**Campus Network Security Assessment & Attack Surface Report**

**Cisco Packet Tracer Topology Review | Internal Red Team Perspective** Date: 18 Aug 2025 10:00 P.M

**Problem Statement**: You are a part of the cybersecurity student team at your college, freshly enrolled in the Cisco Neta cad Cybersecurity course. With access to Cisco Packet Tracer and your growing knowledge of security fundamentals, you've been given your first real-world challenge.

Your task is to analyse your own college network as if you were part of an internal red team. Begin by mapping the current infrastructure using Cisco Packet Tracer, identifying devices, access points, firewalls, segmentation boundaries, and any existing security controls.

Assess how effective these controls are in today’s threat landscape. Where are the weak points? Are there flat zones that allow lateral movement? What would an attacker target first, and how would you stop them?

Assume budgets are tight and staff are limited. Using the knowledge from your Neta cad course and insights gained through simulation, conduct an attack surface analysis and present findings with risk-based recommendations.

**A diagram of a computer network

AI-generated content may be incorrect.Figure 1: Existing Campus Topology (Packet Tracer)**

**1. Identified Trust Zones in Topology**

Based on the existing topology , typical trust zones and segments:

* Campus Blocks (**BLOCK\_A / BLOCK\_B / BLOCK\_C / BLOCK\_D / BLOCK\_E / LIBRARY / DIGLIBRARY):**  
  Internal user zones with moderate trust, intended for students, staff, or device endpoints separated by VLANs**.**
* **Server Zone:**  
  Hosts EMAIL, DNS, and WEB servers, likely more trusted/internal and possibly more restricted.
* **Network Core/Router Zone:**  
  Routers and switches forming the backbone between blocks – assumed trusted if physically secure.
* **Internet/External Zone:**  
  Least trusted; traffic from outside the campus network passes through the ASA firewall.

**2. Documented Security Controls**

**Physical & Logical Controls:**

* Firewalls:

ASA (ASAO) is present, presumably at the network perimeter (between core routers and outside/internet). Likely enforces inbound/outbound rules.

* Authentication Servers:

EMAIL/WEB may use LDAP/Active Directory or local authentication for users, advised to centralize for robust access control.

* VLAN Segmentation:

Blocks separated at Layer2; traffic between VLANs needs Layer3 routing (on routers), helps compartmentalize risks.

* Access Control Lists (ACLs):

Can be applied on routers/ASA to restrict inter-VLAN and inbound/outbound traffic.

**3. Recommended Controls to Add/Verify:**

* **IDS/IPS:**

No visible IDS/IPS from topology, but recommended to detect attacks and policy breaches in real time.

* **ASA/Firewall Zone:**Demilitarized zone (DMZ) and/or boundary protection – highest security control enforcing rules between zones.
* **Endpoint Security:**

Antivirus, host firewall, regular patching for labs, library, and administrative machines.

* **Strong Authentication:**

Multi-factor authentication (MFA) for admin resources, sensitive apps, remote access.

**4.  Attack Surface Mapping :** **ToolsNmap (host discovery), Wireshark (validation)**

* User Endpoints (PCs, Laptops, Tablets, Smartphones):  
  Phishing, malware, credential theft risks.
* Access Points:  
  Potential wireless attack vector – ensure WPA2/WPA3 and strong passwords.
* Inter-VLAN Routing:  
  Unauthorized lateral movement if router ACLs are insufficient.
* Servers (EMAIL, DNS, WEB):  
  Web/mail exploits, credential stuffing, DDoS, exposed services.
* Core Routers/Switches:  
  Misconfiguration, default passwords, SNMP/management exposure.
* ASA Firewall:  
  Single point of perimeter policy – must be correctly configured, patched, monitored.
* Internet Link:  
  DDoS, brute force, SQLi, web vulnerabilities - direct exposure.

**5. Improved Topology with Enhanced Security: (Figure 2)**

**A diagram of a computer network

AI-generated content may be incorrect.**

**6.Observation and Recommendation:**

| **Zone** | **Controls Present** | **Recommended Controls** | **Key Risks** | **Mitigation Suggestions** |
| --- | --- | --- | --- | --- |
| **Campus VLANs** | **VLAN, router** | **Endpoint security, ACLs** | **Malware, lateral movement** | **Harden ACLs, user endpoint security** |
| **Server Zone** | **Dedicated VLAN** | **Auth, SIEM, IDS/IPS** | **Data theft, web/email exploits** | **MFA, monitoring, least privilege** |
| **Network Core** | **Physical/logical** | **SNMPv3, mgmt. port lockdown** | **Config, privilege escalation** | **Secure mgmt., restrict SNMP** |
| **ASA/Firewall** | **Firewall** | **IDS/IPS, SIEM, patching** | **Misconfigure, policy gaps** | **Regular review/audit, rule tightening** |
| **Internet Zone** | **Outbound through ASA** | **DDoS, WAF, strong ACLs** | **All external threats** | **DDoS defences, limit inbound exposure** |

**7. CONCLUSION:**

The current campus network provides a strong foundation but suffers from flat zones, limited visibility, and insufficient segmentation. By adopting the above recommendations—particularly improved ACLs, IDS/IPS deployment, and network segmentation—the attack surface can be significantly reduced while staying within budget and resource constraints.

**Hybrid Secure Access Network Design for College Campus**

**PART 2:**

**Problem Statement**: After your impressive audit in Part 1, the college IT department has invited you to contribute to a new project: enabling a hybrid access model for students and faculty. Faculty members will now work flexibly from home or campus, and require uninterrupted, secure access to teaching tools, research repositories, and internal services. Students, on the other hand, will continue using personal devices to access shared academic portals and lab resources. But here’s the catch: the administration has made it clear that the internal services must never be exposed directly to the internet. Your task is to design a secure hybrid network architecture that supports remote access while enforcing strict boundaries. Think like a network engineer and evaluate options like VPN, SASE, identity-aware proxies, or split tunneling. Consider not only how to connect, but how to ensure the right people access the right services at the right time. Can your design balance simplicity, security, and scale without overwhelming the existing infrastructure?

Following a comprehensive security audit, the college has embarked on enhancing its network to support a **hybrid access model** that accommodates both on-campus and remote users. Faculty members require secure, uninterrupted remote access to internal teaching and research resources, while students continue accessing academic portals and lab resources from campus devices. The core design priority is to prevent direct exposure of internal services to the internet, ensuring consistent security boundaries.

**2. Network Segmentation and User Roles**

The network is segmented based on user roles to maintain strong security boundaries:

* **Faculty VLAN:** Dedicated on-campus segment for faculty with unrestricted access.
* **Student VLANs:** Segmented VLANs per academic block with limited resource access.
* **Admin VLAN:** Restricted segment for administrative management services.
* **DMZ:** Isolated subnet hosting shared services such as mail, web, and DNS servers.

**Remote access segmentation distinguishes:**

* **Faculty and Admin remote users** connecting securely via VPN.
* **Students** limited to on-campus access with no direct internet access to internal services.

**3. Secure Access Tools and Architecture**

**VPN Gateway**

A campus perimeter VPN gateway terminates faculty and admin remote sessions securely using SSL VPN. This provides encrypted tunnels ensuring confidentiality and integrity of data in transit.

**Identity-Aware Proxy**

An identity-aware access proxy verifies user credentials and enforcement of role-based access controls before granting access to specific internal applications. This enables granular access control, multi-factor authentication (MFA), and session visibility.

**Split Tunneling**

For remote faculty and admins, split tunneling allows traffic destined to campus resources to route via VPN while internet-bound traffic flows directly to local ISPs, optimizing performance and reducing campus bandwidth load.

**Optional SASE Adoption**

Cloud-delivered Secure Access Service Edge (SASE) architectures can be integrated for scalable policy enforcement, advanced threat protection, and seamless cloud resource access in future phases.

**4. Trust Model and Authentication Flow**

* **Users authenticate** locally via Active Directory integrated with VPN gateway and identity proxy.
* **Faculty and Admins** require strong authentication with MFA, gaining access aligned with their role’s permissions.
* **Students** authenticate with campus credentials but are confined within student VLANs and limited application scope.
* **Management access** is restricted to the admin VLAN with additional security and auditing.

Access flows are designed such that:  
Remote user → VPN Gateway → Identity Proxy → Campus VLAN/DMZ Services

**5. Updated Network Topology Overview**

The updated network includes:

* **VPN Gateway** at perimeter for remote connections.
* **Identity Proxy** between perimeter firewall and campus core enforcing access policies.
* **Segmentation** of faculty, student, admin VLANs.
* **DMZ zone** for critical servers insulated behind an internal firewall.
* **Clear pathway for remote access** ensuring users traverse policy enforcement zones.

**6. Risk Analysis and Mitigation**

| **Risk** | **Mitigation** |
| --- | --- |
| Exposure of internal services to internet | VPN termination, no direct internet routing to internal VLANs |
| Unauthorized access | Strong authentication, MFA, role-based access |
| Credential theft and session hijacking | Encrypted tunnels, identity-aware proxy session monitoring |
| Lateral movement by compromised devices | VLAN segmentation, ACLs restricting inter-VLAN traffic |
| Bandwidth and latency issues | Split tunneling for internet bound traffic |
| Administrative account compromise | Restricted admin VLAN and logging |

Fallback strategies include:

* Proxy access as an alternative if VPN is unavailable.
* Local admin accounts with controlled physical access.
* Incident response plans and segmentation to limit breach impact.

**7. Advantages of Proposed Architecture**

* **Security:** Strong boundaries, robust authentication, and multi-layer Defense.
* **Scalability:** Easily expanded by adding VLANs, proxy policies, and additional VPN users.
* **User Experience:** Seamless connectivity for faculty and admins, controlled but straightforward access for students.
* **Performance:** Split tunnelling balances latency and campus load demands.
* **Compliance:** Meets modern best practices for educational network security.

**8. Conclusion**

This hybrid access solution balances simplicity, security, and flexibility. It supports evolving campus demands without exposing internal resources to undue risk, ensuring faculty and administrative productivity while preserving student access within controlled limits. Future enhancements, including cloud-based SASE integration, can be evaluated for extended scalability and threat responsiveness.

**Web Access Policy Framework for College Campus: Managing Hybrid User Behaviour**

**PART 3:**

**Problem Statement:** Soon after the hybrid model rolls out, complaints start coming in: students are streaming videos during lectures, torrenting files in labs, and bypassing basic restrictions using browser extensions and proxies. The administration turns to you again, and this time for a solution that restricts web access smartly, without creating backlash or blocking legitimate research. You must design a policy framework that considers:

● Who the user is (student, faculty, guest)

● When they’re online (class hours, weekends)

● What content they’re trying to access (education, social media, games, etc.)

Explore modern filtering tools: DNS-based filtering, L7 firewalls, proxies, and endpoint-based enforcement. Draft simple, understandable rules, but back them with solid policy logic and enforcement mechanisms. Don’t just stop at blocking sites but instead log events, anticipate circumvention attempts, and define how violations should be reported.

**1. Comparison of Filtering Solutions**

| **Filtering Solution** | **Description** | **Pros** | **Cons** | **Suitability** |
| --- | --- | --- | --- | --- |
| **DNS-based Filtering** | Blocks access to domains at DNS resolution level | Easy to deploy, lightweight, broad coverage | Limited granularity, bypassable by custom DNS | Good baseline, quick blocking |
| **Layer 7 (Application) Firewall** | Inspects traffic for application type and URL | Precise control over traffic, supports protocols beyond HTTP/S | Requires powerful hardware, complex to configure | Ideal for fine granular control |
| **Proxy-based Filtering** | All user HTTP/S traffic routed via proxy | Enforces user/group policies, logging, URL categorization | Requires user device config or inline proxy, may add latency | Strong control, best logging |
| **Client-side Enforcement** | Software installed on endpoints to monitor/control | Device-specific control, offline enforcement | Management complexity, user resistance | Useful complement, especially for laptops |

**2. Policy Design Principles**

**User Groups**

* **Students:** Restricted access during class hours; moderate restrictions after hours.
* **Faculty:** Generally unrestricted but monitored.
* **Guests:** Highly restricted, limited to basic internet.

**Time-based Access**

* **Class Hours (e.g., 8 AM - 5 PM weekdays):** Strong restrictions against streaming, gaming, torrents.
* **Off Hours (evenings/weekends):** Relaxed to allow more access to entertainment; still blocked for malicious or illegal sites.

**Content Categories**

| **Category** | **Students** | **Faculty** | **Guests** |
| --- | --- | --- | --- |
| Educational | Allowed | Allowed | Allowed |
| Social Media | Block during class, limited off-hours | Allowed | Limited |
| Streaming Video | Block during class, limited off-hours | Allowed | Blocked |
| Gaming | Blocked | Allowed | Blocked |
| Torrent/Fileshare | Blocked | Blocked | Blocked |
| Proxy/VPN | Blocked | Allowed | Blocked |

**3. Enforcement Architecture and Components**

* **Next-Generation Firewall (NGFW) or Layer 7 Firewall:** Positioned at perimeter to inspect, categorize, and control web traffic based on user identity and time rules.
* **DNS Filtering Service:** Cloud-based DNS filtering to block known malicious or unwanted domains.
* **Proxy Server (Optional):** Authenticating users with explicit access policies; web caching to improve performance.
* **Endpoint Enforcement:** Install lightweight endpoint agents on faculty/staff laptops for enhanced control and offline monitoring.
* **Logging & SIEM Integration:** Centralized logging of policy violations, user actions; alerting security staff on suspicious behaviour.

**4. Simulation of Enforcement Logic (Pseudo-Policies)**

policy "Student Web Access"

if user.Role == "student" and time in SchoolHours then

block category StreamingVideo

block category SocialMedia

block category Gaming

block category Torrent

log all access attempts

else if user.role == "student" and time in OffHours then

allow category StreamingVideo (limit bandwidth)

allow category SocialMedia (limit time)

block category Torrent

log all suspicious activity

end

policy "Faculty Web Access"

if user.role == "faculty" then

allow all except blacklist malicious domains

audit logs daily

end

policy "Guest Web Access"

if user.role == "guest" then

allow basic browsing and educational sites only

block VPN/proxy tools

log all traffic

end

**5. Updated Network Topology for Enforcement**

* **Next-Gen Firewall/Layer 7 Firewall:** Added at the perimeter or inline with ASA firewall for deep packet inspection.
* **DNS Filtering Cloud Service:** Configured on all campus DHCP scopes and VPNs.
* **Proxy Server:** Inserted in the path of HTTP/S traffic, requiring authentication.
* **Endpoint Agents:** Installed on faculty and staff laptops.
* **SIEM/Log Server:** Centralized log collector connected to firewall, proxy, DNS logs.

**6. Logging, Monitoring, and Reporting**

* **Centralized Log Collection:** To correlate user activity with policy violations.
* **Real-Time Alerts:** For attempts to access blacklisted content or policy violations.
* **Regular Reports:** Distributed to administration summarizing usage trends, violations.
* **Incident Response:** Defined process for handling repeat offenders, including warnings and potential network access restrictions.

**7. Handling Circumvention Attempts**

* Detect common proxy/browser extension signatures.
* Block known VPN and proxy IP addresses via firewall and DNS filtering.
* Endpoint monitoring to alert on unauthorized software usage.
* Education campaigns to inform students about acceptable use policies.

**8. Advantages of the Proposed Policy Framework**

* **Granular Control:** Differentiated treatment by user role and time.
* **Balanced Approach:** Allows legitimate academic research while curbing abuse.
* **Scalability:** Uses cloud and on-premises tools adaptable to growing user base.
* **Easy Monitoring:** Integrated logging and alerts for proactive response.
* **User Awareness:** Transparent policy enforcement with educational initiatives reduces backlash.

**9. Conclusion**

The proposed policy framework smartly integrates modern filtering technologies and user-role awareness to effectively manage web access in the hybrid campus environment. It strikes a balance between enabling academic freedom and controlling bandwidth/cyber risks while building a platform for future enhancements like SASE or machine-learning-based threat detection.