Introduction:

In this lab we created a remote access VPN that used Secure Socket Layer (SSL). This allowed for a computer to use a web browser to remote desktop into a computer on the on-premise network. The benefit of using SSL over something like IPSec is the ability to use a web browser to remote access instead of using a downloaded client.

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. SSL VPN in particular runs on the application layer of the OSI model which allows it to protect specific services or application.

SSL is a type of Internet encryption-based protocol developed to secure internet connections. Webpages that use SSL (or TLS which replaced SSL) has HTTPS in its URL instead of HTTP. SSL uses handshakes to initiate authentication between two devices to authenticate the devices are legitimate.

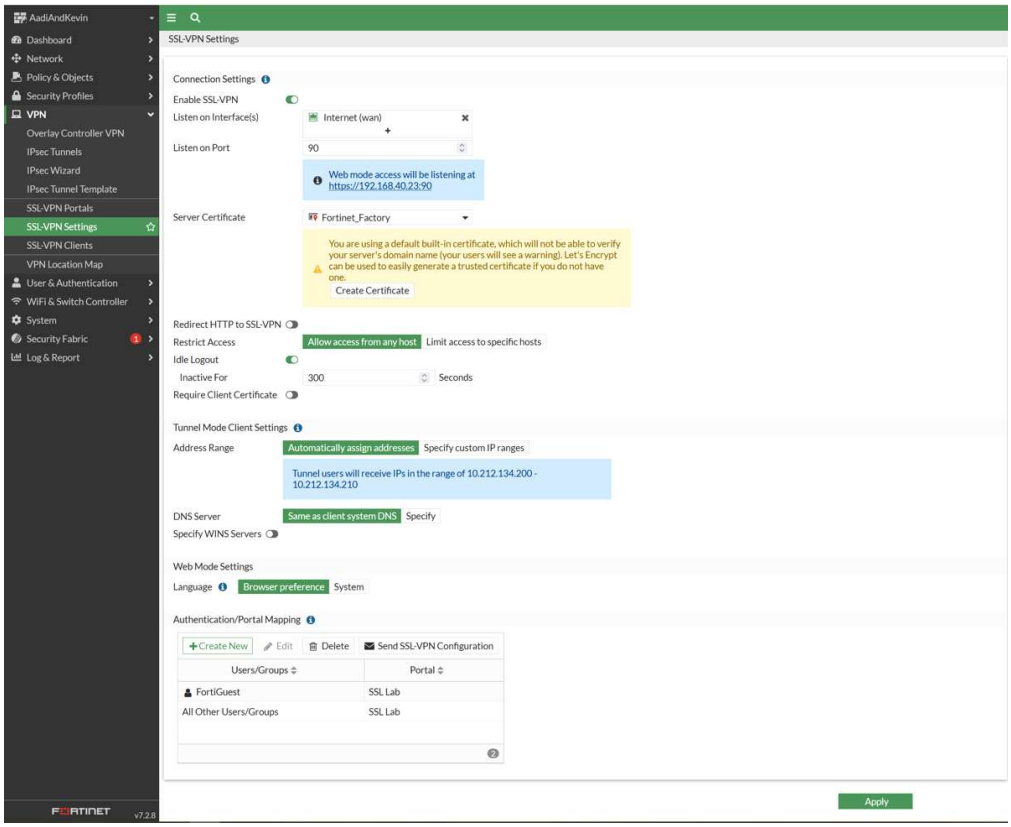
This lab uses SSL in tunnel mode which is a VPN that allows a web browser to securely access network devices via a SSL tunnel. This ensures that a user can remotely access applications or networks that are not normally accessible over the internet from across the world securely. This is great for remote workers that need to access resources from their company without being on site.

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:

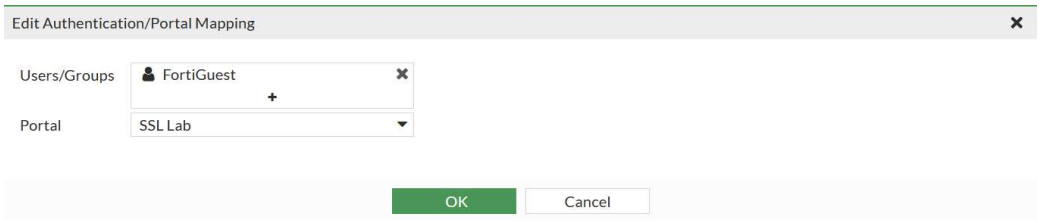
SSL is simple to set up with a FortiGate 40f firewall. It consists of 4 parts. First, edit the SSL-VPN settings to change the listening interface and port and create a new authentication user and portal mapping. Secondly, edit the VPN portal to enable tunnel mode with based off destination policy and to create a preset bookmark with the IP address of the internal, on-premise PC. Next, create 2 firewall policies, this is to allow traffic to pass through the firewall from the internal LAN to the SSL VPN tunnel. Lastly, enable remote Desktop on the on-premise PC in order be able to remote desktop into that PC.

Step-by-Step:

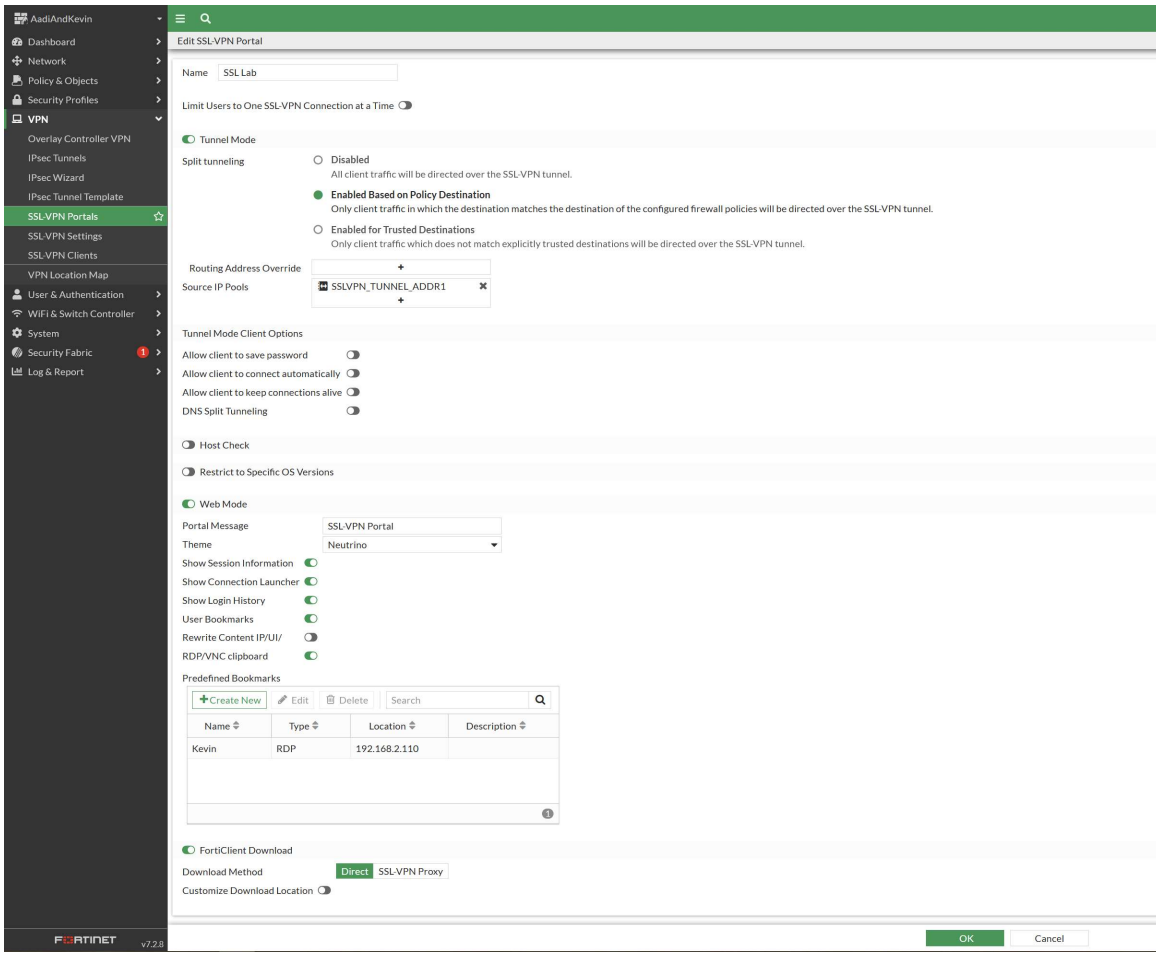


1: Go to SSL-VPN and configure the listen interface to be your outside WAN interface

We selected port 90 as it is a “dead” port



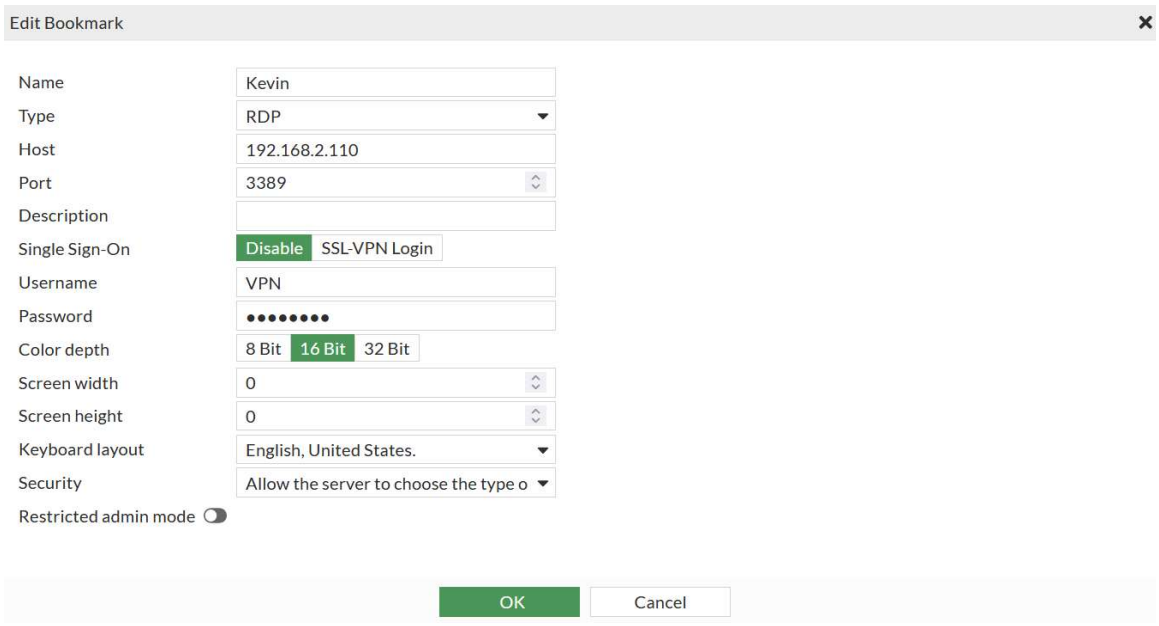
2: Create a user called, we called ours FortiGuest and set the portal to be tunnel-access, (called SSL lab here).



3: Go to SSL-VPN portal and enable tunnel mode with split tunneling as shown above.

Create a predefined bookmark of the PC in the network that will be RDPed into.

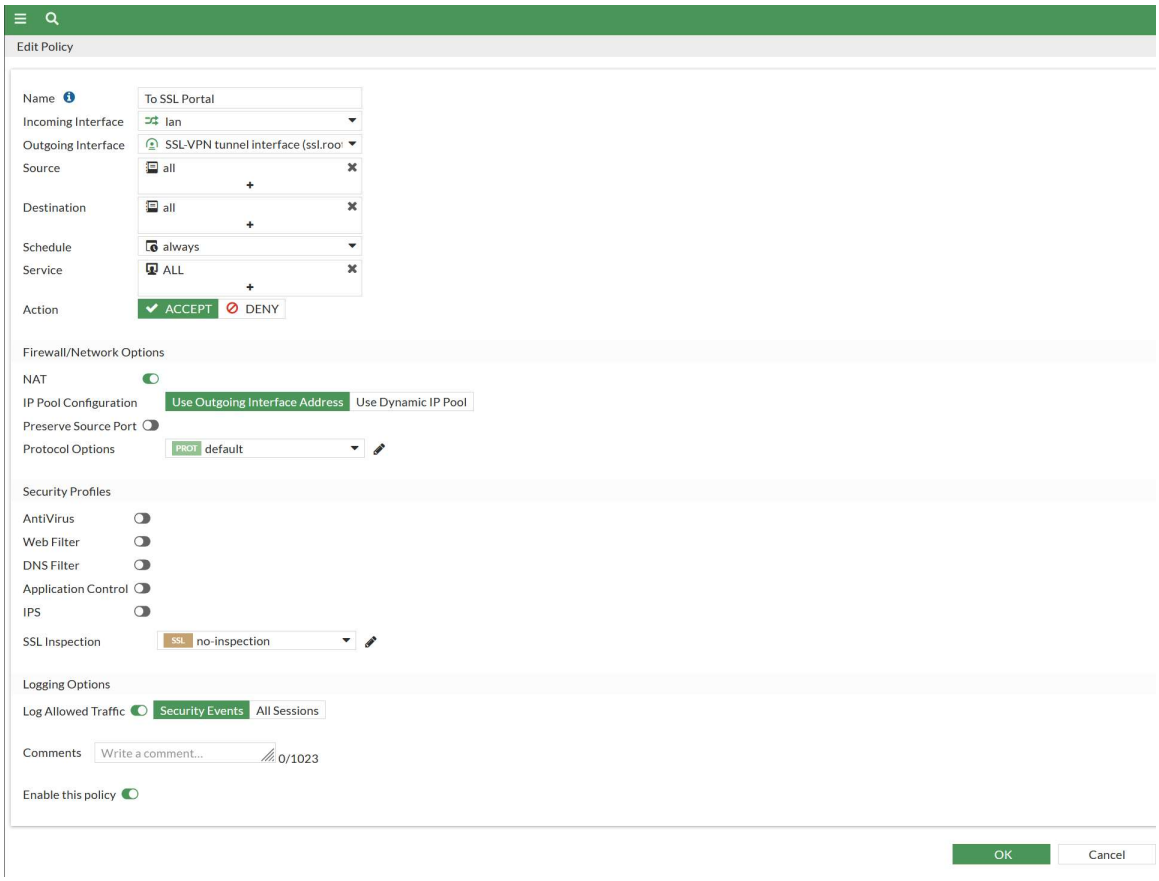
Ensure all your settings are the same as shown above.



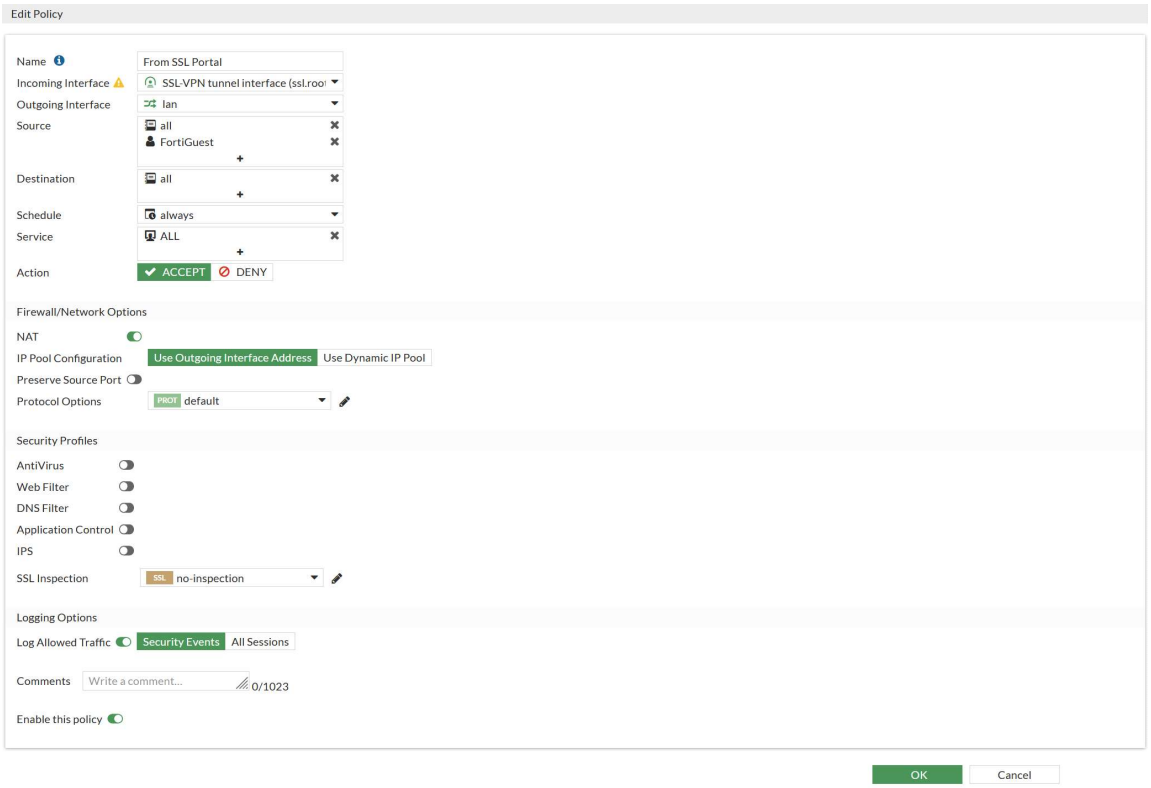
4: set the name and the type to RDP

Then set the host to be the IP of the on-premise PC

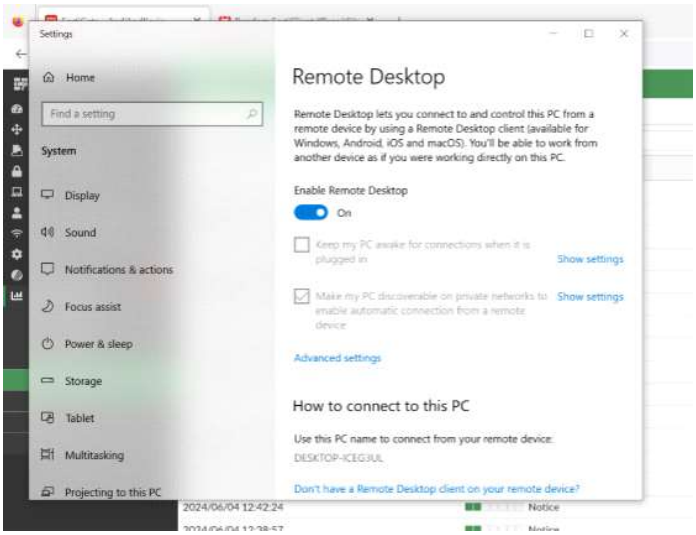
Finally create a username and password



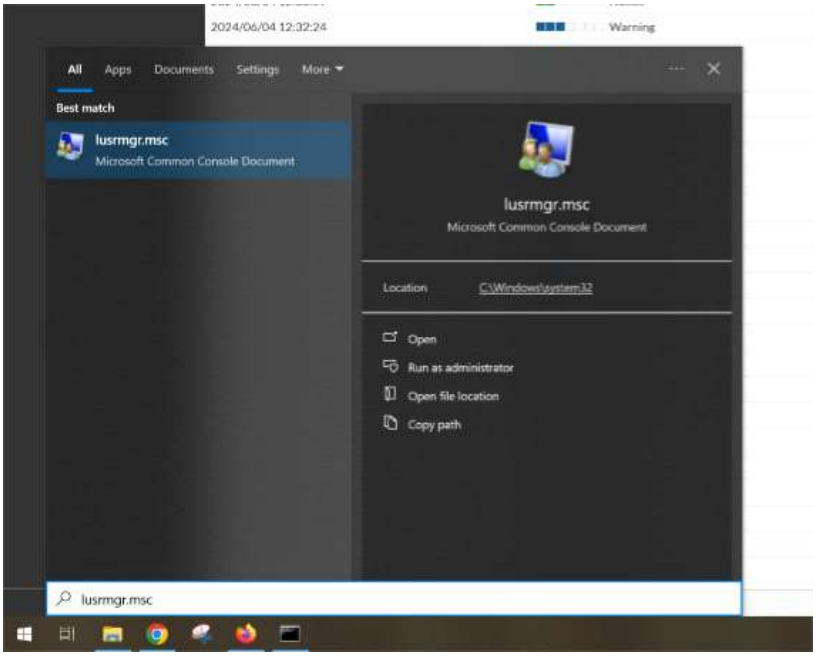
5: Edit the SSL firewall policy to as seen above, incoming should be lan and outgoing should be the SSL-VPN tunnel interface.



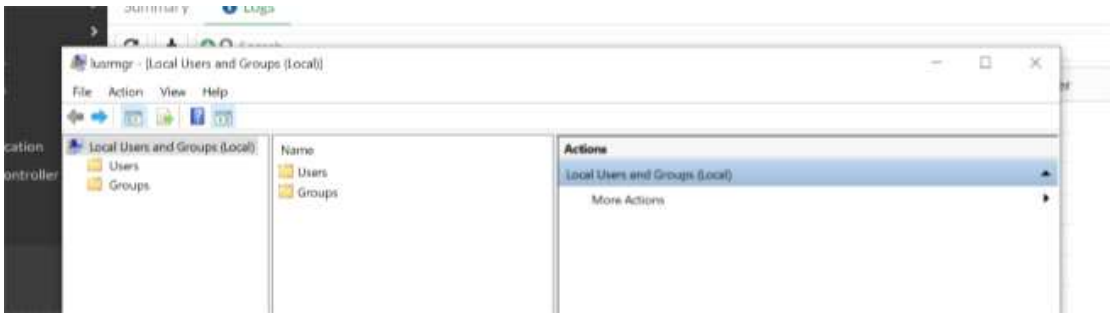
6: Create the other interface and with the reversed incoming and outgoing interfaces as shown above. Firewall policies are needed to allow both incoming and outgoing traffic.



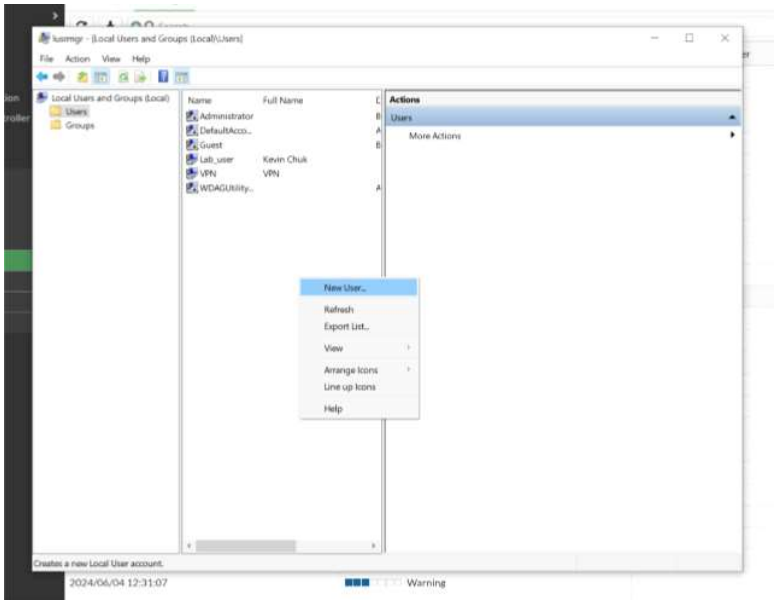
7: Enable Remote Desktop.



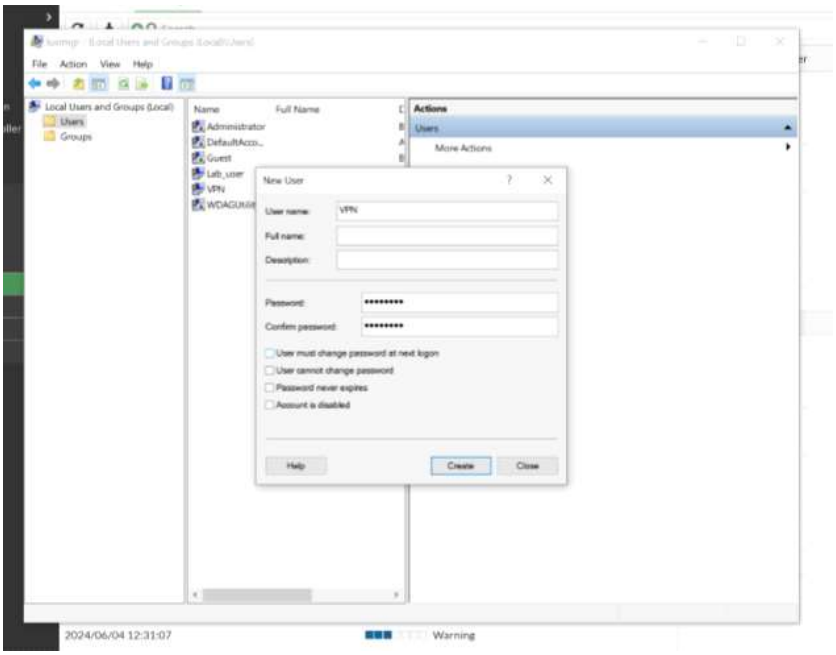
8: go to lusmgr.msc



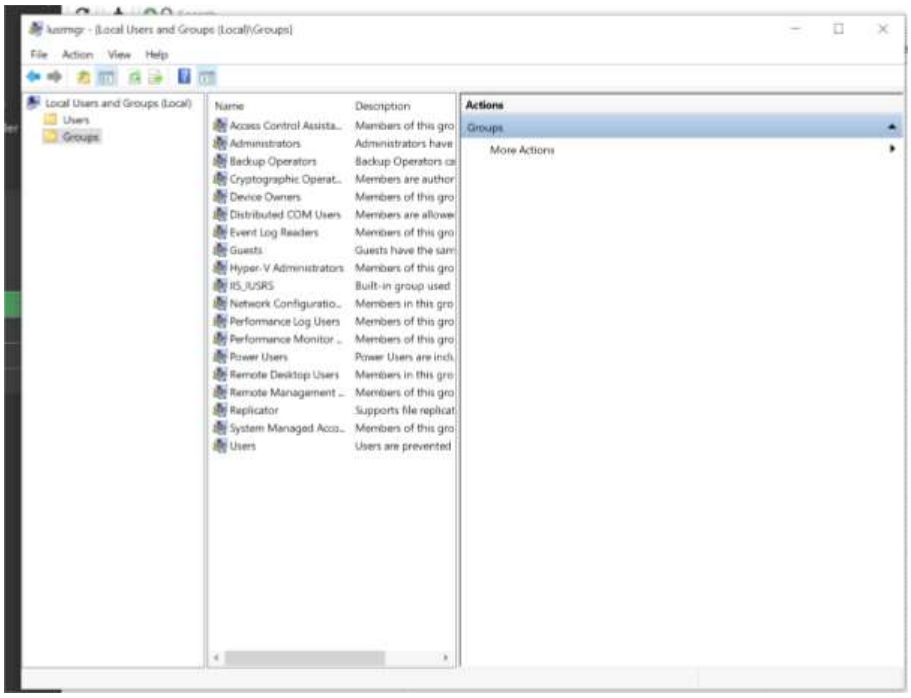
9: go to local user and groups > users



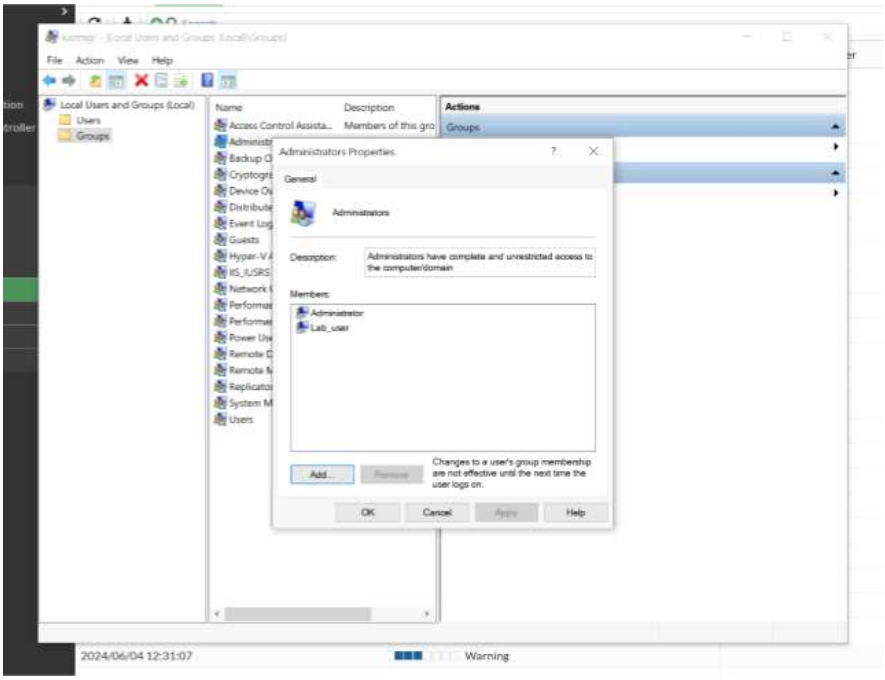
10: Right Click and click New User.



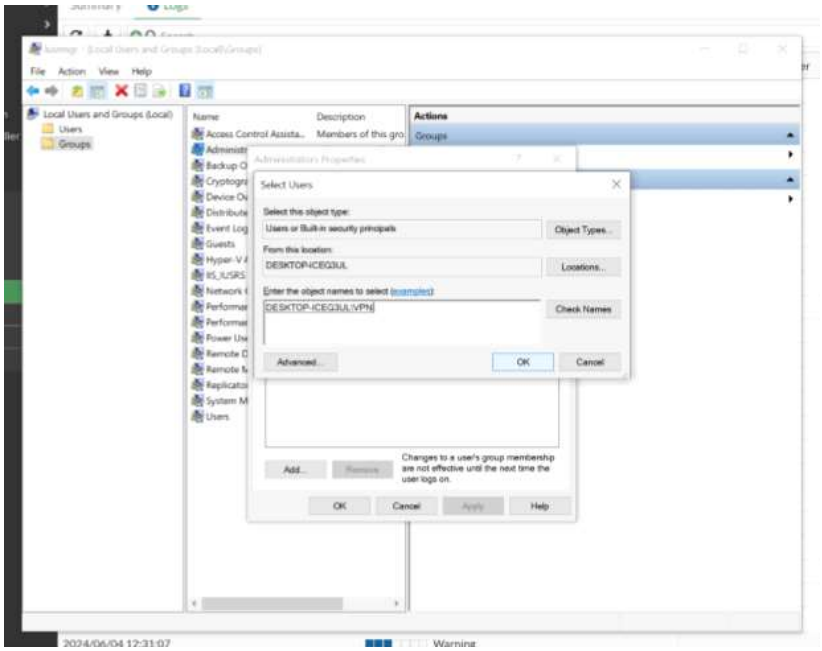
11: Create a New User with a username and password. Create.



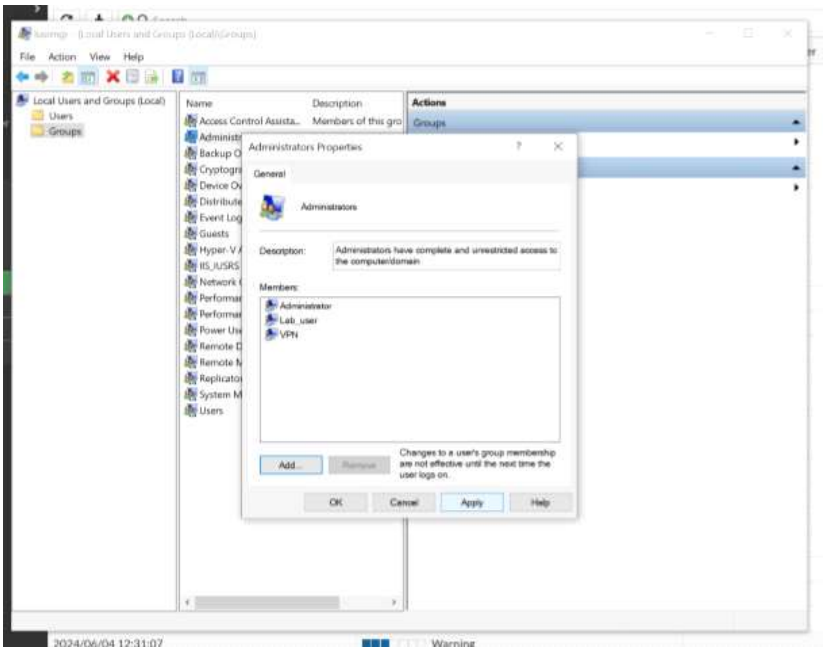
12: Go to Groups > Administrators.


File Action View Help
Local Users and Groups (Local)
Users
Groups
Name
Description
Actions
Groups
Administrators Properties
General
Administrators
Description:
Administrators have complete and unrestricted access to the computer/domain
Members:
Administrator
Lab_user
Add...
Remove
Changes to a user's group membership are not effective until the next time the user logs on.
OK
Cancel
Apply
Help
2024/06/04 12:31:07
Warning

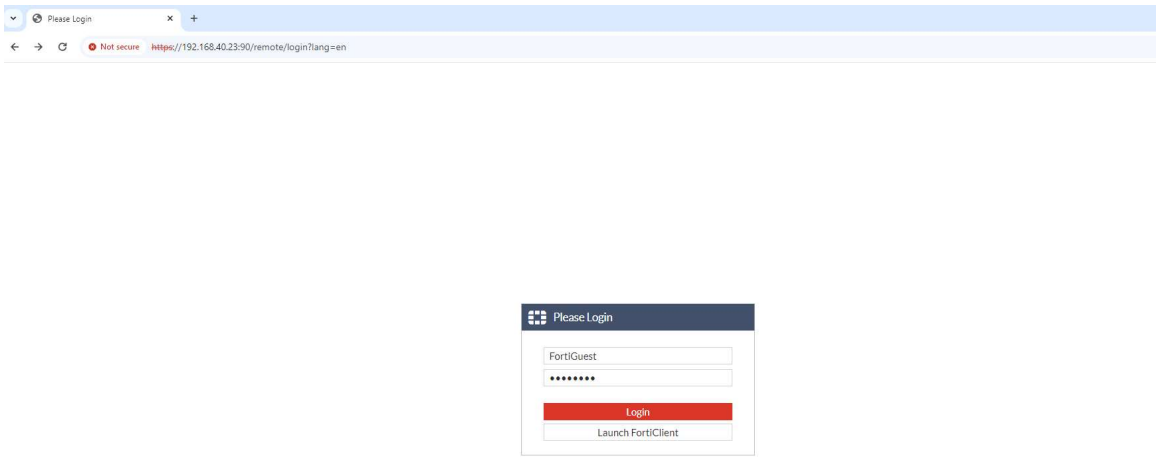
13: Click add.



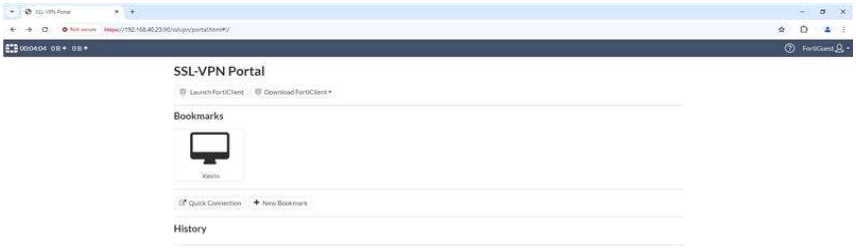
14: Add the user with your desktop name\username


File Action View Help
Local Users and Groups (Local)
Users
Groups
Name
Description
Access Control Assista...
Members of this gro
Actions
Groups
Administrators Properties
General
Administrators
Description:
Administrators have complete and unrestricted access to the computer/domain
Members:
Administrator
Lab_user
VPN
Add...
Remove
Changes to a user's group membership are not effective until the next time the user logs on.
OK
Cancel
Apply
Help
Guests
Users
Warning

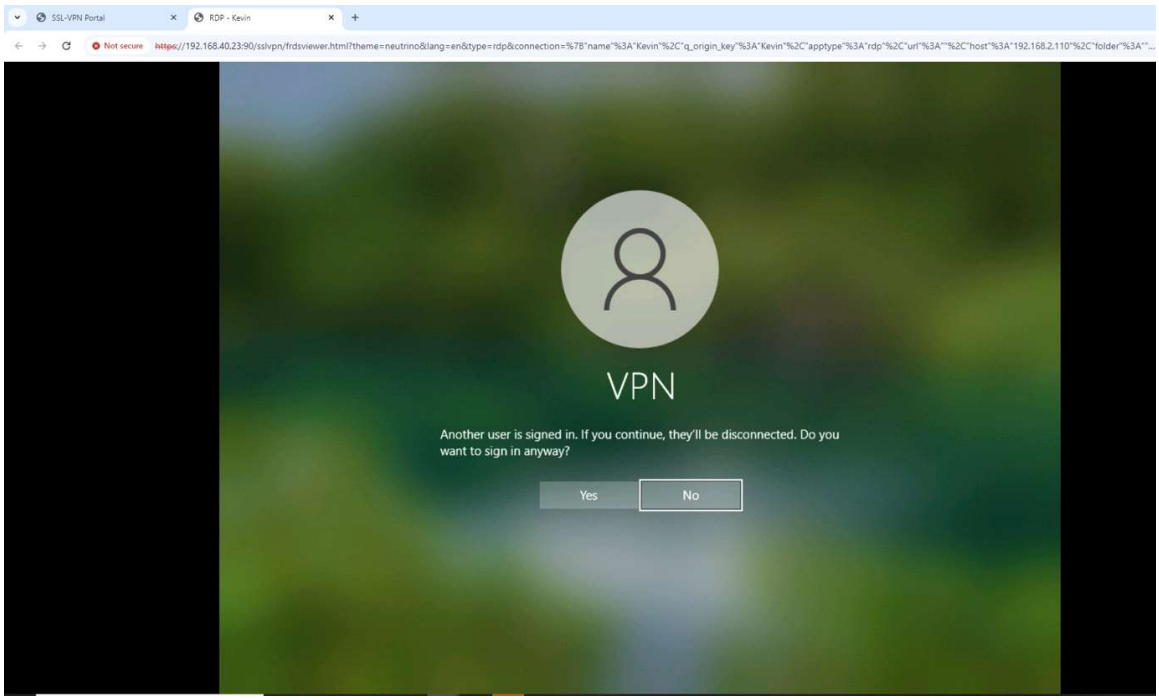
15: Apply.



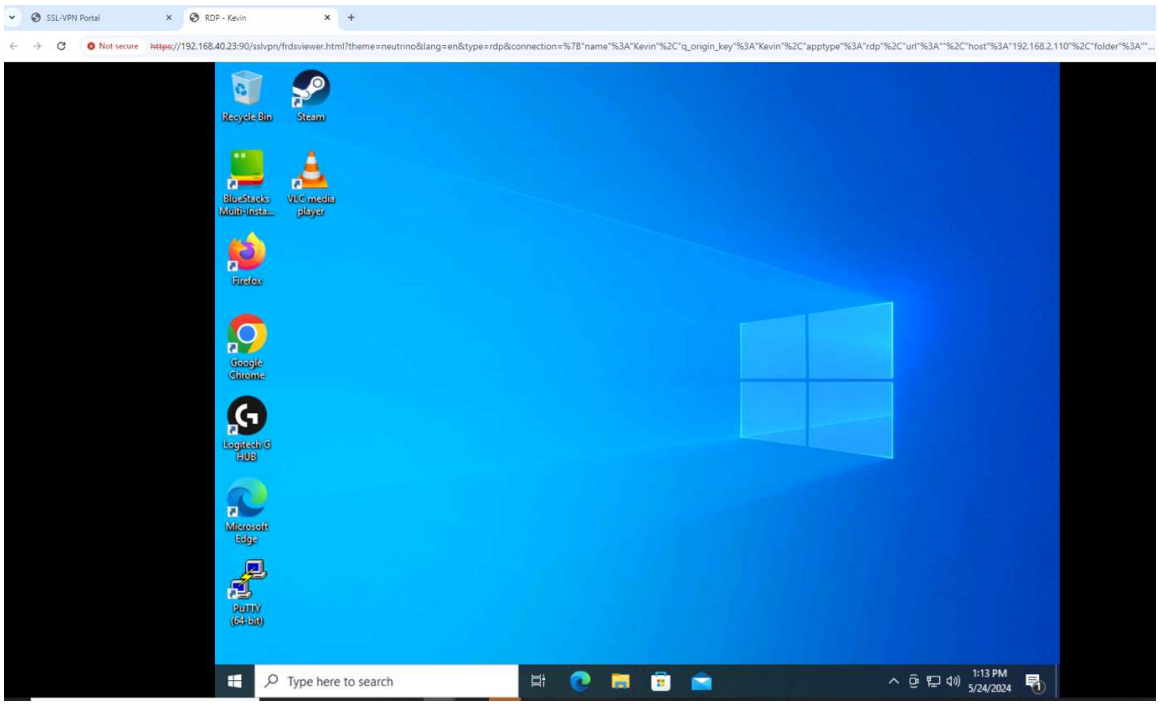
16: Go to the IP address of your router's WAN IP address and enter the username and password of the user you set in step 2.



17: Click on the bookmark you set during step 3.


SSL-VPN Portal
RDP - Kevin
Not secure
VPN
Another user is signed in. If you continue, they'll be disconnected. Do you want to sign in anyway?
Yes
No

18: Click Yes.



19: You're now remote desktop-ed into the on-premise PC.

Issues:

One issue we ran into was that the on-premise PC and the remote PC had different encryption protocols, the Remote Desktop Protocol (RDP) connection in the bookmark preset was different than the one on the Remote PC. This resulted in the tunnel connection termination right after creation. The way we fixed this was allowing the on-premise PC to decide the encryption method which would allow for the encryption protocols to sync up and establish a tunnel connection without termination.

Conclusion:

This lab was fairly simple, not requiring any downloads on the client side as SSL enables you to use a web browser to remote access into an on-premise PC. Though SSL is more simple to use compared to something like IPSec, it is less secure as it features fewer levels of security compared to IPSec. It is still a useful tool for many users and companies due to its ease of setup and use.