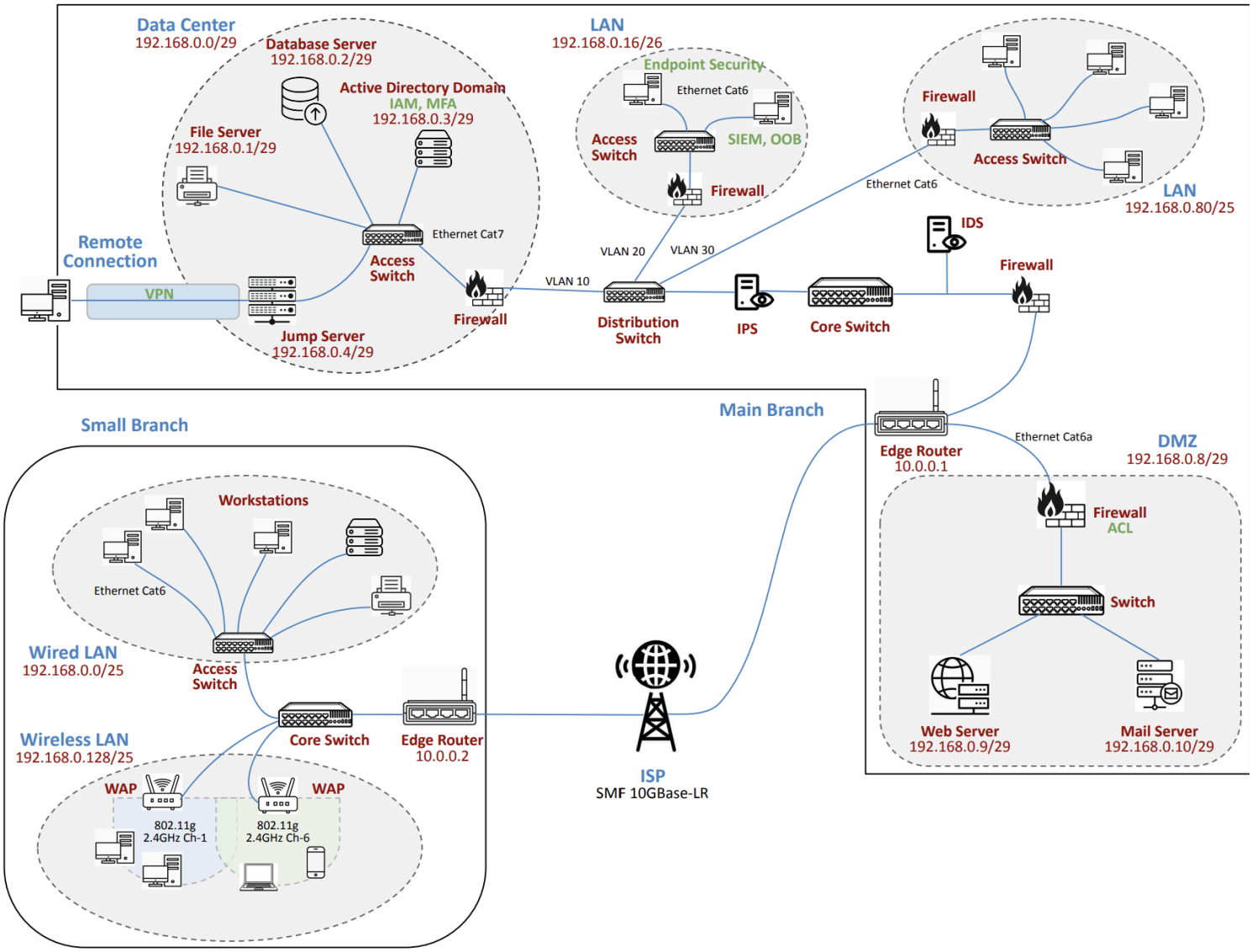
Secure Network Design

ITN 262, Network Comm, Security & Authentication

May Pwint Phyu

12th August, 2024

In this project, you are a new employee and your first task on the job is to design and document the company's network. This includes creating a secure network design, integrating Zero Trust concepts, and supply chain risk management (SCRM).



The organization consists of two branches, located approximately 35 miles apart, with IP addresses 10.0.0.1 and 10.0.0.2. Both branches connect to the internet via ISP using Single Mode Fiber (10GBase-LR), ensuring long-range, high-speed communication with minimal signal attenuation.

Branch Networks

Small Branch:

The company is equipped with both wired and wireless networking. It is designed with Wi-Fi 4 (802.11n) operates at 2.4GHz, using channels 1 and 6 to minimize interference.

Main Branch:

It is segmented into a DMZ, local LANs, and a data center using Variable Length Subnet Masking (VLSM) for efficient IP resource allocation and future scalability. The DMZ (192.168.0.8/29) is placed near the edge, isolating it from the internal network using 802.3 Cat 6a for fast data access. It contains the firewall, switch, web server (192.168.0.9) and the email server (192.168.0.10).

Internal Network Architecture

The private network is structured in a three-tiered hierarchy using core switches, distribution switches and access switches. The distribution switch isolates each subnet; VLAN 10 for the data center, 20 and 30 to the local LANs (192.168.0.16/26 and 192.168.80/25 networks), allowing usage of approximately 40 and 70 users, respectively. All workstations are equipped with Microsoft Defender for antivirus and firewall protection for endpoint security.

Network-based next generation Palo Alto firewalls are placed at the edge of each network for strict access to the assets and block unauthorized access to the resources. These firewalls have strong traffic inspection, malware protection, and security technologies providing concise scanning and control of the network traffic. Service-based Palo Alto Networks Prisma Access is used at the perimeter of the network to ensure Zero Trust Network Access to the internal resources by deploying strict identity verification, device security posture, and continuous trust evaluation. Along the spine of the network, network-based Intrusion Detection System (IDS) is connected in parallel and Intrusion Prevention System (IPS) in line for continuous network monitoring, SIEM management by using Splunk. Splunk can be used to search, analyze and visualize the data in the communication, that can visualize real time security monitoring, incident response and management, advanced threat detection and hunting, compliance, automation and orchestration.

In the data center (192.168.0.0/29 network), there are a file server (192.168.0.1), a database server (192.168.0.2), and an Active Directory domain, which is hosted on a server (192.168.0.3), and Ethernet Cat 7 cable is used for rapid data communication. The AD handles the logon credentials for signing in to the system on client workstations, where additional access control is incorporated to implement Multi-Factor Authentication (MFA) using Microsoft Authenticator. It is an application developed by the Microsoft corporation that supports multi-factor authentication, push notification, passwordless sign-in, multi-account support, backup and restore, and integration with Azure AD. It is compatible with both Android and iOS. Azure Entra ID is an Active Directory management system that offers Identity and Access Management IAM supporting SSO, MFA, identity protection, B2B and B2C identity

management. For any remote connection to the data center, whether it is accessed from an internal client for network configuration or from external devices remotely, will have to use VPN for secure connection and will land on the jump server for strict allowance and filtration of access to the center. Any unauthorized client will be denied access to the servers.

Supply Chain Risk Management (SCRM)

To maintain business continuity, it's essential to secure every phase of the supply chain: planning, procurement, production, distribution, logistics, etc. It is also important to take account of the potential risks such as natural disasters, cyberattacks (internal & external), supplier insolvency, inventory and procurement failures, financial and production disruptions. These can cause the disruption of seamless flow of services and information across the system, leading to significant impact on the efficiency, security, and availability of service, as well as reputational damage.

There is an asset, there will be risk. Although they are possible to mitigate, it is impossible to completely eliminate them to zero. Therefore, it is important to perform an in-depth analysis and plan the mitigation strategies ahead should one of the risks break out. This include diversification of suppliers (having different suppliers to avoid single supplier dependency just in case if some discrepancy happen with one source), systematic and proper inventory management to keep track of assets, license and life cycle management of the assets, enhanced security measure in the network topology by incorporating strong security protocols to protect the system, playbooks and runbooks for risk management plan with detail on how to effectively and timely handle a outbreak of the system to the supply chain.

By integrating well-founded mitigating strategies, the business can comprehensively reduce the vulnerabilities and risks that could disrupt the continuous flow of the supply chain operations.

References

IBM. (2023, December 2). *What Is Supply Chain Risk Management?* IBM. https://www.ibm.com/topics/supply-chain-risk-management

Microsoft. (n.d.). *About Microsoft Authenticator*. Microsoft Support. https://support.microsoft.com/en-us/account-billing/about-microsoft-authenticator-9783c865-0308-42fb-a519-8cf666fe0acc

Microsoft. (n.d.). *Microsoft Entra ID (formerly Azure Active Directory)*. Microsoft. https://www.microsoft.com/en-us/security/business/identity-access/microsoft-entra-id

Microsoft. (2024, May 2). *Microsoft Defender Antivirus in Windows Overview - Microsoft Defender for Endpoint*. Learn Microsoft. https://learn.microsoft.com/en-us/defender-endpoint/microsoft-defender-antivirus-windows

Palo Alto Networks. (n.d.). *Security Service Edge | Prisma Access*. Palo Alto Networks. https://www.paloaltonetworks.com/sase/access

Wopat, C. (2023, August 25). *Splunk Security Use Cases*. Splunk. https://www.splunk.com/en_us/blog/security/introducing-splunk-security-use-cases.html