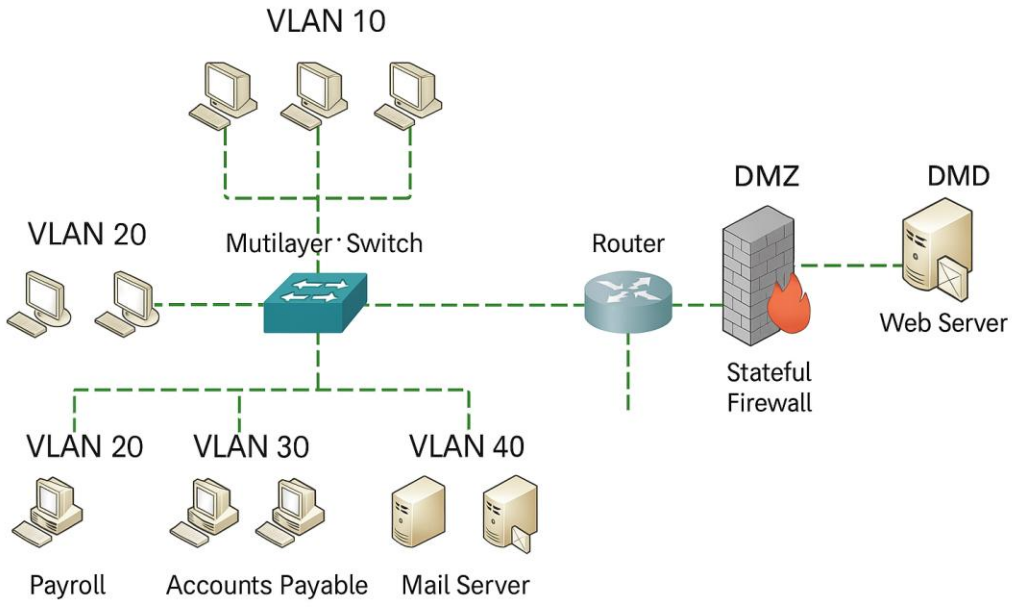
Secure Network Infrastructure Design
Azizul Rahaman
MSIN641 – Touro University
April 2025

1. Introduction

In today's cybersecurity landscape, creating a secure and resilient network infrastructure is critical for any organization. This design follows a defense-in-depth strategy---implementing multiple security layers to ensure that if one control fails, others remain to protect internal assets. The design supports four departments and accounts for both internal protections and required external access.

2. Network Overview and Department Requirements



Network Topology Diagram

Clarification: The diagram has been updated to show dual firewall protection for the DMZ (or a single firewall with separate DMZ interfaces), ensuring proper traffic inspection between Internet, DMZ, and internal networks.

The network is designed to support the following departments:

- Payroll (6 computers)
- Research and Development (10 computers)
- IT (5 computers)
- Accounts Payable (10 computers)

Each department will be assigned its own VLAN to segment traffic, enhance security, and reduce broadcast domains. A multilayer switch will route traffic between VLANs, while a central router and firewall manage Internet access.

3. IP Addressing and VLAN Segmentation

Departments are assigned private IPv4 subnets and internal IPv6 ULAs:

- VLAN 10: Payroll -- 192.168.10.0/29
- VLAN 20: R&D -- 192.168.20.0/28
- VLAN 30: IT -- 192.168.30.0/29
- VLAN 40: Accounts Payable -- 192.168.40.0/28

IPv6 addresses follow a unique local address format (fd00::/8). Devices communicate internally over private IPs, and use NAT or a global IPv6 address for external access.

4. Name Resolution (DNS)

A split-horizon DNS setup will be used. Internal DNS servers handle local name resolution mapped to Active Directory (AD) for centralized authentication and resource management. An external DNS service manages public-facing records (e.g., mail.company.com, www.company.com). DNSSEC will be enabled to protect data integrity.

5. Network Address Translation (NAT)

Implementation: The perimeter firewall handles all NAT operations:

- Port Address Translation (PAT) for internal users sharing the single public IPv4 address
- Static NAT mappings for DMZ servers (web/email)
- IPv6 uses global addressing without NAT

6. Firewall Configuration and Security

A stateful perimeter firewall with DMZ interfaces enforces the following rules:

- Allow outbound traffic for HTTP/HTTPS, SMTP, IMAP, and DNS
- Allow inbound HTTPS (port 443) to web servers only
- Allow inbound SMTP (port 25) to email server only
- Block all other inbound traffic
- **DMZ Protection:** Separate firewall policies inspect traffic between:
  - Internet ↔ DMZ
  - DMZ ↔ Internal network
- Restrict access between VLANs with ACLs
- Enable logging, intrusion detection, and alerting for suspicious traffic

7. Web, Email, and VPN Security

Public-facing servers (Web, Mail) are hosted in a DMZ (Demilitarized Zone). They are:

- Hardened and regularly patched
- Protected by a Web Application Firewall (WAF) and TLS encryption
- Only required ports (443, 25) are open to the Internet

Email security includes SPF, DKIM, DMARC, and spam filtering. A VPN service allows IT staff secure remote access using multi-factor authentication (MFA) and encryption.

8. Internal Controls and Defense-in-Depth

Security policies enforced internally include:

- Strong password policies with forced expiration

- MFA for privileged access
- Antivirus and endpoint protection for all hosts
- VLAN segmentation to limit lateral movement
- Regular vulnerability scanning and backups
- Physical security and access control to core devices

9. Conclusion

This network design provides strong, layered protection for both internal and external communication. It supports departmental separation, efficient IP usage, secure web/email access, and proactive defense strategies. By combining NAT, DNS, VLANs, firewalls, and internal policies, the organization ensures secure, reliable infrastructure aligned with cybersecurity best practices.