VILNIUS GEDIMINAS TECHNICAL UNIVERSITY

FACULTY OF FUNDAMENTAL SCIENCES

DEPARTMENT OF INFORMATION SYSTEMS

SECURE ENTERPRISE NETWORK ARCHITECTURE LAB

Prepared by: Simonas Riška

Checked by: lect. [redacted]

VILNIUS 2025

Table of Contents

1. Task and Objectives

The task of this assignment is to design a secure Layer 2/Layer 3 enterprise network architecture using Microsoft Visio (or a similar tool), the objective is to create a realistic and technically accurate network diagram that demonstrates secure segmentation, layered defense and infrastructure planning aligned with security best practices.

The designed network must reflect a detailed and implementable setup using real-world technologies and devices commonly used in enterprise environments.

The network architecture includes:

- Multiple subnets and VLANs ensuring segmentation between roles and services (for example, Employee VLAN, Server VLAN, Guest/IoT VLAN, Management VLAN and Honeypot VLAN).
- Demilitarized Zone (DMZ) that hosts public-facing services such as a web server, email server, FTP server and application server.
- Internal endpoints such as laptops, desktop computers, IoT devices, printers and file servers.
- Perimeter security using firewalls with deep packet inspection and VPN access for remote users.
- Layered monitoring and protection, including Wireless IDS/IPS (WIDPS), Web Application Firewall (WAF) and Secure Web Gateway (SWG).
- Centralized log collection and network monitoring using Zabbix and the Elastic Stack (ELK).
- Hardware models from enterprise vendors such as Cisco, Fortinet, Dell and Aruba.
- VPN implementation to simulate secure remote access for hybrid work environments.

The goal is to deliver a realistic network infrastructure that balances performance, scalability and security controls.

2. Scenario

This network architecture represents a secure enterprise network deployed in a centralized office environment – design emphasizes network segmentation, traffic control and layered security, ensuring both operational efficiency and strong protection against internal and external threats.

Key zones and functionalities:

- Security Perimeter – all incoming internet traffic is first inspected by the Palo Alto PA-3220 firewall, which performs deep packet inspection and threat filtering, then traffic flows through the Fortinet FortiGate FG-1500D, providing additional security functions such as intrusion prevention, web filtering and antivirus scanning. Also, Aruba ClearPass is integrated to enforce access control and authenticate devices within the internal network.
- DMZ Zone – Dell PowerEdge R760 hosts externally accessible services, including a web server, email server, FTP server and application server – these services are isolated in the DMZ to minimize risk to internal resources while enabling public access.
- Internal Endpoints – internal network consists of laptops, desktop computers, file servers, IoT devices and printers – these devices are organized into VLANs to support role-based access control and optimize network performance.
- VLAN Segmentation
  The network is divided into several VLANs:
  - VLAN 10 – employees.
  - VLAN 20 – server infrastructure.
  - VLAN 30 – guest/IoT devices.
  - VLAN 40 – network management.
  - VLAN 99 – honeypot environment for threat detection and analysis.
- Network Infrastructure – core switching and routing functions are provided by two Cisco Catalyst C9300-48P switches and a Cisco ISR 4331 router. Wireless access is delivered via Fortinet FortiAP 231F access point supporting internal wireless users and IoT devices and also VPN connectivity is also implemented, allowing secure access for remote users.
- Security and Monitoring – the environment incorporates multiple layered security and visibility tools such as Honeypot VLAN to detect unauthorized activity, Web Application Firewall (WAF) to protect web services, Wireless IDS/IPS (WIDPS) for monitoring wireless threats, Zabbix for infrastructure monitoring, Elastic Stack (ELK) for centralized log collection and analysis, Secure Web Gateway (SWG) for outbound traffic filtering.

This architecture provides layered defense through segmentation, isolation of critical services and centralized visibility into network activity, following modern security design principles.

3. Reasoning Behind Selected Devices and Security Measures

The devices and technologies selected for this architecture reflect realistic, enterprise-grade solutions widely used in modern secure network environments – each component was chosen with both functional purpose and security alignment in mind.

Security Perimeter:

- Palo Alto PA-3220 – selected for its robust firewall capabilities, including application-aware filtering, threat prevention and initial traffic inspection.
- Fortinet FortiGate FG-1500D – acts as a secondary layer of defense, providing deep packet inspection, intrusion prevention, VPN support and web filtering.

Access Control:

- Aruba ClearPass – used for centralized network access control and identity-based authentication, enforcing policies on who and what can connect to the internal network.

Segmentation and Infrastructure:

- VLANs – logical separation of network traffic across Employee (10), Server (20), Guest/IoT (30), Management (40) and Honeypot (99) segments limits lateral movement, improves performance and enforces least privilege access.
- Cisco Catalyst C9300-48P Switches – enterprise-class Layer 2/Layer 3, offering VLAN support, security policies and high-speed access.
- Cisco ISR 4331 Router – serves as a core routing device capable of handling inter-VLAN routing, WAN connectivity and quality of service for critical applications.

DMZ and Public Services:

- Dell PowerEdge R760 – selected to host critical public-facing services (web, email, FTP, application) and it is isolated in the DMZ zone to reduce risk and contain threats from external access points.

Wireless Access:

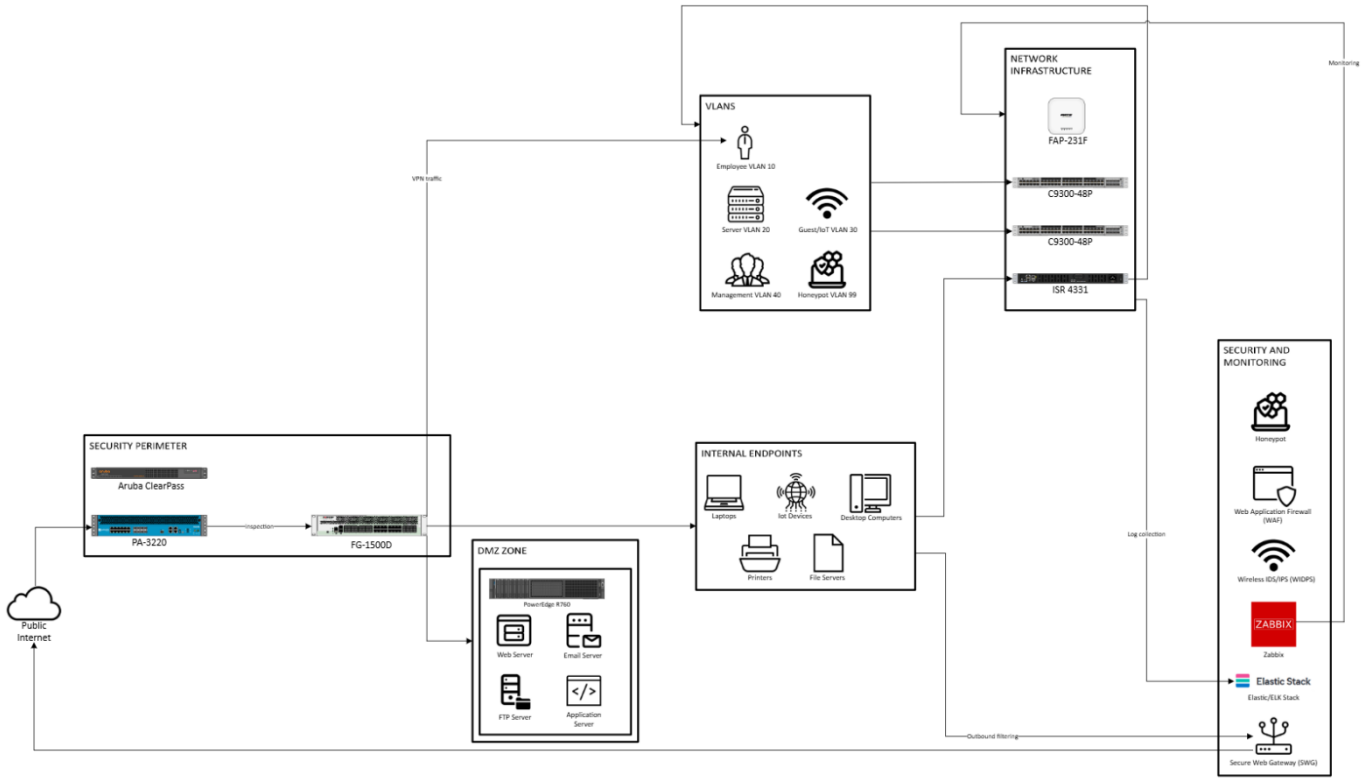
- Fortinet FortiAP 231F – a secure wireless access point that integrates with Fortinet security infrastructure, allowing centralized management and WIDPS support.

Monitoring and Detection:

- Honeypot VLAN (99) – a designated area for luring, detecting and analyzing malicious behavior without risking production systems.
- Zabbix – provides active monitoring, alerting and performance metrics for infrastructure devices and services.
- Elastic Stack (ELK) – aggregates logs from across the network, allowing for search, analysis and visualization of security-relevant data.
- Web Application Firewall (WAF) – protects public-facing applications by inspecting HTTP/HTTPS traffic and blocking common web exploits.
- Wireless IDS/IPS (WIDPS) – detects rogue access points, Wi-Fi threats and abnormal behavior on wireless channels.
- Secure Web Gateway (SWG) – filters outbound web traffic, enforces browsing policies and protects users from malicious or inappropriate content.

Each device and security measure were selected to enforce the principles of segmentation, visibility and control, aligning with best practices for building a resilient and secure enterprise network.

4. Network Diagram



5. References

Palo Alto Networks – PA-3220 Firewall

https://docs.paloaltonetworks.com/hardware/pa-3200-hardware-reference/pa-3220-series-overview

Aruba Networks – ClearPass Policy Manager

https://www.hpe.com/asia_pac/en/aruba-clearpass-policy-manager.html

Cisco – Catalyst C9300-48P Switches

https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9300-series-switches/nb-06-cat9300-ser-data-sheet-cte-en.html

Cisco – ISR 4331 Router

https://www.cisco.com/c/en/us/support/routers/4331-integrated-services-router-isr/model.html

Dell – PowerEdge R760 Rack Server

https://www.delltechnologies.com/asset/en-us/products/servers/technical-support/poweredge-r760-technical-guide.pdf

Elastic – ELK Stack (Elasticsearch, Logstash, Kibana)

https://www.elastic.co/elastic-stack

Zabbix – Monitoring Platform

https://www.zabbix.com/manuals

Icons & Stencils

https://www.cisco.com/c/en/us/products/visio-stencil-listing.html

https://www.paloaltonetworks.com/company/press-kit.html

https://www.visiocafe.com/hpe.htm

https://www.fortinet.com/resources/icon-library

https://www.visiocafe.com/dell.htm

https://www.f5.com/resources/visio-stencils