Windows Server 2016 : VPN





Summary

- 1. Introduction
- 2. Setting Up the VPN

1. Introduction

A virtual private network is "tunnelled" through a wide area network WAN like the Internet. That means the network can't be located on one physical location like a LAN. However, by using encryption and other security measures, a VPN can scramble all the data sent through the wide area network, so the network is "virtually" private.



2. Setting Up the VPN

On a first time, we have to install "Remote Access"



Add Roles and Features Wizard × <u>....</u> DESTINATION SERVER Select role services LykosS1 Select the role services to install for Remote Access Before You Begin Installation Type Role services Description Server Selection DirectAccess gives users the DirectAccess and VPN (RAS) experience of being seamlessly Server Roles Routing Web Application Proxy connected to their corporate Features network any time they have Internet access. With DirectAccess, mobile Remote Access computers can be managed any Role Services time the computer has Internet connectivity, ensuring mobile users Web Server Role (IIS) stay up-to-date with security and Role Services system health policies. VPN uses the connectivity of the Internet plus a Confirmation combination of tunnelling and data encryption technologies to connect remote clients and remote offices. < Previous Next > Install Cancel

In "Role Services" category, select "DirectAccess and VPN".

On the next steps, you only have to use the default settings. After that you can look at the screen preview and install the role.



When the functions are installed (sometimes you have to wait few minutes) you will find on this page the link to the starting up assistant. Click on "Open the Getting Started Wizard".



A new window is opening, you have to choose "Deploy VPN Only".



That opens the management console to Routing and Remote Access.



Right click your server's name and select "Configure and Enable Routing

🚊 Routing and Remote A File Action View He		- D	×	
	14			
Routing and Remote A	Access Routing and Remote Access			
LYKOSS1 (local)	Configure and Enable Routing and Remote Access Disable Routing and Remote Access	Access emote access to private networks. ne following:	^	
	All Tasks	tworks.		
	Delete Refresh	on the Action menu, click Add Server.		
	Properties			
	Help			
			~	
Configures Routing and Re	mote Access for the selected server			

and Remote Access".

Select "Custom configuration".

Routing and Rem	ote Access	- 🗆	\times
File Action View	Routing and Remote Access Server Setup Wizard Configuration You can enable any of the following combinations of services, or you can customize this server.		
() LYKUSSI (loca	OSS1 (loca C 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. C Ngtwork address translation (NAT) Allow internal clients to connect to the Internet using one public IP address. 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. Secure connection between two private networks Connect this network to a remote network, such as a branch office. Custom configuration Select any combination of the features available in Routing and Remote Access.		~
	< <u>B</u> ack <u>N</u> ext > Cancel		~

Edy BELAFRADJI

All Secure Ltd

Here, you have to select the "VPN Access" service to activate it.

🚊 Routing and Rem	ote Access	85		×
File Action View	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. Image: WPN access Image: Dial-up access Image: Degmand-dial connections (used for branch office routing) Image: NAT Image: LAN routing		orks.	0
		k Add	Server.	
	< <u>B</u> ack <u>N</u> ext > Cancel			~

A new window appears to recap the services you could use.



If you have a Firewall between your Internet and your Windows server, you have to open these ports to transfer them to your Windows Server.

For PPTP: 1723 TCP and Protocol 47 GRE (also known as PPTP Pass-through)

For L2TP on IPSEC: 1701 TCP and 500 UDP

For SSTP: 443 TCP

GRE; Tunnels GRE are made to help to not keep a state, that means each termination doesn't keep information of state or disponibility of the remove termination. It is used with PPTP

PPTP: Point-a-Point Tunnel Protocol is conceived by Microsoft. It's on every machines since Windows 2000.

L2TP: The Layer 2 Tunneling Protocol, based on the point a point protocol PPP is for sure one of the biggest virtual private network access. It brings the advantages of L2F and PPTP protocols.

STTP: Secure Socket Tunneling Protocol is a kind of VPN tunnel which give a mechanism to transport PPP or L2TP to a SSL 3.0 channel. SSL assure a transport security with keys negotiation, encryption, and control the datas' integrity.

Open the "Computer Management". Users have to be activated for the distant access to connect to your VPN server.

If you don't have a DHCP server around you, you have to add a pool of IP static addresses. It's usually the case if you have servers hosted on a service provider.

On your VPN server's properties, you can click on IPv4 to activate and configure the "static addresses pool".



In order to users can access to the server, configure an IP address to the network interface of your server which shared the same subnet than your addresses static pool.

Edy BELAFRADJI

Training Period