University of Information Technology

Faculty of Computer Network and Communications

PHẠM THANH TÂM – 21522573

NGUYỄN ĐÌNH KHA – 21520948

NGUYỄN VĂN ANH TÚ – 21520514

FINAL REPORT

Subject: System And Network Administration

SQUID PROXY

CLASS: NT132.O11.ATCL

LECTURER: TRẦN THỊ DUNG

HO CHI MINH CITY, 2023

Table of Contents

I. INTRODUCTION

1.1 General Information

1.1.1 What is Proxy?

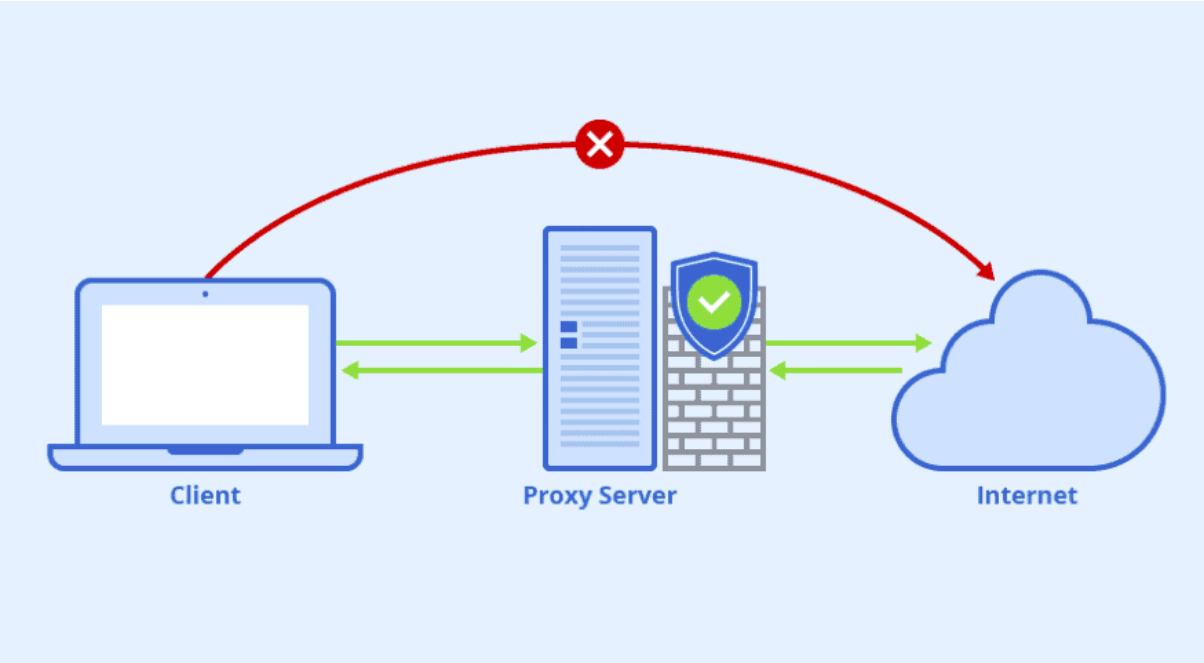
Proxy, Server Proxy, or Proxy Server (which are essentially the same thing) can be understood as a separate computer tasked with processing data, acting as an intermediary for Internet signals. By connecting through one or multiple proxy servers, a user's computer will send request signals through the proxy server, where the information will be processed and returned to the user, resulting in what is seen when accessing the Internet. In this understanding, the Proxy plays the role of an intermediary between the user's computer and the entire external Internet environment. Additionally, Proxies are also used for filtering and blocking websites, or more precisely, specific website content based on the needs of governments, service providers, etc.

1.1.2 Squid Proxy

Squid is a proxy cache server which provides proxy and cache services for Hyper Text Transport Protocol (HTTP), File Transfer Protocol (FTP), and other popular network protocols. It’s improve the performance and optimised the network bandwidth. It can also filter web traffic, helping to improve security.

Along with actual caching, Squid offers a wide range of features:

- Distributing load over intercommunicating hierarchies of proxy servers
- Defining strict access control lists for all clients accessing the proxy server
- Allowing or denying access to specific Web pages using other applications
- Generating statistics about frequently-visited Web pages for the assessment of surfing habits



1.2 Components

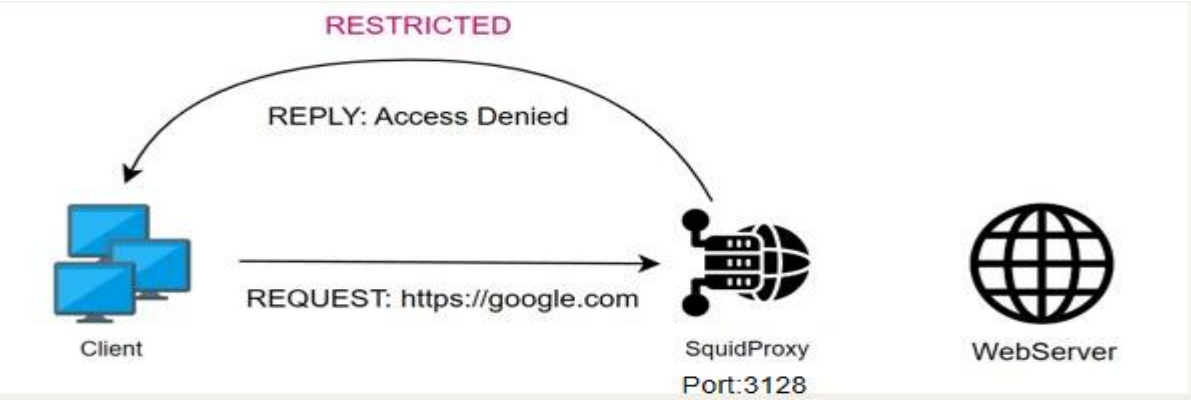
Squid proxy contains 2 main elements in its configuration file:

- **Access-list (ACL) elements**: including lines that specify the object that needs access control and begin with the letter "acl"
- **Access-list (ACL) rules**: includes restrictions on the use of ACL Elements objects. ACL rules operate by individually comparing ACL elements to specified rules, if a match is found, the rule is applied and the comparison is immediately terminated. The logical and operation will be used to compare ruless that contain multiple ACL items (all ACL elements must match the ACL rule)

```
acl Safe_ports port 280     # http-mgmt
acl Safe_ports port 488     # gss-http
acl Safe_ports port 591     # filemaker
acl Safe_ports port 777     # multiling http
acl whitelist dstdomain .symcb.com
acl CONNECT method CONNECT

#
# Recommended minimum Access Permission configuration:
#

# Only allow cachemgr access from localhost
http_access allow whitelist #make sure this is added before your acl proxy_auth configuration
http_access allow localhost manager
http_access deny manager

# Deny requests to certain unsafe ports
http_access deny !Safe_ports
```

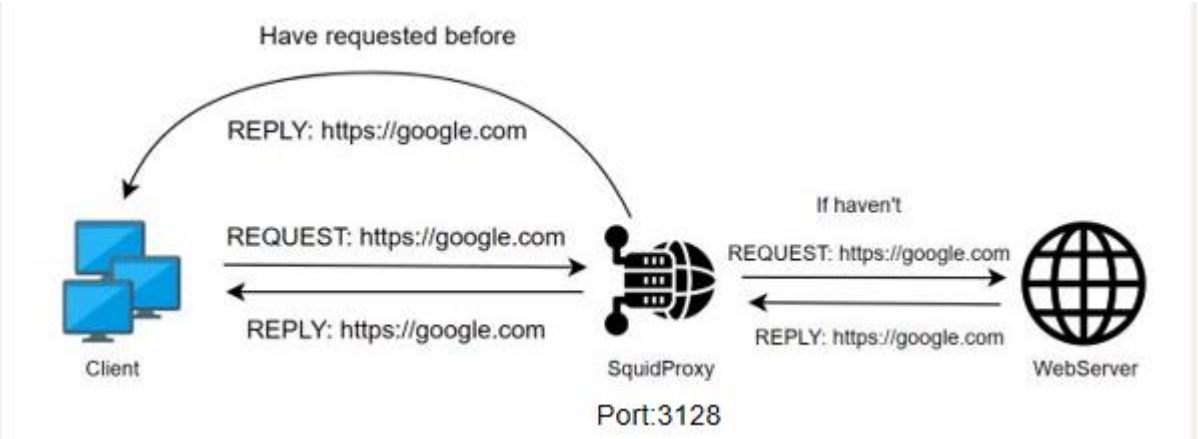
1.3 Operation

- Case 1: The user's REQUEST is restricted by squid proxy



- When a client sends a REQUEST to the web server but is denied by the Squid Proxy, the access is immediately denied and the client is limited without sending the request to the web server.

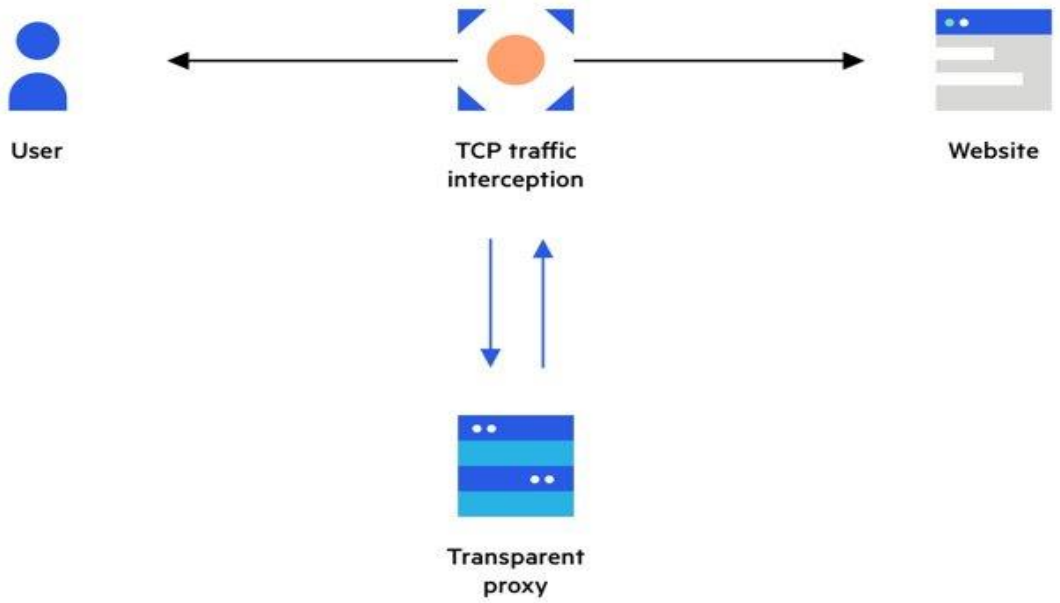
- Case 2: The user's REQUEST is allowed/not restricted by Squid Proxy



• The Squid Proxy will request the website's server if the client has never requested to that url before. Once the web server responds, Squid will reply to the client and cache the information for future requests.

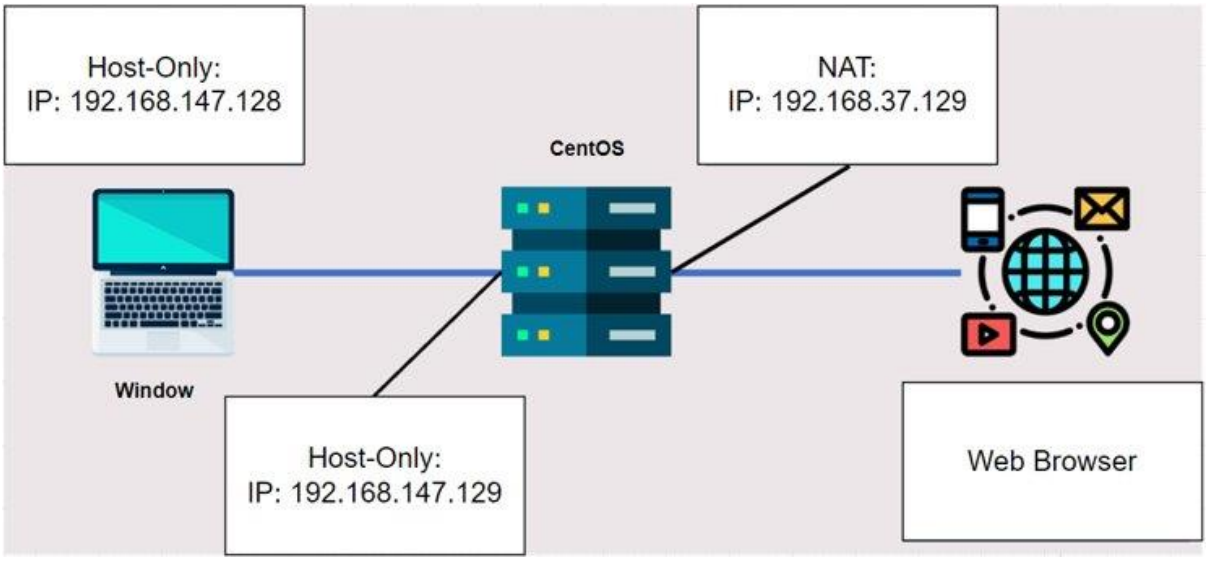
• If the client has already accessed this web server, Squid will immediately return the RESPONSE to the client without making another request to the web server.

- Transparent Mode : Squid as transparent proxy acts as a gateway between internets and users.



II. IMPLEMENTATION

2.1 Topology



Host	IP Address	OS
Squid Proxy Server	NAT: 192.168.37.129/24 Host-Only: 192.168.147.129/24	CentOS 7/Linux
Client	Host-Only: 192.168.147.128/24	Windows 10

2.2 Installation

- Install the Squid Proxy by using the following command:

```
[root@localhost kop]# yum -y install squid
```

- Start the squid service:

```
[root@localhost kop]# systemctl start squid
```

- Add the Squid Service to autostart:

```
[root@localhost kop]# systemctl enable squid
```

- Check the Squid Status to make sure that the service have installed and running:

```
[root@localhost kop]# systemctl status squid
● squid.service - Squid caching proxy
   Loaded: loaded (/usr/lib/systemd/system/squid.service; enabled; vendor preset
: disabled)
   Active: active (running) since Sun 2023-11-12 22:00:18 +07; 47s ago
 Main PID: 3381 (squid)
    Tasks: 3
   CGroup: /system.slice/squid.service
           ├─3381 /usr/sbin/squid -f /etc/squid/squid.conf
           ├─3388 (squid-1) -f /etc/squid/squid.conf
           └─3393 (logfile-daemon) /var/log/squid/access.log

Nov 12 22:00:18 localhost.localdomain systemd[1]: Starting Squid caching prox...
Nov 12 22:00:18 localhost.localdomain systemd[1]: Started Squid caching proxy.
Nov 12 22:00:18 localhost.localdomain squid[3381]: Squid Parent: will start 1...
Nov 12 22:00:18 localhost.localdomain squid[3381]: Squid Parent: (squid-1) pr...
Hint: Some lines were ellipsized, use -l to show in full.
```

2.3 Configuration

- File squid.conf by default:

```
# Example rule allowing access from your local networks.
# Adapt to list your (internal) IP networks from where browsing
# should be allowed
acl localnet src 10.0.0.0/8     # RFC1918 possible internal network
acl localnet src 172.16.0.0/12  # RFC1918 possible internal network
acl localnet src 192.168.0.0/16 # RFC1918 possible internal network
acl localnet src fc00::/7       # RFC 4193 local private network range
acl localnet src fe80::/10      # RFC 4291 link-local (directly plugged) machines

acl SSL_ports port 443
acl Safe_ports port 80          # http
acl Safe_ports port 21          # ftp
acl Safe_ports port 443         # https
acl Safe_ports port 70          # gopher
acl Safe_ports port 210         # wais
acl Safe_ports port 1025-65535  # unregistered ports
acl Safe_ports port 280         # http-mgmt
acl Safe_ports port 488         # gss-http
acl Safe_ports port 591         # filemaker
acl Safe_ports port 777         # multiling http
acl CONNECT method CONNECT

#
# Recommended minimum Access Permission configuration:
#
# Deny requests to certain unsafe ports
http_access deny !Safe_ports

# Deny CONNECT to other than secure SSL ports
http_access deny CONNECT !SSL_ports

# Only allow cachemgr access from localhost
http_access allow localhost manager
http_access deny manager

# We strongly recommend the following be uncommented to protect innocent
# web applications running on the proxy server who think the only
# one who can access services on "localhost" is a local user
```

- Use the following command to config Squid Proxy:

```
[root@localhost kop]# vim /etc/squid/squid-conf
```

- Squid normally listens to port 3128:

```
# Squid normally listens to port 3128
http_port 3128
```

- Adjust cache memory and cache directory:

```
#cache_dir ufs /var/spool/squid 100 16 256
cache_mem 512 MB
cache_dir ufs/var/spool/squid 4096 100 256
# Leave coredumps in the first cache dir
```

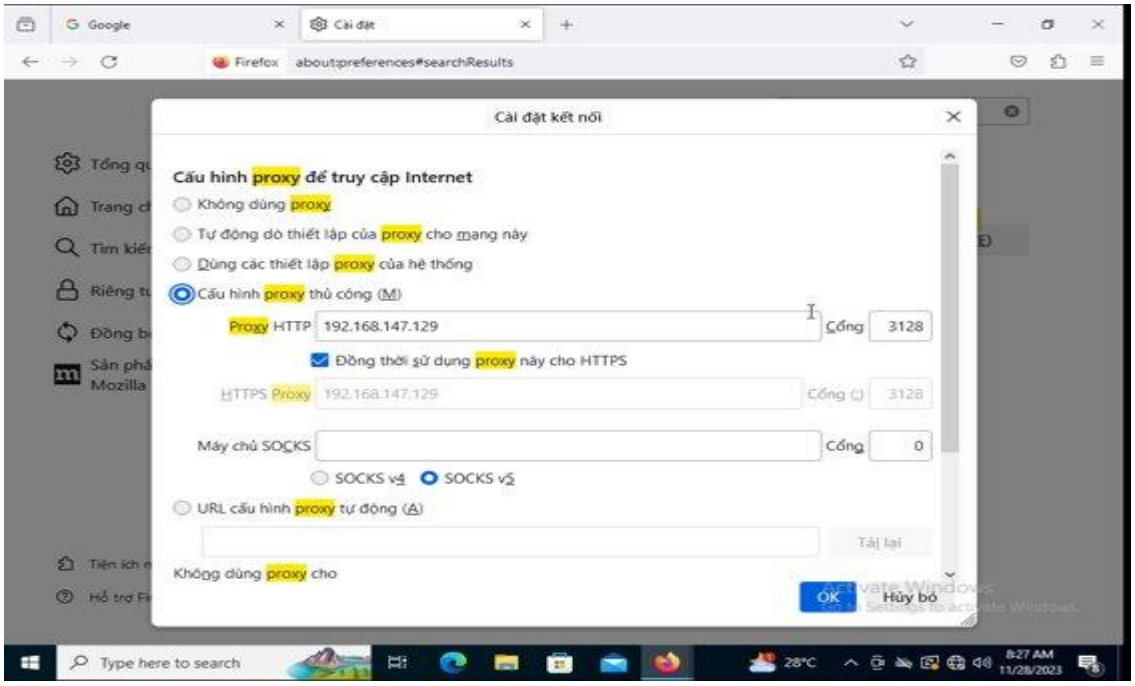
- Add rule to the Squid.conf, these command will allow LAN IP address can connect:

```
acl LAN1 src 192.168.71.0/24
acl localnet src 10.0.0.0/8     # RFC1918 possible internal network

http_access allow LAN1
```

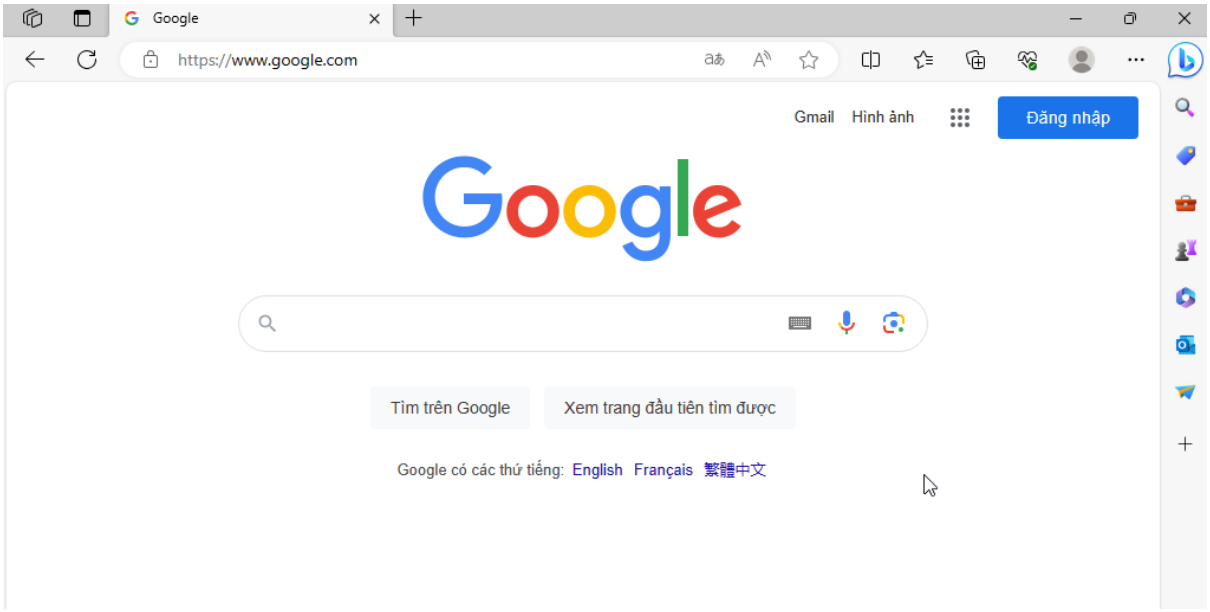
- Restart the Squid Proxy and turn off the firewall:

```
[root@localhost kop]# systemctl restart squid
[root@localhost kop]# systemctl stop firewall
Failed to stop firewall.service: Unit firewall.service not loaded.
[root@localhost kop]# systemctl stop firewalld
```

- Settings the proxy for the client (using Squid Proxy's IP Address and Port):



- The client can connect to the website normally so the configuration have successfully.



2.3.1 Basic

- Restrict client access to some websites:

- Create a blocksites list:

```
[root@localhost kop]# vi /etc/squid/blocksites.acl
[root@localhost kop]#
```

- Set up access list to block the sites:

```
#BlockSites
acl blocksites dstdomains "/etc/squid/blocksites"
http_access deny blocksites
```

- Restrict client download or view some kind of files (.html, etc.)

```
#block html
acl blockhtml urlpath_regex .html
http_access deny blockhtml
```

- Restrict worktime for client:

```
#TimeLimit
acl timelimit time 00:00 - 23:59
http_access deny timelimit
```

2.3.2 Advance

- Enable IP Forwarding on Squid:

```
[root@localhost squid]# sysctl -w net.ipv4.ip_forward=1
net.ipv4.ip_forward = 1
```

- Configure iptables with the following command:

```
[root@localhost kop]# iptables -t nat -A PREROUTING -p tcp --dport 80 -j REDIRECT --to-port 3128
```

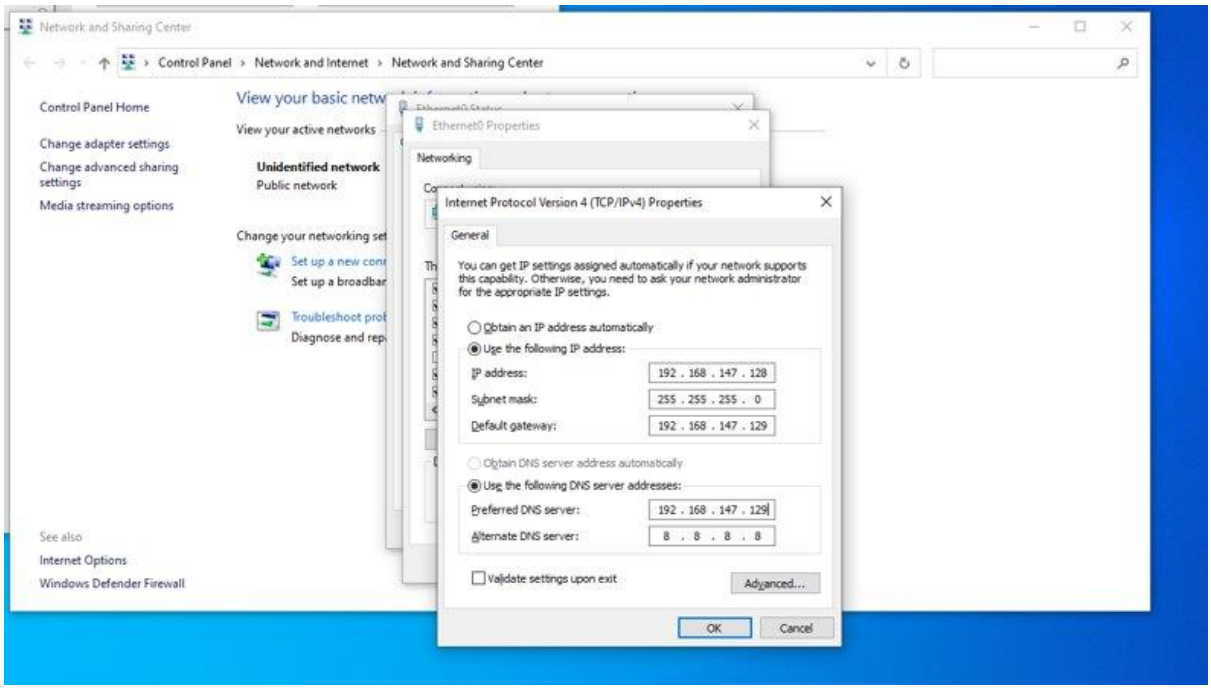
```
[root@localhost kop]# iptables -t nat -A PREROUTING -i ens34 -p tcp --dport 80 -j REDIRECT --to-port 3128
[root@localhost kop]# iptables -t nat -A POSTROUTING -o ens33 -j MASQUERADE
```

- Save and restart IPTables:

```
[root@localhost kop]# iptables-save > /etc/sysconfig/iptables
```

```
[root@localhost kop]# systemctl restart iptables
```

- Import the Squid's IP to work as a default-gateway and create an IP for client which have the same host to Squid:

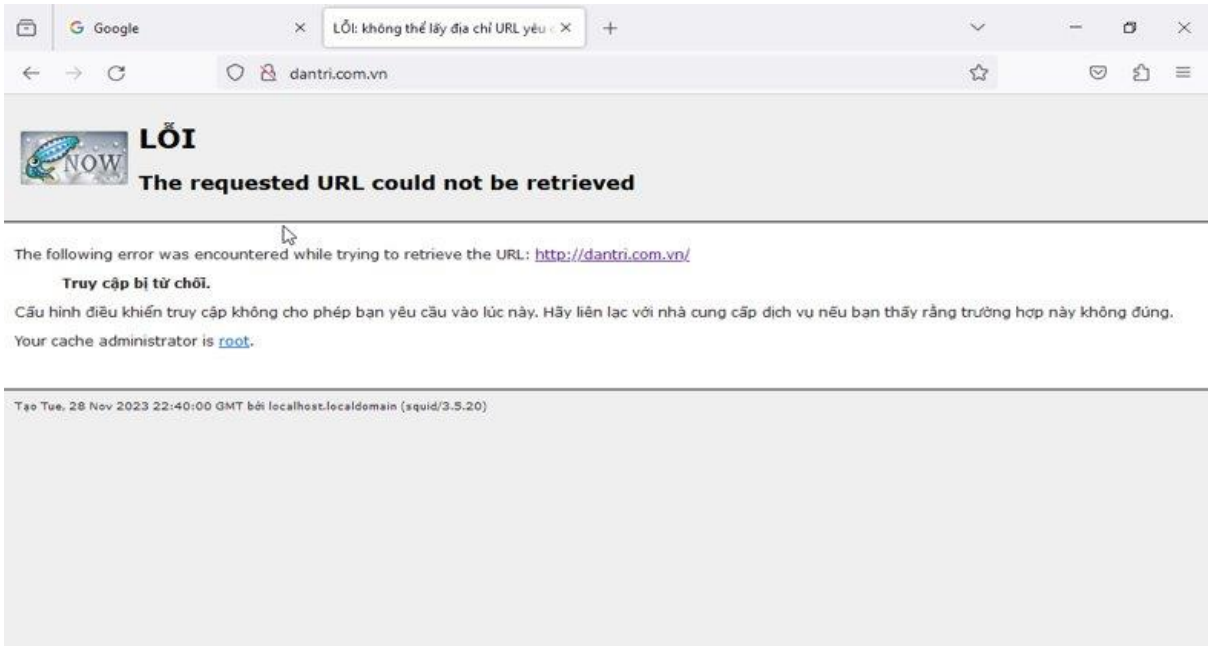


III. RESULT AND CONCLUSION

3.1 Result

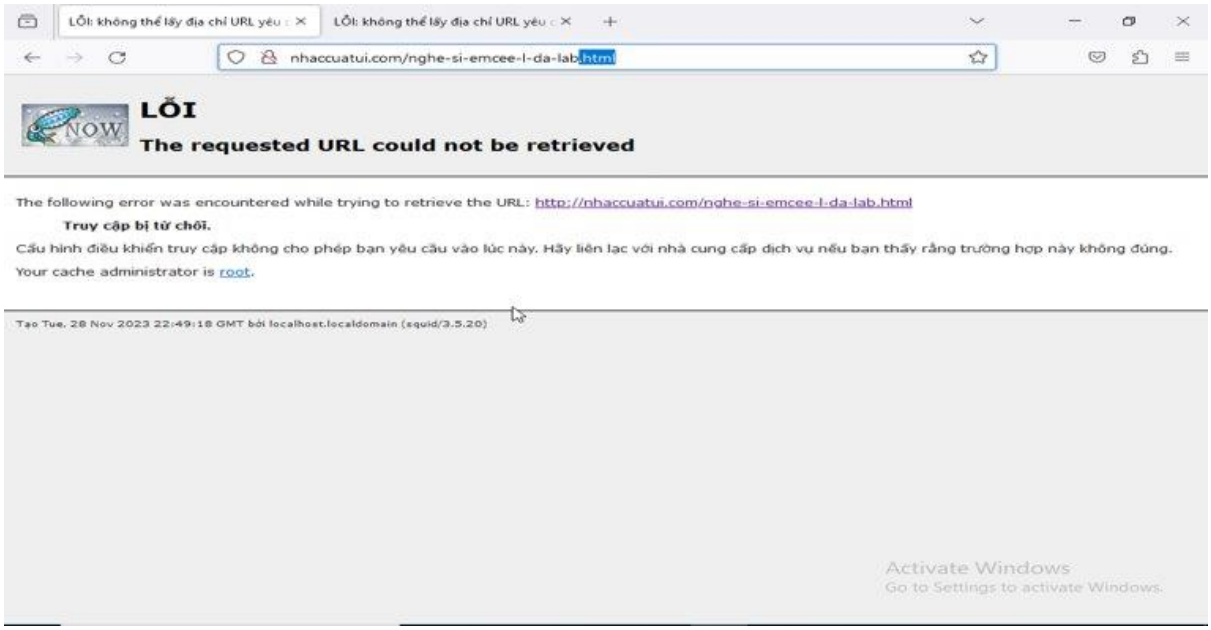
Basic:

- Restrict client access to some websites:



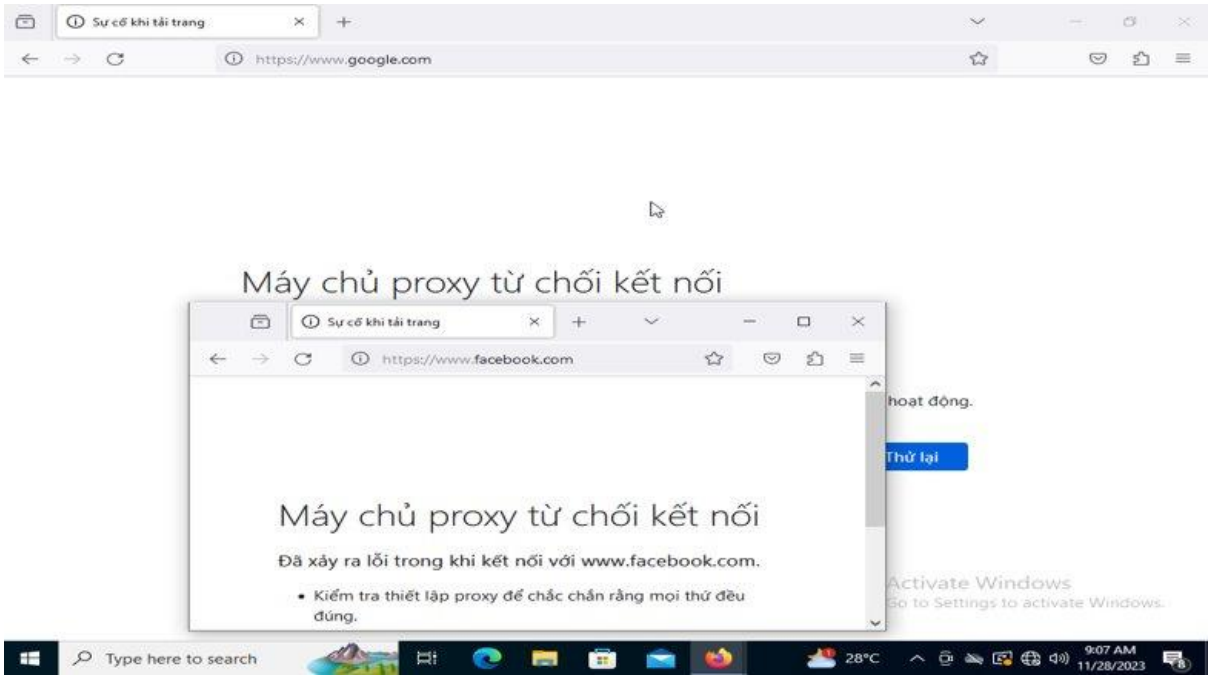
- Dantri.com.vn is blocked by Squid proxy

- Restrict client download or view some kind of files (.html, etc.)



- Squid blocked (.html) files

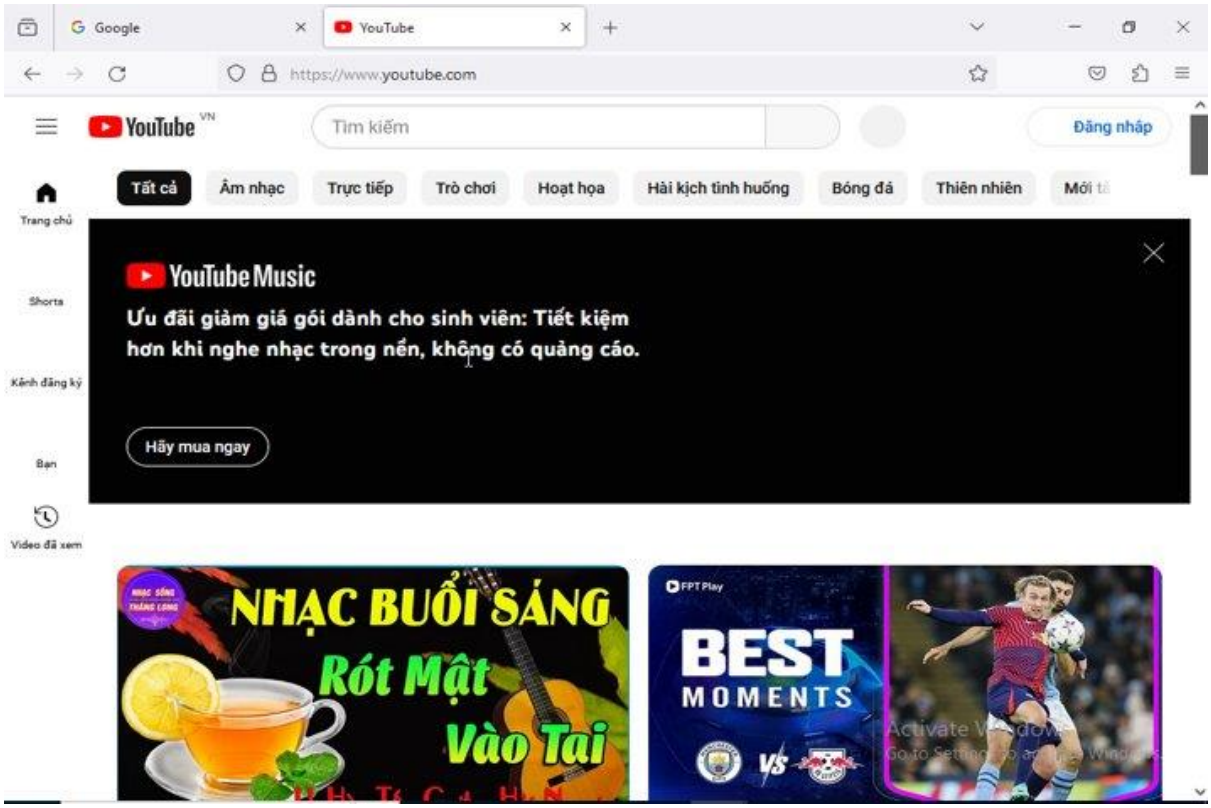
- Restrict worktime for client:



- Squid restricted time to connect to the internet

Advanced:

- Client can connect to the Internet by Squid Proxy without importing IP for each and every browser:



3.2 Conclusion

The experimental results of the entire model have successfully met the following requirements:

- The Squid Proxy have restricted the websites, some kind of files and timelimit successfully
- The Squid Proxy have worked as a router and the client can connect to the internet successfully

IV. WORK ASSIGNMENT AND EVALUATIONS

4.1 Work assignments

Member	Task	Complete (%)
Pham Thanh Tam	Advance requirements, Report	100
Nguyen Dinh Kha	Basic requirements, Slide	100
Nguyen Van Anh Tu	Basic requirements, Slide	100

4.2 Self-assessment

Citeria	**4**	**3**	**2**	**1**
Report format (1 point)	X			
Presentation (1 point)		X		
Theory (2 point)	X			
Demonstration (5 point)		X		
Total	**8.5**			

4.3 Question

Question 1: We want to set up HTTPS proxy server instead of HTTP proxy server. What are the steps for setting up?

Answer 1:

- Generate ECC Private Key and CSR using OpenSSL:

```
openssl req -newkey ec -pkeyopt ec_paramgen_curve:prime256v1 -keyout ecc_private_key.pem -out ecc_csr.pem
```

- Configure Squid with ECC Certificate:

```
https_port 3128 cert=/path/to/ecc_certificate.pem key=/path/to/ecc_private_key.pem
```

- Restart Squid:

```
sudo systemctl restart squid
```

- Configure Client Devices and Testing

Question 2: Is it possible to authenticate user access in Squid Proxy?

Answer 2: Yes, Squid Proxy supports various methods for authenticating user access but it’s not in my scopes of project requirements.

Question 3: Why using IP Tables instead of Firewall to set up?

Answer 3: When configuring Squid Proxy in transparent mode, meaning the proxy operates without requiring explicit proxy configuration on the client, HTTP requests from the client are automatically redirected through the proxy. To achieve this, you typically need to use iptables to set up packet redirection rules. The use of iptables ensures that all HTTP packets are redirected through Squid Proxy without the need to modify the configuration on each client.

Question 4: Do you use Squid to block harmful content such as viruses and malware?

Answer 4: No. We don’t but Squid Proxy has the capability to block harmful content, including viruses and malware, through the implementation of various filtering mechanisms. Squid Proxy itself primarily focuses on web content caching and proxying, but it can be extended with additional features and tools to enhance security.