Devices and use

1. Router the router is used to direct incoming and outgoing traffic from the network. The router can be used a first stop to securing the network and can be set up to filter out some amount of unwanted traffic. If deemed necessary we can use it to block specific traffic and sites/IPs from our network.
2. Firewall will be used as a more specific way to block unwanted traffic to the network from the internet, or from the network to the internet. We can use an Application-Aware firewall with IDS/IPS capabilities to help protect the network from being attacked or allowing a compromised computer from sending anything out of the network until it can be located and shutdown.
3. Switches will be used to separate the traffic internally by identifying MAC addresses and ports. The switches will forward packets within the network and decide if the traffic should be sent to an internal machine, a server located in the DMZ or if the request should be sent to the gateway to the internet. This can also help the Network Administrator and other networking professionals to monitor the traffic on the network.
   The switches can also be used to break the network into VLANs and help to filter/limit traffic from different groups of authorized individuals.
4. VPN Concentrator will used for anyone who needs to access work materials over wireless or through the use of a home computer. This is device will allow an encrypted connection to the network for authorized individuals and will help to protect any information that is transmitted over the connections from being viewed by unauthorized individuals.
5. Proxy Servers will be used for access to the servers or the internal network. The proxy will help to help the identity of the different devices on the network and use its own IP in place of the network device. This helps to hide the amount and type of devices being used on the network. Proxies can also be used to help filter traffic that passes through it and will be another layer of network security.
6. Wireless APs can be used to help support employees who need to be more mobile within the building and also allow visitors the ability to use an internet connection while on company property. These will be separated into Public and Private VLANs for visitors and employees so that visitors can be allowed no access to internal devices and employees can be allowed limited access to network devices. Employee access over the wireless can be controlled better through group authentication rules. The Private Wireless AP can also be given more VLANs so that employees are better grouped and will provide another layer of protection.

First Principles

1. Domain Separation in this network is carried out through the use of VLANs to keep different users and interior systems separated from each other. It is also done through the use of a DMZ for the exterior facing servers to help minimize the attack surface that can be seen by the public.

4. Least Privilege will be handled through the grouping of the different users. The groups will only be able to access portions of the network and data that are essential to their job duties.

5. Layering, if you view the diagram is easily spotted. There are many layers of security that a connection must go through to access different areas and other resources connected to the network.

6. Abstraction and obscuring the resources on the network is done through the use of a proxy and reverse proxy server. These two machines hide the amount and types of systems that are connected to the network from any outside intruders.

8. Modularity in theory will be an easy step because the network devices will be bought from common vendors. So in order to plan for the future and also to make sure that if a device goes down, we can replace it, the devices will be purchased with extra available option.

9. Simplicity of Design as you can see it is not a difficult network to work through. The design is straight forward with different layers of security to protect it.

10. Minimization is carried out through the use of the DMZ. The only portion of the network that can be seen by the outside world is the three servers.