

ĐẠI HỌC QUỐC GIA THÀNH PHỐ HỒ CHÍ MINH
TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN
KHOA MẠNG MÁY TÍNH VÀ TRUYỀN THÔNG
-----000-----



BÁO CÁO ĐỒ ÁN
MÔN QUẢN TRỊ MẠNG VÀ HỆ THỐNG
Tên đề tài: Tìm hiểu và triển khai Squid proxy

Giảng viên hướng dẫn : ThS. Đỗ Hoàng Hiển

Lớp : NT132.O11.ANTT

Khoá : 16

Sinh viên thực hiện: **MSSV:**

- | | |
|----------------------|----------|
| - Nguyễn Huy Cường | 21520667 |
| - Phan Gia Khánh | 21522213 |
| - Nguyễn Đức Tài | 21521395 |
| - Nguyễn Hoài Phương | 21520408 |
| - Trần Minh Duy | 21522010 |

TP. Hồ Chí Minh, tháng 12 năm 2023

LỜI MỞ ĐẦU

Trong thời đại hiện nay, việc truy cập internet đã trở thành một phần không thể thiếu trong cuộc sống hàng ngày của chúng ta. Tuy nhiên, khi số lượng người truy cập internet tăng đáng kể, cùng với đó là sự gia tăng về lưu lượng truy cập và các yêu cầu mạng, việc quản lý và kiểm soát truy cập trở nên phức tạp hơn bao giờ hết. Sự ra đời của proxy server như Squid Proxy Server trở nên cần thiết.

Squid Proxy Server là một phần mềm proxy mã nguồn mở được phát triển mạnh mẽ và rất phổ biến. Nó hoạt động như một trung gian giữa client và server, cho phép kiểm soát, lưu trữ và tăng cường hiệu suất truy cập internet. Với Squid, các yêu cầu truy cập từ client được xử lý thông qua proxy server trước khi đến server và ngược lại, tạo ra một môi trường an toàn và hiệu quả cho việc truy cập internet.

Sử dụng Squid Proxy Server, tổ chức và doanh nghiệp có thể tận dụng nhiều lợi ích. Một trong những lợi ích quan trọng nhất là khả năng caching, cho phép lưu trữ các nội dung phổ biến như hình ảnh, tệp tin và trang web, giúp giảm tải cho server và cải thiện thời gian truy cập. Ngoài ra, Squid cung cấp các tính năng quản lý truy cập linh hoạt như content filtering, access control và authentication, giúp ngăn chặn truy cập không ủy quyền và bảo vệ mạng.

Trong báo cáo này, chúng tôi sẽ giới thiệu chi tiết về Squid Proxy Server, từ cách cài đặt và cấu hình, đến các tính năng quan trọng như caching, filtering và quản lý truy cập. Nội dung báo cáo gồm 5 chương. Chương 1 sẽ giới thiệu khái quát về proxy server. Chương 2, chúng tôi sẽ trình bày chi tiết về Squid proxy server. Chương 3 và chương 4 sẽ trình bày về mô hình hệ thống để triển khai và các kịch bản mà chúng tôi xây dựng để trình bày các chức năng của Squid proxy server. Cuối cùng là những kết luận mà chúng tôi thu được sẽ được trình bày ở trong chương 5. Hi vọng thông qua báo cáo này sẽ giúp mọi người hiểu rõ hơn về Squid proxy và cách để triển khai nó thực tế.

MỤC LỤC

CHƯƠNG 1 GIỚI THIỆU	1
1.1 Proxy Server	1
1.2 Phân loại Proxy server.....	1
1.2.1 Proxy Forward.....	1
1.2.2 Proxy Reverse.....	1
1.2.3 Proxy Transparent.....	1
1.2.4 Proxy Anonymous	1
1.2.5 Proxy High Anonymity.....	2
1.3 Các phần mềm proxy server phổ biến được sử dụng hiện nay.....	2
1.3.1 Squid.....	2
1.3.2 Nginx	2
1.3.3 Apache HTTP Server.....	2
1.3.4 HAProxy	2
1.3.5 Privoxy.....	2
1.3.6 Tinyproxy.....	2
CHƯƠNG 2 SQUID PROXY SERVER	3
2.1 Khái niệm	3
2.2 Các thành phần của Squid proxy	3
2.2.1 Squid core	3
2.2.2 Access Control Lists (ACLs).....	3
2.2.3 Cache manager	4
2.2.4 Logging.....	4
2.2.5 SquidGuard.....	5
2.5.6 Authentication Modules.....	5
2.3 Chức năng của Squid proxy.....	5
CHƯƠNG 3 TRIỀN KHAI HỆ THỐNG.....	7
3.1 Cài đặt và cấu hình Squid proxy trên hệ điều hành Ubuntu và CentOS	7
3.1.1 Cài đặt và cấu hình Squid proxy trên Ubuntu	7
3.1.2 Cài đặt và cấu hình Squid proxy trên CentOS.....	7

3.2 Mô hình triển khai	8
CHƯƠNG 4 THỰC NGHIỆM VÀ ĐÁNH GIÁ	10
4.1. Thực nghiệm tính năng Caching	10
4.2. Thực nghiệm tính năng Content Filtering	12
4.2.1. Thực nghiệm tính năng Block Domain trong ContentFiltering	12
4.2.2. Thực nghiệm tính năng Block Words trong ContentFiltering	16
4.2.3. Thực nghiệm tính năng Block Download trong ContentFiltering	21
4.3. Thủ nghiệm tính năng Authentication	26
4.4. Thủ nghiệm tính năng Access Control List.....	31
4.5. Thủ nghiệm tổng hợp tất cả tính năng trong 1 Squid Proxy Server.....	36
4.6. Đánh giá sau thử nghiệm	44
CHƯƠNG 5 KẾT LUẬN	45
5.1 Kết quả thu được	45
5.2 Đánh giá ưu điểm và hạn chế khi sử dụng Squid Proxy	45
5.2.1 Ưu điểm	45
5.2.2 Hạn chế	46
5.3 Hướng phát triển	47
DANH MỤC TÀI LIỆU THAM KHẢO	48

DANH MỤC HÌNH ẢNH

Hình 1 Nội dung file cache.log.....	4
Hình 2 Nội dung file access.log	5
Hình 3 Mô hình triển khai	8
Hình 4 Cấu hình Squid Proxy để thực hiện chức năng Caching	10
Hình 5 Kiểm tra trạng thái của Squid proxy sau khi restart lần 1	11
Hình 6 Phản hồi của trang web trên máy Client 2 khi truy cập đến trang web lần đầu tiên	11
Hình 7 Phản hồi của trang web trên máy Client 2 khi truy cập đến trang web lần thứ hai	12
Hình 8 Kiểm tra lịch sử truy cập trên Squid proxy	12
Hình 9 Cấu hình Squid proxy để thực hiện chức năng Block Domain	13
Hình 10 Kiểm tra trạng thái của Squid proxy sau khi restart lần 2	14
Hình 11 Phản hồi của trang web khi gửi yêu cầu đến có đi qua Squid proxy	15
Hình 12 Phản hồi nhận được khi truy cập trang web bị chặn (1).....	15
Hình 13 Phản hồi nhận được khi truy cập trang web bị chặn (2).....	16
Hình 14 Phản hồi nhận được khi truy cập trang web không bị chặn (3).....	16
Hình 15 Nội dung file blacklist.txt	17
Hình 16 Cấu hình Squid proxy để thực hiện chức năng Block words	17
Hình 17 Kiểm tra trạng thái của Squid proxy sau khi restart lần 3	18
Hình 18 Phản hồi nhận được khi truy cập trang web có chứa từ có trong blacklist (1)....	19
Hình 19 Phản hồi nhận được khi truy cập trang web có chứa từ có trong blacklist (2)....	19
Hình 20 Phản hồi nhận được khi truy cập trang web có chứa từ có trong blacklist (3)....	20
Hình 21 Phản hồi nhận được khi truy cập trang web có chứa từ có trong blacklist (4)....	20
Hình 22 Phản hồi nhận được khi truy cập trang web không chứa từ có trong blacklist ...	20
Hình 23 Cấu hình Squid proxy để thực hiện chức năng block download.....	21
Hình 24 Kiểm tra trạng thái của Squid proxy sau khi restart lần 4	22
Hình 25 Cấu hình Squid proxy để block download file .mp3	23
Hình 26 Kiểm tra trạng thái Squid proxy sau khi restart lần 5.....	24
Hình 27 Phản hồi nhận được khi thực hiện tải file có phần mở rộng bị chặn (1)	24
Hình 28 Phản hồi nhận được khi thực hiện tải file có phần mở rộng bị chặn (2)	25
Hình 29 Phản hồi nhận được khi thực hiện tải file có phần mở rộng mp3 khi chưa bị chặn	25
Hình 30 Phản hồi nhận được khi thực hiện tải file có phần mở rộng bị chặn (3)	25
Hình 31 Phản hồi nhận được khi thực hiện tải file có phần mở rộng bị chặn (4)	26
Hình 32 Phản hồi nhận được khi thực hiện tải file có phần mở rộng mp3 khi đã bị chặn	26
Hình 33 Cài đặt apache2-utils	27
Hình 34 Tạo và cấp quyền thực thi cho file password	27
Hình 35 Tạo password cho Client 2	27

Hình 36 Cấu hình Squid proxy để thực hiện chức năng xác thực	28
Hình 37 Kiểm tra trạng thái của Squid proxy sau khi restart lần 6	29
Hình 38 Phản hồi nhận được khi nhập sai password.....	29
Hình 39 Phản hồi nhận được khi nhập đúng password (1)	30
Hình 40 Thông báo nhập username và password trước khi truy cập trang web	30
Hình 41 Phản hồi nhận được khi nhập đúng password (2)	31
Hình 42 Phản hồi nhận được khi nhập đúng password (3)	31
Hình 43 Cấu hình Squid proxy để thực hiện chức năng Access control list	32
Hình 44 Kiểm tra trạng thái của Squid proxy sau khi restart lần 7	33
Hình 45 Phản hồi nhận được khi truy cập trang web trên Client 2	33
Hình 46 Phản hồi nhận được khi truy cập trang web không qua Squid proxy trên Client 1	34
Hình 47 Phản hồi nhận được khi truy cập trang web qua Squid proxy trên Client 1 (1)..	34
Hình 48 Phản hồi nhận được khi truy cập trang web qua Squid proxy trên Client 1 (2)..	35
Hình 49 Phản hồi nhận được khi truy cập trang web qua Squid proxy trên Client 1 (3)..	35
Hình 50 Lịch sử hoạt động của Squid proxy (1)	36
Hình 51 Cấu hình Squid proxy để thực hiện tổng hợp chức năng	36
Hình 52 Cấu hình chức năng caching.....	37
Hình 53 Cấu hình chức năng Block domain	37
Hình 54 Cấu hình chức năng Block words.	37
Hình 55 Cấu hình chức năng Block download.....	37
Hình 56 Cấu hình chức năng xác thực (1).....	37
Hình 57 Cấu hình chức năng xác thực (2).....	37
Hình 58 Cấu hình chức năng Access control list (1)	37
Hình 59 Cấu hình chức năng Access control list (2)	37
Hình 60 Kiểm tra trạng thái Squid proxy sau khi restart lần 8.....	38
Hình 61 Phản hồi nhận được trên máy Client 2 (1).....	39
Hình 62 Phản hồi nhận được trên máy Client 2 (2).....	39
Hình 63 Phản hồi nhận được trên máy Client 2 (3).....	40
Hình 64 Phản hồi nhận được trên máy Client 2 (4).....	40
Hình 65 Phản hồi nhận được trên máy Client 2 (5).....	41
Hình 66 Phản hồi nhận được trên máy Client 2 (6).....	41
Hình 67 Phản hồi nhận được trên máy Client 1 (1).....	42
Hình 68 Phản hồi nhận được trên máy Client 1 (2).....	42
Hình 69 Phản hồi nhận được trên máy Client 1 (3).....	43
Hình 70 Lịch sử hoạt động của Squid proxy (2)	43
Hình 71 Lịch sử hoạt động của Squid proxy (3)	43

CHƯƠNG 1

GIỚI THIỆU

1.1 Proxy Server

Proxy Server (Máy chủ proxy) 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. Các máy chủ proxy cung cấp các chức năng bảo mật và riêng tư khác nhau phụ thuộc vào nhu cầu của bạn hoặc chính sách công ty.

Khi sử dụng máy chủ proxy, lưu lượng truy cập Internet sẽ truyền qua máy chủ proxy theo đường của nó đến địa chỉ bạn yêu cầu. Sau đó, yêu cầu này sẽ trở lại cùng một máy chủ proxy và máy chủ proxy đó sẽ xử lý và chuyển tiếp dữ liệu nhận được từ website đến người dùng.

Các máy chủ proxy hiện đại thực hiện nhiều công việc hơn ngoài việc chuyển tiếp các yêu cầu web, nó còn thực hiện bảo mật dữ liệu và tăng hiệu suất mạng. Các máy chủ proxy hoạt động như tường lửa và bộ lọc web, cung cấp chia sẻ kết nối mạng và dữ liệu bộ nhớ cache để tăng tốc các yêu cầu thông thường. Một máy chủ proxy tốt sẽ bảo vệ người dùng và mạng nội bộ khỏi các thứ không mong muốn từ Internet. Cuối cùng, máy chủ proxy có thể cung cấp mức độ riêng tư cao.

1.2 Phân loại Proxy server

1.2.1 Proxy Forward

Proxy server này hoạt động như một trung gian giữa người dùng và máy chủ đích. Nó nhận yêu cầu từ người dùng và chuyển tiếp nó đến máy chủ đích, sau đó trả về phản hồi cho người dùng. Proxy forward thường được sử dụng để tăng tốc độ truy cập và giảm tải cho máy chủ đích.

1.2.2 Proxy Reverse

Proxy server này hoạt động ngược lại với proxy forward. Nó đóng vai trò là một trung gian giữa máy chủ và người dùng. Khi người dùng gửi yêu cầu đến máy chủ, proxy reverse nhận yêu cầu đó và chuyển tiếp nó đến máy chủ thích hợp. Proxy reverse thường được sử dụng để cân bằng tải và bảo mật máy chủ.

1.2.3 Proxy Transparent

Proxy server này hoạt động mà không yêu cầu người dùng cấu hình hoặc biết về sự tồn tại của nó. Nó tự động chuyển tiếp yêu cầu và phản hồi giữa người dùng và máy chủ đích. Proxy transparent thường được sử dụng để kiểm soát và giám sát lưu lượng mạng.

1.2.4 Proxy Anonymous

Proxy server này ẩn danh thông tin của người dùng khi gửi yêu cầu đến máy chủ đích. Máy chủ đích không biết về nguồn gốc của yêu cầu và không thể xác định danh tính của người dùng. Proxy anonymous thường được sử dụng để bảo vệ quyền riêng tư và truy cập vào các trang web bị chặn.

1.2.5 Proxy High Anonymity

Proxy server này cung cấp mức độ ẩn danh cao nhất cho người dùng. Nó không chỉ ẩn danh thông tin của người dùng mà còn giả mạo địa chỉ IP và thông tin khác để che giấu danh tính thực sự. Proxy high anonymity thường được sử dụng trong các hoạt động truy cập web ẩn danh và bảo mật.

1.3 Các phần mềm proxy server phổ biến được sử dụng hiện nay

Trên thị trường hiện nay có nhiều phần mềm proxy server được sử dụng với các mục đích khác nhau. Trong phần này, chúng tôi xin giới thiệu một số phần mềm phổ biến nhất hiện nay.

1.3.1 Squid

Squid là một phần mềm proxy server mã nguồn mở và được sử dụng rộng rãi trên nhiều hệ điều hành. Nó hỗ trợ nhiều giao thức như HTTP, HTTPS, FTP và giao thức SOCKS. Squid có khả năng lưu cache, kiểm soát truy cập và cân bằng tải.

1.3.2 Nginx

Mặc dù Nginx thường được sử dụng như một web server, nhưng nó cũng có thể hoạt động như một reverse proxy server. Nginx có khả năng xử lý đồng thời hàng ngàn kết nối và cân bằng tải giữa các máy chủ đích.

1.3.3 Apache HTTP Server

Apache HTTP Server cũng có thể được cấu hình để hoạt động như một proxy server. Nó cung cấp các module như mod_proxy và mod_rewrite để thực hiện chức năng proxy và cân bằng tải.

1.3.4 HAProxy

HAProxy là một phần mềm proxy server và cân bằng tải mã nguồn mở. Nó hỗ trợ nhiều giao thức như HTTP, HTTPS, TCP và UDP. HAProxy có khả năng cân bằng tải, điều hướng yêu cầu và giám sát máy chủ.

1.3.5 Privoxy

Privoxy là một phần mềm proxy server mã nguồn mở, được sử dụng chủ yếu để bảo vệ quyền riêng tư và kiểm soát truy cập. Nó có thể chặn quảng cáo, loại bỏ thông tin riêng tư và áp dụng các quy tắc lọc trên nhiều giao thức.

1.3.6 Tinyproxy

Tinyproxy là một proxy server nhẹ và dễ cấu hình. Nó hỗ trợ giao thức HTTP và có khả năng lưu cache và kiểm soát truy cập.

CHƯƠNG 2

SQUID PROXY SERVER

2.1 Khái niệm

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. Khi khách hàng gửi yêu cầu về nội dung, Squid sẽ tìm nạp nội dung từ máy chủ web và tạo một bản sao cục bộ. Sau đó, nếu một yêu cầu được thực hiện lại, nó sẽ hiển thị bản sao cục bộ, được lưu trong bộ nhớ đệm thay vì thực hiện một yêu cầu khác tới máy chủ web. Bằng cách này, hiệu suất được cải thiện và băng thông mạng được tối ưu hóa. Nó cũng có thể lọc lưu lượng truy cập web, giúp cải thiện tính bảo mật.

Squid proxy server đưa ra các kỹ thuật lưu trữ ở cấp mức độ cao của các web client, đồng thời hỗ trợ các dịch vụ thông thường như 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.

Hiện nay, trên thị trường có rất nhiều chương trình proxy-server nhưng chúng lại có hai nhược điểm, thứ nhất là phải trả tiền để sử dụng, thứ hai là hầu hết không hỗ trợ Internet Cache Protocol (ICP được sử dụng để cập nhật những thay đổi về nội dung của những URL có trong cache- là nơi lưu trữ những trang web đã từng đi qua). Squid là sự lựa chọn tốt nhất cho một proxy-cache server, squid đáp ứng hai yêu cầu là sử dụng miễn phí và có hỗ trợ ICP.

2.2 Các thành phần của Squid proxy

2.2.1 Squid core

Đây là thành phần chính của Squid Proxy Server, chịu trách nhiệm xử lý các yêu cầu và phản hồi HTTP/HTTPS từ client và server. Squid Core thực hiện các chức năng như lưu trữ bộ nhớ cache, quản lý kết nối mạng, xử lý các yêu cầu định tuyến và kiểm soát truy cập.

Trong hệ điều hành Ubuntu, tệp thực thi /usr/sbin/squid (Squid core) chứa mã nguồn chính của Squid Proxy Server và được sử dụng để khởi động và quản lý hoạt động của Squid trên hệ thống.

2.2.2 Access Control Lists (ACLs)

ACLs là thành phần cho phép Squid Proxy Server kiểm soát quyền truy cập dựa trên các điều kiện nhất định. ACLs có thể xác định quyền truy cập dựa trên địa chỉ IP, tên miền, URL, phương thức HTTP và nhiều yếu tố khác. ACLs giúp Squid quyết định xem liệu yêu cầu của client có được chấp nhận hay không.

Trong Squid Proxy Server, Access Control Lists (ACLs) thường được định nghĩa và cấu hình trong tệp cấu hình chính của Squid (squid.conf). Tệp cấu hình này thường được đặt tại đường dẫn /etc/squid/squid.conf

Một số ví dụ về cách sử dụng ACLs trong Squid proxy:

```
acl localnet src 192.168.0.0/24  
acl allowed_sites dstdomain .example.com  
acl restricted_sites dstdomain .facebook.com  
http_access allow localnet allowed_sites  
http_access deny localnet restricted_sites
```

2.2.3 Cache manager

Quản lý và giám sát bộ nhớ đệm của Squid Proxy. Nó cung cấp thông tin chi tiết về việc sử dụng bộ nhớ đệm, bao gồm thông tin về các tài nguyên được lưu trữ và kích thước của chúng.

Trong Squid Proxy Server, Cache manager thường được chứa ở trong tệp /var/log/squid/cache.log.

```
2023/12/02 14:24:15 kid1| Set Current Directory to /var/spool/squid  
2023/12/02 14:24:15 kid1| Creating missing swap directories  
2023/12/02 14:24:15 kid1| No cache_dir stores are configured.  
2023/12/02 14:24:15| Removing PID file (/run/squid.pid)  
2023/12/02 14:24:15 kid1| Set Current Directory to /var/spool/squid  
2023/12/02 14:24:16 kid1| Starting Squid Cache version 5.7 for x86_64-pc-linux-gnu...  
2023/12/02 14:24:16 kid1| Service Name: squid  
2023/12/02 14:24:16 kid1| Process ID: 26533  
2023/12/02 14:24:16 kid1| Process Roles: worker  
2023/12/02 14:24:16 kid1| With 1024 file descriptors available  
2023/12/02 14:24:16 kid1| Initializing IP Cache...  
2023/12/02 14:24:16 kid1| DNS Socket created at [::], FD 8  
2023/12/02 14:24:16 kid1| DNS Socket created at 0.0.0.0, FD 9  
2023/12/02 14:24:16 kid1| Adding nameserver 127.0.0.53 from /etc/resolv.conf  
2023/12/02 14:24:16 kid1| Adding domain localdomain from /etc/resolv.conf  
2023/12/02 14:24:16 kid1| Logfile: opening log daemon:/var/log/squid/access.log  
2023/12/02 14:24:16 kid1| Logfile Daemon: opening log /var/log/squid/access.log  
2023/12/02 14:24:16 kid1| Local cache digest enabled; rebuild/rewrite every 3600/3600 sec  
2023/12/02 14:24:16 kid1| Store logging disabled  
2023/12/02 14:24:16 kid1| Swap maxSize 0 + 262144 KB, estimated 20164 objects  
2023/12/02 14:24:16 kid1| Target number of buckets: 1008  
2023/12/02 14:24:16 kid1| Using 8192 Store buckets  
2023/12/02 14:24:16 kid1| Max Mem size: 262144 KB  
2023/12/02 14:24:16 kid1| Max Swap size: 0 KB  
2023/12/02 14:24:16 kid1| Using Least Load store dir selection  
2023/12/02 14:24:16 kid1| Set Current Directory to /var/spool/squid  
2023/12/02 14:24:16 kid1| Finished loading MIME types and icons.  
2023/12/02 14:24:16 kid1| HTTP Disabled.  
2023/12/02 14:24:16 kid1| Pinger socket opened on FD 14  
2023/12/02 14:24:16 kid1| Squid plugin modules loaded: 0  
2023/12/02 14:24:16 kid1| Adaptation support is off.  
2023/12/02 14:24:16 kid1| Accepting HTTP Socket connections at conn3 local=[::]:3128 remote=[::] FD 12 flags=9  
2023/12/02 14:24:17 kid1| storeLateRelease: released 0 objects  
2023/12/02 14:24:21| pinger: Initialising ICMP pinger ...  
2023/12/02 14:24:21| pinger: ICMP socket opened.  
2023/12/02 14:24:21| pinger: ICMPv6 socket opened  
2023/12/02 14:49:32 kid1| Preparing for shutdown after 0 requests
```

Hình 1 Nội dung file cache.log

2.2.4 Logging

Trong Squid Proxy Server, file /var/log/squid/access.log ghi lại các yêu cầu gửi đến Squid Proxy Server và thông tin về việc truy cập của các máy khách.

```

access.log.access.1 content.log cache.log.1
squidproxy@squidproxy-virtual-machine:/var/log/squid$ sudo cat /var/log/squid/access.log.1
1701267258.238      1 192.168.37.138 TCP_DENIED/403 422 HEAD http://duckduckgo.com/ - HIER_NONE/- text/html
1701267295.611      0 192.168.37.138 TCP_DENIED/403 422 HEAD http://duckduckgo.com/ - HIER_NONE/- text/html
1701267406.577      441 192.168.37.138 TCP_MISS/301 2426 HEAD http://duckduckgo.com/ - HIER_DIRECT/52.250.42.157 text/html
1701267489.432      82853 192.168.37.138 TCP_TUNNEL/200 3616 CONNECT duckduckgo.com:443 - HIER_DIRECT/52.250.42.157 -
1701267490.872      0 192.168.37.138 TCP_MEM_HIT/301 2433 HEAD http://duckduckgo.com/ - HIER_NONE/- text/html
1701267492.672      1799 192.168.37.138 TCP_TUNNEL/200 5943 CONNECT duckduckgo.com:443 - HIER_DIRECT/52.250.42.157 -
1701267549.257      0 192.168.37.138 TCP_MEM_HIT/301 2434 HEAD http://duckduckgo.com/ - HIER_NONE/- text/html
1701267550.945      1686 192.168.37.138 TCP_TUNNEL/200 5921 CONNECT duckduckgo.com:443 - HIER_DIRECT/52.250.42.157 -
1701268121.670      0 192.168.37.138 TCP_DENIED/403 422 HEAD http://youtube.com/ - HIER_NONE/- text/html
1701268131.995      0 192.168.37.138 TCP_DENIED/403 422 HEAD http://facebook.com/ - HIER_NONE/- text/html
1701268165.121      63 192.168.37.138 TCP_MISS/200 1044 POST http://f3.o.lencr.org/ - HIER_DIRECT/118.69.17.77 application/ocsp-response
1701268165.203      43 192.168.37.138 TCP_TUNNEL/200 39 CONNECT push.services.mozilla.com:443 - HIER_DIRECT/34.107.243.93 -
1701268166.529      121 192.168.37.138 TCP_TUNNEL/200 4324 CONNECT www.google.com:443 - HIER_DIRECT/172.217.27.36 -
1701268166.625      37 192.168.37.138 TCP_TUNNEL/200 39 CONNECT www.google.com:443 - HIER_DIRECT/172.217.27.36 -
1701268167.068      552 192.168.37.138 TCP_MISS/200 880 POST http://ocsp.pki.goog/gtsic3 - HIER_DIRECT/142.250.72.163 application/ocsp-response
1701268167.174      407 192.168.37.138 TCP_MISS/200 880 POST http://ocsp.pki.goog/gtsic3 - HIER_DIRECT/142.250.72.163 application/ocsp-response
1701268172.105      0 192.168.37.138 TCP_DENIED/403 4085 CONNECT www.youtube.com:443 - HIER_NONE/- text/html
1701268180.988      0 192.168.37.138 TCP_DENIED/403 4088 CONNECT www.facebook.com:443 - HIER_NONE/- text/html
1701268185.880      12 192.168.37.138 TCP_MISS/200 1044 POST http://f3.o.lencr.org/ - HIER_DIRECT/118.69.17.77 application/ocsp-response
1701268203.587      562 192.168.37.138 TCP_MISS/200 880 POST http://ocsp.pki.goog/gtsic3 - HIER_DIRECT/142.250.72.163 application/ocsp-response
1701268204.559      553 192.168.37.138 TCP_MISS/200 881 POST http://ocsp.pki.goog/gtsic3 - HIER_DIRECT/142.250.72.163 application/ocsp-response
1701268204.577      572 192.168.37.138 TCP_MISS/200 881 POST http://ocsp.pki.goog/gtsic3 - HIER_DIRECT/142.250.72.163 application/ocsp-response
1701268204.684      793 192.168.37.138 TCP_TUNNEL/200 83852 CONNECT www.gstatic.com:443 - HIER_DIRECT/172.217.24.67 -

```

Hình 2 Nội dung file access.log

2.2.5 SquidGuard

SquidGuard là một thành phần bổ sung cho Squid Proxy Server, cung cấp khả năng triển khai bộ lọc nội dung (content filtering) dựa trên danh sách đen và danh sách trắng. SquidGuard cho phép quản lý và kiểm soát truy cập vào các nội dung không phù hợp hoặc độc hại.

2.5.6 Authentication Modules

Squid Proxy Server hỗ trợ nhiều module xác thực, bao gồm NTLM, LDAP, Basic, Digest và nhiều phương thức xác thực khác. Các module này cho phép Squid xác thực người dùng trước khi cho phép truy cập vào các dịch vụ bên ngoài.

2.3 Chức năng của Squid proxy

Squid proxy có hai chức năng chính là content filtering và caching.

Chức năng lọc nội dung (content filtering): Squid Proxy có khả năng áp dụng bộ lọc nội dung để ghi lại, chặn thậm chí điều chỉnh gói tin. Bộ lọc nội dung có thể 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. Điều này giúp ngăn chặn truy cập vào các trang web đáng ngờ, nội dung độc hại, spam hoặc các nguồn tài nguyên không an toàn.

Chức năng caching: Squid Proxy có khả năng lưu cache (bộ nhớ đệm) các tài nguyên được yêu cầu từ máy chủ mục tiêu. Khi một người dùng yêu cầu truy cập vào một tài nguyên, Squid sẽ kiểm tra xem liệu nó đã lưu trữ tài nguyên đó trong cache hay chưa. Nếu có, Squid sẽ trả về tài nguyên từ cache mà không cần tải lại từ máy chủ mục tiêu. Điều này 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.

Ngoài hai chức năng chính trên, Squid proxy còn có một số chức năng khác và cũng có vai trò quan trọng như: chuyển tiếp (forwarding), kiểm soát truy cập (Access control), xác thực (authentication), tối ưu hóa lưu lượng truy cập (Traffic Optimization).

Proxy cung cấp được các chức năng phổ biến và cần thiết của một proxy cần đáp ứng. Vì vậy, nó là một máy chủ phổ biến được sử dụng rộng rãi trong mạng doanh nghiệp, nhà cung cấp dịch vụ Internet, trường học và tổ chức giáo dục, tổ chức chính phủ và phi chính phủ, cũng như trong các hệ thống cloud và trung tâm dữ liệu.

CHƯƠNG 3

TRIỂN KHAI HỆ THỐNG

Squid Proxy là một phần mềm proxy máy chủ mạnh mẽ và phổ biến, có khả năng hoạt động trên nhiều hệ điều hành khác nhau như Ubuntu, CentOS, Fedora, Red Hat,... Trong báo cáo này, chúng tôi xin trình bày về cách cài đặt và cấu hình Squid proxy trên hệ điều hành Ubuntu và CentOS. Đồng thời, chúng tôi cũng sẽ trình bày về mô hình triển khai để thể hiện các chức năng của Squid proxy.

3.1 Cài đặt và cấu hình Squid proxy trên hệ điều hành Ubuntu và CentOS

3.1.1 Cài đặt và cấu hình Squid proxy trên Ubuntu

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
```

3.1.2 Cài đặt và cấu hình Squid proxy trên CentOS

Bước 1: Tiến hành update OS, clean all các package lỗi và cài đặt Squid từ Repo của Centos:

```
$ yum update -y  
$ yum clean all
```

Bước 2: Cài đặt Squid từ Repo của Centos:

```
$ yum -y 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:

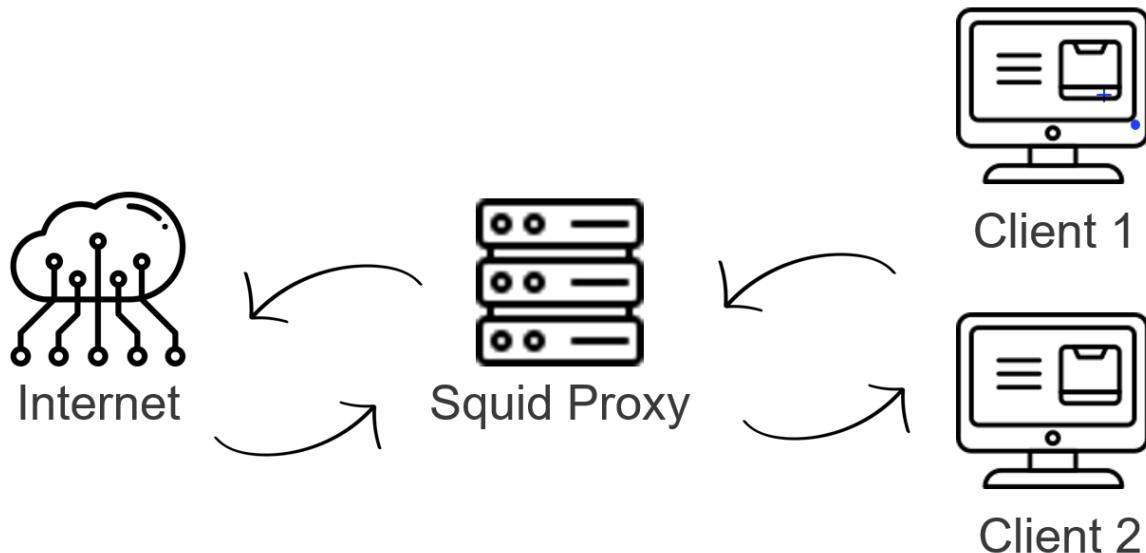
```
$ sudo systemctl status squid
```

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

```
$ vi /etc/squid/squid.conf
```

3.2 Mô hình triển khai

Để thể hiện các chức năng của Squid proxy, chúng tôi sẽ thực hiện qua năm kịch bản là caching http, block domain, authentication, ACL và tổng hợp bốn kịch bản trên. Để thực hiện được điều này, chúng ta sẽ thực hiện qua mô hình mạng bao gồm 01 máy ảo đóng vai trò client, 01 máy ảo đóng vai trò là Squid proxy. Máy client sẽ được cấu hình để giao tiếp internet phải thông qua máy đóng vai trò là Squid proxy. Mô hình minh họa như dưới:



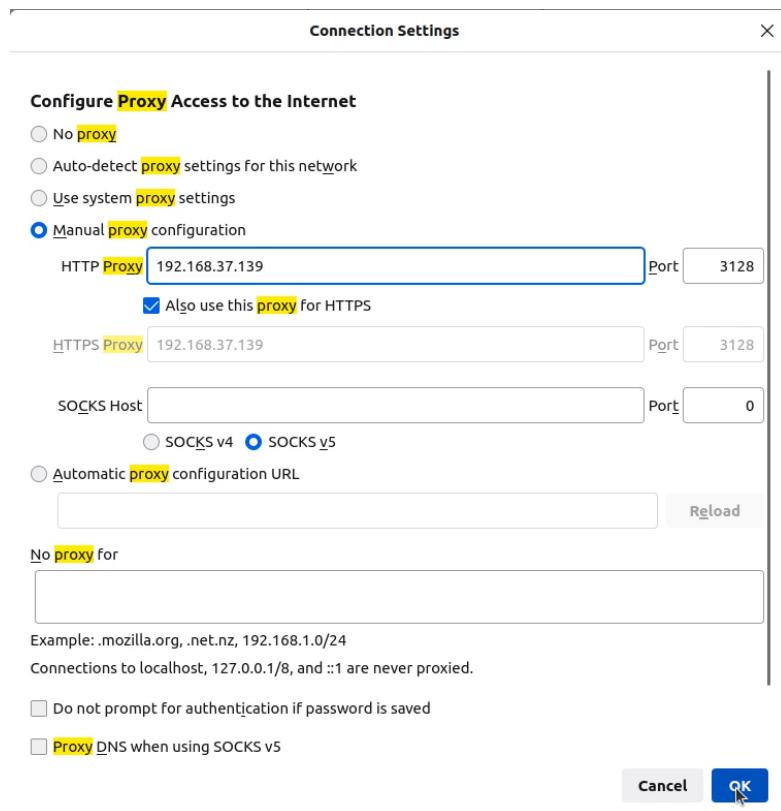
Hình 3 Mô hình triển khai

Chúng tôi lựa chọn hệ điều hành Ubuntu phiên bản 22.04.06 để cài đặt và triển khai mô hình trên. Chúng tôi cài đặt thông qua phần mềm VMware workstation để cài đặt 03 máy ảo sử dụng hệ điều hành Ubuntu trên tương ứng với 01 máy đóng vai trò Squid proxy và 02 máy đóng vai trò Client.

Thông tin địa chỉ IP của các máy như sau:

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

Cài đặt proxy trên các trình duyệt của máy Client 1 và Client 2:



CHƯƠNG 4

THỰC NGHIỆM VÀ ĐÁNH GIÁ

4.1. Thực nghiệm tính năng Caching

- Các bước thực nghiệm chức năng Caching:

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

```
squidproxy@squidproxy-virtual-machine:/etc/squid$ grep -vE '^$|^#' /etc/squid/squid.conf
acl localnet src 0.0.0.1-0.255.255.255 # RFC 1122 "this" network (LAN)
acl localnet src 10.0.0.0/8 # RFC 1918 local private network (LAN)
acl localnet src 100.64.0.0/10 # RFC 6598 shared address space (CGN)
acl localnet src 169.254.0.0/16 # RFC 3927 link-local (directly plugged) machines
acl localnet src 172.16.0.0/12 # RFC 1918 local private network (LAN)
acl localnet src 192.168.0.0/16 # RFC 1918 local private network (LAN)
acl localnet src fc00::/7 # RFC 4193 local private network range
acl localnet src fe80::/10 # RFC 4291 link-local (directly plugged) machines
acl SSL_ports port 443
acl Safe_ports port 80      # http
acl Safe_ports port 21      # ftp
acl Safe_ports port 443     # https
acl Safe_ports port 70      # gopher
acl Safe_ports port 210     # wais
acl Safe_ports port 1025-65535 # unregistered ports
acl Safe_ports port 280     # http-mgmt
acl Safe_ports port 488     # gss-http
acl Safe_ports port 591     # filemaker
acl Safe_ports port 777     # multiling http
http_access deny !Safe_ports
http_access deny CONNECT !SSL_ports
http_access allow localhost manager
http_access deny manager
include /etc/squid/conf.d/*.conf
http_access allow localhost
acl client2 src 192.168.37.0/24
http_access allow client2
http_access deny all
http_port 192.168.37.139:3128
http_port 3128
cache_dir ufs /var/spool/squid 100 16 256
coredump_dir /var/spool/squid
refresh_pattern ^ftp:          1440    20%    10080
refresh_pattern ^gopher:       1440    0%     1440
refresh_pattern -i (/cgi-bin/|/\?) 0    0%     0
refresh_pattern \/(Packages|Sources)(|\.bz2|\.gz|\.xz)$ 0 0% 0 refresh-ims
refresh_pattern \/Release(|\.gpg)$ 0 0% 0 refresh-ims
refresh_pattern \/InRelease$ 0 0% 0 refresh-ims
refresh_pattern \/(Translation-..*)(|\.bz2|\.gz|\.xz)$ 0 0% 0 refresh-ims
refresh_pattern .               0    20%    4320
squidproxy@squidproxy-virtual-machine:/etc/squid$
```

Hình 4 Cấu hình Squid Proxy để thực hiện chức năng Caching

*Giải thích cấu hình: Sử dụng câu lệnh sau để thực hiện chức năng caching

cache_dir ufs /var/spool/squid 100 16 256

+ Bước 2: Áp dụng các cấu hình ở bước 1 vào Squid Proxy

```

squidproxy@squidproxy-virtual-machine:~$ sudo systemctl restart squid
squidproxy@squidproxy-virtual-machine:~$ sudo systemctl status squid
● squid.service - Squid Web Proxy Server
   Loaded: loaded (/lib/systemd/system/squid.service; enabled; vendor preset: enabled)
     Active: active (running) since Wed 2023-11-29 21:16:28 +07; 7s ago
       Docs: man:squid(8)
   Process: 40460 ExecStartPre=/usr/sbin/squid --foreground -z (code=exited, status=0/SUCCESS)
 Main PID: 40464 (squid)
    Tasks: 5 (limit: 4558)
      Memory: 16.4M
        CPU: 297ms
      CGroup: /system.slice/squid.service
              └─ 40464 /usr/sbin/squid --foreground -z
                  ├─ 40466 "(squid-1)" --kid squid-1 --foreground -z
                  ├─ 40467 "(logfile-daemon)" /var/log/squid/access.log
                  ├─ 40468 "(unlinkd)"
                  └─ 40469 "(pinger)"

Thg 11 29 21:16:28 squidproxy-virtual-machine squid[40466]:          0 Objects cancelled.
Thg 11 29 21:16:28 squidproxy-virtual-machine squid[40466]:          0 Duplicate URLs purged.
Thg 11 29 21:16:28 squidproxy-virtual-machine squid[40466]:          0 Swapfile clashes avoided.
Thg 11 29 21:16:28 squidproxy-virtual-machine squid[40466]: Took 0.01 seconds ( 0.00 objects/sec).
Thg 11 29 21:16:28 squidproxy-virtual-machine squid[40466]: Beginning Validation Procedure
Thg 11 29 21:16:28 squidproxy-virtual-machine squid[40466]: ERROR: listen(..., 256) system call failed: (98) Address already in use
                                         listening port: 3128
Thg 11 29 21:16:28 squidproxy-virtual-machine squid[40466]: Completed Validation Procedure
Thg 11 29 21:16:28 squidproxy-virtual-machine squid[40466]: Validated 0 Entries
Thg 11 29 21:16:28 squidproxy-virtual-machine squid[40466]: store_swap_size = 0.00 KB
Thg 11 29 21:16:29 squidproxy-virtual-machine squid[40466]: storeLateRelease: released 0 objects

```

Hình 5 Kiểm tra trạng thái của Squid proxy sau khi restart lần 1

+ Bước 3: 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
```

- Kết quả thực nghiệm thu được:

+ Lần truy cập trang web đầu tiên ở máy Client2

```

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://duckduckgogg42xjoc72x3jasowoarfbcnvvfimaftt6twagswczad.onion/ https://spreadprivacy.com ; manifest-src https://duckduckgo.com https://*.duckduckgo.com https://duckduckgogg42xjoc72x3jasowoarfbcnvvfimaftt6twagswczad.onion/ https://spreadprivacy.com ; script-src blob: https://duckduckgo.com https://*.duckduckgo.com https://duckduckgogg42xjoc72x3jasowoarfbcnvvfimaftt6twagswczad.onion/ https://spreadprivacy.com ; style-src https://duckduckgo.com https://*.duckduckgo.com https://duckduckgogg42xjoc72x3jasowoarfbcnvvfimaftt6twagswczad.onion/ https://spreadprivacy.com ; font-src data: https://duckduckgo.com https://*.duckduckgo.com https://duckduckgogg42xjoc72x3jasowoarfbcnvvfimaftt6twagswczad.onion/ https://spreadprivacy.com ; media-src https://duckduckgo.com https://*.duckduckgo.com https://duckduckgogg42xjoc72x3jasowoarfbcnvvfimaftt6twagswczad.onion/ https://spreadprivacy.com ; frame-src https://duckduckgo.com https://*.duckduckgo.com https://duckduckgogg42xjoc72x3jasowoarfbcnvvfimaftt6twagswczad.onion/ https://spreadprivacy.com ; frame-ancestors 'self' ; base-uri 'self' ; block-all-mixed-content ;
X-Frame-Option: 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
Cache: MISS from squidproxy-virtual-machine
X-Cache-Lookup: MISS from squidproxy-virtual-machine:3128
Vla: 1.1 squidproxy-virtual-machine (squid/5.7)
Connection: keep-alive

```

Hình 6 Phản hồi của trang web trên máy Client 2 khi truy cập đến trang web lần đầu tiên

➔ Không sử dụng Cache của squidproxy-virtual-machine

+ Lần truy cập trang web lần thứ 2 ở máy Client2

```

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://duckduckgogg42xjoc72x3sjasowoarfbgcmvflmafft6twagswczad.onion/ https://spreadprivacy.com ; manifest-src https://duckduckgo.com https://duckduckgogg42xjoc72x3sjasowoarfbgcmvflmafft6twagswczad.onion/ https://spreadprivacy.com ; media-src https://duckduckgo.com https://duckduckgogg42xjoc72x3sjasowoarfbgcmvflmafft6twagswczad.onion/ https://spreadprivacy.com ; script-src blob: https://duckduckgo.com https://duckduckgogg42xjoc72x3sjasowoarfbgcmvflmafft6twagswczad.onion/ https://spreadprivacy.com ; style-src https://duckduckgo.com https://duckduckgogg42xjoc72x3sjasowoarfbgcmvflmafft6twagswczad.onion/ https://spreadprivacy.com ; unsafe-inline ; font-src data: https://duckduckgo.com https://duckduckgogg42xjoc72x3sjasowoarfbgcmvflmafft6twagswczad.onion/ https://spreadprivacy.com ; img-src data: https://duckduckgo.com https://duckduckgogg42xjoc72x3sjasowoarfbgcmvflmafft6twagswczad.onion/ https://spreadprivacy.com ; object-src 'none' ; worker-src blob: https://duckduckgo.com https://duckduckgogg42xjoc72x3sjasowoarfbgcmvflmafft6twagswczad.onion/ https://spreadprivacy.com ; frame-src blob: https://duckduckgo.com https://duckduckgogg42xjoc72x3sjasowoarfbgcmvflmafft6twagswczad.onion/ https://spreadprivacy.com ; form-action https://duckduckgo.com https://duckduckgogg42xjoc72x3sjasowoarfbgcmvflmafft6twagswczad.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
Referer-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

```

Hình 7 Phản hồi của trang web trên máy Client 2 khi truy cập đến trang web lần thứ hai

➔ Đã sử dụng Cache của squidproxy-virtual-machine

+ Lịch sử truy cập của Squid Proxy

```

squidproxy@squidproxy-virtual-machine:/var/log/squid$ sudo cat access.log
1701267258.238      1 192.168.37.138 TCP_DENIED/403 422 HEAD http://duckduckgo.com/ - HIER_NONE/- text/html
1701267295.611      0 192.168.37.138 TCP_DENIED/403 422 HEAD http://duckduckao.com/ - HIER_NONE/- text/html
1701267406.577      441 192.168.37.138 TCP_MISS/301 2426 HEAD http://duckduckgo.com/ - HIER_DIRECT/52.250.42.157 text/html
1701267489.432     82853 192.168.37.138 TCP_TUNNEL/200 3616 CONNECT duckduckao.com:443 - HIER_DIRECT/52.250.42.157 -
1701267490.872      0 192.168.37.138 TCP_MEM_HIT/301 2433 HEAD http://duckduckgo.com/ - HIER_NONE/- text/html
1701267492.672     1799 192.168.37.138 TCP_TUNNEL/200 5943 CONNECT duckduckgo.com:443 - HIER_DIRECT/52.250.42.157 -

```

Hình 8 Kiểm tra lịch sử truy cập trên Squid proxy

4.2. Thực nghiệm tính năng Content Filtering

4.2.1. Thực nghiệm tính năng Block Domain trong ContentFiltering

- Các bước thực nghiệm tính năng Block Domain

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

```

squidproxy@squidproxy-virtual-machine:/etc/squid$ grep -vE '^$|^#' /etc/squid/squid.conf
acl localnet src 0.0.0.1-0.255.255.255 # RFC 1122 "this" network (LAN)
acl localnet src 10.0.0.0/8           # RFC 1918 local private network (LAN)
acl localnet src 100.64.0.0/10        # RFC 6598 shared address space (CGN)
acl localnet src 169.254.0.0/16       # RFC 3927 link-local (directly plugged) machines
acl localnet src 172.16.0.0/12         # RFC 1918 local private network (LAN)
acl localnet src 192.168.0.0/16        # RFC 1918 local private network (LAN)
acl localnet src fc00::/7             # RFC 4193 local private network range
acl localnet src fe80::/10            # RFC 4291 link-local (directly plugged) machines
acl SSL_ports port 443
acl Safe_ports port 80      # http
acl Safe_ports port 21      # ftp
acl Safe_ports port 443     # https
acl Safe_ports port 70      # gopher
acl Safe_ports port 210     # wais
acl Safe_ports port 1025-65535 # unregistered ports
acl Safe_ports port 280     # http-nginx
acl Safe_ports port 488     # gss-http
acl Safe_ports port 591     # filemaker
acl Safe_ports port 777     # multiling http
http_access deny !Safe_ports
http_access deny CONNECT !SSL_ports
http_access allow localhost manager
http_access deny manager
include /etc/squid/conf.d/*.conf
http_access allow localhost
acl blocked_websites dstdomain .youtube.com .facebook.com .twitter.com .reddit.com
acl client2 src 192.168.37.0/24
http_access deny blocked_websites
http_access allow client2
http_access deny all
http_port 192.168.37.139:3128
http_port 3128
coredump_dir /var/spool/squid
refresh_pattern ^ftp:          1440    20%    10080
refresh_pattern ^gopher:        1440    0%     1440
refresh_pattern -i (/cgi-bin/|/?) 0      0%     0
refresh_pattern /(Packages|Sources)(|\.bz2|\.gz|\.xz)$ 0 0% 0 refresh-ims
refresh_pattern /Release(\\.gpg)$ 0 0% 0 refresh-ims
refresh_pattern /InRelease$ 0 0% 0 refresh-ims
refresh_pattern /(Translation-*)(|\.bz2|\.gz|\.xz)$ 0 0% 0 refresh-ims
refresh_pattern .               0      20%    4320
squidproxy@squidproxy-virtual-machine:/etc/squid$ 

```

Hình 9 Cấu hình Squid proxy để thực hiện chức năng Block Domain

*Giải thích: Sử dụng 2 câu lệnh sau để thực hiện tính năng Block Domain

acl blocked_websites dstdomain .youtube.com .facebook.com .twitter.com .reddit.com

http_access deny blocked_websites

+ Bước 2: Áp dụng các cấu hình ở bước 1 vào Squid Proxy

```

squidproxy@squidproxy-virtual-machine:~$ sudo systemctl restart squid
squidproxy@squidproxy-virtual-machine:~$ sudo systemctl status squid
● squid.service - Squid Web Proxy Server
   Loaded: loaded (/lib/systemd/system/squid.service; enabled; vendor preset: enabled)
     Active: active (running) since Wed 2023-11-29 21:28:22 +07; 7s ago
       Docs: man:squid(8)
   Process: 40546 ExecStartPre=/usr/sbin/squid --foreground -z (code=exited, status=0/SUCCESS)
 Main PID: 40549 (squid)
    Tasks: 4 (limit: 4558)
      Memory: 16.1M
        CPU: 220ms
       CGroup: /system.slice/squid.service
           ├─40549 /usr/sbin/squid --foreground -sYC
           ├─40551 "(squid-1)" --kid squid-1 --foreground -sYC
           ├─40552 "(logfile-daemon)" /var/log/squid/access.log
           └─40553 "(pinger)"

Thg 11 29 21:28:22 squidproxy-virtual-machine squid[40551]: Finished loading MIME types and icons.
Thg 11 29 21:28:22 squidproxy-virtual-machine squid[40551]: HTTP Disabled.
Thg 11 29 21:28:22 squidproxy-virtual-machine squid[40551]: Pinger socket opened on FD 15
Thg 11 29 21:28:22 squidproxy-virtual-machine squid[40551]: Squid plugin modules loaded: 0
Thg 11 29 21:28:22 squidproxy-virtual-machine squid[40551]: Adaptation support is off.
Thg 11 29 21:28:22 squidproxy-virtual-machine squid[40551]: Accepting HTTP Socket connections at conn3 local=192.168.37.139:3128 remote=[::] FD 12 flags=9
Thg 11 29 21:28:22 squidproxy-virtual-machine systemd[1]: Started Squid Web Proxy Server.
Thg 11 29 21:28:22 squidproxy-virtual-machine squid[40551]: Accepting HTTP Socket connections at conn5 local=[::]:3128 remote=[::] FD 13 flags=9
Thg 11 29 21:28:22 squidproxy-virtual-machine squid[40551]: ERROR: listen(..., 256) system call failed: (98) Address already in use
                                                listening port: 3128
Thg 11 29 21:28:23 squidproxy-virtual-machine squid[40551]: storeLateRelease: released 0 objects
squidproxy@squidproxy-virtual-machine:~$ █

```

Hình 10 Kiểm tra trạng thái của Squid proxy sau khi restart lần 2

+ Bước 3: 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
```

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

- Kết quả thực nghiệm:

+ Sử dụng câu lệnh trong terminal

```

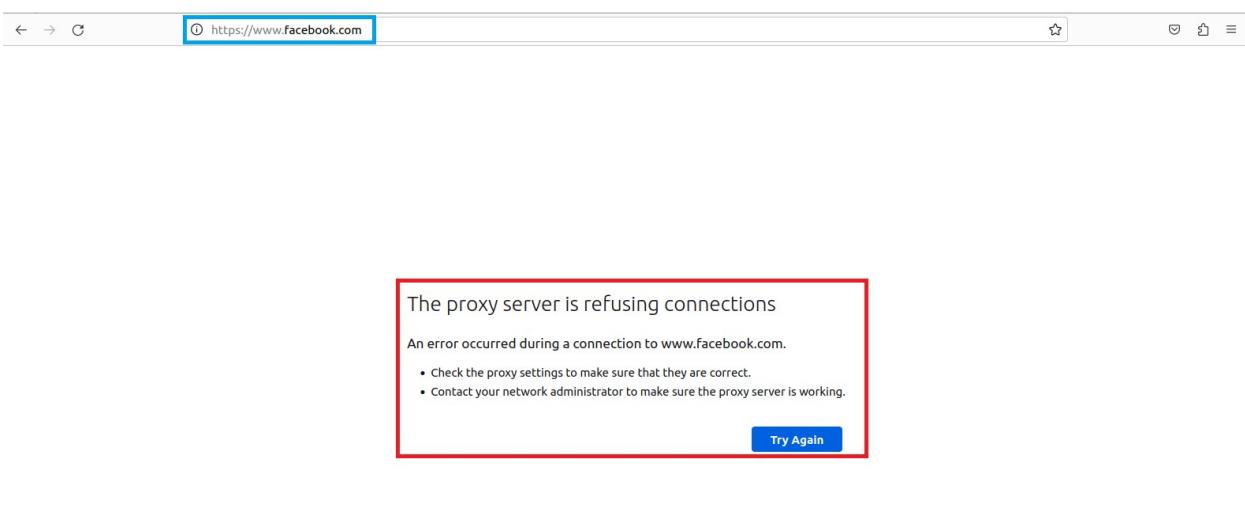
client2@client2-virtual-machine:~$ curl -x http://192.168.37.139:3128 -I -L http://youtube.com
HTTP/1.1 403 Forbidden
Server: squid/5.7
Mime-Version: 1.0
Date: Wed, 29 Nov 2023 14:28:41 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 3539
X-Squid-Error: ERR_ACCESS_DENIED 0
Vary: Accept-Language
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

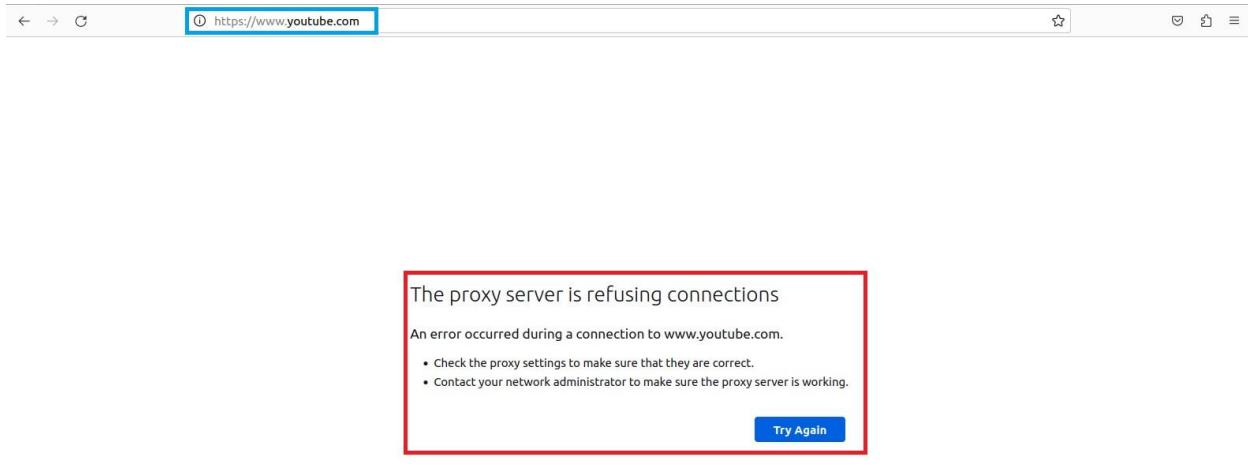
```

Hình 11 Phản hồi của trang web khi gửi yêu cầu đến có đi qua Squid proxy

- ➔ Client 2 đã bị từ chối truy cập vào các trang web trong danh sách domain bị block
+ Sử dụng trình duyệt Firefox:



Hình 12 Phản hồi nhận được khi truy cập trang web bị chặn (1)



Hình 13 Phản hồi nhận được khi truy cập trang web bị chặn (2)

➔ Client 2 đã bị từ chối truy cập vào các trang web trong danh sách domain bị block



Hình 14 Phản hồi nhận được khi truy cập trang web không bị chặn (3)

➔ Client 2 được phép khi truy cập các trang web không có trong danh sách domain bị block

4.2.2. Thực nghiệm tính năng Block Words trong ContentFiltering

- Các bước thực nghiệm tính năng Block Words

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

```

GNU nano 6.2
gambling
drugs
violence
hacking
torrent
social-media
gaming
phishing
malware
war
crypto
youtube
spotify
facebook
binance

```

Hình 15 Nội dung file blacklist.txt

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

```

squidproxy@squidproxy-virtual-machine:~$ grep -vE '^$|^#' /etc/squid/squid.conf
acl localnet src 0.0.0.1-0.255.255.255 # RFC 1122 "this" network (LAN)
acl localnet src 10.0.0.0/8 # RFC 1918 local private network (LAN)
acl localnet src 100.64.0.0/10 # RFC 6598 shared address space (CGN)
acl localnet src 169.254.0.0/16 # RFC 3927 link-local (directly plugged) machines
acl localnet src 172.16.0.0/12 # RFC 1918 local private network (LAN)
acl localnet src 192.168.0.0/16 # RFC 1918 local private network (LAN)
acl localnet src fc00::/7 # RFC 4193 local private network range
acl localnet src fe80::/10 # RFC 4291 link-local (directly plugged) machines
acl SSL_ports port 443
acl Safe_ports port 80 # http
acl Safe_ports port 21 # ftp
acl Safe_ports port 443 # https
acl Safe_ports port 70 # gopher
acl Safe_ports port 210 # wais
acl Safe_ports port 1025-65535 # unregistered ports
acl Safe_ports port 280 # http-mgmt
acl Safe_ports port 488 # gss-http
acl Safe_ports port 591 # filemaker
acl Safe_ports port 777 # multiling http
http_access deny !Safe_ports
http_access deny CONNECT !SSL_ports
http_access allow localhost manager
http_access deny manager
include /etc/squid/conf.d/*.conf
acl blacklist url_regex -i "/etc/squid/blacklist.txt"
http_access deny blacklist
http_access allow localhost
acl client2 src 192.168.37.0/24
http_access allow client2
http_access deny all
http_port 192.168.37.139:3128
http_port 3128
cache_dir ufs /var/spool/squid 100 16 256
coredump_dir /var/spool/squid
refresh_pattern ^ftp: 1440 20% 10080
refresh_pattern ^gopher: 1440 0% 1440
refresh_pattern -i (/cgi-bin/|\.?) 0 0% 0
refresh_pattern /(Packages|Sources)(|\.bz2|\.gz|\.xz)$ 0 0% 0 refresh-ims
refresh_pattern /Release(|\.gpg)$ 0 0% 0 refresh-ims
refresh_pattern /InRelease$ 0 0% 0 refresh-ims
refresh_pattern /(Translation-.*)(|\.bz2|\.gz|\.xz)$ 0 0% 0 refresh-ims
refresh_pattern . 0 20% 4320
squidproxy@squidproxy-virtual-machine:~$
```

Hình 16 Cấu hình Squid proxy để thực hiện chức năng Block words

*Giải thích: Sử dụng 2 câu lệnh sau để thực hiện tính năng Block Word

acl blacklist url_regex -i “/etc/squid/blacklist.txt”

http_access deny blacklist

+ Bước 3: Áp dụng các cấu hình ở bước 2 vào Squid Proxy

```
squidproxy@squidproxy-virtual-machine: $ sudo nano /etc/squid/blacklist.txt
squidproxy@squidproxy-virtual-machine: $ sudo systemctl restart squid
squidproxy@squidproxy-virtual-machine: $ sudo systemctl status squid
● squid.service - Squid Web Proxy Server
   Loaded: loaded (/lib/systemd/system/squid.service; enabled; vendor preset: enabled)
   Active: active (running) since Thu 2023-11-30 20:35:21 +07; 5s ago
     Docs: man:squid(8)
     Process: 2861 ExecStartPre=/usr/sbin/squid --foreground -z (code=exited, status=0/SUCCESS)
    Main PID: 2864 (squid)
       Tasks: 5 (limit: 4556)
      Memory: 16.5M
        CPU: 615ms
       CGroup: /system.slice/squid.service
           ├─2864 /usr/sbin/squid --foreground -sYC
           ├─2866 "(squid-1)" --kid squid-1 --foreground -sYC
           ├─2867 "(logfile-daemon)" /var/log/squid/access.log
           ├─2868 "(unlinkd)"
           └─2869 "(pinger)"

Thg 11 30 20:35:21 squidproxy-virtual-machine squid[2866]:          0 Objects cancelled.
Thg 11 30 20:35:21 squidproxy-virtual-machine squid[2866]:          0 Duplicate URLs purged.
Thg 11 30 20:35:21 squidproxy-virtual-machine squid[2866]:          0 Swapfile clashes avoided.
Thg 11 30 20:35:21 squidproxy-virtual-machine squid[2866]: Took 0.03 seconds (4990.21 objects/sec).
Thg 11 30 20:35:21 squidproxy-virtual-machine squid[2866]: Beginning Validation Procedure
Thg 11 30 20:35:21 squidproxy-virtual-machine squid[2866]: ERROR: listen(..., 256) system call failed: (98) Address already in use
                                                listening port: 3128
Thg 11 30 20:35:21 squidproxy-virtual-machine squid[2866]: Completed Validation Procedure
Thg 11 30 20:35:21 squidproxy-virtual-machine squid[2866]: Validated 130 Entries
Thg 11 30 20:35:21 squidproxy-virtual-machine squid[2866]: store_swap_size = 2124.00 KB
Thg 11 30 20:35:22 squidproxy-virtual-machine squid[2866]: storeLateRelease: released 0 objects
squidproxy@squidproxy-virtual-machine: $
```

Hình 17 Kiểm tra trạng thái của Squid proxy sau khi restart lần 3

Bước 4: 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://crypto.com
```

- Cách 2: Sử dụng trình duyệt Firefox để truy cập các trang web có chứa từ trong danh sách block và các từ không có danh sách block

- Kết quả thực nghiệm

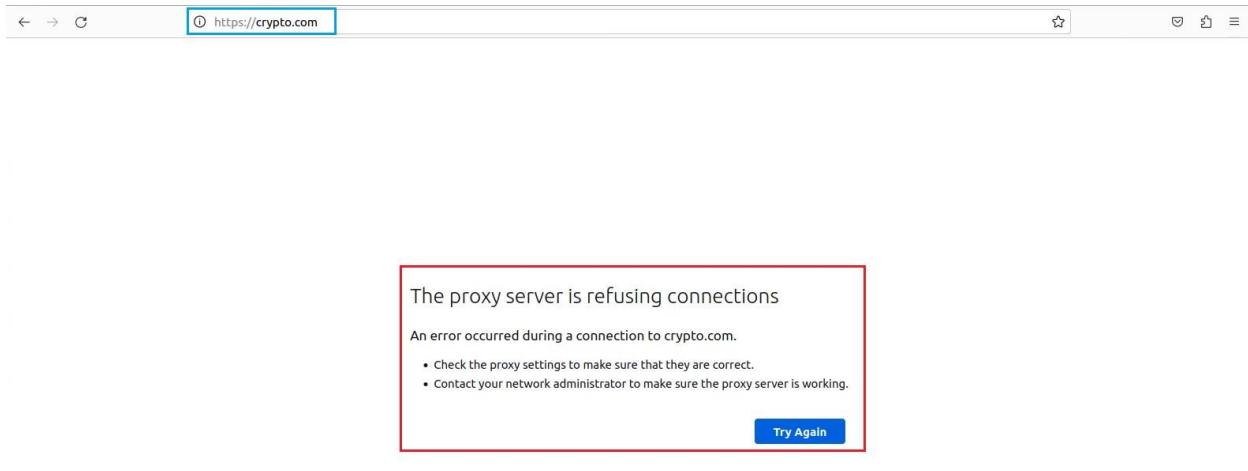
+ Sử dụng câu lệnh terminal:

```
client2@client2-virtual-machine:~$ curl -x http://192.168.37.139:3128 -I https://crypto.com
HTTP/1.1 403 Forbidden
Server: squid/5.7
Mime-Version: 1.0
Date: Thu, 30 Nov 2023 13:35:35 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 3523
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

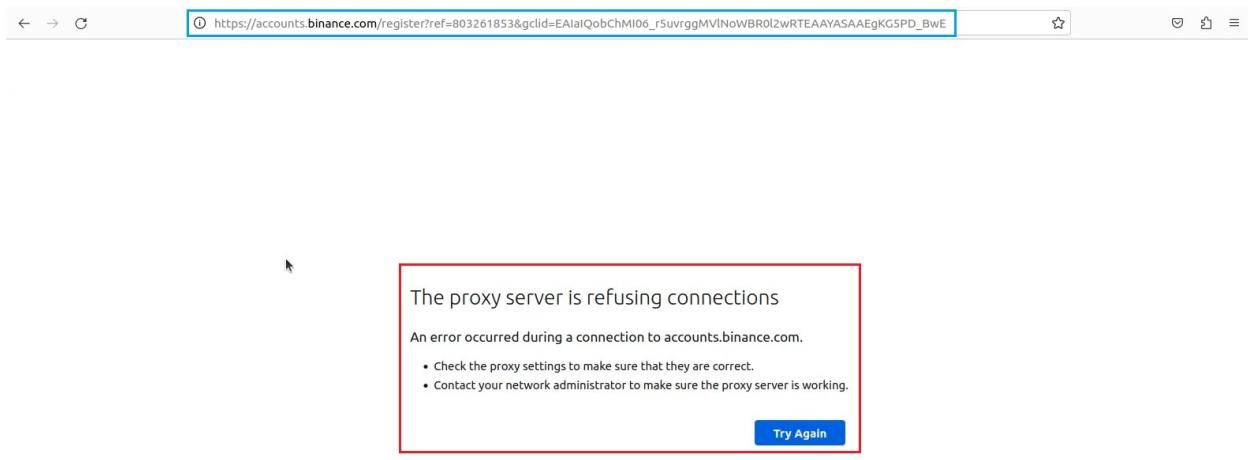
curl: (56) Received HTTP code 403 from proxy after CONNECT
client2@client2-virtual-machine:~$
```

Hình 18 Phản hồi nhận được khi truy cập trang web có chứa từ có trong blacklist (1)

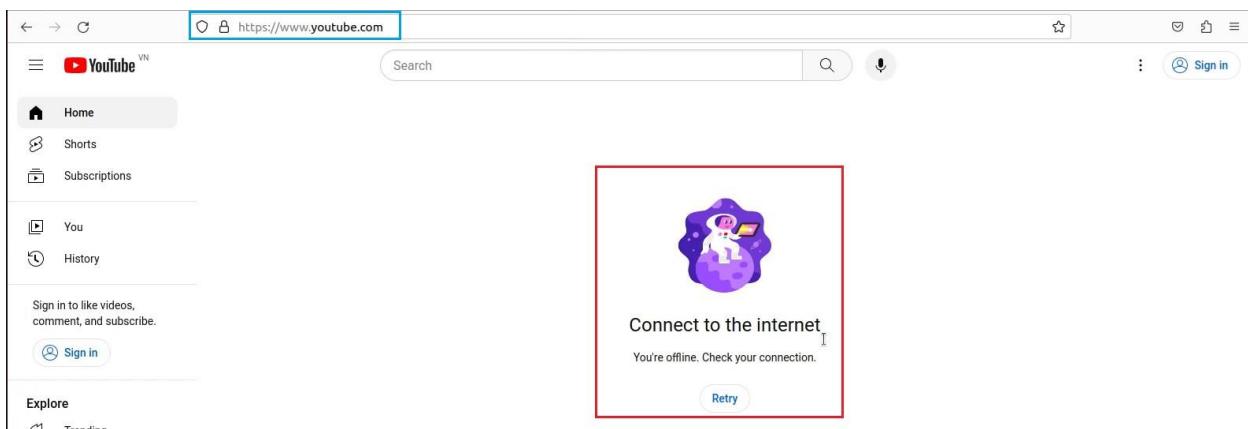
- ➔ Client 2 đã bị từ chối truy cập vào các trang web có từ nằm trong danh sách blacklist
+ Sử dụng trình duyệt Firefox:



Hình 19 Phản hồi nhận được khi truy cập trang web có chứa từ có trong blacklist (2)



Hình 20 Phản hồi nhận được khi truy cập trang web có chứa từ có trong blacklist (3)



Hình 21 Phản hồi nhận được khi truy cập trang web có chứa từ có trong blacklist (4)

➔ Client 2 đã bị từ chối truy cập vào các trang web có từ nằm trong danh sách blacklist



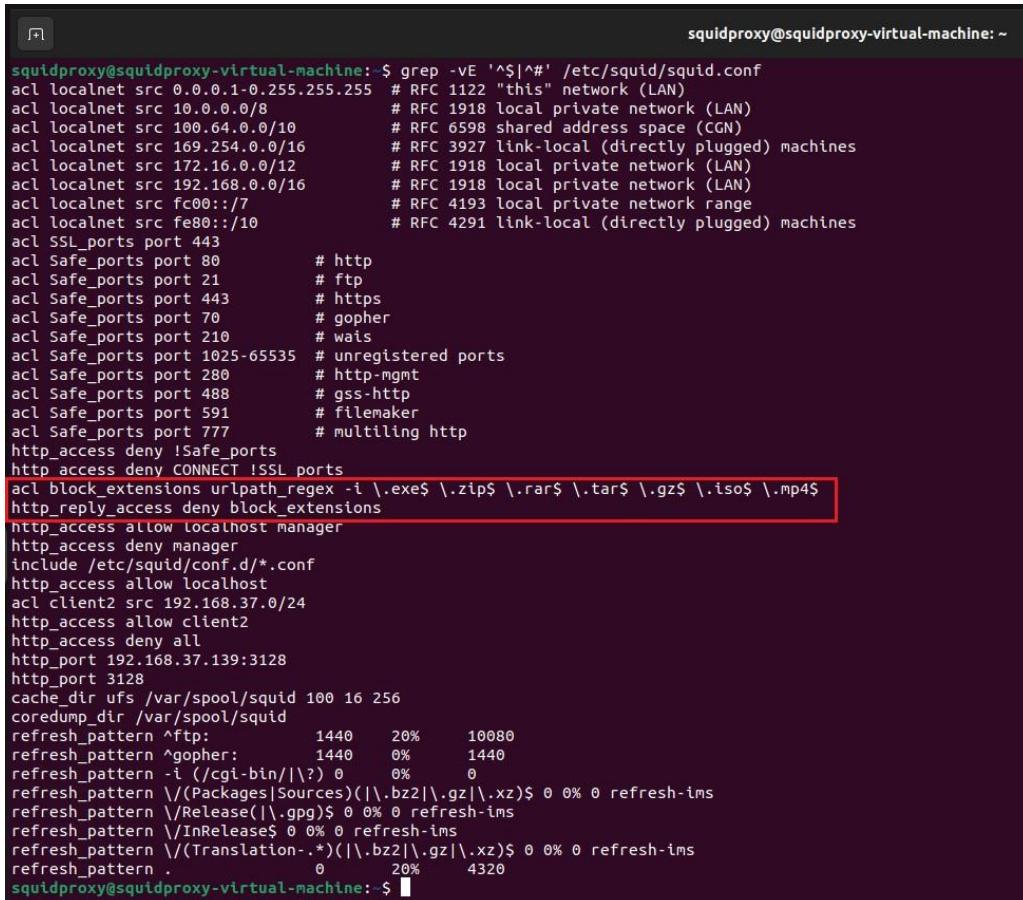
Hình 22 Phản hồi nhận được khi truy cập trang web không chứa từ có trong blacklist

➔ Client 2 được phép khi truy cập các trang web không có từ nằm trong danh sách blacklist

4.2.3. Thực nghiệm tính năng Block Download trong ContentFiltering

- Các bước thực nghiệm tính năng Block Download:

+ Bước 1: Cấu hình Squid Proxy để thực hiện chức năng trên (nhưng thiếu file có phần mở rộng .mp3)



```
squidproxy@squidproxy-virtual-machine: ~
squidproxy@squidproxy-virtual-machine: $ grep -EV '^$|^#' /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
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
refresh_pattern ^ftp:          1440    20%    10080
refresh_pattern ^gopher:       1440    0%     1440
refresh_pattern -i (/cgi-bin/|\.?) 0    0%    0
refresh_pattern \/(Packages|Sources)(\|.bz2|\|.gz|\|.xz)\$ 0 0% 0 refresh-ims
refresh_pattern \/Release(\|.gpg)\$ 0 0% 0 refresh-ims
refresh_pattern \/InRelease\$ 0 0% 0 refresh-ims
refresh_pattern \/(Translation-.*)(\|.bz2|\|.gz|\|.xz)\$ 0 0% 0 refresh-ims
refresh_pattern .               0    20%   4320
squidproxy@squidproxy-virtual-machine: $
```

Hình 23 Cấu hình Squid proxy để thực hiện chức năng block download

* Giải thích: Sử dụng 2 câu lệnh sau để thực hiện tính năng Block Download

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

+ Bước 2: Áp dụng các cấu hình ở bước 1 vào Squid Proxy

```

squidproxy@squidproxy-virtual-machine:~$ sudo systemctl restart squid
squidproxy@squidproxy-virtual-machine:~$ sudo systemctl status squid
● squid.service - Squid Web Proxy Server
   Loaded: loaded (/lib/systemd/system/squid.service; enabled; vendor preset: enabled)
   Active: active (running) since Thu 2023-11-30 21:24:19 +07; 7s ago
     Docs: man:squid(8)
 Process: 3928 ExecStartPre=/usr/sbin/squid --foreground -z (code=exited, status=0/SUCCESS)
 Main PID: 3932 (squid)
   Tasks: 5 (limit: 4556)
    Memory: 16.6M
      CPU: 332ms
     CGroup: /system.slice/squid.service
             └─3932 /usr/sbin/squid --foreground -sYC
                 ├─3934 "(squid-1)" --kid squid-1 --foreground -sYC
                 ├─3935 "(logfile-daemon)" /var/log/squid/access.log
                 ├─3936 "(unlndkd)"
                 └─3937 "(pinger)"

Thg 11 30 21:24:19 squidproxy-virtual-machine squid[3934]:          0 Objects cancelled.
Thg 11 30 21:24:19 squidproxy-virtual-machine squid[3934]:          0 Duplicate URLs purged.
Thg 11 30 21:24:19 squidproxy-virtual-machine squid[3934]:          0 Swapfile clashes avoided.
Thg 11 30 21:24:19 squidproxy-virtual-machine squid[3934]: Took 0.01 seconds (8966.14 objects/sec).
Thg 11 30 21:24:19 squidproxy-virtual-machine squid[3934]: Beginning Validation Procedure
Thg 11 30 21:24:19 squidproxy-virtual-machine squid[3934]: ERROR: listen(..., 256) system call failed: (98) Address already in use
                                         listening port: 3128
Thg 11 30 21:24:19 squidproxy-virtual-machine squid[3934]: Completed Validation Procedure
Thg 11 30 21:24:19 squidproxy-virtual-machine squid[3934]: Validated 130 Entries
Thg 11 30 21:24:19 squidproxy-virtual-machine squid[3934]: store_swap_size = 2124.00 KB
Thg 11 30 21:24:20 squidproxy-virtual-machine squid[3934]: storeLateRelease: released 0 objects
squidproxy@squidproxy-virtual-machine:~$ █

```

Hình 24 Kiểm tra trạng thái của Squid proxy sau khi restart lần 4

- + Bước 3: 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 block
- + Bước 4: Thực hiện cấu hình lại Squid Proxy có cả block file .mp3 để chứng minh thực nghiệm đúng

```

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\$ \.mp3\$ \.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
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
refresh_pattern ^ftp:          1440    20%    10080
refresh_pattern ^gopher:       1440    0%     1440
refresh_pattern -i (/cgi-bin/|/\?) 0    0%     0
refresh_pattern \/(Packages|Sources)(|\.\bz2|\.\gz|\.\xz)\$ 0 0% 0 refresh-ims
refresh_pattern \/Release(|\.\gpg)\$ 0 0% 0 refresh-ims
refresh_pattern \/InRelease\$ 0 0% 0 refresh-ims
refresh_pattern \/(Translation-.*)(|\.\bz2|\.\gz|\.\xz)\$ 0 0% 0 refresh-ims
refresh_pattern .              0    20%    4320
squidproxy@squidproxy-virtual-machine:~$ 

```

Hình 25 Cấu hình Squid proxy để block download file .mp3

* Giải thích: Sử dụng 2 câu lệnh sau để thực hiện tính năng Block Download

acl block_extensions urlpath_regex -I \.exe\\$ \.zip\\$ \.rar\\$ \.tar\\$ \.gz\\$ \.iso\\$ \.mp3\\$ \.mp4\\$

http_access deny block_extensions

+ Bước 5: Áp dụng các cấu hình ở bước 4 vào Squid Proxy

```

squidproxy@squidproxy-virtual-machine:~$ sudo systemctl restart squid
squidproxy@squidproxy-virtual-machine:~$ sudo systemctl status squid
● squid.service - Squid Web Proxy Server
   Loaded: loaded (/lib/systemd/system/squid.service; enabled; vendor preset: enabled)
   Active: active (running) since Thu 2023-11-30 21:26:06 +07; 10s ago
     Docs: man:squid(8)
 Process: 3958 ExecStartPre=/usr/sbin/squid --foreground -z (code=exited, status=0/SUCCESS)
 Main PID: 3961 (squid)
    Tasks: 5 (limit: 4556)
      Memory: 16.6M
        CPU: 295ms
       CGroup: /system.slice/squid.service
           ├─3961 /usr/sbin/squid --foreground -SYC
           ├─3963 "(squid-1)" --kid squid-1 --foreground -SYC
           ├─3964 "(logfile-daemon)" /var/log/squid/access.log
           ├─3965 "(unlinkd)"
           └─3966 "(pinger)"

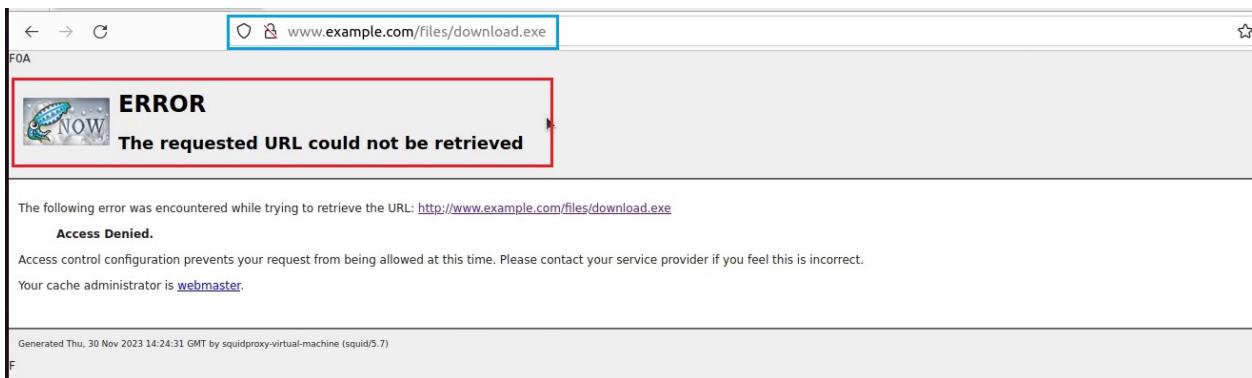
Thg 11 30 21:26:06 squidproxy-virtual-machine squid[3963]:          0 Objects cancelled.
Thg 11 30 21:26:06 squidproxy-virtual-machine squid[3963]:          0 Duplicate URLs purged.
Thg 11 30 21:26:06 squidproxy-virtual-machine squid[3963]:          0 Swapfile clashes avoided.
Thg 11 30 21:26:06 squidproxy-virtual-machine squid[3963]: Took 0.01 seconds (10044.82 objects/sec).
Thg 11 30 21:26:06 squidproxy-virtual-machine squid[3963]: Beginning Validation Procedure
Thg 11 30 21:26:06 squidproxy-virtual-machine squid[3963]: ERROR: listen(..., 256) system call failed: (98) Address already in use
                                         listening port: 3128
Thg 11 30 21:26:06 squidproxy-virtual-machine squid[3963]: Completed Validation Procedure
Thg 11 30 21:26:06 squidproxy-virtual-machine squid[3963]: Validated 130 Entries
Thg 11 30 21:26:06 squidproxy-virtual-machine squid[3963]: store_swap_size = 2124.00 KB
Thg 11 30 21:26:07 squidproxy-virtual-machine squid[3963]: storeLateRelease: released 0 objects
squidproxy@squidproxy-virtual-machine:~$
```

Hình 26 Kiểm tra trạng thái Squid proxy sau khi restart lần 5

+ Bước 6: Thực hiện tương tự với bước 3

- Kết quả thực nghiệm:

+ Đối với trường hợp thiếu file .mp3 trong cấu hình:



Hình 27 Phản hồi nhận được khi thực hiện tải file có phần mở rộng bị chặn (1)

The screenshot shows a web browser window with the URL www.example.com/files/download.iso. A red box highlights the error message area. The message reads "ERROR" with a small icon, followed by "The requested URL could not be retrieved". Below this, a smaller text box contains the following error details:

The following error was encountered while trying to retrieve the URL: <http://www.example.com/files/download.iso>

Access Denied.

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

Your cache administrator is [webmaster](#).

Generated Thu, 30 Nov 2023 14:24:44 GMT by squidproxy-virtual-machine (squid/5.7)

Hình 28 Phản hồi nhận được khi thực hiện tải file có phần mở rộng bị chặn (2)

The screenshot shows a web browser window with the URL www.example.com/files/download.mp3. A red box highlights the error message area. The message reads "Example Domain" with a small icon, followed by "This domain is for use in illustrative examples in documents. You may use this domain in literature without prior coordination or asking for permission." Below this, a link "More information..." is visible.

Hình 29 Phản hồi nhận được khi thực hiện tải file có phần mở rộng mp3 khi chưa bị chặn

➔ Client 2 không thể download các phần mở rộng có trong danh sách block. File .mp3 chưa có cấu hình nên Client 2 có thể truy cập đến và download thành công.

+ Đối với trường hợp có file .mp3 trong cấu hình:

The screenshot shows a web browser window with the URL www.example.com/files/download.exe. A red box highlights the error message area. The message reads "ERROR" with a small icon, followed by "The requested URL could not be retrieved". Below this, a smaller text box contains the following error details:

The following error was encountered while trying to retrieve the URL: <http://www.example.com/files/download.exe>

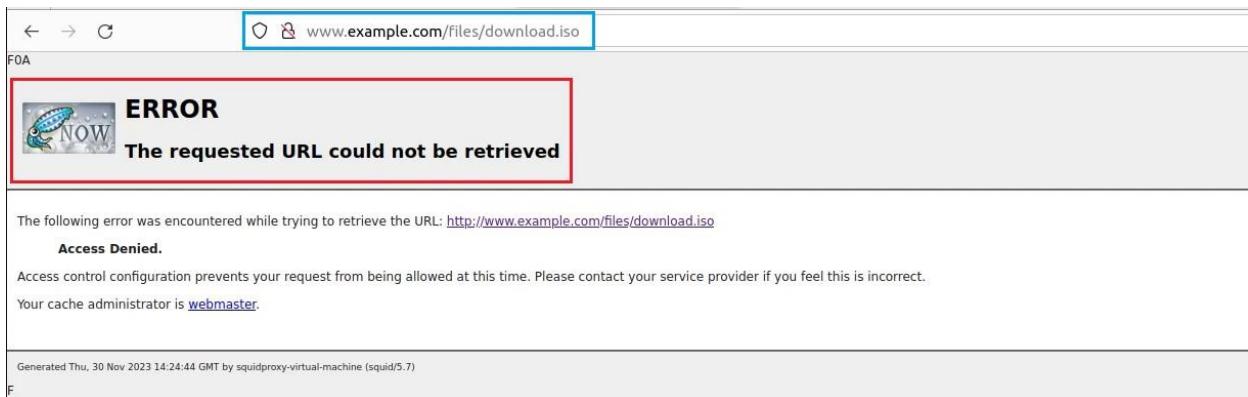
Access Denied.

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

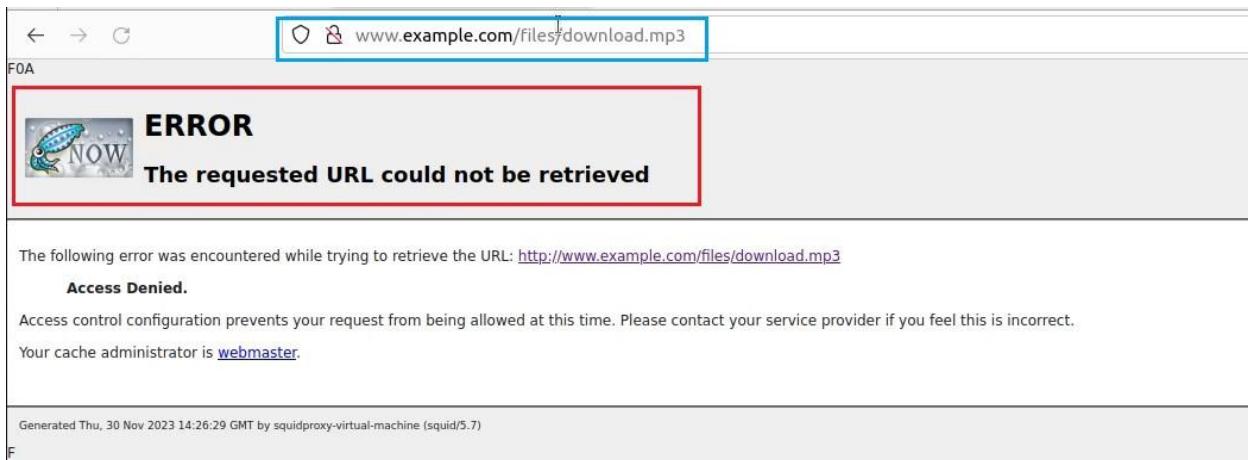
Your cache administrator is [webmaster](#).

Generated Thu, 30 Nov 2023 14:24:31 GMT by squidproxy-virtual-machine (squid/5.7)

Hình 30 Phản hồi nhận được khi thực hiện tải file có phần mở rộng bị chặn (3)



Hình 31 Phản hồi nhận được khi thực hiện tải file có phần mở rộng bị chặn (4)



Hình 32 Phản hồi nhận được khi thực hiện tải file có phần mở rộng mp3 khi đã bị chặn

➔ Client 2 không thể download các phần mở rộng có trong danh sách block. File .mp3 hiện tại đã có trong danh sách block được cấu hình nên Client 2 đã bị từ chối truy cập đến và download thành công.

4.3. Thủ nghiệm tính năng Authentication

- Các bước thực nghiệm tính năng Authentication:

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

```
Thu 23 21:28:23 squidproxy virtual-machine:~$ sudo apt install apache2-utils -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  libapreq1 libaprutil1
The following NEW packages will be installed:
  apache2-utils libapreq1 libaprutil1
0 upgraded, 3 newly installed, 0 to remove and 3 not upgraded.
Need to get 290 kB of archives.
After this operation, 992 kB of additional disk space will be used.
Get:1 http://vn.archive.ubuntu.com/ubuntu jammy-updates/main amd64 libapreq1 amd64 1.7.0-8ubuntu0.22.04.1 [108 kB]
Get:2 http://vn.archive.ubuntu.com/ubuntu jammy-updates/main amd64 libaprutil1 amd64 1.6.1-5ubuntu4.22.04.2 [92,8 kB]
Get:3 http://vn.archive.ubuntu.com/ubuntu jammy-updates/main amd64 apache2-utils amd64 2.4.52-1ubuntu4.7 [88,8 kB]
Fetched 290 kB in 6s (51,1 kB/s)
Selecting previously unselected package libapreq1:amd64.
(Reading database ... 201159 files and directories currently installed.)
Preparing to unpack .../libapreq1_1.7.0-8ubuntu0.22.04.1_amd64.deb ...
Unpacking libapreq1:amd64 (1.7.0-8ubuntu0.22.04.1) ...
Selecting previously unselected package libaprutil1:amd64.
Preparing to unpack .../libaprutil1_1.6.1-5ubuntu4.22.04.2_amd64.deb ...
Unpacking libaprutil1:amd64 (1.6.1-5ubuntu4.22.04.2) ...
Selecting previously unselected package apache2-utils.
Preparing to unpack .../apache2-utils_2.4.52-1ubuntu4.7_amd64.deb ...
Unpacking apache2-utils (2.4.52-1ubuntu4.7) ...
Setting up libapreq1:amd64 (1.7.0-8ubuntu0.22.04.1) ...
Setting up libaprutil1:amd64 (1.6.1-5ubuntu4.22.04.2) ...
Setting up apache2-utils (2.4.52-1ubuntu4.7) ...
Processing triggers for man-db (2.10.2-1) ...
Processing triggers for libc-bin (2.35-0ubuntu3.4) ...
```

Hình 33 Cài đặt apache2-utils

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

```
Processing triggers for libc-bin (2.35-0ubuntu3.4) ...
squidproxy@squidproxy-virtual-machine:~$ sudo touch /etc/squid/passwd
squidproxy@squidproxy-virtual-machine:~$ sudo chown squidproxy: /etc/squid/passwd
```

Hình 34 Tạo và cấp quyền thực thi cho file password

+ Bước 3: Tạo password cho Client2

```
squidproxy@squidproxy-virtual-machine:~$ sudo htpasswd /etc/squid/passwd client2
New password:
Re-type new password:
Adding password for user client2
```

Hình 35 Tạo password cho Client 2

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

```

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
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
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
refresh_pattern /(Packages|Sources)(|\.bz2|\.gz|\.xz)$ 0 0% 0 refresh-ims
refresh_pattern /\Release(|\.gpg)$ 0 0% 0 refresh-ims
refresh_pattern /\InRelease$ 0 0% 0 refresh-ims
refresh_pattern /(Translation-..*)(|\.bz2|\.gz|\.xz)$ 0 0% 0 refresh-ims
refresh_pattern .               0      20%    4320
squid:deoxy@squid-deoxy:virtual_machine: ~

```

Hình 36 Cấu hình Squid proxy để thực hiện chức năng xác thực

*Giải thích: Sử dụng những câu lệnh sau để thực hiện tính năng Authentication

```

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

```

+ Bước 5: Áp dụng các cấu hình ở bước 2 vào Squid Proxy

```

[squidproxy@squidproxy-virtual-machine:~$ sudo systemctl restart squid
squidproxy@squidproxy-virtual-machine:~$ sudo systemctl status squid
● squid.service - Squid Web Proxy Server
   Loaded: loaded (/lib/systemd/system/squid.service; enabled; vendor preset: enabled)
   Active: active (running) since Wed 2023-11-29 21:54:26 +07; 8s ago
     Docs: man:squid(8)
 Process: 40969 ExecStartPre=/usr/sbin/squid --foreground -z (code=exited, status=0/SUCCESS)
 Main PID: 40969 (squid)
   Tasks: 5 (limit: 4558)
    Memory: 16.4M
      CPU: 299ms
     CGroup: /system.slice/squid.service
             └─40969 /usr/sbin/squid --foreground -z
                 ├─40971 "(squid-1)" --kid squid-1 --foreground -z
                 ├─40972 "(logfile-daemon)" /var/log/squid/access.log
                 ├─40973 "(unlinkd)"
                 └─40974 "(pinger)"

Thg 11 29 21:54:26 squidproxy-virtual-machine squid[40971]:          0 Objects cancelled.
Thg 11 29 21:54:26 squidproxy-virtual-machine squid[40971]:          0 Duplicate URLs purged.
Thg 11 29 21:54:26 squidproxy-virtual-machine squid[40971]:          0 Swapfile clashes avoided.
Thg 11 29 21:54:26 squidproxy-virtual-machine squid[40971]: Took 0.01 seconds ( 84.40 objects/sec).
Thg 11 29 21:54:26 squidproxy-virtual-machine squid[40971]: Beginning Validation Procedure
Thg 11 29 21:54:26 squidproxy-virtual-machine squid[40971]: ERROR: listen(..., 256) system call failed: (98) Address already in use
                                         listening port: 3128
Thg 11 29 21:54:26 squidproxy-virtual-machine squid[40971]: Completed Validation Procedure
Thg 11 29 21:54:26 squidproxy-virtual-machine squid[40971]: Validated 1 Entries
Thg 11 29 21:54:26 squidproxy-virtual-machine squid[40971]: store_swap_size = 4.00 KB
Thg 11 29 21:54:27 squidproxy-virtual-machine squid[40971]: storeLateRelease: released 0 objects
squidproxy@squidproxy-virtual-machine:~$ 

```

Hình 37 Kiểm tra trạng thái của Squid proxy sau khi restart lần 6

+ Bước 6: Vào máy Client2 để kiểm tra hoạt động của Squid Proxy bằng cách 2 cách

- Cách 1: Sử dụng câu lệnh trên terminal với 2 trường hợp nhập sai password và nhập đúng password:

```
curl -x http://192.168.37.139:3128 --proxy-user client:password -I http://crypto.com
```

```
curl -x http://192.168.37.139:3128 --proxy-user client:123456789 -I http://crypto.com
```

- Cách 2: Sử dụng trình duyệt Firefox với 2 trường hợp nhập sai password và nhập đúng password

- Kết quả thử nghiệm:

+ Sử dụng câu lệnh trên terminal:

- Trường hợp 1: Nhập sai password

```

client2@client2-virtual-machine:~$ curl -x http://192.168.37.139:3128 --proxy-user client2:password -I http://duckduckgo.com
HTTP/1.1 407 Proxy Authentication Required
Server: squid/5.7
Mime-Version: 1.0
Date: Wed, 29 Nov 2023 14:54:49 GMT
Content-Type: text/html;charset=utf-8
Content-Length: 3672
X-Squid-Error: ERR_CACHE_ACCESS_DENIED 0
Vary: Accept-Language
Content-Language: en
Proxy-Authenticate: Basic realm="Squid Basic Authentication"
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

```

Hình 38 Phản hồi nhận được khi nhập sai password

➔ Client 2 bị từ chối truy cập trang web vì xác thực thất bại

- Trường hợp 2: Nhập đúng password

```
client2@client2-virtual-machine:~$ curl -x http://192.168.37.139:3128 --proxy-user client2:123456789 -I 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=(none)
Content-Security-Policy: default-src 'none'; connect-src https://duckduckgo.com https://*.duckduckgo.com https://duckduckgogg42xjoc72x3jasoawrfbgcmvflmafft6twagswczad.onion/ https://spreadprivacy.com; manifest-src https://duckduckgo.com https://*.duckduckgo.com https://duckduckgogg42xjoc72x3jasoawrfbgcmvflmafft6twagswczad.onion/ https://spreadprivacy.com; script-src blob: https://*.duckduckgo.com https://duckduckgogg42xjoc72x3jasoawrfbgcmvflmafft6twagswczad.onion/ https://spreadprivacy.com; unsafe-inline' 'unsafe-eval' ; font-src data: https://duckduckgo.com https://*.duckduckgo.com https://duckduckgogg42xjoc72x3jasoawrfbgcmvflmafft6twagswczad.onion/ https://spreadprivacy.com; img-src data: https://duckduckgo.com https://*.duckduckgo.com https://duckduckgogg42xjoc72x3jasoawrfbgcmvflmafft6twagswczad.onion/ https://spreadprivacy.com; object-src 'none' ; worker-src blob: child-src blob: https://duckduckgo.com https://*.duckduckgo.com https://duckduckgogg42xjoc72x3jasoawrfbgcmvflmafft6twagswczad.onion/ https://spreadprivacy.com; frame-src blob: https://duckduckgo.com https://*.duckduckgo.com https://duckduckgogg42xjoc72x3jasoawrfbgcmvflmafft6twagswczad.onion/ https://spreadprivacy.com; form-action https://duckduckgo.com https://*.duckduckgo.com https://duckduckgogg42xjoc72x3jasoawrfbgcmvflmafft6twagswczad.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
Referer-Policy: origin
Expect-CT: max-age=0
Expires: Thu, 28 Nov 2024 14:16:46 GMT
Cache-Control: max-age=31536000
Age: 2299
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
```

Hình 39 Phản hồi nhận được khi nhập đúng password (1)

➔ Client 2 được phép truy cập trang web vì xác thực thành công

+ Sử dụng trình duyệt Firefox:

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

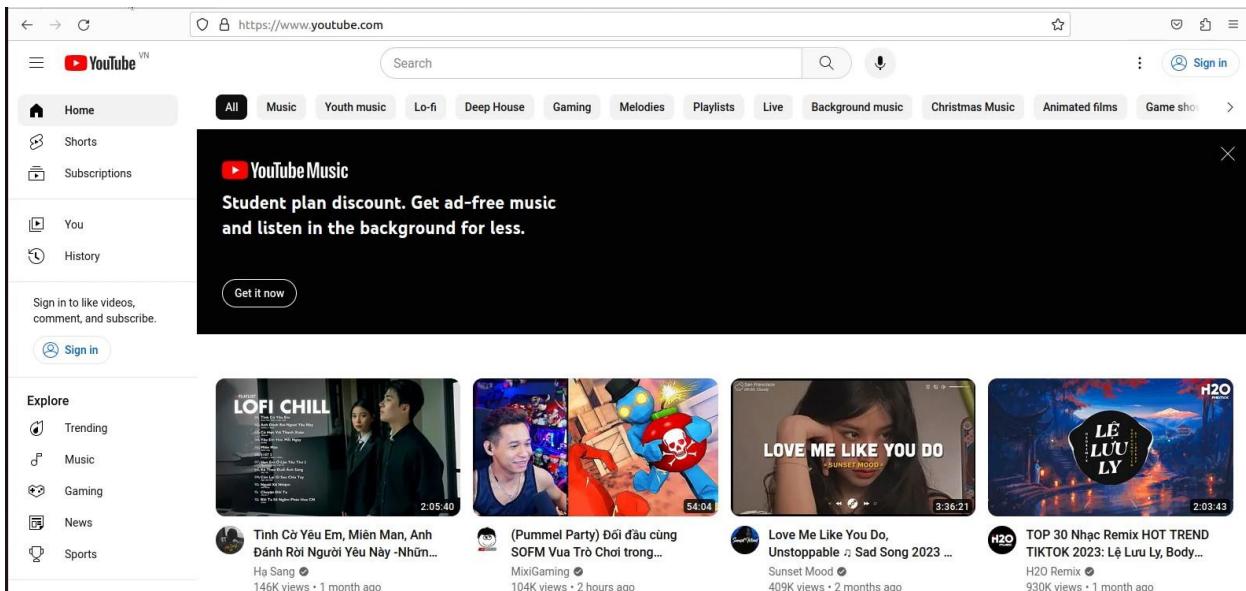


Hình 40 Thông báo nhập username và password trước khi truy cập trang web

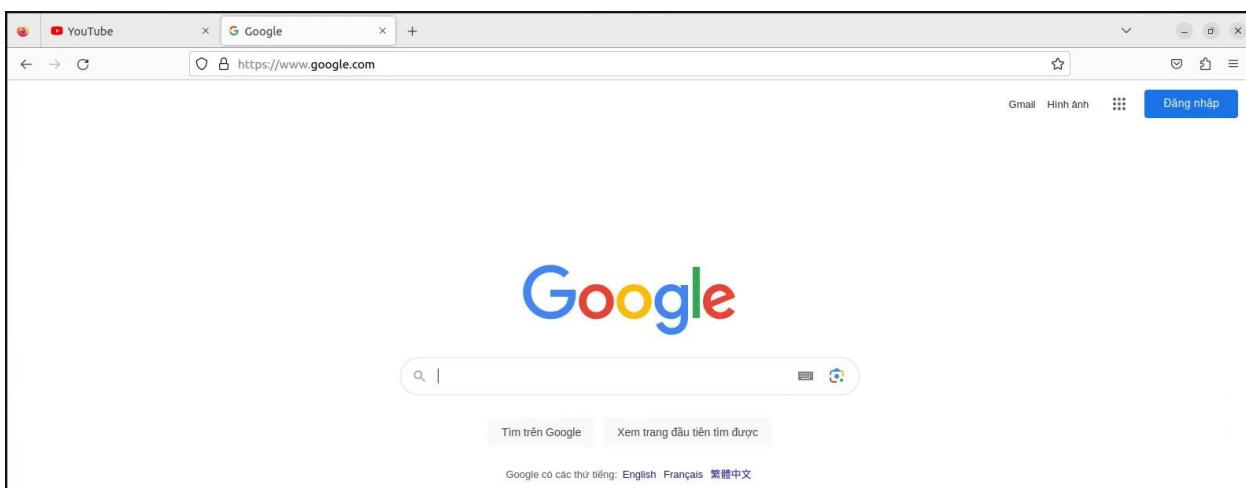
- Trường hợp 1: Nhập sai password

Client 2 phải nhập username và password liên tục cho đến khi xác thực đúng. Đồng thời Client 2 không thể thao tác gì trên trình duyệt đồng nghĩa với việc không thể truy cập vào internet nếu xác thực thất bại

- Trường hợp 2: Nhập đúng password



Hình 41 Phản hồi nhận được khi nhập đúng password (2)



Hình 42 Phản hồi nhận được khi nhập đúng password (3)

➔ Client 2 có thể truy cập vào internet một cách bình thường.

4.4. Thử nghiệm tính năng Access Control List

- Các bước thực nghiệm tính năng Access Control List:

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

```

squidproxy@squidproxy-virtual-machine: $ grep -vE '^$|^#' /etc/squid/squid.conf
acl localnet src 0.0.1-0.255.255.255 # RFC 1122 "this" network (LAN)
acl localnet src 10.0.0.0/8           # RFC 1918 local private network (LAN)
acl localnet src 100.64.0.0/10        # RFC 6598 shared address space (CGN)
acl localnet src 169.254.0.0/16        # RFC 3927 link-local (directly plugged) machines
acl localnet src 172.16.0.0/12        # RFC 1918 local private network (LAN)
acl localnet src 192.168.0.0/16        # RFC 1918 local private network (LAN)
acl localnet src fc00::/7             # RFC 4193 local private network range
acl localnet src fe80::/10             # RFC 4291 link-local (directly plugged) machines
acl SSL_ports port 443               # https
acl Safe_ports port 80                # http
acl Safe_ports port 21                # ftp
acl Safe_ports port 443               # https
acl Safe_ports port 70                # gopher
acl Safe_ports port 210               # wais
acl Safe_ports port 1025-65535       # unregistered ports
acl Safe_ports port 280               # http-mgmt
acl Safe_ports port 488               # gss-ftp
acl Safe_ports port 591               # filemaker
acl Safe_ports port 777               # multiling http
http_access deny !Safe_ports
http_access deny CONNECT !SSL_ports
http_access allow localhost manager
http_access deny manager
include /etc/squid/conf.d/*.conf
http_access allow localhost
acl client2 src 192.168.37.138
acl client1 src 192.168.37.128
http_access allow client2
http_access deny client1
http_access deny all
http_port 192.168.37.139:3128
http_port 3128
cache_dir ufs /var/spool/squid 100 16 256
coredump_dir /var/spool/squid
refresh_pattern ^ftp:          1440   20%   10080
refresh_pattern ^gopher:        1440   0%    1440
refresh_pattern -i (/cgi-bin/|/?) 0     0%    0
refresh_pattern /(Packages|Sources)(|\.bz2|\.gz|\.xz)$ 0 0% 0 refresh-ims
refresh_pattern /(Release|\.gpg)$ 0 0% 0 refresh-ims
refresh_pattern /InRelease$ 0 0% 0 refresh-ims
refresh_pattern /(Translation-.*)(|\.bz2|\.gz|\.xz)$ 0 0% 0 refresh-ims
refresh_pattern .              0     20%   4320

```

Hình 43 Cấu hình Squid proxy để thực hiện chức năng Access control list

*Giải thích: Sử dụng những câu lệnh sau để thực hiện tính năng Access Control List

acl client2 src 192.168.37.138

acl client1 src 192.168.37.128

http_access allow client2

http_access deny client1

+ Bước 2: Áp dụng các cấu hình ở bước 1 vào Squid Proxy

```

squidproxy@squidproxy-virtual-machine: $ sudo systemctl restart squid
squidproxy@squidproxy-virtual-machine: $ sudo systemctl status squid
● squid.service - Squid Web Proxy Server
   Loaded: loaded (/lib/systemd/system/squid.service; enabled; vendor preset: enabled)
     Active: active (running) since Thu 2023-11-30 21:41:02 +07; 7s ago
       Docs: man:squid(8)
   Process: 4070 ExecStartPre=/usr/sbin/squid --foreground -z (code=exited, status=0/SUCCESS)
 Main PID: 4074 (squid)
    Tasks: 5 (limit: 4556)
      Memory: 16.5M
        CPU: 357ms
       CGroup: /system.slice/squid.service
           └─ 4074 /usr/sbin/squid --foreground -sYC
             ├─ 4076 "(squid-1)" --kid squid-1 --foreground -sYC
             ├─ 4077 "(logfile-daemon)" /var/log/squid/access.log
             ├─ 4078 "(unlinkd)"
             └─ 4079 "(pinger)"

Thg 11 30 21:41:02 squidproxy-virtual-machine squid[4076]:          0 Objects cancelled.
Thg 11 30 21:41:02 squidproxy-virtual-machine squid[4076]:          0 Duplicate URLs purged.
Thg 11 30 21:41:02 squidproxy-virtual-machine squid[4076]:          0 Swapfile clashes avoided.
Thg 11 30 21:41:02 squidproxy-virtual-machine squid[4076]: Took 0.02 seconds (6520.21 objects/sec).
Thg 11 30 21:41:02 squidproxy-virtual-machine squid[4076]: Beginning Validation Procedure
Thg 11 30 21:41:02 squidproxy-virtual-machine squid[4076]: ERROR: listen(..., 256) system call failed: (98) Address already in use
                                                listening port: 3128
Thg 11 30 21:41:02 squidproxy-virtual-machine squid[4076]: Completed Validation Procedure
Thg 11 30 21:41:02 squidproxy-virtual-machine squid[4076]: Validated 130 Entries
Thg 11 30 21:41:02 squidproxy-virtual-machine squid[4076]: store_swap_size = 2124.00 KB
Thg 11 30 21:41:03 squidproxy-virtual-machine squid[4076]: storeLateRelease: released 0 objects
squidproxy@squidproxy-virtual-machine: $ 

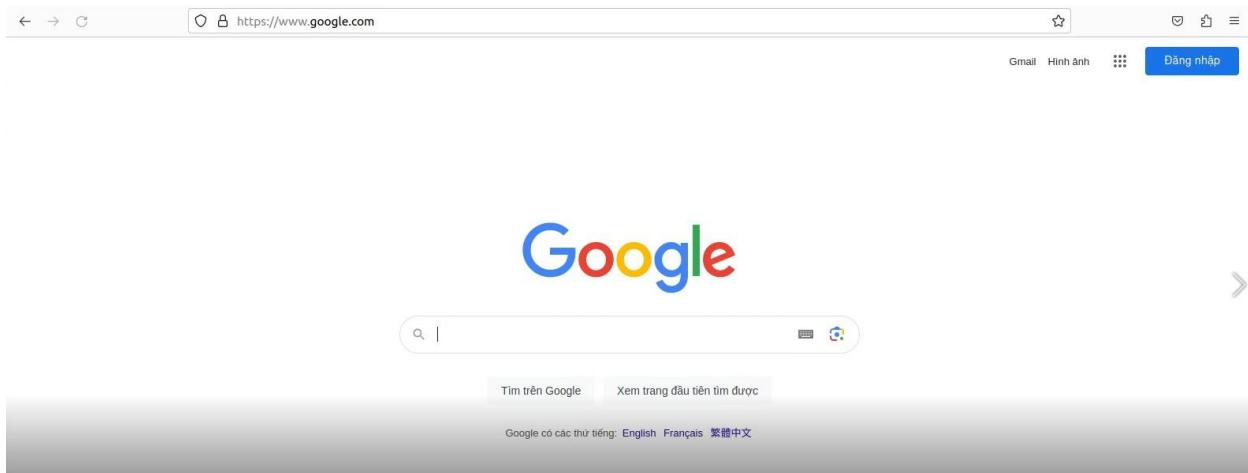
```

Hình 44 Kiểm tra trạng thái của Squid proxy sau khi restart lần 7

+ Bước 3: Lần lượt vào máy Client2 và Client 1 sử dụng trình duyệt để kiểm tra hoạt động của Squid Proxy. Đối với Client 1 chia làm 2 trường hợp sử dụng Proxy và không sử dụng Proxy để thấy rõ sự hoạt động của Squid Proxy

- Kết quả thực nghiệm:

+ Đối với Client 2:

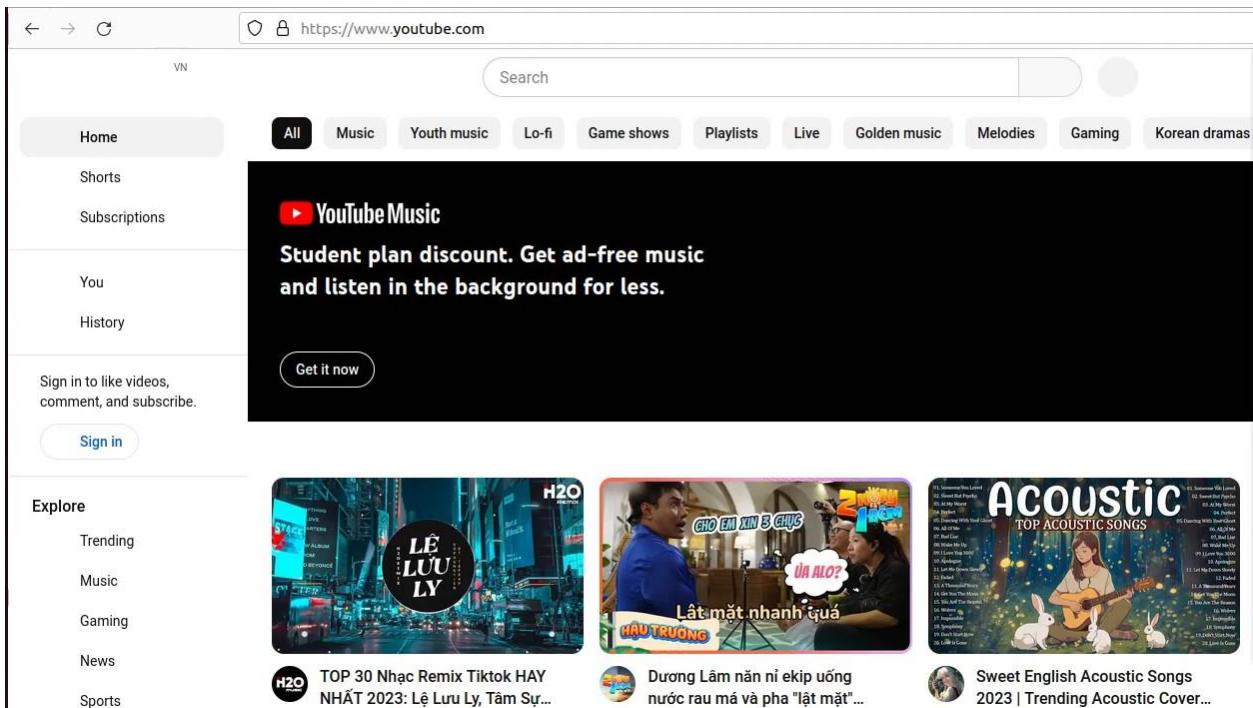


Hình 45 Phản hồi nhận được khi truy cập trang web trên Client 2

➔ Client 2 có thể truy cập vào internet một cách bình thường

+ Đối với Client 1:

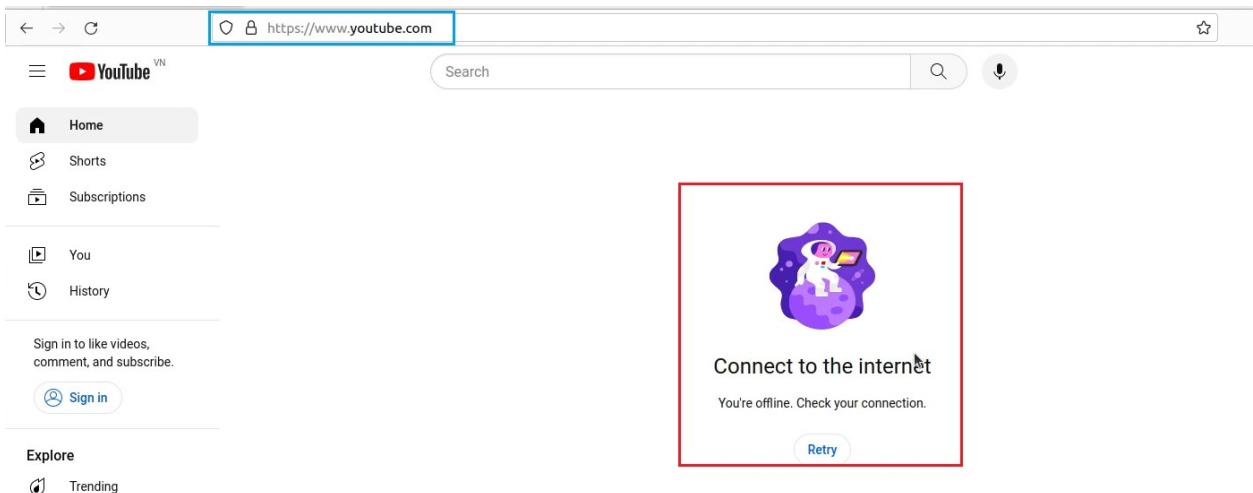
- Trường hợp 1: Không sử dụng Proxy



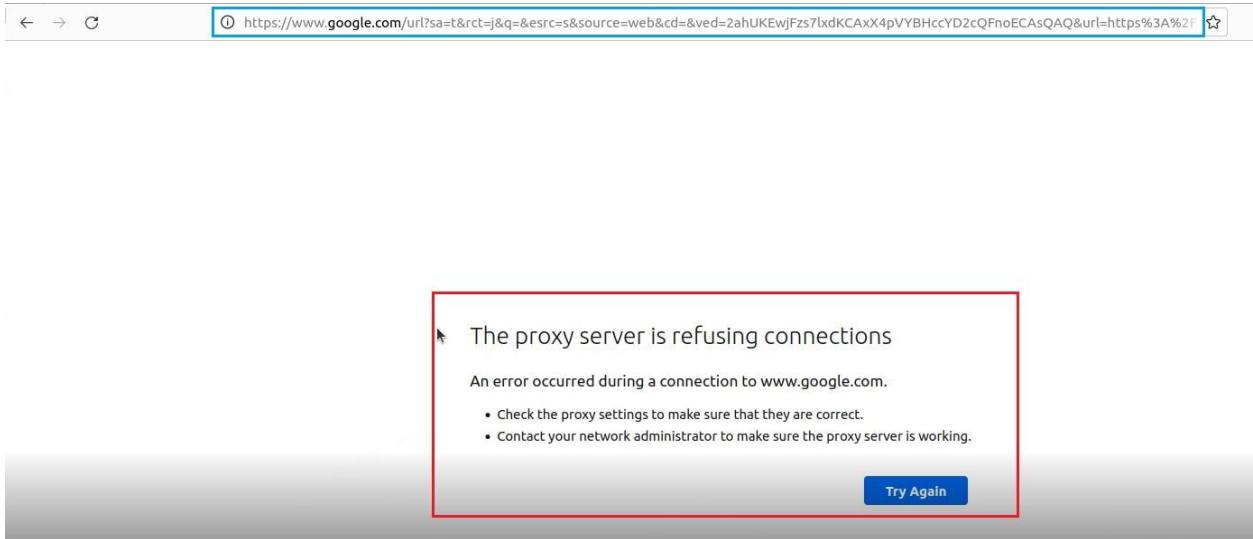
Hình 46 Phản hồi nhận được khi truy cập trang web không qua Squid proxy trên Client 1

➔ Client 1 truy cập internet 1 cách bình thường, không gặp trở ngại gì

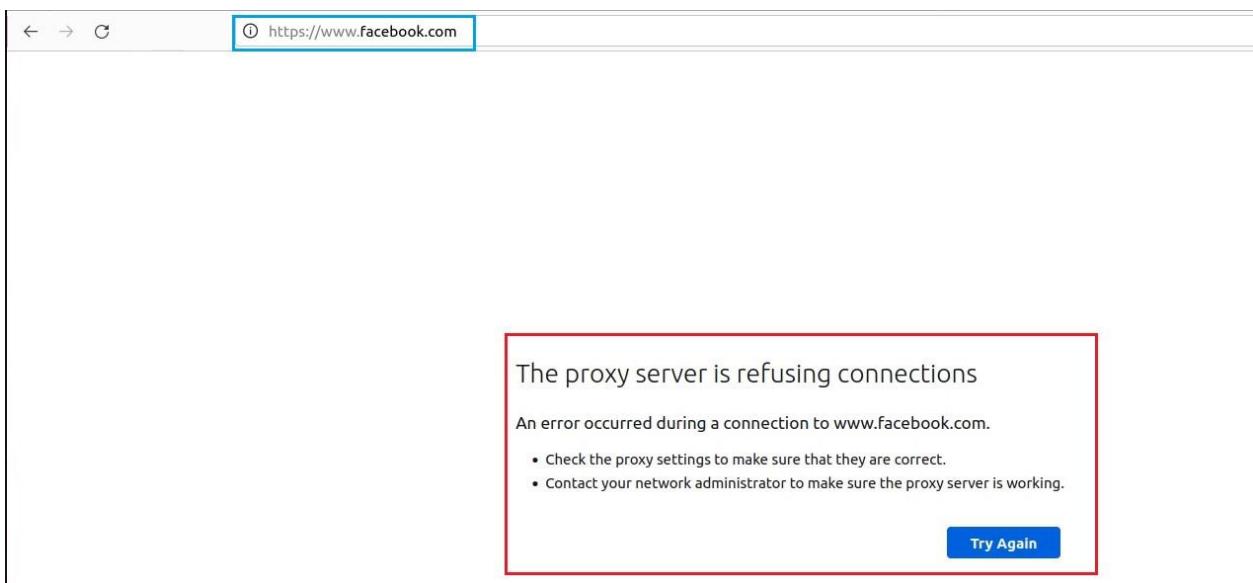
- Trường hợp 2: Sử dụng Proxy



Hình 47 Phản hồi nhận được khi truy cập trang web qua Squid proxy trên Client 1 (1)



Hình 48 Phản hồi nhận được khi truy cập trang web qua Squid proxy trên Client 1 (2)



Hình 49 Phản hồi nhận được khi truy cập trang web qua Squid proxy trên Client 1 (3)

➔Client 1 hiện tại không thể truy cập vào internet được nữa.

+ Xem lịch sử trên Squid Proxy:

1701355362.993	0	192.168.37.128	TCP_DENIED/403	1085	CONNECT www.youtube.com:443 - HIER_NONE/- text/html
1701355363.052	0	192.168.37.128	TCP_DENIED/403	1085	CONNECT www.youtube.com:443 - HIER_NONE/- text/html
1701355363.230	0	192.168.37.128	TCP_DENIED/403	1085	CONNECT www.youtube.com:443 - HIER_NONE/- text/html
1701355363.231	0	192.168.37.128	TCP_DENIED/403	1082	CONNECT www.google.com:443 - HIER_NONE/- text/html
1701355363.231	0	192.168.37.128	TCP_DENIED/403	1091	CONNECT www.google.com.vn:443 - HIER_NONE/- text/html
1701355363.399	0	192.168.37.128	TCP_DENIED/403	1085	CONNECT www.youtube.com:443 - HIER_NONE/- text/html
1701355364.798	1	192.168.37.128	TCP_DENIED/403	1093	CONNECT jnn-pa.googleapis.com:443 - HIER_NONE/- text/html
1701355364.856	0	192.168.37.128	TCP_DENIED/403	106	CONNECT static.doubleclick.net:443 - HIER_NONE/- text/html
1701355365.799	0	192.168.37.128	TCP_DENIED/403	1085	CONNECT www.youtube.com:443 - HIER_NONE/- text/html
1701355365.818	0	192.168.37.128	TCP_DENIED/403	1093	CONNECT jnn-pa.googleapis.com:443 - HIER_NONE/- text/html
1701355375.244	0	192.168.37.128	TCP_DENIED/403	1189	GET http://detectportal.firefox.comcanonical.html - HIER_NONE/- text/html
1701355375.245	0	192.168.37.128	TCP_DENIED/403	1189	GET http://detectportal.firefox.comcanonical.html - HIER_NONE/- text/html
1701355375.246	0	192.168.37.128	TCP_DENIED/403	1189	GET http://detectportal.firefox.comcanonical.html - HIER_NONE/- text/html
1701355375.246	0	192.168.37.128	TCP_DENIED/403	1189	GET http://detectportal.firefox.comcanonical.html - HIER_NONE/- text/html
1701355375.247	0	192.168.37.128	TCP_DENIED/403	1189	GET http://detectportal.firefox.comcanonical.html - HIER_NONE/- text/html
1701355375.249	0	192.168.37.128	TCP_DENIED/403	1189	GET http://detectportal.firefox.comcanonical.html - HIER_NONE/- text/html
1701355377.179	0	192.168.37.128	TCP_DENIED/403	1082	CONNECT www.google.com:443 - HIER_NONE/- text/html
1701355377.583	0	192.168.37.128	TCP_DENIED/403	1082	CONNECT www.google.com:443 - HIER_NONE/- text/html
1701355378.421	0	192.168.37.128	TCP_DENIED/403	1082	CONNECT www.google.com:443 - HIER_NONE/- text/html
1701355378.626	0	192.168.37.128	TCP_DENIED/403	1082	CONNECT www.google.com:443 - HIER_NONE/- text/html
1701355378.739	0	192.168.37.128	TCP_DENIED/403	1082	CONNECT www.google.com:443 - HIER_NONE/- text/html
1701355381.325	0	192.168.37.128	TCP_DENIED/403	1082	CONNECT www.google.com:443 - HIER_NONE/- text/html
1701355381.481	0	192.168.37.128	TCP_DENIED/403	1082	CONNECT www.google.com:443 - HIER_NONE/- text/html
1701355384.538	0	192.168.37.128	TCP_DENIED/403	1082	CONNECT www.google.com:443 - HIER_NONE/- text/html
1701355384.538	0	192.168.37.128	TCP_DENIED/403	1082	CONNECT www.google.com:443 - HIER_NONE/- text/html

Hình 50 Lịch sử hoạt động của Squid proxy (1)

➔ Đã từ chối tất cả các truy cập của Client 1 đến internet

4.5. Thủ nghiệm tổng hợp tất cả tính năng trong 1 Squid Proxy Server

- Các bước thực nghiệm tất cả tính năng:

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

```

acl localnet src 0.0.0.1-0.255.255.255 # RFC 1122 "this" network (LAN)
acl localnet src 10.0.0/8                 # 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
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
acl blocked_websites dstdomain .youtube.com .facebook.com .twitter.com .reddit.com
http_access deny blocked_websites
acl block_extensions urlpath_regex -i \.exe\$ \.zip\$ \.rar\$ \.tar\$ \.gz\$ \.iso\$ \.mp3\$ \.mp4\$
http_reply_access deny block_extensions
acl blacklist url_regex -i "/etc/squid/blacklist.txt"
http_access deny blacklist

http_access allow localhost
acl client2 src 192.168.37.138
acl client1 src 192.168.37.128
http_access deny client1
http_access allow auth_users
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
refresh_pattern ^ftp:          1440   20%   10080

```

Hình 51 Cấu hình Squid proxy để thực hiện tổng hợp chức năng

* Giải thích:

- Câu lệnh thể hiện tính năng caching:

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

Hình 52 Câu hình chức năng caching

- Câu lệnh thể hiện tính năng Block Domain:

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

Hình 53 Câu hình chức năng Block domain

- Câu lệnh thể hiện tính năng Block Words:

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

Hình 54 Câu hình chức năng Block words

- Câu lệnh thể hiện tính năng Block Download:

```
acl block_extensions urlpath_regex -i \.exe$ \.zip$ \.rar$ \.tar$ \.gz$ \.iso$ \.mp3$ \.mp4$  
http_reply_access deny block_extensions
```

Hình 55 Câu hình chức năng Block download

- Câu lệnh thể hiện tính năng xác thực (Authentication):

```
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
```

Hình 56 Câu hình chức năng xác thực (1)

```
http_access allow auth_users
```

Hình 57 Câu hình chức năng xác thực (2)

- Câu lệnh thể hiện tính năng Access Control List:

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

Hình 58 Câu hình chức năng Access control list (1)

```
http_access allow client2
```

Hình 59 Câu hình chức năng Access control list (2)

- Luồng thực hiện của cấu hình:
 - Đầu tiên Squid Proxy sẽ sử dụng Access Control List để cho phép 1 máy nào đó có thể truy cập vào internet.
 - Nếu máy đầu được phép truy cập vào internet thì Squid Proxy sẽ yêu cầu username và password để có thể chứng thực người dùng hợp lệ truy cập internet.
 - Sau khi đã chứng thực thành công, người dùng có thể truy cập vào internet. Nhưng nếu người dùng truy cập vào các domain bị block hay trang web có từ bị block hay tải xuống 1 file có extension bị block thì sẽ bị Squid Proxy từ chối ngay lập tức.

+ Bước 2: Áp dụng các cấu hình ở bước 1 vào Squid Proxy

```
squidproxy@squidproxy-virtual-machine: $ sudo systemctl status squid
● squid.service - Squid Web Proxy Server
   Loaded: loaded (/lib/systemd/system/squid.service; enabled; vendor preset: enabled)
   Active: active (running) since Thu 2023-11-30 22:51:44 +07; 53s ago
     Docs: man:squid(8)
   Process: 4486 ExecStartPre=/usr/sbin/squid --foreground -z (code=exited, status=0/SUCCESS)
 Main PID: 4490 (squid)
    Tasks: 5 (limit: 4556)
      Memory: 16.7M
        CPU: 652ms
       CGroup: /system.slice/squid.service
           └─4490 /usr/sbin/squid --foreground -sYC
              ├─4492 "(squid-1)" --kid squid-1 --foreground -sYC
              ├─4493 "(logfile-daemon)" /var/log/squid/access.log
              ├─4494 "(unlinkd)"
              └─4495 "(pinger)"

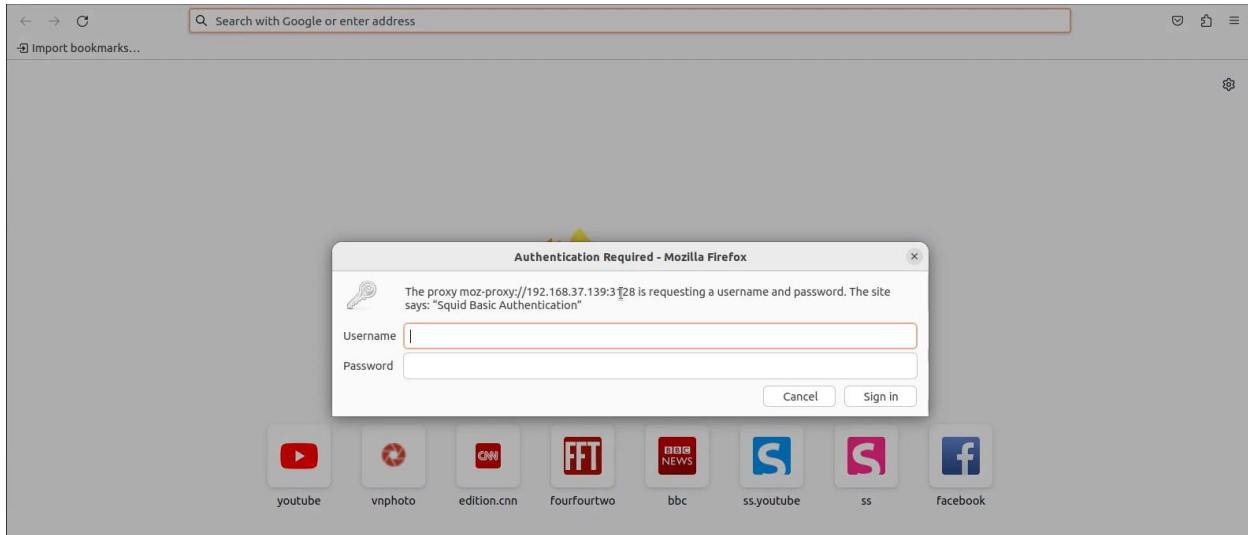
Thg 11 30 22:51:44 squidproxy-virtual-machine squid[4492]:          0 Objects cancelled.
Thg 11 30 22:51:44 squidproxy-virtual-machine squid[4492]:          0 Duplicate URLs purged.
Thg 11 30 22:51:44 squidproxy-virtual-machine squid[4492]:          0 Swapfile clashes avoided.
Thg 11 30 22:51:44 squidproxy-virtual-machine squid[4492]: Took 0.02 seconds (6227.25 objects/sec).
Thg 11 30 22:51:44 squidproxy-virtual-machine squid[4492]: Beginning Validation Procedure
Thg 11 30 22:51:44 squidproxy-virtual-machine squid[4492]: ERROR: listen(..., 256) system call failed: (98) Address already in use
                                                listening port: 3128
Thg 11 30 22:51:44 squidproxy-virtual-machine squid[4492]: Completed Validation Procedure
Thg 11 30 22:51:44 squidproxy-virtual-machine squid[4492]: Validated 130 Entries
Thg 11 30 22:51:44 squidproxy-virtual-machine squid[4492]: store_swap_size = 2124.00 KB
Thg 11 30 22:51:45 squidproxy-virtual-machine squid[4492]: storeLateRelease: released 0 objects
squidproxy@squidproxy-virtual-machine: $
```

Hình 60 Kiểm tra trạng thái Squid proxy sau khi restart lần 8

+ Bước 3: Lần lượt vào máy Client2 và Client 1 sử dụng trình duyệt để kiểm tra hoạt động của Squid Proxy với tất cả tính năng.

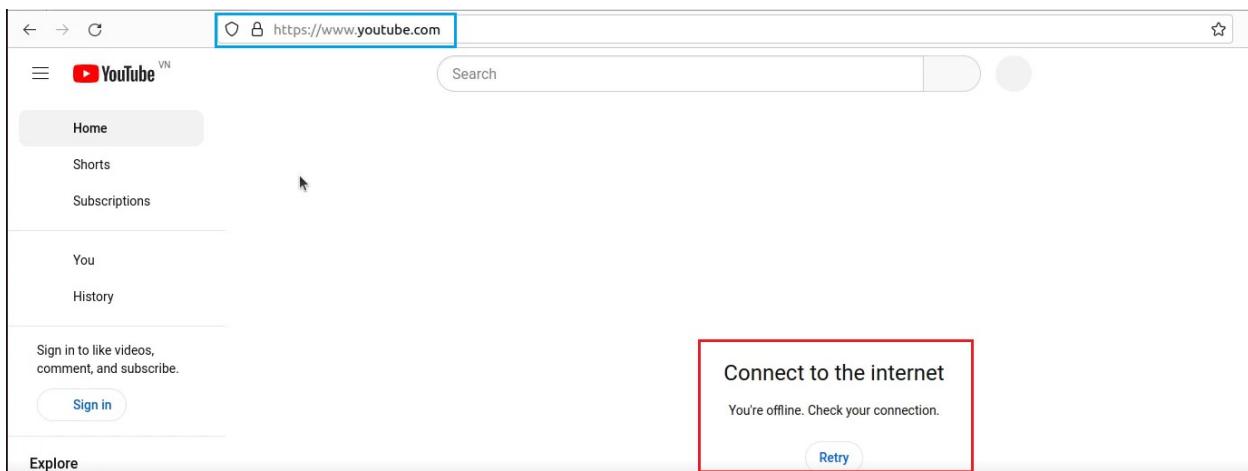
- Kết quả thực nghiệm:

+ Đổi với máy Client2:

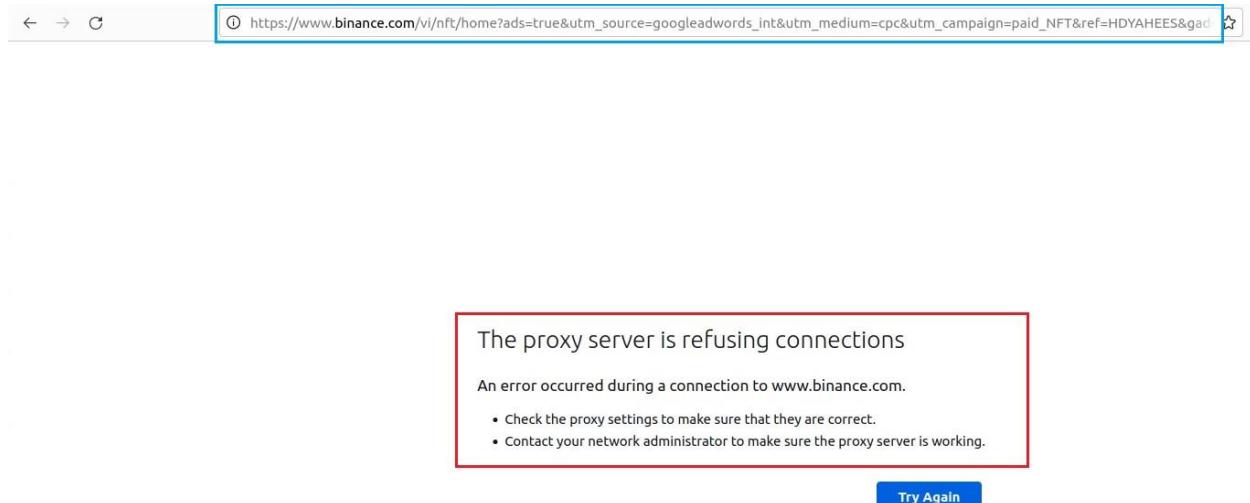


Hình 61 Phản hồi nhận được trên máy Client 2 (1)

➔ Squid Proxy yêu cầu nhập username và password để xác thực người dùng trước khi vào internet



Hình 62 Phản hồi nhận được trên máy Client 2 (2)



Hình 63 Phản hồi nhận được trên máy Client 2 (3)

The screenshot shows a web browser window with the URL <http://www.example.com/files/download.iso>. A red box highlights the error message area, which contains:

ERROR
The requested URL could not be retrieved

The following error was encountered while trying to retrieve the URL: <http://www.example.com/files/download.iso>

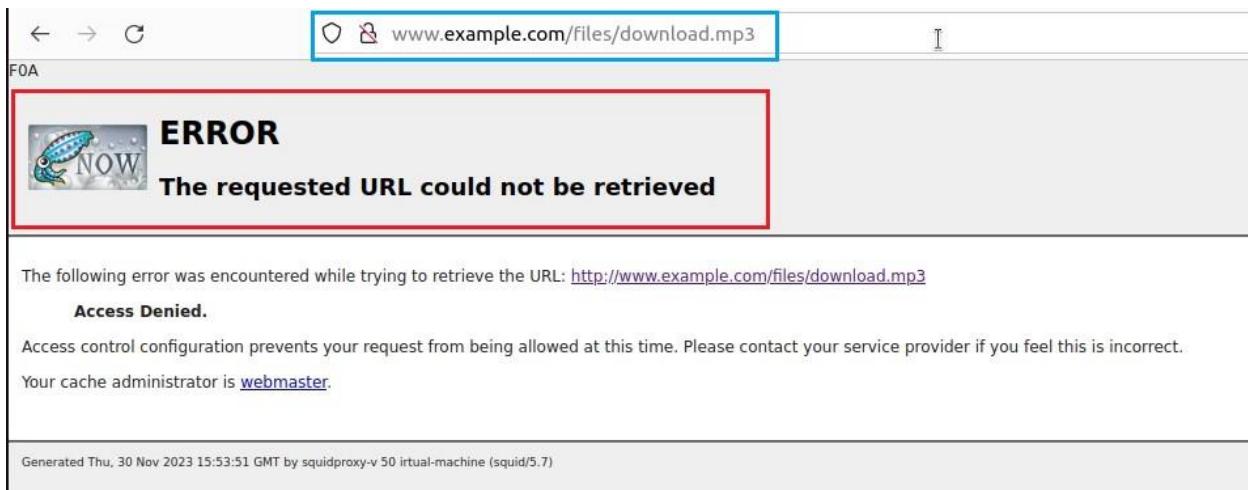
Access Denied.

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

Your cache administrator is [webmaster](#).

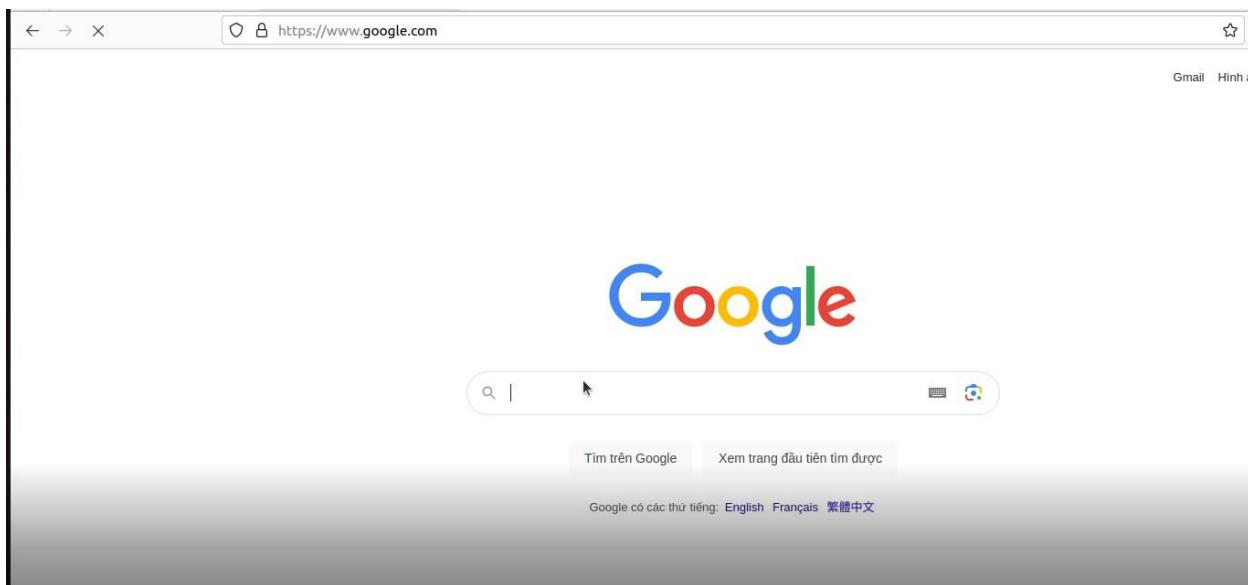
Generated Thu, 30 Nov 2023 15:53:37 GMT by squidproxy-v 50 virtual-machine (squid/5.7)

Hình 64 Phản hồi nhận được trên máy Client 2 (4)



Hình 65 Phản hồi nhận được trên máy Client 2 (5)

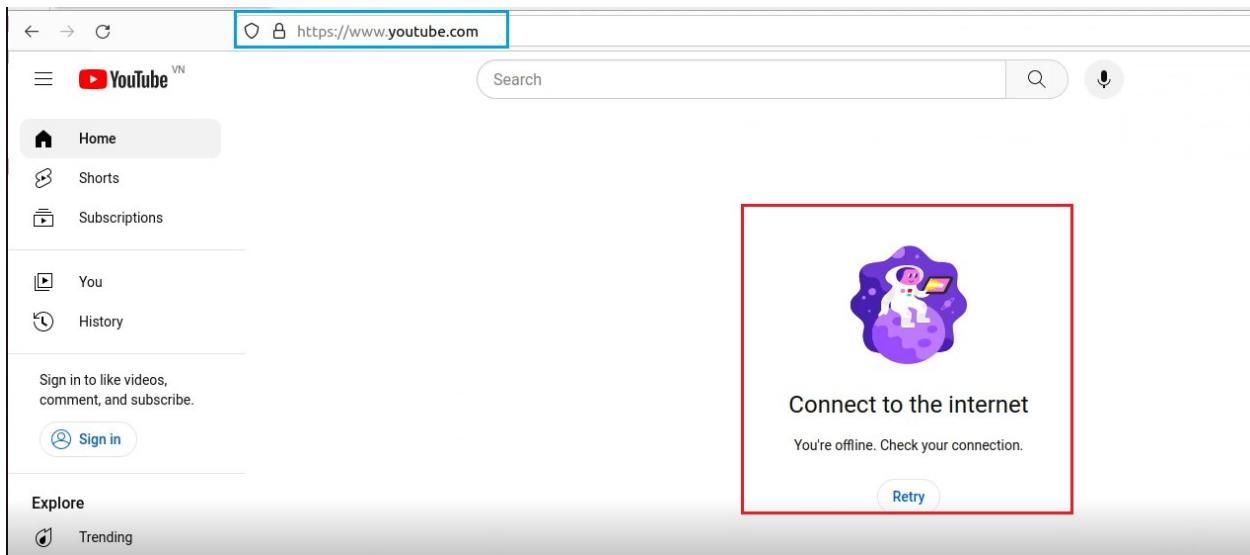
➔ Client 2 bị từ chối truy cập vào các Domain trong danh sách block cũng như URL của trang web có chứa từ nằm trong Black list và extension bị block.



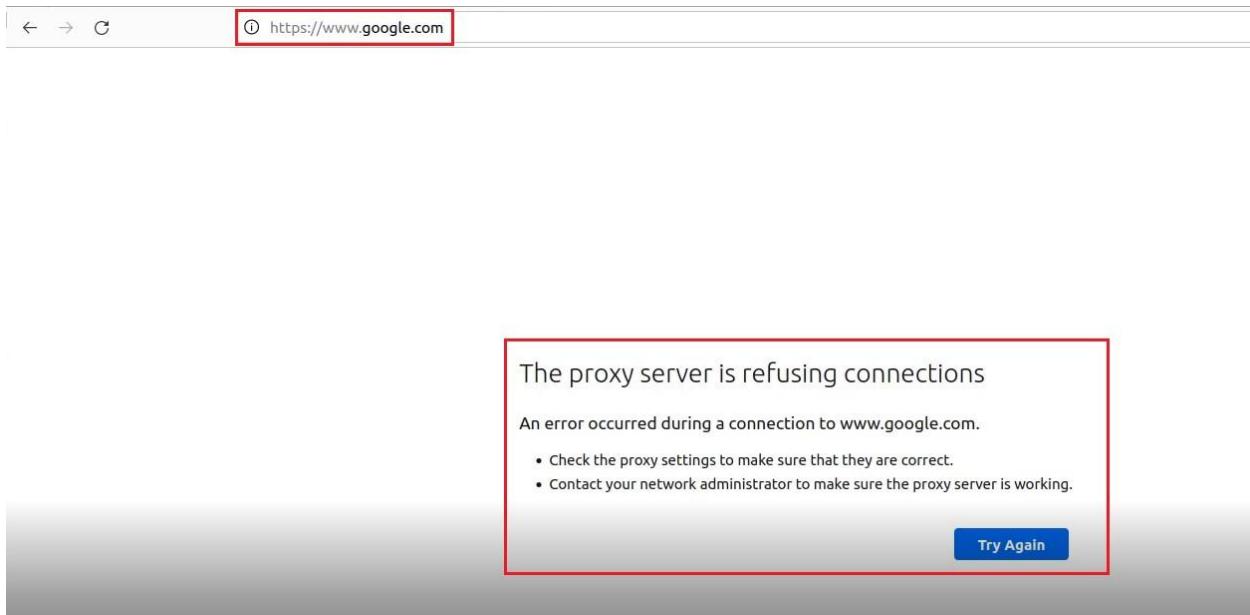
Hình 66 Phản hồi nhận được trên máy Client 2 (6)

➔ Client được chấp nhận truy cập vào các trường hợp còn lại không vi phạm đến các yêu cầu trong cấu hình của Squid Proxy

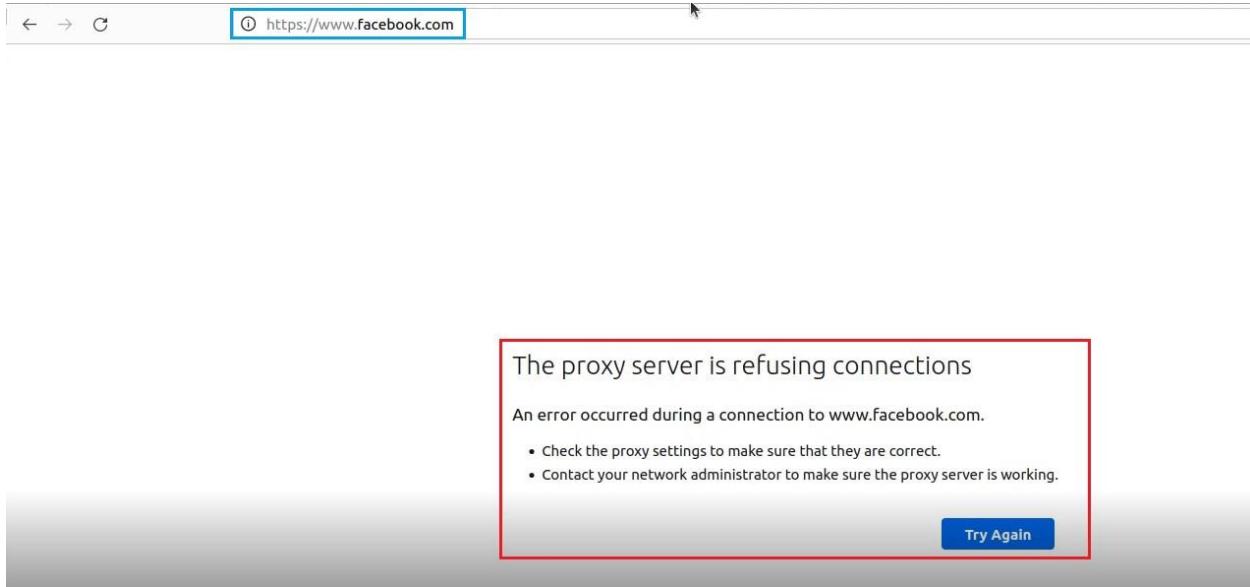
- Đối với máy Client 1:



Hình 67 Phản hồi nhận được trên máy Client 1 (1)



Hình 68 Phản hồi nhận được trên máy Client 1 (2)



Hình 69 Phản hồi nhận được trên máy Client 1 (3)

➔ Client 1 bị từ chối truy cập vào internet.

+ Xem lịch sử trên Squid Proxy:

1701359656.411	0	192.168.37.128	TCP_DENIED/403	4085	CONNECT	www.youtube.com:443	- HIER_NONE/- text/html
1701359656.533	0	192.168.37.128	TCP_DENIED/403	4085	CONNECT	www.youtube.com:443	- HIER_NONE/- text/html
1701359656.559	0	192.168.37.128	TCP_DENIED/403	4085	CONNECT	www.youtube.com:443	- HIER_NONE/- text/html
1701359656.562	0	192.168.37.128	TCP_DENIED/403	4085	CONNECT	www.youtube.com:443	- HIER_NONE/- text/html
1701359656.564	0	192.168.37.128	TCP_DENIED/403	4085	CONNECT	www.youtube.com:443	- HIER_NONE/- text/html
1701359656.590	0	192.168.37.128	TCP_DENIED/403	4139	CONNECT	rr1---sn-t0a7lnee.googlevideo.com:443	- HIER_NONE/- text/html
1701359656.593	0	192.168.37.128	TCP_DENIED/403	4139	CONNECT	rr1---sn-t0a7lnee.googlevideo.com:443	- HIER_NONE/- text/html
1701359656.680	0	192.168.37.128	TCP_DENIED/403	4139	CONNECT	rr1---sn-t0a7lnee.googlevideo.com:443	- HIER_NONE/- text/html
1701359656.696	0	192.168.37.128	TCP_DENIED/403	4139	CONNECT	rr1---sn-t0a7lnee.googlevideo.com:443	- HIER_NONE/- text/html
1701359656.818	0	192.168.37.128	TCP_DENIED/403	4085	CONNECT	www.youtube.com:443	- HIER_NONE/- text/html
1701359656.825	0	192.168.37.128	TCP_DENIED/403	4139	CONNECT	rr1---sn-t0a7lnee.googlevideo.com:443	- HIER_NONE/- text/html
1701359656.839	0	192.168.37.128	TCP_DENIED/403	4139	CONNECT	rr1---sn-t0a7lnee.googlevideo.com:443	- HIER_NONE/- text/html
1701359656.999	2	192.168.37.128	TCP_DENIED/403	4085	CONNECT	www.youtube.com:443	- HIER_NONE/- text/html
1701359657.090	0	192.168.37.128	TCP_DENIED/403	4085	CONNECT	www.youtube.com:443	- HIER_NONE/- text/html
1701359657.158	0	192.168.37.128	TCP_DENIED/403	4085	CONNECT	www.youtube.com:443	- HIER_NONE/- text/html
1701359657.262	0	192.168.37.128	TCP_DENIED/403	4085	CONNECT	www.youtube.com:443	- HIER_NONE/- text/html
1701359657.289	0	192.168.37.128	TCP_DENIED/403	4082	CONNECT	www.google.com:443	- HIER_NONE/- text/html
1701359657.291	0	192.168.37.128	TCP_DENIED/403	4091	CONNECT	www.google.com.vn:443	- HIER_NONE/- text/html

Hình 70 Lịch sử hoạt động của Squid proxy (2)

➔ Từ chối tất cả các yêu cầu truy cập vào internet của máy Client 1

1701359593.566	1591	192.168.37.138	TCP_TUNNEL	200	6047	CONNECT	rr1---sn-aigl6nsd.googlevideo.com:443	client2 HIER_DIRECT/74.125.105.38 -
1701359593.854	1876	192.168.37.138	TCP_TUNNEL	200	6047	CONNECT	rr1---sn-aigl6nsd.googlevideo.com:443	client2 HIER_DIRECT/74.125.105.38 -
1701359595.337	1452	192.168.37.138	TCP_TUNNEL	200	6047	CONNECT	rr1---sn-aigl6nsd.googlevideo.com:443	client2 HIER_DIRECT/74.125.105.38 -
1701359595.338	1492	192.168.37.138	TCP_TUNNEL	200	6047	CONNECT	rr1---sn-aigl6nsd.googlevideo.com:443	client2 HIER_DIRECT/74.125.105.38 -
1701359597.163	994	192.168.37.138	TCP_TUNNEL	200	6047	CONNECT	rr1---sn-aigl6nsd.googlevideo.com:443	client2 HIER_DIRECT/74.125.105.38 -
1701359597.647	1476	192.168.37.138	TCP_TUNNEL	200	6047	CONNECT	rr1---sn-aigl6nsd.googlevideo.com:443	client2 HIER_DIRECT/74.125.105.38 -
1701359598.594	88	192.168.37.138	TCP_TUNNEL	200	39	CONNECT	www.gstatic.com:443	client2 HIER_DIRECT/172.217.27.35 -

Hình 71 Lịch sử hoạt động của Squid proxy (3)

➔ Cho phép tất cả các yêu cầu truy cập vào internet của máy Client nếu nó không vi phạm vào các yêu cầu được đề ra trong cấu hình của Squid Proxy

4.6. Đánh giá sau thử nghiệm

Trong quá trình thực hiện đồ án môn học, nhóm đã tiến hành thử nghiệm và đánh giá các tính năng của Squid Proxy. Để đánh giá hiệu suất, nhóm đã thiết lập một môi trường thử nghiệm với hệ điều hành Ubuntu bao gồm 2 máy khách và máy chủ được kết nối với Squid Proxy.

Trước khi thực hiện thử nghiệm, nhóm đã thiết lập Squid Proxy với cấu hình cần thiết để thực nghiệm các chức năng cơ bản, cần thiết trong hệ thống mạnh. Sau đó, nhóm đã sử dụng các máy khách để kiểm tra xem việc hoạt động của Proxy theo cấu hình đã được định nghĩa trước đó.

Kết quả thử nghiệm cho thấy Squid Proxy hoạt động hiệu quả trong việc cung cấp dịch vụ proxy. Squid Proxy cũng giảm tải trọng cho máy chủ bằng cách nạp cache và tái sử dụng các tài nguyên đã được tải trước đó. Bên cạnh đó, Squid Proxy cũng cung cấp các tính năng bảo mật và kiểm soát truy cập linh hoạt. Nhóm cũng đã thử nghiệm các chính sách kiểm soát truy cập và xác thực trong Squid Proxy và kết quả cho thấy nó hoạt động đáng tin cậy và hiệu quả.

Tổng kết lại, đánh giá thử nghiệm đã xác nhận rằng Squid Proxy là một giải pháp mạnh mẽ và hiệu quả để triển khai dịch vụ proxy trong môi trường mạng. Hiệu suất cao, tính năng bảo mật và kiểm soát truy cập linh hoạt là những lợi ích chính mà Squid Proxy mang lại. Tuy nhiên, việc triển khai và quản lý Squid Proxy đòi hỏi sự hiểu biết và kỹ năng kỹ thuật phù hợp.

CHƯƠNG 5

KẾT LUẬN

Sau thời gian nghiên cứu và triển khai mô hình quản lý truy cập Internet cho hệ thống mạng LAN sử dụng Squid Proxy, chúng tôi đã tiếp cận được những kiến thức cơ bản về các hệ thống mạng, quy tắc hoạt động cơ bản của Squid Proxy, cách triển khai nó ứng dụng của Squid Proxy vào hệ thống mạng. Mô hình đưa ra này có thể ứng dụng được vào thực tế để giải quyết được bài toán đặt ra là làm giảm tải cho Server đồng thời giảm được lượng thông tin truyền trên Internet và tăng hiệu quả công việc của nhân viên trong các cơ quan, tổ chức. Tổng quan về kết quả nghiên cứu chúng tôi cũng đã triển khai và hiện thực thành công các kịch bản đã đề ra thể hiện được 04 tính năng nổi bật nhất của Squid Proxy bao gồm chức năng caching, content filtering, authentication, access control list. Tuy nhiên, trong quá trình thực hiện đề tài chúng tôi cũng gặp một số khó khăn nhất định chẳng hạn như không thể hiện thực cơ chế “*https caching*” do phiên bản hiện tại trên Squid Proxy không có quá nhiều tài liệu hỗ trợ để hiện thực hóa,... Tuy nhiên, nhìn chung nhóm nghiên cứu của chúng tôi cũng đã đạt được những mục tiêu mà trước đó đã đề ra và hoàn thành nó trước hạn.

5.1 Kết quả thu được

Chúng tôi đã thực hiện thành công được 07 kịch bản triển khai để thể hiện các tính năng của Squid proxy dựa trên mô hình đã được đề cập ở phần trước. 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. Qua đó, chứng minh được tính hiệu quả của Squid proxy.

5.2 Đánh giá ưu điểm và hạn chế khi sử dụng Squid Proxy

5.2.1 Ưu điểm

Với Squid Proxy là một mã nguồn mở, doanh nghiệp có thể tiết kiệm chi phí do không cần mua bản quyền phần mềm. Điều này đặc biệt quan trọng đối với các doanh nghiệp nhỏ và trung bình. Đồng thời Squid Proxy cũng cho phép doanh nghiệp tùy chỉnh Squid Proxy theo nhu cầu cụ thể của họ. Điều này mang lại sự linh hoạt và khả năng điều chỉnh theo môi trường kinh doanh cụ thể. Đồng thời Squid Proxy còn mang đến khá nhiều lợi ích trong đó phải kể đến:

Tốc độ duyệt web nhanh hơn: Squid Proxy lưu trữ các trang web được truy cập thường xuyên, do đó giảm thời gian tải trang web và mang lại tốc độ duyệt web nhanh hơn.

Giảm mức sử dụng băng thông: Máy chủ Squid Proxy lưu trữ các trang web và giảm nhu cầu tải chúng xuống mỗi khi có yêu cầu. Điều này dẫn đến việc giảm băng thông sử dụng, tiết kiệm chi phí cho người dùng.

Lọc nội dung: Squid Proxy có các tính năng tích hợp có thể chặn các trang web hoặc nội dung cụ thể dựa trên các danh mục như nội dung người lớn hoặc nền tảng truyền thông

xã hội. Điều này đặc biệt có lợi cho các tổ chức trong việc quản lý việc truy cập internet cho nhân viên.

Bảo mật được cải thiện: Squid Proxy có thể hoạt động như một tường lửa và bảo vệ người dùng khỏi phần mềm độc hại và vi-rút có thể xâm nhập thông qua các trang web độc hại. Nó cũng làm giảm bớt mặt tấn công của mạng bằng cách tạo vùng đệm giữa internet và mạng của người dùng.

Nhìn chung, Squid Proxy cung cấp giải pháp duyệt internet an toàn, nhanh chóng và tiết kiệm chi phí, khiến nó trở thành lựa chọn phổ biến cho cả doanh nghiệp và cá nhân. Với cộng đồng lớn và tính minh bạch của mã nguồn mở, Squid Proxy thường được cập nhật định kỳ với các bản vá bảo mật mới. Điều này giúp đảm bảo rằng doanh nghiệp sử dụng một hệ thống an toàn và bảo mật.

5.2.2 Hạn chế

Squid Proxy không phải không có nhược điểm và một nhược điểm tiềm ẩn là độ phức tạp của nó. Squid Proxy là một công cụ phức tạp đòi hỏi trình độ chuyên môn kỹ thuật nhất định để thiết lập và định cấu hình đúng cách. Những người thiếu các kỹ năng cần thiết có thể gặp khó khăn trong quá trình cài đặt và có thể cần phải nhờ đến sự hỗ trợ của chuyên gia.

Squid cũng có một số hạn chế liên quan đến việc lọc nội dung. Mặc dù Squid Proxy được thiết kế để chặn lưu lượng truy cập không mong muốn nhưng đôi khi nó có thể phân loại sai lưu lượng truy cập hợp pháp hoặc không chặn được lưu lượng truy cập không mong muốn một cách hiệu quả. Điều này có thể tạo ra các lỗ hổng bảo mật và dẫn đến vi phạm dữ liệu, điều quan trọng là phải giám sát và khắc phục sự cố hệ thống thường xuyên.

Khi xem xét việc sử dụng Squid Proxy, điều quan trọng là phải biết các yêu cầu về tài nguyên của nó. Squid Proxy có thể là một ứng dụng sử dụng nhiều tài nguyên và có thể yêu cầu tài nguyên bộ nhớ và CPU đáng kể để hoạt động tối ưu. Điều này có nghĩa là các tổ chức sử dụng Squid Proxy có thể cần đầu tư thêm phần cứng hoặc phân bổ nhiều tài nguyên hơn cho các máy chủ chạy Squid Proxy.

Squid Proxy cần có các IP cụ thể để được cấu hình, khiến người dùng thường xuyên thay đổi địa chỉ IP khó có thể sử dụng proxy một cách hiệu quả. Tính không thể đoán trước này có thể dẫn đến thay đổi cấu hình thường xuyên và gây ra sự gián đoạn trong quá trình lưu vào bộ nhớ đệm. Mặc dù các dịch vụ DNS động và kết nối VPN có thể giải quyết vấn đề này nhưng chúng yêu cầu bảo trì, thời gian thiết lập bổ sung và có thể làm tăng thêm độ phức tạp tổng thể.

Cuối cùng, vì nó hoạt động như một máy chủ proxy nên Squid Proxy có thể gây ra sự cố với một số ứng dụng không được thiết kế để hoạt động với nó.

5.3 Hướng phát triển

Trong quá trình thực hiện nghiên cứu, mặc dù nhóm đã triển khai 07 kịch bản để chứng tỏ tính khả thi của mô hình đưa ra, nhưng do thời gian có hạn nên công việc triển khai chưa thật sự chứng minh được toàn bộ những ưu điểm của mô hình này.

Mục tiêu tiếp theo của quá trình nghiên cứu sắp tới là 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. Đồng thời, trong quá trình nghiên cứu nhóm cũng nhận thấy rằng người dùng vẫn có thể dùng các phần mềm khác để vượt qua Proxy trong ngữ cảnh ngăn chặn truy cập. Điều này nhóm nghiên cứu cũng sẽ tiến hành tìm hiểu và triển khai để khắc phục vấn đề này.

Về mục tiêu dài hạn, nhóm có thể áp dụng Squid Proxy cho những mô hình mạng phức tạp hơn, thiết lập một cụm Proxy liên kết với nhau, mục đích của việc này là để 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. Như vậy mô hình mới ngoài khả năng giảm tải cho Server, nó còn có thêm khả năng chịu lỗi trong chính các Proxy, giảm thiểu đáng kể rủi ro khi một Proxy gặp sự cố

DANH MỤC TÀI LIỆU THAM KHẢO

About Squid proxy servers. Available at: <https://ubuntu.com/server/docs/proxy-servers-squid>

How To Setup and Configure a Proxy Server – Squid Proxy. Available at: <https://devopscube.com/setup-and-configure-proxy-server/>

How to Setup “Squid Proxy” Server on Ubuntu and Debian. Available at: <https://www.tecmint.com/install-squid-in-ubuntu/>

How to Setup Proxy Server with Squid. Available at: https://adamtheautomator.com/squid-proxy/?fbclid=IwAR1gnY742GDU4Y2AyoFM0V6Obqxbu_fioE29CKNji_DpcYBW8nrL4PGKjnE

Squid content filtering: Block / download of music MP3, mpg, mpeg, exec file by extensions. Available at: <https://www.cyberciti.biz/faq/squid-content-filter-block-files/>

Squid: Optimising Web Delivery. Available at: <http://www.squid-cache.org/>

Squid Proxy Advantages And Disadvantages. Available at: <https://proxygeek.su/squid-proxy-advantages-and-disadvantages/>

Squid Proxy Server 3.1 Beginner's Guide by Kulbir Saini [Book]

Squid: The Definitive Guide by Duane Wessels [Book]