Brit Stevens 5/29/24

Fortinet IPsec VPN Configuration

**Purpose:**

The purpose of this lab is to introduce a new VPN method of the FortiGate

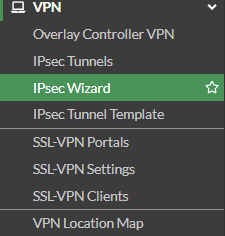
**Background Information on lab concepts:**

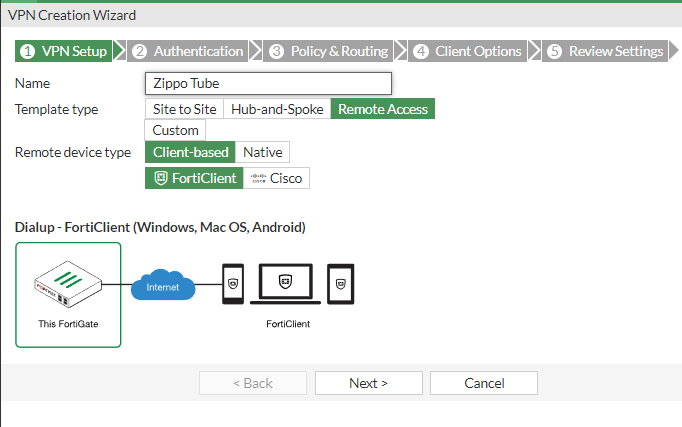
* **FortiGate IPsec VPN**
  + This IPsec VPN is used to establish a connection between different networks or between a remote user and a network through the FortiGate. It uses IPsec to provide encryption and authentication for all data transmitted between the networks.
* **IPsec**
  + **Purpose:** IPsec 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.

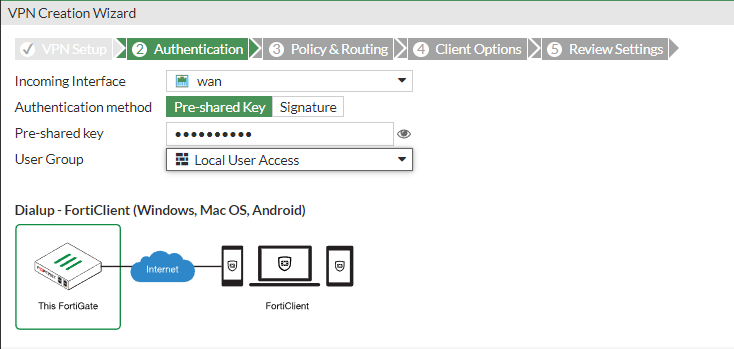
**Required Resources:**

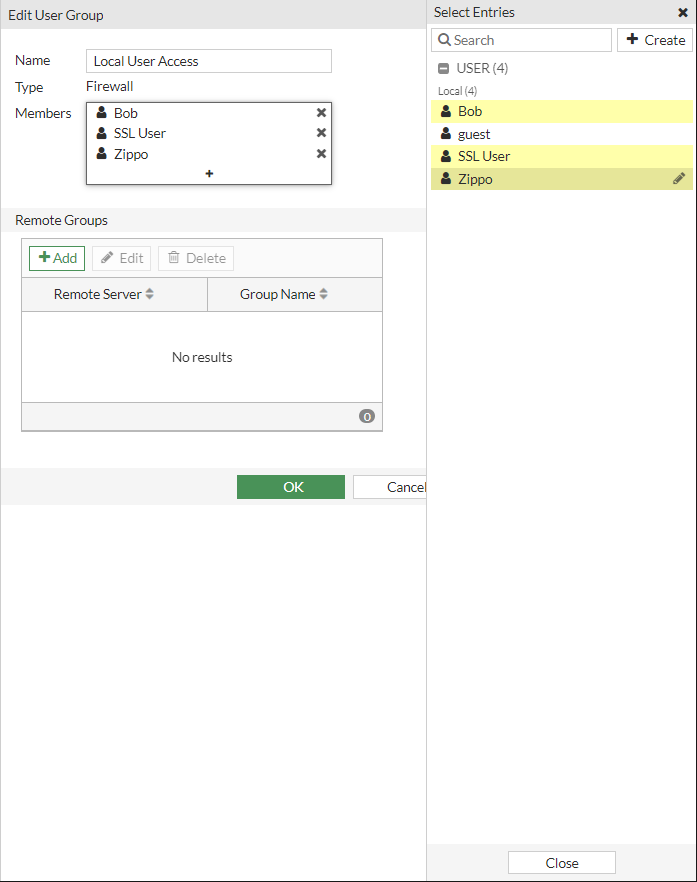
* ***Switch (Catalyst 3560 series PoE-24).***
* ***Access to the Internet through a switch.***
* ***Desktop on the inside network.***
* ***Desktop on the outside network.***
* ***FortiClient Software.***
* ***FortiGate 40F.***

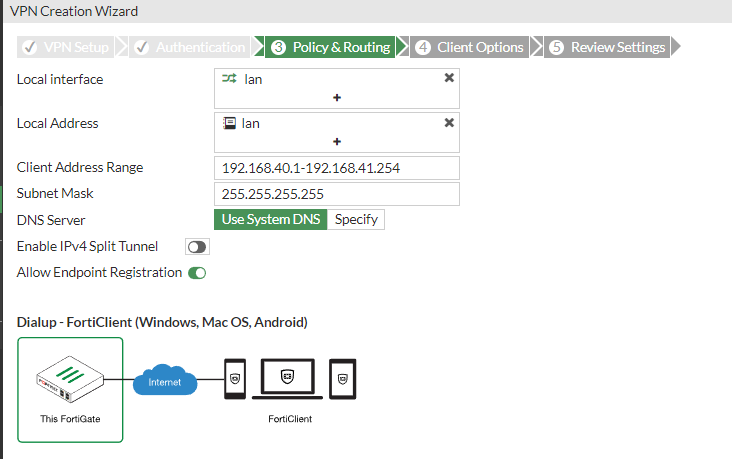
**Lab Summary:**

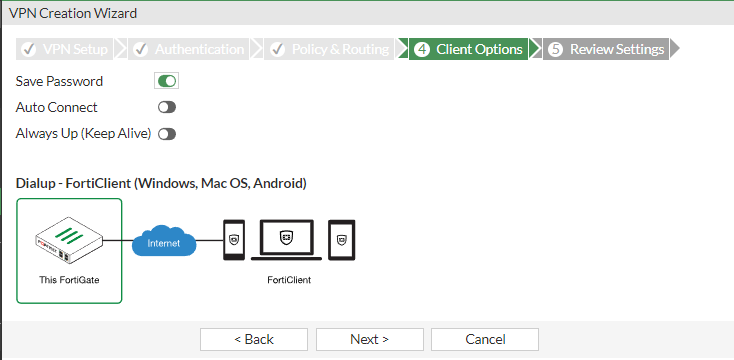


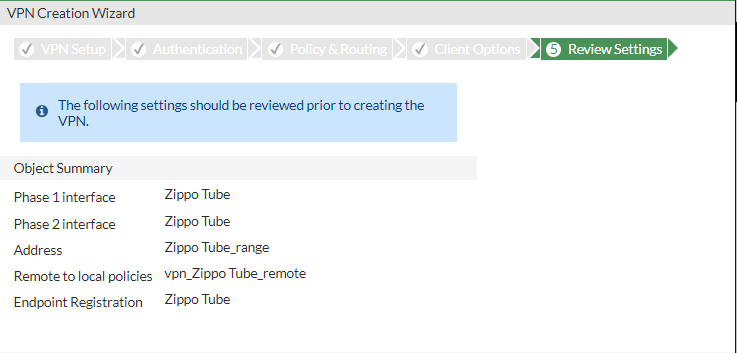


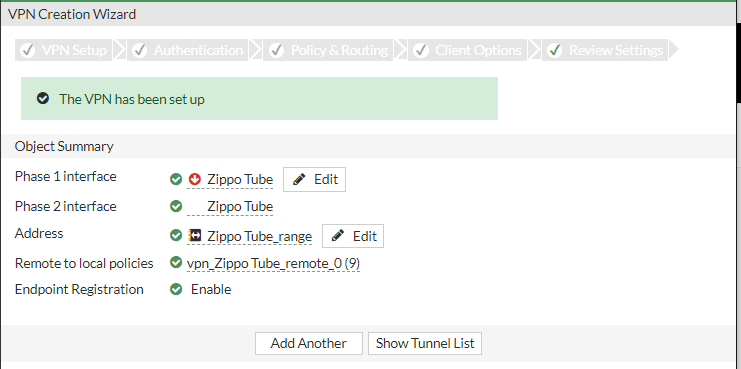


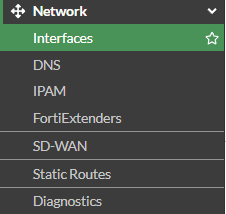


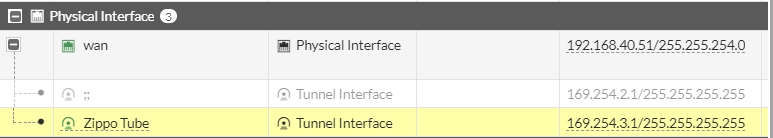


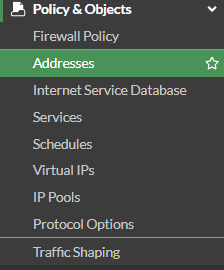


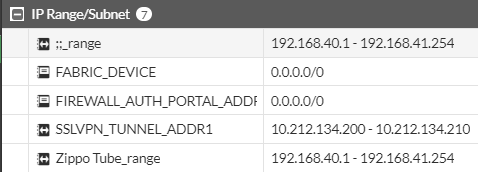


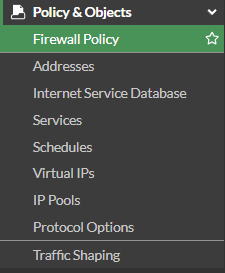










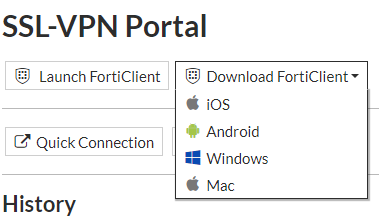


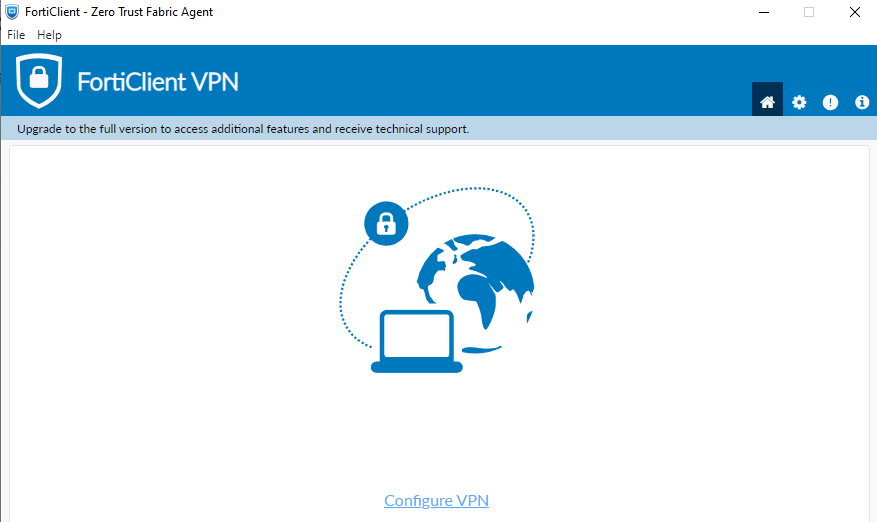


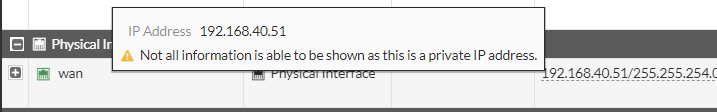
Next we need to configure FortiClient



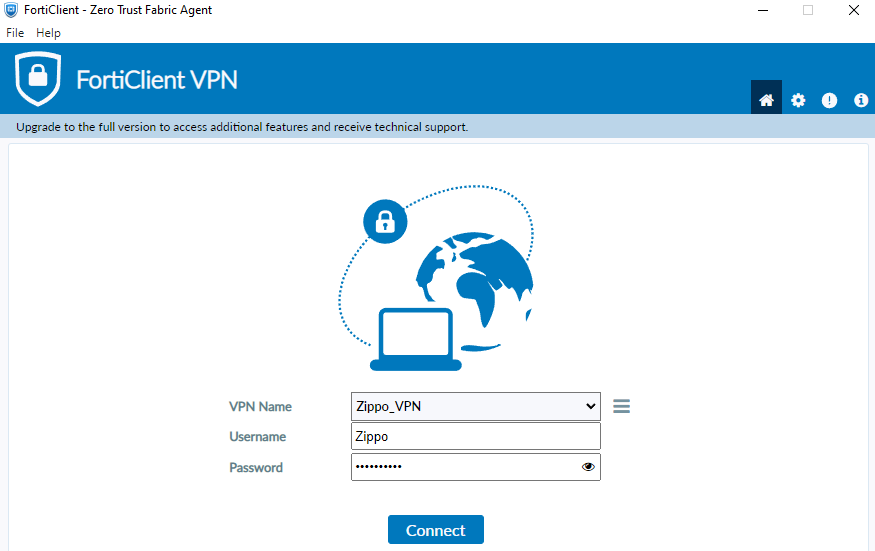
The way we got the client was through our SSL portal.

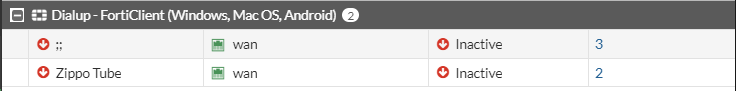


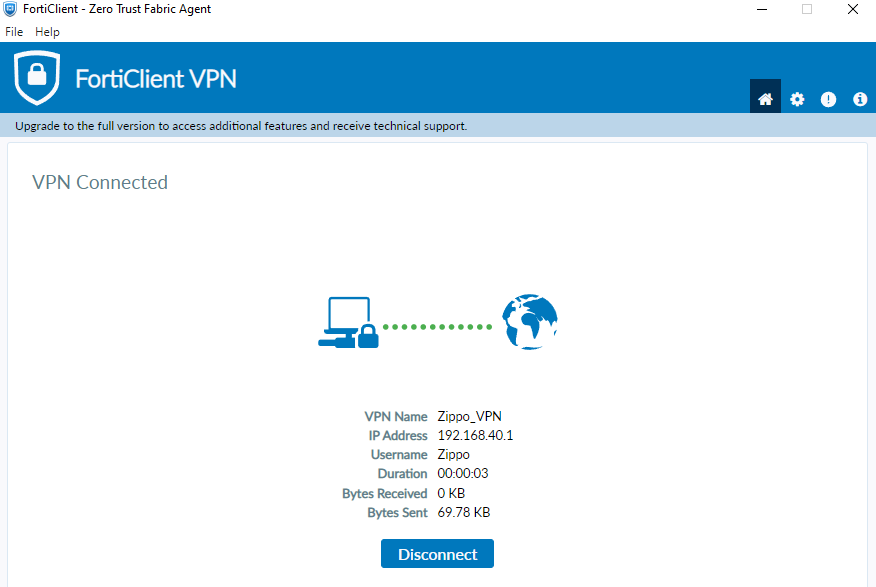


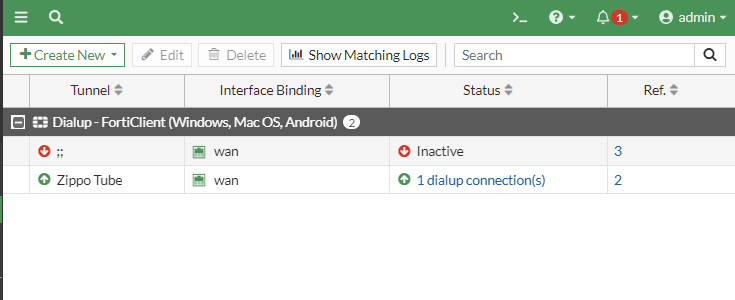


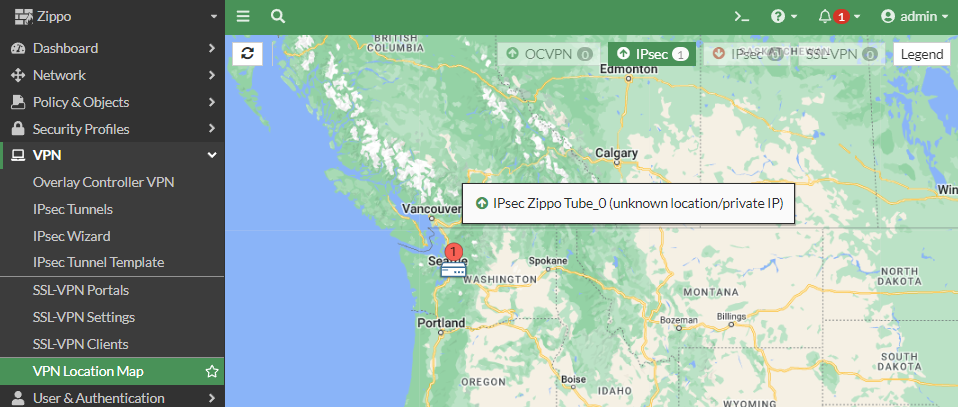


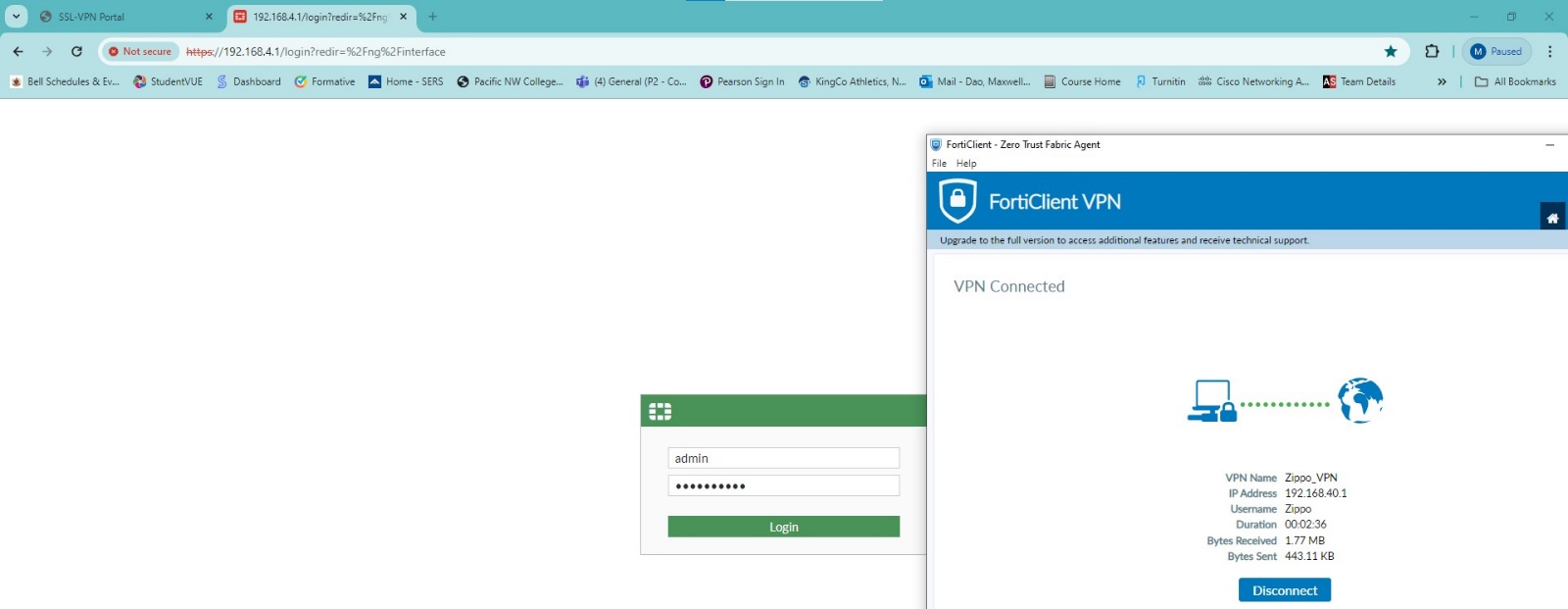


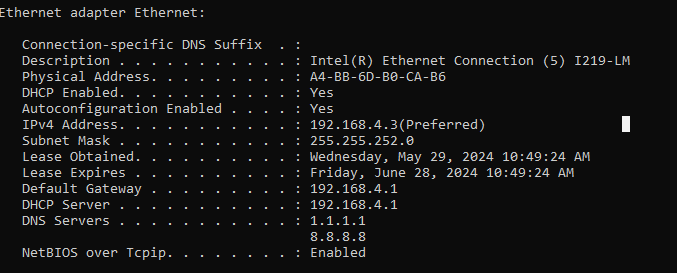


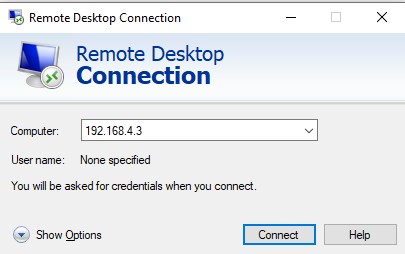


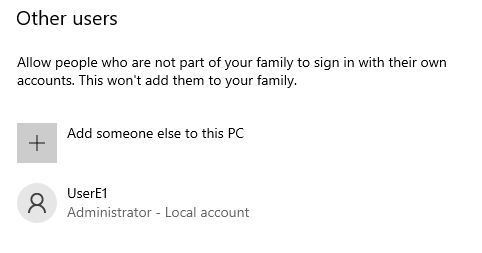


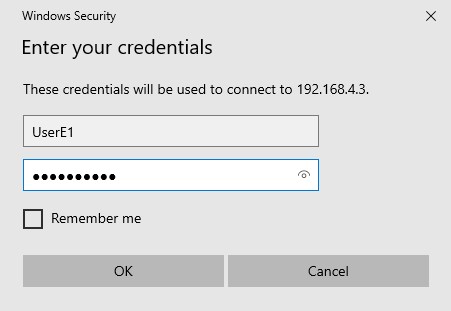






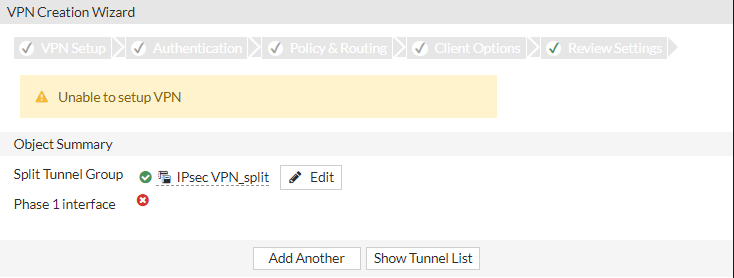






****

**Problems:**



* Could not start VPN
  + Created a new tunnel with different configuration
* Wrong address range set for incoming, cant be all users
  + Changed address range to ISP network
* Could not start remote desktop
  + Had an additional firewall blocking connection
    - Turned off firewall for the lab
* 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
* Unable to access VPN
  + On reset the firewall DHCP address changed so we could not use the same IPsec VPN saved profile to login
    - Needed to change IPsec Remote gateway

**Conclusion: s**

