Introduction:

IPSec (Internet Protocol Secure) is a combination of protocols used to secure traffic across public networks. This lab uses it to create a VPN where we will use an external PC to securely remote desktop to another PC on the internal network of our FortiGate 40f. The FortiGate, with its ease of setting up will be used to set up most of the configurations that we will need.

Background Information:

The FortiGate 40F is a "next-gen" firewall that enables small and midsized businesses (SMB) to get enterprise level security on a budget. Featuring many integrated security services such as: Firewall, VPN, Antivirus, Intrusion prevention. VPNs allow for users to remotely access resources in a secure way over the open internet. IPsec VPNs allow for secure tunnels over the open internet allowing secured with IPSec. IPSec runs on the network layer of the OS model and on top of the IP protocol.

IPSec consists of multiple protocols that are design to secure IP communications by encrypting data across public networks. Operating on the network layer, it makes it versatile to use across applications and networks. IPSec consists of Authentication Header (AH), responsible for data integrity and authentication and Encapsulating Security Payload (EAP), responsible for encryption and integrity and authentication. This lab used tunnel mode which has full packet encryption and allows users remote users to connect to a company network.

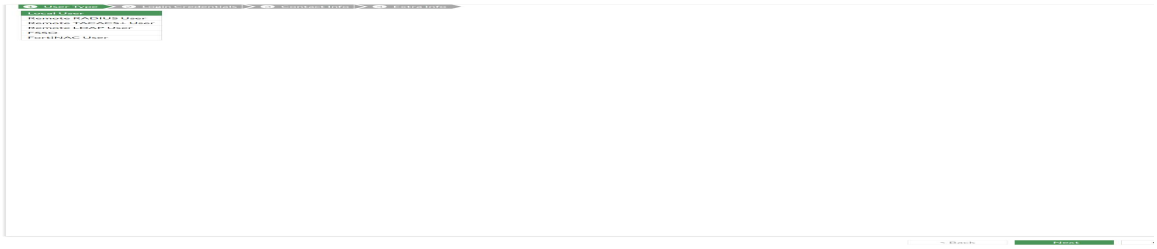
Remote Desktop on Windows (only available for Windows Pro, Enterprise and Server editions) is a feature that enables users to remotely connect to their Windows desktop and use it as if they were on it remotely from anywhere in the world, provided that they have internet access. This is extremely useful for use cases such as remote work or over the web troubleshooting.

Lab Summary:

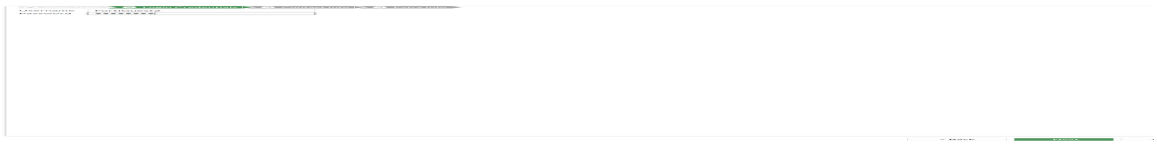
In order to set up IPSec on a FortiGate 40f, first a user must be set with a

username and password and set it up with a user group. Then use the VPN creation wizard to set up the VPN with interfaces, pre-shared keys, and client-side IP addresses. We then must download the FortiClient and IPSec into the on-premise network from the remote PC. Finally, we set up remote desktop on the on-premise windows PC by setting up a user and giving it administrator permissions. Because of the IPSec VPN, the remote PC will already be on the internal network of the firewall, now simply open remote desktop and enter the private IP address of the on-premise PC.

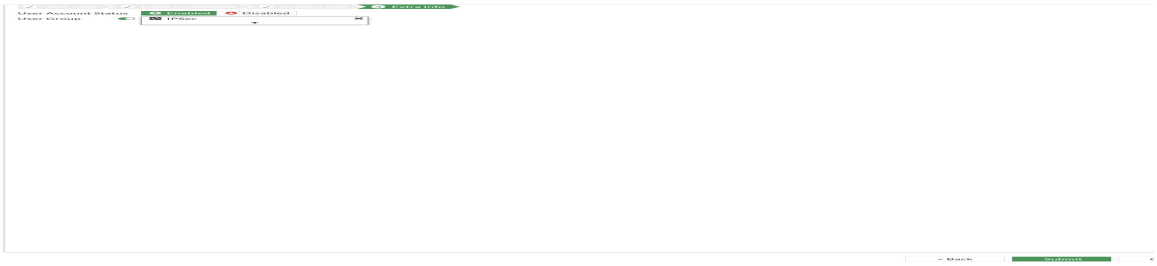
Step-by-Step:



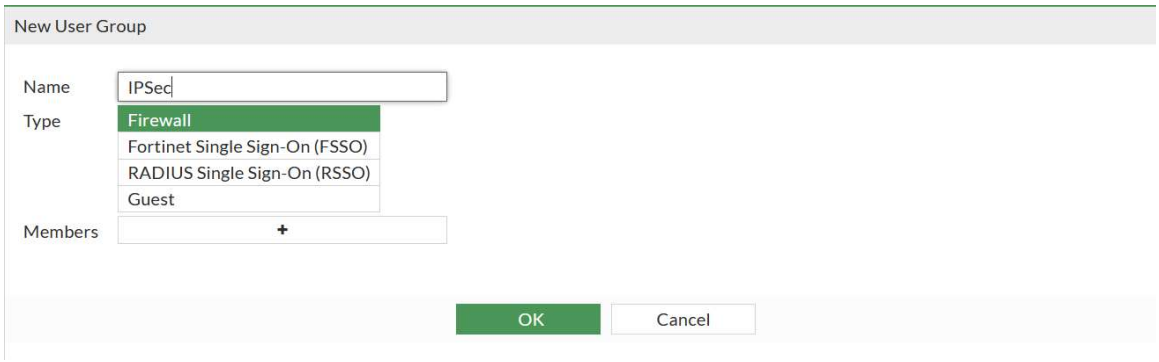
1: Go to User & Authentication > User Definition. Select Local User, next.



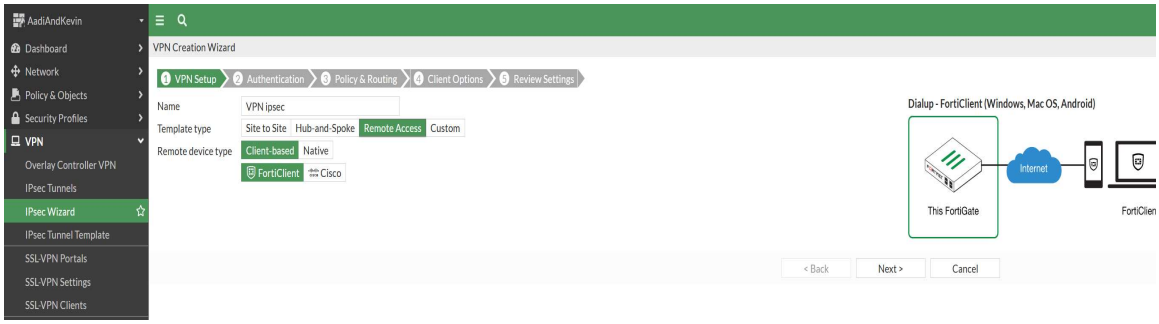
2: Enter a username and password, next.



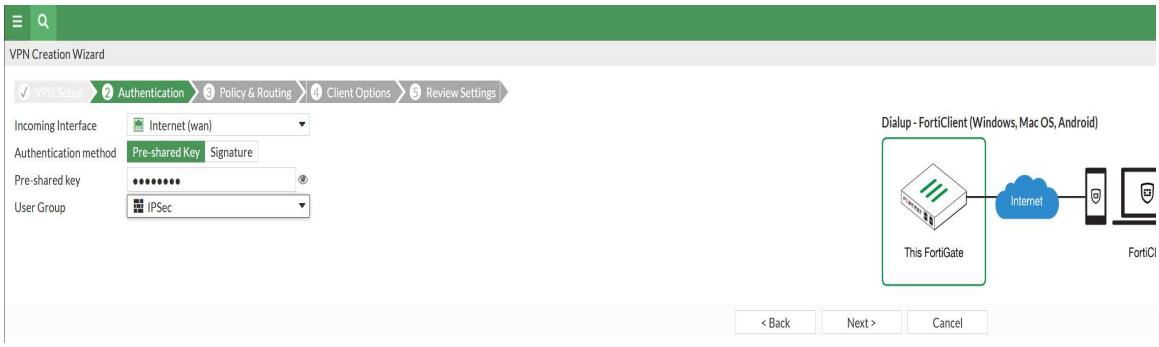
3: Add a User Group



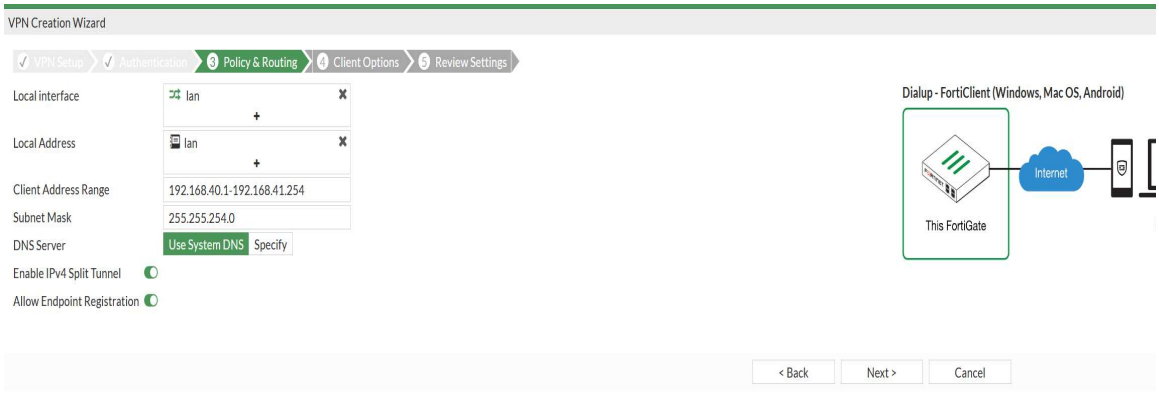
4: Create a new User Group and set the Type to Firewall



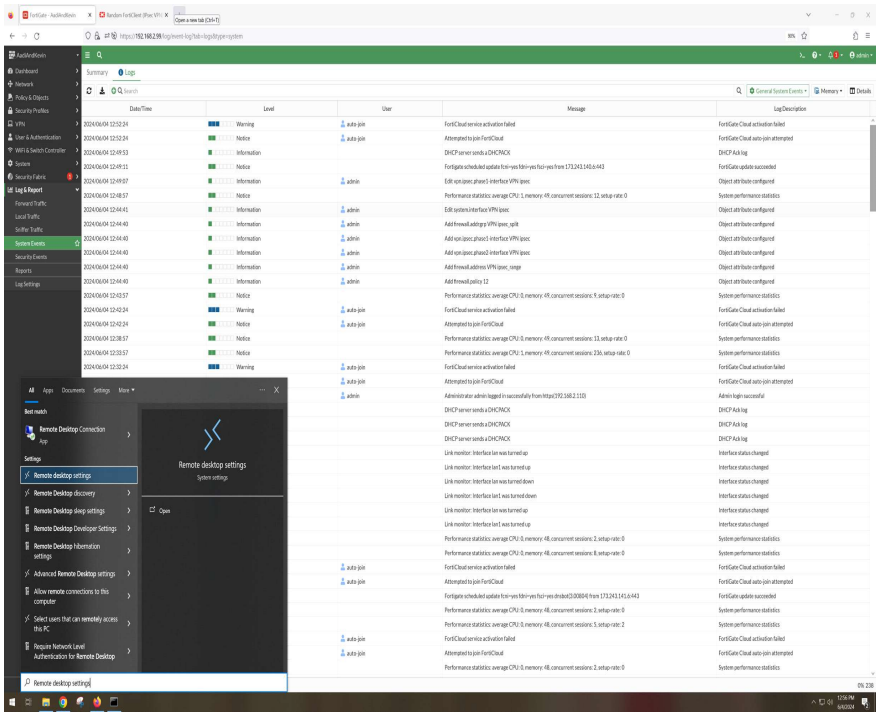
5: Go to IPSec Wizard and add a Name, set Template type to Remote Access. Remote device type should be Client-Based and FortiClient.



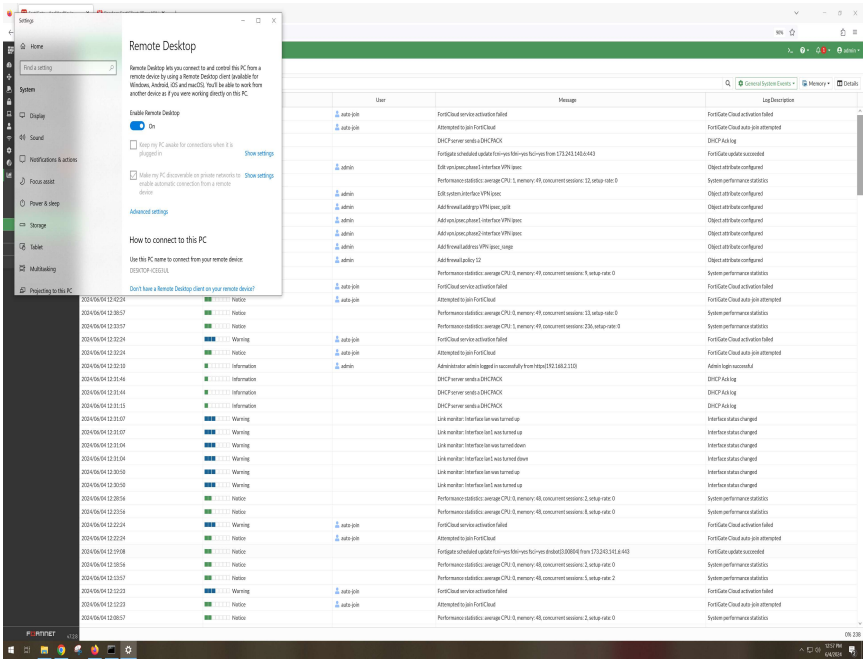
6: Set the Incoming interface to use the WAN port and set a pre-shared key. Select your User Group.



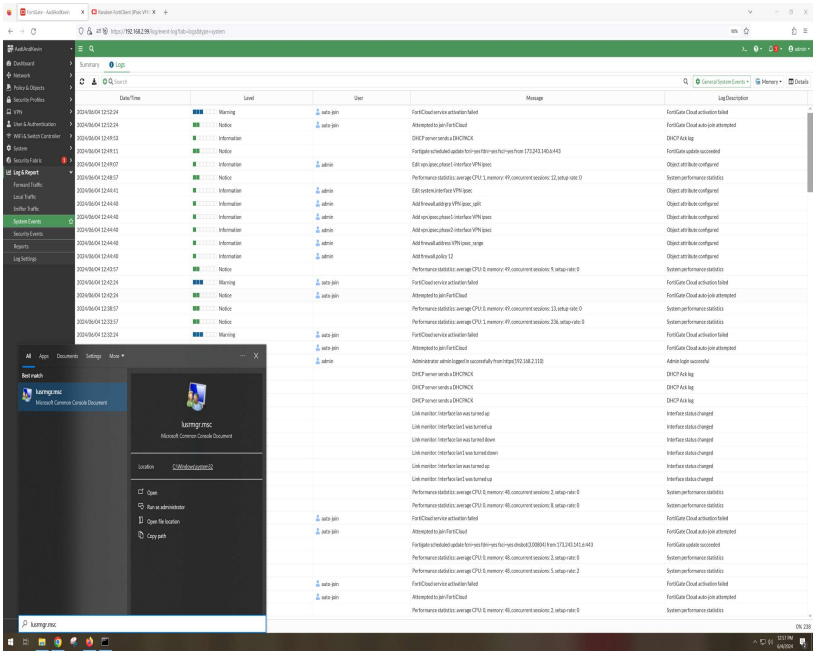
7: Set your Local interface to LAN and local address do use LAN as well. Client Address should be a range of what your remote PC should be. (Our WAN is another private network with addresses ranging between 192.168.40.1-192.168.41.254). Set the other settings as seen above.



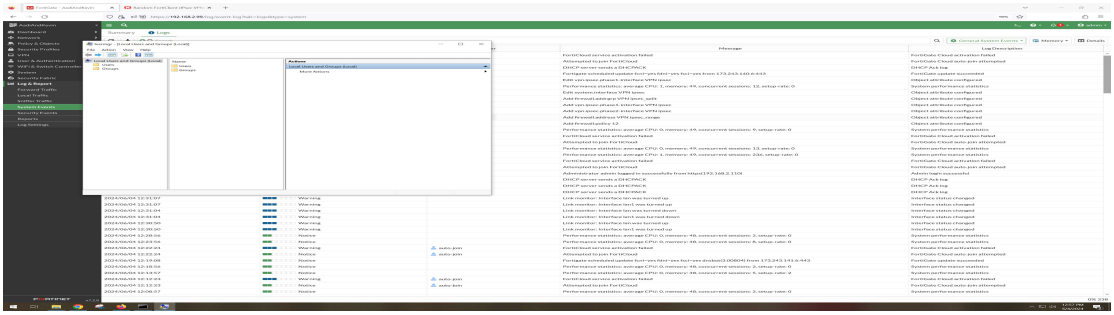
8: Go to remote Desktop Settings.



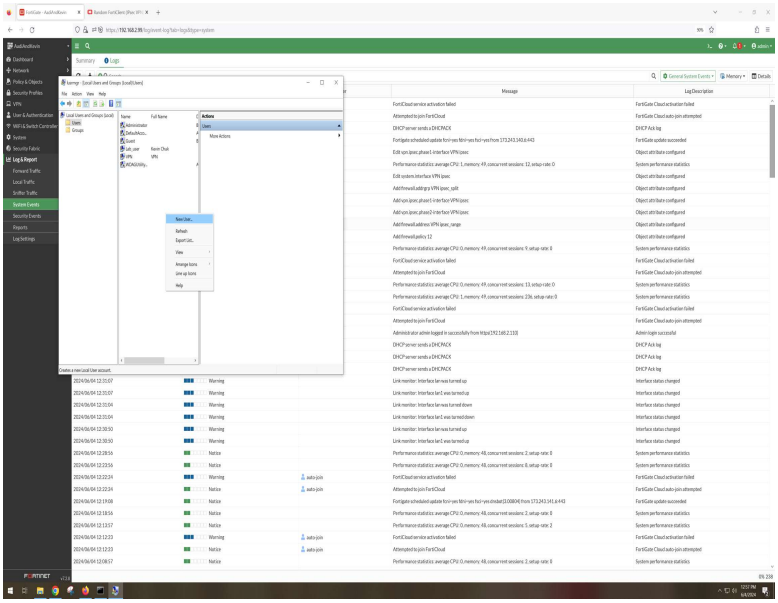
9: Enable Remote Desktop.



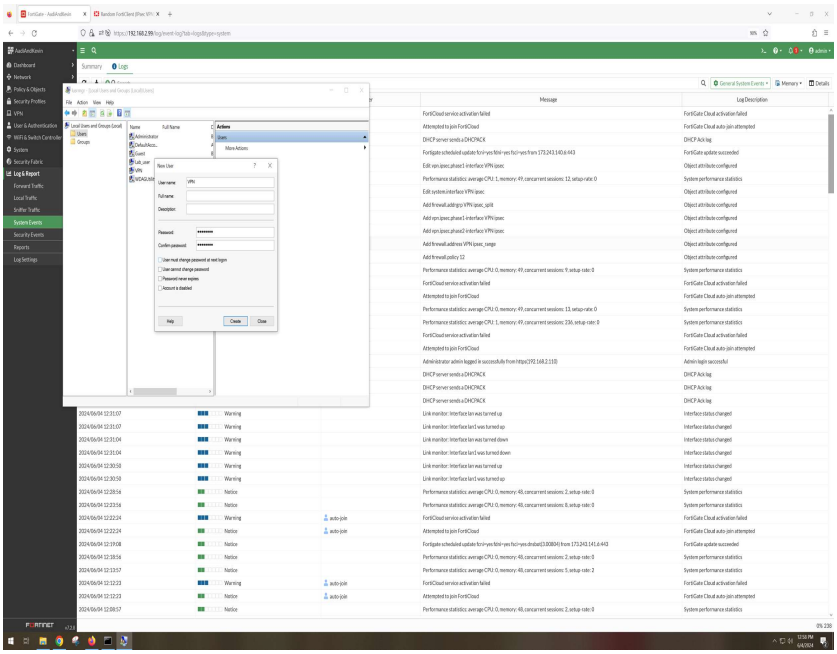
10: go to lusmgr.msc



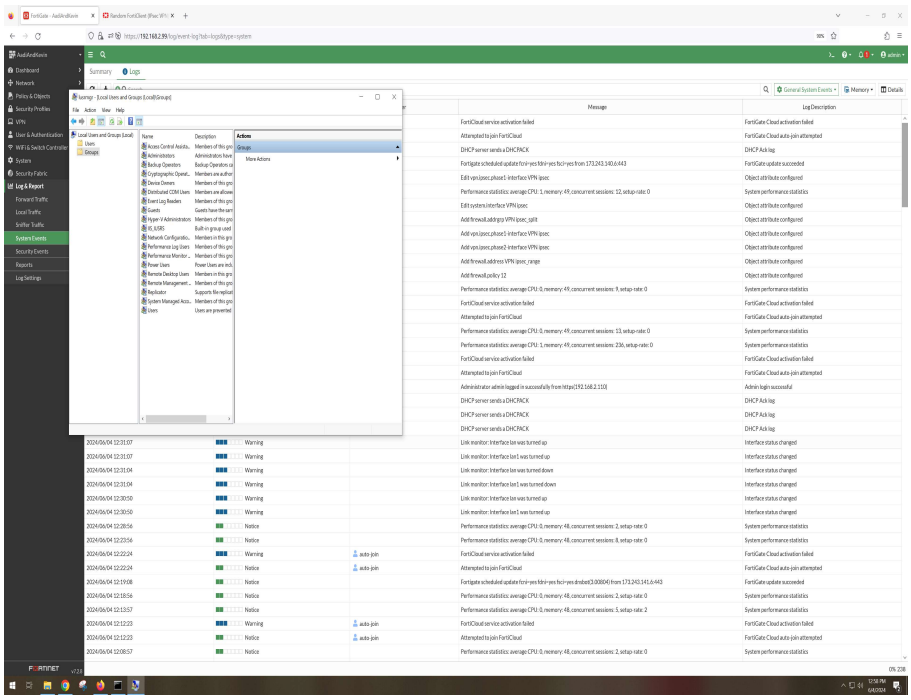
11: go to local user and groups > users



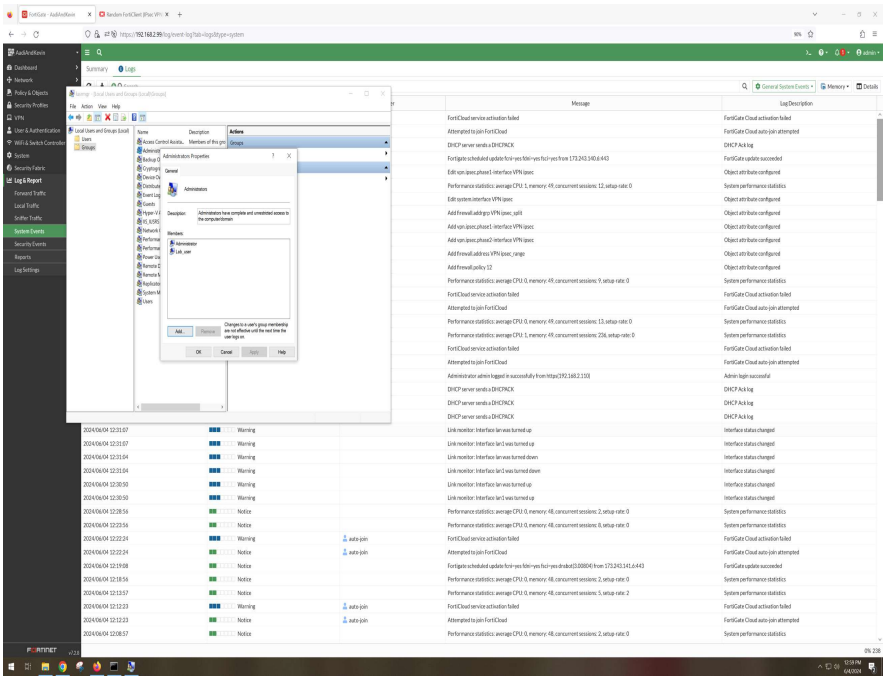
12: Right Click and click New User.



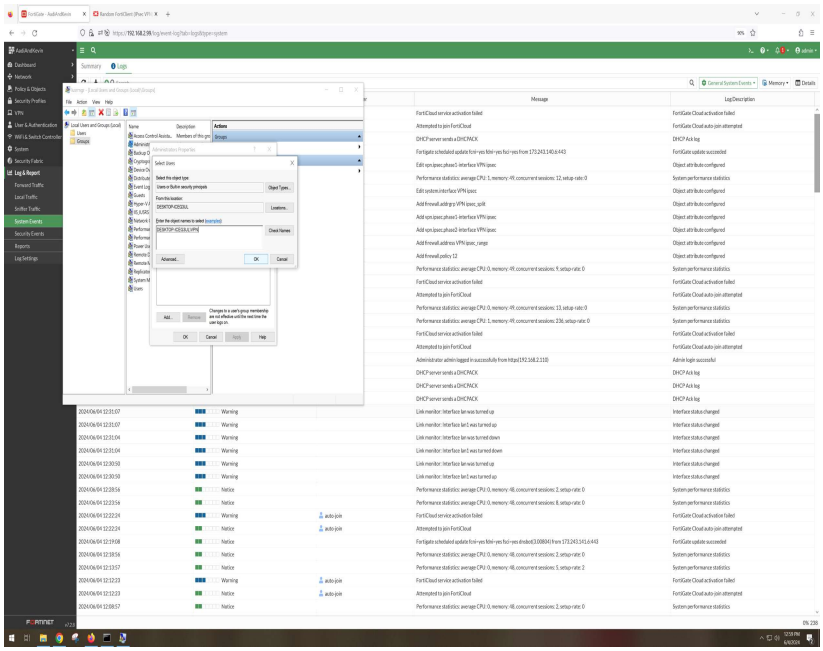
13: Create a New User with a username and password. Create.



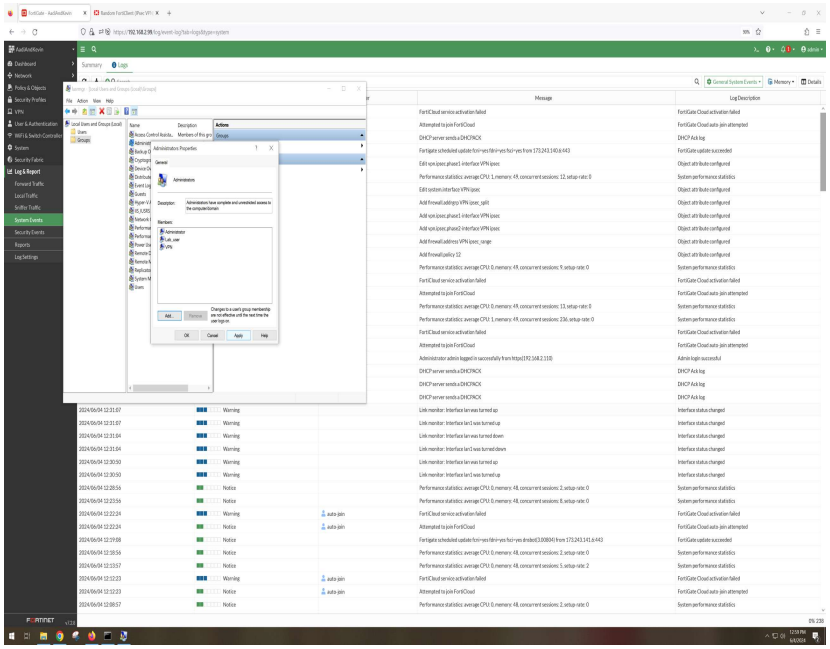
14: Go to Groups > Administrators.



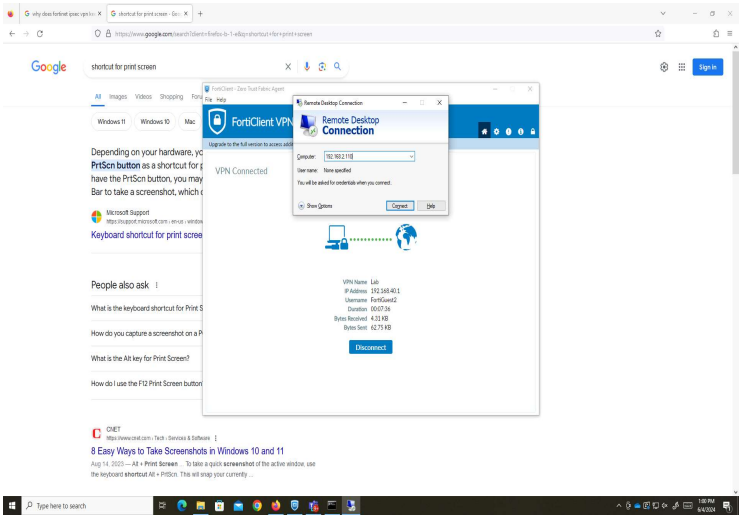
15: Click add.



16: Add the user with your desktop name\username



17: Apply.

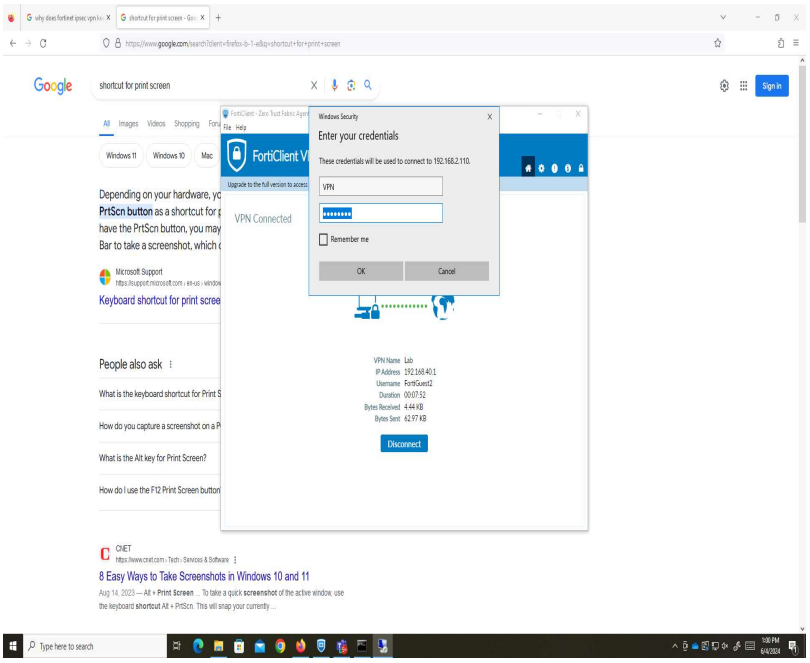


18: On the remote PC, download (https://www.fortinet.com/support/product-

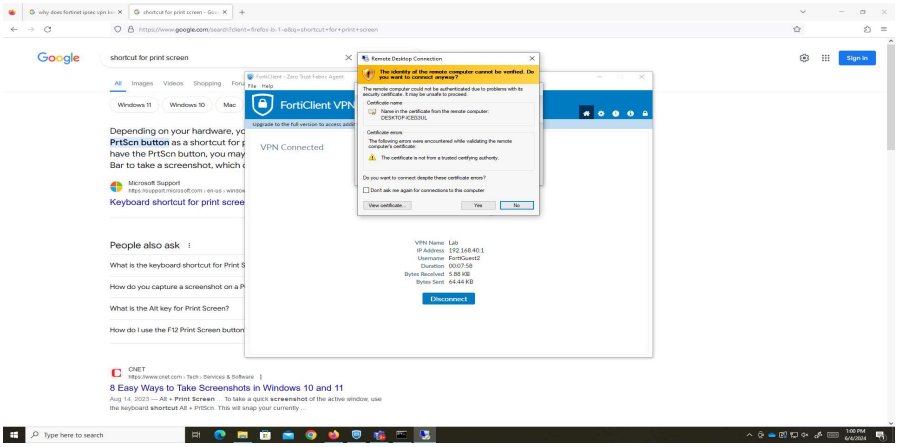
downloads) and use the FortiClient to connect to the network of your Firewall.

*Make sure you download the correct VPN version of the FortiClient

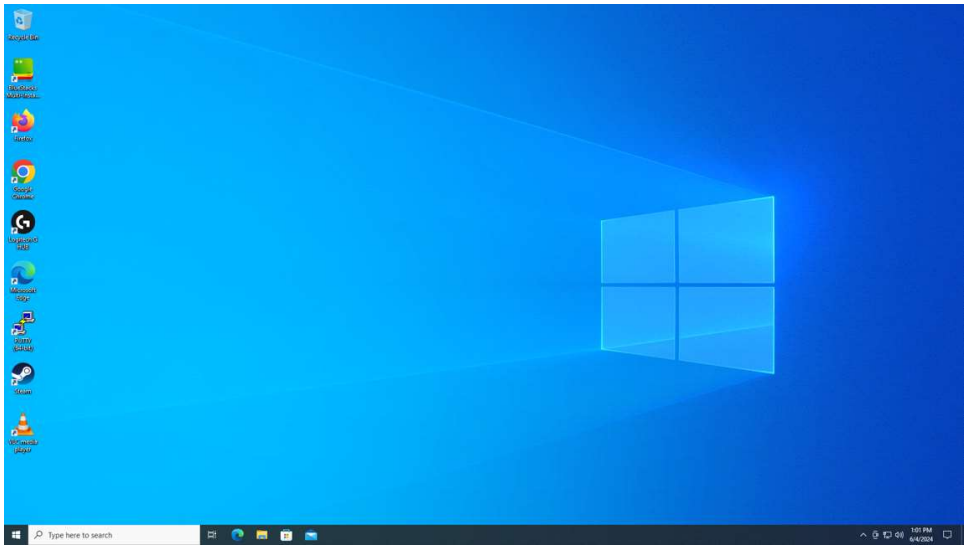
19: Open the Remote Desktop Connection application and enter the IP address of your on-premise PC.



20: Enter your local user login credentials.



21: Click YES.



22: You have now remotely connected to your on-premise PC using IPSec.

Issues:

The first issue we faced on this IPSec lab was that we downloaded the wrong FortiClient that was unable to be used with our IPSec tunnel. Simple fix, download the right client.

The second issue was that after 20 seconds the connection will time out and terminate. Looking through the settings of the firewall we found a dead-peer setting which we turn off. This, however, did not fix the issue because the FortiClient also had a dead-peer setting. After turning both settings off, we were able to hold a tunnel connection for more than 20 seconds.

Conclusion:

This lab was more difficult than the SSL one that proceeded it; however, it was still a walk in the park because of how user friendly FortiOS is. These two past labs taught me about the use cases of both IPSec and SSL VPN tunneling which both have use cases where one is better than the other. This is the last lab of the year for Cyber Security, and the class has taught me, over everything else, about the user friendliness of Fortinet Firewall OSs. If I were to ever buy commercial level equipment for use, I would likely go Fortinet over Palo Alto, and definitely over Cisco.