

BÁO CÁO THỰC HÀNH

Môn học: An toàn mạng

Tên chủ đề: Linux Firewall Exploration and VPN Tunnel

GVHD: Tô Trọng Nghĩa

Nhóm: 18

1. THÔNG TIN CHUNG:

(Liệt kê tất cả các thành viên trong nhóm)

Lớp: NT140.O11.ANTT.1

STT	Họ và tên	MSSV	Email
1	Nguyễn Lê Thảo Ngọc	21521191	21521191@gm.uit.edu.vn
2	Trần Lê Minh Ngọc	21521195	21521195@gm.uit.edu.vn

2. NỘI DUNG THỰC HIỆN:¹

STT	Nội dung	Tình trạng
1	Yêu cầu 1	100%
2	Yêu cầu 2	100%
3	Yêu cầu 3	70%
4	Yêu cầu 4	70%

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

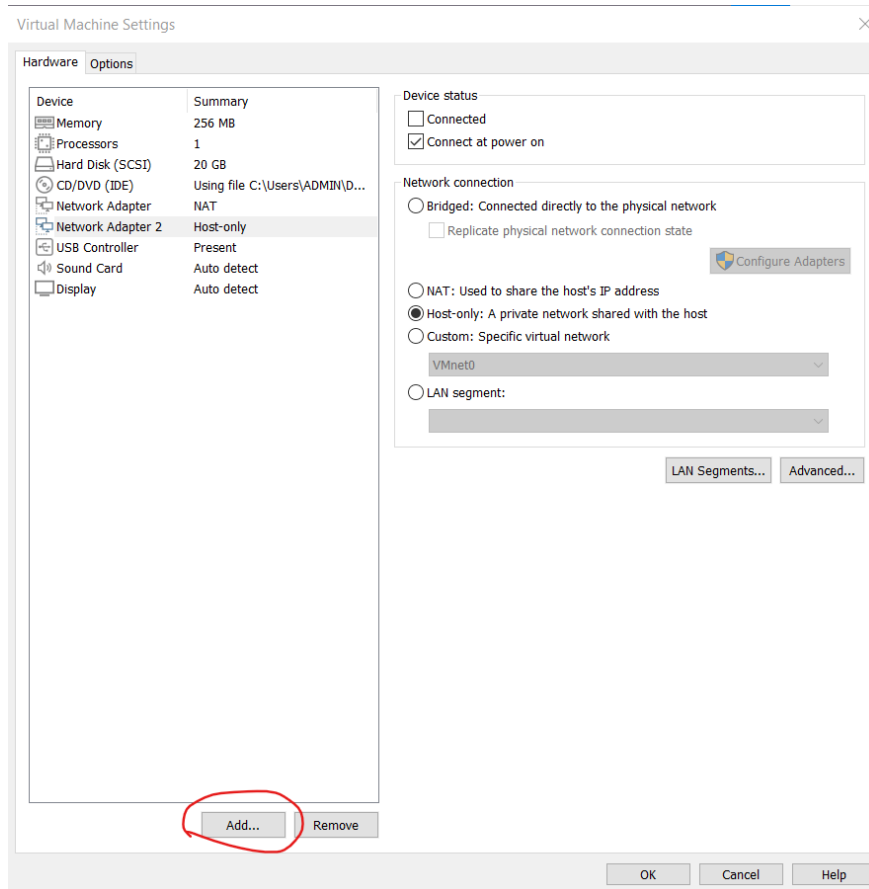
1. Cài đặt pfSense firewall

Tại máy ảo cài đặt Firewall

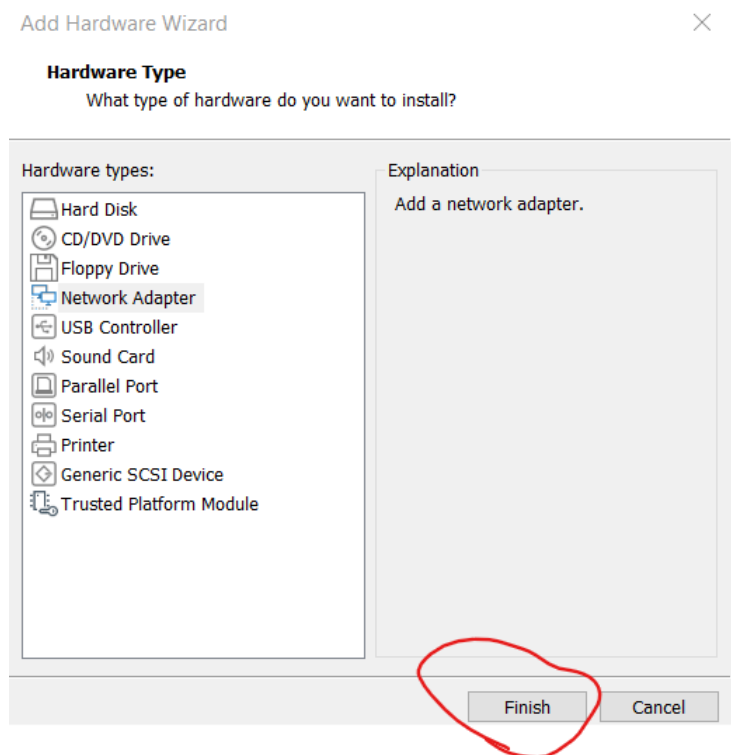
Bước 1: Tạo 2 card mạng (NAT và Host only)

Vì VM (tạo từ file cài đặt pfsense) đã có sẵn card mạng NAT nên chúng ta sẽ chỉ tạo thêm 1 card mạng là Host only.

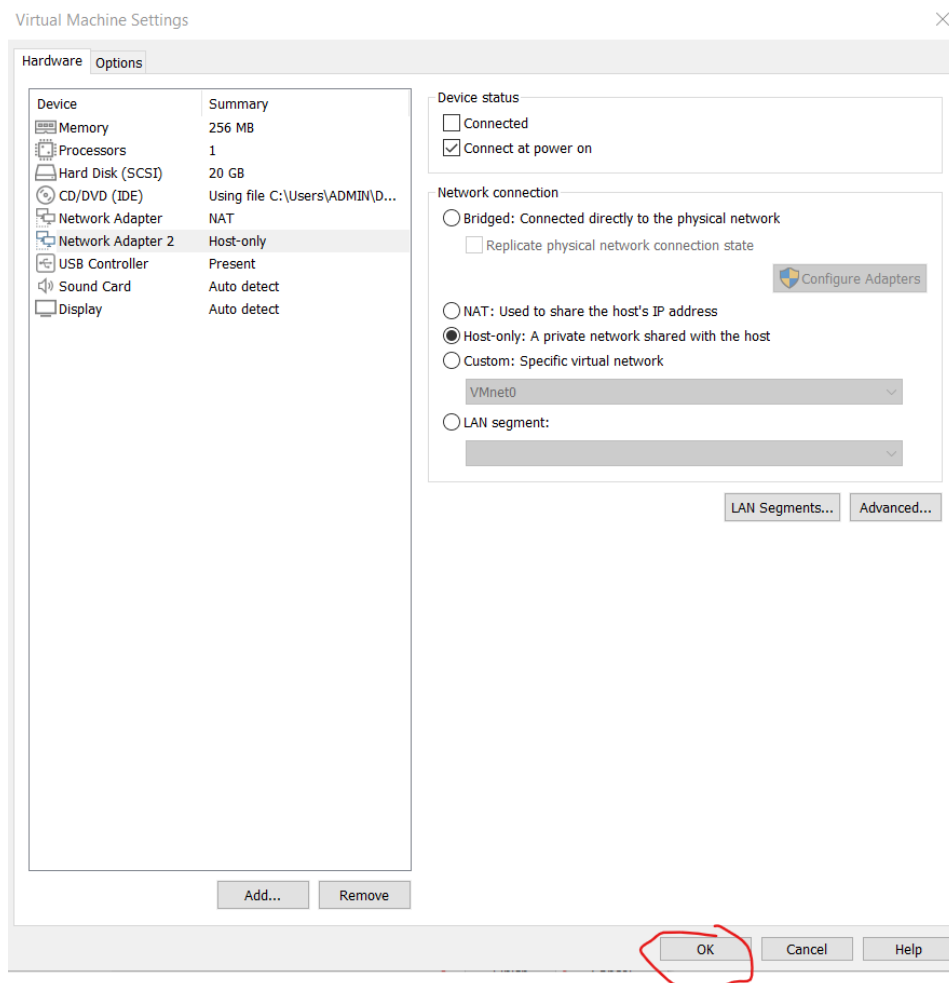
- Chọn Add để thêm 1 Hardware



- Chọn Network Adapter để thêm 1 card mạng -> Chọn Finish để xác nhận



- Chọn loại kết nối Host Only trong mục Network connection



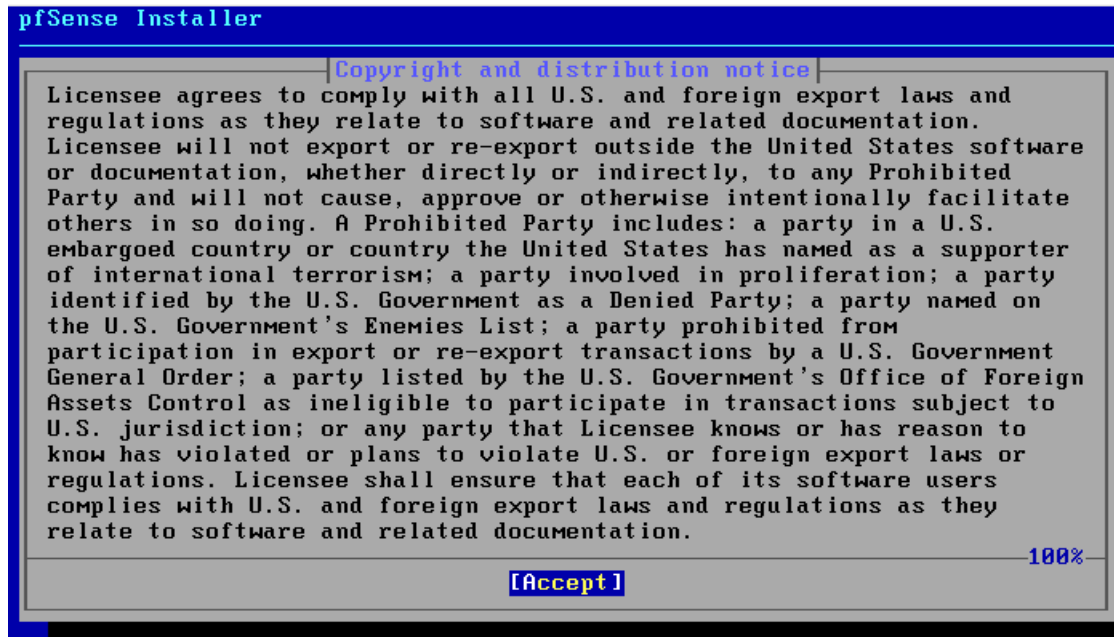
- Xem địa chỉ MAC của card mạng bằng cách chọn mục Network Adapter (mà mình muốn xem), trong bảng thông tin của adapter -> chọn Advanced -> xem mục MAC Address

Bước 2: Reset lại VM và nhấn start để chạy máy ảo

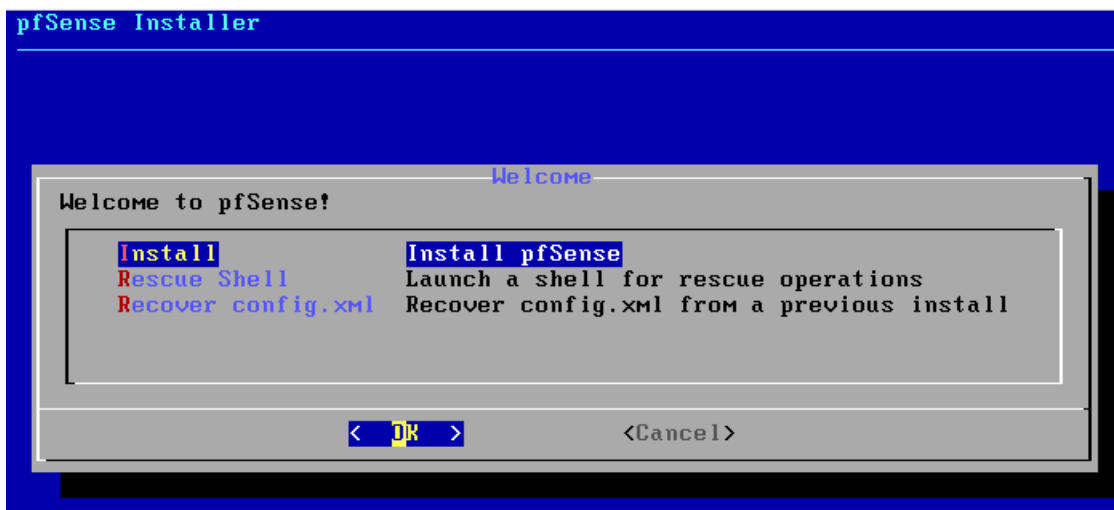
em0: NAT

em1: host only

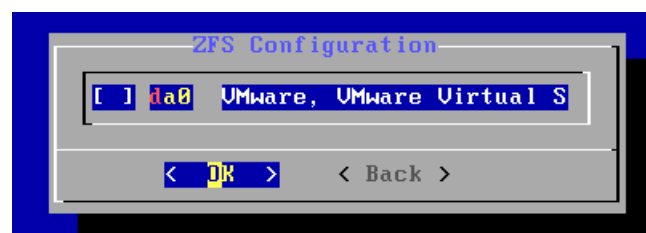
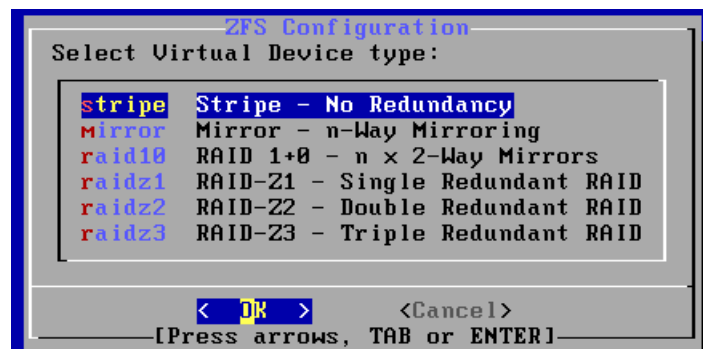
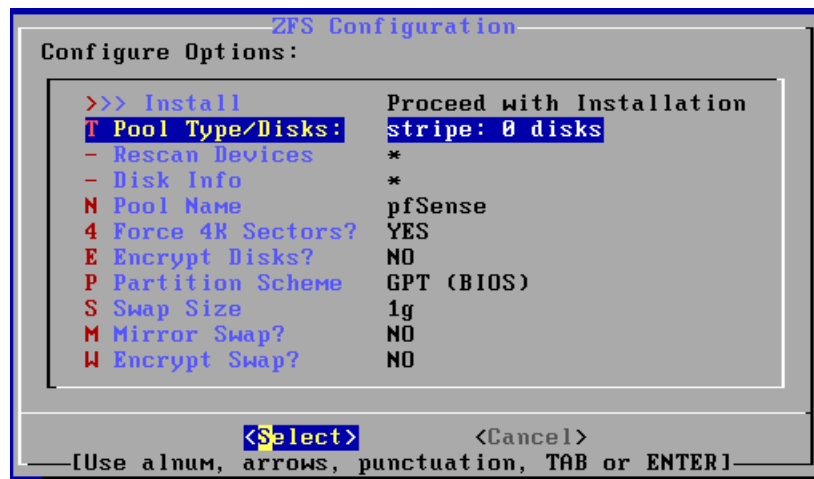
Bước 3: Thực hiện các bước theo hướng dẫn của trình cài đặt. Quá trình cài đặt sẽ yêu cầu khởi động lại để đến bước cấu hình.



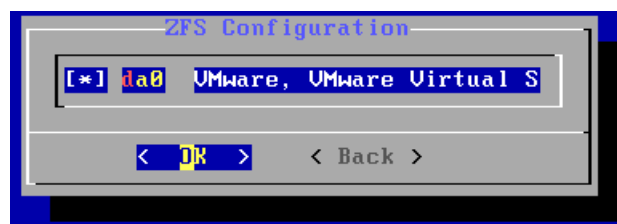
- Chọn Install để cài đặt pfSense firewall



- Chọn auto (ZFS)

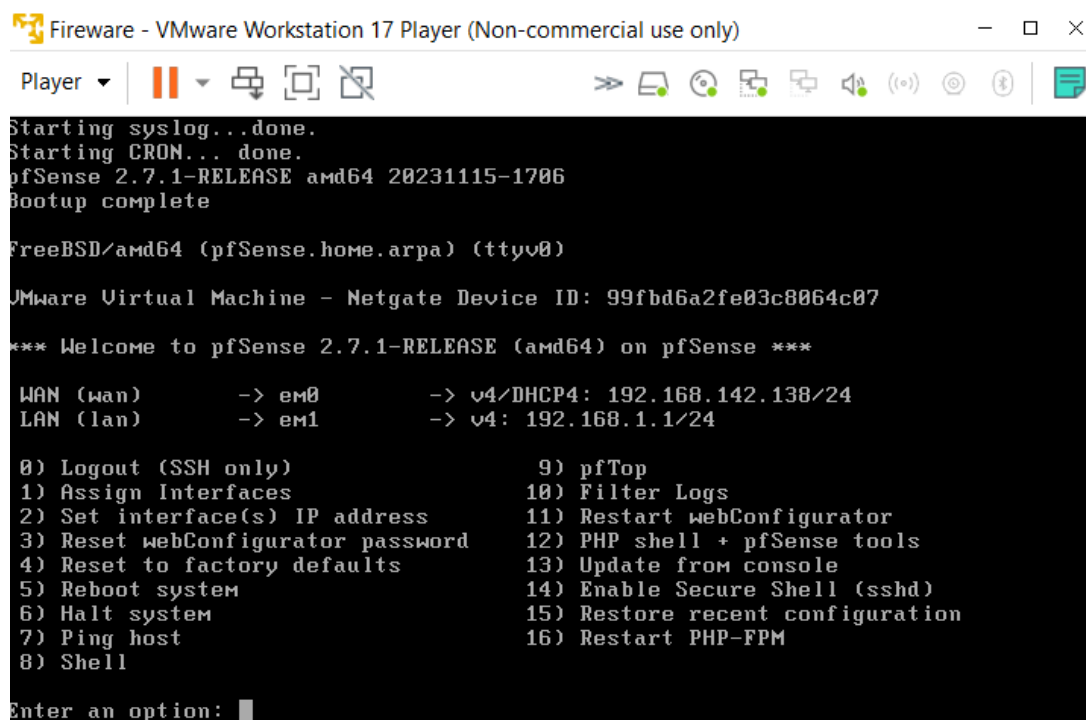


- Nhấn phím cách để chọn 1 drive





Bước 4: Sau khi máy ảo Firewall thực hiện xong việc reboot thì chúng ta thấy giao diện như sau:



Bước 5: Thực hiện đặt lại địa chỉ ip cho các interfaces:

Chọn mục số 2 -> Nhập số tương ứng với Interface cần cấu hình:

- Cấu hình cho WAN:

1. Đặt địa chỉ IP: 10.0.3.2

2. Subnet mask: 24

```
Enter an option: 2
Available interfaces:
1 - WAN (em0 - dhcp, dhcp6)
2 - LAN (em1 - static)
Enter the number of the interface you wish to configure: 1
Configure IPv4 address WAN interface via DHCP? (y/n) n
Enter the new WAN IPv4 address. Press <ENTER> for none:
> 10.0.3.2
Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
     255.255.0.0   = 16
     255.0.0.0     = 8
Enter the new WAN IPv4 subnet bit count (1 to 32):
> 24
For a WAN, enter the new WAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>
```

3. WAN IPv4 upstream gateway address: địa chỉ gateway của mạng NAT (10.0.3.1);

4. Không sử dụng IPv6.

```
For a WAN, enter the new WAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
> 10.0.3.1
Should this gateway be set as the default gateway? (y/n) n
Configure IPv6 address WAN interface via DHCP6? (y/n) n
Enter the new WAN IPv6 address. Press <ENTER> for none:
>
Do you want to enable the DHCP server on WAN? (y/n) n
```

5. Tắt DHCP,

```
Do you want to enable the DHCP server on WAN? (y/n) n
Disabling IPv4 DHCPD...
Disabling IPv6 DHCPD...
Do you want to revert to HTTP as the webConfigurator protocol? (y/n) n
```

- Cấu hình địa chỉ Ipv4 cho LAN

1. Đặt địa chỉ IP: 10.0.3.2

2. Subnet mask: 24

3. WAN IPv4 upstream gateway address: địa chỉ gateway của mạng NAT (10.0.3.1);

```

Enter an option: 2
Available interfaces:
1 - WAN (em0 - static)
2 - LAN (em1 - static)
Enter the number of the interface you wish to configure: 2
Configure IPv4 address LAN interface via DHCP? (y/n) n
Enter the new LAN IPv4 address. Press <ENTER> for none:
> 192.168.3.2
Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
     255.255.0.0   = 16
     255.0.0.0     = 8
Enter the new LAN IPv4 subnet bit count (1 to 32):
> 24
For a WAN, enter the new LAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>

```

4. Không sử dụng IPv6.

5. Tắt DHCP,

```

Enter the new LAN IPv6 address. Press <ENTER> for none:
>
Do you want to enable the DHCP server on LAN? (y/n) n
Disabling IPv4 DHCPD...
Disabling IPv6 DHCPD...
Do you want to revert to HTTP as the webConfigurator protocol? (y/n) n

Do you want to enable the DHCP server on LAN? (y/n) n
Disabling IPv4 DHCPD...
Disabling IPv6 DHCPD...
Do you want to revert to HTTP as the webConfigurator protocol? (y/n) n

Please wait while the changes are saved to LAN...
Reloading filter...
Reloading routing configuration...
DHCPD...

The IPv4 LAN address has been set to 192.168.3.2/24
You can now access the webConfigurator by opening the following URL in your web
browser:
      https://192.168.3.2/
Press <ENTER> to continue.

```

Bước 6: Kiểm tra lại IP của interface wan và lan. Sau đó reboot để hiện thực những thay đổi


```

The IPv4 LAN address has been set to 192.168.3.2/24
You can now access the webConfigurator by opening the following URL in your web
browser:
    http://192.168.3.2/

Press <ENTER> to continue.
VMware Virtual Machine - Netgate Device ID: 894d5fb3331b2922db44

*** Welcome to pfSense 2.7.1-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4: 10.0.3.2/24
LAN (lan)      -> em1      -> v4: 192.168.3.2/24

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

```

- Thực hiện reboot lại

```

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: 5

```

Bước 7: Thiết lập IP mới cho máy VM A

Bên VM A (OS:Ubuntu):

- Thực hiện cấu hình lại IP:

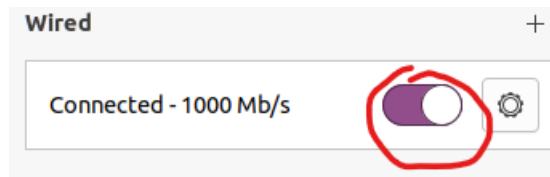
Vào mục Network -> chọn setting (biểu tượng bánh răng)

The screenshot shows the 'Wired' network configuration window. The 'IPv4' tab is active. Under 'IPv4 Method', the 'Manual' option is selected. The 'Addresses' section contains a table with the following data:

Address	Netmask	Gateway
192.168.3.3	255.255.255.0	192.168.3.2

In the 'DNS' section, the 'Automatic' toggle is turned on, and the DNS server is set to 8.8.8.8.

- Sau khi nhấn Apply để lưu cấu hình thì khởi động lại kết nối bằng cách bật và tắt công tắc



- Kiểm tra kết nối

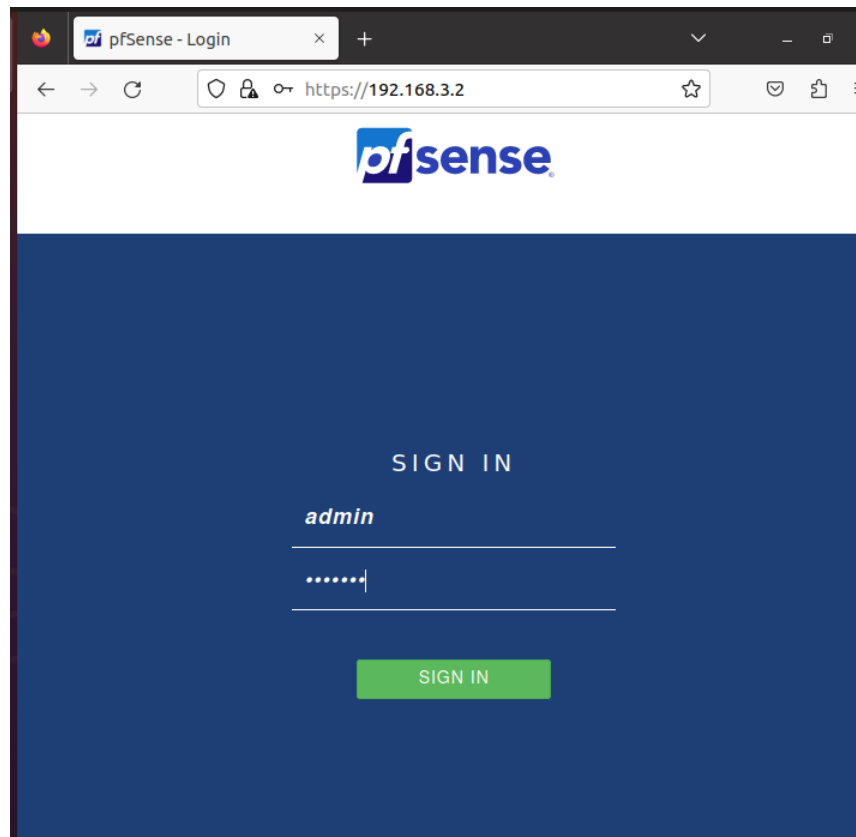
```
test@ubuntu:~/Desktop$ ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.3.3 netmask 255.255.255.0 broadcast 192.168.3.255
    inet6 fe80::b:f52:4757:99e3 prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:3a:5b:c2 txqueuelen 1000 (Ethernet)
    RX packets 1578 bytes 136325 (136.3 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 2127 bytes 183173 (183.1 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 2881 bytes 235810 (235.8 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 2881 bytes 235810 (235.8 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

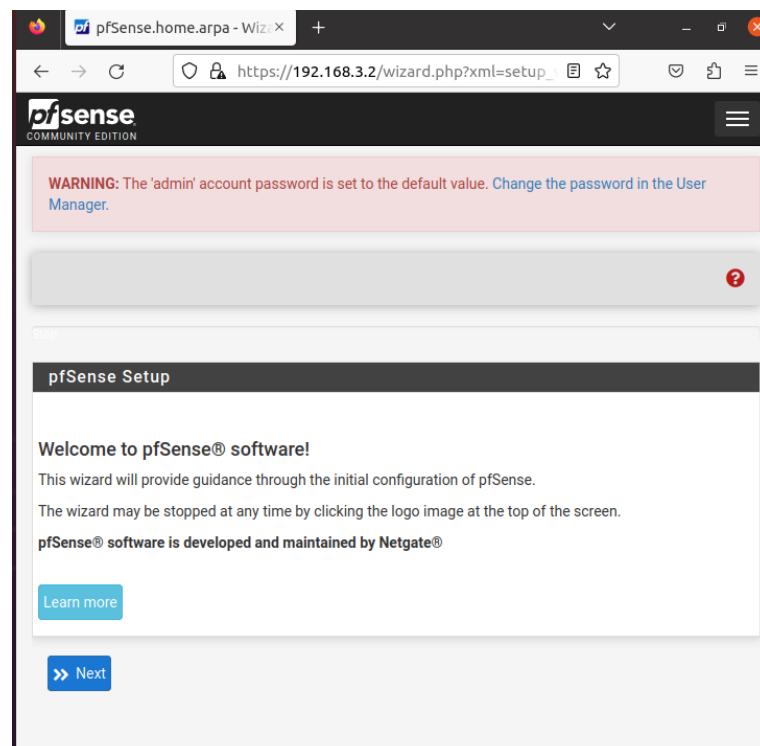
- Ping từ VM A tới interface HostOnly của Firewall

```
test@ubuntu:~/Desktop$ ping 192.168.3.2
PING 192.168.3.2 (192.168.3.2) 56(84) bytes of data.
64 bytes from 192.168.3.2: icmp_seq=1 ttl=64 time=0.395 ms
64 bytes from 192.168.3.2: icmp_seq=2 ttl=64 time=0.549 ms
64 bytes from 192.168.3.2: icmp_seq=3 ttl=64 time=0.434 ms
^Z
[ Show Applications          ping 192.168.3.2
t sktop$
```

- Truy cập trang quản trị: Trên máy VM A, mở trình duyệt web và truy cập đến địa chỉ <http://192.168.3.2>
- Mở browser và nhập URL: <https://192.168.3.2/>



- Đăng nhập vào trang web với tài khoản mặc định:
account: admin
password: pfsense
- Giao diện web chính:



- Cấu hình cho pfsense tại các trường sau:

System

Hostname

Name of the firewall host, without domain part.

Domain

Domain name for the firewall.

Do not end the domain name with '.local' as the final part (Top Level Domain, TLD). The 'local' TLD is **widely used** by mDNS (e.g. Avahi, Bonjour, Rendezvous, Airprint, Airplay) and some Windows systems and networked devices. These will not network correctly if the router uses 'local' as its TLD. Alternatives such as 'home.arpa', 'local.lan', or 'mylocal' are safe.

DNS Server Settings

DNS Servers

DNS Hostname

Delete

Address
Enter IP addresses to be used by the system for DNS resolution. These are also used for the DHCP service, DNS Forwarder and DNS Resolver when it has DNS Query Forwarding enabled.
DNS Hostname
Hostname
Enter the DNS Server Hostname for TLS Verification in the DNS Resolver (optional).
Delete

Localization

Timezone

Asia/Ho_Chi_Minh

Select a geographic region name (Continent/Location) to determine the timezone for the firewall. Choose a special or "Etc" zone only in cases where the geographic zones do not properly handle the clock offset required for this firewall.

Timeservers

2.pfsense.pool.ntp.org

Use a space to separate multiple hosts (only one required). Remember to set up at least one DNS server if a host name is entered here!

Language

English

Choose a language for the webConfigurator

RFC1918 Networks

Block RFC1918 Private Networks

☐ Block private networks from entering via WAN

When set, this option blocks traffic from IP addresses that are reserved for private networks as per RFC 1918 (10/8, 172.16/12, 192.168/16) as well as loopback addresses (127/8). This option should generally be left turned on, unless the WAN network lies in such a private address space, too.

Block bogon networks

Block bogon networks

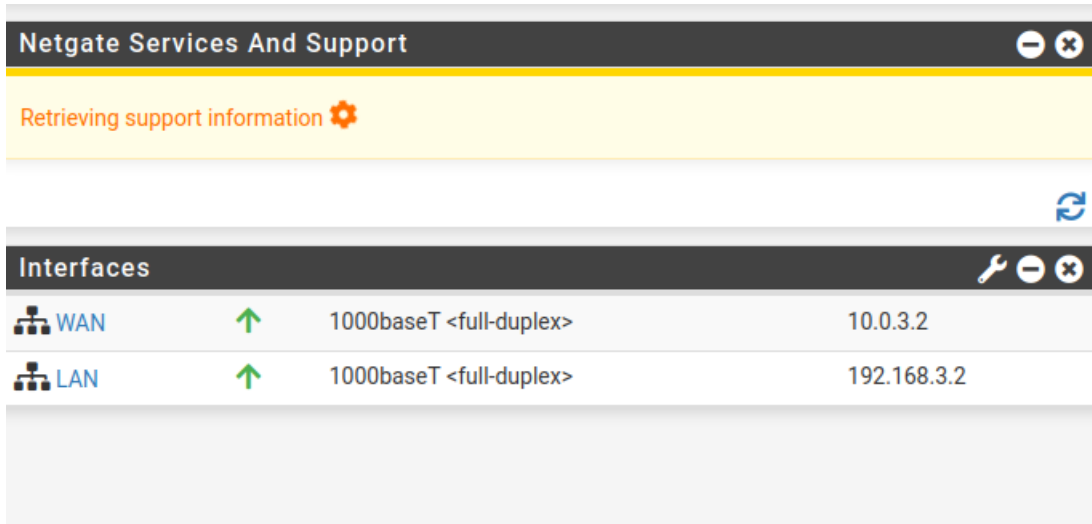
☒ Block non-Internet routed networks from entering via WAN

When set, this option blocks traffic from IP addresses that are reserved (but not RFC 1918) or not yet assigned by IANA. Bogons are prefixes that should never appear in the Internet routing table, and obviously should not appear as the source address in any packets received.

- Chọn Save để lưu cấu hình

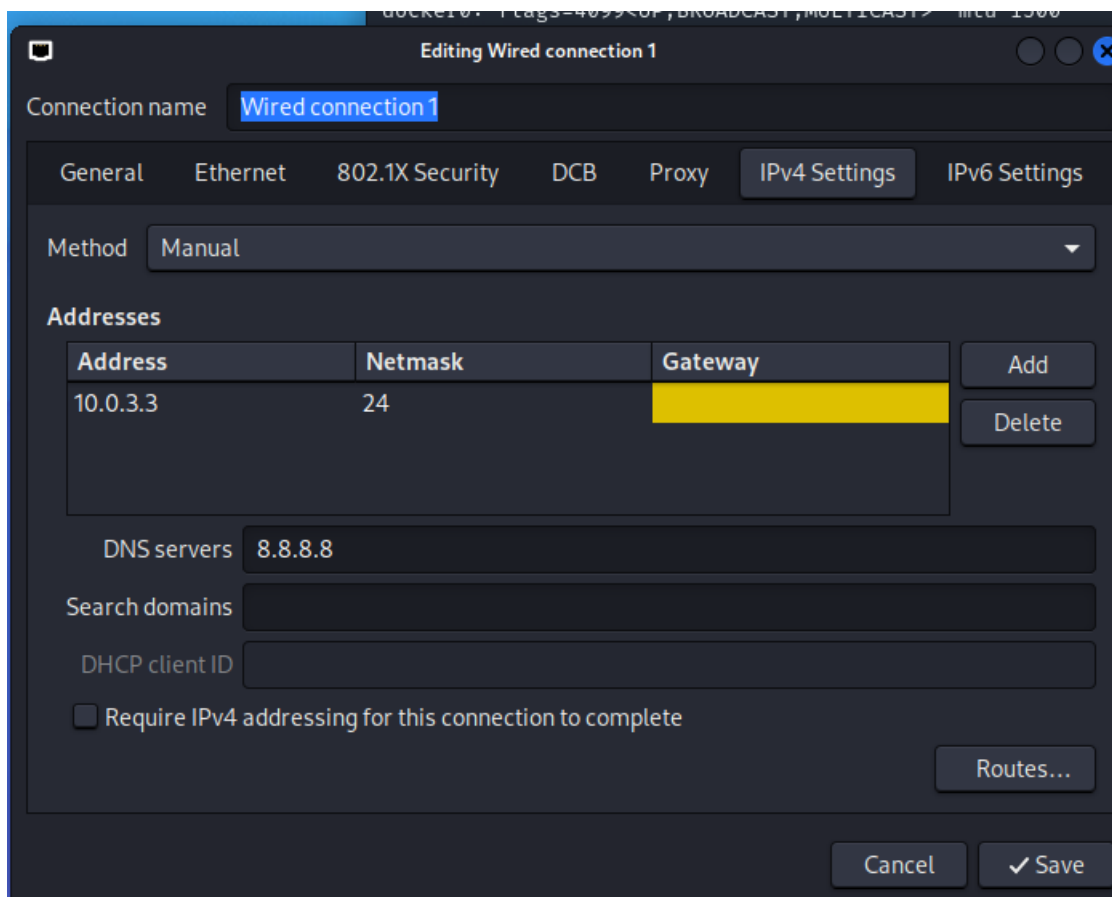
The screenshot shows the pfSense web interface in a browser window. The address bar shows the URL `https://192.168.3.2/system.php`. The page content includes several sections: 'Alias Poupups' with a checkbox 'Disable details in alias popups', 'Disable dragging' with a checkbox 'Disable dragging of firewall/NAT rules', 'Login page color' with a dropdown menu set to 'Dark Blue', and 'Login hostname' with a checkbox 'Show hostname on login banner'. At the bottom left, a blue 'Save' button with a floppy disk icon is circled in red.

- Vô trang Dashboard để xem thông tin cấu hình Firewall

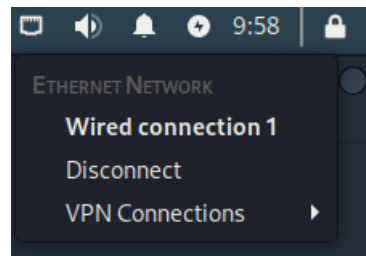


Bên VM B (OS:KalilLinux):

- Thực hiện cấu hình lại IP
- Vô mục Network Connections-> chọn 1 cổng Ethernet
- Cấu hình ipv4



- Sau khi nhấn Save để lưu cấu hình thì khởi động lại kết nối bằng disconnect rồi connect lại



- Kiểm tra kết nối

```
(bun@kali)-[~]
$ ifconfig
docker0: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
    inet 172.17.0.1 netmask 255.255.0.0 broadcast 172.17.255.255
    ether 02:42:6d:b6:b9:03 txqueuelen 0 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.0.3.3 netmask 255.255.255.0 broadcast 10.0.3.255
    inet6 fe80::e23f:ddee:b5ab:895f prefixlen 64 scopeid 0<link>
    ether 00:0c:29:64:0b:77 txqueuelen 1000 (Ethernet)
    RX packets 219 bytes 24285 (23.7 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 68 bytes 13526 (13.2 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

- Ping từ VM A tới VM B

```
test@ubuntu:~/Desktop$ 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=0.774 ms
64 bytes from 10.0.3.3: icmp_seq=2 ttl=63 time=0.901 ms
64 bytes from 10.0.3.3: icmp_seq=3 ttl=63 time=0.806 ms
64 bytes from 10.0.3.3: icmp_seq=4 ttl=63 time=0.986 ms
^Z
[ Show Applications ] ping 10.0.3.3
```

- Ping từ VM B tới VM A

```
(bun@kali)-[~]
$ ping 192.168.3.3
PING 192.168.3.3 (192.168.3.3) 56(84) bytes of data.
From 10.0.3.3 icmp_seq=1 Destination Host Unreachable
From 10.0.3.3 icmp_seq=2 Destination Host Unreachable
From 10.0.3.3 icmp_seq=3 Destination Host Unreachable
From 10.0.3.3 icmp_seq=4 Destination Host Unreachable
From 10.0.3.3 icmp_seq=5 Destination Host Unreachable
From 10.0.3.3 icmp_seq=6 Destination Host Unreachable
^Z
zsh: suspended ping 192.168.3.3
```

**Vì nhóm dùng VMware Players nên không cấu hình mạng cho VMware được do đó nhóm sẽ dùng DHCP ip

Máy ảo	Interfaces	Thông tin
Firewall	NAT 192.168.142.139/24 Gateway: 192.168.142.1	Cài đặt pfSense (hướng dẫn trong phần 1 – Nội dung thực hành) sử dụng 2 card mạng: Card NAT: dùng để kết nối ra internet; Card Host Only: để kết nối đến VM A
	Host Only 192.168.3.2/24	
VM A	Host Only 192.168.3.3/24 Gateway: 192.168.3.2	Hệ điều hành Ubuntu (khuyến khích phiên bản 18.04 trở lên) sử dụng card mạng Host Only để kết nối đến máy Firewall.
VM B	NAT 192.168.142.3/24	Hệ điều hành Ubuntu (khuyến khích phiên bản 18.04 trở lên) sử dụng card mạng NAT để kết nối đến Internet. Cài đặt thêm telnetd và ssh (server).

- Thực hiện lại các bước config firewall như trước đó chỉ thay đổi IP thôi

```

VMware Virtual Machine - Netgate Device ID: bb125bd30f2e159cabf6
*** Welcome to pfSense 2.7.1-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4/DHCP4: 192.168.142.139/24
LAN (lan)      -> em1      -> v4: 192.168.3.2/24

```

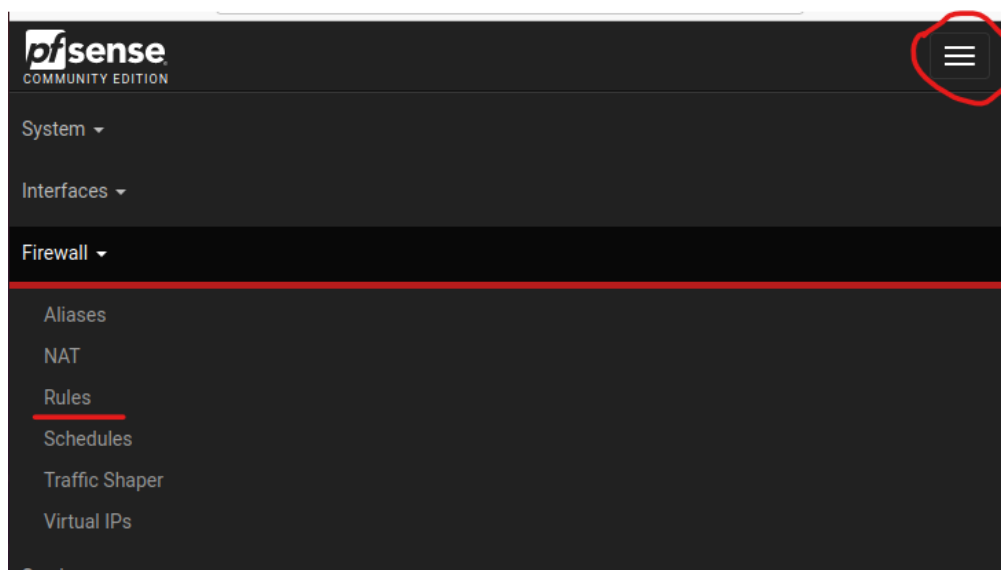
2. Thiết lập chính sách trên Firewall để bảo vệ mạng nội bộ

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.

Máy VM A:

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



- Nhấn Add để thêm 1 rule

Floating WAN LAN

Rules (Drag to Change Order)

Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
	LAN Address	443 80	*	*		Anti-Lockout Rule	
*	*	*	*	none		Default allow LAN to any rule	
*	*	*	*	none		Default allow LAN IPv6 to any rule	

Add
 Add
 Delete
 Toggle
 Copy
 Save
 Separator

- Thêm rule có nội dung như sau:

Edit

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

ICMP

Choose which IP protocol this rule should match.

ICMP Subtypes

any

Alternate Host
Datagram conversion error
Echo reply

For ICMP rules on IPv4, one or more of these ICMP subtypes may be specified.

Source

Source ☐ Invert match Network 192.168.3.0 / 24

Destination

Destination ☐ Invert match Address or Alias 192.168.142.3 /

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 Prevent hosts in net 192.168.3.0 ping to VM B
A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.

Advanced Options [Display Advanced](#)

[Save](#)

- Chọn Save để lưu
- Hiện thực các thay đổi bằng cách nhấn Apply Changes

pfSense
COMMUNITY EDITION

WARNING: The 'admin' account password is set to the default value. [Change the password in the User Manager.](#)

LAN

The firewall rule configuration has been changed.
The changes must be applied for them to take effect. [Apply Changes](#)

Floating WAN LAN

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	
<input checked="" type="checkbox"/>	1/2.08 MiB	*	*	*	LAN Address	443 80	*	*		
<input type="checkbox"/>	0/0 B	IPv4 ICMP any	192.168.3.0/24	*	10.0.3.3/24	*	*	none		
<input type="checkbox"/>	14/363 KiB	IPv4 *	LAN subnets	*	*	*	*	none		
<input type="checkbox"/>	0/0 B	IPv6 *	LAN subnets	*	*	*	*	none		

[Add](#) [Add](#) [Delete](#) [Toggle](#) [Copy](#) [Save](#) [Separator](#)

[i](#)

- Trước khi áp dụng rule

```

rtt min/avg/max/mdev = 0.347/1.343/2.122/0.302 ms
u@ubuntu:/etc/netplan$ ping 192.168.142.3
PING 192.168.142.3 (192.168.142.3) 56(84) bytes of data.
 64 bytes from 192.168.142.3: icmp_seq=1 ttl=63 time=0.422 ms
 64 bytes from 192.168.142.3: icmp_seq=2 ttl=63 time=0.945 ms
 64 bytes from 192.168.142.3: icmp_seq=3 ttl=63 time=0.350 ms
 64 bytes from 192.168.142.3: icmp_seq=4 ttl=63 time=0.463 ms
 64 bytes from 192.168.142.3: icmp_seq=5 ttl=63 time=0.397 ms
 64 bytes from 192.168.142.3: icmp_seq=6 ttl=63 time=1.20 ms
 64 bytes from 192.168.142.3: icmp_seq=7 ttl=63 time=0.406 ms
 64 bytes from 192.168.142.3: icmp_seq=8 ttl=63 time=1.66 ms
 64 bytes from 192.168.142.3: icmp_seq=9 ttl=63 time=1.59 ms
 64 bytes from 192.168.142.3: icmp_seq=10 ttl=63 time=0.367 ms
^C
--- 192.168.142.3 ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9133ms
rtt min/avg/max/mdev = 0.350/0.779/1.658/0.499 ms
u@ubuntu:/etc/netplan$

```

=> 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

```

rtt min/avg/max/mdev = 0.107/0.809/2.055/1.055 ms
u@ubuntu:/etc/netplan$ ping 192.168.142.3
PING 192.168.142.3 (192.168.142.3) 56(84) bytes of data.
^C
--- 192.168.142.3 ping statistics ---
43 packets transmitted, 0 received, 100% packet loss, time 43005ms
u@ubuntu:/etc/netplan$

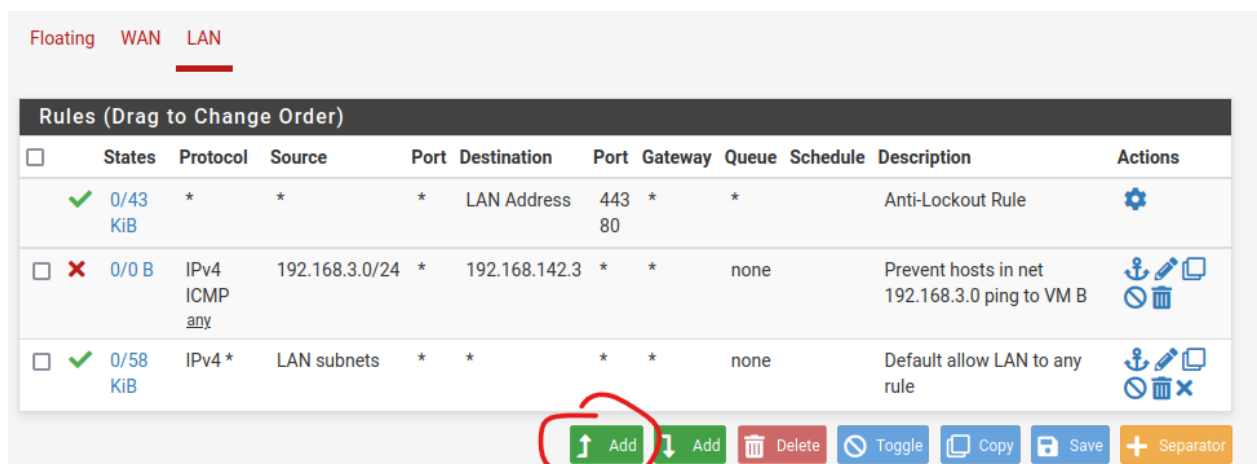
```

=> Không còn ping được nữa

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



- Thêm rule có nội dung như sau:

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

☐ Invert match

Network

192.168.3.0 / 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

☐ Invert match

Any

Destination Address /

Destination Port Range

HTTP (80)

From

Custom

HTTP (80)

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

Prevent local network access website at HTTP 80 port

A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.

Advanced Options

Display Advanced

Save

- Chọn Save để lưu
- Hiện thực các thay đổi bằng cách nhấn Apply Changes
- Trước khi áp dụng Rule này


Tìm và truy cập web http:

← → ↻ <https://www.google.com/search?channel=fs&client=ubuntu&q=HTTP+web+exa>

Google HTTP web examples ✕ 🖨️ 🗨️ 🔍

🔍 Tất cả 🖼️ Hình ảnh 📺 Video 📰 Tin tức 📖 Sách ⋮ Thêm Công cụ


Khoảng 4.210.000.000 kết quả (0,40 giây)

 **Columbia University**
<http://www.columbia.edu/~fdc/sample> · Dịch trang này ⋮

Sample Web Page - a beginner's HTML tutorial

17 thg 9, 2021 — Create a new directory ("folder") for your website, and then put the web-page files (HTML plus any pictures) in it. Use NotePad or other plain- ...

[Creating a Web Page](#) · [HTML Syntax](#) · [Converting Plain Text to HTML](#) · [Links](#)

 **San Jose State University**
<http://www.cs.sjsu.edu/web/html> · Dịch trang này ⋮

URLs and HTTP

The requested web page is identified by its Uniform Resource Locator (URL). The format of a

🔥 pfSense.home.arpa - Fire × 🗑️ Sample Web Page × +

← → ↻ www.columbia.edu/~fdc/sample.html 📄 ⚙️

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



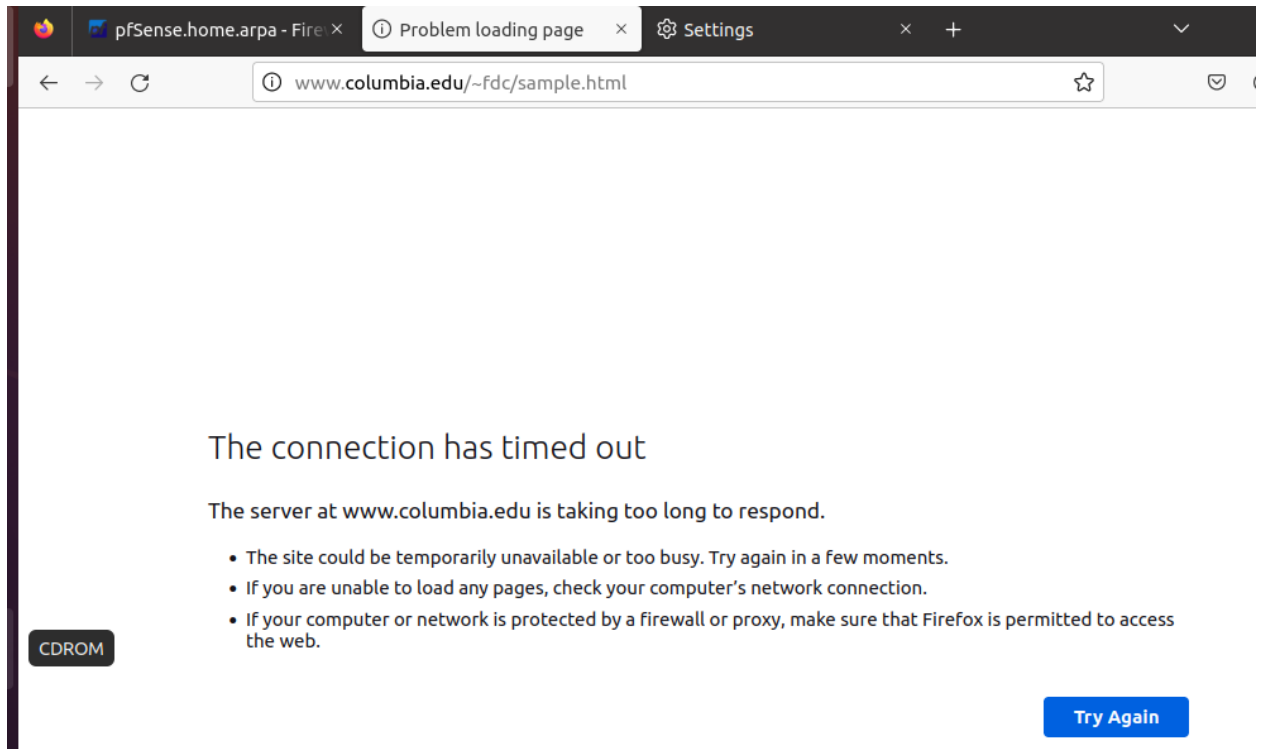
A random photo... (The Hudson River at 125th Street about 2002)

[Frank da Cruz](#)

Updated in 2019 and 2021 for HTML5 and "fluidity".

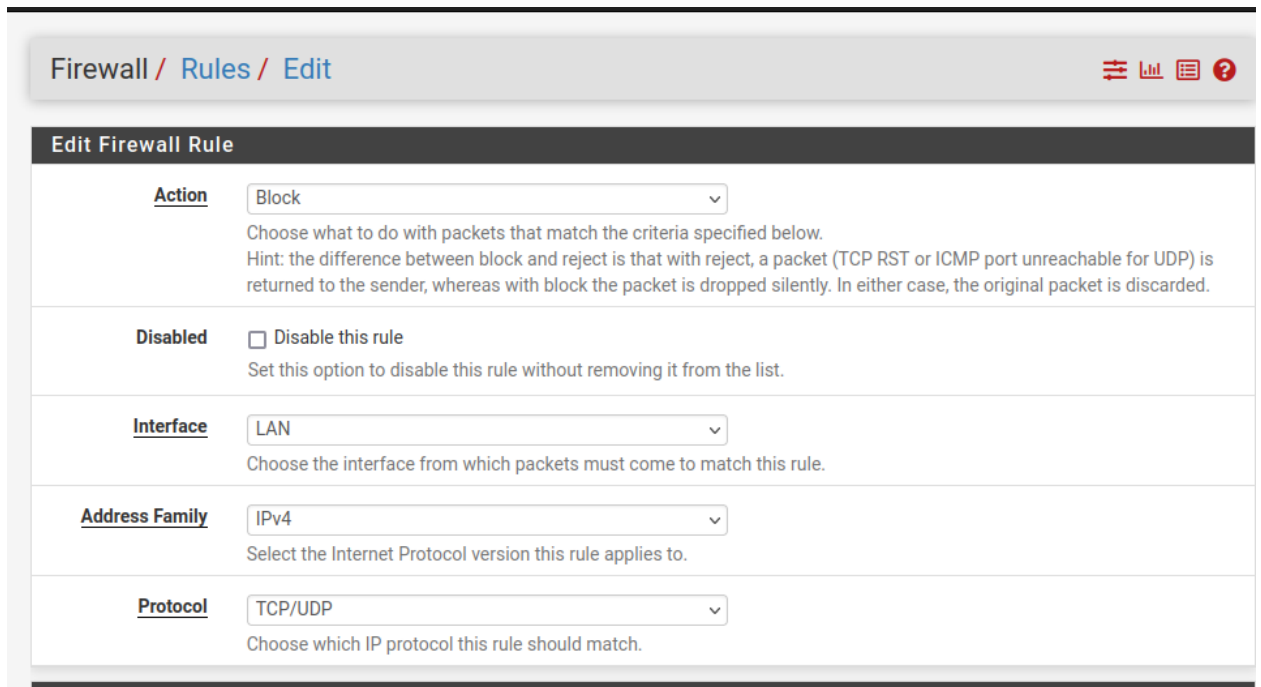
This page shows how to create Web pages by hand, the original way. Although today most Web pages are created by "Web authoring systems" that are designed to shield you from technical details, the fact is that HTML (the "programming" language of the

- Sau khi áp dụng rule



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 Firewall



Source

Source

☐ Invert match

Network

192.168.3.0

/

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

☐ Invert match

Any

Destination Address

/

Destination Port Range

Telnet (23)

From

Custom

Telnet (23)

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

Prevent hosts in LAN from telnetting to WAN

A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.

Advanced Options

Display Advanced

Rule Information

Tracking ID

1704355542

Created

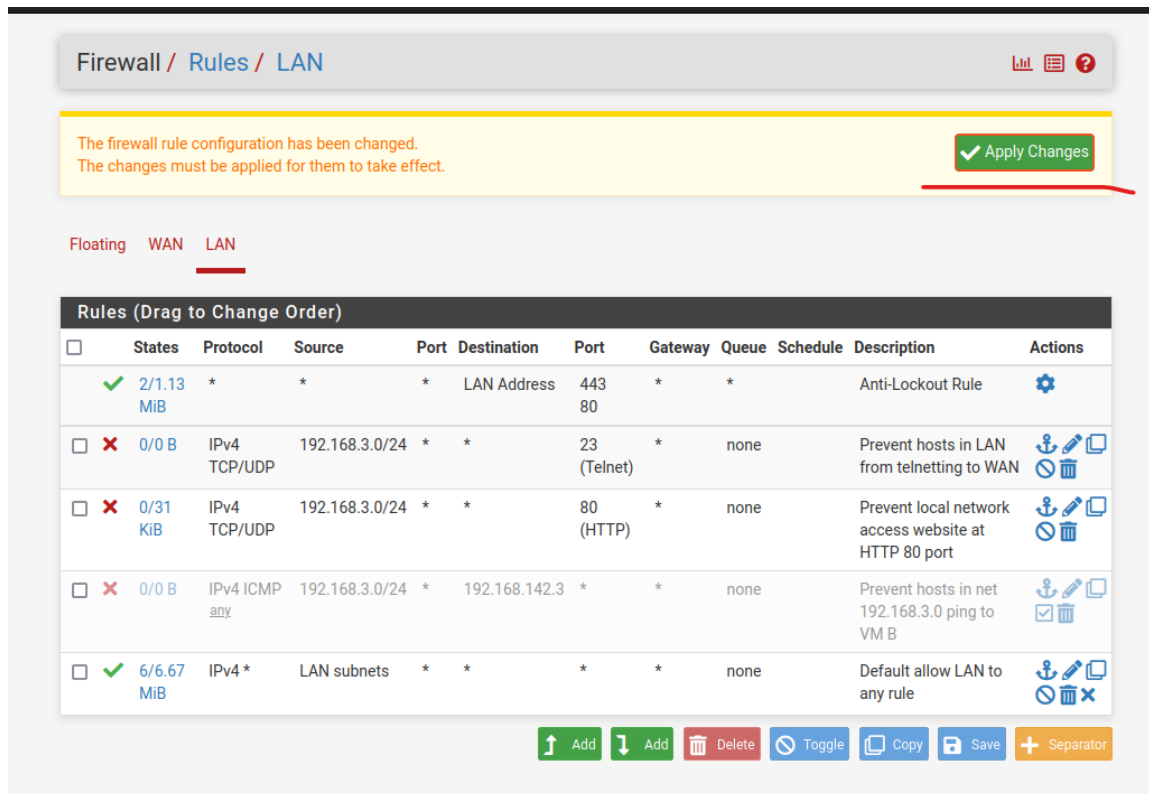
1/4/24 15:05:42 by admin@192.168.3.3 (Local Database)

Updated

1/4/24 15:06:24 by admin@192.168.3.3 (Local Database)

Save

- Nhấn Save để lưu
- Hiện thực các thay đổi bằng cách nhấn Apply Changes



- Sau khi áp dụng Rule:

```
u@ubuntu:/etc/netplan$ telnet 192.168.142.3
Trying 192.168.142.3...
telnet: Unable to connect to remote host: Connection refused
```

=> VM A (host thuộc LAN) không thể telnet tới VM B(host thuộc WAN)

4. Không cho phép các máy trong mạng nội bộ truy cập đến www.facebook.com và [youtube.com](https://www.youtube.com). Sau khi triển khai các rules trên, sử dụng máy VM A để kiểm tra.

- Tìm các ip ứng với domain facebook.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

Sau khi ping tới domain “facebook.com” thì tìm được 1 ip của domain này

```
u@ubuntu:/etc/netplan$ ping facebook.com
PING facebook.com (163.70.158.35) 56(84) bytes of data.
64 bytes from edge-star-mini-shv-01-hkg1.facebook.com (163.70.158.35): icmp_seq=1 ttl=127 time=32.3 ms
64 bytes from edge-star-mini-shv-01-hkg1.facebook.com (163.70.158.35): icmp_seq=2 ttl=127 time=44.4 ms
64 bytes from edge-star-mini-shv-01-hkg1.facebook.com (163.70.158.35): icmp_seq=3 ttl=127 time=56.0 ms
64 bytes from edge-star-mini-shv-01-hkg1.facebook.com (163.70.158.35): icmp_seq=4 ttl=127 time=50.5 ms
^X64 bytes from edge-star-mini-shv-01-hkg1.facebook.com (163.70.158.35): icmp_seq=5 ttl=127 time=44.8 ms
^C
--- facebook.com ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4049ms
rtt min/avg/max/mdev = 32.333/45.619/56.025/7.890 ms
u@ubuntu:/etc/netplan$ ping facebook.com
PING facebook.com (163.70.158.35) 56(84) bytes of data.
64 bytes from edge-star-mini-shv-01-hkg1.facebook.com (163.70.158.35): icmp_seq=1 ttl=127 time=48.0 ms
64 bytes from edge-star-mini-shv-01-hkg1.facebook.com (163.70.158.35): icmp_seq=2 ttl=127 time=45.1 ms
64 bytes from edge-star-mini-shv-01-hkg1.facebook.com (163.70.158.35): icmp_seq=3 ttl=127 time=46.5 ms
^C
--- facebook.com ping statistics ---
4 packets transmitted, 3 received, 25% packet loss, time 3032ms
rtt min/avg/max/mdev = 45.071/46.505/47.964/1.181 ms
u@ubuntu:/etc/netplan$
```

- Tương tự vậy tìm được 1 ip của youtube.com

```
ssh: connect to host 192.168.142.3 port 22: Connection refused
u@ubuntu:~/Desktop$ ping youtube.com
PING youtube.com (172.217.25.14) 56(84) bytes of data.
64 bytes from hkg12s35-in-f14.1e100.net (172.217.25.14): icmp_seq=1 ttl=127
=31.7 ms
64 bytes from hkg12s35-in-f14.1e100.net (172.217.25.14): icmp_seq=2 ttl=127
=45.5 ms
64 bytes from hkg12s35-in-f14.1e100.net (172.217.25.14): icmp_seq=3 ttl=127
=41.1 ms
^C
--- youtube.com ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 31.683/39.407/45.468/5.749 ms
u@ubuntu:~/Desktop$
```

- Tạo danh sách alias dựa trên IP vừa tìm được

Firewall / Aliases / Edit

Properties

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

Description IP which found first
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 163.70.158.35 / 16 Description Delete

Save Add Network

Firewall / Aliases / Edit

Properties

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

Description IP which found first
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 172.217.25.14 / 16 Description Delete

Save Add Network

- Nhấn Apply changes để thực hiện các thay đổi

Firewall / Aliases / IP

The alias list has been changed.
The changes must be applied for them to take effect.

Apply Changes

IP Ports URLs All

Firewall Aliases IP				
Name	Type	Values	Description	Actions
FacebookIpList	Network(s)	163.70.158.35/16	IP which found first	

+ Add Import

- Sau khi tạo được 2 list như bên dưới thì chuyển sang tạo các Rule để ngăn các máy tính thuộc mạng LAN truy cập tới trang web facebook và youtube

Firewall / Aliases / IP

The changes have been applied successfully. The firewall rules are now reloading in the background.
Monitor the filter reload progress.

IP Ports URLs All

Firewall Aliases IP				
Name	Type	Values	Description	Actions
FacebookIpList	Network(s)	163.70.158.35/16	IP which found first	
YoutubelpList	Network(s)	172.217.25.14/16	IP which found first	

+ Add Import

- Thực hiện tạo các Rules để ngăn chặn việc truy cập website cụ thể nào đó
 - Rule cho facebook

← → ↻ https://192.168.3.2/firewall_rules_edit.php?id=3 ☆

piSense COMMUNITY EDITION System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Help ▾

Firewall / Rules / Edit

Edit Firewall Rule

Action
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
Choose the interface from which packets must come to match this rule.

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

Protocol
Choose which IP protocol this rule should match.

Source

Source ☐ Invert match /

[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 ☐ Invert match /

Destination Port Range From To

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
A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.

Advanced Options [Display Advanced](#)

Rule Information

Tracking ID	1704357303
Created	1/4/24 15:35:03 by admin@192.168.3.3 (Local Database)
Updated	1/4/24 15:35:03 by admin@192.168.3.3 (Local Database)

[Save](#)

- Nhấn Save để lưu
- Hiện thực các thay đổi bằng cách nhấn Apply Changes
 - Rule cho youtube

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

☐ Invert match

Network

192.168.3.0

/

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

☐ Invert match

Address or Alias

YoutubelpList

/

Destination Port Range

any

From

Custom

To

any

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

Prevent hosts in LAN access to Youtube.com

A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.

Advanced Options

Display Advanced

Save

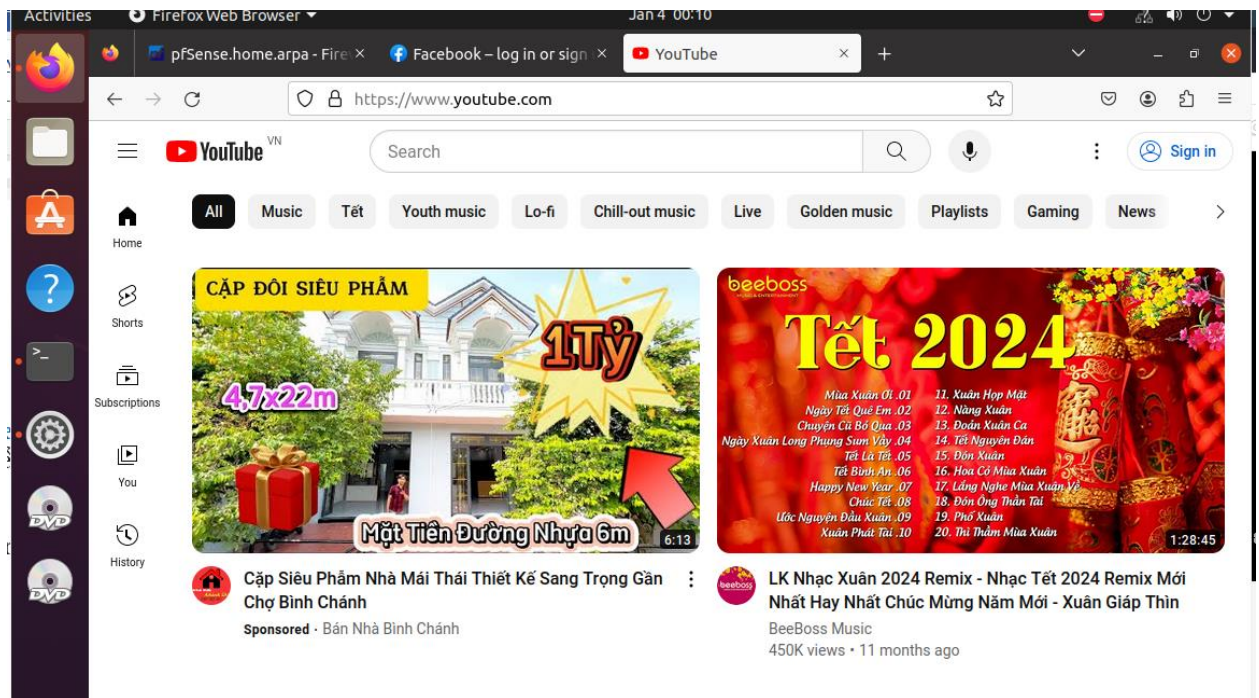
- Nhấn Save để lưu
- Hiện thực các thay đổi bằng cách nhấn Apply Changes
- Trước khi triển khai các rules theo yêu cầu

Máy VM A truy cập được www.facebook.com và youtube.com

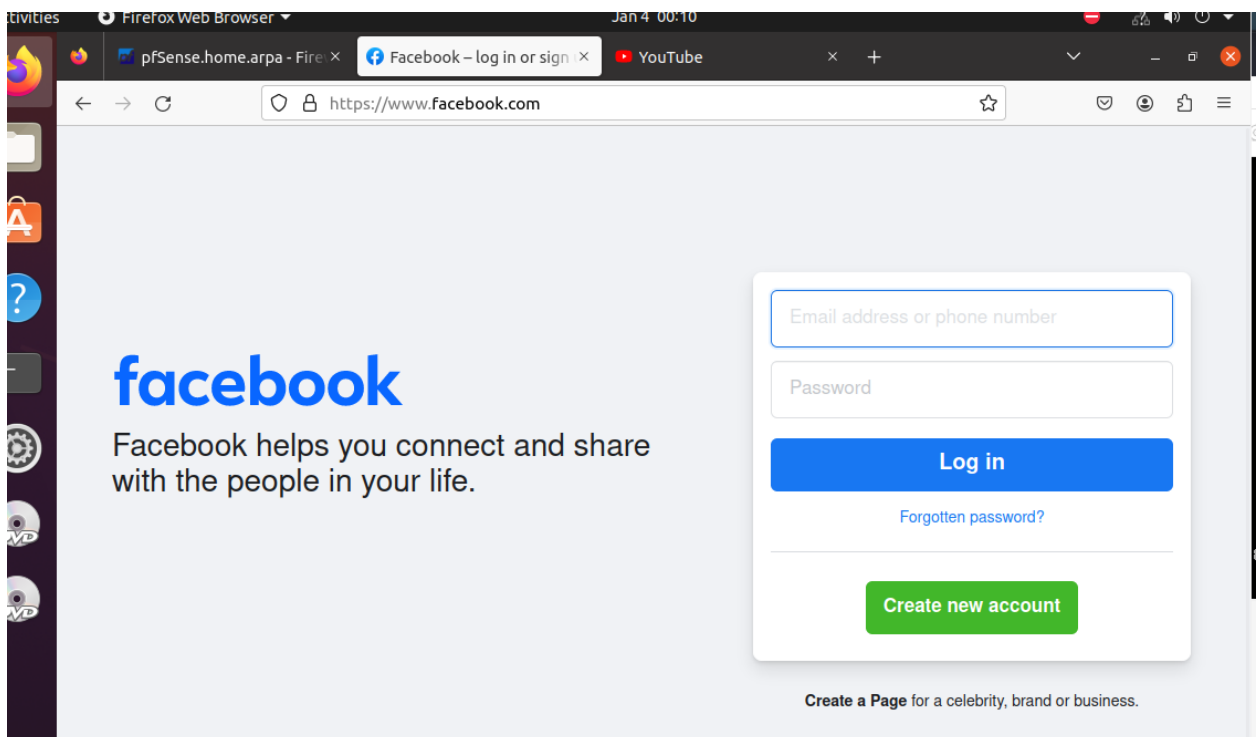
PHÒNG THÍ NGHIỆM
AN TOÀN THÔNG TIN

Báo cáo Lab05
HỌC KỲ 1 – NĂM HỌC 2023-2024

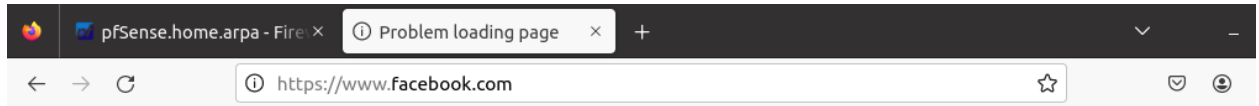
Truy cập Youtube thành công



Truy cập Facebook thành công



- Sau khi áp dụng rules:



The connection has timed out

An error occurred during a connection to www.facebook.com.

- The site could be temporarily unavailable or too busy. Try again in a few moments.
- 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 access the web.

Try Again

=> Không thể truy cập được facebook bằng VM A

3. Vượt qua sự kiểm soát của Firewall

a) Thực hiện Telnet từ máy A đến máy B

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 VM_B_username@VM_B_IP`

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]
- ssh: thực hiện kết nối ssh

VM_B_username: tên của máy được kết nối tới

VM_B_IP: địa chỉ IP của máy được kết nối tới

telnet localhost 8000

Giải thích câu lệnh:

- telnet: thực hiện kết nối telnet
- localhost : tên/địa chỉ IP của máy cần kết nối tới
- 8000: port cần kết nối

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?

- Khi sử dụng telnet thực chất các gói tin này vẫn đi qua firewall nhưng đi qua tại port khác (port không bị chặn), cụ thể là port 8000.
- Vì chúng ta đã tạo rule ngăn các máy trong LAN kết nối telnet ra bên ngoài nên các kết nối tới port 23 sẽ bị chặn. Tuy nhiên SSH tunnel sử dụng port 8000 để thực hiện kết nối ra bên ngoài do đó nó không bị tường lửa chặn. Vì vậy việc kết nối này thành công.

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:

```
(bun@kali)-[/etc/netplan]
$ sudo apt-get install squid -y
Reading package lists... Done
Building dependency tree... Done

(bun@kali)-[/etc/netplan]
$ sudo service squid start

(bun@kali)-[/etc/netplan]
$ sudo 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.

The screenshot shows the 'Connection Settings' dialog box in Firefox. The 'Manual proxy configuration' option is selected. The 'HTTP Proxy' is set to '192.168.142.3' with 'Port' '3128'. The 'HTTPS Proxy' is also set to '192.168.142.3' with 'Port' '3128'. The 'SOCKS Host' is empty with 'Port' '0'. The 'SOCKS v4' and 'SOCKS v5' options are both unselected. The 'Automatic proxy configuration URL' is empty. The 'No proxy for' field is empty. The 'Do not prompt for authentication if password is saved' and 'Proxy DNS when using SOCKS v5' options are both unselected. The 'Cancel' and 'OK' buttons are at the bottom right.

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` và khởi động lại squid.

```
bun@kali: /etc/netplan
File Actions Edit View Help
GNU nano 7.2 /etc/squid/squid.conf
# permissive Squid installation could introduce new attack vector>
# network by proxying external TCP connections to unprotected ser>
http_access allow localhost

# The two deny rules below are unnecessary in this default config>
# because they are followed by a "deny all" rule. However, they m>
# critically important when you start allowing external requests >

# Protect web applications running on the same server as Squid. T>
# assume that only local users can access them at "localhost" por>
http_access deny to_localhost

# Protect cloud servers that provide local users with sensitive i>
# their server via certain well-known link-local (a.k.a. APIPA) a>
http_access deny to_linklocal

#
# INSERT YOUR OWN RULE(S) HERE TO ALLOW ACCESS FROM YOUR CLIENTS
#
include /etc/squid/conf.d/*.conf

# For example, to allow access from your local networks, you may >
# following rule (and/or add rules that match your definition of >
# http_access allow localnet

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

Thay đổi: “http_access deny all” thành “http_access allow all”

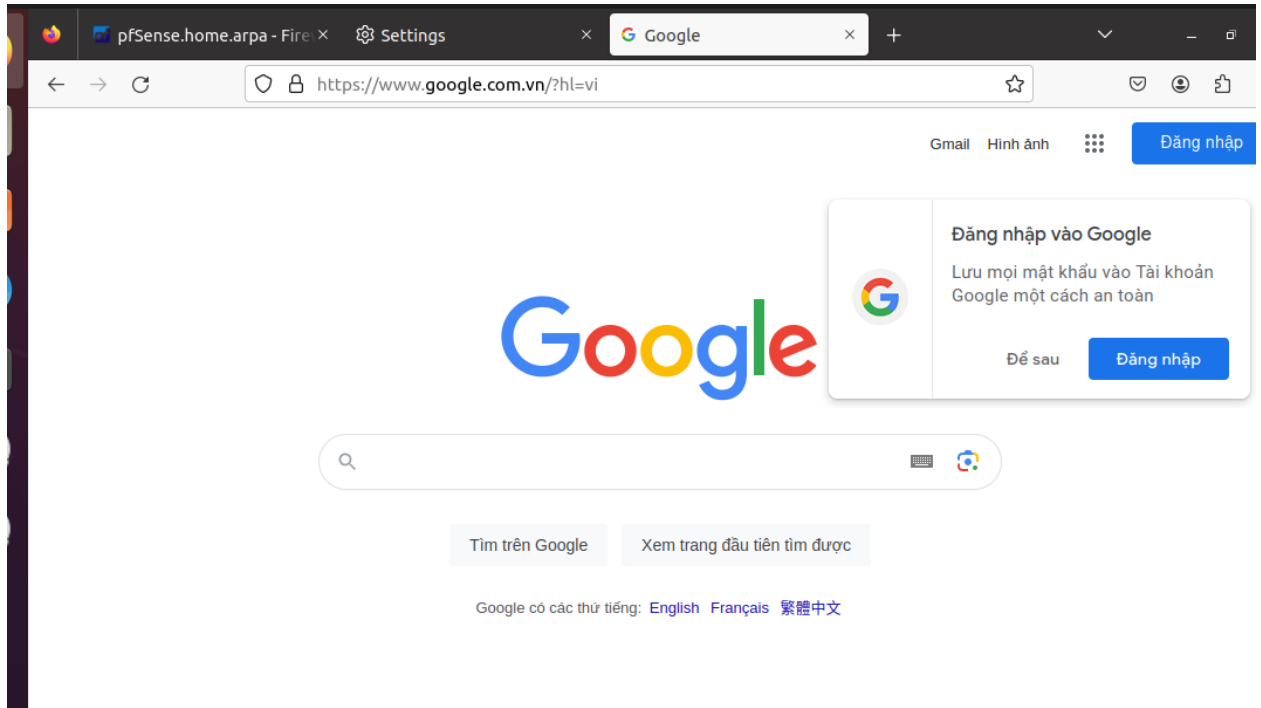
```
# And finally deny all other access to this proxy
http_access allow all
```

Sau khi lưu file thì khởi động lại service

```
(bun@kali)-[/etc/netplan]
$ sudo nano /etc/squid/squid.conf

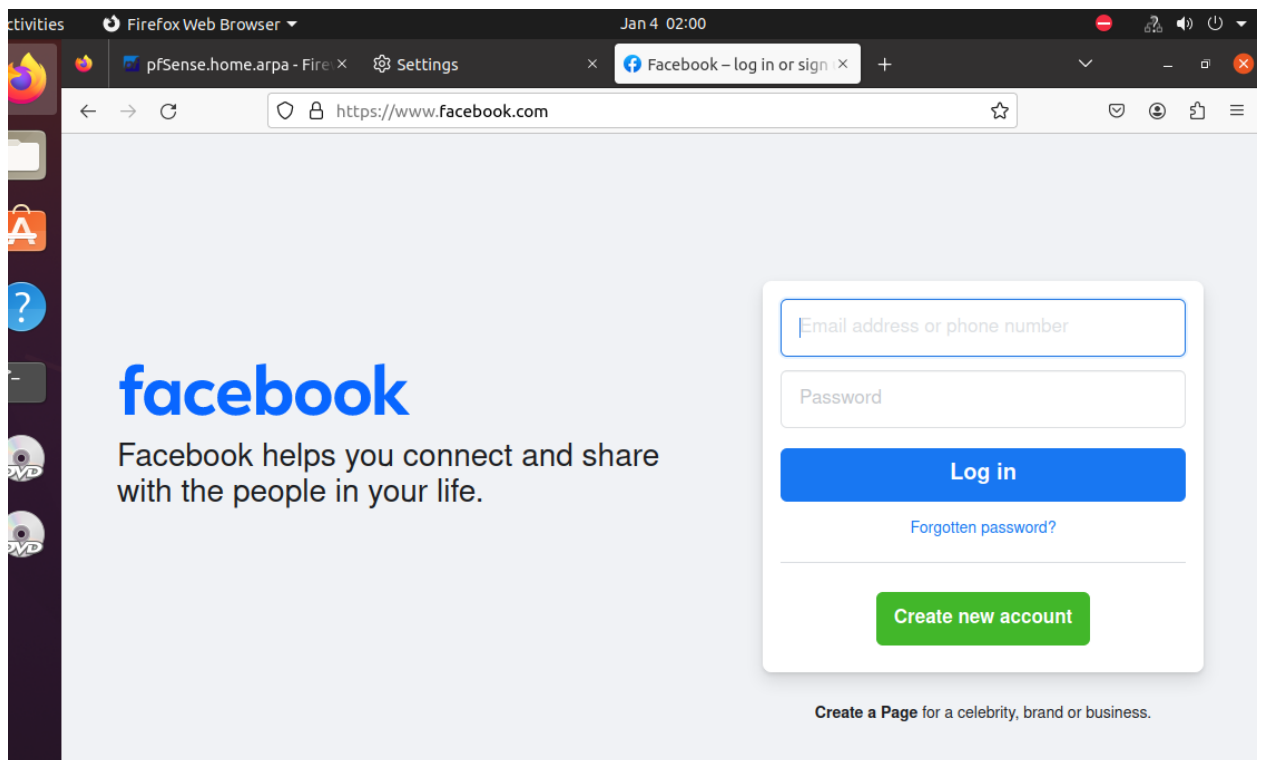
(bun@kali)-[/etc/netplan]
$ sudo service squid restart
```

Bước 4: Từ máy A, truy cập vào các trang web <https://google.com> để kiểm tra web proxy đã hoạt động hay chưa.



=> Máy VM A truy cập được google.com

Máy A có thể truy cập được website <https://www.facebook.com> không?



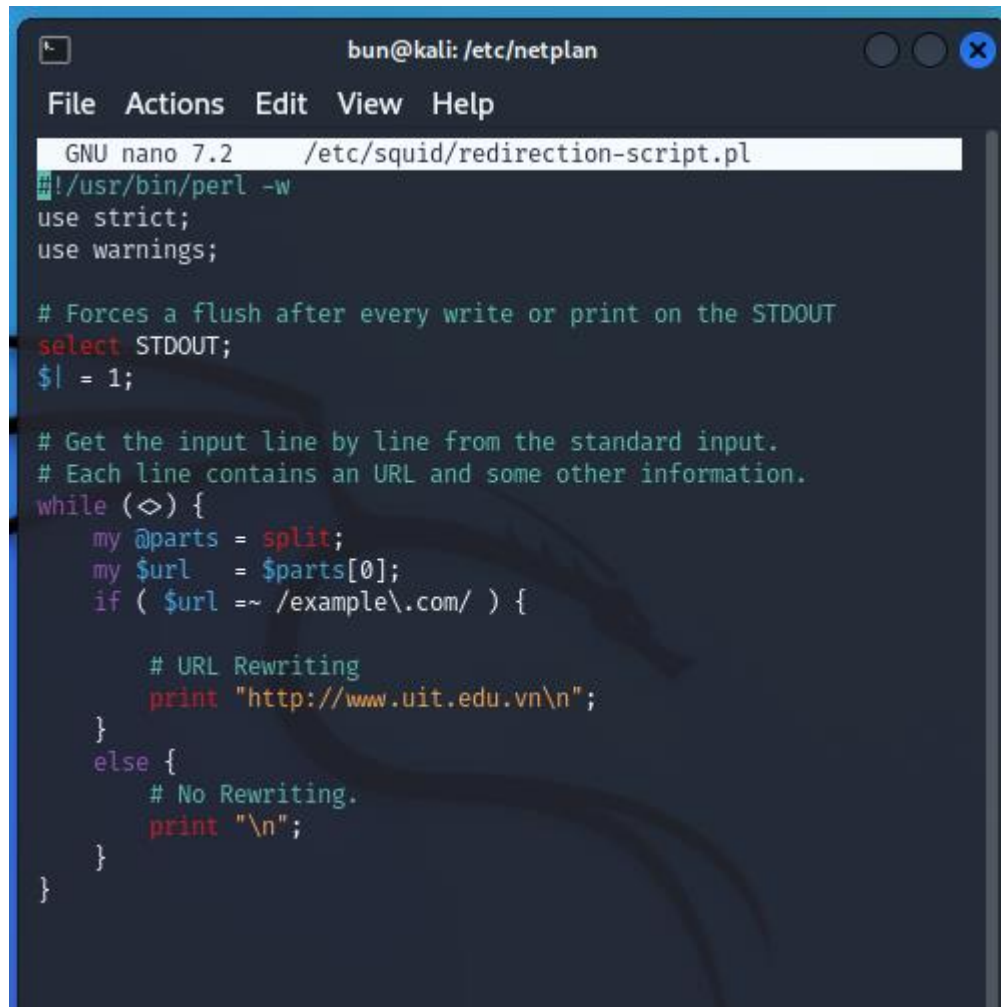
=> Máy VM A đã truy cập được facebook dù pfsense firewall vẫn đang bật rule chặn truy cập trang này

Nếu có, giải thích tại sao Firewall đã chặn máy A truy cập mà vẫn có thể truy cập được. Nếu không, giải thích lý do tại sao? Mô tả cơ chế hoạt động.

Firewall đã chặn máy A truy cập mà vẫn có thể truy cập được vì chúng ta đã thực hiện trở trực tiếp web proxy của VM A tới proxy Squid tại VM B nên traffic sẽ không đi qua pfSense firewall do đó nó không bị chặn lại.

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

Bước 1: Tại máy B, tạo file script sau (/etc/squid/script.pl) sử dụng ngôn ngữ Perl



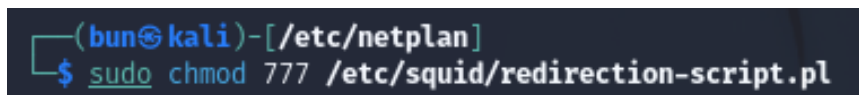
```
bun@kali: /etc/netplan
File Actions Edit View Help
GNU nano 7.2 /etc/squid/redirection-script.pl
#!/usr/bin/perl -w
use strict;
use warnings;

# 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 (chmod) cho phép thực thi (`chmod +x /etc/squid/script.pl`)



```
(bun@kali)-[/etc/netplan]
$ sudo chmod 777 /etc/squid/redirection-script.pl
```

Bước 2: Tìm trong file cấu hình /etc/squid/squid.conf và chỉnh sửa thành nội dung dưới đây để sử dụng url_rewrite_program với chương trình trên.

```
# channel-ID value, Squid sends a number between 0 and concurrency-1.
# The helper must echo back the received channel-ID in its response.
#
# By default, Squid does not use a URL rewriter.
#Default:
# none

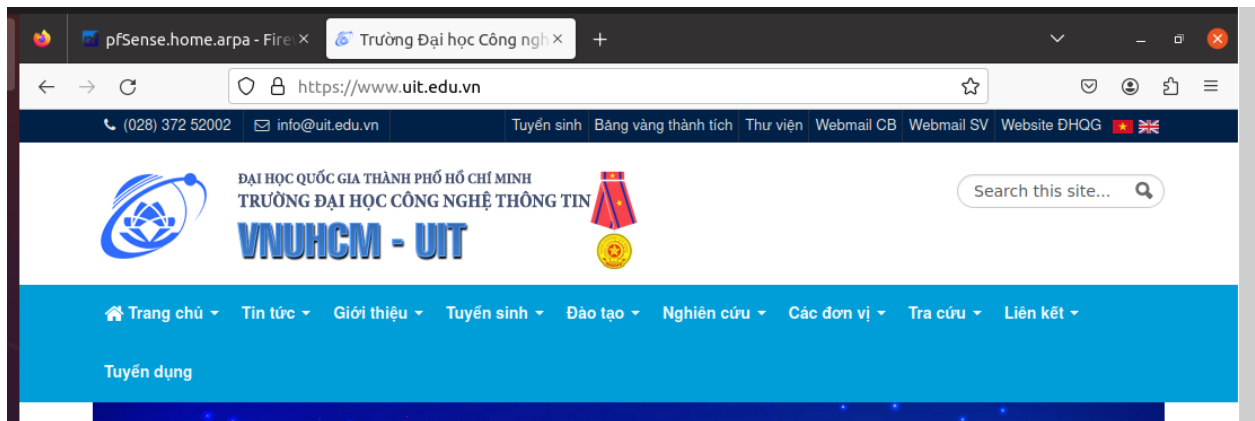
url_rewrite_program /etc/squid/redirection-script.pl
url_rewrite_children 5

# TAG: url_rewrite_children
# Specifies the maximum number of redirector processes that Squid may
```

Sau đó, khởi động lại squid.

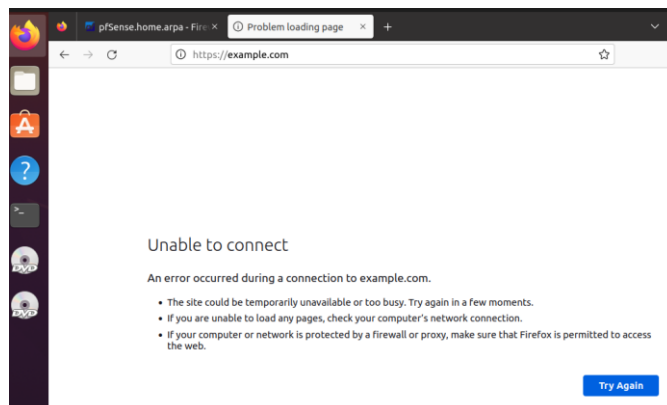
```
(bun@kali)-[/etc/netplan]
$ sudo service squid restart
```

Bước 3: Từ máy A, sử dụng trình duyệt truy cập vào website <http://example.com> ta thấy tự động chuyển sang website <http://www.uit.edu.vn> thì đã cấu hình đúng.



=> Thành công chuyển hướng trang web

Tuy nhiên khi truy cập web bằng https thì bị thất bại



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

Chương trình dùng để thực hiện việc viết lại URL trên một tệp có chứa URL. Nếu URL chứa chuỗi "example.com", tập lệnh sẽ thay thế chuỗi đó bằng "http://www.uit.edu.vn". Nếu URL không chứa chuỗi "example.com", tập lệnh sẽ giữ nguyên chuỗi đó.

Mô tả hoạt động của chương trình:

- Chương trình script trên sẽ đọc từng dòng lệnh một bằng lệnh WHILE
- Với mỗi dòng đọc được, chương trình này sẽ thực hiện các lệnh như trong vòng lặp While để tìm đoạn chứa URL cần rewrite, nếu tìm được thì sẽ viết lại URL theo như mong muốn người viết script.

Ý nghĩa của từng dòng lệnh trong chương trình script:

my @parts = split;

Chia 1 dòng lệnh thành một mảng các chuỗi bằng cách sử dụng hàm split với dấu phân cách mặc định (ký tự khoảng trắng).

my \$url = \$parts[0];

Lưu trữ phần tử đầu tiên của mảng kết quả trong biến \$url.

if (\$url =~ /example\.com/) {.....}

else { ...}

Thực hiện so sánh giá trị trong phần tử đầu tiên của mảng với chuỗi cần thay thế. Nếu đúng thì sẽ in ra chuỗi viết lại. Nếu không đúng thì sẽ in ra ký tự xuống dòng.

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?

pfSense là một hệ thống tường lửa mã nguồn mở được xây dựng trên nền tảng FreeBSD và cung cấp nhiều tính năng mạnh mẽ, bao gồm hỗ trợ cho nhiều giao thức thiết lập kết nối VPN (Virtual Private Network). Dưới đây là một số giao thức VPN phổ biến được pfSense hỗ trợ và một số đặc điểm khác nhau của chúng:

- OpenVPN:

OpenVPN là một giao thức mã nguồn mở, linh hoạt và an toàn.

Hỗ trợ cả kết nối UDP và TCP.

Sử dụng mô hình mạng riêng ảo SSL/TLS để bảo vệ dữ liệu truyền qua mạng.

Dễ cấu hình và hỗ trợ trên nhiều nền tảng (Windows, Linux, macOS).

- IPsec (Internet Protocol Security):

Là một giao thức VPN tiêu chuẩn được tích hợp sâu vào các hệ điều hành.

Hỗ trợ các chế độ kết nối như Transport Mode và Tunnel Mode.

Sử dụng các giao thức bảo mật như ESP (Encapsulating Security Payload) để đảm bảo tính toàn vẹn và bảo mật dữ liệu.

- L2TP/IPsec (Layer 2 Tunneling Protocol over IPsec):

Kết hợp giữa L2TP và IPsec để tạo một kênh an toàn cho việc truyền dữ liệu.

Thường được sử dụng cho kết nối từ xa và hỗ trợ trên nhiều thiết bị.

- PPTP (Point-to-Point Tunneling Protocol):

Một giao thức VPN lỗi thời và không nên được sử dụng nếu có lựa chọn khác.

Thiết lập kết nối bằng cách sử dụng PPP (Point-to-Point Protocol) và tạo một kênh truyền thông trực tiếp giữa hai thiết bị.

- IKEv2 (Internet Key Exchange version 2):

Một giao thức mạnh mẽ, linh hoạt và hiệu quả.

Hỗ trợ tái thiết lập kết nối tự động khi có sự gián đoạn đường truyền.

Đặc biệt hiệu quả cho kết nối di động và từ xa.

Mỗi giao thức VPN có những đặc điểm riêng biệt và ưu điểm tùy thuộc vào yêu cầu cụ thể của môi trường và ứng dụng. Khi triển khai pfSense, lựa chọn giao thức VPN phù hợp sẽ phụ thuộc vào yêu cầu bảo mật, hiệu suất, và tính linh hoạt của hệ thống.