EDUCLOUD SERVER

Network and Security Guide

v10.4.2.2
September, 2023

EduCloud Server Service – Network and Security Guide

EduCloud Networks

There are 3 types of Organization Virtual Data Center (Org VDC) networks supported in EduCloud:

1. Direct
2. Routed
3. Isolated

vCloud Director Cross-VDC networks are not currently supported in EduCloud.

Direct Networks

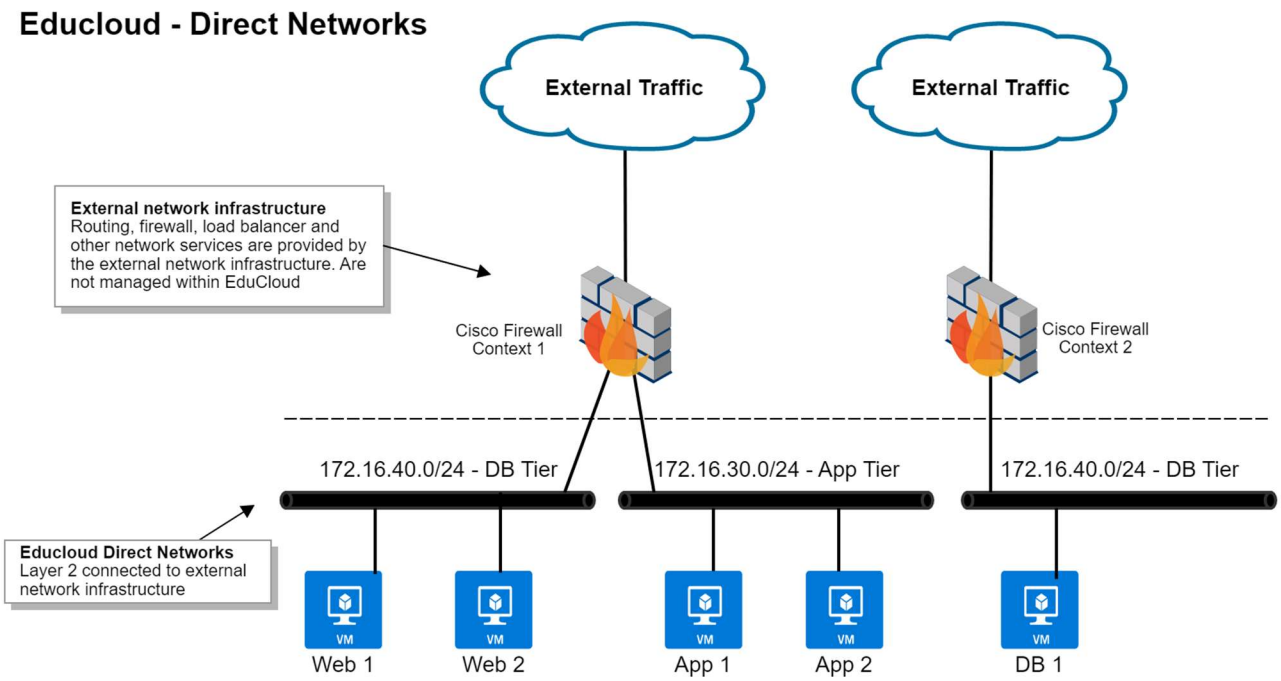
Direct Networks provide direct layer 2 connectivity to an external network. They can only be configured by EduCloud system administrators.

Direct networks are used to:

- Provide external connectivity to an organizations NSX networks via their edge gateways.
- Provide direct layer2 connectivity to external networks for VMs within an organization.

For organizations using NSX all external access is provided by a direct network attached to the edge gateway external interface. All BCNET and newer UBC organizations use NSX.

Direct networks are used by older UBC organizations to provide VMs direct access to campus networks and resources – a model used prior to NSX being licensed for UBC workloads. Routing, firewall, NAT and load balancing services are provided at the network layer and cannot be managed or configured within the EduCloud service.



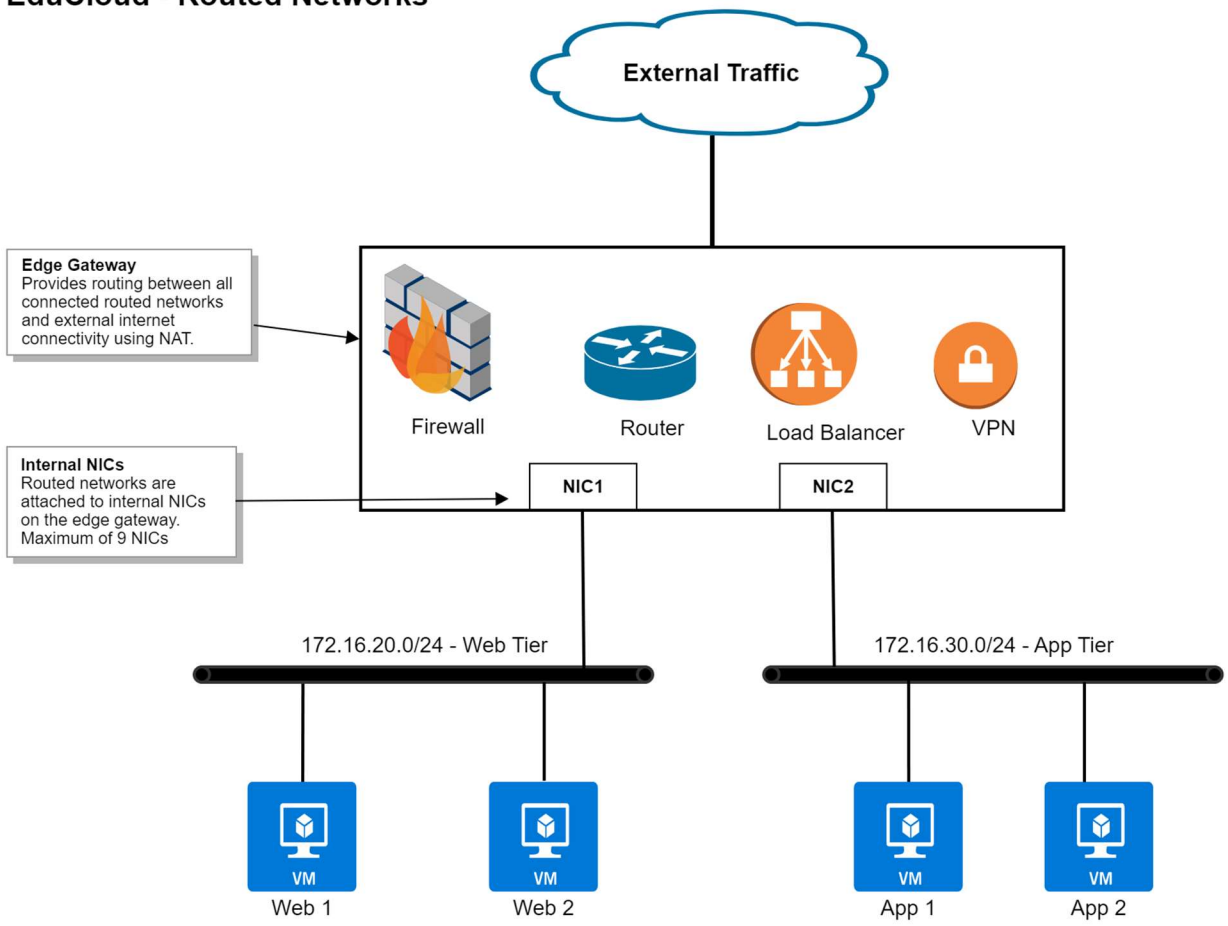
Routed Networks

Routed Networks are configured within an organization VDC and only VMs in that VDC can be connected to it.

A routed network is connected to an edge gateway. The edge gateway provides routing between all the routed networks you create within your VDC, and external internet connectivity using NAT. Organization administrators can configure NAT, firewall, VPN, load balancing and other services on the edge gateway to provide appropriate access to and from VMs in the organization.

If a routed network is “shared” it is available across all your organization VDC’s at the same site.

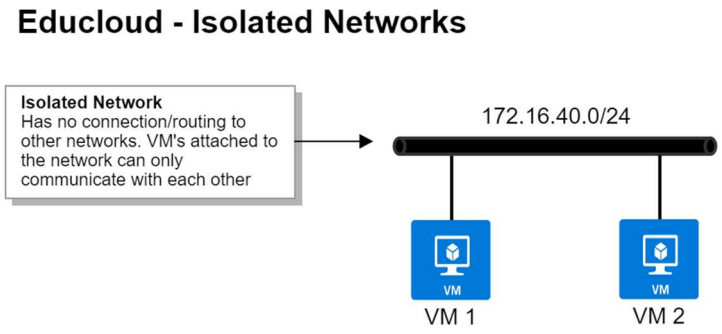
EduCloud - Routed Networks



Isolated Networks

Isolated Networks are configured within an organization VDC and only VMs in that VDC can be connected to it. There is no connection to or any routing to other networks.

An isolated network can also be "shared" across all your VDC's at the same site.



Network Management

Adding Networks to an Organization Virtual Datacenter

Create a Direct Org VDC Network

UBC EduCloud organizations using direct networks must submit a service request ticket. Direct networks can only be created and managed by EduCloud system administrators.

Create a Routed Org VDC Network

A routed Org VDC network can be created by Organization Administrators to provide a network with connectivity to external networks, as well as to other routed networks within the organization.

1. From the EduCloud homepage, click on the Organization Virtual Center card
2. From the left panel under **Networking** click **Networks → New** and click **Next** on **"Current Organization Virtual Data Center"**
3. **Network Type -** select **Routed** and click **Next**
4. **Edge Connection**- select the appropriate Edge and click **Next**
5. **General** – Fill in the information and click **Next**
   - **Name** - enter a name for the network
   - **Gateway CIDR** - enter network information in **Gateway IP/subnet mask** e.g. 192.168.56.254/24
   - **Description** - enter description (optional)
6. **Static IP Pools** – enter an IP range and click **Add** and then **Next** e.g. 192.168.56.1-192.168.56.100

7. **DNS** – Fill in Primary/Secondary DNS and DNS suffix (optional)
8. **Ready to Complete** – review settings and, if necessary, click **Previous** to go back and change any setting
9. Click **Finish** to create network.

Create an Isolated Org VDC Network

An isolated Org VCD network can be created by Organization Administrators to provide connectivity within an organization. No external connectivity is available.

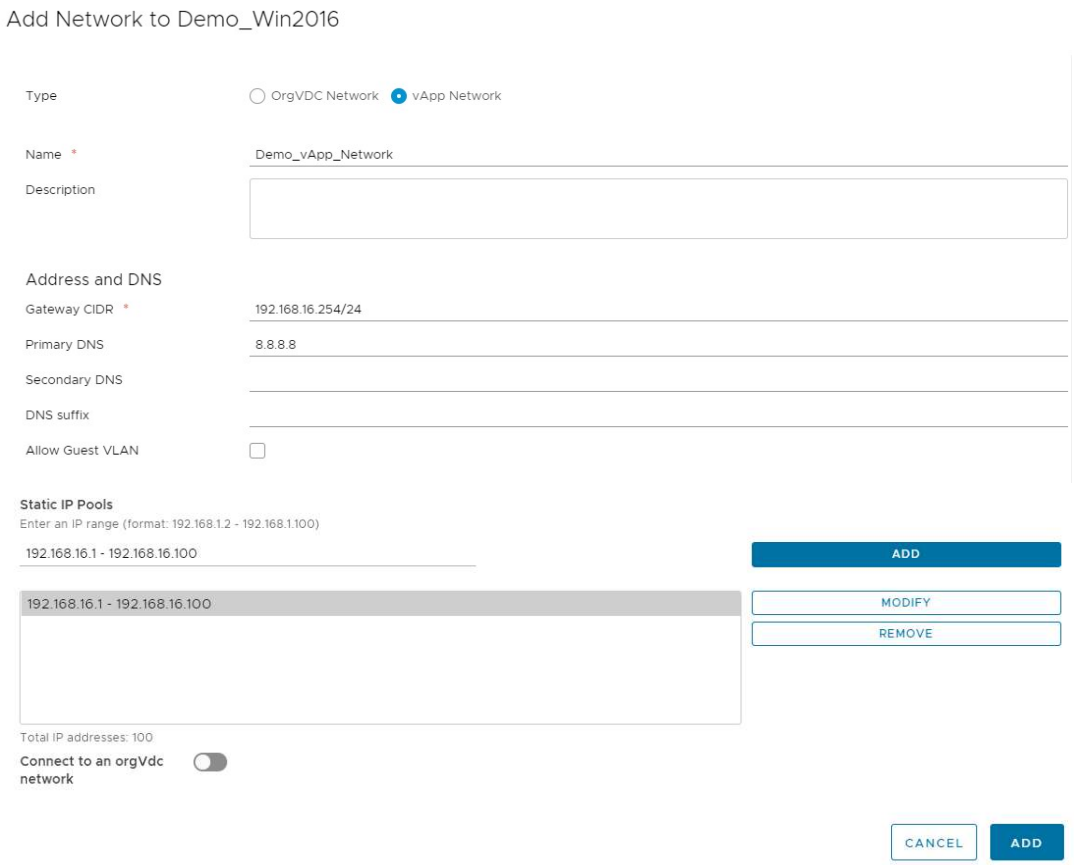
1. From the EduCloud homepage, click on the Organization Virtual Center card
2. From the left panel under **Networking** click **Networks → New** and click **Next** on **"Current Organization Virtual Data Center"**
3. **Network Type -** select **Isolated** and click **Next**
4. **General** – Fill in the information and click **Next**
    - **Name** - enter a name for the network
    - **Gateway CIDR** - enter network information in **Gateway IP/subnet mask** e.g. 192.168.56.254/24
    - **Description** - enter description (optional)
5. **Static IP Pools** – enter an IP range and click **Add** and then **Next** e.g. 192.168.56.1-192.168.56.100
6. **DNS** – Fill in Primary/Secondary DNS and DNS suffix (optional)
7. **Ready to Complete** – review settings and, if necessary, click **Previous** to go back and change any setting
8. Click **Finish** to create network.

Once the network is configured, then configure DHCP, Firewall, NAT, etc

1. From the EduCloud homepage, click on the Organization Virtual Center card
2. Under **Networking** click on **Networks**
3. Click on the Network you created.
4. **IP Management**:
    - **Static IP Pools –** Edit the static IP Pool configuration
    - **DNS** – Edit the DNS configuration
    - **DHCP** – Add/Edit a DHCP Pool
    - **IP Usage** – View IP Usage/Assignment

Adding Networks to a vApp/VM

1. From the EduCloud homepage, click on the Organization Virtual Center card
2. Under **Compute** in the left menu click on **vApps**
3. Click on the vApp you want to add network to.
4. Under the **Networks** menu click on **New**
    - **OrgVDC Network** – select your preconfigured OrgVDC Network from the list
    - **vApp Network** – creates a new vApp network
        i. Fill in the details for the vApp network



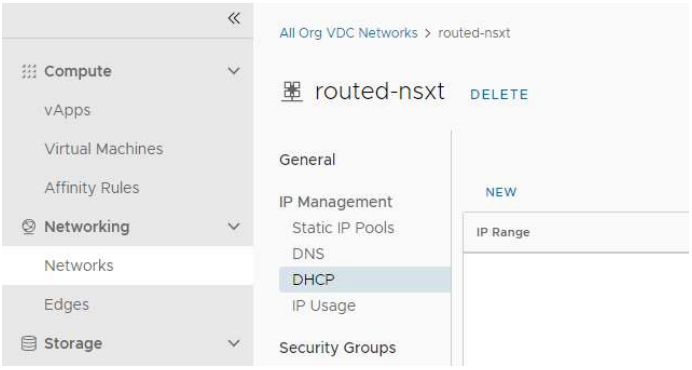
5. Click **Add**
6. Click **Virtual Machines** from the vApp menu.
7. Click on the name of the virtual machine
8. Under **Hardware** click **NICs** from the left panel
9. Click **Edit**
10. In the Network column, select the newly added network from the list
11. Click **Save**

Edge Gateway Services

DHCP

You can configure edge gateways to provide DHCP services to virtual machines connected to the associated Org VDC networks.

1. From the EduCloud homepage, click on the Organization Virtual Center card
2. From the left panel under **Networking**, click **Networks**
3. Click on a **Routed** network
4. Under **IP Management** click **DHCP**



5. If you haven't yet Activated DHCP you may need to click **Activate** first.
6. Click on **New**
    - **IP Pool:** IPs/Range available for DHCP

7. Click **Save**

NAT

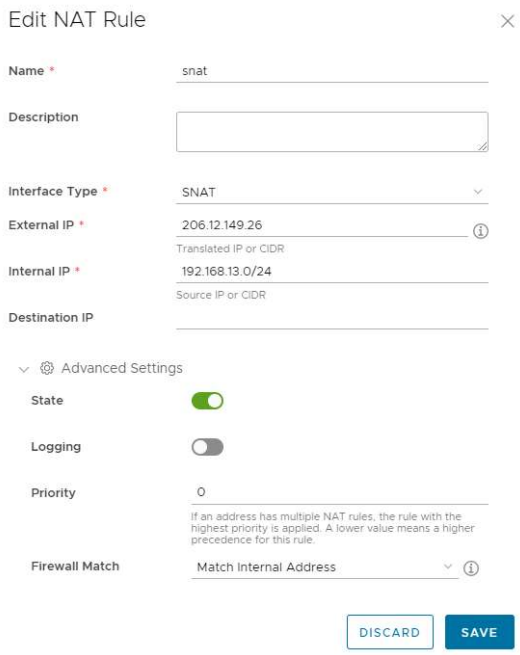
Add a Source NAT (SNAT) Rule

A source NAT rule translates the source IP address of outgoing packets from an Org VDC network.

1. From the EduCloud homepage, click on the Organization Virtual Center card
2. From the left panel under **Networking**, click **Edges**
3. Click on the Edge Gateway name
4. Under **Services** click **NAT**
5. Click **New**
6. Under **Add NAT Rule:**
    - **Name –** Provide a name for the rule
    - **Description –** (optional)
    - **Interface Type –**SNAT
    - **External IP –** Enter external IP
    - **External Port –** (optional)

- **Internal IP –** Enter internal IP
- **Application –** Click Edit (optional)

7. Advanced Settings
    - **State** – Enable/Disable Switch
    - **Logging** - Enable/Disable Switch
    - **Priority** – Set Priority level
    - **Firewall Match** – See info tab



The IP addresses of outgoing packets on the Org VDC network are translated according to the specifications of the source NAT rule.

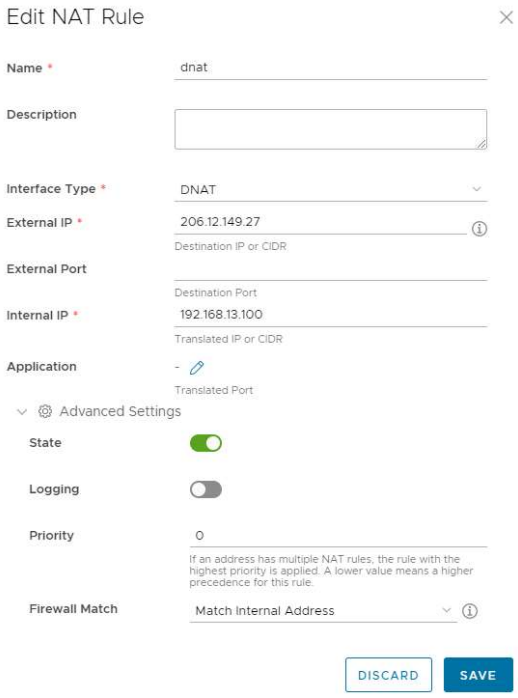
Add a Destination NAT (DNAT) Rule

A destination NAT rule translates the IP address and port of packets received by an Org VDC network.

1. From the EduCloud homepage, click on the Organization Virtual Center card
2. From the left panel under **Networking**, click **Edges**
3. Click on the Edge Gateway name
4. Under **Services** click **NAT**
5. Click **New**
6. Under **Add NAT Rule:**
    - **Name –** Provide a name for the rule
    - **Description –** (optional)
    - **Interface Type –**DNAT
    - **External IP –** Enter external IP
    - **External Port –** (optional)

- **Internal IP –** Enter internal IP
- **Application –** Click Edit (optional)

7. Advanced Settings
    - **State** – Enable/Disable Switch
    - **Logging** - Enable/Disable Switch
    - **Priority** – Set Priority level
    - **Firewall Match** – See info tab



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

Load Balancer

The load balancer accepts incoming network traffic on behalf of an application and balances that network traffic across multiple servers hosted on internal network created on the edge gateway..

Key Concepts

- Virtual Server – The service your customers connect to in order to access your load balanced application. Represented by a unique combination of IP, port, protocol and possibly application profile.
- Server Pool – a group of back end servers. The Load Balancer distributes traffic across members of the pool.
- Server Pool Member – represents the back-end server in a pool.
- Service Monitor - defines how to probe the health status of server pool members
- Application Profile – contains the TCP, UDP, persistence, and certificate configuration for a given application.

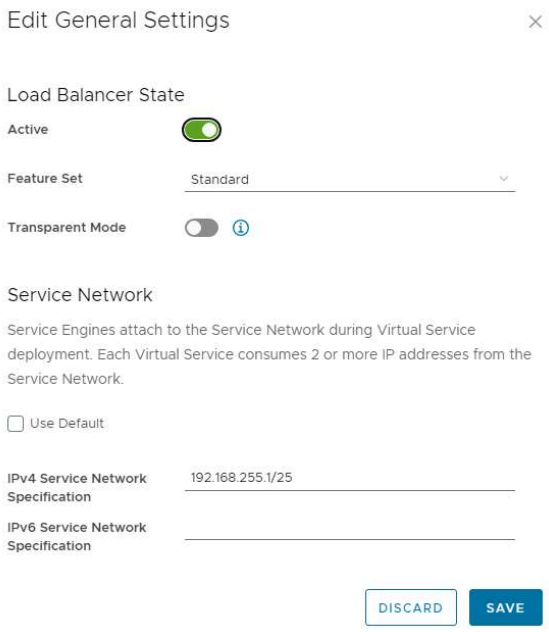
This section provides an example of configuring a very simple web application for load balancing – one that does not use SSL, or require any form of session persistence.

For more advanced Load Balancing configurations, see the "*Load Balancing*" section under "*Advanced Networking Capabilities for vCloud Director Tenants*" in the on-line help.

Pre-Requisite: Open a support request to enable and provision the ability to use Load Balancing prior to proceeding with the steps below:

Enable Load Balancer

1. From the EduCloud homepage, click on the Organization Virtual Center card
2. From the left panel under **Networking**, click **Edges**
3. Click on the Edge Gateway name
4. Under **Load Balancer** click **General Settings**
5. Click **Edit** to configure the load balancer settings
6. Toggle **Active** to enable the load balancer and click **SAVE**



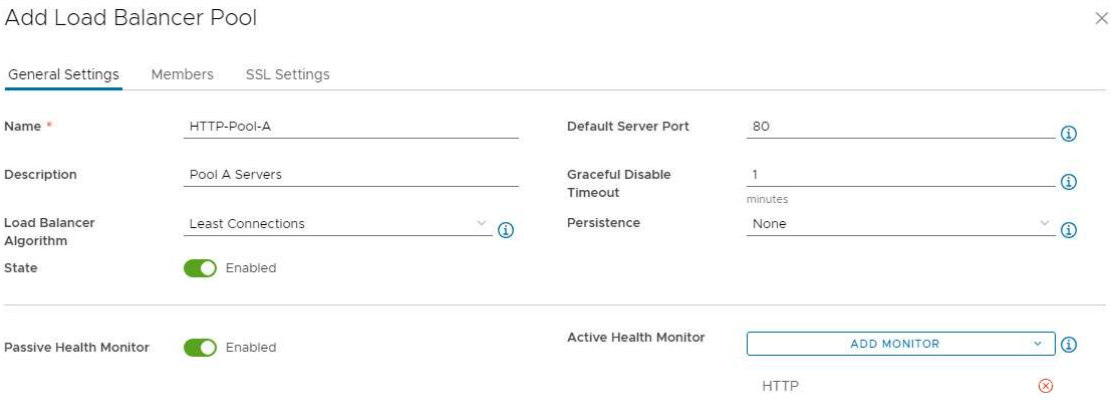
7. You will now see more options under **Load Balancer**

Create a Server Pool

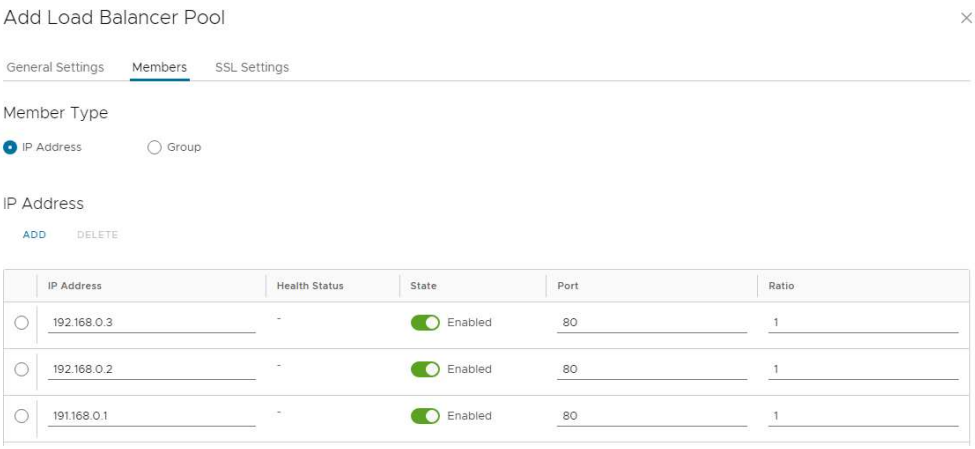
A pool manages all of the backend servers that serve your application. It defines the algorithm used to balance load and health check parameters.

1. From the EduCloud homepage, click on the Organization Virtual Center card

2. From the left panel under **Networking**, click **Edges**
3. Click on the Edge Gateway name
4. Under **Load Balancer** click on **Pools**
5. Click **ADD**
6. Under **General Settings** tab edit Pool Info
    - **Name:** Pool Name
    - **Description:** Enter Description
    - **Algorithm:** Load Balancing method
    - **State:** Toggle Enable/Disable
    - **Default Server Port:** Set port (Eg:80/443)
    - **Passive Health Monitor:** Toggle Enable/Disable
    - **Active Health Monitor:** Click **Add Monitor** and choose the appropriate monitor for server health checks. If a server fails a health check, that pool member will be taken out of circulation. It is restored to circulation when the health check is successful.



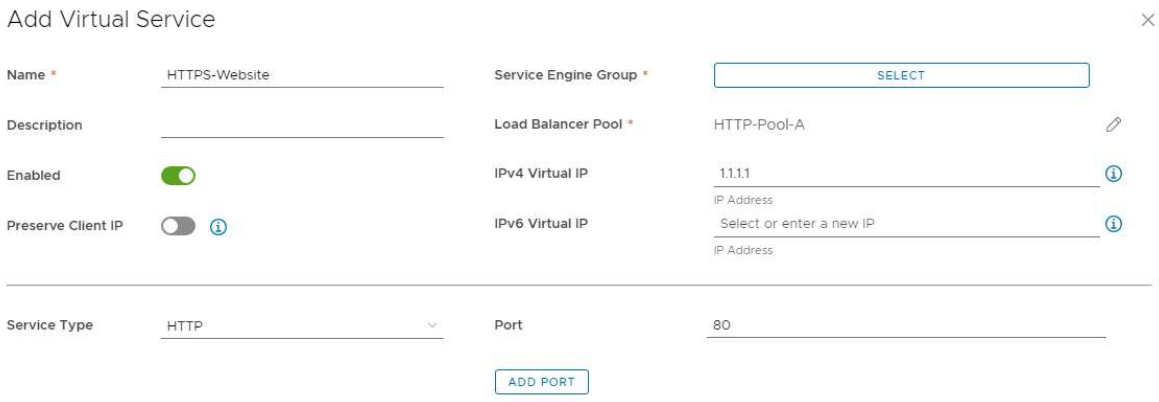
7. Add Pool Members.
    - Click on **Members** tab
    - **Member Type:** IP Address or Group
      (In this example we will use IP addresses)
    - **IP Address:** IP Address of pool member
      (Alternatively choose Group and setup an IP Set)
    - **State:** Toggle Enable/Disable
    - **Port:** port to communicate with pool member
    - **Ratio:** portion of traffic pool member will handle



8. Click **SAVE** to save pool configuration

Create Virtual Server

1. From the EduCloud homepage, click on the Organization Virtual Center card
2. From the left panel under **Networking**, click **Edges**
3. Click on the Edge Gateway name
4. Under **Load Balancer** click on **Virtual Services**
5. Click **ADD**
6. Enter Virtual Service Info
    - **Name:** Enter a Name
    - **Description:** Enter a description
    - **Enabled:** Toggle Enable/Disable
    - **Service Engine Group:** Select service engine group
    - **Load Balancer Pool:** Select the pool you created
    - **IP Address:** Enter a valid public IP address you have available
    - **Service Type:** Select service type
    - **Port:** enter port number



7. Click **SAVE**

VPN (Virtual Private Network)

VPN can be enabled on an edge gateway to create a secure tunnel between external networks and routed networks attached to the edge gateway.

EduCloud supports VPN connections between EduCloud edge gateways, and connections between edge gateways and external services.

This section provides a brief overview of the steps to initially set up an IPSec VPN connection

For a full overview of all tasks, see the "*VMware Cloud Director Documentation*" in the online help https://docs.vmware.com/en/VMware-Cloud-Director/index.html

At least one connection must be configured before the IPSec VPN Service can be enabled

Create IPsec VPN Connection

1. From the EduCloud homepage, click on the Organization Virtual Center card
2. From the left panel under **Networking**, click **Edges**
3. Click on the Edge Gateway name
4. Under **Services** click on **IPSec VPN**
5. Click **New**
6. **Add IPSec VPN Tunnel:**
    - **Name** – Optional connection name
    - **Description** – (Optional)
    - **Security Profile**: Default
    - **Status** – Enable/Disable Switch
    - **Logging** – Enable/Disable Switch
    - Click **NEXT**
    - **Authentication Mode** – Pre-Shared Key
    - **Pre-Shared Key**- enter pre-shared key
    - **Local Endpoint**
        - **IP Address -** Enter the external IP address of the edge gateway
        - **Networks** – List the local subnets to be peered in CIDR format, comma separated
    - **Remote Endpoint**
        - **IP Address** - Enter the IP address of the remote VPN device
        - **Networks** – List the remote peer subnets in CIDR format, comma separated
7. Click **NEXT** and **FINISH**

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

Edit Security Profile

- Select the VPN tunnel radio button and select **Security Profile Customization**
- **IKE Profiles**
    - **Version** - select one of the IKE versions
    - **Encryption** – choose encryption. Must match the remote site
    - **Digest** – select one of the secure hashing algorithms
    - **Diffie-Hellman Group** – select cryptography scheme. Must match remote site
    - **Association Life Time -** 86400

- **Tunnel Configuration**
    - **Enable Perfect Forward Secrecy** – Enable/Disable Switch
    - **Defragmentation Policy** – Copy
    - **Encryption** – choose encryption. Must match the remote site
    - **Digest** – select one of the secure hashing algorithms
    - **Diffie-Hellman Group** – select cryptography scheme. Must match remote site
    - **Association Life Time –** 3600

- **DPD Configuration**
    - **Probe Interval -** 60

Currently used Security Profile is Default. Changing any of the tunnel's connection properties will set the Security Profile to "User Defined".

Activate VPN Configuration

Once you have created an IPsec VPN Connection, activate the VPN tunnel

1. From the EduCloud homepage, click on the Organization Virtual Center card
2. From the left panel under **Networking**, click **Edges**
3. Click on the Edge Gateway name
4. Under **Services** click on **IPSec VPN**
5. Select the VPN tunnel radio button and click **Edit**
6. Enable Tunnel with **Status** switch
7. Click **SAVE**

Common VPN Issues

If the VPN is not working, some common issues are:

- Firewall blocking traffic. Make sure that your firewalls allow traffic between the subnets on either end of the VPN tunnel. Both the EduCloud Edge Firewall and any firewall on the other site.

- Configuration at the two ends of the VPN do not match. Specifically
    - Diffie-Hellman Group
    - Encryption Algorithm
    - Shared Key

Security Objects

A brief description of the security objects

- Static Groups – Create a static group and add networks to associate VMs
- IP Sets – An IP set is a group of IP addresses that you can add, for example, as the source or destination in a firewall rule
- Application Port Profiles – Custom application port profiles are available for use only by the Edge Gateway on which you create them.

EduCloud Network Security

Edge Gateway Firewall

The edge gateway firewall is a perimeter firewall that:

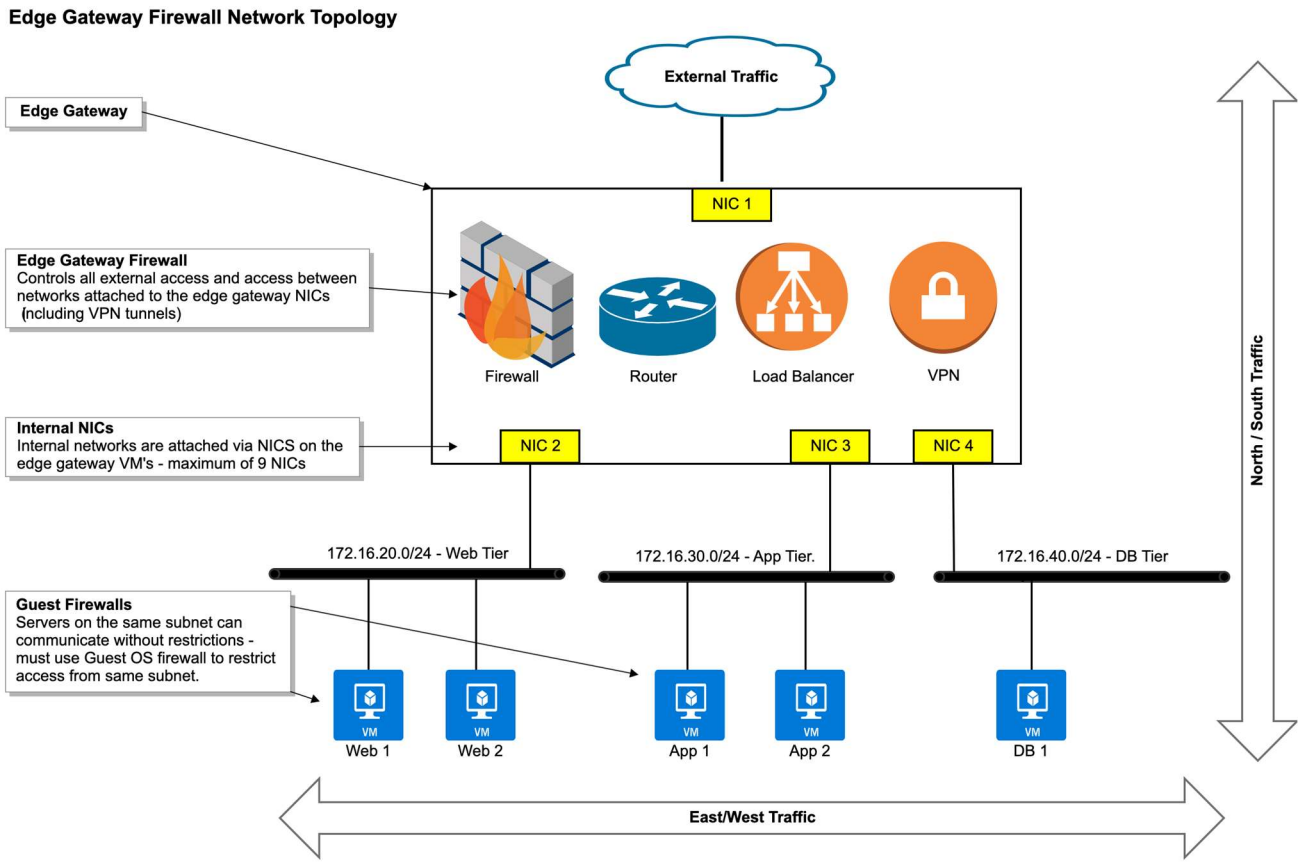
- Can control external access to services as traffic enters the edge gateway
- Can control the access permitted between all internal networks that are attached to it.
- Cannot see or control traffic that flows between VMs on the same network.
- Uses IP addresses/subnet definitions and groupings (IP Sets) as source/destination in rules

Network design plays an important role in the network security model because traffic had to traverse between networks to be seen and enforced.

A two (sometimes three) tier network design is commonly used, with application servers requiring public access being placed on the lower security network (DMZ), and supporting servers being placed on a higher security network. This allows the firewall to control:

- External access to the DMZ services
- Access between DMZ servers to supporting servers

Controlling access between servers on the same network requires enabling and managing the firewalls in each guest VM. This adds significant management overhead and challenges to fully analyze the network security posture of an application – data needs to be collected from many places.



Edge Gateway Firewall

Note: If you do not intend to use the firewall, put in a default rule that allows all traffic.

Rules are enforced in the order they are listed with the first match determining the action taken. The last rule is the default rule, which on a newly deployed edge gateway allows all traffic. Don't forget to change the default rule to deny once you have created your initial firewall rule set.

This section provides a brief overview of the most common tasks performed to manage the firewall.

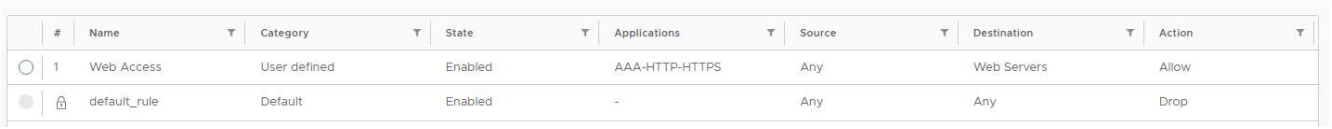
For a full overview of all tasks, see the "*VMware Cloud Director Documentation*" in the online help https://docs.vmware.com/en/VMware-Cloud-Director/index.html

Add Firewall Rule

Rules can be created to apply to incoming traffic, outgoing traffic or both.

1. From the EduCloud homepage, click on the Organization Virtual Center card
2. From the left panel under **Networking**, click **Edges**
3. Click the Edge Gateway name
4. Under **Services** click **Firewall**
5. Click **Edit Rules**

6. You can edit an existing rule or click **New On Top** to create a new rule
7. Enter a **Name** for the new rule.
8. For **Source** and **Destination**, select the Edit pencil
9. Add an **IP Set** or leave as **Any** (See creating IP sets below)
10. Set an **Applications** for specific ports (or leave blank for Any) and what **Action** (allow, reject, drop)
11. If the application/port required is not listed you will need to create an **Application Port Profile** first. (See steps below)



#	Name	Category	State	Applications	Source	Destination	Action
1	Web Access	User defined	Enabled	AAA-HTTP-HTTPS	Any	Web Servers	Allow
	default_rule	Default	Enabled	-	Any	Any	Drop

12. Click **Save**

Reorder Firewall Rules

Firewall rules are enforced in the order in which they appear in the firewall list.
If you wish to re-order the rules:

1. From the EduCloud homepage, click on the Organization Virtual Center card
2. From the left panel under **Networking**, click **Edges**
3. Click the Edge Gateway name
4. Under **Services** click **Firewall**
5. Click **Edit Rules**
6. Select the radio button of the rule you wish to re-order, then click on **Move Up** or **Move Down**
7. Click **Save**

Deleting Firewall Rules

Any "**user-defined rule**" can be deleted from the **Firewall Rules**

1. From the EduCloud homepage, click on the Organization Virtual Center card
2. From the left panel under **Networking**, click **Edges**
3. Click the Edge Gateway name
4. Under **Services** click **Firewall**
5. Select the radio button of rule you wish to delete and click **Delete**
6. Confirm the deletion and click **Delete** again to delete rule

IP Sets

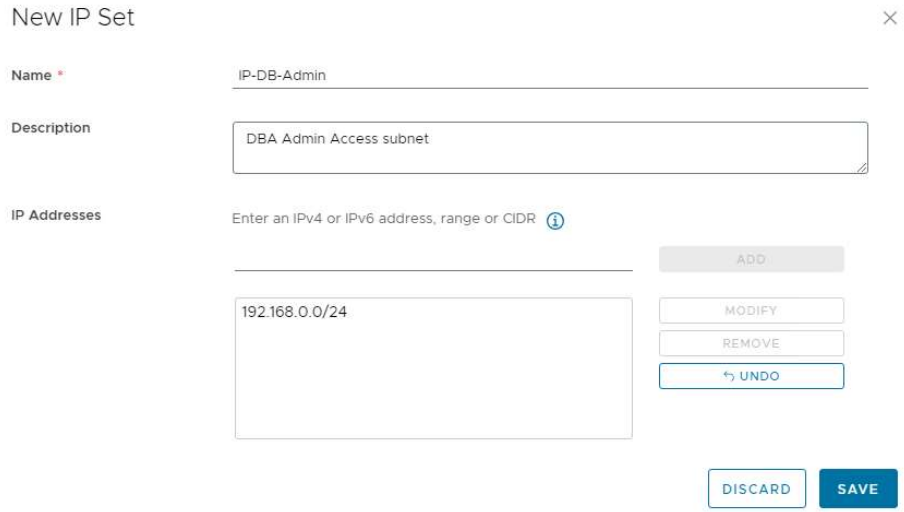
IP address group (IP set) is a way of grouping a list of IP addresses or a range of IP addresses. You can create an IP address group and then add this group as the source or destination in a firewall rule.

To create an IP set:

1. From the EduCloud homepage, click on the Organization Virtual Center card

2. From the left panel under **Networking**, click **Edges**
3. Under **Security** click **IP Sets**
4. Click **NEW**
5. Fill out the fields in the *New IP* set dialog box:

Field	Action
Name	Enter a name for the IP set. It is highly recommended to start with IP as a prefix, followed by App + Environment, ideally without any space or special characters. For example, **IP-DB-Admin**.
Description	Enter the description for the IP set. For example, "**DBA Admin Access subnet**"
IP Addresses	Enter the IP addresses that you want to include in the IP set. You can include a combination of individual IP addresses and IP ranges. You can also use CIDR format, for example 192.168.1.1/24.

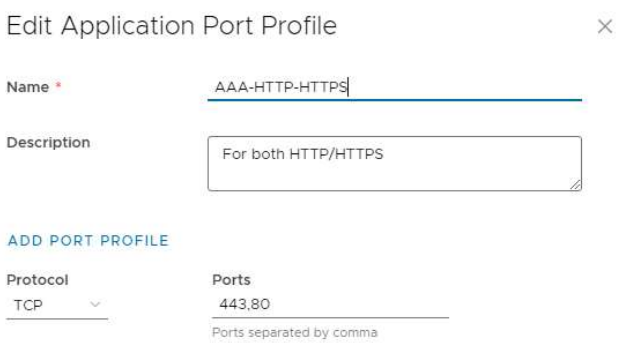


6. When you are done, click **SAVE**

Application Port Profiles

Application Port Profiles can be created for Ports to apply to incoming traffic, outgoing traffic or both.

1. From the EduCloud homepage, click on the Organization Virtual Center card
2. From the left panel under **Networking**, click **Edges**
3. Click the Edge Gateway name
4. Under **Security** click **Application Port Profiles**
5. Click **New**
6. Enter details:
    - **Name:** Name of Application Port Profile
    - **Description:** Enter optional description
    - **Protocol:** Choose correct protocol
    - **Ports:** Specify which ports



7. Click **Save** to create new application port profile