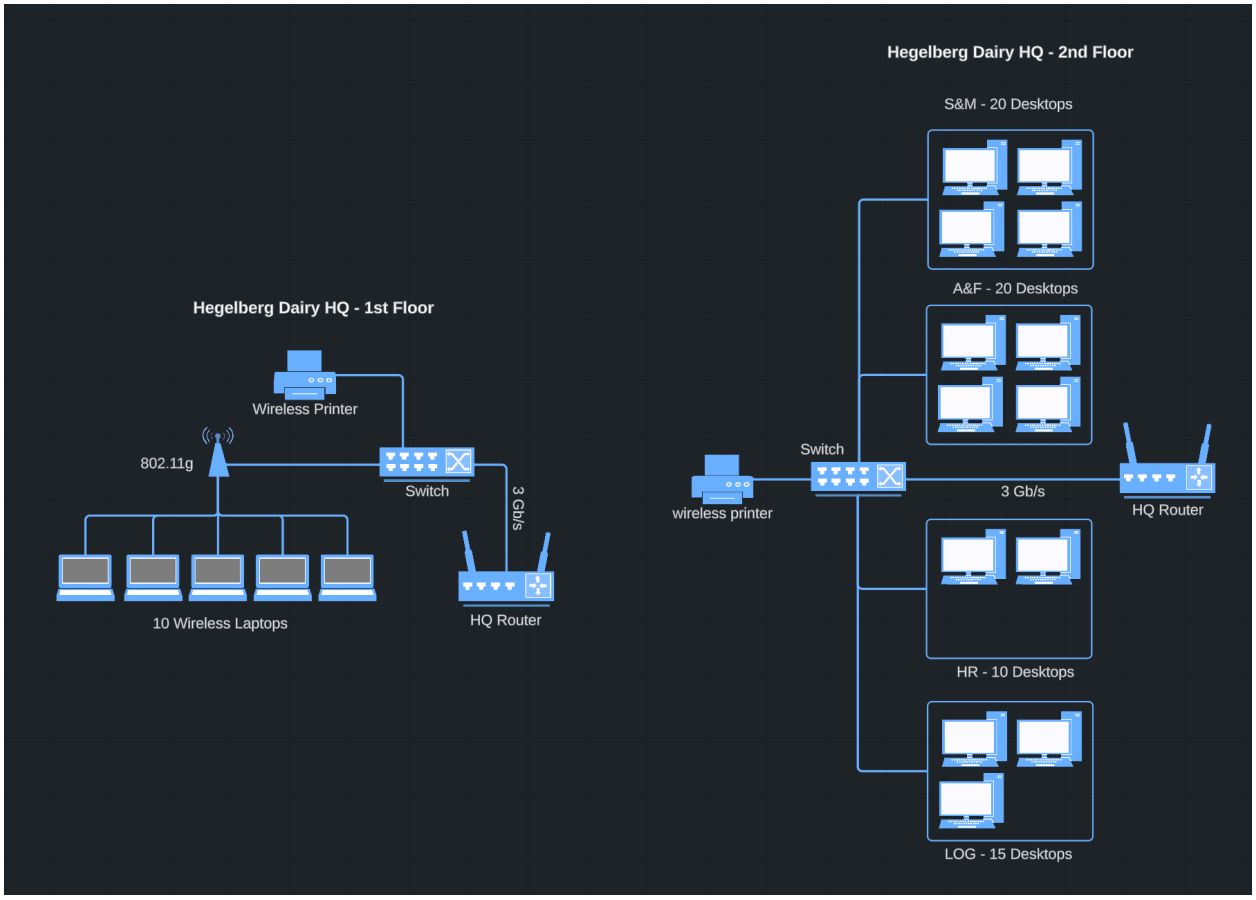
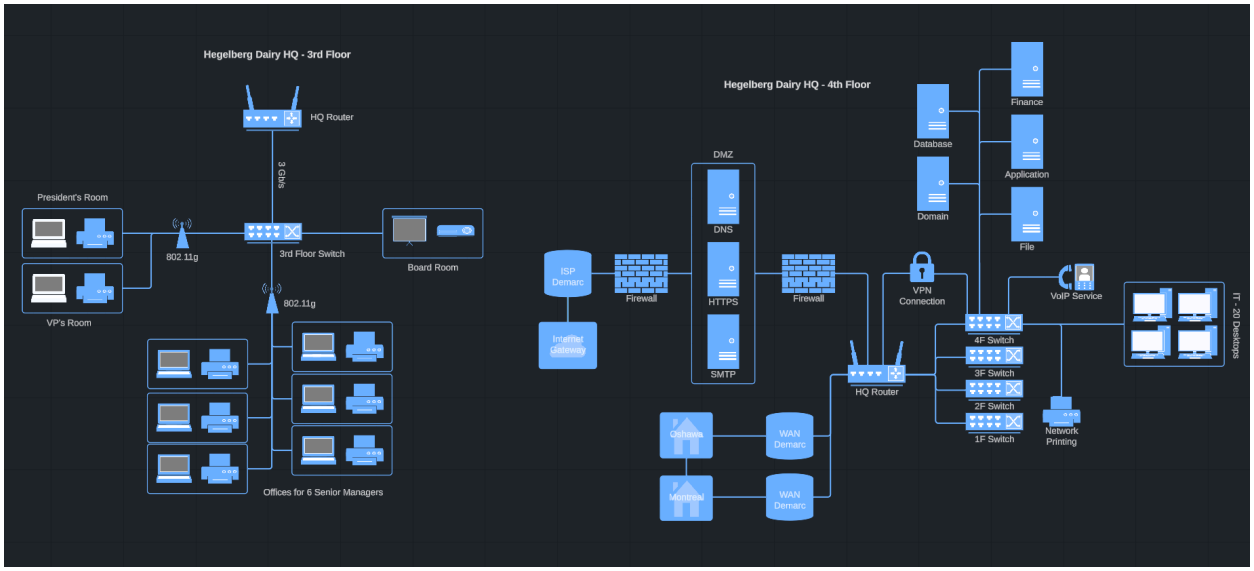
CITM301 DJ0 - IT Infrastructure
Final Group Project
Group 1

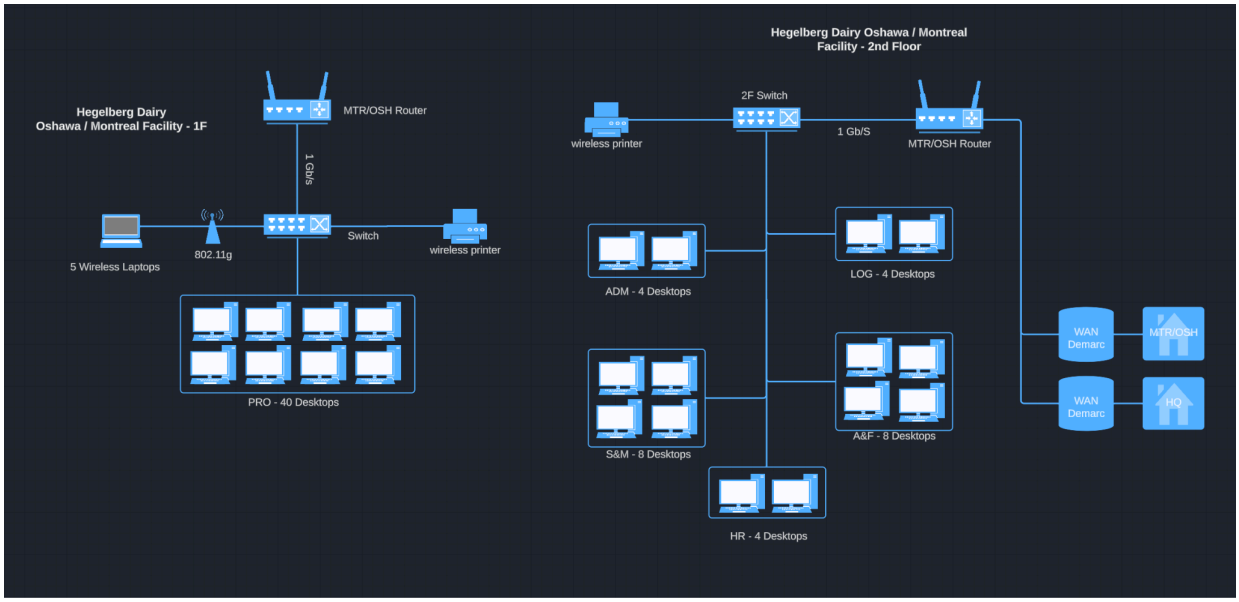
Professor Farid Shirazi
April 6, 2024

Members:
Chabeshan Kandiah (500961136)
Luxsan Navayogaratnam (501195053)
Luis Alitagtag (501110330)
Rommel Barbieto (501033054)

1) Draw a diagram for the above scenario using a drawing program such as Microsoft Visio - ***Luis***







2) Provide a LAN solution for each location connecting computers and printers. Explain all connectivity devices used by your network infrastructure from cabling to routing - ***Chabeshan***

I'll describe the LAN solution that links PCs and printers at each location (HQ, Oshawa, and Montreal), as well as the connectivity devices incorporated into the network architecture.

HQ (Headquarters):

LAN Solution:

Production Department (First Floor):

- Use Ethernet cabling to connect all desktop PCs and portable wireless laptops that are necessary for production line operations.
- Connect network-attached printer/copier/fax to the LAN.

Sales & Marketing, Accounting & Finance, HR, Logistics Departments (Second Floor):

- Connect each department's desktop computers with Ethernet cables to the LAN.
- Install network-attached printers for each department.

Executive Offices (Third Floor):

- Connect desktop computers in the executive offices to the LAN using Ethernet cabling.
- Ensures that there is wireless internet connection used by administration personnel.
- Utilize network-attached printers for office use.

IT Department (Fourth Floor):

- Interlink all computer systems and servers via an Ethernet cable system.
- Enable connectivity for network-attached printers.
- Ensure high-speed LAN connectivity so as to facilitate efficient IT operations.

Connectivity Devices:

1. **Ethernet Cabling:**

- To connect desktop PCs, servers, and printers across the building, use Cat6 Ethernet cables.
- Ensure high-speed data transmission and minimal crosstalk for optimal performance.

2. **Switches:**
    - To connect devices to the LAN, install high-speed switches on every floor.
    - Make use of managed switches with trunk ports to improve VLAN segmentation and network administration.
3. **Wireless Access Points (APs):**
    - Install wireless access points (APs) on the third floor to give laptops wireless connectivity.
    - Ensures that there is sufficient bandwidth and coverage for smooth wireless connectivity.
4. **Print Servers:**
    - Set up print servers to effectively manage printers connected to networks.
    - Ensure proper print queue management and security protocols.
5. **Router:**
    - Install a router to facilitate communication between the LAN and external networks.
    - Put in place security measures including a firewall to prevent unwanted access to the network.

Facilities in Oshawa and Montreal:

LAN Solution:

Production Department (First Floor):

- Use Ethernet cabling to connect all desktop PCs and wireless mobile laptops for production control.
- Set up printers connected to a network for usage in production.

Other Departments (Second Floor):

- Use Ethernet cabling to link each department's desktop PCs to the LAN.
- Set up printers connected to a network for usage in each respective department.

Connectivity Devices:

Ethernet Cabling:

- Cat6 Ethernet cables are used to connect devices within each facility.

Switches:

- Install switches on each floor to connect devices to the LAN.
- Ensure proper segmentation and VLAN configuration for network optimization.

Wireless Access Points (APs):

- Install wireless access points (APs) as needed to provide wireless connectivity..
- Ensures that there is sufficient bandwidth and coverage for dependable wireless connectivity.

Print Servers:

- Configure print servers to effectively handle printers that are connected to networks.
- Implement print policies and access controls to manage printing resources effectively.

Router:

- Install routers for each facility to manage network traffic and ensure connectivity.
- Implement security measures such as firewall and VPN to safeguard the network infrastructure.

Other connections/connectivity devices and explanations:

Type 1 Hypervisors:

- To virtualize computing resources, use Type 1 hypervisors on IT department servers.
- Permit efficient resource allocation and management for various server tasks.

Demarcation Points:

- Establish demarcation points at the entry point of the building for clear separation between internal and external network responsibilities.
- Implement demarcation devices to mark the boundary of the network service provider's responsibility.

CAT6 Cables and RJ-45 Connectors:

- Because of their large bandwidth capacity and little interference, CAT6 cables are preferred for high-speed data transfer.
- To ensure uniform connectivity for Ethernet devices, terminate CAT6 cables using RJ-45 connectors.

Optical Ports:

- Attach fiber optic cables to network devices via their optical ports to guarantee quick and long distance data transfer.

MDF and IDF:

- Install Main Distribution Frames (MDFs) to terminate and connect backbone cabling on every floor.
- Connect horizontal cabling from particular rooms or departments to the MDF using the Intermediate Distribution Frame (IDF) to facilitate effective cable management and troubleshooting.

Overall, each location can ensure efficient connectivity for computers and printers while maintaining network security and performance by implementing these LAN solutions and utilizing appropriate connectivity devices.

3) Provide automated IP address solutions for the above locations using a DHCP server (5%). Note: You need to explain how this server will assign IP addresses to its clients and how this

server is related to the DNS server. ***- Luxsan***

In order to provide an automated IP solution for Hagelberg Dairy Inc, a Dynamic Host Configuration protocol (DHCP) server will be needed at the main headquarter in Mississauga as it spans in multiple locations. For example, the DHCP server dynamically assigns IP addresses, default gateways and other network parameters to client devices in all locations, including Oshawas and Montreal.

The DHCP appoints IP addresses to hosts in a client-server model through four steps known as **DORA** (Discover, Offer, Request, Acknowledge). The first step is **Discovery**, where the DHCP clients send out a broadcast message over the network in search of DHCP servers. In this step, relay agents on routers, firewalls, and other gateways play a critical role. For example, they monitor the communications and make certain that DHCP messages from clients are routed to the DHCP server, which enables clients from various locations, including those behind firewalls to successfully communicate with the DHCP server to obtain IP addresses. In the second step, **Offer**, upon receiving the discovery message, the DHCP server sends an offer message back to the client. This message contains the IP address that the server can provide to the client with a lease duration of eight days. In the third step, **Request**, upon receiving the offer, the client sends a request message to the DHCP server for the offered IP address, suggesting that the client wishes to accept the offered IP address. In the final step, **Acknowledgement**, the DHCP completes the process by sending an acknowledgment message to the client. This message confirms that the IP address has now been officially assigned to the client, enabling them to connect to the network. The DHCP server and the Domain Name System (DNS) are related since the DHCP server can notify the DNS server of a new IP address. This update uses Dynamic DNS (DDNS), which is a DNS extension that updates IP addresses for domain names in real-time.

4) Provide a secure remote connectivity solution among all locations as well as the main office with XYZ-bank by using an IPsec-based VPN ***- Luxsan***

Remote connectivity enables users the ability to connect to a private network from a different location, which can be anywhere outside of the network's physical location. This also includes users being able to access network resources, data, applications, or any other services without having to be physically present in the location where the network is located. This gives employees the luxury to work from home or other locations while still having a secure connection. Remote Connectivity in a firm can be exceptionally beneficial as it is proven to increase productivity, cost efficiency, flexibility, healthier employees, etc. With that being said, businesses can employ numerous employees from numerous countries, which enables activities to function around the clock by tapping into several time zones, hence increasing production and operational efficiency. However, to achieve this, a Virtual Private Network (VPN) will be needed. A VPN creates a digital connection between your personal device and a remote server that is owned by a VPN provider, which creates a point-to-point tunnel that encrypts your personal information, hides your IP address, and allows you to bypass internet website blocks and firewalls. They allow users to exchange data over shared or public networks as if their computers were directly connected to the private network. This implies that employees can connect to their company's network safely from anywhere in the world. In this case, using an IPsec-based VPN is essential as it enables secure internet communications across an IP network by authenticating and encrypting each IP packet. IPsec-based VPN

also has enhanced security protocols. For example, if data were to be intercepted, it would still be encrypted and inaccessible without the proper decryption key, protecting sensitive information from unauthorized access. Another secure reason to use an IPsec-based VPN is that it is primarily used for site-to-site connectivity which is essential since Hegelberg needs to be connected to more than one branch (Mississauga, Montreal, Oshawa) and the XYZ- Bank. All in all, using an IPsec-based VPN is crucial for Hegelberg Inc. as it ensures secure data transmission and reliable remote access across all branches and with XYZ-Bank. Not only does this approach strengthen the company's network security, but also greatly increases the workplace environment's flexibility and productivity.

5) Provide a VoIP solution between the HQ and other locations. ***- Luis***

Hegelberg Dairy HQ must consider several things before providing a Voice over Internet Protocol solution between HQ and other locations. They must ensure that their network infrastructure has sufficient bandwidth (3Gb/s backbone at the HQ and 1Gb/s backbone at the other locations) to accommodate the increased VoIP traffic without interfering with other network services and impairing service quality.

We recommend designing Quality of Service (QoS) policies to regulate traffic, prevent excess bandwidth usage, and maintain VoIP performance with limited network capacity. Hegelberg Dairy may also reinforce network security by using a VLAN or physical network to isolate the voice traffic from the data network. This segmentation makes it easier to monitor and manage the network, such that if the VoIP system is threatened, the attack will not compromise the rest of the network. To increase network security, they may also consider implementing encryption methods like virtual private networks and end-to-end encryption to prevent against common VoIP threats like eavesdropping and phishing attempts.

Hegelberg Dairy should also install a VoIP server on the third floor of the headquarters to act as a central point for handling voice communications, including call routing, and voicemail. On that topic, they may want to consider upgrading or adding more access points to handle the extra traffic and ensure coverage.They should also consider giving staff with IP phones equipped with softphone programs that allow them to make and receive calls directly from their laptops. Staff in general must be instructed on how to operate the VoIP system, as people play an important part in IT infrastructure.

6) Provide a secure Web as well as email services to all employees, suppliers, and other stakeholders. Place these servers along with the other related servers (e.g., VPN server) in a DMZ area. Note: The DMZ is connected to the Internet through a firewall (20%). ***- Chabeshan***

Establishing a Demilitarized Zone (DMZ) where servers for the Web and email, along with other relevant servers like VPN servers are located, is crucial to providing secure Web and email services to all workers, suppliers, and stakeholders while ensuring their protection. Here's a quick overview of the setup:

DMZ Configuration:

- A network segment that is separated from the internal network but still accessible from the internet is known as the DMZ. It serves as a barrier between the internal network and the internet.

- Include the DNS server, email (SMTP), VPN, Secure Web (HTTPS), and any other servers that are accessible to the public in the DMZ.
- These servers, which serve all three sites as well as external stakeholders, are all virtual servers running on one machine that is connected to the router on the fourth level of the headquarters.
- The DMZ safeguards the headquarters router from potential internet attacks
    - Since a WAN point-to-point link between the branches and the headquarters exists, no protection against the branch traffic is required.

Firewall:

- Via a firewall, link the DMZ to the internet. The firewall needs to be set up to prevent unwanted access to other internal resources while permitting the specialized traffic required for email, VPN, and online services.
- Stateful firewalls filters permit/deny traffic flow or sessions which means that it enables the private network to be accessed from the Internet.
    - Firewall is installed between the virtual servers and the ISP
    - The virtual servers are situated in the DMZ for this reason
- Set up the firewall's Access Control Lists (ACLs) to regulate traffic entering and leaving the DMZ.
- There is an NIPS (network-based intrusion prevention system) for further security.

Web Server:

- The company website and any web-based apps should be hosted on a secure web server (like Apache or Nginx) that has been installed and configured in the DMZ.
- Use SSL/TLS encryption along with the HTTPS protocol to ensure safe communication between clients and the web server.
- Update and fix the web server frequently to reduce security flaws.

Email Server:

- Set up an email server in the DMZ to handle incoming and outgoing emails.
- Use encryption methods like SSL/TLS and SMTPS to send emails securely.

VPN Server:

- Set up a VPN server (such as OpenVPN or IPSec) in the DMZ to allow stakeholders, suppliers, and staff to have secure remote access.
- Use robust authentication techniques such as client certificates, two-factor authentication (2FA), and username/password.
- For secrecy and integrity, encrypt VPN traffic using protocols like IPsec or SSL VPN.

Security Measures:

- Update all software and servers often to fix known vulnerabilities and improve security posture.
- Put intrusion detection/prevention systems (IDS/IPS) in place to keep an eye out for and prevent malicious activity occurring inside the DMZ.
- Set up systems for logging and monitoring to keep an eye on and examine server activity, network traffic, and security occurrences.
- To find and fix security flaws, conduct routine penetration tests and security audits.

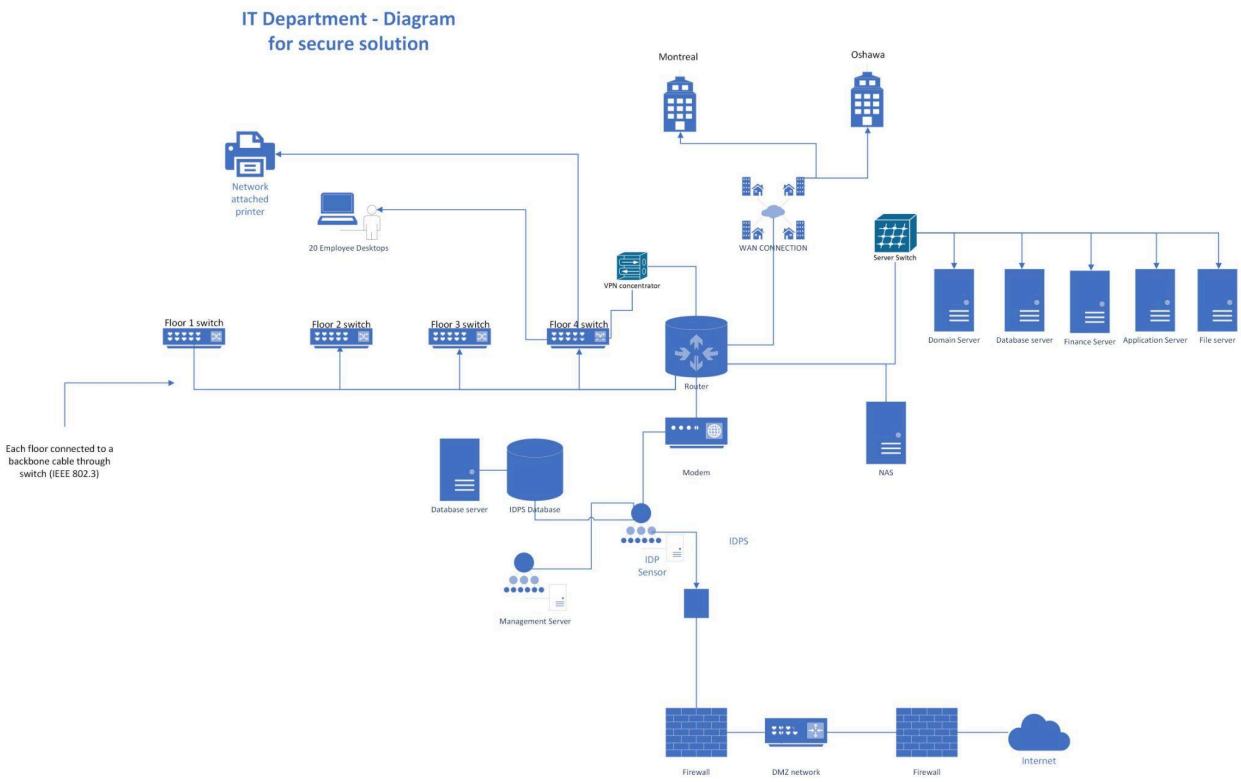
By following these guidelines, you can establish a secure DMZ environment to host web, email, and VPN services, ensuring data confidentiality, integrity, and availability for employees, suppliers, and stakeholders.

7) There are five main LAN servers located in the IT department: A domain server (authentication server), a Database server, a File Server, an application server, and a Finance server. These servers provide services to all employees as well as managers in these locations.

You need to provide a secure solution for these servers. Use a graphical presentation for your solution and explain how these servers are secured. (20%) - ***Rommel***

In order to provide these servers a secure solution across all the locations of the HQ, Oshawa and Montreal, we must apply these actions:

- Firewall: To deny access and potential threats.
- VPN: To keep communication between locations over the internet safe and secure. We will need a VPN concentrator because Hegelberg HQ is operated as an enterprise and that the company has over 100 employees. This will help build multiple VPNs for them.
- Encryption: Keep sensitive information safe by encrypting it.
- IDPS: For monitoring any activities that are suspicious. This will help monitor and analyze network traffic if there is any suspicious activity.
- Backup: Backing up data if there is a potential loss.
- Employee habits of making sure their sensitive data is safe. Example: Changing password frequently.



The diagram above represents a comprehensive solution across the areas and locations of the fourth floor of Hegelberg Dairy HQ. Implementing a combination of VPN, IDPS, a NAS, and Firewall, a safe and secure solution is provided to ensure the safety and security of our employees and data. A VPN is essential so that locations can communicate with each other safely. Since the HQ is operating as an enterprise, there will be extremely high volumes of workers and users. So a VPN concentrator is used because of its reliable solutions where its dedicated software supports multiple VPN connections. IDPS is important because if there is any suspicious activity, IDPS will handle it via monitoring and analyzing. Backup frequently is a great way to prevent any loss of data through a NAS; providing a secure solution for these servers does mean it is 100% secure. So to ensure that data is being prevented from being lost, frequent backups are recommended. Firewall is important because it is a network security where it monitors any network traffic and determines if it should allow or deny certain traffic depending on security rules.

References

What Is the Dora Process? (With Definition and Benefits) | Indeed.Com ..., in.indeed.com/career-advice/career-development/dora-process.

"What Is a DHCP Server?" *Infoblox*, 17 Jan. 2024, www.infoblox.com/glossary/dhcp-server/#:~:text=A%20DHCP%20Server%20is%20a,to%20broadcast%20queries%20by%20clients.

What Is DDNS? - Dynamic DNS Explained - AWS, aws.amazon.com/what-is/dynamic-dns/.

"What Is DHCP: Relay Agent: Dora Process - A Complete Guide." *PyNet Labs*, 19 Mar. 2024, www.pynetlabs.com/what-is-dhcp/#:~:text=DORA%20stands%20for%20Discover%2C%20Offer,to%20connect%20to%20the%20network.

Schneider, Stefanie. "DHCP and DNS: Introduction, Functions and Options." *Univention*, 22 Mar. 2023,www.univention.com/blog-en/2019/03/brief-introduction-dhcp-dns/#:~:text=DHCP%20and%20DNS%20are%20two,be%20found%20by%20their%20names.

"What Is Remote Access? How Does It Work?" *Fortinet*,www.fortinet.com/resources/cyberglossary/remote-access#:~:text=A%20remote%20access%20connection%20gives,device%20with%20another%20user's%20device.

16 Benefits of Work from Home for Employers | Indeed.Com, www.indeed.com/career-advice/career-development/benefits-of-work-from-home-for-employers.

"What Is a VPN? Why Should I Use a VPN?: Microsoft Azure." *Why Should I Use a VPN? | Microsoft Azure*, azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-vpn#:~:text=A%20VPN%2C%20which%20stands%20for,and%20firewalls%20on%20the%20internet.

Dolnicek, Lukas. "IPsec VPN Explained: How IPsec Works: IPsec VS SSL." *RSS*, GoodAccess, 2 Aug. 2023, www.goodaccess.com/blog/ipsec-vpn#:~:text=IPsec%20VPN%20securely%20interconnects%20entire,browser%20to%20a%20particular%20application.

What Is IPsec? | How IPsec Vpns Work | Cloudflare, www.cloudflare.com/learning/network-layer/what-is-ipsec/.

"Site-to-Site VPN Overview." *Moved*, docs.oracle.com/en-us/iaas/Content/Network/Tasks/overviewIPsec.htm#:~:text=Site%2Dto%2DSite%20VPN%20provides,the%20traffic%20when%20it%20arrives.

Cisco. (2024, February 23). *What is a Firewall?*. Cisco. https://www.cisco.com/c/en_ca/products/security/firewalls/what-is-a-firewall.html

Modules, P. by Genuine. (2023, November 28). *Genuine modules*. Genuine Transceiver Modules. https://www.genuinemodules.com/what-is-a-server-switch_a1599#:~:text=A%20server%20switch%2C%20also%20known%20as%20a%20data%20center%20switch,equipment%20within%20a%20data%20center.

Pecha, P. (2023, August 1). *VPN concentrator explained*. RSS. https://www.goodaccess.com/blog/vpn-concentrator-explained#:~:text=In%20Summary-,What%20Is%20a%20VPN%20Concentrator%3F,number%20of%20simultaneous%20Internet%20connections.

Vigderman, A. (2024, March 4). *What is a VPN concentrator?*. Security.org. https://www.security.org/vpn/what-is-a-vpn-concentrator/#:~:text=If%20you%20run%20a%20large,you%20need%20a%20VPN%20concentrator.

What is a switch, router, Gateway, Subnet, firewall & DMZ? (guest blog). Certified Wireless Network Professional CWNP. (n.d.-a). https://www.cwnp.com/what-is-a-switch-router-gateway-subnet-firewall-dmz/

What is a switch, router, Gateway, Subnet, firewall & DMZ? (guest blog). Certified Wireless Network Professional CWNP. (n.d.-b). https://www.cwnp.com/what-is-a-switch-router-gateway-subnet-firewall-dmz/

Doan, A. (2024). How Does VoIP work? *The Beginner's Guide to VoIP Phone Systems*. Nextiva. https://www.nextiva.com/blog/how-does-voip-work.html