BCNET 2019

Welcome to BCNET 2019

EduCloud Server And Backup

The Nuts and Bolts of BCNET’s Private Cloud Offering

Brent Dunington

Chris Krusch

Agenda

EduCloud Server

- Service Overview
- Under the Covers
- vCD 9.5 - New features
- What's Around the Bend

EduCloud Backup

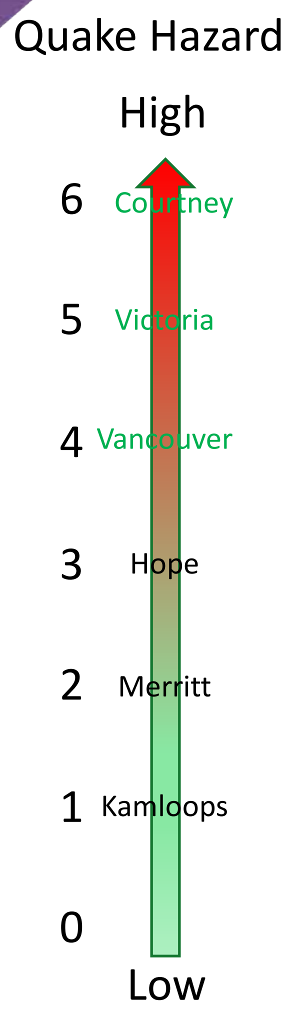
- Service Overview
- Under the Covers

BCNET 2019

What is EduCloud Server?

- Provides secure, multi-tenant infrastructure as a service for higher education institutions in British Columbia.
- Each institution is allocated virtual compute, storage and network resources which can be used to deploy robust, highly available applications and services.
- Billing is based on assigned resources + Annual per VM
- Self-service web portal provides simplified, self-managed access for your IT administrators and service users

Two Sites: Vancouver (Van), Kamloops (Kam)



Quake Hazard

High

6 Courtney

5 Victoria

4 Vancouver

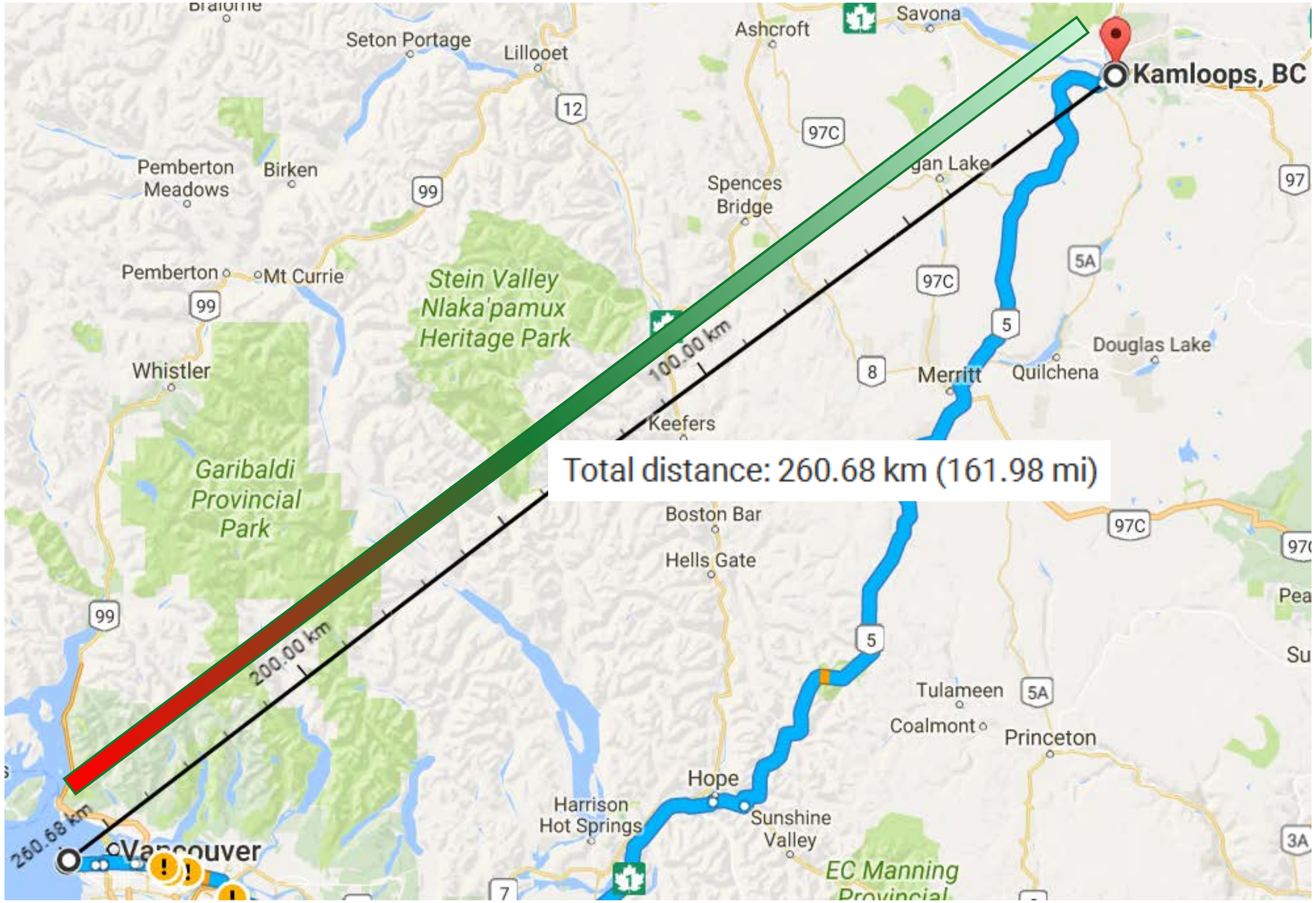
3 Hope

2 Merritt

1 Kamloops

0

Low



Total distance: 260.68 km (161.98 mi)

Networking

- Networking at EduCloud sites is independent.
- No private backbone or tunnel linking sites – all traffic between sites transits over BCNET ORAN
- Internet transit exchanges are independent
  - Kamloops – via Kamloops city hall (KAMTX)
  - Vancouver – via Harbour Centre (VANTX).
- Site to site IPSEC VPN can be used to allow routing of private IP between sites.
- Private IP space used must be unique across all sites

Compute and Storage Tiers

- **Std** – Standard Performance – 2.2 GHz
  - Available in Vancouver and Kamloops
- **High** – High Performance – 3.2 GHz
  - Available in Kamloops
  - For applications that require higher CPU clock speed to achieve desired performance
- **Storage**
  - All SSD in Kamloops; Vancouver migration to SSD over the summer

Underlying Software

Hypervisor:

VMware vSphere – 6.5 to 6.7

Network Virtualization:

VMware NSX – 6.4.4

Multi-Tenant Self Service:

VMware vCloud Director – 9.5.0.3 (vCD)

Backups:

Veeam Backup and Replication – 9.5 U4a

vCD - Organization (Org)

- Supports multi-tenancy through use of organizations
- Unit of administration for a collection of users, groups, compute and network resources.
- Organization administrators manage:
  - Users and user authentication
  - Groups and group membership
  - Roles and privileges assigned to users and groups
- Org admins have full access to all features an org is permitted to use.

vCD – Virtual Datacenter (vDC)

- A vDC contains compute, memory, and storage resources in which virtual servers can be deployed.
- vDC’s are created based on location + compute performance tier

<org>-Van-Std	Vancouver Standard Performance
<org>-Kam-Std	Kamloops Standard Performance
<org>-Kam-High	Kamloops High Performance

- Requested amount of CPU, memory and disk resources are mapped into each vDC

vCD – vAPP (vDC)

- vAPP – A container for VMs that make up an application + supporting operational parameters
  - Container for application VMs
  - Manage vm startup/shutdown sequences
  - Manage network configuration for contained VM’s
- Vapps can be:
  - Powered on, powered off, suspended
  - Snapshot
  - Cloned
  - Published to a catalog
  - Deployed from a catalog

vCD – Edge Gateway (EG)

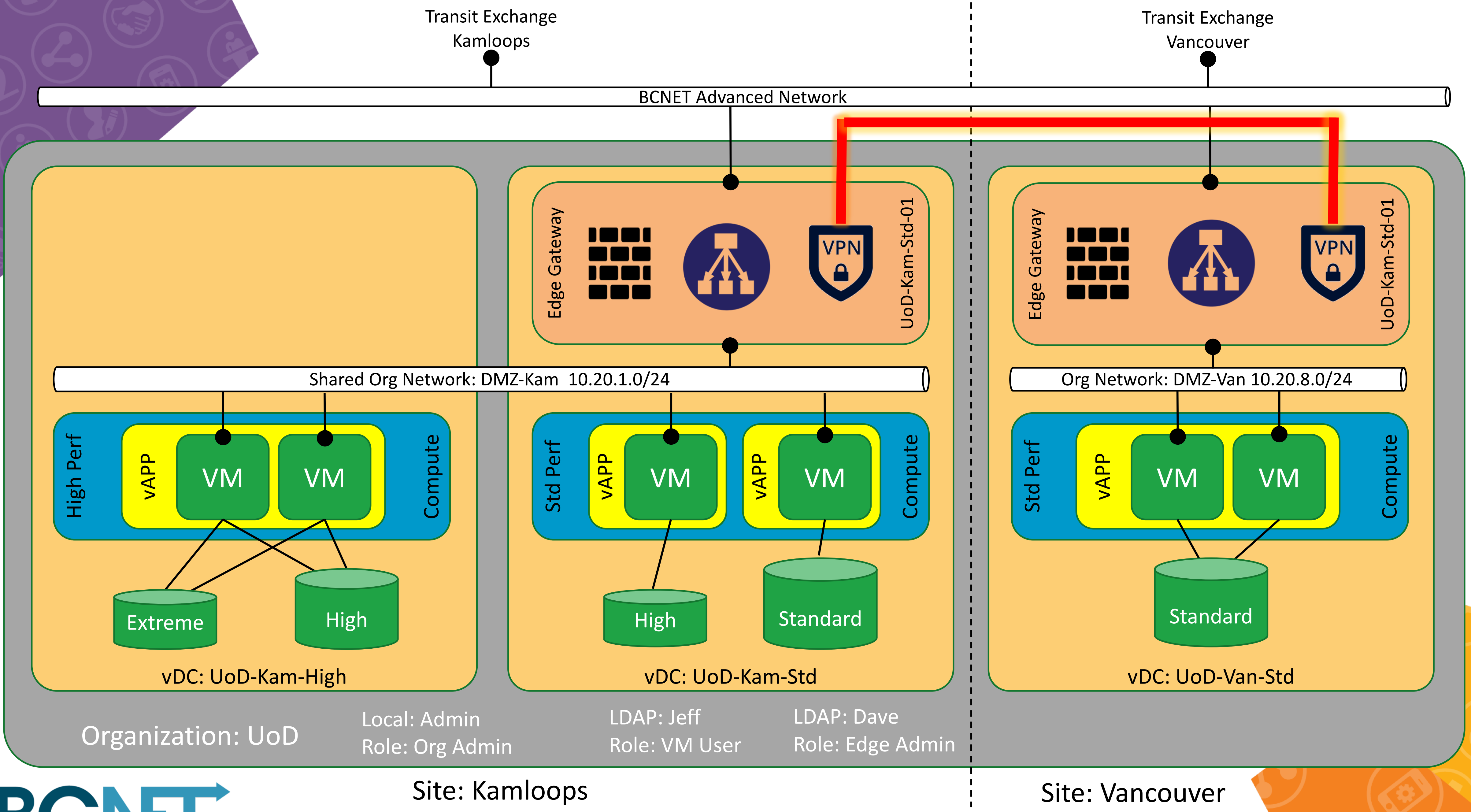
- Is a highly available virtual router that provides your routed org vDC networks with external connectivity.
- It can be configured to provide network services:
  - DHCP
  - DNS Relay
  - Firewall
  - Static Routing
  - NAT
  - Load Balancing
  - Layer 2 VPN
  - SLL VPN
- Each site requires 1 edge gateway

System Admin Role

- BCNET + UBC IT Systems Teams
- Consult to understand compute/storage/network needs.
- Provision an EduCloud Organization for your institution
- Set up Org Administrator account & provide credentials
- Provision vDC’s and assign resources
- Provision Edge Gateways to provide network connectivity
- Adjust vDC’s and assigned resources as requested by client
- Provide ongoing support & design assistance to Org Admins

Organization Admin Role

- Configure authentication mechanism (local, LDAP, SAML)
- Configure and provision users and groups
- Create and/or assign roles to users and groups
- Provide first line support to your user community:
  - Design & usage assistance
  - Problem assistance
- Escalate issues or request assistance from system admins


Transit Exchange
Kamloops
Transit Exchange
Vancouver
BCNET Advanced Network
Edge Gateway
VPN
UoD-Kam-Std-01
Edge Gateway
VPN
UoD-Kam-Std-01
Shared Org Network: DMZ-Kam 10.20.1.0/24
Org Network: DMZ-Van 10.20.8.0/24
High Perf
vAPP
VM
VM
Compute
Extreme
High
vDC: UoD-Kam-High
Std Perf
vAPP
VM
vAPP
VM
Compute
High
Standard
vDC: UoD-Kam-Std
Std Perf
vAPP
VM
VM
Compute
Standard
vDC: UoD-Van-Std
Organization: UoD
Local: Admin
Role: Org Admin
LDAP: Jeff
Role: VM User
LDAP: Dave
Role: Edge Admin
Site: Kamloops
Site: Vancouver

vCD 9.5 Upgrade – What's New?

- HTML 5 interface – feature parity with old flash interface
- Flash interface will be deprecated and dropped in future
- Enhanced role based access controls – Org admins can now create Org specific Rights/Roles
- Advanced Gateway – all edge gateways updated
  - Enhanced load balancing – L4 and L7 engines, SSL offload, L7 supports advance packet manipulation and DDOS mitigation. Improved health check scripting capabilities.
  - Sslvpn service
- Performance Metrics
- Operations manager tenant app

EduCloud Server Upgrade Journey

- VMware vCloud Director, vSphere, vROps, NSX, Veeam Backup, Zerto, HPE Servers, Cisco UCS, Nimble Storage, HPE 3Par, NetApp, SQL, EMC Data Domain, Edge Gateways, Distributed Switches, VMFS

- Upgrade plan is created and presented to the team
  - includes pre-requisites, implementation plan and rollback
  - Confirm no known issues and validate upgrade with vendor
  - Investigate any known issues in KBs or forums

- Date is set and communications sent out to clients

Just Around the Bend…

Distributed Logical Router (DLR)

- High performance, low overhead first-hop routing
- Implemented as a Hypervisor Kernel Module
- Traffic between your VM's will route directly between the hosts the VM's are running on
- Results in efficient East/West traffic flow

EduCloud supports:

- 1 DLR attached to an Edge Gateway
- Up to 991 subnets per DLR

Just Around the Bend…

Distributed Firewall(DFW)

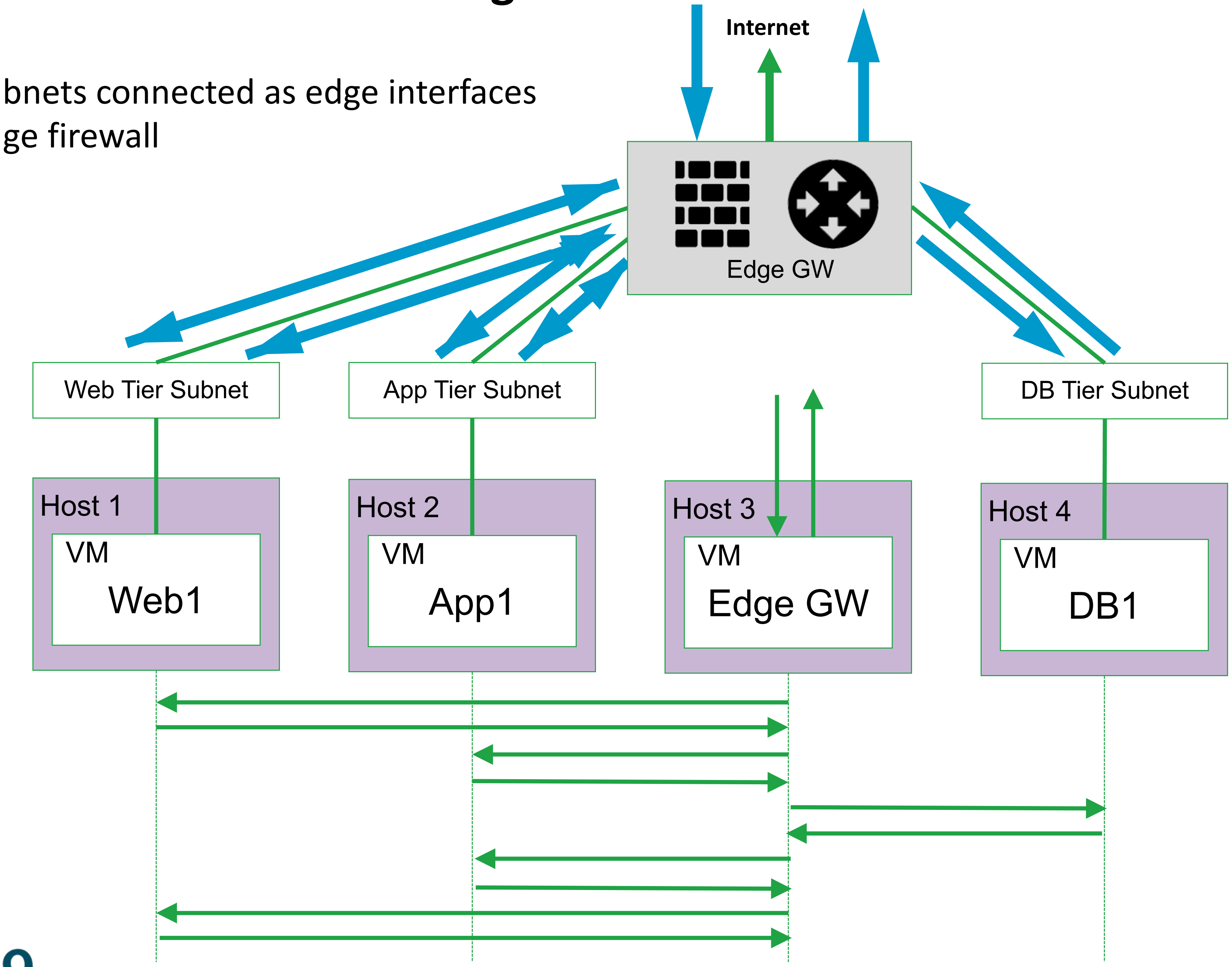
- High performance hypervisor embedded firewall
- Implements "MicroSegmentation" – workloads can be secured and isolated individually – even if in the same subnet
- Effectively places a firewall in each NIC of a VM
- Can create policies based on EduCloud Objects – VM Names and Tags, vDC's, IP's, VLANs, Edge Gateways, Subnets, …..

Firewall Policy Scope:

- Virtual DataCenter – each vDC will have its own policy set

Traditional 3 Tier Design

- Subnets connected as edge interfaces
- Edge firewall



BCNET 2019

Traditional 3 Tier - Challenges

Security

- Multiple subnets required to create separate security zones
- Edge firewall can only control traffic flowing between subnets
- No security between VMs on same subnet (Guest Firewalls)

Routing

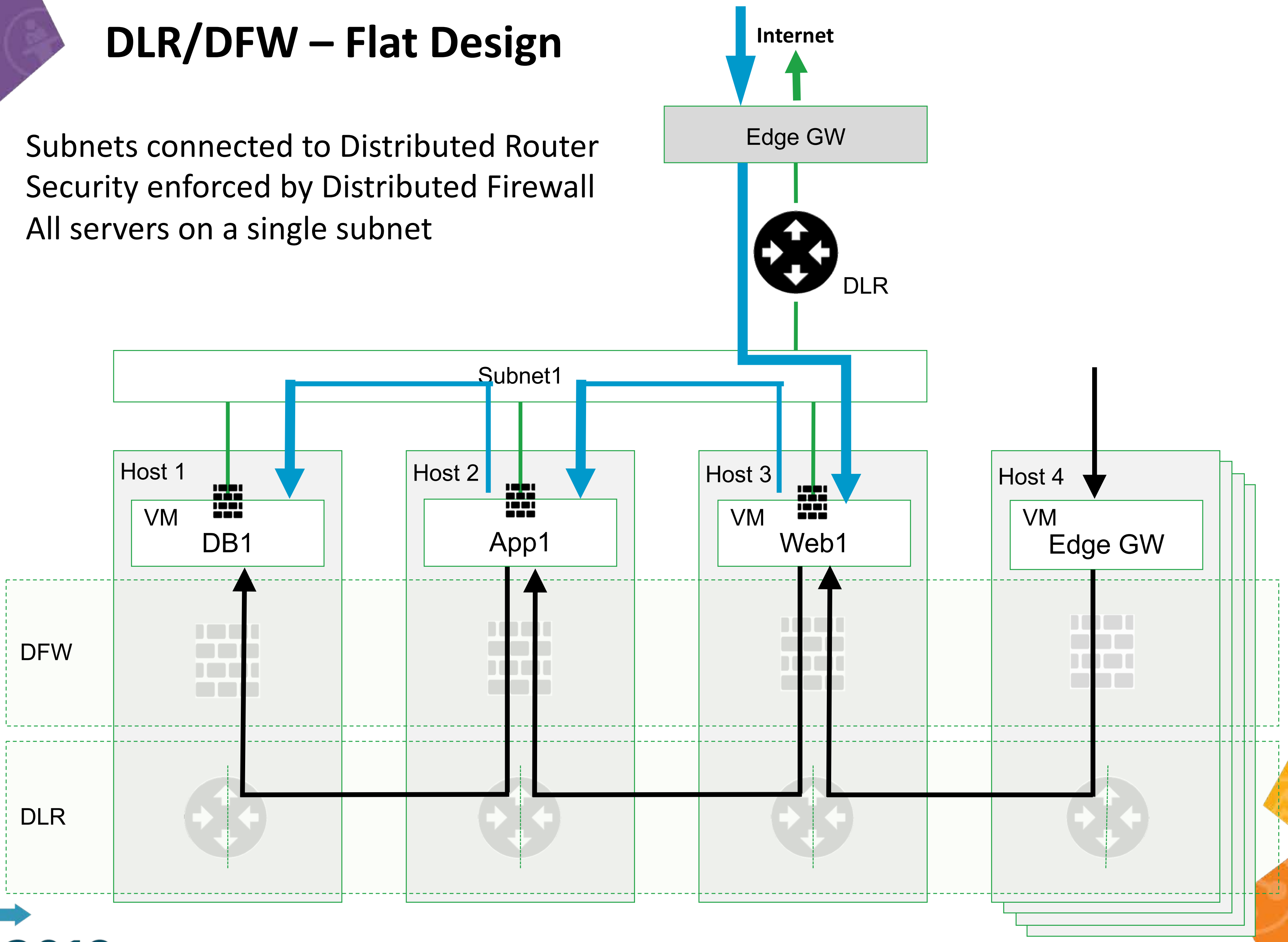
- East/west traffic between zones must traverse Edge Gateway

Other

- Tends to waste IP space (don’t want to undersize subnets)

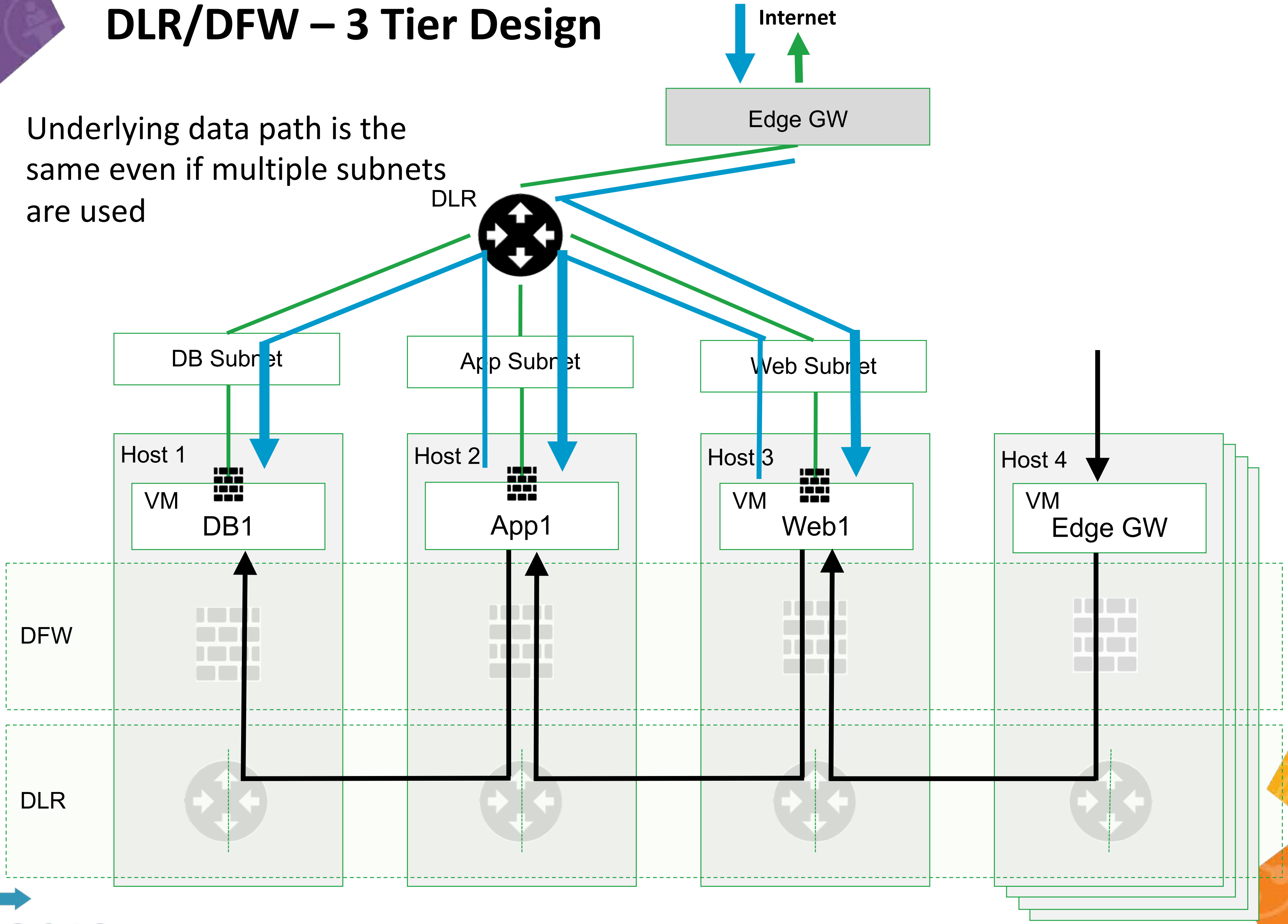
DLR/DFW – Flat Design

- Subnets connected to Distributed Router
- Security enforced by Distributed Firewall
- All servers on a single subnet



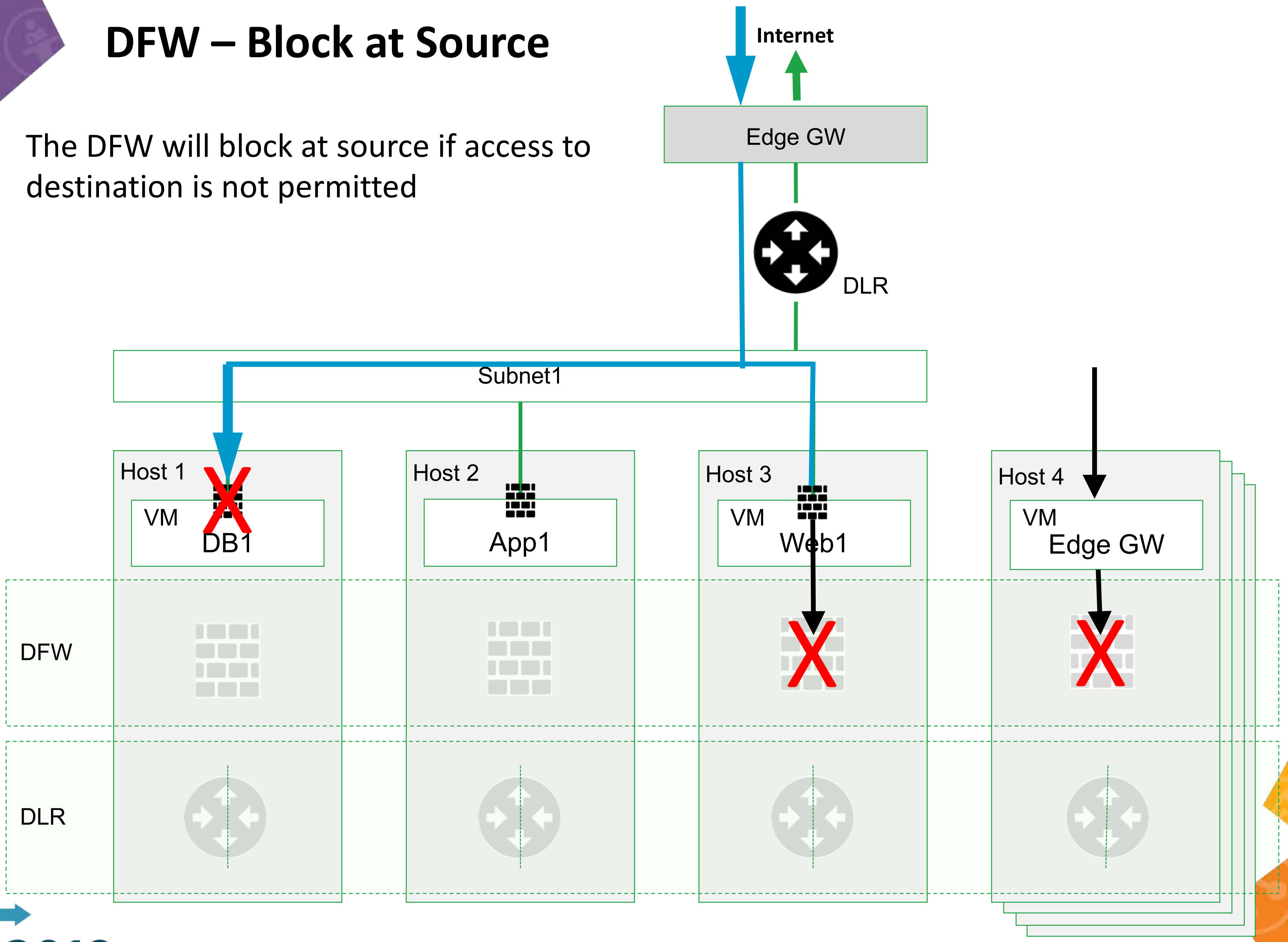
DLR/DFW – 3 Tier Design

- Underlying data path is the same even if multiple subnets are used



DFW – Block at Source

- The DFW will block at source if access to destination is not permitted



DLR/DFW - Advantages

- Full security/isolation enforced at VM NIC interface
- Security/Isolation no longer drives network design
- Improved FW performance – Kernel + block at source
- Efficient east/west traffic – routing directly between VM hosts

Further Down the Road

Network Uplinks – Vancouver

- Network traffic currently traverses UBC core and border protections
- BCNET EduCloud workloads are subject to all border protections and port blocking UBC puts in place
- Investigate feasibility of separate uplinks for BCNET EduCloud Infrastructure

Further Down the Road

- Containers as a service
  - CSE (Container Service Extension) brings Kubernetes-as-a-service to EduCloud
- Infrastructure as code (e.g. Terraform)
- HTML 5 interface enhancements and bug squashing
- Backup infrastructure improvements
- Global search
- IPV6
- Feature Requests for Operations Manager
  - Self-service alerting
  - NSX monitoring

Further Down the Road – Multi-Site

- Ability to stretch L2 NSX networks across Org VDCs in a VDC Group
    - vCloud Director creates the Universal DLR when creating a VDC Group
- The user also has the ability to configure the VDC Group to be Active-Active or Active-Standby
- L2 stretched network is created in all the VDCs that span the VDC Group – resizing is done automatically
- Ability to utilize the same IP pools across multiple sites
- NSX load balancer configuration allows for redundant services between multiple sites

What is EduCloud Backup?

- Simple and cost-effective cloud backup solution for your backup infrastructure.
- Integrates with your current backup infrastructure
- Allows for continued self-management of backup job schedules and data restores
- Service availability 7-days a week, 24-hours a day
- Scalable infrastructure compliant with BC privacy legislation and FIPPA requirements

What is EduCloud Backup?

- EduCloud Backup is built on EMC Data Domain
- Utilizes secure multitenancy to keep tenant data completely isolated
- Global deduplication benefits all tenants while keeping data isolated
- Leverages DDBoost – source side deduplication to reduce bandwidth and unnecessary transit of data
- Supported by majority of backup vendors (compatibility matrix)

Questions

- Thank you