Phòng thí nghiệm An toàn Thông tin InsecLab
Trường Đại học Công nghệ Thông tin (UIT)

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	Từ Chí Kiên	22520713	22520713@gm.uit.edu.vn

2. NỘI DUNG THỰC HIỆN:[1]

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.

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

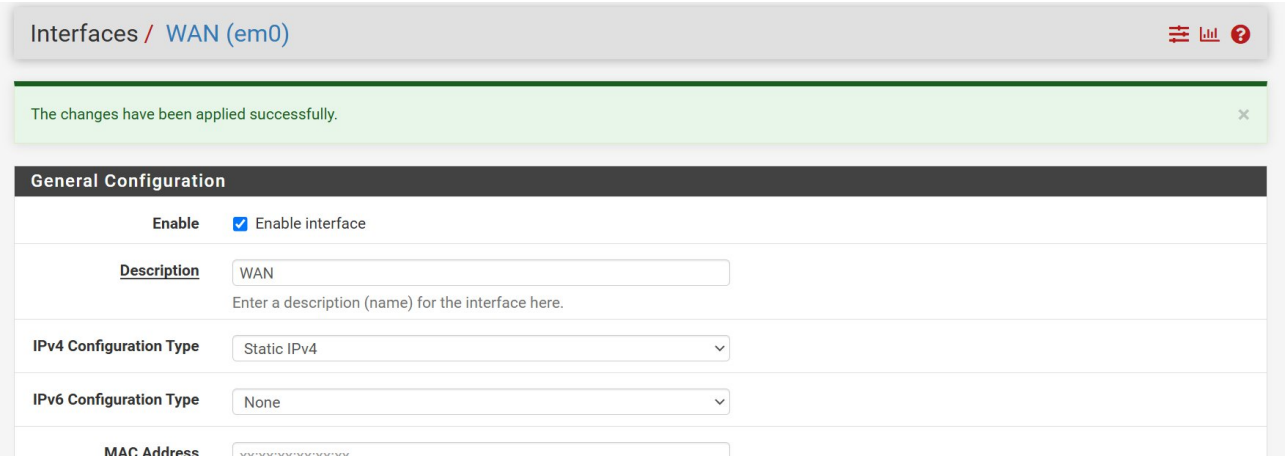
BÁO CÁO CHI TIẾT

A. THỰC HÀNH

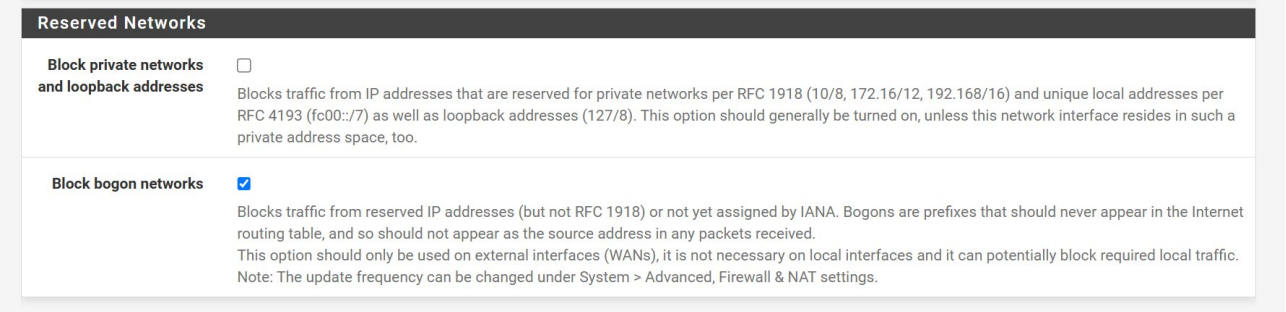
1. Cài đặt pfSense firewall

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:



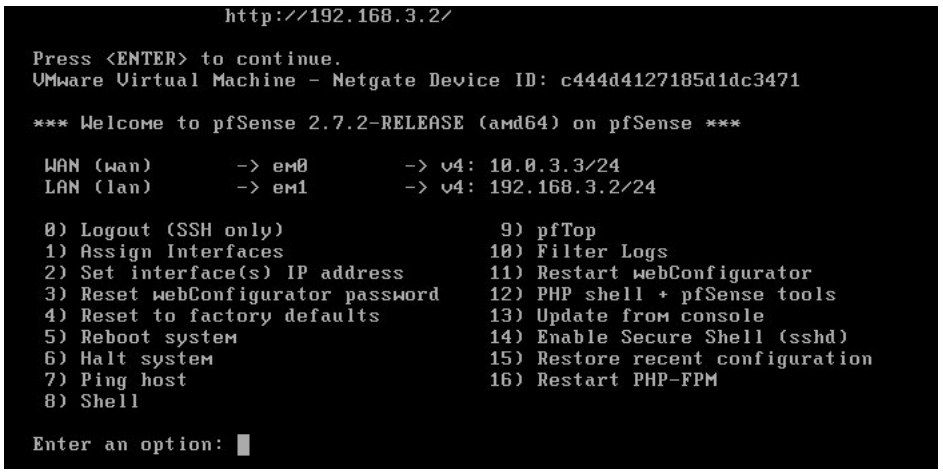
Và tắt phần **Block private networks and loopback addresses**



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



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

Máy B thì cấu hình:

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
☐ ✓	0/0 B	IPv4 *	*	*	WAN subnets	*	*	none			
☐ ✓	0/0 B	IPv4 *	WAN subnets	*	*	*	*	none			

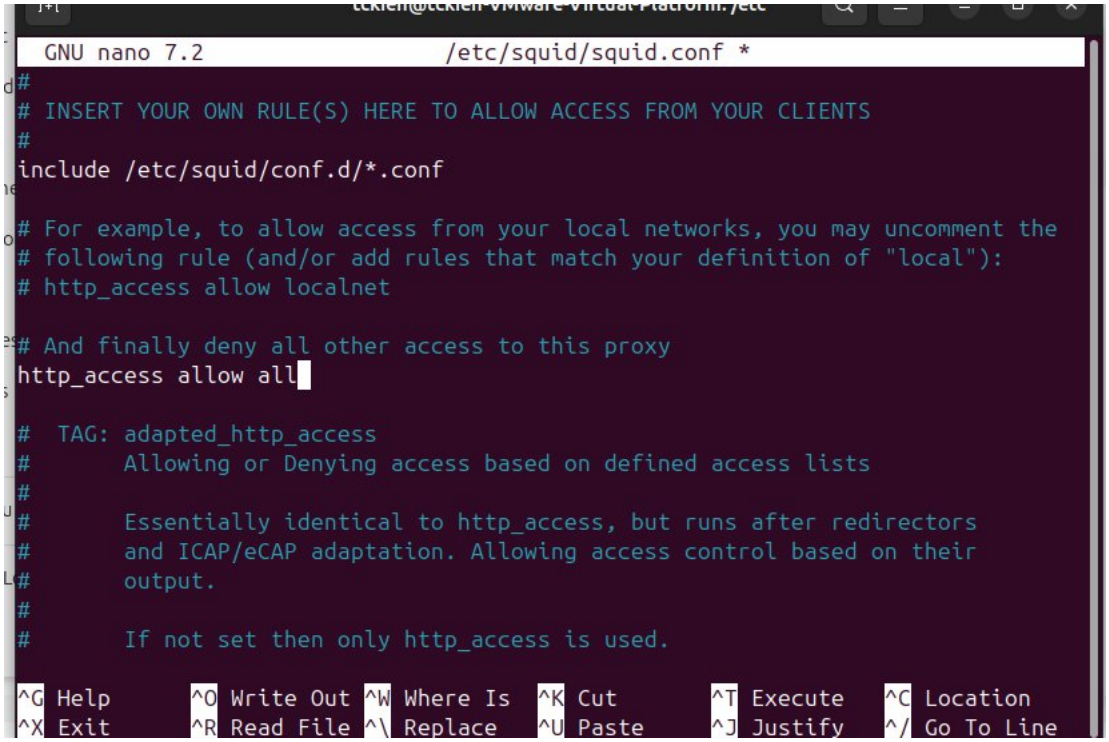
Thì ping được

```
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
```

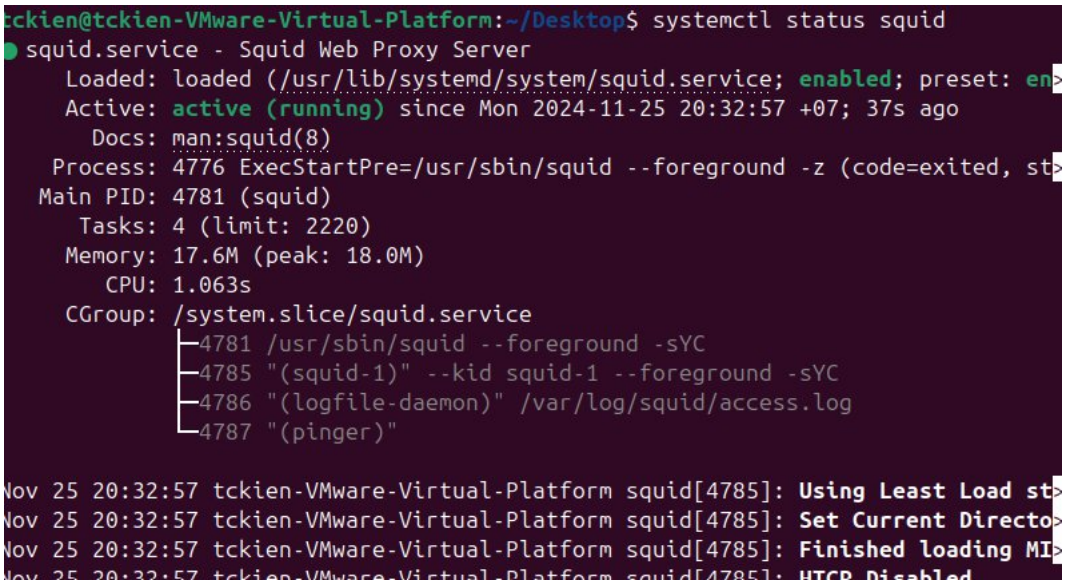
2. Triển khai Web Proxy (Application Firewall)

a) Cài đặt và cấu hình Squid

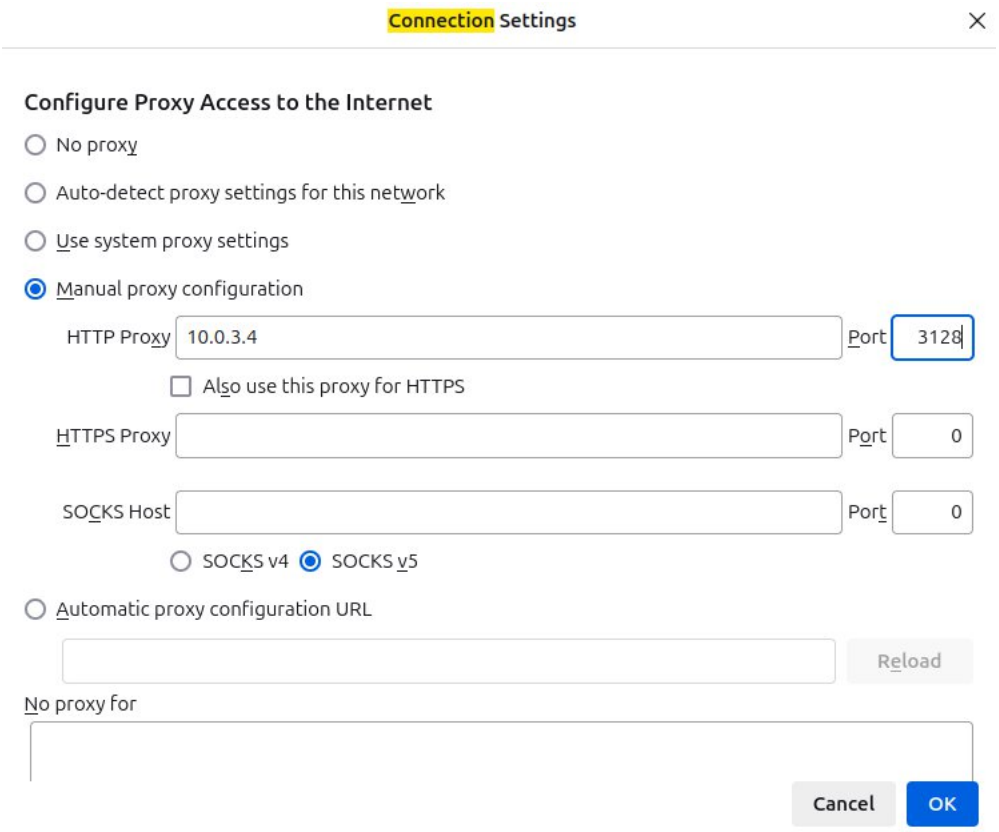
Sửa lại tệp http để cho phép http



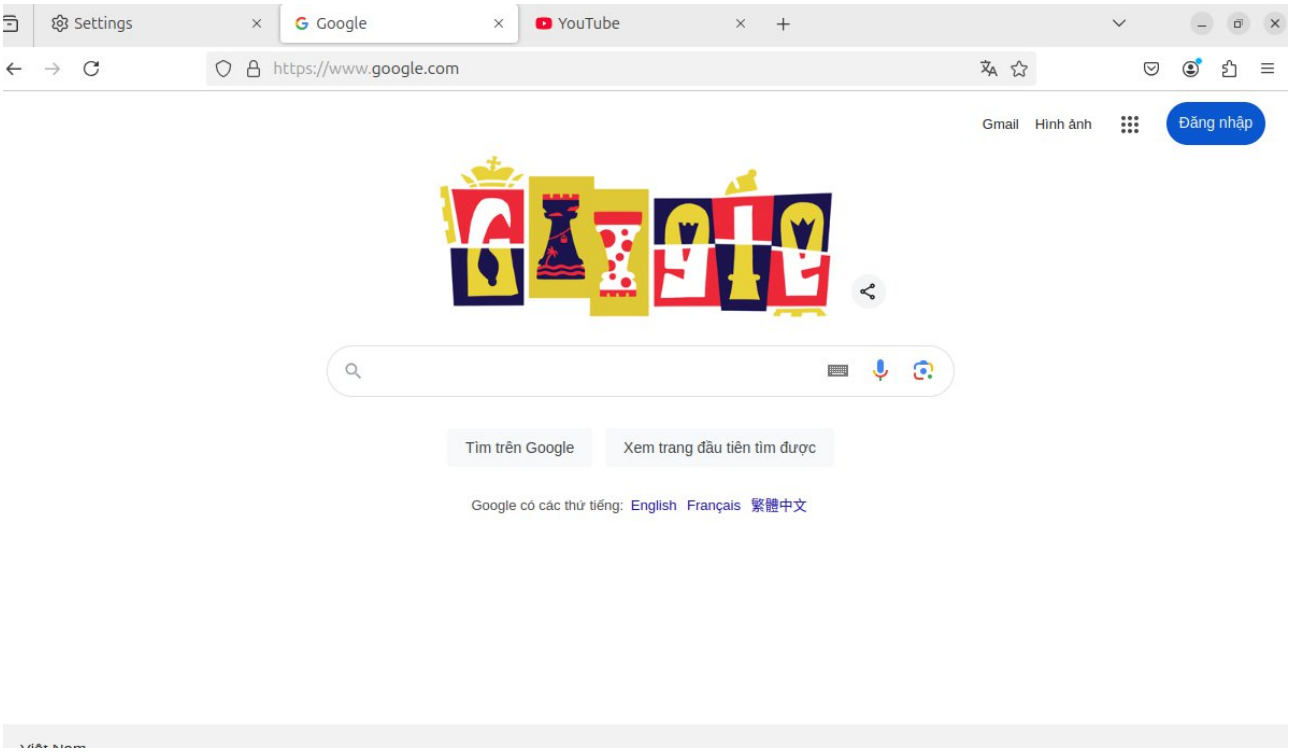
Kiểm tra xem squid có đang hoạt động không

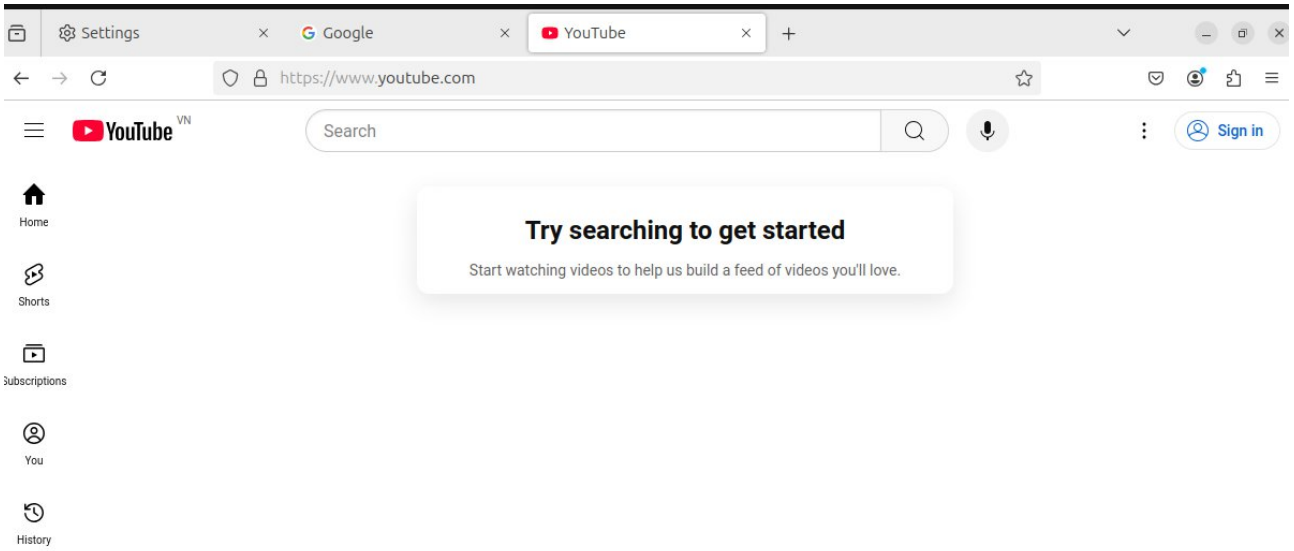


Cấu hình proxy bằng địa chỉ máy B và cổng 3128 trên máy A:



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";
  }
}
```

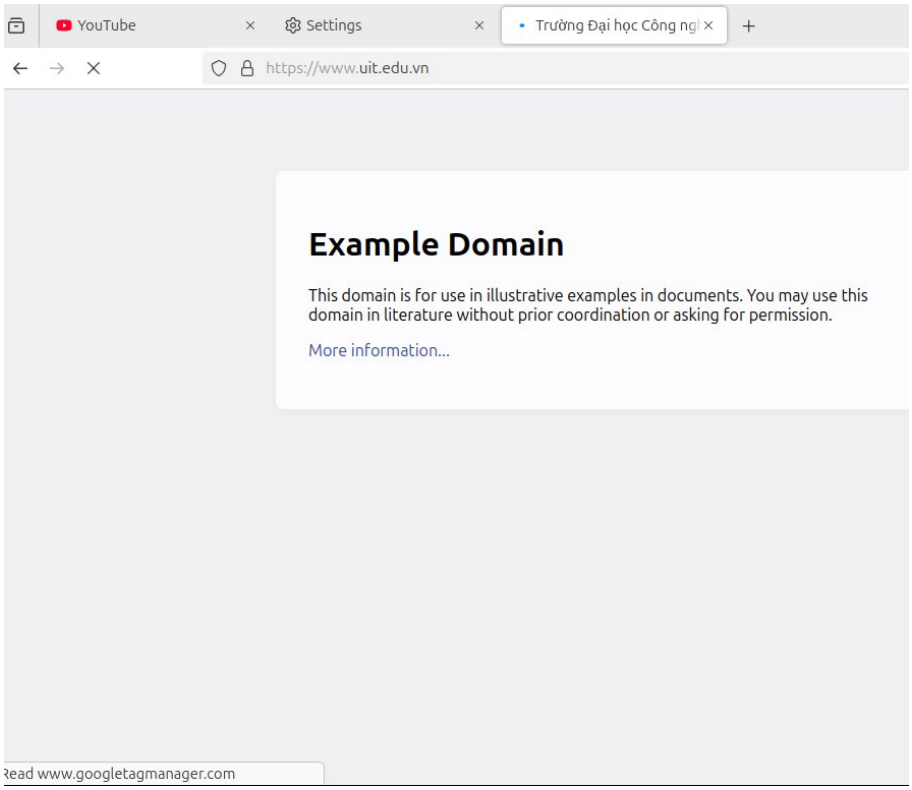
Sau đó trong tệp conf thêm hai đoạn sau để chạy chương trình

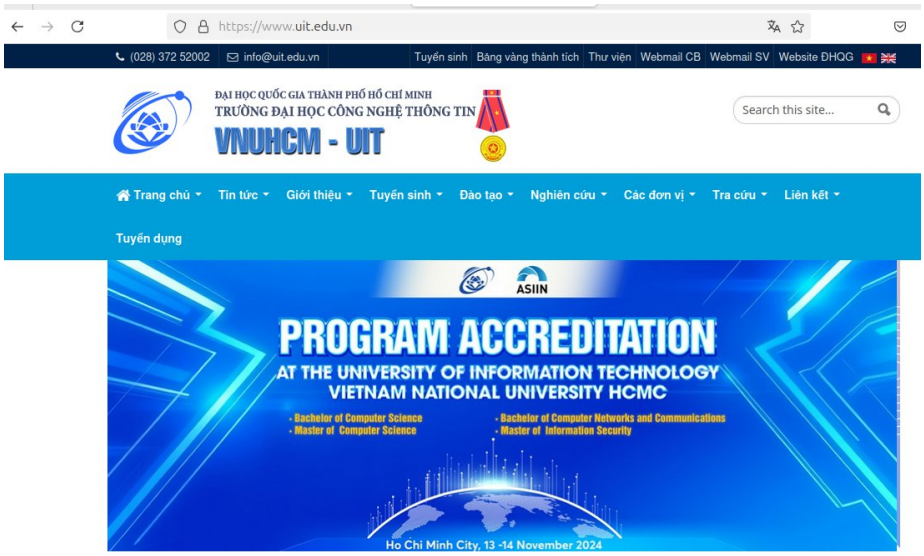
```
 GNU nano 7.2                                  /etc/squid/squid.conf *
# unlinkd_program /usr/lib/squid/unlinkd

#  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-VMware-Virtual-Platform:~/Desktop$ sudo nano /etc/squid/script.pl
tckien@tckien-VMware-Virtual-Platform:~/Desktop$ sudo nano /etc/squid/squid.conf
tckien@tckien-VMware-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-VMware-Virtual-Platform:~/Desktop$ sudo cp /etc/squid/stop-sign.jpg /var/www/html
```

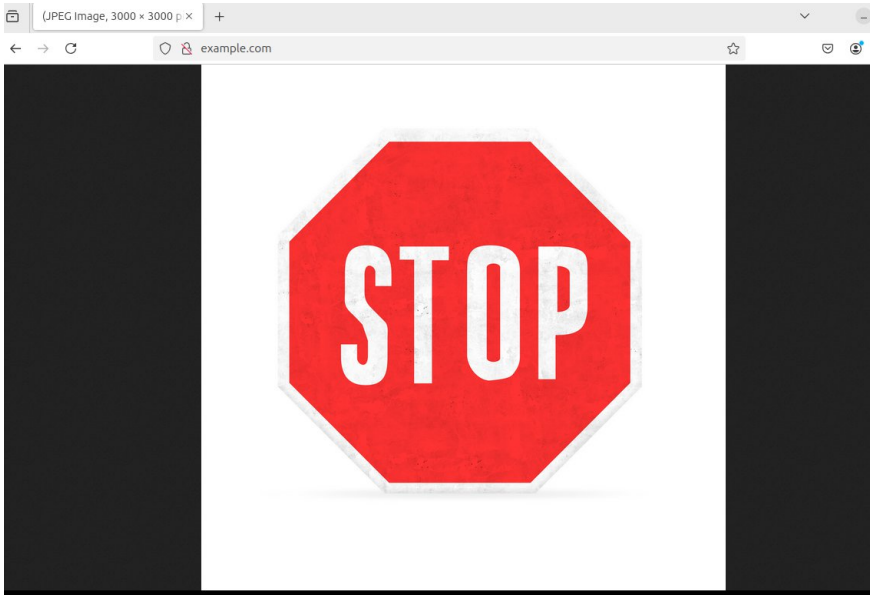
Sửa lại chương trình squid trên với địa chỉ lưu trữ hình.

```
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 hoạ 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 hoạ 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

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

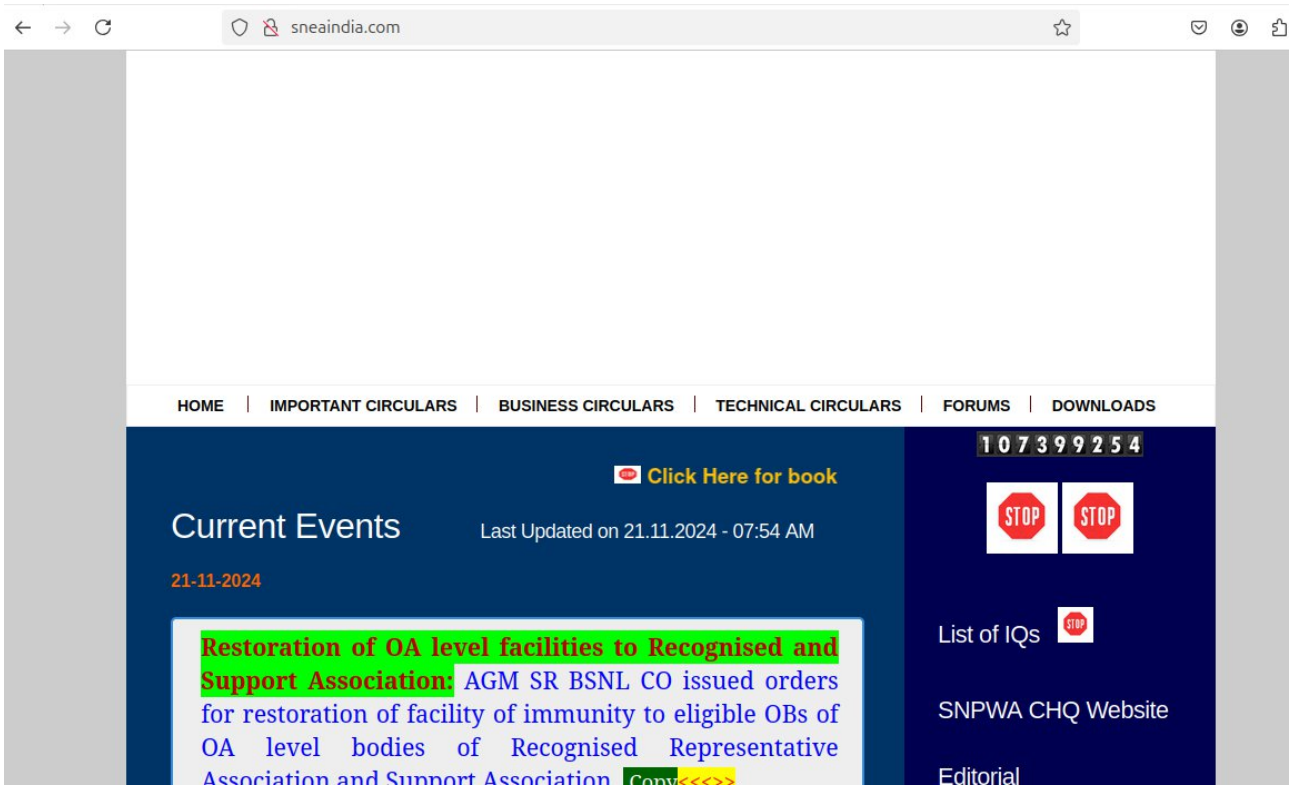
Sau đó ở cuối tệp squid.conf thêm 2 đoạn sau để vô hiệu hóa caching

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.



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	-Giao thức VPN hiện đại -Mã nguồn mở -Hoạt động ở tầng mạng	-Tốc độ cao -Cấu hình đơn giản -Bảo mật hiện đại	-Chưa được hỗ trợ rộng rãi -Đang trong quá trình phát triển
L2TP/IPsec	-Kết hợp giữa L2TP và IPsec -Hoạt động ở tầng mạng và dữ liệu	-Hỗ trợ trên nhiều hệ điều hành -Mã hóa mạnh mẽ	-Hiệu suất thấp hơn OpenVPN và WireGuard -Xuyên NAT kém
PPTP	-Giao thức VPN cũ -Hoạt động ở tầng dữ liệu	-Tốc độ cao -Dễ cấu hình	-Bảo mật yếu -Đã bị bẻ khóa bởi NSA

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:

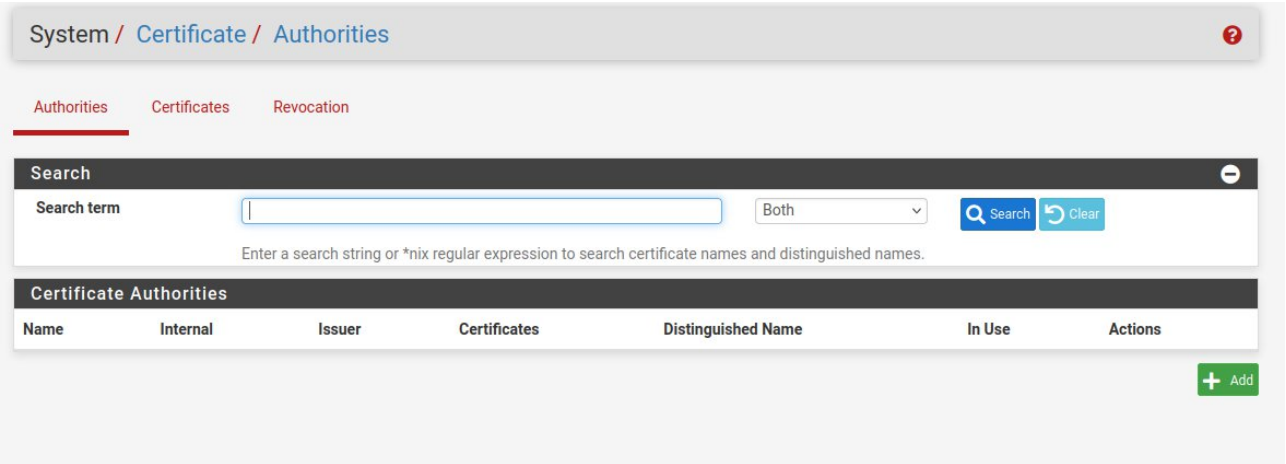
-Tạo hạ tầng khóa công khai (PKI Infrastructure)

-Cấu hình OpenVPN trên PFSense

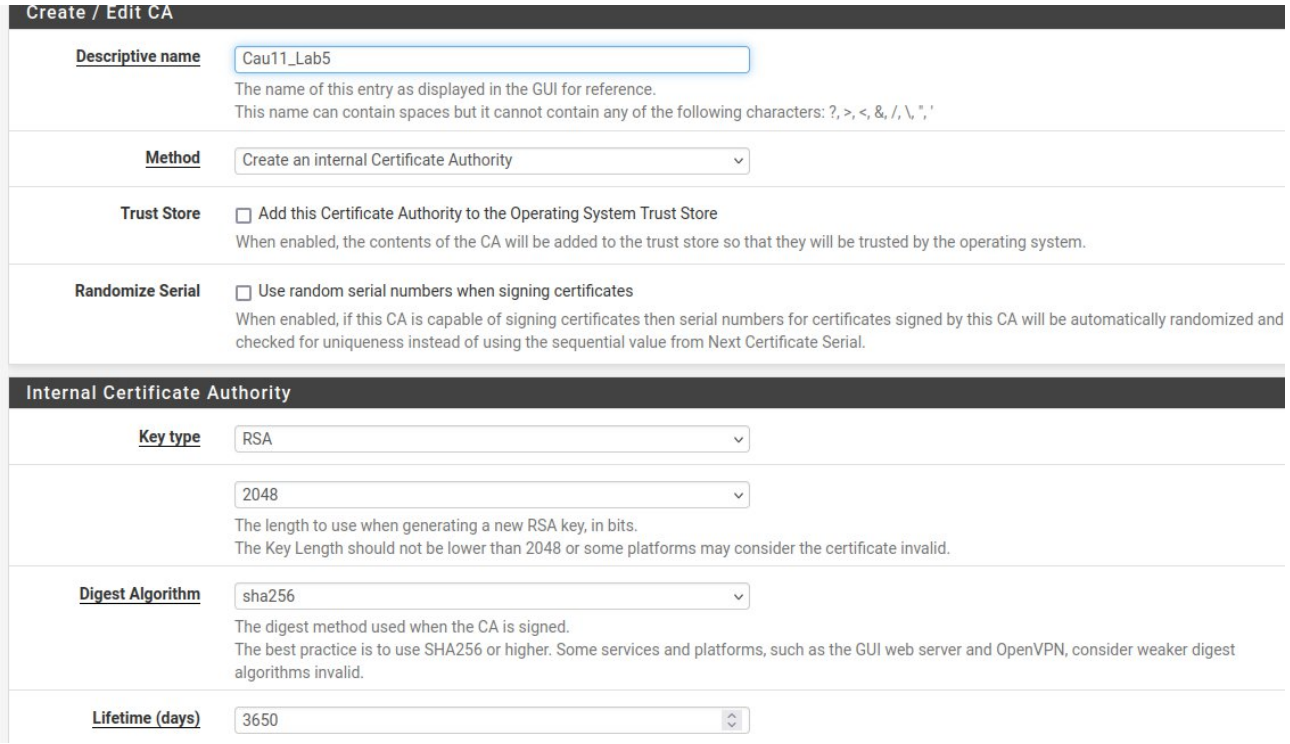
-Cấu hình quyền truy cập của client

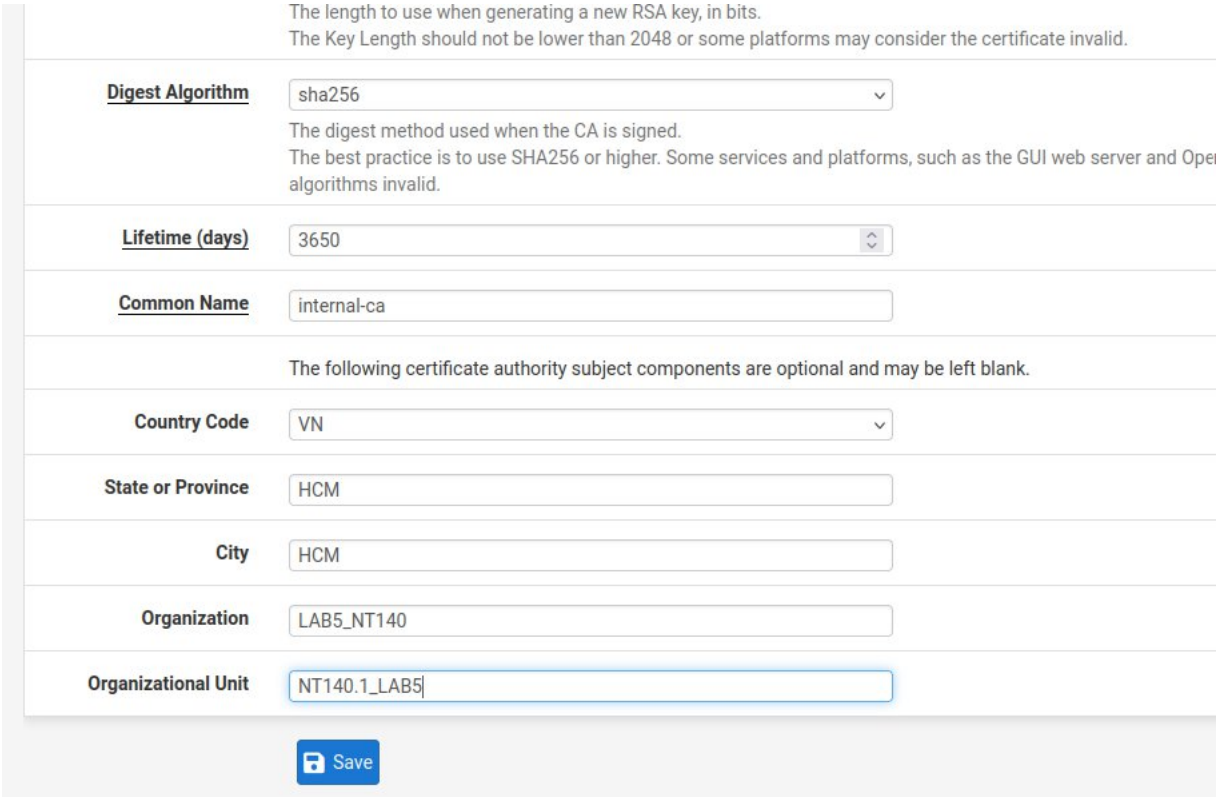
Bước 1: Tạo hạ tầng khóa công khai PKI

Vào authorize:

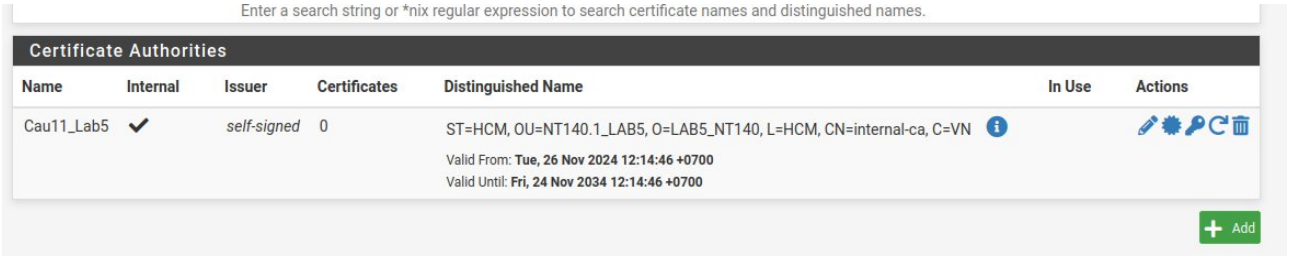

System / Certificate / Authorities
Authorities
Certificates
Revocation
Search
Search term
Both
Search
Clear
Enter a search string or *nix regular expression to search certificate names and distinguished names.
Certificate Authorities
Name
Internal
Issuer
Certificates
Distinguished Name
In Use
Actions
Add

Đặt tên

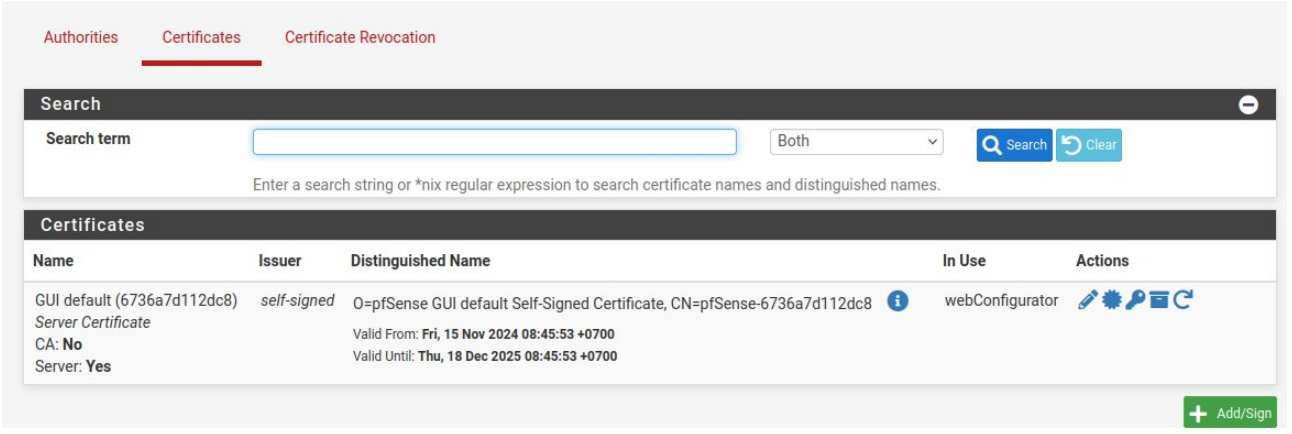

Create / Edit CA
Descriptive name
Cau11_Lab5
The name of this entry as displayed in the GUI for reference.
This name can contain spaces but it cannot contain any of the following characters: ?, >, <, &, /, \, ", '
Method
Create an internal Certificate Authority
Trust Store
Add this Certificate Authority 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.
Randomize Serial
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.
Internal Certificate Authority
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 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.
Lifetime (days)
3650

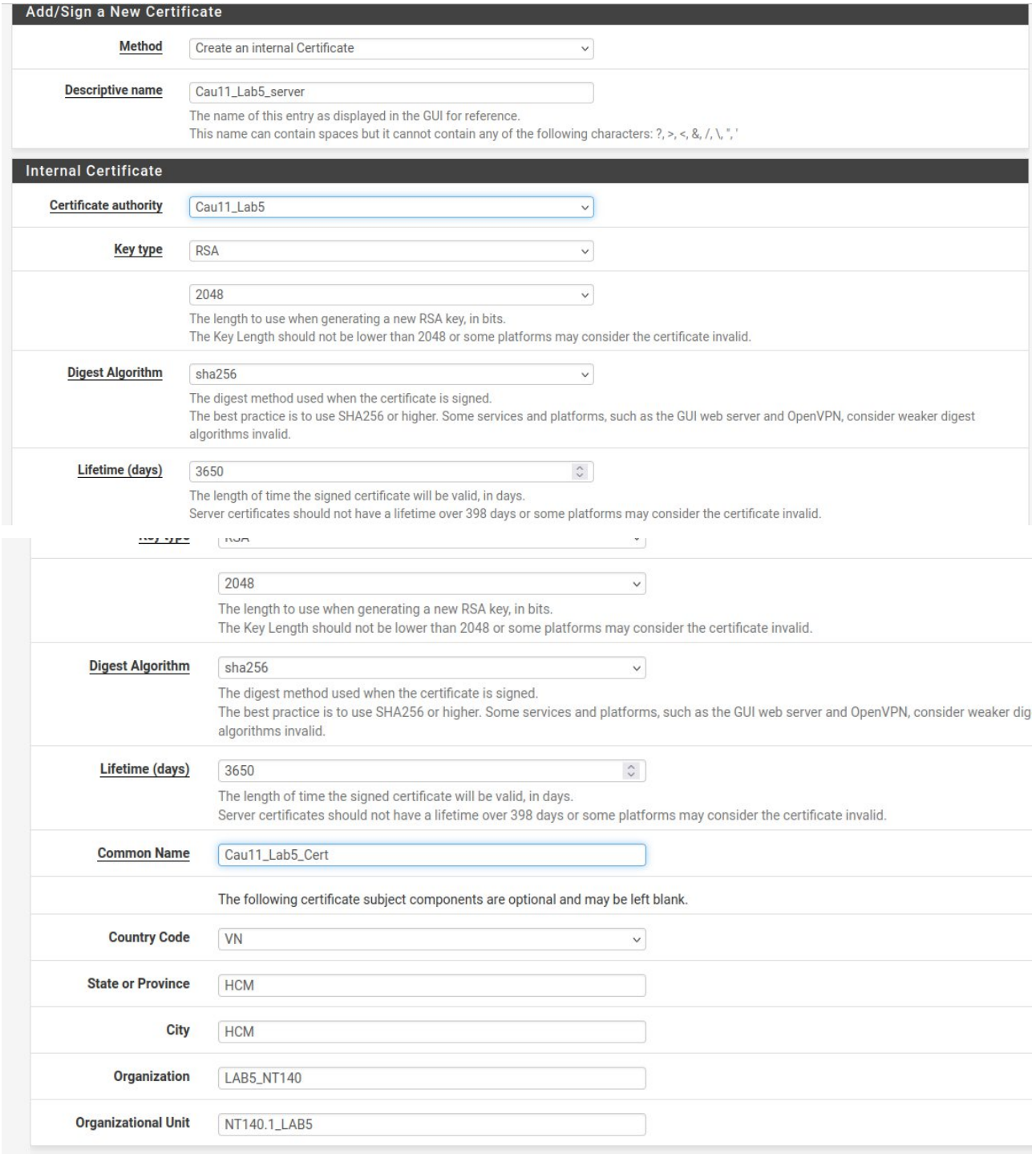


Tạo thành công:

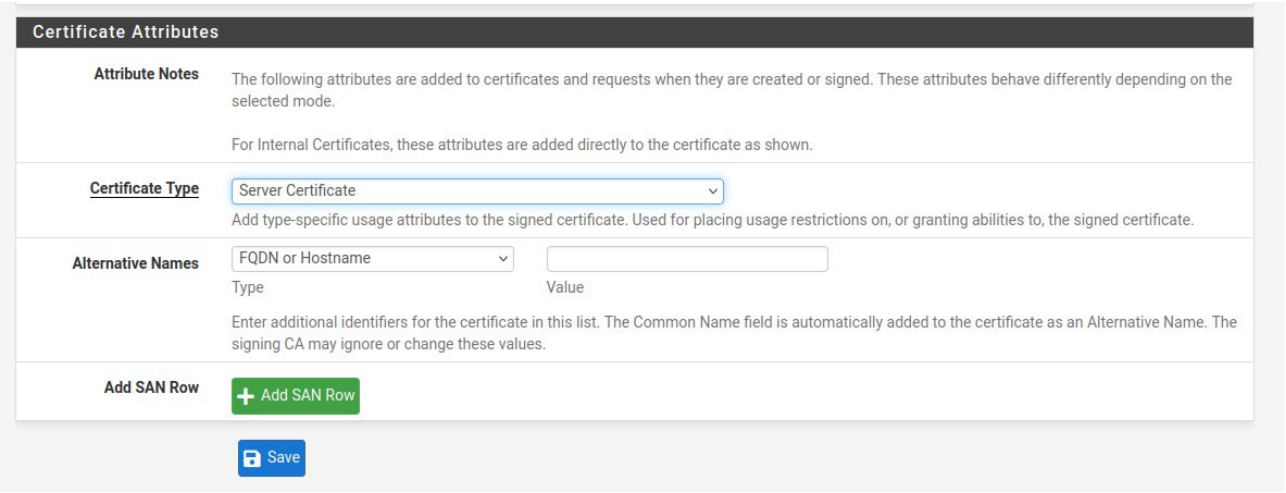


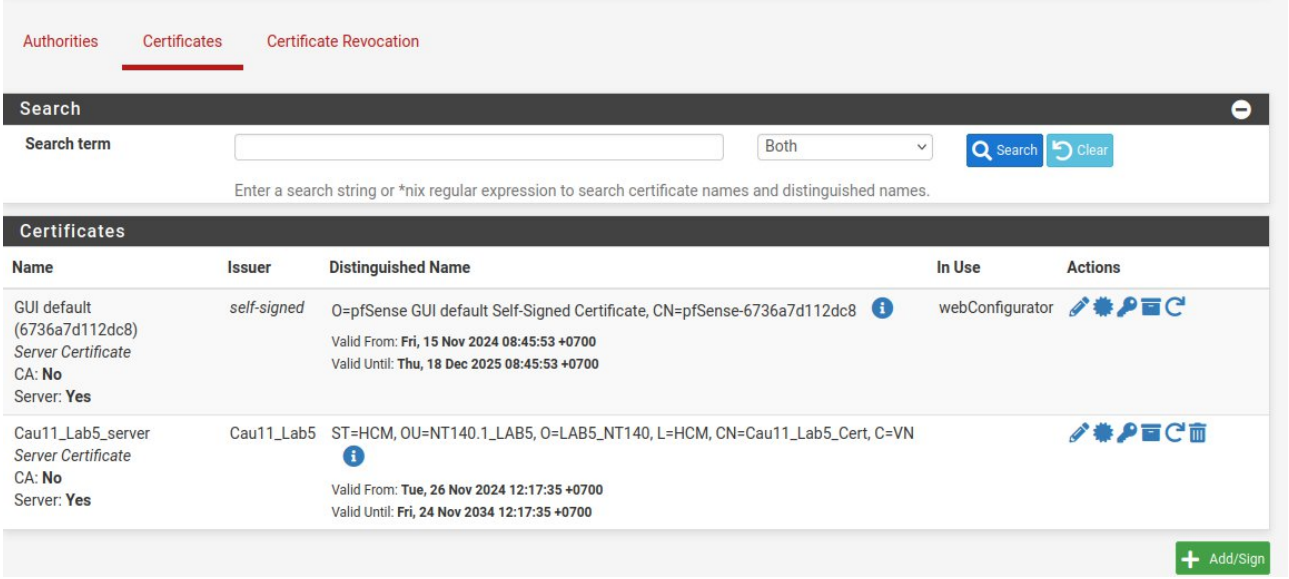
Server:




Add/Sign a New Certificate
Method
Create an internal Certificate
Descriptive name
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: ?, >, <, &, /, \, ", '
Internal Certificate
Certificate authority
Cau11_Lab5
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 SHA256 or higher. Some services and platforms, such as the GUI web server and OpenVPN, consider weaker digest algorithms invalid.
Lifetime (days)
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.

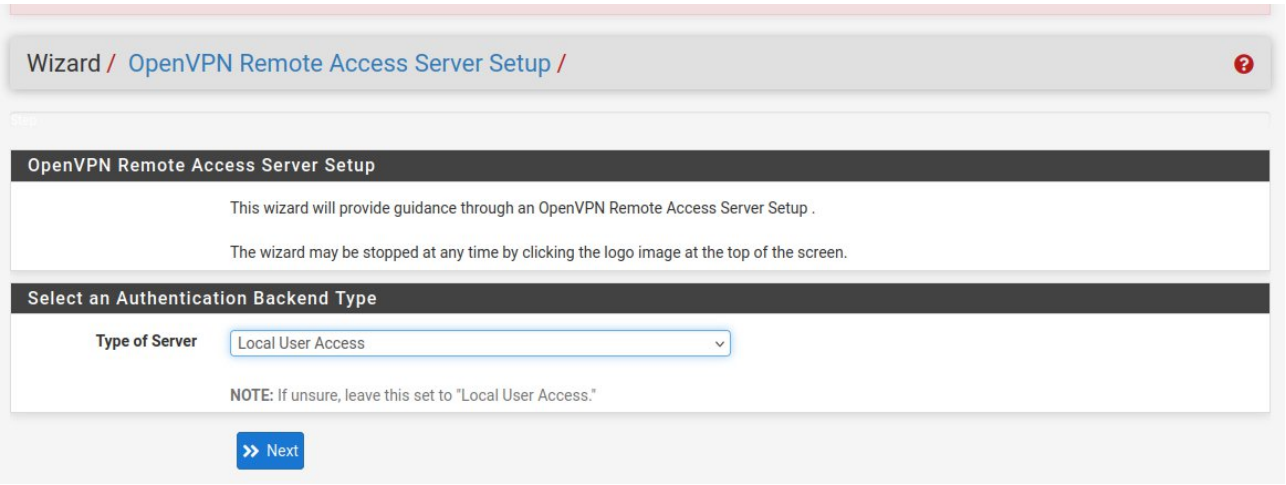
2048
The length to use when generating a new RSA key, in bits.
The Key Length should not be lower than 2048 or some platforms may consider the certificate invalid.
Digest Algorithm
sha256
The digest method used when the certificate is signed.
The best practice is to use SHA256 or higher. Some services and platforms, such as the GUI web server and OpenVPN, consider weaker dig
algorithms invalid.
Lifetime (days)
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.
Common Name
Cau11_Lab5_Cert
The following certificate subject components are optional and may be left blank.
Country Code
VN
State or Province
HCM
City
HCM
Organization
LAB5_NT140
Organizational Unit
NT140.1_LAB5



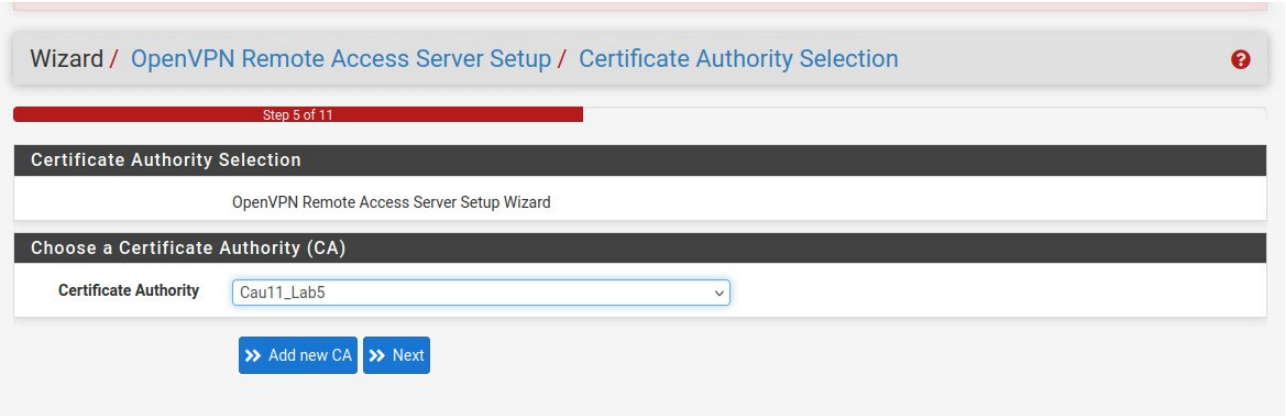


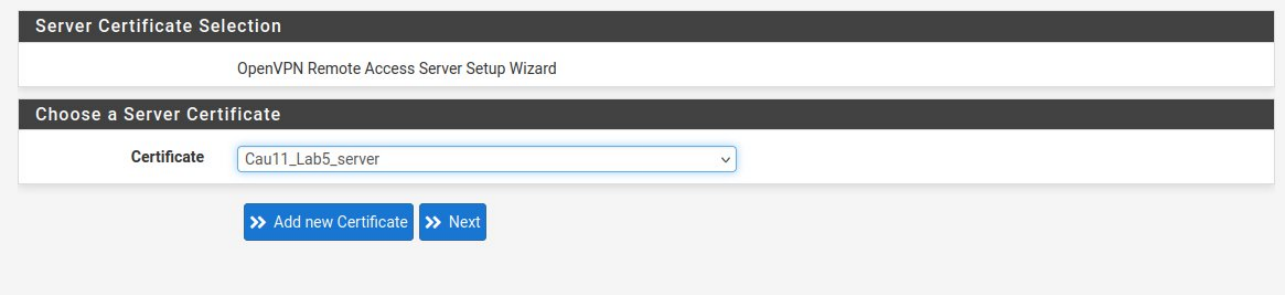
Bước 2: Cấu hình OpenVPN

Vào openvpn:

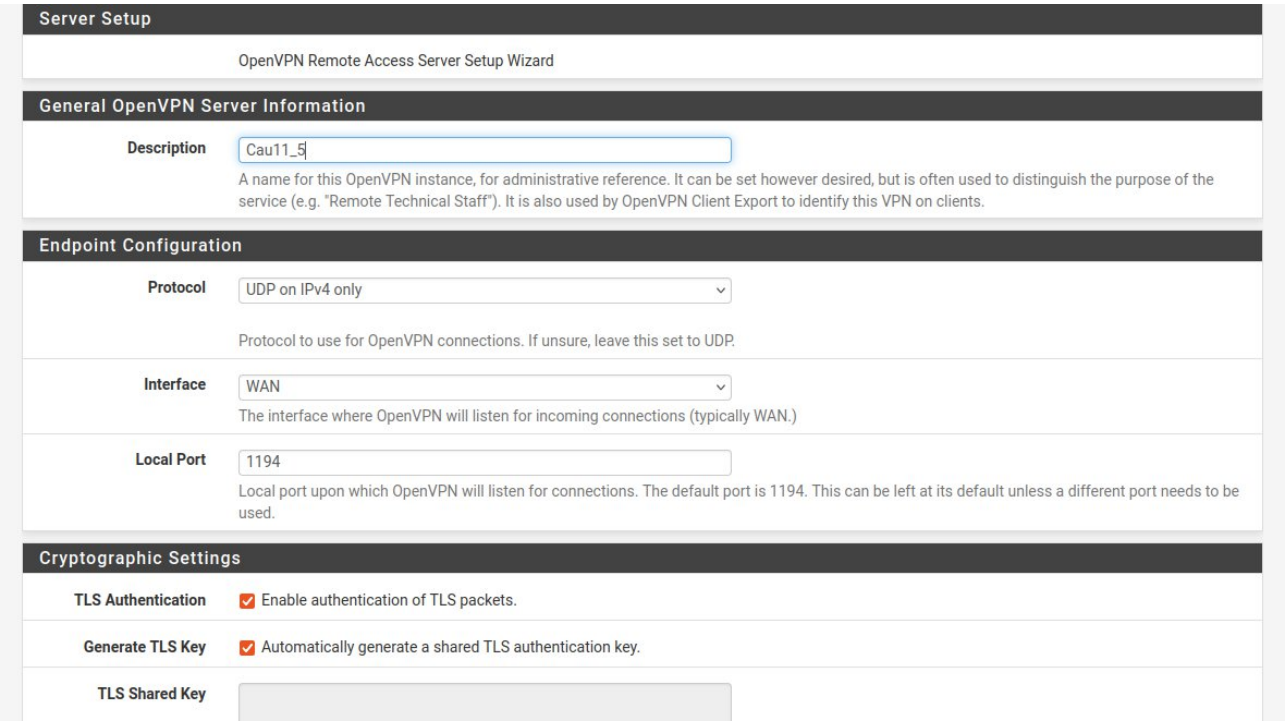


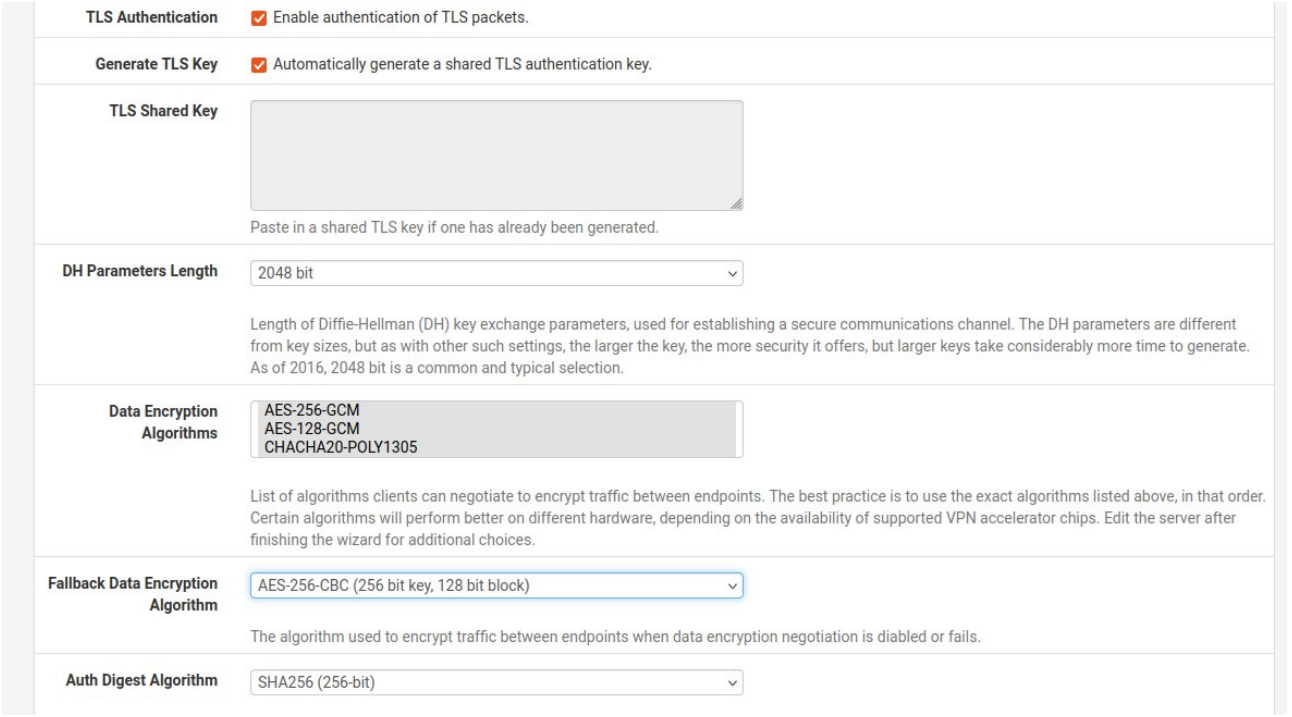
Chọn khóa đã tạo

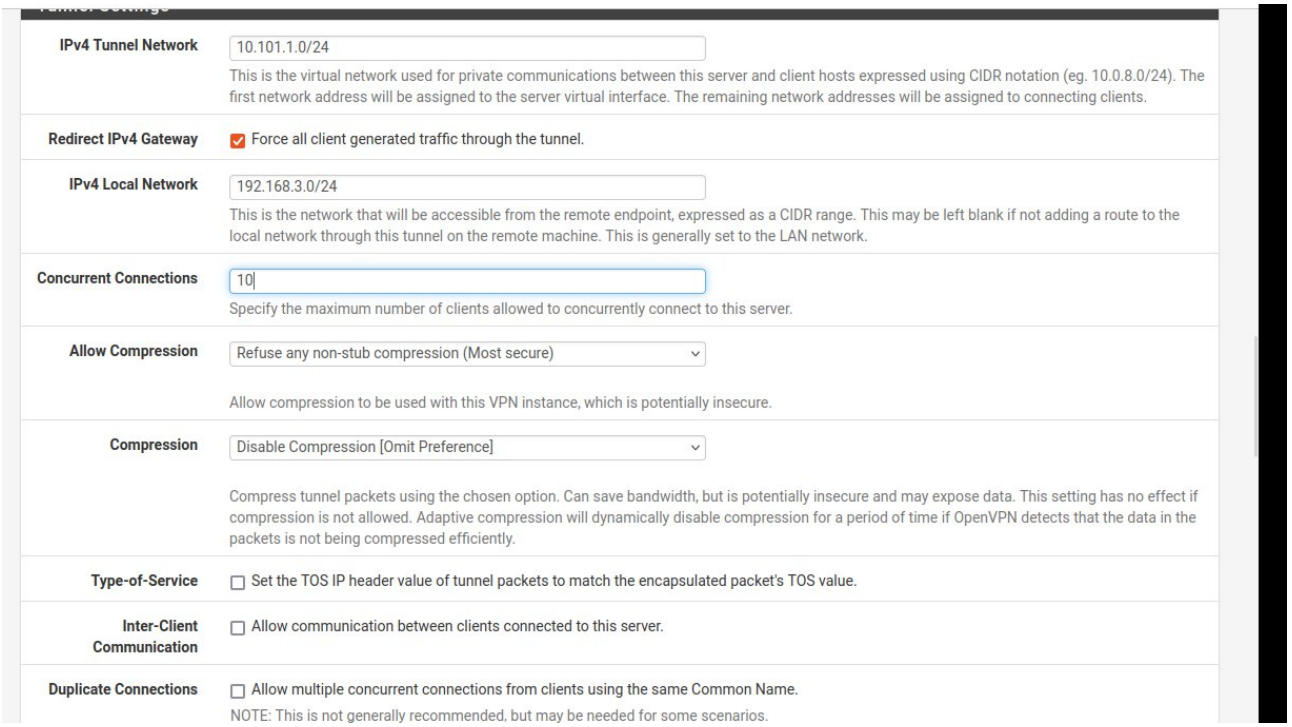


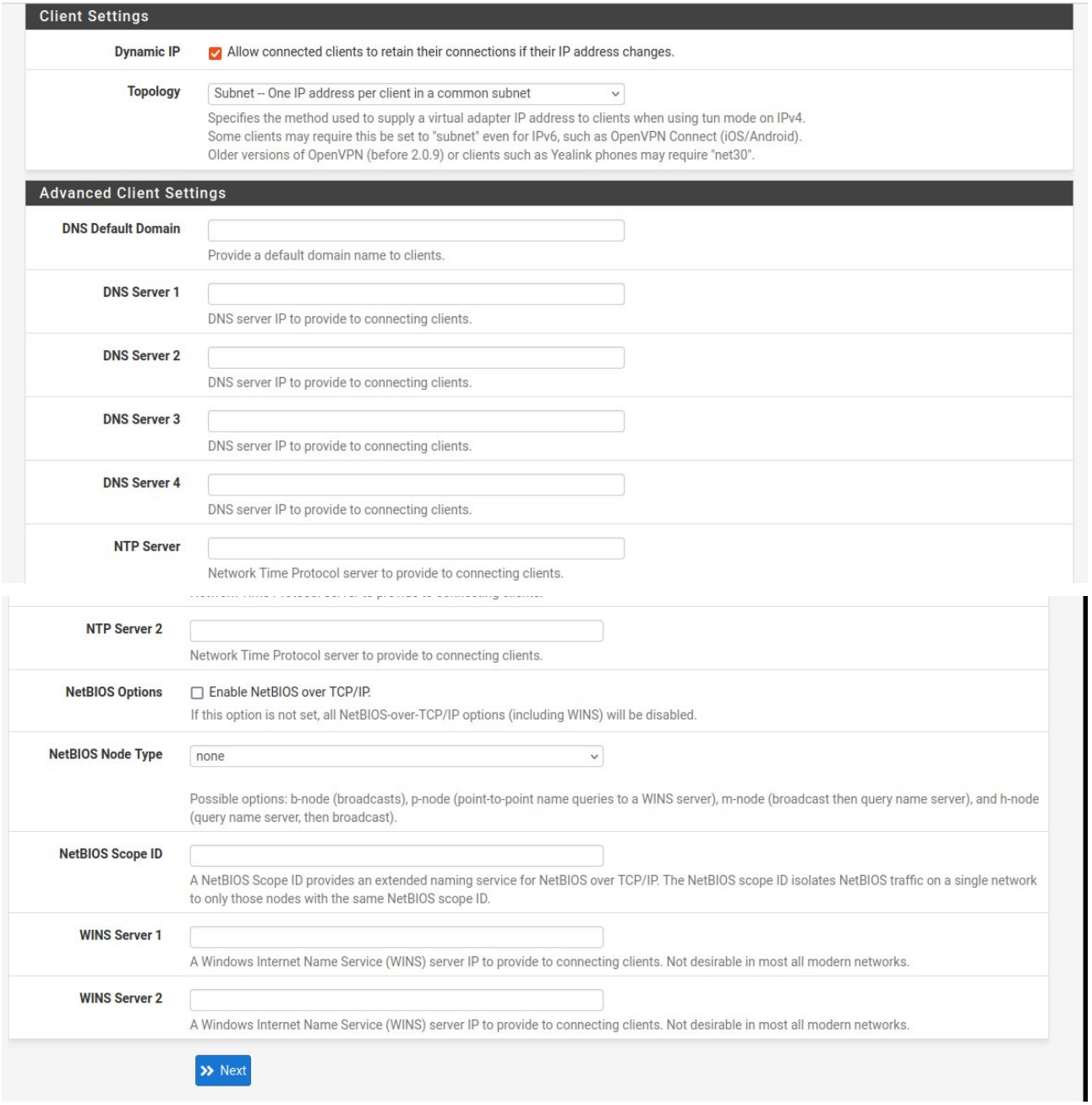


Sau đó thêm tên

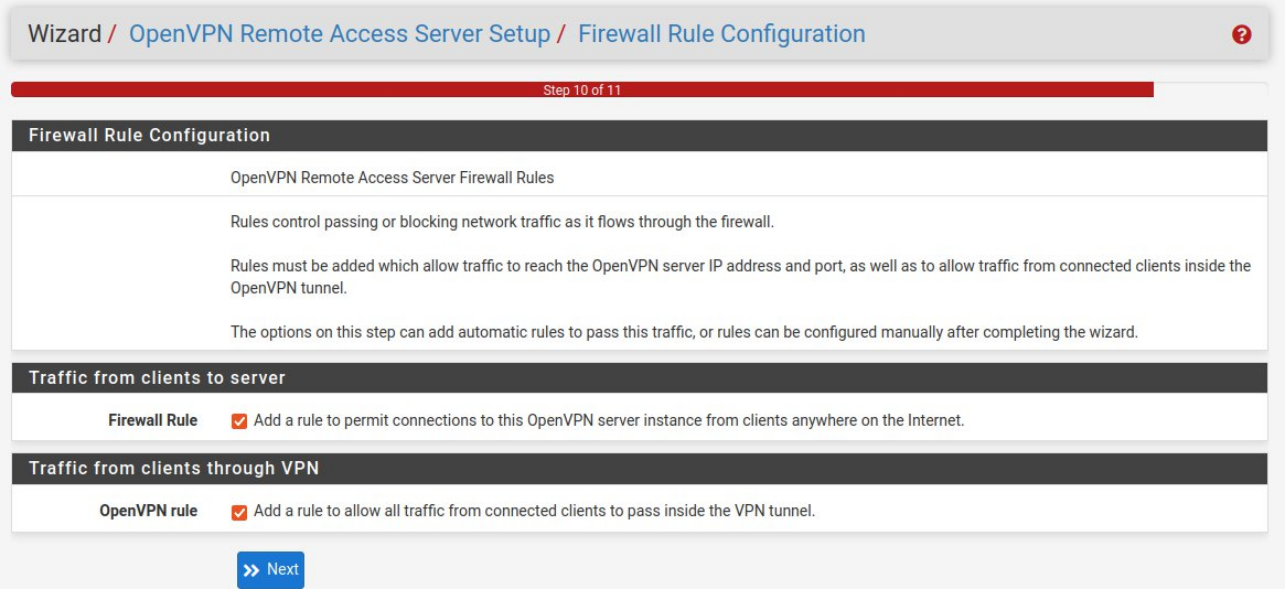


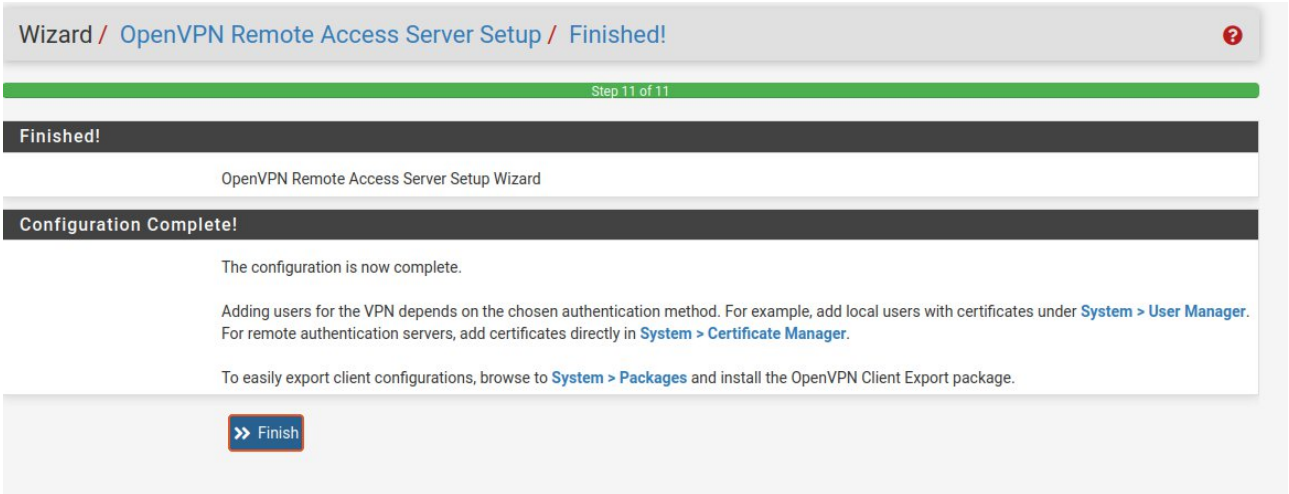

TLS Authentication
Enable authentication of TLS packets.
Generate TLS Key
Automatically generate a shared TLS authentication key.
TLS Shared Key
Paste in a shared TLS key if one has already been generated.
DH Parameters Length
2048 bit
Length of Diffie-Hellman (DH) key exchange parameters, used for establishing 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.
Data Encryption Algorithms
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.
Fallback Data Encryption Algorithm
AES-256-CBC (256 bit key, 128 bit block)
The algorithm used to encrypt traffic between endpoints when data encryption negotiation is diabled or fails.
Auth Digest Algorithm
SHA256 (256-bit)

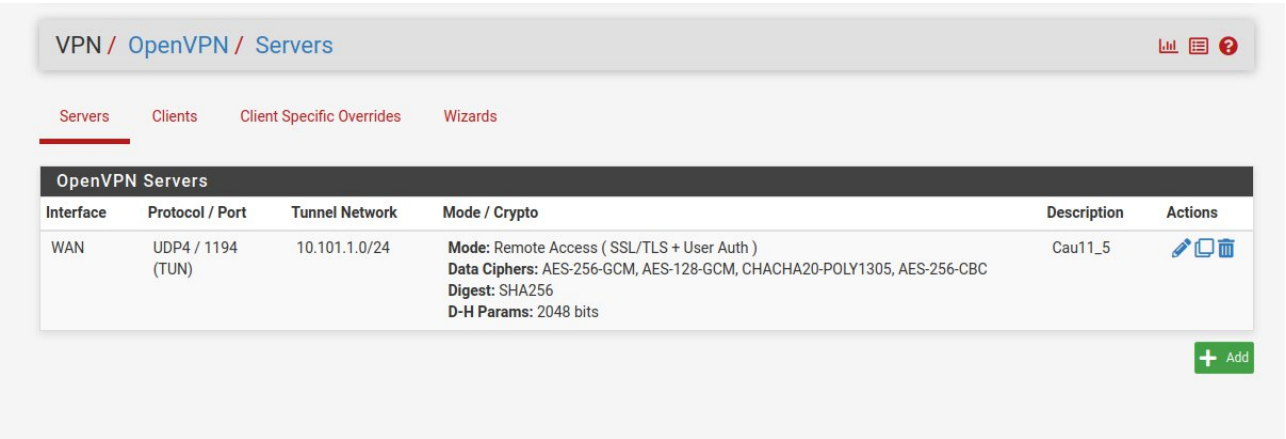

IPv4 Tunnel Network
10.101.1.0/24
This is the virtual network used for private communications between this server and client hosts expressed using CIDR notation (eg. 10.0.8.0/24). The first network address will be assigned to the server virtual interface. The remaining network addresses will be assigned to connecting clients.
Redirect IPv4 Gateway
Force all client generated traffic through the tunnel.
IPv4 Local Network
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.
Concurrent Connections
10
Specify the maximum number of clients allowed to concurrently connect to this server.
Allow Compression
Refuse any non-stub compression (Most secure)
Allow compression to be used with this VPN instance, which is potentially insecure.
Compression
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.
Type-of-Service
Set the TOS IP header value of tunnel packets to match the encapsulated packet's TOS value.
Inter-Client Communication
Allow communication between clients connected to this server.
Duplicate Connections
Allow multiple concurrent connections from clients using the same Common Name.
NOTE: This is not generally recommended, but may be needed for some scenarios.


Client Settings
Dynamic IP
Allow connected clients to retain their connections if their IP address changes.
Topology
Subnet -- One IP address per client in a common subnet
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
Provide a default domain name to clients.
DNS Server 1
DNS server IP to provide to connecting clients.
DNS Server 2
DNS server IP to provide to connecting clients.
DNS Server 3
DNS server IP to provide to connecting clients.
DNS Server 4
DNS server IP to provide to connecting clients.
NTP Server
Network Time Protocol server to provide to connecting clients.
NTP Server 2
Network Time Protocol server to provide to connecting clients.
NetBIOS Options
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
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
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
A Windows Internet Name Service (WINS) server IP to provide to connecting clients. Not desirable in most all modern networks.
WINS Server 2
A Windows Internet Name Service (WINS) server IP to provide to connecting clients. Not desirable in most all modern networks.
Next

Tick 2 rules:

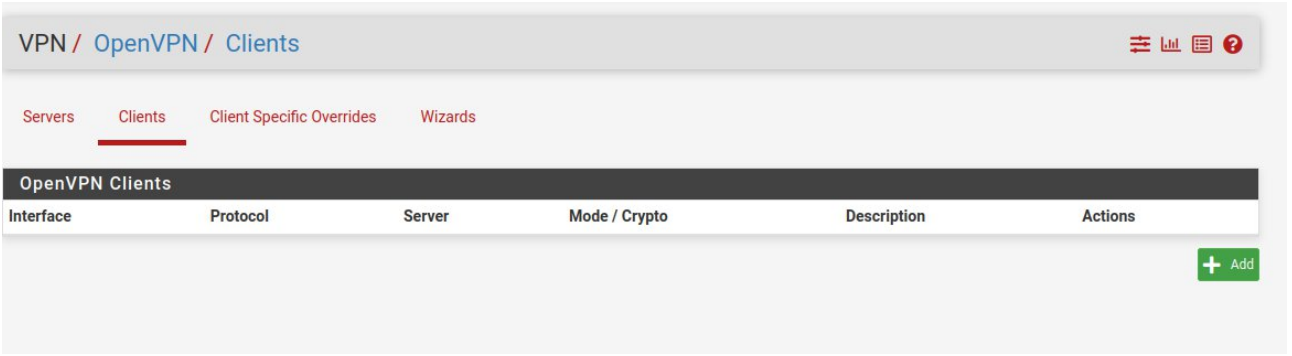




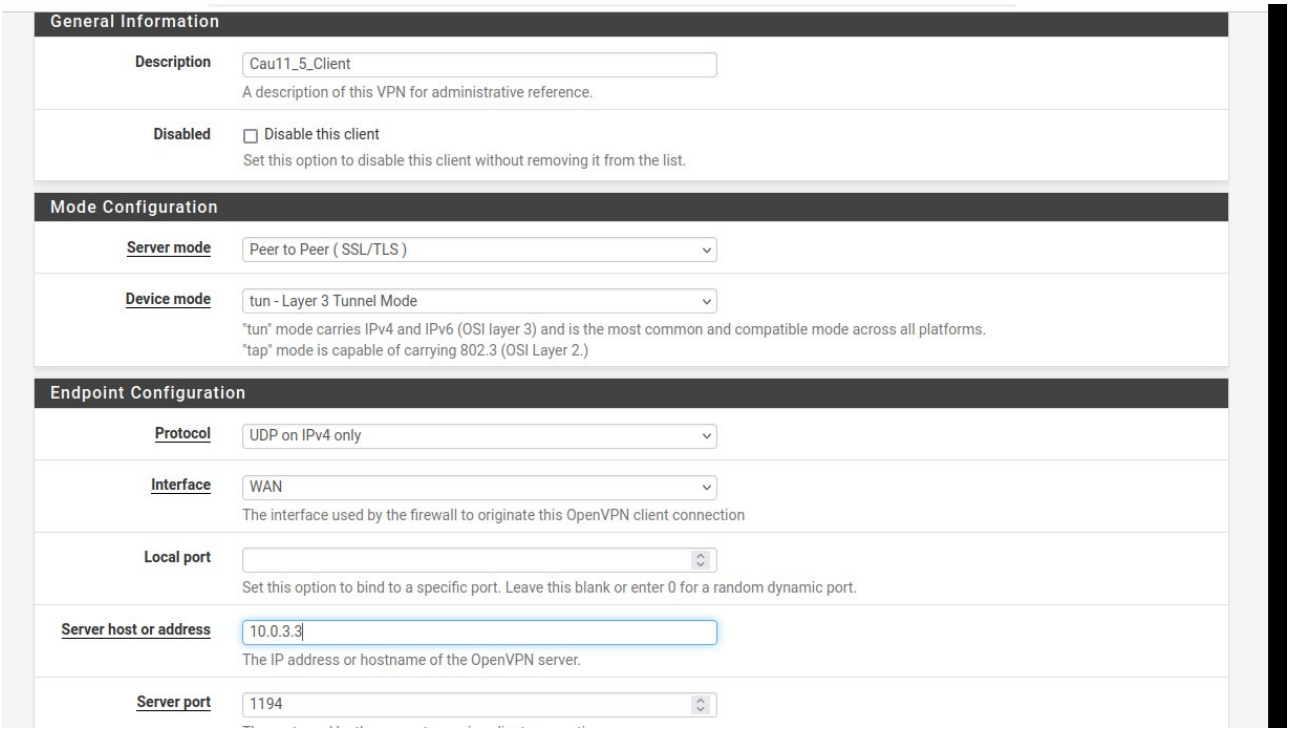


Bước 3: Cấu hình quyền truy cập của client

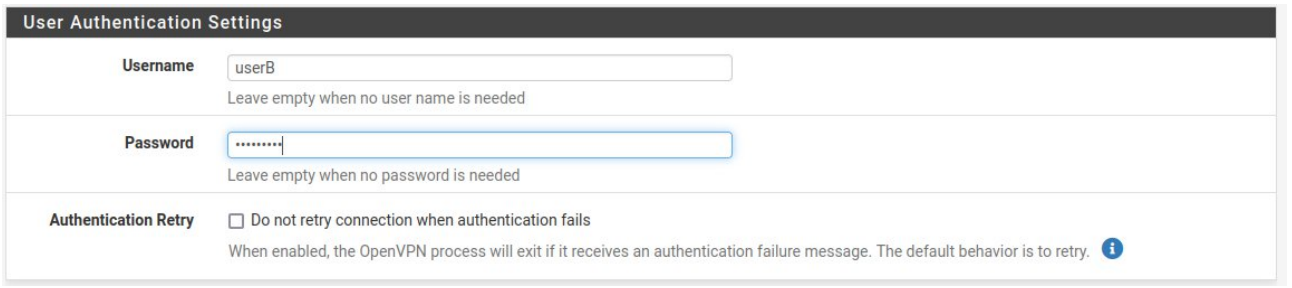
Giờ đến client:



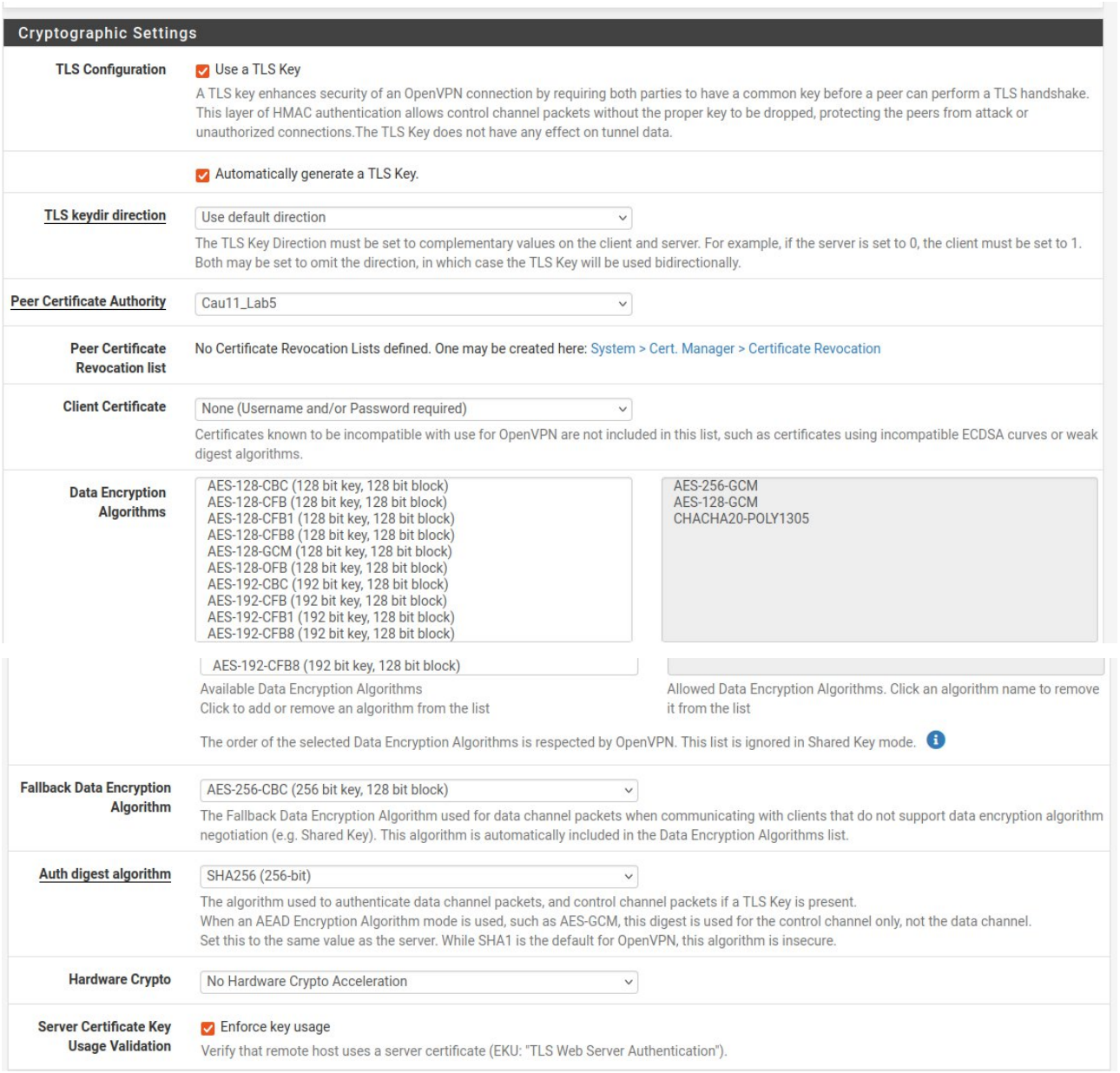
Địa chỉ server là địa chỉ NAT của pfsense:



Đặt tên là userB và mật khẩu là userB@123

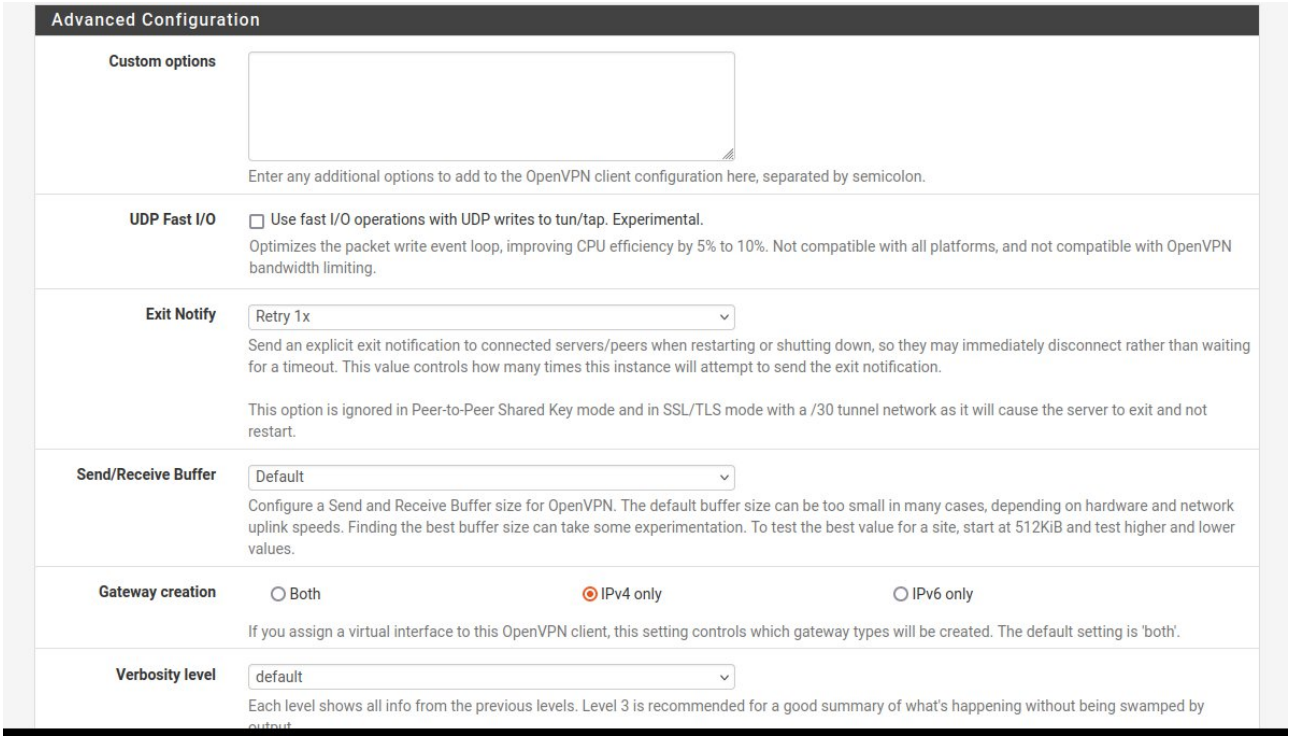


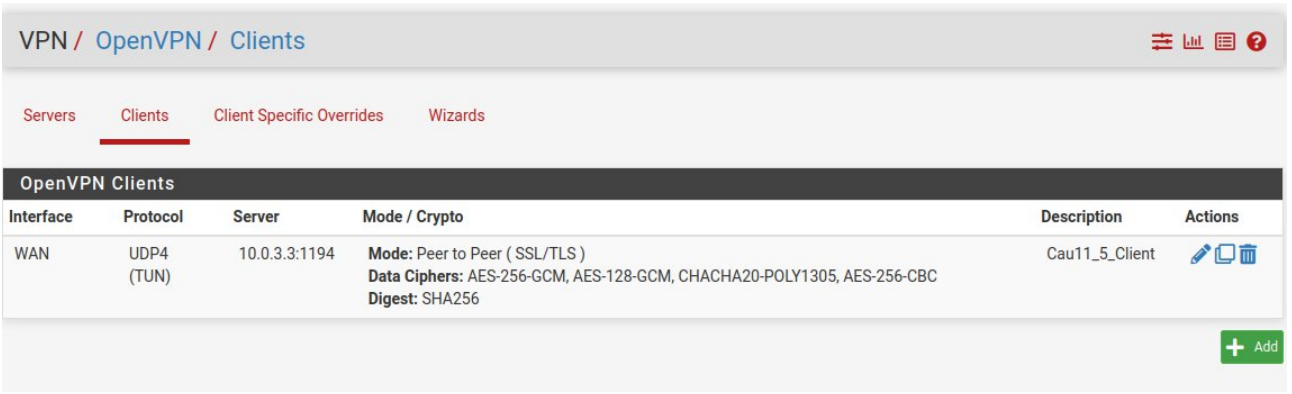
Phần tiếp theo giữ yên



Giữ yên mặc định những cấu hình sau đó.

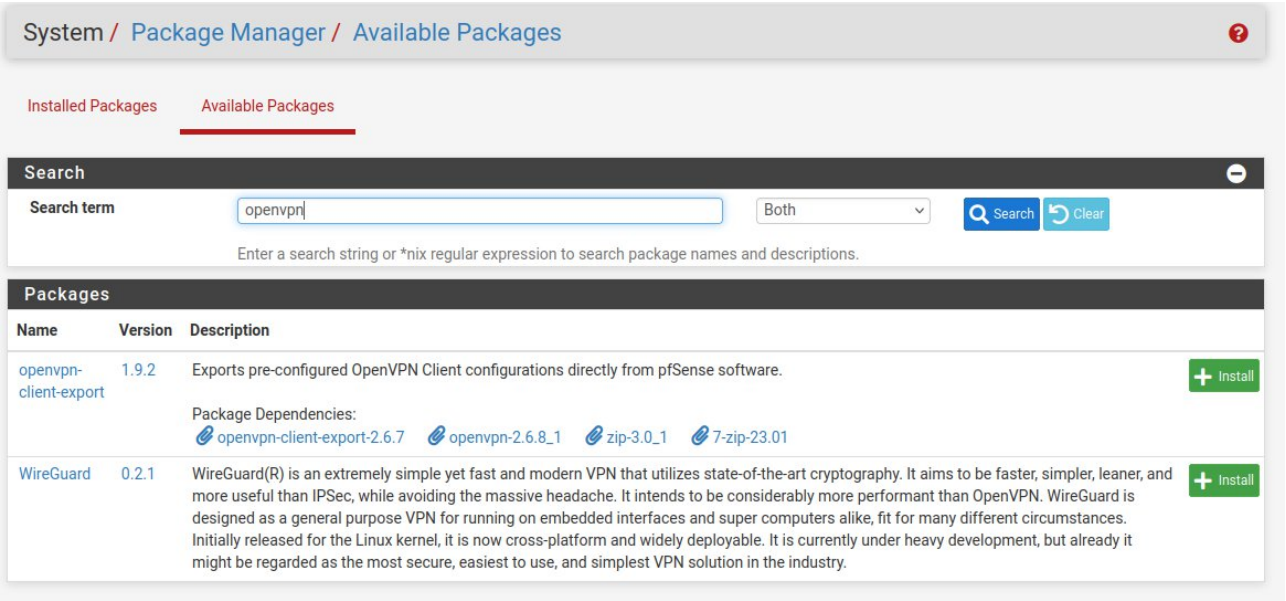
Đến Advanced Configuration chọn IPv4:



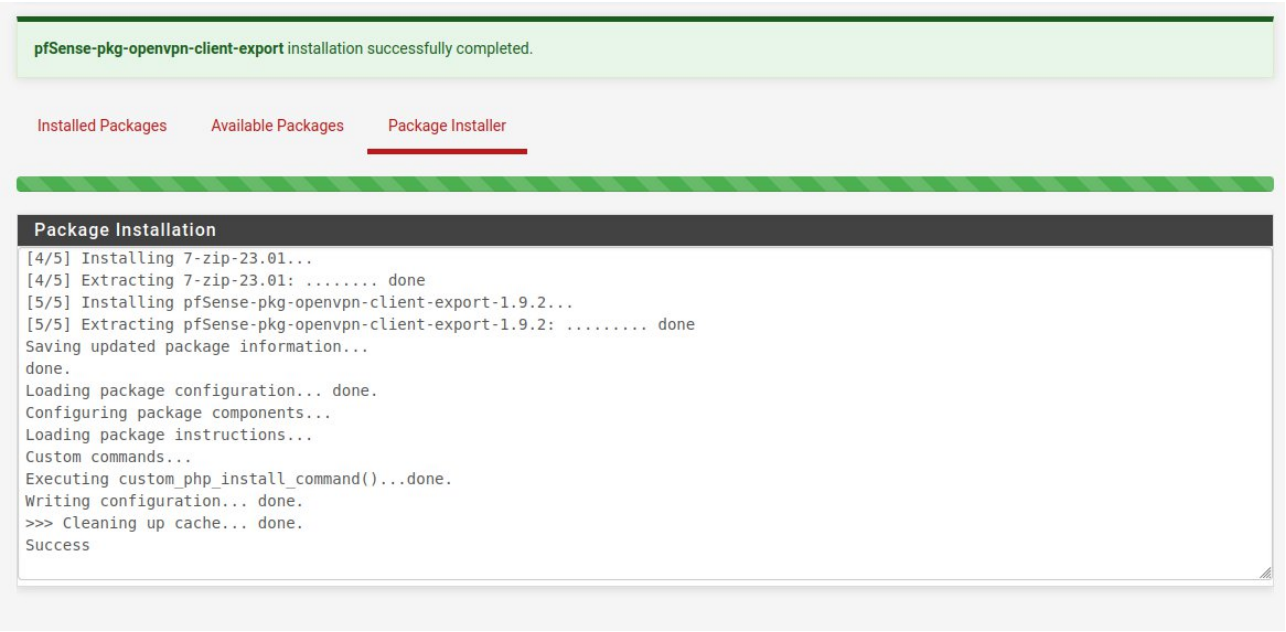


Ta cài tiếp gói OpenVPN Client Export để xuất các file cấu hình client kết nối tới máy chủ OpenVPN

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



Nhấn install openvpn-clientexport và chọn confirm

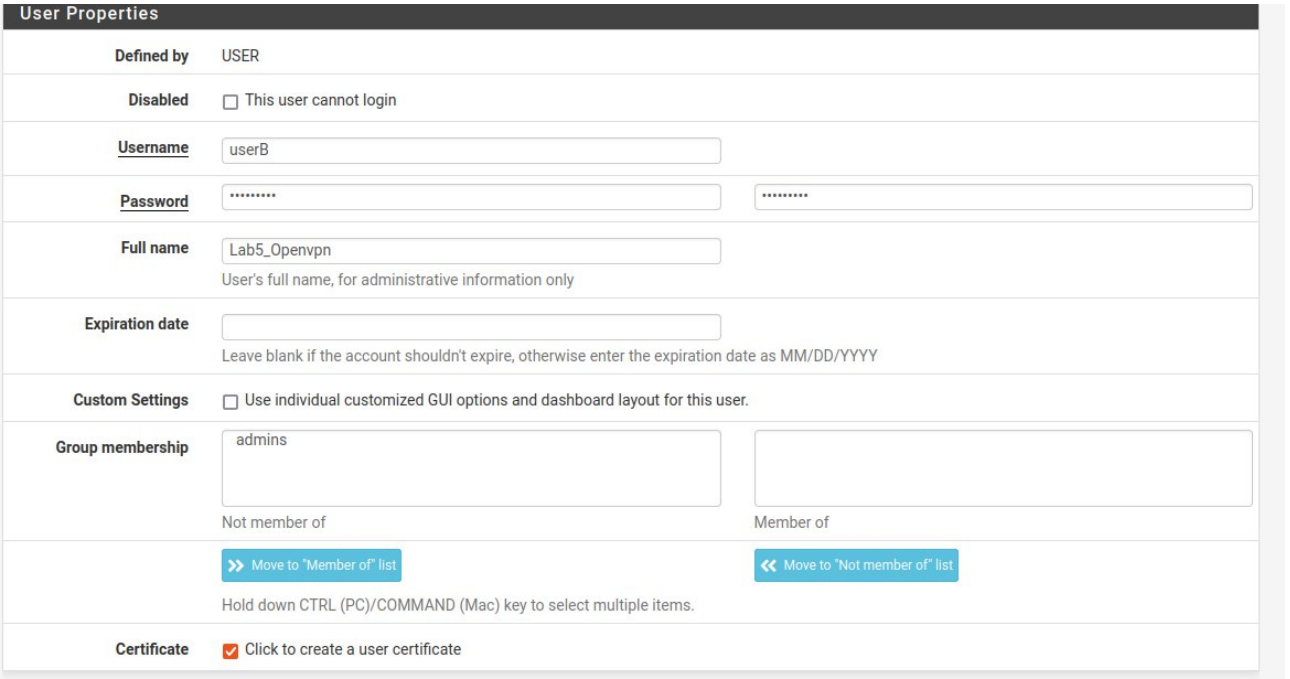


Tạo user VPN

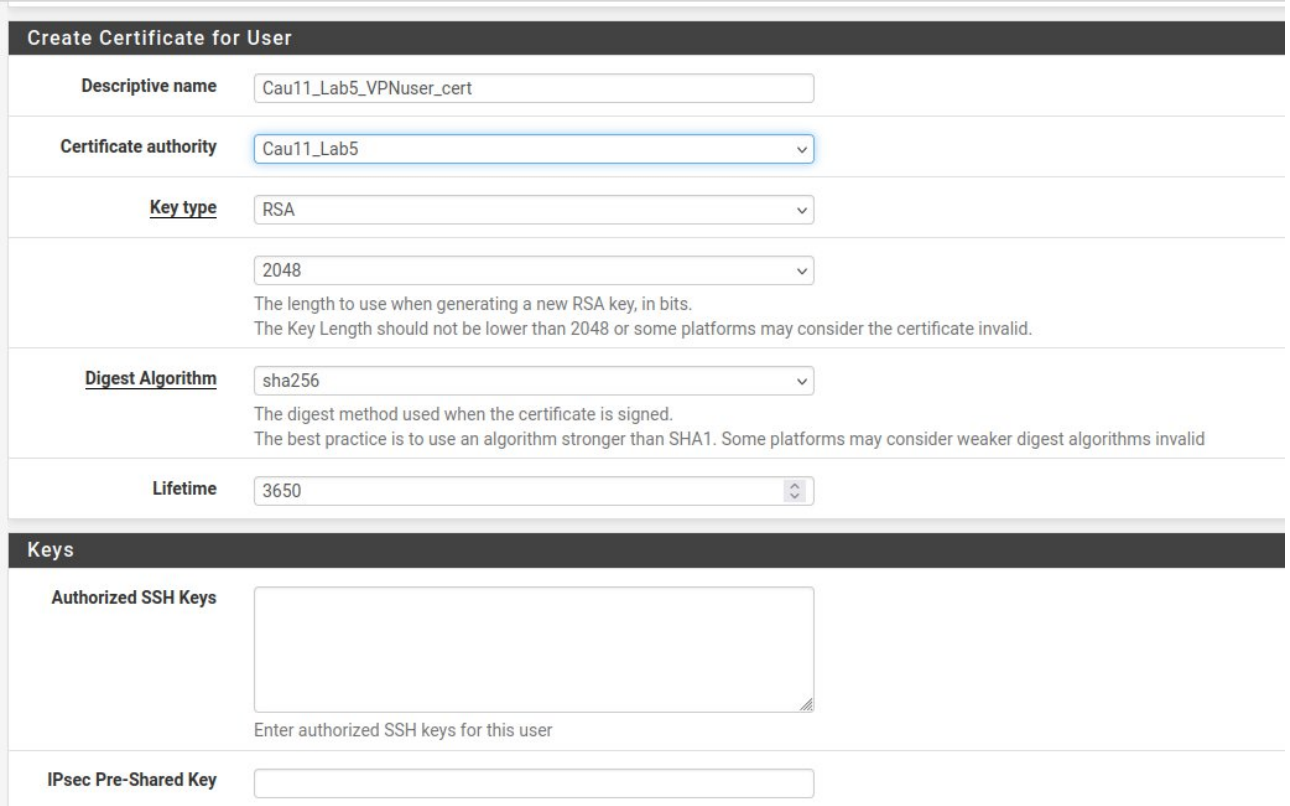
Tài khoản sẽ là tài khoản ta tạo ở phía trên khi cấu hình OpenVPN

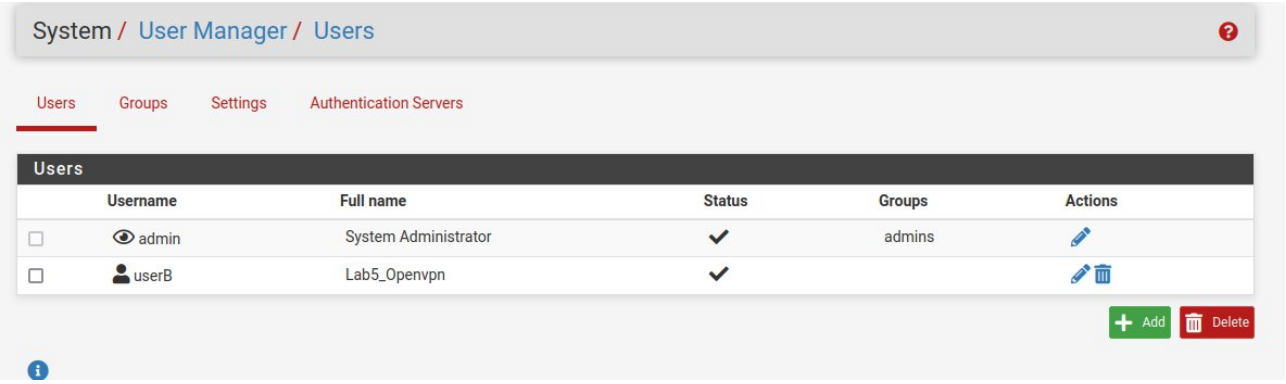
Vào System -> User Manager -> Users -> Edit

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

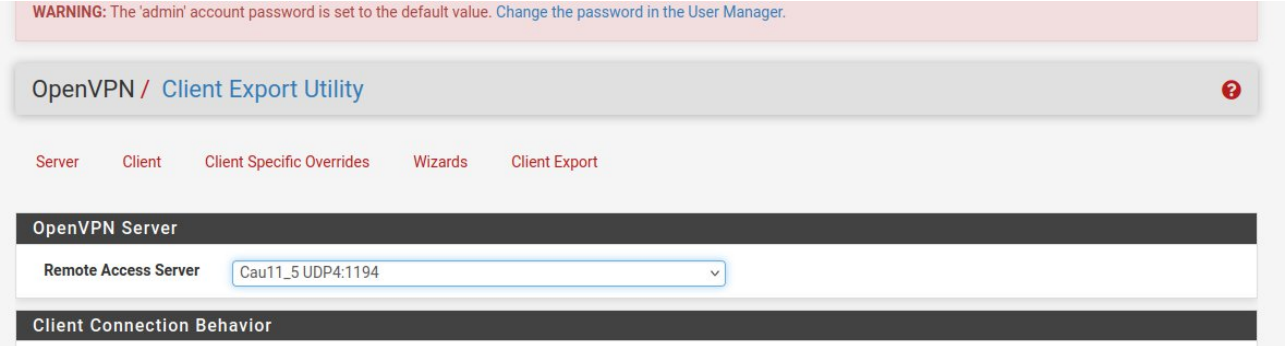


Đặt tên cho cert

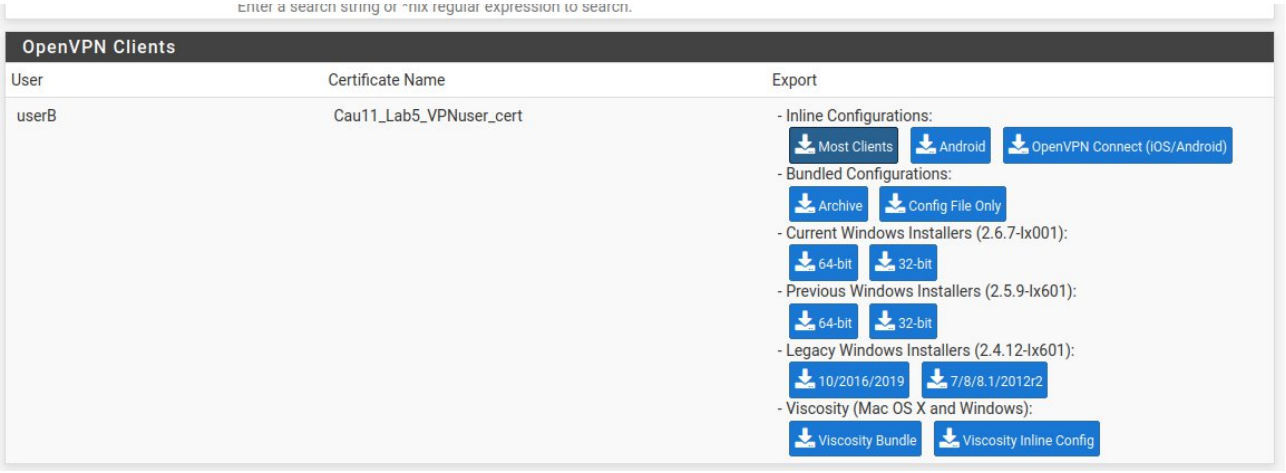




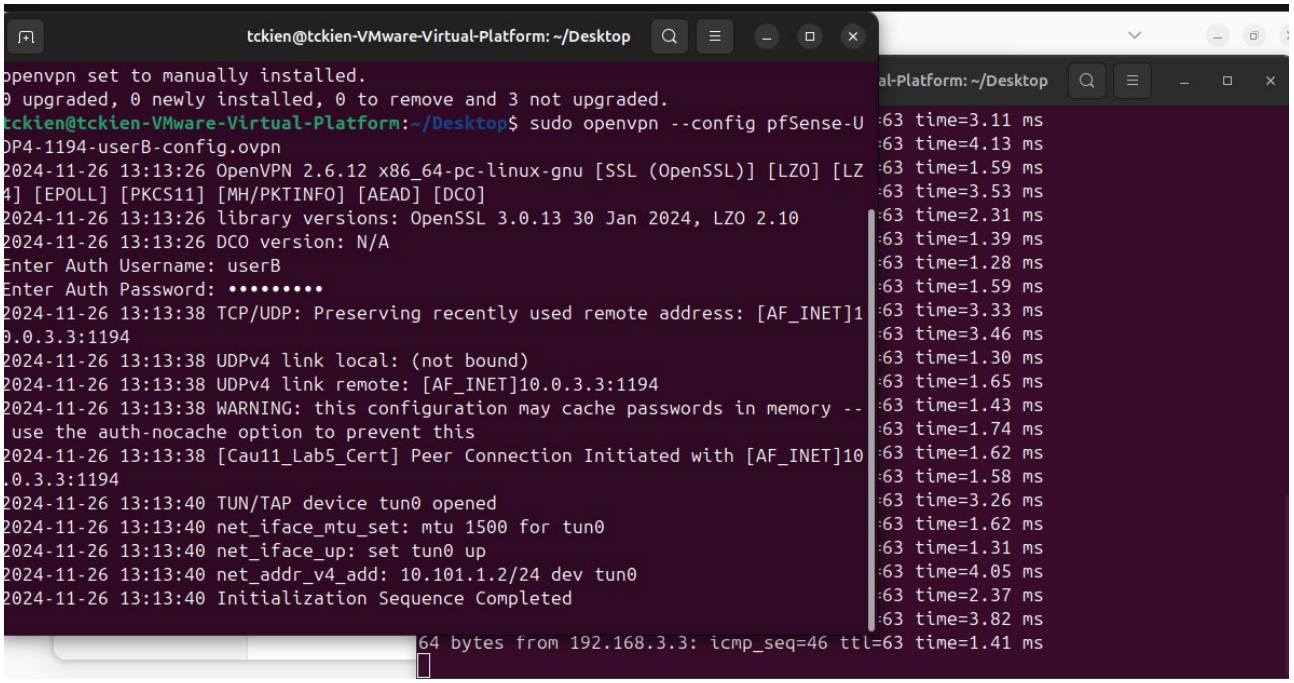
Tiếp theo, điều hướng đến Client Export dưới menu OpenVPN để tải bộ cấu hình Client Configuration.



Chọn most client:



Chạy tệp đó và ping đến máy A:



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