

EduCloud Server Service – Network Guide

EduCloud Networks	1
Direct Networks	1
Routed Networks	2
Isolated Networks	2
Network Management.....	3
Adding Networks to an Organization Virtual Datacenter	3
Create a Direct Org VDC Network	3
Create a Routed Org VDC Network	3
Create an Isolated Org VDC Network	4
Adding Networks to a vApp/VM.....	5
Adding an Org VDC Network.....	5
Adding a vApp Network	5
Fencing a vApp	6
Configuring Edge Gateway Services.....	7
DHCP Configuration.....	7
Add a Source NAT (SNAT) Rule.....	8
Add a Destination NAT (DNAT) Rule	9
Firewall Configuration	10
Enable/Disable Firewall	10
Add Firewall Rule	11
Reorder Firewall Rules.....	11
Load Balancer Configuration	12
Load Balancing Key Concepts	12
Load Balancing Initial Global Configuration	12
Create a Server Pool	13
Create Virtual Server	14
VPN (Virtual Private Network)	15
Create IPsec VPN Connection	15
Activate VPN Configuration	16
Common VPN Issues.....	16

EduCloud Networks

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

1. Direct
2. Routed
3. Isolated

vCloud Director also can define Cross-VDC networks. But this feature is not currently supported in EduCloud.

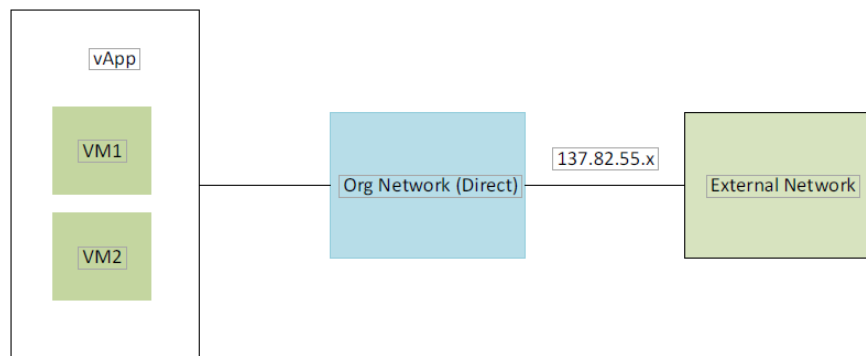
Direct Networks

Direct Networks provide direct layer 2 connectivity.

Depending on the setup of the network and its configuration in EduCloud, it may connect virtual machines (VMs) to others within an organization, to other organizations and/or to outside EduCloud. Network configurations such as firewalls and NAT are outside of EduCloud.

Direct Networks are also used in EduCloud to provide external connectivity to Edge Gateways and thus to other types of Org VDC Networks.

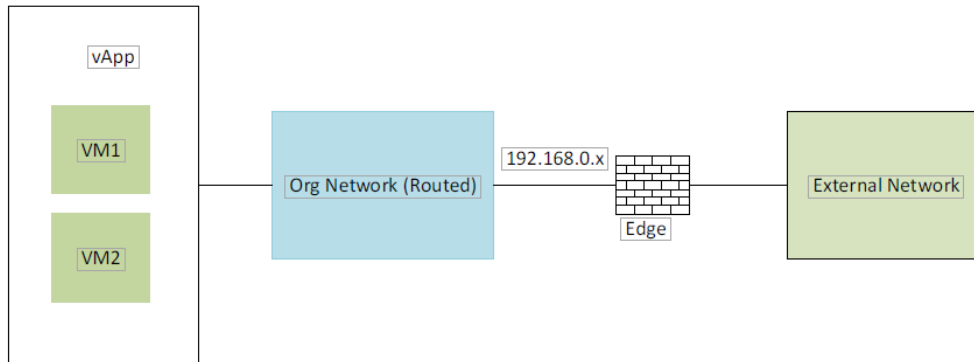
Direct Networks can only be configured by EduCloud system administrators. They are primarily used for external connectivity and by some University of BC organizations.



Routed Networks

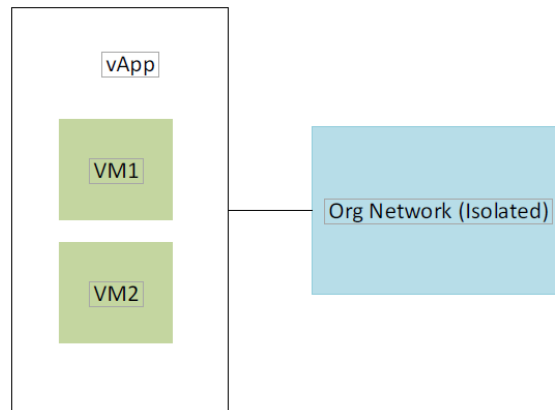
Routed Networks are configured within an organization and only VMs in the organization can be connected to it.

A routed network provides access to external networks subject via NAT on an Edge Gateway. Organization administrators can configure NAT, firewalls and VPN, configuring access to and from VMs in the organization.



Isolated Networks

Isolated Networks are configured within an organization and only VMs in the organization can be connected to it. There is no connectivity to anything outside the organization on these networks.



Network Management

Adding Networks to an Organization Virtual Datacenter

Create a Direct Org VDC Network

For an Organizations using Direct Networks, please submit a ticket. Generally, in EduCloud, this is only for University of B.C. orgs.

Create a Routed Org VDC Network

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

- **Datcenters** → **Networking** → **Networks** → **NEW**
- **Org VDC** – choose as appropriate
- **Name** – enter a name for the network
- **Type** - select **Routed network connected to an existing edge gateway**
- **Edge Gateway**- select the appropriate Edge
- **Interface Type** – choose **Internal**
- Enter network info

Add Org VDC Network

Org VDC * EduDemo-Kam-Std

Name * external-vdcorg-net

Description

Share this network with other VDCs in this organization

Type *

Isolated network within this Virtual Data Center

Routed network connecting to an existing edge gateway

Name	# External Networks	# Org VDC Networks	# Available Networks
EduDemo-Kam01	1	0	9

1 - 1 of 1 items

Allow Guest VLAN

Interface type Internal

Address and DNS

Network 192.168.56.254/24

Gateway CIDR *

Use Gateway DNS

Primary DNS 8.8.8.8

Secondary DNS

DNS suffix

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

192.168.56.1 - 192.168.56.2

Total IP addresses in pool: 250

NEW

MODIFY

REMOVE

SAVE DISCARD

Note that the Network Gateway CIDR format is **Gateway/subnet mask**

- Click **SAVE**

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.

- Creation is the same as the previous section – just choose **Isolated network within this Virtual Data Center** and you won't have an **Edge Gateway** to select

The screenshot shows the 'Add Org VDC Network' configuration page. The form is divided into several sections:

- Org VDC:** A dropdown menu showing 'EduDemo-Kam-Std'.
- Name:** A text input field containing 'isolated-org-vdc-net'.
- Description:** A large empty text area.
- Type:** Three radio button options:
 - Share this network with other VDCs in this organization
 - Isolated network within this Virtual Data Center
 - Routed network connecting to an existing edge gateway
- Address and DNS:**
 - Network:** Text input field with '192.168.56.254/24'.
 - Gateway CIDR:** Text input field with 'Use Gateway DNS' checkbox.
 - Primary DNS:** Text input field with '10.10.10.10'.
 - Secondary DNS:** Text input field.
 - DNS suffix:** Text input field.
- Static IP Pool:**
 - Text input field with '192.168.56.1 - 192.168.56.2'.
 - Buttons: 'N', 'MO', 'REN'.
 - Text below: 'Total IP addresses in pool: 250'.

At the bottom of the form are two buttons: 'SAVE' and 'DISCARD'.

Adding Networks to a vApp/VM

To add a network to a VM:

1. Add it to the vApp first
2. Then add/configure a NIC with the network to the VM

Adding an Org VDC Network

To add an Org VDC network to a vApp (for use by a VM):

- **Datcenters** → **Compute** → **vApps** → **Details** → **Networks** tab
- **NEW**
- Choose **Org VDC Network**
- Select the Org VDC Network
- **ADD**

Adding a vApp Network

To add a vApp network (for use by a VM):

- **Datcenters** → **Compute** → **vApps** → **Details** → **Networks** tab
- **NEW**
- Choose **vApp Network** and enter Network information
- Choose whether to connect to an orgVDC network and if so, select the orgVDC Network

Add Network to Demo_Win2016

Type OrgVDC Network vApp Network

Name * Dem-+Win2016_vApp_Network

Description

Address and DNS

Gateway * 10.10.25.254

Network mask * 255.255.255.0

Primary DNS 8.8.8.8

Secondary DNS

DNS suffix

Allow Guest VLAN

Static IP Pool

Enter an IP range (format: 192.168.1.2 - 192.168.1.100)

10.10.25.1-10.10.25.99

ADD

MODIFY

REMOVE

Connect to an orgVDC network

Status	Name	Org VDC	Gateway address	Routing	Connected To	IP Pool Consumed
✓	ACCESS-PROD	EduDemo-Kam-Std	137.82.164.190/26	Direct	DR-ACCESS-PROD	0%
✓	UBC-IT	EduDemo-Kam-Std	10.10.3.1/24	Isolated	UBC-IT	1%
✓	external-vdcorg-net	EduDemo-Kam-Std	192.168.56.254/24	Routed	EduDemo-Kam01	0%
✓	UBC-IT-BAK	EduDemo-Kam-Std	10.10.16.1/24	Isolated	UBC-IT-BAK	0%

CANCEL ADD

- **ADD**

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

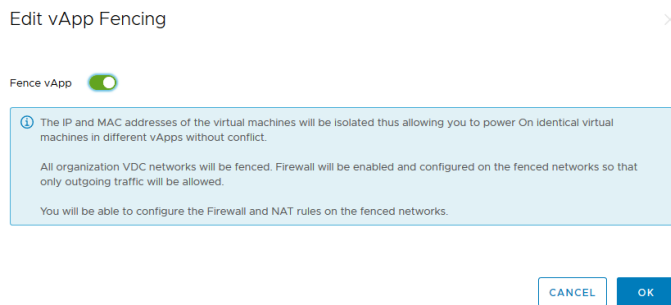
- **Datacenters** → **Compute** → **vApps** → **Details** → **Networks** tab
- Click on the vApp Network
- **Configure**
 - **IP Management** tab for DNS, DHCP, IP Allocations
 - **Services** tab for Firewall
 - **Routing** tab for NAT to the orgVDC network

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:

- **Datacenters** → **Compute** → **vApps** → **Details** → **Networks** tab
- vApp Fencing → [EDIT](#)
- Toggle **Fence vApp**



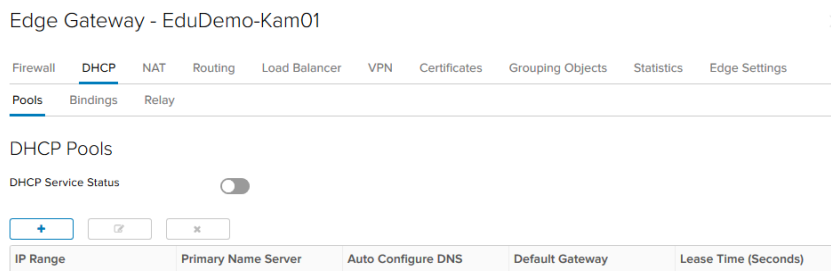
- **OK**

Configuring Edge Gateway Services

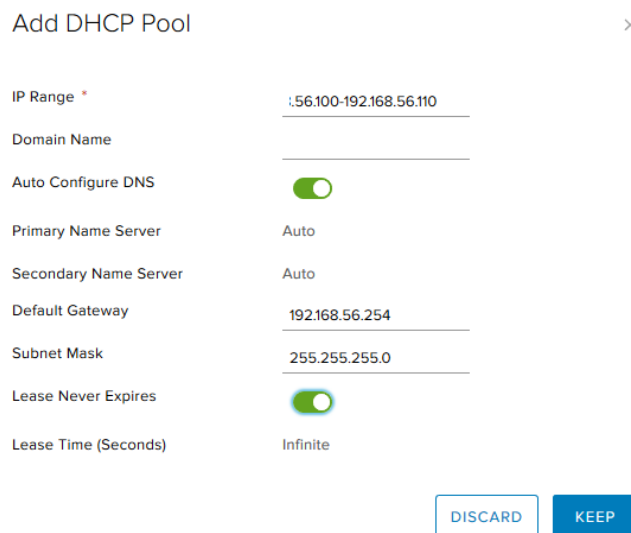
DHCP Configuration

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

- **Datacenters** → **Networking** → **Edges** → Select the Edge
- **CONFIGURE SERVICES**



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



- Click [Save changes](#)

Add a Source NAT (SNAT) Rule

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

- Datacenters → Networking → Edges → [CONFIGURE SERVICES](#)
- Click the **NAT** tab and click + [SNAT RULE](#).
- Select an Org VDC network to be **Applied On** from the drop- down menu.
- Type the original IP address or range of IP addresses to apply this rule on in the Original (Internal) source IP/range text box.
- 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.
- Select Enabled and click **KEEP**

Add SNAT Rule ×

Applied On:

Original Source IP/Range *

Translated Source IP/Range *

Description

Enabled

Enable logging

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.

- Datacenters → Networking → Edges → [CONFIGURE SERVICES](#)
 - Click the **NAT** tab and click [+ DNAT RULE](#).
 - Select an external network or another Org VDC network **Applied On** from the drop-down menu.
 - Type the original IP address or range of IP addresses to apply this rule on in the Original (External) IP/range text box.
 - Choose the Protocol to apply this rule on from the drop-down menu.
- To apply this rule on all protocols, select **Any**.
- (Optional) Select an Original port to apply this rule to.
 - (Optional) Select an ICMP type to apply this rule to if this rule applies to ICMP.
 - 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.
 - (Optional) Select a port for inbound packets to be translated to from the Translated port drop-down menu.
 - Select Enabled, and click **KEEP**.

Add DNAT Rule ×

Applied On:

Original IP/Range *

Protocol

Original Port

ICMP Type

Translated IP/Range *

Translated Port

Description

Enabled

Enable logging

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

Firewall Configuration

Enable/Disable Firewall

- Datacenters → Networking → Edges → [CONFIGURE SERVICES](#)
- Click the **Firewall** tab and select **Enabled** to enable firewall services, or deselect it to disable firewall services.
- Click [Save changes](#).

On a new Edge Gateway, you will see some pre-defined Firewall Rules. You can hide them by selecting **Show only user-defined rules**.

As with many Firewall configurations, rules are enforced in the order they are listed. Thus, the last rule will be the default rule. On a new Edge, unless modified or superseded by another rule, that predefined last rule allows all traffic.

Edge Gateway - EduDemo-Kam01

[Firewall](#) [DHCP](#) [NAT](#) [Routing](#) [Load Balancer](#) [VPN](#) [Certificates](#) [Grouping Objects](#) [Statistics](#) [Edge Settings](#)

Firewall Rules

Enabled



Show only user-defined rules

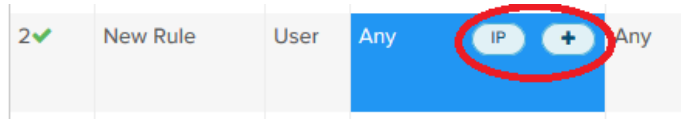


No.	Name	Type	Source	Destination	Service	Action	Enable logging
1 ✓	firewall	Internal	vse	Any	Any	Accept	<input type="checkbox"/>
2 ✓	highAvailability	Internal	169.254.1.41/30 169.254.1.42/30	169.254.1.41/30 169.254.1.42/30 224.0.0.81	Any	Accept	<input type="checkbox"/>
3 ✓	default rule for ir	Default	Any	Any	Any	Deny	<input type="checkbox"/>

Add Firewall Rule

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

- Datacenters → Networking → Edges → [CONFIGURE SERVICES](#)
- Click the **Firewall** tab then
- Enter a name for the rule.
- For **Source** and **Destination**, hover over the field and select **IP** and/or + as appropriate. Add an IP range or object. Or leave as the default **Any**



- 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"/>

- Then [Save 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. Datacenters → Networking → Edges → [CONFIGURE SERVICES](#)
2. Click the **Firewall** tab
3. Click in a rule you wish to re-order, then the appropriate arrow or
4. Click [Save changes](#).



Load Balancer Configuration

Load Balancing is configured on the external interface of an Edge and can distribute incoming traffic from external networks to servers in EduCloud.

To create a basic Load Balanced service:

- Initial Configuration of the Load Balancer Service on the Edge Gateway.
- Create a Server Pool
Containing the internal servers that are being load balanced to.
- Create a Virtual Server
With a public IP address to service the external requests

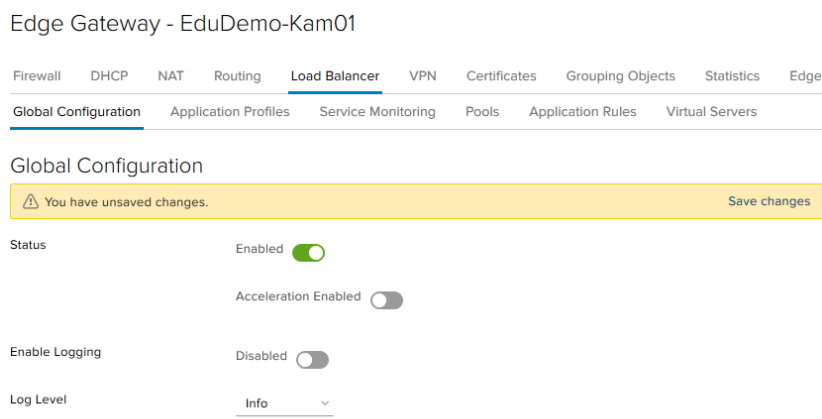
For more advanced Load Balancing configurations, see the on-line help.

Load Balancing Key Concepts

- Virtual Server – the external connection to a Load Balancer instance. 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 a back-end server
- Application Profile - the TCP, UDP, persistence, and certificate configuration for a given application.

Load Balancing Initial Global Configuration

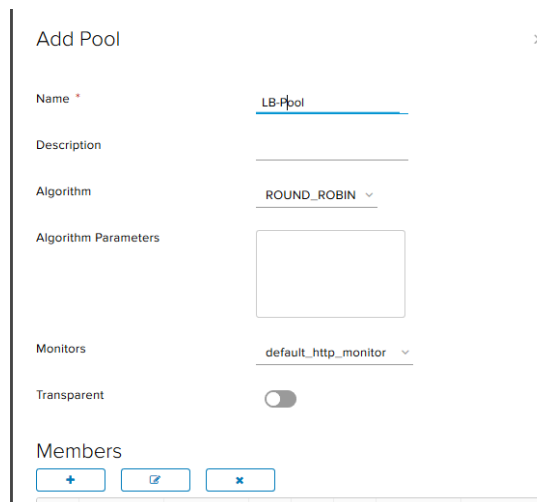
- Datacenters → Networking → Edges → [CONFIGURE SERVICES](#)
- **Load Balancer** tab → **Global Configuration**
- Click **Enabled**
And if required enable Acceleration and Logging
- Click [Save changes](#)



Create a Server Pool

A pool manages and shares backend servers defining load balancer distribution methods and health check parameters.

- Datacenters → **Networking** → **Edges** → [CONFIGURE SERVICES](#)
- **Load Balancer** tab → **Pools** →
- Enter Pool Info
 - **Name:** Pool Name
 - **Algorithm:** Load Balancing method
 - **Monitors:** choose the appropriate monitor for server health checks. If a monitor fails a health check, that pool member will be taken out of circulation. And restored to circulation, if it recovers.
 - **Transparent:** select to make client IP addresses visible to the pool members. If selected, the Edge Gateway must be selected as the default gateway



The screenshot shows a modal window titled "Add Pool" with a close button (X) in the top right corner. The form contains the following fields and controls:

- Name:** A text input field containing "LB-Pool".
- Description:** An empty text input field.
- Algorithm:** A dropdown menu with "ROUND_ROBIN" selected.
- Algorithm Parameters:** An empty rectangular text area.
- Monitors:** A dropdown menu with "default_http_monitor" selected.
- Transparent:** A toggle switch currently turned off.
- Members:** A section with three buttons: a plus sign (+), a refresh icon (circular arrow), and a minus sign (-).

- 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

Add Member

Enabled

Name * Web-Server-1

IP Address * 192.168.56.1

Port 80

Monitor Port 80

Weight * 1

Min Connections

Max Connections

- **KEEP**
- **KEEP**

Create Virtual Server

- Datacenters → Networking → Edges → [CONFIGURE SERVICES](#)
- **Load Balancer** tab → **Pools** →
- 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 * Web-Service

Description

IP Address * 206.12.149.9

Protocol * HTTP

Port * 80

Default Pool LB-Pool

Connection Limit

Connection Rate Limit (CPS)

KEEP and **KEEP**

VPN (Virtual Private Network)

VPNs can be enabled for Org VDCs backed by an edge gateway to create a secure tunnel between an Org VDC network and another network.

EduCloud supports VPNs between Org VDC networks backed by edge gateways and other Org VDC networks and/or remote networks.

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

Create IPsec VPN Connection

- Datacenters → Networking → Edges → [CONFIGURE SERVICES](#)
- VPN tab → IPsec VPN Sites →
 - **Enable** - 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
 - **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

The screenshot shows a web form titled "Add IPsec VPN" with the following fields and values:

- Enable perfect forward secrecy (PFS)**:
- Name**: Tuktoyaktuk-Site
- Local Id ***: 206.12.149.10
- Local Endpoint ***: 206.12.149.10
- Local Subnets ***: 192.168.56.254/24
- Peer Id ***: 94.94.6.1
- Peer Endpoint ***: 94.94.6.1
- Peer Subnets ***: 192.168.92.1/23,192.168.101/24
- Encryption Algorithm**: AES256
- Authentication**: PSK
- Change Shared Key**:
- Pre-Shared Key ***: [Redacted]
- Display Shared Key**:
- Diffie-Hellman Group**: DH14
- Extension**: [Empty text box]

At the bottom, there are "DISCARD" and "KEEP" buttons. A note at the bottom states: "Extension could be passthroughSubnets=192.168.1.0/24,192.168.2.0"

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

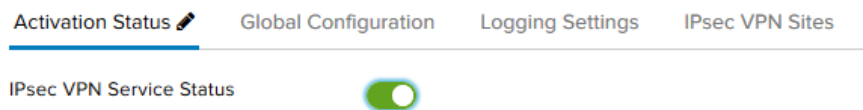
- IP Protocol ID 50 (ESP)
- IP Protocol ID 51 (AH)
- UDP Port 500 (IKE)
- UDP Port 4500

Activate VPN Configuration

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

- Datacenters → **Networking** → **Edges** → [CONFIGURE SERVICES](#)
- **VPN** tab → **IPSec VPN Service Status** →
- [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