w

**IPSec Site-to-Site**

**VPN on FortiGate 40F**

Ryan Chen

6/7/2025

**Purpose:**

The primary purpose of this lab is to configure and test an IPsec VPN on a generic Fortinet Fortigate 40F firewall. Building off of previous information form the SSL VPN configuration, as well as basic networking concepts learned through Palo Alto configuration, this lab aims to successfully setup an IPsec based Site to Site VPN.

**Background Information:**

A VPN, or virtual private network, is a commonly used service that provides a multitude of different privacy, security, and convenience functions. At its core, they work by encrypting traffic between an end-user and the server, allowing a secure connection to be established from anywhere. Given that this traffic is encrypted, it is essentially improbable for an adversary to read it. Even if they do manage to get hold of the traffic by sniffing it off the network, they will be unable to read it without the key.

For this reason, VPN’s are commonly used to secure traffic from an unsecure network into a secure network. By establishing this secure connection, attacks like a MITM (Man in the Middle) become less of a threat, since traffic is encrypted. Likewise, people also use VPN’s for their ability to “tunnel” traffic. This refers to the ability to establish a connection that emulates the device directly on a local network. This is useful for many different use cases, but commonly required by companies when employees are doing remote work. In order to keep company traffic secure even from an unsecure network, companies can configure a VPN to tunnel employee traffic back into the network. This allows employees to work remotely on company networks, all while keeping traffic secure. In our test case, this is the primary usage that we aim to target with our configuration.

Now that we know the basic use cases of a VPN, we can start to cover how it works at a base level. Typically for a VPN to successfully send and receive traffic, end users must connect through an application configured by the VPN provider. This application works by establishing a secure connection through the use of certificates and encryption, allowing end user traffic to be encrypted in transit and decrypted by the VPN at the end.

This lab targets the IPsec protocol based VPN, which is commonly used to connect two different enterprise sites (in different locations) together. This is typically used to provide security in cases where companies may need to remote access into assets from a different location. IPsec is an older protocol, and was the primary VPN configuration protocol before SSL/TLS existed. Configuration is slightly more complicated, but it generally provides more robustness and is a widely used and trusted option for VPNs.

Finally, one of the key concepts of this lab is remote access. For this purpose, we use the RDP (Remote Desktop Protocol) provided by Windows. This protocol allows us to configure one machine inside the network as a server, and the other machine as a end user that will ultimately establish a connection to the server to demonstrate that the VPN is working. RDP gives us the ability to remotely view another Windows desktop, a common use case for companies that want to enable employees to do remote work. We demonstrate functionality of the VPN through the FortiClient connection, and then through RDP.

**Network Diagram:**A diagram of a computer network

AI-generated content may be incorrect.

**Lab Summary:**

IPsec VPN configuration, while still relatively simple, is indeed more complicated than SSL. Fortinet makes it easy to create the IPsec VPN with their built in IPsec VPN Wizard tool. This tool automatically configures most of the things, but custom policies must still be created for both ends of the connection in order to allow traffic to actually pas through. Overall, the process is not difficult, simplifying deployment a lot.

**Lab Commands:**

1. Navigate to VPN > VPN Wizard. Create a new VPN and give it a name. Set the template to Remote Access, and make sure that the VPN is using FortiClient.

A screenshot of a computer

AI-generated content may be incorrect.

1. Set the agreed upon PSK with the other partner end, and set the User Group accordingly (we later changed ours to Cisco).

A screenshot of a computer

AI-generated content may be incorrect.

1. Set the address and LAN interface for the receiving end.

A screenshot of a computer

AI-generated content may be incorrect.

1. Create the new VPN object. The process will automatically create a new VPN tunnel. However, we still need to create the firewall policies to allow traffic to flow.

A screenshot of a computer

AI-generated content may be incorrect.

1. Upon creating the VPN tunnel, check that the object has the correct addresses. You may define addresses either with Fortinet objects, or directly type them in. We later changed our configuration to explicitly show address spaces.

A screenshot of a computer

AI-generated content may be incorrect.

1. Before creating firewall policies, navigate to Policies & Objects > Addresses and create a new Address Group. We need to create two different address groups, one for our local address space, and one for the remote address space. We chose our local subnet to be 192.168.3.0, and Calvin, our lab partner, was set as 192.168.1.0.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

1. Now, create a new firewall policy. You will need two policies: one to allow traffic from the tunnel to LAN, and one to allow LAN back to the tunnel. You may create them in either order.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

1. Finally, double check that the firewall policies are correctly configured and up.





1. Now that the firewall policies are up, our configuration is complete. If the other end has the same configuration and everything is connected, you should see the tunnel go up if you navigate to VPN > IPsec Tunnels.

A screenshot of a computer

AI-generated content may be incorrect.

1. With the tunnel up, all that’s left to do is connect via FortiClient, and then initiate an RDP connection. This was done on our partner’s device, and as such, there is no screenshot to display here. You can double check the configuration is working by looking at the firewall policies. You should see that the data fields increase in size, as the amount of data between the two tunnels flows. This means the configuration is successfully completed!

**Problems:**

1. **Required Firewall Policy**

At first, we were unaware that a firewall policy was required for the IPsec VPN, similar to the SSL VPN. We also incorrectly assumed that the Fortinet UI would automatically create this firewall policy after we created the IPsec object, but it did not. This caused the connection to fail. Upon adding the policy, everything worked fine.

1. **IPsec Tunnel Down**

Though the IPsec tunnel may bring itself up automatically if the device on the other end of the tunnel is configured correctly, it also has the possibility not to go up by itself. We were unaware of this the first time, and realized that we had to manually bring the tunnel up. There is an option to Bring Tunnel Up in the IPsec tunnel page, and upon clicking this, the tunnel turns green.

1. **IP Address Ranges**

Our IP address ranges for one of the IPsec tunnel endpoints was configured with poor subnetting, and as a result cut out the address space that the device was located in. Upon changing this, we were able to initiate an RDP connection, and the configuration worked as expected.

**Conclusion:**

This lab was definitely more challenging than the SSL VPN, however, it provides a great introduction to IPsec configuration on Fortinet devices. The VPN Wizard makes the process relatively easy, having only to complete the firewall policy parts. This lab was also a great refresher on debugging, since our tunnel was initially not working. We realized later on that it was an issue with the subnet configuration, as we had mistakenly set the subnet to a value smaller than the actual contained addresses. To solve this issue, we were required to work backwards.

Fortinet IPsec Remote Access

Ryan Chen, P3-4 Cisco Cybersecurity, Mr. Mason

A white paper with a logo on it

AI-generated content may be incorrect.

