

BAN CƠ YẾU CHÍNH PHỦ
HỌC VIỆN KỸ THUẬT MẬT MÃ



MODULE THỰC HÀNH
AN TOÀN MẠNG MÁY TÍNH

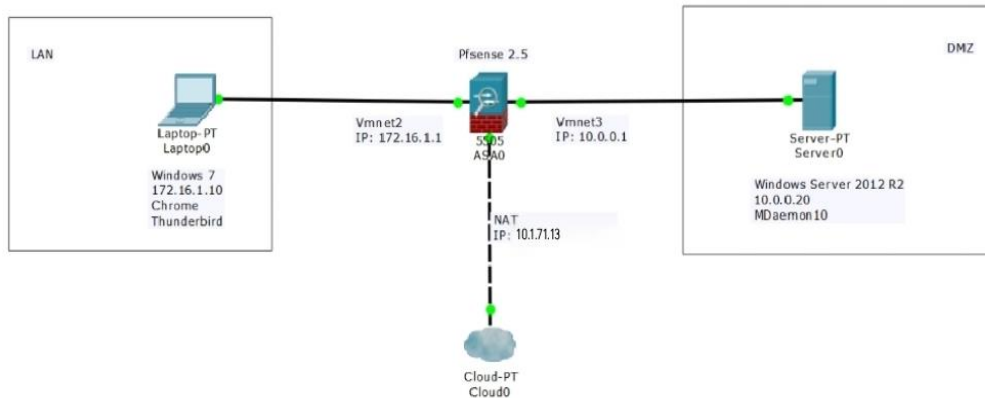
BÀI THỰC HÀNH SỐ 02
Triển khai tường lửa PfSense

Sinh viên thực hiện:

Nguyễn Đức Mạnh - AT170432

1. CHUẨN BỊ

Vẽ lại mô hình mạng chuẩn bị thực hành (bao gồm các kết nối, địa chỉ IP, hệ điều hành, tên máy, ứng dụng được cài đặt) và dán vào bên dưới.



2. THỰC HÀNH

Phần 1. Cài đặt tường lửa PfSense

Chụp ảnh các địa chỉ IP được gán cho các giao diện của tường lửa và dán vào bên dưới.

```
rom: 172.16.1.20

Message from syslogd@pfSense at May 26 05:57:20 ...
php-fpm[3351]: /index.php: Successful login for user 'admin' from: 172.16.1.20
ocal Database)

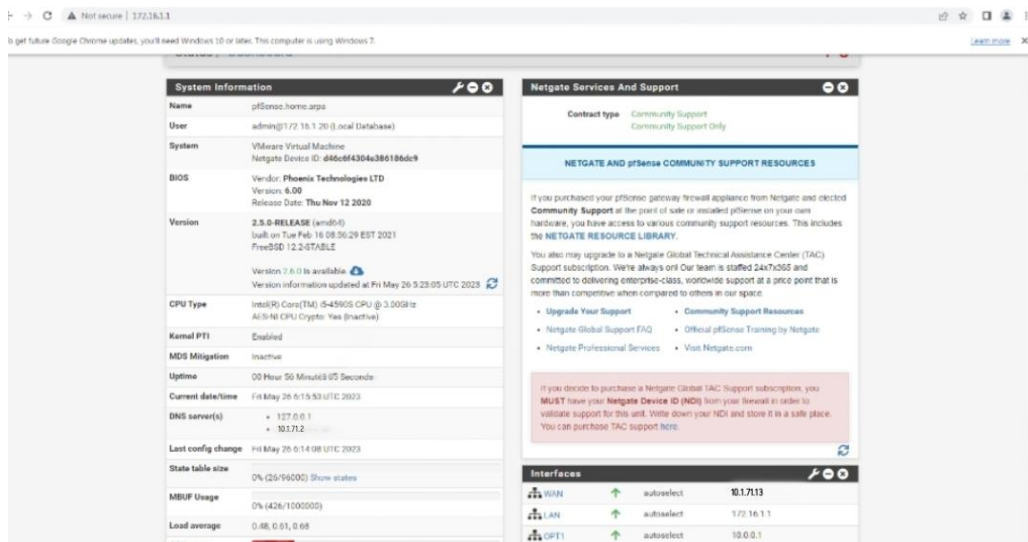
VMware Virtual Machine - Netgate Device ID: d46c6f4304e386186dc9

*** Welcome to pfSense 2.5.0-RELEASE (amd64) on pfSense ***

WAN (wan)      -> le0      -> v4/DHCP4: 192.168.217.130/24
LAN (lan)      -> le1      -> v4: 172.16.1.1/24
OPT1 (opt1)    -> le2      -> v4: 10.0.0.1/24

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
```

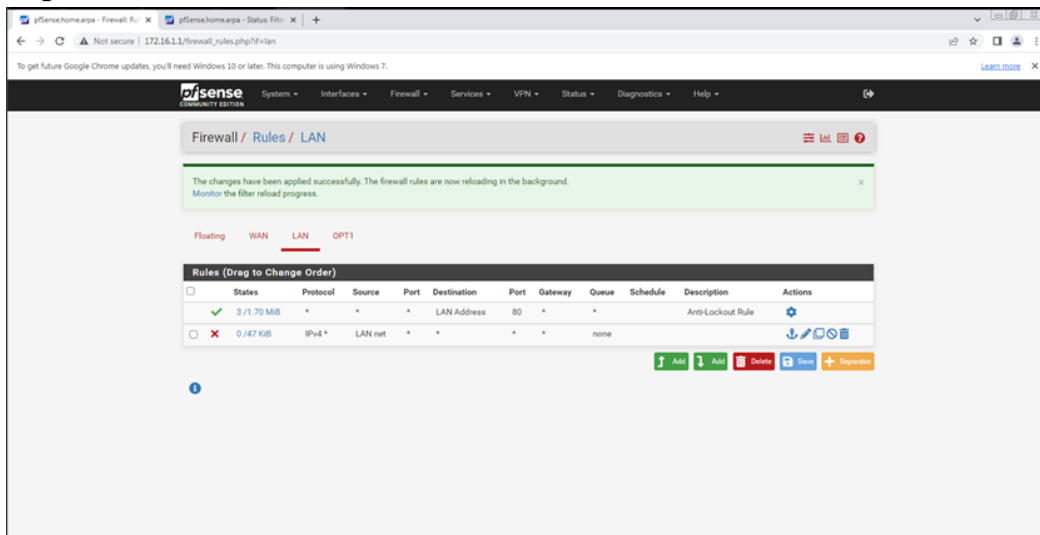
Chụp ảnh kết quả đăng nhập thành công vào tường lửa PfSense và dán vào bên dưới.



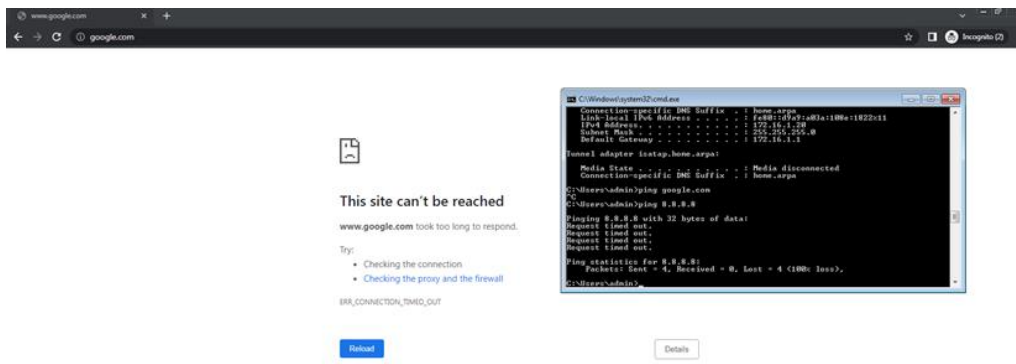
Phần 2. Quản trị tường lửa PfSense

2.1. Quản trị phân vùng mạng LAN

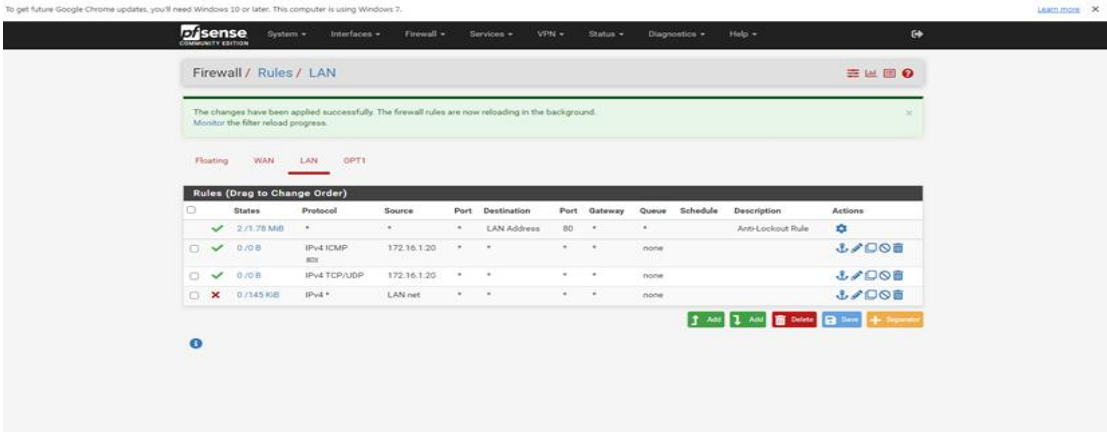
Thiết lập luật để chặn toàn bộ máy trong mạng LAN truy cập ra Internet và chụp ảnh, dán vào bên dưới.



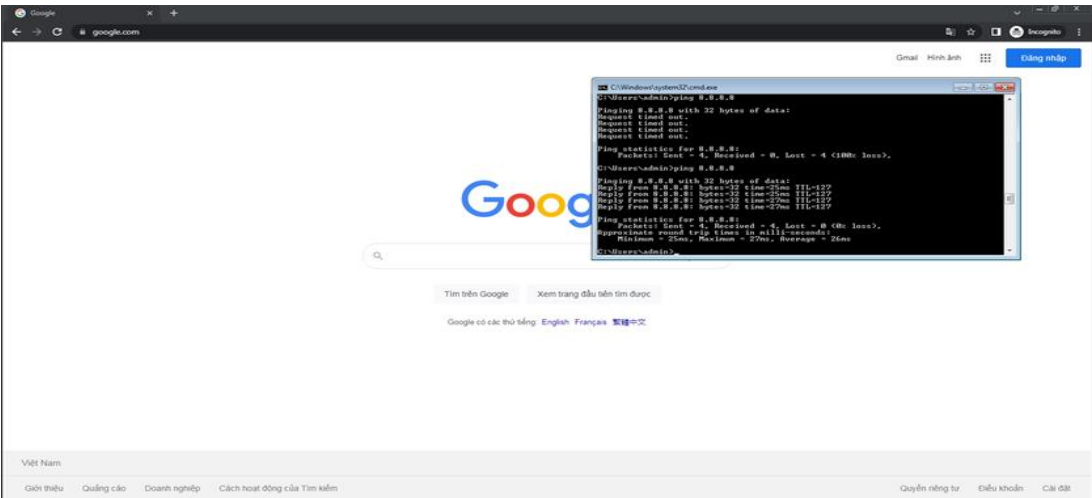
Thử nghiệm đứng từ 1 máy trong mạng LAN truy cập ra Internet và chụp ảnh, dán vào bên dưới.



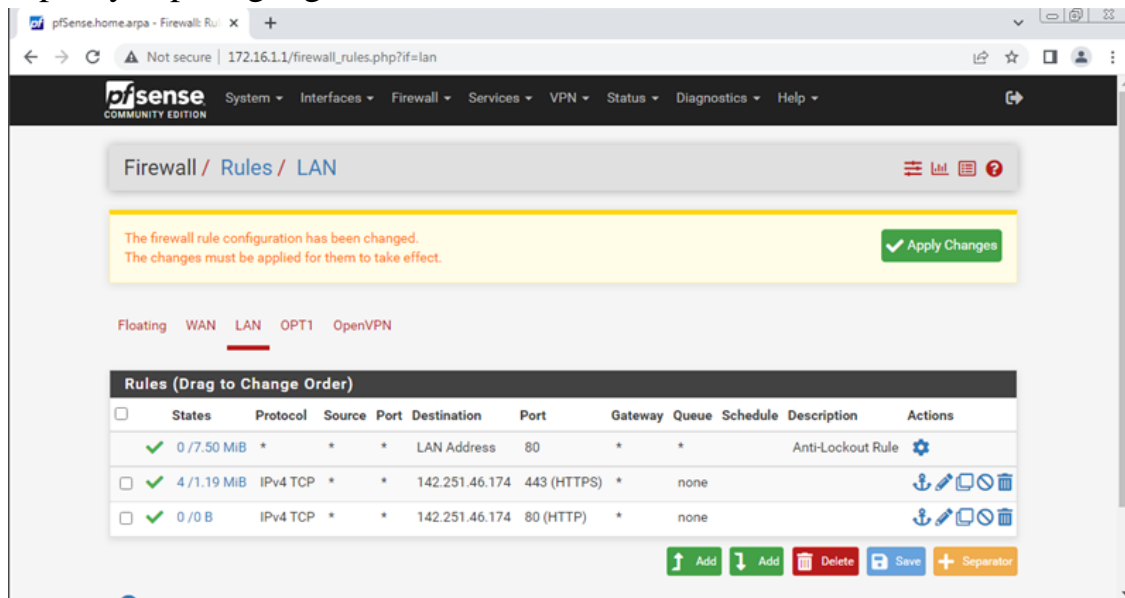
Thiết lập luật số 1 máy trong mạng LAN có thể truy cập ra Internet và chụp ảnh, dán vào bên dưới.



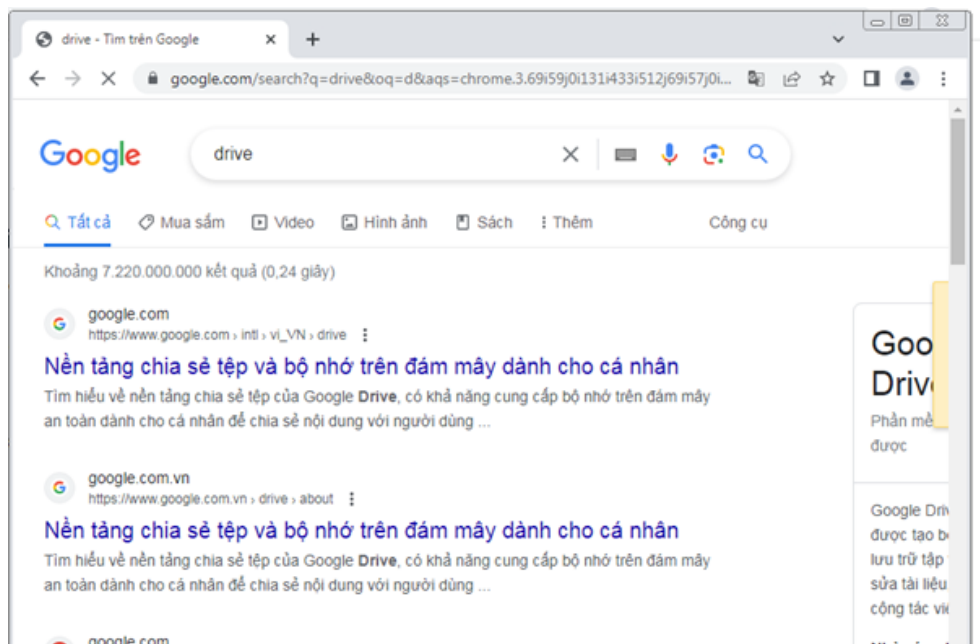
Thử nghiệm đứng từ máy đó truy cập ra Internet và chụp ảnh, dán vào bên dưới.



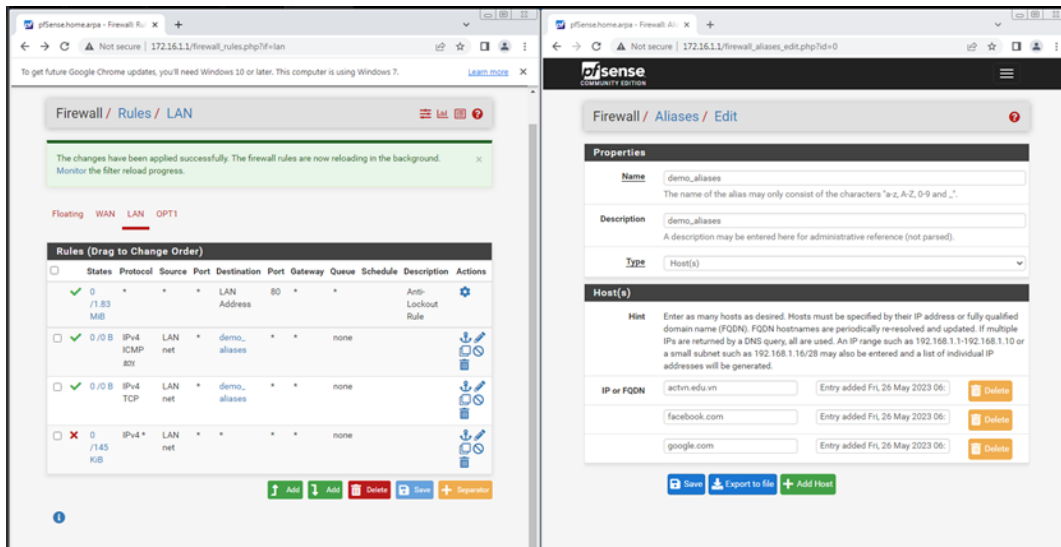
Thiết lập luật để cho phép các máy trong mạng LAN truy cập được tới 1 địa chỉ bên ngoài Internet (địa chỉ tùy sinh viên thiết lập) và chụp ảnh, dán vào bên dưới. Cho phép truy cập tới google.com



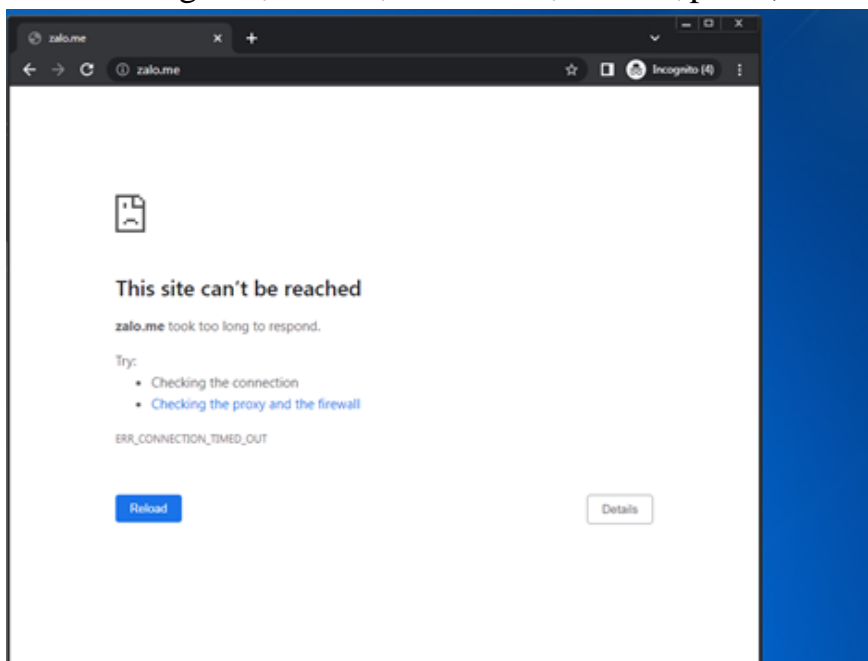
Thử nghiệm đứng từ 1 máy trong mạng LAN truy tới liên kết ở trên và chụp ảnh, dán vào bên dưới.



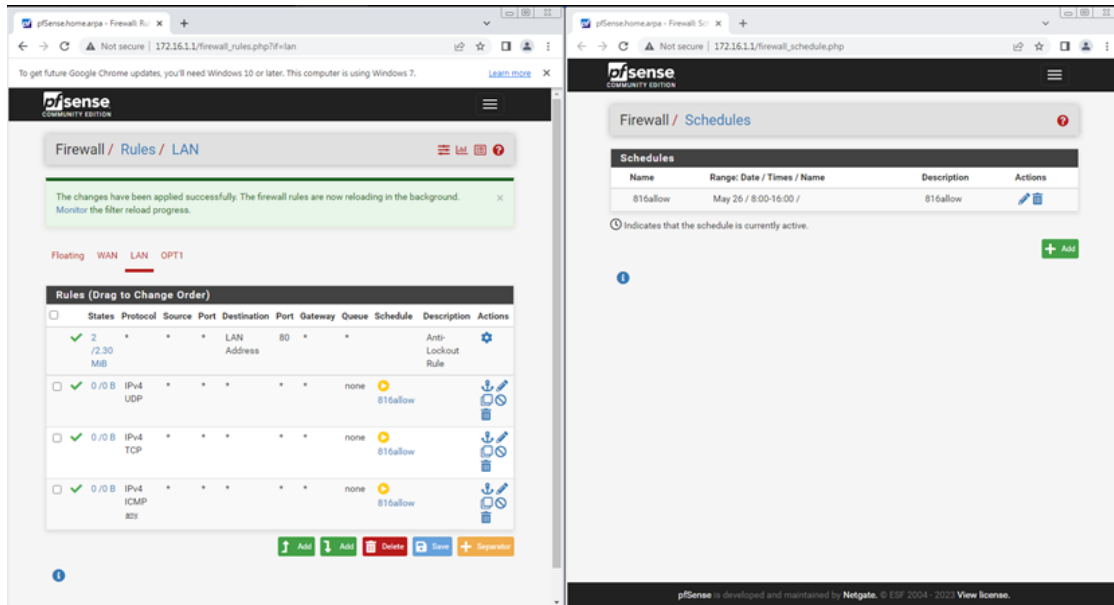
Thiết lập luật để chặn các máy trong mạng LAN truy cập được tới 3 địa chỉ bên ngoài Internet theo kiểu chặn aliases (địa chỉ tùy sinh viên thiết lập) và chụp ảnh, dán vào bên dưới.



Thử nghiệm đứng từ 1 máy trong mạng LAN truy tới liên kết ở trên và 1 liên kết khác không thuộc các địa chỉ IP chặn và chụp ảnh, dán vào bên dưới.

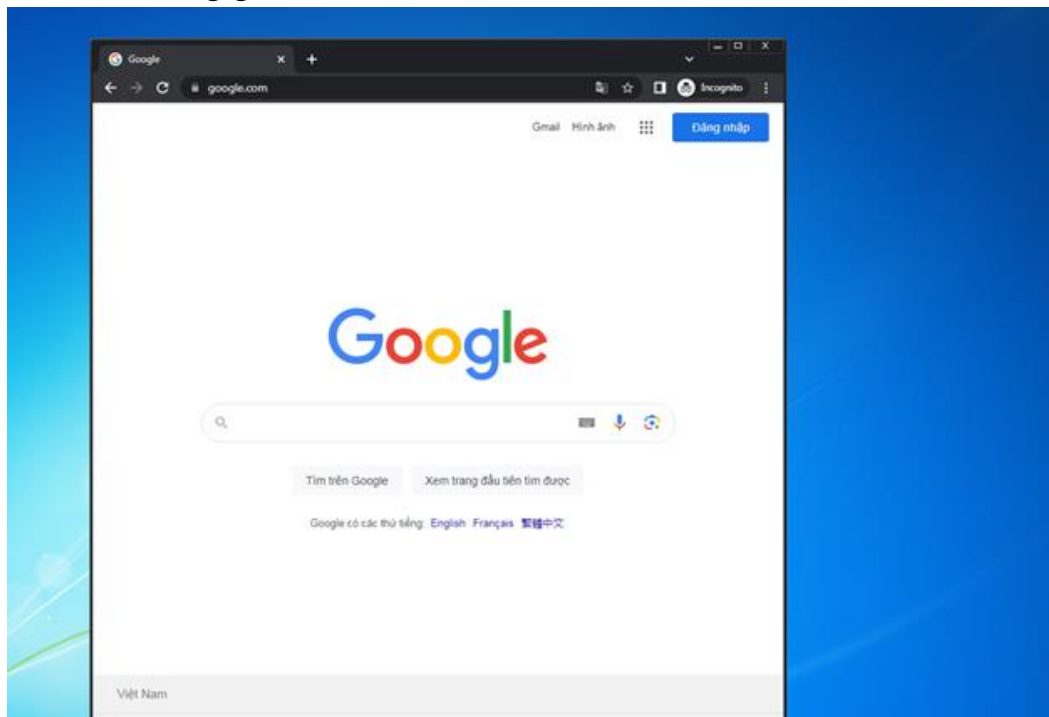


Thiết lập luật để chỉ cho phép các máy trong mạng LAN được truy cập ra bên ngoài Internet từ khoảng thời gian 8h00 đến 16h00 và chụp ảnh, dán vào bên dưới.

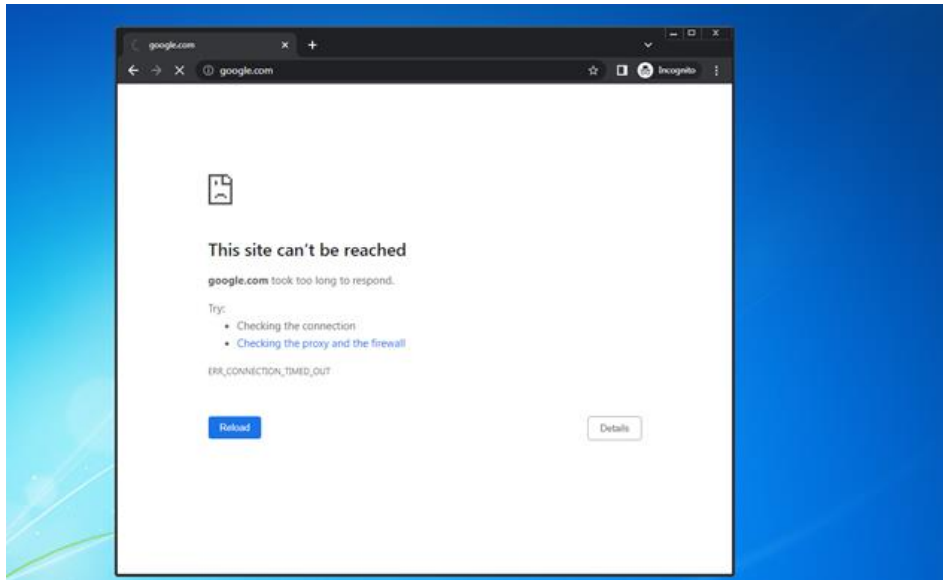


Thử nghiệm đứng từ 1 máy trong mạng LAN truy cập ra ngoài Internet trong khung giờ từ 8h00 đến 16h00 và trong khung giờ từ 17h00 đến 6h00 và chụp ảnh, dán vào bên dưới.

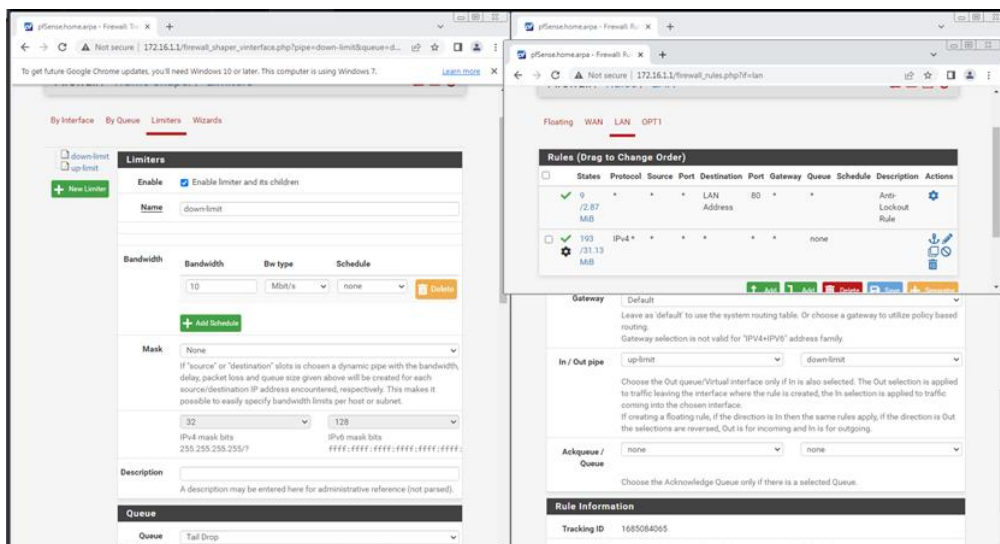
❖ Khung giờ 8h00-16h00



❖ Khung giờ 17h00-6h00



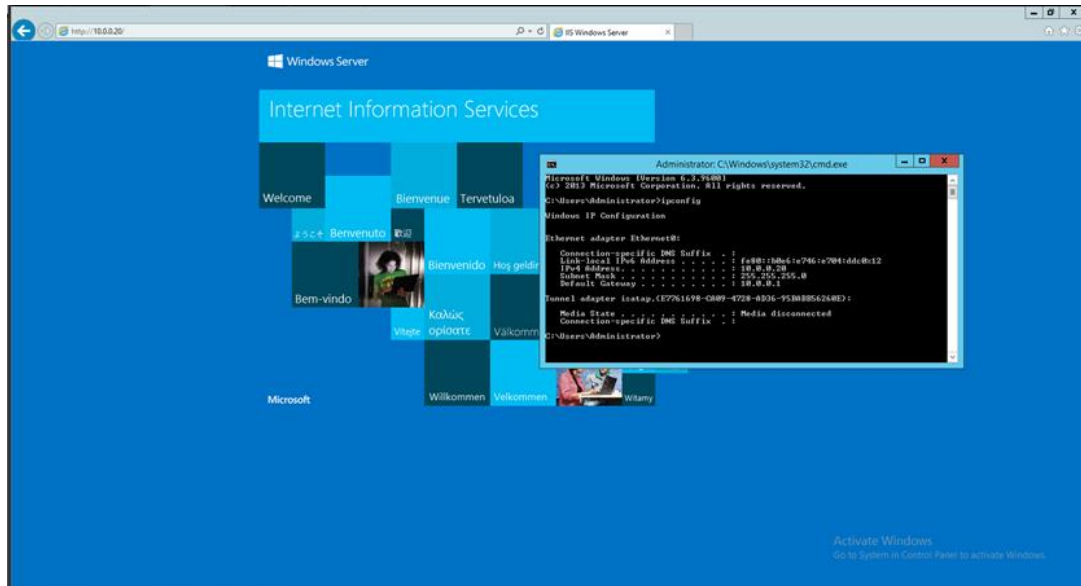
Thiết lập luật để giới hạn tốc độ của các máy trong mạng LAN (tối đa 20Mb tốc độ Upload, Download) và chụp ảnh, dán vào bên dưới.



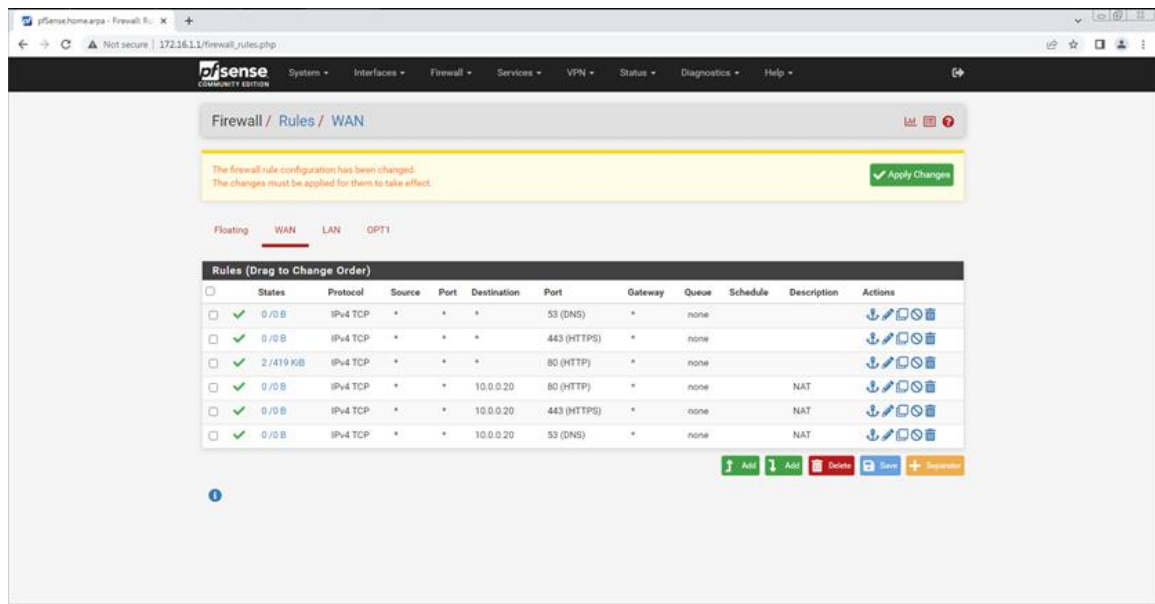
Thử nghiệm đứng từ 1 máy trong mạng LAN sử dụng SpeedTest đo tốc độ và chụp ảnh, dán vào bên dưới.

2.2. Quản trị phân vùng mạng DMZ

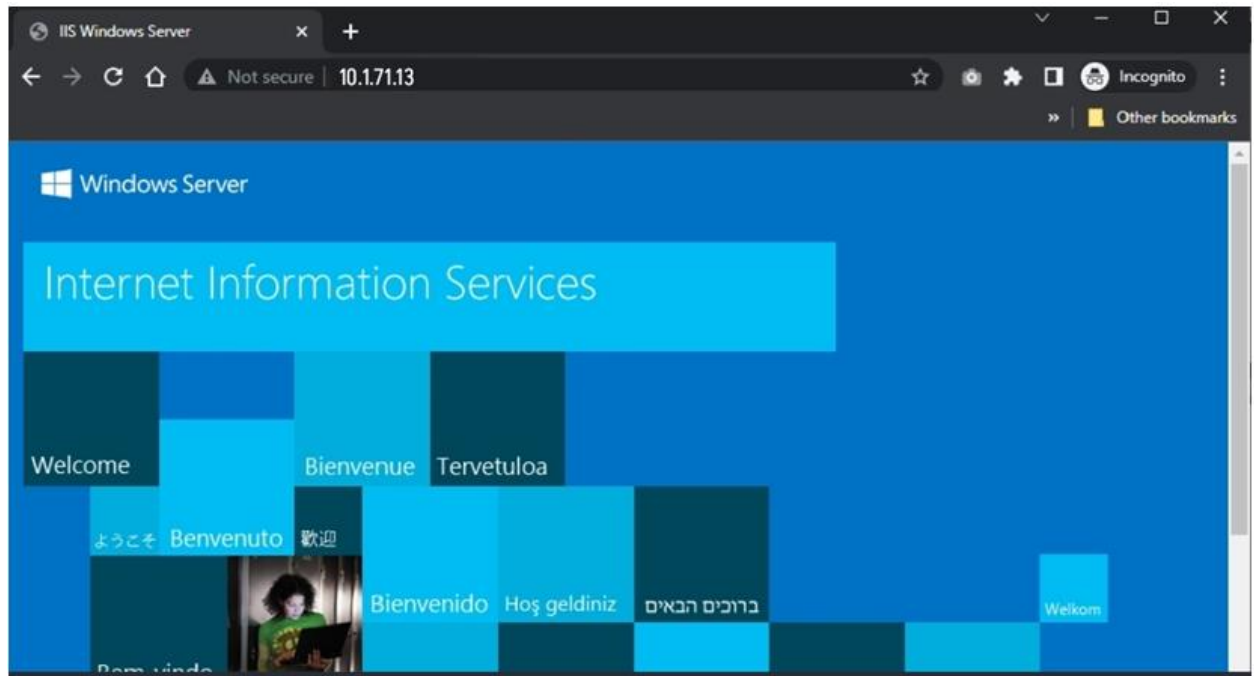
Cài đặt và cấu hình 1 WebServer, sử dụng WebBrowser truy cập tới địa chỉ WebServer và chụp ảnh, dán vào bên dưới.



Thiết lập luật để cho phép từ bên ngoài được truy cập tới WebServer qua giao thức HTTP/HTTPS/DNS thông qua địa chỉ IP Public và chụp ảnh, dán vào bên dưới.

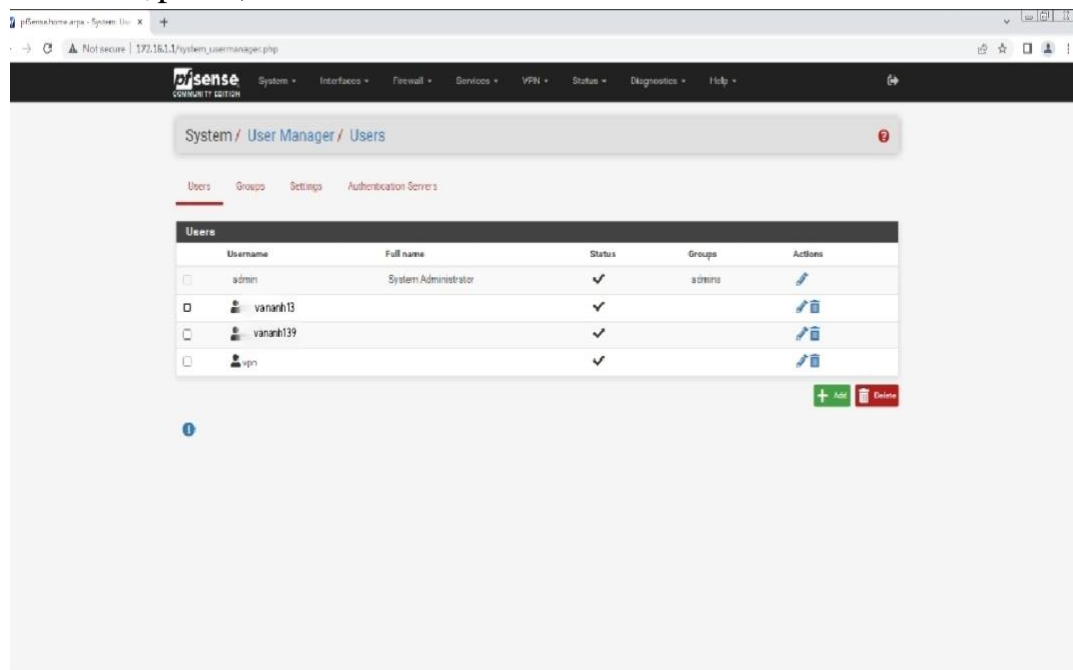


Thử nghiệm đứng từ 1 máy bên ngoài truy cập tới địa chỉ IP Public của WebServer và chụp ảnh, dán vào bên dưới.



2.3. Cấu hình VPN

Cấu hình VPN trên tường lửa PfSense. Tại phần tạo User, tạo 2 user lấy tên sinh viên và chụp ảnh, dán vào bên dưới.



Cấu hình Tunnel Network và Local Network, chụp ảnh và dán vào bên dưới.

generated from the same CA as the server.

Strict User-CN Matching ☐ Enforce match
When authenticating users, enforce a match between the common name of the client certificate and the username given at login.

Tunnel Settings

IPv4 Tunnel Network 10.1.0.0/24
This is the IPv4 virtual network used for private communications between this server and client hosts expressed using CIDR notation (e.g. 10.0.0.0/24). 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 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.

IPv4 Local network(s) 10.0.0.0/24,172.16.10.0/24
IPv4 networks that will be accessible from the remote endpoint. Expressed as a comma-separated list of one or more CIDR ranges. 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.

IPv6 Local network(s)
IPv6 networks that will be accessible from the remote endpoint. Expressed as a comma-separated list of one or more IPv6/PREFIX. 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 5
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.
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, TMLE, 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.

Thiết lập luật cho VPN để cho phép kết nối VPN từ xa qua cổng 1194, chụp ảnh và dán vào bên dưới.

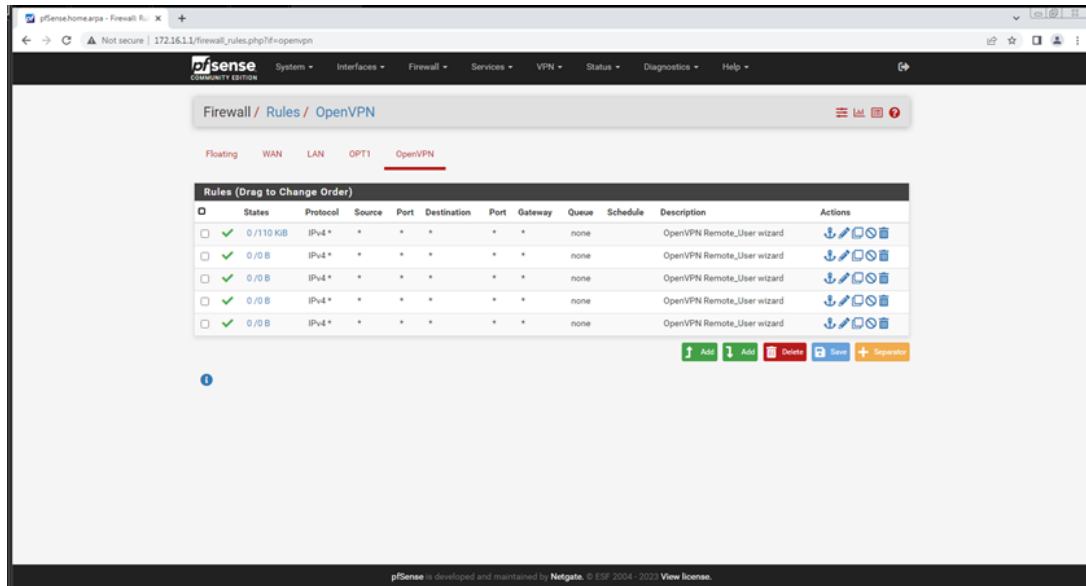
Firewall / Rules / WAN

Rules (Drag to Change Order)

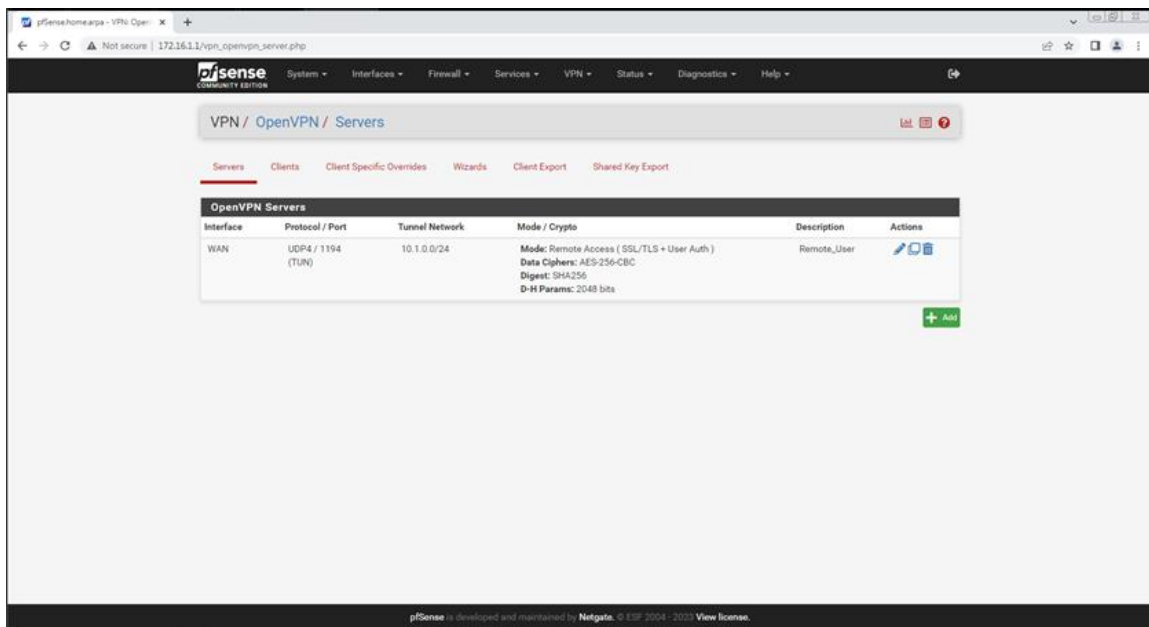
States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	IPv4 *	*	*	*	*	*	none			Add Edit Delete
<input checked="" type="checkbox"/>	IPv4 TCP	*	*	WAN address	1194 (OpenVPN)	*	none			Add Edit Delete
<input checked="" type="checkbox"/>	IPv4 TCP	*	*	*	1194 (OpenVPN)	*	none			Add Edit Delete
<input checked="" type="checkbox"/>	IPv4 UDP	*	*	WAN address	1194 (OpenVPN)	*	none		OpenVPN Remote_User wizard	Add Edit Delete
<input checked="" type="checkbox"/>	IPv4 UDP	*	*	WAN address	1194 (OpenVPN)	*	none		OpenVPN Remote_User wizard	Add Edit Delete

[Add](#) [Add](#) [Delete](#) [Save](#) [Generate](#)

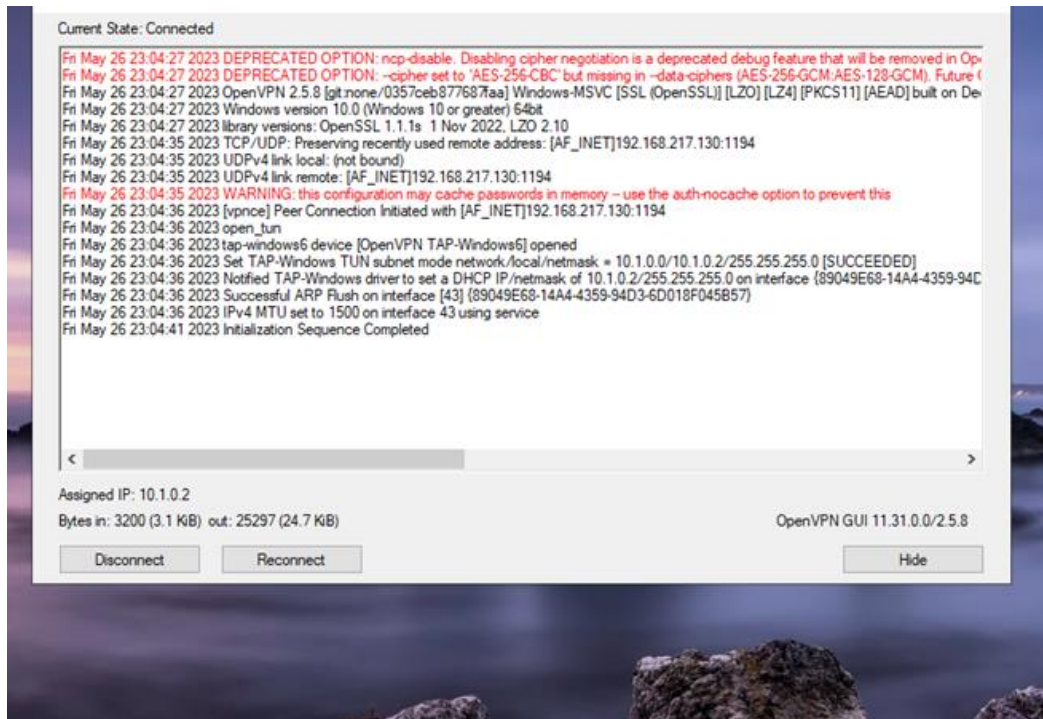
pSense is developed and maintained by Netgate. © 1997-2024. 2021 View license.



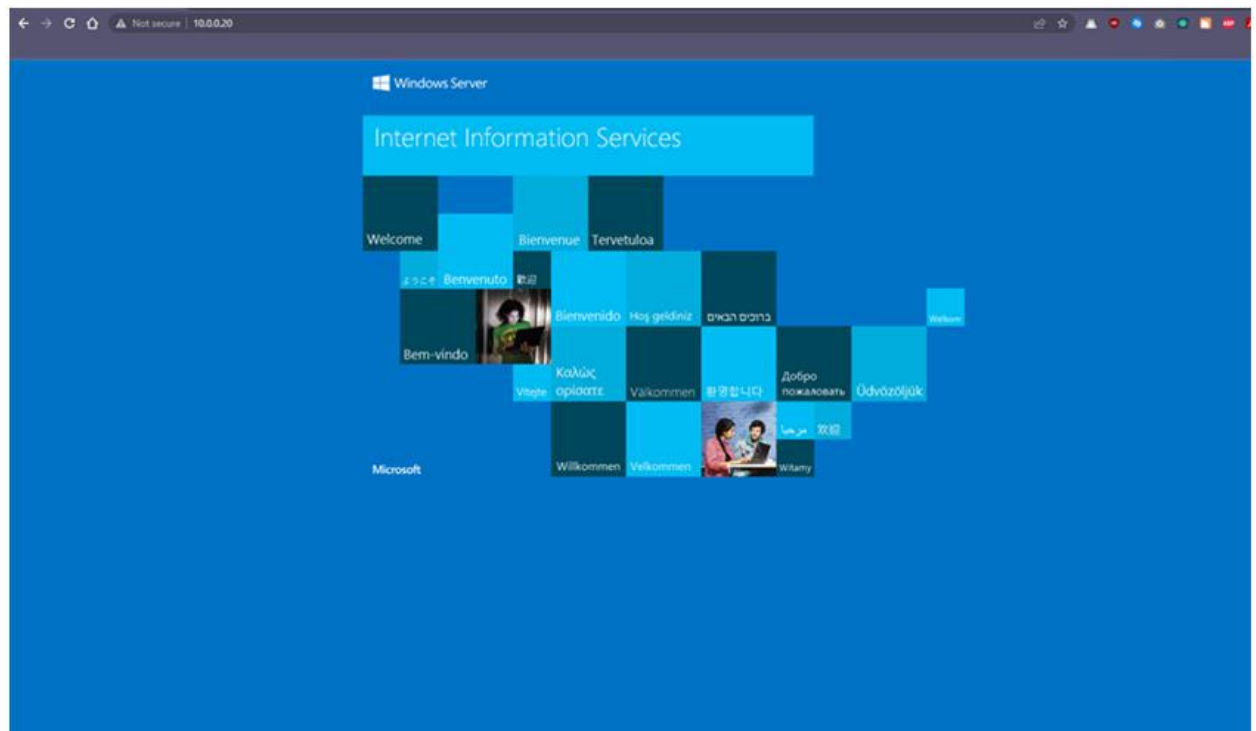
Tại phần VPN/OpenVPN/Servers, chụp ảnh các server VPN và dán vào bên dưới.



Sử dụng 1 máy Windows, cài đặt VPN Client và kết nối tới VPN Server, sau đó chụp ảnh, dán vào bên dưới.

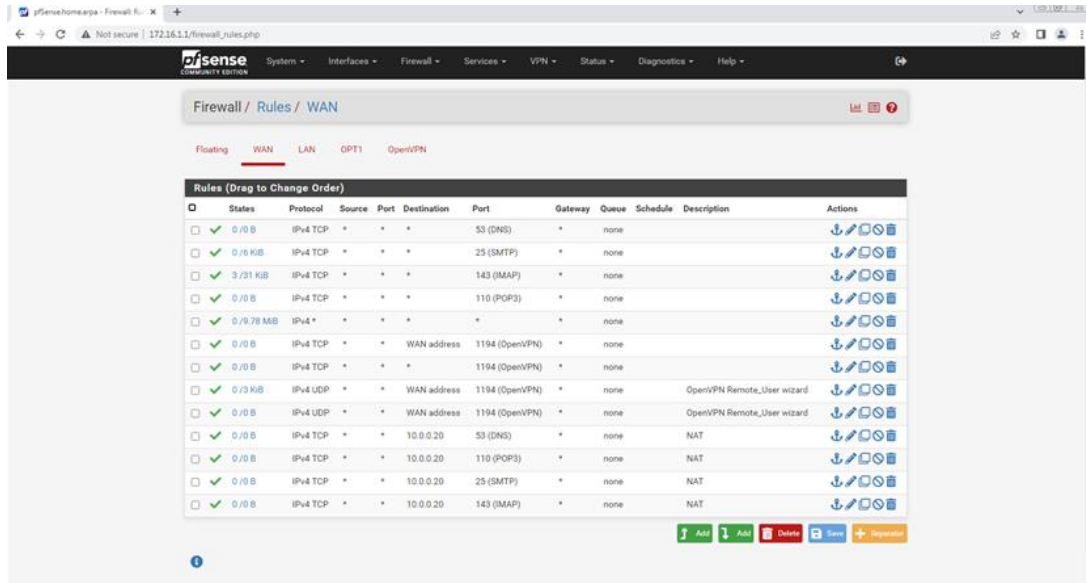


Thử nghiệm đứng từ 1 máy bên ngoài truy cập tới địa chỉ IP Public của WebServer và chụp ảnh, dán vào bên dưới.

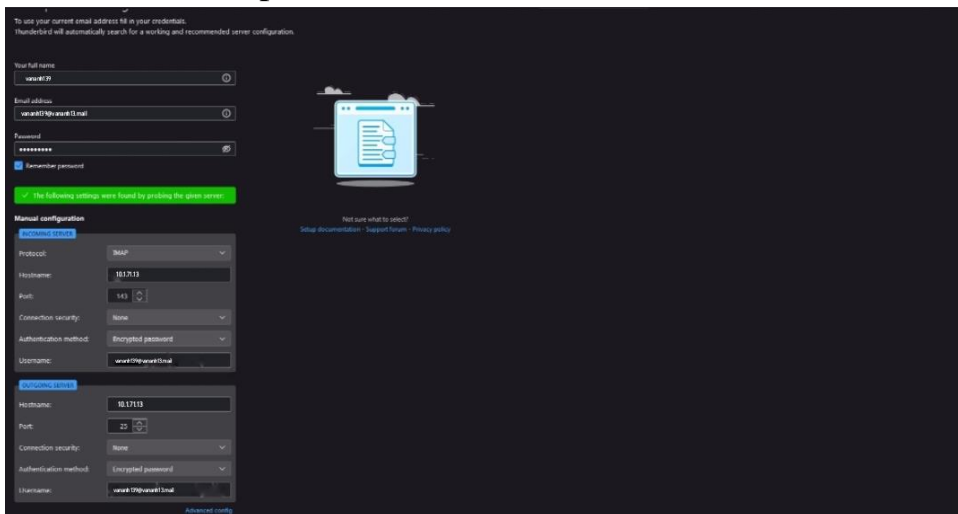


Phần 3. Sinh viên tự thực hành

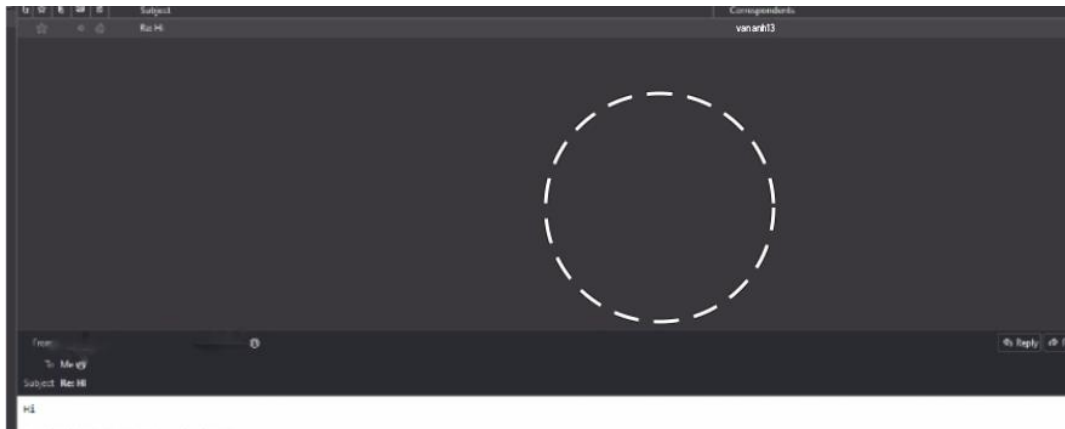
Cấu hình luật trên tường lửa cho phép từ bên ngoài truy cập được tới MailServer qua giao thức SMTP/POP3/IMAP/DNS thông qua địa chỉ IP Public và chụp ảnh, dán vào bên dưới.



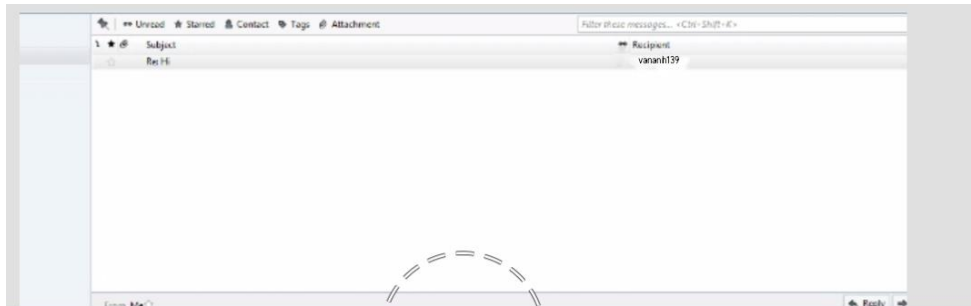
Đứng từ 1 máy bên ngoài, sử dụng Thunderbird để cấu hình quản lý 1 tài khoản email vừa tạo ra và chụp ảnh, dán vào bên dưới.



Đứng từ máy bên ngoài, sử dụng Thunderbird để gửi email tới tài khoản email thứ 2 và chụp ảnh, dán vào bên dưới.



Đứng từ máy bên trong, sử dụng Thunderbird để nhận email gửi từ máy bên ngoài, đồng thời gửi mail reply lại và chụp ảnh, dán vào bên dưới.



Đứng từ máy bên ngoài, sử dụng Thunderbird để kiểm tra email vừa gửi từ tài khoản thứ 2 của máy bên trong và chụp ảnh, dán vào bên dưới.

