Network Security Project

Jacob Jeffers

University of the Cumberlands

ISOL 532 – Telecomm and Network Security

Dr. Joanna Patterson

4/15/2021

Abstract

This project serves as the applied project for this course. Eight sections within the prompt and ten requirements must be met for the organization.

Network Security Project

1. For this network design, I used an MPLS VPN connection to connect the two remote locations. There are four routers with VPN capabilities, eight distribution switches to connect PCs across the three floors, and thirty-six switches. I wrote it out by hand because while this looks bad, my attempt at it on the computer was way worse.

Diagram

Description automatically generated

1. I recommend using category six and fiber optic for a high-speed data connection for the cables.
2. The server closet will be located on the second floor at each location. There will also be switch closets located on each floor. I chose this because a server on the ground floor is susceptible to motor accidents from the outside, and it is generally accepted that the server should not be placed on the top floor (Stewart, 2014).
3. We should implement password complexity requirements, monthly password changes for access into the company’s resources, and two-factor verification. Also, implementing acceptable use policies, access control measures, and firewall barriers are vital to keeping the network secure (Stewart, 2014). There needs to be a dedicated blue team security staff managing the packets on each network. This will help protect each location from hackers (Stewart, 2014). In addition to these, another recommendation would be to upgrade our physical security – man traps, key cards, perimeter fencing, video cameras, and biometric scanners for access into the location are another important protective piece for an organization. Regular user training on social engineering attacks should be implemented.
4. A honeypot would be the best for this situation (Stewart, 2014). We could attract hackers with this technique to view their attempted methods for accessing the network. The honeypot system could work on its own and would provide valuable insight to the security team.
5. My recommendation for the WAN would be to utilize an MPLS VPN for connecting the two locations. I chose this because it allows for a more secure connection than the public internet (Stewart, 2014).
6. The solution to this is to choose servers with high redundancy (Stewart, 2014). My recommendation would be for the organization to choose the technology that best suits their business needs while also maintaining a high redundancy so that the availability of the data is not compromised.
7. These recommendations have been made to the best of my abilities within the hardware, networking, and security realms. I hope it is helpful to the organization, but I also hope it showcases my growth. I am way more confident protecting the network than designing the network, but I am confident I have met most requirements for this project. I appreciate all feedback as it helps me to correct mistakes that I have made in the future.

References

Stewart, J. M. (2014). *Network security, firewalls, and VPNs*. Burlington, MA: Jones & Bartlett Learning.