

CHƯƠNG 3: TRIỂN KHAI TƯỜNG LỬA BẰNG PFSENSE

3.1. Chuẩn bị

- 01 máy ảo hệ điều hành Windows 10:
 - Sử dụng card mạng VmNet2 (Host-only).
 - Địa chỉ IP: 192.168.10.150
 - Default gateway: 192.168.10.1
- 01 máy ảo hệ điều hành Ubuntu (đã cài Webserver DVWA):
 - Sử dụng card mạng VmNet3 (Host-only).
 - Địa chỉ IP: 192.168.20.100
 - Default gateway: 192.168.20.1
- 01 máy ảo hệ điều hành Windows server 2012
 - Sử dụng card mạng VmNet2 (Host-only).
 - Địa chỉ IP: 192.168.10.100
 - Default gateway: 192.168.10.1
- 01 máy ảo hệ điều hành Kali Linux:
 - Sử dụng card mạng NAT
 - Địa chỉ IP: 192.168.38.130
 - Default gateway: 192.168.38.128
- 01 máy ảo Pfsense làm tường lửa:

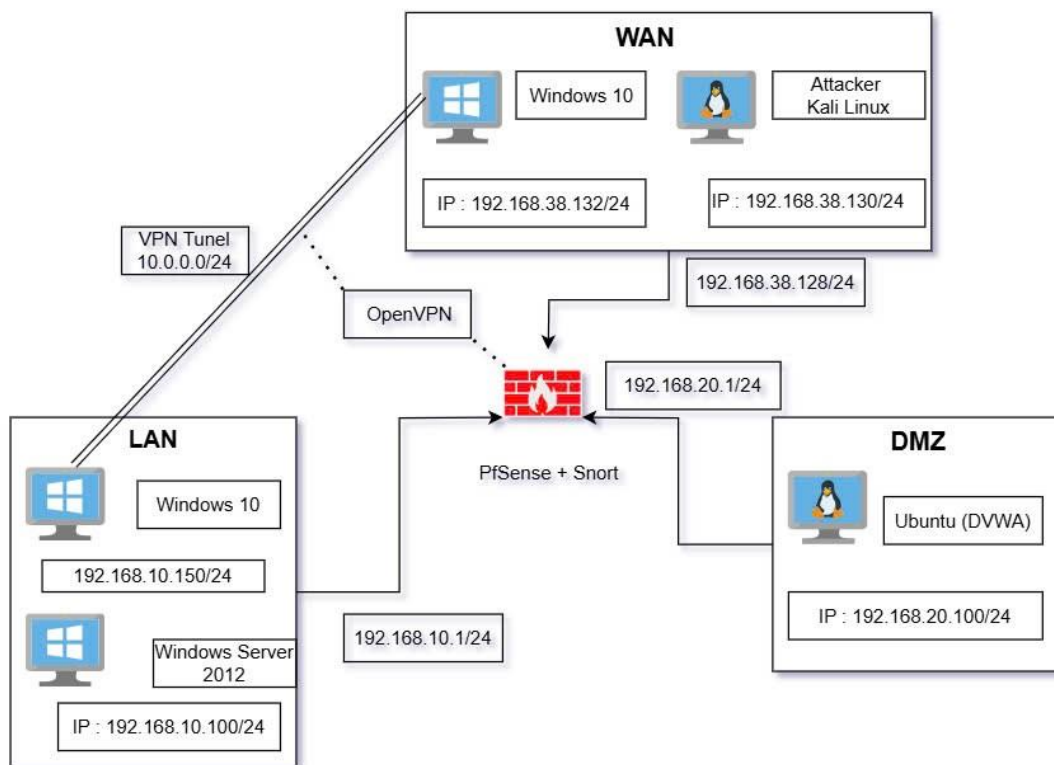
```
*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4/DHCP4: 192.168.38.128/24
LAN (lan)      -> em1      -> v4: 192.168.10.1/24
DMZ (opt1)     -> em2      -> v4: 192.168.20.1/24

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

Enter an option: █
```

3.2. Mô hình



- WAN: 192.168.38.0/24. Sử dụng card mạng NAT – Phân vùng mạng kết nối Internet.
- LAN: 192.168.10.0/24. Sử dụng card mạng VmNet2 (Host-only) – Phân vùng mạng nội bộ.
- DMZ: 192.168.20.0/24. Sử dụng card mạng VmNet3 (Host-only) – Phân vùng đặt các máy chủ Web.

3.3. Cấu hình tường lửa cơ bản

- Cấu hình IP tĩnh (Static IP Address)

Chọn số 2: Set interface(s) IP address

```
Enter an option: 2

Available interfaces:

1 - WAN (em0 - dhcp, dhcp6)
2 - LAN (em1 - static)
3 - DMZ (em2 - static)
```

```
Enter the number of the interface you wish to configure: █
```

Chọn tiếp số 2: Chọn LAN

```
Enter the number of the interface you wish to configure: 2

Configure IPv4 address LAN interface via DHCP? (y/n) n

Enter the new LAN IPv4 address. Press <ENTER> for none:
> 192.168.10.1

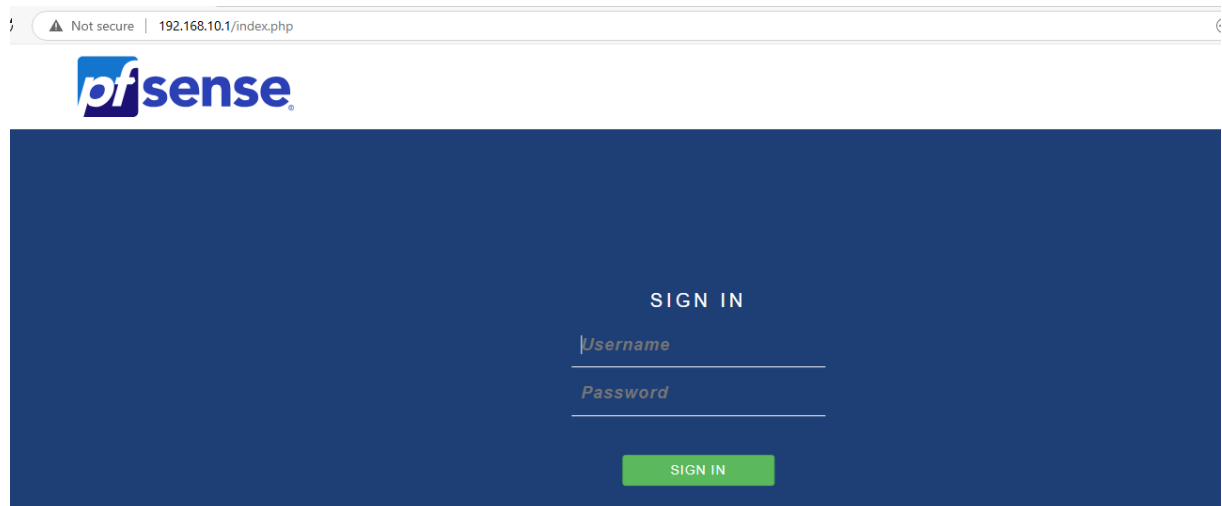
Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
     255.255.0.0   = 16
     255.0.0.0     = 8

Enter the new LAN IPv4 subnet bit count (1 to 32):
> 24
```

- Hỏi về DHCP thì chọn n
- Nhập IP: 192.168.10.1 và Subnet: 24
- Bỏ qua các bước còn lại

- Sử dụng trình duyệt trên máy Win 10 để quản trị tường lửa PfSense qua giao diện.

Truy cập theo đường dẫn: <http://192.168.10.1>



- Username: admin
- Password: pfsense

3.4. Thiết lập luật theo kịch bản

3.4.1. Thiết lập luật trong mạng LAN

a. Chặn toàn bộ máy trong mạng LAN không truy cập được mạng

Mặc định pfSense cho phép các client trong mạng LAN có thể truy cập mạng

Firewall / Rules / LAN

Floating WAN LAN DMZ

Rules (Drag to Change Order)

<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	2/3.02 MiB	*	*	*	LAN Address	80	*	*		Anti-Lockout Rule	
<input type="checkbox"/>	13/11.73 MiB	IPv4 *	LAN subnets	*	*	*	*	none		Default allow LAN to any rule	
<input type="checkbox"/>	0/0 B	IPv6 *	LAN subnets	*	*	*	*	none		Default allow LAN IPv6 to any rule	

- Đây là các rule mặc định

Ta bấm vào hình bút chì để chỉnh sửa rule và chọn disabled để vô hiệu hoá rule.

Firewall / Rules / Edit

Edit Firewall Rule

Action

Pass

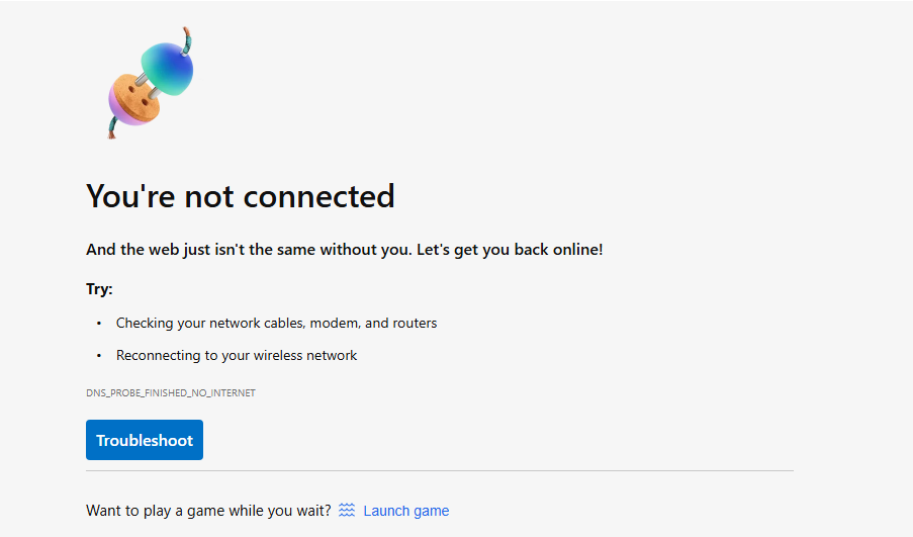
Choose what to do with packets that match the criteria specified below.
Hint: the difference between block and reject is that with reject, a packet (TCP RST c
whereas with block the packet is dropped silently. In either case, the original packet

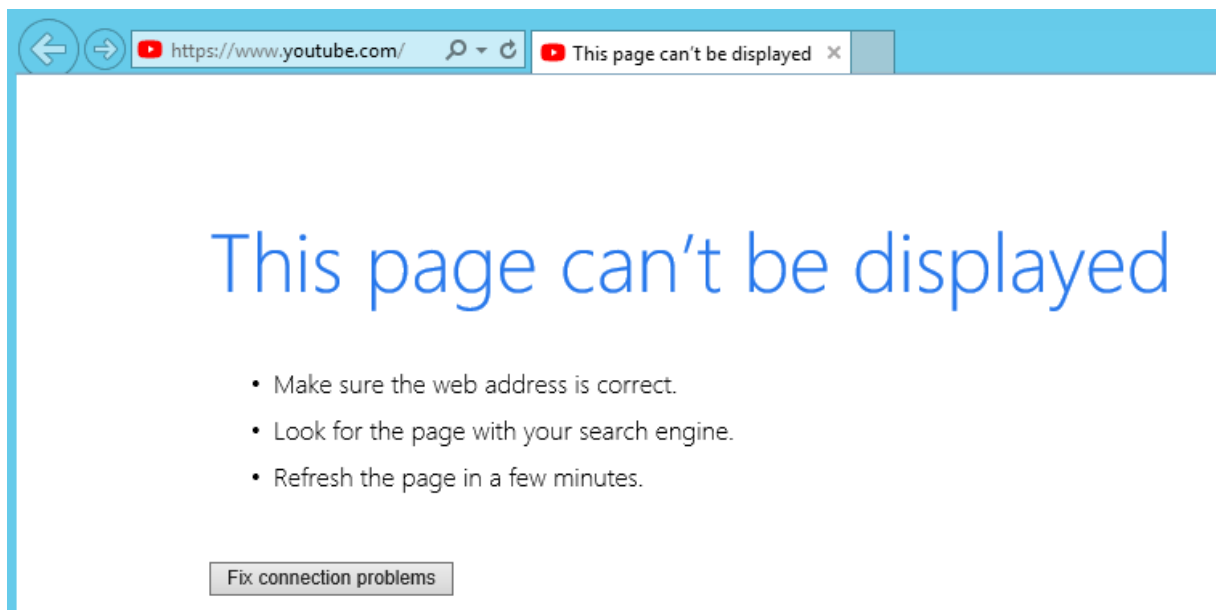
Disabled

☒ Disable this rule

Set this option to disable this rule without removing it from the list.

Kết quả cả 2 máy trong mạng LAN không truy cập được internet





b. Chỉ cho phép 1 máy trong mạng LAN được truy cập vào phần cài đặt (web GUI) của tường lửa pfSense.

Ở đây, ta sẽ tiến hành cho phép chỉ máy Windows 10 được truy cập vào phần cài đặt (web GUI) của tường lửa pfSense.

Ta bấm Add để tạo rule mới trong Firewall/ Rules/ LAN

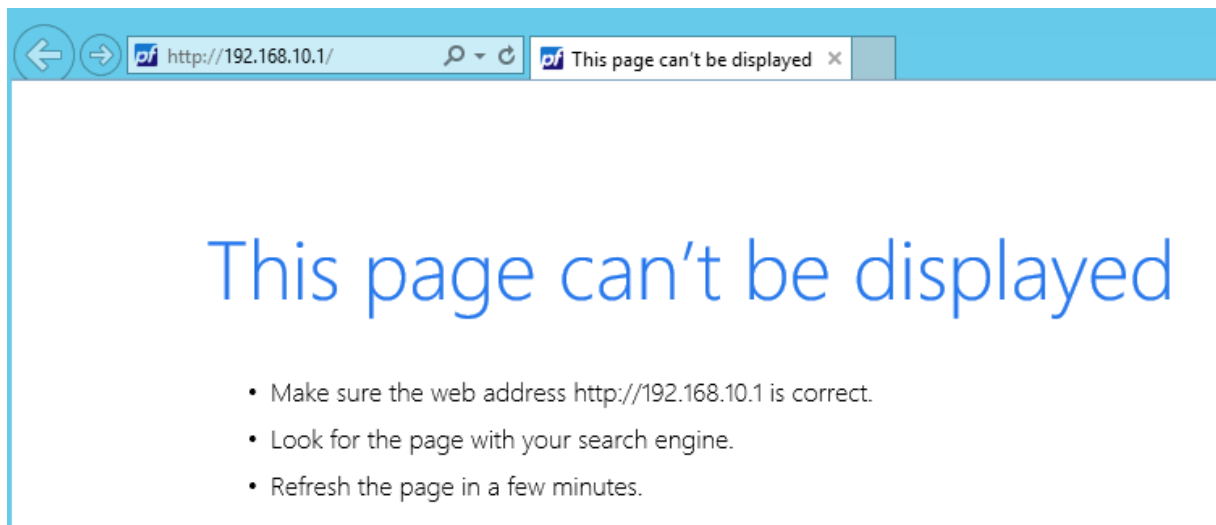
Rules (Drag to Change Order)											
<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	2/3.22 MiB	*	*	*	LAN Address	80	*	*		Anti-Lockout Rule	
<input type="checkbox"/>	0/0 B	IPv4 TCP	192.168.10.150	*	This Firewall (self)	443 (HTTPS)	*	none		Allow admin access from 192.168.10.150	

- **Thêm rule cho phép địa chỉ máy Windows 10 truy cập**
- **Action:** Pass
- **Interface:** LAN
- **Address Family:** IPv4
- **Protocol:** TCP
- **Source:** Address or alias → nhập IP: 192.168.10.150
- **Destination:** This Firewall
- **Destination port range:** HTTPS (443)

Firewall / Rules / LAN											
Floating WAN LAN DMZ											
Rules (Drag to Change Order)											
<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	0/144 B	IPv4 TCP	192.168.10.150	*	This Firewall (self)	80 (HTTP)	*	none		Allow admin access from 192.168.10.150	
<input checked="" type="checkbox"/>	0/6 KiB	IPv4 TCP	*	*	This Firewall (self)	80 (HTTP)	*	none		Block web GUI access from others	

- **Thêm rule chặn tất cả các địa chỉ IP khác truy cập**
- **Action:** Block
- **Interface:** LAN
- **Address Family:** IPv4
- **Protocol:** TCP
- **Source:** any
- **Destination:** This Firewall
- **Destination port range:** HTTP (80)

Kết quả máy Windows server 2012 không thể truy cập vào trang cài đặt tường lửa



c. Chặn web với Aliase

Ta sẽ chặn 2 trang web Facebook, Youtube.

```
Pinging facebook.com [57.144.150.1] with 32 bytes of data:
Reply from 57.144.150.1: bytes=32 time=44ms TTL=127
Reply from 57.144.150.1: bytes=32 time=42ms TTL=127
Reply from 57.144.150.1: bytes=32 time=44ms TTL=127
Reply from 57.144.150.1: bytes=32 time=43ms TTL=127
```

```
Pinging youtube.com [142.250.76.14] with 32 bytes of data:
Reply from 142.250.76.14: bytes=32 time=33ms TTL=127
Reply from 142.250.76.14: bytes=32 time=33ms TTL=127
Reply from 142.250.76.14: bytes=32 time=33ms TTL=127
Reply from 142.250.76.14: bytes=32 time=33ms TTL=127
```

Sau đó ta vào Firewall/Aliases/IP

Chọn Add để tạo nhóm các IP, ở đây có tên Blockweb

Firewall / Aliases / Edit

Properties

Name

Blockweb

The name of the alias may only consist of the characters "a-z, A-Z, 0-9 and _".

Description

A description may be entered here for administrative reference (not parsed).

Type

Host(s)

Host(s)

Hint

Enter as many hosts as desired. Hosts must be specified by their IP address or fully qualified domain name (FQDN). FQDN hostnames are periodically re-resolved and updated. If multiple IPs are returned by a DNS query, all are used. An IP range such as 192.168.1.1-192.168.1.10 or a small subnet such as 192.168.1.16/28 may also be entered and a list of individual IP addresses will be generated.

IP or FQDN

57.144.150.1

facebook.com

Delete

142.250.76.14

youtube.com





Delete

- Cấu hình như hình trên

Tiếp đến ta vào Firewall/Rules/LAN để tạo rule mới.

Floating WAN LAN DMZ

Rules (Drag to Change Order)

<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✗ 0/0 B	IPv4 *	*	*	Blockweb	*	*	none			   


Kết quả:

Máy Windows 10 trong mạng LAN vẫn tìm kiếm được từ khoá facebook nhưng khi truy cập vào facebook.com thì không truy cập được

Microsoft Bing facebook

ALL SEARCH COPILOT IMAGES VIDEOS MAPS MORE TOOLS

Copilot Answer

 Facebook
https://www.facebook.com

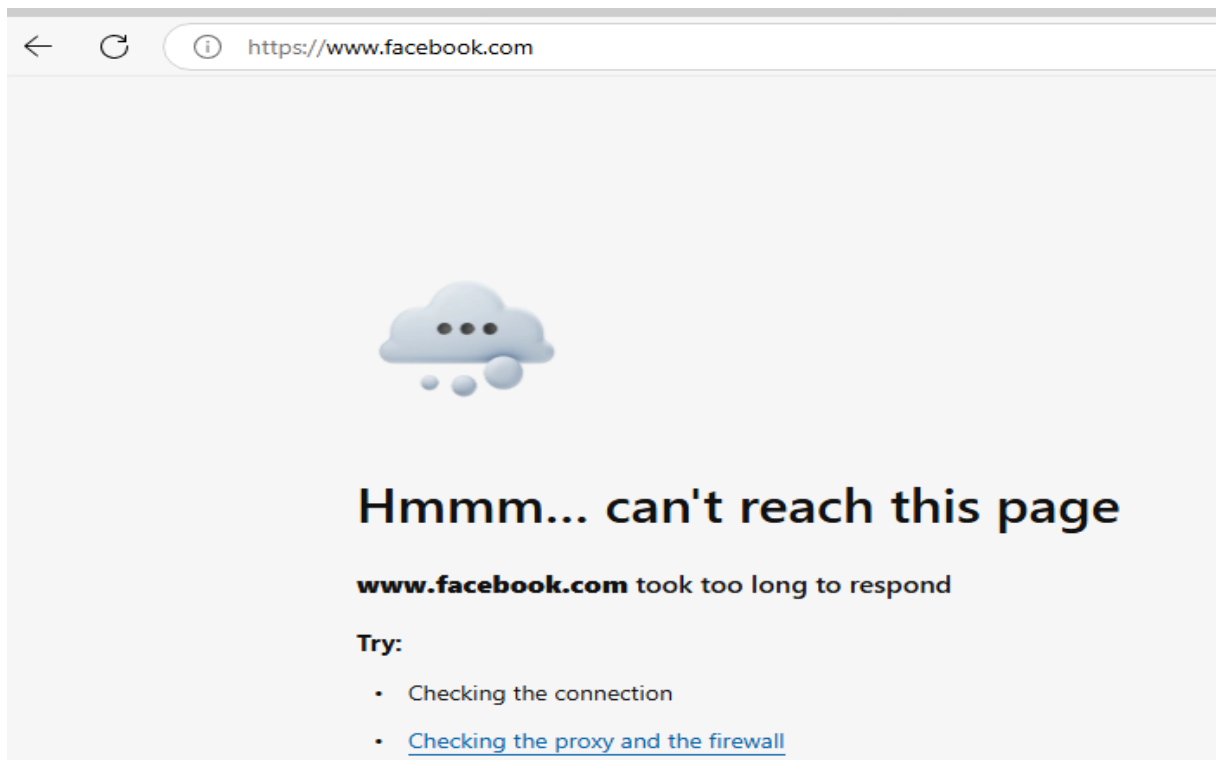
Facebook - log in or sign up

Log into Facebook to start sharing and connecting with your friends, family, and people you know.

Type of site

Social networking service

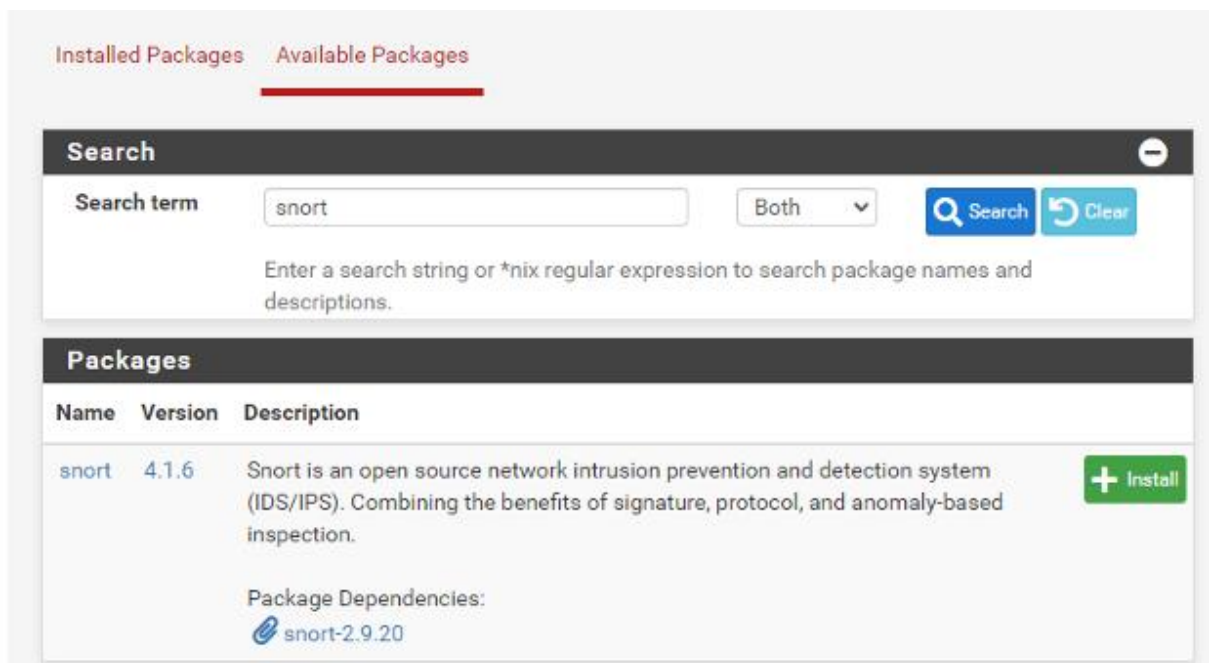
Founded



3.4.2. Cài đặt Snort trên pfsense để ngăn chặn bypass

Để cài đặt Snort ta vào System/ Package Manager/ Available Packages

Tìm kiếm Snort và bấm Install



General Settings

Enable

☐ Enable interface

Interface

WAN (em0)

Choose the interface where this Snort instance will inspect traffic.

Description

snort WAN

Enter a meaningful description here for your reference.

Snap Length

1518

Enter the desired interface snaplen value in bytes. Default is 1518 and is suitable for most applications.

- Bắt đầu thiết lập chức năng trên interface, trường hợp này chọn card WAN, do muốn phát hiện và chặn trên đường truyền WAN.

Block Settings

Block Offenders

☒ Checking this option will automatically block hosts that generate a Snort alert. Default is Not Checked.

IPS Mode

Legacy Mode

Select blocking mode operation. Legacy Mode inspects copies of packets while Inline Mode inserts the Snort inspection engine into the network stack between the NIC and the OS. Default is Legacy Mode.

Legacy Mode uses the PCAP engine to generate copies of packets for inspection as they traverse the interface. Some "leakage" of packets will occur before Snort can determine if the traffic matches a rule and should be blocked. Inline mode instead intercepts and inspects packets before they are handed off to the host network stack for further processing. Packets matching DROP rules are simply discarded (dropped) and not passed to the host network stack. No leakage of packets occurs with Inline Mode. WARNING: Inline Mode only works with NIC drivers which properly support Netmap! Supported drivers: bnxt, cc, cxgbe, cxl, em, em, ena, ice, igb, igc, ix, ixgbe, ixl, lem, re, vmx, vtnet. If problems are experienced with Inline Mode, switch to Legacy Mode instead.

Kill States

☒ Checking this option will kill firewall established states for the blocked IP. Default is checked.

Which IP to Block

BOTH

Select which IP extracted from the packet you wish to block. Default is BOTH.

- Block Offenders: Snort sẽ tự động block IP nếu phát hiện packet vi phạm rules
- Legacy Mode: Snort chỉ xem bản sao packet
- Kill States: Ngắt kết nối hiện tại từ IP bị chặn
- Which IP to Block: BOTH Block cả IP nguồn và IP đích

Sang tab WAN Categories để bật các nhóm rules.

Enable	Ruleset: ET Open Rules	Enable	Ruleset: Snort Text Rules	Enable	Ruleset: Snort SO Rules	Snort OPENAPPID rules are not enabled.
<input type="checkbox"/>	emerging-activex.rules	<input type="checkbox"/>	snort_app-detect.rules	<input type="checkbox"/>	snort_browser-chrome.so.rules	
<input type="checkbox"/>	emerging-attack_response.rules	<input type="checkbox"/>	snort_attack-responses.rules	<input type="checkbox"/>	snort_browser-ie.so.rules	
<input type="checkbox"/>	emerging-botcc.portgrouped.rules	<input type="checkbox"/>	snort_backdoor.rules	<input type="checkbox"/>	snort_browser-other.so.rules	
<input type="checkbox"/>	emerging-botcc.rules	<input checked="" type="checkbox"/>	snort_bad-traffic.rules	<input type="checkbox"/>	snort_browser-webkit.so.rules	
<input type="checkbox"/>	emerging-chat.rules	<input type="checkbox"/>	snort_blacklist.rules	<input type="checkbox"/>	snort_exploit-kit.so.rules	
<input type="checkbox"/>	emerging-ciarmy.rules	<input type="checkbox"/>	snort_botnet-cnc.rules	<input type="checkbox"/>	snort_file-executable.so.rules	
<input type="checkbox"/>	emerging-compromised.rules	<input type="checkbox"/>	snort_browser-chrome.rules	<input type="checkbox"/>	snort_file-flash.so.rules	
<input type="checkbox"/>	emerging-current_events.rules	<input type="checkbox"/>	snort_browser-firefox.rules	<input type="checkbox"/>	snort_file-image.so.rules	
<input type="checkbox"/>	emerging-deleted.rules	<input type="checkbox"/>	snort_browser-ie.rules	<input type="checkbox"/>	snort_file-java.so.rules	
<input type="checkbox"/>	emerging-dns.rules	<input type="checkbox"/>	snort_browser-other.rules	<input type="checkbox"/>	snort_file-multimedia.so.rules	
<input type="checkbox"/>	emerging-dos.rules	<input type="checkbox"/>	snort_browser-plugins.rules	<input type="checkbox"/>	snort_file-office.so.rules	
<input type="checkbox"/>	emerging-drop.rules	<input type="checkbox"/>	snort_browser-webkit.rules	<input type="checkbox"/>	snort_file-other.so.rules	
<input type="checkbox"/>	emerging-dshield.rules	<input type="checkbox"/>	snort_chat.rules	<input type="checkbox"/>	snort_file-pdf.so.rules	
<input type="checkbox"/>	emerging-exploit.rules	<input type="checkbox"/>	snort_content-replace.rules	<input type="checkbox"/>	snort_indicator-shellcode.so.rules	
<input type="checkbox"/>	emerging-ftp.rules	<input type="checkbox"/>	snort_ddos.rules	<input type="checkbox"/>	snort_malware-cnc.so.rules	

Để chặn một số kỹ thuật bypass như gửi các gói phân mảnh, spoofed source thì ta sẽ tick chọn các rule như:

- decoder.rules: Phát hiện lỗi/biến dạng trong packet header (phân mảnh bất thường, TTL 0, checksum sai...)
- frag3-engine.rules: Phát hiện các gói phân mảnh bất thường như tiny fragment, overlap fragment – kỹ thuật Nmap -f
- bad-traffic.rules: Phát hiện các gói có IP spoof, source port = 0, địa chỉ loopback hoặc reserved
- preprocessor.rules: Giám sát hành vi không tuân chuẩn TCP/IP hoặc cố tình evade detection
- emerging-scan.rules: Phát hiện các loại scan như Nmap NULL, XMAS, FIN, decoy scan, stealth scan
- emerging-netbios.rules: Phát hiện scan hoặc exploit qua giao thức NetBIOS có thể dùng phân mảnh
- policy.rules: Phát hiện các gói sai chuẩn RFC – gói trống flag, không checksum, hành vi bất thường
- dos.rules: Tấn công từ chối dịch vụ qua phân mảnh chồng lấn, fragment flood, malformed packets
- backdoor.rules: Phát hiện mã độc hoặc C2 giao tiếp dùng source port bất thường như 53, 20, hoặc phân mảnh payload
- experimental.rules: Các rule đang thử nghiệm để phát hiện kỹ thuật evade hoặc tunneling nâng cao.
- emerging-policy.rules: Phát hiện traffic trái phép (giả mạo DNS, NTP...)

Trước khi áp dụng rule:

```
(kali@kali)-[~]  
$ nmap 192.168.20.100  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-05-12 10:00 EDT  
Nmap scan report for 192.168.20.100.non-exists.ptr.local (192.168.20.100)  
Host is up (0.0015s latency).  
Not shown: 999 closed tcp ports (reset)  
PORT      STATE SERVICE  
80/tcp    open  http  
  
Nmap done: 1 IP address (1 host up) scanned in 0.27 seconds
```

```
(kali㉿kali)-[~]
$ nmap -g 53 192.168.20.100
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-05-12 10:03 EDT
Nmap scan report for 192.168.20.100.non-exists.ptr.local (192.168.20.100)
Host is up (0.0015s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
80/tcp    open  http

Nmap done: 1 IP address (1 host up) scanned in 0.25 seconds
```




```
(kali㉿kali)-[~]
$ nmap -f 192.168.20.100
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-05-12 10:01 EDT
Nmap scan report for 192.168.20.100.non-exists.ptr.local (192.168.20.100)
Host is up (0.00080s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
80/tcp    open  http

Nmap done: 1 IP address (1 host up) scanned in 0.26 seconds
```

```
(kali㉿kali)-[~]
$ nmap -D 192.168.20.190 192.168.20.100
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-05-12 10:05 EDT
Nmap scan report for 192.168.20.100.non-exists.ptr.local (192.168.20.100)
Host is up (0.0019s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
80/tcp    open  http

Nmap done: 1 IP address (1 host up) scanned in 0.25 seconds
```

Sau khi áp dụng rule:

Interface Settings Overview					
Interface	Snort Status	Pattern Match	Blocking Mode	Description	Actions
<input type="checkbox"/> WAN (em0)	 	AC-BNFA	LEGACY MODE	snort WAN	  

```
(kali㉿kali)-[~]
$ nmap -f 192.168.20.100
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-05-12 10:07 EDT
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.13 seconds
```

```
(kali㉿kali)-[~]
$ nmap -g 53 192.168.20.100
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-05-12 10:08 EDT
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.10 seconds
```

```
(kali@kali)-[~]
$ nmap -D 192.168.20.190 192.168.20.100
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-05-12 10:08 EDT
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.12 seconds
```

3.4.3. Cài đặt OpenVPN trên Pfsense (2.7.2) và cấu hình Client-To-Site

Trước khi cài đặt, ta kiểm tra ping từ máy Client tới Pfsense (192.168.38.128) và mạng LAN (192.168.10.1)

```
Pinging 192.168.38.128 with 32 bytes of data:
Reply from 192.168.38.128: bytes=32 time<1ms TTL=64
Reply from 192.168.38.128: bytes=32 time<1ms TTL=64
Reply from 192.168.38.128: bytes=32 time<1ms TTL=64
Reply from 192.168.38.128: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.38.128:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

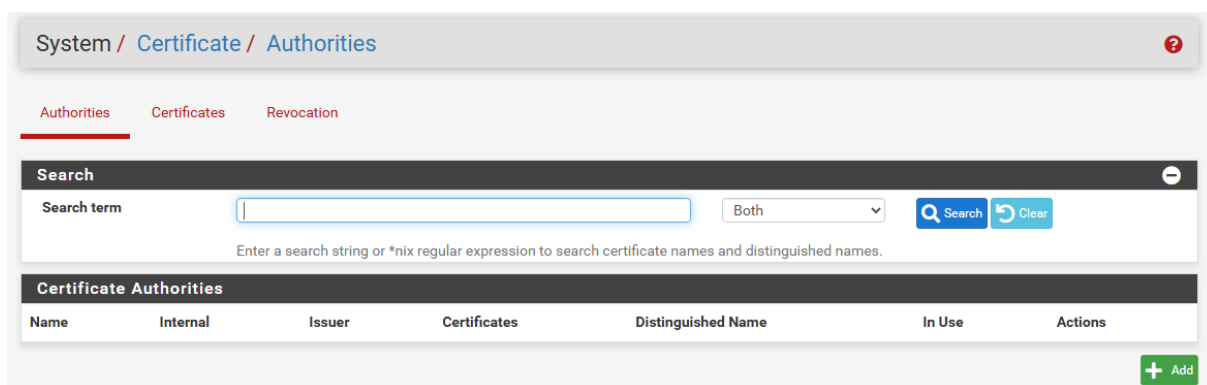
C:\Users\Chuxi>ping 192.168.10.1

Pinging 192.168.10.1 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.10.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Tiến hành tạo CA và Certificate trên máy Win 10 ở mạng LAN để xác thực người dùng và server.

Vào Web GUI của pfsense và vào System/ Certificate/ Authorities



Chọn Add để tạo CA (Certificate Authority) mới

Create / Edit CA

Descriptive name

pfsense_rootca

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.

- Descriptive name: pfsense_rootca
- Method: chọn Create an internal certificates authority
- Trust Store: có thể chọn
- Các thiết lập tại Internal Certificate Authority có thể tùy chọn hoặc bỏ qua (để trống)

Certificate Authorities						
Name	Internal	Issuer	Certificates	Distinguished Name	In Use	Actions
pfsense_rootca	✓	self-signed	0	CN=internal-ca Valid From: Tue, 13 May 2025 09:54:54 +0700 Valid Until: Fri, 11 May 2035 09:54:54 +0700		    

Tiếp theo chuyển sang tab Certificates để tạo Sign mới cho OpenVPN. Chọn Add/Sign

System / Certificates / Certificates

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 (681eebab0151b) Server Certificate CA: No Server: Yes	self-signed	O=pfSense GUI default Self-Signed Certificate, CN=pfSense-681eebab0151b Valid From: Sat, 10 May 2025 13:01:15 +0700 Valid Until: Fri, 12 Jun 2026 13:01:15 +0700		    

+ Add/Sign

- Method: chọn Create an internal certificates
- Descriptive name: vpn_ser_cert
- Certificate authority: chọn CA vừa tạo ban này (pfsense_rootca)
- Common Name: 192.168.38.128
- Certificate Type: Server Certificates

Certificates				
Name	Issuer	Distinguished Name	In Use	Actions
GUI default (681eebab0151b) Server Certificate CA: No Server: Yes	self-signed	O=pfSense GUI default Self-Signed Certificate, CN=pfSense-681eebab0151b Valid From: Sat, 10 May 2025 13:01:15 +0700 Valid Until: Fri, 12 Jun 2026 13:01:15 +0700		
vpn_ser-cert Server Certificate CA: No Server: Yes	pfsense_rootca	CN=192.168.38.128 Valid From: Tue, 13 May 2025 12:41:59 +0700 Valid Until: Fri, 11 May 2035 12:41:59 +0700		

Tiếp theo ta tiến hành cấu hình OpenVPN. Vào VPN/ OpenVPN/ Wizards

Wizard / OpenVPN Remote Access Server Setup /

Step 1

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

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

Ta bấm Next

Wizard / OpenVPN Remote Access Server Setup / Certificate Authority Selection

Step 5 of 11

Certificate Authority Selection

OpenVPN Remote Access Server Setup Wizard

Choose a Certificate Authority (CA)

Certificate Authority

Add new CA Next

- Certificate Authority: pfsense_rootca

Ta bấm Next

Server Certificate Selection

OpenVPN Remote Access Server Setup Wizard

Choose a Server Certificate

Certificate

- Certificate: vpn_ser-cert

Ta bấm Next

Wizard / OpenVPN Remote Access Server Setup / Server Setup ?

Step 9 of 11

Server Setup

OpenVPN Remote Access Server Setup Wizard

General OpenVPN Server Information

Description

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.)

- Description: remote user
- IPv4 Tunnel Network: 10.0.0.0/24
- Redirect IPv4 Gateway: check
- IPv4 Local Network: IP LAN
- Concurrent Connections: 5
- Advanced client settings: bỏ qua

Next và check 2 tùy chọn như bên dưới

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.

Vậy là ta đã cấu hình xong phần server cho OpenVPN

VPN / OpenVPN / Servers 📊 📄 ?

Servers Clients Client Specific Overrides Wizards

OpenVPN Servers					
Interface	Protocol / Port	Tunnel Network	Mode / Crypto	Description	Actions
WAN	UDP4 / 1194 (TUN)	10.0.0.0/24	Mode: Remote Access (SSL/TLS + User Auth) Data Ciphers: AES-256-GCM, AES-128-GCM, CHACHA20-POLY1305, AES-256-CBC Digest: SHA256 D-H Params: 2048 bits	remote user	✎ 📄 🗑

+ Add

Tiếp theo ta sang tab Clients để cấu hình client cho OpenVPN

VPN / OpenVPN / Clients

Servers Clients Client Specific Overrides Wizards

OpenVPN Clients

Interface	Protocol	Server	Mode / Crypto	Description	Actions
-----------	----------	--------	---------------	-------------	---------

+ Add

Chọn Add

VPN / OpenVPN / Clients / Edit

Servers Clients Client Specific Overrides Wizards

General Information

Description

user vpn

A description of this VPN for administrative reference.

Disabled

☐ Disable this client

Set this option to disable this client without removing it from the list.

Mode Configuration

Server mode

Peer to Peer (SSL/TLS)

Device mode

tun - Layer 3 Tunnel Mode

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




Endpoint Configuration

- Description: user vpn
- Server host or address: IP WAN
- Nhập Username: vpn và Password: 123456
- Gateway creation: IPv4 only
- Chọn SAVE và hoàn tất

VPN / OpenVPN / Clients

Servers Clients Client Specific Overrides Wizards

OpenVPN Clients

Interface	Protocol	Server	Mode / Crypto	Description	Actions
WAN	UDP4 (TUN)	192.168.38.128:1194	Mode: Peer to Peer (SSL/TLS) Data Ciphers: AES-256-GCM, AES-128-GCM, CHACHA20-POLY1305, AES-256-CBC Digest: SHA256	user vpn	  

+ Add

Tiếp theo ta tạo user trong System/ User Manager/ Users để phân quyền

System / User Manager / Users

Users Groups Settings Authentication Servers

Users

	Username	Full name	Status	Groups	Actions
<input type="checkbox"/>	admin	System Administrator	✓	admins	

Add Delete

Chọn Add

System / User Manager / Users / Edit

Users Groups Settings Authentication Servers

User Properties

Defined by USER

Disabled ☐ This user cannot login

Username

Password

Full name
User's full name, for administrative information only

Certificate ☒ Click to create a user certificate

Create Certificate for User

Descriptive name

Certificate authority

- Nhập Username và Password như trên
- Chọn ô Certificate và nhập như hình

System / User Manager / Users

Users Groups Settings Authentication Servers

Users

	Username	Full name	Status	Groups	Actions
<input type="checkbox"/>	admin	System Administrator	✓	admins	
<input type="checkbox"/>	vpn	vpn user	✓		

Add Delete

- User này dùng để export cấu hình của OpenVPN

Tiếp theo ta tải gói “openvpn-client-export” tại System/ Package Manager/ Available Package

System / Package Manager / Available Packages

Installed Packages Available Packages

Search

Search term Both

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

Packages

Name	Version	Description
openvpn-client-export	1.9.2	Exports pre-configured OpenVPN Client configurations directly from pfSense software.

Package Dependencies: [openvpn-client-export-2.6.7](#) [openvpn-2.6.8_1](#) [zip-3.0_1](#) [7-zip-23.01](#)

- Tìm kiếm “openvpn-client-export” và bấm Install

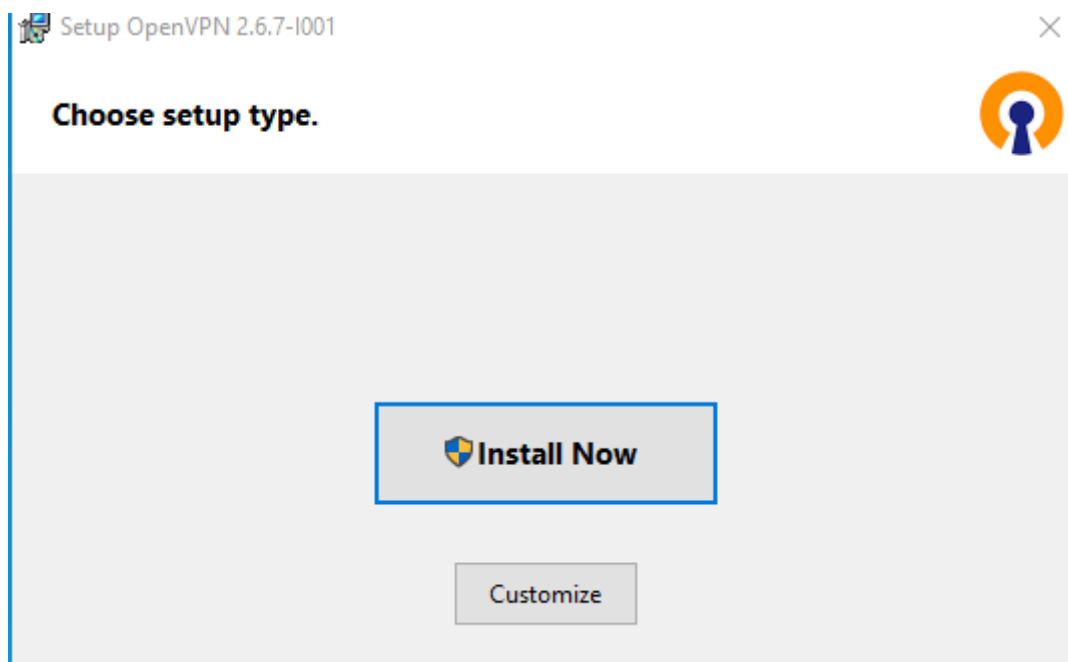
Sau khi cài đặt xong trong VPN/ OpenVPN sẽ có tab Client Export. Ở dưới sẽ có các bản cài đặt cho Client

OpenVPN Clients

User	Certificate Name	Export
vpn	vpn_user_cert	<div><p>- Inline Configurations:</p><p><input type="button" value="Most Clients"/> <input type="button" value="Android"/> <input type="button" value="OpenVPN Connect (iOS/Android)"/></p><p>- Bundled Configurations:</p><p><input type="button" value="Archive"/> <input type="button" value="Config File Only"/></p><p>- Current Windows Installers (2.6.7-1x001):</p><p><input type="button" value="64-bit"/> <input type="button" value="32-bit"/></p><p>- Previous Windows Installers (2.5.9-1x601):</p><p><input type="button" value="64-bit"/> <input type="button" value="32-bit"/></p><p>- Legacy Windows Installers (2.4.12-1x601):</p><p><input type="button" value="10/2016/2019"/> <input type="button" value="7/8/8.1/2012/2"/></p><p>- Viscosity (Mac OS X and Windows):</p><p><input type="button" value="Viscosity Bundle"/> <input type="button" value="Viscosity Inline Config"/></p></div>

Tải bản cần cài đặt và chuyển file sang máy Client (WAN).

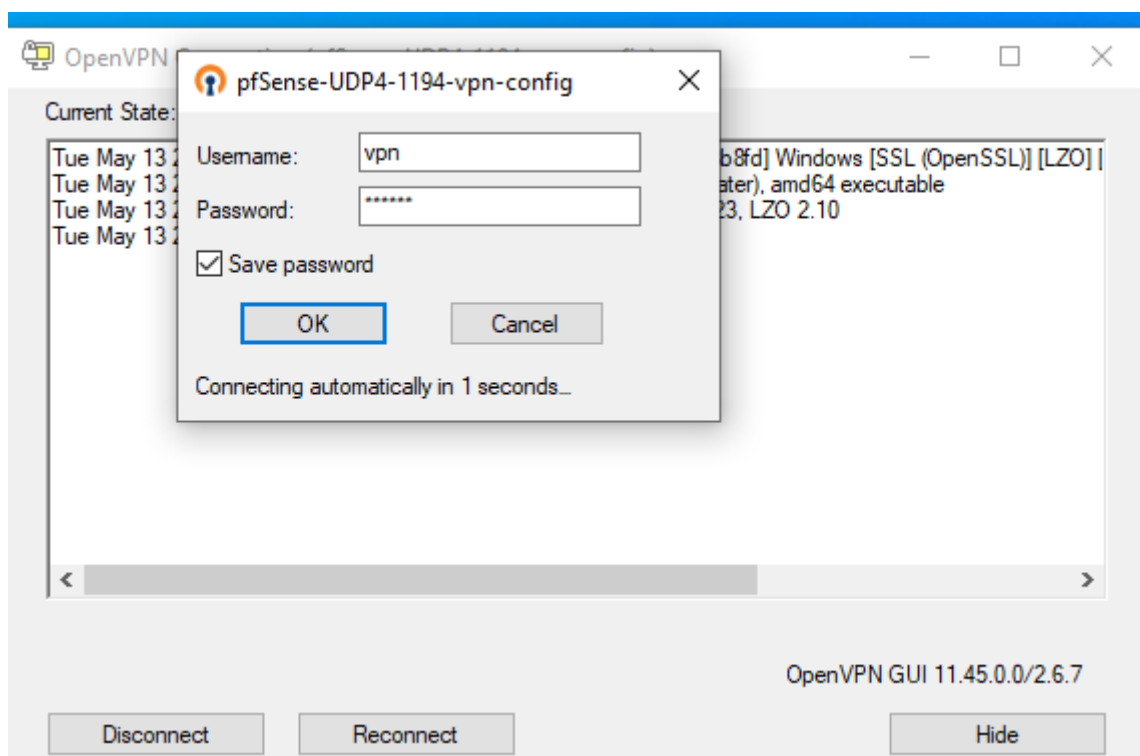
Tiến hành cài đặt trên máy Client (WAN).



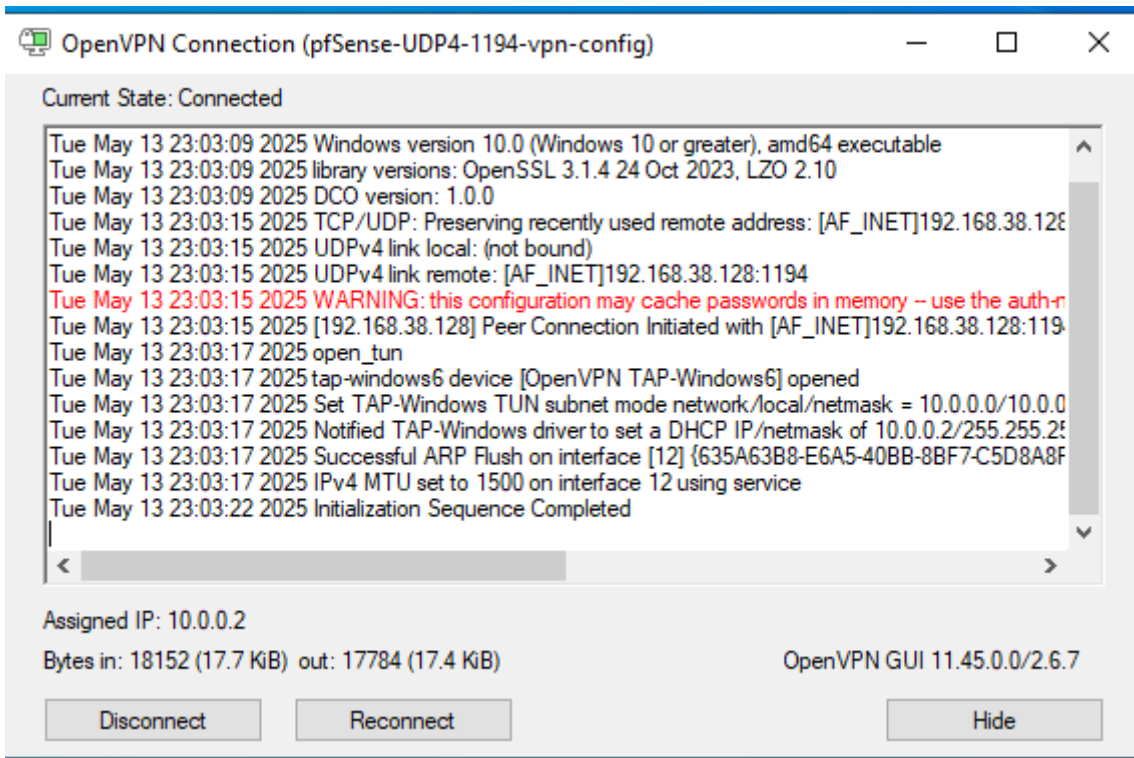
- Chọn Install

Khởi chạy và kết nối

Đăng nhập tài khoản vừa tạo ban nãy



Quá trình kết nối thành công sẽ hiển thị IP cấp cho VPN



Kiểm tra lại trong Status/ OpenVPN sẽ thấy thông tin Client

Status / OpenVPN

ovpn1: remote user UDP4:1194 / Client Connections: 1

Common Name	Real Address	Virtual Address	Last Change	Bytes Sent	Bytes Received	Cipher	Actions
vpn	192.168.38.132:61869	10.0.0.2	2025-05-13 23:03:17	18 KiB	18 KiB	AES-256-GCM	✕ ✕
vpn							✓ ↺ ↻

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

Kiểm tra kết quả:

Máy Client có thể Ping tới mạng LAN

```
C:\Users\Chuxi>ping 192.168.10.1

Pinging 192.168.10.1 with 32 bytes of data:
Reply from 192.168.10.1: bytes=32 time<1ms TTL=64
Reply from 192.168.10.1: bytes=32 time=1ms TTL=64
Reply from 192.168.10.1: bytes=32 time=1ms TTL=64
Reply from 192.168.10.1: bytes=32 time=1ms TTL=64

Ping statistics for 192.168.10.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Kiểm tra gói tin bằng Wireshark

1689	73.111416	192.168.38.132	192.168.38.128	OpenVPN	562	MessageType: P_DATA_V2
1690	73.111416	192.168.38.132	192.168.38.128	OpenVPN	1506	MessageType: P_DATA_V2
1691	73.111466	192.168.38.132	192.168.38.128	OpenVPN	190	MessageType: P_DATA_V2
1702	73.112183	192.168.38.128	192.168.38.132	OpenVPN	106	MessageType: P_DATA_V2
1703	73.112268	192.168.38.128	192.168.38.132	OpenVPN	106	MessageType: P_DATA_V2
1704	73.112302	192.168.38.128	192.168.38.132	OpenVPN	106	MessageType: P_DATA_V2
1705	73.112360	192.168.38.128	192.168.38.132	OpenVPN	106	MessageType: P_DATA_V2
1706	73.112405	192.168.38.128	192.168.38.132	OpenVPN	106	MessageType: P_DATA_V2
1708	73.166268	192.168.38.128	192.168.38.132	OpenVPN	213	MessageType: P_DATA_V2
1709	73.167409	192.168.38.132	192.168.38.128	OpenVPN	144	MessageType: P_DATA_V2
1710	73.167571	192.168.38.132	192.168.38.128	OpenVPN	144	MessageType: P_DATA_V2

Wireshark · Follow UDP Stream (udp.stream eq 46) · Ethernet0

```
8)}_.....M.w....\o.....U(F{f...I.....h#pW.....
@...jZ.`{...N.....}.3>.....tw.....h#pY.....)
)}_.....P.s.H5%U...X.8.....>BQk....I.9.....h#pW.....jZ.`{.....
W...~...Q.'3.I.\.2.....c..t.K.e.....;4`).dp.....#.u.....\...2......0.....+./...$.(.k.#.'.g.
...9.
...3.....
.....
.*.(.....
.....+.....3.&,$...+..g.....P}i+<...8...3.8./..3Y
...jZ.`{.8..6.q.X.#.Y.,Lv'+...|u.8.e..R.....h#pY.....)}_.....z...v...=?T.t.V.4.....T).-.(}R?...e.....;4`).dp.....#.u.....\.....
+.....3.$...y.G..*...|f...@_...;3D...F..V7#.....6...[h..4x.....
--H.....>aw{8w...?.....d...u.....K...N...==#MCJ].....#QH.....}.Et.....&x...X.e...z.DA.r.sJ.A.G&.'/h.V@=...B...t.,<.....P.*.Lj..
.....jIU..
HP..l.&a.E...H...I"H.Y....].m..W...b..0.[...G.E.....tJ....cc..3..].....6.3Lt..R...
...M...j.....|.}.S.J..r'
_...@>.h.3A..bVw...V...F...6{".A.t.:j...7.{i^..T.#,...D.OI..3~7,:'.CZ...7....|B...|.&{..DAa..zA...O.Z.L...E.l'.h.....{E2p.<..M.?..*I1.\nD
.o$.$.j..fkIY...t#..*.;.@dMI...S..*...j.....a.
F.....h.@.J.F16,...!Mj.F.07...KfnZ...F=.....\).F.....LD...rWU=...).6.V.I.ct.....16.....K..#.....-1V...B.y....>..Y8..w...+w..{.%5...
.....*K...~...z)}r..3&qu..C.c.D...f.W.....=
```

- Các gói tin đã được mã hóa