Bộ môn An toàn Thông tin – Khoa MMT&TT
Trường Đại học Công nghệ Thông tin (UIT)

BÁO CÁO BÀI TẬP

Môn học: An toàn mạng máy tính

Kỳ báo cáo: Buổi 04 (Session 04)

Tên chủ đề: Firewall

GV: Nghi Hoàng Khoa

Ngày báo cáo: xx/xx/20xx

Nhóm: 07 (nếu không có xoá phần này)

1. THÔNG TIN CHUNG:

(Liệt kê tất cả các thành viên trong nhóm)

Lớp: NT101.N11.ANTN

STT	Họ và tên	MSSV	Email
1	Võ Anh Kiệt	20520605	20520605@gm.uit.edu.vn
2	Nguyễn Bảo Phương	20520704	20520704@gm.uit.edu.vn

2. NỘI DUNG THỰC HIỆN:[1]

STT	Công việc	Kết quả tự đánh giá
1	Câu 8 câu 9 bài về nhà	0% (Do thiết bị phần cứng và card mạng không đáp ứng)
2	Các câu còn lại	100%

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

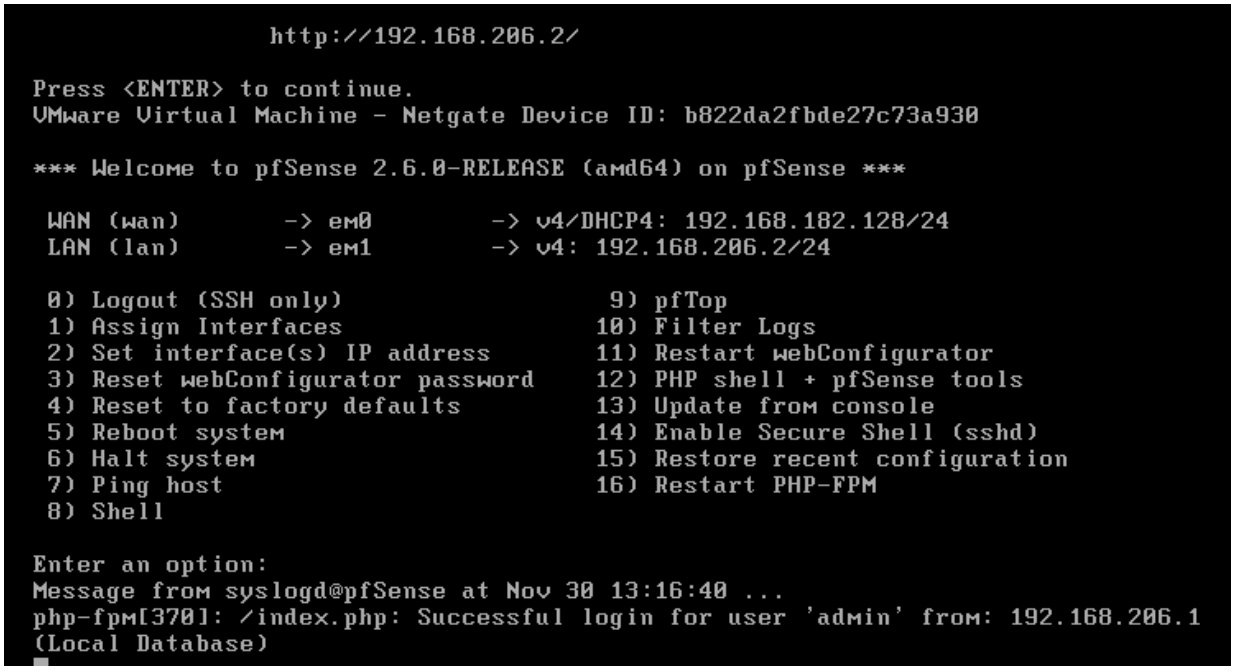
[1] Ghi nội dung công việc, các kịch bản trong bài Thực hành

BÁO CÁO CHI TIẾT

Môi trường

Máy ảo	Interfaces
Firewall	Host-only: 192.168.206.2/24
	NAT: 192.168.182.128/24
VM-A	Host-only: 192.168.206.128/24
VM-B	192.168.208.129.129/24

Firewall



Máy A

```
ubuntu_vm@ubuntuvm2:~$ ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.206.128  netmask 255.255.255.0  broadcast 192.168.206.255
        inet6 fe80::d2b5:f769:30f9:7b4  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:c9:77:6d  txqueuelen 1000  (Ethernet)
        RX packets 216  bytes 19976 (19.9 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 3576  bytes 294424 (294.4 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 3115  bytes 251873 (251.8 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 3115  bytes 251873 (251.8 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Máy B

```
nbp@nbp-virtual-machine:~$ ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.182.129  netmask 255.255.255.0  broadcast 192.168.182.255
        inet6 fe80::48ca:2bae:42bf:6c59  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:57:43:93  txqueuelen 1000  (Ethernet)
        RX packets 45805  bytes 67895563 (67.8 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 4452  bytes 325448 (325.4 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 190  bytes 17388 (17.3 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 190  bytes 17388 (17.3 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Bài tập trên lớp

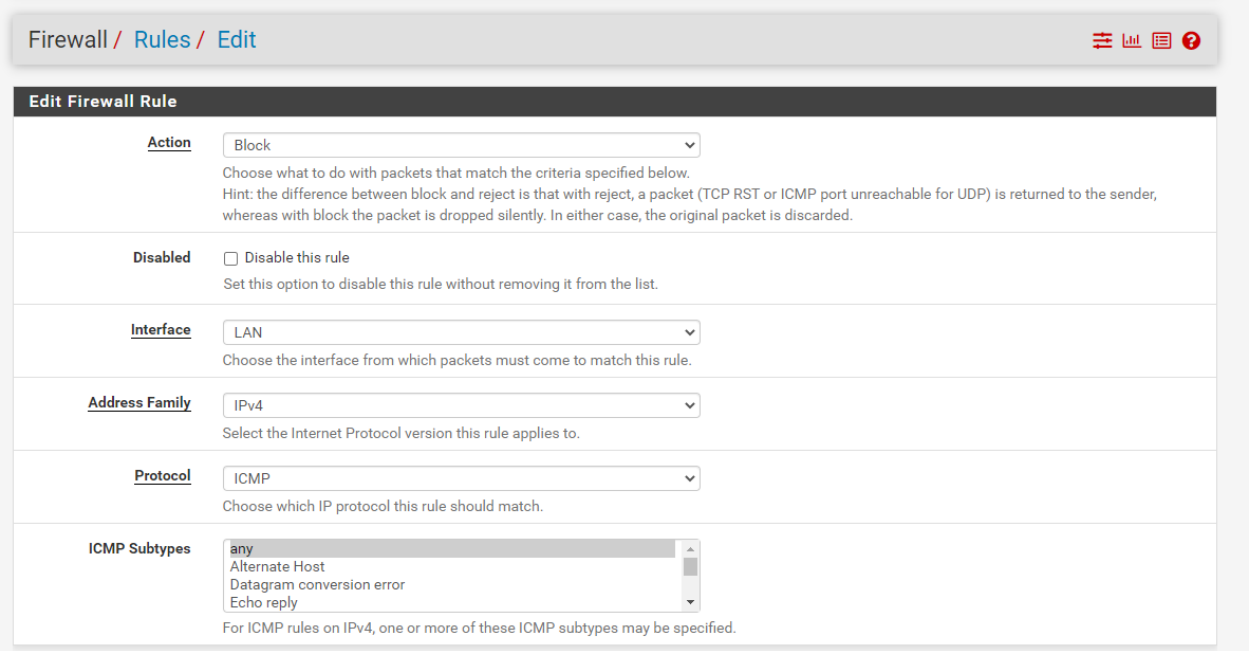
Câu 1. Không cho phép các máy trong mạng nội bộ (192.168.206.0/24) thực hiện ping đến máy VM B.

Trước khi set rule, ta dùng VM-A ping được tới máy B

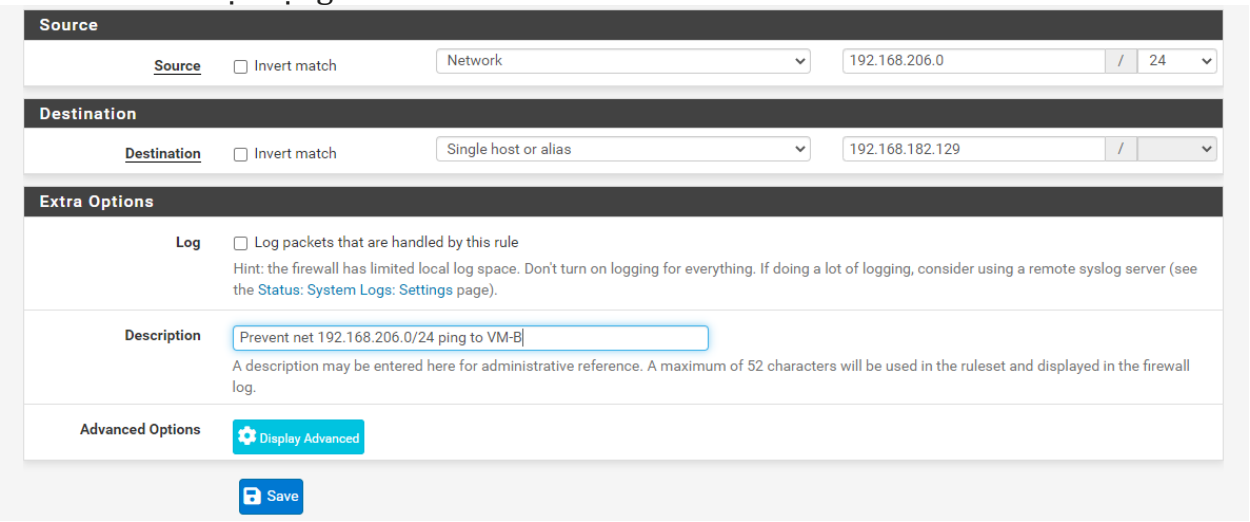
Máy VM-B có địa chỉ IP là 192.168.182.129

```
ubuntu_vm@ubuntuvm2:~$ ping 192.168.182.129
PING 192.168.182.129 (192.168.182.129) 56(84) bytes of data.
64 bytes from 192.168.182.129: icmp_seq=1 ttl=63 time=15.5 ms
64 bytes from 192.168.182.129: icmp_seq=2 ttl=63 time=2.45 ms
64 bytes from 192.168.182.129: icmp_seq=3 ttl=63 time=3.78 ms
64 bytes from 192.168.182.129: icmp_seq=4 ttl=63 time=3.76 ms
64 bytes from 192.168.182.129: icmp_seq=5 ttl=63 time=3.96 ms
^C
--- 192.168.182.129 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4009ms
rtt min/avg/max/mdev = 2.452/5.887/15.484/4.828 ms
```

Ta truy cập vào Firewall -> Rules -> Add
Chọn Action là Block để tạo rule chặn gói tin



Ta để Source là mạng 192.168.206.0 (mạng LAN), Destination là địa chỉ IP của máy B
Cuối cùng ta thêm mô tả để dễ phân biệt, nhấn Save, sau đó chọn Apply Changes để rule bắt đầu hoạt động



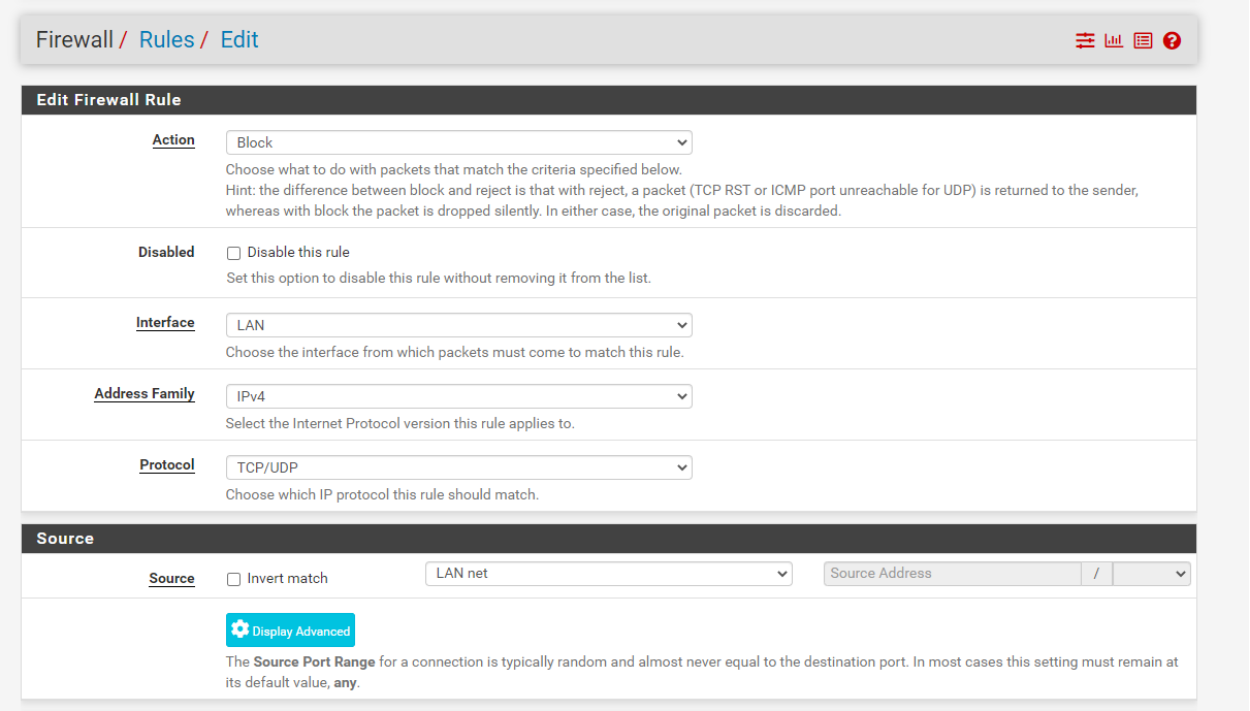
Sau khi set rule, ta đã không ping được tới máy B

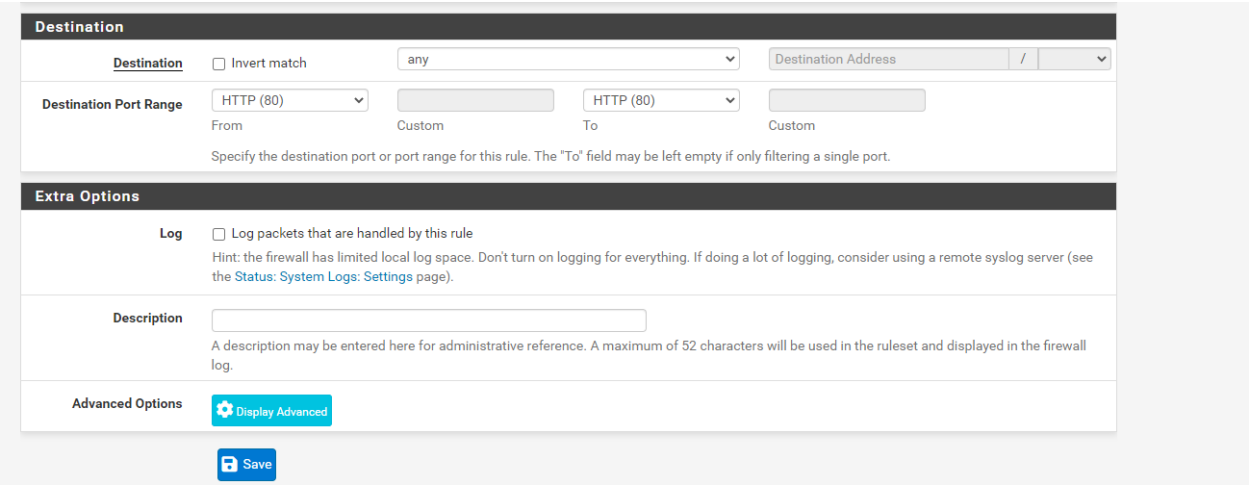
```
ubuntu_vm@ubuntuvm2:~$ ping 192.168.182.129
PING 192.168.182.129 (192.168.182.129) 56(84) bytes of data.
^C
--- 192.168.182.129 ping statistics ---
4 packets transmitted, 0 received, 100% packet loss, time 3070ms
```

Câu 2. Không cho phép các máy trong mạng nội bộ truy cập các website sử dụng giao thức http (cổng 80).

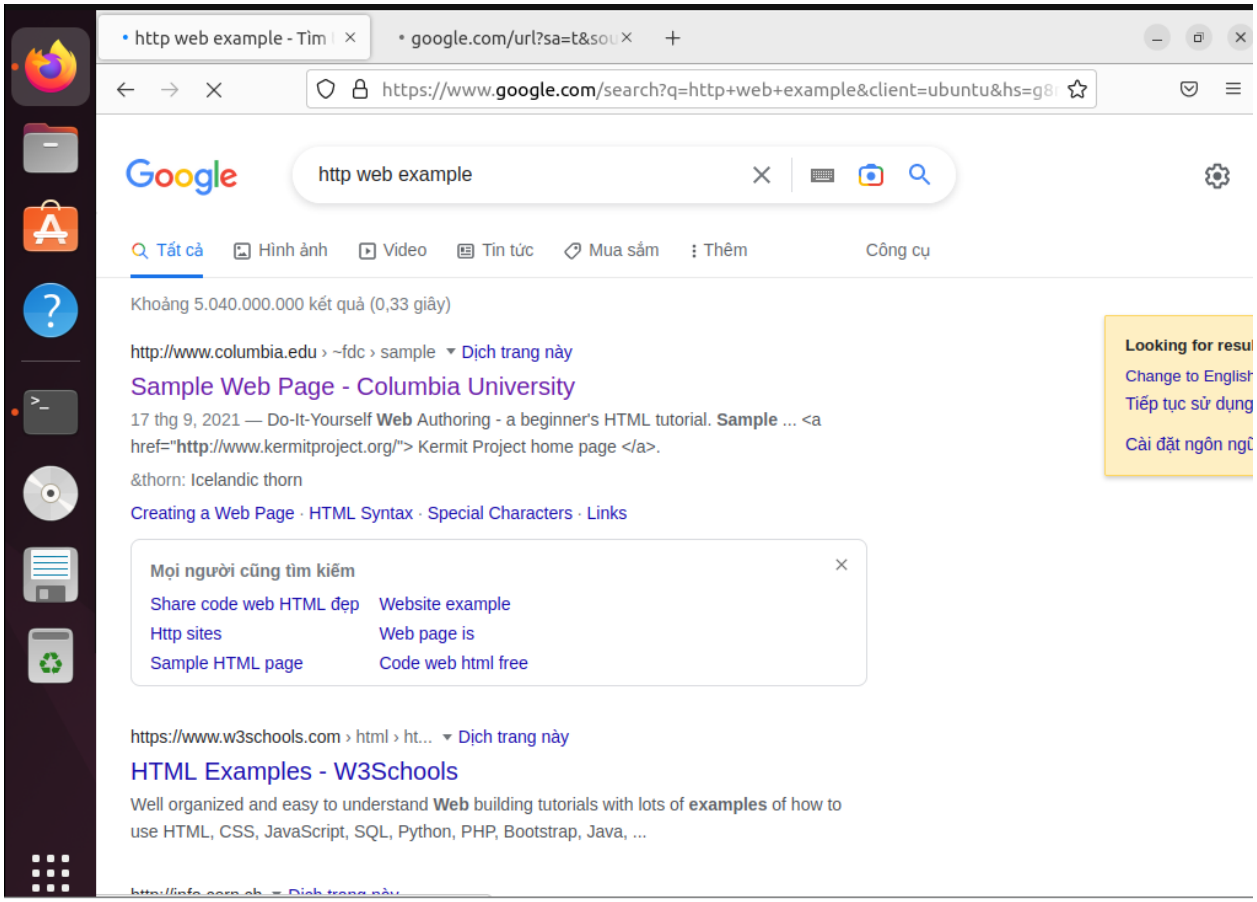
Ta vào Firewall -> Rule -> Add

Tạo action Block, chọn Source là LAN net và Destination là any với port là HTTP 80

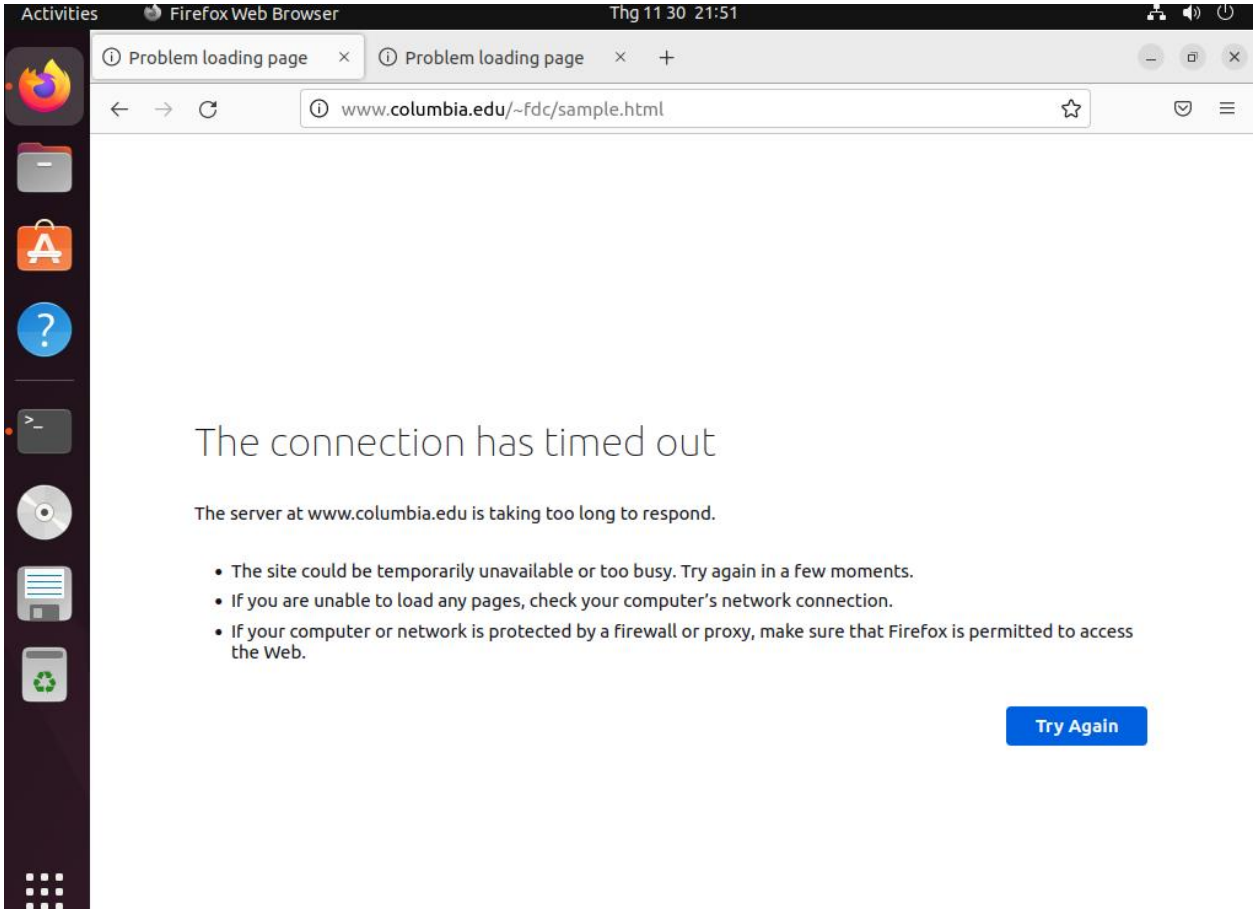




Ta lên google search kiếm 1 trang web http



Truy cập tới và thấy kết nối không thành công



Câu 3. Chặn kết nối telnet từ mạng nội bộ ra bên ngoài.

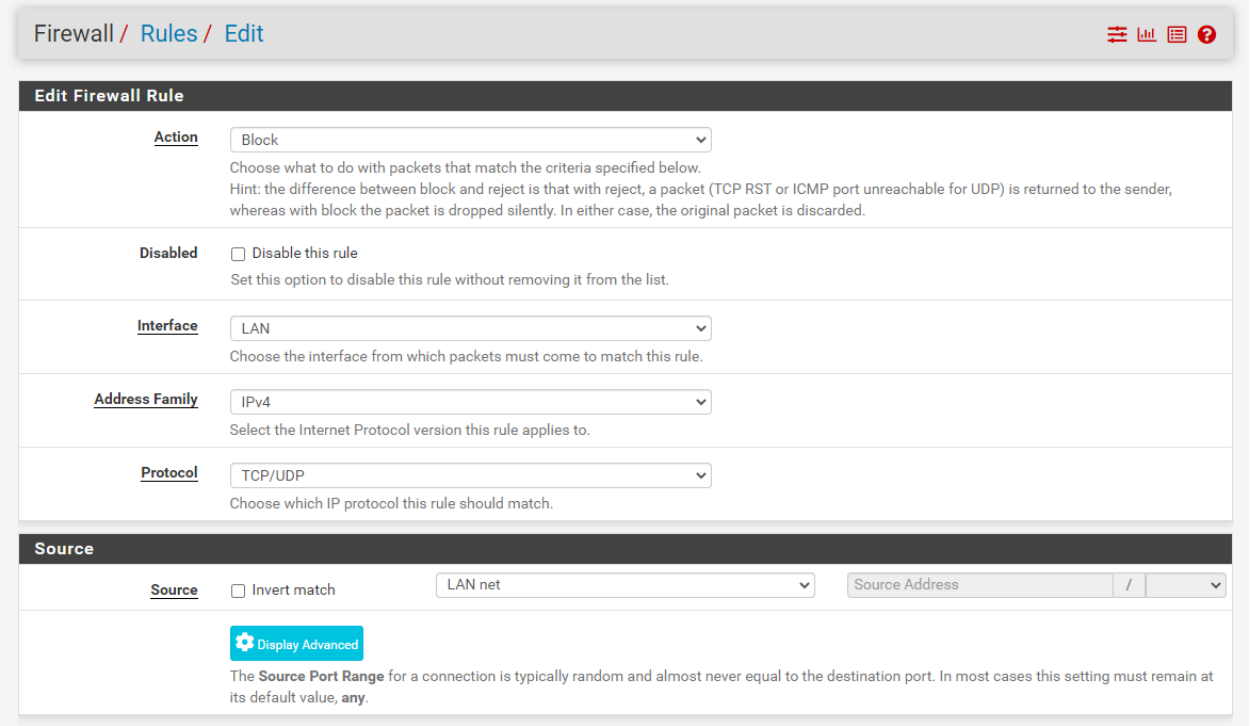
Ta cần cài đặt telnet ở cả 2 máy A và B trước khi bắt đầu

Trước khi set rule, ta telnet được tới máy B (192.168.182.129)

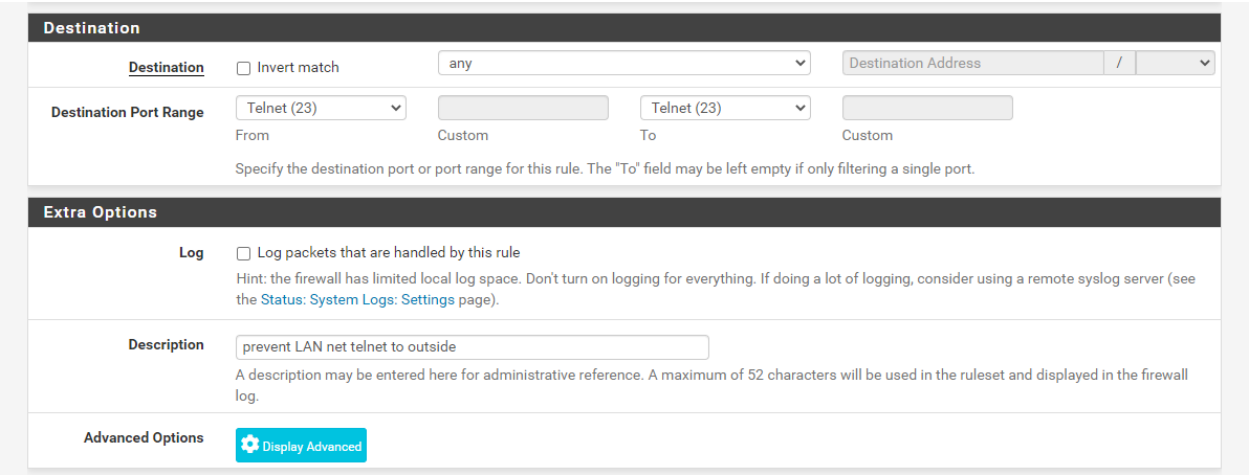
```
ubuntu_vm@ubuntuvm2:~$ telnet 192.168.182.129
Trying 192.168.182.129...
Connected to 192.168.182.129.
Escape character is '^]'.
Ubuntu 22.04.1 LTS
nbp-virtual-machine login:
```

Bắt đầu set rule chặn telnet từ mạng nội bộ tới máy B

Vào Firewall -> Rules -> Add



Làm giống như câu 2 nhưng sửa Destination Port Range thành Telnet(23)



Sau khi set rule, ta thử telnet lại tới máy B và thấy kết quả

```
ubuntu_vm@ubuntuvm2:~$ telnet 192.168.182.129
Trying 192.168.182.129...
```

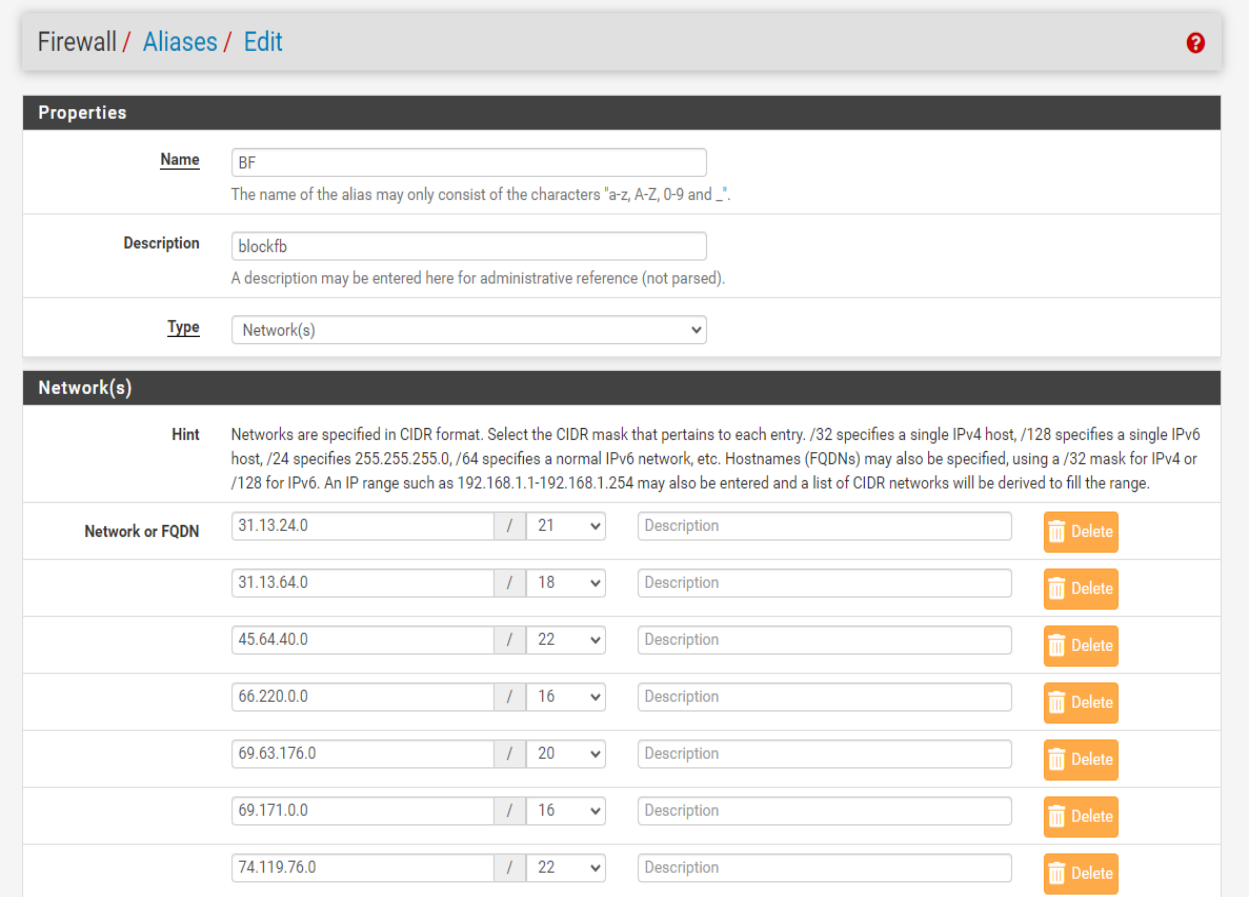
Câu 4. Không cho phép các máy trong mạng nội bộ truy cập đến www.facebook.com và youtube.com.

Chặn các máy nội bộ truy cập tới www.facebook.com
Trước khi block hết ip của facebook

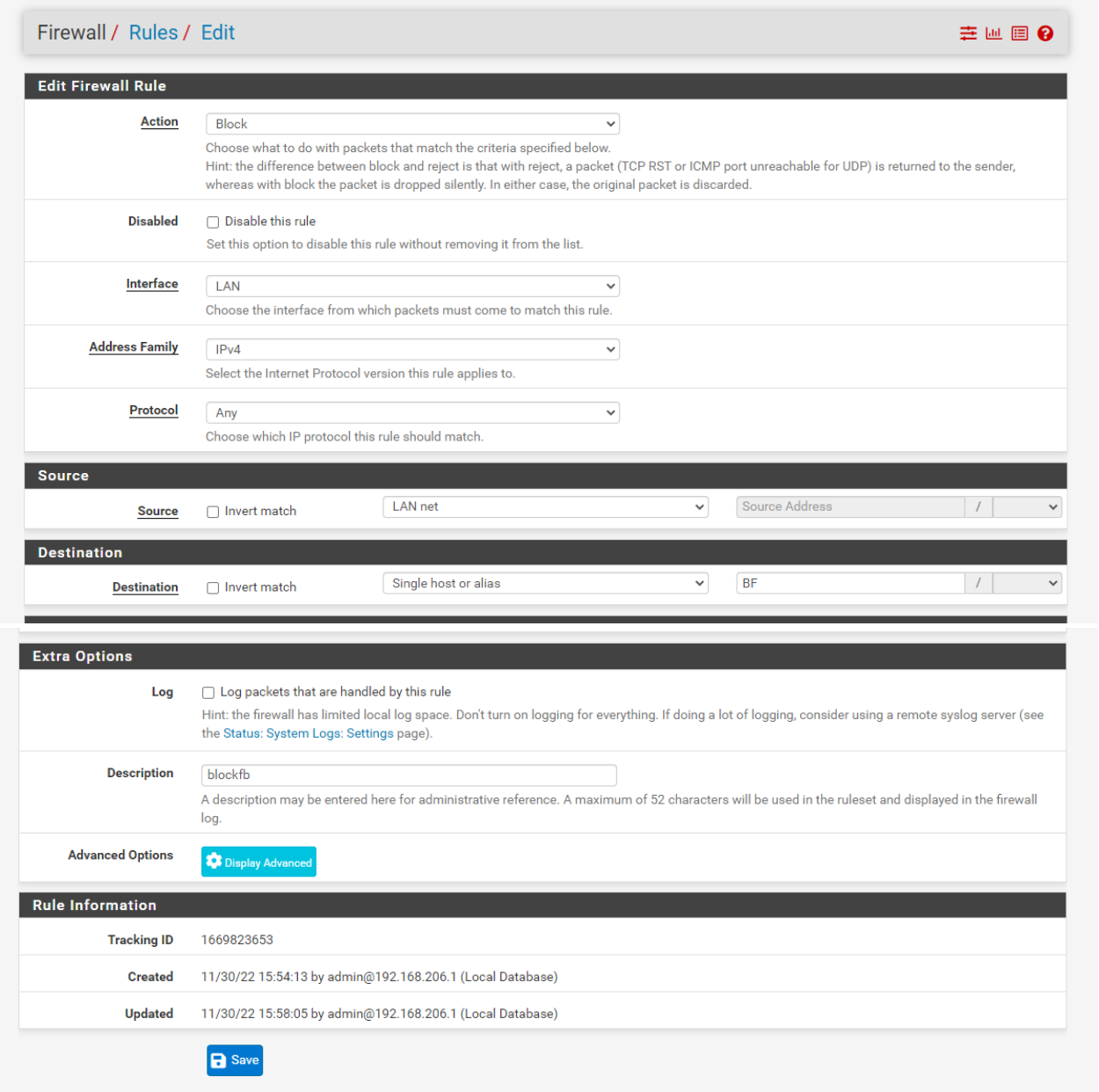
```
ubuntu_vm@ubuntuvm2:~$ ping www.facebook.com
PING star-mini.c10r.facebook.com (157.240.199.35) 56(84) bytes of data.
64 bytes from 157.240.199.35: icmp_seq=1 ttl=127 time=37.4 ms
64 bytes from edge-star-mini-shv-01-hkg4.facebook.com (157.240.199.35): icmp_seq=2 t
tl=127 time=36.1 ms
64 bytes from edge-star-mini-shv-01-hkg4.facebook.com (157.240.199.35): icmp_seq=3 t
tl=127 time=36.3 ms
64 bytes from edge-star-mini-shv-01-hkg4.facebook.com (157.240.199.35): icmp_seq=4 t
tl=127 time=35.5 ms
64 bytes from edge-star-mini-shv-01-hkg4.facebook.com (157.240.199.35): icmp_seq=5 t
tl=127 time=35.9 ms
64 bytes from edge-star-mini-shv-01-hkg4.facebook.com (157.240.199.35): icmp_seq=6 t
tl=127 time=35.6 ms
64 bytes from edge-star-mini-shv-01-hkg4.facebook.com (157.240.199.35): icmp_seq=7 t
tl=127 time=35.9 ms
64 bytes from edge-star-mini-shv-01-hkg4.facebook.com (157.240.199.35): icmp_seq=8 t
tl=127 time=35.6 ms
```

Trước tiên ta edit aliases:

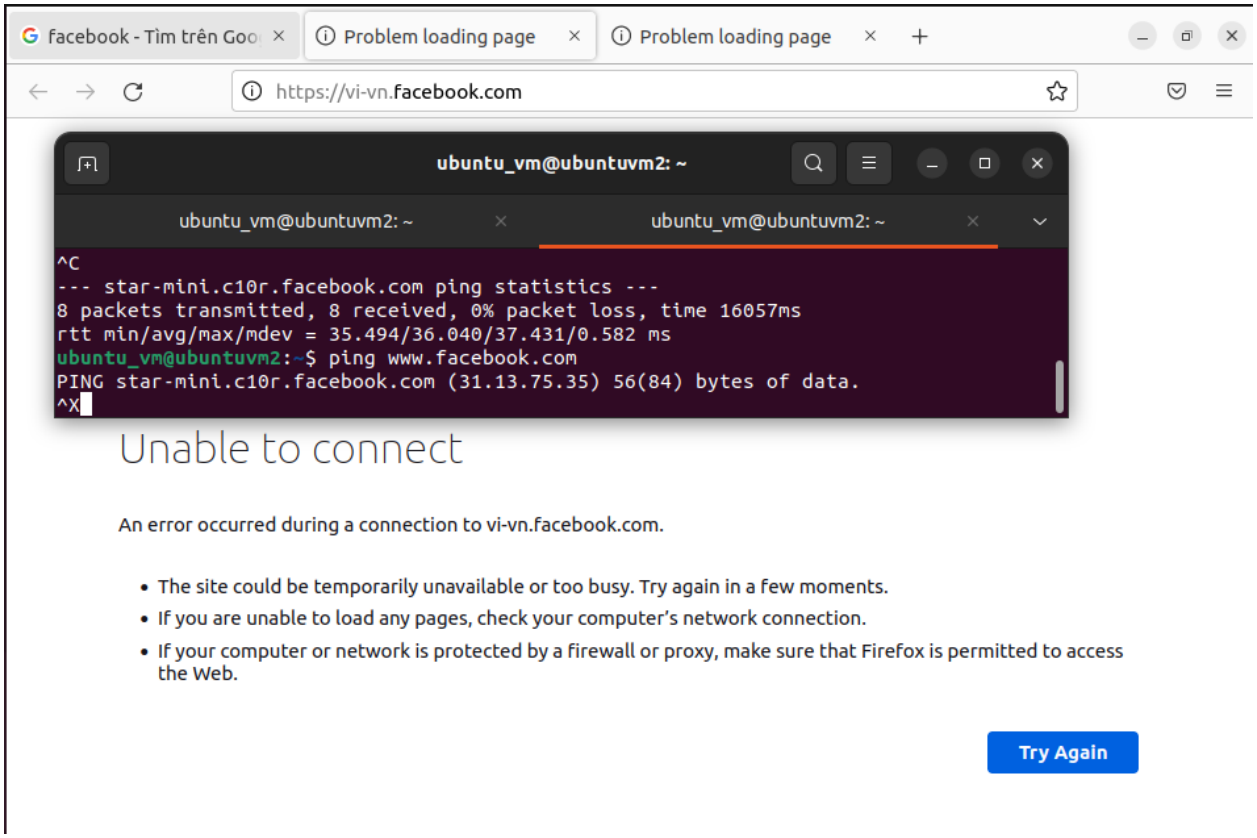
Tạo danh sách các IP của facebook với name là BF

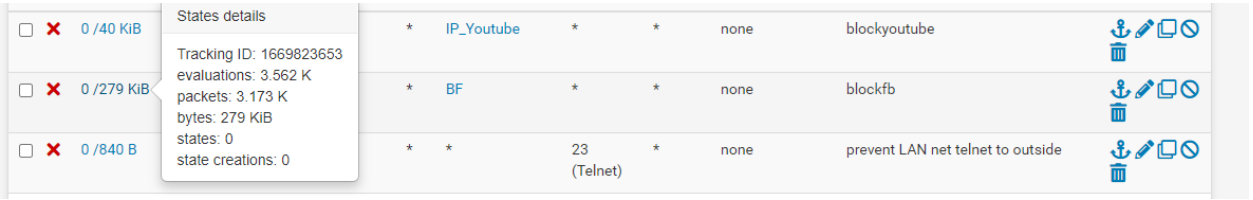


Sau đó ta sẽ cài rule



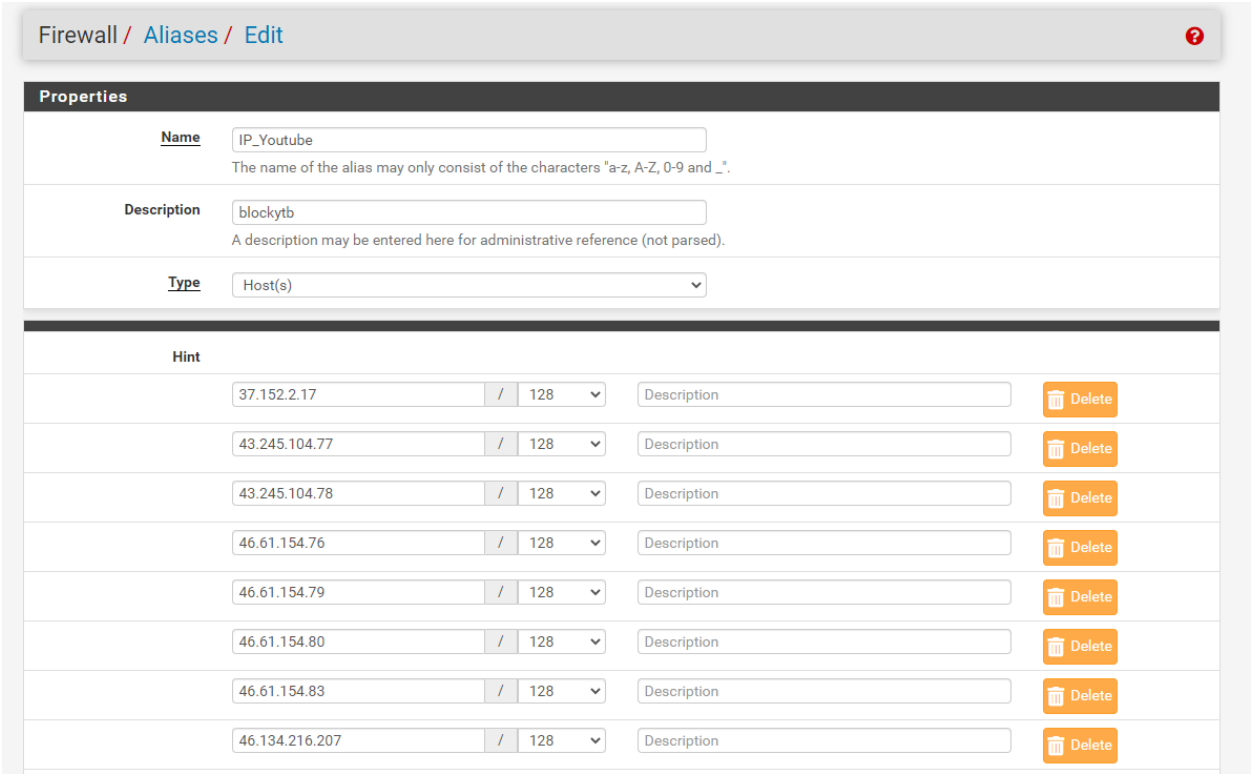
Sau khi block hết ip của facebook, ta vào lại để kiểm tra thì thấy thông báo “Unable to connect”,
ta không thể truy cập vào facebook, cũng không thể ping tới.



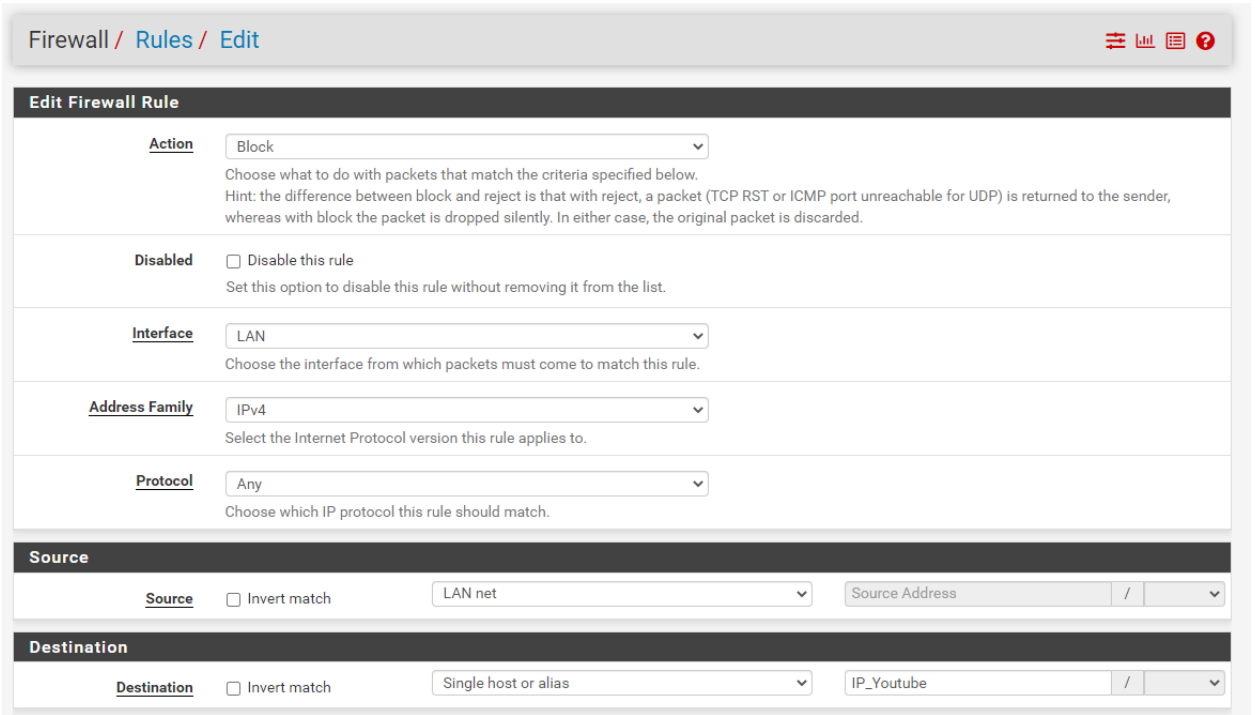


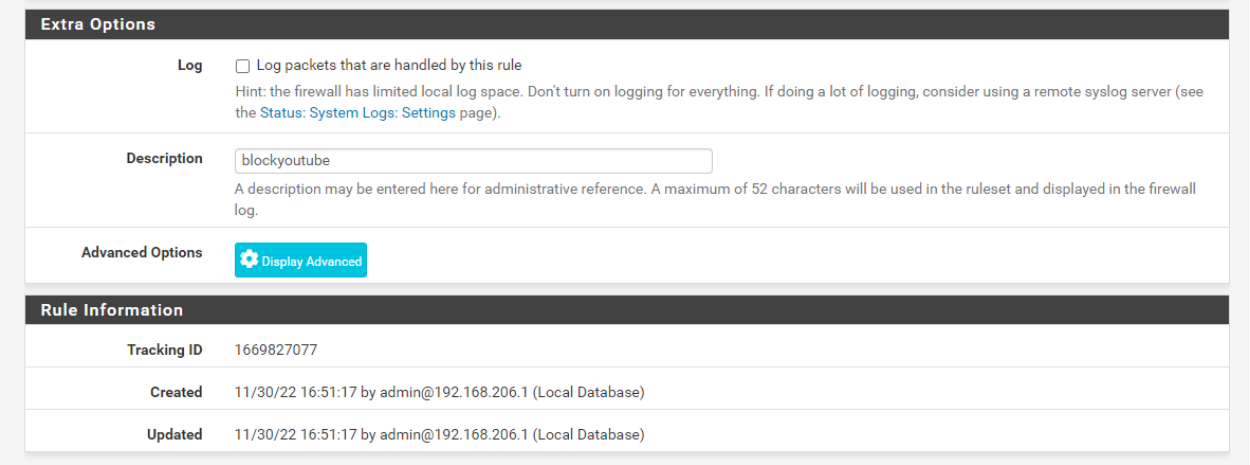
3173 gói tin từ fb đã bị chặn

Kế tiếp ta sẽ chặn các máy nội bộ truy cập tới youtube.com
Tạo danh sách IP của youtube

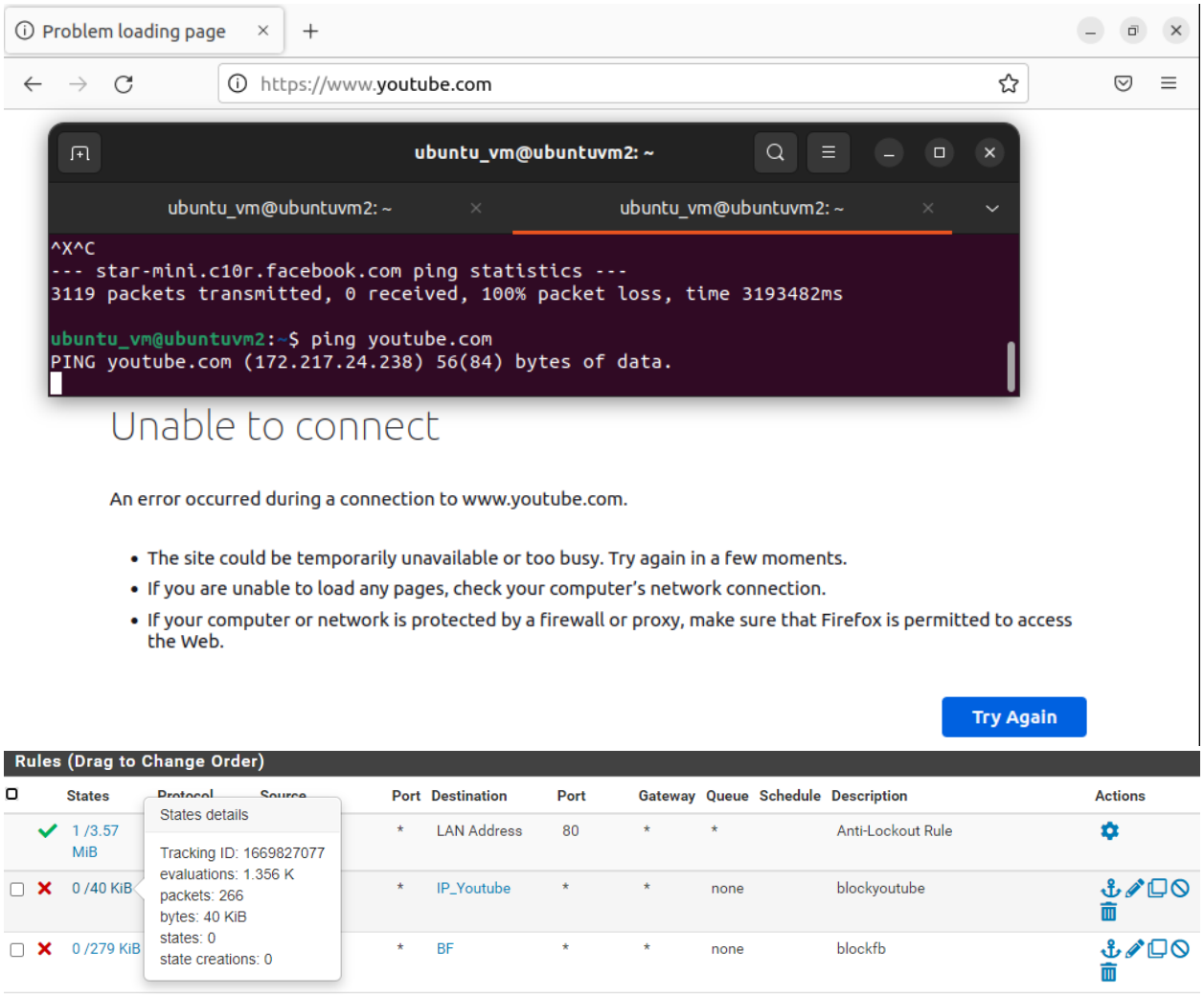


Cài rule chặn các IP của youtube





Sau khi set rule chặn, ta không thể truy cập vào youtube, cũng không thể ping tới.



266 gói tin từ youtube đã bị chặn

Vậy ta đã thành công chặn truy cập tới youtube và facebook

Bài tập về nhà

3. Vượt qua sự kiểm soát của firewall

a)Thực hiện telnet từ máy A tới máy B:
Trước tiên ta sẽ cài đăt ssh và telnet ở cả hai máy

```
ubuntu_vm@ubuntuvm2:~$ ssh -fN -L 8000:localhost:23 nbp@192.168.182.129
The authenticity of host '192.168.182.129 (192.168.182.129)' can't be establishe
d.
ED25519 key fingerprint is SHA256:2yPduADps22ahN1mENpz3uJMTXTLgq3LmDwr/M44dSg.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.182.129' (ED25519) to the list of known host
s.
nbp@192.168.182.129's password:
```

```
ubuntu_vm@ubuntuvm2:~$ telnet localhost 8000
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
Ubuntu 22.04.1 LTS
nbp-virtual-machine login: ubuntu
Password:

Login incorrect
nbp-virtual-machine login: nbp
Password:
Welcome to Ubuntu 22.04.1 LTS (GNU/Linux 5.15.0-53-generic x86_64)

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

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

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

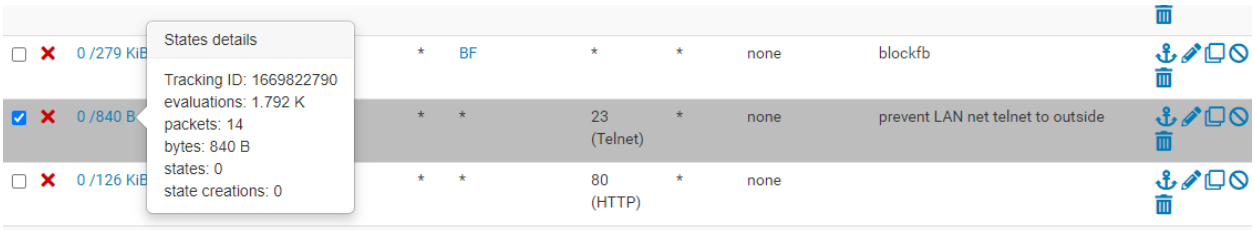
ssh -fN -L 8000:localhost:23 nbp@192.168.182.129

Giải thích câu lệnh:
-f : Để ssh chạy dưới nền trước khi thực thi câu lệnh
-N : Không thực thi lệnh remote
-L: Xác định tham số của bind address theo [port:host:hostport]

telnet localhost 8000
Kết nối tới cổng 8000 của localhost, do đã tạo tunnel của cổng 23 của máy A tới cổng 22 máy B nên lệnh này đã kết nối được tới 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 vẫn đi qua firewall, nhưng firewall không giữ lại vì không chặn cổng SSH Bởi vì do lệnh thiết lập ssh tunnel ở phía trên đã gắn tất cả kết nối ssh cổng 23 từ máy A tới máy B vào cổng 8000, khi ta dùng lệnh này chính là đang telnet thông qua một kết nối ssh. Vậy nên khi gói tin đi qua firewall, nó chỉ thấy kết nối ssh từ cổng 8000 của máy A tới cổng 22 (SSH) của máy B.

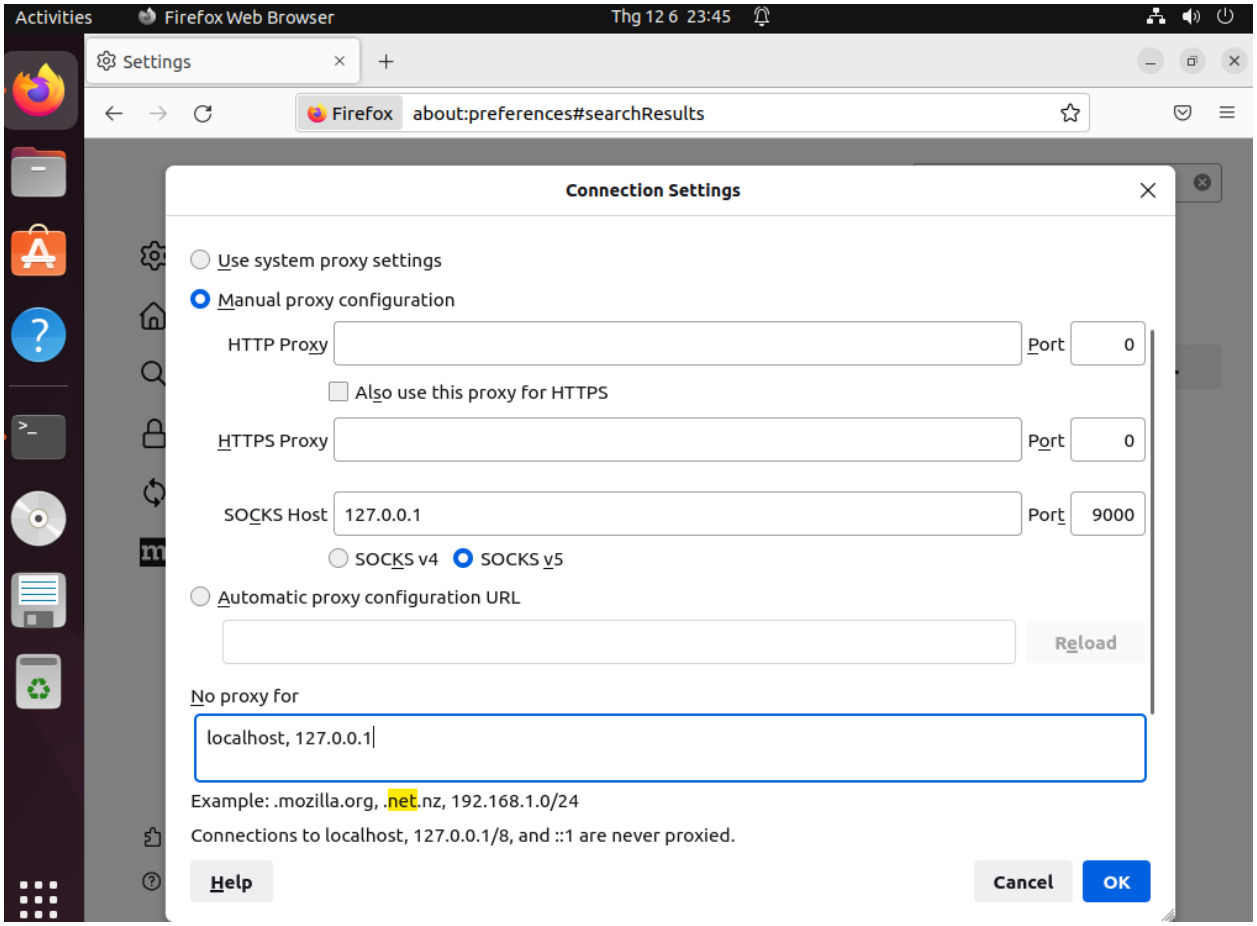
b) Kết nối tới facebook sử dụng ssh tunnel
Ta dùng lệnh ps aux | grep 8000 để xem thông tin các tiến trình đang chạy ở cổng 8000
Dùng lệnh kill -9 <pid> để tắt tiến trình ở pid

```
ubuntu_vm@ubuntuvm2:~$ ps aux | grep 8000
ubuntu_+    3568  0.0  0.2  28444  4828 ?        Ss   21:03   0:00 ssh -fN -L 8000:localhost:
23 nbp@192.168.182.129
ubuntu_+    3570  0.0  0.2  28448  4088 ?        Ss   21:03   0:00 ssh -fN -L 8000:localhost:
23 nbp@192.168.182.129
ubuntu_+    3682  0.0  0.1  20740  2548 pts/0    S+   21:21   0:00 grep --color=auto 8000
ubuntu_vm@ubuntuvm2:~$ kill -9 3568
ubuntu_vm@ubuntuvm2:~$ kill -9 3570
ubuntu_vm@ubuntuvm2:~$ ps aux | grep 8000
ubuntu_+    3688  0.0  0.1  20740  2588 pts/0    S+   21:22   0:00 grep --color=auto 8000
```

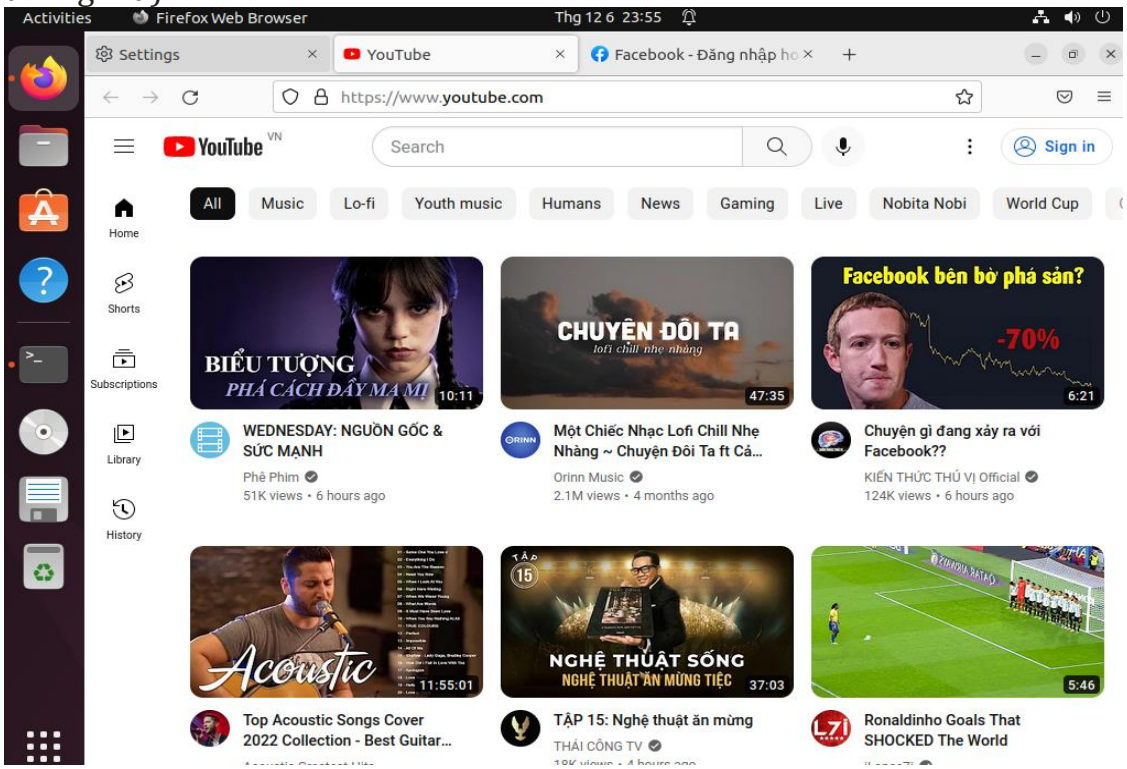
Ta thiết lập ssh tunnel mới

```
ubuntu_vm@ubuntuvm2:~$ ssh -D 9000 -C nbp@192.168.182.129
nbp@192.168.182.129's password:
Welcome to Ubuntu 22.04.1 LTS (GNU/Linux 5.15.0-53-generic x86_64)

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

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

Last login: Tue Dec  6 21:04:14 2022 from localhost
```

Chỉnh lại proxy của firefox theo yêu cầu của bài

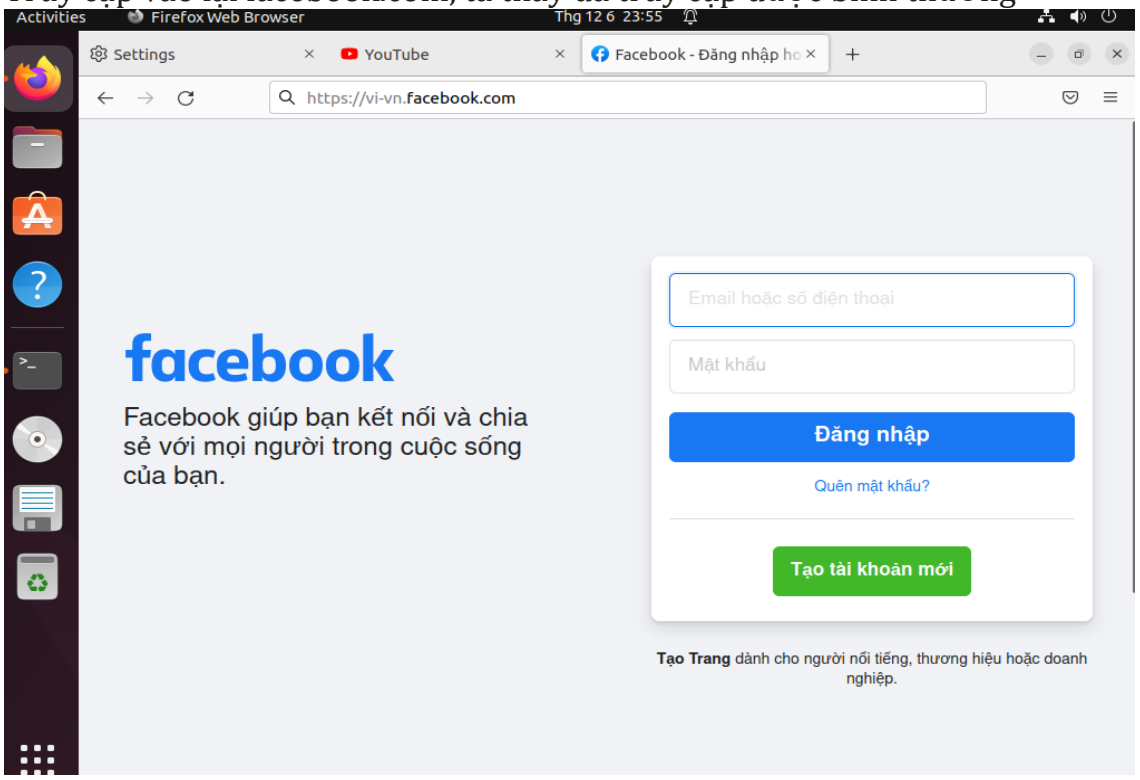


Ta truy cập vào thử youtube thì thấy đã truy cập lại bình thường (thành công đi qua tường lửa)



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

Truy cập vào lại facebook.com, ta thấy đã truy cập được bình thường



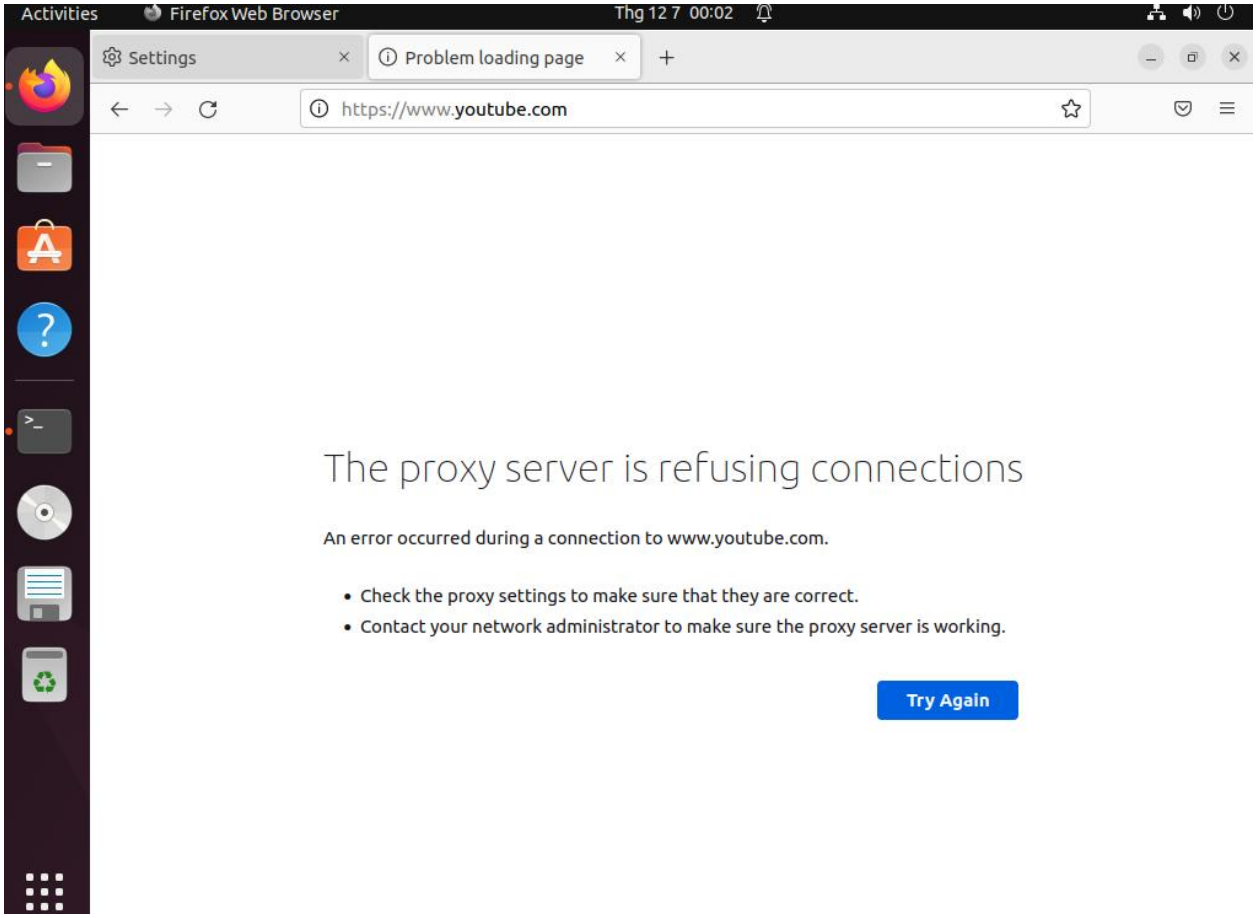
Truy cập vào facebook.com và lướt một lúc, vào lại pfSense thì ta thấy vẫn có gói tin đi qua, vậy ta đã thiết lập tunnel thành công.

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?

Ta ngắt tunnel và kiểm tra lại

```
^Cubuntu_vm@ubuntuvm2:~ps aux | grep 9000
ubuntu_+    5763  0.0  0.1  20740  2432 pts/0    S+   00:01   0:00 grep --color=aut
o 9000
```

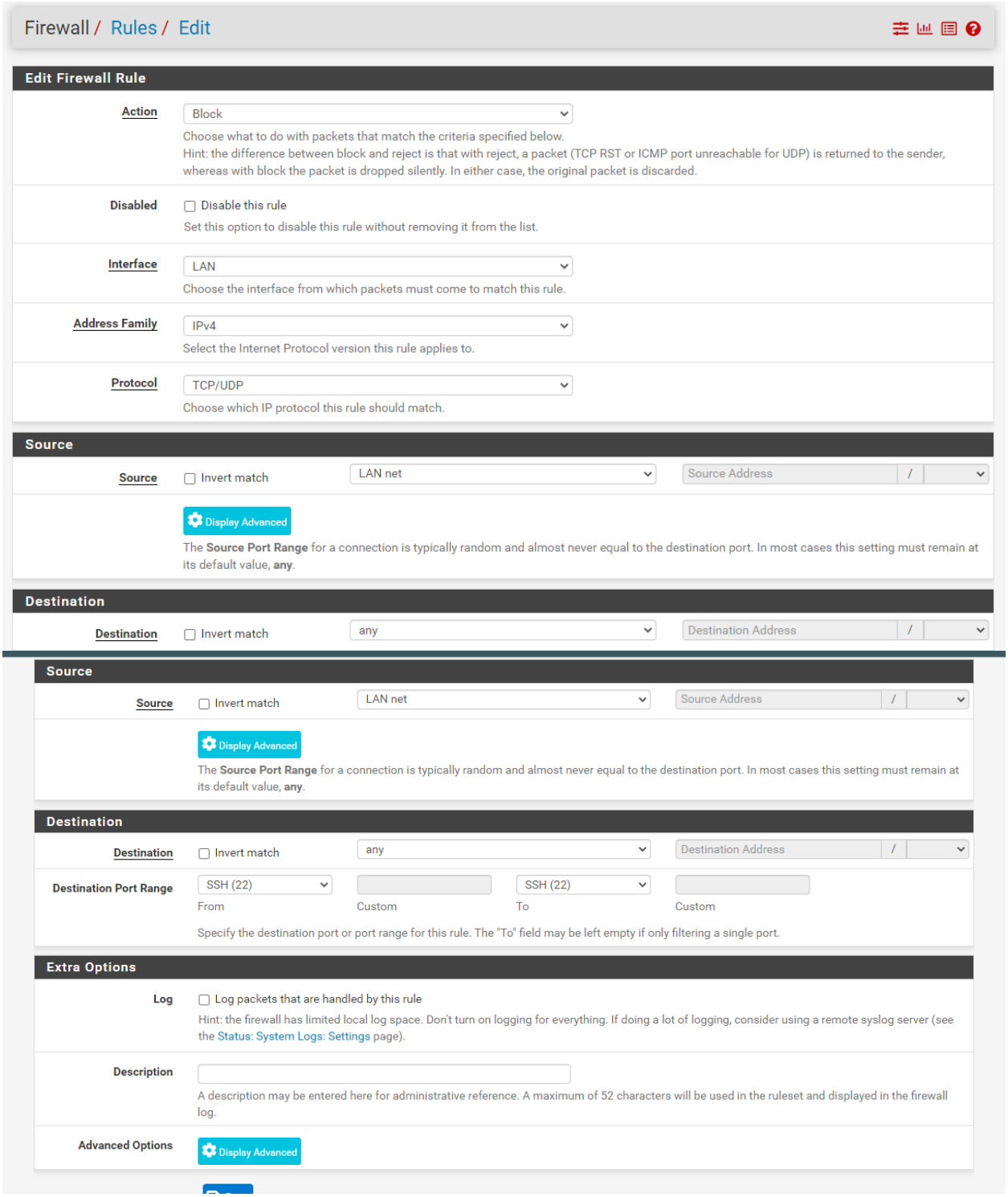
Xóa cache trên trình duyệt



=> Ta thấy đã không thể kết nối được tới www.facebook.com

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?

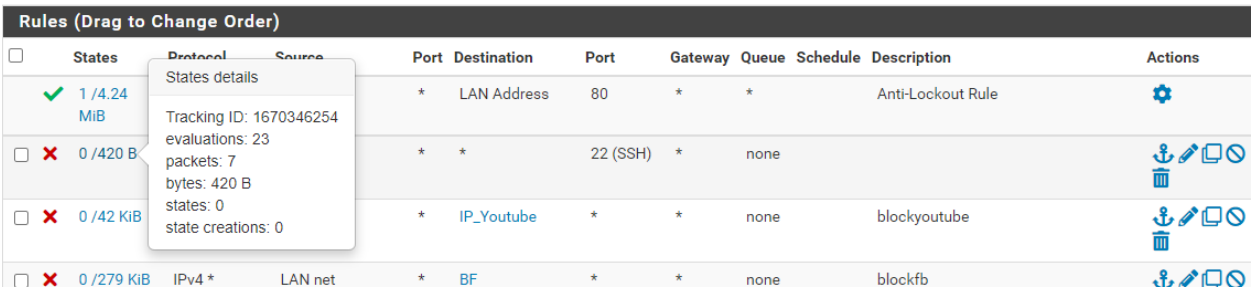
Bước đầu, ta sẽ set rule chặn mạng nội bộ tới port SSH(22)



Ta thực hiện thiết lập tunnel lại thì thấy không thành công

```
ubuntu_vm@ubuntuvm2:~$ ssh -D 9000 -C nbp@192.168.182.129
ssh: connect to host 192.168.182.129 port 22: Connection timed out
```

Vào pfSense kiểm tra thì phát hiện rule ta vừa thiết lập ở phía trên đã chặn được 7 gói tin



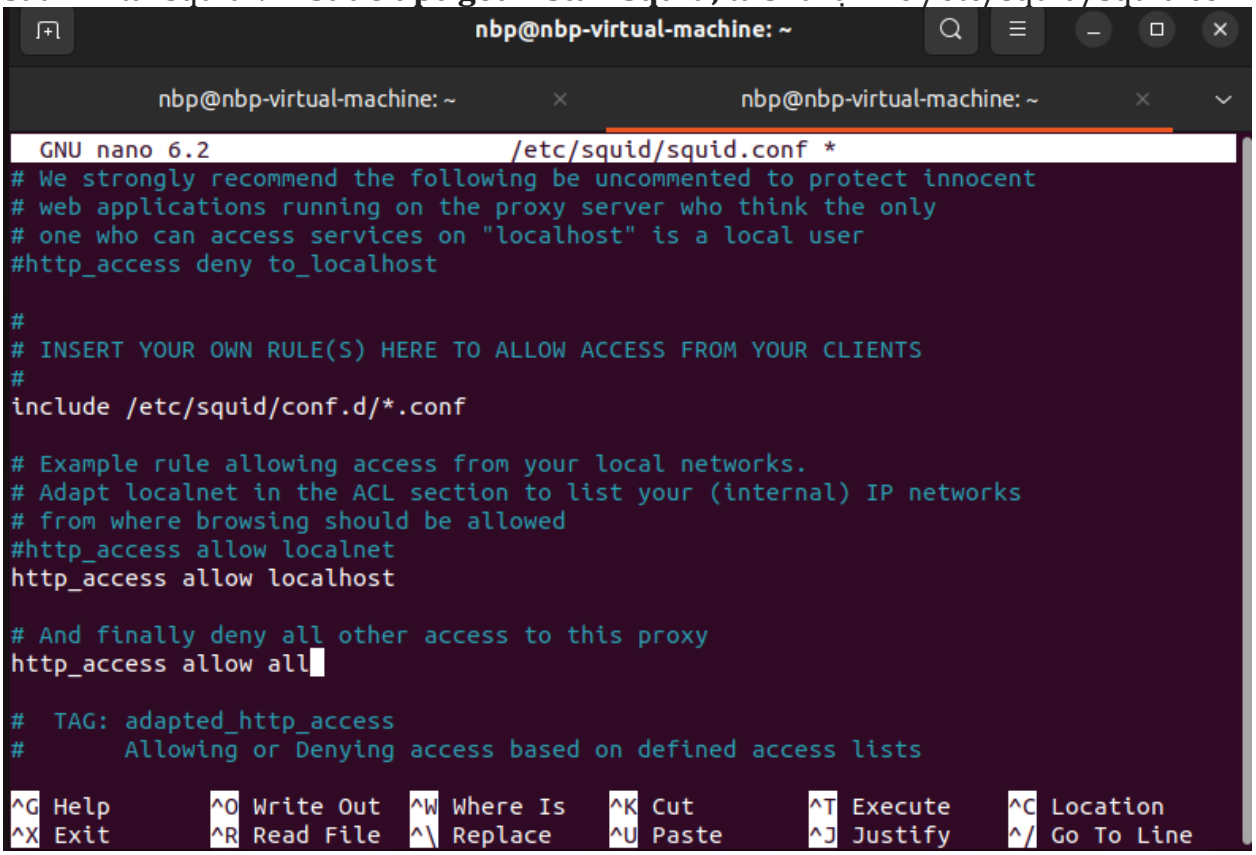
=> Lệnh thiết lập ssh tunnel sẽ giúp ta kết nối A đến B rồi ra Internet qua tunnel ssh, nên khi chặn port ssh, thì ta không thể thiết lập ssh tunnel

Câu 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.
Theo em thì ta nên chặn port SSH để tránh tình trạng SSH tunnel.

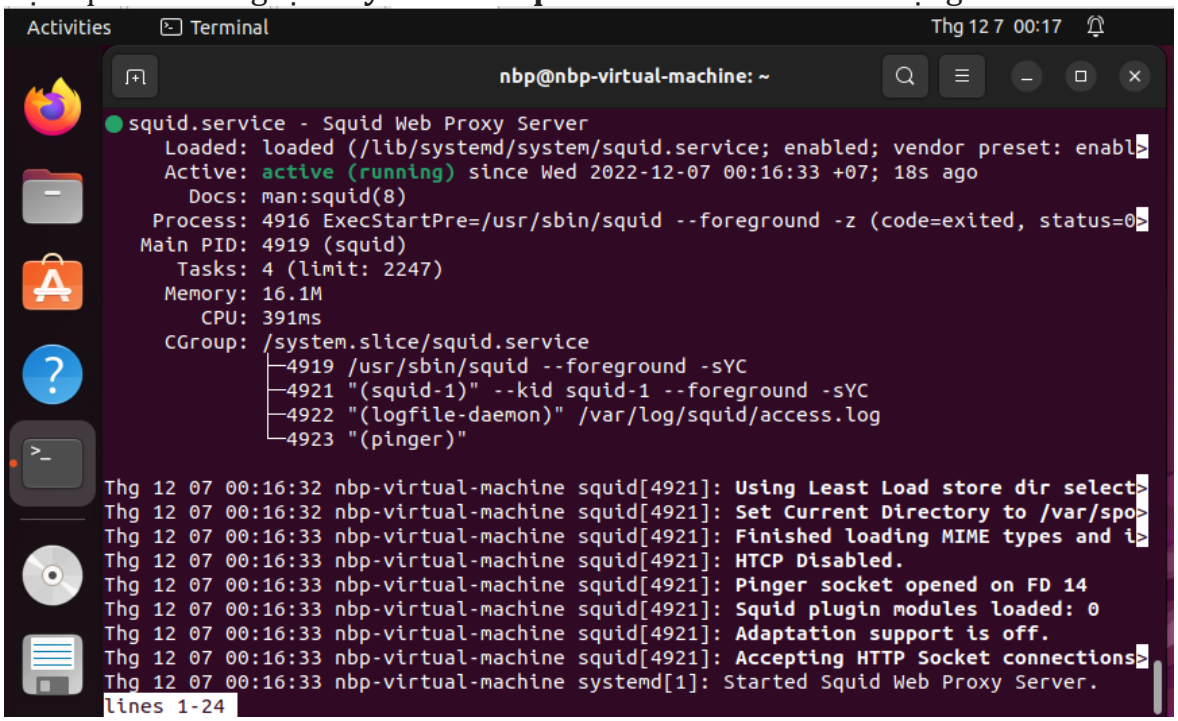
4. Triển khai web proxy

a)Cài dặt và thiết lập cấu hình squid

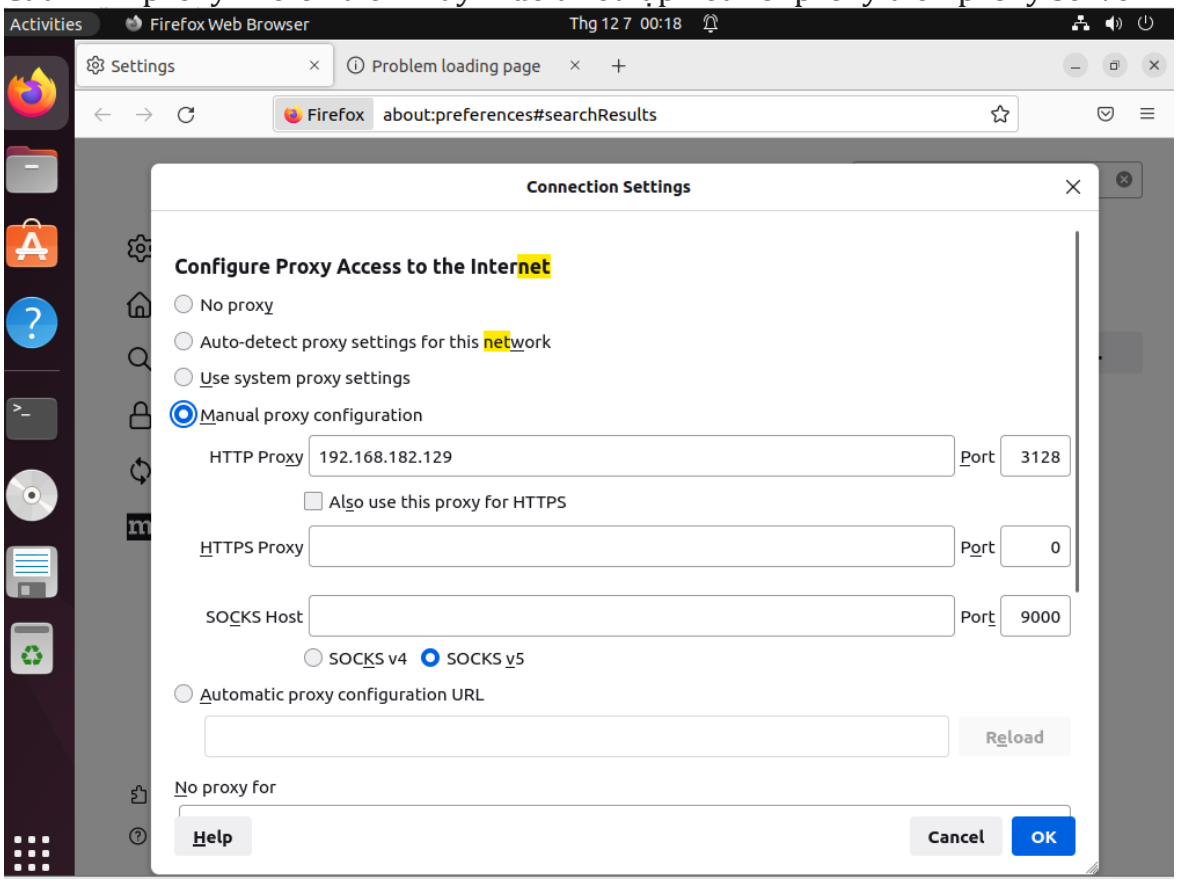
Sau khi tải squid với **sudo apt-get install squid,** ta sửa lại file /etc/squid/squid.conf



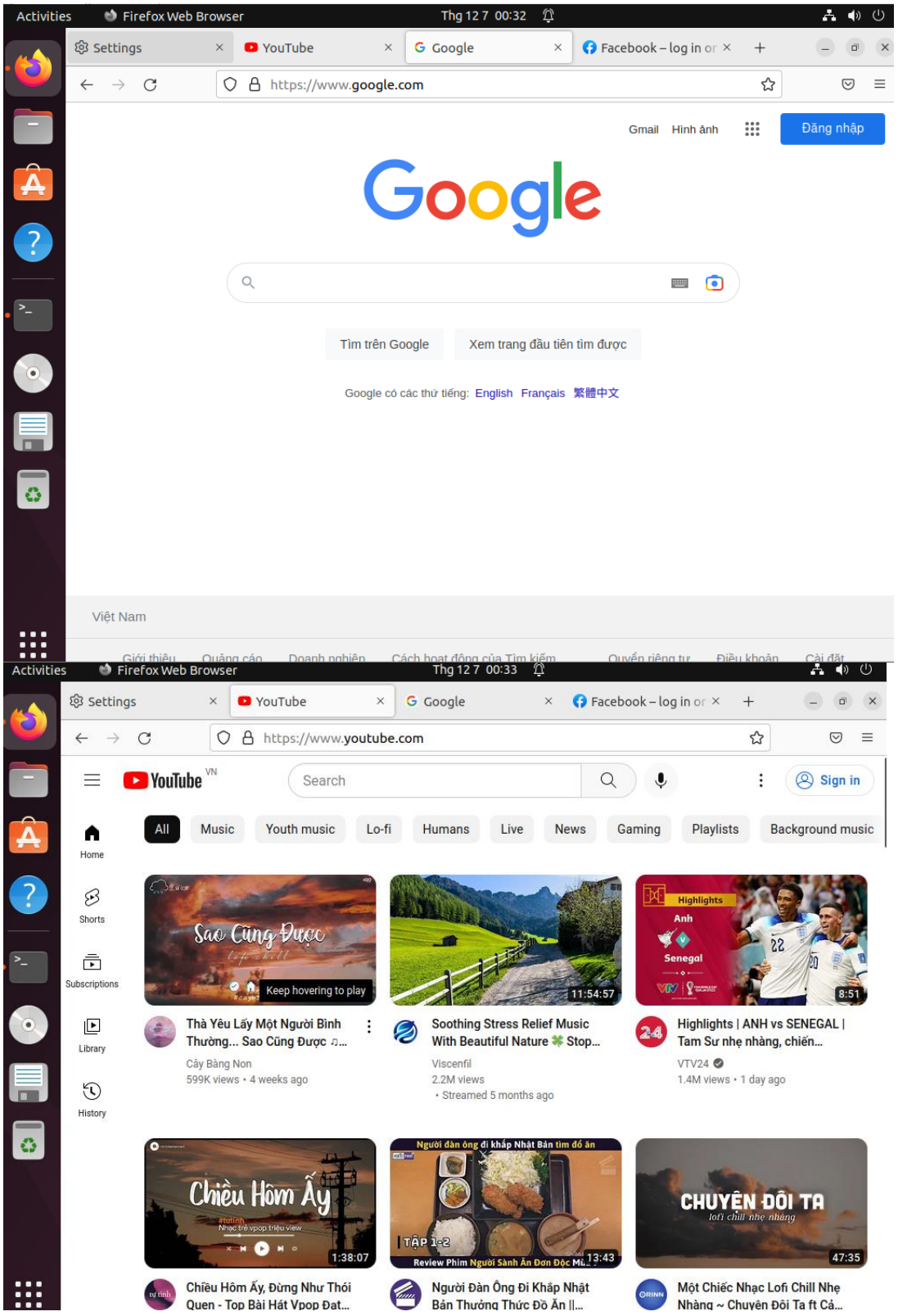
Bật squid và dùng lệnh **systemctl squid status** để kiểm tra trạng thái



Cấu hình proxy firefox trên máy A để thiết lập kết nối proxy trên proxy server máy B

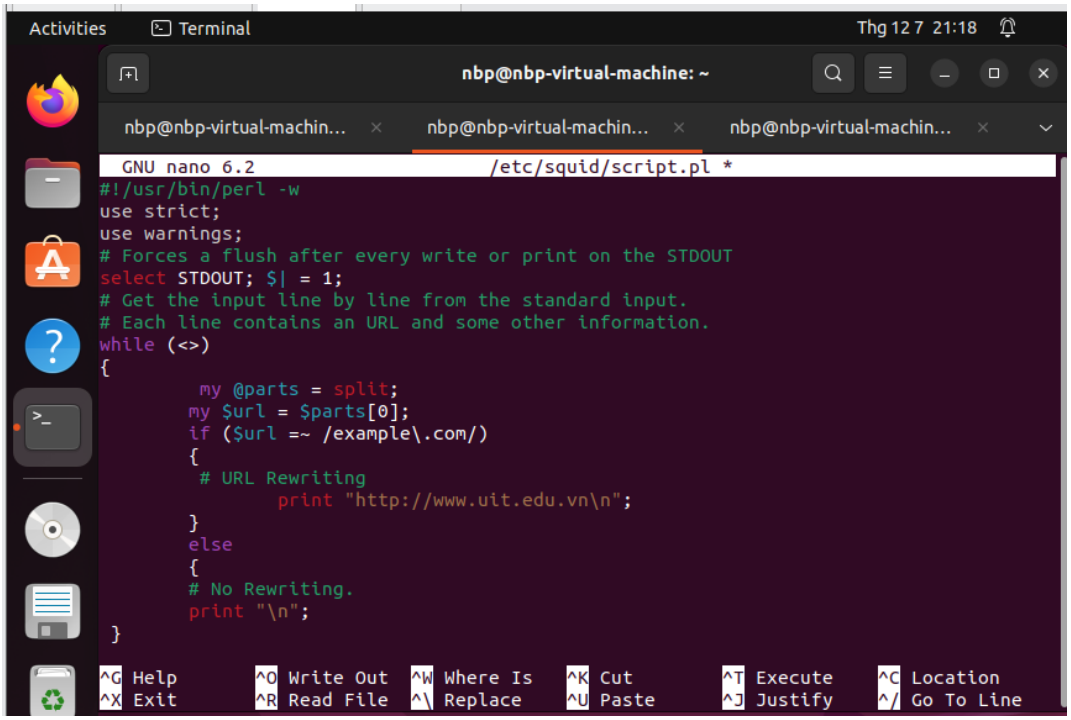


Ta thành công truy cập vào google, youtube trên máy A qua proxy server.

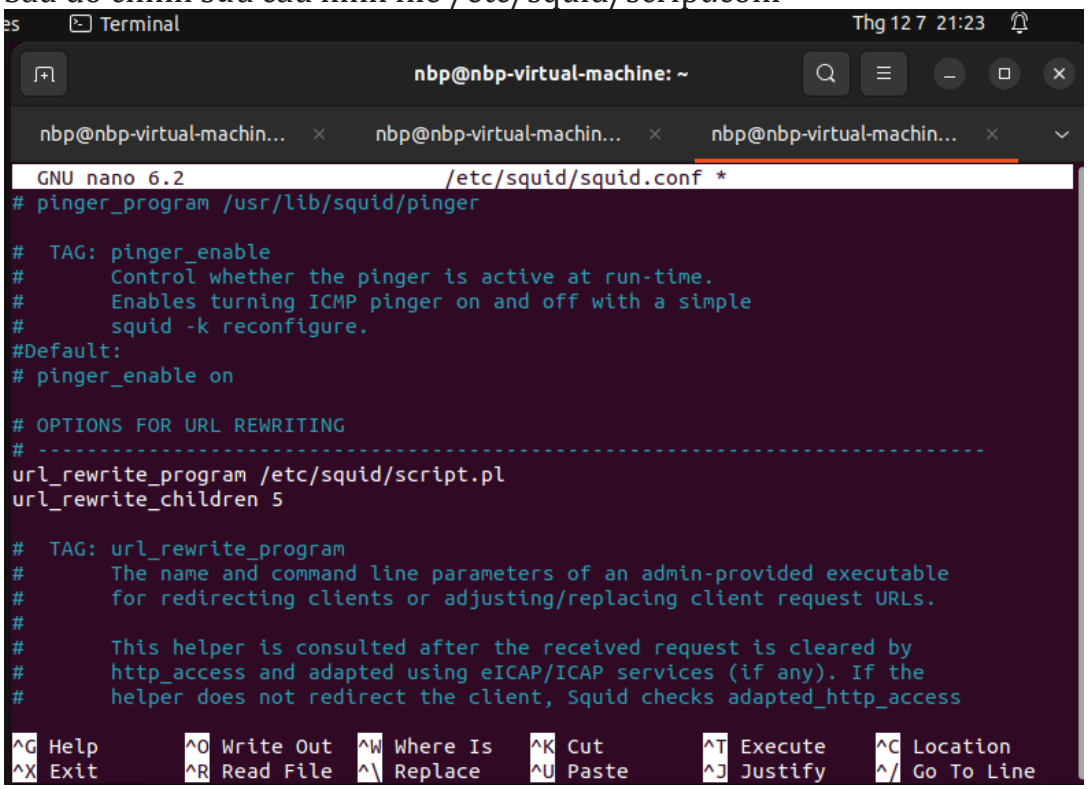


b) Thiết lập chuyển hướng

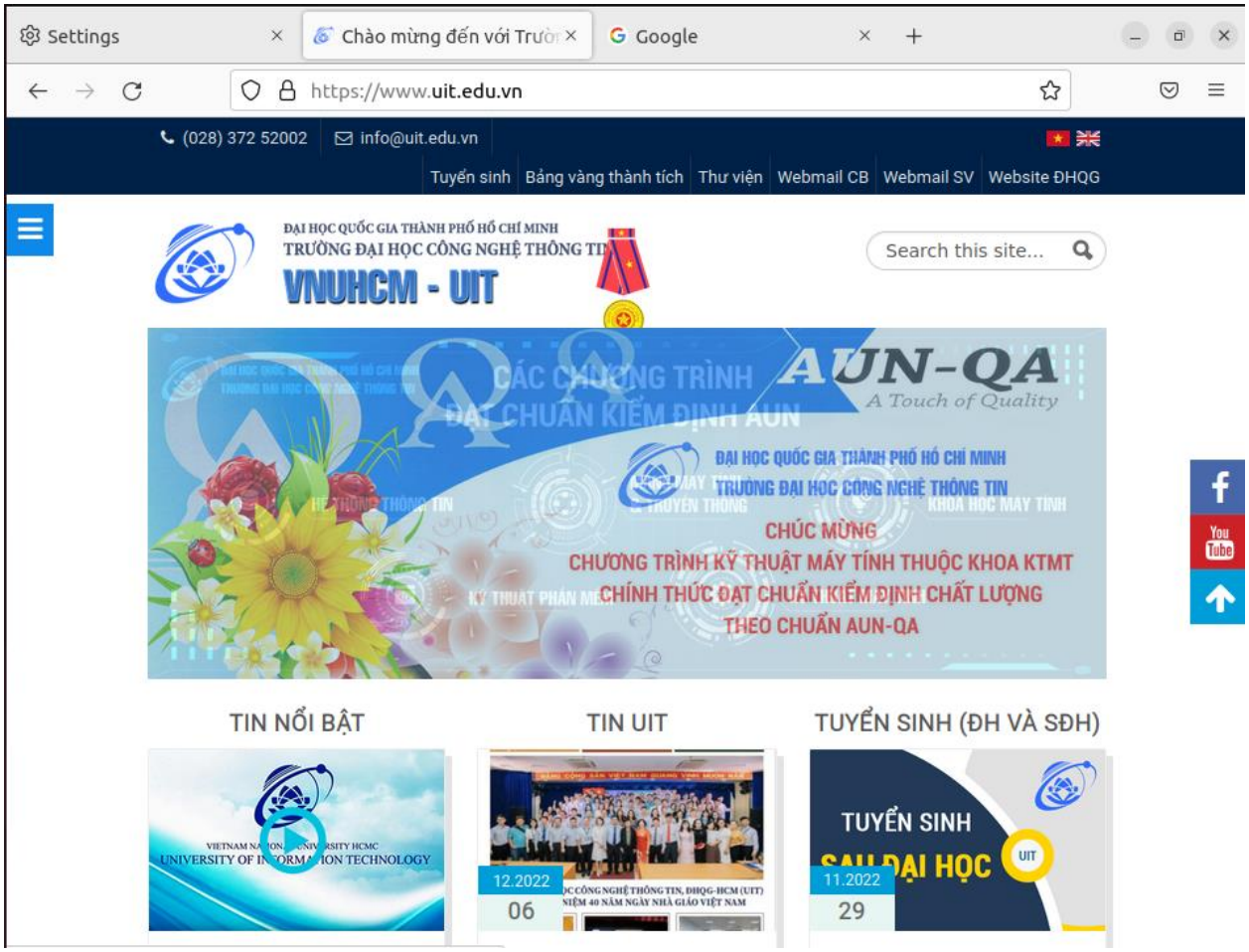
Ta tạo file /etc/squid/script.pl với nội dung từ đề



Sau đó chỉnh sửa cấu hình file /etc/squid/script.conf



Truy cập vào http://example.com, ta thấy kết quả là trang tự điều hướng qua uit.edu.vn



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

Đoạn trên của chương trình là khai báo 2 thư viện **strict** và **warnings**
Dùng **strict** để hạn chế các cấu trúc không an toàn, **warnings** cảnh báo chúng ta nếu chúng ta gõ sai.
Kế đó với mỗi stdout, output sẽ được flush

```
#!/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";
   }
}
```

Khi ta truy cập vào một trang web, vòng lặp while này sẽ chia nhỏ từng phần của request và viết lại url "example.com" để chuyển hướng tới trang "uit.edu.vn", nếu không phải url "example.com" thì vẫn tới trang web gốc

Câu 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).

Câu 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).

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

PfSense hỗ trợ các giao thức thiết lập kết nối VPN: IPSec, OpenVPN, L2PP, PPTP

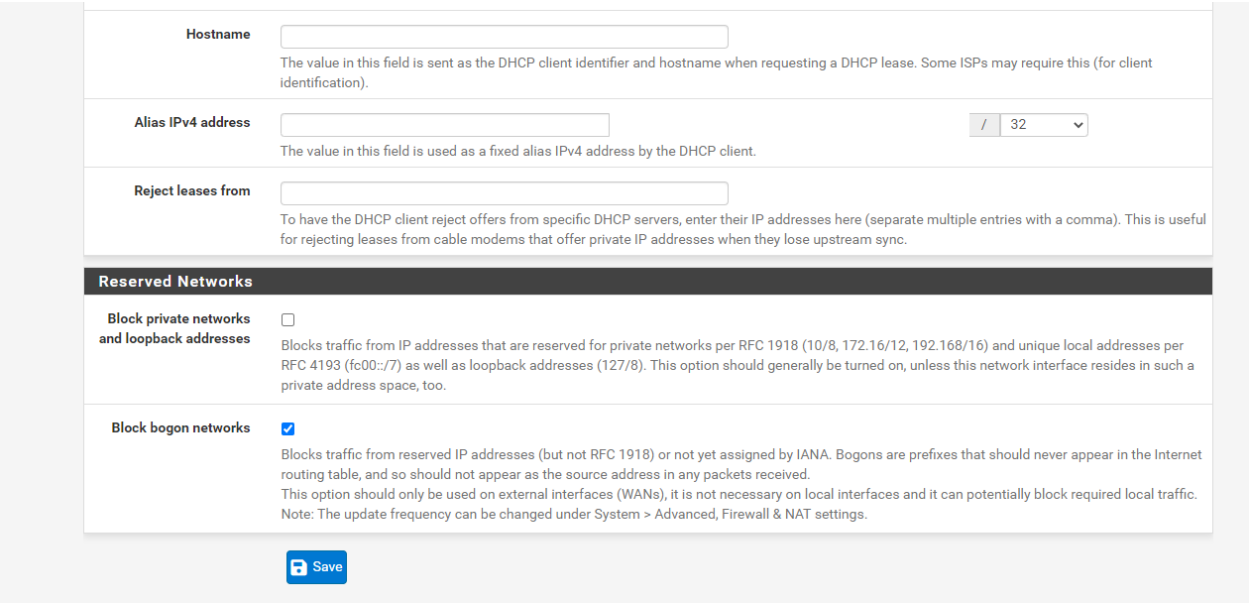
	Ưu điểm	Nhược điểm

IPSec	- Được đánh giá là bảo mật. - Cài đặt sẵn trên tất cả OS và thiết bị gần đây. - Thiết lập dễ dàng.	- Chậm hơn so với OpenVN - Có thể bị mở khóa bởi NSA. - Có thể có vấn đề nếu được sử dụng với các tường lửa. - Khả năng NSA đã cố tình làm suy yếu giao thức.
PPTP	- Nhanh - Phần mềm trạm máy trên nhiều hệ điều hành - Thiết lập cấu hình dễ	- Đã bị bẻ khóa bởi NSA - Không hoàn toàn bảo mật
OpenVPN	- Khả năng vượt hầu hết các firewall - Tùy chỉnh cao - Do là phần mềm mã nguồn mở nên có thể dùng để phòng hờ - Tương thích với nhiều thuật toán mã hóa - Bảo mật cao	- Thiết lập khó - Cần thêm phần mềm thứ ba

Câu 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.

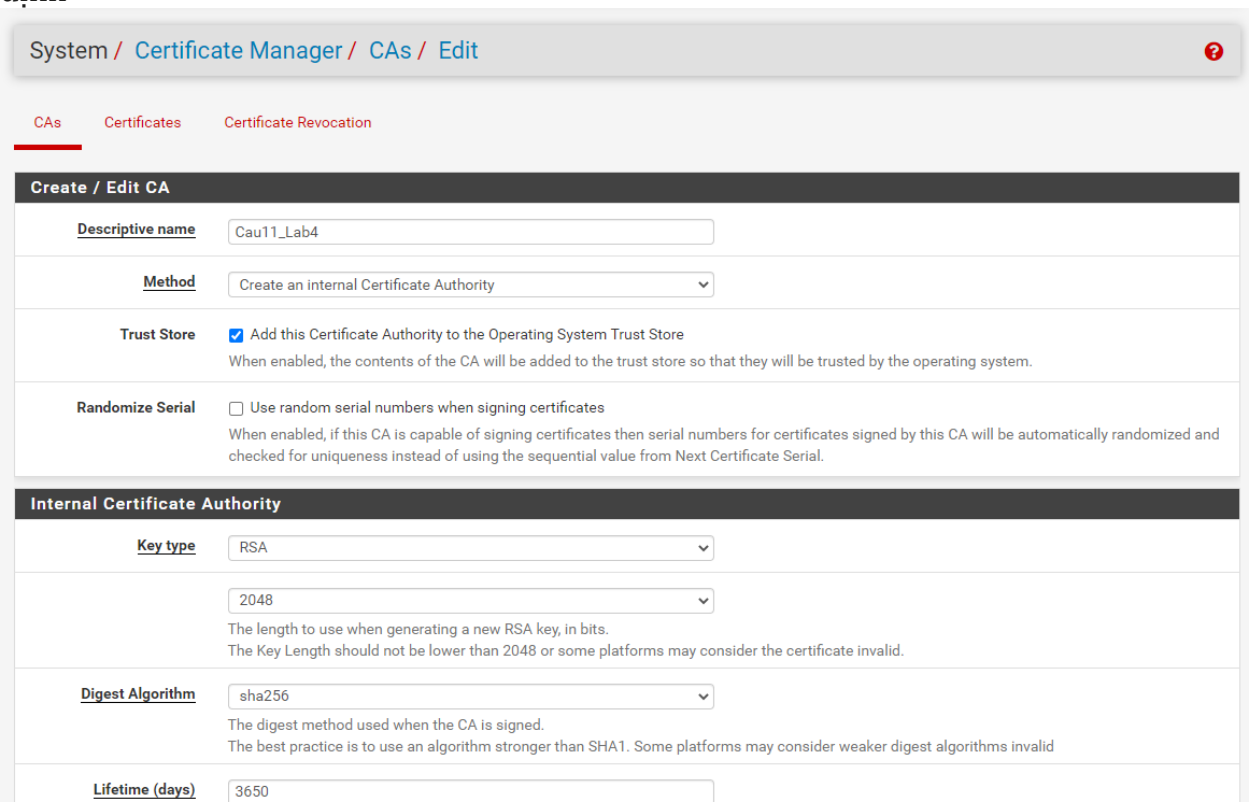
Ba bước chính để cấu hình OpenVPN trên pfsense
- Tạo hạ tầng khóa công khai (PKI Infrastructure)
- Cấu hình OpenVPN trên PFSense
- Cấu hình quyền truy cập của client

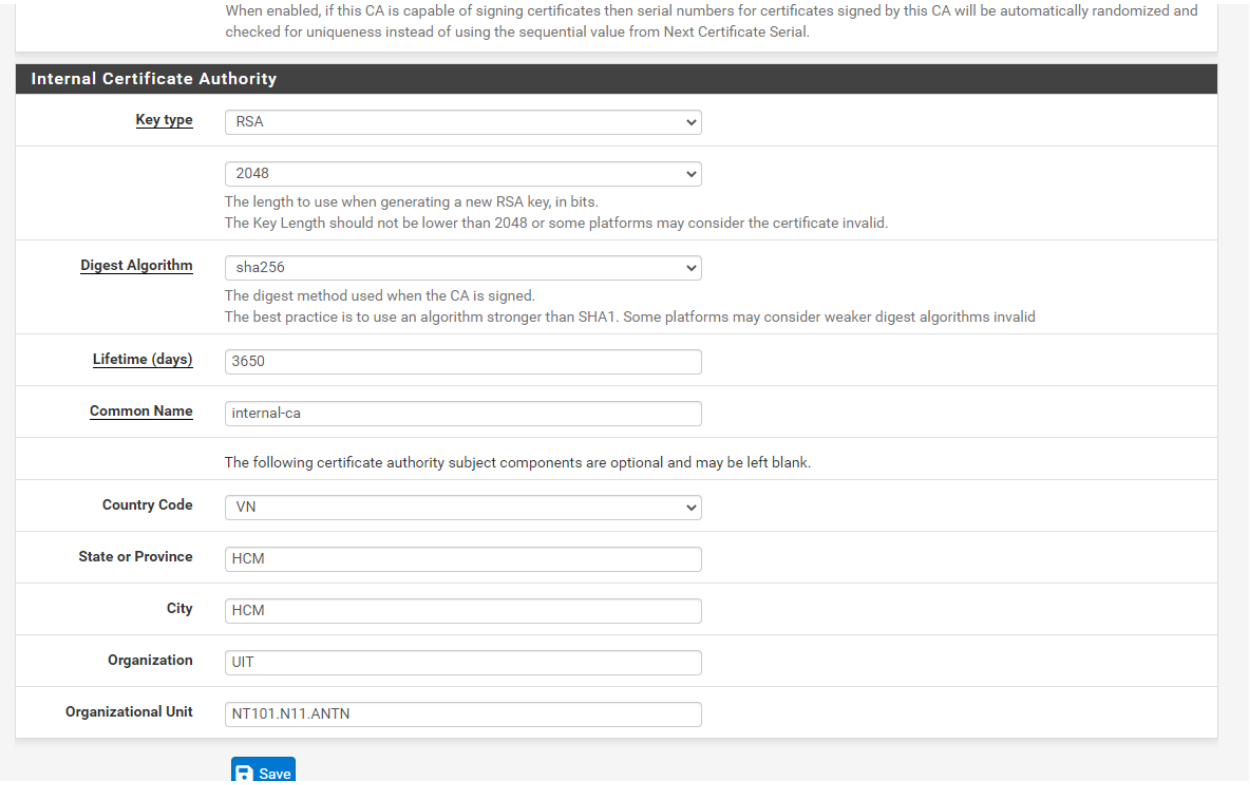
Trước hết vào Interface -> WAN và tắt tính năng “Block private networks and loopback addresses” để có thể ping tới WAN interface



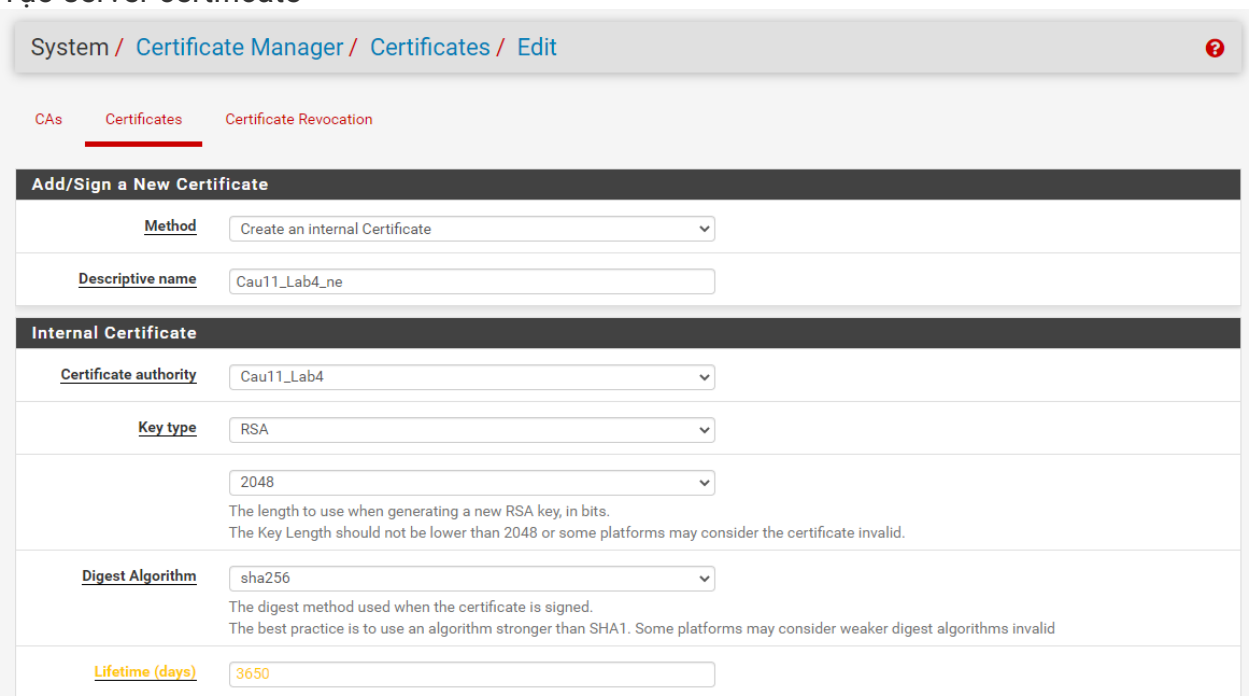
Bước 1: Tạo hạ tầng khóa công khai PKI

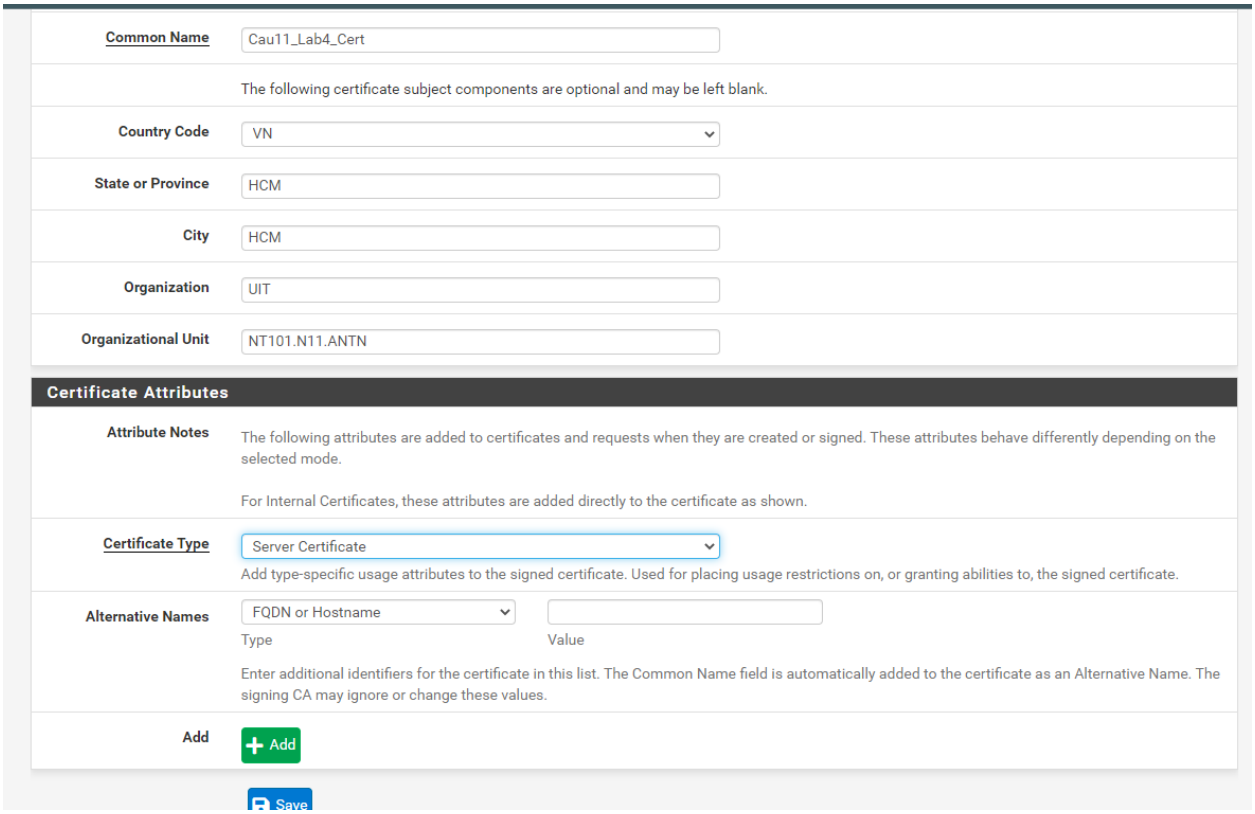
Tạo CA trên pfSense, tại đây ta cần điền method và name, còn lại có thể để như mặc định

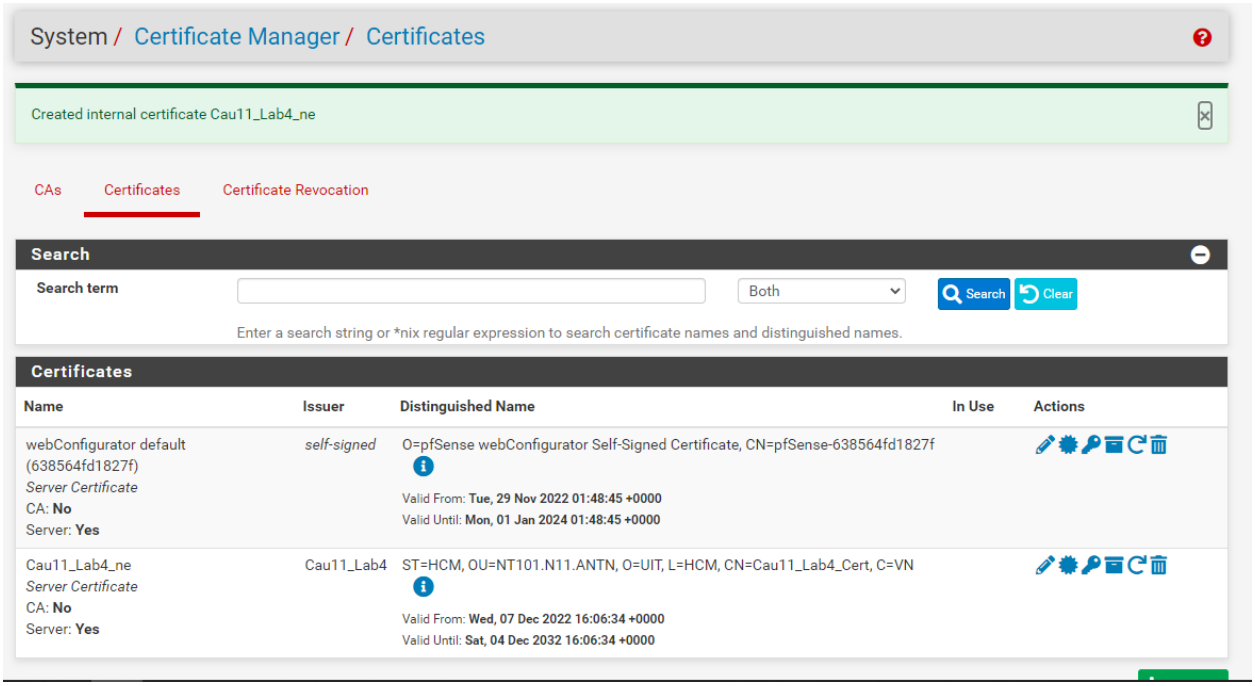




Tạo server certificate



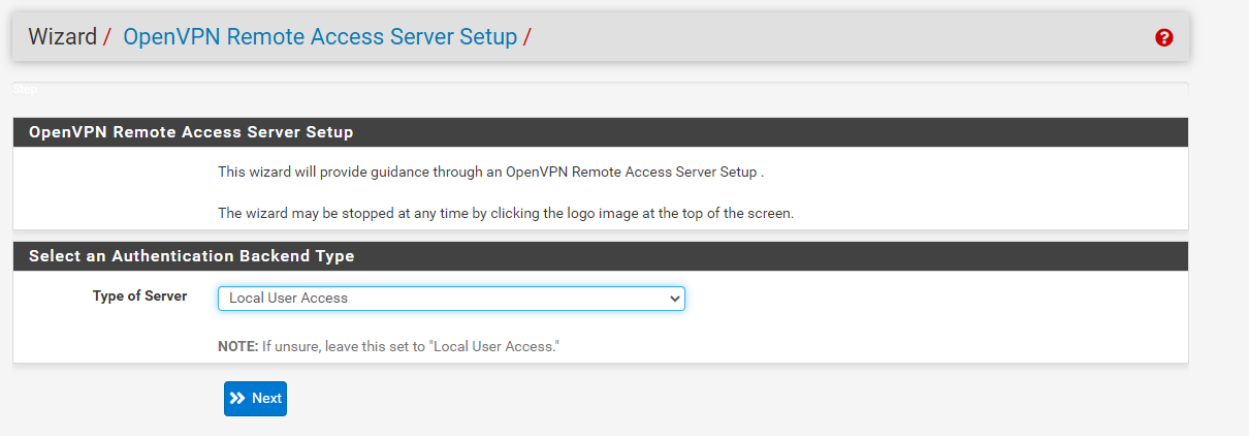




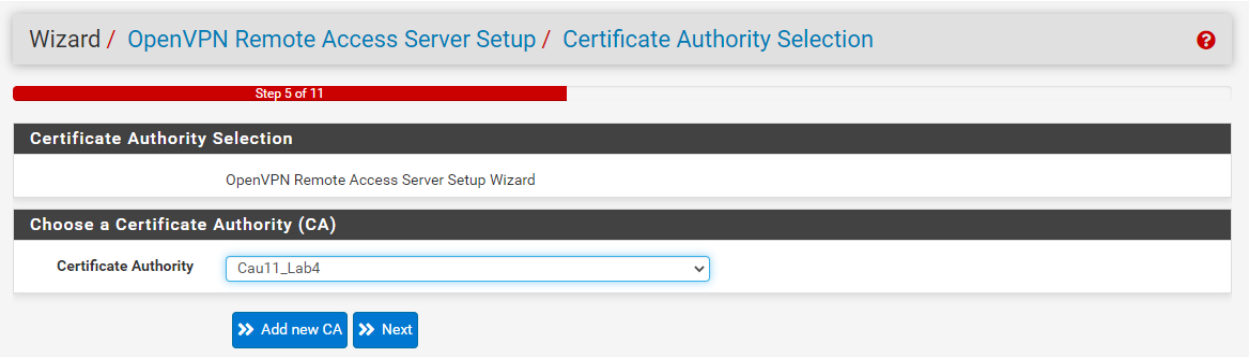
=> Hoàn thành tạo hạ tầng khóa công khai PKI

Bước 2: Cấu hình OpenVPN

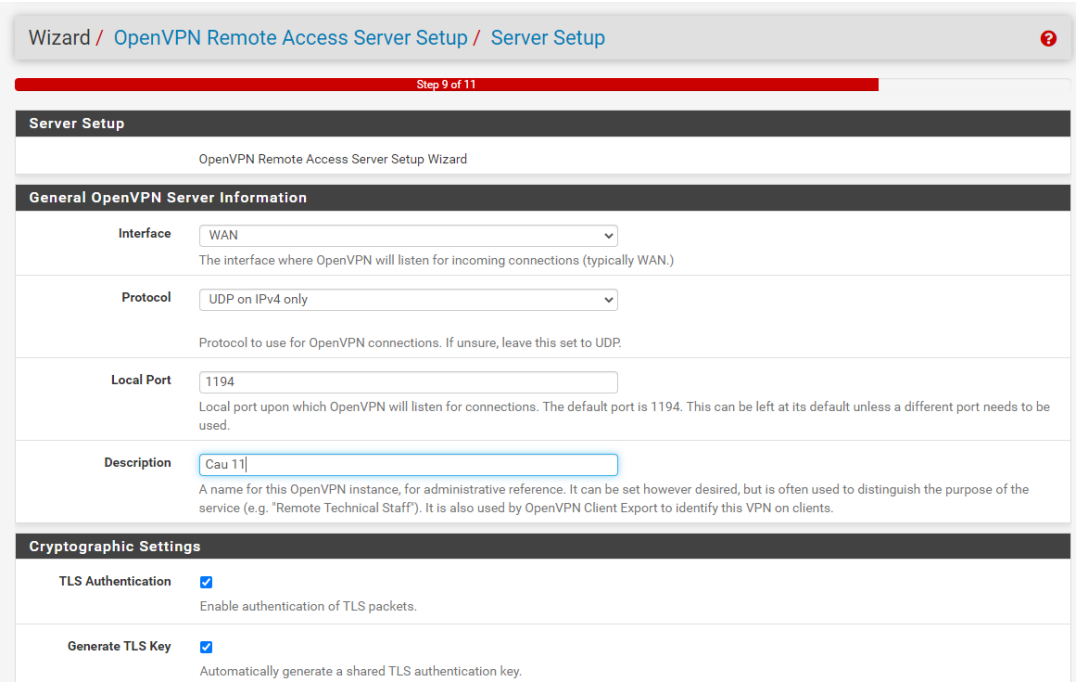
VPN -> OpenVPN -> Wizard

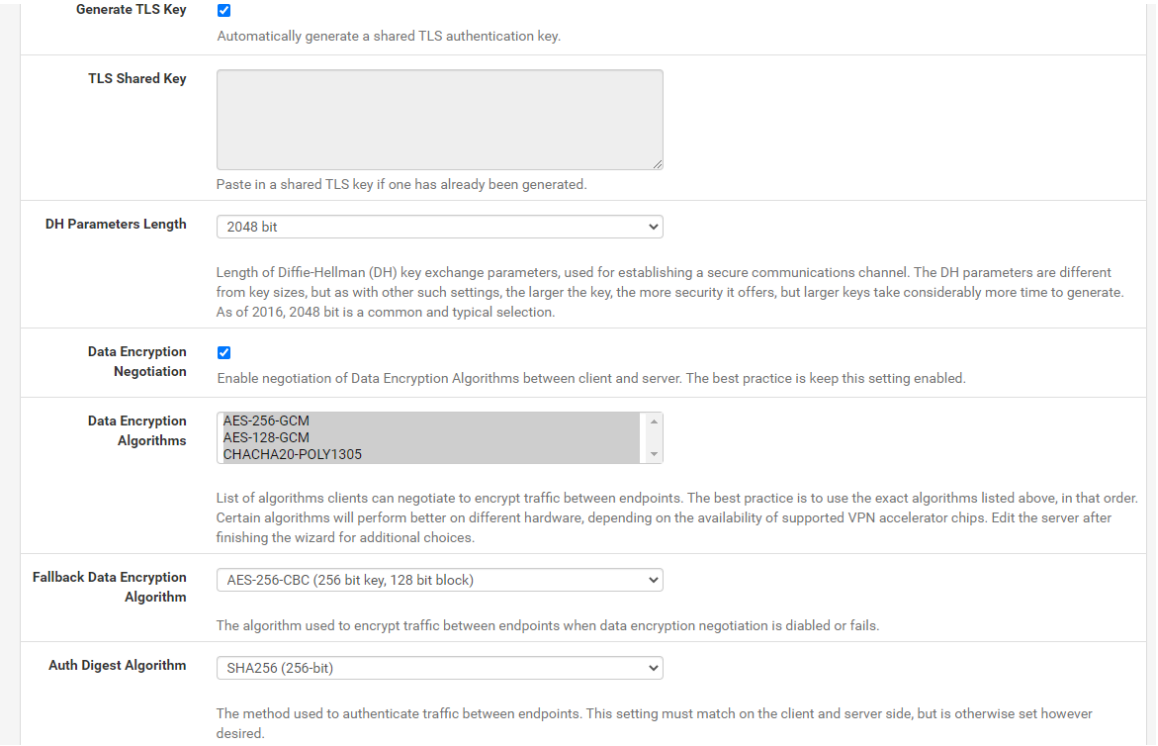


Chọn Local User Access và nhấn next



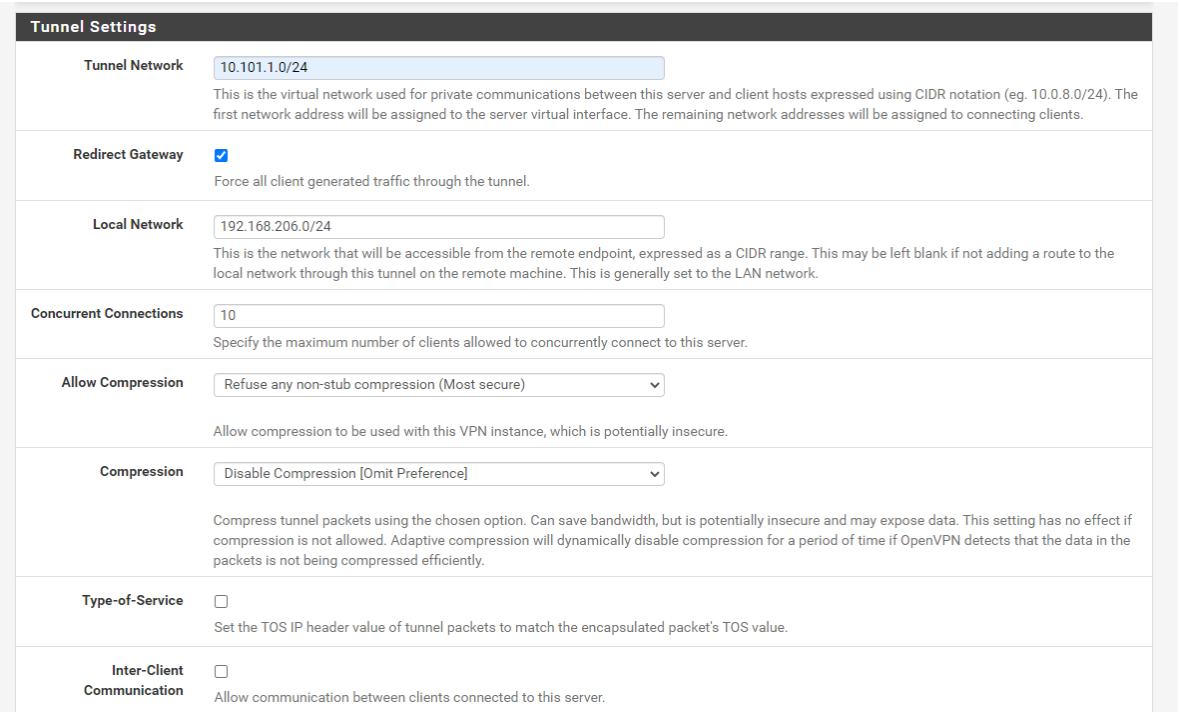
Chọn khóa CA đã tạo ở phía trên và nhấn Next



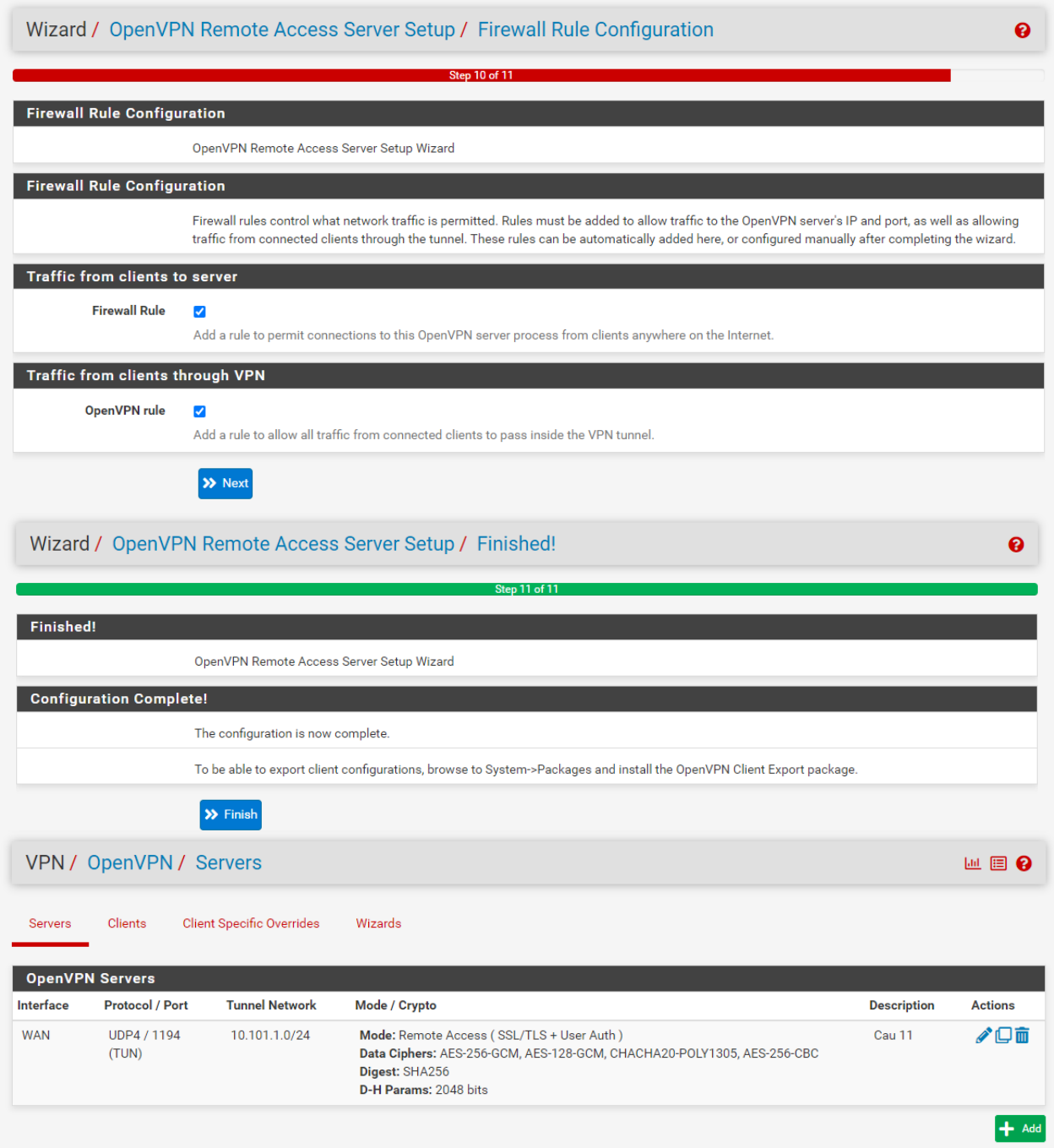


Điền địa chỉ IP ở tunnel network

Ở local network, điền địa chỉ mạng LAN của pfSense

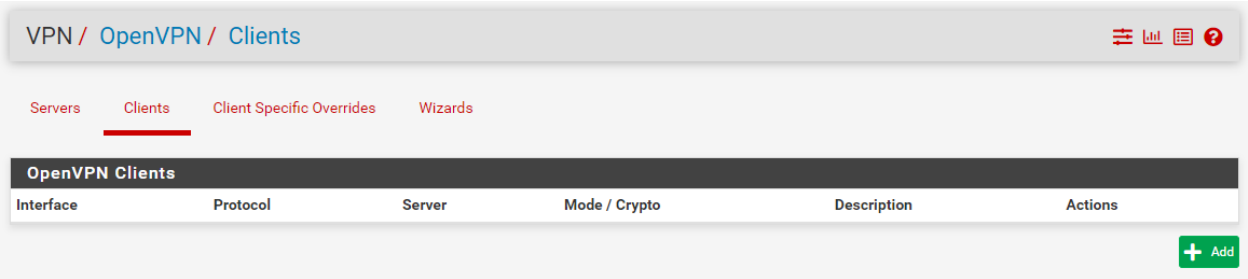


Nhấn tick vào 2 ô Firewall Rule, OpenVPN rule

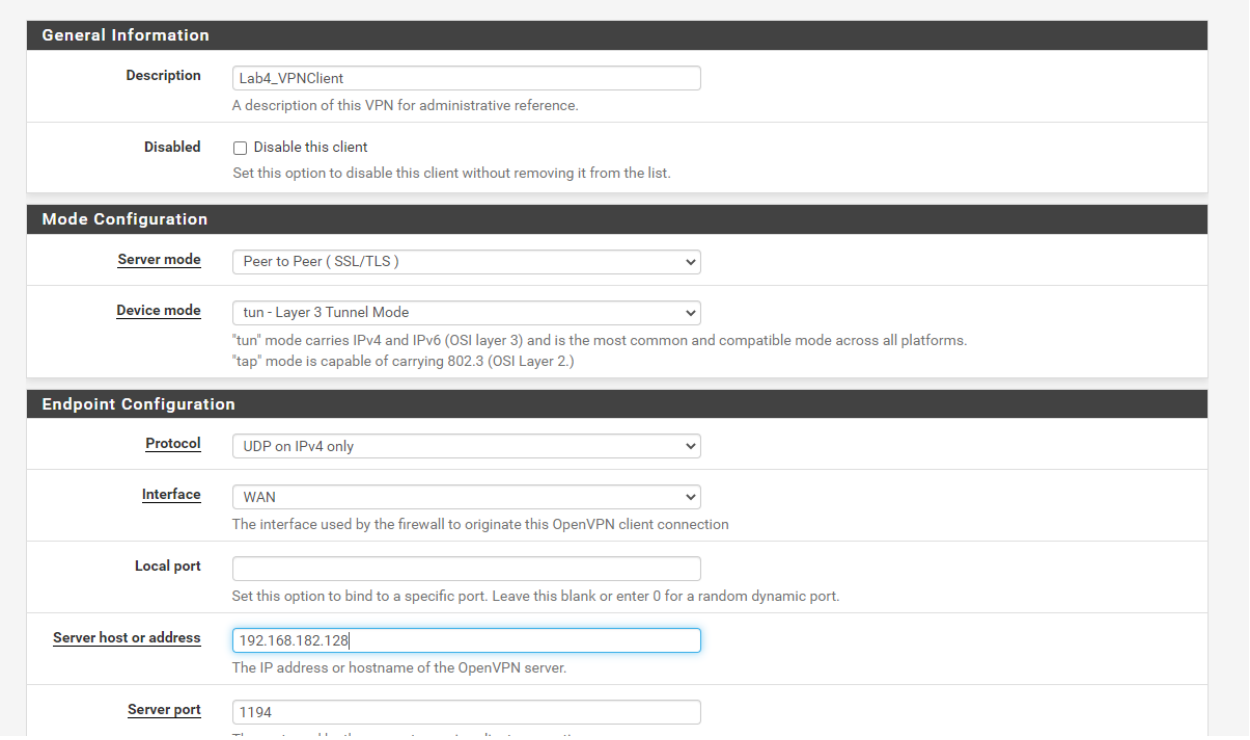


=> Hoàn tất cấu hình OpenVPN

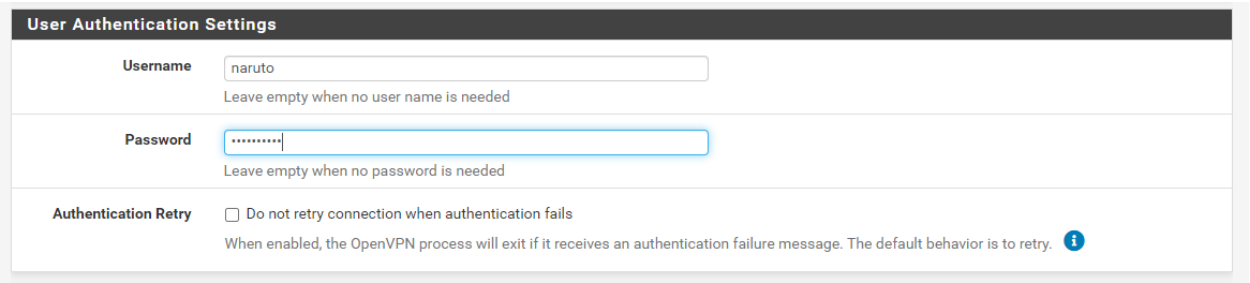
Cấu hình quyền truy cập của client:

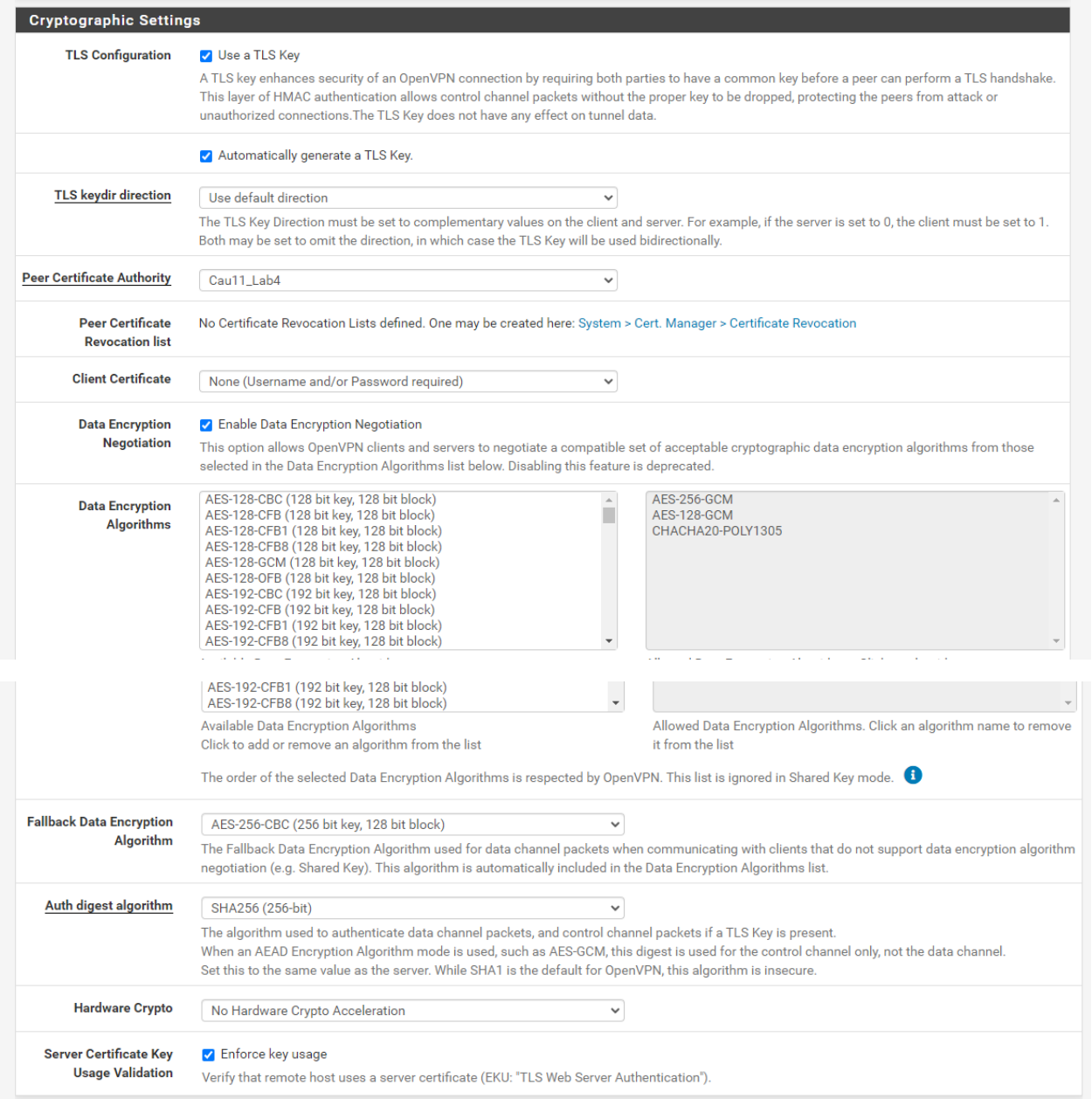


Địa chỉ server là địa chỉ máy pfSense

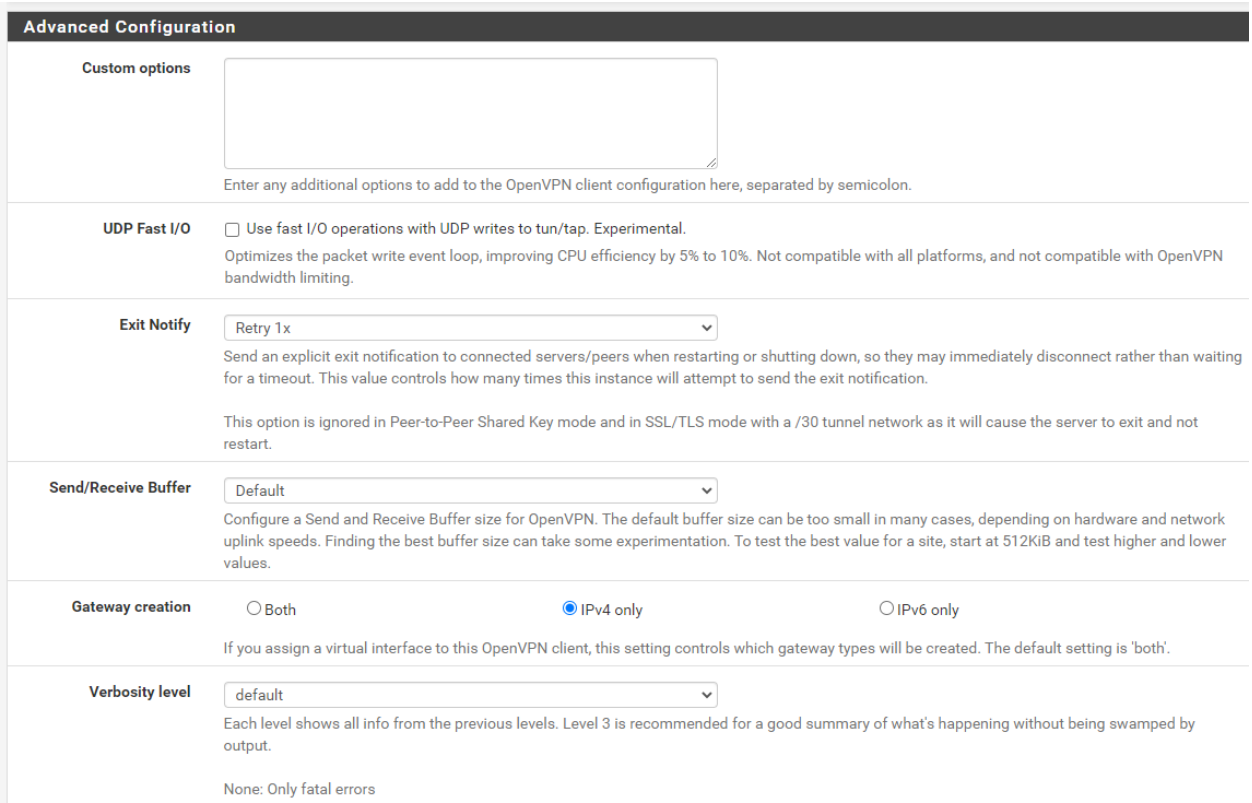


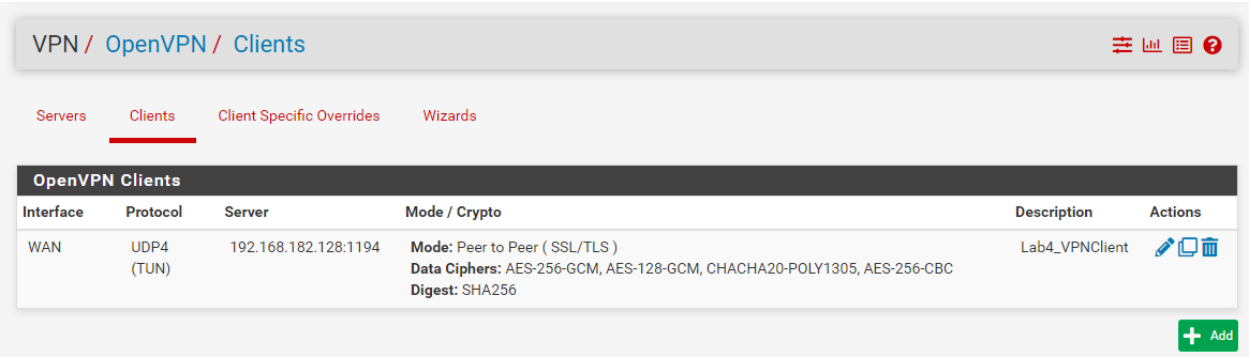
Tạo tài khoản naruto:naruto@123





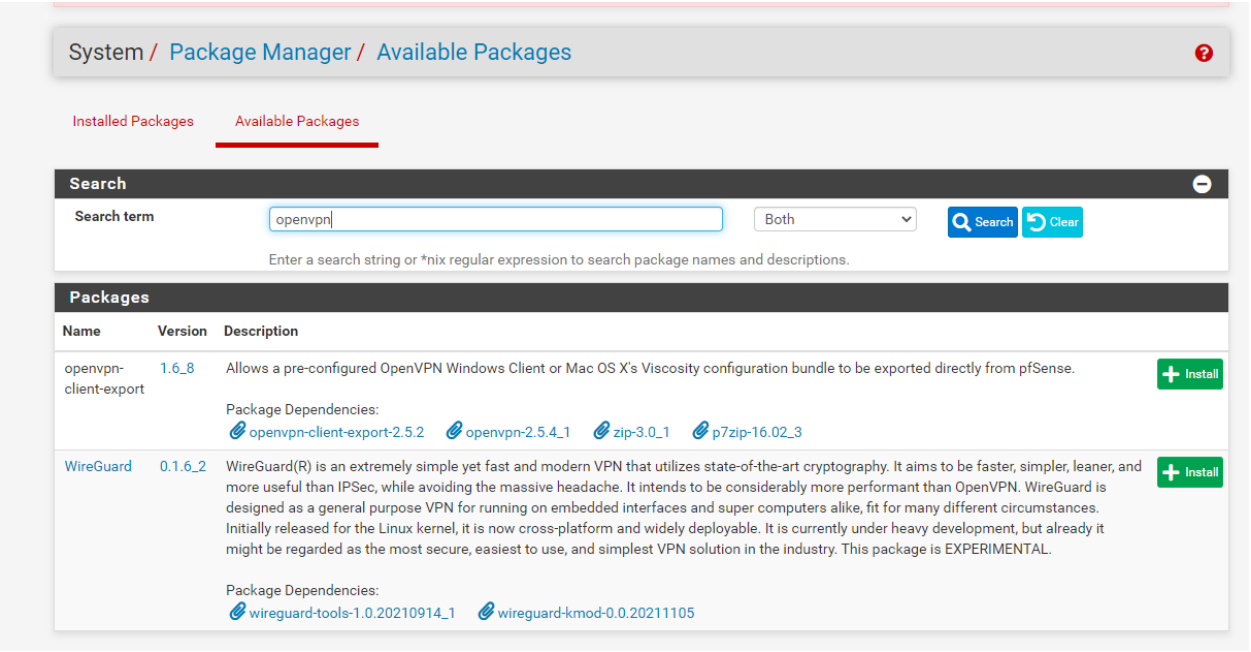
Ở Gateway creation, tick vào IPv4 only





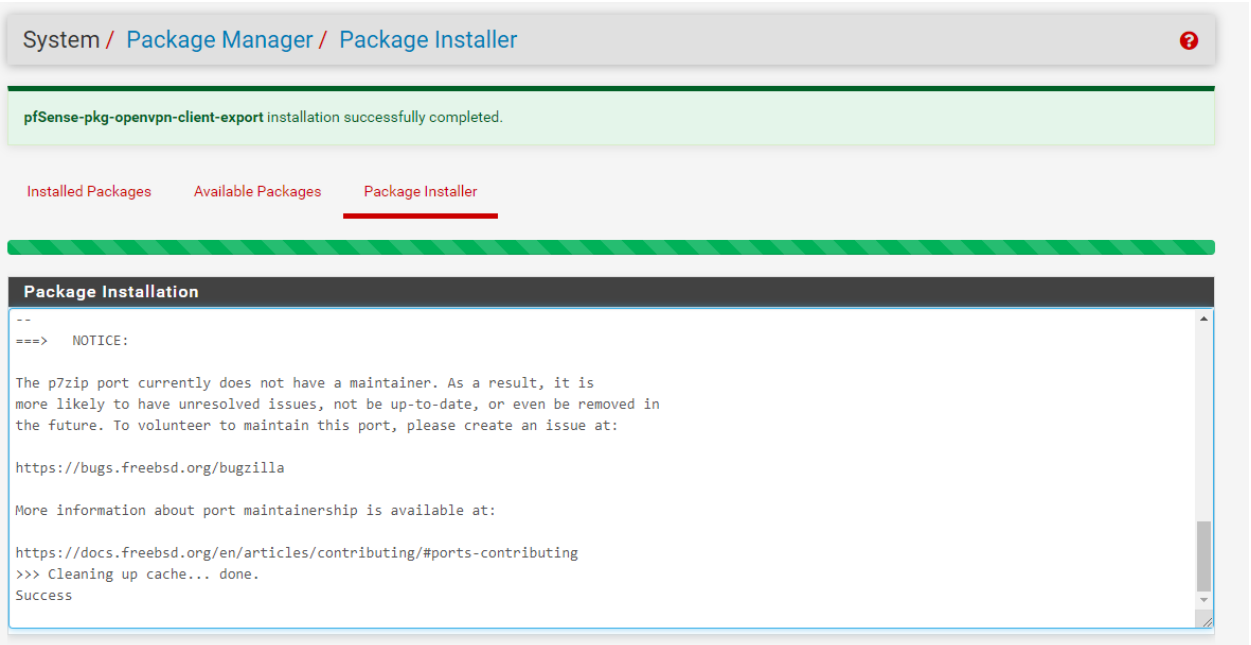
Ta cài tiếp gói OpenVPN Client Export để xuất các file cấu hình client kết nối tới máy chủ OpenVPN

System -> Package Manager -> Available Packages và search openvpn



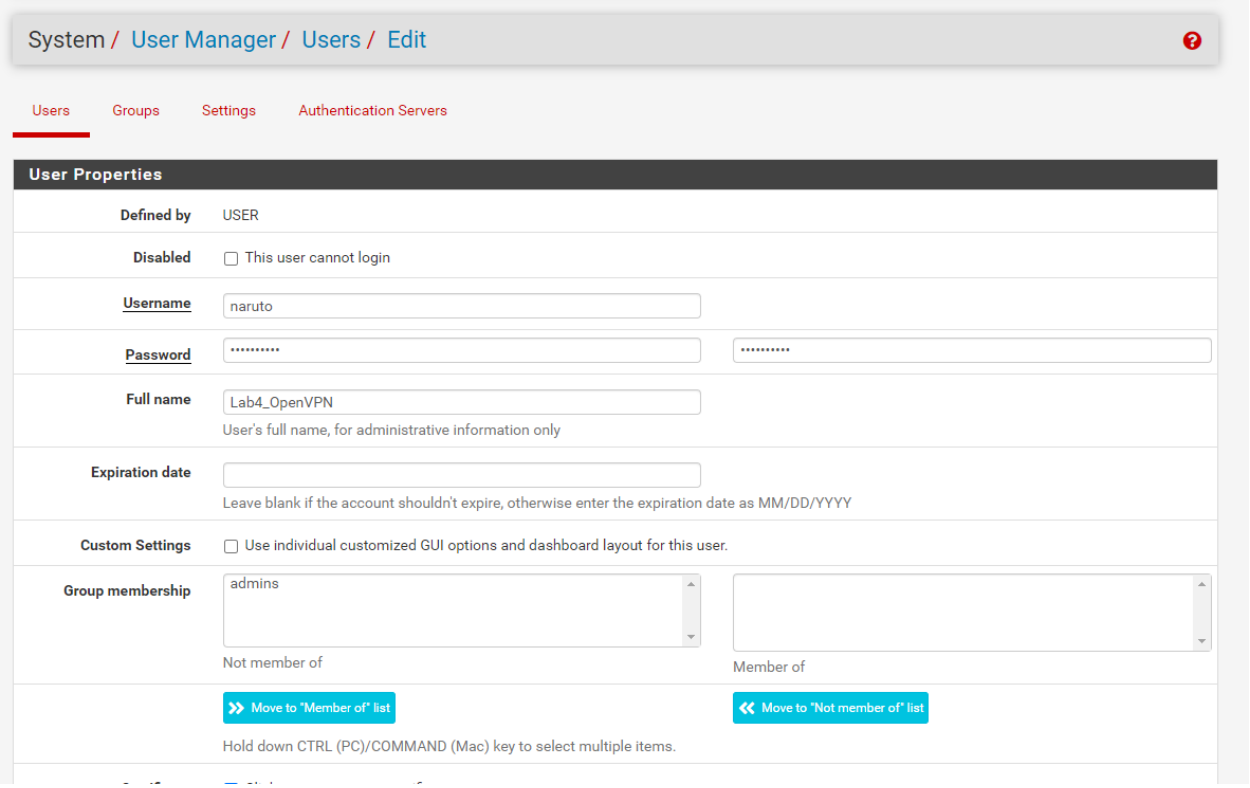
Nhấn install openvpn-clientexport và chọn confirm

Màn hình tải hoàn tất

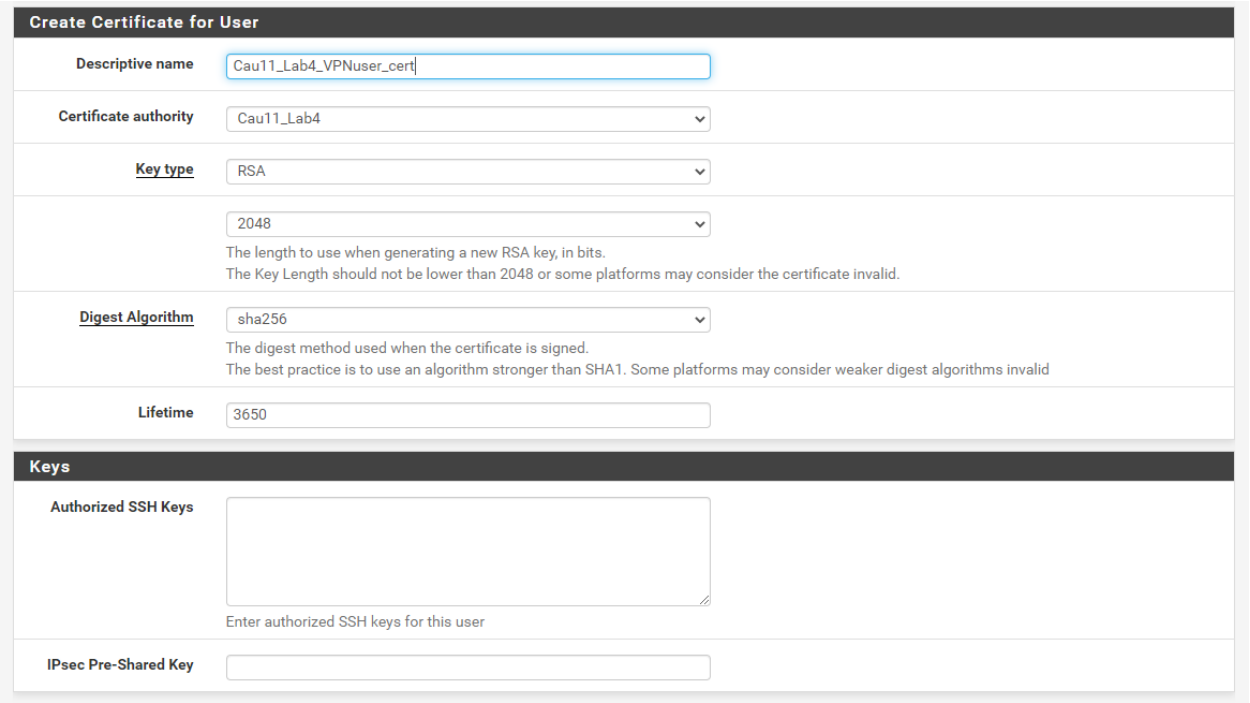


Tạo user VPN

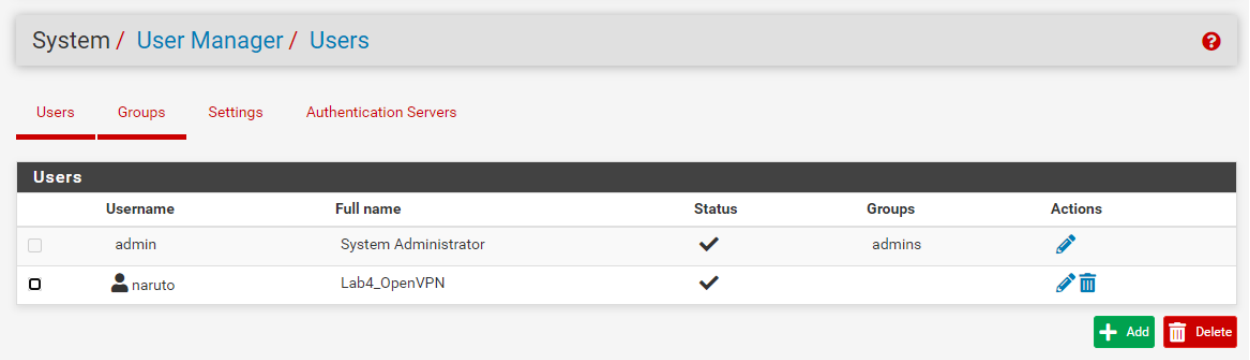
Tài khoản sẽ là tài khoản ta tạo ở phía trên khi cấu hình OpenVPN



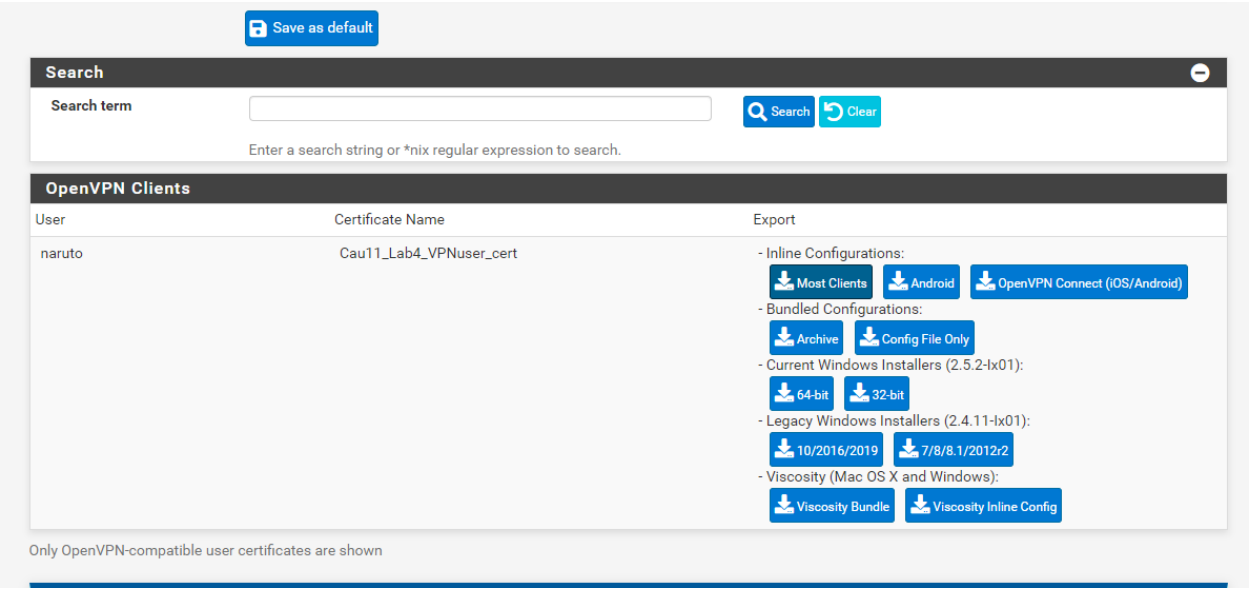
Tạo certificate cho người dùng



Nhấn save để lưu

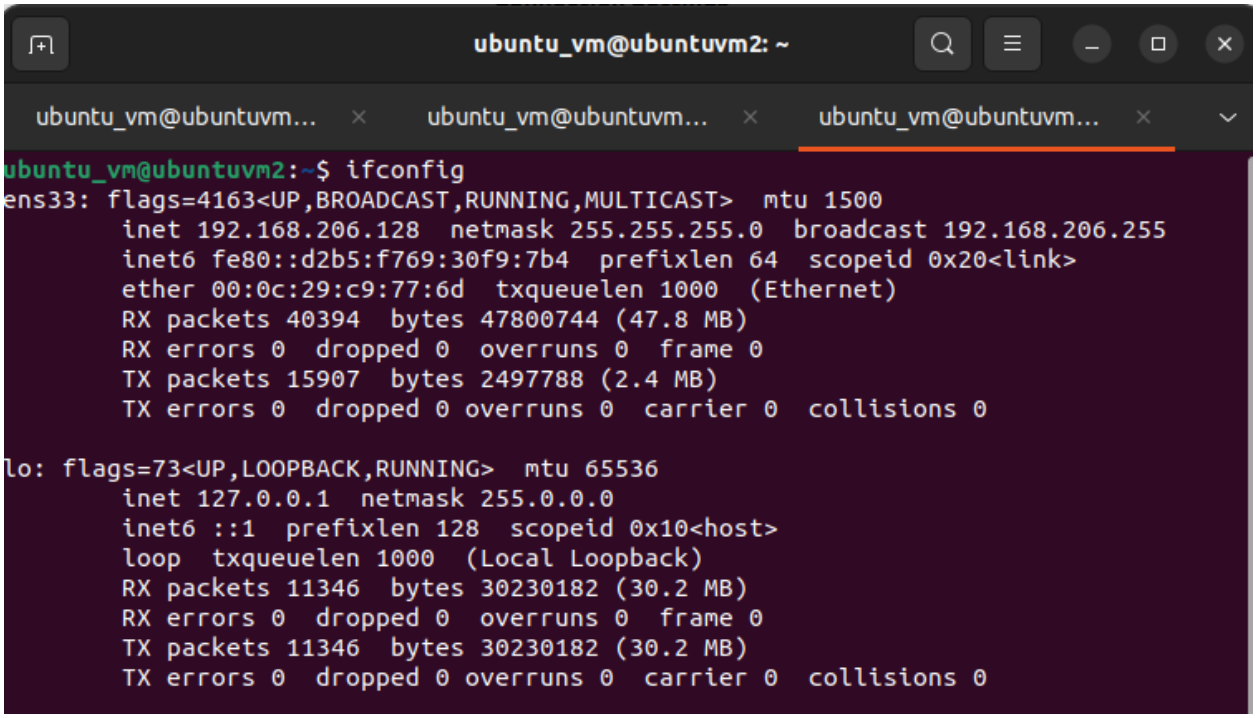


Export file openvpn cho user

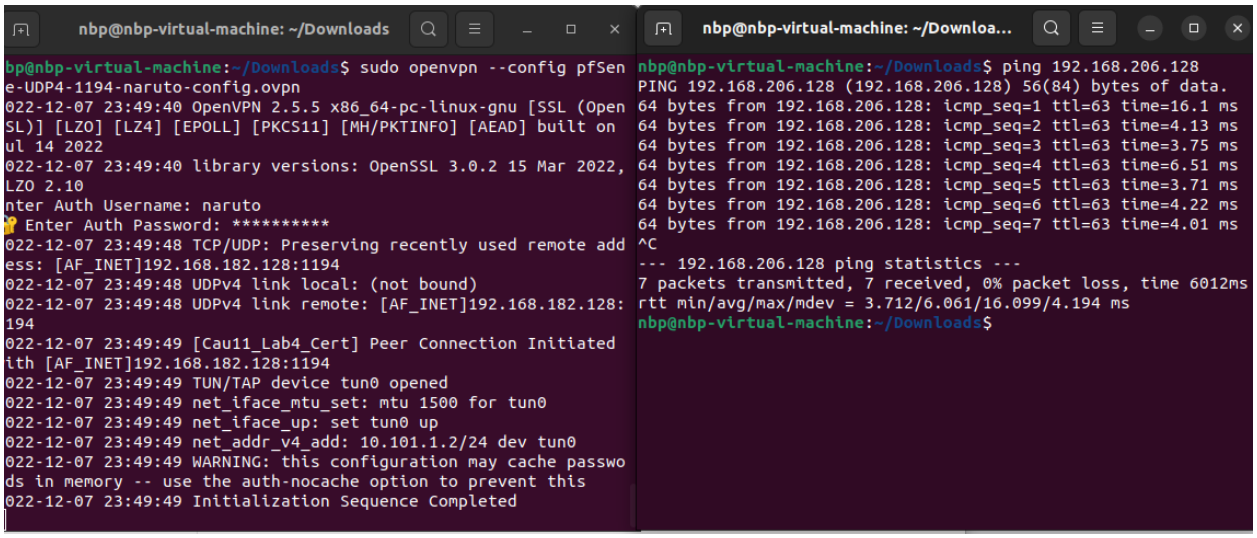


Chuyển file openvpn được export ra tới máy B, chạy file config và thử ping tới máy A

Ip máy A:



Kết quả khi ping từ B sang A



Vậy ta đã tạo tunnel OpenVPN, giờ ta đã có thể thực hiện các kết nối từ máy B vào mạng nội bộ của pfSense.

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

Sinh viên đọc kỹ yêu cầu trình bày bên dưới trang này

YÊU CẦU CHUNG

- Sinh viên tìm hiểu và thực hành theo hướng dẫn.
- Nộp báo cáo kết quả chi tiết những việc (**Report**) bạn đã thực hiện, quan sát thấy và kèm ảnh chụp màn hình kết quả (nếu có); giải thích cho quan sát (nếu có).
- Sinh viên báo cáo kết quả thực hiện và nộp bài.

Báo cáo:

- File .PDF. Tập trung vào nội dung, không mô tả lý thuyết.
- Nội dung trình bày bằng Font chữ Times New Romans/ hoặc font chữ của mẫu báo cáo này (UTM Neo Sans Intel/UTM Viet Sach)– cỡ chữ 13. Canh đều (Justify) cho văn bản. Canh giữa (Center) cho ảnh chụp.
- Đặt tên theo định dạng: [Mã lớp]-SessionX_GroupY. (trong đó X là Thứ tự buổi Thực hành, Y là số thứ tự Nhóm Thực hành/Tên Cá nhân đã đăng ký với GV).

  *Ví dụ: [*NT101.K11.ANTT*]-Session1_Group3.*
- Nếu báo cáo có nhiều file, nén tất cả file vào file .ZIP với cùng tên file báo cáo.
- Không đặt tên đúng định dạng – yêu cầu, sẽ **KHÔNG** chấm điểm.
- Nộp file báo cáo trên theo thời gian đã thống nhất tại courses.uit.edu.vn.

Đánh giá: Sinh viên hiểu và tự thực hiện. Khuyến khích:

- Chuẩn bị tốt.
- Có nội dung mở rộng, ứng dụng trong kịch bản/câu hỏi phức tạp hơn, có đóng góp xây dựng.

Bài sao chép, trễ, … sẽ được xử lý tùy mức độ vi phạm.

HẾT