A brochure of a remote access lab

AI-generated content may be incorrect.

**Purpose:**

The purpose of this lab is to continue to utilize Fortinet’s security tools and set up remote desktop access through an SSL VPN connection.

**Background:**

Fortinet is a cybersecurity company that is based in Sunnyvale, California that sells and innovates cybersecurity solutions. It is known for its FortiGate firewalls, which are considered one of the most deployed network firewalls in the world due to its condensed and easy-to-understand interface.

Dynamic Host Configuration Protocol (DHCP) is a process that automatically assigns devices with an IP address from a predetermined pool of IP addresses. This simplifies network assignments and reduces the potential for manually configured errors.

Remote Desktop is a mechanic that allows users to access and control a different device using their current device over a network, provided that they are authenticated. It is commonly used in IT so that users can access resources stored in different locations.

SSL (Secure Sockets Layer) is a security protocol that creates a secure VPN connection through web browser. It typically uses HTTPS/Port 443, a TCP connection. It allows remote users to securely access internal network resources without needing specialized VPN software.

**Lab Summary:**

First, we wired our firewall as we always do, except we also want to connect a second host into the system as well. We then entered our firewall’s GUI and configured our SSL VPN settings before making firewall policies to support these configurations. Afterwards, we used the Fortigate client to activate our SSL VPN, then added our users into the system’s permitted list of Remote Desktop users so that we can establish a connection.

**Lab Procedure:**

1. Go to VPN > SSL-VPN Settings. Select your outgoing WAN port for Listen on Interface. It is also recommended to change Listen on Port to something other than the default HTTPS port (443) to prevent potential interferences. In our case, we used Port 4433.

A screenshot of a computer

AI-generated content may be incorrect.

1. Scroll down to Authentication/Portal Mapping. Here, we give all of the users that we’ve created and want to have access to connecting through our SSL VPN permission to access the portal. These users have all been set up with a username and password for authentication purposes.

A screenshot of a computer

AI-generated content may be incorrect.

1. Go to Policy & Objects > Firewall Policy. Click “Create New”.   
   A screenshot of a computer

   AI-generated content may be incorrect.
2. The screenshot shown has the SSL VPN tunnel as our incoming and our LAN as our outgoing, but we will also need another policy with the two interfaces switched so that traffic can come from both ways. Make sure Source is set to “all”, Destination is set to “all”, Schedule is set to “always”, and Service is set to “ALL”.

A screenshot of a computer

AI-generated content may be incorrect.

1. Scroll down and make sure NAT is turned off. Keep all other settings default.

A screenshot of a computer

AI-generated content may be incorrect.

1. Go to Fortinet’s website and download FortiClient. Make sure that “Secure Remote Access” is checked.

A screenshot of a computer

AI-generated content may be incorrect.

1. Once you have logged into the client, go to Remote Access tab. Click “Configure VPN”.

A screenshot of a computer

AI-generated content may be incorrect.

1. Set the Remote Gateway to the IP of the LAN interface. We also need to check “Customize Port” and input the same port that we set earlier.

A screenshot of a computer

AI-generated content may be incorrect.

1. Enter the VPN name, then enter the username and password that you set for your intended user.

A screenshot of a computer

AI-generated content may be incorrect.

If the connection succeeds, you should see this screen.

A screenshot of a computer

AI-generated content may be incorrect.

1. Search “Remote Desktop Settings” into the Windows search bar. Make sure the switch for Remote Desktop is turned on for both computers.

A screenshot of a computer

AI-generated content may be incorrect.

1. On either the device you are trying to remote access into or the device that you are using to perform remote access, use the keyboard shortcut Windows + R, then type “lusrmgr.msc” once the field prompts you to.

A screenshot of a computer error

AI-generated content may be incorrect.

1. Go to Local Users and Groups (Local) > Users. Then, under the Actions sidebar, hover over Users > New User.

A screenshot of a computer

AI-generated content may be incorrect.

1. Create a new user with a username and password.

**A screenshot of a computer screen

Description automatically generated**

1. Once completed, you should see a new user created on the list.

A white background with black text

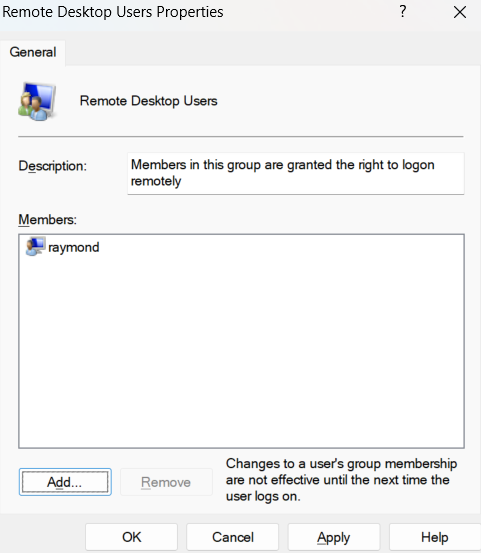
AI-generated content may be incorrect.

1. Go to Local Users and Groups (Local) > Groups. Select Remote Desktop Users. On the Actions sidebar, hover over More Actions > Add to Group.

A screenshot of a computer

AI-generated content may be incorrect.

1. Select the user that you intend to add.



1. Finally, on the computer that you want to remote access, do an ipconfig to see its current IP. Then, on the computer that you are using to perform remote access, open up the Remote Desktop Connection application and type in the IP that you see on the ipconfig output screen.

A screenshot of a computer

AI-generated content may be incorrect.

1. You should be prompted to sign on using the credentials you just created. Do so and click “Ok”.

A screenshot of a computer screen

AI-generated content may be incorrect.

You will know that your remote access is successful when you see this. A screenshot of a computer

AI-generated content may be incorrect.

A wooden dock in the water

AI-generated content may be incorrect.

**Problems:**

We had a few minor issues while doing the lab.

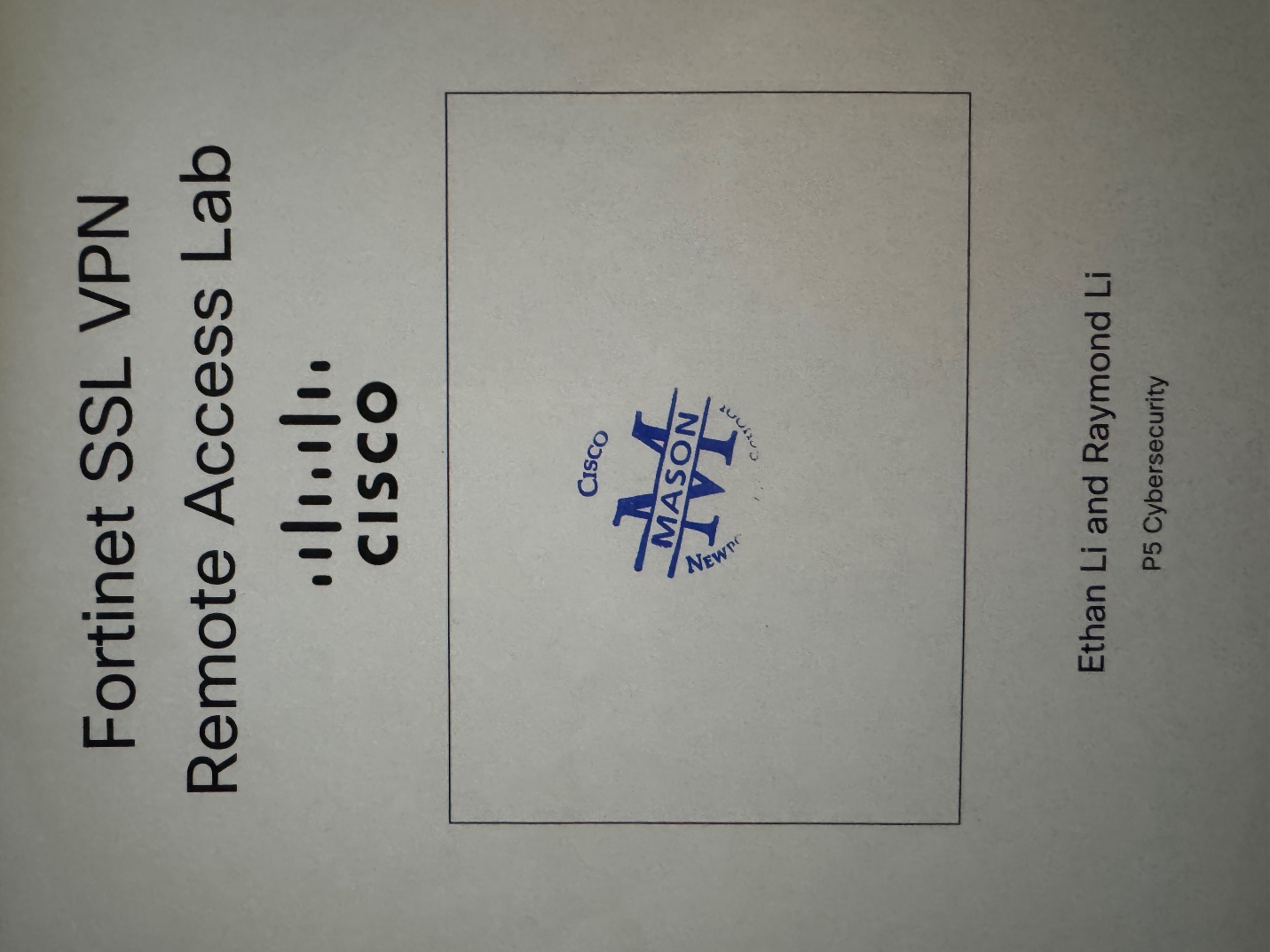
The first of which was that we physically cabled our system wrong at the start, connecting Host 2 directly to the ISP when we should’ve connected it to the switch, then have another cable running from the switch to the ISP. This resulted in us not being able to connect to the internal LAN network from our Host 2 and also failing to establish our VPN connection. We noticed the issue when we reviewed our earlier screenshots and noticed that the network that the SSL VPN was trying to listen on was the 10.0.0 network.

Our second issue was that we forgot to turn on remote desktop for both devices. This was a relatively simple fix to perform and figure out as we got an error message that told us so.

**Conclusion:**

In this lab, we successfully configured our Fortigate 40F to support remote desktop. This was done through configuring an SSL VPN tunnel, then creating firewall policies to support the flow of traffic through the VPN. We then used Fortinet’s VPN client Fortigate to remotely connect through a secondary host. Understanding how to configure SSL VPNs and firewall policies not only enhances our technical proficiency but also reinforces best practices in securing remote connections against unauthorized access.

**Sign Off:**

****