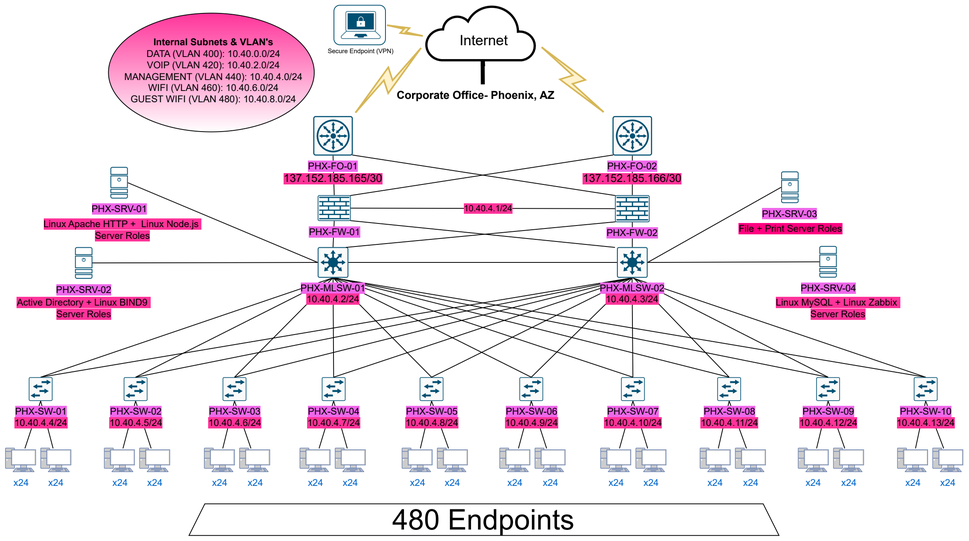


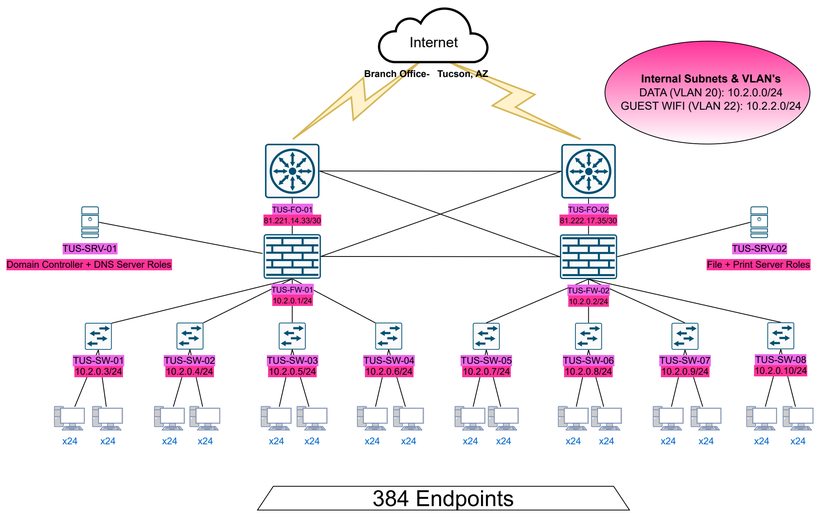
CANYON AERONAUTICS

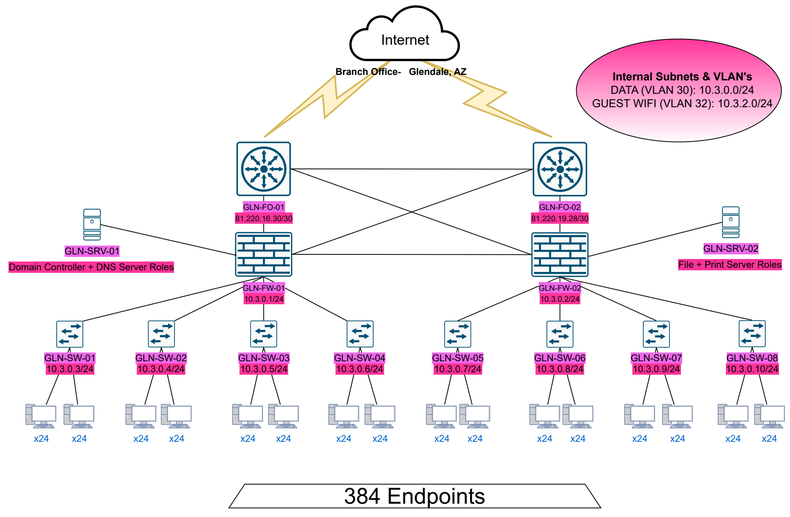
Network Engineer:
Grant Shell

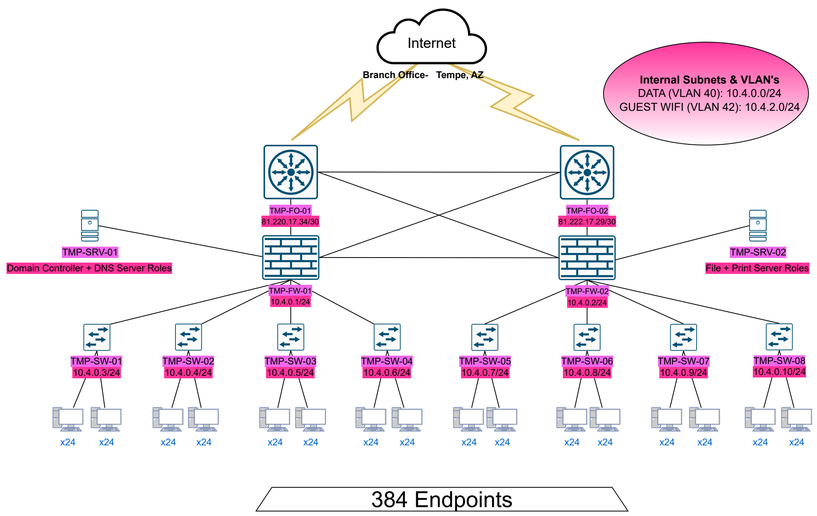
Total PC's = 2,016

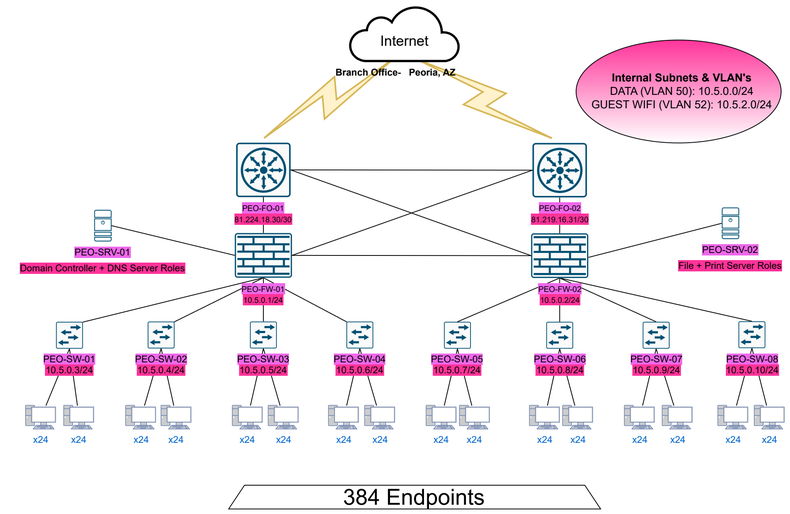
The Impact of Physical vs. Virtual Servers

Physical servers and virtualized servers impact my network topology in very different ways. With physical servers, each machine is tied to its own hardware and operating system, which makes my topology a little more rigid. Scaling requires adding new servers, switches, and cabling, which raises both cost and complexity. In contrast, integrating virtualized servers (VMs) would allow multiple server instances to share the same hardware, which would change how my topology is structured. Instead of each workload needing its own physical presence, several logical servers can connect through one interface while still appearing as separate devices. This flexibility makes it easier to scale my topology without physically expanding equipment. It also introduces internal traffic between virtual servers on the same machine, which reduces external switch traffic. Overall, physical servers make my topology simpler and more predictable but less adaptable, while virtualized servers create a more scalable and efficient design that reduces physical spread, yet requires closer attention to logical traffic flow and allocation of resources.









Server Roles

Web Server

A web server is usually placed at the network edge, where it handles HTTP/HTTPS requests from external clients and delivers web content. This separation reduces risk if the server is compromised, as it prevents direct access to internal systems. A web server is essential if an organization hosts its own website or web-based applications, though it may not be necessary if third-party cloud hosting is used (Is, 2024).

Application Server

An application server is typically located in the internal application layer of a network, behind the web server. It executes business logic, processes API requests, and connects to backend databases. Isolating the application layer improves scalability and protects sensitive data from direct internet exposure. While not required for simple static websites, application servers are vital for dynamic, enterprise-level systems (McDonald et al., 2022).

Active Directory

Active Directory (AD) is a centralized directory service hosted on domain controllers in the secure internal network. It provides authentication, authorization, and centralized policy enforcement for users and devices. Because of its critical role, AD should not exposed externally, and redundancy is essential to ensure resilience. AD is necessary in Windows-based enterprise environments but may not be required for organizations that rely on cloud identity solutions (Is, 2024; McDonald et al., 2022).

DNS Server

A Domain Name System (DNS) server translates human-readable names into IP addresses, supporting both internal and external communications. In a topology, public authoritative DNS servers often answer external queries, while recursive or forwarding DNS servers reside inside the internal network. DNS is fundamental to modern networking, although small organizations sometimes outsource the service to ISPs or third-party providers (Lyu et al., 2022; Xu et al., 2023).

File Server

A file server is located on the internal LAN, providing shared storage, permissions enforcement, and backup capabilities for authorized users. It centralizes file access, ensuring consistency and collaboration across an organization. File servers are often essential in traditional IT infrastructures, though in some modern environments they may be replaced by cloud storage platforms (Lyu et al., 2022).

Print Server

A print server, also located in the internal LAN, manages print queues, distributes drivers, and logs printing activities. This role allows centralized control and reduces the administrative overhead of configuring individual printers. While not always required in smaller sites where direct printer connections suffice, print servers remain valuable in larger organizations for efficiency and auditing (Xu et al., 2023).

Database Server

A database server stores and manages structured data using relational systems. Positioned in the internal network close to application servers, it ensures performance while remaining shielded from direct internet access. Database servers are essential for dynamic applications and business systems but unnecessary for static or lightweight services (McDonald et al., 2022).

Monitoring Tools

Monitoring servers are deployed within the internal management network, where they can poll systems, collect logs, and issue alerts. Their role is to track uptime, performance, and anomalies across infrastructure components. While not mandatory in small setups, monitoring tools are considered best practice for maintaining operational awareness and detecting issues proactively (Lyu et al., 2022).

References

Is, H. (2024). A novel approach to enhancing Active Directory security in academic institutions. Balkan Journal of Electrical and Computer Engineering, 12(4), 394–402. https://dergipark.org.tr/en/pub/bajece/issue/89866/1567393

Lyu, M., Habibi Gharakheili, H., Russell, C., & Sivaraman, V. (2022). Analyzing enterprise DNS traffic to classify assets and track cyber-health. arXiv preprint arXiv:2201.07352. https://arxiv.org/abs/2201.07352

McDonald, G., Papadopoulos, P., Pitropakis, N., Ahmad, J., & Buchanan, W. J. (2022). Ransomware: Analysing the impact on Windows Active Directory Domain Services. Sensors, 22(3), 953. https://doi.org/10.3390/s22030953

Xu, C., Zhang, Y., Shi, F., Shan, H., Guo, B., Li, Y., & Xue, P. (2023). Measuring the centrality of DNS infrastructure in the wild. Applied Sciences, 13(9), 5739. https://doi.org/10.3390/app13095739