ĐẠI HỌC QUỐC GIA TP.HỒ CHÍ MINH

TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN KHOA MẠNG MÁY TÍNH VÀ TRUYỀN THÔNG

FINAL REPORT

NETWORKS AND SYSTEMS ADMINISTRATIONS

TOPIC

SQUID PROXY

.

Group 3:

Trương Tuấn Phi	20521741
Nguyễn Trần Anh Quân	20521793
Nguyễn Đức Toàn	20522026

TP. Hồ Chí Minh, tháng 1 năm 2023

\

Table of Contents

I. INTRODUCTION **3**

1.1. Overview *3*

1.2. Components *3*

1.3. Operations *4*

II. IMPLEMENTATION **4**

2.1. Topology *4*

2.2. Installation *5*

2.3. Configuration *6*

III. RESULT AND CONCLUSION **7**

3.1. Basic *7*

3.2. Advance: *12*

IV. WORK ASSIGNMENTS AND EVALUATIONS **15**

4.1. Work assignments *15*

4.2. Self-assessment *15*

4.3. Question *15*

\

I. INTRODUCTION

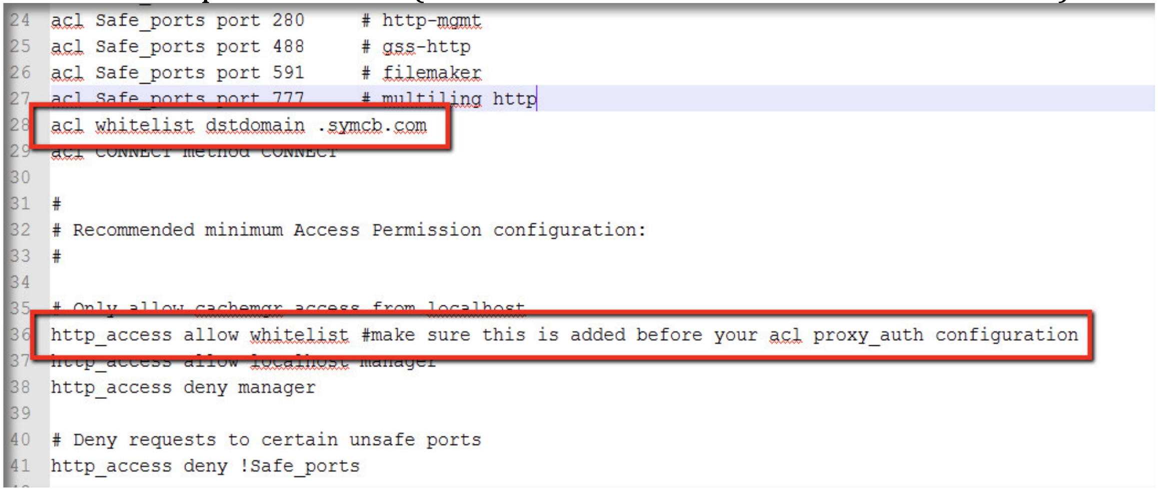
1.1. Overview

- **A proxy server** acts as a gateway between users and the Internet. It's an intermediary server separating end users from the websites they browse. Depending on the use case, needs, or company policy, proxy servers provide varying levels of functionality, security, and privacy. Proxy sersers act as a firewall and web filter, provide shared network connections, and cache data to speed up common requests
- **Squid proxy** is a full-featured web proxy cache server application which provides proxy and cache services for Hyper Text Transport Protocol (HTTP), File Transfer Protocol (FTP), and other popular network protocols. It reduces bandwidth and improves response times by caching and reusing frequently-requested web pages or works as a firewall to restrict or allow users access to certain areas of the Internet

1.2. Components

Squid proxy contains 2 main elements in its configuration file

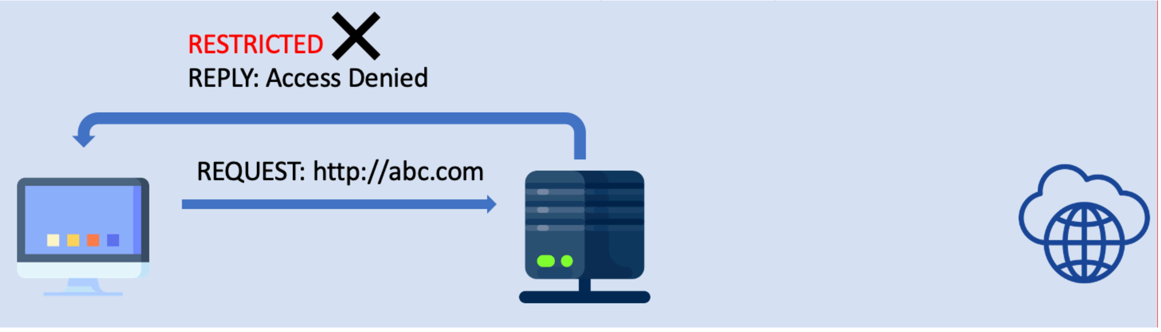
- **Access-list (ACL) elements**: including lines that specify the object that needs access control and begin with the letter "acl"
- **Access-list (ACL) rules**: includes restrictions on the use of ACL Elements objects. ACL rules operate by individually comparing ACL elements to specified rules, if 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
```

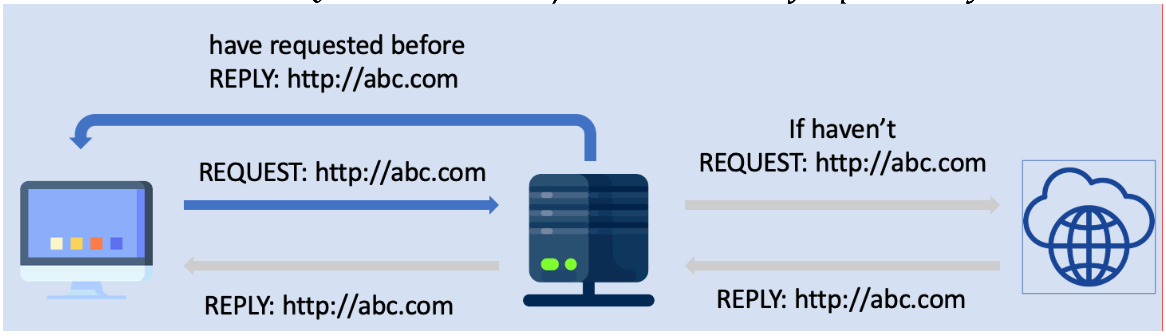
1.3. Operations

- *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.

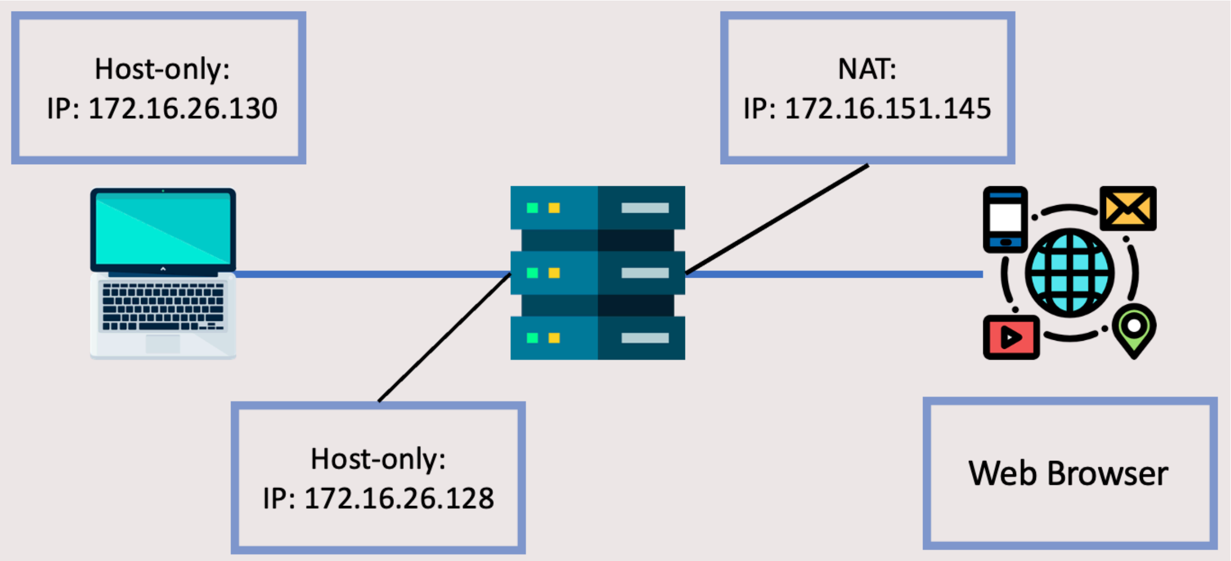
- *Case 2:* *The user's REQUEST is allowed/not restricted by Squid Proxy*

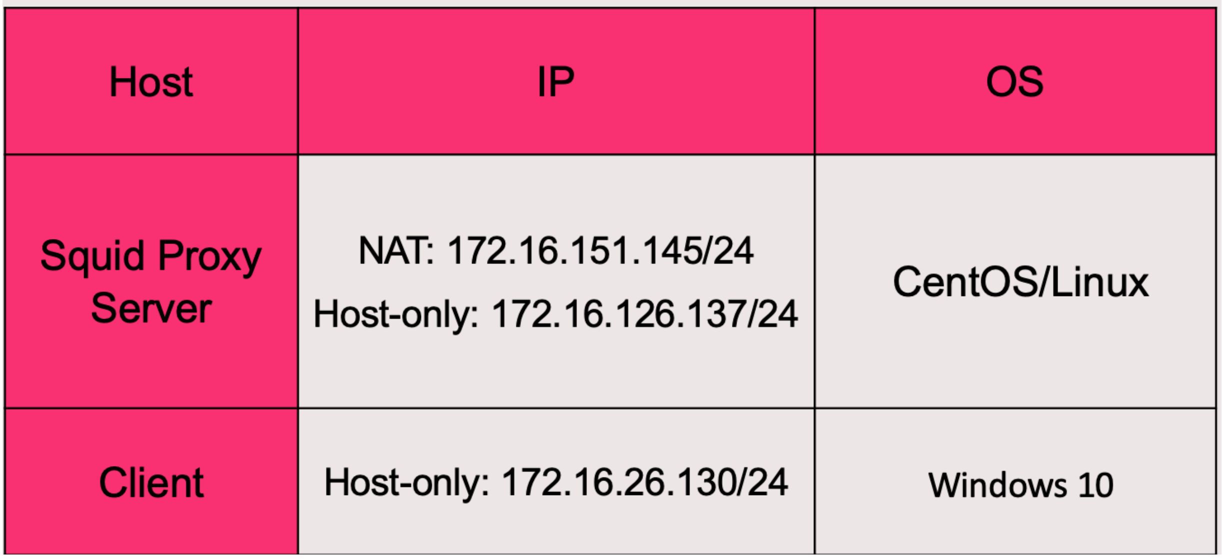


- The Squid Proxy will request the website's server if the client has never requested to that url before. Once the web server responds, Squid will reply to the client and cache the information for future requests.
- If the client has already accessed this web server, Squid will immediately return the RESPONSE to the client without making another request to the web server.

II. IMPLEMENTATION

2.1. Topology



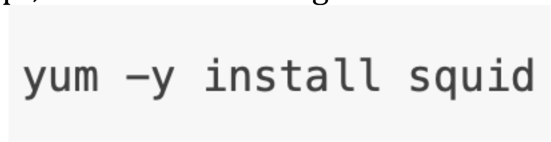


Host	IP	OS
Squid Proxy Server	NAT: 172.16.151.145/24 Host-only: 172.16.126.137/24	CentOS/Linux
Client	Host-only: 172.16.26.130/24	Windows 10

Two virtual machines were utilized for the demonstration of this topic. With the CentOS/Linux Operation System and Network interface cards that are NAT and Host-only, we employed the Squid Proxy Server. Moreover, the client computer we utilized had a Host-only card and was Windows 10

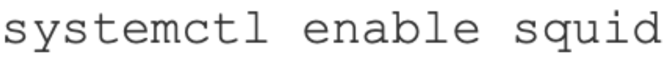
2.2. Installation

- At a terminal prompt, enter the following command to install the Squid server:



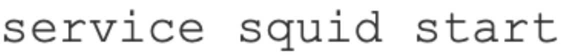
```
yum -y install squid
```

- Add the Squid service to autostart. To do so, execute the command



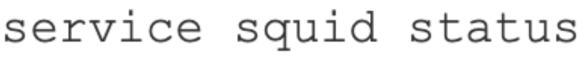
```
systemctl enable squid
```

- Start the Squid service. To do so, execute the command:



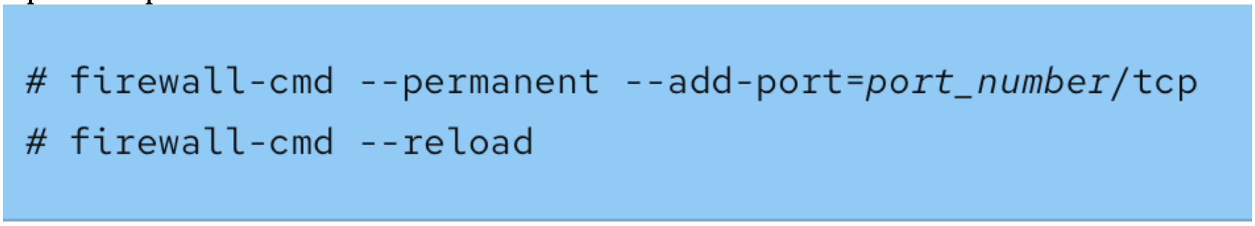
```
service squid start
```

- Check the status of the Squid service. To do so, execute the command:



```
service squid status
```

- Open the port in firewall then reload



```
# firewall-cmd --permanent --add-port=port_number/tcp
# firewall-cmd --reload
```

2.3. Configuration

- To add rule, Squid is configured by editing the directives contained within the **/etc/squid/squid.conf** configuration file
- Squid works on the the default port “3128”, this port can be changed mannually

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

- It is recommended to configure SSL Bumping in the Squid service to handle encrypted connections. If SSL Bumping is not configured, the proxy server cannot intervene in the process of establishing an encrypted connection. To make things clearer, Squid Proxy Server can only execute on the HTTP protocol and has no impact on HTTPS if SSL Bump is not used.
- Create a self-signed SSL certificate

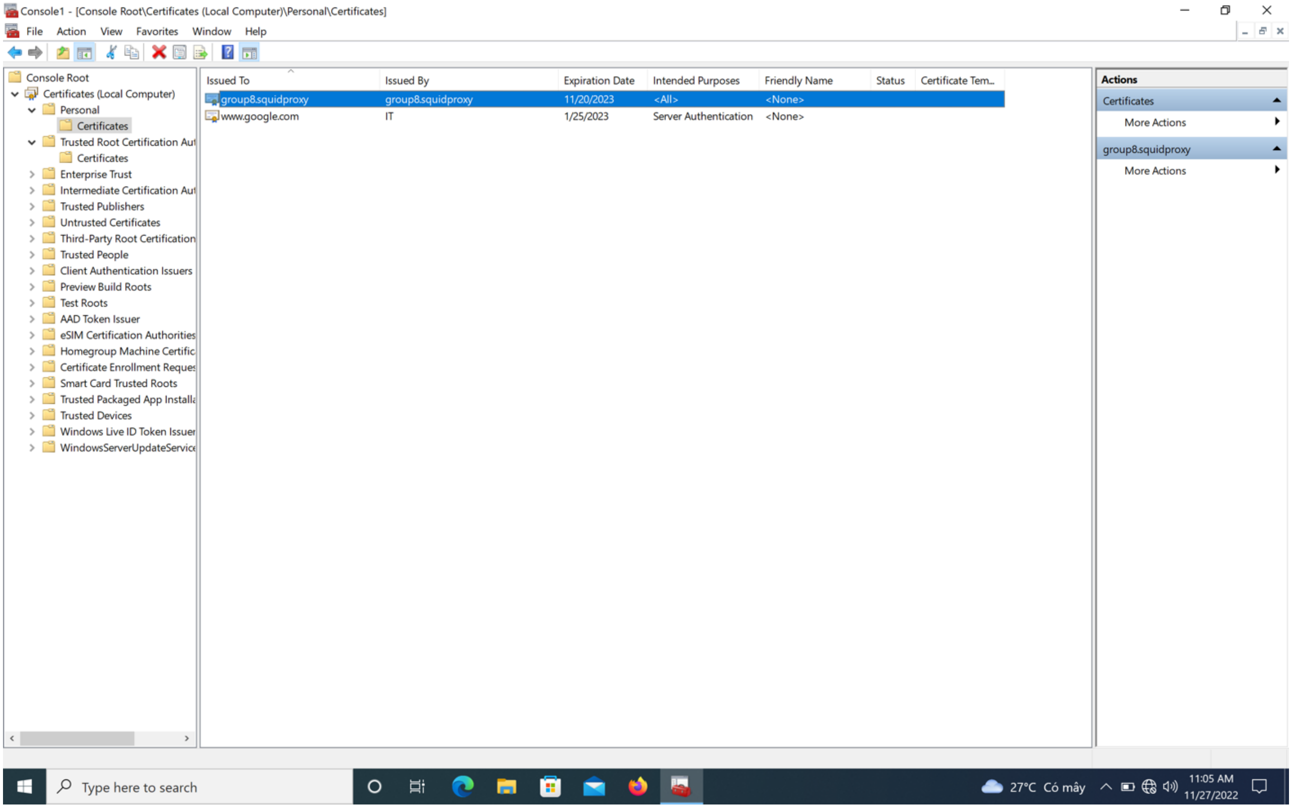
```
openssl req -new -newkey rsa:2048 -days <certificate validity period in days> -nodes -x509 -keyout squidCA.pem
-out squidCA.pem
```

Replace `http_port 3128` with `http_port 3128 ssl-bump generate-host-certificates=on dynamic_cert_mem_cache_size=4MB cert=/etc/squid/squidCA.pem.`

- Create a trusted certificate to be imported into client’s machine

```
openssl x509 -in squidCA.pem -outform DER -out squid.der
```

- Import the certificate into the client machine



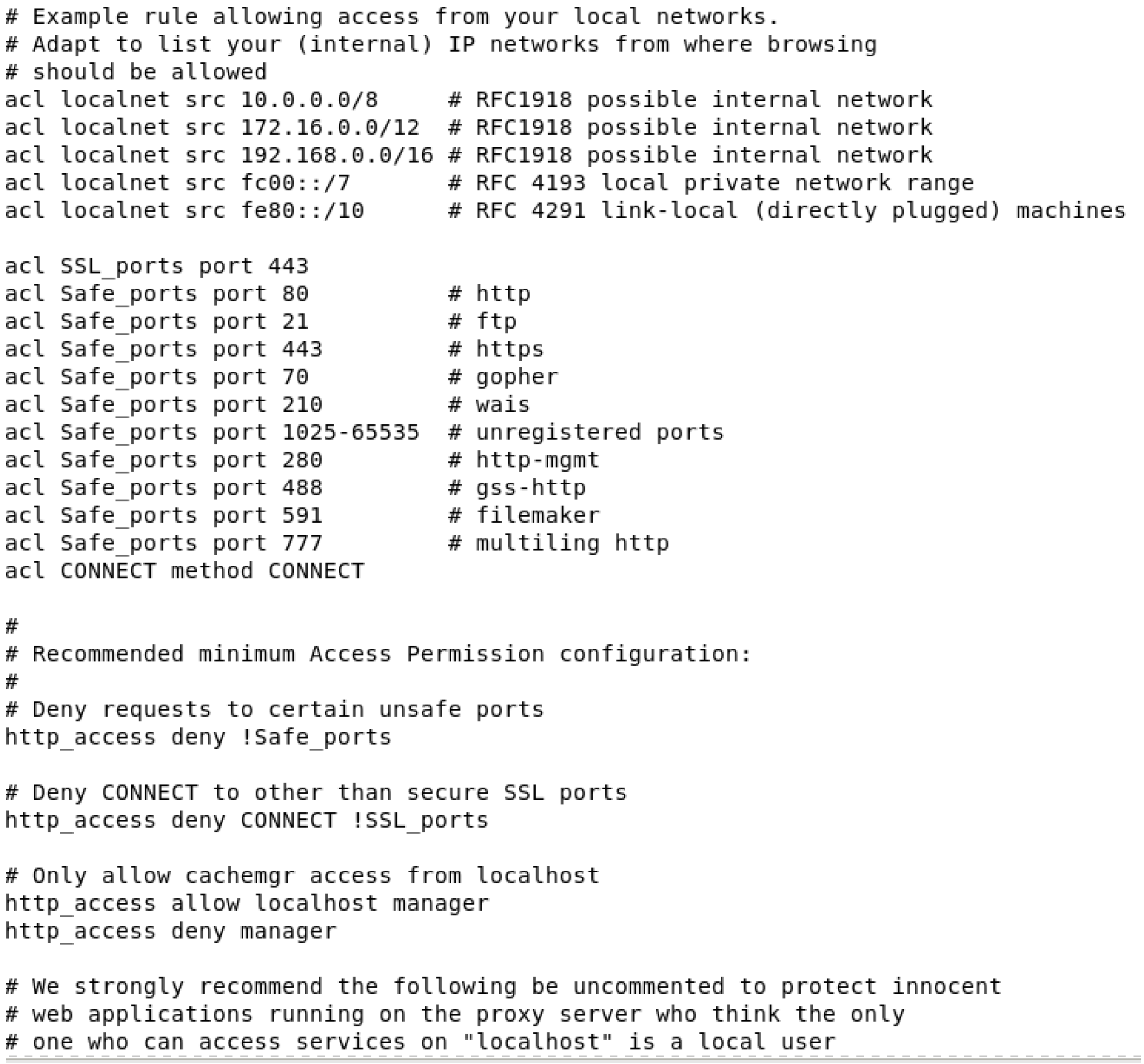
Console1 - [Console Root\Certificates (Local Computer)\Personal\Certificates]

Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name	Status	Certificate Tem...
group8.squidproxy	group8.squidproxy	11/20/2023	<All>	<None>		
www.google.com	IT	1/25/2023	Server Authentication	<None>		

III. RESULT AND CONCLUSION

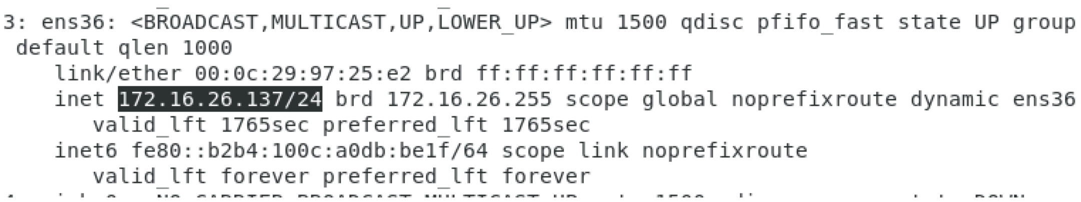
3.1. Basic

- ***File squid.conf by default***



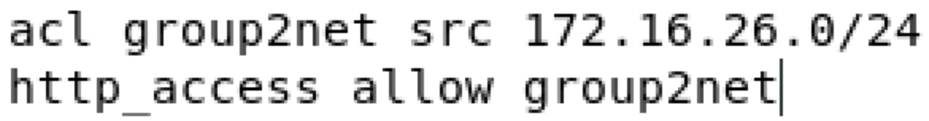
```
# Example rule allowing access from your local networks.
# Adapt to list your (internal) IP networks from where browsing
# should be allowed
acl localnet src 10.0.0.0/8     # RFC1918 possible internal network
acl localnet src 172.16.0.0/12  # RFC1918 possible internal network
acl localnet src 192.168.0.0/16 # 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
```

- ***Create a rule that allows the system at LAN IP address to connect***
  - LAN host



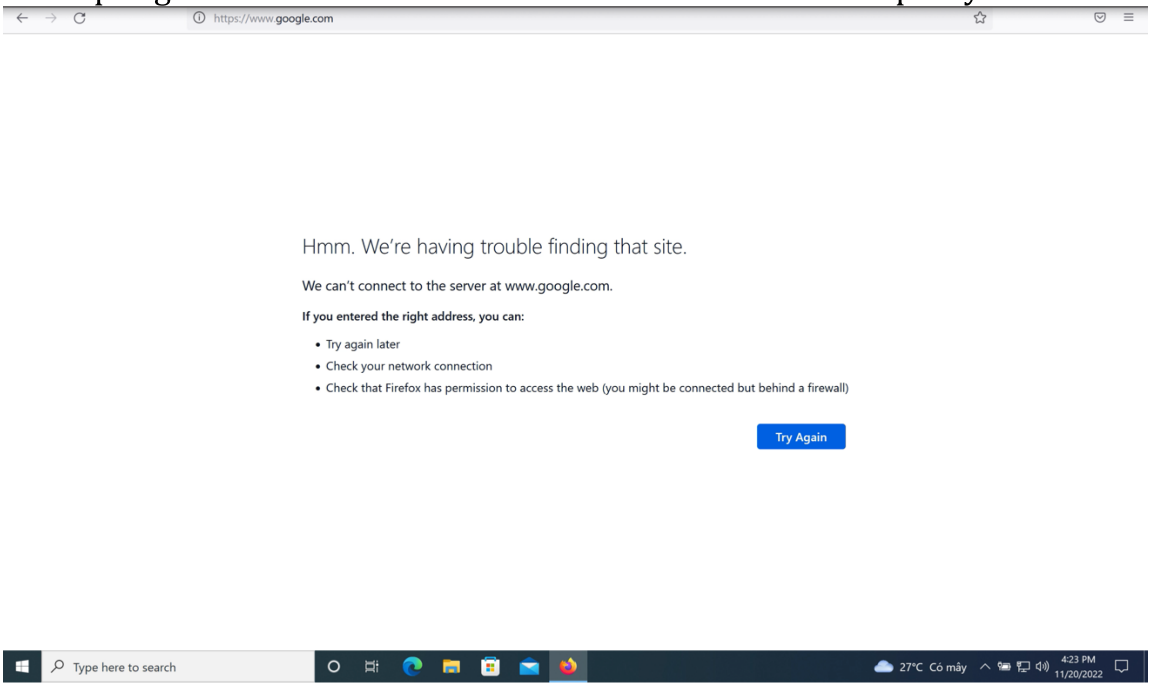
```
3: ens36: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group
 default qlen 1000
    link/ether 00:0c:29:97:25:e2 brd ff:ff:ff:ff:ff:ff
    inet 172.16.26.137/24 brd 172.16.26.255 scope global noprefixroute dynamic ens36
       valid_lft 1765sec preferred_lft 1765sec
    inet6 fe80::b2b4:100c:a0db:be1f/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

- ACL rule



```
acl group2net src 172.16.26.0/24
http_access allow group2net
```

- Attempting to use client VM to access the Internet without a proxy



https://www.google.com

Hmm. We're having trouble finding that site.

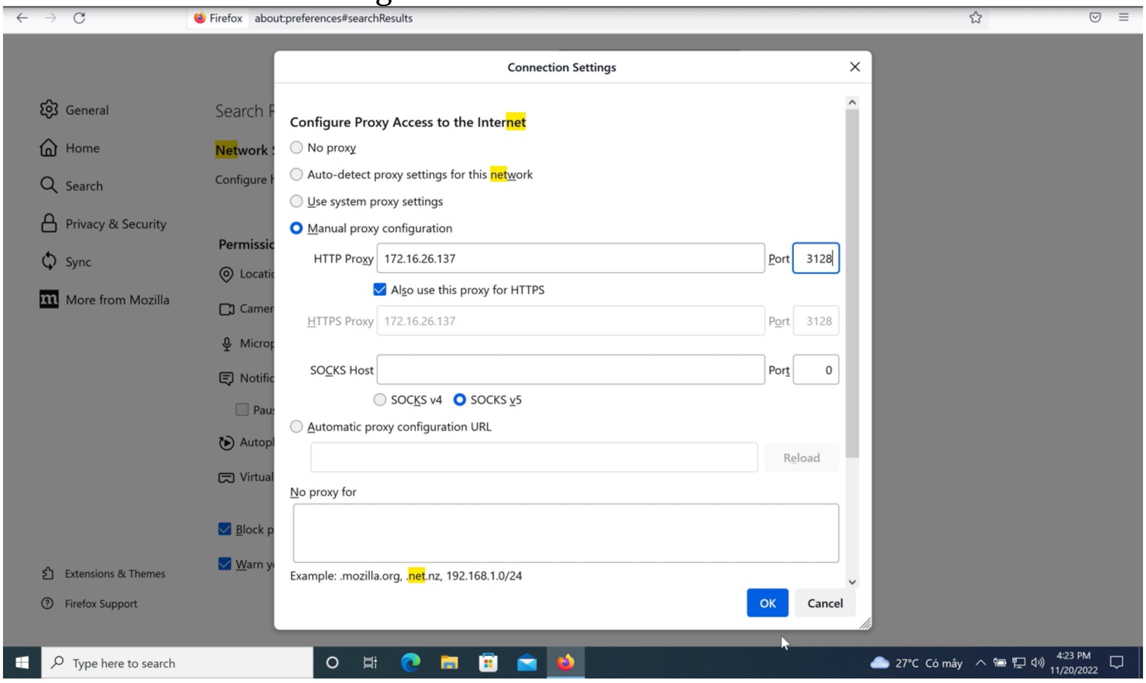
We can't connect to the server at www.google.com.

If you entered the right address, you can:

- Try again later
- Check your network connection
- Check that Firefox has permission to access the web (you might be connected but behind a firewall)

Because of the Host-only NIC, client machine cannot access to the Internet

- Then manually import Squid machine's IP and port to the client machine's Browser's Network Configuration



Configure Proxy Access to the Internet

○ No proxy
○ Auto-detect proxy settings for this network
○ Use system proxy settings
● Manual proxy configuration

HTTP Proxy 172.16.26.137 Port 3128

☑ Also use this proxy for HTTPS

HTTPS Proxy 172.16.26.137 Port 3128

SOCKS Host Port 0

○ SOCKS v4 ● SOCKS v5

○ Automatic proxy configuration URL

No proxy for

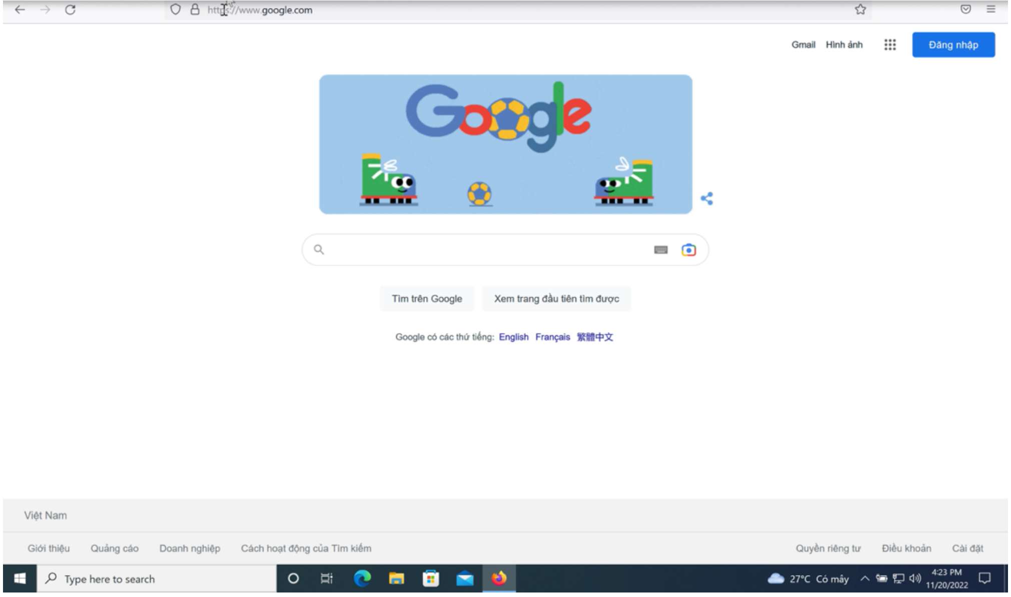
Example: .mozilla.org, .net.nz, 192.168.1.0/24

- Restart the squid service to execute the ACL rule

  ```
  [root@localhost squid]# systemctl restart squid
  [root@localhost squid]#
  ```

  This action need to be repeated every time when adding new rules

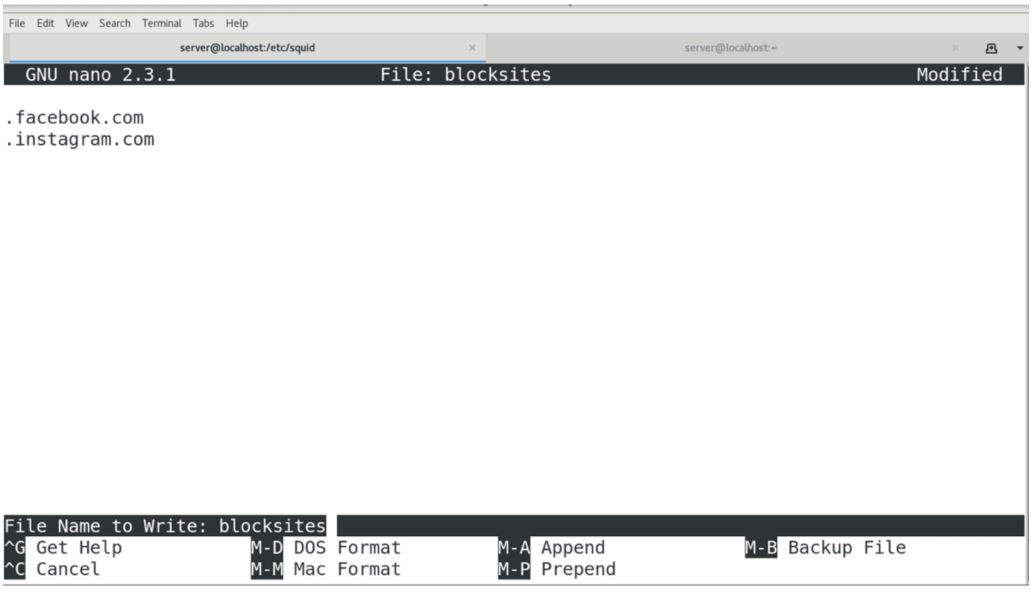
- Client machine after imported the proxy can connect to the Internet



- *Restrict client access to some websites*

```
#Block website-------------------------------
acl blocksites dstdomain "/etc/squid/blocksites"
http_access deny blocksites
```

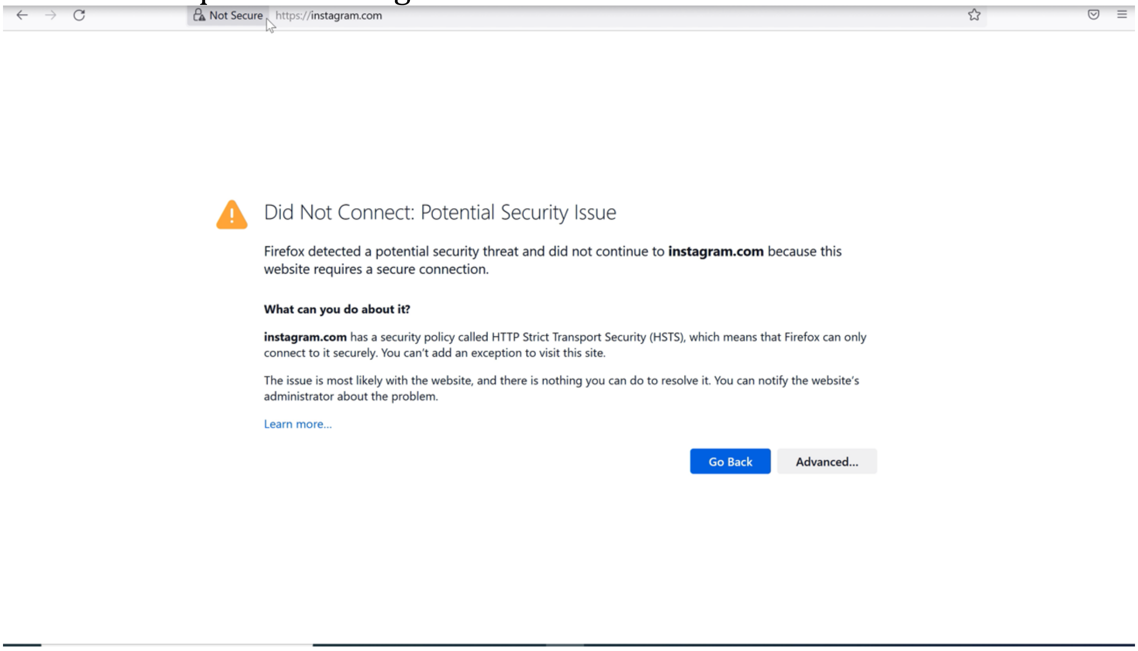
- dstdomain: destination (server) domain name
- "/etc/squid/blocksites": path of the text file that contains the websites want to block


File Edit View Search Terminal Tabs Help
server@localhost:/etc/squid
server@localhost:~

```
  GNU nano 2.3.1                 File: blocksites                       Modified

.facebook.com
.instagram.com

File Name to Write: blocksites
^G Get Help            M-D DOS Format         M-A Append             M-B Backup File
^C Cancel              M-M Mac Format         M-P Prepend
```

⇨ Deny all of the websites that exist in the text file

- Restart the squid service again and check the result



Not Secure https://instagram.com

Did Not Connect: Potential Security Issue

Firefox detected a potential security threat and did not continue to **instagram.com** because this website requires a secure connection.

What can you do about it?

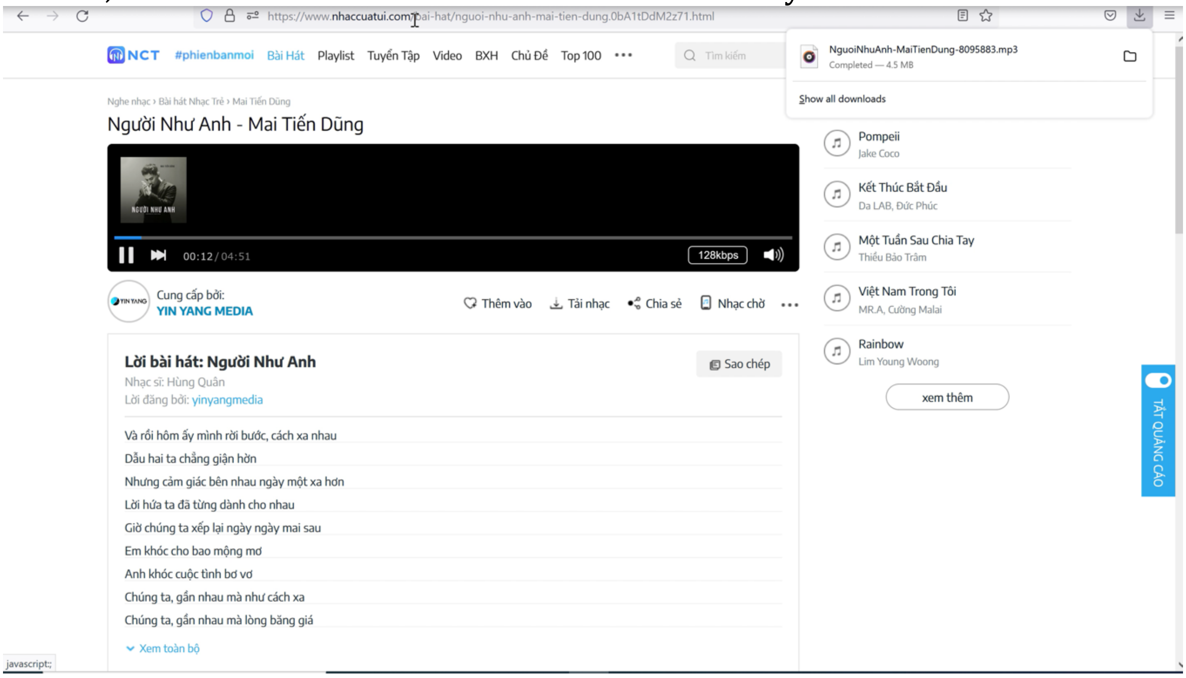
instagram.com has a security policy called HTTP Strict Transport Security (HSTS), which means that Firefox can only connect to it securely. You can't add an exception to visit this site.

The issue is most likely with the website, and there is nothing you can do to resolve it. You can notify the website's administrator about the problem.

Learn more…

- ***Restrict client download or view some kind of files (.mp3, .html, etc.)***

- At first, the client machine can download file normally



https://www.nhaccuatui.com/bai-hat/nguoi-nhu-anh-mai-tien-dung.0bA1tDdM2z71.html

NguoiNhuAnh-MaiTienDung-8095883.mp3
Completed — 4.5 MB

Show all downloads

Nghe nhạc › Bài hát Nhạc Trẻ › Mai Tiến Dũng

Người Như Anh - Mai Tiến Dũng

Pompeii
Jake Coco

Kết Thúc Bắt Đầu
Da LAB, Đức Phúc

Một Tuần Sau Chia Tay
Thiều Bảo Trâm

Việt Nam Trong Tôi
MR.A, Cường Malai

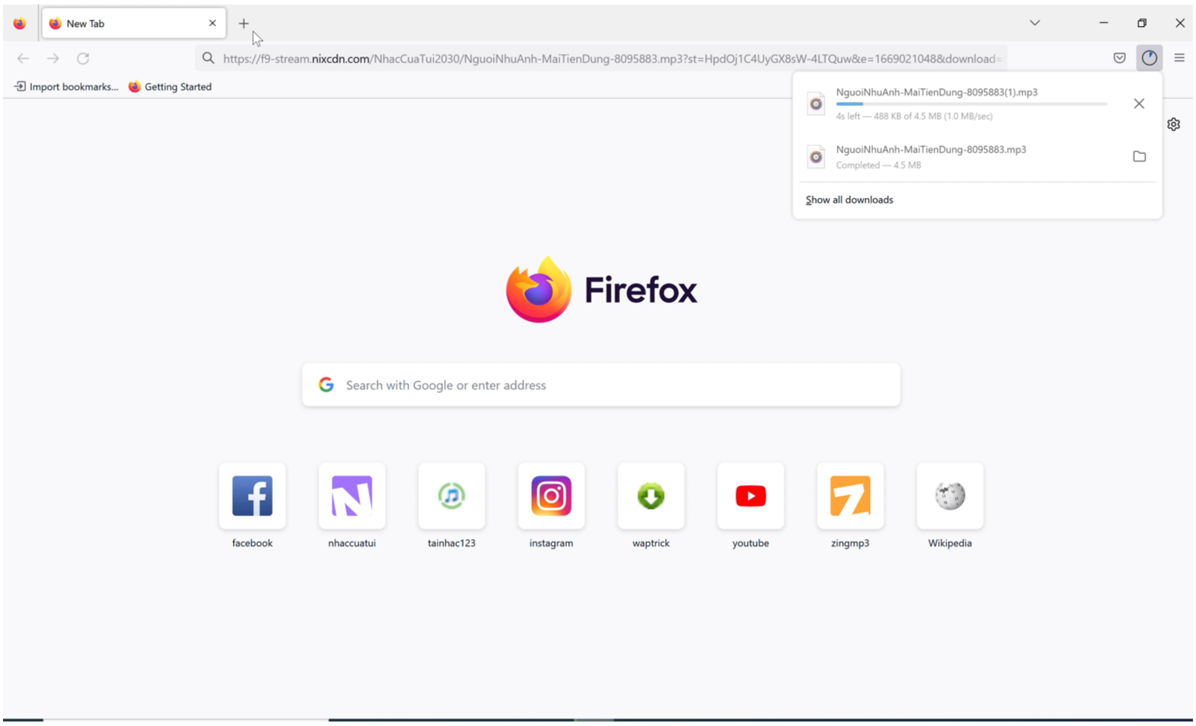
Rainbow
Lim Young Woong

Lời bài hát: Người Như Anh
Nhạc sĩ: Hùng Quân
Lời đăng bởi: yinyangmedia

Và rồi hôm ấy mình rời bước, cách xa nhau
Dẫu hai ta chẳng giận hờn
Nhưng cảm giác bên nhau ngày một xa hơn
Lời hứa ta đã từng dành cho nhau
Giờ chúng ta xếp lại ngày ngày mai sau
Em khóc cho bao mộng mơ
Anh khóc cuộc tình bơ vơ
Chúng ta, gần nhau mà như cách xa
Chúng ta, gần nhau mà lòng băng giá

Xem toàn bộ

- When clicking download, it will redirect client to another url to making download, and can see that, there was kind of extension file (.mp3) in the url path



New Tab

https://f9-stream.nixcdn.com/NhacCuaTui2030/NguoiNhuAnh-MaiTienDung-8095883.mp3?st=HpdOj1C4UyGX8sW-4LTQuw&e=1669021048&download=

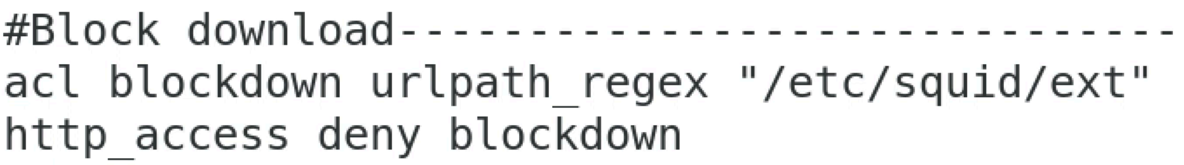
Import bookmarks... Getting Started

NguoiNhuAnh-MaiTienDung-8095883(1).mp3
4s left — 488 KB of 4.5 MB (1.0 MB/sec)

NguoiNhuAnh-MaiTienDung-8095883.mp3
Completed — 4.5 MB

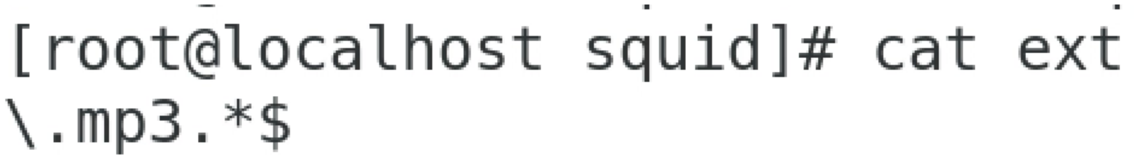
Show all downloads

⇨ **So the idea is to block the extension word in the path of download url**



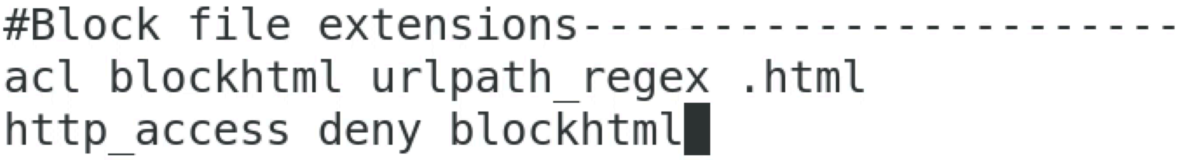
```
#Block download-----------------------------
acl blockdown urlpath_regex "/etc/squid/ext"
http_access deny blockdown
```

- urlpath_regex: url-path regular expression pattern matching, leaves out the protocol and hostname
- Text file that contains extension name want to block

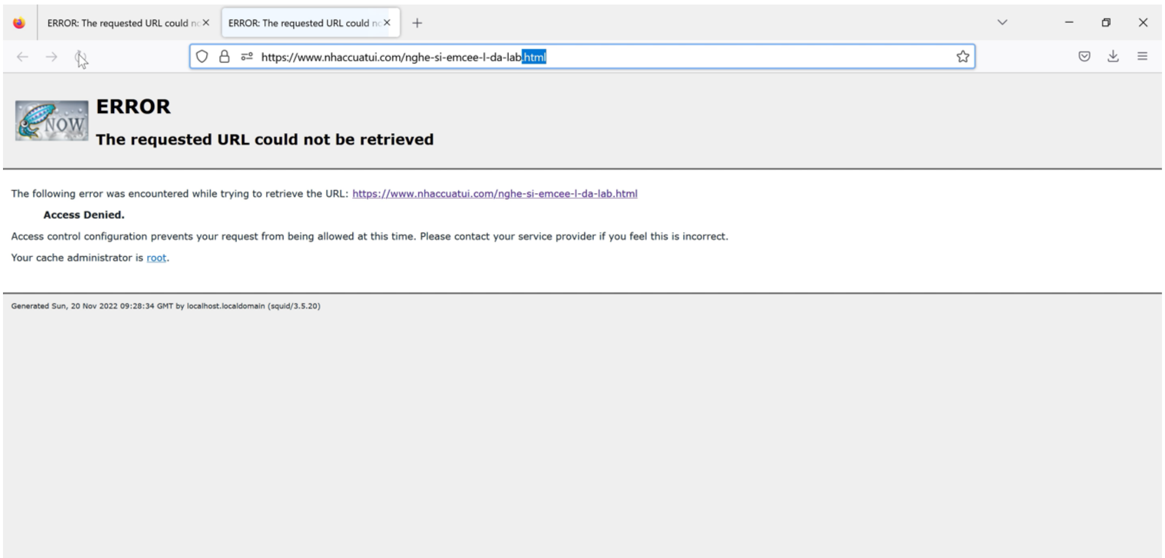


```
[root@localhost squid]# cat ext
\.mp3.*$
```

- Do the same steps to prevent client to view some kind of file (for example: .html)



```
#Block file extensions----------------------
acl blockhtml urlpath_regex .html
http_access deny blockhtml
```



ERROR: The requested URL could n ✕ | ERROR: The requested URL could n ✕

https://www.nhaccuatui.com/nghe-si-emcee-l-da-lab.html

ERROR

The requested URL could not be retrieved

The following error was encountered while trying to retrieve the URL: https://www.nhaccuatui.com/nghe-si-emcee-l-da-lab.html

Access Denied.

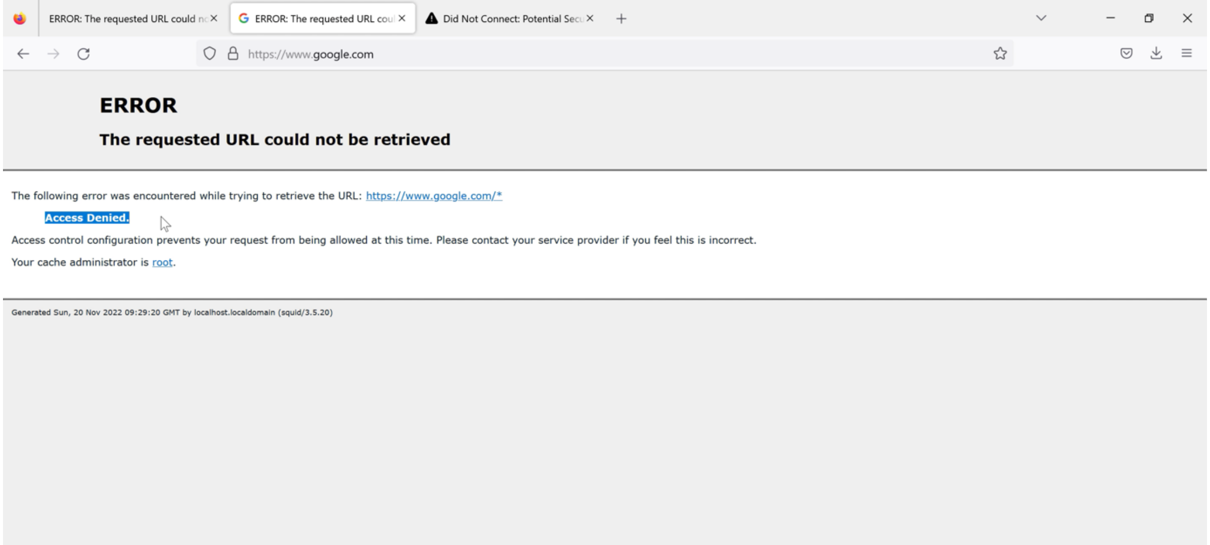
Access control configuration prevents your request from being allowed at this time. Please contact your service provider if you feel this is incorrect.

Your cache administrator is root.

Generated Sun, 20 Nov 2022 09:28:34 GMT by localhost.localdomain (squid/3.5.20)

- ***Limited work time for client***

```
#Limited Time----------------------------------
acl worktime time 00:00-23:59
http_access deny worktime
```



ERROR: The requested URL could n ✕ | ERROR: The requested URL cou ✕ | Did Not Connect: Potential Secu ✕

https://www.google.com

ERROR

The requested URL could not be retrieved

The following error was encountered while trying to retrieve the URL: https://www.google.com/*

Access Denied.

Access control configuration prevents your request from being allowed at this time. Please contact your service provider if you feel this is incorrect.

Your cache administrator is root.

Generated Sun, 20 Nov 2022 09:29:20 GMT by localhost.localdomain (squid/3.5.20)

⇨ We can create a limit for any time period, and also limit the days of the week

3.2. Advance

Use the IP of the Squid machine to act as a gateway on the client computer so that the client machine can connect to the Internet in order to make the Squid Proxy Server functioning as a router without importing IP for each and every browser.

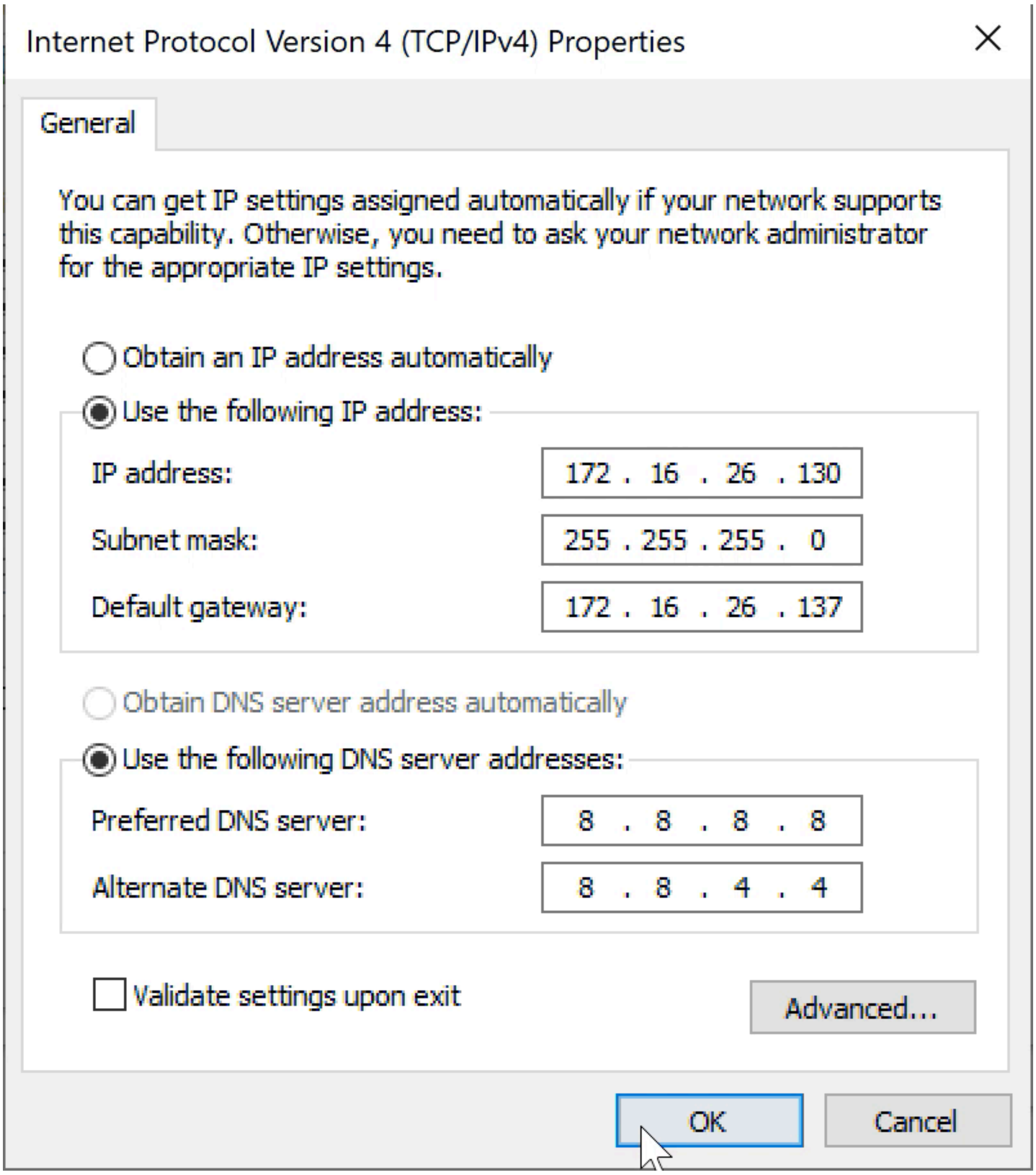
- First, enable IP forwarding on Squid machine

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

- Then configure the iptables with these commands

```
2. iptables configuration
        iptables -t nat -A PREROUTING -i [LAN int] -p tcp --dport 80 -j DNAT --to [WAN IP]:3128
        iptables -t nat -A PREROUTING -i [WAN int] -p tcp --dport 80 -j REDIRECT --to-port 3128
```

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



Internet Protocol Version 4 (TCP/IPv4) Properties

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 172 . 16 . 26 . 130

Subnet mask: 255 . 255 . 255 . 0

Default gateway: 172 . 16 . 26 . 137

○ Obtain DNS server address automatically

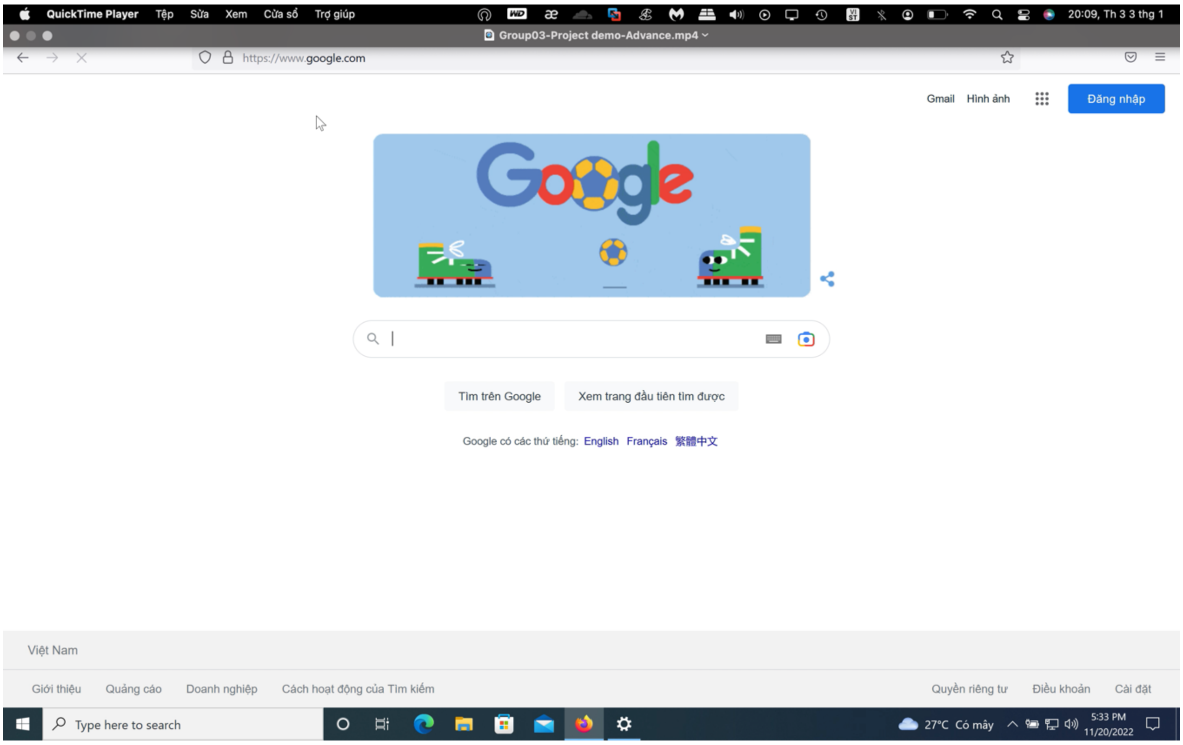
● Use the following DNS server addresses:

Preferred DNS server: 8 . 8 . 8 . 8

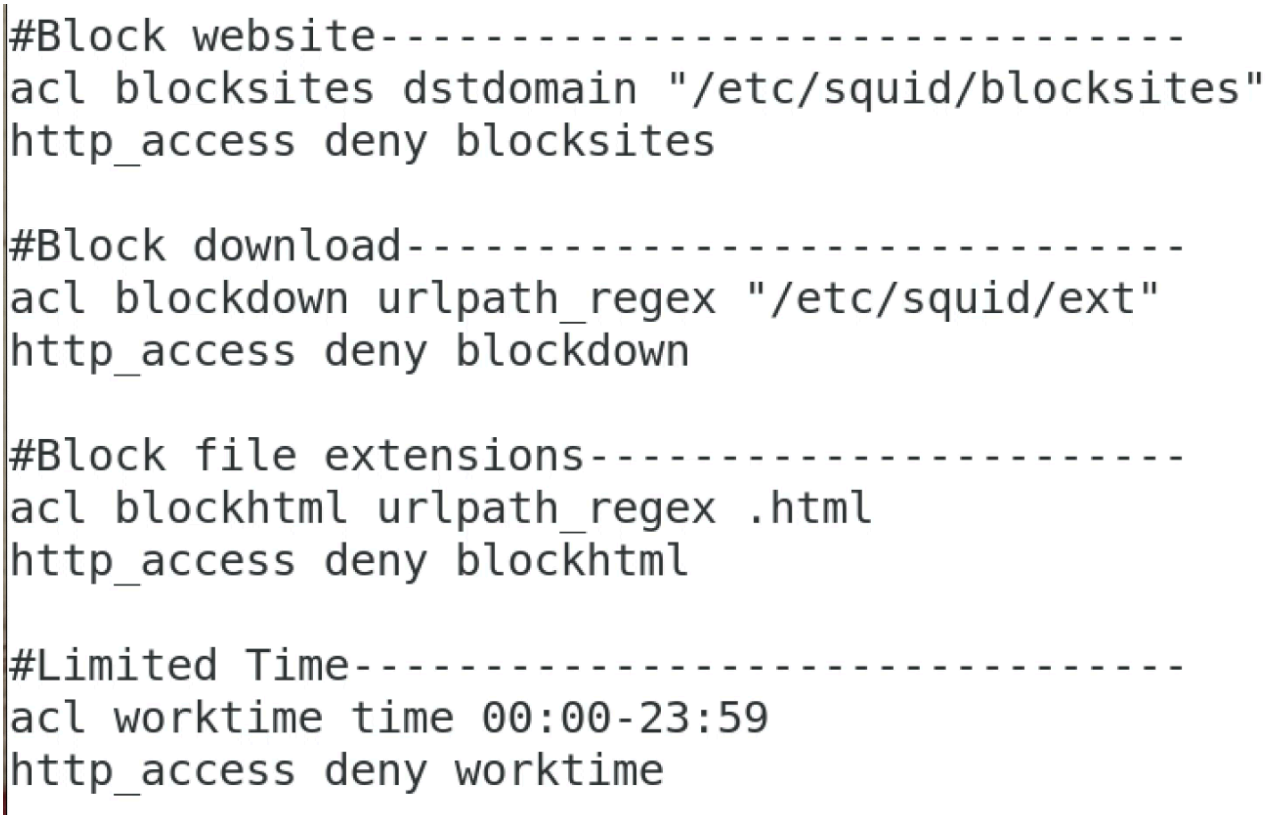
Alternate DNS server: 8 . 8 . 4 . 4

□ Validate settings upon exit

- Result:



- ACL lists


```
#Block website-----------------------------------
acl blocksites dstdomain "/etc/squid/blocksites"
http_access deny blocksites

#Block download----------------------------------
acl blockdown urlpath_regex "/etc/squid/ext"
http_access deny blockdown

#Block file extensions---------------------------
acl blockhtml urlpath_regex .html
http_access deny blockhtml

#Limited Time------------------------------------
acl worktime time 00:00-23:59
http_access deny worktime
```

IV. Work assignments and evaluations

4.1. Work assignments

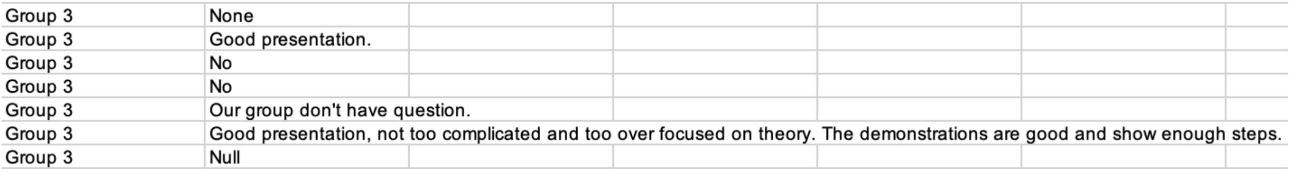
Member	Task	Complete (%)
Nguyen Tran Anh Quan	Building environment, performing requirements from basic to advanced	100
Truong Tuan Phi	Learning theories and offer solutions	100
Nguyen Duc Toan	Designing slides	80

4.2. Self-assessment

	4	3	2	1
Report	√			
Presentation		√		
Theory	√			
Demonstration	√			

⇨ Self-assessment total score: 8.75

4.3. Question



Group 3	None
Group 3	Good presentation.
Group 3	No
Group 3	No
Group 3	Our group don't have question.
Group 3	Good presentation, not too complicated and too over focused on theory. The demonstrations are good and show enough steps.
Group 3	Null