Phase-3

*Project: Cyber Shield Internship – Secure Remote Access Architectu*re

Submitted by: KSHITIJ PAWAR

Date: August 2025

Tools Used: Cisco Packet Tracer, Markdown, GitHub, VPN Gateway (simulated), GRE Tunnel, youtube

📍 Objective

Design and implement a hybrid access architecture that enables secure connectivity for both on-campus and remote users. This phase introduces VLAN segmentation, VPN simulation, split tunneling, and fallback strategies to ensure continuous access and layered security.

✅ Step 1: Segment Users & Define Trust Zones

🔧 VLAN Configuration

VLAN Name	VLAN ID	Purpose
Students	10	Semi-trusted internal users
Faculty	20	Trusted internal users
Guests	30	Untrusted external users
Remote	60	Off-campus VPN users

Configured using:

```
Switch(config)# vlan 10

Switch(config-vlan)# name Students

...

Switch(config)# vlan 60

Switch(config-vlan)# name Remote
```

🔐 Trust Zones

Zone Name	Description
Internal	On-campus wired users (VLANs 10, 20)
External	Internet-facing services (DMZ, Web Server)
Remote	Off-campus users accessing via VPN (VLAN 60)

✅ Step 2: Add Remote Access Tools

□ VPN Gateway Simulation

- Added Router-PT labeled “VPN-Gateway”
- Connected to Core Switch via Ethernet
- Configured GRE Tunnel to simulate encrypted remote access

```
Router(config)# interface tunnel0
Router(config-if)# ip address 192.168.100.1 255.255.255.0
Router(config-if)# tunnel source fa0/0
Router(config-if)# tunnel destination 192.168.100.2
```

□□

Remote endpoint:

```
Router(config)# interface tunnel0
Router(config-if)# ip address 192.168.100.2 255.255.255.0
Router(config-if)# tunnel source fa0/0
Router(config-if)# tunnel destination 192.168.100.1
```

□□

🔀 Split Tunneling Logic

- Internal traffic routed via tunnel

- Internet traffic routed via default gateway

```
Router(config)# ip route 10.0.0.0 255.0.0.0 tunnel0

Router(config)# ip route 0.0.0.0 0.0.0.0 fa0/0
```

✅ Step 3: Document Architecture & Authentication Flow

🗺 Updated Topology Diagram

(Include your Packet Tracer diagram showing VPN-Gateway, VLAN 60, tunnel paths, and trust zones)

🔐 Authentication Flow

Remote User → VPN Login Portal → Credential Verification → Tunnel Established → Access Granted to Internal VLANs

⍰⍰

□ Identity-Aware Proxy & SASE Mention

- Documented SASE (Secure Access Service Edge) as a future upgrade

- Explained identity-aware proxy:

- Access decisions based on user identity, device posture, and location

- Ideal for cloud-based apps and zero-trust enforcement

⚠ Risks & Fallback Strategies

Risk Scenario	Impact	Fallback Strategy
VPN Gateway Failure	Remote users lose access	Allow access to DMZ web portal via public IP
Identity Proxy Misconfiguragion	Users denied access	Revert to ACL-based access control
Split Tunnel Leak	Data exposure risk	Enforce DNS filtering and endpoint firewall

Example ACL for fallback:

```
Router(config)# access-list 110 permit tcp any host [DMZ_Web_IP] eq 80

Router(config)# access-list 110 deny ip any any

Router(config)# interface fa0/1

Router(config-if)# ip access-group 110 in
```

⍰⍰

📌 Summary

The hybrid access design successfully integrates remote connectivity with strong segmentation and fallback controls. VPN simulation and split tunneling provide flexibility, while the architecture remains scalable for future SASE and identity-aware upgrade

Phase-4

Internship: AICTE–Cisco Virtual Internship 2025

Submitted by: KSHITIJ PAWAR

Focus: Network Access Control, Content Filtering, ACL Simulation

Tools: Cisco Packet Tracer, ACLs, Conceptual DNS/Proxy/Firewall Models

🎯 ***Objective***

Implement and document web filtering policies across user zones (Student, Faculty, Guest) to enforce acceptable use, enhance security, and maintain productivity. This phase includes tool comparison, policy design, ACL-based simulation, and a formal policy document with enforcement logic and alerting strategy.

✅ Step 1: Compare Filtering Tools

Category	Tools Used	Functionality Summary
DNS Filtering	OpenDNS, Quad9	Blocks access to malicious or restricted domains via DNS resolution
Layer 7 Firewall	Palo Alto, FortiGate	Inspects application-level traffic, enforces granular policies
Proxy Filtering	Squid, Zscaler	Intercepts and filters web traffic (HTTP/HTTPS)
Client-Side Control	Windows Group Policy, browser extensions	Enforces restrictions directly on user devices

🔍 Note: In Packet Tracer, DNS and Layer 7 filtering are simulated using ACLs and annotations.

✅ Step 2: Design Access Policies

👩🎓 Students

- ⛔ Block social media during class hours (9am–5pm)

- ✅ Allow educational sites anytime

👨‍🏫 Faculty

- ✅ Full access to research tools
- ⊖ Block entertainment sites during work hours

🧑‍💼 Guests

- ✅ Internet access only
- ⊖ No access to internal VLANs or servers

✅ Step 3: Simulate Enforcement in Packet Tracer

🔧 ACL Configuration Examples

🔹 Block HTTP (Port 80) for Students During Class Hours

```
Router(config)# time-range CLASS_HOURS
Router(config-time-range)# periodic weekdays 9:00 to 17:00

Router(config)# access-list 110 deny tcp any any eq 80 time-range CLASS_HOURS
Router(config)# access-list 110 permit ip any any

Router(config)# interface fa0/1
Router(config-if)# ip access-group 110 in
```

□□

🔹 Block Guest Access to Internal VLANs

```
Router(config)# access-list 120 deny ip 192.168.30.0 0.0.0.255 10.0.0.0 0.255.255.255
Router(config)# access-list 120 permit ip any any

Router(config)# interface fa0/3
Router(config-if)# ip access-group 120 in
```

⍰⍰

🖼 Topology Annotations

- Label router interfaces with zone names (e.g., STUDENT_VLAN, GUEST_VLAN)

- Add notes: “Simulated Proxy”, “DNS Filter Concept”, “ACL Applied Here”

- Use color-coded lines to show filtered vs unrestricted paths

✅ Step 4: Policy Document

📜 Policy Rules (Natural Language & Pseudo-Code)

```
IF user = Student AND time = 9am–5pm THEN block social_media_sites

IF user = Faculty AND time = 9am–5pm THEN block entertainment_sites

IF user = Guest THEN allow internet_only AND deny internal_access
```

🔐 Enforcement Logic

- ACLs applied per VLAN interface

- Time-based ACLs simulate scheduled restrictions

- Proxy and DNS filtering represented via annotations

- VLAN segmentation ensures zone isolation

📢 Logging & Alerting Plan

Event Type	Logging Method	Alert Mechanism
Blocked Access Attempt	Syslog (router logs)	Email alert to admin (conceptual)
ACL Match	Packet Tracer CLI	Manual log review
Policy Violation	Simulated via notes	Future upgrade: SNMP trap or SIEM integration

▯ ***Summary***

This phase demonstrates how filtering policies can be tailored to user roles and enforced using ACLs in a simulated environment. While Packet Tracer lacks full DNS or Layer 7 capabilities, annotations and ACL logic effectively convey the design. The documented policy and alerting plan provide a strong foundation for real-world deployment using enterprise-grade tools.