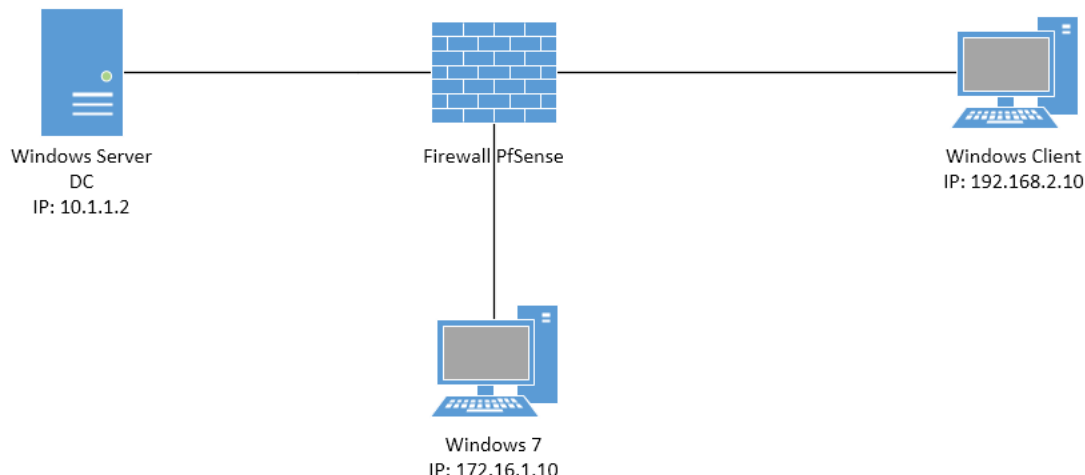


# Bài thực hành Triển khai VPN trên tường lửa PfSense sử dụng OpenVPN và xác thực RADIUS

## Sơ đồ triển khai



## Mô tả:

Triển khai công nghệ VPN đảm bảo an toàn truy cập từ xa từ máy trạm tới máy chủ chia sẻ dữ liệu trong mạng nội bộ. Sử dụng OpenVPN trên tường lửa PfSense và sử dụng phương thức xác thực RADIUS.

## Các bước thực hiện:

### Chuẩn bị:

Cài đặt tường lửa PfSense và cấu hình mạng theo mô hình:

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

WAN (wan)      -> le0      -> v4: 192.168.2.5/24
LAN (lan)      -> le1      -> v4: 172.16.1.1/24
OPT1 (opt1)    -> le2      -> v4: 10.1.1.1/24

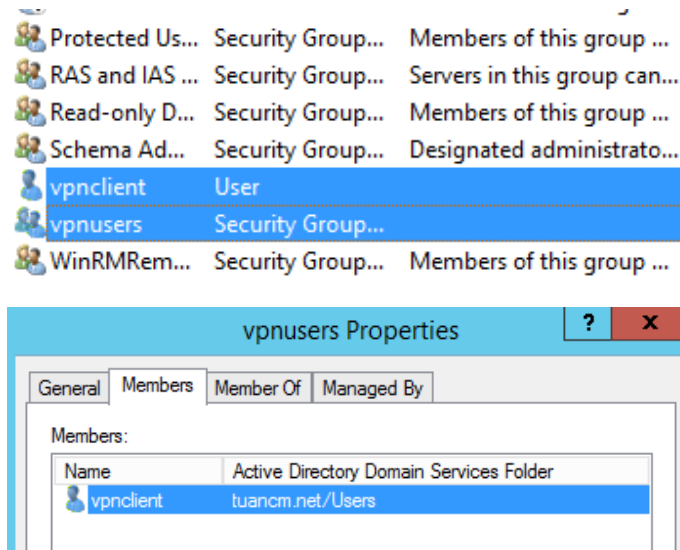
0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults  13) Update from console
5) Reboot system              14) Enable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

### 1. Thực hiện trên máy chủ Windows

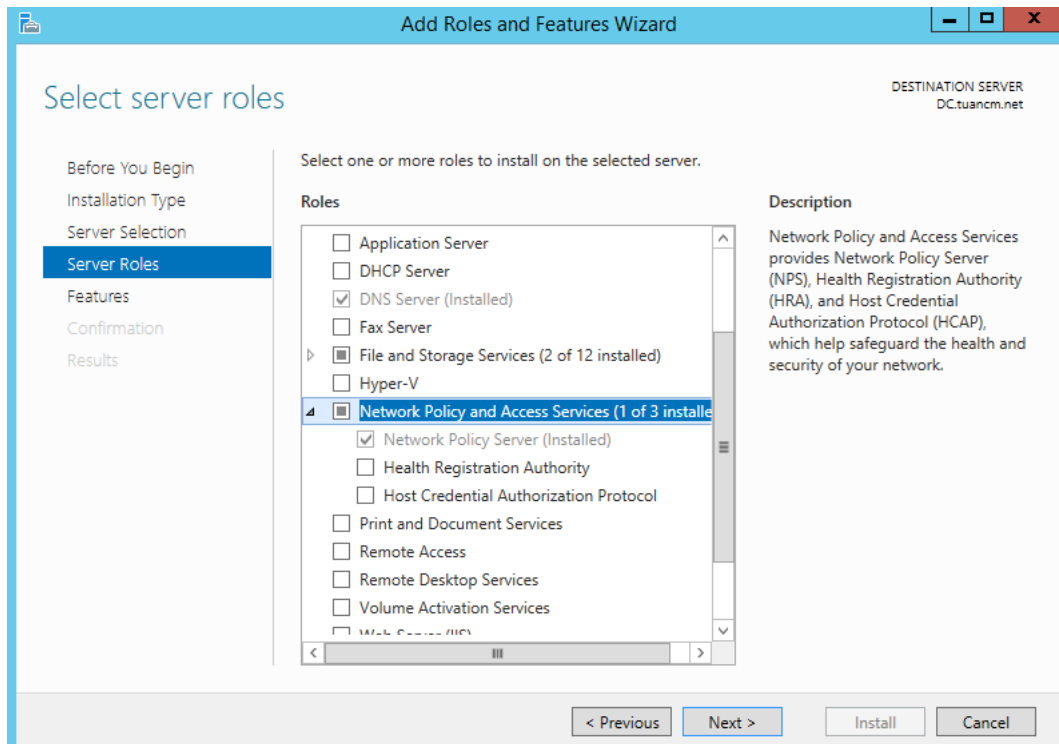
#### Bước 1. Nâng cấp lên DC

Tham khảo tài liệu [1] bài 1.1.2

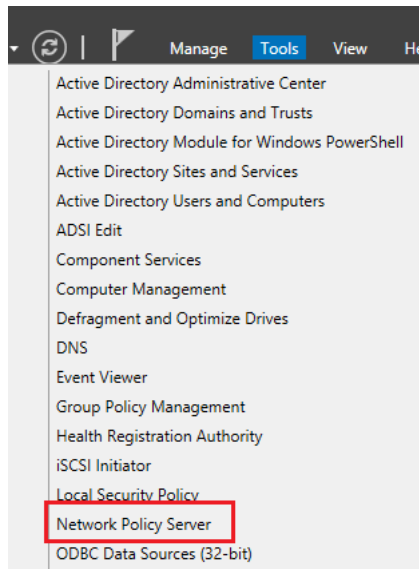
## Bước 2. Tạo tài khoản và nhóm VPN



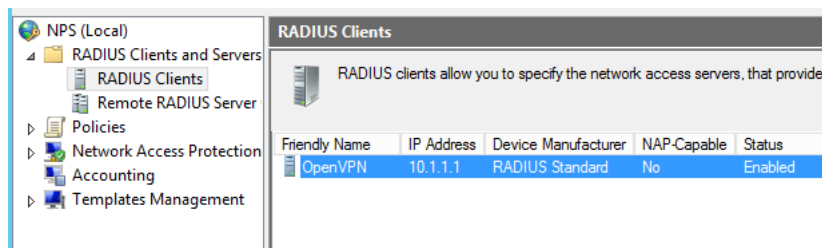
## Bước 3. Cài đặt Network Policy and Access Services



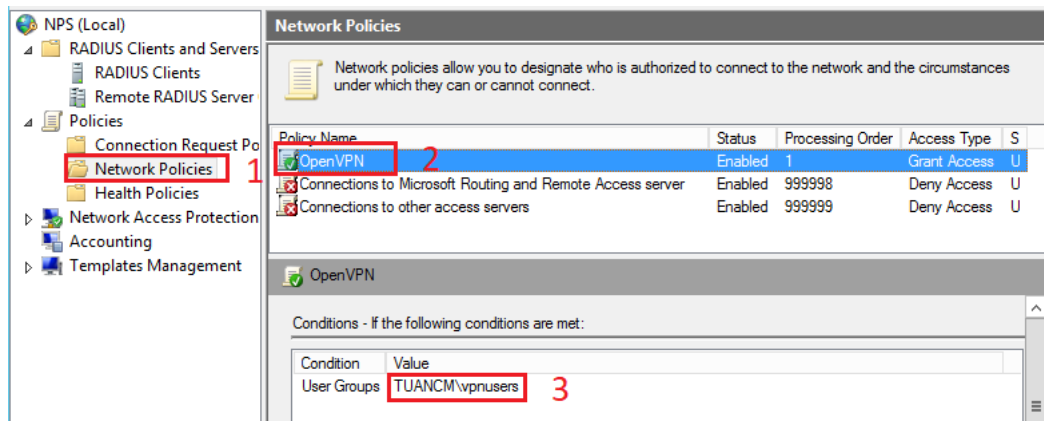
## Bước 4. Cấu hình RADIUS client (pfsense) trong Network Policy Server



Tạo mới và khai báo thông tin về Radius client:



Tạo mới và thiết lập chính sách cho nhóm người dùng truy cập từ xa:



## 2. Thực hiện trên máy PfSense

Bước 1. Tạo trung tâm cấp phát chứng thư số CA local:

Tham khảo tài liệu [1] bài 3.2.4.2

Kết quả:

System / Certificate Manager / CAs

CAs

Certificates

Certificate Revocation

Search

Search term

Both

Search

Clear

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

Certificate Authorities

Name	Internal	Issuer	Certificates	Distinguished Name	In Use	Actions
Tuancm CA	✓	self-signed	2	ST=Ha Noi, OU=ATTT, O=HVKTMM, L=Ha Noi, CN=internal-ca, C=VN Valid From: Tue, 06 Dec 2022 08:34:20 +0000 Valid Until: Fri, 03 Dec 2032 08:34:20 +0000	OpenVPN Server	

Bước 2. Tạo chứng thư số cho máy chủ VPN

Tham khảo tài liệu [1] bài 3.2.4.3

Kết quả:

Certificates

Name	Issuer	Distinguished Name	In Use	Actions
webConfigurator default (638f5cda6efd2) Server Certificate CA: No Server: Yes	self-signed	O=pfSense webConfigurator Self-Signed Certificate, CN=pfSense-638f5cda6efd2 Valid From: Tue, 06 Dec 2022 15:16:42 +0000 Valid Until: Mon, 08 Jan 2024 15:16:42 +0000		
<div>Server Cert</div> Server Certificate CA: No Server: Yes	Tuancm CA	ST=Ha Noi, OU=ATTT, O=HVKTMM, L=Ha Noi, CN=Server Cert, C=VN Valid From: Tue, 06 Dec 2022 08:35:40 +0000 Valid Until: Fri, 03 Dec 2032 08:35:40 +0000	OpenVPN Server	
cert user User Certificate CA: No Server: No	Tuancm CA	ST=Ha Noi, OU=ATTT, O=HVKTMM, L=Ha Noi, CN=user vpn cert, C=VN Valid From: Tue, 06 Dec 2022 08:44:45 +0000 Valid Until: Fri, 03 Dec 2032 08:44:45 +0000		

Bước 3. Cấu hình xác thực Radius

System / User Manager / Authentication Servers

Users

Groups

Settings

Authentication Servers

Authentication Servers

Server Name	Type	Host Name	Actions
RADIUS	RADIUS	10.1.1.2	
Local Database		pfSense	

Bước 4. Cấu hình OpenVPN

Tham khảo tài liệu [1] bài 3.2.4.5

Kết quả:

VPN / OpenVPN / Servers

Servers

Clients




Client Specific Overrides

Wizards

Client Export

Shared Key Export

OpenVPN Servers

Interface	Protocol / Port	Tunnel Network	Mode / Crypto	Description	Actions
WAN	UDP4 / 1194 (TUN)	10.2.2.0/24	<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	Openvpn server	  

## Bước 5. Kiểm tra luật trên tường lửa cho phép kết nối VPN

Firewall / Rules / WAN

Floating

WAN

LAN

OPT1

OpenVPN

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 UDP	*	*	This Firewall	1194 (OpenVPN)	*	none		<div><div></div><div></div><div></div><div></div><div></div></div>

## Bước 6. Tạo chứng thư số cho người dùng truy cập vpn

System / Certificate Manager / Certificates

CAs

Certificates

Certificate Revocation

Search

Search term
















Both

Search

Clear

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

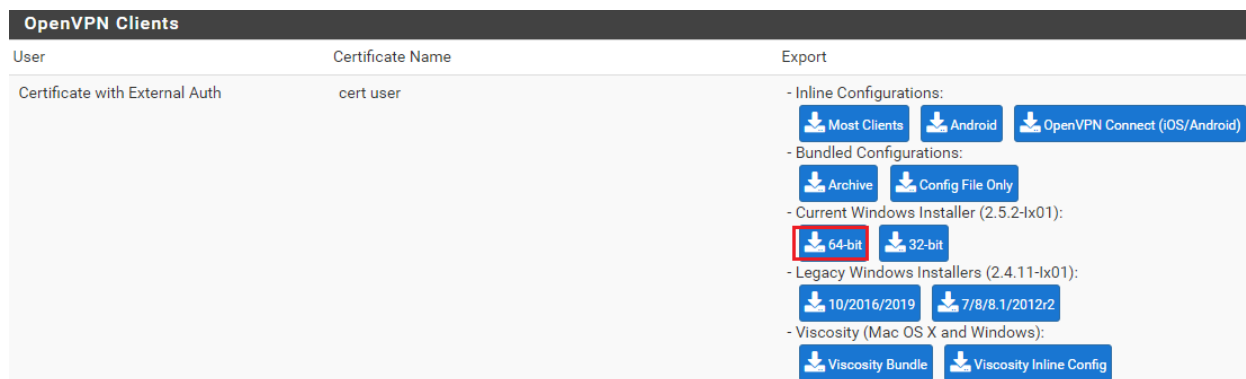
Certificates

Name	Issuer	Distinguished Name	In Use	Actions
webConfigurator default (638f5cda6efd2) Server Certificate CA: No Server: Yes	self-signed	O=pfSense webConfigurator Self-Signed Certificate, CN=pfSense-638f5cda6efd2 Valid From: Tue, 06 Dec 2022 15:16:42 +0000 Valid Until: Mon, 08 Jan 2024 15:16:42 +0000		    
Server Cert Server Certificate CA: No Server: Yes	Tuancm CA	ST=Ha Noi, OU=ATTT, O=HVKTMM, L=Ha Noi, CN=Server Cert, C=VN Valid From: Tue, 06 Dec 2022 08:35:40 +0000 Valid Until: Fri, 03 Dec 2032 08:35:40 +0000	OpenVPN Server	    
cert user User Certificate CA: No Server: No	Tuancm CA	ST=Ha Noi, OU=ATTT, O=HVKTMM, L=Ha Noi, CN=user vpn cert, C=VN Valid From: Tue, 06 Dec 2022 08:44:45 +0000 Valid Until: Fri, 03 Dec 2032 08:44:45 +0000		    

## Bước 7. Cài đặt và trích xuất cấu hình VPN (Openvpn client export)

Tham khảo tài liệu [1] bài 3.2.4.6

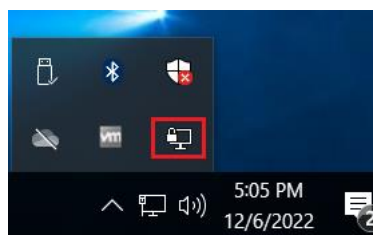
Kết quả:



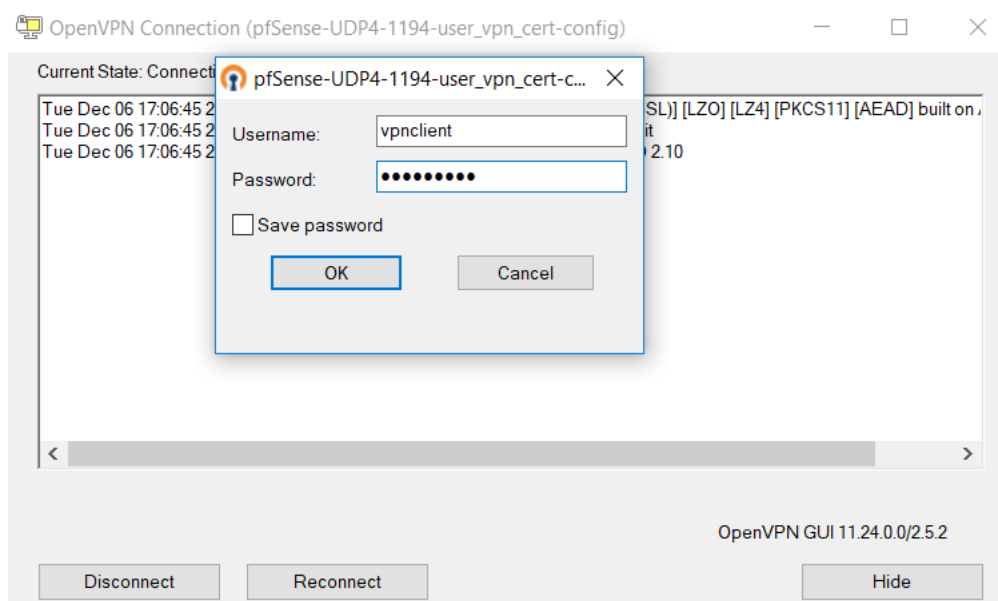
### 3. Thực hiện trên máy Windows 10

Cài đặt gói phần mềm Openvpn vừa trích xuất trên máy chủ PfSense:

Sau khi cài đặt thành công trên máy trạm có biểu tượng kết nối VPN như sau:

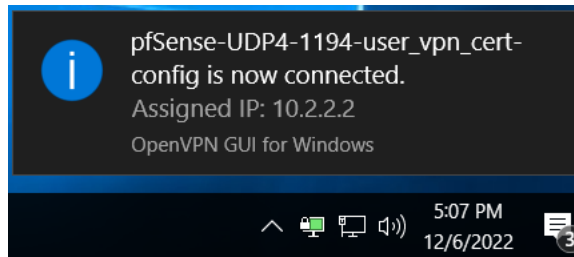


Kết nối VPN tới máy chủ PfSense:



Chương trình yêu cầu tài khoản truy cập. Trong bài này cấu hình xác thực Radius nên tài khoản này là tài khoản đã tạo trong DC.

Kết quả kết nối thành công:



Kiểm tra kết nối tới máy chủ DC:

Ping thành công:

```
C:\Users\tuanc>ping 10.1.1.2

Pinging 10.1.1.2 with 32 bytes of data:
Reply from 10.1.1.2: bytes=32 time=429ms TTL=127
Reply from 10.1.1.2: bytes=32 time=8ms TTL=127
Reply from 10.1.1.2: bytes=32 time=1ms TTL=127
Reply from 10.1.1.2: bytes=32 time=1ms TTL=127
```

Truy cập tới dữ liệu chia sẻ nội bộ thành công:

