# Fortigate 40F Firewall SSL VPN Configuration

Andrew Pai

Period 5 Cybersecurity

CISCO

paloalto® NETWORKS

## Purpose:

The purpose of this lab was to have our group configure our Fortigate 40F firewall with an SSL VPN. This will allow another remote desktop to access a PC on our firewall's network with the correct user credentials and authorization. To do this, we'll be utilizing the Fortigate firewall's GUI as well as the Forticlient VPN software and Microsoft's Remote Desktop Protocol (RDP).

## Background Information:

This lab focuses on implementing an SSL VPN on our Fortigate 40F firewall. Like mentioned in a previous lab for configuring the Global Protect VPN on a Palo Alto firewall, VPNs are known as Virtual Private Networks and are used to connect to a private network while not actually being in that network. VPNs are useful to ensure that data transmitted from remote locations is secure and encrypted and cannot be attacked. Many people use VPNs to do things like avoid Internet censorship, while large companies can use VPNs to allow employees to access the company network while working at home.

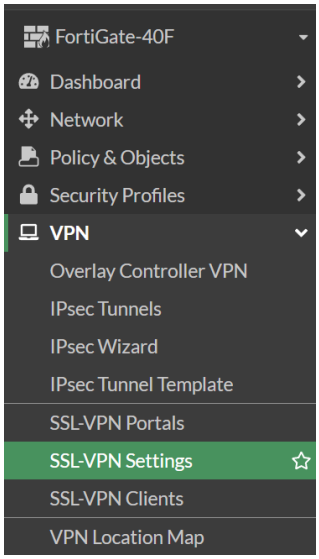
The VPN that we'll be configuring on the Fortigate firewall in this lab uses SSL and TLS, the Secure Sockets Layer and Transport Layer Security protocols. SSL as a protocol ensures that data is encrypted and secure when it's transmitted. It does this by creating a secure connection with the desired target through a handshake process. During this process, the target and sender decide on what type of encryption to use and exchange the necessary keys to encrypt and decrypt data. Both asymmetric and symmetric encryption algorithms may be used in SSL VPNs, with common examples being the RSA, ECC, and AES algorithms. TLS is the more updates version of SSL and is more secure than SSL because it has a stronger handshake and cipher mechanisms. While many VPNs say that they use SSL, the type of encryption that they really use is TLS, which is used in common VPNS like OpenVPN and AnyConnect.

In order to connect from a remote desktop to the firewall's internal network through the SSL VPN, our group will be using Fortinet's Forticlient VPN software. Forticlient is a typical VPN client that allows users to connect to an internal network through both SSL and IPSec VPNS. While IPSec is an option for Forticlient, our group will be addressing that in a different lab instead of

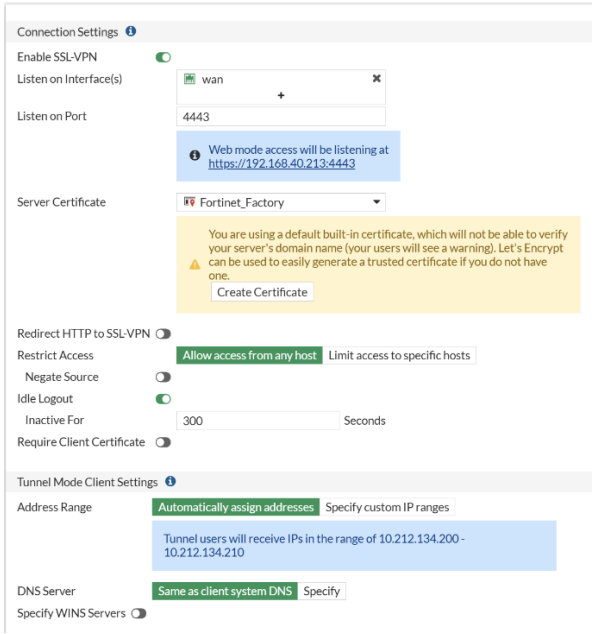
this one. Forticlient also has various other authentication methods like two factor authentication and can use split tunneling.

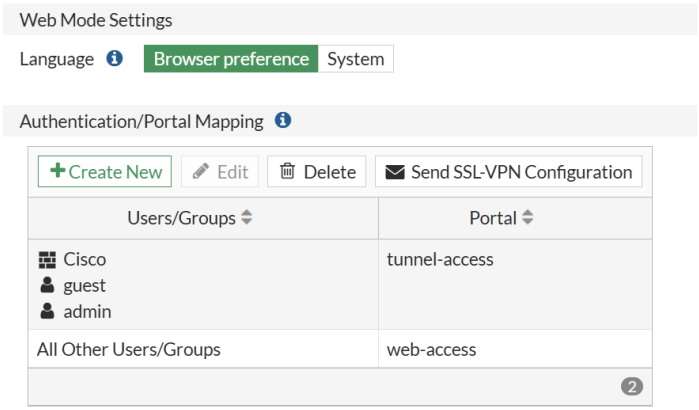
## Lab Summary:

In the GUI of your Fortigate 40F firewall, navigate to the SSL-VPN Settings section on the left taskbar.

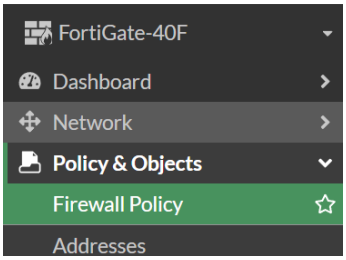



Create a new VPN and enable it to use the WAN interface of your network. Create a custom port that you'll use on Forticlient and use the default Fortinet_Factory Certificate. Add the user groups that you'll need to use the VPN into the VPN settings.

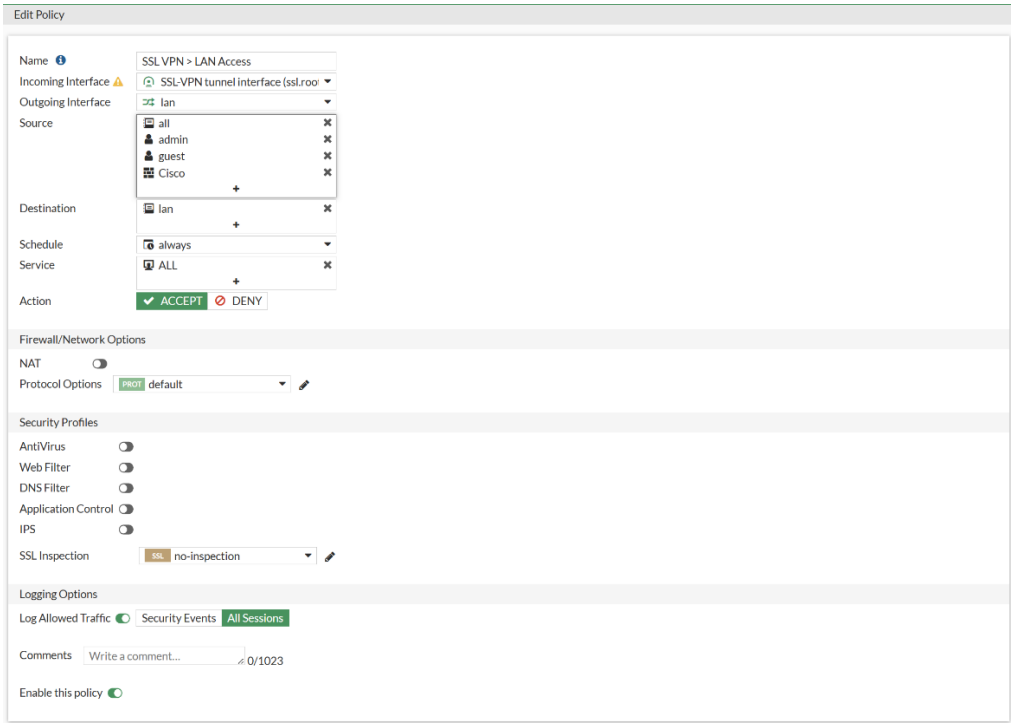




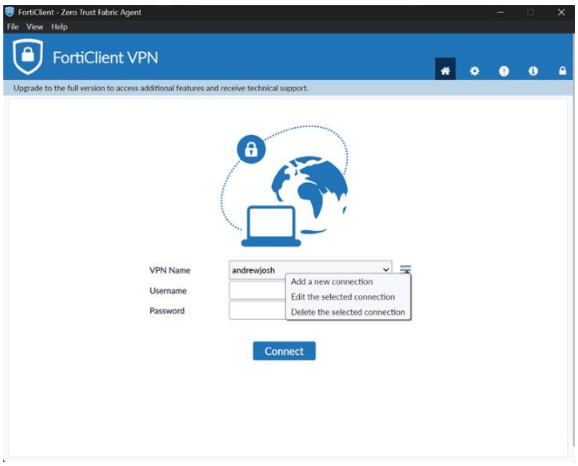

Navigate to Firewall Policies under Policy & Objects on the left taskbar and create a new policy.



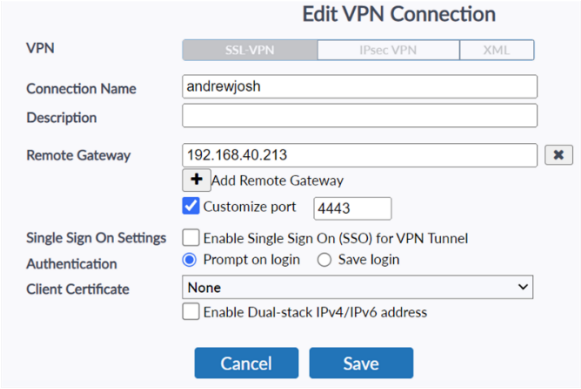

Set the outgoing interface to your LAN's interface, with the incoming interface as the SSL VPN tunnel you just created. Add your intended user groups to source and your LAN to destination.



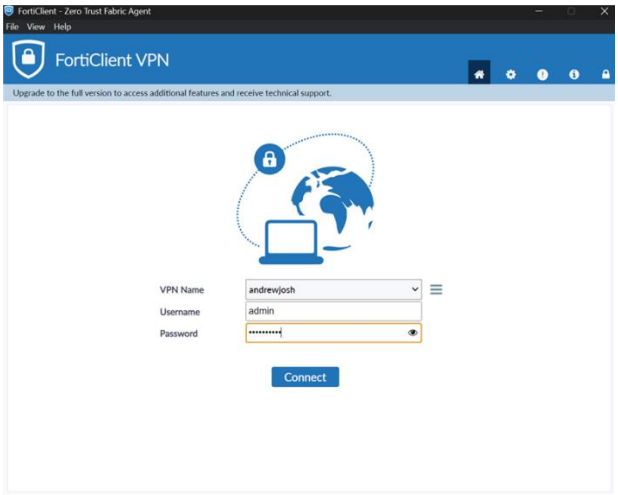
Download the Forticlient VPN software onto another PC and click on “Add a new connection” so you can create a new VPN.



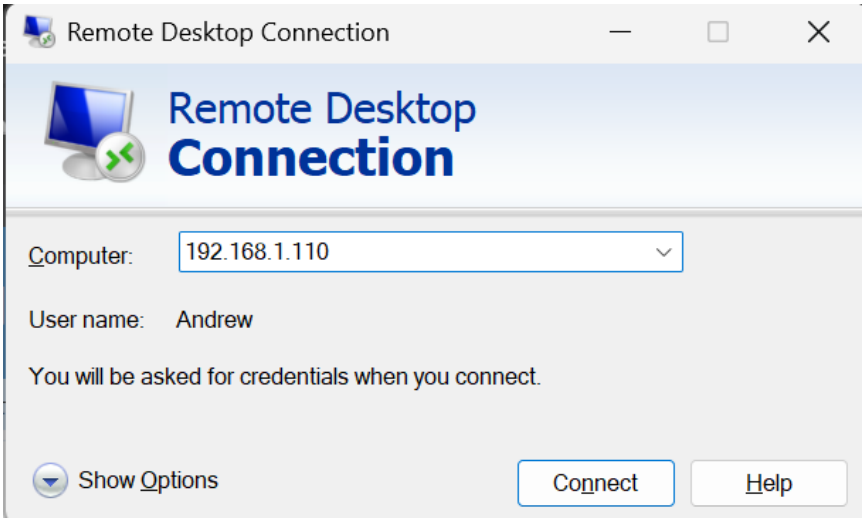

Select “SSL VPN,” add the IP of the firewall that you’re using, and add in the port that you configured for your SSL VPN earlier in the lab.



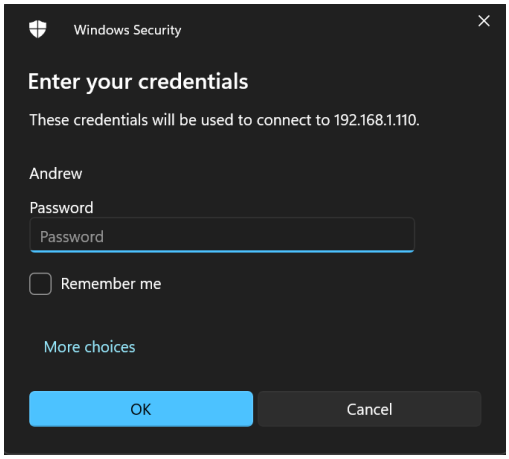

Once you’ve created your VPN settings on Forticlient, attempt to log in with one of the user authentication credentials you set up earlier.



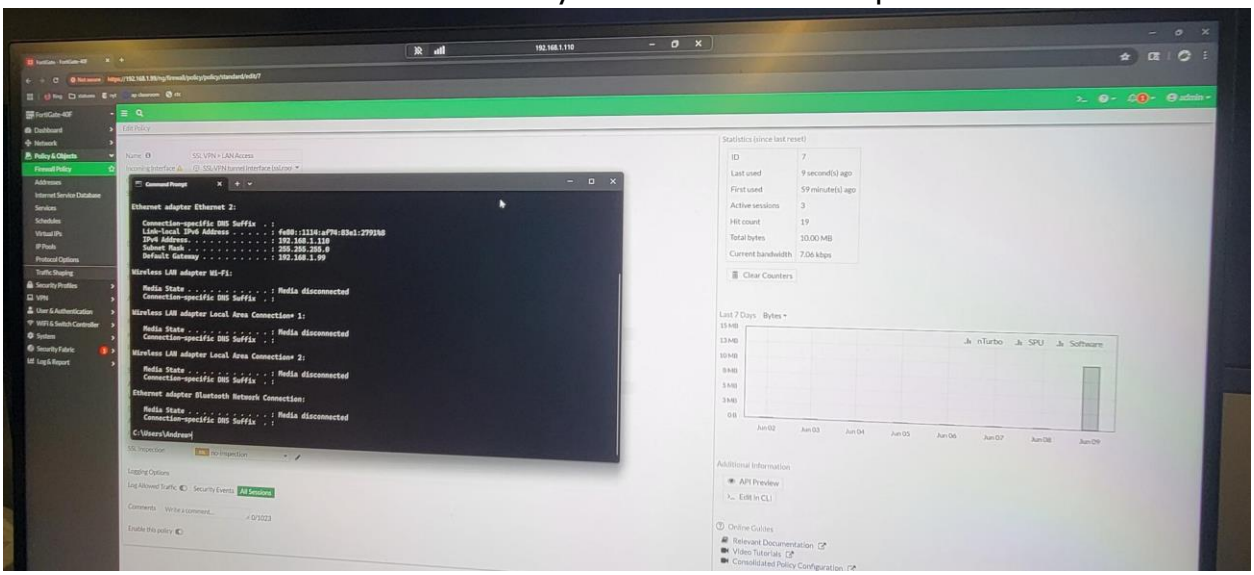

Finally, in order to actually use your VPN, log in to Window's Remote Desktop Connection and type in the IP of the PC you're trying to reach.




Enter in the credentials of your computer when asked to connect.



Once you've entered your credentials, RDP should let you control the PC inside the firewall's network from your remote desktop.



## Problems:

One of the problems that our group had was that our DHCP server wasn't working and it either gave our PC no IP address or an IP address completely off of the network that we'd configured our VPN for. We solved this by troubleshooting Layers 1 and 2 to get the DHCP server working and eventually was able to access our VPN afterwards.

Another similar problem was our group not realizing that we didn't have a default gateway for our PCs. This was because we'd statically set our PC's IP addresses earlier in the lab to test some other things and had forgotten to put it back on DHCP. Because of this, we couldn't ping or access the other PCs. This was a simple fix of just changing the PC's IP back to DHCP though.

## Conclusion:

In conclusion, this lab has familiarized our group with creating and setting up an SSL VPN. We gained skills relating to how to set up firewall policies on the Fortigate, how to create SSL VPN's on the Fortigate, as well as how to use both Forticlient and Remote Desktop Connection on Windows computers.

## Lab Signoff:

Fortinet SSL VPN Remote Access

Andrew Pai Cybersecurity Mr. Mason