

**HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG**

**Cơ sở tại thành phố Hồ Chí Minh**

-----



## **ĐỀ TÀI**

**AN TOÀN MẠNG**

**Chủ đề: THIẾT LẬP FIREWALL TOPOLOGY CHO  
MẠNG DOANH NGHIỆP**

**Giảng viên : Đàm Minh Lịnh**

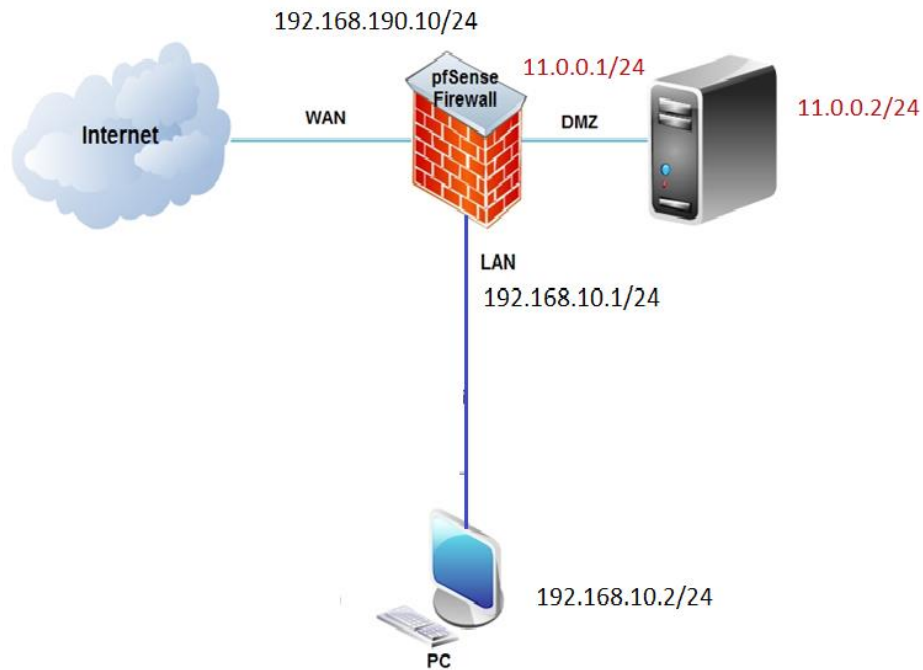
**Sinh viên thực hiện: Trần Ngô Gia Tự – N20DCAT055**

**Ngô Huỳnh Vĩnh Phú – N20DCAT043**

**Lớp: D20CQAT01-N**

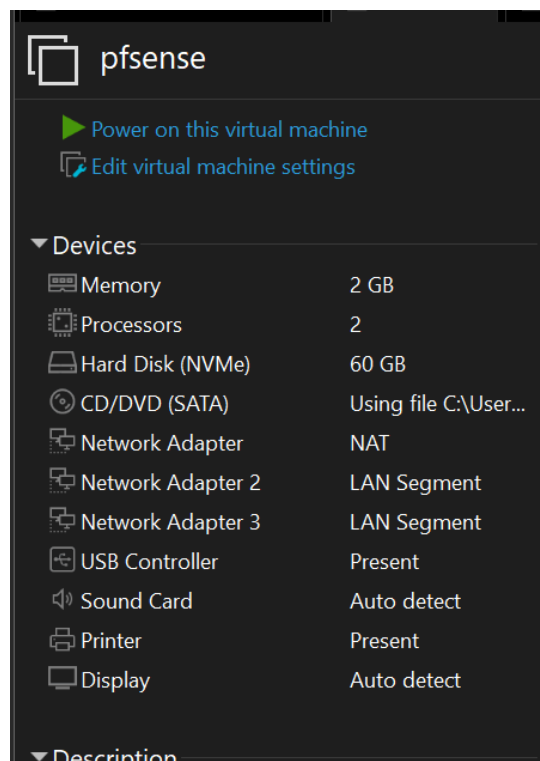
**TP. HỒ CHÍ MINH - 2023**

## I. Sơ đồ:

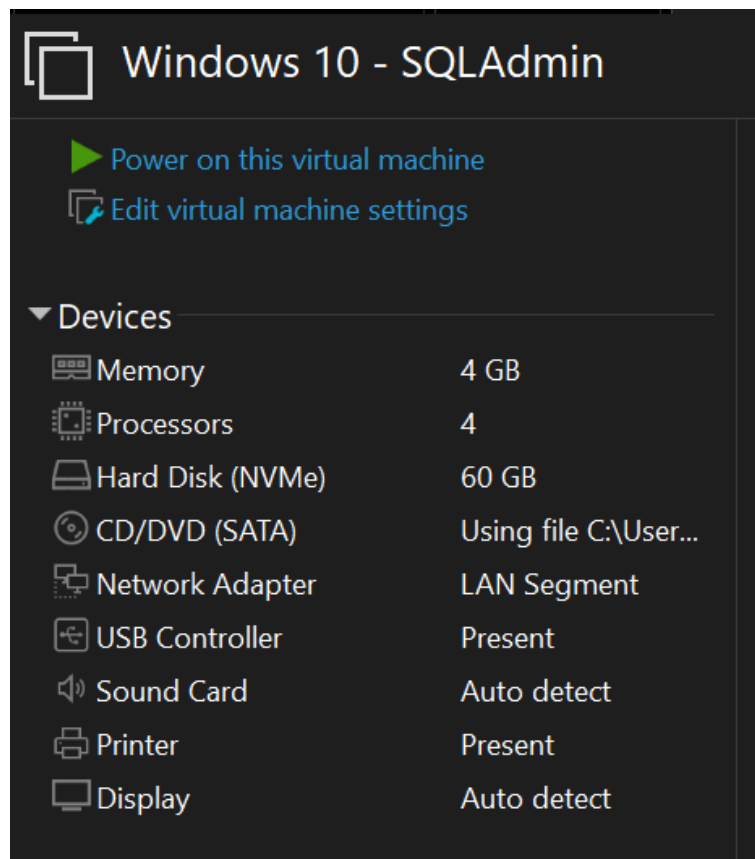


## II. Sơ lược thiết bị:

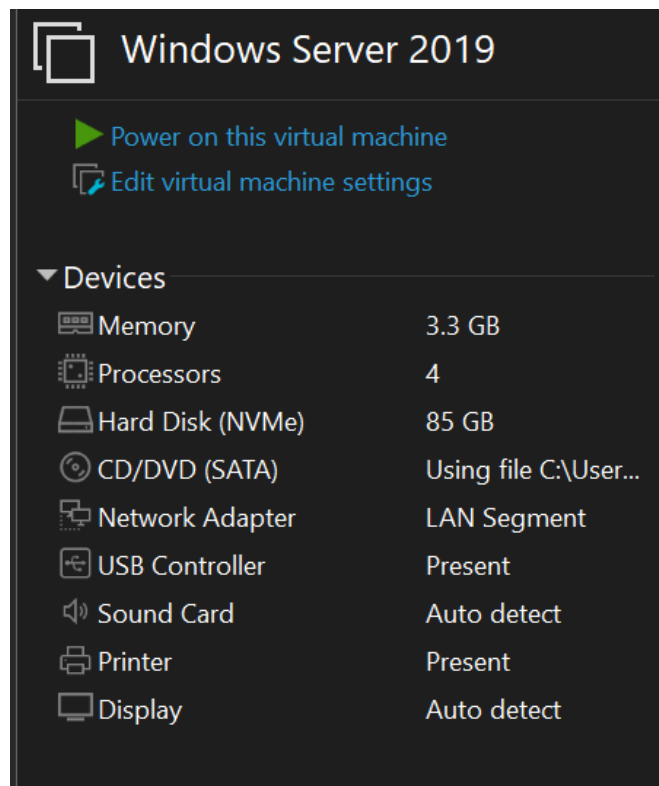
- Tường lửa pfsense:



- Máy LAN: hệ điều hành Win 10.



- Máy DMZ: hệ điều hành Window Server 2019.



## II. Các bước cấu hình:

- Cấu hình interface LAN trên pfsense:

```
Enter an option: 2

Available interfaces:

1 - WAN (em0 - dhcp, dhcp6)
2 - LAN (em1 - static)

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

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

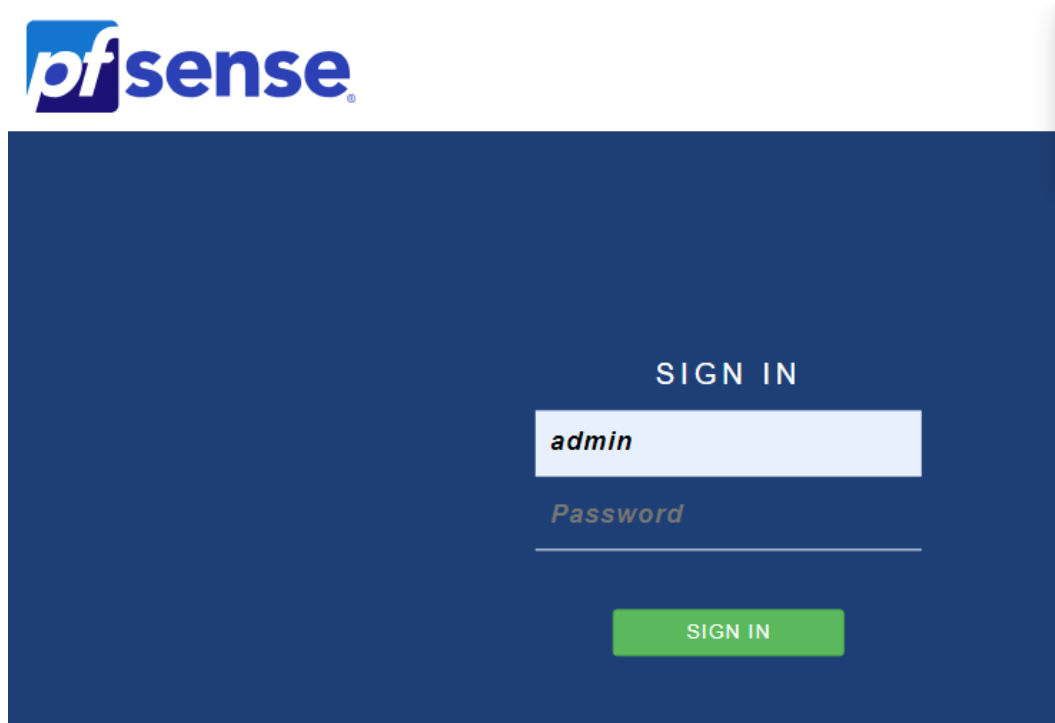
Enter the new LAN IPv4 address. Press <ENTER> for none:
> 192.168.10.1

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

For a WAN, enter the new LAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
> █
```

- Truy cập giao diện cấu hình dạng web của pfsense với tên đăng nhập: admin, password: pfsense.



- Cấu hình domain, hostname, dns.

**General Information**

On this screen the general pfSense parameters will be set.

**Hostname**   
Name of the firewall host, without domain part.  
Examples: pfsense, firewall, edgefw

**Domain**   
Domain name for the firewall.  
Examples: home.arpa, example.com  
Do not end the domain name with '.local' as the final part (Top Level Domain, TLD). The Rendezvous, Airprint, Airplay) and some Windows systems and networked devices. The Alternatives such as 'home.arpa', 'local.lan', or 'mylocal' are safe.

The default behavior of the DNS Resolver will ignore manually configured DNS servers if manually configured DNS servers below for client queries, visit Services > DNS Resolver

**Primary DNS Server**

**Secondary DNS Server**

**Override DNS** ☒  
Allow DNS servers to be overridden by DHCP/PPP on WAN

- Cấu hình thời gian, múi giờ.

Wizard / pfSense Setup / Time Server Information

Step 3 of 9

**Time Server Information**

Please enter the time, date and time zone.

**Time server hostname**   
Enter the hostname (FQDN) of the time server.

**Timezone**

>> Next

- Cấu hình interface WAN.

Wizard / pfSense Setup / Configure WAN Interface

Step 4 of 9

### Configure WAN Interface

On this screen the Wide Area Network information will be configured.

SelectedType: DHCP

#### General configuration

MAC Address:

This field can be used to modify ("spoof") the MAC address of the WAN interface in the following format: xx:xx:xx:xx:xx:xx or leave blank.

- Cấu hình interface LAN.

Wizard / pfSense Setup / Configure LAN Interface

Step 5 of 9

### Configure LAN Interface

On this screen the Local Area Network information will be configured.

LAN IP Address: 192.168.10.1

Type dhcp if this interface uses DHCP to obtain its IP address.

Subnet Mask: 24

>> Next

- Thiết lập lại mật khẩu admin.

Wizard / pfSense Setup / Set Admin WebGUI Password

Step 6 of 9

**Set Admin WebGUI Password**

On this screen the admin password will be set, which is used to access the \

Admin Password

Admin Password AGAIN

[» Next](#)

- Click finish để hoàn thành thao tác.

Step 9 of 9

**Wizard completed.**

**Congratulations! pfSense is now configured.**

We recommend that you check to see if there are any software updates available. Keep things you can do to maintain the security of your network.

[Check for updates](#)

**Remember, we're here to help.**

[Click here](#) to learn about Netgate 24/7/365 support services.

**User survey**

Please help all the people involved in improving and expanding pfSense software by (anonymous)

[Anonymous User Survey](#)

**Useful resources.**

- Learn more about Netgate's product line, services, and pfSense software from [our website](#)
- To learn about Netgate appliances and other offers, [visit our store](#)
- Become part of the pfSense community. Visit our [forum](#)
- Subscribe to our [newsletter](#) for ongoing product information, software announcements, and more.

[Finish](#)

- Thêm vùng DMZ.

Interfaces / Interface Assignments

Interface Assignments
Interface Groups
Wireless
VLANs
QinQs
PPPs
GREs
GIFs
Bridges
LAGGs

Interface	Network port	
WAN	em0 (00:0c:29:0d:bd:9c)	
LAN	em1 (00:0c:29:0d:bd:a6)	Delete
DMZ	em2 (00:0c:29:0d:bd:b0)	Delete
Available network ports:	ovpns1 (VPN Server)	Add

Save

- Cấu hình chi tiết interface DMZ.

General Configuration

Enable

☒ Enable interface

Description

DMZ

Enter a description (name) for the interface here.

IPv4 Configuration Type

Static IPv4

IPv6 Configuration Type

None

MAC Address

xx:xx:xx:xx:xx:xx

This field can be used to modify ("spoof") the MAC address of this interface.  
Enter a MAC address in the following format: xx:xx:xx:xx:xx:xx or leave blank.

MTU

If this field is blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary in some circumstances.

MSS

If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 for IPv4 (TCP/IPv4 header size) and minus 60 for IPv6 (TCP/IPv6 header size) will be in effect.

Speed and Duplex

Default (no preference, typically autoselect)

Explicitly set speed and duplex mode for this interface.  
WARNING: MUST be set to autoselect (automatically negotiate speed) unless the port this interface connects to has its speed and duplex forced.

Static IPv4 Configuration

IPv4 Address

11.0.0.1

/ 24

IPv4 Upstream

None

Add a new gateway



- DMZ sử dụng ip tĩnh.

```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ipconfig

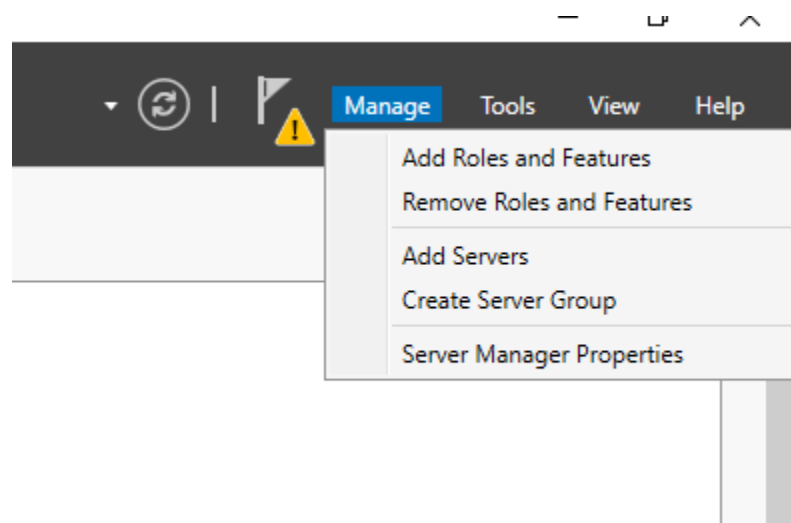
Windows IP Configuration

Ethernet adapter Ethernet0:

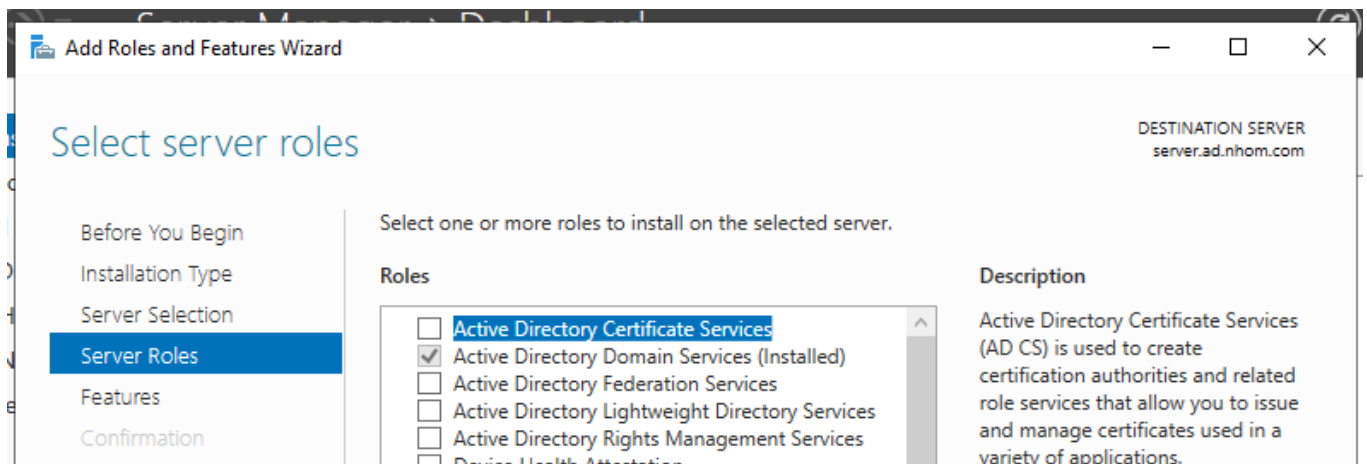
    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::55ea:ed73:70ad:7c95%15
    IPv4 Address. . . . . : 11.0.0.2
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 11.0.0.1

C:\Users\Administrator>
```

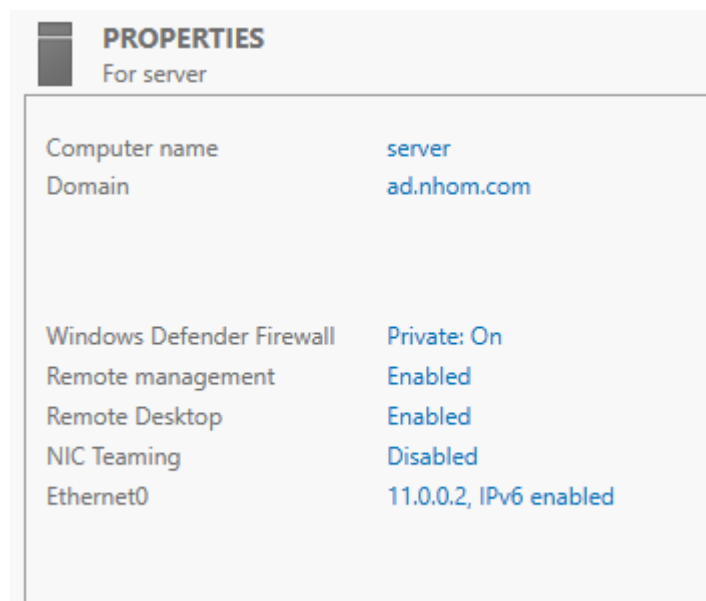
- Cấu hình lên AD cho DMZ.
  - + Chọn Manage → Add Roles and Features.



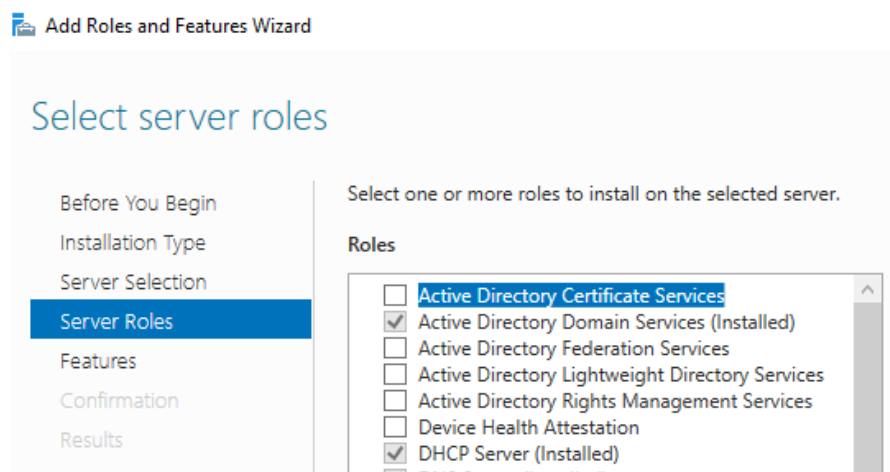
+ Chọn dịch vụ Active Directory Certificate Services.



+ Máy DMZ đã lên domain sẵn.

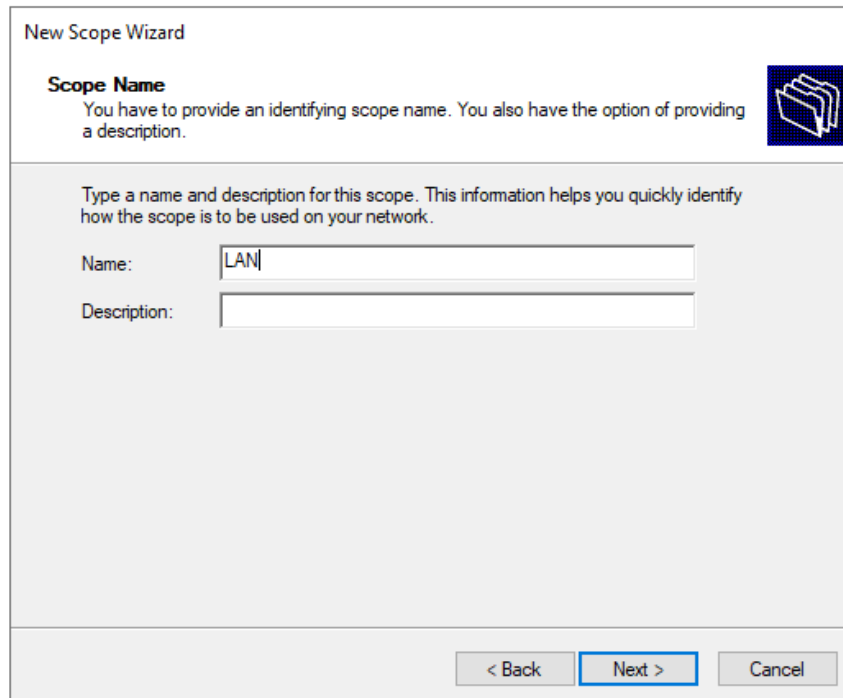


- Cài đặt dịch vụ DHCP cho máy DMZ.



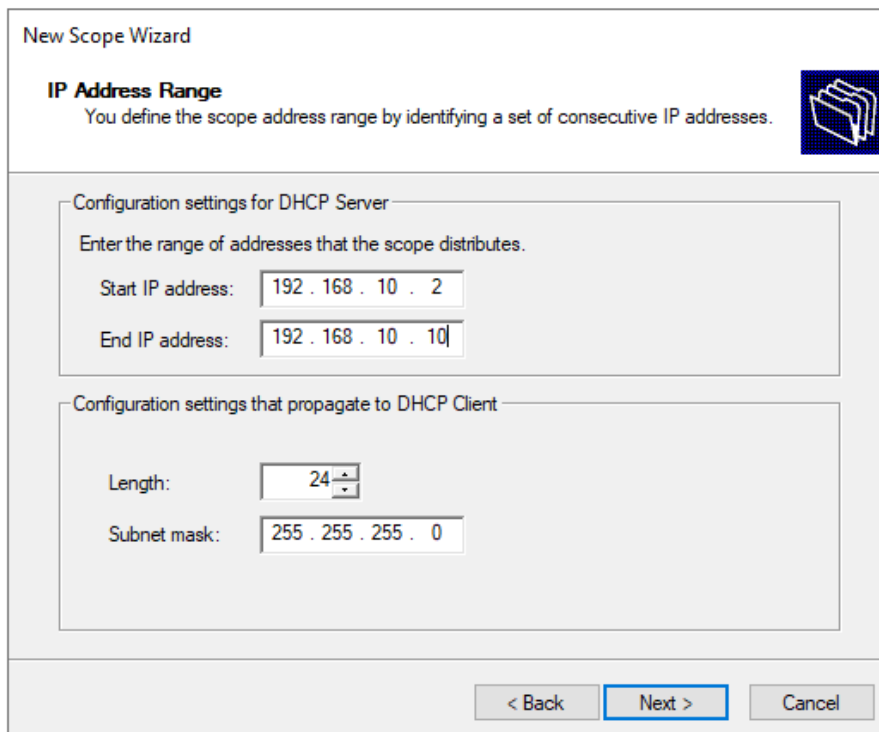
- Cấu hình chi tiết dịch vụ DHCP trên máy DMZ.

+ Tạo Scope trên DHCP Server.



The image shows the 'New Scope Wizard' window, specifically the 'Scope Name' step. The title bar says 'New Scope Wizard'. Below the title, there's a section titled 'Scope Name' with a sub-instruction: 'You have to provide an identifying scope name. You also have the option of providing a description.' To the right of this text is a small icon of a folder. Below the instruction, there's a text box for 'Name' containing the text 'LAN' and an empty text box for 'Description'. At the bottom right, there are three buttons: '< Back', 'Next >' (which is highlighted with a blue border), and 'Cancel'.

+ Cấu hình dải IP tĩnh.



The image shows the 'New Scope Wizard' window, specifically the 'IP Address Range' step. The title bar says 'New Scope Wizard'. Below the title, there's a section titled 'IP Address Range' with a sub-instruction: 'You define the scope address range by identifying a set of consecutive IP addresses.' To the right of this text is a small icon of a folder. Below the instruction, there's a section titled 'Configuration settings for DHCP Server' with a sub-instruction: 'Enter the range of addresses that the scope distributes.' This section contains two text boxes: 'Start IP address:' with the value '192 . 168 . 10 . 2' and 'End IP address:' with the value '192 . 168 . 10 . 10'. Below this, there's another section titled 'Configuration settings that propagate to DHCP Client' containing two text boxes: 'Length:' with the value '24' and 'Subnet mask:' with the value '255 . 255 . 255 . 0'. At the bottom right, there are three buttons: '< Back', 'Next >' (which is highlighted with a blue border), and 'Cancel'.

## + Cấu hình Default Gateway.

New Scope Wizard

**Router (Default Gateway)**  
You can specify the routers, or default gateways, to be distributed by this scope.

To add an IP address for a router used by clients, enter the address below.

IP address:

192 . 168 . 10 . 1

Add

Remove

Up

Down

< Back Next > Cancel

## + Cấu hình thêm DNS.

New Scope Wizard

**Domain Name and DNS Servers**  
The Domain Name System (DNS) maps and translates domain names used by clients on your network.

You can specify the parent domain you want the client computers on your network to use for DNS name resolution.

Parent domain: ad.nhom.com

To configure scope clients to use DNS servers on your network, enter the IP addresses for those servers.

Server name:

IP address:

11 . 0 . 0 . 2

Add

Remove

Up

Down

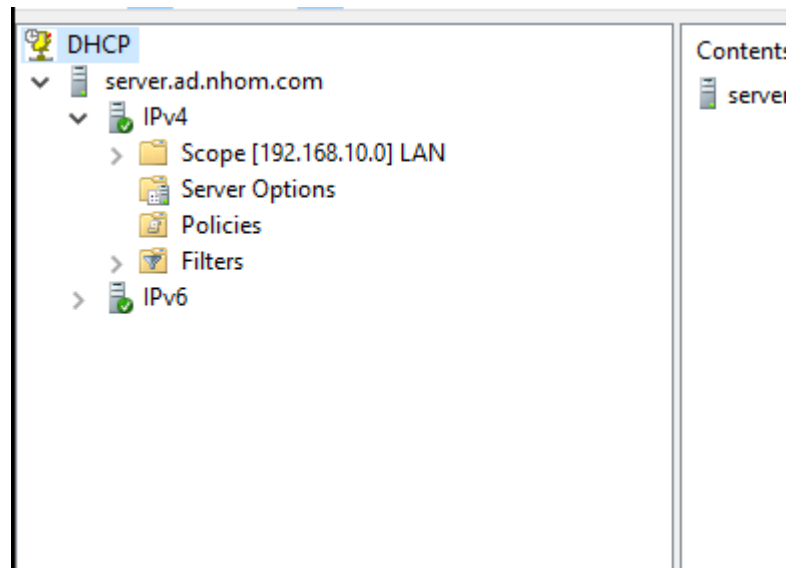
8.8.8.8

8.8.4.4

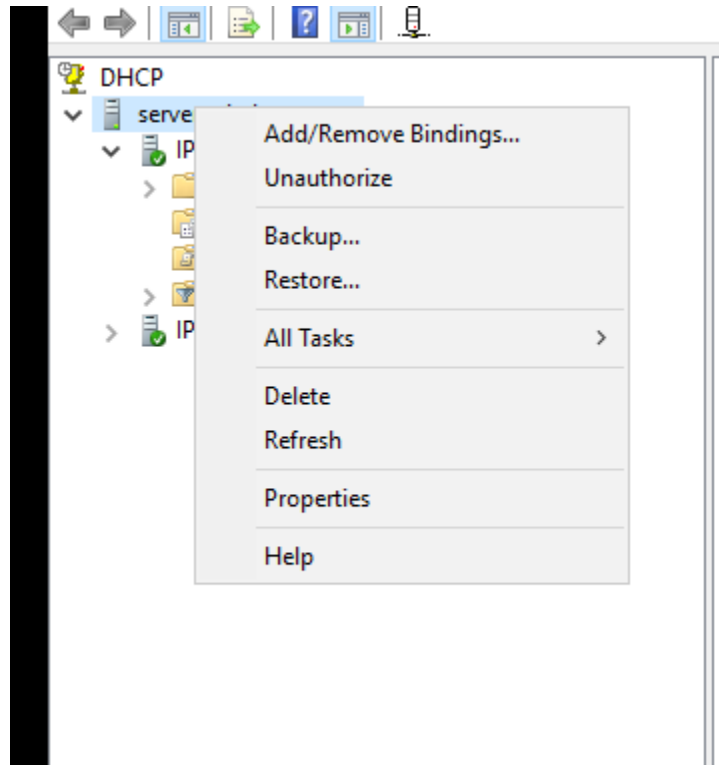
Resolve

< Back Next > Cancel

+ Tạo thành công.



+ Ủy quyền DHCP Server.



- Cấu hình DHCP Relay trên pfsense.

Services / DHCP Relay

### DHCP Relay Configuration

**Enable** ☒ Enable DHCP Relay on interface

**Interface(s)** WAN  
LAN  
DMZ

Interfaces without an IP address will not be shown.

**CARP Status VIP** none

Used to determine the HA MASTER/BACKUP status. DHCP Relay will be stopped when the interface is in BACKUP status and started in MASTER status.

☐ Append circuit ID and agent ID to requests  
If this is checked, the DHCP Relay will append the circuit ID (pfSense interface number) and request.

**Destination server** 11.0.0.2

This is the IPv4 address of the server to which DHCP requests are relayed.

**Save** **+ Add server**

- Máy LAN đã có IP.

```

C:\Users\tranj>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet0:

    Connection-specific DNS Suffix  . : ad.nhom.com
    Link-local IPv6 Address . . . . . : fe80::8a21:b8dc:c6f7:a831%5
    IPv4 Address. . . . . : 192.168.10.2
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.10.1

Ethernet adapter Bluetooth Network Connection:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

C:\Users\tranj>

```

#### IV. Cấu hình NAT.

## - Cấu hình NAT Port Forward.

Firewall / NAT / Port Forward

Port Forward 1:1 Outbound NPT

Rules										
<input type="checkbox"/>	Interface	Protocol	Source Address	Source Ports	Dest. Address	Dest. Ports	NAT IP	NAT Ports	Description	Actions
<input type="checkbox"/>	<input checked="" type="checkbox"/> WAN	TCP/UDP	*	80 (HTTP)	WAN address	80 (HTTP)	DMZ address	80 (HTTP)		
<input type="checkbox"/>	<input checked="" type="checkbox"/> WAN	TCP/UDP	*	80 (HTTP)	WAN address	80 (HTTP)	LAN address	80 (HTTP)		
<input type="checkbox"/>	<input checked="" type="checkbox"/> WAN	TCP/UDP	*	443 (HTTPS)	WAN address	443 (HTTPS)	DMZ address	443 (HTTPS)		
<input type="checkbox"/>	<input checked="" type="checkbox"/> WAN	TCP/UDP	*	443 (HTTPS)	WAN address	443 (HTTPS)	LAN address	443 (HTTPS)		

Add Add Delete Toggle Save Separator

Legend

## - Cấu hình cho interface LAN.

+ HTTP.

Choose which protocol this rule should match. In most cases TCP is specified.

Source

Source ☐ Invert match. Any / Address/mask

Source port range HTTP From port Custom HTTP To port Custom

Specify the source port or port range for this rule. This is usually random and almost never equal to the destination port range (and should usually be 'any'). The 'to' field may be left empty if only filtering a single port.

Destination ☐ Invert match. WAN address / Address/mask

Destination port range HTTP From port Custom HTTP To port Custom

Specify the port or port range for the destination of the packet for this mapping. The 'to' field may be left empty if only mapping a single port.

Redirect target IP LAN address Address

Enter the internal IP address of the server on which to map the ports. e.g.: 192.168.1.12 for IPv4  
In case of IPv6 addresses, it must be from the same "scope", i.e. it is not possible to redirect from link-local addresses scope (fe80::) to local scope (::1)

Redirect target port HTTP Port Custom

Specify the port on the machine with the IP address entered above. In case of a port range, specify the beginning port of the range (the end port will be calculated automatically). This is usually identical to the "From port" above.

## + HTTPS

Address Family

IPv4

Select the Internet Protocol version this rule applies to.

Protocol

TCP/UDP

Choose which protocol this rule should match. In most cases "TCP" is specified.

Source

Hide Advanced

Source

☐ Invert match.

Any

Type

Address/mask

Source port range

HTTPS

From port

Custom

HTTPS

To port

Custom

Specify the source port or port range for this rule. This is usually random and almost never equal to the destination port range (and should usually be 'any'). The 'to' field may be left empty if only filtering a single port.

Destination

☐ Invert match.

WAN address

Type

Address/mask

Destination port range

HTTPS

From port

Custom

HTTPS

To port

Custom

Specify the port or port range for the destination of the packet for this mapping. The 'to' field may be left empty if only mapping a single port.

Redirect target IP

LAN address

Type

Address

Enter the internal IP address of the server on which to map the ports. e.g.: 192.168.1.12 for IPv4  
In case of IPv6 addresses, it must be from the same "scope", i.e. it is not possible to redirect from link-local addresses scope (fe80:\*) to local scope (::1)

Redirect target port

HTTPS

Port

Custom

Restore pages

Microsoft Edge closed unexpectedly.

## - Cấu hình NAT cho DMZ.

### + HTTP

Address Family

IPv4

Select the Internet Protocol version this rule applies to.

Protocol

TCP/UDP

Choose which protocol this rule should match. In most cases "TCP" is specified.

Source

Hide Advanced

Source

☐ Invert match.

Any

Type

Address/mask

Source port range

HTTP

From port

Custom

HTTP

To port

Custom

Specify the source port or port range for this rule. This is usually random and almost never equal to the destination port range (and should usually be 'any'). The 'to' field may be left empty if only filtering a single port.

Destination

☐ Invert match.

WAN address

Type

Address/mask

Destination port range

HTTP

From port

Custom

HTTP

To port

Custom

Specify the port or port range for the destination of the packet for this mapping. The 'to' field may be left empty if only mapping a single port.

Redirect target IP

DMZ address

Type

Address

Enter the internal IP address of the server on which to map the ports. e.g.: 192.168.1.12 for IPv4  
In case of IPv6 addresses, it must be from the same "scope", i.e. it is not possible to redirect from link-local addresses scope (fe80:\*) to local scope (::1)

Redirect target port

HTTP

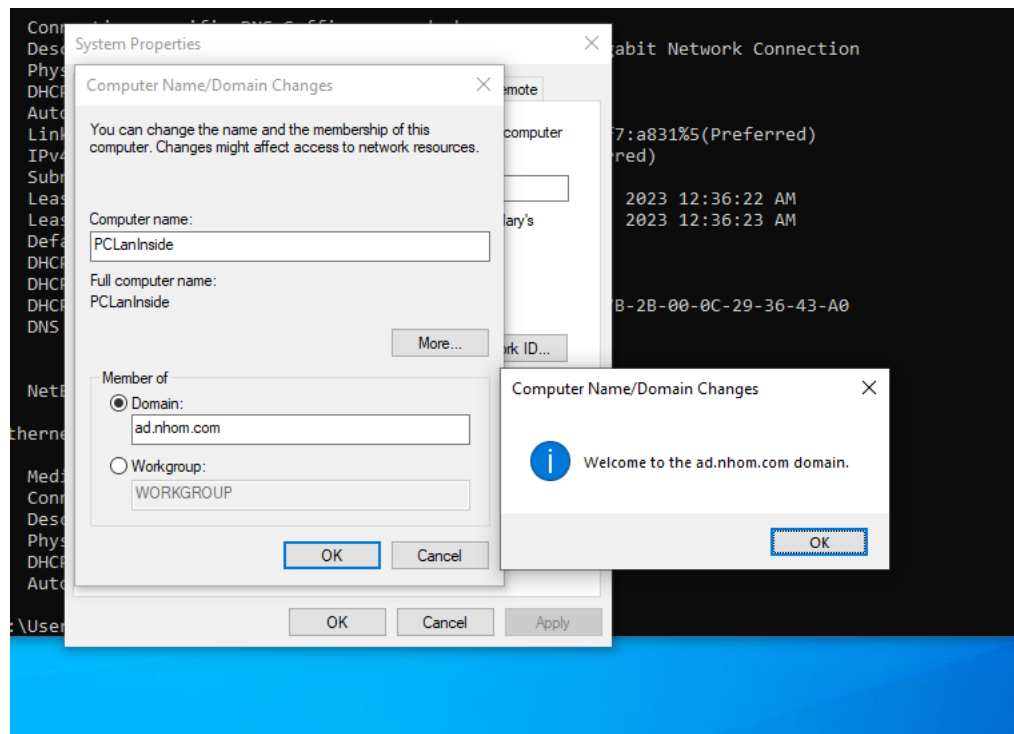
Port

Custom

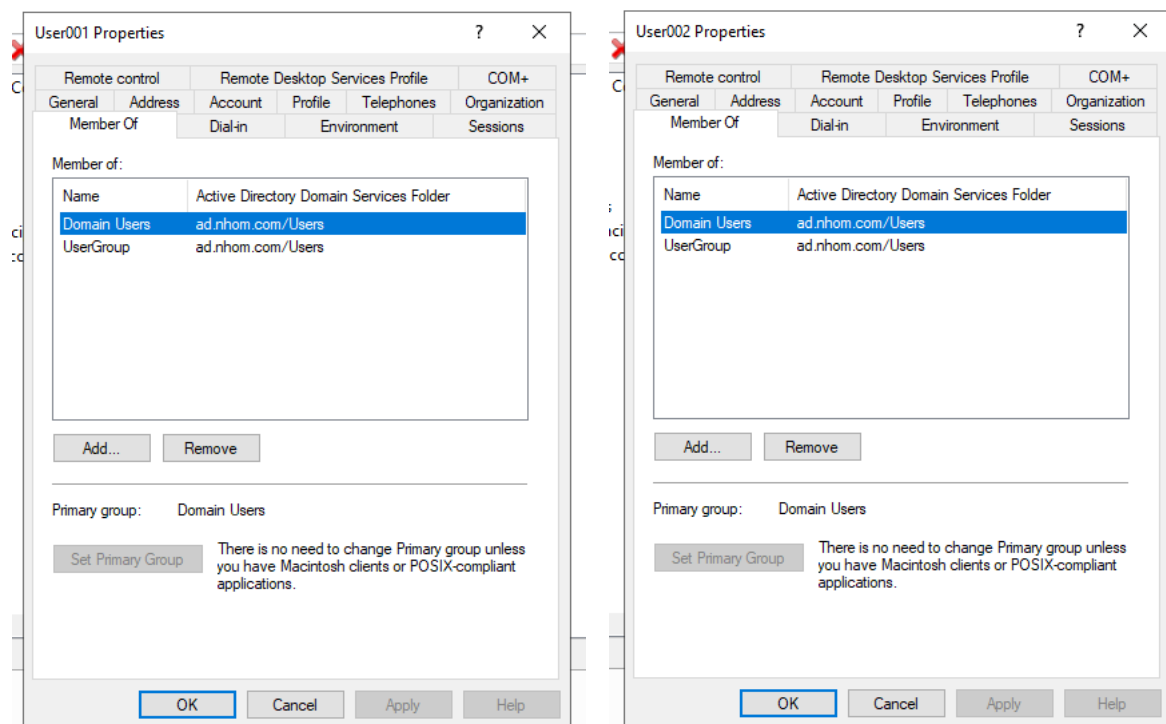


## V. Tạo user và join domain.

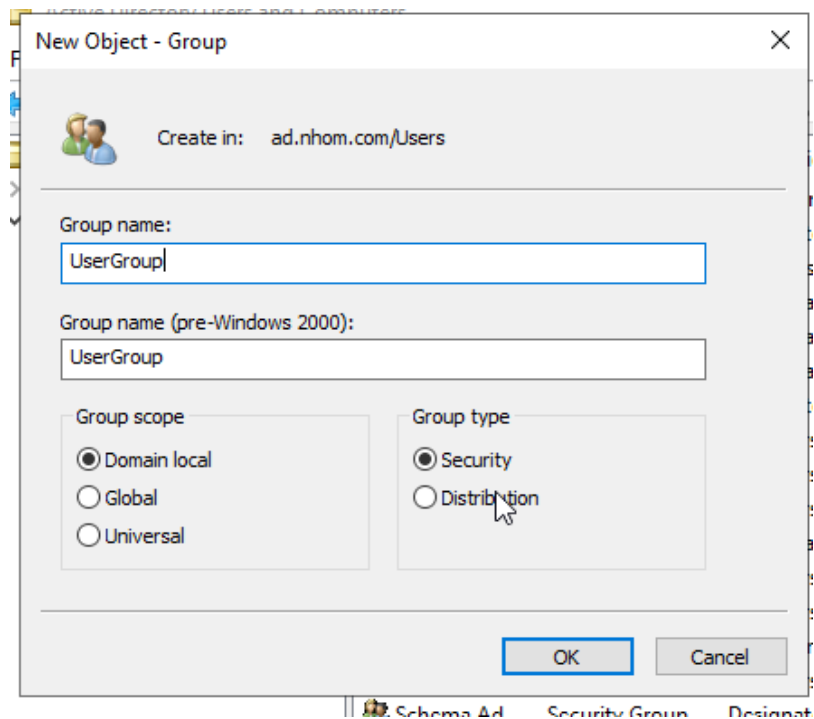
- Join domain cho máy LAN.



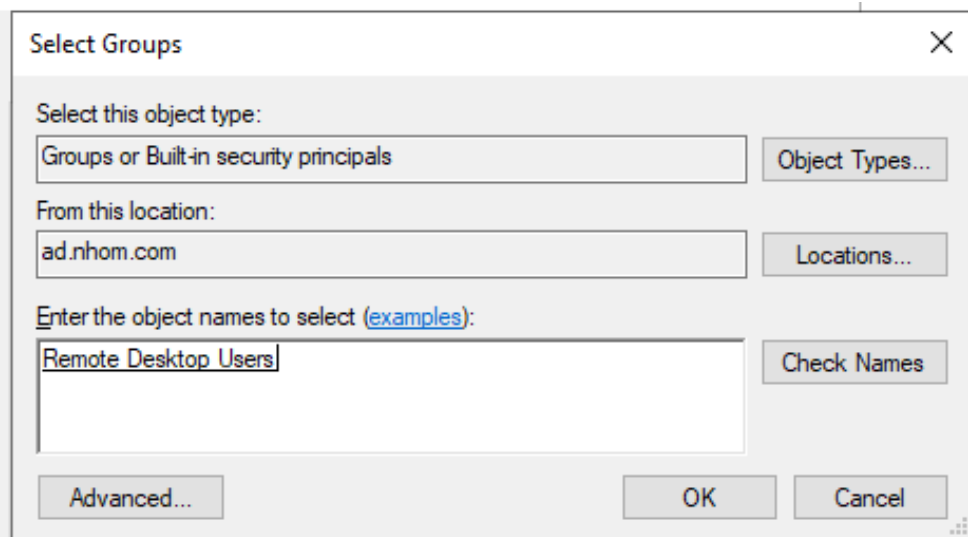
- Tạo hai user lần lượt User001 và User002.



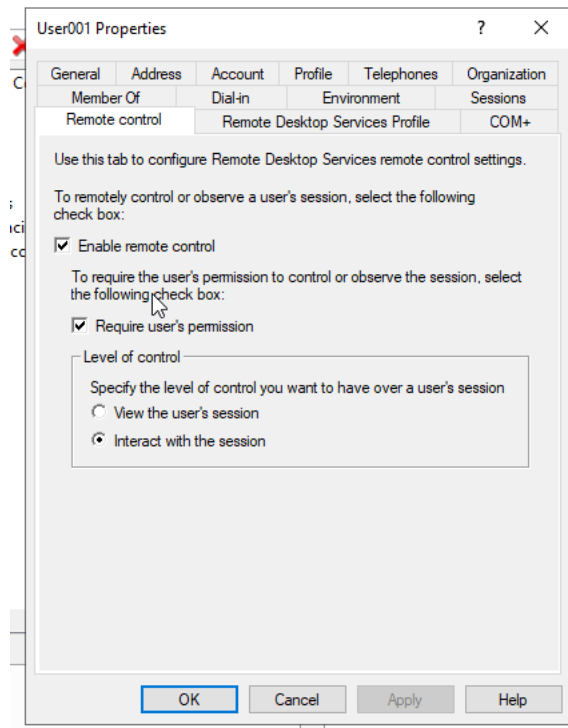
- Tạo group chứa các user.



- Gán quyền User control cho User001.



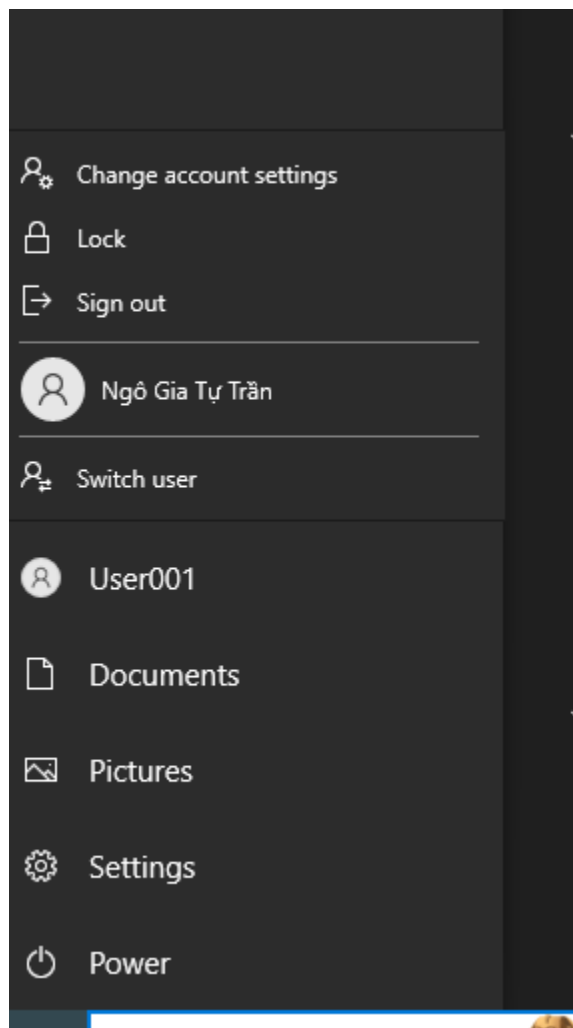
- Cho User001 gia nhập và tương tác với phiên.



- Đăng nhập Win 10 với user vừa mới khởi tạo.



- Đăng nhập thành công.



## **VI. Remote từ máy LAN đến DMZ.**

- Ping từ máy LAN đến DMZ.

```
Command Prompt
Microsoft Windows [Version 10.0.19045.3570]
(c) Microsoft Corporation. All rights reserved.

C:\Users\User001>ping 11.0.0.2

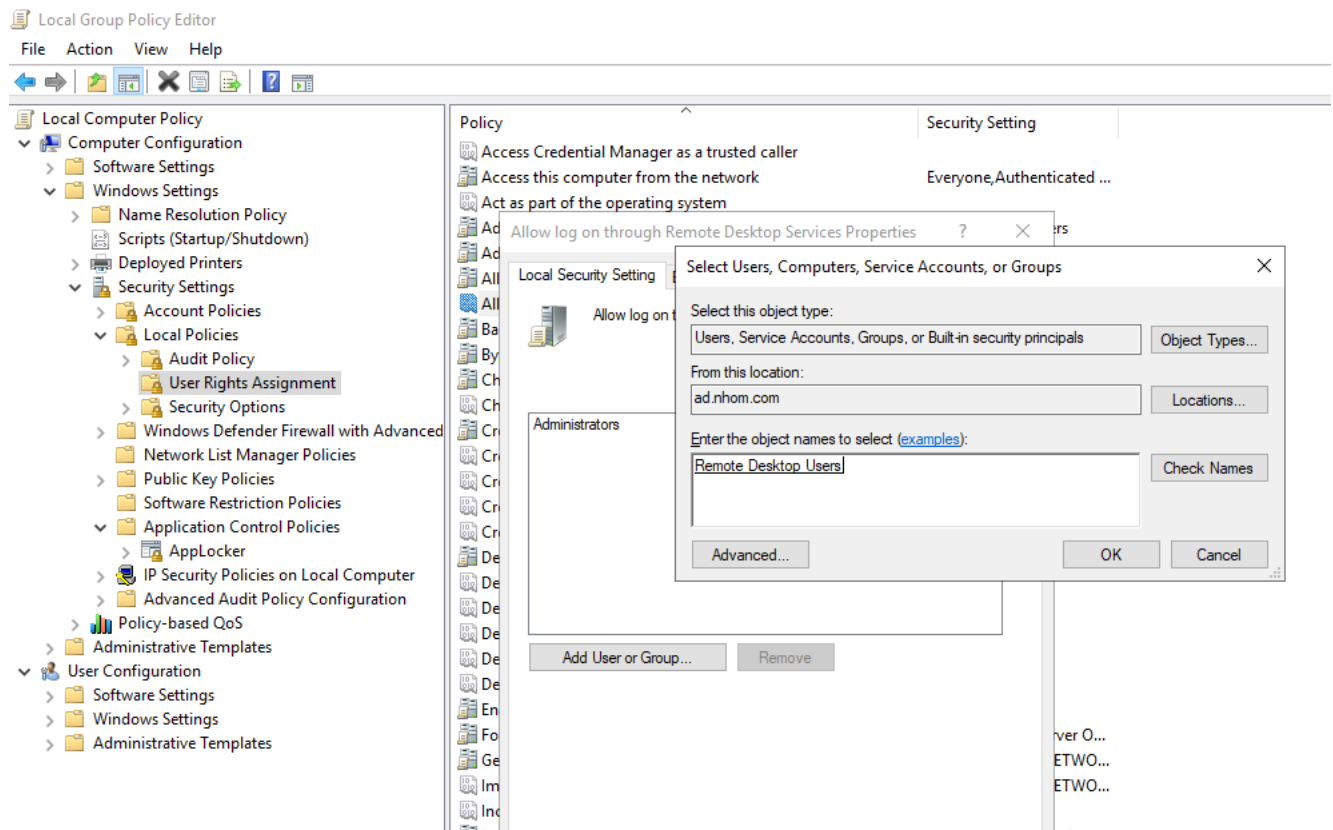
Pinging 11.0.0.2 with 32 bytes of data:
Reply from 11.0.0.2: bytes=32 time=1ms TTL=127
Reply from 11.0.0.2: bytes=32 time=1ms TTL=127
Reply from 11.0.0.2: bytes=32 time=1ms TTL=127
Reply from 11.0.0.2: bytes=32 time=1ms TTL=127

Ping statistics for 11.0.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0%
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms

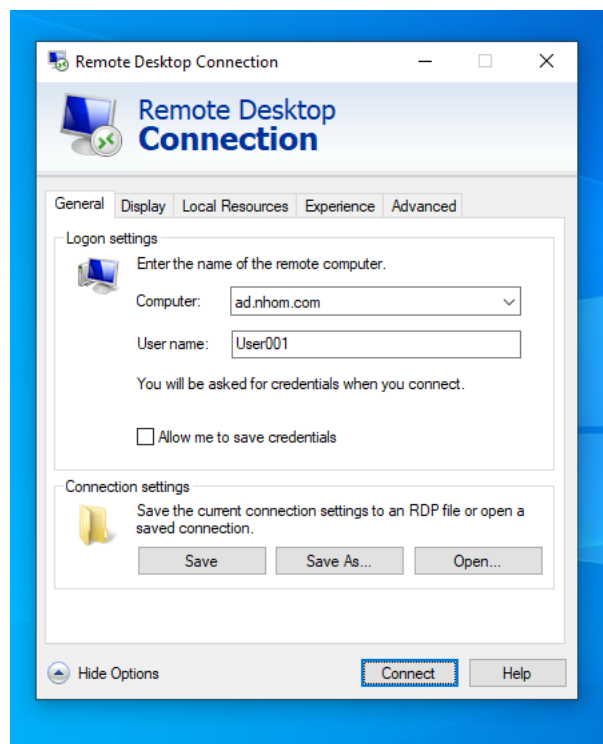
C:\Users\User001>
```

- Remote đến của Window Server 2019.

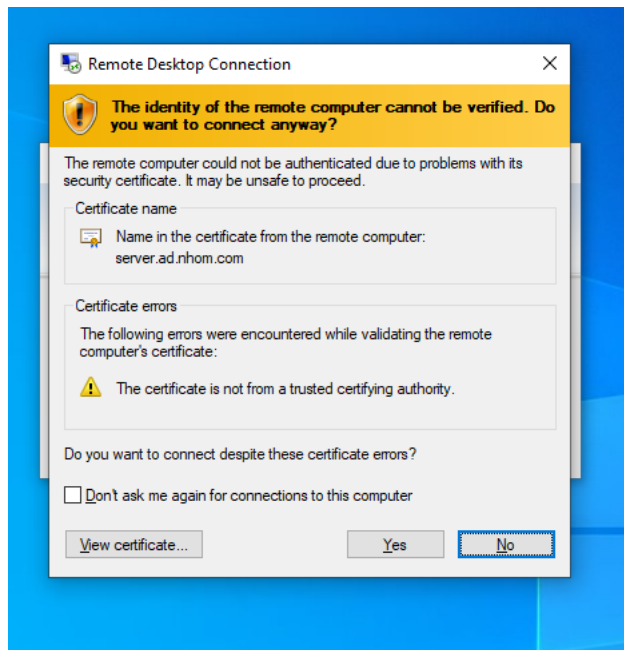
+ Thiết lập lại quyền remote.



+ Remote từ User001.



+ Xác nhận kết nối.

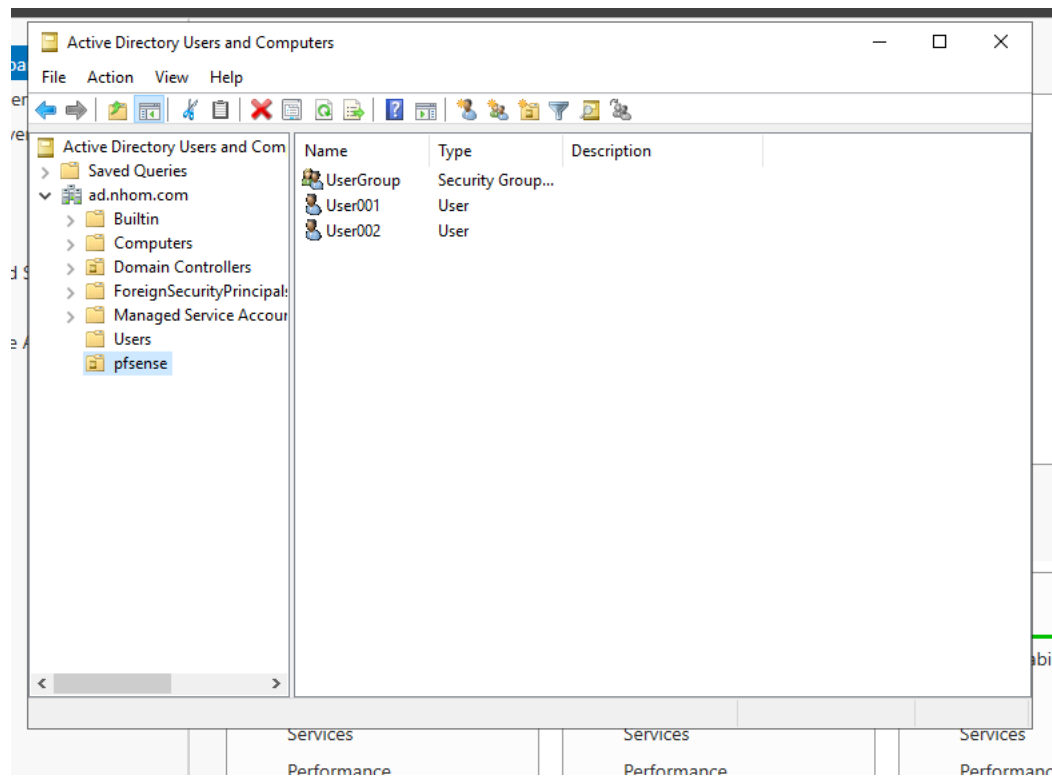


+ Remote thành công.

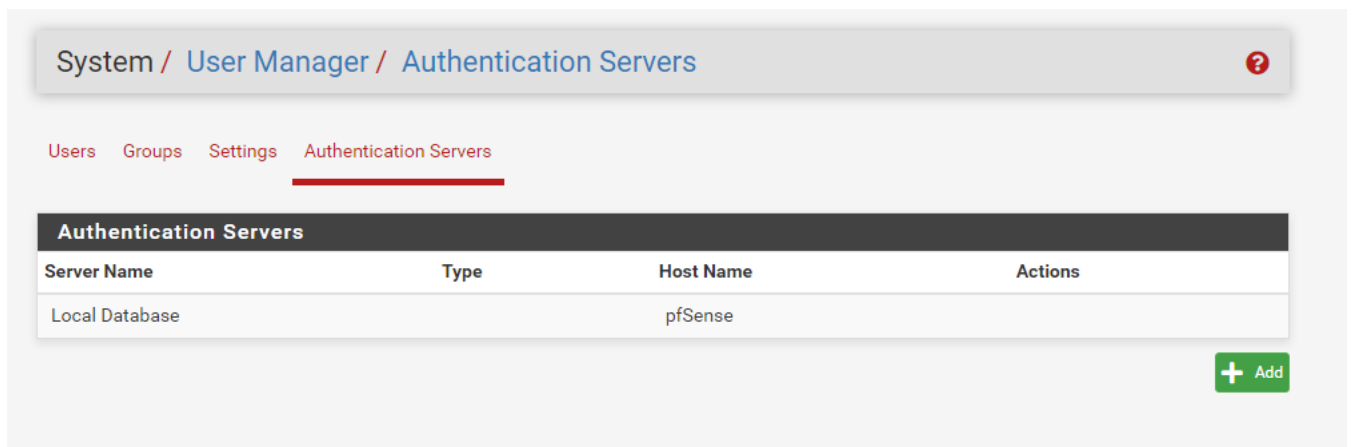


## VII. Triển khai dịch vụ OpenVPN và RDP từ máy vật lý vào máy LAN.

- Tạo Organization Unit cho Group lần hai User mang tên pfsense.



- Truy cập firewall pfsense tạo authentication server xác thực server DMZ.

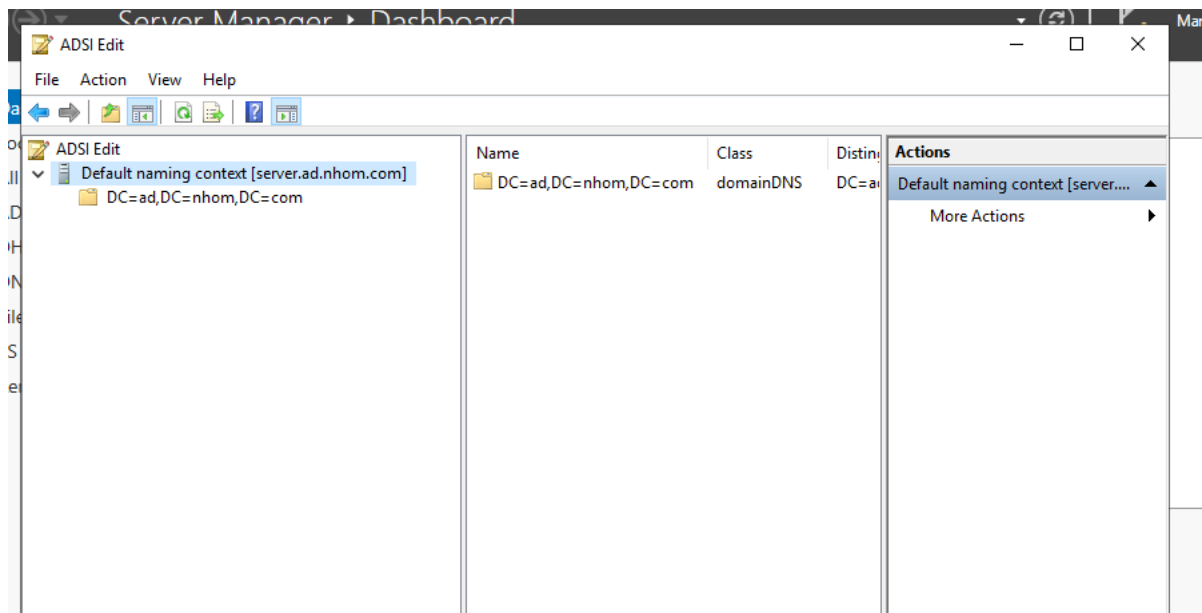


- Gán IP của máy Window Server.

The screenshot shows the 'LDAP Server Settings' configuration window. It includes fields for 'Descriptive name' (ActiveDirectory), 'Type' (LDAP), 'Hostname or IP address' (11.0.0.2), 'Port value' (389), 'Transport' (Standard TCP), 'Peer Certificate Authority' (Global Root CA List), 'Protocol version' (3), 'Server Timeout' (25), and 'Search scope' (Level, Entire Subtree). A note states: 'NOTE: When using SSL/TLS or STARTTLS, this hostname MUST match a Subject Alternative Name (SAN) or the Common Name (CN) of the LDAP server SSL/TLS Certificate.'

<b>Descriptive name</b>	ActiveDirectory
<b>Type</b>	LDAP
<b>LDAP Server Settings</b>	
<b>Hostname or IP address</b>	11.0.0.2 <small>NOTE: When using SSL/TLS or STARTTLS, this hostname MUST match a Subject Alternative Name (SAN) or the Common Name (CN) of the LDAP server SSL/TLS Certificate.</small>
<b>Port value</b>	389
<b>Transport</b>	Standard TCP
<b>Peer Certificate Authority</b>	Global Root CA List <small>This CA is used to validate the LDAP server certificate when 'SSL/TLS Encrypted' or 'STARTTLS Encrypted' Transport is active. This CA must match the CA used by the LDAP server.</small>
<b>Protocol version</b>	3
<b>Server Timeout</b>	25 <small>Timeout for LDAP operations (seconds)</small>
<b>Search scope</b>	Level Entire Subtree

- Sử dụng công cụ ADSI để truy xuất thông tin Base DN, Authentication containers, Bind credentials.





<div> <div>ADSI Edit</div> <div> <div>Default naming context [server.ad.nhom.com]</div> <div> <div>DC=ad,DC=nhom,DC=com</div> </div> </div> </div>			
Name	Class	Distinguished Name	
CN=Builtin	builtinDomain	CN=Builtin,DC=ad,DC=nhom,DC=com	
CN=Computers	container	CN=Computers,DC=ad,DC=nhom,DC=com	
OU=Domain Controllers	organization...	OU=Domain Controllers,DC=ad,DC=nhom,DC=com	
CN=ForeignSecurityPrincip...	container	CN=ForeignSecurityPrincipals,DC=ad,DC=nhom,DC=com	
CN=Keys	container	CN=Keys,DC=ad,DC=nhom,DC=com	
CN=LostAndFound	lostAndFound	CN=LostAndFound,DC=ad,DC=nhom,DC=com	
CN=Managed Service Acco...	container	CN=Managed Service Accounts,DC=ad,DC=nhom,DC=com	
CN=NTDS Quotas	msDS-Quota...	CN=NTDS Quotas,DC=ad,DC=nhom,DC=com	
OU=pfsense	organization...	OU=pfsense,DC=ad,DC=nhom,DC=com	
CN=Program Data	container	CN=Program Data,DC=ad,DC=nhom,DC=com	
CN=System	container	CN=System,DC=ad,DC=nhom,DC=com	
CN=TPM Devices	msTPM-Info...	CN=TPM Devices,DC=ad,DC=nhom,DC=com	
CN=Users	container	CN=Users,DC=ad,DC=nhom,DC=com	
CN=Infrastructure	infrastructur...	CN=Infrastructure,DC=ad,DC=nhom,DC=com	

<div> <div>ADSI Edit</div> <div> <div>Default naming context [server.ad.nhom.com]</div> <div> <div>DC=ad,DC=nhom,DC=com</div> <div> <div>CN=Builtin</div> <div>CN=Computers</div> <div>OU=Domain Controllers</div> <div>CN=ForeignSecurityPrincipals</div> <div>CN=Keys</div> <div>CN=LostAndFound</div> <div>CN=Managed Service Accounts</div> <div>CN=NTDS Quotas</div> <div>OU=pfsense</div> <div>CN=Program Data</div> <div>CN=System</div> <div>CN=TPM Devices</div> <div>CN=Users</div> </div> </div> </div> </div>			
Name	Class	Distinguished Name	
CN=Admin	user	CN=Admin,CN=Users,DC=ad,DC=nhom,DC=com	
CN=Administrator	user	CN=Administrator,CN=Users,DC=ad,DC=nhom,DC=com	
CN=Allowed RODC Passwo...	group	CN=Allowed RODC Password Replication Group,CN=Users,DC=ad,DC=nhom,DC=com	
CN=Cert Publishers	group	CN=Cert Publishers,CN=Users,DC=ad,DC=nhom,DC=com	
CN=Cloneable Domain Co...	group	CN=Cloneable Domain Controllers,CN=Users,DC=ad,DC=nhom,DC=com	
CN=Denied RODC Passwor...	group	CN=Denied RODC Password Replication Group,CN=Users,DC=ad,DC=nhom,DC=com	
CN=DHCP Administrators	group	CN=DHCP Administrators,CN=Users,DC=ad,DC=nhom,DC=com	
CN=DHCP Users	group	CN=DHCP Users,CN=Users,DC=ad,DC=nhom,DC=com	
CN=DnsAdmins	group	CN=DnsAdmins,CN=Users,DC=ad,DC=nhom,DC=com	
CN=DnsUpdateProxy	group	CN=DnsUpdateProxy,CN=Users,DC=ad,DC=nhom,DC=com	
CN=Domain Admins	group	CN=Domain Admins,CN=Users,DC=ad,DC=nhom,DC=com	
CN=Domain Computers	group	CN=Domain Computers,CN=Users,DC=ad,DC=nhom,DC=com	
CN=Domain Controllers	group	CN=Domain Controllers,CN=Users,DC=ad,DC=nhom,DC=com	
CN=Domain Guests	group	CN=Domain Guests,CN=Users,DC=ad,DC=nhom,DC=com	
CN=Domain Users	group	CN=Domain Users,CN=Users,DC=ad,DC=nhom,DC=com	
CN=Enterprise Admins	group	CN=Enterprise Admins,CN=Users,DC=ad,DC=nhom,DC=com	
CN=Enterprise Key Admins	group	CN=Enterprise Key Admins,CN=Users,DC=ad,DC=nhom,DC=com	

Search scope	Level	Entire Subtree
	Base DN	DC=ad,DC=nhom,DC=com
Authentication containers	OU=pfsense,DC=ad,DC=nhom,DC=com	<div>Select a container</div> <p>Note: Semi-Colon separated. This will be prepended to the search base dn above or the full container path can be specified containing a dc= component. Example: CN=Users;DC=example,DC=com or OU=Staff;OU=Freelancers</p>
Extended query	<input type="checkbox"/> Enable extended query	
Bind anonymous	<input type="checkbox"/> Use anonymous binds to resolve distinguished names	
Bind credentials	CN=Administrator,CN=Users,DC=ad,DC=nhom,DC=com	*****

## - Thiết lập user manager.

Settings

Session timeout

Time in minutes to expire idle management sessions. The default is 4 hours (240 minutes). Enter 0 to never expire sessions. NOTE: This is a security risk!

Authentication Server

ActiveDirectory

Password Hash Algorithm

bcrypt – Blowfish-based crypt

Selects which algorithm the firewall will use when creating hashes for local user passwords. The most secure option is currently bcrypt. Some users may prefer SHA-512-based crypt hashes for compatibility or compliance purposes.

Shell Authentication

☐ Use Authentication Server for Shell Authentication  
 If RADIUS or LDAP server is selected it is used for console and SSH authentication. Otherwise, the Local Database is used. To allow logins with RADIUS credentials, equivalent local users with the expected privileges must be created first. To allow logins with LDAP credentials, Shell Authentication Group DN must be specified on the LDAP server configuration page.

Auth Refresh Time

Time in seconds to cache authentication results. The default is 30 seconds, maximum 3600 (one hour). Shorter times result in more frequent queries to authentication servers.

Save

Save & Test

## - Kết nối thành công.

LDAP settings

Test results

Attempting connection to	11.0.0.2	OK
Attempting bind to	11.0.0.2	OK
Attempting to fetch Organizational Units from	11.0.0.2	OK
Organization units found CN=Users,DC=ad,DC=nhom,DC=com CN=Users,CN=Builtin,DC=ad,DC=nhom,DC=com OU=Domain Controllers,DC=ad,DC=nhom,DC=com OU=pfSense,DC=ad,DC=nhom,DC=com		

- Nhận diện User002 thành công.

User User002 authenticated successfully. This user is a member of groups:

### Authentication Test

Authentication Server

ActiveDirectory

Select the authentication server to test against.

Username

User002

Password

.....

Debug

☐ Set debug flag

Sets the debug flag when performing authentication, which may trigger additional diagnostic entries in the system log (e.g. for LDAP).

Test

- Cấu hình dịch vụ OpenVPN.

Chọn Wizard.

VPN / OpenVPN / Servers

Servers Clients Client Specific Overrides Wizards

### OpenVPN Servers

Interface	Protocol / Port	Tunnel Network	Mode / Crypto	Description	Actions
-----------	-----------------	----------------	---------------	-------------	---------

+ Add

Bắt đầu tiến hành giai đoạn cấu hình.

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

LDAP

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

>> Next

## - Đặt tên server LDAP.

Wizard / OpenVPN Remote Access Server Setup / LDAP Server Selection

Step 1 of 11

LDAP Server Selection

OpenVPN Remote Access Server Setup Wizard

LDAP Authentication Server List

LDAP servers

ActiveDirectory

>> Add new LDAP server

>> Next

## - Tạo chứng chỉ cho giao thức VPN.

Create a New Certificate Authority (CA) Certificate

Descriptive name

CA-VPN-Connection

A name for administrative reference, to identify this certificate.

Randomize Serial

☒ Use random serial numbers when signing certificates.

When enabled, serial numbers for certificates signed by this CA will be automatically randomized and checked for uniqueness instead of using sequential values.

Key length

2048 bit

Size of the key which will be generated. The larger the key, the more security it offers, but larger keys take considerably more time to generate, and take slightly longer to validate leading to a slight slowdown in setting up new sessions (not always noticeable). As of 2016, 2048 bit is the minimum and most common selection and 4096 is the maximum in common use. For more information see [keylength.com](http://keylength.com)

Lifetime

3650

Lifetime in days. This is commonly set to 3650 (Approximately 10 years.)

Common Name

The internal name of the CA, used as a part of the CA subject. If left blank, the descriptive name will be used instead.

Country Code

VN

Two-letter ISO country code (e.g. US, AU, CA)

State or Province

Ho Chi Minh

Full State or Province name, not abbreviated (e.g. Texas, Indiana, Ontario).

City

Thu Duc

City or other Locality name (e.g. Austin, Indianapolis, Toronto).

Organization

PTIT

- Tạo chứng chỉ cho server xác thực.

Create a New Server Certificate	
Descriptive name	<input type="text" value="CA-VPN-Cert"/> A name for administrative reference, to identify this certificate.
Key length	<div>2048 bit</div> <div>Size of the key which will be generated. The larger the key, the more security it offers, but larger keys take considerably more time to generate, and take slightly longer to validate leading to a slight slowdown in setting up new sessions (not always noticeable). As of 2016, 2048 bit is the minimum and most common selection and 4096 is the maximum in common use. For more information see <a href="http://keylength.com">keylength.com</a></div>
Lifetime	<div>398</div> <div>Lifetime in days. Server certificates should not have a lifetime over 398 days or some platforms may consider the certificate invalid.</div>
Common Name	<div></div> <div>The internal name of the server certificate, used as a part of the certificate subject. Typically set to the hostname of this system. This value is also used as a Subject Alternative Name (SAN). If left blank, the Descriptive Name value will be used for the Common Name and SAN instead.</div>
Country Code	<div>VN</div> <div>Two-letter ISO country code (e.g. US, AU, CA)</div>
State or Province	<div>Ho Chi Minh</div> <div>Full State or Province name, not abbreviated (e.g. Texas, Indiana, Ontario).</div>
City	<div>Thu Duc</div> <div>City or other Locality name (e.g. Austin, Indianapolis, Toronto).</div>
Organization	<div>PTIT</div> <div>Organization name, often the company or group name</div>

## - Setup VPN Server.

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**

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

**Interface**

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

**Local Port**

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**

## - Cho phép các dòng lưu lượng qua OpenVPN.

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](#)

Trở lại với LDAP chỉnh lại mục peer certificate authority sau tạo LDAP Server xong.

Users Groups Settings **Authentication Servers**

---

**Server Settings**

Descriptive name

Type

**LDAP Server Settings**

Hostname or IP address   
NOTE: When using SSL/TLS or STARTTLS, this hostname MUST match a Subject Alternative Name (SAN) or the Common Name (CN) of the LDAP server SSL/TLS Certificate.

Port value

Transport

Peer Certificate Authority   
This CA is used to validate the LDAP server certificate when 'SSL/TLS Encrypted' or 'STARTTLS Encrypted' Transport is active. This CA must match the CA used by the LDAP server.

Protocol version

Thêm gói package tiện ích của OpenVPN trong mục Package Manager.

System / **Package Manager** / Available Packages ?

Installed Packages **Available Packages**

**Search**

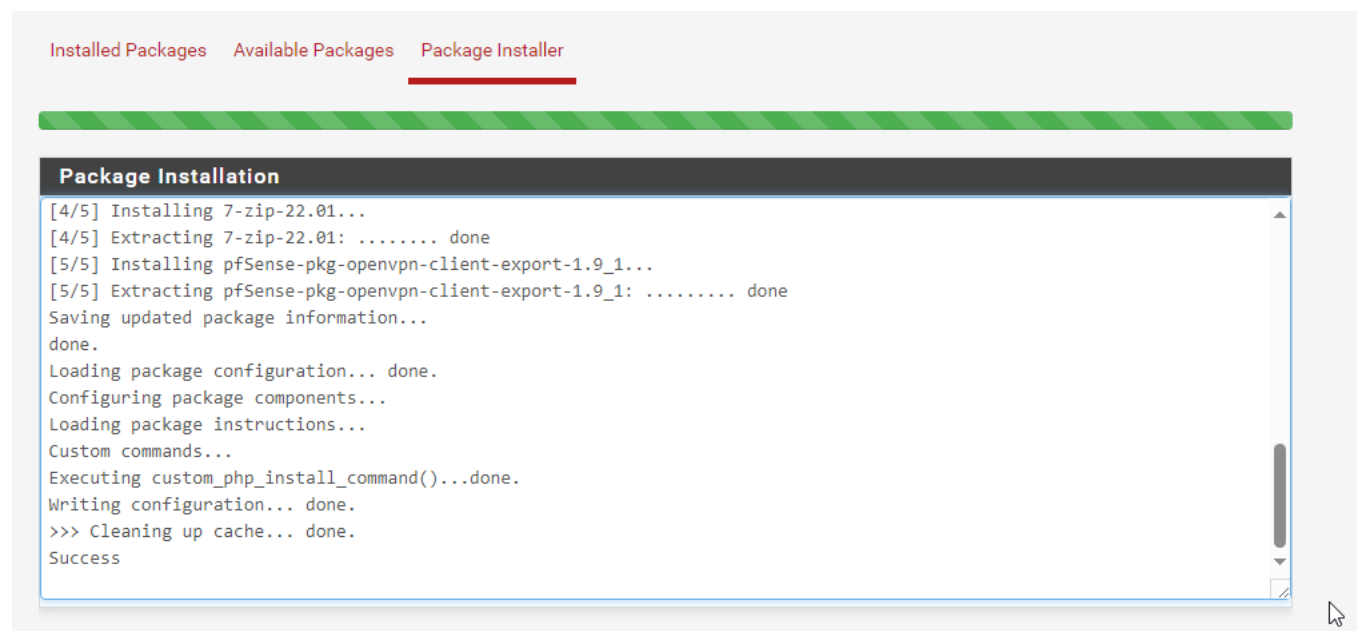
Search term  Both

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

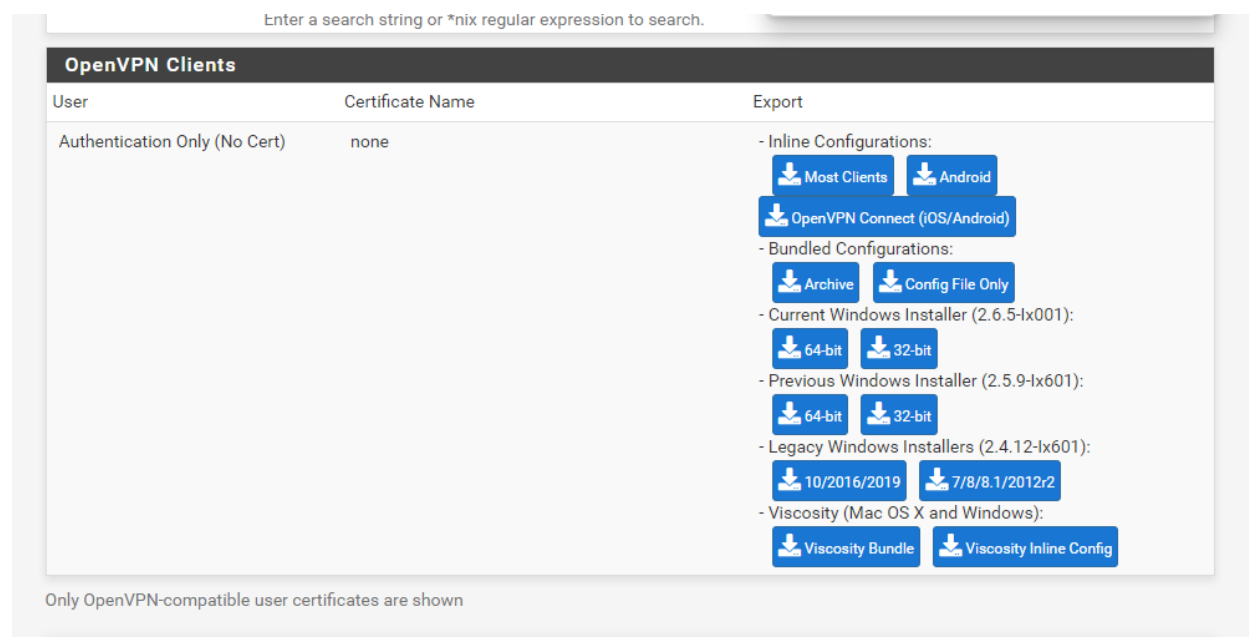
**Packages**

Name	Version	Description
openvpn-client-export	1.9_1	Exports pre-configured OpenVPN Client configurations directly from pfSense software.
Package Dependencies: <a href="#">openvpn-client-export-2.6.5</a> <a href="#">openvpn-2.6.4</a> <a href="#">zip-3.0_1</a> <a href="#">7-zip-22.01</a>		

## Cài đặt tiện ích thành công.

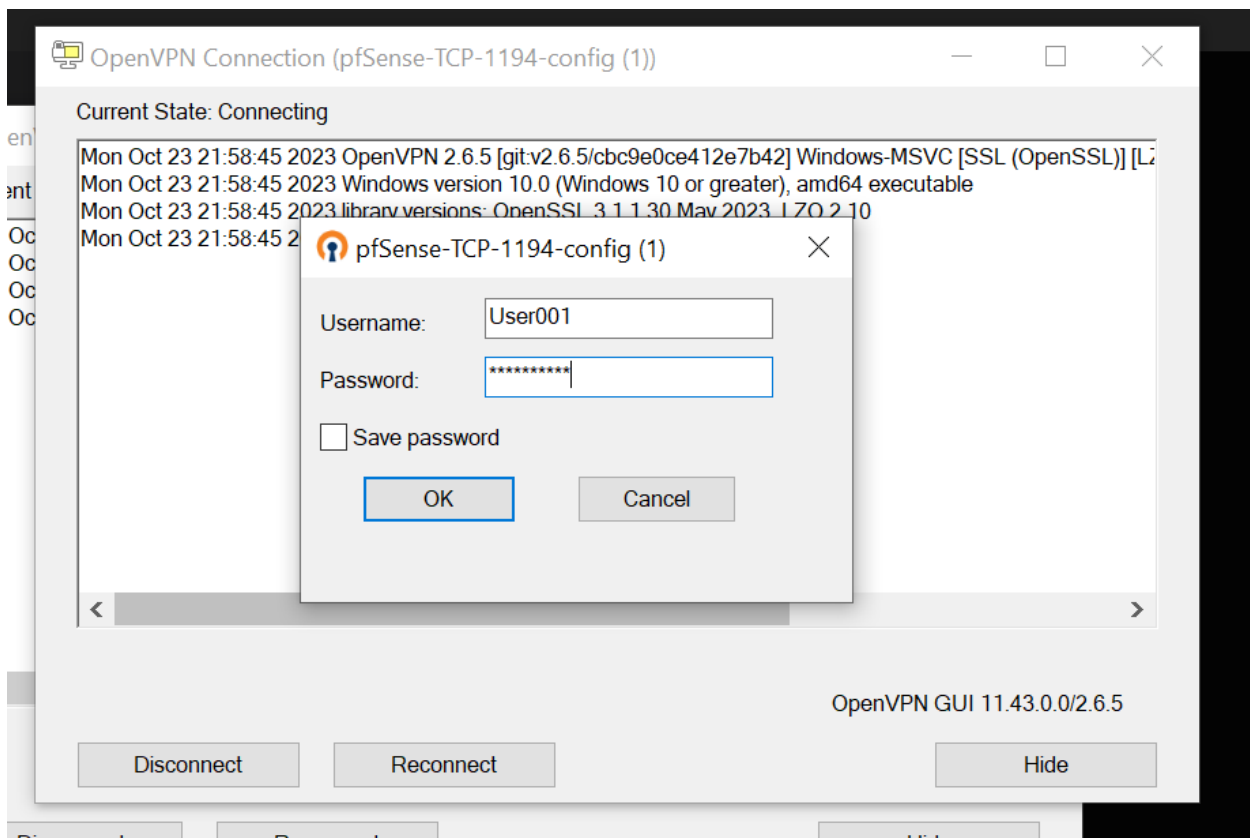


## Tải file thực thi ở mục Current Windows Installer.

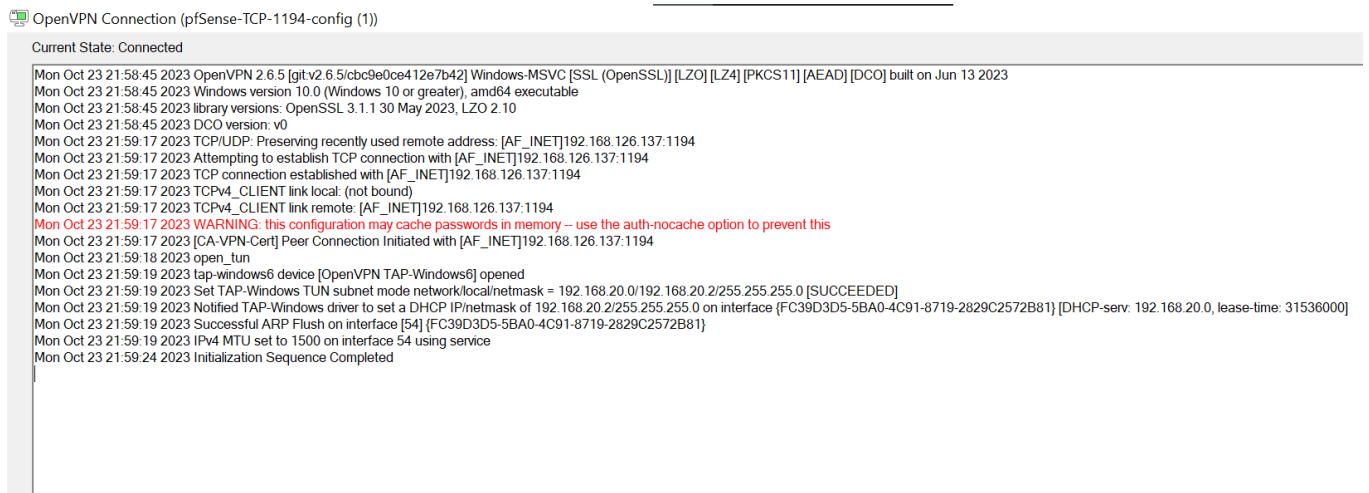




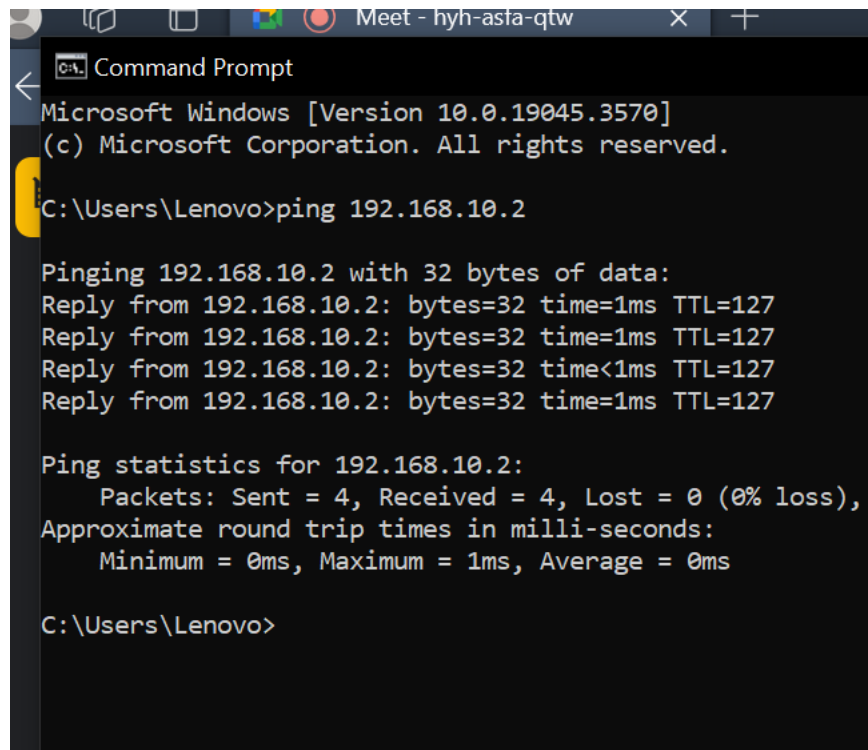
Đăng nhập với tên User001.



- Kết nối thành công.



- Ping đến máy LAN từ máy thật.



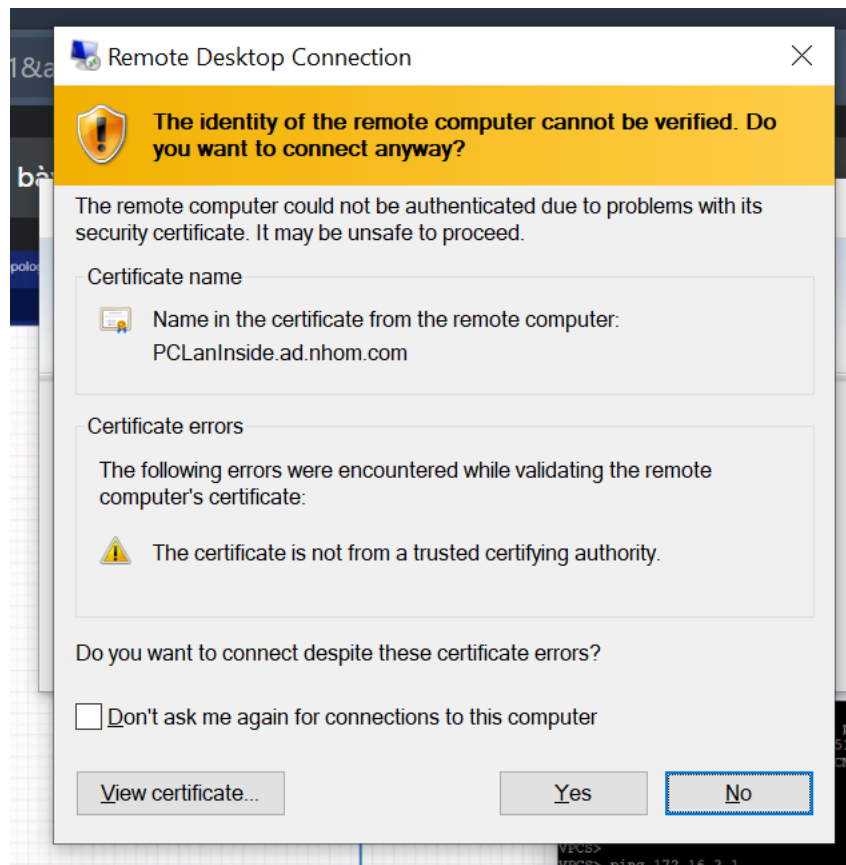
```
C:\Users\Lenovo>ping 192.168.10.2

Pinging 192.168.10.2 with 32 bytes of data:
Reply from 192.168.10.2: bytes=32 time=1ms TTL=127
Reply from 192.168.10.2: bytes=32 time=1ms TTL=127
Reply from 192.168.10.2: bytes=32 time<1ms TTL=127
Reply from 192.168.10.2: bytes=32 time=1ms TTL=127

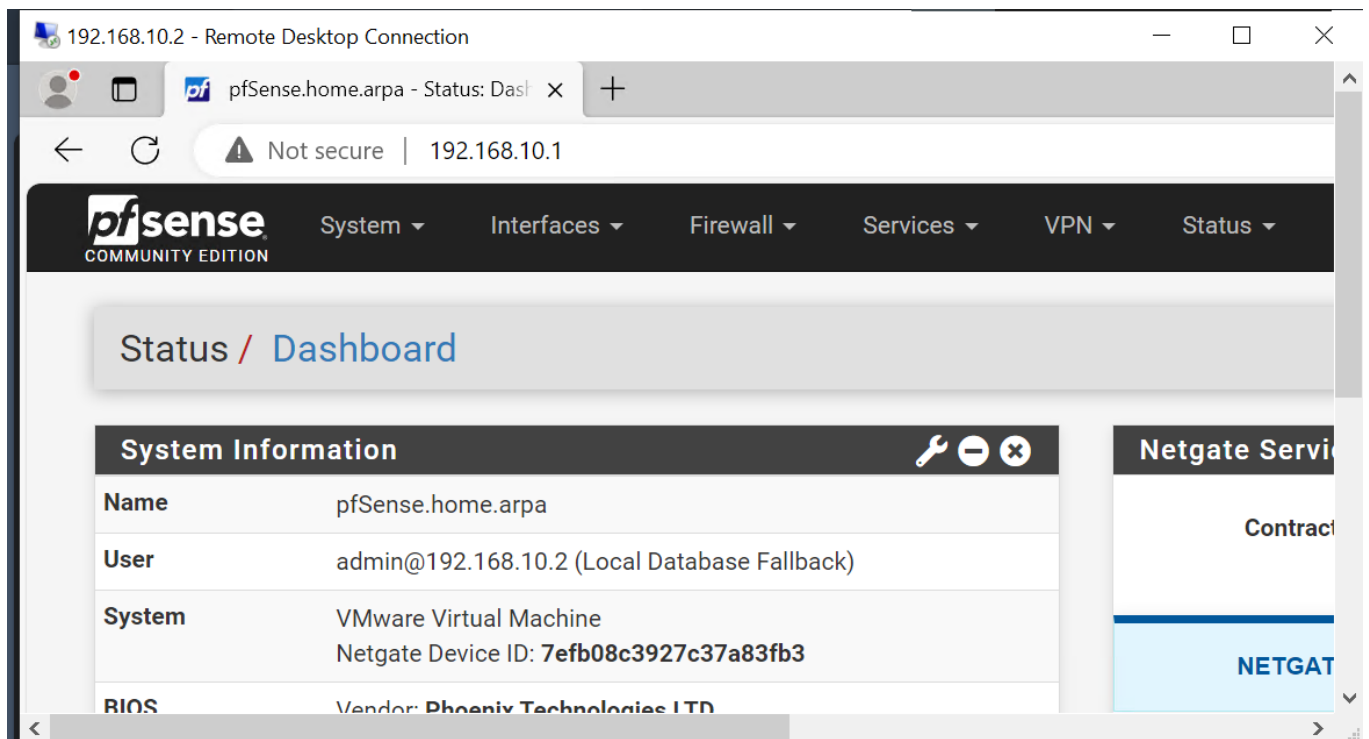
Ping statistics for 192.168.10.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\Users\Lenovo>
```

Xác nhận để remote máy User001 từ máy thật.



- Remote thành công.



The screenshot shows a Remote Desktop Connection window titled "192.168.10.2 - Remote Desktop Connection". Inside the window is a web browser displaying the pfSense Status Dashboard. The browser's address bar shows "192.168.10.1" with a "Not secure" warning. The pfSense header includes the logo and navigation tabs: System, Interfaces, Firewall, Services, VPN, and Status. The main content area is titled "Status / Dashboard".

The "System Information" widget displays the following data:

System Information	
Name	pfSense.home.arpa
User	admin@192.168.10.2 (Local Database Fallback)
System	VMware Virtual Machine Netgate Device ID: 7efb08c3927c37a83fb3
BIOS	Vendor: Phoenix Technologies LTD

To the right, a "Netgate Services" widget is partially visible, showing a "Contract" section and a "NETGATE" logo.