slide 1

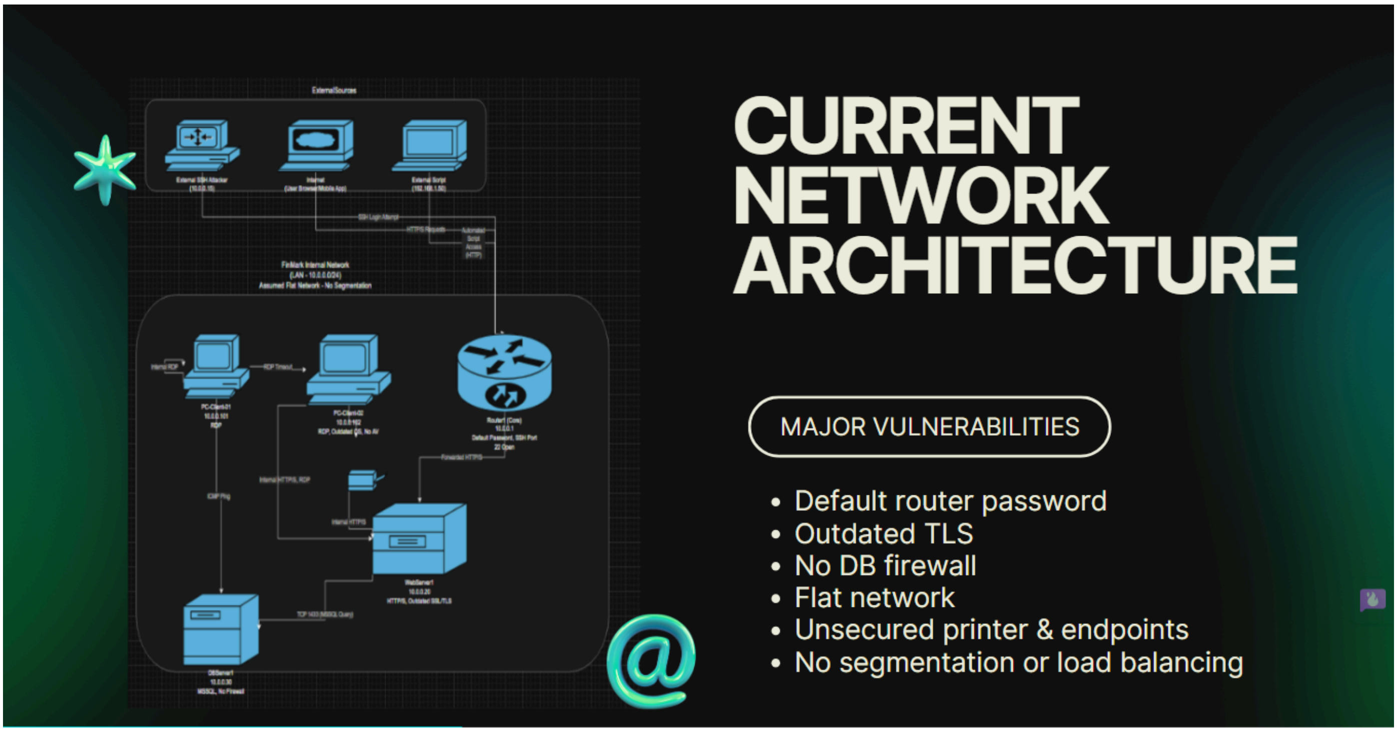
BUILDING A SECURE, RESILIENT NETWORK

PLATFORM TECHNOLOGIES

H3101 - NETWORK AND CYBERSECURITY 1 (CSN11)

MAY 2025

slide 2

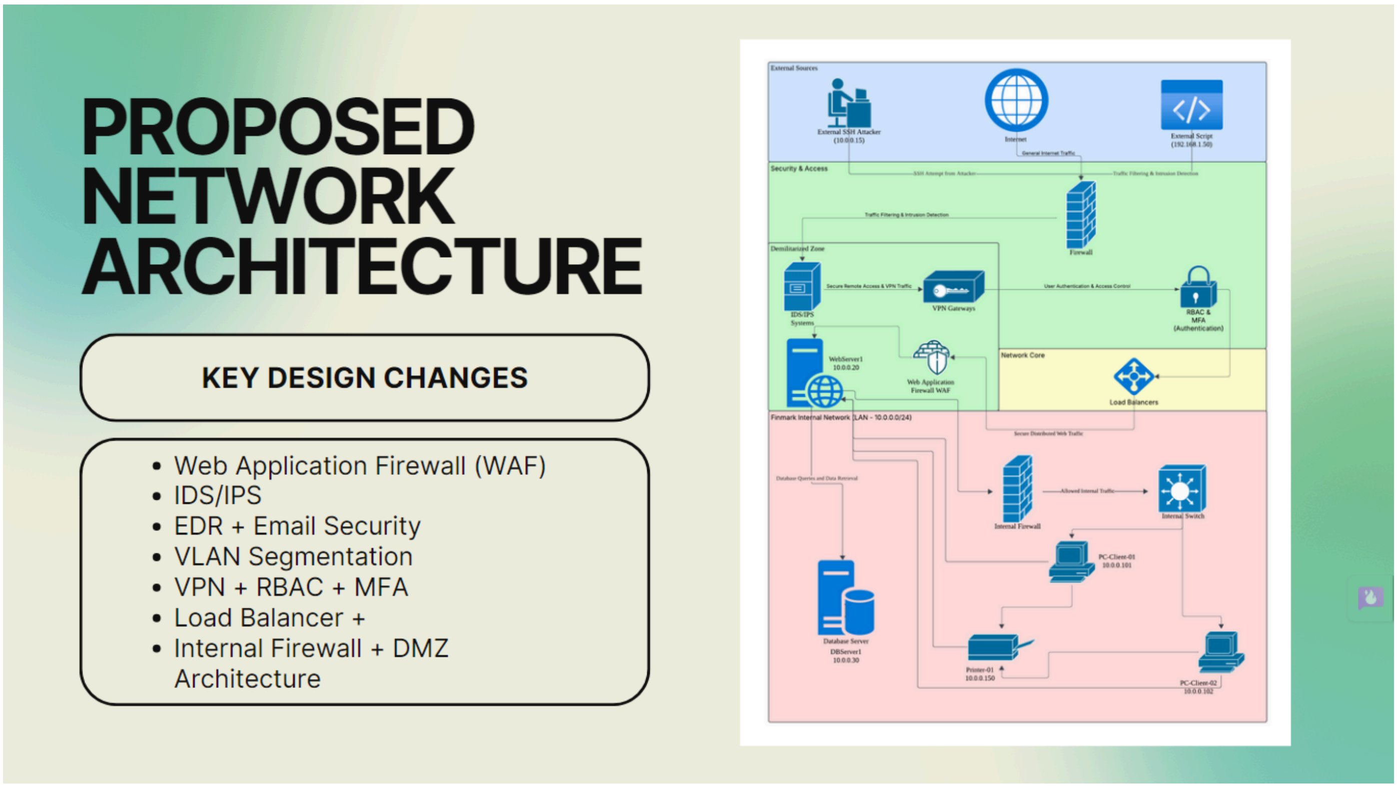


CURRENT NETWORK ARCHITECTURE

MAJOR VULNERABILITIES

- Default router password
- Outdated TLS
- No DB firewall
- Flat network
- Unsecured printer & endpoints
- No segmentation or load balancing

slide 3

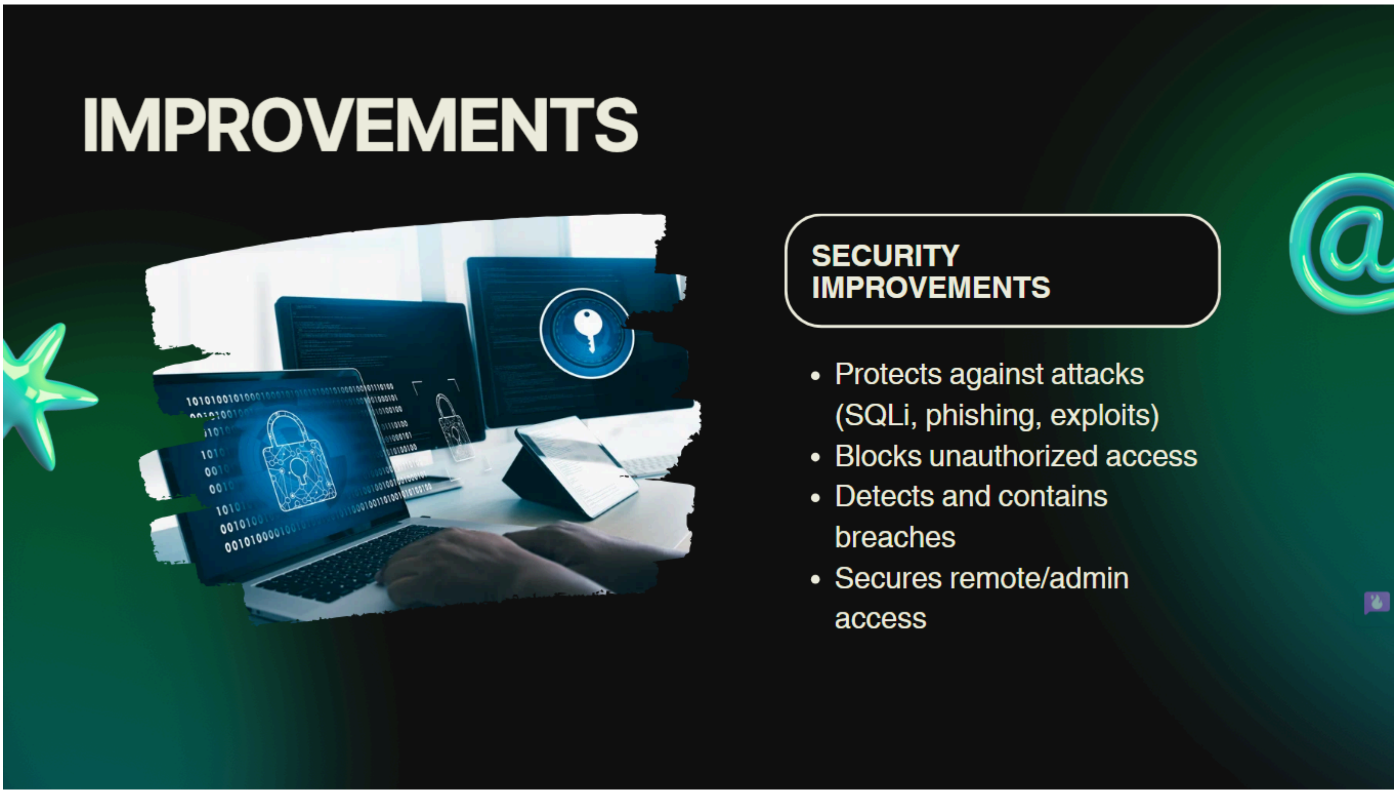


PROPOSED NETWORK ARCHITECTURE

KEY DESIGN CHANGES

- Web Application Firewall (WAF)
- IDS/IPS
- EDR + Email Security
- VLAN Segmentation
- VPN + RBAC + MFA
- Load Balancer +
- Internal Firewall + DMZ Architecture

slide 4

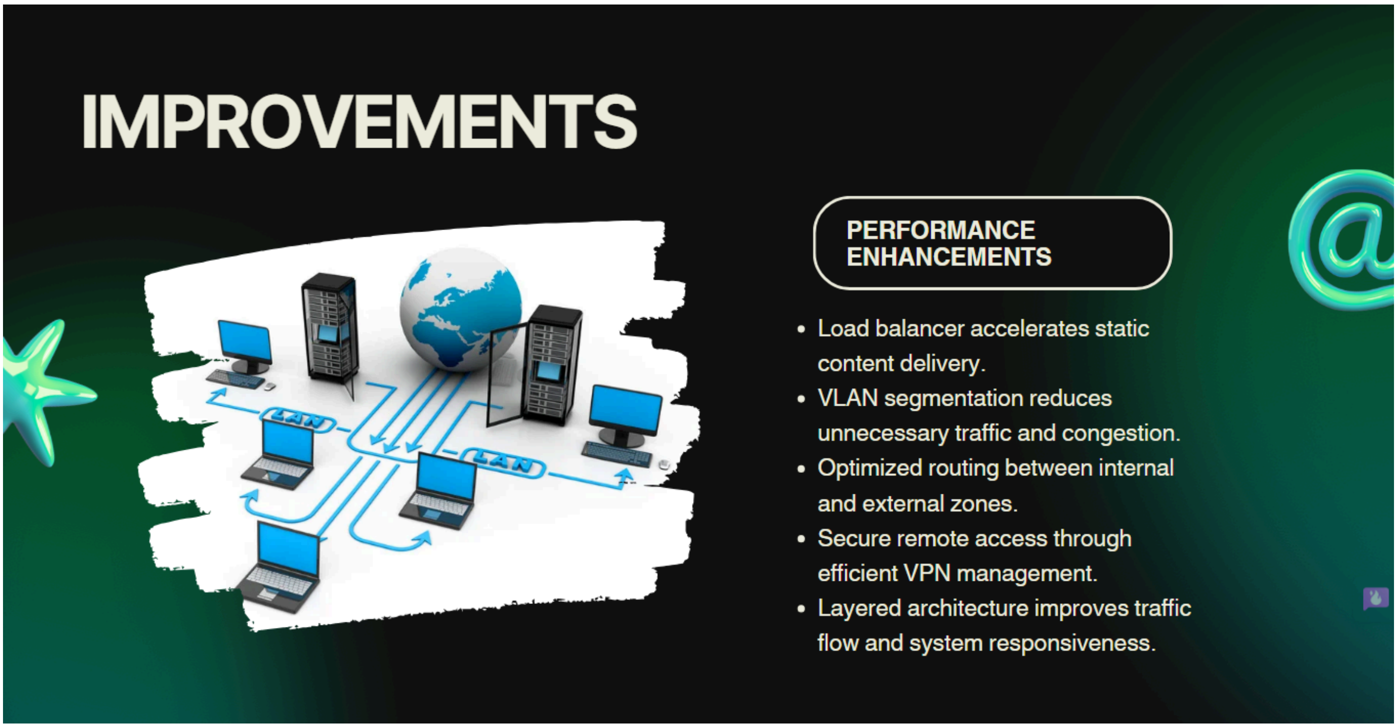


IMPROVEMENTS

SECURITY IMPROVEMENTS

- Protects against attacks (SQLi, phishing, exploits)
- Blocks unauthorized access
- Detects and contains breaches
- Secures remote/admin access

slide 5



IMPROVEMENTS

PERFORMANCE ENHANCEMENTS

- Load balancer accelerates static content delivery.
- VLAN segmentation reduces unnecessary traffic and congestion.
- Optimized routing between internal and external zones.
- Secure remote access through efficient VPN management.
- Layered architecture improves traffic flow and system responsiveness.

slide 6

IMPROVEMENTS

RELIABILITY UPGRADES

- Prevents lateral movement through VLAN segmentation
- Segmentation isolates faults
- Continuous threat monitoring and faster incident response
- EDR enables rapid containment and recovery
- Email filtering reduces malware-related disruptions
- Layered security increases system fault tolerance
- Separate traffic zones improve service stability