Corporate VPN

A Virtual Private Network is used to encrypt the connection between your device and the network you are connecting to over the internet.

There are many reasons individuals may choose to use VPN's but for corporations, it's important to keep the company data secure and private. Remote work is growing in popularity and because corporations are sending their employees home, they need to have something in place to ensure the company's data is only accessed by employees. Requiring an employee to login through a VPN allows the company to maintain its security measures by allowing certain data to certain employees and keeping access to the databases safe and secure from hackers.

Some disadvantages of using a VPN include slower speeds, dropped connections, and cost. When you compare the disadvantages to the advantages for a large corporation with sensitive data, pros outweigh the cons.

In Project 1, I had four virtual machines on the Red Team Network: JumpBox, Web1, Web2, and the ELK Server. I used inbound and outbound security rules to control access to and from the internet. I didn't use a VPN, instead, I used ssh connectivity to the JumpBox. A rule was set to only allow my IP address to access the JumpBox. This rule was advantageous because it limited anyone else accessing the network. Once I was connected to the JumpBox, I could complete necessary tasks with the other servers.

The disadvantage to using ssh and inbound security rules is that a rule would need to be created for every user at every location. A VPN could be created using Azure by creating a new virtual network and virtual network gateway for the Red Team. A VPN device with a static public IP would be necessary. Saas apps and productivity suites can help IT admins onboard users. Each user would have their own login credentials that would meet the company's security policies.

A VPN may be overkill for Project 1's access control requirements. As of now, I am the only one that needs to access the network. My ability to access the JumpBox and control the network through that server is all that is needed at this point. A VPN would allow full access to the entire network, putting it at greater risk for security issues. Passwords can be decrypted so that leaves another vulnerability when discussing VPN connection.

A VPN would be a great solution if I needed to onboard new users and allow access to several users in several locations. A virtual private network is a great solution for company wide access with security measures and user restrictions in place. Password policies, multi factor authentication, strong encryption, database management and authorized users, antivirus software and firewall policies should be considered when opening up a network to VPN connectivity.

A., Zohair. "What Are the Advantages and Disadvantages of VPN?" *Online Security News, Reviews, How To and Hacks,* 17 Nov. 2021, https://securitygladiators.com/vpn/advantages-disadvantages/. *Accessed 17 March 2022.*