

## A. Client to Gateway VPN (Remote Access VPN)

1. Xây dựng hệ thống mạng sao cho thỏa sơ đồ sau:



- 2. Tạo một tài khoản người dùng mới (VD: VPNUSER1) và cấp quyền truy cập VPN tại Winserver
  - a. Vào Server ManagerTrên Server Manager dashboard chọn Tools -> chọn Computer Management.
  - b. Lúc này cửa sổ Computer Management sẽ hiện ra. Tiếp theo, ta trỏ chuột vào Local Users and Groups -> chọn User -> chọn tab Action -> chọn New User -> Tạo tài khoản: VPNUSER1 có mật khẩu.

-		Co	omputer Management		_ 🗆 X
File Action View Help					
🗢 🔿 🙇 📰 🖸 📑 🛽		_	-		
🛃 Computer Management (Local	Name	Full Name	Description		Actions
⊿ is System Tools	Administrator		Built-in account for administering		Users 🔺
First Scheduler	👧 Guest		Built-in account for guest access t		More Actions
<ul> <li>Reserve Folders</li> <li>Reserve And State And St</li></ul>			New User		
Users Groups		User name: vpnu	ser1		
▷ N Performance		Full name:			
A Storage		Description:			
Windows Server Backup				-	
Disk Management		Password:	•••••		
Services and Applications		Confirm anonymatic	[		
		Commin password.		-	
		User must change pa	assword at next logon		
		User cannot change	password		
		Password never expi	res		
		Account is disabled			
				_	
				_	
		Help	Create Close		
	l				
< III >					



Webs

c. Tại Properties của tài khoản chọn tab Dial-in, đánh dấu vào mục Allow Access trong phần Remote Access Permission

	vpn	user1 Prop	erties	?	x		
General	Member Of	Profile	Environment	Sess	ions		
Remote control     Remote Desktop Services Profile     Dial-in       Network Access Permission     Image: Control access     Image: Control access       C     Control access through NPS Network Policy       Verify Caller-ID:       Callback Options							
No Callback     Set by Caller (Routing and Remote Access Service only)     Always Callback to:							
Assign Static IP Addresses     Define IP addresses to enable for this     Dial-in connection.     Static IP Addresses							
Define rou connection	Define routes to enable for this Dial-in Static Routes						
	ОК	Cancel	Apply	He	elp		

- 3. Cấu hình PC1 thành VPN Gateway với loại kết nối là Client to Gateway (Remote Access VPN)
  - a. Tại Server Manager dashboard, chỏ chuột vào đường dẫn Add Roles And Features (số 2)
  - b. Khi màn hình hiển thị bảng Before you begin xuất hiện, bấm next.
  - c. Tiếp theo chọn role-based or feature-based installation sau đó bấm Next
  - d. Tại trang, Server Selection, chọn A Server From The Server Pool và chọn server trong phần Server Pool. Sau đó bấm next

Select server ro Before You Begin Installation Type Server Selection Server Roles	CS Select one or more roles to install on the selected server. Roles DHCP Server DHCP Server Roles	DESTINATION SERVER srv Description Remote Access provides seamless connectivity through DirectAccess, VPN and Web Application Provy
Features Remote Access Role Services Confirmation Results	□       Fax Server         □       File and Storage Services (1 of 12 installed)         □       Hyper-V         □       ■         □       Print and Document Services         □       Print and Document Services         □       Remote Access         □       Volume Activation Services         □       Web Server (IIS)         □       Windows Deployment Services         □       Windows Server Essentials Experience         □       Windows Server Update Services	DirectAccess provides an Always On and Always Managed experience. RAS provides traditional VPN services, including site-to-site (branch-office or cloud-based) connectivity. Web Application Proxy enables the publishing of selected HTTP- and HTTPS-based applications from your corporate network to client devices outside of the corporate network. Routing provides traditional routing capabilities, including NAT and othe connectivity options. RAS and Routing can be deployed in single- tenant or multi-tenant mode.



- e. Trên trang Select Server Roles, chỏ chuột hộp Remote Access
- f. Tại trang Features, ta bấm Next để bỏ qua
- g. Ở trang Remote Access, ta sẽ chọn DirectAccess And VPN (RAS) -> bấm Add Features
- h. Cuối cùng, tại trang Confimation, chọn Install để tiến hành cài vai trò Remote Access

<b>a</b>	Add Roles and Features Wizard	-		x
Confirm ins	stallation selections		SERVE	R ∾
Before You Begin	To install the following roles, role services, or features on selected server, click Install.	ing o		<u> </u>
Installation Type Server Selection Server Roles Features	Restart the destination server automatically if required Optional features (such as administration tools) might be displayed on this page because been selected automatically. If you do not want to install these optional features, click Pre- their check boxes.	they ha	ave o clei	ar
Remote Access Role Services	Remote Access DirectAccess and VPN (RAS) Remote Server Administration Tools			
Results	Role Administration Tools Remote Access Management Tools Remote Access GUI and Command-Line Tools Remote Access module for Windows PowerShell			
	Export configuration settings Specify an alternate source path Go to System	Vind	OW	'S of Pan
	< Previous Next > acti Install/Viro	OW <b>Ca</b>	ncel	

- i. Cấu hình VPN Gateway: Tại Server Manager dashboard -> chọn Tools-> chọn Routing and Remote Access
- j. Trỏ chuột phải vào tên server, (trong trường hợp này là SRV) -> Bấm chọn Configure and Enable Routing and Remote Access.
- k. Sau đó trên màn hình sẽ xuất hiện Routing and Remote Access wizard -> bấm next



## I. Ở phần Configuration, chọn Remote access (dial-up or VPN)

Routing and Remote Access Server Setup Wizard
<b>Configuration</b> You can enable any of the following combinations of services, or you can customize this server.
<ul> <li>Remote access (dial-up or VPN) Allow remote clients to connect to this server through either a dial-up connection or a secure virtual private network (VPN) Internet connection.</li> <li>Network address translation (NAT) Allow internal clients to connect to the Internet using one public IP address.</li> <li>Virtual private network (VPN) access and NAT Allow remote clients to connect to this server through the Internet and local clients to connect to the Internet using a single public IP address.</li> <li>Secure connection between two private networks Connect this network to a remote network, such as a branch office.</li> <li>C ustom configuration Select any combination of the features available in Routing and Remote Access.</li> </ul>
< Back Next > Cancel
m. Ó mục Remote Access -> chọn VPN -> Next

- n. Chọn Ethernet adapter kết nối với mạng Internet -> Next
- o. ở phần IP Address Assignment -> chọn Automatically ->Next
- p. Ở mục Managing Multiple Remote Access Servers -> Bấm No -> Next -> Finish
- q. Nếu ta nhận được thông bó về DHCP Relay Agent ->bấm OK





DC: 276 - 278 Ung Văn Khiêm, P.25, Q.Bình Thạnh, Tp Hồ Chí Minh DT: (028) 35124257 | Hotline: 0933427079 Email: vnpro@vnpro.org

	Routing and Remote Access Server Setup Wizard						
VPN Connection To enable VPN clients to connect to this server, at least one network interface must be connected to the Internet.							
Selec	t the network interface Net <u>w</u> ork interfaces:	that connects this server to the Inte	emet.				
	Name Ethernet Ethernet	Description Intel(R) PRO/1000 MT Intel(R) PRO/1000 MT	IP Address 10.10.10.1 192.168.1.254				
	Enable security on the selected interface by setting up static packet filters. Static packet filters allow only VPN traffic to gain access to this server through the selected interface.						
		< <u>B</u> ack	Next > Cancel				

Tiếp theo ta chọn Next -> Remote Access (Dial-up or VPN) -> VPN ->Chọn card mạng kết nối với mạng internet -> không chọn "Enable security on the selected interface..." Cuối cùng ta chọ Next -> Chọn: "No, use Routing and Remote Access to authenticate connection requests" -> Next -> Finish

- 4. Tại PC2(là máy Remote Access client) cấu hình kết nối VPN để có thể truy cập vào nội mạng LAN (192.168.1.0/24)
  - a. Ta vào Network and Sharing Center ->Chọn Set up a connection or network -> Connect to a workplace -> Next -> Use my Internet connection (VPN) -> I'll set up an Internet connection later -> nhập Internet address: 10.10.10.1 là địa chỉ IP của VPN server -> Create.



– 🗆 X

~	🜆 Connect to a Workplace
---	--------------------------

Internet address:	10.10.10.1
Destination name:	VPN Connection 1
Use a smart card	
🗹 Remember my c	redentials
Allow other peop This option allow	ple to use this connection vs anyone with access to this computer to use this connection.

- Tiếp theo tại Network and Sharing Center, ta chọn change adapter settings -> Chọn card mạng VPN vừa tạo -> Connect -> Nhập tài khoản và mật khẩu được tạo tại Server VPN

Windows S	ecurity	N		×
Sign in	1	63		
8	User name			]
	Password			]
	Domain:			
	OK		Cancel	

r. Kiểm tra:

Tại PC này, thực hiện cmd -> ipconfig /all -> Kiểm tra IP trên card mạng VPN.



Vậy là chúng ta đã kết nối VPN thành công. Card mạng VPN lúc này là 192.168.1.104

Ethernet adapter Ethernet:

Connection-specific DNS Suffix . : Link-local IPv6 Address . . . . : fe80::e9ed:e8dc:6c94:516a%5 IPv4 Address. . . . . . . . . : 10.10.10.2 Subnet Mask . . . . . . . . . : 255.255.255.0 Default Gateway . . . . . . . : : PPP adapter VPN Connection: Connection-specific DNS Suffix . :

- Tại PC2: cmd -> ping 192.168.1.1

Lúc này hai PC có thể ping được với nhau.



## B. Gateway to Gateway VPN (Site to Site VPN)

 Xây dựng hệ thống mạng sao cho thỏa sơ đồ sau: Các Window Server vẫn phải cấu hình thành VPN Gateway. Cách cấu hình giống bài phía trên.

19	2.168.1.0/24			10.10.10.0/24				172.16.1.0/24		
	e0					-      -				
► PC2		2 Winserver2	.1		.2	Winserver1	.2		.1	► PC1

- Tạo tài khoản người dùng Local mới và cấp quyền truy cập VPN (dial-in) tại Winserver1 và Winserver2.
  - Winserver1: username: hcm, password: P@ssw0rd1
  - Winserver2: username: hanoi, password: P@ssw0rd2
- Cấu hình Winserver1, Winserver2 thành VPN Server với loại kết nối Gateway to Gateway: Cấu hình trên Winserver1 (Winserver2 thực hiện tương tự)
  - a. Trong cửa sổ Routing and Remote Access ->nhấp chuột phải vào tên server -> Configure and Enable Routing and Remote Access
  - b. Không như trường hợp Client to Gateway VPN, ta chọn Custom Configuration



- c. Ở mục Custom Configuration, ta chọn:
  - VPN access.
  - Demand-dial connections (Used for branch office routing).
  - LAN routing

Routing and Remote Access Server Setup Wizard
Custom Configuration When this wizard closes, you can configure the selected services in the Routing and Remote Access console.
Select the services that you want to enable on this server.  VPN access  Dial-up access  Demand-dial connections (used for branch office routing )  NAT
I LAN routing
< Back Next > Cancel

- d. Sau đó, ta chọn finish -> OK
- e. Khai báo thông tin kết nối giữa hai VPN Server: tại cửa sổ Routing and Remote Access -> SRV1 (local)
- f. Bấm chuột phải vào Network Interfaces -> chọn New Demand-dial Interface.
- g. Ta gõ phần Interface name: tùy ý -> chọn Next
- h. Ở mục Connection Type, ta chọn Connect using virtual private networking (VPN) -> chọn Next
- i. Ở mục VPN Type, ta chọn Point to Point tunneling protocol (PPTP).-> chọn Next
- j. Ở mục Destination Address: địa chỉ Public của Server là Winserver2 cần thiết lập kết nối VPN ở phía bên kia (trong trường hợp này là 10.10.10.2).
- k. Ở mục Protocol and Security: chọn Route IP packet on this interface.
- I. Ở mục Static Route for Remote Networks: Network Address Winserver2 (172.16.1.0/24).





Static Route	×
Remote Network Supp	port using IPv4
Destination:	172 . 16 . 1 . 0
Network Mask:	255 . 255 . 255 . 0
Metric:	1
Remote Network Supp	oort using IPv6
Destination:	
Prefix Length:	
Metric:	
	OK Cancel

- m. Ở mục Dial Out Credentials: thông tin tài khoản người dùng do Winserver2 tạo ra (Username "hanoi", password "P@ssw0rd2").
- n. Cấu hình cấp địa chỉ cho các máy kết nối VPN: Routing and Remote Access -> nhấp chuột phải vào tên server -> Propertiese -> ở tab IPv4 -> ta chọn Static Address Pool (192.168.1.100- 192.168.1.150) -> Add.



Х

?

WIN-QQUKR54GU9M (local) Properties

General	Securi able IPv4 address server c Dynamic Static ad	ty IP 4 Forw assign an ass Host ( dress p	arding ament — sign IPv Configur pool	Pv6 4 add ation	IKEv2 resses by Protocol (	PPP using: (DHCP)	Logg	jing
	From		To		Number	IP Ad	ldre	Mask
	192.16	5	192.168	5	100	192.1	168	255.255
			A	dd		Edit		Remove
Enz	able broz	adcast	name re	esolut	ion			
Use the following adapter to obtain DHCP, DNS, and WINS addresses for dial-up clients.								
Adapte	r:  /	Allow F	RAS to s	elect	adapter			•
			[		ОК	Ca	ncel	Apply

- o. Tại Network Interfaces chỏ chuột phải vào Interface vừa tạo -> Connect.
- 4. Cấu hình sử dụng giao thức L2TP sử dụng chìa khóa chia sẻ trước (Preshared key) giữa 2 VPN server.
  - Tại Winserver1:
    - Tại cửa sổ Routing and Remote Access -> chuột phải vào tên server (local) -> Properties -> chọn tab Security -> Chọn Allow custom IPSec policy for L2TP connection.



Tại mục Pre-shared Key, nhập mã bất kỳ (VD: P@ss24).

General	Security	IPv4	IPv6	IKEv2	PPP	Logging	
The Authentication provider validates credentials for remote access clients and demand-dial routers.							
Authent	Authentication provider:						
Windo	ws Authent	tication				Cor	nfigure
Auth	entication	Methods					
The acc	ounting pr	ovider ma	aintains a	a log of co	onnection	n requests	and
A							
Accoun	ting provid	er:			_	1	<i>c</i> 1
Windo	ws Accour	iting				Lor	ntigure
The custom IPsec policy specifies a preshared key for L2TP/IKEv2 connections. The Routing and Remote Access service should be started to set this option. IKEv2 initiators configured to authenticate this server using certificate will not be able to connect.							
🔽 Allo	w custom I	Psec pol	icy for Li	2TP/IKEv	2 conne	ction	
Preshar	red Key:						
P@ss24							
SSLO	Certificate E	Bindina:					
Select the certificate the Secure Socket Tunneling Protocol (SSTP) server should use to bind with SSL (Web Listener)							
Certifi	cate: De	efault			•	Viev	V
			_				
			(	ОК	Car	icel	Apply

- Tại Winserver2:
  - Interface vừa tạo ở câu trên -> Action -> Properties -> Security -> Chỉnh lại giao thức kết nối (Type of VPN) thành L2TP/IPSec VPN.



hanoi Droportion	
and Properties	×
General Options Security Networking	
Type of VPN:	
Layer 2 Tunneling Protocol with IPsec (L2TP/IPsec)	$\sim$
Advanced Setti Data encryption:	ngs
Require encryption (disconnect if server declines)	$\sim$
Authentication	
O Use Extensible Authentication Protocol (EAP)	
	$\sim$
Properties	
<ul> <li>Allow these protocols</li> <li>Unencrypted password (PAP)</li> </ul>	
Challenge Handshake Authentication Protocol (CHAP)	
a charcinge handanare / an endedition i horocol (ch/h)	
Microsoft CHAP Version 2 (MS-CHAP v2)	
Microsoft CHAP Version 2 (MS-CHAP v2)	
Microsoft CHAP Version 2 (MS-CHAP v2)	
Microsoft CHAP Version 2 (MS-CHAP v2)	

 Advanced Settings -> chọn "Use preshared key for authentication" -> nhập mật khẩu đã tạo ở trên (VD: P@ss24).

Advanced	Properties		×
L2TP			
🖲 Use j	preshared key for auth	nentication	
Key:	P@ss24	Ţ	
O Use (	certificate for authenti	cation	
V 🗸	erify the Name and Us	age attributes of the server's certific	ate
		OK Car	ncel

 Thực hiện tương tự nhưng đổi vai trò của Winserver1 và Winserver2 để cấu hình chứng thực ngược lại.

Website: www.vnpro.vn | Forum: www.vnpro.org | Video: https://www.youtube.com/@vnpro149



- Tại Winserver1, Winserver2: "Disconnect" interface vừa tạo sau đó "connect" lại thành công.