Fortinet Cybersecurity Academy: Configuring an IPSec Site-to-Site VPN on a FortiGate 40-F Firewall

Colin J. Faletto, CCNA

FORTINET

Purpose

This lab is intended to show off the intricate VPN capabilities of the FortiGate-40F firewall by showing off an IPSec site to site VPN connection, which is a common type of connection used to provide a secure connection between different remote networks. The lab employs the use of Microsoft's Remote Desktop Protocol (RDP) to show off a common use of an site-to-site VPN between remote networks.

Background

Fortinet is a cybersecurity company founded in 2000 in Sunnyvale, CA. They are known for their flagship product, the FortiGate firewall, as well as a wide variety of other networking and security devices, such as the FortiSwitch and the FortiAP, and services such as FortiSandbox, FortiAuthenticator, FortiVoice, and FortiDDoS. Fortigate is an S&P 500 component and is listed on the NASDAQ as $FTNT.

The FortiGate 40-F is a firewall developed by Fortinet. It has capabilities expected of a modern firewall such as full routing capability, DHCP server capability, and support for a variety of filtering methods. The 40-F also supports running its own local RADIUS server with a feature called Local Auth (Authentication). The 40-F uses a fanless design, allowing it to operate silently. The 40-F has a small form factor at 1.5 x 8.5 x 6.3 inches, meaning it can easily fit into existing networking setups. By default, the 40-F gives out DHCP addresses in the 192.168.1.0/24 subnet to its clients (from .110-.210, specifically) and its GUI client can be accessed via HTTPS at 192.168.1.99.

A virtual private network, or a VPN, is a method of creating a secure tunnel between networks. VPNs allow computers that are physically located offsite to be treated the same as computers physically inside of a network**.** In the business world, VPNs are often used to allow employees working from home to access company resources located on internal servers. VPN services are commonly sold commercially, allowing consumers to connect to private network-sharing servers. These servers are often located in multiple countires or regions, enabling consumers to spoof their location and hide network traffic from their ISP.

There are two primary types of VPNs: site-to-site and remote access. They primarily differ in that site-to-site VPNs connect entire networks while remote access VPNs connect individual hosts to a remote network. Site-to-site VPNs often don't require separate host-based software while RA VPNs often do. Site-to-site VPNs are most commonly used to connect two branch locations of a company and allow them to act as if they were on the same physical network. Remote access VPNs are most commonly used to allow a remote employee to access resources on a secure internal company network.

Internet Protocol Security, or IPSec, is a set of protocols that provide authentication and encryption over an IP network. IPsec uses Encapsulating Security Protocol to provide the encryption and verify that a packet came from a given source. IPsec uses Authentication Headers to ensure the integrity of packets via a hash

function. Internet Security Association and Key Management Protocol (ISAKMP) is also used by IPsec facilitate the exchanging of encryption keys.

Remote Desktop Protocol, or RDP, is a Microsoft-proprietary protocol that allows a user to remotely view and control a connected Windows PC. RDP employs a client/server model, with the client being included on all versions of Windows and the server being exclusive to the operating system's higher tiers. RDP uses port 3389 with both TCP and UDP. RDP was introduced during Microsoft's transition from MS-DOS to the NT kernel with Windows NT 4.0 Terminal Services Edition, and the server has been included on every version of Windows (other than Home) since XP.

Lab Summary

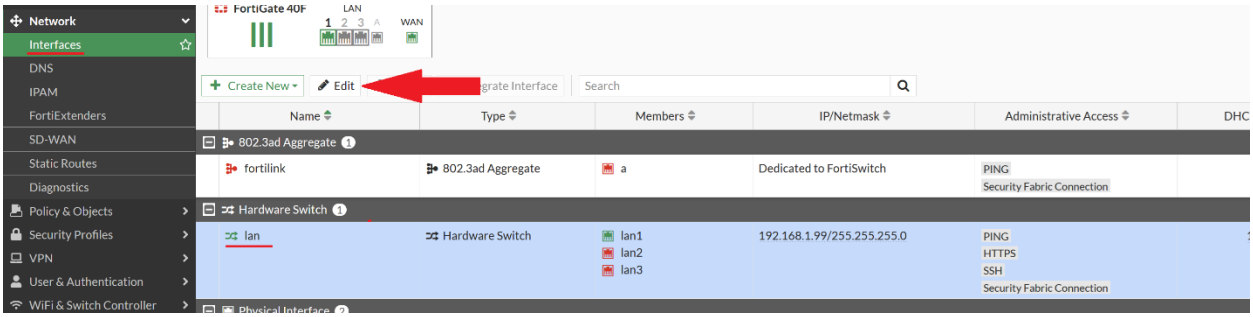
This lab creates a site-to-site VPN tunnel between two Fortinet 40-F firewalls. This VPN tunnel uses a PSK for authentication and allows private traffic to be transmitted over our "public" lab network.

Lab Commands

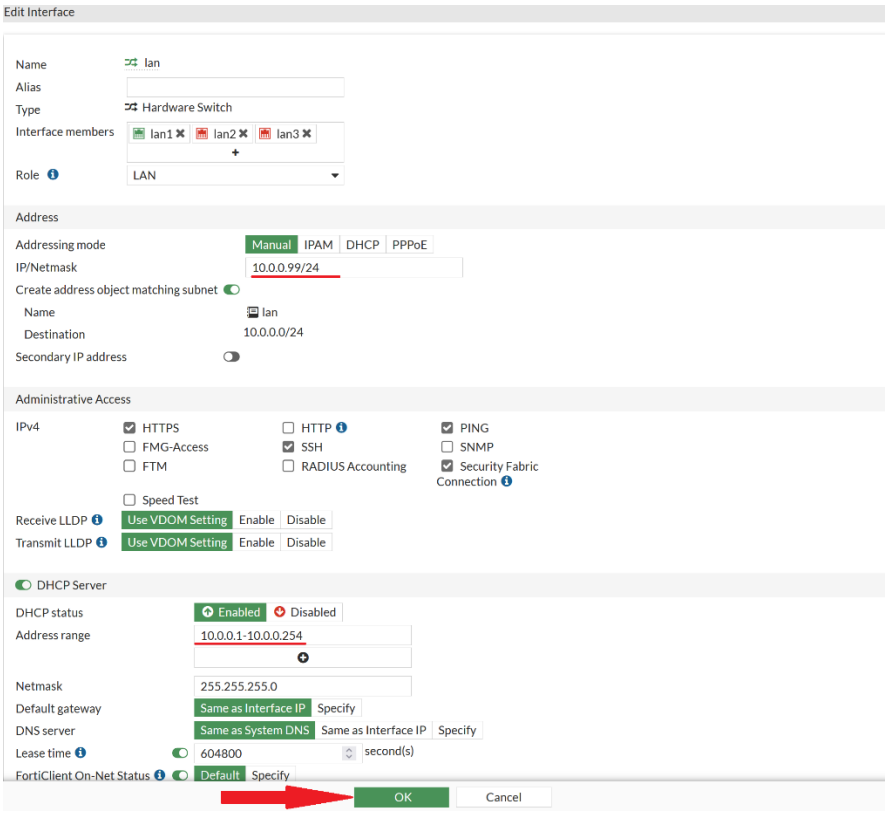
This lab requires the use of two different firewalls. Complete all the following steps on BOTH firewalls.

First, change your LAN IP address range to be different than the remote gateway's address range.

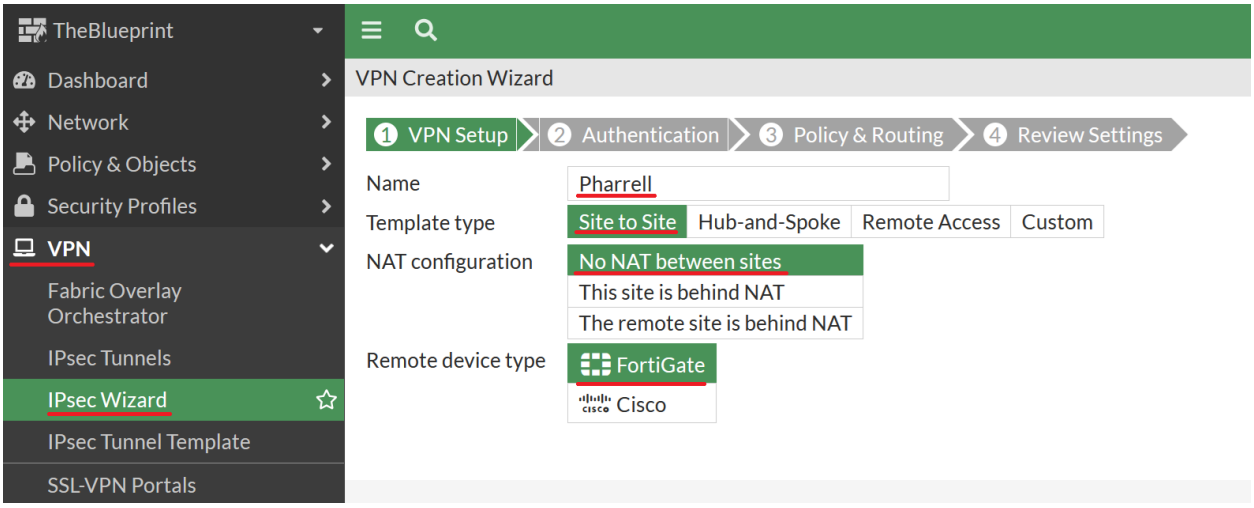
Go to Interfaces > LAN and click Edit.



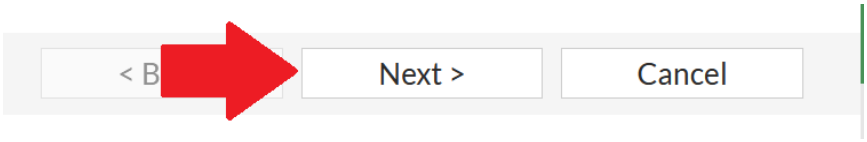
Change the IP/Netmask and DHCP address range to another valid private IP address range. Click OK.



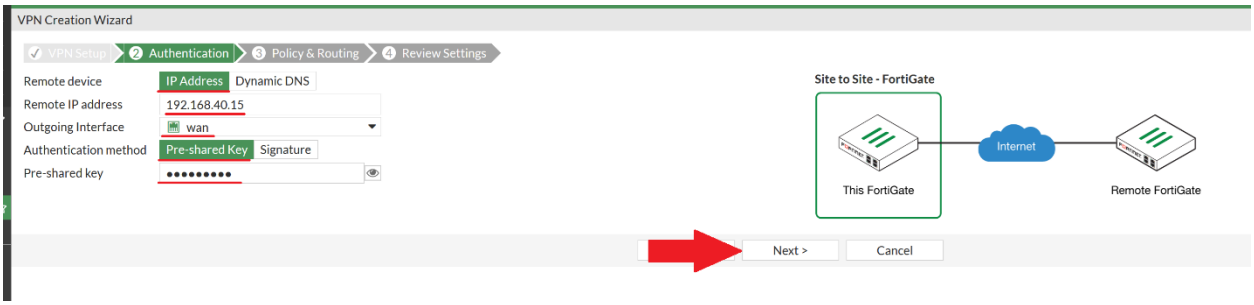
Go to VPN > IPSec Wizard. Give the VPN a name, set the template type to Site-to-Site, set the NAT configuration to No NAT between sites, and set the remote device type to FortiGate.



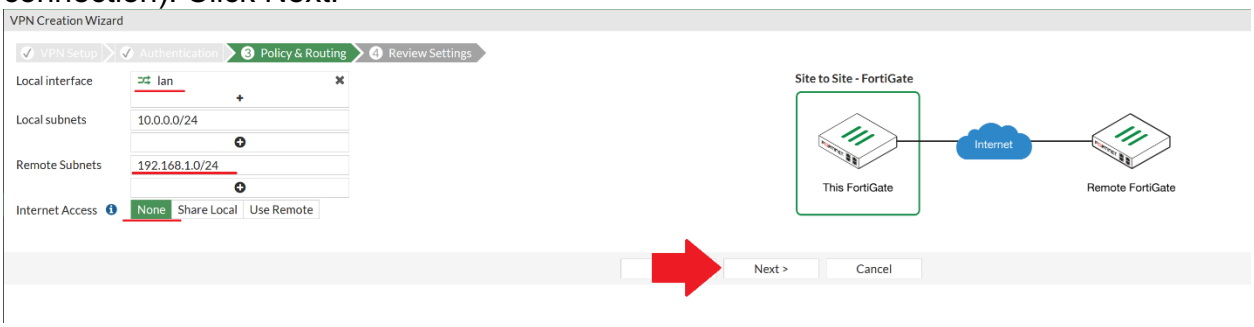
Click Next.



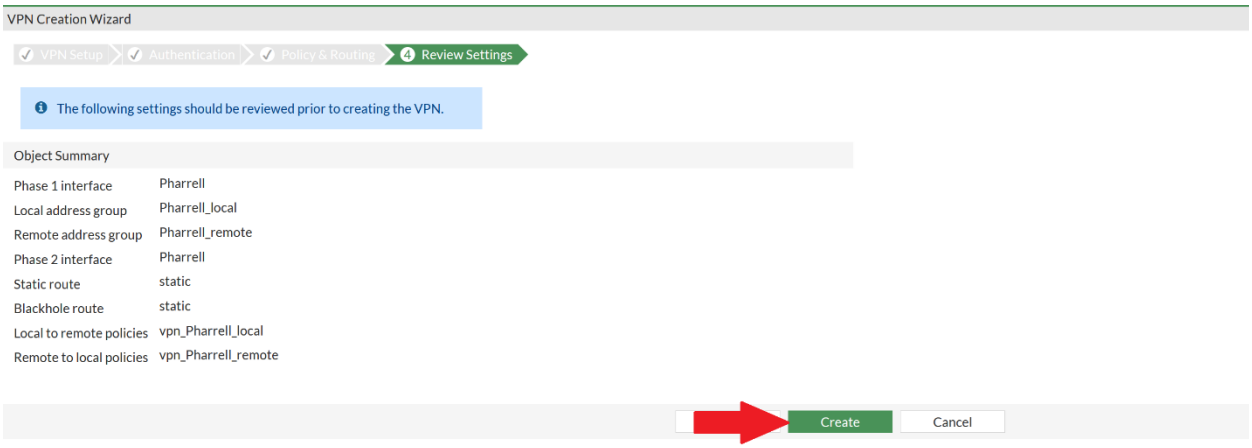
Set Remote Device to IP Address, the Remote IP Address to the IP of your partner firewall's outward-facing IP, the outgoing interface to WAN, the authentication method to pre-shared key, and agree on an identical pre-shared key between firewalls. Click Next.



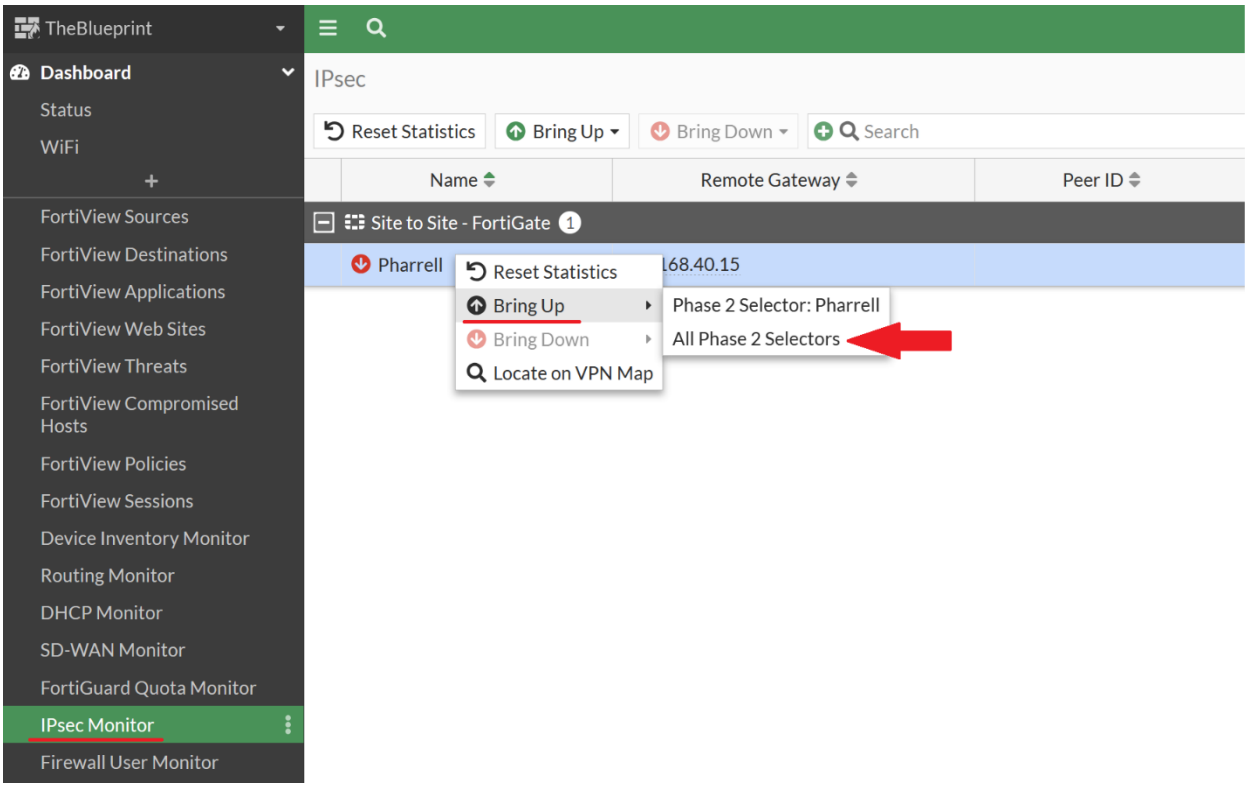
Set the local interface to LAN, and the local subnet will be filled in automatically. Set the remote subnet to the internal subnet of your partner firewall and set internet access to none (internet access does not need to be shared as both firewalls already have a WAN connection). Click Next.



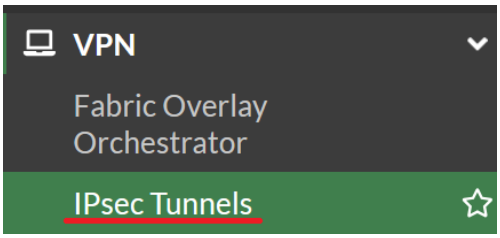
Ensure all settings look correct and click Create.



Next, go to IPSec Monitor. Right-click the VPN and click Bring Up > All Phase 2 Selectors.

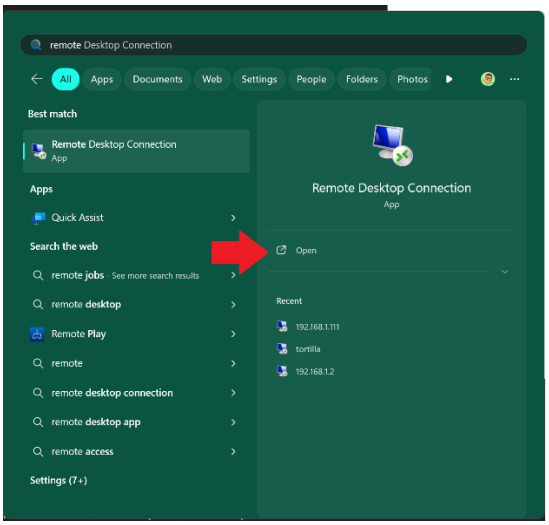


If the VPN is connected correctly, go to VPN > IPSec Tunnels.



You should see a green arrow next to the VPN name.

To test if the connection works, open the Remote Desktop Connection app.

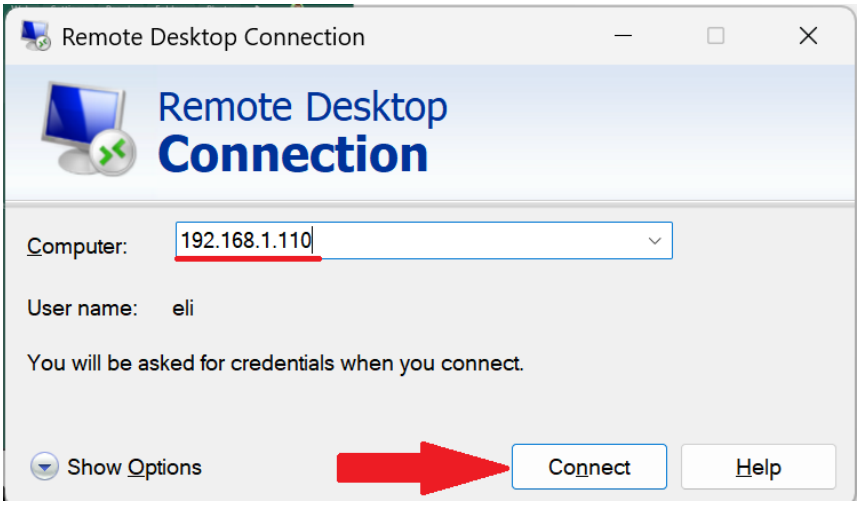


Get the IP address of the remote PC on the other side of the VPN.

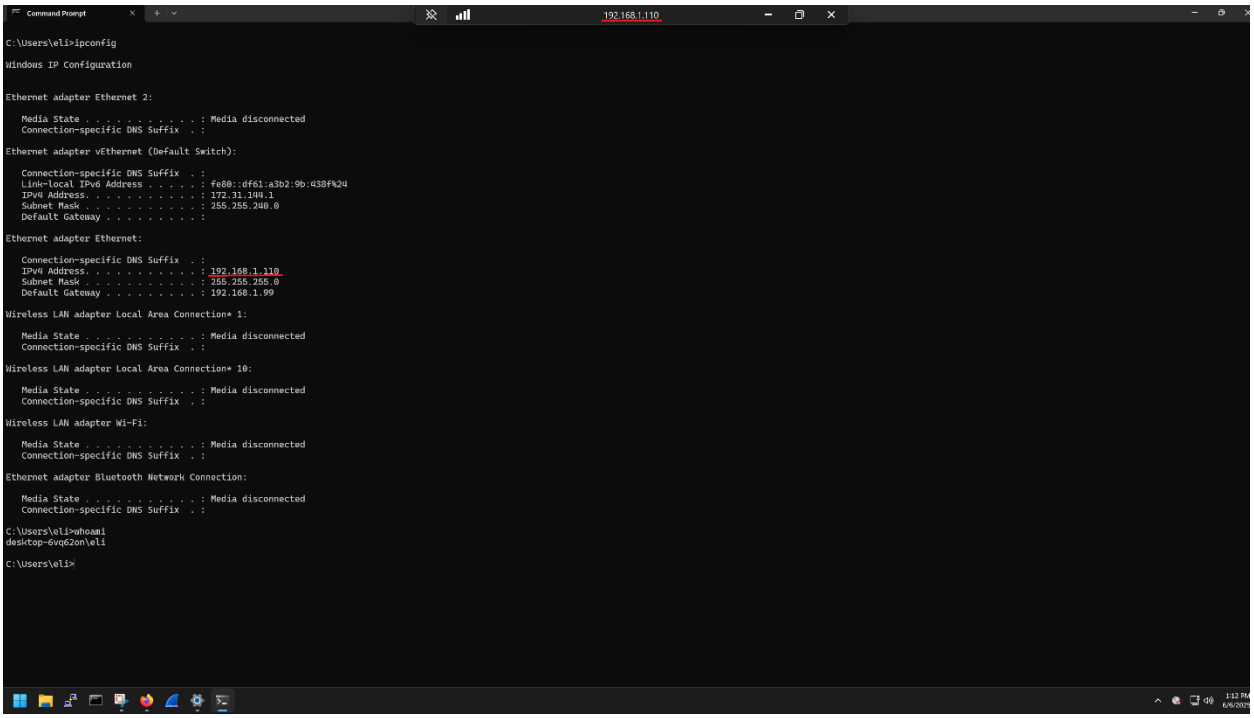
```
Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   IPv4 Address. . . . . . . . . . . : 192.168.1.110
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.1.99
```

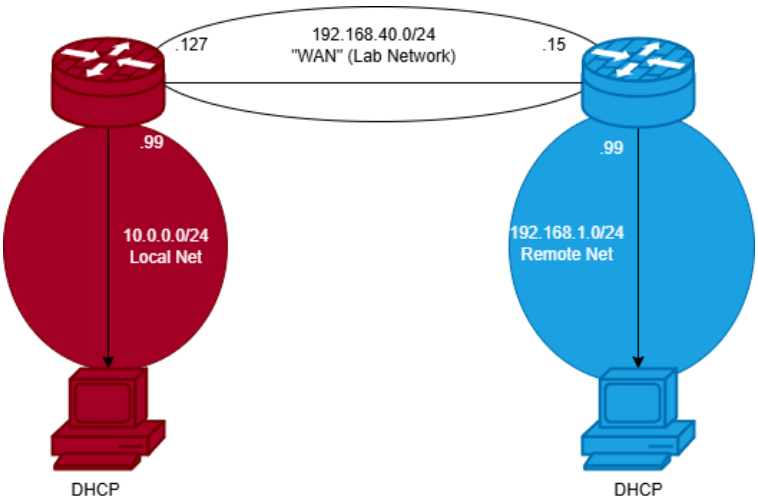
Enter the IP address of the computer on the other network and click Connect.



Here's a screenshot of a remote desktop connection to the remote PC:



Network Diagram (IPv4)



Problems

Originally, we had an issue where our firewall refused to negotiate with the remote firewall. This was likely caused by a mistyped PSK, as re-entering the PSK on both ends fixed the connection.

Conclusion

To wrap up, I now have a much greater understanding of site-to-site VPNs and fully understand how they are different than remote access VPNs. I am confident that I could replicate this configuration with Fortinet devices in a real-world environment between two remote sites.