

# BÁO CÁO THỰC HÀNH

Môn học: An Toàn Mạng

Tên chủ đề: Khai thác tường lửa trong Linux

GVHD: Tô Trọng Nghĩa

Nhóm: 3

## 1. THÔNG TIN CHUNG:

(Liệt kê tất cả các thành viên trong nhóm)

Lớp: NT140.P11.ANTT.1

STT	Họ và tên	MSSV	Email
1	Hà Minh Quân	22521177	22521177@gm.uit.edu.vn
2	Tù Chí Kiên	22520713	22520713@gm.uit.edu.vn

## 2. NỘI DUNG THỰC HIỆN:<sup>1</sup>

STT	Nội dung	Tình trạng	Trang
1	Vượt qua sự kiểm soát của Firewall	%	Xem mục lục
2	Triển khai Web Proxy (Application Firewall)	100%	Xem mục lục
3	VPN	100%	Xem mục lục
Điểm tự đánh giá			10/10

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

A.	THỰC HÀNH.....	2
1.	Cài đặt pfSense firewall.....	2
2.	Triển khai Web Proxy (Application Firewall).....	4
a)	Cài đặt và cấu hình Squid.....	4
b)	Thiết lập chuyển hướng (Rewrite / URL Redirection).....	7
7.	Đoạn chương trình script.pl trên hoạt động như thế nào? .....	9
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)....	9
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).....	11
3.	VPN.....	13
10.	Firewall pfSense hỗ trợ các giao thức thiết lập kết nối VPN nào? Những giao thức này có đặc điểm gì khác nhau? .....	13
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.....	14

## A. THỰC HÀNH

### 1. Cài đặt pfSense firewall

Trước khi làm bài nhóm em đã thử sử dụng gateway là 10.0.3.1 nhưng không kết nối được internet, vậy sau khi tìm hiểu là NAT của máy nhóm em sử dụng 10.0.3.2 để truy cập internet nên sử dụng 10.0.3.2 là gateway và 10.0.3.3 là ip WAN của pfsense và máy B là 10.0.3.4

Và phải vào cấu hình interface wan của pfsense:

Và tắt phần **Block private networks and loopback addresses**

The screenshot shows the 'Reserved Networks' section of the pfSense configuration. It includes two options: 'Block private networks and loopback addresses' (unchecked) and 'Block bogon networks' (checked). The checked option is described as blocking traffic from reserved IP addresses (RFC 1918 and RFC 4193) and loopback addresses (127/8), noting it should be turned on unless the interface resides in such a private address space. A note at the bottom states that update frequency can be changed under System > Advanced, Firewall & NAT settings.

Cấu hình trên pfSense:

Cho WAN là NAT (máy B) với địa chỉ ip là 10.0.3.3

Cho LAN là Host only (máy A) với địa chỉ là 192.168.3.2

```
http://192.168.3.2/
Press <ENTER> to continue.
VMware Virtual Machine - Netgate Device ID: c444d4127185d1dc3471

*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***
WAN (wan)      -> em0      -> v4: 10.0.3.3/24
LAN (lan)      -> em1      -> v4: 192.168.3.2/24

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

Enter an option: ■
```

Trên máy A thì cấu hình địa chỉ tĩnh và gateway:

```
tckien@tckien-VMware-Virtual-Platform:~/Desktop$ ip route
default via 192.168.3.2 dev ens33 proto static metric 100
192.168.3.0/24 dev ens33 proto kernel scope link src 192.168.3.3 metric 100
```

Máy B thì cấu hình:

```
tckien@tckien-VMware-Virtual-Platform:~/Desktop$ ip route
default via 10.0.3.3 dev ens33 proto static metric 20100
10.0.3.0/24 dev ens33 proto kernel scope link src 10.0.3.4 metric 100
```

Trước khi thực hiện sử dụng ping để kiểm tra kết nối:

Từ A đến B thì ping thành công:

```
tckien@tckien-VMware-Virtual-Platform:~/Desktop$ 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=7.12 ms
64 bytes from 10.0.3.4: icmp_seq=2 ttl=63 time=3.51 ms
64 bytes from 10.0.3.4: icmp_seq=3 ttl=63 time=2.97 ms
^C
--- 10.0.3.4 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 2.973/4.532/7.115/1.839 ms
tckien@tckien-VMware-Virtual-Platform:~/Desktop$
```

Máy B đến A:

Trước đó phải thêm rules để có thể kết nối từ WAN đến mạng LAN:

Rules (Drag to Change Order)											
	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓ 0/0 B	IPv4 *	*	*	WAN subnets	*	*	none			
<input type="checkbox"/>	✓ 0/0 B	IPv4 *	WAN subnets	*	*	*	*	none			

Thì ping được

```
tckien@tckien-VMware-Virtual-Platform:~/Desktop$ 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=63 time=5.33 ms
64 bytes from 192.168.3.3: icmp_seq=2 ttl=63 time=3.00 ms
^C
--- 192.168.3.3 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1002ms
rtt min/avg/max/mdev = 3.001/4.163/5.326/1.162 ms
```

## 2. Triển khai Web Proxy (Application Firewall)

### a) Cài đặt và cấu hình Squid

Sửa lại tệp http để cho phép http

## Lab 01: DEF

### Nhóm GHI

```
tckien@tckien-VMware-Virtual-Platform:~/.Desktop$ nano /etc/squid/squid.conf
GNU nano 7.2          /etc/squid/squid.conf *

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

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

# 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
#
#
# Essentially identical to http_access, but runs after redirectors
# and ICAP/eCAP adaptation. Allowing access control based on their
# output.
#
#      If not set then only http_access is used.

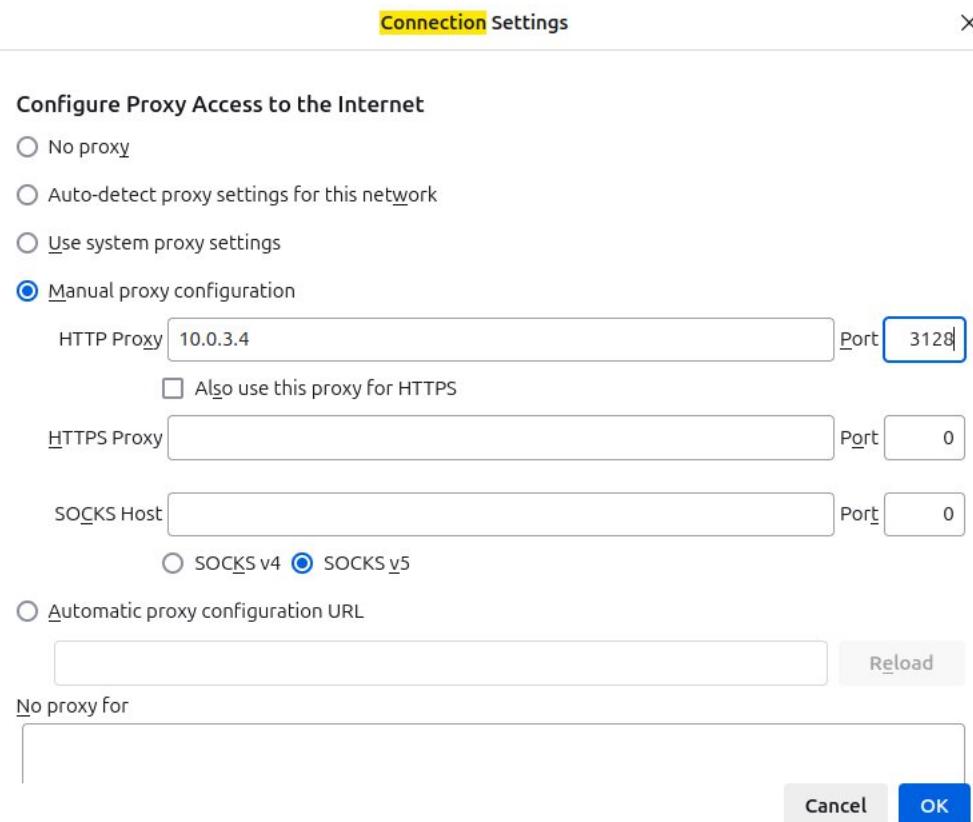
^G Help      ^O Write Out  ^W Where Is  ^K Cut      ^T Execute  ^C Location
^X Exit      ^R Read File  ^Y Replace   ^U Paste    ^J Justify  ^/ Go To Line
```

Kiểm tra xem squid có đang hoạt động không

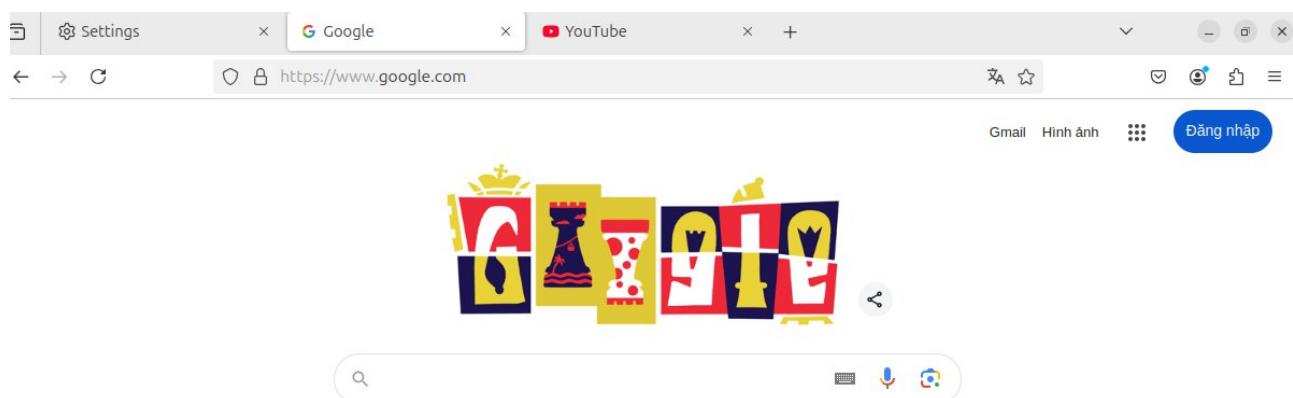
```
tckien@tckien-VMware-Virtual-Platform:~/Desktop$ systemctl status squid
● squid.service - Squid Web Proxy Server
  Loaded: loaded (/usr/lib/systemd/system/squid.service; enabled; preset: enabled)
  Active: active (running) since Mon 2024-11-25 20:32:57 +07; 37s ago
    Docs: man:squid(8)
   Process: 4776 ExecStartPre=/usr/sbin/squid --foreground -z (code=exited, st>
 Main PID: 4781 (squid)
    Tasks: 4 (limit: 2220)
   Memory: 17.6M (peak: 18.0M)
     CPU: 1.063s
    CGroup: /system.slice/squid.service
            └─4781 /usr/sbin/squid --foreground -sYC
              ├─4785 "(squid-1)" --kid squid-1 --foreground -sYC
              ├─4786 "(logfile-daemon)" /var/log/squid/access.log
              ├─4787 "(pinger)"

Nov 25 20:32:57 tckien-VMware-Virtual-Platform squid[4785]: Using Least Load strategy
Nov 25 20:32:57 tckien-VMware-Virtual-Platform squid[4785]: Set Current Directory to /
Nov 25 20:32:57 tckien-VMware-Virtual-Platform squid[4785]: Finished loading MI
Nov 25 20:32:57 tckien-VMware-Virtual-Platform squid[4785]: HTTP Disabled
```

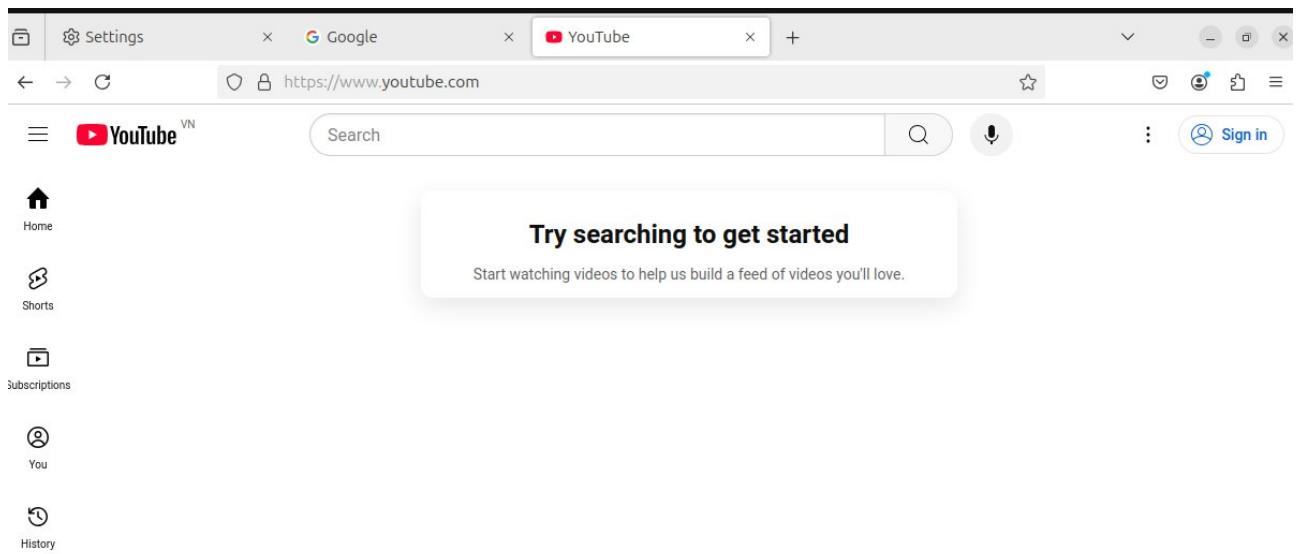
Cấu hình proxy bằng địa chỉ máy B và cổng 3128 trên máy A:



Kiểm tra thì thấy vẫn có thể truy cập google.com và youtube.com:



.../.../...



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

Đầu tiên tạo một script điều hướng

```
GNU nano 7.2                               /etc/squid/script.pl
#!/usr/bin/perl -w
use strict;
use warnings;

#Force 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";
    }
}
```

Sau đó trong tệp conf thêm hai đoạn sau để chạy chương trình



```
GNU nano 7.2                               /etc/squid/squid.conf *
# unlinkd_program /usr/lib/squid/unlinkd

# TAG: pinger_program
#       Specify the location of the executable for the pinger process.
#Default:
# 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

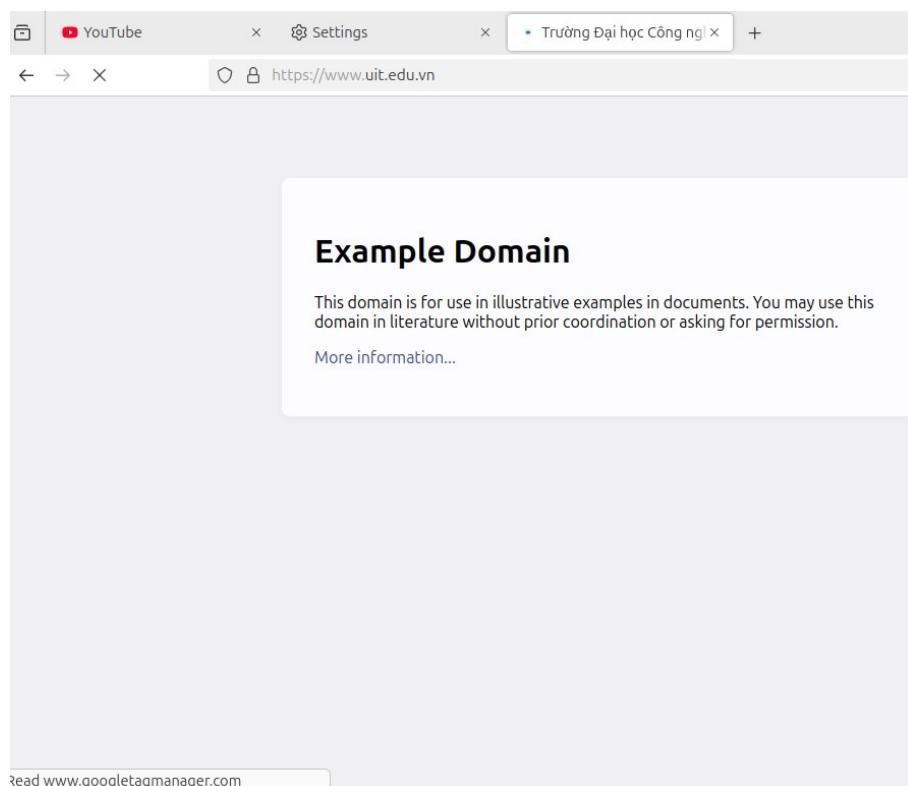
# OPTIONS FOR URL REWRITING
# -----
url_rewrite_program /etc/squid/script.pl
url_rewrite_children 5

# 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
#       and may consult the cache or forward the request to the next hop.
#
```

Sau đó restart lại dịch vụ.

```
tckien@tckien-Virtual-Platform:~/Desktop$ sudo nano /etc/squid/script.pl
tckien@tckien-Virtual-Platform:~/Desktop$ sudo nano /etc/squid/squid.conf
tckien@tckien-Virtual-Platform:~/Desktop$ service squid restart
```

Khi truy cập trang <http://example.com> thì sẽ được chuyển hướng đến <http://www.uit.edu.vn>



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

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

Squid đầu tiên sẽ chuyển thông tin của mỗi yêu cầu web đến script thông qua STDIN.

Sau đó phần url nằm ở đầu mỗi yêu cầu sẽ được tách ra.

Những yêu cầu có url chứa từ khóa "example.com" sẽ được lọc ra, những yêu cầu này sẽ được script in ra <http://www.uit.edu.vn>, tương ứng với việc squid chuyển hướng url. Còn ngược lại sẽ giữ nguyên url.

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)

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).

Để làm được việc đó thì đầu tiên tải một ảnh stop về:



Sau đó copy đến thư mục /var/www/html

```
tckien@tckien-Virtual-Platform:~/Desktop$ sudo cp /etc/squid/stop-sign.jpg /var/www/html
```

Sửa lại chương trình squid trên với địa chỉ lưu trữ hình.

## Lab 01: DEF

### Nhóm GHI

```
tckien@tckien-VMware-Virtual-Platform: ~/Desktop
GNU nano 7.2                                         /etc/squid/script.pl
#!/usr/bin/perl -w
use strict;
use warnings;

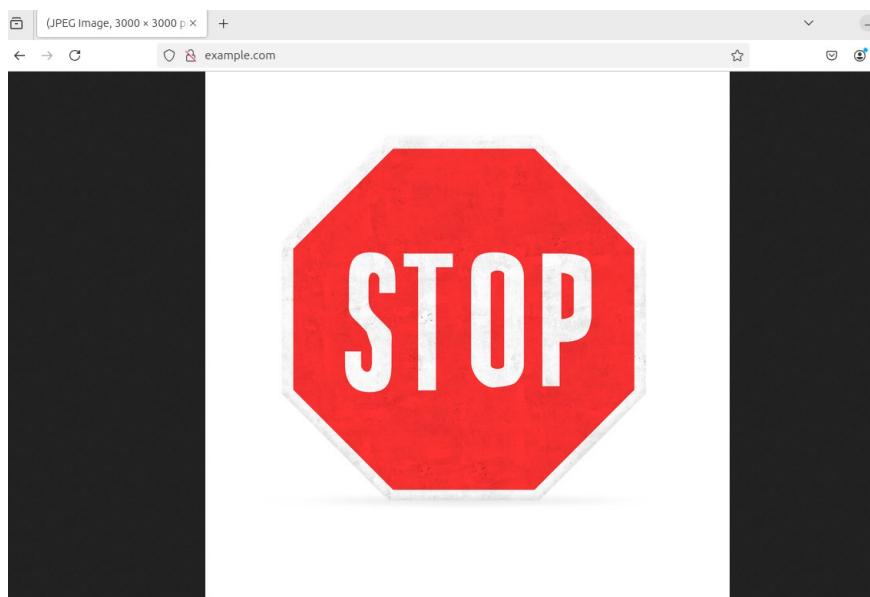
#Force a flush after every write or print on the STDOUT
select STDOUT; $| = 1;

# 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/)
    {
        # File Rewriting
        print "http://10.0.3.4/stop-sign.jpg\n";
    }
    else
    {
        # No Rewriting.
        print "\n";
    }
}
```

Mở dịch vụ apache và restart lại squid

```
tckien@tckien-VMware-Virtual-Platform:~/Desktop$ sudo service squid restart
tckien@tckien-VMware-Virtual-Platform:~/Desktop$ sudo nano /etc/squid/script.pl
tckien@tckien-VMware-Virtual-Platform:~/Desktop$ sudo service apache2 start
```

Sau đó truy cập <http://example.com> trên máy A



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)

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).

Đầu tiên để dễ làm tìm đến một trang sử dụng http.



Sau đó sửa lại thành phần kiểm tra:

- Đầu tiên là url phải là url của trang
- Sau đó kiểm tra xem url phải là url của một tệp ảnh hoặc gif
- Cuối cùng, do phải thay nhiều ảnh khác nhau nên phải đảm bảo mỗi ảnh được thay phải có tên khác nhau để tránh việc caching

## Lab 01: DEF

### Nhóm GHI

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

#Force 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 =~ /sneaindia\.com/)
    {
        # File Rewrite
        if($url =~ /\.(jpg|jpeg|png|gif)$/i){
            print "http://10.0.3.4/stop-sign.jpg?time=". time() ."\n";
        }
        else{
            print "\n";
        }
    }
    else
    {
        # No Rewriting.
        print "\n";
    }
}
```

Sau đó ở cuối tệp squid.conf thêm 2 đoạn sau để vô hiệu hóa caching

Open squid.conf  
/etc/squid (Administrator)

```
# The following Happy Eyeballs directives place additional connection
# opening restrictions: happy_eyeballs_connect_timeout and
# happy_eyeballs_connect_gap. See the former for related terminology.
#Default:
# no artificial limit on the number of concurrent spare attempts

#Disable caching
cache deny all

#Enable debugging to verify URL rewriting
debug_options ALL,1 28,3]
```

Sau khi restart lại dịch vụ và đi đến trang web trên ở máy A thì thấy mọi hình trong đó điều bị sửa lại thành ảnh stop.

The screenshot shows a web browser window with the URL [sneaindia.com](http://sneaindia.com). The page header includes a back button, forward button, and a search bar. The main menu at the top has links for HOME, IMPORTANT CIRCULARS, BUSINESS CIRCULARS, TECHNICAL CIRCULARS, FORUMS, and DOWNLOADS. Below the menu, there's a banner with a red STOP sign graphic and the text "Click Here for book". The main content area displays a news item titled "Restoration of OA level facilities to Recognised and Support Association" dated 21-11-2024. To the right of the news item are two smaller boxes: one for "List of IQs" and another for "SNPWA CHQ Website". At the bottom right of the page is an "Editorial" link.

### 3. 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?

#### Bài tập về nhà (yêu cầu làm)

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

Firewall pfSense hỗ trợ OpenVPN, IPsec, WireGuard, L2TP/IPsec, PPTP

	Đặc điểm	Ưu điểm	Nhược điểm
OpenVPN	-Bảo mật cao -Tùy biến cao -Chạy trên nhiều cổng -Hỗ trợ đa nền tảng	-Khả năng xuyên NAT tốt -Mã nguồn mở -Tích hợp tốt trên pfSense	-Khó cấu hình -Hiệu suất phụ thuộc vào mã hóa -Cần thêm phần mềm thứ ba
IPsec	-Sử dụng các giao thức tiêu chuẩn -Hoạt động ở tầng mạng -Hỗ trợ Site-to-Site và Remote	-Tính tương thích cao -Bảo mật mạnh mẽ -Hiệu suất cao	-Xuyên NAT kém hơn OpenVPN -Có thể bị mở khóa bởi NSA. -Cấu hình phức tạp

	Access.		-Có thể có vấn đề nếu được sử dụng với các tường lửa.
WireGuard	<ul style="list-style-type: none"> <li>-Giao thức VPN hiện đại</li> <li>-Mã nguồn mở</li> <li>-Hoạt động ở tầng mạng</li> </ul>	<ul style="list-style-type: none"> <li>-Tốc độ cao</li> <li>-Cấu hình đơn giản</li> <li>-Bảo mật hiện đại</li> </ul>	<ul style="list-style-type: none"> <li>-Chưa được hỗ trợ rộng rãi</li> <li>-Đang trong quá trình phát triển</li> </ul>
L2TP/IPsec	<ul style="list-style-type: none"> <li>-Kết hợp giữa L2TP và IPsec</li> <li>-Hoạt động ở tầng mạng và dữ liệu</li> </ul>	<ul style="list-style-type: none"> <li>-Hỗ trợ trên nhiều hệ điều hành</li> <li>-Mã hóa mạnh mẽ</li> </ul>	<ul style="list-style-type: none"> <li>-Hiệu suất thấp hơn OpenVPN và WireGuard</li> <li>-Xuyên NAT kém</li> </ul>
PPTP	<ul style="list-style-type: none"> <li>-Giao thức VPN cũ</li> <li>-Hoạt động ở tầng dữ liệu</li> </ul>	<ul style="list-style-type: none"> <li>-Tốc độ cao</li> <li>-Dễ cấu hình</li> </ul>	<ul style="list-style-type: none"> <li>-Bảo mật yếu</li> <li>-Đã bị bẻ khóa bởi NSA</li> </ul>

*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.*

**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.**

Cần thực hiện 3 bước:

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

Bước 1: Tạo hạ tầng khóa công khai PKI

Vào authorize:

System / Certificate / Authorities

Authorities   Certificates   Revocation

Search

Search term:  Both

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
						<input type="button" value="Add"/>

## Đặt tên

Create / Edit CA

<u>Descriptive name</u>	<input type="text" value="Cau11_Lab5"/>	The name of this entry as displayed in the GUI for reference. This name can contain spaces but it cannot contain any of the following characters: ?, >, <, &, /, \, ", '
<u>Method</u>	<input type="button" value="Create an internal Certificate Authority"/>	
<u>Trust Store</u>	<input type="checkbox"/> Add this Certificate Authority to the Operating System Trust Store When enabled, the contents of the CA will be added to the trust store so that they will be trusted by the operating system.	
<u>Randomize Serial</u>	<input type="checkbox"/> Use random serial numbers when signing certificates 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.	
<b>Internal Certificate Authority</b>		
<u>Key type</u>	<input type="button" value="RSA"/>	
	<input type="button" value="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>	<input type="button" value="sha256"/>	
	The digest method used when the CA is signed. The best practice is to use SHA256 or higher. Some services and platforms, such as the GUI web server and OpenVPN, consider weaker digest algorithms invalid.	
<u>Lifetime (days)</u>	<input type="button" value="3650"/>	

# Lab 01: DEF

## Nhóm GHI

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 SHA256 or higher. Some services and platforms, such as the GUI web server and OpenSSL, do not support lower digest algorithms.	
<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>	LAB5_NT140
<u>Organizational Unit</u>	NT140.1_LAB5

**Save**

Tạo thành công:

Certificate Authorities						
Name	Internal	Issuer	Certificates	Distinguished Name	In Use	Actions
Cau11_Lab5 ✓		self-signed	0	ST=HCM, OU=NT140.1_LAB5, O=LAB5_NT140, L=HCM, CN=internal-ca, C=VN	<a href="#">i</a>	

Valid From: Tue, 26 Nov 2024 12:14:46 +0700  
Valid Until: Fri, 24 Nov 2034 12:14:46 +0700

**Add**

Server:

Authorities	Certificates	Certificate Revocation		
<b>Search</b>				
Search term	<input type="text"/>	Both <a href="#">Search</a> <a href="#">Clear</a>		
Enter a search string or *nix regular expression to search certificate names and distinguished names.				
<b>Certificates</b>				
Name	Issuer	Distinguished Name	In Use	Actions
GUI default (6736a7d112dc8) Server Certificate CA: No Server: Yes	self-signed	O=pfSense GUI default Self-Signed Certificate, CN=pfSense-6736a7d112dc8	<a href="#">i</a>	webConfigurator

**Add/Sign**

**Add/Sign a New Certificate**

<b>Method</b>	<input type="button" value="Create an internal Certificate"/>
<b>Descriptive name</b>	Cau11_Lab5_server
The name of this entry as displayed in the GUI for reference. This name can contain spaces but it cannot contain any of the following characters: ?, >, <, &, /, \, ", '	
<b>Internal Certificate</b>	
<b>Certificate authority</b>	Cau11_Lab5
<b>Key type</b>	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.
<b>Digest Algorithm</b>	sha256
The digest method used when the certificate is signed. The best practice is to use SHA256 or higher. Some services and platforms, such as the GUI web server and OpenVPN, consider weaker digest algorithms invalid.	
<b>Lifetime (days)</b>	3650
The length of time the signed certificate will be valid, in days. Server certificates should not have a lifetime over 398 days or some platforms may consider the certificate invalid.	
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.
<b>Digest Algorithm</b>	sha256
The digest method used when the certificate is signed. The best practice is to use SHA256 or higher. Some services and platforms, such as the GUI web server and OpenVPN, consider weaker digest algorithms invalid.	
<b>Lifetime (days)</b>	3650
The length of time the signed certificate will be valid, in days. Server certificates should not have a lifetime over 398 days or some platforms may consider the certificate invalid.	
<b>Common Name</b>	Cau11_Lab5_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>	LAB5_NT140
<b>Organizational Unit</b>	NT140.1_LAB5

# Lab 01: DEF

## Nhóm GHI

**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 SAN Row** + Add SAN Row

**Save**

**Authorities** **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
GUI default (6736a7d112dc8)	self-signed	O=pfSense GUI default Self-Signed Certificate, CN=pfSense-6736a7d112dc8	i	webConfigurator
Server Certificate		Valid From: Fri, 15 Nov 2024 08:45:53 +0700		
CA: No		Valid Until: Thu, 18 Dec 2025 08:45:53 +0700		
Server: Yes				
Cau11_Lab5_server	Cau11_Lab5	ST=HCM, OU=NT140.1_LAB5, O=LAB5_NT140, L=HCM, CN=Cau11_Lab5_Cert, C=VN	i	
Server Certificate		Valid From: Tue, 26 Nov 2024 12:17:35 +0700		
CA: No		Valid Until: Fri, 24 Nov 2034 12:17:35 +0700		
Server: Yes				

+ Add/Sign

## Bước 2: Cấu hình OpenVPN

Vào openvpn:

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 khóa đã tạo

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\_Lab5

>> Add new CA >> Next

Server Certificate Selection

OpenVPN Remote Access Server Setup Wizard

#### Choose a Server Certificate

Certificate: Cau11\_Lab5\_server

>> Add new Certificate >> Next

Sau đó thêm tên

Server Setup

OpenVPN Remote Access Server Setup Wizard

#### General OpenVPN Server Information

Description: Cau11\_5

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.

#### Endpoint Configuration

Protocol: UDP on IPv4 only

Protocol to use for OpenVPN connections. If unsure, leave this set to UDP.

Interface: WAN

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

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.

#### Cryptographic Settings

TLS Authentication:  Enable authentication of TLS packets.

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

TLS Shared Key: [Redacted]

# Lab 01: DEF

## Nhóm GHI

<b>TLS Authentication</b>	<input checked="" type="checkbox"/> Enable authentication of TLS packets.
<b>Generate TLS Key</b>	<input checked="" type="checkbox"/> Automatically generate a shared TLS authentication key.
<b>TLS Shared Key</b>	<input type="text"/>
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 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)
<b>Tunnel Settings</b>	
<b>IPv4 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 IPv4 Gateway</b>	<input checked="" type="checkbox"/> Force all client generated traffic through the tunnel.
<b>IPv4 Local Network</b>	192.168.3.0/24
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.
<b>Duplicate Connections</b>	<input type="checkbox"/> Allow multiple concurrent connections from clients using the same Common Name. NOTE: This is not generally recommended, but may be needed for some scenarios.

# Lab 01: DEF

## Nhóm GHI

**Client Settings**

Dynamic IP	<input checked="" type="checkbox"/> Allow connected clients to retain their connections if their IP address changes.
Topology	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".	

**Advanced Client Settings**

DNS Default Domain	<input type="text"/>
Provide a default domain name to clients.	
DNS Server 1	<input type="text"/>
DNS server IP to provide to connecting clients.	
DNS Server 2	<input type="text"/>
DNS server IP to provide to connecting clients.	
DNS Server 3	<input type="text"/>
DNS server IP to provide to connecting clients.	
DNS Server 4	<input type="text"/>
DNS server IP to provide to connecting clients.	
NTP Server	<input type="text"/>
Network Time Protocol server to provide to connecting clients.	
NTP Server 2	<input type="text"/>
Network Time Protocol server to provide to connecting clients.	
NetBIOS Options	<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.
NetBIOS Node Type	<input 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).	
NetBIOS Scope ID	<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.	
WINS Server 1	<input type="text"/>
A Windows Internet Name Service (WINS) server IP to provide to connecting clients. Not desirable in most all modern networks.	
WINS Server 2	<input type="text"/>
A Windows Internet Name Service (WINS) server IP to provide to connecting clients. Not desirable in most all modern networks.	

**>> Next**

Tick 2 rules:

# Lab 01: DEF

## Nhóm GHI

**Wizard / OpenVPN Remote Access Server Setup / Firewall Rule Configuration**

Step 10 of 11

**Firewall Rule Configuration**

OpenVPN Remote Access Server Firewall Rules

Rules control passing or blocking network traffic as it flows through the firewall.

Rules must be added which allow traffic to reach the OpenVPN server IP address and port, as well as to allow traffic from connected clients inside the OpenVPN tunnel.

The options on this step can add automatic rules to pass this traffic, or rules can be configured manually after completing the wizard.

**Traffic from clients to server**

Firewall Rule  Add a rule to permit connections to this OpenVPN server instance 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.

Adding users for the VPN depends on the chosen authentication method. For example, add local users with certificates under [System > User Manager](#). For remote authentication servers, add certificates directly in [System > Certificate Manager](#).

To easily 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	Cau11_5	

**+ Add**

Bước 3: Cấu hình quyền truy cập của client

Giờ đến client:

## Lab 01: DEF

### Nhóm GHI

Địa chỉ server là địa chỉ NAT của pfSense:

Đặt tên là userB và mật khẩu là userB@123

Phần tiếp theo giữ yên

# Lab 01: DEF

## Nhóm GHI

**Cryptographic Settings**

<b>TLS Configuration</b>	<input checked="" type="checkbox"/> <b>Use a TLS Key</b> 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"/> <b>Automatically generate a TLS Key.</b>
<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_Lab5
<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)
	Certificates known to be incompatible with use for OpenVPN are not included in this list, such as certificates using incompatible ECDSA curves or weak digest algorithms.
<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-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"/> <b>Enforce key usage</b> Verify that remote host uses a server certificate (EKG: "TLS Web Server Authentication").

Giữ yên mặc định những cấu hình sau đó.

Đến Advanced Configuration chọn IPv4:

The screenshot shows the Winbox interface for configuration. At the top, it says "Advanced Configuration". Below that, there's a "Custom options" section with a text input field and a note: "Enter any additional options to add to the OpenVPN client configuration here, separated by semicolon." There are several configuration sections:

- UDP Fast I/O**: A checkbox labeled "Use fast I/O operations with UDP writes to tun/tap. Experimental." with a note: "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**: A dropdown set to "Retry 1x" with a note: "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." Below this, a note states: "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**: A dropdown set to "Default" with a note: "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**: Radio buttons for "Both", "IPv4 only", and "IPv6 only". A note below says: "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**: A dropdown set to "default" with a note: "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."

Below this, the interface shows "VPN / OpenVPN / Clients". Under "Clients", there are tabs for "Servers", "Clients" (which is selected), "Client Specific Overrides", and "Wizards". The "Clients" table lists one client entry:

OpenVPN Clients					
Interface	Protocol	Server	Mode / Crypto	Description	Actions
WAN	UDP4 (TUN)	10.0.3.3:1194	<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	Cau11_5_Client	

A green "Add" button is located at the bottom right of the table.

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

## Lab 01: DEF

### Nhóm GHI

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	1.9.2	Exports pre-configured OpenVPN Client configurations directly from pfSense software.	+ Install
WireGuard	0.2.1	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.	+ Install

Nhấn install openvpn-clientexport và chọn confirm

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

Installed Packages Available Packages Package Installer

**Package Installation**

```
[4/5] Installing 7-zip-23.01...
[4/5] Extracting 7-zip-23.01: .... done
[5/5] Installing pfSense-pkg-openvpn-client-export-1.9.2...
[5/5] Extracting pfSense-pkg-openvpn-client-export-1.9.2: .... done
Saving updated package information...
done.
Loading package configuration... done.
Configuring package components...
Loading package instructions...
Custom commands...
Executing custom_php_install_command()...done.
Writing configuration... done.
>>> Cleaning up cache... done.
Success
```

Tạo user VPN

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

Vào System -> User Manager -> Users -> Edit

userB và mật khẩu là userB@123 và tick phần tạo user certificate

# Lab 01: DEF

## Nhóm GHI

**User Properties**

Defined by	USER
Disabled	<input type="checkbox"/> This user cannot login
Username	userB
Password	*****
Full name	Lab5_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	<input type="text" value="admins"/> <div style="display: flex; justify-content: space-between;"> <div>Not member of</div> <div>Member of</div> </div> <div style="display: flex; justify-content: space-around; margin-top: 10px;"> <span>&gt;&gt; Move to "Member of" list</span> <span>&lt;&lt; Move to "Not member of" list</span> </div> <p>Hold down CTRL (PC)/COMMAND (Mac) key to select multiple items.</p>
Certificate	<input checked="" type="checkbox"/> Click to create a user certificate

### Đặt tên cho cert

**Create Certificate for User**

Descriptive name	<input type="text" value="Cau11_Lab5_VPNuser_cert"/>
Certificate authority	<input type="text" value="Cau11_Lab5"/>
Key type	<input type="text" value="RSA"/>
<input type="text" value="2048"/> <p>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.</p>	
Digest Algorithm	<input type="text" value="sha256"/>
<p>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</p>	
Lifetime	<input type="text" value="3650"/>

**Keys**

Authorized SSH Keys	<input type="text"/>
<p>Enter authorized SSH keys for this user</p>	
IPsec Pre-Shared Key	<input type="text"/>

## Lab 01: DEF

### Nhóm GHI

The screenshot shows the 'Users' section of the User Manager. It lists two users: 'admin' (System Administrator) and 'userB' (Lab5\_Openvpn). Both users have a checked status and belong to the 'admins' group. There are edit and delete icons for each user.

Username	Full name	Status	Groups	Actions
admin	System Administrator	✓	admins	
userB	Lab5_Openvpn	✓		

Tiếp theo, điều hướng đến Client Export dưới menu OpenVPN để tải bộ cấu hình Client Configuration.

The screenshot shows the 'Client Export Utility' section of the OpenVPN interface. It displays the 'OpenVPN Server' configuration for 'Cau11\_5 UDP4:1194'. Below it, the 'Client Connection Behavior' section is visible.

Chọn most client:

The screenshot shows the 'OpenVPN Clients' section. It lists a single client named 'userB' with a certificate named 'Cau11\_Lab5\_VPNuser\_cert'. On the right, there are various export options for this client, including 'Inline Configurations' (Most Clients, Android, OpenVPN Connect), 'Bundled Configurations' (Archive, Config File Only), and specific installers for Windows (64-bit, 32-bit), Previous Windows (64-bit, 32-bit), Legacy Windows (10/2016/2019, 7/8/8.1/2012/2), and Viscosity (Viscosity Bundle, Viscosity Inline Config).

Chạy tệp đó và ping đến máy A:

# Lab 01: DEF

## Nhóm GHI

```

openvpn set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 3 not upgraded.
tckien@tckien-VMware-Virtual-Platform:~/Desktop$ sudo openvpn --config pfSense-UDP4-1194-userB-config.ovpn
2024-11-26 13:13:26 OpenVPN 2.6.12 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL] [PKCS11] [MH/PKTINFO] [AEAD] [DCO]
2024-11-26 13:13:26 library versions: OpenSSL 3.0.13 30 Jan 2024, LZO 2.10
2024-11-26 13:13:26 DCO version: N/A
Enter Auth Username: userB
Enter Auth Password: *****
2024-11-26 13:13:38 TCP/UDP: Preserving recently used remote address: [AF_INET]10.0.3.3:1194
2024-11-26 13:13:38 UDPv4 link local: (not bound)
2024-11-26 13:13:38 UDPv4 link remote: [AF_INET]10.0.3.3:1194
2024-11-26 13:13:38 WARNING: this configuration may cache passwords in memory -- use the auth-nocache option to prevent this
2024-11-26 13:13:38 [Cau11_Lab5_Cert] Peer Connection Initiated with [AF_INET]10.0.3.3:1194
2024-11-26 13:13:40 TUN/TAP device tun0 opened
2024-11-26 13:13:40 net_iface_mtu_set: mtu 1500 for tun0
2024-11-26 13:13:40 net_iface_up: set tun0 up
2024-11-26 13:13:40 net_addr_v4_add: 10.101.1.2/24 dev tun0
2024-11-26 13:13:40 Initialization Sequence Completed
64 bytes from 192.168.3.3: icmp_seq=46 ttl=63 time=1.41 ms

```

Vào status và kiểm tra thấy có một connection là thành công:

ovpn1: Cau11_5 UDP4:1194 / Client Connections: 1									
Common Name	Real Address	Virtual Address	Last Change	Bytes Sent	Bytes Received	Cipher	Actions		
userB	10.0.3.4:36387	10.101.1.2	2024-11-26 13:13:38	13 KIB	21 KIB	AES-256-GCM	<span style="color: red;">X</span>	<span style="color: green;">C</span>	<span style="color: blue;">O</span>

[Show Routing Table](#) - Display OpenVPN's internal routing table for this server.

Client Instance Statistics									
Name	Status	Last Change	Local Address	Virtual Address	Remote Host	Bytes Sent	Bytes Received	Service	
ovpnclient2	Reconnecting (Ping Restart)	Tue Nov 26 13:10:36 2024	(pending)		(pending)	0 B	0 B	<span style="color: green;">C</span>	