# EDUCLOUD SERVER

## Concepts and Overview

VCD 10.2.2

Revision 0.9

# Contents


Introduction ..... 3
Organization ..... 4
Users and Groups ..... 4
Site ..... 5
Organization Virtual Datacenter (VDC) ..... 5
Virtual Application (vApp) ..... 6
Virtual Machine (VM) ..... 7
  Supported Guest Operating Systems ..... 7
  VMware Tools and Open VM Tools ..... 8
Cloud Resources ..... 8
  Hosts ..... 9
  Compute Tiers ..... 9
  Storage ..... 10
Backup and Retention ..... 10
Snapshots ..... 10
Catalogs ..... 11
  Sharing ..... 11
  Publish/Subscribe ..... 12
  EduCloud Public Catalogs ..... 12
Organization Virtual Data Center Networking ..... 12
  Organization Network Configurations ..... 13
  Direct Networks ..... 13
  Routed Networks ..... 13
  Isolated Networks ..... 14
  vApp Networking ..... 14
  IP Addresses ..... 15
Edge Gateway ..... 15
  Multiple Edge Gateways ..... 16
  Site to Site Communications ..... 16
Distributed Firewall ..... 17
Requesting/Mapping Resources ..... 18
Bringing the Concepts Together ..... 19

# Introduction

EduCloud Server Service is a private, higher education cloud service which allows provisioning and management of virtual servers at a fraction of the cost of implementing physical servers.

The self-service portal allows organization administrators and users flexibility to deploy, redistribute, and remove server resources as needed - anytime, anywhere.

More information about the service and its costs can be found on the EduCloud Server service catalogue page at https://it.ubc.ca/services/web-servers-storage/educloud-server-service

This guide provides an overview of the features available within the EduCloud Server service, the concepts and constructs that underpin the service, and the processes for requesting resources.

Step by step instructions for performing common tasks can be found in the "*EduCloud Server User Guide*" and the "*EduCloud Server Networking and Security Guide"* which can be downloaded from the EduCloud Server service catalogue.

Full documentation for vCloud Director (the product used to implement EduCloud Server) is available from the web portal by selecting "Help" from the Help menu located at the top right corner of the screen. Any vCloud documentation referenced in this document can be found there.

For the remainder of this document, "EduCloud Server Service" will be abbreviated as "EduCloud".

## Organization

In EduCloud, an organization (Org) is a unit of administration for a collection of users, groups, and computing resources. EduCloud uses Orgs to provide multi-tenancy.

Organizations are set up and configured by the EduCloud system administrators.

The organization is then managed by organization administrators. Organization administrators are responsible for:

- Managing the cloud resources assigned to the organization (via requests to the system administrators)
- Creating organization users and groups and assigning them appropriate rights and roles.
- Managing organization catalogs
- Managing Distributed Firewall Rules
- For NSX Networking based organizations:
    - Creating and managing Organization VDC networks
    - Managing edge gateway services - firewall access rules, network address translation, static routing, and load balancing.

Organization administrators may delegate some or all of the above responsibilities to other organization users by assigning them appropriate roles.

Organization administrators and users access EduCloud services via their organization URL:

https://bcnet.educloud.ubc.ca/tenant/*<org-name>*/

The specific URL is provided when the Org is created.

## Users and Groups

An organization can contain an arbitrary number of users and groups.

User accounts can be managed locally or imported from a directory service such as LDAP. Groups may only be imported from a directory service – they are not available for local accounts.

Permissions within an organization are controlled through the assignment of roles to users and groups.

A full description of the pre-defined roles, and associated rights can be found in the "*vCloud Director Tenant Portal Guide*" under "*Managing Users, Groups and Roles → Roles and Rights*".

Organization administrators manage all users, groups and assigned roles. They can configure access to an LDAP directory server for user/group management. They can also create custom roles for their organization and control the assigned rights if needed.

## Site

A site is a geographic location where cloud resources are available. Sites are independent, each having their own physical infrastructure (building, power/generation, cooling), cloud resources, and network uplinks.

Multiple sites can be leveraged for disaster recovery or to build disaster tolerant applications – applications that can continue to function in the event an entire site becomes non-functional.

EduCloud currently has two sites:

- **Van** – Vancouver
- **Kam** – Kamloops

The site abbreviations (in bold) appear in EduCloud resource names (e.g. VDCs) to help identify the site the resource is located at.

Vancouver is located in a moderate to high risk seismic zone, Kamloops in a low risk zone.

## Organization Virtual Datacenter (VDC)

Within an organization, a virtual datacenter (VDC) provides a collection of compute, memory and storage resources to an organization. It provides an environment where virtual machines can be stored, deployed and operated. It also provides storage for virtual media, such as ISO images.

A single organization can have multiple VDCs - the number depends on sites and compute performance tiers in which resources are requested.

An organization using the standard compute performance tier at the Vancouver site and the standard and high performance tiers at the Kamloops site would have three VDCs:

- *<org-name>*-Van-Std
- *<org-name>*-Kam-Std
- *<org-name>*-Kam-High

Organization VDCs are created and resources assigned by the EduCloud system administrators based on requests from organization administrators.

EduCloud billing is based on the resources assigned to your organization VDC's.

## Virtual Application (vApp)

Within a VDC, a vApp (virtual application) is a container that can:

- Contain multiple VMs (virtual machines) - up to 128
- Be powered on, off, or suspended – affecting all VMs they contain
- Control start and stop behavior and order for the VMs they contain
- Be copied or moved as a unit.
- Be added to a catalog so others can deploy copies.
- Contain isolated or routed vApp networks.
- Be shared (read-only, read/write, full-control) with other users in an organization

When choosing how many VMs to include in a vApp, keep in mind that:

- vApps and their contained VMs cannot span VDCs – all must be deployed in one VDC.
- Some vApp operations (e.g. moving) require the vApp (and therefore all VMs it contains) to be stopped.

A user must have at least the "*vApp Author*" role to create or modify vApps and the VMs they contain.

A user with the "*vApp User*" role can access a vApp and its VMs, but cannot modify the configuration of the vApp or the VMs it contains.

More information can be found in the "*EduCloud User Guide*" and the "*vCloud Director Tenant Portal Guide*" under "*Working with vApps*".

## Virtual Machine (VM)

A virtual machine is a "software" computer that, like a physical computer, runs an operating system and applications. Every virtual machine has virtual devices and resources (CPU, memory, disk(s), network adapters, etc.) that provide the same functionality as physical hardware and have additional benefits in terms of portability, manageability, and security.

The virtual machine is the workhorse of the EduCloud service – it runs the operating systems on which your applications run.

Note that:

- A VM is usually within a vApp. Stand alone VMs can be created, but there are some operations that cannot be performed on Standalone VMs
- The vApp's VDC determines the site, compute and storage resource available to its VMs

More information can be found in the "*EduCloud User Guide*" and the "*vCloud Director Tenant Portal Guide*" under "*Working with Virtual Machines*".

### Supported Guest Operating Systems

A guest operating system is the operating system that runs within a VM.

The following 64-bit guest operating systems are supported by EduCloud, including standard templates that can be used to build vApps:

- Microsoft Windows Server 2019 Standard
- Microsoft Windows Server 2016 Standard
- Microsoft Windows Server 2012 R2 Standard
- Microsoft Windows 10 Enterprise
- RedHat Enterprise Linux 8
- RedHat Enterprise Linux 7
- Ubuntu 18.04 LTS

Many other guest operating systems are also supported by EduCloud, but on a more limited basis. See the "*EduCloud Server User Guide"* for information on creating new vApps/VMs from installation media.

## VMware Tools and Open VM Tools

VMware Tools is a suite of utilities that enhances the performance of a VM's guest operating system, and enables features that allow the infrastructure to properly manage the VM and its guest operating system. VMware develops and distributes VMware Tools

Open VM Tools (open-vm-tools) is an open source implementation of VMware Tools. It allows operating system vendors, communities and/or virtual appliance vendors to bundle VMware Tools into their product releases.

VMware Tools or Open VM Tools must be installed in your guest operating system for your VM and operating system to function properly and reliably within the EduCloud Server service.

Some features will not work or may operate in a degraded mode if VMware/Open VM Tools are not installed.

VMware recommends that you use Open VM Tools if it is provided with your operating system release, and to download and install VMware Tools if not.

VMware Tools or open-vm-tools is already preinstalled and tested on all EduCloud Public Catalog templates.

For information on installing VMware Tools or open-vm-tools for a VM not deployed from one of the Public Catalog templates, please see:

- VMware Tools - https://kb.vmware.com/s/article/1014294
- Open VM Tools - https://kb.vmware.com/s/article/2073803

# Cloud Resources

Cloud resources are an abstraction of the underlying physical resources used to provide the EduCloud Server service. These resources are:

- Compute – CPU and memory for running virtual servers.
- Storage – disk for storage of operating systems, applications and data.
- Networking – network connectivity and associated features such as firewalls, Network Address Translation (NAT), load balancing, static routes, etc.

## Hosts

A host is the physical computer on which your virtual machine runs. The system may automatically move your VM to other hosts to evenly balance loads across the hosts within a tier. Your VM may also be moved when maintenance needs to be performed on a host. These moves occur dynamically and are non-disruptive.

Host failures are infrequent, but when they do occur, all VMs running on that host will experience an outage. The system will detect the host failure and restart all impacted VMs on other hosts within the tier – this typically occurs within 5 minutes of the failure.

Sometimes it is desirable to ensure certain VMs never run on the same host, or always run on the same host. How VMs are placed on hosts can be influenced using affinity/anti-affinity rules. See the "*EduCloud Server User Guide"*

## Compute Tiers

EduCloud Server offers two compute performance tiers – each tier contains hosts with different performance capabilities:

- **Std** – Standard Performance – 2.2 GHz clock speed
- **High** – High Performance – 3.2 GHz clock speed (Kamloops only)

The standard performance tier is the most cost effective and should meet the performance requirements for the majority of your applications.

The high performance tier is available for applications with components that require a higher CPU clock speed and higher degree of dedicated resources in order to achieve the desired application performance.

The performance tier abbreviations (in bold) will appear in EduCloud resource names (e.g. VDCs) to help you identify the performance tier of the resource.

See the service catalogue to obtain tier pricing and availability.

## Storage

EduCloud uses all-flash enterprise tier storage arrays to provide storage for VMs. Storage is presented to EduCloud users as a Storage Policy that is selected when creating VMs.

Storage Policies can be reviewed by:

- **Datacenters → Storage** Menu → **Storage Policies**

EduCloud also provides Independent Disks. These are standalone virtual disks that are created in Organization VDCs. Independent disks can be added and/or detached from a VM.
Note that independent disks are not backed up by EduCloud.

# Backup and Retention

The standard backup and retention policy for EduCloud is currently:

- Local: 28 daily backups
- Remote: 28 daily backups; 12 weekly and 12 monthly

Local backups are kept at the site of the VDC; remote backups are kept at a different site.

If a restore from backup is required, please submit a service ticket.

# Snapshots

Snapshots preserve the state of a VM or an entire vApp (and all VMs it contains) at a specific point in time and allows the option to revert back to it later.

Snapshots are designed to allow rollback for a short window of time (ideally no more than a few days) – for example during a software upgrade/acceptance window. They should not be left in place for an extended period of time. Snapshots will have a negative impact on both VM and backup performance that will increase with time.

Snapshots do not capture VM networking configuration – any networking changes made after the snapshot is taken will not be reverted if you roll back to a snapshot.

More information about vApp and VM level snapshots can be found in the "*EduCloud Users Guide"* under *"Snapshots"* and in the "*vCloud Director Tenant Portal Guide*" under "*Working with vApps*" and "*Work with Virtual Machines*".

## Catalogs

Catalogs store vApp templates and media files such as ISOs.

EduCloud has public catalogs containing supported OS vApp templates. Templates include industry standard security settings and common packages. The public catalogs are duplicated across EduCloud sites.

Catalogs can be created within an organization and shared to users within the organization and/or published to other organizations.

Users with access to a catalog can deploy their own vApps from it. They can also attach media from the catalog to a VM.

If your organization uses multiple EduCloud sites, and has vApps or VMs that will be frequently deployed at those sites, we recommend you maintain a copy of any Org catalogs at each site. There are two options:

1. Create a catalog at each site and manually maintain the catalog contents
2. Maintain a catalog at one site, and use publish/subscribe to synchronize a copy of the catalog to the other sites.

When deploying a vApp or VM from a catalog, where possible select from a catalog located at the site you are deploying to. This will speed up the deployment.

Media files in a catalog can be attached to virtual machines – e.g. a ISO file can be attached to a VM as a virtual DVD drive. Again, for best performance, select media from a catalog located at the same site.

An organization administrator or user with the "*Catalog Author*" role can create/upload/manage vApp templates and media files.

More information can be found in the "*EduCloud User Guide*" under "*Catalogs*" and in the "*vCloud Director Tenant Portal Guide*" under "*Working with Catalogs*".

### Sharing

Catalogs can be shared to specific users or groups, or to all users within your organization.

## Publish/Subscribe

Publishing a catalog makes it available for any vCloud organization (inside or outside of EduCloud) to subscribe to. A published catalog will be assigned a URL, and a password can be used to restrict subscription to the catalog.

Any vCloud Director organization that knows both the URL and password of the published catalog, can create a subscribed catalog linked to it. All items in the published catalog will be synchronized to any subscribed catalogs. The subscribed catalog will consume the same amount of disk space within your organization as the space used by the published catalog.

This mechanism can be used to share your catalogs with other EduCloud organizations, or to synchronize your catalog across multiple sites within your organization.

## EduCloud Public Catalogs

The EduCloud administrators maintain a public catalog that contains the following 64-bit OS images:

- Microsoft Windows Server 2019 Standard
- Microsoft Windows Server 2016 Standard
- Microsoft Windows Server 2012 R2 Standard
- Microsoft Windows 10 Enterprise
- RedHat Enterprise Linux 8
- RedHat Enterprise Linux 7
- Ubuntu 18.04 LTS

All organizations can deploy vApps/VMs from the public catalog, but are responsible for obtaining proper licensing for each copy of the operating system being deployed.

A copy of the public catalog is maintained at each EduCloud site:

- EduAdmin-Kam – Kamloops catalog
- EduAdmin-Van – Vancouver catalog

For fast and efficient provisioning, be sure to select from the catalog located at the same site as the services you are deploying.

The EduCloud public catalog OS images fully support guest OS customization and are patched and tested monthly

# Organization Virtual Data Center Networking

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

1. Direct
2. Routed
3. Isolated

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

## Organization Network Configurations

Organizations can be configured with:

1. Direct Networks – direct layer 2 connections to external networks.
2. NSX Virtualized Networking and Security – provides layer 3 and enhanced network services (e.g. firewall, NAT, load balancing) via an edge gateway.

## 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. See the “Edge Gateway” section for more details.

Direct networks are in use within many UBC organizations to provide the VMs direct access to campus networks and resources – a model used to provide network access prior to NSX being licensed for UBC workloads. For VM’s deployed on these networks, services such as firewalls, NAT and load balancing are provided at the network layer and cannot be managed or configured within the EduCloud service.

All BCNET and newer UBC organizations use NSX based networking with edge gateways. Some UBC organizations may have a mixture of both NSX and Direct Networks as they transition.

## 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. See the "Edge Gateway" section for more details

If a routed network is "shared" it is made available across all your organization VDC's at the same site.

## 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.

## vApp Networking

There are three types of networks that can be configured for use within a vApp:

- Org VDC network – maps an existing org VDC network (direct, isolated or routed) into the vApp. Allow VM's in the vApp to connect directly to the org VDC network.
- Isolated vApp Network – A network that is isolated and available only to VMs within the vApp. VM's in other vApps cannot connect to it.
- Routed vApp Network – A network that is available only to VMs within the vApp, but is connected to an org VDC network via a dedicated gateway providing routing, and optionally DHCP, NAT and Firewall services.

The routed vApp network allows the vApp to be repeatedly deployed with the VMs always using the same IPs. Each deployment is accessed by a different IP assigned to its gateway. For example, this could facilitate quick deployment of identical classroom lab environments or easy cloning of test environments.

Routed vApp networks are not recommended for critical workloads with high availability requirements. The gateway appliance used to provide network services for a routed vApp network cannot be configured for high-availability.

More information on working with vApp networks can be found in the "*EduCloud User Guide*" and in the "*vCloud Director Tenant Portal Guide*" under "*Working with vApps → Working with Networks in a vApp*"

Users with the "vApp Author" or higher role can create and manage vApp networking.

## IP Addresses

When defining a network, a pool (range) of static IP's to be used on the network is created. When a VM NIC is connected to the network, it can be configured in one of three IP Modes:

- **Static – IP Pool** - an IP is automatically assigned from the network pool and associated with the VM NIC.
- **DHCP** – an IP is assigned by DHCP. Configured separately, on the edge gateway appliance
- **Static – Manual**- an IP is assigned manually while configuring the NIC. This mode may be used when migrating from other infrastructure.

In all of these instances, the IP Address and other network settings are configured in the guest operating system when guest OS customization is initiated.

# Edge Gateway

An edge gateway is a virtual router for routing traffic between your organization VDC networks and external networks. It also provides a suite of additional network services that can be enabled and used: An Edge gateway is necessary to provide routing and other services for all except Direct Org VDC networks.

| Service | Description |
|---|---|
| DHCP | Simple DHCP services for automatic IP address assignment. No MAC address pinning so VM could get different IP after lease expiry. |
| NAT | Both source (SNAT) and destination (DNAT) network address translation |
| Firewall | Packet filtering firewall to control inbound/outbound access to each attached network. |
| Static Routing | Configure and manage static routes |
| VPN | IPSec VPN service. Establish site-to-site VPN between EduCloud edge gateways or third party VPN gateways. |
| Load Balancing | Load balancing services for TCP, HTTP, and HTTPS traffic (SSL offload for HTTPS only) |
| SSL VPN-Plus | Provide end user VPN access to the networks managed by the edge gateway. |

It also provides facilities for managing the SSL certificates used by edge gateway services and displaying connection statistics

Edge gateways can be deployed in several sizes (to meet different network bandwidth needs), and can be configured for high availability. Each edge gateway supports up to 9 internal network interfaces

The uplink interface is connected to an external direct network that provides routing to the internet and between EduCloud Organizations at a site. Public IP addresses on the external network are allocated for use by your organization - one is consumed for the edge gateway IP address, others can be used for NAT or load balancing virtual IPs.

The uplink network will use public IP addresses, while the internal networks will typically use private IP addresses. NAT or load balancing is used to make any servers publicly accessible.

More information on managing edge gateways and associated services can be found in the "*EduCloud Networking and Security Guide*" and in the "*vCloud Director Administrator's Guide*" under "*Advanced Network Capabilities for vCloud Director Tenants*"

Edge gateways are created and connected to external networks by EduCloud system administrators. Organization administrators can add organization VDC networks to the edge gateway and manage all gateway services.

## Multiple Edge Gateways

Each site has independent networking and requires its own edge gateway to manage routing and extended features (firewall, load balancing, VPN, etc.) for that site. If your organization is utilizing resources at both the Vancouver and Kamloops sites, it will have two edge gateways. Each edge gateway will have a different pool of public IPs allocated to it.

## Site to Site Communications

Communications between services hosted in different EduCloud Server sites occurs through the edge gateways and across the external network. You cannot directly route private IP space between sites – you must either:

- Provide public IPs (via NAT or other means) to servers that must communicate across sites
- Set up a site to site IPsec VPN connection between edge gateways to allow secure direct routing of private IP between sites

Avoid overlapping IP assignments for your Org VDC networks (e.g. assigning 192.168.0.0/24 in both Vancouver and Kamloops) or you will be unable to establish a site to site VPN connection.

Developing a private IP assignment strategy can simplify the site to site setup and routing rules. For example:

- 192.168.0.0/19 – Range used for Org VDC Networks – Vancouver
- 192.168.32.0/19 – Range used for Org VDC Networks – Kamloops

Traffic on the site-to-site connection will traverse the edge gateway firewall – when setting up VPN connections, also be sure to add appropriate firewall rules to allow communication through the connection.

## 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 – enforcing rules as traffic enters/exits the virtual machine network interface. This means that even traffic flowing between VM's on the same network can 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 – separate networks (security zones) are no longer a necessity.

More information on EduCloud network and security, network design considerations and the distributed firewall see the "*EduCloud Networking and Security Guide*" and the "*vCloud Director Tenant Portal Guide*" under "*Advanced Network Capabilities for vCloud Director Tenants*"

## Requesting/Mapping Resources

When requesting net-new services or adding tiers:

- Review the service catalogue for available sites, the compute and storage tiers offered at each site, and the resource pricing for each site/tier
- Specify which sites services need to be deployed in.
- For each of the sites provide:
    a. The number of public IPs required
    b. The compute performance tiers that will be used.
- For each site and compute performance tier, provide:
    a. The amount of CPU (in GHz) and memory (in GB) to be allocated in the tier.
    b. The storage tiers required, and the amount of space to allocate in each tier (in GB or TB).

The services will be mapped into your organization as follows:

- An edge gateway will be created for each site at which services will be deployed
- The requested number of public IPs will be assigned to each edge gateway
- An organization virtual datacenter (VDC) will be created for each site and compute performance tier that you request.
- The storage you requested for each compute tier will be assigned to its associated VDC.

When requesting resource changes, be sure to specify the VDC and which resources need to be increased, decreased, added or removed.

## Bringing the Concepts Together

This example runs through the request, provisioning and deployment process for the EduDemo organization. It demonstrates how compute, storage and networking (Edge-gateways, organization VDC networks) map into your EduCloud organization, and how some simple applications might be deployed.

The following request for resources was received from the EduDemo administrator:

| | |
|---|---|
| Site: Vancouver | |
| Public IPs: | 12 |
| Compute Tier: Standard Performance | |
| CPU | 15 GHz |
| Memory | 50 GB |
| Storage | 50 TB |
| | |
| Site: Kamloops | |
| Public IPs: | 8 |
| Compute Tier: Standard Performance | |
| CPU | 10 GHz |
| Memory | 32 GB |
| Storage" | 50 TB |
| Compute Tier: High Performance | |
| CPU | 20 GHz |
| Memory | 64 GB |
| Storage: | 50 TB |

The EduCloud system administrators' then provision:

**An Organization**

The EduDemo organization. The organization administrator is provided with an account with organization administrator permissions and the URL for accessing the organizations EduCloud web portal.

**Three Virtual Datacenters**

The **EduDemo-Van-Std** VDC is created at the Vancouver site – 15GHz of standard performance CPU and 50 GB of memory are allocated to the VDC. 50 TB storage are allocated to the VDC.

The **EduDemo-Kam-Std** VDC is created at the Kamloops site – 10GHz of standard performance CPU and 32 GB of memory are allocated to the VDC. 50 TB storage are allocated to the VDC.

The **EduDemo-Kam-High** VDC is created at the Kamloops site – 20GHz of high performance CPU and 64 GB of memory are allocated to the VDC. 50TB of storage are allocated to the VDC.

**Two Edge Gateways**

The **EduDemo-Van-Std-01** edge gateway is created at the Vancouver site. Its external interface is attached to the "Van-Gateway" external network and assigned the public IP address 103.40.50.27. Eleven additional IP addresses (.28 through .38) are reserved for use by edge gateway services (e.g. NAT).

The **EduDemo-Kan-Std-01** edge gateway is created at the Kamloops site. Its external interface is attached to the "Kam-Gateway" external network and assigned the public IP address 206.80.100.12. Seven additional IP addresses (.13 through .19) are reserved for use by edge gateway services (e.g. NAT).

The external "Gateway" networks provide connectivity to the BCNET Advanced Network and internet via the local BCNET routers.

The organization administrator provisions:

**Org VDC Networks**

The **DMZ-Van** organization VDC network is created at the Vancouver site. Subnet 192.168.1.0/24 is assigned to the network. The gateway IP address is set to 192.168.1.254, and the remaining IPs on the subnet are assigned to the networks IP pool.

The **DMZ-Kam** organization VDC network is created at the Vancouver site. Subnet 192.168.32.0/24 is assigned to the network. The gateway IP address is set to 192.168.32.254, and the remaining IPs on the subnet are assigned to the networks IP pool. The "shared" option is selected so the network is available in all VDCs at the site.

**Site-to-Site VPN**

Servers on the DMZ-Kam and DMZ-Van network need to communicate directly with each other. To achieve this, VPN services are enabled on the edge gateway, and a site-to-site VPN configuration entered to peer the DMZ-Van (192.168.1.0/24) and DMZ-Kam (192.168.32.0/24) networks. Firewall rules are created on both the Kamloops and Vancouver edge gateways to allow all IP traffic to flow between these networks.

**vApps/VMs**

The **Email** vApp and associated VMs is built and deployed in the EduDemo-Van-Std VDC. IP addresses are assigned to VM NICs from the network pool. OS Images are selected from the EduAdmin-Van public catalog.

The **DataMart** and **WebSite** vApps and associated VMs are built and deployed in the EduDemo-Kam-High and EduDemo-Kam-Std VDCs. IP addresses are assigned to VM NICs from the network pool. OS Images are selected from the EduAdmin-Kam public catalog.

**NAT/Firewall**

Note: in this example, services are secured using the edge gateway firewall.

The DataMart and WebSite applications each have a web interface that must be made publicly available on port 443. A NAT rule is put in place for each application to provide a public IP. Firewall rules are put in place to allow access to port 443.

The Email application must make SMTP services publicly available on port 25. A NAT rule is put in place to provide a public IP. A Firewall rule is put in place to allow access to port 25.

The following diagram provides a visual representation of the deployed services: