w

**SSL-VPN on**

**FortiGate 40F**

Ryan Chen

6/7/2025

**Purpose:**

The primary purpose of this lab is to configure and test an SSL VPN on a generic Fortinet Fortigate 40F firewall. Building off of previously learned concepts in configuring Palo Alto devices, this lab translates past information and applies it towards Fortinet devices. Furthermore, this configuration continues to utilize basic SOHO and Fortinet configuration knowledge learned in previous labs.

**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.

However, this lab is specifically targeted towards configuring an SSL VPN, which functions using the Secure Socket Layer (SSL) protocol. This protocol, which is most commonly seen in securing browser web traffic, can also be used to secure VPN data. Because of the ubiquitous nature of browsers, SSL can be found on almost any device, and thus is a suitable way to implement the VPN. It simplifies VPN connections to allow for much easier configuration and usage.

SSL VPN’s can provide two main features: browser-based access, and tunnel-based access. Both use the SSL protocol to send data, but function in different ways. Browser based access generates a session directly in the browser, giving secure access to a webpage through the session. This simplifies deployment, but also limits applications that can run within the web interface. On the other hand, tunnel mode creates an encrypted tunnel as if the client machine were on the local network of the SSL VPN server. This typically allows full access and much finer configuration controls. This lab focuses on tunnel based access through Fortinet’s proprietary VPN client, FortiClient VPN.

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:**

SSL VPN configuration is relatively painless on the Fortinet firewall, especially with the help of the easily navigable GUI. First, we have to define an SSL VPN configuration where we can set connection port, name, etc. From there, we simply create a firewall policy to allow the SSL VPN configuration to pass through our firewall, and our configuration is complete. Fortinet makes the SSL VPN as painless to setup as possible.

Again, since we are configuring tunnel mode access, this simplifies the configuration steps that we have to complete.

**Lab Commands:**

1. First, navigate to the VPN > SSL-VPN settings area. Create a new VPN, and populate it with the following fields:

A screenshot of a computer

AI-generated content may be incorrect.

1. Ensure that the listening port is on a non-commonly used port. This is to prevent the VPN tunnel from potentially overlapping with any guest services. The rest of the settings can stay default. We want an Idle Logout for extra security, and our tunnel mode should automatically assign addresses (these addresses will be able to ping in our internal network).

A screenshot of a computer

AI-generated content may be incorrect.

1. Finally, make sure that the user groups are set to allow FortiClient to login with certain credentials. You will need to know these credentials when connecting with FortiClient. In this case, we have a user group allowed.

A screenshot of a computer

AI-generated content may be incorrect.

1. Next, we need to create a firewall policy to allow our SSL VPN traffic to actually pass our traffic through to LAN. Navigate to the Policy and Objects section.

A screenshot of a computer

AI-generated content may be incorrect.

1. Create a new firewall policy. Populate the fields, setting the incoming interface as the SSL VPN object that we created, allowing it to pass to LAN. Allow all traffic to flow through from the previously determined user groups.

A screenshot of a computer

AI-generated content may be incorrect.

1. After creating this policy, our SSL VPN configuration is completed! Now, we have to test our configuration by connecting via FortiClient and RDP’ing to an internal machine. Navigate to <https://www.fortinet.com/support/product-downloads> and download the VPN-only file.

A close-up of a white background

AI-generated content may be incorrect.

1. Go through the installation, and create a new SSL-VPN tunnel from the three selections at the top.

A screenshot of a computer

AI-generated content may be incorrect.

1. Populate the fields with the outwards IP address of the firewall configuration. In this case, our outward facing IP is actually a private network, as this is a simulated environment. However, in a real-world configuration, this global IP should be accessible from the broader internet, and assigned statically by an ISP. Add the target port (4433).

A screenshot of a computer

AI-generated content may be incorrect.

1. Save the VPN and connect to it. Expected behavior should be a loading screen, and then a successful connection to the IP.

A screenshot of a computer

AI-generated content may be incorrect.

1. Ensure that Windows RDP connections are turned on in Windows.

A screenshot of a computer

AI-generated content may be incorrect.

1. Find the IP address of the RDP host using “ipconfig” in a CMD terminal. This will give you the local address that we will use to connect.

A screenshot of a computer

AI-generated content may be incorrect.

1. On the machine with the VPN connected, initiate an RDP connection.

A screenshot of a computer

AI-generated content may be incorrect.

1. Success! Our VPN connection has initiated a tunnel in which we can access local resources, like a computer through RDP!

A screenshot of a computer

AI-generated content may be incorrect.

1. Disconnect the VPN client and stop the RDP connection. Our configuration is now complete.

A screen shot of a computer

AI-generated content may be incorrect.

**Problems:**

1. **Required Firewall Policy**

At first, we were unaware that a firewall policy was required for our SSL VPN to pass through to LAN. We assumed that the Fortinet UI would automatically create this firewall policy after we set the SSL VPN object, but it did not. This caused the connection to fail. Due to incorrectly configured logging, this didn’t show up either. After adding the policy, everything worked fine.

1. **External IP Configuration**

Due to the nature of this lab environment, our “external” facing IP is actually an internal, private network configured on the broader Cisco local network. We forgot about this fact, and were searching for a public IP at first to connect to. The IP we actually should have been using was the one attached to our WAN port, in the 192.168.40.X range.

**Conclusion:**

Overall, this lab was a great introduction to the SSL VPN capabilities of Fortinet firewalls. It definitely showed that SSL VPN’s are far easier to configure on Fortinet than Palo Alto. The Fortinet firewall GUI takes care of the heavy work, and there is little configuration involved for us.

Fortinet SSL VPN Remote Access

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

A white paper with a blue logo

AI-generated content may be incorrect.

