Windows Server 2016 : VPN

Windows Server 2016

Erasmus+

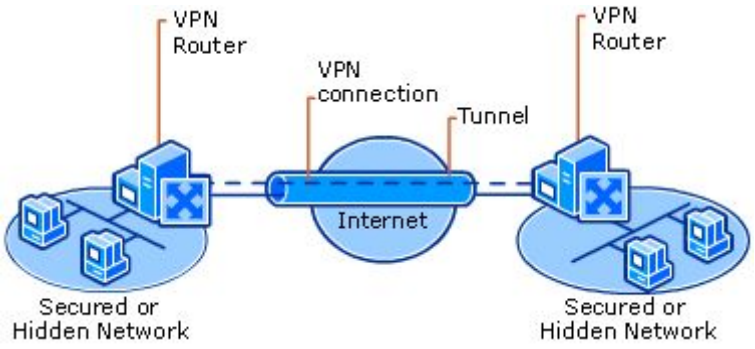
Summary

1. Introduction

2. Setting Up the VPN

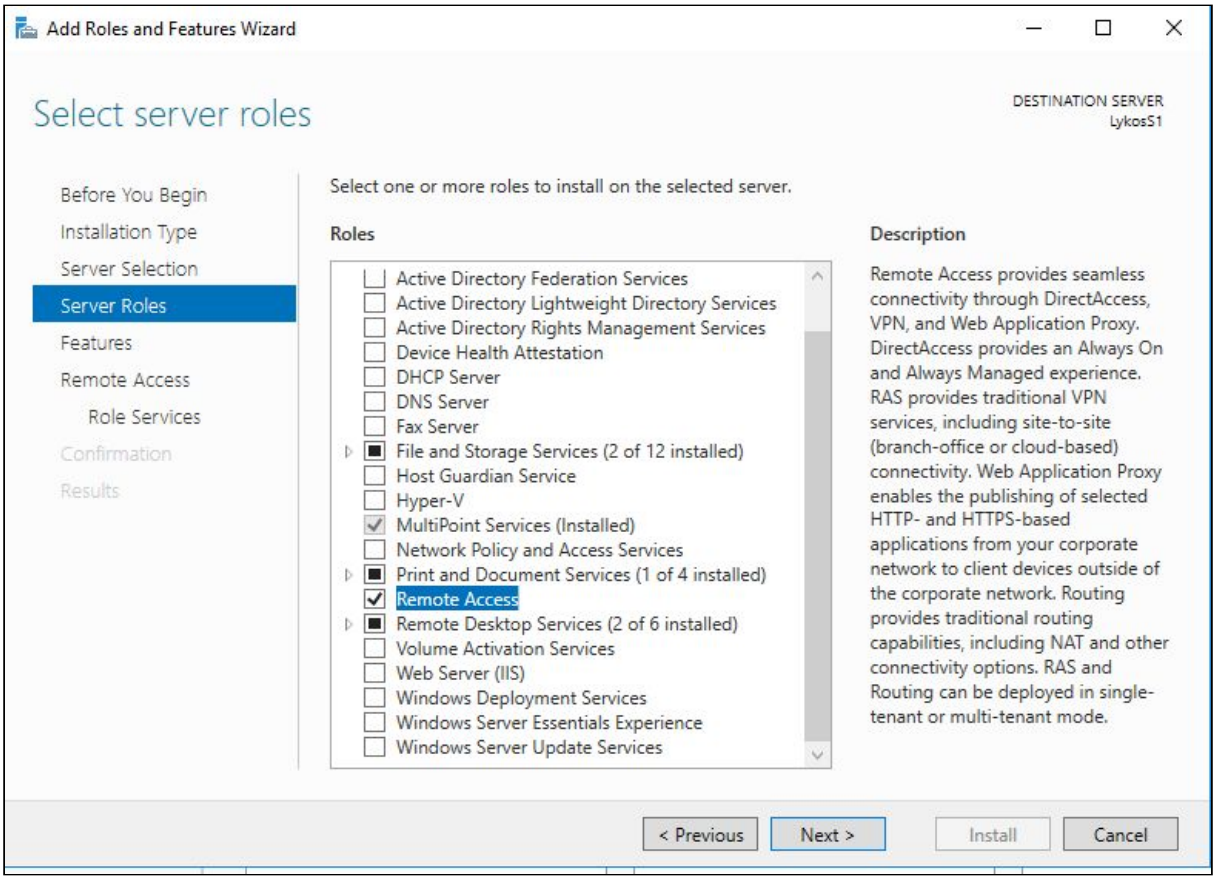
1. Introduction

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.

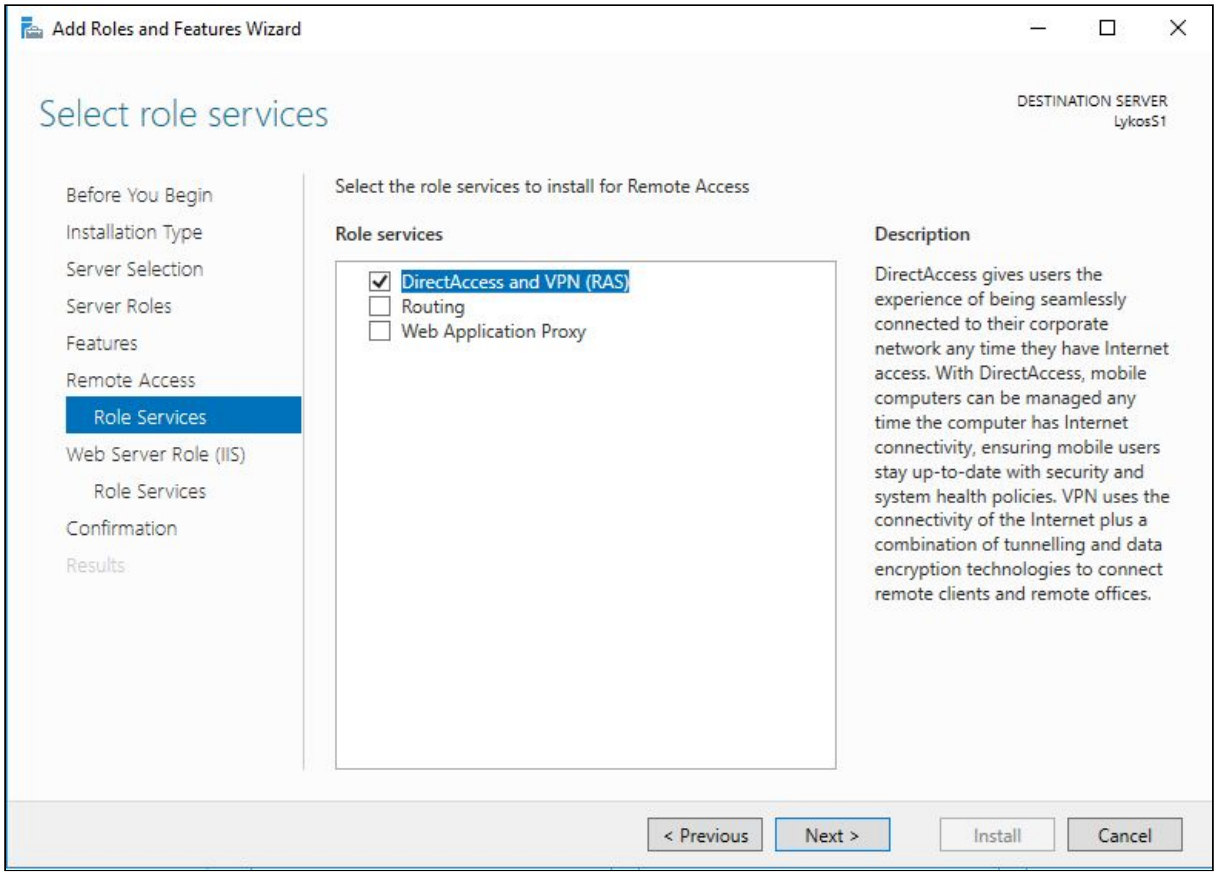


2. Setting Up the VPN

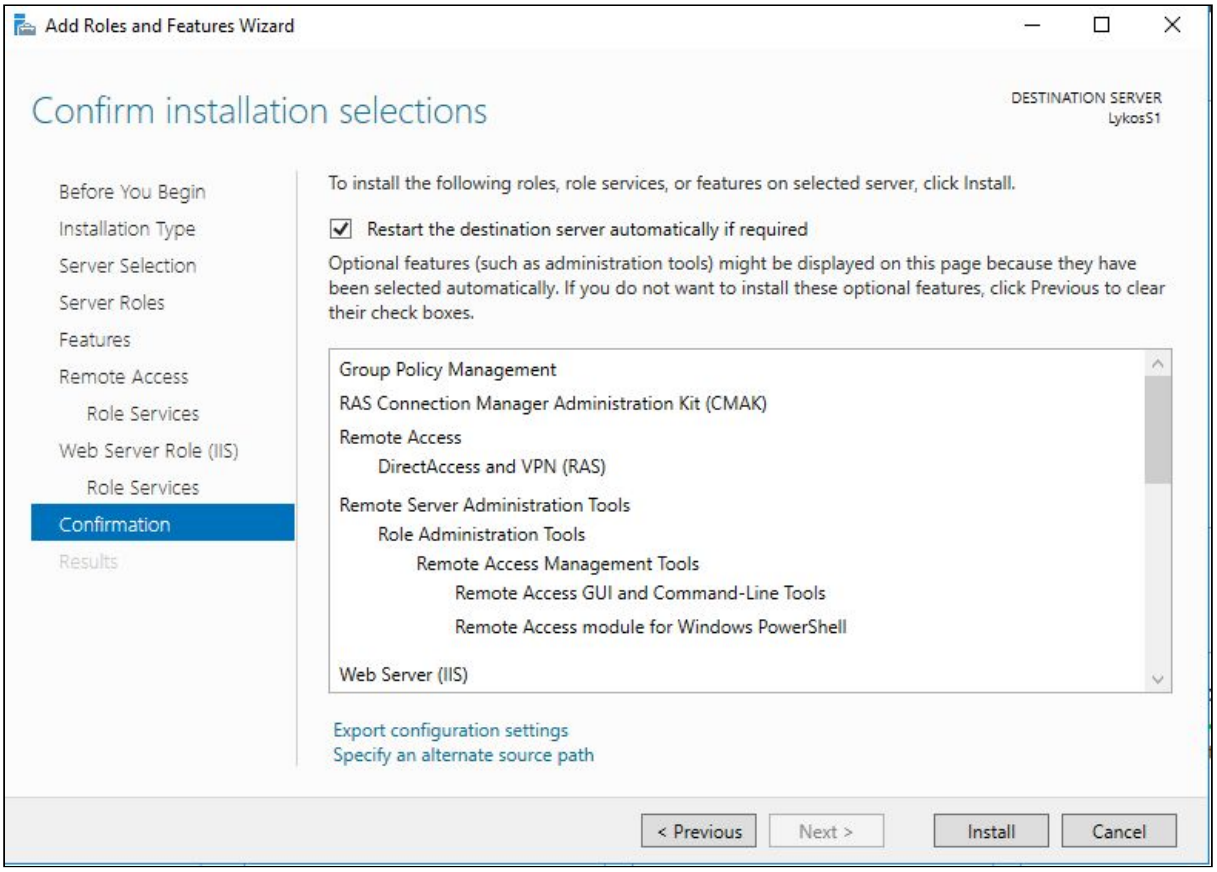
On a first time, we have to install “Remote Access”



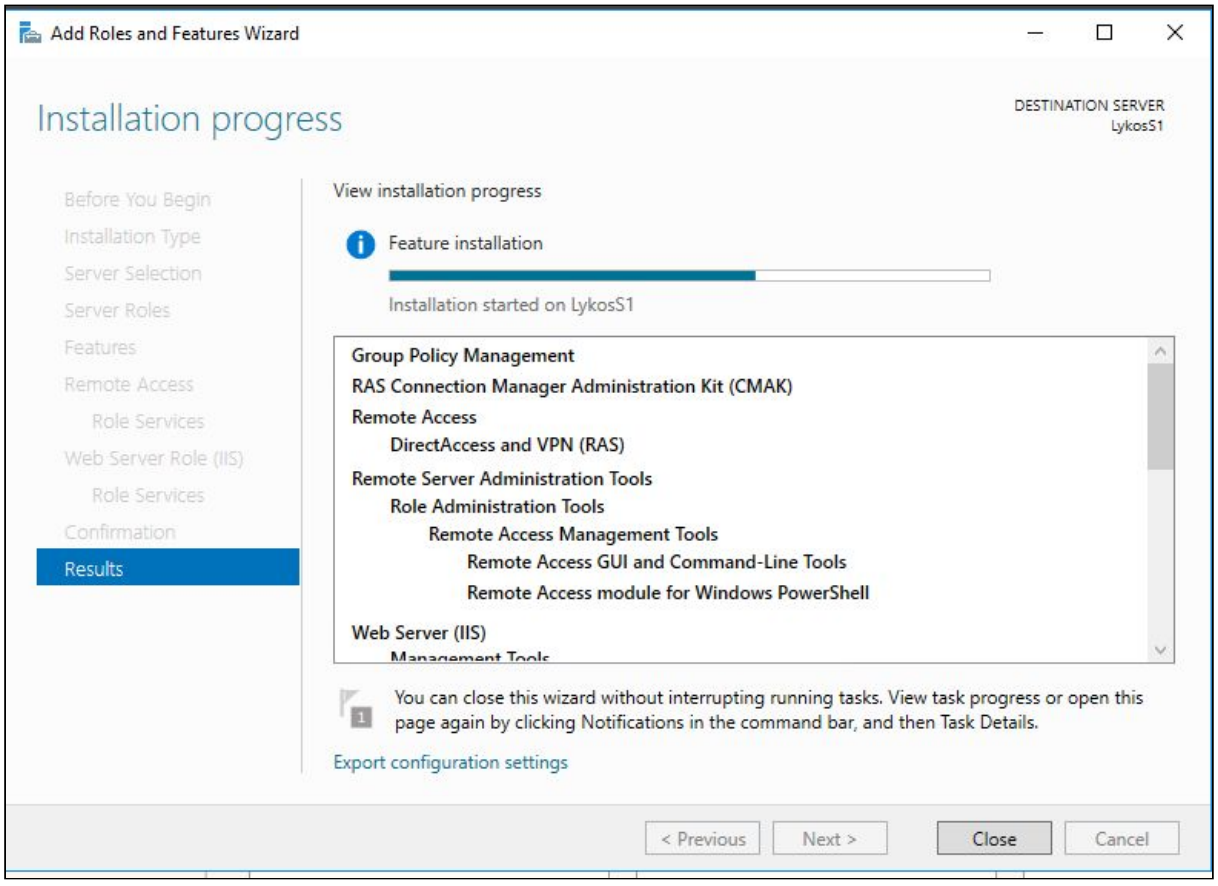
In “Role Services” category, select “DirectAccess and VPN”.



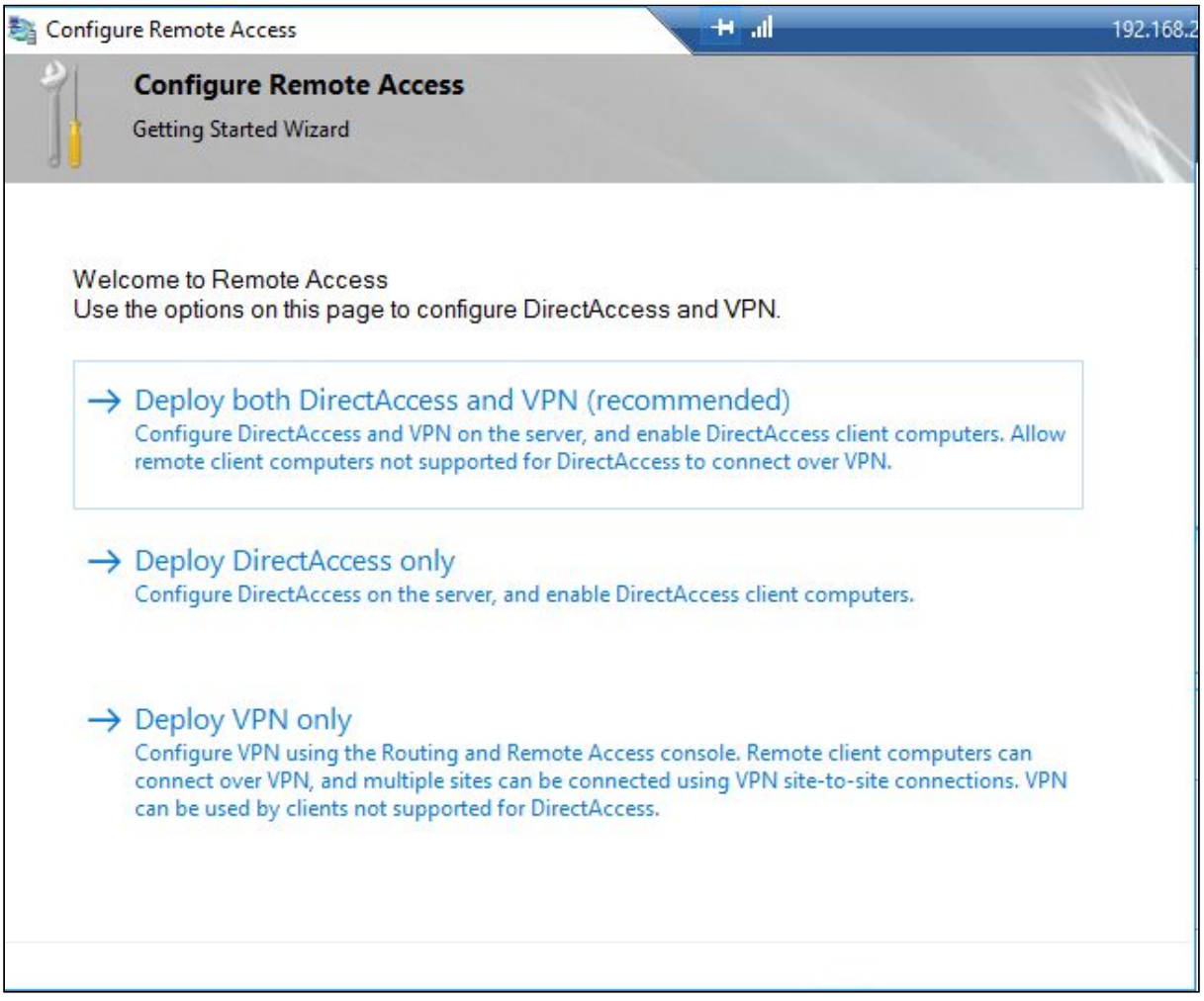
On the next steps, you only have to use the default settings.
After that you can look at the screen preview and install the role.



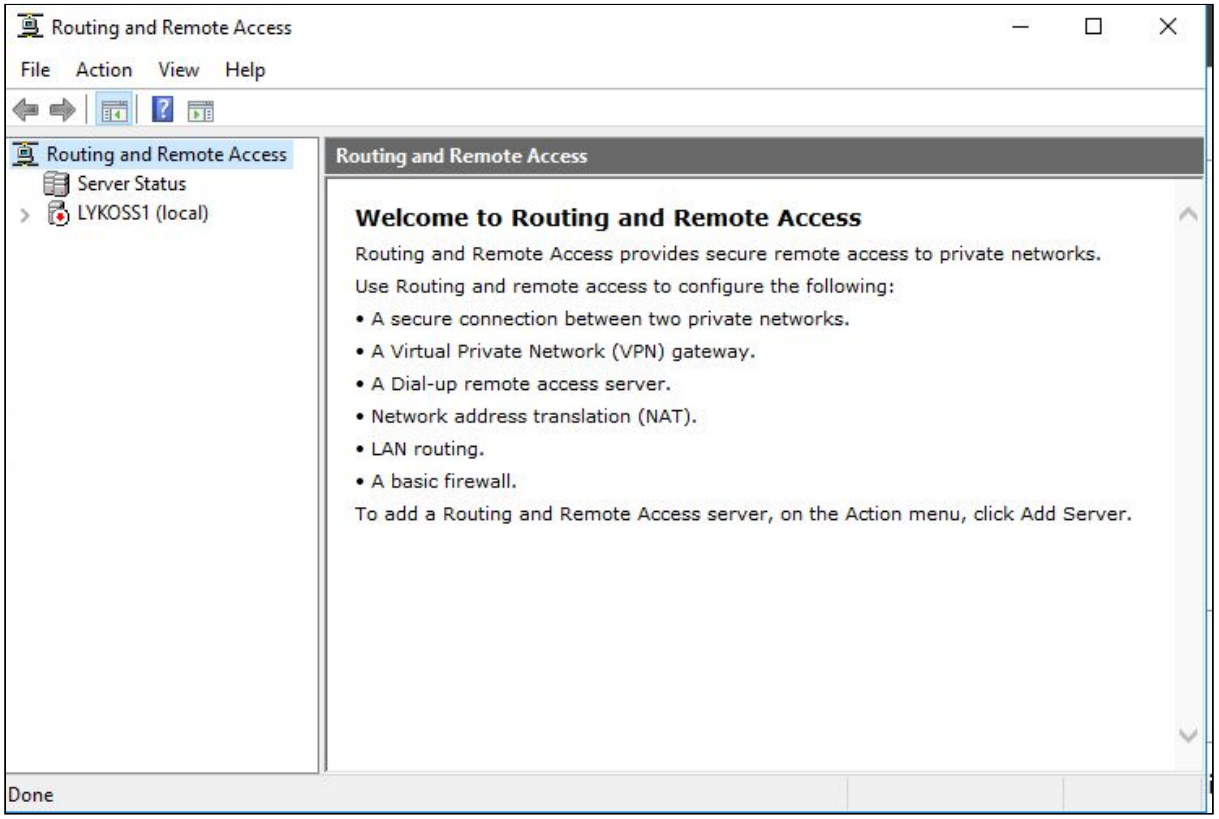
When the functions are installed (sometimes you have to wait few minutes) you will find on this page the link to the starting up assistant. Click on “Open the Getting Started Wizard”.



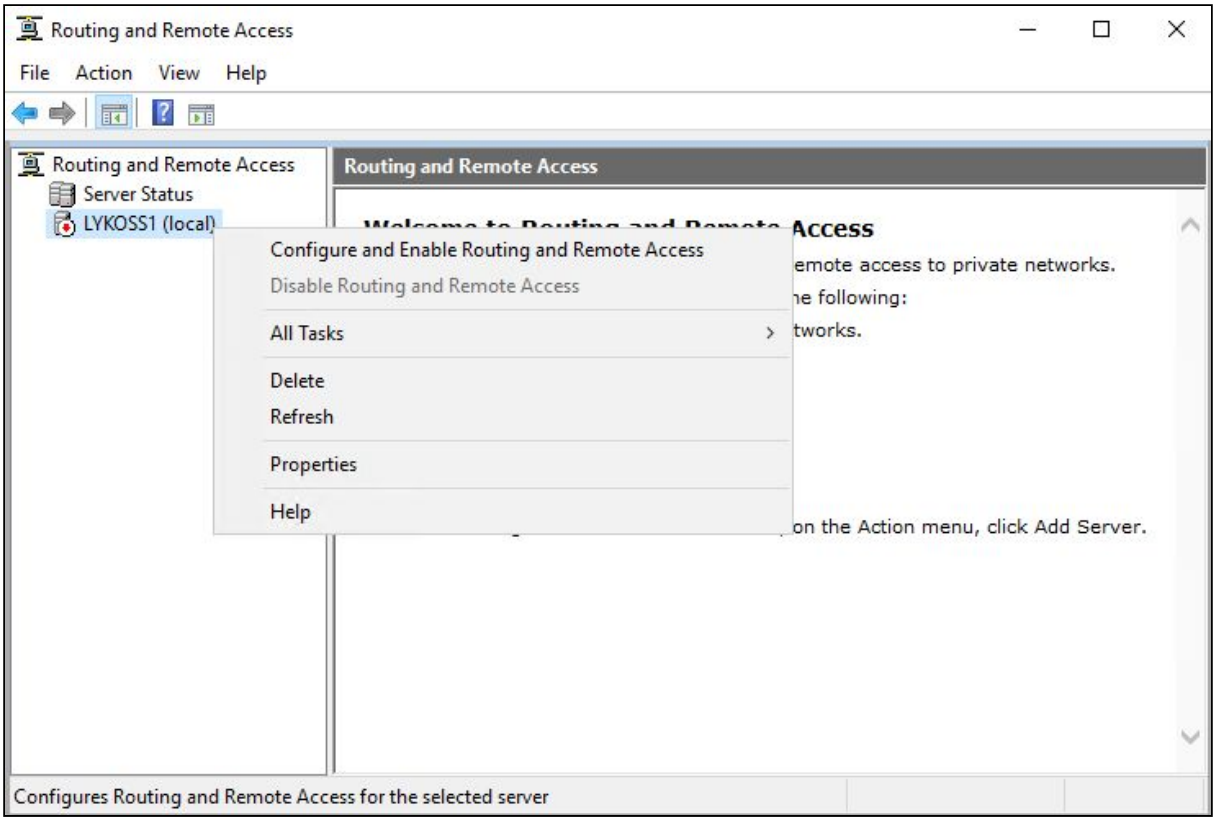
A new window is opening, you have to choose “Deploy VPN Only”.



That opens the management console to Routing and Remote Access.

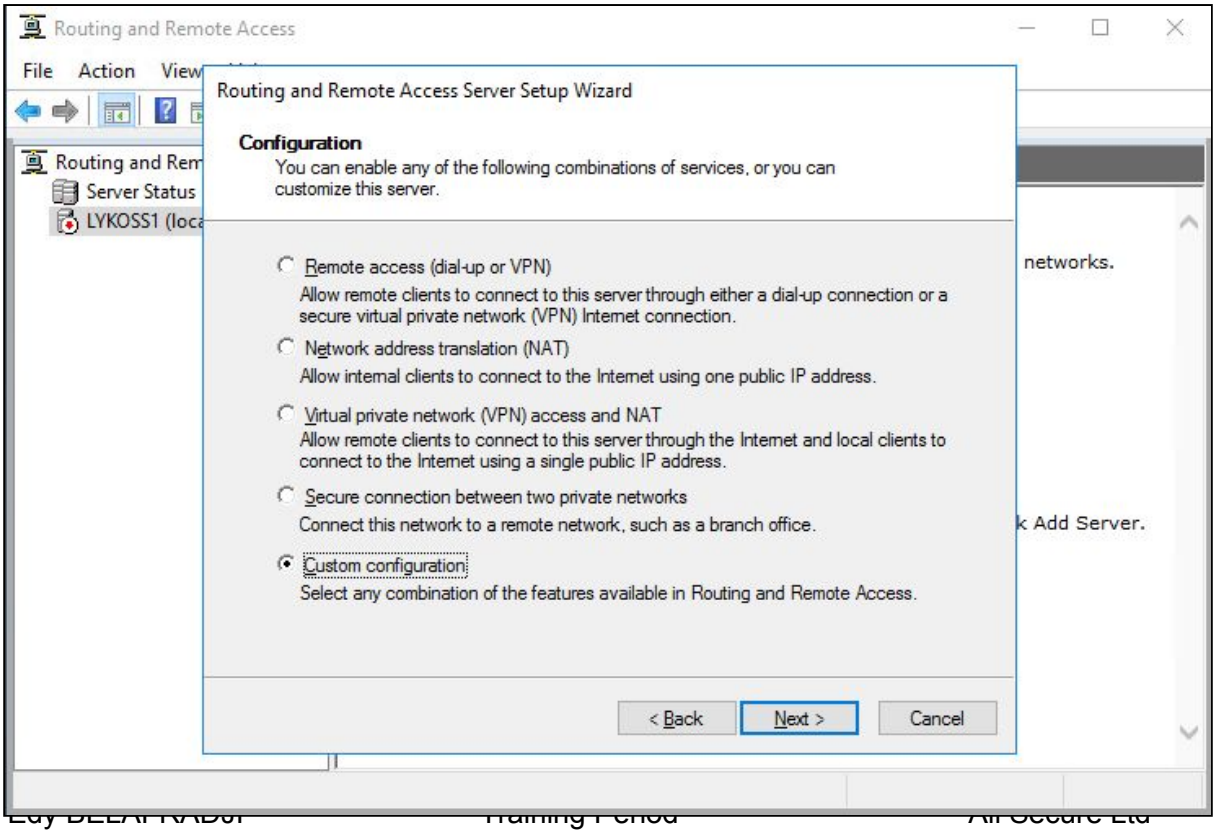


Right click your server's name and select "Configure and Enable Routing

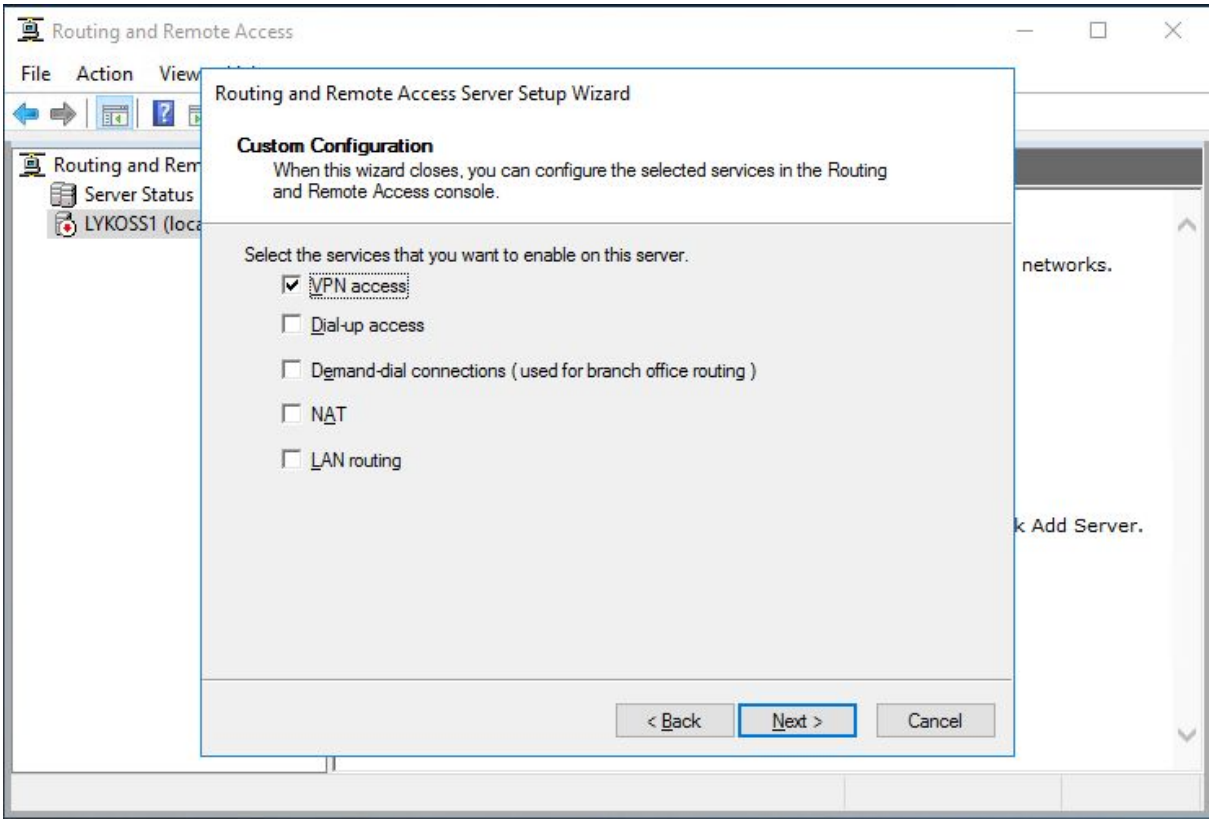


and Remote Access".

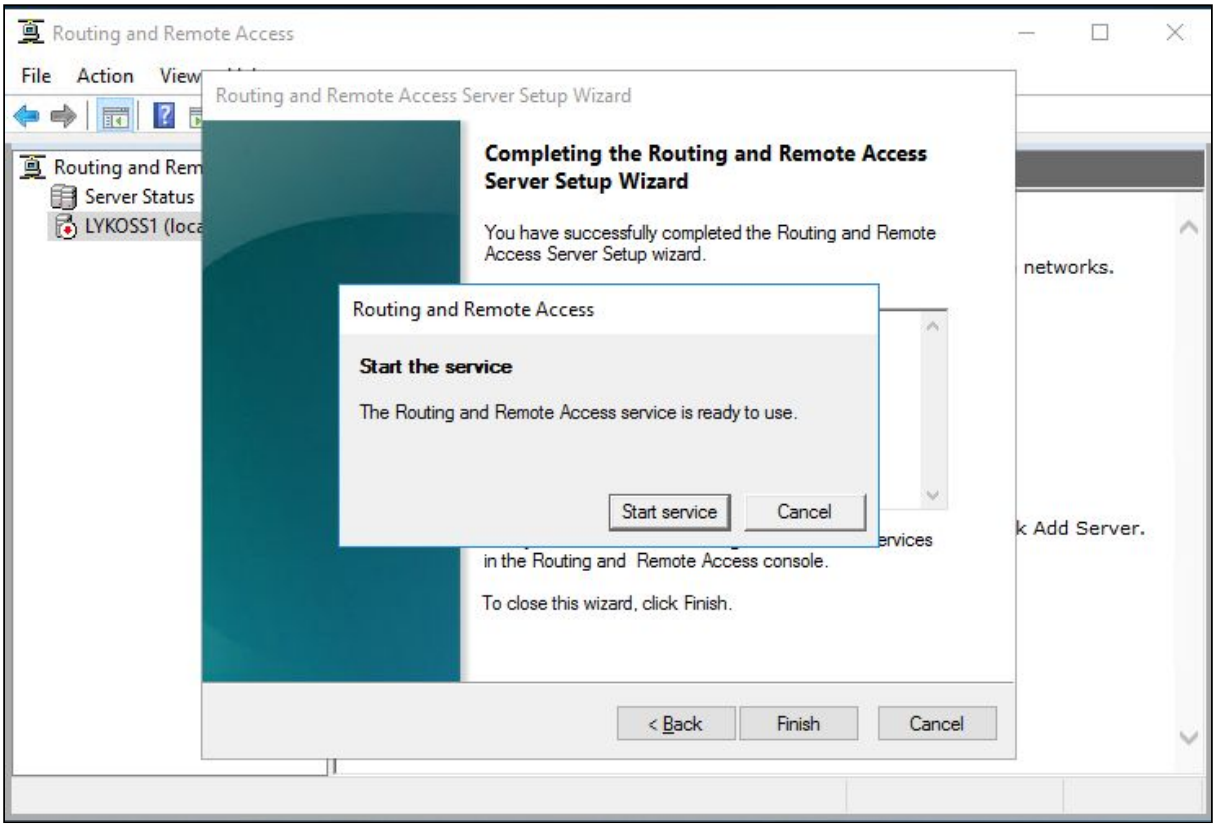
Select "Custom configuration".



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


Routing and Remote Access
File
Action
View
Routing and Rem
Server Status
LYKOSS1 (loca
networks.
k Add Server.
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
LAN routing
< Back
Next >
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

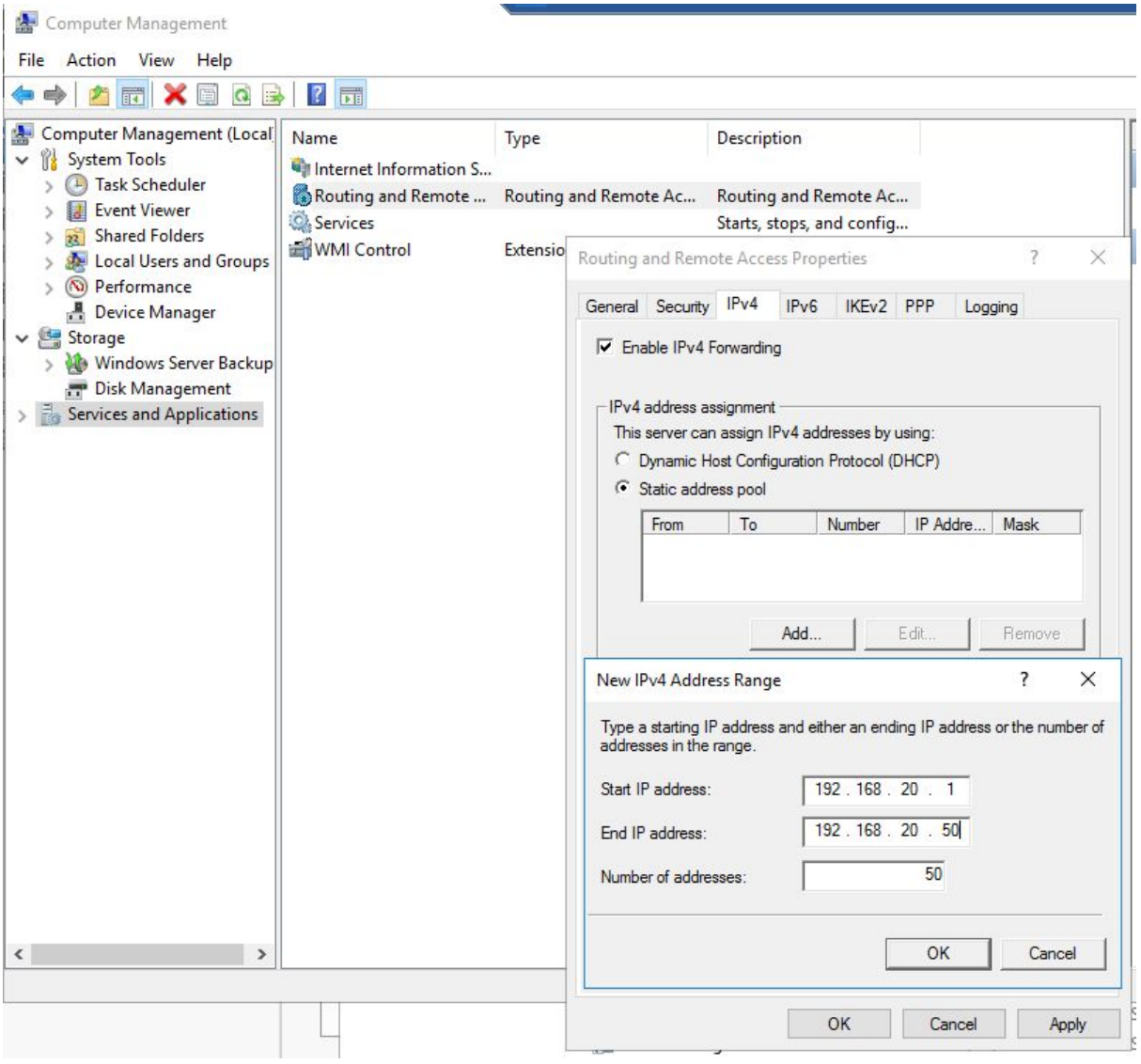
PPTP: Point-a-Point Tunnel Protocol is conceived by Microsoft. It's on every machines since Windows 2000.

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.