

# EDUCLOUD SERVER

## Network and Security Guide

# EduCloud Server Service – Network and Security Guide

EduCloud Networks .....	1
Direct Networks .....	1
Routed Networks .....	2
Isolated Networks .....	4
Network Management.....	4
Adding Networks to an Organization Virtual Datacenter .....	4
Create a Direct Org VDC Network .....	4
Create a Routed Org VDC Network .....	4
Create an Isolated Org VDC Network .....	5
Adding Networks to a vApp/VM .....	6
Fencing a vApp.....	6
Edge Gateway Services .....	7
DHCP.....	7
NAT .....	8
Add a Source NAT (SNAT) Rule .....	8
Add a Destination NAT (DNAT) Rule.....	9
Load Balancer .....	10
Enable Load Balancer .....	11
Create a Server Pool .....	11
Create Virtual Server .....	12
VPN (Virtual Private Network) .....	13
Create IPsec VPN Connection .....	13
Activate VPN Configuration.....	15
Common VPN Issues.....	15
SSL VPN Plus .....	15
Common SSL VPN Plus Issues .....	16
Certificates .....	16
Grouping Objects.....	16
Statistics .....	17
Edge settings .....	17
EduCloud Network Security .....	17

Edge Gateway Firewall .....	18
Distributed Firewall .....	19
Security/Network Design Considerations .....	20
Edge Gateway Firewall .....	21
Add Firewall Rule .....	21
Reorder Firewall Rules .....	22
Change Firewall Rules .....	22
Deleting Firewall Rules .....	23
Distributed Firewall .....	24
Best Practices .....	24
Grouping Object Naming Convention .....	24
Rule Naming/Ordering convention .....	25
Minimize applied to scope .....	26
Grouping Objects .....	27
Security Tags .....	27
IP Sets .....	29
Security Groups .....	31
MAC Sets .....	33
Adding Firewall Rule .....	33
Reorder Firewall Rule .....	34
Deleting Firewall Rule .....	35

## 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.

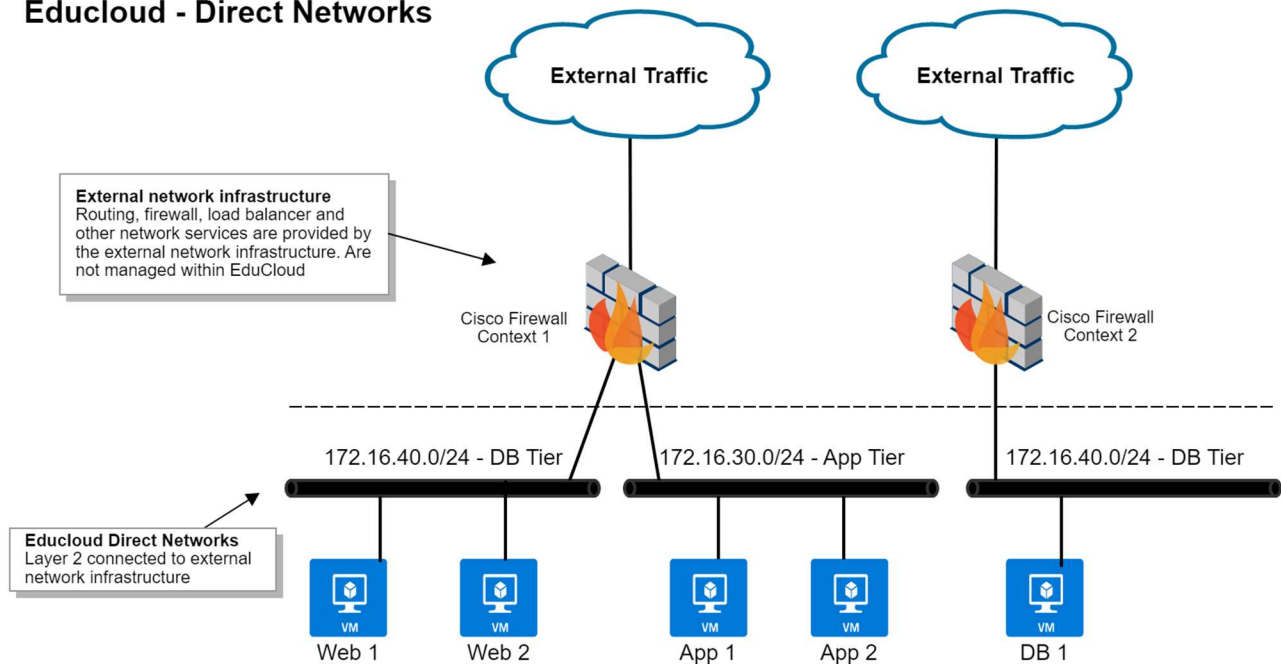
Direct networks are used to:

- 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.

## Educloud - Direct Networks



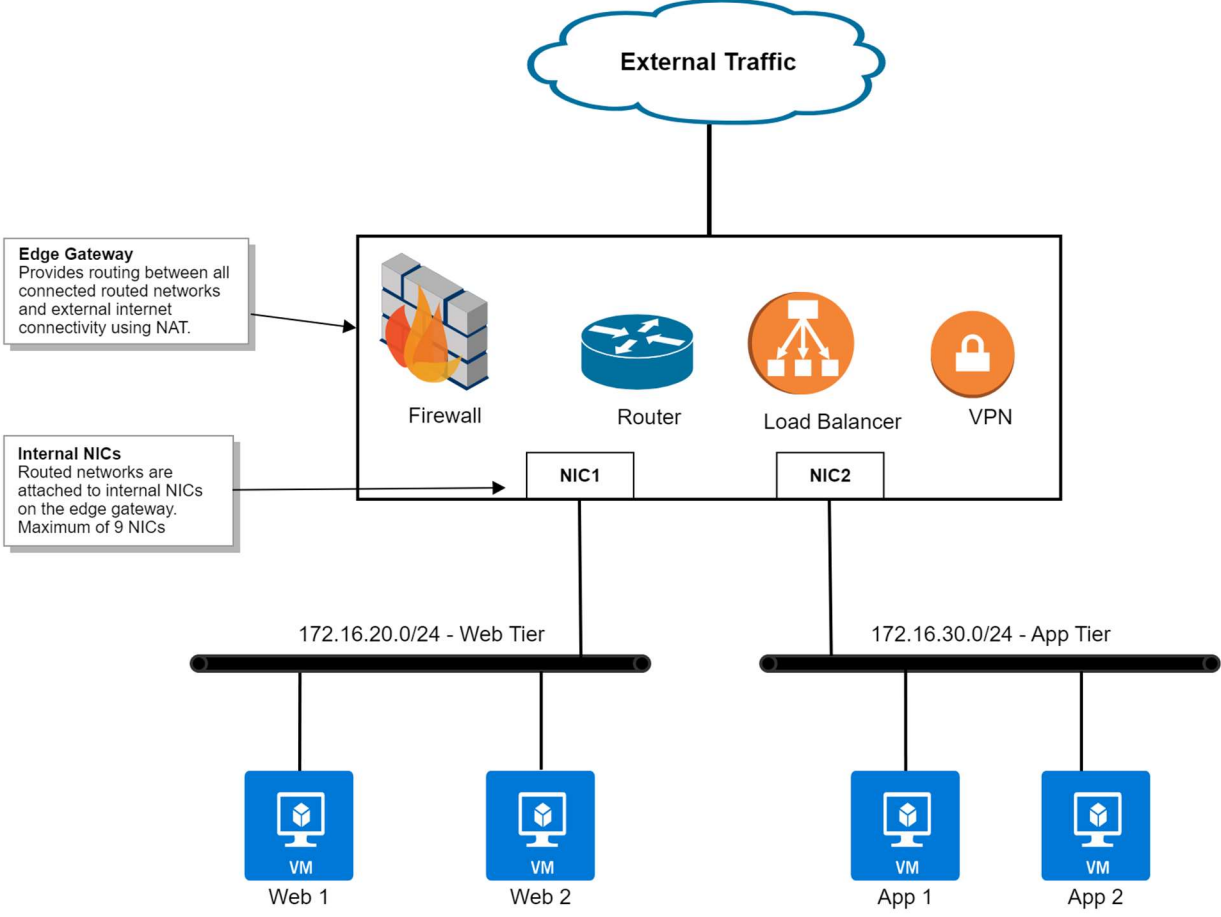
## Routed Networks

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

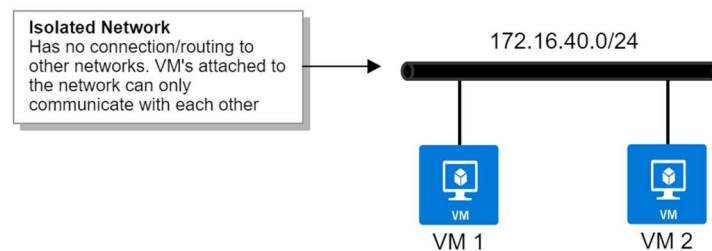


## Isolated Networks

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.

### Educloud - Isolated Networks



## 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, **Networks** → **New** and click **Next**
3. **Network Type** - select **Routed** and click **Next**
4. **Edge Connection**- select the appropriate Edge
5. **Interface Type** – select one of the three options available
  - **Internal** – attach network directly to an edge gateway interface
  - **Subinterface** – attach network via a trunked interface on the edge gateway.
  - **Distributed** – distributed networks not supported.
6. **Guest VLAN Allowed** – enable this option to enable tagging of guest VLANs in this network
7. Click **Next**
8. **Name** – enter a name for the network
9. **Gateway CIDR** – enter network information in **Gateway IP/subnet mask**, e.g. 192.168.56.254/24
10. **Description** – enter description

11. **Shared** – enable if you want to share this network across all your org VDC’s at the same site
12. Click **Next**
13. **Static IP Pools** – enter an IP range, e.g. 192.168.56.1-192.168.56.100
14. Click **Add**
15. Click **Next**
16. **DNS** – select an option:
  - **Use Edge DNS** – use DNS relay preconfigured on the gateway
  - To enter your own DNS information, deslect **Use Edge DNS**
17. Click **Next**
18. **Ready to Complete** – review settings and, if necessary, click Previous to go back and change any setting
19. Click **Finish**

Note: Each “Internal” network will consume a network interface on the edge gateway.  
 One edge gateway network interface is consumed for all “Subinterface” networks.  
 Edge gateway interface maximum = 9. Maximum subinterface networks = 200.

### 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, **Networks** → **New** and click **Next**
3. **Network Type** – select **Isolated** and click **Next**
4. **Name** – enter a name for the network
5. **Gateway CIDR** – enter network information in **Gateway IP/subnet mask**, e.g. 192.168.56.254/24
6. **Description** – enter description
7. **Shared** – enable if you want to share this network across all your org VDC’s at the same site
8. Click **Next**
9. **Static IP Pools** – enter an IP range, e.g. 192.168.56.1-192.168.56.100
10. Click **Add**
11. Click **Next**
12. **DNS** – enter DNS information
13. Click **Next**
14. **Ready to Complete** – review settings and, if necessary, click Previous to go back and change any setting
15. Click **Finish**



## Adding Networks to a vApp/VM

1. From the EduCloud homepage, click on the Organization Virtual Center card
2. On the vApp card, click **Actions** → **Add** → **Add Network** – select an option:
  - **OrgVDC Network** – select a preconfigured OrgVDC Network from the list
  - **vApp Network** – creates a new vApp network
    - i. Fill in the details for the vApp network

Add Network to Demo\_Win2016

Type  OrgVDC Network  vApp Network

Name \* Demo\_vApp\_Network

Description

Address and DNS

Gateway CIDR \* 192.168.16.254/24

Primary DNS 8.8.8.8

Secondary DNS

DNS suffix

Allow Guest VLAN

**Static IP Pools**  
Enter an IP range (format: 192.168.1.2 - 192.168.1.100)

192.168.16.1 - 192.168.16.100

192.168.16.1 - 192.168.16.100

Total IP addresses: 100

Connect to an orgVdc network

ADD

MODIFY

REMOVE

CANCEL ADD

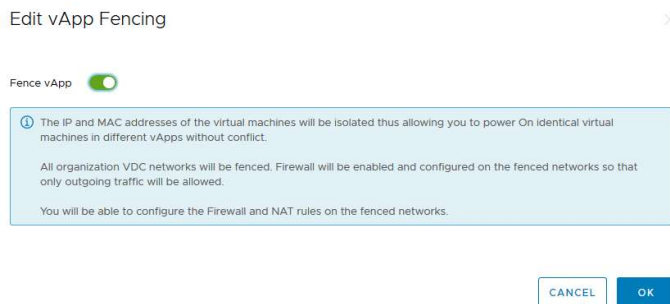
- ii. Click **Add**
3. Click **Add**
  4. On the vApp card, click **Details**
  5. Click **Virtual Machines** from the left panel
  6. Click on the name of the virtual machine
  7. Click **NICs** from the left panel
  8. Click **Edit**
  9. In the Network column, select the newly added network from the list
  10. Click **Save**

## Fencing a vApp

Fencing allows identical virtual machines in different vApps to be powered on without conflict by isolating the MAC and IP addresses of the virtual machines.

To Fence a vApp:

1. Make sure that the vApp is powered off
2. From the EduCloud homepage, click on the Organization Virtual Center card
3. Click on the vApp card
4. From the vApp menu, click on **Networks**
5. vApp Fencing → **EDIT**
6. Toggle **Fence vApp**



7. Click **OK**

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

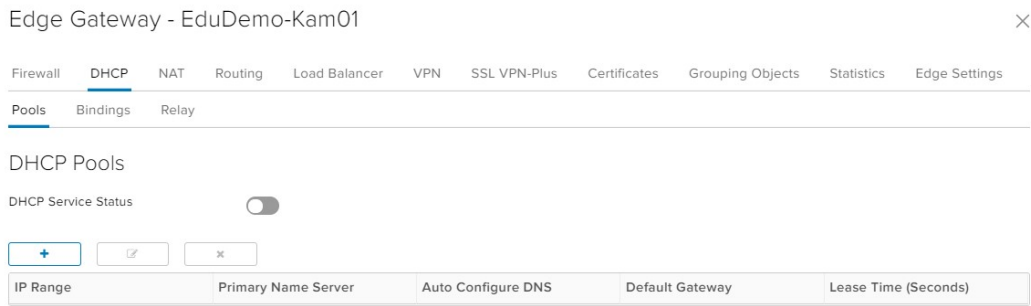
1. From the EduCloud homepage, click on the Organization Virtual Center card
2. Click on the vApp card
3. From the vApp menu, click on **Networks**
4. Click on the vApp Network
5. Configure
  - **IP Management** section for DNS, DHCP, IP Allocations
  - **Services** section for Firewall and NAT (if in a fenced vApp)

## Edge Gateway Services

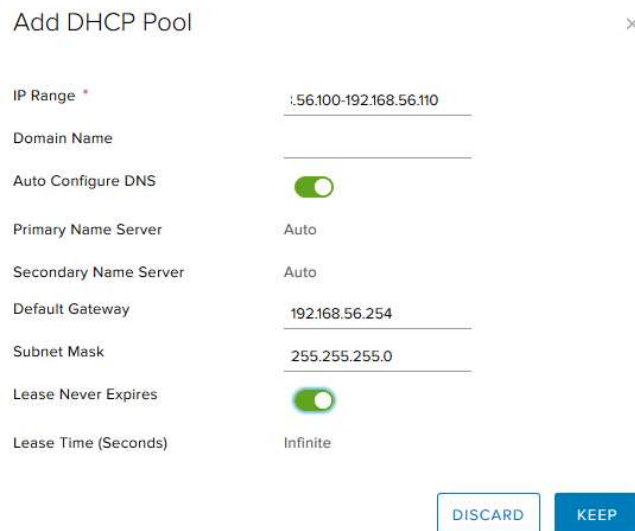
### DHCP

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, click **Edges**
3. Click the radio button on the selected Edge Gateway
4. Click **Services**



5. Click the **DHCP** tab and toggle **DHCP Service Status** if necessary.
6. Click  and enter:
  - **IP Range:** IPs available for DHCP
  - **Domain Name:** if necessary
  - **Name Servers:** or select Auto Configure to use the values set for this network
  - **Default Gateway and Subnet Mask**
  - **Lease Information**
  - **KEEP**



7. Click **KEEP**

## 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, click **Edges**

3. Click the radio button on the selected Edge Gateway
4. Click **Services**
5. Click the **NAT** tab and click + **SNAT RULE**.
6. Select an Org VDC network to be **Applied On** from the drop- down menu.
7. Type the original IP address or range of IP addresses to apply this rule on in the Original (Internal) source IP/range text box.
8. 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.
9. Select Enabled and click KEEP

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, click **Edges**
3. Click the radio button on the selected Edge Gateway
4. Click **Services**
5. Click the **NAT** tab and click + **DNAT RULE**.
6. Select an external network or Org VDC network **Applied On** from the drop-down menu.
7. Type the original IP address or range of IP addresses to apply this rule on in the Original (External) IP/range text box.
8. Choose the Protocol to apply this rule on from the drop-down menu. 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 **KEEP**.

Add DNAT Rule
✕

Applied On: Q9DC-GATEWAY2 ▾

Original IP/Range \* 206.12.149.10

Protocol TCP ▾

Original Port 80 ▾

ICMP Type ▾

Translated IP/Range \* 192.168.56.5

Translated Port any ▾

Description

Enabled

Enable logging

DISCARD
KEEP

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

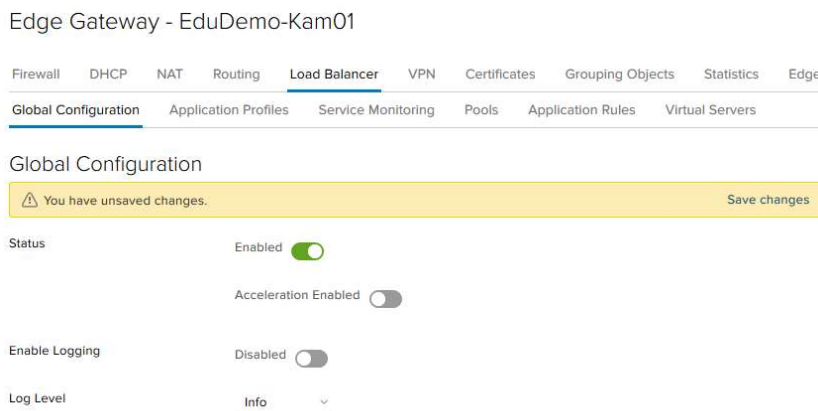
given application.

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.


## Enable Load Balancer

1. From the EduCloud homepage, click on the Organization Virtual Center card
2. From the left panel, click **Edges**
3. Click the radio button on the selected Edge Gateway
4. Click **Services**
5. **Load Balancer** tab → **Global Configuration**
6. Click **Enabled**
7. If required enable Acceleration and Logging
8. Click **Save changes**



## 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, click **Edges**
3. Click the radio button on the selected Edge Gateway
4. Click **Services**
5. **Load Balancer** tab → **Pools** → 
6. Enter Pool Info
  - **Name:** Pool Name
  - **Algorithm:** Load Balancing method
  - **Monitors:** 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.

- **Transparent:** If selected makes the client IP addresses visible to the server pool members. Transparent load balancing has special network and security design requirements to function correctly – contact us if you require it.

#### 7. Add Pool Members. For each pool member

- →
- **Name:** name for pool member
- **IP Address:** IP Address of pool member
- **Port:** port to communicate with pool member
- **Monitor Port:** port that monitor will communicate with pool member on
- **Weight:** portion of traffic pool member will handle

- **Click KEEP**

#### 8. Click **KEEP**

### Create Virtual Server

1. From the EduCloud homepage, click on the Organization Virtual Center card
2. From the left panel, click **Edges**
3. Click the radio button on the selected Edge Gateway
4. Click **Services**

5. **Load Balancer** tab → **Virtual Servers** →

6. Enter Info

- **Enable Virtual Server**
- **Name:** Enter a Name
- **IP Address:** Enter a valid public IP address  
Or click on  and choose one
- **Protocol** and **Port:** for external connections to the Virtual Server
- **Default Pool:** Choose the Pool
- **Limits:** Set limits if you wish

Add Virtual Server

General    Advanced

Enable Virtual Server

Enable Acceleration

Application Profile

Name \*

Description

IP Address \*

Protocol \*

Port \*

Default Pool

Connection Limit

Connection Rate Limit (CPS)

- Click **KEEP**

7. Click **KEEP**

## VPN (Virtual Private Network)

VPNs 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 “*Secure Access Using Virtual Private Networks*” section under “*Advanced Networking Capabilities for vCloud Director Tenants*” in the on-line help.

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, click **Edges**
3. Click the radio button on the selected Edge Gateway
4. Click **Services**
5. **VPN** tab → **IPSec VPN Sites** →



- **Enabled** - Enable this connection
- **Enable PFS** - Enable this option to have the system generate unique public keys for all IPsec VPN sessions your users initiate.
- **Name** – Optional connection name
- **Local Id** - Enter the external IP address of the edge gateway
- **Local Endpoint**- Enter the external IP address of the edge gateway
- **Local Subnets** – List the local subnets to be peered in CIDR format, comma separated
- **Peer Id** - Enter the IP address of the remote VPN device
- **Peer Endpoint**- Enter the IP address of the remote VPN device
- **Peer Subnets** – List the remote peer subnets in CIDR format, comma separated
- **Encryption Algorithm** – choose encryption. Must match the remote site
- **Authentication** – PSK, pre shared key or Certificate
- **Pre-Shared Key**- if using PSK authentication
- **Diffie-Hellman Group** – select cryptography scheme. Must match remote site
- **Digest Algorithm** – select one of the secure hashing algorithms
- **IKE Option** – select one of the IKE protocols to set up a security association in the IPsec protocol suite
- **IKE Responder Only** –
- **Session Type** – select one of the following session types:
  - Policy Based** - IPsec tunnels are used to connect multiple local subnets that are behind the NSX Edge node with peer subnets on the remote VPN site
  - Session Based** - tunneling is provided on traffic that is based on routes that were learned dynamically over a virtual tunnel interface (VTI) using a preferred protocol, such as BGP. IPsec secures all the traffic flowing through the VTI.

Add IPsec VPN
✕

Enable perfect forward secrecy (PFS)

Name

Local Id \*

Local Endpoint \*

Local Subnets \*

Subnets should be entered in CIDR format with comma as separator.

Peer Id \*

Peer Endpoint \*

Endpoint should be a valid IP, FQDN or any.

Peer Subnets \*

Subnets should be entered in CIDR format with comma as separator.

Encryption Algorithm

Authentication

Change Shared Key

Pre-Shared Key \*

Display Shared Key

The global pre-shared key (PSK) is shared by all the sites whose peer endpoint is set to "any". If a global PSK is already set, changing the PSK to an empty value and saving it has no effect on the existing setting.

Diffie-Hellman Group

Extension

Extension could be passthroughSubnets=192.168.10/24, 192.168.2.0

DISCARD
KEEP

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

### Activate VPN Configuration

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

1. From the EduCloud homepage, click on the Organization Virtual Center card
2. From the left panel, click **Edges**
3. Click the radio button on the selected Edge Gateway
4. Click **Services**
5. **VPN tab** → **IPSec VPN Service Status** →
6. Click **Save changes**

And you should then see



### 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

### SSL VPN Plus

SSL VPN-Plus enables individual remote users to connect securely to private networks behind an organizations edge gateways. The SSL encrypted tunnel is established between the client (user) and the edge gateway.

For details on SSL VPN-Plus and its configuration, see the “*Secure Access Using Virtual Private Networks*” section under “*Advanced Networking Capabilities for vCloud Director Tenants*” in the on-line help.

<https://docs.vmware.com/en/VMware-Cloud->

[Director/10.0/com.vmware.vcloud.tenantportal.doc/GUID-E0F6FEDA-2169-4E25-8B27-69ACC386AF0B.html](https://www.vmware.com/resources/compatibility/details.aspx?productGroup=vCloud%20Director&productLine=vCloud%20Director&productVersion=10.0&osFamily=Windows&osVersion=Windows%20Server%202016%20Datacenter&cpuArchitecture=amd64&appProfile=VMware%20vSphere%206.0%20U1%20ESXi%206.0%20U1&appVersion=6.0%20U1&appProfile=VMware%20vSphere%206.0%20U1%20ESXi%206.0%20U1&appVersion=6.0%20U1)

Here are additional references to other useful documents on SSL VPN-Plus setup.

<https://gogreencloud.com/knowledge-base/advanced-edge-ssl-vpn-plus-setup/>

<https://www.wavecom.ee/en/ssl-vpn-plus>

## Common SSL VPN Plus Issues

MacOS compatibility – the SSL VPN-Plus client downloaded from the edge gateway, does not support OSX Mojave or later. Install the latest “SSL VPN Plus 64-bit Client for Mac OS” available at VMware downloads. See VMware knowledge base article 76023 at <https://kb.vmware.com/s/article/76023>

## Certificates

The Secure Sockets Layer (SSL) is used by a number of edge gateway services for establishing secure encrypted communications. The SSL certificates required by these services are managed here.

SSL certificates are used by the following services:

- VPN – IPSec and L2
- SSL VPN-Plus
- Load balancing – for configurations utilizing HTTPS offload

The edge gateways support self-signed certificates, certificates signed by a Certification Authority (CA), and certificates generated and signed by a CA. Using the tenant portal, you can generate certificate signing requests (CSRs), import the certificates, manage the imported certificates, and create certificate revocation lists (CRLs).

Instructions for managing SSL certificates are found in the “*SSL Certificate Management Using the Tenant Portal*” section under “*Advanced Networking Capabilities for vCloud Director Tenants*” in the on-line help.

## Grouping Objects

A brief description of the grouping objects

- IP Sets – An IP set is a group of IP addresses that you can add as the source or destination in a firewall rule or in DHCP relay configuration
- Mac Sets – Layer 2, a MAC set is a group of MAC addresses that you can add as the source or destination in a firewall rule. There should be hardly/little need to create any mac address layer.
- Services – Pre-defined list of services/service protocols that can be used in firewall rules. It cannot be edited via tenant portal.
- Service Groups –services (as defined above) grouped by application

## Statistics

You can use the tenant portal to view statistics on the Edge Gateway Services.

1. From the EduCloud homepage, click on the Organization Virtual Center card
2. From the left panel, click **Edges**
3. Click the radio button on the selected Edge Gateway
4. Click **Services**
5. Click the **Statistics** tab
6. Navigate through the tabs depending on the type of statistics you want to see

Here is an example of IPsec VPN statistics.

Connections **IPsec VPN** L2 VPN

---

IPsec Statistics  
Last refreshed at Mar 12, 2020

IPsec VPN Statistics & Status

Peer ID	Local IP Address	Peer IP Address	Last Message	Channel Status
142.103.90.97	137.82.55.24	142.103.90.97	None	✓
192.12.177.2	137.82.55.24	192.12.177.2	None	✓
69.70.85.30	137.82.55.24	69.70.85.30	None	✓
52.138.39.61	137.82.55.24	52.138.39.61	None	✓

IPsec VPN Tunnel Statistics & Status

Local Subnet	Peer Subnet	Last Message	Tunnel Status
192.168.200.0/24	192.168.241.0/24	None	✗
192.168.200.0/24	192.168.46.0/24	None	✓
192.168.200.0/24	192.168.61.0/24	None	✓
192.168.200.0/24	10.20.0.0/24	None	✓

## Edge settings

You can customize the Syslog server for the networking-related logs of your edge gateway for those services that have logging enabled.

## EduCloud Network Security

The EduCloud service now offers two tools for managing your network access security – the edge gateway firewall, and the more recently introduced distributed firewall.

The distributed firewall offers some powerful new features that permits implementing a higher level of application security with simplified network configurations.

**Note:** The distributed firewall is disabled by default. Please submit a ticket to enable the distributed firewall for your Organization Virtual Data Center.

## 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

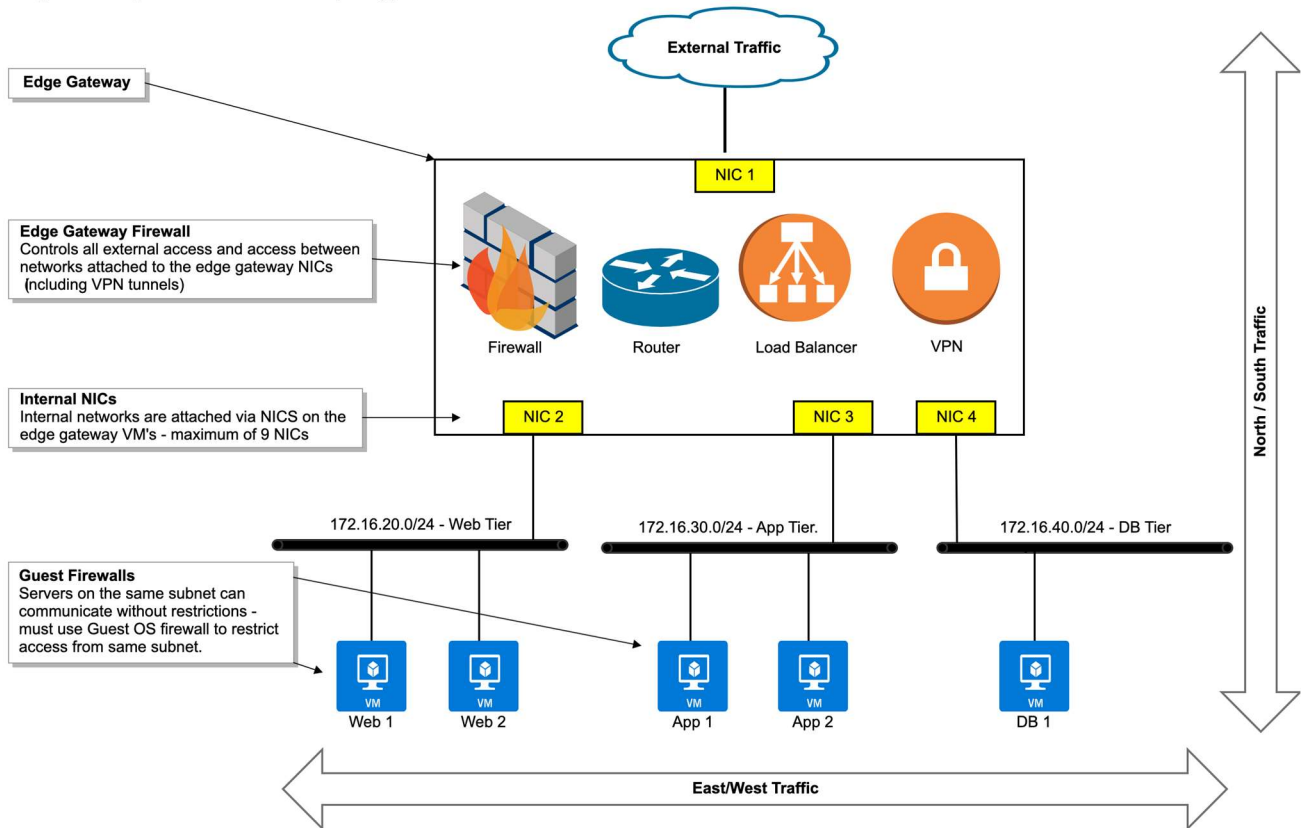
Network design plays an important role in the network security model because traffic had to traverse between networks to be seen and enforced.

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 Network Topology



## Distributed Firewall

The distributed firewall is implemented at a lower layer in the network stack. It is a hypervisor kernel-embedded firewall that:

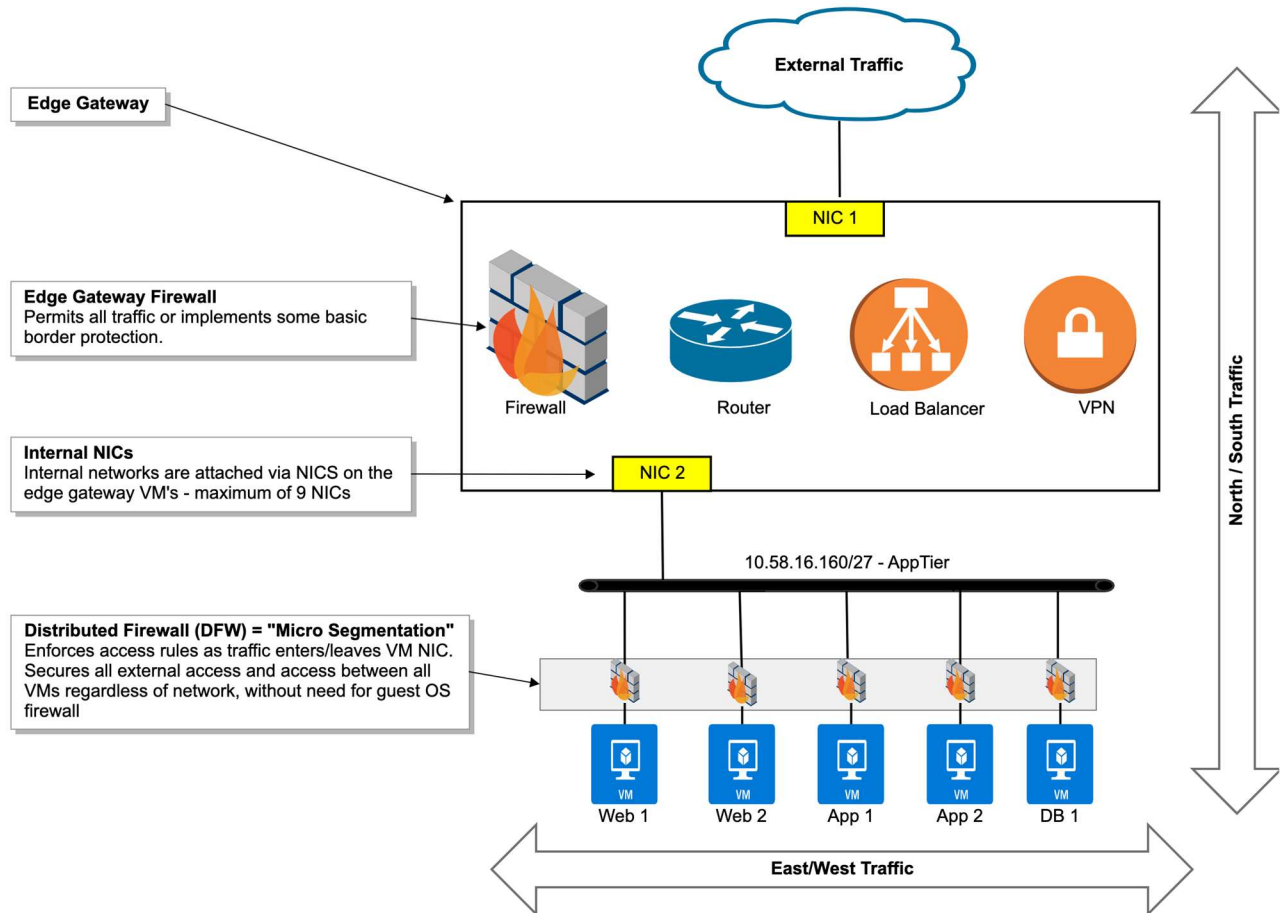
- Enforces access as traffic enters/leaves a VM's Network interface
- Is vCloud Director object aware so can also create access control policies based on VDC's, virtual machine names/tags and other objects in addition to using IP addresses and IP sets

External access and access between all VMs in your vDC can be fully controlled from one central location without the need for guest firewall management. Object awareness increases management flexibility as access controls can follow objects as they change (e.g. changing network/IP of a VM). There's one place to look to analyze an application's network security posture.

It implements microsegmentation – providing more granular network security and allowing you to better isolate workloads from one another and secure them individually.

In this model, security requirements have much less impact on network design – the applications could be secured equally well if deployed on a single network.

## Distributed Firewall Network Topology



## Security/Network Design Considerations

Customers may choose to use the edge gateway firewall, distributed firewall, or both for securing services.

If only using the edge gateway firewall, continue to design networks to provide the appropriate security zones in which to place application servers.

If only using the distributed firewall, network design is less critical for security – you may stick with traditional security zones, or deploy on a single network – both can be secured equally well.

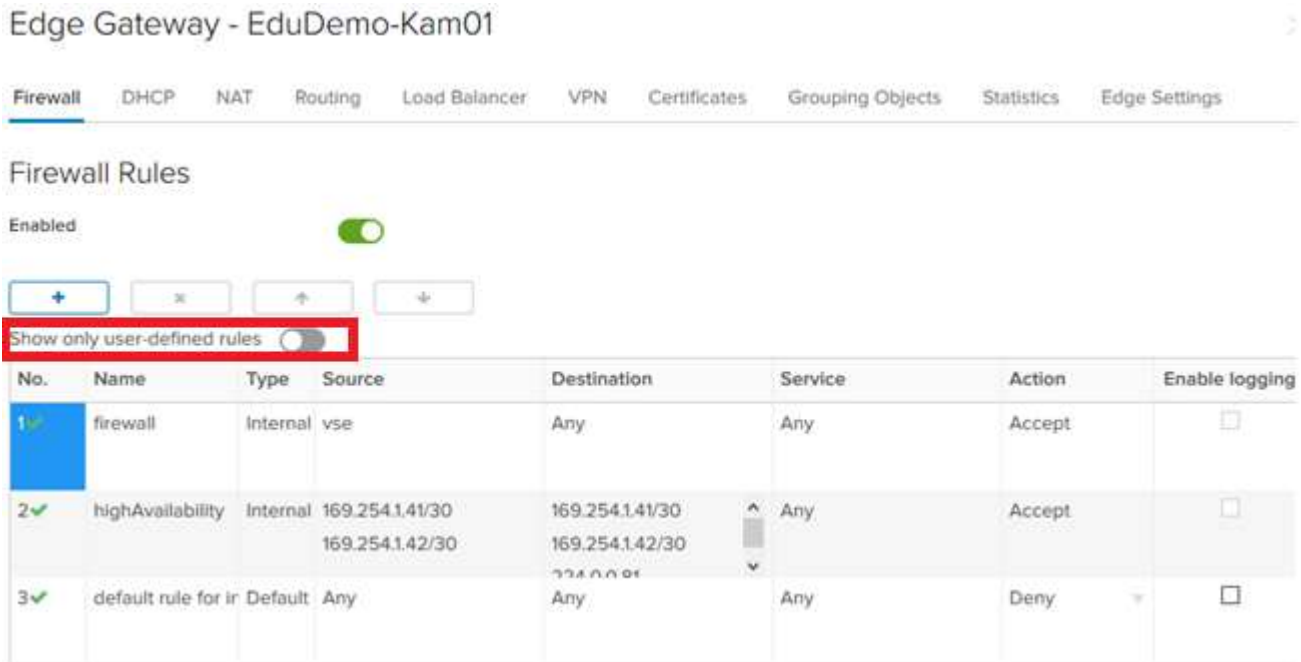
If you are considering using both firewalls in your security design, we recommend using the edge gateway firewall only for basic perimeter protection (e.g. broadly blocking all unused ports or malicious IP's at edge) and the distributed firewall for the granular access rules. Complicated rule sets in both firewalls could make analyzing and troubleshooting access control issues difficult.

Transparent load balancing for non-web based applications (where the server must see the real client IP in the TCP header) has specific network and security requirements. If you have this requirement, please contact us for assistance and we can provide you with more detailed information.

## Edge Gateway Firewall

**Note:** The edge gateway firewall tab presents an option to enable/disable the firewall. **Do not** disable the firewall – the NAT and Load Balancing services require it to be enabled in order to function. If you do not intend to use the firewall, put in a default rule that allows all traffic.

Some of the other edge gateway services will automatically create and maintain firewall rules. You can hide the system maintained rules by selecting **Show only user-defined rules**.



No.	Name	Type	Source	Destination	Service	Action	Enable logging
1	firewall	Internal	vse	Any	Any	Accept	<input type="checkbox"/>
2	highAvailability	Internal	169.254.1.41/30 169.254.1.42/30	169.254.1.41/30 169.254.1.42/30	Any	Accept	<input type="checkbox"/>
3	default rule for ir	Default	Any	Any	Any	Deny	<input type="checkbox"/>

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 “*Firewall Configuration Using the Tenant Portal*” section under “*Advanced Networking Capabilities for vCloud Director Tenants*” in the on-line help.

### 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, click **Edges**
3. Click the radio button on the selected Edge Gateway
4. Click **Services**
5. Click the **Firewall** tab then
6. Enter a name for the rule.



7. For **Source** and **Destination**, hover over the field and select **IP** and/or + as appropriate.
  - to add a new object, clicking 
  - to add a new IP range click 
8. Add an IP range or object. Or leave as the default **Any**
9. Choose the appropriate **Service** and **Action** and **Enable logging** if required.

show only user defined rules

No.	Name	Type	Source	Destination	Service	Action	Enable logging
1	New Rule	User	vnic-1	8.8.8.8	tcp:any:any	Deny	<input type="checkbox"/>



10. Then **Save changes**

 This rule set has unsaved changes. Save to start deploying. Save changes Discard changes

## 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, click **Edges**
3. Click the radio button on the selected Edge Gateway
4. Click **Services**
5. Click the **Firewall** tab
6. Click in a rule you wish to re-order, then the appropriate arrow  
 or 
7. Click **Save changes**.

 This rule set has unsaved changes. Save to start deploying. Save changes Discard changes

## Change Firewall Rules

Firewall rules can be changed by editing the values of any existing rules in the rule table.

1. From the EduCloud homepage, click on the Organization Virtual Center card
2. From the left panel, click **Edges**
3. Click the radio button on the selected Edge Gateway
4. Click **Services**
5. Click the **Firewall** tab
6. Modify the rules you wish to change.
  - Hover over a field:
    - to add a new object, clicking 
    - to enable/disable an object click 

- to add a new IP range click 
  - to delete the object, click on the “X” that appears next to it
7. Click Save changes.



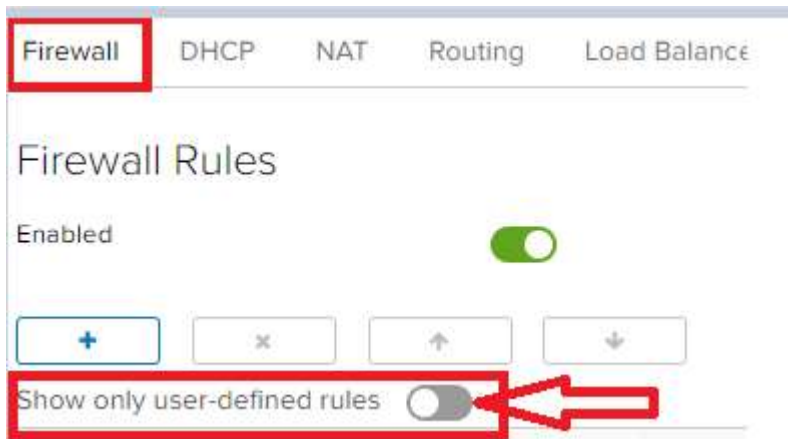
**Note:** After changing a single item in a firewall rule, the above yellow action bar may not appear until you click on a different column/row or click outside the firewall table.

**Hint:** You might have to make a table column wider in order to view/click the “X” to delete a value.

### 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, click **Edges**
3. Click the radio button on the selected Edge Gateway
4. Click **Services**
5. Click the **Firewall** tab
6. Click on “**Show only user-defined rule**”



7. Select the rule which you are planning to delete and click on **X**

## Firewall Rules

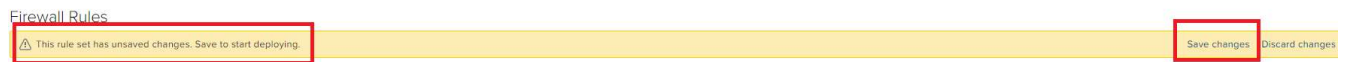
Enabled



Show only user-defined rules

No.	Name	Type	Source
1 <input checked="" type="checkbox"/>	Test Rule	User	Any

8. It will prompt with a message, click **Save changes**



## Distributed Firewall

Traditional firewall security (such as the edge gateway firewall) only allows traffic flowing between the different network interfaces the firewall controls to be secured. Traffic between individual VMs deployed on the same network could only be secured through use of the guest OS firewall.

The distributed firewall enforces firewall rules at the VM level. It inspects every packet and frame coming to and leaving the VM regardless of the network topology. This allows traffic flowing between VM's on the same network to be fully secured without needing to use guest OS firewalls, a feature known as **microsegmentation**.

This mechanism makes network security more granular, and allows for full security to be implemented using much simpler network architectures. Thus, separate networks (security zones) are no longer a necessity.

Please note: It is imperative to use vmware tools when VM names are used as security tags in NSX distributed firewall. The distributed firewall rules will fail to apply on VM's without VMware tools.

**Note:** The distributed firewall is disabled by default. Please submit a ticket to enable the distributed firewall for your Organization Virtual Data Center.

## Best Practices

### Grouping Object Naming Convention

In many situations, you may want to use the same set of objects in multiple rules. For example, you may want to group web servers or other application servers together to use in a ruleset. Grouping objects help keep the ruleset clean and easy to read.

When viewing objects in the firewall rules table, it can be difficult to tell the type of object being referenced. To assist with quick identification of object type we recommend prefixing grouping object names with a type identifier.

- IP- = IP Set
- ST- = Security Tag
- SG- = Security Groups

Where possible, follow the prefix with the same naming standards you adopt for rule naming (next section) so the relationship between the grouping objects and firewall rules can be easily identified.

In the following example we use the same “app-environment” standard adopted for rule names to name security tags and security groups.

IP sets also often identify specific networks or locations (not app specific), so a consistent convention was adopted for naming these IP sets

The above standards result in a natural grouping of rules by service or purpose when sorted by name.

Examples of the adopted convention are given in the following table

*Grouping object naming examples:*

<b>Objects Type</b>	<b>Name</b>	<b>Description</b>
Security Group	SG-SVC1-STG-WEB	Service 1 web servers - staging
	SG-SVC1-STG-APP	Service 1 app servers - staging
	SG-SVC1-STG-DB	Service 1 DB servers -staging
	SG-SVC1-STG-USERS	Service allowed users - staging
	SG-DBA-ADMIN	DBA Admin access rights
Security Tag	ST-SVC1-STG-WEB	Service 1 web server tag - staging
	ST-SVC1-STG-APP	Service 1 app server tag - staging
	ST-SVC1-STG-DB	Service 1 db server tag - staging
IP Set	IP-UBC-Campus	UBC campus IP space
	IP-UBC-PG	UBC Point Grey Campus IP space
	IP-UBC-VPN	MyVPN IP subnets
	IP-SVC1-STG-KAM	Service 1 Kamloops staging servers

### **Rule Naming/Ordering convention**

Similar to grouping objects, establishing a naming convention for firewall rules, and keeping related rules grouped together makes it simpler to analyze, understand and modify the firewall rule set.

We recommend beginning firewall rule names with an application + environment prefix, followed by any other descriptive information needed to clearly identify the purpose of the rule. The name field accepts up to 255 characters – it is effectively the description field for your rule.

There may be some types of rules that are global or not application specific. Try to adopt a consistent naming standard for them.

Order your firewall rules so all rules with the same prefix or purpose are grouped together.

The following table shows a sample ruleset following the above guidelines. Only a subset of the firewall columns are shown (The applied to column is not shown):

#	Name	Source	Destination	Service	Action	Dir
1	LDAP-DEV – Client access	IP-UBC-CAMPUS	SG-LDAP-DEV-SRV	ldaps	Allow	In
2	LDAP-DEV – Admin access	SG-LDAP-DEV-Admins	SG-LDAP-DEV-SRV	Ldap:ldaps:ssh	Allow	In
3	SVC1-DEV – Clients to web	Any	SG-SVC1-DEV-WEB	443	Allow	In
4	SVC1-DEV – Web to app	SG-SVC1-DEV-WEB	SG-SVC1-DEV-APP	443	Allow	In
5	SVC1-DEV – App to DB	SG-SVC1-DEV-APP	SG-SVC1-DEV-DB	1433	Allow	In
6	ADMIN - Puppet	IP-UBC-ADMIN-NET	SG-PUPPET-Clients	22:8140	Allow	In
7	ADMIN - Monitoring	10.20.55.92	SG-MONITOR-Clients	80:443	Allow	In
8	Allow Ping	Any	Any	ICMP Echo	Allow	In
9	Allow all outbound	Any	Any	Any	Allow	Out
10	Default Deny Rule	Any	Any	Any	Deny	In/Out

### Minimize applied to scope

Don't apply the rule to everything if it can be applied to a subset – it is more efficient for the firewall to process and consumes less resources.

If both the source and destination targets contain vCD objects, the *applied to* scope must include all of those objects for the rule to work correctly.

In the table below, the first rule shows a rule applied at the VDC level. The second a more efficient version of the same rule applied only against the source and destination objects.

#	Name	Source	Destination	Service	Action	Dir	Applied To
1	SVC1-DEV – Web to app Server	SG-SVC1-DEV-WEB	SG-SVC1-DEV-APP	https	Allow	In	OrgVDC
2	SVC1-DEV – Web to app Server	SG-SVC1-DEV-WEB	SG-SVC1-DEV-APP	https	Allow	In	<b>SG-SVC1-DEV-WEB</b> <b>SG-SVC1-DEV-APP</b>

By default a new rule will be applied across the entire virtual datacenter.

## Grouping Objects

### Security Tags

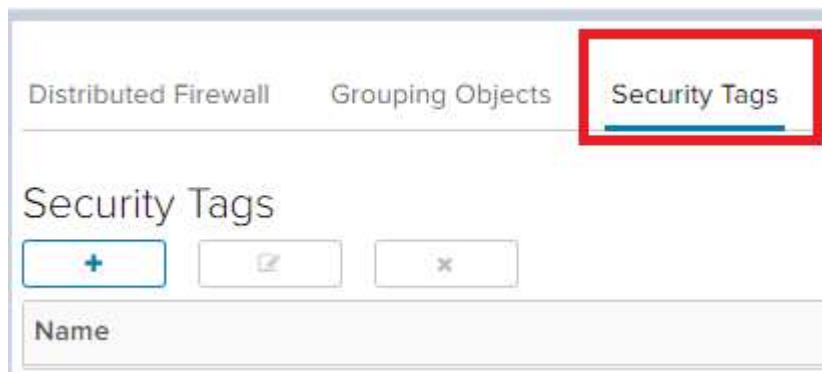
Security tags are labels which can be associated with a virtual machine or a group of virtual machines. Only VM's can be tagged. Security tags are designed to be used with security groups. Once you create the security tags, you associate them with a security group which can be used in firewall rules. You can create, edit, or assign a user-defined security tag. You can also view which virtual machines or security groups have a particular security tag applied.

To configure Security Tag:

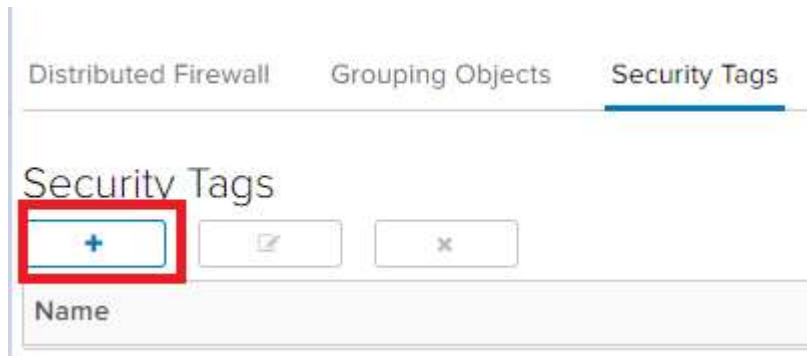
1. From the EduCloud homepage, click on the Organization Virtual Center card
2. From the left panel, click **Security**
3. Select a Security Service from the list
4. Click **Configure Services**



5. In the **Services** dialog box, select the **Security Tags** tab



6. In the Security Tags, click the + button



7. Fill out the fields in the *New Security Tag* dialog box

Field	Action
Name	Enter a name for the Security Tag. It is highly recommended to start with ST as a prefix, followed by App + Environment, ideally without any space or special characters. For example, <b>ST-KRB-STG</b> .
Description	Enter the description for the Security Tag. For example, “ <b>UBC.CA Kerberos Realm - Staging</b> ”
Browse Objects of type	Select “Virtual Machines”
Filter	Select a label which can be associated with a virtual machine or a group of virtual machines

Name ST-KRB-STG

Description ubc.ca Kerberos Realm  
- Staging

**ASSIGN / UNASSIGN VMS**

Browse objects of Virtual Machines type:

VIRTUAL MACHINES ▶

Filter...

<ul style="list-style-type: none"> <li><b>EAD-SDCT8</b></li> <li></li> <li>IAM_ELDAP2_STG_eldap</li> <li></li> <li>IAM_CAC_STG_...</li> </ul>	<p>←</p> <p>→</p>	<ul style="list-style-type: none"> <li><b>IAM_StgKrb1k-6nDc</b></li> </ul>
---	-------------------	--

Current page:

**DISCARD** **KEEP**

8. When you are done, click **Keep**

### 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



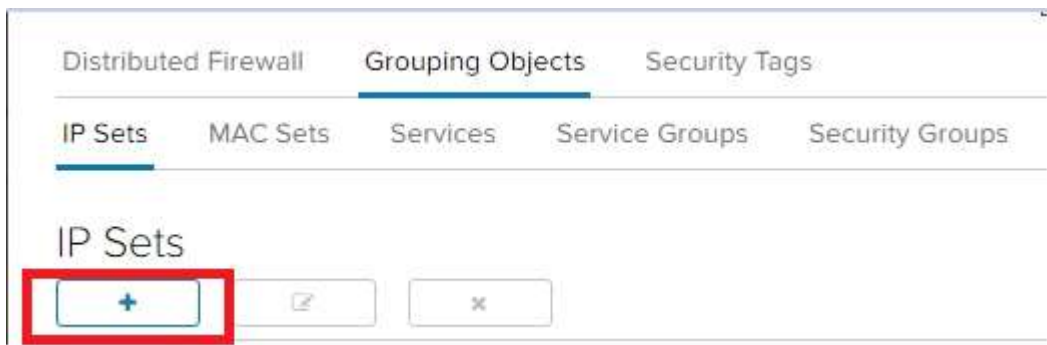
- From the left panel, click **Security**
- Select a Security Service from the list
- Click **Configure Services**



- In the **Services** dialog box, select the **Grouping objects** tab



- In the **IP Sets** tab, click the + button



- 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, <b>IP-DB-Admin</b> .
Description	Enter the description for the IP set. For example, “ <b>DBA Admin Access subnet</b> ”
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.
Inheritance	Select this option to enable the IP set to be consumed by underlying scopes.

## New IP Set ×

Name \*

Description

IP Addresses \*

eg: 192.168.200.1,192.168.200.1/24, 192.168.200.1-192.168.200.24

Inheritance

8. When you are done, click **Keep**

### Security Groups

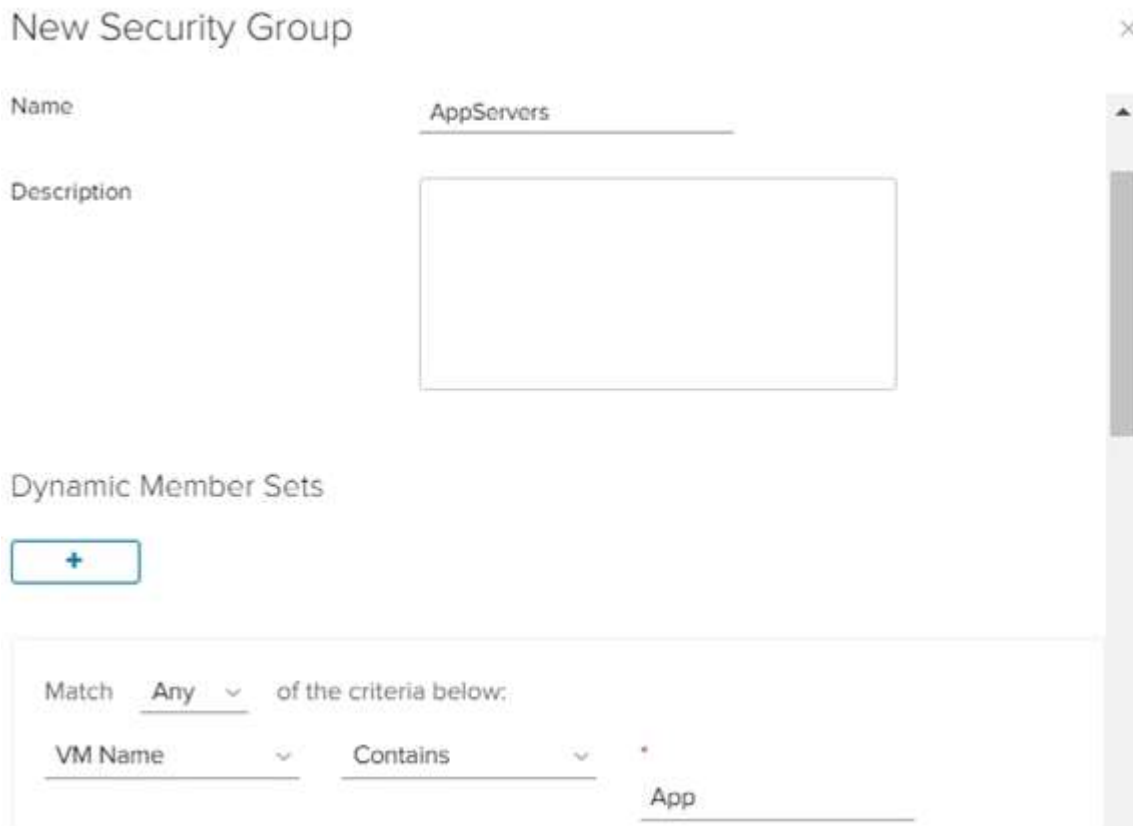
A security group is a collection of assets or grouping objects, such as virtual machines, Org VDC network, or security tags. Security groups can have dynamic membership criteria based on security tags, VM name, VM Guest OS name, or VM Guest Host name. For example, all VM's that have the security tag "web" will be automatically added to a specific security group destined for Web servers. After creating a security group, a security policy is applied to that group.

To create a Security Group:

1. From the EduCloud homepage, click on the Organization Virtual Center card
2. From the left panel, click **Security**
3. Select a Security Service from the list
4. Click **Configure Services**
5. In the **Services** dialog box, click the **Grouping Objects** tab
6. In the Security Groups tab, click the + button



7. In the *New Security Group* dialog box, enter a **Name** and **Description** for the security group. For naming convention, it is highly recommended to start with SG as a prefix, followed by App + Environment, ideally without any space or special characters. For example, **SG-SHIB-STG**
8. In the *Dynamic Member Sets* section, click the + button and specify the criteria for the security group. In the image below any existing VM with **App** in its name and any VM created in the future with **App** in its name will be included in the security group.

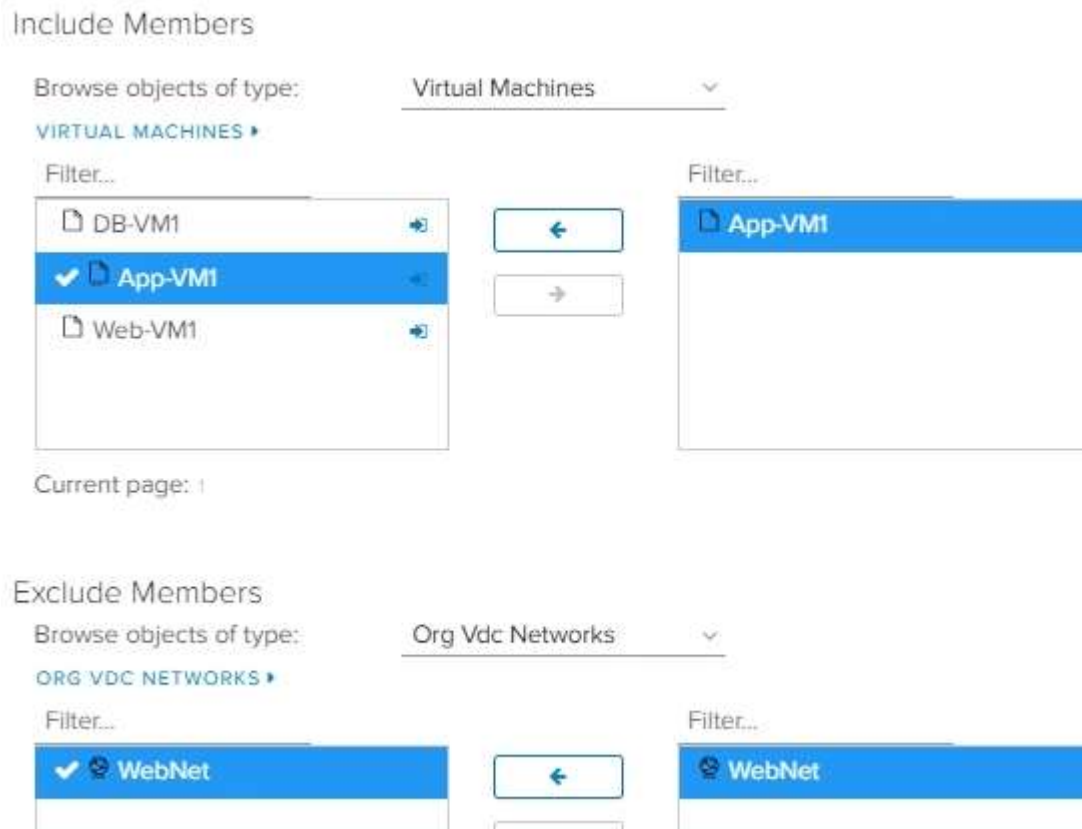


9. In the *Include Members* section, instead of creating the members of the group dynamically, you can explicitly specify members to include in the group. Members can include VMs, Org VDC networks, IP sets, MAC sets or security tags.

Select the type of object, then select individual objects and click the right arrow to add them to the group.

10. In the Exclude Members section, you can exclude specific objects from the security group.

Select the type of object, then select individual objects and click the right arrow to exclude them from the group.



11. When you are done, click **Keep**

## MAC Sets

If you want to use MAC address based filtering, it is easier to group the addresses in a MAC set. Please note: MAC address filtering is NOT often used, since MAC address can change, e.g. if you remove/add NIC.

## Adding Firewall Rule

To Create firewall rule:

1. From the EduCloud homepage, click on the Organization Virtual Center card
2. From the left panel, click **Security**

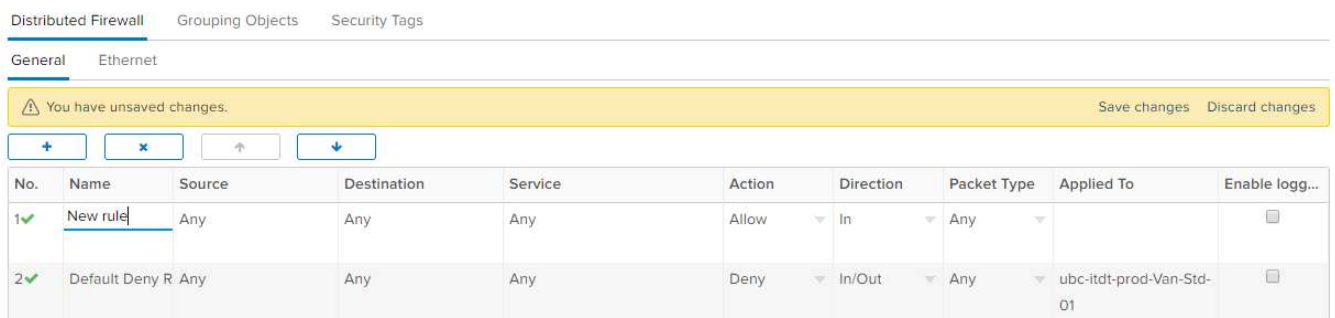
3. Select a Security Service from the list
4. Click **Configure Services**
5. Select the **Distributed Firewall** tab



6. Click the + button to add a new row to the firewall rules table.



7. For the New **Rule**, specify a **Name**



8. In the **Source** and **Destination** fields, specify the source and destination addresses for the firewall rule
9. Select whether the rule is an **Accept** or **Deny** rule
10. If you have a syslog server configured, select the **Enable logging** check box
11. Click **Save changes**

## Reorder Firewall Rule

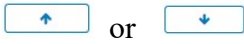
Firewall rules are enforced in the order in which they appear in the firewall list.

To re-order the rules:

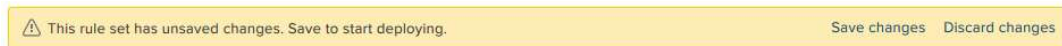
1. From the EduCloud homepage, click on the Organization Virtual Center card
2. From the left panel, click **Security**
3. Select a Security Service from the list
4. Click **Configure Services**
5. Click the **Distributed Firewall** tab



6. Click in a rule you wish to re-order, then the appropriate arrow



7. Click **Save changes**.



## Deleting Firewall Rule

To delete Firewall rules:

1. From the EduCloud homepage, click on the Organization Virtual Center card
2. From the left panel, click **Security**
3. Select a Security Service from the list
4. Click **Configure Services**
5. Select the **Distributed Firewall** tab
6. Select the rule to be deleted
7. Click on the “X”

