

SQUID PROXY

NT132.ANTT.011
GROUP 12



SQUID PROXY

01

01 Giới thiệu

03 Triển khai hệ thống

02 Squid Proxy Server

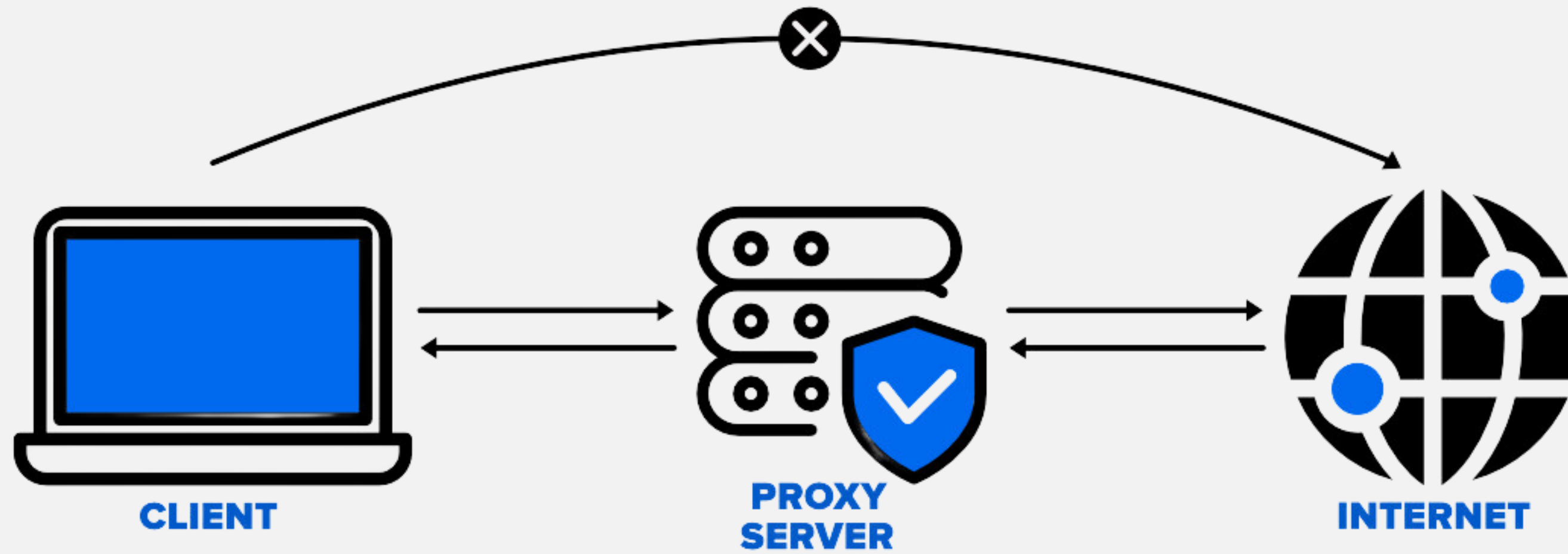
04 Thực nghiệm và Đánh giá

05 Kết luận

01

Giới thiệu

02



Proxy Server hoạt động như một cổng nối giữa người dùng và Internet. Đây là một server trung gian giữa người dùng cuối và trang web họ truy cập.

- **Proxy Forward** thường được sử dụng để tăng tốc độ truy cập và giảm tải cho máy chủ đích.
- **Proxy Reverse** thường được sử dụng để cân bằng tải và bảo mật máy chủ.
- **Proxy Transparent** thường được sử dụng để kiểm soát và giám sát lưu lượng mạng.
- **Proxy Anonymous** thường được sử dụng để bảo vệ quyền riêng tư và truy cập vào các trang web bị chặn.
- **Proxy High Anonymity** thường được sử dụng trong các hoạt động truy cập web ẩn danh và bảo mật.



02

Squid Proxy Server



Squid là phần mềm proxy cache server cung cấp dịch vụ proxy và cache qua các giao thức như **HTTP, FTP** và các giao thức mạng phổ biến. Nó hoạt động như một trung gian giữa các máy chủ web và máy khách

Squid proxy server lưu trữ web client, FTP, Gopher và HTTP. Squid lưu trữ thông tin mới nhất của các dịch vụ trong RAM, quản lý một cơ sở dữ liệu lớn của các thông tin trên đĩa, có một kỹ thuật điều khiển truy cập phức tạp, hỗ trợ giao thức SSL cho các kết nối bảo mật thông qua proxy. Hơn nữa, Squid có thể liên kết với các cache của các proxy server khác trong việc sắp xếp lưu trữ các trang web một cách hợp lý.



Squid Proxy

**Content
filtering**

Áp dụng bộ lọc nội dung để ghi lại, chặn thậm chí điều chỉnh gói tin

Dựa trên các từ khóa, danh sách đen (**blacklist**), danh sách trắng (**whitelist**), danh sách đen chặn (blocklist), danh sách đáng ngờ (**suspicious list**) và các quy tắc tùy chỉnh khác.

Caching

Lưu cache (bộ nhớ đệm) các tài nguyên được yêu cầu từ máy chủ mục tiêu

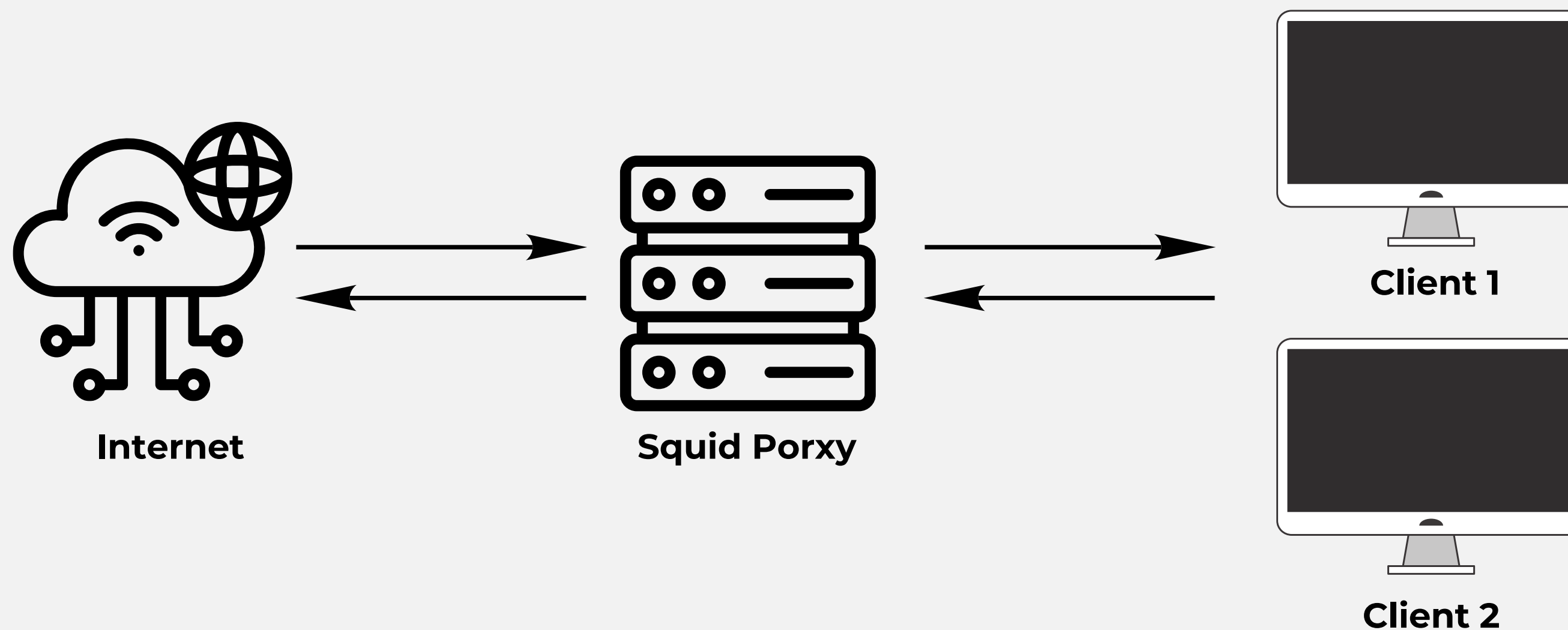
Giúp tăng tốc độ truy cập và giảm tải cho máy chủ mục tiêu, đồng thời giảm lưu lượng mạng và tiết kiệm băng thông.

Chuyển tiếp (forwarding), **kiểm soát truy cập** (Access control), **xác thực** (authentication), **tối ưu hoá lưu lượng truy cập** (Traffic Optimization),...

- Sử dụng ít băng thông hơn trên kết nối Internet của bạn khi lướt Web
- Giảm lượng thời gian tải trang web
- Bảo vệ các máy tính trong mạng nội bộ của bạn bằng cách kiểm soát lưu lượng truy cập web của chúng
- Thu thập số liệu thống kê về lưu lượng truy cập web trên mạng của bạn
- Ngăn người dùng truy cập các trang web không phù hợp tại cơ quan hoặc trường học
- Giảm tải cho (các) máy chủ web của riêng bạn

03

Triển khai hệ thống



Mô hình triển khai

- Hệ điều hành: Ubuntu 22.04.06
 - 1 máy - Squid Proxy
 - 2 máy - Client

Tên	Địa chỉ IP	Subnet mask	Địa chỉ IP của Proxy
Squid Proxy	192.168.37.139	255.255.255.0	
Client 1	192.168.37.128	255.255.255.0	192.168.37.139
Client 2	192.168.37.138	255.255.255.0	192.168.37.139

Bước 1: Cập nhật các packages:

- **\$ sudo apt update**

Bước 2: Cài đặt Squid thông qua lệnh sau:

- **\$ sudo apt install squid**

Bước 3: Khởi động dịch vụ Squid proxy trên hệ thống và cho phép Squid proxy tự động khởi động cùng với hệ thống

- **\$ sudo systemctl start squid**
- **\$ sudo systemctl enable squid**

Bước 4: Xác minh trạng thái của Squid proxy trên hệ thống:

- **\$ sudo systemctl status squid**

Bước 5: Cấu hình Squid proxy để hoạt động theo các chức năng mong muốn trong file cấu hình của Squid proxy (squid.conf):

- **\$ sudo vim /etc/squid/squid.conf**

Connection Settings

Configure Proxy Access to the Internet

☐ No proxy

☐ Auto-detect proxy settings for this network

☐ Use system proxy settings

☒ Manual proxy configuration

HTTP Proxy

192.168.37.139

Port

3128

☒ Also use this proxy for HTTPS

HTTPS Proxy

192.168.37.139

Port

3128

SOCKS Host

Port

0

☐ SOCKS v4

☒ SOCKS v5

☐ Automatic proxy configuration URL

Reload

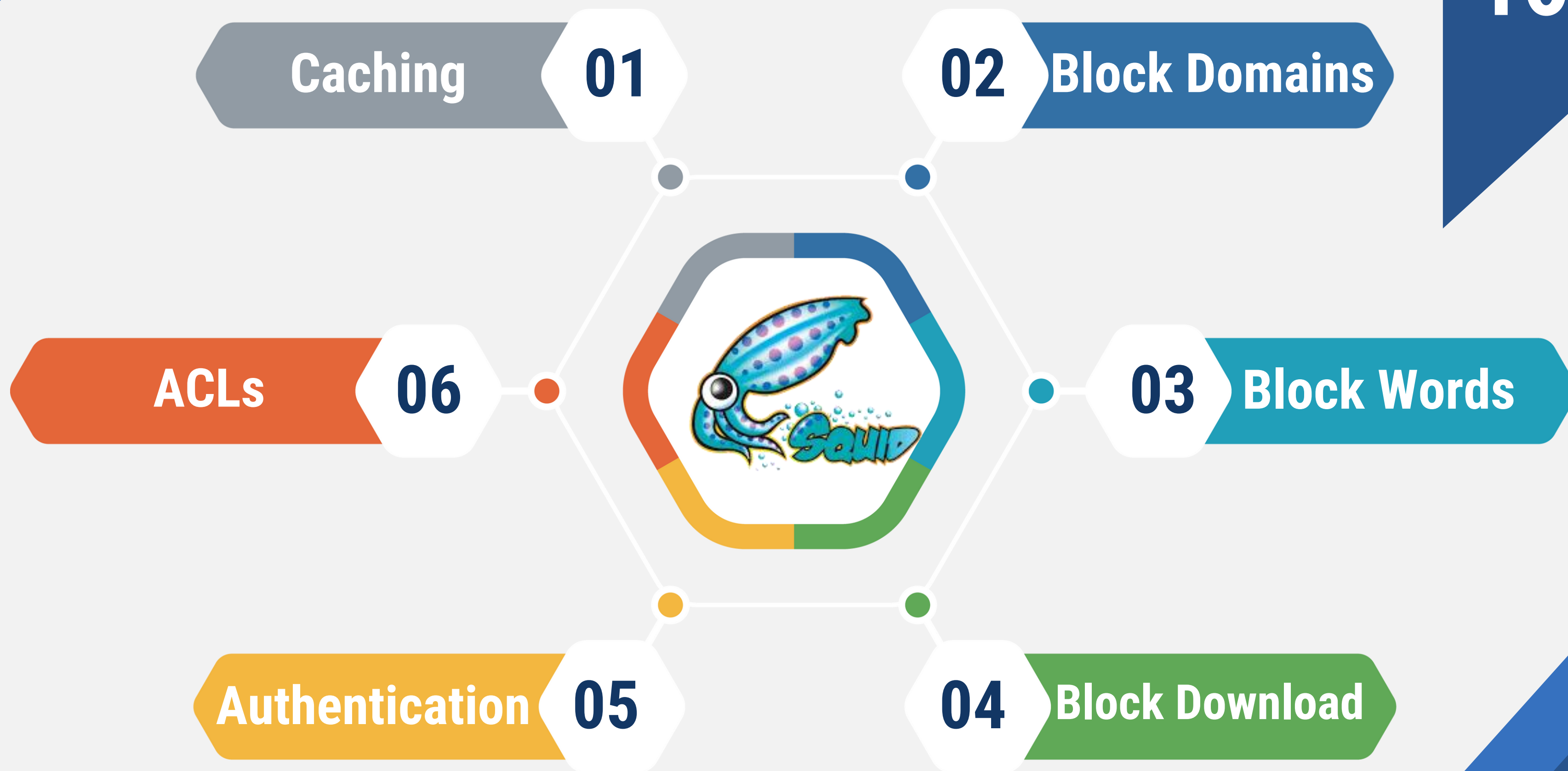
No proxy for

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

Connections to localhost, 127.0.0.1/8, and ::1 are never proxied.

04

Thực nghiệm và Đánh giá



Bước 1: : Cấu hình Squid Proxy để thực hiện chức năng trên

```
cache_dir ufs /var/spool/squid 100 16 256
```

```
squidproxy@squidproxy-virtual-machine: /etc/squid$ grep -vE '^$|^#' /etc/squid/squid.conf
acl localnet src 0.0.0.1-0.255.255.255 # RFC 1122 "this" network (LAN)
acl localnet src 10.0.0.0/8 # RFC 1918 local private network (LAN)
acl localnet src 100.64.0.0/10 # RFC 6598 shared address space (CGN)
acl localnet src 169.254.0.0/16 # RFC 3927 link-local (directly plugged) machines
acl localnet src 172.16.0.0/12 # RFC 1918 local private network (LAN)
acl localnet src 192.168.0.0/16 # RFC 1918 local private network (LAN)
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
http_access deny !Safe_ports
http_access deny CONNECT !SSL_ports
http_access allow localhost manager
http_access deny manager
include /etc/squid/conf.d/*.conf
http_access allow localhost
acl client2 src 192.168.37.0/24
http_access allow client2
http_access deny all
http_port 192.168.37.139:3128
http_port 3128
cache_dir ufs /var/spool/squid 100 16 256
coredump_dir /var/spool/squid
```


Bước 2: Vào máy Client2 để kiểm tra hoạt động của Squid Proxy bằng cách sử dụng câu lệnh sau

```
curl -x http://192.168.37.139:3128 -I http://duckduckgo.com
```

Lần **đầu tiên** truy cập vào Website

```
client2@client2-virtual-machine:~$ curl -x http://192.168.37.139:3128 -I -L http://duckduckgo.com
HTTP/1.1 301 Moved Permanently
Server: nginx
Date: Wed, 29 Nov 2023 14:16:46 GMT
Content-Type: text/html
Content-Length: 162
Location: https://duckduckgo.com/
Permissions-Policy: interest-cohort=()
Content-Security-Policy: default-src 'none' ; connect-src https://duckduckgo.com https://*.duckduckgo.com https://duckduckgogg42xjoc72x3sjasowarfbgcmvfimaftt6twagswzczad.onion/ https://spreadprivacy.com ; manifest-src https://duckduckgo.com https://*.duckduckgo.com https://duckduckgogg42xjoc72x3sjasowarfbgcmvfimaftt6twagswzczad.onion/ https://spreadprivacy.com ; media-src https://duckduckgo.com https://*.duckduckgo.com https://duckduckgogg42xjoc72x3sjasowarfbgcmvfimaftt6twagswzczad.onion/ https://spreadprivacy.com ; script-src blob: https://duckduckgo.com https://*.duckduckgo.com https://duckduckgogg42xjoc72x3sjasowarfbgcmvfimaftt6twagswzczad.onion/ https://spreadprivacy.com 'unsafe-inline' 'unsafe-eval' ; font-src data: https://duckduckgo.com https://*.duckduckgo.com https://duckduckgogg42xjoc72x3sjasowarfbgcmvfimaftt6twagswzczad.onion/ https://spreadprivacy.com ; img-src data: https://duckduckgo.com https://*.duckduckgo.com https://duckduckgogg42xjoc72x3sjasowarfbgcmvfimaftt6twagswzczad.onion/ https://spreadprivacy.com ; style-src https://duckduckgo.com https://*.duckduckgo.com https://duckduckgogg42xjoc72x3sjasowarfbgcmvfimaftt6twagswzczad.onion/ https://spreadprivacy.com 'unsafe-inline' ; object-src 'none' ; worker-src blob: ; child-src blob: https://duckduckgo.com https://*.duckduckgo.com https://duckduckgogg42xjoc72x3sjasowarfbgcmvfimaftt6twagswzczad.onion/ https://spreadprivacy.com ; frame-src blob: https://duckduckgo.com https://*.duckduckgo.com https://duckduckgogg42xjoc72x3sjasowarfbgcmvfimaftt6twagswzczad.onion/ https://spreadprivacy.com ; form-action https://duckduckgo.com https://*.duckduckgo.com https://duckduckgogg42xjoc72x3sjasowarfbgcmvfimaftt6twagswzczad.onion/ https://spreadprivacy.com ; frame-ancestors 'self' ; base-uri 'self' ; block-all-mixed-content ;
X-Frame-Options: SAMEORIGIN
X-XSS-Protection: 1;mode=block
X-Content-Type-Options: nosniff
Referrer-Policy: origin
Expect-CT: max-age=0
Expires: Thu, 28 Nov 2024 14:16:46 GMT
Cache-Control: max-age=31536000
X-Cache: MISS from squidproxy-virtual-machine
X-Cache-Lookup: MISS from squidproxy-virtual-machine:3128
Via: 1.1 squidproxy-virtual-machine (squid/5.7)
Connection: keep-alive
```


Bước 2: Vào máy Client2 để kiểm tra hoạt động của Squid Proxy bằng cách sử dụng câu lệnh sau

```
curl -x http://192.168.37.139:3128 -I http://duckduckgo.com
```

Lần **thứ hai** truy cập vào Website

```
client2@client2-virtual-machine:~$ curl -x http://192.168.37.139:3128 -I -L http://duckduckgo.com
HTTP/1.1 301 Moved Permanently
Server: nginx
Date: Wed, 29 Nov 2023 14:16:46 GMT
Content-Type: text/html
Content-Length: 162
Location: https://duckduckgo.com/
Permissions-Policy: interest-cohort=()
Content-Security-Policy: default-src 'none' ; connect-src https://duckduckgo.com https://*.duckduckgo.com https://duckduckgogg42xjoc72x3sjasowarfbgcmvfimaftt6twagswzczad.onion/ https://spreadprivacy.com ; manifest-src https://duckduckgo.com https://*.duckduckgo.com https://duckduckgogg42xjoc72x3sjasowarfbgcmvfimaftt6twagswzczad.onion/ https://spreadprivacy.com ; media-src https://duckduckgo.com https://*.duckduckgo.com https://duckduckgogg42xjoc72x3sjasowarfbgcmvfimaftt6twagswzczad.onion/ https://spreadprivacy.com ; script-src blob: https://duckduckgo.com https://*.duckduckgo.com https://duckduckgogg42xjoc72x3sjasowarfbgcmvfimaftt6twagswzczad.onion/ https://spreadprivacy.com 'unsafe-inline' 'unsafe-eval' ; font-src data: https://duckduckgo.com https://*.duckduckgo.com https://duckduckgogg42xjoc72x3sjasowarfbgcmvfimaftt6twagswzczad.onion/ https://spreadprivacy.com ; img-src data: https://duckduckgo.com https://*.duckduckgo.com https://duckduckgogg42xjoc72x3sjasowarfbgcmvfimaftt6twagswzczad.onion/ https://spreadprivacy.com ; style-src https://duckduckgo.com https://*.duckduckgo.com https://duckduckgogg42xjoc72x3sjasowarfbgcmvfimaftt6twagswzczad.onion/ https://spreadprivacy.com 'unsafe-inline' ; object-src 'none' ; worker-src blob: ; child-src blob: https://duckduckgo.com https://*.duckduckgo.com https://duckduckgogg42xjoc72x3sjasowarfbgcmvfimaftt6twagswzczad.onion/ https://spreadprivacy.com ; frame-src blob: https://duckduckgo.com https://*.duckduckgo.com https://duckduckgogg42xjoc72x3sjasowarfbgcmvfimaftt6twagswzczad.onion/ https://spreadprivacy.com ; form-action https://duckduckgo.com https://*.duckduckgo.com https://duckduckgogg42xjoc72x3sjasowarfbgcmvfimaftt6twagswzczad.onion/ https://spreadprivacy.com ; frame-ancestors 'self' ; base-uri 'self' ; block-all-mixed-content ;
X-Frame-Options: SAMEORIGIN
X-XSS-Protection: 1;mode=block
X-Content-Type-Options: nosniff
Referrer-Policy: origin
Expect-CT: max-age=0
Expires: Thu, 28 Nov 2024 14:16:46 GMT
Cache-Control: max-age=31536000
Age: 143
X-Cache: HIT from squidproxy-virtual-machine
X-Cache-Lookup: HIT from squidproxy-virtual-machine:3128
Via: 1.1 squidproxy-virtual-machine (squid/5.7)
Connection: keep-alive
```


04 Triển khai thực nghiệm | Tính năng Block Domain Content Filtering

21

Bước 1: Cấu hình Squid Proxy để thực hiện chức năng trên

```
acl blocked_websites dstdomain .youtube.com .facebook.com .twitter.com .reddit.com
http_access deny blocked_websites
```

```
squidproxy@squidproxy-virtual-machine: /etc/squid$ grep -vE '^$|^#' /etc/squid/squid.conf
acl localnet src 0.0.0.1-0.255.255.255 # RFC 1122 "this" network (LAN)
acl localnet src 10.0.0.0/8 # RFC 1918 local private network (LAN)
acl localnet src 100.64.0.0/10 # RFC 6598 shared address space (CGN)
acl localnet src 169.254.0.0/16 # RFC 3927 link-local (directly plugged) machines
acl localnet src 172.16.0.0/12 # RFC 1918 local private network (LAN)
acl localnet src 192.168.0.0/16 # RFC 1918 local private network (LAN)
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
http_access deny !Safe_ports
http_access deny CONNECT !SSL_ports
http_access allow localhost manager
http_access deny manager
include /etc/squid/conf.d/*.conf
http_access allow localhost
acl client2 src 192.168.37.0/24
http_access allow client2
http_access deny all
http_port 192.168.37.139:3128
http_port 3128
cache_dir ufs /var/spool/squid 100 16 256
coredump_dir /var/spool/squid
```

04 Triển khai thực nghiệm | Tính năng Block Domain Content Filtering

22

Bước 2: Vào máy Client2 để kiểm tra hoạt động của Squid Proxy bằng cách 2 cách:

•Cách 1: Sử dụng câu lệnh trên terminal

```
curl -x http://192.168.37.139:3128 -I http://youtube.com
```

```
curl -x http://192.168.37.139:3128 -I http://facebook.com
```

```
client2@client2-virtual-machine:~$ curl -x http://192.168.37.139:3128 -I -L http://youtube.com
HTTP/1.1 403 Forbidden
Server: squid/5.7
Mime-Version: 1.0
Date: Wed, 29 Nov 2023 14:28:41 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 3539
X-Squid-Error: ERR_ACCESS_DENIED 0
Vary: Accept-Language
Content-Language: en
X-Cache: MISS from squidproxy-virtual-machine
X-Cache-Lookup: NONE from squidproxy-virtual-machine:3128
Via: 1.1 squidproxy-virtual-machine (squid/5.7)
Connection: keep-alive

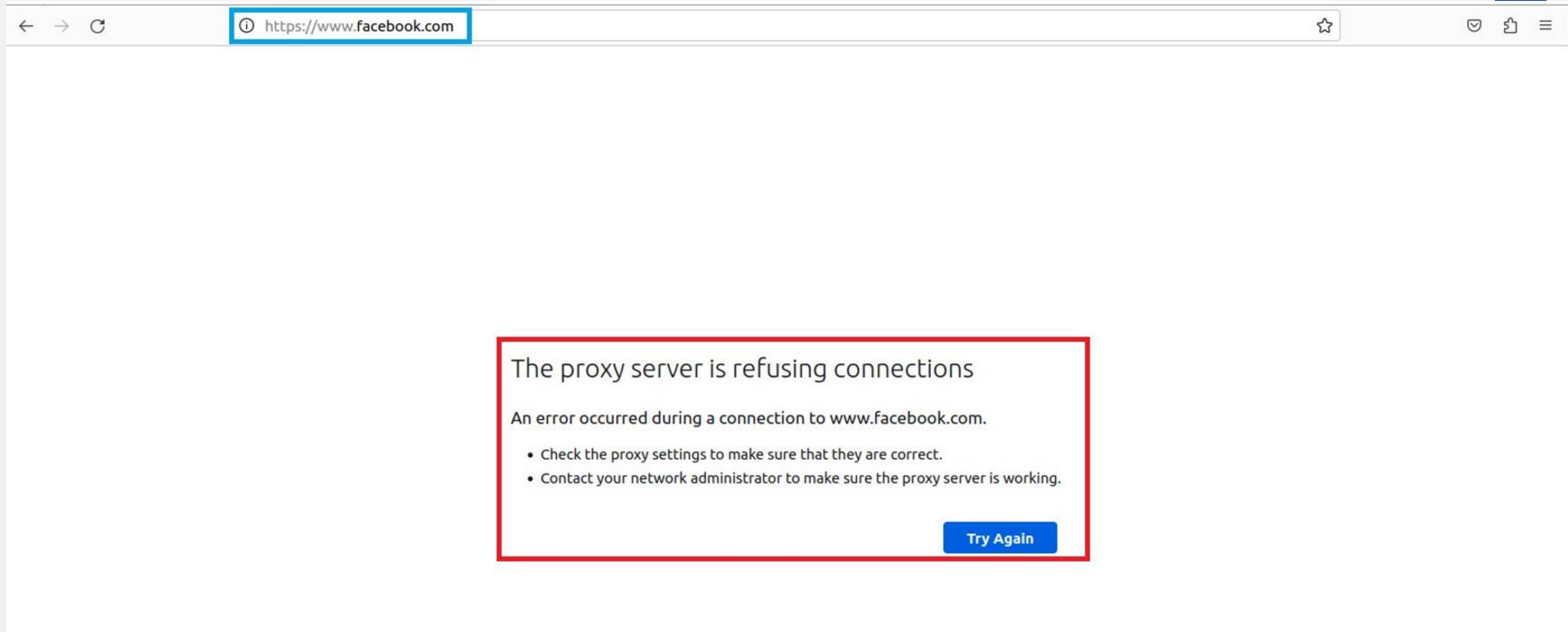
client2@client2-virtual-machine:~$ curl -x http://192.168.37.139:3128 -I -L http://facebook.com
HTTP/1.1 403 Forbidden
Server: squid/5.7
Mime-Version: 1.0
Date: Wed, 29 Nov 2023 14:28:51 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 3542
X-Squid-Error: ERR_ACCESS_DENIED 0
Vary: Accept-Language
Content-Language: en
X-Cache: MISS from squidproxy-virtual-machine
X-Cache-Lookup: NONE from squidproxy-virtual-machine:3128
Via: 1.1 squidproxy-virtual-machine (squid/5.7)
Connection: keep-alive
```


04 Triển khai thực nghiệm | Tính năng Block Domain Content Filtering

23

Bước 2: Vào máy Client2 để kiểm tra hoạt động của Squid Proxy bằng cách 2 cách:

• **Cách 2: Sử dụng trình duyệt Firefox để truy cập các trang web trong danh sách block**





Bước 1: Tạo tập tin **blacklist.txt** gồm những từ sẽ bị cấm truy cập vào

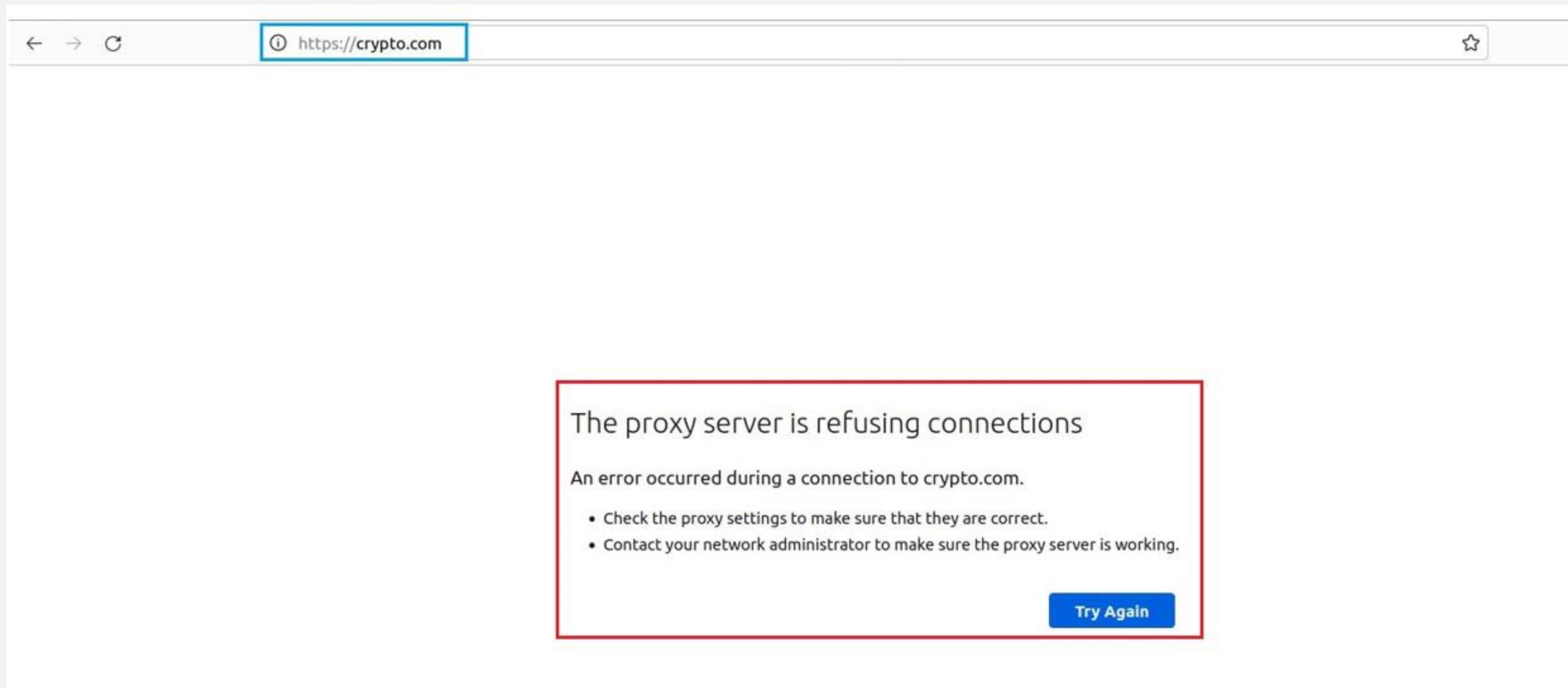
```
squidproxy@squidproxy-virtual-machine: ~  
GNU nano 6.2 /etc/squid/blacklist.txt *  
gambling  
drugs  
violence  
hacking  
torrent  
social-media  
gaming  
phishing  
malware  
war  
crypto  
youtube  
spotify  
facebook  
binance
```

Bước 2: Cấu hình Squid Proxy để thực hiện chức năng trên

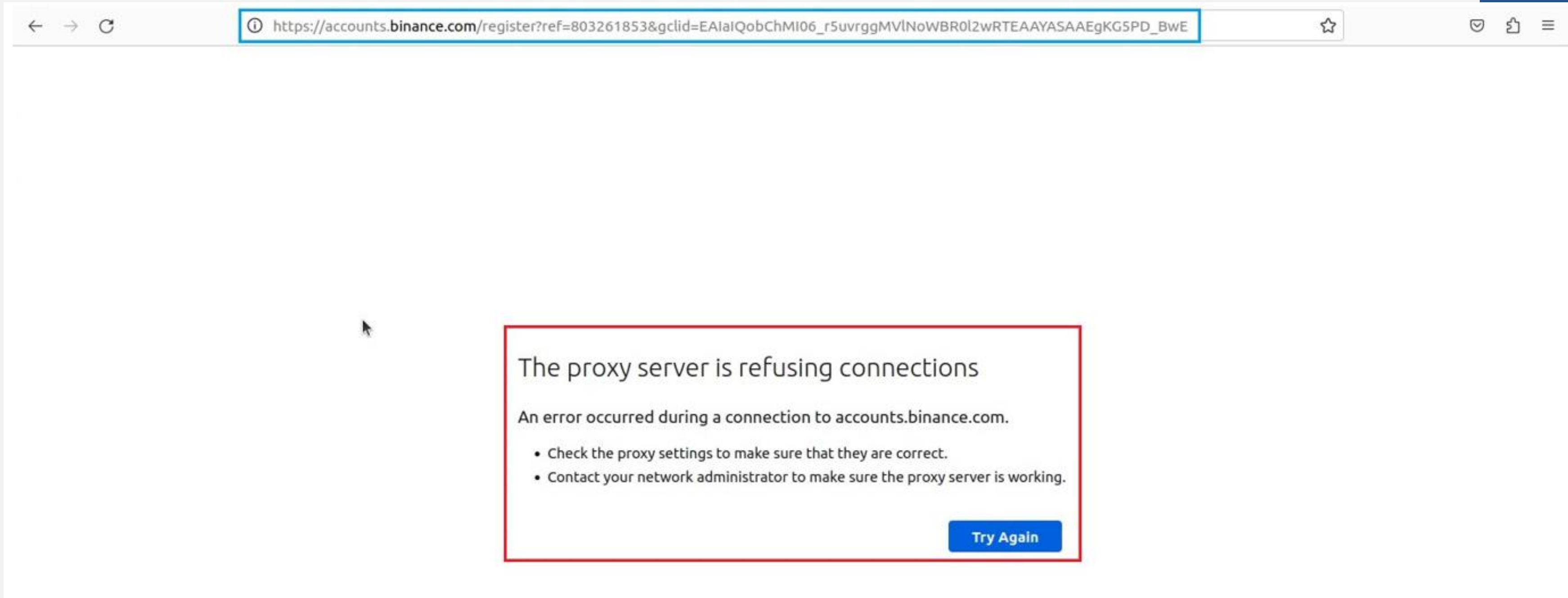
```
acl blacklist url_regex -i "/etc/squid/blacklist.txt"  
http_access deny blacklist
```

```
squidproxy@squidproxy-virtual-machine:~$ grep -vE '^$|^#' /etc/squid/squid.conf  
acl localnet src 0.0.0.1-0.255.255.255 # RFC 1122 "this" network (LAN)  
acl localnet src 10.0.0.0/8 # RFC 1918 local private network (LAN)  
acl localnet src 100.64.0.0/10 # RFC 6598 shared address space (CGN)  
acl localnet src 169.254.0.0/16 # RFC 3927 link-local (directly plugged) machines  
acl localnet src 172.16.0.0/12 # RFC 1918 local private network (LAN)  
acl localnet src 192.168.0.0/16 # RFC 1918 local private network (LAN)  
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  
http_access deny !Safe_ports  
http_access deny CONNECT !SSL_ports  
http_access allow localhost manager  
http_access deny manager  
include /etc/squid/conf.d/*.conf  
acl blacklist url_regex -i "/etc/squid/blacklist.txt"  
http_access deny blacklist  
http_access allow localhost  
acl client2 src 192.168.37.0/24
```


Bước 3: Vào máy Client2 để kiểm tra hoạt động của Squid Proxy



Bước 3: Vào máy Client2 để kiểm tra hoạt động của Squid Proxy





Triển khai thực nghiệm | Tính năng Block Download Content Filtering

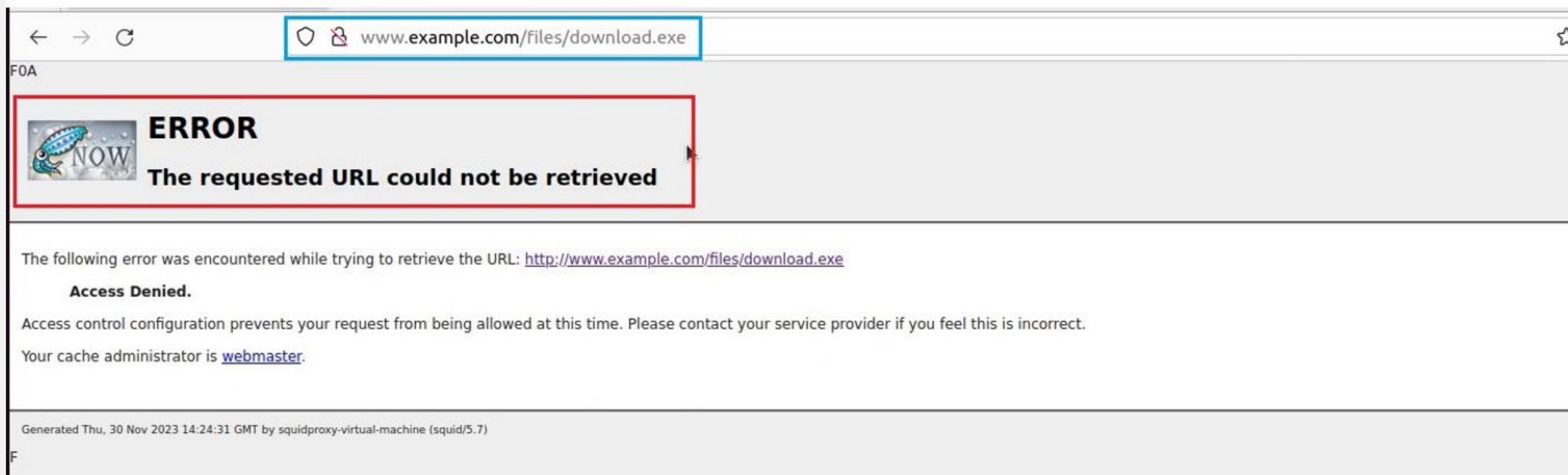
Bước 1: Cấu hình Squid Proxy để thực hiện chức năng trên (không chặn file **.mp3**)

```
acl block_extensions urlpath_regex -I \.exe$ \.zip$ \.rar$ \.tar$ \.gz$ \.iso$ \.mp4$  
http_access deny block_extensions
```

```
squidproxy@squidproxy-virtual-machine:~$ grep -vE '^$|^#' /etc/squid/squid.conf  
acl localnet src 0.0.0.1-0.255.255.255 # RFC 1122 "this" network (LAN)  
acl localnet src 10.0.0.0/8 # RFC 1918 local private network (LAN)  
acl localnet src 100.64.0.0/10 # RFC 6598 shared address space (CGN)  
acl localnet src 169.254.0.0/16 # RFC 3927 link-local (directly plugged) machines  
acl localnet src 172.16.0.0/12 # RFC 1918 local private network (LAN)  
acl localnet src 192.168.0.0/16 # RFC 1918 local private network (LAN)  
acl localnet src fc00::/7 # RFC 4193 local private network range  
acl localnet src fe80::/10 # RFC 4291 link-local (directly plugged) machines  
acl SSL_ports port 443  
acl Safe_ports port 80 # http  
acl Safe_ports port 21 # ftp  
acl Safe_ports port 443 # https  
acl Safe_ports port 70 # gopher  
acl Safe_ports port 210 # wais  
acl Safe_ports port 1025-65535 # unregistered ports  
acl Safe_ports port 280 # http-mgmt  
acl Safe_ports port 488 # gss-http  
acl Safe_ports port 591 # filemaker  
acl Safe_ports port 777 # multiling http  
http_access deny !Safe_ports  
http_access deny CONNECT !SSL_ports  
acl block_extensions urlpath_regex -i \.exe$ \.zip$ \.rar$ \.tar$ \.gz$ \.iso$ \.mp4$  
http_reply_access deny block_extensions  
http_access allow localhost manager  
http_access deny manager  
include /etc/squid/conf.d/*.conf  
http_access allow localhost
```


Triển khai thực nghiệm | Tính năng Block Download Content Filtering

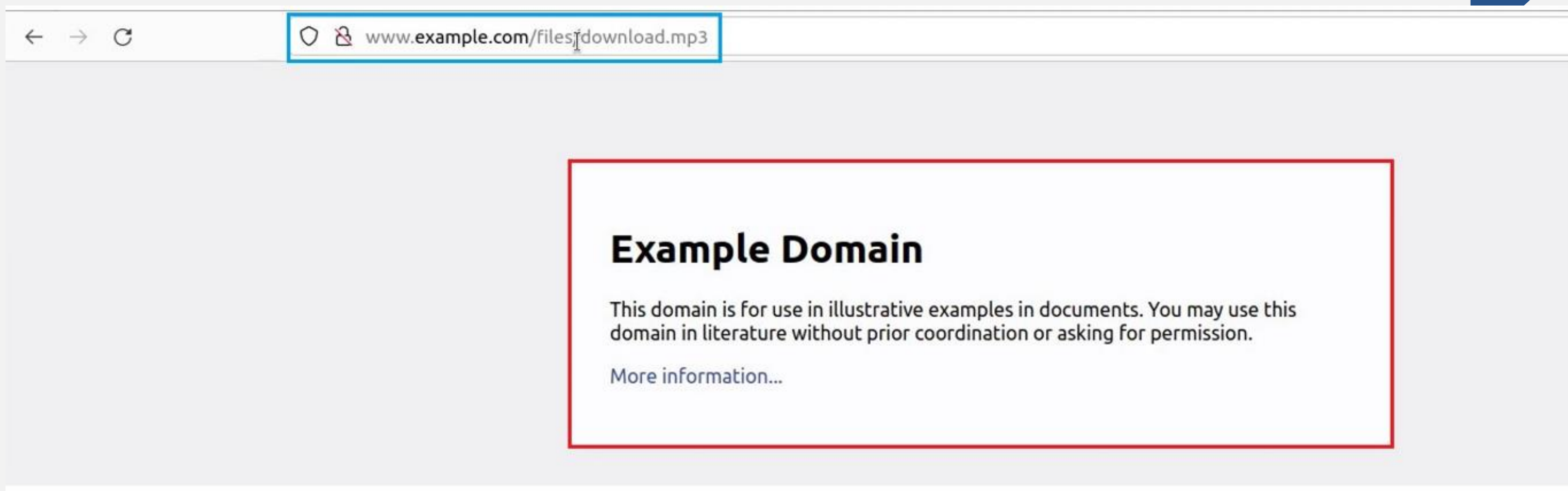
Bước 2: Vào máy Client2 để kiểm tra hoạt động của Squid Proxy bằng cách sử dụng trình duyệt vào các trang web để tải các file có phần mở rộng bị chặn.



*Các tệp có phần mở rộng **.exe** đã bị chặn*

Triển khai thực nghiệm | Tính năng Block Download Content Filtering

Bước 2: Vào máy Client2 để kiểm tra hoạt động của Squid Proxy bằng cách sử dụng trình duyệt vào các trang web để tải các file có phần mở rộng không bị chặn.



*Các tệp có phần mở rộng **.mp3** không bị chặn*

Bước 1: Cài đặt apache2-utils để có thể sử dụng htpasswd

```
sudo apt install apache2-utils
```

Bước 2: Tạo file chứa password của user và cấp quyền thực thi cho file đó

```
sudo touch /etc/squid/passwd  
sudo chown squidproxy: /etc/squid/passwd
```

Bước 3: Tạo password cho Client2

```
sudo htpasswd /etc/squid/passwd client2
```

Bước 4: Cấu hình Squid Proxy để thực hiện chức năng trên

```
auth_param basic program /usr/lib/squid/basic_ncsa_auth /etc/squid/passwd
auth_param basic children 5
auth_param basic realm Squid Basic Authentication
auth_param basic credentialsttl 2 hours
acl auth_users proxy_auth REQUIRED
http_access allow auth_users
```

```
acl Safe_ports port 777          # multiling http
http_access deny !Safe_ports
http_access deny CONNECT !SSL_ports
http_access allow localhost manager
http_access deny manager
include /etc/squid/conf.d/*.conf
auth_param basic program /usr/lib/squid/basic_ncsa_auth /etc/squid/passwd
auth_param basic children 5
auth_param basic realm Squid Basic Authentication
auth_param basic credentialsttl 2 hours
acl auth_users proxy_auth REQUIRED
http_access allow auth_users
http_access allow localhost
acl client2 src 192.168.37.0/24
http_access allow client2
http_access deny all
http_port 192.168.37.139:3128
http_port 3128
cache_dir ufs /var/spool/squid 100 16 256
```

Bước 5: Vào máy Client2 để kiểm tra hoạt động của Squid Proxy

Khi vào trình duyệt, Client 2 cần nhập username và password ngay lập tức để có thể truy cập website.



Authentication Required - Mozilla Firefox

 The proxy moz-proxy://192.168.37.139:3128 is requesting a username and password. The site says: "Squid Basic Authentication"

Username

Password

Cancel Sign in

Bước 1: Cấu hình Squid Proxy để thực hiện chức năng trên

```
acl client2 src 192.168.37.138
acl client1 src 192.168.37.128
http_access allow client2
http_access deny client1
```

```
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
http_access deny !Safe_ports
http_access deny CONNECT !SSL_ports
http_access allow localhost manager
http_access deny manager
include /etc/squid/conf.d/*.conf
http access allow localhost
acl client2 src 192.168.37.138
acl client1 src 192.168.37.128
http_access allow client2
http_access deny client1
http_access deny all
http_port 192.168.37.139:3128
http_port 3128
cache_dir ufs /var/spool/squid 100 16 256
coredump_dir /var/spool/squid
refresh_pattern ^ftp:      1440      20%      10080
refresh_pattern ^gopher:   1440      0%      1440
refresh_pattern -i (/cgi-bin/|\?) 0      0%      0
```

Bước 1: Cấu hình Squid Proxy để thực hiện chức năng trên

```
acl client2 src 192.168.37.138
acl client1 src 192.168.37.128
http_access allow client2
http_access deny client1
```

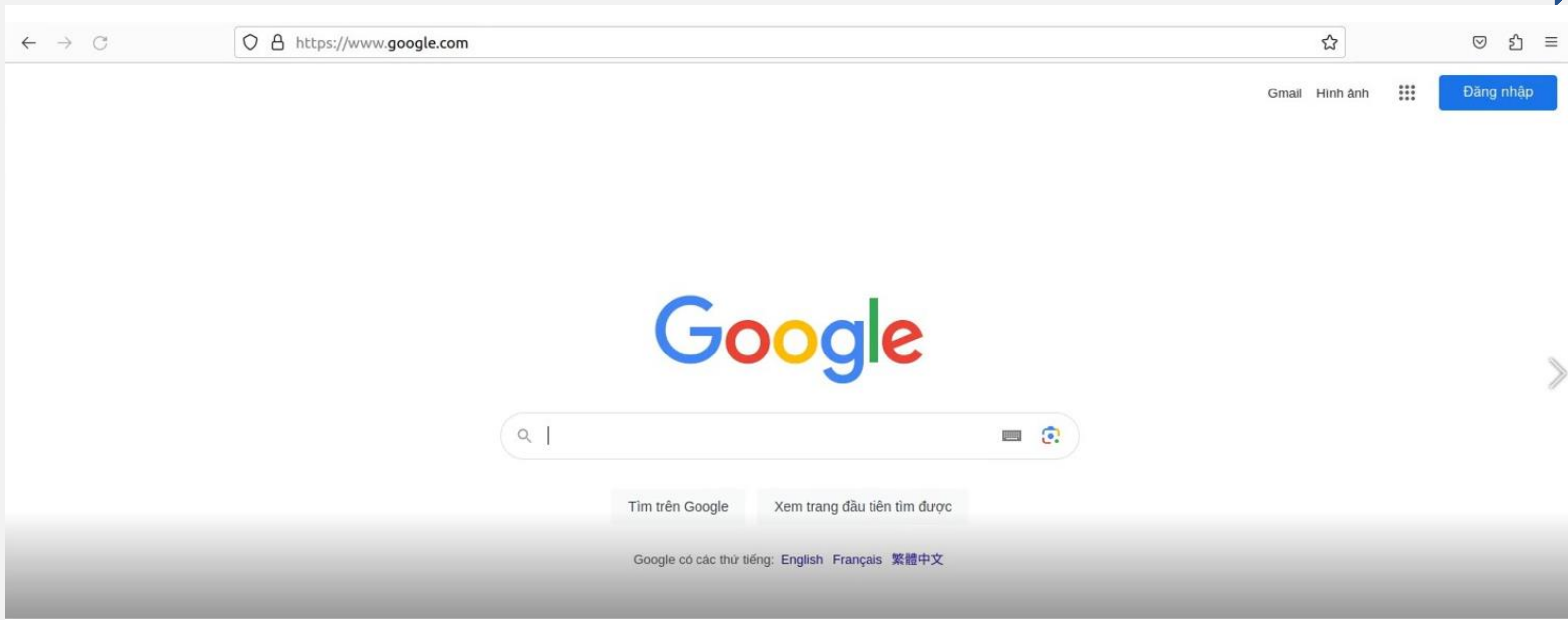
```
acl Safe_ports port 1025-65535 # unregistered ports
acl Safe_ports port 280      # http-mgmt
acl Safe_ports port 488      # gss-http
acl Safe_ports port 591      # filemaker
acl Safe_ports port 777      # multiling http
http_access deny !Safe_ports
http_access deny CONNECT !SSL_ports
http_access allow localhost manager
http_access deny manager
include /etc/squid/conf.d/*.conf
http access allow localhost
acl client2 src 192.168.37.138
acl client1 src 192.168.37.128
http_access allow client2
http_access deny client1
http_access deny all
http_port 192.168.37.139:3128
http_port 3128
cache_dir ufs /var/spool/squid 100 16 256
coredump_dir /var/spool/squid
refresh_pattern ^ftp:      1440      20%      10080
refresh_pattern ^gopher:   1440      0%       1440
refresh_pattern -i (/cgi-bin/|\?) 0      0%       0
```


04 Triển khai thực nghiệm | Tính năng Access Control List

40

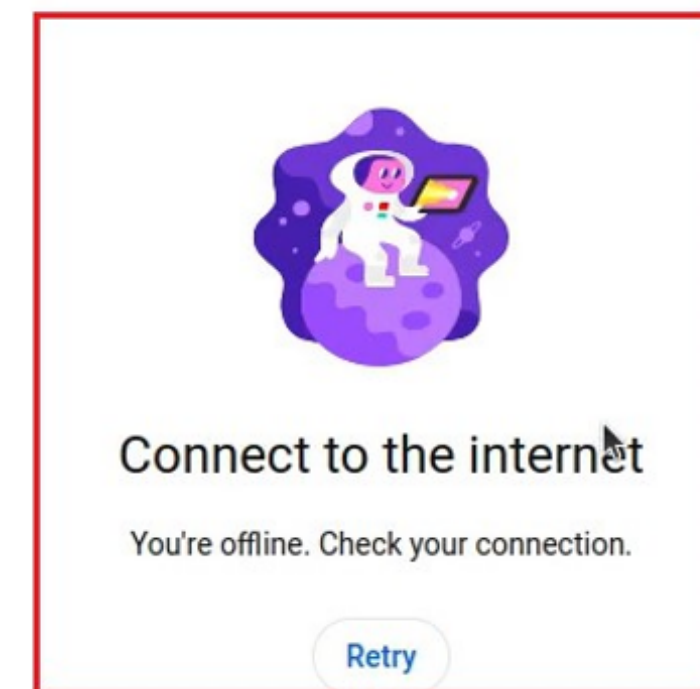
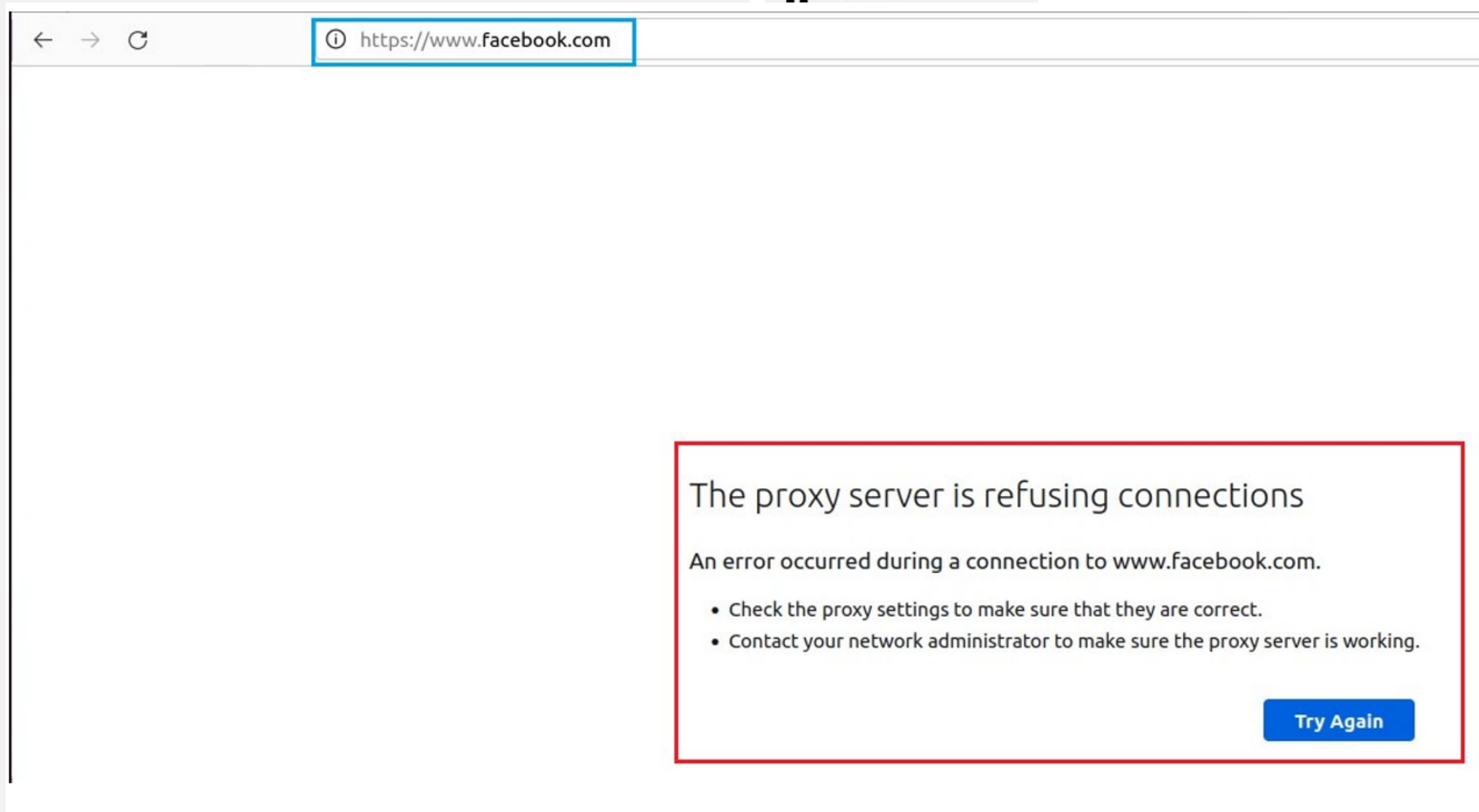
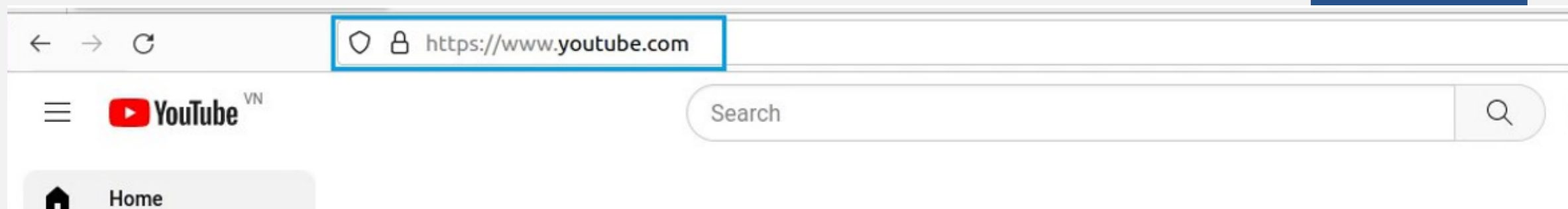
Bước 2: Lần lượt vào máy Client2 và Client 1 sử dụng trình duyệt để kiểm tra hoạt động của Squid Proxy

Máy Client 2



Bước 2: Lần lượt vào máy Client2 và Client 1 sử dụng trình duyệt để kiểm tra hoạt động của Squid Proxy

Máy Client 1



05

Kết luận

- Thực hiện 07 kịch bản triển khai để thể hiện các tính năng của Squid proxy
- Mô hình đưa ra các giải pháp giúp làm cải thiện tốc độ truy cập trang web, chặn truy cập độc hại, phân quyền, xác thực người dùng khi truy cập internet.

Ưu điểm	Hạn chế
<ul style="list-style-type: none">• Là mã nguồn mở, giúp tiết kiệm chi phí cho cơ quan, doanh nghiệp nhỏ• Có nhiều tính năng có thể tùy chỉnh.• Giúp làm tăng tốc độ duyệt website• Giảm mức sử dụng băng thông• Có thể lọc chặn một số nội dung không muốn người dùng truy cập.• Tăng cường khả năng bảo mật.	<ul style="list-style-type: none">• Là công cụ phức tạp, đòi hỏi người dùng phải có hiểu biết về kỹ thuật.• Có thể chặn sai nội dung truy cập được cho phép và bỏ sót nội dung truy cập không được phép.• Cần đầu tư thêm tài nguyên phần cứng để sử dụng Proxy.• Squid Proxy yêu cầu địa chỉ IP cụ thể để cấu hình khiến việc thay đổi địa chỉ IP thường xuyên trở nên khó khăn khi sử dụng proxy

- Thực nghiệm với một quy mô lớn hơn và thực nghiệm những kịch bản triển khai để chứng minh những nhược điểm của mô hình.
- Người dùng vẫn có thể dùng các phần mềm khác để vượt qua Proxy trong ngữ cảnh ngăn chặn truy cập cần tìm hiểu và triển khai để khắc phục vấn đề này.
- Có thể áp dụng Squid Proxy cho những mô hình mạng phức tạp hơn, thiết lập một cụm Proxy liên kết với nhau, khi một Proxy gặp sự cố thì Proxy hỏng có thể được tạm thời thay thế bằng cách hướng đường truyền của các Client phía sau nó sang cho Squid Proxy khác.



THANK YOU

