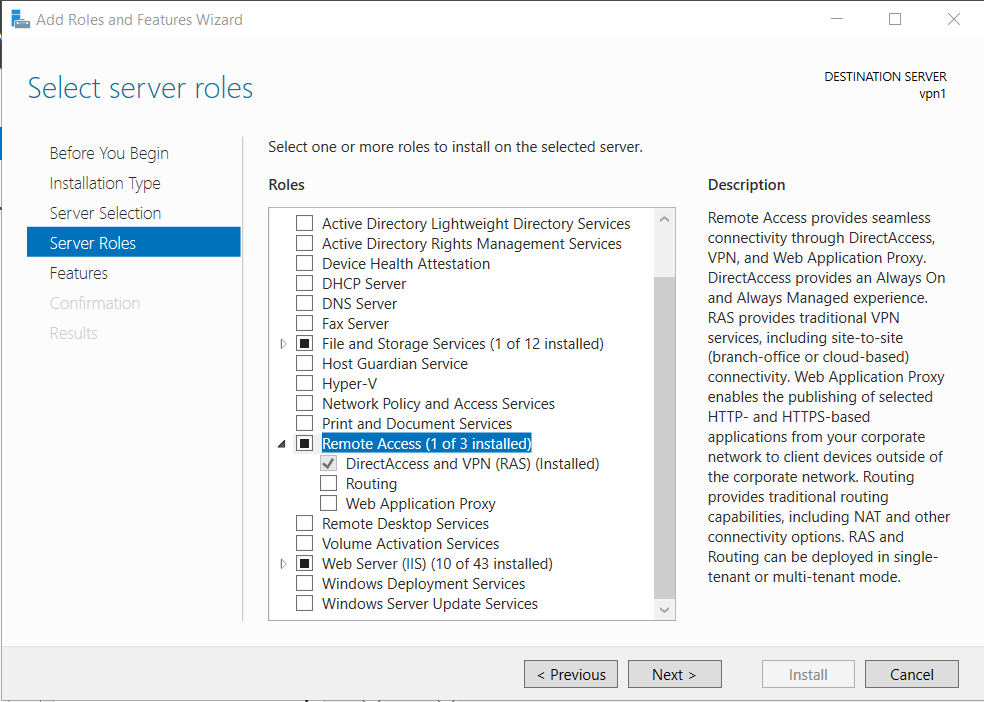
# Site-to-Site VPN configuration-Windows Server 2019

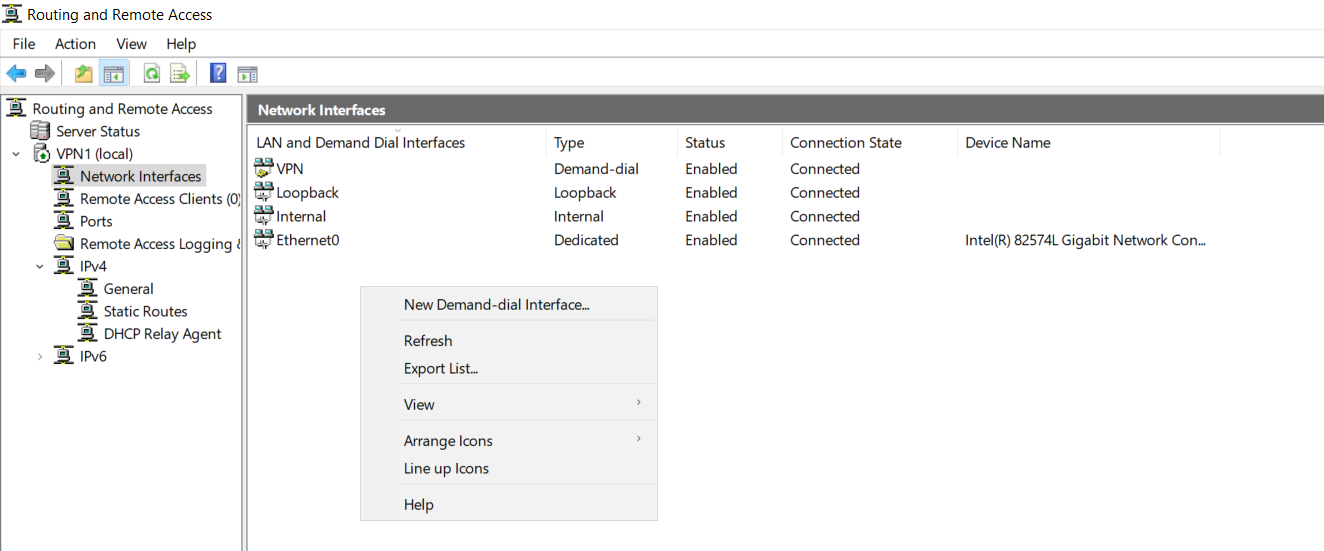
Setup:

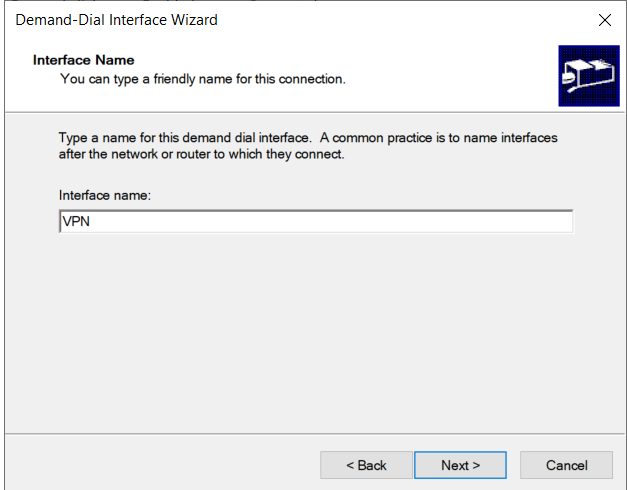
-Windows-Debian subnet: 10.10.10.0/24

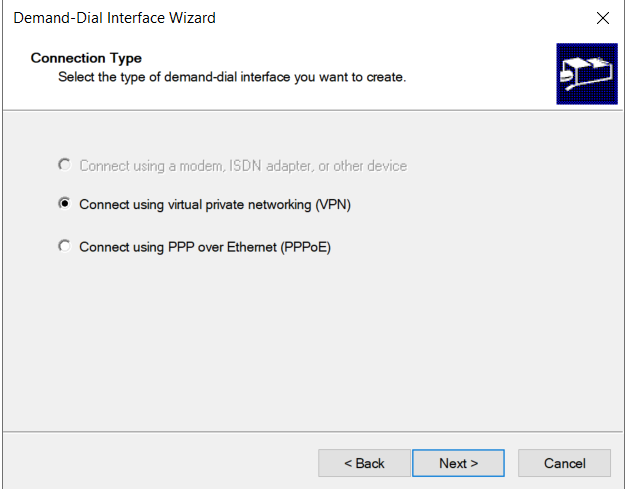
-First GRE subnet: 10.20.20.0/24

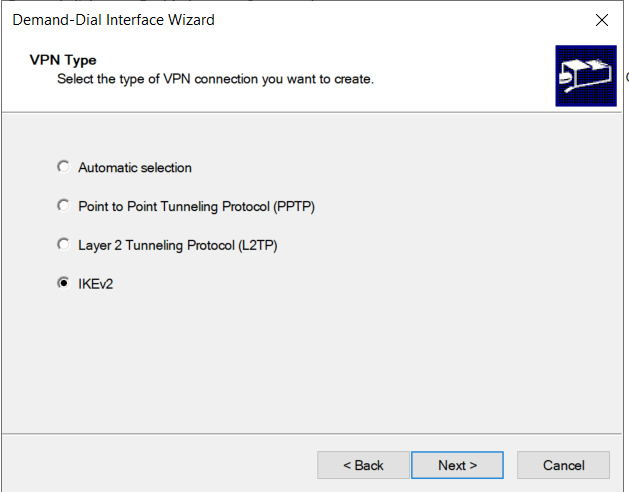
-Second GRE subnet: 10.30.30.0/24

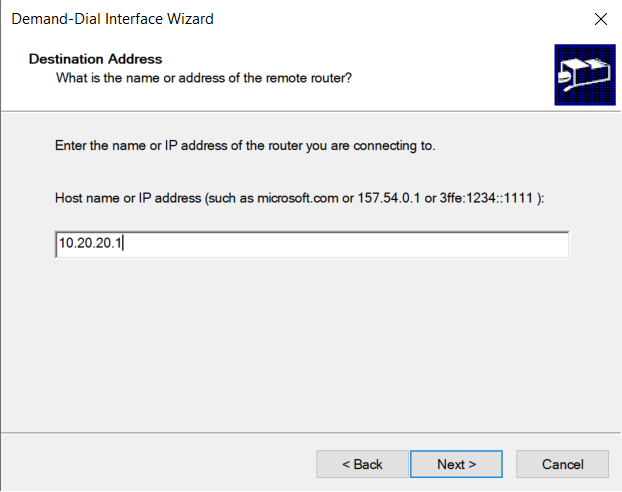
-Install Remote Access -> DirectAccess and VPN (RAS)

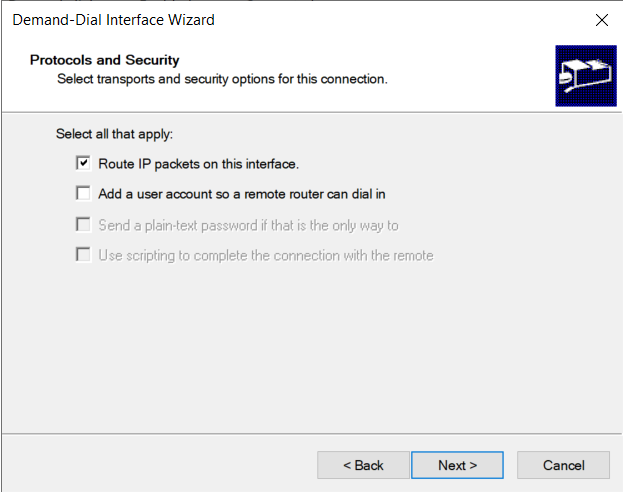
-In Routing and Remote Access -> New Demand-dial Interface

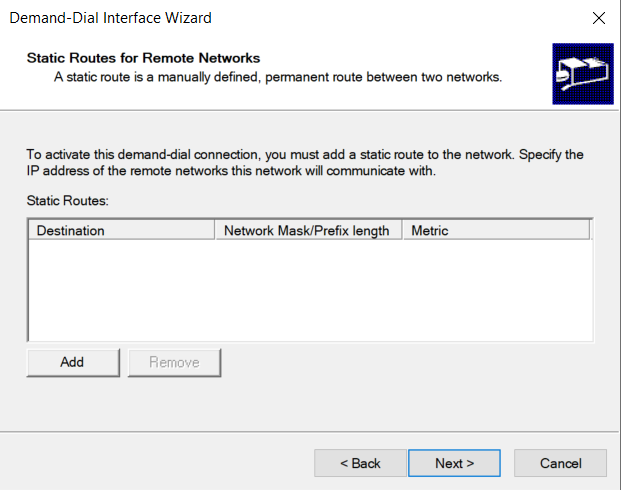
-Give the interface a name

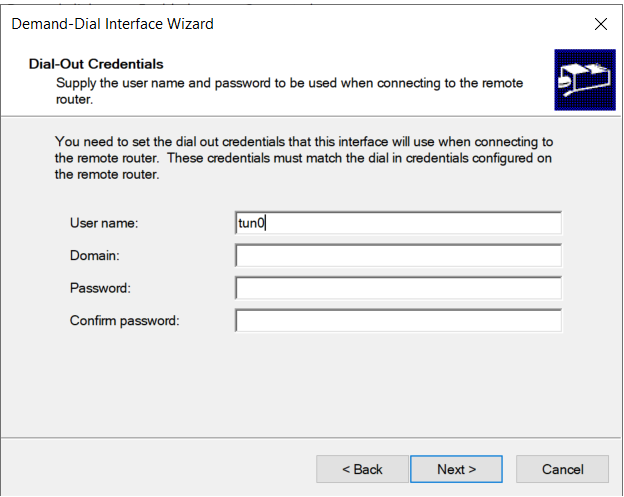
-Connect using VPN

-Select Ikev2 as VPN type

-Destination address: Other VPN server to connect to

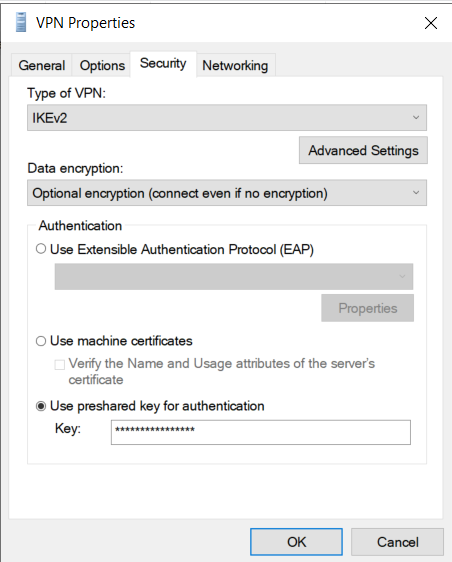
-Tick only: Route IP packets on this interface

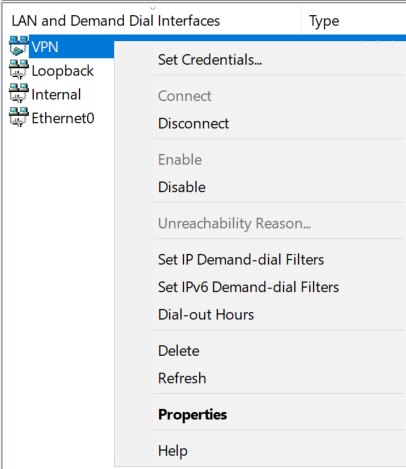
-Don’t need to add static route

-Set the username to tun0, after this click finish

-Right click on the new interface and go to Properties -> Security;

-Set data encryption to: Optional encryption then select: Use preshared key for authentication, then add a preshared key

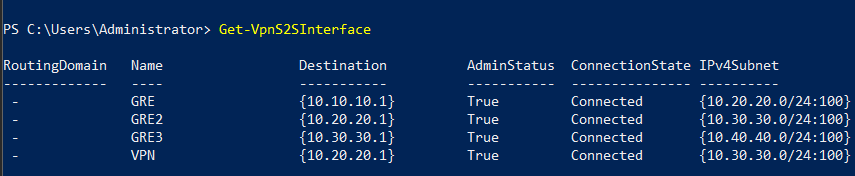


-Right click on the interface again and click on connect to connect to the other VPN server

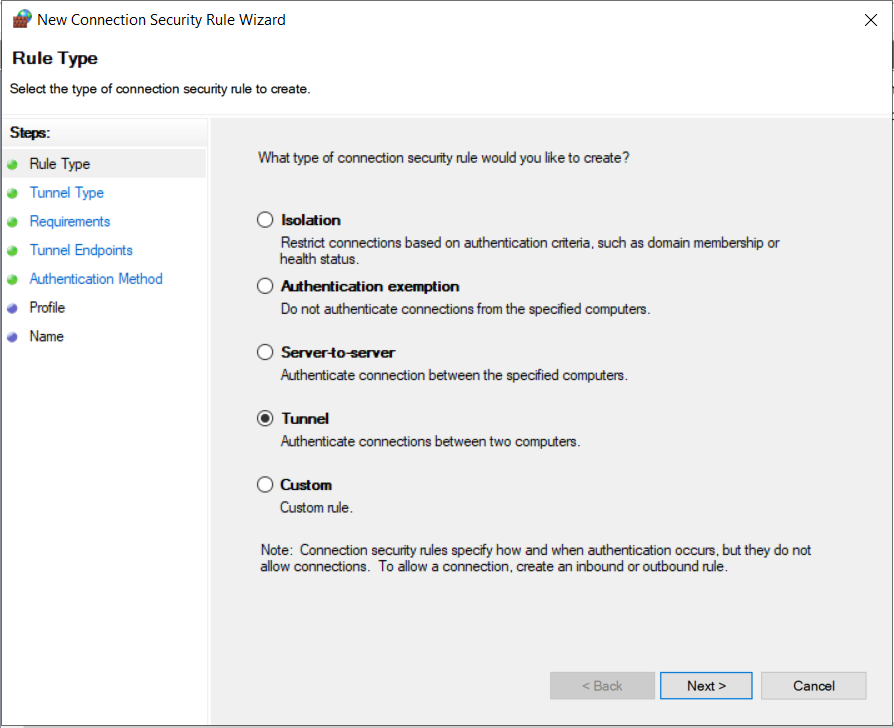
-Open Powershell and create 2 GRE tunnels with the following commands, just fill out with the appropriate values

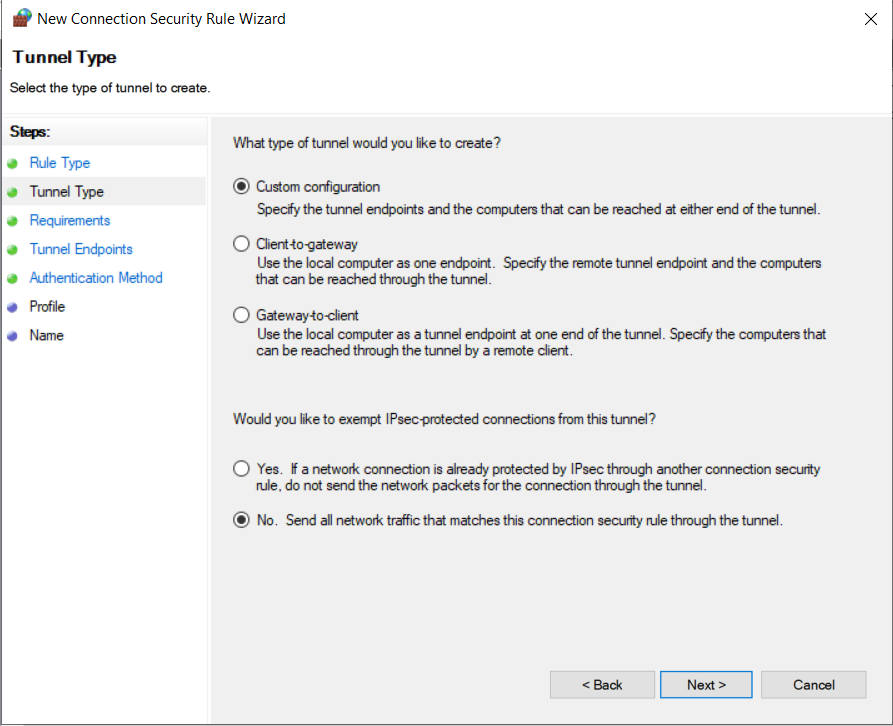
Add-VpnS2SInterface -Name GRE -Destination 10.10.10.1 -IPv4Subnet 10.20.20.0/24:100 -PassThru -SourceIpAddress 10.10.10.2 -GreTunnel -IPv4Address 10.20.20.2

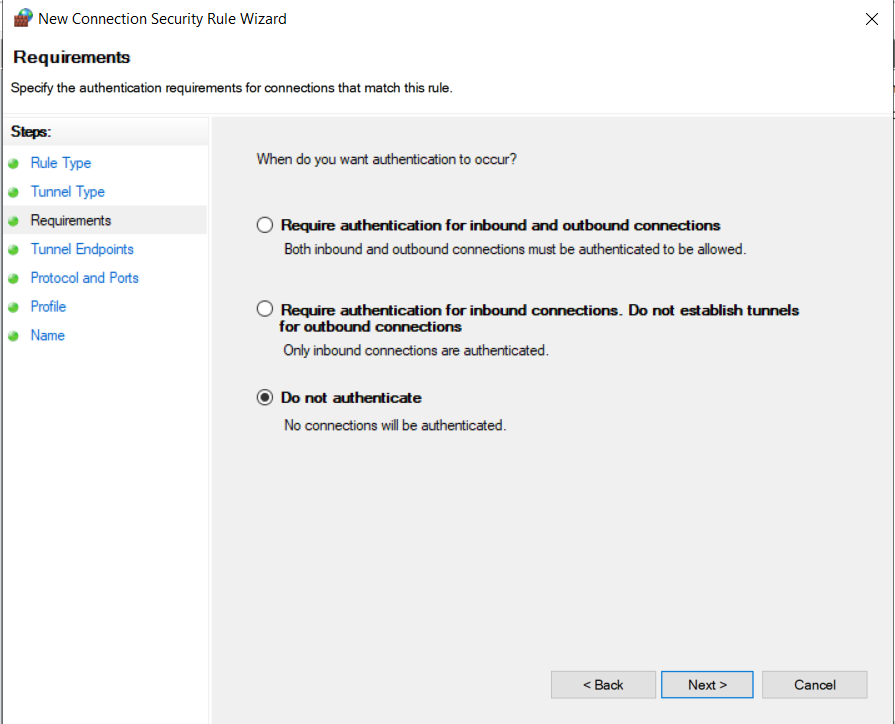
Add-VpnS2SInterface -Name GRE2 -Destination 10.20.20.1 -IPv4Subnet 10.30.30.0/24:100 -PassThru -SourceIpAddress 10.20.20.2 -GreTunnel -IPv4Address 10.30.30.2

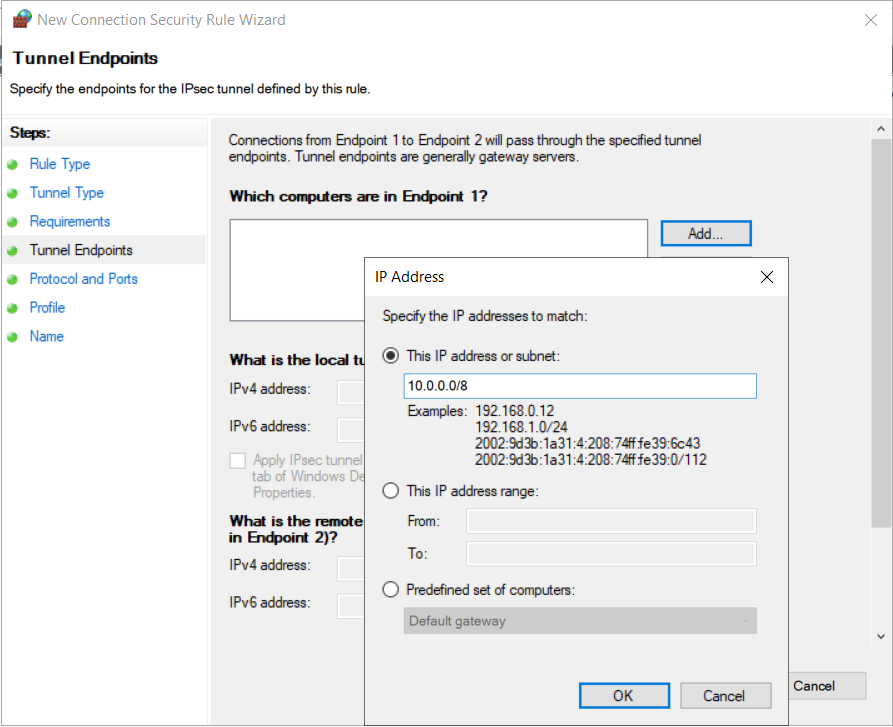
-You can check the interfaces with: Get-VpnS2SInterface

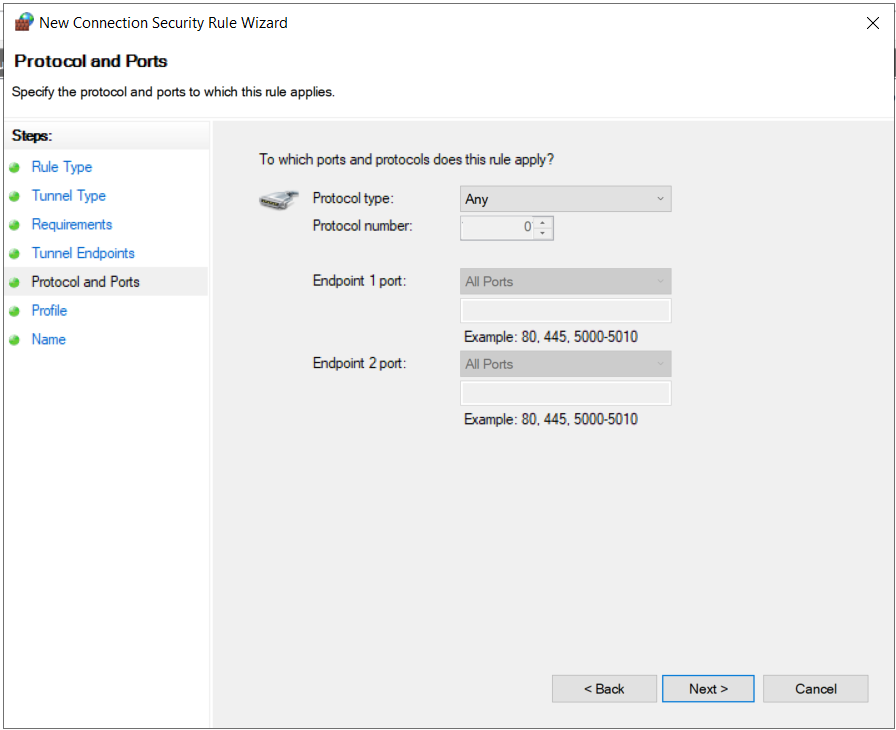
-Open Windows Firewall and go to Connection Security Rules -> Right click and click on New rule…

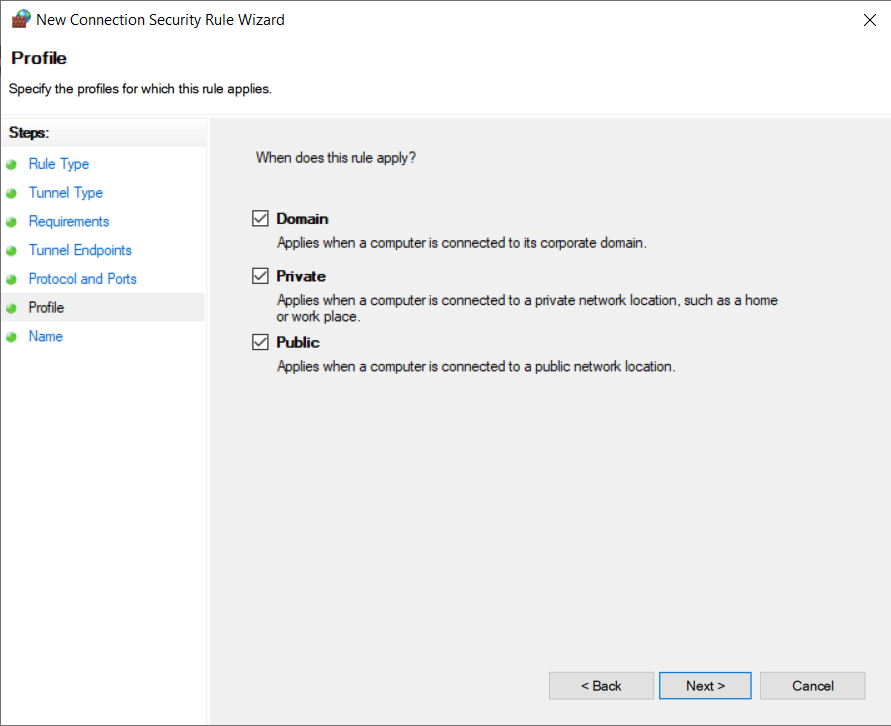
-On Rule type click on Tunnel

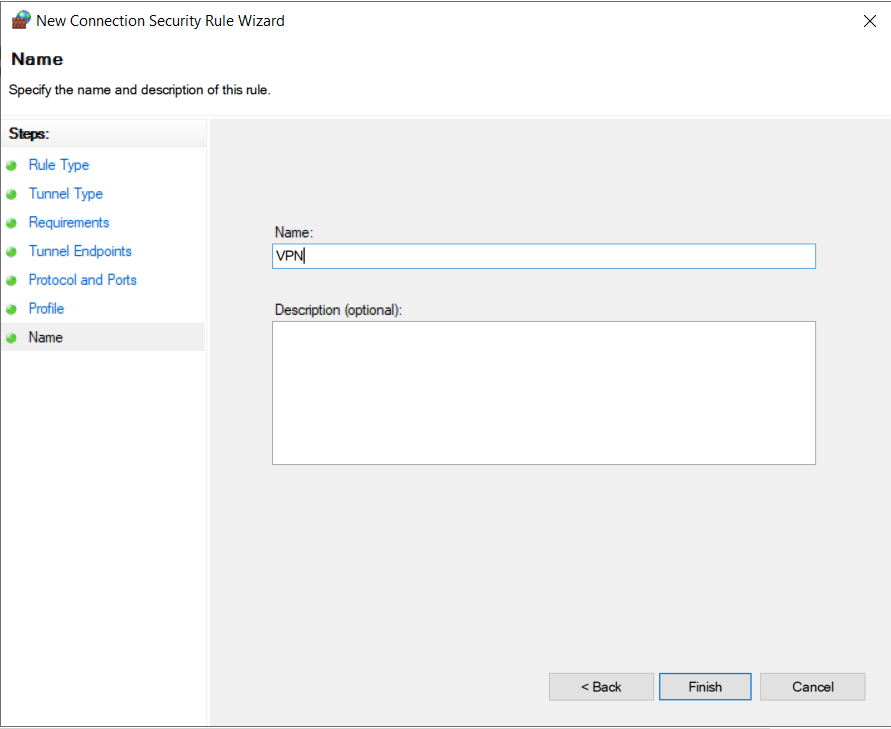
-On Tunnel type, select Custom configuration on top and select No at the bottom

-On Requirements click on Do not authenticate

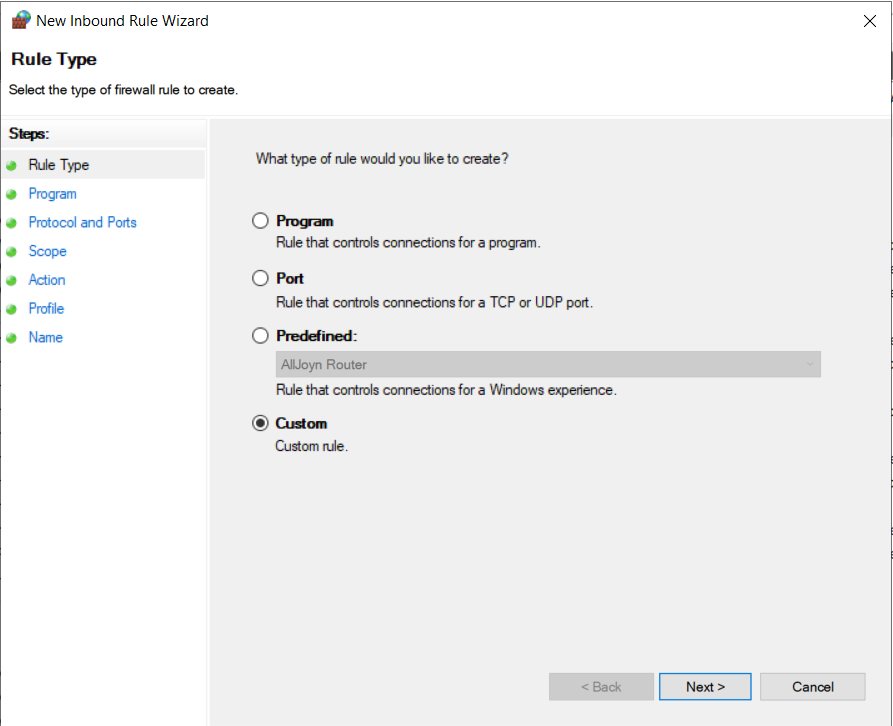
-On Tunnel Endpoints click on Add and add a subnet that contains every subnet that the VPN uses. In this setup: 10.0.0.0/8

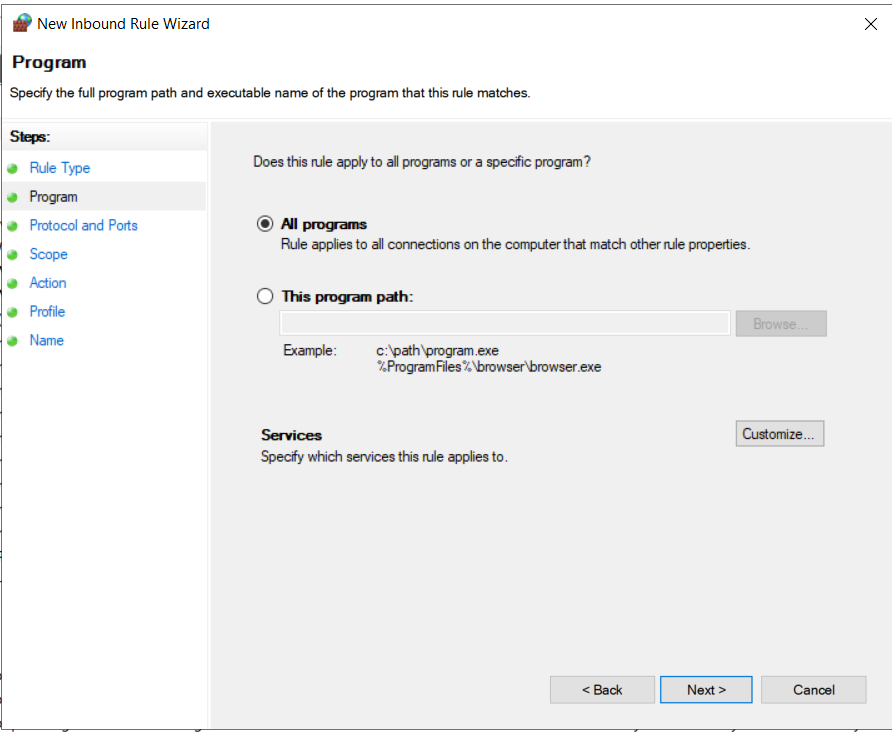
-On Protocols and Ports select Any as protocol type

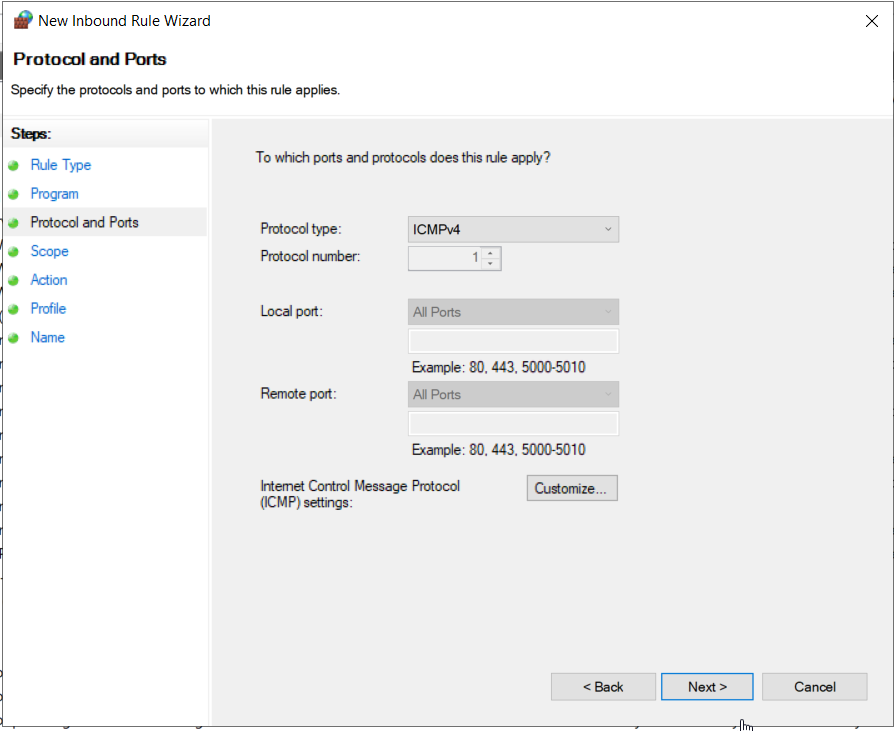
-On Profile, tick everything

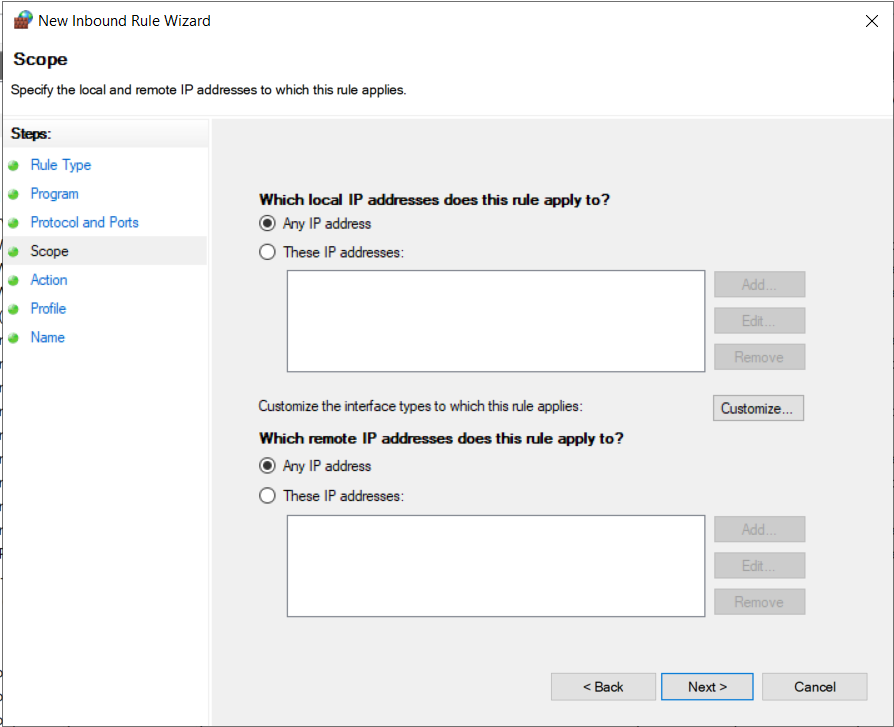
-On Name give the rule a name

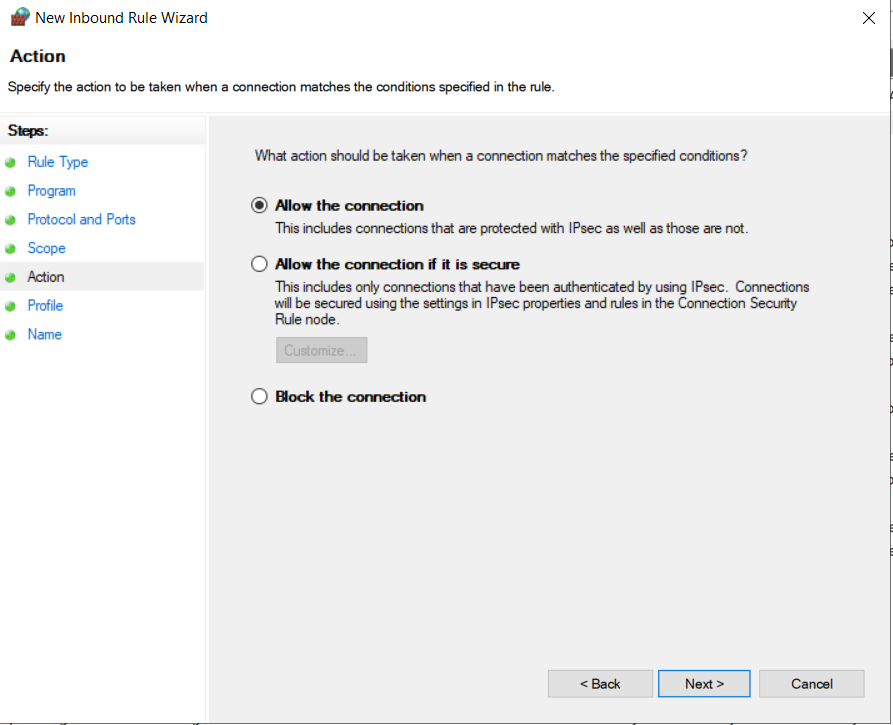
-Enable pinging to test the connection and encryption:

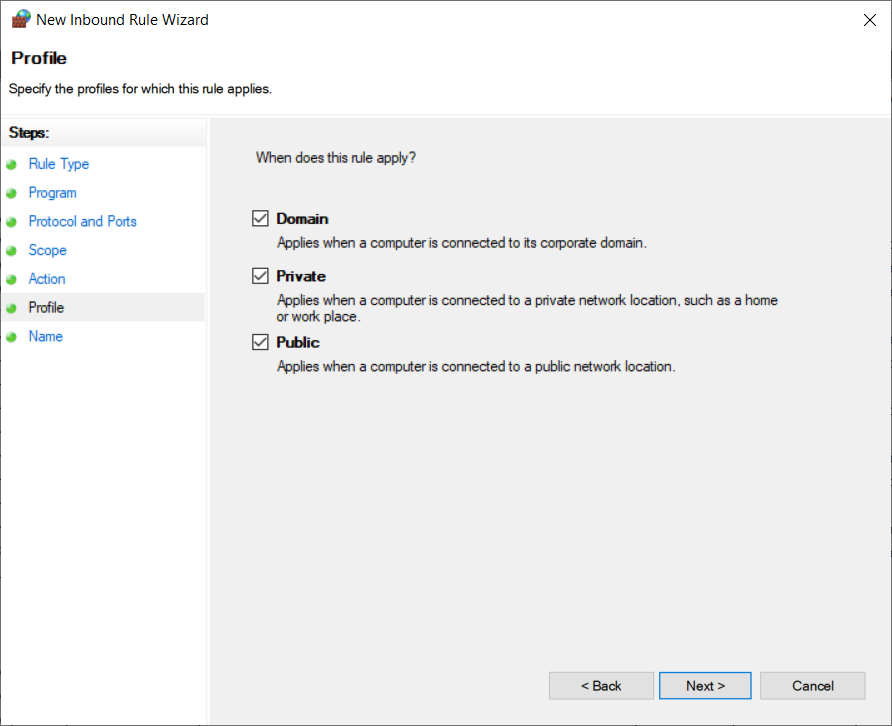
-Go to Inbound rules and click on New rule… -> On Rule type click on Custom

-On Program select All programs

-On Protocols and Ports select ICMPv4 as protocol type

-On scope leave any address on both local and remote IP addresses

-On Action select Allow the connection

-On profile, tick everything

-On name, give the rule a name then finish