Brit Stevens 5/29/24

Fortinet IPsec VPN Configuration

**Purpose:**

The purpose of the lab was to learn how to configure an IPsec VPN tunnel on a FortiGate in contrast to a PaloAlto device. It also shows us how this kind of VPN tunnel can be configured to for different connections like a RD connection for this lab. We need to learn the intricacies of how to configure this tunnel and set up FortiClient.

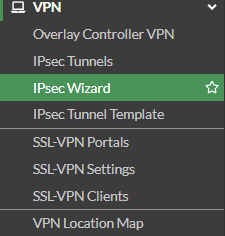
**Background Information on lab concepts:**

* **FortiGate IPsec VPN**
  + This IPsec VPN is used to establish a connection between different networks or between a remote user and a network through the FortiGate. It uses IPsec to provide encryption and authentication for all data transmitted between the networks.
* **IPsec**
  + **Purpose:** IPsec is meant to keep the data transferred confidential and untampered with. It does this by encrypting packets sent through the use of checksums to very data is the exact same as when it was sent, authenticating to make sure the data is coming from the place it’s supposed to, and the use of Internet Key Exchanges to encrypt and decrypt files successfully.
  + **Site to Site:** A connection between two physical sites that are separated by a network through the internet. It could be used to connect users or databases between company buildings.
  + **Hub to Hub:** A connection between multiple hubs that needs to be secure. A hub is a device used to connect desktops to a LAN. Although it may sound similar to a switch, it only works at the physical level meaning it has no intelligent routing and sends all data to every port. Because of this data broadcast, it is crucial to have the data secured and encrypted.
  + **Remote Access**
    - **Client based:** This is the kind of IPsec VPN used in this lab required a form of VPN client software to be able to access the inside network.
    - **Native:** This kind of IPsec VPN uses built in VPN functionalities of operating systems to establish a connection. This could be with the use of VPN in the Windows settings, Apple OS settings, etc.
    - **Forti-Client:** This is one of the clients that can be used for a Client based IPsec VPN. Forti-Client is developed and updated by Fortinet to ensure the it is functional with both IPsec and SSL VPNs while providing internet security like antivirus for the connection.
    - **Signature Authentication vs PSK:** For an IPsec VPN there are two main ways to authenticate the connection between devices: PSKs and Digital Certificate Signatures. PSK is a password known and entered between the communicating devices. This method is more simple than Signature Authentication but less secure. Signature Authentication is achieved with Digital Certificates, also known as Public Key Certificates, which are documents that prove the a key establishing the IPsec Tunnel is authentic. It uses a mix of credentials of the device details, network details, and validity from a CA with a signature to verify the authenticity.
  + **IPv4 Split Tunnel:** When split tunneling is enabled, it allows VPN connections to not only reach the inside network and access information there, but also access the internet from the inside network. If this feature isn’t enabled, the VPN user can only access the internal network.

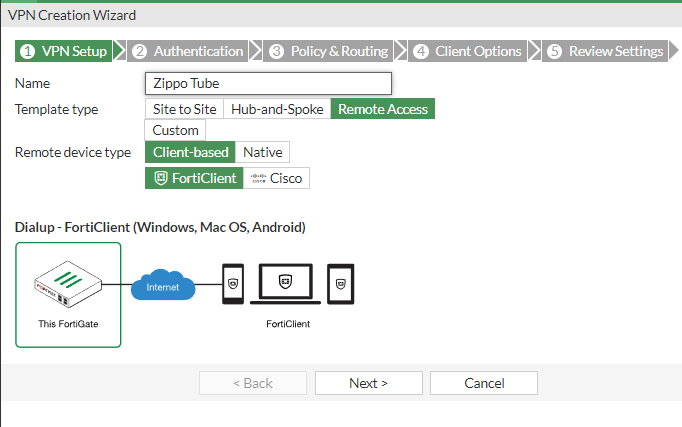
**Required Resources:**

* ***Switch (Cisco Catalyst 3560 series PoE-24).***
* ***Access to the Internet through a switch.***
* ***Desktop on the inside network.***
* ***Desktop on the outside network.***
* ***FortiClient Software.***
* ***FortiGate 40F.***

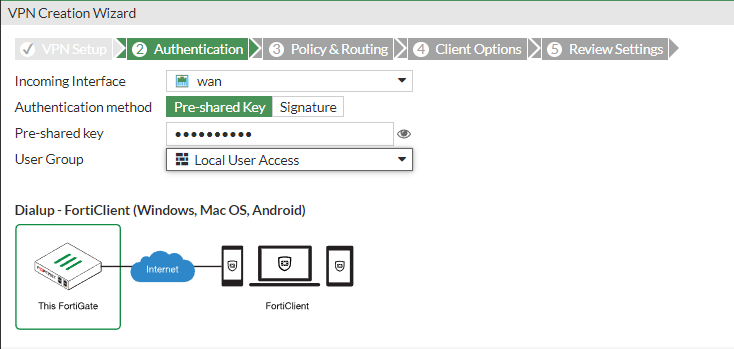
**Lab Summary:**



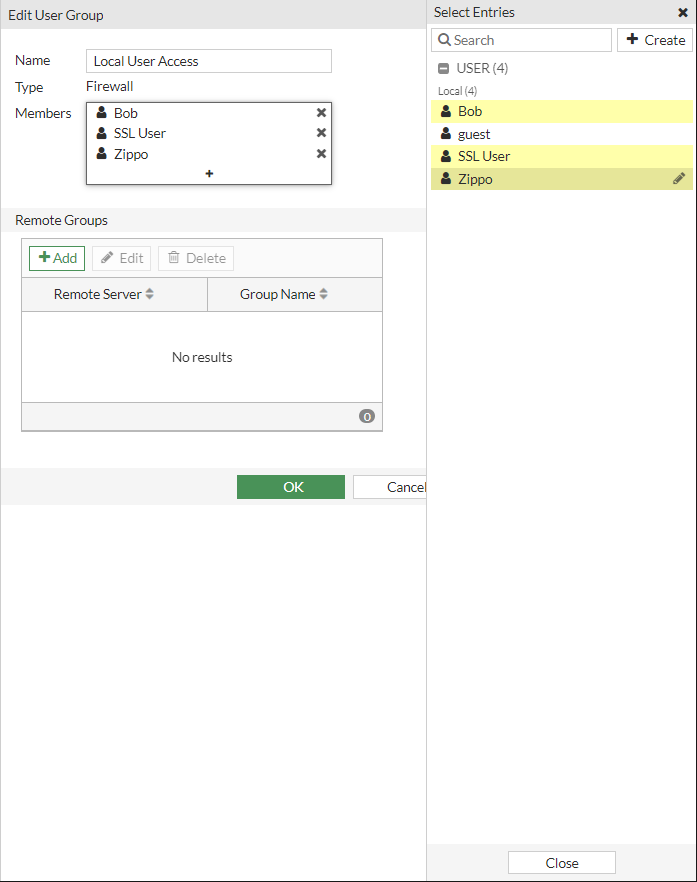
Navigate to the IPsec Wizard to begin configuration.



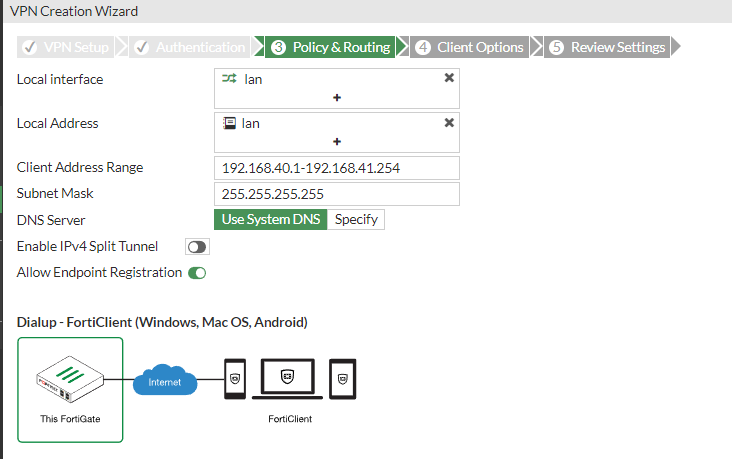
From here it is a step by step process guided by the wizard. Name the VPN tunnel, select remote access, client-based, and choose FortiClient for the client-based software. These settings will configure access to the VPN tunnel to require a client application on a desktop, phone, etc.



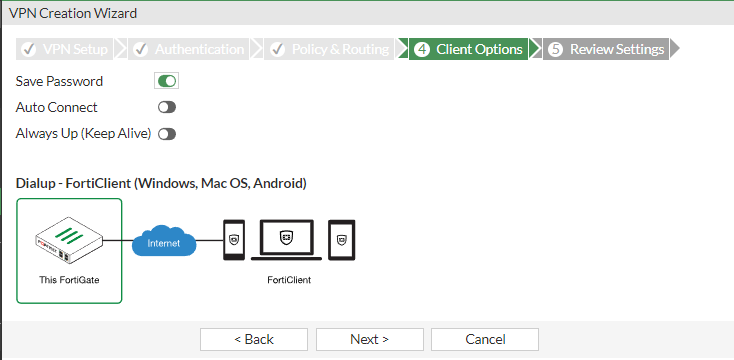
Next for the authentication select Wan as the incoming interface and choose pre-shared key as the authentication method. Enter your pre-shared key and select the user group you want to be able to access the VPN tunnel.



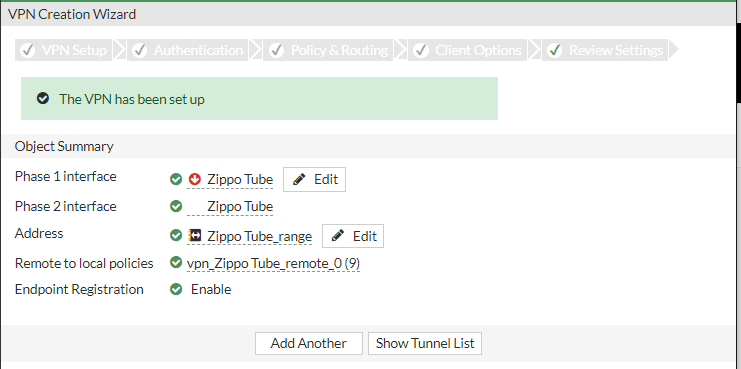
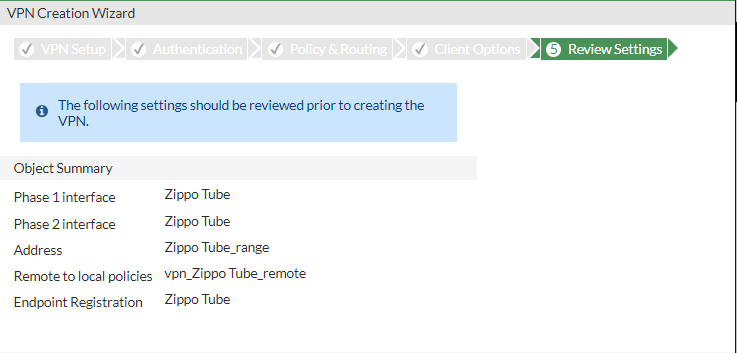
Add any users to this user group that you want to be able to access with the client.



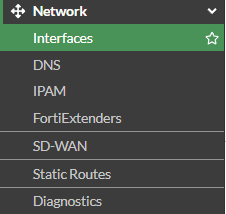
Next in policy and routing, for local interface and address choose the LAN. This will give the connected user an IP address from the configured LAN addresses of the inside network. For client address range enter a range of IPS that the connecting desktop could have to ensure it can access the VPN. If you are unsure what your PC's IP address may be or you won't be able to access it from any other network, set this range to all usable addresses.

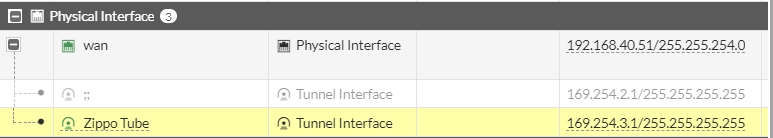


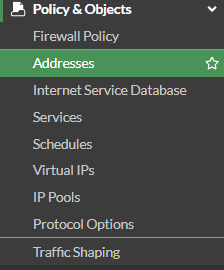
For client options, select any options you see fit for your use.

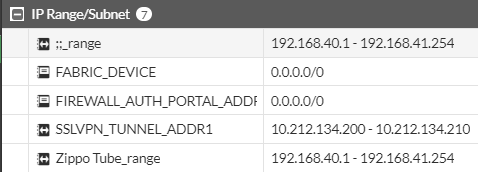


Your Tunnel is configured.

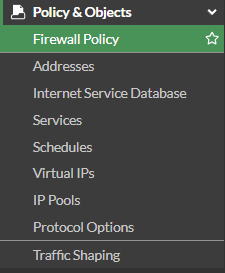








You can verify your tunnel has been configured under network interfaces and policy and object addresses where your tunnel has created an interface and an address range.

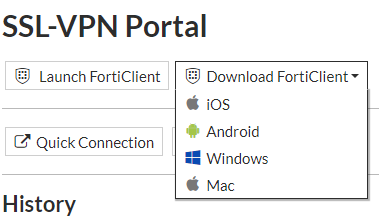




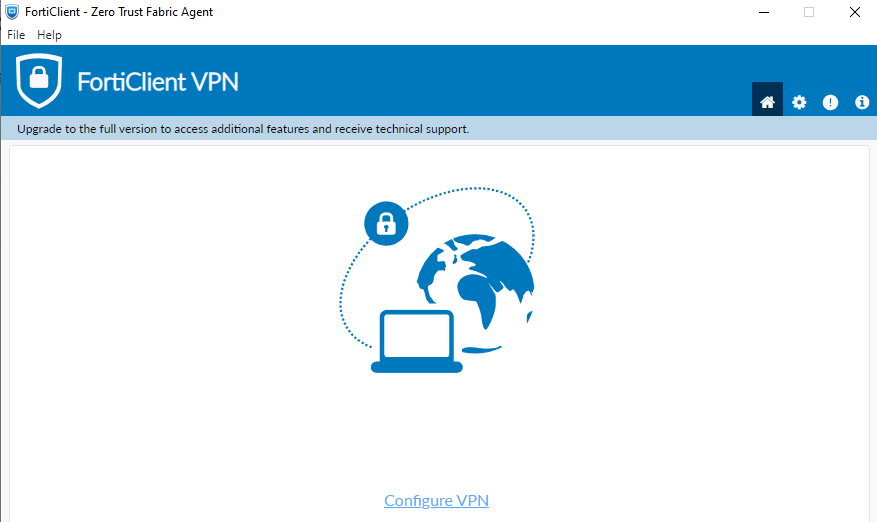
next we need to create a firewall policy to allow traffic from the tunnel into the inside network. This policy should have been made automatically but if not configure to except traffic from the VPN tunnel to the LAN interface.

Next we need to configure FortiClient.

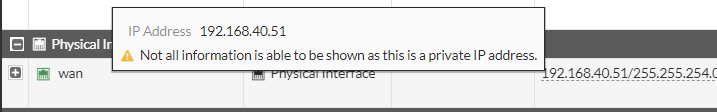




One way to access FortiClient is through the SSL-VPN portal where you can download it off the home page.



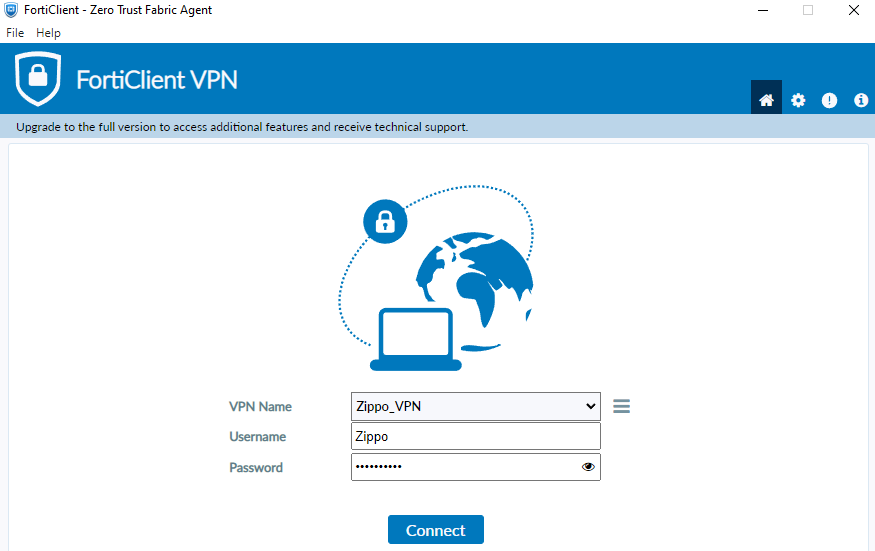
once downloaded open and select configure VPN.



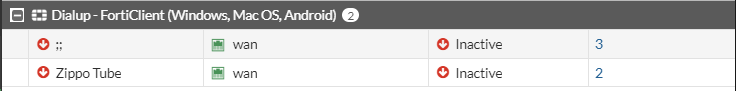
find the address of your FortiGate by going to interfaces and hovering over the Wan interface.

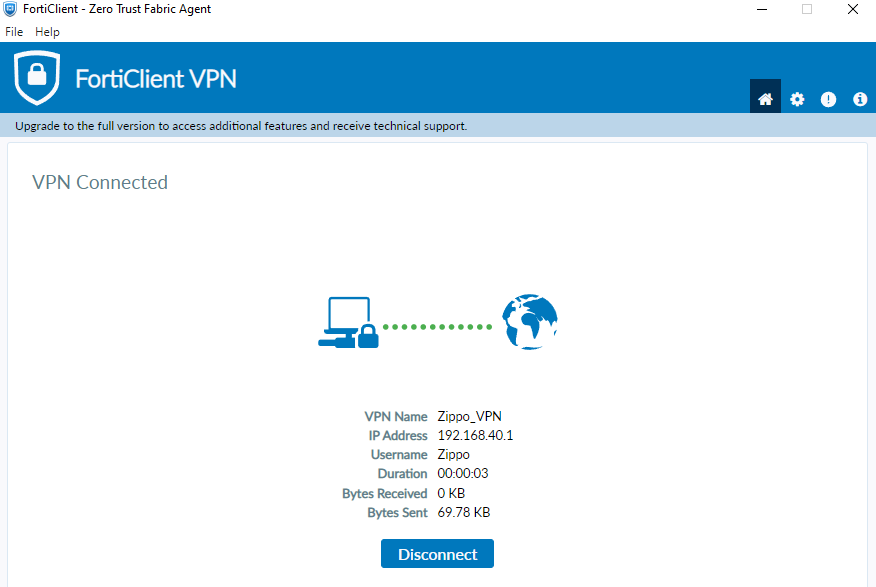


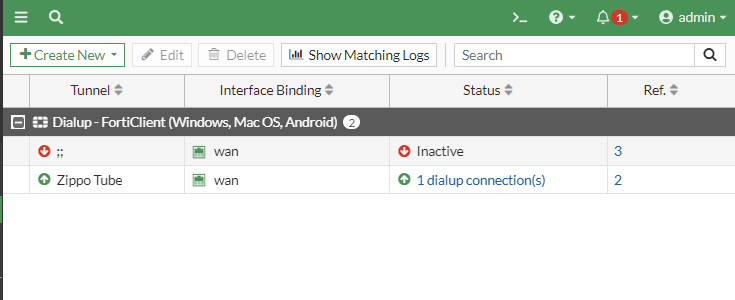
Select IPsec VPN, name the connection for future use, enter the IP address of the Wan interface for your remote gateway, and finally select pre-shared key for the authentication method and enter the pre-shared key.



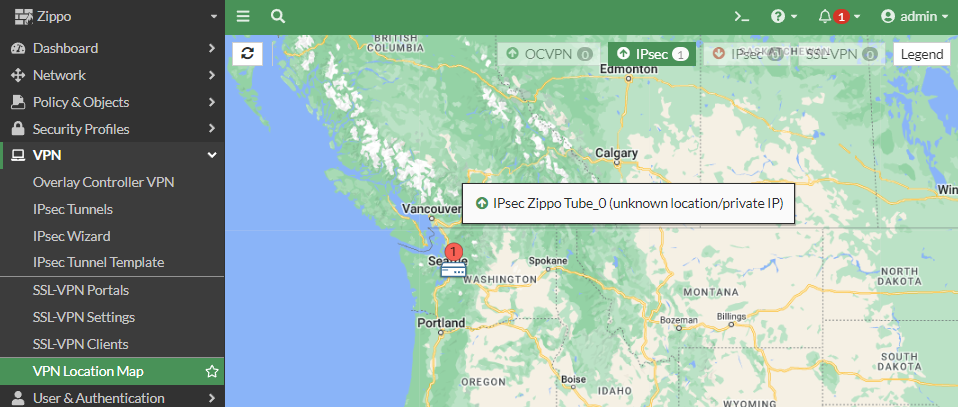
Enter the login for one of the users configured to be able to access the VPN tunnel.

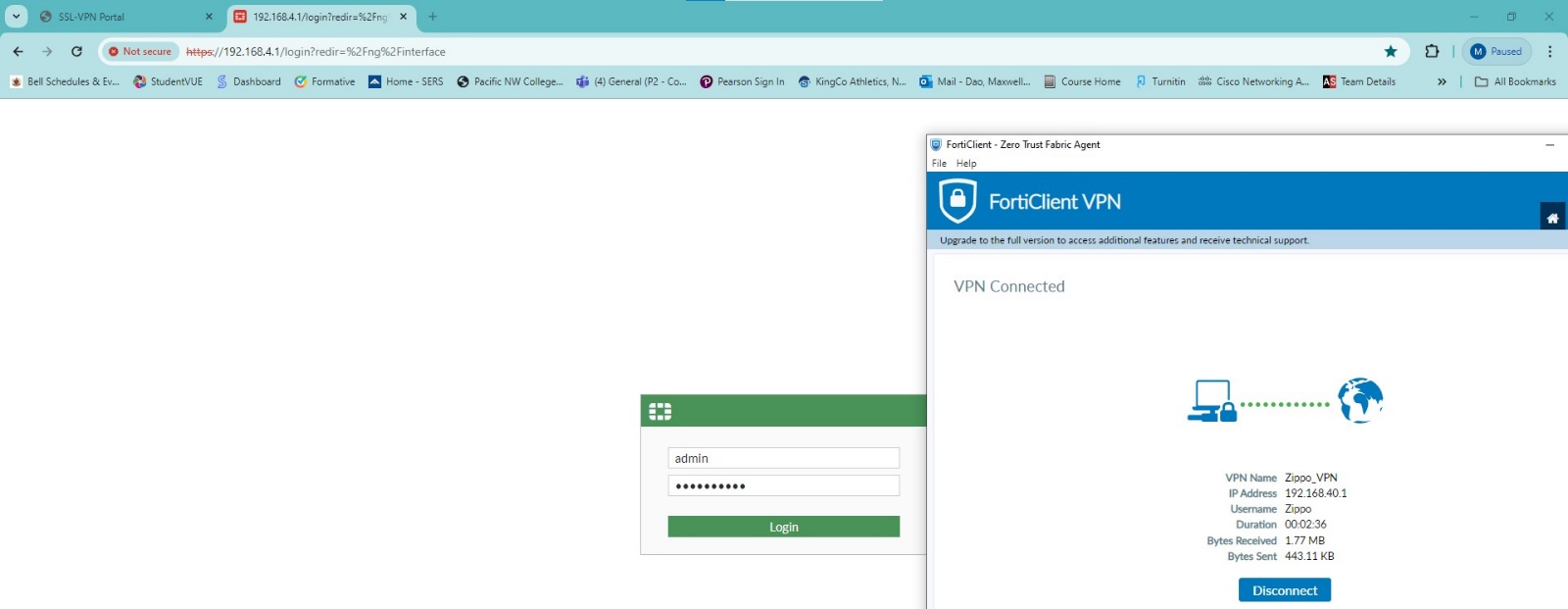


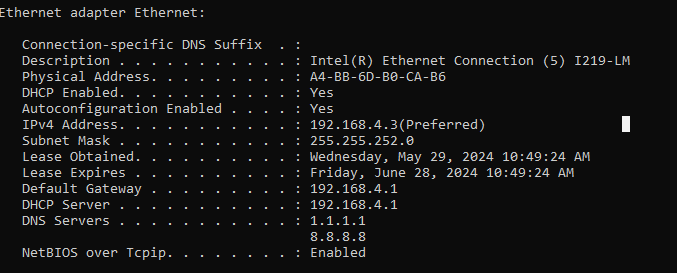




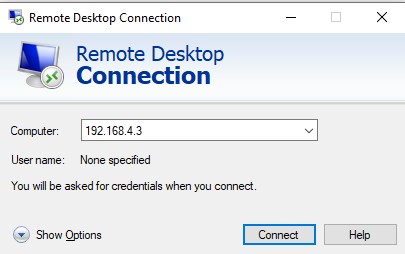
Once connected it will show your VPN tunnel is up on the FortiGate and also that the VPN is connected in the Forticlient.



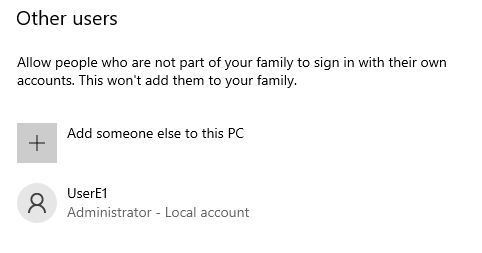


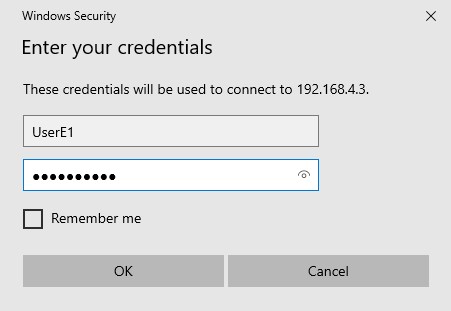


You can verify the connection to the inside network in numerous other ways such as VPN location map it's showing that the connection is up, being able to access the firewall GUI from a web browser, or opening a CLI interface and viewing your IP address which should be an address from the inside network. Another way to confirm is with RDP.



Open remote desktop connection and type in IP address of a PC on the inside network.

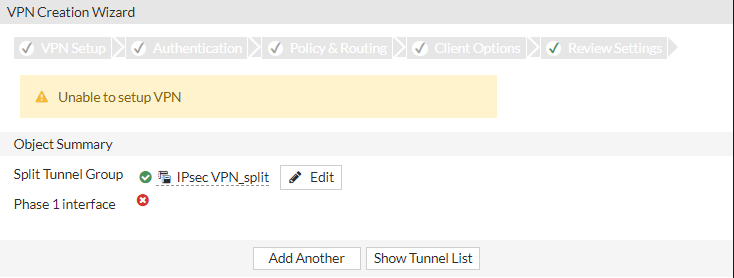




Confirm a user login toward this connection and enter the credentials. The connection successful when you are given a prompt to log into the desktop.

****

**Problems:**



* Could not start VPN
  + Created a new tunnel with a different configuration which was successful.
* Wrong address range set for incoming users.
  + Because we knew what the address would be, we changed address range to ISP network.
* Could not start remote desktop.
  + Had an additional firewall blocking connection on the PCs.
    - Turned off the firewall for the lab under network settings.
* Previous IPsec VPN tunnel up from failed attempt
  + Shut down the tunnel but could not delete it
    - Determined if the tunnel stayed down and there were no attempts to access that tunnel by users, it was okay to leave it for now. This is a security risk but we’re in a protected environment.
* Unable to access VPN tunnel from remote PC.
  + On reset the firewall DHCP address changed so we could not use the same IPsec VPN saved profile to login after the first time.
    - Needed to change IPsec Remote gateway each time the firewall is rebooted.

**Conclusion:**

Overall this lab was very easy as we had done this lab before with a PaloAlto device so we knew the concepts and overall how to configure it. The main difference between the labs was FortiGate’s simplicity and user-friendly design leaving little room for error. This made the lab as easy as it was and has convinced me that FortiGate should be the go-to Firewall since it has many if not all the capabilities of competitors like PaloAlto with the addition of user management and ease of use. My biggest takeaway from this lab is finding a company that fits your wants for devices like firewalls can have very positive outcomes because once you are familiar with some of their hardware, other devices they produce will likely be similar letting you understand how to configure it before entering configuration. This can be useful when you need to determine which device to buy for a specific task in a short time frame.

