

# BÁO CÁO THỰC HÀNH

Môn học: NT140.P12.ANTT – An Toàn Mạng

Tên chủ đề: Lab 5 - Khai thác tường lửa trong Linux

GVHD: Tô Trọng Nghĩa

Nhóm: 6

## 1. THÔNG TIN CHUNG:

(Liệt kê tất cả các thành viên trong nhóm)

Lớp: NT140.P12.ANTT.2

STT	Họ và tên	MSSV	Email
1	Lại Quan Thiên	22521385	22521385@gm.uit.edu.vn
2	Mai Nguyễn Nam Phương	22521164	22521164@gm.uit.edu.vn
3	Hồ Diệp Huy	22520541	22520541@gm.uit.edu.vn
4	Đặng Đức Tài	22521270	22521270@gm.uit.edu.vn

## 2. NỘI DUNG THỰC HIỆN:

STT	Nội dung	Tình trạng	Thực hiện	Trang
1	Cấu hình Môi trường Thực hành	100%	Quan Thiên	2
2	Task 1	100%	Quan Thiên	9
3	Task 2	100%	Diệp Huy	24
4	Task 3	100%	Nam Phương	26
5	Task 4	100%	Đức Tài	30
6	Task 5	100%	Diệp Huy, Đức Tài	37
Điểm tự đánh giá			10/10	

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

# CẤU HÌNH MÔI TRƯỜNG THỰC HÀNH

## Pfsense (192.168.1.1/24 và 10.0.2.5/24):

- Sau khi ta cài đặt xong Pfsense, được kết quả như sau:

Pfsense - VMware Workstation

Workstation | | | | | | | | | |

New\_Ubuntu 20.04.6 X Ubuntu 20.04.6 X Pfsense X

Reloading filter...  
Reloading routing configuration...  
DHCPD...

The IPv4 WAN address has been set to 10.0.2.5/24  
Press <ENTER> to continue.  
VMware Virtual Machine - Netgate Device ID: b524c94d3398b0313c75

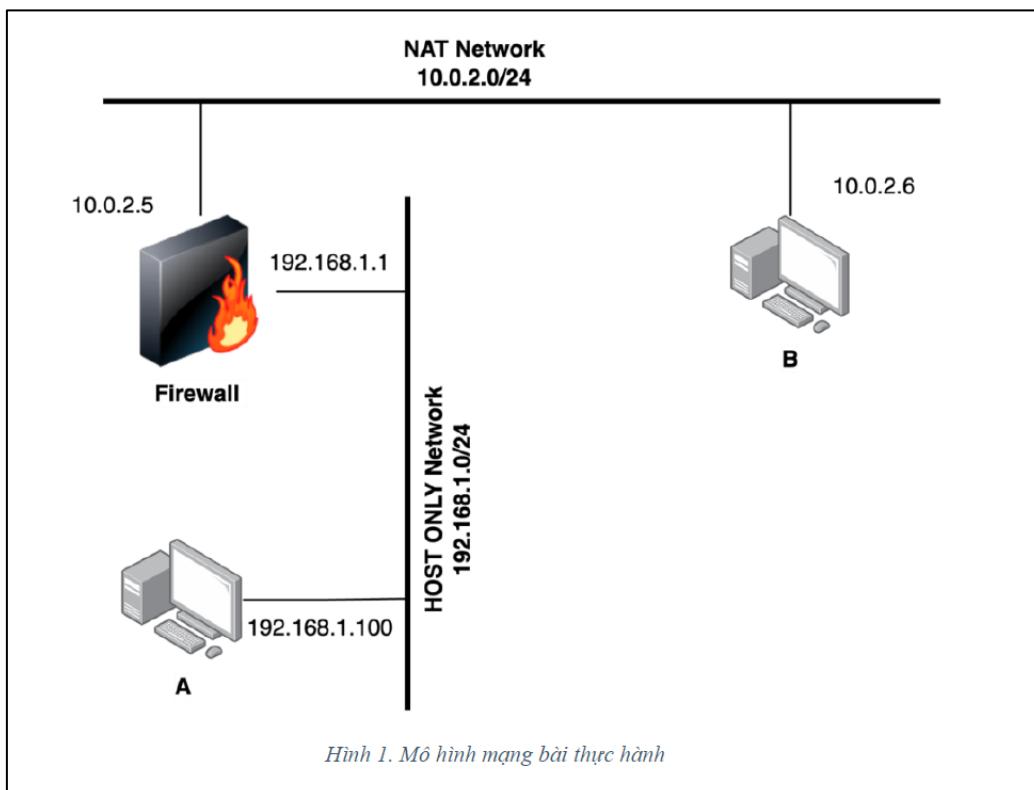
\*\*\* Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense \*\*\*

WAN (wan) -> em0 -> v4: 10.0.2.5/24  
LAN (lan) -> em1 -> v4: 192.168.1.1/24

0) Logout (SSH only) 9) pfTop  
1) Assign Interfaces 10) Filter Logs  
2) Set interface(s) IP address 11) Restart webConfigurator  
3) Reset webConfigurator password 12) PHP shell + pfSense tools  
4) Reset to factory defaults 13) Update from console  
5) Reboot system 14) Enable Secure Shell (sshd)  
6) Halt system 15) Restore recent configuration  
7) Ping host 16) Restart PHP-FPM  
8) Shell

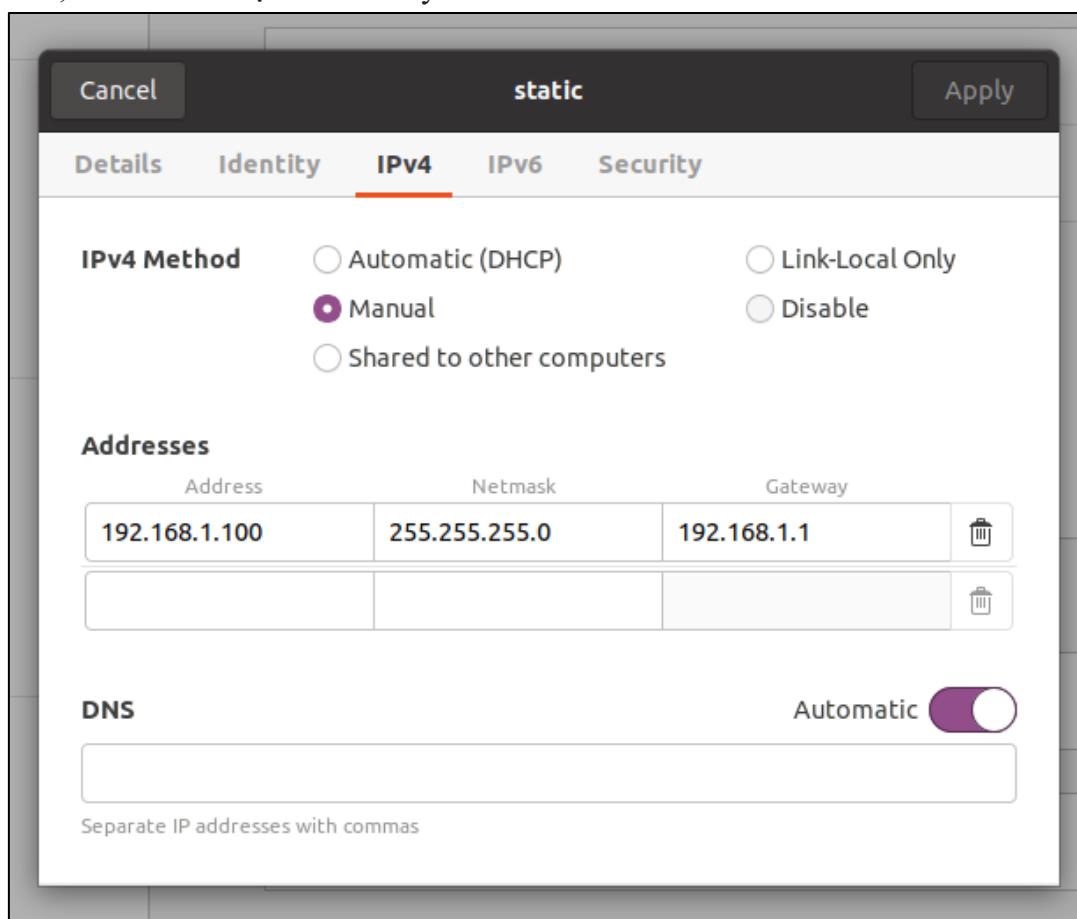
Enter an option: ■

- Nhắc lại mô hình triển khai:



**VM A (192.168.1.100/24):**

- Tiếp theo, ta cấu hình địa chỉ IP máy ảo A như sau:



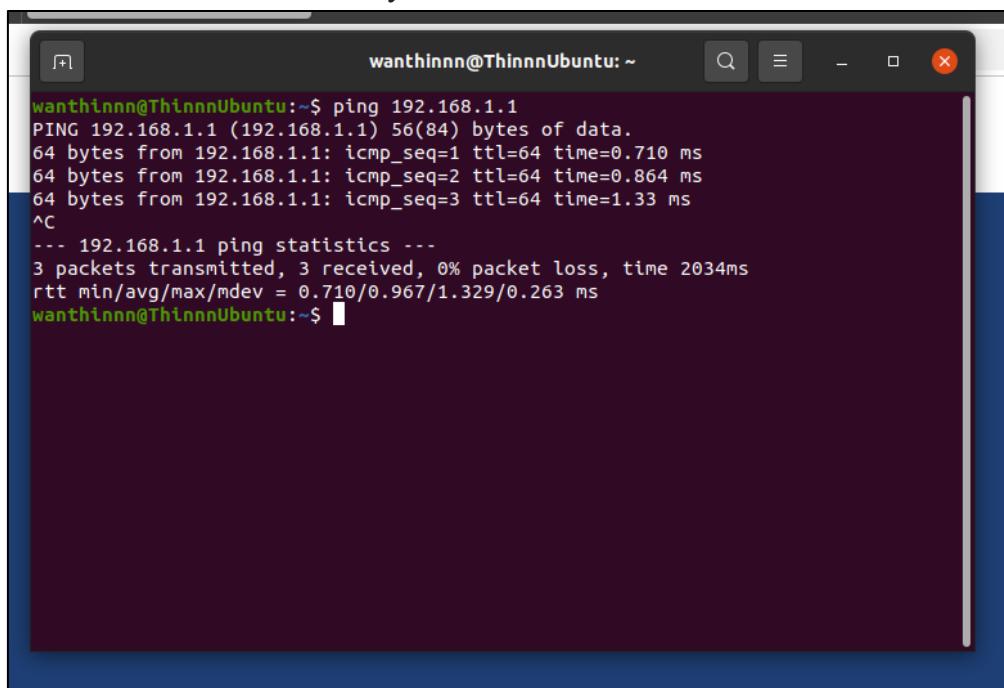
- Kiểm tra lại:

```
wanthin@ThinnnUbuntu:~$ ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.100  netmask 255.255.255.0  broadcast 192.168.1.255
              inet6 fe80::92d:b432:961a:41b6  prefixlen 64  scopeid 0x20<link>
                ether 00:0c:29:f1:92:12  txqueuelen 1000  (Ethernet)
                  RX packets 17908 bytes 17710850 (17.7 MB)
                  RX errors 0 dropped 0 overruns 0 frame 0
                  TX packets 13671 bytes 1770246 (1.7 MB)
                  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 33468 bytes 2569356 (2.5 MB)
                  RX errors 0 dropped 0 overruns 0 frame 0
                  TX packets 33468 bytes 2569356 (2.5 MB)
                  TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

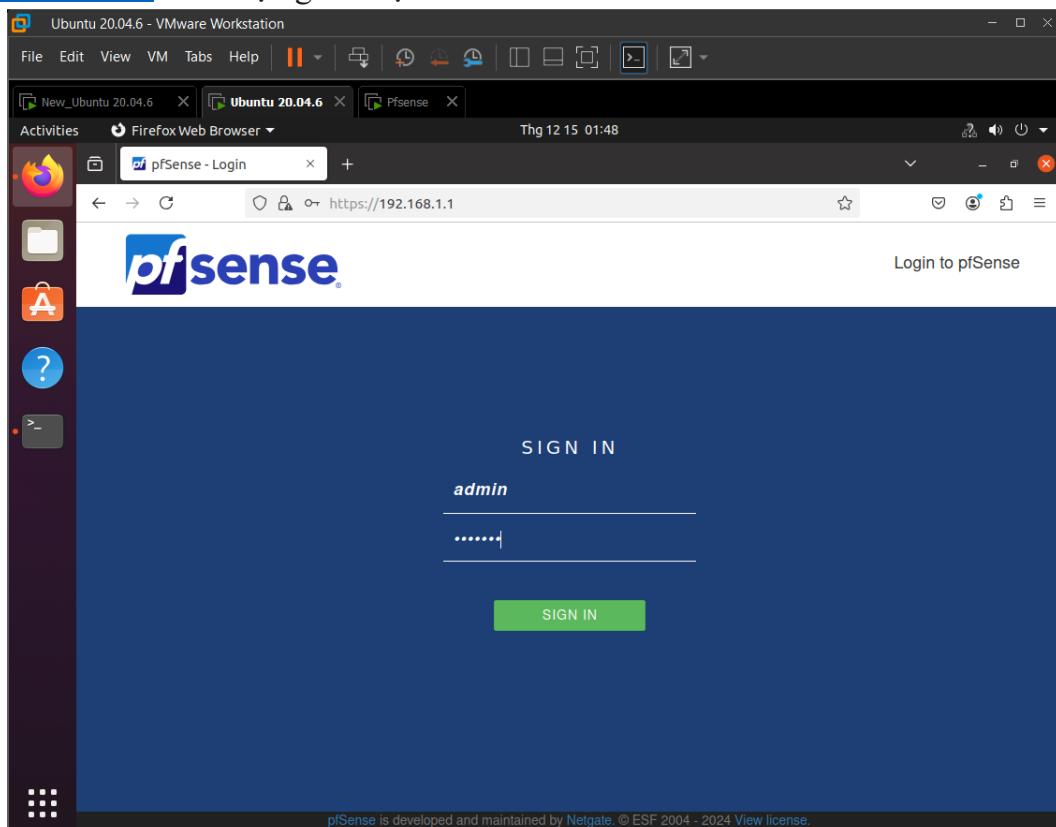
wanthin@ThinnnUbuntu:~$
```

- Ping từ VM A tới interface HostOnly của Firewall



```
wanthinnn@ThinnnUbuntu:~$ ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1) 56(84) bytes of data.
64 bytes from 192.168.1.1: icmp_seq=1 ttl=64 time=0.710 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=64 time=0.864 ms
64 bytes from 192.168.1.1: icmp_seq=3 ttl=64 time=1.33 ms
^C
--- 192.168.1.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2034ms
rtt min/avg/max/mdev = 0.710/0.967/1.329/0.263 ms
wanthinnn@ThinnnUbuntu:~$
```

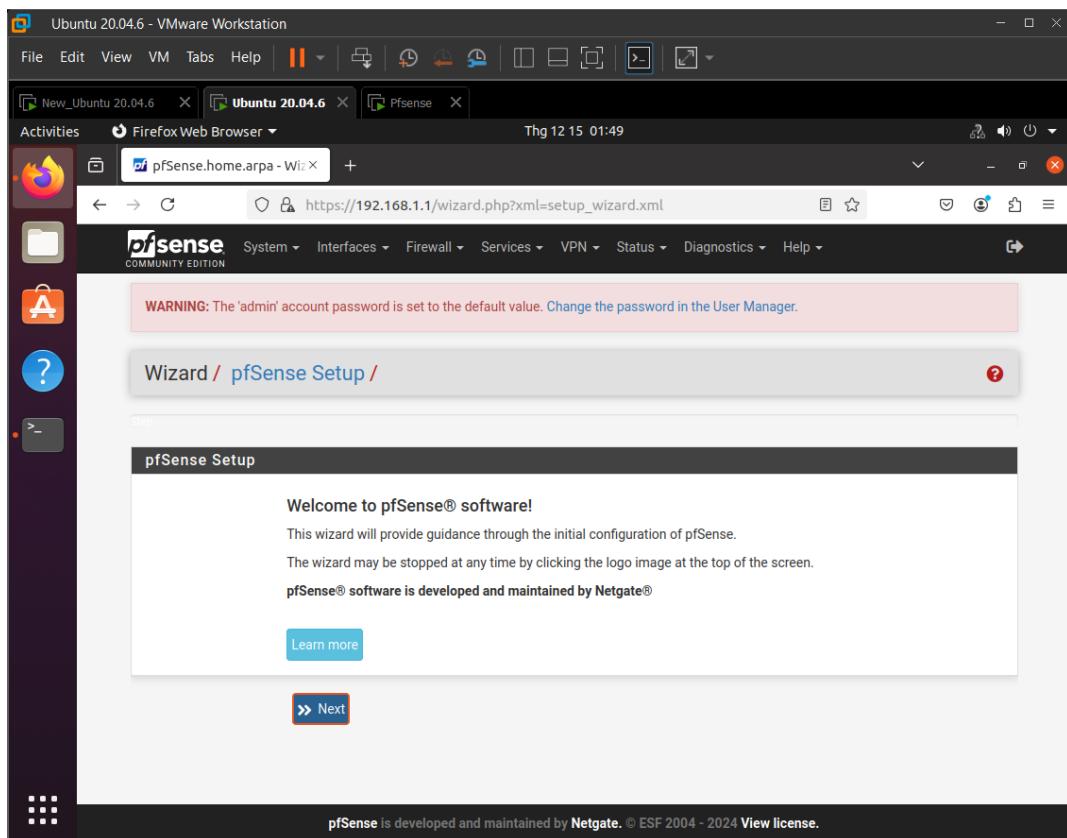
- Truy cập trang quản trị: Trên máy VM A, mở trình duyệt web và truy cập đến địa chỉ <https://192.168.1.1>. Ta được giao diện như hình dưới:



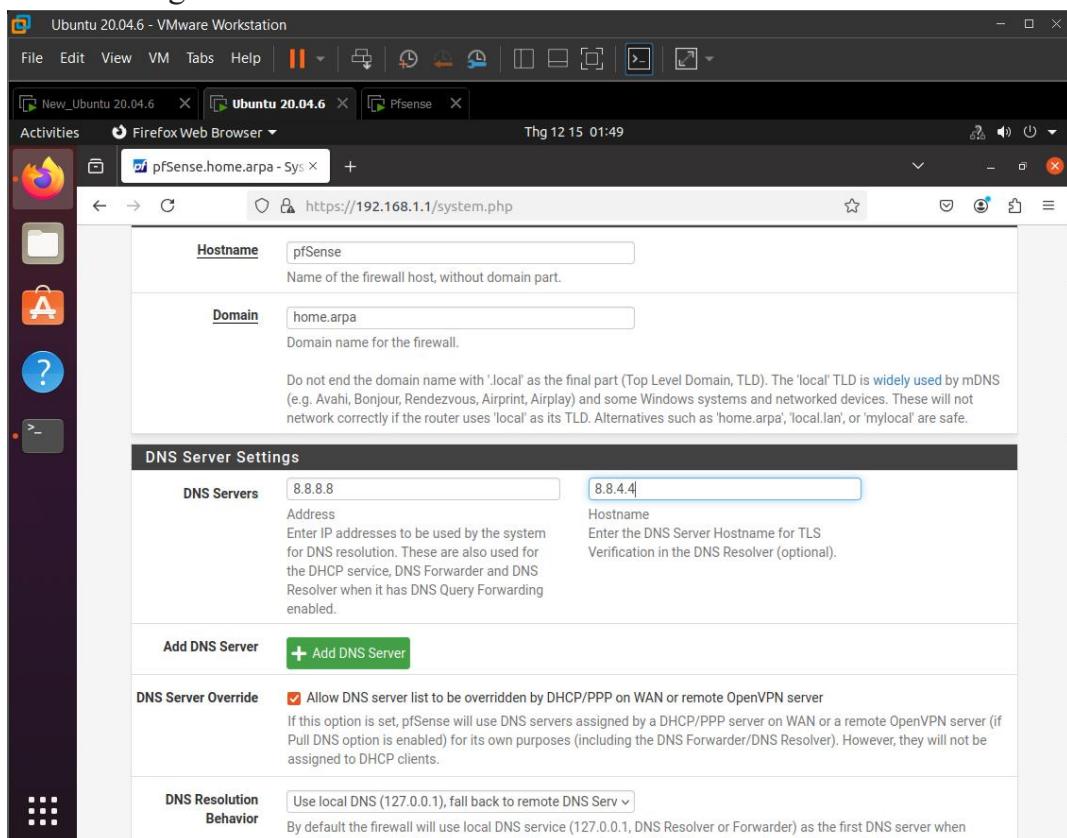
- Sau đó, đăng nhập vô trang web với tài khoản mặc định:

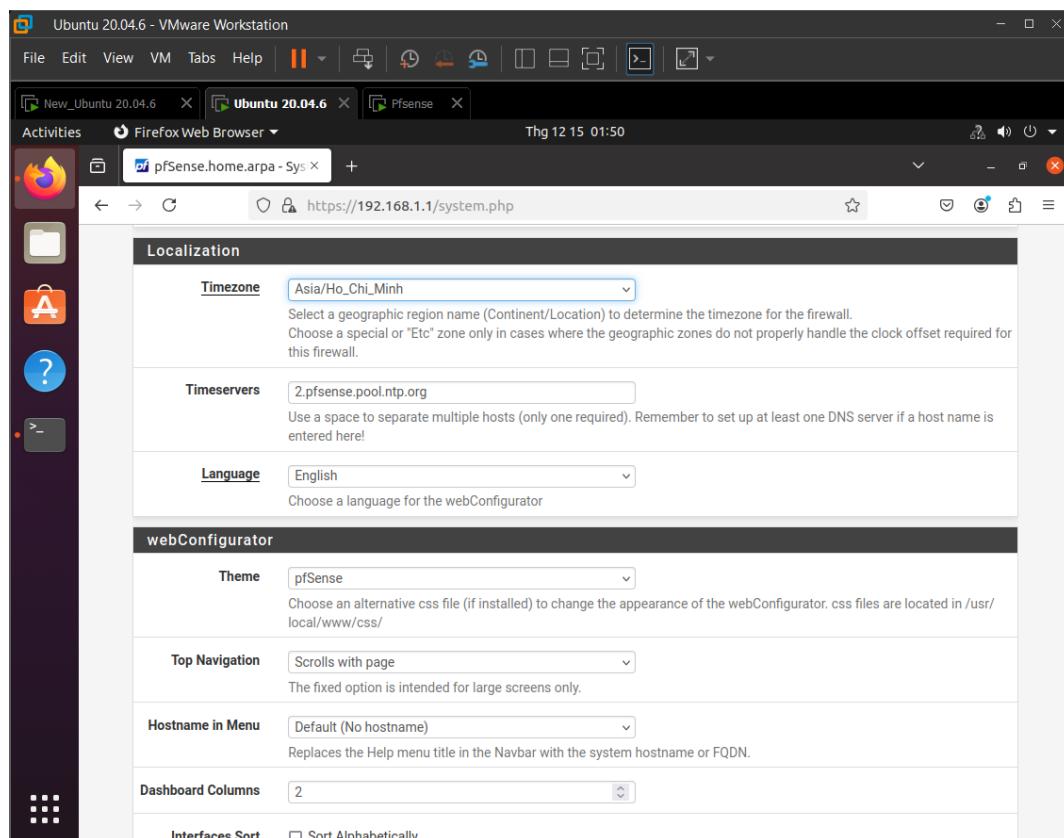
+ account: admin  
+ password: pfsense

- Giao diện chính:

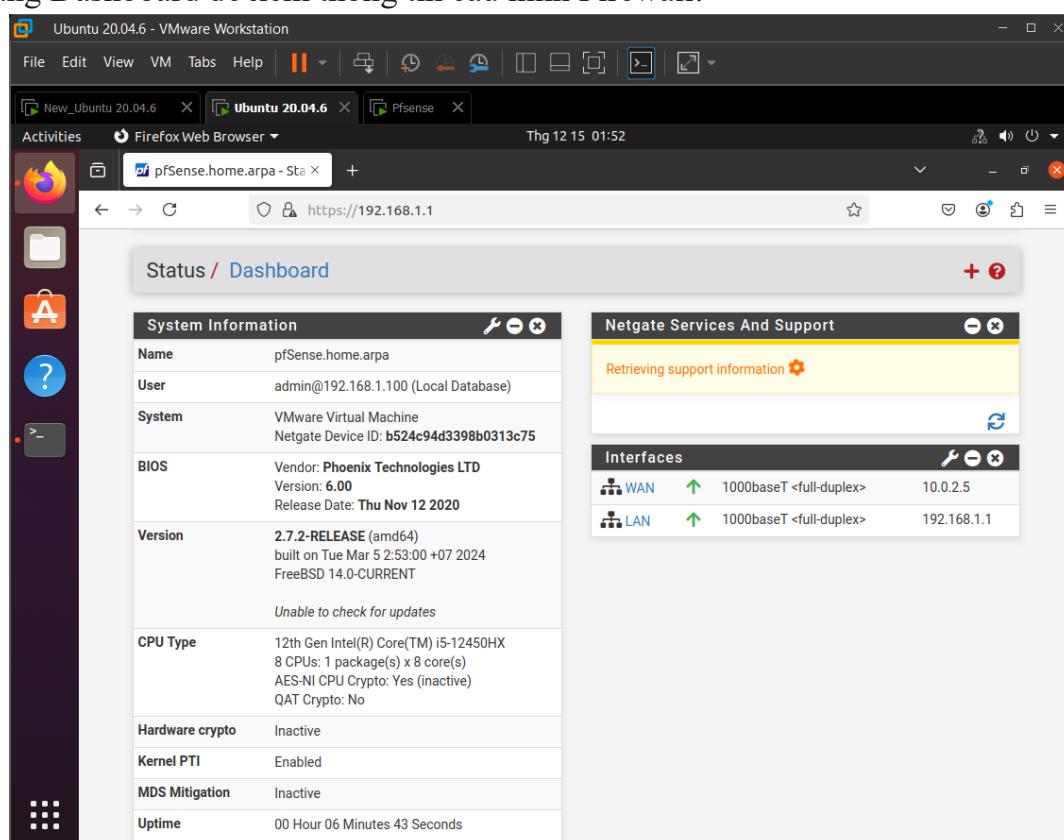


- Cấu hình các thông tin cơ bản:



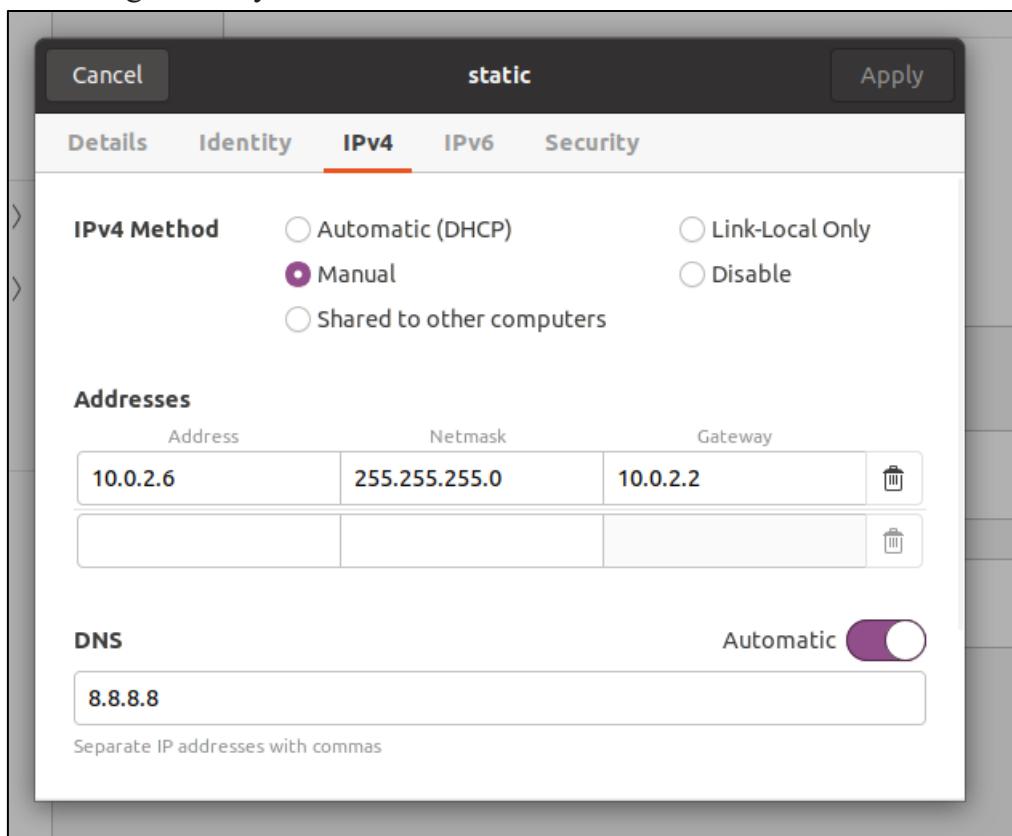


- Vô trang Dashboard để xem thông tin cấu hình Firewall:



**VM B (10.0.2.6/24):**

- Ta cấu hình mạng cho máy ảo B như sau:



- Kiểm tra lại:

```
wanthin@ThinnnUbuntu:~$ ifconfig
ens3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.6  netmask 255.255.255.0  broadcast 10.0.2.255
                ether 00:0c:29:85:f1:c0  txqueuelen 1000  (Ethernet)
                RX packets 8149  bytes 7802730 (7.8 MB)
                RX errors 0  dropped 0  overruns 0  frame 0
                TX packets 3982  bytes 615504 (615.5 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
                loop  txqueuelen 1000  (Local Loopback)
                RX packets 6681  bytes 571829 (571.8 KB)
                RX errors 0  dropped 0  overruns 0  frame 0
                TX packets 6681  bytes 571829 (571.8 KB)
                TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0

wanthin@ThinnnUbuntu:~$
```

**Kiểm Tra:**

- Ping từ máy A đến máy B:

```
wanthinnn@ThinnnUbuntu:~$ ping 10.0.2.6
PING 10.0.2.6 (10.0.2.6) 56(84) bytes of data.
64 bytes from 10.0.2.6: icmp_seq=1 ttl=63 time=2.08 ms
64 bytes from 10.0.2.6: icmp_seq=2 ttl=63 time=2.32 ms
64 bytes from 10.0.2.6: icmp_seq=3 ttl=63 time=1.19 ms
^C
--- 10.0.2.6 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 1.190/1.864/2.324/0.487 ms
wanthiinnn@ThinnnUbuntu:~$
```

- Ping từ máy B đến máy A:

```
wanthinnn@ThinnnUbuntu:~$ ping 192.168.1.100
PING 192.168.1.100 (192.168.1.100) 56(84) bytes of data.
^C
--- 192.168.1.100 ping statistics ---
23 packets transmitted, 0 received, 100% packet loss, time 22527ms
wanthiinnn@ThinnnUbuntu:~$
```

## BÁO CÁO CHI TIẾT

**Task 1:** Hiểu và thực hiện các rules sau (theo thứ tự):

1. Không cho phép các máy trong mạng nội bộ (192.168.1.0/24) 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.

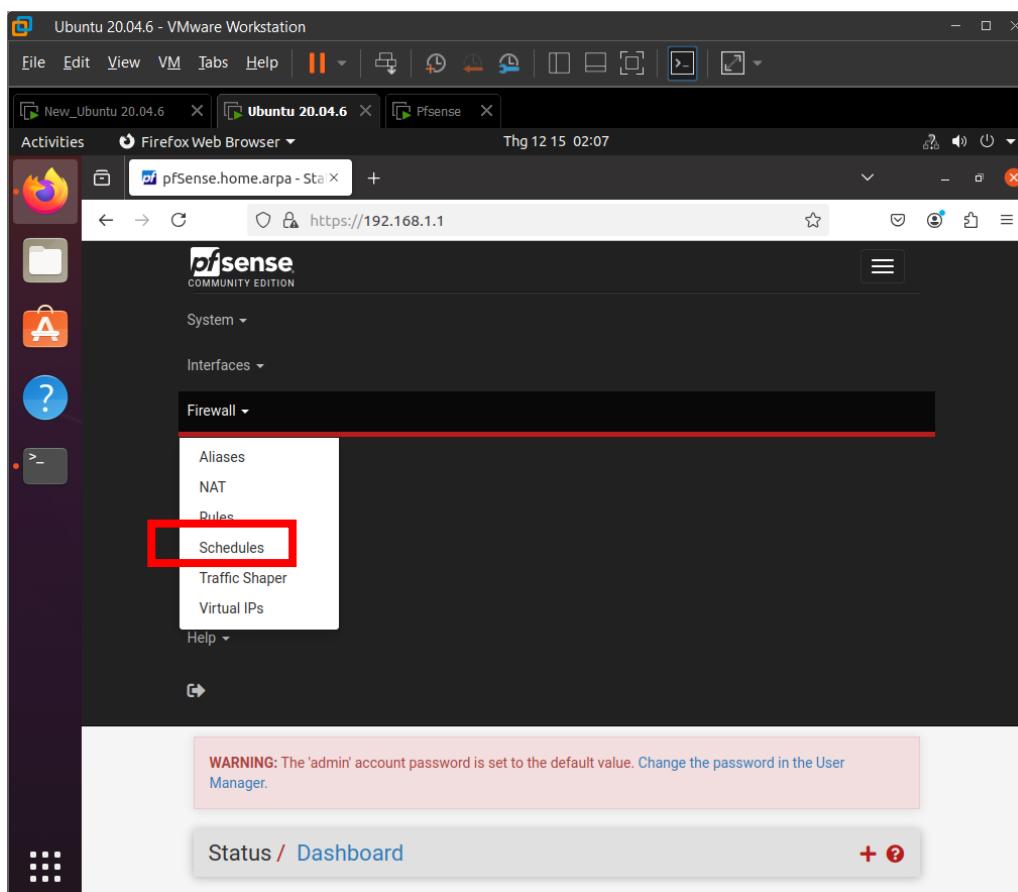
Sau khi triển khai các rules trên, sử dụng máy VM A để kiểm tra.

### Trả lời:

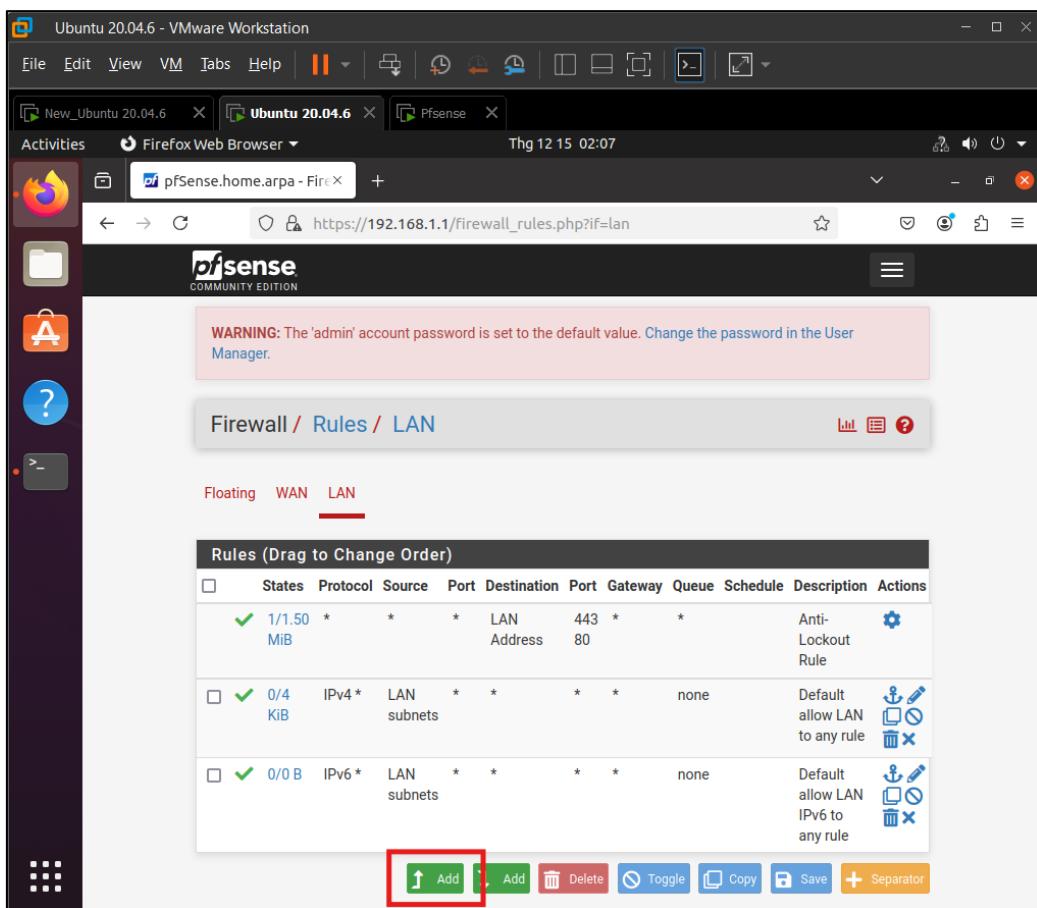
1. Không cho phép các máy trong mạng nội bộ (192.168.1.0/24) thực hiện ping đến máy VM B.

### Máy VM A:

- Trong trang webConfig firewall, trong tab menu, chọn Firewall -> Rules



- Nhấn Add để thêm 1 rule





- Thêm rule có nội dung như sau:

The screenshot shows the 'Edit Firewall Rule' screen in the pfSense web interface. The rule is being configured with the following parameters:

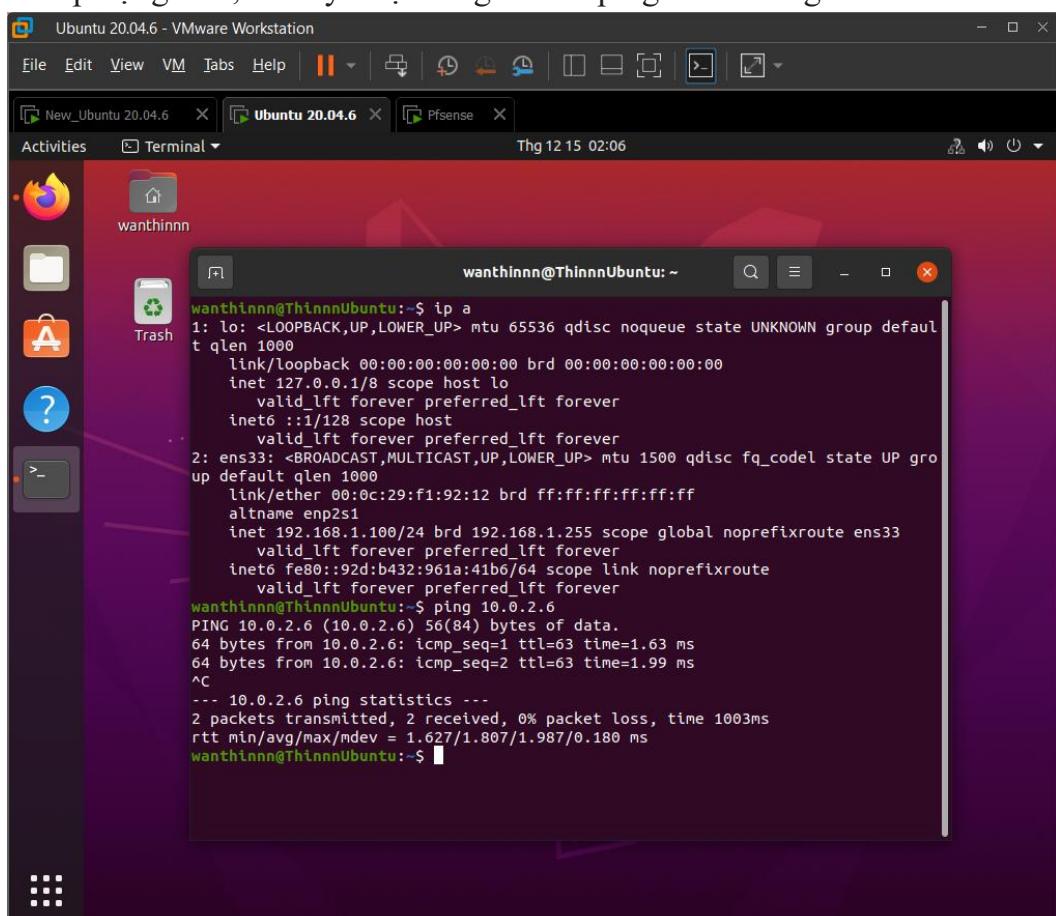
- Action:** Block
- Disabled:**  Disable this rule
- Interface:** LAN
- Address Family:** IPv4
- Protocol:** ICMP
- ICMP Subtypes:** any (Alternate Host, Datagram conversion error, Echo reply)
- Source:** Source: Network / 192.168.1.0 / 24
- Destination:** Destination: Address or Alias / 10.0.2.6
- Extra Options:**
  - Log:**  Log packets that are handled by this rule
  - Description:** Chan khong cho may A ping may B
  - Advanced Options:** Display Advanced
- Rule Information:**
  - Tracking ID:** 1734203307
  - Created:** 12/15/24 02:08:27 by admin@192.168.1.100 (Local Database)
  - Updated:** 12/15/24 02:53:07 by admin@192.168.1.100 (Local Database)

A blue 'Save' button is visible at the bottom left of the form.

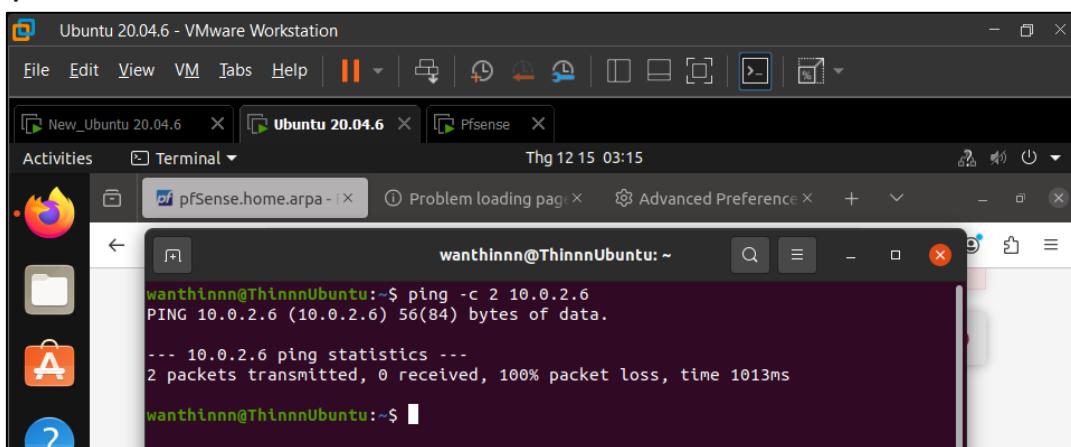
- Chọn Save để lưu
- Hiện thực các thay đổi bằng cách nhấn Apply Changes
- Ta được kết quả như sau:



- Trước khi áp dụng rule, ta thấy được rằng VM A ping thành công tới VM B-



- Sau khi tạo và áp dụng Rule, thực hiện lại việc ping từ VM A tới VM B. VM A không thể ping được đến VM B



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

### Máy VM A

- Trong trang webConfig firewall, trong tab menu, chọn Firewall -> Rules
- Nhấn Add để thêm 1 rule

The screenshot shows the pfSense Firewall Rules configuration interface. At the bottom, there is a toolbar with several buttons: 'Add' (highlighted with a red box), 'Delete', 'Toggle', 'Copy', 'Save', and 'Separator'. The 'Add' button is green with a white upward arrow icon.

Index	Action	Protocol	Source	Dest	Interface	Flags	Log	Policy	Comment
1	Allow	IPv4	LAN subnets	*	*	*	*	none	Default allow LAN to any rule
2	Allow	IPv6	LAN subnets	*	*	*	*	none	Default allow LAN IPv6 to any rule
3	Deny	IPv4 ICMP	any	*	*	*	*	none	

- Thêm rule có nội dung như sau:

The screenshot shows the pfSense firewall rules edit interface. A warning message at the top states: "WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager." The main section is titled "Edit Firewall Rule".

**Action:** Block

**Disabled:**  Disable this rule

**Interface:** LAN

**Address Family:** IPv4

**Protocol:** TCP/UDP

**Source:**

- Source: Network / 192.168.1.0 / 24
- Invert match
- Display Advanced**

The Source Port Range is set to "any".

**Destination:**

- Destination: Any
- Destination Port Range: HTTP (80) From Custom To Custom

The Destination Port Range is set to "HTTP (80)" from "Custom" to "Custom".

**Extra Options:**

- Log packets that are handled by this rule
- Description:** Chia mang noi bo truy cap vao website HTTP/80
- Advanced Options:** **Display Advanced**

**Rule Information:**

- Tracking ID: 1734204273
- Created: 12/15/24 02:24:33 by admin@192.168.1.100 (Local Database)
- Updated: 12/15/24 03:09:05 by admin@192.168.1.100 (Local Database)

- Chọn Save để lưu
- Hiện thực các thay đổi bằng cách nhấn Apply Changes
- Trước khi áp dụng Rule này, ta thấy VM A truy cập vào được web HTTP:

The screenshot shows a VMware Workstation interface with three virtual machines running. The central machine, labeled 'Ubuntu 20.04.6', has its desktop environment visible. A Firefox browser window is open, displaying a web page about HTML authoring. The page features a large photograph of a city skyline across a body of water, identified as the Hudson River at 125th Street around 2002. Below the photo, there is descriptive text and a list of links to other hand-coded websites.

**Do-It-Yourself Web Authoring - a beginner's HTML tutorial**

A random photo... (The Hudson River at 125th Street about 2002)

[Frank da Cruz](#)  
Updated in 2019 and 2021 for HTML5 and "fluidity".

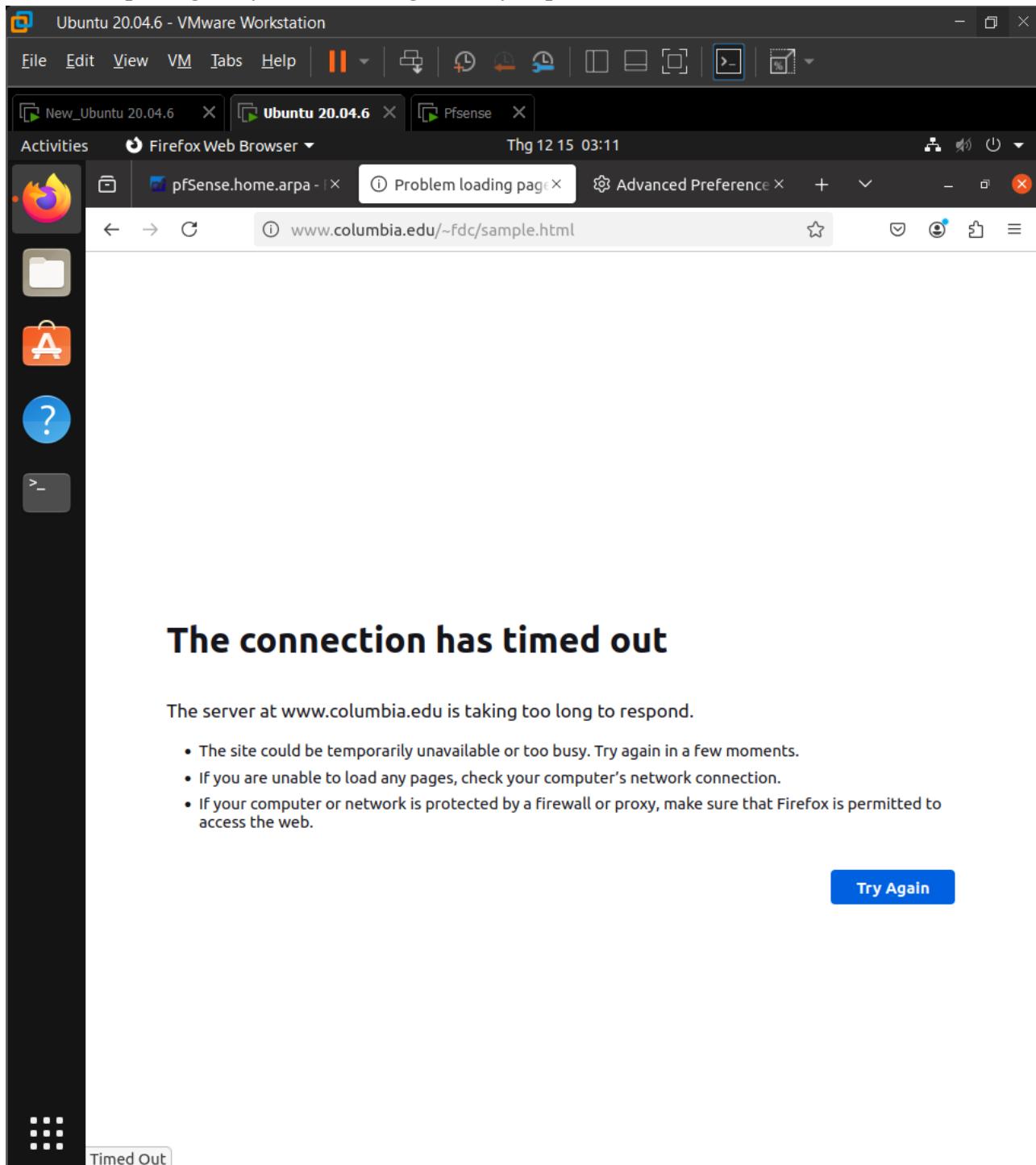
This page shows how to create Web pages by hand, the original way. Although today most Web pages are created by "Web authoring systems" that are designed to shield you from technical details, the fact is that HTML (the "programming" language of the Web) is not that difficult, as you can see if you follow this tutorial. To get an idea of what is possible with this technique, see these 100% hand-made websites:

- [The New Deal in New York City 1933-1943](#)
- [The History of Computing at Columbia University 1890-2005](#)
- [The Washington DC Nation Mall in World War II](#)
- [Arlington, Virginia, 1956-61: The Hall's Hill Segregation Wall](#)
- [Frankfurt, Germany, 1959-61](#)

**CONTENTS**

1. [Creating a Web Page](#)
2. [HTML Syntax](#)
3. [Special Characters](#)
4. [Converting Plain Text to HTML](#)
5. [Effects](#)
6. [Lists](#)

- Sau khi áp dụng, máy VM A không thể truy cập vào được :



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

- Tạo rule để chặn kết nối telnet từ mạng Lan ra bên ngoài Fireware:

The screenshot shows the pfSense Firewall Rules Edit interface. A warning message at the top states: "WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager." The main configuration area is titled "Edit Firewall Rule".

**Action:** Block  
 Choose what to do with packets that match the criteria specified below.  
 Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

**Disabled:**  Disable this rule  
 Set this option to disable this rule without removing it from the list.

**Interface:** LAN  
 Choose the interface from which packets must come to match this rule.

**Address Family:** IPv4  
 Select the Internet Protocol version this rule applies to.

**Protocol:** TCP/UDP  
 Choose which IP protocol this rule should match.

**Source:**

- Source:** Network / 192.168.1.0 / 24
- Display Advanced**

The Source Port Range for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, any.

**Destination:**

- Destination:** Any
- Destination Port Range:** Telnet (23) / From Custom To Custom

Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.

**Extra Options:**

- Log:**  Log packets that are handled by this rule  
 Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the Status: System Logs: Settings page).
- Description:** Chặn mạng nội bộ telnet ra bên ngoài
- Advanced Options:** **Display Advanced**

**Save**

- Nhấn Save để lưu
- Hiện thực các thay đổi bằng cách nhấn Apply Changes
- Trước khi áp dụng rule, ta telnet đến telehack.com port 23 vẫn bình thường:

```
wanthinnn@ThinnnUbuntu:~$ telnet telehack.com 23
Trying 64.13.139.230...
Connected to telehack.com.
Escape character is '^]'.

Connected to TELEHACK port 61

It is 12:24 pm on Saturday, December 14, 2024 in Mountain View, California, USA.
There are 115 local users. There are 26648 hosts on the network.

May the command line live forever.

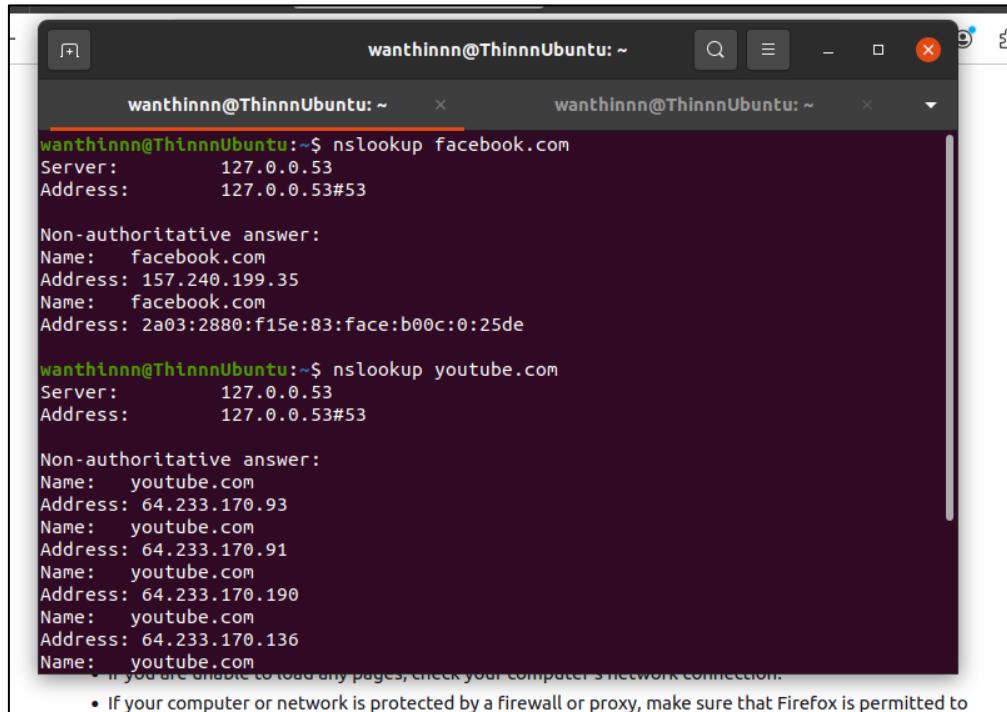
Command, one of the following:
 2048      ?      a2      advent      aquarium      basic
 bf        c8      cal      calc       callsign      cat
 ching     clear    cowsay   ddate      delta       diff
 dir       echo     eliza    exit       factor      finger
 fnord    head     help     mac        md5        minesweeper
 morse    netstat  newuser  octopus   phoon      pig
 ping     pong     privacy  qr        rain       rainbow
 rand     rfc      rig      rockets   roll       rot13
 run      salvo    starwars sudoku   tail       typespeed
 units    uumap    uuplot   weather  when      zc
```

- Sau khi áp dụng rule, không thể telnet được:

```
wanthinnn@ThinnnUbuntu:~$ telnet telehack.com 23
Trying 64.13.139.230...
^C
wanthinnn@ThinnnUbuntu:~$
```

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

- Tìm các ip ứng với domain facebook.com và youtube.com. Vì có khá nhiều ip nên ở bài lab này chúng ta sẽ lấy ip đầu tiên tìm được rồi tạo alias cho mạng phù hợp với IP đó. Sử dụng lệnh nslookup <domain> để tìm:



```
wanthinnn@ThinnnUbuntu:~$ nslookup facebook.com
Server: 127.0.0.53
Address: 127.0.0.53#53

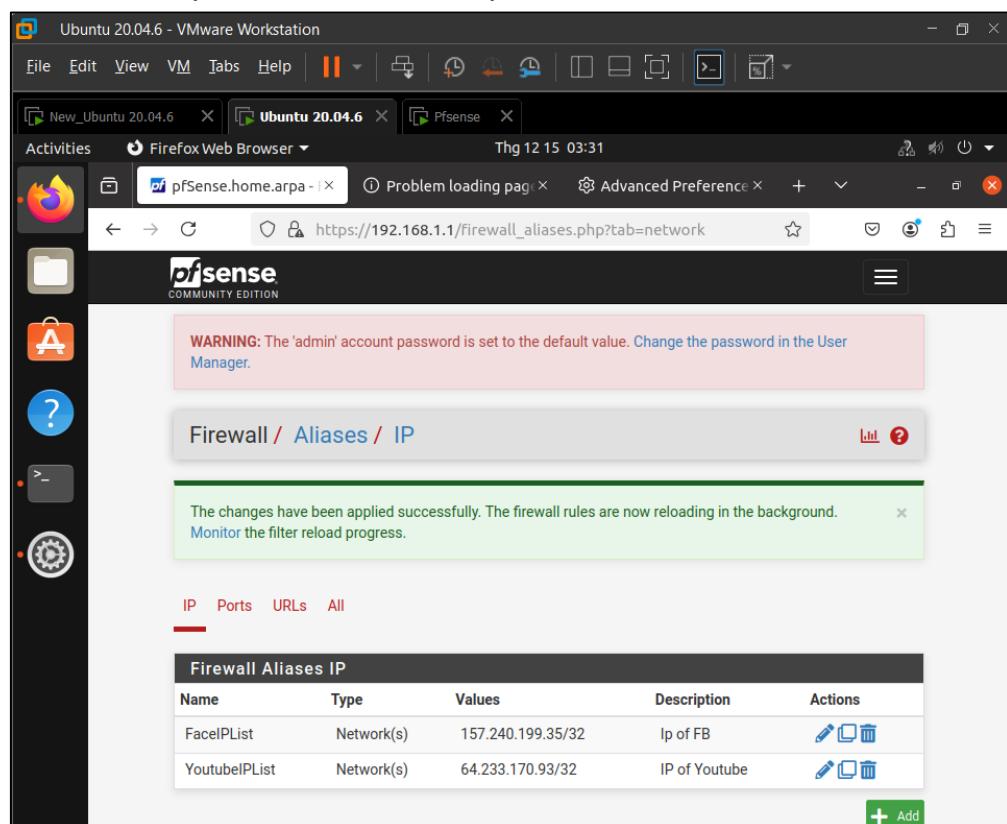
Non-authoritative answer:
Name: facebook.com
Address: 157.240.199.35
Name: facebook.com
Address: 2a03:2880:f15e:83:face:b00c:0:25de

wanthinnn@ThinnnUbuntu:~$ nslookup youtube.com
Server: 127.0.0.53
Address: 127.0.0.53#53

Non-authoritative answer:
Name: youtube.com
Address: 64.233.170.93
Name: youtube.com
Address: 64.233.170.91
Name: youtube.com
Address: 64.233.170.190
Name: youtube.com
Address: 64.233.170.136
Name: youtube.com
```

If you are unable to load any pages, check your computer's network connection.  
• If your computer or network is protected by a firewall or proxy, make sure that Firefox is permitted to

- Tạo danh sách alias dựa trên IP vừa tìm được:



- Thực hiện tạo các Rules để ngăn chặn việc truy cập web:

+ Rule cho Facebook:

The screenshot shows the 'Edit Firewall Rule' configuration window in the pfSense interface. The 'Action' is set to 'Block'. The 'Interface' is 'LAN'. The 'Address Family' is 'IPv4'. The 'Protocol' is 'TCP/UDP'. In the 'Source' section, the 'Source' is 'Network' with address '192.168.1.0 / 24'. In the 'Destination' section, the 'Destination' is 'FacelPList' and the 'Port Range' is 'From 0 To 0'. The 'Description' is 'Chặn mạng nội bộ truy cập vào FB'. A 'Save' button is at the bottom.

+ Rule cho Youtube:

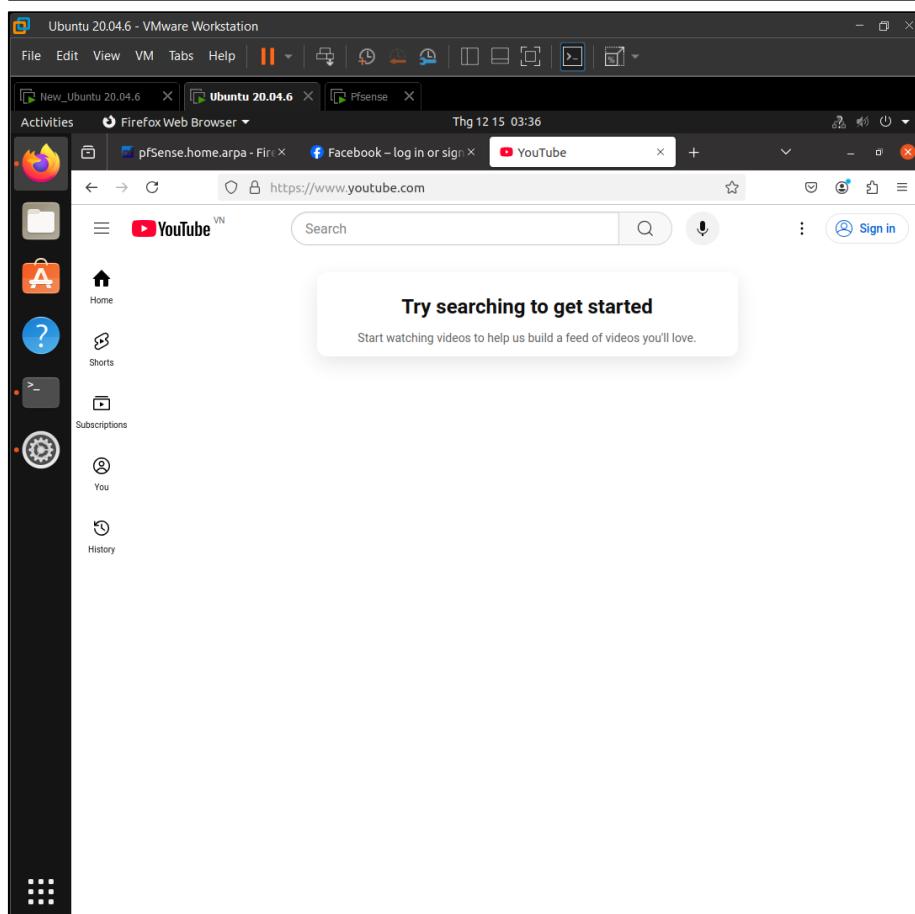
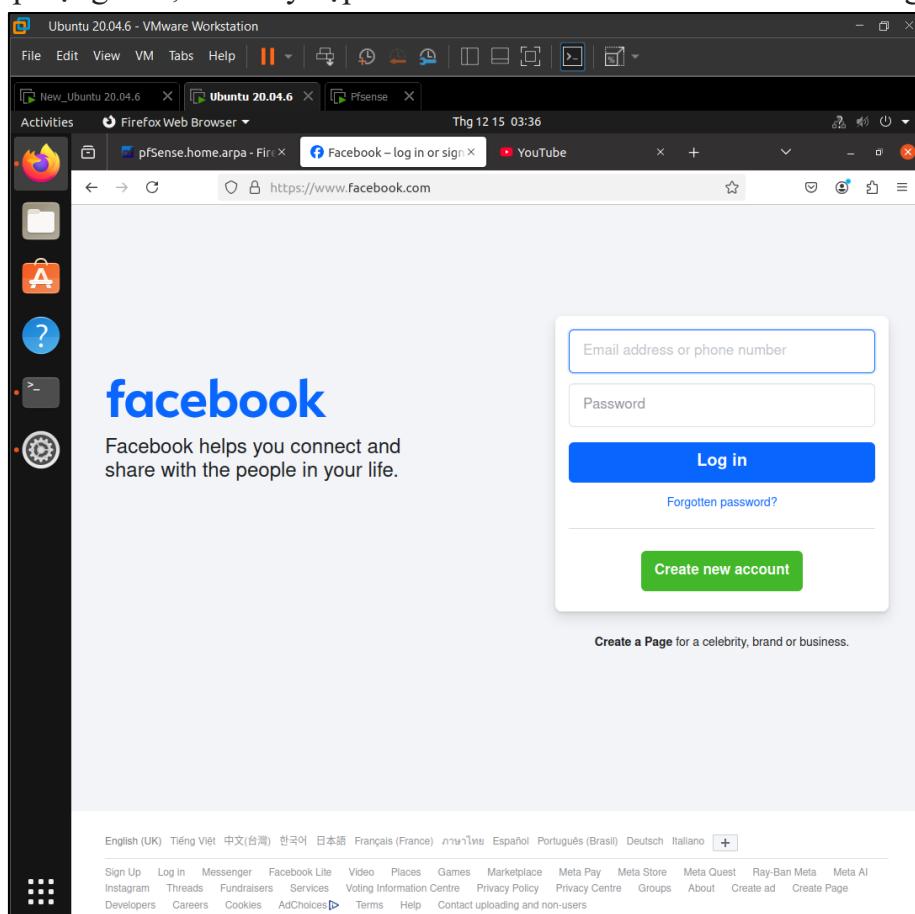
The screenshot shows the pfSense Firewall Rules Edit interface. A new rule is being created with the following details:

- Action:** Block
- Disabled:**  Disable this rule
- Interface:** LAN
- Address Family:** IPv4
- Protocol:** TCP/UDP
- Source:** Source: Network 192.168.1.0 / 24
- Destination:** Destination: Address or Alias YoutubelPList
- Destination Port Range:** any / any
- Extra Options:**
  - Log:**  Log packets that are handled by this rule
  - Description:** Chan mang noi bo truy cap vao Youtube
  - Advanced Options:**  Display Advanced

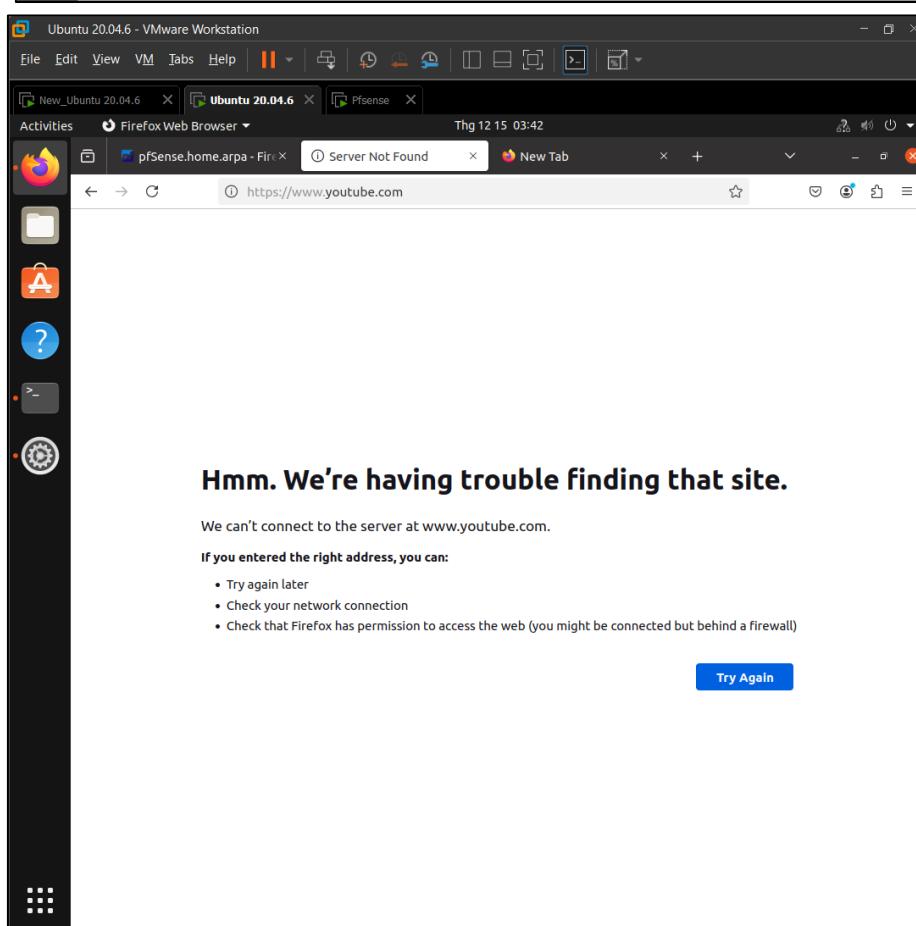
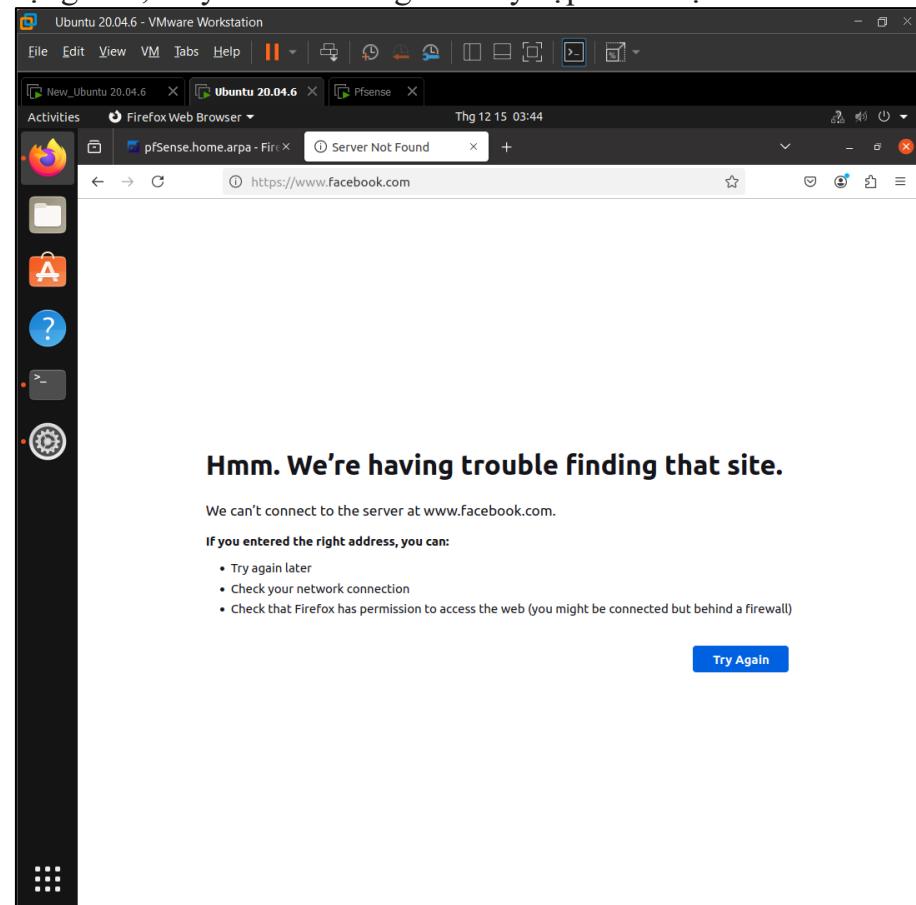
The bottom of the screen displays the pfSense footer: "pfSense is developed and maintained by Netgate. © ESF 2004 - 2024 View license."

- Tiến hành kiểm tra:

+ Trước khi áp dụng rule, vẫn truy cập vào Facebook với Youtube bình thường:



+ Sau khi áp dụng rule, máy VM A không thể truy cập vào được Facebook và Youtube:



**Task 2:**

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

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?

**Trả lời:**

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

- Lệnh đầu tiên để thiết lập SSH tunnel từ máy A đến máy B: **ssh -fN -L 8000:localhost:23 VM\_B\_username@VM\_B\_IP**

- **ssh**: Lệnh SSH để kết nối tới một máy chủ từ xa và thực hiện các thao tác bảo mật qua mạng.
- **-f**: Tham số này yêu cầu SSH chạy ở chế độ nền (background) sau khi xác thực. SSH sẽ tiếp tục làm việc mà không chiếm dụng terminal của bạn.
- **-N**: Tham số này yêu cầu SSH không thực thi bất kỳ lệnh nào trên máy chủ từ xa. Nó chỉ thiết lập kết nối mà không thực thi các lệnh từ xa.
- **-L 8000:localhost:23**: Đây là phần quan trọng của lệnh. Nó tạo ra một **local port forwarding**, nghĩa là:
  - **8000**: Cổng trên máy A (local machine) mà các kết nối sẽ được gửi tới. Khi ta kết nối tới cổng này trên máy A, dữ liệu sẽ được chuyển qua SSH tunnel.
  - **localhost**: Đây là máy chủ mà SSH sẽ chuyển tiếp lưu lượng đến, ở đây là máy B (thực tế là localhost trên máy B).
  - **23**: Cổng của dịch vụ Telnet trên máy B. Lưu lượng đến cổng 8000 trên máy A sẽ được chuyển qua SSH tunnel và đến cổng 23 (Telnet) trên máy B.
- **VM\_B\_username@VM\_B\_IP**: Tài khoản và địa chỉ IP của máy B. Đây là nơi mà SSH sẽ kết nối đến, để tạo một tunnel giữa máy A và máy B.

- Lệnh thứ hai để thực hiện kết nối Telnet: **telnet localhost 8000**

- **localhost**: Đây là địa chỉ máy tính mà ta đang thực hiện kết nối từ. Trong trường hợp này, nó chỉ đến máy A.
- **8000**: Cổng mà ta đã chỉ định trong lệnh SSH trước đó. Khi kết nối đến cổng 8000 trên máy A, các gói dữ liệu sẽ được chuyển tiếp qua SSH tunnel tới máy B trên cổng Telnet (23).

**2. Khi sử dụng lệnh telnet, thực chất các gói tin này có đi qua máy Firewall không? Nếu có, tại sao Firewall không can thiệp vào kết nối 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 không đi qua Firewall của mạng (giữa máy A và máy B) trong trường hợp này. Vì lý do sau:

+ SSH Tunnel là một kết nối mã hóa giữa máy A và máy B thông qua cổng 22 (cổng SSH) của máy B. Khi thiết lập SSH tunnel, tất cả các gói Telnet từ máy A sẽ được mã hóa và gửi qua cổng SSH (cổng 22) đến máy B. Sau khi đến máy B, chúng sẽ được giải mã và chuyển tiếp tới cổng Telnet (cổng 23) trên máy B.

+ Do đó, tất cả dữ liệu Telnet từ máy A sẽ không trực tiếp đi qua các cổng như 23 (cổng Telnet) hay các cổng khác trên máy B. Nó được mã hóa và vận chuyển qua cổng SSH, cổng mà Firewall không can thiệp vào (vì Firewall chủ yếu kiểm tra lưu lượng mạng không mã hóa).

+ Firewall không chặn lưu lượng Telnet trong trường hợp này vì:

- Các gói Telnet đã được mã hóa và đóng gói trong một kết nối SSH.
- Mạng chỉ thấy lưu lượng trên cổng 22 (SSH), và không thể nhận diện được lưu lượng Telnet bên trong.

Task 3:

1. Truy cập website www.facebook.com. Mô tả quá trình bạn quan sát được.
  2. 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?
  3. 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?
- Bonus: Đề xuất giải pháp để phát hiện và ngăn chặn các cách thức vượt qua sự kiểm soát của Firewall trong trường hợp trên.

Trả lời:

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

- Thực hiện truy cập thiết lập SSH tunnel:

```
(kali㉿kali)-[~]
$ ssh -D 9000 -C namphuong11@10.0.2.131
namphuong11@10.0.2.131's password:
Welcome to Ubuntu 20.04.6 LTS (GNU/Linux 5.15.0-124-generic x86_64)

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

 * Introducing Expanded Security Maintenance for Applications.
 Receive updates to over 25,000 software packages with your
 Ubuntu Pro subscription. Free for personal use.
 https://ubuntu.com/pro

Expanded Security Maintenance for Applications is not enabled.

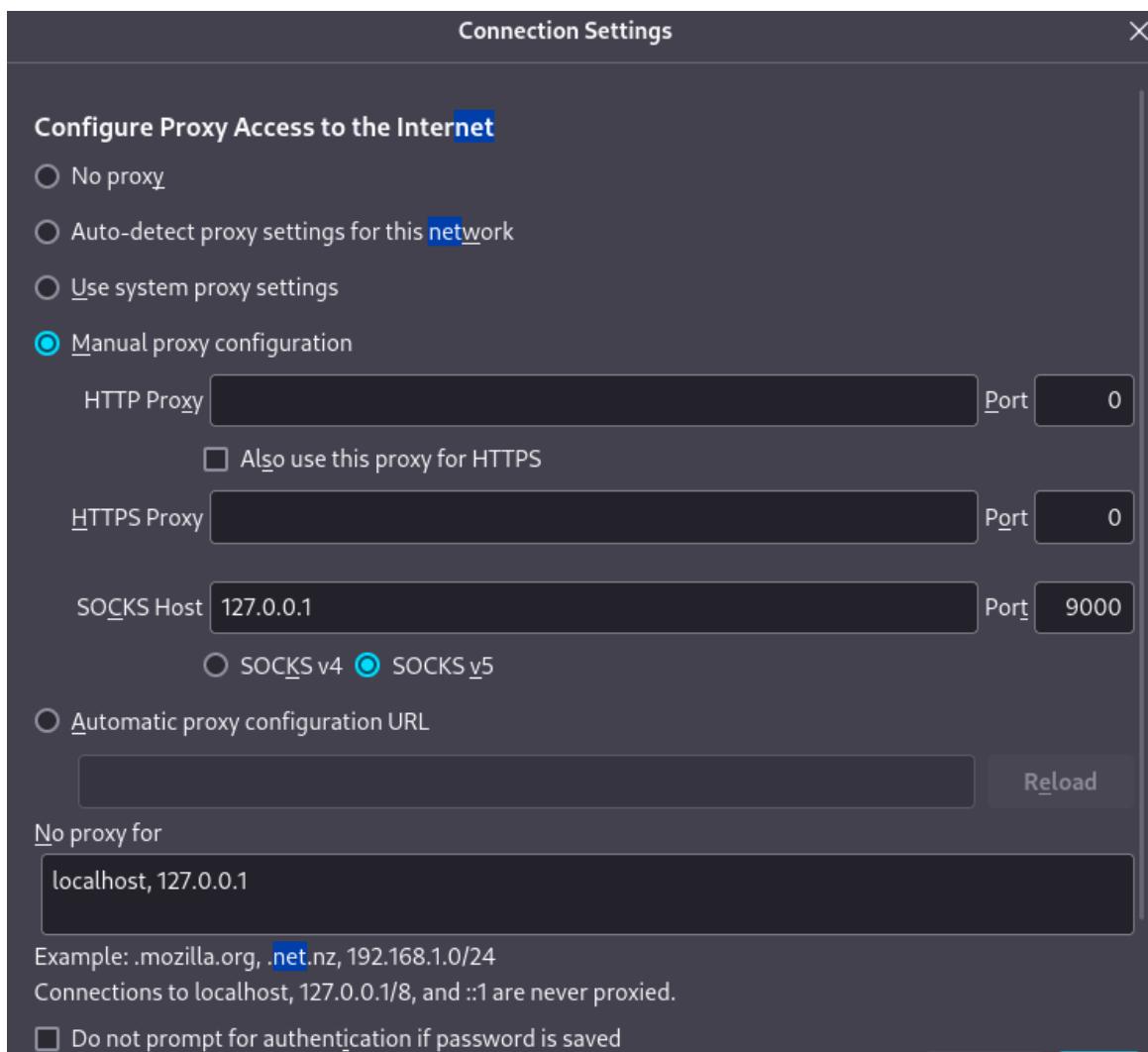
0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

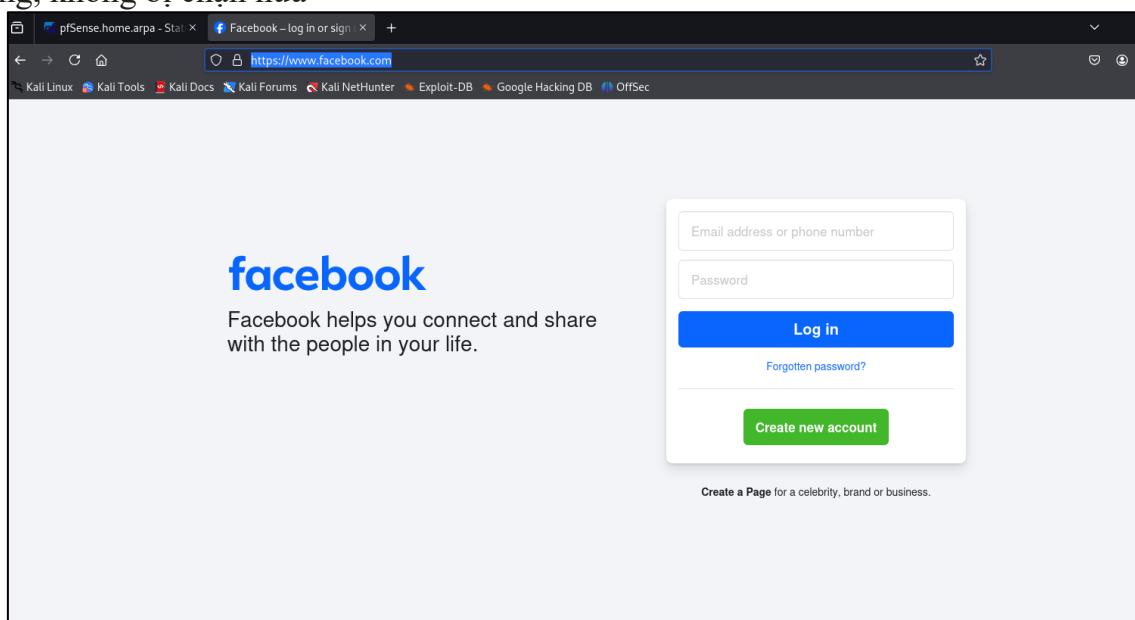
The list of available updates is more than a week old.
To check for new updates run: sudo apt update
New release '22.04.5 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Your Hardware Enablement Stack (HWE) is supported until April 2025.
Last login: Sat Dec 14 16:26:35 2024 from 10.0.2.130
namphuong11@namphuong11-ubuntu:~$ Dec 14 08:59:50      LAN      [2405:4803:b4dc:fa]
```

- Cấu hình Firefox:

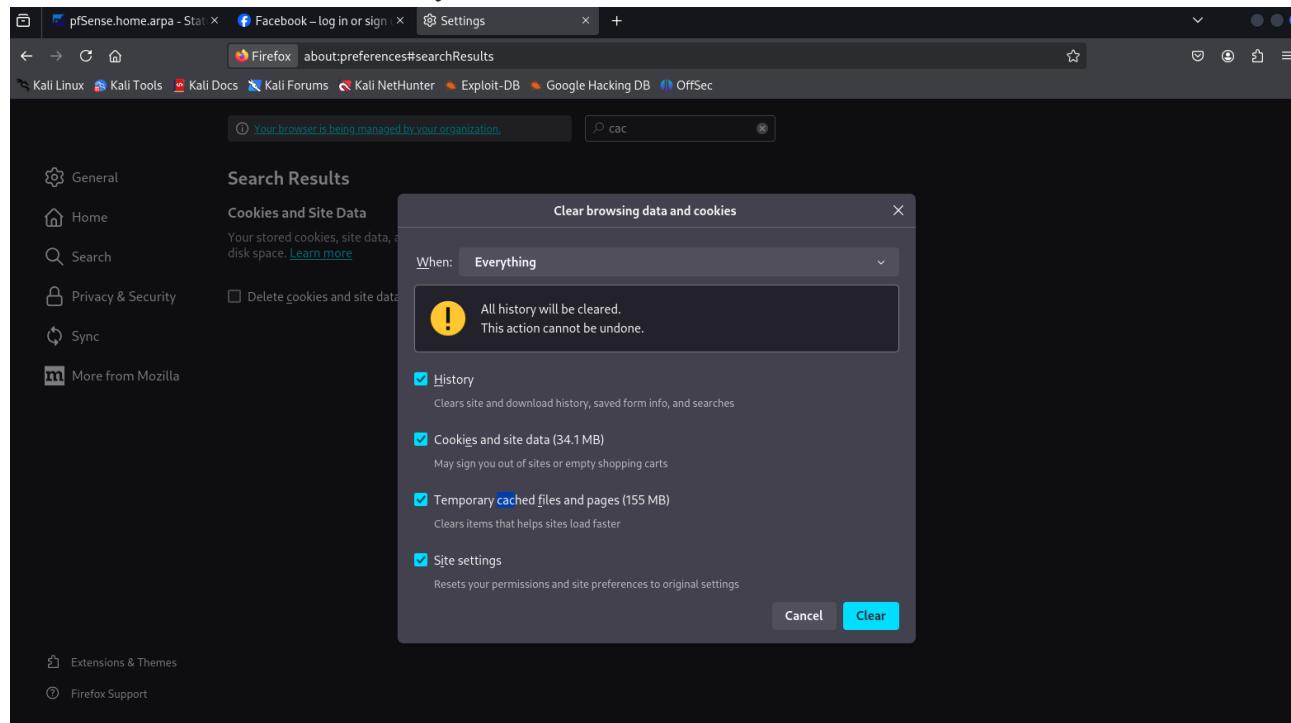


- Sau khi thực hiện các thao tác trên thì ta sẽ truy cập website [www.facebook.com](https://www.facebook.com) bình thường, không bị chặn nữa

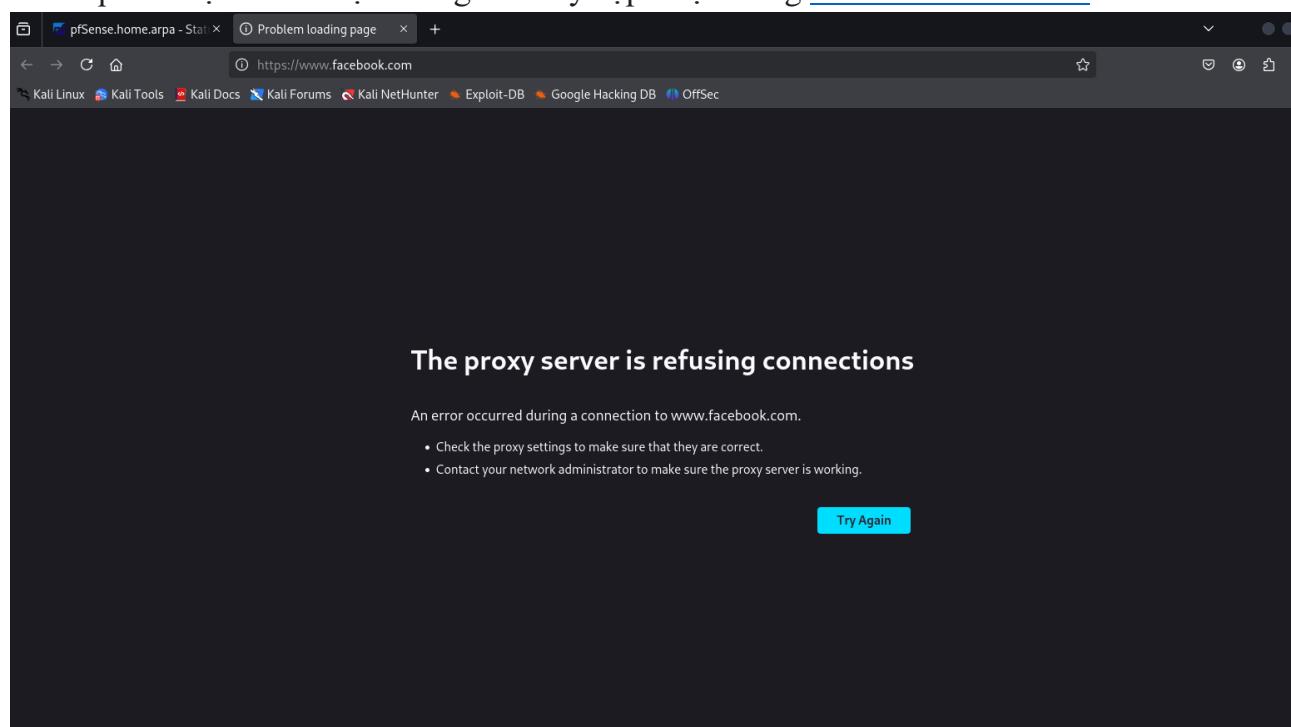


2. Thực hiện ngắt SSH Tunnel, xoá cache của trình duyệt và truy cập lại trang [www.facebook.com](https://www.facebook.com). Lúc này, còn truy cập được trang web Facebook không?

- Thực hiện xóa cache trình duyệt:



- Kết quả trả lại sẽ là ta lại không thể truy cập được trang [www.facebook.com](https://www.facebook.com) nữa



3. 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?

- Thực hiện thêm Rules chặn Port 22

pfSense.home.arpa - Fire □ Problem loading page +

192.168.168.128/firewall\_rules\_edit.php?if=wan&after=-1

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

<b>Action</b>	<input type="text" value="Block"/>					
Choose what to do with packets that match the criteria specified below. Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.						
<b>Disabled</b>	<input type="checkbox"/> Disable this rule Set this option to disable this rule without removing it from the list.					
<b>Interface</b>	<input type="text" value="LAN"/>					
Choose the interface from which packets must come to match this rule.						
<b>Address Family</b>	<input type="text" value="IPv4"/>					
Select the Internet Protocol version this rule applies to.						
<b>Protocol</b>	<input type="text" value="TCP"/>					
Choose which IP protocol this rule should match.						
<b>Source</b>						
<b>Source</b>	<input type="checkbox"/> Invert match	<input type="text" value="Network"/>	<input type="text" value="10.0.2.0"/>	/	24	<input type="button" value="▼"/>
<input type="button" value="Display Advanced"/>						
The Source Port Range for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, any.						
<b>Destination</b>						
<b>Destination</b>	<input type="checkbox"/> Invert match	<input type="text" value="any"/>	<input type="text" value="Destination Address"/>	/	<input type="button" value="▼"/>	
<b>Destination Port Range</b>	<input type="text" value="SSH (22)"/>	<input type="text" value="Custom"/>	<input type="text" value="SSH (22)"/>	<input type="text" value="Custom"/>		
From	Custom	To	Custom			
Specify the destination port or port range for this rule. The 'To' field may be left empty if only filtering a single port.						

- Vì 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

```
namphuong11@namphuong11-ubuntu:~$ ssh -D 9000 -C kali@10.0.2.130
ssh: connect to host 10.0.2.130 port 22: Connection refused
namphuong11@namphuong11-ubuntu:~$ ssh -fN -L 8000:localhost:23 kali@10.0.2.130
ssh: connect to host 10.0.2.130 port 22: Connection refused
namphuong11@namphuong11-ubuntu:~$
```

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

- Ngăn chặn port SSH mặc định (port 22).
  - Theo dõi và quản lý các port lạ trên máy, kiểm tra chức năng các port và đóng các port không cần thiết.
  - Thực hiện kiểm tra định kỳ các chính sách bảo mật và cập nhật tường lửa
  - Tắt tính năng AllowTcpForwarding và GatewayPorts trên SSH server để ngăn Reverse SSH Tunnel
  - Dùng IDS/IPS để phát hiện và ngăn chặn các hành vi xâm nhập vào hệ thống mạng

**Task 4:**

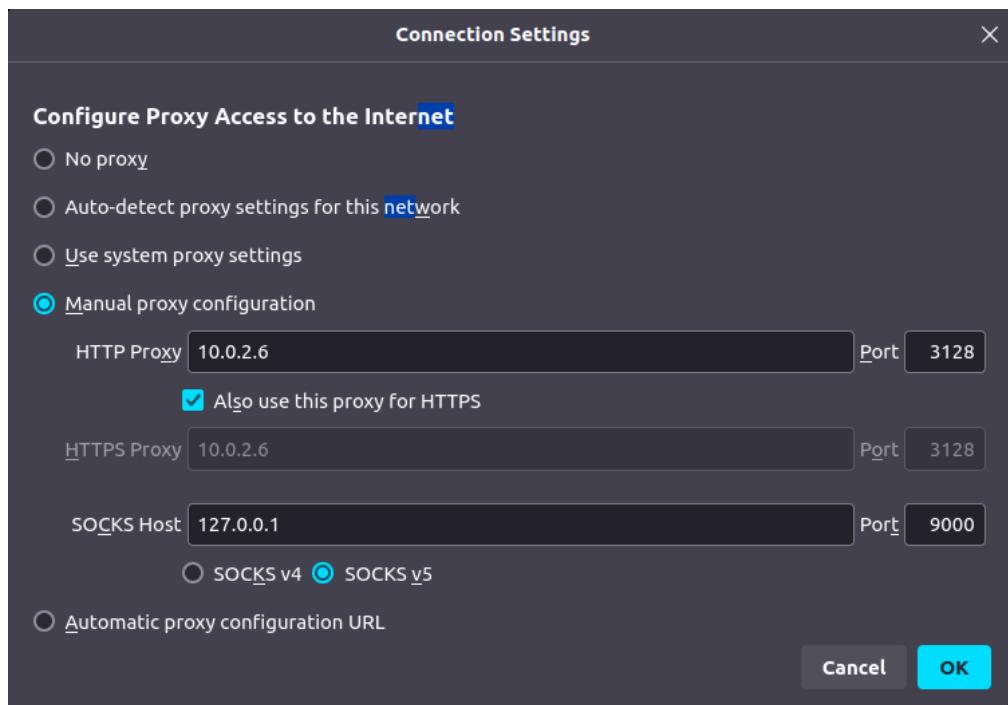
1. Đoạn chương trình script.pl trên hoạt động như thế nào?
2. Thay đổi nội dung đoạn chương trình trên để khi truy cập vào website example.com, một hình ảnh cảnh báo dừng lại xuất hiện (như hình dưới).
3. Thay đổi nội dung chương trình để khi truy cập website, tất cả các hình ảnh đều được thay bằng hình ảnh bạn thích (như hình minh họa dưới).

**Trả lời:**

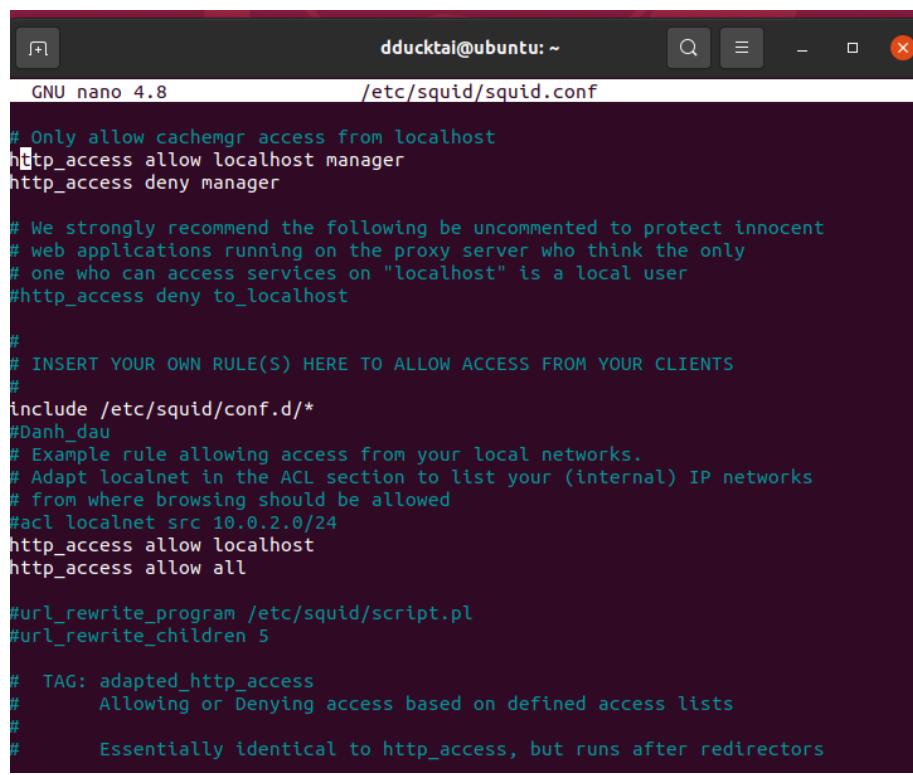
- Cài đặt và cấu hình Squid:

Tên máy	Interface	
	IP	Gateway
VM A	Host-only: 192.168.1.100	192.168.1.2
VM B	NAT: 10.0.2.6	10.0.2.5
pfSense	Host-only: 192.168.1.2	
	NAT: 10.0.2.5	10.0.2.2

+ Trên máy A:



+ Trên máy B:



```

GNU nano 4.8          /etc/squid/squid.conf

# Only allow cachemgr access from localhost
http_access allow localhost manager
http_access deny manager

# We strongly recommend the following be uncommented to protect innocent
# web applications running on the proxy server who think the only
# one who can access services on "localhost" is a local user
#http_access deny to_localhost

#
# INSERT YOUR OWN RULE(S) HERE TO ALLOW ACCESS FROM YOUR CLIENTS
#
include /etc/squid/conf.d/*
#Danh_dau
# Example rule allowing access from your local networks.
# Adapt localnet in the ACL section to list your (internal) IP networks
# from where browsing should be allowed
#acl localnet src 10.0.2.0/24
http_access allow localhost
http_access allow all

#url_rewrite_program /etc/squid/script.pl
#url_rewrite_children 5

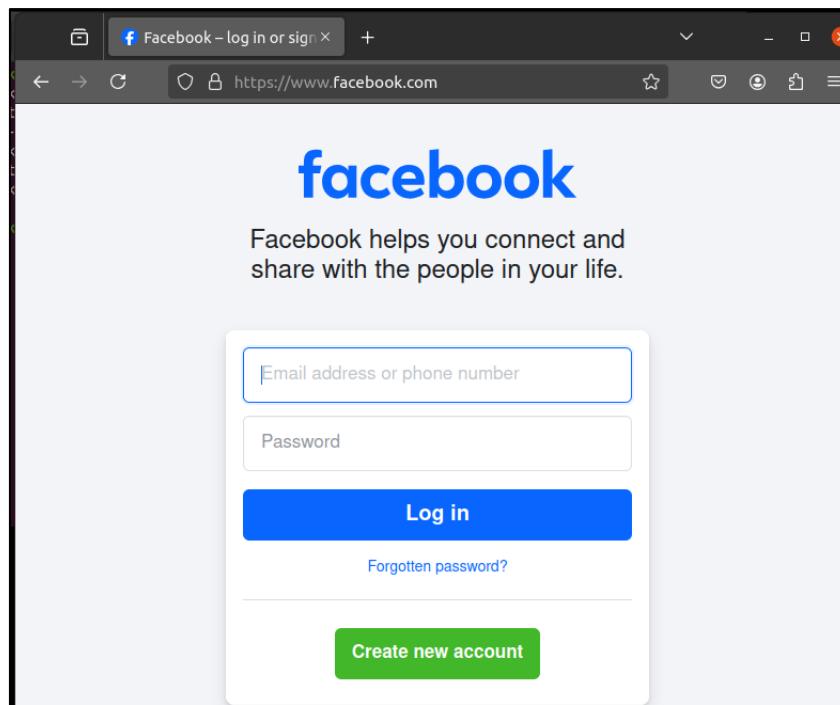
# TAG: adapted_http_access
#     Allowing or Denying access based on defined access lists
#
# Essentially identical to http_access, but runs after redirectors

```

- Sau khi cài đặt và cấu hình Squid xong, ta truy cập được Facebook từ máy A do:

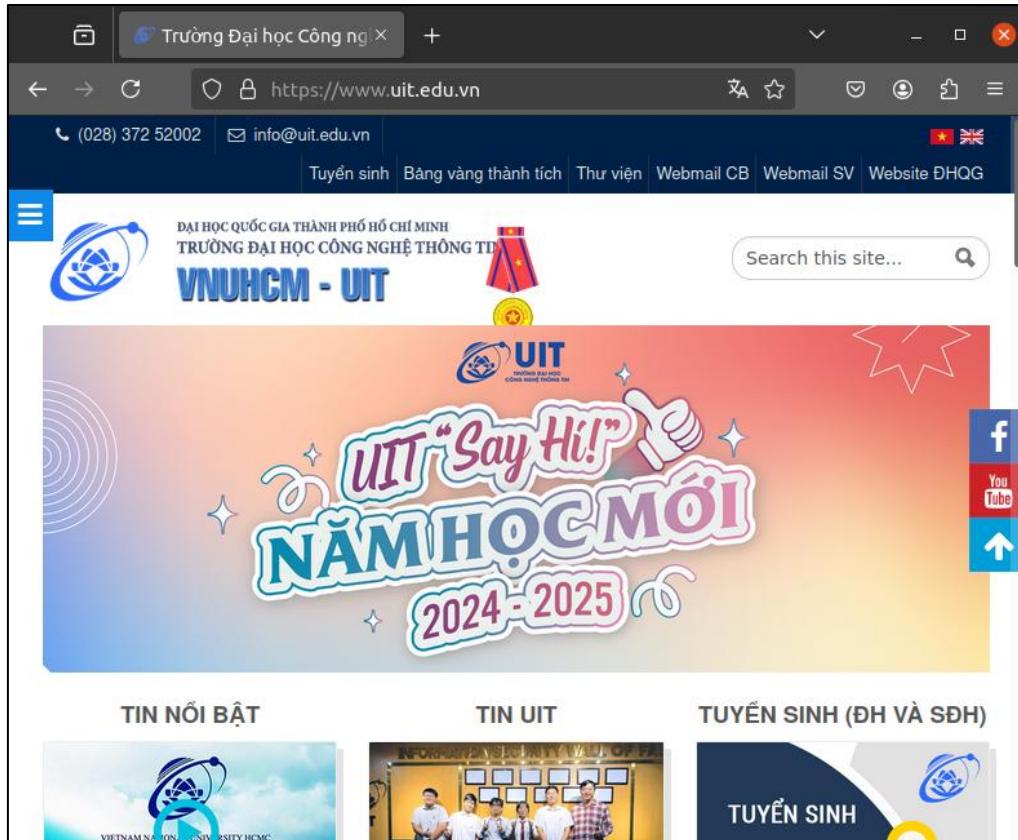
+ Squid không xử lý HTTPS nếu không cấu hình đặc biệt cho SSL, vì vậy, khi truy cập các trang web sử dụng HTTPS (như Facebook), Squid không thể can thiệp vào lưu lượng đó và ta có thể truy cập bình thường.

+ Để chặn HTTPS, cần cấu hình Squid với tính năng SSL Bumping hoặc thực hiện cấu hình tường lửa chặn các kết nối tới các cổng HTTPS (443).



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

- Trên máy A, truy cập vào trang web <http://example.com>, trang web tự động chuyển sang <https://www.uit.edu.vn>



## 1. Đoạn chương trình script.pl trên hoạt động như thế nào?

```
#!/usr/bin/perl -w use strict; use warnings;
```

- use strict;: Yêu cầu tuân thủ các quy tắc chặt chẽ trong việc khai báo và sử dụng biến, giúp tránh lỗi do khai báo nhầm.
- use warnings;: Bật cảnh báo để thông báo lỗi hoặc hành vi bất thường trong mã.

```
select STDOUT; $|=1;
```

- Dòng này yêu cầu chương trình flush (xóa bộ đệm) ngay sau mỗi lần ghi hoặc in ra STDOUT

```
while (<>) { my @parts = split; my $url = $parts[0];
```

- split: Tách đầu vào thành các phần tử theo khoảng trắng, lưu vào mảng @parts
- \$url = \$parts[0]: Lấy phần tử đầu tiên trong mảng (giả định đây là URL)

```
if ($url =~ /example\.com/)
{ # URL Rewriting print "http://www.uit.edu.vn\n"; }
else { # No Rewriting. print "\n"; }
```

- if (\$url =~ /example\.com/): Sử dụng regular expression để kiểm tra xem \$url có chứa chuỗi example.com hay không. Dấu \. dùng để thoát ký tự vì trong biểu thức chính quy, \. có nghĩa là "bất kỳ ký tự nào".

- Nếu khớp (example.com có trong URL): In ra dòng “http://www.uit.edu.vn”.

- Nếu không khớp (example.com không có trong URL): In ra dòng trống.

**Tóm lại, chương trình đọc đầu vào, kiểm tra xem dòng đó có chứa example.com hay không. Nếu có, chương trình thay thế URL bằng "http://www.uit.edu.vn"; Và nếu không phải url "example.com" thì vẫn tới trang web gốc.**

2. 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).

- Ta chỉnh đoạn code lại như sau:

```
#!/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://10.0.2.6/images.png\n";
    }
    else
    {
        # No Rewriting.
        print "\n";
    }
}
```

- Trên máy A, ta mở lại trang <http://example.com>, kết quả là đã chèn hình thành công:



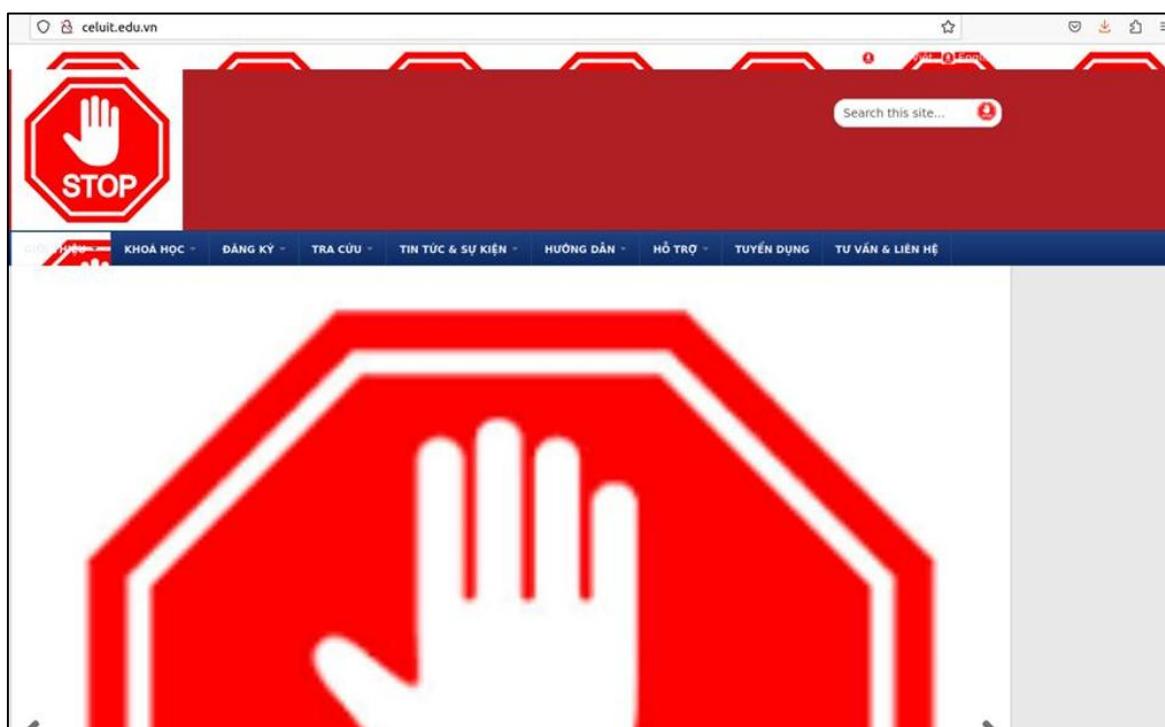
**3. Thay đổi nội dung chương trình để khi truy cập website, tất cả các hình ảnh đều được thay bằng hình ảnh bạn thích (như hình minh họa dưới).**

- Sử dụng website của Trung tâm Ngoại ngữ trường Đại học Công nghệ Thông tin: celuit.edu.vn.

- Ta chỉnh đoạn code lại như sau:

```
#!/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://10.0.2.6/images.png\n";
    }
    else
    {
        # No Rewriting.
        print "\n";
    }
}
```

- Kết quả:



**Task 5:**

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

**Trả lời:**

- 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 nhiều giao thức thiết lập kết nối VPN khác nhau. Các giao thức chính mà pfSense hỗ trợ bao gồm:

**+ IPsec (Internet Protocol Security)****• Đặc điểm:**

- IPsec là một giao thức bảo mật tầng mạng (Layer 3) dùng để bảo vệ và mã hóa các gói tin truyền qua mạng.
- IPsec thường được sử dụng cho các kết nối VPN site-to-site và remote access.
- Giao thức này cung cấp mã hóa, xác thực, và bảo vệ tính toàn vẹn của dữ liệu.
- IPsec sử dụng các thuật toán mã hóa mạnh như AES, DES, và có thể sử dụng X.509 certificates cho xác thực.
- Chế độ Tunnel của IPsec mã hóa toàn bộ gói tin, giúp bảo vệ dữ liệu và giúp mạng dễ dàng vượt qua các tường lửa hoặc NAT (Network Address Translation).

**• Ưu điểm:**

- Bảo mật rất cao, đặc biệt là khi sử dụng với chế độ Tunnel.
- Thiết lập dễ dàng.
- Phổ biến và ổn định, hỗ trợ tốt trong các môi trường doanh nghiệp.

**• Nhược điểm:**

- Cấu hình có thể phức tạp hơn, đặc biệt khi sử dụng với các phương thức xác thực như IPsec certificates.
- Không linh hoạt như các giao thức VPN khác về mặt cấu hình và kết nối.

**+ L2TP over IPsec (Layer 2 Tunneling Protocol)****• Đặc điểm:**

- L2TP là một giao thức tunneling (tạo đường hầm) và khi kết hợp với IPsec sẽ cung cấp tính bảo mật, mã hóa.
- L2TP cung cấp khả năng kết nối giữa hai điểm thông qua tunnel, nhưng nó không mã hóa dữ liệu. Mã hóa và bảo mật được cung cấp bởi IPsec.
- L2TP/IPsec thường được sử dụng cho VPN remote access và có thể vượt qua các NAT devices nhờ tính năng NAT Traversal.

**• Ưu điểm:**

- Đơn giản hơn IPsec về mặt cấu hình, nhưng vẫn đảm bảo mức độ bảo mật cao khi kết hợp với IPsec.

- Thích hợp cho các kết nối từ xa, đặc biệt là khi người dùng ở các mạng có NAT.
- Có thể dễ dàng cấu hình trên nhiều thiết bị và hệ điều hành khác nhau.

**• Nhược điểm:**

- Mặc dù bảo mật cao khi kết hợp với IPsec, nhưng vẫn yêu cầu các thiết lập phức tạp khi so với OpenVPN.
- Kết nối thường có độ trễ cao hơn so với các giao thức khác khi sử dụng IPsec.

**+ OpenVPN****• Đặc điểm:**

- OpenVPN là một giao thức mã nguồn mở rất mạnh mẽ và linh hoạt, hỗ trợ cả TCP và UDP cho kết nối.
- OpenVPN sử dụng SSL/TLS để mã hóa và xác thực, hỗ trợ mã hóa với các thuật toán như AES, RSA.
- Phù hợp cho cả VPN remote access và VPN site-to-site.
- Có khả năng vượt qua các NAT devices nhờ tính năng NAT Traversal, giúp dễ dàng triển khai trên các mạng khác nhau.

**• Ưu điểm:**

- Rất linh hoạt và có khả năng tùy chỉnh cao.
- Bảo mật rất mạnh mẽ và mã nguồn mở, có thể dễ dàng được kiểm tra và cải thiện.
- Dễ dàng triển khai và cấu hình, hỗ trợ nhiều hệ điều hành.
- Hoạt động rất tốt trong môi trường có tường lửa và NAT.

**• Nhược điểm:**

- Cần cài đặt phần mềm OpenVPN client trên thiết bị người dùng (đối với VPN remote access).
- Cấu hình có thể phức tạp khi cần tích hợp vào các hệ thống phức tạp hoặc các thiết bị firewall khác.

- Tóm lại:

+ **IPsec** phù hợp với các môi trường yêu cầu bảo mật cao và kết nối site-to-site hoặc remote access, nhưng yêu cầu cấu hình phức tạp hơn.

+ **L2TP over IPsec** dễ cấu hình hơn IPsec đơn lẻ và thường được sử dụng cho kết nối VPN từ xa.

+ **OpenVPN** là lựa chọn linh hoạt nhất, dễ triển khai và cấu hình, đồng thời bảo mật cao, thích hợp cho cả các môi trường VPN site-to-site và remote access.

2. 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 System -> Package Manager -> Package Installer để tìm và tải package có tên là “openvpn-client-export”

Name	Category	Version	Description
✓ openvpn-client-export	security	1.9.2	Exports pre-configured OpenVPN Client configurations

Package Dependencies:

- [openvpn-client-export-2.6.7](#)
- [openvpn-client-export-2.6.7](#)

- Vào System -> Certificates -> Authorities, nhấn “Add” để thêm chứng chỉ CA. Điền các thông tin vào CA, sau đó nhấn “Save”:

Name	Internal	Issuer	Certificates	Distinguished Name	In Use	Actions
CA_VPN	✓	self-signed	0	ST=Ho Chi Minh, OU=UIT, O=UIT, L=Ho Chi Minh, CN=internal-ca, C=VN	<a href="#">i</a>	<a href="#">Edit</a> <a href="#">Delete</a> <a href="#">Copy</a>

- Vào System -> Certificates -> Certificates, nhấn “Add” để thêm chứng chỉ Server

Server_Cert	CA_VPN	ST=Ho Chi Minh, OU=UIT, O=UIT, L=Ho Chi Minh, CN=forexample, C=VN	<a href="#">i</a>	<a href="#">Edit</a> <a href="#">Delete</a> <a href="#">Copy</a>
-------------	--------	---	-------------------	--

- Khi tạo chứng chỉ xong, ta tiến hành cấu hình VPN, ta vào VPN -> OpenVPN -> Wizard để tiến hành cấu hình. Kết quả:

The screenshot shows the 'OpenVPN Servers' section of the configuration interface. It lists one server entry:

Interface	Protocol / Port	Tunnel Network	Mode / Crypto	Description	Actions
WAN	UDP4 / 1194 (TUN)	10.0.8.0/24	Mode: Remote Access ( SSL/TLS + User Auth ) Data Ciphers: AES-256-GCM, AES-128-GCM, CHACHA20-POLY1305 Digest: SHA256 D-H Params: 4096 bits	OpenVPN	

A green 'Add' button is located at the bottom right.

- Khi tạo Server cho VPN xong, ta tiến hành tạo user:

The screenshot shows the 'OpenVPN Clients' section of the configuration interface. It lists one client entry:

Interface	Protocol	Server	Mode / Crypto	Description	Actions
WAN	UDP4 (TUN)	10.0.2.5:1194	Mode: Peer to Peer ( SSL/TLS ) Data Ciphers: AES-256-GCM, AES-128-GCM, CHACHA20-POLY1305, AES-256-CBC Digest: SHA256	client1	

A green 'Add' button is located at the bottom right.

- Sau khi tái xong, ta vào System -> User Manager -> Users, nhấn “Add” để thêm mới user vào:

The screenshot shows the 'Users' section of the User Manager interface. It lists two users:

Username	Full name	Status	Groups	Actions
admin	System Administrator	✓	admins	
client1		✓		

A green 'Add' button is located at the bottom right.

- Sau khi tạo xong, ta vào VPN -> OpenVPN -> Client export để tiến hành tải file ovpn về, ta sẽ chọn loại “Most Client”:



- Sau khi tải xong, ta gửi file qua máy B và tiến hành cài đặt, ta dùng lệnh:

```
sudo openvpn --config <tên file>.ovpn
```

```
dducktai@ubuntu:~$ sudo openvpn --config /home/dducktai/pfSense-UDP4-1194-vpnuser1.ovpn
Sat Dec 14 22:29:06 2024 WARNING: file 'pfSense-UDP4-1194-vpnuser1-tls.key' is
group or others accessible
Sat Dec 14 22:29:06 2024 OpenVPN 2.4.12 x86_64-pc-linux-gnu [SSL (OpenSSL) ] [L
ZO] [LZ4] [EPOLL] [PKCS11] [MH/PKTINFO] [AEAD] built on Jun 27 2024
Sat Dec 14 22:29:06 2024 library versions: OpenSSL 1.1.1f 31 Mar 2020, LZO 2.1.
0
Enter Auth Username: client1
Enter Auth Password: *****
Sat Dec 14 22:29:58 2024 TCP/UDP: Preserving recently used remote address: [AF
INET]10.0.2.5:1194
Sat Dec 14 22:29:58 2024 UDPv4 link local: (not bound)
Sat Dec 14 22:29:58 2024 UDPv4 link remote: [AF_INET]10.0.2.5:1194
Sat Dec 14 22:29:58 2024 [example] Peer Connection Initiated with [AF_INET]10.0
.2.5:1194
Sat Dec 14 22:29:59 2024 TUN/TAP device tun0 opened
Sat Dec 14 22:29:59 2024 /sbin/ip link set dev tun0 up mtu 1500
Sat Dec 14 22:29:59 2024 /sbin/ip addr add dev tun0 10.0.8.2/24 broadcast 10.0
.8.145
Sat Dec 14 22:29:59 2024 WARNING: this configuration may cache passwords in mem
ory -- use the auth-nocache option to prevent this
Sat Dec 14 22:29:59 2024 Initialization Sequence Completed
```

- Khi cài xong, ta dùng ifconfig để kiểm tra, ta thấy đường hầm vpn đã được thêm thành công:

```
3: tun0: <POINTOPOINT, MULTICAST, NOARP, UP, LOWER_UP> mtu 1500 qdisc fq_codel state UNKNOWN group default qlen 100  
    link/none  
    inet 10.0.8.2/24 brd 10.0.8.255 scope global tun0  
        valid_lft forever preferred_lft forever  
    inet6 fe80 :: b03d:a5c3:ca6c:3c5c/64 scope link stable-privacy  
        valid_lft forever preferred_lft forever
```

- Ta tiến hành ping để kiểm tra kết nối:

```
dducktai@ubuntu:~$ ping 192.168.1.100  
PING 192.168.1.100 (192.168.1.100) 56(84) bytes of data.  
64 bytes from 192.168.1.100: icmp_seq=1 ttl=63 time=0.945 ms  
64 bytes from 192.168.1.100: icmp_seq=1 ttl=63 time=1.014 ms  
64 bytes from 192.168.1.100: icmp_seq=1 ttl=63 time=1.123 ms  
^C
```

----- HẾT -----