

BÁO CÁO THỰC HÀNH

Môn học: AN TOÀN MẠNG

Tên chủ đề: LAB 5 – KHAI THÁC TƯỜNG LỬA TRONG LINUX

GVHD: Tô Trọng Nghĩa

Nhóm: 12

1. THÔNG TIN CHUNG:

Lớp: NT140.P11.ANTT.2

STT	Họ và tên	MSSV	Email
1	Thái Ngọc Diễm Trinh	22521541	22521541@gm.uit.edu.vn
2	Phan Nguyễn Nhật Trâm	22521501	22521501@gm.uit.edu.vn

2. NỘI DUNG THỰC HIỆN:¹

STT	Nội dung	Tình trạng	Trang
1	Thiết lập chính sách trên Firewall để bảo vệ mạng nội bộ	100%	2 – 10
2	Vượt qua sự kiểm soát của Firewall	100%	11 – 16
3	Triển khai Web Proxy (Application Firewall)	100%	17 – 21
4	VPN	100%	22 – 36
Điểm tự đánh giá			10/10

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

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

BÁO CÁO CHI TIẾT

A. Cài đặt pfSense firewall

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

Trước khi triển khai các rule trên firewall:

- Máy A: ping đến pfSense, máy B, Internet

```
vm-a-lan@lan:~$ ping 10.0.3.2
PING 10.0.3.2 (10.0.3.2) 56(84) bytes of data.
64 bytes from 10.0.3.2: icmp_seq=1 ttl=64 time=2.07 ms
64 bytes from 10.0.3.2: icmp_seq=2 ttl=64 time=0.815 ms
64 bytes from 10.0.3.2: icmp_seq=3 ttl=64 time=1.37 ms
^C
--- 10.0.3.2 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2004ms
rtt min/avg/max/mdev = 0.815/1.420/2.073/0.514 ms
vm-a-lan@lan:~$ ping 10.0.3.4
PING 10.0.3.4 (10.0.3.4) 56(84) bytes of data.
64 bytes from 10.0.3.4: icmp_seq=1 ttl=63 time=8.58 ms
64 bytes from 10.0.3.4: icmp_seq=2 ttl=63 time=1.50 ms
^C
--- 10.0.3.4 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1003ms
rtt min/avg/max/mdev = 1.499/5.037/8.575/3.538 ms
vm-a-lan@lan:~$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=127 time=29.2 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=127 time=24.7 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=127 time=25.5 ms
^C
--- 8.8.8.8 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2005ms
rtt min/avg/max/mdev = 24.707/26.476/29.220/1.967 ms
vm-a-lan@lan:~$
```

- Máy B: ping đến pfSense, máy A, Internet

```
vm-b-wan@wan:~$ ping 10.0.3.2
PING 10.0.3.2 (10.0.3.2) 56(84) bytes of data.
64 bytes from 10.0.3.2: icmp_seq=1 ttl=64 time=1.48 ms
64 bytes from 10.0.3.2: icmp_seq=2 ttl=64 time=0.873 ms
^C
--- 10.0.3.2 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1005ms
rtt min/avg/max/mdev = 0.873/1.177/1.481/0.304 ms
vm-b-wan@wan:~$ ping 192.168.3.3
PING 192.168.3.3 (192.168.3.3) 56(84) bytes of data.
64 bytes from 192.168.3.3: icmp_seq=1 ttl=128 time=7.00 ms
64 bytes from 192.168.3.3: icmp_seq=2 ttl=128 time=1.44 ms
^C
--- 192.168.3.3 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1002ms
rtt min/avg/max/mdev = 1.444/4.224/7.004/2.780 ms
vm-b-wan@wan:~$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=128 time=23.4 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=128 time=23.7 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=128 time=23.2 ms
^C
--- 8.8.8.8 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2005ms
rtt min/avg/max/mdev = 23.192/23.441/23.715/0.214 ms
vm-b-wan@wan:~$
```

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.

- Thiết lập rule trong pfSense: Chặn các kết nối trong mạng LAN, giao thức ICMP, từ mạng 192.168.3.0/24 đến máy B (10.0.3.4)

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.

ICMP Subtypes
Alternate Host
Datagram conversion error
Echo reply
For ICMP rules on IPv4, one or more of these ICMP subtypes may be specified.

Source
 ☐ Invert match /

Destination
 ☐ Invert match

- Trước khi thiết lập rule: Máy A vẫn có thể ping được đến máy B

```
vm-a-lan@lan:~$ ping 10.0.3.4
PING 10.0.3.4 (10.0.3.4) 56(84) bytes of data.
64 bytes from 10.0.3.4: icmp_seq=1 ttl=63 time=5.35 ms
64 bytes from 10.0.3.4: icmp_seq=2 ttl=63 time=2.43 ms
64 bytes from 10.0.3.4: icmp_seq=3 ttl=63 time=2.27 ms
^C
--- 10.0.3.4 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2006ms
rtt min/avg/max/mdev = 2.273/3.351/5.351/1.415 ms
```

- Sau khi thiết lập rule: Máy A không thể ping đến máy B được nữa

```
vm-a-lan@lan:~$ ping 10.0.3.4
PING 10.0.3.4 (10.0.3.4) 56(84) bytes of data.
^C
--- 10.0.3.4 ping statistics ---
4 packets transmitted, 0 received, 100% packet loss, time 3105ms
```

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

- Thiết lập rule trong pfSense: Chặn các kết nối trong mạng LAN, giao thức TCP/UDP, từ mạng 192.168.3.0/24 đến cổng 80 (HTTP)

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**.

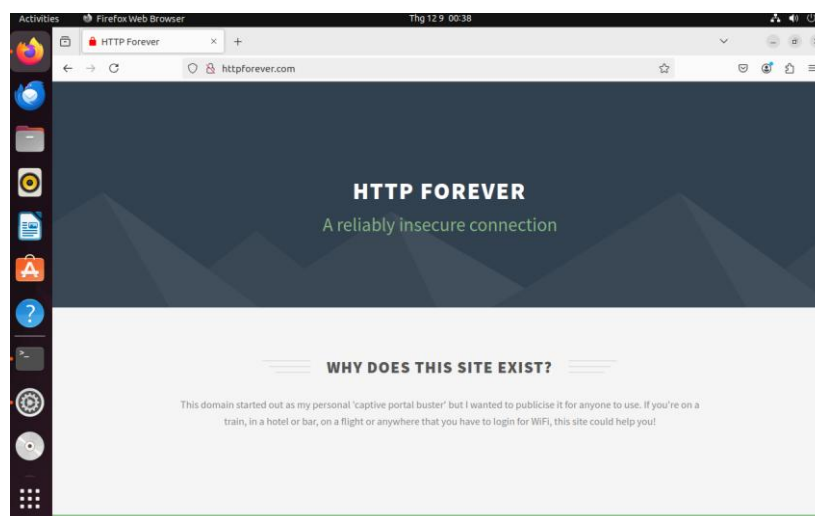
Destination

Destination ☐ Invert match /

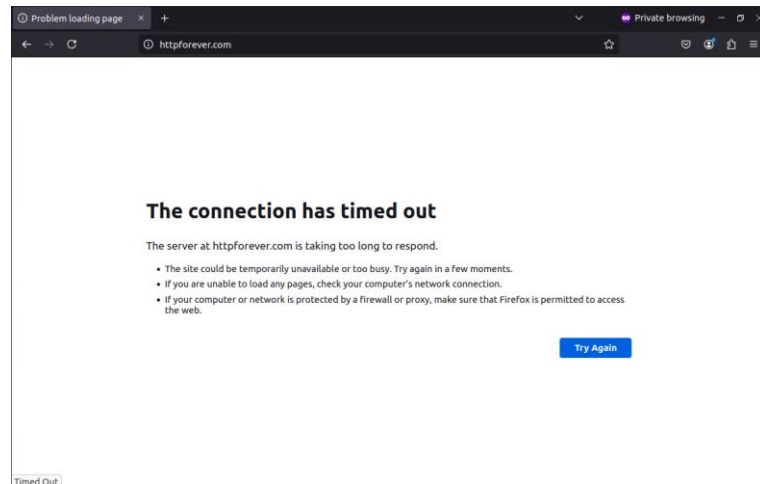
Destination Port Range
From To

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

- Trước khi thiết lập rule: Máy A vẫn có thể truy cập vào 1 trang web http bất kì



- Sau khi thiết lập rule: Máy A không thể truy cập được trang web http nữa



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

- Thiết lập rule trong pfSense: Chặn các kết nối trong mạng LAN, giao thức TCP/UDP, từ mạng 192.168.3.0/24 đến cổng 23

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 ☐ 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 Telnet (23) From Custom To Custom
Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.

- Trước khi thiết lập rule:
 - Trên máy B bật dịch vụ Telnet

```
vm-b-wan@wan:~$ sudo systemctl status inetd
● inetd.service - Internet superserver
   Loaded: loaded (/lib/systemd/system/inetd.service; enabled; vendor preset: ena
   Active: active (running) since Fri 2024-12-13 00:00:34 +07; 11h ago
     Docs: man:inetd(8)
   Main PID: 6837 (inetd)
    Tasks: 1 (limit: 2213)
   Memory: 1.1M
      CPU: 177ms
   CGroup: /system.slice/inetd.service
           └─6837 /usr/sbin/inetd

Thg 12 13 00:00:34 wan systemd[1]: Starting Internet superserver...
Thg 12 13 00:00:34 wan systemd[1]: Started Internet superserver.
Thg 12 13 11:45:58 wan in.telnetd[7800]: connect from 10.0.3.2 (10.0.3.2)
Thg 12 13 11:46:10 wan login[7801]: pam_unix(login:auth): check pass; user unknow
Thg 12 13 11:46:10 wan login[7801]: pam_unix(login:auth): authentication failure
Thg 12 13 11:46:12 wan login[7801]: FAILED LOGIN (1) on '/dev/pts/1' from '10.0.3
lines 1-17/17 (END)
```

- Máy A thực hiện telnet đến máy B thành công

```
vm-a-lan@lan:~$ telnet 10.0.3.4
Trying 10.0.3.4...
Connected to 10.0.3.4.
Escape character is '^'.
Ubuntu 22.04.5 LTS
wan login: vm-b-wan
Password:
Welcome to Ubuntu 22.04.5 LTS (GNU/Linux 6.8.0-40-generic x86_64)

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

Expanded Security Maintenance for Applications is not enabled.

137 updates can be applied immediately.
110 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable

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

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

Last login: Fri Dec 13 11:48:12 +07 2024 from 10.0.3.2 on pts/2
vm-b-wan@wan:~$ ls
Desktop  Documents  Downloads  Music  Pictures  Public  snap  Templates  Videos
vm-b-wan@wan:~$ whoami
vm-b-wan
vm-b-wan@wan:~$
```

- Sau khi thiết lập rule: Máy A không thể telnet đến máy B được nữa

```
vm-a-lan@lan:~$ telnet 10.0.3.4
Trying 10.0.3.4...
telnet: Unable to connect to remote host: Connection timed out
vm-a-lan@lan:~$
```

4. Không cho phép các máy trong mạng nội bộ truy cập đến www.facebook.com và [youtube.com](https://www.youtube.com).

Cách 1: Sử dụng DNS Resolver để khi máy A thực hiện phân giải tên miền facebook.com và youtube.com, kết quả sẽ trả về địa chỉ loopback (127.0.0.1) thay vì địa chỉ IP thực của các tên miền này

- Truy cập DNS Resolver trong pfSense, ở tab Domain Override, thêm thông tin tên miền cần đổi

Lab 05: KHAI THÁC TƯỜNG LỬA TRONG LINUX

Nhóm 12



- Facebook

Services / DNS Resolver / General Settings / Edit Domain Override

Domains to Override with Custom Lookup Servers

Domain	facebook.com
Domain whose lookups will be directed to a user-specified DNS lookup server.	
IP Address	127.0.0.1
IPv4 or IPv6 address of the authoritative DNS server for this domain. e.g.: 192.168.100.100 To use a non-default port for communication, append an '@' with the port number.	
TLS Queries	<input type="checkbox"/> Use SSL/TLS for DNS Queries forwarded to this server When set, queries to all DNS servers for this domain will be sent using SSL/TLS on the default port of 853.
TLS Hostname	
An optional TLS hostname used to verify the server certificate when performing TLS Queries.	
Description	Blocking Facebook
A description may be entered here for administrative reference (not parsed).	

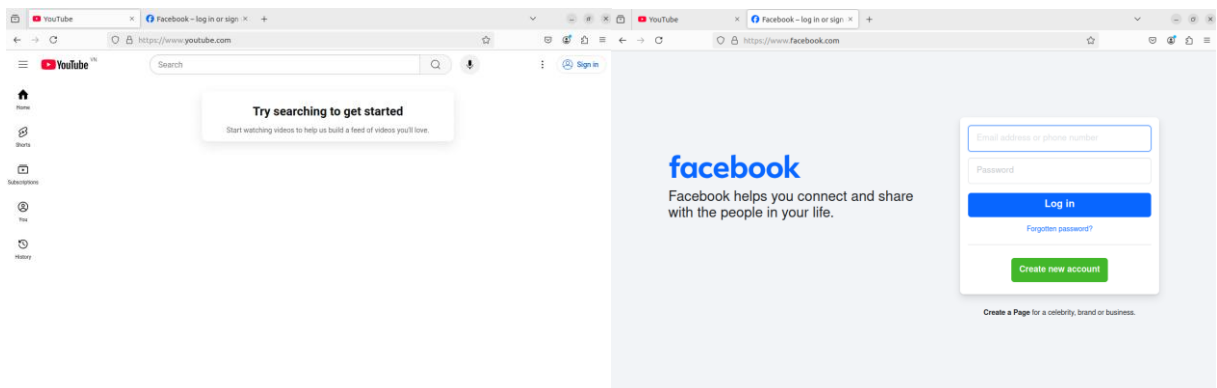
- Youtube

Services / DNS Resolver / General Settings / Edit Domain Override

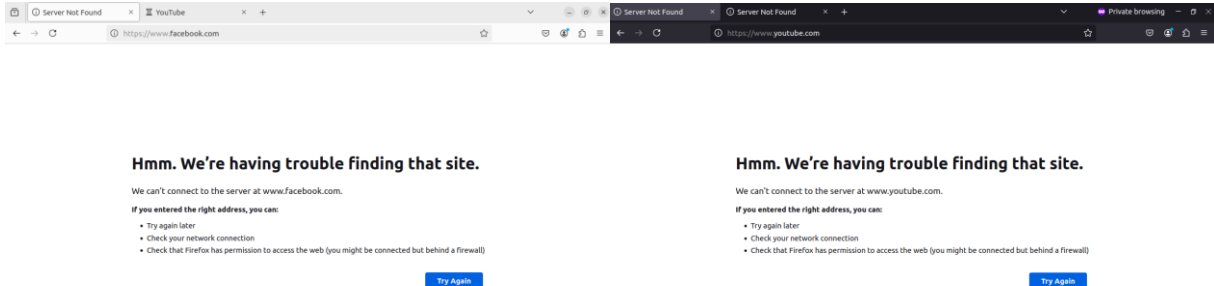
Domains to Override with Custom Lookup Servers

Domain	youtube.com
Domain whose lookups will be directed to a user-specified DNS lookup server.	
IP Address	127.0.0.1
IPv4 or IPv6 address of the authoritative DNS server for this domain. e.g.: 192.168.100.100 To use a non-default port for communication, append an '@' with the port number.	
TLS Queries	<input type="checkbox"/> Use SSL/TLS for DNS Queries forwarded to this server When set, queries to all DNS servers for this domain will be sent using SSL/TLS on the default port of 853.
TLS Hostname	
An optional TLS hostname used to verify the server certificate when performing TLS Queries.	
Description	Blocking Youtube
A description may be entered here for administrative reference (not parsed).	

- Trước khi thiết lập rule: Máy A vẫn có thể truy cập facebook.com và youtube.com



- Sau khi thiết lập rule: Máy A không thể phân giải tên miền facebook.com và youtube.com \Rightarrow không thể truy cập trang web. Tuy nhiên nếu máy A đổi DNS Server thành địa chỉ khác (như 8.8.8.8,...) thay vì là địa chỉ của pfSense (192.168.3.2) thì vẫn có thể truy cập được



Cách 2: Chặn các địa chỉ IP của facebook.com và youtube.com

- Trong Aliases, chọn Bulk import để có thể tạo 1 danh sách chứa nhiều địa chỉ IP cùng một lúc

Firewall / Aliases / Bulk import

IP Alias Details

Alias Name	facebook_youtube
The name of the alias may only consist of the characters "a-z, A-Z, 0-9 and _".	
Description	Blocking Facebook and Youtube
A description may be entered here for administrative reference (not parsed).	
Aliases to import	<div>185.60.216.0/24 185.60.218.0/23 185.158.208.0/24 186.208.210.0/24 187.7.116.0/24</div> <p>Paste in the aliases to import separated by a carriage return. Common examples are lists of IPs, networks, blacklists, etc. The list may contain IP addresses, with or without CIDR prefix, IP ranges, blank lines (ignored) and an optional description after each IP. e.g.:</p> <ul style="list-style-type: none">• 172.16.1.2• 172.16.0.0/24• 10.11.12.100-10.11.12.200• 192.168.1.254 Home router• 10.20.0.0/16 Office network• 10.40.1.10-10.40.1.19 Managed switches

Đối với địa chỉ facebook, nhóm sử dụng lệnh nslookup để tìm. Đối với địa chỉ của youtube.com, nhóm sử dụng danh sách này

(<https://raw.githubusercontent.com/touhidurrr/iplist-youtube/main/cidr4.txt>)

Lab 05: KHAI THÁC TƯỜNG LỬA TRONG LINUX

Nhóm 12



- Thiết lập rule trên pfSense: Chặn các kết nối trong mạng LAN, giao thức TCP/UDP, từ mạng 192.168.3.0/24 đến các địa chỉ trong alias vừa tạo (chứa địa chỉ của facebook.com và youtube.com)

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 ☐ 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.

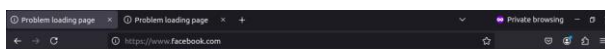
Destination

Destination ☐ Invert match Single host or alias facebook_youtube

Destination Port Range any From Custom To Custom

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

- Sau khi thiết lập rule: Máy A không thể truy cập được facebook.com và youtube.com



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](#)

Timed Out:

The connection has timed out

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](#)

Timed Out:

Toàn bộ các rule đã được thiết lập:

<input type="checkbox"/>	<input checked="" type="checkbox"/>	0 / 3 KiB	IPv4 TCP/UDP	192.168.3.0/24	*	facebook_ youtube	*	*	none	Không cho phép các máy trong mạng nội bộ truy cập đến www.facebook.com và youtube.com	
<input type="checkbox"/>	<input checked="" type="checkbox"/>	0 / 3 KiB	IPv4 TCP/UDP	192.168.3.0/24	*	*	23 (Telnet)	*	none	Chặn kết nối telnet từ mạng nội bộ ra bên ngoài	
<input type="checkbox"/>	<input checked="" type="checkbox"/>	0 / 3.68 MiB	IPv4 TCP/UDP	192.168.3.0/24	*	*	80 (HTTP)	*	none	Không cho phép các máy trong mạng nội bộ truy cập các website sử dụng giao thức http (cổng 80).	
<input type="checkbox"/>	<input checked="" type="checkbox"/>	0 / 1008 B	IPv4 ICMP any	192.168.3.0/24	*	10.0.3.4	*	*	none	Không cho phép các máy trong mạng nội bộ (192.168.3.0/24) thực hiện ping đến máy VM B	

C. Vượt qua sự kiểm soát của Firewall

1. Thực hiện Telnet từ máy A đến máy B

Chạy ssh và telnet trên máy B

```
vm-b-wan@wan:~$ sudo systemctl status ssh inetd
● ssh.service - OpenBSD Secure Shell server
   Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: en
   Active: active (running) since Fri 2024-12-13 14:43:51 +07; 1min 1s ago
     Docs: man:sshd(8)
           man:sshd_config(5)
    Main PID: 59878 (sshd)
      Tasks: 1 (limit: 2213)
     Memory: 1.7M
        CPU: 80ms
    CGroup: /system.slice/ssh.service
            └─59878 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

Thg 12 13 14:43:51 wan systemd[1]: Starting OpenBSD Secure Shell server...
Thg 12 13 14:43:51 wan sshd[59878]: Server listening on 0.0.0.0 port 22.
Thg 12 13 14:43:51 wan sshd[59878]: Server listening on :: port 22.
Thg 12 13 14:43:51 wan systemd[1]: Started OpenBSD Secure Shell server.

● inetd.service - Internet superserver
   Loaded: loaded (/lib/systemd/system/inetd.service; enabled; vendor preset: en
   Active: active (running) since Fri 2024-12-13 11:52:23 +07; 2h 52min ago
     Docs: man:inetd(8)
    Main PID: 8112 (inetd)
      Tasks: 1 (limit: 2213)
     Memory: 212.0K
        CPU: 2.320s
    CGroup: /system.slice/inetd.service
            └─8112 /usr/sbin/inetd

Thg 12 13 11:52:23 wan systemd[1]: Starting Internet superserver...
Thg 12 13 11:52:23 wan systemd[1]: Started Internet superserver.
lines 1-30/30 (END)
```

Tạo 1 SSH Tunnel ở máy A, sau đó kết nối telnet đến máy B thông qua tunnel

```
vm-a-lan@lan:~$ ssh -fN -L 8000:localhost:23 vm-b-wan@10.0.3.4
vm-b-wan@10.0.3.4's password:
vm-a-lan@lan:~$ telnet localhost 8000
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^J'.
Ubuntu 22.04.5 LTS
wan login: vm-b-wan
Password:
Welcome to Ubuntu 22.04.5 LTS (GNU/Linux 6.8.0-40-generic x86_64)

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

Expanded Security Maintenance for Applications is not enabled.

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

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

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

*** System restart required ***
Last login: Fri Dec 13 15:01:25 +07 2024 from 10.0.3.2 on pts/2
vm-b-wan@wan:~$ whoami
vm-b-wan
vm-b-wan@wan:~$
```

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-wan@10.0.3.4

- ssh: Sử dụng giao thức SSH
- -f: SSH sẽ chạy ở chế độ nền sau khi xác thực
- -N: Dùng để thiết lập tunnel mà không cần thực thi bất kỳ lệnh nào trên máy từ xa.
- -L 8000:localhost:23: Cấu hình local port forwarding, tạo một tunnel giữa cổng 8000 trên máy cục bộ (local) và cổng 23 trên máy từ xa
 - 8000: Cổng trên máy cục bộ (máy A)
 - localhost: Địa chỉ máy từ xa (vm-b-wan@10.0.3.4)
 - 23: Cổng trên máy từ xa muốn truy cập qua tunnel (Telnet)
- vm-b-wan@10.0.3.4: Thông tin người dùng và địa chỉ IP của máy từ xa đang kết nối đến.

- telnet localhost 8000

- telnet: Sử dụng giao thức telnet
- localhost: Đây là địa chỉ của máy tính cục bộ
- 8000: Đây là cổng đã chuyển tiếp từ máy cục bộ đến máy từ xa thông qua SSH. Với lệnh ssh -L 8000:localhost:23 vm-b-wan@10.0.3.4, tạo một SSH tunnel trên cổng 8000 của máy cục bộ. Do đó, khi chạy telnet localhost 8000, lưu lượng sẽ được chuyển tiếp qua SSH tunnel đến cổng 23 trên máy từ xa, nơi dịch vụ Telnet đang chạy.

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, các gói tin vẫn đi qua Firewall.

Nguyên nhân: Firewall chỉ được cấu hình để chặn các gói tin trao đổi qua cổng 23 (Telnet), ở ví dụ trên, các gói tin được trao đổi qua dịch vụ ssh nằm ở cổng 22, lưu lượng telnet đã được mã hóa qua kết nối ssh nên firewall không thể phát hiện được.

2. Kết nối đến Facebook sử dụng SSH Tunnel

• Bước 1: Tạo SSH Tunnel trên máy A

```
vm-a-lan@lan:~$ ssh -D 9000 -C vm-b-wan@10.0.3.4
vm-b-wan@10.0.3.4's password:
Welcome to Ubuntu 22.04.5 LTS (GNU/Linux 6.8.0-40-generic x86_64)

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

Expanded Security Maintenance for Applications is not enabled.

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

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

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

*** System restart required ***
Last login: Fri Dec 13 15:13:29 2024 from localhost
vm-b-wan@wan:~$
```

• Bước 2: Cấu hình proxy trên trình duyệt

Connection Settings

☐ Use system proxy settings

☒ Manual proxy configuration

HTTP Proxy Port

☐ Also use this proxy for HTTPS

HTTPS Proxy Port

SOCKS Host Port

☐ SOCKS v4 ☒ SOCKS v5

☐ Automatic proxy configuration URL

No proxy for

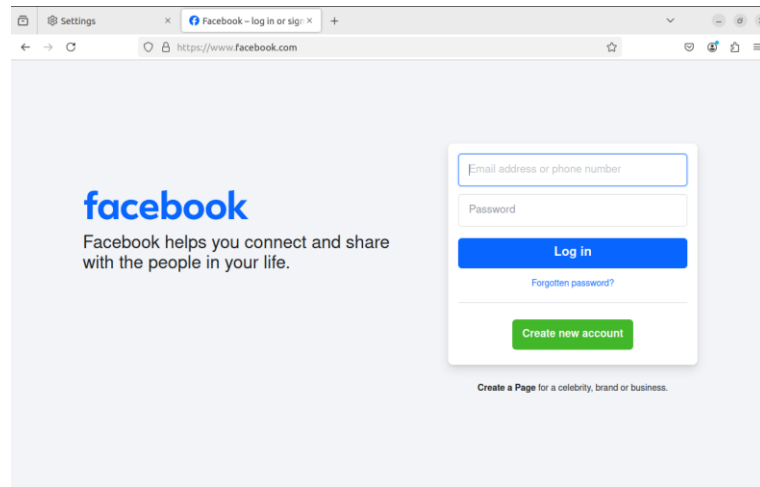
Example: .mozilla.org, .net.nz, 192.168.1.0/24
Connections to localhost, 127.0.0.1/8, and ::1 are never proxied.

☐ Do not prompt for authentication if password is saved

☐ Proxy DNS when using SOCKS v4

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

Lúc này máy A sẽ có thể truy cập được facebook.com

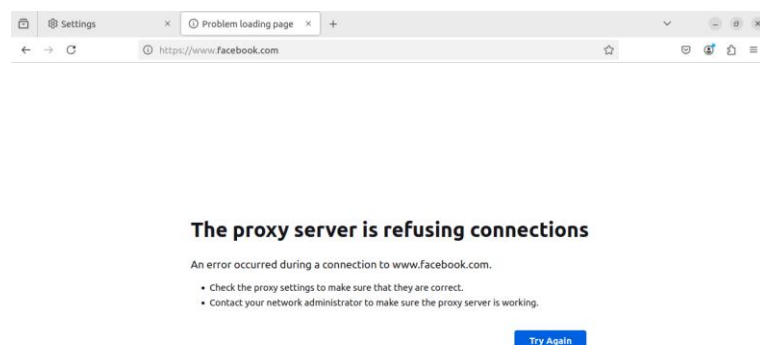


4. Thực hiện ngắt SSH Tunnel, xóa cache của trình duyệt và truy cập lại trang www.facebook.com. Lúc này, còn truy cập được trang web Facebook không?

- **Bước 1:** Ngắt SSH Tunnel và xóa cache của trình duyệt

```
vm-a-lan@lan:~$ sudo ss -tln
[sudo] password for vm-a-lan:
Netid State Recv-Q Send-Q Local Address:Port Peer Address:Port Process
udp UNCONN 0 0 0.0.0.0:48665 0.0.0.0:*
udp UNCONN 0 0 0.0.0.0:631 0.0.0.0:*
udp UNCONN 0 0 127.0.0.53%lo:53 0.0.0.0:*
udp UNCONN 0 0 0.0.0.0:5353 0.0.0.0:*
udp UNCONN 0 0 [::]:46976 [::]:*
udp UNCONN 0 0 [::]:5353 [::]:*
tcp LISTEN 0 4096 127.0.0.53%lo:53 0.0.0.0:*
tcp LISTEN 0 128 127.0.0.1:631 0.0.0.0:*
tcp LISTEN 0 128 127.0.0.1:8000 0.0.0.0:*
tcp LISTEN 0 128 [::]:8000 [::]:*
tcp LISTEN 0 128 [::]:631 [::]:*
vm-a-lan@lan:~$ sudo lsof -t -i:8000
20787
vm-a-lan@lan:~$ sudo kill -9 20787
```

- **Bước 2:** Kết quả khi truy cập lại 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 1:** Thiết lập rule trên pfSense: Chặn các kết nối trong mạng LAN, giao thức TCP, từ mạng 192.168.3.0/24 đến máy B, cổng 22 (SSH)

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 ☐ 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
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 Single host or alias 10.0.3.4
Destination Port Range SSH (22) From Custom To Custom
Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.

- **Bước 2:** Kết quả sau khi thiết lập rule: máy A không thể thực hiện SSH Tunnel đến máy B được nữa

```
vm-a-lan@lan:~$ ssh -D 9000 -C vm-b-wan@10.0.3.4
ssh: connect to host 10.0.3.4 port 22: Connection timed out
vm-a-lan@lan:~$
```

Giải thích: SSH Tunnel được thiết lập qua dịch vụ SSH (port 22), khi chặn dịch vụ này ở Firewall, tunnel không thể thiết lập thành công vì các gói tin đã bị chặn.

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.

- Bật tường lửa
- Thêm các Rules cấm hoặc giới hạn kết nối SSH từ các IP không xác định, dịch vụ telnet và các dịch vụ không bảo mật khác.
- Giám sát, theo dõi, phân tích lưu lượng ssh qua firewall.
- Sử dụng hệ thống phát hiện xâm nhập (IDS/IPS).
- Sử dụng SSL/TLS hoặc VPN để đảm bảo an toàn cho các kết nối.

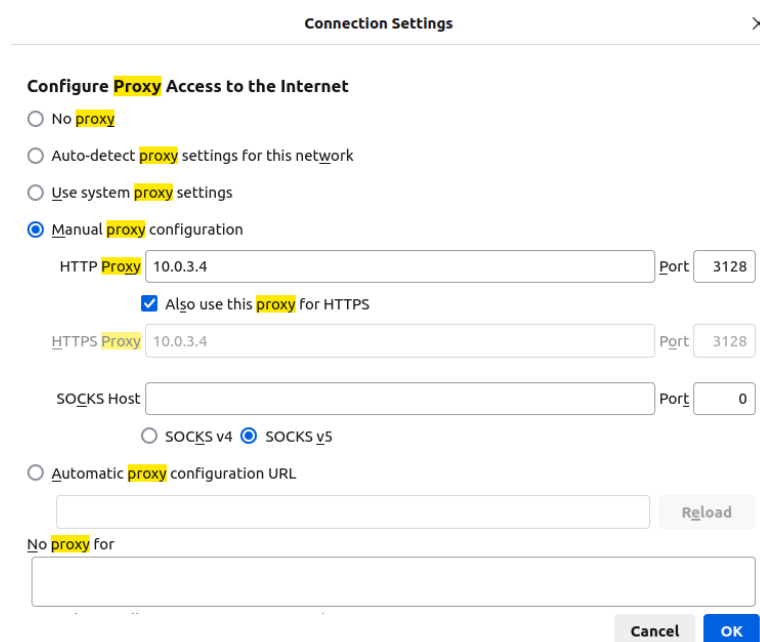
D. Triển khai Web Proxy (Application Firewall)

1. Cài đặt và cấu hình Squid

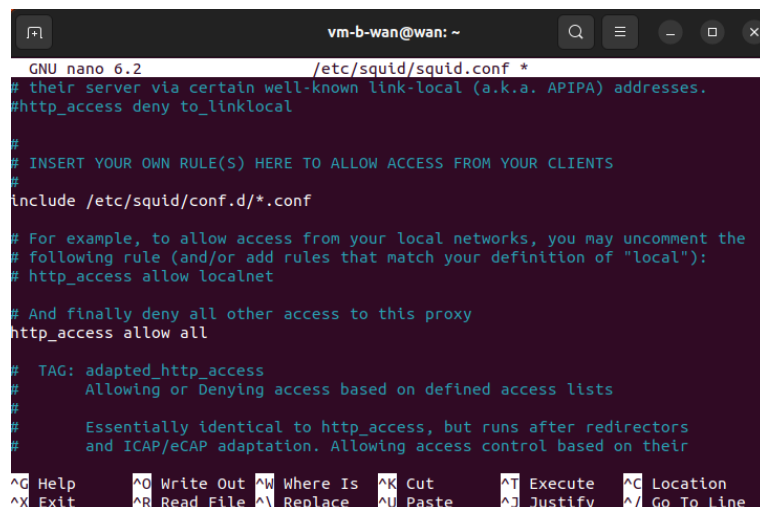
- **Bước 1:** Ở máy B, cài đặt squid và khởi động lại squid. Cấu hình firewall cho phép port 3128 hoạt động

```
vm-b-wan@wan:~$ sudo ufw allow 3128/tcp
Rule added
Rule added (v6)
vm-b-wan@wan:~$ sudo service squid restart
```

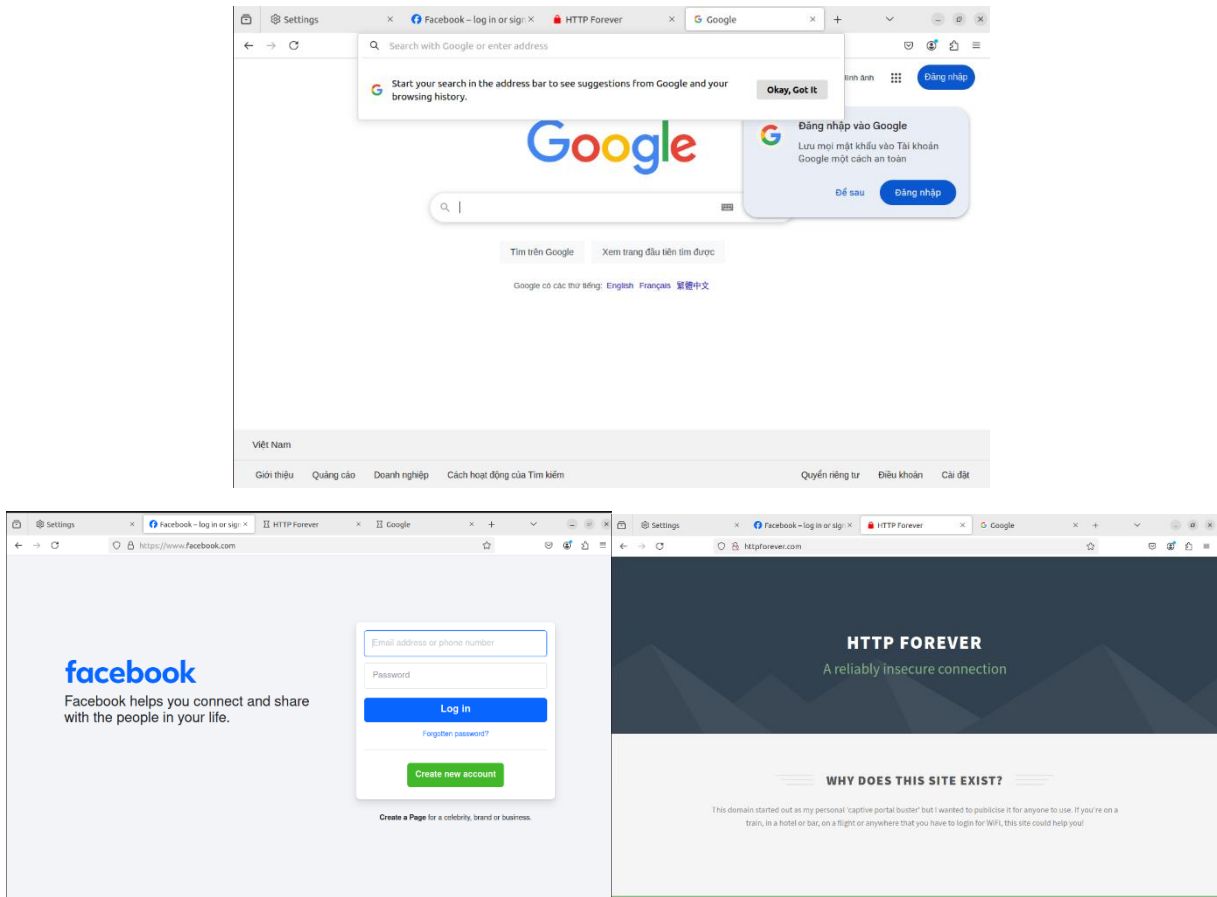
- **Bước 2:** Ở máy A, cấu hình trình duyệt để sử dụng kết nối proxy qua proxy server của VM B. Từ Firefox browser, truy cập vào phần thiết lập Network.



- **Bước 3:** Chỉnh sửa file /etc/squid/squid.conf để squid cho phép truy cập tất cả các trang web và khởi động lại squid.



- **Bước 4:** Lúc này máy A có thể truy cập vào các trang web <https://google.com>, <https://facebook.com>, trang web HTTP,... 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.



2. Thiết lập chuyển hướng (Rewrite / URL Redirection)

- **Bước 1:** Ở máy B, tạo file script sau (/etc/squid/script.pl) sử dụng ngôn ngữ Perl và cấp quyền (chmod) cho phép thực thi (chmod +x /etc/squid/script.pl)

```
vn-b-wan@wan:~$ sudo chmod 777 /etc/squid/script.pl
vn-b-wan@wan:~$ sudo cat /etc/squid/script.pl
#!/usr/bin/perl -w
use strict;
use warnings;

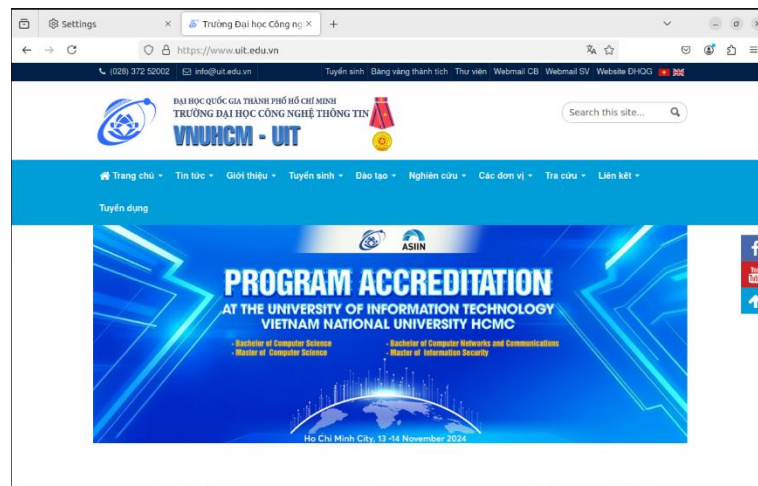
select STDOUT; $| = 1;

while (<=)
{
    my @parts = split;
    my $url = $parts[0];
    if ($url =~ /example\.com/)
    {
        print "http://www.uit.edu.vn\n";
    }
    else
    {
        print "\n";
    }
}
vn-b-wan@wan:~$
```

- **Bước 2:** Chỉnh sửa file cấu hình /etc/squid/squid.conf để sử dụng url_rewrite_program với chương trình trên

```
GNU nano 6.2 /etc/squid/squid.conf *
# The cli_conn_tag=TAG pair is treated as a regular transaction
# annotation for the current request and also annotates future
# requests on the same client connection. A helper may update
# the TAG during subsequent requests by returning a new kv-pair.
#
# Helper messages contain the channel-ID part if and only if the
# url_rewrite_children directive specifies positive concurrency. As a
# 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/script.pl
url_rewrite_children 5
# TAG: url_rewrite_children
# Specifies the maximum number of redirector processes that Squid may
^G Help ^O Write Out ^W Where Is ^K Cut ^T Execute ^C Location
^X Exit ^R Read File ^I Replace ^U Paste ^J Justify ^_/ Go To Line
```

- **Bước 3:** Khởi động lại squid ở máy B. Lúc này ở máy A khi truy cập <http://example.com> sẽ được chuyển hướng sang <https://www.uit.edu.vn>



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

- Mục tiêu: Chuyển hướng trang web người dùng nhập bằng cách thay thế url.
- Cách hoạt động:
 - Vòng lặp while giúp đọc từng dòng đầu vào, sau đó kiểm tra phần đầu tiên của dòng xem có chứa example.com hay không.
 - Nếu có, chương trình sẽ viết lại url thành “http://www.uit.edu.vn” và in ra.
 - Nếu không, in ra kí tự xuống dòng,

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).

- **Bước 1:** Khởi động nginx và thêm rule vào firewall

```
vm-b-wan@wan:~/Desktop$ sudo systemctl start nginx
vm-b-wan@wan:~/Desktop$ sudo ufw allow "Nginx Full"
Rule added
Rule added (v6)
```

- **Bước 2:** Di chuyển hình ảnh vào thư mục `/var/www/html` và cấp quyền

```
vm-b-wan@wan:~/Downloads$ sudo mv ./sign.jpeg /var/www/html
[sudo] password for vm-b-wan:
vm-b-wan@wan:~/Downloads$ sudo chown www-data /var/www/html/sign.jpeg
```

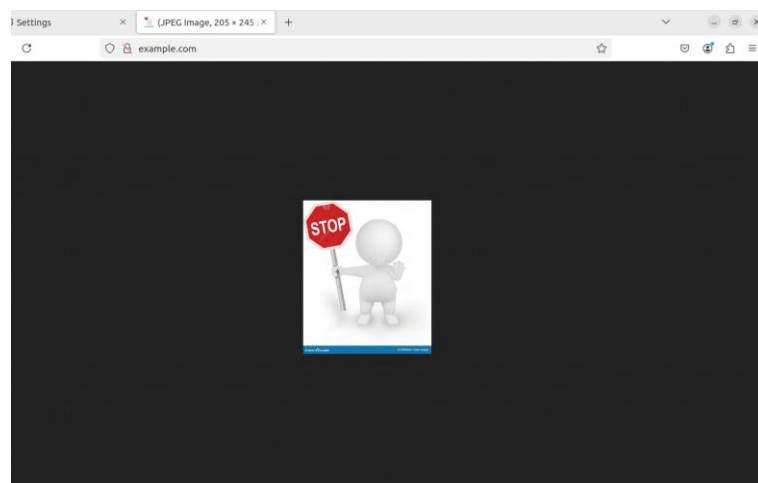
- **Bước 3:** Chỉnh sửa file `/etc/squid/script.pl` và khởi động lại squid

```
vm-b-wan@wan:~/Downloads$ sudo cat /etc/squid/script.pl
#!/usr/bin/perl -w
use strict;
use warnings;

select STDOUT; $| = 1;

while (<>)
{
    my @parts = split;
    my $url = $parts[0];
    if ($url =~ /example\.com/)
    {
        print "http://10.0.3.4/sign.jpeg\n";
    }
    else
    {
        print "\n";
    }
}
vm-b-wan@wan:~/Downloads$ sudo service squid restart
vm-b-wan@wan:~/Downloads$
```

- **Bước 4:** Máy A truy cập <http://example.com> sẽ hiển thị hình ảnh cảnh báo



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).

- **Bước 1:** Trang web <http://www.celuit.edu.vn/> ban đầu



- **Bước 2:** Chỉnh sửa file `/etc/squid/script.pl` và khởi động lại squid

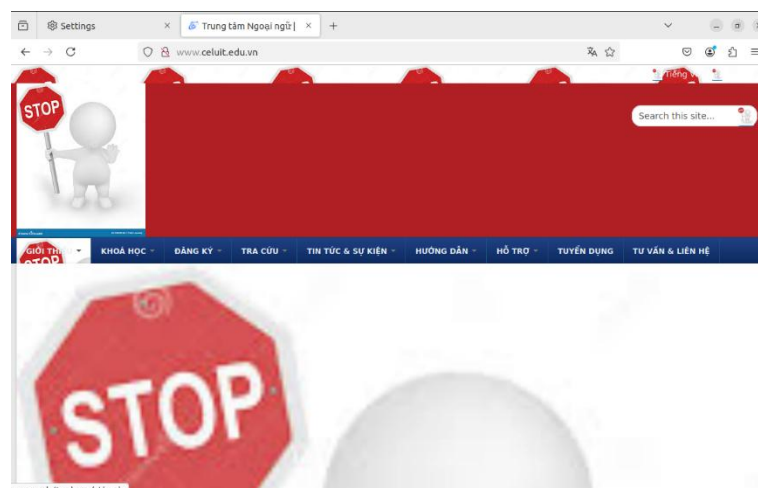
```
vn-b-wan@wan:~/Downloads$ sudo cat /etc/squid/script.pl
#!/usr/bin/perl -w
use strict;
use warnings;

select STDOUT; $| = 1;

while (<=)
{
    my @parts = split;
    my $url = $parts[0];
    if ($url =~ /celuit.edu.vn\/.*\.(png|jpg|jpeg|gif|bmp|svg)(.*)/)
    {
        print "http://10.0.3.4/sign.jpeg\n";
    }
    else
    {
        print "\n";
    }
}

vn-b-wan@wan:~/Downloads$ sudo service squid restart
vn-b-wan@wan:~/Downloads$
```

- **Bước 3:** Truy cập lại <http://www.celuit.edu.vn/>, các hình ảnh của trang đã bị đổi thành hình cảnh báo



E. 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?

- Các giao thức:
 - IPSec
 - OpenVPN
 - IKEv2
 - L2TP / IPSec
- Bảng so sánh đặc điểm các giao thức

Tiêu chí	IPSec	OpenVPN	IKEv2	L2TP
Tầng hoạt động	Network	Transport	Network	Datalink
Bảo mật	Mã hóa mạnh (AES, 3DES), xác thực bằng IKEv1/2	Mã hóa SSL/TLS (AES, RSA), linh hoạt	Mã hóa mạnh (AES, ChaCha20), tương thích IPSec	Bảo mật phụ thuộc vào IPSec (L2TP chỉ là giao thức tunneling)
Hiệu suất	Trung bình đến cao	Trung bình (phụ thuộc vào cấu hình)	Cao	Thấp đến trung bình (thêm overhead của L2TP)
Độ tin cậy	Cao	Cao, dễ xuyên qua NAT	Cao, tự phục hồi kết nối khi mạng gián đoạn	Trung bình
Hỗ trợ NAT Traversal	Có (UDP port 500, 4500)	Tốt (dùng TCP/UDP, bất kỳ port nào)	Có (tương tự IPSec)	Có (dựa trên IPSec)
Cấu hình	Khó hơn so với OpenVPN, WireGuard	Dễ, linh hoạt	Trung bình (dễ hơn IPSec thông thường)	Dễ (nếu hệ điều hành hỗ trợ sẵn)

Tương thích thiết bị	Rộng rãi trên hầu hết thiết bị hiện đại	Cần cài đặt client riêng trên nhiều thiết bị	Tốt (hỗ trợ mạnh trên thiết bị di động)	Rộng rãi trên thiết bị cũ và hiện đại
Độ phổ biến	Rất phổ biến trong doanh nghiệp	Phổ biến trong môi trường đa dạng	Phổ biến, đặc biệt trên thiết bị di động	Ít phổ biến hơn do thay thế bởi giao thức hiện đại

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.

- Địa chỉ IP máy A

```
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:fa:3d:dd brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 192.168.3.128/24 brd 192.168.3.255 scope global dynamic noprefixroute ens33
        valid_lft 1793sec preferred_lft 1793sec
    inet6 fe80::69e1:1caf:18ee:3687/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
```

- Địa chỉ IP máy B

```
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:af:f2:8c brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 10.0.3.4/24 brd 10.0.3.255 scope global dynamic noprefixroute ens33
        valid_lft 1707sec preferred_lft 1707sec
    inet6 fe80::5460:6c38:67a:4cde/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
```

- Địa chỉ IP pfSense

```
*** Welcome to pfSense 2.4.5-RELEASE-p1 (amd64) on pfSense ***  
  
WAN (wan)      -> em0      -> v4: 10.0.3.2/24  
LAN (lan)      -> em1      -> v4: 192.168.3.2/24
```

- Kết quả ping từ máy B đến máy A, PFSense, Internet

```
userb@userb:~$ ping 192.168.3.128  
PING 192.168.3.128 (192.168.3.128) 56(84) bytes of data.  
64 bytes from 192.168.3.128: icmp_seq=1 ttl=128 time=1.53 ms  
64 bytes from 192.168.3.128: icmp_seq=2 ttl=128 time=0.954 ms  
64 bytes from 192.168.3.128: icmp_seq=3 ttl=128 time=1.35 ms  
^C  
--- 192.168.3.128 ping statistics ---  
3 packets transmitted, 3 received, 0% packet loss, time 2004ms  
rtt min/avg/max/mdev = 0.954/1.279/1.534/0.242 ms  
userb@userb:~$ ping 10.0.3.2  
PING 10.0.3.2 (10.0.3.2) 56(84) bytes of data.  
64 bytes from 10.0.3.2: icmp_seq=1 ttl=128 time=0.300 ms  
64 bytes from 10.0.3.2: icmp_seq=2 ttl=128 time=1.26 ms  
64 bytes from 10.0.3.2: icmp_seq=3 ttl=128 time=0.228 ms  
^C  
--- 10.0.3.2 ping statistics ---  
3 packets transmitted, 3 received, 0% packet loss, time 2030ms  
rtt min/avg/max/mdev = 0.228/0.597/1.264/0.472 ms  
userb@userb:~$ ping 8.8.8.8  
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.  
64 bytes from 8.8.8.8: icmp_seq=1 ttl=128 time=57.9 ms  
64 bytes from 8.8.8.8: icmp_seq=2 ttl=128 time=56.4 ms  
^C  
--- 8.8.8.8 ping statistics ---  
3 packets transmitted, 2 received, 33.333% packet loss, time 2004ms  
rtt min/avg/max/mdev = 56.431/57.189/57.948/0.758 ms
```

- Kết quả ping từ máy A đến PFSense, máy B, Internet

```
nhattram@nhattram:~$ ping 10.0.3.2  
PING 10.0.3.2 (10.0.3.2) 56(84) bytes of data.  
64 bytes from 10.0.3.2: icmp_seq=1 ttl=64 time=1.36 ms  
64 bytes from 10.0.3.2: icmp_seq=2 ttl=64 time=2.20 ms  
64 bytes from 10.0.3.2: icmp_seq=3 ttl=64 time=1.32 ms  
^C  
--- 10.0.3.2 ping statistics ---  
3 packets transmitted, 3 received, 0% packet loss, time 2005ms  
rtt min/avg/max/mdev = 1.317/1.623/2.197/0.406 ms  
nhattram@nhattram:~$ ping 10.0.3.4  
PING 10.0.3.4 (10.0.3.4) 56(84) bytes of data.  
64 bytes from 10.0.3.4: icmp_seq=1 ttl=63 time=4.22 ms  
64 bytes from 10.0.3.4: icmp_seq=2 ttl=63 time=6.65 ms  
^C  
--- 10.0.3.4 ping statistics ---  
2 packets transmitted, 2 received, 0% packet loss, time 1003ms  
rtt min/avg/max/mdev = 4.222/5.434/6.646/1.212 ms  
nhattram@nhattram:~$ ping 8.8.8.8  
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.  
64 bytes from 8.8.8.8: icmp_seq=1 ttl=127 time=205 ms  
64 bytes from 8.8.8.8: icmp_seq=2 ttl=127 time=121 ms  
^C  
--- 8.8.8.8 ping statistics ---  
2 packets transmitted, 2 received, 0% packet loss, time 1003ms  
rtt min/avg/max/mdev = 121.406/163.274/205.142/41.868 ms
```


- Tạo hạ tầng khóa công khai cho PFSense và OpenVPN
 - Tạo Certificate Authority (CA) trên PFSense

System / Certificate Manager / CAs / Edit

CA'sCertificatesCertificate Revocation

Create / Edit CA

Descriptive name

nhattram_claire

Method

Create an internal Certificate Authority

Internal Certificate Authority

Key length (bits)

2048

Digest Algorithm

sha256

NOTE: It is recommended to use an algorithm stronger than SHA1 when possible.

Lifetime (days)

3650

Common Name

internal-ca

The following certificate authority subject components are optional and may be left blank.

Country Code

VN

State or Province

e.g. Texas

City

Ho Chi Minh

Organization

UIT

Organizational Unit

NT140 Lab 5

System / Certificate Manager / CAs

CA'sCertificatesCertificate Revocation

Search

Search term





Both

Search

Clear

Enter a search string or *nix regular expression to search certificate names and distinguished names.

Certificate Authorities

Name	Internal	Issuer	Certificates	Distinguished Name	In Use	Actions
nhattram_claire	✓	self-signed	0	OU=NT140 Lab 5, O=UIT, L=Ho Chi Minh, CN=internal-ca, C=VN Valid From: Tue, 17 Dec 2024 08:21:25 +0000 Valid Until: Fri, 15 Dec 2034 08:21:25 +0000		   

- Tạo server certificate cho OpenVPN trên PFSense

CAs

Certificates

Certificate Revocation

Add/Sign a New Certificate

Method

Create an internal Certificate

Descriptive name

vpn_server

Internal Certificate

Certificate authority

nhattram_claire

Key length

2048

Digest Algorithm

sha256

NOTE: It is recommended to use an algorithm stronger than SHA1 when possible.

Lifetime (days)

3650

Common Name

www.nt140lab5.vn

The following certificate subject components are optional and may be left blank.

Country Code

VN

State or Province

e.g. Texas

City

Ho Chi Minh

Organization

UIT

Organizational Unit

NT140 Lab 5

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.

Certificate Type

Server Certificate

Add type-specific usage attributes to the signed certificate. Used for placing usage restrictions on, or granting abilities to, the signed certificate.

Alternative Names

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

System / Certificate Manager / Certificates

CAs

Certificates

Certificate Revocation

Search

Search term

Both

Search

Clear

Enter a search string or *nix regular expression to search certificate names and distinguished names.

Certificates

Name	Issuer	Distinguished Name	In Use	Actions
webConfigurator default (67612a435f3b4) Server Certificate CA: No Server: Yes	self-signed	O=pfSense webConfigurator Self-Signed Certificate, CN=pfSense-67612a435f3b4 Valid From: Tue, 17 Dec 2024 07:37:39 +0000 Valid Until: Mon, 19 Jan 2026 07:37:39 +0000		
vpn_server Server Certificate CA: No Server: Yes	nhattram_claire	OU=NT140 Lab 5, O=UIT, L=Ho Chi Minh, CN=www.nt140lab5.vn, C=VN Valid From: Tue, 17 Dec 2024 08:26:23 +0000 Valid Until: Fri, 15 Dec 2034 08:26:23 +0000		

- Cấu hình OpenVPN trên PFSense
- Cấu hình General OpenVPN Server Information

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

NT140 Lab 5

- Cấu hình Cryptographic Settings

Cryptographic Settings

TLS Authentication

☒

Enable authentication of TLS packets.

Generate TLS Key

☒

Automatically generate a shared TLS authentication key.

TLS Shared Key

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

DH Parameters Length

2048 bit

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

Encryption Algorithm

AES-128-CBC (128 bit key, 128 bit block)

The algorithm used to encrypt traffic between endpoints. This setting must match on the client and server side, but is otherwise set however desired. Certain algorithms will perform better on different hardware, depending on the availability of supported VPN accelerator chips.

Auth Digest Algorithm

SHA256 (256-bit)

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

Hardware Crypto

No Hardware Crypto Acceleration

• Cấu hình Tunnel

Tunnel Settings

IPv4 Tunnel Network

10.101.1.0/24

This is the IPv4 virtual network or network type alias with a single entry used for private communications between this server and client hosts expressed using CIDR notation (e.g. 10.0.8.0/24). The first usable address in the network will be assigned to the server virtual interface. The remaining usable addresses will be assigned to connecting clients.

IPv6 Tunnel Network

This is the IPv6 virtual network or network type alias with a single entry used for private communications between this server and client hosts expressed using CIDR notation (e.g. fe80::/64). The first usable address in the network will be assigned to the server virtual interface. The remaining addresses will be assigned to connecting clients.

Redirect IPv4 Gateway

☒ Force all client-generated IPv4 traffic through the tunnel.

Redirect IPv6 Gateway

☐ Force all client-generated IPv6 traffic through the tunnel.

IPv6 Local network(s)

IPv6 networks that will be accessible from the remote endpoint. Expressed as a comma-separated list of one or more IP/PREFIX or host/network type aliases. 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.

Concurrent connections

10

Specify the maximum number of clients allowed to concurrently connect to this server.

Allow Compression

Decompress incoming, do not compress outgoing (Asymmetric)

Allow compression to be used with this VPN instance.
Compression can potentially increase throughput but may allow an attacker to extract secrets if they can control compressed plaintext traversing the VPN (e.g. HTTP). Before enabling compression, consult information about the VORACLE, CRIME, TIME, and BREACH attacks against TLS to decide if the use case for this specific VPN is vulnerable to attack.

Asymmetric compression allows an easier transition when connecting with older peers.

Compression

Disable Compression [Omit Preference]

Deprecated. Compress tunnel packets using the LZO algorithm.
Compression can potentially dangerous and insecure. See the note on the Allow Compression option above.

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.

Push Compression

☐ Push the selected Compression setting to connecting clients.

Type-of-Service

☐ Set the TOS IP header value of tunnel packets to match the encapsulated packet value.

Inter-client communication

☐ Allow communication between clients connected to this server

Duplicate Connection

☐ Allow multiple concurrent connections from the same user
When set, the same user may connect multiple times. When unset, a new connection from a user will disconnect the previous session.

Users are identified by their username or certificate properties, depending on the VPN configuration. This practice is discouraged security reasons, but may be necessary in some environments.

- Cấu hình Client Settings

Client Settings	
Dynamic IP	<input checked="" type="checkbox"/> Allow connected clients to retain their connections if their IP address changes.
Topology	<div>Subnet – One IP address per client in a common subnet</div> <div>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".</div>
DNS Default Domain	<div></div> <div>Provide a default domain name to clients.</div>
DNS Server 1	<div></div> <div>DNS server IP to provide to connecting clients.</div>
DNS Server 2	<div></div> <div>DNS server IP to provide to connecting clients.</div>
DNS Server 3	<div></div> <div>DNS server IP to provide to connecting clients.</div>
DNS Server 4	<div></div> <div>DNS server IP to provide to connecting clients.</div>
NTP Server	<div></div> <div>Network Time Protocol server to provide to connecting clients.</div>
NTP Server 2	<div></div> <div>Network Time Protocol server to provide to connecting clients.</div>
NetBIOS Options	<div><input type="checkbox"/></div> <div>Enable NetBIOS over TCP/IP. If this option is not set, all NetBIOS-over-TCP/IP options (including WINS) will be disabled.</div>
NetBIOS Node Type	<div>none</div> <div>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).</div>
NetBIOS Scope ID	<div></div> <div>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.</div>
WINS Server 1	<div></div> <div>A Windows Internet Name Service (WINS) server IP to provide to connecting clients. Not desirable in most all modern networks.</div>
WINS Server 2	<div></div> <div>A Windows Internet Name Service (WINS) server IP to provide to connecting clients. Not desirable in most all modern networks.</div>

- Tạo rule firewall

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.

- Hoàn tất cấu hình openVPN

VPN / OpenVPN / Servers 📊 📄 ?

Servers Clients Client Specific Overrides Wizards Client Export Shared Key Export

OpenVPN Servers

Interface	Protocol / Port	Tunnel Network	Mode / Crypto	Description	Actions
WAN	UDP4 / 1194 (TUN)	10.101.1.0/24	Mode: Remote Access (SSL/TLS + User Auth) Data Ciphers: AES-128-GCM, AES-256-CBC Digest: SHA256 D-H Params: 2048 bits	NT140 Lab 5	  

- Cấu hình quyền truy cập của client
 - Tạo OpenVPN Client trên PFSense

General Information	
Disabled	<input type="checkbox"/> Disable this client Set this option to disable this client without removing it from the list.
Server mode	Peer to Peer (SSL/TLS)
Protocol	UDP on IPv4 only
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.)
Interface	WAN The interface used by the firewall to originate this OpenVPN client connection
Local port	<input type="text"/> Set this option to bind to a specific port. Leave this blank or enter 0 for a random dynamic port.
Server host or address	10.0.3.2 The IP address or hostname of the OpenVPN server.
Server port	1194 The port used by the server to receive client connections.
Proxy host or address	<input type="text"/> The address for an HTTP Proxy this client can use to connect to a remote server. TCP must be used for the client and server protocol.
Proxy port	<input type="text"/>
Proxy Authentication	none The type of authentication used by the proxy server.
Description	vpn client A description may be entered here for administrative reference (not parsed).
User Authentication Settings	
Username	nhattram Leave empty when no user name is needed
Password	***** Leave empty when no password is needed
Authentication Retry	<input type="checkbox"/> 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. 

Cryptographic Settings

TLS Configuration ☒ 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.

☒ Automatically generate a TLS Key.

TLS keydir direction

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.

Peer Certificate Authority

nhattram_claire

Peer Certificate
Revocation list

No Certificate Revocation Lists defined. One may be created here: [System > Cert. Manager > Certificate Revocation](#)

Client Certificate

None (Username and/or Password required)

Encryption Algorithm

AES-128-CBC (128 bit key, 128 bit block)

The Encryption Algorithm used for data channel packets when Negotiable Cryptographic Parameter (NCP) support is not available.

Enable NCP

☒ Enable Negotiable Cryptographic Parameters

Check this option to allow OpenVPN clients and servers to negotiate a compatible set of acceptable cryptographic Encryption Algorithms from those selected in the NCP Algorithms list below. [i](#)

NCP Algorithms

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)

Available NCP Encryption Algorithms

Click to add or remove an algorithm from the list

The order of the selected NCP Encryption Algorithms is respected by OpenVPN. [i](#)

AES-128-GCM

Allowed NCP Encryption Algorithms. Click an algorithm name to remove it from the list

Auth digest algorithm

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.

Hardware Crypto

No Hardware Crypto Acceleration

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

Disabled

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.

Send/Receive Buffer

Default

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

default

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
Default through 4: Normal usage range
5: Output R and W characters to the console for each packet read and write. Uppercase is used for TCP/UDP packets and lowercase is used for TUN/TAP packets.
6-11: Debug info range

VPN / OpenVPN / Clients




Servers

Clients

Client Specific Overrides

Wizards

OpenVPN Clients

Interface	Protocol	Server	Description	Actions
WAN	UDP4	10.0.3.2:1194	vpn client	  

- Cài đặt gói OpenVPN Client Export

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

- Thêm người dùng VPN

System / User Manager / Users / Edit

Users **Groups** **Settings** **Authentication Servers**

User Properties

Defined by USER

Disabled ☐ This user cannot login

Username nhattram

Password

Full name Phan Nguyen Nhat Tram
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 ☐ Use individual customized GUI options and dashboard layout for this user.

Group membership

admins

Not member of

Member of

>> Move to "Member of" list

<< Move to "Not member of" list

Hold down CTRL (PC)/COMMAND (Mac) key to select multiple items.

Certificate ☒ Click to create a user certificate

Create Certificate for User

Descriptive name

vpn_user

Certificate authority

nhattram_claire

Key type

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.

Digest Algorithm

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

Lifetime

3650

Keys

Authorized SSH Keys

Enter authorized SSH keys for this user

IPsec Pre-Shared Key

System / User Manager / Users

Users

Groups

Settings

Authentication Servers

Users

	Username	Full name	Status	Groups	Actions
<input type="checkbox"/>	admin	System Administrator	✓	admins	
<input type="checkbox"/>	nhattram	Phan Nguyen Nhat Tram	✓		

- Export openVPN client cho user

OpenVPN Clients

User	Certificate Name	Export
nhattram	vpn_user	<div>- Inline Configurations: Most Clients Android OpenVPN Connect (iOS/Android)</div> <div>- Bundled Configurations: Archive Config File Only</div> <div>- Current Windows Installers (2.5.8-lx04): 64-bit 32-bit</div> <div>- Legacy Windows Installers (2.4.12-lx01): 10/2016/2019 7/8/8.1/2012r2</div> <div>- Viscosity (Mac OS X and Windows): Viscosity Bundle Viscosity Inline Config</div>

- Chuyển file openvpn được export ra tới máy B, chạy file config

```
userb@userb: ~  
able_win32_dll=yes enable_wolfssl_options_h=yes enable_x509_alt_username=yes wi  
th_aix_soname=aix with_crypto_library=openssl with_gnu_ld=yes with_mem_check=no  
with_openssl_engine=auto with_sysroot=no  
userb@userb:~$ sudo openvpn --config pfSense-UDP4-1194-nhattram-config.ovpn  
2024-12-17 21:43:43 OpenVPN 2.6.12 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [L  
Z4] [EPOLL] [PKCS11] [MH/PTINFO] [AEAD] [DCO]  
2024-12-17 21:43:43 library versions: OpenSSL 1.1.1f 31 Mar 2020, LZO 2.10  
2024-12-17 21:43:43 DCO version: N/A  
Enter Auth Username: nhattram  
Enter Auth Password: *****  
2024-12-17 21:44:00 TCP/UDP: Preserving recently used remote address: [AF_INET]  
10.0.3.2:1194  
2024-12-17 21:44:00 UDPv4 link local: (not bound)  
2024-12-17 21:44:00 UDPv4 link remote: [AF_INET]10.0.3.2:1194  
2024-12-17 21:44:00 WARNING: this configuration may cache passwords in memory -  
- use the auth-nocache option to prevent this  
2024-12-17 21:44:00 [www.nt140lab5.vn] Peer Connection Initiated with [AF_INET]  
10.0.3.2:1194  
2024-12-17 21:44:00 TUN/TAP device tun0 opened  
2024-12-17 21:44:00 net_iface_mtu_set: mtu 1500 for tun0  
2024-12-17 21:44:00 net_iface_up: set tun0 up  
2024-12-17 21:44:00 net_addr_v4_add: 10.101.1.2/24 dev tun0  
2024-12-17 21:44:00 Initialization Sequence Completed
```

- Ping từ máy B đến máy A

```
userb@userb: ~  
userb@userb:~$ ip a  
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default  
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00  
    inet 127.0.0.1/8 scope host lo  
        valid_lft forever preferred_lft forever  
    inet6 ::1/128 scope host  
        valid_lft forever preferred_lft forever  
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP gro  
    up default qlen 1000  
    link/ether 00:0c:29:af:f2:8c brd ff:ff:ff:ff:ff:ff  
    altname enp2s1  
    inet 10.0.3.4/24 brd 10.0.3.255 scope global dynamic noprefixroute ens33  
        valid_lft 1457sec preferred_lft 1457sec  
    inet6 fe80::8b87:bf67:bfdd:2aff/64 scope link noprefixroute  
        valid_lft forever preferred_lft forever  
3: tun0: <POINTOPOINT,MULTICAST,NOARP,UP,LOWER_UP> mtu 1500 qdisc fq_codel state  
    UNKNOWN group default qlen 500  
    link/none  
    inet 10.101.1.2/24 scope global tun0  
        valid_lft forever preferred_lft forever  
    inet6 fe80::5182:df1d:934f:47f1/64 scope link stable-privacy  
        valid_lft forever preferred_lft forever  
userb@userb:~$ ping 192.168.3.128  
PING 192.168.3.128 (192.168.3.128) 56(84) bytes of data.  
64 bytes from 192.168.3.128: icmp_seq=1 ttl=63 time=2.00 ms  
64 bytes from 192.168.3.128: icmp_seq=2 ttl=63 time=2.15 ms  
64 bytes from 192.168.3.128: icmp_seq=3 ttl=63 time=2.70 ms  
^C  
--- 192.168.3.128 ping statistics ---  
3 packets transmitted, 3 received, 0% packet loss, time 2003ms  
rtt min/avg/max/mdev = 2.001/2.282/2.701/0.301 ms  
userb@userb:~$
```

- Link tham khảo:
 - <https://vietnix.vn/cau-hinh-openvpn-tren-pfsense/#h-c-i-t-g-i-openvpn-client-export>
 - <https://docs.netgate.com/pfsense/en/latest/recipes/openvpn-ra.html>