want to add a firewall rule.
3. Click the **Firewall Rules** tab.
4. Click the **Add** button.
   
   The Add a Firewall “Allow” Exception dialog box appears.
5 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 Enable this to enable the rule for the gateway. Note: Selecting the Log network traffic for this exception option is unnecessary because you cannot access firewall logging data in vCloud Air at this time.</td>
</tr>
<tr>
<td>Protocol</td>
<td>Choose a protocol to which the rule applies from the drop-down menu: any, TCP, UDP, TCP/UDP, or ICMP. By default, the protocol is set to “any” so that network traffic from all protocols will traverse the firewall.</td>
</tr>
<tr>
<td>Source</td>
<td>Choose an option from the drop-down menu: Any: allows traffic from any source on the external network to reach the virtual machines. Internal: apply this rule to all internal traffic. External: apply this rule to all external traffic. Specific CIDR, IP, or IP Range: type the CIDR notation of traffic to 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 reach your virtual machines on your internal network.</td>
</tr>
<tr>
<td>Destination</td>
<td>Choose an option from the drop-down menu: Any: allows traffic from any virtual machine on your internal network to access the external network. Internal: apply this rule to all internal traffic. External: apply this rule to all external traffic. Specific CIDR, IP, or IP Range: type the CIDR notation of traffic to 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 your virtual machines to reach the external network.</td>
</tr>
</tbody>
</table>

6 Click Save.

VPN and Remote Networks

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

vCloud Air supports Internet, secure VPN, and Direct Connect secure connections between your remote site and the vCloud Air cloud.

Each type of connection has different security features:

- Secure Internet connectivity with firewall rules (a gateway service)
  See “About Firewall Rules,” on page 31 in this guide for information.

- Secure VPN:
  - IPsec VPN—secure site-to-site VPN
    See “About IPsec VPN,” on page 33 and “Set up an IPsec VPN Connection to a Remote Site,” on page 35 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 36 in this guide for information.

- Direct Connect—private connectivity providing a dedicated, connection (ideal for regulated applications)
Create an IPsec VPN connection by using vCloud Air 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 supports using IPsec to create a secure VPN connection between your vCloud Air service 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 35 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 vCloud Air and between a remote site and vCloud Air. Setting up an IPsec VPN connection from a remote network to vCloud Air is the most common scenario.
Using vCloud Director, you configure an IPsec VPN connection for vCloud Air 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, 192.168.1099.0/24.

- **Local Endpoint (LEP)**: specifies the network in vCloud Air 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. Typically, the local ID is the public IP address.

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

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

![Diagram of IPsec VPN configuration](image)

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 above, the peer ID and peer IP for the vCloud Air 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 another device, specifically 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 vCloud Air 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 vCloud Air and a remote site. In this procedure, you configure the vCloud Air 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 vCloud Air.

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. In vCloud Air, click the Gateways tab.
   
The complete list of gateways configured for vCloud Air appears. The virtual data center to which each gateway belongs is displayed next to the gateway name.

2. Click the gateway for which you want to set up an IPsec VPN connection.

3. Click Manage Advanced Gateway Settings under the In vCloud Director heading.
   
The vCloud Director Administration page > Edge Gateway tab displays.

4. Select the gateway name, right-click and choose Edge Gateway Services > VPN tab.

5. Check Enable VPN to enable the VPN networking service for the gateway.

6. If necessary, click Configure Public IPs to add a public IP address for the external network.

7. Click Add.
   
The Add a Site-to-Site VPN configuration dialog box appears.

8. 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 networks to which the VPN connects.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong>: 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 vCloud Air 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>
</tbody>
</table>
| Peer ID         | Enter the peer ID, which is the public IP address of the remote device terminating the VPN connection.  
|                 | **Note**: 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. |
| Peer IP         | Enter the peer IP, which is the public IP address of the remote device to which you are connecting.  
|                 | **Note**: If NAT is configured for the peer, you enter the public IP address that the devices uses for NAT.                                                                                         |
| Encryption protocol | Select the encryption type from the drop-down list.  
|                 | **Note**: The encryption type you select must match the encryption type configured on the remote site VPN device.                                                                                 |
| Shared Key      | Enter an alphanumeric string between 32 and 128 characters, which includes at least one uppercase letter, one lowercase letter, and one number.  
|                 | **Note**: The shared key must match the key that is configured on the remote site VPN device.                                                                                                      |
| MTU             | 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.                                                                        |

9 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—vCloud Air and your on-premises facility. This procedure details how to configure the connection for vCloud Air. 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 vCloud Air while retaining the same IP addresses and MAC addresses. Data Center Extension is a Layer 2 extension from your existing enterprise network to vCloud Air 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 vCloud Air, 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 vCloud Air 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 vCloud Air:

- 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 vCloud Air.

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 vCloud Air, 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 gateway network or to an internal network. An internal network does not have Internet connectivity. Internal networks have an internal subnet assigned and an IP Pool 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.

Related Information

See “Allocation of Public IP Addresses,” on page 12 for more information about how you allocate IP addresses to virtual machines.

For information about VMware Tools, see the following VMware documentation:

- [Installing VMware Tools in vCloud Director User’s Guide](#)
- [Installing and Configuring VMware Tools](#)

This chapter includes the following topics:

- “Connect a Virtual Machine to a Network,” on page 40
- “Change Network Assignments for a Virtual Machine,” on page 40
- “Connect a Virtual Machine to the Internet,” on page 41
Connect a Virtual Machine to a Network

You can connect virtual machines to internal networks or gateway 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 gateway network.

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

Prerequisites

Verify that you have end user or virtual infrastructure administrator privileges.

Procedure

1. Locate the virtual machine to be connected.
   a. If you are a virtual infrastructure administrator, click the virtual data center that contains the virtual machine and the Virtual Machines tab.
   b. If you are an end user, in My Virtual Machines, select the virtual machine.

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 Add a Network.

6. Select a 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 machines 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.

Change Network Assignments for a Virtual Machine

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

Prerequisites

Verify that you have network administrator privileges.

Procedure

1. In the Dashboard tab, click the virtual data center that contains the virtual machine.

2. Click the Virtual Machines tab.

3. If the virtual machine is powered on, select it and click Power Off.

4. Click the name of the virtual machine.

5. Click the Networks tab, and click Edit Network Assignment.

6. Set the new network assignments:
   - Select a new network for the virtual machine.
   - Deselect a network to disconnect the virtual machine from it.
Connect a Virtual Machine to the Internet

You can connect virtual machines to gateway 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 pool.

**Important** 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 both firewall and NAT rules on a gateway for the virtual machines on a gateway 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. Locate the virtual machine to be connected.
   a. If you are a virtual infrastructure administrator, click the virtual data center that contains the virtual machine and the Virtual Machines tab.
   b. If you are a end user, in My Virtual Machines, select the virtual machine.

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 gateway 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 machines 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 internal network address of the virtual machine so that it can receive network traffic from the Internet.

   See “**Add a NAT Rule**,” on page 26 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**,” on page 31 for the steps to create a firewall rule allowing Internet access for the virtual machine.
Direct Connect for vCloud Air

For vCloud Air, you can order a direct network connection between your premises or colocation center and a vCloud Air region. Using a direct network connection ensures a degree of dedicated bandwidth to a Dedicated Cloud and a Virtual Private Cloud.

In vCloud Air, route traffic from your virtual machines through your direct network connection.

**Note:** Read this section when you have ordered Direct Connect from VMware for your vCloud Air instance. If you are not a Direct Connect customer, you will not see a Direct Connect network in your vCloud Air Web console.

This chapter includes the following topics:
- “Features of Direct Connect,” on page 43
- “Reasons to Order Direct Connect,” on page 44
- “Direct Connect Service Overview,” on page 45
- “Direct Connect with Cross Connect,” on page 46
- “Direct Connect for Network Exchange,” on page 47
- “Direct Connect Use Cases,” on page 48
- “About the Ordering and Provisioning Workflow,” on page 49
- “Work with Your Provider to Set up Connection,” on page 51
- “Order Direct Connect to vCloud Air,” on page 52
- “Work with VMware to Complete Order,” on page 53
- “View Direct Connect in vCloud Air,” on page 54
- “Route Traffic Through Direct Connect,” on page 54

**Features of Direct Connect**

Using a direct network connection to connect your premises or colocation center to your vCloud Air location provides the following key features:
- Dedicated and higher bandwidth between your premises or colocation center and your vCloud Air location. High-speed connections enable hybrid architectures ranging from secure multipoint networks to analytics applications that transfer large amounts of data between data centers.
- Increased security when accessing virtual machines and cloud-based applications running in vCloud Air versus accessing your cloud through the Internet or by using VPN.
When transferring corporate data and customer information, using Direct Connect provides increased security; for example, you require that vCloud Air appear as an extension of your MPLS network or as a secure access location on your corporate network.

- Increased network and application performance due to higher available bandwidth
  Direct Connect can be connected to a dedicated virtual circuit, enabling high-throughput and low-latency connections for performance-sensitive applications.

- Potentially lower cost as the data rate to and from your vCloud Air increases
  Direct Connect allows multiple endpoints to share a dedicated link, simplifying the support of branch and remote offices within the same vCloud Air instance.

- Increased flexibility
  A high-throughput, low-latency connection enables custom architectures in which vCloud Air connects to specialized network, storage, or compute hardware and appliances. Using Direct Connect expands the ways companies can leverage the extended the capacity of vCloud Air.

- Built in high availability architecture
  Direct Connect is configured for high availability with link aggregation group (LAG) redundancy and redundant switches.

### Reasons to Order Direct Connect

Ordering a direct network connection to connect to vCloud Air is often necessary when you are using your cloud in the following ways:

- You plan to run the following types of Web sites by using vCloud Air:
  - High-traffic Web sites with a database or storage on the premises
  - E-commerce applications with PCI compliance requirements

- You plan to run applications in vCloud Air that have the following characteristics:
  - Are time-sensitive
  - Do not allow external access
  - Are regulated
  - Consist of front-end Web services that connect to back-end main frames
  - Are packaged and host internal applications

- You have specific compliance requirements, such as requirements against using VPN ports or private connectivity requirements for government compliance.

- You are running sensitive workloads where network traffic should not pass through the Internet.

Ordering a direct cross connection from your customer cage to vCloud Air in the same data center is often necessary when you have the following requirements:

- You want to use vCloud Air as a capacity extension.

- You require specialized equipment (such as, hardware-based networking, routing, and security solutions, hardware-based application monitoring solutions, or specialized storage or servers) as part of your cloud-based application deployment.
  VMware does not support customer deployment of hardware-based appliances for vCloud Air.

- You want to manage your data (due to privacy or compliance requirements) but still have the data in close proximity to your applications running in the cloud. You require a high-speed cross connection between vCloud Air and your storage solutions (located in your customer cage in the same data center).
Direct Connect Service Overview

VMware delivers Direct Connect jointly with our vCloud Air network partners. The partner network service providers (NSPs)

Customers work with NSPs to set up end-to-end private connections from their locations to vCloud Air. (To set up a connection from a customer cage in the same data center as vCloud Air, customers work with the data center owner to connect to a patch panel in the Meet Me Room.) For connections from remote locations, NSPs provide the circuits to the vCloud Air connection point in the Meet Me Room. VMware provides the port connectivity and the cross connection from the Meet Me Room (the NSP termination point or data center patch panel) to the vCloud Air environment.

Direct Connect supports the following dedicated connection options from your customer premises or co-located equipment:

- “Direct Connect with Cross Connect,” on page 46
- “Direct Connect for Network Exchange,” on page 47

These two options differ primarily around the time in which you can obtain a dedicated connection to vCloud Air.

Connection Components

For both connection options, the connection from your equipment to vCloud Air has two components:

- External to vCloud Air: the connection from your customer location or your co-located equipment in the vCloud Air data center to the termination point in the Meet Me Room within a data center
- Internal to vCloud Air: the connection from the NSP termination point or data center patch panel to your gateway for your vCloud Air service

Figure 5-1. Connection Components for Direct Connect to vCloud Air
The connect from your customer equipment to the vCloud Air switch is configured as an untagged layer 2 connection (VLAN).

Within your vCloud Air cloud, networking is implemented using software-defined networking (VxLAN-based networks).

**Standard Connection versus Direct Connect**

The following table summarizes the differences between the standard connection to vCloud Air and a Direct Connect connection.

<table>
<thead>
<tr>
<th>Table 5-1. Connection Comparison</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Connection Details</strong></td>
</tr>
<tr>
<td>Speed</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Connection Type</td>
</tr>
<tr>
<td>Secure Connection</td>
</tr>
<tr>
<td>Single or Multi-point</td>
</tr>
<tr>
<td>Cost</td>
</tr>
</tbody>
</table>

**Related Documentation**

For additional information about Direct Connect for vCloud Air, see the following documentation and resources:

- **Dedicated Connectivity – Direct Connect** for the following information:
  - The locations from which Direct Connect is available, including the termination addresses and all connection points
  - The list of all Network Service Providers (NSPs) for Direct Connect
  - The list of all Network Exchange Network Service Providers for Direct Connect

- **Getting Started with Direct Connect** for an overview of the set up process

- **Direct Connect Data Sheet** for examples of the types of use cases Direct Connect enables for vCloud Air

- **Direct Connect FAQ** for additional information including what partner options are supported by Direct Connect for vCloud Air (see the question “What deployment architectures are available?”)

- **Cloud Computing Pricing Guide**, which includes pricing for Direct Connect under “Optional Services”

**Direct Connect with Cross Connect**

Direct Connect with Cross Connect supports the following types of connections:

- Connections for customers who want to connect to vCloud Air from remote locations, for example to extend their MPLS connections to vCloud Air for long distance WAN connectivity

- Connections for customers who have a presence in the same data center as vCloud Air and want to cross connect to vCloud Air within that data center

**Site-to-Site Private Line Connectivity**
You can set up your direct network connection to use an end-to-end virtual circuit from your premises.

The type of connection and bandwidth you provision from your site (such as a colocation facility, headquarters, or branch office) to the data center in which vCloud Air is located depends on the capabilities and service catalog from the network service provider you choose to provide the connectivity. For example, you might choose the following technologies to implement your private WAN connection:

- Multiprotocol Label Switching (MPLS)
- Virtual Private LAN Service (VPLS)

For information about the connection options supported by Direct Connect for vCloud Air, see the question “What deployment architectures are available?” in the Direct Connect FAQ.

Your network service provider (NSP) or telecommunications partner manages this connection. The connection bridges your customer premises to your NSP’s terminating switch in the data center where vCloud Air is located. Your NSP is responsible for patching the connection to a port on the vCloud Air switch in the data center Meet Me Room (MMR) or to the carrier termination device, such as the main distribution frame (MDF) for the data center.

**Figure 5-2. Areas of Responsibility for Direct Connect with Cross Connect**

Cross Connections from Co-located Infrastructure

You can set up your direct network connection to use an intra data center cross connect. Cross connect provides directly connected network circuits between your existing pod in the data center and the vCloud Air service in the same facility. Using an intra data center cross connect allows you to connect two physically isolated organizations within the data center; specifically, your customer cage and the vCloud Air infrastructure.

VMware provides one or more access ports for your cage in the data center where you access your vCloud Air service. Cross connect is a point-to-point connection that does not use your network service provider’s equipment to route traffic.

**Direct Connect for Network Exchange**

VMware provides the connection option Direct Connect for Network Exchange.

VMware has partnered with specific NSPs to provide Direct Connect for Network Exchange. VMware and select NSPs offer joint connectivity to bring fast, dedicated, right-sized connectivity to vCloud Air and Horizon Air customers from anywhere on the NSPs’ global MPLS networks.
For the list of all Network Exchange Network Service Providers for Direct Connect and the vCloud Air locations where it is available, see Dedicated Connectivity – Direct Connect.

Direct Connect for Network Exchange provides the following benefits:

- Dedicated connectivity: 1 or 10Gbps options
- Fastest time-to-value; often connections are provisioned in less than 7 days
- Supports access to the vCloud Air Advanced Networking Service
- Supports additional value-added services from NSPs (varies by NSP)

Figure 5-3. Areas of Responsibility with Direct Connect for Network Exchange

Direct Connect Use Cases

The way that you connect your premises to a vCloud Air data center by using Direct Connect can vary depending on your requirements and goals.

- Connection partners

For information about which connection partners have point-of-presence (POP) in the vCloud Air data centers where Direct Connect is available, contact a vCloud Air SE Specialist or VMware Support. Your ability to contract a service provider that does not have a POP in a vCloud Air data center depends on their capabilities. To work with such a provider, the provider must be able to deliver a network-to-network interface (NNI) to the network service providers (or telecommunications carriers that have a POP in the vCloud Air data center.

For the list of all NSPs for Direct Connect, see Dedicated Connectivity – Direct Connect.

- Network hardware

To inquire about using your network equipment located in a colocation cage at a vCloud Air data center, contact a vCloud Air SE Specialist or your VMware sales representative.

- Redundant Direct Connect connections

**NOTE** Customers who have a Dedicated Cloud service can set up redundancy for their direct network connection by ordering two or more SKUs from My VMware. Ordering two or more connections allows you to have redundant connections from the same gateway for vCloud Air to your premises or colocation center.

To provide redundancy, order multiple Direct Connect connections of the same or different speeds to terminate at the same gateway or different gateways; however, you cannot use one Direct Connect connection to terminate at multiple virtual data centers or gateways.
Connecting to multiple vCloud Air offerings

Using one, shared Direct Connect connection to connect from on-premises to multiple vCloud Air offerings (namely, Dedicated Cloud, Virtual Private Cloud, Desktop as a Service (DaaS), and Disaster Recovery as a Service (DRaaS)) is not supported.

To connect multiple vCloud Air offerings, order a cross connection for each of your vCloud Air environments and configure static routing between them. See “Order Direct Connect to vCloud Air,” on page 52 and “Direct Connect Service Overview,” on page 45 for information.

Dynamic routing

Direct Connect supports dynamic routing (for example with OSPF and BGP) for network traffic between on-premises and vCloud Air and between vCloud Air instances.

**NOTE** Configuring dynamic routing with Direct Connect is supported only when you have a vCloud Air Dedicated Cloud subscription service.

Unsupported Use Cases

Direct Connect is not supported for the following implementations:

- Ethernet over copper (EoC) connections
  
  Direct connect does not support your network service provider delivering an EoC connection from your premises to the vCloud Air data center. A Direct Connect connection requires single-mode fiber with a Lucent Connector (LC).

- VLAN trunks and subnets
  
  Direct Connect does not support VLAN trunks or multiple subnets. A Direct Connect connection supports one subnet or VLAN.

- Public IP address porting
  
  vCloud Air does not support using your own public IP address space with Direct Connect.

About the Ordering and Provisioning Workflow

The workflow to order and provision a direct network connection to vCloud Air follows this sequence of hand offs between you, your network service provider (or telecommunications carrier), the data center owner, and your vCloud Air Customer Success Team.

Prerequisites

- Determine which vCloud Air data center you want to connect to.
  
  You can establish a direct network connection between one or multiple vCloud Air locations.

- Determine which type of connection you need:

  - “Direct Connect with Cross Connect,” on page 46
  - Logical private WAN connectivity

  **NOTE** The type of connection you order from your customer premises to the vCloud Air data center (such as MPLS, VPLS, or E-Line) depends on the capabilities and service catalog from the network service provider you choose to provide the connectivity. See also “Direct Connect Use Cases,” on page 48 for the connection requirements.

- Intra data center cross connect
  
  You must have your own colocation equipment in each vCloud Air data center.
High-level Workflow for a Private WAN Connection

The hand-offs between you, your network service provider (or telecommunications carrier), and VMware use the following high-level workflow and timeline.

The following diagram shows the workflow for provisioning a logical private WAN connection. Provisioning an intra data center cross connect (to connect your equipment in your cage within the same data center) follows a similar process except you do not order a circuit from your customer premises.

**Figure 5-4.** Order and Provisioning Workflow and Timeline for Direct Connect with Cross Connect

<table>
<thead>
<tr>
<th>NSP</th>
<th>Customer</th>
<th>VMware</th>
<th>Data center</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set up circuit and provide LOA-CFA</td>
<td>Order circuit from NSP</td>
<td>Order Direct Connect in My VMware</td>
<td>Contact customer about connection</td>
</tr>
<tr>
<td></td>
<td>Order Direct Connect in My VMware</td>
<td>Send connection details and LOA-CFA to CST</td>
<td>Forward LOA-CFA to Network Ops</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Provision port and order cross connect</td>
<td>Provision port and order cross connect</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Meet to test and verify connection</td>
<td>Meet to test and verify connection</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Configure cross-connect to vCA switch</td>
</tr>
</tbody>
</table>

**Figure 5-5.** Direct Connect for Network Exchange Order Process

<table>
<thead>
<tr>
<th>NSP</th>
<th>Customer</th>
<th>VMware</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set up circuit for customer</td>
<td>Order circuit from NSP</td>
<td>Receive connection setup details from NSP portal</td>
</tr>
<tr>
<td></td>
<td>Order Direct Connect through Partner &amp; My VMware</td>
<td>Provision port &amp; assign VLAN in NSP portal</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Set up connection to vCloud Air instance</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Meet to test and verify connection</td>
</tr>
</tbody>
</table>

Details About Implementing a Private WAN Connection

The following steps detail the workflow for provisioning a logical private WAN connection. Provisioning an intra data center cross connect (to connect your equipment in your cage within the same data center) follows a similar process except that you do not order a circuit from your customer premises.

1. Work with your network service provider (or telecommunications carrier) to set up your customer connection to the facility containing vCloud Air.

For information about supported technologies for the connection from your customer premises, see “Direct Connect Use Cases,” on page 48.
For details about setting up your connection to the vCloud Air data center, see “Work with Your Provider to Set up Connection,” on page 51.

NOTE If you require an intra data center cross connection, work with the data center owner to set up the connection from your equipment in your customer cage to vCloud Air.

2 Log into your My VMware account and order Direct Connect to the vCloud Air data center where you want to connect.

See “Order Direct Connect to vCloud Air,” on page 52 for information.

After VMware processes your order, the vCloud Air Customer Success Team provides a Letter of Authorization – Customer Facility Assignment (LOA-CFA) form for your connection set up.

3 VMware will contact you for information to complete the LOA-CFA form. The LOA-CFA provides the cabinet, patch panel, and port number of the vCloud Air equipment. For the list of information VMware requires for the LOA-CFA form, see “Work with VMware to Complete Order,” on page 53.

4 VMware completes the connection and configuration from the NSP’s terminating device or the data center patch panel to the vCloud Air infrastructure in the data center.

5 By working with VMware, participate in a test and verify meeting to validate that the end-to-end connection to vCloud Air is functioning as expected.

The Direct Connect network appears in the vCloud Air Web UI.

6 Log into vCloud Air and view your Direct Connect network details.

See “View Direct Connect in vCloud Air,” on page 54 for information.

7 Route traffic from customer premises (or customer cage depending on your connection) to your virtual machines in vCloud Air.

See “Route Traffic Through Direct Connect,” on page 54 for information.

Work with Your Provider to Set up Connection

When implementing a logical private WAN connection, work with your network service provider to set up a connection from your customer premises to the data center location for vCloud Air.

How you work with your NSP to set up the connection depends on which Direct Connect options you have:

- “Direct Connect with Cross Connect,” on page 46
  Contact your network service provider prior to ordering Direct Connect in My VMware because provisioning the connection from your customer premises to the vCloud Air data center can take up to 90 days.

- “Direct Connect for Network Exchange,” on page 47
  When setting up Direct Connect for Network Exchange, you connect to a pre-established network fabric. Provisioning this connection from your customer location to the vCloud Air data center can take less than 7 days.

You work with your network service provider independently of VMware to enable connectivity from your customer premises to the provider’s endpoint (specifically, the provider’s termination device) in the data center containing vCloud Air.

The network service provider sets up the connection at your facilities and terminates the connection at the vCloud Air data center. Your network service provider completes your connection and hands off the provisioning process to vCloud Air Customer Success Team.

NOTE A customer who needs an intra data center cross connection to vCloud Air works with the data center owner to set up the connection to the vCloud Air connectivity points.
The data centers in which Direct Connect is available provide a Meet Me Room. The Meet Me Room within the data center provides an area where network service providers and telecommunications companies can physically connect to one another and customers, and exchange data without incurring local loop fees.

VMware connects the vCloud Air infrastructure equipment to the Meet Me Room so that customers can choose which network service providers to partner with for the connection from their customer premises to the data center location.

**Order Direct Connect to vCloud Air**

Order a direct network connection by using My VMware to specify the connection options you require.

You order Direct Connect as an add-on SKU to your current Dedicated Cloud or Virtual Private Cloud subscription. The length of your Direct Connect subscription co-terms with your current subscription; for example, if you have ordered a 12 month Dedicated Cloud subscription and you have 6 months remaining for your subscription, your Direct Connect order will remain in effect for the remaining 6 months.

You are billed for your Direct Connect subscription monthly and Direct Connect monthly charges do not include the costs or charges from your network service provider providing the connection from your customer equipment to the vCloud Air data center location. The monthly port connection fee from VMware includes the data center cross connect fee; although additional circuit fees can vary by NSP.

**NOTE** Customers who have the Dedicated Cloud service can set up redundancy for their direct network connection by ordering two or more SKUs from My VMware. Ordering two or more connections allows you to have redundant connections from the same gateway for vCloud Air to your premises or colocation center.

To provide redundancy, order multiple Direct Connect connections of the same or different speeds to terminate at the same gateway or different gateways; however, you cannot use one Direct Connect connection to terminate at multiple virtual data centers or gateways.

**Prerequisites**

Before ordering Direct Connect, you must meet the following prerequisites:

- You have the Account Administrator privilege in vCloud Air.
- You have determined the vCloud Air location to connect to using Direct Connect.
- You have selected a connection partner who has a presence in the vCloud Air data center for which you want to connect.

**NOTE** You have the option to choose a “Direct Connect with Cross Connect,” on page 46 connection or a “Direct Connect for Network Exchange,” on page 47 connection.

- Your connection partner has completed their portion of the connection from your customer cage or customer premises to the connection partner’s terminating device in the data center. See Figure 5-1 for a description of the connection between your customer equipment and the connection partner’s terminating device.

**Procedure**

1. Log into your My VMware portal with your email address or customer number for your My VMware account and enter your password.

   Or

   Log into vCloud Air with your email address and password. From the Dashboard, click Purchase More Resources under Related Links.

   Your My VMware portal appears.

2. Navigate to the Subscription Services.
3. From the **Available Add-ons** tab, select the Direct Connect SKU for the connection you require.

Direct Connect SKUs are available for combinations of the following options:

- Location of the vCloud Air data center where Direct Connect is available
- Your type of vCloud Air service—Dedicated Cloud and Virtual Private Cloud
- For Dedicated Cloud service, a choice of a 10Gbps port or a 1Gbps port

*Note* Direct Connect for Virtual Private Cloud subscriptions are configurable with 1Gbps port speeds only.

4. Click **Buy Now**.

The Add-on Request Order page appears.

5. Agree to the terms and conditions of the order and click **Submit Request**.

A confirmation message appears indicating that your order was submitted successfully and displays your Request ID number.

**What to do next**

Within 24-48 hours, you receive an email confirmation of your order. Your vCloud Air portal indicates that you have ordered a direct network connection from your premises to vCloud Air but the connection has not provisioned in vCloud Air.

After VMware processes your order, your vCloud Air Customer Success Team provides a Letter of Authorization – Customer Facility Assignment (LOA-CFA) form for your connection set up. Deliver the LOA-CFA form from VMware to your connection partner. Your connection partner requires the LOA-CFA form to establish the connection from their equipment to the vCloud Air switch. The LOA-CFA provides the cabinet, patch panel, and port number of the vCloud Air equipment to connect your customer circuit.

**Work with VMware to Complete Order**

After ordering a direct network connection, you work with the vCloud Air Customer Success Team to provide the information necessary to set up the connection within vCloud Air and vCloud Director.

When contacted, provide the following information to the VMware representative:

- The name of the virtual data center that contains the virtual machines to which you will connect
- Direct Connect connectivity option—logical private WAN connection or intra data center cross connection
- Network service provider (or the data center owner when ordering an intra data center cross connection) setting up the connection from your customer equipment
- Which type of connection you require to your virtual machines in vCloud Air:
  - Routed connection—a connection to the virtual machines that is routed through a gateway
  - Direct connection—a direct connection to the virtual machines from the outside network
- For a routed connection only:
  - The name of the gateway for the virtual data center configured in vCloud Air
  - The gateway IP address
  - The gateway subnet mask

All your virtual machines in vCloud Air will use this gateway IP address for Internet connectivity.
IP Pool—Reserve the pool of IP addresses from the Direct Connect subnet

The IP address range to use in vCloud Air

**NOTE** If you have a Dedicated Cloud service and more than one gateway configured for the virtual data center containing the Direct Connect network, determine which gateway to use to terminate the Direct Connect connection. You cannot use one Direct Connect connection to terminate at multiple virtual data centers or gateways.

**NOTE** If you change or add IP address ranges in vCloud Air, you must update your connection provider so that they can properly configure routing to those IP address ranges.

You can provide a private IP address range to configure on the Direct Connect interface. The Direct Connect interface and the virtual machines connected to the Direct Connect interface can be configured with this private IP address range.

**View Direct Connect in vCloud Air**

After your network service provider provisions your physical connection, log in to the vCloud Air Web UI to view the details about the connection.

The Direct Connect network interface is the second external interface. The vCloud Air supports two external network interfaces.

**Prerequisites**

- Your network service provider has physically provisioned your direct network connection to the colocation center.
- You have informed your vCloud Air Customer Success Team that the circuit to vCloud Air is provisioned.
- Your Customer Success Team has confirmed provisioning is complete.

**Procedure**

1. Sign in to vCloud Air with your email address and password.
   
   The cloud regions page appears.
2. Click the region for which you ordered your direct network connection.
3. Click the **Gateway** tab and click the gateway name that you provided to your vCloud Air Customer Success Team to configure as the gateway for termination.
   
   The details about networks associated with that gateway and the details for the networks appear.
   
   You can see the status of the connection (such as, on, active, redundancy enabled, and failover state) and the speed of the connection.

**Route Traffic Through Direct Connect**

After your direct network connection is provisioned for vCloud Air, use the vCloud Air Web UI to set up your virtual machines to route traffic through the connection. To route traffic for your virtual machines through your direct network connection, you must create NAT rules for the virtual machines so that they route traffic through the connection.

**NOTE** For information about configuring NAT rules, see “Add a NAT Rule,” on page 26.
Prerequisites

- Your network service provider has physically provisioned your direct network connection to the vCloud Air data center and VMware has completed the set up.
- You have Network Administrator privilege in vCloud Air.

Procedure

1. In the **Gateway** tab, click the gateway name that you provided to your vCloud Air Customer Success Team to configure as the gateway for termination.

2. Click the **NAT Rules** tab.

   The list of NAT rules configured for the gateway appear.

3. To route traffic from your vCloud Air gateway to the router on your premises or to the router of your network service provider, select Destination NAT from the Add One drop-down list.

   The IP address of the destination router depends on the type of connection.

   The Add a Destination NAT Rule dialog box appears. Complete the settings to add a DNAT rule.

4. To create static routes to your virtual machines, click **Manage in vCloud Director**. See Enable Static Routing for an Organization Virtual Datacenter Network in the vCloud Director documentation.

   Choose the NAT IP address from the IP Pool range that appears in the details for your direct network connection.

5. To route traffic from the router at your premises or from your network service provider’s router to the vCloud Air gateway, select Source NAT from the Add One drop-down list.

   The Add a Source NAT Rule dialog box appears. Complete the settings to add an SNAT rule.
Index

A
Active Directory 36
add networks 23
antivirus appliances 18

B
bandwidth 8

C
CIDR, firewall rules 31

D
Data Center Extension 32, 36
Dedicated Cloud service
deleting gateways 23
IP addresses 12
default
  firewall setup 31
  isolated network 8
  routed network 8
  setup 8
destination NAT 14
DHCP
  changing DNS settings 17
  IP addresses 12
  IP pools 16
  overview 16
  virtual machines 39
Direct Connect
  completing order 53
  connection technology 48
deleting network 25
direct connection 53
features 43
network service provider 51
ordering 52
overview 43
provisioning 49
routed connection 53
routing setup 54
secure access 32
SLA 43
use cases 48
viewing connection 54

DNS
  external servers 17
  overview 17
dynamic routing 33

E
encryption 35
external network
  NAT 14, 26
  static routing 18

F
firewall
  adding rules 21, 31
  default setup 31
  IPsec 35
  overview 31

G
gateway networks, viewing 24
gateways
  adding 22
  adding networks 25
  compact configuration 8
  default IP address 8
  default setup 8
delete 23
DNS servers 17
high availability 8, 22
interfaces 8
IP addresses 16
links to advanced management 21
load balancer 16
local ID 33
networking services 13
viewing 21
viewing networks 24
VPN connections 33

H
high availability 8, 22

I
ICMP type 26
intended audience 5
interfaces, primary NIC 41
internal networks, default setup 8
Internet
  connectivity 8
  secure connectivity 32
  virtual machine access 41
IP pools
  suballocated 16
  virtual machines 39
  virtual machines using 40
IP addresses
  Dedicated Cloud service 12
  DHCP 16
  free or allocated 21
  overlapping 33
  peer 33
  public 12
  static 12
  static pool 39
  suballocation from multiple subnets 12
Virtual Private Cloud service 12
IP range, See IP pools
IPsec
  encryption 35
  overview 33
  setup 35
  setup overview 33
isolated networks
  DHCP 16
  security 29

L
layer 2 networking 32, 36
load balancer 16
local endpoints 33
local ID 33

M
MAC addresses 36
Microsoft Active Directory 36
multi-interface mode 8

N
NAT
  adding rules 21, 26
  example 14
IPsec 33
networking
  components 8
  infrastructure 7
  layer 2 32, 36
  managing 21
  overview 7
  privileges 21
security 29
segementation 29
software defined data center 7
software stack 7
subnets 33
virtualization 7
networks
  adding to gateway 25
  changing assignments 40
  deleting 25
  Direct Connect 32
  peer 33
  remote 32
  stretched 32, 36
  viewing 23

O
on-premises, IPsec configuration 33
Org VDC networks
  DHCP 16
  DNS 17

P
peer networks 33
peer IP addresses 33
pool servers 16
ports
  firewall rules 31
  NAT 26
  UDP 35
primary NIC 41
Private Link Connect, See Direct Connect
public IP addresses 12

R
redundancy, for Direct Connect 48
related documentation 5, 13
remote site, connectivity 35
routed networks
  DHCP 16
  security 29

S
security, benefits 29
server pools 16
SLA, Direct Connect 43
software defined data center 7
source NAT 14
SSL VPN 32, 36
static routing, for Direct Connect 48
stretched networks 32, 36
suballocate IP pools 16
T
third-party appliances 18, 29
threat mitigation 29

U
unicast traffic 33

V
vApp 36
vCloud Director
  configuring network services 13
deleting gateways 23
IPsec configuration 33
static routing 18
vCloud Networking and Security Edge Gateway 8
vCloud Air offerings, connecting 48
virtual machines
  connecting to networks 40
  DHCP 39
  editing networks 40
virtual servers 16
virtual data centers
  deleting networks 25
gateways 22
  viewing networks 23
Virtual Private Cloud service, IP addresses 12
Virtual Private Cloud OnDemand service, security 29
virtualization 7
VMware Tools 39
VPN
  Direct Connect for 43
  enabling 35
  overview 32
  setup 35
vSphere 7

X
XVLAN 7, 8