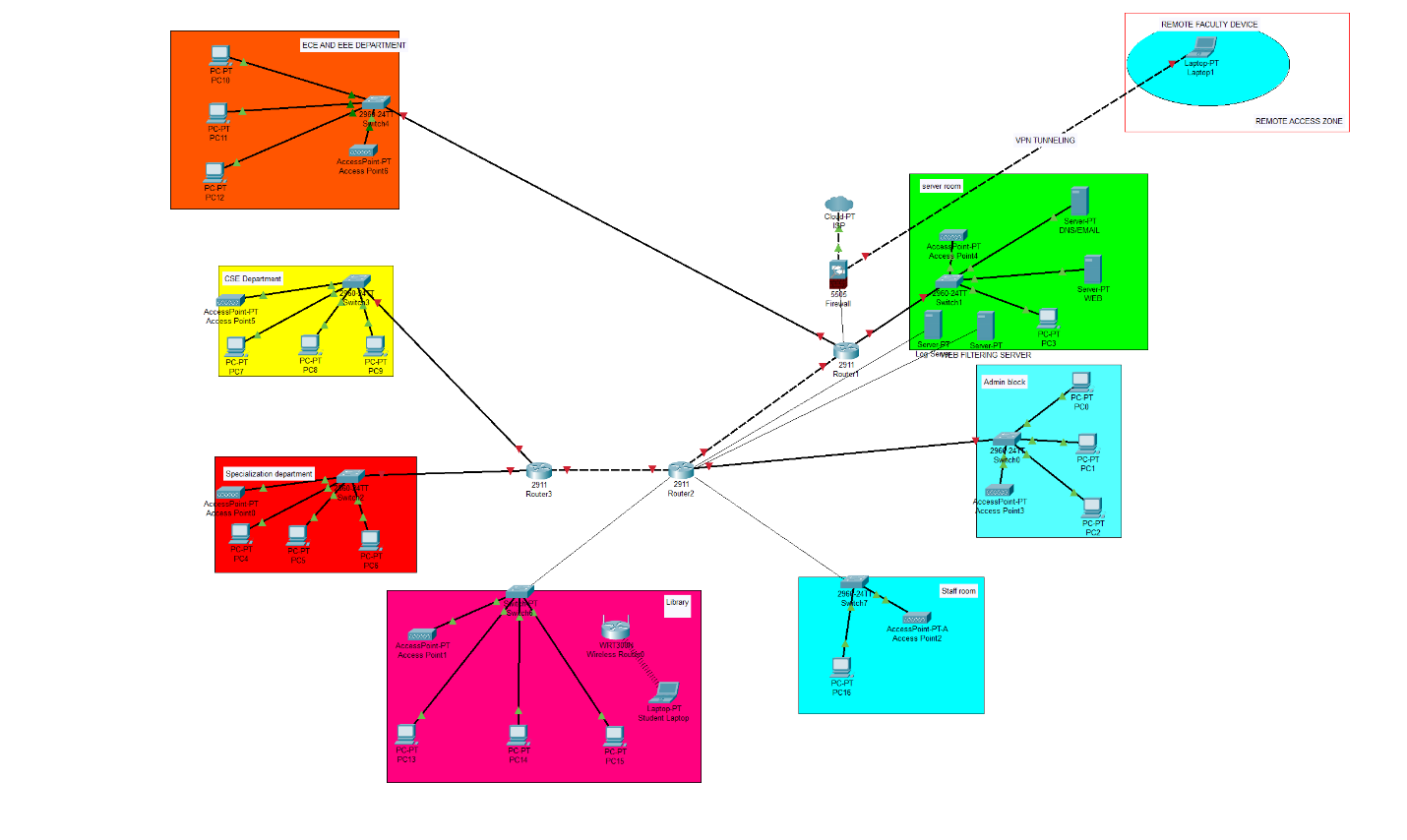
**Web Access Policy and Filtering Framework  
Network Topology Diagram:  
**

**Problem Background**

After implementing the hybrid network, we started getting complaints about students streaming videos during lectures, downloading torrents in computer labs, and bypassing basic restrictions using browser extensions and proxies. The administration needed a smart filtering solution that controls access without blocking legitimate academic research.

**Filtering Technology Comparison**

**DNS-Based Filtering:**

* *Advantages*: Easy to set up, low resource usage, works on all devices
* *Disadvantages*: Easy to bypass with alternative DNS servers, limited granular control
* *Best for*: Basic blocking of known bad domains

**Layer 7 Firewall Filtering:**

* *Advantages*: Deep packet inspection, application-aware, hard to bypass
* *Disadvantages*: More expensive, requires more processing power
* *Best for*: Comprehensive control with detailed policies

**Proxy-Based Filtering:**

* *Advantages*: Good balance of control and cost, detailed logging, content inspection
* *Disadvantages*: Can slow down browsing, requires client configuration
* *Best for*: Medium-sized networks like ours

**Client-Side Enforcement:**

* *Advantages*: Works even outside campus network
* *Disadvantages*: Students can disable or bypass easily
* *Best for*: Additional layer, not primary solution

**Chosen Solution: Hybrid Approach**

I recommend combining **Proxy-based filtering** as primary method with **DNS filtering** as backup, because:

* Proxy gives us detailed control and logging
* DNS filtering catches bypass attempts
* Cost-effective for college budget
* Can handle both HTTP and HTTPS traffic

**User Group Access Policies**

**Students (Most Restrictive)**

**During Class Hours (8 AM - 5 PM, Monday-Friday):**

* ✅ **ALLOWED**: Educational websites, research databases, library resources, email
* ✅ **LIMITED**: News websites (max 30 min/day), educational YouTube videos
* ❌ **BLOCKED**: Social media, gaming sites, streaming services, file sharing, adult content

**After Hours & Weekends:**

* ✅ **ALLOWED**: All educational content plus limited social media
* ⏰ **TIME LIMITED**: Social media (2 hours/day), streaming (1 hour/day)
* ❌ **ALWAYS BLOCKED**: Torrents, inappropriate content, security threats

**Faculty (Moderate Restrictions)**

**All Times:**

* ✅ **ALLOWED**: Academic and research sites, professional social media, educational streaming
* ⏰ **BANDWIDTH LIMITED**: Personal streaming during peak hours (9 AM - 5 PM)
* ❌ **BLOCKED**: File sharing networks, inappropriate content, security threats
* 🔍 **MONITORED**: All activity for security purposes only

**Administrative Staff (Least Restrictive)**

**All Times:**

* ✅ **ALLOWED**: Most business and educational content
* ❌ **BLOCKED**: Only known malicious sites, inappropriate content
* 🔍 **MONITORED**: Bandwidth usage and security threats

**Guest Network (Heavily Restricted)**

**All Times:**

* ✅ **ALLOWED**: Basic web browsing, email
* ⏰ **TIME LIMITED**: 2 hours per day, 500 MB data limit
* ❌ **BLOCKED**: Social media, streaming, downloads, file sharing

**Policy Enforcement Logic**

**Time-Based Rules Implementation:**

IF (current\_time BETWEEN 08:00 AND 17:00) AND (weekday) THEN

apply\_strict\_student\_policy()

ELSE IF (current\_time BETWEEN 17:00 AND 23:00) THEN

apply\_relaxed\_student\_policy()

ELSE

apply\_minimal\_access\_policy()

**Content Category Rules:**

STUDENT\_BLOCKED\_CATEGORIES = [

"social\_media", "gaming", "streaming", "file\_sharing",

"adult\_content", "proxy\_services"

]

FACULTY\_LIMITED\_CATEGORIES = [

"personal\_streaming", "non\_work\_social\_media"

]

**Bandwidth Management:**

* Students: 10 Mbps during class, 25 Mbps after hours
* Faculty: 50 Mbps always, unlimited for research
* Admin: 100 Mbps for business needs
* Guests: 5 Mbps maximum

**Network Implementation**

**Components Added:**

* **Web Filtering Server**: Handles proxy filtering and policy enforcement
* **Log Server**: Stores access logs and generates reports
* **DNS Server**: Provides DNS-based blocking as secondary layer

**Traffic Flow:**

1. User requests website
2. Request goes to Web Filtering Server
3. Server checks user group and current time
4. Applies appropriate policy rules
5. Either allows, blocks, or rate-limits the request
6. Logs all activity to Log Server

**Bypass Prevention Strategies**

**Common Bypass Methods & Countermeasures:**

**VPN Services:**

* Block known VPN provider IPs and domains
* Monitor for VPN-like traffic patterns
* Educational campaign about policy violations

**Proxy Websites:**

* Maintain updated list of proxy sites
* Block categories containing proxy services
* Use keyword filtering for new proxy sites

**DNS Changes:**

* Block external DNS queries at firewall level
* Force all devices to use campus DNS servers
* Monitor DNS traffic for tunneling attempts

**Mobile Hotspots:**

* Policy education about personal device usage
* WiFi signal monitoring in labs (where appropriate)
* Data usage reporting to identify excessive mobile usage

**Logging and Monitoring**

**Information Logged:**

* User identity and device information
* Websites accessed and time stamps
* Blocked attempts and reasons
* Bandwidth usage per user
* Policy violation attempts

**Alert Triggers:**

* Multiple policy violations by same user
* Attempts to access blocked categories repeatedly
* Unusual bandwidth usage patterns
* Suspected bypass attempts
* Malware or phishing site access attempts

**Reporting:**

* Daily summary of blocked content by category
* Weekly user activity reports for departments
* Monthly bandwidth usage analysis
* Violation reports for administration review

**Policy Intent and Educational Approach**

**Primary Goals:**

* Maintain academic focus during class hours
* Prevent network abuse and excessive bandwidth usage
* Protect users from malicious content
* Comply with legal requirements for educational institutions

**Educational Component:**

* Clear communication of policies to all users
* Regular reminders about appropriate usage
* Digital citizenship training for students
* Faculty guidance on academic freedom vs. policy compliance

**Enforcement Philosophy:**

* Progressive discipline: warning → restriction → escalation
* Focus on education rather than punishment
* Consider academic needs and research requirements
* Regular policy review and updates based on feedback

**Advantages of This Framework**

1. **Flexible**: Different rules for different users and times
2. **Educational**: Balances control with learning opportunities
3. **Scalable**: Can adjust rules based on network capacity
4. **Transparent**: Clear policies communicated to users
5. **Reasonable**: Allows legitimate academic and personal use

**Policy Review Process**

* Quarterly review of blocked categories and user feedback
* Annual assessment of policy effectiveness
* Regular updates to bypass prevention measures
* Continuous monitoring of network performance impact

This framework provides comprehensive web access control while respecting the educational mission of the institution and the legitimate needs of faculty and students.