

# BÁO CÁO BÀI TẬP

Môn học: An toàn mạng máy tính

Kỳ báo cáo: Buổi 04 (Session 04)

Tên chủ đề: Firewall

GV: Nghi Hoàng Khoa

Ngày báo cáo: xx/xx/20xx

Nhóm: 07 (nếu không có xoá phần này)

## 1. THÔNG TIN CHUNG:

(Liệt kê tất cả các thành viên trong nhóm)

Lớp: NT101.N11.ANTN

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

## 2. NỘI DUNG THỰC HIỆN:<sup>1</sup>

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

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

<sup>1</sup> Ghi nội dung công việc, các kịch bản trong bài Thực hành

# BÁO CÁO CHI TIẾT

Môi trường

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

Firewall

```

http://192.168.206.2/
Press <ENTER> to continue.
VMware Virtual Machine - Netgate Device ID: b822da2fbde27c73a930

*** Welcome to pfSense 2.6.0-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4/DHCP4: 192.168.182.128/24
LAN (lan)      -> em1      -> v4: 192.168.206.2/24

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

Enter an option:
Message from syslogd@pfSense at Nov 30 13:16:40 ...
php-fpm[370]: /index.php: Successful login for user 'admin' from: 192.168.206.1
(Local Database)

```

Máy A

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

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

Máy B

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

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

### Bài tập trên lớp

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

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

Máy VM-B có địa chỉ IP là 192.168.182.129

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

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

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

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

**Source**

Source:  Invert match Network 192.168.206.0 / 24

**Destination**

Destination:  Invert match Single host or alias 192.168.182.129

**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 net 192.168.206.0/24 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**

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

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

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

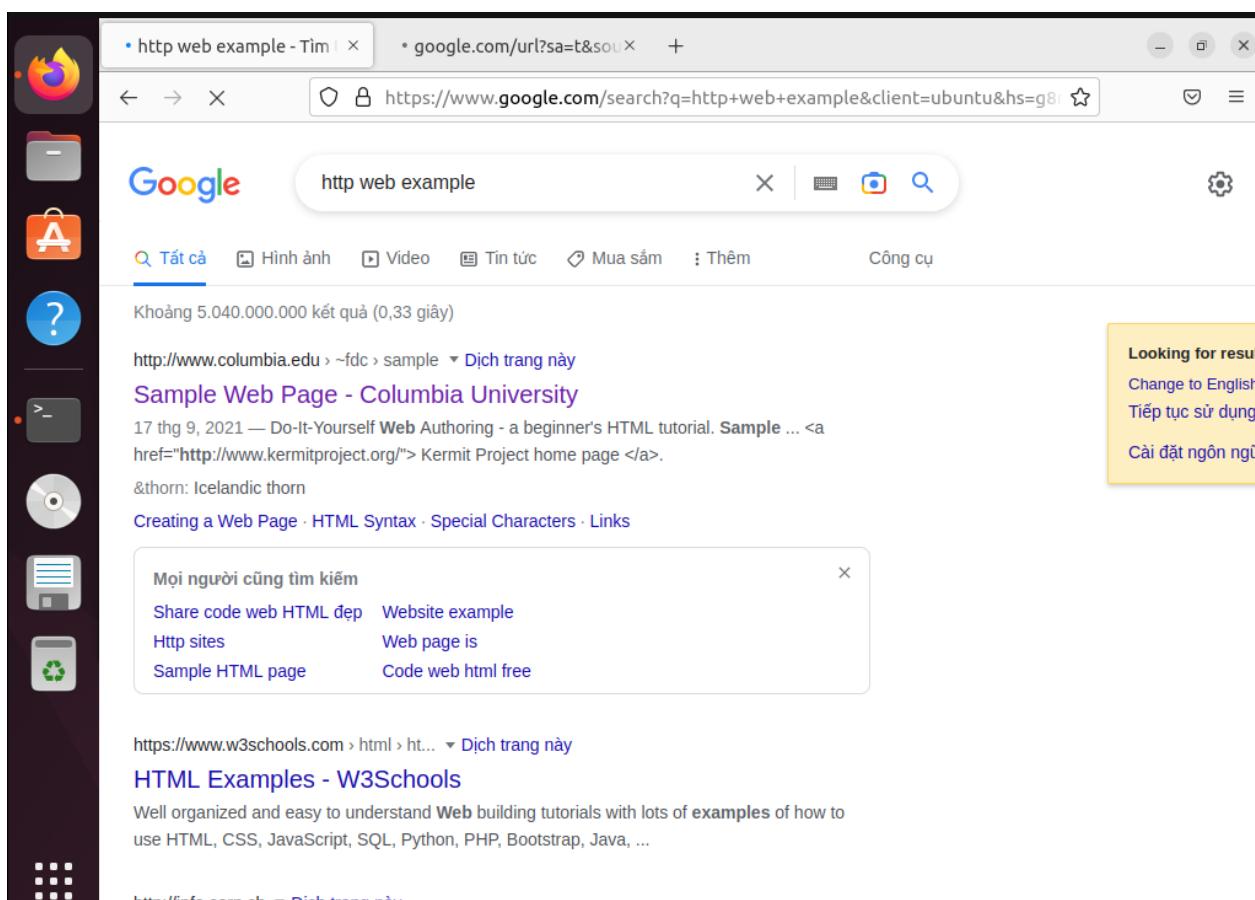
Ta vào Firewall -> Rule -> Add

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

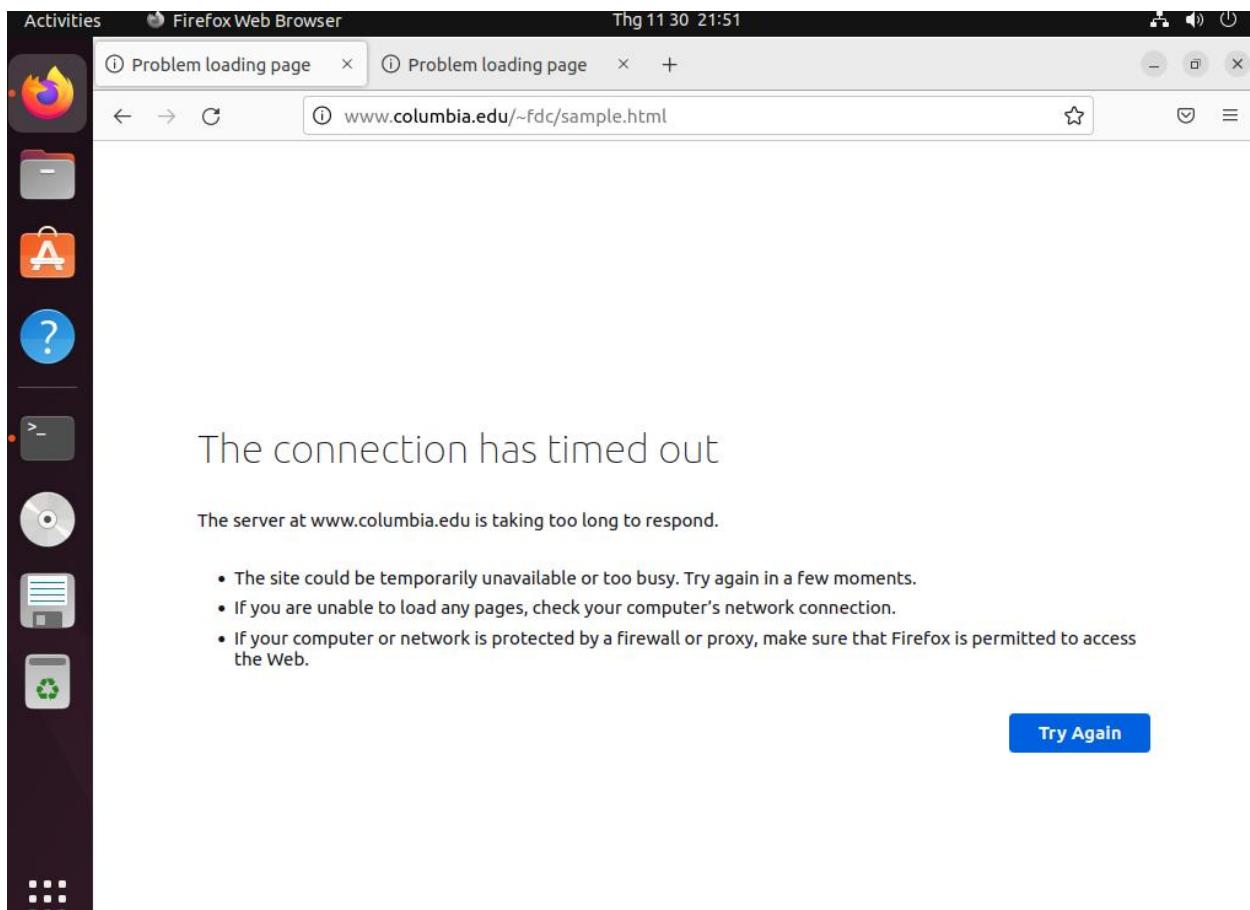
The screenshot shows the 'Edit Firewall Rule' interface. The 'Action' dropdown is set to 'Block'. The 'Source' section shows 'Source' set to 'LAN net'. The 'Destination' section shows 'Destination' set to 'any' and 'Destination Port Range' set to 'HTTP (80)'. The 'Extra Options' section includes 'Log' (unchecked), 'Description' (empty), and 'Advanced Options' (button). A 'Save' button is at the bottom.

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	<input type="checkbox"/> 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.	
<b>Source</b>	
Source	<input type="checkbox"/> Invert match      LAN net      Source Address /
<a href="#">Display Advanced</a>	
The <b>Source Port Range</b> 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>	
Destination	<input type="checkbox"/> Invert match      any      Destination Address /
Destination Port Range	From: <input type="button" value="HTTP (80)"/> Custom      To: <input type="button" value="HTTP (80)"/> Custom
Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.	
<b>Extra Options</b>	
Log	<input type="checkbox"/> 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 <a href="#">Status: System Logs: Settings</a> page).
Description	<input type="text"/>
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	<a href="#">Display Advanced</a>
<b>Save</b>	

Ta lên google search kiếm 1 trang web http



Truy cập tới và thấy kết nối không thành công



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

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

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

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

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

Vào Firewall -> Rules -> Add

The screenshot shows the 'Edit Firewall Rule' configuration page. The 'Action' dropdown is set to 'Block'. The 'Disabled' section contains a checkbox for 'Disable this rule'. The 'Interface' dropdown is set to 'LAN'. The 'Address Family' dropdown is set to 'IPv4'. The 'Protocol' dropdown is set to 'TCP/UDP'. The 'Source' section includes a 'Source' dropdown set to 'any', an 'Invert match' checkbox, and a 'LAN net' dropdown. A 'Display Advanced' button is present. The 'Destination' section shows 'any' selected for both 'From' and 'To' fields under 'Destination Port Range'. The 'Extra Options' section includes a 'Log' checkbox, a 'Description' field containing 'prevent LAN net telnet to outside', and a 'Display Advanced' button.

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

The screenshot shows the 'Edit Firewall Rule' configuration page. The 'Action' dropdown is set to 'Block'. The 'Disabled' section contains a checkbox for 'Disable this rule'. The 'Interface' dropdown is set to 'LAN'. The 'Address Family' dropdown is set to 'IPv4'. The 'Protocol' dropdown is set to 'TCP/UDP'. The 'Source' section includes a 'Source' dropdown set to 'any', an 'Invert match' checkbox, and a 'LAN net' dropdown. A 'Display Advanced' button is present. The 'Destination' section shows 'any' selected for both 'From' and 'To' fields under 'Destination Port Range'. The 'Extra Options' section includes a 'Log' checkbox, a 'Description' field containing 'prevent LAN net telnet to outside', and a 'Display Advanced' button.

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

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

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

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

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

Trước tiên ta edit aliases:

Tạo danh sách các IP của facebook với name là BF

The screenshot shows the configuration interface for a new alias named 'BF'. The 'Properties' section includes fields for Name (BF), Description (blockfb), and Type (Network(s)). The 'Network(s)' section lists several CIDR network entries: 31.13.24.0/21, 31.13.64.0/18, 45.64.40.0/22, 66.220.0.0/16, 69.63.176.0/20, 69.171.0.0/16, and 74.119.76.0/22. Each entry has a 'Delete' button next to it.

Properties			
Name	BF		
The name of the alias may only consist of the characters "a-z, A-Z, 0-9 and _".			
Description	blockfb		
A description may be entered here for administrative reference (not parsed).			
Type	Network(s)		

Network(s)			
<b>Hint</b> 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	31.13.24.0	/ 21	Description
Network or FQDN	31.13.64.0	/ 18	Description
Network or FQDN	45.64.40.0	/ 22	Description
Network or FQDN	66.220.0.0	/ 16	Description
Network or FQDN	69.63.176.0	/ 20	Description
Network or FQDN	69.171.0.0	/ 16	Description
Network or FQDN	74.119.76.0	/ 22	Description

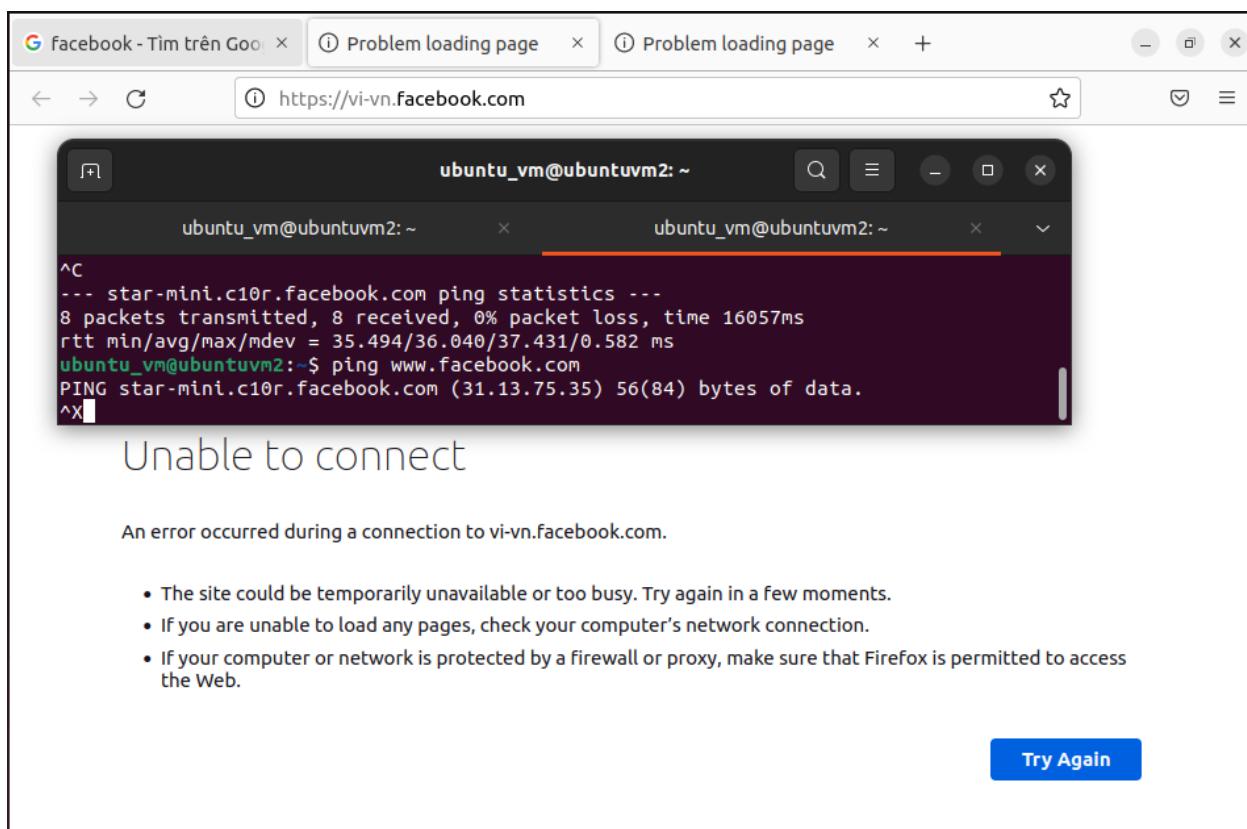
<input type="text" value="74.119.76.0"/>	/	22	<input type="button" value="Delete"/>
<input type="text" value="102.132.96.0"/>	/	20	<input type="button" value="Delete"/>
<input type="text" value="103.4.96.0"/>	/	22	<input type="button" value="Delete"/>
<input type="text" value="129.134.0.0"/>	/	16	<input type="button" value="Delete"/>
<input type="text" value="147.75.208.0"/>	/	20	<input type="button" value="Delete"/>
<input type="text" value="157.240.0.0"/>	/	16	<input type="button" value="Delete"/>
<input type="text" value="173.252.64.0"/>	/	18	<input type="button" value="Delete"/>
<input type="text" value="179.60.192.0"/>	/	22	<input type="button" value="Delete"/>
<input type="text" value="185.60.216.0"/>	/	22	<input type="button" value="Delete"/>
<input type="text" value="185.89.216.0"/>	/	22	<input type="button" value="Delete"/>
<input type="text" value="204.15.20.0"/>	/	22	<input type="button" value="Delete"/>
<input type="text" value="31.13.24.0"/>	/	21	<input type="button" value="Delete"/>
<input type="text" value="31.13.64.0"/>	/	19	<input type="button" value="Delete"/>
<input type="text" value="31.13.64.0"/>	/	24	<input type="button" value="Delete"/>
<input type="text" value="31.13.69.0"/>	/	24	<input type="button" value="Delete"/>
<input type="text" value="31.13.70.0"/>	/	24	<input type="button" value="Delete"/>
<input type="text" value="69.171.224.0"/>	/	19	<input type="button" value="Delete"/>
<input type="text" value="69.171.224.0"/>	/	20	<input type="button" value="Delete"/>
<input type="text" value="69.171.224.37"/>	/	16	<input type="button" value="Delete"/>
<input type="text" value="69.171.229.11"/>	/	16	<input type="button" value="Delete"/>
<input type="text" value="69.171.239.0"/>	/	24	<input type="button" value="Delete"/>
<input type="text" value="69.171.240.0"/>	/	20	<input type="button" value="Delete"/>
<input type="text" value="69.171.242.11"/>	/	16	<input type="button" value="Delete"/>
<input type="text" value="69.171.255.0"/>	/	24	<input type="button" value="Delete"/>
<input type="text" value="74.119.76.0"/>	/	22	<input type="button" value="Delete"/>
<input type="text" value="173.252.64.0"/>	/	19	<input type="button" value="Delete"/>
<input type="text" value="173.252.70.0"/>	/	24	<input type="button" value="Delete"/>
<input type="text" value="173.252.96.0"/>	/	19	<input type="button" value="Delete"/>
<input type="text" value="204.15.20.0"/>	/	22	<input type="button" value="Delete"/>

Sau đó ta sẽ cài rule

The screenshot shows the 'Edit Firewall Rule' interface in Winbox. The rule is set to 'Block' and is disabled. It applies to the 'LAN' interface, IPv4, and any protocol. The source is 'LAN net' and the destination is 'BF'. Advanced options include logging ('Log') and a description ('blockfb'). The rule information shows it was created and updated by 'admin@192.168.206.1' on 11/30/22.

Edit Firewall Rule	
Action	<input type="button" 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.	
Disabled	<input type="checkbox"/> Disable this rule Set this option to disable this rule without removing it from the list.
Interface	<input type="button" value="LAN"/>
Choose the interface from which packets must come to match this rule.	
Address Family	<input type="button" value="IPv4"/>
Select the Internet Protocol version this rule applies to.	
Protocol	<input type="button" value="Any"/>
Choose which IP protocol this rule should match.	
<b>Source</b>	
Source	<input type="checkbox"/> Invert match <input type="button" value="LAN net"/> Source Address / <input type="button" value=""/>
<b>Destination</b>	
Destination	<input type="checkbox"/> Invert match <input type="button" value="Single host or alias"/> BF / <input type="button" value=""/>
<b>Extra Options</b>	
Log	<input type="checkbox"/> 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	<input type="text" value="blockfb"/> 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	<input type="button" value="Display Advanced"/>
<b>Rule Information</b>	
Tracking ID	1669823653
Created	11/30/22 15:54:13 by admin@192.168.206.1 (Local Database)
Updated	11/30/22 15:58:05 by admin@192.168.206.1 (Local Database)
<input type="button" value="Save"/>	

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



	States details	*	IP_Youtube	*	*	none	blockyoutube				
<input type="checkbox"/> 0 / 40 KIB	Tracking ID: 1669823653 evaluations: 3.562 K packets: 3.173 K bytes: 279 KIB states: 0 state creations: 0	*	BF	*	*	none	blockfb				
<input type="checkbox"/> 0 / 279 KIB		*	*	23	*	none	prevent LAN net telnet to outside				
<input type="checkbox"/> 0 / 840 B		*	*	(Telnet)	*	none					

3173 gói tin từ fb đã bị chặn

Kế tiếp ta sẽ chặn các máy nội bộ truy cập tới youtube.com

Tạo danh sách IP của youtube

Firewall / Aliases / Edit

**Properties**

Name	IP_Youtube	The name of the alias may only consist of the characters "a-z, A-Z, 0-9 and _".
Description	blockytb	A description may be entered here for administrative reference (not parsed).
Type	Host(s)	

**Hint**

37.152.2.17	/ 128	Description	Delete
43.245.104.77	/ 128	Description	Delete
43.245.104.78	/ 128	Description	Delete
46.61.154.76	/ 128	Description	Delete
46.61.154.79	/ 128	Description	Delete
46.61.154.80	/ 128	Description	Delete
46.61.154.83	/ 128	Description	Delete
46.134.216.207	/ 128	Description	Delete

Cài rule chặn các IP của youtube

Firewall / Rules / 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	<input type="checkbox"/> 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	Any	Choose which IP protocol this rule should match.

**Source**

Source	<input type="checkbox"/> Invert match	LAN net	Source Address	/
--------	---------------------------------------	---------	----------------	---

**Destination**

Destination	<input type="checkbox"/> Invert match	Single host or alias	IP_Youtube	/
-------------	---------------------------------------	----------------------	------------	---

The screenshot shows a configuration page for a firewall rule. At the top, there's an 'Extra Options' section with a 'Log' checkbox (unchecked) and a note about logging packets. Below it is a 'Description' field containing 'blockyoutube'. Under 'Advanced Options', there's a 'Display Advanced' button. The main section is 'Rule Information', which includes tracking ID (1669827077), creation date (11/30/22 16:51:17 by admin@192.168.206.1 (Local Database)), and update information.

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

The browser window shows an error message: "Unable to connect" and "An error occurred during a connection to www.youtube.com". The terminal window shows two ping operations: one to star-mini.c10r.facebook.com and another to youtube.com, both failing with 100% packet loss.

An error occurred during a connection to www.youtube.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**

The screenshot shows a table of firewall rules. The first rule, 'Anti-Lockout Rule', is a stateless rule for port 80 from LAN Address to \* with no gateway, queue, schedule, and a description of 'Anti-Lockout Rule'. The second rule, 'blockyoutube', is a stateful rule for port 80 from IP\_Youtube to \* with no gateway, queue, and a description of 'blockyoutube'. The third rule, 'blockfb', is a stateful rule for port 80 from BF to \* with no gateway, queue, and a description of 'blockfb'.

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
1 / 3.57 MiB	States details		*	LAN Address	80	*	*		Anti-Lockout Rule	
0 / 40 KiB	Tracking ID: 1669827077 evaluations: 1.356 K packets: 266 bytes: 40 KiB states: 0 state creations: 0		*	IP_Youtube	*	*	none		blockyoutube	
0 / 279 KiB			*	BF	*	*	none		blockfb	

266 gói tin từ youtube đã bị chặn

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

Bài tập về nhà

### 3. Vượt qua sự kiểm soát của firewall

**a) Thực hiện telnet từ máy A tới máy B:**

Trước tiên ta sẽ cài đặt ssh và telnet ở cả hai máy

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

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

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

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

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

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

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

Giải thích câu lệnh:

-f : Để ssh chạy dưới nền trước khi thực thi câu lệnh

-N : Không thực thi lệnh remote

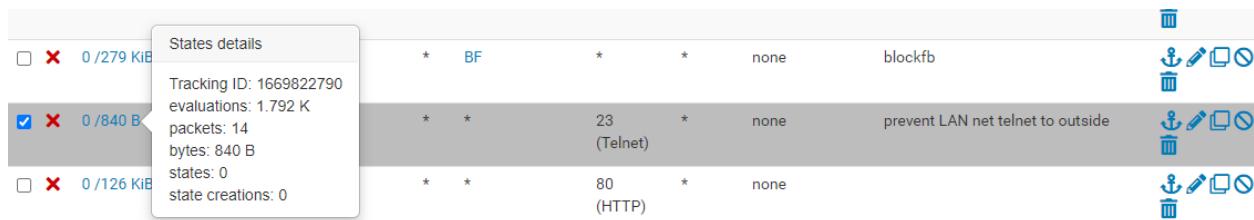
-L: Xác định tham số của bind address theo [port:host:hostport]

**telnet localhost 8000**

Kết nối tới cổng 8000 của localhost, do đã tạo tunnel của cổng 23 của máy A tới cổng 22 máy B nên lệnh này đã kết nối được tới máy B

**2. Khi sử dụng lệnh telnet, thực chất các gói tin này có đi qua máy Firewall không? Nếu có, nguyên nhân tại sao Firewall không việc sử dụng telnet này? Nếu**

không, thì kết nối từ máy A đến máy B như thế nào để không đi qua máy Firewall?



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

b) Kết nối tới facebook sử dụng ssh tunnel

Ta dùng lệnh ps aux | grep 8000 để xem thông tin các tiến trình đang chạy ở cổng 8000  
Dùng lệnh kill -9 <pid> để tắt tiến trình ở pid

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

Ta thiết lập ssh tunnel mới

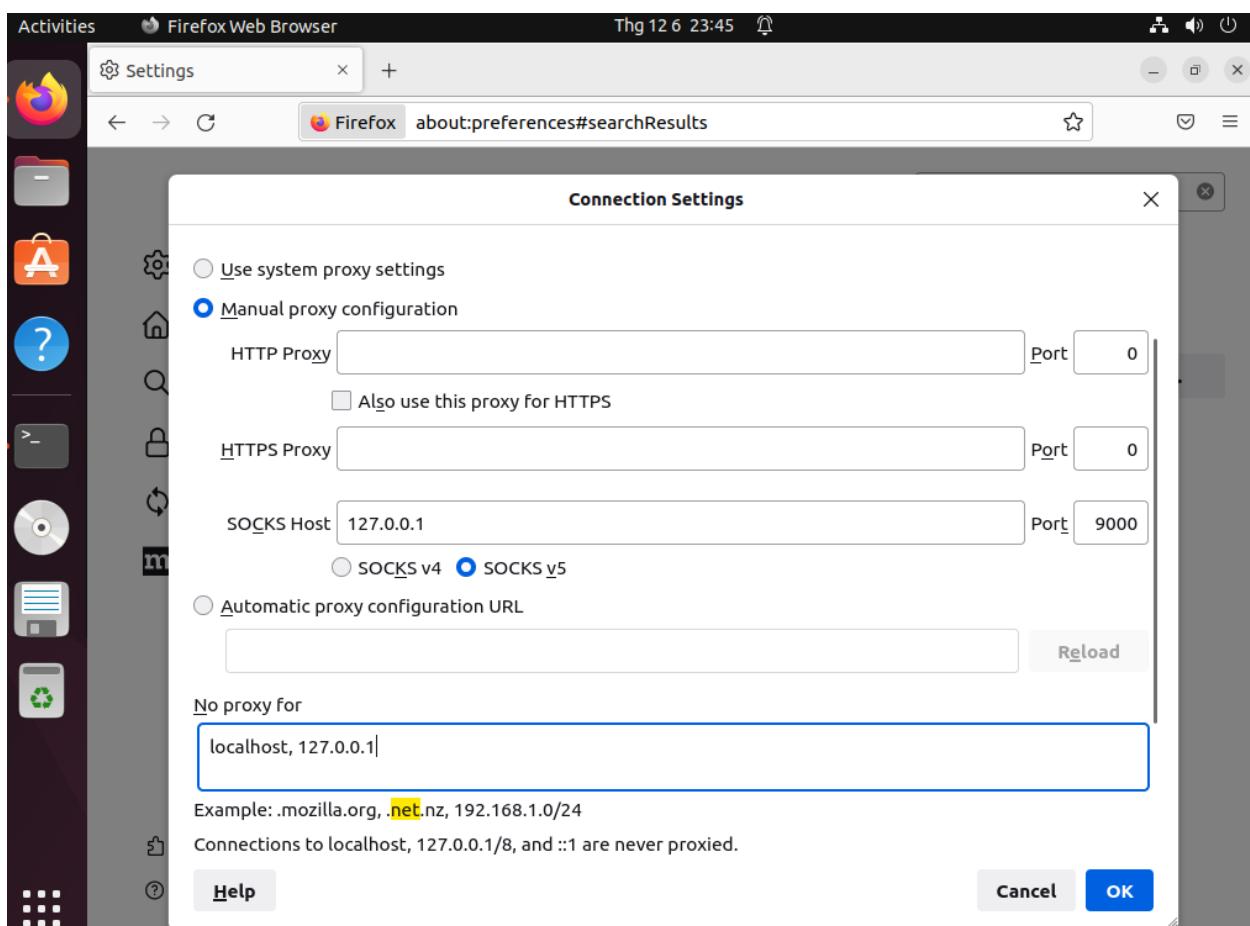
```
ubuntu_vm@ubuntuvm2:~$ ssh -D 9000 -C nbp@192.168.182.129
nbp@192.168.182.129's password:
Welcome to Ubuntu 22.04.1 LTS (GNU/Linux 5.15.0-53-generic x86_64)

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

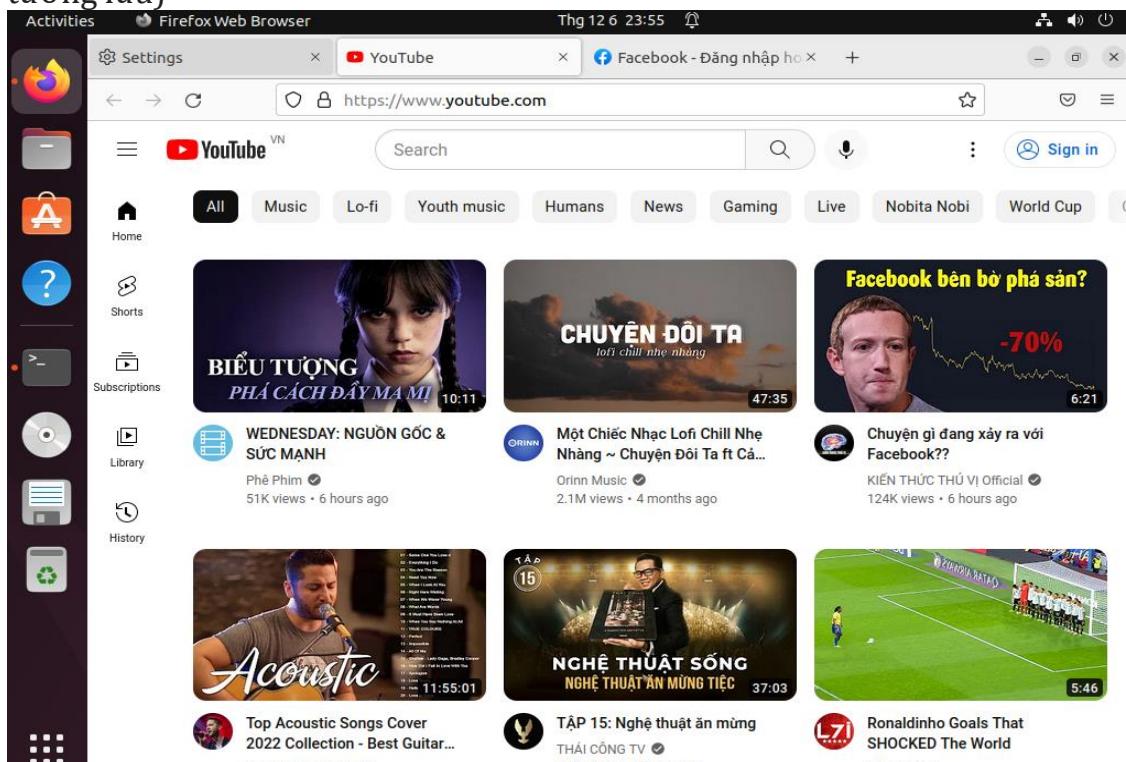
39 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

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

Chỉnh lại proxy của firefox theo yêu cầu của bài

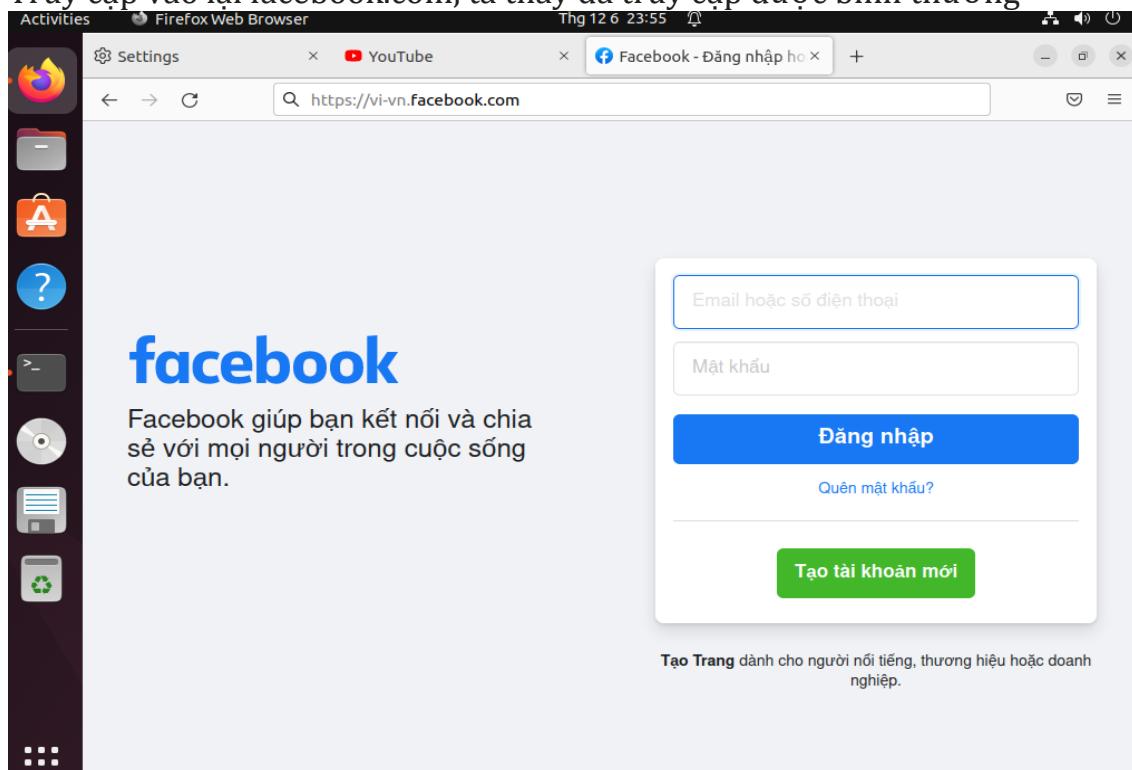


Ta truy cập vào thử youtube thì thấy đã truy cập lại bình thường (thành công đi qua tường lửa)



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

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



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

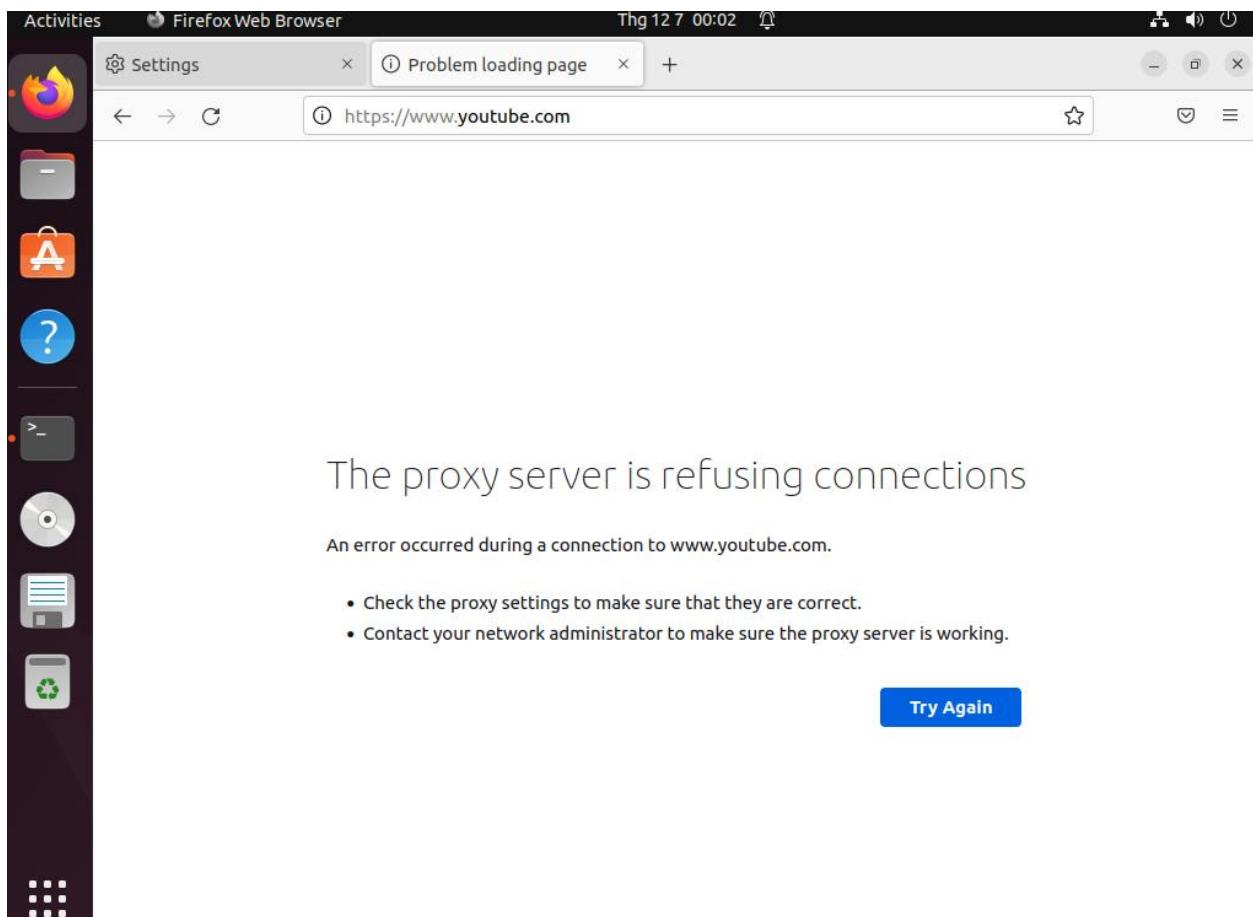
<input type="checkbox"/> X 0 /42 KiB	States details	*	IP_Youtube	*	*	none	blockyoutube		
<input type="checkbox"/> X 0 /279 KiB	Tracking ID: 1669823653 evaluations: 4.878 K packets: 3.173 K bytes: 279 KiB states: 0 state creations: 0	*	BF	*	*	none	blockfb		
<input checked="" type="checkbox"/> X 0 /840 B		*	*	23	*	none	prevent LAN net telnet to outside		

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

Ta ngắt tunnel và kiểm tra lại

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

Xóa cache trên trình duyệt



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

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

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

Firewall / Rules / 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	<input type="checkbox"/> 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.				
<b>Source</b>				
Source	<input type="checkbox"/> Invert match LAN net			
<a href="#">Display Advanced</a>				
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>				
Destination	<input type="checkbox"/> Invert match any			
Destination Address /				
<b>Source</b>				
Source	<input type="checkbox"/> Invert match LAN net			
<a href="#">Display Advanced</a>				
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>				
Destination	<input type="checkbox"/> Invert match any			
Destination Address /				
Destination Port Range	SSH (22)	From Custom	To SSH (22)	Custom
Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.				
<b>Extra Options</b>				
Log	<input type="checkbox"/> 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	<input type="text"/>			
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	<a href="#">Display Advanced</a>			

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

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

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

Rules (Drag to Change Order)										
States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/> 1 /4.24 MiB		States details Tracking ID: 1670346254 evaluations: 23 packets: 7 bytes: 420 B states: 0 state creations: 0	*	LAN Address	80	*	*		Anti-Lockout Rule	
<input type="checkbox"/> 0 /420 B			*	*	22 (SSH)	*	none			
<input type="checkbox"/> 0 /42 KiB			*	IP_Youtube	*	*	none		blockyoutube	
<input type="checkbox"/> 0 /279 KiB	IPv4	*	*	BF	*	*	none		blockfb	

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

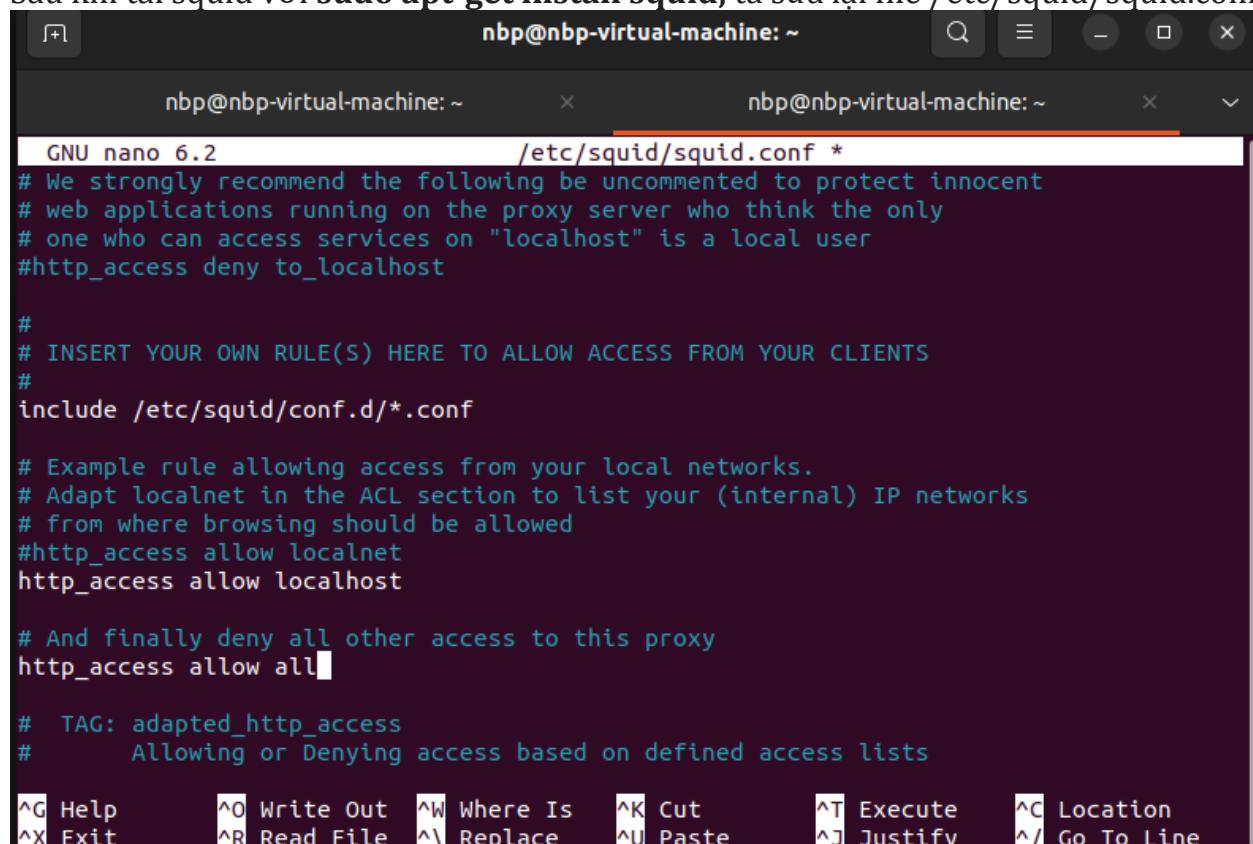
#### Câu 6. Đề xuất giải pháp để phát hiện và ngăn chặn các cách thức vượt qua sự kiểm soát của Firewall trong trường hợp trên.

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

#### 4. Triển khai web proxy

a) Cài đặt và thiết lập cấu hình squid

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



```

GNU nano 6.2                               /etc/squid/squid.conf *
# 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/*.conf

# 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
#http_access allow localnet
http_access allow localhost

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

# TAG: adapted_http_access
#      Allowing or Denying access based on defined access lists

```

^O Help ^O Write Out ^W Where Is ^K Cut ^T Execute ^C Location  
 ^X Exit ^R Read File ^\ Replace ^U Paste ^J Justify ^/ Go To Line

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

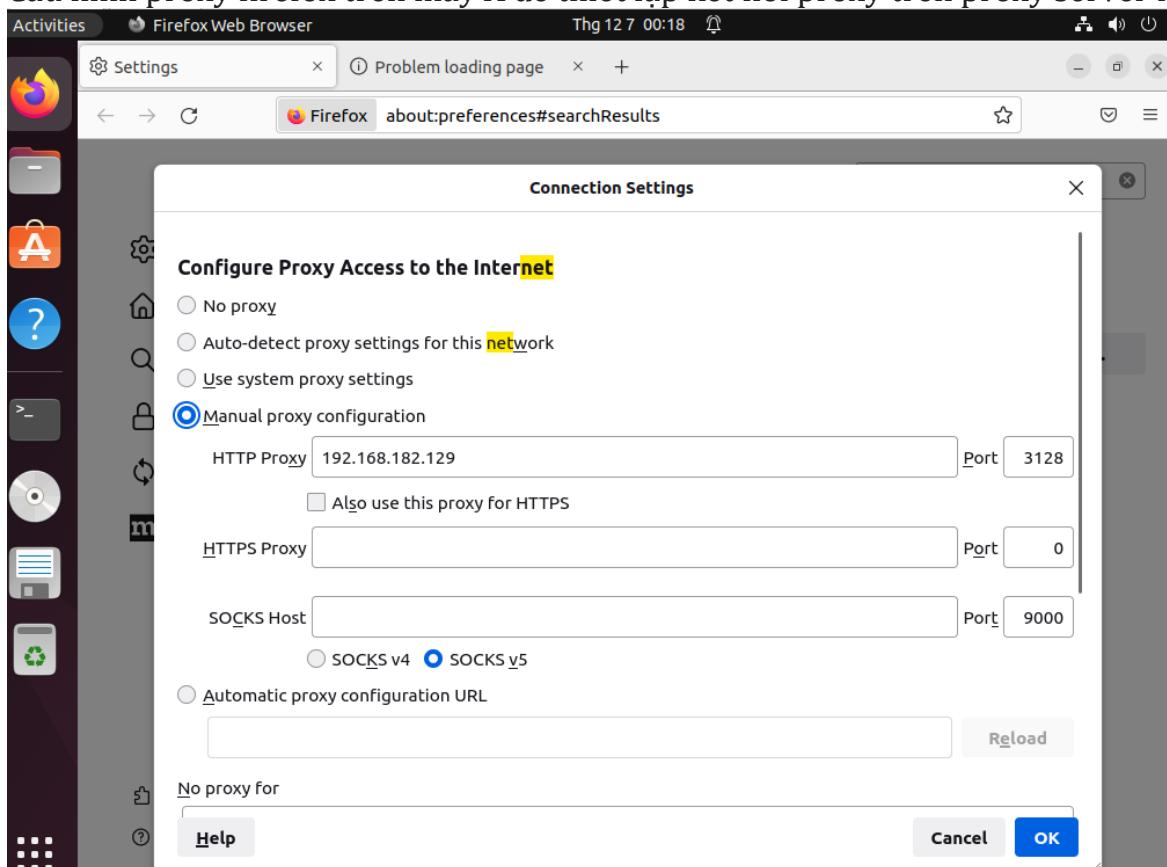
```

Activities Terminal Thg 12 7 00:17
● squid.service - Squid Web Proxy Server
  Loaded: loaded (/lib/systemd/system/squid.service; enabled; vendor preset: enabled)
  Active: active (running) since Wed 2022-12-07 00:16:33 +07; 18s ago
    Docs: man:squid(8)
   Process: 4916 ExecStartPre=/usr/sbin/squid --foreground -z (code=exited, status=0>
 Main PID: 4919 (squid)
   Tasks: 4 (limit: 2247)
  Memory: 16.1M
     CPU: 391ms
    CGroup: /system.slice/squid.service
            └─4919 /usr/sbin/squid --foreground -sYC
              ├─4921 "(squid-1)" --kid squid-1 --foreground -sYC
              ├─4922 "(logfile-daemon)" /var/log/squid/access.log
              └─4923 "(pinger)"

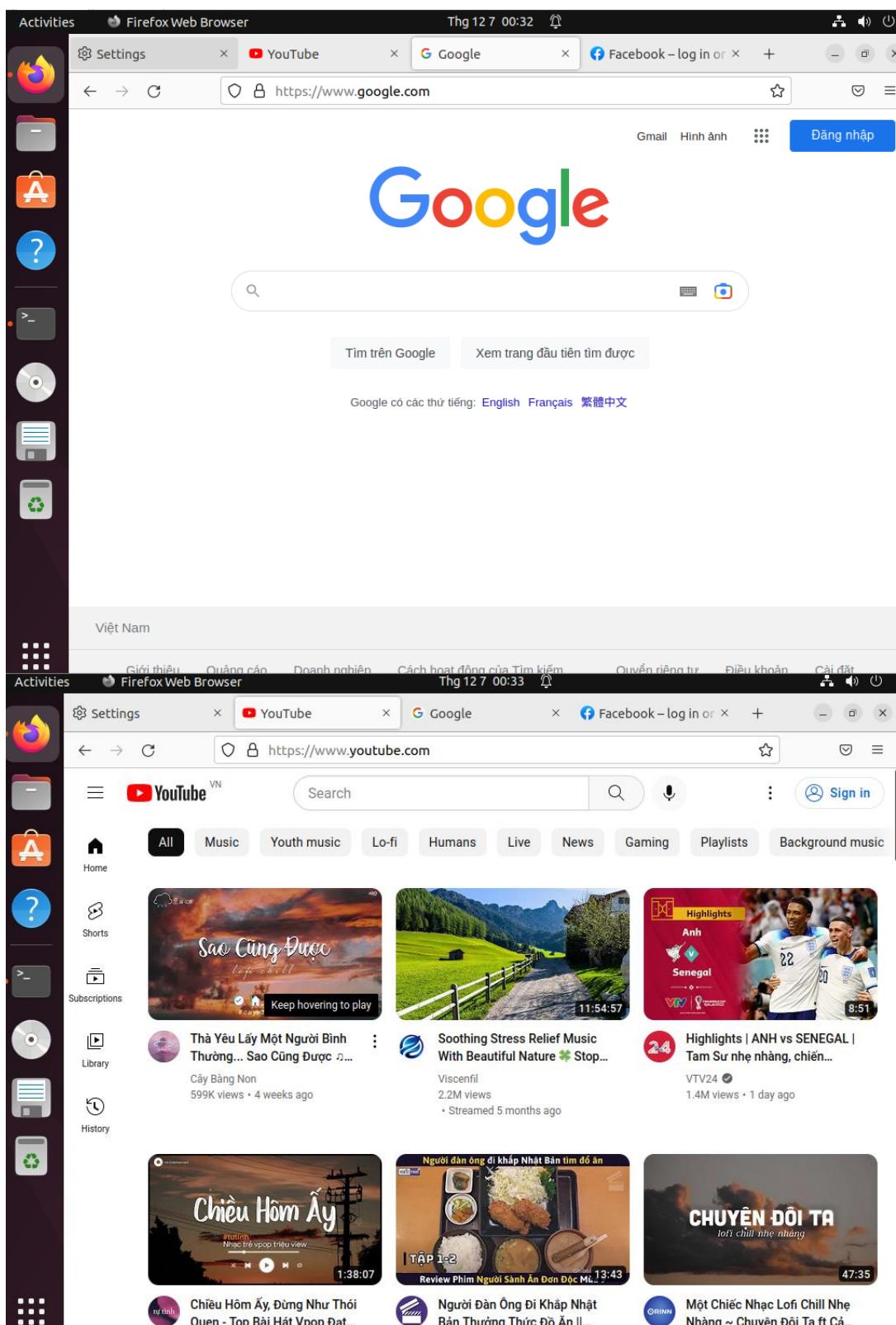
Thg 12 07 00:16:32 nbp-virtual-machine squid[4921]: Using Least Load store dir select>
Thg 12 07 00:16:32 nbp-virtual-machine squid[4921]: Set Current Directory to /var/spo>
Thg 12 07 00:16:33 nbp-virtual-machine squid[4921]: Finished loading MIME types and i>
Thg 12 07 00:16:33 nbp-virtual-machine squid[4921]: HTCP Disabled.
Thg 12 07 00:16:33 nbp-virtual-machine squid[4921]: Pinger socket opened on FD 14
Thg 12 07 00:16:33 nbp-virtual-machine squid[4921]: Squid plugin modules loaded: 0
Thg 12 07 00:16:33 nbp-virtual-machine squid[4921]: Adaptation support is off.
Thg 12 07 00:16:33 nbp-virtual-machine squid[4921]: Accepting HTTP Socket connections>
Thg 12 07 00:16:33 nbp-virtual-machine systemd[1]: Started Squid Web Proxy Server.
lines 1-24

```

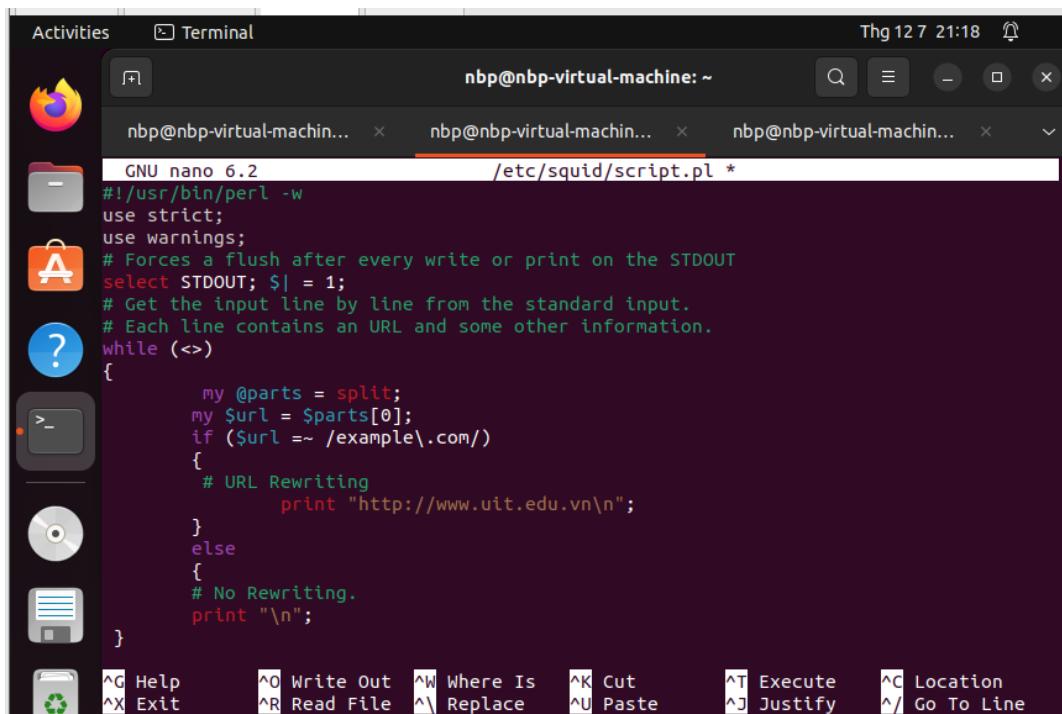
Cấu hình proxy firefox trên máy A để thiết lập kết nối proxy trên proxy server máy B



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



b) Thiết lập chuyển hướng  
Ta tạo file /etc/squid/script.pl với nội dung từ đề

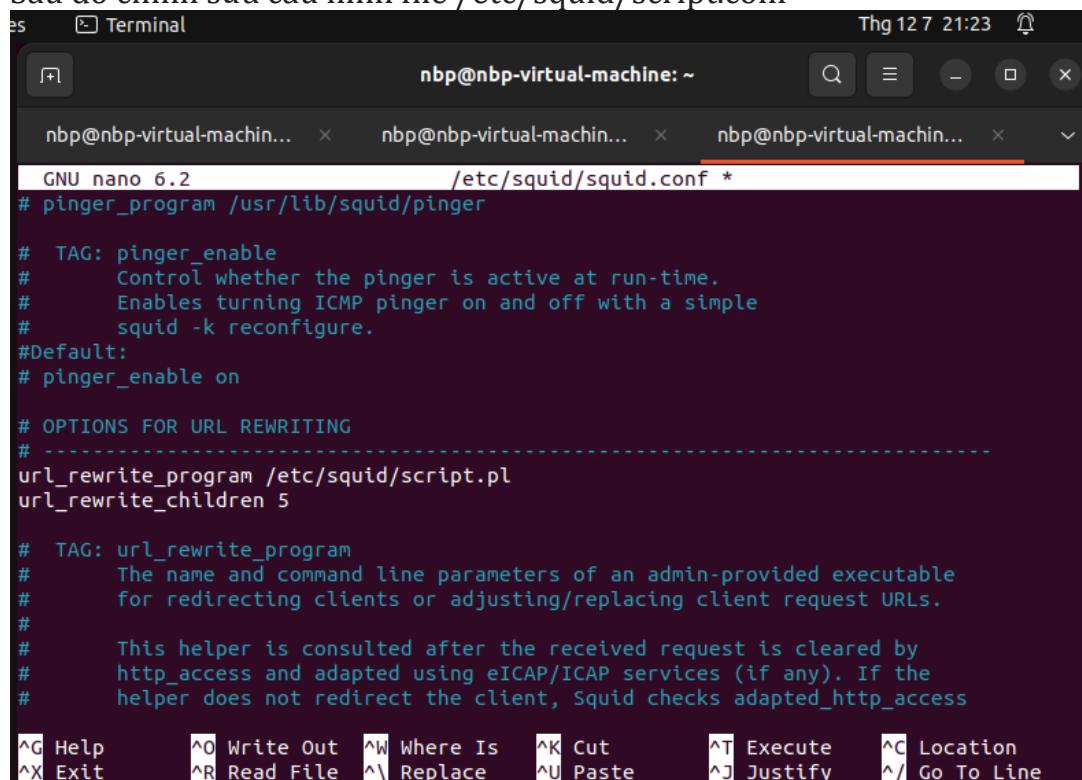


```

#!/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";
    }
}
  
```

^G Help ^O Write Out ^W Where Is ^K Cut ^T Execute ^C Location  
^X Exit ^R Read File ^\ Replace ^U Paste ^J Justify ^/ Go To Line

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



```

# pinger_program /usr/lib/squid/pinger

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

# OPTIONS FOR URL REWRITING
#
url_rewrite_program /etc/squid/script.pl
url_rewrite_children 5

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

#       This helper is consulted after the received request is cleared by
#       http_access and adapted using eICAP/ICAP services (if any). If the
#       helper does not redirect the client, Squid checks adapted_http_access
  
```

^G Help ^O Write Out ^W Where Is ^K Cut ^T Execute ^C Location  
^X Exit ^R Read File ^\ Replace ^U Paste ^J Justify ^/ Go To Line

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

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

Đoạn trên của chương trình là khai báo 2 thư viện **strict** và **warnings**

Dùng **strict** để hạn chế các cấu trúc không an toàn, **warnings** cảnh báo chúng ta nếu chúng ta gõ sai.

Kế đó với mỗi stdout, output sẽ được flush

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

# Forces a flush after every write or print on the STDOUT
select STDOUT; $| = 1;
```

```

# Get the input line by line from the standard input.
# Each line contains an URL and some other information.
while (<>)
{
    my @parts = split;
    my $url = $parts[0];
    if ($url =~ /example\.com/)
    {
        # URL Rewriting
        print "http://www.uit.edu.vn\n";
    }
    else
    {
        # No Rewriting.
        print "\n";
    }
}

```

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

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

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

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

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

	Ưu điểm	Nhược điểm
--	---------	------------

IPSec	<ul style="list-style-type: none"> <li>- Được đánh giá là bảo mật.</li> <li>- Cài đặt sẵn trên tất cả OS và thiết bị gần đây.</li> <li>- Thiết lập dễ dàng.</li> </ul>	<ul style="list-style-type: none"> <li>- Chậm hơn so với OpenVN.</li> <li>- Có thể bị mở khóa bởi NSA.</li> <li>- Có thể có vấn đề nếu được sử dụng với các tường lửa.</li> <li>- Khả năng NSA đã cố tình làm suy yếu giao thức.</li> </ul>
PPTP	<ul style="list-style-type: none"> <li>- Nhanh</li> <li>- Phần mềm trạm máy trên nhiều hệ điều hành</li> <li>- Thiết lập cấu hình dễ</li> </ul>	<ul style="list-style-type: none"> <li>- Đã bị bẻ khóa bởi NSA</li> <li>- Không hoàn toàn bảo mật</li> </ul>
OpenVPN	<ul style="list-style-type: none"> <li>- Khả năng vượt hầu hết các firewall</li> <li>- Tùy chỉnh cao</li> <li>- Do là phần mềm mã nguồn mở nên có thể dùng để phòng hờ</li> <li>- Tương thích với nhiều thuật toán mã hóa</li> <li>- Bảo mật cao</li> </ul>	<ul style="list-style-type: none"> <li>- Thiết lập khó</li> <li>- Cần thêm phần mềm thứ ba</li> </ul>

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

Ba bước chính để cấu hình OpenVPN trên pfsense

- Tạo hạ tầng khóa công khai (PKI Infrastructure)
- Cấu hình OpenVPN trên PFSense
- Cấu hình quyền truy cập của client

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

The screenshot shows the 'DHCP Client' configuration page. It includes fields for 'Hostname', 'Alias IPv4 address' (with a subnet mask of 32), and 'Reject leases from'. Below these are sections for 'Reserved Networks' and 'Bogon networks'. Under 'Reserved Networks', 'Block private networks and loopback addresses' is unchecked. Under 'Bogon networks', 'Block bogon networks' is checked. A 'Save' button is at the bottom.

### Bước 1: Tạo hạ tầng khóa công khai PKI

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

The screenshot shows the 'Create / Edit CA' page under 'System / Certificate Manager / CAs / Edit'. The 'CAs' tab is selected. The 'Descriptive name' field contains 'Cau11\_Lab4'. The 'Method' dropdown is set to 'Create an internal Certificate Authority'. The 'Trust Store' checkbox is checked, with a note explaining it adds the CA to the OS trust store. The 'Randomize Serial' checkbox is unchecked, with a note explaining it uses random serial numbers. The 'Internal Certificate Authority' section includes fields for 'Key type' (RSA), 'Key Length' (2048 bits), 'Digest Algorithm' (sha256), and 'Lifetime (days)' (3650). A note for digest algorithm states SHA1 is weaker than sha256.

## Session 04: Firewall

When enabled, if this CA is capable of signing certificates then serial numbers for certificates signed by this CA will be automatically randomized and checked for uniqueness instead of using the sequential value from Next Certificate Serial.

**Internal Certificate Authority**

<u>Key type</u>	RSA
2048	
The length to use when generating a new RSA key, in bits. The Key Length should not be lower than 2048 or some platforms may consider the certificate invalid.	
<u>Digest Algorithm</u>	sha256
The digest method used when the CA is signed. The best practice is to use an algorithm stronger than SHA1. Some platforms may consider weaker digest algorithms invalid	
<u>Lifetime (days)</u>	3650
<u>Common Name</u>	internal-ca
The following certificate authority subject components are optional and may be left blank.	
<u>Country Code</u>	VN
<u>State or Province</u>	HCM
<u>City</u>	HCM
<u>Organization</u>	UIT
<u>Organizational Unit</u>	NTI01.NI1.ANTN

**Save**

### Tạo server certificate

System / Certificate Manager / Certificates / Edit

CAs Certificates **Certificate Revocation**

**Add/Sign a New Certificate**

<u>Method</u>	Create an internal Certificate
<u>Descriptive name</u>	Cau11_Lab4_ne

**Internal Certificate**

<u>Certificate authority</u>	Cau11_Lab4
<u>Key type</u>	RSA
2048	
The length to use when generating a new RSA key, in bits. The Key Length should not be lower than 2048 or some platforms may consider the certificate invalid.	
<u>Digest Algorithm</u>	sha256
The digest method used when the certificate is signed. The best practice is to use an algorithm stronger than SHA1. Some platforms may consider weaker digest algorithms invalid	
<u>Lifetime (days)</u>	3650

<b>Common Name</b>	Cau11_Lab4_Cert
The following certificate subject components are optional and may be left blank.	
<b>Country Code</b>	VN
<b>State or Province</b>	HCM
<b>City</b>	HCM
<b>Organization</b>	UIT
<b>Organizational Unit</b>	NT101.N11.ANTN

**Certificate Attributes**

**Attribute Notes**: The following attributes are added to certificates and requests when they are created or signed. These attributes behave differently depending on the selected mode.

For Internal Certificates, these attributes are added directly to the certificate as shown.

<b>Certificate Type</b>	Server Certificate
Add type-specific usage attributes to the signed certificate. Used for placing usage restrictions on, or granting abilities to, the signed certificate.	
<b>Alternative Names</b>	FQDN or Hostname
Type	Value
Enter additional identifiers for the certificate in this list. The Common Name field is automatically added to the certificate as an Alternative Name. The signing CA may ignore or change these values.	
Add	+ Add
<b>Save</b>	

System / Certificate Manager / Certificates

Created internal certificate Cau11\_Lab4\_ne

CA	Certificates	Certificate Revocation															
<b>Search</b>	Search term <input type="text"/> Both <input type="button" value="Search"/> <input type="button" value="Clear"/> Enter a search string or *nix regular expression to search certificate names and distinguished names.																
<b>Certificates</b> <table border="1"> <thead> <tr> <th>Name</th> <th>Issuer</th> <th>Distinguished Name</th> <th>In Use</th> <th>Actions</th> </tr> </thead> <tbody> <tr> <td>webConfigurator default (638564fd1827f) Server Certificate CA: No Server: Yes</td> <td>self-signed</td> <td>O=pfSense webConfigurator Self-Signed Certificate, CN=pfSense-638564fd1827f  Valid From: Tue, 29 Nov 2022 01:48:45 +0000 Valid Until: Mon, 01 Jan 2024 01:48:45 +0000</td> <td></td> <td> </td> </tr> <tr> <td>Cau11_Lab4_ne Server Certificate CA: No Server: Yes</td> <td>Cau11_Lab4</td> <td>ST=HCM, OU=NT101.N11.ANTN, O=UIT, L=HCM, CN=Cau11_Lab4_Cert, C=VN  Valid From: Wed, 07 Dec 2022 16:06:34 +0000 Valid Until: Sat, 04 Dec 2032 16:06:34 +0000</td> <td></td> <td> </td> </tr> </tbody> </table>			Name	Issuer	Distinguished Name	In Use	Actions	webConfigurator default (638564fd1827f) Server Certificate CA: No Server: Yes	self-signed	O=pfSense webConfigurator Self-Signed Certificate, CN=pfSense-638564fd1827f  Valid From: Tue, 29 Nov 2022 01:48:45 +0000 Valid Until: Mon, 01 Jan 2024 01:48:45 +0000			Cau11_Lab4_ne Server Certificate CA: No Server: Yes	Cau11_Lab4	ST=HCM, OU=NT101.N11.ANTN, O=UIT, L=HCM, CN=Cau11_Lab4_Cert, C=VN  Valid From: Wed, 07 Dec 2022 16:06:34 +0000 Valid Until: Sat, 04 Dec 2032 16:06:34 +0000		
Name	Issuer	Distinguished Name	In Use	Actions													
webConfigurator default (638564fd1827f) Server Certificate CA: No Server: Yes	self-signed	O=pfSense webConfigurator Self-Signed Certificate, CN=pfSense-638564fd1827f  Valid From: Tue, 29 Nov 2022 01:48:45 +0000 Valid Until: Mon, 01 Jan 2024 01:48:45 +0000															
Cau11_Lab4_ne Server Certificate CA: No Server: Yes	Cau11_Lab4	ST=HCM, OU=NT101.N11.ANTN, O=UIT, L=HCM, CN=Cau11_Lab4_Cert, C=VN  Valid From: Wed, 07 Dec 2022 16:06:34 +0000 Valid Until: Sat, 04 Dec 2032 16:06:34 +0000															

=> Hoàn thành tạo hạ tầng khóa công khai PKI

Bước 2: Cấu hình OpenVPN

VPN -> OpenVPN -> Wizard

Wizard / OpenVPN Remote Access Server Setup /

**OpenVPN Remote Access Server Setup**

This wizard will provide guidance through an OpenVPN Remote Access Server Setup.

The wizard may be stopped at any time by clicking the logo image at the top of the screen.

**Select an Authentication Backend Type**

Type of Server: Local User Access

NOTE: If unsure, leave this set to "Local User Access."

» Next

Chọn Local User Access và nhấn next

Wizard / OpenVPN Remote Access Server Setup / Certificate Authority Selection

Step 5 of 11

**Certificate Authority Selection**

OpenVPN Remote Access Server Setup Wizard

**Choose a Certificate Authority (CA)**

Certificate Authority: Cau11\_Lab4

» Add new CA   » Next

Chọn khóa CA đã tạo ở phía trên và nhấn Next

Wizard / OpenVPN Remote Access Server Setup / Server Setup

Step 9 of 11

**Server Setup**

OpenVPN Remote Access Server Setup Wizard

**General OpenVPN Server Information**

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

Protocol: UDP on IPv4 only  
Protocol to use for OpenVPN connections. If unsure, leave this set to UDP.

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

Description: Cau 11  
A name for this OpenVPN instance, for administrative reference. It can be set however desired, but is often used to distinguish the purpose of the service (e.g. "Remote Technical Staff"). It is also used by OpenVPN Client Export to identify this VPN on clients.

**Cryptographic Settings**

TLS Authentication:   
Enable authentication of TLS packets.

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

## Session 04: Firewall

<b>Generate TLS Key</b>	<input checked="" type="checkbox"/>	Automatically generate a shared TLS authentication key.
<b>TLS Shared Key</b>		
Paste in a shared TLS key if one has already been generated.		
<b>DH Parameters Length</b>	2048 bit	
Length of Diffie-Hellman (DH) key exchange parameters, used for establishing a secure communications channel. The DH parameters are different from key sizes, but as with other such settings, the larger the key, the more security it offers, but larger keys take considerably more time to generate. As of 2016, 2048 bit is a common and typical selection.		
<b>Data Encryption Negotiation</b>	<input checked="" type="checkbox"/>	
Enable negotiation of Data Encryption Algorithms between client and server. The best practice is keep this setting enabled.		
<b>Data Encryption Algorithms</b>	AES-256-GCM AES-128-GCM CHACHA20-POLY1305	
List of algorithms clients can negotiate to encrypt traffic between endpoints. The best practice is to use the exact algorithms listed above, in that order. Certain algorithms will perform better on different hardware, depending on the availability of supported VPN accelerator chips. Edit the server after finishing the wizard for additional choices.		
<b>Fallback Data Encryption Algorithm</b>	AES-256-CBC (256 bit key, 128 bit block)	
The algorithm used to encrypt traffic between endpoints when data encryption negotiation is disabled or fails.		
<b>Auth Digest Algorithm</b>	SHA256 (256-bit)	
The method used to authenticate traffic between endpoints. This setting must match on the client and server side, but is otherwise set however desired.		

Điền địa chỉ IP ở tunnel network

Ở local network, điền địa chỉ mạng LAN của pfSense

Tunnel Settings	
<b>Tunnel Network</b>	10.101.1.0/24
This is the virtual network used for private communications between this server and client hosts expressed using CIDR notation (eg. 10.0.8.0/24). The first network address will be assigned to the server virtual interface. The remaining network addresses will be assigned to connecting clients.	
<b>Redirect Gateway</b>	<input checked="" type="checkbox"/>
Force all client generated traffic through the tunnel.	
<b>Local Network</b>	192.168.206.0/24
This is the network that will be accessible from the remote endpoint, expressed as a CIDR range. This may be left blank if not adding a route to the local network through this tunnel on the remote machine. This is generally set to the LAN network.	
<b>Concurrent Connections</b>	10
Specify the maximum number of clients allowed to concurrently connect to this server.	
<b>Allow Compression</b>	Refuse any non-stub compression (Most secure)
Allow compression to be used with this VPN instance, which is potentially insecure.	
<b>Compression</b>	Disable Compression [Omit Preference]
Compress tunnel packets using the chosen option. Can save bandwidth, but is potentially insecure and may expose data. This setting has no effect if compression is not allowed. Adaptive compression will dynamically disable compression for a period of time if OpenVPN detects that the data in the packets is not being compressed efficiently.	
<b>Type-of-Service</b>	<input type="checkbox"/>
Set the TOS IP header value of tunnel packets to match the encapsulated packet's TOS value.	
<b>Inter-Client Communication</b>	<input type="checkbox"/>
Allow communication between clients connected to this server.	

**Client Settings**

<b>Dynamic IP</b>	<input checked="" type="checkbox"/>	Allow connected clients to retain their connections if their IP address changes.
<b>Topology</b>	Subnet -- One IP address per client in a common subnet <input type="button" value="▼"/>	
Specifies the method used to supply a virtual adapter IP address to clients when using tun mode on IPv4. Some clients may require this be set to "subnet" even for IPv6, such as OpenVPN Connect (iOS/Android). Older versions of OpenVPN (before 2.0.9) or clients such as Yealink phones may require "net30".		
<b>DNS Default Domain</b>	<input type="text"/>	
Provide a default domain name to clients.		
<b>DNS Server 1</b>	<input type="text"/>	
DNS server IP to provide to connecting clients.		
<b>DNS Server 2</b>	<input type="text"/>	
DNS server IP to provide to connecting clients.		
<b>DNS Server 3</b>	<input type="text"/>	
DNS server IP to provide to connecting clients.		
<b>DNS Server 4</b>	<input type="text"/>	
DNS server IP to provide to connecting clients.		
<b>NTP Server</b>	<input type="text"/>	
Network Time Protocol server to provide to connecting clients.		
<b>NTP Server 2</b>	<input type="text"/>	
Network Time Protocol server to provide to connecting clients.		
<b>DNS Server 4</b>	<input type="text"/>	
DNS server IP to provide to connecting clients.		
<b>NTP Server</b>	<input type="text"/>	
Network Time Protocol server to provide to connecting clients.		
<b>NTP Server 2</b>	<input type="text"/>	
Network Time Protocol server to provide to connecting clients.		
<b>NetBIOS Options</b>	<input type="checkbox"/>	Enable NetBIOS over TCP/IP. If this option is not set, all NetBIOS-over-TCP/IP options (including WINS) will be disabled.
<b>NetBIOS Node Type</b>	<input style="width: 100px; height: 20px; border: 1px solid #ccc; padding: 2px; margin-bottom: 5px;" type="button" value="none"/>	
Possible options: b-node (broadcasts), p-node (point-to-point name queries to a WINS server), m-node (broadcast then query name server), and h-node (query name server, then broadcast).		
<b>NetBIOS Scope ID</b>	<input type="text"/>	
A NetBIOS Scope ID provides an extended naming service for NetBIOS over TCP/IP. The NetBIOS scope ID isolates NetBIOS traffic on a single network to only those nodes with the same NetBIOS scope ID.		
<b>WINS Server 1</b>	<input type="text"/>	
A Windows Internet Name Service (WINS) server IP to provide to connecting clients. Not desirable in most all modern networks.		
<b>WINS Server 2</b>	<input type="text"/>	
A Windows Internet Name Service (WINS) server IP to provide to connecting clients. Not desirable in most all modern networks.		

**>> Next**

Nhấn tick vào 2 ô Firewall Rule, OpenVPN rule

Wizard / OpenVPN Remote Access Server Setup / Firewall Rule Configuration

Step 10 of 11

### Firewall Rule Configuration

OpenVPN Remote Access Server Setup Wizard

### Firewall Rule Configuration

Firewall rules control what network traffic is permitted. Rules must be added to allow traffic to the OpenVPN server's IP and port, as well as allowing traffic from connected clients through the tunnel. These rules can be automatically added here, or configured manually after completing the wizard.

#### Traffic from clients to server

Firewall Rule

Add a rule to permit connections to this OpenVPN server process from clients anywhere on the Internet.

#### Traffic from clients through VPN

OpenVPN rule

Add a rule to allow all traffic from connected clients to pass inside the VPN tunnel.

**>> Next**

Wizard / OpenVPN Remote Access Server Setup / Finished!

Step 11 of 11

### Finished!

OpenVPN Remote Access Server Setup Wizard

### Configuration Complete!

The configuration is now complete.

To be able to export client configurations, browse to System->Packages and install the OpenVPN Client Export package.

**>> Finish**

VPN / OpenVPN / Servers

Servers Clients Client Specific Overrides Wizards

### OpenVPN Servers

Interface	Protocol / Port	Tunnel Network	Mode / Crypto	Description	Actions
WAN	UDP4 / 1194 (TUN)	10.101.1.0/24	<b>Mode:</b> Remote Access ( SSL/TLS + User Auth ) <b>Data Ciphers:</b> AES-256-GCM, AES-128-GCM, CHACHA20-POLY1305, AES-256-CBC <b>Digest:</b> SHA256 <b>D-H Params:</b> 2048 bits	Cau 11	

**+ Add**

=> Hoàn tất cấu hình OpenVPN

Cấu hình quyền truy cập của client:

VPN / OpenVPN / Clients

Servers Clients Client Specific Overrides Wizards

### OpenVPN Clients

Interface	Protocol	Server	Mode / Crypto	Description	Actions

Địa chỉ server là địa chỉ máy pfSense

**General Information**

**Description**: Lab4\_VPNClient  
A description of this VPN for administrative reference.

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

**Mode Configuration**

**Server mode**: Peer to Peer (SSL/TLS)

**Device mode**: tun - Layer 3 Tunnel Mode  
"tun" mode carries IPv4 and IPv6 (OSI layer 3) and is the most common and compatible mode across all platforms.  
"tap" mode is capable of carrying 802.3 (OSI Layer 2.)

**Endpoint Configuration**

**Protocol**: UDP on IPv4 only

**Interface**: WAN  
The interface used by the firewall to originate this OpenVPN client connection

**Local port**:  
Set this option to bind to a specific port. Leave this blank or enter 0 for a random dynamic port.

**Server host or address**: 192.168.182.128  
The IP address or hostname of the OpenVPN server.

**Server port**: 1194

Tạo tài khoản naruto:naruto@123

**User Authentication Settings**

**Username**: naruto  
Leave empty when no user name is needed

**Password**:  \*\*\*\*\*  
Leave empty when no password is needed

**Authentication Retry**:  Do not retry connection when authentication fails  
When enabled, the OpenVPN process will exit if it receives an authentication failure message. The default behavior is to retry. i

**Cryptographic Settings**

<b>TLS Configuration</b>	<input checked="" type="checkbox"/> Use a TLS Key A TLS key enhances security of an OpenVPN connection by requiring both parties to have a common key before a peer can perform a TLS handshake. This layer of HMAC authentication allows control channel packets without the proper key to be dropped, protecting the peers from attack or unauthorized connections. The TLS Key does not have any effect on tunnel data.  <input checked="" type="checkbox"/> Automatically generate a TLS Key.	
<b>TLS keydir direction</b>	Use default direction	
The TLS Key Direction must be set to complementary values on the client and server. For example, if the server is set to 0, the client must be set to 1. Both may be set to omit the direction, in which case the TLS Key will be used bidirectionally.		
<b>Peer Certificate Authority</b>	Cau11_Lab4	
<b>Peer Certificate Revocation list</b>	No Certificate Revocation Lists defined. One may be created here: <a href="#">System &gt; Cert. Manager &gt; Certificate Revocation</a>	
<b>Client Certificate</b>	None (Username and/or Password required)	
<b>Data Encryption Negotiation</b>	<input checked="" type="checkbox"/> Enable Data Encryption Negotiation This option allows OpenVPN clients and servers to negotiate a compatible set of acceptable cryptographic data encryption algorithms from those selected in the Data Encryption Algorithms list below. Disabling this feature is deprecated.	
<b>Data Encryption Algorithms</b>	AES-128-CBC (128 bit key, 128 bit block) AES-128-CFB (128 bit key, 128 bit block) AES-128-CFB1 (128 bit key, 128 bit block) AES-128-CFB8 (128 bit key, 128 bit block) AES-128-GCM (128 bit key, 128 bit block) AES-128-OFB (128 bit key, 128 bit block) AES-192-CBC (192 bit key, 128 bit block) AES-192-CFB (192 bit key, 128 bit block) AES-192-CFB1 (192 bit key, 128 bit block) AES-192-CFB8 (192 bit key, 128 bit block)	AES-256-GCM AES-128-GCM CHACHA20-POLY1305
	AES-192-CFB1 (192 bit key, 128 bit block) AES-192-CFB8 (192 bit key, 128 bit block)	Available Data Encryption Algorithms Click to add or remove an algorithm from the list
		Allowed Data Encryption Algorithms. Click an algorithm name to remove it from the list
	The order of the selected Data Encryption Algorithms is respected by OpenVPN. This list is ignored in Shared Key mode. <a href="#">i</a>	
<b>Fallback Data Encryption Algorithm</b>	AES-256-CBC (256 bit key, 128 bit block)	The Fallback Data Encryption Algorithm used for data channel packets when communicating with clients that do not support data encryption algorithm negotiation (e.g. Shared Key). This algorithm is automatically included in the Data Encryption Algorithms list.
<b>Auth digest algorithm</b>	SHA256 (256-bit)	The algorithm used to authenticate data channel packets, and control channel packets if a TLS Key is present. When an AEAD Encryption Algorithm mode is used, such as AES-GCM, this digest is used for the control channel only, not the data channel. Set this to the same value as the server. While SHA1 is the default for OpenVPN, this algorithm is insecure.
<b>Hardware Crypto</b>	No Hardware Crypto Acceleration	
<b>Server Certificate Key Usage Validation</b>	<input checked="" type="checkbox"/> Enforce key usage Verify that remote host uses a server certificate (EKG: "TLS Web Server Authentication").	

Ở Gateway creation, tick vào IPv4 only

**Advanced Configuration**

Custom options

Enter any additional options to add to the OpenVPN client configuration here, separated by semicolon.

**UDP Fast I/O**  Use fast I/O operations with UDP writes to tun/tap. Experimental.  
Optimizes the packet write event loop, improving CPU efficiency by 5% to 10%. Not compatible with all platforms, and not compatible with OpenVPN bandwidth limiting.

**Exit Notify**  Send an explicit exit notification to connected servers/peers when restarting or shutting down, so they may immediately disconnect rather than waiting for a timeout. This value controls how many times this instance will attempt to send the exit notification.  
This option is ignored in Peer-to-Peer Shared Key mode and in SSL/TLS mode with a /30 tunnel network as it will cause the server to exit and not restart.

**Send/Receive Buffer**  Configure a Send and Receive Buffer size for OpenVPN. The default buffer size can be too small in many cases, depending on hardware and network uplink speeds. Finding the best buffer size can take some experimentation. To test the best value for a site, start at 512KIB and test higher and lower values.

**Gateway creation**  Both  IPv4 only  IPv6 only  
If you assign a virtual interface to this OpenVPN client, this setting controls which gateway types will be created. The default setting is 'both'.

**Verbosity level**  Each level shows all info from the previous levels. Level 3 is recommended for a good summary of what's happening without being swamped by output.  
None: Only fatal errors

VPN / OpenVPN / Clients

Servers Clients Client Specific Overrides Wizards

**OpenVPN Clients**

Interface	Protocol	Server	Mode / Crypto	Description	Actions
WAN	UDP4 (TUN)	192.168.182.128:1194	<b>Mode:</b> Peer to Peer ( SSL/TLS ) <b>Data Ciphers:</b> AES-256-GCM, AES-128-GCM, CHACHA20-POLY1305, AES-256-CBC <b>Digest:</b> SHA256	Lab4_VPNClient	

Add

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

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

System / Package Manager / Available Packages

Installed Packages Available Packages

**Search**

Search term: openvpn

Enter a search string or \*nix regular expression to search package names and descriptions.

Name	Version	Description	Action
openvpn-client-export	1.6_8	Allows a pre-configured OpenVPN Windows Client or Mac OS X's Viscosity configuration bundle to be exported directly from pfSense.	+ Install
WireGuard	0.1.6_2	WireGuard(R) is an extremely simple yet fast and modern VPN that utilizes state-of-the-art cryptography. It aims to be faster, simpler, leaner, and more useful than IPSec, while avoiding the massive headache. It intends to be considerably more performant than OpenVPN. WireGuard is designed as a general purpose VPN for running on embedded interfaces and super computers alike, fit for many different circumstances. Initially released for the Linux kernel, it is now cross-platform and widely deployable. It is currently under heavy development, but already it might be regarded as the most secure, easiest to use, and simplest VPN solution in the industry. This package is EXPERIMENTAL.	+ Install

Package Dependencies:

- openvpn-client-export-2.5.2
- openvpn-2.5.4\_1
- zip-3.0\_1
- p7zip-16.02\_3
- wireguard-tools-1.0.20210914\_1
- wireguard-kmod-0.20211105

Nhấn install openvpn-clientexport và chọn confirm

Màn hình tải hoàn tất

System / Package Manager / Package Installer

pfSense-pkg-openvpn-client-export installation successfully completed.

Installed Packages Available Packages Package Installer

**Package Installation**

```
--> NOTICE:
The p7zip port currently does not have a maintainer. As a result, it is
more likely to have unresolved issues, not be up-to-date, or even be removed in
the future. To volunteer to maintain this port, please create an issue at:
https://bugs.freebsd.org/bugzilla

More information about port maintainership is available at:
https://docs.freebsd.org/en/articles/contributing/#ports-contributing
>>> Cleaning up cache... done.
Success
```

Tạo user VPN

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

System / User Manager / Users / Edit

Users Groups Settings Authentication Servers

### User Properties

Defined by	USER
Disabled	<input type="checkbox"/> This user cannot login
Username	naruto
Password	*****
Full name	Lab4_OpenVPN
User's full name, for administrative information only	
Expiration date	
Leave blank if the account shouldn't expire, otherwise enter the expiration date as MM/DD/YYYY	
Custom Settings	<input type="checkbox"/> Use individual customized GUI options and dashboard layout for this user.
Group membership	admins
Not member of <span style="float: right;">Member of</span> <span style="border: 1px solid #ccc; padding: 2px;">» Move to "Member of" list</span> <span style="border: 1px solid #ccc; padding: 2px;">« Move to "Not member of" list</span> <small>Hold down CTRL (PC)/COMMAND (Mac) key to select multiple items.</small>	

Tạo certificate cho người dùng

### Create Certificate for User

Descriptive name	Cau11_Lab4_VPNuser_cert
Certificate authority	Cau11_Lab4
Key type	RSA
2048 <small>The length to use when generating a new RSA key, in bits. The Key Length should not be lower than 2048 or some platforms may consider the certificate invalid.</small>	
Digest Algorithm	sha256
sha256 <small>The digest method used when the certificate is signed. The best practice is to use an algorithm stronger than SHA1. Some platforms may consider weaker digest algorithms invalid</small>	
Lifetime	3650

### Keys

Authorized SSH Keys	
Enter authorized SSH keys for this user <small>(Leave empty to disable)</small>	
IPsec Pre-Shared Key	

Nhấn save để lưu

The screenshot shows the 'Users' section of the User Manager. It lists two users: 'admin' (System Administrator) and 'naruto' (Lab4\_OpenVPN). Both users have a checked status and belong to the 'admins' group. There are edit and delete icons for each user. Below the table are 'Add' and 'Delete' buttons.

Username	Full name	Status	Groups	Actions
admin	System Administrator	✓	admins	
naruto	Lab4_OpenVPN	✓		

Export file openvpn cho user

The screenshot shows the 'OpenVPN Clients' section. It lists a single user 'naruto' with a certificate named 'Cau11\_Lab4\_VPNuser\_cert'. Below the table, there are several download options for different clients and configurations.

User	Certificate Name	Export
naruto	Cau11_Lab4_VPNuser_cert	<ul style="list-style-type: none"> <li>- Inline Configurations:</li> <li> Most Clients  Android  OpenVPN Connect (iOS/Android)</li> <li>- Bundled Configurations:</li> <li> Archive  Config File Only</li> <li>- Current Windows Installers (2.5.2-1x01):</li> <li> 64-bit  32-bit</li> <li>- Legacy Windows Installers (2.4.11-1x01):</li> <li> 10/2016/2019  7/8/8.1/2012/2</li> <li>- Viscosity (Mac OS X and Windows):</li> <li> Viscosity Bundle  Viscosity Inline Config</li> </ul>

Only OpenVPN-compatible user certificates are shown

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

Ip máy A:

```
ubuntu_vm@ubuntuvm2:~$ ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
        inet 192.168.206.128 netmask 255.255.255.0 broadcast 192.168.206.255
        inet6 fe80::d2b5:f769:30f9:7b4 prefixlen 64 scopeid 0x20<link>
          ether 00:0c:29:c9:77:6d txqueuelen 1000 (Ethernet)
            RX packets 40394 bytes 47800744 (47.8 MB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 15907 bytes 2497788 (2.4 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 11346 bytes 30230182 (30.2 MB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 11346 bytes 30230182 (30.2 MB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Kết quả khi ping từ B sang A

```
bp@nbp-virtual-machine:~/Downloads$ sudo openvpn --config pfSense-UDP4-1194-naruto-config.ovpn
PING 192.168.206.128 (192.168.206.128) 56(84) bytes of data.
64 bytes from 192.168.206.128: icmp_seq=1 ttl=63 time=16.1 ms
64 bytes from 192.168.206.128: icmp_seq=2 ttl=63 time=4.13 ms
64 bytes from 192.168.206.128: icmp_seq=3 ttl=63 time=3.75 ms
64 bytes from 192.168.206.128: icmp_seq=4 ttl=63 time=6.51 ms
64 bytes from 192.168.206.128: icmp_seq=5 ttl=63 time=3.71 ms
64 bytes from 192.168.206.128: icmp_seq=6 ttl=63 time=4.22 ms
64 bytes from 192.168.206.128: icmp_seq=7 ttl=63 time=4.01 ms
^C
--- 192.168.206.128 ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6012ms
rtt min/avg/max/mdev = 3.712/6.061/16.099/4.194 ms
bp@nbp-virtual-machine:~/Downloads$
```

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

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

---

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

## YÊU CẦU CHUNG

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

### Báo cáo:

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

*Ví dụ: [NT101.K11.ANTT]-Session1\_Group3.*

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

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

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

*Bài sao chép, trẽ, ... sẽ được xử lý tùy mức độ vi phạm.*

**HẾT**