

Network Design

Steven Counterman and Sasha Crawford

Department of Science, DeSales University

CS-416: Security

May 2, 2025

Project Part 1: Network Design

Network Design

Corporation Tech's current network consists of a large variety of devices and access points for both users and employee work stations. To achieve the highest network efficiency whilst also maintaining a high level of security, the company should utilize a layered security approach that controls traffic and segments domains. To enhance security, a demilitarized zone (DMZ) should be implemented. A DMZ acts as a protection layer or buffer between outside requests and internal company requests. The buffer reduces the risk of attacks from direct access to company application servers or databases. Furthermore, when the DMZ receives requests from users, the DMZ will arrange sessions independently and create a separation between networks connected to a dual firewall.

Beyond that, it is essential to segment the internal network into Virtual LANs (VLANs). VLAN segmentation would occur between different departments, as well as web servers, application servers, database servers, etc. The segmentation, when utilized through Access Control Lists (ACLs), allows for specific authorization of traffic

communication. Additionally, the utilization of VLANs improves security, performance and traffic control.

Network Topologies

Physical Topology

The best-fit network topology for Corporation Tech is a star topology. This star-based hierarchical structure allows for high

availability, security, and scalability. To start,

Cisco Firepower 2130 Firewalls are placed

the network edge. They serve to filter

inbound and outbound traffic and separate

internal network from the internet. This

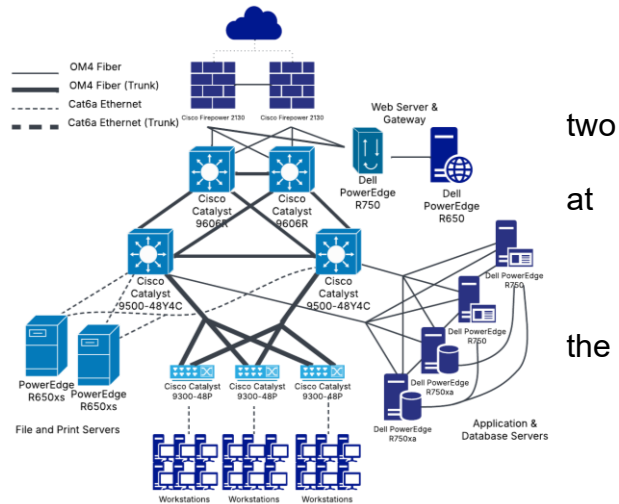
firewall supports up to 5.4 Gbps Intrusion

Prevention System throughput (Cisco, Cisco Firepower NGFW, 2017) and ensures high performance to handle enterprise-level traffic and provide room for future scalability.

Built-in Cisco Firepower Threat Defense provides an IPS, Advanced Malware

Protection, and URL filtering.

Two critical components that require careful network placement for security, performance, and interoperability are the web server and the protocol translator gateway. Both devices are physically separated from the rest of the network, connected solely to the firewalls. The main purpose of the protocol translator gateway is to translate the web server that runs Linux/Apache to Windows for the other servers and workstations. The choice of the PowerEdge R650 for the web server provides for a compact, high-performance design that is compatible with Linux and Windows. This



server supports OM4 fiber connectivity with 4TB RAM support for fast storage when serving web content. The protocol gateway will be utilizing a PowerEdge R750, which has dual redundant power supplies that ensure consistent uptime, and an Intel Xeon Scalable Processor to handle requests efficiently (Dell, n.d.).

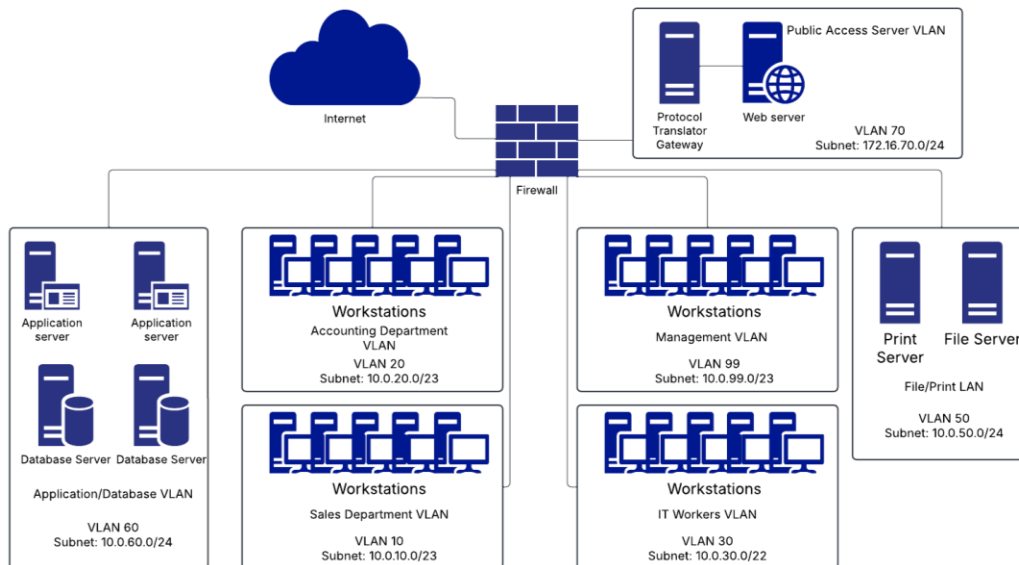
The core layer is the backbone of the network, connected to both the firewalls and distribution switches via OM4 fiber cabling. Dual layer 3 core switches prevent a single point of failure and focus on fast layer 3 switching. The Cisco Catalyst 9606R switch features a chassis-based 6-slot design which allows for modular expansion, ensuring future scalability. They can support up to 25.6 Tbps switching capacity, Virtual Switching System support to eliminate switching loops, and QoS features that can be used to prioritize critical traffic (Cisco, 2024). The distribution layer acts as a central aggregation point for access switches and servers, reducing the number of direct connections to the core. These switches also handle layer 3 inter-VLAN routing, which reduces the load on the core switches. The Cisco Catalyst 9500-48Y4C switch model has 48 25GbE ports, supporting fiber uplinks from access layer switches and fast server connectivity. The 4 100GbE uplinks provide high-speed connectivity to core switches (Cisco, 2024). With up to 6.4 Tbps switching capacity and ACL support, this model handles the tasks of this role effectively.

The application and database servers are connected to the distribution layer switches via OM4 fiber, separating them from the public network so that only authorized users can access them. The application and database servers are connected to each other in a full mesh fashion to provide maximum redundancy and minimal latency. The PowerEdge R750xa model used for the database servers is a 2U server, permitting 8

2.5-inch SATA, SAS, or NVMe drives supporting up to 122.88 TB of storage. This can be increased further by direct-attach NVMe SSDs, supporting up to another 92.1 TB of storage (Dell, 2022). The file and print servers are also connected to the distribution layer switches via Cat6a ethernet cable as they require significantly less throughput than that which OM4 provides. PowerEdge R650xs server models are used here. They are 1U rack servers which optimize space and can accommodate up to 16 Dual Inline Memory Modules to handle simultaneous file and print requests.

The access layer is responsible for providing devices, such as workstations, with network connectivity. For this layer, the Cisco Catalyst 9300-48P switch model is used. This switch offers 48x Gigabit Ethernet ports and Power over Ethernet for possible usage for wireless access points if a wireless network were to be necessary (Cisco, 2024). There will be a total of 25 switches with 48 ports each, totaling 1200 ports for workstations and other devices. All workstations can be connected to these switches as they are logically separated into VLANs.

Logical Topology



This network is segmented into multiple VLANs, ensuring logical isolation of traffic, enhanced security, and reliable performance. Each VLAN has ACLs and firewall rules to restrict unauthorized traffic between different network areas. All VLAN-to-VLAN communication is routed through the distribution layer. Also, all VLAN traffic between switches is carried over 802.1Q trunk links to ensure proper VLAN segmentation and interconnectivity across the network layers while maintaining logical separation of network traffic. All internet-bound traffic passes through the firewalls at the network edge before reaching the ISP connection. The web server resides in the DMZ, meaning it can be accessed externally, but cannot directly communicate with internal servers. The application servers communicate directly with the database servers, but users cannot directly access databases. The file and print servers allow authorized users to store and retrieve documents but are restricted to internal traffic. To avoid single points of failure, this network is designed with dual firewalls in Active/Passive mode, dual core

switches, stacked distribution switches, and link aggregation control protocol for access layer switches.

High-Level Availability Plan

To maintain continuous network availability, this network design includes redundancy, failure mechanisms, and proactive monitoring to guarantee maximum uptime. Redundant connections for network-critical devices are made to avoid single points of failure. Virtual Switching System (VSS) allows both switches to act as one logical unit for failover. Dual firewalls ensure that one is always active, and the second can take over in an instance of failure. Trunk links between switches utilize LACP to balance traffic and provide backup paths to automatically reroute traffic and avoid routing loops. Dual power supplies are included with switches and servers to prevent outages. Generators should be on standby as a source of long-term power in the case of extended outages. Proactive monitoring with SNMP should be used to alert hardware failures and security threats, along with proactive response teams to ensure fast resolution. Regular firmware updates and security patches are to be applied periodically, along with network tests for potential bottlenecks. A structured response plan will be developed so that network failures, cyberattacks, and disasters have a standard operating procedure to minimize damage. RAID 10 will be utilized for database servers to have additional copies of data and offsite data replication will be used to avoid total data loss. Finally, all network-critical devices will have on-site replacements in case of hardware failure or reaching the device's time-to-live.

Continuing IPv4

Currently, Corporation Tech operates on an IPv4 system. IPv4 allows for easy integration with the company's current devices and services without large upgrades taxing the system. It would be in the company's best interest to continue IPv4. Not only would this continuation be cost effective based on lower transition costs and utilization of existing network infrastructure, but it also includes a widespread compatibility with workstations. It is also important to note that the company's current devices may not transition or support IPv6 – eventually increasing costs of implementation and creating complex issues to resolve.

While there are a few limitations to IPv4, such as minimal address space and inability for high level encryption, it is not necessary to make the costly transition. IPv6 offers an increased space utilizing 128 bit IP as opposed to IPv4 with 32-bit addresses and security through data authentication and encryption. However, the network of Corporation Tech is not physically connected to external networks. The lack thereof of connection to external networks reduces risk and makes the company much less vulnerable to cyber attacks or unauthorized access. Private IP addressing through IPv4 is sufficient for Corporation Tech. Evidently, due to high costs and complex transitions, it is most beneficial for the company to continue use of IPv4.

Firewall Selection

Upon completion of research, the Cisco Firepower 2130 should be used for this network. They cost approximately \$9300 per unit. Their throughput is 5.4Gbps, which is sufficient to support enterprise-level traffic and future scalability (Cisco, 2024a). Built-in Cisco Firepower Threat Defense provides an intrusion detection system, intrusion prevention system, Advanced Malware Protection, and URL filtering (Cisco, 2024b).

Next-Gen Firewalls (NGFWs) are inherently cost-effective, as they combine the functionality of multiple devices into one. In being cost-effective, using this same model for each implementation keeps network management uniform and centralized. They are flexible, high-performing, and well-suited to this network architecture designed for scalability. This firewall model can perform audits, authenticate users, and offer role-based access control and centralized security management. Implementation can be complex due to the wide range of features NGFWs provide, but the organization's expertise in IT support should make deployment relatively straightforward.

I recommend the purchase of six units: two for the network edge, one for each of the two server VLANs, and one for the workstations. The final firewall should be kept on-hand in case of hardware failure to minimize downtime. The servers would connect to their respective firewalls, and the firewalls to their respective distribution layer switches. The distribution layer switches handle inter-VLAN routing and are connected to one another for redundancy, so the single workstation firewall should be physically connected to a distribution layer switch to provide support at this level. Finally, the two firewalls at the network edge will filter incoming traffic and separate the DMZ from the internal network.

DMZ Plan

Since this network is logically separated using VLANs, creating a DMZ can be done by creating a separate VLAN, having physical separation from the LAN, and setting firewall rules and Access Control Lists. First, the DMZ should be physically separated from the remainder of the LAN. The DMZ contains the web server and the protocol translator gateway, which should be directly connected to both firewalls on the

network edge for redundancy. Second, the DMZ will be logically separated by residing on its own VLAN. This can be accomplished by creating a new VLAN (70) and assigning a subnet (such as 172.16.70.0/24). Along with logical separation through VLANs, firewall rules and Access Control Lists need to be created.

Firewall rules should be implemented as follows. Allow incoming TCP traffic on specific ports (such as 80 for HTTP and 443 for HTTPS) to enable external users to create secure connections with the web server. Only return traffic (i.e., pre-established sessions) from the DMZ should be allowed. This prevents the server from starting outbound connections to the public internet, reducing exfiltration risk. Preventing compromised DMZ hosts from reaching internal systems is of utmost importance. This requires establishing a zero-trust security policy. A rule will be implemented to block all traffic from the DMZ to the LAN by default. To ensure proper access to resources, an exception will allow a host in the management VLAN to access the DMZ for updates and backups. Specific LAN-to-DMZ traffic will be permitted to maintain essential accessibility. This protects DMZ hosts from lateral movement and unauthorized internal access. Access Control Lists build upon firewall rules, enforcing tighter restrictions at the switch level. There are two specific concerns at this level. First, block any traffic from the DMZ VLAN trying to route to other VLANs unless it is explicitly allowed. Additionally, ACLs will drop unauthorized inter-VLAN traffic at the switch before it reaches the VLAN firewalls. In summary, creating an isolated DMZ logically and physically separates the DMZ from the internal LAN, preventing unauthorized traffic from reaching sensitive systems and stopping many cyberattacks before they start.

Network Authentication

Corporation Techs should implement a multi-layered authentication system to improve security. The company should take on a more centralized authentication approach to keep the usernames and passwords more secure. The single sign on (SSO) protocol allows for a single user to sign on to multiple applications without revealing a secure password. This protocol utilizes a service that has its own database but does not have a unique HTTP interface. Furthermore, when the user is required to input their secure username and password, it is best there is multi-factor authentication as well. Multi-factor authentication can either be a security question that must be entered correction, a biometric, or a one-time passcode that is accessible from a separate device. This increases security even if the credentials of their user and pas were compromised. Lastly, encrypting communications will increase the overall network security. Unencrypted networks can leave credentials vulnerable to attacks over the network.

Secure Authentication for Internal Network Resources

To best secure internal network resources, the combination of firewalls, MFA, SSO, and encrypted communication will provide the best security and usability. The Cisco Firepower 2130 firewalls provide high levels of protection whilst still being scalable. As Corporation Techs evolves, this firewall will be able to satisfy their demands. Utilizing DMZ furthers the network security approach and safeguards internal resources from external threats. Additionally, utilizing SSO with MFA reduces the risk of unauthorized access to the company and to the company's resources. Finally, encrypting all communications across servers creates secure data transmission and

limits the possibility for information interception. This plan allows room for growth in the company while being efficient and secure.

SSL VPN

As Corporation Tech begins to expand its workforce to include a remote workforce, a secure virtual private network (VPN) is paramount for the protection of sensitive data and authorizing access to internal resources. Corporation Tech should implement an SSL tunnel VPN, accessible through a trusted vendor like Cisco AnyConnect or Fortinet. An SSL VPN would allow workers to access the organization's network remotely without special software (Fortinet, n.d.). They function at the application layer and utilize standard web browsers for connectivity. There are two modes for these types of VPNs: SSL portal VPNs and SSL tunnel VPNs. The former provides access to specific applications through a web interface. Meanwhile, tunnel VPNs establish a secure tunnel that allows a wide range of accessibility that the workers would need, besides just web apps.

IPSec VPN

The other option I compared was an IPSec VPN. These VPNs operate at the network layer and encrypt and authenticate IP packets between endpoints. Typically, they are used for site-to-site connections. They require specialized client software and configurations. On one hand, IPSec VPNs provide robust security but have a complex setup and require frequent maintenance. These requirements prevent it from being a viable option for scalable remote access (Fortinet, n.d.).

Given Corporation Tech's need for comprehensive remote access, the SSL tunnel VPN option is preferred. Remote workers would have access to multiple internal services

rather than solely web applications. SSL/TLS protocols are used for data encryption, which protects against eavesdropping and man-in-the-middle attacks. The accessibility of these VPNs reduces the complexity of client-side installation as they are accessed through standard web browsers. Finally, SSL tunnel VPNs provide scalability in that they allow for the addition of new users without extensive infrastructure changes.

Best VPN Choice

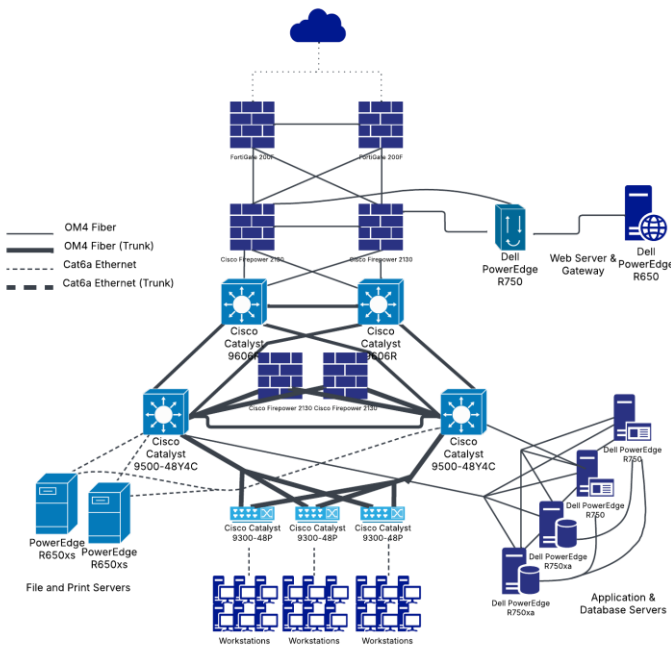
As the senior architect requested, the SSL tunnel VPN option will prevent unauthorized access and protect against snooping. Authentication methods such as digital signatures and MFA can be applied to the VPN gateway. This ensures that only verified users can access internal resources. SSL/TLS VPNs utilize Transport Layer Security (TLS) encryption protocols (Fortinet, n.d.). TLS guarantees that all traffic between the remote workers and the company's servers has end-to-end encryption. Any eavesdropping or man-in-the-middle attacks would be thwarted due to this encryption. Administrators can configure the subnets so that only specified services are accessible through the tunnel. Lateral movement through the network subnets and minimized attack surface are resulting security benefits to this (Fortinet, n.d.).

Other VPN Options

An alternative remote access that could be used would be SSH for example. Secure Shell is useful for remote administrative access to internal servers and infrastructure. The protocol, SSH, utilizes cryptography in order to enable secure communication between remote machines. Furthermore, all SSH access should be tunneled through the SSL VPN to ensure that internal systems are secure from public

access. This layered approach prevents unauthorized access attempts and mitigates the risk of brute-force attacks.

Adjusted Network Design



Above is the completed network diagram. Several updates were made to the physical layout but the VLANs and logical separation remain unchanged. Upon review of our selection of firewalls, we determined that a firewall at each subnet would result in inefficient costs and diminishing returns.

Instead, this design utilizes dual redundant firewalls at the distribution layer, which enforce access control for inter-VLAN routing.

On the distribution layer switches, Policy-Based Routing (PBR) will be used to selectively inspect critical inter-VLAN traffic. This approach balances security, network efficiency, and cost, while also providing fault tolerance in the event of firewall failure. Additionally, a pair of redundant bastion firewalls have been deployed at the network edge to absorb and inspect incoming external traffic. We selected FortiGate 200F firewalls, as having different software stacks provides firewall diversity and reduces similar vulnerabilities. FortiGate also provides a strong IPS, anti-botnet, and web filtering engine (Fortinet, 2024).

Overall, this provides defense in depth, meaning that if the bastion firewalls were to come under attack, and are eventually compromised, the internal network would remain

operational, and the attack would be contained. Finally, host-based software firewalls will be deployed on each workstation to enforce node-level access control and reduce the risk of lateral movement through the network.

Conclusion

The design and implementation of a secure, high-performance network for Corporation Tech provides the ability to accommodate the company's future growth, operational efficiency, and cybersecurity posture. Through careful planning and integration of industry best practices, this network design addresses the core requirements of reliability, scalability, security, and manageability.

Starting with the selection of robust, enterprise-grade hardware and devices, such as Cisco switches and Fortinet firewalls, the network infrastructure is built to handle current demands while remaining flexible enough to accommodate future expansion. Logical and physical topologies were designed to support clear segmentation between departments, ensure streamlined communication paths, and provide redundancy in case of device failure or cyberattack. The implementation of the DMZ (Demilitarized Zone) and VLANs enables Corporation Tech to isolate critical resources, protect internal assets, and facilitate secure external access to public-facing services.

Security is a cornerstone of this design. Multi-layered protections—ranging from packet-filtering firewalls to access control lists, VPN tunneling, and multi-factor authentication—are woven throughout the network to uphold the principles of zero-trust architecture. This ensures that users and devices must be authenticated and authorized before being granted access, significantly reducing the attack surface.

Furthermore, the IPv4 addressing scheme was carefully constructed to support hierarchical network management, efficient routing, and scalable subnetting. Network Address Translation (NAT) provides an added layer of security for internal addresses, while Dynamic Host Configuration Protocol (DHCP) automates IP assignment to reduce administrative overhead. The inclusion of Domain Name System (DNS) services ensures seamless resolution of internal and external resources.

Business continuity and disaster recovery are also embedded in this design. Redundant paths, failover mechanisms, regular backups, and monitoring systems such as Intrusion Detection and Prevention Systems (IDPS) are included to guarantee availability and quick recovery from disruptions. These features align with the critical goals of uptime, resilience, and data integrity.

References

Cisco. (2017, September). *Cisco Firepower NGFW*. Retrieved from

<https://www.secureitstore.com/datasheets/security/Cisco-Firepower-NGFW-Datasheet.pdf>

Cisco. (2024a, January 29). Cisco Firepower 2100 Series.

<https://www.cisco.com/site/in/en/products/security/firewalls/firepower-2100-series/index.html>

Cisco. (2024b, June 4). *Cisco Catalyst 9000 Switching Platform FAQ*. Retrieved from

<https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9000/nb-06-cat9k-swit-plat-faq-cte-en.html>

Cisco. (2024c, July 11). Integrated network threat appliances.

<https://www.cisco.com/c/en/us/products/collateral/security/ngips/datasheet-c78-742472.html>

Dell. (2022, November). *Purpose built server designed to address emerging and highly extensive GPU workload*. Retrieved from

https://i.dell.com/sites/csdocuments/Product_Docs/en/poweredge-R750xa-spec-sheet.pdf

Dell. (n.d.). *PowerEdge: Rack Servers Hardware Tech Specifications - Documentation*.

Retrieved from <https://www.dell.com/support/kbdoc/en->

References cont.

us/000203856/poweredge-rack-and-tower-servers-hardware-tech-specifications-documentation-videos

Fortinet. (n.d.). What Is SSL VPN? Retrieved from

<https://www.fortinet.com/resources/cyberglossary/ssl-vpn>

Fortinet. (2024). [https://www.fortinet.com/content/dam/fortinet/assets/data-](https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/pdf/fortigate-200f-series.pdf)

[sheets/pdf/fortigate-200f-series.pdf](https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/pdf/fortigate-200f-series.pdf)

Okta. (2025, January 14). *What is central authentication service (CAS)?* Okta.

<https://www.okta.com/identity-101/central-authentication-service/>