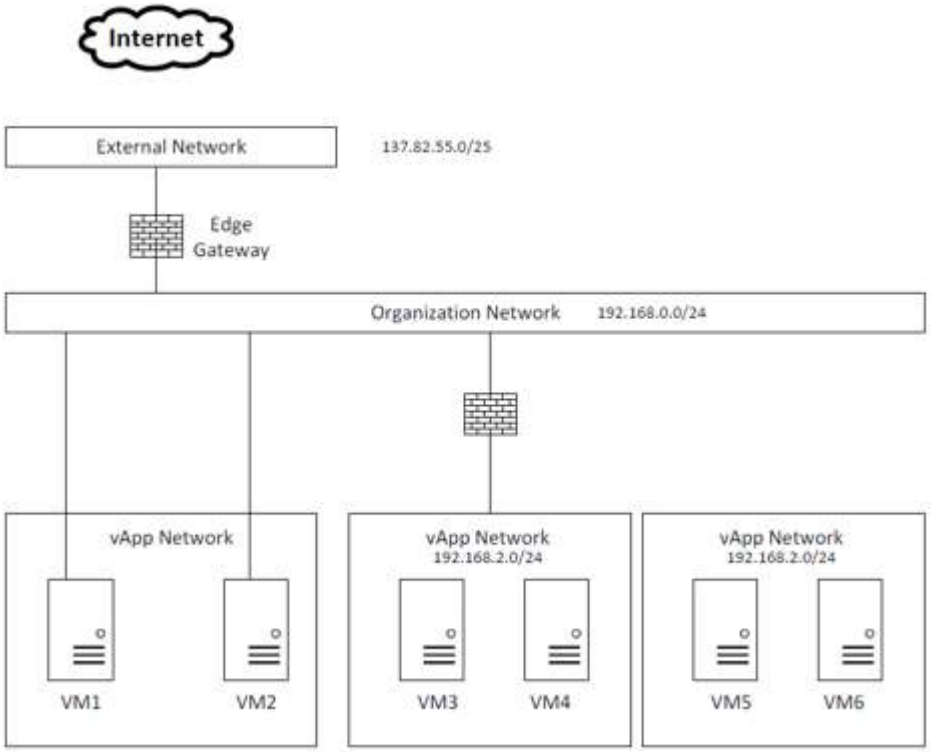
Working with Networks

Contents

EduCloud Networks

There are 3 layers of networking in EduCloud:

1. External Network
2. Organization Network
3. vApp Network



External Network

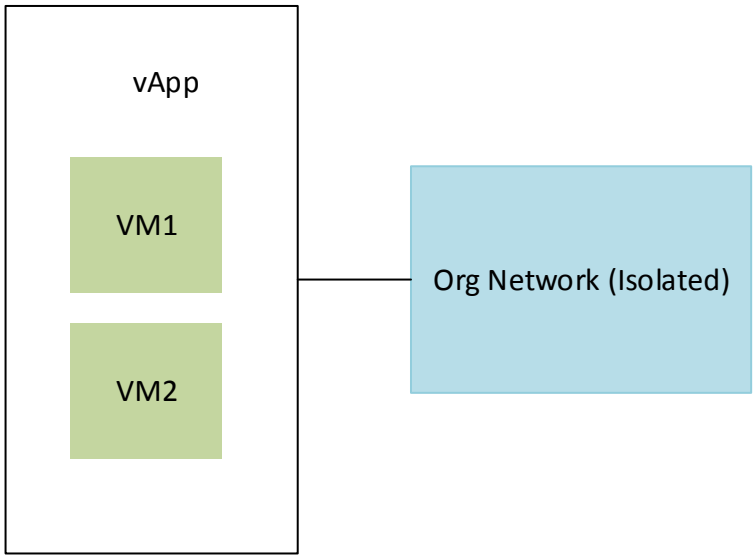
An External Network provides the connection from the cloud to the outside world and is port group based. This allows connections from EduCloud to external VLANS or the internet. An External Network provides connectivity to multiple organizations.

Organization Network

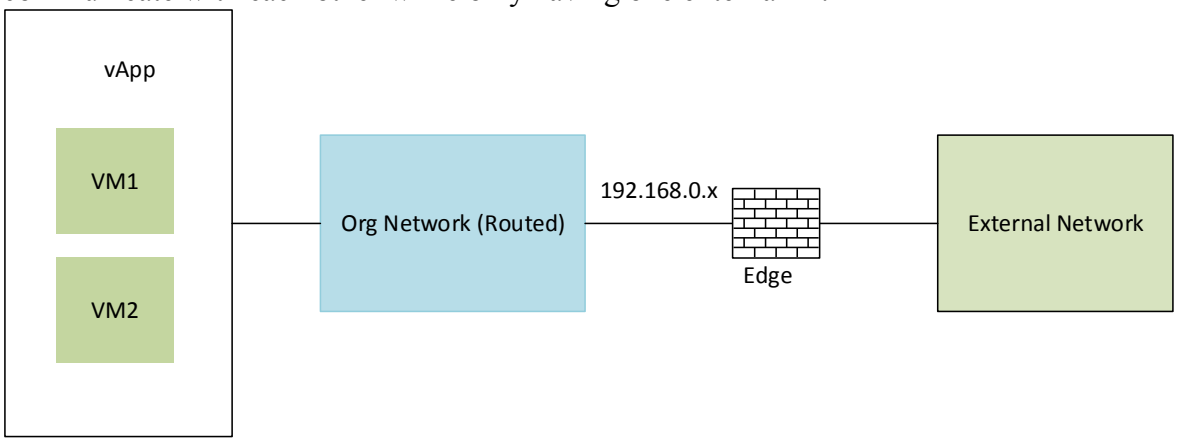
An Organization Network provides network services to a particular organization. This type of network allows vApps within an organization to communicate with each other or to other organizations.

An Organization Network can be set up in 3 ways:

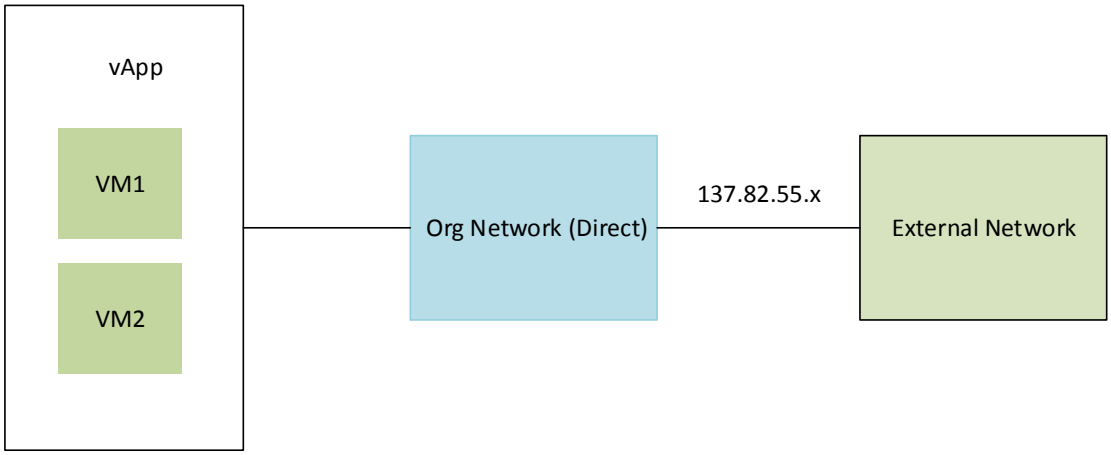
- Internal – no connection to the external network. vApps within the organization will be able to talk to each other but there is no traffic into or out of the organization.



- NAT (routed) Connected – connects to the external network through a vShield Device. The vShield Edge device provides port-forwarding services, NAT, DNS forwarding, and DHCP services to the network. A NAT connection allows for virtual machines to communicate with each other while only having one external IP.



- Direct – the organization would use an external network
to connect to external systems, such as the internet. External users will be able to connect directly to a VM in the organization.

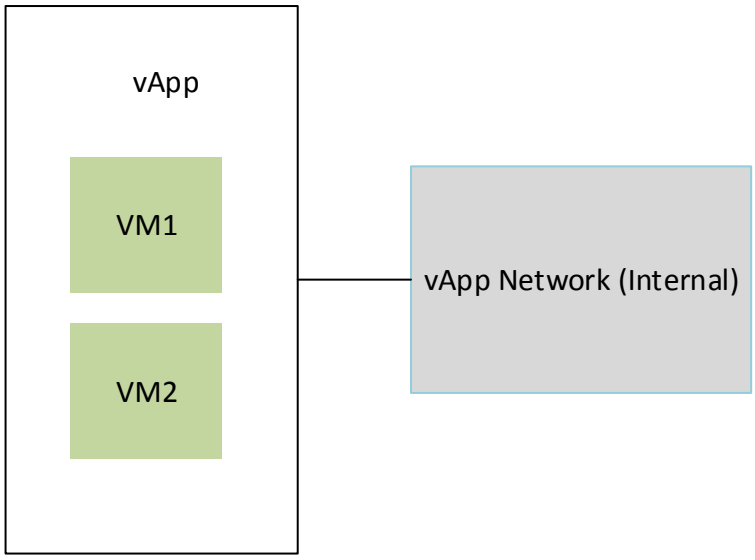


vApp Network

The vApp Network allows communication between VMs in a vApp or to VMs in other vApps in the organization.

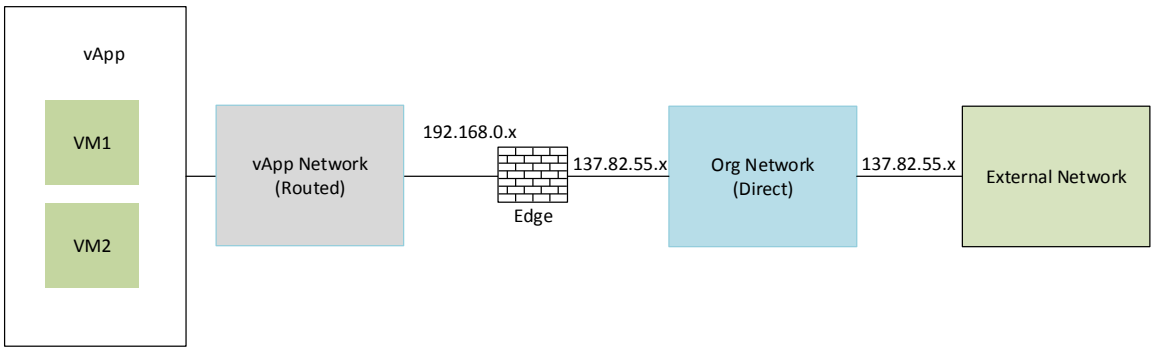
A vApp Network can be set up in 3 ways:

- Internal – not connected to any other network. This can be used to isolate communication between a web and database server within a vApp.

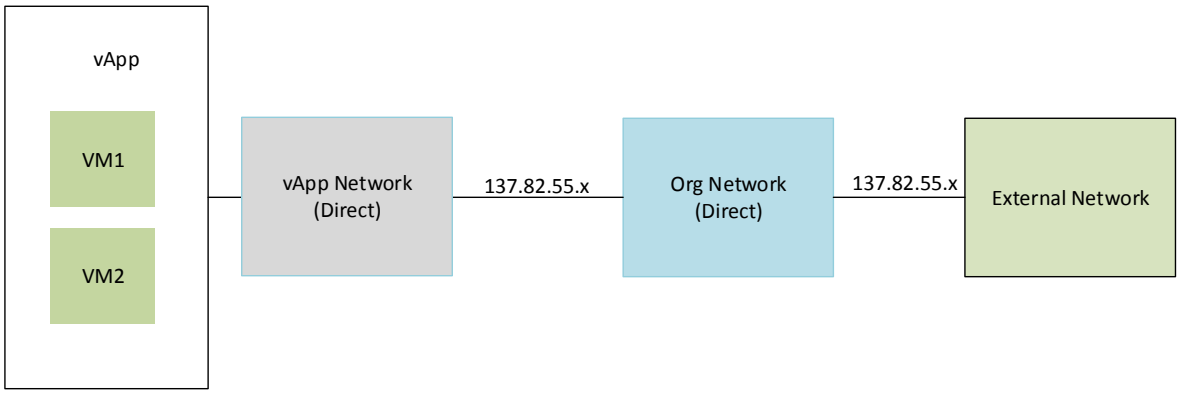


- NAT (routed) Connected – connects to the Organization Network through a vShield Device. As with a routed Organization Network, the vShield Edge device provides port-forwarding services, NAT, DNS forwarding, and DHCP services to the vApp network. Fencing can be used to isolate a vApp from the rest of the network. Each vApp can have

its own Private Internal Network and VMs within a vApp can consume the same IPs as VMs in another vApp. This is ideal for classroom lab scenarios.



- Direct – the vApp Network is connected directly to the Organization Network. This can be used if the vApp needs to be accessed from anywhere in the organization.



Network Management

Adding Networks to an Organization Virtual Datacenter

Create an External Direct Organization Virtual Datacenter Network

You can create an external direct organization virtual datacenter network that multiple organizations can access. You typically use the external network to connect to the Internet. The organization connects directly to this network.

1. Click the Manage & Monitor tab and click Organization VDCs in the left pane.
2. Double-click the organization virtual datacenter name to open the organization virtual datacenter.
3. Click the Org VDC Networks tab and click Add Network
4. Select Connect directly to an external network.
5. Select an external network and click Next.

6. Type a name and optional description.
7. (Optional) Select Share this network with other VDCs in the organization to make the organization virtual datacenter network available to other organization virtual datacenters in the organization.
8. Click Next.
9. Review the settings for the organization virtual datacenter network.

Click Finish to accept the settings and create the organization virtual datacenter network, or click Back to modify the settings.

Create an External Routed Organization Virtual Datacenter Network

You can create an external routed organization virtual datacenter network that only this organization can access.

1. Click the Manage & Monitor tab and click Organization VDCs in the left pane.
2. Double-click the organization virtual datacenter name to open the organization virtual datacenter.
3. Click the Org VDC Networks tab and click Add Network.
4. Select Create a routed network by connecting to an existing edge gateway.
5. Select an edge gateway and click Next.
6. Type a Gateway address and Network mask for the organization virtual datacenter network.
7. (Optional) Select Use gateway DNS to use the DNS relay of gateway.
   This option is available only if the gateway has DNS relay enabled.
8. (Optional) Enter DNS settings to use DNS.
9. (Optional) Enter an IP address or range of IP addresses and click Add to create a static IP pool.
   Repeat this step to add multiple static IP pools.
10. Click Next.
11. Type a name and optional description.
12. (Optional) Select Share this network with other VDCs in the organization to make the organization virtual datacenter network available to other organization virtual datacenters in the organization.
13. Click Next.
14. Review the settings for the organization virtual datacenter network.

Click Finish to accept the settings and create the organization virtual datacenter network, or click Back to modify the settings.

Create an Internal Organization Virtual Datacenter Network

You can create an internal organization virtual datacenter network that only this organization can access. The new network provides the organization with an internal network to which multiple vApps can connect.

1. Click the Manage & Monitor tab and click Organization VDCs in the left pane.

2. Double-click the organization virtual datacenter name to open the organization virtual datacenter.
3. Click the Org VDC Networks tab and click Add Network.
4. Select Create an isolated network within this virtual datacenter and click Next.
5. Type a Gateway address and Network mask for the organization virtual datacenter network.
6. (Optional) Select Use gateway DNS to use the DNS relay of gateway.
   This option is available only if the gateway has DNS relay enabled.
7. (Optional) Enter DNS settings to use DNS.
8. (Optional) Enter an IP address or range of IP addresses and click Add to create a static IP pool.
   Repeat this step to add multiple static IP pools.
9. Click Next.
10. Type a name and optional description.
11. (Optional) Select Share this network with other VDCs in the organization to make the organization virtual datacenter network available to other organization virtual datacenters in the organization.
12. Click Next.
13. Review the settings and click Finish to accept the settings.

Configuring Edge Gateway Services

DHCP Configuration

You can configure edge gateways to provide DHCP services to virtual machines connected to associated organization virtual datacenter networks.

1. Click the Manage & Monitor tab and click Organization VDCs in the left pane.
2. Double-click the organization virtual datacenter name to open the organization virtual datacenter.
3. Click the Edge Gateways tab, right-click the edge gateway name and select Edge Gateway Services.
4. Click the DHCP tab and select Enable DHCP.
5. Click Add and type a range of IP addresses.
6. Set the default lease time and maximum lease time or use the default values.
7. Click OK.

Add a Source NAT (SNAT) Rule

A source NAT rule translates the source IP address of outgoing packets on an organization virtual datacenter that are being sent to another organization virtual datacenter network or an external network.

1. Click the Manage & Monitor tab and click Organization VDCs in the left pane.
2. Double-click the organization virtual datacenter name to open the organization virtual datacenter.

3. Click the Edge Gateways tab, right-click the edge gateway name and select Edge Gateway Services.
4. Click the NAT tab and click Add SNAT.
5. Select an organization virtual datacenter network to apply this rule on from the Apply to drop-down menu.
6. Type the original IP address or range of IP addresses to apply this rule on in the Original (Internal) source IP/range text box.
7. Type the IP address or range of IP addresses to translate the addresses of outgoing packets to in the Translated (External) source IP/range text box.
8. Select Enabled and click OK.

The IP addresses of outgoing packets on the organization virtual datacenter network are translated according to the specifications of the source NAT rule.

Add a Destination NAT (DNAT) Rule

A destination NAT rule translates the IP address and port of packets received by an organization virtual datacenter network coming from another organization virtual datacenter network or an external network.

1. Click the Manage & Monitor tab and click Organization VDCs in the left pane.
2. Double-click the organization virtual datacenter name to open the organization virtual datacenter.
3. Click the Edge Gateways tab, right-click the edge gateway name and select Edge Gateway Services.
4. Click the NAT tab and click Add DNAT.
5. Select an external network or another organization virtual datacenter network to apply this rule on from the Apply to drop-down menu.
6. Type the original IP address or range of IP addresses to apply this rule on in the Original (External) IP/range text box.
7. Choose the Protocol to apply this rule on from the drop-down menu.
8. To apply this rule on all protocols, select Any.
9. (Optional) Select an Original port to apply this rule to.
10. (Optional) Select an IMCP type to apply this rule to if this rule applies to IMCP.
11. Type the IP address or range of IP addresses for the destination addresses on inbound packets to be translated to in the Translated (Internal) IP/range text box.
12. (Optional) Select a port for inbound packets to be translated to from the Translated port drop-down menu.
13. Select Enabled, and click OK.

The destination IP address and port are translated according to the destination NAT rule's specifications.

Firewall Configuration

Enable Firewall

1. Click Administration and double click the organization virtual datacenter.

2. Click the Org VDC Networks tab, right-click the organization virtual datacenter network name, and select Configure Services.
3. Click the Firewall tab and select Enable firewall to enable firewall services, or deselect it to disable firewall services.
4. Select the default firewall action.
5. (Optional) Select the Log check box to log events related to the default firewall action.
6. Click OK.

Add Firewall Rule

An organization administrator can configure certain organization virtual datacenter networks to provide firewall services. Enable the firewall on an organization virtual datacenter network to enforce firewall rules on incoming traffic, outgoing traffic, or both.

When you enable the firewall, you can specify a default firewall action to deny all incoming and outgoing traffic or to allow all incoming and outgoing traffic. You can also add specific firewall rules to allow or deny traffic that matches the rules to pass through the firewall. These rules take precedence over the default firewall action.

1. Click Administration and double click the organization virtual datacenter.
2. On the Org VDC Networks tab, right-click the organization virtual datacenter network name and select Configure Services.
3. Click the Firewall tab and click Add.
4. Type a name for the rule.
5. Type the traffic Source.

Option	Description
IP address	Type a source IP address to apply this rule on.
Range of IP addresses	Type a range of source IP addresses to apply this rule on.
CIDR	Type the CIDR notation of traffic to apply this rule on.
internal	Apply this rule to all internal traffic.
external	Apply this rule to all external traffic.
any	Apply this rule to traffic from any source.

6. Select a Source port to apply this rule on from the drop-down menu.
7. Type the traffic Destination.

Option	Description
IP address	Type a source IP address to apply this rule on.
Range of IP addresses	Type a range of source IP addresses to apply this rule on.
CIDR	Type the CIDR notation of traffic to apply this rule on.

internal	Apply this rule to all internal traffic.
external	Apply this rule to all external traffic.
any	Apply this rule to traffic from any source.

8. Select the Destination port to apply this rule on from the drop-down menu.
9. Select the Protocol to apply this rule on from the drop-down menu.
10. Select the action. A firewall rule can allow or deny traffic that matches the rule.
11. Select the Enabled check box.
12. (Optional) Select the Log network traffic for firewall rule check box. If you enable this option, vCloud Director sends log events to the syslog server for connections affected by this rule. Each syslog message includes logical network and organization UUIDs.

13. Click OK and click OK again.

Reorder Firewall Rules

Firewall rules are enforced in the order in which they appear in the firewall list.

When you add a firewall rule to an organization virtual datacenter network, the new rule appears at the bottom of the firewall rule list. To enforce the new rule before an existing rule, reorder the rules.

1. Click Administration and double click the organization virtual datacenter.
2. Click the Org VDC Networks tab, right-click the organization virtual datacenter network name, and select Configure Services.
3. Click the Firewall tab.
4. Drag the firewall rules to establish the order in which the rules are applied.
5. Click OK.

Load Balancer Configuration

Edge gateways provide load balancing for TCP, HTTP, and HTTPS traffic.

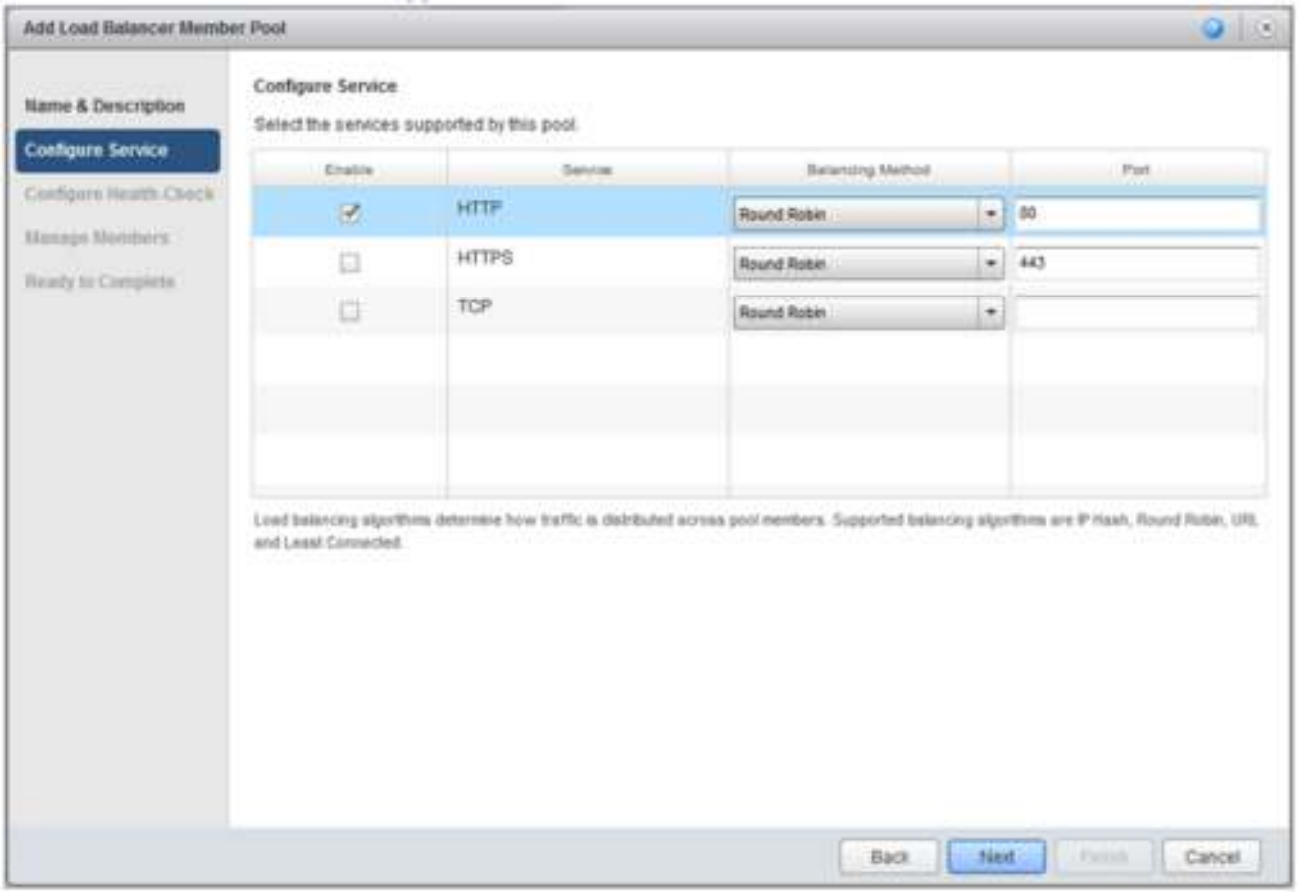
You map an external, or public, IP address to a set of internal servers for load balancing. The load balancer accepts TCP, HTTP, or HTTPS requests on the external IP address and decides which internal server to use. Port 809 is the default listening port for TCP, port 80 is the default port for HTTP, and port 443 is the default port for HTTPS.

Add a Pool Server to an Edge Gateway

You can add a pool server to manage and share back-end servers flexibly and efficiently. A pool is comprised of one or more back-end servers called members and it manages health check monitors and load balancer distribution methods.

1. Click the Administration tab and click Virtual Datacenters in the left pane.
2. Double-click the organization virtual datacenter name to open the organization virtual datacenter.
3. Click the Edge Gateways tab, right-click the edge gateway name, and select Edge Gateway Services.
4. On the Load Balancer tab, click Pool Servers and click Add.
5. Type a name and optionally a description for the pool server and click Next.

6. Click Enable for each service to support.

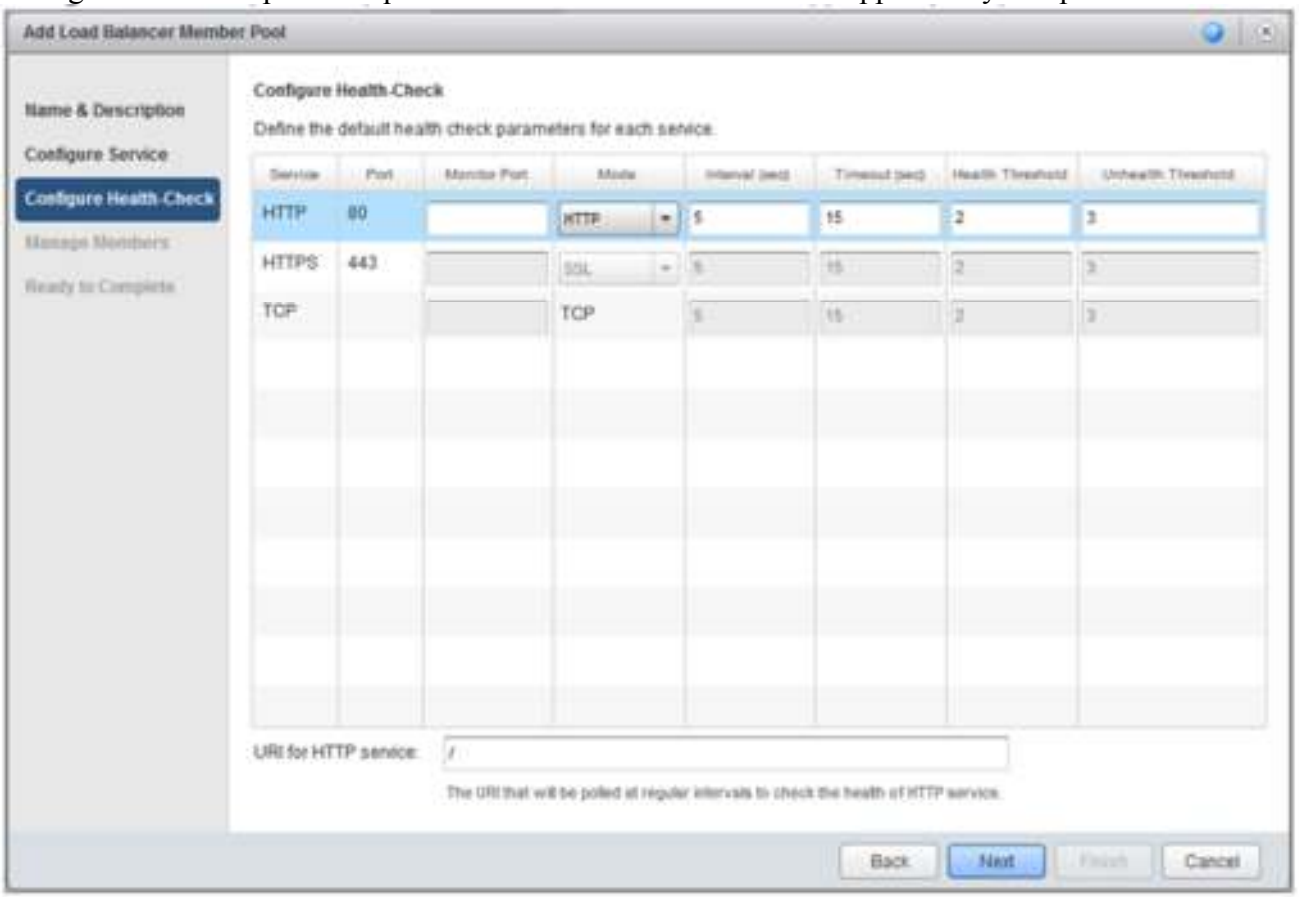


7. Select a balancing method from the drop-down menu for each enabled service.

Option	Description
IP Hash	Selects a server based on a hash of the source and destination IP address of each packet.
Round Robin	Each server is used in turn according to the weight assigned to it. This is the smoothest and fairest algorithm when the server's processing time remains equally distributed.
URI	The left part of the URI (before the question mark) is hashed and divided by the total weight of the running servers. The result designates which server will receive the request. This ensures that a URI is always directed to the same server as long as no server goes up or down.
Least Connected	Distributes client requests to multiple servers based on the number of connections already on the server. New connections are sent to the server with the fewest connections.

8. (Optional) Change the default port for each enabled service if necessary.
9. Click Next.

10. Change the monitor port if required for each service that is to be supported by this pool.

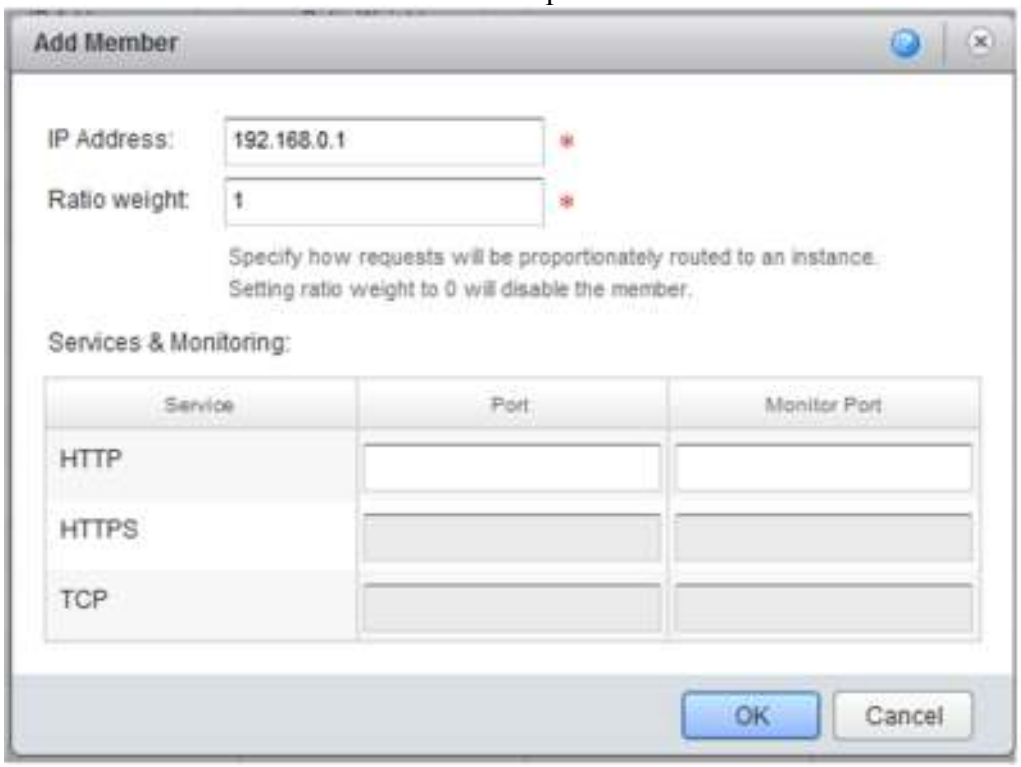


11. Select the health check mode from the drop-down menu for each service.

12. (Optional) Change the default health check parameters if necessary.

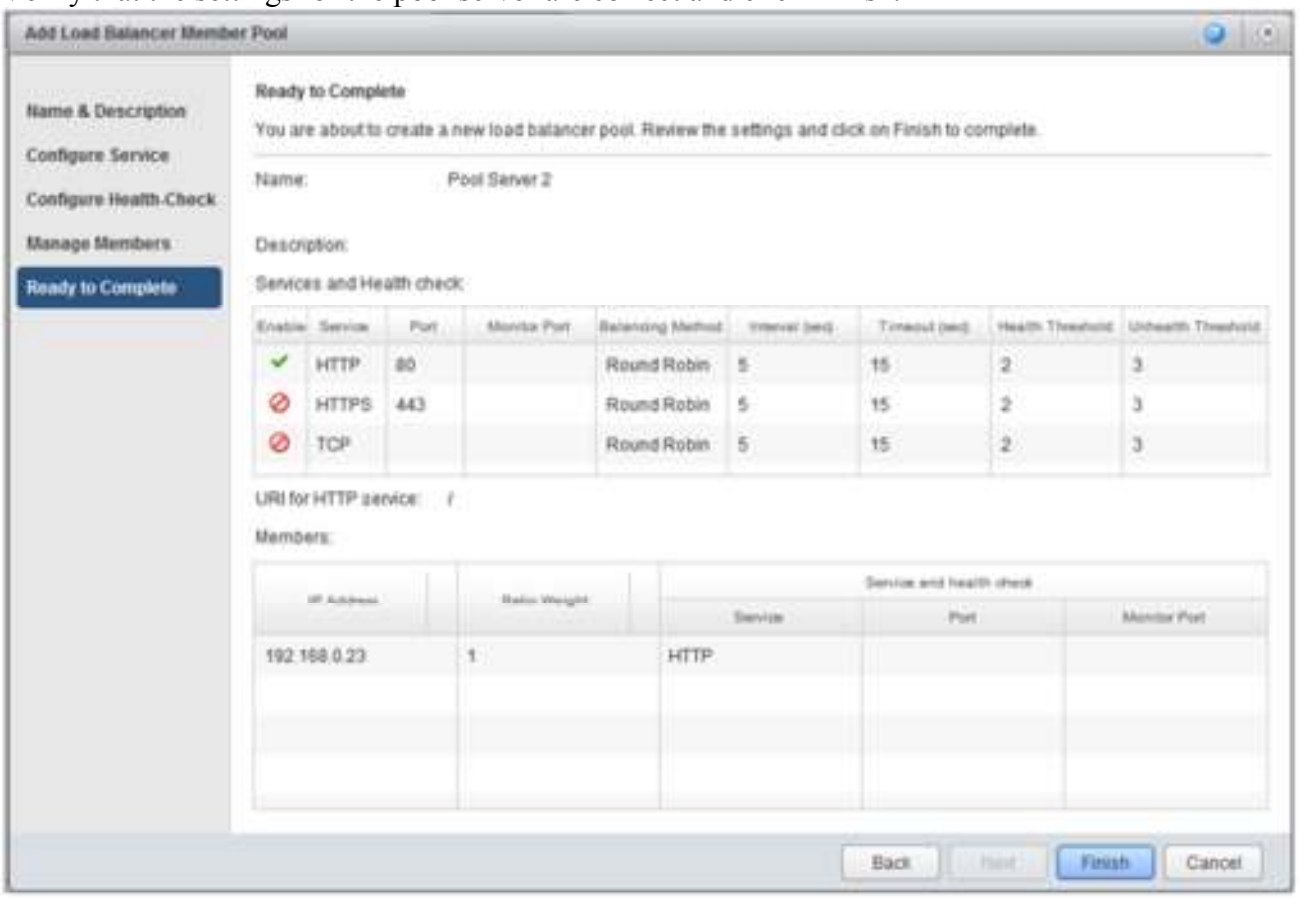
Option	Description
SSL	Tests servers using SSLv3 client hello messages. The server is considered valid only when the response contains server hello messages.
HTTP	The GET / default method is used to detect server status. Only responses 2xx and 3xx are valid. Other responses (including a lack of response) indicate a server failure.
TCP	TCP connection check.
Option	Description
Interval	Interval at which a server is pinged.
Timeout	Time within which a response from the server must be received.
Health Threshold	Number of consecutive successful health checks before a server is declared operational.
Unhealth Threshold	Number of consecutive unsuccessful health checks before a server is declared dead.

13. If using HTTP, type the URI referenced in the HTTP ping requests at the bottom of the screen.
14. Click Next.
15. Click Add to add a back-end server to the pool.



16. Type the IP address of the server.
17. Type the weight to indicate the ratio of how many requests are to be served by this back-end server.
18. Change the default port and monitor port for the server if required.
19. Click OK.
20. (Optional) Repeat Step 15 through Step 19 to add additional servers.
21. Click Next.

22. Verify that the settings for the pool server are correct and click Finish.



Edit Pool Server Settings

1. Click the Administration tab and click Virtual Datacenters in the left pane.
2. Double-click the organization virtual datacenter name to open the organization virtual datacenter.
3. Click the Edge Gateways tab, right-click the edge gateway name, and select Edge Gateway Services.
4. On the Load Balancer tab, click Pool Servers.
5. Select the pool server to modify and click Edit.
6. Make the appropriate changes and click OK.

Delete a Pool Server

Before you can delete a server pool from an edge gateway, verify that no virtual servers are using this pool server.

1. Click the Administration tab and click Virtual Datacenters in the left pane.
2. Double-click the organization virtual datacenter name to open the organization virtual datacenter.

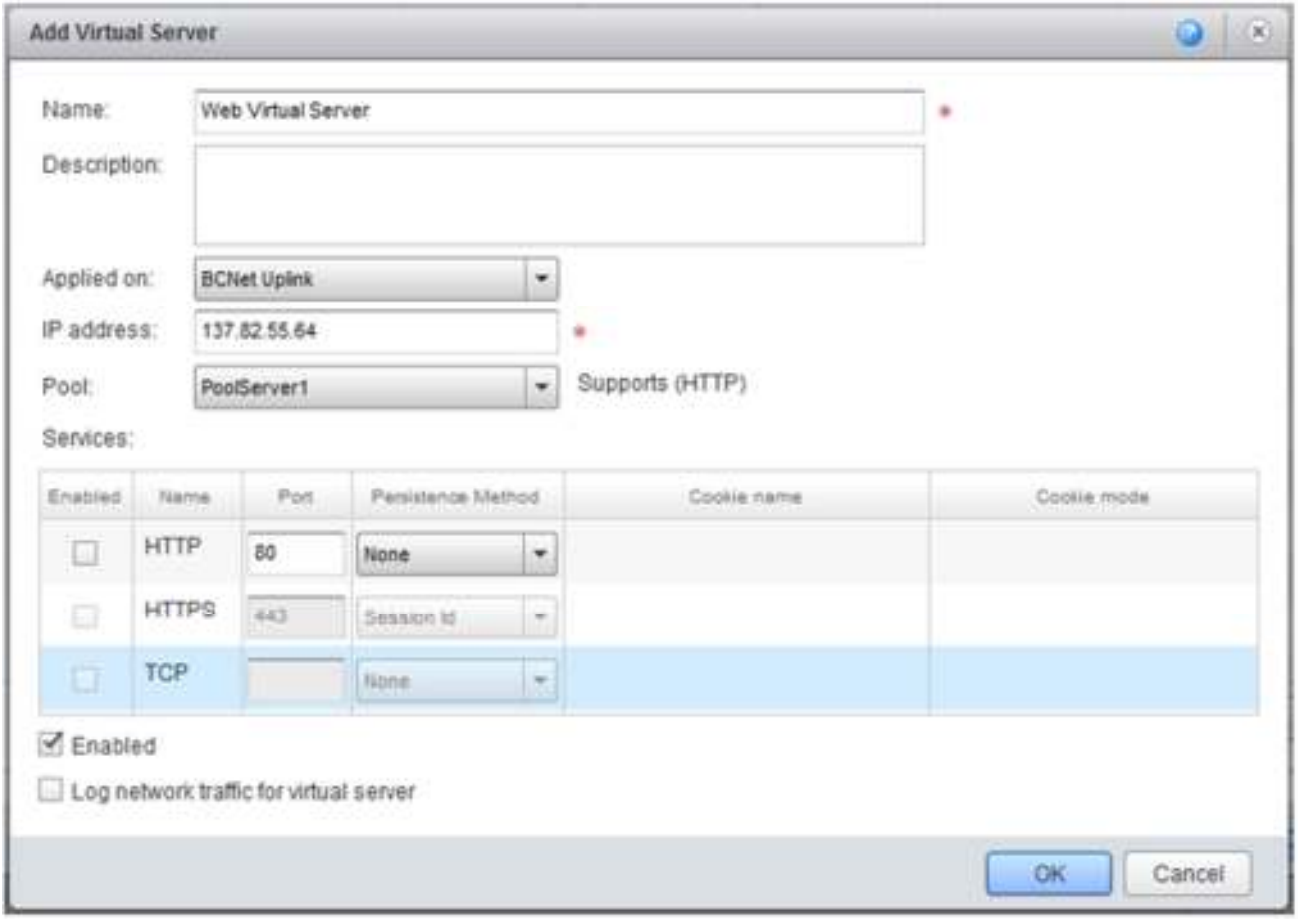
3. Click the Edge Gateways tab, right-click the edge gateway name, and select Edge Gateway Services.
4. On the Load Balancer tab, click Pool Servers.
5. Select the pool server and click Delete.

Add a Virtual Server to an Edge Gateway

A virtual server is a highly scalable and highly available server built on a cluster of servers called members. It serves as the entry point for any external traffic which needs to access the back end servers. The edge gateway must have at least one pool server.

1. Click the Administration tab and click Virtual Datacenters in the left pane.
2. Double-click the organization virtual datacenter name to open the organization virtual datacenter.
3. Click the Edge Gateways tab, right-click the edge gateway name, and select Edge Gateway Services.
4. On the Load Balancer tab, click Virtual Servers and click Add.
5. Type a name for the virtual server.
6. (Optional) Type a description for the virtual server.
7. Select an external network from the Applied on drop-down menu.
8. Type the IP address of the virtual server.
9. Select a pool from the drop-down menu to be associated with the virtual server.
10. In Services, select Enable for each service to be supported.
11. Change the default Port, Persistence Method, Cookie Name, and Cookie Mode values for each enabled service as required.
12. Click Enabled to enable the virtual server.

13. (Optional) Click Log network traffic for virtual server.



14. Click OK. consists of a suite of virtualization utilities that improves the functionality, administration, and management of virtual machines within a VMware environment.

Enable VPN

You can enable VPN for organization virtual datacenters backed by an edge gateway and create a secure tunnel from one of those organization virtual datacenter networks to another network.

EduCloud supports VPN between organization virtual datacenter networks backed by edge gateways and both organization virtual datacenter networks in the same organization and remote networks.

1. Click the Manage & Monitor tab and click Organization VDCs in the left pane.
2. Double-click the organization virtual datacenter name to open the organization virtual datacenter.
3. Click the Edge Gateways tab, right-click the edge gateway name and select Edge Gateway Services.
4. Click the VPN tab and select Enable VPN.
5. (Optional) Click Configure Public IPs, type a public IP address, and click OK.
6. Click OK.

Creating VPN Tunnels

You can create VPN tunnels between organization virtual datacenter networks on the same organization, between organization virtual datacenter networks on different organizations, and between an organization virtual datacenter network and an external network.

EduCloud does not support multiple VPN tunnels between the same two edge gateways. If there is an existing tunnel between two gateways and you want to add another subnet to the tunnel, delete the existing VPN tunnel and create a new one that includes the new subnet.

Create a VPN Tunnel In an Organization for an Organization Virtual Datacenter Network Backed by an Edge Gateway

You can create a VPN tunnel between an organization virtual datacenter network that is backed by edge gateway and another organization virtual datacenter in the same organization.

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

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

Prerequisites

Verify that you have at least two routed organization virtual datacenter networks in the organization. One of these networks must be backed by the edge gateway. Both organization virtual datacenter networks must have VPN enabled.

1. Click the Manage & Monitor tab and click Organization VDCs in the left pane.
2. Double-click the organization virtual datacenter name to open the organization virtual datacenter.
3. Click the Edge Gateways tab, right-click the edge gateway name. and select Edge Gateway Services.
4. Click the VPN tab and click Add.
5. Type a name and optional description.
6. Select a network in this organization from the drop-down menu and select local and peer networks.
7. Review the tunnel settings and click OK.

vCloud Director configures both peer network endpoints.

Create a VPN Tunnel Between Organizations

You can create a VPN tunnel between two organization virtual datacenter networks in different organizations. The organizations can be part of the same vCloud Director installation or a different installation.

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

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

Prerequisites

Verify that you have a routed organization virtual datacenter network in each of the organizations. The organization virtual datacenter networks must have non-overlapping IP subnets and site-to-site VPN enabled.

1. Click the Manage & Monitor tab and click Organization VDCs in the left pane.
2. Double-click the organization virtual datacenter name to open the organization virtual datacenter.
3. Click the Edge Gateways tab, right-click the edge gateway name and select Edge Gateway Services.
4. Click the VPN tab and click Add.
5. Type a name and optional description.
6. Select a network in another organization from the drop-down menu.
7. Click Connect to another organization, type the login information for the peer organization, and click Continue.
   vCloud URL - The base URL of the vCloud instance that contains the peer organization. For example, https://www.example.com. Do not include /cloud or /cloud/org/orgname in the URL.
   Organization - The organization name that is used as the unique identifier in the organization URL. For example, if the organization URL is https://www.example.com/cloud/org/myOrg, type myOrg.
   Username - The user name of an organization administrator or system administrator that has access to the organization.
   Password - The password associated with the user name.
8. Select a peer network.
9. Review the tunnel settings and click Connect.

vCloud Director configures both peer network endpoints.

Create a VPN Tunnel From an Organization Virtual Datacenter Network Backed by an Edge Gateway to a Remote Network

You can create a VPN tunnel between an organization virtual datacenter network that is backed by an edge gateway and a remote network.

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

- IP Protocol ID 50 (ESP)
- IP Protocol ID 51 (AH)

- UDP Port 500 (IKE)
- UDP Port 4500

Prerequisites

Verify that you have a routed remote network that uses IPSec and an organization virtual datacenter network backed by an edge gateway.

1. Click the Manage & Monitor tab, and click Organization VDCs in the left pane.
2. Double-click the organization virtual datacenter name to open the organization virtual datacenter.
3. Click the Edge Gateways tab, right-click the edge gateway name, and select Edge Gateway Services.
4. Click the VPN tab and click Add.
5. Type a name and optional description.
6. Select a remote network from the drop-down menu.
7. Select the local organization virtual datacenter network.
8. Type the peer settings.
9. Review the tunnel settings and click OK.

vCloud Director configures the organization peer network endpoint.