

**BỘ GIÁO DỤC VÀ ĐÀO TẠO  
HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG  
KHOA CÔNG NGHỆ THÔNG TIN 2**



**BÁO CÁO**

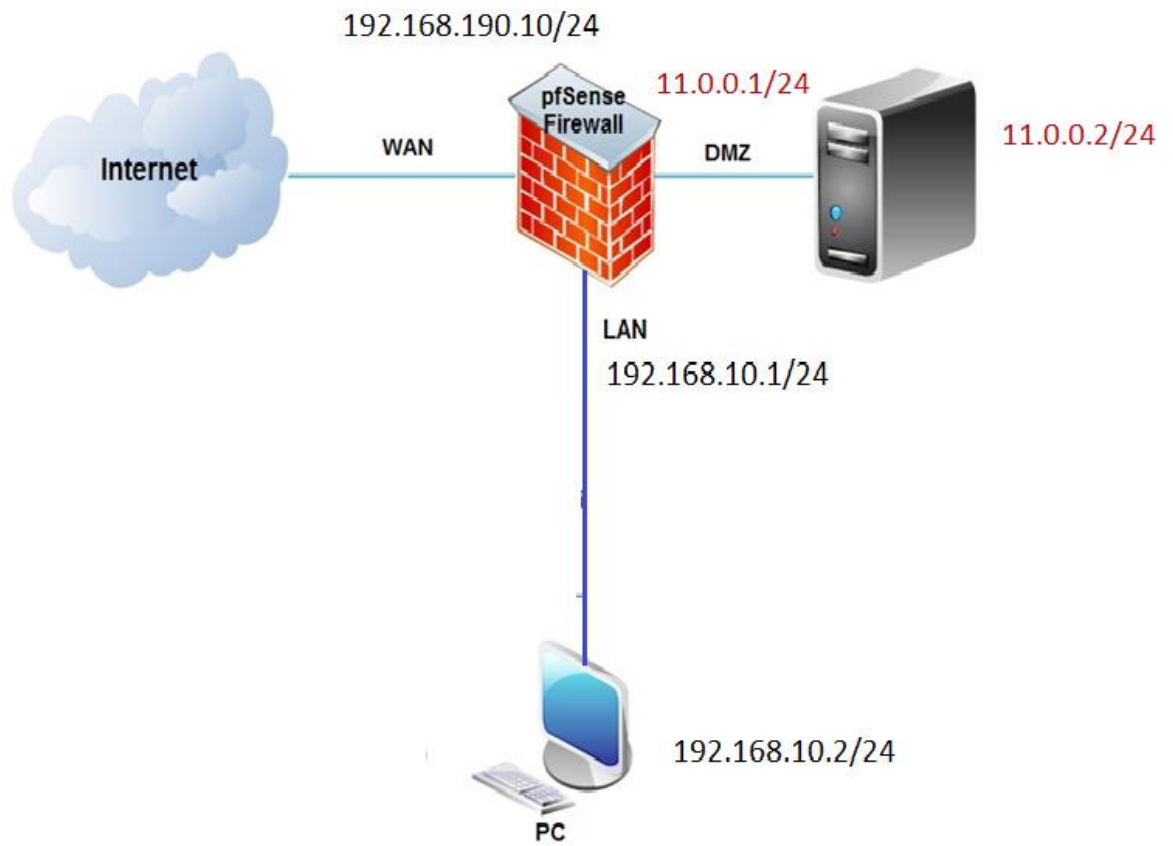
**THIẾT LẬP FIREWALL TOPOLOGY CHO MẠNG DOANH  
NGHIỆP**

Sinh viên: Võ Thanh Phong N20DCAT041 D20CQAT01-N

Viên Ngọc Tân N20DCAT051 D20CQAT01-N

Giảng viên hướng dẫn: Đàm Minh Linh

## I. Sơ đồ:



## II. Chuẩn bị thiết bị

- Pfsense:



 Power on this virtual machine

 Edit virtual machine settings

### ▼ Devices

 Memory	256 MB
 Processors	1
 Hard Disk (SCSI)	20 GB
 CD/DVD (IDE)	Using file D:\Pro...
 Network Adapter	NAT
 Network Adapter 2	LAN Segment
 Network Adapter 3	LAN Segment
 USB Controller	Present
 Sound Card	Auto detect
 Display	Auto detect










- Máy Lan là Win10:

## Windows 10

 [Power on this virtual machine](#)

 [Edit virtual machine settings](#)

### ▼ Devices

 Memory	2 GB
 Processors	4
 Hard Disk (NVMe)	60 GB
 CD/DVD (SATA)	Auto detect
 Network Adapter	LAN Segment
 USB Controller	Present
 Sound Card	Auto detect
 Printer	Present
 Display	Auto detect








- Máy DMZ là Windows Server:

## Windows Server 2019

 Power on this virtual machine

 Edit virtual machine settings

### ▼ Devices

 Memory	2 GB
 Processors	2
 Hard Disk (NVMe)	60 GB
 CD/DVD (SATA)	Auto detect
 Network Adapter	LAN Segment
 USB Controller	Present
 Sound Card	Auto detect
 Printer	Present
 Display	Auto detect

### III. Cấu hình

- Cấu hình cổng Lan cho pfsense:

```

Enter an option: 2

Available interfaces:

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

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

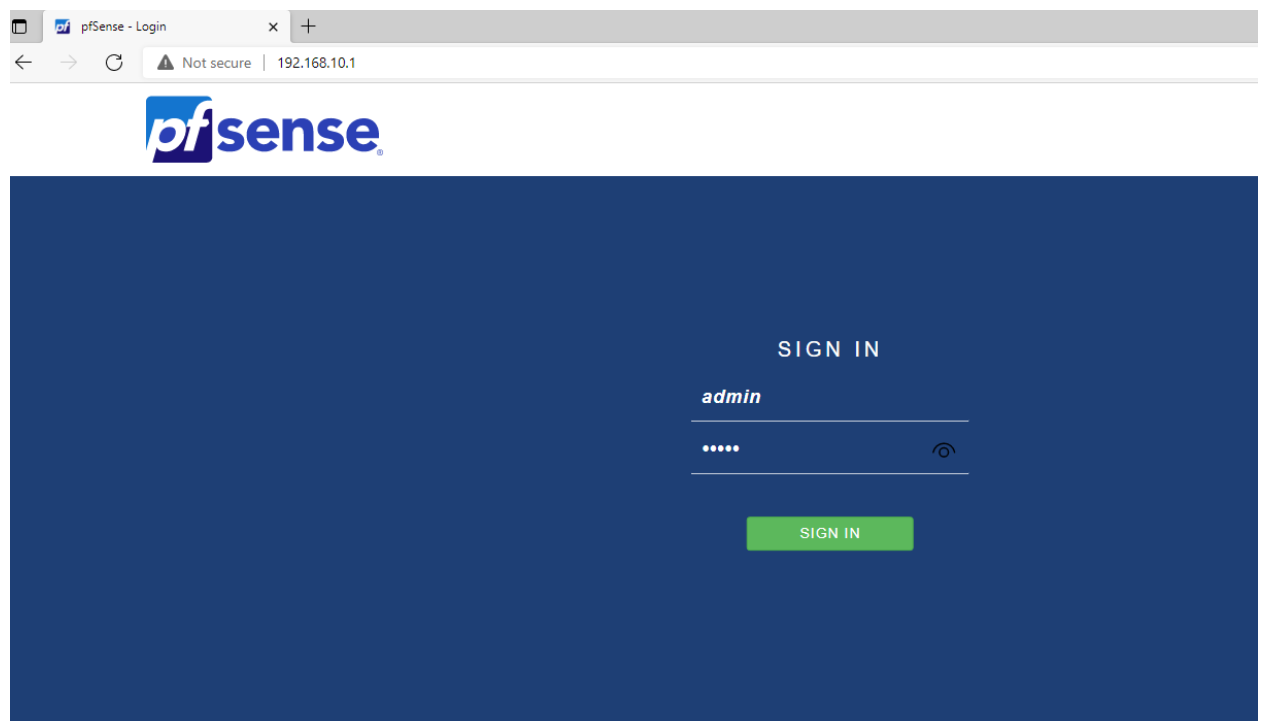
Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
     255.255.0.0   = 16
     255.0.0.0     = 8

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

```

- Cấu hình web cho pfsense

Đăng nhập vào web với username/password là admin/pfsense



Cấu hình hostname, domain, dns

General Information	
On this screen the general pfSense parameters will be set.	
Hostname	<input type="text" value="pfSense"/> Name of the firewall host, without domain part.  Examples: pfsense, firewall, edgefw
Domain	<input type="text" value="pfsense.com"/> 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 'local' TLD is widely used by Apple (iCloud, iMessage, Airprint, Airplay) and some Windows systems and networked devices. These will not network correctly. Alternatives such as 'home.arpa', 'local.lan', or 'mylocal' are safe.
The default behavior of the DNS Resolver will ignore manually configured DNS servers for client queries and manually configured DNS servers below for client queries, visit Services > DNS Resolver and enable DNS Query	
Primary DNS Server	<input type="text" value="8.8.8.8"/>
Secondary DNS Server	<input type="text" value="8.8.4.4"/>
Override DNS	<input checked="" type="checkbox"/> Allow DNS servers to be overridden by DHCP/PPP on WAN

## Cấu hình thời gian

Wizard / pfSense Setup / Time Server Information	
Step 3 of 9	
Time Server Information	
Please enter the time, date and time zone.	
Time server hostname	<input type="text" value="2.pfsense.pool.ntp.org"/> Enter the hostname (FQDN) of the time server.
Timezone	<input type="text" value="Asia/Ho_Chi_Minh"/>
<input type="button" value="» Next"/>	

## Cấu hình 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**

### General configuration

**MAC Address**

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

## Cấu hình 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**

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

**Subnet Mask**

[» Next](#)

## Đặt mật khẩu mới cho 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 WebGUI.

Admin Password

•

Admin Password AGAIN

•

>> Next

## Chọn Finish

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 your system up to date with the latest security patches and other 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 taking a short survey (your responses are kept anonymous).

[Anonymous User Survey](#)

#### Useful resources.

- Learn more about Netgate's product line, services, and pfSense software from our [documentation](#).
- 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

# Add vùng DMZ

Interfaces / Interface Assignments

Interface has been deleted.

Interface AssignmentsInterface GroupsWirelessVLANsQinQsPPPsGRGsGIFsBridgesLAGGs

Interface	Network port
WAN	em0 (00:0c:29:1b:6f:96)
LAN	em1 (00:0c:29:1b:6f:a0) <span>Delete</span>
Available network ports:	em2 (00:0c:29:1b:6f:aa) <span>Add</span>

Save

# Cấu hình DMZ

Enable☒ Enable interface

Restore p  
Microsoft E

Description

DMZ

Enter a description (name) for the interface here.

IPv4 Configuration Type

Static IPv4

IPv6 Configuration Type

None

MAC Address

xxxxxxxxxxxx

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 gateway

None

Add a new gateway

If this interface is an Internet connection, select an existing Gateway from the list or add a new one using the "Add" button.  
On local area network interfaces the upstream gateway should be "none".

# Cấu hình IP tĩnh cho DMZ

## Internet Protocol Version 4 (TCP/IPv4) Properties



**General**

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

☐ Obtain an IP address automatically

☒ Use the following IP address:

IP address:	11 . 0 . 0 . 2
Subnet mask:	255 . 0 . 0 . 0
Default gateway:	11 . 0 . 0 . 1

☐ Obtain DNS server address automatically

☒ Use the following DNS server addresses:

Preferred DNS server:	8 . 8 . 8 . 8
Alternate DNS server:	8 . 8 . 4 . 4

☐ Validate settings upon exit

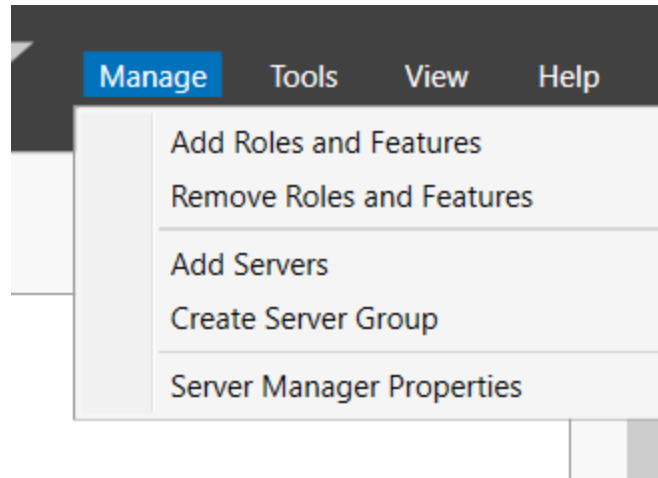
Advanced...

OK Cancel

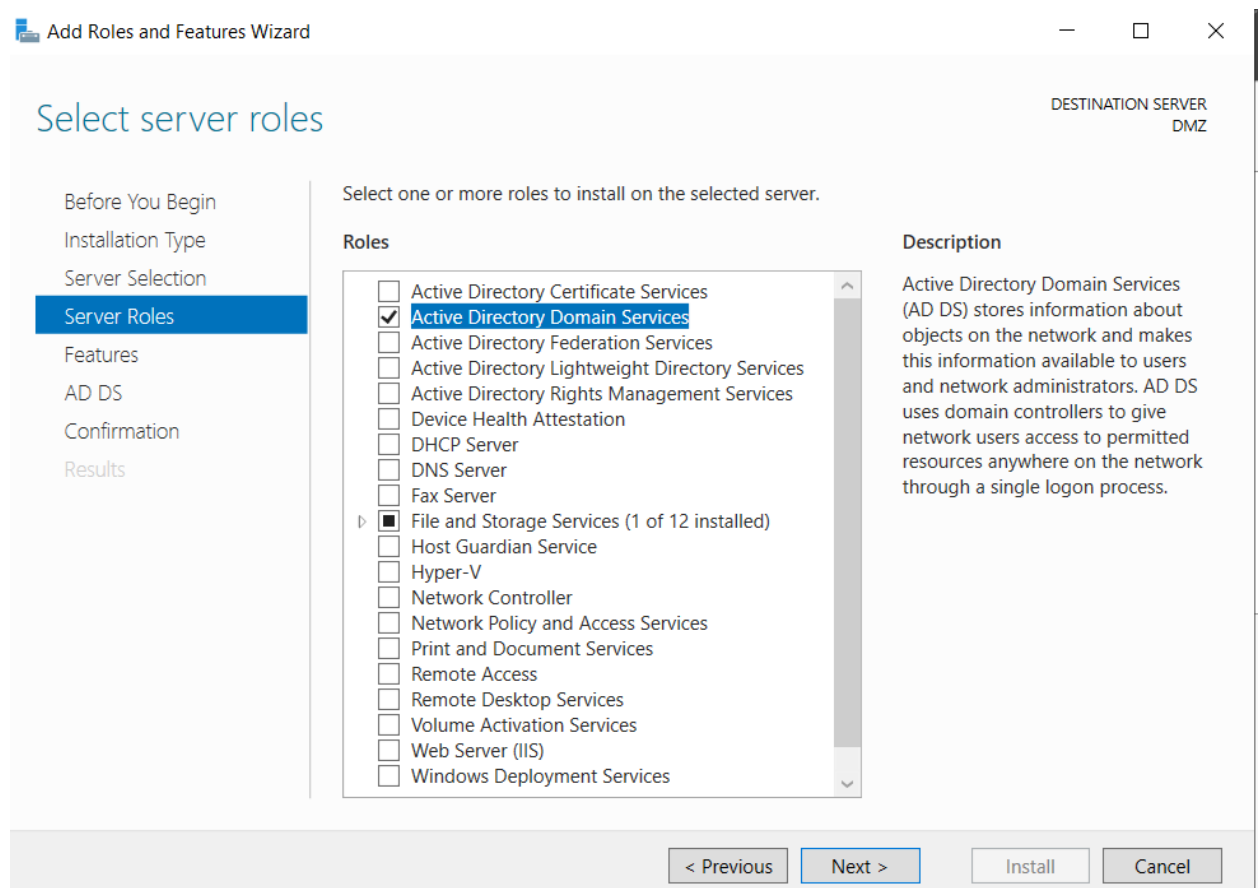
Subnet phải là 255.255.255.0

- Cấu hình AD trên DMZ

Chọn Manage > Add Roles and Features



## Chọn Active Directory Domain Services



## Cấu hình domain

## Deployment Configuration

TARGET SERVER  
DMZ

## Deployment Configuration

Domain Controller Options

Additional Options

Paths

Review Options

Prerequisites Check

Installation

Results

Select the deployment operation

- ☐ Add a domain controller to an existing domain
- ☐ Add a new domain to an existing forest
- ☒ Add a new forest

Specify the domain information for this operation

Root domain name:

n20dcat041.com

[More about deployment configurations](#)

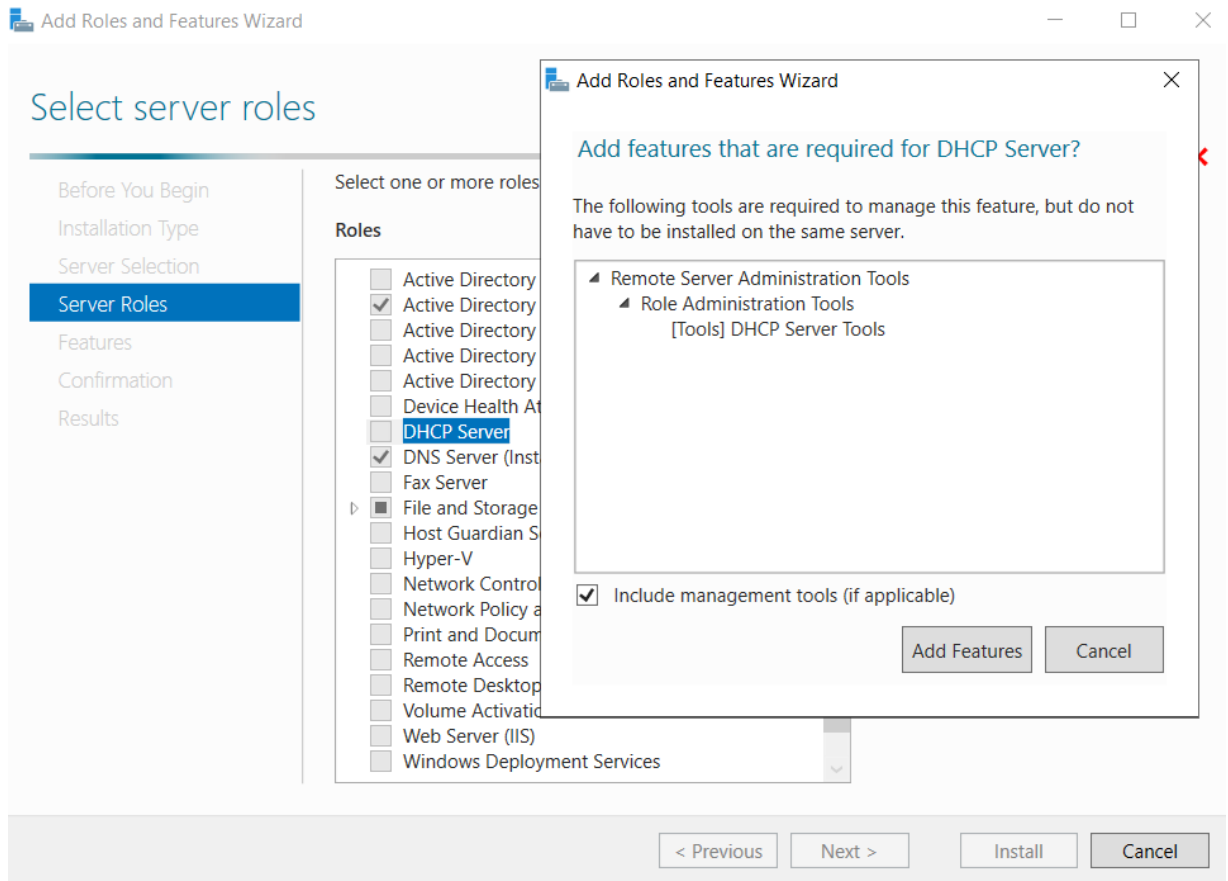
&lt; Previous

Next &gt;

Install

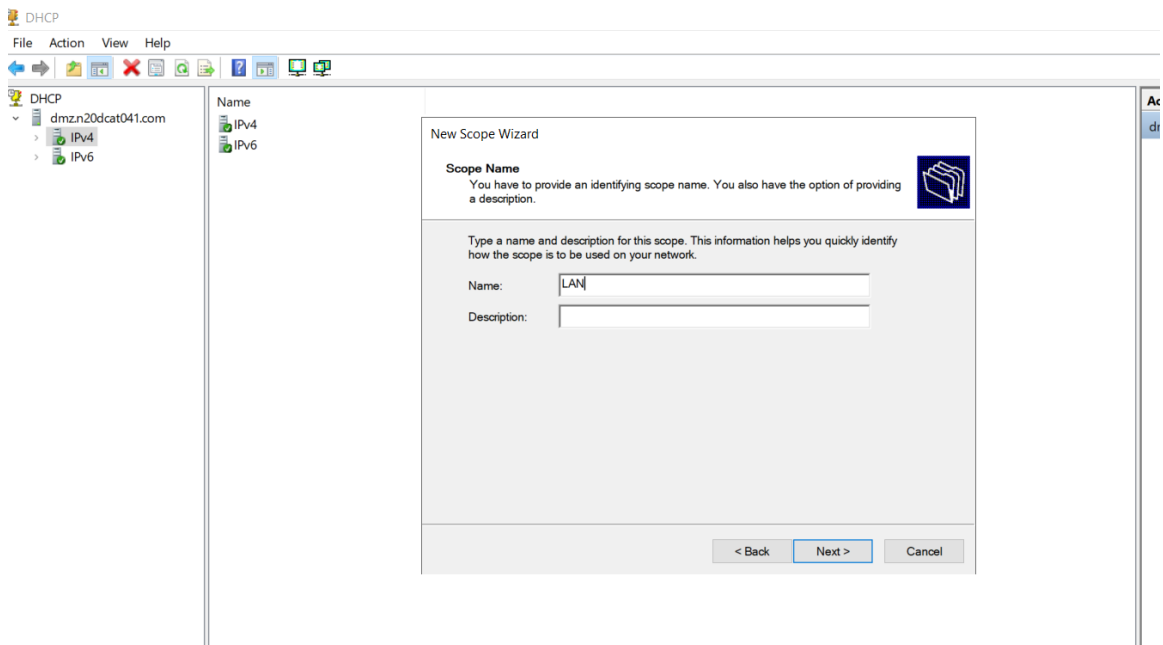
Cancel

Cài đặt DHCP server cho window server



- Cấu hình DHCP server trên window server

Tạo Scope mới cho DHCP server



## New Scope Wizard

### IP Address Range

You define the scope address range by identifying a set of consecutive IP addresses.



#### Configuration settings for DHCP Server

Enter the range of addresses that the scope distributes.

Start IP address:

End IP address:

#### Configuration settings that propagate to DHCP Client

Length:

Subnet mask:

< Back

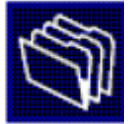
Next >

Cancel

## 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.

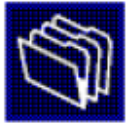
IP address:



## 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:

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

Server name:

IP address:

Add

Resolve

11.0.0.2

8.8.8.8

8.8.4.4

Remove

Up

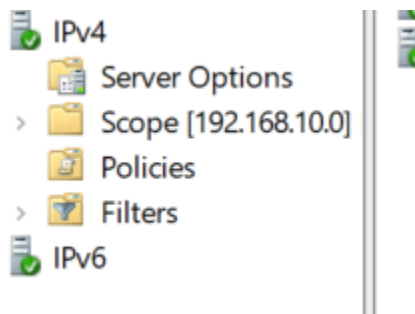
Down

< Back

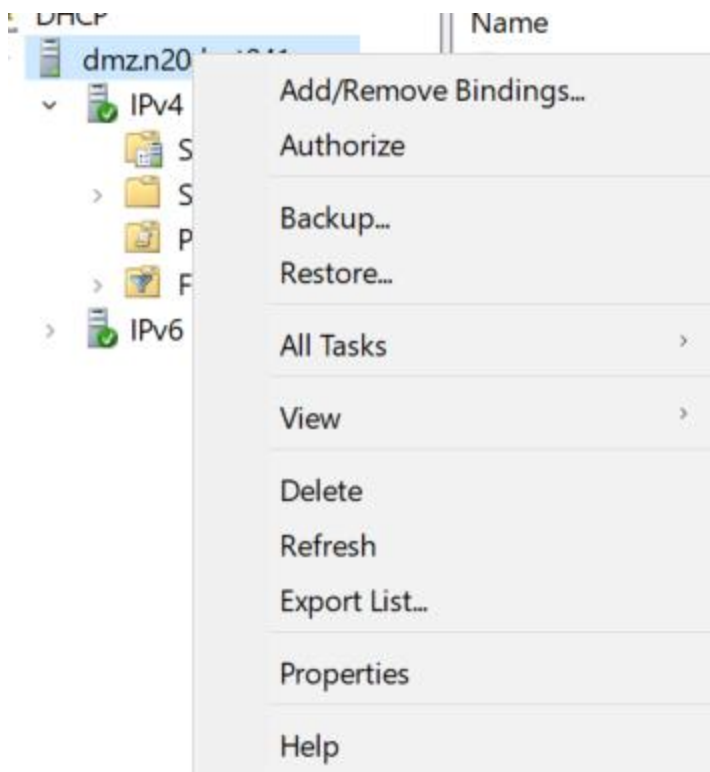
Next >

Cancel

Tạo thành công



Authorize 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 chosen VIP is in a non-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 the agent ID to the request.

---

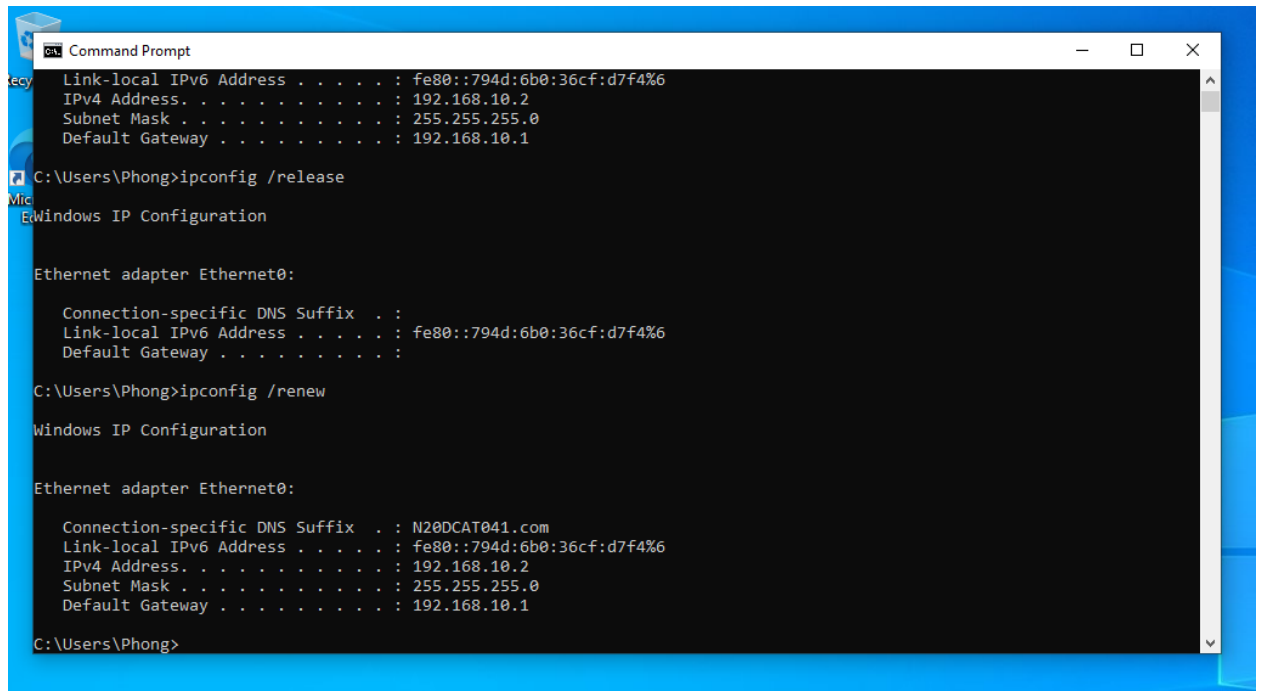
**Destination server** 11.0.0.2

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

---

[Save](#) [+ Add server](#)

Máy Lan đã có IP



```
Command Prompt
Link-local IPv6 Address . . . . . : fe80::794d:6b0:36cf:d7f4%6
IPv4 Address. . . . . : 192.168.10.2
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.10.1

C:\Users\Phong>ipconfig /release

Windows IP Configuration

Ethernet adapter Ethernet0:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::794d:6b0:36cf:d7f4%6
    Default Gateway . . . . . : 

C:\Users\Phong>ipconfig /renew

Windows IP Configuration

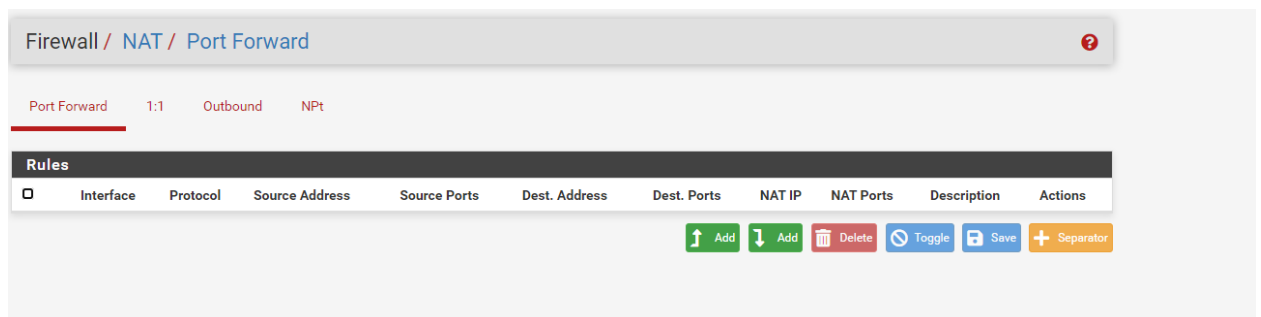
Ethernet adapter Ethernet0:

    Connection-specific DNS Suffix  . : N20DCAT041.com
    Link-local IPv6 Address . . . . . : fe80::794d:6b0:36cf:d7f4%6
    IPv4 Address. . . . . : 192.168.10.2
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.10.1

C:\Users\Phong>
```

## IV. Cấu hình NAT

- Tiến hành cấu hình



- Cấu hình cho LAN

HTTP:

This option is rarely needed. Don't use this without thorough knowledge of the implications.

<b>Interface</b>	WAN		
	Choose which interface this rule applies to. In most cases "WAN" is specified.		
<b>Address Family</b>	IPv4		
	Select the Internet Protocol version this rule applies to.		
<b>Protocol</b>	TCP/UDP		
	Choose which protocol this rule should match. In most cases "TCP" is specified.		
<b>Source</b>	<a href="#">Display Advanced</a>		
<b>Destination</b>	<input type="checkbox"/> Invert match.	WAN address	
		Type	Address/mask
<b>Destination port range</b>	HTTP		HTTP
	From port	Custom	To port
	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.		
<b>Redirect target IP</b>	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)		
<b>Redirect target port</b>	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:

<b>Interface</b>	WAN		
	Choose which interface this rule applies to. In most cases "WAN" is specified.		
<b>Address Family</b>	IPv4		
	Select the Internet Protocol version this rule applies to.		
<b>Protocol</b>	TCP/UDP		
	Choose which protocol this rule should match. In most cases "TCP" is specified.		
<b>Source</b>	<a href="#">Display Advanced</a>		
<b>Destination</b>	<input type="checkbox"/> Invert match.	WAN address	
		Type	Address/mask
<b>Destination port range</b>	HTTPS		HTTPS
	From port	Custom	To port
	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.		
<b>Redirect target IP</b>	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)		
<b>Redirect target port</b>	HTTPS		
	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)		

Win10 đã có mạng

```

C:\Users\Phong>ping google.com

Pinging google.com [172.217.24.78] with 32 bytes of data:
Reply from 172.217.24.78: bytes=32 time=102ms TTL=127
Reply from 172.217.24.78: bytes=32 time=161ms TTL=127
Reply from 172.217.24.78: bytes=32 time=143ms TTL=127
Reply from 172.217.24.78: bytes=32 time=94ms TTL=127

Ping statistics for 172.217.24.78:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 94ms, Maximum = 161ms, Average = 125ms

```

## - Cấu hình NAT cho DMZ

### HTTP:

<b>Interface</b>	WAN		
	Choose which interface this rule applies to. In most cases "WAN" is specified.		
<b>Address Family</b>	IPv4		
	Select the Internet Protocol version this rule applies to.		
<b>Protocol</b>	TCP/UDP		
	Choose which protocol this rule should match. In most cases "TCP" is specified.		
<b>Source</b>	Display Advanced		
<b>Destination</b>	<input type="checkbox"/> Invert match.	WAN address	
		Type	Address/mask
<b>Destination port range</b>	HTTP		HTTP
	From port	Custom	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.		
<b>Redirect target IP</b>	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)		
<b>Redirect target port</b>	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 is calculated automatically).		

### HTTPS:

<b>Interface</b>	WAN		
Choose which interface this rule applies to. In most cases "WAN" is specified.			
<b>Address Family</b>	IPv4		
Select the Internet Protocol version this rule applies to.			
<b>Protocol</b>	TCP/UDP		
Choose which protocol this rule should match. In most cases "TCP" is specified.			
<b>Source</b>	Display Advanced		
<b>Destination</b>	<input type="checkbox"/> Invert match.	WAN address	
		Type	Address/mask
<b>Destination port range</b>	HTTPS		HTTPS
	From port	Custom	To port
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.			
<b>Redirect target IP</b>	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)			
<b>Redirect target port</b>	HTTPS		
	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			

## Cấu hình rule để cho phép DMZ kết nối mạng

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 or ICMP port unreachable for UDP) is returned to th  
 whereas with block the packet is dropped silently. In either case, the original packet is discarded.

**Disabled**
☐ Disable this rule

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

**Interface**
DMZ

Choose the interface from which packets must come to match this rule.

**Address Family**
IPv4

Select the Internet Protocol version this rule applies to.

**Protocol**
Any

Choose which IP protocol this rule should match.

Source

**Source**
☐ Invert match
 DMZ net

Source Address

Destination

**Destination**
☐ Invert match
 any

Destination Address

## DMZ đã có mạng

```
C:\Users\Phong>ping goolge.com


Pinging goolge.com [142.250.66.100] with 32 bytes of data:
Reply from 142.250.66.100: bytes=32 time=55ms TTL=127
Reply from 142.250.66.100: bytes=32 time=135ms TTL=127
Reply from 142.250.66.100: bytes=32 time=172ms TTL=127
Reply from 142.250.66.100: bytes=32 time=170ms TTL=127

Ping statistics for 142.250.66.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 55ms, Maximum = 172ms, Average = 133ms
```

- V. Tạo user cho Lan
- Join domain cho máy Lan

- Tạo Group user

New Object - Group ×

 Create in: N20DCAT041.com/Users

---

Group name:

Group name (pre-Windows 2000):


<p>Group scope</p> <p><input checked="" type="radio"/> Domain local</p> <p><input type="radio"/> Global</p> <p><input type="radio"/> Universal</p>	<p>Group type</p> <p><input checked="" type="radio"/> Security</p> <p><input type="radio"/> Distribution</p>
--	--

---

- Tạo user 1

## New Object - User



 Create in: N20DCAT041.com/Users

---

First name:  Initials:

Last name:

Full name:

User logon name:

@N20DCAT041.com

User logon name (pre-Windows 2000):

---

## PhongUser1 Properties



Remote control		Remote Desktop Services Profile		COM+	
General	Address	Account	Profile	Telephones	Organization
Member Of		Dial-in	Environment	Sessions	

Member of:

Name	Active Directory Domain Services Folder
Domain Users	N20DCAT041.com/Users
N20DCAT041_G...	N20DCAT041.com/Users

---

Primary group: Domain Users

There is no need to change Primary group unless you have Macintosh clients or POSIX-compliant applications.



Cho user1 là remote control

Select Groups ✕

Select this object type:

Groups or Built-in security principals Object Types...

From this location:

N20DCAT041.com Locations...

Enter the object names to select ([examples](#)):

Remote Desktop Users Check Names

Advanced... OK Cancel

## PhongUser1 Properties



General	Address	Account	Profile	Telephones	Organization
Member Of	Dial-in	Environment		Sessions	
Remote control		Remote Desktop Services Profile			COM+

Use this tab to configure Remote Desktop Services remote control settings.

To remotely control or observe a user's session, select the following check box:

☒ Enable remote control

To require the user's permission to control or observe the session, select the following check box:

☒ Require user's permission

Level of control

Specify the level of control you want to have over a user's session

☐ View the user's session

☒ Interact with the session

OK Cancel Apply Help

- Tạo user2 và add vào group

## PhongUser2 Properties



Remote control		Remote Desktop Services Profile			COM+
General	Address	Account	Profile	Telephones	Organization
Member Of		Dial-In	Environment		Sessions

Member of:

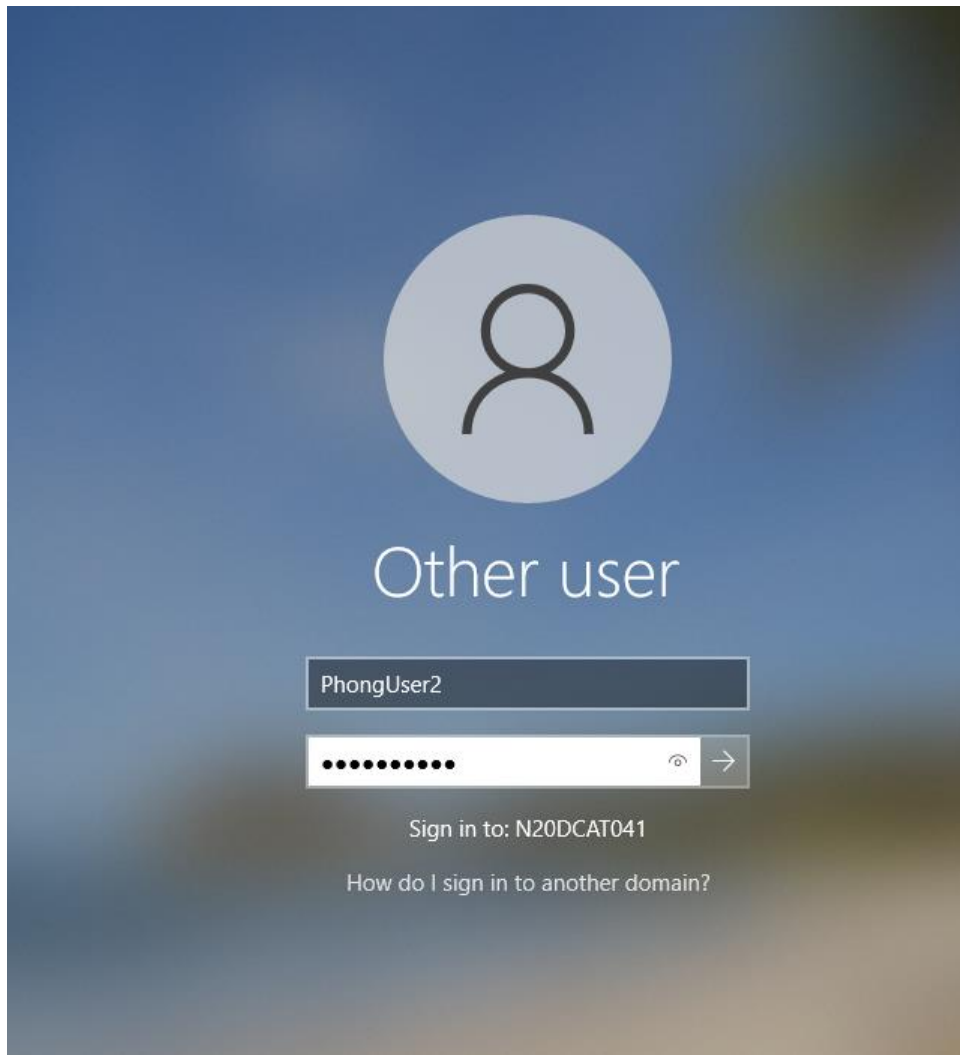
Name	Active Directory Domain Services Folder
Domain Users	N20DCAT041.com/Users
N20DCAT041_G...	N20DCAT041.com/Users

---

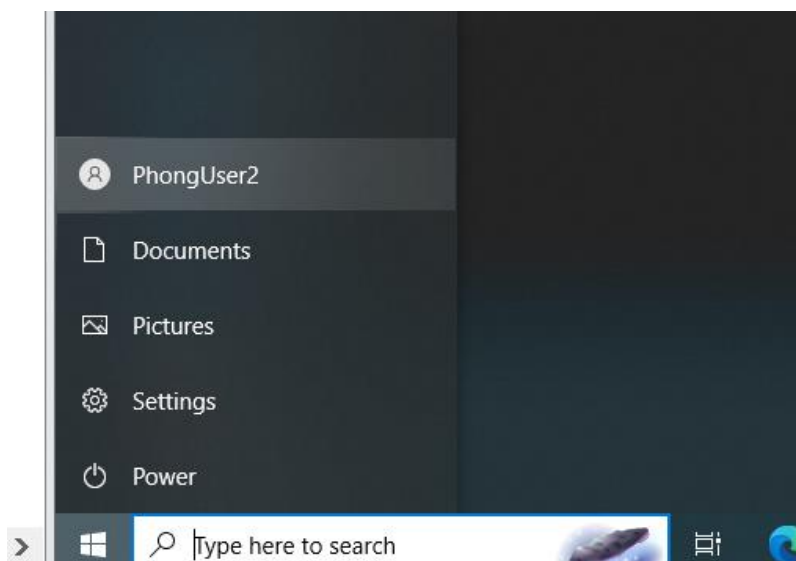
Primary group: Domain Users

There is no need to change Primary group unless you have Macintosh clients or POSIX-compliant applications.

- Login vào win 10 bằng user

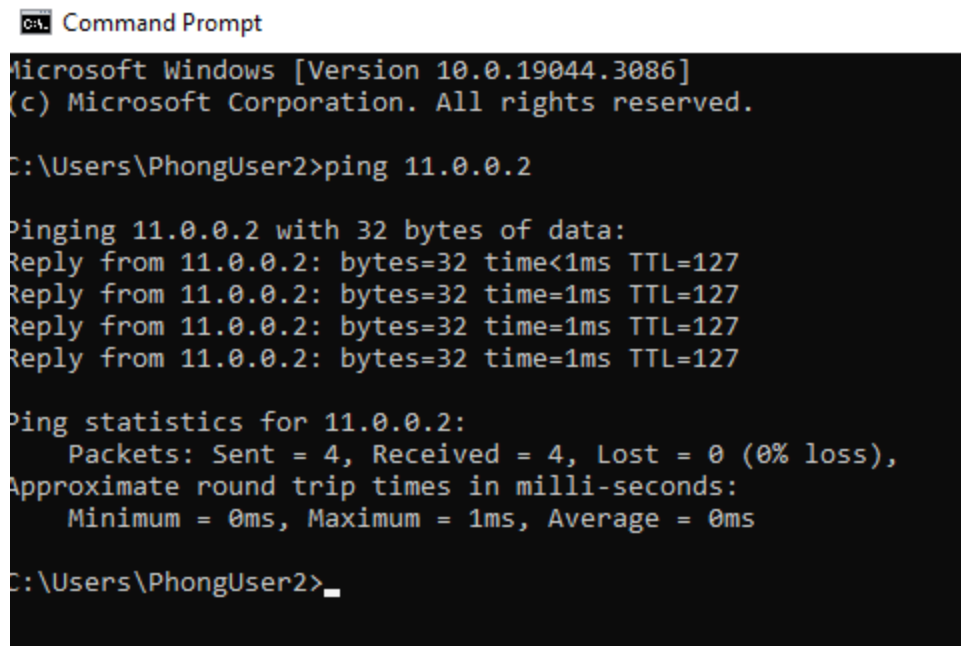


- Login thành công



## VI. Remote từ Lan đến Windows server

- Ping từ Lan đến Windows server



```
Command Prompt

Microsoft Windows [Version 10.0.19044.3086]
(c) Microsoft Corporation. All rights reserved.

C:\Users\PhongUser2>ping 11.0.0.2

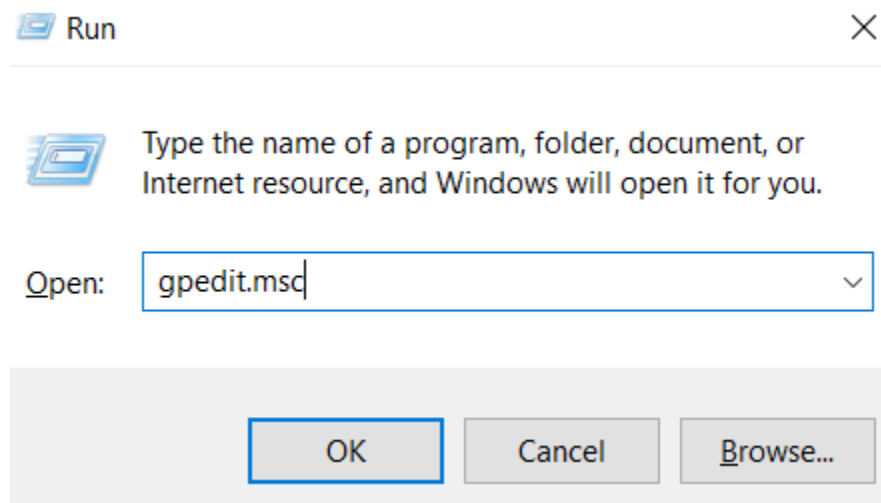
Pinging 11.0.0.2 with 32 bytes of data:
Reply from 11.0.0.2: bytes=32 time<1ms TTL=127
Reply from 11.0.0.2: bytes=32 time=1ms TTL=127
Reply from 11.0.0.2: bytes=32 time=1ms TTL=127
Reply from 11.0.0.2: bytes=32 time=1ms TTL=127

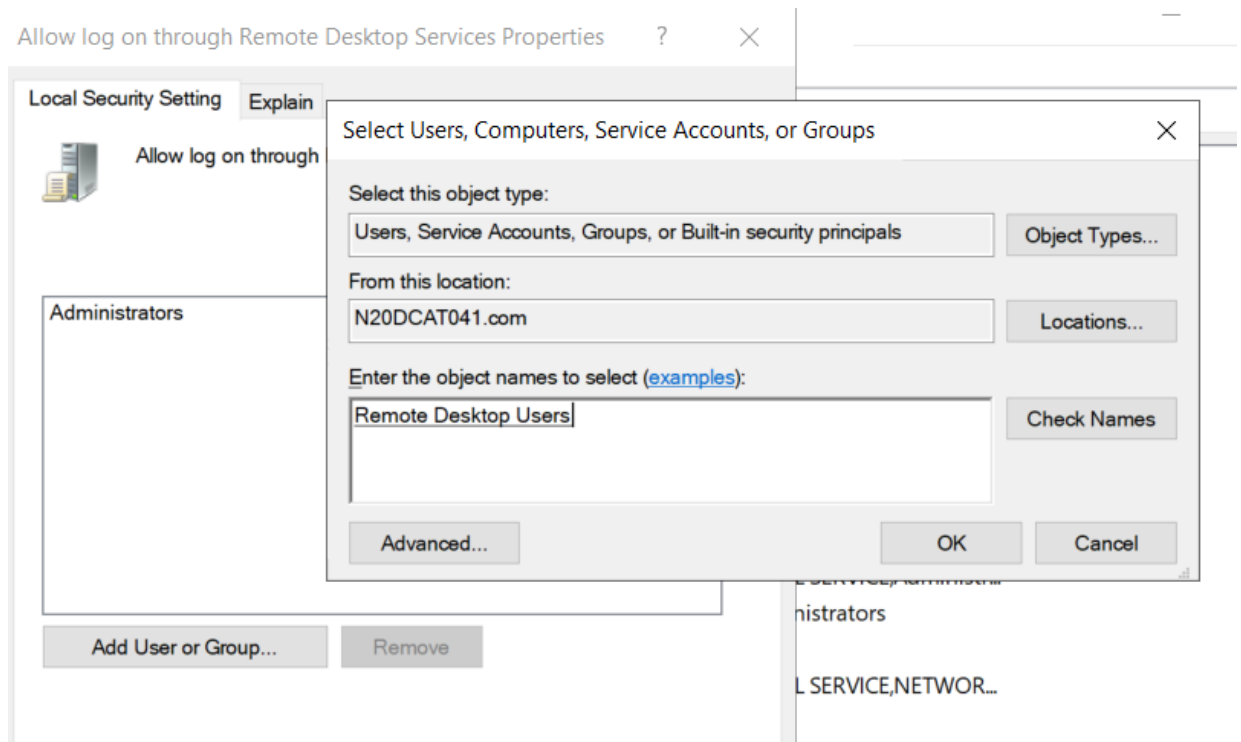
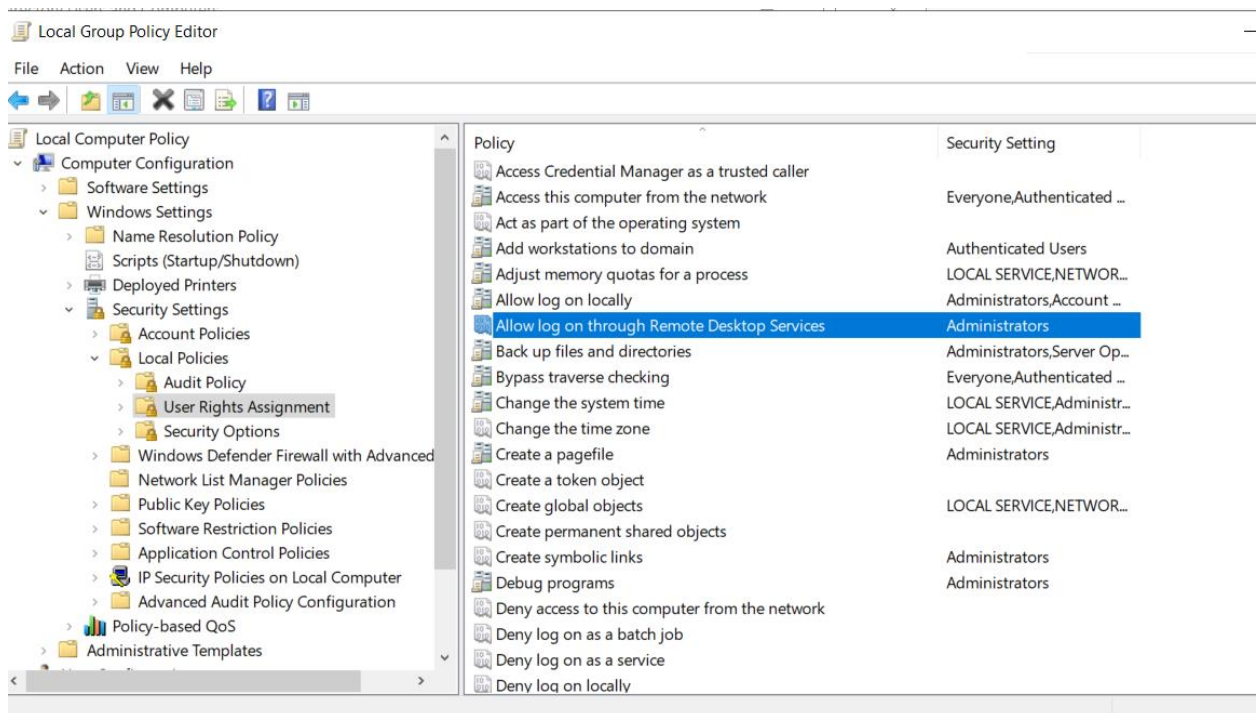
Ping statistics for 11.0.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

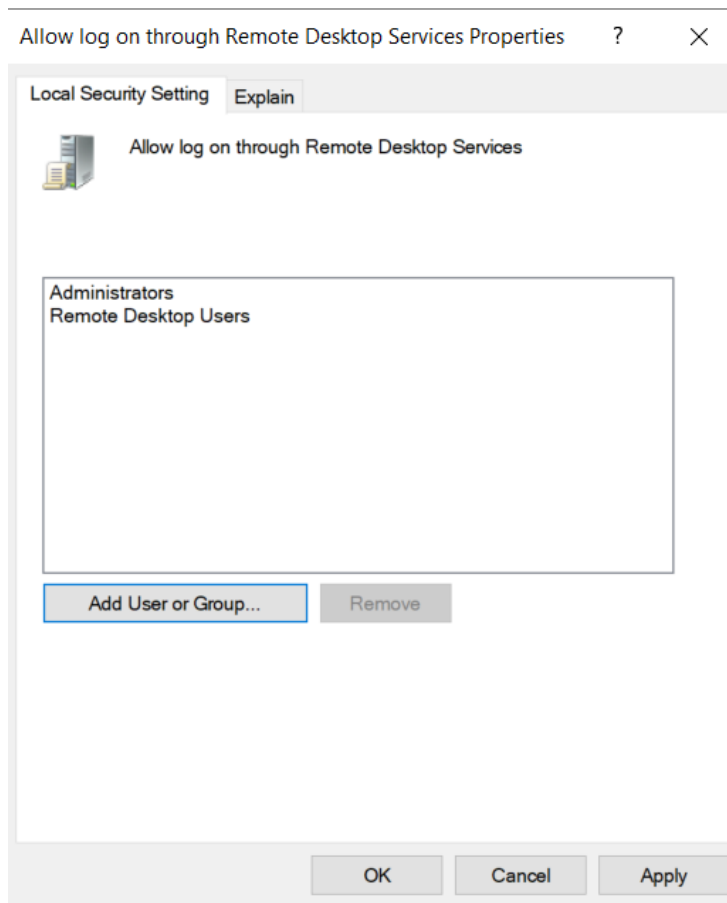
C:\Users\PhongUser2>
```

- Remote đến Windows server

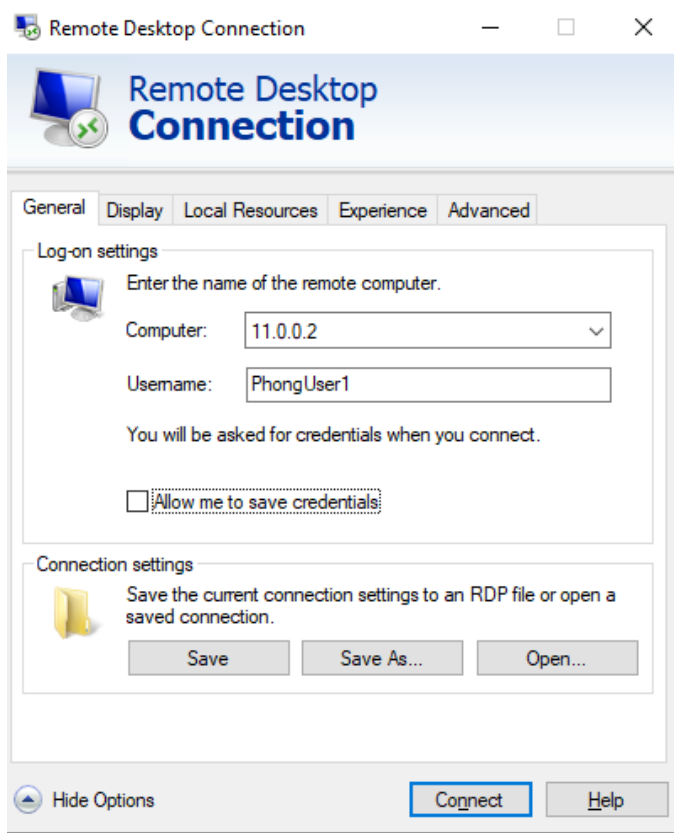
Cài đặt lại quyền remote



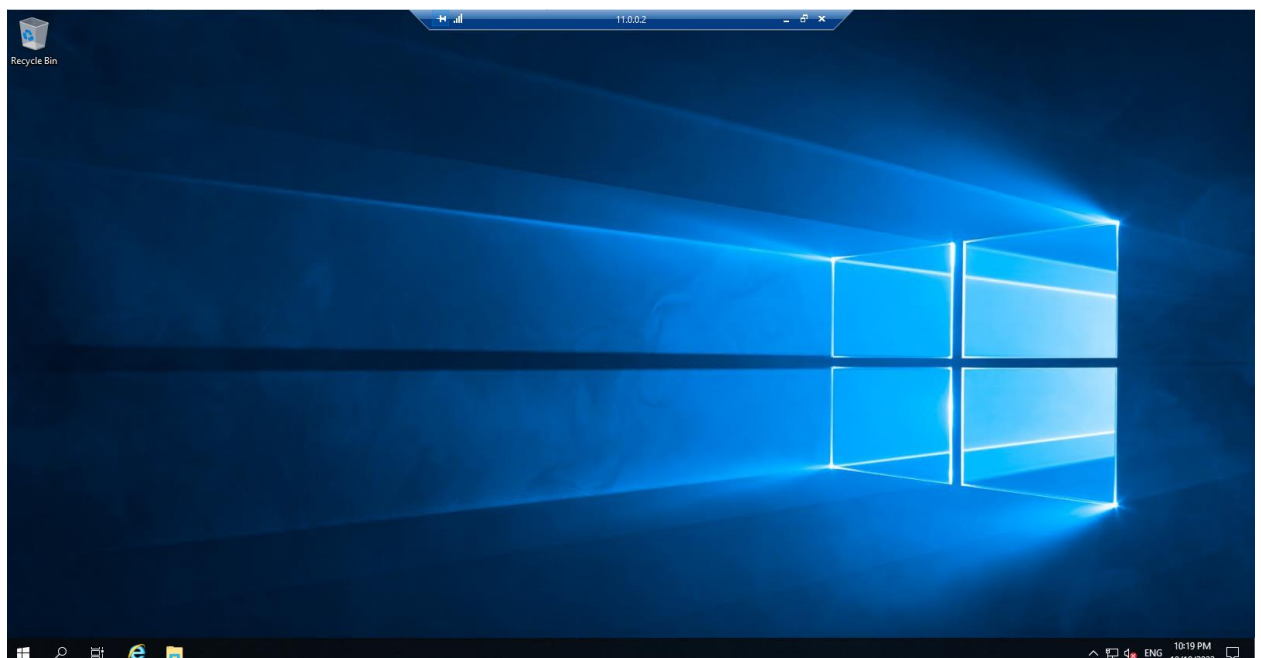




Remote bằng user1



Remote thành công



- VII. OpenVPN và Remote desktop từ máy Internet vào LAN
- Tạo LDAP để liên kết tài khoản windows server với pfsense



Tạo Organization Unit pfsense trong AD và chuyển 2 tài khoản đã tạo vào

Active Directory Users and Comp	Name	Type	Description
> Saved Queries			
✓ N20DCAT041.com			
> Built-in	N20DCAT041_Group	Security Group ...	
> Computers	PhongUser1	User	
> Domain Controllers	PhongUser2	User	
> ForeignSecurityPrincipals			
> Managed Service Account			
Users			
pfsense			

Tạo Authentication Server

System / User Manager / Authentication Servers			
Users	Groups	Settings	Authentication Servers
Authentication Servers			
Server Name	Type	Host Name	Actions
Local Database		pfSense	
+ Add			

Users
Groups
Settings
Authentication Servers

Server Settings

Descriptive nameAD

TypeLDAP

LDAP Server Settings

Hostname or IP address11.0.0.2

NOTE: When using SSL/TLS or STARTTLS, this hostname MUST match a Subject Alternative Name (SAN) c server SSL/TLS Certificate.

Port value389

TransportStandard TCP

Peer Certificate AuthorityGlobal Root CA List

This CA is used to validate the LDAP server certificate when 'SSL/TLS Encrypted' or 'STARTTLS Encrypted' CA used by the LDAP server.

Protocol version3

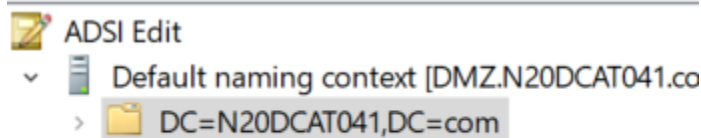
Server Timeout25

Timeout for LDAP operations (seconds)

Search scopeLevel

Entire Subtree

Sử dụng ADSI để lấy Base DN, Authentication containers, Bind credentials



Name	Class	Distinguished Name
CN=Builtin	builtinDomain	CN=Builtin,DC=N20DCAT041,DC=com
CN=Computers	container	CN=Computers,DC=N20DCAT041,DC=com
OU=Domain Controllers	organization...	OU=Domain Controllers,DC=N20DCAT041,DC=com
CN=ForeignSecurityPrincipals	container	CN=ForeignSecurityPrincipals,DC=N20DCAT041,DC=com
CN=Keys	container	CN=Keys,DC=N20DCAT041,DC=com
CN=LostAndFound	lostAndFound	CN=LostAndFound,DC=N20DCAT041,DC=com
CN=Managed Service Accou...	container	CN=Managed Service Accounts,DC=N20DCAT041,DC=com
CN=NTDS Quotas	msDS-Quota...	CN=NTDS Quotas,DC=N20DCAT041,DC=com
OU=pfsense	organization...	OU=pfsense,DC=N20DCAT041,DC=com
CN=Program Data	container	CN=Program Data,DC=N20DCAT041,DC=com

Name	Class	Distinguished Name
CN=Administrator	user	CN=Administrator,CN=Users,DC=N20DCAT041,DC=com
CN=Allowed RODC Password Replication Group	group	CN=Allowed RODC Password Replication Group,CN=Users,DC=N20DCAT041,DC=com

Base DN

---

**Authentication containers**  
 [Select a container](#)

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

---

**Extended query** ☐ Enable extended query

---

**Bind anonymous** ☐ Use anonymous binds to resolve distinguished names

---

**Bind credentials**

---

**Initial Template**

## Setting User manager

System / [User Manager](#) / [Settings](#)

[Users](#)
[Groups](#)
[Settings](#)
[Authentication Servers](#)

### Settings

**Session timeout**

Time in minutes to expire idle management sessions. The default is 4 hours (240 minutes). Risk!

---

**Authentication Server**

---

**Password Hash Algorithm**

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 algorithms.

---

**Shell Authentication** ☐ Use Authentication Server for Shell Authentication

If RADIUS or LDAP server is selected it is used for console and SSH authentication. To allow logins with RADIUS credentials, equivalent local users with the expected password must be created. To allow logins with LDAP credentials, Shell Authentication Group DN must be specified.

---

**Auth Refresh Time**

Time in seconds to cache authentication results. The default is 30 seconds, maximum is 60 seconds.

## 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		
OU=Domain Controllers,DC=N20DCAT041,DC=com		
OU=pfsense,DC=N20DCAT041,DC=com		
CN=Users,DC=N20DCAT041,DC=com		
CN=Users,CN=Builtin,DC=N20DCAT041,DC=com		

## Thử đăng nhập bằng tài khoản user1

Diagnostics / Authentication

User PhongUser1 authenticated successfully. This user is a member of groups:

Authentication Test

Authentication Server

AD

Select the authentication server to test against.

Username

PhongUser1

Password

.....

Debug

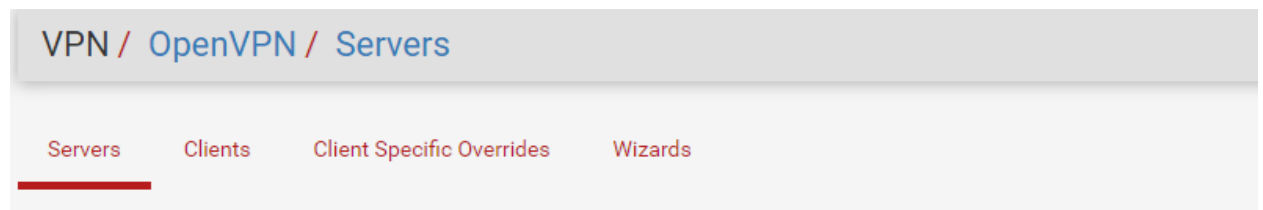
☐ Set debug flag

Sets the debug flag when performing authentication, which may trigger additional

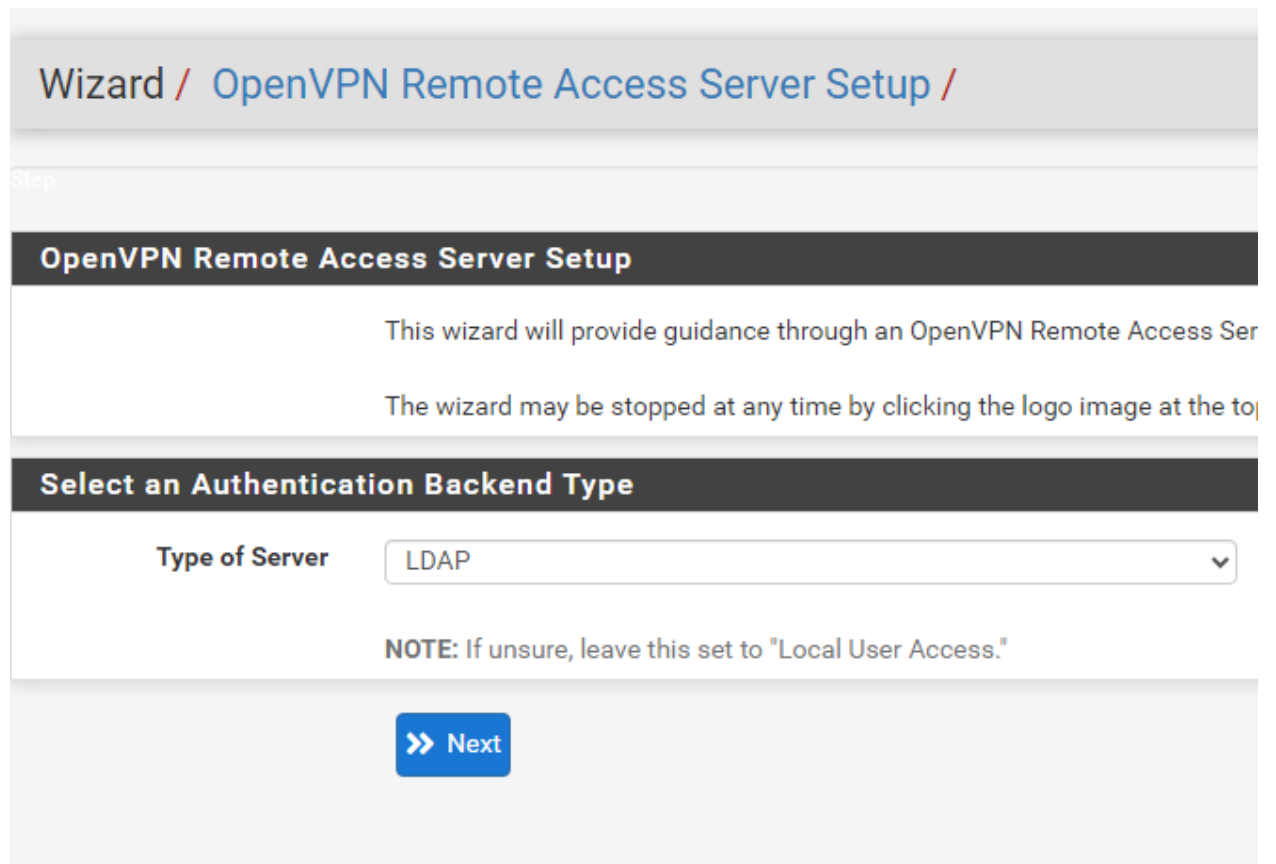
Test

## - Cấu hình OpenVPN

Chọn Wizard



Bắt đầu cấu hình



Step 1 of 11

## LDAP Server Selection

OpenVPN Remote Access Server Setup Wizard

### LDAP Authentication Server List


LDAP servers

AD



» Add new LDAP server

» Next

<b>Descriptive name</b>	<input type="text" value="CA-VPN"/>
A name for administrative reference, to identify this certificate.	
<b>Randomize Serial</b>	<input checked="" type="checkbox"/> Use random serial numbers when signing certificates. When enabled, serial numbers for certificates signed by this CA will be automatically sequential values.
<b>Key length</b>	<input type="text" value="2048 bit"/> 
Size of the key which will be generated. The larger the key, the more security slightly longer to validate leading to a slight slowdown in setting up new sessions. 2048 is the most common selection and 4096 is the maximum in common use. For more information see <a href="#">this link</a> .	
<b>Lifetime</b>	<input type="text" value="3650"/>
Lifetime in days. This is commonly set to 3650 (Approximately 10 years.)	
<b>Common Name</b>	<input type="text"/>
The internal name of the CA, used as a part of the CA subject. If left blank, the descriptive name will be used.	
<b>Country Code</b>	<input type="text" value="VN"/>
Two-letter ISO country code (e.g. US, AU, CA)	
<b>State or Province</b>	<input type="text" value="Ho Chi Minh"/>
Full State or Province name, not abbreviated (e.g. Texas, Indiana, Ontario).	
<b>City</b>	<input type="text" value="Thu Duc"/>
City or other Locality name (e.g. Austin, Indianapolis, Toronto).	
<b>Organization</b>	<input type="text" value="PTIT"/>
Organization name, often the company or group name.	
<b>Organizational Unit</b>	<input type="text" value="PTIT"/>
Organizational Unit name, often the department or division name.	

## Create a New Server Certificate

**Descriptive name**

A name for administrative reference, to identify this certificate.

**Key length**

Size of the key which will be generated. The larger the key, the more security it offers, but slightly longer to validate leading to a slight slowdown in setting up new sessions (not most common selection and 4096 is the maximum in common use. For more information see [Key Length](#)).

**Lifetime**

Lifetime in days. Server certificates should not have a lifetime over 398 days or some p

**Common Name**

The internal name of the server certificate, used as a part of the certificate subject. Typ used as a Subject Alternative Name (SAN). If left blank, the Descriptive Name value wil

**Country Code**

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

**State or Province**

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

**City**

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

**Organization**

Organization name, often the company or group name.

**Organizational Unit**



## General OpenVPN Server Information

### Description

A name for this OpenVPN instance, for administrative reference. It can be set however desired for the service (e.g. "Remote Technical Staff"). It is also used by OpenVPN Client Export to identify the service.

## 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 port must be open on the firewall.

## Tunnel Settings

### IPv4 Tunnel Network

This is the IPv4 virtual network or network type alias with a single entry used for private or public addresses. It can be expressed using CIDR notation (e.g. 10.0.8.0/24). The first usable address in the network (the network address) will be assigned to connecting clients.

A tunnel network of /30 or smaller puts OpenVPN into a special peer-to-peer mode which has several options, including Exit Notify, and Inactive.

### IPv6 Tunnel Network

This is the IPv6 virtual network or network type alias with a single entry used for private or public addresses. It can be expressed using CIDR notation (e.g. fe80::/64). The ::1 address in the network 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)

IPv4 networks that will be accessible from the remote endpoint. Expressed as a comma-separated list of network type aliases. This may be left blank if not adding a route to the local network through this tunnel.

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 OpenVPN tunnel.

The options on this step can add automatic rules to pass this traffic.

Traffic from clients to server

Firewall Rule

☒ Add a rule to permit connections to this OpenVPN server in

Traffic from clients through VPN

OpenVPN rule

☒ Add a rule to allow all traffic from connected clients to pass

>> Next

Trở lại với LDAP chỉnh lại mục peer certificate authority

Users

Groups

Settings

Authentication Servers

Server Settings

Descriptive name

AD

Type

LDAP

LDAP Server Settings

Hostname or IP address

11.0.0.2

NOTE: When using SSL/TLS or STARTTLS, this hostname MUST match a Subject Alternative Name server SSL/TLS Certificate.

Port value

389

Transport

Standard TCP

Peer Certificate Authority

CA-VPN

This CA is used to validate the LDAP server certificate when 'SSL/TLS Encrypted' or 'STARTTLS Encrypted' is selected. This CA is used by the LDAP server.

## Cài thêm package OpenVPN client export

System / Package Manager / Available Packages

Installed Packages

Available Packages

Search

Search term

openvpn

Both

Search

Clear

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>		

Install

## System / Package Manager / Package Installer

**pfSense-pkg-openvpn-client-export** installation successfully completed.

Installed Packages

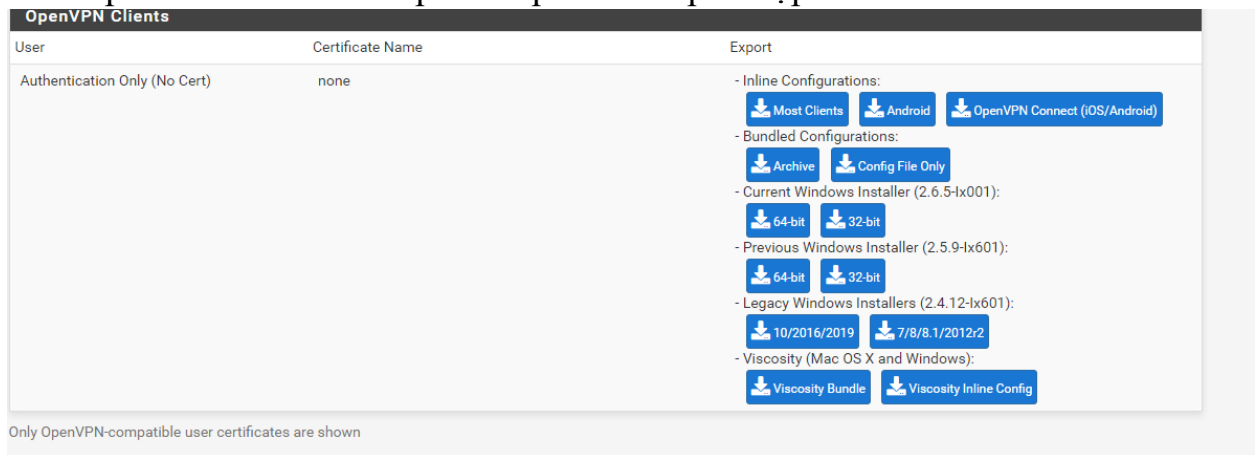
Available Packages

Package Installer

### Package Installation

```
[4/5] Installing 7-zip-22.01...
[4/5] Extracting 7-zip-22.01: ..... done
[5/5] Installing pfSense-pkg-openvpn-client-export-1.9_1...
[5/5] Extracting pfSense-pkg-openvpn-client-export-1.9_1: ..... done
Saving updated package information...
done.
Loading package configuration... done.
Configuring package components...
Loading package instructions...
Custom commands...
Executing custom_php_install_command()...done.
Writing configuration... done.
>>> Cleaning up cache... done.
Success
```

Vào OpenVPN > Client Export tải phiên bản phù hợp

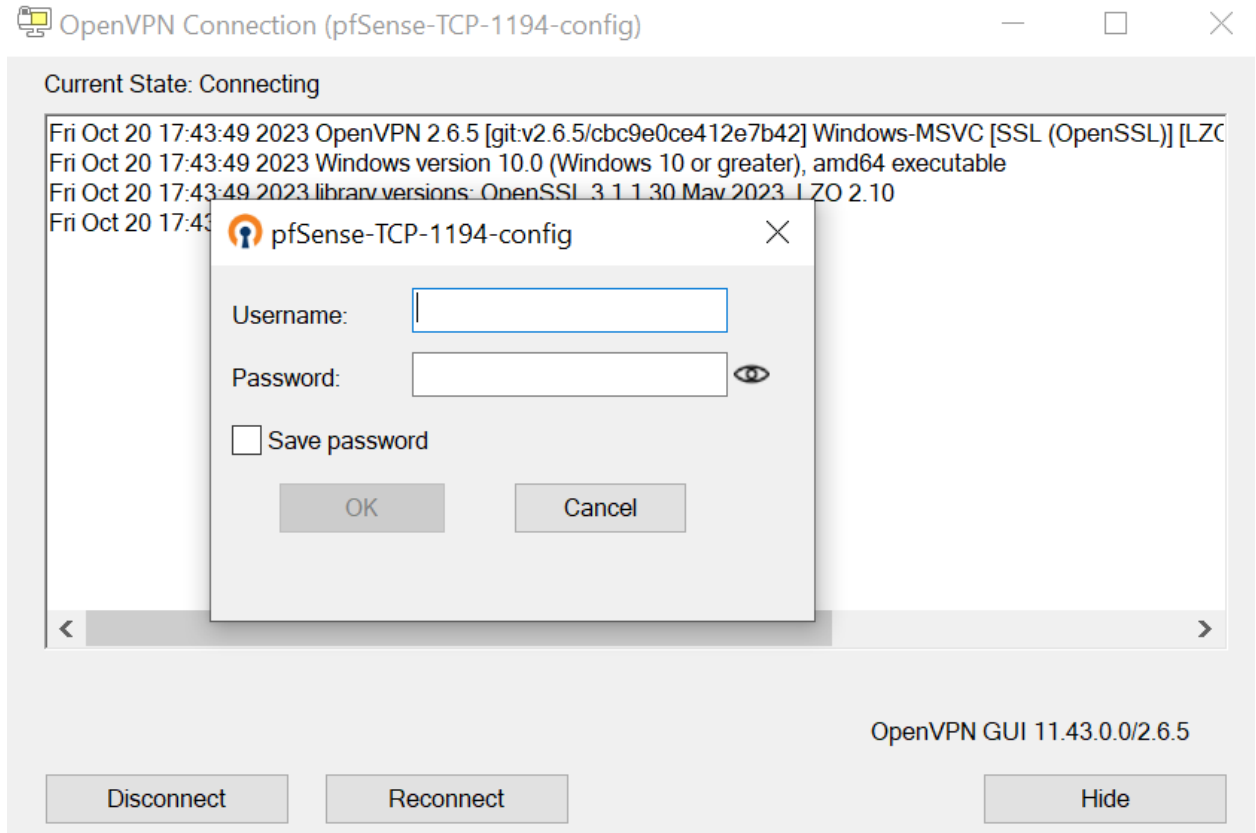


The screenshot shows the 'OpenVPN Clients' interface. The 'Export' section is active, displaying a list of download buttons for different configurations and operating systems. The buttons are organized into several categories:

- Inline Configurations:** Most Clients, Android, OpenVPN Connect (iOS/Android).
- Bundled Configurations:** Archive, Config File Only.
- Current Windows Installer (2.6.5-ix001):** 64-bit, 32-bit.
- Previous Windows Installer (2.5.9-ix601):** 64-bit, 32-bit.
- Legacy Windows Installers (2.4.12-ix601):** 10/2016/2019, 7/8/8.1/2012r2.
- Viscosity (Mac OS X and Windows):** Viscosity Bundle, Viscosity Inline Config.

Below the buttons, a note states: 'Only OpenVPN-compatible user certificates are shown'.

Cài đặt trên máy thật và tiến hành kết nối vpn



The screenshot shows the 'OpenVPN Connection (pfSense-TCP-1194-config)' window. The 'Current State' is 'Connecting'. The log area displays the following information:

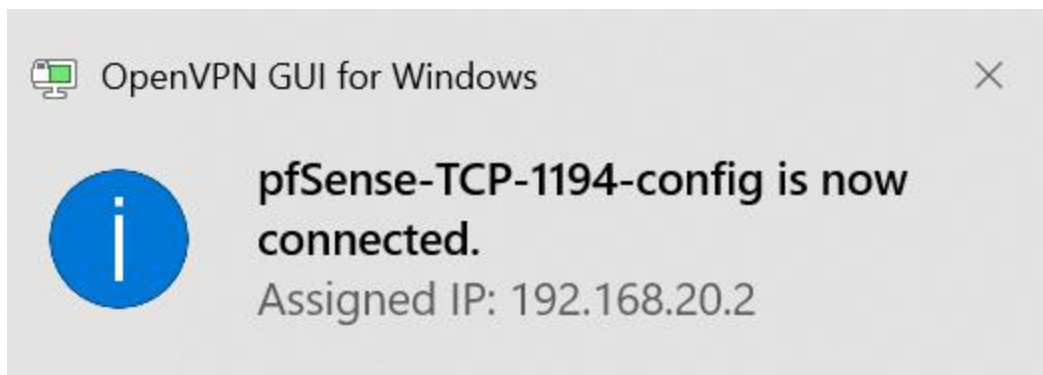
```
Fri Oct 20 17:43:49 2023 OpenVPN 2.6.5 [git.v2.6.5/cbc9e0ce412e7b42] Windows-MSVC [SSL (OpenSSL)] [LZO]
Fri Oct 20 17:43:49 2023 Windows version 10.0 (Windows 10 or greater), amd64 executable
Fri Oct 20 17:43:49 2023 library versions: OpenSSL 3.1.1 30.May.2023, LZO 2.10
Fri Oct 20 17:43:49 2023
```

A login dialog box is overlaid on the window, titled 'pfSense-TCP-1194-config'. It contains the following fields and controls:

- Username:** A text input field.
- Password:** A password input field with a toggle icon (eye) to show/hide the password.
- Save password:** A checkbox.
- Buttons:** OK and Cancel.

At the bottom of the window, the version 'OpenVPN GUI 11.43.0.0/2.6.5' is displayed. Below the version, there are three buttons: Disconnect, Reconnect, and Hide.

Kết nối thành công



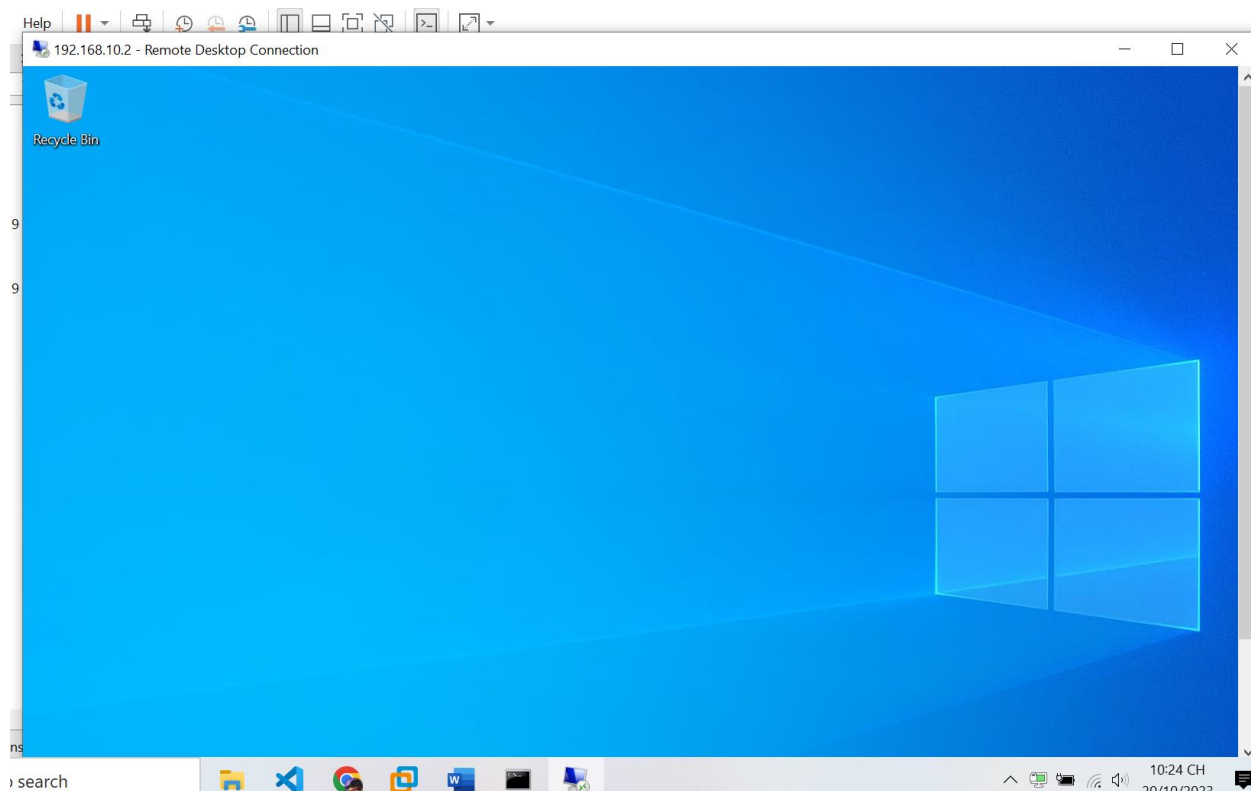
Ta đã có thể ping tới máy trong Lan

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

Pinging 192.168.10.2 with 32 bytes of data:
Reply from 192.168.10.2: bytes=32 time=1368ms TTL=127
Reply from 192.168.10.2: bytes=32 time=1ms TTL=127
Reply from 192.168.10.2: bytes=32 time=14ms TTL=127
Reply from 192.168.10.2: bytes=32 time=6ms 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 = 1ms, Maximum = 1368ms, Average = 347ms
```

Remote Desktop thành công



## Bắt gói tin bằng wireshark

1	0.000000	192.168.10.2	192.168.20.2	TLSv1.2	105 Application Data
2	0.045315	192.168.20.2	192.168.10.2	TCP	54 15008 → 3389 [ACK] Seq=1 Ack=52 Win=8195 Len=0
3	2.002847	192.168.10.2	192.168.20.2	TLSv1.2	105 Application Data
4	2.047579	192.168.20.2	192.168.10.2	TCP	54 15008 → 3389 [ACK] Seq=1 Ack=103 Win=8195 Len=0
5	2.402194	192.168.20.2	192.168.10.2	RDPUDP	51 [Malformed Packet]
6	2.407851	192.168.10.2	192.168.20.2	RDPUDP	60 [Malformed Packet]
7	2.417671	192.168.20.2	192.168.10.2	RDPUDP	53 [Malformed Packet]
8	3.016709	192.168.10.2	192.168.20.2	TLSv1.2	105 Application Data
9	3.062018	192.168.20.2	192.168.10.2	TCP	54 15008 → 3389 [ACK] Seq=1 Ack=154 Win=8194 Len=0
10	5.045662	192.168.10.2	192.168.20.2	TLSv1.2	105 Application Data
11	5.090539	192.168.20.2	192.168.10.2	TCP	54 15008 → 3389 [ACK] Seq=1 Ack=205 Win=8194 Len=0
12	6.060862	192.168.10.2	192.168.20.2	TLSv1.2	105 Application Data