Project 2: Secure Network Infrastructure Design

Architecture for 50 End-points with Multi-layered Security Implementation

Prepared for:

Abdelrahman wael

Topic:	Advanced Network Security Design
Servers:	Web, Email, File Servers
Security Devices:	16 Specialized Appliances
Scale:	50 End-user Devices

December 24, 2025

Contents

1 Introduction **3**

1.1 Project Scope . . . 3

2 Network Architecture Diagram **4**

3 Security Component Specifications **6**

3.1 Detailed Device List . . . 6

4 Server Infrastructure Analysis **8**

4.1 Web Server . . . 8

4.2 Email Server . . . 8

4.3 File Server . . . 8

5 Endpoint Management (50 Devices) **9**

5.1 Security Policy for Endpoints . . . 9

5.2 Traffic Flow Logic . . . 9

6 Technical Specifications and Configurations **10**

6.1 Firewall Rule Sets . . . 10

6.2 IPS/IDS Signature Tuning . . . 10

6.3 WAF Policies . . . 10

6.4 DLP Sensitivity Levels . . . 11

6.5 Honeypot Strategy . . . 11

6.6 SIEM Correlation Rules . . . 11

6.7 PAM (Privileged Access Management) . . . 11

6.8 NAC Implementation . . . 11

6.9 VPN Gateway Configuration . . . 11

6.10 HSM Integration . . . 12

6.11 Proxy Server Benefits . . . 12

6.12 Endpoint Detection Response (EDR) . . . 12

7 Conclusion 13

A Glossary of Terms 14

Chapter 1

Introduction

Designing a robust network requires more than just connectivity; it demands a layered defense strategy (Defense in Depth). This project illustrates a corporate network architecture housing 50 devices, three core enterprise servers (Web, Email, and File), and an integrated stack of 16 security appliances.

The objective is to visualize the traffic flow from the public internet, through the Demilitarized Zone (DMZ), and into the internal secure local area network (LAN), highlighting where each security control sits in the hierarchy.

1.1 Project Scope

The scope includes:

- Visual representation of 50 endpoints.
- Deployment of 3 specialized servers.
- Implementation of 16 security controls.
- Structural hierarchy without IP addressing (Logical Architecture).

Chapter 2

Network Architecture Diagram

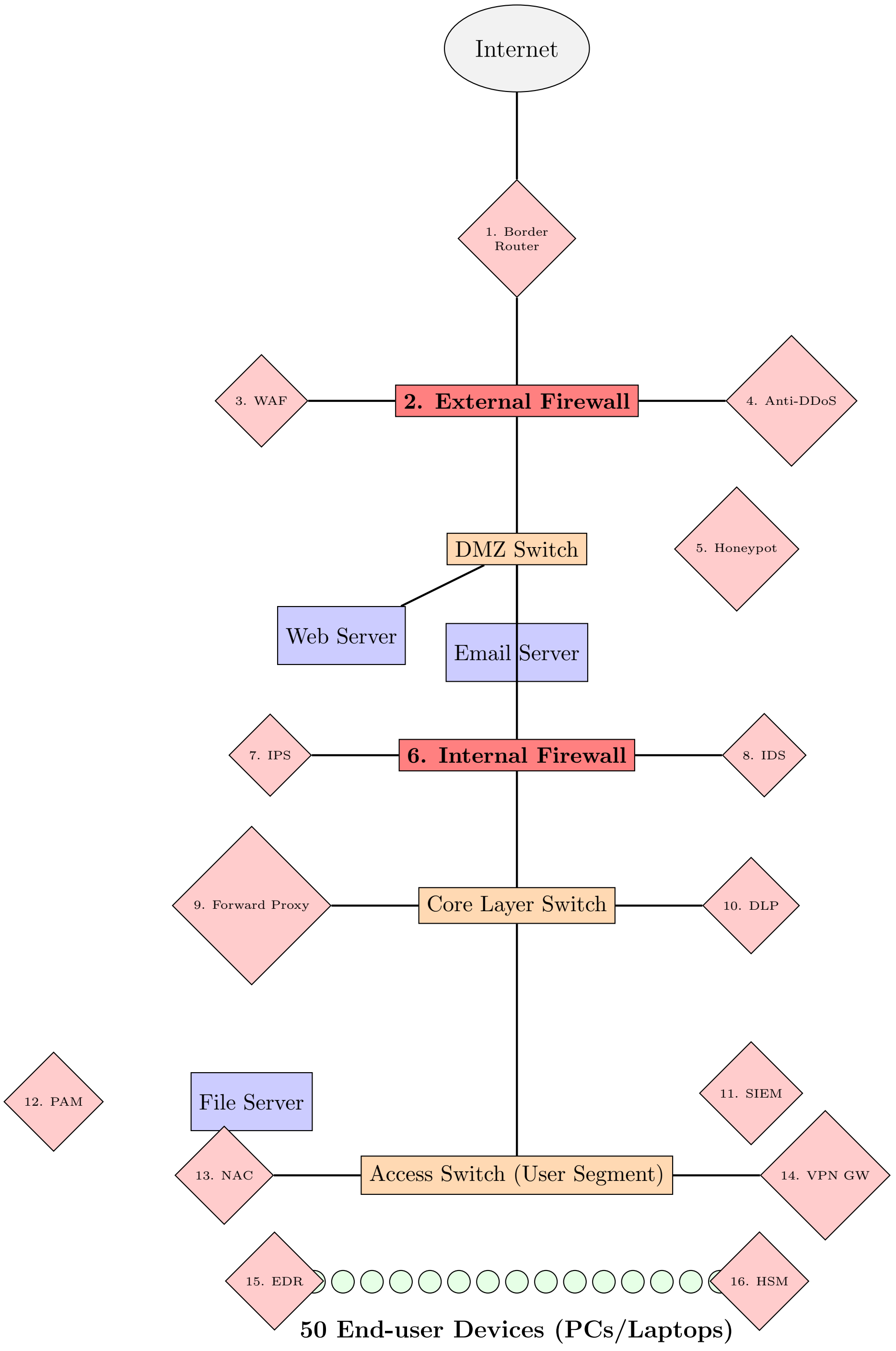

Figure 2.1: Proposed Logical Network Architecture with Layered Security

Chapter 3

Security Component Specifications

In this section, we define the 16 security components integrated into the architecture and their specific roles in protecting the 50 devices and 3 servers.

3.1 Detailed Device List

#	Security Device	Technical Function and Role
1	Border Router	The first point of contact with the ISP. It handles basic ACLs and routing protocols (BGP/OSPF).
2	External Firewall (NGFW)	Performs Deep Packet Inspection (DPI) and filters traffic based on application-level rules.
3	WAF (Web App Firewall)	Specifically protects the **Web Server** from SQL Injection, XSS, and CSRF attacks.
4	Anti-DDoS Appliance	Mitigates volumetric attacks (UDP/ICMP Floods) before they saturate the bandwidth.
5	Honeypot	A decoy system placed in the DMZ to lure attackers and study their techniques without risking real data.
6	Internal Firewall	Segregates the DMZ from the internal trusted LAN. If the DMZ is breached, this is the next line of defense.
7	IPS (Prevention System)	Actively drops packets that match known attack signatures or anomalous patterns.
8	IDS (Detection System)	Monitors network traffic for suspicious activity and alerts the SOC team for investigation.
9	Forward Proxy	Intercepts internal user requests to the internet for caching, URL filtering, and anonymity.
10	DLP (Data Loss Prevention)	Inspects outgoing traffic to ensure sensitive data (like company files) is not leaked.
11	SIEM	Collects and correlates logs from all 50 devices and all servers for real-time monitoring.

#	Security Device	Technical Function and Role
12	PAM (Privileged Access)	Manages and audits high-level access to the **File Server** and core switches.
13	NAC (Network Access Control)	Ensures only compliant and authorized devices (the 50 PCs) can connect to the access switch.
14	VPN Gateway	Provides secure, encrypted tunnels for remote employees to access the internal network.
15	EDR (Endpoint Detection)	Installed on each of the **50 devices** to detect and respond to advanced persistent threats.
16	HSM (Hardware Security Module)	A physical device that manages digital keys for the **Email Server's** encryption (S/MIME).

Chapter 4

Server Infrastructure Analysis

The network hosts three critical servers. Each has a specific security profile based on its location and usage.

4.1 Web Server

Located in the DMZ. It is protected by the WAF and External Firewall. It handles public traffic. No direct connection is allowed from the Web Server to the internal File Server.

4.2 Email Server

Handles SMTP/IMAP traffic. It is filtered by an Email Security Gateway (often integrated into the Firewall or as a separate appliance) to block phishing and spam.

4.3 File Server

The most sensitive asset. Located in the deepest layer of the internal network. Protected by the Internal Firewall, DLP, and PAM. Only the 50 authorized internal devices can access this server via authenticated sessions.

Chapter 5

Endpoint Management (50 Devices)

The network is designed to support 50 end-user devices. These devices are connected via Access Layer switches.

5.1 Security Policy for Endpoints

Each of the 50 devices must undergo:

0. **Identity Verification:** Through the NAC system.

0. **Posture Assessment:** Checking if the OS is updated and antivirus is active.

0. **Traffic Monitoring:** Via the IDS/IPS located at the core.

0. **Log Harvesting:** Sent to the SIEM for 24/7 analysis.

5.2 Traffic Flow Logic

When an internal user (one of the 50 PCs) requests a file from the **File Server**: 1. The request hits the Access Switch. 2. The NAC checks the device status. 3. The Core Switch routes the traffic. 4. The Internal Firewall verifies the user's permissions. 5. The PAM logs the administrative session if applicable.

Chapter 6

Technical Specifications and Configurations

6.1 Firewall Rule Sets

The External Firewall (Device #2) follows a ”Deny All” default policy.

- Rule 1: Allow TCP 80, 443 to Web Server.
- Rule 2: Allow SMTP to Email Server.
- Rule 3: Drop all fragmented packets.

6.2 IPS/IDS Signature Tuning

The IPS (Device #7) is configured with over 5000 signatures specifically targeting:

- Remote Code Execution (RCE).
- SQL Injection patterns.
- Brute force attempts on the 50 user machines.

6.3 WAF Policies

The WAF (Device #3) operates at Layer 7. It inspects:

- HTTP Headers.
- Cookies (to prevent session hijacking).
- POST request bodies for the Web Server.

6.4 DLP Sensitivity Levels

The DLP (Device #10) monitors for:

- Credit card number patterns.
- Social security numbers.
- Proprietary source code keywords from the File Server.

6.5 Honeypot Strategy

The Honeypot (Device #5) mimics a vulnerable Windows 10 machine among the 50 devices. It serves as an early warning system. If any internal device tries to communicate with the Honeypot, it indicates lateral movement of a virus.

6.6 SIEM Correlation Rules

The SIEM (Device #11) is the brain of the network. It correlates logs: *"If Firewall shows 10 failed logins AND IDS shows a port scan from the same IP, THEN trigger an Incident Response alert."*

6.7 PAM (Privileged Access Management)

Access to the File Server is strictly controlled. PAM provides "Just-In-Time" (JIT) access, meaning the 50 users don't have permanent admin rights; they request them only when needed.

6.8 NAC Implementation

NAC (Device #13) uses 802.1X authentication. If one of the 50 devices is brought from outside and is infected, the NAC will isolate it in a "Quarantine VLAN" until it is cleaned.

6.9 VPN Gateway Configuration

The VPN (Device #14) uses AES-256 encryption. It allows remote access to the Email and File servers through the external firewall using a dedicated tunnel.

6.10 HSM Integration

The HSM (Device #16) protects the private keys of the enterprise. This ensures that even if an attacker gains root access to the Email Server, they cannot decrypt the encrypted emails.

6.11 Proxy Server Benefits

The Proxy (Device #9) reduces bandwidth for the 50 devices by caching frequent web pages and provides a single exit point for better monitoring.

6.12 Endpoint Detection Response (EDR)

EDR (Device #15) is the last line of defense. Even if an attacker bypasses the 15 other devices, the EDR monitors memory and process execution on the 50 PCs to stop ransomware.

Chapter 7

Conclusion

This architecture provides a comprehensive security posture for a 50-device network. By integrating 16 distinct security technologies and isolating the Web, Email, and File servers into appropriate zones, we ensure that the network remains resilient against modern cyber threats. The design prioritizes visibility, control, and rapid response.

Appendix A

Glossary of Terms

- **DMZ:** Demilitarized Zone.
- **NGFW:** Next-Generation Firewall.
- **VLAN:** Virtual Local Area Network.
- **AES:** Advanced Encryption Standard.