Report 2 – Secure Hybrid Access Model

Prepared for: Cisco Networking Academy – Virtual Internship Program 2025

Prepared by: Kasmya Bhatia (23FE10CAI00010)

Date: August 2025

Objective: To design a secure, scalable, and role-based hybrid network architecture that enables faculty to work remotely or on campus with uninterrupted access to teaching and research tools, ensures students can connect to academic portals from personal devices, and keeps internal services isolated from direct internet exposure.

Network Segmentation by User Role

- Faculty Zone (VLAN 10): Full access to research repositories, teaching platforms, and relevant internal applications.
- Student Zone (VLAN 20): Limited access to academic portals, labs, and general internet browsing.
- Server Center: Restricted zone containing sensitive resources; only accessible to authorized segments through secure gateways.
- Guest Zone: Fully isolated network for visitors, allowing internet access only.

Secure Access Tools and Components

- VPN Gateway:
    - Hosts secure, encrypted tunnels for remote faculty/staff.
    - Integrated with RADIUS or Active Directory for identity verification.
    - All traffic from remote faculty routed through campus firewall (split tunneling disabled).
- Identity-Aware Proxies:
    - Gate access to apps and resources based on user identity, device compliance, and assigned role.
- Firewalls & ACLs:
    - Enforce strict traffic control between VLANs and block unauthorized cross-zone access.
- Network Segmentation:
    - Logical separation between faculty, student, guest, and server zones to limit breach impact.

Authentication Flow

1. Faculty Remote Access:
    - VPN client → VPN gateway → Role verification via RADIUS/Active Directory → Role-based access policy assigned → Access to faculty VLAN and approved internal services.
2. Student On-Campus Access:
    - Wi-Fi/Ethernet connection → Captive portal or 802.1X authentication → VLAN assignment with access limited to academic and lab resources.

Risks & Mitigation

- VPN Credential Theft: Implement MFA and monitor for suspicious logins.
- Bandwidth Congestion: Apply QoS to prioritize academic traffic over recreational use.
- VPN Gateway as Single Point of Failure: Deploy redundant VPN gateways with failover.
- Compromised Student Devices: Restrict inter-VLAN communication and enforce endpoint security policies.
- Configuration Drift: Schedule regular firewall and VPN audits with documented changes.

Use Cases

- Faculty Member at Home: Securely connects via VPN to research databases and teaching resources in the Server Center.
- Student Using Library Wi-Fi: Authenticated access to online academic resources through the student VLAN.

Fallback Strategies

- Maintain backup VPN gateways to ensure continued service during outages.
- Use anomaly detection tools (IDS/IPS) to identify and respond to suspicious activity.

Deliverables

- Updated Network Topology Diagram: Showing VLAN segmentation, VPN gateway, identity-aware proxy placement, firewall configuration, and policy enforcement points.
- Technical Documentation: Detailed explanation of chosen tools, architecture, authentication flows, risks, and mitigations.

Conclusion

The secure hybrid network design delivers strong protection for internal services while supporting flexible academic operations. By integrating VPN access with MFA, identity-aware proxies, strict VLAN segmentation, and proactive risk management, the college achieves a balance between accessibility, performance, and security.