

ĐẠI HỌC QUỐC GIA TP. HỒ CHÍ MINH
TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN



BÁO CÁO ĐỒ ÁN
MÔN: QUẢN TRỊ MẠNG VÀ HỆ THỐNG

**ĐỀ TÀI: TÌM HIỂU VÀ TRIỂN KHAI
SQUID PROXY**

Giảng viên hướng dẫn: ThS. Đỗ Hoàng Hiển

Lớp: NT132.P12.ANTT

Nhóm thực hiện:

Trần Tuấn Anh	22520080
Nguyễn Khắc Hậu	22520410
Huỳnh Minh Hiển	22520415
Ngô Trung Hiếu	22520437

Ngành: An Toàn Thông Tin

NHẬN XÉT VÀ CHẤM ĐIỂM CỦA GIẢNG VIÊN

Họ và tên: Th.S Đỗ Hoàng Hiển

Tên đề tài: Tìm hiểu và triển khai Squid Proxy

Nội dung nhận xét:

Djêm:

Bằng số:

Bằng chữ:

MỤC LỤC

CHƯƠNG 1: GIỚI THIỆU	8
1.1. Tên đề tài	8
1.2. Lý do thực hiện đề tài	8
1.3. Mục đích nghiên cứu	8
1.4. Đối tượng và phạm vi nghiên cứu	8
1.5. Phương pháp nghiên cứu	8
CHƯƠNG 2: CƠ SỞ LÝ THUYẾT.....	9
2.1. Giới thiệu Proxy Server.....	9
2.2. Giới thiệu về Squid	10
2.2.1. Squid là gì?	10
2.2.2. Những tính năng chính của Squid	10
2.2.3. Ưu và nhược điểm của Squid.....	11
CHƯƠNG 3: THIẾT KẾ MÔ HÌNH TRIỂN KHAI	12
3.1. Mô hình triển khai	12
3.2. Vai trò của các thành phần trong mô hình.....	12
3.3. Tương tác giữa các thành phần trong mô hình.....	12
CHƯƠNG 4: HIỆN THỰC ĐỀ TÀI.....	13
4.1. Cài đặt môi trường	13
4.2. Cài đặt Squid trên Proxy Server	15
4.3. Cấu hình Proxy trên Client.....	19
4.4. Cấu hình các kịch bản	21
4.4.1. Kịch bản 1: Kiểm soát truy cập (Access Control)	21
4.4.2. Kịch bản 2: Caching	23
4.4.3. Kịch bản 3: Quản lý băng thông (Bandwidth management)	24
4.4.4. Kịch bản 4: Ẩn danh người dùng (Anonymization)	25
4.4.5. Kịch bản 5: Giám Sát và Ghi Log Hoạt Động Người Dùng	26
4.5. Cấu hình FTP	27
4.6. Cấu hình Transparent Proxy.....	28
CHƯƠNG 5: THỰC NGHIỆM ĐỀ TÀI.....	30
5.1. Kịch bản 1: Kiểm soát truy cập (Access Control)	30
5.2. Kịch bản 2: Caching.....	34

5.3. Kịch bản 3: Quản lý băng thông (Bandwidth Management)	40
5.4. Kịch bản 4: Ân danh người dùng (Anonymization)	40
5.5. Kịch bản 5: Giám sát và ghi log hoạt động người dùng	42
5.6. FTP	44
5.7. Transparent Proxy	46
5.8. Đánh giá thực nghiệm	49
CHƯƠNG 6: KẾT LUẬN VÀ HƯỚNG PHÁT TRIỂN	51
6.1. Kết quả đạt được	51
6.2. Khó khăn và hạn chế	51
6.3. Hướng phát triển	51
TÀI LIỆU THAM KHẢO.....	52

DANH MỤC HÌNH

Hình 1: Cách hoạt động của Proxy Server	9
Hình 2: Logo Squid.....	10
Hình 3: Mô hình triển khai.....	12
Hình 4: Cấu hình IP	13
Hình 5: IP các interface của Proxy Server	14
Hình 6: IP các interface của Client1	14
Hình 7: IP các interface của Client2	15
Hình 8: Kết quả sau khi giải nén mã nguồn.....	15
Hình 9: Thư mục cài đặt Squid	15
Hình 10: Cài đặt thành công	16
Hình 11: Nội dung file service Squid.....	16
Hình 12: Cấu hình người dùng chạy Squid.....	16
Hình 13: Tình trạng của Squid.....	17
Hình 14: Kết quả tạo khóa và chứng chỉ.....	17
Hình 15: Khởi tạo ssl_db	17
Hình 16: Tình trạng Squid sau khi cấu hình SSL bump.....	18
Hình 17: Định nghĩa mạng 192.168.1.0/24.....	19
Hình 18: Cho phép truy cập từ mạng vừa định nghĩa	19
Hình 19: Cấu hình Proxy trong cài đặt Network	20
Hình 20: Cấu hình Proxy trong trình duyệt 1.....	20
Hình 21: Cấu hình Proxy trong trình duyệt 2.....	21
Hình 22: Kiểm tra sau khi cấu hình Proxy	21
Hình 23: Nội dung file liệt kê tên miền bị chặn.....	22
Hình 24: Định nghĩa các ACL.....	22
Hình 25: Áp dụng ACL cho mạng localnetwork.....	22
Hình 26: Cấu hình caching	23
Hình 27: Cấu hình quản lý băng thông	25
Hình 28: Cấu hình ẩn danh người dùng	25
Hình 29: Các file log của Squid	27
Hình 30: Nội dung file access.log.....	27
Hình 31: Nội dung file cache.log	27
Hình 32: Cấu hình log format	27
Hình 33: Ví dụ định nghĩa access listl port 21	28
Hình 34: Ví dụ áp dụng access list đã định nghĩa	28
Hình 35: Ví dụ định nghĩa người dùng FTP	28
Hình 36: Truy cập Facebook trước khi cấu hình.....	30
Hình 37: Truy cập Youtube trước khi cấu hình	30
Hình 38: Truy cập Web không bị chặn trước khi cấu hình	31
Hình 39: Truy cập Facebook sau khi cấu hình ngoài thời gian cho phép	31
Hình 40: Truy cập Youtube sau khi cấu hình ngoài thời gian cho phép.....	32
Hình 41: Truy cập Web không bị chặn sau khi cấu hình ngoài thời gian cho phép	32
Hình 42: Truy cập Web không bị chặn sau khi cấu hình trong thời gian cho phép.....	33
Hình 43: Truy cập Facebook sau khi cấu hình trong thời gian cho phép.....	33
Hình 44: Truy cập Youtube sau khi cấu hình trong thời gian cho phép	34
Hình 45: Tải file trên client 1	34
Hình 46: Tải file trên client 2.....	34

Hình 47: Tải file từ server test trên client 1	34
Hình 48: Log của Server khi client 1 tải file.....	35
Hình 49: Tải file từ server test trên client 2	35
Hình 50: Log của Server khi client 2 tải file.....	36
Hình 51: Tải file 258KB trước khi cache.....	36
Hình 52: Tải file 1MB trước khi cache	37
Hình 53: Tải file 10MB trước khi cache.....	37
Hình 54: Tải file 50MB trước khi cache	37
Hình 55: Tải file 100MB trước khi cache	37
Hình 56: Tải file 400MB trước khi cache	38
Hình 57: Tải file 800MB trước khi cache	38
Hình 58: Tải file 285KB sau khi cache	38
Hình 59: Tải file 1MB sau khi cache	38
Hình 60: Tải file 10MB sau khi cache	39
Hình 61: Tải file 50MB sau khi cache	39
Hình 62: Tải file 100MB sau khi cache	39
Hình 63: Tải file 400MB sau khi cache	39
Hình 64: Tải file 800MB sau khi cache	40
Hình 65: Tải file khi chưa cấu hình quản lý băng thông.....	40
Hình 66: Tải file khi đã cấu hình quản lý băng thông.....	40
Hình 67: Client truy cập Server test trước khi cấu hình.....	40
Hình 68: Bắt gói tin HTTP trước khi cấu hình.....	41
Hình 69: Truy cập server test sau khi cấu hình	41
Hình 70: Bắt gói tin HTTP sau khi đã cấu hình.....	42
Hình 71: Log được ghi lại khi truy cập vào trang web bắt kí	42
Hình 72: Log được ghi lại khi truy cập vào trang web bị chặn.....	43
Hình 73: Log được ghi lại khi truy cập đối tượng được cache	43
Hình 74: Tải file từ FTP Server	44
Hình 75: Log của Squid	44
Hình 76: Log của FTP server	44
Hình 77: Tải file từ FTP server sau khi cấu hình cache	44
Hình 78: Log của request tải file cache.....	44
Hình 79: Log của FTP server	44
Hình 80: Định nghĩa ACL	45
Hình 81: Áp dụng ACL	45
Hình 82: Tải file sau khi cấu hình từ chối truy cập	45
Hình 83: Log của request bị từ chối truy cập.....	45
Hình 84: Tải file với thông tin đăng nhập	45
Hình 85: Log của Squid	45
Hình 86: Log của Server	45
Hình 87: Xoá cấu hình proxy trên trình duyệt	46
Hình 88: Xóa cấu hình proxy trong cài đặt mạng	46
Hình 89: Truy cập lại Internet trên Client	47
Hình 90: Log được ghi lại trên Squid	47
Hình 91: Cấu hình cache trên Squid	48
Hình 92: Tải file trước khi cấu hình cache.....	48
Hình 93: Tải file sau khi cấu hình cache	48
Hình 94: Định nghĩa acl chặn truy cập	48

Hình 95: Áp dụng acl đã định nghĩa	48
Hình 96: Truy cập vào trang bị chặn.....	49

LỜI MỞ ĐẦU

Trong bối cảnh mạng máy tính ngày càng phát triển, việc quản lý và tối ưu hóa tài nguyên mạng đóng vai trò thiết yếu nhằm đảm bảo hiệu suất hoạt động và nâng cao trải nghiệm người dùng. Squid Proxy là một trong những giải pháp phổ biến được sử dụng để hỗ trợ việc lưu trữ cache, tăng tốc độ truy cập, quản lý băng thông, và nâng cao bảo mật trong hệ thống mạng.

Báo cáo này được thực hiện nhằm mục đích tìm hiểu về Squid Proxy, bao gồm các tính năng, cấu hình và ứng dụng thực tế. Trong quá trình nghiên cứu, nhóm đã triển khai các thử nghiệm để minh họa rõ hơn cách thức hoạt động và hiệu quả của công cụ này.

Qua đây, chúng em không chỉ tích lũy được kiến thức về Proxy Server mà còn có cơ hội tiếp cận với các kỹ thuật quản trị mạng hiện đại, đồng thời phát triển các kỹ năng cần thiết trong việc triển khai và tối ưu hóa hệ thống mạng. Chúng em hy vọng rằng báo cáo sẽ mang lại những thông tin hữu ích cho những ai quan tâm và muốn triển khai Squid Proxy trong thực tiễn.

Xin chân thành cảm ơn thầy Đỗ Hoàng Hiển đã hướng dẫn chúng em, cho chúng em cơ hội để hiện thực hóa đề án này.

CHƯƠNG 1: GIỚI THIỆU

1.1. Tên đề tài

ĐỀ TÀI “TÌM HIỂU VÀ TRIỂN KHAI SQUID PROXY”

1.2. Lý do thực hiện đề tài

Hiện nay, lưu lượng truy cập Internet ngày càng gia tăng kéo theo nhu cầu tối ưu hóa băng thông, cải thiện tốc độ truy cập, và đảm bảo an toàn cho người dùng mạng nội bộ. Các tổ chức và doanh nghiệp luôn tìm kiếm giải pháp hiệu quả để đáp ứng nhu cầu trên khiến việc quản trị mạng trở nên hiệu quả.

Squid Proxy là một công cụ mạnh mẽ trong việc quản lý truy cập Internet, lưu trữ cache, và giảm tải cho đường truyền mạng. Không chỉ tiết kiệm tài nguyên, Squid Proxy còn hỗ trợ các tính năng kiểm soát băng thông, lọc nội dung, và tăng cường bảo mật, giúp đảm bảo hoạt động mạng ổn định và hiệu quả.

1.3. Mục đích nghiên cứu

Mục đích của đồ án này là tìm hiểu cách cài đặt và sử dụng Squid Proxy. Triển khai được trong một mô hình mạng cụ thể và thể hiện được các tính năng chính, nổi bật của Squid Proxy.

Cung cấp cho mỗi thành viên trong nhóm cơ hội để vận dụng kiến thức đã học, tìm hiểu cộng nghệ mới và áp dụng vào sản phẩm thực tiễn. Từ đó phát triển kỹ năng lập trình và kỹ năng quản lý dự án.

1.4. Đối tượng và phạm vi nghiên cứu

Đối tượng nghiên cứu: Squid Proxy.

Phạm vi nghiên cứu: Các bước cài đặt và cấu hình để vận hành của mô hình mạng có áp dụng Squid Proxy.

1.5. Phương pháp nghiên cứu

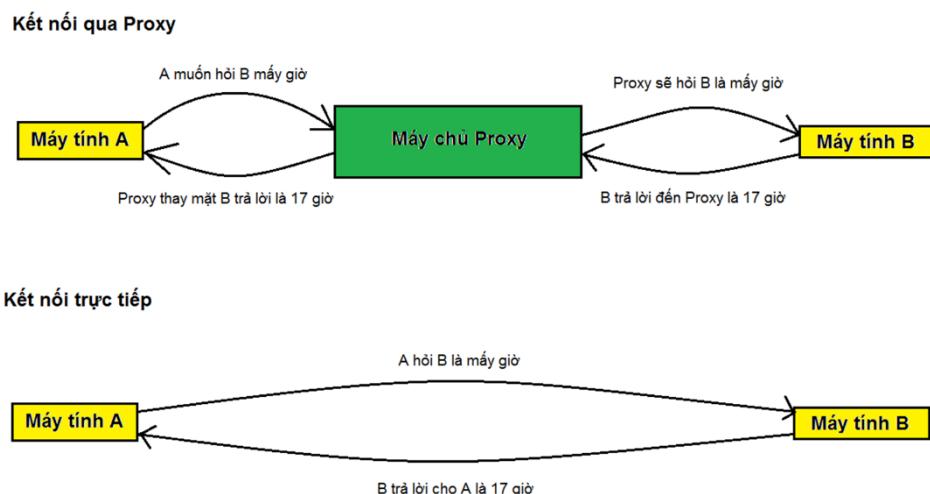
- Thu thập tài liệu từ documentation và các hướng dẫn từ cộng đồng sử dụng Squid Proxy.
- Tìm hiểu các khái niệm liên quan đến kiểm soát truy cập, caching, quản lý băng thông, lọc nội dung và các tính năng bảo mật.
- Nghiên cứu xây dựng mô hình mạng và triển khai theo kịch bản đã đề ra.

CHƯƠNG 2: CƠ SỞ LÝ THUYẾT

2.1. Giới thiệu Proxy Server

Proxy Server là một máy chủ trung gian giữa **người dùng cuối** và **trang web** mà họ truy cập.

Các Proxy Server cung cấp các chức năng, bảo mật và riêng tư khác nhau phụ thuộc vào nhu cầu của người dùng hoặc chính sách doanh nghiệp. Nhóm người dùng Proxy Server chủ yếu đến từ những tổ chức cần bảo mật thông tin riêng tư và điển hình là các doanh nghiệp. [1]



Hình 1: Cách hoạt động của Proxy Server

Nếu đang sử dụng Proxy Server, lưu lượng truy cập Internet sẽ truyền qua máy chủ theo đường của nó đến địa chỉ người dùng cuối yêu cầu. Sau đó, yêu cầu này sẽ trở lại cùng một Proxy Server và nó sẽ chuyển tiếp dữ liệu nhận được từ địa chỉ yêu cầu đến người dùng.

Khi Proxy Server chuyển tiếp yêu cầu của người dùng, nó có thể thay đổi dữ liệu đó mà vẫn lấy thông tin theo đúng yêu cầu. Proxy Server có thể thay đổi các thông tin trong yêu cầu để máy chủ web không thể nắm rõ được chính xác vị trí của người dùng.Thêm vào đó, Proxy Server có thể giúp chặn các truy cập vào các trang web cụ thể dựa trên địa chỉ IP.

2.2. Giới thiệu về Squid

2.2.1. Squid là gì?



Hình 2: Logo Squid

Squid là một phần mềm proxy mã nguồn mở đầy đủ tính năng.

Squid cung cấp một môi trường phong phú về kiểm soát truy cập, xác thực và ghi nhật ký, hỗ trợ phát triển các ứng dụng proxy web và cung cấp các dịch vụ liên quan.

Squid còn mang đến một tập hợp đa dạng các tùy chọn tối ưu hóa lưu lượng, hầu hết trong số đó được kích hoạt mặc định để đơn giản hóa việc cài đặt và đạt hiệu suất cao. [2]

2.2.2. Những tính năng chính của Squid

Squid có những tính năng chính như:

- **Caching:** Squid lưu trữ các tài nguyên như hình ảnh, video và trang web, giúp giảm thời gian tải trang khi người dùng truy cập lại.
- **Lọc nội dung (Content Filtering) :** Squid có thể chặn hoặc lọc nội dung truy cập dựa trên URL, địa chỉ IP hoặc từ khóa.
- **Kiểm soát truy cập (Access Control):** Cung cấp khả năng kiểm soát truy cập dựa trên thời gian, địa chỉ IP hoặc whitelist/blacklist.
- **Quản lý băng thông (Bandwidth Management) :** Quản lý và giới hạn băng thông cho từng nhóm người dùng hoặc truy cập nhất định tránh trường hợp băng thông bị chiếm dụng không hiệu quả.
- **Ẩn danh người dùng (Anonymization):** Squid có thể chỉnh sửa các yêu cầu để ẩn địa chỉ IP cũng như các thông tin khác của người dùng nhằm bảo vệ quyền riêng tư khi truy cập internet.
- **Giám sát và ghi log hoạt động người dùng:** Ghi lại mọi hoạt động truy cập web giúp quản trị viên có thể giám sát và phân tích hoạt động của người dùng từ đó phát hiện ra các rủi ro về bảo mật trong hệ thống mạng.

2.2.3. Ưu và nhược điểm của Squid

Ưu điểm của Squid là gì?

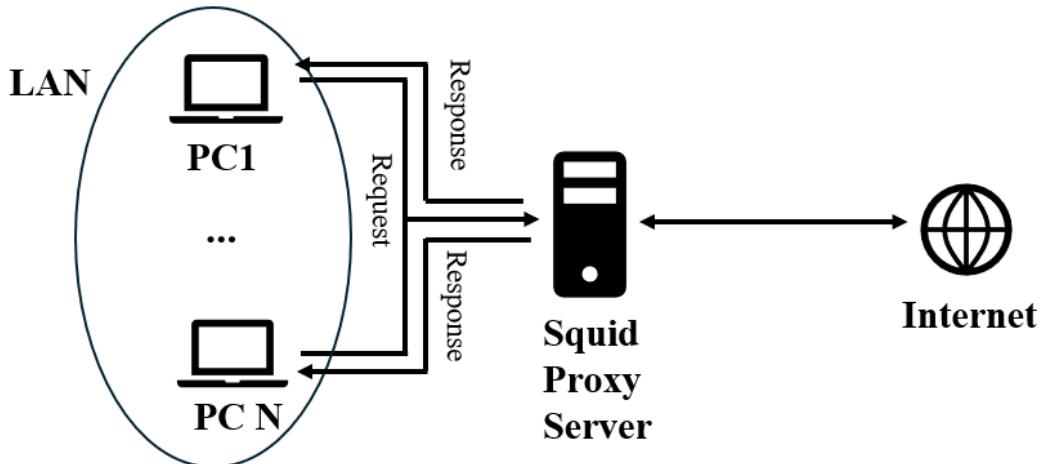
- Không mất phí để cài đặt và sử dụng.
- Có khả năng lưu trữ tạm (cache) các tài nguyên web, giúp tăng tốc độ truy cập của người dùng.
- Squid hỗ trợ tính năng **delay pools** để quản lý băng thông.
- Squid cho phép cấu hình các quy tắc kiểm soát truy cập thông qua Access Control Lists (ACLs).
- Hỗ trợ nhiều giao thức HTTP/HTTPS, FTP, và SSL/TLS.
- Squid hỗ trợ nhiều phương thức xác thực như Basic Authentication, LDAP, và Kerberos.

Nhược điểm của Squid là gì?

- Cấu hình phức tạp: Quản trị viên cần có kiến thức sâu về hệ thống để triển khai hiệu quả..
- Không hỗ trợ cân bằng tải động (Dynamic Load Balancing).
- Không hỗ trợ đa luồng.
- Không được thiết kế tính năng chặn quảng cáo.

CHƯƠNG 3: THIẾT KẾ MÔ HÌNH TRIỂN KHAI

3.1. Mô hình triển khai



Hình 3: Mô hình triển khai

Thông tin các máy

Tên máy	Hệ điều hành	Địa chỉ IP
Squid Proxy Server	Ubuntu 18.04	192.168.1.1/24
Client 1	Ubuntu 18.04	192.168.1.101/24
Client 2	Ubuntu 18.04	192.168.1.102/24

3.2. Vai trò của các thành phần trong mô hình

Client: Thực hiện các yêu cầu đến Internet gửi các yêu cầu (requests) truy cập tài nguyên trên Internet. Ví dụ: trang web hoặc dữ liệu.

Squid Proxy Server : Nhận yêu cầu từ các máy trong mạng LAN, chuyển tiếp chúng ra Internet và chuyển tiếp lại những phản hồi nhận từ Internet.

3.3. Tương tác giữa các thành phần trong mô hình

Client gửi các yêu cầu (requests) đến Internet.

Các yêu cầu sẽ được gửi đến Squid Proxy Server, Server sẽ kiểm tra xem yêu cầu đã được cache chưa:

- Nếu có, gửi lại phản hồi từ cache.
- Nếu không, gửi yêu cầu ra Internet.

Ngoài ra, Squid Proxy Server thực hiện một số chức năng như quản lý băng thông, kiểm soát truy cập dựa vào các thông tin trong yêu cầu, chỉnh sửa yêu cầu để tăng tính bảo mật.

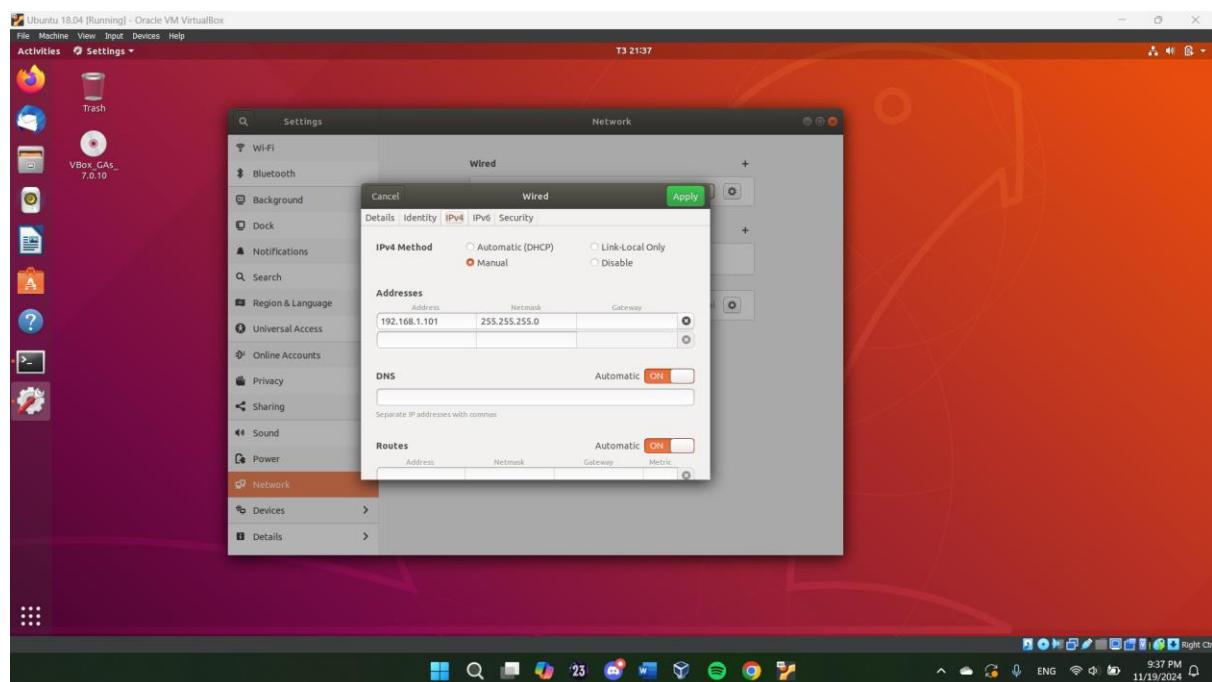
Squid Proxy Server nhận phản hồi từ Internet và chuyển tiếp lại nội dung đến Client yêu cầu.

CHƯƠNG 4: HIỆN THỰC ĐỀ TÀI

4.1. Cài đặt môi trường

Thiết lập IP cho các máy ảo Ubuntu 18.04

Vào **Settings > Network > Wired Settings > IPv4 >** Chọn **Manual** > Nhập địa chỉ IP và subnet mask



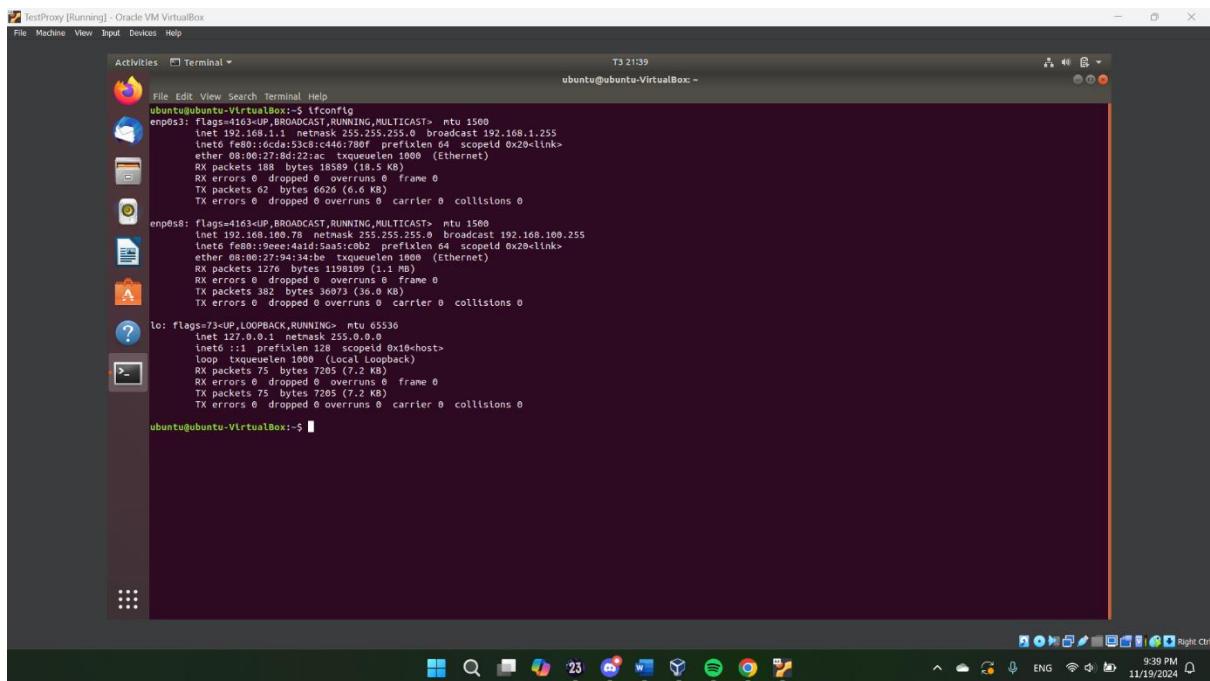
Hình 4: Cấu hình IP

Chọn **Apply** > Kết nối lại mạng để áp dụng cài đặt

Proxy Server

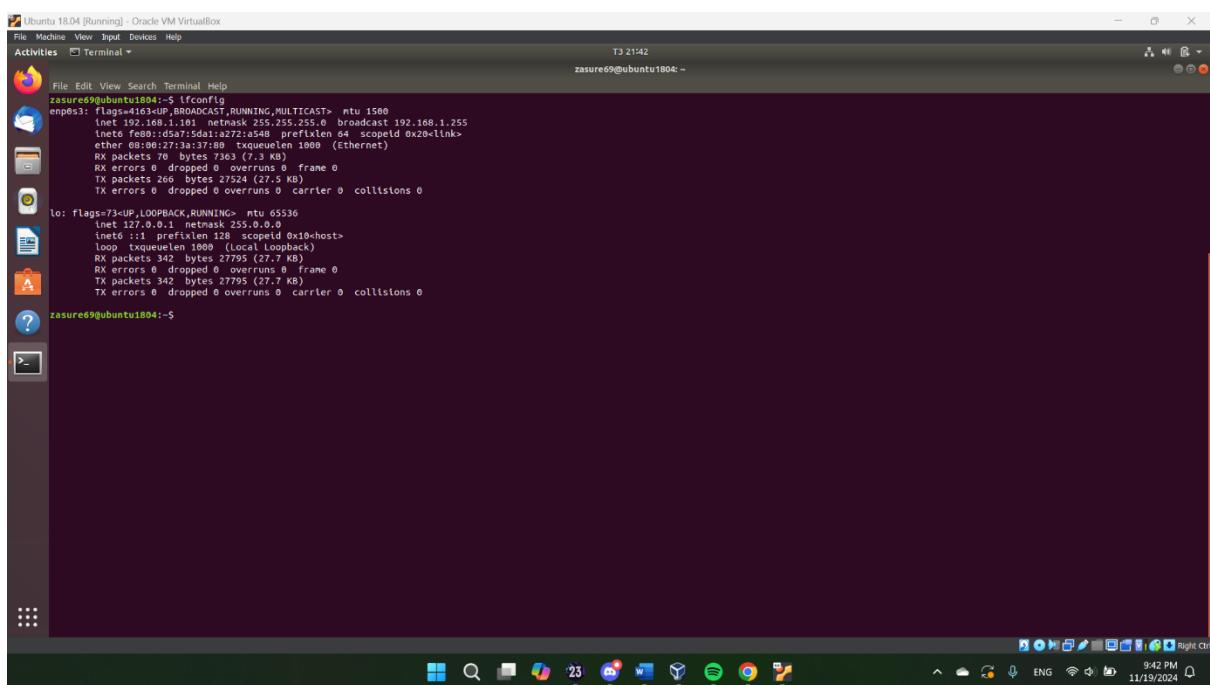
Interface enp0s3 dùng để kết nối với mạng local 192.168.1.0/24

Interface enp0s8 dùng để kết nối với Internet



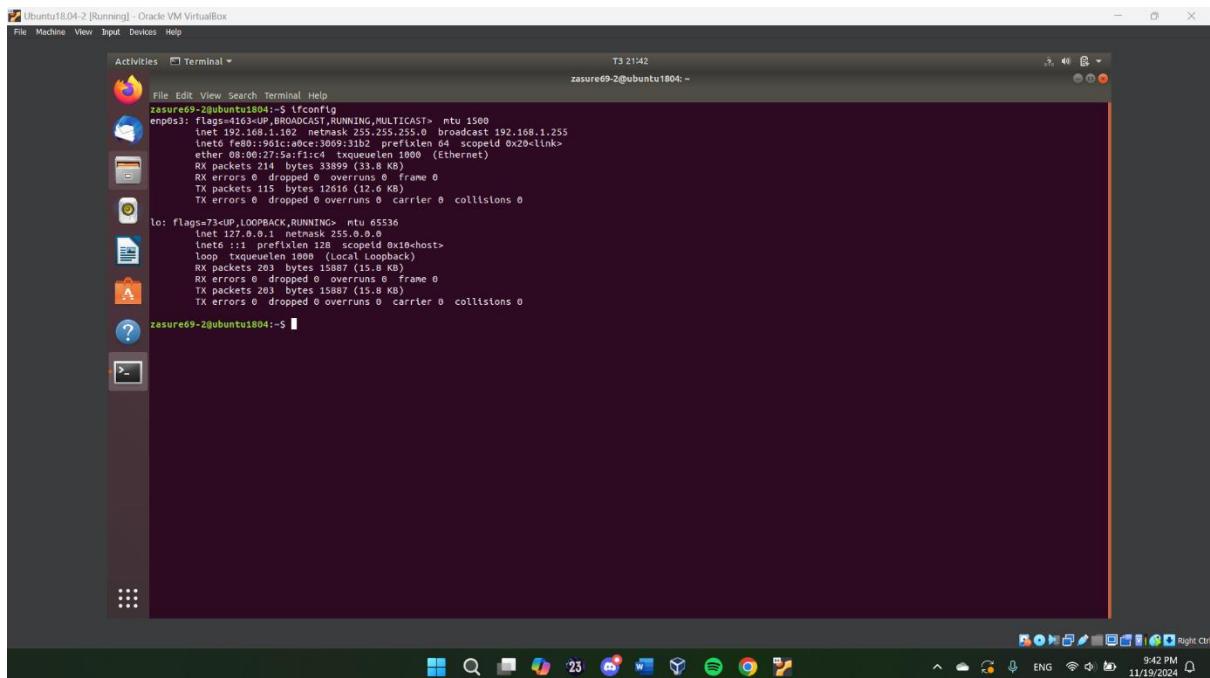
Hình 5: IP các interface của Proxy Server

Client 1



Hình 6: IP các interface của Client1

Client 2



Hình 7: IP các interface của Client2

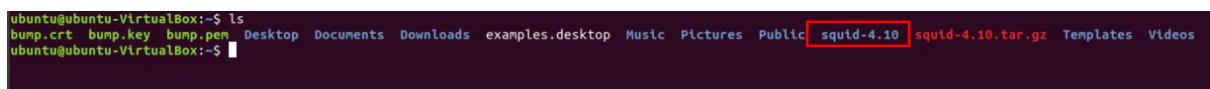
4.2. Cài đặt Squid trên Proxy Server [3]

Bước 1: Tải và giải nén mã nguồn Squid (phiên bản 4.10)

```

wget http://www.squid-cache.org/Versions/v4/squid-
4.10.tar.gz
tar -xvzf squid-4.10.tar.gz

```



Hình 8: Kết quả sau khi giải nén mã nguồn

Bước 2: Thực hiện configure và cài đặt mã nguồn

```

cd squid-4.10
./configure --enable-ssl-crtd --with-openssl --enable-
delay-pools
make -j $(nproc)
sudo make install

```

Squid sẽ được cài đặt tại thư mục /usr/local/squid.

```

ubuntu@ubuntu-VirtualBox:/usr/local/squid$ ls
bin etc libexec sbin share var
ubuntu@ubuntu-VirtualBox:/usr/local/squid$ 

```

Hình 9: Thư mục cài đặt Squid

Thực hiện lệnh /usr/local/squid/sbin/squid -v.

```
ubuntu@ubuntu-VirtualBox:/usr/local/squid$ /usr/local/squid/sbin/squid -v
Squid Cache: Version 4.10
Service Name: squid

This binary uses OpenSSL 1.1.1 11 Sep 2018. For legal restrictions on distribution see https://www.openssl.org/source/license.html
configure options: '--enable-ssl-crt' '--with-openssl' '--enable-delay-pools' --enable-ltdl-convenience
ubuntu@ubuntu-VirtualBox:/usr/local/squid$
```

Hình 10: Cài đặt thành công

Kết quả như hình cho thấy đã cài đặt thành công.

Bước 3: Tạo file service và khởi động Squid

Thực hiện lệnh sudo nano /etc/systemd/system/squid.service để tạo file với nội dung :

```
File Edit View Search Terminal Help
GNU nano 2.9.3
/etc/systemd/system/squid.service

[Unit]
Description=Squid Web Proxy Server
After=network.target

[Service]
Type=forking
ExecStart=/usr/local/squid/sbin/squid -f /usr/local/squid/etc/squid.conf
ExecReload=/usr/local/squid/sbin/squid -k reconfigure -f /usr/local/squid/etc/squid.conf
ExecStop=/usr/local/squid/sbin/squid -k shutdown -f /usr/local/squid/etc/squid.conf
PIDFile=/usr/local/squid/var/run/squid.pid

[Install]
WantedBy=multi-user.target
```

Hình 11: Nội dung file service Squid

Thực hiện các lệnh để cho phép Squid service

```
sudo systemctl daemon-reload
sudo systemctl enable squid
```

Cấu hình người dùng chạy Squid trong file cấu hình /usr/local/squid/etc/squid.conf

```
[refresh_pattern]
# Config user run squid
cache_effective_user proxy
cache_effective_group proxy
```

Hình 12: Cấu hình người dùng chạy Squid

Cấu hình quyền cho thư mục /usr/local/squid và khởi động Squid

```
sudo chown proxy:proxy -Rf /usr/local/squid
sudo systemctl start squid
```

Kiểm tra tình trạng của Squid: sudo systemctl status squid

```
ubuntu@ubuntu-VirtualBox:~$ sudo systemctl status squid
● squid.service - Squid Web Proxy Server
   Loaded: loaded (/etc/systemd/system/squid.service; enabled; vendor preset: enabled)
   Active: active (running) since Tue 2024-11-19 22:19:24 +07; 2s ago
     Process: 2989 ExecStop=/usr/local/squid/sbin/squid -k shutdown -f /usr/local/squid/etc/squid.> (code=exited, status=1/FAILURE)
    Process: 2991 ExecStart=/usr/local/squid/sbin/squid -f /usr/local/squid/etc/squid.conf (code=exited, status=0/SUCCESS)
   Main PID: 2992 (squid)
      Tasks: 4 (limit: 4656)
        CGroup: /system.slice/squid.service
            └─2992 /usr/local/squid/sbin/squid -f /usr/local/squid/etc/squid.conf
              ├─2994 (squid-1) -kid squid-1 -f /usr/local/squid/etc/squid.conf
              ├─2995 (logfile-daemon) /usr/local/squid/var/logs/access.log
              └─2996 (unlinkd)

Thg 11 19 22:19:24 ubuntu-VirtualBox systemd[1]: Starting Squid Web Proxy Server...
Thg 11 19 22:19:24 ubuntu-VirtualBox squid[2992]: squid.service: Failed to parse PID from file /usr/local/squid/var/run/squid.pid: Invalid argument
Thg 11 19 22:19:24 ubuntu-VirtualBox squid[2992]: Squid Parent: will start 1 kids
Thg 11 19 22:19:24 ubuntu-VirtualBox squid[2992]: Squid Parent: (squid-1) process 2994 started
Thg 11 19 22:19:24 ubuntu-VirtualBox systemd[1]: Started Squid Web Proxy Server.
ubuntu@ubuntu-VirtualBox:~$
```

Hình 13: Tình trạng của Squid

Bước 4: Cấu hình SSL Bump cho Squid Proxy để có thể giải mã và xử lý các gói tin HTTPS [4]

Tạo khóa và chứng chỉ

```
openssl req -new -newkey rsa:2048 -days 365 -nodes -x509
-keyout bump.key -out bump.crt
openssl x509 -in bump.crt -outform PEM -out bump.pem
```

```
ubuntu@ubuntu-VirtualBox:/usr/local/squid/etc/ssl_cert$ ls -l
total 12
-rw-r--r-- 1 proxy proxy 1326 Thg 1 17 09:39 bump.crt
-rw-r--r-- 1 proxy proxy 1704 Thg 1 17 09:38 bump.key
-rw-r--r-- 1 proxy proxy 1326 Thg 1 17 09:40 bump.pem
ubuntu@ubuntu-VirtualBox:/usr/local/squid/etc/ssl_cert$
```

Hình 14: Kết quả tạo khóa và chứng chỉ

Cấu hình SSL Bump trong file cấu hình /usr/local/squid/etc/squid.conf

Khởi tạo cơ sở dữ liệu SSL (ssl_db)

```
sudo /usr/local/squid/libexec/security_file_certgen -c -
-s /usr/local/squid/var/squid/ssl_db -M 20MB
```

```
ubuntu@ubuntu-VirtualBox:~$ sudo /usr/local/squid/libexec/security_file_certgen -c -s /usr/local/squid/var/squid/ssl_db -M 20MB
Initialization SSL db...
Done
ubuntu@ubuntu-VirtualBox:~$
```

Hình 15: Khởi tạo ssl_db

Thêm các dòng sau vào file cấu hình

```
#Tạo ACL cho các giao dịch liên quan đến lấy chứng chỉ trung gian
acl intermediate_fetching transaction_initiator certificate-
fetching
# Áp dụng ACL intermediate_fetching
http_access allow intermediate_fetching
#Xác định chương trình tạo chứng chỉ và lưu tối đa 20MB ở ssl_db
sslcrtd_program /usr/local/squid/libexec/security_file_certgen -s
/usr/local/squid/var/squid/ssl_db -M 20MB
#Cho phép tiếp tục nối ngay cả khi gặp lỗi chứng chỉ
sslproxy_cert_error allow all
#Xử lý chứng chỉ SSL song song, tối đa là 5
sslcrtd_children 5
#Cấu hình SSL cho http_port
http_port 3128 ssl-bump generate-host-certificates=on
dynamic_cert_mem_cache_size=20MB cert=/path/to/certificate
key=/path/to/key options=NO_SSLv3
#Xác định bước 1 của SSL bump và kiểm tra tiêu đề SNI (Server Name
#Indication)
acl step1 at_step SslBump1
ssl_bump peek step1
#Chặn và giải mã các lưu lượng https
ssl_bump bump all
```

Thực hiện lệnh sudo systemctl restart squid để áp dụng cấu hình.

Thực hiện lệnh sudo systemctl status squid để kiểm tra tình trạng Squid

```
ubuntu@ubuntu-VirtualBox:~$ sudo systemctl restart squid
[sudo] password for ubuntu:
ubuntu@ubuntu-VirtualBox:~$ sudo systemctl status squid
● squid.service - Squid Web Proxy Server
   Loaded: loaded (/etc/systemd/system/squid.service; enabled; vendor preset: enabled)
   Active: active (running) since Tue 2024-11-19 22:54:13 +07; 9s ago
     Process: 3062 ExecStop=/usr/local/squid/sbin/squid -k shutdown -f /usr/local/squid/etc/squid.> (code=exited, status=1/FAILURE)
    Process: 3063 ExecStart=/usr/local/squid/sbin/squid -f /usr/local/squid/etc/squid.conf (code=exited, status=0/SUCCESS)
   Main PID: 3064 (squid)
      Tasks: 9 (limit: 4656)
     CGroup: /system.slice/squid.service
             ├─3064 /usr/local/squid/sbin/squid -f /usr/local/squid/etc/squid.conf
             ├─3066 (squid-1) --pid squid-1 -f /usr/local/squid/etc/squid.conf
             ├─3067 (security_file_certgen) -s /usr/local/squid/var/squid/ssl_db -M 20MB
             ├─3068 (security_file_certgen) -s /usr/local/squid/var/squid/ssl_db -M 20MB
             ├─3069 (security_file_certgen) -s /usr/local/squid/var/squid/ssl_db -M 20MB
             ├─3070 (security_file_certgen) -s /usr/local/squid/var/squid/ssl_db -M 20MB
             ├─3071 (security_file_certgen) -s /usr/local/squid/var/squid/ssl_db -M 20MB
             ├─3072 (logfile-daemon) /usr/local/squid/var/logs/access.log
             └─3073 (unlinkd)

Thg 11 19 22:54:13 ubuntu-VirtualBox systemd[1]: Starting Squid Web Proxy Server...
Thg 11 19 22:54:13 ubuntu-VirtualBox systemd[1]: Started Squid Web Proxy Server.
Thg 11 19 22:54:13 ubuntu-VirtualBox squid[3064]: Squid Parent: will start 1 kids
Thg 11 19 22:54:13 ubuntu-VirtualBox squid[3064]: Squid Parent: (squid-1) process 3066 started
ubuntu@ubuntu-VirtualBox:~$
```

Hình 16: Tình trạng Squid sau khi cấu hình SSL bump

Bước 5: Cấu hình lớp mạng 192.168.1.0/24

Định nghĩa ACL lớp mạng và cho phép mạng truy cập vào file cấu hình

```
acl localnetwork src 192.168.1.0/24
http_access allow localnetwork #đặt trên http_access deny all
```

```
GNU nano 2.9.3                                         /usr/local/squid/etc/squid.conf

#
# Recommended minimum configuration:
#
# Example rule allowing access from your local networks.
# Adapt to list your (internal) IP networks from where browsing
# should be allowed
# Define local network
acl localnetwork src 192.168.1.0/24
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
```

Hình 17: Định nghĩa mạng 192.168.1.0/24

```
http_access allow localnetwork
# And finally deny all other access to this proxy
http_access deny all
```

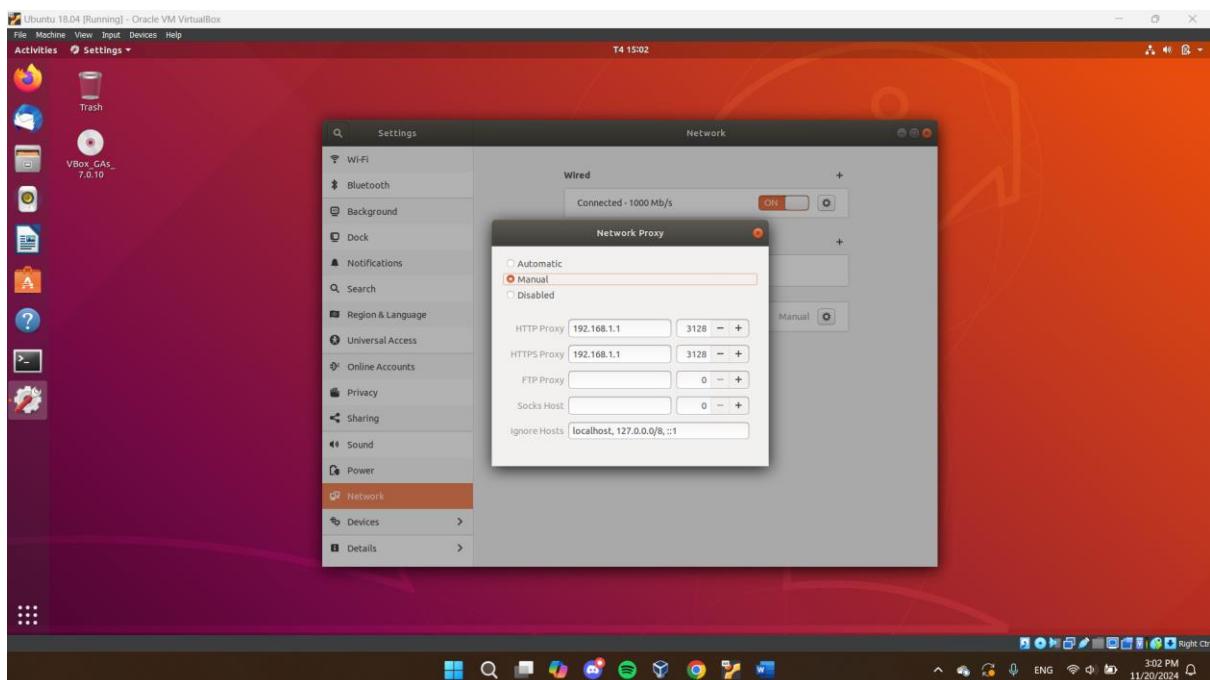
Hình 18: Cho phép truy cập từ mạng vừa định nghĩa

Thực hiện lệnh sudo systemctl status squid để áp dụng cấu hình.

4.3. Cấu hình Proxy trên Client

Cấu hình trong cài đặt Network

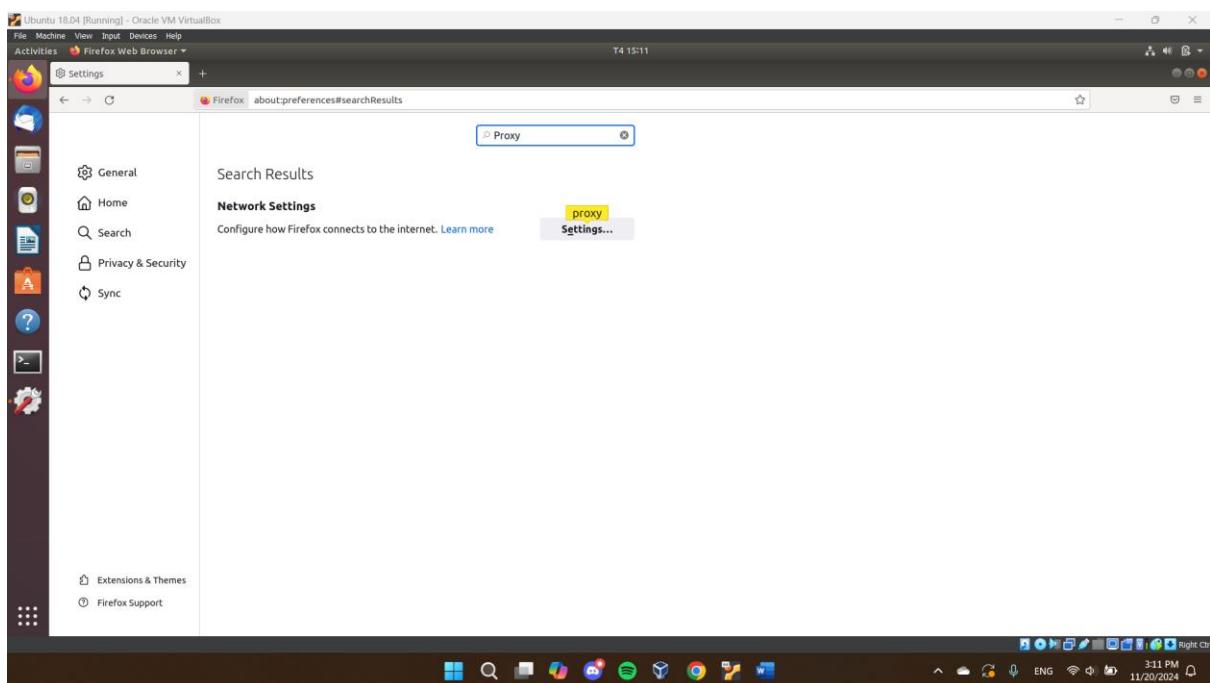
Vào **Settings > Network > Chọn Network Proxy > Chọn Manual > Nhập IP và port** (nếu không chỉnh port trong file cấu hình Squid thì mặc định là 3128) của Proxy Server vào HTTP Proxy và HTTPS Proxy



Hình 19: Cấu hình Proxy trong cài đặt Network

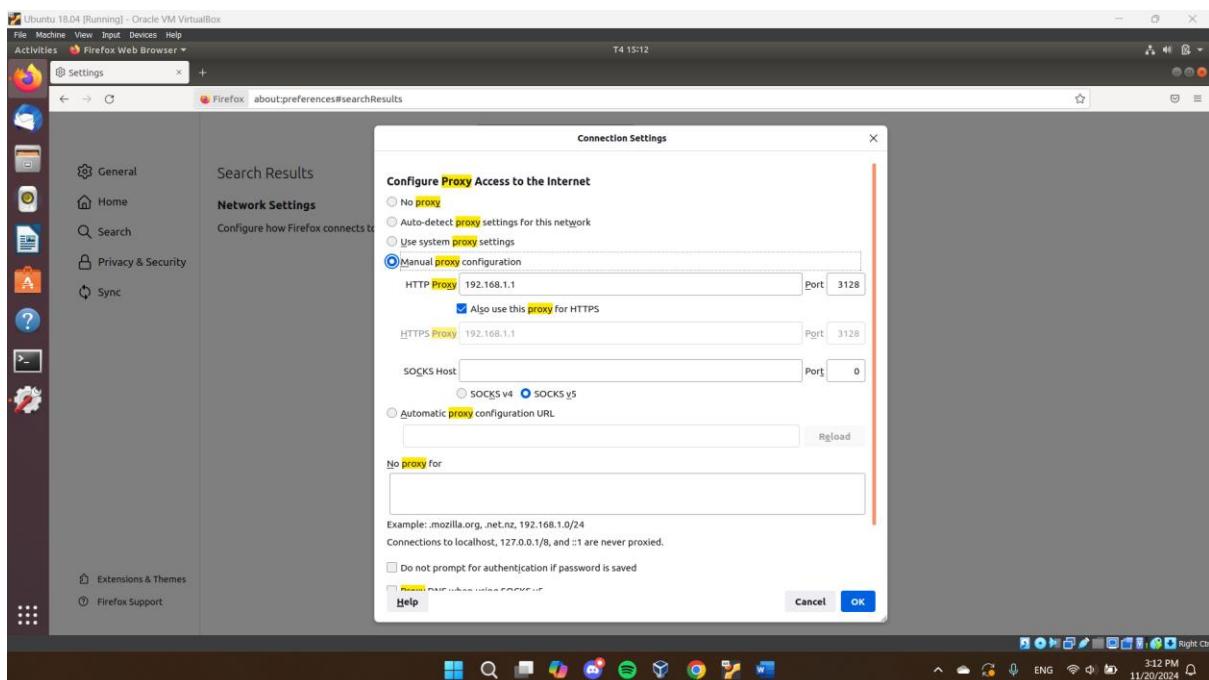
Cấu hình Proxy trong Trình duyệt (Firefox)

Vào Settings > Tìm kiếm Proxy



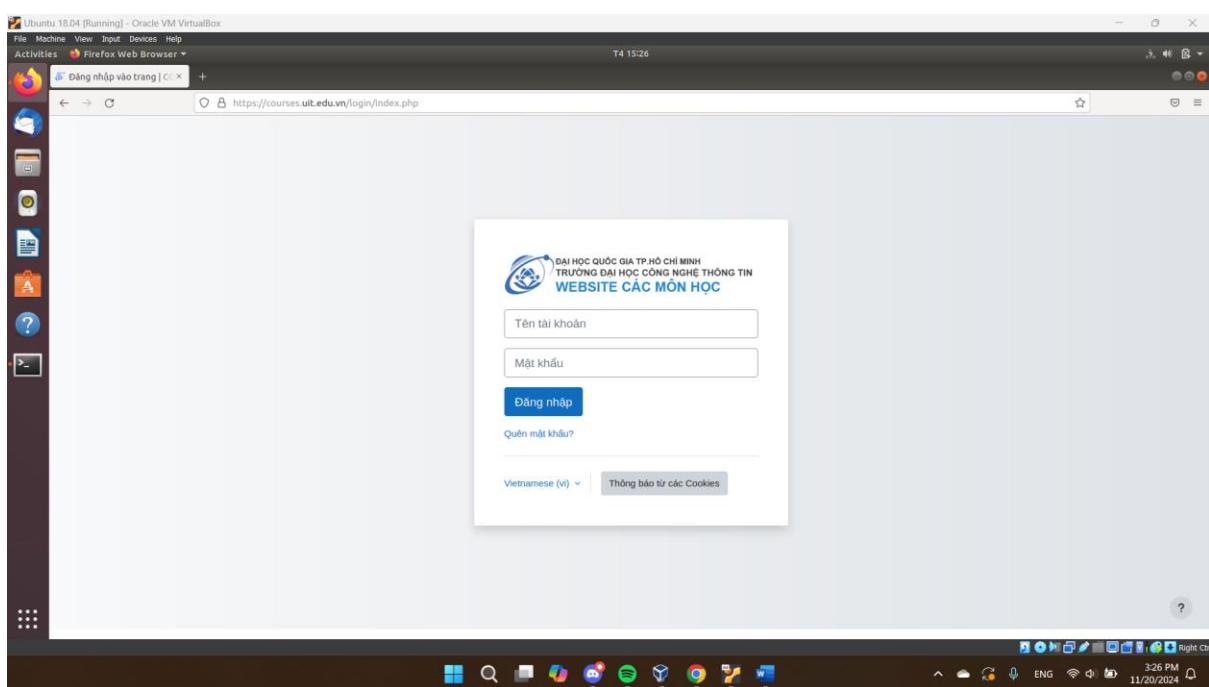
Hình 20: Cấu hình Proxy trong trình duyệt I

Vào Network Settings > Chọn Manual proxy configuration > Nhập IP và port của Proxy Server > Tích vào tùy chọn Also use this proxy for HTTPS



Hình 21: Cấu hình Proxy trong trình duyệt 2

Truy cập một trang web bất kì để kiểm tra



Hình 22: Kiểm tra sau khi cấu hình Proxy

→ Proxy hoạt động

4.4. Cấu hình các kịch bản

4.4.1. Kịch bản 1: Kiểm soát truy cập (Access Control) [5]

Mục tiêu: Giới hạn quyền truy cập vào các trang web cụ thể cho một nhóm người dùng trong mạng.

Mô tả kịch bản:

- Người dùng trong mạng con 192.168.1.0/24 sẽ chỉ được phép truy cập Internet trong giờ làm việc (từ 9:00 đến 18:00, tất cả các ngày trong tuần).
- Ngoài ra, họ sẽ không thể truy cập vào các trang web như Facebook và YouTube trong suốt thời gian làm việc.

Định nghĩa các ACL

Chặn truy cập theo thời gian:

Cú pháp: acl <name> time <days> <time-range>

- days: Sunday – S, Monday – M, Tuesday – T, Wednesday – W, Thursday – H, Friday – F, Saturday – A.

Chặn truy cập web theo tên miền:

Cú pháp: acl <acl_name> dstdomain "/path/to/file/blocked"

```
GNU nano 2.9.3                                         /usr/local/squid/etc/blacklist.txt

.facebook.com
.youtube.com
```

Hình 23: Nội dung file liệt kê tên miền bị chặn

Chặn truy cập vào facebook.com và youtube.com kể cả các tên miền phụ.

```
# Scenario 1: Access Control
## Access network in work hours 9:00-18:00 (Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, Saturday)
acl work_hours time SMTWHFA 09:00-18:00

## access denied to domain in blacklist
acl domain_blacklist dstdomain "/usr/local/squid/etc/blacklist.txt"
```

Hình 24: Định nghĩa các ACL

Áp dụng các acl vào mạng localnetwork

Cú pháp: http_access <deny|allow> <tên mạng> <acl_name>

```
# Adapt localnetwork in the ACL list
http_access deny localnetwork domain_blacklist
http_access allow localnetwork work_hours
#http_access allow localnetwork
# And finally deny all other access to this proxy
http_access deny all
```

Hình 25: Áp dụng ACL cho mạng localnetwork

4.4.2. Kịch bản 2: Caching [5]

Mục tiêu: Sử dụng tính năng **caching** của Squid Proxy để lưu trữ các nội dung thường xuyên truy cập từ Internet, giúp giảm thời gian tải và tăng tốc độ download của người dùng mạng nội bộ.

Mô tả kịch bản:

- Khi người dùng A tải một tài liệu lớn lần đầu tiên, file sẽ được tải từ Internet và Squid Proxy sẽ lưu nó vào bộ nhớ đệm (cache).
- Khi người dùng B (và các người dùng khác) yêu cầu tải xuống cùng tài liệu, Squid Proxy sẽ phục vụ file từ bộ nhớ đệm thay vì tải lại từ Internet.

Cú pháp:

```
cache_dir <type> <directory> <disk-size> <L1> <L2> [options]
```

- type: Kiểu lưu trữ cache (ví dụ: ufs, aufs, diskd, rock).
 - ufs: Hệ thống lưu trữ mặc định.
 - aufs: Giống với “ufs” nhưng tận dụng luồng POSIX để tránh chặn tiến trình Squid chính trên disk-IO.
 - diskd: Giống với “ufs” nhưng sử dụng một tiến trình riêng để tránh chặn tiến trình Squid chính trên disk-IO.
 - rock: Lưu trữ theo kiểu cơ sở dữ liệu. Tất cả các mục được lưu vào bộ nhớ đệm đều được chứa trong tập tin “database” và sử dụng một slot có kích thước cố định. Một mục duy nhất chiếm một hoặc nhiều slot.
- directory: Đường dẫn đến thư mục lưu cache.
- disk-size: Kích thước tối đa của cache trên đĩa, tính bằng MB.
- L1: Số thư mục con cấp 1 (layer 1) bên trong thư mục cache.
- L2: Số thư mục con cấp 2 (layer 2) bên trong mỗi thư mục cấp 1.
- [options]: Các tùy chọn bổ sung, không bắt buộc (ví dụ: no-store, min-size, max-size).

```
# Scenario 2: Caching
# Uncomment and adjust the following to add a disk cache directory.
minimum_object_size 0 KB
maximum_object_size 200 MB
cache_dir ufs /usr/local/squid/var/cache/squid 1000 16 256
```

Hình 26: Cấu hình caching

maximum_object_size và minimum_object_size dùng để quy định đối tượng có kích thước bao nhiêu thì được lưu vào cache.

Cấu hình đang áp dụng quy định đối tượng có kích thước lớn hơn 200MB sẽ không được lưu vào cache.

4.4.3. Kịch bản 3: Quản lý băng thông (Bandwidth management) [6]

Mục tiêu: Giới hạn băng thông cho một nhóm người dùng để tối ưu hóa việc sử dụng mạng.

Mô tả kịch bản:

- Người dùng trong mạng **192.168.1.0/24** bị giới hạn băng thông tổng là **64 KB/s** và mỗi kết nối cá nhân chỉ được phép sử dụng **16 KB/s**.
- Điều này giúp tránh tình trạng sử dụng quá mức băng thông và đảm bảo phân phối băng thông đồng đều cho mọi người dùng.

Cấu hình

Cú pháp: `delay_pools <number_of_pools>`

`delay_class <pool_number> <class_type>`

- class 1: Mọi thứ đều bị giới hạn bởi một bộ chứa tổng hợp duy nhất (aggregate bucket).
- class 2 Mọi thứ bị giới hạn bởi:
 - Một bộ chứa tổng hợp duy nhất (aggregate bucket).
 - Một bộ chứa "cá nhân" (individual bucket), được xác định từ các bit 25 đến 32 của địa chỉ IPv4.
- class 3: Mọi thứ bị giới hạn bởi:
 - Một bộ chứa tổng hợp duy nhất (aggregate bucket).
 - Một bộ chứa "mạng" (network bucket), được xác định từ các bit 17 đến 24 của địa chỉ IP.
 - Một bộ chứa "cá nhân" (individual bucket), được xác định từ các bit 17 đến 32 của địa chỉ IP.
- class 4: Giống lớp 3, nhưng bổ sung giới hạn theo từng người dùng dựa trên tài khoản.
- class 5: Các yêu cầu được nhóm lại theo thẻ (tag), được xác định thông qua phản hồi `tag=` từ ACL bên ngoài (external_acl).

`delay_parameters <pool_number> [options]`

Các options:

- **aggregate:** Các tham số giới hạn tốc độ cho bộ chứa tổng hợp (*aggregate bucket*) (*Áp dụng cho lớp 1, 2, 3*).
- **individual:** Các tham số giới hạn tốc độ cho các bộ chứa cá nhân (*individual buckets*) (*Áp dụng cho lớp 2, 3*).
- **network:** Các tham số giới hạn tốc độ cho các bộ chứa mạng (*network buckets*) (*Áp dụng cho lớp 3*).

- **user:** Các tham số giới hạn tốc độ cho các bộ chứa người dùng (*user buckets*) (*Áp dụng cho lớp 4*).
- **tagrate:** Các tham số giới hạn tốc độ cho các bộ chứa theo nhãn (*tag buckets*) (*Áp dụng cho lớp 5*).

Cập tham số delay_parameters viết dưới dạng restore/maximum:

- Restore (Tốc độ phục hồi): Là tốc độ mà băng thông được nạp lại vào "bucket" mỗi giây. Giá trị này quyết định tốc độ tối đa mà người dùng có thể nhận được tại bất kỳ thời điểm nào.
- Maximum (Dung lượng tối đa): Là dung lượng băng thông tối đa mà "bucket" có thể tích lũy được tại một thời điểm. Giá trị này quyết định lượng băng thông mà người dùng có thể tiêu thụ ngay lập tức mà không cần chờ phục hồi.

```
delay_access <pool_number> <allow|deny> <acl_name>
```

Trong kịch bản này, ta cần giới hạn băng thông cho toàn bộ mạng và mỗi người dùng nên sử dụng class 2 để cấu hình.

```
# Scenario 3: Bandwidth Management
delay_pools 1
delay_class 1 2
delay_parameters 1 64000/64000 16000/16000
delay_access 1 allow localnetwork
```

Hình 27: Cấu hình quản lý băng thông

4.4.4. Kịch bản 4: Ẩn danh người dùng (Anonymization) [6]

Mục tiêu: Sử dụng Squid Proxy để ẩn thông tin về người dùng (IP, headers) khi truy cập các trang web để bảo vệ quyền riêng tư.

Mô tả kịch bản:

- Proxy sẽ loại bỏ tất cả các thông tin có thể tiết lộ danh tính của người dùng khi gửi yêu cầu tới các trang web từ client.
- Người dùng truy cập qua proxy này sẽ có quyền riêng tư cao hơn, vì không có thông tin định danh nào của họ bị tiết lộ cho máy chủ web đích.

Cấu hình

```
# Scenario 4: Anonymization
# Disable header that exposes this request adapted by proxy
via off
# X-Forwarded-for: unknown
forwarded_for off
# Disable User-Agent header
request_header_access User-Agent deny localnetwork
```

Hình 28: Cấu hình ẩn danh người dùng

Cú pháp:

via <on|off>

Nếu được đặt là on, Squid sẽ thêm Via headers vào requests và response cho biết đã được chuyển tiếp qua proxy: Via: 1.1 ubuntu-VirtualBox (squid/4.10)

forwarded_for <on|off|transparent|delete|truncate>

- Nếu được đặt là "on", Squid sẽ thêm địa chỉ IP của máy khách của bạn vào các yêu cầu HTTP mà nó chuyển tiếp. Mặc định, nó sẽ xuất hiện như sau: X-Forwarded-For: 192.1.2.3
- Nếu được đặt là "off", nó sẽ xuất hiện dưới dạng: X-Forwarded-For: unknown
- Nếu được đặt là "transparent", Squid sẽ không thay đổi tiêu đề X-Forwarded-For theo bất kỳ cách nào.
- Nếu được đặt là "delete", Squid sẽ xóa toàn bộ tiêu đề X-Forwarded-For.
- Nếu được đặt là "truncate", Squid sẽ xóa tất cả các mục hiện có trong tiêu đề X-Forwarded-For và chỉ đặt địa chỉ IP của máy khách làm mục duy nhất.

request_header_access <header_name> <allow|deny> <acl_name>

Kiểm soát việc chấp nhận hoặc từ chối các HTTP header từ các yêu cầu HTTP mà Squid nhận được

4.4.5. Kịch bản 5: Giám Sát và Ghi Log Hoạt Động Người Dùng

Mục tiêu: Sử dụng Squid Proxy để ghi lại toàn bộ hoạt động truy cập web của người dùng nhằm giám sát và phân tích, giúp tăng cường kiểm soát và bảo mật trong hệ thống mạng.

Mô tả kịch bản:

- Một công ty cần giám sát hoạt động truy cập Internet của nhân viên để đảm bảo rằng họ không sử dụng thời gian làm việc cho các hoạt động cá nhân hoặc các trang web không liên quan đến công việc.
- Quản trị viên mạng muốn biết các trang web nào được truy cập, thời gian truy cập, và thông tin chi tiết về việc truy cập như kích thước dữ liệu tải lên hoặc tải xuống.

Squid Proxy cung cấp các tệp log để giám sát hoạt động của proxy, giúp quản trị viên theo dõi, phân tích và khắc phục sự cố. Các tệp log chính trong Squid bao gồm:

- **access.log:** Ghi lại chi tiết tất cả các yêu cầu HTTP mà Squid xử lý. Đây là tệp log quan trọng nhất để theo dõi lưu lượng truy cập qua proxy.
- **cache.log:** Ghi lại các sự kiện liên quan đến hoạt động của Squid, chẳng hạn như lỗi, cảnh báo, khởi động, cấu hình hoặc các thông tin gỡ lỗi.

```
ubuntu@ubuntu-VirtualBox:/usr/local/squid/var/logs$ ls
access.log  cache.log
ubuntu@ubuntu-VirtualBox:/usr/local/squid/var/logs$
```

Hình 29: Các file log của Squid

Sử dụng lệnh: sudo tail -f /path/to/file/log để hiển thị các dòng mới được thêm vào khi tệp cập nhật.

```
ubuntu@ubuntu-VirtualBox:/usr/local/squid/var/logs$ sudo tail -f access.log
[sudo] password for ubuntu:
[20/Nov/2024:17:15:04 +0700.979   69 192.168.1.101 TCP_MISS/200 237 GET https://safebrowsing.googleapis.com/v4/threatListUpdates:fetch? - HIER_DIRECT/142.250.76.10 ap
plcation/x-protobuf "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:92.0) Gecko/201001 Firefox/92.0"
[20/Nov/2024:17:26:05 +0700.622   88 192.168.1.101 NONE/200 0 CONNECT contile.services.mozilla.com:443 - HIER_DIRECT/34.117.188.166 - "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:92.0) Gecko/201001 Firefox/92.0"
[20/Nov/2024:17:26:06 +0700.806   175 192.168.1.101 TCP_MISS/403 218 GET https://contile.services.mozilla.com/v1/tiles - HIER_DIRECT/34.117.188.166 - "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:92.0) Gecko/201001 Firefox/92.0"
[20/Nov/2024:17:33:43 +0700.893   137 192.168.1.101 NONE/200 0 CONNECT push.services.mozilla.com:443 - HIER_DIRECT/34.107.243.93 - "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:92.0) Gecko/201001 Firefox/92.0"
[20/Nov/2024:17:33:43 +0700.263   162 192.168.1.101 TCP_MISS/500 344 GET https://push.services.mozilla.com/ - HIER_DIRECT/34.107.243.93 application/json "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:92.0) Gecko/201001 Firefox/92.0"
[20/Nov/2024:17:41:05 +0700.675   92 192.168.1.101 NONE/200 0 CONNECT contile.services.mozilla.com:443 - HIER_DIRECT/34.117.188.166 - "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:92.0) Gecko/201001 Firefox/92.0"
[20/Nov/2024:17:41:05 +0700.856   167 192.168.1.101 TCP_MISS/403 218 GET https://contile.services.mozilla.com/v1/tiles - HIER_DIRECT/34.117.188.166 - "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:92.0) Gecko/201001 Firefox/92.0"
[20/Nov/2024:17:41:05 +0700.466   91 192.168.1.101 NONE/200 0 CONNECT safebrowsing.googleapis.com:443 - HIER_DIRECT/142.251.10.95 - "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:92.0) Gecko/201001 Firefox/92.0"
[20/Nov/2024:17:45:35 +0700.463   48 192.168.1.101 TCP_MISS/200 7556 GET https://safebrowsing.googleapis.com/v4/threatListUpdates:fetch? - HIER_DIRECT/142.251.10.95 ap
plcation/x-protobuf "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:92.0) Gecko/201001 Firefox/92.0"
[20/Nov/2024:21:19:06 +0700.805   3 192.168.1.101 TCP_DENIED/200 0 CONNECT extensions.gnome.org:443 - HIER_NONE/- - "gnome-software/3.28.1"
```

Hình 30: Nội dung file access.log

```
ubuntu@ubuntu-VirtualBox:/usr/local/squid/var/logs$ sudo tail -f cache.log
2024/11/20 21:15:42 kid1|          0 Objects cancelled.
2024/11/20 21:15:42 kid1|          0 Duplicate URLs purged.
2024/11/20 21:15:42 kid1|          0 Swapfile clashes avoided.
2024/11/20 21:15:42 kid1| Took 0.03 seconds ( 0.00 objects/sec).
2024/11/20 21:15:42 kid1| Beginning Validation Procedure
2024/11/20 21:15:42 kid1| Completed Validation Procedure
2024/11/20 21:15:42 kid1| Validated 0 Entries
2024/11/20 21:15:42 kid1| store_swap_size = 0.00 KB
2024/11/20 21:15:43 kid1| storeLateRelease: released 0 objects
security_file_certgen helper database '/usr/local/squid/var/squid/ssl_db' failed: Failed to open file /usr/local/squid/var/squid/ssl_db/index.txt
```

Hình 31: Nội dung file cache.log

Ngoài ra, có thể tùy chỉnh log format bằng cách thêm các câu lệnh:

```
logformat <name> <format specification>
access_log <module>:<place> [<logformat name> [acl acl ...]]
```

```
# Scenario 5: Log
# reference: https://www.squid-cache.org/Doc/config/logformat/
logformat custom_log $tl.%03tu %>a %Ss/%03-Hs %<t %rm %ru %un %Sh/%<a %mt "%{User-Agent}>h"
# tl - Local time; tu - subsecond time(ms); tr - response time (ms); >a - Client source IP; Ss-Squid request status (etc TCP_MISS);
# >Hs-HTTP status code sent to the client; <t - Total size of reply sent to client (after adaptation)
# rm - Request method; ru - Request URL received; un - Username; Sh - Squid hierarchy status; <a-Server IP address of the last server or peer connection
# mt-MIME (Multipurpose Internet Mail Extensions) content type; >h - Original received request header
access_log daemon:/usr/local/squid/var/logs/access.log custom_log
```

Hình 32: Cấu hình log format

4.5. Cấu hình FTP

Định nghĩa acl để cho phép các kết nối đến port 21 (FTP)

Cú pháp: acl <acl name> port 21

Và áp dụng acl đã được định nghĩa

Cú pháp :

```
http_access allow <acl name> hoặc
```

```
http_access deny !<acl name>
```

```
acl Safe_ports port 21 # ftp
```

Hình 33: Ví dụ định nghĩa access list port 21

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

Hình 34: Ví dụ áp dụng access list đã định nghĩa

Định nghĩa người dùng để xác thực với máy chủ FTP

Cú pháp: ftp_user user:password

```
ftp_user kali:kali
```

Hình 35: Ví dụ định nghĩa người dùng FTP

4.6. Cấu hình Transparent Proxy

Cài đặt Squid với tùy chọn configure ‘--enable-linux-netfilter’

Chuyển chế độ của squid sang transparent mode

```
http_port 3128 intercept
```

```
https_port 3129 intercept ssl-bump \
    generate-host-certificates=on \
    dynamic_cert_mem_cache_size=20MB \
    cert=/usr/local/squid/etc/ssl_cert/bump.pem \
    key=/usr/local/squid/etc/ssl_cert/bump.key
    options=NO_SSLv3
```

```
http_port 3130
```

http_port dùng để xử lý http request

https_port dùng để xử lý https request

Squid yêu cầu phải luôn có một cổng lắng nghe không phải ở chế độ transparent nên nhóm đã sử dụng port 3130.

Cấu hình firewall để chuyển hướng traffic HTTP và HTTPS sang port của Squid

```
iptables -t nat -A PREROUTING -s <địa chỉ mạng local> \
```

```
-p tcp -m tcp --dport 443 -j REDIRECT --to-port 3129  
iptables -t nat -A PREROUTING -s <địa chỉ mạng local> \  
-p tcp -m tcp --dport 80 -j REDIRECT --to-port 3128
```

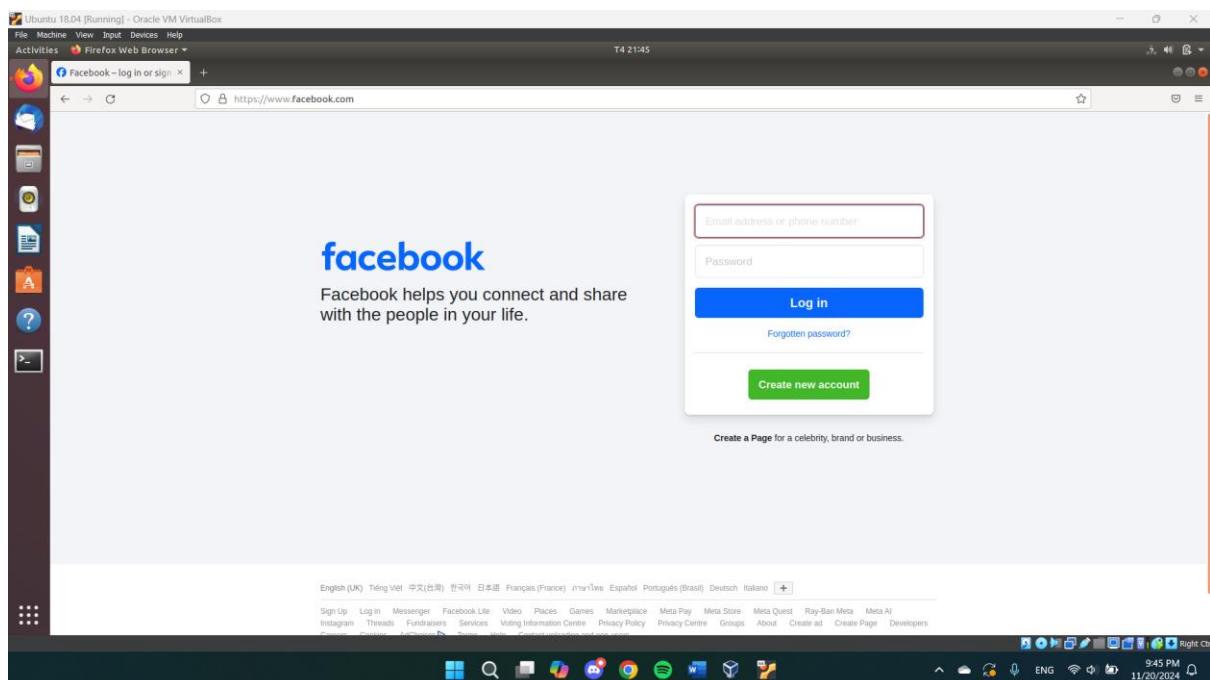
Để client có thể ra internet thì firewall trên gateway phải cho phép các port 3128, 3129 và các port cần thiết khác như 80, 443, 53.

Firewall cũng cần có rule để NAT IP của mạng local sang IP public.

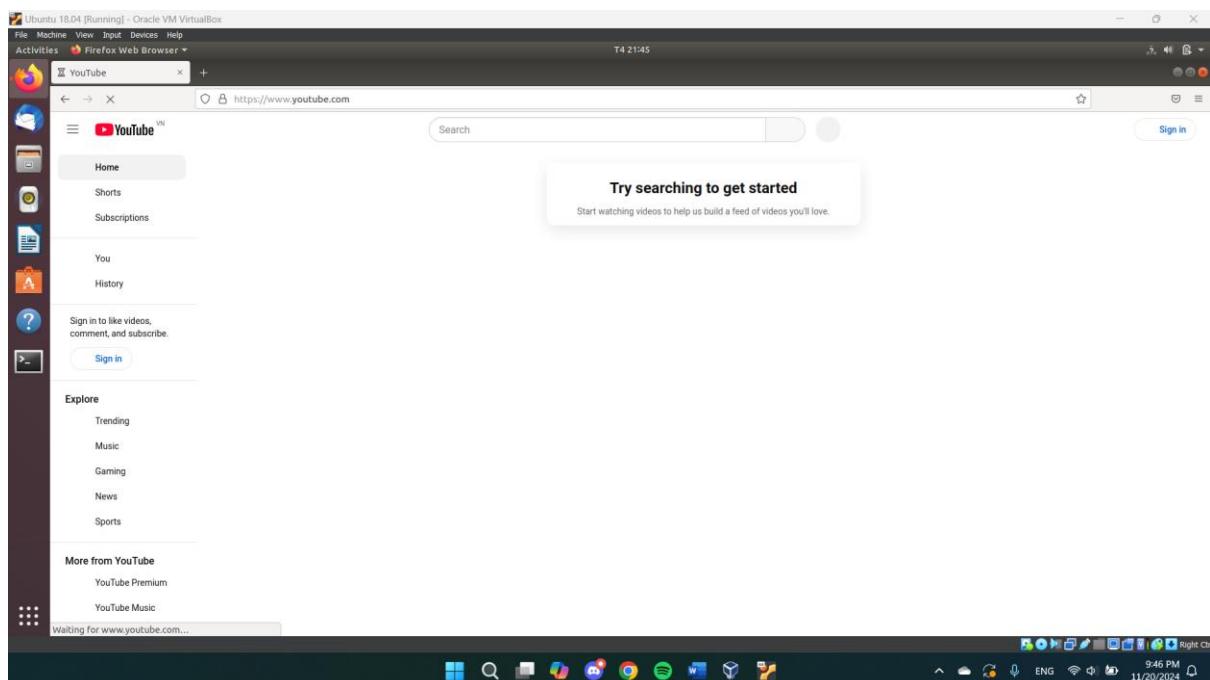
CHƯƠNG 5: THỰC NGHIỆM ĐỀ TÀI

5.1. Kịch bản 1: Kiểm soát truy cập (Access Control)

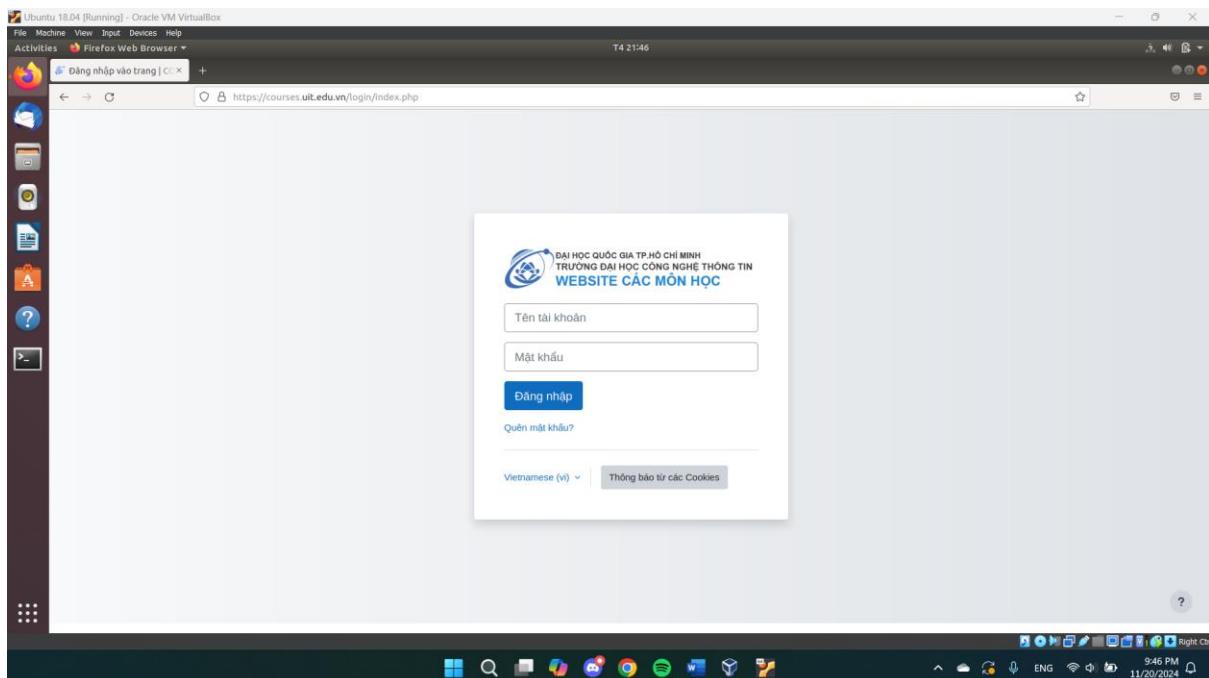
Truy cập trước khi cấu hình vào lúc 21:45:



Hình 36: Truy cập Facebook trước khi cấu hình

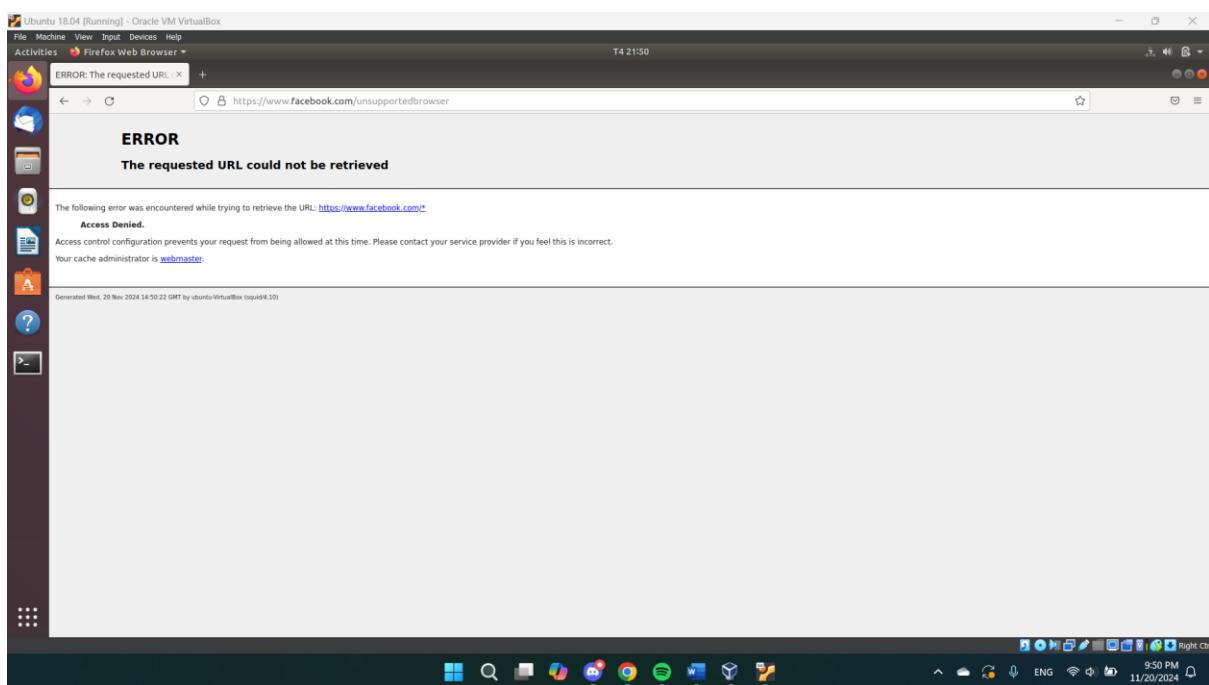


Hình 37: Truy cập Youtube trước khi cấu hình

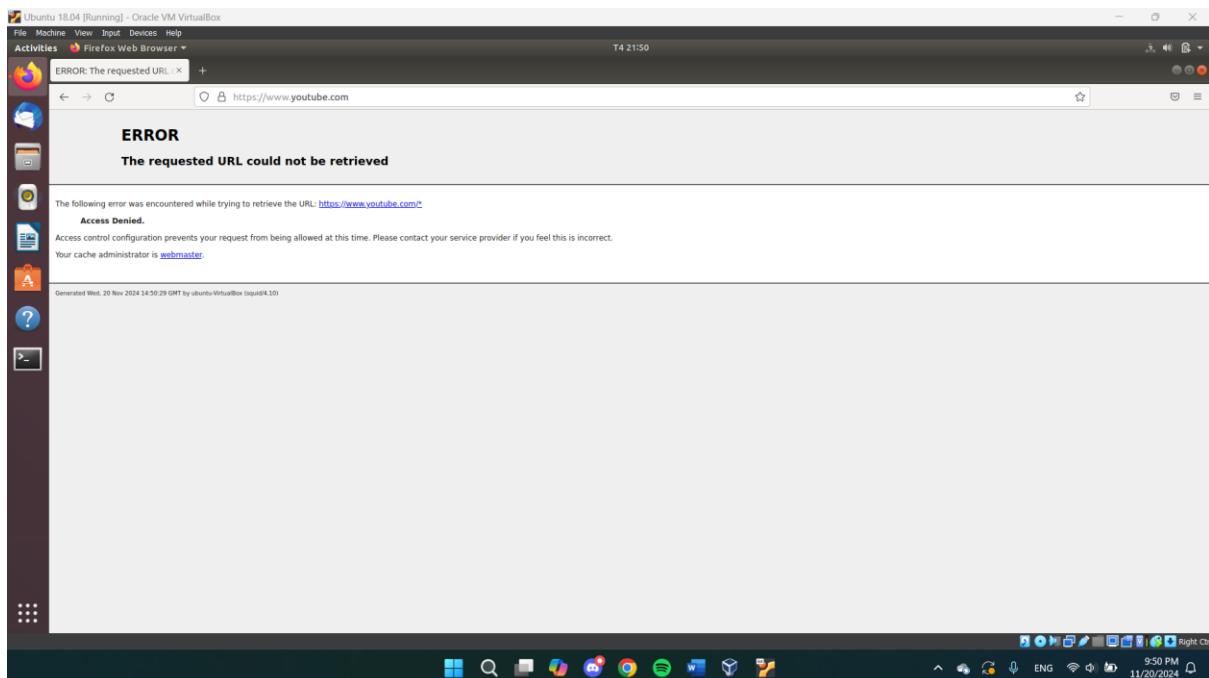


Hình 38: Truy cập Web không bị chặn trước khi cấu hình

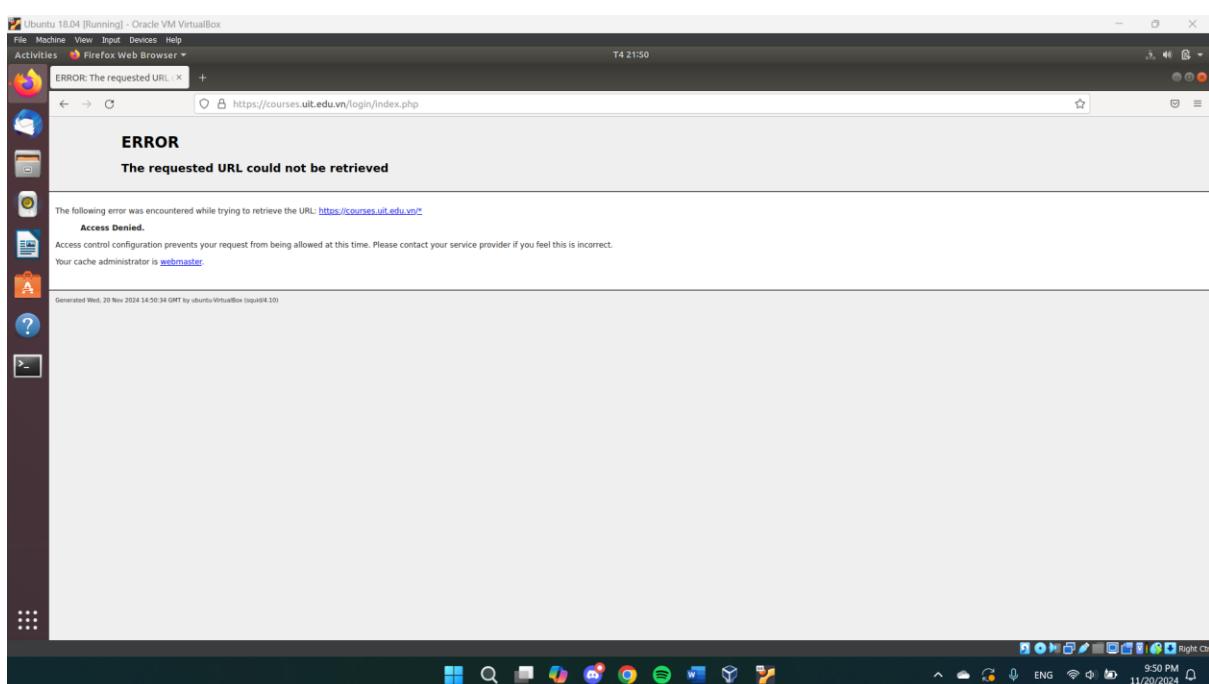
Truy cập sau khi thực hiện cấu hình lúc 21:49 (Ngoài thời gian cho phép truy cập):



Hình 39: Truy cập Facebook sau khi cấu hình ngoài thời gian cho phép

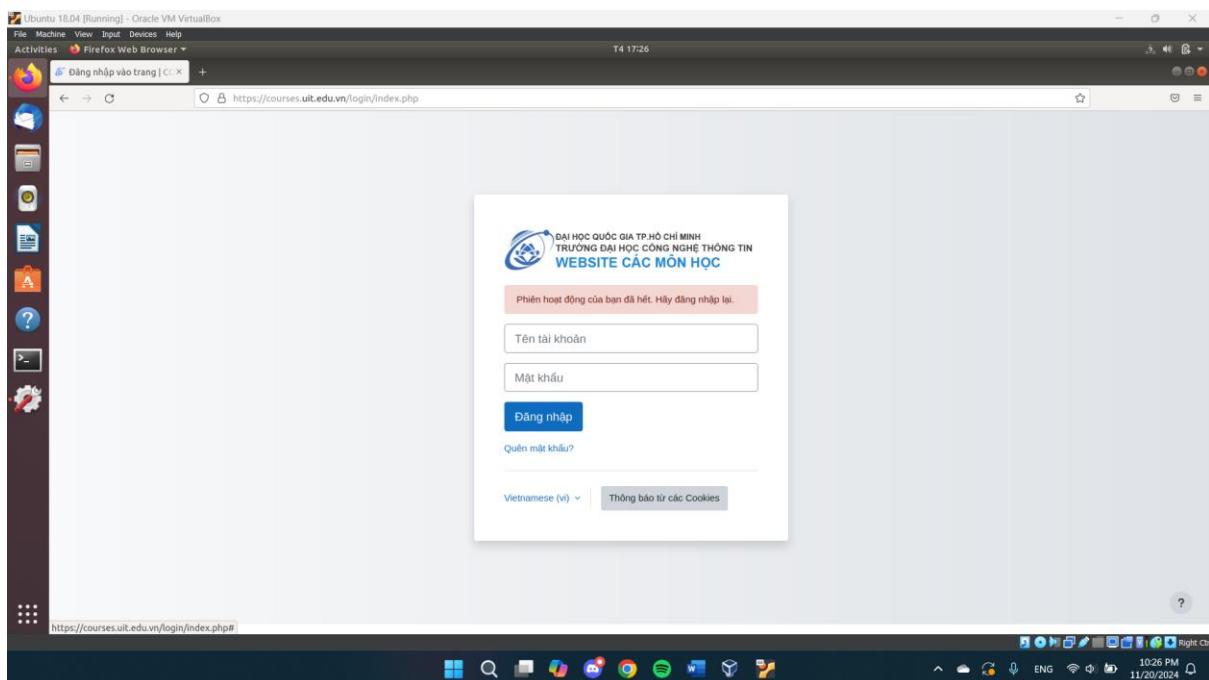


Hình 40: Truy cập Youtube sau khi cấu hình ngoài thời gian cho phép

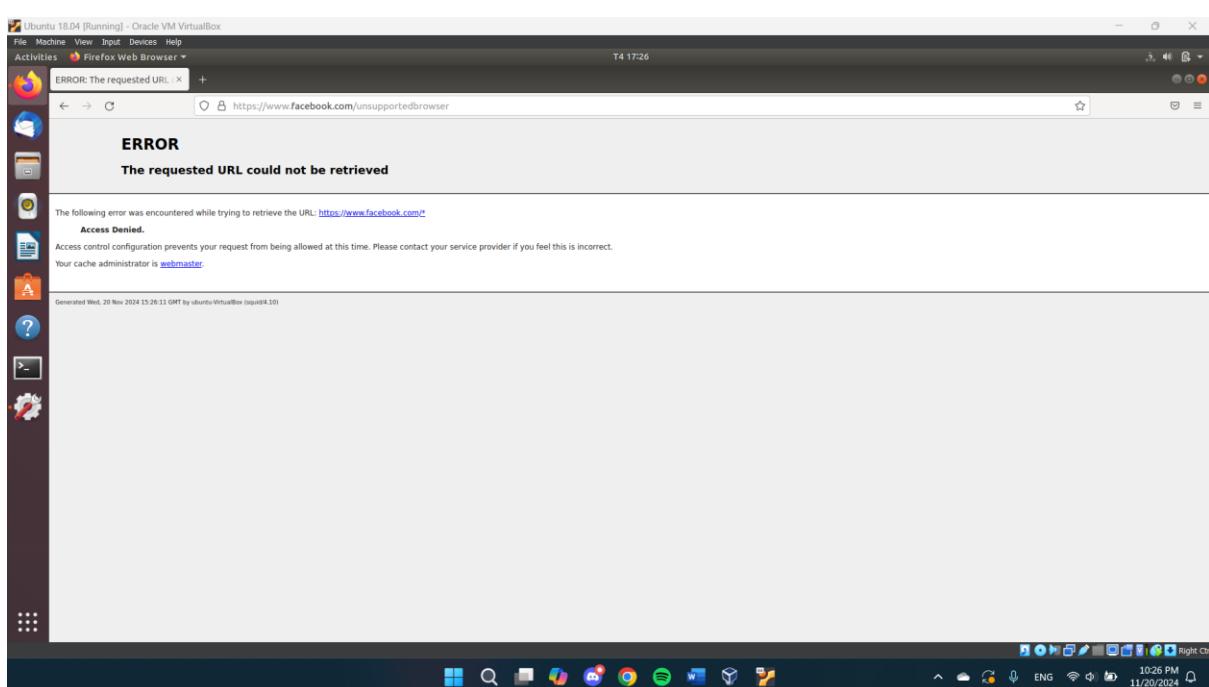


Hình 41: Truy cập Web không bị chặn sau khi cấu hình ngoài thời gian cho phép

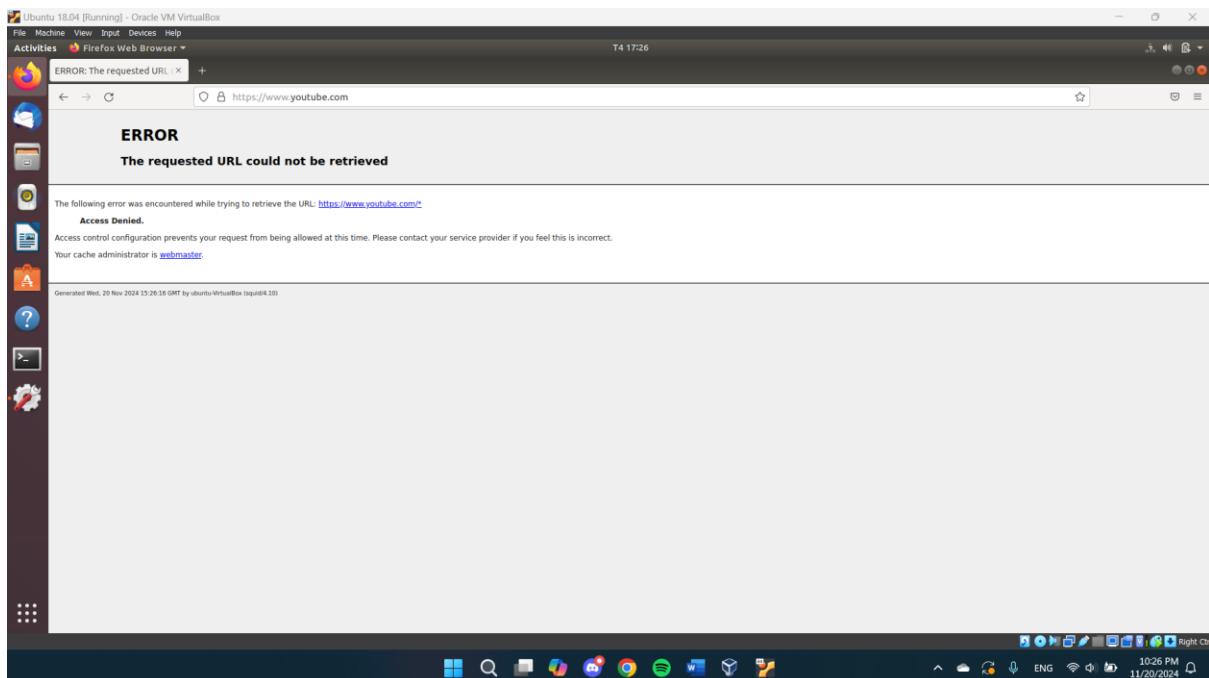
Thực hiện truy cập sau khi cấu hình lúc **17:25 (Trong thời gian cho phép truy cập)**:



Hình 42: Truy cập Web không bị chặn sau khi cấu hình trong thời gian cho phép



Hình 43: Truy cập Facebook sau khi cấu hình trong thời gian cho phép



Hình 44: Truy cập Youtube sau khi cấu hình trong thời gian cho phép

5.2. Kịch bản 2: Caching

Thực hiện tải một file pdf 35MB trên client 1:

```
zasure69@ubuntu1804:~$ curl -o -L "https://cbqluz9dtwobj.vcdn.cloud/PUBLIC/MEDIA/CambridgeIELTS_16_Academic_b9f737c819.pdf" -x "http://192.168.1.1:3128" -k
% Total    % Received % Xferd  Average Speed   Time   Time  Current
          Dload  Upload   Total Spent   Left  Speed
100 35.0M  100 35.0M    0     0  3179k      0  0:00:11  0:00:11  --:--:-- 3691k
```

Hình 45: Tải file trên client 1

Thực hiện tải một file pdf 35MB trên client2 sau khi tải trên client1:

```
zasure69-2@ubuntu1804:~$ curl -o -L "https://cbqluz9dtwobj.vcdn.cloud/PUBLIC/MEDIA/CambridgeIELTS_16_Academic_b9f737c819.pdf" -x "http://192.168.1.1:3128" -k
% Total    % Received % Xferd  Average Speed   Time   Time  Current
          Dload  Upload   Total Spent   Left  Speed
100 35.0M  100 35.0M    0     0  73.8M      0  --:--:--  --:--:-- 73.7M
zasure69-2@ubuntu1804:~$
```

Hình 46: Tải file trên client 2

Tốc độ tải của client 2 sau khi được cache lớn hơn rất nhiều so với client 1, và tốc độ tải nhanh hơn.

Thực hiện tải một file pdf từ server test trên client 1:

```
zasure69@ubuntu1804:~$ curl -o -L http://192.168.100.73:8000/test.pdf -x http://192.168.1.1:3128
% Total    % Received % Xferd  Average Speed   Time   Time  Current
          Dload  Upload   Total Spent   Left  Speed
100 35.0M  100 35.0M    0     0  61.7M      0  --:--:--  --:--:-- 61.7M
zasure69@ubuntu1804:~$
```

Hình 47: Tải file từ server test trên client 1

Quan sát log server:

The screenshot shows two terminal windows side-by-side. The left window is titled 'kali [Running] - Oracle VM VirtualBox' and shows a user running 'python3 simple_server.py' on port 8000, with a log message indicating a GET request for '/test.pdf'. The right window is titled 'kali@kali:~/storage/server_test' and shows the command 'tail -f server.log' being run, displaying a continuous stream of log entries from November 17, 2024, at 09:24:25.313 to November 20, 2024, at 10:47:14.945. The logs detail multiple requests for '/test.pdf' from various clients, including one from 'curl/7.58.0' and another from 'ubuntu-VirtualBox (squid/4.10)'. The desktop environment includes a taskbar with icons for file manager, browser, terminal, and system status.

Hình 48: Log của Server khi client 1 tải file

Proxy đã gửi một request GET đến server.

Thực hiện tải trên client 2:

```
zasure69-2@ubuntu1804:~$ curl -o -L http://192.168.100.73:8000/test.pdf -x http://192.168.1.1:3128
% Total    % Received % Xferd  Average Speed   Time   Time     Current
          Dload  Upload   Total Spent  Left Speed
100 35.0M  100 35.0M    0      0  172M      0 --:--:-- --:--:-- 172M
zasure69-2@ubuntu1804:~$
```

Hình 49: Tải file từ server test trên client 2

Server không nhận được request từ Proxy → Proxy gửi lại response từ cache.

The screenshot shows two terminal windows side-by-side. The left window displays a command-line session where a simple HTTP server is running on port 8000, serving a PDF file. The right window shows the log file for this server, detailing multiple requests from a client over several days, illustrating how the server handles repeated requests after caching.

Hình 50: Log của Server khi client 2 tải file

Bảng thống kê tốc độ, thời gian tải trước và sau khi cache:

Kích thước file	Tốc độ tải trước khi cache	Thời gian tải trước khi cache	Tốc độ tải sau khi cache	Thời gian tải sau khi cache
285KB	54,4 MB/s	0,005s	65,3 MB/s	0,004s
1MB	64 MB/s	0,02s	56,8 MB/s	0,02s
10MB	82,2 MB/s	0,1s	117 MB/s	0,08s
50MB	76,1 MB/s	0,6s	142 MB/s	0,3s
100MB	77,6 MB/s	1,3s	316 MB/s	0,3s
400MB	78,7 MB/s	5,1s	175 MB/s	2,3s
800MB	73,9 MB/s	11s	280 MB/s	2,9s

→ Kích thước file nhỏ có tốc độ, thời gian tải trước và sau khi cache không chênh lệnh nhiều, nhưng khi kích thước file càng lớn thì tốc độ, thời gian tải sau khi cache nhanh hơn nhiều so với trước khi cache.

```
zasure69@ubuntu1804:~$ wget http://192.168.100.18:8000/285kb.txt
--2024-12-08 21:29:14-- http://192.168.100.18:8000/285kb.txt
Connecting to 192.168.1.1:3128... connected.
Proxy request sent, awaiting response... 200 OK
Length: 291056 (284K) [text/plain]
Saving to: '285kb.txt'

285kb.txt          100%[=====] 284,23K  --.-KB/s   in 0,005s

2024-12-08 21:29:14 (54,4 MB/s) - '285kb.txt' saved [291056/291056]
```

Hình 51: Tải file 258KB trước khi cache

```
zasure69@ubuntu1804:~$ wget http://192.168.100.18:8000/1mb.txt
--2024-12-08 21:32:04-- http://192.168.100.18:8000/1mb.txt
Connecting to 192.168.1.1:3128... connected.
Proxy request sent, awaiting response... 200 OK
Length: 1143714 (1,1M) [text/plain]
Saving to: '1mb.txt'

1mb.txt          100%[=====] 1,09M  --.-KB/s   in 0,02s

2024-12-08 21:32:04 (68,0 MB/s) - '1mb.txt' saved [1143714/1143714]
```

Hình 52: Tải file 1MB trước khi cache

```
zasure69@ubuntu1804:~$ wget http://192.168.100.18:8000/10mb.txt
--2024-12-08 21:43:21-- http://192.168.100.18:8000/10mb.txt
Connecting to 192.168.1.1:3128... connected.
Proxy request sent, awaiting response... 200 OK
Length: 10293426 (9,8M) [text/plain]
Saving to: '10mb.txt'

10mb.txt         100%[=====] 9,82M  --.-KB/s   in 0,1s

2024-12-08 21:43:21 (82,2 MB/s) - '10mb.txt' saved [10293426/10293426]
```

Hình 53: Tải file 10MB trước khi cache

```
zasure69@ubuntu1804:~$ wget http://192.168.100.18:8000/50mb.txt
--2024-12-08 21:44:54-- http://192.168.100.18:8000/50mb.txt
Connecting to 192.168.1.1:3128... connected.
Proxy request sent, awaiting response... 200 OK
Length: 51770257 (49M) [text/plain]
Saving to: '50mb.txt'

50mb.txt         100%[=====] 49,37M  76,1MB/s   in 0,6s

2024-12-08 21:44:55 (76,1 MB/s) - '50mb.txt' saved [51770257/51770257]
```

Hình 54: Tải file 50MB trước khi cache

```
zasure69@ubuntu1804:~$ wget http://192.168.100.18:8000/100mb.txt
--2024-12-08 21:46:32-- http://192.168.100.18:8000/100mb.txt
Connecting to 192.168.1.1:3128... connected.
Proxy request sent, awaiting response... 200 OK
Length: 103540514 (99M) [text/plain]
Saving to: '100mb.txt'

100mb.txt        100%[=====] 98,74M  77,6MB/s   in 1,3s

2024-12-08 21:46:34 (77,6 MB/s) - '100mb.txt' saved [103540514/103540514]
```

Hình 55: Tải file 100MB trước khi cache

```
zasure69@ubuntu1804:~$ wget http://192.168.100.18:8000/400mb.txt
--2024-12-08 21:47:51-- http://192.168.100.18:8000/400mb.txt
Connecting to 192.168.1.1:3128... connected.
Proxy request sent, awaiting response... 200 OK
Length: 422480274 (403M) [text/plain]
Saving to: '400mb.txt'

400mb.txt          100%[=====] 402,91M 79,6MB/s    in 5,1s

2024-12-08 21:47:56 (78,7 MB/s) - '400mb.txt' saved [422480274/422480274]
```

Hình 56: Tải file 400MB trước khi cache

```
zasure69@ubuntu1804:~$ wget http://192.168.100.18:8000/800mb.txt
--2024-12-08 21:49:00-- http://192.168.100.18:8000/800mb.txt
Connecting to 192.168.1.1:3128... connected.
Proxy request sent, awaiting response... 200 OK
Length: 844960546 (806M) [text/plain]
Saving to: '800mb.txt'

800mb.txt          100%[=====] 805,82M 76,5MB/s    in 11s

2024-12-08 21:49:10 (73,9 MB/s) - '800mb.txt' saved [844960546/844960546]
```

Hình 57: Tải file 800MB trước khi cache

```
zasure69-2@ubuntu1804:~$ wget http://192.168.100.18:8000/285kb.txt
--2024-12-08 22:14:35-- http://192.168.100.18:8000/285kb.txt
Connecting to 192.168.1.1:3128... connected.
Proxy request sent, awaiting response... 200 OK
Length: 291056 (284K) [text/plain]
Saving to: '285kb.txt'

285kb.txt          100%[=====] 284,23K  ---KB/s    in 0,004s

2024-12-08 22:14:35 (65,3 MB/s) - '285kb.txt' saved [291056/291056]
```

Hình 58: Tải file 285KB sau khi cache

```
zasure69-2@ubuntu1804:~$ wget http://192.168.100.18:8000/1mb.txt
--2024-12-08 22:15:02-- http://192.168.100.18:8000/1mb.txt
Connecting to 192.168.1.1:3128... connected.
Proxy request sent, awaiting response... 200 OK
Length: 1143714 (1,1M) [text/plain]
Saving to: '1mb.txt'

1mb.txt          100%[=====] 1,09M  ---KB/s    in 0,02s

2024-12-08 22:15:02 (56,8 MB/s) - '1mb.txt' saved [1143714/1143714]
```

Hình 59: Tải file 1MB sau khi cache

```
zasure69-2@ubuntu1804:~$ wget http://192.168.100.18:8000/10mb.txt
--2024-12-08 22:15:56-- http://192.168.100.18:8000/10mb.txt
Connecting to 192.168.1.1:3128... connected.
Proxy request sent, awaiting response... 200 OK
Length: 10293426 (9,8M) [text/plain]
Saving to: '10mb.txt'

10mb.txt          100%[=====] 9,82M  -.- KB/s   in 0,08s

2024-12-08 22:15:56 (117 MB/s) - '10mb.txt' saved [10293426/10293426]
```

Hình 60: Tải file 10MB sau khi cache

```
zasure69-2@ubuntu1804:~$ wget http://192.168.100.18:8000/50mb.txt
--2024-12-08 22:16:04-- http://192.168.100.18:8000/50mb.txt
Connecting to 192.168.1.1:3128... connected.
Proxy request sent, awaiting response... 200 OK
Length: 51770257 (49M) [text/plain]
Saving to: '50mb.txt'

50mb.txt          100%[=====] 49,37M  142MB/s   in 0,3s

2024-12-08 22:16:04 (142 MB/s) - '50mb.txt' saved [51770257/51770257]
```

Hình 61: Tải file 50MB sau khi cache

```
zasure69-2@ubuntu1804:~$ wget http://192.168.100.18:8000/100mb.txt
--2024-12-08 22:16:10-- http://192.168.100.18:8000/100mb.txt
Connecting to 192.168.1.1:3128... connected.
Proxy request sent, awaiting response... 200 OK
Length: 103540514 (99M) [text/plain]
Saving to: '100mb.txt'

100mb.txt          100%[=====] 98,74M  316MB/s   in 0,3s

2024-12-08 22:16:11 (316 MB/s) - '100mb.txt' saved [103540514/103540514]
```

Hình 62: Tải file 100MB sau khi cache

```
zasure69-2@ubuntu1804:~$ wget http://192.168.100.18:8000/400mb.txt
--2024-12-08 22:16:16-- http://192.168.100.18:8000/400mb.txt
Connecting to 192.168.1.1:3128... connected.
Proxy request sent, awaiting response... 200 OK
Length: 422480274 (403M) [text/plain]
Saving to: '400mb.txt'

400mb.txt          100%[=====] 402,91M  175MB/s   in 2,3s

2024-12-08 22:16:18 (175 MB/s) - '400mb.txt' saved [422480274/422480274]
```

Hình 63: Tải file 400MB sau khi cache

```
zasure69@ubuntu1804:~$ wget http://192.168.100.18:8000/800mb.txt
--2024-12-08 22:16:21--  http://192.168.100.18:8000/800mb.txt
Connecting to 192.168.1.1:3128... connected.
Proxy request sent, awaiting response... 200 OK
Length: 844960546 (806M) [text/plain]
Saving to: '800mb.txt'

800mb.txt          100%[=====] 805,82M   280MB/s    in 2,9s

2024-12-08 22:16:24 (280 MB/s) - '800mb.txt' saved [844960546/844960546]
```

Hình 64: Tải file 800MB sau khi cache

5.3. Kịch bản 3: Quản lý băng thông (Bandwidth Management)

Thực hiện tải một file khi chưa cấu hình:

```
zasure69@ubuntu1804:~$ curl -O -L "https://cbqluz9dtwobj.vcdn.cloud/PUBLIC/MEDIA/CambridgeIELTS_16_Academic_b9f737c819.pdf" -x "http://192.168.1.1:3128" -k
% Total % Received % Xferd Average Speed Time Time Time Current
          Dload Upload Total Spent Left Speed
100 35.0M 100 35.0M 0     0 4445k 0 0:00:08 0:00:08 --:--:-- 4557k
zasure69@ubuntu1804:~$
```

Hình 65: Tải file khi chưa cấu hình quản lý băng thông

→ Tốc độ tải trung bình là 4,4 Mbps.

Thực hiện tải file khi đã cấu hình:

```
zasure69@ubuntu1804:~$ curl -O -L "https://cbqluz9dtwobj.vcdn.cloud/PUBLIC/MEDIA/CambridgeIELTS_16_Academic_b9f737c819.pdf" -x "http://192.168.1.1:3128" -k
% Total % Received % Xferd Average Speed Time Time Time Current
          Dload Upload Total Spent Left Speed
100 35.0M 100 35.0M 0     0 4445k 0 0:00:08 0:00:08 --:--:-- 4557k
zasure69@ubuntu1804:~$ curl -O -L "https://cbqluz9dtwobj.vcdn.cloud/PUBLIC/MEDIA/CambridgeIELTS_16_Academic_b9f737c819.pdf" -x "http://192.168.1.1:3128" -k
% Total % Received % Xferd Average Speed Time Time Time Current
          Dload Upload Total Spent Left Speed
0 35.0M 0 241k 0     0 15662 0 0:39:09 0:00:15 0:38:54 15904^C
zasure69@ubuntu1804:~$
```

Hình 66: Tải file khi đã cấu hình quản lý băng thông

→ Tốc độ tải trung bình sẽ xấp xỉ 16 Kbps.

5.4. Kịch bản 4: Ẩn danh người dùng (Anonymization)

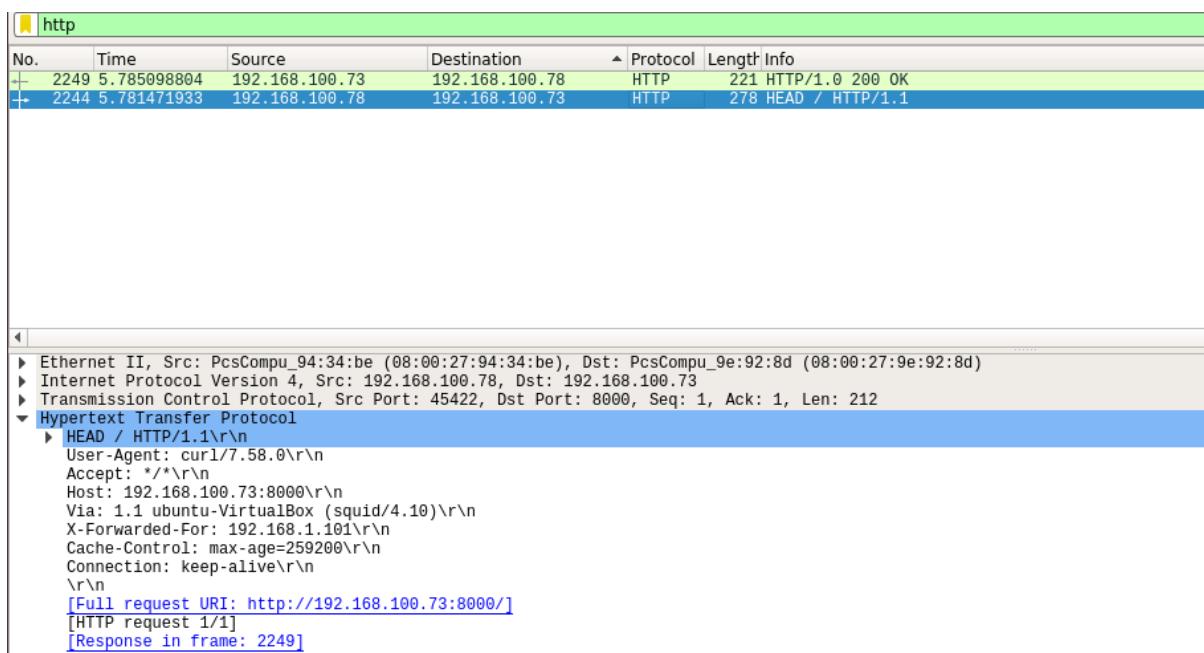
Trên Client thực hiện truy cập vào server test:

```
zasure69@ubuntu1804:~$ curl -I "http://192.168.100.73:8000"
HTTP/1.1 200 OK
Server: SimpleHTTP/0.6 Python/3.11.9
Date: Wed, 20 Nov 2024 16:07:10 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 453
X-Cache: MISS from ubuntu-VirtualBox
Via: 1.1 ubuntu-VirtualBox (squid/4.10)
Connection: keep-alive

zasure69@ubuntu1804:~$
```

Hình 67: Client truy cập Server test trước khi cấu hình

Trên Server dùng Wireshark để bắt gói tin sẽ được Squid Proxy gửi đi.



Hình 68: Bắt gói tin HTTP trước khi cấu hình

Các header của gói tin đã để lộ một số thông tin như: IP của client trong mạng (X-Forwarded-For), gói tin đã được xử lý qua Proxy (Via), Phiên bản trình duyệt client dùng (User-Agent).

Thực hiện truy cập lại sau khi cấu hình trên client:

```
zasure69@ubuntu1804:~$ curl -I "http://192.168.100.73:8000"
HTTP/1.1 200 OK
Server: SimpleHTTP/0.6 Python/3.11.9
Date: Wed, 20 Nov 2024 16:12:35 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 453
X-Cache: MISS from ubuntu-VirtualBox
Connection: keep-alive

zasure69@ubuntu1804:~$
```

Hình 69: Truy cập server test sau khi cấu hình

Và dùng Wireshark bắt gói tin trên Server ở interface kết nối ra Internet:

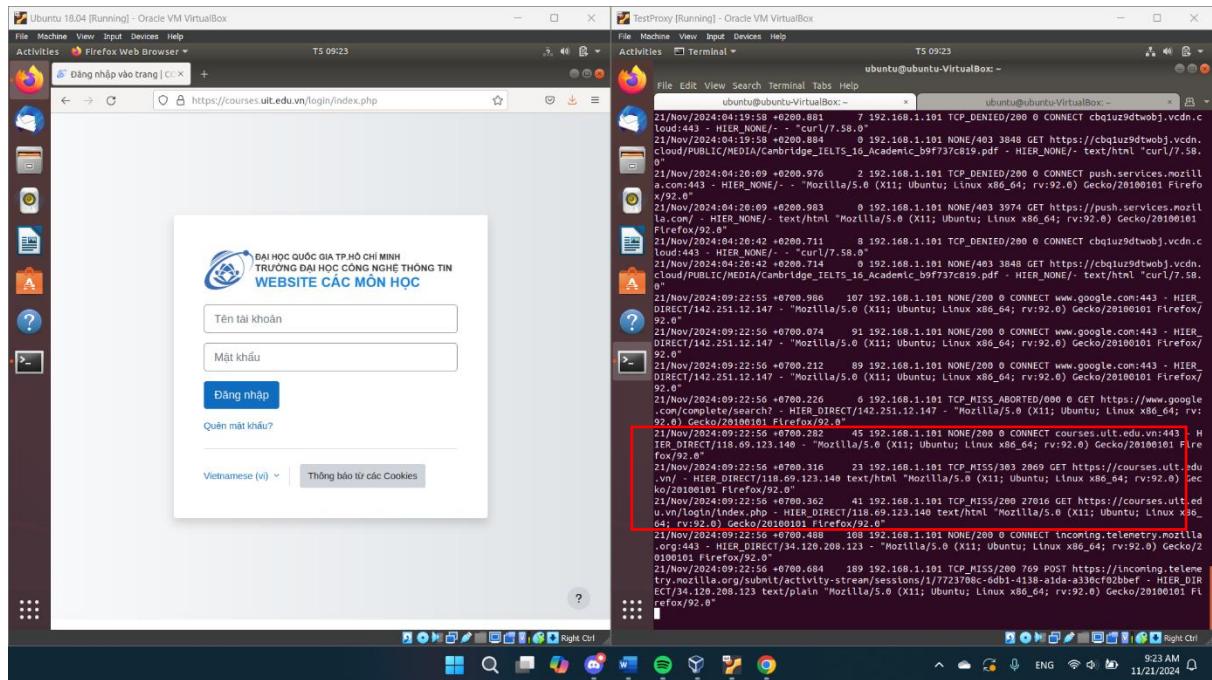
Wireshark screenshot showing captured HTTP traffic. The table lists network frames with details like source and destination IP addresses, protocol, and length. A specific frame (Frame 1958) is expanded to show its detailed structure, including the HEAD request line and the full request URI.

Hình 70: Bắt gói tin HTTP sau khi đã cấu hình

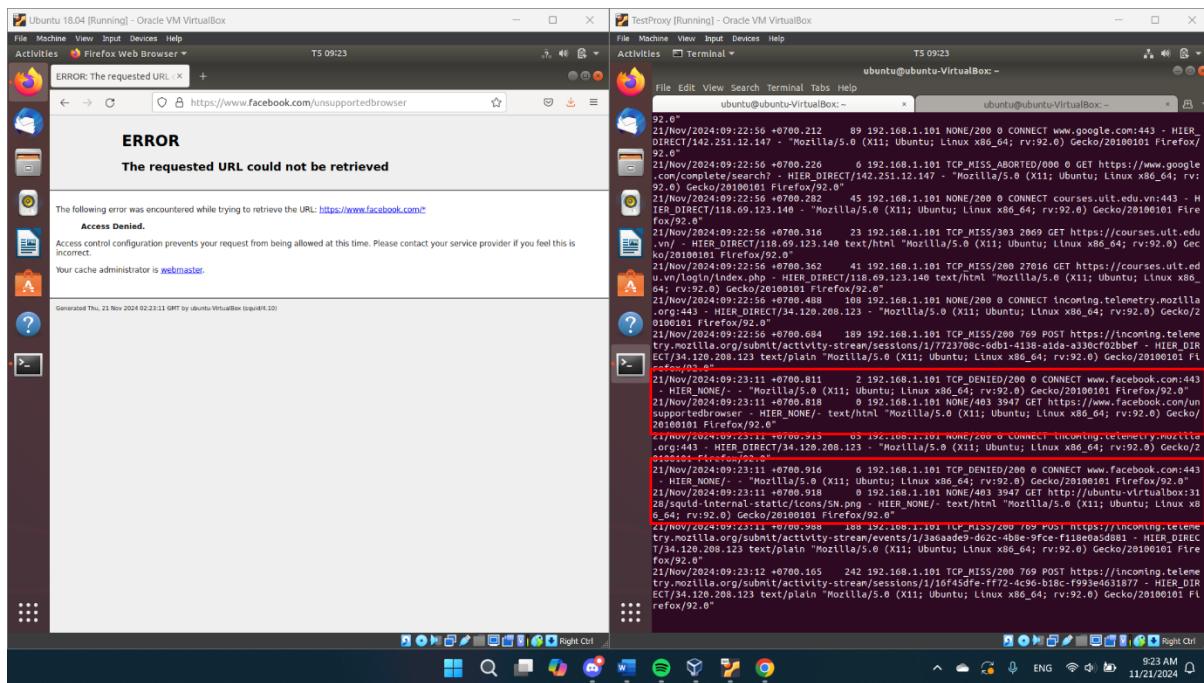
5.5. Kịch bản 5: Giám sát và ghi log hoạt động người dùng

Sử dụng lệnh sudo tail -f /path/to/file/log để xem log.

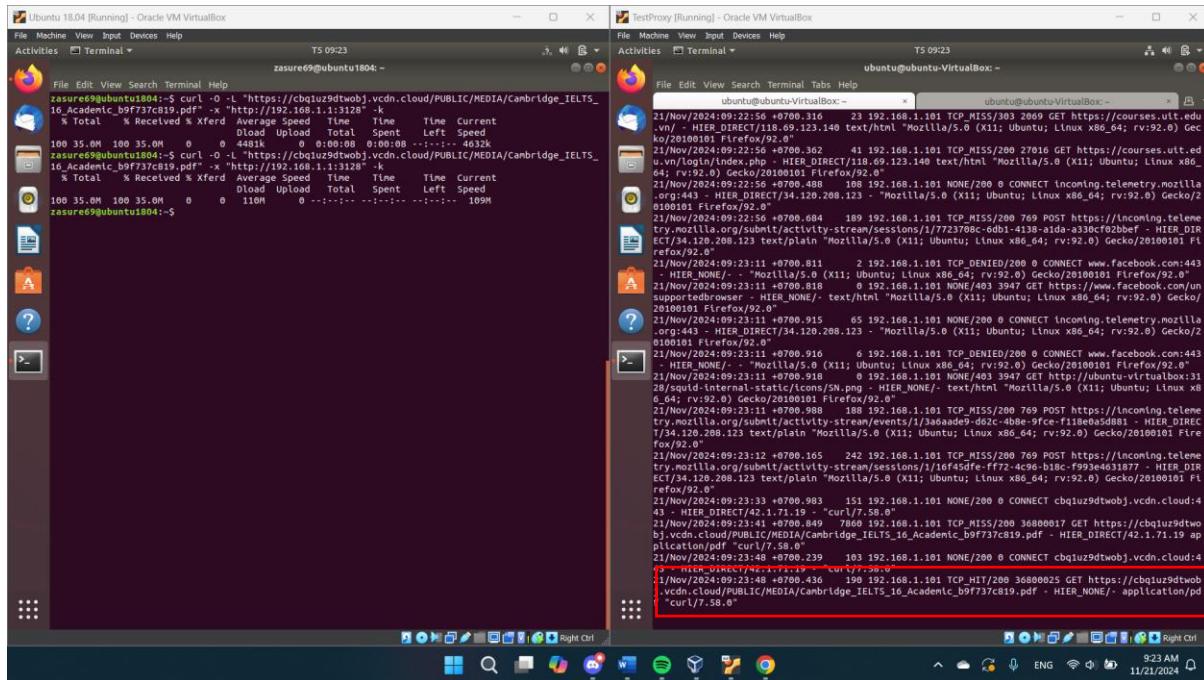
Truy cập trang web bất kì, squid sẽ ghi vào cuối file access.log



Hình 71: Log được ghi lại khi truy cập vào trang web bất kì



Hình 72: Log được ghi lại khi truy cập vào trang web bị chặn



Hình 73: Log được ghi lại khi truy cập đối tượng được cache

Dựa vào log format cấu hình, log trong hình hiển thị các thông tin như:

- 21/Nov/2024:09:23:48 +0700.436: thời điểm Squid nhận được yêu cầu.
- 190: Thời gian phản hồi (tính bằng ms).
- 192.168.1.101: IP của client.
- TCP_HIT/200: Tình trạng request và HTTP status code.
- 36800025 : Kích thước phản hồi mà Squid gửi lại cho client.

- GET: Phương thức của request.
- https://cbq1uz9dtwoj.vcdn.cloud/PUBLIC/MEDIA/CambridgeIELTS_16_Academic_b9f737c819.pdf: URL mà client muốn kết nối đến.
- HIER_NONE/- : Tên người dùng, Squid hierarchy status, địa chỉ IP của Server (Theo thứ tự từ trái qua phải).
- application/pdf : Kiểu nội dung phản hồi.
- "curl/7.58.0": User-Agent.

5.6. FTP

Thực hiện tải file từ máy chủ ftp server trên client

```
zasure69@user1:~$ curl -x 192.168.1.1:3128 ftp://192.168.100.73/50mb.txt -o 50mb.txt
% Total    % Received % Xferd  Average Speed   Time     Time      Time  Current
                                         Dload  Upload   Total Spent   Left  Speed
100 49.3M     0 49.3M     0       0  60.9M      0 --:--:-- --:--:-- --:--:-- 60.8M
```

Hình 74: Tải file từ FTP Server

→ Tải thành công

```
21/Dec/2024:13:13:48 +0700.614      809 192.168.1.101 TCP_MISS/200 51871220 GET ftp://192.168.100.73/50mb.txt - HIER_DIRECT/192.168.100.73 text/plain "curl/7.58.0"
```

Hình 75: Log của Squid

→ TCP_MISS → Request đã được gửi đến FTP Server

```
Sat Dec 21 01:13:47 2024 [pid 93220] CONNECT: Client "::ffff:192.168.100.78"
Sat Dec 21 01:13:47 2024 [pid 93219] [ftp] OK LOGIN: Client "::ffff:192.168.100.78", anon password "kali:kali"
Sat Dec 21 01:13:48 2024 [pid 93221] [ftp] OK DOWNLOAD: Client "::ffff:192.168.100.78", "/50mb.txt", 51770257 bytes, 76457.24Kbyte/sec
```

Hình 76: Log của FTP server

→ Server đã nhận và phản hồi request.

Thực hiện cấu hình cache trên Squid và thực hiện tải lại file

```
zasure69@user1:~$ curl -x 192.168.1.1:3128 ftp://192.168.100.73/50mb.txt -o 50mb.txt
% Total    % Received % Xferd  Average Speed   Time     Time      Time  Current
                                         Dload  Upload   Total Spent   Left  Speed
100 49.3M     0 49.3M     0       0 238M      0 --:--:-- --:--:-- 238M
```

Hình 77: Tải file từ FTP server sau khi cấu hình cache

→ Tốc độ tải nhanh hơn đáng kể

```
21/Dec/2024:13:14:43 +0700.314      204 192.168.1.101 TCP_HIT/200 51871689 GET ftp://192.168.100.73/50mb.txt - HIER_NONE/- text/plain "curl/7.58.0"
```

Hình 78: Log của request tải file cache

→ TCP_HIT cho thấy là response được trả về từ bộ nhớ Cache

```
Sat Dec 21 01:13:47 2024 [pid 93220] CONNECT: Client "::ffff:192.168.100.78"
Sat Dec 21 01:13:47 2024 [pid 93219] [ftp] OK LOGIN: Client "::ffff:192.168.100.78", anon password "kali:kali"
Sat Dec 21 01:13:48 2024 [pid 93221] [ftp] OK DOWNLOAD: Client "::ffff:192.168.100.78", "/50mb.txt", 51770257 bytes, 76457.24Kbyte/sec
[...]
inet6 fe80::e036:d1ff:fe6e:5c71 prefixlen 64 scopeid 0x20<link>
```

Hình 79: Log của FTP server

→ Trên FTP server không nhận được request → Squid không gửi request đến server

Thực hiện cấu hình acl không cho phép truy cập FTP server

```
acl ftp_server dst 192.168.100.73
```

Hình 80: Định nghĩa ACL

```
http_access deny ftp_server
```

Hình 81: Áp dụng ACL

Tải lại file trên client

```
zasure69@user1:~$ curl -x 192.168.1.1:3128 ftp://192.168.100.73/50mb.txt -o 50mb.txt
% Total    % Received % Xferd  Average Speed   Time     Time      Time  Current
          % Received % Xferd  Average Speed   Time     Time      Time  Current
                                         Dload  Upload   Total Spent   Left  Speed
100  3551  100  3551    0     0  385k      0 --:--:-- --:--:-- --:--:-- 385k
```

Hình 82: Tải file sau khi cấu hình từ chối truy cập

```
21/Dec/2024:13:15:33 +0700.151      0 192.168.1.101 TCP_DENIED/403 3898 GET ftp://192.168.100.73/50mb.txt - HIER_NONE/- text/html "curl/7.58.0"
```

Hình 83: Log của request bị từ chối truy cập

Log của Squid cho thấy TCP_DENIED → Request đã bị từ chối

Tuy nhiên thì Squid chỉ cache được với những kết nối anonymous đến FTP Server, những kết nối kèm theo thông tin đăng nhập không được cache

Thực hiện tải file kèm thông tin đăng nhập

```
zasure69@user1:~$ curl -x 192.168.1.1:3128 ftp://kali:kali@192.168.100.73/50mb.txt -o 50mb.txt
% Total    % Received % Xferd  Average Speed   Time     Time      Time  Current
          % Received % Xferd  Average Speed   Time     Time      Time  Current
                                         Dload  Upload   Total Spent   Left  Speed
100 49.3M    0 49.3M    0  42.3M      0 --:--:-- 0:00:01 --:--:-- 42.3M
zasure69@user1:~$ curl -x 192.168.1.1:3128 ftp://kali:kali@192.168.100.73/50mb.txt -o 50mb.txt
% Total    % Received % Xferd  Average Speed   Time     Time      Time  Current
          % Received % Xferd  Average Speed   Time     Time      Time  Current
                                         Dload  Upload   Total Spent   Left  Speed
100 49.3M    0 49.3M    0  46.3M      0 --:--:-- 0:00:01 --:--:-- 46.3M
```

Hình 84: Tải file với thông tin đăng nhập

```
21/Dec/2024:13:29:18 +0700.658  1164 192.168.1.101 TCP_MISS/200 51861475 GET ftp://kali:kali@192.168.100.73/50mb.txt - HIER_DIRECT/192.168.100.73 text/plain "curl/7.58.0"
21/Dec/2024:13:29:21 +0700.005  1062 192.168.1.101 TCP_MISS/200 51868846 GET ftp://kali:kali@192.168.100.73/50mb.txt - HIER_DIRECT/192.168.100.73 text/plain "curl/7.58.0"
```

Hình 85: Log của Squid

→ 2 Request đều là TCP_MISS → Request không được cache lại

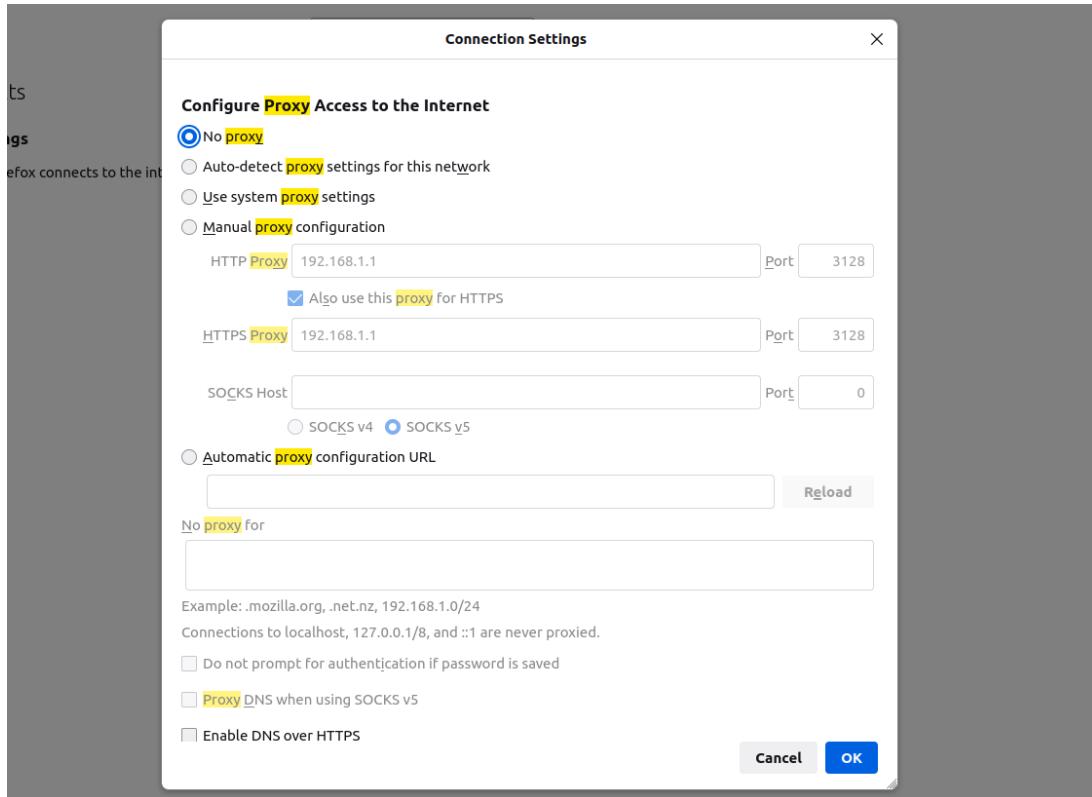
```
Sat Dec 21 01:29:17 2024 [pid 100625] CONNECT: Client "::ffff:192.168.100.78"
Sat Dec 21 01:29:17 2024 [pid 100624] [kali] OK LOGIN: Client "::ffff:192.168.100.78"
Sat Dec 21 01:29:18 2024 [pid 100626] [kali] OK DOWNLOAD: Client "::ffff:192.168.100.78", "/home/kali/50mb.txt", 51770257 bytes, 52223.23Kbyte/sec
Sat Dec 21 01:29:19 2024 [pid 100646] CONNECT: Client "::ffff:192.168.100.78"
Sat Dec 21 01:29:19 2024 [pid 100645] [kali] OK LOGIN: Client "::ffff:192.168.100.78"
Sat Dec 21 01:29:20 2024 [pid 100647] [kali] OK DOWNLOAD: Client "::ffff:192.168.100.78", "/home/kali/50mb.txt", 51770257 bytes, 51162.76Kbyte/sec
```

Hình 86: Log của Server

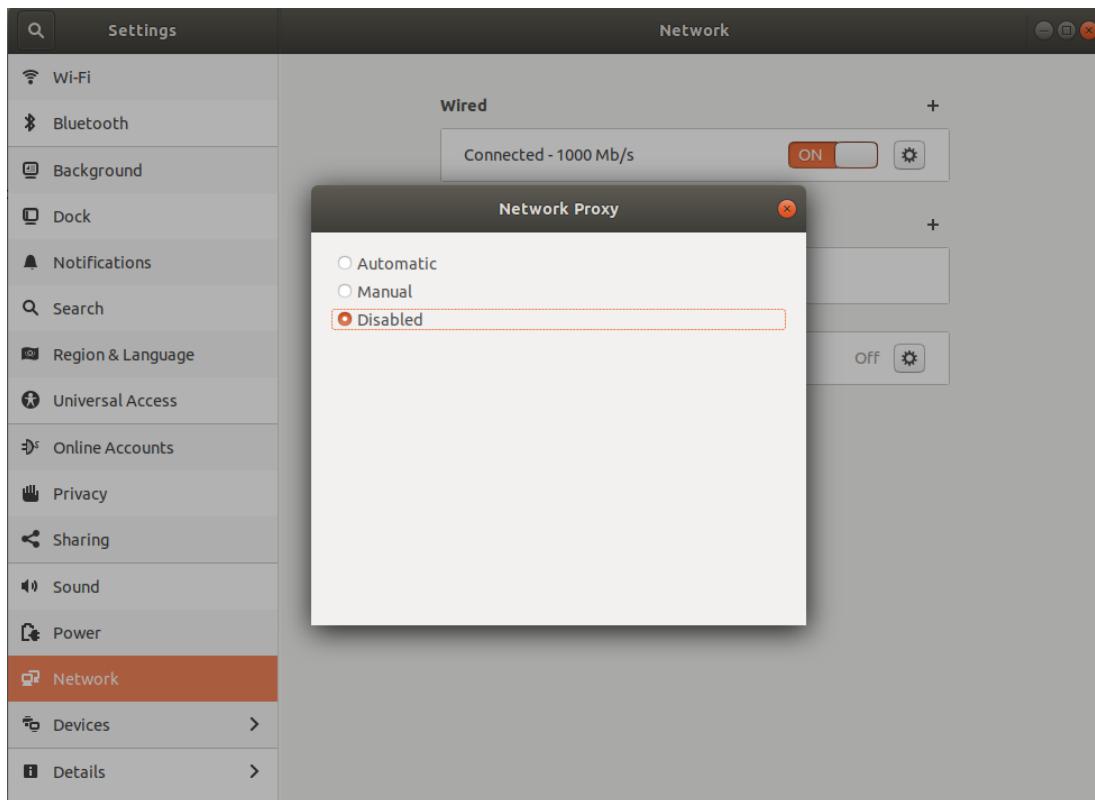
→ 2 request đều được Squid gửi đến FTP Server

5.7. Transparent Proxy

Thực hiện xóa các cấu hình về proxy trên client

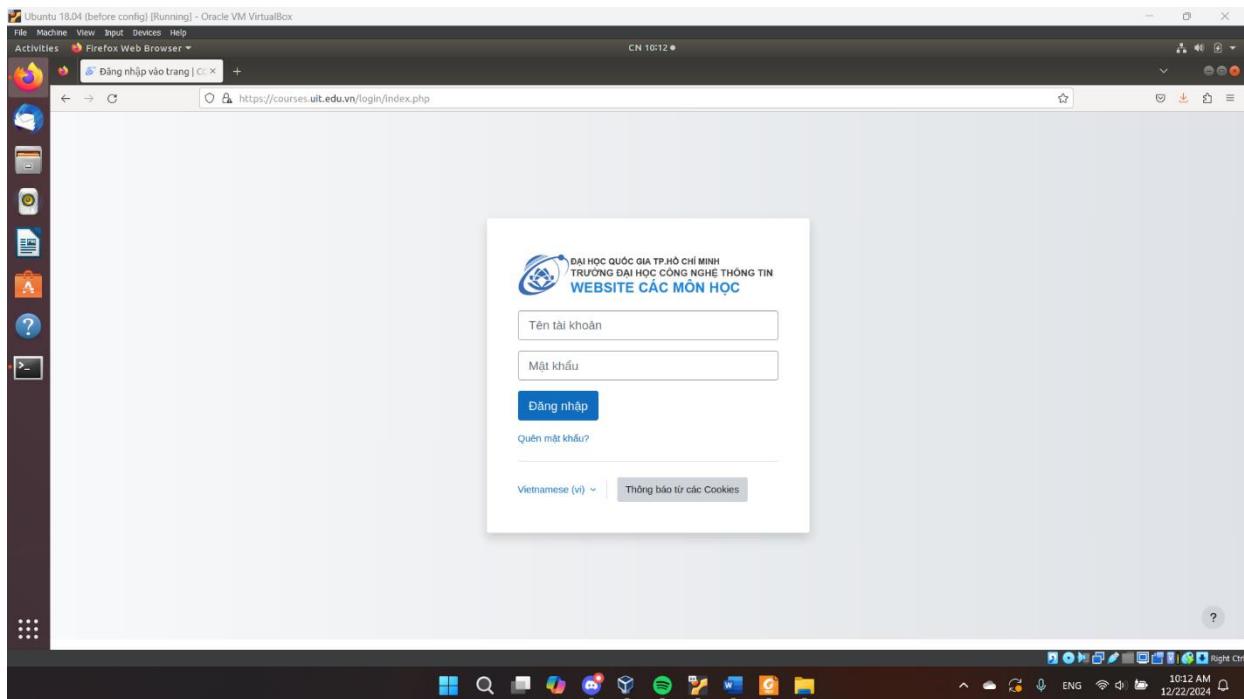


Hình 87: Xoá cấu hình proxy trên trình duyệt



Hình 88: Xoá cấu hình proxy trong cài đặt mạng

Thực hiện truy cập lại Internet sau khi đã cấu hình transparent mode



Hình 89: Truy cập lại Internet trên Client

```
SEED-Ubuntu20.04 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal Dec 22, 10:13
seed@VM: ~ seed@VM: ~ seed@VM: ~
seed@VM: ~ seed@VM: ~ seed@VM: ~
22/Dec/2024:10:03:00 +0700.375 88 192.168.1.101 TCP_MISS/200 27033 GET https://courses.uit.edu.vn/login/index.php - ORIGINAL_DST/45.122.249.78 text/html "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:109.0) Gecko/201001 Firefox/113.0" "-"
22/Dec/2024:10:03:41 +0700.829 1 192.168.1.101 TCP_DENIED/200 0 CONNECT 45.122.249.78:443 - HIER_NONE/- "-" "-"
22/Dec/2024:10:03:41 +0700.842 0 192.168.1.101 NONE/403 3728 GET https://courses.uit.edu.vn/login/index.php - HIER_NONE/- text/html "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:109.0) Gecko/201001 Firefox/113.0" "-"
22/Dec/2024:10:03:41 +0700.909 2 192.168.1.101 TCP_DENIED/200 0 CONNECT 45.122.249.78:443 - HIER_NONE/- "-" "-"
22/Dec/2024:10:03:41 +0700.910 0 192.168.1.101 NONE/403 3720 GET http://vm:3130/squid-internal-static/icons/SN.png - HIER_NONE/- text/html "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:109.0) Gecko/201001 Firefox/113.0" "-"
22/Dec/2024:10:04:02 +0700.489 85 192.168.1.101 NONE/200 0 CONNECT 42.1.110.90:443 - ORIGINAL_DST/42.1.110.90 - "-" "-"
22/Dec/2024:10:04:11 +0700.010 8512 192.168.1.101 TCP_MISS/200 36800028 GET https://cbqluz9dtwobj.vcdn.cloud/PUBLIC/MEDIA/Cambridge_IELTS_16_Academic_b9f737c819.pdf - ORIGINAL_DST/42.1.110.90 application/pdf "Wget/1.19.4 (linux-gnu)" "-"
22/Dec/2024:10:04:43 +0700.697 107 192.168.1.101 NONE/200 0 CONNECT 42.1.110.91:443 - ORIGINAL_DST/42.1.110.91 - "-" "-"
22/Dec/2024:10:04:43 +0700.945 242 192.168.1.101 TCP_HIT/200 36800121 GET https://cbqluz9dtwobj.vcdn.cloud/PUBLIC/MEDIA/Cambridge_IELTS_16_Academic_b9f737c819.pdf - HIER_NONE/- application/pdf "Wget/1.19.4 (linux-gnu)" "-"
22/Dec/2024:10:04:48 +0700.231 626 192.168.1.101 TCP_MISS/204 234 GET http://connectivity-check.ubuntu.com/ - ORIGINAL_DST/185.125.190.96 - "-" "-"
22/Dec/2024:10:05:18 +0700.953 118 192.168.1.101 NONE/200 0 CONNECT 172.253.118.95:443 - ORIGINAL_DST/172.253.118.95 - "-" "-"
22/Dec/2024:10:05:19 +0700.169 150 192.168.1.101 TCP_MISS/200 366 GET http://detectportal.firefox.com/canonical.html - ORIGINAL_DST/34.107.2.221.82 text/html "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:109.0) Gecko/201001 Firefox/113.0" "-"
22/Dec/2024:10:05:19 +0700.280 49 192.168.1.101 TCP_MISS/200 284 GET http://detectportal.firefox.com/success.txt? - ORIGINAL_DST/34.107.2.21.82 text/plain "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:109.0) Gecko/201001 Firefox/113.0" "-"
22/Dec/2024:10:09:48 +0700.272 597 192.168.1.101 TCP_MISS/204 238 GET http://connectivity-check.ubuntu.com/ - ORIGINAL_DST/91.189.91.48 - "-" "-"
22/Dec/2024:10:11:35 +0700.521 59 192.168.1.101 NONE/200 0 CONNECT 45.122.249.78:443 - ORIGINAL_DST/45.122.249.78 - "-" "-"
22/Dec/2024:10:11:35 +0700.641 110 192.168.1.101 TCP_MISS/200 27039 GET https://courses.uit.edu.vn/login/index.php - ORIGINAL_DST/45.122.249.78 text/html "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:109.0) Gecko/201001 Firefox/113.0" "-"
22/Dec/2024:10:11:43 +0700.762 121 192.168.1.101 NONE/200 0 CONNECT 34.117.188.166:443 - ORIGINAL_DST/34.117.188.166 - "-" "-"
22/Dec/2024:10:11:43 +0700.922 89 192.168.1.101 TCP_MISS/200 366 GET http://detectportal.firefox.com/canonical.html - ORIGINAL_DST/34.107.2.221.82 text/html "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:109.0) Gecko/201001 Firefox/113.0" "-"
22/Dec/2024:10:11:44 +0700.012 37 192.168.1.101 TCP_MISS/200 284 GET http://detectportal.firefox.com/success.txt? - ORIGINAL_DST/34.107.2.21.82 text/plain "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:109.0) Gecko/201001 Firefox/113.0" "-"
```

Hình 90: Log được ghi lại trên Squid

→ Truy cập Internet thành công và Squid đã bắt được request

Thực hiện cấu hình cache

```
cache_dir ufs /usr/local/squid/var/cache/squid 1000 16 256
```

Hình 91: Cấu hình cache trên Squid

Thực hiện tải file trên client

```
zasure69@user1:~$ wget "https://cbqluz9dtwobj.vcdn.cloud/PUBLIC/MEDIA/CambridgeIELTS_16_Academic_b9f737c819.pdf"
--no-check-certificate
--2024-12-22 10:04:05-- https://cbqluz9dtwobj.vcdn.cloud/PUBLIC/MEDIA/CambridgeIELTS_16_Academic_b9f737c819.pdf
Resolving cbqluz9dtwobj.vcdn.cloud (cbqluz9dtwobj.vcdn.cloud)... 42.1.110.90
Connecting to cbqluz9dtwobj.vcdn.cloud (cbqluz9dtwobj.vcdn.cloud)|42.1.110.90|:443... connected.
WARNING: cannot verify cbqluz9dtwobj.vcdn.cloud's certificate, issued by 'CN=Not trusted by \\\"192.168.1.1:3128\\\"
,OU=NC,O=UIT,L=Thu Duc,ST=HCM,C=VN':
  Unable to locally verify the issuer's authority.
HTTP request sent, awaiting response... 200 OK
Length: 36799436 (35M) [application/pdf]
Saving to: 'CambridgeIELTS_16_Academic_b9f737c819.pdf.2'

CambridgeIELTS_16_Academic_ 100%[=====] 35,09M 4,11MB/s in 8,5s

2024-12-22 10:04:14 (4,15 MB/s) - 'CambridgeIELTS_16_Academic_b9f737c819.pdf.2' saved [36799436/36799436]
```

Hình 92: Tải file trước khi cấu hình cache

→ Khi chưa cấu hình cache tốc độ tải file là 4.11MB/s và tải trong thời gian 8.5s

```
zasure69@user1:~$ wget "https://cbqluz9dtwobj.vcdn.cloud/PUBLIC/MEDIA/CambridgeIELTS_16_Academic_b9f737c819.pdf"
--no-check-certificate
--2024-12-22 10:04:46-- https://cbqluz9dtwobj.vcdn.cloud/PUBLIC/MEDIA/CambridgeIELTS_16_Academic_b9f737c819.pdf
Resolving cbqluz9dtwobj.vcdn.cloud (cbqluz9dtwobj.vcdn.cloud)... 42.1.110.91
Connecting to cbqluz9dtwobj.vcdn.cloud (cbqluz9dtwobj.vcdn.cloud)|42.1.110.91|:443... connected.
WARNING: cannot verify cbqluz9dtwobj.vcdn.cloud's certificate, issued by 'CN=Not trusted by \\\"192.168.1.1:3128\\\"
,OU=NC,O=UIT,L=Thu Duc,ST=HCM,C=VN':
  Unable to locally verify the issuer's authority.
HTTP request sent, awaiting response... 200 OK
Length: 36799436 (35M) [application/pdf]
Saving to: 'CambridgeIELTS_16_Academic_b9f737c819.pdf.3'

CambridgeIELTS_16_Academic_ 100%[=====] 35,09M 134MB/s in 0,3s

2024-12-22 10:04:47 (134 MB/s) - 'CambridgeIELTS_16_Academic_b9f737c819.pdf.3' saved [36799436/36799436]
```

Hình 93: Tải file sau khi cấu hình cache

→ Sau khi cấu hình tốc độ tải là 134MB/s và tải trong 0.3s → Cấu hình đã được thực hiện

Thực hiện định nghĩa một acl để chặn truy cập trang courses.uit.edu.vn và áp dụng acl lên mạng 192.168.1.0/24

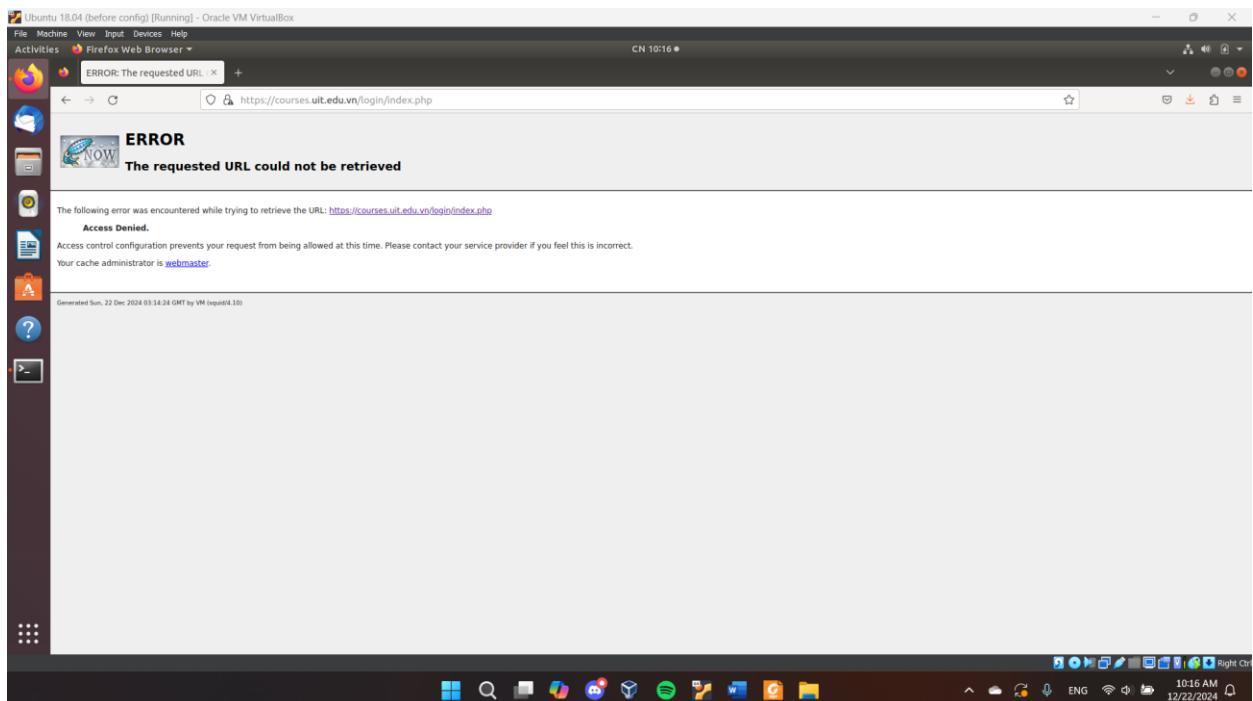
```
acl allowed_sites dstdomain courses.uit.edu.vn
```

Hình 94: Định nghĩa acl chặn truy cập

```
http_access deny local_network allowed_sites
```

Hình 95: Áp dụng acl đã định nghĩa

Truy cập lại trang web trên client



Hình 96: Truy cập vào trang bị chặn

→ Truy cập đã bị chặn → Cấu hình đã được thực hiện

5.8. Đánh giá thực nghiệm

Kịch bản 1:

- Người dùng bị chặn không thể truy cập các trang web bị chặn.
- Ngoài thời gian cho phép người dùng không thể truy cập được vào Internet.
- Hệ thống phản hồi nhanh, không xảy ra lỗi truy cập ngoài ý muốn.

Kịch bản 2:

- Tốc độ tải file tăng rất nhiều.
- Tiết kiệm băng thông cho mạng vì giảm việc gửi yêu cầu Internet.

Kịch bản 3:

- Tốc độ tải của từng người dùng ổn định, không vượt quá giới hạn đã định.
- Lưu lượng mạng tổng thể được phân phối đều, giảm thiểu nghẽn mạng.

Kịch bản 4:

- Các header để lộ thông tin đã được chỉnh sửa: X-Forwarded-For chính thành unknown, header Via và User-Agent đã bị loại bỏ.
- Dịch vụ web không thể xác định chính xác nguồn gốc của các yêu cầu.

Kịch bản 5:

- Tất cả yêu cầu HTTP/HTTPS đều được ghi lại đầy đủ.
- Log hiển thị chi tiết thông tin truy cập của người dùng.

FTP:

- Có thể sử dụng làm FTP proxy
- Thực hiện được các chức năng như cache, access control

Transparent Proxy:

- Client có thể truy cập internet sau khi cấu hình
- Squid có thể xử lý các request từ client
- Thực hiện được các chức năng giống như Explicit mode

Nhận xét:

- Các kịch bản thử nghiệm đạt được kết quả như kỳ vọng.
- Squid Proxy hỗ trợ được các giao thức phổ biến như HTTP, HTTPS, FTP.
- Squid Proxy có thể cấu hình trên 2 chế độ Transparent và Explicit.
- Hệ thống Squid Proxy không chỉ giúp tối ưu hóa tài nguyên mạng mà còn đảm bảo an toàn và kiểm soát truy cập hiệu quả.

CHƯƠNG 6: KẾT LUẬN VÀ HƯỚNG PHÁT TRIỂN

6.1. Kết quả đạt được

- Biết được Squid Proxy là gì, cách cài đặt và triển khai trong mô hình mạng.
- Xây dựng được mô hình mạng có áp dụng Squid Proxy Server và thực hiện được một số các chức năng chính mà Squid cung cấp.

6.2. Khó khăn và hạn chế

- Khó khăn trong quá trình thực hiện:
 - + Phải tìm hiểu công nghệ mới khiến việc sử dụng ban đầu còn gặp nhiều lỗi, mất thêm thời gian tìm hiểu để sửa.
 - + Cấu hình máy tính không đủ triển khai được nhiều máy ảo hơn.
- Hạn chế: Kiến thức về mạng, proxy server và kiến thức thực tế còn hạn một vài tính năng hoạt động chưa được tối ưu.

6.3. Hướng phát triển

- Cài đặt và triển khai Squid Proxy Server trong một mô hình mạng phức tạp hơn.
- Cấu hình chi tiết hơn các tính năng đã demo và thêm các tính năng khác để đạt được hiệu quả tối ưu hơn.

TÀI LIỆU THAM KHẢO

- [1] V. IDC, "Proxy Server là gì? Cách thức hoạt động của Proxy Server," 06 09 2021. [Online]. Available: <https://www.viettelidc.com.vn/tin-tuc/proxy-server-la-gi-cach-thuc-hoat-dong-cua-proxy-server>.
- [2] Squid, "squid-cache.org," [Online]. Available: <https://www.squid-cache.org/Intro/>.
- [3] T. IT, "Squid Proxy v.6.10 - building from source in 5 min," [Online]. Available: <https://www.youtube.com/watch?v=48HyBjgsSj4>.
- [4] "Configuring SSL Bumping in the Squid service," [Online]. Available: <https://support.kaspersky.com/KWTS/6.1/en-US/166244.htm>.
- [5] R. Hat, "Configuring the Squid Caching Proxy Server," [Online]. Available: https://docs.redhat.com/en/documentation/red_hat_enterprise_linux/7/html/networking_guide/configuring-the-squid-caching-proxy-server#configuring-the-squid-caching-proxy-server.
- [6] Squid, "Squid configuration directives," [Online]. Available: <https://www.squid-cache.org/Doc/config/>.
- [7] Squid, "Interception Caching," [Online]. Available: <https://wiki.squid-cache.org/SquidFaq/InterceptionProxy>.
- [8] S. Quick, "Transparent HTTP+HTTPS Proxy with Squid and iptables," [Online]. Available: https://youtu.be/Bogdplu_lsE?si=AGMEXgUIaUZn6Fbr.