Unit 4 Activity

1. I would set up the firewall so that everything that comes in and out needs to be approved, so that the company is aware of the incoming or outgoing traffic. I would have ports open for some things (DNS, NTP, 80, 443), but it would be as restrictive as possible.

2. I would choose an unmanaged switch as it doesn't require a lot to get up and running and can work out of the box. I would have 802.1x authentication set up, so that only the people who should be connecting to the network are connecting to the network.

3. To secure wireless devices, I would need to set up a good router. I would even consider getting a VPN router. It works just like having a VPN on your computer, but just built into the router instead. This would encrypt all the data going between the devices that are connected to the network, which is very beneficial, especially for when it comes to transmitting sensitive and confidential information. Also, the passwords need to be top-level secure. Numbers, symbols, and everything included.

4. I would set up a VLAN. A VLAN is a custom network created from one or more existing LANs. It lets devices from more than one network combine into one network. A lot of businesses use one to prioritize voice traffic for their telephony system over data traffic. They also use one to segment private and public networks. I would also make sure that all equipment and ports are physically secure. If they are visible to visitors/the public, someone may get rid of the encryption or reset the router which would cause big headaches.

5. Any server within a company needs to be protected. Confidential information, such as info about the business and operational things, will be held on the server(s). To secure them, I would make sure that user activity is tracked, implement some sort of antivirus, and simply just keep the server up-to-date.

6. One of the best tools for monitoring network traffic and ports is Network Performance Monitor + Network Configuration Manager. "It thoroughly monitor switch ports for the most comprehensive possible network monitoring scheme.[1]" Both virtual and hardware switch port monitoring are offered in this program, and you can have an overview of any switch port setup. "The program has functions of a switch traffic monitor with a high degree of complexity[1]." This ensures port availability and overall network health. They also offer a 30-day free trial, so you can test all the features out at no cost.

[1] www.dnsstuff.com/switch-port-monitoring-software

7. An IDS (Intrusion Detection System) "monitors and analyzes computer network traffic to protect a system from network-based threats[2]." Hackers aim for smaller business, as they don't have a complex system set up as compared to a big company like Microsoft or Apple. For implementing one, I would use SolarWinds Security Event Manager. The program collects network intrusion detection system logs and combines that information with other logs. "This data is constantly optimizing the security systems and processes of your IDS or informing the creation of more efficient procedures better equipped to protect your network[3]." You also get a 30-day free trial to test out all the features, at no cost.

8. So that the manager has remote access, he would be included on a remote access policy that would be set up within the organization. Each kind of person would have a specific role within the policy, depending on their role within the company. The manager would have a higher role within this policy, as I would be walking through with them showing how everything works. They would be one of the people in charge of maintaining everything, along with my help when needed.

[2] www.garnetriver.com/2018/06/01/5-reasons-why-your-company-might-need-an-intrusion-detection-system
[3] www.dnsstuff.com/network-intrusion-detection-software#solarwinds-security-event-manager