n

Sibusiso Sekhoto ST10125398

NWAR5122 Final Poe

NWAR5112

Final Poe

FINAL POE

NETWORK DESIGN DIAGRAM WITH VISIO:

NB: Please zoom in:



This is my explanation of my network diagram as we can tell this is a Ring topology In a ring topology, every node is connected to two other nodes, forming a loop. Data flows from one node to the next in a continuous sequence we selected this topology because we are using fibre optic cables for connection that will allow for a fast ,minimal interference and reliable transfer of data.

And as you can see we have a separate network for the main network from the rest of the network. Why? This is because the guest Wi-Fi and remote access can’t be of the same connection so we have firewall as well as switches that help with as well as the employees they are all separate in case of a breach the hacker cannot gain or escalate their attack .I further isolated the main office of that includes the 4 computers and the fail over servers are in that department in case the network fails that was my best way to understand and design it .

**So we have these security setting implemented**.

**Remote access:**

For remote access clients we have them directly connected to the internet to the companies network and we have a modem as well as firewall that will protect the company from unauthorised access we will get to the firewall in a few .Clients can connect using laptop, desktop or smartphone in order to complete their work for remote access we have the following security measures implemented for the protection of the network.

* Use strong passwords.
* Use Two-factor authentication.
* Updated software.
* Restrict access using firewalls.
* Enable Network Level Authentication.
* Limit users who can log in using Remote Desktop

I have utilized the following for secure remote connection:

<https://learn.microsoft.com/en-us/windows-server/remote/remote-access/remote-access>

* Used a virtual private network (VPN): VPN encrypts internet traffic and secures the connection between the employee's device and the company's network. It prevents unauthorized access and protects sensitive data.
* Secure home Wi-Fi: Employees should secure their home Wi-Fi network with a strong password and encryption. Encouraged them to keep the Wi-Fi router firmware up to date and change the default admin credentials to prevent unauthorized access.
* we also have to Provide company-issued devices: Ensure that employees have company-issued devices that have updated security software, firewalls, and encryption. This reduces the risk of using personal devices that may have weaker security measures.
* Regular software updates and patches: Encourage employees to regularly update their operating systems, applications, and antivirus software as these updates often include security patches to address vulnerabilities.
* Strong and unique passwords: Encourage employees to use strong, unique passwords for all their accounts and avoid reusing them across multiple platforms. They should also consider using a password manager to securely store their passwords.
* Restricted access to sensitive data: Implement access controls and permissions, ensuring that employees only have access to the data and systems necessary for their job roles. And we will Regularly review and update user privileges to maintain least privilege access.
* Monitor and log activities: Implement logging and monitoring solutions to track and identify any unusual or suspicious activities. This helps in identifying security incidents and provides a way to respond in a timely manner.

<https://www.cloudwards.net/best-remote-access-vpn/>

By implementing these measures, you can help ensure secure access for employees working from home and protect sensitive company data.

So we have the modem the VoIP, modem and the router for internet access after the firewall why?

Because they bring in the external connection from the internet as well as internal connection .So we need to have the firewall before these components so we can assure a safe connection of network and connection to our ISPs but then we know security has a lot of security risks so having firewall rules that block external traffic ensures we are protected from the following .

* Malware. Malware (or malicious software) is a cyber-attack that “executes unauthorized actions on the system”.
* Viruses. Although there are different types of viruses, all are programmed to harm your hardware so systems need to be protected.
* Ransomware.
* Phishing. .
* Password Hacking.

Firewall

Firewall segmentation: Firewalls are deployed inside a network or data centre to create internal zones to segment functional areas from each other in order to limit attack surfaces, thereby preventing threats from spreading beyond a zone. For example we have separated the central file server from the network and connected to a switch this allows us to configure the central file server we have configured it only to the LAN and not the internet for extra security precautions and safety.

And we have configured the file server like this for extra security.

* Regularly update server software: Keep all server software, including the operating system and applications, up to date with the latest security patches and updates.
* Implement strong access controls: Create individual user accounts for each person who needs access to the server and enforce strong passwords. Ensure that each user has the appropriate level of access based on their responsibilities.
* Use a firewall: we have Configured the firewall to restrict access to the server and only allow necessary connections.
* Enable encryption: Enable encryption for sensitive data, both in transit and at rest. using technologies like SSL/TLS for network connections and full-disk encryption for storage.
* Employ intrusion detection and prevention systems (IDPS): Install IDPS software to detect and prevent unauthorized access and potential attacks. Regularly review the generated logs for any suspicious activity.
* Implement strong backup and recovery procedures: Regularly back up the server data and ensure backups are stored securely in an off-site location. Test the backups periodically to ensure they are functioning correctly, and have a documented recovery plan in place.
* We have also disabled unnecessary services and ports: so we Identified and disabled any unnecessary services or ports to minimize potential attack vectors. And Only kept the necessary services for the server's functionality.

.

So in our network we have a proxy firewall implemented why ?

* A proxy firewall acts as a gateway between internal users and the internet. It can be installed on an organization's network or on a remote server that is accessible by the internal network. It provides security to the internal network by monitoring and blocking traffic that is transmitted to and from the internet. So as the security admin we set rules that meet the standards of the business like blocking certain sites or IP addresses.
* Improved security: A firewall proxy acts as a barrier between our network and the external network, filtering and monitoring incoming and outgoing traffic. It can block unauthorized access attempts, prevent malware and malicious data from entering our network, and protect sensitive information from being leaked.

<https://www.fortinet.com/resources/cyberglossary/proxy-firewall#:~:text=A%20proxy%20firewall%2C%20also%20known,or%20inspect%20application%20protocol%20traffic>.

* Access control: A firewall proxy allows us to control and restrict access to specific websites, applications, or services. We have set up rules to allow or deny access based on IP addresses, domain names, or other criteria. This can help prevent employees from accessing potentially harmful or non-work-related websites, improving productivity and reducing security risks.
* Enhanced privacy: By implementing a firewall proxy, we can hide our network's IP address and location, making it more difficult for attackers to target our network.
* Bandwidth management: A firewall proxy can optimize network performance by caching frequently accessed websites or content. This helps reduce bandwidth usage, speeds up website access, and improves overall network efficiency.
* Traffic monitoring and reporting: Firewall proxies often provide detailed logs and reports on network traffic. This can help us identify potential security threats, track user activities, and generate insights for network optimization and troubleshooting purposes.
* Overall, implementing a firewall proxy adds an additional layer of security, control, and management to our network, ensuring a safer and more efficient network environment for your organization.

**Backup procedures we have in place are:**

We have a data backup for the file server as everything is stored on the and used for the companies exchange of information as well as its storage of the information so in order to backup it up correctly we are going to:

2. we have `AWS cloud-based backups, external hard drives we will utilise Toshiba X300

. That we have implemented because these are easy to handle and the data is easily backed up in case of a failover.

3. Establish a backup schedule: we are going to have 3 monthly backups just to ensure everything is running smoothly as we going to have the data accessed on the regular as the data is an enormous size.

Onna use

4. Automate backups: we are going to use system centre data protection manager from Microsoft and azure backup .Use backup software or tools that allow you to schedule automatic backups. This reduces the risk of forgetting to perform regular backups.

.

6. Test backups regularly: Regularly test your backups to ensure that the data can be successfully restored when needed. This will verify the integrity of your backups and allow you to address any issues promptly.

<https://webuyusedtape.net/2022/07/14/how-many-servers-do-you-need/>

9. As the business grow we will Regularly review and update backup procedures . This includes considering changes in data volume, technology, and storage options.

Lit of hardware:

* VPN onion
* System centre data protection manager
* Toshiba X300
* 13 dell desktops
* 3 hp laptops
* 2 Samsung smartphones
* Fibre optic cables
* 3 cisco switches
* 3 Fortinet routers
* 1 Huawei Wi-Fi router
* 2 IBM servers
* 1 Lenovo modem
* Proxy firewall software

**Design justification:**

My design meets the business plan because all 20 employees are connected and as well as the remote workers have access to a secure network without any fault. The remote access is secure as well as the data flow and the security measures ensure that the company and its assets are secure. The installed software and the choices of the equipment meet the standards of the network without any fault .The routers ,switches and wireless access points are all included and they are properly configured to keep the business safe without any fault or vulnerabilities the IDS in place ensure that the company is being alerted of any threats that may come from any outside threats. Also show the flow of the network from the arrows being used and is understandable.

The backup procedures are clearly stated and explains how they can be met and how they are configured.

My design meets requirements as all the minimum are meant and clearly stated throughout the poe or the network design itself as all hardware and software components are included and clearly listed for us to see understand. The external void and internal void and how they communicate is shown and explained to us .Wireless access points are clearly stated and shown the configuration details are all included and meet the minimum requirements for the business of 20 employees is clearly stated to us.

The design shows how these devices are going to communicate over the internet with the greatest of efficiency and provide a good flow of the network in this diagram and understanding of it is important

Reference list:

<https://learn.microsoft.com/en-us/windows-server/remote/remote-access/remote-access>

<https://www.cloudwards.net/best-remote-access-vpn/>

<https://www.fortinet.com/resources/cyberglossary/proxy-firewall#:~:text=A%20proxy%20firewall%2C%20also%20known,or%20inspect%20application%20protocol%20traffic>.

<https://webuyusedtape.net/2022/07/14/how-many-servers-do-you-need/>