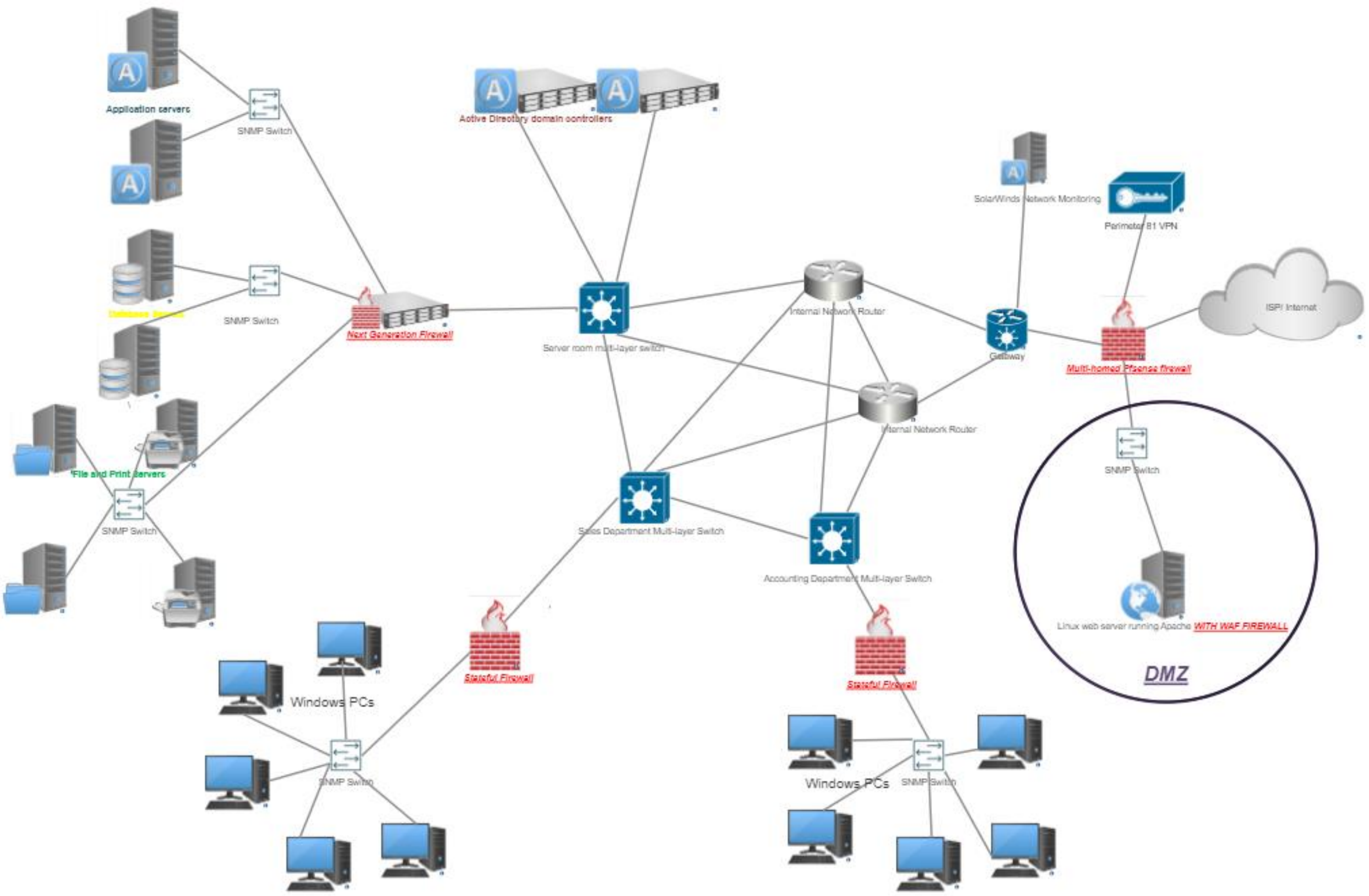
## This is a made-up company and the report is realistic to hypotheticals



# Corporation Tech Network Design Recommendations

The network design I recommend for Corporation Tech's would be a traditional three-tier architecture including a core layer, distribution layer, and access layer. The network would start at the ISP or internet provider, and moving left you would find a dual-homed firewall. This is an enhancement to the border firewall on the network. The dual-homed firewall allows for firewall rules to be set for the WAN and LAN interfaces to block unwanted traffic. The dual-homed firewall runs pfsense, an open-source Linux-based Firewall solution that performs as a router and a firewall.

The firewall will function on a dedicated Linux system and be accessible via the web on the web configurator within the network. The web configurator will allow the firewall administrator to set rules for the firewall isolating the web server and the internal interface. This firewall will forward/route WAN/outside HTTP traffic to the IP address of the Linux-based Apache web server. The web server would then be isolated from the internal network by the firewall. All HTTP traffic destined for the server will be forwarded to it safely, and without involving the internal network.

Moving further from the firewall is the network gateway that logically separates the internal network from the WAN/web server. This network gateway offers DHCP services and Network Address Translation for internet communication. The gateway being at the core layer of the network connects itself to a SolarWinds Network Monitoring system. This network monitoring software will allow network administrators to view network traffic and statistics across the internal network in one unified solution. This allows for easy network monitoring using the SNMP simple network management protocol. SolarWinds will then allow you to view network statistics by polling the management information bases on the network devices to obtain all critical performance metrics.

SolarWinds will poll all smart devices such as the windows servers in the server subnet, as well as the multilayer managed switches to aggregate and organize network information in one easily accessible place. This will leverage the goal of constant and

24/7 communications by ensuring network bottlenecks or errors/issues are caught early on through monitoring.

Connected to the network gateway is two internal routers. These routers will allow distribution layer switches to route packets to different subnets that are logically separated. Both internal routers are connected to each other and to the network gateway. This is to ensure redundant communications in case of a point of failure. This is also to allow clients to route packets outside of the internal network to the gateway for internet browsing.

The first switch belongs to the server room/server subnet that is logically separated from the other subnetworks. The switch is a multi-layer managed switch that offers SNMP compatibility for network monitoring. The multi-layer switch allows for layer 3 switching using IP addresses between the subnetworks. This allows for redundant communications in the presence of router issues/errors. This switch is also connected to the 2 other multi-layer switches as well as the two internal routers. Again, this is for redundant communications 24/7.

The server room switch is connected to three separate L2 switches. The first L2 switch connects to the two application servers running Microsoft Windows Server. They are isolated with their own switch to reduce bandwidth use when clients just need to access applications, not necessarily all servers. The second L2 switch is connected to the database servers running Microsoft windows Server with SQL. Those two servers sit isolated from the application servers for bandwidth efficiency. The third L2 switch is connected to the file and print servers. They are together keeping in mind that often clients may need to print files located on the file servers.

The second multi-layer switch is connected to the Sales department subnetwork which is connected to the first muti-layer switch for the servers as well as the third multi-layer switch for the accounting department and the two internal routers. These many connections allow for redundant communications and prevent a single point of failure from causing dreaded downtime.

The Sales department multi-layer switch is a managed switch with SNMP compatibility for network monitoring at the core network gateway. It is connected to an L2 switch. The L2 switch is connected to the Sales department client Windows workstations.

The accounting department multi-layer switch is also a managed switch with SNMP compatibility for network monitoring at the gateway. The accounting multi-layer switch is connected to the sales department switch and the server switch, along with the two internal routers. This allows the network to have a mesh logical topology and ensures communication redundancy in case of a single point of failure.

Both sales and accounting departments carry client workstations that are logged in with active directory accounts to authenticate and access shared resources being the application, database, file, and print servers.

The network will continue to utilize IPv4 addressing to reduce network bandwidth use and network resources. It is extremely widespread and is most common among devices on the network. The deployment process for IPv4 remains the most efficient compared to IPv6. Even though IPv6 offers good security, firewall selection and network placement will handle most security concerns the network might face. It is wise to take more time and investment into ensuring firewall security instead of relying on complicated IPv6 addressing. There is no need to worry about NAT translation as the gateway offers that service by default. NAT speeds are mainly dependent on the ISPs service and most ISPs serve IPv4 NAT translation/addressing at much more reasonable prices and at comparable speeds to IPv6.

These next recommendations will include my firewall and network authentication recommendation and placements on the corporation Techs' Network. The network will house and monitor a total of four main network firewalls. The network will also include a demilitarized zone to increase perimeter security and protect the internal network. The network will include two domain controllers running active directory and advanced authentication to network resources.

Starting at the perimeter of the network is a Demilitarized zone connected to the perimeter firewall. Since the perimeter firewall is old, I recommend upgrading to the pfsense firewall and using it as a multihomed firewall with three separate interfaces. It is an open-source firewall solution that can also work as a next-generation firewall. Pfsense will allow Corporation Tech to set important firewall rules for the DMZ. It would be configured to check the source IP address and forward packets to the publicly accessible web server. With Pfsense, your corporation will be able to set multiple rules for the DMZ. The DMZ interface will be facing the publicly accessible web server and judge what can enter. You will also be able to install additional packages to increase DMZ interface security. Within the DMZ is the publicly available web server. To protect this server, I recommend an application firewall installed to act as a proxy to the web server and handle all HTTP requests in a secure manner.

Along with the pfsense DMZ facing interface, your corporation will also be able to set the VPN-facing interface security. You will be able to set rules for the VPN interface to allow only certain clients in. You will also be able to set standards for what clients can join the VPN server. The pfsense firewall will function to also route packets as a gateway to the internal network in case clients are accessing the internet. There are also IDS and IPS solutions Pfsense will also function to filter not only ingress rules but egress. Packets that exit the internal network will be filtered to make sure nothing exits the network that shouldn't, such as ICMP replies.

Moving to the internal firewalls are the two stateful packet inspection firewalls placed between the two departments and the layer 3 switches that connect them to the routers. These two firewalls have all the normal firewall features with ACLs that will be redundant to the pfsense as well as offering inspection of packets. The stateful packet inspection firewalls will be able to track packets going into the two departments and out. This will prevent unauthorized attempts coming from the clients as well as forged messages. Stateful firewalls intercept packets at the network layer and then derive and analyze data from every communication layer to improve security. Information about connection state and other contextual data is stored and dynamically updated. This provides valuable context when evaluating future communication attempts.

To prevent DDOS or DOS attacks, a network monitoring server is recommended for the network connected to the network gateway. Because each device is smart, you can monitor network devices with SNMP protocol and watch out for irregular activity to respond accordingly. SolarWinds is my recommended software to use for complete network monitoring. It is easy to use and aggregates all data in one uniform solution for analysis.

Moving to the server room; there is a next-generation firewall to prevent unauthorized access and provide a uniform solution to all security needs for the server room. I recommend Palo alto for firewall implementation. It is voted best in many lists as a next-generation firewall and provides IDS and IPS, anti-malware, anti-virus, ACL, and much more. This is crucial since server resources are a very important asset to protect, if not, the most important.

For network resource authentication, I understand your business need to improve upon the normal username and password approach. That is why I recommend the implementation of active directory and two domain controllers to authenticate clients requesting  to access the network resources. Using the Microsoft server active directory, you will be able to set firewall rules and authentication rules for clients. Additionally, you can add the service ManageEngine ADSelfService Plus which integrates into active directory, incorporates Zero Trust, Multi-factor authentication, and password-less sign-on.

For client machines in the sales and accounting department, I recommend additional antimalware and antivirus software besides the native firewall from Microsoft defender. I recommend Bitdefender for all client PCs in the office. Bitdefender is an economic solution to help prevent malware and virus from infecting client PCs. Not only that but Bitdefender offers plans to best suit your business needs and there is always room for expansion and growth with the plans they offer.

The domain controllers connected closely with the servers near the server room need a local IPS system to prevent intrusion trying to get to the domain controller. The IPS software I recommend being installed on the domain controllers is Azure Firewall Premium IDPS. This easily integrates within Microsoft and would greatly benefit the domain controller systems. It offers 24/7 network monitoring, Intrusion rules enforcement, Malicious presence detection, and Malicious presence blocking.

Today, many employees need to work from home and access work resources remotely. To facilitate remote work, ensuring work-from-home employees have secure and zero-trust access to the internal network is extremely important to the business. With remote access, there are many VPN solutions that could work for Corporation Tech to ensure a high level of security is maintained. After having done my research and considering the different options, I recommend installing Perimeter 81's VPN solution.

Perimeter 81s VPN solution would be located and connected to the pfsense border firewall. The reason why Pfsense will not be the main VPN solution for the company is to segregate and spread out the network resources and allow Pfsense to manage less load on its own. It is also because Perimeter 81 integrates better with active directory services and has more admin control/options to be configured. Perimeter 81 will then run on its own standalone server to handle VPN requests and isolate VPN communications for the best performance.

More information on Perimeter 81 is available on their website. I will summarize high-level features that are included. Perimeter 81s VPN solution uses IPsec as its VPN protocol. Although SSL may seem more secure at face value because it allows users to access one specific resource or server on the network, active directory users that will be working from home will inherently need to communicate with the entire network instead of just one server. Since Corporation Tech is an office with physical hardware components that need accessing compared to cloud infrastructure, IPsec is the preferred VPN protocol to use. With IPsec is increased productivity and an equal level of access as compared to being in the office.

You need not worry about hackers accessing the network since IPsec will encrypt the VPN traffic in a secure manner. Not only that but by ensuring the correct configuration policies are followed on the rest of the network, this VPN solution proves itself most secure compared to SSL. Another reason why IPsec is better suited for your company is that your employees can access almost anything on the network that you could if you were locally connected such as servers, printers, and attached storage which you have set up in your server room. IPsec operates at the Network Layer of the OSI model, meaning users have full access to their corporate network regardless of application. A good VPN setup should provide remote users with the opportunity to achieve the same level of productivity as if they are sitting at their desks connected to the LAN.

On to Perimeter 81s VPN solution features. Perimeter 81s VPN solution offers one cloud-based platform to connect and secure all local resources on your network. It includes access management, monitoring, security and much more. It also offers the options to enable 2FA, single sign-on, and automatic Wi-Fi protection for mobile devices, PC and Mac desktops, and the web when connected. Not only that but you can reduce your attack surface by implementing least-privilege access policies on top of the pfsense border firewall. With Perimeter 81, you can also define the IP addresses that are allowed to access the network, allowing your IT team more control over security and the ability to assign static IPs to trusted sources of traffic.

One very important and valuable part of Perimeter 81s VPN solution is that it allows for IT administrators to control the security posture of those employees that connect remotely. Security posture control is ensuring that the devices that request connection to the internal network through VPN are approved based on the security posture of their devices. This means that each employee device connecting to the VPN will run through a series of standards that determine whether they are able to secure a connection. If the device or device configurations do not adhere to the IT admin standards created by the company, the connection is not made available to them.

What this means for Corporation Tech is additional and defense-in-depth security for those who connect to the internal network. As an IT admin, you can set standards to check for software versions making sure it’s up to date. You can ensure only specific kinds of devices are able to connect, for example, only Windows PCs of a certain type may connect. You can ensure the device that tries to form a connection has certain firewall software installed and running. Perimeter 81 DPC (device posture check) rules check all kinds of operating system devices before and during access and work to remove any devices where there’s a discrepancy between the admin policy and current posture.

To summarize my report, I will go over each network enhancement in simple terms which I have recommended. As a growing business, you will need to improve your border security, the larger the company, the larger the threats will be. Therefore, I have recommended a multi-homed firewall such as the Pfsense firewall. It is open source so it will allow the allocation of other business expenses to go toward internal security. This provides your company balanced security standing instead of only relying on border security. The Multi-homed Pfsense firewall allows ease of access and control as it allows you to configure your rules through the web. This will make business operations more efficient as it is one less thing to worry about.

Your IT team will appreciate the level of customization and personalization that Pfsense will give to the business. Because your company has lots of work-from-home employees, it was crucial to make sure that area is locked down and secured. I have recommended Perimeter 81s solution as it works well with customer accounts, takes the load of work off the IT team, saves time, and strengthens login security with multi-factor authentication. This VPN solution will save the IT team more time to work on more important projects that need their attention. The VPN solution I have chosen for your network keeps intruders from getting in at a granular level and would best match the security policies you have already created for the company internally.

The next enhancement I have chosen for your company is active directory accounts and domain controllers on the network. I have chosen this to allow clients to have an easier time and a more secure way of using the different servers that are on the network. Along with that comes the network monitoring solution. Because you have requested 24/7 communication, I have recommended SolarWinds network monitoring so the IT admin can view the statistics of the network and be able to spot issues before any major downtime takes place. Speaking of constant communication, I have advised multiple repetitive connections between systems to allow for redundant communication in case one routing system goes down, communication keeps going.

Another enhancement I have made is adding two stateful inspection firewalls for the two departments. This is mainly to make sure each piece of communication in and out of the two departments is carefully inspected for common attacks and prevented by the firewall. Another major enhancement is the addition of a next-generation firewall in the server room. This is a unified solution for anti-malware, antivirus, and complete firewall support to make sure your most valuable assets are protected in the most complete way.

As for the two domain controllers, they will house a Microsoft-based Intrusion protection system. Domain controllers control the network servers and the employee’s active directory accounts, we need to make sure all attempts of intrusion are prevented. For all client computers, I recommended Bitdefender, it is an economic solution that allows your IT staff the freedom to configure and fine-tune the security of multiple client access avenues, whether that’s the local system, internet connection, or internal communication.