



TECHNICAL PROPOSAL FOR DIGITAL IMAGING CENTER

BAIS3995 NETWORK MANAGEMENT CAPSTONE

GABRIEL KWAN, GBOLAHAN AIYETORO, DHRUV PATEL,
JITTAWAT WARAMMANUSAI

PREAMBLE

This document contains the technical proposal presented to DIC for its IT infrastructure. It will involve recommendations and general information from VLAB consulting on hardware, services, service configuration, security policies, and networking with the goal of scalable, secure and highly available IT infrastructure across multiple sites. Should the proposal be chosen, this technical document can server as basis for continued administration and expansion for IT infrastructure for DIC.

TABLE OF CONTENTS

PREAMBLE.....	i
TABLE OF FIGURES.....	x
LIST OF TABLES.....	xiii
1 CLIENT / SERVER INFRASTRUCTURE	1
1.1 SERVER HARDWARE SOLUTION.....	1
1.1.1 DELL POWEREDGE R7525	1
1.1.2 DELL POWEREDGE R6515	4
1.1.3 DELL EMC SC7020	6
1.2 SERVER HYPERVISOR SOLUTION: VSPHERE SUITE.....	8
1.3 SERVER OS SOLUTION: WINDOWS SERVER 2019 AND UBUNTU SERVER 18.04 LTS	17
1.4 SERVICE CONFIGURATION.....	19
1.4.1 AD SITES AND SERVICES DESIGN	19
1.4.2 DNS.....	21
1.4.3 DHCP.....	22
1.4.4 DFS / FILE REPLICATION SOLUTION	25
1.4.5 NETWORK PRINTING SERVICES	27

1.4.6	CERTIFICATE AUTHORITY	29
1.4.7	RADIUS AUTHENTICATION	29
1.5	AD USER AND GROUP CREATION STRATEGY.....	30
1.6	ACTIVE DIRECTORY GROUP POLICY OBJECTS DESIGN AND STRATEGY	33
1.6.1	SOFTWARE DEPLOYMENT GPO	33
1.7	CLIENT SOLUTIONS.....	36
1.7.1	OPERATING SYSTEM: WINDOWS 10 ENTERPRISE AND UBUNTU 18.04 LTS.....	36
1.7.2	THIN CLIENT: WYSE 5070 CELERONS.....	37
1.7.3	LAPTOPS/DESKTOPS: DELL OPTIPLEX 5070 AND DELL VOSTRO 3490	37
1.7.4	MOBILE DEVICES AND MDM: IPHONE AND AIRWATCH.....	38
1.7.5	REMOTE DESKTOP ACCESS: REMOTE DESKTOP, ANYDESK AND SSH	39
1.7.6	OFFICE PRODUCTIVITY SUITE/SOFTWARE	40
1.8	BACKUP SOLUTION	40
1.9	PATCH MANAGEMENT STRATEGY	41
2	NETWORK INFRASTRUCTURE	41
2.1	NETWORK DESIGN.....	41

2.1.1	EDGE NETWORK LAYER.....	42
2.1.2	CORE NETWORK LAYER.....	43
2.1.3	DISTRIBUTION NETWORK LAYER	44
2.1.4	COLLAPSED CORE LAYER.....	45
2.1.5	NETWORK VIRTUALIZATION	46
2.2	NETWORK DESIGN SPECIFICATIONS ON SITE BASIS	47
2.3	INFRASTRUCTURE ADDRESSING SCHEME AND IP MANAGEMENT SOLUTION.....	51
2.3.1	EDMONTON HEADQUARTER (HQ).....	52
2.3.2	IQALUIT.....	53
2.3.3	EDMONTON RESEARCH & INNOVATION FACILITY.....	54
2.3.4	RED DEER.....	54
2.3.5	SOUTH EDMONTON.....	56
2.3.6	WEST EDMONTON	57
2.4	FULLY MANAGED NETWORK SOLUTION	58
2.5	QOS IMPLEMENTATION.....	61
3	COMMUNICATIONS INFRASTRUCTURE.....	62
3.1	EMAIL SOLUTION.....	62
3.2	VOICE OVER IP SOLUTION.....	63

3.3	CONFERENCE CALLING/ IM PRESENCE SOLUTION	64
3.4	COLLABORATION SOLUTIONS	64
4	WEB SERVICE INFRASTRUCTURE.....	65
4.1	SECURE FTP	65
4.2	CLOUD INTEGRATION AND SECURED WWW.....	66
4.3	DOMAIN REGISTERING PROCESS EXPLAINED/REGISTERED DOMAIN.....	66
5	SECURITY STRATEGY.....	67
5.1	SECURITY AUDIT – PROCESSES AND RESULTS.....	67
5.2	INCIDENT RESPONSE.....	68
5.2.1	OVERVIEW.....	68
5.2.2	PURPOSE.....	69
5.2.3	SCOPE.....	69
5.2.4	POLICY	69
5.2.5	POLICY COMPLIANCE.....	71
5.3	FIREWALL SOLUTION	72
5.4	SITE-TO-SITE VIRTUAL PRIVATE NETWORK (VPN).....	75
5.5	SECURED SD-WAN.....	78
5.6	MULTI-FACTOR AUTHENTICATION	79

5.7	REMOTE ACCESS VPN	80
5.8	INTRUSION DETECTION AND PREVENTION SYSTEM	82
5.9	THREAT INTELLIGENCE.....	83
5.10	WEB, CONTENT AND DNS FILTERING	84
5.11	SSL INSPECTION	84
5.12	NETWORK ANTIMALWARE (ANTIVIRUS & ANTISPYWARE).....	85
5.13	MICROSEGMENTATION	86
5.14	HOST-BASED SECURITY	88
5.15	DEVICE HARDENING.....	89
5.16	SECURITY INFORMATION AND EVENT MANAGEMENT.....	89
5.17	DATA BACKUP STRATEGY.....	90
5.18	IT SECURITY POLICIES.....	92
5.18.1	PASSWORD PROTECTION POLICY	92
5.18.2	HARDWARE DISPOSAL POLICY	96
5.18.3	ROUTER AND SWITCH SECURITY POLICY.....	100
6	WIRELESS INFRASTRUCTURE	105
6.1	INTERNAL	106
6.2	EXTERNAL	107
6.3	GUEST	107

7	IT SERVICES MANAGEMENT	108
	REFERENCES	109
8	APPENDIX	119
8.1	NETWORKING	119
8.1.1	VLAN CONFIGURATION.....	119
8.1.2	PHYSICAL CABLING	119
8.1.3	PHYSICAL SWITCHES	119
8.1.4	LOGICAL DISTRIBUTED SWITCHES	120
8.2	LAYER 3 CONNECTIVITY	121
8.2.1	OSPF IPV4 & CONNECTIVITY	121
8.2.2	OSPF IPV6 & CONNECTIVITY	121
8.2.3	QOS.....	121
8.2.4	IP ADDRESS MANAGEMENT.....	122
8.2.5	WIRELESS.....	122
8.3	SEVER VIRTUALIZATION AND INFRASTRUCTURE.....	124
8.3.1	EXSI HOSTS	124
8.3.2	VM MANAGEMENT	124
8.3.3	NETWORK VIRTUALIZATION	126
8.3.4	VDI.....	139

8.4	SERVICES	141
8.4.1	CERTIFICATE AUTHORITY	141
8.4.2	SPICEWORKS TICKETING	141
8.4.3	DISTRIBUTED FILE STORAGE.....	141
8.4.4	WEB PRESENCE	141
8.4.5	PACS/RIS (LAMP STACK).....	142
8.4.6	REMOTE MANAGEMENT SOFTWARE	142
8.4.7	MICROSOFT NETWORK POLICY SERVER AAA	142
8.4.8	DIRECTORY SERVICES	143
8.4.9	DNS.....	144
8.4.10	DHCP.....	144
8.4.11	PRINT SERVER.....	144
8.4.12	PATCH MANAGEMENT.....	145
8.4.13	SFTP	145
8.5	CLIENT AND SOFTWARE	145
8.5.1	USER CREATION AUTOMATION	145
8.5.2	THIN CLIENTS	147
8.5.3	DESKTOP OPERATING SYSTEMS.....	147
8.5.4	OFFICE SUITE.....	147

8.5.5	MOBILE DEVICES.....	148
8.5.6	SOFTWARE DEPLOYMENT VIA GPO	148
8.6	SECURITY AND FIREWALL.....	148
8.6.1	FIREWALL.....	148
8.6.2	VPN.....	149
8.6.3	UNIFIED THREAT MANAGEMENT (UTM)	152
8.6.4	FIREWALL POLICIES.....	153
8.7	COMMUNICATIONS INFRASTRUCTURE.....	154
8.7.1	VMWARE AIRWATCH.....	154
8.7.2	SHAREPOINT.....	154
8.7.3	EXCHANGE	155
8.7.4	CISCO CUCM	155
8.8	MONITORING.....	156
8.8.1	SECURITY MONITORING.....	156
8.8.2	PERFORMANCE MONITORING.....	156
8.8.3	NETWORK MONITORING TOOL	156
8.8.4	BACKUP SOLUTION.....	157

TABLE OF FIGURES

FIGURE 1 DELL POWEREDGE R7525 (DELL EMC POWEREDGE R7525 RACK SERVER DELL USA, N.D.)	1
FIGURE 2 RAID 50 DRIVE TOPOLOGY, UP TO A SINGLE DRIVE FAILURE ON EACH RAID 5 INSTNACE	6
FIGURE 3 DELL EMC SC 7020 (DELL SC7020 STORAGE ARRAY, N.D.)	6
FIGURE 4 THREE SERVER HYPER-CONVERGED CLUSTER	8
FIGURE 5 WORKFLOW OF CALLCENTER-VDI DESKTOP POOL.....	16
FIGURE 6 SITES AND REPLICATION TOPOLOGY	19
FIGURE 7 HIGH LEVEL OVERVIEW OF THE ORDER OF PRECEDENCE FOR DHCP REQUEST FROM CLIENT IN RED DEER	23
FIGURE 8 ORDER FOR PRECEDENCE FOR PROFILE NAMESPACE WHEN CLIENT ACCESSING FROM RED DEER	25
FIGURE 9 DFS REPLICATION TOPOLOGY FOR ANY PARTICULAR NAMESPACE	26
FIGURE 10 IMAGECLASS D1650	28
FIGURE 11 OU CONFIGURATION FOR NON-PRIVILEGED USER ACCOUNTS	31
FIGURE 12 OU CONFIGURATION FOR ADMINISTRATIVE ACCOUNTS	32
FIGURE 13 SUGGESTED NETWORK SOLUTION FOR EDMONTON HQ	49
FIGURE 14 SUGGESTED NETWORK SOLUTION FOR IQALUIT, RED DEER, WEST EDMONTON, SOUTH EDMONTON, R&I	50

FIGURE 15 OVERVIEW OF LAYER 2 MAP ON NETCRUNCH.....	60
FIGURE 16 OVERVIEW OF NETWORK ATLAS ON NETCRUNCH.....	61
FIGURE 17 FORTIGATE NGFW 1500D MODEL (FORTINET, 2020).....	73
FIGURE 18 FIREWALL POLICY EXAMPLE (FORTINET, N.D.-G).....	75
FIGURE 19 INTER-SITE VPN CONNECTIONS.....	76
FIGURE 20 FORTIAUTHENTICATOR(FORTINET, 2019)	79
FIGURE 21 REMOTE ACCESS VPN USING MFA VIA FORTIAUTHENTICATOR (FORTINET, N.D.-J)	81
FIGURE 22 REMOTE ACCESS USING FULL TUNNELING (FORTINET, N.D.-I)	82
FIGURE 23 MICROSEGMENTATION FOR EAST-WEST TRAFFIC (PALOALTO, N.D.)	87
FIGURE 24 FORTIAP 421E MODEL (FORTINET, N.D.-A)	106
FIGURE 25 DISTRIBUTED SWITCH AND DISTRIBUTED PORT GROUP	120
FIGURE 26 DASHBOARD OF NSX ACCESS FROM VCENTER.....	127
FIGURE 27 TRANSPORT ZONE OF NSX	128
FIGURE 28 EDGE ROUTER ON NSX.....	129
FIGURE 29 INTERFACES OF NSX EDGE ROUTER.....	130
FIGURE 30 INTERFACE CONFIGURATION	131
FIGURE 31 EDGE INTERFACE CONNECTION TO PHYSICAL PORT THROUGH DISTRIBUTED PORT GROUP	132
FIGURE 32 ROUTING OPTIONS ON EDGE ROUTER.....	133

FIGURE 33 OSPF CONFIGURATION ON NSX EDGE	134
FIGURE 34 IPV6 STATIC ROUTE CONFIGURATION.....	135
FIGURE 35 FIREWALL RULES CONFIGURATION ON NSX EDGE	136
FIGURE 36 DISTRIBUTED ROUTER ON NSX FOR PLAZA	137
FIGURE 37 LOGICAL SWITCH ON ALL SITES	138
FIGURE 38 SEGMENT ID POOL ON NSX.....	138
FIGURE 39 NSX CONTROLLER FOR VIRTUALIZATION PLATFORM.....	139
FIGURE 40 MANAGED SERVICES BY NETCRUNCH MONITORING TOOL	Error! Bookmark not defined.

LIST OF TABLES

TABLE 1 EDMONTON HQ IP ADDRESSES SCHEMES	52
TABLE 2 IQALUIT IP ADDRESSES SCHEMES.....	53
TABLE 3 RESEARCH & INNOVATION IP ADDRESSES SCHEMES	54
TABLE 4 RED DEER IP ADDRESSES SCHEMES	54
TABLE 5 SOUTH EDMONTON IP ADDRESSES SCHEMES.....	56
TABLE 6 WEST EDMONTON IP ADDRESSES SCHEMES	57

1 CLIENT / SERVER INFRASTRUCTURE

1.1 SERVER HARDWARE SOLUTION

For the hardware server solution, VLAB recommends deployment of Dell PowerEdge Rack Servers. Specific models or adjustments will be issued based the operation requirements. Dell PowerEdge R7525 2U Rack Server will be used for EXSI hosts. The R7525 provides a good balance of scalable performance x86-64 performance, good vendor support for hypervisors and relatively low physical footprint. For services and sites that require less power, a more lightweight PowerEdge R6515 1U Rack Servers should be deployed. With this in mind, we recommend a total of 3 R7525s on major sites for the primary services. Major sites include Red Deer, Edmonton HQ, and R&I. All other sites will contain deploy 1-2 R6515s as will HQ for its DMZ servers.

1.1.1 DELL POWEREDGE R7525



Figure 1 Dell PowerEdge R7525 (Dell EMC PowerEdge R7525 Rack Server | Dell USA, n.d.)

Per Dell Datasheets, each R7525 supports up to 32 Dual in-line Memory modules (DIMM) and there are two types of memory that can be used. Those two DIMM type are Registered DIMMs (RDIMMS) and Load Reduced DIMMs (LRDIMMS). RDIMMS support a max of 2 Terabytes (TB) of total capacity of random-access memory (RAM) and a max of 4TB for Load Reduced (LR) DIMMs. Although LR DIMMS will double the potential capacity of RAM, VLAB does not recommend the use of LR DIMMS over Registered DIMMS for two reasons(*Dell EMC PowerEdge R7525 Rack Server* | Dell USA, n.d.). First, we do not anticipate the need to scale up to 4TB of RAM. Given the current and anticipated operational requirements, RAM usage should not exceed even 2 TB. Secondly, there is an increase in latency with LR DIMMS. Given that operational requirements do not require DIC to have up to 4TB of RAM and better performance can be gained with RDIMMS, RDIMMS are VLABs recommendation.

In terms of CPU, the R7525 supports up to 128 cores per CPUs spread across two 2nd Generation EPYC processors. Here at VLAB, we recommend two AMD EPYC 7542 2.90GHZ 32 core processors over Intel offerings. There are two major reasons. First is performance per dollar, AMD offers a much better value from their EPYC line of processors when compared to their Intel offerings across a variety of synthetic benchmarks (Gelas, 2019; Larabel, 2019). Furthermore, Intel is much more exposed in terms of speculative exploits that are currently plaguing the x86 CPU market. Per Armasu's research on *Tom's Hardware*, Intel had 242 publicly disclosed vulnerabilities compared to AMD's 16 as of 2019 (Armasu, 2019). Given this lopsided

trend and the significant decreases in performance on account of fixes required to prevent these speculative attacks, VLAB expects a significant decrease in performance and scalability over time if Intel were to be the primary CPU vendor. As such AMD processors are our recommendation.

In terms of storage VM storage on these servers, there are two major options under consideration. Those are solid state drives (SSD) and hard disk drives (HDD). Although HDDs offer a better storage to dollar ratio, SSD are slowly catching up in terms of cost effectiveness. Furthermore, SSDs offer much better read and write performances when compared to HDDs. Given that the storage on these servers will primarily use for the VM system storage rather than application data. Because the R7525 can support up to 16 2.5-inch drives, our recommendation, if deployed with 14 3.8TB SSDs capacity drives, this will give us a total of approximately 83TB of shared storage in the mirrored configuration. In this configuration, up to 1 host failures can be tolerated.

With the addition of riser cards, each server can support up to 5 full length PCIe cards. This can be used for either graphic processing units or additional networking cards. For most of the servers of this type, additional network cards will be used. There needs to be a minimum of 4 network connections are required for both general connectivity as well hypervisor utilities such as vMotion, and vSAN. Additional ports can be used in conjunction with/or failover within EXSI. If additional GPU/FPGA compute or GPU passthrough is required, NVIDIA Tesla cards should be used.

As for the default configuration of R7525s, the following is the recommendation for current deployment:

2x AMD EPYC 7542 2.90GHZ 32C/64T with 128M of Cache

256 GB RDIMM at 3200MT/s Dual Rank (8*32 RDIMMs)

14x 3.8TB SAS SSDs Read Intensive (Capacity)

2x 800 TB Flash SSD Write Intensive Usage (Caching)

1x 960GB NVME boot drive

The following are dependent on the specific use case:

1-2x Intel i350 Quad Port 1 GbE - OR – Intel X710 Quad Port 10GbE SFP+ -OR- 3x NVIDIA® Tesla™ M10 w VDI

Note: RAM can easily be extended without major change in hardware as only 4 of Currently factored storage exceeds the current needs and is done in consideration of ballooning size of imaging as quality increases.

1.1.2 DELL POWEREDGE R6515

The Dell PowerEdge R6515 is essentially a 1U version of the R7525 with half the available DIMM slots (16), 10x 2.5 slots and 1 CPU instead of 2 (*Dell EMC PowerEdge R6515 Rack Server*, n.d.). However, given that these servers will likely not be operating in a clustered fashion at the hypervisor level, hardware RAID will be used for storage on these devices. In choosing the hardware RAID type to use, VLAB have

determined that RAID 50 is the best balance between complexity, performance and storage capacity. Within the RAID 0 array, there will be 3 RAID 5 arrays composed of the said drives

Although more complex than RAID 5, RAID 50 will allow for increased number of disk failure as well as providing increased performance. Up to 1 drive failure per RAID 5 instance within RAID 50. Conversely, RAID 60 is also possible with the H730P RAID controller. However, there is a significant decrease in available storage and decreased read speeds. As such we believe that RAID 50 is the best balance. With 9 0.96 TB disks utilized in 2 RAID-5 units under a RAID-0 cluster, total storage is at 5.76 GB with 6x read speeds. Up to 3 drives, one in each RAID-5 node in the RAID-50 cluster, can fail.

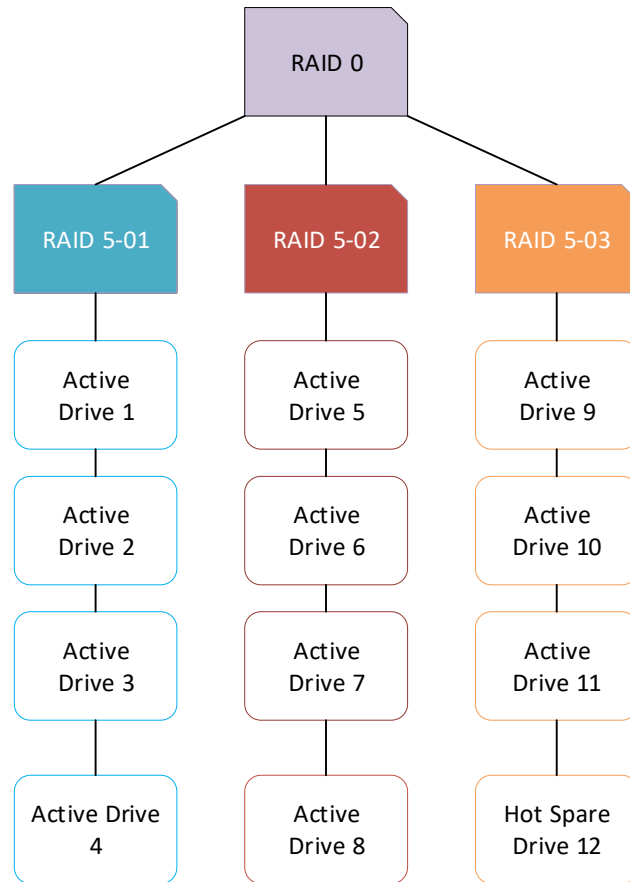


Figure 2 RAID 50 drive TOPOLOGY, up to a single drive failure on each RAID 5 instance

1.1.3 DELL EMC SC7020



Figure 3 Dell EMC SC 7020 (Dell SC7020 Storage Array, n.d.)

Although vSAN is designed to be scalable, it cannot match the scalability of more traditional storage solutions if storage is the only criteria. Furthermore, it is important to maintain a separate storage solution for backups and long-term storage. As such additional storage outside of the computing servers is required. For this additional external storage, VLAB recommends the Dell EMC SC7020. This SAN storage device can support up to 30 2.5 drive bays internal (*Dell SC7020 Storage Array*, n.d.). With 30 SAS drives at 4TB, we have a total storage of 108TB in RAID 50 configuration. As mentioned, these storage solutions can scale much better than vSAN through additional enclosures. These enclosures can add up to an additional 80 drives. If the same 4TB drives are used, an additional 78 drives in a 3 Parity RAID configuration can add up to 300 TB of storage space with 75x read speeds. If a 4 parity RAID 50 is employed using all 80 drive slots, 304 TB of storage can be achieved with 76x read speeds. Our recommendation is to start with two of each of the primary sites and add enclosures as required. One for dedicated for backups and another for long-term storage.

1.2 SERVER HYPERVISOR SOLUTION: VSPHERE SUITE

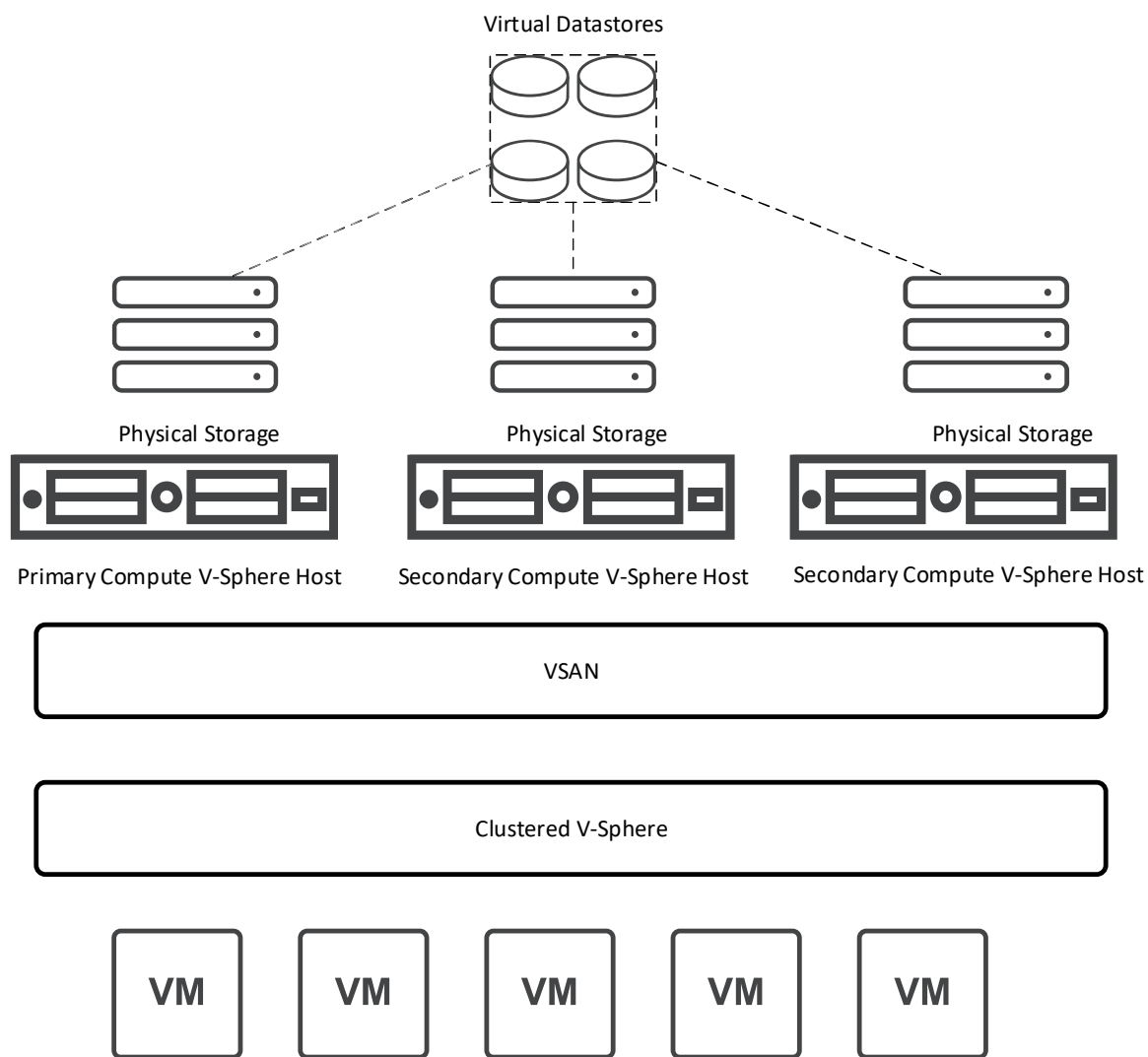


Figure 4 three Server Hyper-Converged Cluster

For the type 1 hypervisor solution that will be used on all the servers, VLAB's recommendation is VMware's vSphere Suite version 6.7. Although 7.0 was released as of the writing of this document, we do not recommend going for the latest version as there are likely to be issues that will need to be resolved before it is production ready. vSphere is an industry leading hypervisor solution composed primarily of

vSphere EXSI hypervisors, vCenter Management for centralized EXSI management, vSAN for hyper-converged storage, automation, and integration with vCloud. Furthermore, with version 6.7 there is 2-3x increase in performance for vCenter Operations, memory allocation, and DRS related functions (Manuro, 2018). Other options included Microsoft's own Hyper-V solution which integrates well with Microsoft System Center Ecosystem. Nonetheless VLAB still recommends VMWare solution over Hyper-V. The following sections will describe components and features of vSphere and how they will help enable DIC infrastructure to be highly available and scalable.

1.2.1.1 EXSI

One of the major benefits of ESXI over Hyper-V is its lightweight nature and more resilient than its Hyper-V counterpart. EXSi inherently requires minimal system resources and has an incredibly low footprint of 70mb allowing it to run entirely in memory(Lee, 2019; Reed, 2018). It employs its VMKernel that controls the resources made available to Virtual machines. To manage ESXi, ESXi has its own built-in web GUI vSphere Client that enables it to be managed directly but is primarily managed through other independent virtual appliances such as vCenter. Even in the case that a management appliance such as vCenter crashes, the virtual machines remain active and running so long as the VMKernel is still active.

In contrast, Hyper-V is based on Windows Server and stores the host operating system and guest VMs in a what Microsoft describes as partitions. In order to manage the hypervisor, a user needs to access the Parent partition which is typically either a full-blown Windows Server install with the Hyper-V role installed or the lighter-weight Windows Hyper-V Server operating system. Virtual Machines in Hyper-V are then stored in guest partitions that are provided with virtualized hardware via a Virtualization Service Provider (VSP) or are given direct access to hardware via Hyper-V's Virtualization Service Client (VSC). This parent partition is required for the hypervisor to be managed. If the parent partition crashes, all guest partitions will also crash.

Another major benefit of ESXi over Hyper-V is its advanced fine tune resource usage. Although Hyper-V has the ability specify startup random access memory (RAM), minimum RAM, maximum RAM, Memory Buffer and Memory weight, a virtual machine with these settings are locked to a single NUMA node or CPU (Lee, 2019). This means that if Hyper-V is running on a server with multiple CPUs with their independent memory controllers, a virtual machine that operating a CPU cannot be allocated additional RAM associated with another CPU. Conversely, ESXi can provide this RAM from another CPU if required albeit with some sacrifice in performance. Furthermore, the VMKernel can dynamically change the CPU that the server is being hosted on to one with more available resources (Zimmer, 2019). In addition to these dynamic features, administrators can use also Resource Pools to group appliances or virtual machines. This enables said administrators to delegate

resource management and compartmentalize resource within an ESXi cluster including CPU and memory usages.

1.2.1.2 VCENTER

vCenter is the primary means of managing EXSi hosts and enables many of the features that were previously mentioned. It is deployed as its own virtual appliance and authentication can be integrated with Windows Active Directory although it does have its own directory service. Once the appliance has been deployed it can connect to EXSi hosts, an administrator can administer the EXSi hosts via HTML5 or Flash vSphere Client. This includes the creation of vSAN cluster, EXSi High Availability, DRS cluster, vMotion for live migration of compute or storage, software defined network via NSX management. When combined, these features help ensure availability of virtual machines on the EXSi hosts managed by vCenter. While vCenter availability has been available since version 6.5, it requires its own private network and additional witness nodes. Given that EXSi can largely operate independent of vCenter, restoring from backups or short downtimes for patching will be easier to manage. Furthermore, because vCenter will be deployed in a 3-node cluster with vSAN, even if the node containing vCenter goes down, it can easily be brought back on an active node quite rapidly.

1.2.1.3 VSAN

vSAN provides a software defined storage solution that enables sharing of storage resource amongst multiple systems without the need for a dedicated SAN or NAs device. Furthermore, it provides QoS for storage allowing the system to dynamical shift data to storage based on policy and operational requirements. It can operate in 3 modes, RAID-1, RAID-5 and RAID-6 mode. Microsoft has a similar offering provided in Windows Server called Storage Spaces Direct, which enables using locally available storage to be shared among a Hyper-V cluster and storage QoS based on defined policies (Microsoft, 2019). Like vSAN, Storage Spaces Direct offers RAID-1 style mirror as well as RAID-5 and RAID-6 style mirroring of data. Although they share the name of hardware/software RAID modes, they are not direct equivalents.

vSAN RAID-1 mirror mode requires a minimum 2 servers and a witness node, or a 3-server node. Drives that are on these nodes pool together their raw data capacity with 50% of the raw storage as usable storage in a 3-node setup. This useable storage is then replicated across all three nodes. As such, any one of the nodes has access to the virtual SAN at any given time. This enables clustering of three servers without the need for an additional physical SAN device. In this setup, up to 1 node failure is allowed.

Although Direct Storage allows RAID-1 equivalent 2-way mirrors with two hosts rather than 3, it is less efficient when compared to vSAN Higher RAID levels. Both systems still require 4 nodes and if a 3rd node is added, it can only operate in a

3-way mirror mode. This means 33.3% storage efficiency compared to vSAN's 50% across 3 nodes per VMware's vSAN ReadyNode Sizer(VMware, n.d.).

As mentioned, other RAID modes require at-least 1-2 more nodes depending on the RAID mode in either system. Much like their traditional RAID equivalents, vSAN RAID-5 and vSAN RAID-6 support additional node failures, provide additional performance gains as well as better storage usage efficiency. For a better idea of the storage requirements and/or availability of storage with any given setup, it is best to use the vSAN calculator provided by VMWare.

Given our recommendation is 3 server nodes in each cluster among the sites, vSAN provides a more efficient storage solution in RAID-1 mode when compared to Microsoft Storage Spaces Direct. Furthermore, vSAN is well integrated with vSphere. Microsoft's Storage Spaces Direct could be used as it is independent from the Hyper-V, to use it for Hyper-Visor storage would be convoluted and circumvents the point of using hyper-converged storage solutions for our hypervisors.

1.2.1.4 VREALIZE – AUTOMATION – ORCHESTRATOR

Outside of vCenter Policies and Templates, the vRealize Orchestrator and Automation appliance can be deployed to provide template and workflows for repetitive tasks, as well as enable self-provisioning for virtual machine resources.

The Orchestrator portion of the vRealize Orchestrator and Automation appliance provides templates for workflows and repetitive tasks such as bulk VM deployment, bulk migration of VMs to servers based on user specified criteria, and

bulk creation of NSX objects and logical networking objects. Furthermore, it allows the creation of workflows based on templates or even combine multiple tasks for additionally complex operations. An example for a basic task that would be useful for DIC is the deployment of servers from a template. Using this template, servers can be automatically provisioned from specified template. Additional actions can be performed on the server such as running sysprep, joining the domain and even run custom scripts to install server roles upon completion. Furthermore, the tasks can be configured to send status reports on the task via email for long and multi-step tasks. Once a task has been programmed to an administrator's liking the task can be reused or even scheduled to be repeated.

Conversely, the vRealize Automation portion of the appliance enables the creation of web portals to enable self-provisioning of resources on the vSphere clusters. This may be useful in the researchers at R&I who may wish to request resources for their resources. While an administrator could manually create and provision the resources the researchers require, the vRealize automation can allow administrators to safely delegate pools of resources to users to create Virtual Machines without the need for the Administrator to intervene directly.

1.2.1.5 VMWARE HORIZON

VMware Horizon is VMware's equivalent to Windows App-V and Microsoft Remote Desktop Services solutions and provides remote access to automatically provisioned Virtual Desktops organized into Desktop Pools on a vSphere ESXi host or cluster. Although these Windows solutions provide a comparable experience, Horizon

provides better integration with the vSphere product stack. Integration with Active Directory also enables authentication and entitlements to resources using Windows Security groups and/or users.

In terms of the desktop pools, users can use either dedicated assignment or floating assignment. Dedicated assignment enables stateful virtual machines in which users will maintain files and configurations every time they access Horizon. Given the limited number of current users, dedicated-assignment pools can be used. However, as the operation scales and resources become more limited, floating assignment is recommended. Using this method, virtual machines will be dynamically created and destroyed as need arises. Furthermore, potential application data such as booking information should not be stored locally but accessed through intranet web applications such as SharePoint. As such our recommendation is to use floating-assignment pools.

Based on the request and our recommendation, deployment will consist of a Windows Servers running VMWare Horizon Connection Server and Horizon View Composer in HQ for the Call Center Thin Clients. In conjunction with vCenter, Horizon Connection server will enable the management of a “CallCenter-VDI” desktop pools and provide the Active Directory “Call Center” security group entitlement to that said Desktop Pool. With Horizon View Composer, Horizon Connection server can create linked clones for the “Call Center-VID”. Linked clones share a base virtual disk with user made changes stored in a separate virtual disk. This helps reduce storage utilize as well as increase the deployment speed.

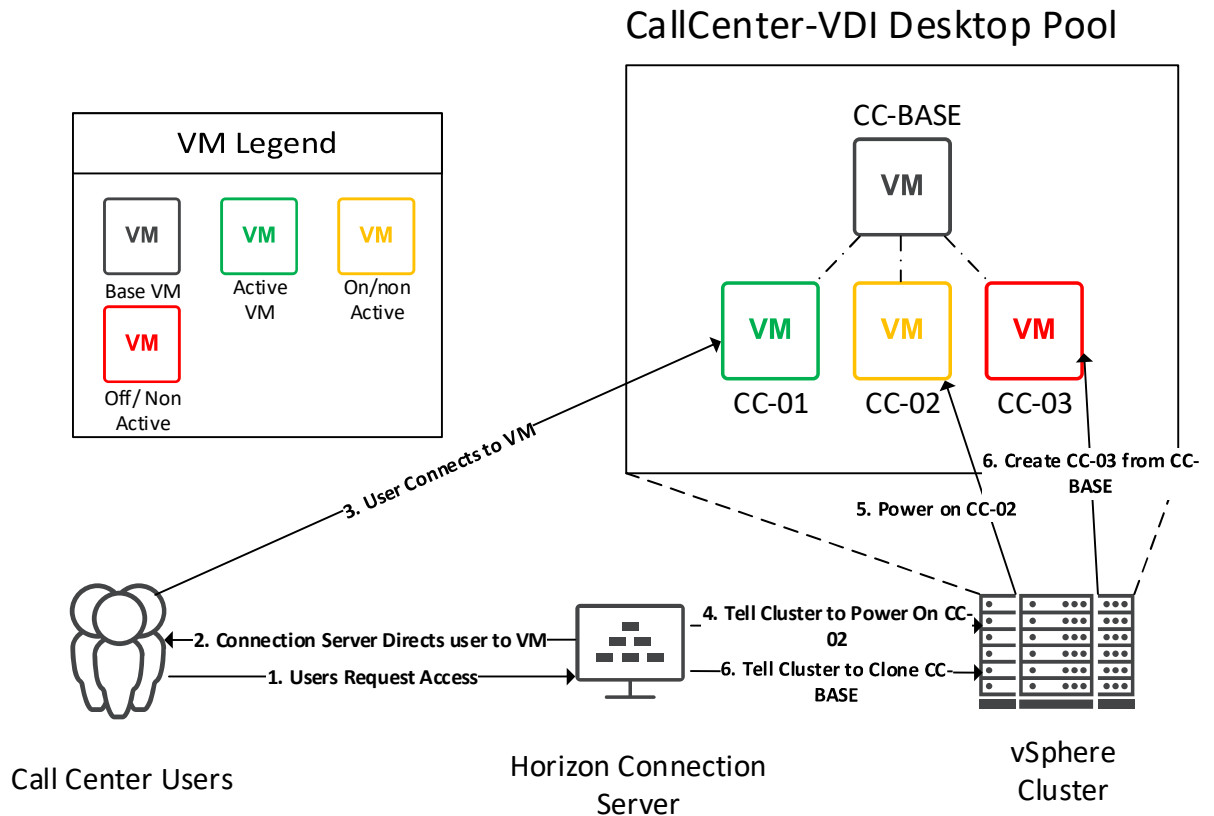


Figure 5 Workflow of CallCenter-VDI Desktop Pool

To ensure speedy access and deployment of VMs additional deployment parameters for the Desktop Pool should be set. We recommend maintaining a minimum of 2 un-used VMs to be provisioned. Furthermore, one of those machines should always be powered on. The maximum VMs provisioned and powered on at any given time should be 12 based on the employee list provided but can be adjusted as more call center agents are added. With this configuration, when a user connects to the connection server using Horizon View client, Horizon Connection server will direct the user to the pre-provisioned and powered-on VM within the pool. At the same time, Connection Server and Horizon View will power on the other VM and provision another in a powered off state to maintain the desktop pool policy. See

Figure 5 for a high-level overview of the process. Once a user logs off, the VMs will be removed and redeployed as required to maintain the policy.

1.2.1.6 VM SECURITY

VMs and virtual disks associated with them should be encrypted in the case that physical security has failed to prevent access to the servers. This is especially important given the sensitive nature of the data DIC will be storing on their servers. For VM encryption at rest, VMware requires a Key Management Servers such as Dell Cloud Link. Once linked with vCenter, virtual machines can be encrypted when created or when encryption is applied via storage policies. Needless to say, encryption should be applied on all virtual machines. Without the proper keys from the KMS, attackers will not be able to access the VM configuration nor will they be able to access the contents in the virtual disk even if they have access to the raw data.

1.3 SERVER OS SOLUTION: WINDOWS SERVER 2019 AND UBUNTU SERVER 18.04 LTS

There are two primary server OS solutions that will be deployed. Those are Windows Servers edition 2016 and 2019 where possible. Furthermore, Ubuntu Server for Linux services on the R&I site as requested by the DIC.

The reason we chose to use Windows Server 2019 is its integration with the recommended services as well as provide a centralized client policy with GPOs and directory service through Active Directory. Many of the server-side Microsoft applications VLAB recommends such as Exchange, Network Access, SharePoint and Enterprise Certificate Authority rely on the centralized directory and DNS services

provided by Active Directory. Furthermore, it is compatible with any applications that support LDAPS such as CUCM, LAMP stacks for RIS/PACs systems and more.

In terms of the Linux Operating System, Ubuntu was chosen based on the documentation available for Ubuntu, large number of third-party repositories, Debian base, as well as its set release cycle. In terms of documentation, Ubuntu hosts its Ubuntu Server Guide on its website as well as tutorials for installation and as well as more advanced features such as containers, and Kubernetes(Canonical, 2020). Because it is based on Debian and is open source, Ubuntu is stable and can leverage some of the development and QA hours spent on the former; however, Ubuntu also provides proprietary blobs to ensure compatibility and additional features that are otherwise not found in Debian (Canonical, n.d.). Canonical provides service level agreements for support if required as well.

In terms of the specific version of the operating system, we recommend 18.04 Long Term Support. This version was chosen as it has been available since April 2018. With that in mind, this version has had time to mature and fixes to early issues should have been resolved. Furthermore, it will receive extended security maintenance support until 2028 (*Ubuntu release cycle*, n.d.). Although version 20.04 is to be released by the end of April 2020, VLAB cannot be certain that there will be no issues that may affect deployment.

1.4 SERVICE CONFIGURATION

1.4.1 AD SITES AND SERVICES DESIGN

In terms of active directory forests and domains, there some options in terms of deployment. Those include the use of primary forests and resource forests, or multiple sub-domains within the design. However, we believe that these methods of deployments add unnecessary complication to the topology, administrative overhead and do not provide any clear benefit for this deployment. Instead, VLAB recommends a simpler single forest and domain with multiple sites.

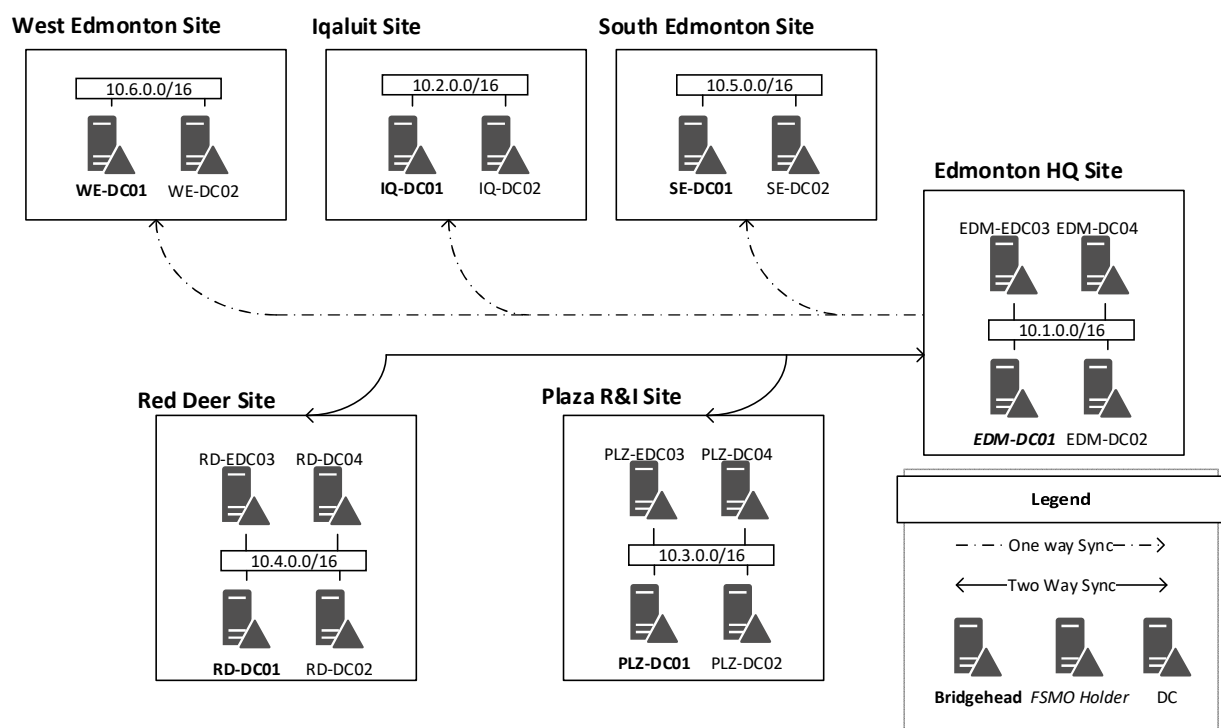


Figure 6 Sites and Replication Topology

In terms of AD sites, each remote office will be its own site with a minimum of two Active Directory servers. These sites will be distinguished via subnets. Each site has a /16 subnet in the 10.0.0.0/8 network assigned. For example, HQ will have the

subnet of 10.1.0.0/16. See the networking section for more details on subnetting. Main offices such as Red Deer, Edmonton HQ and IQ will have 4. Active Directory servers located non-primary sites will be read-only. Administration should not be done on these servers and this will help reduce the attack surface area should these sites be compromised. Bridgeheads server will be automatically determined by the Active Directory KCC for optimal syncing. Furthermore, global catalog (GC) placement is not of concern as there will be no cross-forest queries.

Per Microsoft recommendations, Active Directory FSMO roles will also be located on a single Active Directory Server located in HQ site given that there is a single forest (*FSMO placement and optimization on Active Directory domain controllers*, 2018). If the primary site does go down, or if maintenance needs to be done on the FSMO server, seizure or transfer of roles can be done, respectively. In the case of site failure, once the Disaster Recovery Team has determined it as necessary, seizure of roles should be initiated to Red Deer or R&I. Backups for domain controllers should be made periodically but should not be used to restore unless all writable domain controllers are out.

Regarding replication scheduling, the default interval of 180 minutes should be enough for sites located in Alberta. In the case that replication is needed outside of security updates, manual replications can be initiated. However, given the less reliable connections to Iqaluit, replication to Iqaluit should be limited to non-peak hours to preserve their limited bandwidth. VLAB suspects that non-peak hours would

be during lunch breaks, after work hours and weekends. However, a more specific schedule can be derived once a baseline for network activity has been confirmed.

1.4.2 DNS

Intranet DNS records will be primary handled by the Active Directory Servers that will be running integrated DNS role. Said servers are located throughout the organization and across all sites. There will be a minimum of 2 Active Directory controllers in each site hosted on hypervisors located on each site in a variety configuration. Because internal DNS is associated with Active Directory, all DNS records should be synced through intra & inter site replication. See AD Sites and Services design better idea of the replication topology. Secured Dynamic updates will be enabled to prevent erroneous DNS updates.

Regarding DNS requests for internet, FortiGate DNS servers will be used, and requests will be verified through DNS filtering done at network edge by the FortiGate firewalls. Furthermore, the primary site will have a have external DNS servers located in the DMZ. This will provide public DNS records for on-premise services such as Exchange, CUCM and any other planned services that are outward facing. Although DNS services can be provided by the domain name registrar, we believe that handling DNS on premise is more efficient and provides the organization more flexibility.

1.4.3 DHCP

DCHP for both IPv4 and IPv6 will be handled via the DHCP role on Windows servers located across all sites. Our recommendation is to have two servers on the major sites and one for all secondary sites. While it is possible to run DHCP on the same servers as the DNS and AD, it is not best practice. A such independent servers will be used for DHCP.

In terms of configuration, DHCPv4 super scopes should be created for each /16 subnet associated with each site. Scopes for specific VLANs will then be nested within said super scopes for ease of management. DNS option in these scopes should include servers within the site first and then DNS servers on other sites. This will ensure that DNS requests will be sent first locally before going to other sites to preserve bandwidth. Option 150 will be enabled to help voice over ip (VOIP) phones reach the Trivial File Transfer Protocol server on CUCM for configuration. Option 67 will only be for PXE boot for SCCM.

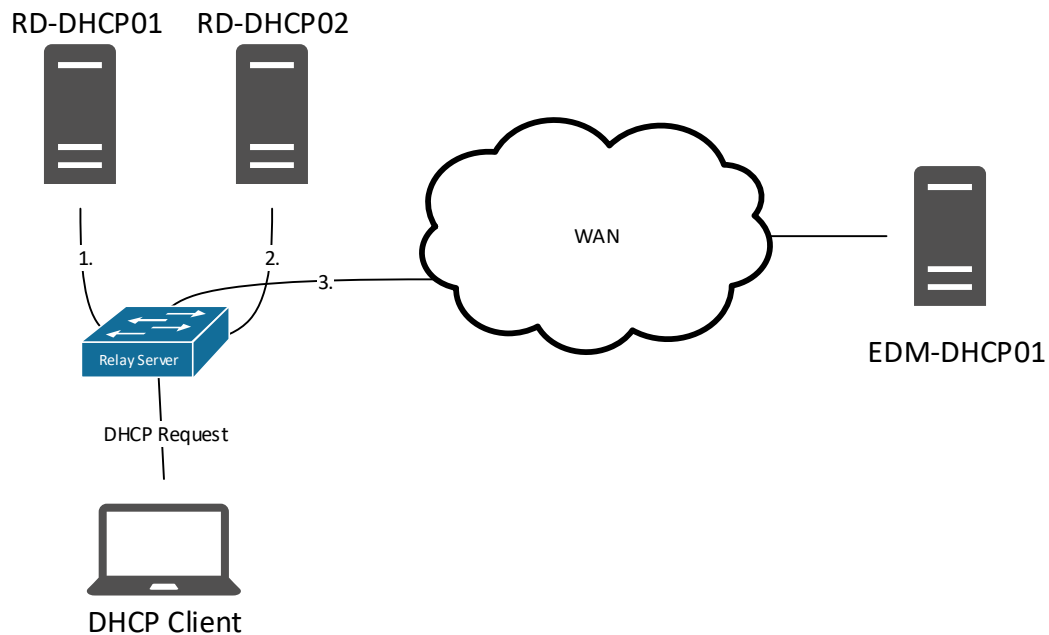


Figure 7 High level Overview of the order of precedence for DHCP Request from Client in RED Deer

To ensure high availability, IPv4 scopes will be configured in failover mode with the site-specific servers being the primary servers. Secondary servers are to be in the Edmonton HQ datacenter. Should all site-specific primary servers become non-functional, the DHCP servers located in HQ will become active. **Error! Reference source not found.** provides a high-level overview of the order of precedence for DHCP request. If the primary active server for the scope is RD-DHCP01 and is unavailable, RD-DHCP02 will become the active DHCP server for that scope. If RD-DHCP02 also becomes inactive, EDM-DHCP01 will take over. EDM-DHCP01 taking over is a worst-case scenario and should be avoided when possible. Because these servers may not be in the same VLANs as the access devices, DHCP relay will be

configured first hop network devices. This may be a physical L3 device for physical hosts, but it may also be a virtualized NSX distributed routers or NSX Edge router for VDI's virtual machines/applications.

DHCPv6 scopes cannot be configured in high availability mode. However, clients should be able to auto-configure their addresses using prefixes advertised through router-advertisements from first hop devices. Furthermore, options can be acquired from IPv6 relays configured on the first hop network devices. As the DHCPv6 servers will not maintain a stateful database, there should be no conflicts of addressing. As such, duplicate IPv6 scopes can be created without any issue to ensure clients are able to get their DNS settings.

1.4.4 DFS / FILE REPLICATION SOLUTION

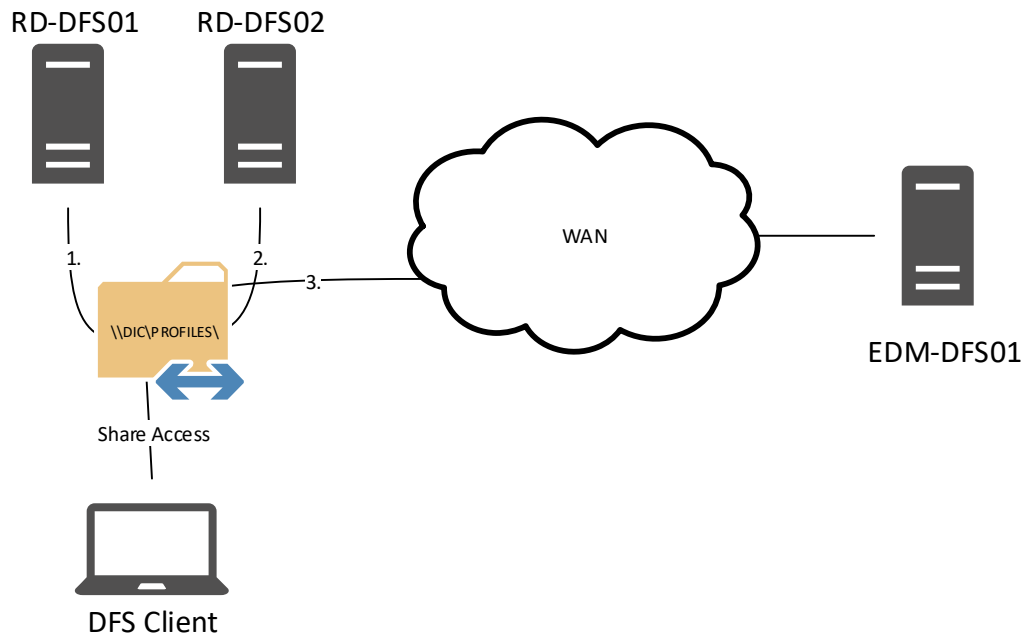


Figure 8 Order for precedence for PROFILE Namespace when Client Accessing from Red Deer

Outside of the preconfigured Distributed File System (DFS) used by Active Directory syncing, DFS will also be configured across sites to ensure certain files are accessible in the most efficient manner possible in all sites. Our recommendations for Namespaces would include \\DIC\SOFTWARE for publish/assigning software and \\DIC\PROFILES for roaming profile storage. With the former, software assignments via group policies can acquire the installation files and scripts from the most convenient fileserver. With the latter, users in the Red Deer site should be able to transparently access their home folders within mapped drive associated with a Namespace without noticing which server they are accessing. Primally, the Red Deer client should be accessing site-local shares first. Only when all site-local options are

exhausted should the client defer to the EDM-DFS01 as shown in **Error! Reference source not found..**

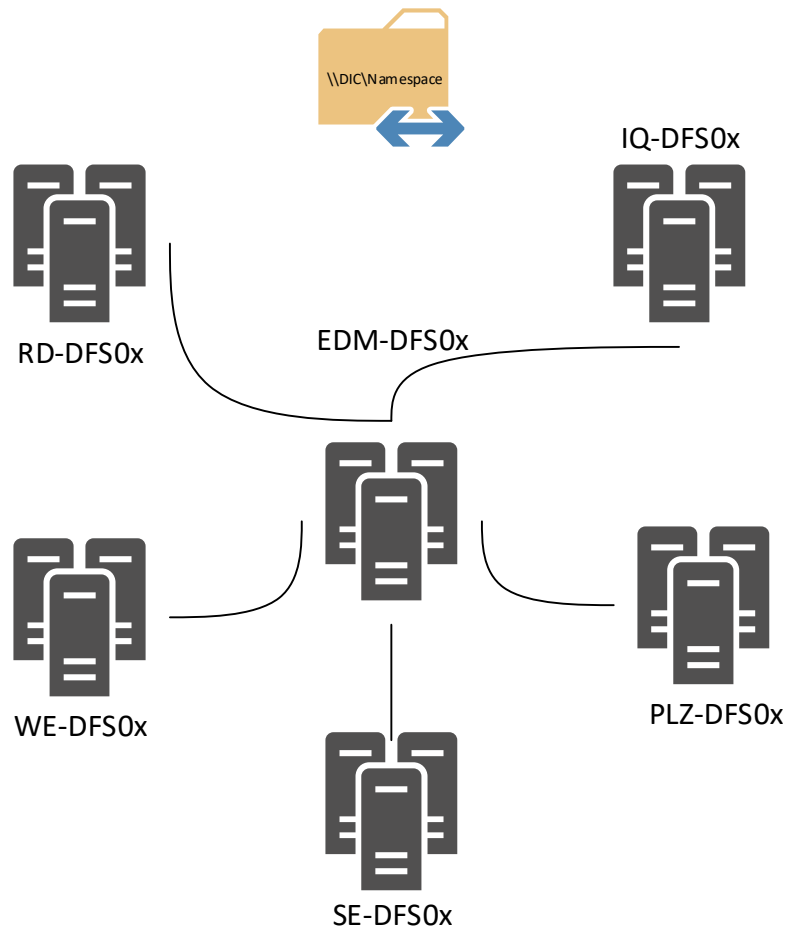


Figure 9 DFS Replication Topology for any particular NameSpace

In terms of replication, DFS replication will be deployed in a hub and spoke manner between sites with Edmonton HQ as the hub. Replication within sites can be point-to-point as bandwidth is more readily available. When scheduling replication, replication bandwidth should be limited over WAN links during peak hours. Bandwidth restrictions should be lifted during off hours to ensure files are

properly synced across sites. Because of this, DFS should not be used as a means of collaborative work. For that scenario, SharePoint and Exchange are better means of exchanging files as files are not instantly replicated to other sites.

1.4.5 NETWORK PRINTING SERVICES

Given the nature of the organization, it is likely that printers will be used extensively for printing out consent and information request forms for customers to fill out to access DIC's imaging services. As such, a centralized platform for managing printers will need to be implemented. Although VLAB would like to use Windows printing server for managing printing, because of use of Linux clients in R&I Plaza our suggestion for this deployment will be to use CUPS on a Linux Servers on each site. Printers associated with CUPS will be assigned to via GPOs applied at the site level. This means that users logging into machines on one site will have printers assigned to them on the site that they are on. This will also apply to laptop users as the machine migrates to different sites.



Figure 10 imageCLASS D1650

In terms of the hardware, we recommend the imageCLASS D1650 on the primary sites. This printer does black and white printing as well as scanning. It supports a legal letter, and statement paper formats and has a copy speed and print speed of 45 PPM. Furthermore, the recommendation is 2000-7000 pages printed per month. Notable features include the supports Department ID authentication to ensure that proper billing of printer jobs. It also supports IPv6 and supports wired and wireless connectivity using enterprise level security. (*ImageCLASS D1650 | Black & White Multifunction Printer*, n.d.) For sites we recommend the imageCLASS MF236n which has many of the same features but with lower ppm of 24 with a

recommended print volume of 500-2000 pages(*Canon imageCLASS MF236n | Black & White Multifunction Printer*, n.d.).

1.4.6 CERTIFICATE AUTHORITY

In order to secure intranet wireless traffic, enable LDAPS, HTTPS, and Exchange, certificates need to be issued to these services. For certificate services, VLAB recommends using Windows Server Certificate Services. Windows Server Certificate Authority integrates well with Windows Deployments within Active Directory and allows certificate manual requests and renewals easily through management consoles or through web enrollment. However, to reduce administrative burden, GPOs will be created to auto-renew computer certificates where possible. The only major exception is Exchange which requires subject alternative names. This will need to be manually requested and renewed as required. In either case, the default policies enabled by Windows CS is This will ensure the validity and encryption via TLS for said services within our network.

1.4.7 RADIUS AUTHENTICATION

RADIUS Authentication is required for managing network devices such as routers, switches, firewalls as well as providing authentication for WPA2 Enterprise wireless authentication and client VPN access. VLAB's choice for deploying this service will be Windows Network Policy Server (NPS) role on Windows Servers. Although FreeRADIUS is a possible alternative, Windows NPS enables seamless integration

with Active Directory. The former is well established in the industry but may be difficult to manage, configure and maintain compared to Windows NPS.

For Deployment, each site will have its own NPS server to help authenticated administrative access to network devices, access wireless networks and or authenticate client VPN access. Each site will be set up to use the HQ NPS Server in the case of service failure. Because this deployment has a Certificate Authority, the authentication method used in policies should default to PEAP-MS CHAPv2. This allows the RADIUS Client to authenticate with the RADIUS Server using a certificate and the user to authenticate with the client using their username and password. Three major policies will be created for Internal Wireless access, External Wireless Access, network device authentication including Cisco devices and FortiGate firewalls, and client VPN access.

1.5 AD USER AND GROUP CREATION STRATEGY

There are variety of ways to organize users, groups and computers within Active Directory to ensure optimal group policy object (GPO) deployment. However, we believe that the optimal organization schema used for DIC will be based primarily on roles with some exceptions. For automated user creation, a script has been created and adapted to DIC needs see User Creation Automation in the Appendix.

For user accounts, they will first be divided into either privileged users or non-privileged users. For non-privileged user accounts OUs related to roles will be organized into a root OU called Staff as shown in Figure 11. Note that IT staff also

have non-privileged accounts. These accounts will be used for accessing services like Exchange, SharePoint, and CUCM; they are not for administrative purposes. OUs for administrative accounts will be created as show in **Error! Reference source not found.** and should be used strictly for administrative purposes. These are our recommendations for OUs for administrative staff. Adjustments should be made once staffing and delegation of roles for IT has been finalized.

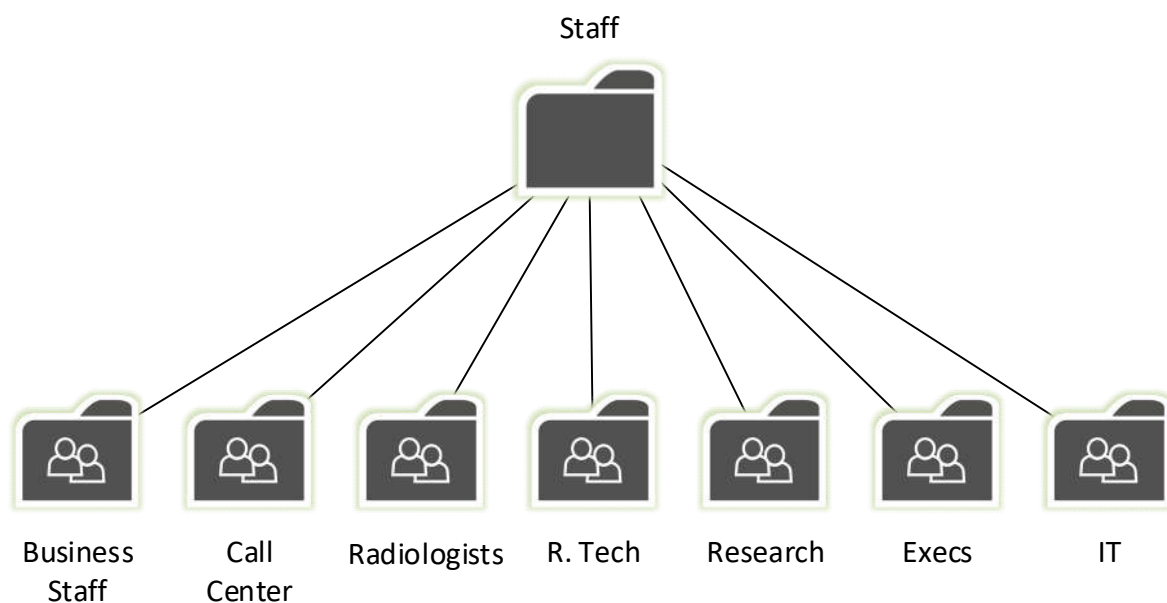


Figure 11 OU configuration for Non-Privileged User Accounts

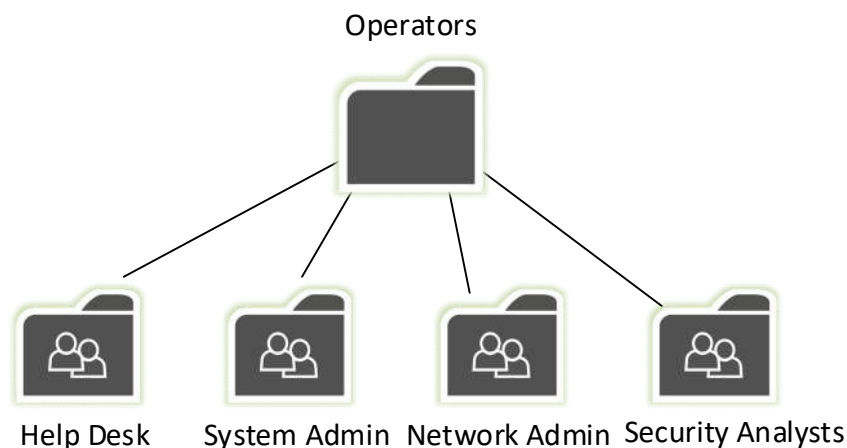


Figure 12 OU configuration for Administrative Accounts

In terms of user security groups, groups associated with the roles should also be created and placed within these OUs, along with associated users. Distribution groups should be also be created for the purpose of distributing emails efficiently to select members of users. Examples may include emails sent to Office Staff. A distribution group containing groups Business Staff, IT and Call Center could be made with an associated email address. Emails sent to that distribution group will be forwarded to every user that is part of the Office Staff group.

There are some unique root OUs for users based on the services they require. One such group be the “Remote Users” OU and group. This OU will contain users that will be permitted to work remotely using client-to-site VPNs connections enabled by FortiGate. OUs and groups to determine wireless access will also be created for the purposes of RADIUS authentication since not everyone will require wireless access. Those OUs and groups will be Internal Wireless, and External Wireless. The former will contain all groups and/or individual users that require wireless access.

The later will contain short term contractor user accounts and are only used for internet access.

For computer OUs and groups, they will be divided into the four types of Windows computers that will be deployed in the organization. Those are Servers, Laptops, Desktops and ThinClients. Computer accounts associated with these devices will be placed in their respective groups and OUs during or post deployment.

1.6 ACTIVE DIRECTORY GROUP POLICY OBJECTS DESIGN AND STRATEGY

While it is possible to manually control Windows User or computer account settings on an individual basis, it is not efficient and there can be lapses constancy. To avoid this, Group Policy Object will be deployed to manage these aspects. Furthermore, additional Administrative Template XMLs may be required to manage settings for those. In particular, the following are some subsections will describe some of the policy objects VLAB recommends implementing.

1.6.1 SOFTWARE DEPLOYMENT GPO

There are three GPO we recommend implementing. The first GPO called “COMMON-SOFTWARE” should be applied to the computer accounts. The second GPO we recommend will be called “IT-SOFTWARE” and applied to the Operator OU. The third software assignment GPO will be “THIN-SOFTWARE”.

The “COMMON-SOFTWARE” GPO should be applied to OUs for laptops and desktops and will include the assignment of commonly used software. Such software will include the assignment of Microsoft Office, end user variant of the AnyDesk,

Jabber, Chrome Web browser and Avast Business Endpoint protection. Servers should not be given these applications and therefore this GPO will not be assigned to their associated OU. This GPO should be applied to the Operator OUs. This will include common IT related software including PuTTY, administrative variant of AnyDesk, Wireshark, Avast antivirus, 7Zip, and Notepad++. Software installation files and scripts should be stored in the \\DIC\SOFTWARE\ DFS namespace to ensure optimal use of bandwidth. The “THIN-SOFTWARE” GPO should be applied to the ThinClients OU. This will assign the Horizon View Client for accessing VDI resources.

1.6.1.1 CERTIFICATE AUTO ENROLLMENT

As mentioned in other sections, this GPO with the certificate auto enrollment policy will enable automatic renewal of existing certificates and remove revoked certificates. This will ensure that that certificates within the organization remain in compliance and ensure TLS functionality were implemented. This GPO should be assigned to the Servers and Domain Controllers OUs.

1.6.1.2 ROAMING PROFILES AND FOLDER REDIRECTION

This GPO will be used to ensure consistency of user settings across machines. In our deployment, it does this by redirecting user profiles to the \\DIC\PROFILES\ DFS Namespace. Folder redirection should also be enabled for Documents and Desktop as these are likely where users are storing their documents. This GPU should be applied to the Staff OU.

1.6.1.3 ACCOUNT LOCKOUT AND DOMAIN PASSWORD POLICIES GPO

This policy should enforce account password policies as part of the Password Protection security policy. This policy will be applied on both Staff, and Operators OUs. Passwords should be changed on a quarterly basis which is 90 days. Up to 12 of the previous passwords will be remembered. Passwords must be complex meaning it must contain at least a number, special character, mix of case and not contain parts of the user's name that exceeds two characters. A minimum password day will be set to 5 days. These settings exceed Microsoft recommendations with the exception of remembered passwords ("How To Configure a Domain Password Policy," 2019).

In terms of Account Lockout, account lockout duration should be 1440 minutes, with 10 invalid login attempts and no timeout for resetting lockout based on Smith's recommendation (Smith, n.d.). If within 24 hours 10 password attempts have been made, the user is locked out until manual intervention by an administrator. If a reset lockout value has been set, then a password guessing attack could resume after the specified period. By forcing the user to communicate directly with the admin, the admin could verify the authenticity of the user.

1.6.1.4 CHROME GPO

Using ADMXs, deployment of chrome should be managed by GPOs and applied to the Staff OU. This includes setting Chrome as the default browser, prevent end-users from modifying chrome settings, homepage, managed bookmarks to intranet resources and blocking usage statistics.

1.6.1.5 PRINTER MAPPING GPO

Printer mapping GPOs should be made applied at the site OU and should be point to specific printer's physical located said site. For example, the printer mapping GPO for HQ should point the SMB printer on HQ Site. It should not be pointing to Red Deer or Iqaluit. This GPO should also be applied at the Edmonton HQ Site. Configuration of the other printers and sites should follow this pattern.

1.7 CLIENT SOLUTIONS

1.7.1 OPERATING SYSTEM: WINDOWS 10 ENTERPRISE AND UBUNTU 18.04 LTS

Most of our clients will be running Windows 10 Pro and will be enrolled and deployed via System Center Configuration Manager. Although Windows 10 Enterprise offers an abundant of enterprise features, many of those features are associated with Microsoft's own VDI solutions and are not relevant in this deployment (*Windows 10 Pro vs. Enterprise*, 2019). Conversely, Windows 10 pro offers enough level of features that are required for this deployment and has support for bit locker whereas Windows 10 home does not (*Compare Windows 10 Home vs Pro | Microsoft Windows*, n.d.). Images will be tuned for both laptops and desktops in mind. For the Linux clients in the R&I site, Desktop Ubuntu 18.04 images will be configured on SCCM as well and deployed similarly with laptops and desktops in mind. Ubuntu is recommended as a means to reduce administrative burden of dealing with multiple distinct distributions of Linux. Furthermore, Dell does offer versions of the Dell XPS with Linux pre-

installed and we can be sure that driver support in Linux is available with Dell laptop models.

1.7.2 THIN CLIENT: WYSE 5070 CELERONS

In order to save space in the call center, thin clients using VDI will be deployed rather than traditional PCs. Based on the recommendations from VMware Compatibility Guide, the thin client that will be deployed for the Call Center will be Wyse 5070 Celerons running Windows 10 Enterprise LTSC with the VMware Horizon Client installed. This model offers sufficient connectivity including monitor outputs, RJ45, and audio outputs and inputs. These systems will use built-in Windows Kiosk Mode to ensure that only Horizon View can be used by the end user. Given that the actual compute will be handled by VMWare horizon VDI infrastructure desktop pools, the processing capability does not need to be high on the thin clients.

1.7.3 LAPTOPS/DESKTOPS: DELL OPTIPLEX 5070 AND DELL VOSTRO 3490

Although there might be specific requirements for uses, it is preferable that the models deployed are standardized for ease of management, part replacement and/or device replacement. For both Laptops and Desktop deployment, our recommendation is to use the OptiPlex 5070 as our recommendation providing a 9th generation Intel I5 processor, 8GB of memory, and 256GB SSD for internal storage (*OptiPlex 5070 Commercial Tower and Small Form Factor PC | Dell USA*, n.d.). For Laptops we are recommending the Dell Vostro 3490 which features a 10th generation i5 mobile processor, 8GB of memory, 256 GB of SSD storage and a 14-inch display (*Vostro 14"*

3490 Laptop With Essential Productivity | Dell Canada, n.d.). We believe these configurations are enough in providing the desktop and laptop computing needs of the organization.

1.7.4 MOBILE DEVICES AND MDM: IPHONE AND AIRWATCH

For cellphone to be deployed we recommend going with iPhone XRs. Although not the latest phones from Apple, these devices are enough in performance and will integrate with the proposed AirWatch Mobile Device Management easily. Furthermore, Apple tends to provide support and OS updates for their devices considerably longer than compared to their Android counterparts like Samsung or Google. Google has not guaranteed support past 2019 supported the original Pixel XL despite providing OS updates (*The OG Google Pixel was left out of the November security update, 2019*). Likewise, Samsung also has 3-year life maximum for monthly security updates before shifting to quarterly security updates (*Android Security Updates Scope | Samsung Mobile Security, n.d.*). Furthermore, Samsung has left devices such the S7 release in 2016 on android version 8 (*What version of Android can I upgrade my Samsung phone to?, n.d.*). Conversely, Apple is still providing its latest IOS 13 updates to iPhone 6s and later, a phone released two years before the S7 (*Apple security updates, n.d.*). With this in mind, we believe that Apple phones to be a superior choice in ensuring extended support when compared to an Android device.

On-Premise AirWatch will be used for mobile device management. Although there are comparable alternatives such as JAMF Pro. JAMF pro is Apple specific and requires integration with Microsoft Intune for management outside of Apple's

ecosystem(*Modern Device Management*, n.d.). Whereas the current recommended deployment does not include AirWatch management of devices outside of mobile phones, AirWatch can be used to manage traditional devices such as Windows PCs, Mac computers and even Linux machines. We believe the deployment of AirWatch will give some flexibility if different operating systems will be introduced into the operating environment.

1.7.5 REMOTE DESKTOP ACCESS: REMOTE DESKTOP, ANYDESK AND SSH

For remote management of systems Windows systems VLAB suggests two options. For unattended connections to servers, we are suggesting built in Remote Desktop while using VPN to access internal networks. We believe this is enough for administrators to remotely manage servers outside of RSAT tools. For attended access for troubleshooting clients, we believe AnyDesk is an optimal choice. The criteria that VLAB had for this was real-time chat, remote control, and session recording. Although some reviews cite that AnyDesk is lacking in features, it provides all these major features that other major vendors like TeamViewer provide at a much lower cost. Team View starts with at \$49 and AnyDesk starts at \$20.99 per user (*Buy AnyDesk for your Business*, n.d.; *TeamViewer pricing*, n.d.). Furthermore, AnyDesk allows for the customization of the client. Recommended customizations include branding as well as allowing remote access only or allow remote control for end users and administrators respectively. Linux can also be managed through AnyDesk if running a GUI environment. For non-GUI environments users can access the intranet via VPN and use SSH to access the servers.

1.7.6 OFFICE PRODUCTIVITY SUITE/SOFTWARE

In terms of office suite, our recommendation is Microsoft Office 2019 which includes Word, Excel, Outlook, and PowerPoint. Because we are not using any of Microsoft's cloud subscription offerings, the most optimal edition of Microsoft office that can be acquired for windows. However, because we aren't using Office 365, we will not be able to use Microsoft's cloud versions of the office suite for Linux clients. As such, for the office suite for Linux, we are recommending LibreOffice. Although LibreOffice does not support 100% compatibility, it will allow the researchers to open the documents and do some light document creation and editing.

1.8 BACKUP SOLUTION

In terms of the software that will be used to implement the backup strategy, we will be using VEEAM. VEEAM is highly compatible with vSphere and is capable of automated backups of VMS, restoration of VMs as well as providing encryption, compression and deduplication. Furthermore, through Veeam Explorers, it can backup and restore application level objects from Microsoft Exchange, SharePoint, Microsoft SQL and Active Directory. For example, VEEAM is capable of viewing, restoring and/or exporting mailboxes and even the emails within them from Exchange backups(*Browsing, Searching and Viewing Items—Veeam Backup Explorers Guide*, 2020).

1.9 PATCH MANAGEMENT STRATEGY

Because we are employing Avast as our endpoint protection solution, its natural also to also use Avast's Business Patch Management for our windows computers. Avast Patch Management will help enable the prevention of vulnerabilities, ensure patch compliance and provide a centralized management point for patch management (*Patch Management: Automatic & Comprehensive Patching*, n.d.). Avast Business Patch management works by identifying missing patches for all systems by collecting information during scheduled scans. It then automatically determines what patches need to be acquired and deploy them. Once this is complete feedback from the deployment can be viewed from the Avast dashboard.

2 NETWORK INFRASTRUCTURE

2.1 NETWORK DESIGN

VLAB Consulting is committed to provide redundant, scalable and high-performance network solution for Digital Imaging Center. High performance should be achieved by implementing QoS, load balancing and network virtualization, where it fits best and requirement of organization. Redundancy should be implemented every part of network infrastructure such as edge network layer, core network layer, distribution layer and network virtualization. Each network layer configures with redundancy which provide consistence network connectivity if failover occur in any layer of network infrastructure. Moreover, VLAB-Consultant consider future growth of

organization when designing network solution, increment in number of users or application services should be implemented seamlessly without making drastically change in network design. Network virtualization (VMware NSX) is one of the examples of network scalability, it allows network administrator to create number of virtual network devices in matter of seconds from central management platform.

2.1.1 EDGE NETWORK LAYER

Edge network devices are entry point for any outside traffic coming inside and exit point for internal network traffic to go outside which clarify their duty as well. Edge devices like firewall or routers should log any traffic go inside to outside as well as inspect any traffic coming in from outside network. VLAB-Consultant decided to go for two internet service provider (ISP) for WAN connectivity. The primary reason behind implementation of two ISP is that if one ISP would fail to provide WAN connectivity then other ISP continue business as usual.

VLAB Consulting recommend FortiGate 1500D next generation firewalls (NGFW) for edge network layer. It should provide secure site to site connectivity by implementing full tunnel VPN. FortiGate NGFW offers built in intrusion detection and intrusion prevention features (IDS/IPS) which constantly monitoring network traffic to prevent any possible malicious activity.

FortiGate 1500D offers virtual domain (VDOM) features which allows us to distribute required ports to different domain, each domain works as separate firewall. We can create different virtual domains such as LAN1, LAN2 and DMZ as per organization

needs which extend overall network security of organization. NAT should be configured on FortiGate 1500D firewall which translate internal private IP addresses to public IP address, it should configure with NAT overload feature which allows all inside local addresses to access internet via one inside global IP address. Demilitarized zone (DMZ) is directly connected to edge network firewall which isolate DMZ traffic from internal network (Edmonton HQ), these ensure entire site network security as any traffic in and out from a DMZ must pass through FortiGate NGFW. FortiGate firewall features will be explain in detail in “firewall solution” section.

2.1.2 CORE NETWORK LAYER

Core network layer provide fast packet switching between distribution layer and edge network layer. Core network layer devices should be used to make routing decision for WAN and internet network reachability while intra-site routing should be done by distribution layer switch. We decided that filtering decision should be made by edge network devices which reduce processing power usage on core network devices, so it can make fast packet switching decision. We believe redundancy should be available on core network layer, in case of failover network should provide consistence connectivity.

We suggest that Core network layer should be configured with Cisco 4331 routers. These routers provide 4 gigabyte ethernet port, 16 GB maximum supported flash memory. This router supports redundant power supply (RPS) feature which allows uninterrupted network connectivity if power supply down. This model router supports advanced security features such as intrusion prevention system (IPS), zone-

based firewall, IPsec VPN, etc. This can be configured in future if that should be necessary.

We decided to use OSPF routing protocol for layer 3 functionality. We suggest using OSPFv2 for IPv4 address because VMware NSX edge router does not support OSPFv3, for IPv6 we suggest using OSPFv3 as NSX does not support dynamic routing for IPv6 addresses, we should talk about NSX in detail in network virtualization section.

Following are listed benefits of using OSPF as layer 3 routing functionality.

- OSPF is link state routing protocol which contain complete knowledge of entire AS system which allows them to make faster routing decision to choose secondary route if primary route facing failover.
- As OSPF is open source which allows organization to add different vendors equipment without making drastically changes in configurations.
- Concepts of ABRs (Area Borders Routers) allows routers to reduce routing information exchange between areas by sending summery address of any area. This functionality helps to save huge amount of bandwidth.
- OSPF contain smaller routing table by summarizing other areas network addresses.

2.1.3 DISTRIBUTION NETWORK LAYER

We decided to use distribution network layer devices to make intra-site routing decision and provide WAN and internet network reachability by pointing internal

network traffic to core layer devices. Inter-VLAN routing decision should be made on distribution layer switches which make network faster by dividing workload between different network layers. Redundancy should be configured on distribution layer switches for uninterrupted network connectivity.

VLAB-Consult suggest implementing Cisco 3650 series switches with 24 gigabyte ethernet ports in distribution network layer. It supports multicast routing for IPv4 and IPv6, modular QoS and enhanced security features. EtherChannel should be configure between distribution layer switches as well as access layer switches to provides fault-tolerance and high-speed links between switches.

GLBP (Gateway load balancing routing protocol) should be configure on distribution layer switches to achieve first hope redundancy for internal hosts. We suggested GLBP over other protocols because it provide load balancing for subnet traffic between active and standby gateways. OSPF can be configure for layer 3 routing decision in distribution layer devices.

2.1.4 COLLAPSED CORE LAYER

This layer contains combination of distribution and core network layers functionality in single layer. Concept behind implementation of collapsed core layer instead of core and distributed network layer is that reduce complexity where it does not necessary. This can help to reduce significate amount of cost reduction with same quality of network connectivity. Cisco 3650 series switches should be used in this layer. Figure 14 shows that how collapsed core layer make difference in network design.

2.1.5 NETWORK VIRTUALIZATION

VLAB-Consultant suggest implementing VMware NSX 6.4 for network virtualization platform to achieve datacenter East West network traffic connectivity. NSX implement network virtualization as per SDN (Software defined networking) concept where its separate control plane from data plane which makes network more agile. It provides centralized network control from single management platforms which provides better network management and traffic shaping.

First step of NSX installation is by installing NSX manager on ESXi host. Once NSX manager installed, its needs to be registered with vCenter, without registration with vCenter you should not able to implement NSX network components. NSX offers network components such as logical switches, distributed routers, edge routers, NSX controllers, etc. Distributed and standard switch can be implemented on ESXi hosts, it does not require NSX manager to be installed.

Let me explain functionality of NSX network component in bit detail. NSX logical switches should be created on the top of distributed switches, each logical switch belongs to different VXLAN which started from 5000 in NSX manager. Logical switches work as bridges to connect internal host VMs to distributed or edge router. When we are creating logical switches, it provides us two options unicast and multicast to be select, if we decided to use multicast option then we must specify multicast address range in NSX, we only able to choose unicast option if NSX controller has been installed.

NSX distributed router allows different subnets traffic to talk to each other by configuring routing protocols such as OSPF. The big difference between distributed and edge router in terms of implementation is that distributed router implementation allows network connectivity for east-west traffic on ESXi hosts while edge router allow network connectivity for east-west as well as north south traffic. It usually used to implement virtual to physical infrastructure connectivity (north-south traffic). We can also say that NSX traffic go out for internet via edge router. We suggest implementing distributed router for east-west traffic and edge router for north-south traffic for DICs server infrastructure.

NSX edge router supports dynamic routing protocols such as OSPF, BGP for IPv4 traffic, it does not support for IPv6 traffic in VMware NSX 6.4 version. It supports static route for IPv6 traffic. NSX edge should be implemented configuring with high availability, if one ESXi host down which configured with active edge configuration then other ESXi host with passive edge router should become active and provide consistence network connectivity.

2.2 NETWORK DESIGN SPECIFICATIONS ON SITE BASIS

VLAB Consulting decided to use three-layer hierarchical model for Edmonton HQ site by implementing network solution with edge, core and distribution network layer. Primary reason behind implementing three-layer model is that as site contain data center facility creates significant amount of traffics by providing services to

other sites as well as to internal departments. Figure 13 shows suggested network topology for Edmonton HQ sites.

Moreover, other 5 sites (Red Deer, Research & Innovation, Plaza, South Edmonton, West Edmonton) except Edmonton HQ suggested to use two-layer model for network solution which contain collapsed core layer and edge network layer. These sites have relatively low network traffic and mostly rely on HQ datacenter for major services. However, this can be change in future if network grows by days and required more network resources to handle additional traffics. Server and services should be varied as per site which explained in detail in Client/Server infrastructure section. Figure 14 shows suggested network solution for mentioned 5 sites.

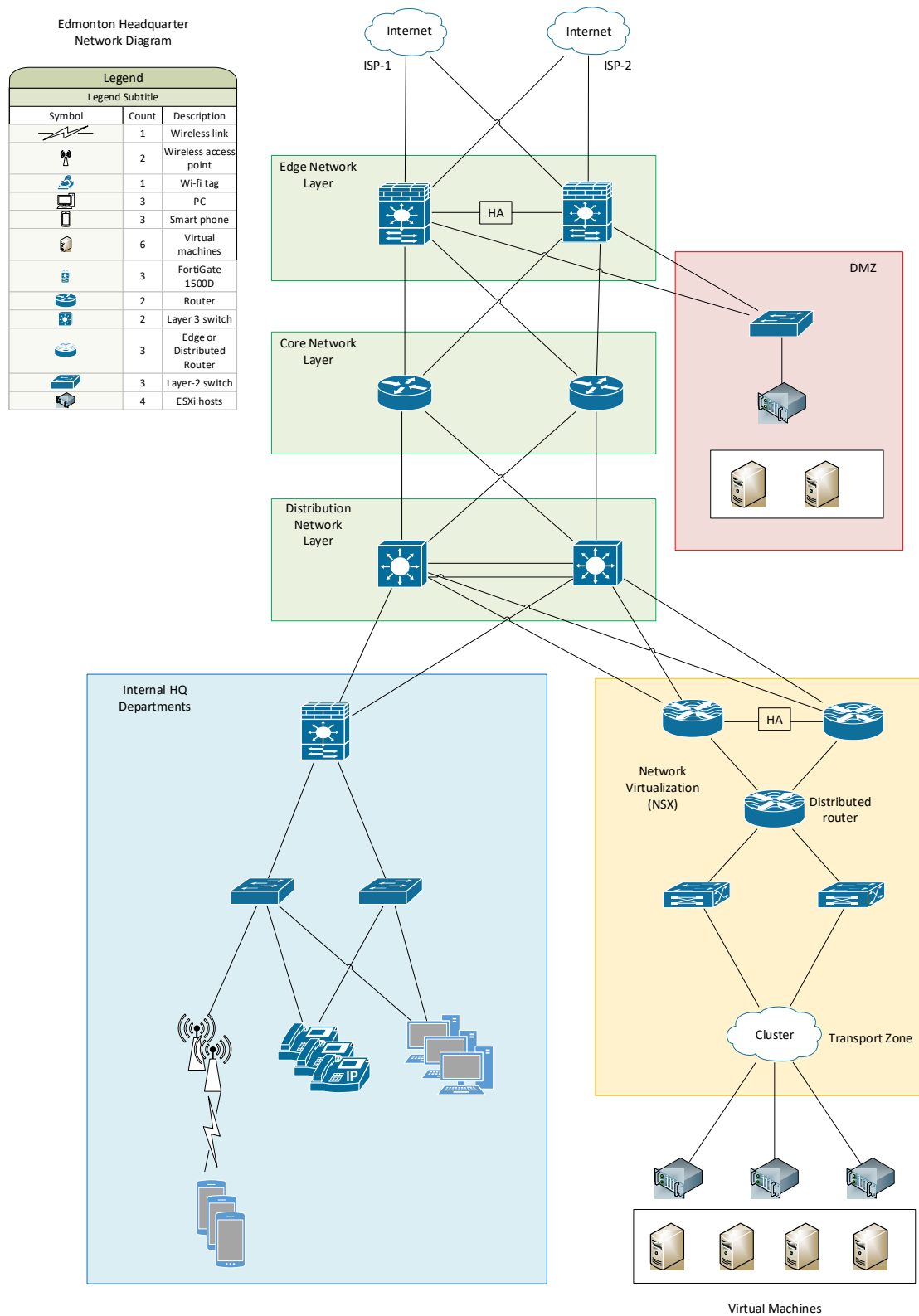














Figure 13 suggested network solution for Edmonton HQ

Legend		
Legend Subtitle		
Symbol	Count	Description
	1	Wireless links
	2	Wireless access point
	3	PC
	3	Smart phone
	4	Virtual machines
	3	FortiGate 1500D
	2	Layer 3 switch
	2	Layer-2 switch
	1	Wi-fi tag
	3	Edge or Distributed router
	2	Logical switches
	3	ESXi server

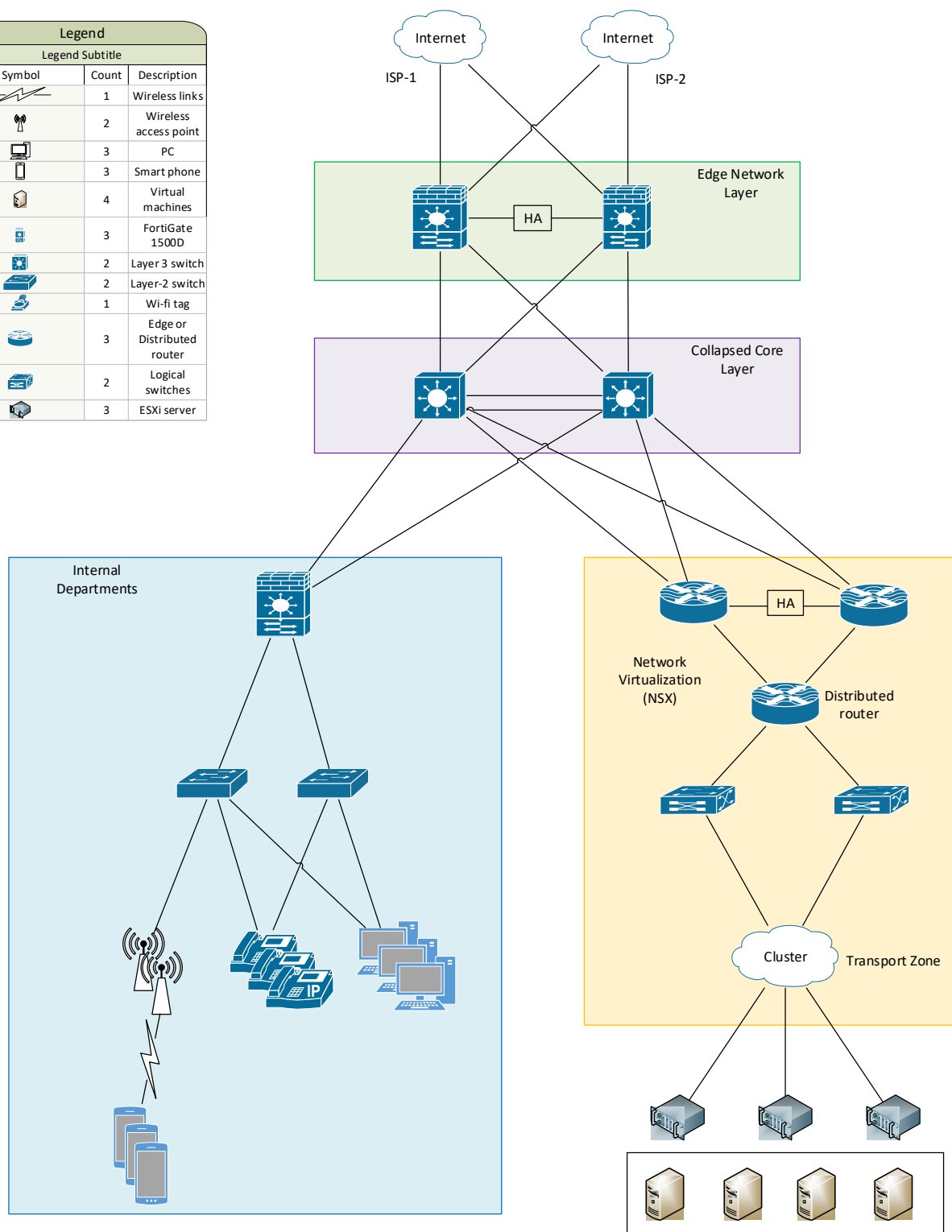


Figure 14 Suggested Network Solution for Iqaluit, Red Deer, west Edmonton, south Edmonton, R&I

2.3 INFRASTRUCTURE ADDRESSING SCHEME AND IP MANAGEMENT SOLUTION

VLAB created IP addressing scheme for both IPv4 and IPv6 addresses. Scalability and consistency are two primary concern which keep in mind during creation of IP addressing scheme. We consider simplicity in route summarization while creating IP addressing scheme, one summary route should represent entire site networks/subnets.

We choose 10.x.x.0/24 subnet for IPv4 addresses and 2020:x:x::0/64 for IPv6 addresses. In Subnet 10.x.x.0/24, first 'x' represents site number where second 'x' matches with VLAN ID. Same methods applies on IPv6 addresses which makes simplicity in IPv6 address allocation and configuration. Following are some bullet point which should keep in mind while using IP addresses.

- Default gateway should be last usable IP address of any subnet, these makes life easy of network operator while doing troubleshooting by keep in mind that there is always last usable IP as default gateway.
- IPv4 and IPv6 addresses must match with site number as well as VLAN ID to keep consistency throughout address allocations.
- Our VLAN ID allocation is like number of 10,20,30.....! for different departments throughout all six sites, these allows any department to grow with consistent allocation of IP addresses. For example, Edmonton HQ 'Executive' department have VLAN ID 10 which makes subnet 10.1.10.0/24, if

all 254 usable addresses have been used then IT department allocate 10.1.11.0/24 which ensure consistency for large number of hosts growth.

2.3.1 EDMONTON HEADQUARTER (HQ)

Table 1 Edmonton HQ IP addresses Schemes

HQ	VLAN ID	IPv4 addresses	IPv6 addresses
Executive	10	10.1.10.0/24	2020:1:10::0/64
Business Management staff	20	10.1.20.0/24	2020:1:20::0/64
General Staff	30	10.1.30.0/24	2020:1:30::0/64
Call Center	40	10.1.40.0/24	2020:1:40::0/64
Doctor (Radiologist)	50	10.1.50.0/24	2020:1:50::0/64
Radiology Tech	60	10.1.60.0/24	2020:1:60::0/64
Exam Rooms (1,4,5,6)	70	10.1.70.0/24	2020:1:70::0/64
Exam Rooms (7,8,9,10)	80	10.1.80.0/24	2020:1:80::0/64
Exam Rooms (11,12,13)	90	10.1.90.0/24	2020:1:90::0/64
Exam Rooms (14,15,16)	100	10.1.100.0/24	2020:1:100::0/64

Tech Rooms (1,2,3,4)	110	10.1.110.0/24	2020:1:110::0/64
Tech Rooms (5,6,7,8)	120	10.1.120.0/24	2020:1:120::0/64
Tech Rooms (9,10,11,12)	130	10.1.130.0/24	2020:1:130::0/64
Management VLAN	140	10.1.140.0/24	2020:1:140::0/64
Network Devices	150	10.1.150.0/24	2020:1:150::0/64
DMZ	160	10.1.160.0/24	2020:1:160::0/64
Wireless	170	10.1.170.0/24	2020:1:150::0/64
VDI VMS	254	10.1.254.0/24	2020:1:254::0/64
Servers	255	10.1.255.0/24	2020:1:255::0/64

2.3.2 IQALUIT

Table 2 Iqaluit IP addresses Schemes

Iqaluit	VLAN ID	IPv4 address	IPv6 address
Business Management Staff	10	10.2.10.0/24	2020:2:10::0/64
Radiology Tech	20	10.2.20.0/24	2020:2:20::0/64
Tech Room	30	10.2.30.0/24	2020:2:30::0/64
Exam Room	40	10.2.40.0/24	2020:2:40::0/64

Management VLAN	140	10.2.140.0/24	2020:2:140::0/64
Network Devices	150	10.2.150.0/24	2020:2:150::0/64
Servers	255	10.2.255.0/24	2020:2:255::0/64

2.3.3 EDMONTON RESEARCH & INNOVATION FACILITY

Table 3 Research & Innovation IP addresses Schemes

R&I	VLAN ID	IPv4 address	IPv6 address
Business Management Staff	10	10.3.10.0/24	2020:3:10::0/64
Researcher	20	10.3.20.0/24	2020:3:20::0/64
Management VLAN	140	10.3.140.0/24	2020:3:140::0/64
Network Devices	150	10.3.150.0/24	2020:3:150::0/64
Servers	255	10.3.255.0/24	2020:3:255::0/64

2.3.4 RED DEER

Table 4 Red Deer IP addresses Schemes

Red Deer	VLAN ID	IPv4 address	IPv6 address
Business Management Staff	10	10.4.10.0/24	2020:4:10::0/64

Doctor (Radiologist)	20	10.4.20.0/24	2020:4:20::0/64
Radiology Tech	30	10.4.30.0/24	2020:4:30::0/64
Exam Rooms (1,4,5,6)	40	10.4.40.0/24	2020:4:40::0/64
Exam Rooms (7,8,9,10)	50	10.4.50.0/24	2020:4:50::0/64
Exam Rooms (11,12,13)	60	10.4.60.0/24	2020:4:60::0/64
Exam Rooms (14,15,16)	70	10.4.70.0/24	2020:4:70::0/64
Tech Rooms (1,2,3,4)	80	10.4.80.0/24	2020:4:80::0/64
Tech Rooms (5,6,7,8)	90	10.4.90.0/24	2020:4:90::0/64
Tech Rooms (9,10,11,12)	100	10.4.100.0/24	2020:4:100::0/64
Management VLAN	140	10.4.140.0/24	2020:4:140::0/64
Network Devices	150	10.4.150.0/24	2020:4:150::0/64
Servers	255	10.4.255.0/24	2020:4:255::0/64

2.3.5 SOUTH EDMONTON

Table 5 South Edmonton IP addresses Schemes

South Edmonton	VLAN ID	IPv4 address	IPv6 address
Business Management staff	10	10.5.10.0/24	2020:5:10::0/64
Doctor (Radiologist)	20	10.5.20.0/24	2020:5:20::0/64
Radiology Tech	30	10.5.30.0/24	2020:5:30::0/64
Exam Rooms (1,4,5,6)	40	10.5.40.0/24	2020:5:40::0/64
Exam Rooms (7,8,9,10)	50	10.5.50.0/24	2020:5:50::0/64
Exam Rooms (11,12,13,14)	60	10.5.60.0/24	2020:5:60::0/64
Tech Rooms (1,2,3,4)	70	10.5.70.0/24	2020:5:70::0/64
Tech Rooms (5,6,7,8)	80	10.5.80.0/24	2020:5:80::0/64
Tech Rooms (9,10,11,12)	90	10.5.90.0/24	2020:5:90::0/64
Management VLAN	140	10.5.140.0/24	2020:5:140::0/64

Network Devices	150	10.5.150.0/24	2020:5:150::0/64
Servers	255	10.5.255.0/24	2020:5:255::0/64

2.3.6 WEST EDMONTON

Table 6 West Edmonton IP addresses Schemes

West Edmonton	VLAN ID	IPv4 address	IPv6 address
Business Management staff	10	10.6.10.0/24	2020:6:10::0/64
Doctor (Radiologist)	20	10.6.20.0/24	2020:6:20::0/64
Radiology Tech	30	10.6.30.0/24	2020:6:30::0/64
Exam Rooms (1,4,5,6)	40	10.6.40.0/25	2020:6:40::0/64
Exam Rooms (7,8,9,10)	50	10.6.50.0/26	2020:6:50::0/64
Exam Rooms (11,12,13,14)	60	10.6.60.0/27	2020:6:60::0/64
Tech Rooms (1,2,3,4)	70	10.6.70.0/28	2020:6:70::0/64
Tech Rooms (5,6,7,8)	80	10.6.80.0/29	2020:6:80::0/64

Tech Rooms (9,10,11,12)	90	10.6.90.0/30	2020:6:90::0/64
Management VLAN	140	10.6.140.0/24	2020:6:140::0/64
Network Devices	150	10.6.150.0/24	2020:6:150::0/64
Servers	255	10.6.255.0/24	2020:6:255::0/64

2.4 FULLY MANAGED NETWORK SOLUTION

VLAB Consulting choose to implement NetCrunch 10.7 as a network monitoring tool. We selected this tool because it can efficiently manage, monitor and troubleshoot entire network. following bullet point explain NetCrunch 10.7 features, benefits and capabilities when we implement for network monitoring.

- NetCrunch is very easy to install. It can be download from link provided below, once it downloaded than you can install on any supported windows operating system. NetCrunch 10.7 support 64-bit windows server (windows 2008, 2012, 2012R2, 2016). After installation, you need to provide network addresses which needs to be monitor, it can automatically start discovering devices belong to those subnets.

<https://www.adremsoft.com/demo/download-product/nctools>

- It does not need to provide additional database for monitoring data as have built-in database, automatically installed during NetCrunch installation.

During installation, we need to provide path where we want to save monitoring data. By default, it should save in C drive, we recommend providing separate SSD drive for monitoring database.

- It required less system resources, windows operating system with 2 processors and 4 GB of RAM can run NetCrunch very well. It is suggested that if using more then 1000+ nodes required to allocate additional RAM and processors.
- NetCrunch monitor Various operating system such as Windows, Mac OS X, Solaris, Linux and BDS. It supports ESXi 5.5, 6 and 6.5 as well.
- NetCrunch provides agentless monitoring system. It can collect Unix based operating system devices information by SSH, Windows by active directory credential, support all SNMP version to gather information from network devices.
- NetCrunch Provides 203 build in monitoring packs for different operating systems and Network devices such as Windows, Cisco, BDS, Solaris, etc. It allows to add more monitoring pack for specific components. NetCrunch 10.7 version introduced some new monitoring packs such as CyberPower environment packs which keep inform us to providing information from humidity and temperatures sensors, IronPort packs which can monitor system, disk and queue utilization of email security devices.
- Automatically discover present connected devices to switch and create layer 2 topology map. It should update changes on layer 2 map when new device is

added, or connection changes discovered. Figure 15 shows example of layer 2 map on NetCrunch.

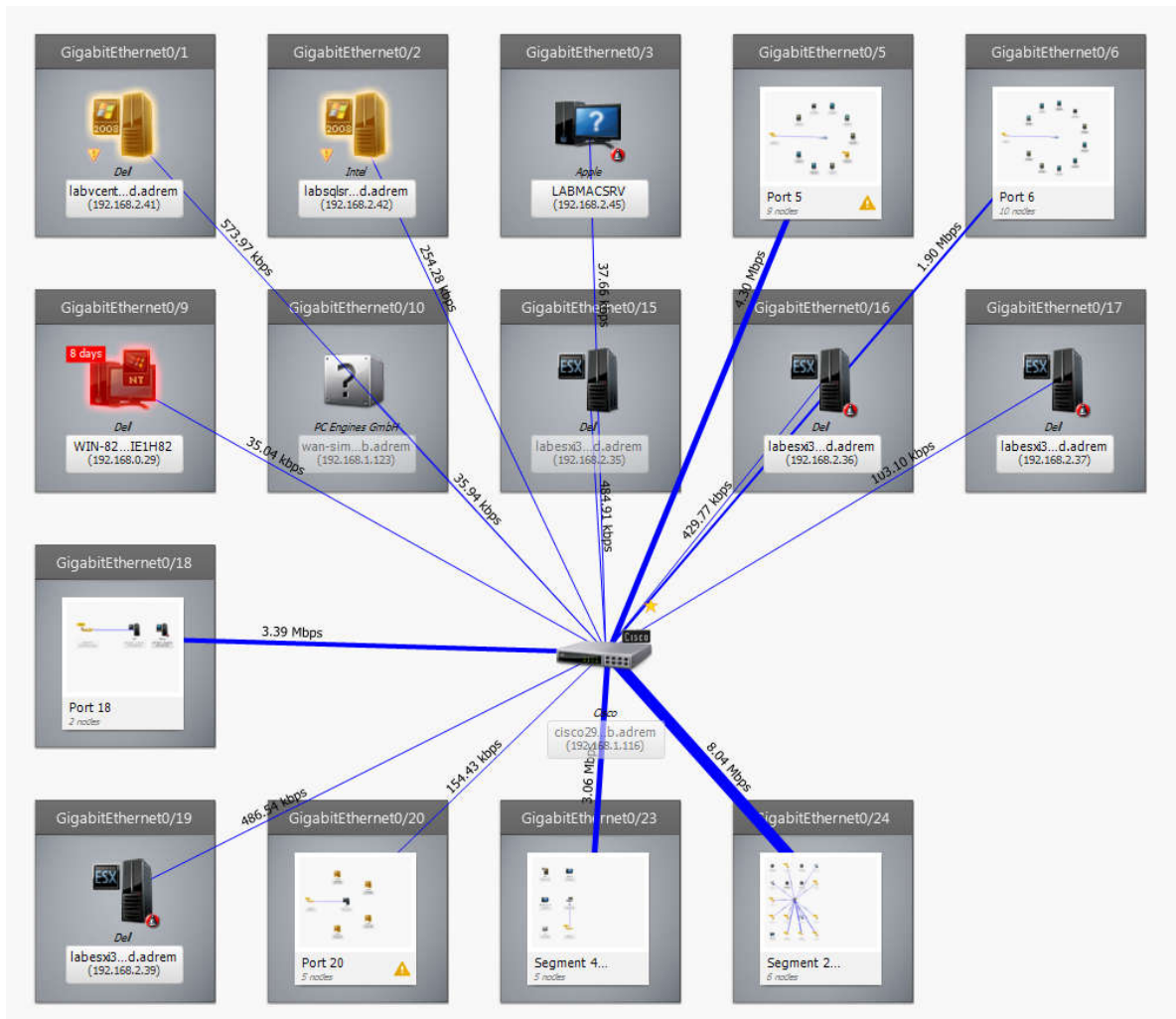


Figure 15 overview of layer 2 map on NetCrunch

- It provides customizable dashboard called 'network atlas' in NetCrunch. figure 16 shows picture shows overview of Network atlas.

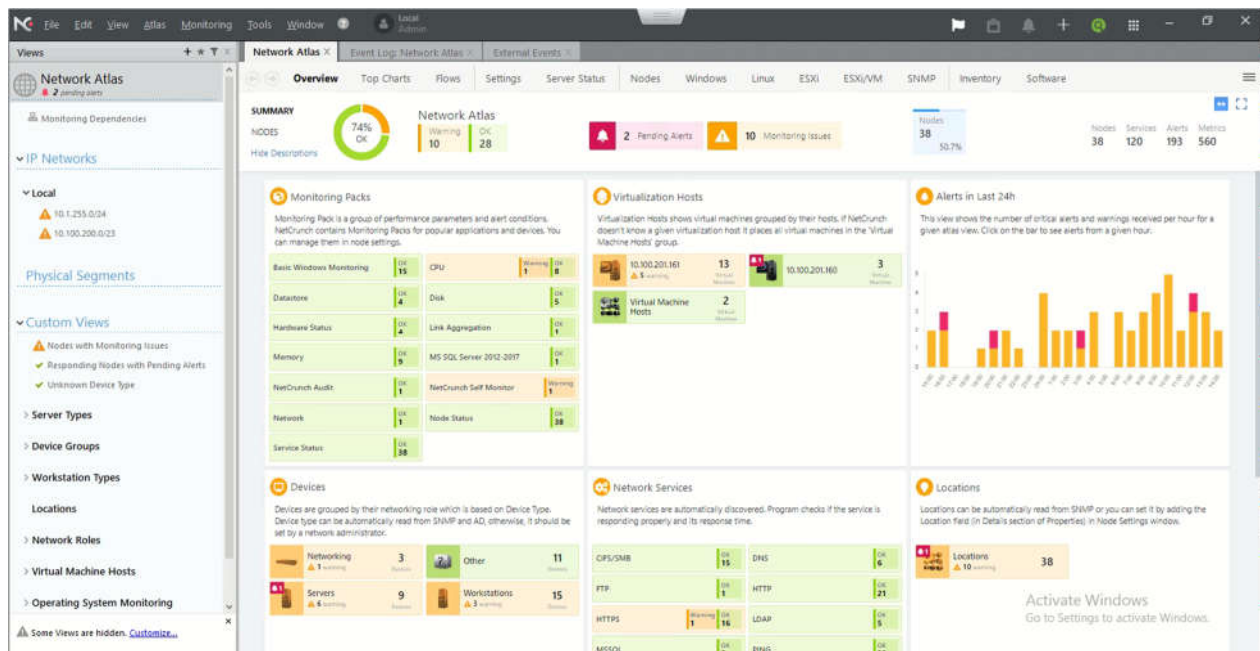


figure 16 overview of network atlas on NetCrunch

2.5 QOS IMPLEMENTATION

Quality of Service (QoS) is one of the important aspects of any organization's IT infrastructure. Implementation of QoS is important as some application are more sensitive to delays than others, application which rely on UDP traffic such as IP phone must be configured with QoS as retransmission of packet is not an option, TCP based application such as FTP have functionality to retransmit packets if its lost during transmission. VLAB-Consultant is committed to provide best user experience by implementing QoS as its best fit in DICs business.

As per a nature of DICs business, Iqaluit site does not contain any radiologist on site instead required assistance of available radiologist from Edmonton clinics over voice

or video call. Moreover, internet reachability from Iqaluit to Edmonton HQ is concerning issues because of insufficient WAN infrastructure. Network administrator should configure QoS on Iqaluit site for uninterrupted communication of voice and video call traffic all the times. Edmonton HQ site also be configured with proper QoS policies as it contains call center facilities.

One of the important aspects of DICs business is to perform medical test on patient regarding to CT scan, X-rays, MRI etc. These data must be sends in timely manner to other sites when its requested by doctors. If QoS policies not implemented for PACS/RIS traffic over WAN links that might create slowdown or lockdowns. QoS should be configure for PACS/RIS traffic over WAN links on all sites of DICs organization. Specifically, site like Iqaluit where patient records needs to be sent over WAN links on regular basis. QoS can be configure on core or collapsed network layer routers for WAN links.

3 COMMUNICATIONS INFRASTRUCTURE

3.1 EMAIL SOLUTION

On premise, we recommend Microsoft Exchange 2016 services with Database Availability Group feature, for high availability and data recovery in case of database/ network/ server failure, and an integration between Exchange and our recommended collaboration solutions, SharePoint, is possible, for ease of access. Why we recommend Microsoft Exchange is because, we are proposing Microsoft Active

Directory as DIC directory services, and compatibility wise, Exchange best suit with Microsoft Active Directory. Since we want to keep DIC patients' records private we won't be looking into cloud Office365, instead we would like to propose an integration between Microsoft Exchange and Office suite into Microsoft collaboration solution, SharePoint, so we can keep patient's records within the organization's database. Our recommendation is to place Exchange DAG in the HQ and have one Exchange server deploy on other sites, those Exchange servers in other sites will be joined to HQ's Exchange DAG, to store all Exchange data and metadata in one centralized database, it's recommended that DIC keep Exchange database centralized in one spot. Deployment of Exchange Edge server in the network perimeter is recommended; Exchange Edge provides security feature for external client's access, mail flow going out to external e-mail servers and e-mail traffic coming back into the organization from external e-mail source.

3.2 VOICE OVER IP SOLUTION

We recommend installing two Cisco CUCM servers, one being a publisher and one subscriber, and pair Cisco CUCM up with physical VoIP phones. Cisco CUCM can auto register phone numbers, associate multiple phone numbers/users to one device, synchronize with Microsoft AD list of users through LDAP, and provide DHCP server dedicated to IP phones. The two required CUCM servers will be installed on DIC's HQ, as those two servers are all DIC need to get CUCM working on all sites. CUCM

web access can be done by registered users from anywhere, anytime through HTTP/HTTPS. We also recommend using FQDN for CUCM web access instead of IP address.

3.3 CONFERENCE CALLING/ IM PRESENCE SOLUTION

We recommend using Cisco CUCM's IM and Presence Administration feature, and Cisco Jabber for instant messaging and conference calling software because: previously proposed Cisco CUCM also has the capability to manage instant messaging and conference call, using the same admin user that is used to manage VoIP phones, and on the conference calling/ IM presence software side, there is Cisco Jabber; Cisco Jabber comes with the purchase of Cisco CUCM appliance or license. We recommend using the same two CUCM servers as the VoIP solution, and Cisco Jabber can be installed in the conference room PC of each DIC's site.

3.4 COLLABORATION SOLUTIONS

We recommend using two Microsoft SharePoint 2019 servers (one server deals with AD users' access and the other one deals with SharePoint's applications), with integration of Microsoft Office suite and Microsoft Exchange. SharePoint infrastructure should be installed on top of a clustered Microsoft SQL 2016 database; this servers clustered Microsoft SQL will lay on top of Microsoft Failover Cluster iSCSI shared virtual disk. Having a clustered servers and databases will help with data redundancy, SharePoint server's role transfer and database failover, in a scenario where some circumstance forces a server or database to shut down. We recommend placing the two SharePoint servers and clustered MS SQL database in

DIC's HQ, because SharePoint has now become private to an organization, so there is no need to install SharePoint on multiple sites. Microsoft SharePoint integration with Microsoft Exchange and Microsoft Office allows DIC's users to access their mailbox and do their work using Microsoft Office, through DIC's SharePoint web page. Additionally, SharePoint Blogs and Wiki should be implemented; the purpose of Blogs would be for the sake of thoughts and knowledges sharing between internal users, and Wiki would be for knowledge base articles about DIC and their operations.

4 WEB SERVICE INFRASTRUCTURE

4.1 SECURE FTP

We recommend secure FTP using Windows Server IIS, secure SSL certificate for secure session would come from the domain Active Directory Certificate Authority. Reason why we choose Windows IIS secure FTP is because: it's Windows Server built-in, it's free, certificate can be made by AD Certificate Authority, secure FTP files' folder can be saved locally, and DIC can set access policy with their own standard. Purpose of implementing secure FTP is to have an on-premise file transfer service available to the organization's internal users from anywhere, types of files include: X-ray, CT scan, SCCM configurations, and network devices' configurations; create individual folder for types of files listed above, and restrict any unauthorized access with Windows' NTFS permission or Group Policy, domain specific SSL certificate can be used to authenticate users who want to access the FTP server. This secure FTP

server can be placed in DIC's Headquarter. Within Microsoft Server IIS management, we can set alias for secure FTP server access, e.g. what users will be typing into the search bar when they try to access DIC's secure FTP server.

4.2 CLOUD INTEGRATION AND SECURED WWW

Most of the intranet services provided will be via SharePoint, and will be secured using TLS from CA. Only internal users will have access to these resources through SharePoint connection with ADDS. It's terms of explicit cloud integrations, we are proposing the deployment of a small internet presence page to provide information on the company to the general public. This will be hosted on a HostPapa Virtual Private Server which is one of the top VPS providers for Canada (Stevens, 2020). Furthermore, Easy!Appointments will be deployed along side this presence site as an additional page. Easy!Appointments is one of the top scheduling software for customer booking of appointments(Rodriguez, n.d.). This application will enable users to quick schedule appointments in intuitive web interface. The website will be secured with a TLS certificate that will be purchased from HostPapa.

4.3 DOMAIN REGISTERING PROCESS EXPLAINED/REGISTERED DOMAIN

Domain registration will be done via GoDaddy. In terms of the name, we recommend going with DIC.ca Although not very descriptive, the using the full Diagnostics Imaging Center in the domain name is overly lengthy and less human readable. Once

the domain name has been purchased and has been registered, migration from GoDaddy DNS servers should be done and pointing towards our DMZ DNS Server.

5 SECURITY STRATEGY

5.1 SECURITY AUDIT – PROCESSES AND RESULTS

In order to assess the state of the security posture of DIC, there is need for a robust security audit. In an enterprise network like DIC that is health sector related, the security audit to be conducted will be a compliance-based security audit. There is need to ensure that the patients' confidential data is strict lockdown in accordance to PIPEDA, PIPA and other related regulations. The security audit will assess compliance and vulnerability of all systems in the company's network. This includes network vulnerabilities, application security, data encryption, controls and access.

A thorough and detailed internal security audit will be recommended. This is due to the fact the security audit process is meant to check the state of security that have just been put in place. Hence, there is need for the internal team to be trained and well abreast of the compliance requirements with respect to security posture and protocols. The following steps will be required steps to conduct a security audit (Katz, 2017):

- Define the company's audit (what should be audited and what shouldn't)
- Define the possible threats to company's assets
- Assess the current security performance of the company

- Prioritize (Risk scoring) the identified possible threats
- Formulate a list of security improvements or solutions to eliminate the threats

Some of the possible results (outcomes) of this security audit will be to provide improved security solutions to address the identified threats. Some of the security solutions can be employee security education awareness, email protection, password safety and access management, software updates and data backup but it is important to carefully review before implementing the security solutions. This conducted security audit should form the baseline and should be improved upon in subsequent audits. Rapid 7 tool will be recommended for the security audit exercise; this is because its robustness and its ability to simulate a real-life scenario attack. It can be used for vulnerability assessment, compliance testing, network, web application, social engineering, mobile application and wireless network penetration testing (*IT Security Solutions*, n.d.).

5.2 INCIDENT RESPONSE

The Incident Response Plan (IRP) for DIC will be proposed as follows (SANS Policy Team, 2014c):

5.2.1 OVERVIEW

The IRP provides the impetus for security and business teams to integrate their efforts from the perspective of awareness and communication, as well as coordinated response in times of crisis (security vulnerability identified or exploited). Specifically,

an IRP defines a product description, contact information, escalation paths, expected service level agreements (SLA), severity and impact classification, and mitigation/remediation timelines. By requiring business units to incorporate an IRP as part of their business continuity operations and as new products or services are developed and prepared for release to consumers, ensures that when an incident occurs, swift mitigation and remediation ensues.

5.2.2 PURPOSE

The purpose of this policy is to establish the requirement that all business units supported by the IT security team develop and maintain an incidence response plan. This ensures that security incident management team has all the necessary information to formulate a successful response should a specific security incident occur.

5.2.3 SCOPE

This policy applies to any established and defined business unit or entity within the DIC.

5.2.4 POLICY

The development, implementation, and execution of the IRP are the primary responsibility of the specific business unit for whom the IRP is being developed in cooperation with the IT security Team. Business units are expected to properly facilitate the IRP for applicable to the service or products they are held accountable.

The business unit security coordinator or champion is further expected to work with the IT security team in the development and maintenance of the IRP.

5.2.4.1 SERVICE OR PRODUCT DESCRIPTION

The product description in an IRP must clearly define the service or application to be deployed with additional attention to data flows, logical diagrams, architecture considered highly useful.

5.2.4.2 CONTACT INFORMATION

The IRP must include contact information for dedicated team members to be available during non-business hours should an incident occur, and escalation be required. This may be a 24/7 requirement depending on the defined business value of the service or product, coupled with the impact to customer. The IRP document must include all phone numbers and email addresses for the dedicated team member(s).

5.2.4.3 TRIAGE

The IRP must define triage steps to be coordinated with the security incident management team in a cooperative manner with the intended goal of swift security vulnerability mitigation. This step typically includes validating the reported vulnerability or compromise.

5.2.4.4 IDENTIFIED MITIGATIONS AND TESTING

The IRP must include a clearly defined process for identifying and testing of mitigations prior to deployment. These details should include both short-term mitigations as well as the remediation process.

5.2.4.5 MITIGATION AND REMEDIATION TIMELINES

The IRP must include levels of response to identified vulnerabilities that define the expected timelines for repair based on severity and impact to consumer, brand, and company. These response guidelines should be carefully mapped to level of severity determined for the reported vulnerability.

5.2.5 POLICY COMPLIANCE

5.2.5.1 COMPLIANCE MEASUREMENT

Each business unit must be able to demonstrate they have a written IRP in place, and that it is under version control and is available via the web. The policy should be reviewed annually.

5.2.5.2 EXCEPTIONS

Any exception to this policy must be approved by the IT security team in advance and have a written record.

5.2.5.3 NON-COMPLIANCE

Any business unit found to have violated (no IRP developed prior to service or product deployment) this policy may be subject to delays in service or product release until such a time as the IRP is developed and approved. Responsible parties may be subject to disciplinary action, up to and including termination of employment, should a security incident occur in the absence of an IRP

5.3 FIREWALL SOLUTION

In an enterprise environment like DIC, the nature of possible threats and attack will be diverse and complex. These threats and attacks include but not limited to advanced persistent threats, malware and several forms of zero-day exploits to name a few. Based on this, the traditional security solutions are not able to protect a modern network infrastructure designed for DIC. against modern day attacks. More importantly, DIC. will be handling patient medical records which are extremely confidential according to federal and provincial laws. Hence, the need for a multi-layer information security approach that is positioned throughout an organization's information technology (IT) infrastructure. This approach is referred to as the defense in depth approach.

The recommended security solution will be providing diverse security measures at different levels of the company's IT infrastructure. It is also on this premise that a United Threat Management (UTM) or Next Generation Firewall (NGFW) that will be able to provide an integrated diverse security solution is proposed for DIC. The diverse set of security solutions includes but not limited to Virtual Private Network (VPN), Multifactor Authentication (MFA), Intrusion Detection and Prevention System (IDS/IPS), Threat Intelligence, Web Filtering, Network AntiVirus (AV) and AntiSpam (AS). It is on this premise that a Fortigate NGFW devices are recommended for DIC. The reason for this choice is that Fortigate is one of the top three vendors of NGFW if not the top vendor of NGFW and it offers easy integration

to other products that will be used such as FortiAP, FortiAuthenticator, FortiGuard and FortiManager (*5 Top Firewall Providers for 2019*, 2019; Gartner, n.d.; Shread, 2018).

The 1500D model, as shown in Figure 17, is recommended for each site because it is a suitable NGFW for large enterprise and data center environments. It possesses eight 10 Gigabits Ethernet (GE) SFP slots and sixteen 1 GE ports. It is able to cater for the number of users available and possible growing numbers in each branch including the headquarters without compromising the security functions and quality of service. It supports 80 Gbps of firewall service, 13 Gbps of Intrusion Prevention System and 7 Gbps of NGFW services. Also, it can handle 20000 IPsec VPN tunnels at 50 Gbps, 10000 concurrent remote users for SSL VPN at 4 Gbps and SSL inspection concurrent session of 800000 at 5.7 Gbps throughput. Furthermore, it supports stateful active-active high availability configuration (Fortinet, 2020).

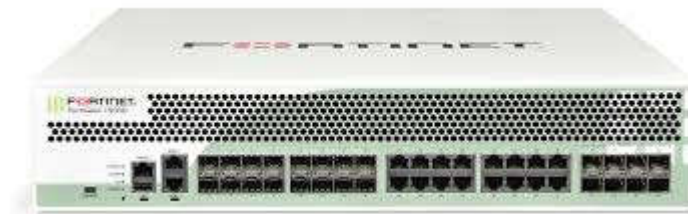


Figure 17 FortiGate NGFW 1500D Model (Fortinet, 2020)

As shown in the Figure 19, there are going to be two NGFW at the network perimeters of the headquarters and each of the branches for the purpose of redundancy, this will ensure if one NGFW goes down, the other NGFW will still be functioning before restoring the main NGFW. This will be achieved using the high availability functionality in the NGFW that is being deployed. All the services

running on one NGFW (master) including the stateful firewall will be synchronized to the backup, such that if the master goes down, the users won't experience any down time, the failing over will be seamless. These NGFWs will provide the security functionalities at the site level by ensuring any internal and external traffic are being inspected by the integrated diverse security measures and subjected to firewall policies configured on them.

Based on the defense in depth approach, beyond the network perimeter, there will be NGFW placed at the ingress/egress of each Virtual LAN (department). This will help ensure that all traffic from one VLAN or department are effectively being monitored. Furthermore, if a user in a department has been compromised, such an attack is limited to that department and not the whole site or company. Hence, such an attack can easily be contained.

Firewall policies are required to be implemented on the FortiGate NGFWs in order to restrict or allow access to network services including the internet. These firewall policies can be applied to hosts, subnets (IPv4 and IPv6) and/or user groups (created in the active directory) since the FortiGate NGFW can be integrated with the active directory. Hence, it is recommended that the most restrictive appropriate firewall policies should be implemented and applied. Below in Figure 18 is an example of a firewall policy created for internet access. Several other security features like site-to-site VPN, remote access VPN, Wi-Fi access etc. also requires firewall policies. The UTM functions like SSL inspection, web filtering, SSL inspection, antivirus and IPS are recommended to be applied to the firewall policies that are created.

Name	Internet	
Incoming Interface	lan	✕
Outgoing Interface	wan1	✕
Source	all	✕
Destination Address	all	✕
Schedule	always	▼
Services	<input checked="" type="checkbox"/> DNS ✕ <input checked="" type="checkbox"/> HTTP ✕ <input checked="" type="checkbox"/> HTTPS ✕	
Action	ACCEPT DENY	

Firewall / Network Options

NAT ☒

Fixed Port ☐

IP Pool Configuration **Use Outgoing Interface Address** Use Dynamic IP Pool

Security Profiles

AntiVirus ☐

Web Filter ☐

IPS ☐

Web Application Firewall ☐

SSL Inspection ☐

Logging Options

Log Allowed Traffic ☒ Security Events **All Sessions**

Capture Packets ☐

Comments

Enable this policy ☒

Figure 18 Firewall Policy Example (Fortinet, n.d.-g)

5.4 SITE-TO-SITE VIRTUAL PRIVATE NETWORK (VPN)

In a multisite enterprise network like that of DIC, it is very crucial to implement a site-to-site VPN among all the sites in order to ensure a secure channel of communications (tunnel) within the public internet infrastructure. More importantly, every of the patient data or other confidential data transmitted from branch to the headquarters or branch to branch needs to be highly encrypted and secured. Hence, site-to-site VPN is an important security mechanism that must be implemented.

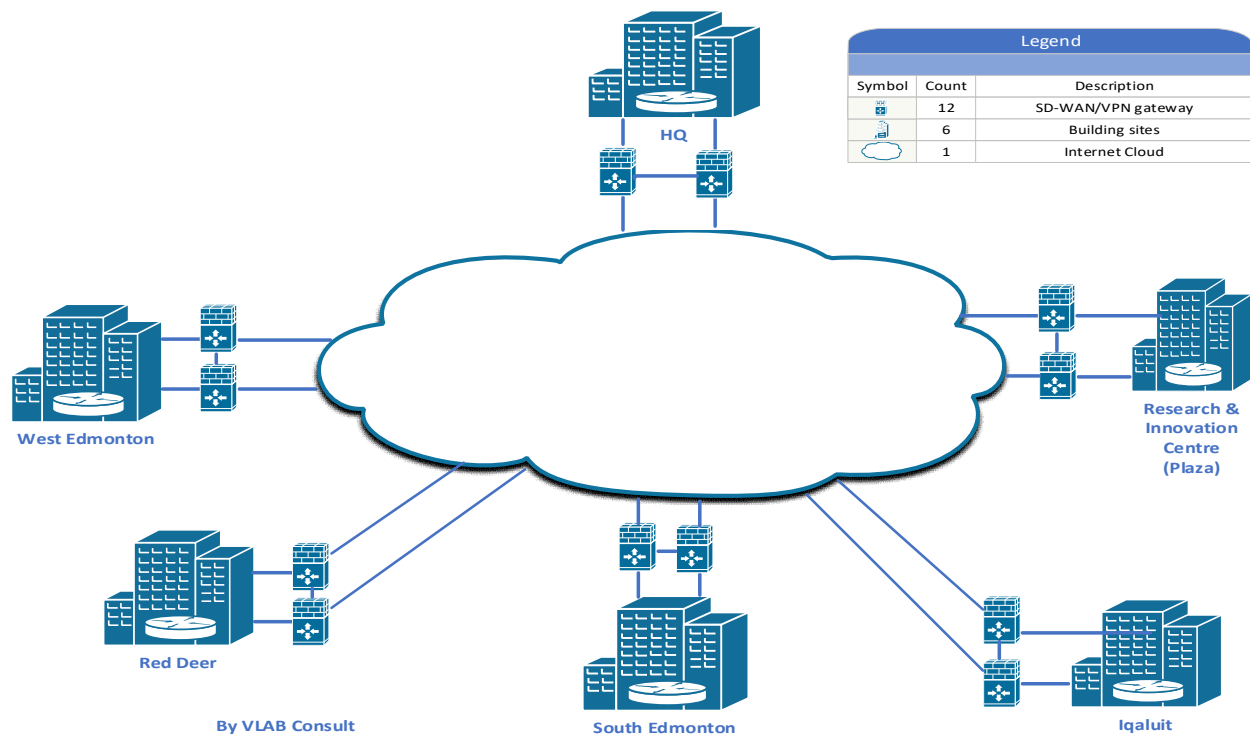


Figure 19 Inter-Site VPN Connections

Though, there are several site-to-site VPN technologies but the Internet Protocol Security (IPSec) with Internet Key Exchange version 2 (IKEv2) remains the most popularly recommended solution for site-to-site VPN due to its stability, relatively high speed and support for high level encryption, integrity and key exchange algorithms (Barker et al., 2019). In order to ensure scalability as DIC intends and is working on increasing its number of branches outside Alberta, a hub-spoke site-to-site VPN architecture that enables each branch to have a VPN connection to the headquarters (hub) is recommended rather than each site having a VPN connection to the other site (full mesh). The One Click VPN with Auto Discovery VPN shortcut will be implemented for DIC. This setup will allow primary and secondary hubs, so in case

the primary hub (headquarters) goes down, the secondary hub (Red Deer) will take over. The auto discovery VPN shortcut feature creates a shortcut for a direct spoke to spoke communications without passing through the hub once the connection is established. This ensures the benefit of a full mesh network in terms of high speed and low latency is achieved while avoiding the complexity of a full mesh architecture (Fortinet, n.d.-g). This option ensures a uniform security policy is used, high level of scalability and easier management of the site-to-site VPNs.

A VPN solution is as good as its configuration; hence, it is important that the appropriate set of algorithms are configured. As recommended by the National Institute of Standards and Technology (NIST) and in line with best practice, a minimum of Advanced Encryption Standard (AES) Galois/Counter Mode (GCM) 256 bit or fall back of AES CBC 256 bits should be used for encryption for both IKE phases. A minimum of Hash based Message Authentication Code (HMAC) SHA-256 (256 bits) is recommended for integrity algorithm while Diffie Hellman (DH) Group 19 is recommended for key exchange algorithm for both IKEv2 phases (Barker et al., 2019). Perfect Forward Secrecy (PFS) integrated with DH group ensures generated keys are never used again. For authentication, a digital certificate issued by the DIC certificate authority or 256 randomized base64 can be used a pre-shared key can be used. The site-to-site VPN will be implemented on NGFWs place at the network perimeter of each site. The UDP ports 500 and 4500 and the Encapsulation Security Payload (ESP) protocol needs to be unblocked in the firewall policy. Also, worth of

note is that the several subnets including IPv6 to an existing site-to-site VPN connection by creating more IKEv2 phase 2 connections.

5.5 SECURED SD-WAN

The Software Defined Wide Area Network (SD-WAN) is an important technology that ensures multiple WAN links to the internet or external network can be fully optimized. Also, it allows Quality of Service (QoS) for several applications including VOIP, Zoom, WebEx, office365, cloud services like AWS, Microsoft Azure and Google Cloud over the WAN links. It is designed to use several Service Level Agreements (SLAs) based on different performance metrics like packet loss, delay, jitter, throughput or hybrid of any. Specific applications of interests can be configured to use the best WAN link or a combination of WAN links (using weighting) based on set SLAs (Fortinet, n.d.-h).

The need to optimize certain traffic types which includes VOIP, Video calls or conferencing for radiologist or doctors to be able to analyze patient images cannot be overemphasized. Hence, the need for SD-WAN technology. More importantly, there is need to fully utilize the multiple ISP WAN links at all DIC sites as all sites have been recommended to use a minimum of two Internet Service providers (ISPs) to prevent any downtime in case of any lack of internet access from one of the ISPs. However, implementing SD-WAN in isolation will lead to unsecure communications over the internet. Hence, the need to not just implement SD-WAN but a secured SD-WAN solution. This can be achieved by running SD-WAN over IPSec VPN technology

and integrating it with the UTM that the NGFW is able to offer (Juniper Networks, n.d.). So, a secured SD-WAN over IPsec VPN Solution and integrated with UTM is recommended for DIC. This is one of the added reasons why IPsec VPN technology is recommended for site-to-site technology. The Secured SD-WAN solution will also be implemented on NGFW positioned on the network perimeter of each site.

5.6 MULTI-FACTOR AUTHENTICATION

Nowadays, username and password only does not suffice as a means of authentication. This is due to the fact that attackers can relatively easily crack passwords depending on the size and complexity of password used by users. Hence, it is very important that another layer(s) of security is used for authentication beyond the use of only password at DIC (Boeckl, 2016). There should be at least two pieces of evidence presented by users as a means of security enhancements in order to have access to company resources or confidential information in DIC. It is on this basis that at least a two-factor authentication is recommended for DIC., this can be achieved using token device that generates a One Time Password (OTP).



Figure 20 FortiAuthenticator(Fortinet, 2019)

The FortiAuthenticator is recommended to actualize this, it will be integrated with the active directory and the RADIUS server. The FortiAuthenticator 400E, as shown

in Figure 19, will provide a centralized user identity management and in addition works with FortiToken for up to 4000 users (Fortinet, 2019). The FortiToken can be installed from Google play and Apple store on user's phone. The Token can then be generated from user's phone. DIC users will now be required to login using username, password and token.

5.7 REMOTE ACCESS VPN

The doctor specialists' access to medical images and diagnostic related applications from home after work hours when on-call services is crucial to the business operations of DIC. Therefore, there is need for doctor specialists' to not just have remote access to the company but a secured remote access in order to protect the patient's radiological images and records. The SSL VPN is recommended as the remote access technology to be implemented by DIC. This is due to the fact that it's the most popularly recommended remote access technology and it's highly secure (Barker et al., 2019; "VPN Encryption Explained," 2019). Furthermore, it can easily be integrated with RADIUS server for the purpose of Authentication Authorization and Accounting (AAA) and allows the use of two factor authentication.

The SSL VPN will be implemented on the NGFW devices on the network perimeter of the sites. The Transport Security Layer (TLS) 1.3 is recommended which the Fortigate 1500D supports. The SSL VPN tunnel mode will be implemented rather than using an SSL VPN portal mode that makes use of web browser (HTTPS) to login. This is because by using the SSL VPN tunnel mode, the FortiClient will be used to

login and as a result this, the in-built security solutions are enforced. This in-built security solutions are Antivirus, web filtering, application firewall, vulnerability scan, compliance enforcement, two-factor authentication and anti-exploit. This in-built security features will enhance the security of the remote access as compared to connecting via a web portal. Also, as part of the implementation two-factor authentication through use of FortiToken and FortiAuthenticator will be deployed as shown in Figure 21. In addition, the existing DIC's active directory and RADIUS server will be integrated for authentication and accounting.

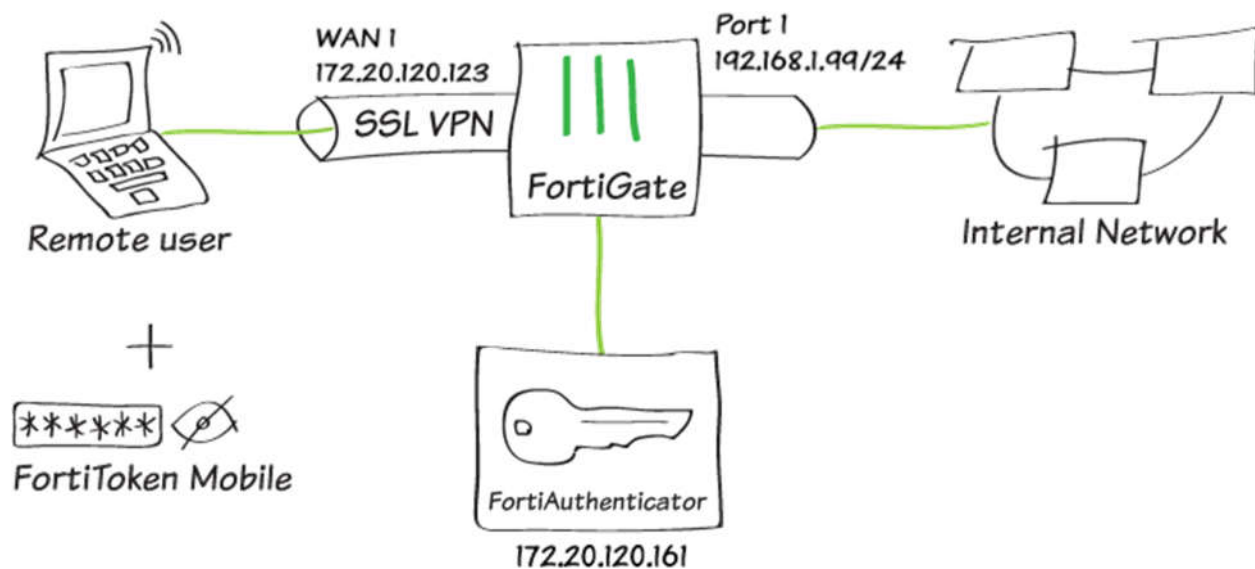


Figure 21 Remote Access VPN using MFA via FortiAuthenticator (Fortinet, n.d.-j)

Finally, the SSL VPN supports split tunneling and full tunneling. The former only routes the company's specific traffic through the SSL VPN tunnel and other traffic via the user's default gateway while, as shown in Figure 22, the latter routes all traffic including internet traffic through the SSL VPN tunnel. In order to ensure that

the security measures put in place within the company still applies to the user while connecting remotely, the full tunneling option is recommended.

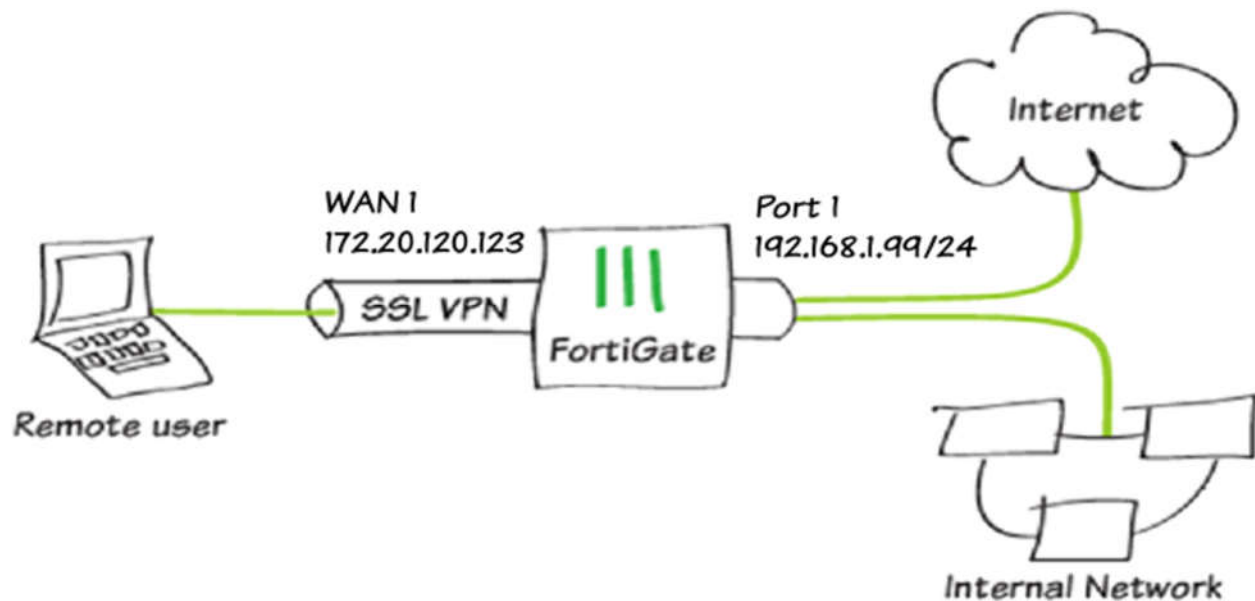


Figure 22 Remote Access using Full Tunneling (Fortinet, n.d.-i)

5.8 INTRUSION DETECTION AND PREVENTION SYSTEM

The increasing number of intrusions in current day network and the need to detect these different forms of cyberattacks before they happen can't be overemphasized. Enterprises like DIC need to defend its network against these everyday cyberattacks and even target attacks. Hence, the need for a Next Generation IPS (NGIPS) that will not only detect these attacks but also prevent them from compromising the company's network. It is on this premise that a NGIPS is recommended for DIC that will be deployed inline as a bump (Fortinet, n.d.-c) in the wire on the NGFWs at the network perimeter and at the ingress/egress of each VLANs or departments within

the company. The deployed NGIPS is expected to perform speedy deep packet inspection in order to detect and prevent any form of cyberattacks including the sophisticated ones without compromising the throughput. The protection provided by the Fortinet NGIPS is signature-based like Snort with robust set of rules and signatures. Furthermore, the NGIPS has been tested by the NSS Labs against different forms of known and unknown cyberattacks in order to guarantee high level performance and minimal false alarms (Williams & Wheeler, 2019).

5.9 THREAT INTELLIGENCE

The rapid growth of the threat landscape on a daily basis is becoming unprecedented and the need to leverage on artificial intelligence and machine learning that is able to analyze hundreds of millions of security events across the globe in order to protect the enterprise network from this evolving threat landscape becomes crucial especially for a company like DIC dealing with several confidential data. It is on this premise that such a threat intelligence like FortiGuard is recommended to DIC. This is due to the fact that the FortiGuard threat intelligence partners with two hundred other cybersecurity intelligence and it ensures up to the minute intelligence in real time to stop latest threats via automated and advanced analytics (Fortinet, n.d.-e). This will be deployed on the NGFWs at the network perimeter and at the ingress/egress of each VLANs or departments within the company. The implementation of this will help enhance the NGIPS as well.

5.10 WEB, CONTENT AND DNS FILTERING

Several employees at DIC as any other company will be browsing web during their stay in the company and access to malicious websites is a major vector to initiate attacks or trigger the downloads of malware, spyware and other form of risky contents. Therefore, there is need to provide adequate security measure against web-based attacks and the first line of defense against such attack is web filtering (Fortinet, n.d.-k). In essence, there is serious need to implement a web filtering solution at DIC to prevent users from any form of malicious websites. The DNS filtering is also recommended in order to inspect all DNS requests and based on the FortiGuard domain rating, blocks malicious DNS requests or allow legitimate requests. In order to implement this, the internal DNS servers must be pointing to the FortiGuard DNS servers. Hence, the web and DNS filtering services via the FortiGuard should be enabled and appropriately configured on all the NGFWs at the network perimeter and at the ingress/egress of each VLANs or departments within the company. This choice has been opted for because the FortiGuard web and DNS filtering service is able to prevent 97.7% of direct malware download (Fortinet, n.d.-k). It is worth noting that there is need for continuous tuning of the web filtering in order to achieve desired result.

5.11 SSL INSPECTION

Several communications between client and server are now been encrypted using SSL encryption. This includes web, email and FTP traffic. They mainly use HTTPS, IMAPS, POP3S, SMTPS and FTPS. This ensures security and its good for the

company, however, attackers exploit this encryption mechanism to encrypt the malware they will be using for attack (Peter, 2019). Hence, the need for deep inspection of encrypted traffic especially in an enterprise network like that of DIC with highly sensitive data. This is actualized by intercepting the traffic (web, email, FTP and SSH) between the client and server then decrypts the encrypted traffic, scan it, then encrypt and send to the destination. In order to implement this, the SSL inspection must be enabled and configured on all the NGFWs at the network perimeter and at the ingress/egress of each VLANs or departments within the company.

It is worth noting that there is need to use the certificate issued by the company's certificate authority and this certificate should be pushed to the web browser of the clients in order for the web browser to be trust the NGFWs. Also, that some websites will not allow such interceptions, so in order to overcome this, this website must be exempted from SSL inspection.

5.12 NETWORK ANTIMALWARE (ANTIVIRUS & ANTISPYWARE)

Malware are been used by hackers to cause data breaches, expose intellectual property and cause disrupt business operations. They cause damages to the network, servers and hosts, and generally consist of different varieties, this include virus, worm, trojan horses and ransomware. DIC cannot afford to suffer from any data breach or disruption of business operations, hence, the need for preventive measures to stop malware starting from the network level. It is on this basis, that a FortiGuard Antivirus service is recommended to be enabled and configured on all the NGFWs at

the network perimeter and at the ingress/egress of each VLANs or departments within the company. The reason for this choice is that it protects the network against latest viruses, worms and content-level threats. It uses the industry-leading advanced detection engines to actualize this. This choice is further corroborated by the selection as the security industry's second-best business antivirus solution for security effectiveness and award of advanced+ (highest award) for file detection and real-world protection. Also, because at every minute of every day the FortiGuard Labs neutralizes about 95000 malwares on mobile, traditional network and IoT platforms.

5.13 MICROSEGMENTATION

Recent studies show that there have been several sophisticated attacks breaching the network perimeter and other studies show that often than none, these breaches are as a result of internal negligence from one of the employees. If and when such breach occurs, there is need to limit the impact of such breach to a very small segment of the network. An enterprise network such as that of DIC needs to further segregate or segment the network into subnets or zones not only for management purpose but also security purpose. Therefore, there is need for network segmentation or microsegmentation to be applied to DIC from a security architecture point of view. This concept allows the division of the bigger enterprise network into subnets or zones (Paloalto, n.d.). The concept of microsegmentation can also be extended to the virtualization environment. This is also done by creating zones in the data center environment in order to isolates different workloads or VMs. Since, private data centers will be implemented where virtual servers will be running from through the

means of VMware technology, there is need for microsegmentation in the virtualization environment as well. The implementation of this at DIC will help enhance the level of defense in depth and zero trust compliance.

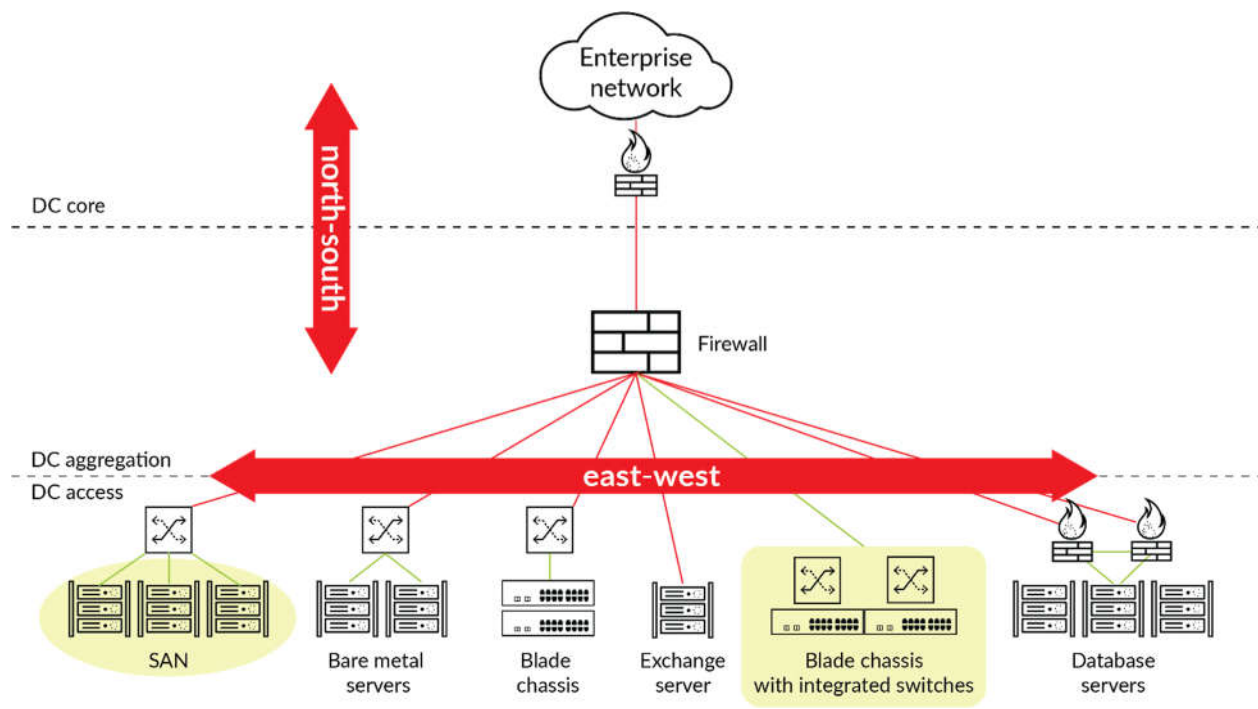


Figure 23 Microsegmentation for east-west traffic (Paloalto, n.d.)

So beyond the network perimeter NGFWs (Fortigate 1500D) taking care of north south network traffic visibility, there is need to have NGFWs at the ingress/egress of each zone, subnet, VLAN or department in order to have network visibility and apply appropriate security policies for east west traffic (within the company) as shown in Figure 23. This can be achieved by placing multiple NGFWs for small medium enterprise or using the virtual instances (virtual domain - VDOM) of large enterprise NGFW like 1500D model for each of the VLANs or departments for the physical network. For the virtual environment, in addition to the Distributed Firewall (DFW)

that the NSX manager of the VMware offers, the Fortigate-VM security solution (node) will be deployed (Fortinet, n.d.-d). This joint solution ensures zero trust security across all the hypervisors deployed at DIC and advanced Layer 7 security (VMware, 2017). It will ensure a policy-based firewall is applied to all the east-west traffic in the data center to be implemented at DIC.

5.14 HOST-BASED SECURITY

Beyond the network and subnetwork security measures, there is need for an additional layer of security for each host or endpoint including the servers and clients in order to have a very strong security posture that an enterprise like DIC should have. This will help guarantee high level of privacy and security as a whole. This host-based security should include but not limited to firewall, IPS and antimalware. This helps provide personal perimeter security posture. There are often two means of deploying host-based security in an enterprise environment, its either as a standalone or agent-based (Lowder, 2019). The latter will be recommended for DIC, this is due to the fact that it can easily be managed from a centralized management console and a uniform security policy can be implemented across all endpoints in the network. There are several vendors providing agent-based endpoint protection system, however, the on-premise version of the Avast Business Pro Plus endpoint protection will be recommended. This is due to that is rated as one of the top if not top endpoint protection system (Witts, 2020). Also, beyond host firewall, antimalware and compliance check, it also provides patch management that ensures all endpoints are up to date with respecting to patching and these patches can be installed from the

centralized management console (Avast, n.d.). Furthermore, it offers identity theft protection, sandbox, Wi-Fi inspector and webcam shield.

5.15 DEVICE HARDENING

The need for network devices just as the host to be secured or hardened can't be overemphasized as these set of devices are responsible for transporting data generated from the hosts from one point to the other. The DIC can't afford any network device's compromise, hence, several network device hardening will be put in place as detailed in the network infrastructure section. This includes the usage of RADIUS (AAA) for all logins in order to ensure proper authentication, authorization and accounting. Also, the usage of type 9 encryption (scrypt) for all local passwords and only SSH for remote administration of devices. In addition, the routing protocols and all other protocols will be making use of the best authentication method to exchange and validate updates among the devices. Furthermore, root guard, BPDU guard, port security, DHCP snooping, IP source guard, shutdown of unused ports and assigning such ports to a specific VLANs will be deployed on all the switches in order to ensure secured network. There will also be a security policy to enforce this.

5.16 SECURITY INFORMATION AND EVENT MANAGEMENT

The need for a log management in an enterprise like DIC is very important in order to keep logs of several events happening within the enterprise network (on both the network devices and the servers), hence, the talk of a syslog server (traditional log management tool). However, there is need for a more sophisticated solution that will

not only offer log management but also collection of non-event-driven data such as vulnerability assessment report as well as perform data correlation, real time analysis of the correlated data (analytics) and alert correlation (Shipley, 2008). Hence, the need for Security Information and Event Management (SIEM) solution for DIC. The SIEM solution will provide a combination of log management, analysis and monitoring. It is on this premise that the Splunk Enterprise Security SIEM solution is recommended. This is because beyond the fact that it can perform real-time security monitoring, advanced threat detection, incident investigation and forensics, incident response, Security Operations Center (SOC) automation and a wide range of security analytics, it is also rated as the best SIEM solution out there (Splunk, n.d., 2020). The usage of syslog-ng on the data sources platform will help filter unimportant log messages and ensures those messages are transported in an encrypted form to the SIEM solution, hence it is recommended that syslog-ng be integrated to the Splunk SIEM solution in order to improve its performance. The SIEM solution will be placed at the research and innovation center and all the data sources will be configured appropriately.

5.17 DATA BACKUP STRATEGY

After the identification of all the data sources that need to back up, there is need for a strategy towards the backing up of these set of data. There are several backup options that can be used. The adopted backup options (backup repositories) will vary from data to data. The sensitivity and impact of the data will determine the backup options to be used.

A robust backup, replication and recovery solution like Veeam availability suite is recommended which details have been provided under server section. This solution has been selected because of its ability to perform reliable backup, fast recovery, secure replication, smart storage, data reuse and cloud portability. This backup solution also ensures adequate encryption of data in flight and data at rest. It should also be able to work with different backup repository solutions. The backup options for DIC will include a minimum of the following:

- Backing up data from varying data sources through the backup and replication solution to the tape, large capacity USB and SSD drives
- Backing up data from varying data sources through the backup and replication solution to an onsite secure FTP server
- Backing up data from varying data sources through the backup and replication solution to on-site SAN (where applicable) and off-site SAN solution
- Backing up asset (data, software or applications) from varying data sources through the backup and replication solution to the cloud platform

All data must be encrypted using a minimum of 256 bits Advanced Encryption Standard (AES) and due to privacy issues, highly confidential and confidential categorized sensitive data can't be backup into the cloud. Each data source should have at least one on-site and one off-site backup repositories. All physical backup must be well secured in CISA physical access security standards. The scheduling

frequency and priority of data backup will be based on the Recovery Time Objective (RTO) and Recovery Point Objective (RPO) metrics. There should be confirmation of successful backup at regular intervals.

5.18 IT SECURITY POLICIES

5.18.1 PASSWORD PROTECTION POLICY

The Password protection policy for DIC will be proposed as follows (SANS Policy Team, 2017):

5.18.1.1 OVERVIEW

Passwords are an important aspect of computer security. A poorly chosen password may result in unauthorized access and/or exploitation of our resources. All staff, including contractors and vendors with access to DIC systems, are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

5.18.1.2 PURPOSE

The purpose of this policy is to establish a standard for creation of strong passwords and the protection of those passwords.

5.18.1.3 SCOPE

The scope of this policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any DIC facility, has access to the DIC network, or stores any non-public DIC information.

5.18.1.4 POLICY

1.0 Password Creation

1.1 All user-level and system-level passwords must conform to the Password Construction Guidelines.

1.2 Users must use a separate, unique password for each of their work-related accounts. Users may not use any work-related passwords for their own, personal accounts.

1.3 User accounts that have system-level privileges granted through group memberships or programs such as “sudo” must have a unique password from all other accounts held by that user to access system-level privileges. In addition, it is highly recommended that some form of multi-factor authentication is used for any privileged accounts

2 Password Change

2.1 Passwords should be changed only when there is reason to believe a password has been compromised.

2.2 Password cracking or guessing may be performed on a periodic or random basis by the IT security Team or its delegates. If a password is guessed or cracked during one of these scans, the user will be required to change it to be in compliance with the Password Construction Guidelines.

5.18.1.5 PASSWORD PROTECTION

1 Passwords must not be shared with anyone, including supervisors and coworkers. All passwords are to be treated as sensitive, Confidential DIC information. Corporate Information Security recognizes that legacy applications do not support proxy systems in place. Please refer to the technical reference for additional details.

2 Passwords must not be inserted into email messages, Alliance cases or other forms of electronic communication, nor revealed over the phone to anyone.

3 Passwords may be stored only in “password managers” authorized by the organization.

4 Do not use the "Remember Password" feature of applications (for example, web browsers).

5 Any user suspecting that his/her password may have been compromised must report the incident and change all passwords.

5.18.1.6 APPLICATION DEVELOPMENT

Application developers must ensure that their programs contain the following security precautions:

1. Applications must support authentication of individual users, not groups.

2.Applications must not store passwords in clear text or in any easily reversible form.

3 Applications must not transmit passwords in clear text over the network.

4 Applications must provide for some sort of role management, such that one user can take over the functions of another without having to know the other's password.

5 Multi-Factor Authentication

5.1 Multi-factor authentication is highly encouraged and should be used whenever possible, not only for work related accounts but personal accounts also.

5.18.1.7 POLICY COMPLIANCE

1 Compliance Measurement

The IT security team will verify compliance to this policy through various methods, including but not limited to, periodic walk-throughs, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

2 Exceptions

Any exception to the policy must be approved by the IT security Team in advance.

3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5.18.1.8 RELATED STANDARDS, POLICIES AND PROCESSES

- Password Construction Guidelines

5.18.2 HARDWARE DISPOSAL POLICY

The hardware disposal policy for DIC will be proposed as follows (SANS Policy Team, 2014b):

5.18.2.1 OVERVIEW

Several hardware often contains parts which cannot simply be thrown away. Proper disposal of hardware is both environmentally responsible and often required by law. In addition, hard drives, USB drives, CD-ROMs and other storage media contain various kinds of DIC's data, some of which is considered sensitive. In order to protect our constituent's data, all storage mediums must be properly erased before being disposed of. However, simply deleting or even formatting data is not considered sufficient. When deleting files or formatting a device, data is marked for deletion, but is still accessible until being overwritten by a new file. Therefore, special tools must be used to securely erase data prior to equipment disposal.

5.18.2.2 PURPOSE

The purpose of this policy is to define the guidelines for the disposal of hardware and related components owned by DIC.

5.18.2.3 SCOPE

This policy applies to any computer/technology hardware or peripheral devices that are no longer needed within DIC including, but not limited to the following: personal computers, servers, hard drives, laptops, mainframes, smart phones, or handheld computers (i.e., Windows Mobile, iOS or Android-based devices), peripherals (i.e., keyboards, mice, speakers), printers, scanners, typewriters, compact and floppy discs, portable storage devices (i.e., USB drives), backup tapes, printed materials.

All DIC employees and affiliates must comply with this policy.

5.18.2.4 POLICY

1.0 Hardware Disposal

1.1 When Technology assets have reached the end of their useful life, they should be sent to the Hardware Disposal Team (HDT) office for proper disposal.

1.2 The HDT will securely erase all storage mediums in accordance with current industry best practices.

1.3 All data including, all files and licensed software shall be removed from hardware using disk sanitizing software that cleans the media overwriting each and every disk sector of the machine with zero-filled blocks, meeting appropriate standards.

1.4 No computer or technology hardware may be sold to any individual other than through the processes identified in this policy (Section 4.2 below).

1.5 No hardware should be disposed of via skips, dumps, landfill etc. Electronic recycling bins may be periodically placed in locations around DIC. These can be used to dispose of hardware. The HDT will properly remove all data prior to final disposal.

1.6 All electronic drives must be degaussed or overwritten with a commercially available disk cleaning program. Hard drives may also be removed and rendered unreadable (drilling, crushing or other demolition methods).

1.7 Hardware refers to desktop, laptop, tablet or netbook computers, printers, copiers, monitors, servers, handheld devices, telephones, cell phones, disc drives or any storage device, network switches, routers, wireless access points, batteries, backup tapes, etc.

1.8 The HDT will place a sticker on the equipment case indicating the disk wipe has been performed. The sticker will include the date and the initials of the technician who performed the disk wipe.

1.9 Hardware with non-functioning memory or storage technology will have the memory or storage device removed and it will be physically destroyed.

2 Employee Purchase of Disposed Hardware

2.1 Hardware, which is working, but reached the end of its useful life to DIC, will be made available for purchase by employees.

2.2 The opportunity to purchase available hardware will be open to all employees.

2.3 All hardware purchases must go through the due process. Employees cannot purchase their office computer directly or “reserve” a system. This ensures that all employees have an equal chance of obtaining equipment.

2.4 Finance and Information Technology will determine an appropriate cost for each item.

2.5 All purchases are final. No warranty or support will be provided with any hardware sold.

2.6 Any unsold hardware or hardware not in working order will be donated or disposed of according to current environmental guidelines.

2.7 Technology has contracted with several organizations to donate or properly dispose of outdated technology assets.

2.8 Prior to leaving DIC’s premises, all equipment must be removed from the Information Technology inventory system.

5.18.2.5 POLICY COMPLIANCE

1 Compliance Measurement

The IT or IT security team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

2 Exceptions

Any exception to the policy must be approved by the IT security Team in advance.

3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5.18.2.6 RELATED STANDARDS, POLICIES AND PROCESSES

None.

5.18.3 ROUTER AND SWITCH SECURITY POLICY

The router and switch security policy for DIC will be proposed as follows (SANS Policy Team, 2014a):

5.18.3.1 OVERVIEW

Network devices security are an important aspect of enterprise security. A poorly configured network device with respect to security may result in unauthorized access and/or exploitation of our resources. All staff, including contractors and vendors with access to DIC network devices, are responsible for taking the appropriate steps, as outlined below, to ensure the minimal security configuration is adhered to.

5.18.3.2 PURPOSE

This document describes a required minimal security configuration for all routers and switches connecting to a production network or used in a production capacity at or on behalf of DIC.

5.18.3.3 SCOPE

All employees, contractors, consultants, temporary and other workers at DIC and its subsidiaries must adhere to this policy. All routers and switches connected to DIC production networks are affected.

5.18.3.4 POLICY

Every router must meet the following configuration standards:

1. No local user accounts are configured on the router. Routers and switches must use RADIUS for all user authentication.
2. The enable password on the router or switch must be kept in a secure encrypted form. The router or switch must have the enable password set to the current production router/switch password from the device's support company.
3. The following services or features must be disabled:
 - a. IP directed broadcasts
 - b. Incoming packets at the router/switch sourced with invalid addresses such as RFC1918 addresses
 - c. TCP small services

- d. UDP small services
 - e. All source routing and switching
 - f. All web services running on router
 - g. DIC's discovery protocol on Internet connected interfaces
 - h. Telnet, FTP, and HTTP services
 - i. Auto-configuration
4. The following services should be disabled unless a business justification is provided:
- a. DIC's discovery protocol and other discovery protocols
 - b. Dynamic trunking
 - c. Scripting environments, such as the TCL shell
5. The following services must be configured:
- a. Password-encryption
 - b. NTP configured to a corporate standard source
6. All routing updates shall be done using secure routing updates.
7. Use corporate standardized SNMP community strings. Default strings, such as public or private must be removed. SNMP must be configured to use

the most secure version of the protocol allowed for by the combination of the device and management systems.

8. Access control lists must be used to limit the source and type of traffic that can terminate on the device itself.

9. Access control lists for transiting the device are to be added as business needs arise.

10. The router must be included in the corporate enterprise management system with a designated point of contact.

11. Each router must have the following statement presented for all forms of login whether remote or local:

"UNAUTHORIZED ACCESS TO THIS NETWORK DEVICE IS PROHIBITED. You must have explicit permission to access or configure this device. All activities performed on this device may be logged, and violations of this policy may result in disciplinary action and may be reported to law enforcement. There is no right to privacy on this device. Use of this system shall constitute consent to monitoring."

12. Telnet may never be used across any network to manage a router, unless there is a secure tunnel protecting the entire communication path. SSH version 2 is the preferred management protocol.

13. Dynamic routing protocols must use authentication in routing updates sent to neighbors. Password hashing for the authentication string must be enabled when supported.

14. The corporate router configuration standard will define the category of sensitive routing and switching devices, and require additional services or configuration on sensitive devices including:

- a. IP access list accounting
- b. Device logging
- c. Incoming packets at the router sourced with invalid addresses, such as RFC1918 addresses, or those that could be used to spoof network traffic shall be dropped
- d. Router console and modem access must be restricted by additional security controls

5.18.3.5 POLICY COMPLIANCE

1 Compliance Measurement

The IT security team will verify compliance to this policy through various methods, including but not limited to, periodic walk-throughs, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

2 Exceptions

Any exception to the policy must be approved by the IT security team in advance.

3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5.18.3.6 Related Standards, Policies and Processes

None.

6 WIRELESS INFRASTRUCTURE

The employees' need to roam around with their laptop and mobile devices (tablets and mobile phones), and still have access to company resources and internet access makes a wireless infrastructure a necessity within the company's premise. There is need for effective wireless network planning in order to know the number of access points (APs) required and their respective locations in all the sites. Since the FortiGate NGFWs that will be deployed has an in-built Wireless LAN Controllers (WLC) that can be used to centrally manage all the access points, then the FortiAPs will be recommended. A FAP-421E model is recommended due to the fact that its designed for high density and provides high performance. In addition, it has a 4 x 4 multiple antenna and can support 1.3 Gbps throughput (Fortinet, n.d.-a). Furthermore, the NGIPS, web filtering, DNS filtering and antivirus can be applied

to the Wi-Fi access. Upon installation of the determined number of FortiAPs at appropriate locations across all the sites, the FortiAPs will be configured via the WLCs. Also, for a good security posture, there is need to separate the wireless access given to the employees (internal), partners (external) and guests. The access to the latter should be adequately restrictive.



Figure 24 FortiAP 421E Model (Fortinet, n.d.-a)

6.1 INTERNAL

This wireless setup will be for the employees. A separate Service Set Identifier (SSID) will be created for this setup on the FortiGate NGFW that the FortiAPs will be connecting to. A Wi-Fi Protected Access III (WPA3) Enterprise authentication method verified by a RADIUS server is recommended (Fortinet, n.d.-f). This authentication method has been chosen because of its robustness for enterprise level security and the fact that it uses AES-256 in GCM mode with SHA-384 as HMAC. An appropriate security policy will be configured allowing the internal Wi-Fi users to

determine what network resources they have access to. The internal Wi-Fi users' group will be created on the active directory.

6.2 EXTERNAL

This wireless setup will be for the workers from partner companies. A SSID will be created for this setup on the FortiGate NGFW that the FortiAPs will be connecting to as well. A Wi-Fi Protected Access III (WPA3) Enterprise authentication method verified by a RADIUS server will also be recommended. This authentication method has been chosen because of the need to be consistent with the internal Wi-Fi users' authentication method. An appropriate security policy will be configured allowing the external Wi-Fi users to determine what network resources they have access to. From the security point of view, a more restrictive access is recommended for the external Wi-Fi users. Only required access will be provided. The external Wi-Fi users' group will be created on the active directory.

6.3 GUEST

This wireless setup will be for clients or guests visiting employees. A SSID will be created for this setup on the FortiGate NGFWs that the FortiAPs will be connecting to. A captive portal is recommended for the purpose of authentication of guest users. An account will be created for the receptionist to have access to only the user management feature on the FortiGate NGFW via web interface in order to create login details for the guest users. On the provision of email address by the guest, a random password will be generated, and the login details will only be valid for a

specified period. This authentication method has been chosen because the guest users will be changing. An appropriate firewall policy will be configured allowing the guest Wi-Fi users to strictly only internet access.

7 IT SERVICES MANAGEMENT

In order to manage and provide IT services to the DIC, a ticketing system will need to be implemented. While there are plenty of options available for ticketing systems, we believe SpiceWorks Help Desk on premise is the most effective solution for DIC. It has a large and active community, minimal setup and maintenance, highly customizable and integrates well with Active Directories. Customizations include custom ticket rules, and views to meet the workflow needs of the organization. SpiceWorks can also keep track of the time spent on tickets, the type of tickets being used, and devices associated with these tickets. With this information, IT staff can determine whether a product should be fixed or replaced. Furthermore, Spiceworks provides a robust user portal with Active Directory integration to allow tickets to be created easily and efficiently by end users(*Self-Hosted Help Desk Software*, n.d.).

REFERENCES

- 5 Top Firewall Providers for 2019*. (2019, January 6). CTC Technologies Inc.
<https://www.ctctechnologies.com/5-top-firewall-providers-for-2019/>
- Admin. (n.d.). *Windows 10 Provisioning Service by VMware AirWatch*. Retrieved April 5, 2020, from <https://docs.vmware.com/en/VMware-Workspace-ONE-UEM/1811/Workspace-ONE-UEM-Windows-Desktop-Device-Management/GUID-AWT-ENROLL-AUTOENROLLMENT.html>
- Adram Software. (n.d.). *Monitoring Systems and Applications*. Retrieved April 7, 2020, from <https://www.adremsoft.com/netcrunch/monitoring/systems-and-applications>
- Adrem Software. (n.d.-a). *Monitor Network Services, Devices, Sensors, Bandwidth, Traffic*. Retrieved April 7, 2020, from <https://www.adremsoft.com/netcrunch/monitoring/network-infrastructure>
- Adrem Software. (n.d.-b). *System Requirements*. Retrieved April 7, 2020, from <https://www.adremsoft.com/adoc/view/netcrunch/391507093795/system-requirements>
- Android Security Updates Scope | Samsung Mobile Security*. (n.d.). Retrieved April 5, 2020, from <https://security.samsungmobile.com/workScope.smsb>
- AnyDesk vs TeamViewer: Which is a Better Remote Desktop Software. (2019, December 26). *Techjockey.Com Blog*. <https://www.techjockey.com/blog/anydesk-vs-teamviewer-which-is-a-better-remote-desktop-software>
- Apple security updates*. (n.d.). Apple Support. Retrieved April 5, 2020, from <https://support.apple.com/en-us/HT201222>

- Armasu, L. (2019, November 4). *Intel vs AMD Processor Security: Who Makes the Safest CPUs?* Tom's Hardware. <https://www.tomshardware.com/features/intel-amd-most-secure-processors>
- Avast. (n.d.). *Business VPN, Password Protection—AVAST Antivirus Pro Plus*. Retrieved April 6, 2020, from <https://www.avast.com/en-ca/business/products/business-antivirus-pro-plus>
- Barker, E., Dang, Q., Scarfone, K., & Wouters, P. (2019). *Guide to Ipsec VPNs*. US Department of Commerce. <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-77r1-draft.pdf>
- Boeckl, K. (2016, June 28). *Back to basics: Multi-factor authentication (MFA)* [Text]. NIST. <https://www.nist.gov/itl/applied-cybersecurity/tig/back-basics-multi-factor-authentication>
- Brandon Lee. (2018, May 4). *Windows Server 2016 Hyper-V SAN vs Storage Spaces Direct*. Vembu.Com. <https://www.vembu.com/blog/windows-server-2016-hyper-v-san-vs-storage-spaces-direct/>
- Browsing, Searching and Viewing Items—Veeam Backup Explorers Guide*. (2020, January 16). Veeam Software Help Center. https://helpcenter.veeam.com/docs/backup/explorers/vee_browsing.html
- Buy AnyDesk for your Business*. (n.d.). AnyDesk. Retrieved April 6, 2020, from <https://anydesk.com/en/order>
- Canon imageCLASS D570 | Black and White Printer*. (n.d.). Retrieved April 6, 2020, from https://www.canon.ca/en/product?name=imageCLASS_D570&category=/en/products/Printers/Office-Printers/Small-Office-and-Home-Office/Black---White-Printers
- Canon imageCLASS MF236n | Black & White Multifunction Printer*. (n.d.). Retrieved April 6, 2020, from

https://www.canon.ca/en/product?name=imageCLASS_MF236n&category=/en/products/Printers/Office-Printers/Small-Office-and-Home-Office/Black---White-Printers

Canonical. (n.d.). *Debian*. Ubuntu. Retrieved April 5, 2020, from <https://ubuntu.com/community/debian>

Canonical. (2020). *Introduction | Server documentation*. Ubuntu. <https://ubuntu.com/server/docs>

Cloud, S. L. in T. E., July 9, in D. C. on, 2010, & Pst, 2:48 Am. (n.d.). *RAID 50 offers a balance of performance, storage capacity, and data integrity*. TechRepublic. Retrieved April 1, 2020, from <https://www.techrepublic.com/blog/the-enterprise-cloud/raid-50-offers-a-balance-of-performance-storage-capacity-and-data-integrity/>

Compare Windows 10 Home vs Pro | Microsoft Windows. (n.d.). Windows. Retrieved April 6, 2020, from <https://www.microsoft.com/en-us/windows/compare-windows-10-home-vs-pro>

Create Bulk Users in Active Directory (Step-By-Step Guide). (2018, January 13). *Active Directory Pro*. <https://activedirectorypro.com/create-bulk-users-active-directory/>

Dell EMC PowerEdge R6515 Rack Server: Server | Dell USA. (n.d.). Retrieved April 7, 2020, from <https://www.dell.com/en-us/work/shop/povw/poweredge-r6515>

Dell EMC PowerEdge R7525 Rack Server | Dell USA. (n.d.). Retrieved April 1, 2020, from <https://www.dell.com/en-us/work/shop/povw/poweredge-r7525>

Dell SC7020 Storage Array: Disk Arrays | Dell USA. (n.d.). Retrieved April 7, 2020, from <https://www.dell.com/en-us/work/shop/povw/storage-sc7020>

Fortinet. (n.d.-a). *FortiAP Series Data Sheet*.

Fortinet. (n.d.-b). *FortiGate Integrated WiFi Management*. Fortinet. Retrieved April 6, 2020, from </products/secure-wifi/fortigate-integrated.html?tab=models-specs>

Fortinet. (n.d.-c). *FortiGate Intrusion Prevention System (IPS)*. Fortinet. Retrieved April 6, 2020, from /products/ips.html

Fortinet. (n.d.-d). *FortiGate VM | VMware NSX-T integration*. Fortinet. Retrieved April 6, 2020, from /products/private-cloud-security/vmware.html

Fortinet. (n.d.-e). *Fortinet Threat Intelligence and Threat Research*. Fortinet. Retrieved April 6, 2020, from /fortiguard/threat-intelligence/threat-research.html

Fortinet. (n.d.-f). *FortiWiFi and FortiAP Configuration Guide | FortiAP / FortiWiFi 6.2.0 | Fortinet Documentation Library*. Retrieved April 6, 2020, from <https://docs.fortinet.com/document/fortiap/6.2.0/fortiwifi-and-fortiap-configuration-guide/961597/configuring-user-authentication>

Fortinet. (n.d.-g). *Hub-Spoke OCVPN with ADVPN shortcut*. Retrieved April 6, 2020, from <https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/853223/hub-spoke-ocvpn-with-advpn-shortcut>

Fortinet. (n.d.-h). *SD WAN Solutions Overview Page*. Fortinet. Retrieved April 6, 2020, from /products/sd-wan/overview.html

Fortinet. (n.d.-i). *SSL VPN Tunnel Mode*. Retrieved April 7, 2020, from <https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/954097/ssl-vpn-tunnel-mode>

Fortinet. (n.d.-j). *SSL VPN with RADIUS and Fortitoken*. Retrieved April 7, 2020, from <https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/207191/ssl-vpn-with-radius-and-fortitoken-mobile-push-on-fortiauthenticator>

Fortinet. (n.d.-k). *Web Filtering*. Fortinet. Retrieved April 6, 2020, from /support/support-services/fortiguard-security-subscriptions/web-filtering.html

Fortinet. (2019). *Data Sheet FortiAuthenticator*.

Fortinet. (2020). *Data Sheet: Fortigate 1500D Series*.

https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiGate_1500D.pdf

Frankel, S., Hoffman, P., Orebaugh, A., & Park, R. (2008). *Guide to SSL VPNs*.

<https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-113.pdf>

FSMO placement and optimization on Active Directory domain controllers. (2018, April 17).

<https://support.microsoft.com/en-us/help/223346/fsmo-placement-and-optimization-on-active-directory-domain-controllers>

Gartner. (n.d.). *Network Firewall Reviews and Comparisons*. Gartner. Retrieved April 7, 2020,

from <https://gartner.com/market/network-firewalls>

Gelas, J. D. (2019, August 7). *AMD Rome Second Generation EPYC Review: 2x 64-core*

Benchmarked. <https://www.anandtech.com/show/14694/amd-rome-epyc-2nd-gen>

Host Requirements | vSAN Space Efficiency Technologies | VMware. (n.d.). Retrieved April 3,

2020, from <https://storagehub.vmware.com/t/vsan-space-efficiency-technologies/host-requirements-1/>

How To Configure a Domain Password Policy. (2019, September 28). *Active Directory Pro*.

<https://activedirectorypro.com/how-to-configure-a-domain-password-policy/>

ImageCLASS D1650 | Black & White Multifunction Printer. (n.d.). Retrieved April 6, 2020, from

https://www.canon.ca/en/product?name=imageCLASS_D1650&category=/en/products/Printers/Office-Printers/Small-Office-and-Home-Office/Black---White-Printers

IT Security Solutions: Prevent and Detect Attacks. (n.d.). Rapid7. Retrieved April 7, 2020, from

<https://www.rapid7.com/solutions/>

JasonGerend. (n.d.). *DFS Replication overview*. Retrieved April 5, 2020, from

<https://docs.microsoft.com/en-us/windows-server/storage/dfs-replication/dfs-overview>

- Juniper Networks. (n.d.). *How Secure Are SD-WANs*. Juniper Networks. Retrieved April 6, 2020, from <http://www.juniper.net/us/en/insights/sd-wan-security/index.page>
- Katz, E. (2017, November 15). How to Conduct an Internal Security Audit in 5 Steps. *Dashlane Blog*. <https://blog.dashlane.com/conduct-internal-security-audit/>
- Larabel, M. (2019, August 7). *AMD EPYC 7502 + EPYC 7742 Linux Performance Benchmarks Review—Phoronix*. <https://www.phoronix.com/scan.php?page=article&item=amd-epyc-7502-7742&num=9>
- Lee, B. (2019, July 2). *Hyper-V vs VMware: A complete Comparison*. Vembu.Com. <https://www.vembu.com/blog/hyper-v-vs-vmware/>
- Lowder, J. (2019). Deploying Host-Based Firewalls across the Enterprise: A Case Study. In H. F. Tipton & M. Krause (Eds.), *Information Security Management* (1st ed., pp. 155–166). Auerbach Publications. <https://doi.org/10.1201/9781351073547-12>
- Manuro, A. (2018, October 31). *Microsoft Hyper-V 2019 vs. VMware vSphere 6.7* [Blog]. VInfrastructure Blog. <https://vinfrastructure.it/2018/10/microsoft-hyper-v-2019-vs-vmware-vsphere-6-7/>
- Microsoft. (2019, June 26). *Storage Spaces Direct overview*. <https://docs.microsoft.com/en-us/windows-server/storage/storage-spaces/storage-spaces-direct-overview>
- Modern Device Management: Mac Alongside Windows*. (n.d.). Retrieved April 6, 2020, from <https://www.jamf.com/resources/white-papers/modern-device-management-mac-alongside-windows/>
- OptiPlex 5070 Commercial Tower and Small Form Factor PC | Dell USA*. (n.d.). Dell. Retrieved April 5, 2020, from <https://www.dell.com/en-us/work/shop/desktops-all-in-one-pcs/new-optiplex-5070-desktop/spd/optiplex-5070-desktop>

Paloalto. (n.d.). *What is Microsegmentation? - Palo Alto Networks*. Retrieved April 6, 2020, from <https://www.paloaltonetworks.com/cyberpedia/what-is-microsegmentation>

Patch Management: Automatic & Comprehensive Patching. (n.d.). Retrieved April 6, 2020, from <https://www.avast.com/en-us/business/services/patch-management>

Peter, C. (2019, October 10). *What Is SSL Inspection? Why Use SSL Inspection? - DZone Security*. Dzone.Com. <https://dzone.com/articles/what-is-ssl-inspection-why-use-ssl-inspection>

PowerEdge-R7525-Spec-Sheet.pdf. (n.d.). Retrieved April 1, 2020, from https://i.dell.com/sites/csdocuments/Product_Docs/en/PowerEdge-R7525-Spec-Sheet.pdf

Prerequisites of installing Exchange 2016. (2016, March 31). *MustBeGeek*. <https://www.mustbegeek.com/prerequisites-of-installing-exchange-2016/>

Reed, J. (2018, December 26). *Hyper-V vs VMware: Complete Comparison of Platforms*. Official NAKIVO Blog. <https://www.nakivo.com/blog/hyper-v-vmware-complete-comparison/>

Rocque, M. (2015, July 10). DDR4 RDIMM and LRDIMM Performance Comparison. *Microway*. <https://www.microway.com/hpc-tech-tips/ddr4-rdimm-lrdimm-performance-comparison/>

Rodriguez, J. (n.d.). *The Top 7 Free and Open Source Appointment Scheduling Software*. Retrieved April 7, 2020, from <https://www.goodfirms.co/blog/top-7-free-and-open-source-appointment-scheduling-software>

SANS Policy Team. (2014a, June). *Router and Switch Security Policy*. <https://www.sans.org/security-resources/policies/network-security/pdf/router-and-switch-security-policy>

SANS Policy Team. (2014b). *Technology Equipment Disposal*. <https://www.sans.org/security-resources/policies/server-security/pdf/technology-equipment-disposal-policy>

SANS Policy Team. (2014c, June 14). *Security Response Plan Policy*.
<https://www.sans.org/security-resources/policies/general/pdf/security-response-plan-policy>

SANS Policy Team. (2017). *Password Protection Policy*. <https://www.sans.org/security-resources/policies/general/pdf/password-protection-policy>

Self-Hosted Help Desk Software: Free from Spiceworks. (n.d.). Spiceworks. Retrieved April 7, 2020, from <https://www.spiceworks.com/free-help-desk-software/self-hosted/>

Sharma, N. (2019, October 2). *Review: IT ecosystem monitoring solution NetCrunch 10.6*. TechGenix. <http://techgenix.com/monitoring-solution-netcrunch-10-6/>

Shipley, G. (2008, June 30). *Are SIEM and log management the same thing?* Network World. <https://www.networkworld.com/article/2280829/are-siem-and-log-management-the-same-thing-.html>

Shread, P. (2018, August 16). *Ten Top Next-Generation Firewall (NGFW) Vendors*. <https://www.esecurityplanet.com/products/top-ngfw-vendors.html>

Smith, R. (n.d.). *Windows Account Lockout Policy*. Retrieved April 6, 2020, from <https://www.ultimatewindowssecurity.com/wiki/page.aspx?spid=AccountLockout>

Splunk. (n.d.). *SIEM – Security Information and Event Management – Driven by Analytics*. Splunk. Retrieved April 6, 2020, from https://www.splunk.com/en_us/siem-security-information-and-event-management.html

Splunk. (2020). *The 2020 Magic Quadrant for SIEM*. Splunk. https://www.splunk.com/en_us/form//en_us/form/gartner-siem-magic-quadrant.html

Stevens, G. (2020, February 28). *2020 Best VPS Hosting Services in Canada (Uptime & Cost)*.

HostingCanada.Org. <https://hostingcanada.org/best-vps-host/>

TeamViewer pricing: Leader in remote desktop and access. (n.d.). TeamViewer. Retrieved April

6, 2020, from <https://www.teamviewer.com/en-us/buy-now/>

The OG Google Pixel was left out of the November security update. (2019, November 4).

Android Central. <https://www.androidcentral.com/google-pixel-stops-receiving-security-updates-right-schedule>

Ubuntu release cycle. (n.d.). Ubuntu. Retrieved April 5, 2020, from

<https://ubuntu.com/about/release-cycle>

Veam Software. (2020). *Veam Backup & Replication Datasheet*.

VMware. (n.d.). *VSAN ReadyNode™ Sizer*. Retrieved April 8, 2020, from

<https://vsansizer.vmware.com/login?src=%2Fhome>

VMware. (2017). *Fortinet VMX with VMWare NSX*.

VMware Compatibility Guide—Horizon (Thin Clients) Search. (n.d.). Retrieved April 5, 2020,

from

https://www.vmware.com/resources/compatibility/detail.php?deviceCategory=vdm&productid=50038&deviceCategory=vdm&details=1&releases_filter=505&horizonVersion=510&page=1&display_interval=10&sortColumn=Partner&sortOrder=Asc

Vostro 14" 3490 Laptop With Essential Productivity | Dell Canada. (n.d.). Dell. Retrieved April

6, 2020, from <https://www.dell.com/en-ca/work/shop/laptops-ultrabooks/new-vostro-14-3490-laptop/spd/vostro-14-3490-laptop>

VPN Encryption Explained: IPsec vs SSL which is faster / more secure? (2019, February 2).

Comparitech. <https://www.comparitech.com/blog/vpn-privacy/ipsec-vs-ssl-vpn/>

VSAN Hardware Calculator. (2014). <https://vsan.virtualappliances.eu/>

VSAN Part 25—How many hosts needed to tolerate failures? (2014, May 15).

CormacHogan.Com. <https://cormachogan.com/2014/05/15/vsan-part-25-how-many-hosts-needed-to-tolerate-failures/>

What version of Android can I upgrade my Samsung phone to? | Samsung Support Australia.

(n.d.). Samsung Au. Retrieved April 5, 2020, from

<https://www.samsung.com/au/support/mobile-devices/android-version-availability/>

Williams, T., & Wheeler, M. (2019). *Next Generation Intrusion Prevention System (NGIPS) Test*

Report. <https://www.fortinet.com/content/dam/fortinet/assets/analyst-reports/nss-labs-2019-ngips-test-report-fortinet-fortigate-100f.pdf>

Windows 10 Pro vs. Enterprise: What Is the Difference? (2019, November 14). Lakeside

Software. <https://www.lakesidesoftware.com/blog/windows-10-pro-vs-enterprise>

Wit, N. D. (2007, February 1). *Digital workflow depends on well-designed networks*. Diagnostic

Imaging. <https://www.diagnosticimaging.com/digital-workflow-depends-well-designed-networks>

Witts, J. (2020, March 17). The Top 11 Endpoint Security Solutions for Business. *Expert*

Insights. <https://www.expertinsights.com/insights/the-top-endpoint-security-solutions-for-business/>

Zimmer, D. (2019, December 23). *VMware vSphere—Why checking NUMA Configuration is so*

important! Medium. <https://itnext.io/vmware-vsphere-why-checking-numa-configuration-is-so-important-9764c16a7e73>

8 APPENDIX

8.1 NETWORKING

8.1.1 VLAN CONFIGURATION

- Edmonton HQ site layer-2 and layer-3 switches configured with VLAN ID for all internal departments.
- VLAN ID configured for HQ datacenter server traffic and management traffic.
- Iqaluit and R&I plaza configure with VXLAN as both implemented on NSX virtualization platform.

8.1.2 PHYSICAL CABLING

- We done cabling for virtual to physical infrastructure connectivity. It has been done by connecting Dell server physical port to rack mounted equipment through patch panel. Final decision left as we ordered new cable for final demonstration.
- Cable connection have been completed for HQ site routers and switches. We have used straight-through cable between routers to switches connection, crossover cable used to connect router to router and switch to switch.

8.1.3 PHYSICAL SWITCHES

- Cisco 2960 switch had been configured for HQ site. EtherChannel configured between Cisco 2960 and two Cisco 3650 switches.
- First hope redundancy protocol configures between mentioned layer 2 and 3 switches.
- Every department VLAN configured on switch.

- Device hardening have been left which we planned to complete on later time.

8.1.4 LOGICAL DISTRIBUTED SWITCHES

- We had created two distributed switches. One for VMs connectivity between two ESXi switch, second for virtual to physical environment connectivity.
- Port-Group created as per site requirement; still final touch left in terms of proper planning for demonstration.
- Following figure shows created distributed switches and distributed port-group under it.

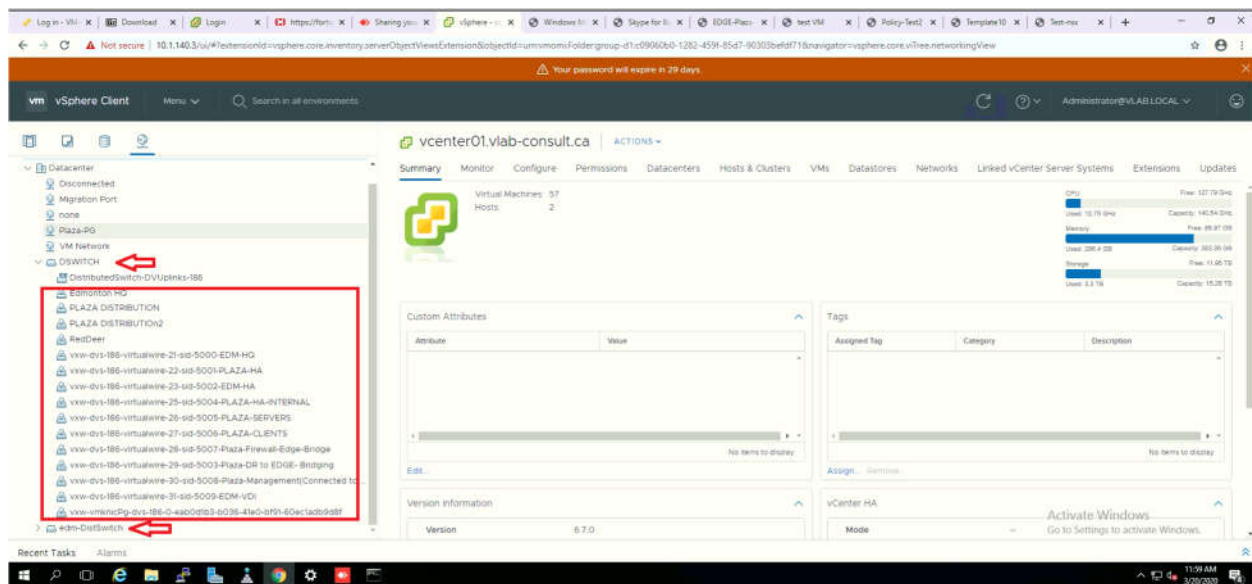


Figure 25 Distributed Switch and Distributed Port Group

8.2 LAYER 3 CONNECTIVITY

8.2.1 OSPF IPV4 & CONNECTIVITY

- Configured IPv4 addresses on every virtual and physical network device.
- OSPF configured on virtual networking devices such as edge and distributed router. Cisco 3650 layer 3 switches and 4321 routers configured with OSPFv3.
- Virtual to physical environment connectivity have been completed. Site to site connectivity completed for two sites, one site left to test site to site connectivity.
- VOIP configuration is left which planned to do in further days.

8.2.2 OSPF IPV6 & CONNECTIVITY

- IPv6 addresses configured for Edmonton HQ and Iqaluit site
- Intra-site IPv6 connectivity working, virtual to physical connectivity for IPv6.
- Configured Static IPv6 route on NSX edge router as it does not support dynamic routing.
- Site to site IPv6 connectivity left which we were about to complete.
- OSPFv3 configured for IPv6 on physical network devices.

8.2.3 QOS

- We did not start to implement QoS policies. We planned to implement QoS for VoIP traffic on Iqaluit and HQ sites. We were also planning to implement QoS for PACS/RIS traffic.

8.2.4 IP ADDRESS MANAGEMENT

8.2.4.1 SUBNETTING DESIGN FOR BOTH IPV6 AND IPV4

- IP addressing scheme completed for both IPv4 and IPv6 addresses. We have documented IP address assignment for all six sites with possible departments in technical documentation portion.

8.2.5 WIRELESS

8.2.5.1 INTERNAL ACCESS

- The FortiAP was configured and new SSID tagged “Internal-V” was created for both 2.4 and 5 GHz
- A new user group called WiFiInternalUsers was created on the active directory
- The RADIUS server was configured for FortiGate as a RADIUS client for WiFi access authentications
- A security policy was configured to allow WiFiInternalUsers for WiFi access.
- The UTM functions like IPS, SSL inspection, web filtering were applied to the security policy

8.2.5.2 EXTERNAL ACCESS

- The FortiAP was configured and new SSID tagged “External-V” was created for both 2.4 and 5 GHz
- A new user group called WiFiExternalUsers was created on the active directory

- The RADIUS server was configured for FortiGate as a RADIUS client for WiFi access authentications
- A security policy was configured to allow WiFiExternalUsers for WiFi access.
- The UTM functions like IPS, SSL inspection, web filtering were applied to the security policy

8.2.5.3 GUEST ACCESS

- The FortiAP was configured and new SSID tagged “Guest WiFi” was created for both 2.4 and 5 GHz
- A captive portal was configured as the means of authentication
- An account was created for the receptionist for guest user management
- Guest WiFi user accounts (their emails and a random password) were then created using the receptionist account
- Disclaimer and authentication web pages which the guest users will use to login were enabled
- A security policy was configured to allow guest users only internet access.
- The UTM functions like IPS, SSL inspection, web filtering were applied to the security policy

8.3 SEVER VIRTUALIZATION AND INFRASTRUCTURE

8.3.1 EXSI HOSTS

8.3.1.1 HOST DATASTORE RAID 50

- This was implemented at the hardware level using Dell's setup utilities

8.3.1.2 VM HIGH AVAILABILITY & DRS

- DRS was enabled but not functional due the need for shared storage
- Was going to move some Virtual Machines to SAN once that was ready to demonstrate DRS
- Cluster was configured but cannot failover until shared storage was configured

8.3.2 VM MANAGEMENT

8.3.2.1 VCENTER WITH EXSI HOST INTEGRATION

- Implemented
 - o A single vCenter System was deployed on the cluster located on the management network of Edmonton HQ using hostname vcenter01.vlab-consult.ca (10.1.140.1) with DNS server located in 10.1.150.1 and .2 located behind distributed edge, distributed routers and logical switches.
 - o EXSi hosts were added to a logical cluster using FQDN records

- Servers were initially on 10.1.140.2 and 10.1.140.3 but were later moved to 10.1.140.10 and .11 due to a change in networking
- Both Management interfaces of Host were on a distributed port group facing physical interfaces on VLAN 140.
- FQDN enabled migration of IP address on hosts without much hassle
- Deployed certificates issued by internal CA for vSphere Client, Host connections as well as connection to NSX
- VMotion was fully working the dedicated p2p 10GB ports
- Built in SSO integration with NSX Manager
- Planned implementation
 - Windows SSO was not implemented yet but did not expect it to take long to configure.

8.3.2.2 TEMPLATES

- This was fully implemented with both windows 10 and Server 2016/19 templates made
- VMWare Policies were also created to help VMS to sysprep, autojoin domain and use VM name as hostname once deployed, no way of specifying IP address per deployment

8.3.2.3 V-REALIZE ORCHESTRATOR/AUTOMATION

- The Appliance used was an older version that was not fully compatible with our version of vCenter and EXSi

- Automation portion of the appliance refused to connect with vCenter SSO, this is used primarily for self-enrollment
- Implemented some basic tasks that allowed deployment of servers from templates but with manual specification of IP addressing method, hostname, and server to be deployed on if necessary.
- Other default tasks included creation of NSX objects, and User Creation on Windows Active Directory

8.3.3 NETWORK VIRTUALIZATION

We have selected VMware NSX 6.4 for network virtualization implementation throughout different sites. Initial stage of capstone project we struggle a lot as this concept is totally new for us which required depth research of technology (SDN) and product (NSX). However, we had successfully implemented Iqaluit and R&I sites completely on VMware NSX. Edmonton HQ datacenter traffic (East-West) managed by NSX which then connected to physical infrastructure for further connectivity to internal departments as well as internet.

8.3.3.1 NSX MANAGER

We started to implement VMware NSX by installing NSX manager on ESXi host. Once installation complete, we must register NSX manager to vCenter in order to enable complete features of NSX. After successfully registered with vCenter, it enables NSX features in vCenter. We can think as vCenter works as management software for NSX manager where we can manage all the NSX components such as

logical switches, Distributed firewall, edge and distributed routers and NSX controllers. Open vCenter and follow menu > Network and Security option. Figure 26 shows network and security option in vCenter.

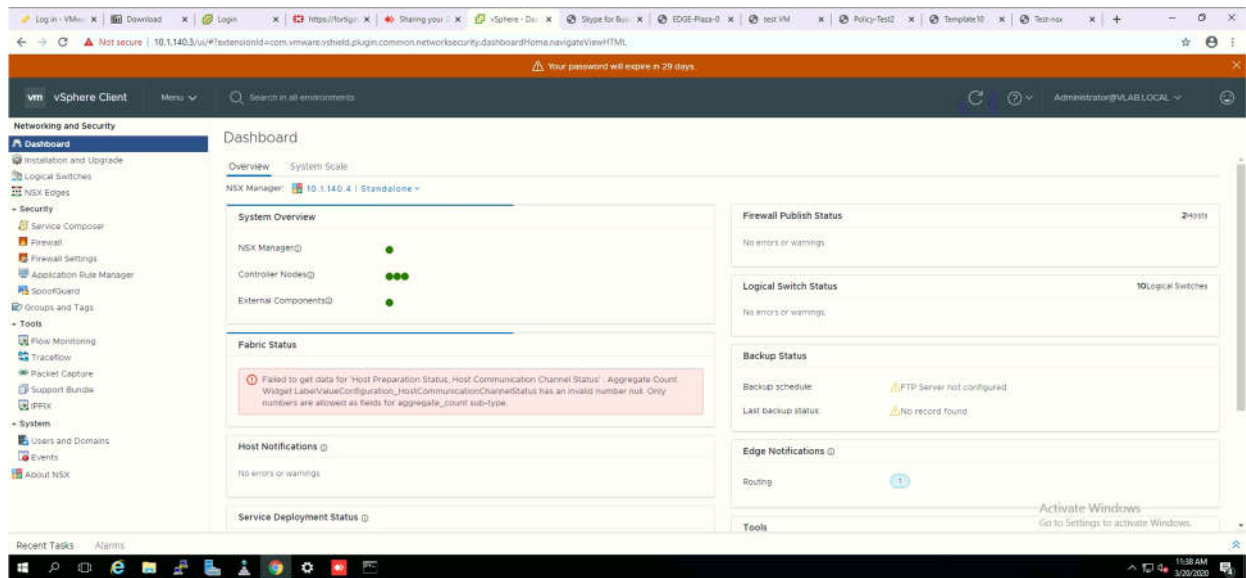


Figure 26 Dashboard of NSX Access from vCenter

We have created one transport zone for whole virtualization platform. Transport zone defined scope for network equipment, cluster has been defined as a source for transport zone. For example, I defined one transport zone while creating logical switch which means logical switch allow to add VMs which belongs to that transport zone. Figure 27 shows that created transport zone for our virtualization platform.

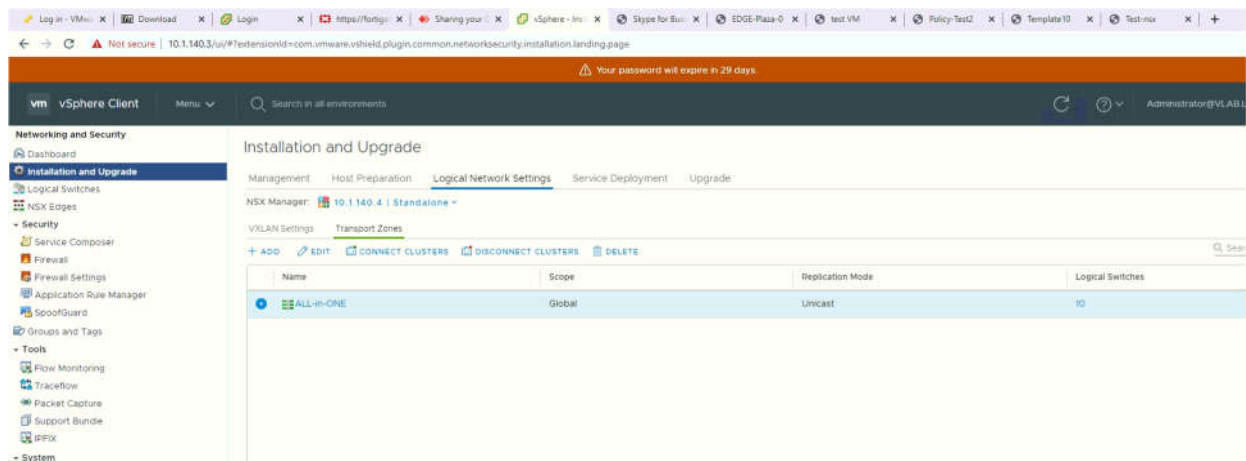


Figure 27 Transport Zone of NSX

8.3.3.2

8.3.3.3 NSX EDGE DEPLOYMENT

Edge router have been implemented for all three different sites. Basically, it is a NSX component which allows virtual infrastructure to connect with physical networking devices, inside vCenter we attach edge uplink interface to vSwitch which is then connect to ESXi host physical port, this port then connect to Cisco 3650 switch (Edmonton HQ). We have panned to implement two edge routers for Edmonton HQ datacenter in order to show redundancy for virtual to physical environment connectivity. Figure 28 shows created edge router for each site.

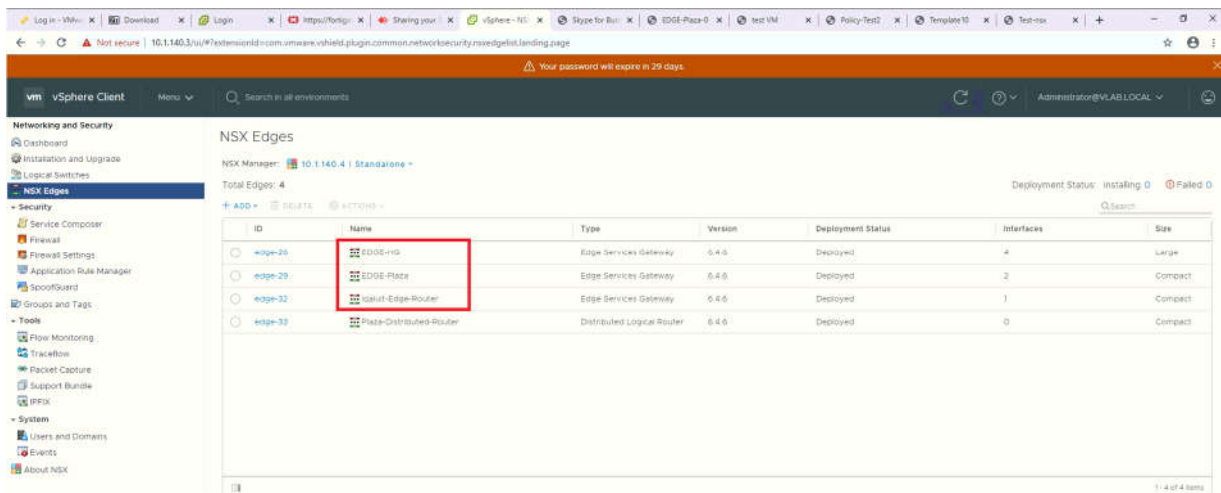


Figure 28 Edge Router on NSX

Figure 29 shows edge interface configuration. Interface configure with uplink is connected to ESXi host physical port via vSwitch, we can also use distributed port group instead vSwitch to connect uplink interface to ESXi physical port. Interface configure with selected type 'internal' can be used to connect distributed router via logical switch, it can also be used to connect VMs machines to edge router via logical switches if decided not to use distributed router. NSX edge router support maximum 10 interfaces.

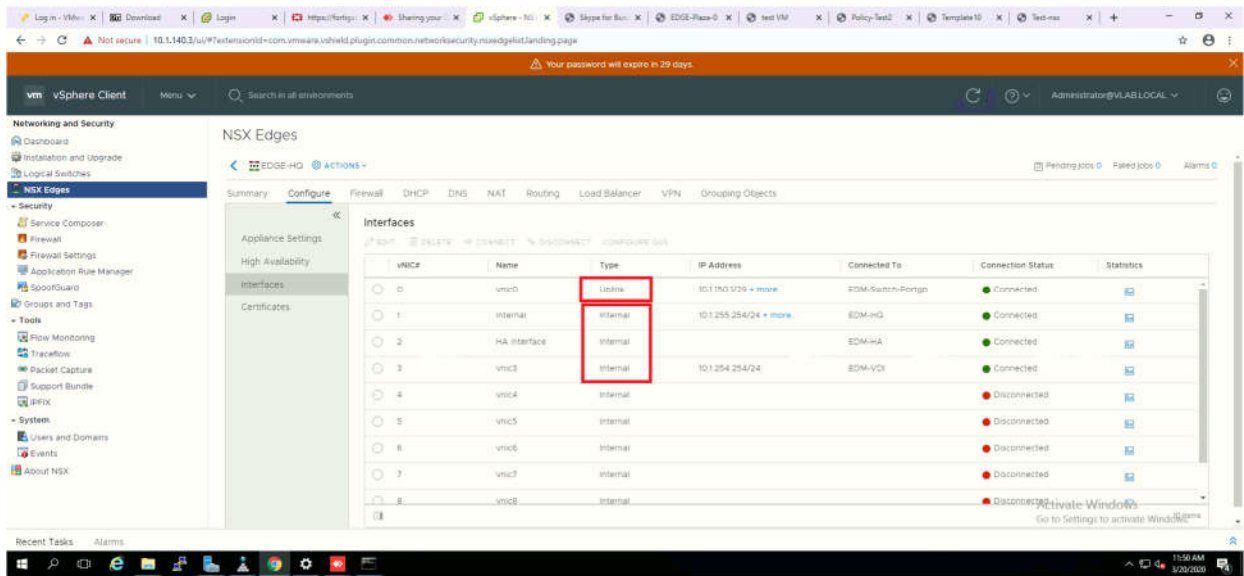


Figure 29 Interfaces of NSX Edge Router

Figure 30 reveals configuration information of Edmonton edge router interface. Here, we configured both IPv4 and IPv6 addresses. Interface can be connected to logical switches or distributed port group. we have connected it to distributed port group named “ED-Switch-Portgp”.

Edit Interface | vnic0

Basic

Advanced

vNIC#

0

Name *

vnic0

Type

☐ Internal
 ☒ Uplink
 ☐ Trunk

Connected To *

EDM-Switch-Portgp

Connectivity Status

☒ Connected

Configure Subnets

+ ADD

DELETE

Q Search

<input type="checkbox"/>	Primary IP Address	Secondary IP Addresses	Subnet Prefix Length
<input type="checkbox"/>	10.1.150.1		29
<input type="checkbox"/>	2020:1:150::1		125

CANCEL

SAVE

Figure 30 Interface Configuration

Figure 31 shows edge router interface (Uplink) connection to distributed switch uplink. When we were creating distributed switch, it asked us to select two uplink which can be two physical port of ESXi hosts. This is how edge router interface go out for internet connectivity through physical network infrastructure.

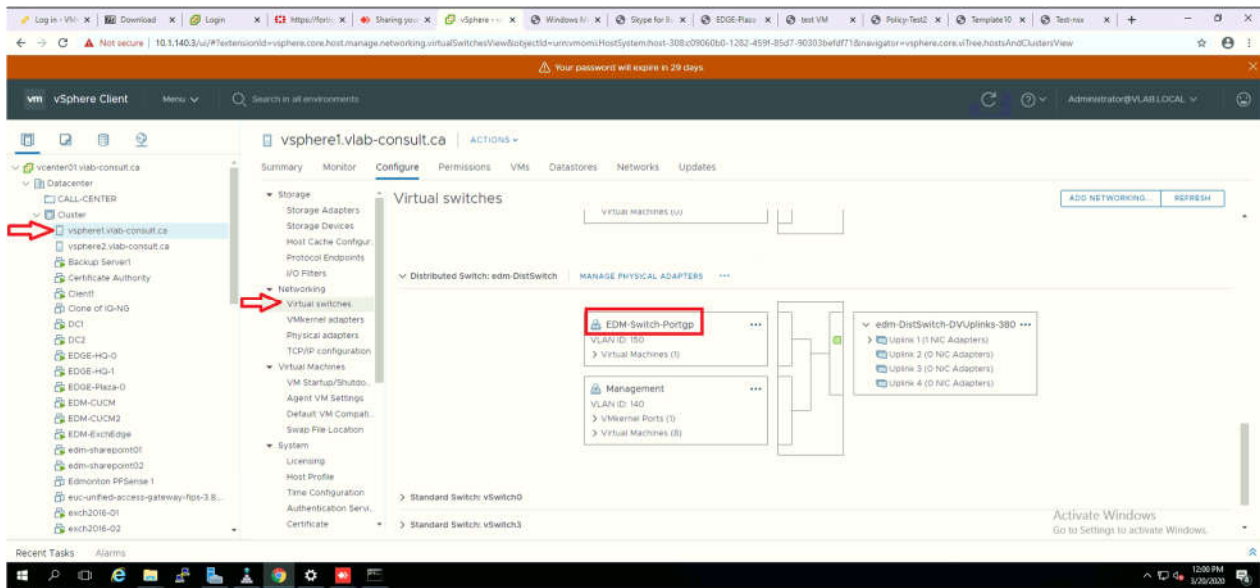


Figure 31 Edge Interface Connection to Physical Port Through Distributed Port group

Once interface have been configured, we configure dynamic routing protocol OSPF on edge router. Figure 32 shows that edge router allows us to configure routing protocol such as OSPF, BGP and static route.

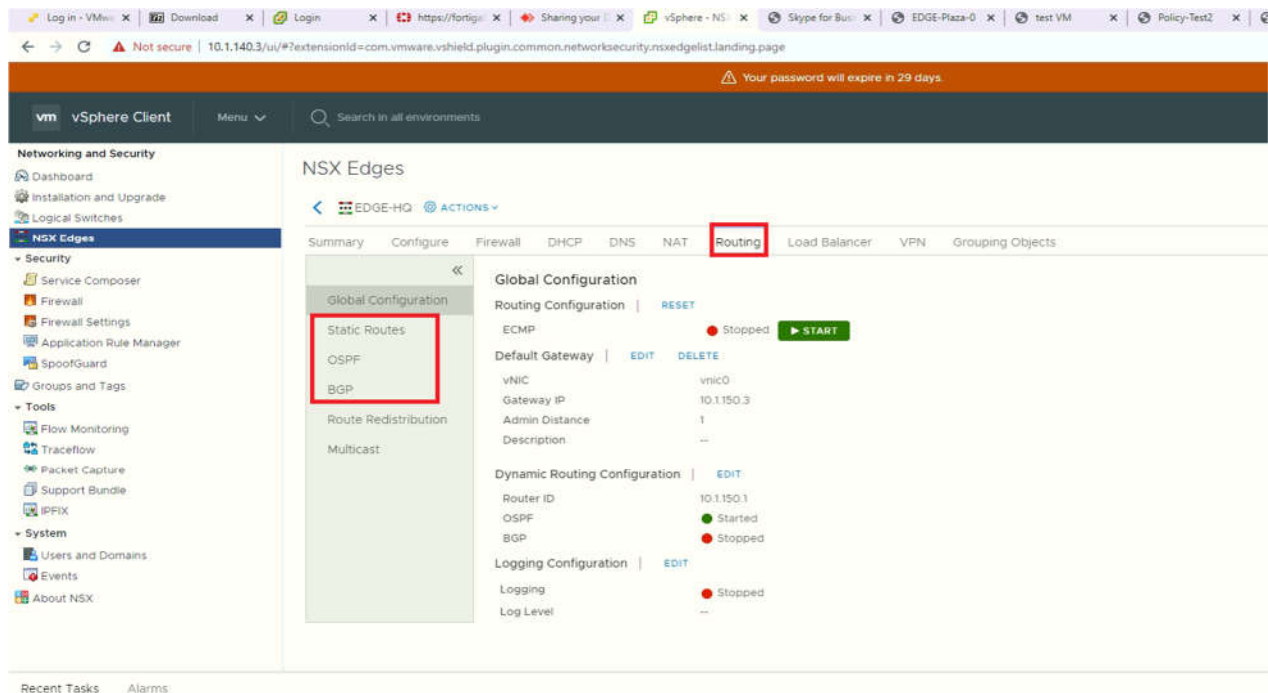


Figure 32 Routing Options on Edge Router

We had configured OSPF routing protocol throughout three different sites on NSX platform. Figure 33 reveals OSPF configuration on Edmonton edge router. Here on edge router, it allows us to configure OSPF area number then we apply that area to an interface. We have configured area 0 and then applied to a different interface.

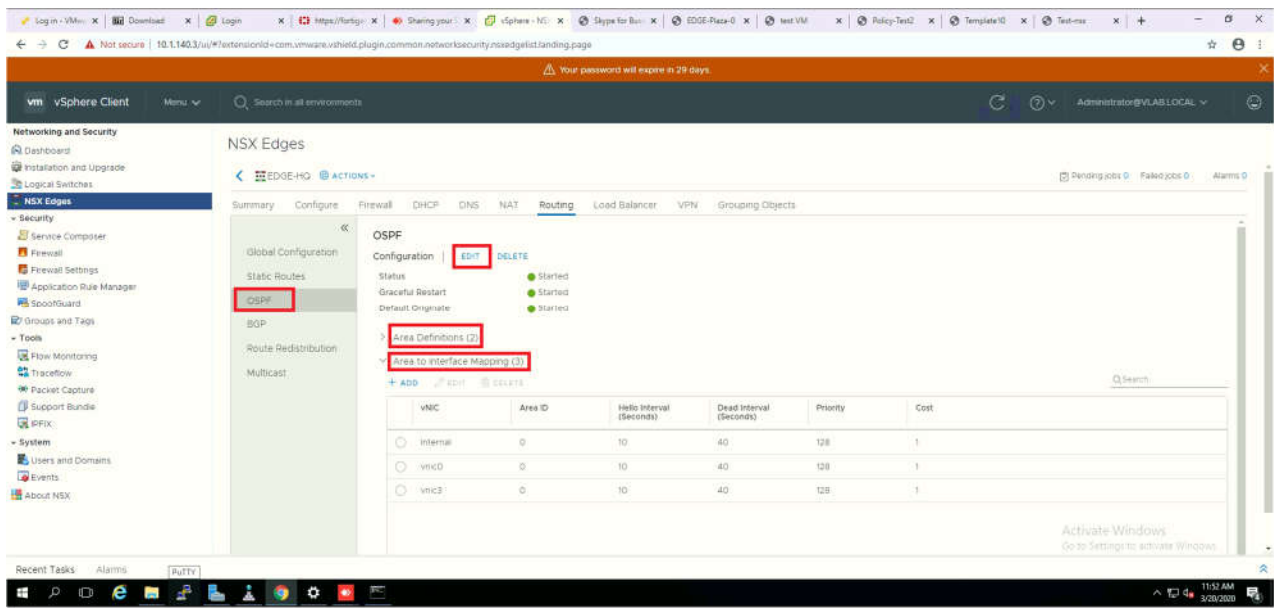


Figure 33 OSPF Configuration on NSX Edge

As we discussed on technical documentation, NSX (Version 6.4.6) edge does not have dynamic routing functionality for IPv6 routing. However, it does allow static route for IPv6 routing, this makes us to configure IPv6 static route throughout all physical network devices for virtualized network IPv6 subnets. (We successfully configure IPv6 connectivity up to Edmonton HQ site FortiGate firewall. We have not got chance to check end to end IPv6 connectivity between two sites, but we are confident that almost about to reach IPv6 connectivity). Figure 34 shows IPv6 static route configuration on edge router.

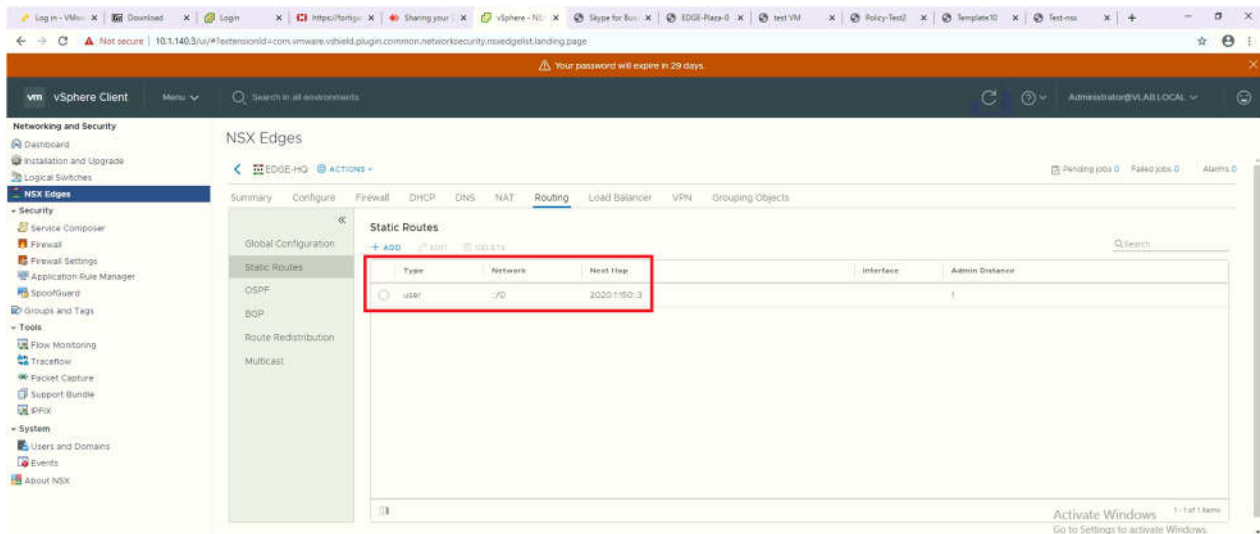


Figure 34 IPv6 Static Route Configuration

Edge router allowed us to configure firewall for network traffic. If you configured everything correctly and packets get dropped, then better to check firewall rules. By default, NSX edge dropped all configured interface traffic. Figure 35 shows edge firewall rule configuration.

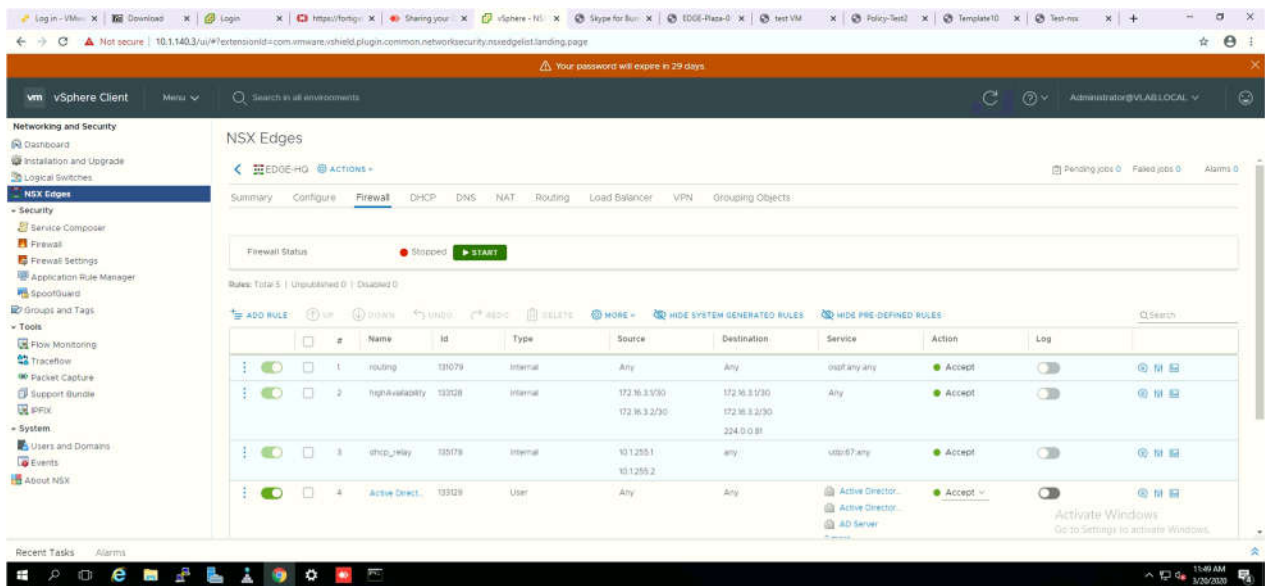


Figure 35 Firewall Rules Configuration on NSX Edge

8.3.3.4 NSX DISTRIBUTED ROUTER

We have decided to configure NSX distributed router for R&I Plaza site where we planned to configure only IPv4 addresses because distributed router does not support IPv6 routing. As per our research, distributed router used to handle datacenter east-west traffic for different networks. It does provide dynamic routing functionality for IPv4 addresses on same level as edge router. Figure 36 shows that we have configured distributed router for Plaza site.

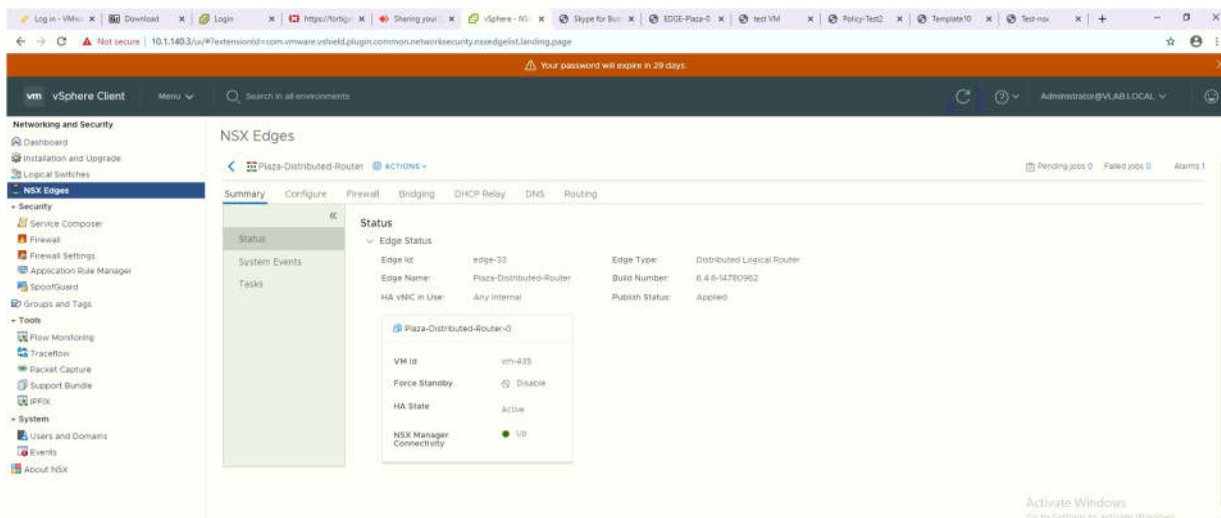


Figure 36 Distributed Router on NSX For Plaza

8.3.3.5 VXLAN OVER DISTRIBUTED SWITCH

We have configured NSX logical switch for all three different sites. Logical switches are work as a bridge to connect VMs machines to distributed or edge router, it can also be used to connect distributed to edge router. we cannot connect directly distributed router interface to edge router interface, logical switch can work as a bridge to provide connectivity.

Each logical switch represents one segment ID, it can automatically choose by NSX controller as soon as you create new logical switch. Segment ID is like VLAN ID, NSX each segment ID represent VXLAN. Segment ID is anything between 1 to 16,777,215, but NSX decided to start number from 5000 to avoid confusion with VLAN ID. We have selected segment ID pool 5000-5500 which allows us to create 500 logical

switches. Figure 37 shows created logical switches, it does required editing, but we did not get chance to do edit it.

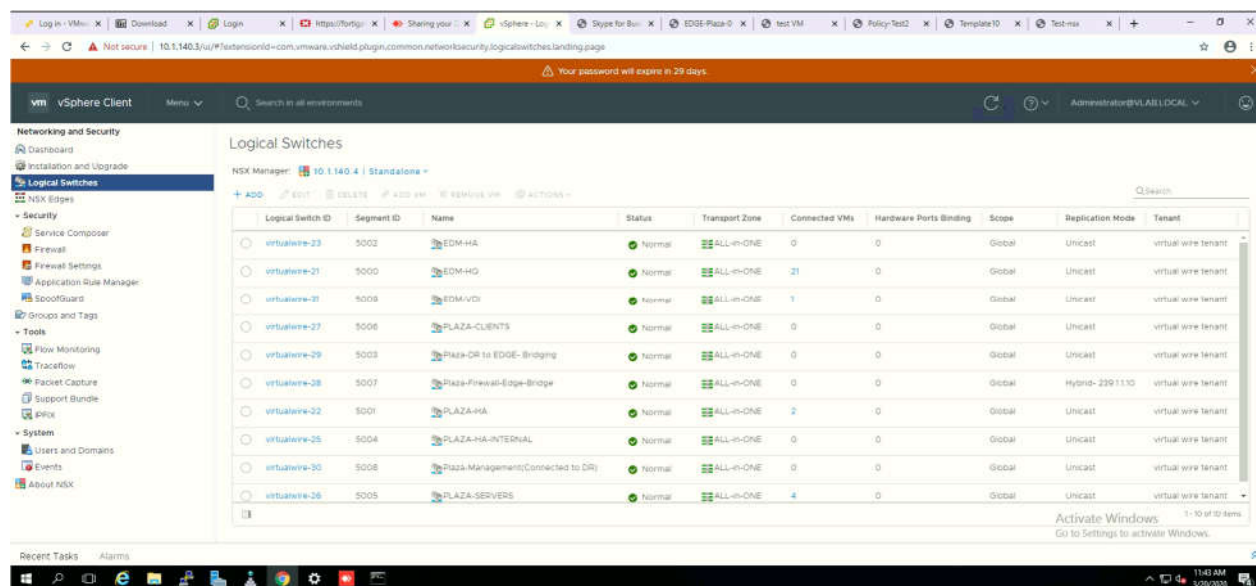


Figure 37 Logical Switch on All Sites

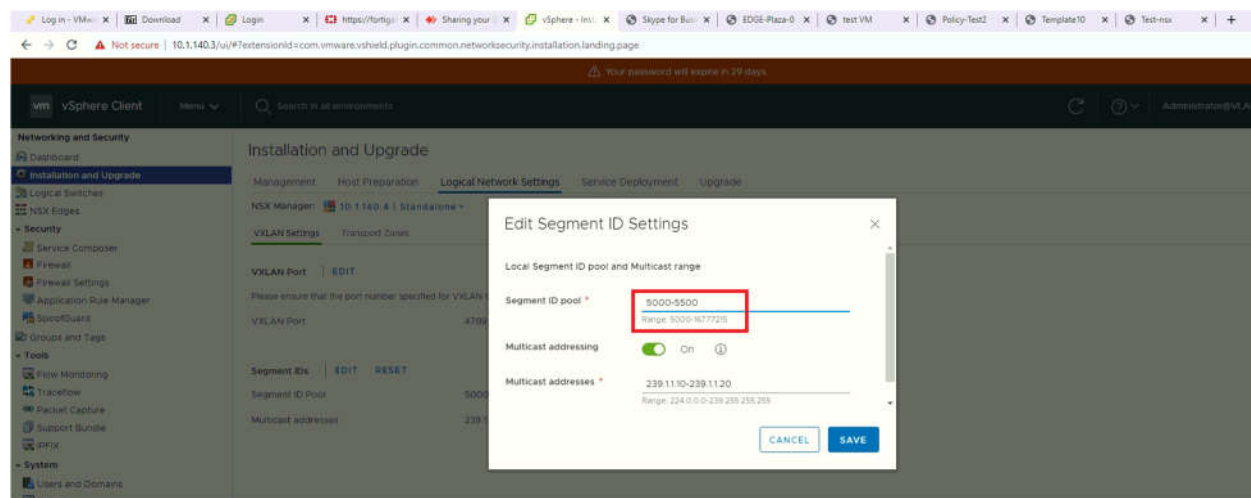


Figure 38 Segment ID Pool on NSX

8.3.3.6 NSX CONTROLLERS

We have created 3 NSX controller to manage virtualization environment for all three sites. Primary reason behind 3 NSX controller is a redundancy, if one controller dies then other two continue provide functionality. NSX controller is like brain for logical switches and distributed routers. Figure 39 shows that we had created three NSX controller for virtualization platform.

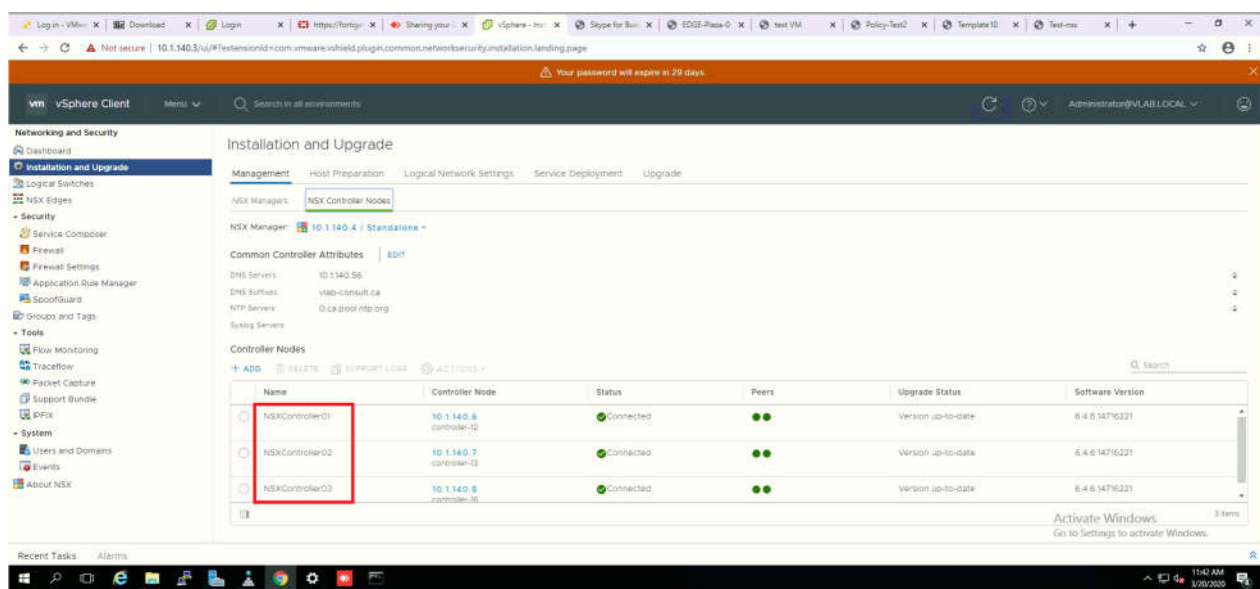


Figure 39 NSX Controller for Virtualization Platform

8.3.4 VDI

8.3.4.1 AUTOMATED FULL CLONE DESKTOP POOL

- This was implemented as a stopgap in the case that linked clones could not be implemented on time

- An additional template that was already joined to domain was created for this purpose. However, clones created from the templates had to be however had the same SID.
- Pool was set up to always have at least 2 ready to be used VMs, with one on and available to be used immediately. Second VM would be powered on if a user has connected to the first VM. A third VM would then automatically be created to meet the requirement of 2 ready VMS.
- With full clone pool there was no option to disable unused VMs
- This was tested using one of the windows 10 VMs using a Horizon View Client
- A test group was created and assigned entitlement so that testing could be used.

8.3.4.2 JMP SERVER

- This was installed on a Windows Server and an additional server was spun up for the required SQL database, but not configured to join Horizon Connection Server. Also, further research during the technical document suggested that I needed the composer rather than the JMP server for linked clones.

8.3.4.3 HORIZON CONNECTION SERVER

- Was installed on a Windows Server, provided with a TLS certificate from Windows CA and connected to Windows Domain for management and distributing entitlements.
- Clients were able to connect to it without issue

8.4 SERVICES

8.4.1 CERTIFICATE AUTHORITY

- A single certificate authority was deployed for the demo with web enrollment enabled to make it easier to submit requests for non-Microsoft Servers
- Certificates that were created include Exchange certificates, Active Directory Server Certificates, NSX Manager, sFTP server, FortiGate, RAS server, and SharePoint

8.4.2 SPICEWORKS TICKETING

- For the demo we were going to show the cloud-based version of Spiceworks. This was fully functional.
- Time permitting, we would have downloaded and installed the on-premise version of Spiceworks ticketing system

8.4.3 DISTRIBUTED FILE STORAGE

- This was not yet configured but was not anticipated to take too long
- Two Namespaces were to be created, one for user profiles/folder redirection and one for the software repository
- The software repository for software assignment was to be moved here once this was completed

8.4.4 WEB PRESENCE

- This was planned to be hosted on Digital Ocean but had not yet been implemented
- Plan was to also have a booking system implemented here as well.

8.4.5 PACS/RIS (LAMP STACK)

- Ubuntu Linux LTS 18.04 server was installed
- LAMP stack which includes Apache, MySQL and PHP was configured and running
- This setup was done to represent the PACs/RIS server

8.4.6 REMOTE MANAGEMENT SOFTWARE

- Free versions of AnyDesk were deployed on some remote access virtual machines to access web GUI interfaces for vSphere and to the Windows Servers.
- However, planned customization of AnyDesk clients and deployments were not completed

8.4.7 MICROSOFT NETWORK POLICY SERVER AAA

- This was installed on standalone server
- Three policies were created on the NPS. One for external Wi-Fi users, one for internal Wi-Fi, and one for client VPNs.
- All were using PEAP or EAP MSCHAPv2 for security with certificates provided via deployed NPS

8.4.8 DIRECTORY SERVICES

8.4.8.1 SITES AND INTER/INTRA REPLICATION

- Only servers in deployed in Edmonton HQ
- Servers were provisioned and ready to be deployed for other sites pending network functionality on other sites and site-to-site VPN completion.
- Sites and subnets however were already provisioned and were pending sever deployment to be populated

8.4.8.2 GPOS

- GPOs for software deployment were configured for Chrome
 - o but missing some software pending the purchase/acquiring of them, those include Office, AnyDesk
 - o Repository was currently located on WBS, but the plan was to move it to a DFS namespace
- GPOs for password policies were enabled and configured. See the GPO section in the technical document for how it was configured.
- GPOs related to specific third-party applications were installed via ADMX
 - o Those included GPOs for Chrome that enabled automatic default browser, homepage setting to our SharePoint installation, blocking statistics
- GPO Policies for desktop configurations such as wallpapers, mapped drives and or printers had yet to be configured but were planned to be completed soon

- GPOs for account lock out had not been configured but were planned to be configured based on the proposal
- GPOs for home folder and user profile redirection was planned but not yet configured

8.4.9 DNS

- DNS records were automatically created for Windows Machines and cluster, except for Edge Server, that was configured manually
- DNS records for vSphere Suite appliances including vCenter, vSpher01, vSphere02, Operations Manager, Orchestrator were manually configured
- External DNS was to rely on registrar DNS
- DNS was integrated with Active Directory Servers

8.4.10 DHCP

- Two DHCP Servers were deployed with additional DHCP servers deployed for each site pending resources available.
- Super scopes and Scopes were configured for all planned demo subnets
- Failover was tested locally for Edmonton scopes
- DHCP relay on NSX routers was functioning for VDI subnet

8.4.11 PRINT SERVER

- Implemented using Microsoft Server

8.4.12 PATCH MANAGEMENT

- Patch management was handled by Avast
- This was tested but not deployed in mass pending deployment of Windows Desktops

8.4.13 SFTP

- Implemented through Microsoft Server IIS using Microsoft Active Directory Certificate Authority's domain specific SSL certificate
- Only accessible through 3rd party FTP client software, access through web browser was not successful

8.5 CLIENT AND SOFTWARE

8.5.1 USER CREATION AUTOMATION

The following slightly modified script was planned to be used for user creation("Create Bulk Users in Active Directory (Step-By-Step Guide)," 2018).

```
# Import active directory module for running AD cmdlets
Import-Module activedirectory

#Store the data from ADUsers.csv in the $ADUsers variable
```

```

$ADUsers = Import-csv C:\it\bulk_users1.csv

#Loop through each row containing user details in the CSV file
foreach ($User in $ADUsers)
{
    #Read user data from each field in each row and assign the data to a variable
    as below

    $Username    = $User.username
    $Password    = $User.password
    $Firstname   = $User.firstname
    $Lastname    = $User.lastname
    $OU          = $User.ou #This field refers to the OU the user account is to be
    created in
    $email       = $User.email
    $streetaddress = $User.streetaddress
    $city        = $User.city
    $zipcode     = $User.zipcode
    $state       = $User.state
    $country     = $User.country
    $telephone   = $User.telephone
    $jobtitle    = $User.jobtitle
    $company     = $User.company
    $department  = $User.department
    $Password    = $User.Password

    #Check to see if the user already exists in AD
    if (Get-ADUser -F {SamAccountName -eq $Username})
    {
        #If user does exist, give a warning
        Write-Warning "A user account with username $Username already exist in Active Directory"
    }
    else
    {
        #User does not exist then proceed to create the new user account

        #Account will be created in the OU provided by the $OU variable read from
        the CSV file
        New-ADUser `
            -SamAccountName $Username `
            -UserPrincipalName "$Username@vlab-consult.local" `
            -Name "$Firstname $Lastname" `

```



```

        -GivenName $Firstname `
        -Surname $Lastname `
        -Enabled $True `
        -DisplayName "$Lastname, $Firstname" `
        -Path $OU `
        -City $city `
        -Company $company `
        -State $state `
        -StreetAddress $streetaddress `
        -OfficePhone $telephone `
        -EmailAddress $email `
        -Title $jobtitle `
        -Department $department `
        -AccountPassword (convertto-securestring $Password -AsPlainText -
Force) -ChangePasswordAtLogon $True
    }
}

```

8.5.2 THIN CLIENTS

- Besides acquiring the thin clients for physical inspection, no configuration was started on the thin clients
- The plan was to deploy Windows and set operate in Kiosk mode for Horizon Connection client use only.

8.5.3 DESKTOP OPERATING SYSTEMS

- The initial plan was to run some VMs on the classroom workstations for desktops, in both Ubuntu and Windows but this was not started

8.5.4 OFFICE SUITE

- This was not started either, the plan was to wait start when desktop operating systems were being deployed
- Plan was to use Microsoft Office 2019 or 365 for demonstration purposes

8.5.5 MOBILE DEVICES

- This was not started, but preliminary research was made as to a potential demo device and local deployment of AirWatch

8.5.6 SOFTWARE DEPLOYMENT VIA GPO

- The GPO for assigning applications applied to computers was configured and was working
- At this point, only chrome putty had been configured but we expect other software to work similarly if MSIs are available.

8.6 SECURITY AND FIREWALL

8.6.1 FIREWALL

- Fortigate 100D Firewall was deployed as the network perimeter firewall for Headquarters (HQ)
- Two OPNSense Firewalls were deployed on two separate VMs on the EXSi Servers as the network perimeter firewalls for the Research and Innovation Center (RIC) Plaza

- High availability was configured by creating virtual IPs and using CARP and Pfsync. An active-backup mode was implemented and tested. Video streaming was done without any breaks.
- One OPNSense Firewall was deployed as the network perimeter firewall for Iqaluit Site. Its dashboard is presented in **Error! Reference source not found..**
- Two Virtual Domains (VDOMs) were configured on the Fortigate Firewall in order to utilize them as internal firewalls in the headquarters.

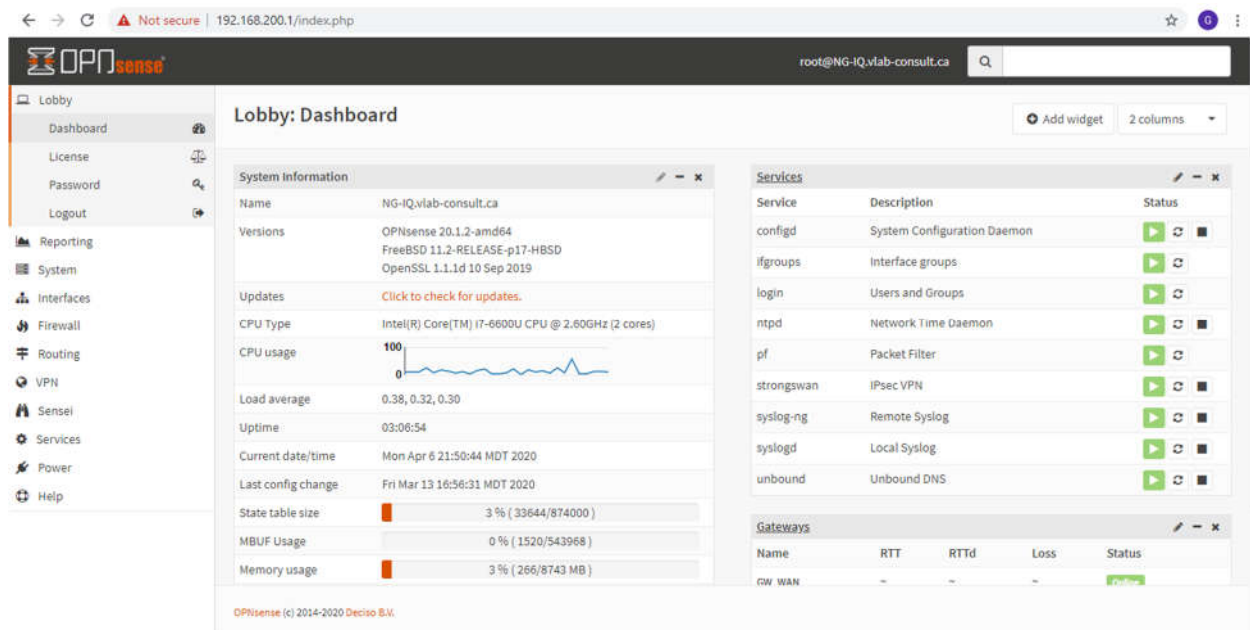


Figure 40 Dashboard of Iqaluit Opnsense

8.6.2 VPN

8.6.2.1 SITE TO SITE VPN

- Strongswan was installed on OPNsense firewalls

- Site-to-Site VPN using IPsec IKEv2 was configured between FortiGate (HQ) and the OPNSense (Iqaluit).
- Site-to-Site VPN using IPsec IKEv2 was configured between FortiGate (HQ) and the OPNSense (RIC).
- As shown in **Error! Reference source not found.**, an encryption of 256 bits AES and SHA 512 hashing algorithm were configured for both phase 1 and 2
- A mutual pre-shared key was configured for authentication and DH group 14 was configured Diffie Hellman key exchange management
- ESP protocol, port 4500 and port 500 were unblocked and other required security policies were configured
- IPv6 site-to-site VPN connection was yet to be deployed

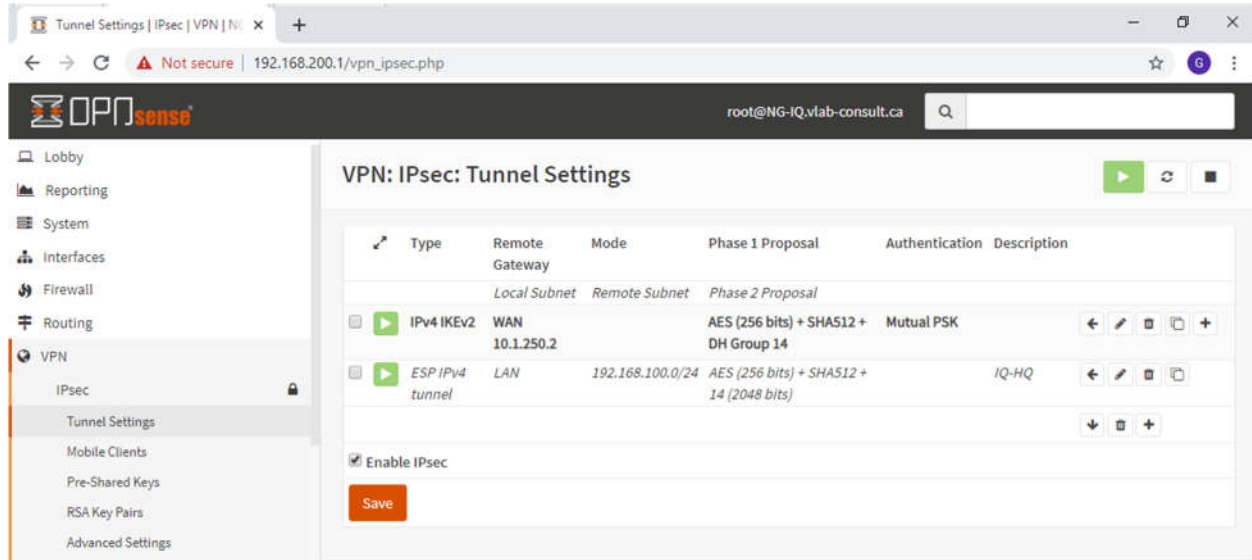


Figure 41 IPSEC IKEv2 Configurations on OPNSense

8.6.2.2 REMOTE ACCESS VPN WITH MFA

- Remote access VPN using SSL VPN was configured on the FortiGate firewall (HQ). The RADIUS and active directory server IP addresses and other required details were configured on the FortiGate firewall.
- A group of RemoteVPNusers was created on the active directory and a firewall policy allowing only remote VPN users was configured on the FortiGate.
- The FortiGate was added to the RADIUS server as a RADIUS client.
- The full tunnel option that allows web portal or FortiClient to be used for logging in, was configured.
- The FortiToken on the FortiGate was also configured and an account (email) was linked to this FortiToken. A FortiToken application was then installed on a phone to generate the OTP that will be used in addition to username and password in order to implement a two-factor authentication.

8.6.2.3 SD-WAN

SD-WAN was configured of Fortigate firewall at the HQ

Two WAN interfaces was used

A policy/rule was configured for real time applications (VOIP, video conferencing etc.) to use the best WAN based on set customized SLA

8.6.3 UNIFIED THREAT MANAGEMENT (UTM)

8.6.3.1 SSL INSPECTION

- Squid was installed on OPNsense firewalls
- Transparent proxy for HTTP (port 3128) and HTTPS (3129) was configured on OPNsense firewalls
- NAT rules were created for HTTP and HTTPS traffic on OPNsense firewalls
- SSL inspection was enabled on the OPNsense firewalls and FortiGate Firewall
- SSL bump was used to exempt sites (financial websites) that won't allow SSL interruption but are legitimate
- The certificates of the OPNsense firewalls were imported to the web browsers as trusted root certification authorities in order for trouble-free browsing

8.6.3.2 WEB FILTERING

- In addition to the squid proxy configuration, a blacklist is downloaded and configured on the OPNsense firewall
- The FortiGuard web filtering was enabled on FortiGate firewall

8.6.3.3 NETWORK ANTI-VIRUS

- Clam AntiVirus (ClamAV) and Internet Content Adaptation Protocol (ICAP) services were installed on OPNSense firewalls
- ClamAV was enabled and signatures were downloaded
- C-ICAP service was then enabled and the filetypes to scanned were updated
- The FortiGuard antivirus was enabled on FortiGate firewall

8.6.3.4 INTRUSION DETECTION AND PREVENTION SYSTEM

- Suricata was installed for IDS/IPS on OPNsense firewalls
- Both IDS and IPS were enabled
- The Hyperscan pattern matcher was selected
- ET Rules were installed and enabled
- The IDS/IPS on OPNSense was applied to the WAN interface
- FortiGuard IPS was enabled for FortiGate firewall

8.6.3.5 THREAT INTELLIGENCE – FORTIGUARD & SENSEI

- The Sensei was installed on OPNsense firewalls
- The Sensei was configured and requires minimum of 8 GB and 4 CPU cores in order to use Elasticsearch otherwise it uses MangoDB.
- The LAN interface was specified, and the cloud servers were selected for Sensei
- The medium restriction was selected for content, web and application filtering for Sensei
- The FortiGuard intelligence was enabled on FortiGate firewall

8.6.4 FIREWALL POLICIES

- Besides the firewall policies for NAT, IPSec VPN, SSL VPN, WiFi access, other necessary firewall policies are yet to be created
- The two VDOM instances was created the call center and a department in the HQ in order to implement microsegmentation but they are yet to be fully configured

- The Distributed Firewall (DFW) for microsegmentation in the virtualized environment haven't been configured

8.7 COMMUNICATIONS INFRASTRUCTURE

8.7.1 VMWARE AIRWATCH

- This was not yet implemented, and the plan was to either use cloud or on-premise if possible.

8.7.2 SHAREPOINT

8.7.2.1 CLUSTERED SQL SERVER BACKEND

- High availability feature on SQL database, in case of one SQL server going down, processes that rely on SQL server could still running due to second redundant server.

8.7.2.2 FRONTEND AND APPLICATION SERVERS

- SharePoint Frontend server would deal with users' credentials and access, Application server would deal with SharePoint integrated applications.

8.7.2.3 WIKI

- A SharePoint wiki site was created and functioning

8.7.2.4 DOCUMENT SHARING

- A SharePoint web interface that allows organization's users to drop and share document
- One Drive client was installed for testing but not fully functional

8.7.2.5 BLOG

- A blog site was created for that enabled publication of articles and comments from users

8.7.3 EXCHANGE

8.7.3.1 DATABASE AVAILABILITY GROUPS

- Microsoft Exchange's database redundancy feature

8.7.3.2 EDGE TRANSPORT SERVER

- An Exchange server installed on the network perimeter, its role is to take care of external users' access to organization Exchange's mailboxes and mail traffic flowing out, and coming back in

8.7.3.3 MAILBOX SERVERS

- Provide Exchange Adminis with an interface to manage organization's Exchange services.

8.7.4 CISCO CUCM

8.7.4.1 PUBLISHER

- First node/server in Cisco CUCM operation, holds the writeable copy of the CUCM's and its database's configurations.

8.7.4.2 SUBSCRIBERS

- Second node/server in Cisco CUCM operation, holds the replicated copy of CUCM's configurations, also provides configurations for platforms associated to CUCM in their respective operations

8.7.4.3 PHONE REGISTRATION

- Process of registering an unregistered phone, by creating a settings node for the phone and associate a phone number to it.

8.7.4.4 I/M SYSTEMS

- Instant messaging systems, live chat through communication software

8.8 MONITORING

8.8.1 SECURITY MONITORING

- Wazuh VM appliance – the security monitoring solution was installed
- The Wazuh manager and agent was configured
- It was used to monitor Windows Server
- It was yet to be fully migrated to the ESXi Servers and the agent hosts

8.8.2 PERFORMANCE MONITORING

- vRealize Operations was installed and tied into vCenter providing a variety of statistics regarding the hypervisors
- Basic statistics were visible in vCenter but more detailed statistics was available on Operations itself

8.8.3 NETWORK MONITORING TOOL

- We installed NetCrunch monitoring system in our network environment. It discovered current available devices and monitor 50% of total devices. However, we implemented monitoring tool which only provide free services for 1 month, we decided to reinstall when one months left for final demonstration.

- Following figure shows that installed monitoring system which monitor our ESXi server configured virtual machines.

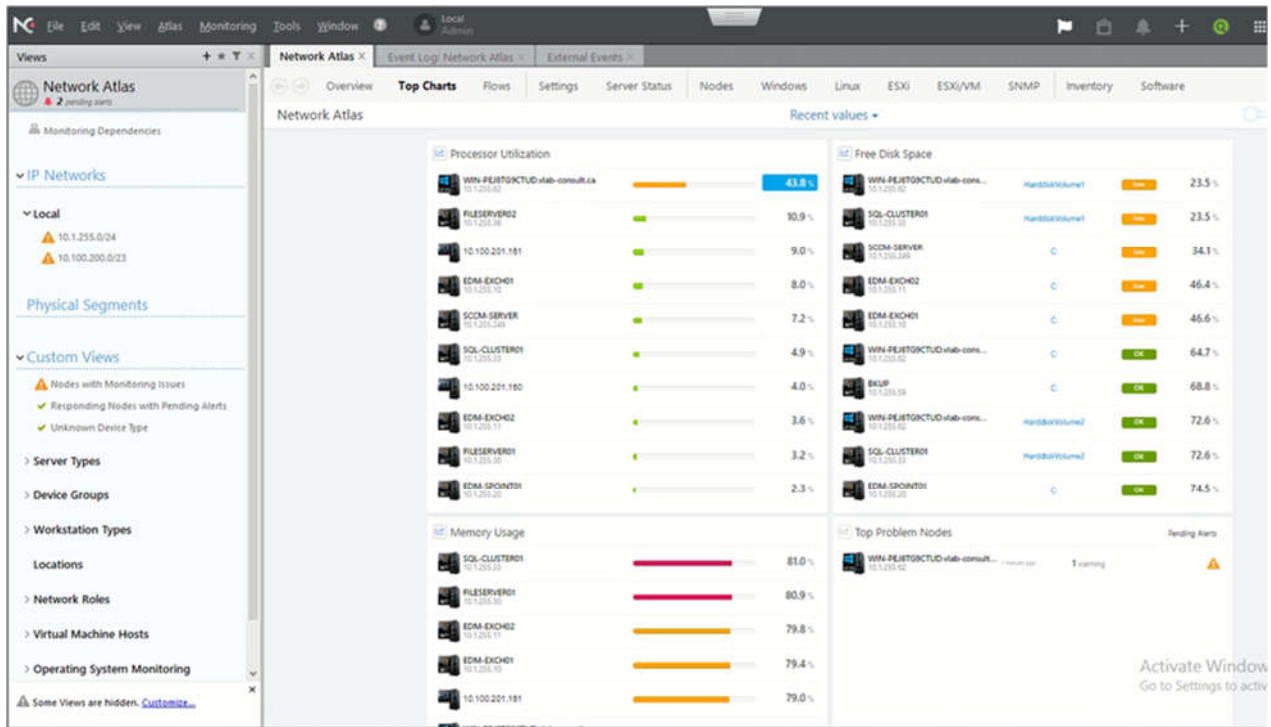


Figure 42 Managed Services by NetCrunch Monitoring Tool

8.8.4 BACKUP SOLUTION

8.8.4.1 SAN CONFIGURATION

- the SAN was reset and initialized, and IPs had been configured
- The plan was to wait on the delivery of additional CAT6 cabling to connect the SAN to BYOD switch and then to a distributed port group on EXSi servers.

8.8.4.2 VEEAM SOLUTION

- The Veeam backup and recovery availability suite was installed on the VM on the data center

- Due to the delay in setting up the SAN, the backup repository configuration was not yet implemented