**Phòng thí nghiệm An toàn Thông tin InsecLab**
**Trường Đại học Công nghệ Thông tin (UIT)**

# BÁO CÁO THỰC HÀNH

**Môn học: An toàn mạng**

**Tên chủ đề: Linux Firewall Exploration**

*GVHD: Tô Trọng Nghĩa*

**Nhóm: 14**

## 1. THÔNG TIN CHUNG:

Lớp: NT140.P11.ANTT.2

| STT | Họ và tên | MSSV | Email |
|---|---|---|---|
| **1** | Nguyễn Khánh Linh | 22520769 | 22520769@gm.uit.edu.vn |
| **2** | Phạm Thị Cẩm Tiên | 22521473 | 22521473@gm.uit.edu.vn |

## 2. NỘI DUNG THỰC HIỆN:[1]

| STT | Nội dung | Tình trạng | Trang |
|---|---|---|---|
| 1 | Thiết lập chính sách trên Firewall để bảo vệ mạng nội bộ | 100% | 2 - 11 |
| 2 | Vượt qua sự kiểm soát của Firewall | 100% | 12 - 18 |
| 3 | Triển khai Web Proxy (Application Firewall) | 100% | 18 - 25 |
| 4 | VPN | 100% | 26 - 33 |
| **Điểm tự đánh giá** | | | **10/10** |

**Phần bên dưới của báo cáo này là tài liệu báo cáo chi tiết của nhóm thực hiện.**

[1] Ghi nội dung công việc, các kịch bản trong bài Thực hành

# BÁO CÁO CHI TIẾT

1. **Cài đặt pfSense firewall**
2. **Thiết lập chính sách trên Firewall để bảo vệ mạng nội bộ**
   - Thực hiện ping giữa các bên để kiểm tra ban đầu trước khi set rule

```
server@server:~/Desktop$ ping 10.0.3.2 -c 4
PING 10.0.3.2 (10.0.3.2) 56(84) bytes of data.
64 bytes from 10.0.3.2: icmp_seq=1 ttl=64 time=0.916 ms
64 bytes from 10.0.3.2: icmp_seq=2 ttl=64 time=1.04 ms
64 bytes from 10.0.3.2: icmp_seq=3 ttl=64 time=0.981 ms
64 bytes from 10.0.3.2: icmp_seq=4 ttl=64 time=1.10 ms

--- 10.0.3.2 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 0.916/1.008/1.099/0.067 ms
server@server:~/Desktop$ ping 8.8.8.8 -c 4
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=128 time=167 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=128 time=74.6 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=128 time=32.9 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=128 time=39.9 ms
```

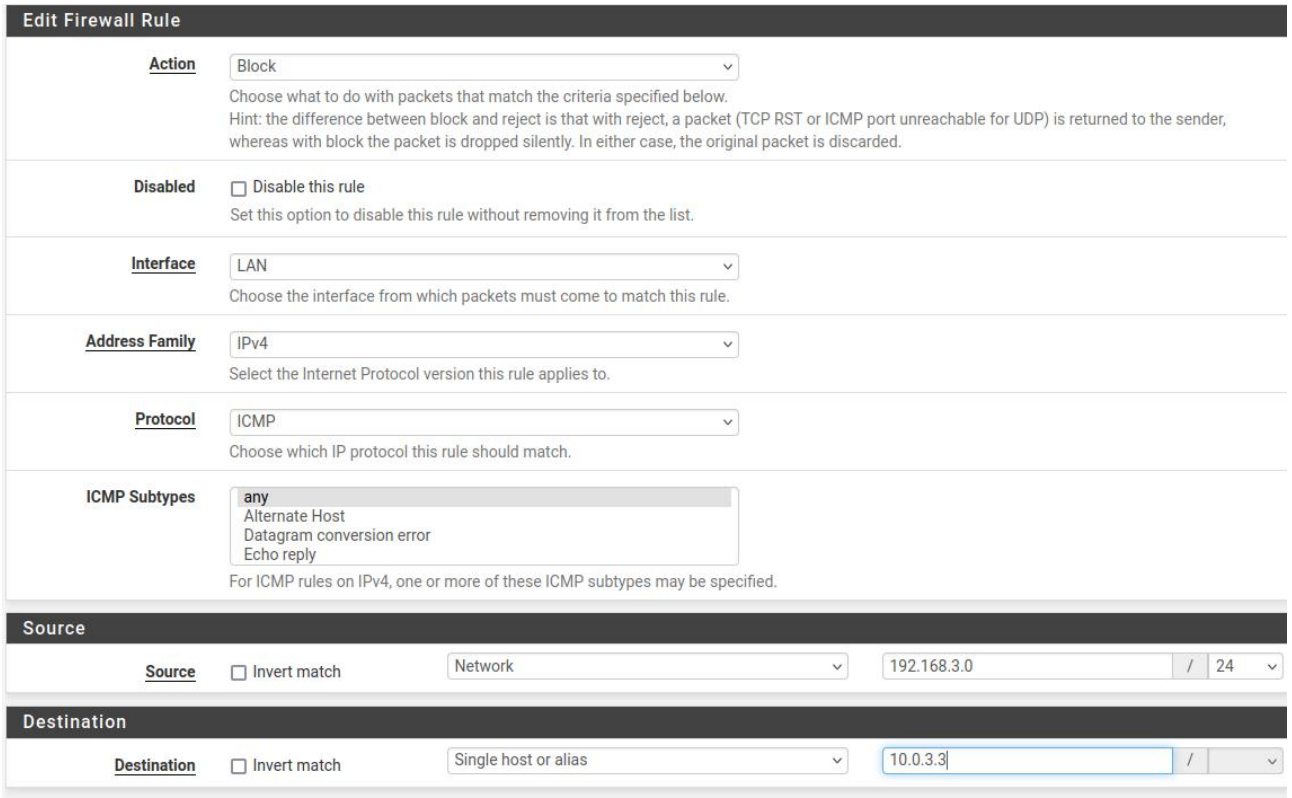
```
lovelily@Lovelily:~$ ping 10.0.3.3 -c 4
PING 10.0.3.3 (10.0.3.3) 56(84) bytes of data.
64 bytes from 10.0.3.3: icmp_seq=1 ttl=63 time=1.66 ms
64 bytes from 10.0.3.3: icmp_seq=2 ttl=63 time=1.87 ms
64 bytes from 10.0.3.3: icmp_seq=3 ttl=63 time=2.06 ms
64 bytes from 10.0.3.3: icmp_seq=4 ttl=63 time=1.84 ms

--- 10.0.3.3 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 1.662/1.858/2.064/0.142 ms
```

*Sinh viên tìm hiểu và thực hiện các rules sau (theo thứ tự):*

1. *Không cho phép các máy trong mạng nội bộ (192.168.3.0/24) thực hiện ping đến máy VM B*
2. *Không cho phép các máy trong mạng nội bộ truy cập các website sử dụng giao thức http (cổng 80).*
3. *Chặn kết nối telnet từ mạng nội bộ ra bên ngoài.*
4. *Không cho phép các máy trong mạng nội bộ truy cập đến www.facebook.com và youtube.com.*

*Sau khi triển khai các rules trên, sử dụng máy VM A để kiểm tra.*

- Cài đặt rule thứ nhất:



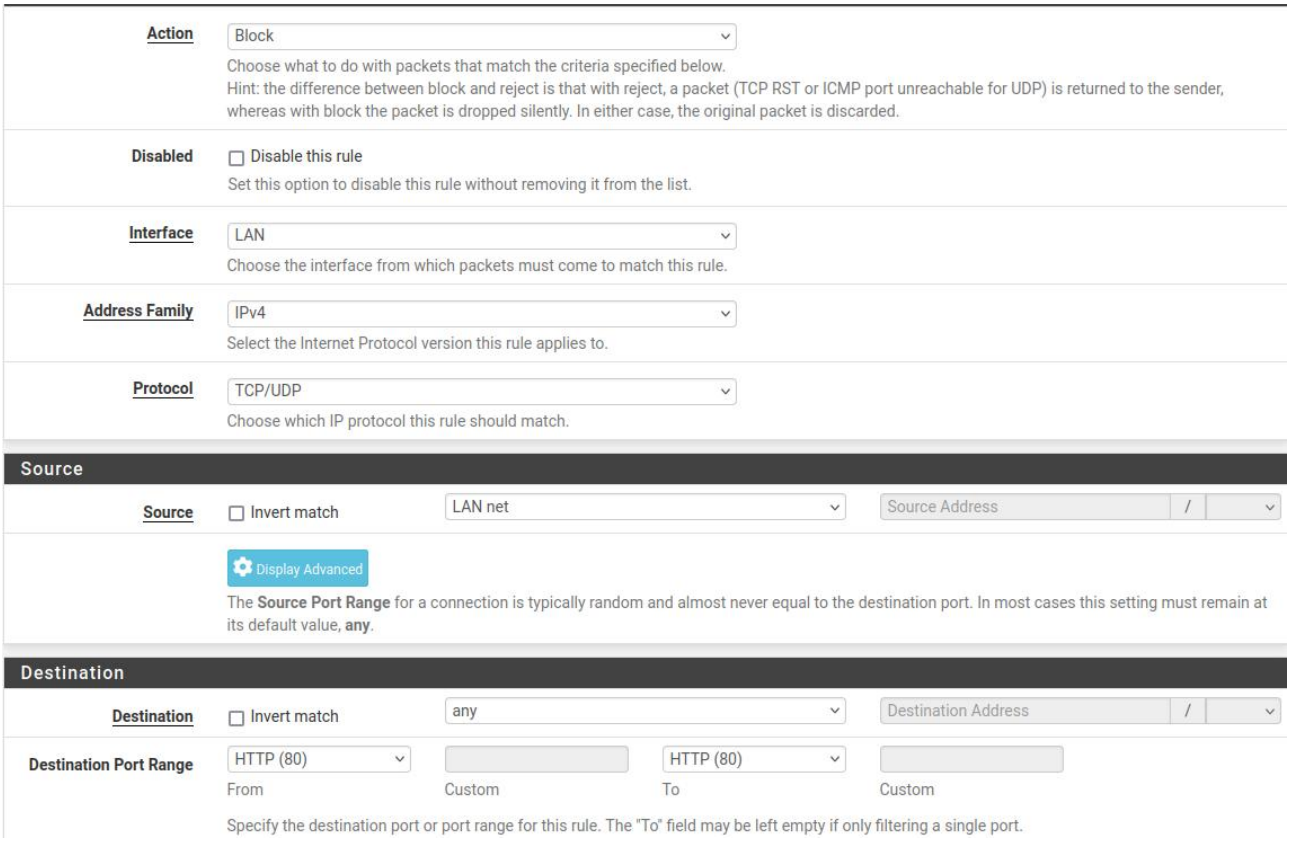

- Thực hiện ping thành công sang máy B trước khi set rule

```
lovelily@Lovelily:~$ ping 10.0.3.3
PING 10.0.3.3 (10.0.3.3) 56(84) bytes of data.
64 bytes from 10.0.3.3: icmp_seq=1 ttl=63 time=1.67 ms
64 bytes from 10.0.3.3: icmp_seq=2 ttl=63 time=1.67 ms
64 bytes from 10.0.3.3: icmp_seq=3 ttl=63 time=1.16 ms
64 bytes from 10.0.3.3: icmp_seq=4 ttl=63 time=1.15 ms
^C
--- 10.0.3.3 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 1.153/1.413/1.670/0.256 ms
```

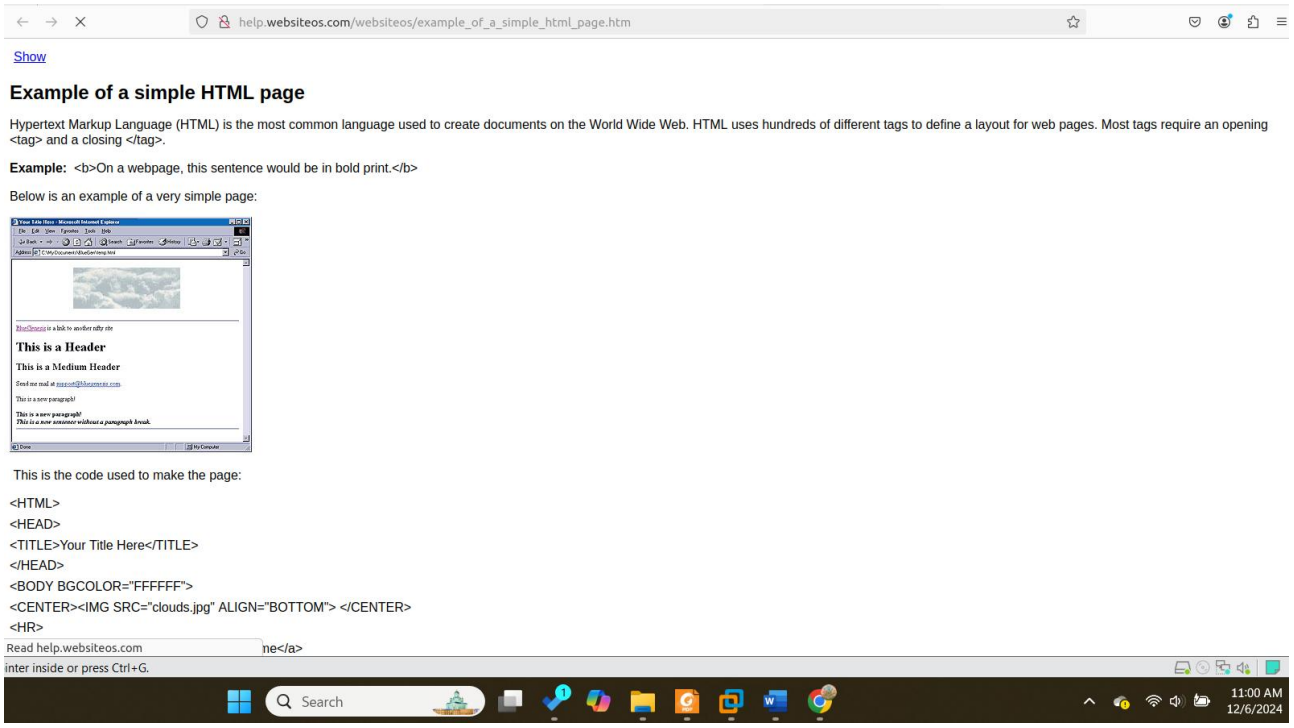
- Sau khi áp dụng rule thì việc ping sang máy B thất bại

```
lovelily@Lovelily:~$ ping 10.0.3.3
PING 10.0.3.3 (10.0.3.3) 56(84) bytes of data.
^C
--- 10.0.3.3 ping statistics ---
4 packets transmitted, 0 received, 100% packet loss, time 3057ms
```

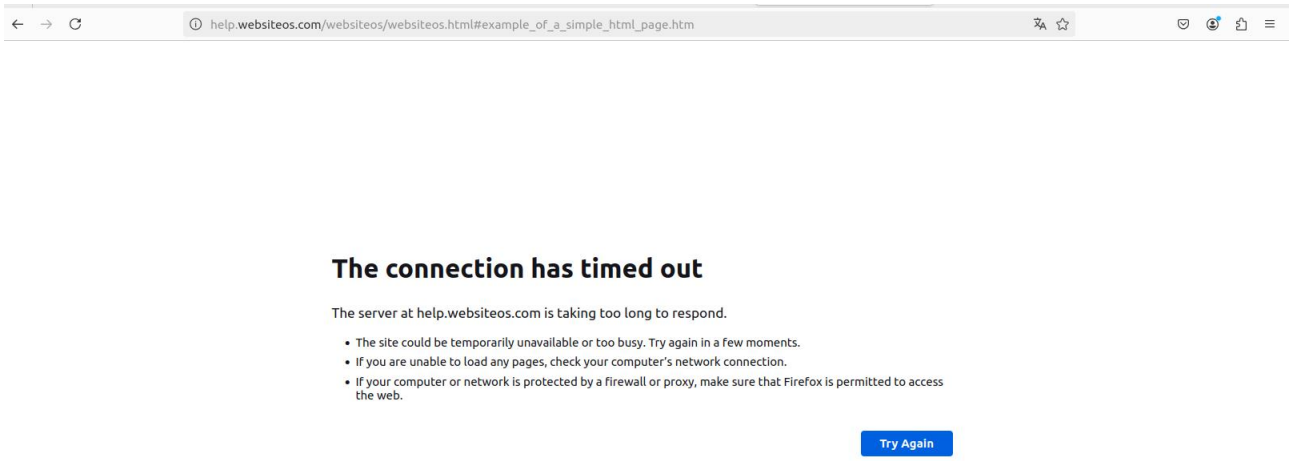
- Cài đặt rule thứ hai:



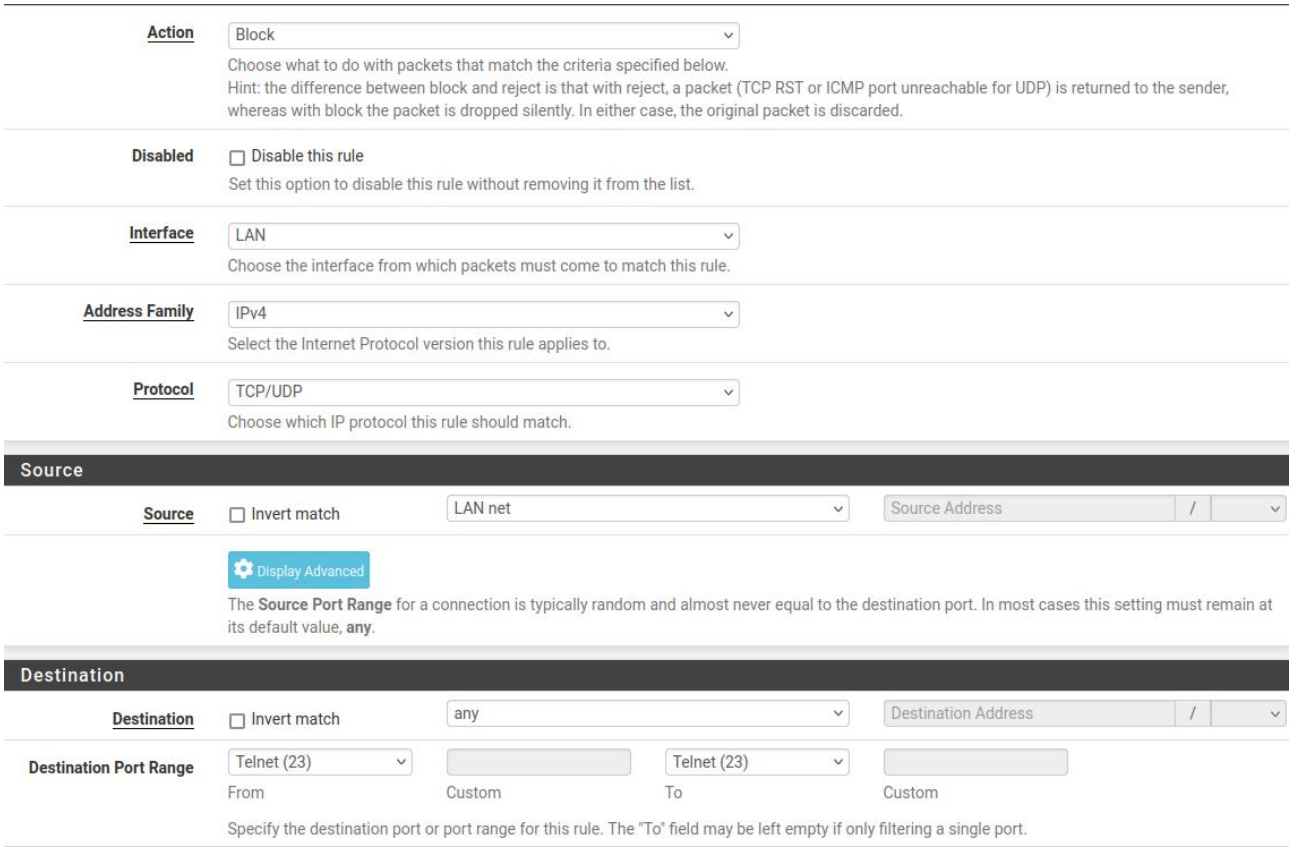

- Truy cập vào một trang web http thành công trước khi rule được áp dụng.
-



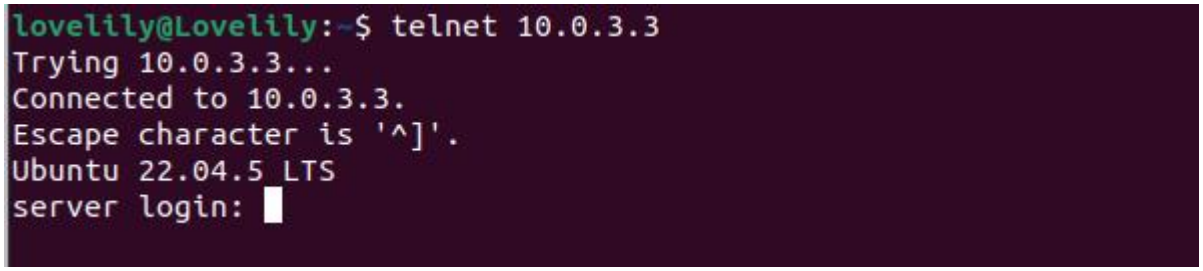

- Sau khi rule được áp dụng thì ta không thể truy cập vào trang web ban đầu được nữa




- Cài đặt rule thứ ba:




- Thực hiện telnet trước khi set rule




- Sau khi set rule thành công, ta không thể telnet đến máy B được nữa

```
lovelily@Lovelily:~$ telnet 10.0.3.3
Trying 10.0.3.3...
```

- Cài đặt rule thứ tư:
  - Đầu tiên, thực hiện ping tới facebook.com và youtube.com để lấy địa chỉ IP:

```
lovelily@Lovelily:~$ ping facebook.com
PING facebook.com (157.240.235.35) 56(84) bytes of data.
^C64 bytes from 157.240.235.35: icmp_seq=1 ttl=127 time=32.0 ms

--- facebook.com ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 31.976/31.976/31.976/0.000 ms
lovelily@Lovelily:~$ ping youtube.com
PING youtube.com (142.251.12.136) 56(84) bytes of data.
^C64 bytes from 142.251.12.136: icmp_seq=1 ttl=127 time=55.0 ms

--- youtube.com ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 54.987/54.987/54.987/0.000 ms
lovelily@Lovelily:~$
```

  - Sau đó, tạo danh sách alias bằng địa chỉ IP tìm được:

**Properties**

**Name**

Facebook

The name of the alias may only consist of the characters "a-z, A-Z, 0-9 and _".

**Description**

IP of Facebook

A description may be entered here for administrative reference (not parsed).

**Type**

Network(s)

**Network(s)**

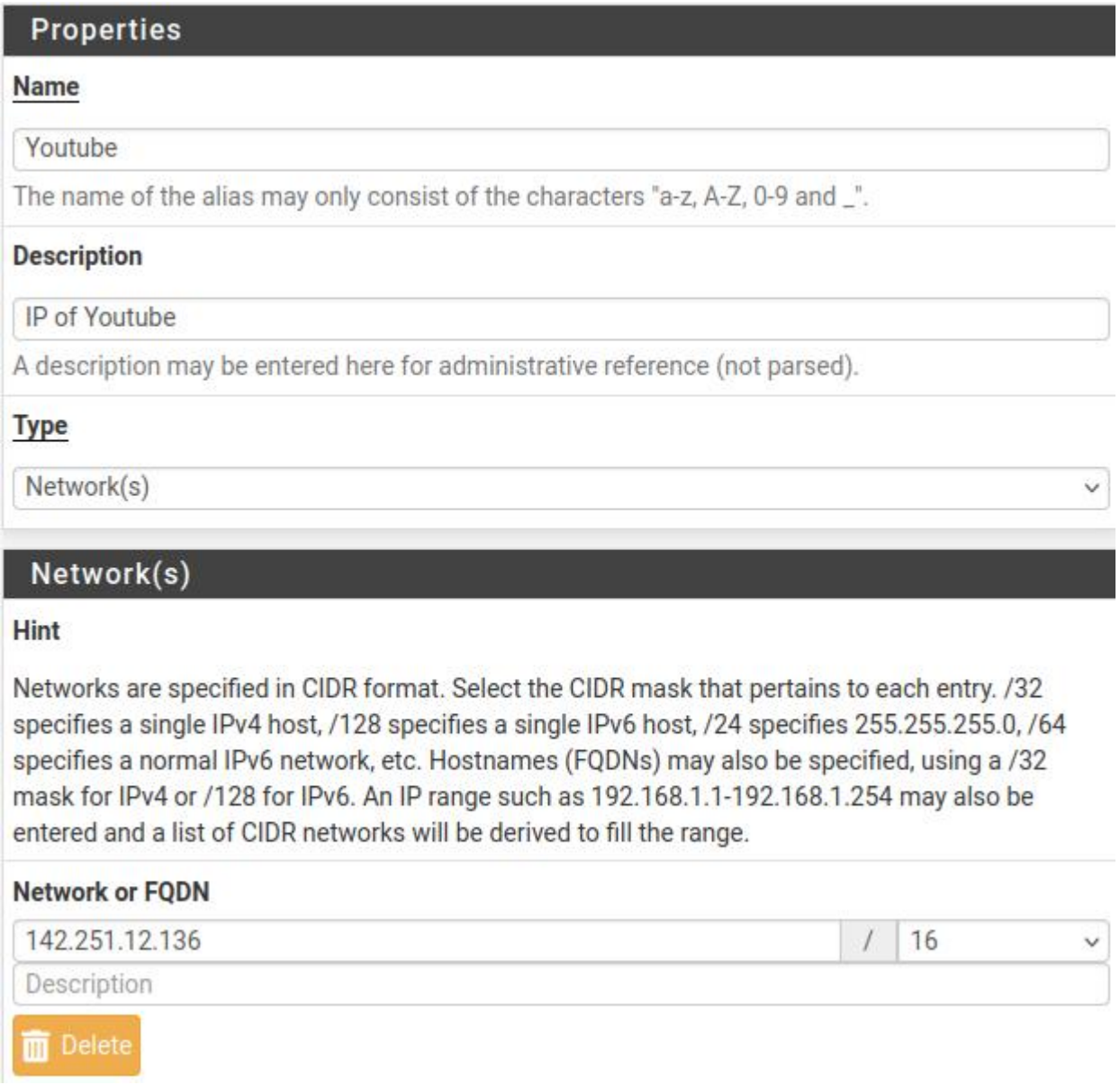
**Hint**

Networks are specified in CIDR format. Select the CIDR mask that pertains to each entry. /32 specifies a single IPv4 host, /128 specifies a single IPv6 host, /24 specifies 255.255.255.0, /64 specifies a normal IPv6 network, etc. Hostnames (FQDNs) may also be specified, using a /32 mask for IPv4 or /128 for IPv6. An IP range such as 192.168.1.1-192.168.1.254 may also be entered and a list of CIDR networks will be derived to fill the range.

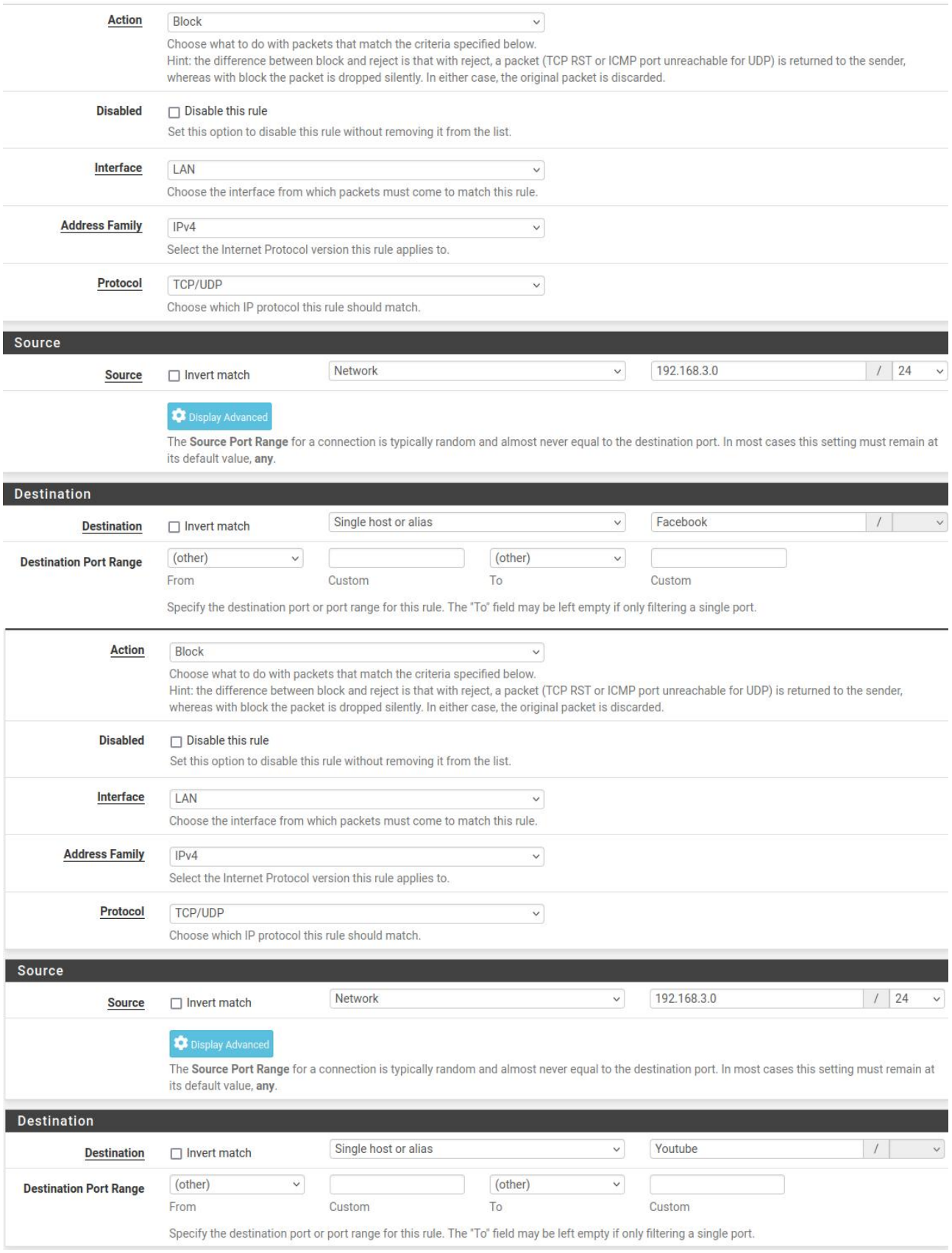
**Network or FQDN**

157.240.235.35 / 16

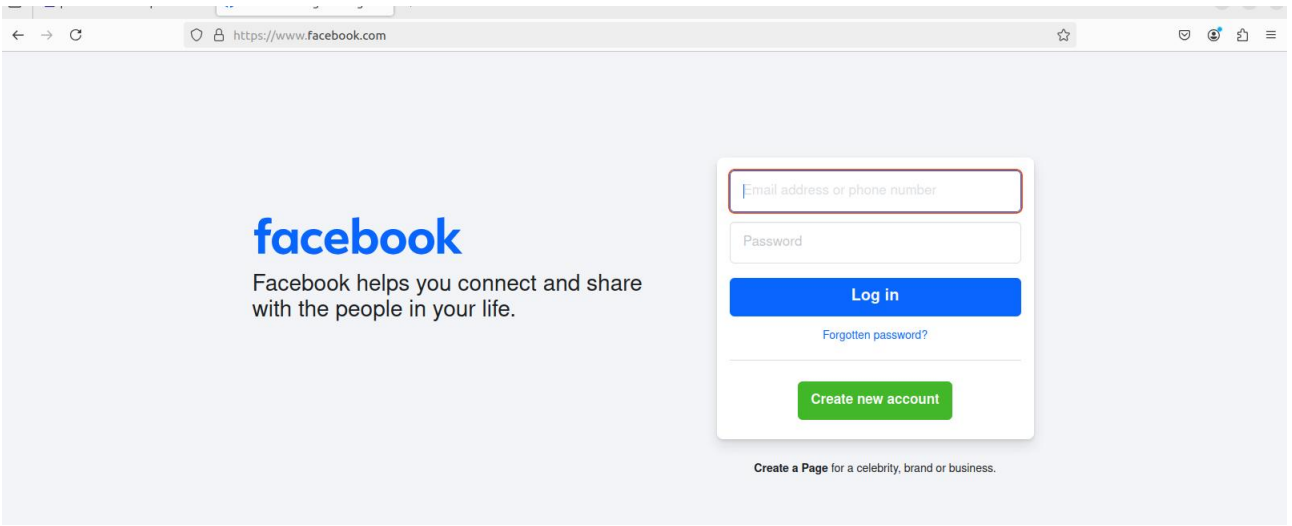
Entry added Fri, 06 Dec 2024 10:23:35 +0700



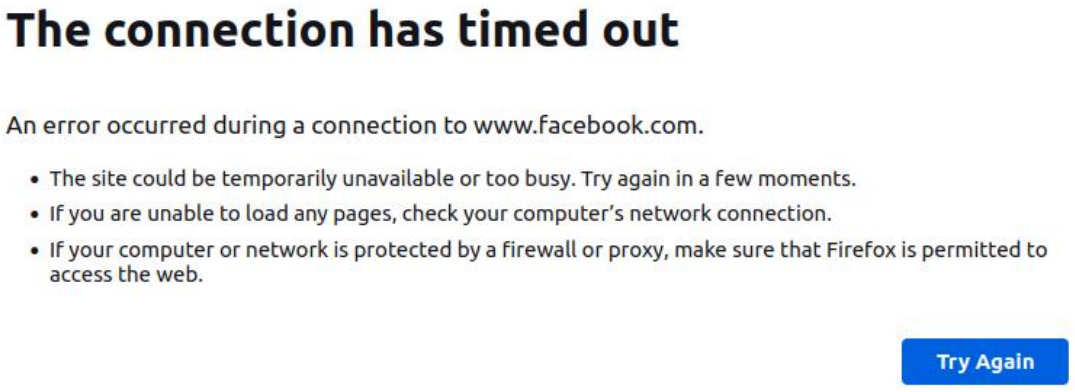

- Sau khi tạo xong danh sách alias, đặt rule theo yêu cầu:



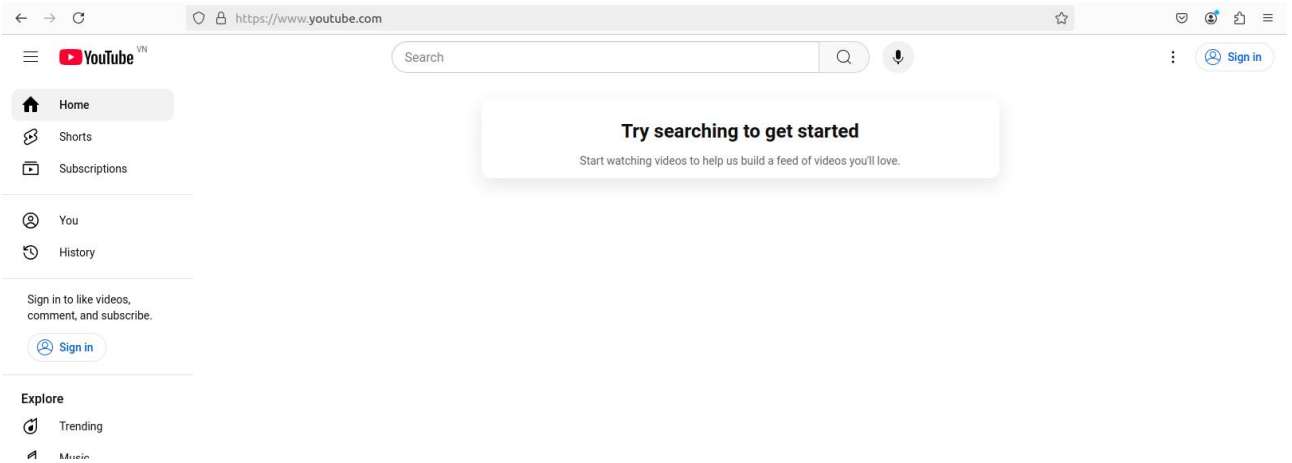

- Ban đầu vẫn có thể truy cập vào facebook bình thường



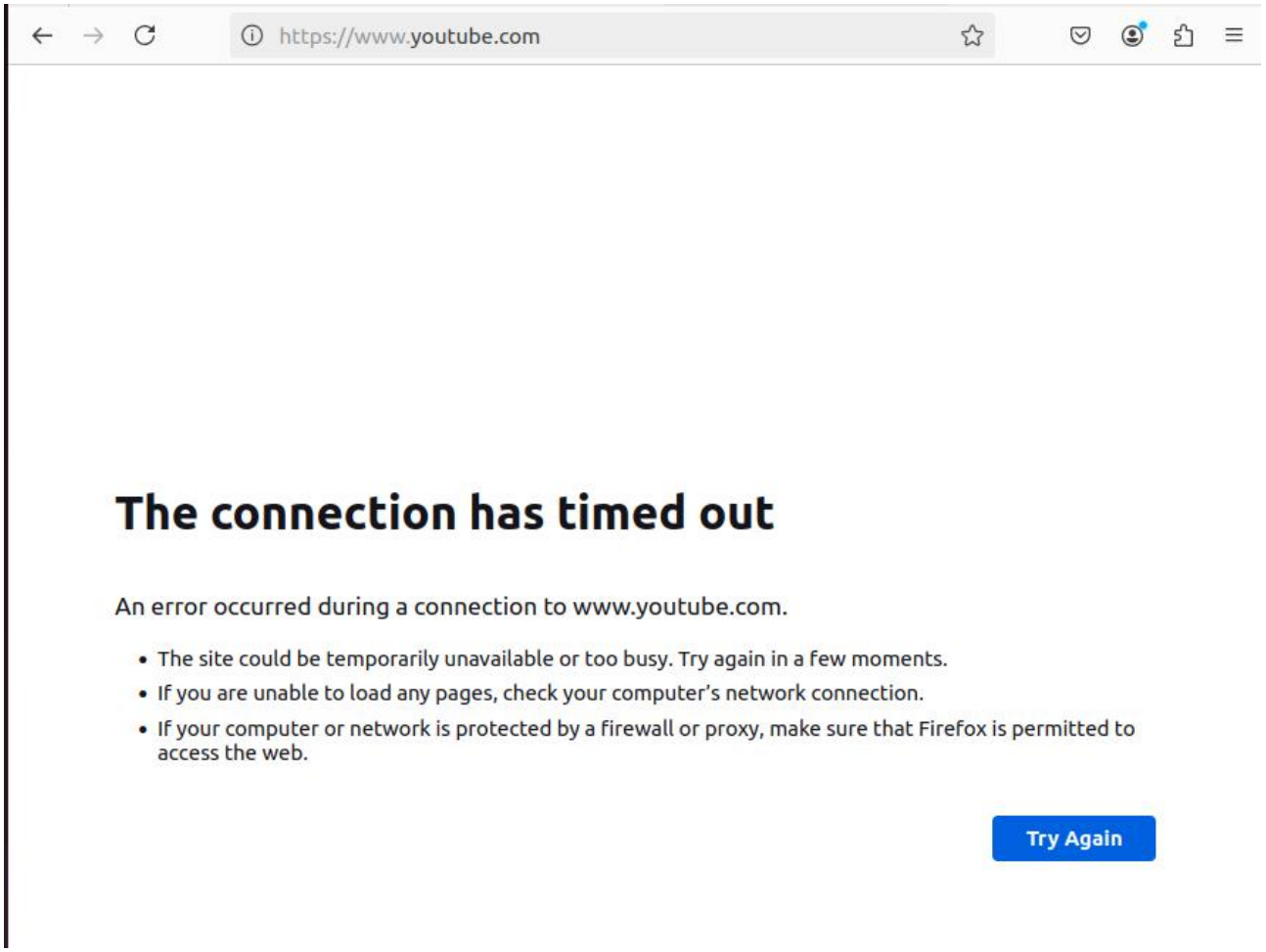

- Sau khi rule được áp dụng thì không thể truy cập vào nữa


- Tương tự như facebook, youtube cũng có thể truy cập bình thường trước khi set rule




- Và không thể truy cập sau khi rule được áp dụng



## 3. Vượt qua sự kiểm soát của Firewall

```
lovelily@Lovelily:~$ ssh -fN -L 8000:localhost:23 server@10.0.3.3
The authenticity of host '10.0.3.3 (10.0.3.3)' can't be established.
ED25519 key fingerprint is SHA256:TIlIyJrX0jKc5syPBq68OPKjHjycxLk7lSnHnO2/SsI.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.0.3.3' (ED25519) to the list of known hosts.
server@10.0.3.3's password:
lovelily@Lovelily:~$ telnet localhost 8000
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
Ubuntu 22.04.5 LTS
server login: server
Password:
Welcome to Ubuntu 22.04.5 LTS (GNU/Linux 6.8.0-49-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

Expanded Security Maintenance for Applications is not enabled.

2 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

7 additional security updates can be applied with ESM Apps.
Learn more about enabling ESM Apps service at https://ubuntu.com/esm

New release '24.04.1 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

server@server:~$
```

*1. Trình bày ý nghĩa các tham số sử dụng trong 2 lệnh thiết lập tunnel và kết nối telnet ở trên.*

- Lệnh thiết lập tunnel:
  - **-f**: chạy ssh ở chế độ background
  - **-N**: không thưckj hiện lệnh từ xa
  - **-L 8000:localhost:23**: thiết lập một kênh chuyển tiếp port (port forwarding). Ở đây port 8000 trên máy A sẽ được chuyển tiếp đến port 23 trên máy B.
  - **server@10.0.3.3**: username và địa chỉ IP của máy B.
- Lệnh kết nối telnet:
  - **Localhost**: địa chỉ của máy A.
  - **8000**: port được thiết lập để chuyển tiếp thông qua tunnel.

➔ Thiết lập một tunnel SSH từ máy A sang máy B. Sau đó sử dụng telnet trên máy A kết nối đến port 8000, nhưng dữ liệu sẽ được chuyển tiếp qua tunnel và kết nối đến port 23 của máy B.

*2. Khi sử dụng lệnh telnet, thực chất các gói tin này có đi qua máy Firewall không? Nếu có, nguyên nhân tại sao Firewall không việc sử dụng telnet này? Nếu không, thì kết nối từ máy A đến máy B như thế nào để không đi qua máy Firewall?*

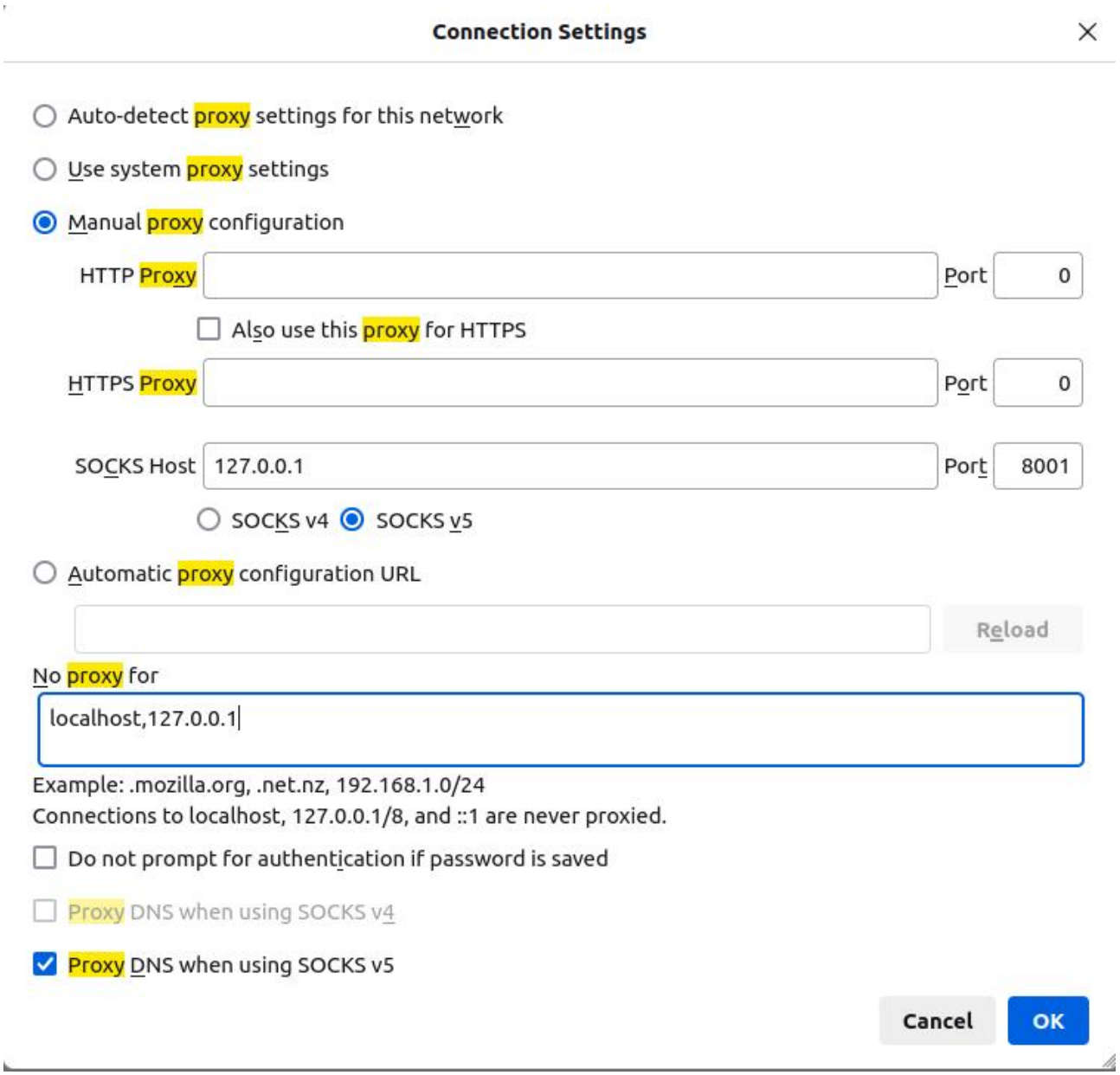
- Các gói tin có đi qua firewall. Nhưng thay vì đi qua cổng 23 của telnet thì gói tin sẽ đi qua cổng 8000 của SSH tunnel.
- Các rule được cài sẵn chỉ chặn port 23 của mạng 192.168.3.0/24 nên các gói tin được gửi qua firewall bình thường mà không bị chặn.
- Các gói tin đi từ port 8000 đến port 23 mà không bị firewall chặn vì kết nối SSH tunnel đã được mã hóa và không thể bị giám sát hoặc can thiệp bởi firewall.

*3. Truy cập website www.facebook.com. Mô tả quá trình bạn quan sát được.*

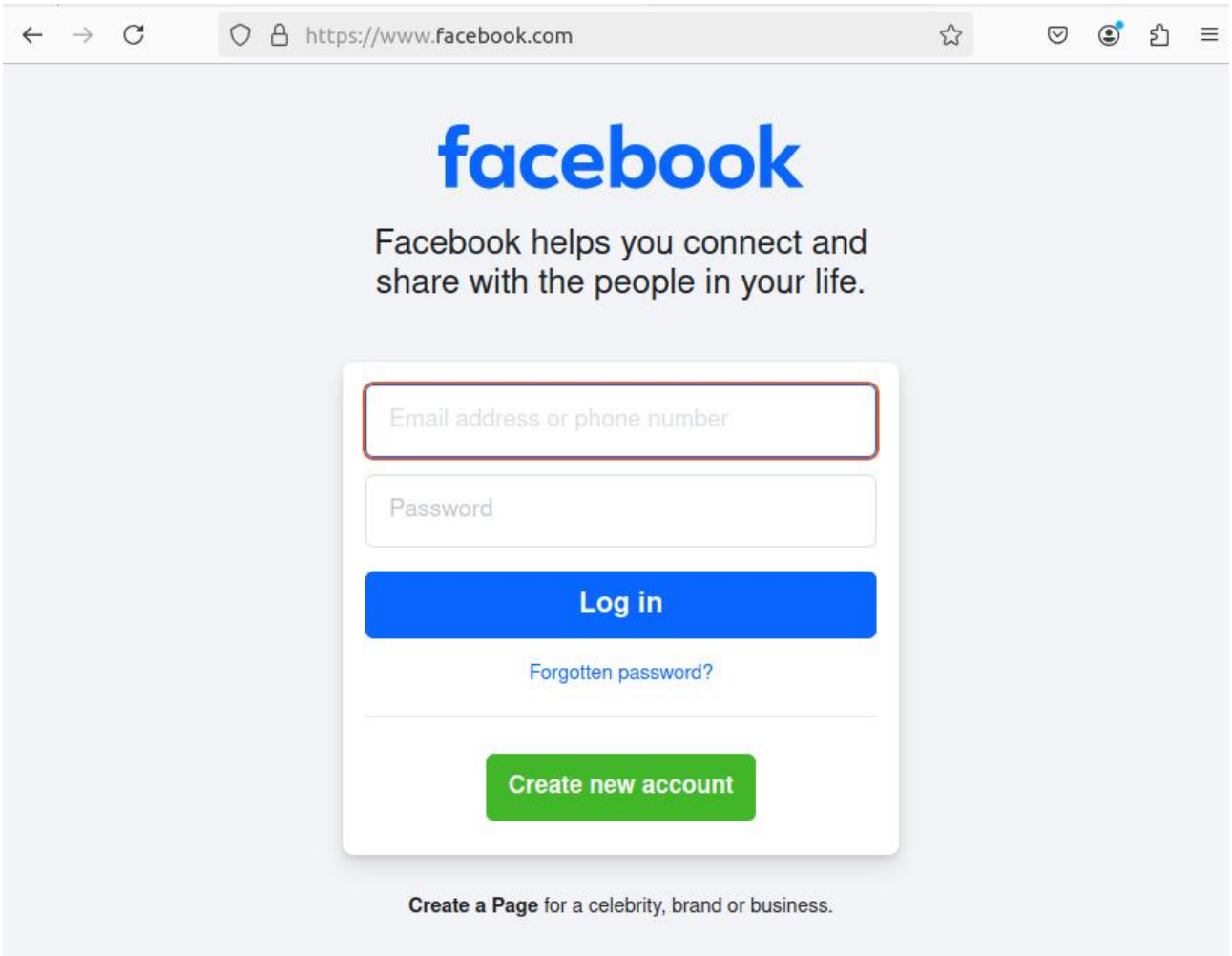
- Đầu tiên, thiết lập tunnel SSH:
  - **-D 8001**: xác định chuyển tiếp port cấp ứng động cục bộ. Nghĩa là máy chủ SSH sẽ tự động tạo quy tắc chuyển tiếp port mới cho mỗi kết nối được tạo với port cục bộ 8001. Sau đó, máy chủ SSH sẽ chuyển tiếp các kết nối đến máy chủ từ xa có địa chỉ IP là 10.0.3.3
  - **-C**: xác định dữ liệu sẽ được nén khi truyền qua tunnel.
  - **server@10.0.3.3**: chỉ định máy chủ từ xa và IP để kết nối đến.

```
lovelily@Lovelily:~$ ssh -D 8001 -C server@10.0.3.3
server@10.0.3.3's password:
Welcome to Ubuntu 22.04.5 LTS (GNU/Linux 6.8.0-49-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

Expanded Security Maintenance for Applications is not enabled.

2 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

7 additional security updates can be applied with ESM Apps.
Learn more about enabling ESM Apps service at https://ubuntu.com/esm

New release '24.04.1 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Sun Dec  8 13:21:32 2024 from localhost
server@server:~$
```

- Sau khi chạy SSH thành công, ta sẽ chỉnh sửa lại cài đặt của trình duyệt web.

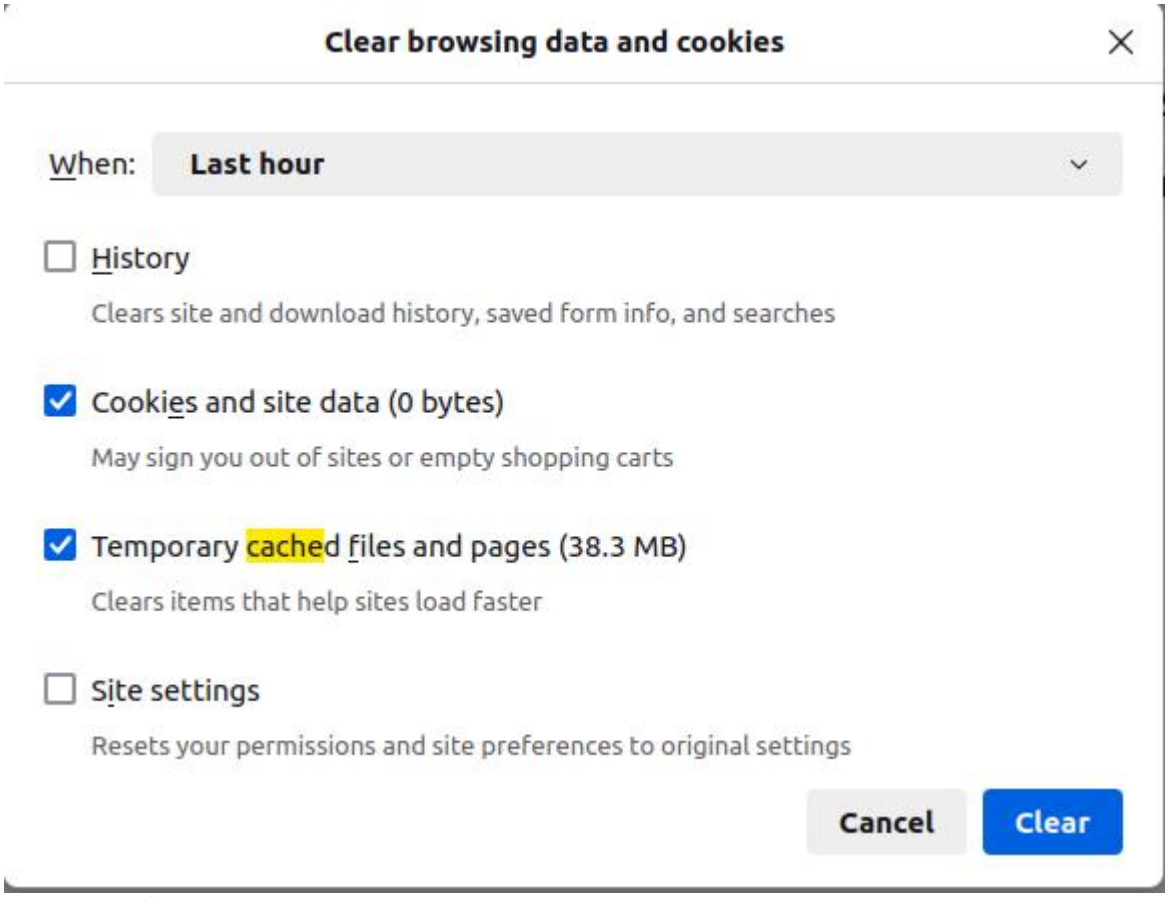



- Truy cập www.facebook.com thành công:




*4. Thực hiện ngắt SSH Tunnel, xoá cache của trình duyệt và truy cập lại trang www.facebook.com. Lúc này, còn truy cập được trang web Facebook không?*

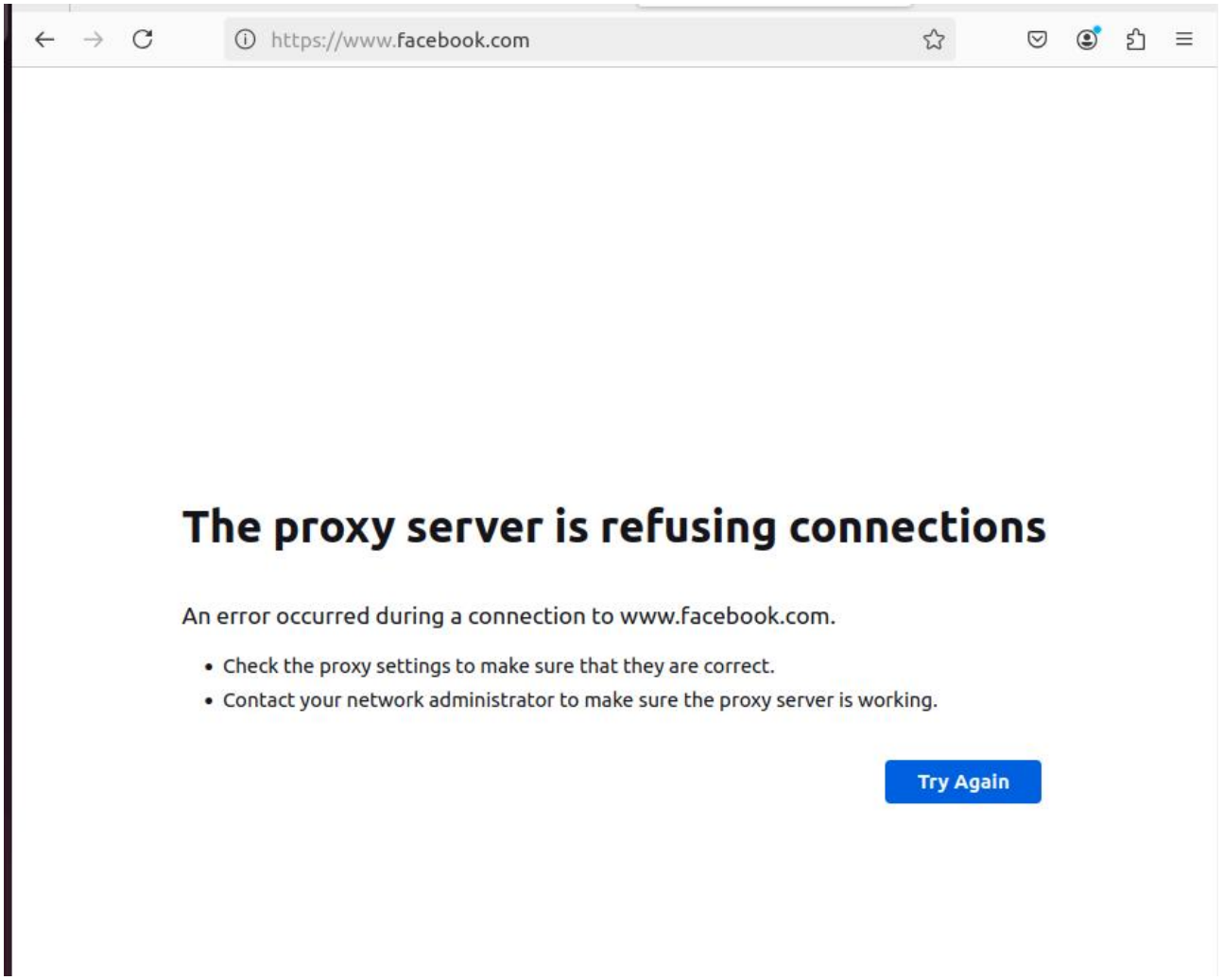
- Thực hiện xóa cache của trình duyệt:




- Ngắt SSH tunnel:

```
lovelily@Lovelily:~$ ps aux | grep 8001
lovelily   10545  0.0  0.0  20744  2816 pts/0    S+   14:40   0:00 grep --color=auto 8001
lovelily@Lovelily:~$
```

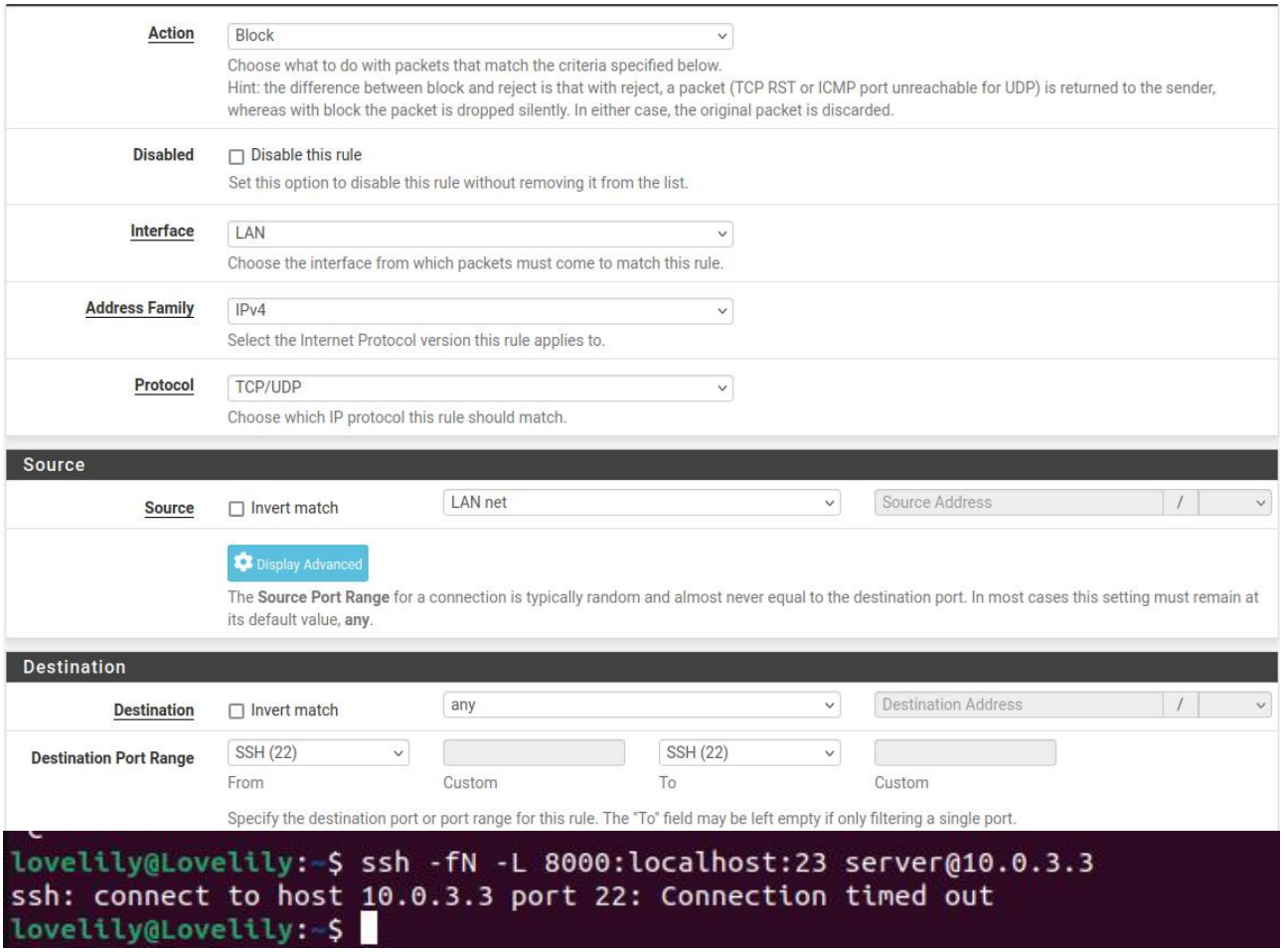
- Truy cập lại www.facebook.com để kiểm tra:




➔ Không thể truy cập được trang web Facebook.

*5. Nếu trên Firewall, áp dụng rule chặn kết nối SSH (port 22), lúc này có thể thiết lập tunnel này được hay không? Tại sao?*

- Nếu trên firewall áp dụng rule chặn kết nối SSH thì lúc này không thể thiết lập tunnel được nữa.
- Vì việc kết nối SSH là trên port 22 và rule của Firewall là block SSH trên port 22 nên việc thiết lập tunnel là không thể.
- Minh chứng:




*6. Đề xuất giải pháp để phát hiện và ngăn chặn các cách thức vượt qua sự kiểm soát của Firewall trong trường hợp trên.*

- Giải pháp phát hiện và ngăn chặn các cách vượt qua Firewall:
  - Kiểm soát port và giao thức SSH:
    - Hạn chế của port SSH chỉ cho phép kết nối từ máy A đến máy B.
    - Sử dụng một port khác ngoài port mặc định.
    - Sử dụng giao thức TCP Wrapper để chỉ cho phép các địa chỉ IP cụ thể kết nối vào port SSH.
  - Thiết lập các quy tắc tường lửa nghiêm ngặt hơn.
  - Sử dụng hệ thống IDS/IPS:
    - Cài đặt và cấu hình một hệ thống IDS/IPS trên pfSense để theo dõi các mô hình hoạt động đáng ngờ.

## 4. Triển khai Web Proxy (Application Firewall)

a) Cài đặt và cấu hình Squid

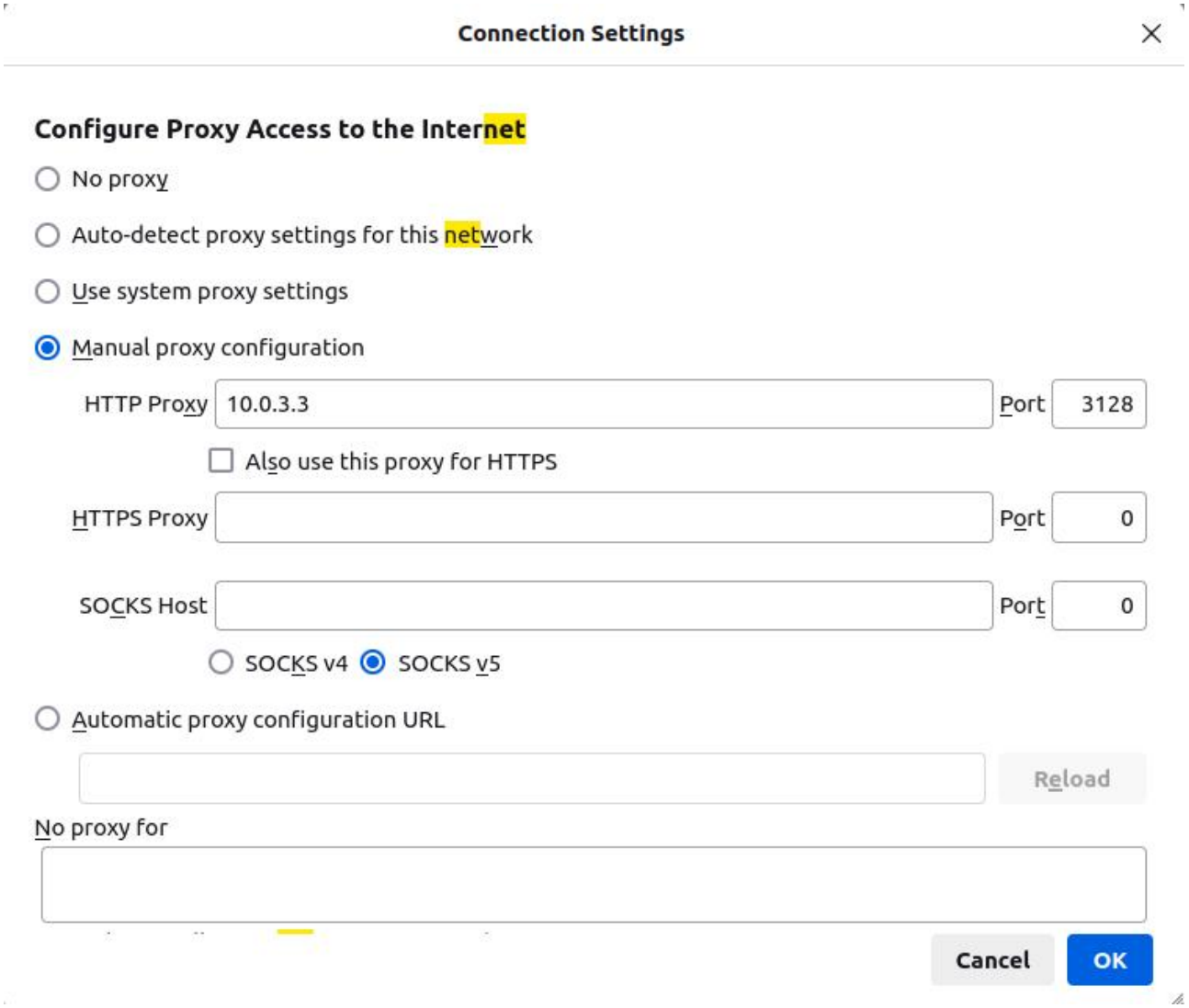
- Bước 1. Cài đặt web proxy server trên máy ảo VM B:

```
lullaby@lullaby-virtual-machine:~$ sudo apt-get install squid
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  libdbi-perl libecap3 squid-common squid-langpack
Suggested packages:
  libmldbm-perl libnet-daemon-perl libsql-statement-perl squidclient squid-cgi squid-purge resolvconf smbclient winbind
The following NEW packages will be installed:
  libdbi-perl libecap3 squid squid-common squid-langpack
0 upgraded, 5 newly installed, 0 to remove and 57 not upgraded.
Need to get 3.809 kB of archives.
After this operation, 14,9 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://vn.archive.ubuntu.com/ubuntu jammy/main amd64 libecap3 amd64 1.0.1-3.2ubuntu4 [17,0 kB]
Get:2 http://vn.archive.ubuntu.com/ubuntu jammy/main amd64 squid-langpack all 20200403-1 [170 kB]
Get:3 http://vn.archive.ubuntu.com/ubuntu jammy-updates/main amd64 squid-common all 5.9-0ubuntu0.22.04.2 [204 kB]
Get:4 http://vn.archive.ubuntu.com/ubuntu jammy/main amd64 libdbi-perl amd64 1.643-3build3 [741 kB]
Get:5 http://vn.archive.ubuntu.com/ubuntu jammy-updates/main amd64 squid amd64 5.9-0ubuntu0.22.04.2 [2.678 kB]
```

Khởi động lại service squid.

```
lullaby@lullaby-virtual-machine:~$  service squid start
lullaby@lullaby-virtual-machine:~$ service squid restart
```

- Bước 2. Trên máy VM A, cấu hình trình duyệt để sử dụng kết nối proxy qua proxy server của VM B. Từ Firefox browser, truy cập vào phần thiết lập Network.



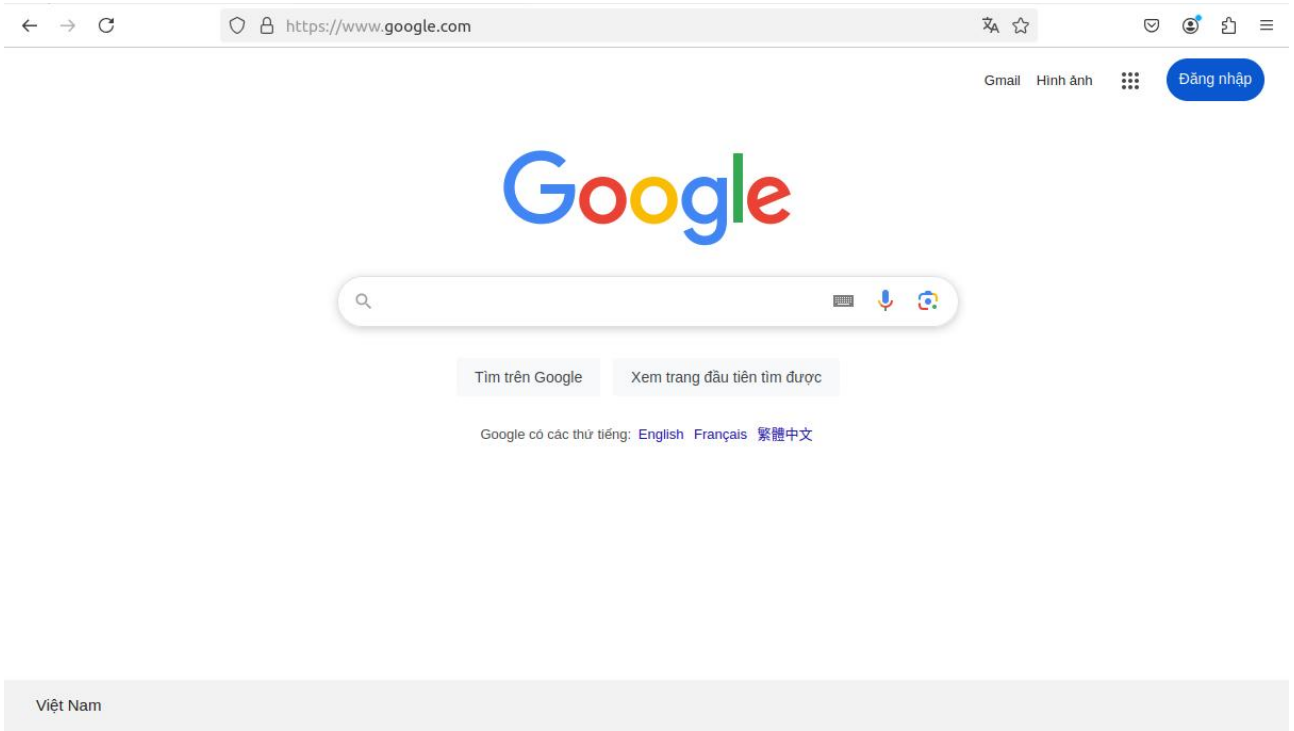
- Bước 3. Mặc định, squid sẽ chặn truy cập tất cả các trang web. Để cho phép truy cập, điều chỉnh trong file /etc/squid/squid.conf.

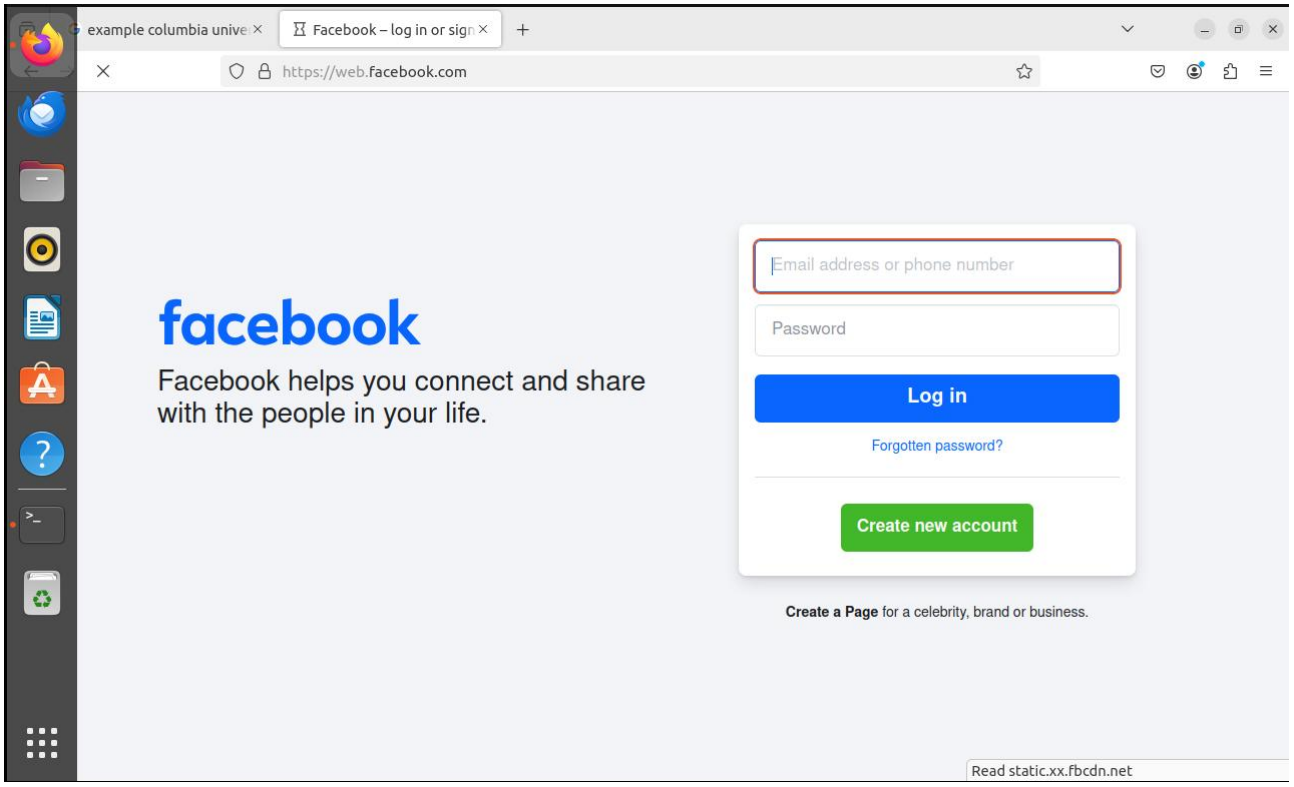
```
  GNU nano 6.2                                  /etc/squid/squid.conf *
# following rule (and/or add rules that match your definition of "local"):
# http_access allow localnet

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

#  TAG: adapted_http_access
#       Allowing or Denying access based on defined access lists
#
#       Essentially identical to http_access, but runs after redirectors
#       and ICAP/eCAP adaptation. Allowing access control based on their
#       output.
#
#       If not set then only http_access is used.
```

Và khởi động lại squid.

```
lullaby@lullaby-virtual-machine:~$ service squid restart
```

- Bước 4. Tại máy A, truy cập vào trang web https://google.com và website https://www.facebook.com.






*Giải thích*: Firewall đã chặn máy A truy cập mà vẫn có thể truy cập được là vì máy A cấu hình trình duyệt để sử dụng kết nối proxy qua proxy server của máy B, máy A sẽ gửi các yêu cầu đến proxy trên máy B mà không gửi trực tiếp đến server đích mà firewall không chặn kết nối giữa máy A và máy B.

b) Thiết lập chuyển hướng (Rewrite / URL Redirection)

Tạo file script với nội dung như hình bên dưới.

```
  GNU nano 6.2                                    /etc/squid/script.pl
#!/usr/bin/perl -w
use strict;
use warnings;
# Forces a flush after every write or print on the STDOUT
select STDOUT; $| = 1;
# Get the input line by line from the standard input.
# Each line contains an URL and some other information.
while (<>)
{
        my @parts = split;
        my $url = $parts[0];
        if ($url =~ /example\.com/)
        {
             # URL Rewriting
             print "http://www.uit.edu.vn\n";
        }
        else
        {
        # No Rewriting.
        print "\n";
        }
}
```

Cấp quyền thực thi cho file trên.

```
lullaby@lullaby-virtual-machine:~$ sudo chmod +x /etc/squid/script.pl
```

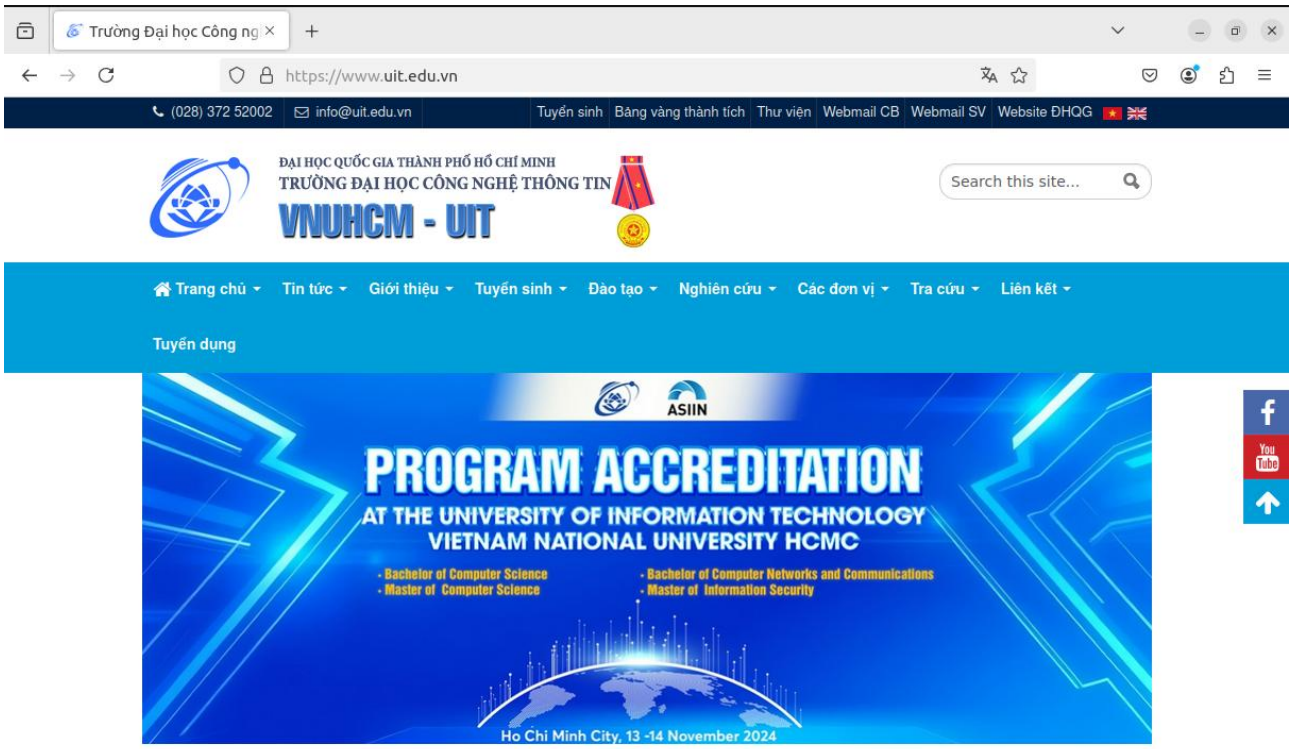
Sửa file cấu hình /etc/squid/squid.conf để sử dụng url_rewrite_program với chương trình trên.

```
 GNU nano 6.2                                  /etc/squid/squid.conf

#  TAG: pinger_program
#       Specify the location of the executable for the pinger process.
#Default:
# pinger_program /usr/lib/squid/pinger

#  TAG: pinger_enable
#       Control whether the pinger is active at run-time.
#       Enables turning ICMP pinger on and off with a simple
#       squid -k reconfigure.
#Default:
# pinger_enable on

# OPTIONS FOR URL REWRITING
# -----------------------------------------------------------------------------

url_rewrite_program /etc/squid/script.pl
url_rewrite_children 5

#  TAG: url_rewrite_program
#       The name and command line parameters of an admin-provided executable
#       for redirecting clients or adjusting/replacing client request URLs.
```

Sau đó, khởi động lại squid.

```
lullaby@lullaby-virtual-machine:~$ sudo service squid restart
```

Từ máy A, truy cập vào website http://example.com ta thấy web tự động chuyển sang website http://www.uit.edu.vn.



*7. Đoạn chương trình script.pl trên hoạt động như thế nào?*

- Đoạn script.pl trên khai báo 2 thư viện strict và warnings
  - Dùng strict để hạn chế các cấu trúc không an toàn.
  - Dùng warnings để cảnh báo chúng ta nếu gõ sai.
- Kế đó, mỗi stdout, output sẽ được flush.
- Mô tả hoạt động:
  - Chương trình script trên sẽ đọc từng dòng lệnh bằng một lệnh while.
  - Với mỗi dòng đọc được, chương trình này sẽ thực hiện các lệnh trong vòng lặp để tìm đoạn chứa URL cần rewrite, nếu tìm được thì sẽ viết thành "http://www/uit.edu.vn\n"

*8. Thay đổi nội dung đoạn chương trình trên để khi truy cập vào website example.com, một hình ảnh cảnh báo dừng lại xuất hiện (như hình dưới).*

Vì bản cài đặt mặc định của Squid chưa thể xử lý các trang web sử dụng giao thức https nên cần sử dụng nginx để dựng và chạy tại localhost.

Đầu tiên, thực hiện cài đặt nginx. Sau đó di chuyển và thay đổi quyền sở hữu file ảnh.

```
lullaby@lullaby-virtual-machine:~$ sudo systemctl start nginx
lullaby@lullaby-virtual-machine:~$ sudo mv /home/lullaby/Downloads/stop.png /var/www/html
lullaby@lullaby-virtual-machine:~$ sudo chown www-data:www-data /var/www/html/stop.png
```

Thay đổi nội dung file script để khi truy cập vào website example.com, một hình ảnh cảnh báo dừng lại xuất hiện.

```
  GNU nano 6.2                                    /etc/squid/script.pl
#!/usr/bin/perl -w
use strict;
use warnings;
# Forces a flush after every write or print on the STDOUT
select STDOUT; $| = 1;
# Get the input line by line from the standard input.
# Each line contains an URL and some other information.
while (<>)
{
        my @parts = split;
        my $url = $parts[0];
        if ($url =~ /example\.com/)
        {
             # URL Rewriting
             print "http://localhost/stop.png\n";
        }
        else
        {
        # No Rewriting.
        print "\n";
        }
}
```

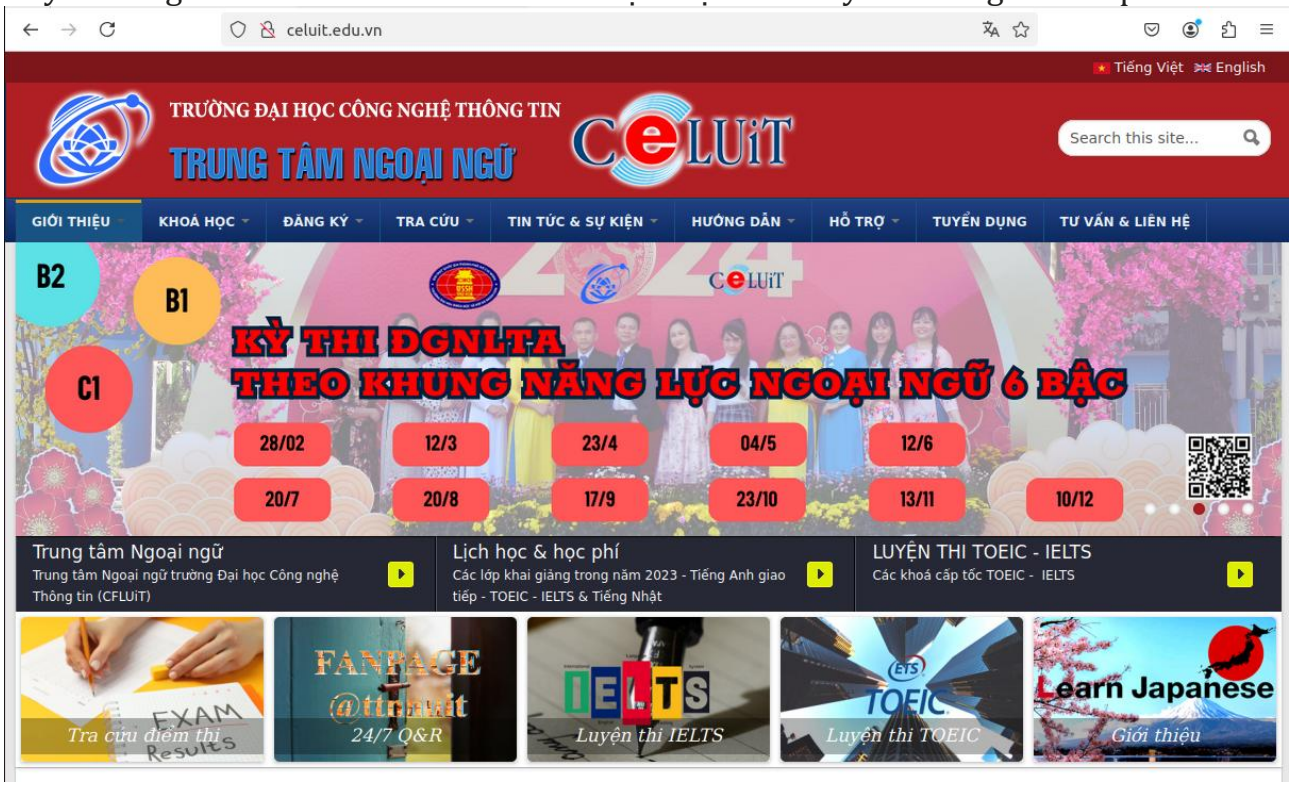
Sau đó, khởi động lại squid.

```
lullaby@lullaby-virtual-machine:~$ sudo service squid restart
```

Khi truy cập vào website example.com, ta thấy xuất hiện hình ảnh cảnh báo dừng lại theo yêu cầu.


*9. Thay đổi nội dung chương trình để khi truy cập website, tất cả các hình ảnh đều được thay bằng hình ảnh bạn thích (như hình minh hoạ dưới)*

Đây là trang web celuit.edu.vn khi chưa thực hiện các thay đổi trong file script.




Đầu tiên, di chuyển và thay đổi quyền sở hữu file ảnh.

```
lullaby@lullaby-virtual-machine:~$ sudo mv /home/lullaby/Downloads/meo-meo.jpg /var/www/html
lullaby@lullaby-virtual-machine:~$ sudo chown www-data:www-data /var/www/html/meo-meo.jpg
```

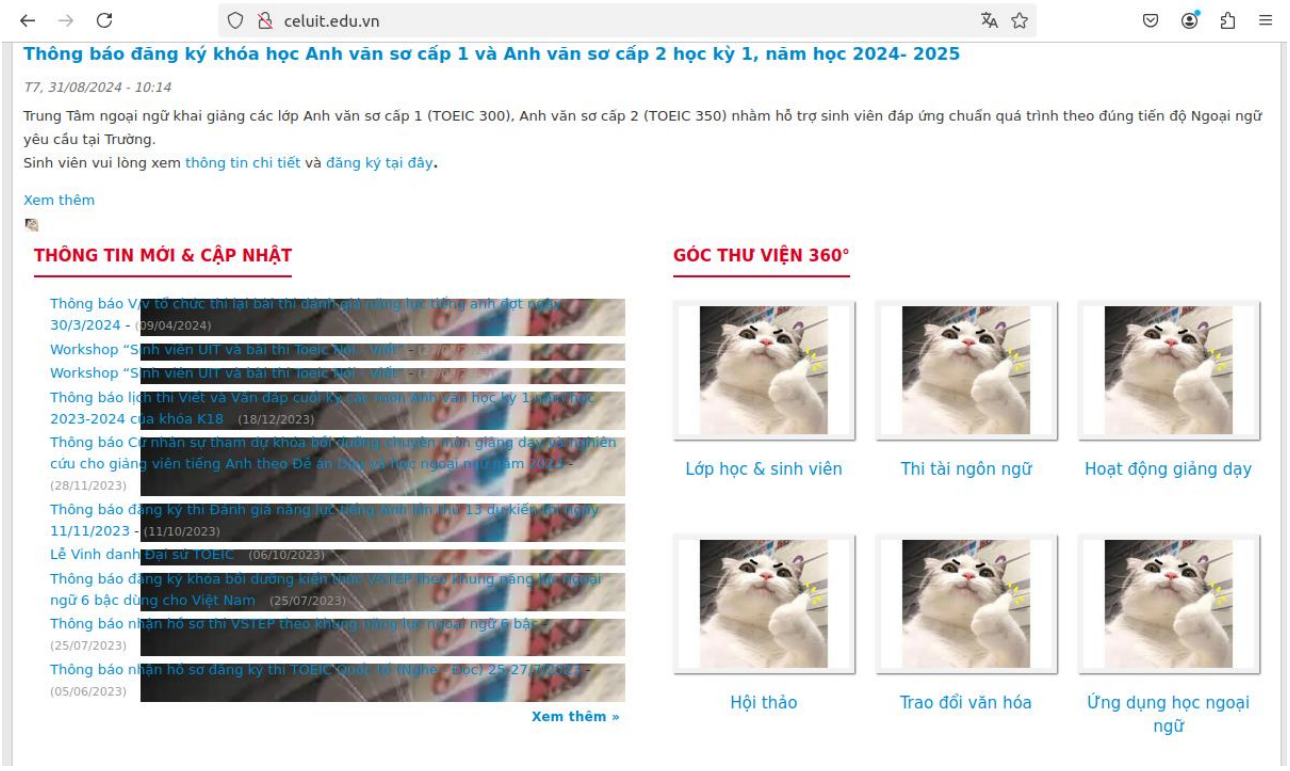
Thay đổi nội dung file script để khi truy cập website, tất cả các hình ảnh đều được thay bằng hình ảnh mong muốn.

```
  GNU nano 6.2                                    /etc/squid/script.pl
#!/usr/bin/perl -w
use strict;
use warnings;
# Forces a flush after every write or print on the STDOUT
select STDOUT; $| = 1;
# Get the input line by line from the standard input.
# Each line contains an URL and some other information.
while (<>)
{
        my @parts = split;
        my $url = $parts[0];
        if ($url =~ /celuit.edu.vn\/.*\.(png|jpg|jpeg|gif|bmp|svg)(.)*/)
        {
             # URL Rewriting
             print "http://localhost/meo-meo.jpg\n";
        }
        else
        {
        # No Rewriting.
        print "\n";
        }
}
```

Sau đó, khởi động lại squid.

```
lullaby@lullaby-virtual-machine:~$ sudo service squid restart
```

Khi truy cập lại vào website celuit.edu.vn ta thấy các hình ảnh đã được thay đổi thành hình ảnh mong muốn (sử dụng Ctrl + Shift + R để tải lại trang web bỏ qua bộ nhớ cache).



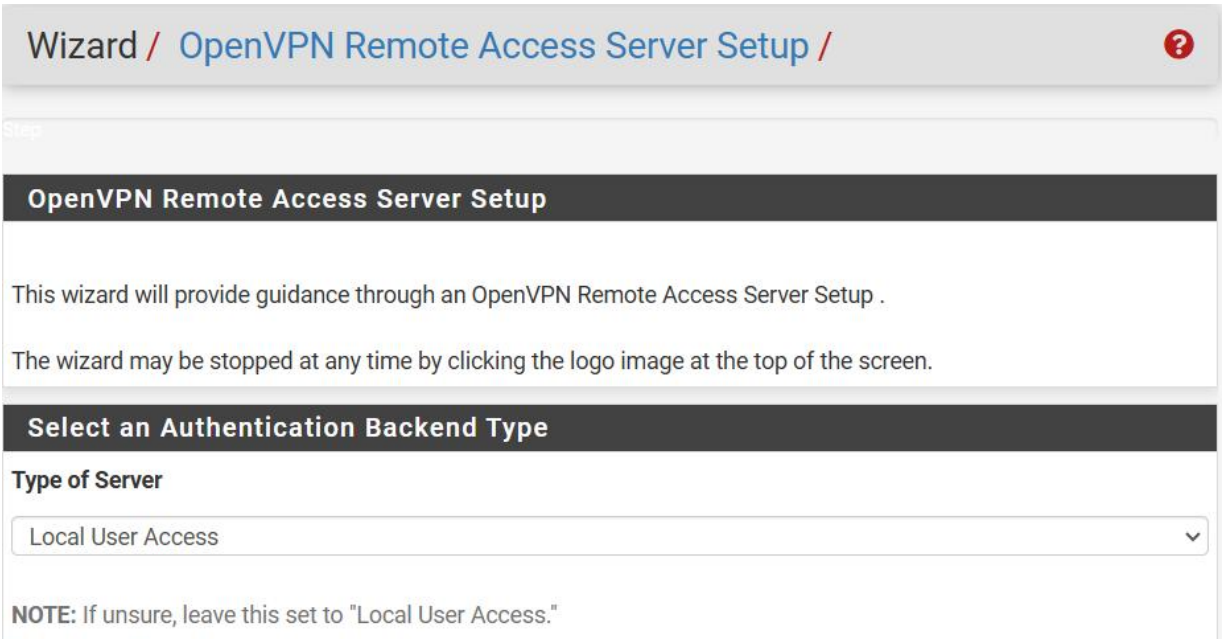
## 5. VPN

*10. Firewall pfSense hỗ trợ các giao thức thiết lập kết nối VPN nào? Những giao thức này có đặc điểm gì khác nhau?*

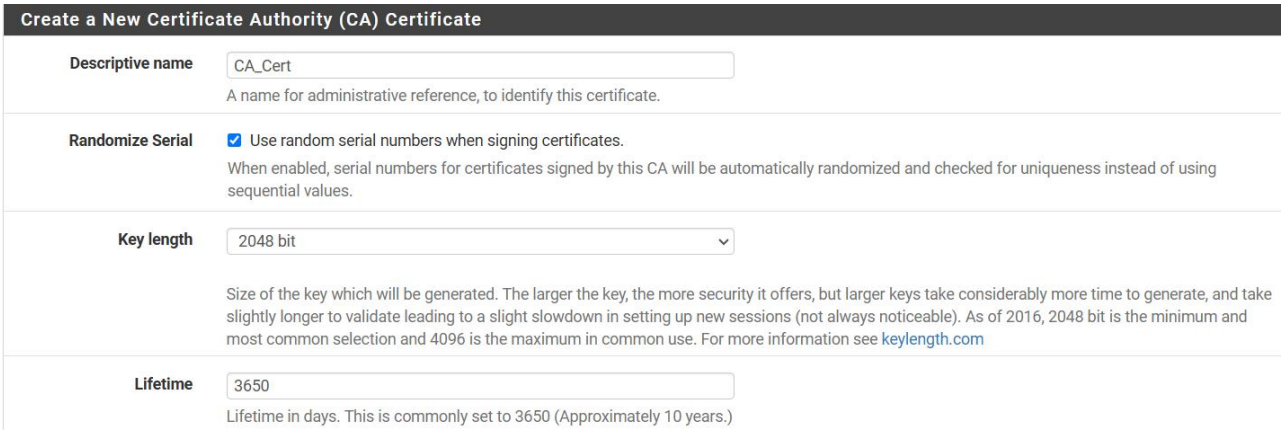
- Firewall pfSense hỗ trợ các giao thức thiết lập kết nối VPN phổ biến như:
  - **OpenVPN**: là giao thức mã nguồn mở và được sử dụng rộng rãi. Nó cung cấp tính bảo mật cao và khả năng tùy chỉnh linh hoạt. OpenVPN sử dụng các cơ chế mã hóa mạnh mẽ và hỗ trợ cả TCP và UDP.
  - **IPsec**: là một giao thức VPN tiêu chuẩn được sử dụng phổ biến trong môi trường doanh nghiệp. IPsec cung cấp tính bảo mật cao và tốc độ kết nối nhanh. Nhưng việc cấu hình có thể phức tạp hơn so với OpenVPN.
  - **L2TP/IPsec**: kết hợp giữa khả năng truy cập từ xa của L2TP và bảo mật của IPsec. Nó thường được sử dụng trên các thiết bị di động và hệ điều hành như iOS hoặc Android.
  - **PPTP**: là một giao thức VPN cổ điển, dễ cấu hình và hoạt động tốt trên nhiều hệ điều hành. Tuy nhiên PPTP không an toàn như các giao thức VPN khác do sử dụng mã hóa yếu.
- Các giao thức VPN này khác nhau về tính bảo mật, tốc độ, khả năng tương thích và cách cấu hình.

*11. Tìm hiểu và thực hiện cấu hình trên pfSense, sao cho từ máy VM B có thể mở kết nối VPN đến pfSense server để truy cập được máy VM A.*

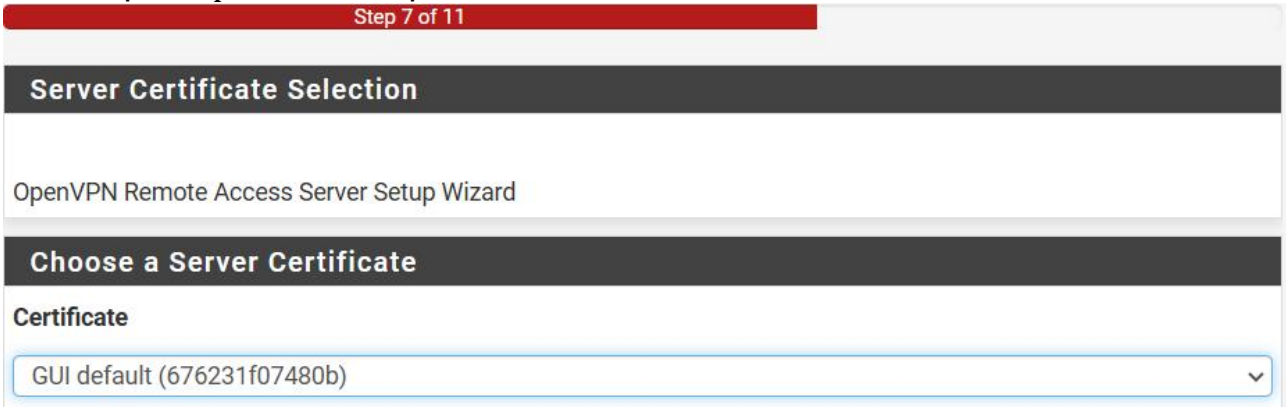
- Vào VPN → OpenVPN → Wizard → Nhấn Next.



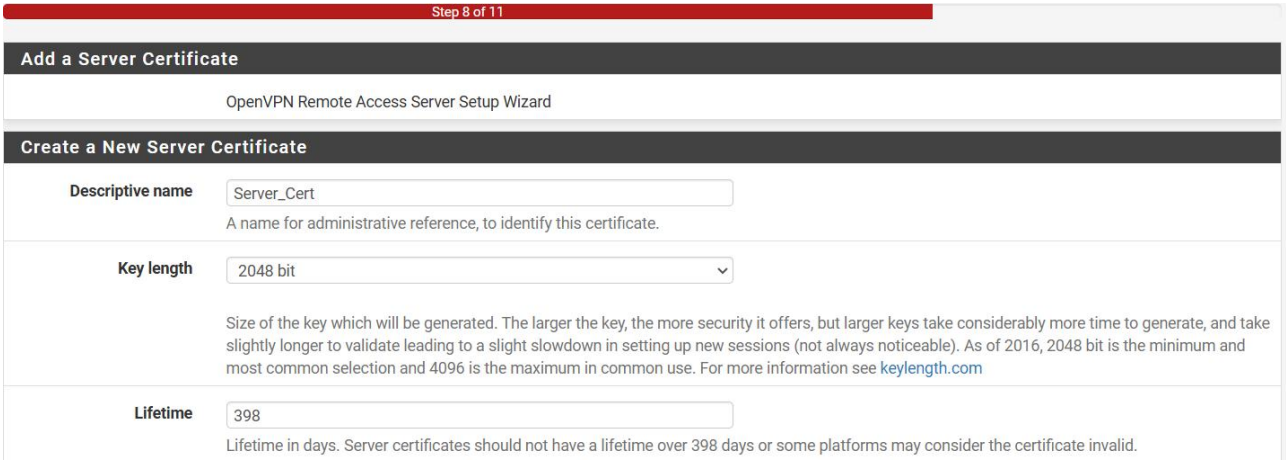

- Tạo Certificate Authority.




- Tại "Step 7 of 11", chọn certificate là **GUI default**




- Tại "Step 8 of 11", thực hiện tạo server certificate.




- Ở bước 9 tại mục Tunnel Settings nhập vào Tunnel Network "10.101.1.0/24"

Step 9 of 11

**Server Setup**

OpenVPN Remote Access Server Setup Wizard

**General OpenVPN Server Information**

**Description**: OpenVPN

A name for this OpenVPN instance, for administrative reference. It can be set however desired, but is often used to distinguish the purpose of the service (e.g. "Remote Technical Staff"). It is also used by OpenVPN Client Export to identify this VPN on clients.

**Endpoint Configuration**

**Protocol**: UDP on IPv4 only

Protocol to use for OpenVPN connections. If unsure, leave this set to UDP.

**Interface**: WAN

The interface where OpenVPN will listen for incoming connections (typically WAN.)

**Local Port**: 1194

Local port upon which OpenVPN will listen for connections. The default port is 1194. This can be left at its default unless a different port needs to be used.

**Cryptographic Settings**

**TLS Authentication**: Enable authentication of TLS packets.

**Generate TLS Key**: Automatically generate a shared TLS authentication key.

**TLS Shared Key**

Paste in a shared TLS key if one has already been generated.

**DH Parameters Length**: 2048 bit

Length of Diffie-Hellman (DH) key exchange parameters, used for establishing a secure communications channel. The DH parameters are different from key sizes, but as with other such settings, the larger the key, the more security it offers, but larger keys take considerably more time to generate. As of 2016, 2048 bit is a common and typical selection.

**Data Encryption Algorithms**: AES-256-GCM, AES-128-GCM, CHACHA20-POLY1305

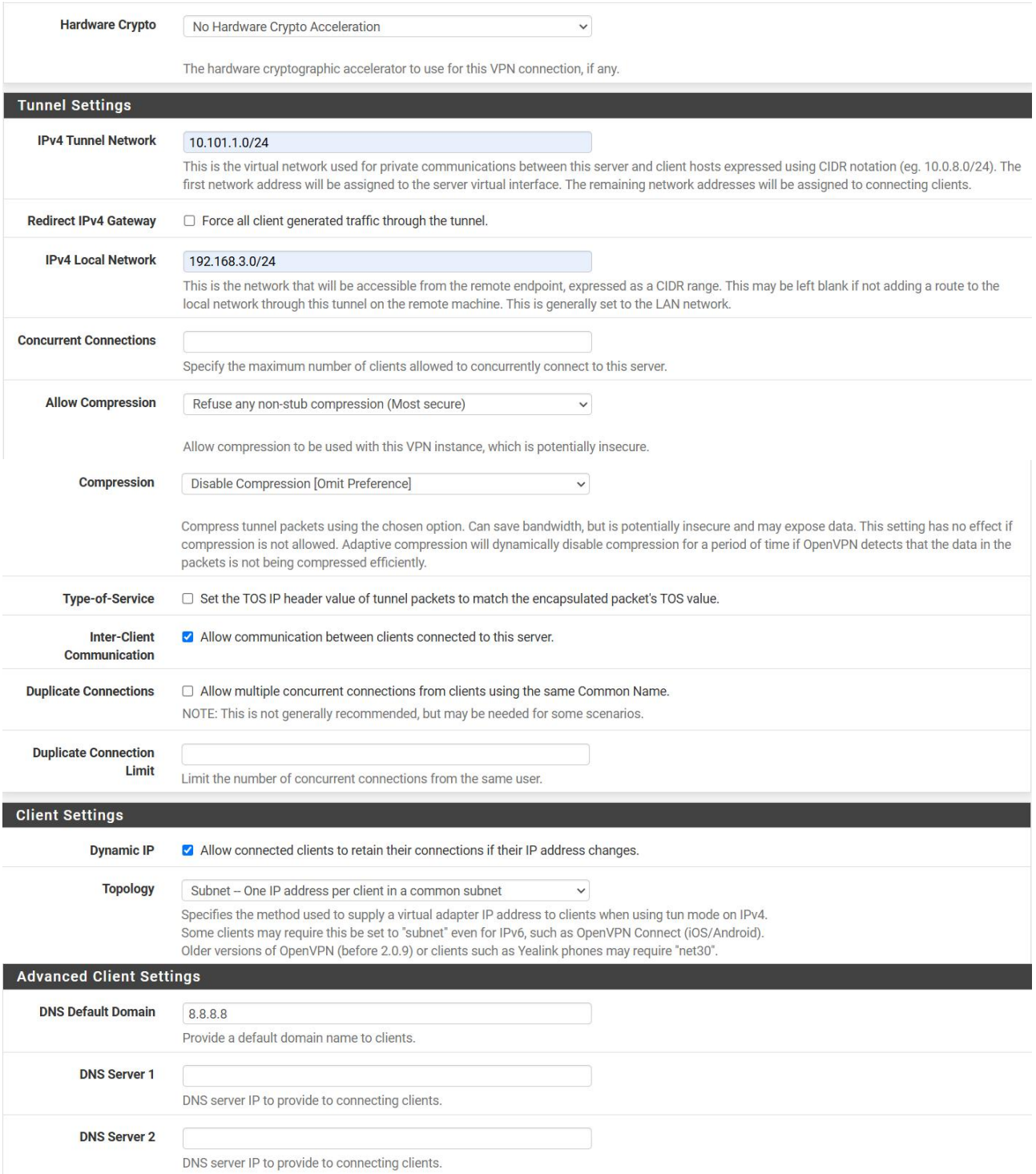
List of algorithms clients can negotiate to encrypt traffic between endpoints. The best practice is to use the exact algorithms listed above, in that order. Certain algorithms will perform better on different hardware, depending on the availability of supported VPN accelerator chips. Edit the server after finishing the wizard for additional choices.

**Fallback Data Encryption Algorithm**: AES-256-CBC (256 bit key, 128 bit block)

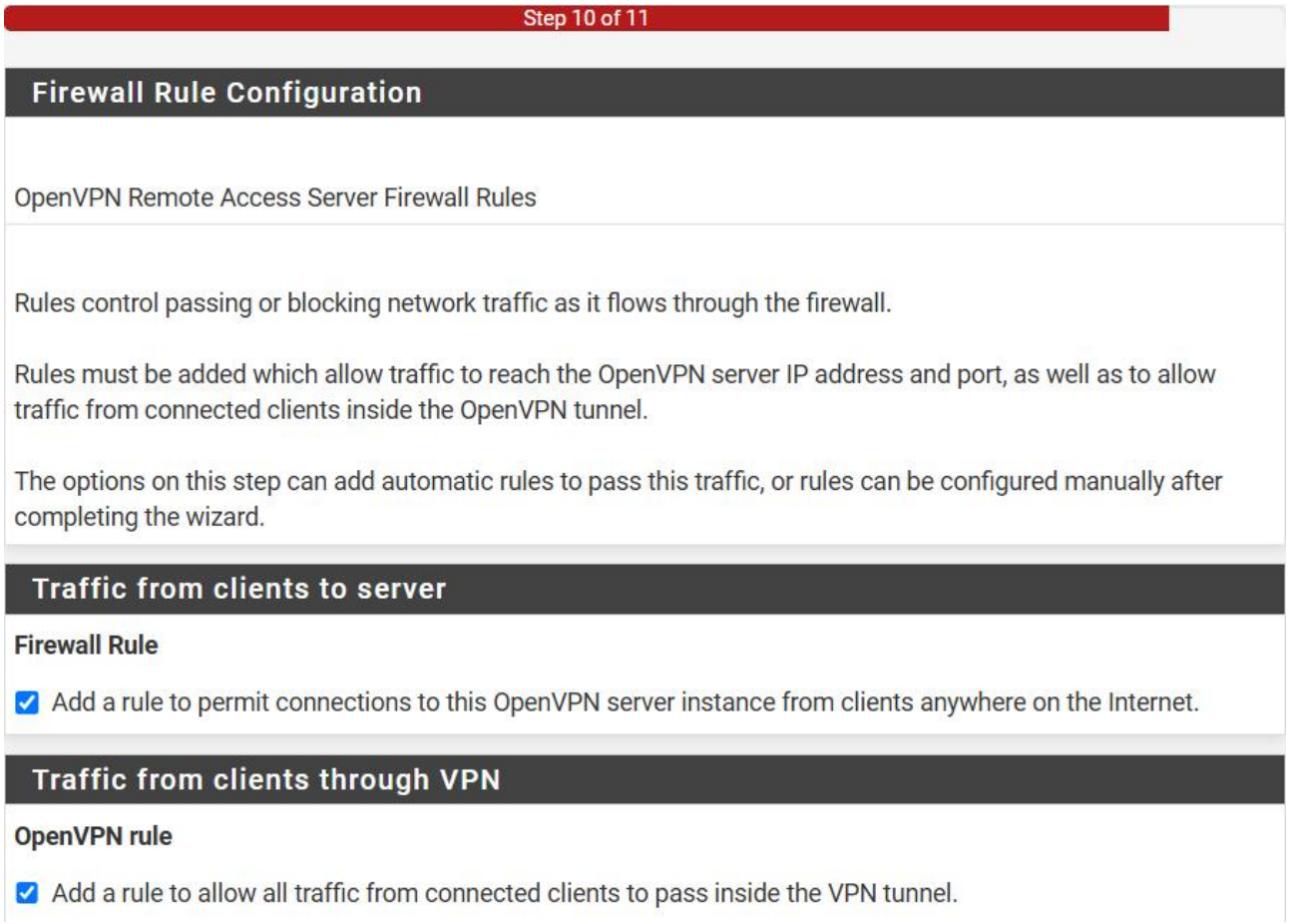
The algorithm used to encrypt traffic between endpoints when data encryption negotiation is diabled or fails.

**Auth Digest Algorithm**: SHA256 (256-bit)

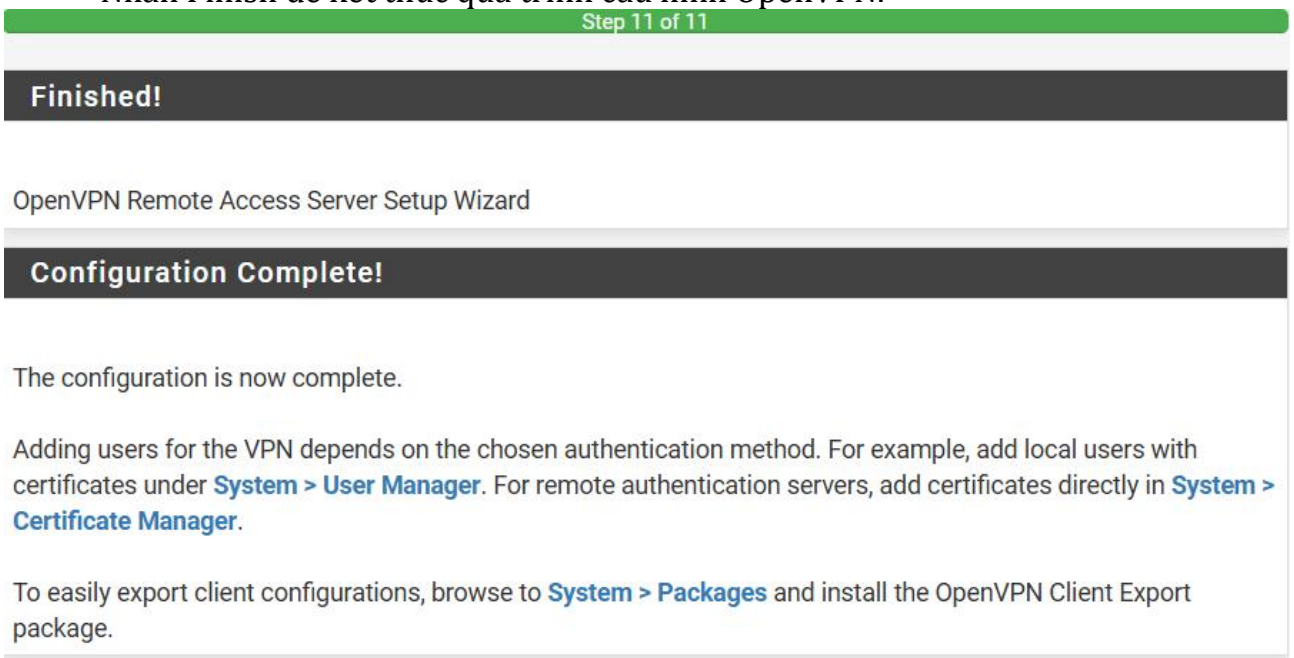
The method used to authenticate traffic between endpoints. This setting must match on the client and server side, but is otherwise set however desired.



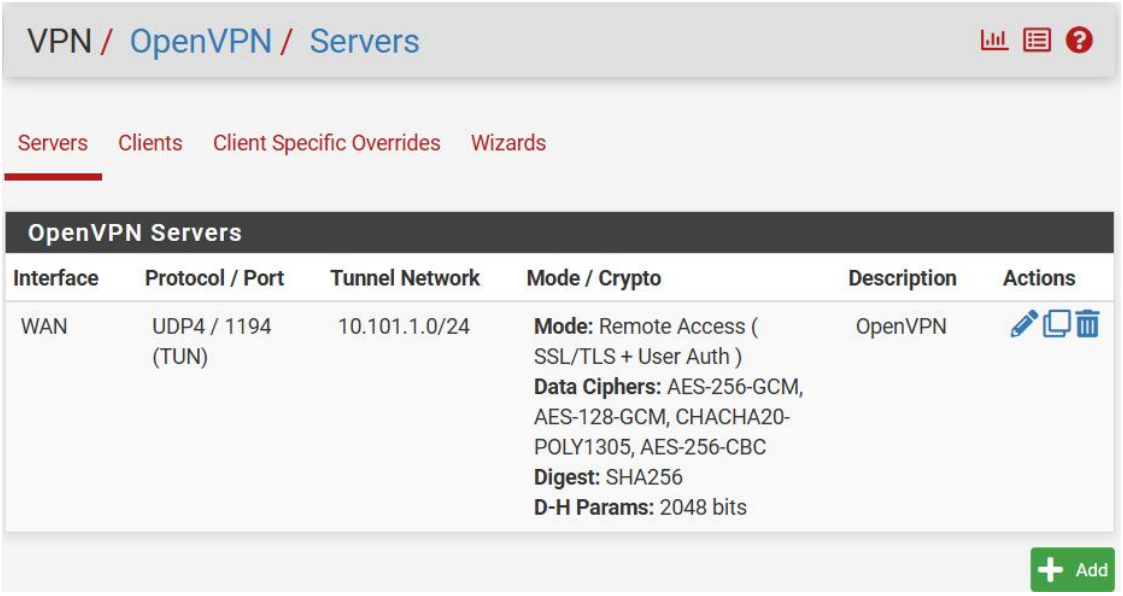

- Nhấn Next, sau đó tick vào 2 giá trị Firewall rule và OpenVPN rule.



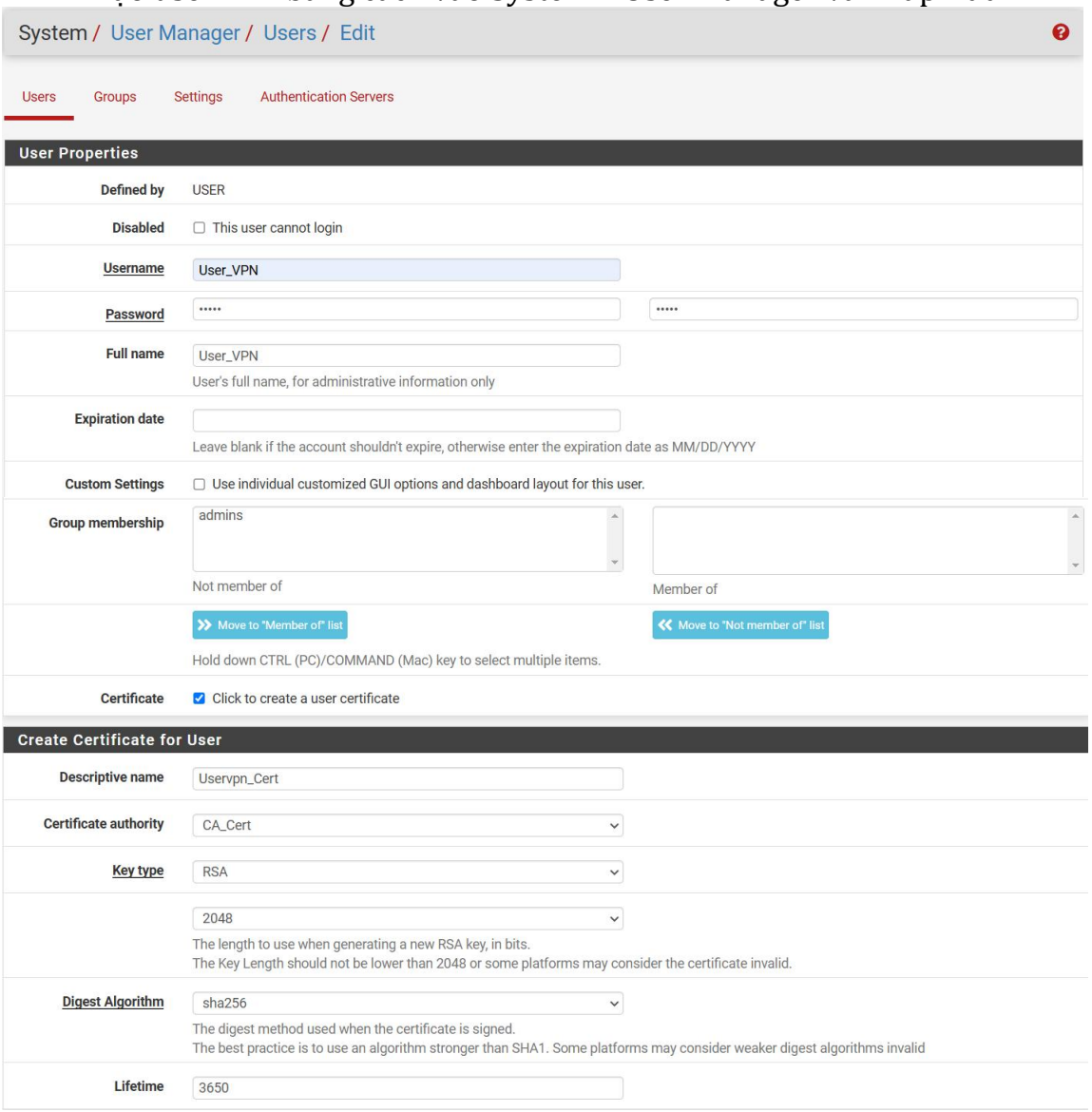

- Nhấn Finish để kết thúc quá trình cấu hình OpenVPN.



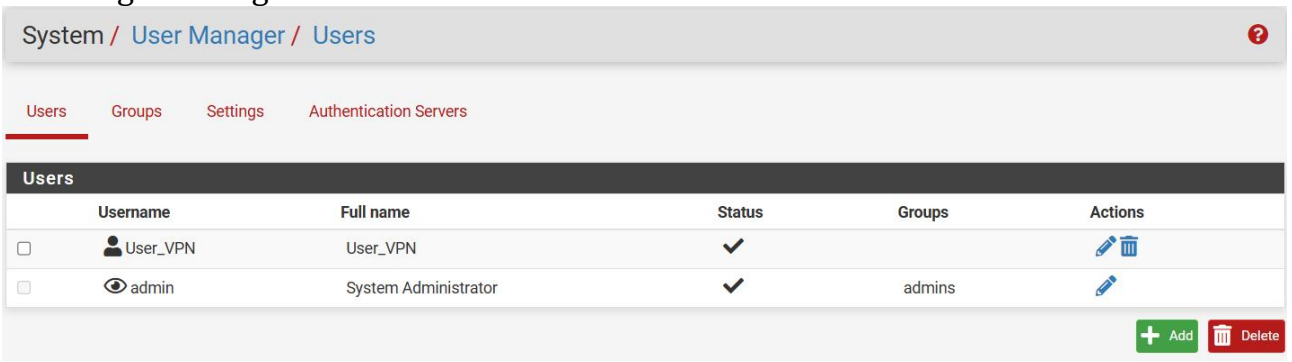

- Cấu hình thành công OpenVPN.



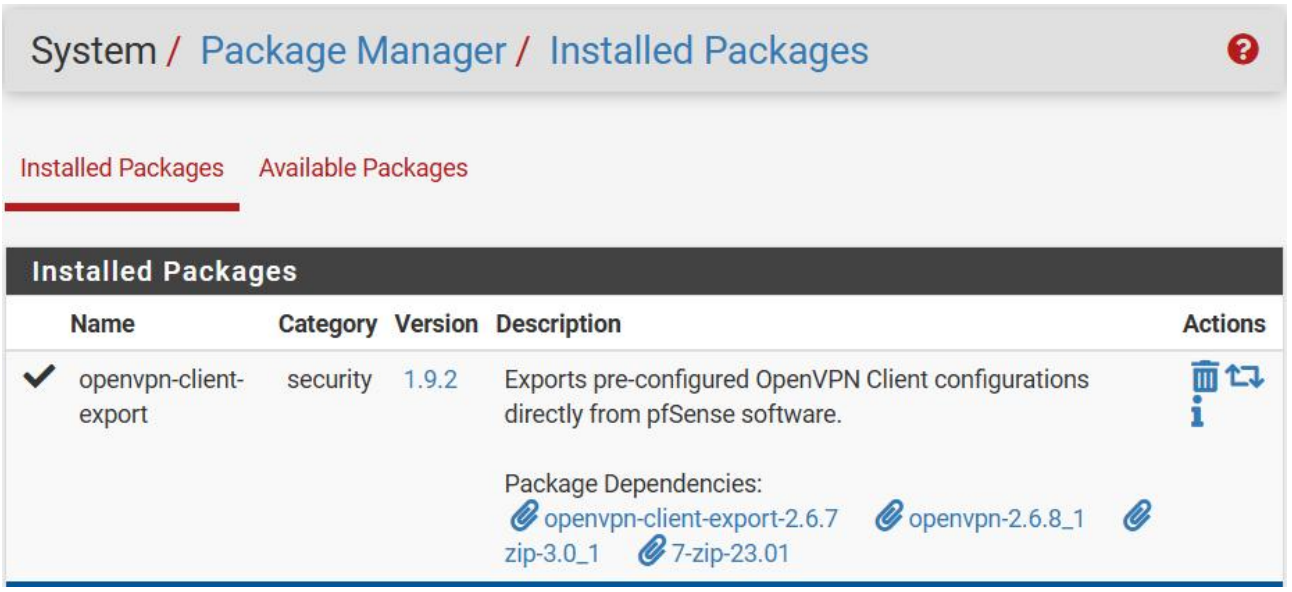

- Tạo user mới bằng cách vào System – User Manager và nhấp Add.



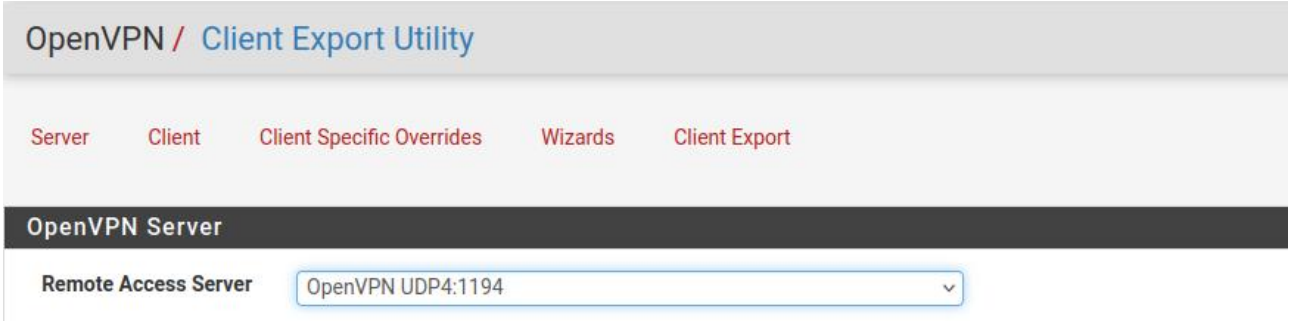
- Sau khi tạo thành công, người dùng vừa tạo sẽ được hiển thị trong danh sách người dùng.



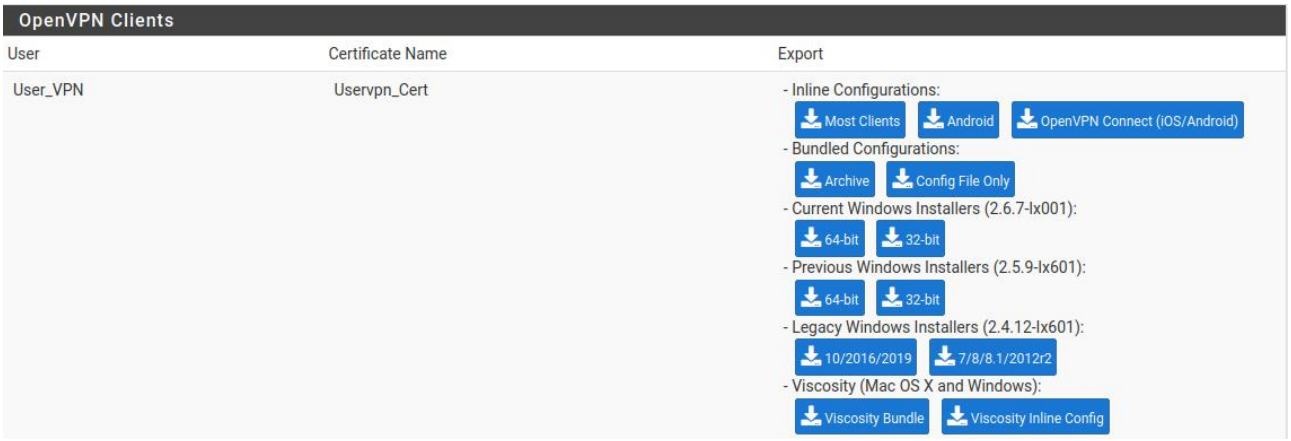

- Tại System → Package Manager → Available Packages → Search "openvpn" → Chọn Install → Chọn Confirm.




Trong OpenVPN, vào thẻ Client Export để tải cấu hình Client Configuration.




- Thực hiện tải file về máy VM B.




- Sau đó cài đặt openvpn về máy bằng lệnh **sudo apt install openvpn** và chạy file config.

```
lullaby@lullaby-virtual-machine:~/Downloads$ sudo openvpn --config pfSense-UDP4-
1194-User_VPN-config.ovpn
2024-12-18 15:48:55 OpenVPN 2.5.11 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [LZ
4] [EPOLL] [PKCS11] [MH/PKTINFO] [AEAD] built on Sep 17 2024
2024-12-18 15:48:55 library versions: OpenSSL 3.0.2 15 Mar 2022, LZO 2.10
Enter Auth Username: User_VPN
🔐 Enter Auth Password: *****
2024-12-18 15:49:02 TCP/UDP: Preserving recently used remote address: [AF_INET]1
0.0.3.2:1194
```

- Sau khi chạy file config, ta sẽ thực hiện ping từ máy B đến máy A. Kết quả là ping thành công.

```
lullaby@lullaby-virtual-machine:~/Downloads$ ping 192.168.3.3
PING 192.168.3.3 (192.168.3.3) 56(84) bytes of data.
64 bytes from 192.168.3.3: icmp_seq=1 ttl=128 time=4.37 ms
64 bytes from 192.168.3.3: icmp_seq=2 ttl=128 time=13.0 ms
64 bytes from 192.168.3.3: icmp_seq=3 ttl=128 time=2.01 ms
^C
--- 192.168.3.3 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2004ms
rtt min/avg/max/mdev = 2.011/6.476/13.047/4.745 ms
```

Tham khảo: https://vietnix.vn/cau-hinh-openvpn-tren-pfsense/