

Report 3 – Smart Web Access Policy

Prepared for: Cisco Networking Academy – Virtual Internship Program 2025

Prepared by: Kasmya Bhatia (23FE10CAI00010)

Date: August 2025

Objective: To create a dynamic and role-based web access policy that restricts harmful and non academic activities during core study hours, preserves network performance, and maintains user satisfaction by allowing flexibility during low demand times.

Policy Intent

The goal is to balance strong network security with academic freedom. Students and faculty should have dependable access to educational resources while non academic or high bandwidth activities, especially those that pose security risks, are limited during busy hours. The policy uses flexible rules that adapt based on user role, time of day, and type of content being accessed.

Policy Rules

Rule ID	Applies To	When	What Happens
P-01	All Users	All Times	Block malware, phishing, illegal sites
P-02	Students	Class Hours (08:00–16:00, Mon–Fri)	Block social media, games, video streaming

P-03	Students	After Hours/Weekends	Allow streaming/games but log activity
P-04	Faculty	All Times	Allow broad access except for blocked risk categories
P-05	All Users	All Times	Permit academic/research sites
P-06	Guests	All Times	Restrict to essential guest portal/info sites

Enforcement Mechanisms

- DNS Filtering: Blocks flagged domains before traffic reaches the campus network; works for all connected devices.
- Layer 7 Firewall: Inspects application-level traffic to block specific activities (e.g., YouTube streaming) without blocking educational content hosted on the same platform.
- User Authentication: Links each web request to a specific user to apply correct rule sets.
- Logging & Alerts: All blocked attempts logged; repeated violations trigger alerts to IT security staff.

Policy Logic & Adaptation

- User Awareness: Policies adapt based on whether the user is a student, faculty member, or guest.
- Time-Based Controls: Stricter during class hours; more relaxed during evenings and weekends.
- Application-Aware Filtering: Allows blocking of risky apps or categories without overblocking educational content.

Circumvention Prevention

- Block unauthorized DNS-over-HTTPS resolvers.
- Restrict installation of unapproved browser extensions.
- Monitor and flag VPN/tunneling activity from student and guest networks.

Deliverables

- Updated Network Diagram: Shows DNS filtering appliance and Layer 7 firewall placement, plus logging server in monitoring zone.
- Web Access Policy Document: Lists all rules, enforcement logic, and exceptions for academic purposes.

Conclusion

The smart web access policy ensures a secure, high performance campus network without unnecessarily restricting academic work. By tailoring access rules to user roles, times, and content types, it reduces misuse, protects against cyber threats, and maintains positive engagement from the college community.