ITN 263 – Project Part 3: Remote Access and VPNs

A diagram of a flowchart

AI-generated content may be incorrect.

For Corporation Techs, the best VPN technology choice is an IPSec VPN because it provides full network access, has better security than an SSL/TLS VPN, and has a more consistent performance operating on a network. While an SSL/TLS VPN technology is more suited for web application layer traffic and web sessions, an IPSec VPN is the better choice in this case because it operates at the network layer and workers will need full network access to servers which would not be provided with another VPN technology. An IPSec VPN also provides a more secure connection because it encrypts the entire network traffic with Encapsulating Security Payload (ESP), Authentication Header (AH), and Internet Key Exchange (IKE). These three protocols are the key factors in making IPSec a secure and efficient way to protect VPN traffic. ESP is used to encrypt, authenticate, and provide integrity of data while also preventing replay attacks from happening, AH also provides data integrity and prevents unauthorized replays of packets while also providing authentication, and IKE uses an encryption key exchange to provide authentication to start secure communications. Using an IPSec VPN over an SSL/TLS VPN on a network will also have a more consistent performance because it operates at the network layer and has less overhead compared to the other VPN which works at the transport layer and establishes sessions that need to be consistently reestablished which will cause inconveniences.

An IPSec VPN will also work better in conjunction with our IEEE 802.1x authentication because both are designed to work at the network layer which allows for seamless integration and ensures consistent and secure performance from both. The 802.1x authenticator will first authenticate the user’s credentials against a database to see if they are authorized to access the system, then the IPSec VPN will create a tunnel that will encrypt the traffic between the device and the network which will secure our traffic from attacks like eavesdropping the data sent and replaying the credentials of our workers while keeping a consistent session without interruption to continue providing 24/7 support to users. Using these two together will allow for a seamless and secure authentication and remote access process that encrypts and protects all data from a device after it has been authenticated as legitimate.

Another form of remote access that can be easily deployed is Remote Desktop Protocol (RDP). This can be done easily because as our servers run Microsoft Windows Server all that would need to be done is to install RDP on the server and the end device, then send a request to connect to the IP address of the server requested with their login credentials. Once the credentials are verified, the RDP protocol establishes a connection from the end device to the server remotely and can send and receive data to and from the server. Using RDP also encrypts data and compresses it to reduce the bandwidth of the network, making it secure and efficient. Using this remote access protocol is an efficient and cost-effective way for Windows devices to connect to our servers because sessions can be quickly established if validated and no additional software will need to be purchased.

Citations:

Stewart, James Michael, and Denise Kinsey. *Network Security, Firewalls, and VPNS*. Jones and Bartlett Learning, 2021.

Topper, Matt. “SSL vs. IPSEC VPN: Understanding the Differences.” ConnectWise, ConnectWise.com, 9 Nov. 2023, www.connectwise.com/blog/cybersecurity/ssl-vs.-ipsec-vpns.

“What Is IP Security (IPSec).” *GeeksforGeeks.Com*, GeeksforGeeks, 3 Feb. 2025, www.geeksforgeeks.org/ip-security-ipsec/.