ITN 263 – Project Part 4: Final Network Design Report

Executive Summary

Corporation Techs is a growing company that plans to increase its client-facing staff due to its unexpected growth. Because of this, maintaining both 24/7 support and the security of the company will be essential to the future of it. As more employees begin to work remotely and an increasing number of clients are relying on our services, we need to make sure that our network is well protected while still maintaining its availability. We can achieve this by implementing an approach that involves various security technologies that will not only keep our services always available but also secure ourselves and our clients. Firstly, creating a diagram of the layout of our network can help us analyze how it is set up both physically and logically to identify what areas are unsecure and could leave us vulnerable to attacks and service disruptions. Doing this allows us to implement necessary improvements to help achieve our objectives. One main way to achieve this is by filtering dangerous and unnecessary traffic coming from the internet onto our network which can be used to attack and disrupt our services. Also, we need to ensure that the employees who are working from home can securely connect to our network without exposing themselves or our network. Using an authentication method that requires users to prove their identity will help protect against unauthorized access to the network and implementing redundant network devices will minimize downtime and support our goal of providing 24/7 services. By implementing these improvements, Corporation Techs will be able to support the growth of its workforce and clients without compromising its security or availability.

Introduction

As Corporation Techs moves towards expanding its remote workforce due to its growth and the need for around-the-clock support to its clients, maintaining the availability and security of our network is vital in ensuring we can achieve this. While analyzing the logical and physical components of our network to see how each component interacts with each other and achieves its purpose, we can see that there is still room to improve our operations to maintain a higher level of availability and security. Creating and improving upon newly updated network diagrams allows us to see what state our network is at and where we can make an improvement, test the improvement, and see what needs to be added next. Because there will be so much differing traffic going in and out of our network, using firewalls placed at the entrance of the network, on and after our public web server, and on each workstation and server will allow us to control the incoming and outgoing network traffic without interrupting our services. Also, using an authentication method will make users who are logging in prove their identity to us with their credentials to prohibit unauthorized users from accessing our network. We also need to enable our remote workers to connect to the network without risking the security of themselves or our company, which can be achieved through a VPN and other remote access technologies. As the availability of our services is a main priority, creating a redundant network is achieved by connecting backup systems that will take the place of any device that fails, immediately. Throughout my network plan and design, I will address these issues and expand on how we can implement these various security technologies and why they will be beneficial to the services of the company.

A diagram of a company

AI-generated content may be incorrect.

Network Design

In the network diagram, I have mapped the connections made in the network while also adding enchantments that will increase the security of the network as a whole. As traffic comes into the network from the internet, it is first filtered through a next-generation firewall as the first line of defense. This firewall acts to prevent any traffic going in and out of the network that is known to be unwanted or malicious. It also provides integrated intrusion detection and prevention to detect threats using their signatures and eradicate them. After going through the next-generation firewall, traffic that is going to the web server goes through a web application firewall that protects the traffic on the web server and protects it from web-based attacks. There is also an internal firewall that is placed after the web server to isolate it so inbound and outbound traffic to and from the web server is thoroughly checked before accessing the web server or network if permitted. Once the traffic towards the internal network is checked by the internal firewall, it is permitted past the switch and authenticated by using IEEE 802.1x which checks the user’s credentials against a database with valid credentials. If the credentials are accepted, the user is allowed access to the network which contains the workstations and servers that are protected by Windows Defender Firewall. There is also another switch in the internal network that connects the servers and workstations together, and a fail-over switch for each of the two internal switches in case either of the switches stops working to continue communication and services 24/7. From the next-generation firewall, a remote user could also connect to the network using an IPSec VPN gateway or connect to the web server by first connecting to a bastion host and then connecting to the web server through SSH which will take the force of any attack.

I think it would be more beneficial to the company to upgrade to IPv6 rather than continue with IPv4 because there has been unprecedented growth that is leading to the client-facing staff being doubled. IPv6 has a much larger address space which allows every new and old staff member to have a unique IP address without needing to use network address translation to find an open IP address for staff members. It also provides substantially better security than IPv4 mainly through IPSec which provides encryption and authentication of packets sent through the internet. IPv6 is also more efficient than IPv4 which allows for better performance because it has a simpler header that makes routing and processing of packets more efficient.

Using this network design and switching from IPv4 to IPv6 will optimize the efficiency and security of the network for its users and our customers. This network design effectively protects the internal network and its endpoints from internet traffic, protects the web server while isolating it from the internal network, enforces proper authentication measures, and allows for secure remote access. IPv6 also creates a more efficient and secure routing process through IPSec and a simpler packet structure.

Firewall Selection and Placement

Assigning firewalls for traffic coming from the internet on the web server, workstations, and other servers will help provide maximum security by ensuring proper access and reduced attack surfaces. When traffic comes into the network from the internet, it is filtered through a next-generation firewall which will filter unwanted traffic while also providing intrusion detection and prevention, deep packet inspection, advanced malware detection, and threat intelligence to identify known threats. These additional security measures will provide thorough protection throughout the network in just one security device. A benefit to having integrated intrusion detection and prevention in this firewall is that threats are detected and prevented by this device in real time. Deep packet inspection will also inspect not just the header of the packets sent in and out but also the full packet’s body which will identify any threats that are hidden deeper down the packet. Also, the threat intelligence feeds and advanced malware detection of the firewall combine to block any domains and IP addresses that are known to be associated with malware and threats.

Using a web application firewall on the public web server will help prevent attacks such as SQL injections, cross-site scripting attacks, and cross-site forgery attempts. The firewall protects the web server from these attacks by looking at malicious HTTP and HTTPS requests made to the web server and blocking them to stop these attacks. Not only will this firewall protect the web server, but it will also protect the network as it will not allow an attacker a path onto the internal network through the web server. There will also be an internal firewall after the web application firewall to block any malicious traffic that has made it past the next-generation firewall or the web server. The placement of the internal firewall after the web server effectively creates a demilitarized zone that isolates the web server because it is public to prevent anyone from making their way onto the internal network. This makes the network more secure by first examining and filtering traffic that is coming from the internet onto the web server then the same for the traffic from the web server onto the network while still allowing legitimate traffic to continue as normal.

For added security, each individual workstation and server will be equipped with Windows Defender Firewall. This firewall will allow only necessary traffic to go in and out of these devices. An example of this would be for workstations to allow HTTP and HTTPS traffic on TCP ports 80 and 443, and servers to allow Remote Desktop Protocol (RDP) connections on TCP port 3389 for remote workers.

As our internal network resources should be heavily protected, I recommend using IEEE 802.1x for our authentication method as it provides the most comprehensive and secure authentication services. It works through a user first sending their authentication credentials to the authenticator which is then forwarded to the RADIUS server and put to check against a database that has stored accepted credentials. It then decides whether to allow or deny the request which is based on whether or not it found a match of the credentials in the database. If the user’s credentials are accepted, then they are allowed to access the internal network. This helps prevent others who have not been authenticated from having the ability to access internal network resources. Using 802.1x as our authentication method makes for an effective and secure authentication method against unauthorized access.

Placing firewalls after the internet, on the web server, after the web server, and on each workstation and server provides a comprehensive solution to unauthorized access and requests. More specifically, these firewalls provide intrusion detection and prevention, protect against web-based attacks, isolate the public web server from the internal network, and protect individual devices on the network. In addition to these firewalls, IEEE 802.1x provides a simple and secure authentication method to allow authorized users to connect while prohibiting unauthorized users from connecting to the network.

Remote Access and VPNs

The VPN technology that is the best-suited choice for Corporation Techs 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. As an SSL/TLS VPN is better suited for web application layer traffic and web sessions, an IPSec VPN operates at the network layer, and our employees will need full network access which is not provided with another VPN solution. An IPSec VPN also provides better security in its connections by encrypting entire network traffic with Encapsulating Security Payload (ESP), Authentication Header (AH), and Internet Key Exchange (IKE). These protocols are the pieces that make 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. An IPSec VPN will also have a more consistent performance because it operates at the network layer and has less overhead compared to an SSL/TLS VPN which operates at the transport layer. This creates a need to consistently reestablish sessions which will cause inconveniences in remote connections.

An IPSec VPN also works better when used with our IEE 802.1x authentication because both are made to work at the network layer. This allows for seamless integration and helps ensure consistent and secure performance from both components. 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 secures our traffic from attacks like eavesdropping the data sent and replaying the credentials of our workers. This also helps keep a consistent session without interruption to continue providing 24/7 support to users. Using both of these together will allow for a seamless and secure authentication and remote access process that encrypts and protects all data and traffic being sent over a remote connection.

Another form of remote access that can be easily deployed is Remote Desktop Protocol (RDP). As our servers run Microsoft Windows Server, this can be done easily because we would only need to install RDP on the server and end device and then send a request to connect using the server’s IP address with the user’s login credentials. After the credentials have been verified, the RDP protocol establishes a connection from the end device to the server remotely which enables the user to send and receive data from it. This protocol also encrypts data and compresses it to reduce the bandwidth of the network and make it more secure and efficient. RDP 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.

In addition to using an IPSec VPN and RDP, having our workers connect to a bastion host firewall and then connect to the public web server using SSH protocol will provide privacy and protection for our network. Connecting to a bastion host before using SSH access to the web server will reduce the attack surface compared to directly accessing the web server through SSH because it will be designed to tank the force of any attack that occurs on the web server. The bastion host is deliberately exposed but configured with very secure controls, so it protects the host device while not exposing that the host is connected to the web server using an SSH connection. It will also protect access attempts to the web server through SSH because it requires authentication factors like a key or multiple factors together before allowing anyone to connect. Not only does the bastion host secure connections to the web server, but the SSH protocol itself provides anonymity and security for the user who is connected. SSH requires authentication before it can authorize users to use its services which stops others from being able to make an unauthorized connection. It will also encrypt communications and data sent over the connection which will protect the network and user from eavesdropping and man-in-the-middle attacks. Together, these components create a strong and private connection that allows workers to make connections to the public web server without risking themselves or the internal network.

Using an IPSec VPN for our company will provide a remote access solution that is secure and private. This is done by providing encryption, authentication, and integrity through ESP, AH, and IKE. This technology also can be used seamlessly with our authentication method, making it an efficient solution. Using SSH on our web server and RDP on our other servers provides a cost-effective addition to our IPSec VPN by allowing for remote access connections to be made quickly without risking the network. A bastion host will also provide users with a device that takes the force of any attack to keep their devices secure.

Conclusion

In conclusion, Corporation Techs is an expanding company that will begin to move most of our employees to remote roles within the next six months. As this happens, we still need to provide the same security and continuous support as we did before and will need to continue to do so once the transition is fully complete. To achieve this, we first need to assess the current security posture of the company. This can most comprehensively be done by creating a diagram of the network’s physical and logical parts and assessing what parts are supporting our goals, what parts aren’t supporting our goals, and what can be added to improve upon our design. We will also need to use firewalls placed throughout the network to control traffic going in and out to prevent dangerous traffic from affecting us. To help secure our remote employee’s connections to our internal network, using remote access technologies like a VPN can provide the needed security and anonymity to protect our workers and our network. Also, making a transition from IPv4 to IPv6 will allow for more employees to have a unique IP address, provide encryption and authentication of network packets, and make the routing and processing of packets in our network more efficient. Implementing these changes will aid in helping transition our workforce into remote roles, enhance the security of our internal network, ensure secure remote access, and provide continuous support to our clients.

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 802.1x? How Does It Work?” SecureW2, 13 Jan. 2025, www.securew2.com/solutions/802-1x.

“What is a Next-Generation Firewall (NGFW)? | Cloudflare.” Cloudflare.com, www.cloudflare.com/learning/security/what-is-next-generation-firewall-ngfw/. Accessed 30 Mar. 2025.

“What is a WAF? | Web Application Firewall Explained | Cloudflare.” Cloudflare.com, www.cloudflare.com/learning/ddos/glossary/web-application-firewall-waf/. Accessed 30 Mar. 2025.

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

“Why IPv6 Matters: Benefits and Beyond in 2024.” *Toxigon.Com*, 13 Dec. 2024, toxigon.com/understanding-ipv6-and-its-benefits.