Portfolio of labs in Cybersecurity

A collection of labs done within CISCO cybersecurity course using Palo Alto PA-220 and Fortigate-40F firewalls.

Jeffrey Yiu Cheung

Contents

Palo-Alto Pa-220

Factory resetting a Palo Alto firewalls

Palo Alto
PA-220 Enterprise
Hardware + Lizenz

Jeffrey Yiu Cheung

Purpose

This lab helps us understand the steps necessary to perform a factory reset on a Palo Alto Pa-220 firewall.

Background information

A factory reset is a function that erases and resets all configuration to original factory settings. When encountering a device that is already pre-configured, a factory reset allows us to still use a device that is already set with a password and start from a clean environment.

Palo Alto is a networking company that offers cybersecurity with products like firewalls and cloud-based applications. It was founded in 2005 and has been the leader in cybersecurity research around the globe for 11th straight years. With cybersecurity threats constantly emerging and improving, the need for cybersecurity is growing by day. ‘

With new technologies constantly enabling the ease of interaction with the web, more information is being uploaded every second. There is useless information, educational information, but there are also sensitive, personal information in the web. To prevent these cybersecurity threats, Palo Alto offers cybersecurity devices and programs like firewalls malware prevention programs.

The Palo Alto Pa-220 is a small firewall device designed to support small organizations and offices with many features that optimize networking and security. It is able to mitigate many threats by having the ability to identify unknown malware and automatically generate protection upon analyzing the behavior, and having many functions that blocks known threats. The raise in Cyber Attacks have become more common and sophisticated, it is important to have protection against these threats. The Palo Alto device has a throughput of up to 500 Mbps, requires 50-60Hz voltage, and is about 3 pounds of weight. It can support up to 64,000 firewall sessions.

Lab summary

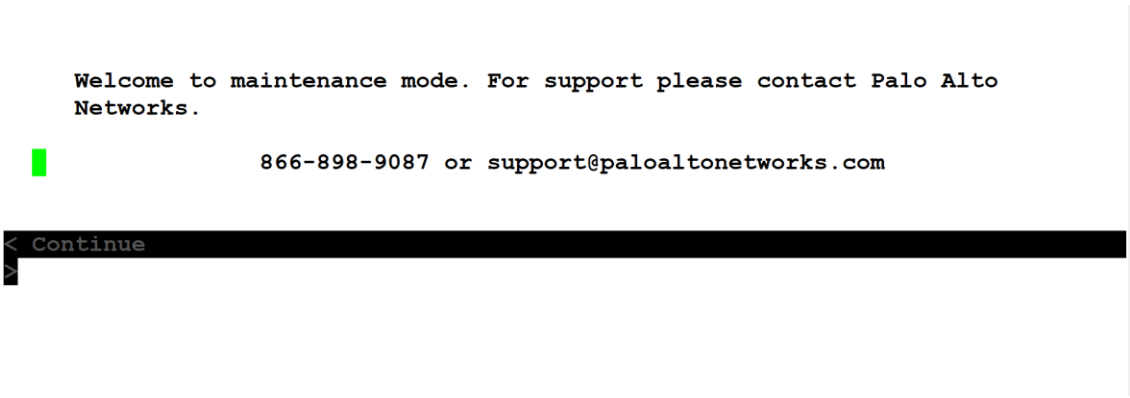
Connect the console cable between the Palo Alto Pa-220 and the host computer to begin. To enter the “Maint” mode, we power cycled our device. After the reboot, this should be what it

looks like:

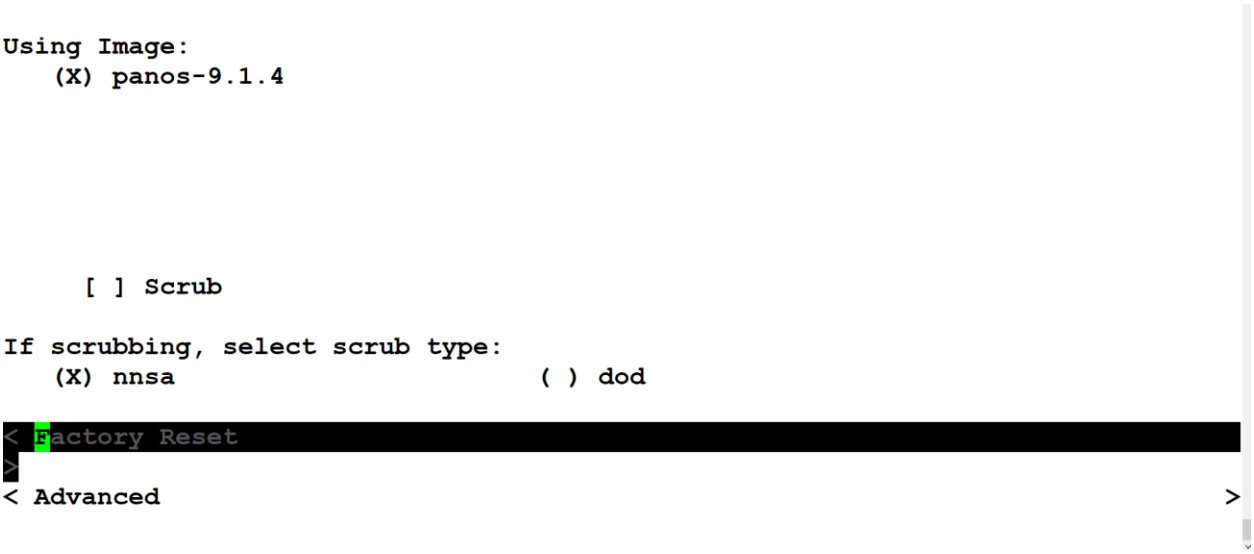
```
DRAM: 8 GiB
Clearing DRAM..... done
Octeon MMC/SD0: 0
Using default environment

MMC:   Octeon MMC/SD0: 0, Octeon MMC/SD0: 0
Net:   octeth0, octeth1, octeth2, octeth3, octeth4, octeth5, octeth6, octeth7,
octrgmii0 [PRIME]
Type the command 'usb start' to scan for USB storage devices.



        Autoboot to default partition in 5 seconds.
        Enter 'maint' to boot to maint partition.

Entry: maint

Booting to maint mode.
```

There is a short time frame when you have to type “maint” to get to the maintenance mode, where there is an option for factory reset.

This should be what it looks like after successfully entering maintenance mode:

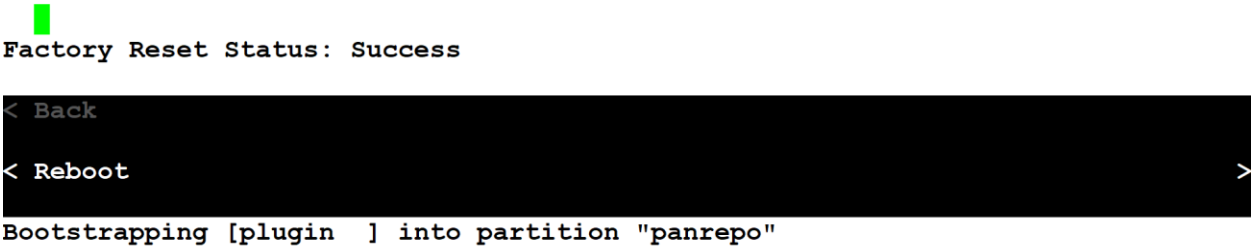


Upon selecting Factory Reset, another menu comes up. Continue with the factory reset by selecting factory reset:



After you continue to factory reset, it should show a progress bar. Now all we have to do is wait.

When it is done the option to reboot is available. After the reboot the device is clean and can be configured.



Problems

This lab was straightforward and did not have many issues, however, it did come at a risk of completely destroying the Palo Alto device, and one should always be careful when choosing options in the maintenance menu. Another problem was that this process is very time consuming, taking about 20 to 30 minutes to complete a reboot.

Conclusion

This lab is straightforward but also necessary. The factory reset function will come up many times, besides cybersecurity. The steps to perform a factory reset on a Palo Alto Pa-22, you first reboot the firewall, enter maintenance mode, select factory reset twice, then wait. After the wait is over, reboot to find a clean device.

Palo-Alto PA-220

Setting a PA-220 as a SOHO router

Palo Alto
PA-220 Enterprise
Hardware + Lizenz

Jeffrey Yiu Cheung

Purpose

This lab teaches a way to set up the Palo-Alto PA220 as a SOHO router for small offices and business.

Background information

SOHO router, aka Small Office/Home Office router is designed to support small businesses or small offices, which is a perfect for the Palo Alto PA220 firewall's specifications. They are stronger than home routers, but weaker than enterprise routers. They are designed to have functions like firewall, VPN, security features tailored for needs of a small office, and great performance under load. They are usually the only point of entry and exit in a network, which makes features like security a necessity.

In the modern age, most modern offices are in large buildings requiring bigger networks, however, small office/home office routers can still benefit many, such as professions like lawyers, consultants, writers, IT workers, etc. Enterprise routers are designed to support bigger networks, redundancy, and scalability.

Palo Alto is a networking company that offers cybersecurity with products like firewalls and cloud-based applications. It was founded in 2005 and has been the leader in cybersecurity research around the globe for the 11th straight year. With cybersecurity threats constantly emerging and improving, the need for cybersecurity is growing by day.

With new technologies constantly enabling the ease of interaction with the web, more information is being uploaded every second. There is useless information, educational information, but there are also sensitive, personal information in the web. To prevent these cybersecurity threats, Palo Alto offers cybersecurity devices and programs like firewalls malware prevention programs.

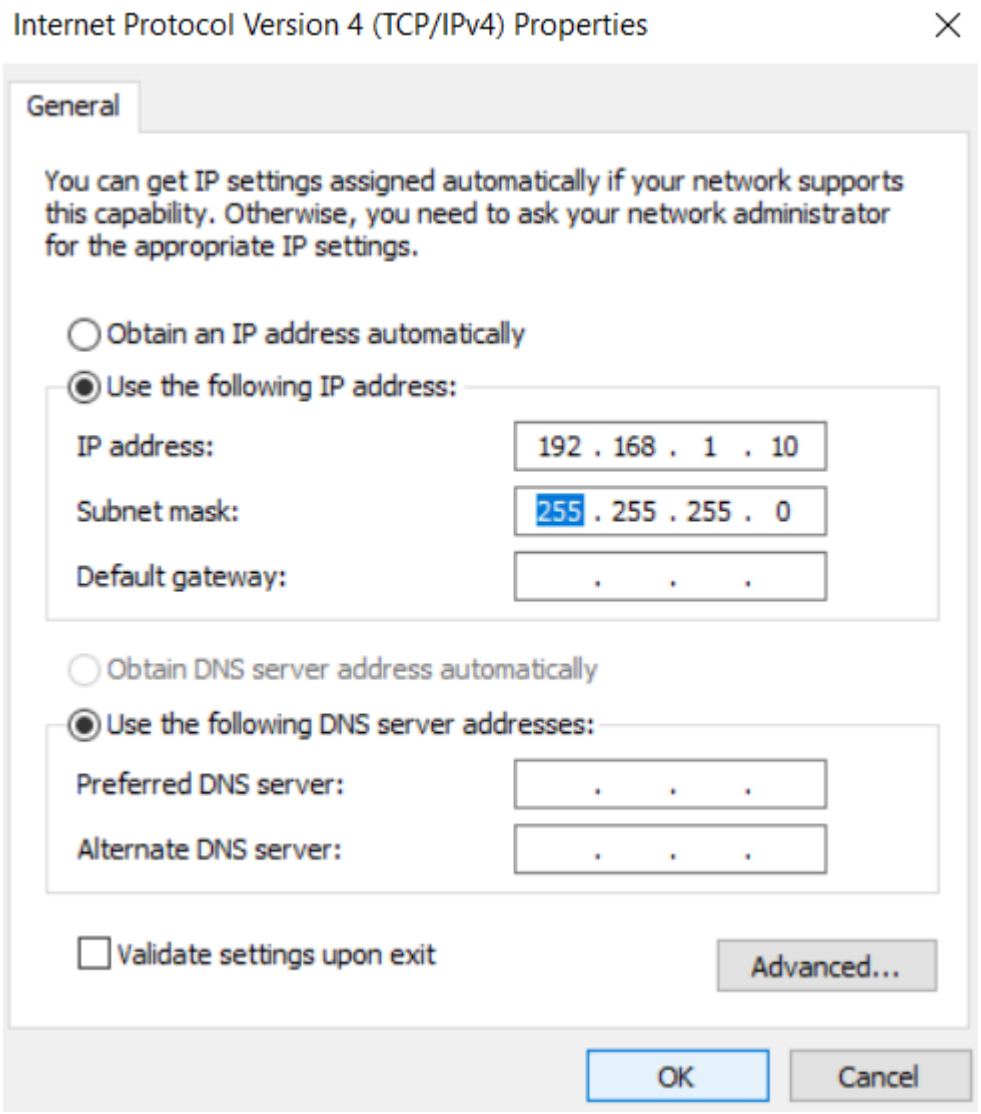
The Palo Alto Pa-220 is a small firewall device designed to support small organizations and offices with many features that optimize networking and security. It is able to mitigate many threats by having the ability to identify unknown malware and automatically generate protection upon analyzing the behavior and having many functions that blocks known threats. The raise in cyber-attacks have become more common and sophisticated, it is important to have protection against these threats. The Palo Alto device has a throughput of up to 500 Mbps, requires 50-60Hz voltage, and is about 3 pounds of weight. It can support up to 64,000 firewall sessions.

Lab summary

First, connect your computer to the management port of the Palo Alto 220.

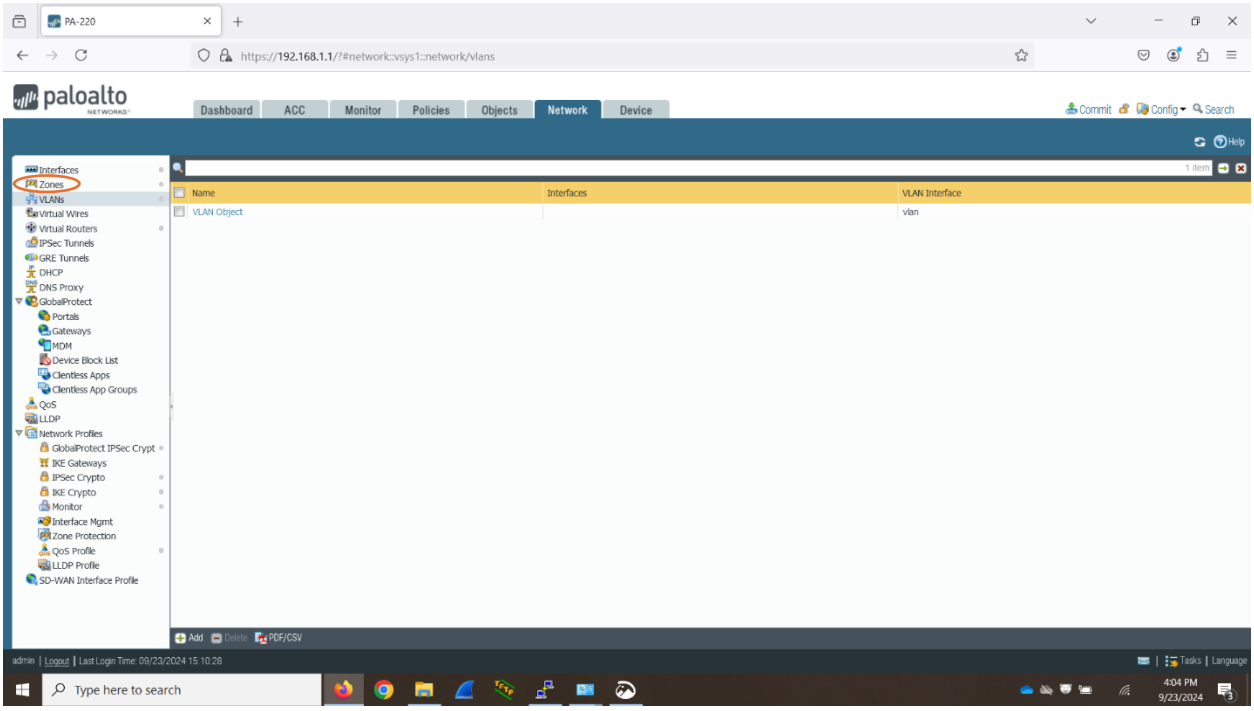
Then, with a console connection and via Putty, commit the change of setting the IP address to 192.168.1.1 with a subnet mask of 255.255.255.0. and commit the change.

Then, configure a static address on your computer's Ethernet port, (e.g. 192.168.1.10) with the netmask 255.255.255.0 in control panel (a default gateway is not required).

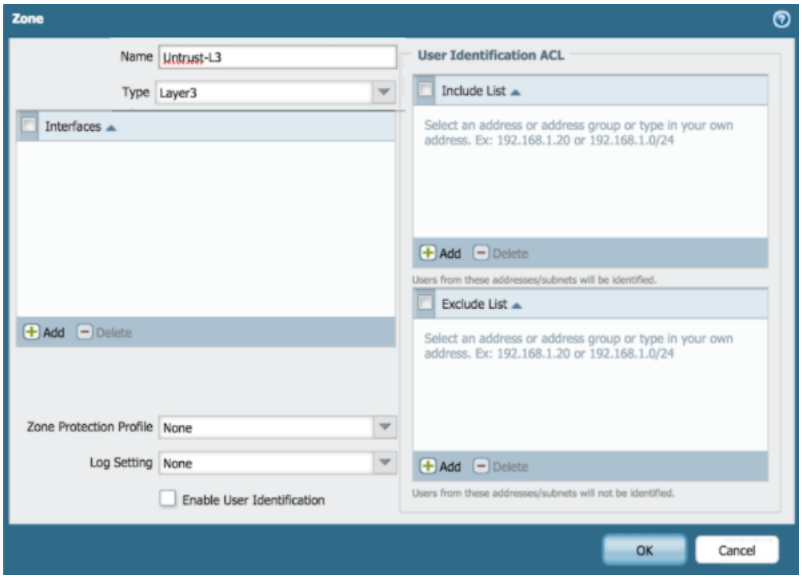


Then, login via a web browser by typing https://192.168.1.1 as URL, and log in with the username and password that you configured (e.g. username: admin, password: CiscoClass1)

Next, create 3 security zones by navigating to Network to Zones, and click add.



The first zone with the name Untrust-L3, and the type as layer 3

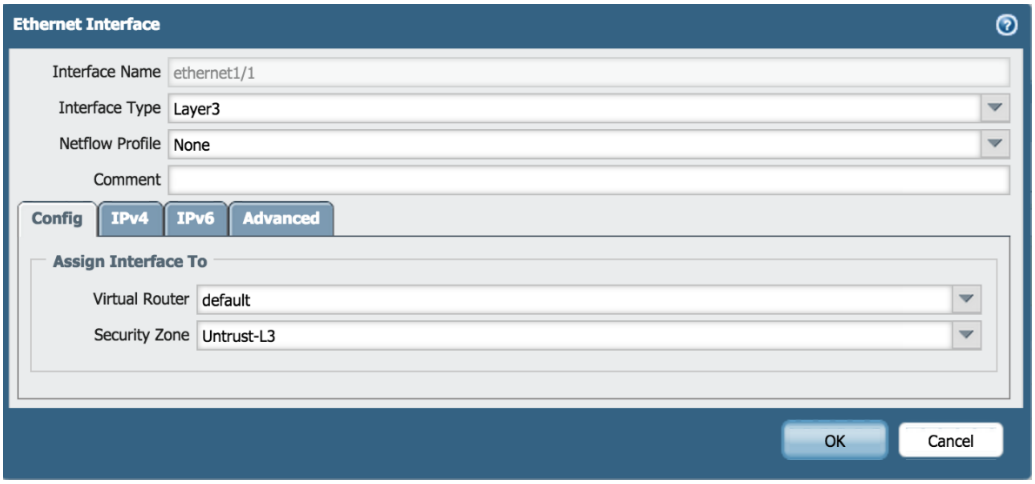


The second zone, with the name Trust-L3, and the type Layer3

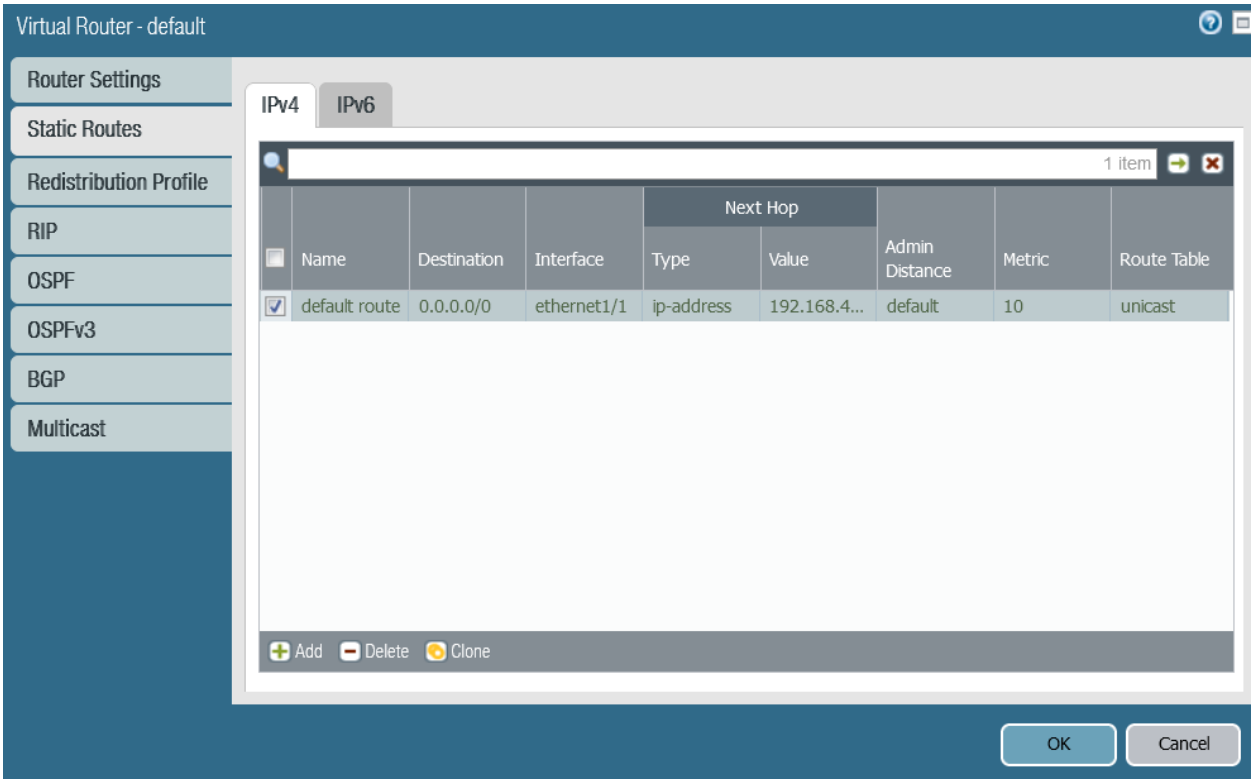
The third zone, with the name Trust-L2, and the type Layer2

Next, configure the interfaces through Network then Interfaces tab.

Configure Ethernet1/1 Interface type to Layer3, set Virtual Router to default, and set the security zone to Untrust-L3. Under the IPv4 tab, set the type as DHCP client and tick on the options for Enable and Automatically creating default route.



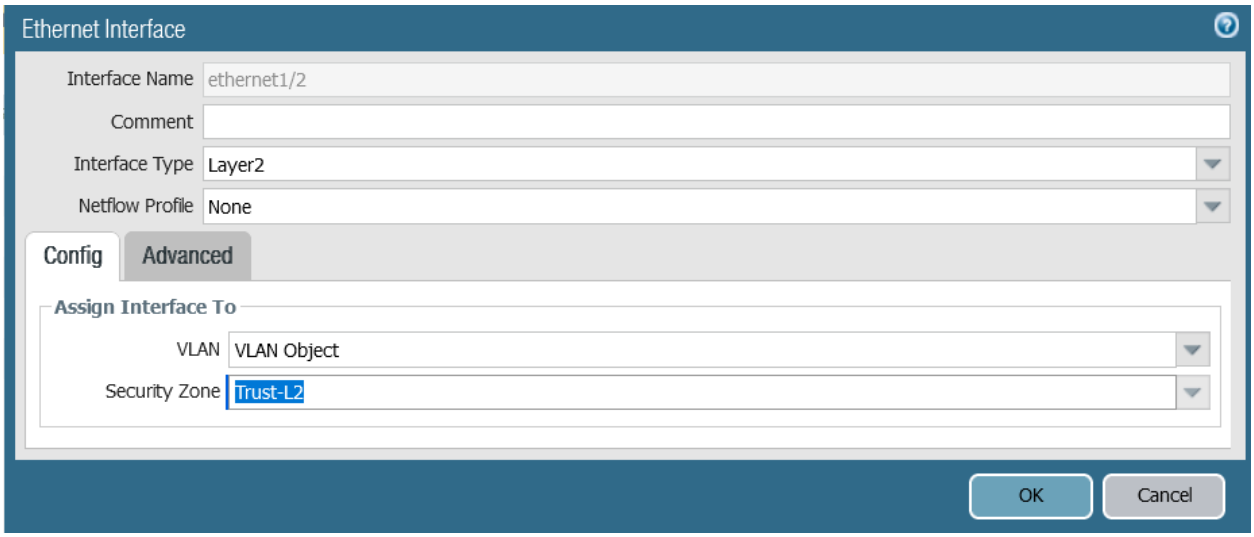
Next, go to Static routes under the default tab under Virtual Routers tab. Add a ipv4 static route pointing to the ISP's next hop.

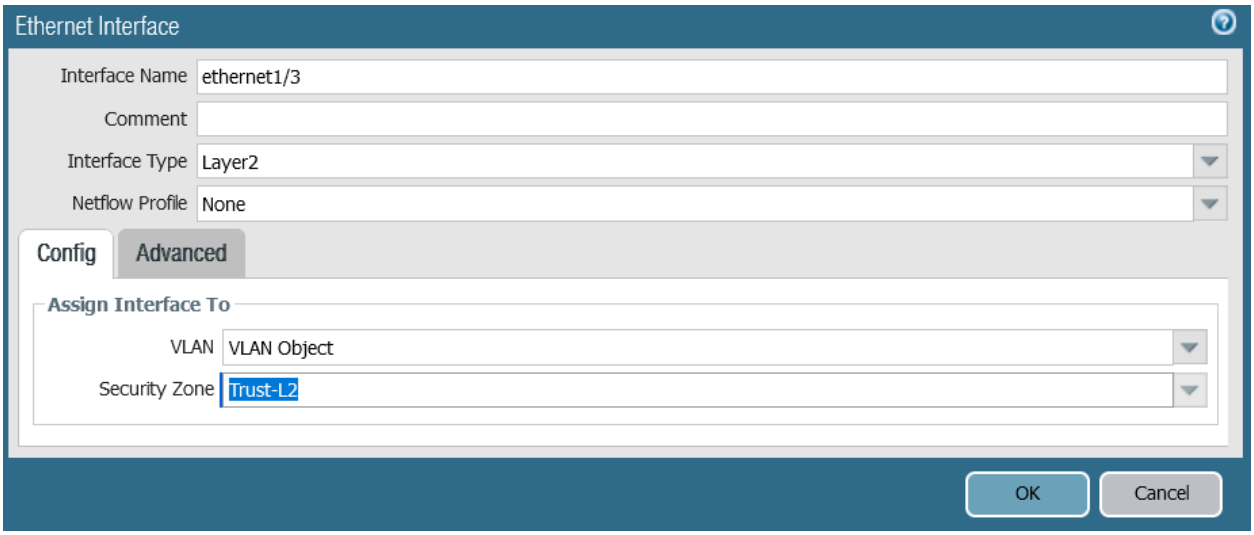


Next, go to VLANs under the Network tab and add a Vlan Object, with the VLAN interface being vlan.

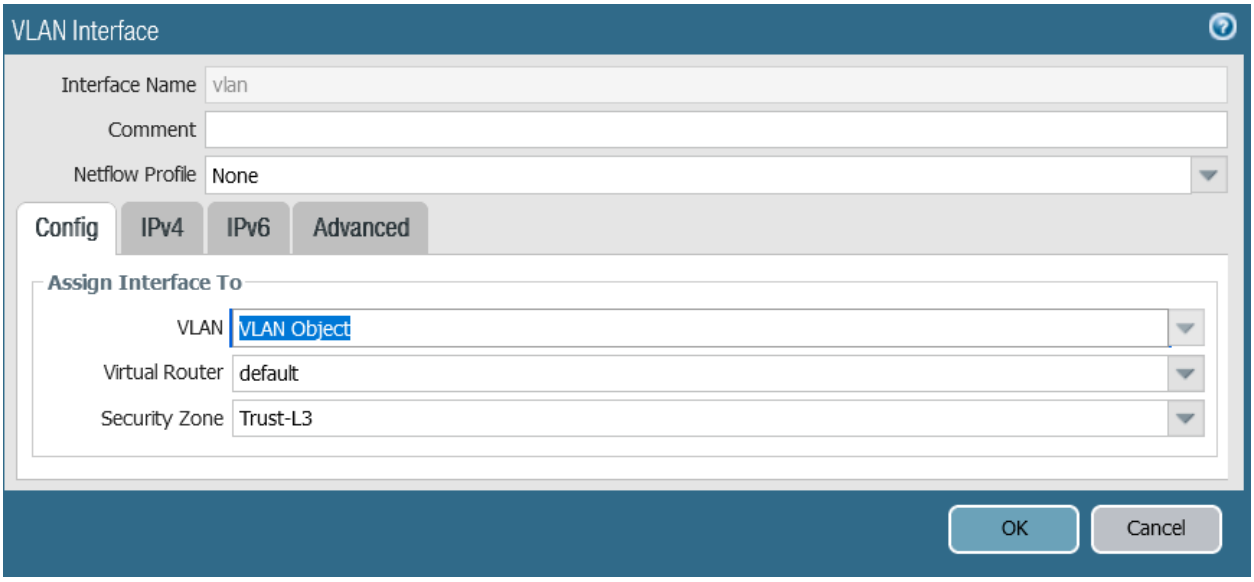
Next, go back to the Interfaces tab under Network, and edit ethernet1/2, and ethernet1/3.

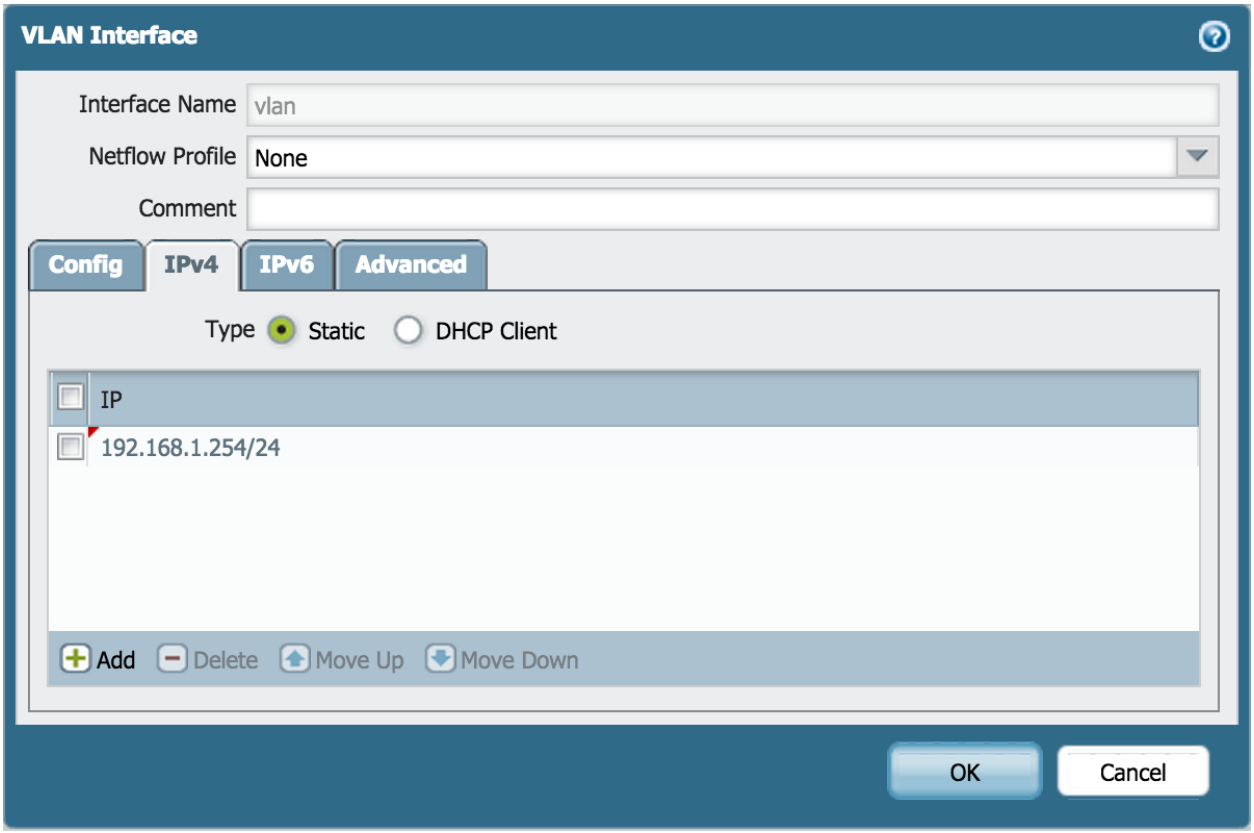
They should all be in Layer2, assigned to VLAN Object, and the security zone Trust-L2.



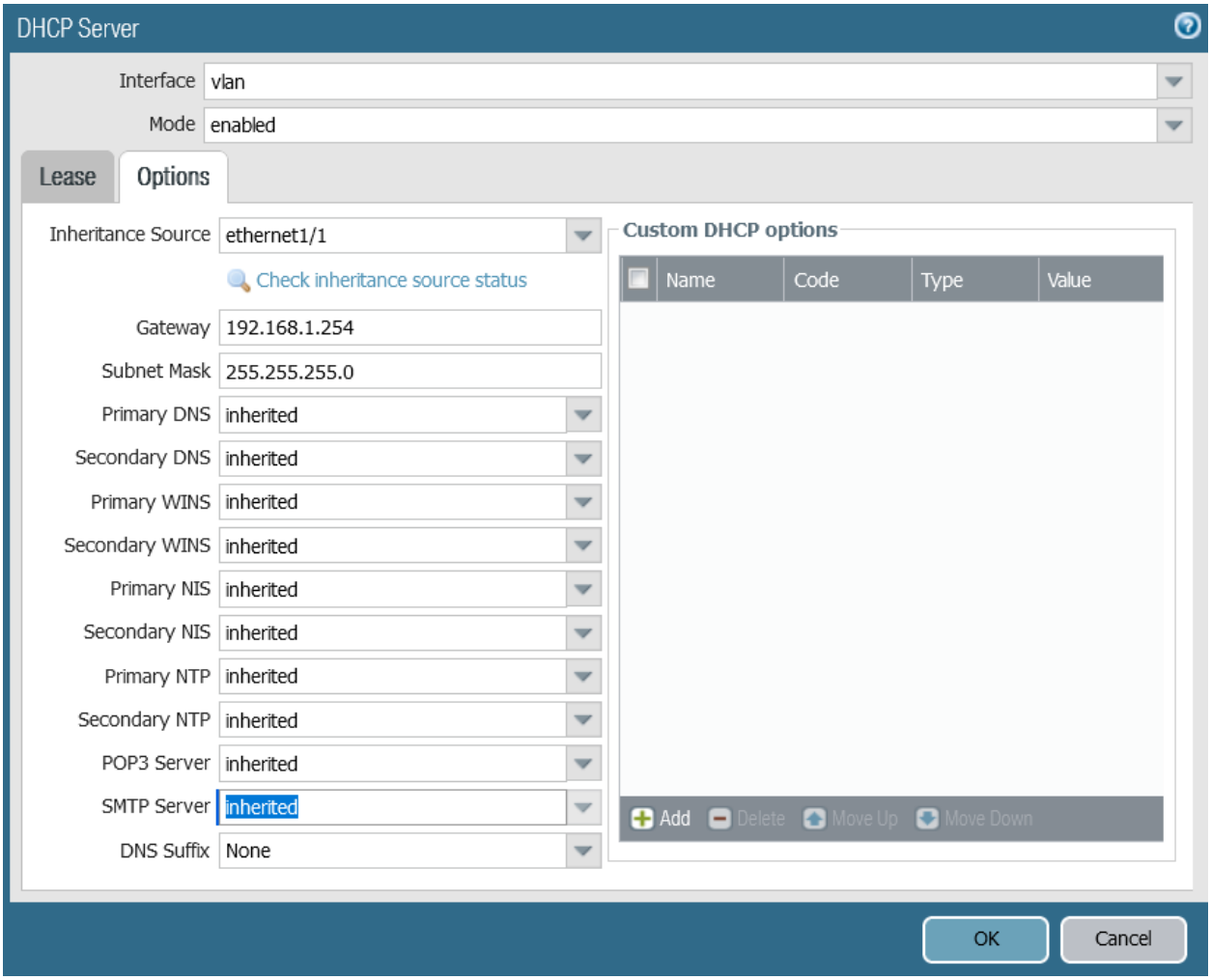


Next, configure vlan under the VLAN interface under the Interfaces tab under Network to be assigned to VLAN Object, default Virtual Router, and the security zone Trust-L3. After that, add the IP address 192.168.1.254/24 under IPv4 tab.

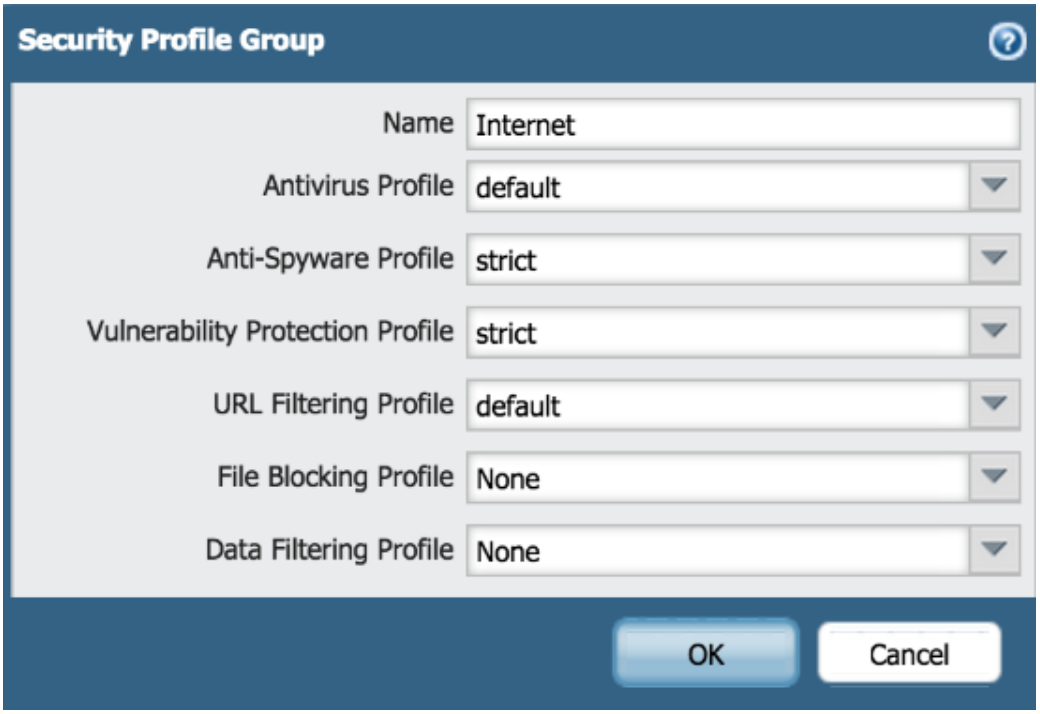




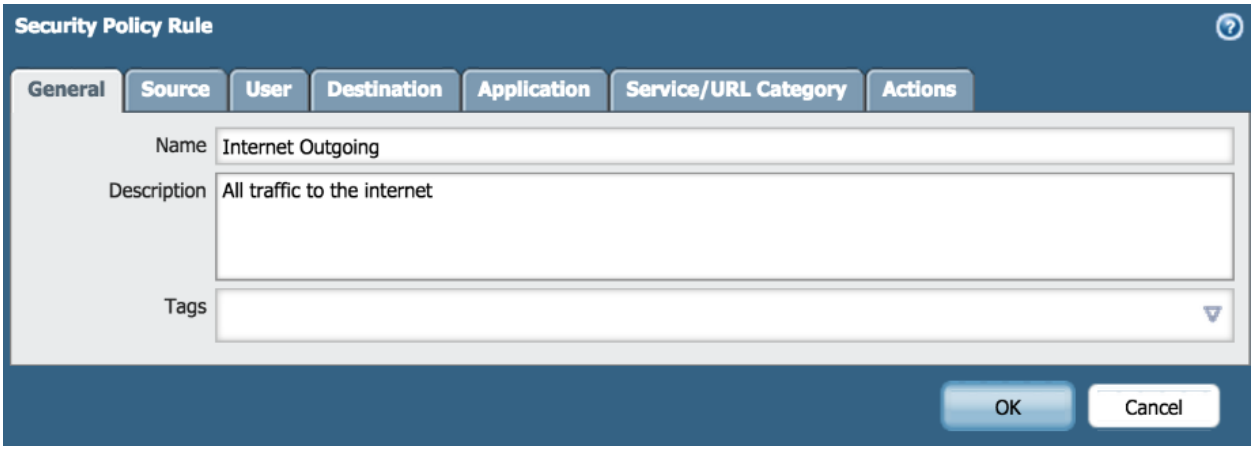
Next, under DHCP server in the DHCP tab under Network, add a DHCP server that is configured with the interface vlan, the inheritance source being ethernet1/1, and the ip pool subnet as 255.255.255.0. finally, set all the settings to inherited, except for DNS Suffix.



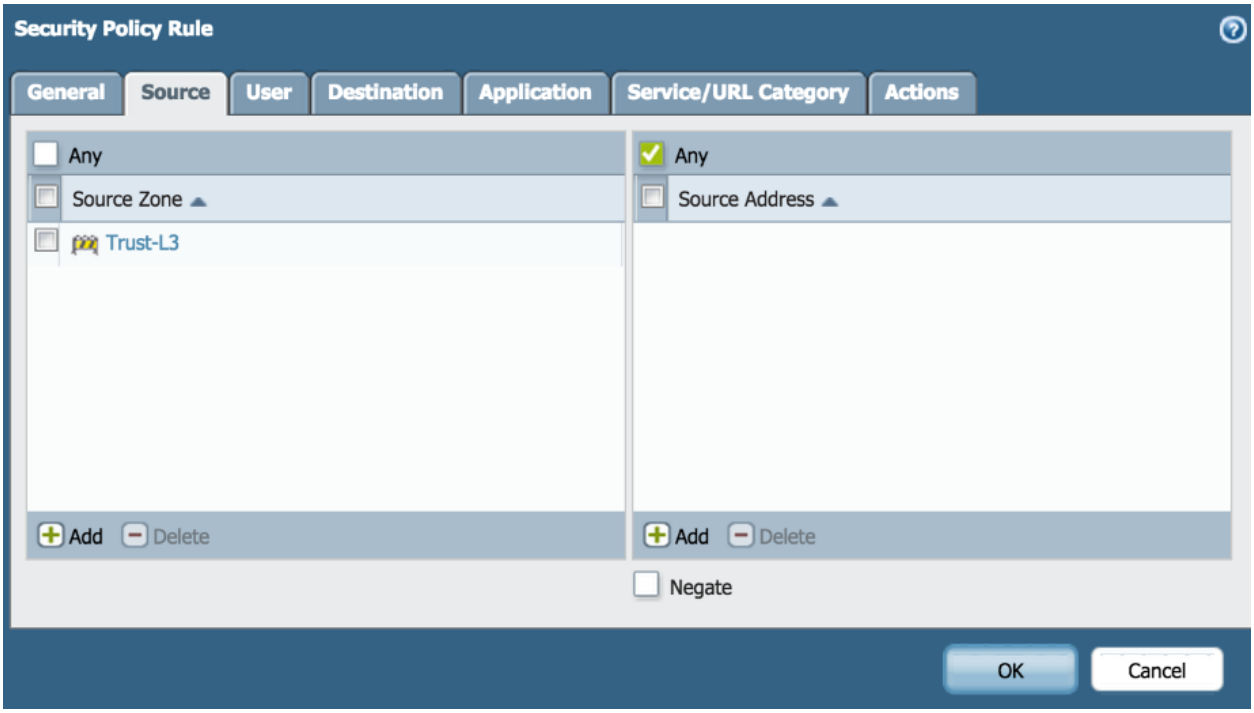
Next, add a Security Profile Group under Objects. Name it Internet, set the Antivirus Profile to default, set the Anti-Spyware Profile and Vulnerability Protection Profile to strict, URL filtering profile to default, and lastly, File Blocking Profile and Data Filtering Profile to none.

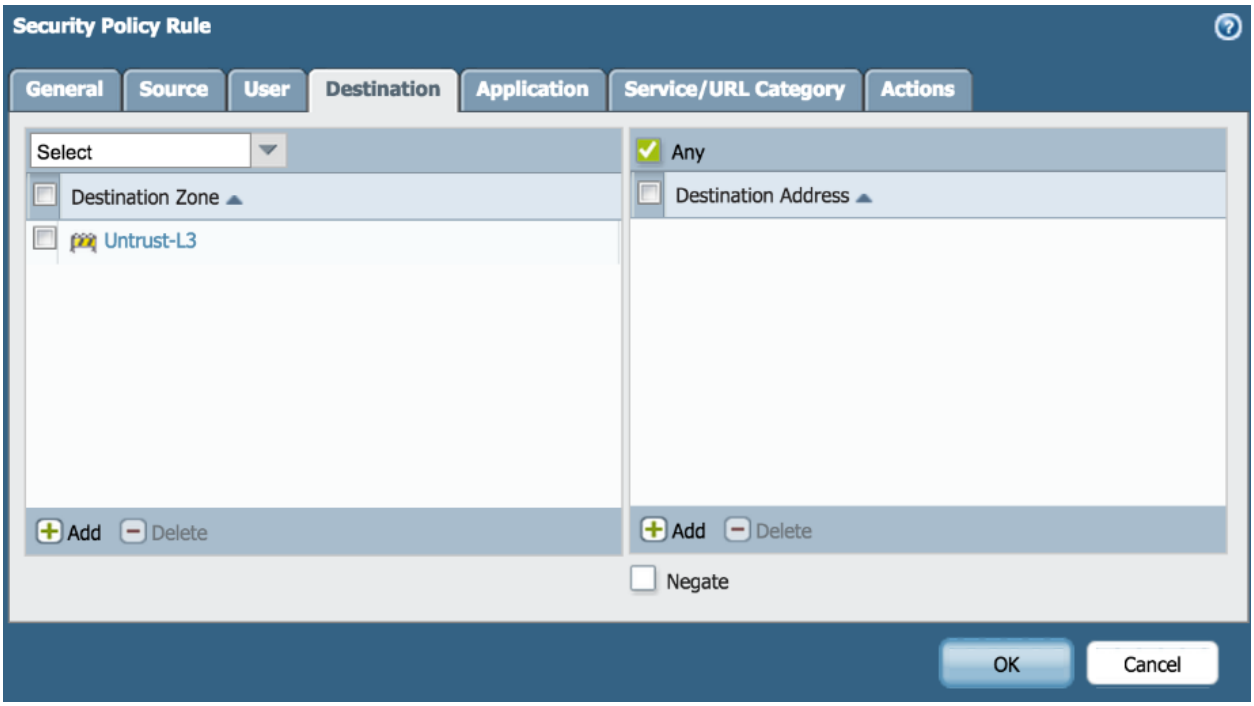


Next, configure the outbound internet security policy by adding a policy under the tab Policies in Security. In the general tab, enter a name and description (e.g. Internet Outgoing, All traffic to internet).

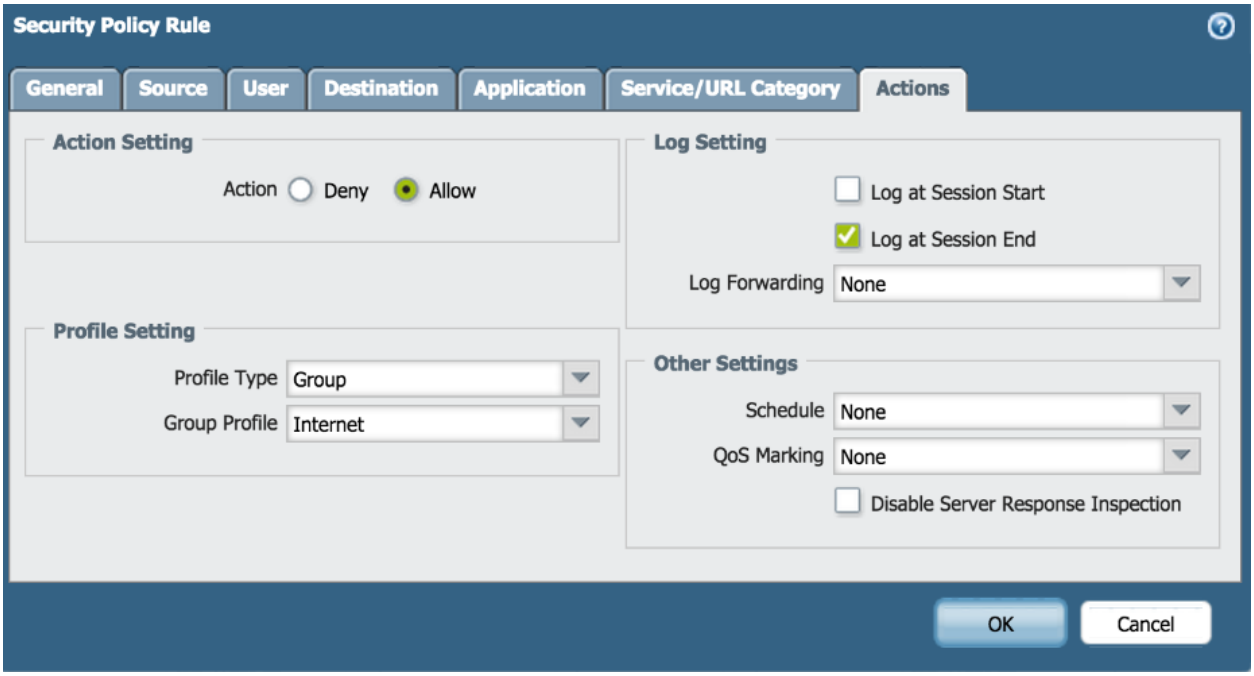


Next, in the Source and Destination tab, Add Source zone and Destination Zone.

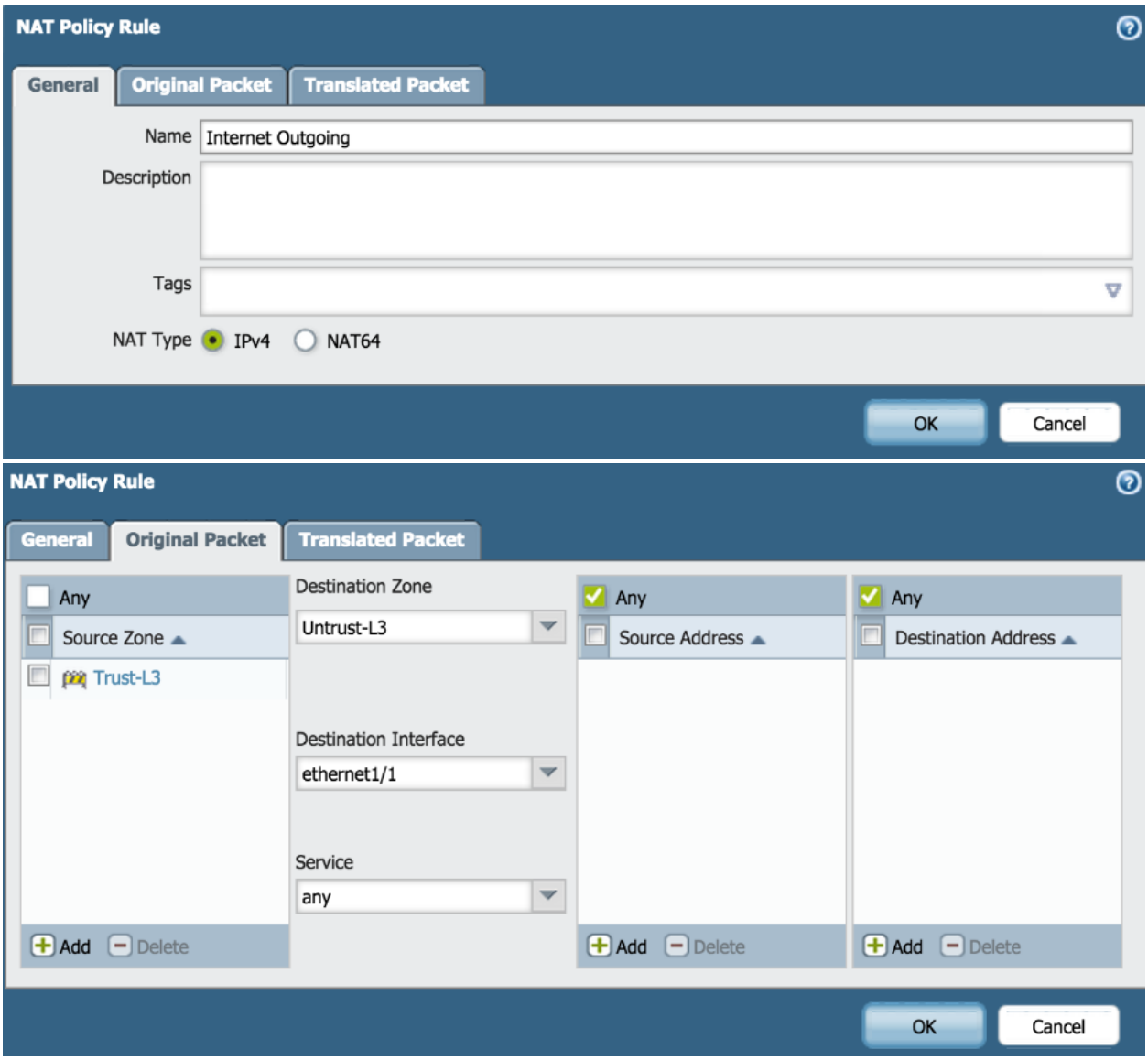

Security Policy Rule
General
Source
User
Destination
Application
Service/URL Category
Actions
Any
Source Zone
Trust-L3
Add
Delete
Any
Source Address
Add
Delete
Negate
OK
Cancel


Security Policy Rule
General
Source
User
Destination
Application
Service/URL Category
Actions
Select
Destination Zone
Untrust-L3
Add
Delete
Any
Destination Address
Add
Delete
Negate
OK
Cancel

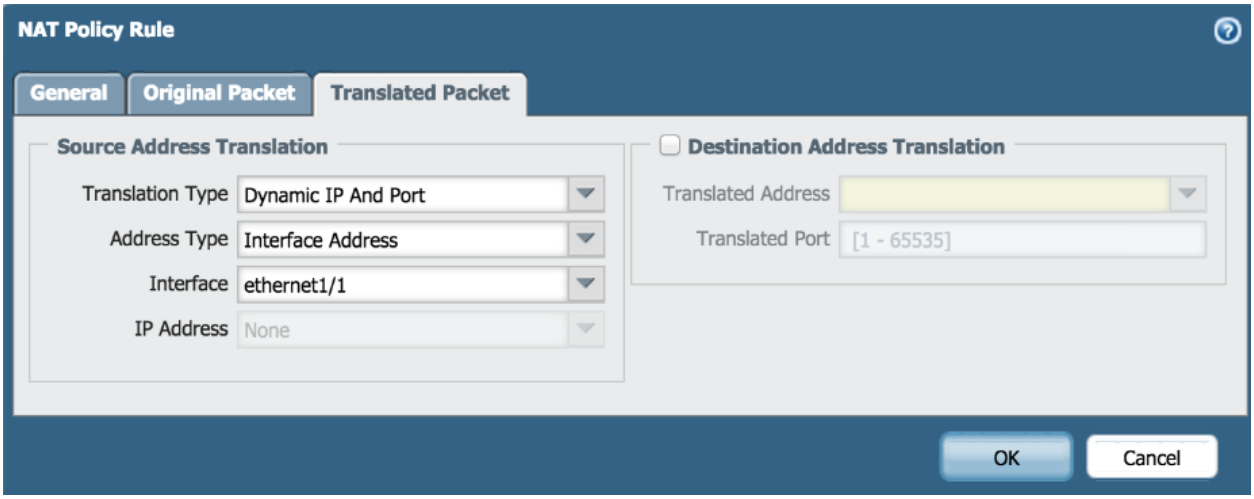
Next, configure the Profile setting in Actions tab.



Next, configure outbound NAT policy under Policies in Security. Add a name (e.g. Internet Outgoing), and specify and Source, Destination zones, and Destination Interface.

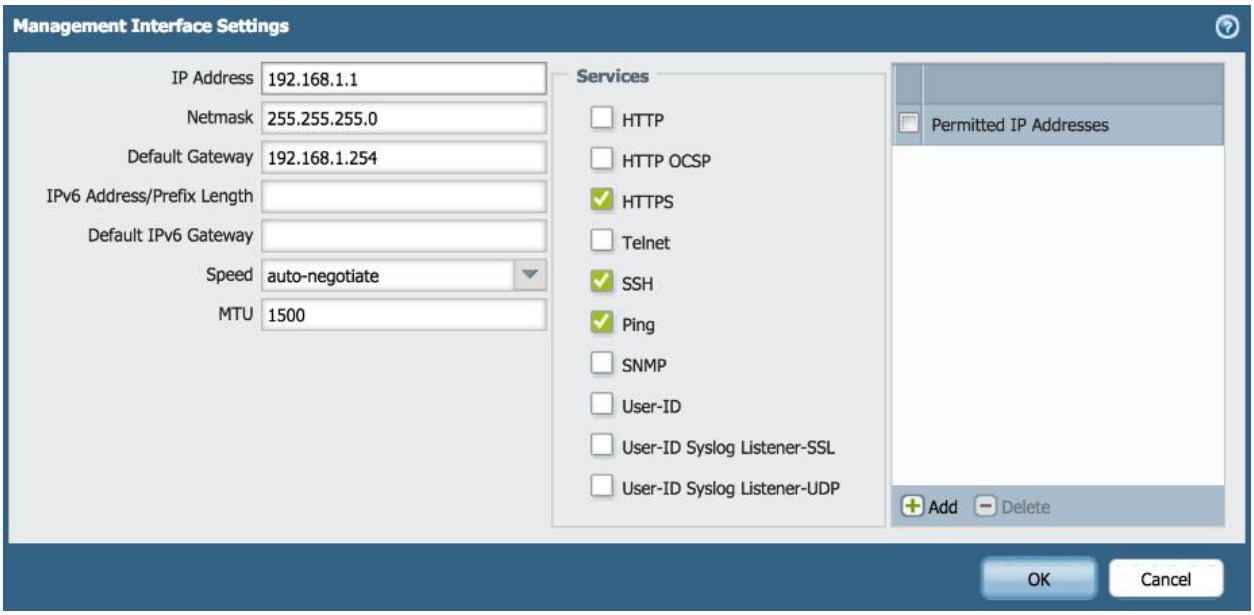


Next, in the Translated Packet part, set translation type to Dynamic IP and Port, Address type to Interface Address, Interface to ethernet1/1.



Click OK once the confirming the configuration.

Next, hop over to the Management tab under Setup under Device. Configure the management interface settings to have a IP address of 192.168.1.1, netmask of 255.255.255.0, and a default gateway of 192.168.1.254.



Finally, finalize by Committing the changes. Check for internet.

Problems

First, the firewall takes a bit to boot up (about 10 to 15 minutes) before things can be configured. On top of that, the setup within the Palo Alto GUI is complex, and is would be hard to do without a guide. Though navigating through the Palo Alto may be challenging, help can usually be found in the Palo Alto forums or other Palo Alto communities. On another note, I suggest checking for updates in the GUI, it may be easier to navigate and load.

Conclusion

In an increasingly digital age, the Palo Alto firewall is an exceptional device that can be set up for SOHO purposes. It provides a balances performance and security and has specifications perfect for being a Small Office/Home Office router.

Palo-Alto PA-220

Setting up URL filter for K-12 students

Palo Alto
PA-220 Enterprise
Hardware + Lizenz

Jeffrey Yiu Cheung

Purpose

This lab introduces a way to filter out inappropriate or unnecessary websites to students k-12's learning.

Background information

Palo Alto is a networking company that offers cybersecurity innovations to help with organizations with products like firewalls and cloud-based applications. It was founded in 2005 and has been the leader in cybersecurity research around the globe for the 11th straight year. With cybersecurity threats constantly emerging and improving, the need for cybersecurity is growing by day.

With new technologies constantly enabling the ease of interaction with the web, more information is being uploaded every second. There is useless information, educational information, but there are also sensitive, personal information in the web. To prevent these learning disruptions or cybersecurity threats, Palo Alto PA-220 offers URL filtering for its customers.

The Palo Alto PA220 firewall is a firewall designed to support t small and medium-sized organizations and can be an excellent option for a small, medium-sized school. It is able to mitigate many threats by having the ability to identify unknown malware and automatically generate protection upon analyzing the behavior and having many functions that blocks known threats. The raise in cyber-attacks have become more common and sophisticated, it is important to have protection against these threats. The Palo Alto device has a throughput of up to 500 Mbps, requires 50-60Hz voltage, and is about 3 pounds of weight. It can support up to 64,000 firewall sessions. However, if the school has high bandwidth usage, or many instances of video streaming/online activity, then it is not recommended.

URL filtering is a cybersecurity tool that prevents users from accessing sites that the admin has blocked. We can use the URL filters to filter out cybersecurity threats or learning disruptions to maximize cyber safety and focus during class.

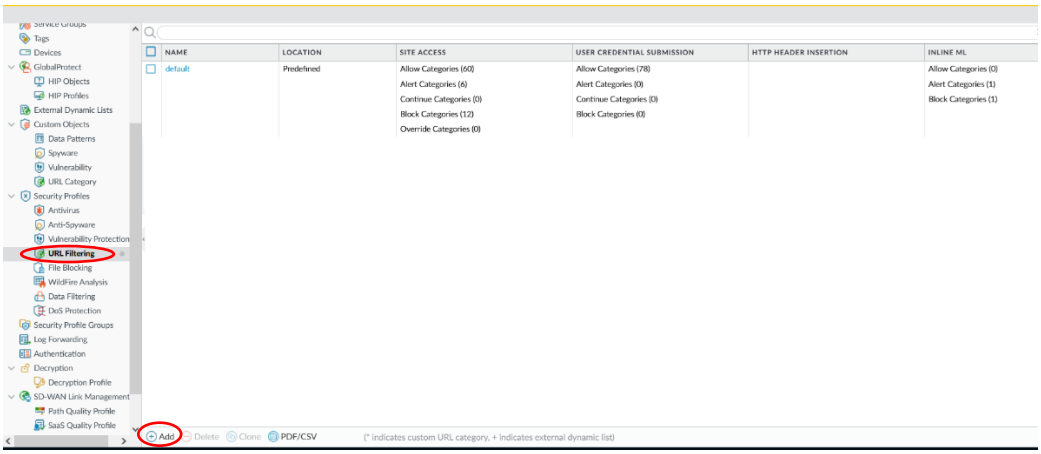
The Palo Alto PA-220 firewall uses the Palo Alto database to categorize websites into categories like Government, Games, Artificial Intelligences, Adult, Nudity. This technique is called Category-based filtering.

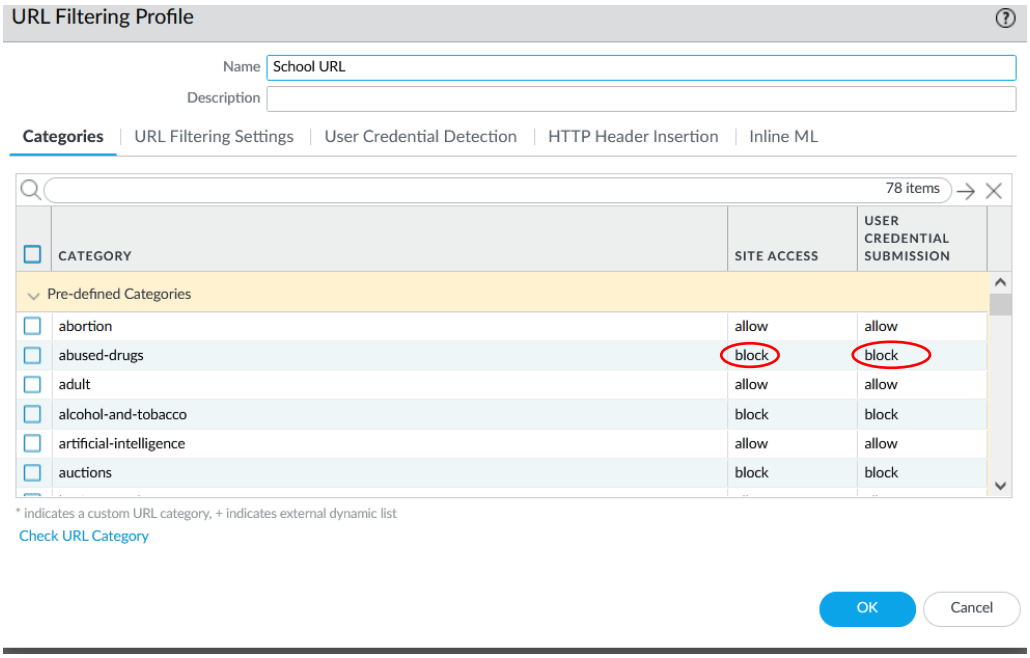
Palo Alto can also detect malicious websites with grayware, malware, phishing attacks, etc. This is a technique called Reputation-Based Filtering. Their cloud-database constantly gets updates about malicious activity and flags them as dangerous to block malicious activities.

While URL filtering is helpful tool which can improve productivity, control over content, and reducing inappropriate activity, URL filters might also categorize legitimate websites as inappropriate and blocked. There are also techniques which can bypass filters to be wary of.

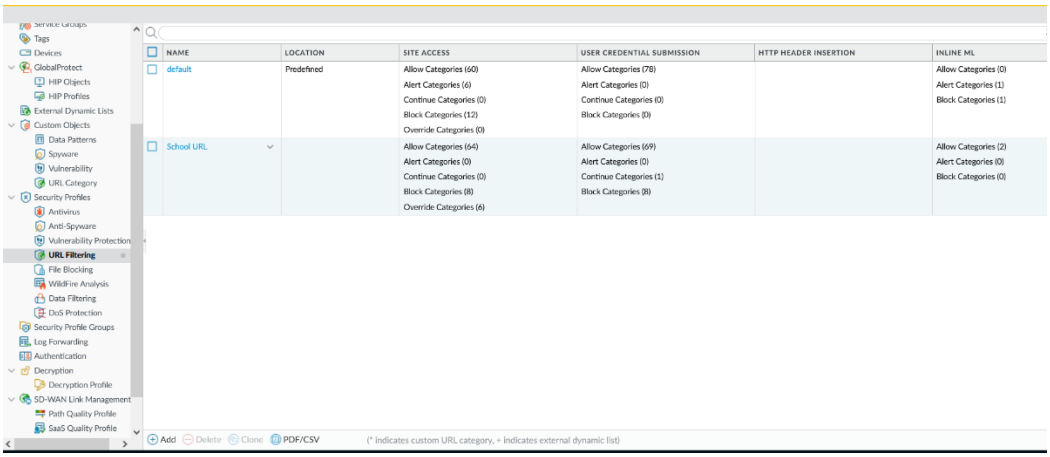
Lab summary

First, under Objects tab, in security profiles, there should be a subtab named URL Filtering. Add a new one, and name it (e.g. School URL). Then within the categories, select the ones you would like to block or override. If you would like to completely block a site (no access from students and no access from admins), you would select block for site access and user credential submission.



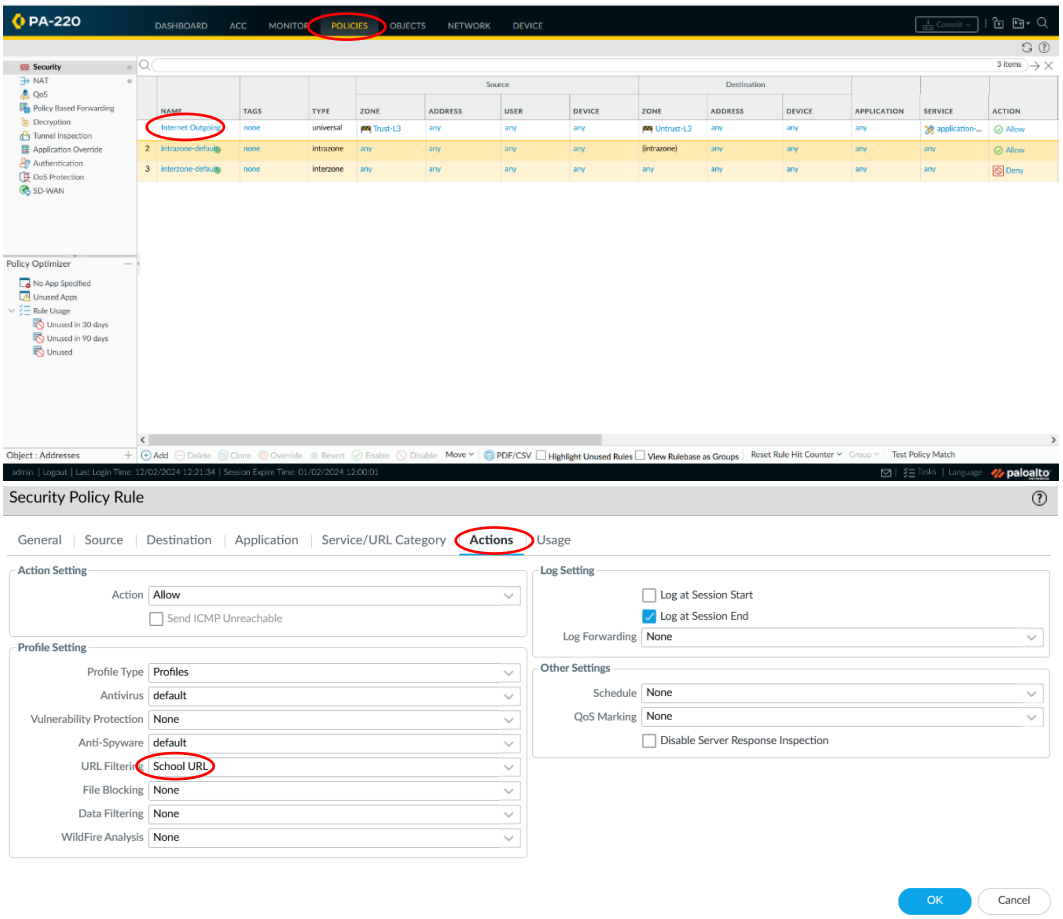


If you want to allow admin override, you change site access to override and user credential submission. To allow, both should be set to allow. We blocked abused-drugs, alcohol and tobacco, auctions, cryptocurrency, nudity, phishing, and weapons. We allowed admin override in categories in games and shopping. We allowed everything else.



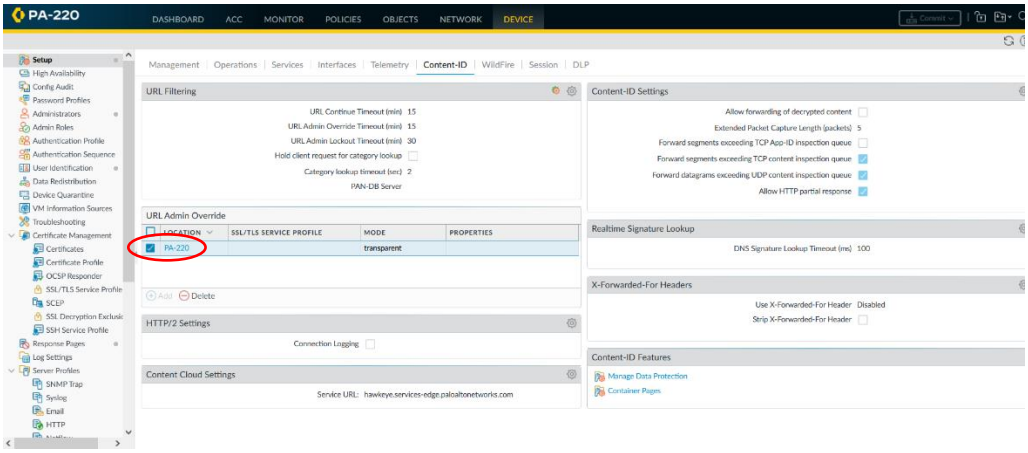
It should look like this after it is finished.

Next, after finishing site access, navigate to the security policy for outbound internet (e.g. Internet Outgoing). You have to attach the URL filter you just created into the internet policy, in the actions tab of the policy.

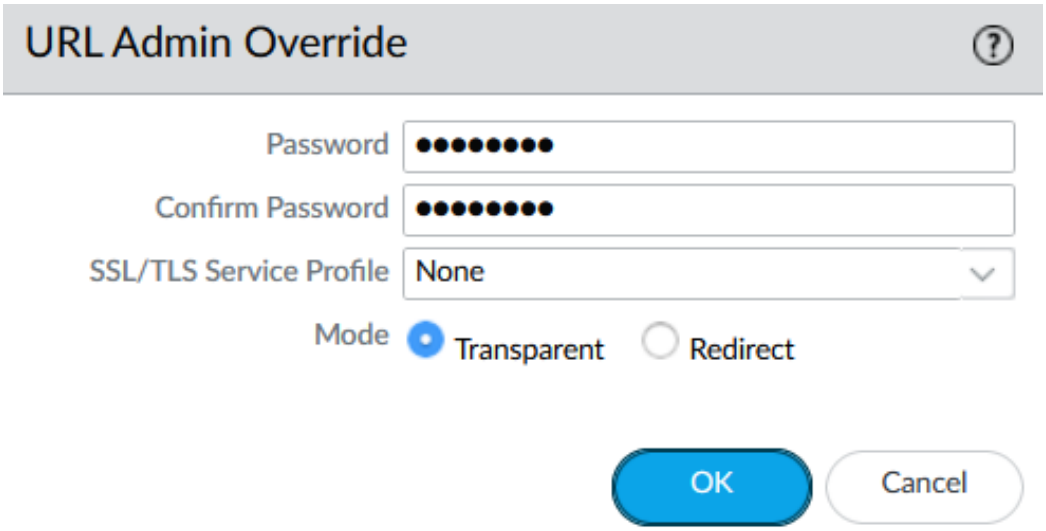


After this process, the websites you blocked should not be accessible.

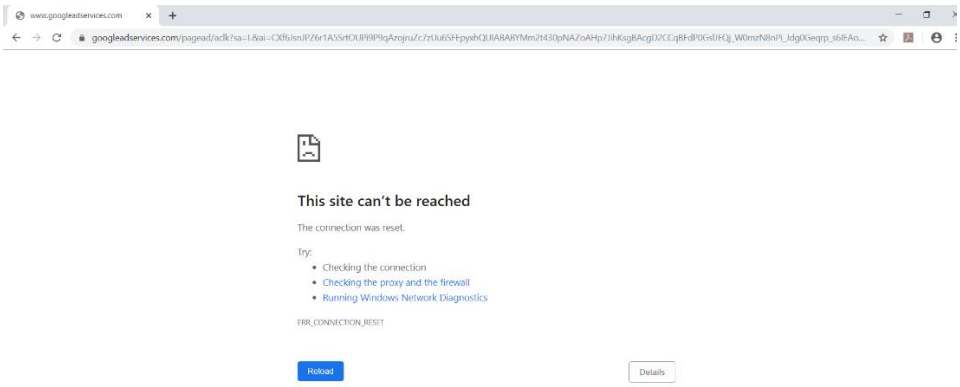
Finally, we need to set an admin password allowing admin override. Navigate to Setup under the Device tab. In Content-ID, there should be a section named URL Admin Override. This is where we create the password for Admin Override.



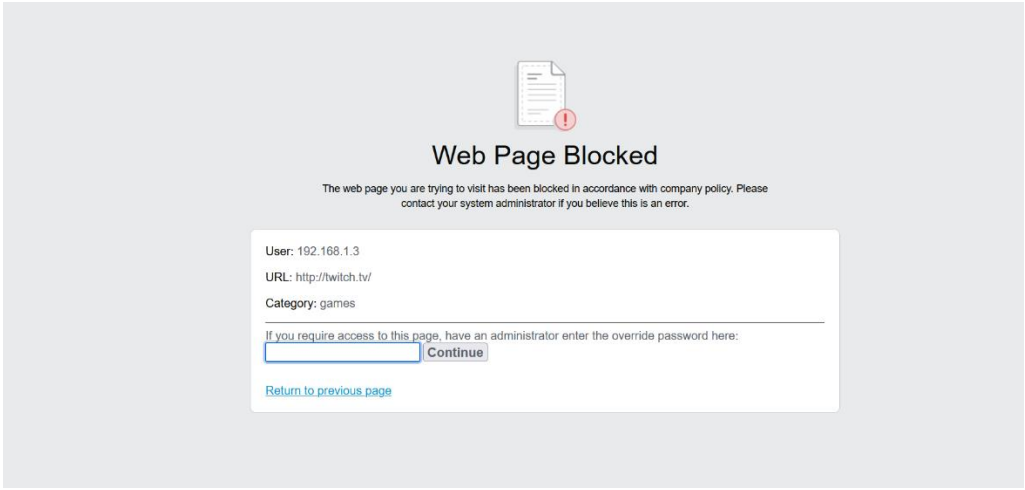
q`



This is what it should look like when the site is blocked:



This is what it should look like when the site can be overridden:



Problems

This lab was straightforward, however time-consuming. For every change and every confirmation, we had to commit, which takes about 5-10 minutes. On top of this, we are on an older version, a newer option may be more optimized. Also, it was hard to deduce how Palo Alto categorizes it's websites, so the site https://urlfiltering.paloaltonetworks.com/ can help a lot.

Conclusion

In conclusion, in a increasingly digital age, more malicious activities are online and it is important to block dangerous sites (not only sites that may steal sensitive information, but also inappropriate sites), especially for children in a k-12 environment. URL filtering is a great tool that can block those sites.

Palo-Alto PA-220

Setting up GlobalProtect VPN and Remote Desktop

Palo Alto
PA-220 Enterprise
Hardware + Lizenz

Jeffrey Yiu Cheung

Purpose

The purpose of this lab is to set up a GlobalProtect VPN on a PA-220 Firewall to enable secure connection with remote networks. This lab also demonstrates how to use Remote Desktop Connection to utilize a computer on a different network.

Background information

In the modern age, being able to securely access private network remotely is important for work and organizations. With cybersecurity threats constantly evolving, hackers can utilize new knowledge to breach sensitive data. To prevent sensitive information from being risked, Palo Alto Networks designed and offered GlobalProtect VPN to its customers.

GlobalProtect VPN is a feature on the PA-220 firewall which allows secure remote connections to the internal network. It creates a tunnel between the user and the destined network and encrypts the data with IPsec or SSL/TLS which passes through. Users can thus use this ability to safely access their internal network while away from home/company. GlobalProtect VPN is a service designed by the Palo Alto Networks to work seamlessly with the PA-220 firewall. Although it is reliable and secure, it can impact the performance of the network due to taking more bandwidth. GlobleProtect also require a lot of complex setups to get up and running.

VPNs, or virtual private networks, is a technology that allows users to securely connect to private networks over the internet. By creating a tunnel and encrypting data with advanced protocols like IPsec and SSL/TLS to ensure protection against eavesdropping attacks and other threats. VPNs provides stronger privacy and security online, and on top of this, it also allows users to bypass geographical limitations.

IPsec, an encryption protocol used by GlobalProtect, is a combination of other security protocols to create a protocol that ensures security, integrity, and authentication. It uses protocols like Authentication Header and Encapsulation Security Payload. IPsec follows AES (Advanced Encryption Standard), a highly secure and efficient encrypting algorithm. Although IPsec is secure, it is resource intensive and may drop performance.

Palo Alto Networks is a cybersecurity company headquartered in Santa Clara, California. Palo Alto Networks offers cybersecurity products and innovations like firewalls and cloud-based applications. It was founded in 2005 and has been awarded as the leader in cybersecurity research around the globe for the 11th straight year.

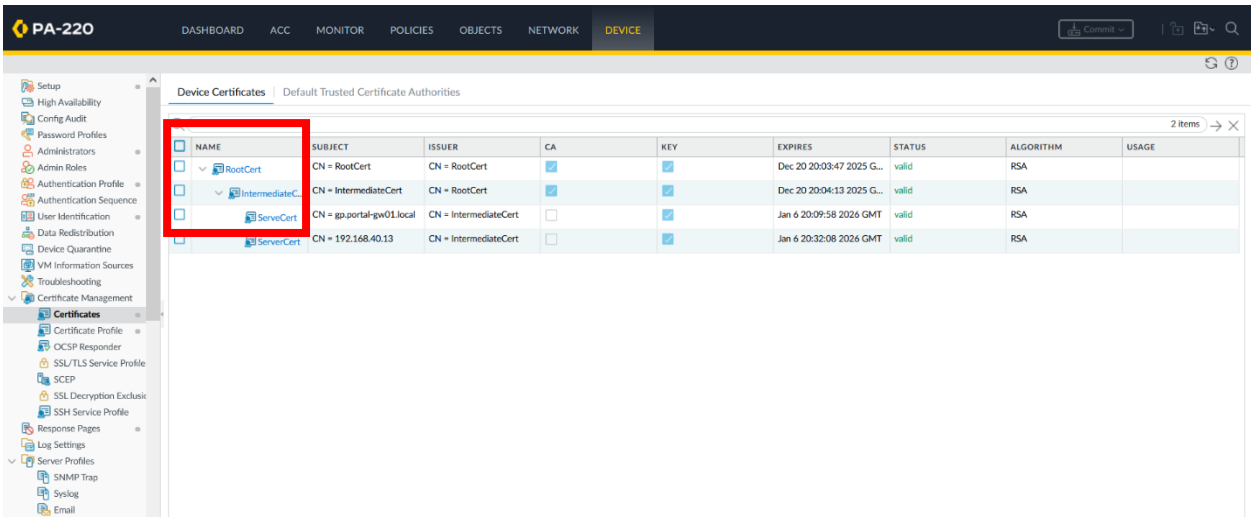
The Palo Alto PA-220 firewall is a firewall designed to support small and medium-sized organizations and can be an excellent option for a small office. It offers features such as URL filtering, GlobalProtect VPN, WildFire (cloud-based threat analysis service), DNS security… etc. Due to cyber-attacks having become more common and sophisticated, it is important to have protection against these threats. The Palo Alto device has a throughput of up to 500 Mbps, requires 50-60Hz voltage, and is about 3 pounds of weight. It can support up to 64,000 firewall sessions.

Remote Desktop Protocol is a service provided by Microsoft which allows users to connect and control another device via IP (or domain name if applicable). This technology allows users to work, access files, using the computer despite not physically having the machine they need. However, RDP needs the devices to be on the same network, and RDP is vulnerable to cyberattacks, with unrestricted port access and other exploits like BlueKeep, and thus is necessary to run it within a VPN.

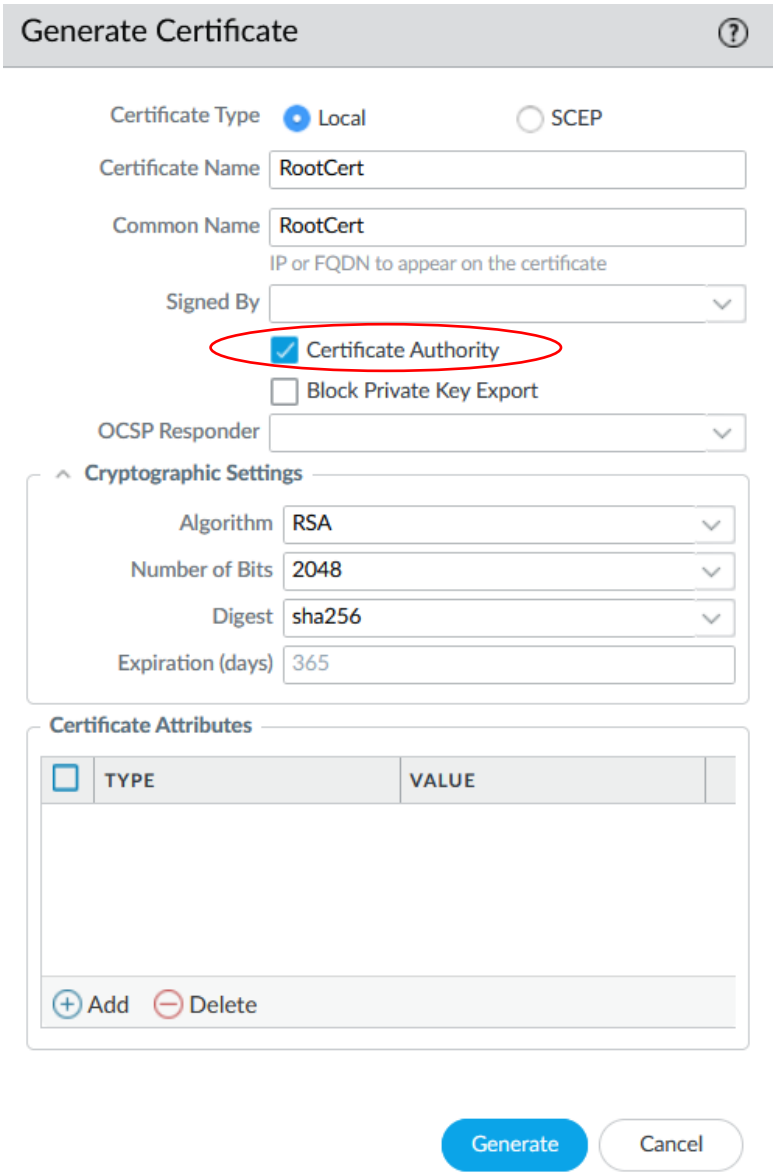
Microsoft is one of the largest and most influential technology company to have exist. Founded in 1975, Microsoft developed and revolutionize how commercial computers are built. Their products range from Operating Systems (windows), computers, software (Microsoft Office), cloud services, and videogames. Today, Microsoft is a technology giant that shape ongoing technology development.

Lab summary

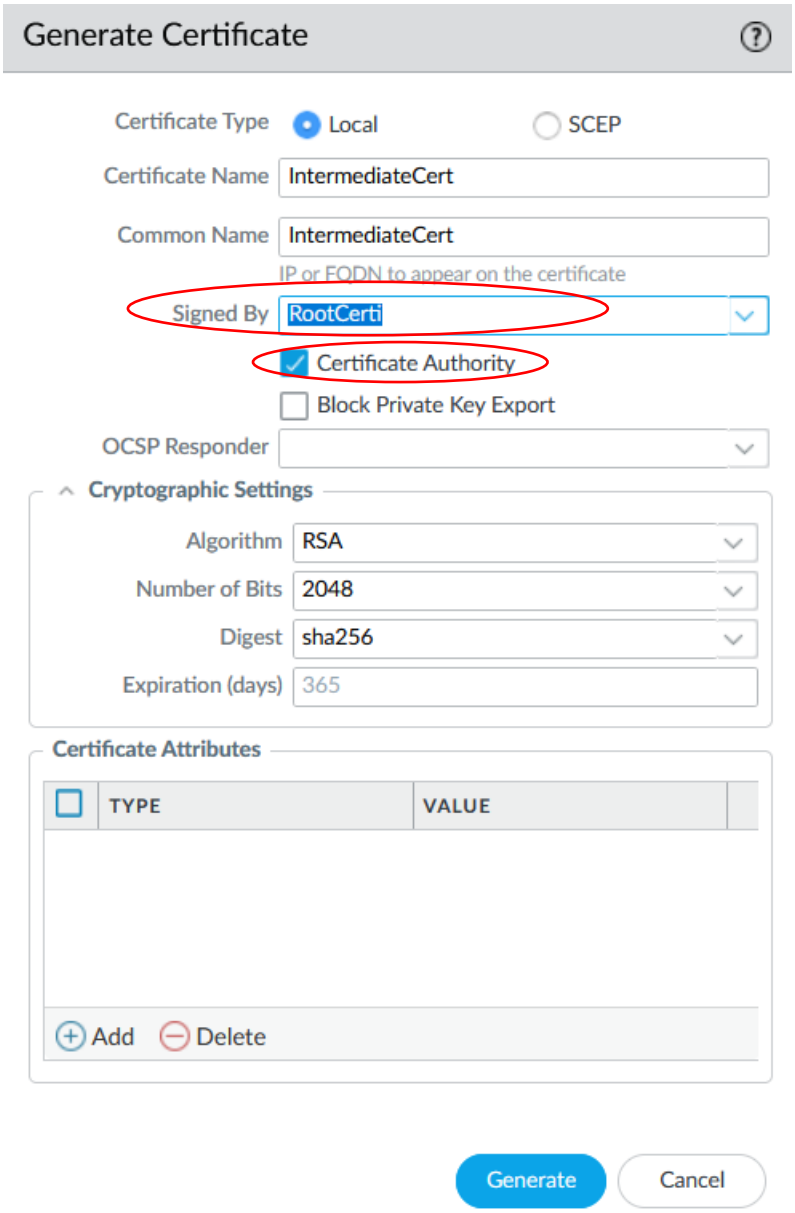
First, we need to generate 3 certificates to match the picture below.



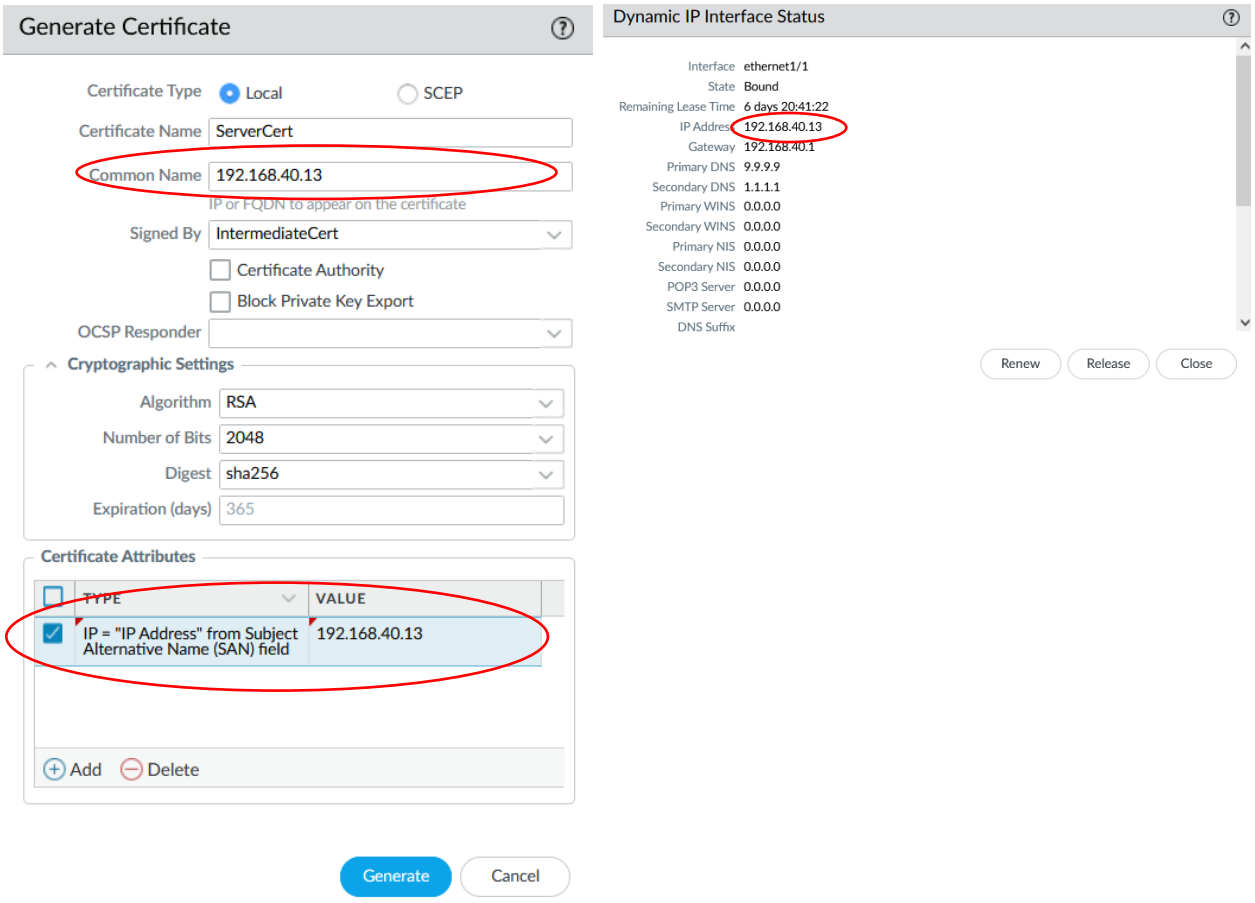
For the first certificate, we need to generate a root certificate. It is under Device > Certificate Management > Certificates > generate. Use the any name for Certificate name and Common Name (except for an IP or FQDN) and check on Certificate Authority.



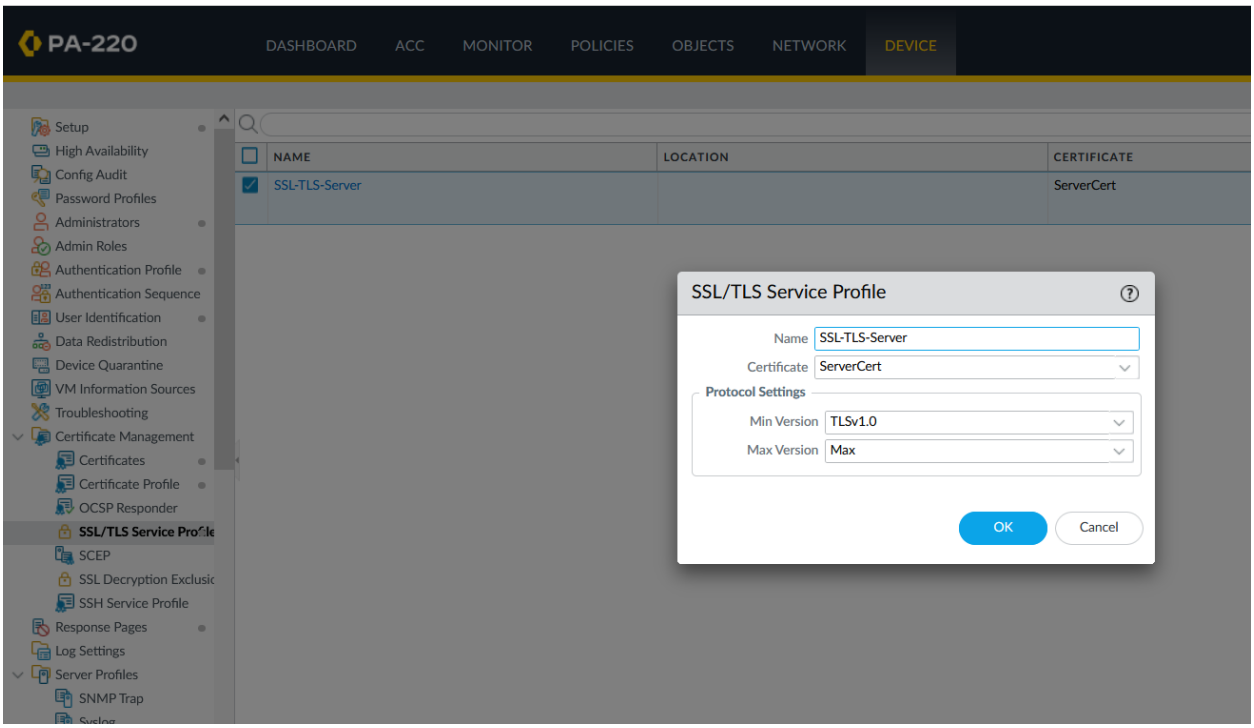
For the second certificate, generate a similar certificate, but signed by the first certificate.



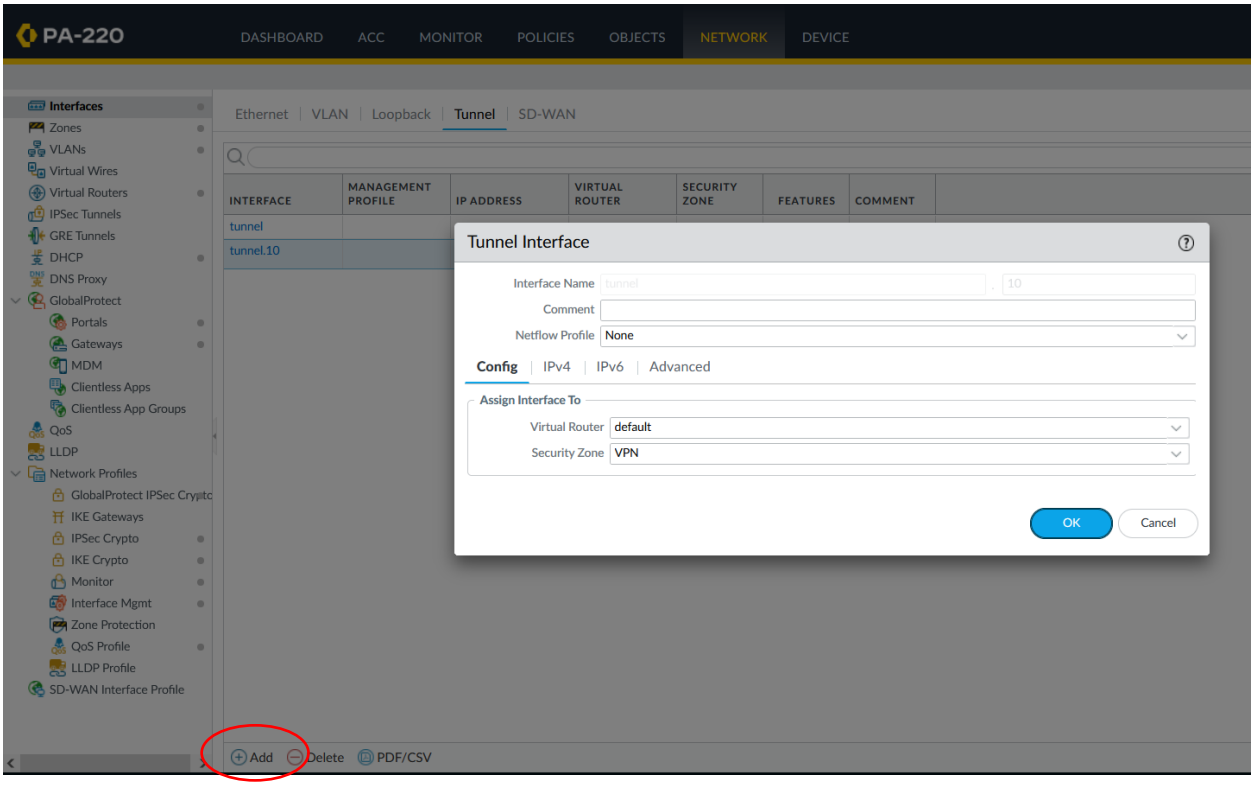
For the third certificate, pick any name you want for the certificate name, but assign the IP of the DNS server address. You can check via Interfaces in the Network tab. It should not be checked as Certificate Authority and should be signed by the second certificate. It should also have an attribute, which is just the DNS server address again.



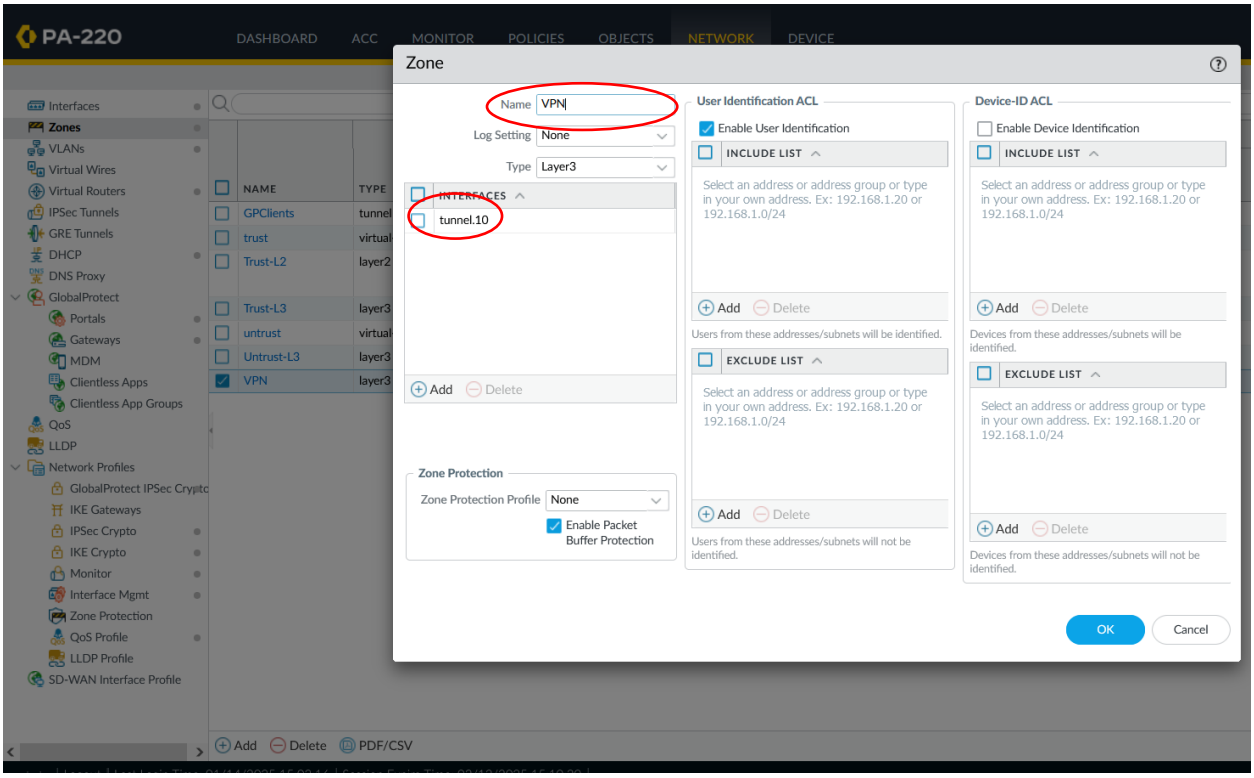
Next, make an SSL/TLS certificate profile. In Device > Certificate Management > SSL/TLS Service Profile > create. Link the third certificate you made (in my case it is ServerCert).



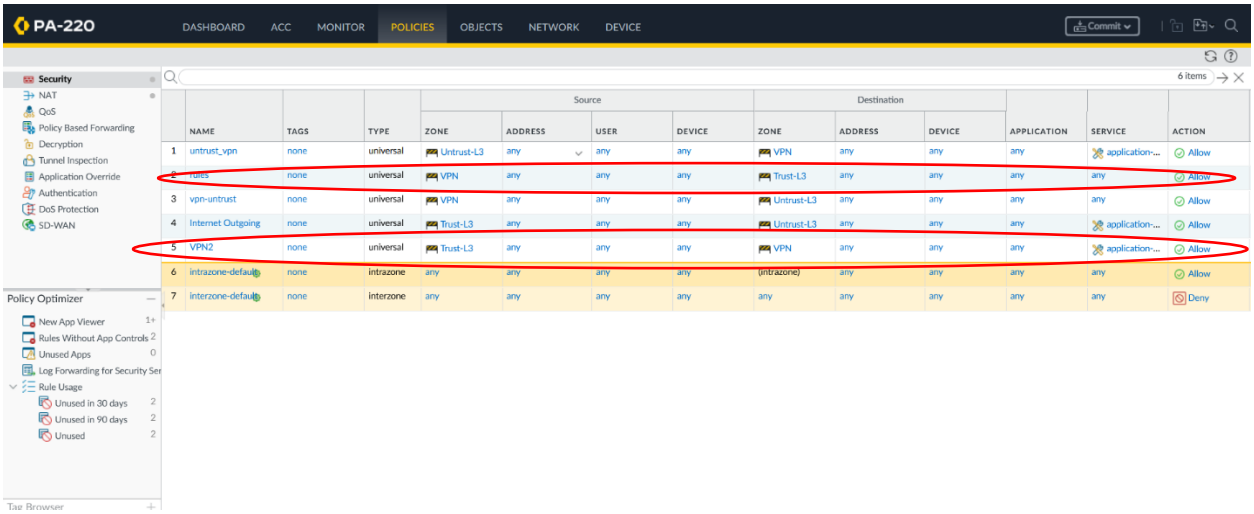
Next, head to Network > Interfaces > Tunnel and create a new tunnel.



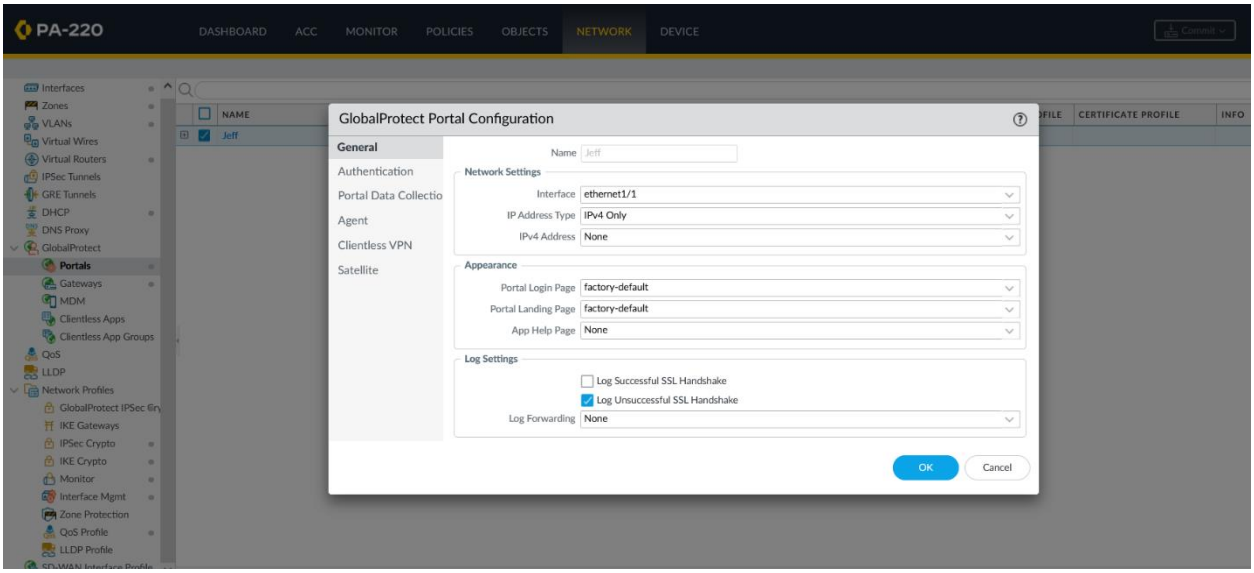
Afterwards, make a new security zone in Network>Zones and attach the newly made tunnel to it.



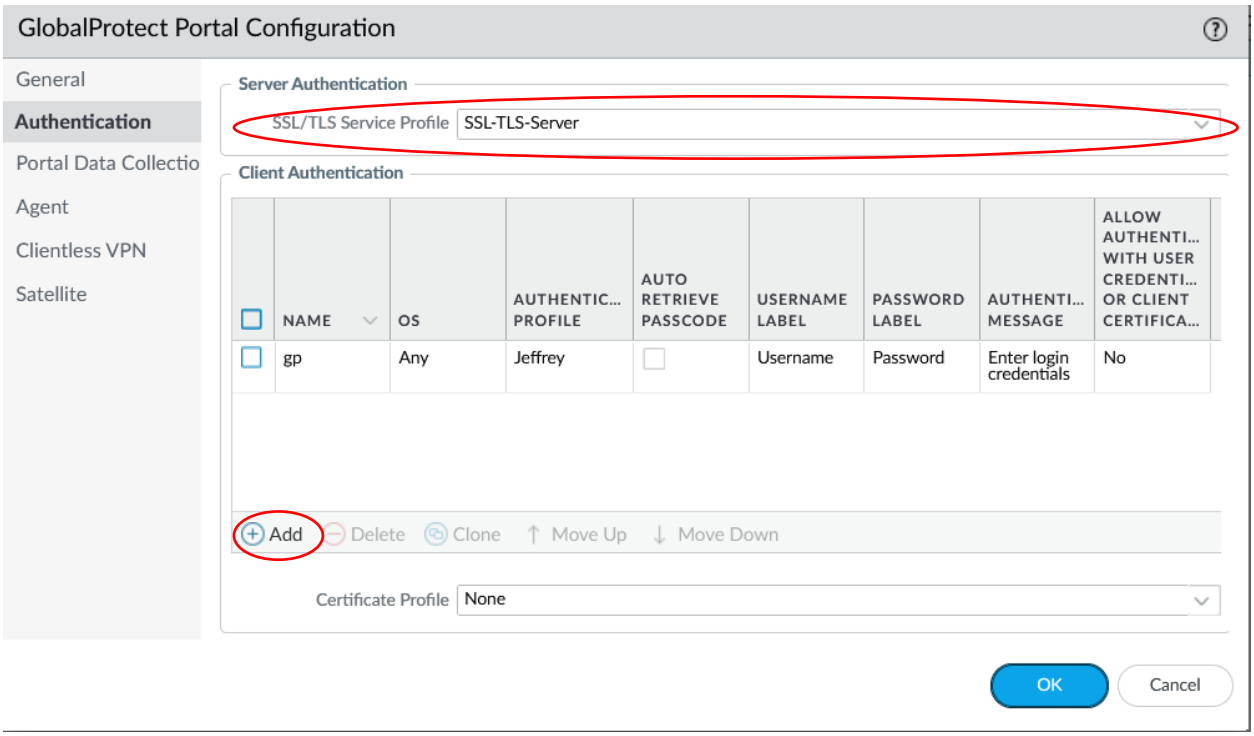
Next, go to Policies>Security Policies and make a couple of security policy that would allow the traffic. One for zone VPN to Trust-L3 and one from Trust-L3 to VPN is necessary.

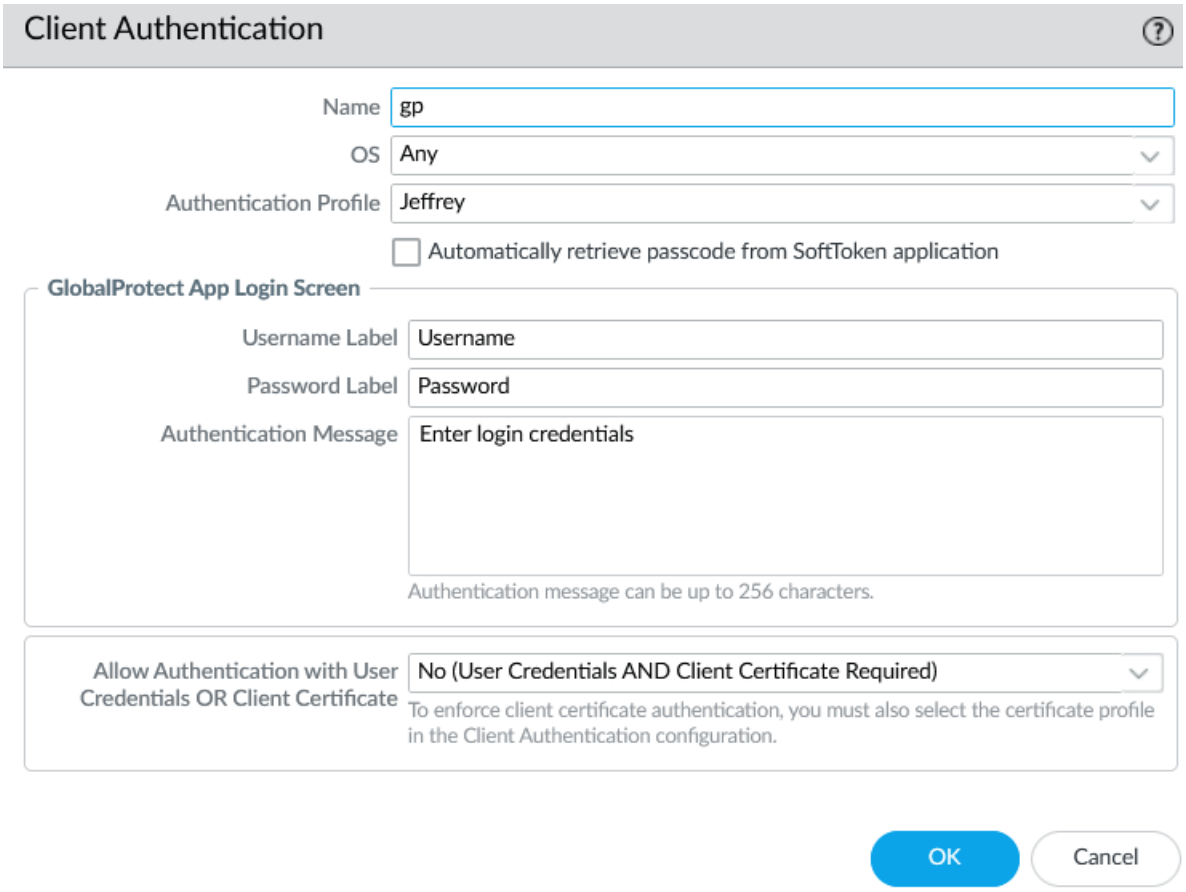


Next, go to Network>GlobalProtect>Portals, and add a new portal configuration.

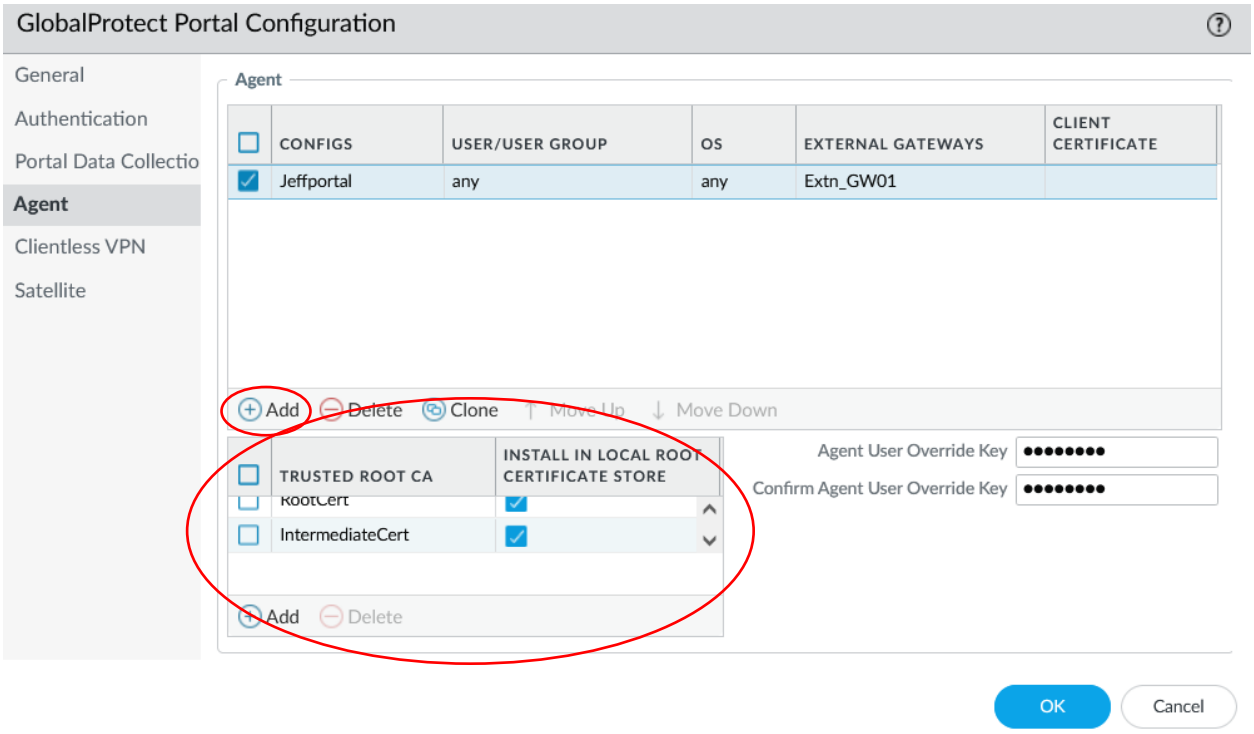


In authentication, attach the SSL/TLS server profile you made earlier and add a authentication profile which allows all.

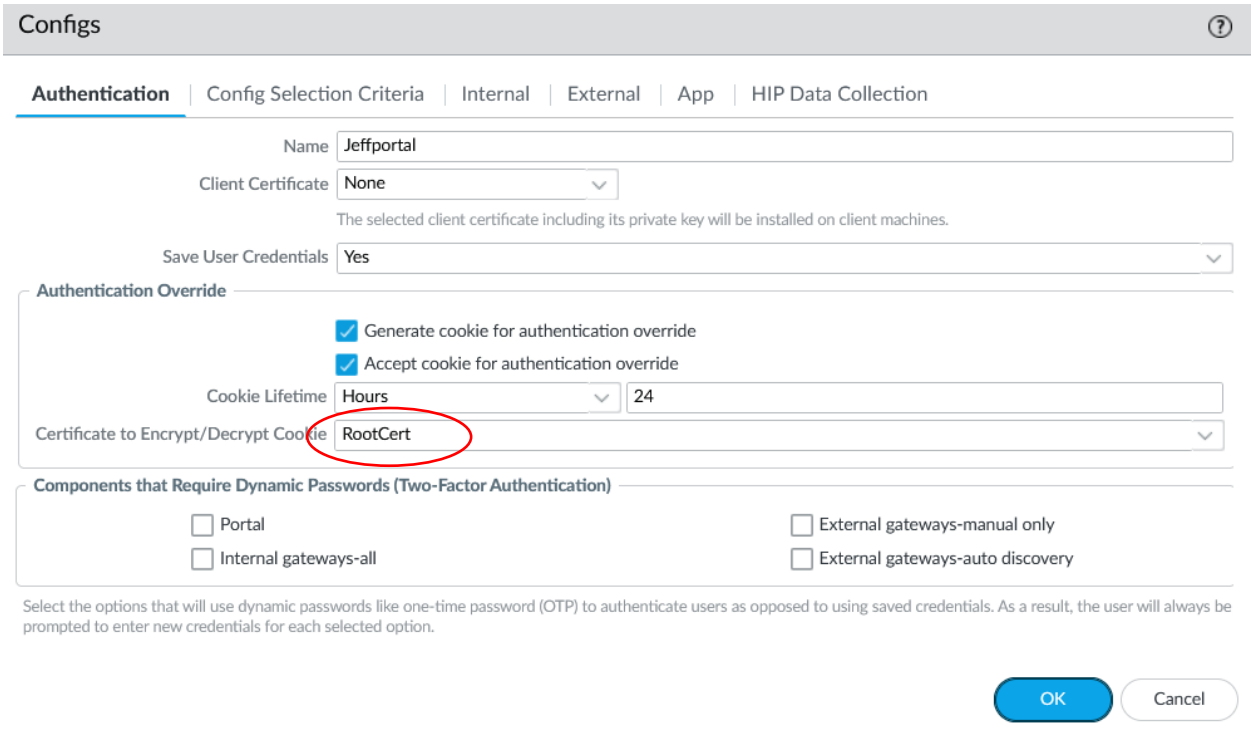




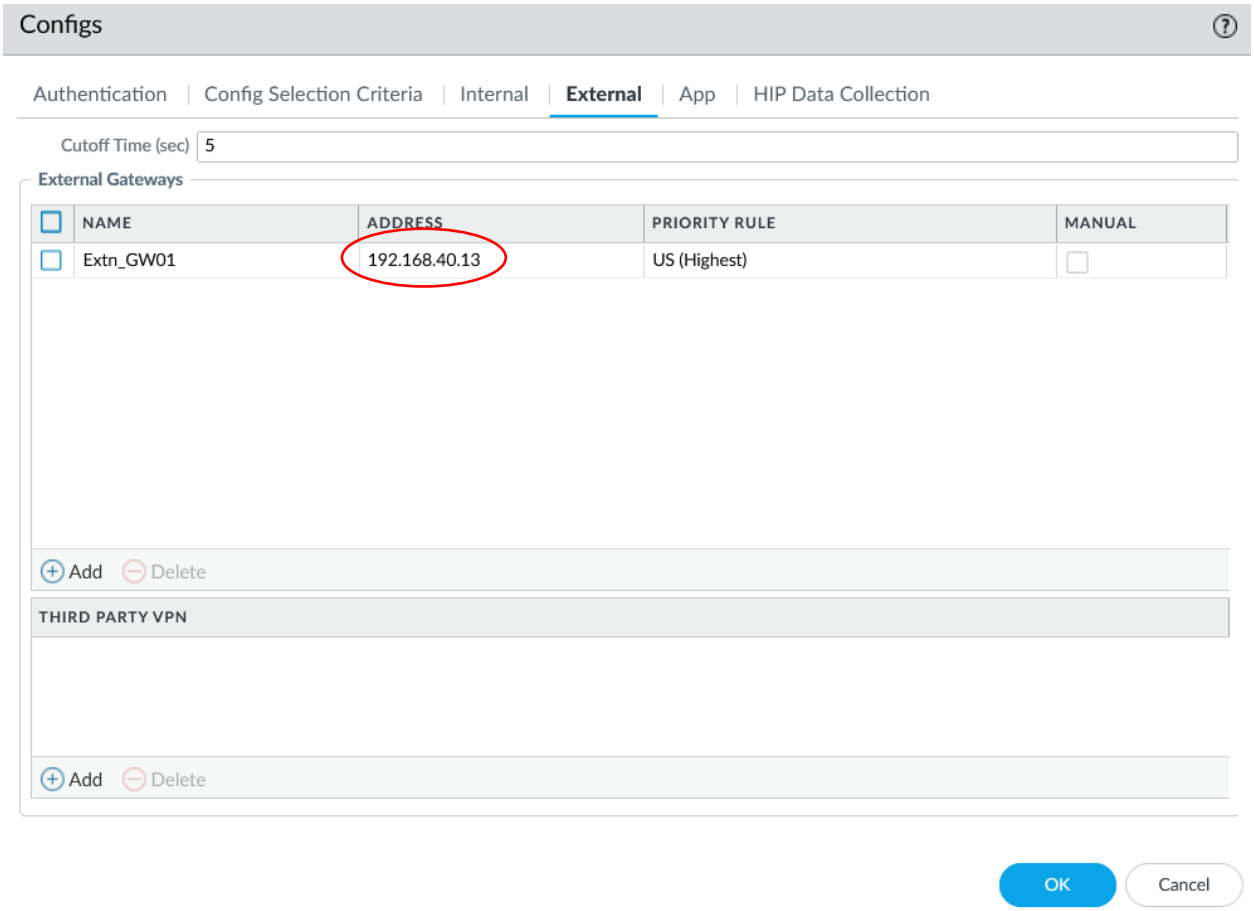
Next, under Agent, add a config, and also add the first and second certificate (Root Cert and Intermediate Cert in my example) in the trusted CA.



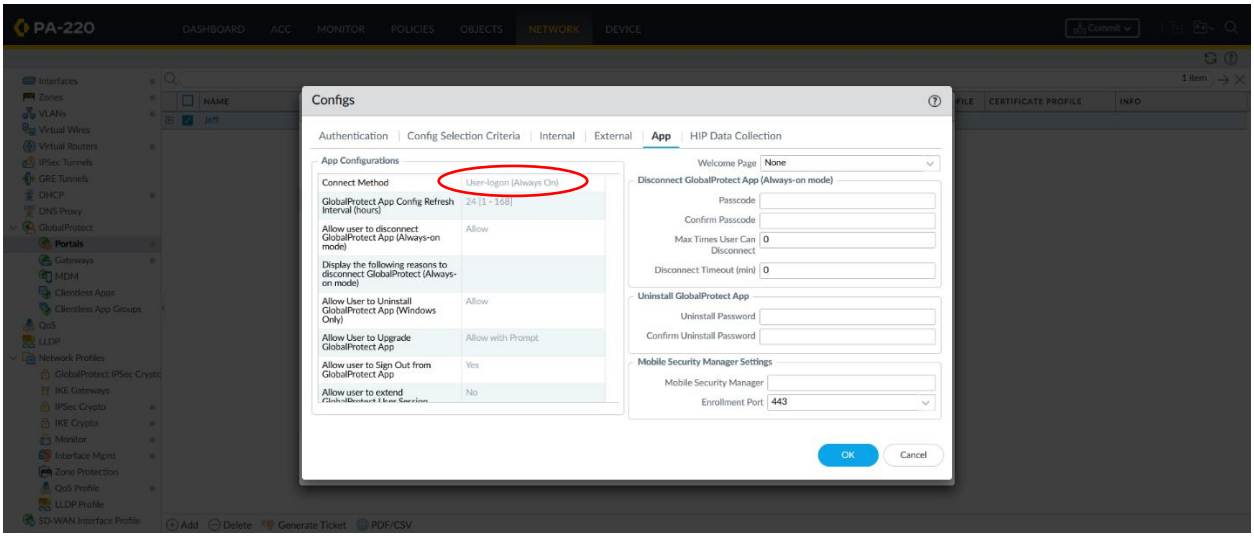
Name it whatever you'd like, set the Certificate to encrypt/decrypt as the first certificate (Root Cert in my case)



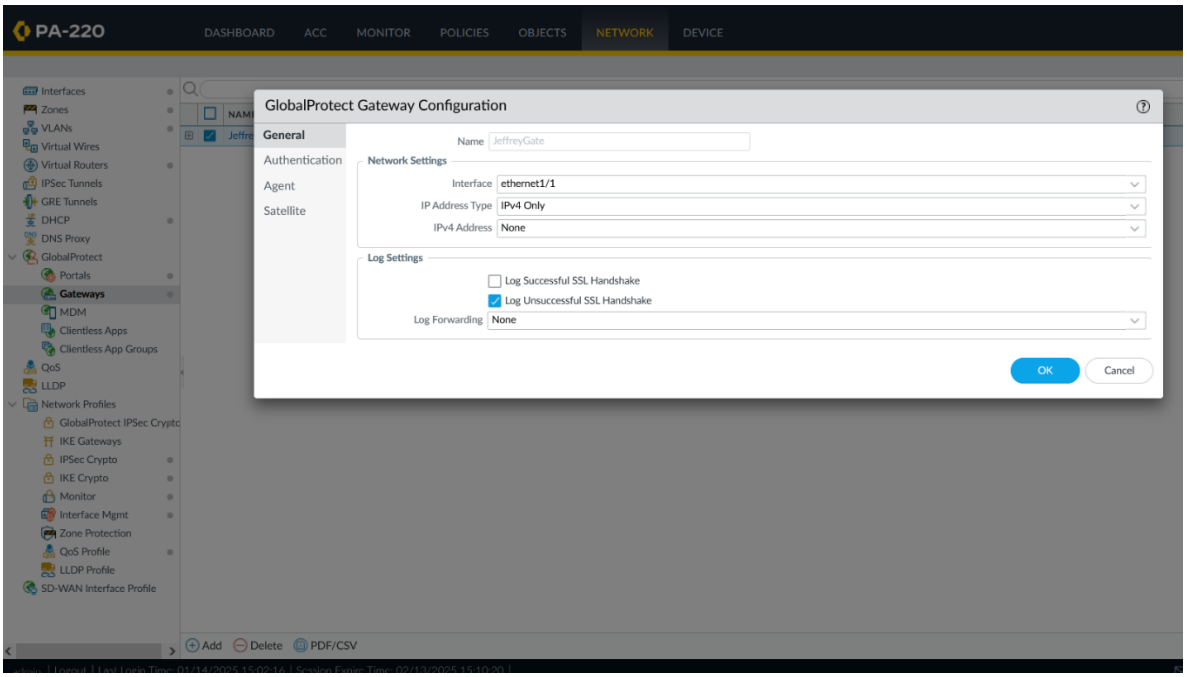
Next, in the External tab, add a gateway with the IP of the DNS server (the same as the Server Certificate's CN)



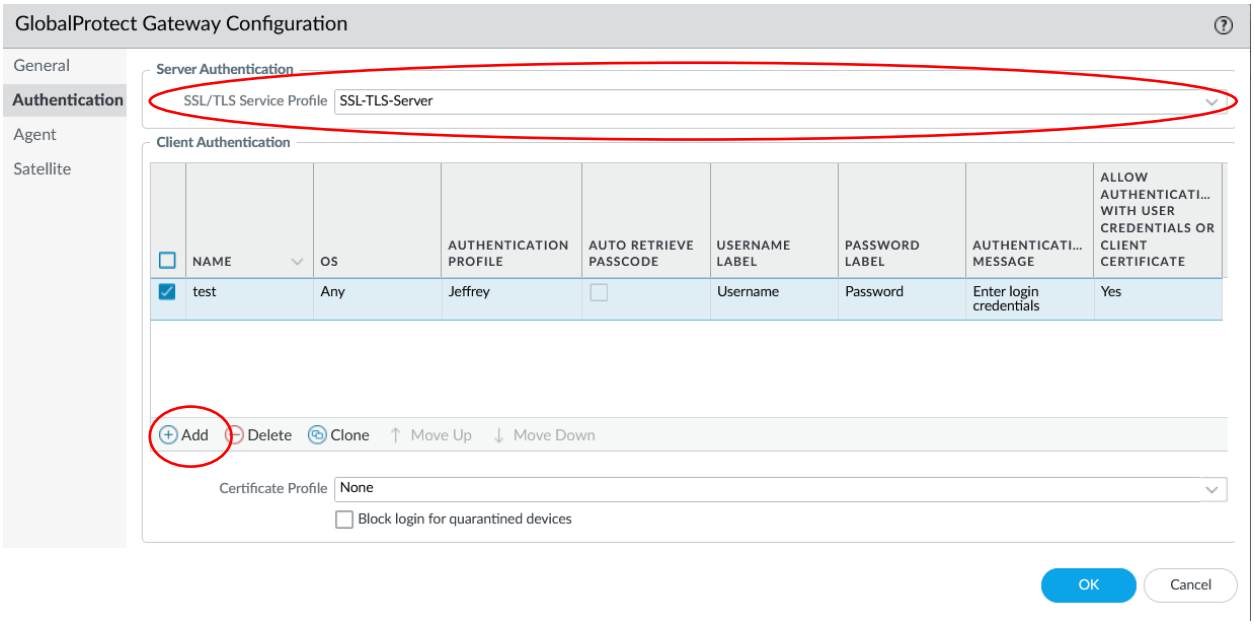
In the App tab, make sure that you've got this setting.



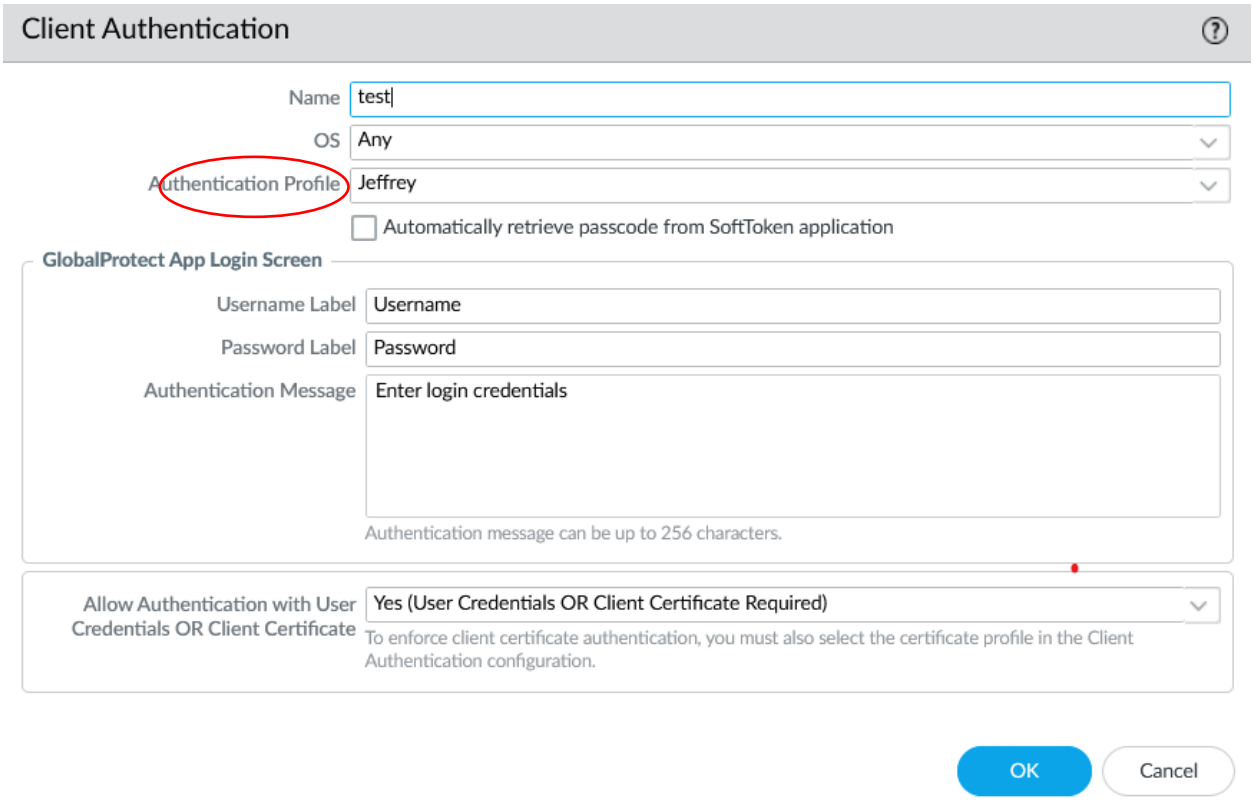
Next, go GlobalProtect>Gateway, and add a configuration.



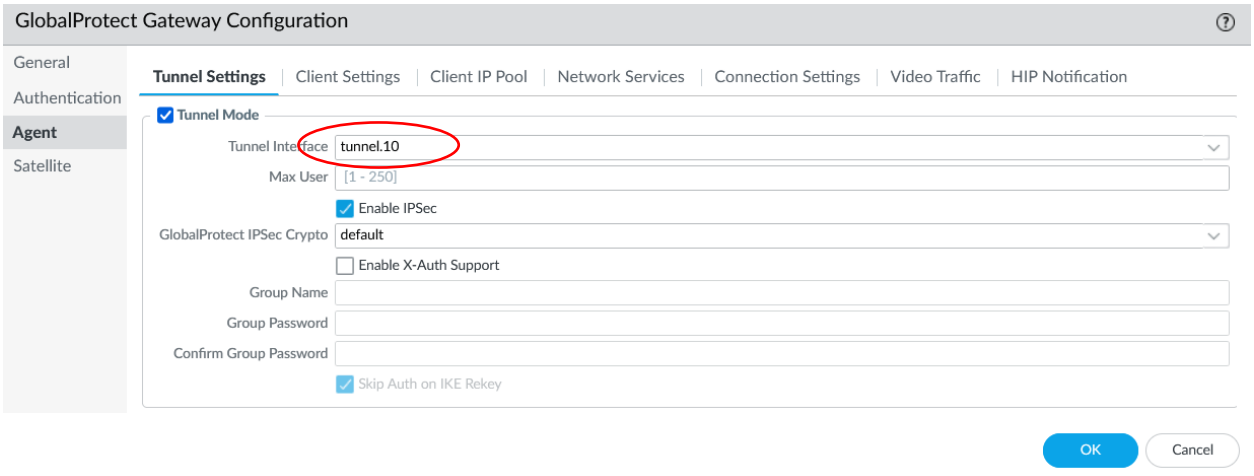
Next, under Authentication, attach the SSL/TLS profile you've made, and also add a Client Authentication profile.



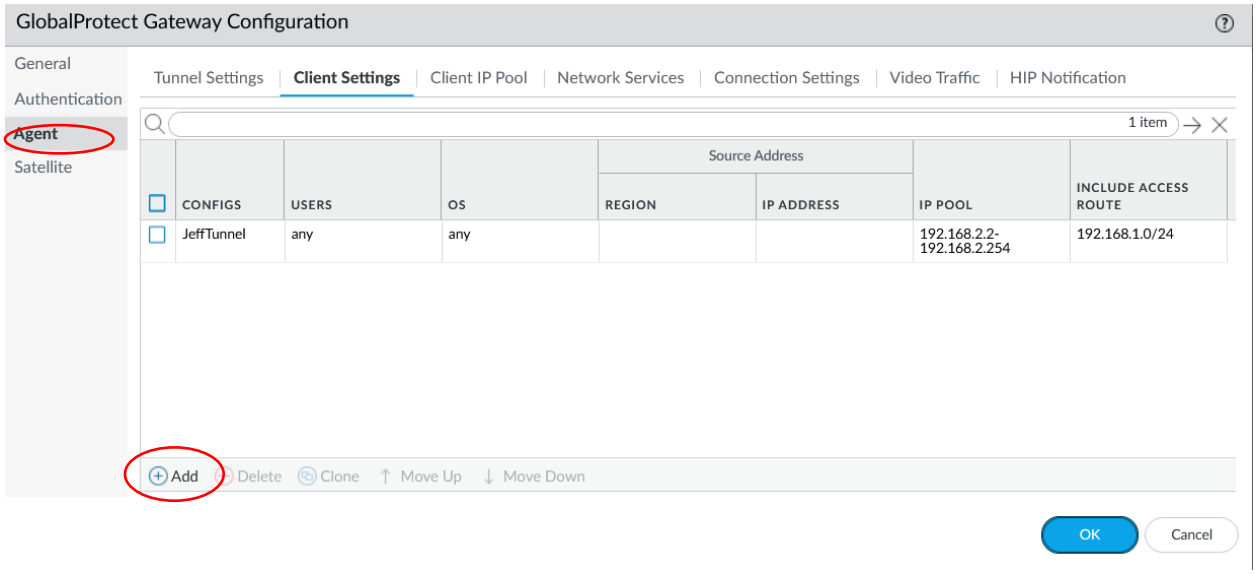
The Client Authentication should look like this.



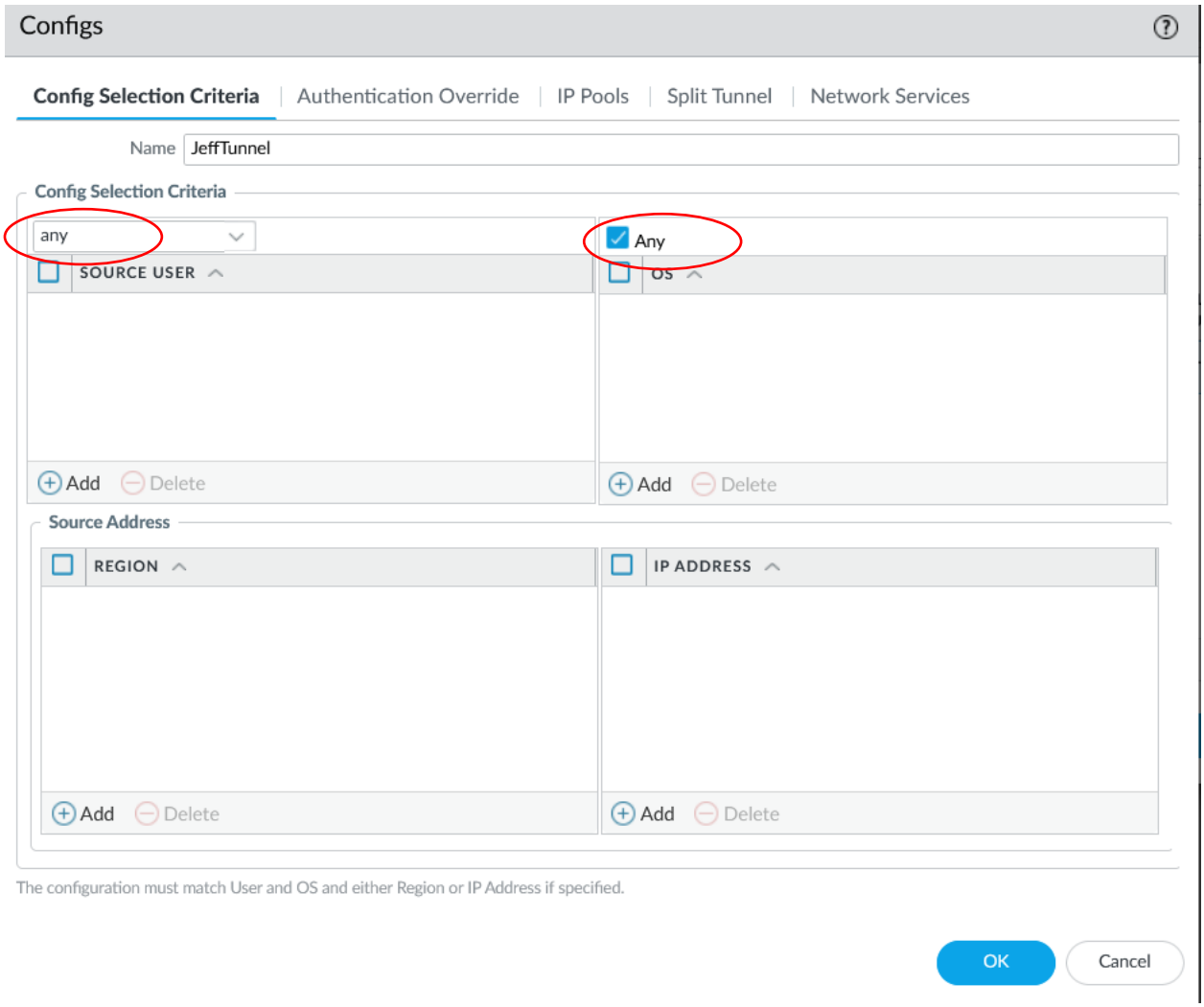
Next, in the Agent tab, put the tunnel you've made as the Tunnel Interface.



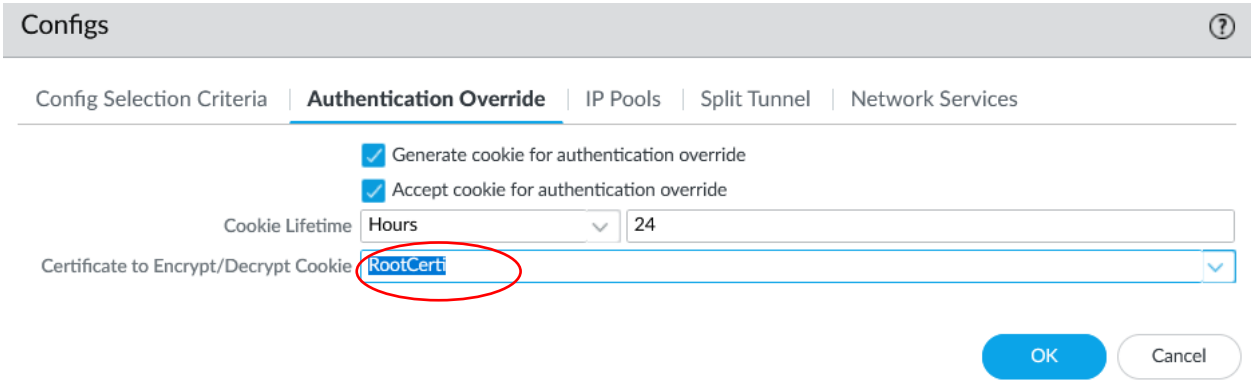
Next, in Client settings, add a configuration.



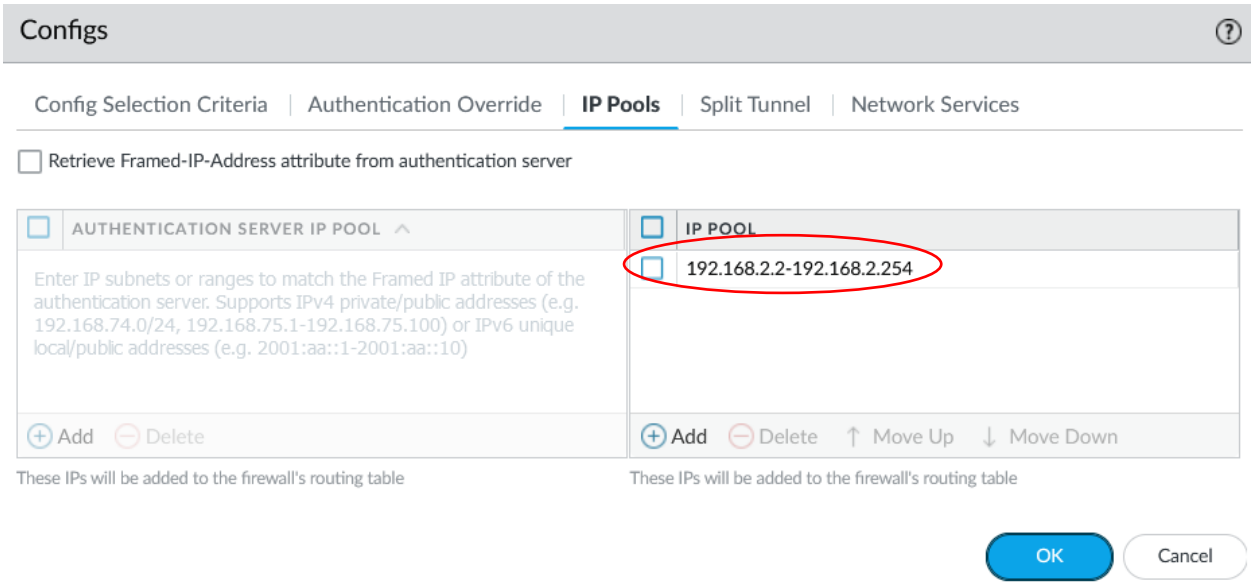
In Config Selection Criteria, the source user and OS should be checked to any.



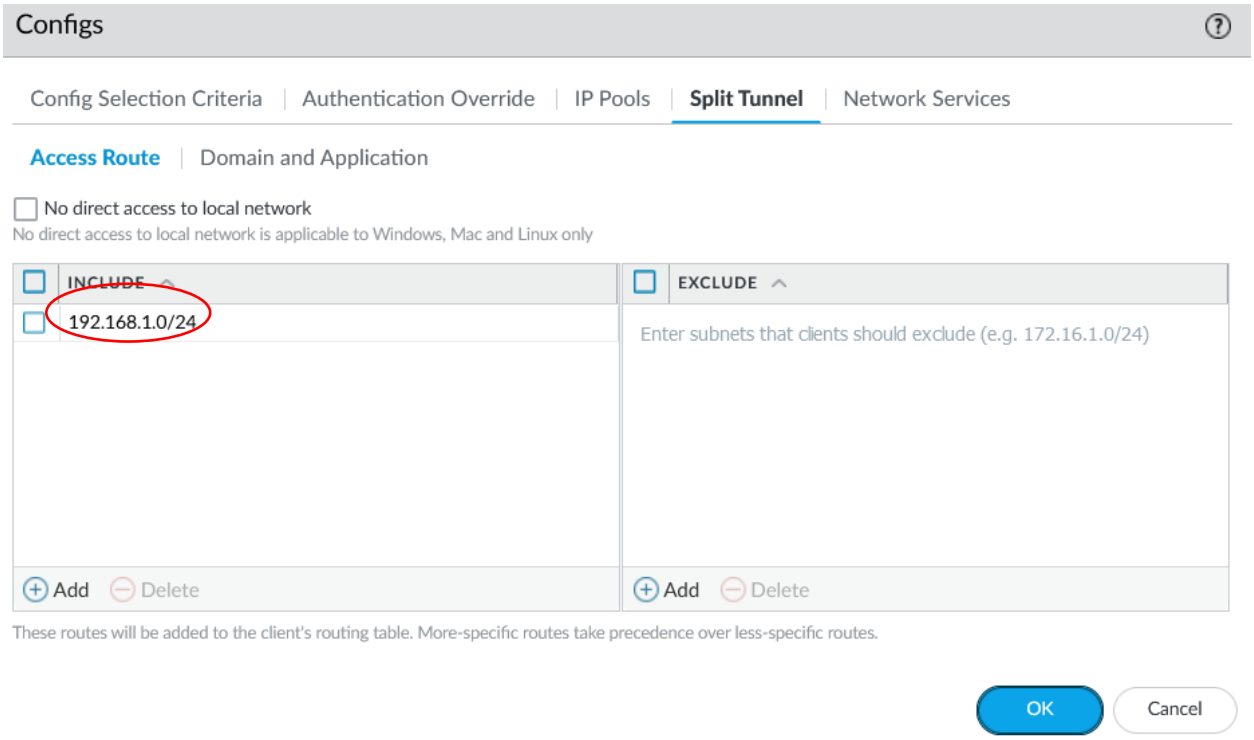
In Authentication Override, the certificate to encrypt/decrypt should be set to your first Certificate (RootCert in my case).



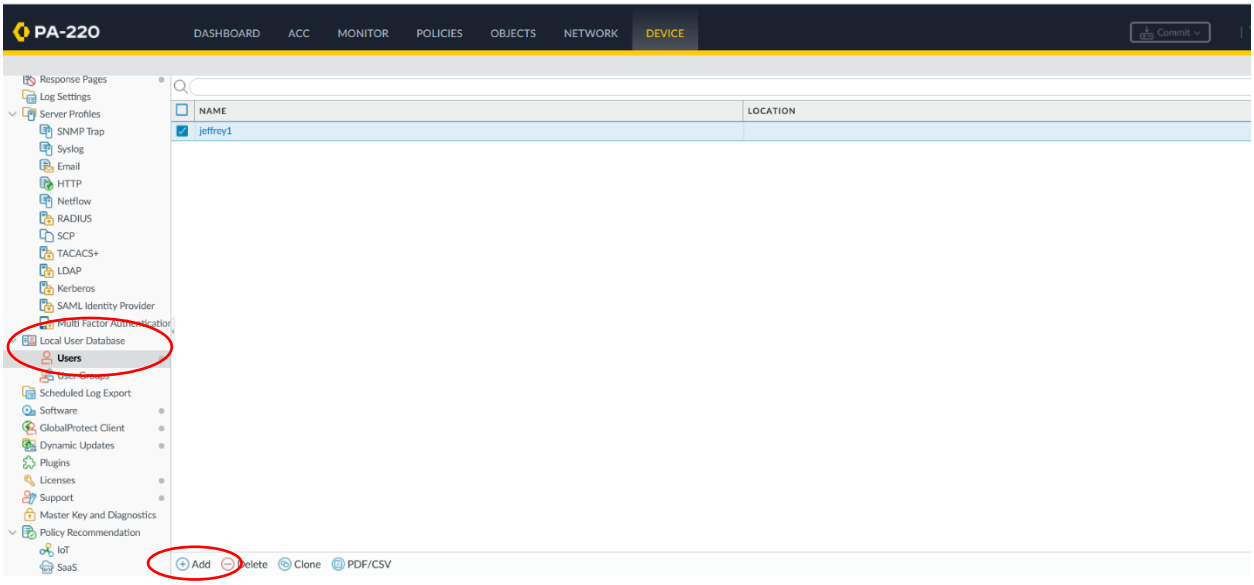
Next, in IP Pools, add an IP pool. Any network except for the one in use by the firewall should suffice.

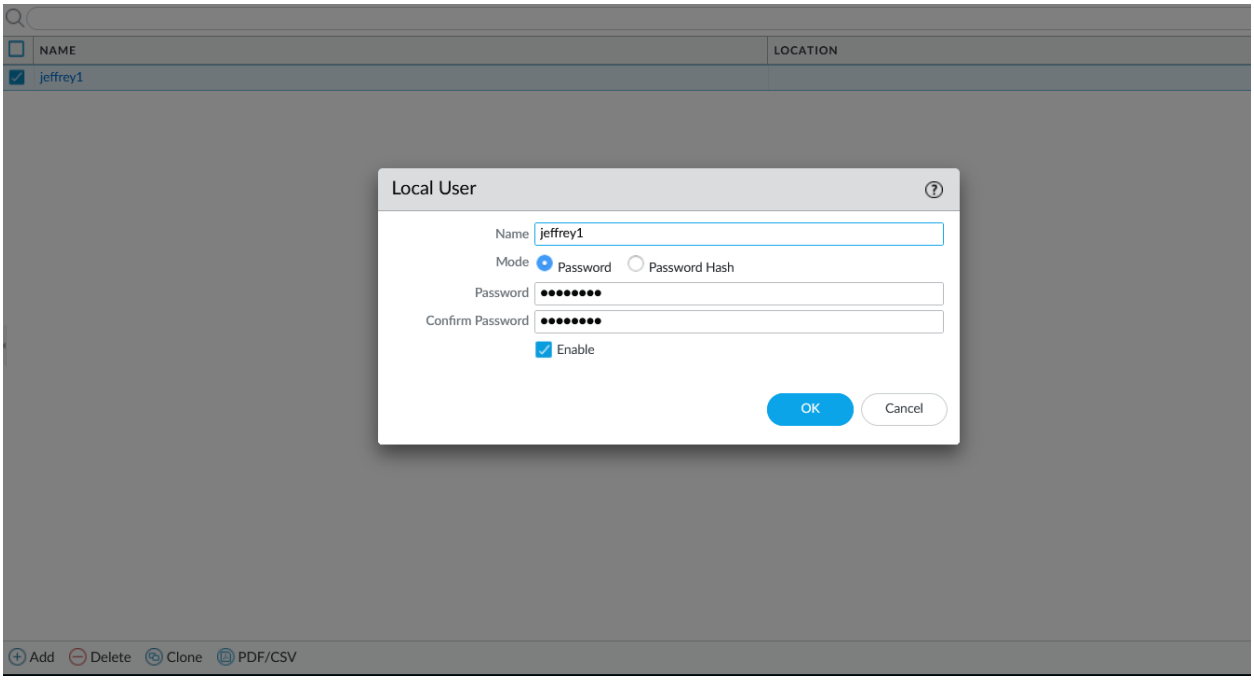


In Split Tunnel, specify your internal network so that the tunnel will only reach it. (Ex. 192.168.x.0/24).

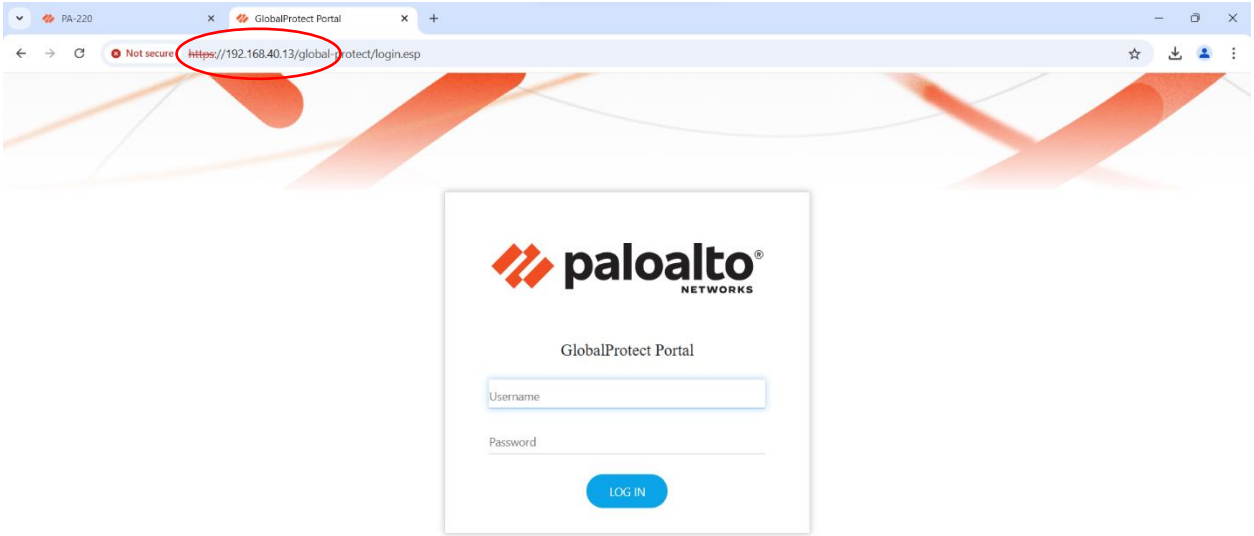


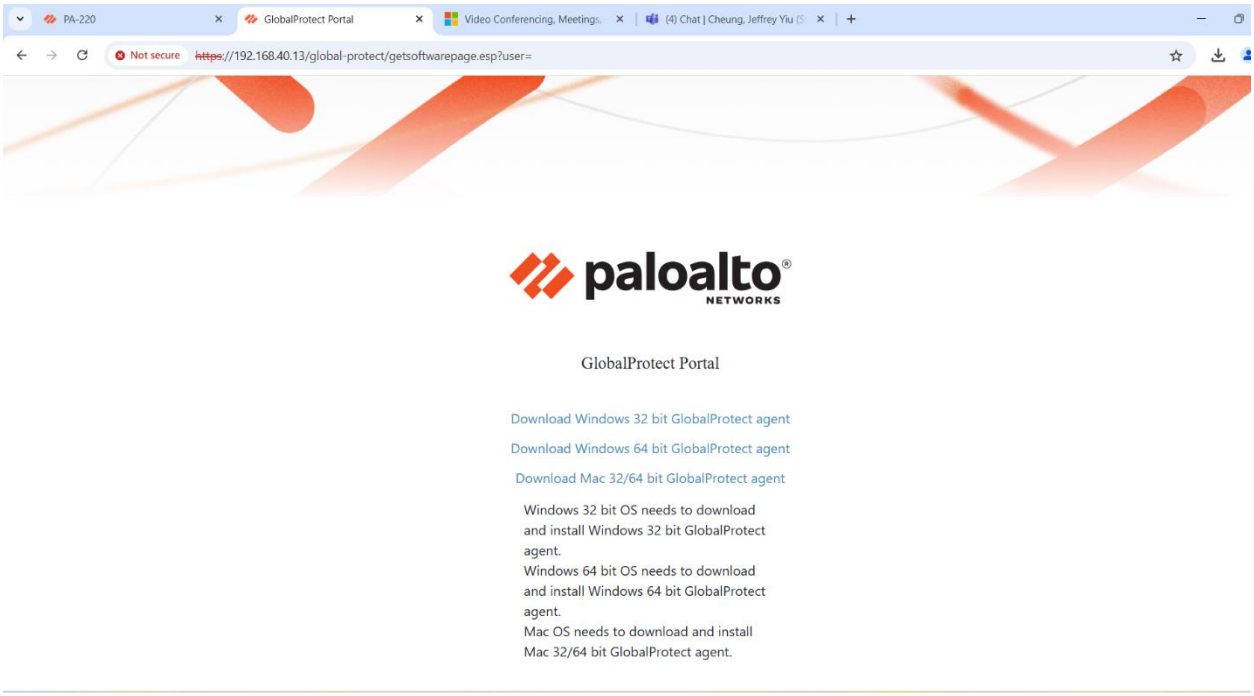
Next, create a local user in Device>Local User Database>Users and give it a password.



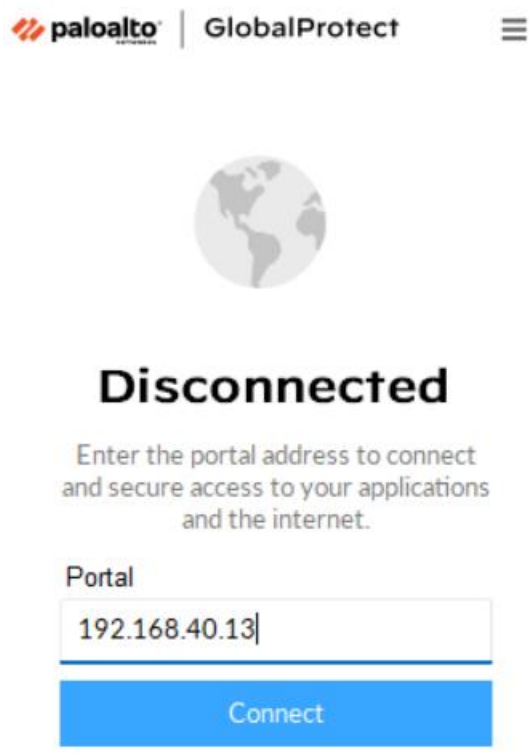


Finally, test if the Global Protect Portal works by visiting the IP of the DNS server. (192.168.40.13 in my case). If it works, login with the user you just created and download GlobalProtect. It should look like this.



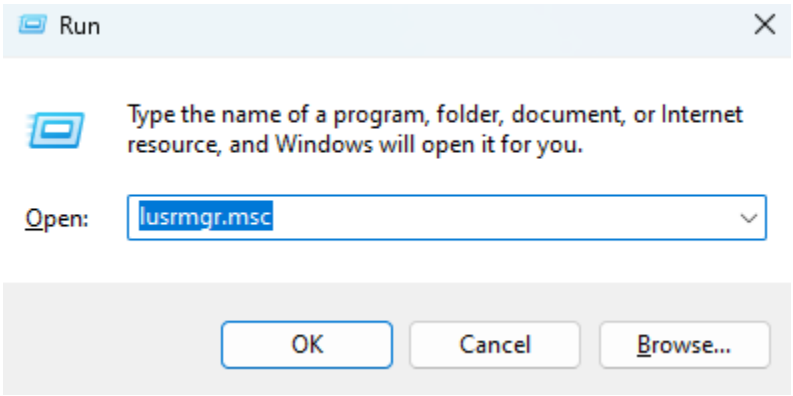


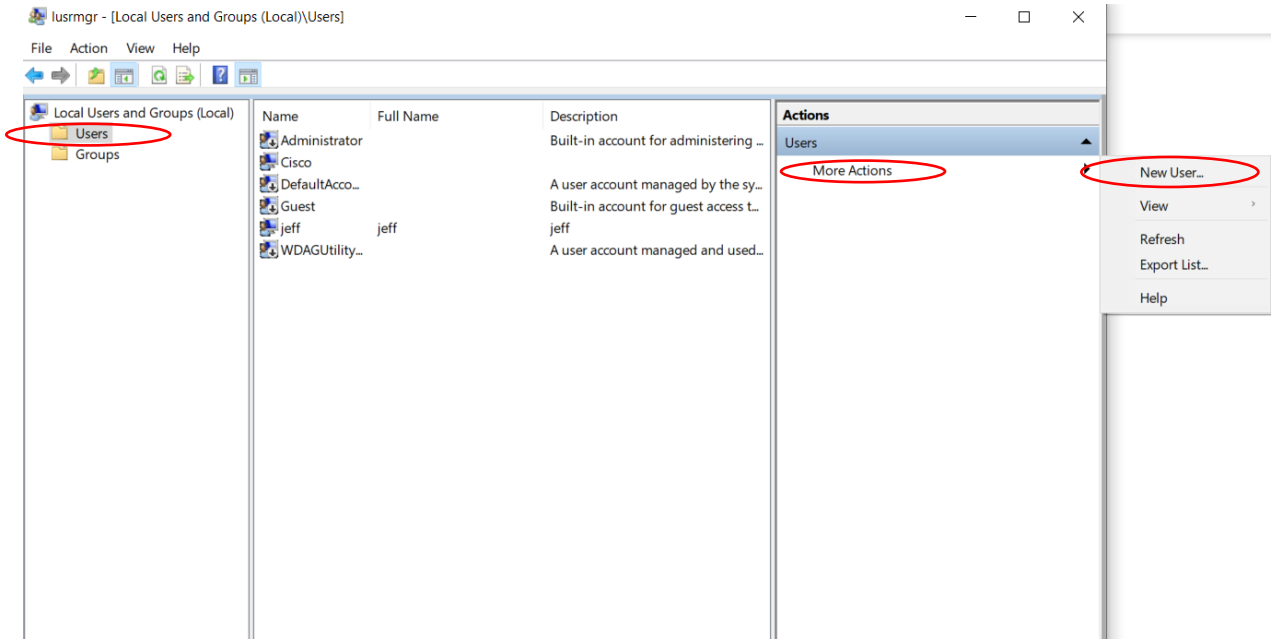
Once it's downloaded, VPN into the internal network using the DHCP address.



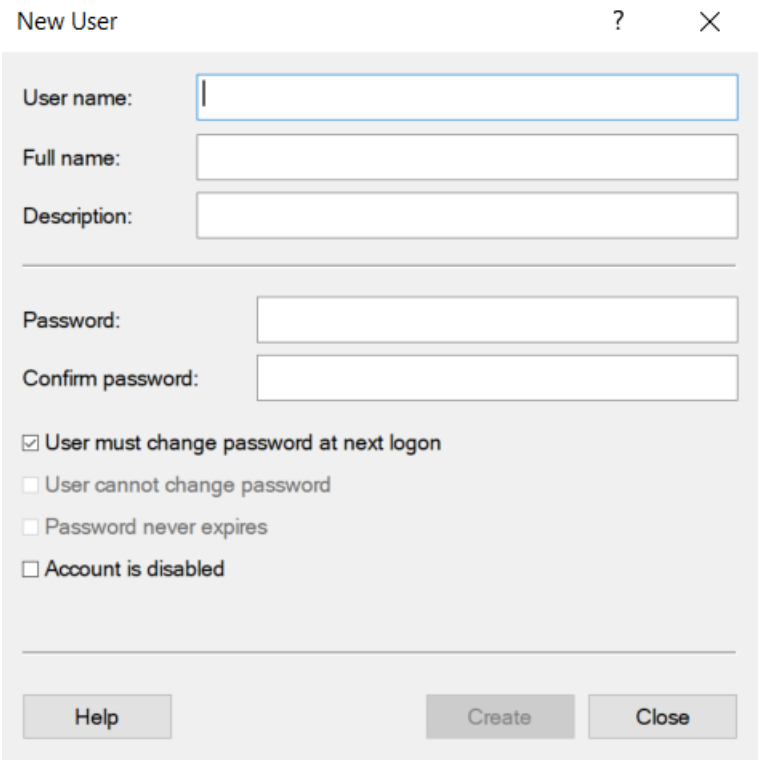
Now, in the device in the internal network, you have to create a user or give an existing user permission to access Remote Desktop.

First, open Run (windows + r on windows, command + space on mac), and type in lusrmgr.msc. This should pop up.





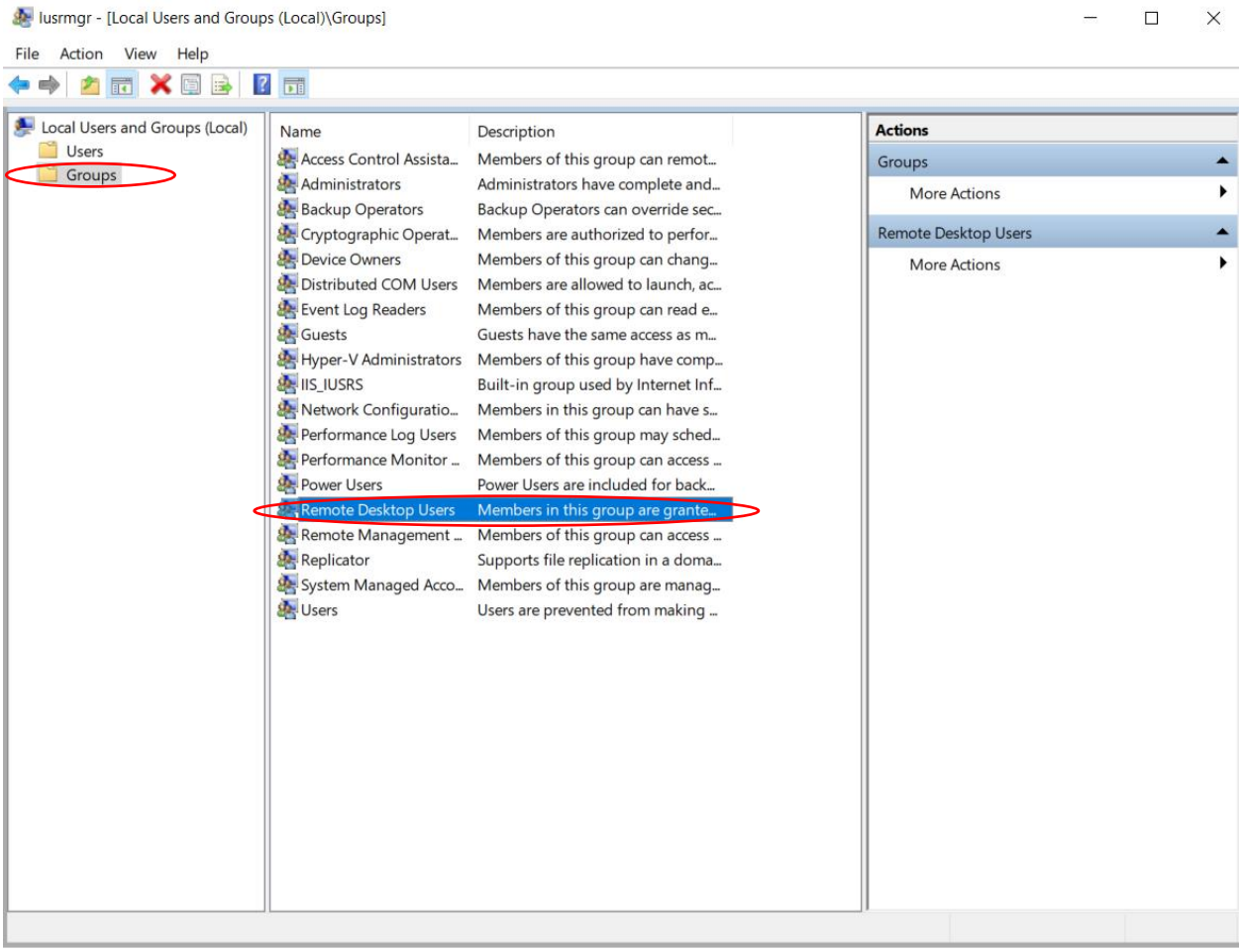
Next, add a user, give it a username and password. You can check off requiring changing password next logon (optional).



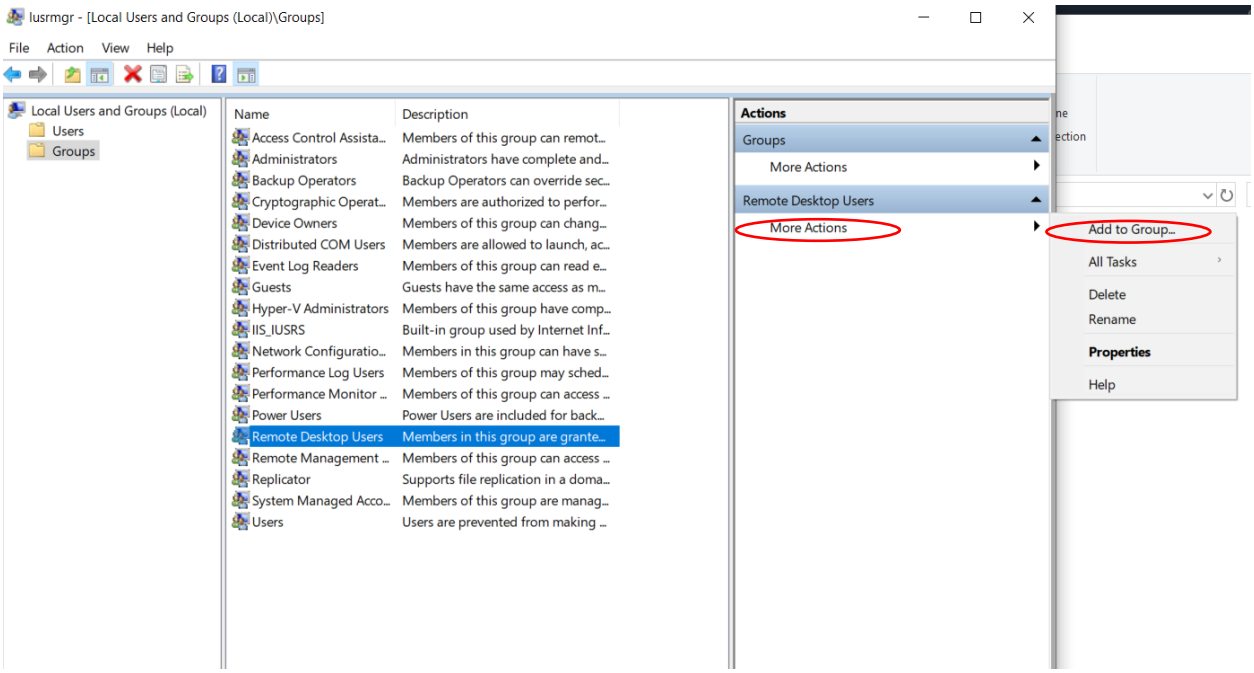
It should look like this.

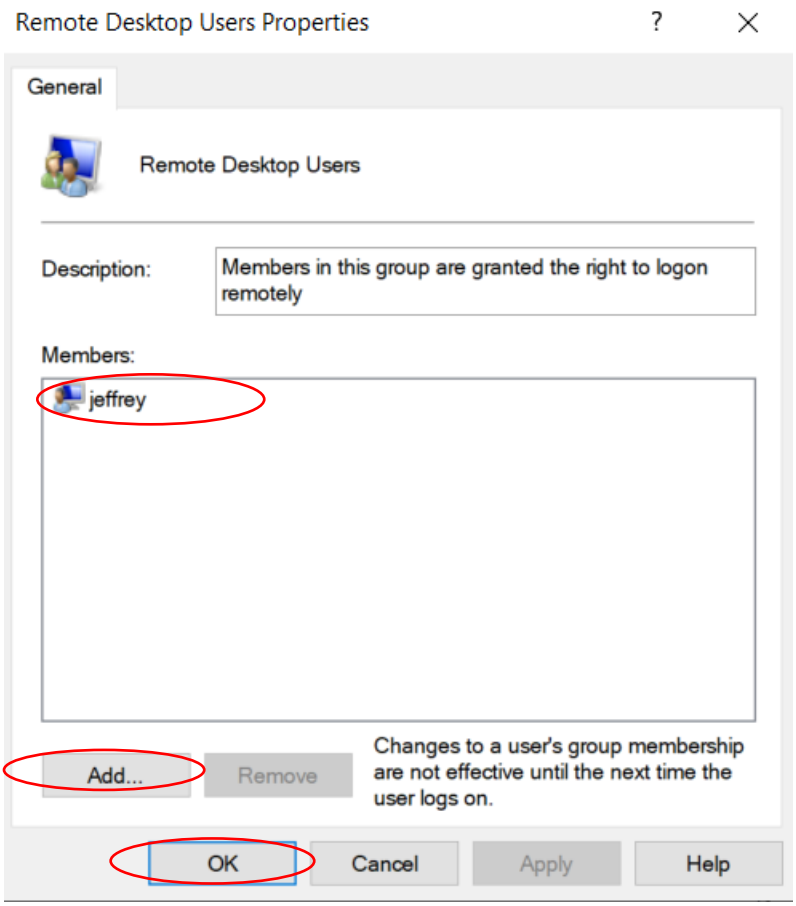
Name	Full Name	Description
Administrator		Built-in account for administering ...
Cisco		
DefaultAcco...		A user account managed by the sy...
Guest		Built-in account for guest access t...
jeff	jeff	jeff
WDAGUtility...		A user account managed and used...

Next, go to groups. There should be a group named Remote Desktop Users.



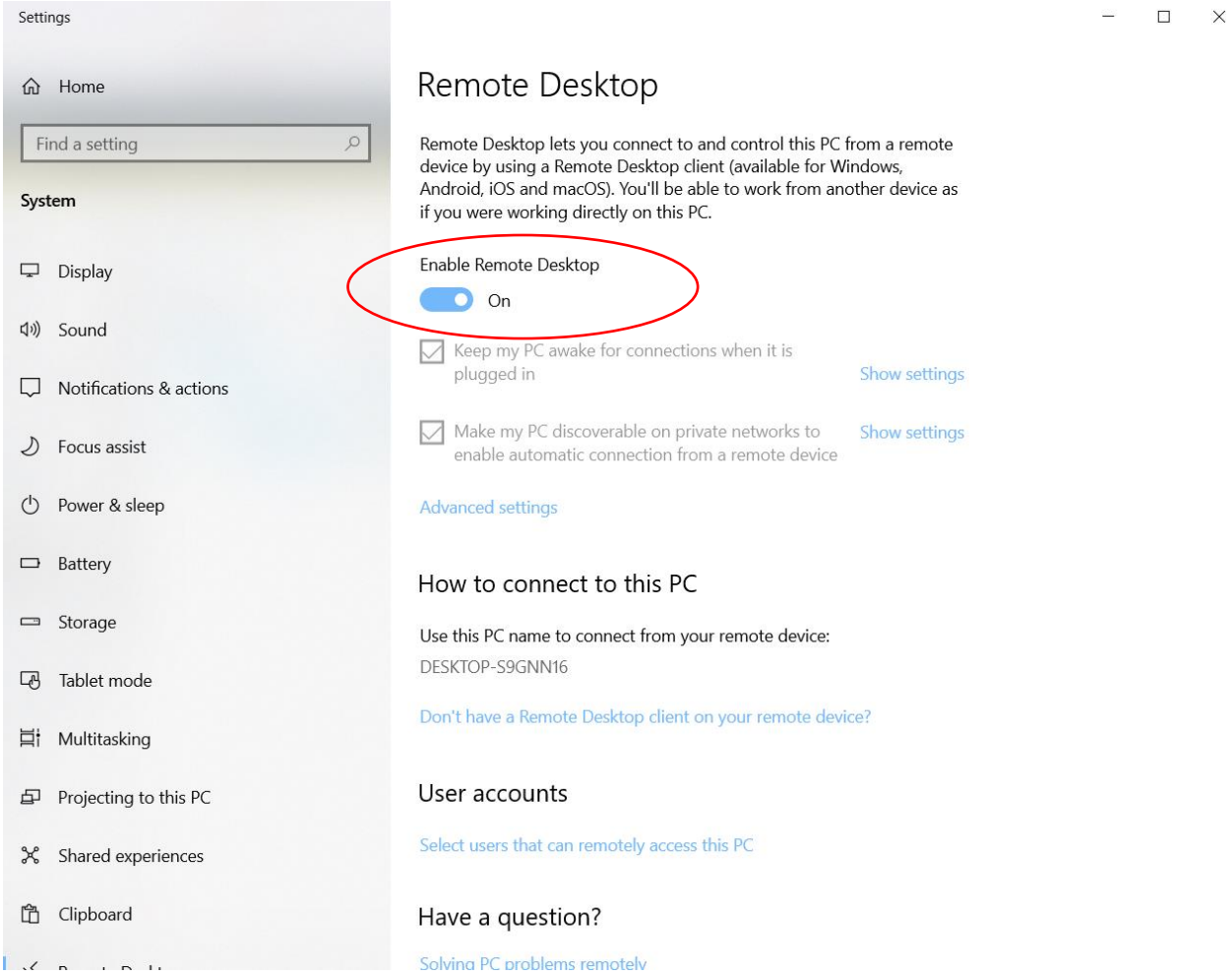
Next, add the user you've made, or an existing user, into the group to give them permission.





If you have reset password on next logon enabled, you have to reset the password before you can use the user.

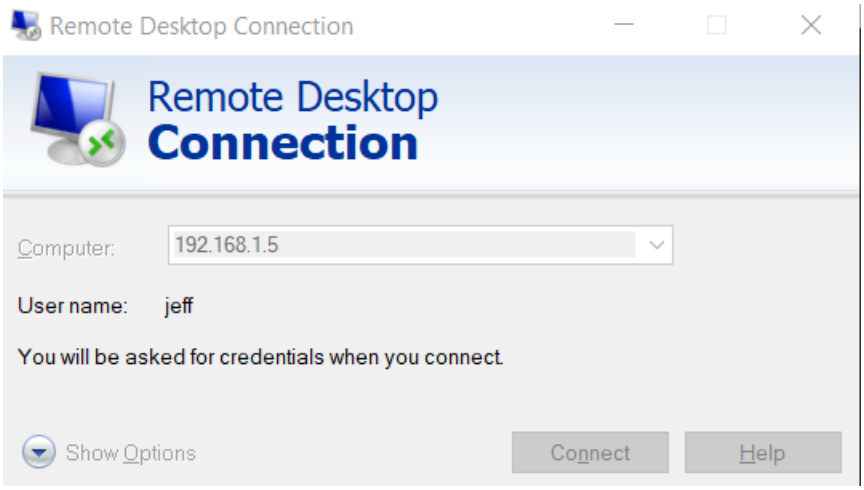
Next, enable Remote Desktop in settings.



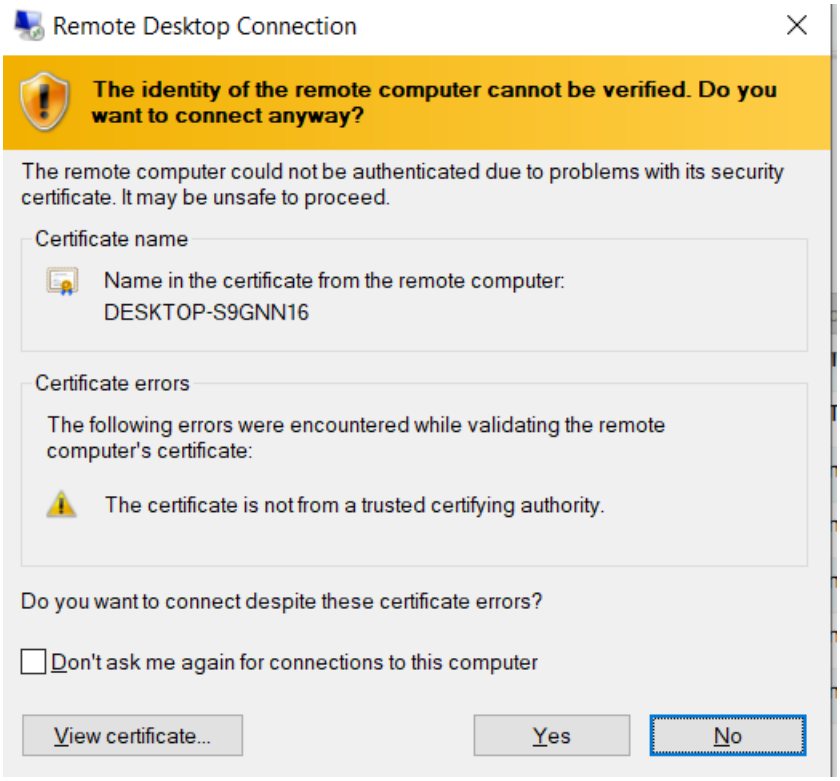
Next, you can use Command Prompt to check the PC's IP address.

```
Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) Ethernet Connection (3) I218-LM
   Physical Address. . . . . . . . . : 54-EE-75-75-94-1D
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::75ec:339b:9a6f:c202%20(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.1.3(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Monday, January 6, 2025 3:06:37 PM
   Lease Expires . . . . . . . . . . : Tuesday, January 7, 2025 3:06:36 PM
   Default Gateway . . . . . . . . . : 192.168.1.254
   DHCP Server . . . . . . . . . . . : 192.168.1.254
   DHCPv6 IAID . . . . . . . . . . . : 206892661
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-2A-C6-6E-3F-54-EE-75-75-94-1D
   DNS Servers . . . . . . . . . . . : 9.9.9.9
                                       1.1.1.1
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

If you've VPN'd into the network, just open up Remote Desktop Connection and connect with the IP of the PC you just found.



If it is successful, you should be prompted with this.

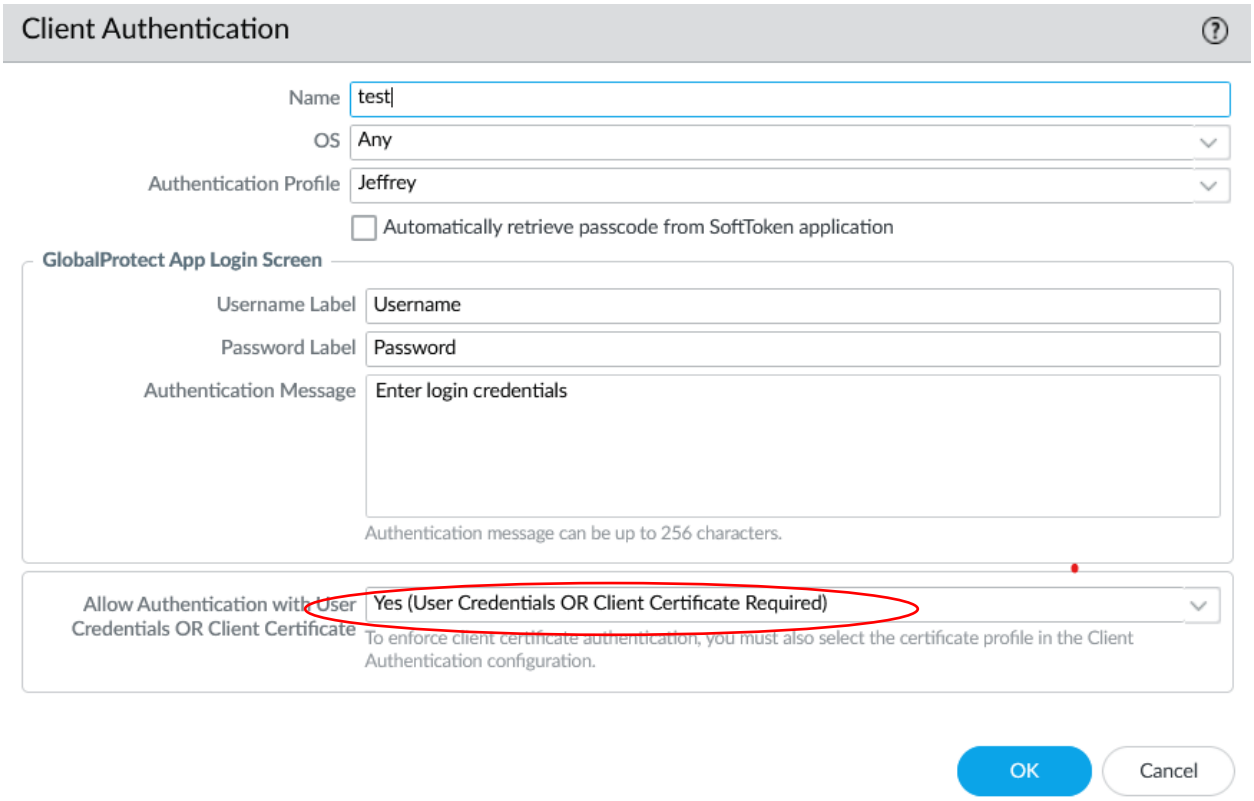


Just click yes, and then it is all set.

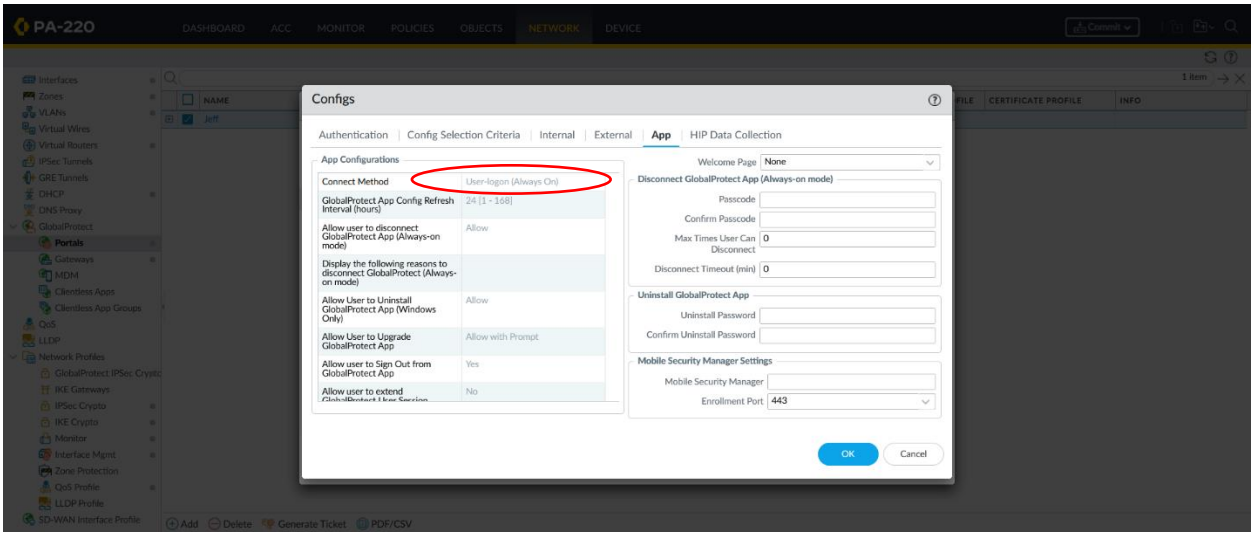
Problems

One of the first problems we encountered was unable to reach the portal despite having the configurations right. One possible issue is that common browsers detect dangerous sites, and the IP of the DNS server gets flagged if you don't use secure hypertext transfer protocol (https). The commit time of the firewall is also time consuming, taking almost 10 minutes every time. When I was debugging, it took a long time to find the bug due to having to commit every time to see the results. If GlobalProtect VPN has trouble recognizing your certificates, there are many details that may contribute to this issue. First, for settings that asks for authentication with user

credentials and/or client certificate, select YES.



Next, it could be some details in the Portal configuration. In the App tab, there are some important details that may turn into an issue. However, it may be hard to tell because all the greyed out.



Conclusion

In conclusion, GlobalProtect VPN is a powerful tool that can mitigate threats and allow private and secure remote access to users. GlobalProtect VPN uses advanced protocols like IPsec and

AES encrypting algorithms to ensure data is encrypted securely and reliably. It also allows users to remote desktop and bypass physical and geographical limitations. GlobalProtect VPN can benefit a wide range of users, from individual use to corporate organizations.

FortiGate FortiGate-40F

Setting a Fortinet Firewall as a SOHO router

Jeffrey Yiu Cheung

Purpose

This lab showcases how to factory reset a FG-40F and how to set up a SOHO router on the Fortinet firewall with an access point.

Background information

SOHO router, AKA Small Office/Home Office router configurations are designed to support small businesses and small offices, which is a good fit for the Fortinet FG40F firewall's specifications. They are designed with functions that maximize security, and performance for small offices. The Fortinet FG40F has a user-friendly GUI (Graphic User Interface).

In the modern age, most offices are in large buildings and uses enterprise routers, however, SOHO routers can still benefit many occupations, such as lawyers, authors, researchers, consultants, accountants, etc.

Fortinet, Inc. is a cybersecurity company headquartered in Sunnyvale, CA. it is a leader in the Cybersecurity industry, securing over 700,000 enterprises and organizations worldwide. It leads the industry in training individuals and has made innovations to incorporate AI into their business. Fortinet made it their mission to educate 1,000,000 people by 2026.

With new technologies constantly enabling the ease of interaction with the web, more information is being uploaded every second. There are useless information, educational information, but there are also sensitive, personal information in the web. To prevent these cybersecurity threats, Fortinet offers cybersecurity devices and programs like firewalls malware prevention programs.

A factory reset is a function that erases and resets all configuration to original factory settings. When encountering a device that is already pre-configured, a factory reset allows us to still use a device that is already set with a password and start from a clean environment.

An Access Point (AP) is a device that allows wireless connectivity to users. It is often used to extend WiFi.

WiFi, AKA Wide Fidelity, is a wireless technology that uses radio waves to wirelessly provide internet access. It connects a local area, and is designed for SOHO uses. It provides flexibility as it is wireless and is less equipment oriented as traditional wired connections. However, WiFi can be easily overwhelmed with high traffic, many devices, environment variables…etc, potentially leading to slower speeds.

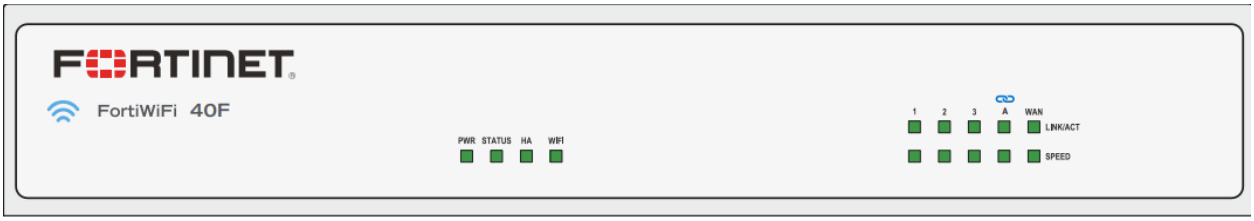
DHCP (Dynamic Host Configuration) is a network protocol that automatically assigns IP addresses to users. Without it, admins would have to manually administer IPs to users for them to connect to the internet, taking more time, effort, and money.

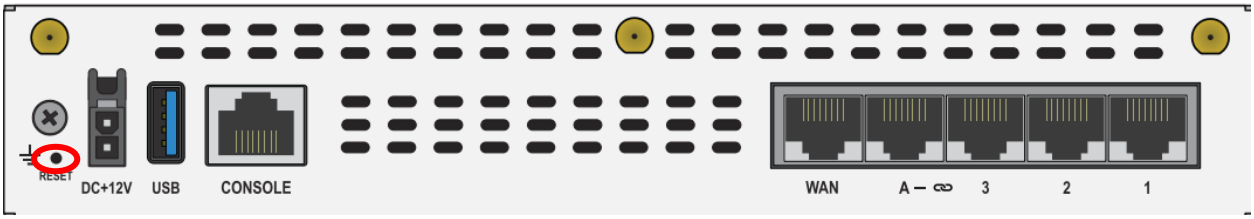
GUI or Graphics Users Interface, is a really good aspect of the Fortinet Firewalls. Fortinet firewall GUI is clean and user-friendly, and an overall great upgrade from other firewalls. GUI is

an underrated and important aspect of firewalls in my opinion. It can have a big impact on efficiency, reduced errors, and improved user experiences.

Lab summary

First, to start with a clean configuration, you may want to factory reset first.

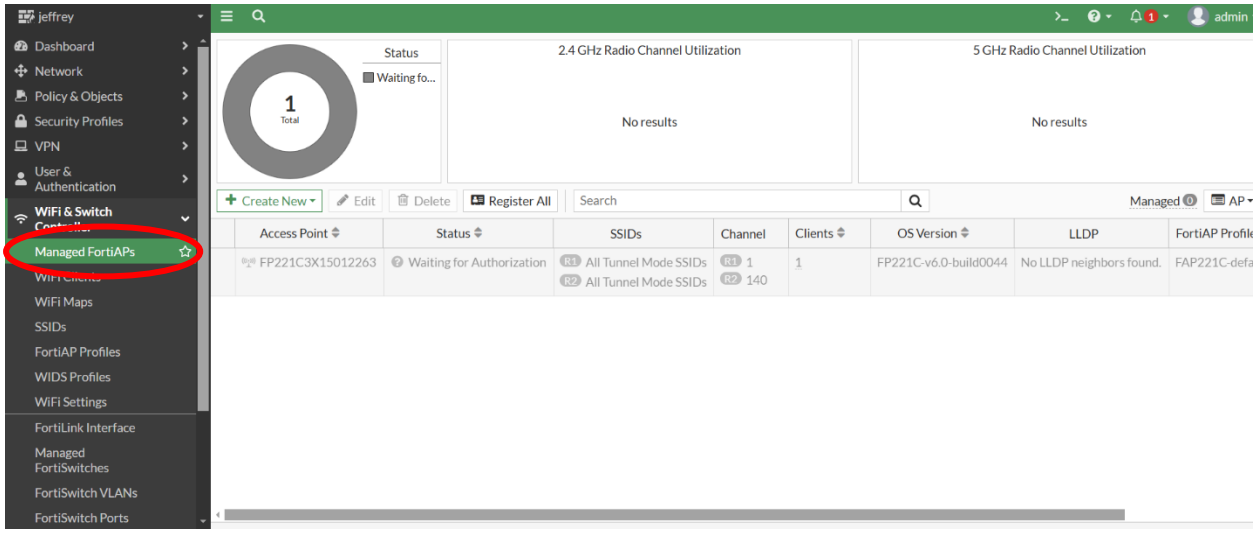


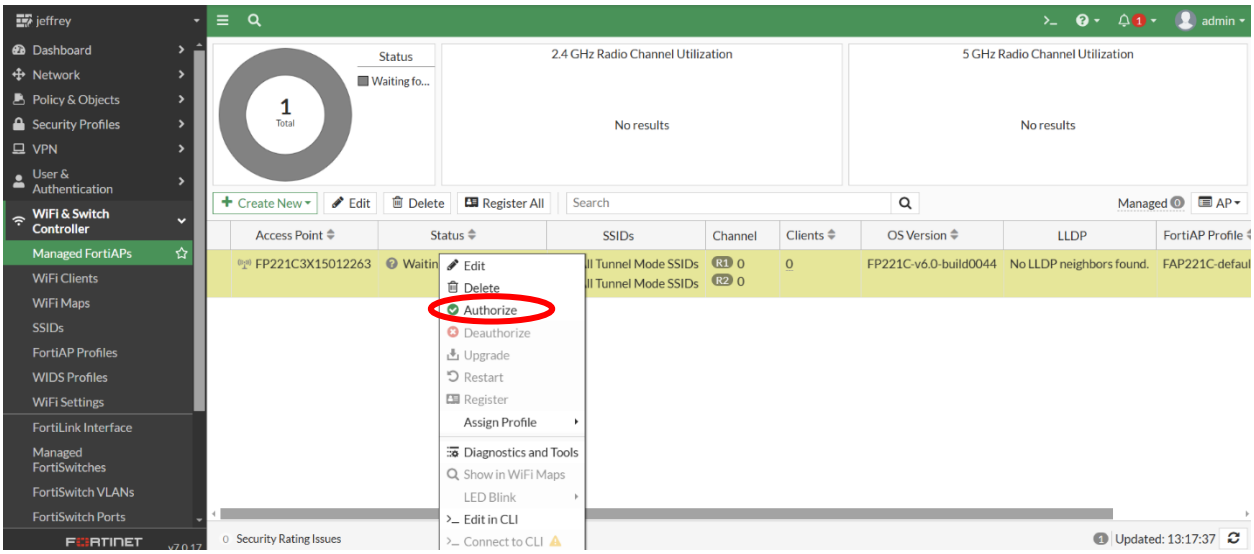


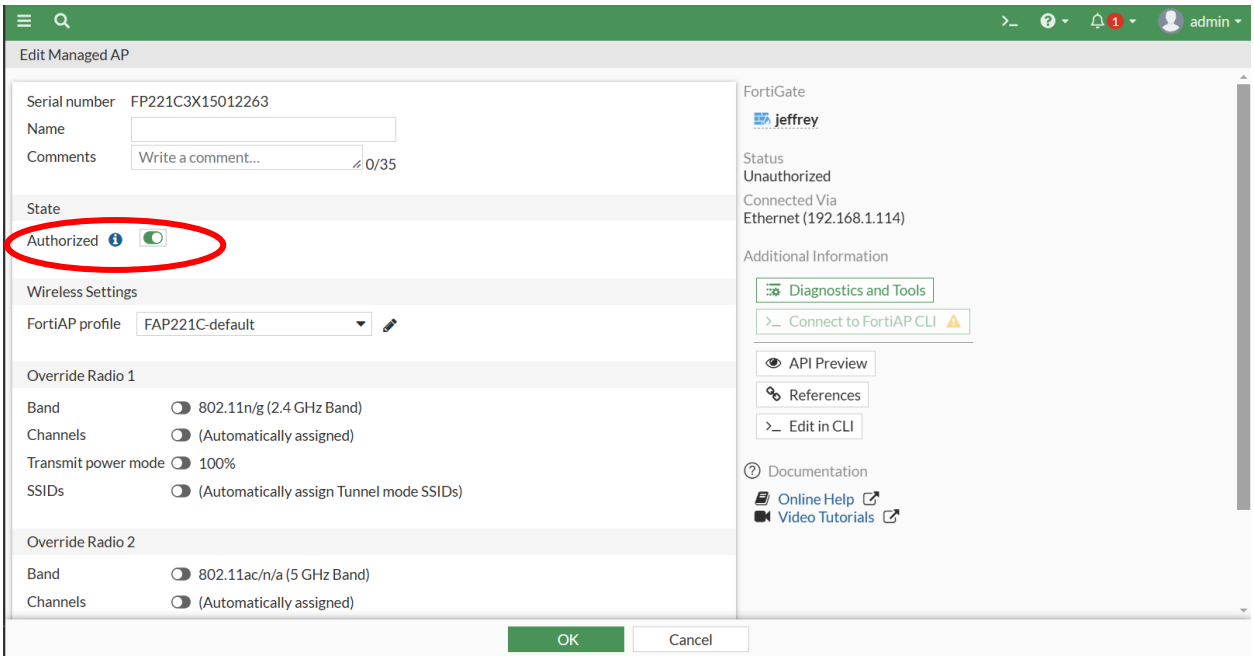
To factory reset, you need to power cycle the device first, then press and hold the factory reset button (you're going to need a pin) until the lights on the switch start flashing. Then wait for the reboot.

Once with a new config, you can start configuring SOHO on the firewall.

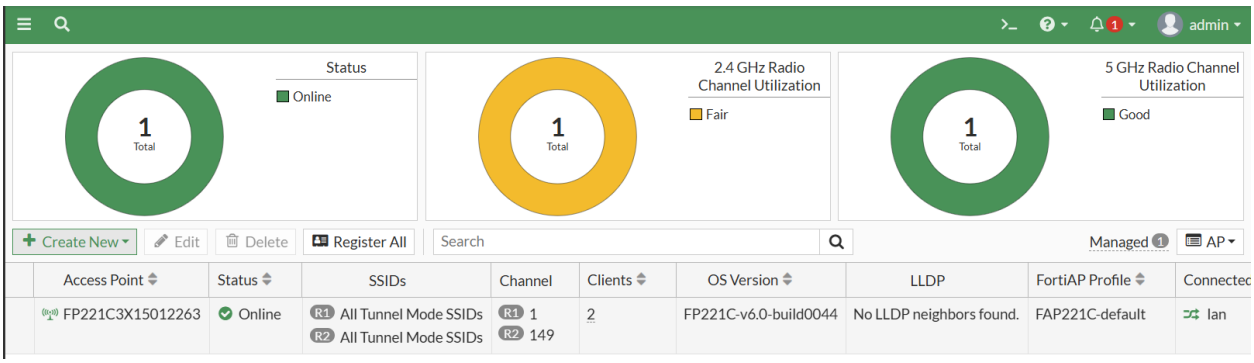
First, when you plug the access point in, the AP will be offline at first. You have to authorize it in Manage FortiAPs.



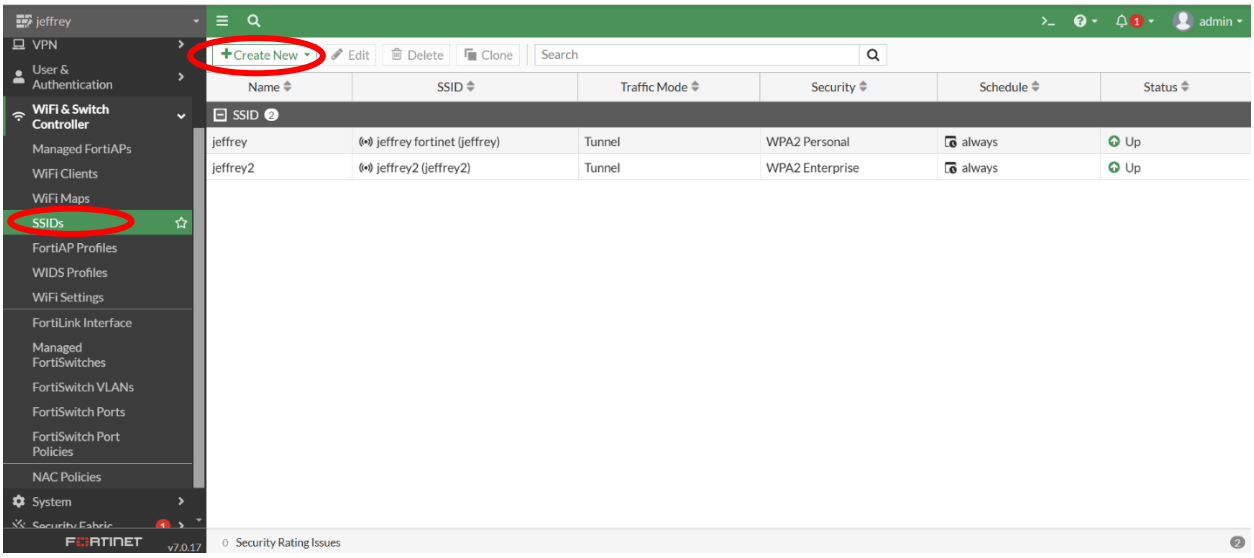




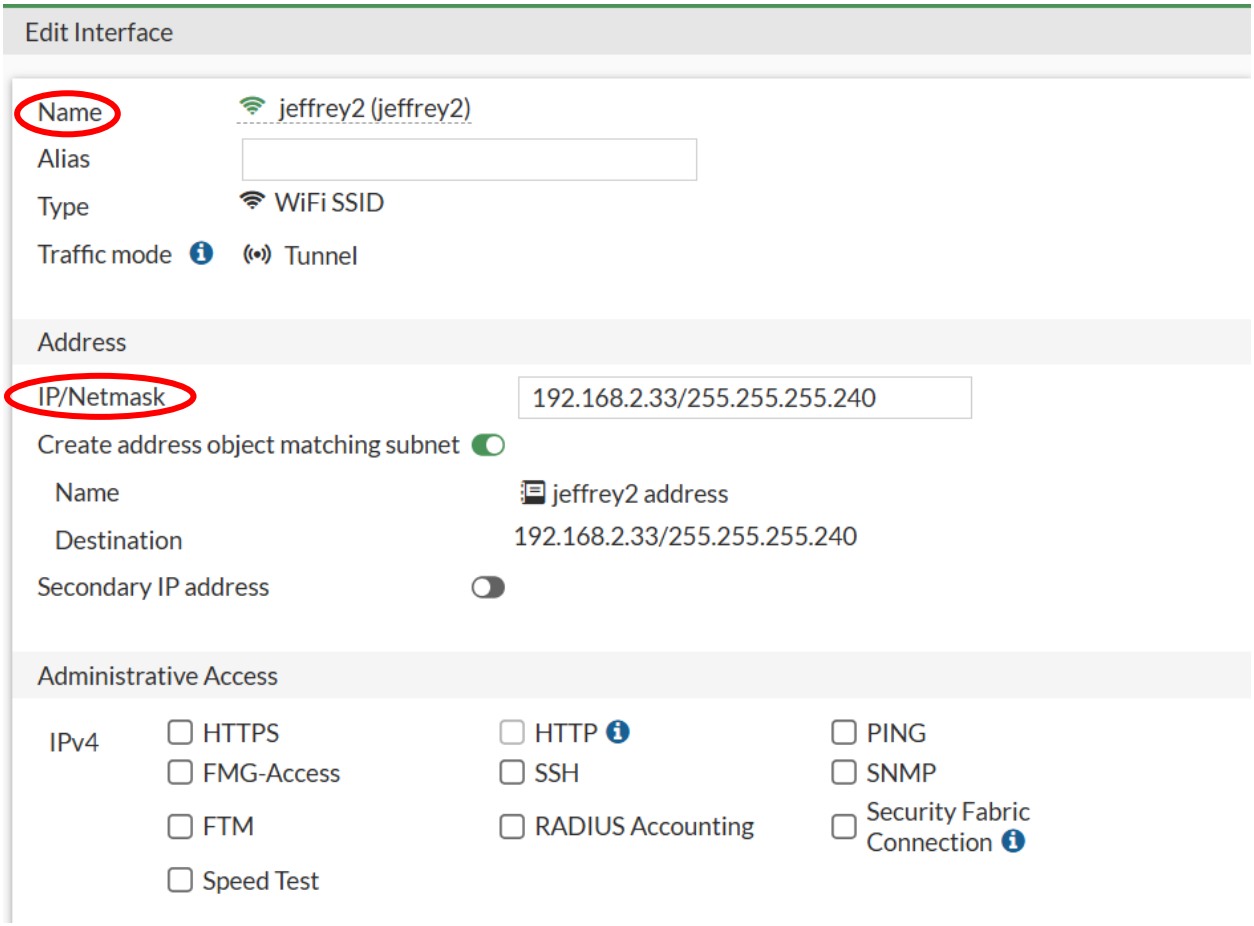
Once authorized, it should turn on. Wait for the lights to flash, and once stable, it will be functional. The interface should look like this after.



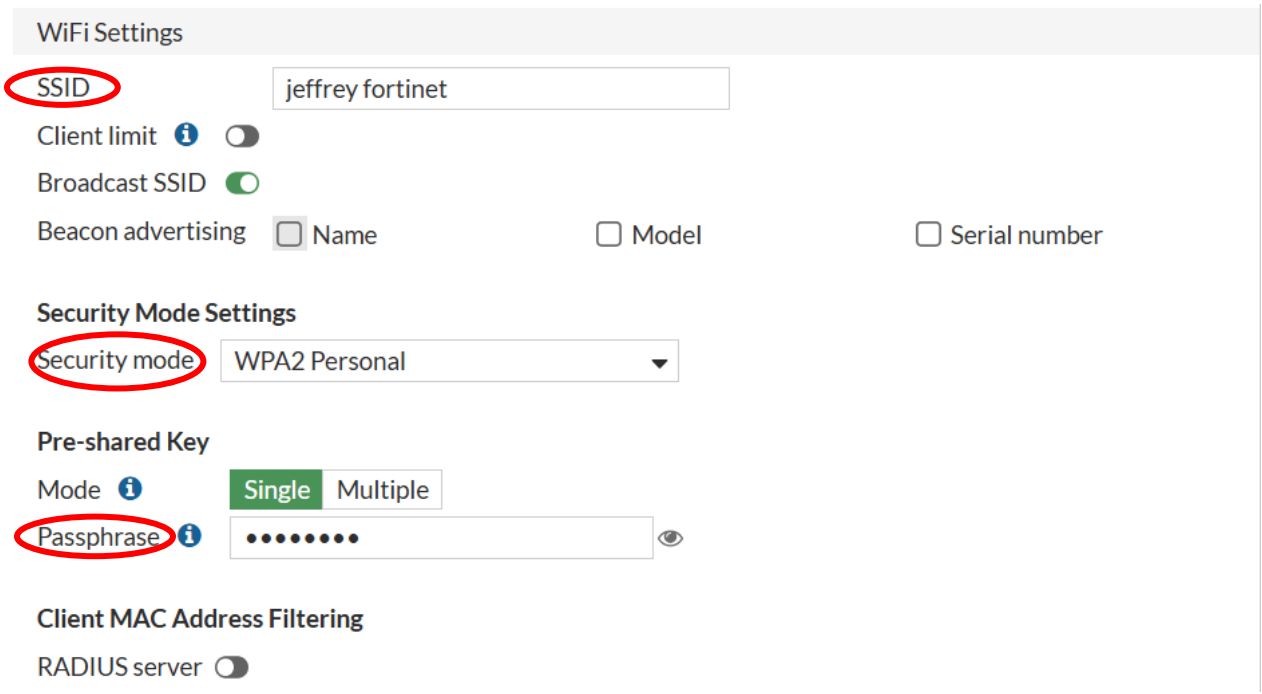
Next, in SSIDs, create 2 new SSIDs, one of them should be for enterprise while the other is personal.



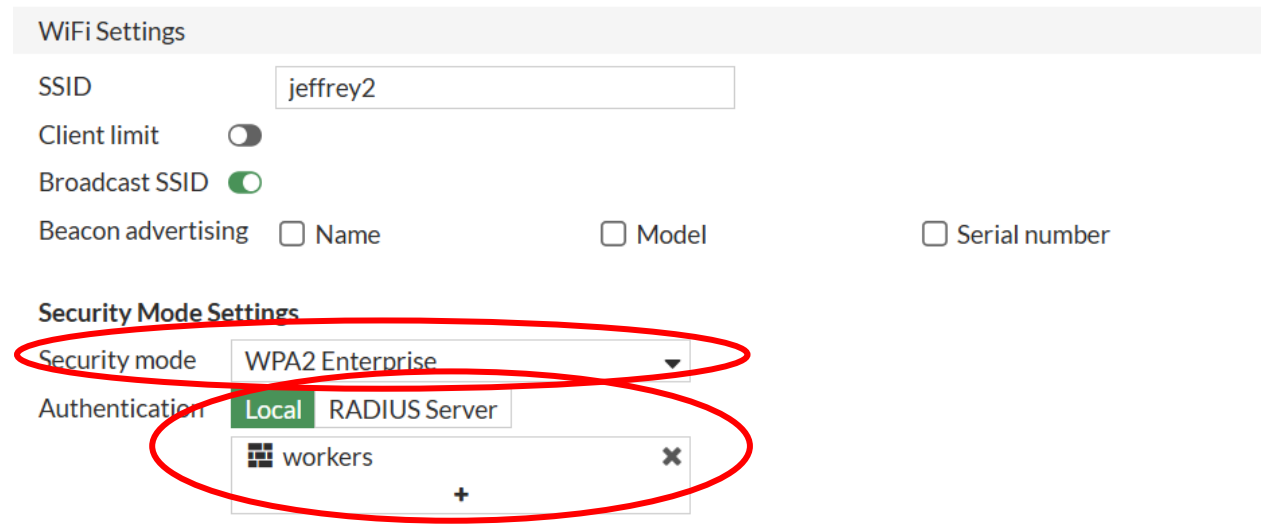
In NAME, name it whatever you'd like (it is not what shows up as the WiFi name), and create the desired ranges in netmask (should have enough space for another network due to making another WiFi).



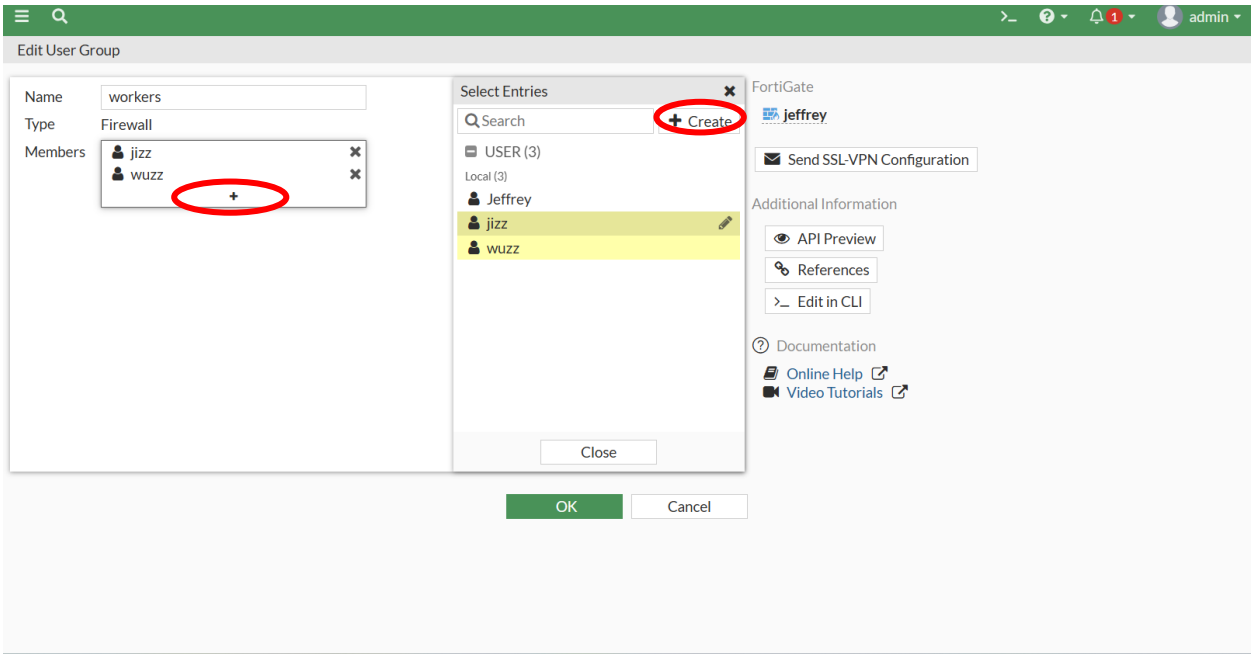
The SSID is what the WiFi will actually show up as, and the toggle for broadcast SSID will determine if it shows up by itself or having to search for it. The security mode is what makes it WPAPersonal or WPAEnterprise. The difference is that WPAEnterprise requires a made username and password so that only authorized people are allowed on the network (it requires a username and password on top of the passphrase). The passphrase is the password for the WiFi.



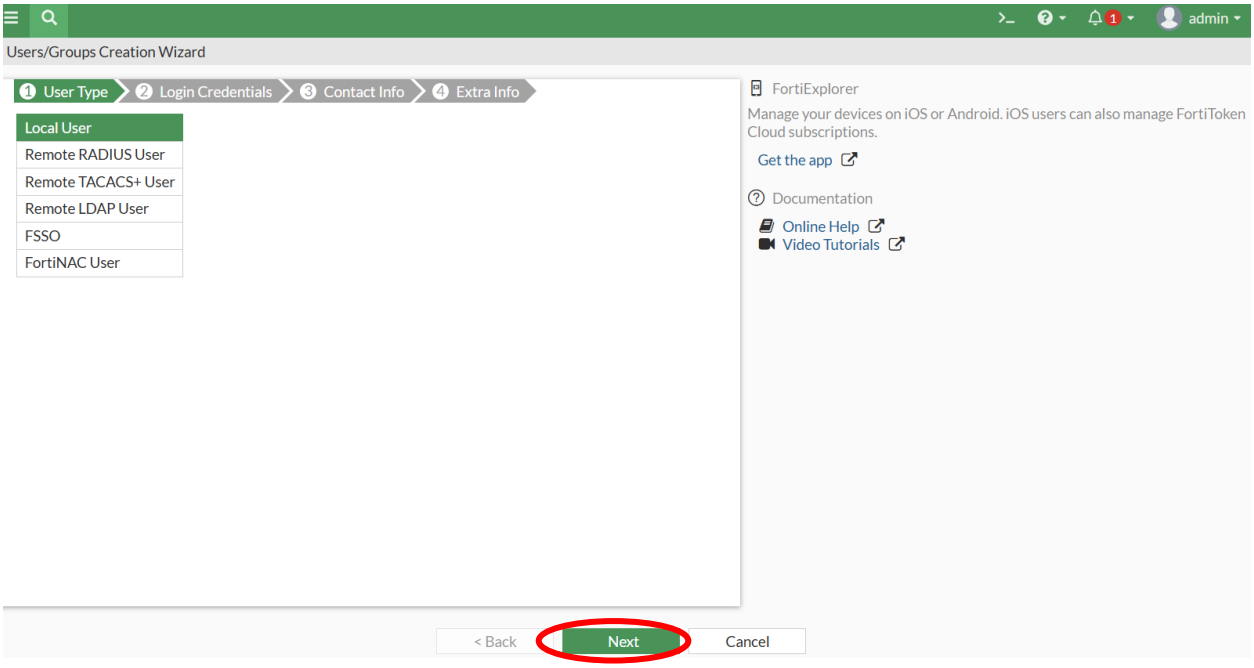
For Enterprise networks, there will be an option for authentication. Select Local and use the default User Group, if there is none, add one with the plus symbol.



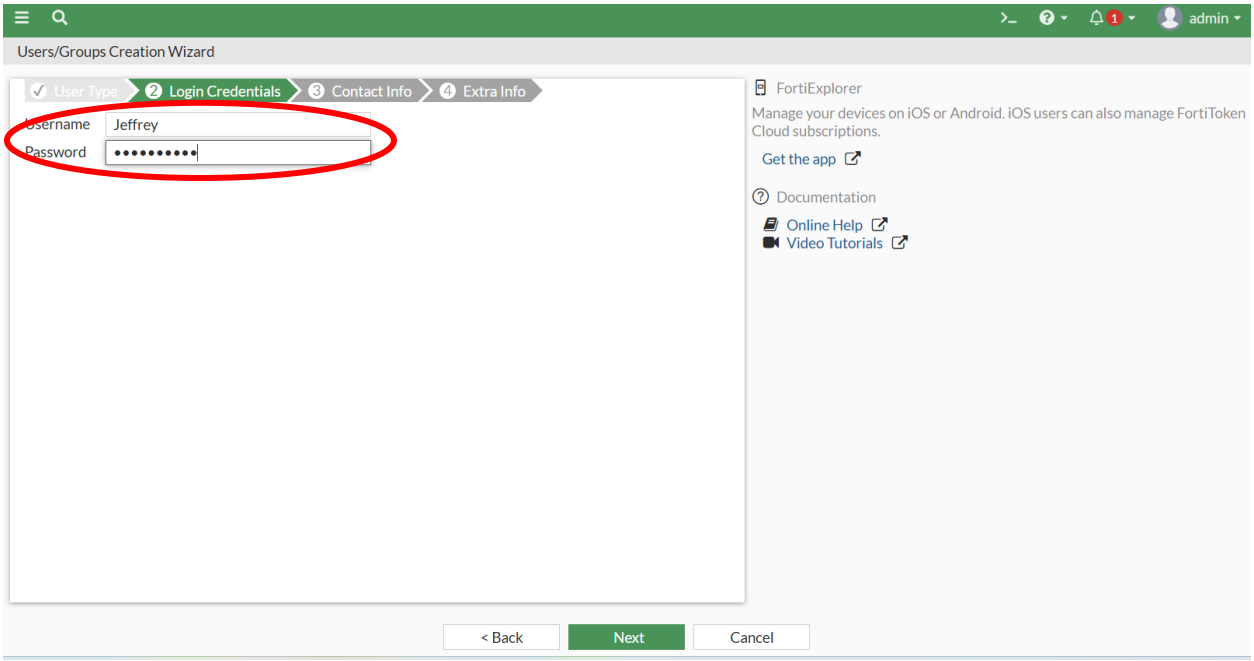
After creating the group, name it and add members to the group.



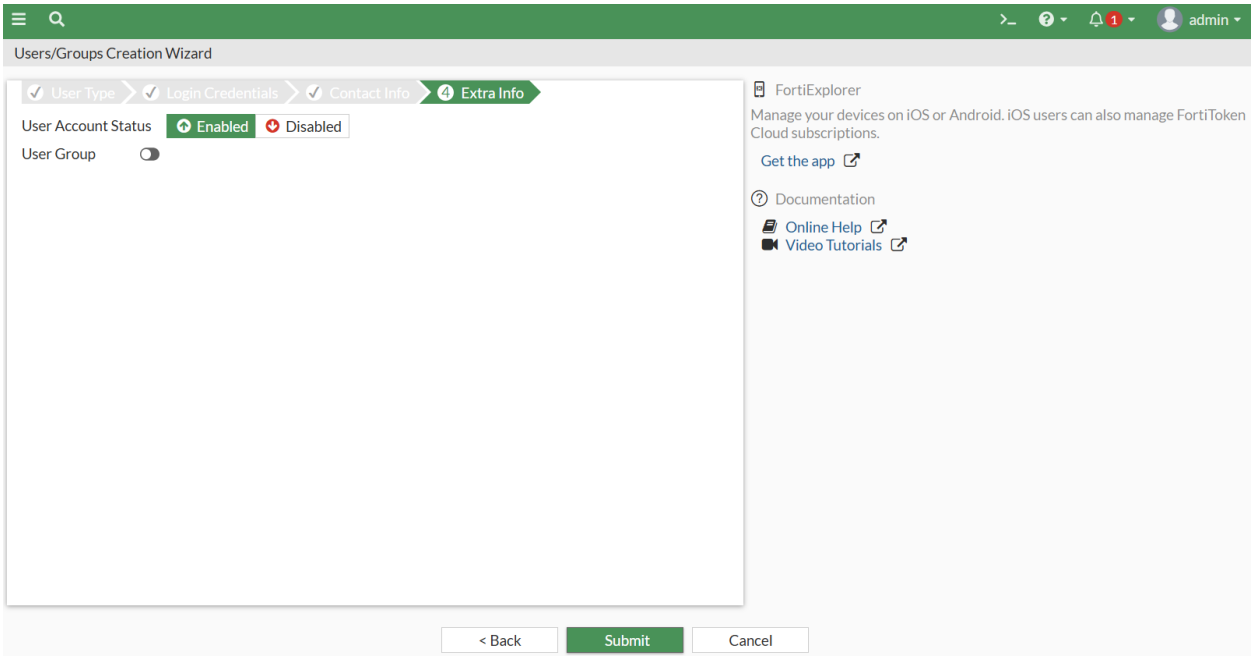
In the wizard, select local user and click next.



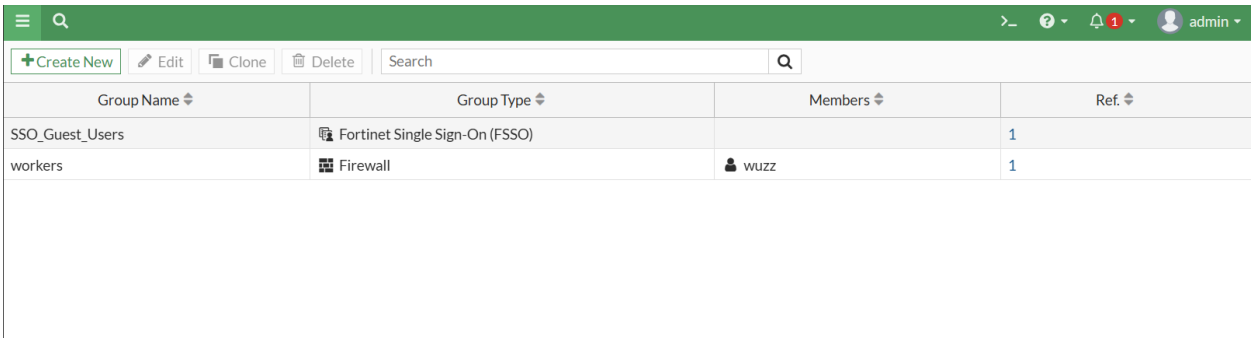
Next, choose a username and password for the user.

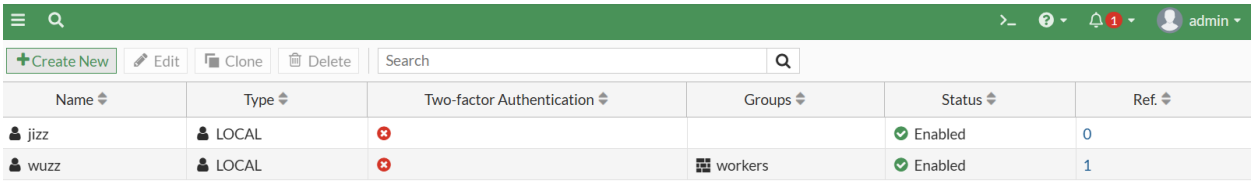


Contact information is optional, and finally, enable the user.

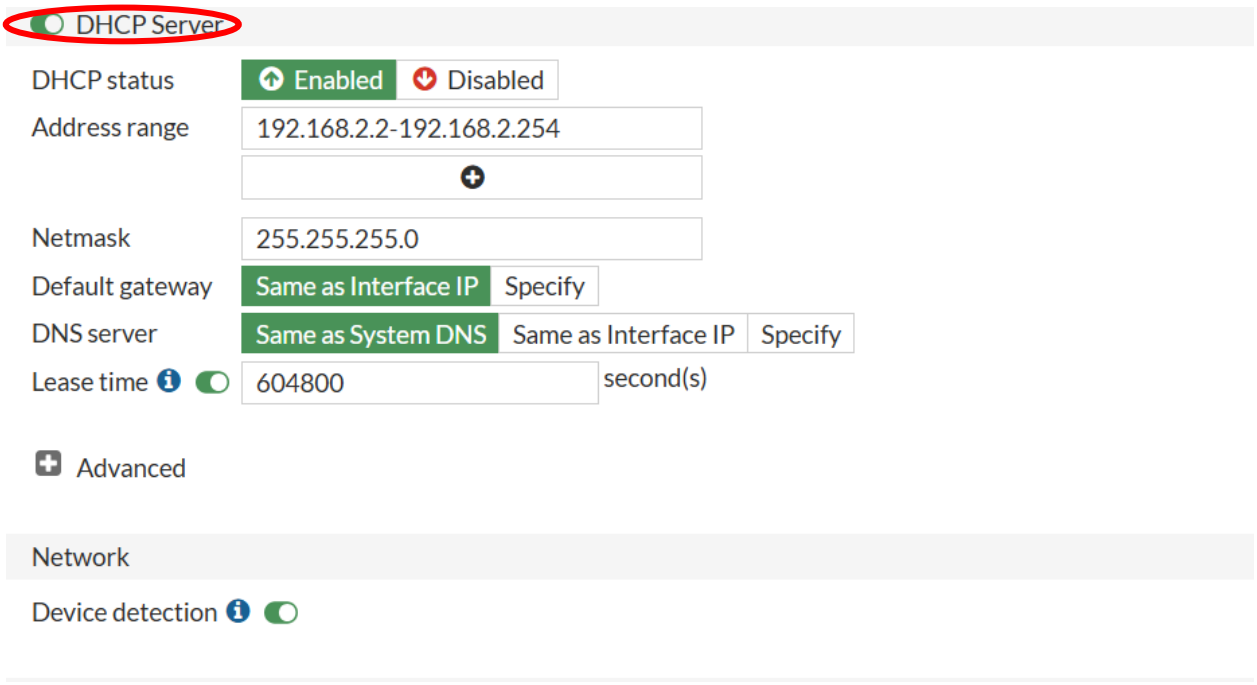


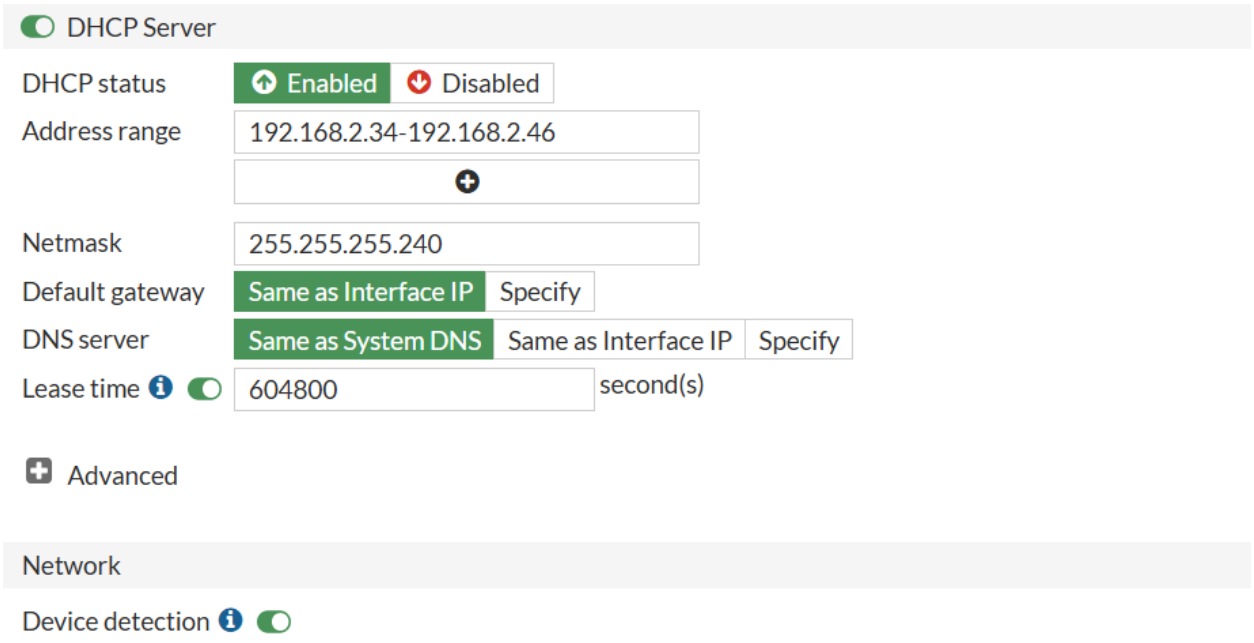
You can also edit the users and groups in it’s own tab.



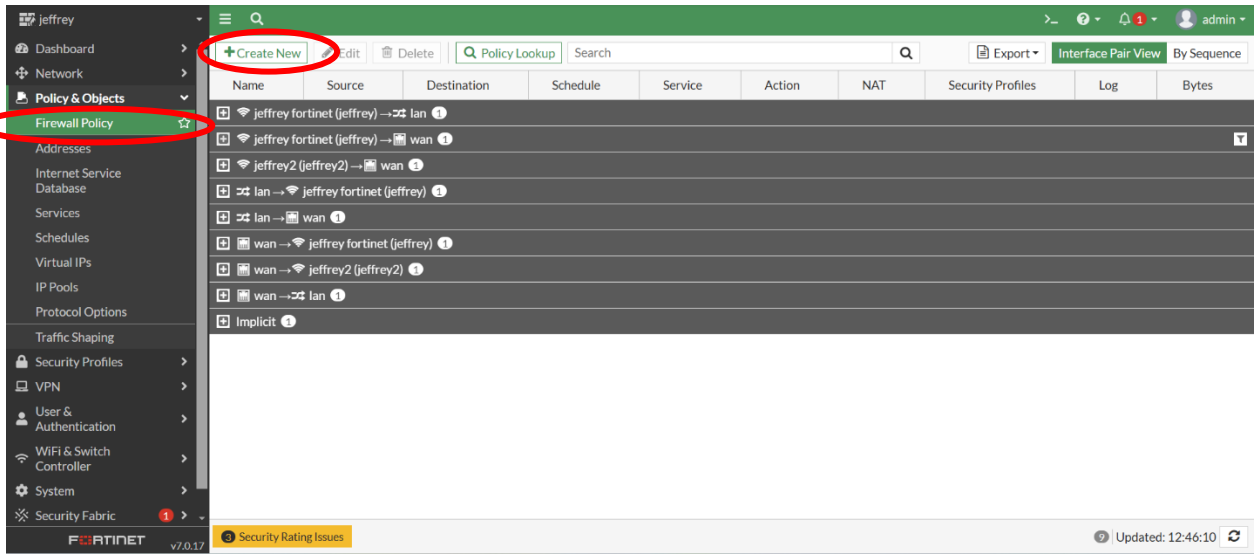


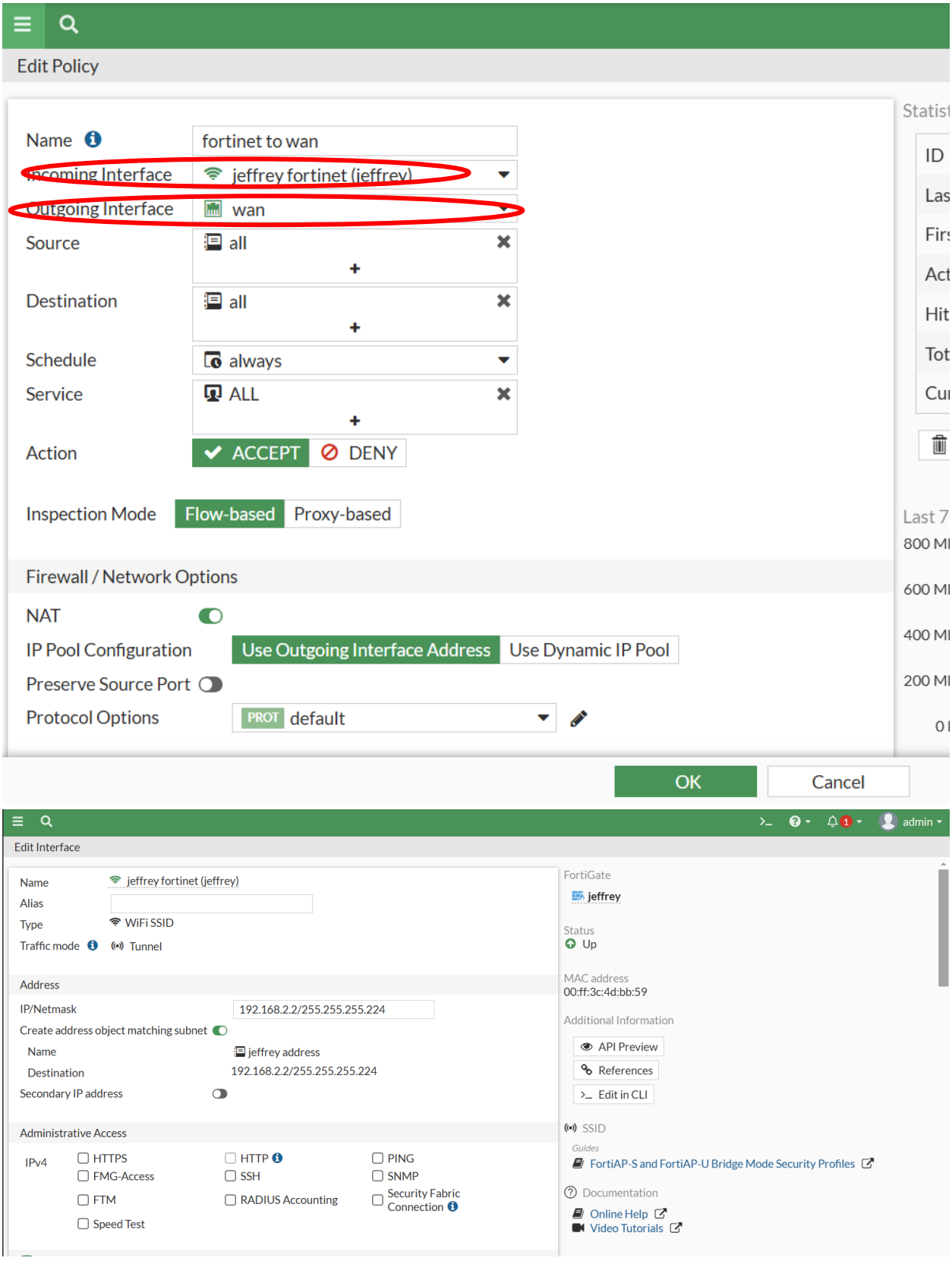
After creating the users, toggle on DHCP Server, and it will automatically assign IPs to those on your network. it should automatically fill the address range.





After finishing the WiFi SSID, move on to firewall policies. You need to make multiple policies, from your SSIDs to your WAN, and from your WAN to your SSIDs.




Edit Policy
Name
fortinet to wan
Incoming Interface
jeffrey fortinet (jeffrey)
Outgoing Interface
wan
Source
all
Destination
all
Schedule
always
Service
ALL
Action
ACCEPT
DENY
Inspection Mode
Flow-based
Proxy-based
Firewall / Network Options
NAT
IP Pool Configuration
Use Outgoing Interface Address
Use Dynamic IP Pool
Preserve Source Port
Protocol Options
PROT
default
OK
Cancel
admin
Edit Interface
Name
jeffrey fortinet (jeffrey)
Alias
Type
WiFi SSID
Traffic mode
Tunnel
Address
IP/Netmask
192.168.2.2/255.255.255.224
Create address object matching subnet
Name
jeffrey address
Destination
192.168.2.2/255.255.255.224
Secondary IP address
Administrative Access
IPv4
HTTPS
HTTP
PING
FMG-Access
SSH
SNMP
FTM
RADIUS Accounting
Security Fabric Connection
Speed Test
FortiGate
jeffrey
Status
Up
MAC address
00:ff:3c:4d:bb:59
Additional Information
API Preview
References
Edit in CLI
SSID
Guides
FortiAP-S and FortiAP-U Bridge Mode Security Profiles
Documentation
Online Help
Video Tutorials

Problems

One problem we encountered when doing this lab was our switch did not support the AP. Thankfully, we had another PoE switch and it worked. Another thing is, the AP may not be compatible with some Fortinet versions, like some of the new versions.

Conclusion

In conclusion, Fortinet firewall is a great firewall that comes with many options, easy to understand GUI, is small and compact, and would be a perfect fit for those working in SOHO settings.

FortiGate FortiGate-40F

Setting up remote access with Fortigate-40F

Jeffrey Yiu Cheung

Purpose

The purpose of this lab is to demonstrate a way to set-up remote access/desktop for users with FortiGate-40F and FortiClient.

Background information

In the modern age, being able to securely access private network remotely is important for work and organizations. With cybersecurity threats constantly evolving, hackers can utilize new knowledge to breach sensitive data. To prevent sensitive information from being risked, Fortinet designed and offers its own VPN to its customers.

Remote Access technology enables users to connect to a computer, network, or system regardless of geographical barriers. This technology can enable the ease of accessing files, managing systems, and running applications. While not all businesses may benefit from this, this technology is a staple to telecommuters (those who work from home), business travels, or those needing to work offsite due to distance or other barriers. While this technology is convenient, it requires for a lot of security to maintain.

Fortinet, Inc. is a cybersecurity company headquartered in Sunnyvale, CA. it is a leader in the Cybersecurity industry, securing over 700,000 enterprises and organizations worldwide. It leads the industry in training individuals and has made innovations to incorporate AI into their business. Fortinet made it their mission to educate 1,000,000 people by 2026.

With new technologies constantly enabling the ease of interaction with the web, more information is being uploaded every second. There is useless information, educational information, but there are also sensitive, personal information in the web. To prevent these cybersecurity threats, Fortinet offers cybersecurity devices and programs like firewalls malware prevention programs.

GUI or Graphics Users Interface, is a really nice aspect of the Fortinet Firewalls. Compared to other firewalls like for example the Palo Alto firewalls' GUI, Fortinet firewall GUI is clean and user-friendly, and an overall great upgrade. GUI is an underrated and important aspect of firewalls and their configurability. It can have a big impact on efficiency, reduced errors, and improved user experiences.

VPNs, or virtual private networks, is a technology that allows users to securely connect to private networks over the internet. By creating a tunnel and encrypting data with advanced protocols like IPsec and SSL/TLS to ensure protection against eavesdropping attacks and other threats. VPNs provides stronger privacy and security online, and on top of this, it also allows users to bypass geographical limitations.

SSL, or Secure Sockets Layer, is a protocol that encrypts data through the application layer. Compared to IPsec, or internet protocol security, it is easier to set up, and completes the same goal if users use web-based applications. However, unlike IPsec, it does not provide end-to-end

encryption for all network traffic and is less broad. While SSL VPN is good for this demonstration, one should consider IPsec to be the better option.

Remote Desktop Protocol is a service provided by Microsoft which allows users to connect and control another device via IP (or domain name if applicable). This technology allows users to work, access files, using the computer despite not physically having the machine they need. However, RDP needs the devices to be on the same network, and RDP is vulnerable to cyberattacks, with unrestricted port access and other exploits like BlueKeep, and thus is necessary to run it within a VPN.

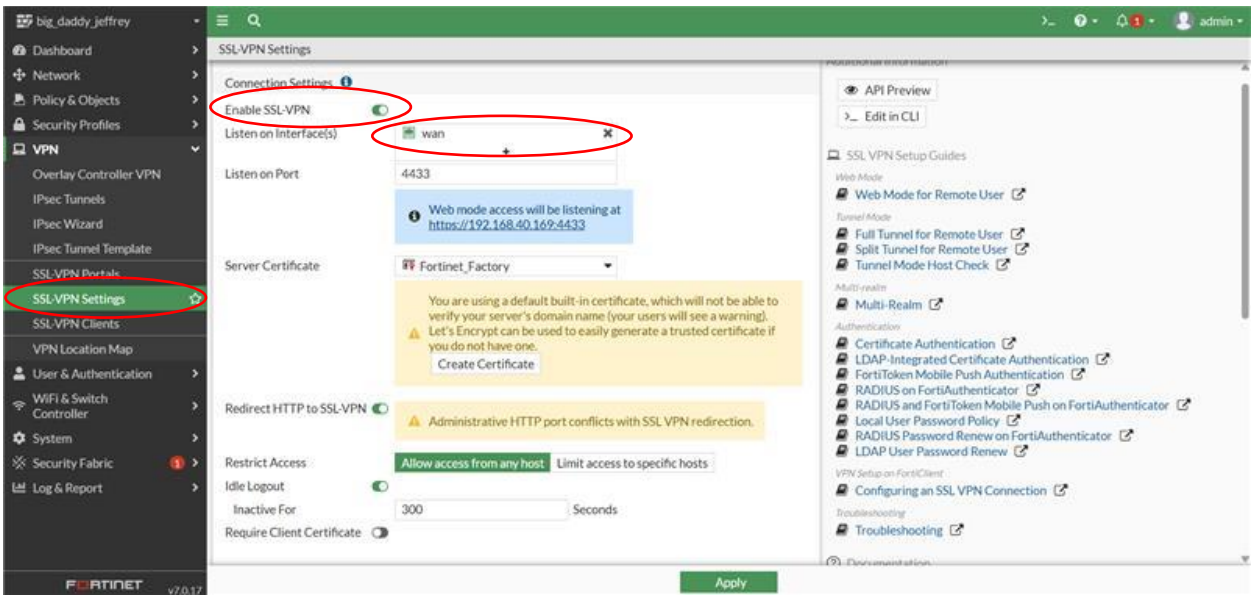
Microsoft is one of the largest and most influential technology company to have exist. Founded in 1975, Microsoft developed and revolutionize how commercial computers are built. Their products range from Operating Systems (windows), computers, software (Microsoft Office), cloud services, and videogames. Today, Microsoft is a technology giant that shape ongoing technology development.

FortiClient is a software designed by Fortinet to ensure secure remote access, ease of access, end-point connection and protection. It also allows secure remote connections to the internal network. It creates a tunnel between the user and the destined network and encrypts the data with SSL/TLS which passes through.

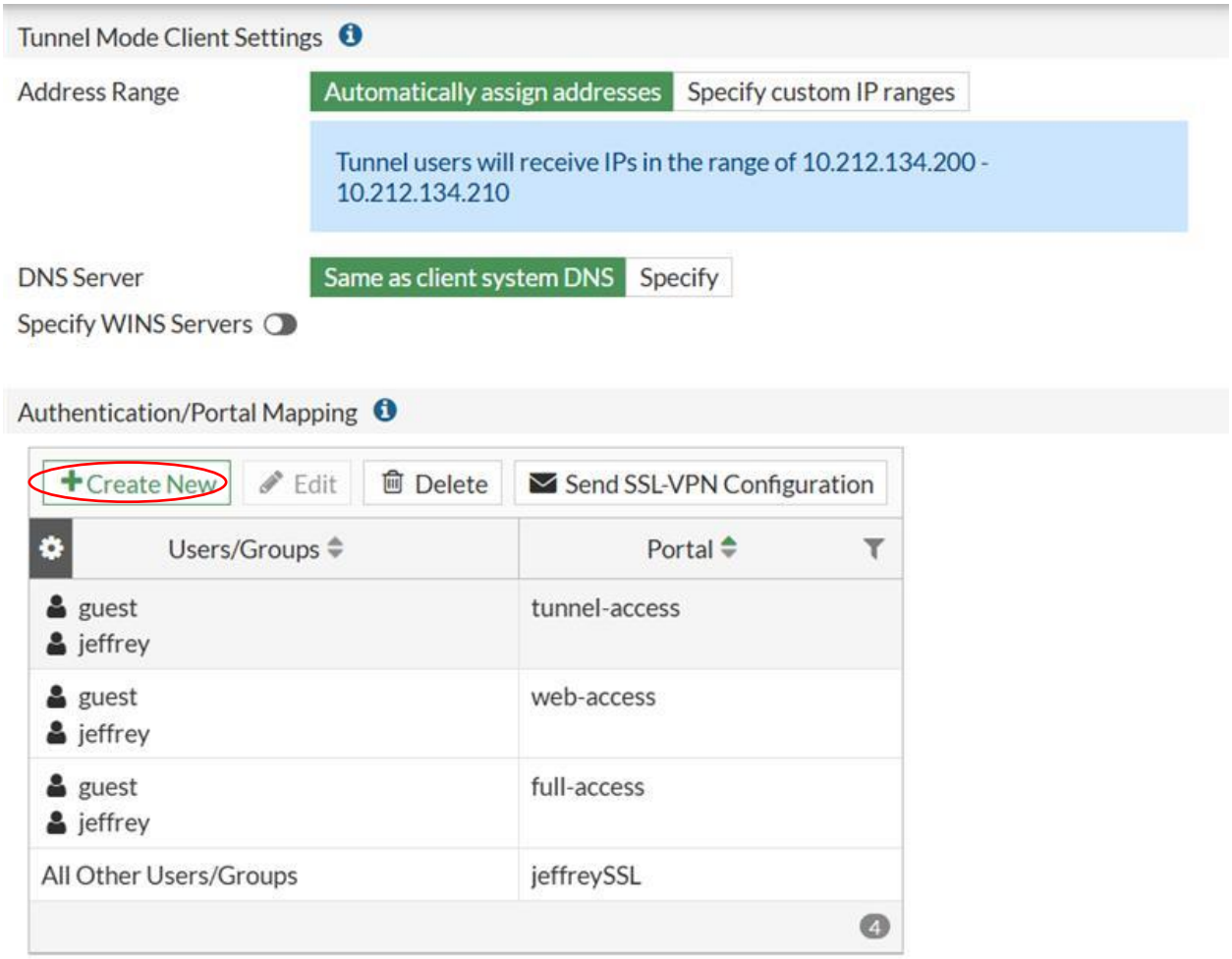
Lab summary

First, configure the SSL-VPN settings in the VPN tab, enable it and set it to listen on your WAN interface. Then, since the default port is 443 (HTTPS) and may interfere with some configuration, you can change the port, in my example I chose port 4433.

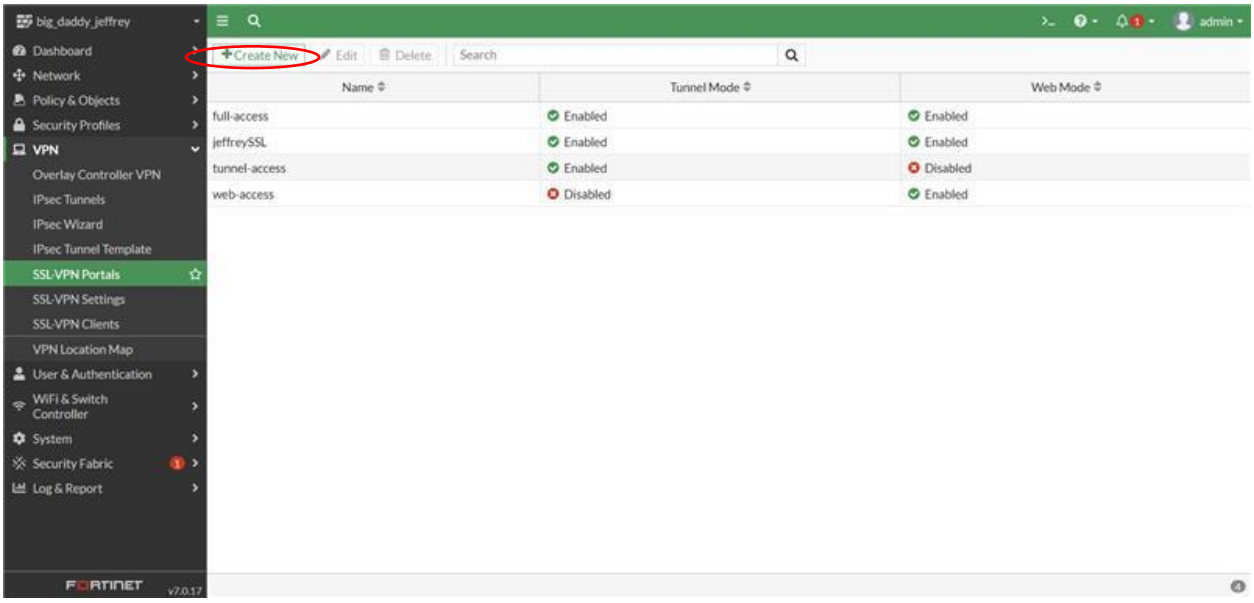
You can also make a Server Certificate for more safety, but in my case, I just use the default Fortinet certificate.



Afterwards, everything should be default in Tunnel Mode Client Settings. In Authentication/Portal Mapping, you can give different users different types of access. Tunnel-access gives access to secure an encrypted tunnel between a device and a remote network. Web-access gives access via a web-portal. Full-access gives full access to users, like using files, websites…

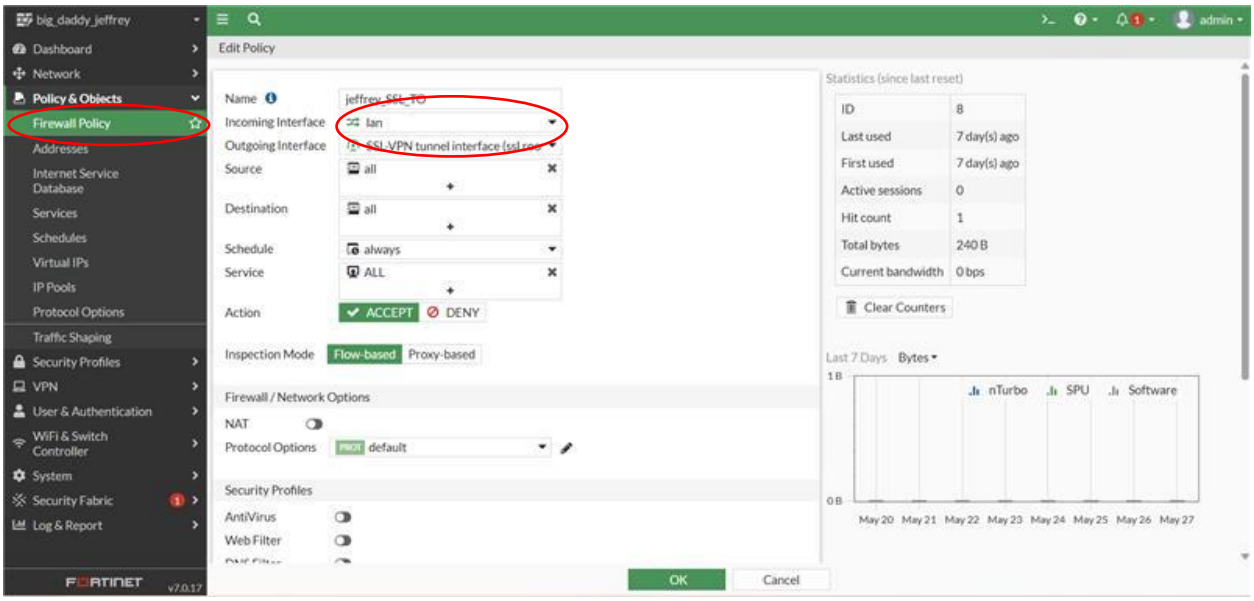


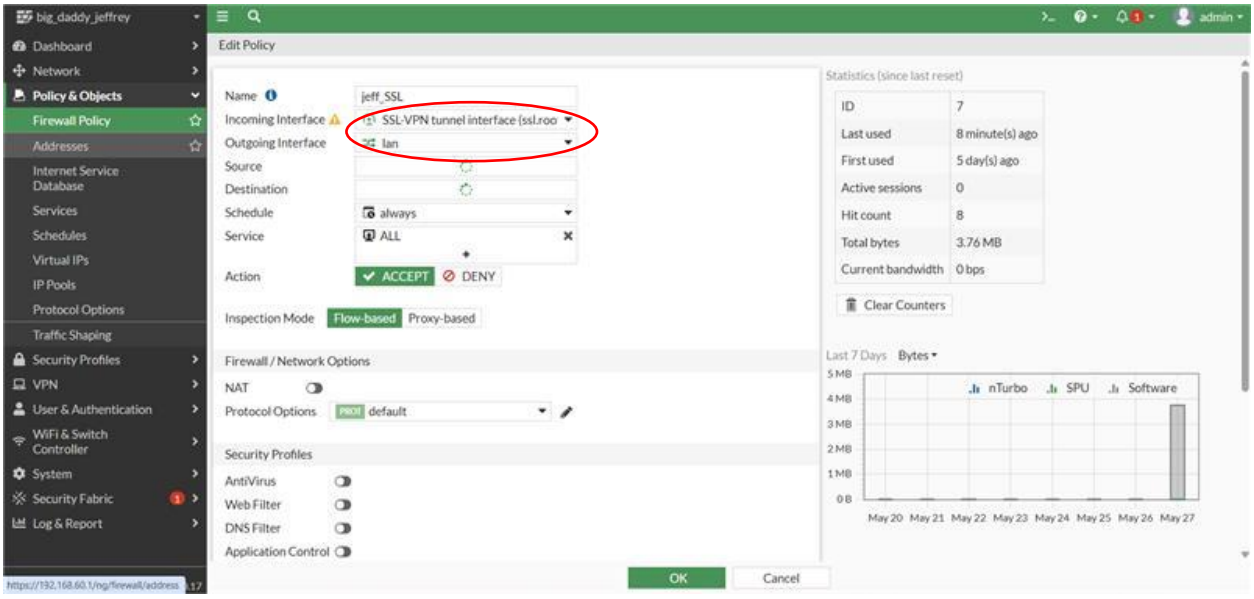
You can configure the types of access or edit existing portals in SSL-VPN Portals. I have created one such and named it jeffreySSL. You can also configure users and their groups.



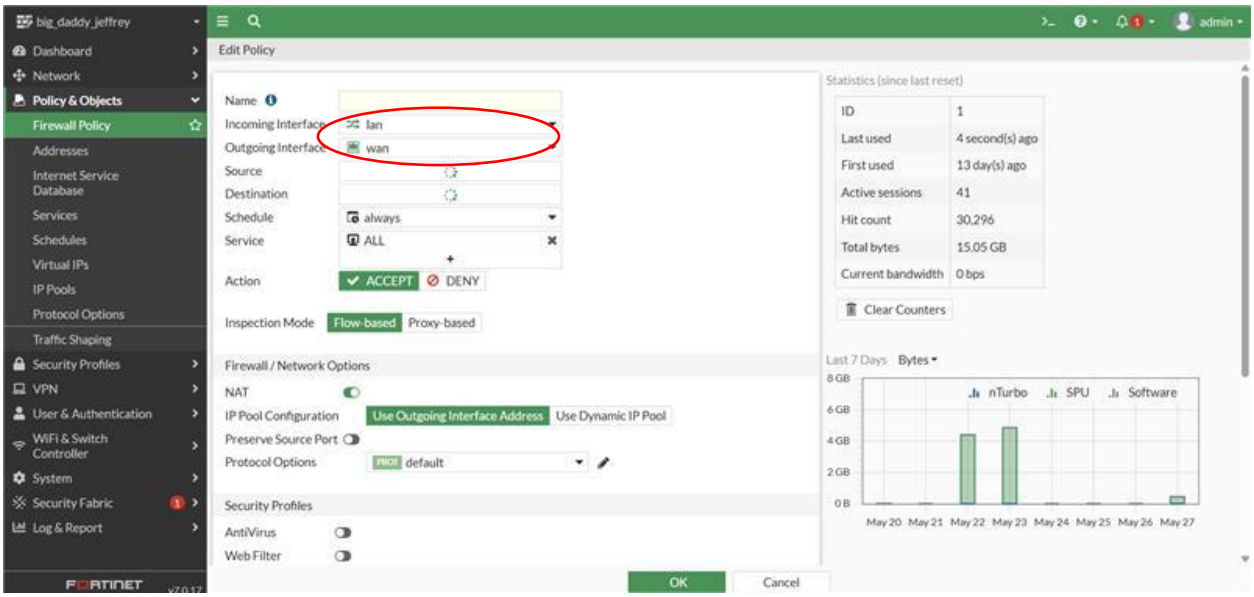
Next, create the Firewall policies so the different interfaces can communicate with each other.

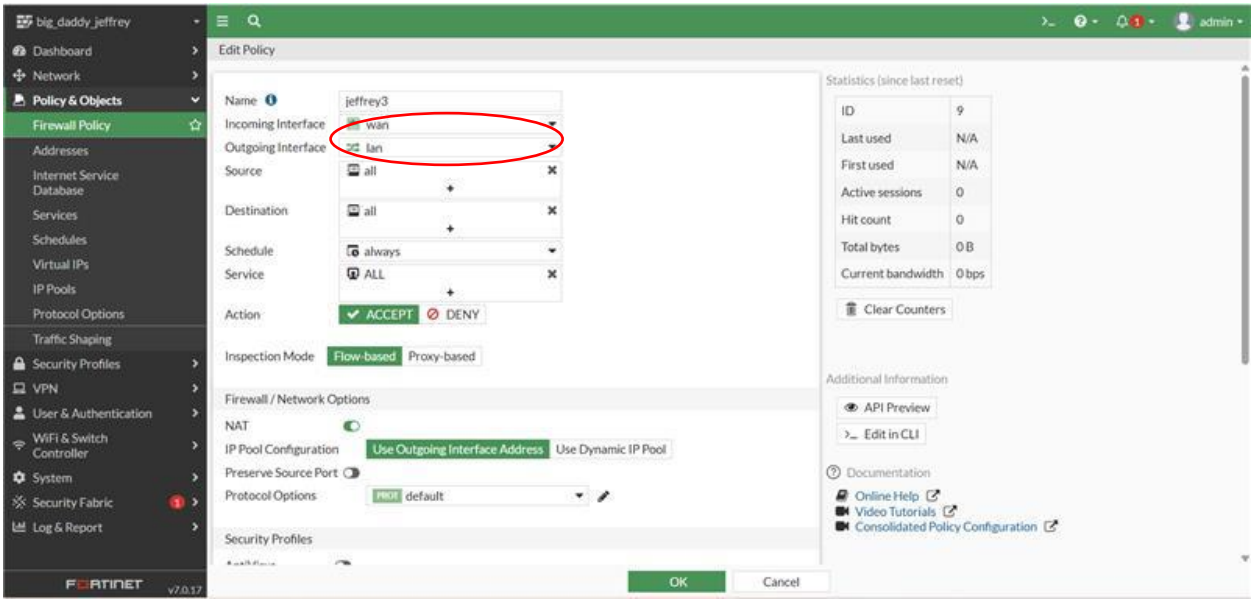
For the first one, create a firewall policy from LAN to the SSL-VPN tunnel interface, and one from SSL-VPN to LAN.



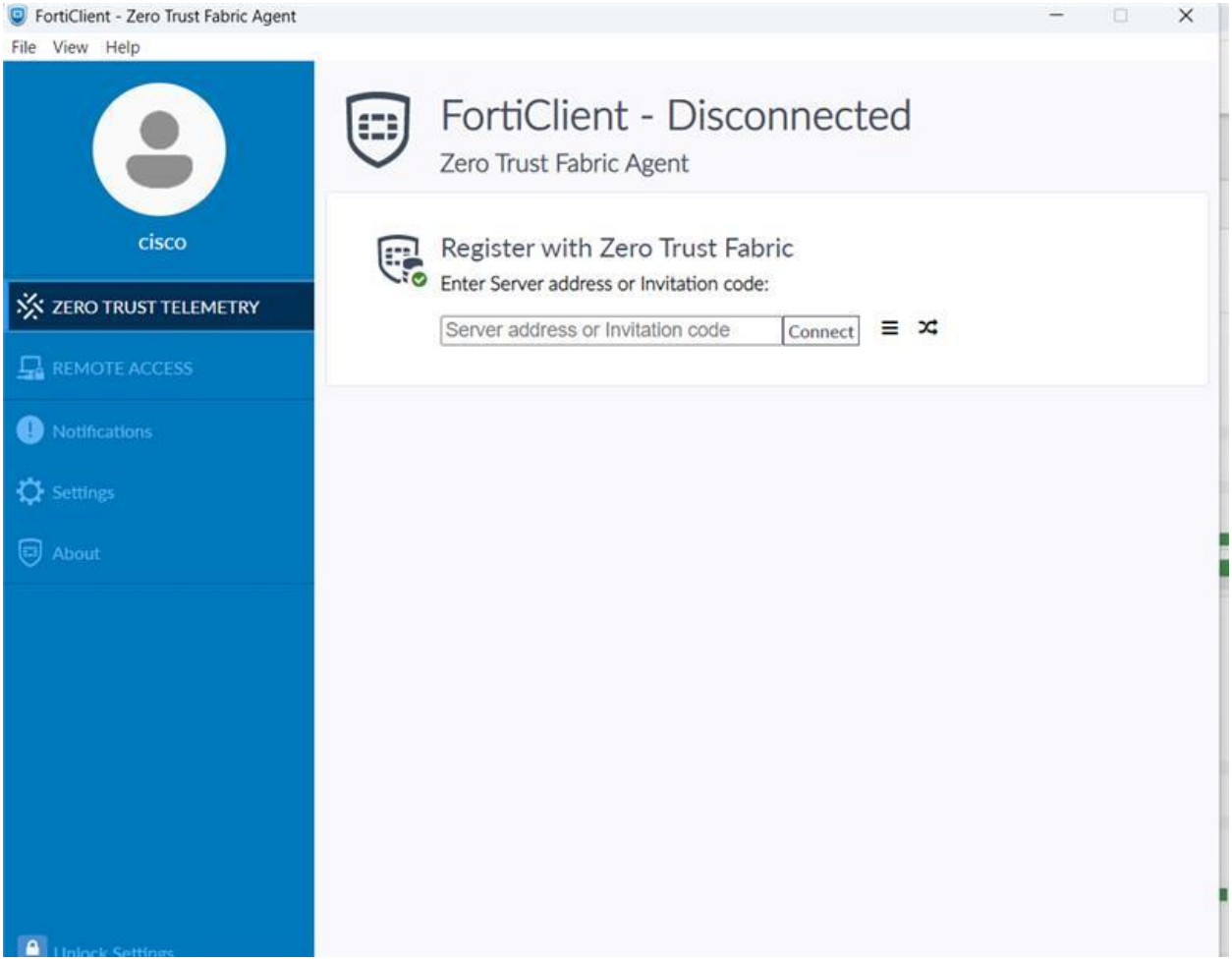


You'd also need firewall policies from LAN to WAN and WAN to LAN if you don't have them already.

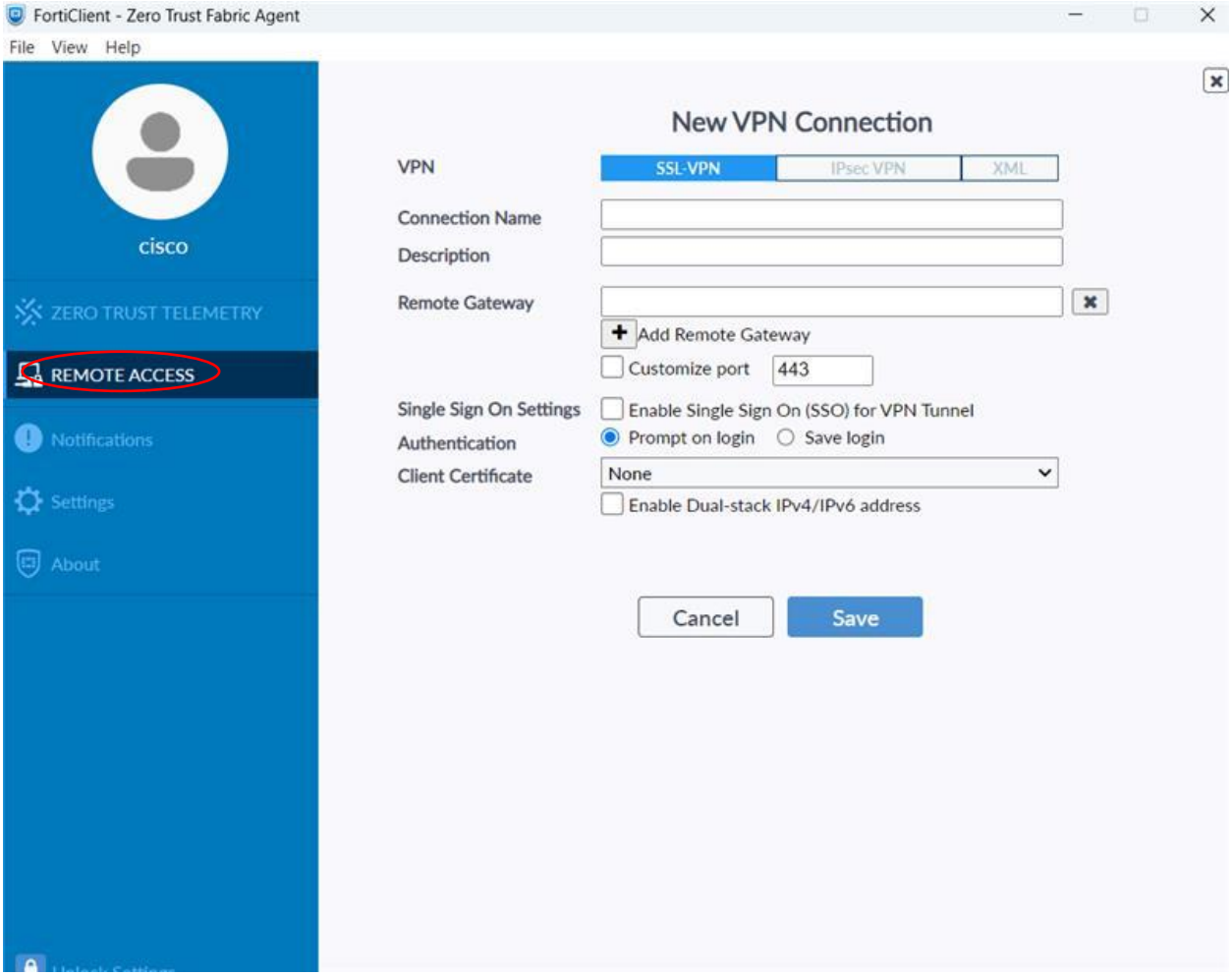


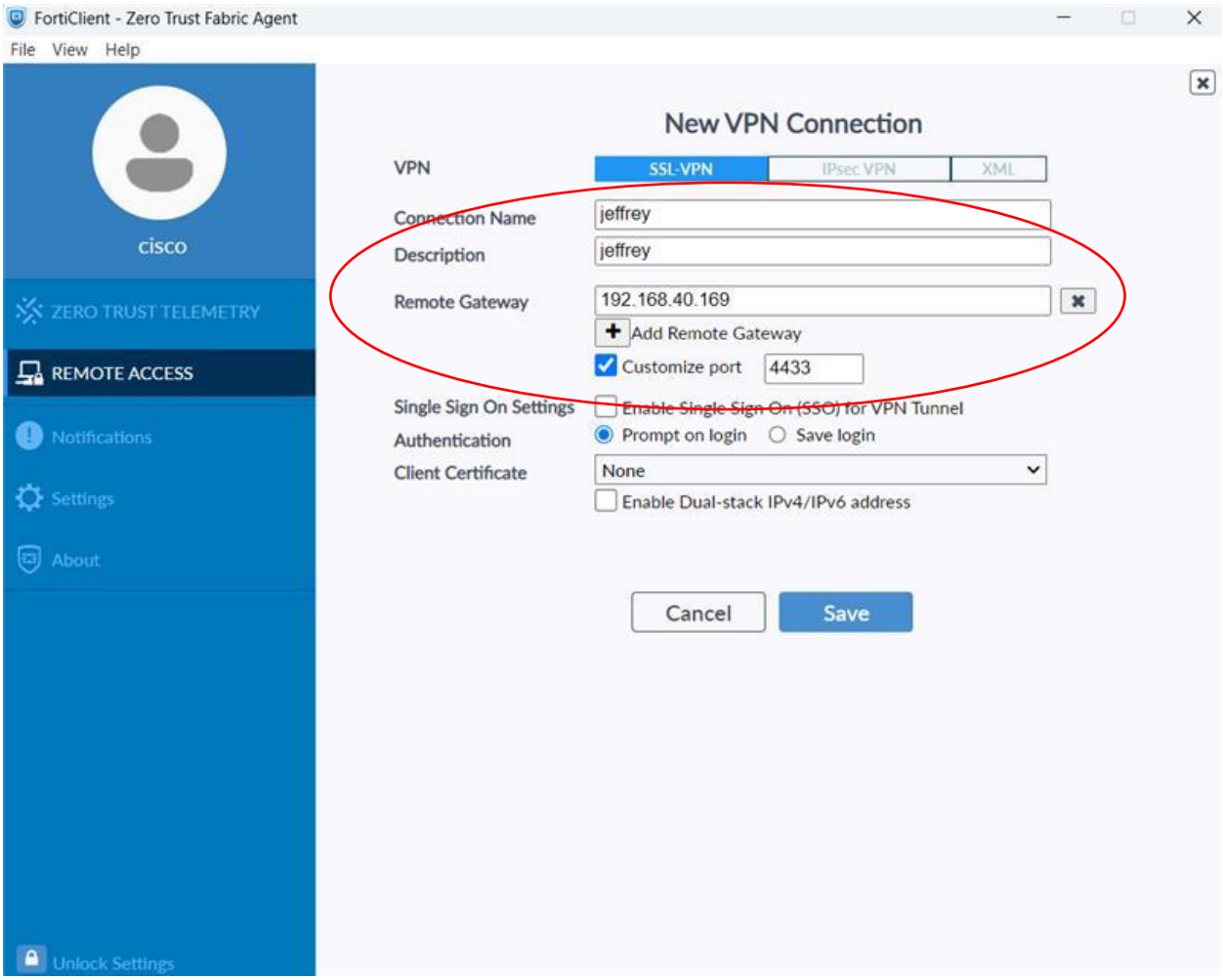


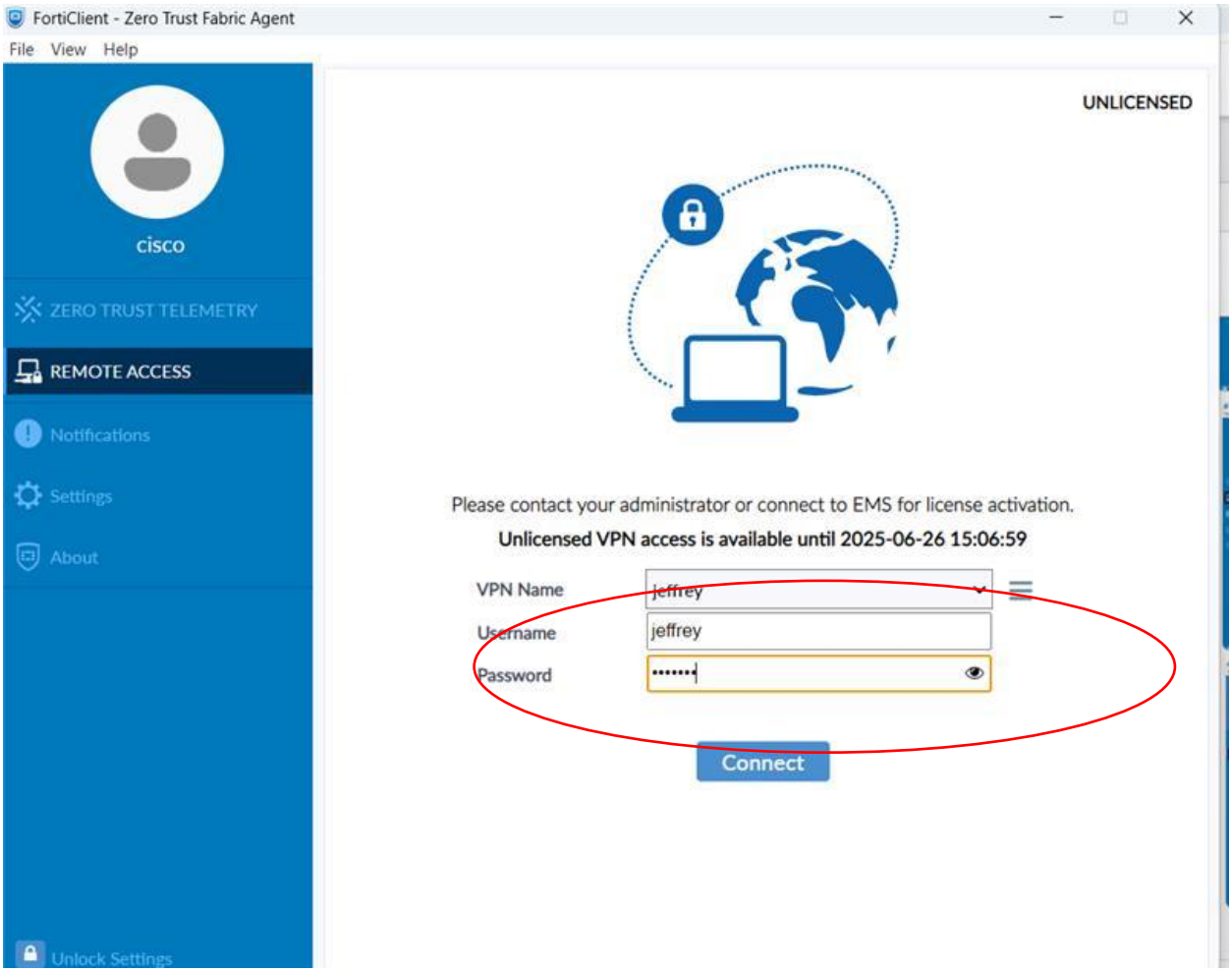
Afterwards, you should be set to use the Fortinet Firewall via SSL-VPN. Download FortiClient from Fortinet's website. Select remote access.



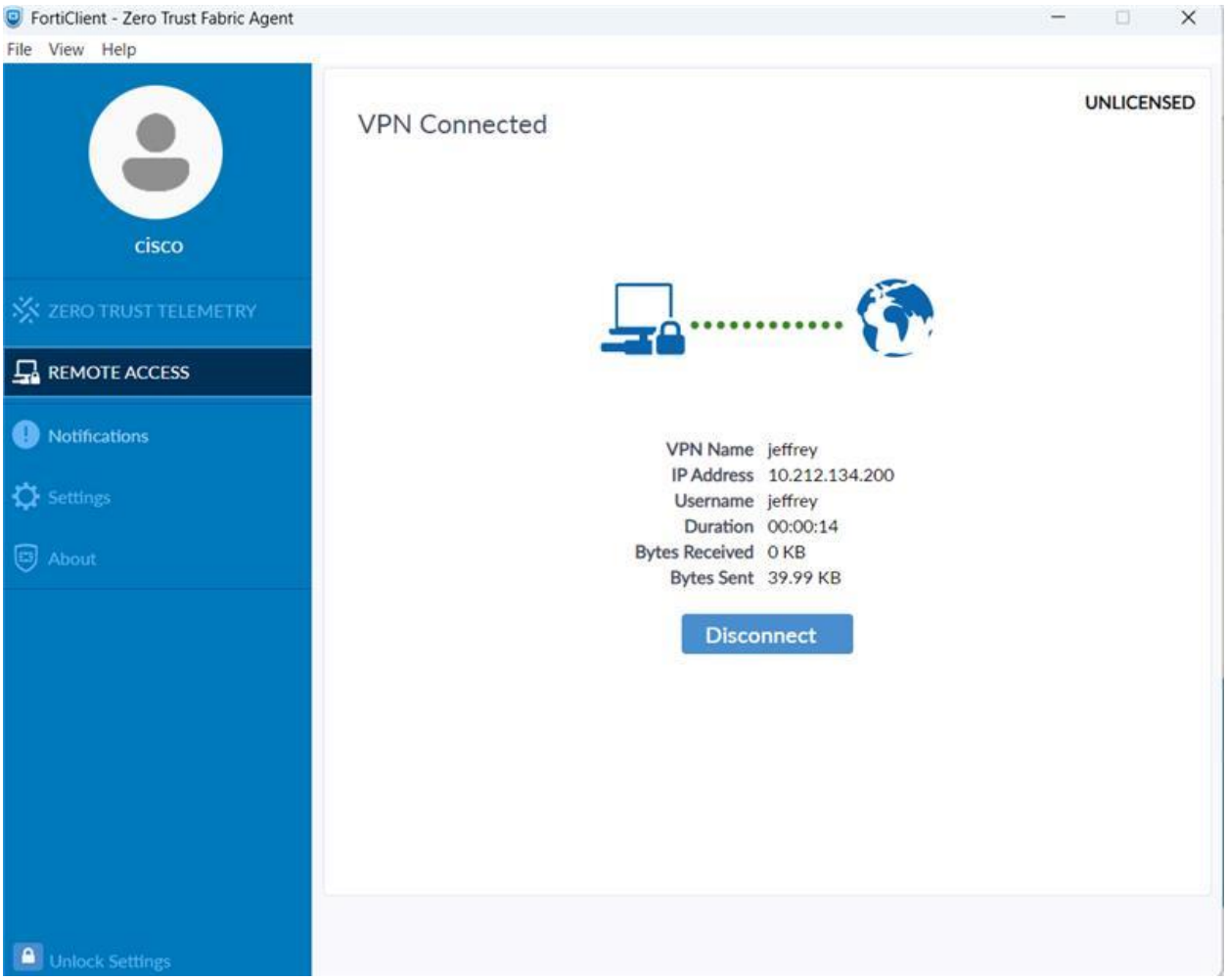
select SSL-VPN, then write whatever in Connection Name and description. In Remote Gateway, put in the IP of your LAN interface. Also, if you configured a different port in SSL-VPN settings, select customize port and the port number you chose.




FortiClient - Zero Trust Fabric Agent
File View Help
cisco
ZERO TRUST TELEMETRY
REMOTE ACCESS
Notifications
Settings
About
Unlock Settings
New VPN Connection
VPN
SSL-VPN
IPsec VPN
XML
Connection Name
jeffrey
Description
jeffrey
Remote Gateway
192.168.40.169
Add Remote Gateway
Customize port
4433
Single Sign On Settings
Enable Single Sign On (SSO) for VPN Tunnel
Authentication
Prompt on login
Save login
Client Certificate
None
Enable Dual-stack IPv4/IPv6 address
Cancel
Save

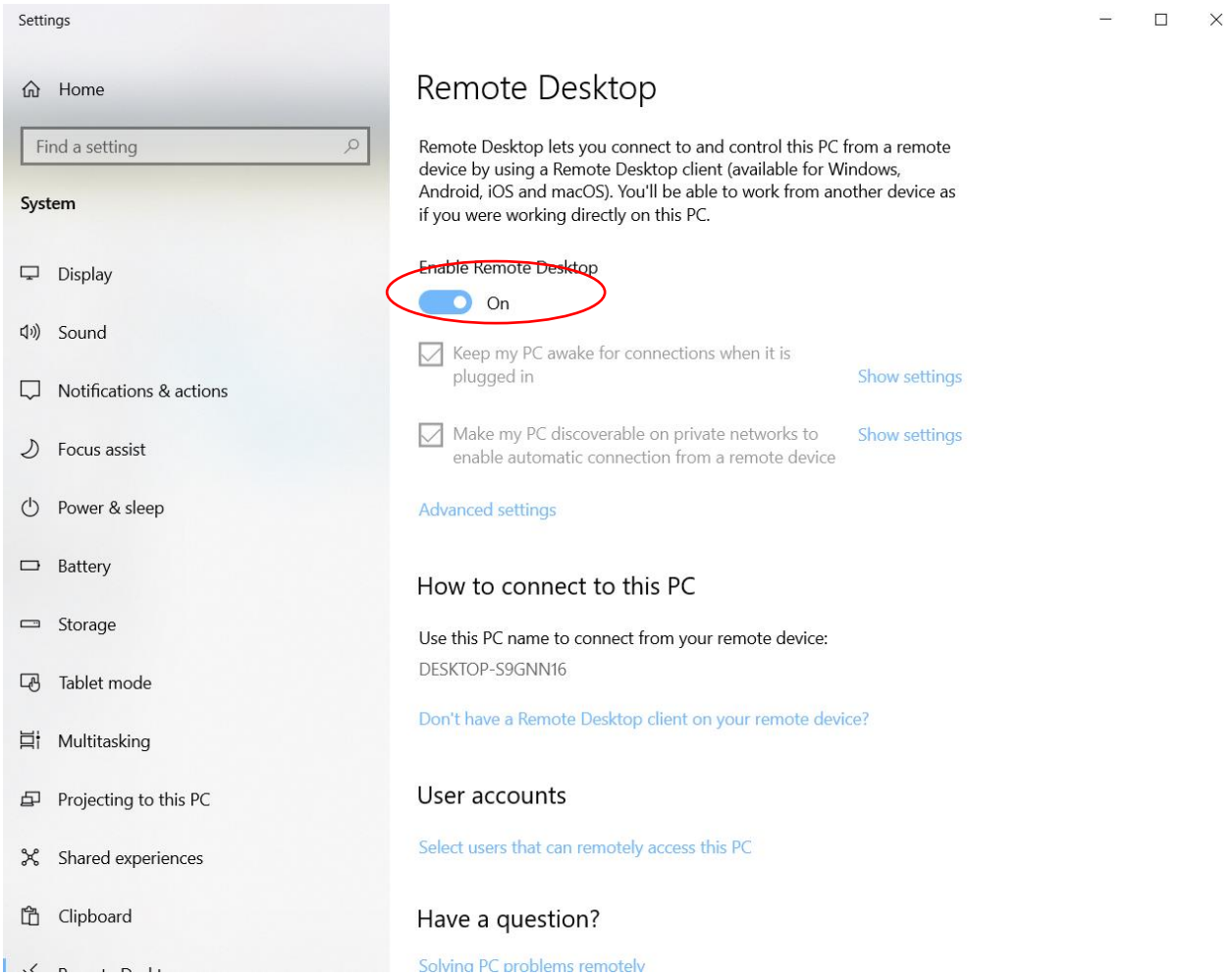


Use the username and password you set for the users enabled for access. Afterwards, it should be set to be connected.



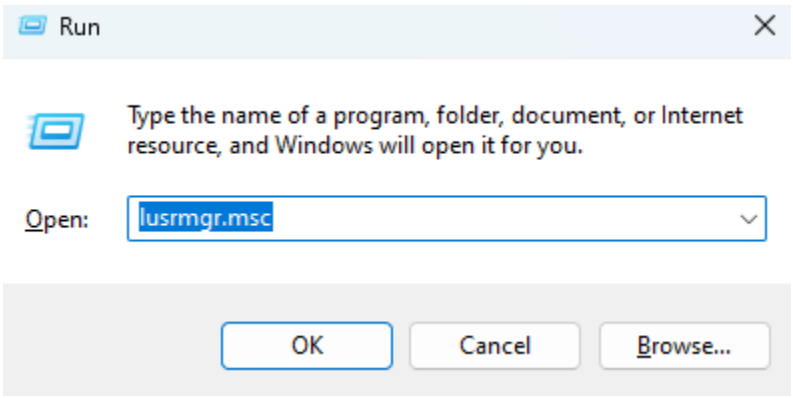
After this, it should be all set and ready to go for remote access.

To successfully remote access, you need to first turn on Remote Access in computer's settings.

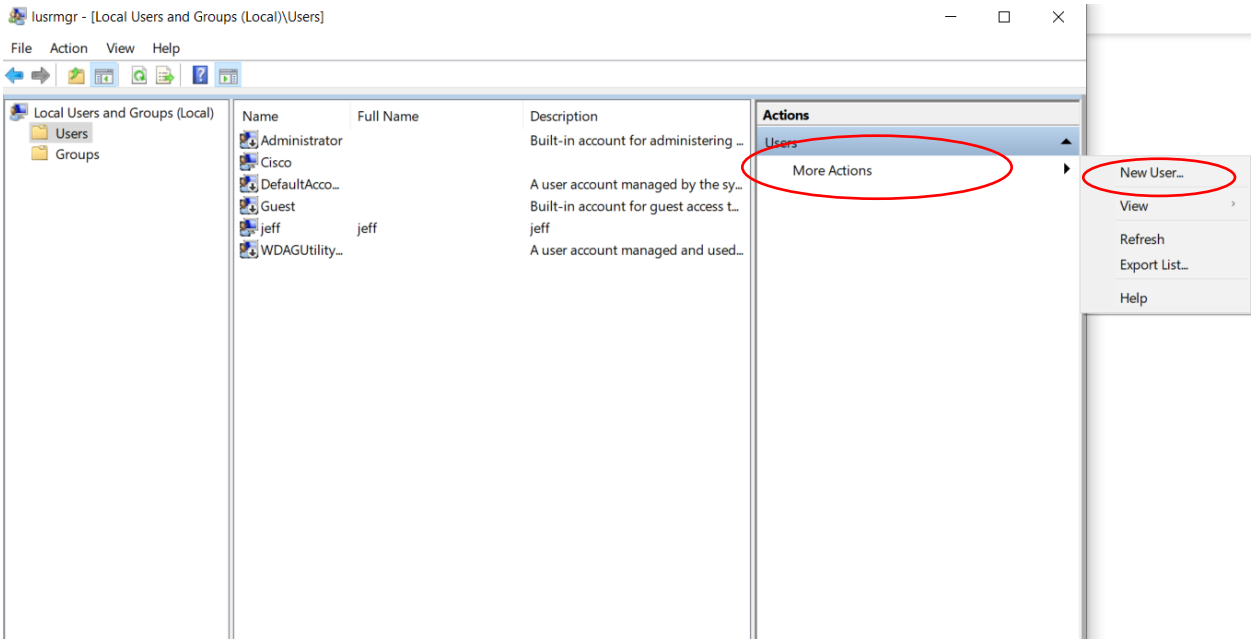


Now, for the device in the internal network, or the device in the network that you want to connect to, create a user or give an existing user permission to access Remote Desktop.

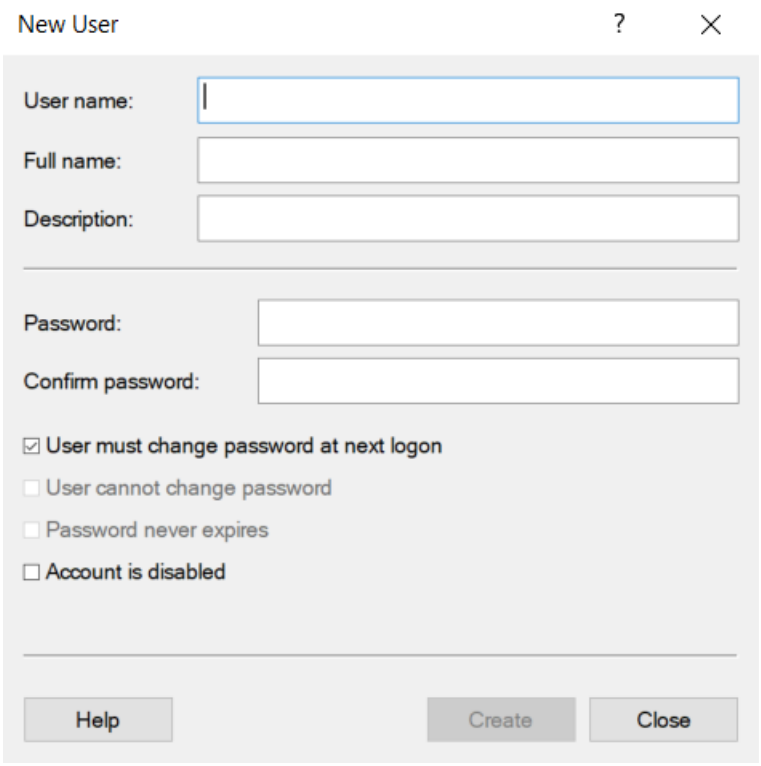
First, open Run (or Windows + r on windows, command + space on mac) and type in lusrmgr.msc.



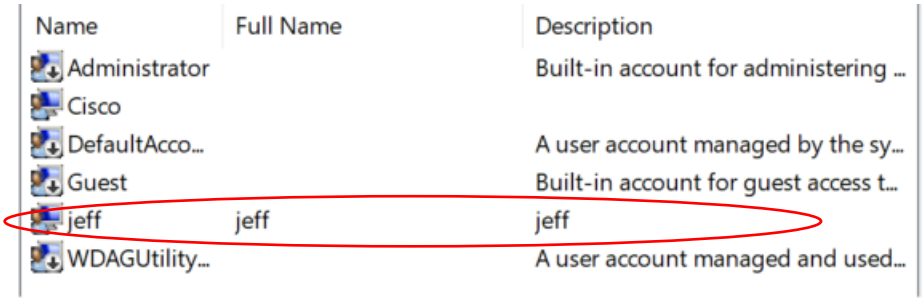
This should pop up. Select Users and add new user (if necessary).



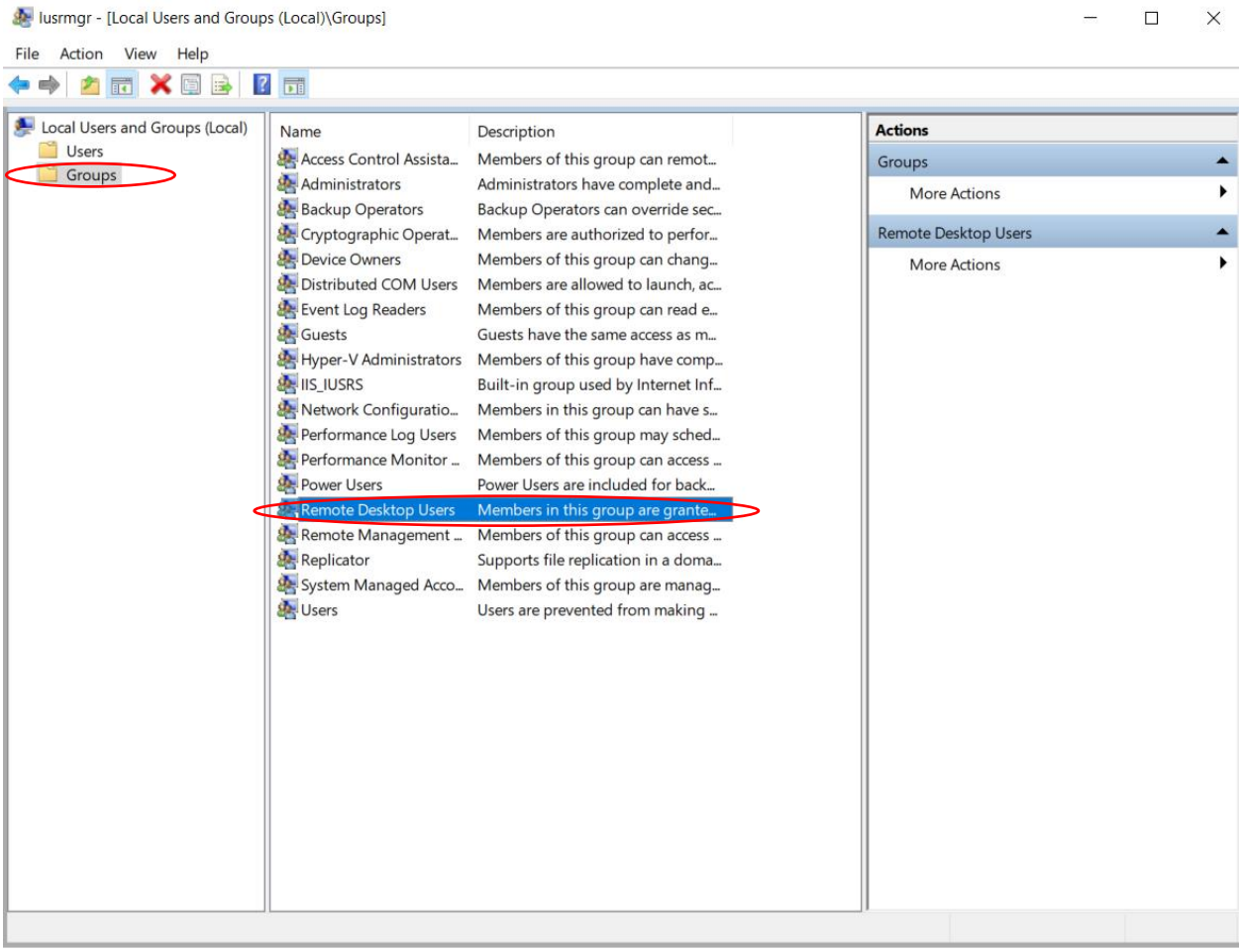
Next, add a user, give it a username and password (if necessary). You can check off requiring changing password next logon (optional).



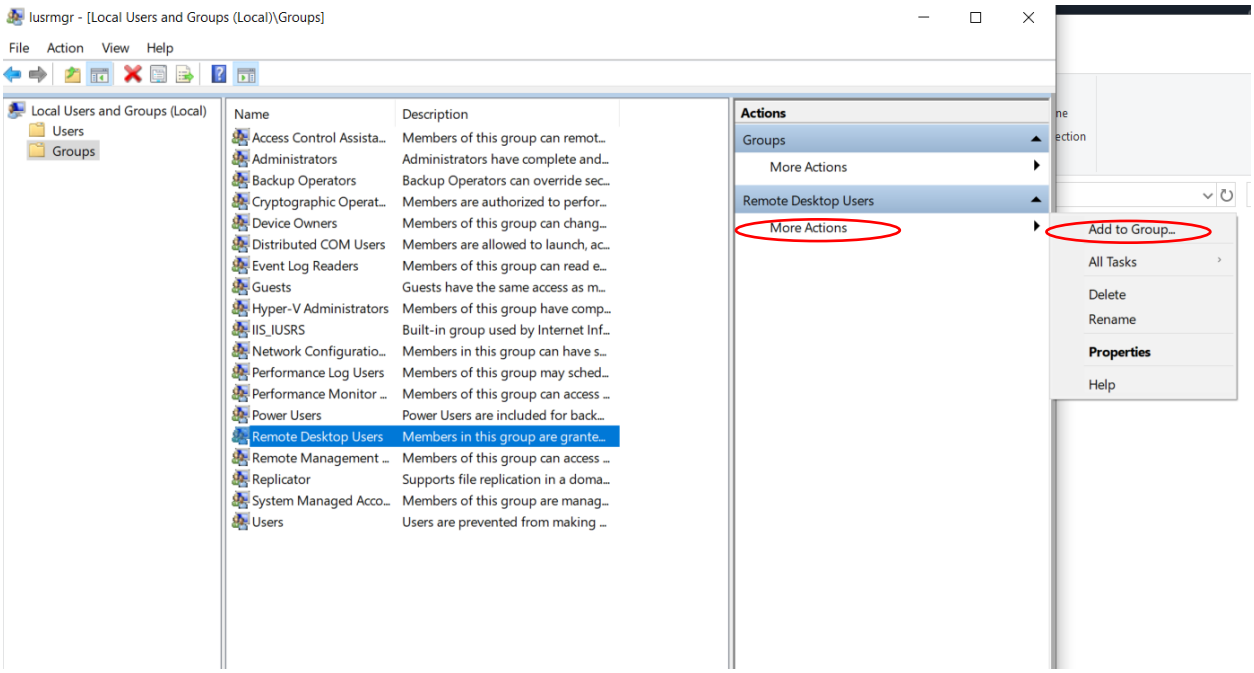
It should look like this.

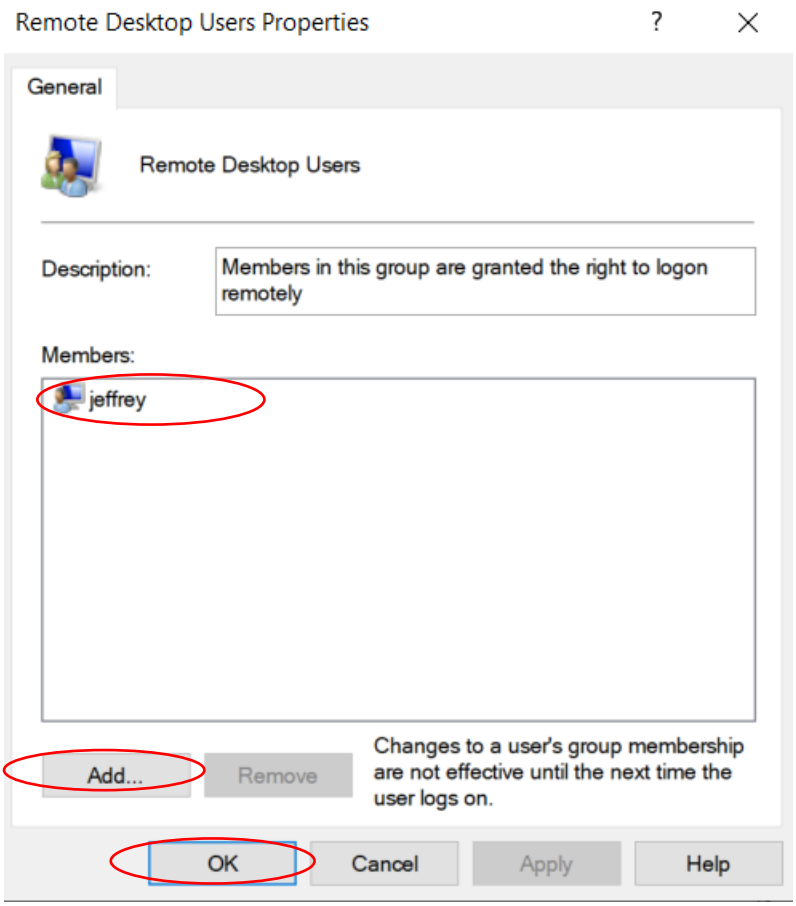


Next, go to groups. There should be a group named Remote Desktop Users.



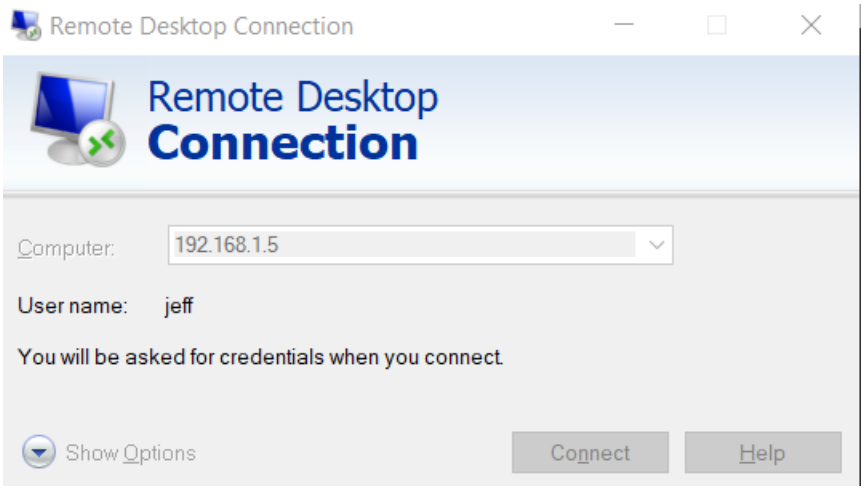
Next, add the user you've made, or an existing user, into the group to give them permission.





If you have reset password on next logon enabled, you have to reset the password before you can use the user.

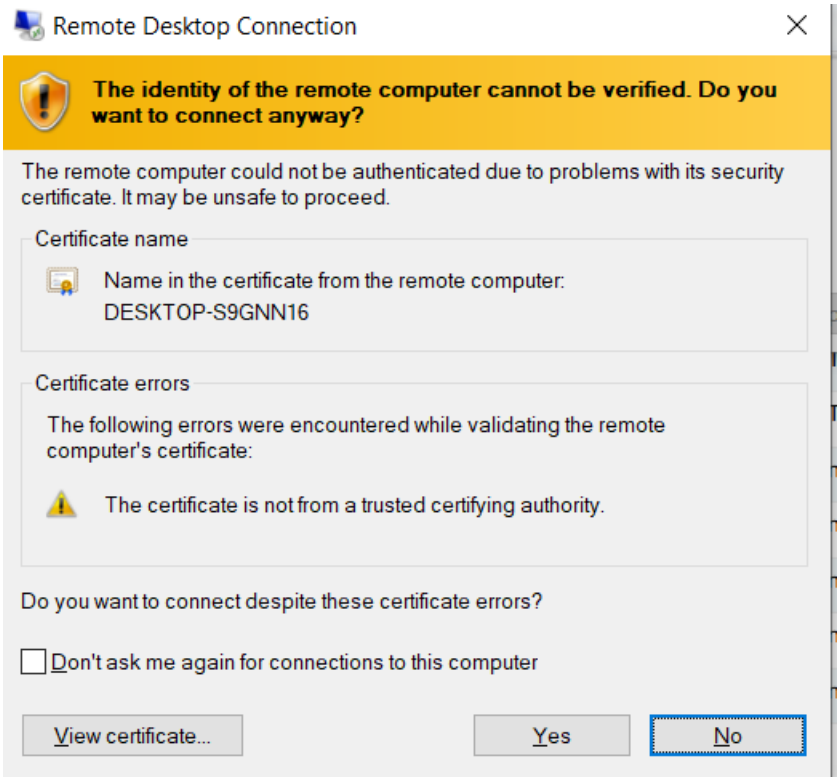
Next, using the other device, remote access into the desired device via Remote Desktop Connection.



In computer, you will need to input the desired device's IP address. This can be found in Command Prompt with the command "ipconfig /all".

```
Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) Ethernet Connection (3) I218-LM
   Physical Address. . . . . . . . . : 54-EE-75-75-94-1D
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::75ec:339b:9a6f:c202%20(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.1.3(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Monday, January 6, 2025 3:06:37 PM
   Lease Expires . . . . . . . . . . : Tuesday, January 7, 2025 3:06:36 PM
   Default Gateway . . . . . . . . . : 192.168.1.254
   DHCP Server . . . . . . . . . . . : 192.168.1.254
   DHCPv6 IAID . . . . . . . . . . . : 206892661
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-2A-C6-6E-3F-54-EE-75-75-94-1D
   DNS Servers . . . . . . . . . . . : 9.9.9.9
                                       1.1.1.1
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

If successful, you should be prompted with this:



Just click Yes, and then you're all set.

Problems

This is a fairly straightforward lab that shouldn't come with any hitches. However, there are some minor tweaks that may need to be made.

In SSL-VPN portal, the default port used is 443, which is also the port number for HTTPS. While this shouldn't interfere with anything, it can be a good habit to change the port number. FYI, you'd also need to tick custom port number and change the port number to the corresponding port number in FortiClient when establishing the connection.

Our lab is a basic demonstration of how this lab can be set up. More changes need to be made if you want a more secure connection, such as custom certificates…

Conclusion

In conclusion, Fortinet is a useful tool that can mitigate threats and risks while providing secure remote access to users. It allows users to remote access desktop and bypass geographical limitations while securely encrypting data. Fortinet VPN can benefit wide range of uses, from individual use to corporate management.

FortiGate FortiGate-40F

Setting up Site to Site VPN and Remote Access with Fortigate-40F

Jeffrey Yiu Cheung

Purpose

This lab report demonstrates a way to set up Site to Site VPN with two Fortinet FortiGate-40F firewalls and enable remote access.

Background information

In the modern age, being able to securely access private network remotely is important for work and organizations. With cybersecurity threats constantly evolving, hackers can utilize new knowledge to breach sensitive data. To prevent sensitive information from being risked, Fortinet designed and offers its own VPN to its customers.

Remote Access technology enables users to connect to a computer, network, or system regardless of geographical barriers. This technology can enable the ease of accessing files, managing systems, and running applications. While not all businesses may benefit from this, this technology is a staple to telecommuters (those who work from home), business travels, or those needing to work offsite due to distance or other barriers. While this technology is convenient, it requires for a lot of security to maintain.

Fortinet, Inc. is a cybersecurity company headquartered in Sunnyvale, CA. it is a leader in the Cybersecurity industry, securing over 700,000 enterprises and organizations worldwide. It leads the industry in training individuals and has made innovations to incorporate AI into their business. Fortinet made it their mission to educate 1,000,000 people by 2026.

With new technologies constantly enabling the ease of interaction with the web, more information is being uploaded every second. There is useless information, educational information, but there are also sensitive, personal information in the web. To prevent these cybersecurity threats, Fortinet offers cybersecurity devices and programs like firewalls malware prevention programs.

GUI or Graphics Users Interface, is a really nice aspect of the Fortinet Firewalls. Compared to other firewalls like for example the Palo Alto firewalls' GUI, Fortinet firewall GUI is clean and user-friendly, and an overall great upgrade. GUI is an underrated and important aspect of firewalls and their configurability. It can have a big impact on efficiency, reduced errors, and improved user experiences.

VPNs, or virtual private networks, is a technology that allows users to securely connect to private networks over the internet. By creating a tunnel and encrypting data with advanced protocols like IPsec and SSL/TLS to ensure protection against eavesdropping attacks and other threats. VPNs provides stronger privacy and security online, and on top of this, it also allows users to bypass geographical limitations.

SSL, or Secure Sockets Layer, is a protocol that encrypts data through the application layer. Compared to IPsec, or internet protocol security, it is easier to set up, and completes the same goal if users use web-based applications. However, unlike IPsec, it does not provide end-to-end

encryption for all network traffic and is less broad. While SSL VPN is good for this demonstration, one should consider IPsec to be the better option.

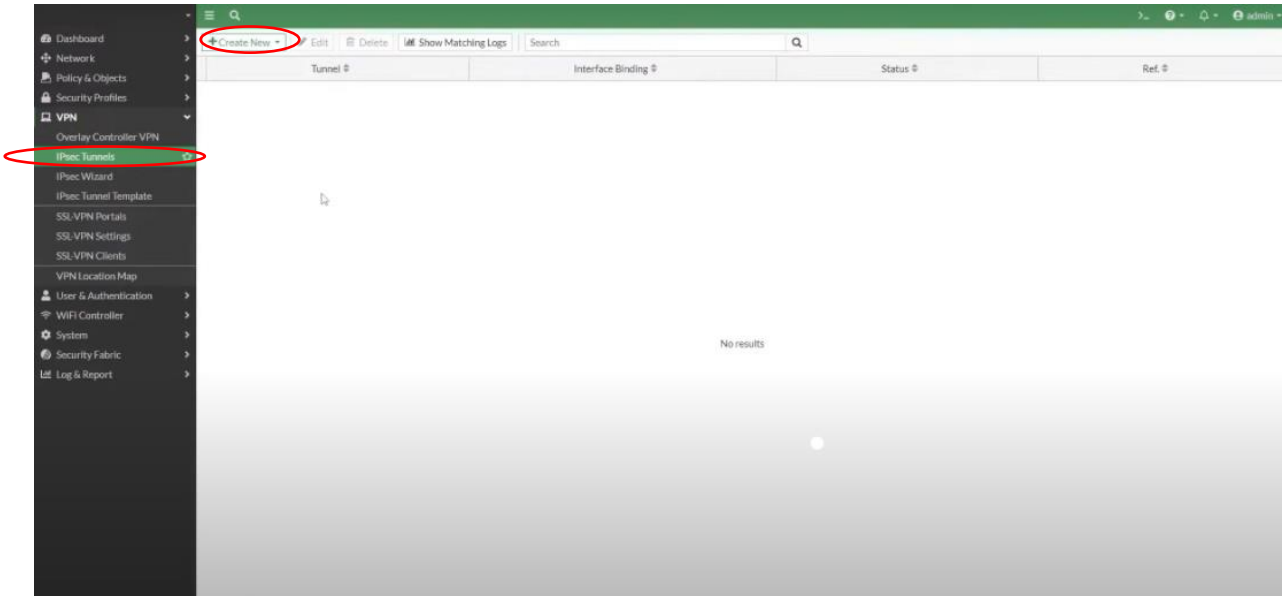
IPsec, an encryption protocol used by GlobalProtect, is a combination of other security protocols to create a protocol that ensures security, integrity, and authentication. It uses protocols like Authentication Header and Encapsulation Security Payload. IPsec follows AES (Advanced Encryption Standard), a highly secure and efficient encrypting algorithm. Although IPsec is secure, it is resource intensive and may drop performance.

Remote Desktop Protocol is a service provided by Microsoft which allows users to connect and control another device via IP (or domain name if applicable). This technology allows users to work, access files, using the computer despite not physically having the machine they need. However, RDP needs the devices to be on the same network, and RDP is vulnerable to cyberattacks, with unrestricted port access and other exploits like BlueKeep, and thus is necessary to run it within a VPN.

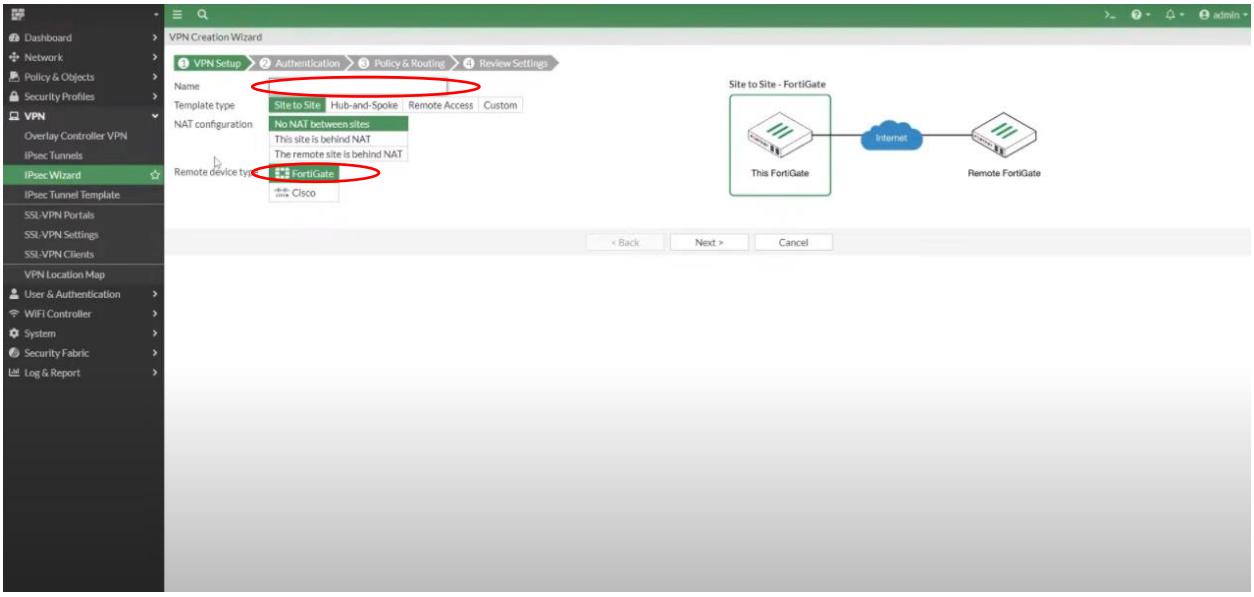
Microsoft is one of the largest and most influential technology company to have exist. Founded in 1975, Microsoft developed and revolutionize how commercial computers are built. Their products range from Operating Systems (windows), computers, software (Microsoft Office), cloud services, and videogames. Today, Microsoft is a technology giant that shape ongoing technology development.

Lab summary

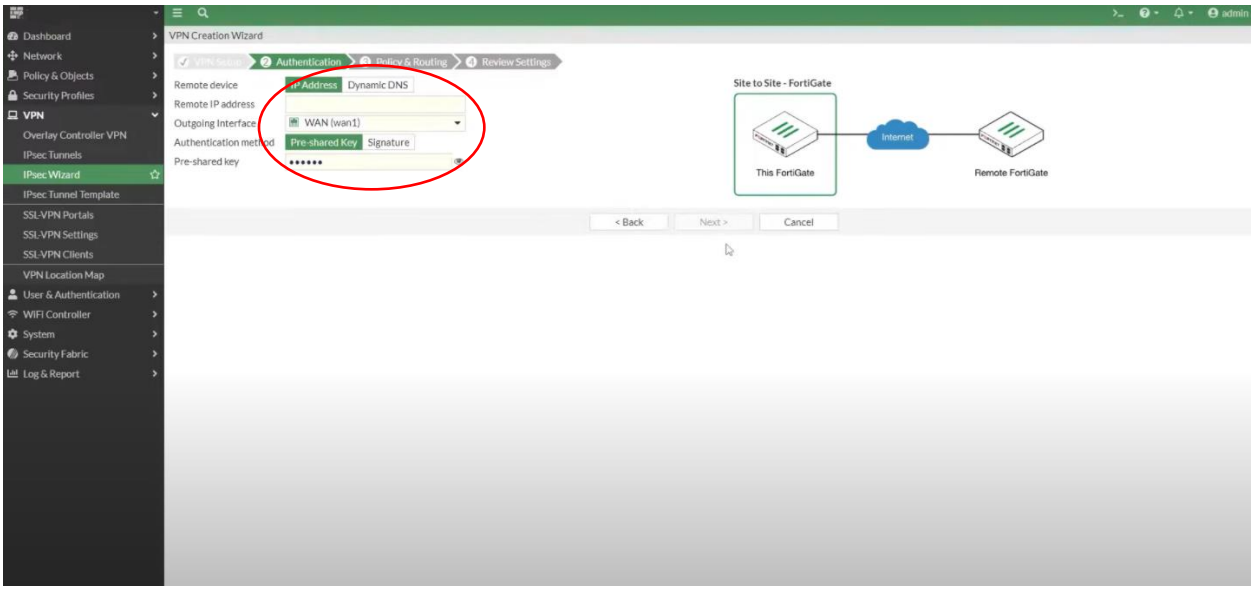
First, create a new IPsec Tunnel in the VPN tab.



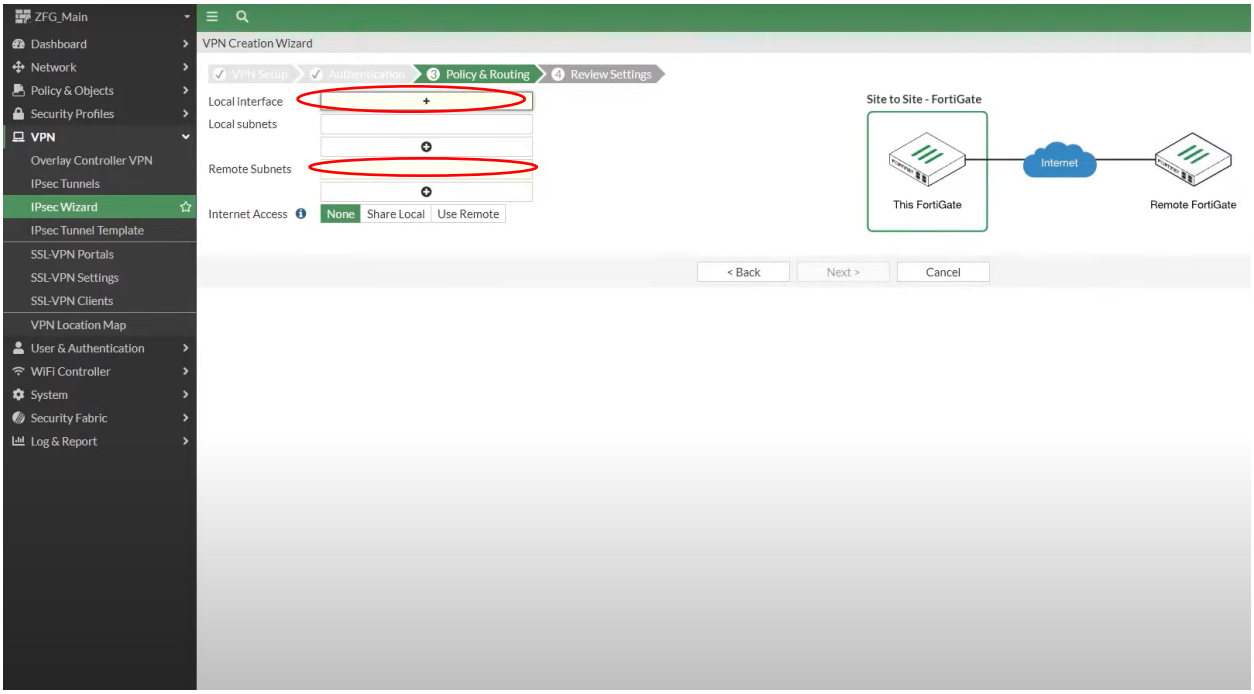
Through the VPN creation Wizard, choose the template type as Site to Site, set the remote device type as FortiGate, and finally, give it a name.



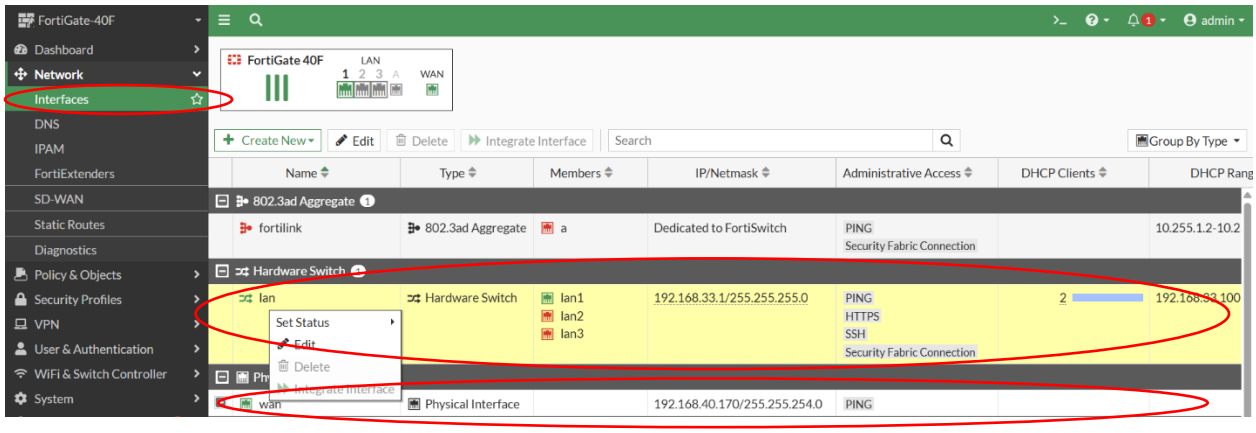
Next, set the outgoing interface as your WAN, and put the Remote IP address as the other device's WAN's IP address. The PSK needs to be the same on both devices.



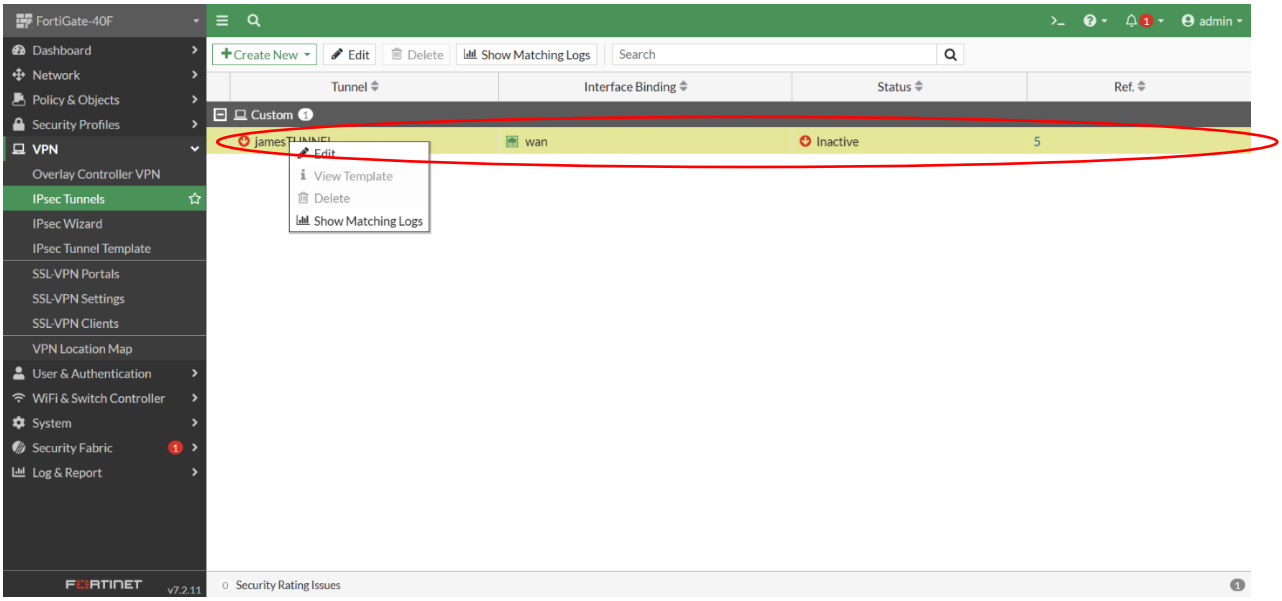
Next, in Policy & Routing, use your LAN as the Local Interface. For the local subnet, use the subnet of your LAN network, and for the Remote local address, use the other device's LAN address.



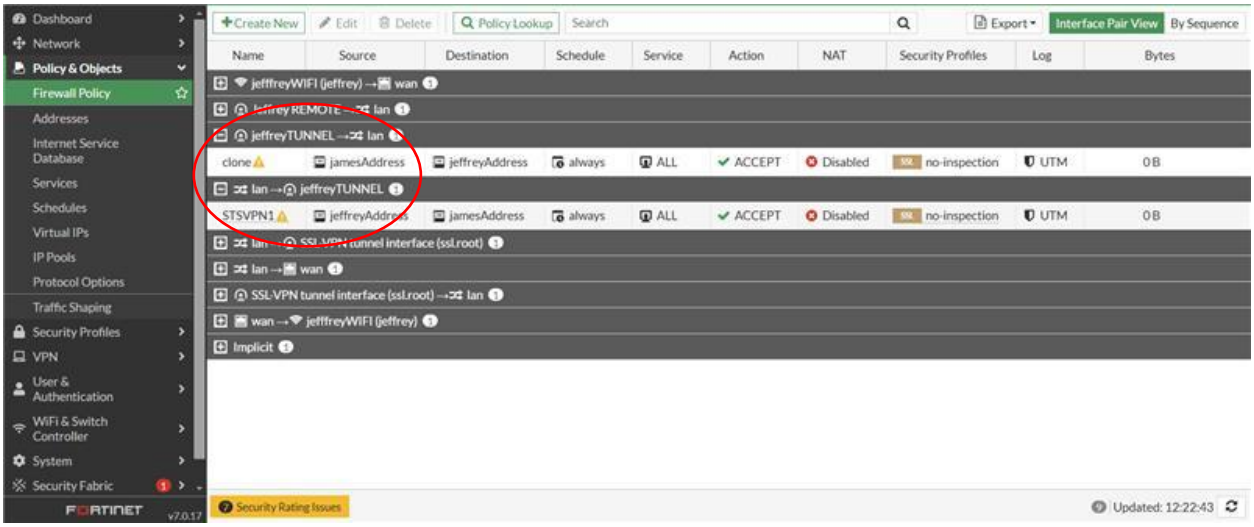
You can check the device's LAN's or WAN's IP address in the Network tab.



Next, review your configuration and finalize, then create. Afterwards, you should have this in your IPsec Tunnel tab.

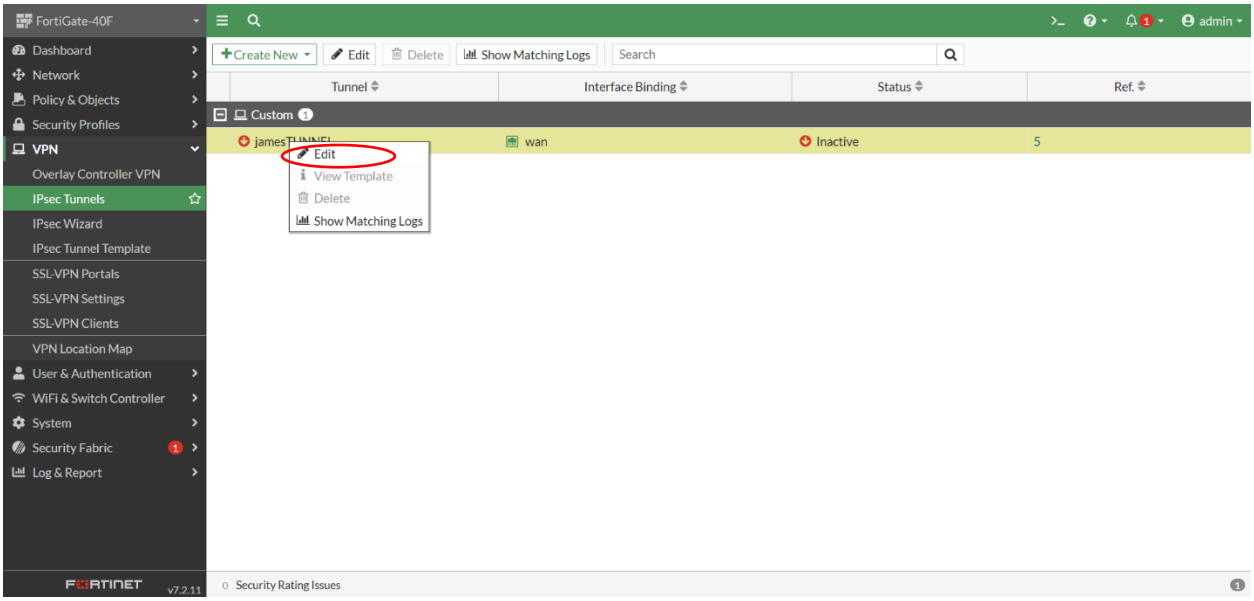


This process should automatically create the firewall policies that allows traffic from the VPN to the LAN, and from LAN to VPN. But if not, you can create through the Firewall Policies Tab.

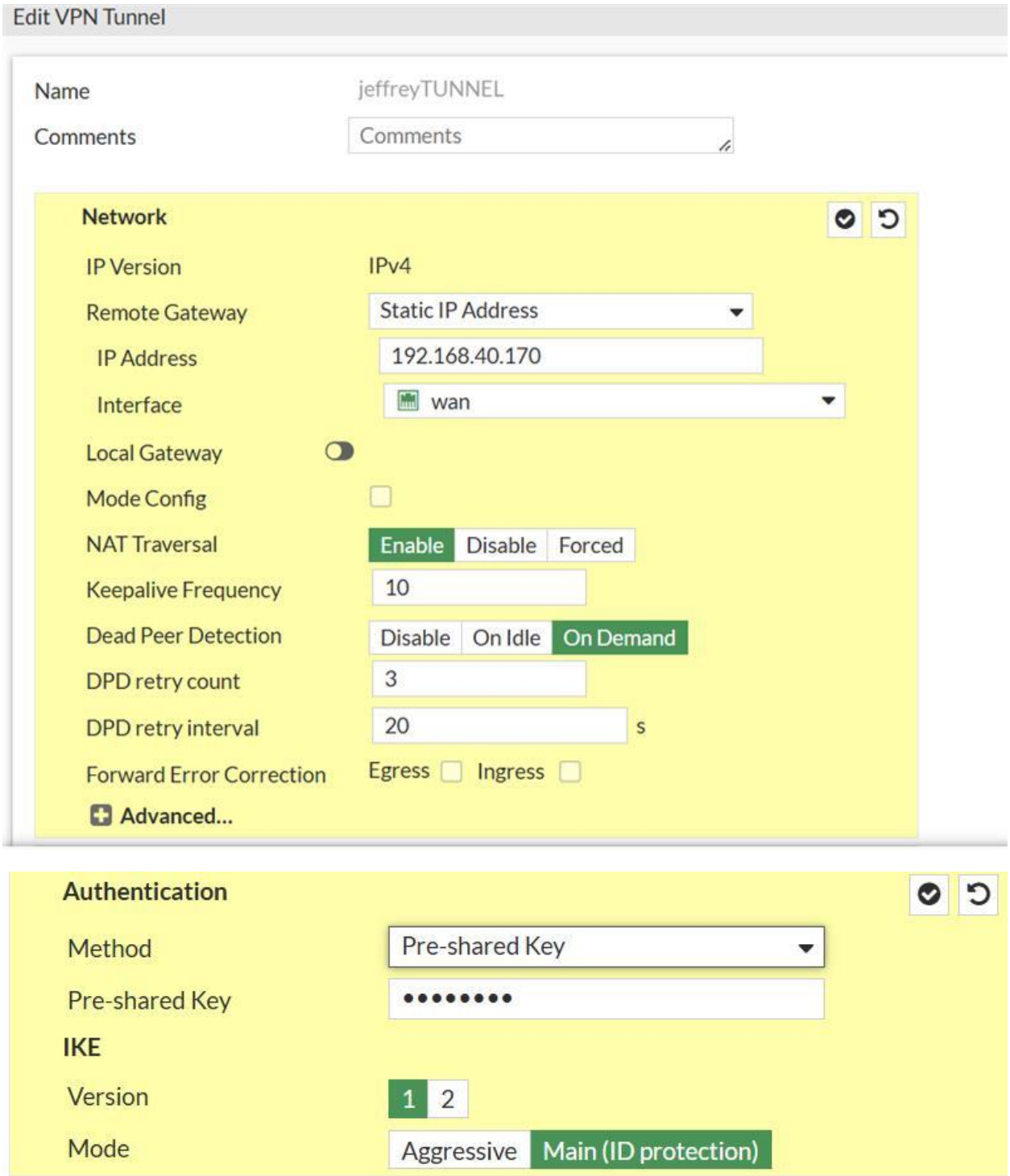


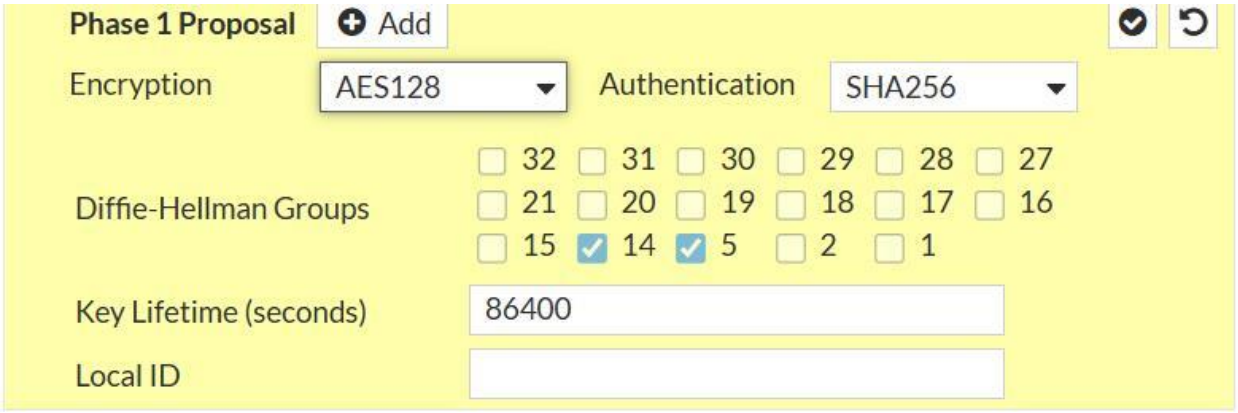
Next, in the other firewall device, create a tunnel with the same configurations aside from the name (optional).

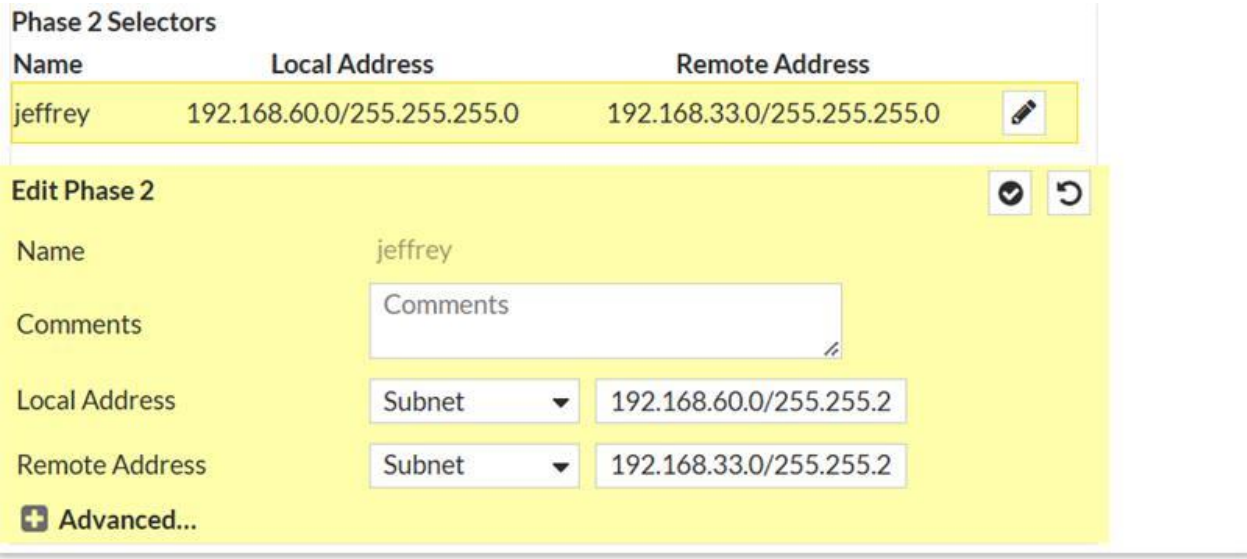
If you want to be sure, you can edit a tunnel to compare the tunnels.



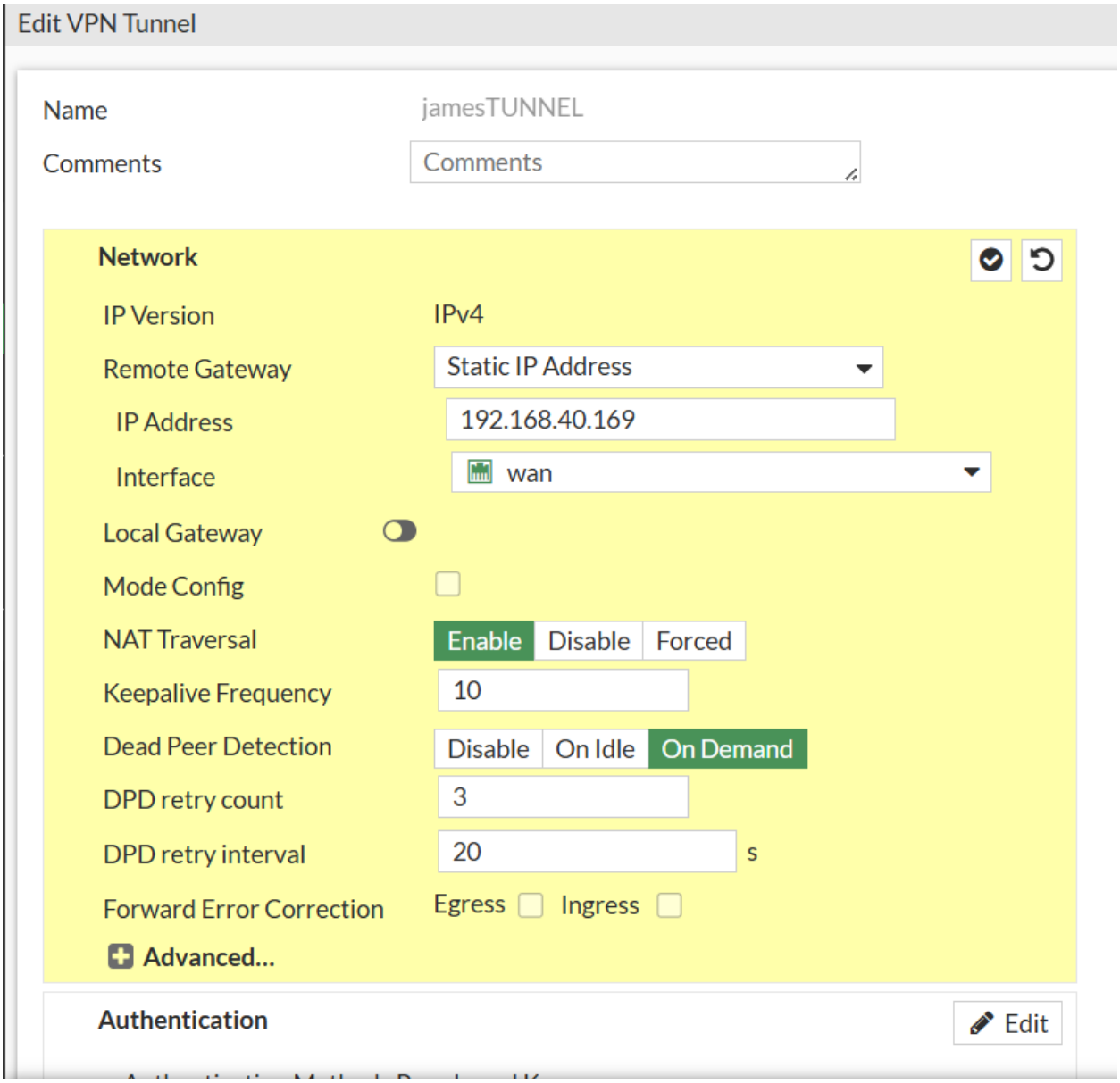
This is the settings for JeffTunnel


Edit VPN Tunnel
Name
jeffreyTUNNEL
Comments
Comments
Network
IP Version
IPv4
Remote Gateway
Static IP Address
IP Address
192.168.40.170
Interface
wan
Local Gateway
Mode Config
NAT Traversal
Enable
Disable
Forced
Keepalive Frequency
10
Dead Peer Detection
Disable
On Idle
On Demand
DPD retry count
3
DPD retry interval
20
s
Forward Error Correction
Egress
Ingress
Advanced...
Authentication
Method
Pre-shared Key
Pre-shared Key
IKE
Version
1
2
Mode
Aggressive
Main (ID protection)



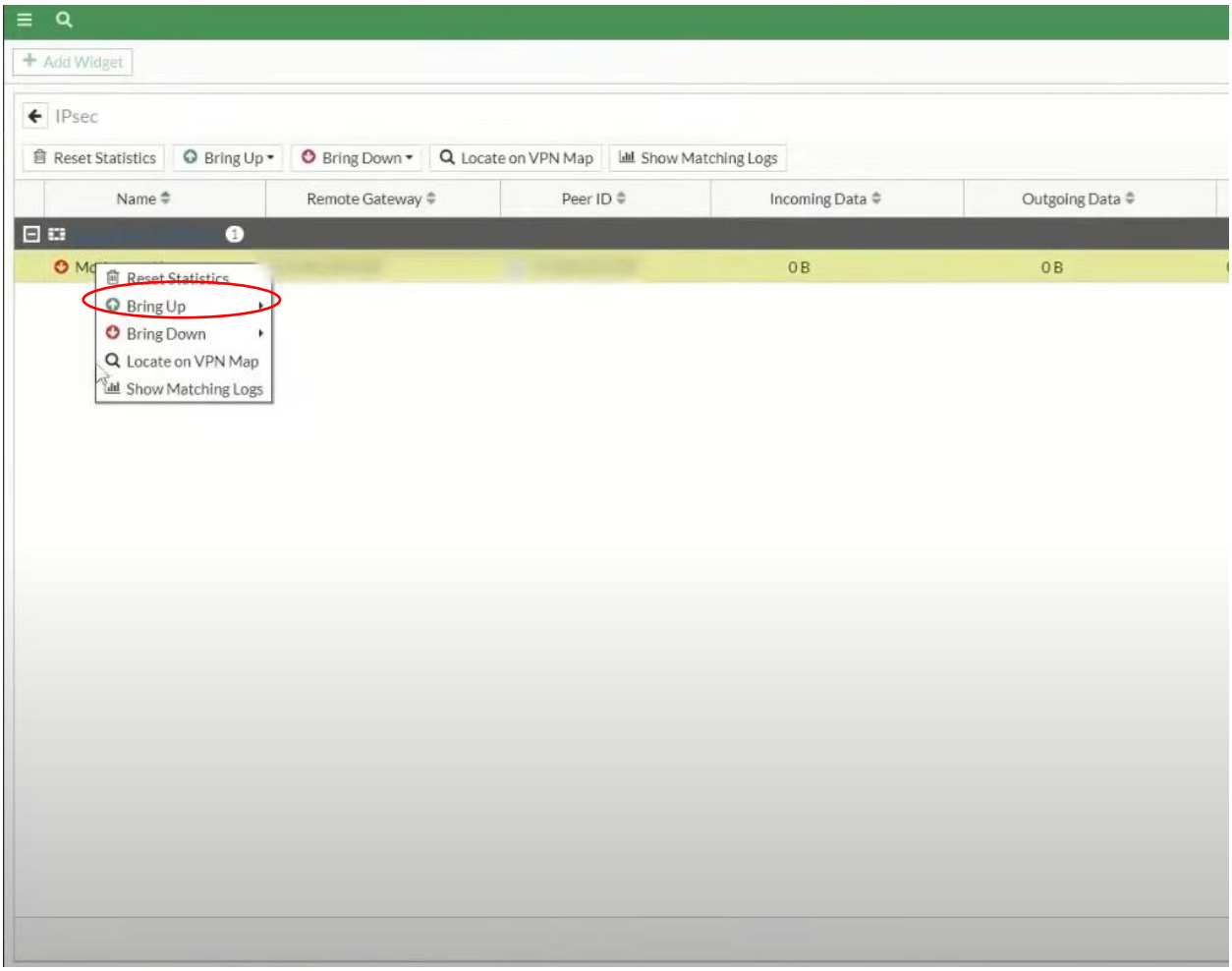


And this is the settings for JamesTunnel


Edit VPN Tunnel
Name
jamesTUNNEL
Comments
Comments
Network
IP Version
IPv4
Remote Gateway
Static IP Address
IP Address
192.168.40.169
Interface
wan
Local Gateway
Mode Config
NAT Traversal
Enable
Disable
Forced
Keepalive Frequency
10
Dead Peer Detection
Disable
On Idle
On Demand
DPD retry count
3
DPD retry interval
20
s
Forward Error Correction
Egress
Ingress
Advanced...
Authentication
Edit

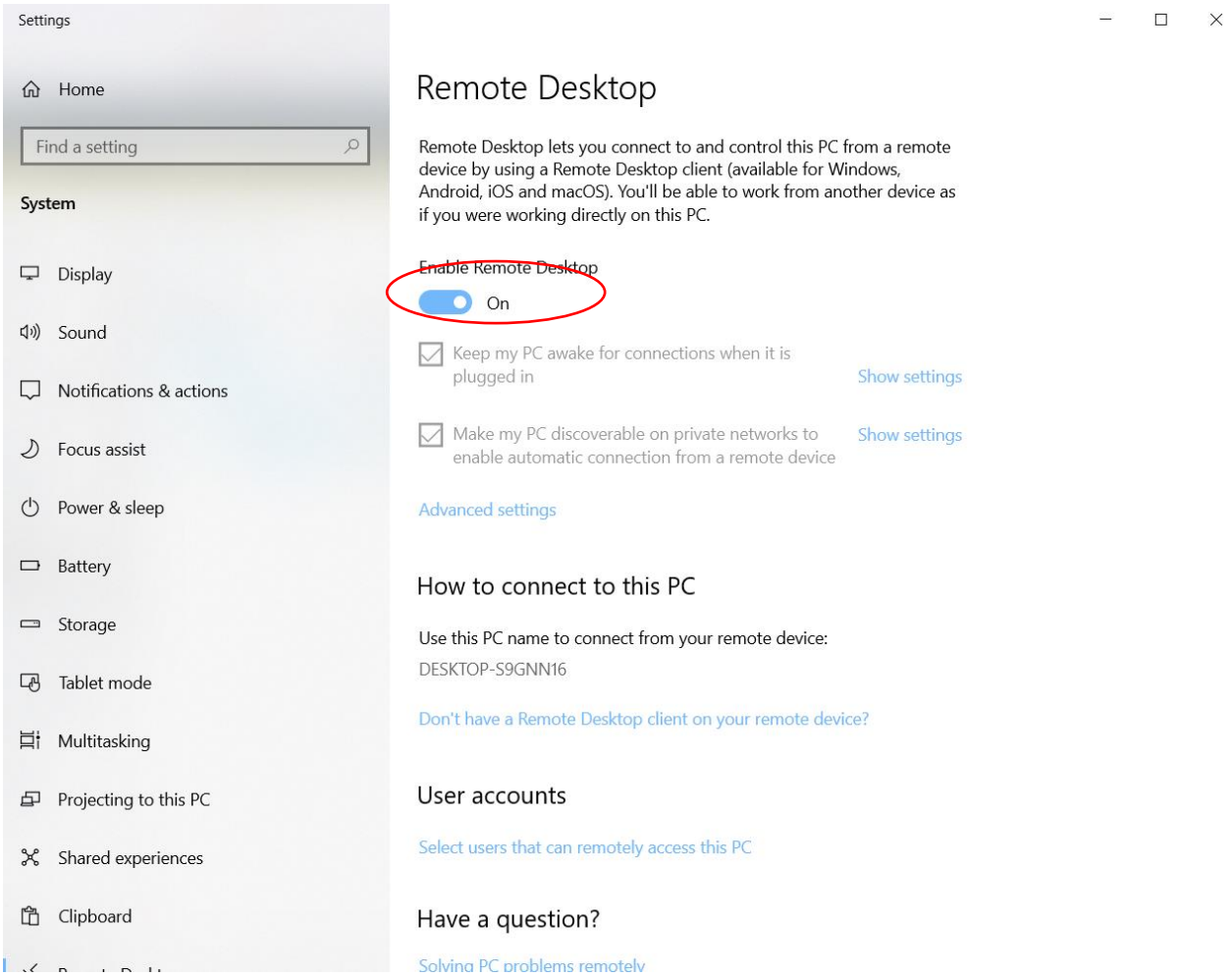
Again, the Pre-shared Keys NEEDS to be the same.

After this, there should be an option to Bring Up the tunnel.



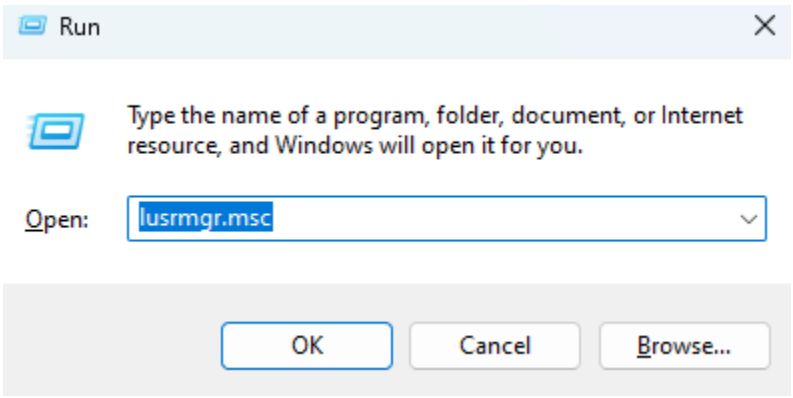
Afterwards, the tunnel is all set.

To set up Remote Access, you need to first turn on Remote Access in computer's settings.

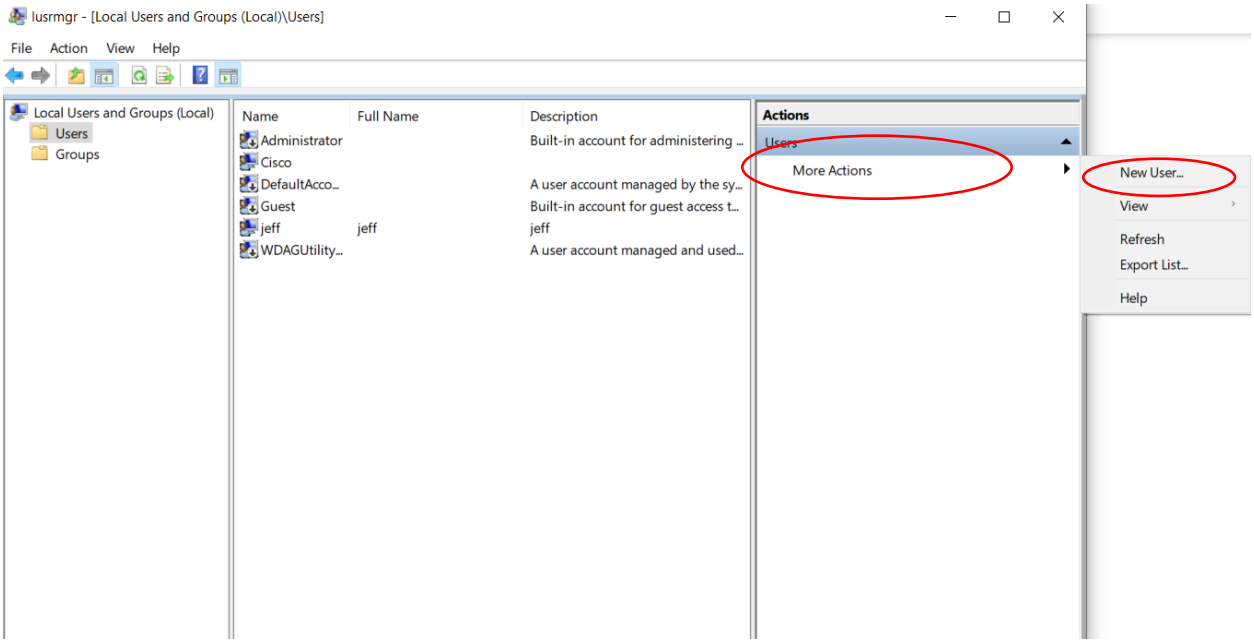


Now, for the device in the internal network, or the device in the network that you want to connect to, create a user or give an existing user permission to access Remote Desktop.

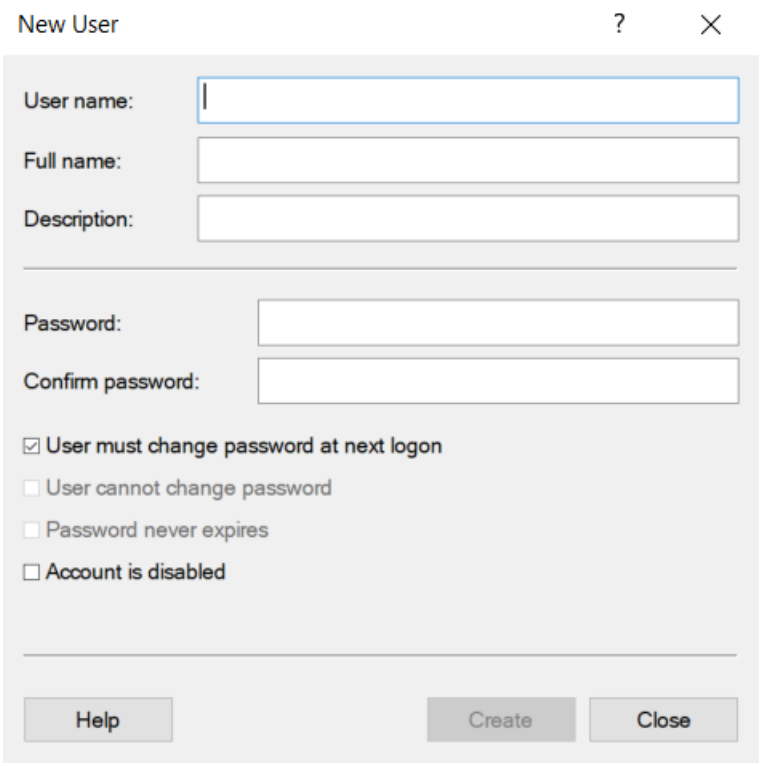
Then, open Run (or Windows + r on windows, command + space on mac) and type in lusrmgr.msc.



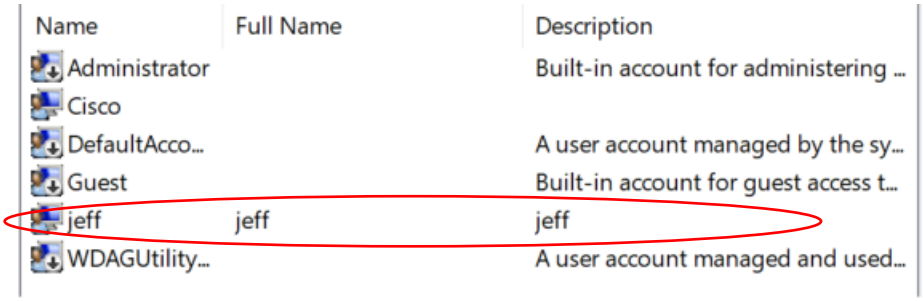
This should pop up. Select Users and add new user (if necessary).



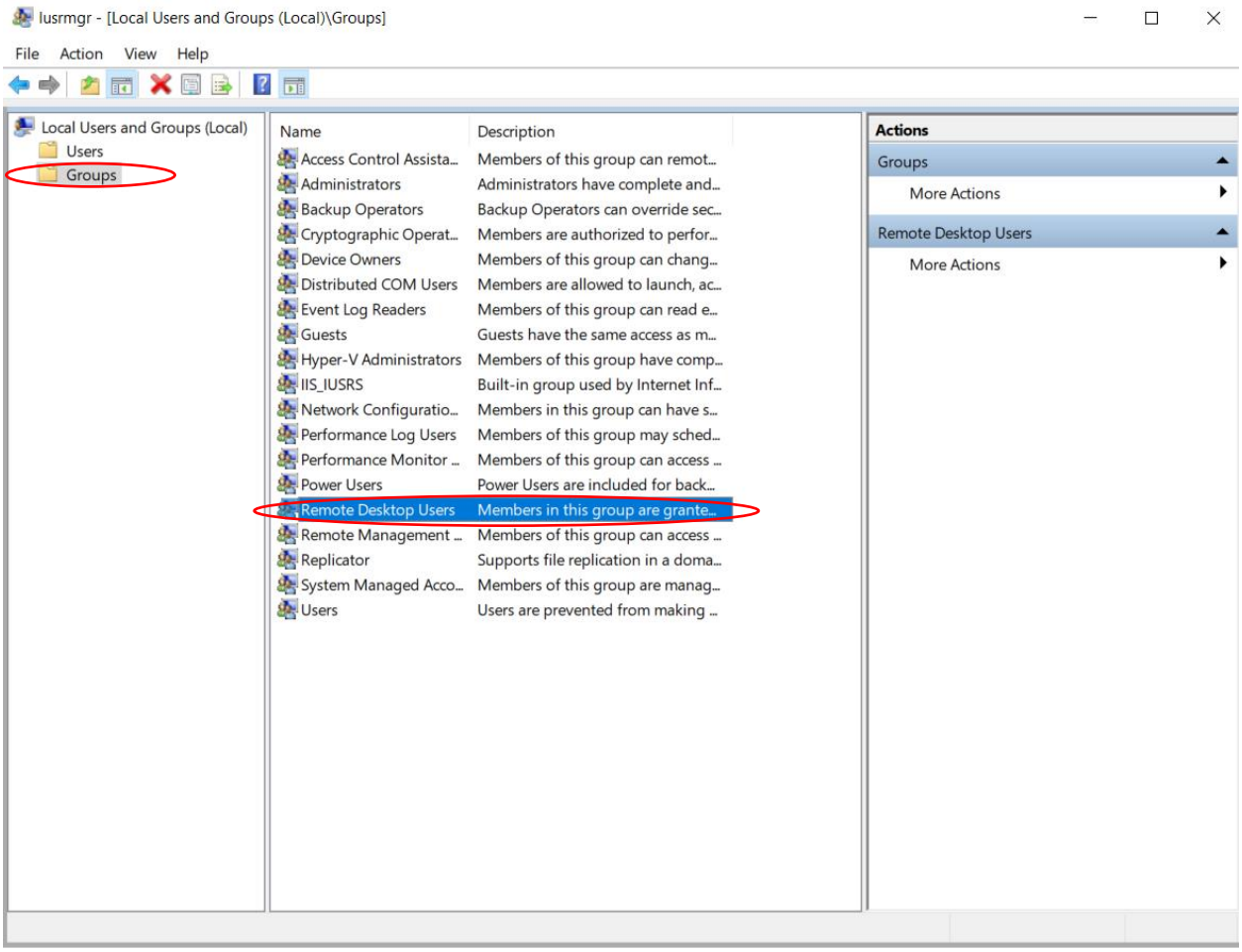
Next, add a user, give it a username and password (if necessary). You can check off requiring changing password next logon (optional).



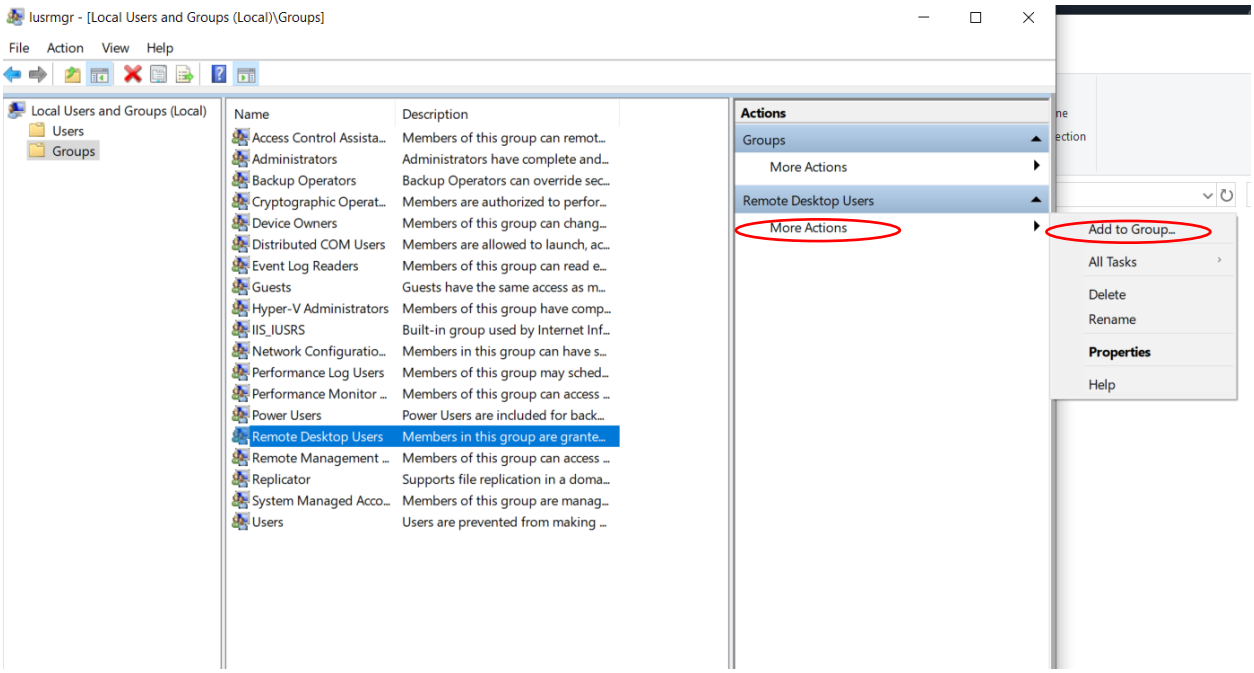
It should look like this.

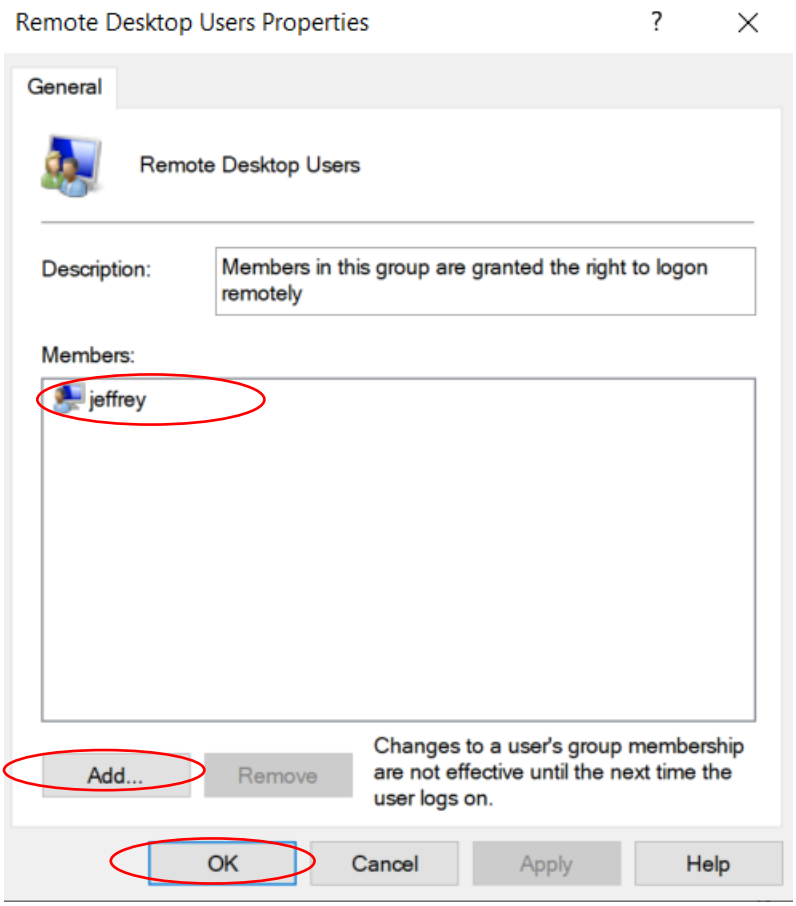


Next, go to groups. There should be a group named Remote Desktop Users.



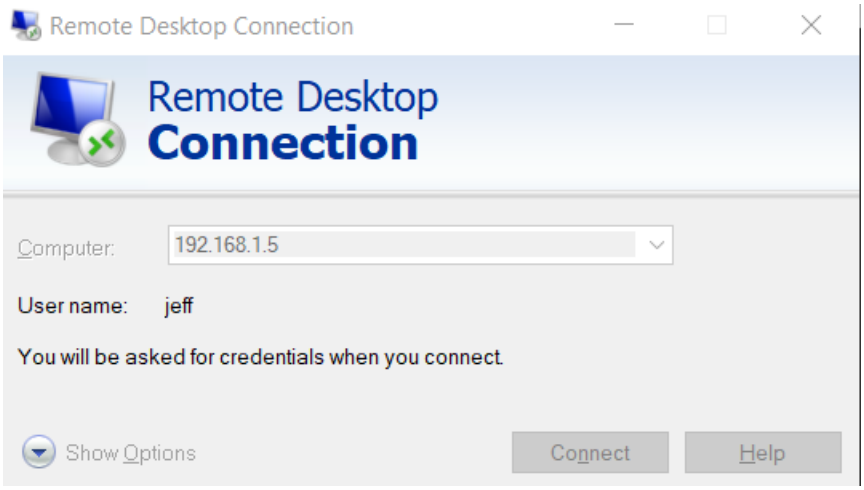
Next, add the user you've made, or an existing user, into the group to give them permission.





If you have reset password on next logon enabled, you have to reset the password before you can use the user.

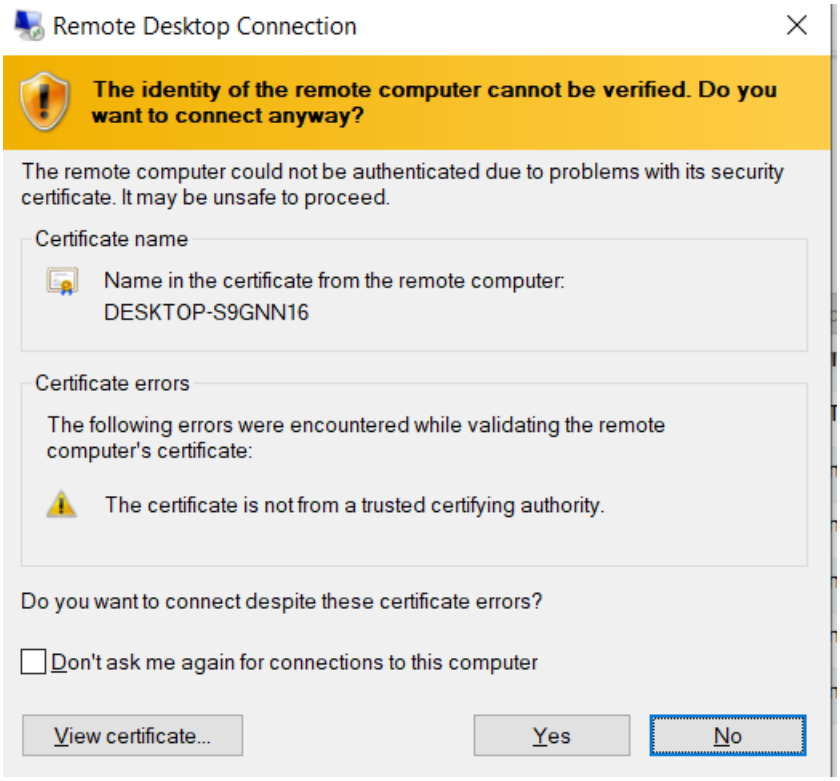
Next, using the other device, remote access into the desired device via Remote Desktop Connection.



In computer, you will need to input the desired device's IP address. This can be found in Command Prompt with the command "ipconfig /all".

```
Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) Ethernet Connection (3) I218-LM
   Physical Address. . . . . . . . . : 54-EE-75-75-94-1D
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::75ec:339b:9a6f:c202%20(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.1.3(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Monday, January 6, 2025 3:06:37 PM
   Lease Expires . . . . . . . . . . : Tuesday, January 7, 2025 3:06:36 PM
   Default Gateway . . . . . . . . . : 192.168.1.254
   DHCP Server . . . . . . . . . . . : 192.168.1.254
   DHCPv6 IAID . . . . . . . . . . . : 206892661
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-2A-C6-6E-3F-54-EE-75-75-94-1D
   DNS Servers . . . . . . . . . . . : 9.9.9.9
                                       1.1.1.1
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

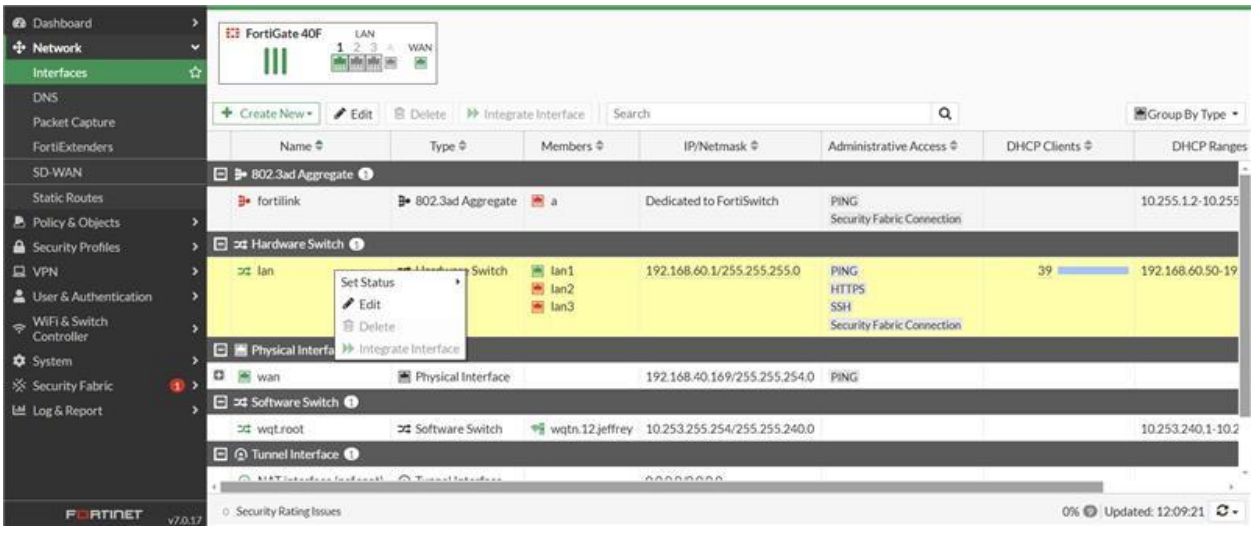
If successful, you should be prompted with this:

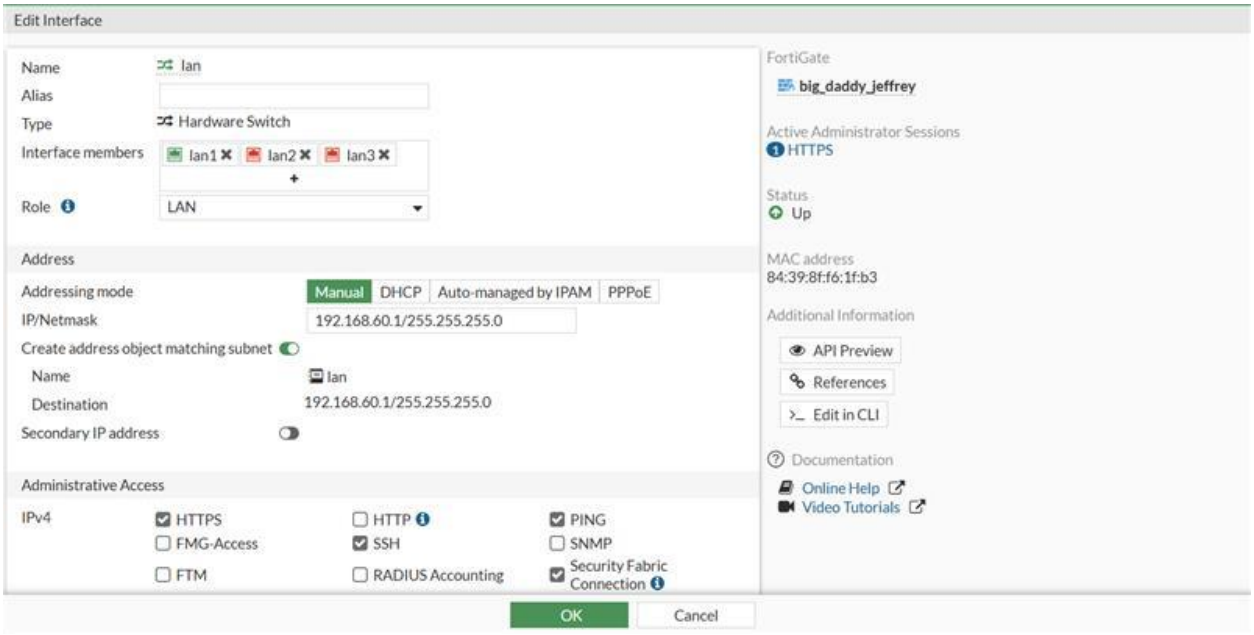


Just click Yes, and then you're all set.

Problems

This is a lab that shouldn't prove to be too difficult. However, we still ran into some encounters with obstacles. In our lab setting, since everybody had the same default LAN at first, we had to change it before getting into the lab.





On top of this, me and my partner were stuck for a little bit when we created the tunnel but couldn't find the option to bring it up. After a while, we found out that it was an option on the other device.

While these were minor nuisances, they can still be annoying to deal with, and there are probably many more that we haven't discovered.

Conclusion

In conclusion, Fortinet Firewalls are useful tools that can mitigate threats and risks while providing secure remote access to users. It can allow users to remote access desktop and bypass geographical limitations while securely encrypting data.