**Network Design and Plan**

Saliman Zadran

ITN 263

**Introduction**

Corporation Techs is taking a crucial step in transforming from an onsite workforce, to now working remotely. Although onsite support will still be a part of their business, most technical representatives are being shifted to remote work. Thus, my duty as a junior network architect is to provide the best solution and plan for them to do so.

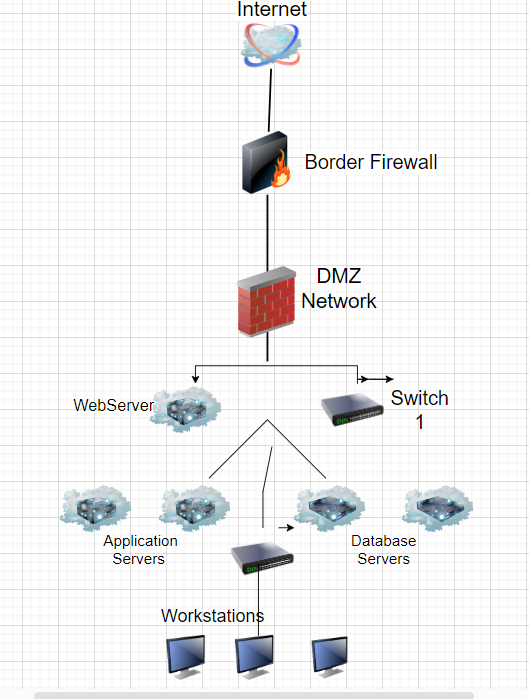
**Part 1 Network Design**

As far as the network design is concerned, we already have crucial information as to what servers, workstations, and network devices already exist. It is crucial that the plan we implement keeps the network secure and helps it operate optimally at all times. This is where the planning and the groundwork for the network are important. When it comes to secure network design and implementation the most secure and viable avenues for the company must be considered. As far as the design is concerned, implementing a DMZ is crucial, as it provides security between the internal and public/external networks. One may be wondering what a DMZ is, it is best defined as, “A DMZ or demilitarized zone is a perimeter network that protects and adds an extra layer of security to an organization’s internal local-area network from untrusted traffic” (Fortinet). The way the DMZ is going to be implemented is with the usage of two firewalls, one for the internal network and for the DMZ network segment. The internal network firewall is going to allow traffic from the DMZ, while the DMZ firewall will allow traffic from the internet. Thus, if any attacks were to happen, it would be contained within the DMZ itself.

As far as physical and logical topology is concerned, it is crucial that the topology is set up in such a way that it can be understood. A well-planned network topology enhances the user experience and helps administrators maximize performance while fulfilling business needs (Cisco). The physical topology will have many different nodes and lays them out all the way down to even the cables and NICs in use, along with the larger components such as servers, gateways, routers, switches, etc. The logical topology will provide an overview of how the dataflow is conducted throughout the network, the placement of network nodes such as switches and servers. All network devices communicate with each other in a way that keeps dataflow and communication persistent. In this case, the routers and switches will be communicating with each other, along with the switches communicating with the servers and conducting traffic as needed. The servers will be communicating with the workstations, along with the workstations being connected to the network via the routers.

Another important part of the network design is ensuring that secure authentication and secure internal access is implemented at all times. Secure internal access can only be ensured with authentication, authorization, and accounting. Authentication, authorization, and accounting (AAA) is a security framework that controls access to computer resources, enforces policies, and audits usage (Fortinet). The usage of a VPN will assist with the internal network access for remote users. This way they can access the necessary company resources in a secure manner. Constant patching of all network nodes, whether it be servers, computers, firewalls, or any other device and software on the network will be crucial as well. Security updates and patches will not be ignored, as it is crucial no vulnerabilities are left unpatched. The sales and accounting departments will have their own subnets too.

**Basic Network Diagram**



This is a basic network diagram showing how the network topology will be setup. Although it is not as detailed a more detailed one will be created using this as the base diagram.

**IPv4 vs IPv6**

When it comes to IPv4 versus IPv6, there are quite a few things to consider. As IPv6 is soon to replace IPv4 due to the lack of IP Addresses available with IPv4. A large benefit of IPv6 is, compared with IPv4, IPv6 has better connectivity, lower packet loss, and similar hop count (Li K-H, Wong K-Y, 2021). Another benefit of IPv6 over IPv4 is the fact that it is what will be used in the future, so why not get ahead of the curve and implement it already? There are truly little to no downsides to its usage anyway, other than higher latency and throughput (Li K-H, Wong K-Y, 2021). Any issues which exist with it currently will be worked out anyway.

Overall, this includes the DMZ security architecture to be implemented, along with the implementation of the different nodes in the topology. The benefits outweigh any negatives that may be associated with the recommended technology. The overall report includes the basic topology diagram which can be used for the network design. Along with the recommendations for IPv4 versus IPv6, the pros and cons. When deciding on the secure network establishment, it should be kept in mind that changes may need to be made down the line. Security changes can be made later as well; however it is always beneficial to first establish a baseline and go from there.

**Part 2 Firewall Selection and Placement**

As per instructions, the existing company border firewall needs to be replaced, an outdated firewall can be a vulnerability. A DMZ establishment is already a part of the network security plan; however, network authentication is something that must be kept in mind as well. There can never be enough security implemented, and choosing the correct firewall is a crucial part of the network security process. A firewall can be the first line of defense for an organization, and there are so many different firewalls that can be chosen from. Usually, a firewall is selected based on an organization's needs and what they can afford to implement. An excellent choice for a firewall for Corporation Techs would be the Next Generation Firewall. A Next generation firewall not only provides the same benefits a regular firewall would, but it also has additional security benefits. The Next-Generation Firewall (NGFW) is a portion of the 3rd generation of firewall technology, which combines a traditional firewall along with other network appliance filtering functions (NAFF) for example, inline intrusion prevention system (IPS) as well as in a deep packet inspection (DPI) (George, A. Shaji & George, A.s.). These extra benefits with the firewall can enhance security and save costs on implementing extra security appliances. For example, with a normal firewall, you would also need an IPS implemented separately. However, with the Next Generation Firewall, the IPS and deep packet inspection are part of it. Intrusion detection and prevention should be the key goal of a network security posture at this level. However, a single firewall implementation is never enough. A defense in depth model of firewall defense is necessary. Along with the usage of the NGFW there needs to be firewall implementation for each individual server and workstation on the network as well.

For this implementation, what can be used is the Microsoft Windows Firewall, a benefit of which is its widespread implementation across webservers and workstations. It can be configured as needed when it comes to ports blocked and opened, along with rules that can be set. Because Windows Defender Firewall is a host-based firewall that is included with the operating system, there is no other hardware or software required (Microsoft). The benefits of a defense in depth strategy can’t be emphasized enough. For now, the NGFW along with the Microsoft Windows Firewall are a good place to start. Any company devices given out will be preconfigured with the same security policies and rules. The group policy and security implementation will be widespread, with no host exceptions.

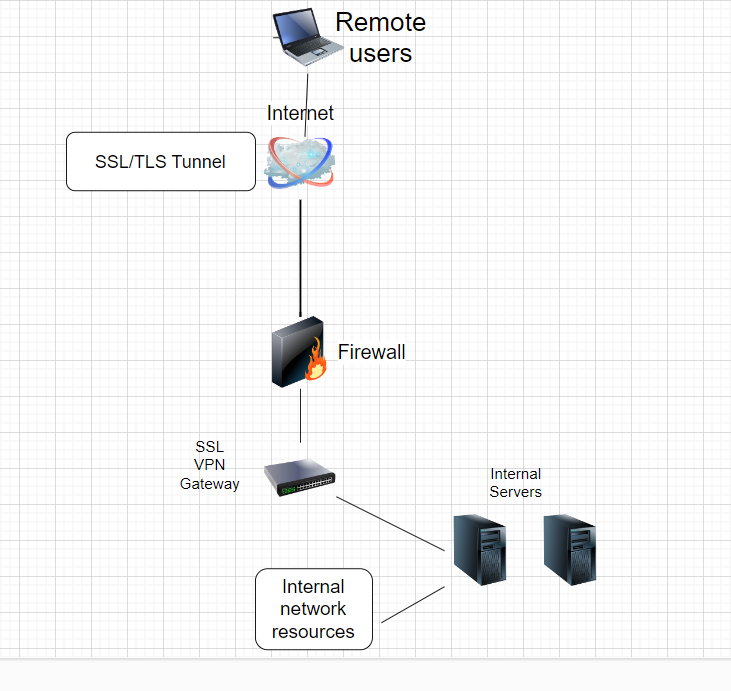
Finally, when it comes to the DMZ, as was stated in part 1 of this design plan, its benefits are vast. The plan and implementation of the DMZ is necessary; identification of the risks the companies will face will occur within the DMZ too. As time goes by, and different threat patterns are discovered, security will continue to be furthered, along with the systems being hardened. There will be a public facing DMZ network segment established, it has the webserver and is connected to the internet through the border firewall. The public facing DMZ Network and internal network are connected via a second firewall which acts as the boundary firewall. The DMZ provides an additional layer of security, providing isolation of external facing servers that are internet facing. It creates a boundary between the internal and external public facing network.

When users join the company network, there must be a strong authentication form implemented. Users will be communicating with the network; data streams will be established. If proper authentication methods are not implemented, that results in a massive security risk, as anyone can authenticate to the network. Internal network access must be behind a proper authentication barrier. There are different forms of authentication are something you are, something you have, and something you know (Farik, Mohammed & Lal, Nilesh & Prasad, Shalendra). One of the most basic authentication policies to be implemented should be a strong password policy, this can be done through the Windows Group policies which will be implemented for all computers within the company domain. Along with that, there will also be the use of two factor authentication, either through a software application, token, or biometric. Depending on the level of access a user needs to the company systems. For example, if it is a company information technology employee working on company systems, or needing access to servers, they will need more than one form of authentication to network resources. However, there will be a baseline of authentication set for all users. Smart card authentication is something that may be considered as well, as both the smartcard and a smartcard pin will be needed to sign into the company computer. There will also be Network Access Controls in place, which will restrict a user based on their identity or device type. Authentication and password policies will be monitored and improved as needed. All employees must adhere to the set authentication policies, and there are no exceptions to these policies. For remote users, in order to connect to the VPN, they will be required to enter the pin code for their smartcard as well.

**Part 3 Remote Access and VPNs**

One of the most impactful steps that Corporation Techs is taking is having most of its technical representatives working remotely. This means that those employees working remotely will no longer be able to physically connect to the network, via ethernet cables, or the internal network Wi-Fi on site. However, there is a solution for this, it is the implementation of the Virtual Private Network (VPN). The usage of VPNs has become vast and widespread, especially since COVID forced many companies to shift to remote work. The VPN allows employees to connect to their internal network while working from home. Corporation Techs being such a large company with so many employees can certainly benefit from this, VPNs are quite cost effective, and they are usually not too difficult to implement. Data is encrypted as it travels between the employee’s computer and the company’s servers. This is done through the tunnel between an organization’s network and a remote user that is “virtually private,” even though the user may be in a public location. This is because the traffic is encrypted, which makes it unintelligible to any eavesdropper (PaloAlto). There are two types of VPNs, an IP Sec VPN and SSL/TLS VPN. They both have their benefits, and it is up to the individual company which one they want to implement.

In our case, here at Corporation Tech, I would recommend the SSL/TLS VPN, the benefits of which are both remote access and network level access via an SSL Secured Tunnel (F5.com). An SSL/TLS VPN also provides the benefit of not having to establish additional network resources for the VPN, as it operates at the application layer. The connection is established through a browser, allowing access to network resources. This also saves time and resources as it doesn’t require the installation of additional VPN software on remote devices. The downsides of IP Sec VPN are the requirement for additional network resources, and requires dedicated software be installed on user devices.

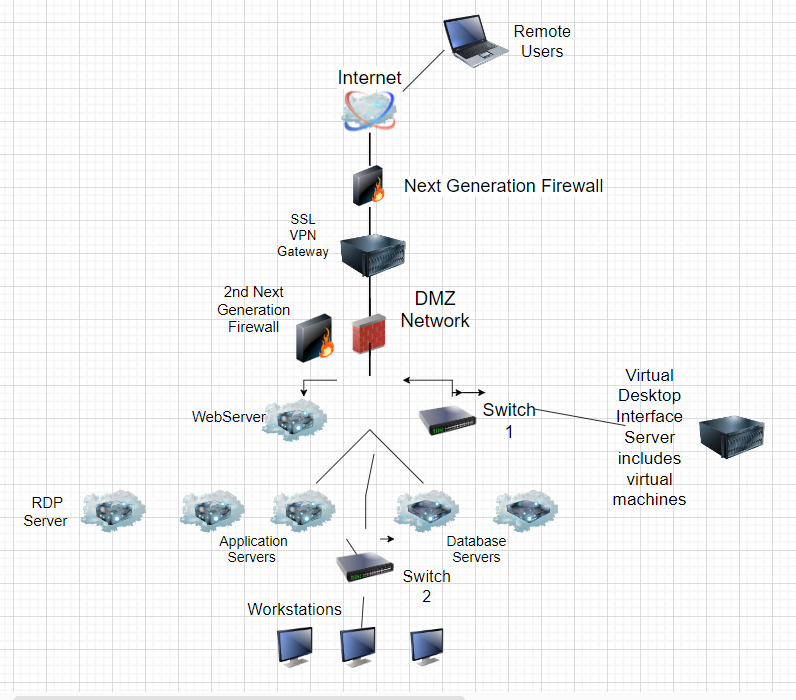


An additional benefit of implementing a VPN for remote access is the fact that it provides an additional form of authentication. When users are accessing the VPN, they must authenticate themselves first, as this is one of the benefits the VPN provides, security. For established VPN connection, the first process is authentication (P. N. Thanh and K. Kim). After a user is authenticated, then they are able to connect to the internal network. Once the VPN connection is established, users can also use other methods of remote access as well.

Among the different types of remote access are RDP, SSH, and VDI. Perhaps some of these may only be used by IT professionals to access resources they may require, such as jumpboxes. However, VDI is certainly something that can be used, perhaps the company has developers who need to use VDI and RDP services. RDP allows users to access company resources by connecting to a remote desktop or server. SSH is a command line tool, this would most likely be used by an IT administrator as well, to access CMD line interfaces on servers. Finally, VDI allows users to access a virtual desktop environment, with the use of a remote connection. The benefits of the VDI are many, as it can be used for testing purposes as well. Also, VDI users can connect to their virtual desktop from any location or device, making it easy for employees to access all their files and applications and work remotely from anywhere in the world (VMWare). Any of these remote access technologies that would be implemented would be configured securely, to prevent unauthorized access. For Corporation Tech, the choice would be RDP and VDI. Generally speaking, it is always good to have at least two ways of remote access to company resources. That way if one form of remote access is down or not working, another form of remote access can be used to perform maintenance or access the network resources an Administrator may need to access. The VDI interface requires a separate VDI server, which will then be used to segment different virtual machines, which remote users can then access.

**Part 4 Final Network Design Report**

Finally, we wrap up this report with the overall network diagram and the way it is going to be implemented. It is crucial that the final design includes the whole network design and infrastructure. This topology will show how the network is segmented and will be easily understandable and established. So far, the changes which have been made will be very beneficial, and it can be immediately noticed. There are two next generation firewalls, one external and one internal. There are two database and application servers, along with a RDP server and VDI server used respectively. There is also two switches, implemented in the most optimal locations on the network. Finally, there are the 50 workstations, all servers and workstations have two factor authentication enabled, and Windows Firewall on them for additional protection as well.



The way this network has been setup is to provide the best security along with the best form of access for both remote and onsite users. The DMZ Network is established in its proper location, providing security for the network. Authentication will always be implemented to allow for secure access and authorized access, both remotely and on site. Systems will continue to be upgraded and improved as necessary, however at this point, this network diagram is the starting point for Corporation Techs, as it includes the securest form of network design. It is understood that there may be additional costs associated with the implementation of this network, however as each specific portion of this network was broken down throughout this report, it shows just how important each aspect is. Whether it be having proper authentication systems, next generation firewalls, or setting up a DMZ network. Every single part of the network attributes to the company’s security. Along with the persistent security monitoring, there must be testing implemented as well, for firewalls, servers, and other network nodes. This is a security practice which needs to be implemented.

**Executive Summary**

As Corporation Techs continues to grow and improve upon its already well-established infrastructure, there are certain changes that need to be made within the company’s Network and Security infrastructure. As technology continues to evolve so does the need for upgrades to organization networks and infrastructure. Here at Corporation Techs, we were at a standstill when it came to network design and security. As I am sure you all are aware, a proper network configuration and design is the baseline for continued operations of a company, as every facet of it relies on the technological side of things. When it comes to security, it can only be properly implemented when the network design is sound and well established. Hence why we went ahead and researched the best systems, configurations, and designs for the Network and security. We have implemented additional security systems, such as next generation firewalls, which will have advanced security capabilities in defending our network. Along with the upgrades to remote access, including a VPN, VDI, and RDP servers. This will allow those of us that work remotely to do so in a secure manner, with complete access to the internal network systems and resources, as if we are on site! This is an exciting advancement and certainly something we were looking forward to establishing. As security threats continue to evolve, a lack of security can result in the demise of a company. We have ensured that proper authentication is implemented on all company systems. This results in the authentication, authorization, and accounting of all company employees who access our systems. Our Next Generation Firewalls will monitor and defend against all security threats the company faces. The networking and security teams of the company will continue to upgrade and enforce security across the board. There will be absolutely no exceptions to security policies, everyone from the Janitor to our highest-level executives must ensure they follow and adhere to the security policies set. Our aim is to continue to ensure our company can operate optimally and securely on all levels. Additionally, we will look into cutting costs but ensuring our company has the best security. Every decision taken with regards to this network design, was while keeping the company’s budget and goals in mind. As we understand the goals we have as an organization, and ensuring we can continue to provide our services and support optimally. In conclusion, this network design will allow all Corporation Tech employees to complete their work efficiently and securely, remotely and on site. It will ensure our network reliability is at its highest, and our redundancy is well established. The networking and security teams will continue to work together to enforce and advance the company’s security, Corporation Techs will continue to evolve!

**Sources Cited**

Cisco. (n.d.). *What is Network Topology?.* <https://www.cisco.com/c/en/us/solutions/automation/network-topology.html>

Farik*, Moham*med & Lal, Nilesh & Prasad, Shalendra. (2016). A Review Of Authentication Methods. International Journal of Scientific & Technology Research. 5. 246-249.

Fortinet. (n.d.). *What is Authentication, Authorization, and Accounting (AAA)?*. <https://www.fortinet.com/resources/cyberglossary/aaa-security>

Fortinet. (n.d.) *What is a DMZ Network?.* <https://www.fortinet.com/resources/cyberglossary/what-is-dmz>

F5. (n.d.). *What is SSL VPN*. <https://www.f5.com/glossary/ssl-vpn#:~:text=An%20SSL%20VPN%20generally%20provides,is%20data%20security%20and%20privacy>.

George, A. Shaji & George, A.s. (2021). A Brief Study on The Evolution of Next Generation Firewall and Web Application Firewall. IJARCCE. 10. 31-37. 10.5281/zenodo.7027397.

Li, K.-H., & Wong, K.-Y. (2021). Empirical Analysis of IPv4 and IPv6 Networks through Dual-Stack Sites. *Information*, *12*(6), 246. MDPI AG. Retrieved from <http://dx.doi.org/10.3390/info12060246>

Microsoft. (2023, February 23). *Windows Defender Firewall With Advanced Security.* <https://learn.microsoft.com/en-us/windows/security/threat-protection/windows-firewall/windows-firewall-with-advanced-security>

PaloAlto. (n.d.). *What is a Remote Access VPN?.* [https://www.paloaltonetworks.com/cyberpe*dia/what-is-a-remote-access-vpn#:~:text=The%20remote%20access%20VPN%20does,it%20unintelligible%20to%20any%20eavesdropper*](https://www.paloaltonetworks.com/cyberpedia/what-is-a-remote-access-vpn#:~:text=The%20remote%20access%20VPN%20does,it%20unintelligible%20to%20any%20eavesdropper)*.*

P. N. Thanh and K. Kim, "Implementation of open Two-Factor Authentication service applied to Virtual Private Network," The International Conference on Information Networking 2013 (ICOIN), Bangkok, Thailand, 2013, pp. 135-140, doi: 10.1109/ICOIN.2013.6496365.

SecureOps. (2018, August 29). *Network Security Design is Critical to Eliminating Security Gaps and Reducing Costs.* [https://secureops.com/blog/effective-network-security-design/.](https://secureops.com/blog/effective-network-security-design/)

VMWare. (n.d.). *What is VDI (Virtual Desktop Infrastructure).* <https://www.vmware.com/topics/glossary/content/virtual-desktop-infrastructure-vdi.html>