Palo Alto / Fortinet Firewall Lab Configurations

Andrew Pai

Table of Contents

Palo Alto PA-220 Firewall Factory Reset

Andrew Pai

Purpose:

The purpose of this lab was to factory reset a Palo Alto PA-220 firewall. This allowed our team to recover access to the firewall and create our own login credentials as well as gain an understanding of the PA-220's boot sequence and maintenance mode.

Background Information:

Palo Alto Networks is a networking company that focuses on providing cybersecurity and devices to clients. Founded in 2005, Palo Alto started out as a firewalls company before expanding to fields such as endpoint protection, malware prevention, machine learning, and data analysis. Some notable aspects of Palo Alto are that they co-founded the Cyber Threat Alliance, intended to raise the standard of cybersecurity by pooling information between companies. They also run the Unit 42 Research Team, which is a group of experts dedicated to discover world-wide cyberthreats such as Gorgon, Xbash, and Cannon.

Like mentioned above, Palo Alto specializes in creating firewalls for public use. Firewalls work to watch traffic going in and out of a device and block off any suspicious activity. Because firewalls separate your own network from other networks like the Internet by sitting on a network edge, firewalls can often be crucial in making sure your network maintains secure. Firewalls work by comparing packets being transmitted in and out of the network to a set of rules and deciding to let it pass based on the results. There are many types of firewalls like packet filtering firewalls, proxy firewalls, stateful inspection firewalls, AI-powered firewalls, and next-generation firewalls.

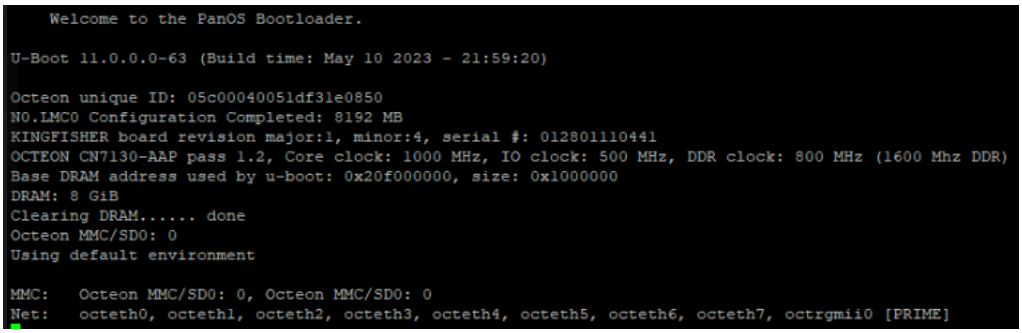
This lab will be focused on the PA-220 firewall that Palo Alto creates, which is a type of next-generation firewall. Next-generation firewalls can provide everything other firewalls like stateful inspection firewalls do, but also provides things like intrusion prevention and URL filtering.

Since firewalls provide such a large amount of security to your network, it is absolutely critical that you know and have the login credentials to your PA-220. In the case that the PA-220 has been passed down and has currently existing login credentials, it is necessary to perform a factory reset which wipes all data, settings, and configurations on the firewall, allowing you to create new login credentials and configure it for your purposes.

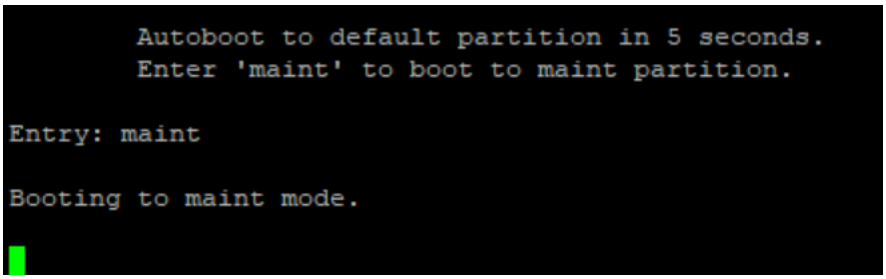
Lab Summary:

Connect your PA-220 device to a computer using a Console cable and power it on.

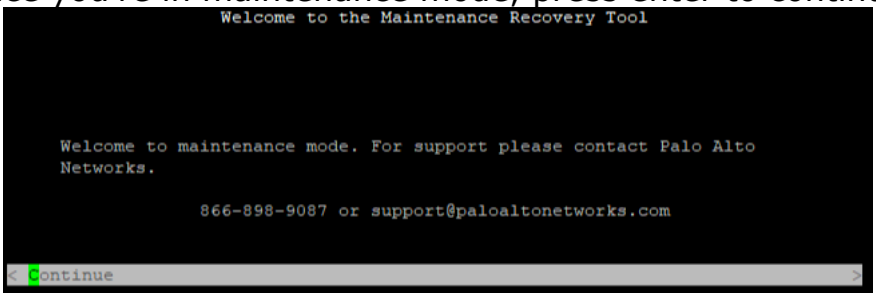
This should automatically put your device into bootloader, as shown below.



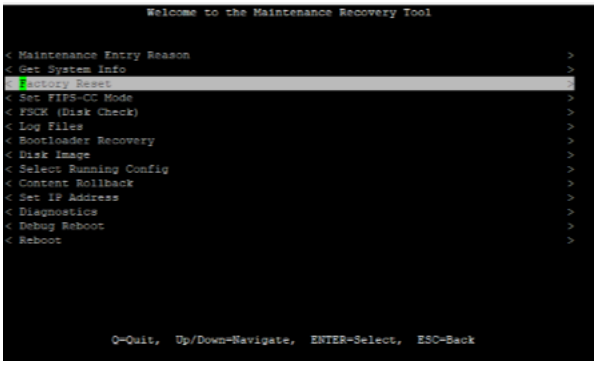
Once prompted, enter maintenance mode by typing “maint” into the “Entry” prompt.



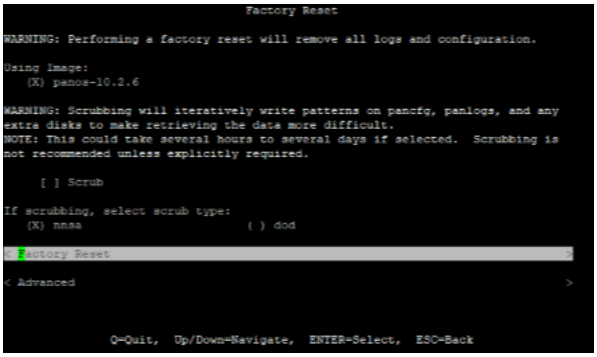
Once you’re in maintenance mode, press enter to continue.



Inside the maintenance recovery tool, arrow down to “Factory Reset” and press enter.

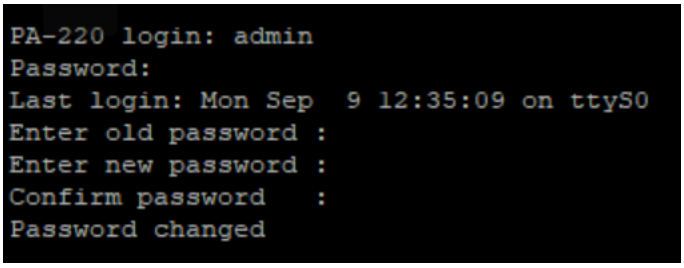


Confirm that you would like to factory reset your PA-220 by arrowing down to “Factory Reset” in the menu and pressing enter.



Once factory resetting, your PA-220 will take anywhere from 10-30 minutes to reset.

Finally, you will be able to reset your PA-220 by using the default login and password of admin/admin for the firewall and setting your own password.



Lab Commands:

The only command used in this lab was the "maint" command, which we entered once the firewall bootloader finished. By entering "maint," our group was able to the PA-220's maintenance mode, which allowed us to access various settings of the firewall. In this lab, getting into maintenance mode was used purely to factory reset our machine by selecting the factory reset option.

Problems:

One of the problems that we had with this lab was mainly the unexpected amount of time that the firewall took to boot up. While we were expecting something around 3-5 minutes for the firewall to boot up, the actual loading time was somewhere around the 20 to 30 minute range. Because the loading time was so much longer than what our group expected, we disconnected and reconnected the firewall to various computers testing if the "problem" was because of a specific cable of computer. This reset our progress every time and caused us to lose time. In the end, what helped us was realizing the 3 lights on the PA-220 would have to all be up for the firewall to have finished loading. This allowed us to gain the patience to wait out the loading period for the firewall and proceed with the factory reset.

Conclusion:

In conclusion, this lab was meant to factory reset a PA-220 firewall from Palo Alto to let our group set our own login credentials instead of using the credentials set by a previous group. To do this, we simply used maintenance mode and Palo Alto's written tutorial to reset our firewall. The biggest challenges that we faced was the fact that we didn't know how long the firewall should load for, and therefore our preconceptions of load time caused us to reset on progress multiple times. Going forth, our group should simply have more patience or truly confirm if there is a problem before trying to fix anything.

Palo Alto PA-220 SOHO Network Configuration

Andrew Pai

Purpose:

The purpose of this lab was to configure our Palo Alto PA-220 firewall to be suitable for a small office home office (SOHO) network. Now that our firewall has been factory reset, we need to make sure that its configuration is able to effectively protect a network. This SOHO configuration includes setting security zones, interfaces, VLANs, DHCP, and DNS.

Background Information:

A Small Office Home Office (SOHO) network is a basic network meant for individuals or small businesses to use. Typically, the range of individuals connected is anywhere from 1 to 10, and usage of a SOHO network allows for the centralization of resources or ability to connect to a corporate network. Because they aren't as big and aren't as complex as other networks, SOHO networks are the easiest to set up and use. SOHO networks are also referred to as "virtual offices" and essentially encompass a local area network (LAN) which can get access to a larger network.

Since we want to ensure that our SOHO networks are secure and that there is no malicious activity being transmitted onto our network, the configuration of the Palo Alto PA-220 firewall is critical to making sure that our network runs as intended. In order to configure the Palo Alto PA-220 firewall our group entered the GUI, or graphical user interface. On the GUI, we configured various things such as security zones, interface settings, VLANs, DHCP, and DNS.

Security zones on a firewall consist of various physical or virtual interfaces grouped together to be controlled as a cluster by the firewall. Security zones allow for the firewall to better manage multiple interfaces at once. For each security zone, there are different security policy rules that determine what the firewall does with different types of packets. While packets and traffic can move around unhindered inside of a security zone, the point of a security zone is to check the traffic between various zones to maintain network integrity.

Firewall interfaces are areas of the firewall that transmit and receive data. In a SOHO configuration, it is important to configure the interface type to determine what type of data it can receive/transmit and the security zone to group the interface with other interfaces that it can trust.

Virtual Local Area Networks (VLANs) are similar to security zones in the way that they group together various interfaces on the firewall. This makes it much more efficient and organized to divide up sections of the firewall and make it so that traffic that should be separated actually is separated.

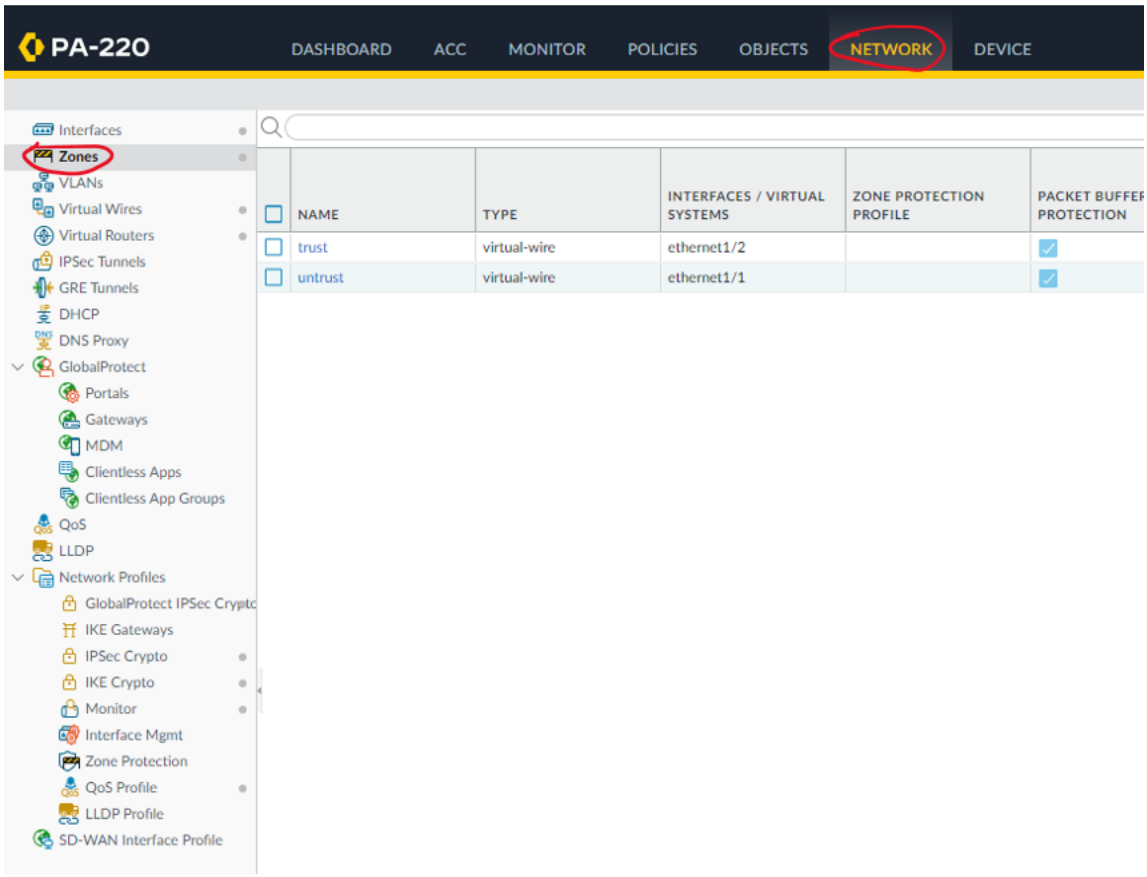
Without security zones and VLANs, the job of one firewall might have to be relegated to multiple firewalls as they would no longer be able to compartmentalize.

Dynamic Host Configuration Protocol (DHCP) and Domain Name System (DNS) are crucial parts of the firewall configuration that come into play for the host computers trying to access networks outside of the SOHO. DHCP is in charge of relegating IP addresses to hosts that need them, allowing traffic to go in and out of hosts. DNS turns domain names into IP addresses, allowing for hosts to successfully transmit and receive traffic from websites online.

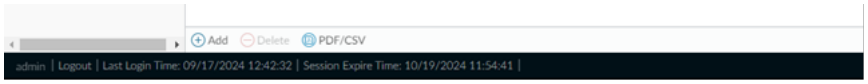
Lab Summary:

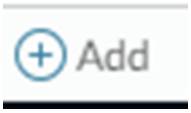
Enter the PA-220's Graphical User Interface (GUI) by inputting the IP address 192.168.1.1 in a web browser. Make sure that the host computer is on the firewall's subnet by setting its IP to something like 192.168.1.2. Enter the login information for the firewall to the box below.

In order to add security zones to the PA-220, first navigate to "Network" on the top taskbar and then to "Zones" on the left taskbar.

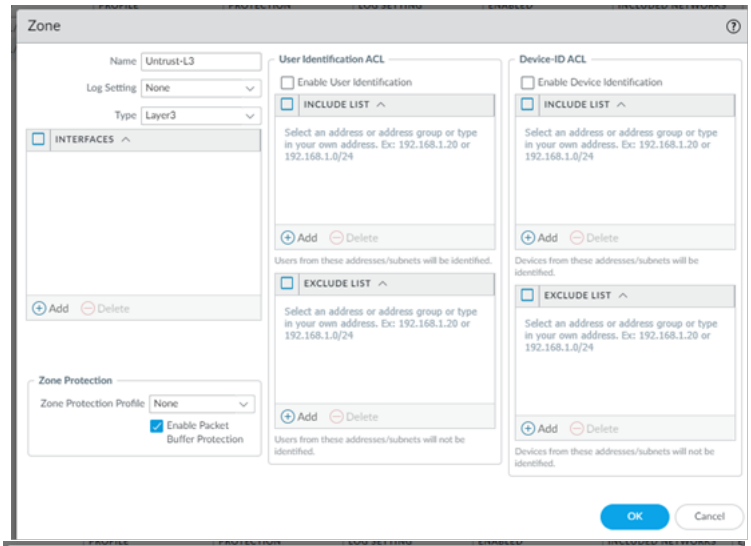


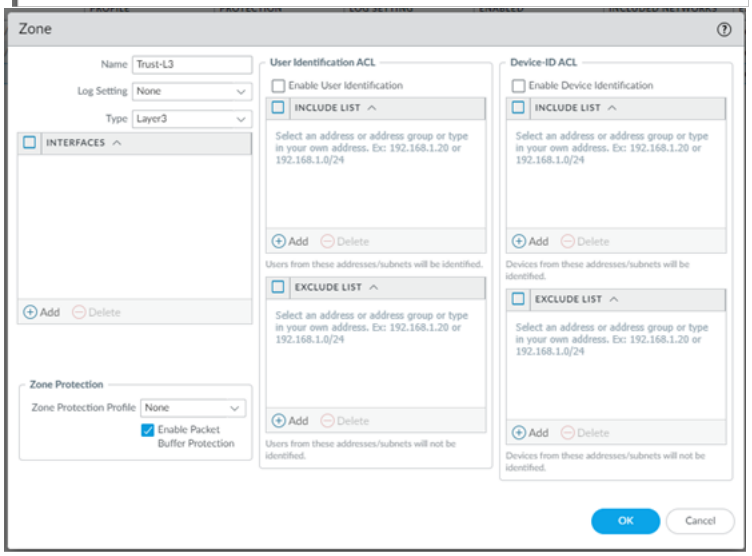
Click “Add” on the very bottom left taskbar in order to add a new zone.

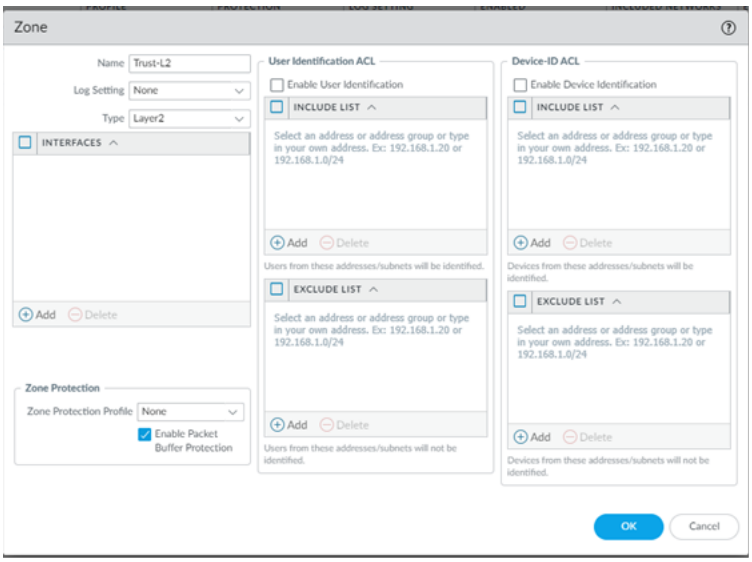




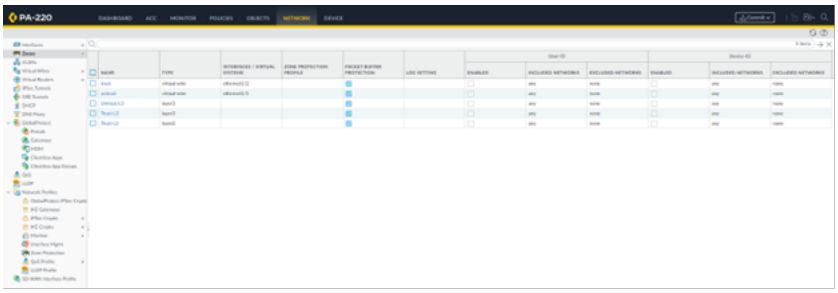
Name the new zone “Untrust-L3” and change the type to “Layer3”. Leave all other settings in the zone untouched. Repeat this process to create a zone named “Trust-L3” that has a “Layer3” type as well as a zone named “Trust-L2” that has a “Layer2” type.


Zone
Name Untrust-L3
Log Setting None
Type Layer3
INTERFACES
Add Delete
Zone Protection
Zone Protection Profile None
Enable Packet Buffer Protection
User Identification ACL
Enable User Identification
INCLUDE LIST
Select an address or address group or type in your own address. Ex: 192.168.1.20 or 192.168.1.0/24
Add Delete
Users from these addresses/subnets will be identified.
EXCLUDE LIST
Select an address or address group or type in your own address. Ex: 192.168.1.20 or 192.168.1.0/24
Add Delete
Users from these addresses/subnets will not be identified.
Device-ID ACL
Enable Device Identification
INCLUDE LIST
Select an address or address group or type in your own address. Ex: 192.168.1.20 or 192.168.1.0/24
Add Delete
Devices from these addresses/subnets will be identified.
EXCLUDE LIST
Select an address or address group or type in your own address. Ex: 192.168.1.20 or 192.168.1.0/24
Add Delete
Devices from these addresses/subnets will not be identified.
OK
Cancel

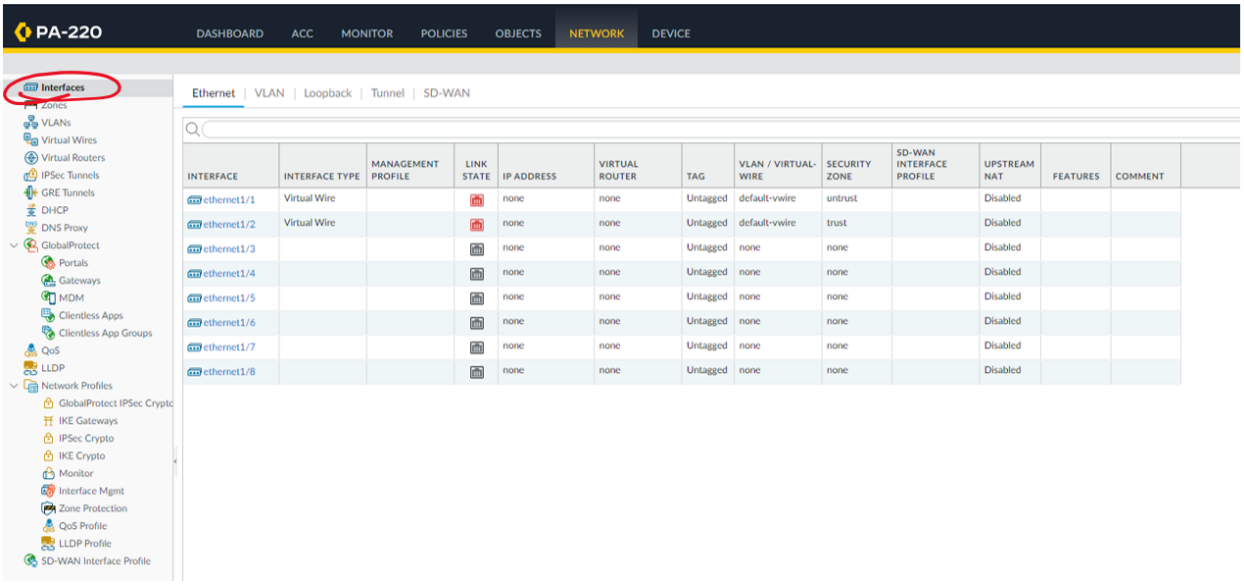

Zone
Name Trust-L3
Log Setting None
Type Layer3
INTERFACES
Add Delete
Zone Protection
Zone Protection Profile None
Enable Packet Buffer Protection
User Identification ACL
Enable User Identification
INCLUDE LIST
Select an address or address group or type in your own address. Ex: 192.168.1.20 or 192.168.1.0/24
Add Delete
Users from these addresses/subnets will be identified.
EXCLUDE LIST
Select an address or address group or type in your own address. Ex: 192.168.1.20 or 192.168.1.0/24
Add Delete
Users from these addresses/subnets will not be identified.
Device-ID ACL
Enable Device Identification
INCLUDE LIST
Select an address or address group or type in your own address. Ex: 192.168.1.20 or 192.168.1.0/24
Add Delete
Devices from these addresses/subnets will be identified.
EXCLUDE LIST
Select an address or address group or type in your own address. Ex: 192.168.1.20 or 192.168.1.0/24
Add Delete
Devices from these addresses/subnets will not be identified.
OK
Cancel


Zone
Name Trust-L2
Log Setting None
Type Layer2
INTERFACES
Add Delete
Zone Protection
Zone Protection Profile None
Enable Packet Buffer Protection
User Identification ACL
Enable User Identification
INCLUDE LIST
Select an address or address group or type in your own address. Ex: 192.168.1.20 or 192.168.1.0/24
Add Delete
Users from these addresses/subnets will be identified.
EXCLUDE LIST
Select an address or address group or type in your own address. Ex: 192.168.1.20 or 192.168.1.0/24
Add Delete
Users from these addresses/subnets will not be identified.
Device-ID ACL
Enable Device Identification
INCLUDE LIST
Select an address or address group or type in your own address. Ex: 192.168.1.20 or 192.168.1.0/24
Add Delete
Devices from these addresses/subnets will be identified.
EXCLUDE LIST
Select an address or address group or type in your own address. Ex: 192.168.1.20 or 192.168.1.0/24
Add Delete
Devices from these addresses/subnets will not be identified.
OK
Cancel

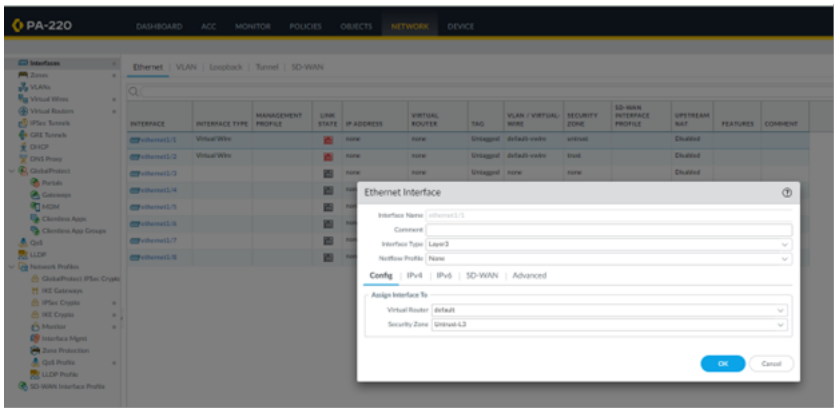
When you finish inputting the three zones, your Zones under Network should look like the picture below.



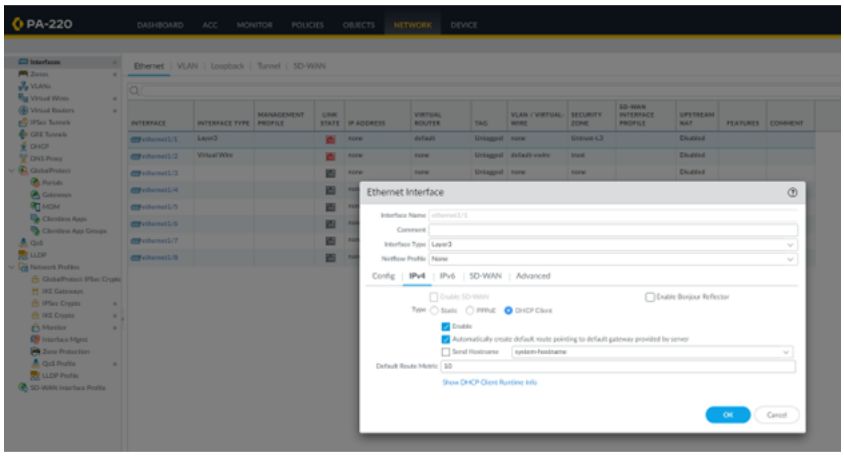
From the Network tab, enter the “Interfaces” section from the left taskbar.



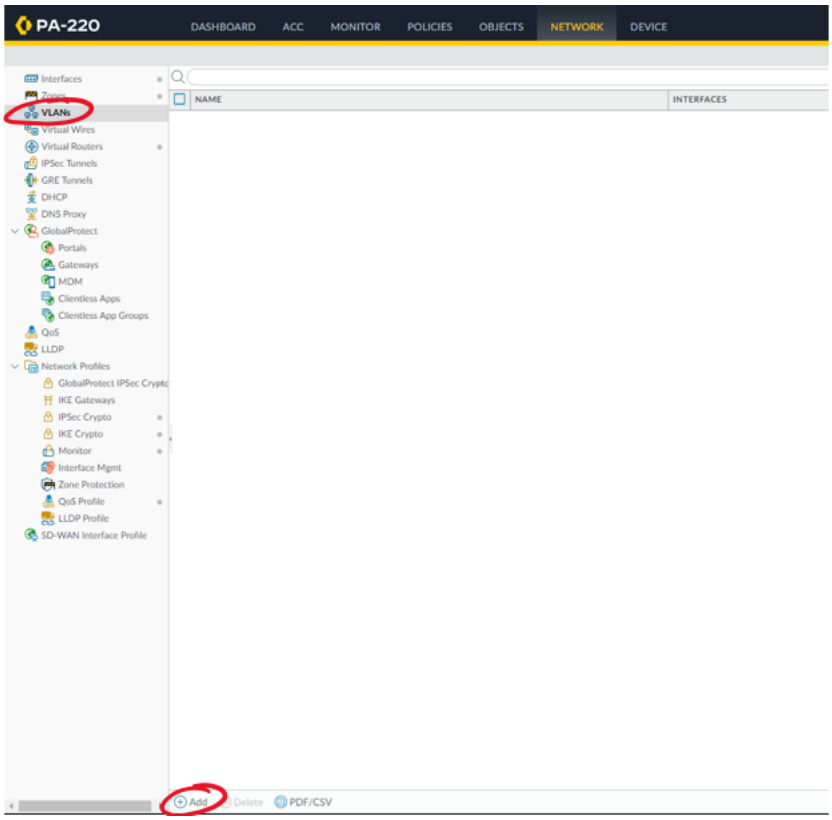
Select the interface ethernet1/1, set the virtual router to “default” and the security zone to “Untrust-L3.”



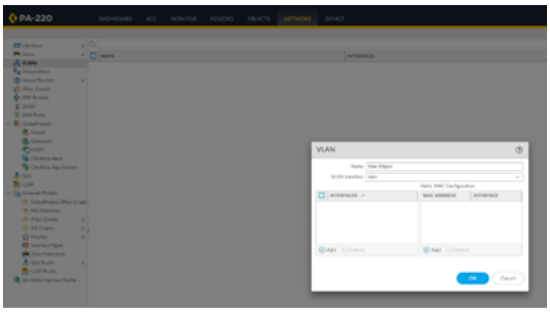
Click the “IPv4” option in the Ethernet Interface and click on “DHCP Client” as the type. Make sure that both “Enable” and the default route are on.



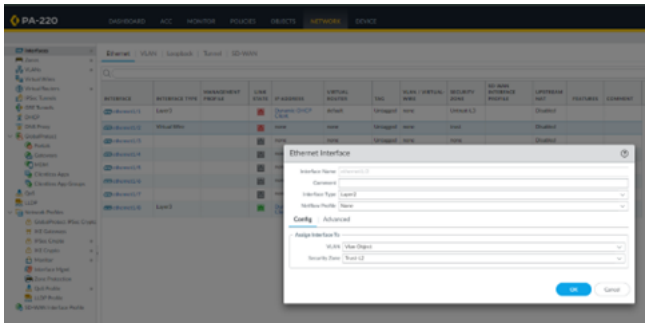
Once done with the first interface, go to the “VLANs” section under Network and add a new VLAN.



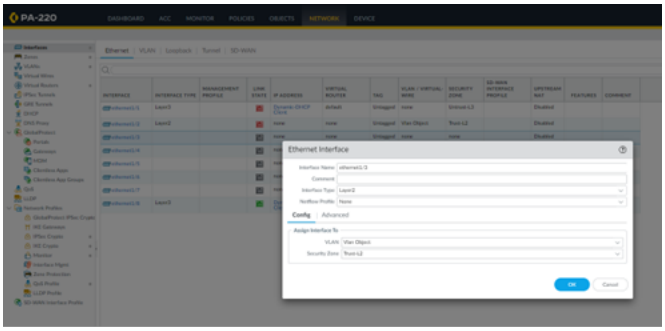
Name your VLAN object and select “vlan” for VLAN interface.

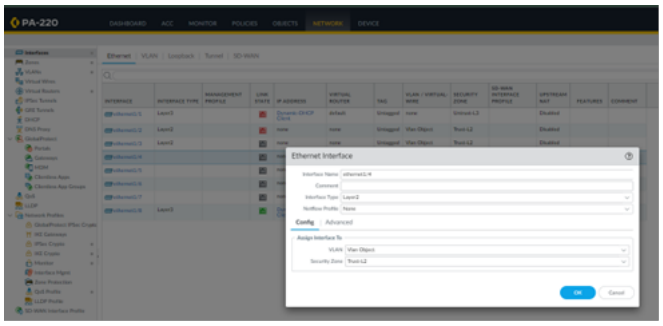


Go back to “Interfaces” and “Ethernet” and enter the interface “ethernet1/2”. Set the interface type to Layer 2, the netflow profile to none, VLAN to the name of your previously made vlan, and security zone to “Trust-L2”.

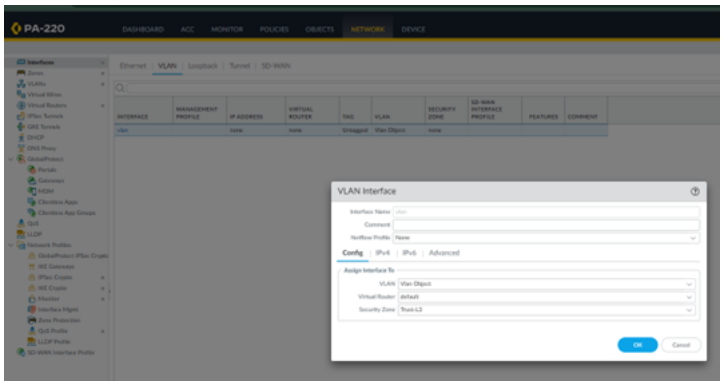


Repeat the steps above for “ethernet1/3” and “ethernet1/4”

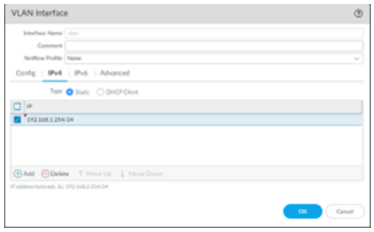




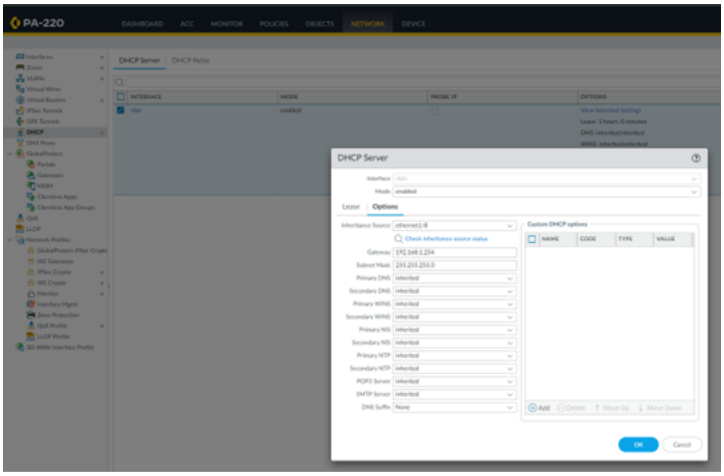
In the Network and Interfaces tab, click the subsection VLAN that's next to the Ethernet button. Set VLAN to the name of your VLAN object, Virtual Router to default, and security zone to "Trust-L3".



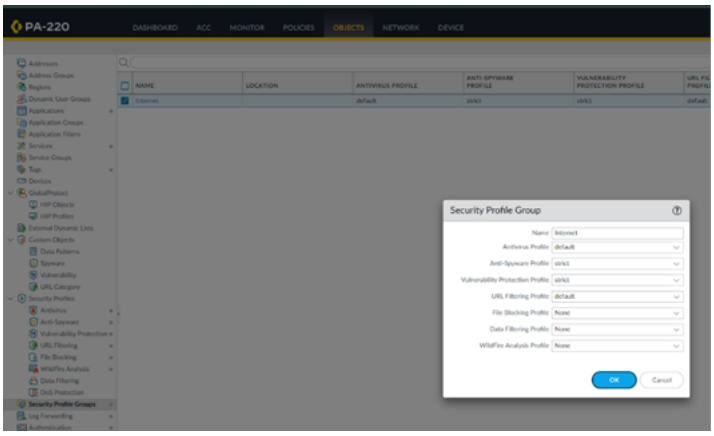
Under the same VLAN Interface, click on the IPv4 section and add an IP address of 192.168.1.254/24.



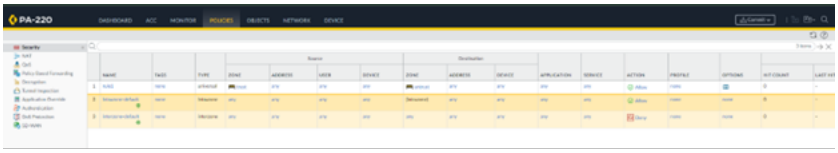
Staying under "Network", navigate to the DHCP and DHCP server section of the GUI. Add a DHCP server and set interface to "vlan" and mode to "enabled". IP Pool should be 192.168.1.2-252, with gateway 192.168.1.254 and subnet 255.255.255.0. The rest of the settings should be automatically inherited or set to "none".



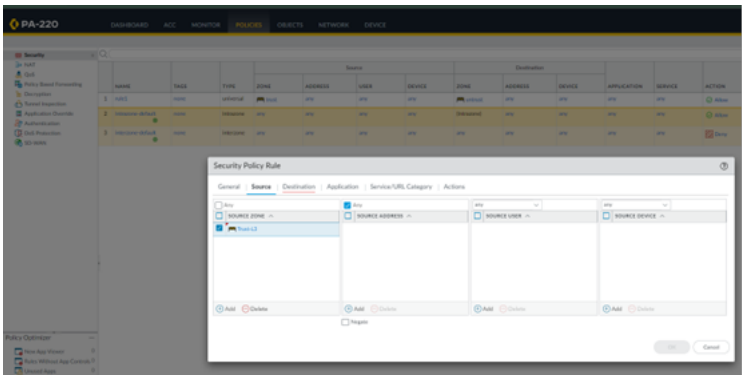
Go to the “Objects” section on the top taskbar and then “Security Profile Groups”. Add a new group and configure the settings as below.



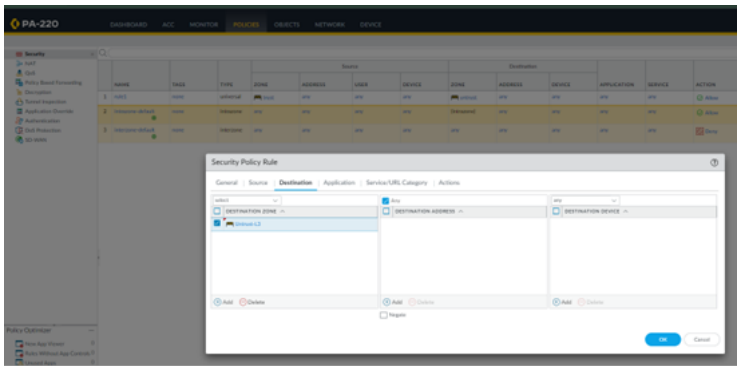
Navigate to the “Policies” section on the top of the dashboard and then to Security on the left taskbar.



Add a new security policy rule and name it “Internet Outgoing” with description “All traffic to the internet”. Under the Source section, add the source zone to be “Trust-L3”.

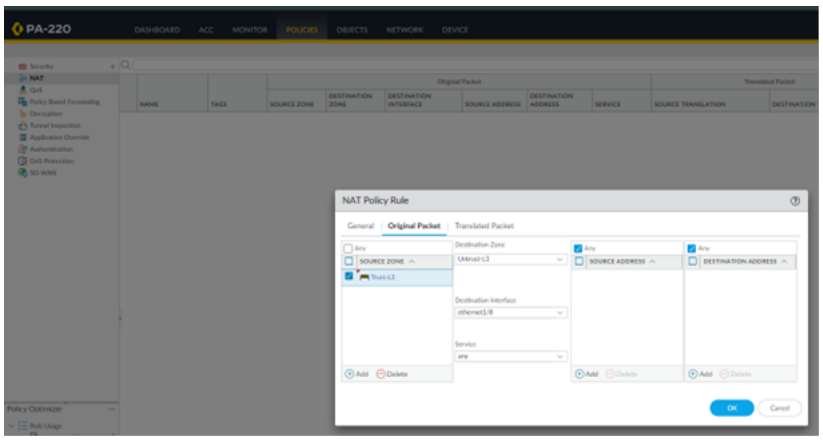


Navigate to the Destination zone and add the zone “Untrust-L3”.

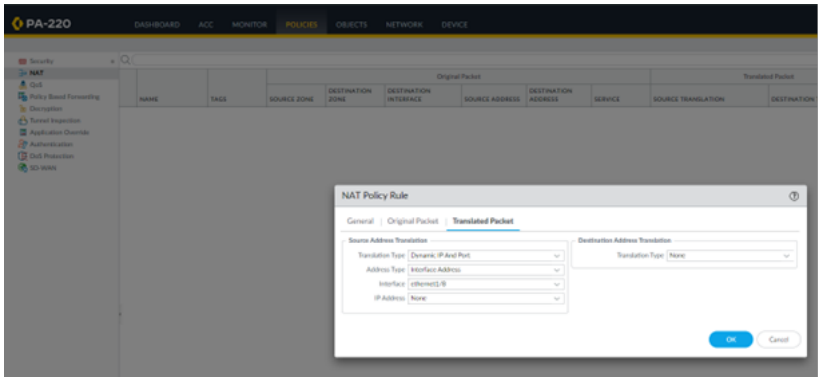


Navigate to “Actions” and make sure to click “Allow” as well as “Log at Session End”. Profile Setting should be Group and Internet.

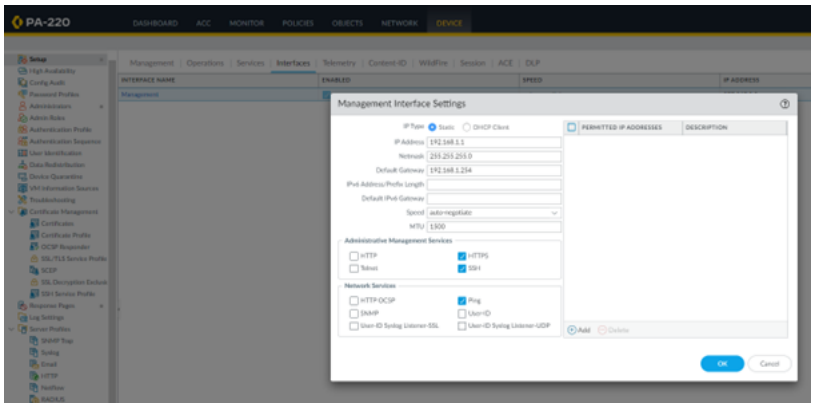
Return to “Policies” homepage and choose “NAT” on the left taskbar. Add a new policy and enter a name and IPv4. Choose “Original Packet” and specify the Source Zone as “Trust-L3”, the Destination Zone as “Untrust-L3”, and the Destination Interface as “ethernet1/1”.



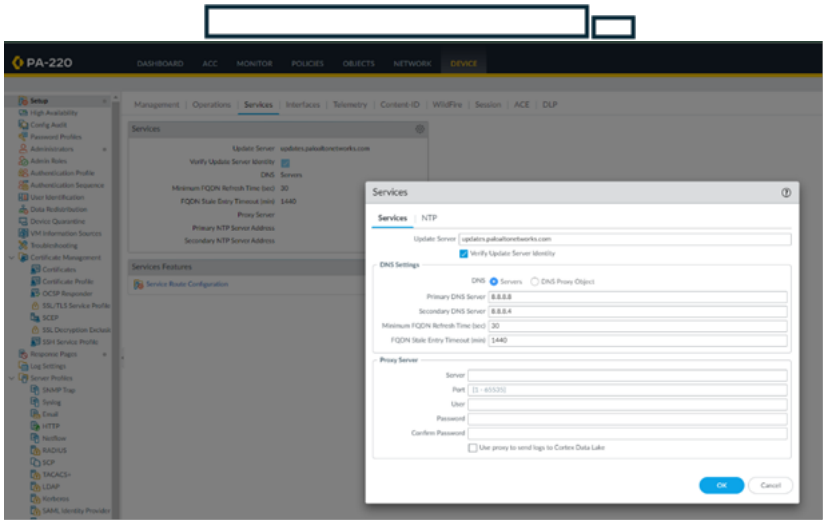
In the “Translated Packet” section, set the Translation Type to Dynamic IP And Port. Make sure Address Type is Interface Address and your interface is the DHCP configured interface.



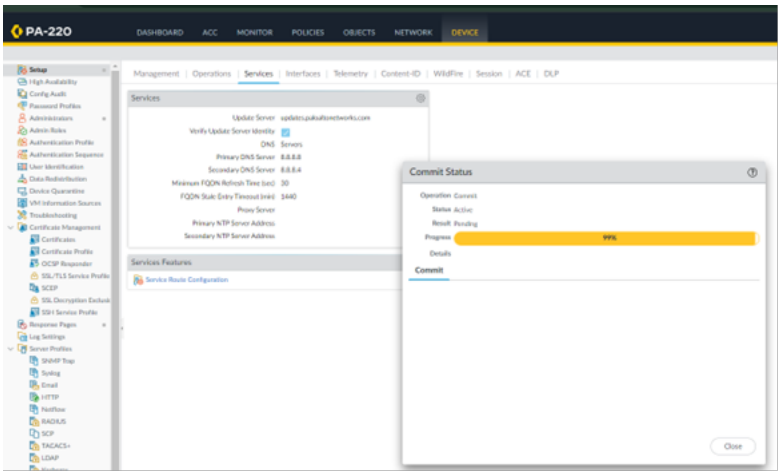
Go to Device, Setup, Interfaces and then Management Interface. Set IP Address to 192.168.1.1, Netmask to 255.255.255.0, and Default Gateway to 192.168.1.254.



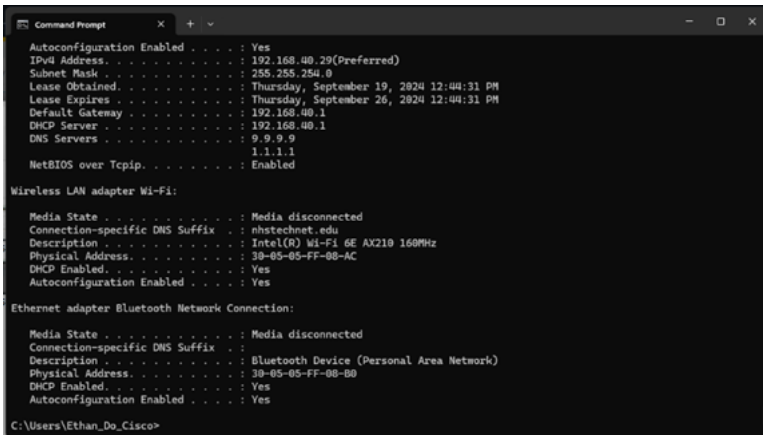
Return to Device, Setup and then click on Services. Enter the DNS server's IPs, 8.8.8.8 and 8.8.4.4 in the case of Google.



Go to Device and commit your changes to the firewall.



Ensure that DHCP works by opening the command prompt on your host computer and typing the command ipconfig /all. Check whether or not the DHCP server supplied a usable IP address and whether or not the default gateway and DHCP server IP addresses are correct.



Lab Commands:

The only new command used in this lab was the ipconfig /all command in command prompt. This command shows the network interface information on a host. For this lab specifically, what we're looking for using the ipconfig /all command is the IP address of the host, DHCP server, and DNS server in order to make sure that the network is functional.

Problems:

One of the problems that we had with this lab was the fact that the firewall failed to commit the changes that we were uploading. This meant that our

firewall was not functional and could not be tested. After experimenting with changes to try and commit for a while, our group figured out that the reason we couldn’t commit was the presence of a virtual wire in our configuration. Once we deleted the virtual wire, the commits started to go through on the configuration.

Another problem that we had was some of our interfaces on the firewall being down. This stopped us from using many of our interfaces. In order to fix this, our group swapped firewalls and reset the new firewall and configured that one.

Conclusion:

In conclusion, this lab was meant to configure a Palo Alto PA-220 firewall to work in a Small Office Home Office (SOHO) network. To do this, we had to make use of the Graphical User Interface (GUI). On the GUI we followed a basic Palo Alto configuration tutorial and set up interfaces, VLANs, security zones, DHCP, and other basic services. The biggest problem we had was getting our firewall to commit changes since we didn’t know that having a virtual wire would interfere with committing.

Palo Alto PA-220 URL Filtering Lab

Andrew Pai

Purpose:

The purpose of this lab was to set up URL filtering on our Palo Alto PA-220 firewall. After having reset and configured the PA-220 for a SOHO network, this next step ensures that our firewall can filter and block various web traffics based on the URL. This will help protect our network and clients from malicious or harmful web threats, even if they're unknown.

Background Information:

This lab focuses on implementing URL filtering for our SOHO network that we set up in our last lab. URL filtering is essentially a method of web protection that can help network administrators prevent their network hosts from performing malicious activity or exposing the network to malware, either purposefully or accidentally. When done correctly, URL filtering can be as specialized as allowing network hosts onto certain websites but preventing actions that may lead to a breach of network security, such as downloading files or entering personal and corporate information into websites. However, the goal for this lab is much broader than that and will focus on preventing users from accessing specific categories of websites.

The form of URL filtering that this lab will focus on is restricting access to certain content groups and websites on the Internet based on the URL. This will be done through utilizing various preset categories that Palo Alto has set up, such as groups like "abused-drugs," "adult," "malware," "nudity," and "weapons." By creating a URL filtering profile on the Palo Alto PA-220, network administrators will be able to stop all URL traffic from websites that fall under the categories they choose. This is useful in helping prevent network hosts from accessing sites that may contain any malware or simply preventing them from accessing sites detrimental to their work or education, a tool crucial to small school labs like ours. However, by setting up an override, network administrators will still be able to access these sites themselves if they ever need to.

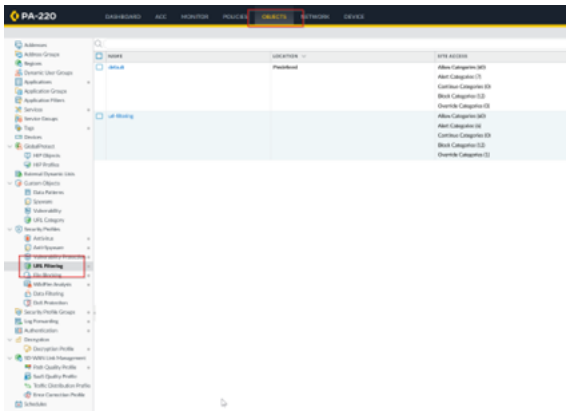
In order to set up URL filtering through the Palo Alto PA-220 GUI, we should first understand how URL filtering works. As mentioned before, Palo Alto has predefined URL filtering categories, which plays into how the PA-220 filters URLs. The first step of URL filtering is for the PA-220 to inspect web traffic from when users try to access websites. The firewall will take the URL or the domain name, and using that, it'll look through the Palo Alto database of URLs, using the categorizations there to determine whether or not to filter the traffic.

However, for HTTPS sites that have encryption and don't allow the firewall to look at the URL or domain name, the PA-220 will use SSL decryption to gain access to the website information. It does this by using Man in the Middle Decryption, where it establishes a connection with the client to intercept SSL handshakes, decrypting the data to inspect it, and re-encrypting the data when it sends it back out. This then allows the firewall to do the same thing it does with HTTP sites, comparing the URL to the Palo Alto database of categories and carrying out proper filtering. One important thing to note about setting up HTTPS filtering is that the SSL decryption requires a certificate for the firewall to be able to establish a connection with clients from the web.

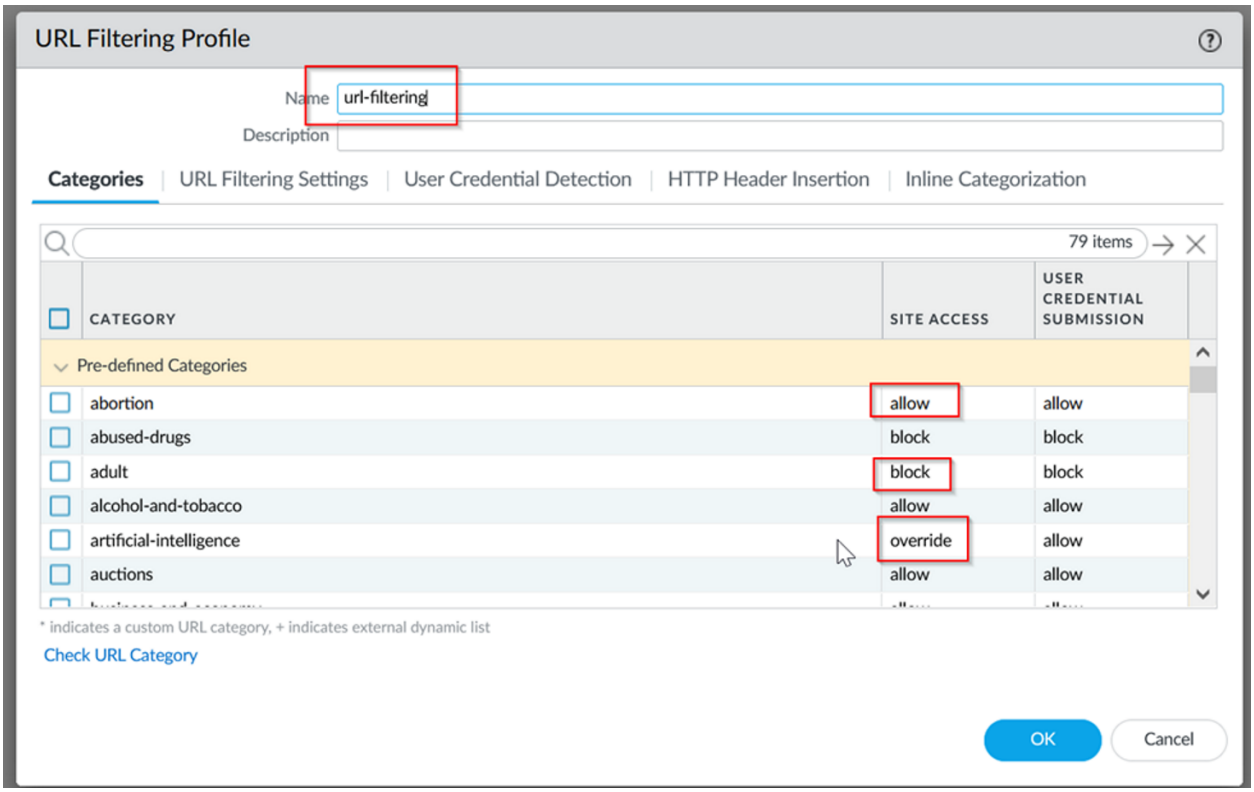
Overall, this lab is designed to give a comprehensive overview of how to set up both HTTP and HTTPS URL filtering on a Palo Alto PA-220. Not only does this lab familiarize the users with setting up URL filtering on the PA-220 GUI, it gives an understanding of what's actually happening to the traffic passed in and out of the firewall.

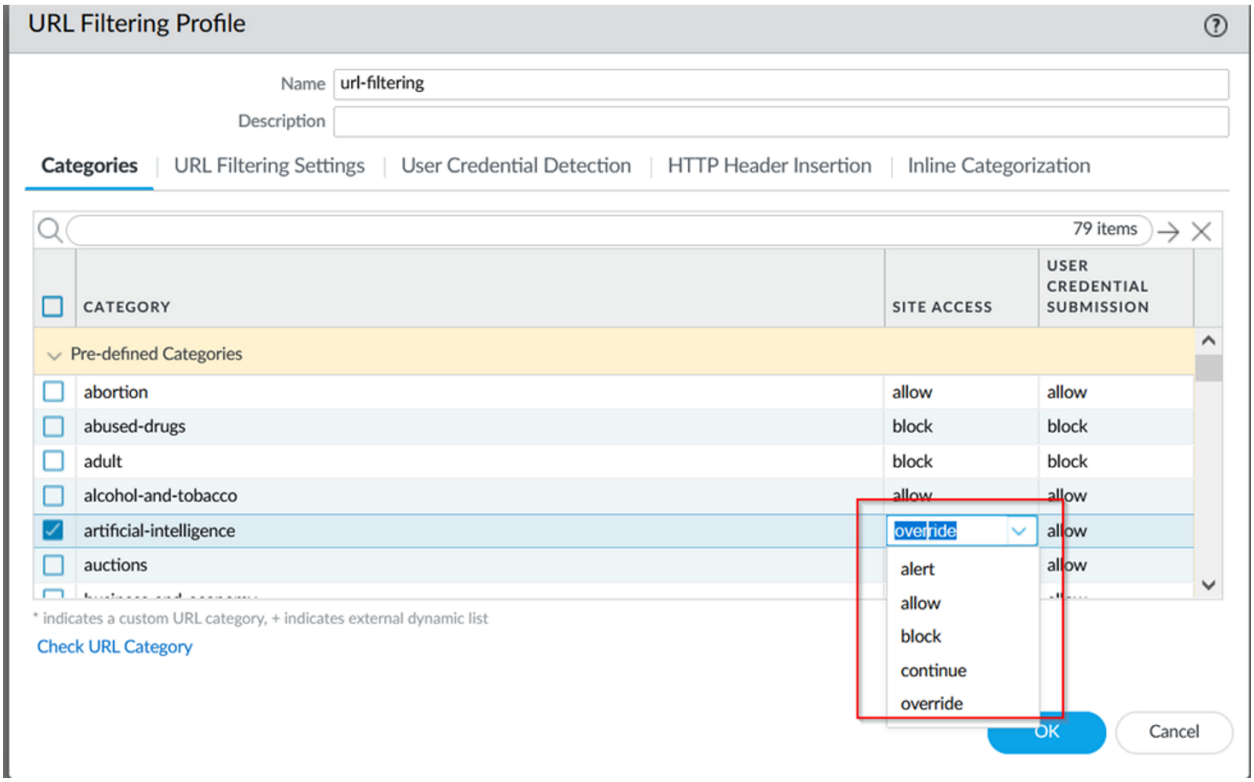
Lab Summary:

Navigate to "Objects" on the upper taskbar and then to "URL Filtering" under "Security Profiles" on the left taskbar. Once there, press "Add" on the bottom left to create a new URL Filtering profile.

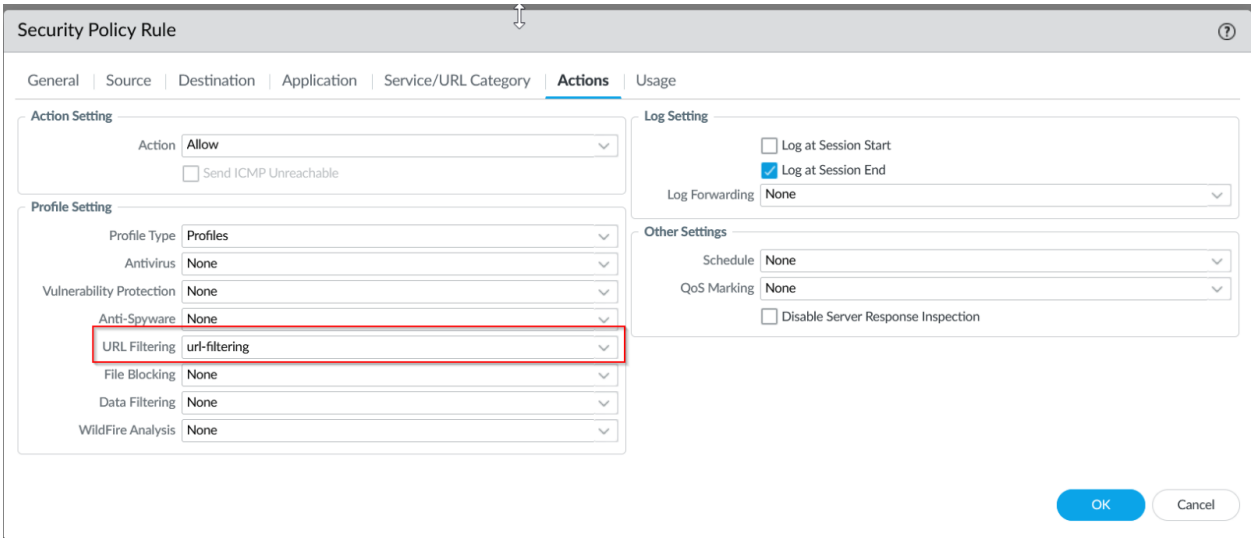


In the URL Filtering profile, create a name and change the access responses to Palo Alto filtering categories. To allow a website means traffic will go through, to block a website means traffic isn't allowed, and to override a category means that a password must be provided.

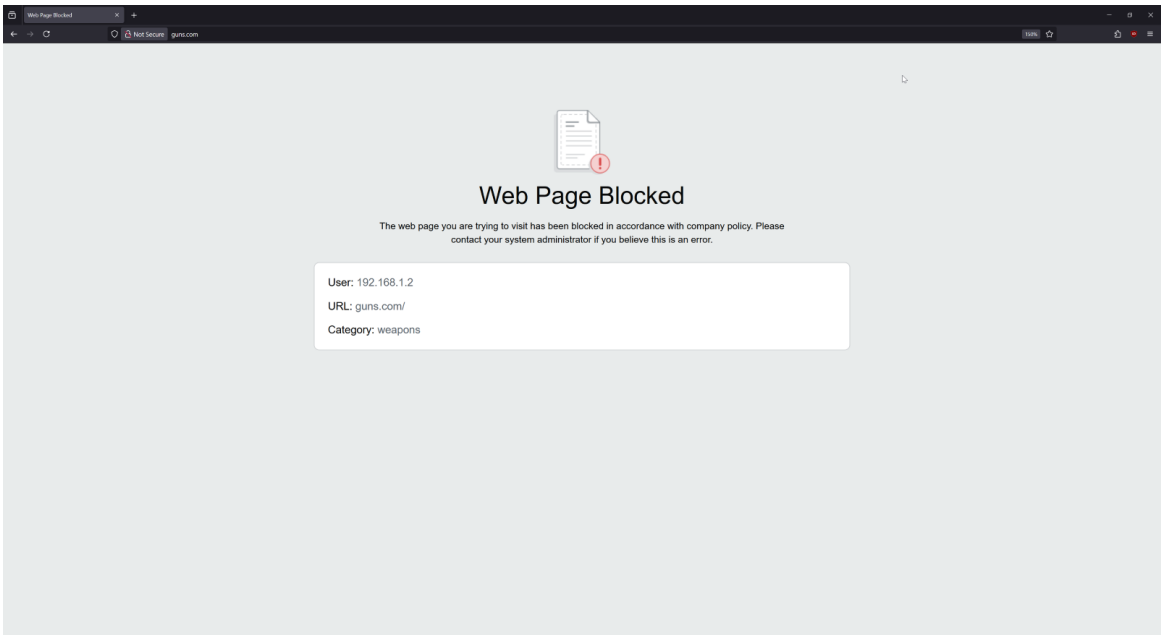

URL Filtering Profile
Name url-filtering
Description
Categories
URL Filtering Settings
User Credential Detection
HTTP Header Insertion
Inline Categorization
79 items
CATEGORY
SITE ACCESS
USER CREDENTIAL SUBMISSION
Pre-defined Categories
abortion allow allow
abused-drugs block block
adult block block
alcohol-and-tobacco allow allow
artificial-intelligence override allow
auctions allow allow
* indicates a custom URL category, + indicates external dynamic list
Check URL Category
OK
Cancel


URL Filtering Profile
Name url-filtering
Description
Categories
URL Filtering Settings
User Credential Detection
HTTP Header Insertion
Inline Categorization
79 items
CATEGORY
SITE ACCESS
USER CREDENTIAL SUBMISSION
Pre-defined Categories
abortion allow allow
abused-drugs block block
adult block block
alcohol-and-tobacco allow allow
artificial-intelligence override allow
auctions allow
alert
allow
block
continue
override
* indicates a custom URL category, + indicates external dynamic list
Check URL Category
OK
Cancel

Once you've created your URL filtering profile, navigate to "Policies" on the upper taskbar of the GUI and then to "Security" on the left taskbar. Select the outgoing security policy, navigate to "Actions" and then select your newly created URL filtering profile under the URL filtering section.



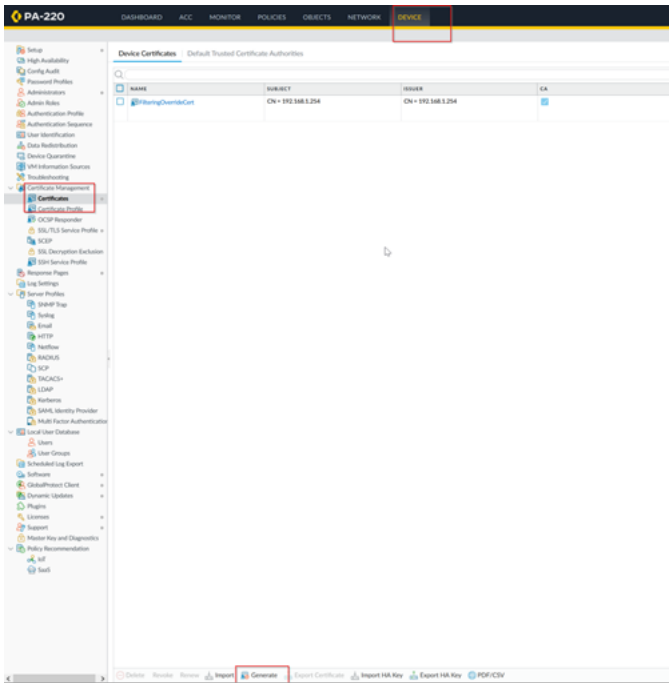
Press "Ok" to save this security policy and commit changes to the firewall. Once these changes to your URL filtering profile and security profile have been saved and committed, your firewall will now block the websites in the categories specified. This will only work for HTTP sites, but check with a website blocked by a category you specified.



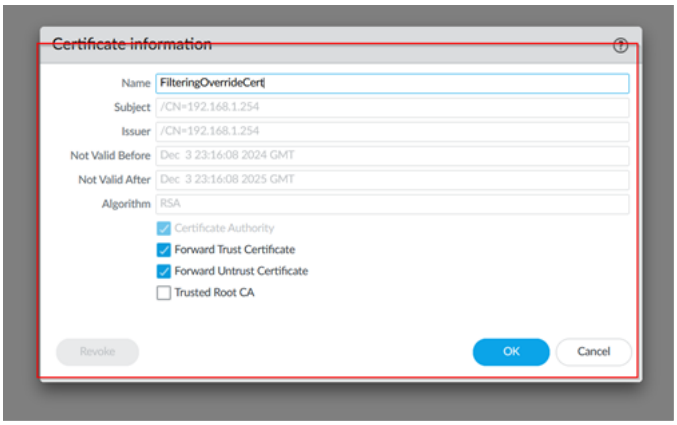
In order to set up HTTPS filtering instead of just HTTP, we should configure certificates as well. Console into the firewall and enter the below command to allow the PA-220 to inject URL filtering pages to an HTTPS session.

```
# set deviceconfig setting ssl-decrypt url-proxy yes
```

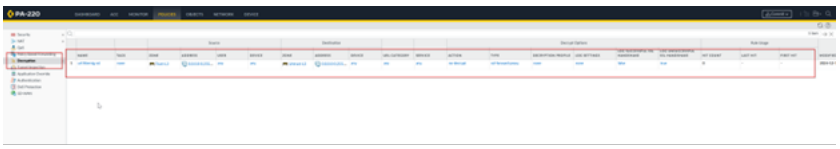
Once your command has been entered, navigate to “Device” on the upper taskbar and then “Certificates” on the left taskbar. Click “Generate” on the bottom to create a new certificate.



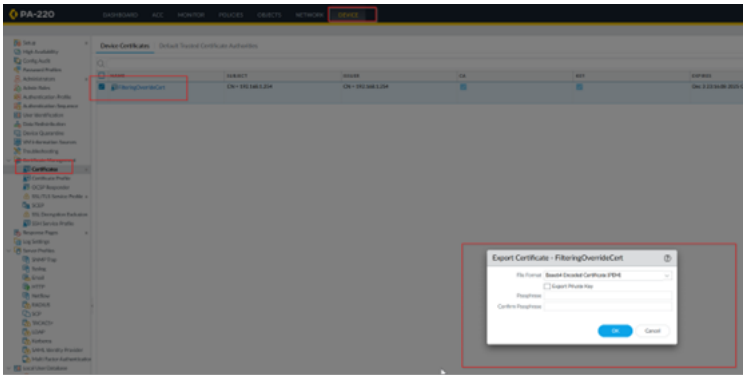
Create a name for your certificate and enter the following information in below. Make sure that Forward Trust and Untrust Certificates are checked off.



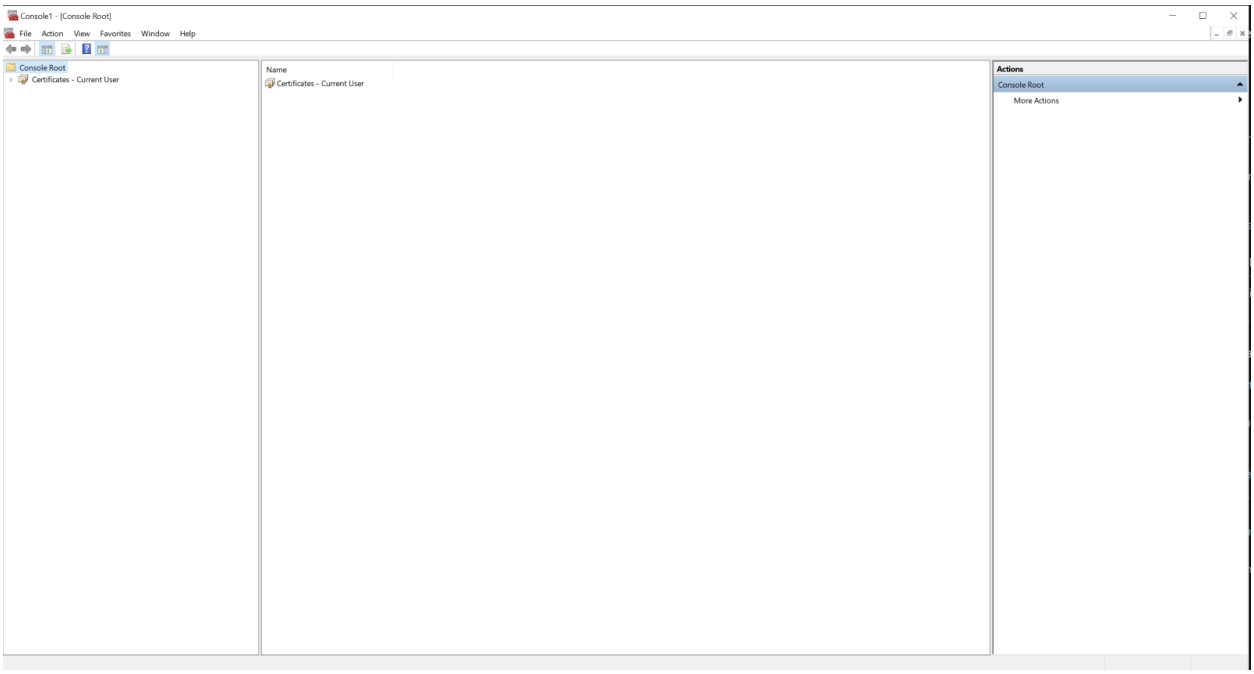
In “Policies” on the top taskbar and “Description” on the left, create a new policy for inbound and outbound traffic, with the type ssl-decrypt-proxy.



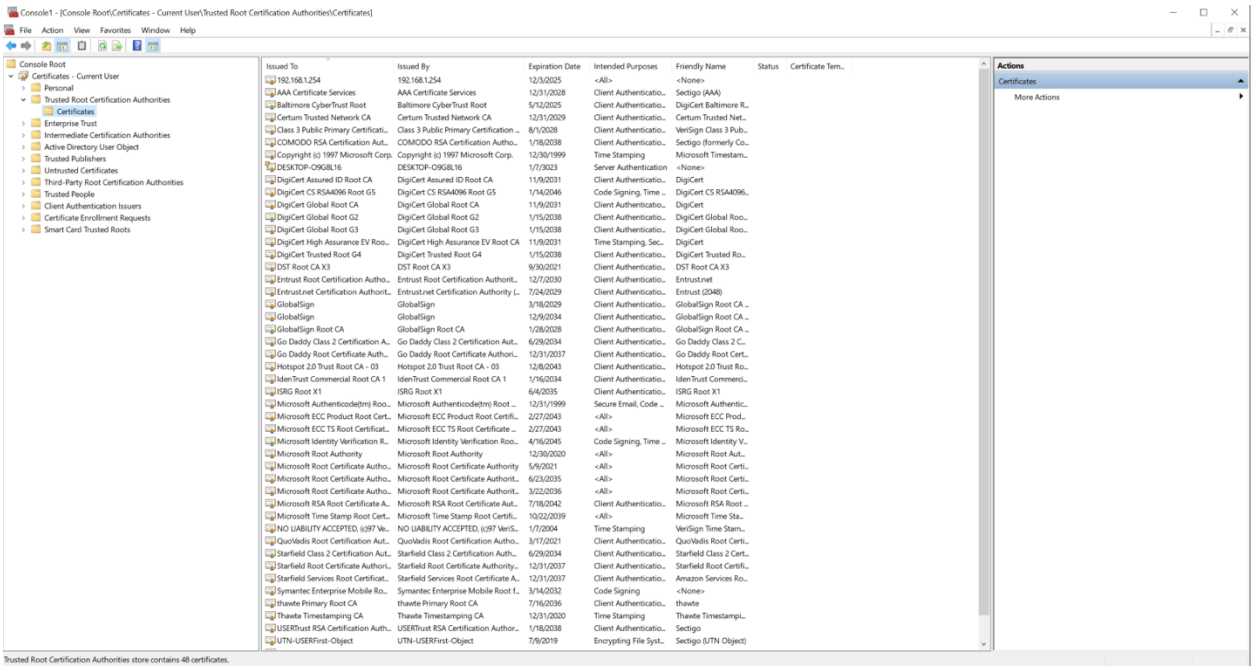
Navigate back to “Device” and “Certificates” to export the certificate to your computer.



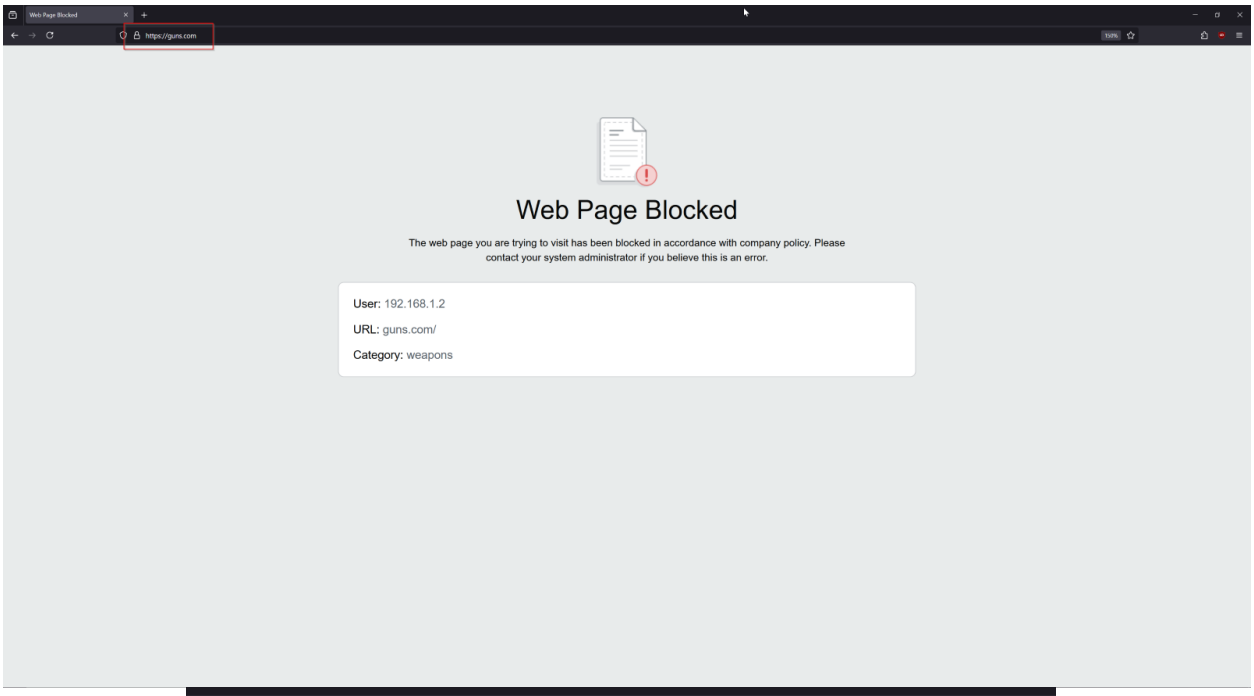
After downloading the root certificate, install it into your computer. For a Windows computer, you’ll need to press “Windows + r” to launch the Windows management console. From there, you can add the certificate to the menu.

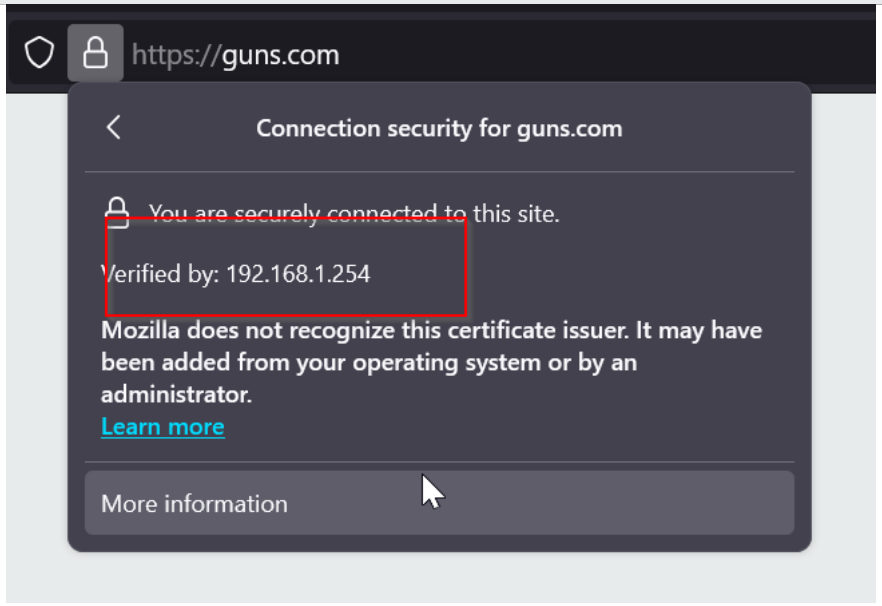


Navigate to “Certificates – Current User,” “Trusted Root Certification Authorities,” and then to “Certificates.” Right click to add a new certificate and add the certificate from where you downloaded it to.

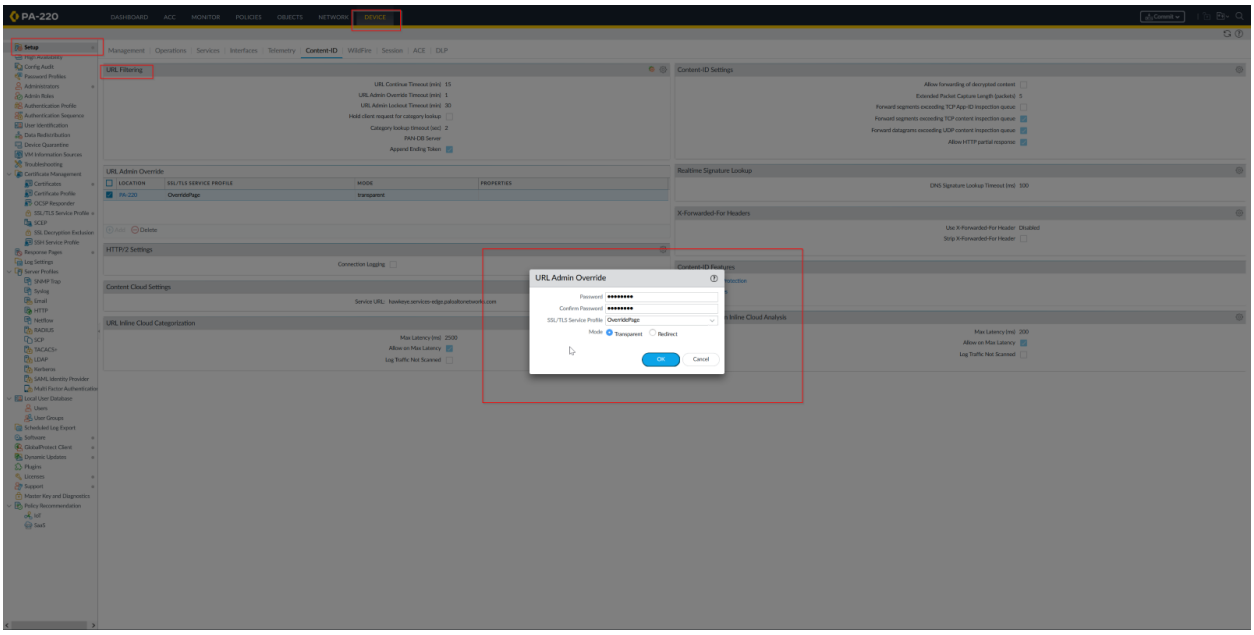


Now that the certificate is installed, your URL filtering should work for HTTPS websites as well.

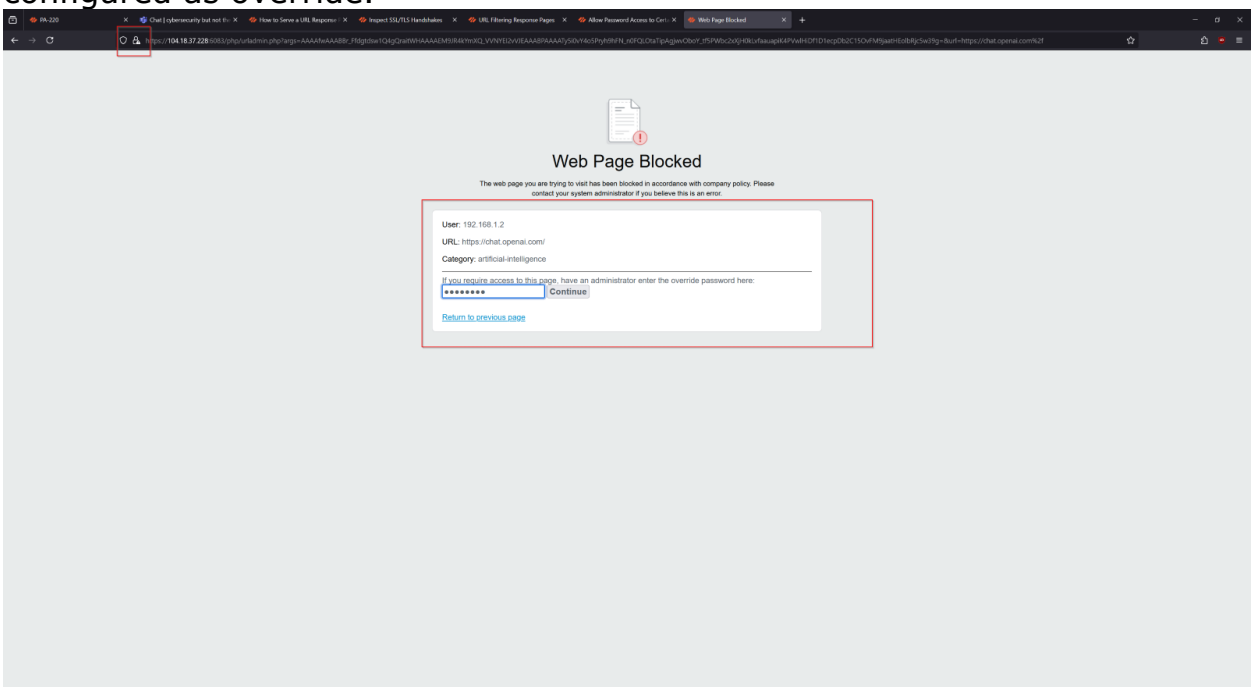


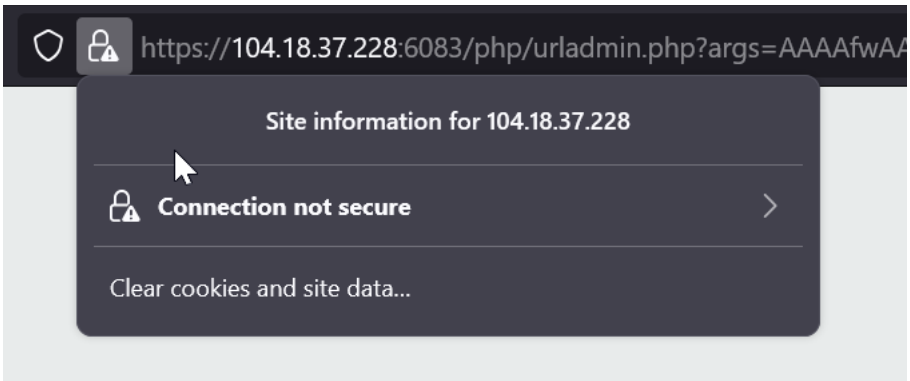


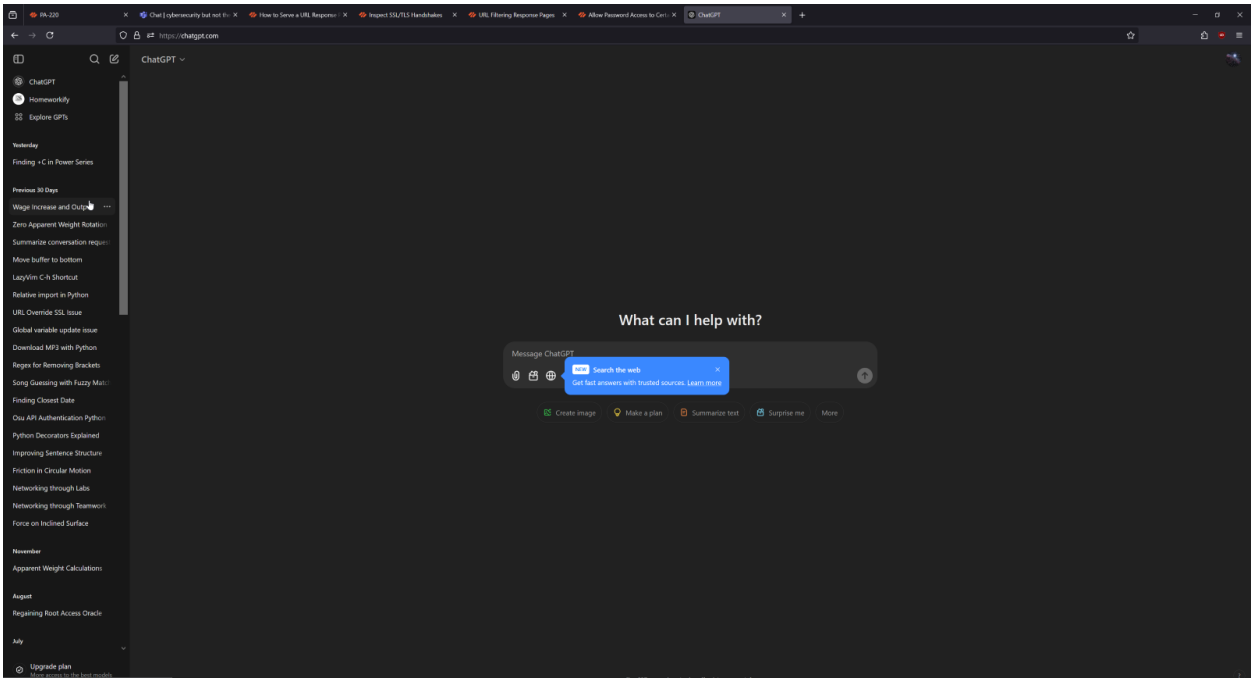
Since we have both HTTP and HTTPS URL filtering, we can add in the "override" settings for admins. In the Palo Alto PA-220 GUI, navigate to "Device" in the top taskbar, and then "Setup" and "URL Filtering." Add a new URL Admin Override profile.



Verify that override works by entering your admin password into a website configured as override.







If override succeeds, URL filtering is now set up properly on your Palo Alto PA-220.

Lab Commands:

The only new command used in this lab was one used to allow our PA-220 to insert the URL block page into HTTPS sessions as shown below.

```
# set deviceconfig setting ssl-decrypt url-proxy yes
```

This command essentially allows the firewall to decrypt SSL traffic so that it can check for security threats and to see if the traffic falls under one of the blocked filtering categories on the PA-220. Without this, our URL filtering

policy wouldn’t be able to work on HTTPS, meaning that a large range of websites would slip out from under our control.

Problems:

The biggest problem that our group had with this lab was with our HTTPS filtering and lack of a CA Certificate. Since HTTPS traffic is encrypted, our group couldn’t figure out how to use the PA-220 to stop and filter URLs the same way that we could with HTTP traffic. This caused us to be stuck on HTTPS filtering for quite a while before figuring out that we needed to actually decrypt the HTTPS traffic by using SSL decryption. SSL decryption allowed us to decrypt, analyze, and stop web traffic just like we did with HTTP, but we needed a CA Certificate in order to implement the connection between firewall and client. Therefore, before moving on with any HTTPS filtering, our group had to go through the process of getting a CA Certificate and installing it. After the certificate was installed and SSL decryption was allowed on our firewall though, HTTPS filtering worked perfectly and allowed us to move onto the override aspect of the lab.

Conclusion:

In conclusion, URL filtering is a critical way to maintain network security and ensure that all network hosts have a safe environment to work in. The URL filtering setup in this lab is applicable to various types of networks, from corporate to educational to personal. This lab was meant to setup URL filtering for both HTTP and HTTPS sites, blocking harmful categories but still allowing admins with an override password to access this traffic. To do this, we used the Palo Alto GUI and had to install a certificate for HTTPS traffic.

Palo Alto PA-220 Global Protect VPN Lab

Andrew Pai

Purpose:

The purpose of this lab was to configure the Global Protect VPN on our Palo Alto PA-220 firewall. This will allow desktops to remotely connect with other desktops that are on a different network.

Background Information:

This lab focuses on implementing the Global Protect VPN on our Palo Alto PA-220 firewall. VPNs, or Virtual Private Networks, are a way for Internet users to act as if they were connected to their own private network while accessing the Internet. This allows users to stay anonymous and keep their otherwise public data protected and private. Common uses of VPNs by the average person may include things like avoiding Internet censorship, protection of data, or accessing resources only available on networks in a different location. For corporations, VPNs can play a large role in allowing employees to access their business' network from a different area, letting them work remotely.

The main reason that people use VPNs is to protect their Internet traffic. Most of the time when people access the Internet, much or all of their data is public and unencrypted. Connections to the user's Internet Service Provider from their device leave much of their information vulnerable to either being logged by the ISP or being taken by malicious activity. As such, people use VPNs to avoid these data logs and attacks.

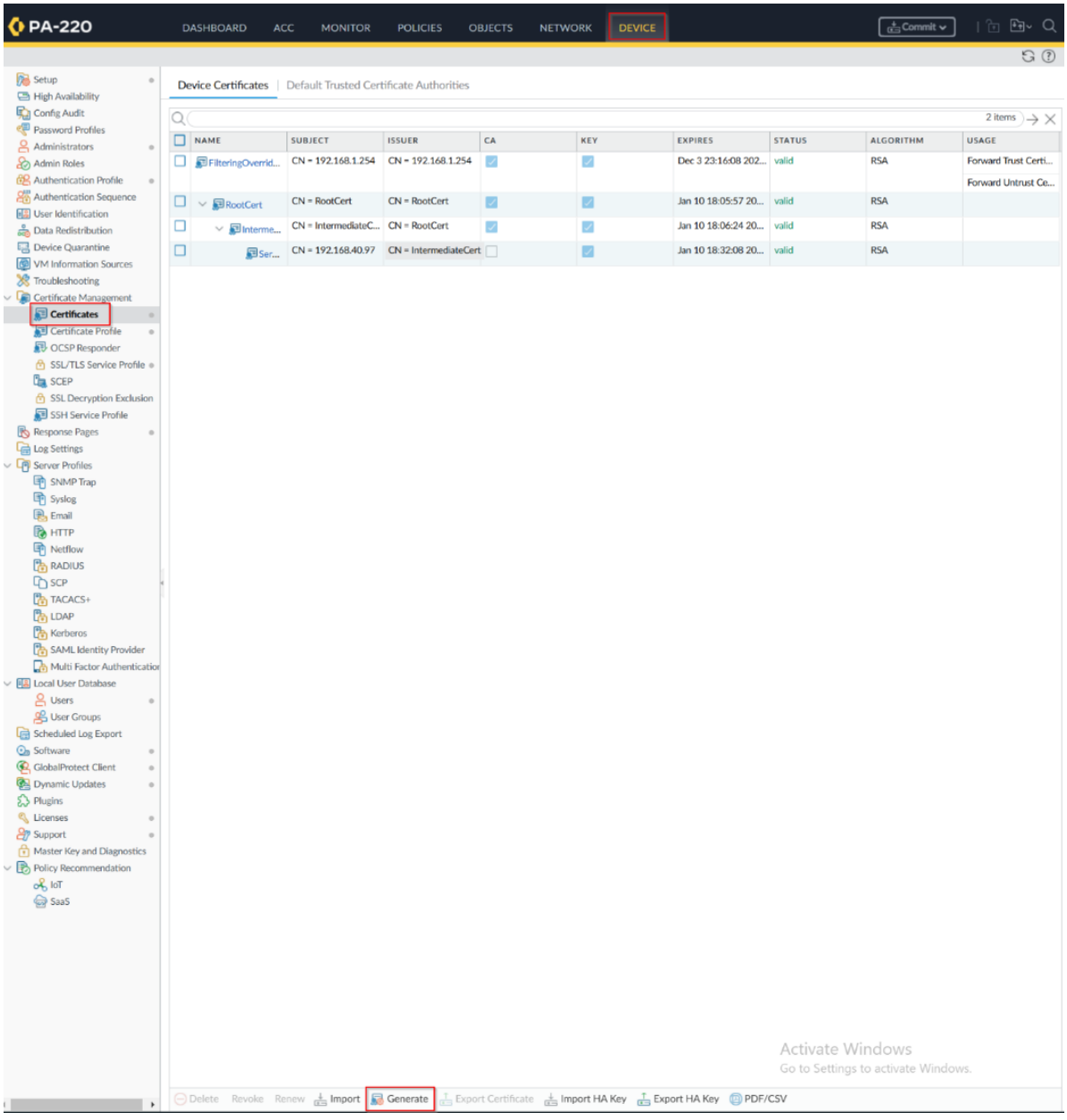
VPNs work through creating a tunnel between the user and the ISP so that user traffic isn't as unprotected as it was before. In creating this tunnel, there are three main components: the VPN client, VPN server, and the Internet itself. As compared to normal Internet usage, which would be the client and Internet, there's a VPN server inserted between the two that's in charge of decrypting and encrypting data so that it's protected. This happens by the VPN client connecting to the VPN server, which authenticates that the client actually has the credentials and authority to access the server. Once this tunnel is established between your VPN client and server, data passed between the client and server is encrypted and hidden from the ISP when it's sent out to the Internet.

The VPN that we're going to be using in this lab is the Global Protect VPN, which is Palo Alto's VPN. Global Protect is mainly unique compared to some other common VPN's because it can work in conjunction with the Palo Alto PA-220's firewall policies, allowing for users to reap the benefits of both a VPN and a firewall. However, it's also a flexible VPN to use for both mobile and desktop environments and can also check on the security and antivirus

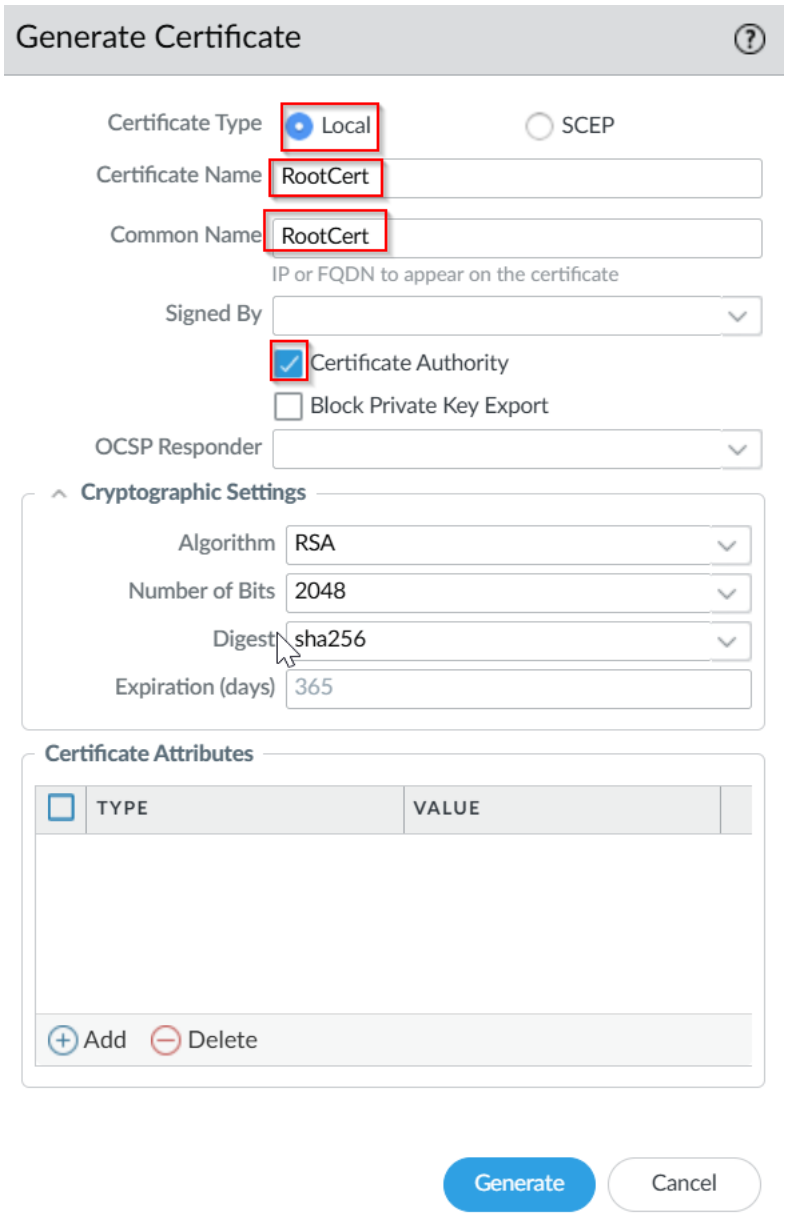
software that a device has before letting it enter the network. For this lab, we'll be using Global Protect to have one of our desktops connect to our network remotely to showcase a common situation where employees may have to work from home.

Lab Summary:

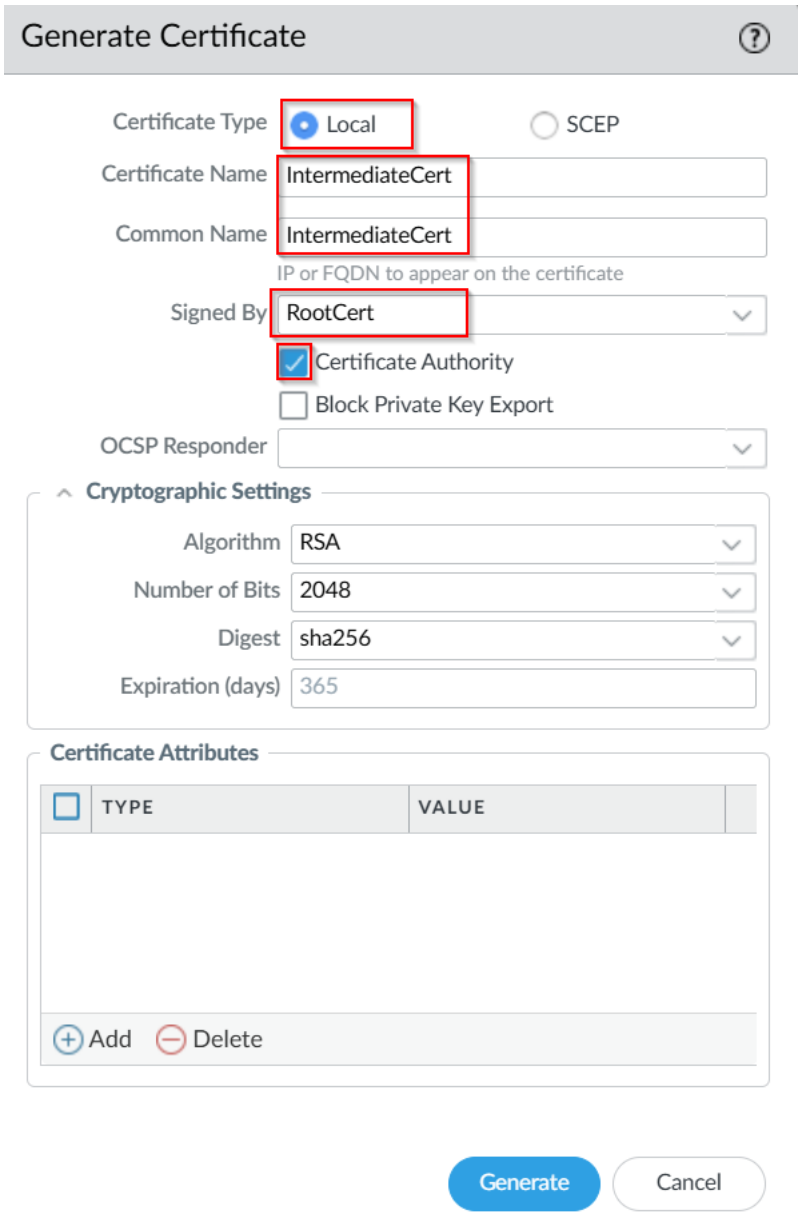
The first step of configuring Global Protect is to configure the PA-220 and end device certificates. In the firewall GUI, navigate to "Device" on the top taskbar and then "Certificate Management" and "Certificates" on the left. Click "Generate" on the very bottom of the screen.



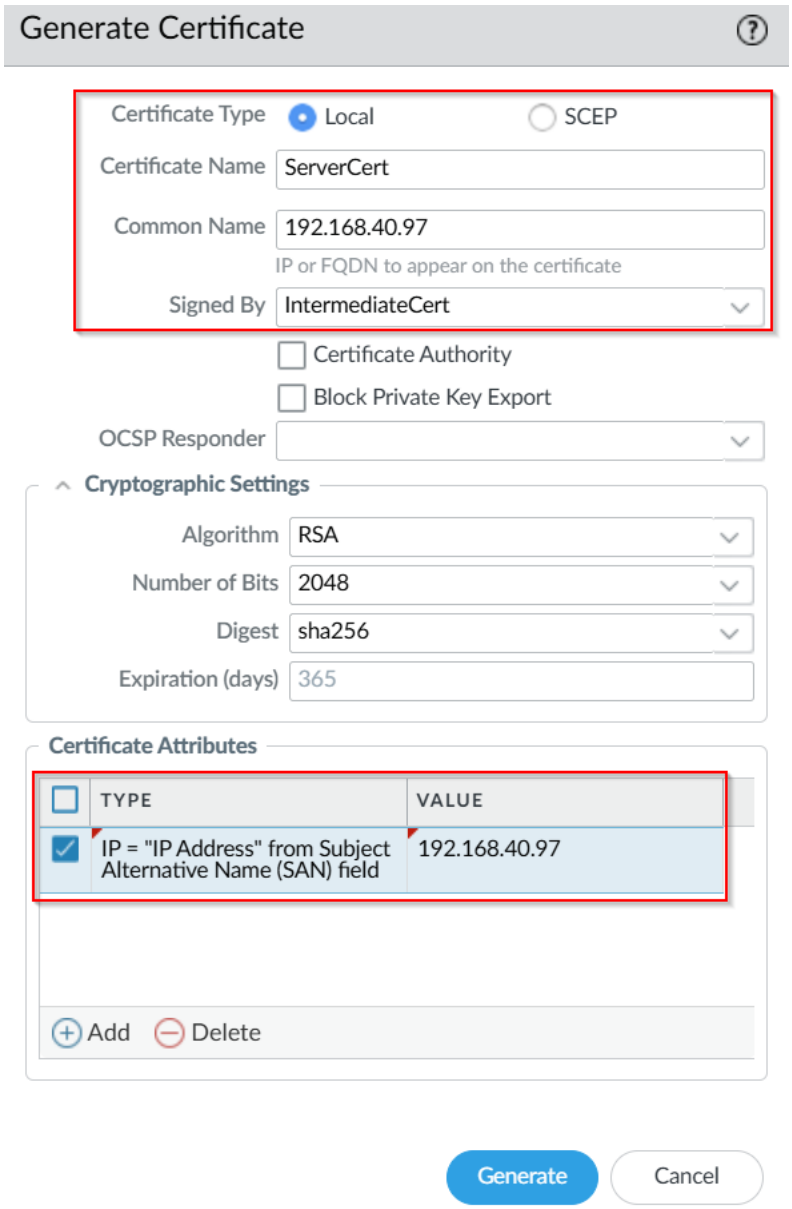
Configure a Local Certificate for your Root Certificate, naming it something like “RootCert.” Ensure that Certificate Authority is checked off. This certificate will not be signed off by any other.



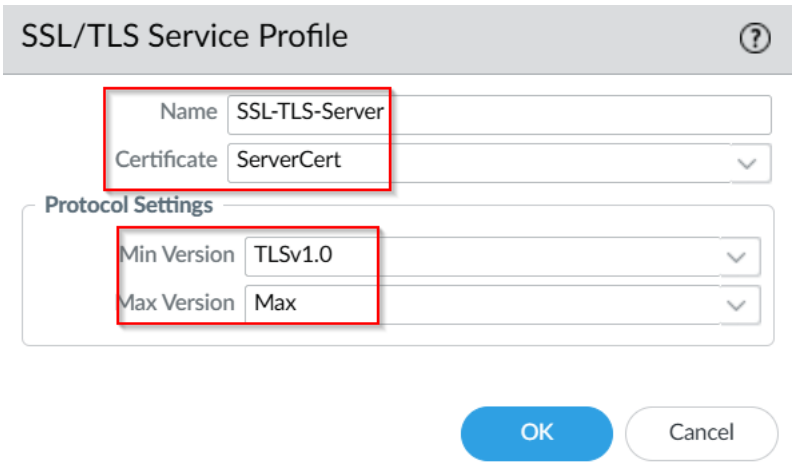
Generate a new certificate, this one called “IntermediateCert.” This certificate will be Local as well, but will be signed off by the “RootCert” certificate we just made.



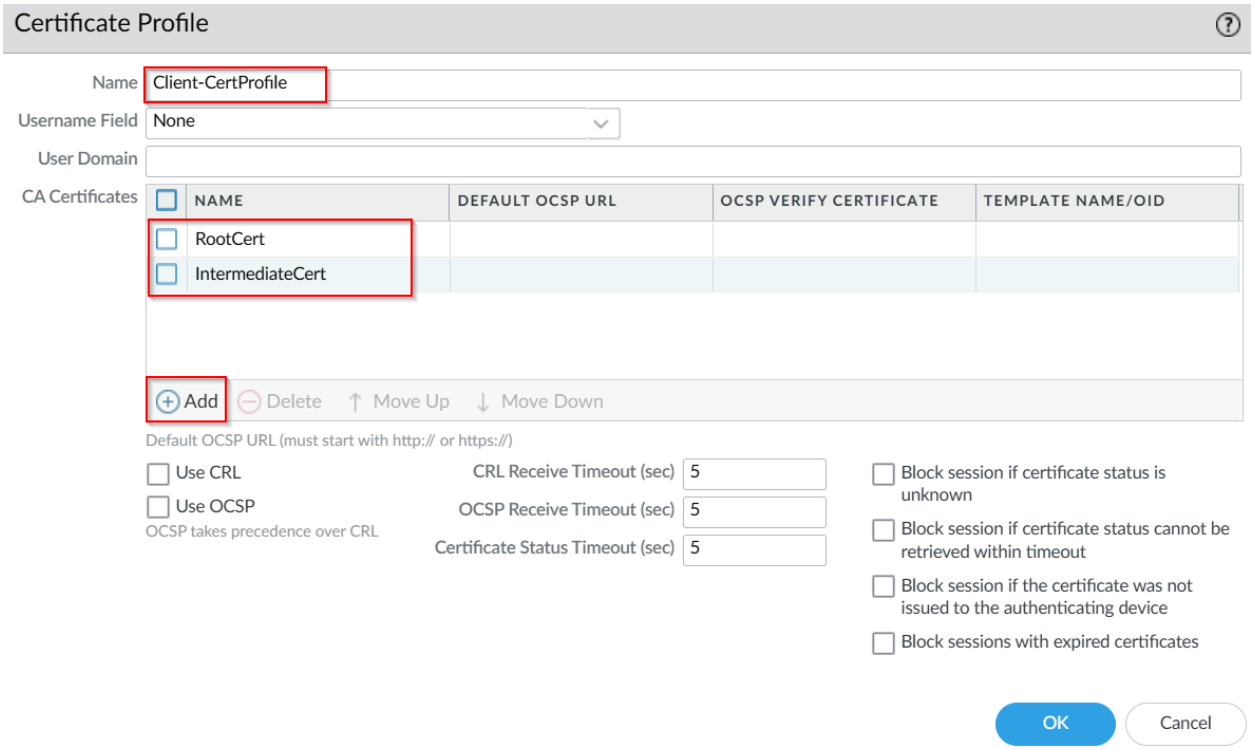
Finally, create another certificate named "ServerCert," which is signed off by the "IntermediateCert" just made. This certificate's Common Name should be the IP of your Global Protect Portal. Once generated, export all 3 certificates.



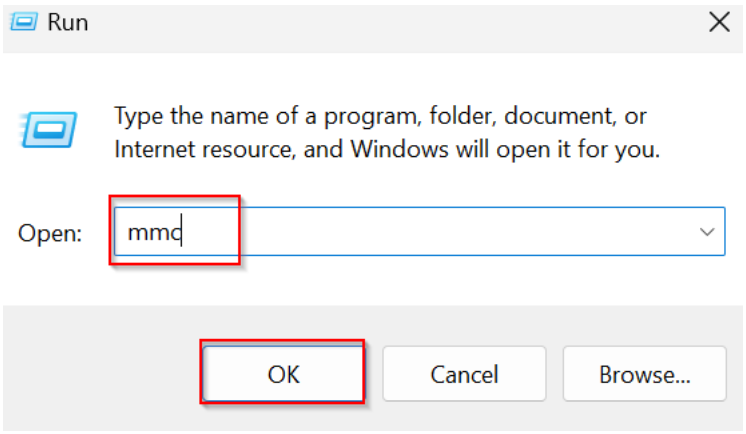
In the GUI, stay in "Device" on the top bar, but navigate to "SSL/TLS Device Profile" and click "Add." Name it "SSL-TLS-Server," and use ServerCert as the Certificate. Put Min Version as TLSv1.0, and Max Version as Max.



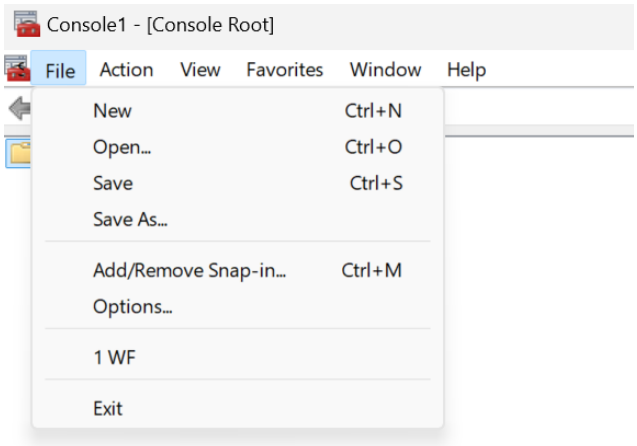
Navigate to "Certificate Management" and then "Certificate Profile" on the GUI's left taskbar and click "Add." Choose an appropriate profile name like "Client-CertProfile," and click "Add" and choose both RootCert and IntermediateCert to add.

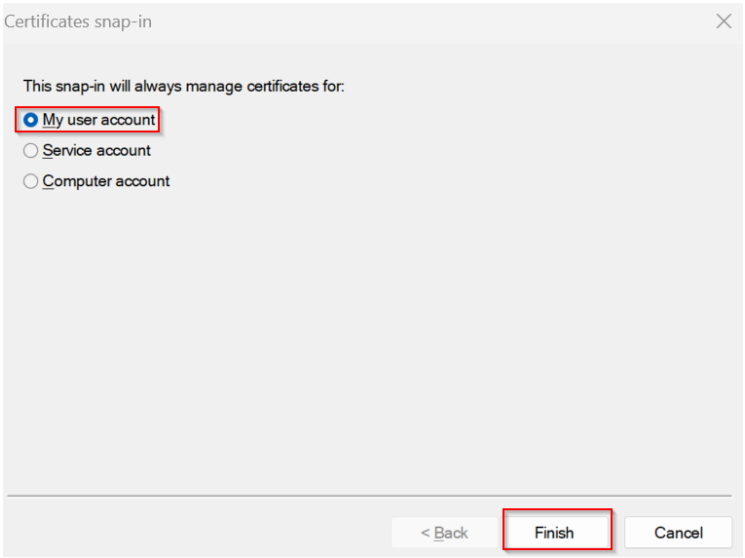


Now that we have the certificates, we'll add them to your device. Using the key commands WIN+R, type "mmc" into the Run Dialog window that pops up.

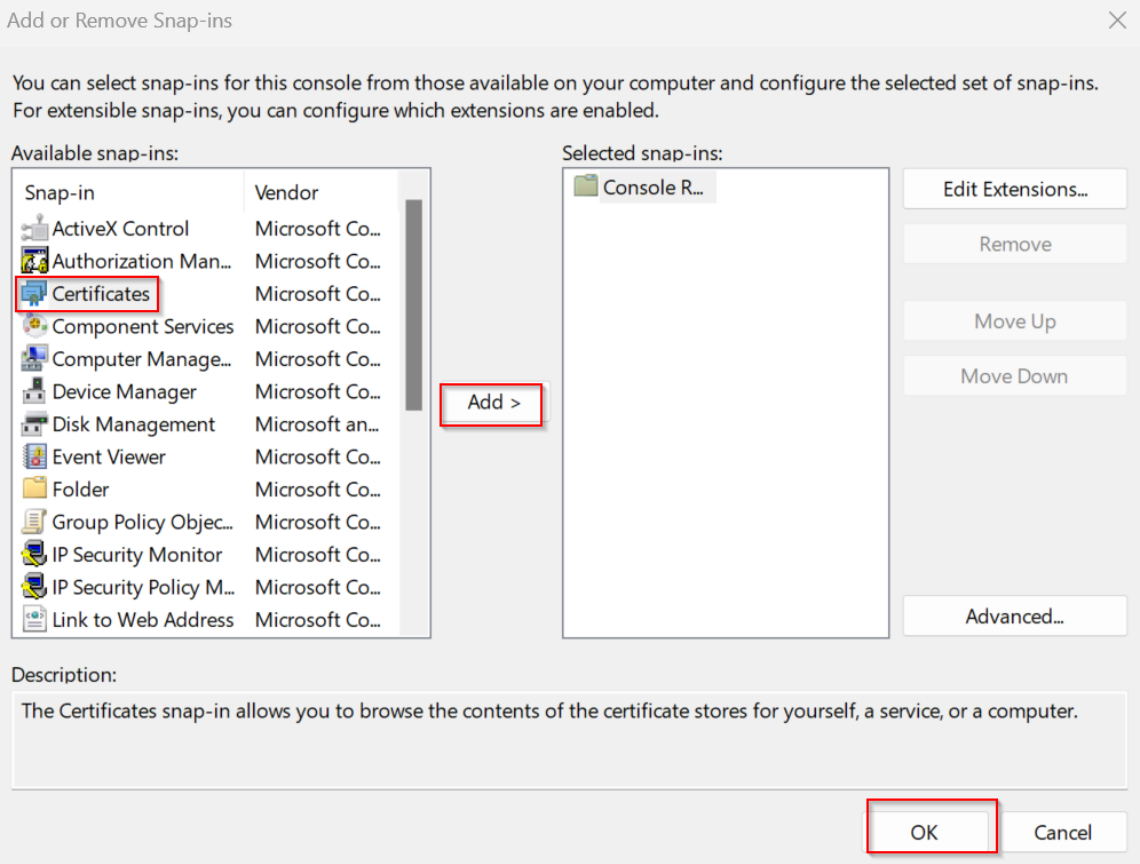


In the Console Root, click "File" on the top left and then "Add/Remove Snap-in." Choose "My user account" if prompted to choose between user, service, and computer account.

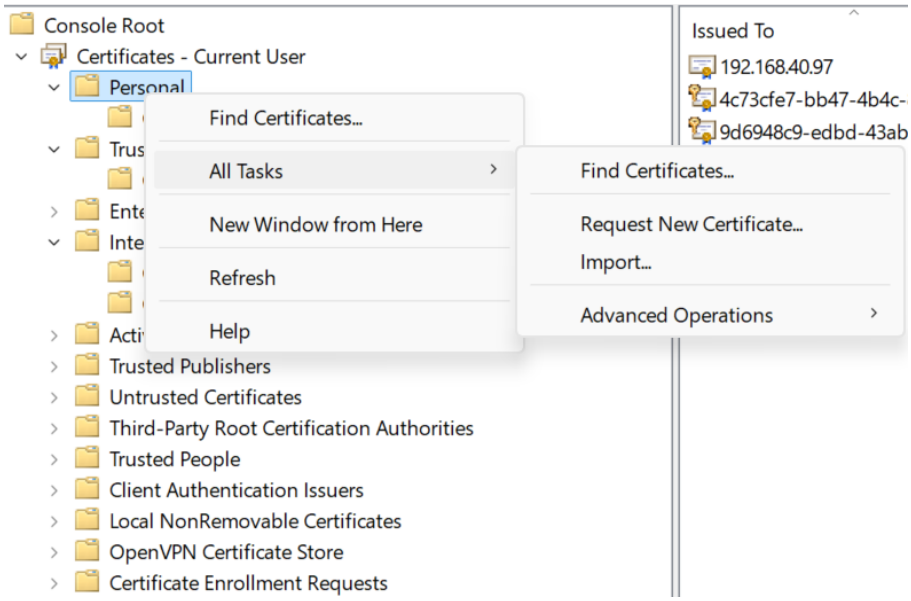




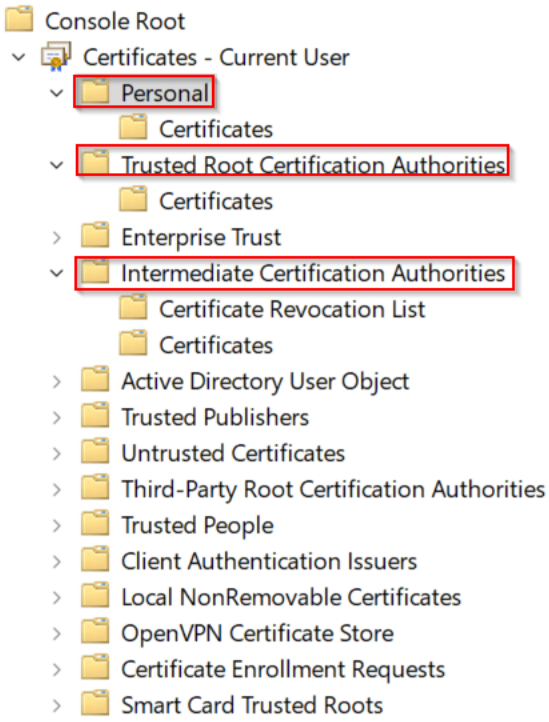
Select "Certificates," "Add," and then "Ok."



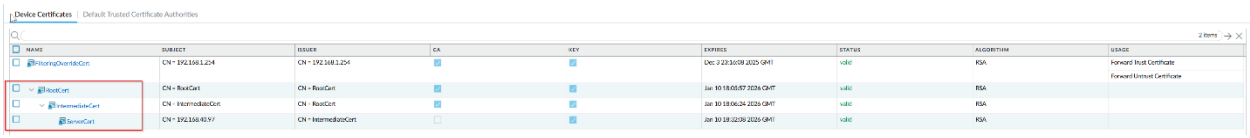
Navigate to "Console Root," "Certificates – Current User," and then "Personal." Right click this "Personal" folder and then click on "All Tasks" and "Import." Select the ServerCert to be imported to this folder.

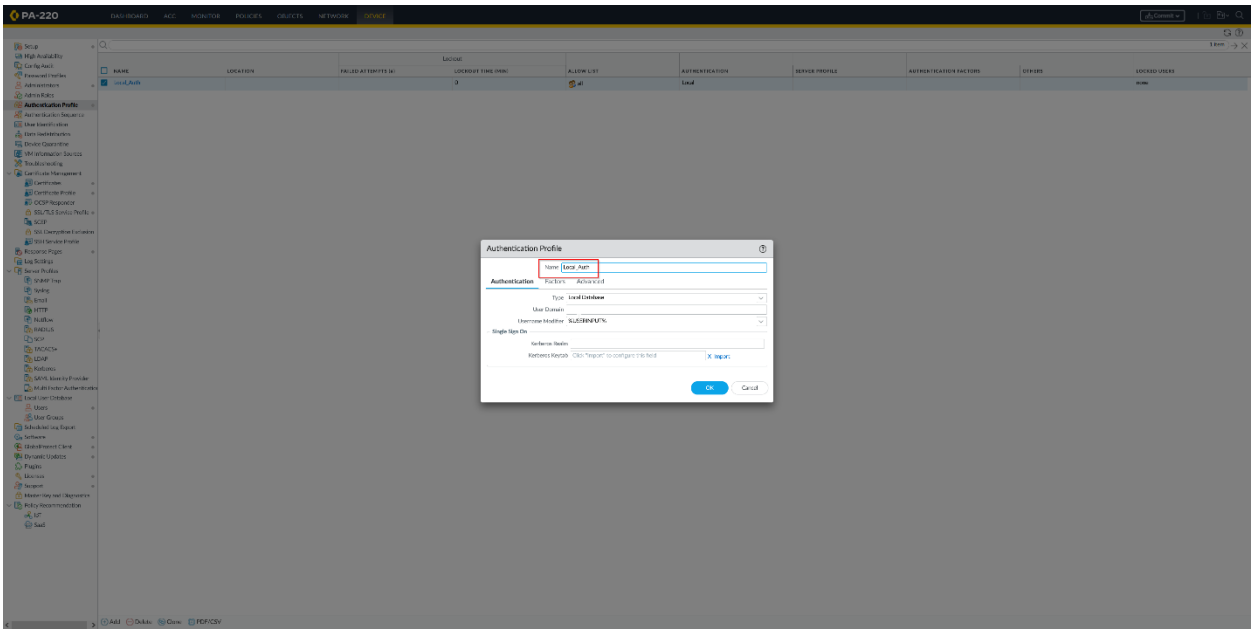


Follow the previous steps to import the Root Certificate into “Trusted Root Certification” and the Intermediate Certificate to “Trusted Intermediate Certification Authorities.”

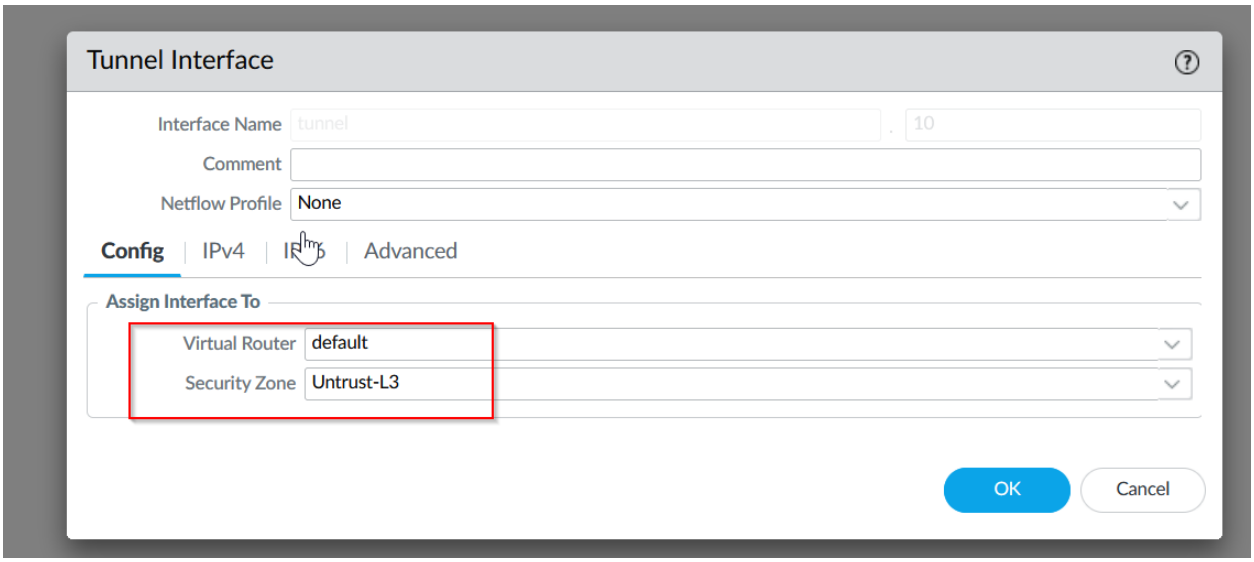


Return to the firewall GUI. Navigate back to “Device” on the top taskbar and then “Authentication Profile” on the left, and “Add.” Type should be Local Database, and you should name it something like “Local_Auth.”

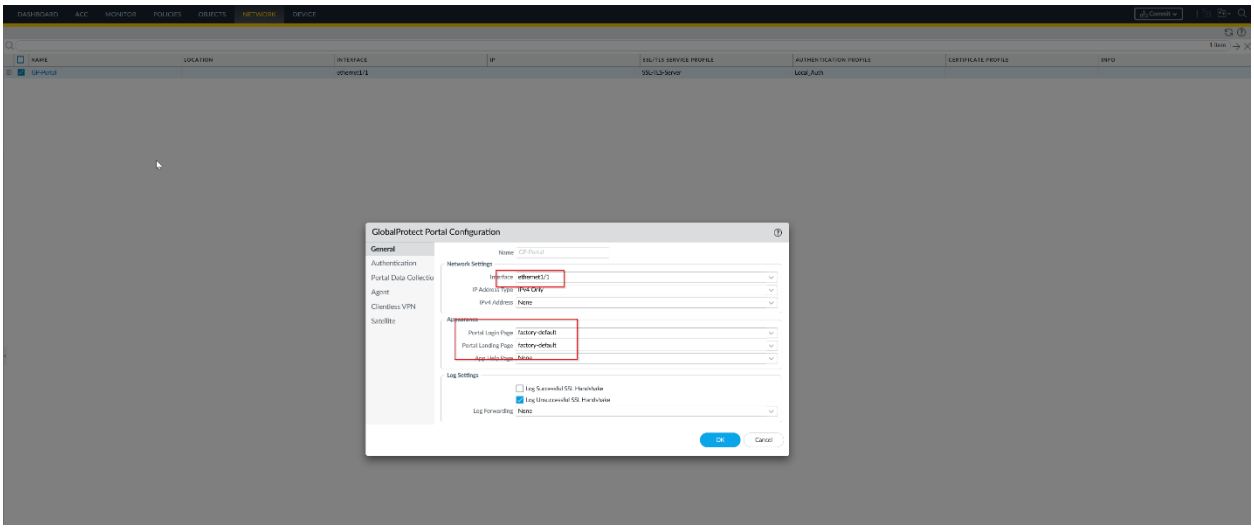


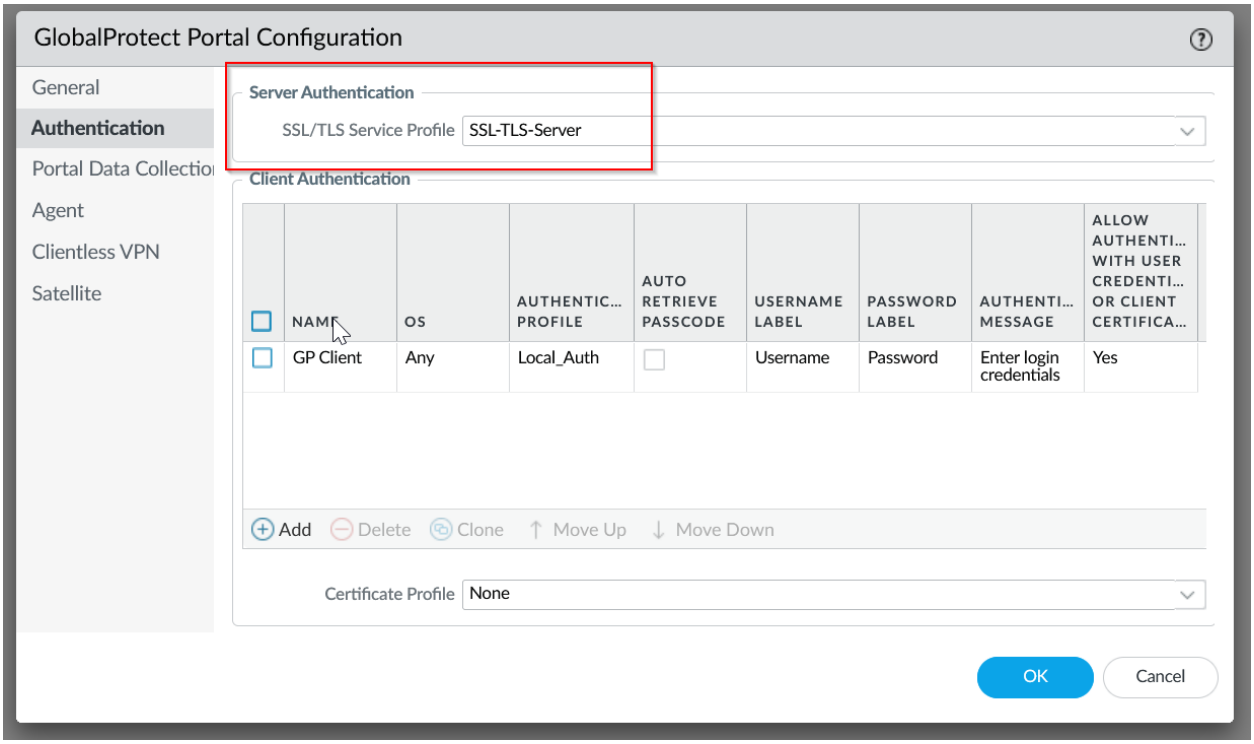


Navigate to “Network” on the GUI’s top taskbar, and then “Interfaces” and “Tunnel” on the left. Add a new interface. The Security Zone is “Untrust-L3,” or whatever outward security zone is on your firewall.

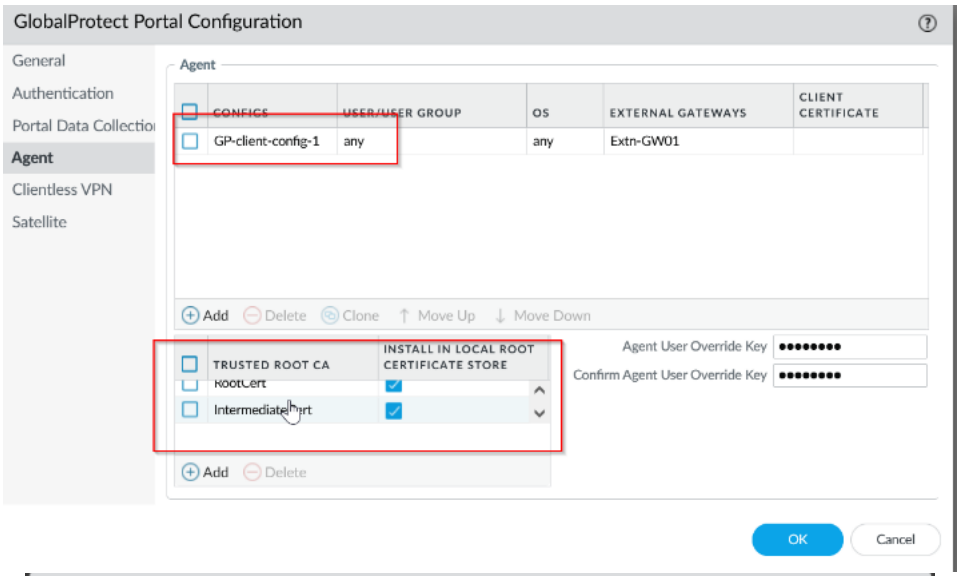


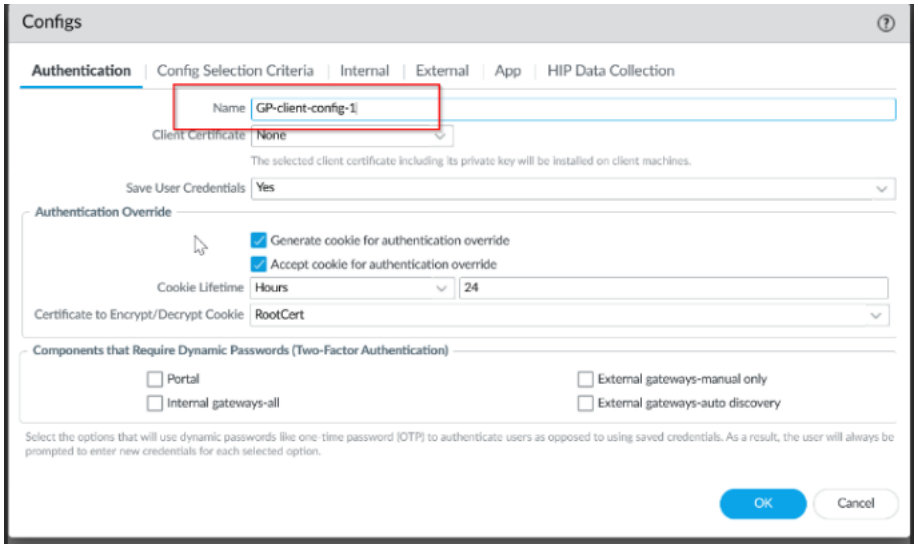
Navigate to “GlobalProtect” and “Portals” on the left and add a new one. The interface for this portal should be the outward interface on your firewall. Once done with the name and interface, click on “Authentication” and make sure the Service Profile is set to “SSL-TLS-Server.” OS is Any, and Auth Profile is Local_Auth.

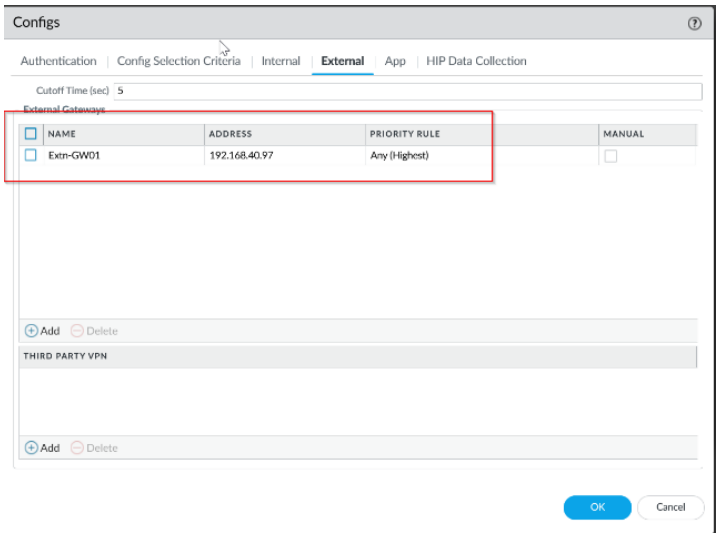




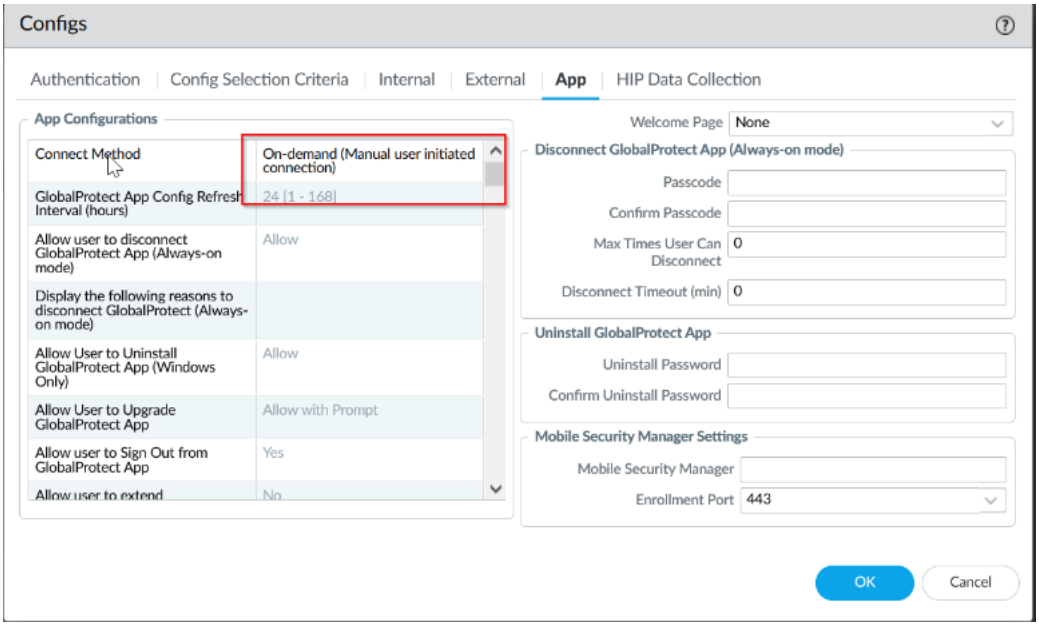
Once finished with the Authentication tab, navigate to “Agent.” Create a name, navigate to “External” and add a gateway with the ServerCert’s Common Name as the IP.


GlobalProtect Portal Configuration
General
Authentication
Portal Data Collection
Agent
Clientless VPN
Satellite
Agent
CONFIGS
USER/USER GROUP
OS
EXTERNAL GATEWAYS
CLIENT CERTIFICATE
GP-client-config-1
any
any
Extn-GW01
Add
Delete
Clone
Move Up
Move Down
TRUSTED ROOT CA
INSTALL IN LOCAL ROOT CERTIFICATE STORE
RootCert
Intermediate Cert
Add
Delete
Agent User Override Key
Confirm Agent User Override Key
OK
Cancel

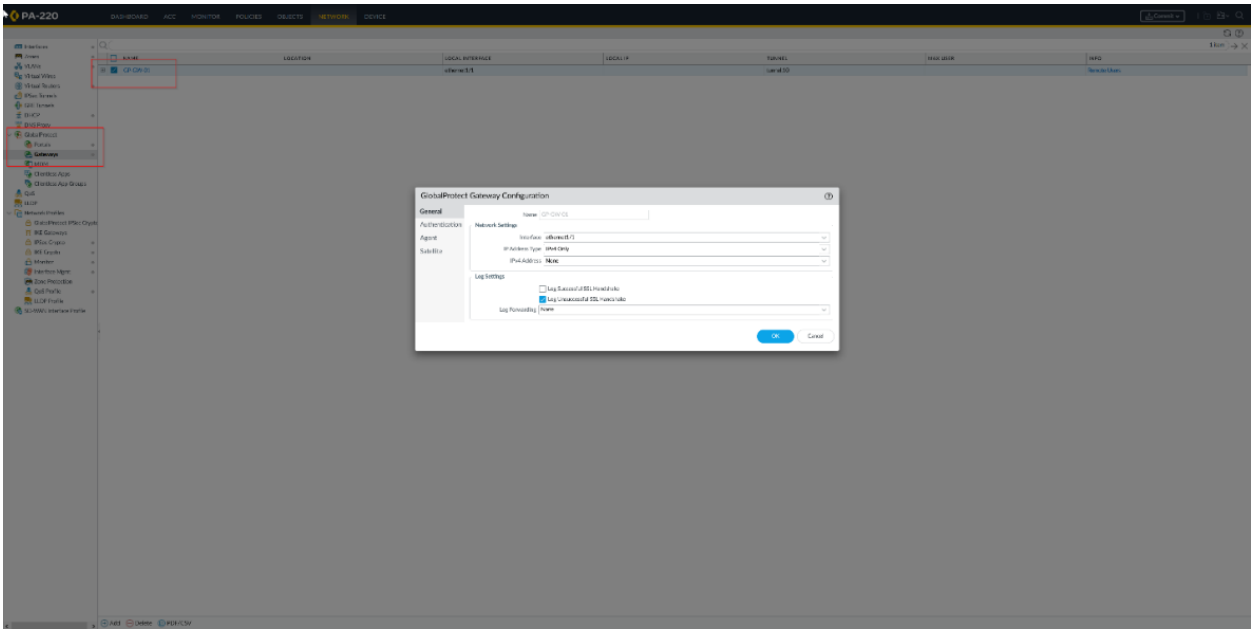

Configs
Authentication
Config Selection Criteria
Internal
External
App
HIP Data Collection
Name
GP-client-config-1
Client Certificate
None
The selected client certificate including its private key will be installed on client machines.
Save User Credentials
Yes
Authentication Override
Generate cookie for authentication override
Accept cookie for authentication override
Cookie Lifetime
Hours
24
Certificate to Encrypt/Decrypt Cookie
RootCert
Components that Require Dynamic Passwords (Two-Factor Authentication)
Portal
Internal gateways-all
External gateways-manual only
External gateways-auto discovery
Select the options that will use dynamic passwords like one-time password (OTP) to authenticate users as opposed to using saved credentials. As a result, the user will always be prompted to enter new credentials for each selected option.
OK
Cancel


Configs
Authentication
Config Selection Criteria
Internal
External
App
HIP Data Collection
Cutoff Time (sec)
5
External Gateways
NAME
ADDRESS
PRIORITY RULE
MANUAL
Extn-GW01
192.168.40.97
Any (Highest)
Add
Delete
THIRD PARTY VPN
Add
Delete
OK
Cancel

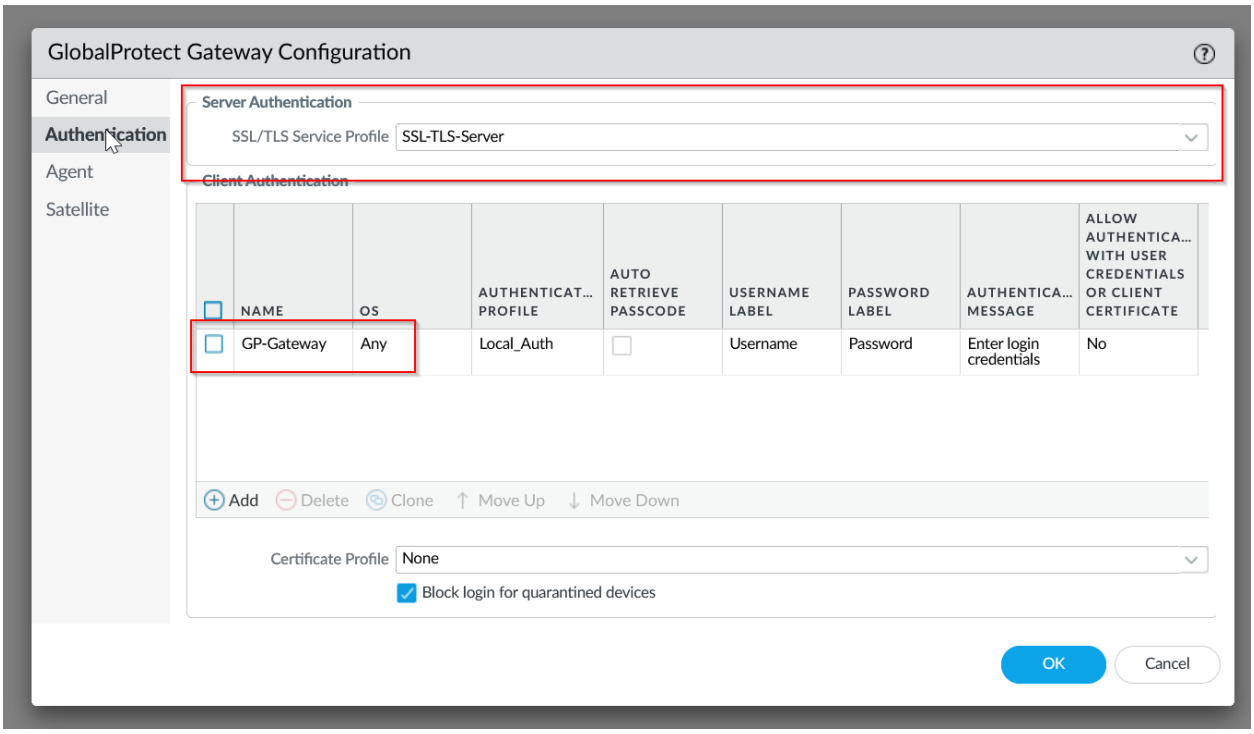
Navigate to “App” and make sure the Connect Method is On demand.



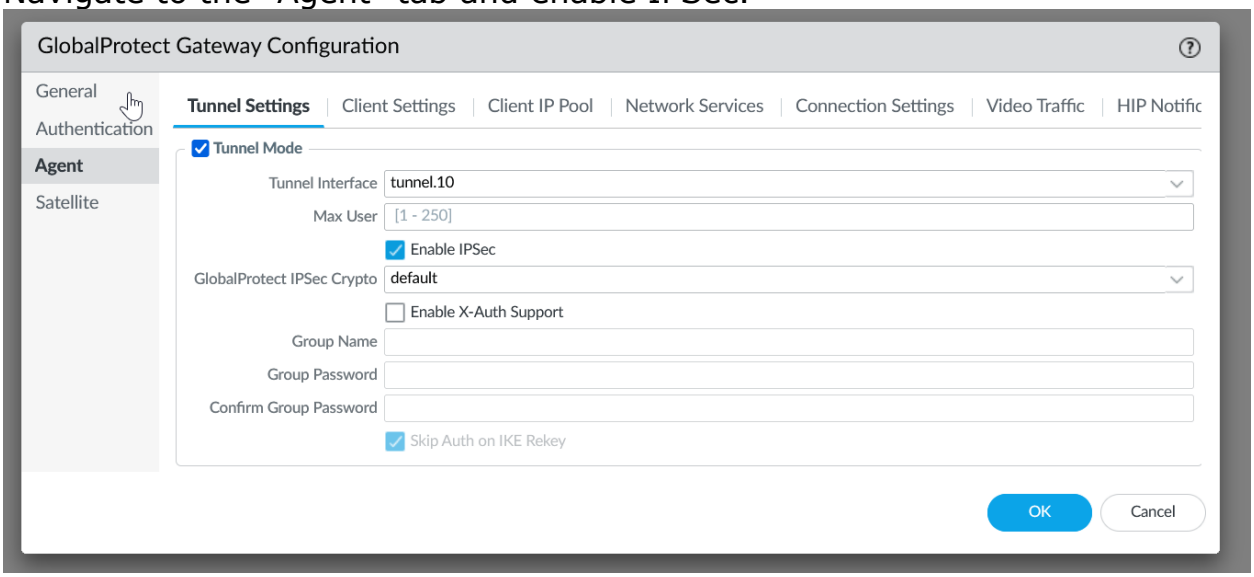
Navigate back to “Network” under the top taskbar of the GUI, and then “GlobalProtect” “Gateways” on the left. Name the gateway and use the same interface as before.



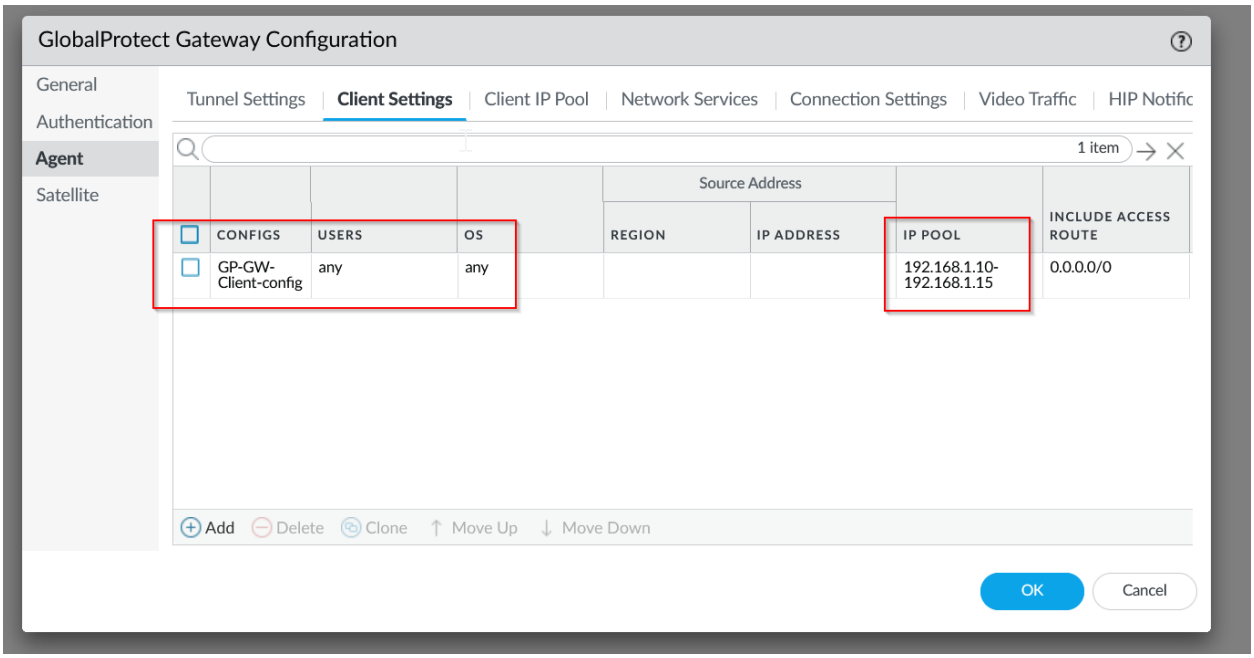
Click “Authentication” and select the previous SSL server we created. Add a new Client Authentication with the previous Authentication Profile created.



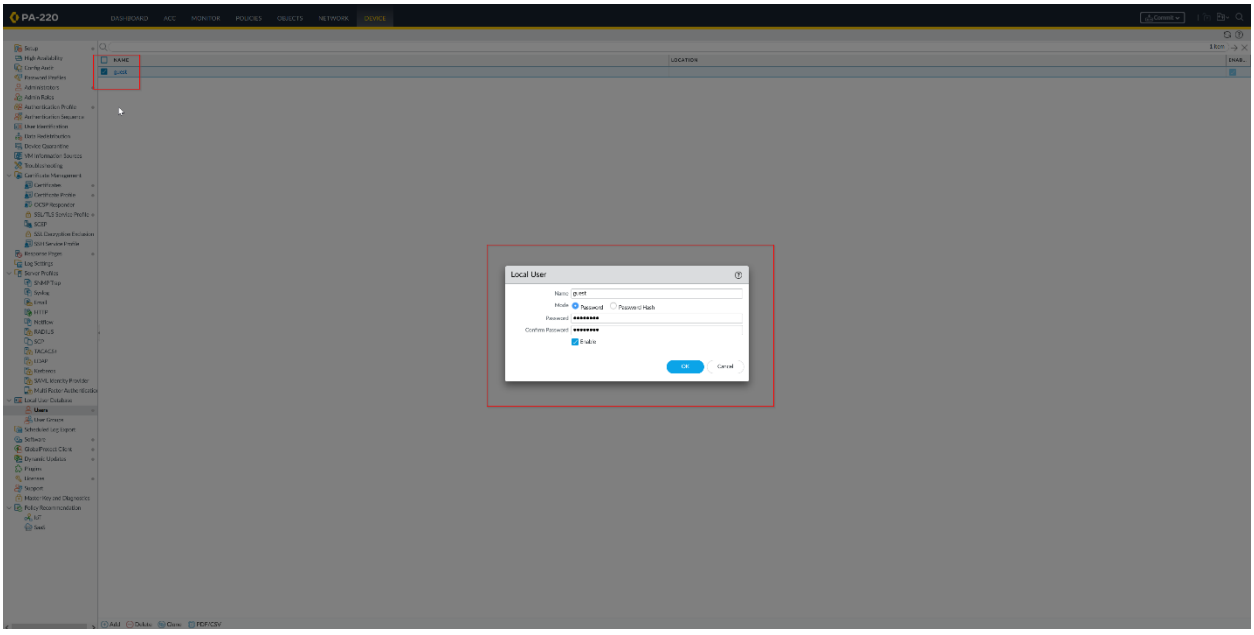
Navigate to the “Agent” tab and enable IPSec.



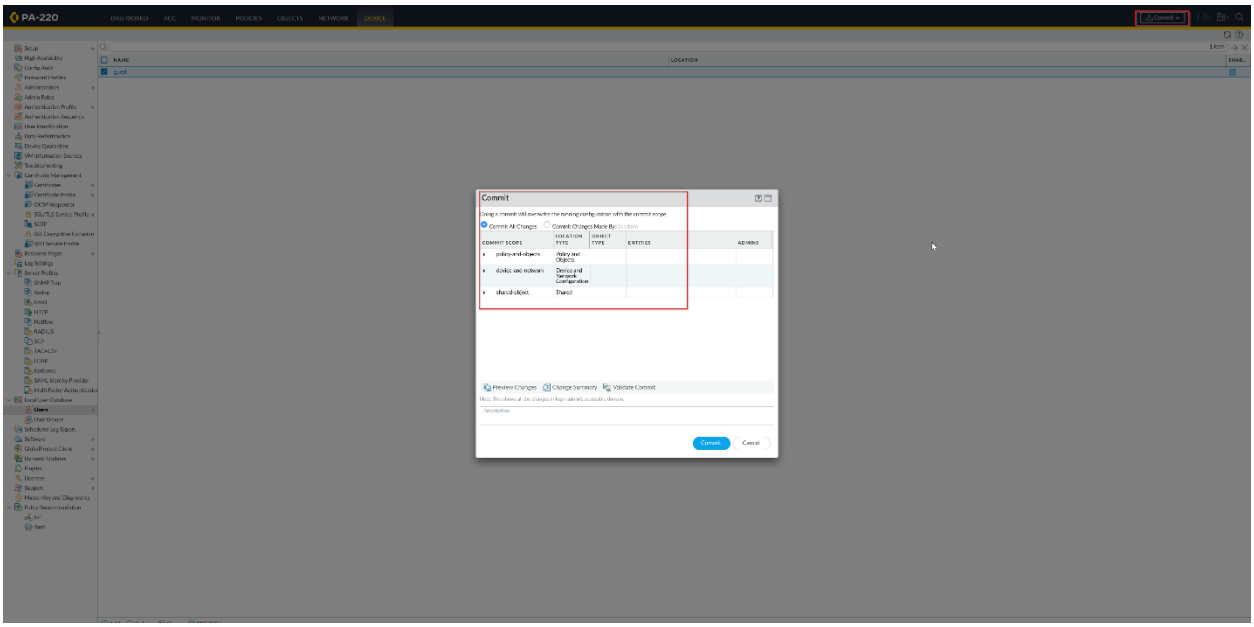
Navigate to the Client Settings under Agent and add an IP pool for end users.



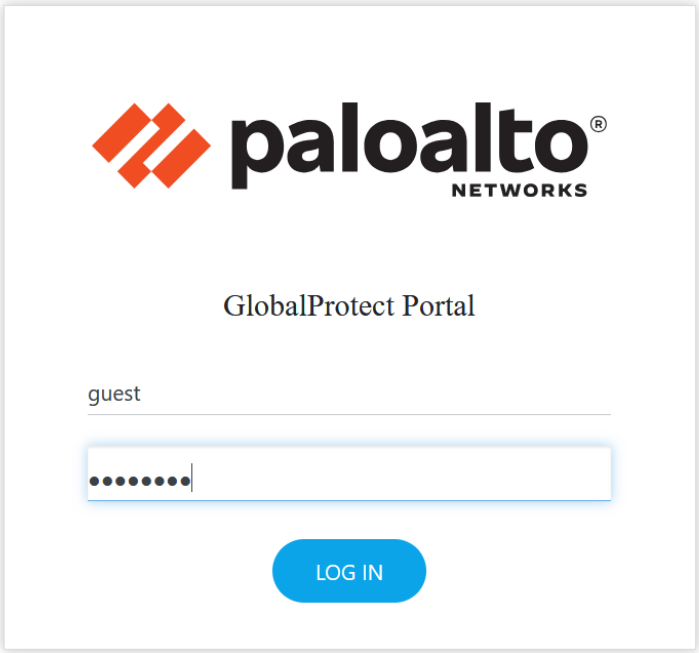
In order to test our Global Protect, navigate to “Device” and “Local User Database” and “Users” on the left taskbar. Make a new user.

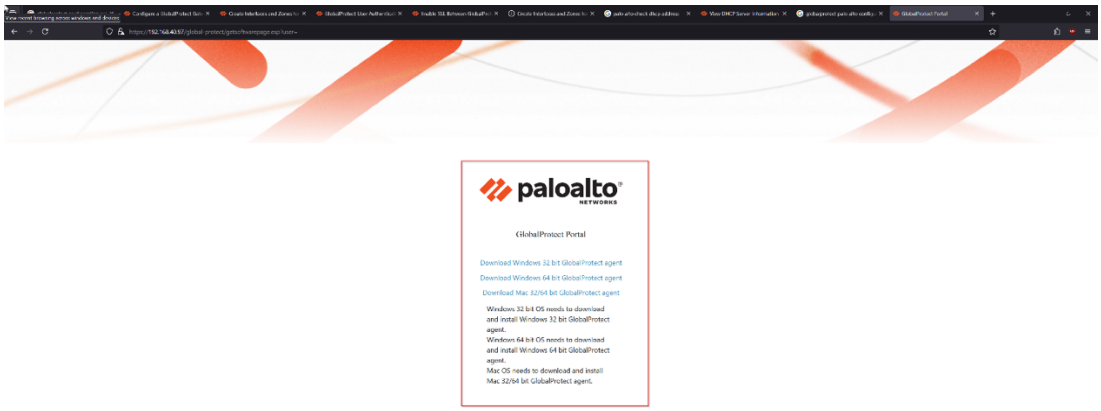


Commit the changes made to the firewall so far.

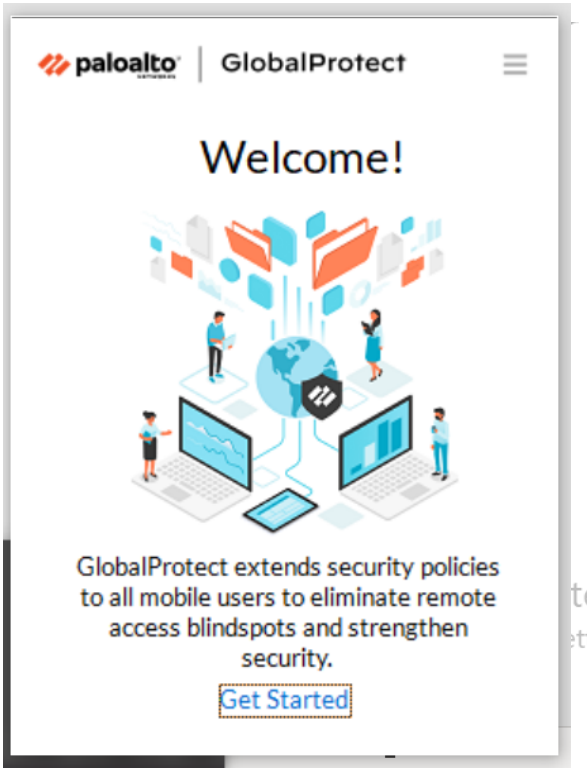


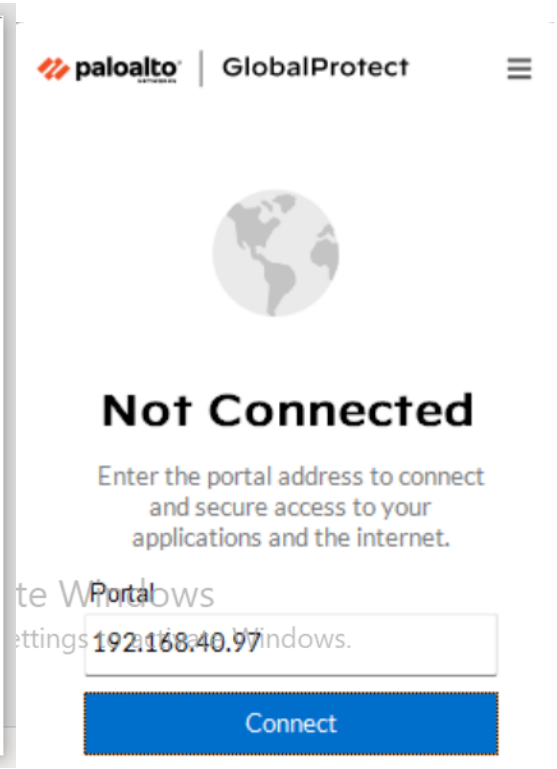
Using the IP address from your portal, enter the user credentials you've just made. Then, download the client.

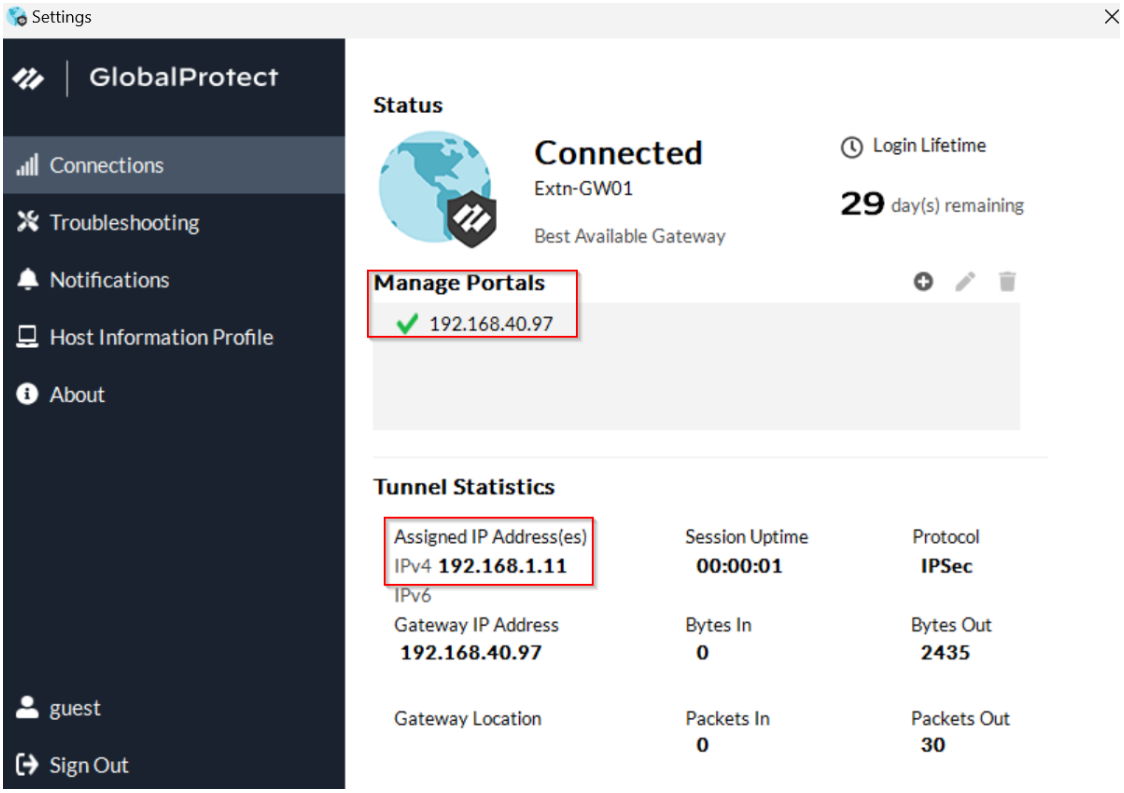




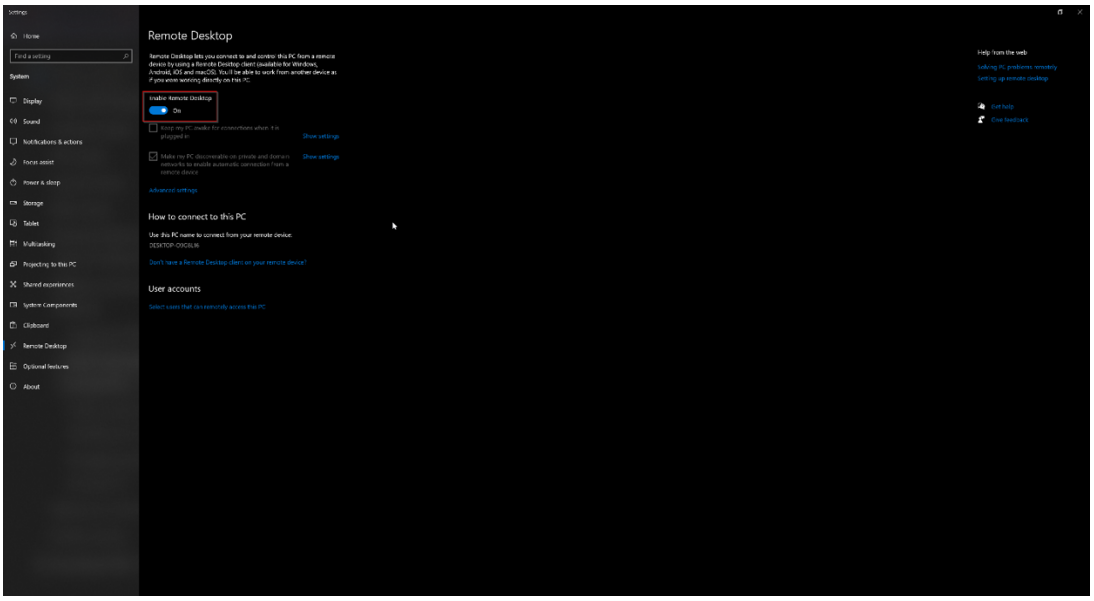
Once your app has been downloaded, click get started and use the portal IP address again. This will connect you to your VPN.



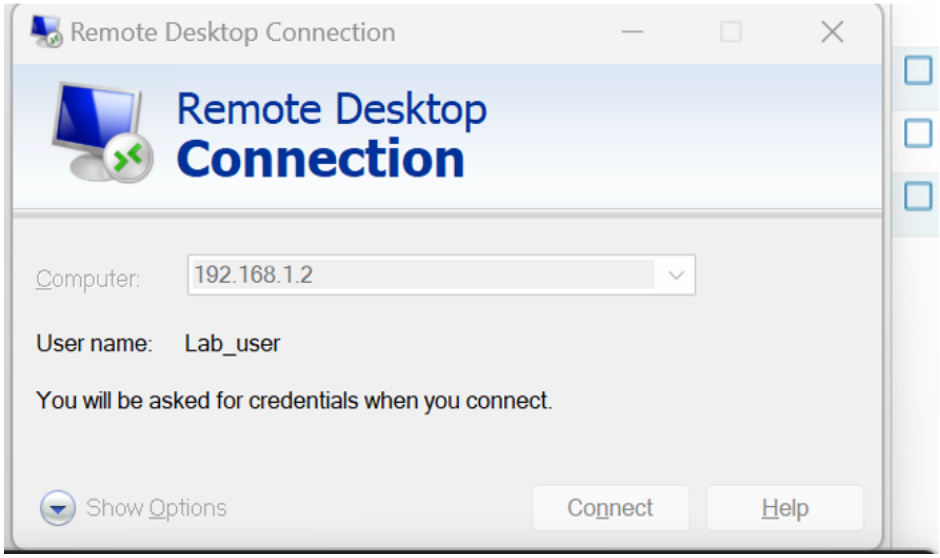


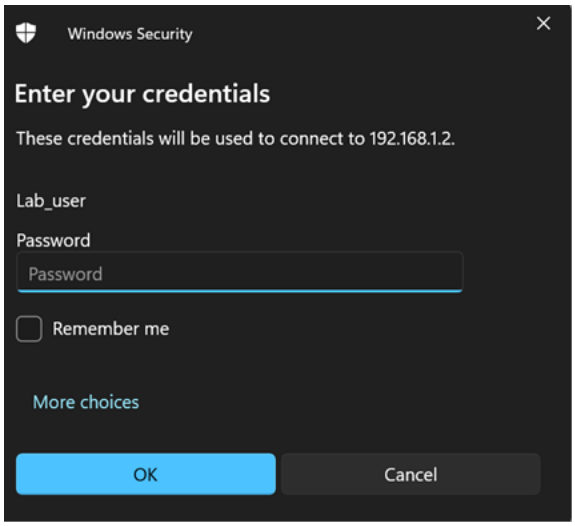


To test this VPN, we'll be using one desktop on the firewall network and another desktop off the network. The desktop off the network should be the one with all the certifications. On the firewall desktop, go to Settings, System, and then Remote Desktop. Enable Remote Desktop.

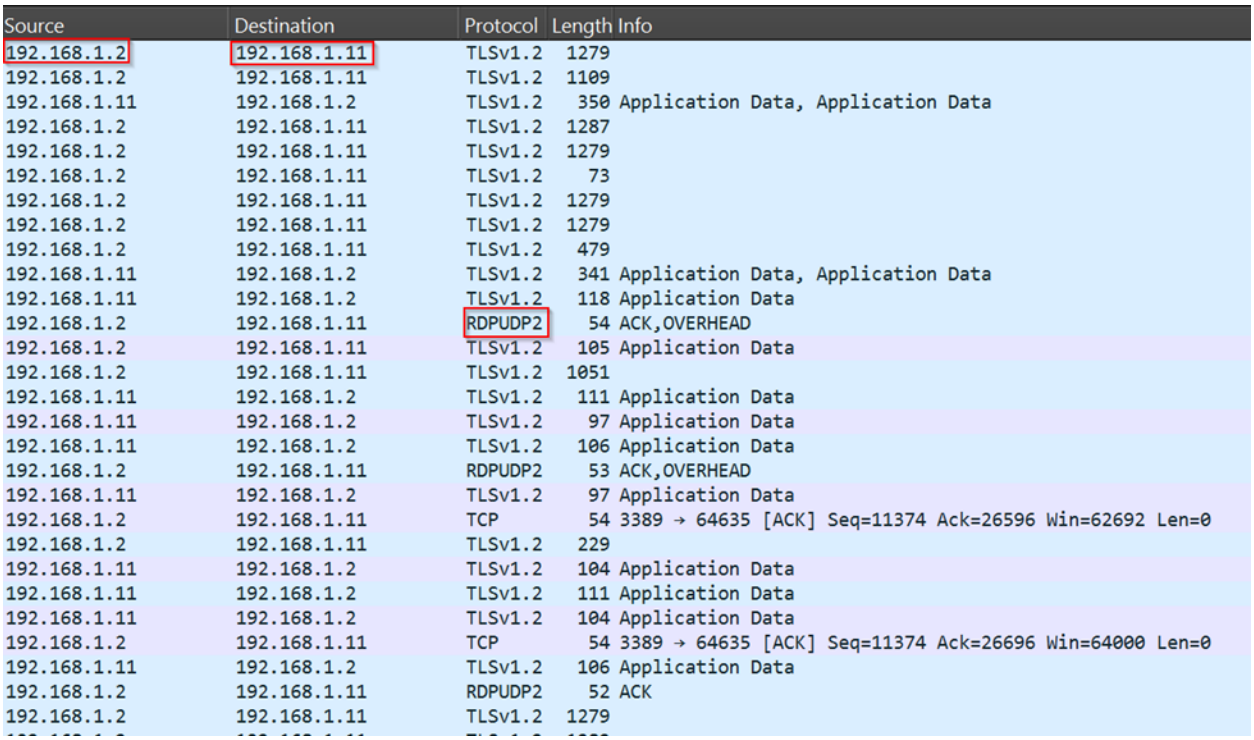


On your desktop off the network, use the Global Protect app and Device A's IP address to connect to Device A. Once you've entered your credentials, you'll be able to access the desktop on the firewall even without being in the network.





To check this, we can use Wireshark to look at the traffic on the firewall desktop. From the image below, we see that the firewall desktop is communicating with the desktop off the network that has an IP of 192.168.1.11, an automatically assigned IP from Global Protect. The protocol is RDP, or Remote Desktop, meaning that we've succeeded in configuring Global Protect.



Source	Destination	Protocol	Length	Info
192.168.1.2	192.168.1.11	TLSv1.2	1279	
192.168.1.2	192.168.1.11	TLSv1.2	1109	
192.168.1.11	192.168.1.2	TLSv1.2	350	Application Data, Application Data
192.168.1.2	192.168.1.11	TLSv1.2	1287	
192.168.1.2	192.168.1.11	TLSv1.2	1279	
192.168.1.2	192.168.1.11	TLSv1.2	73	
192.168.1.2	192.168.1.11	TLSv1.2	1279	
192.168.1.2	192.168.1.11	TLSv1.2	1279	
192.168.1.2	192.168.1.11	TLSv1.2	479	
192.168.1.11	192.168.1.2	TLSv1.2	341	Application Data, Application Data
192.168.1.11	192.168.1.2	TLSv1.2	118	Application Data
192.168.1.2	192.168.1.11	RDPUDP2	54	ACK,OVERHEAD
192.168.1.2	192.168.1.11	TLSv1.2	105	Application Data
192.168.1.2	192.168.1.11	TLSv1.2	1051	
192.168.1.11	192.168.1.2	TLSv1.2	111	Application Data
192.168.1.11	192.168.1.2	TLSv1.2	97	Application Data
192.168.1.11	192.168.1.2	TLSv1.2	106	Application Data
192.168.1.2	192.168.1.11	RDPUDP2	53	ACK,OVERHEAD
192.168.1.11	192.168.1.2	TLSv1.2	97	Application Data
192.168.1.2	192.168.1.11	TCP	54	3389 → 64635 [ACK] Seq=11374 Ack=26596 Win=62692 Len=0
192.168.1.2	192.168.1.11	TLSv1.2	229	
192.168.1.11	192.168.1.2	TLSv1.2	104	Application Data
192.168.1.11	192.168.1.2	TLSv1.2	111	Application Data
192.168.1.11	192.168.1.2	TLSv1.2	104	Application Data
192.168.1.2	192.168.1.11	TCP	54	3389 → 64635 [ACK] Seq=11374 Ack=26696 Win=64000 Len=0
192.168.1.11	192.168.1.2	TLSv1.2	106	Application Data
192.168.1.2	192.168.1.11	RDPUDP2	52	ACK
192.168.1.2	192.168.1.11	TLSv1.2	1279	

Problems:

The only problem that our group had with this lab was downloading Global Protect from the portal. Initially, when we tried to download the app, we didn't get anything from the file and were unable to. After figuring out that the problem lay in our not having installed the Global Protect app onto our firewall, we were able to fix this and install the app to our firewall to then download the app to our computer from the portal.

Conclusion:

In conclusion, Virtual Private Networks are an important method for employees to access business networks from remote locations or for Internet users to protect their data. The VPN setup in this lab was mostly dedicated to the first application of VPNs mentioned and included our group setting up a remote desktop connection. To do this, we used various configurations of the Palo Alto PA-220 GUI as well as the Global Protect App to connect to remote desktops.

Fortinet SOHO and WPA2-PSK/Enterprise Setup

Andrew Pai

Purpose:

The purpose of this lab was to familiarize our group with Fortigate 40F firewalls by setting up a common SOHO network and configuring an access point for both wireless WPA2-PSK and wireless WPA2-Enterprise. This will allow the Fortigate to manage a small network and securely allow wireless users onto the network. In order to do this, we'll also have to factory reset the firewall and gain access to the GUI.

Background Information:

Much like the second lab of our Palo Alto curriculum, this lab is focused on implementing a SOHO (Small Office/Home Office) network, only this time on a Fortigate 40F firewall instead of a Palo Alto firewall. Additionally, our group will be configuring a Fortinet Access Point to utilize WPA2 Pre-Shared Key and Enterprise protocols to allow wireless users onto the network, something that we had never done before on Palo Altos.

To recap, a SOHO network is one that's used by small offices or individuals in a homemade office. They encompass a local area network (LAN) and are both cost effective and flexible. They're also mainly used because their small size makes them easy to set up and they can often connect to a larger network.

For this SOHO network that our lab is going to be setting up, we will be using a Fortigate 40F firewall from Fortinet. Based in Sunnyvale, California and founded by Ken Xie and Michael Xie, Fortinet is a cybersecurity company that creates security solutions like firewalls and intrusion detection systems. Compared to Palo Alto firewalls, their Fortigate 40F firewall may have less capabilities and options, but the GUI is simpler and easier to manage, making it far more intuitive when creating, managing, and maintaining networks. They also use security processing units (SPU) from FortiASIC, which is a Fortinet specific technology that allows for high speed, scale, and efficiency of Fortinet firewalls.

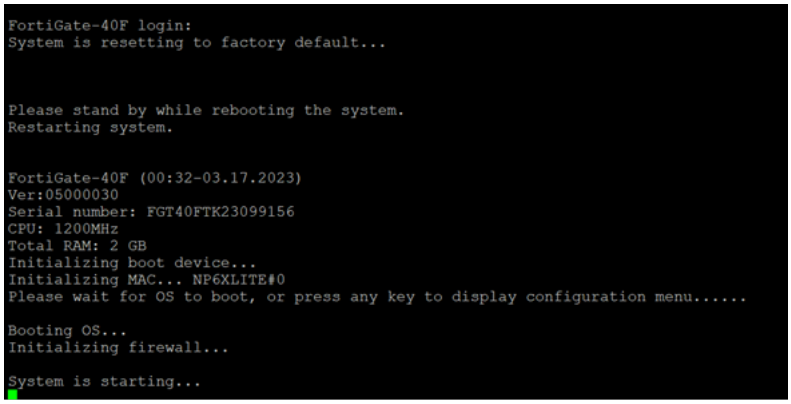
Access points are wireless network devices that essentially allow devices to connect to a LAN without actually being plugged into it. They allow for an increase in the number of devices that can be on the network if all the physical slots are taken up, and extend any existing wireless coverage on a network. For this lab, our group used the security protocols of WPA2-Pre-Shared Key (WPA2-PSK) and WPA2-Enterprise. Security protocols are used to authenticate users and make sure that they should have access to the network. While both WPA2-PSK and WPA2-Enterprise are secure, they differ in the way that they validate and check for whether a user should be

allowed. WPA2-PSK is where one singular password is used to allow hosts onto the network, and anyone with the password can join. A good example of this would be the WiFi password of someone's house, where if you need a new device to join all they need is a password. WPA2-Enterprise on the other hand validates users through creating specific users and passwords linked to those users. While it's more complex and generally takes more sophistication to set up, it has benefits in that one security breach wouldn't compromise the entire network. It also allows for an easier time tracking users and their activity on the network.

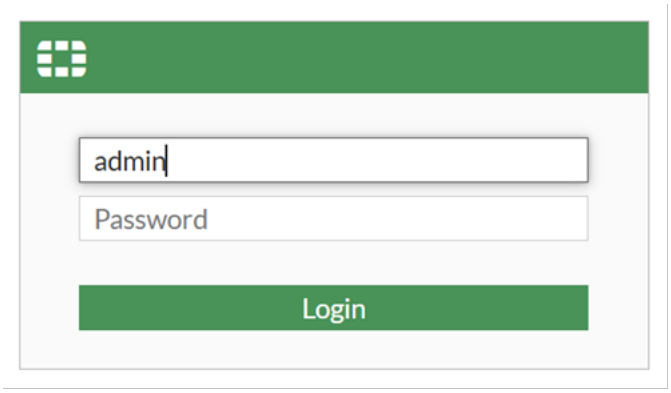
Lab Summary:

Since we're starting with a brand new Fortigate firewall, one thing that we have to do is reset the firewall to enter in new credentials. To do this, unplug the device for 10 seconds, replug it in and hold the reset button until the status light blinks.

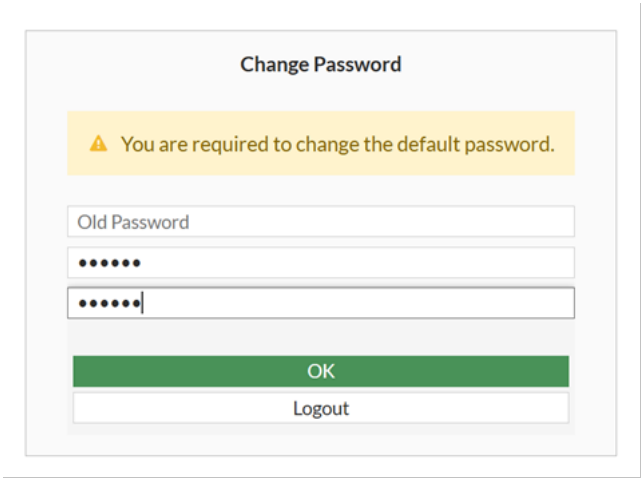
The success of this step can be checked by consoling into the firewall as shown below, where you're able to watch the progress of the firewall's reset.



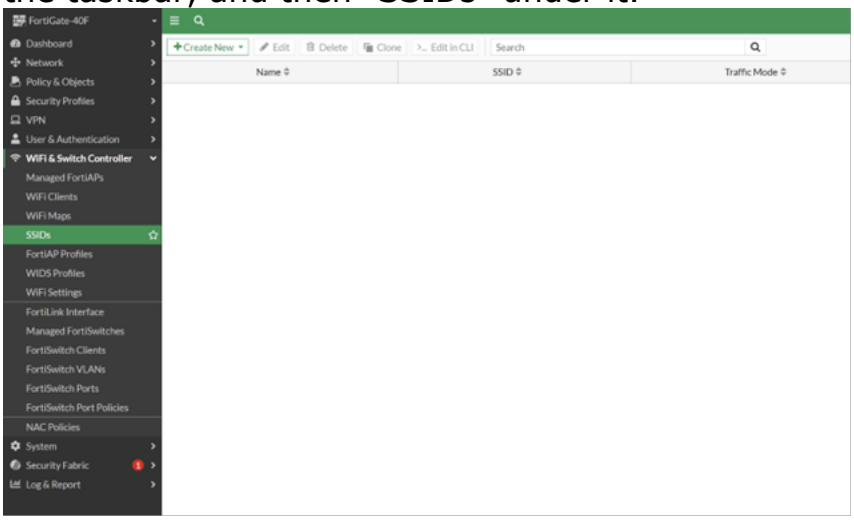
After the firewall has been reset, enter the management IP address of the firewall, which should be 192.168.1.99. This will get you into the GUI of the firewall. From there, you can enter the default credentials of admin and no password.



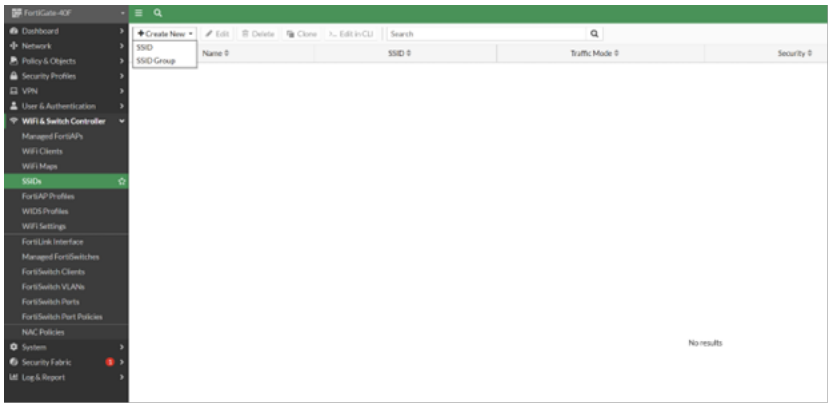
Once you've logged in with default credentials, you should be able to enter your own password and device hostname.



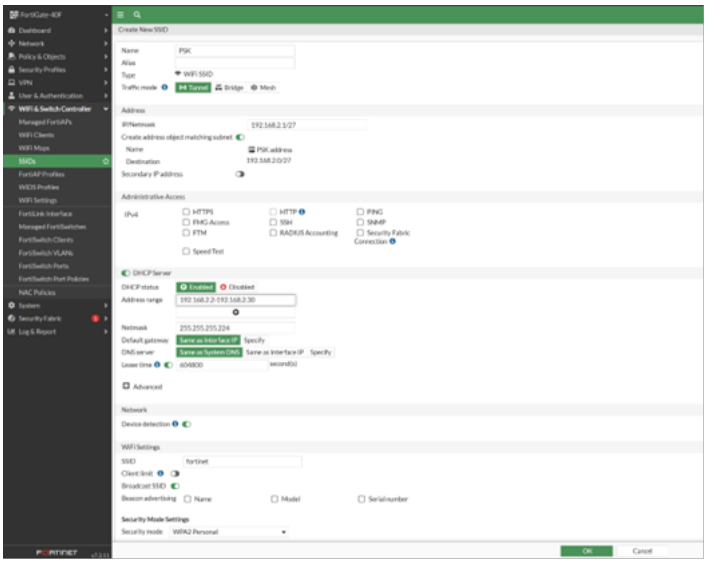
In the GUI, navigate to the "WiFi and Switch Controller" section on the left of the taskbar, and then "SSIDs" under it.

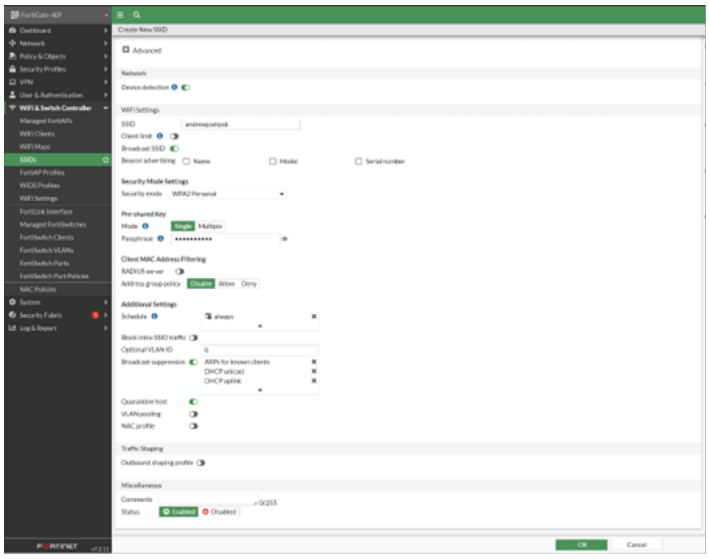


Click "Create New" and the "SSID" in the top left corner of the screen.

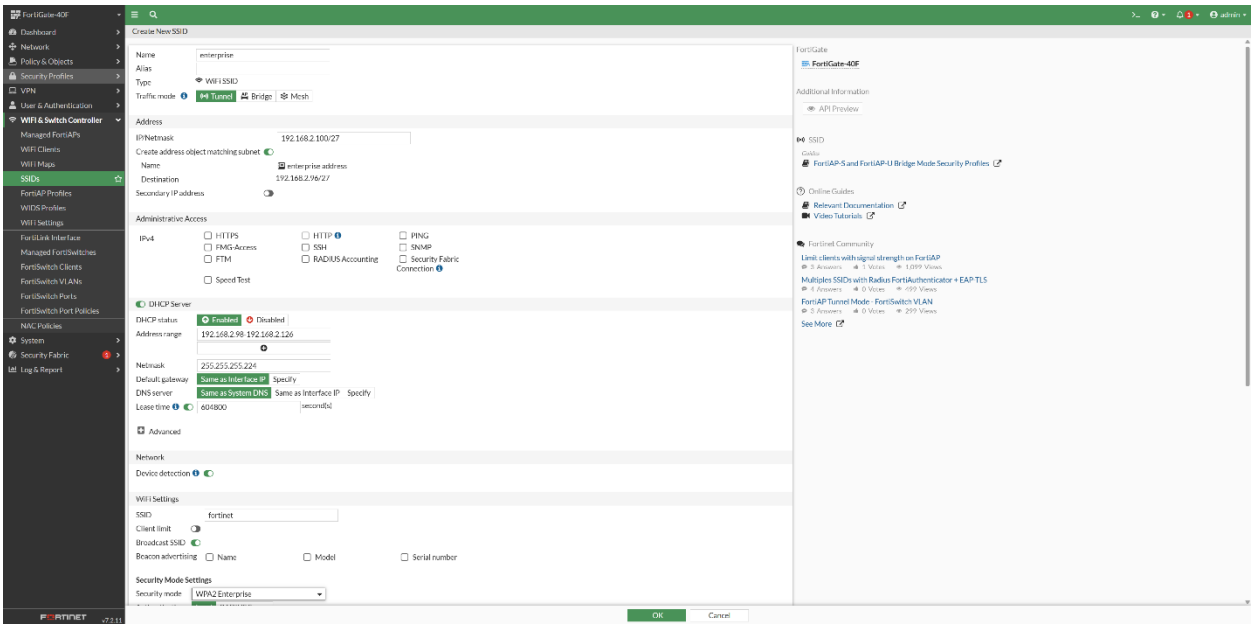


Appropriately name your SSID and enable DHCP. Choose WPA2 Personal for the security mode and then create your pre-shared key.

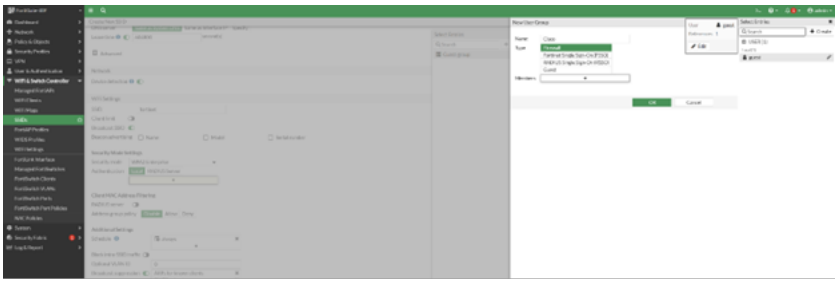


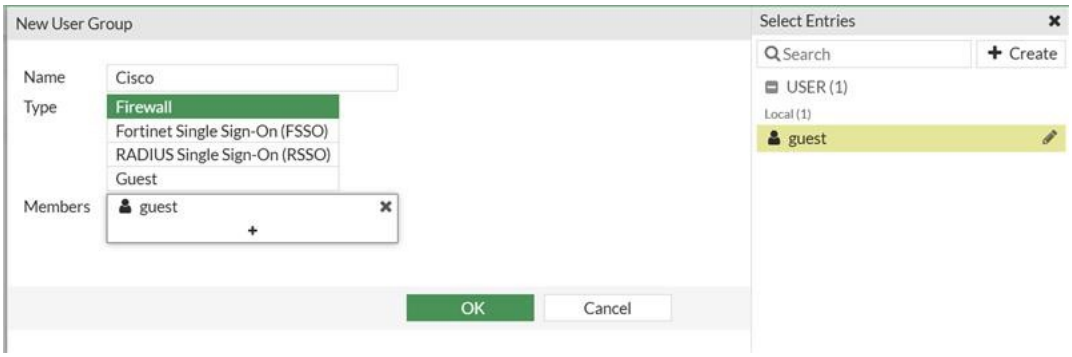


Create another new SSID for the WPA2-Enterprise protocol now, choosing enterprise as the security mode.

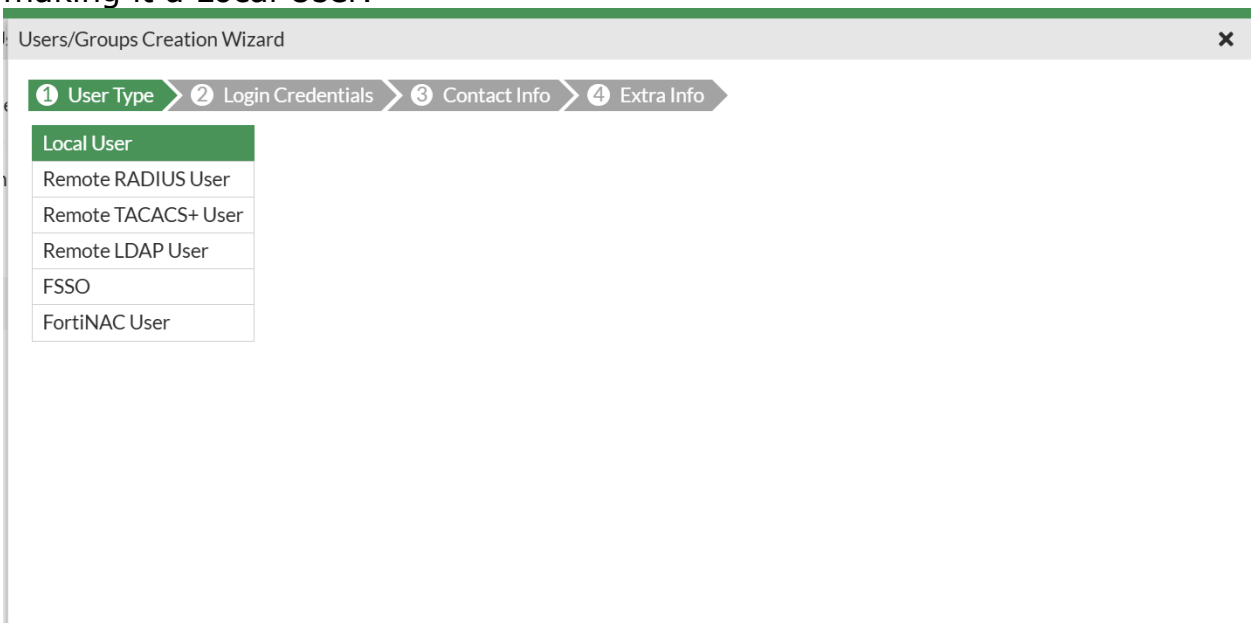


Create a new User Group with the “Firewall” type on the side of the Enterprise SSID creation.

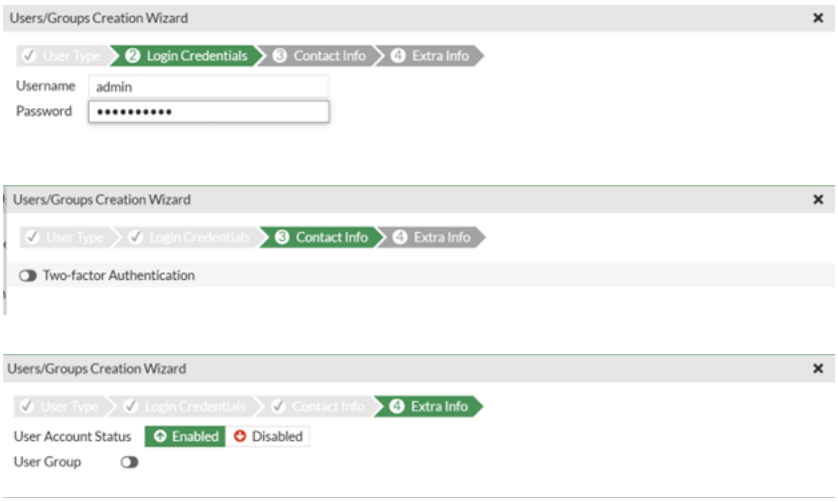




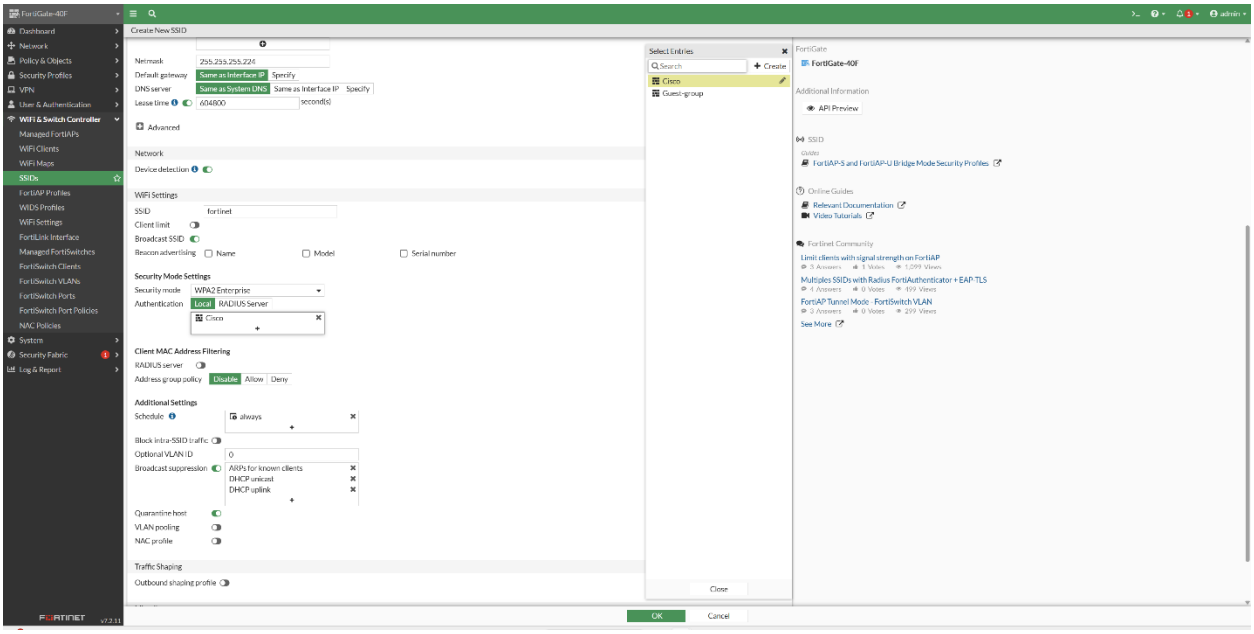
Create another User Group through the User/Groups Creation Wizard, making it a Local User.



Input your chosen login credentials and click through contact info and extra info, making sure two factor authentication is off and user account status is enabled.

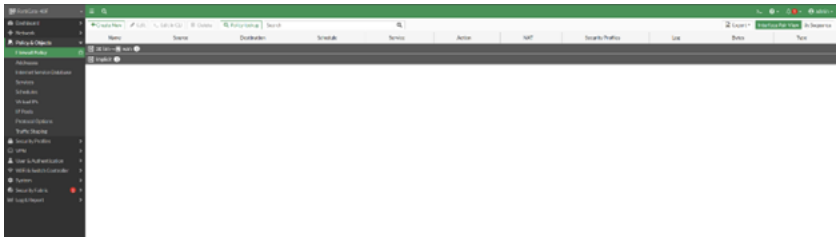


Finish creating your enterprise SSID by clicking “Ok” on the bottom of the screen.

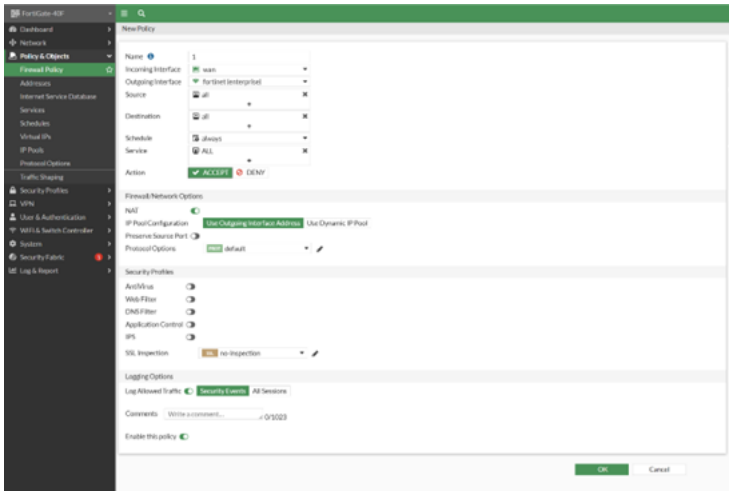


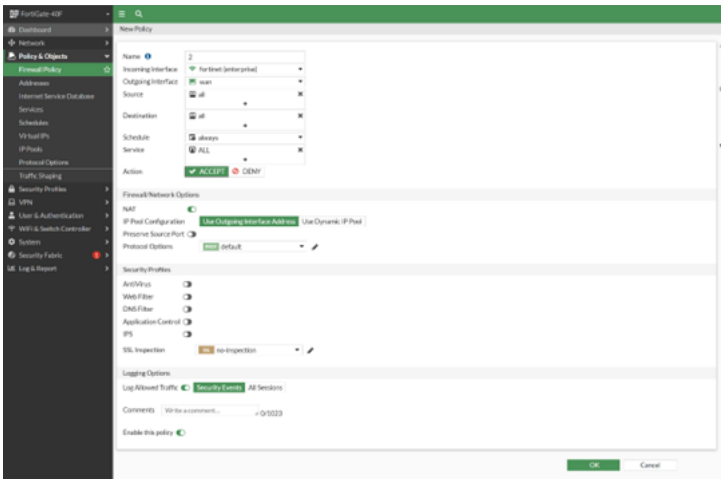
Now in the “SSIDs” section, make sure you have both a PSK and Enterprise SSID.

Navigate to “Policy & Objects” and then to “Firewall Policy.” Through this section, we’ll be creating 4 new Firewall Policies.

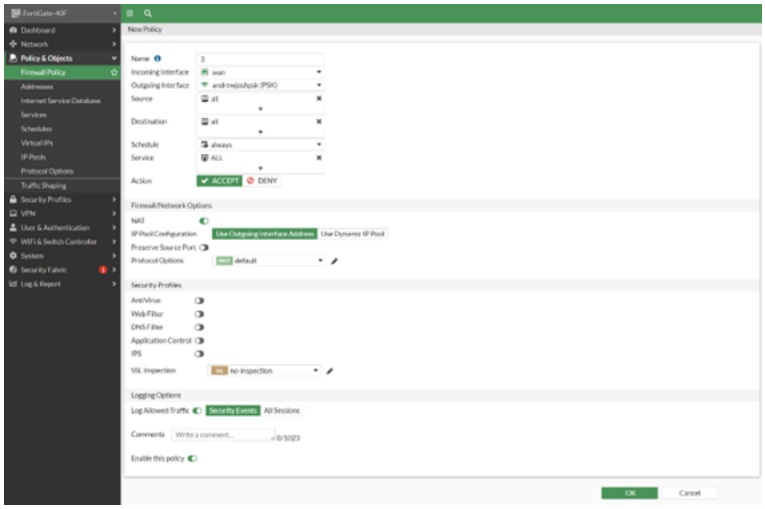


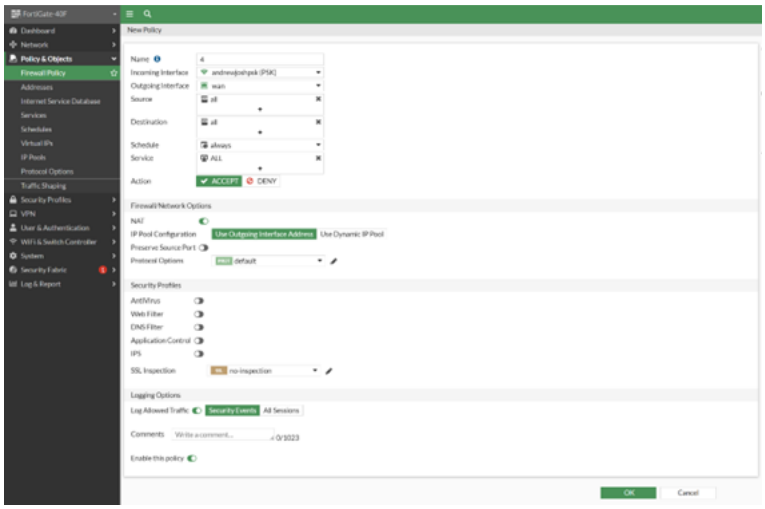
Hit “Create New,” set the incoming interface to “wan” and the outgoing to your enterprise network. Once you do this, create another policy with incoming as enterprise and outgoing as “wan”.



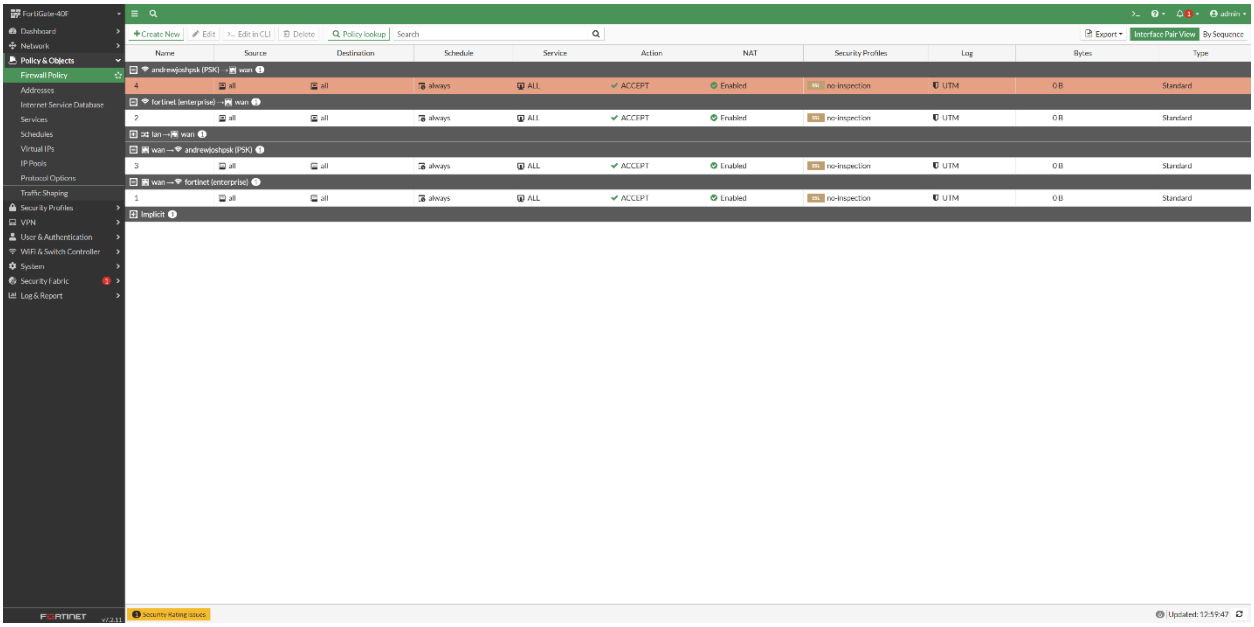


Now that you have your policies for WPA2-Enterprise set up, do the same thing you just did except for WPA2-PSK. Make sure that you have two policies where “wan” and PSK are each in incoming and outgoing interfaces once.

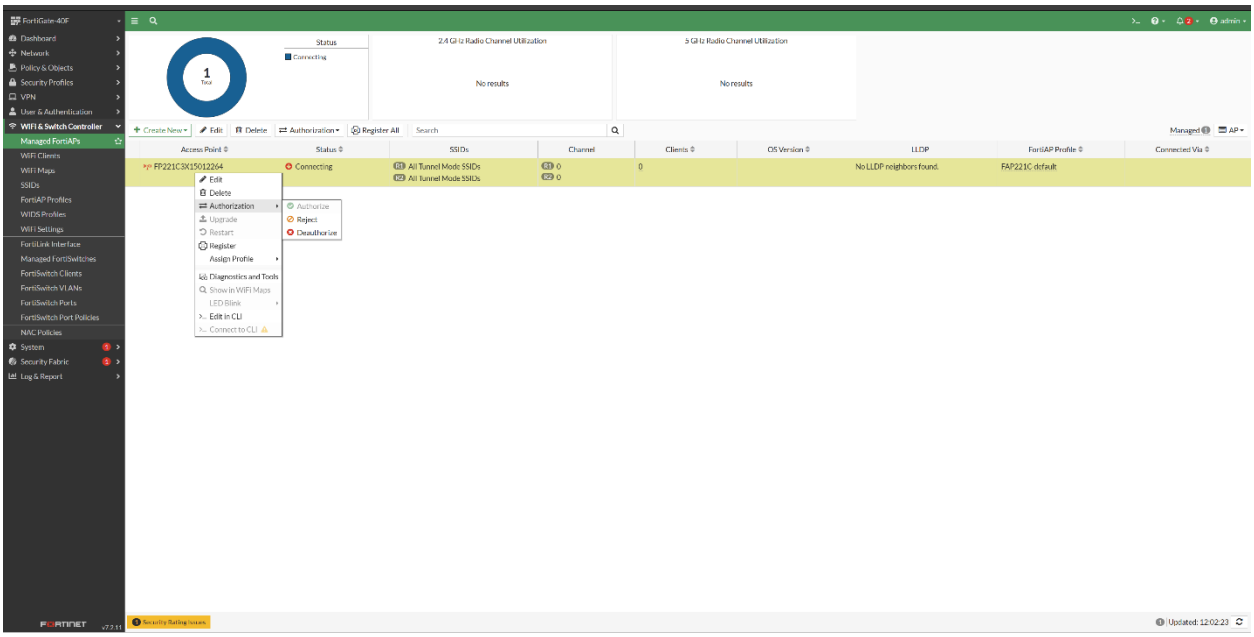




Verify that all 4 of these new policies have been created on your GUI.



Finally, navigate to “WiFi & Switch Controller” and then “Managed FortiAPs.” Find the access point you’re using and authorize it under the authorization tab.



Problems:

One of the problems that our team came across was an error in the physical wiring of the devices. By miswiring our firewall, switches, and ISP, our group stopped ourselves from logging into the GUI of the firewall even after having reset the firewall. This prevented us from making further progress on the lab until we found our error in wiring and fixed it.

Conclusion:

In conclusion, this lab has familiarized our group with factory resetting a Fortigate 40F firewall, setting up a SOHO network on it, and using a FortiAP access point with various security protocols. We are now capable of navigating the Fortigate’s GUI fluently and can confidently set up small networks where needed.

Fortigate 40F Firewall SSL VPN Configuration

Andrew Pai

Purpose:

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

Background Information:

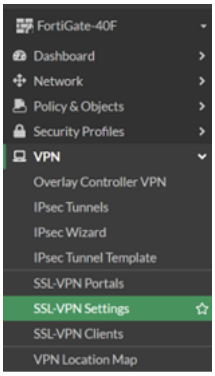
This lab focuses on implementing an SSL VPN on our Fortigate 40F firewall. Like mentioned in a previous lab for configuring the Global Protect VPN on a Palo Alto firewall, VPNs are known as Virtual Private Networks and are used to connect to a private network while not actually being in that network.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

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

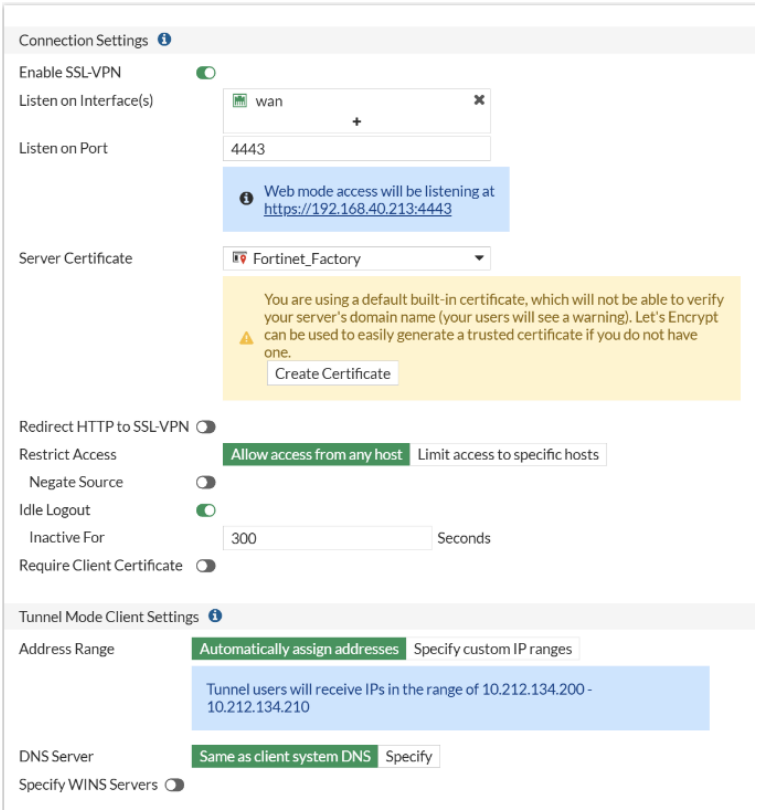
In order to connect from a remote desktop to the firewall's internal network through the SSL VPN, our group will be using Fortinet's Forticlient VPN software. Forticlient is a typical VPN client that allows users to connect to an internal network through both SSL and IPSec VPNS. While IPSec is an option for Forticlient, our group will be addressing that in a different lab instead of this one. Forticlient also has various other authentication methods like two factor authentication and can use split tunneling.

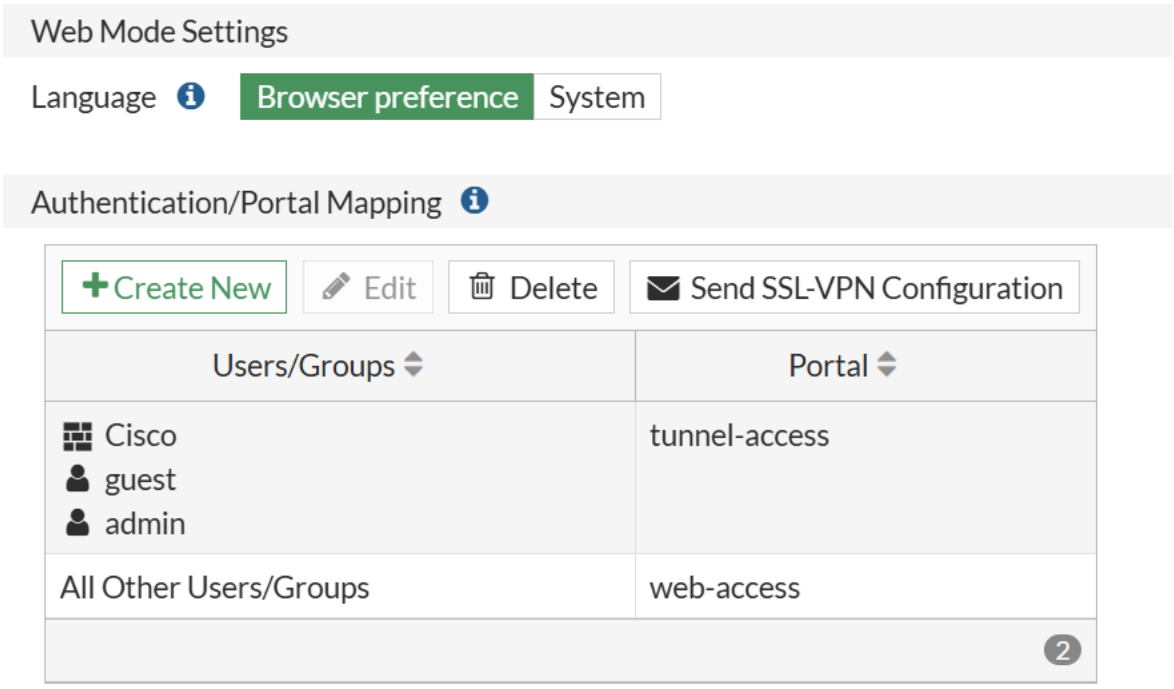
Lab Summary:

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

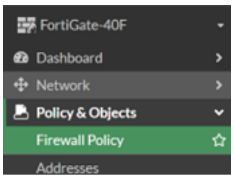


Create a new VPN and enable it to use the WAN interface of your network. Create a custom port that you'll use on Forticlient and use the default Fortinet_Factory Certificate. Add the user groups that you'll need to use the VPN into the VPN settings.

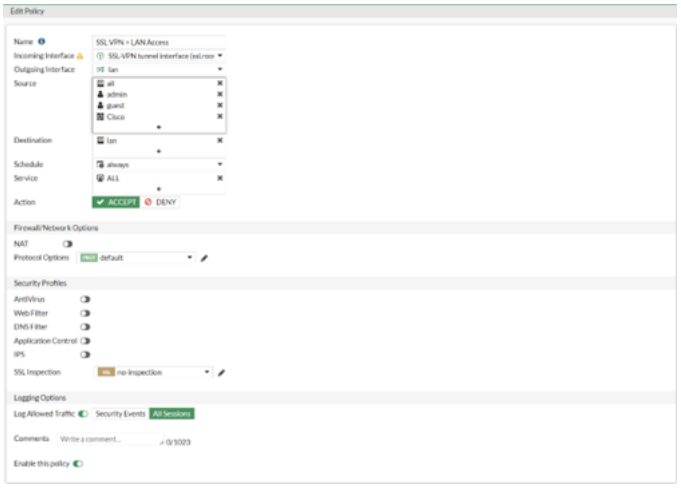




Navigate to Firewall Policies under Policy & Objects on the left taskbar and create a new policy.

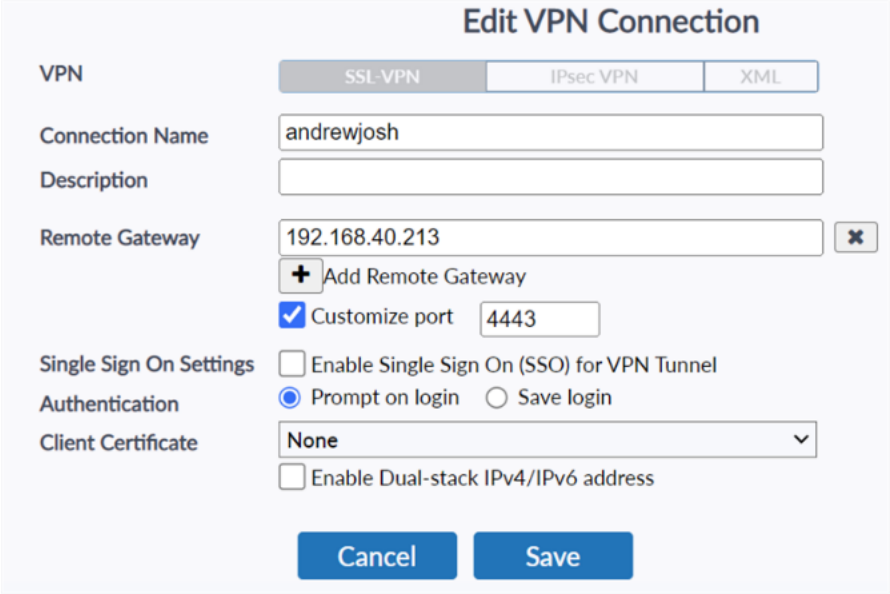


Set the outgoing interface to your LAN's interface, with the incoming interface as the SSL VPN tunnel you just created. Add your intended user groups to source and your LAN to destination.

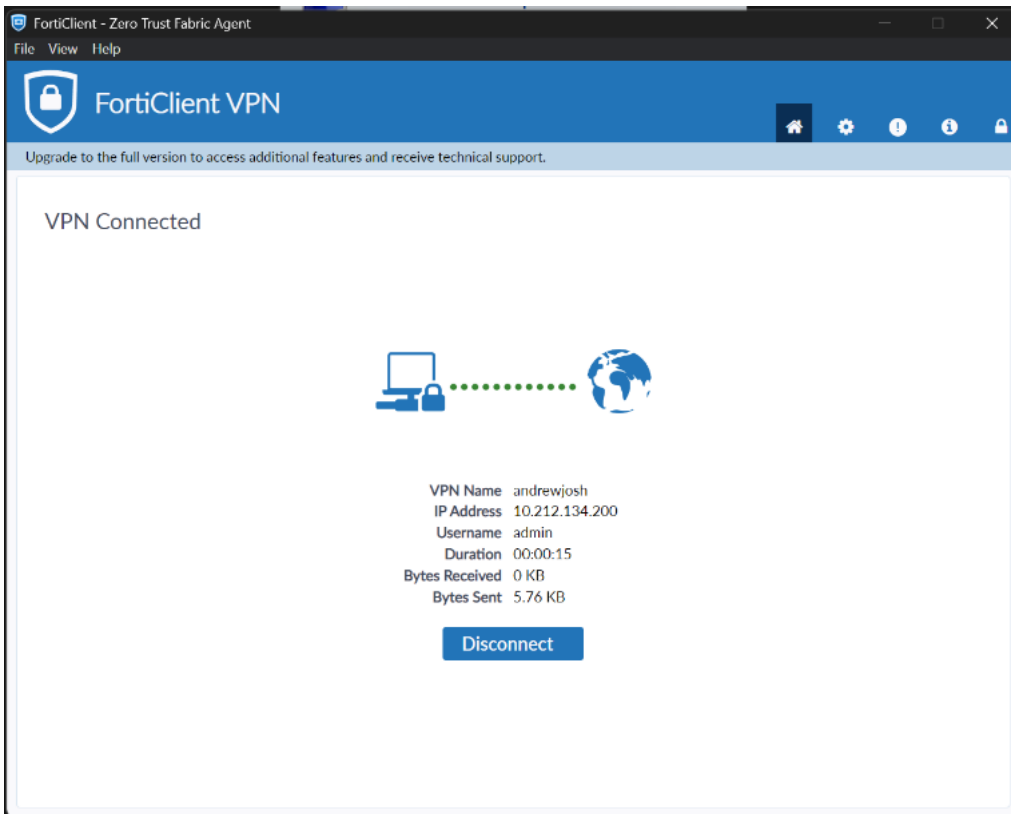


Download the Forticlient VPN software onto another PC and click on "Add a new connection" so you can create a new VPN.

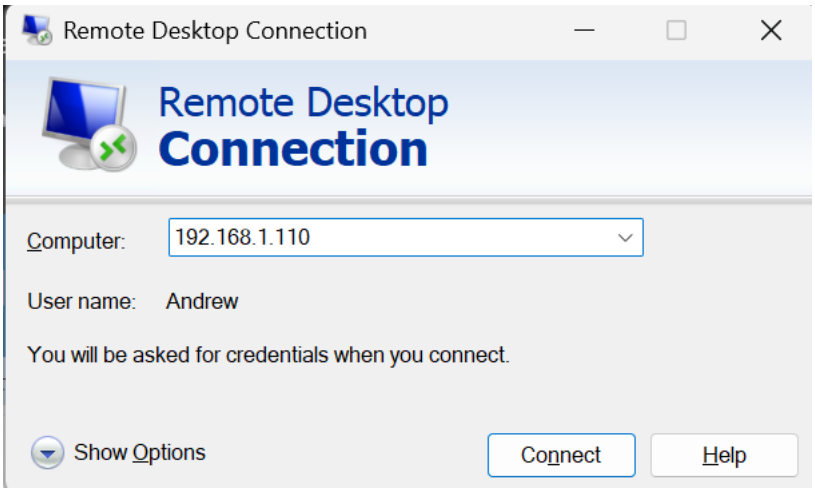
Select "SSL VPN," add the IP of the firewall that you're using, and add in the port that you configured for your SSL VPN earlier in the lab.



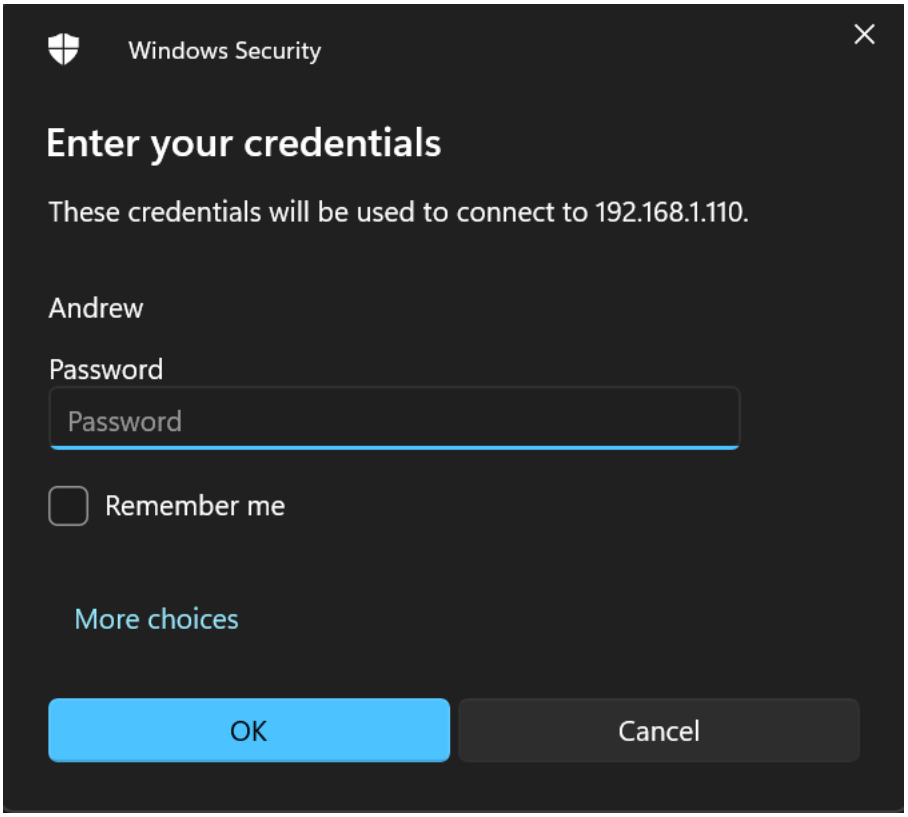
Once you've created your VPN settings on Forticlient, attempt to log in with one of the user authentication credentials you set up earlier.



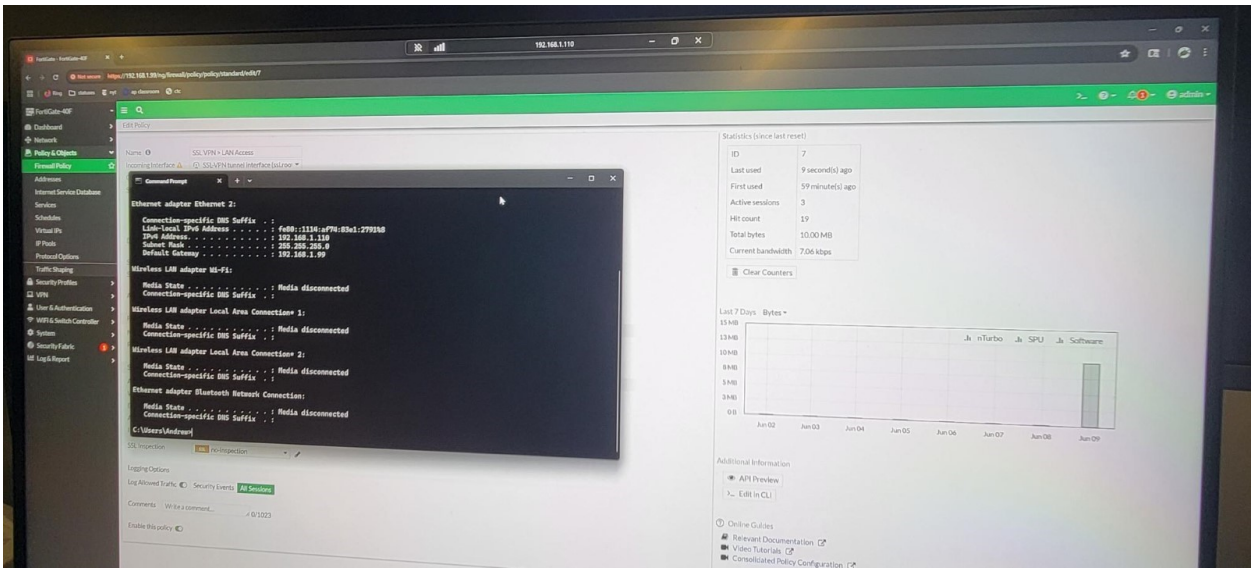
Finally, in order to actually use your VPN, log in to Window's Remote Desktop Connection and type in the IP of the PC you're trying to reach.



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



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



Problems:

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

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

Conclusion:

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

Fortigate 40F Firewall IPSec VPN Configuration

Andrew Pai

Purpose:

The purpose of this lab was to have our group configure our Fortigate 40F firewall with an IPSec VPN. This will allow a PC within our firewall's network to remotely access another PC that's on a different firewall's network. This requires two different groups and firewalls for this lab as well as skills with the Fortigate GUI and RDP.

Background Information:

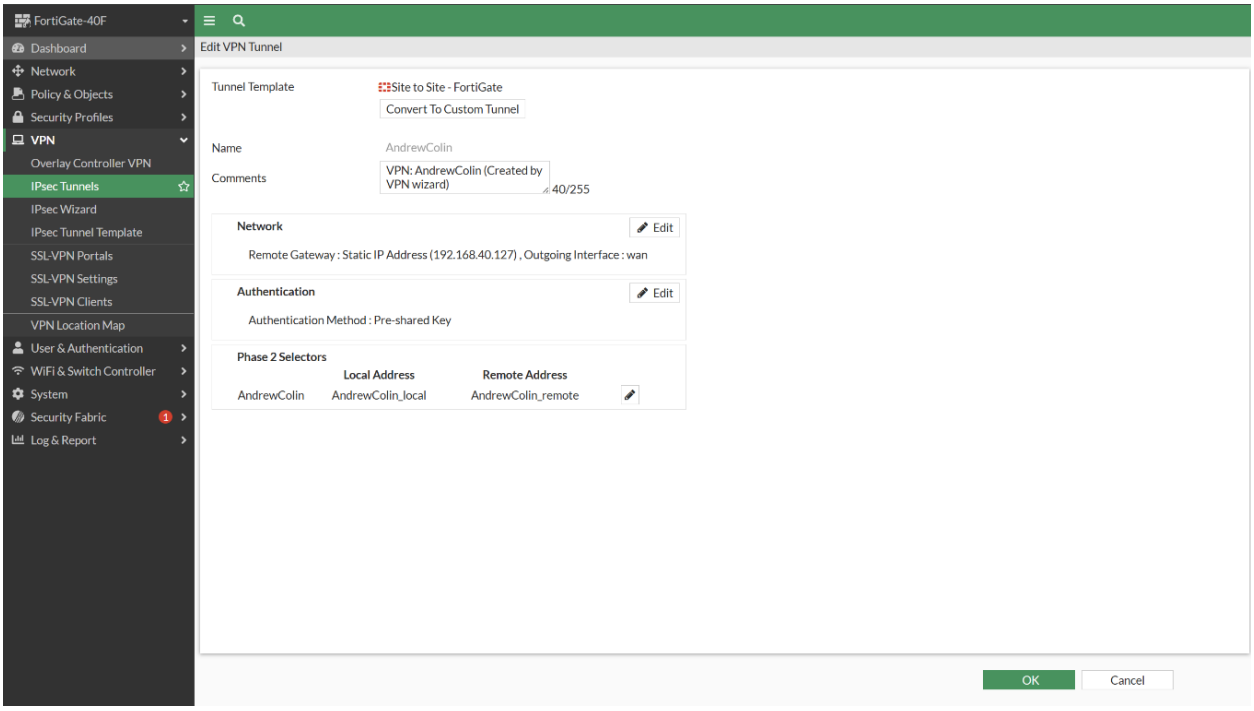
This lab focuses on implementing an IPSec VPN on our Fortigate 40F firewall. As has been covered in both our previous Global Protect VPN and our SSL VPN labs, VPNs stand for Virtual Private Networks. VPNs are used to remotely connect into a network from a device that isn't physically on that network. For companies and corporations this is a large help for people that want to work from home or are on a trip abroad. For the regular person, VPNs are useful to get past location restrictions on a certain site or to get past Internet censorship. VPNs are also just in general helpful to ensure that data is encrypted and secure compared to data that isn't transferred with a VPN.

The VPN that we'll be configuring on the Fortigate firewall in this lab uses the IPSec protocol, also known as Internet Protocol Security. IPSec is used for site to site VPNs, meaning that data goes from one firewall to another firewall, hence the need for two firewalls and groups in this lab. Compared to SSL VPNs, IPSec VPNs operate at the network layer whereas SSL VPNs operate at the transport layer. IPSec VPNs can work in either tunnel or transport mode, where tunnel mode is encryption of all data including packet headers, and tunnel is encryption of just the data payload. The main 2 protocols used by IPSec to authenticate its data is the Authentication Header and Encapsulating Security Protocols (AH and ESP). AH is used for authentication while ESP is used to encrypt data.

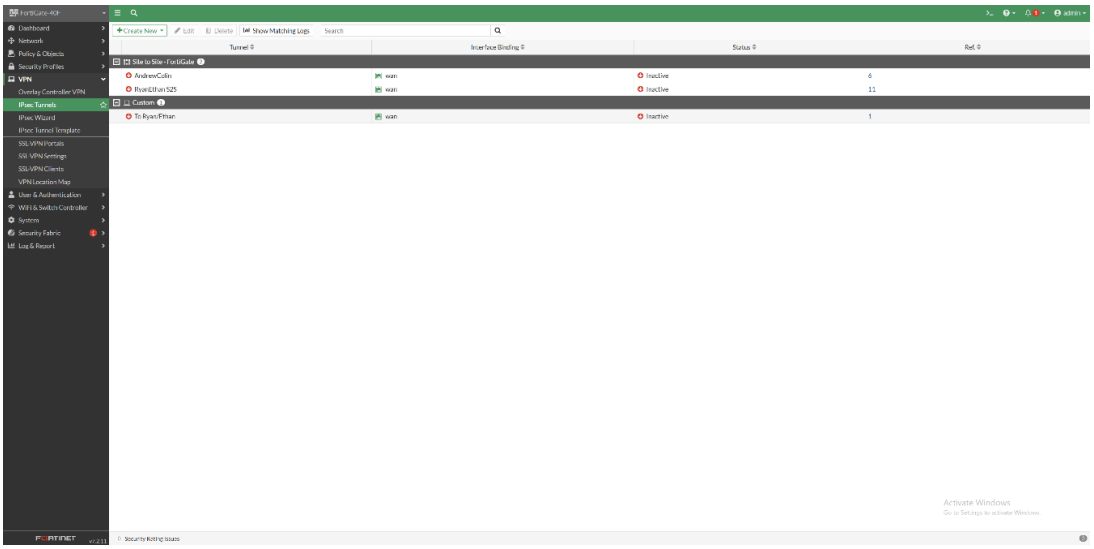
To connect to a PC on the other firewall, our group will be using Microsoft's Remote Desktop Protocol which is a Microsoft proprietary protocol meant for remote access. It uses a client-server architecture where the remote computer being accessed is the server and the user's device is the client. With a port of 3389, RDP essentially allows the user of a desktop to login and control the screen of another desktop while being able to access resources on a private network that it's not actually on.

Lab Summary:

To start configuring your IPSec VPN, navigate to the Fortigate's "IPSec Wizard" section under the VPN section of the left taskbar. Create a new Custom IPSec Tunnel with a proper name, the IP address of your other firewall, and the networks of both firewalls.



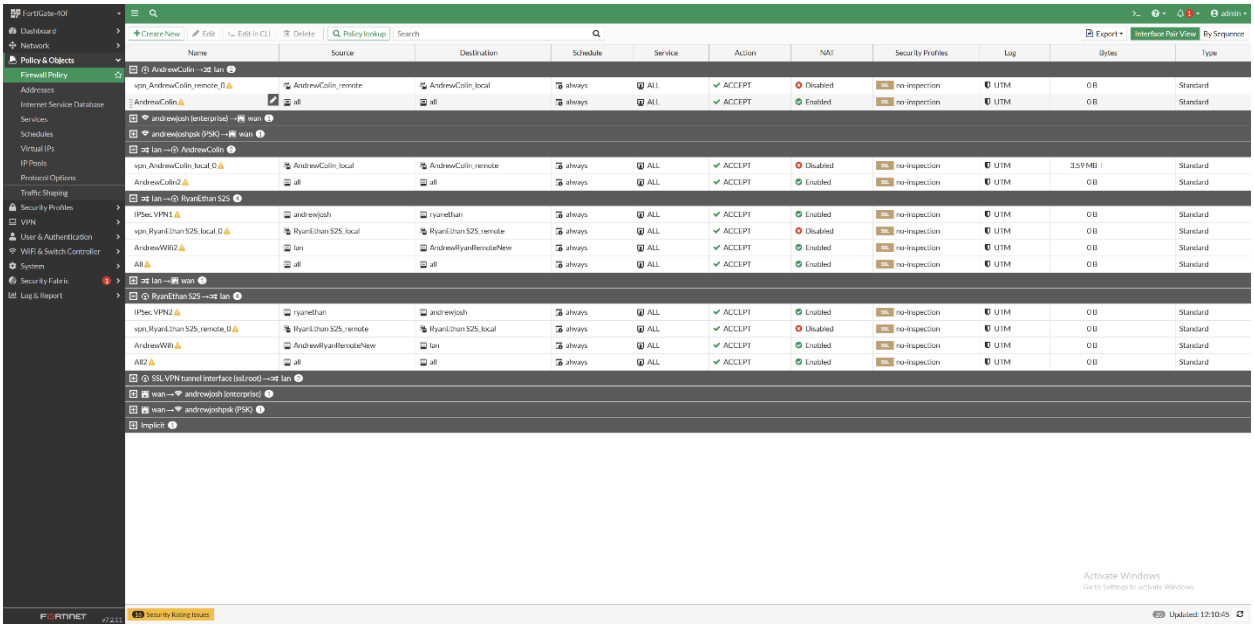
Now in IPSec Tunnels, your tunnel should show up with the proper name as "Inactive."



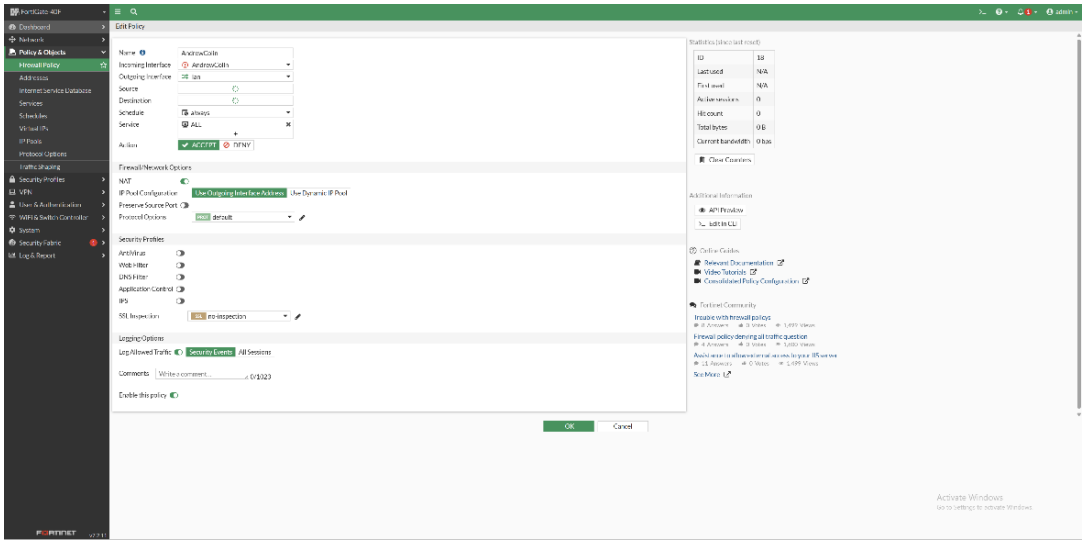
Configure a similar VPN tunnel on your opposite firewall but with reversed destination and source networks, as well as a different remote IP. Once both

tunnels are done, click on one of the tunnels and select the “bring up” option. This will cause your tunnel to come up and be active.

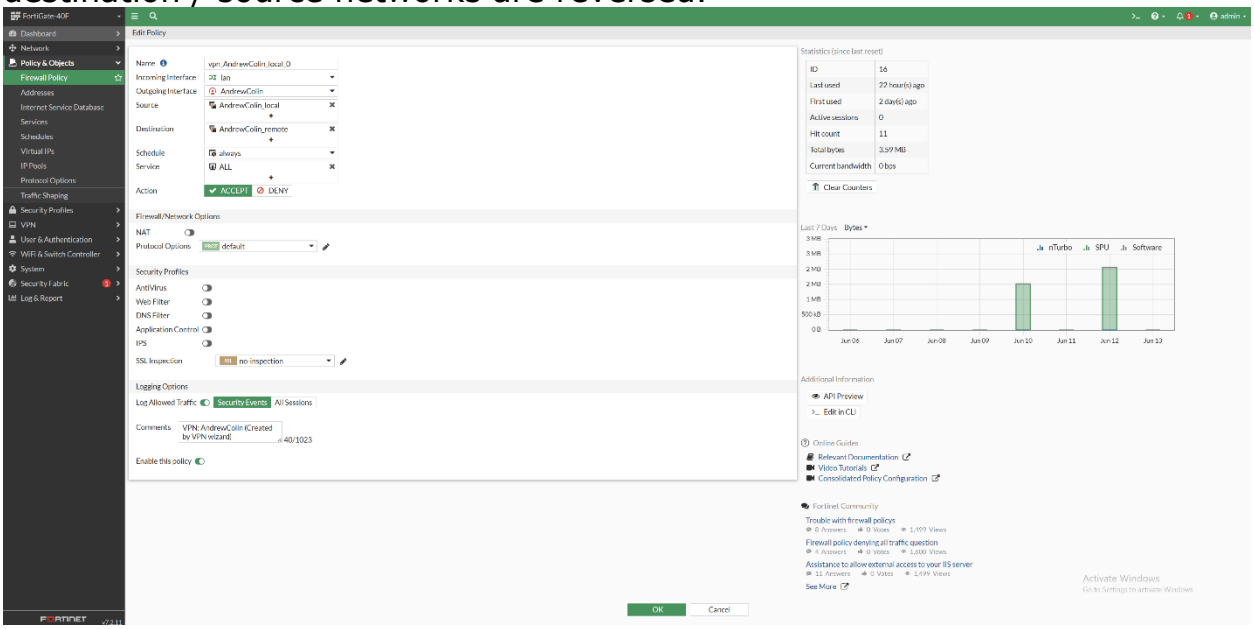
Navigate to the Firewall Policy section under “Policy and Objects” on the left taskbar.



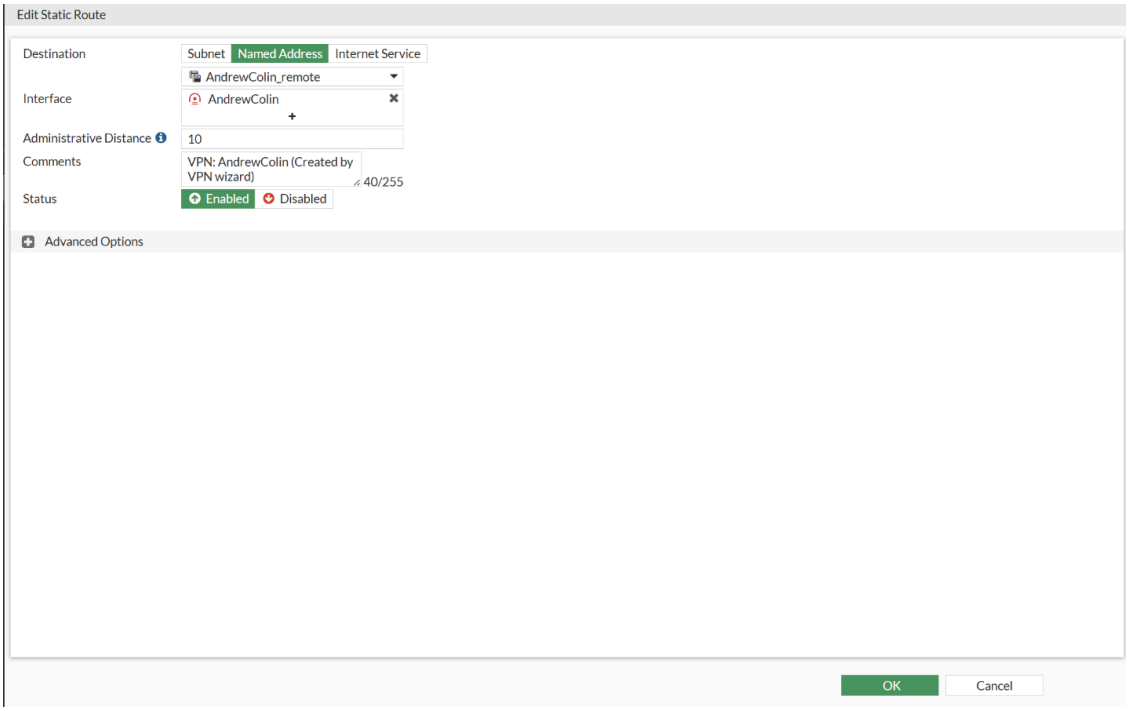
Create a new policy with the VPN Tunnel as the incoming interface, LAN as your outgoing interface, and add in the proper user groups that you want to be able to use the VPN for.

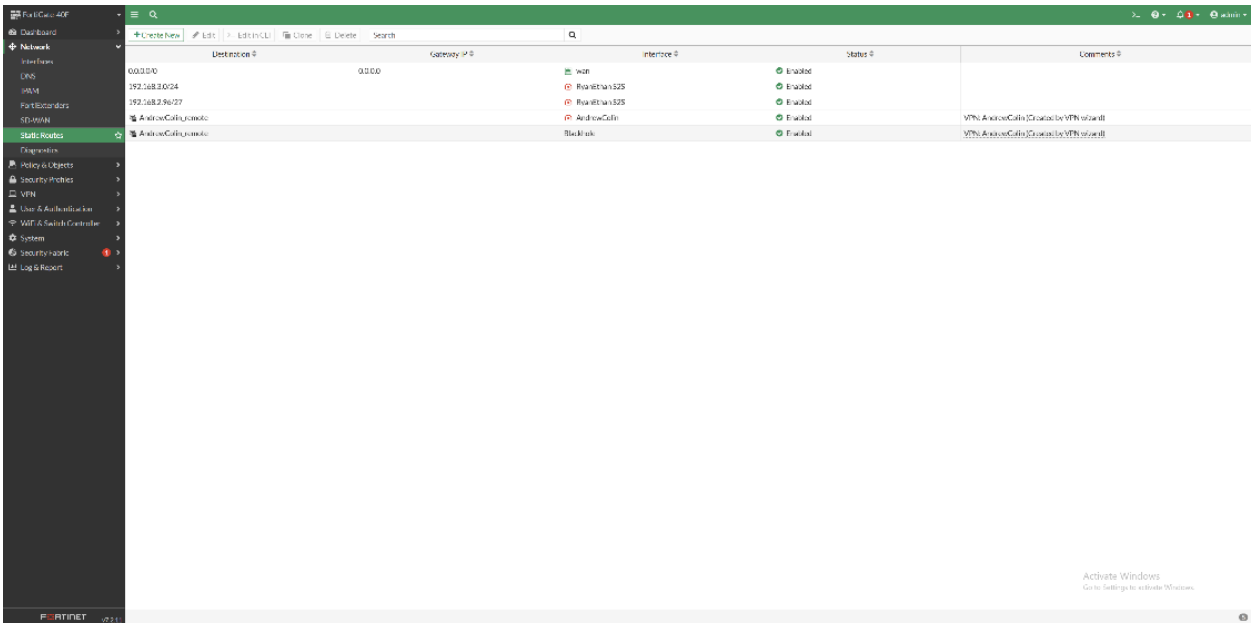


Create another similar firewall policy, but the interfaces are reversed and the destination / source networks are reversed.

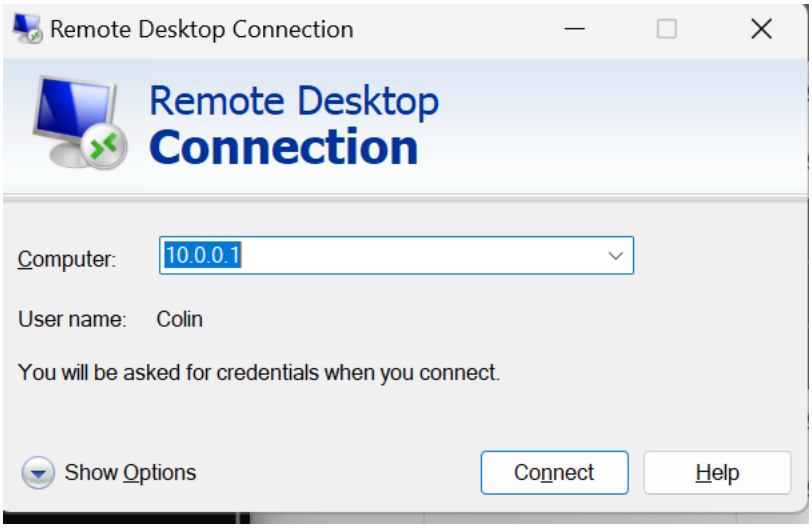


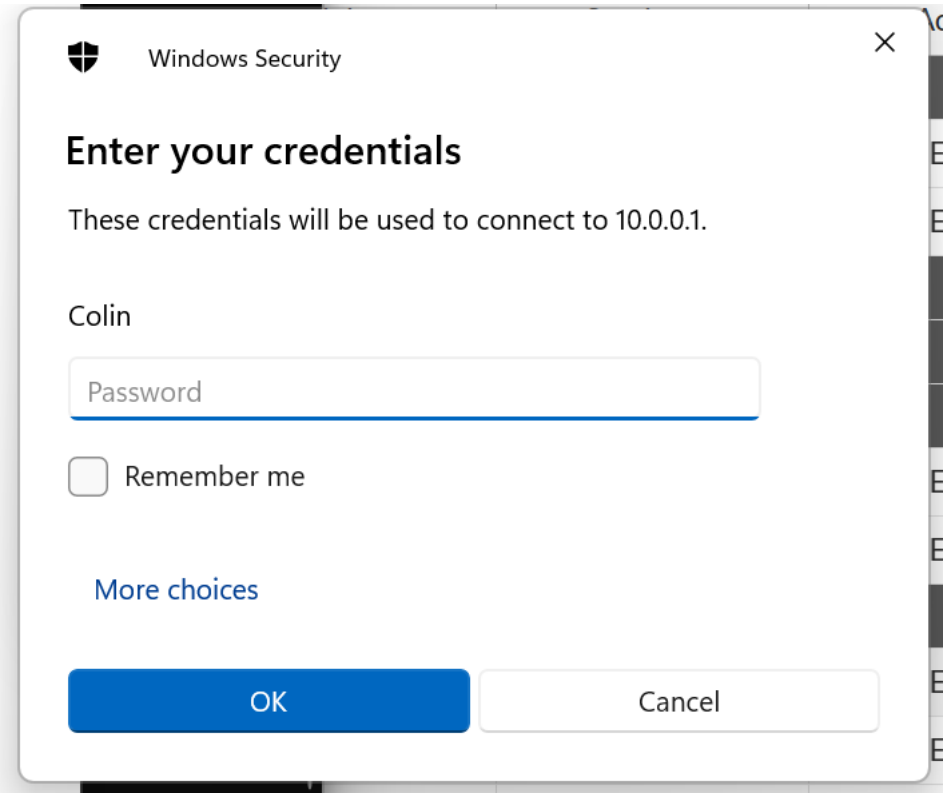
Navigate to Static Routes under the Network section on the left taskbar. Add in a static route that points any traffic going to your other firewall's network towards the VPN tunnel you configured.



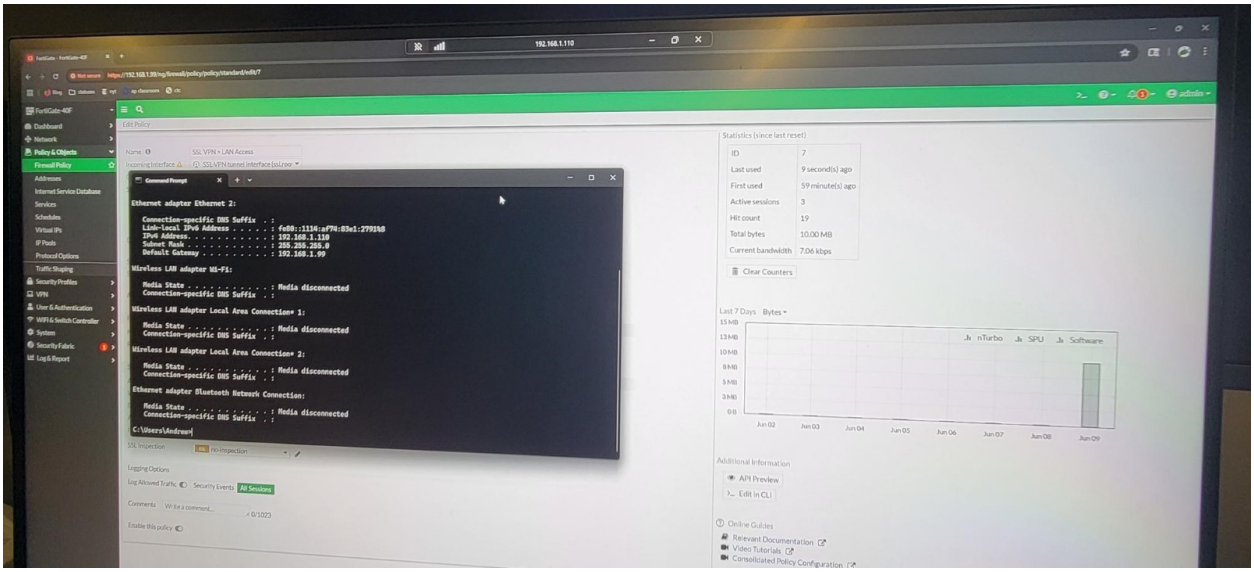


Exit out of the firewall's GUI and open RDP on your device. Type in the IP address of the computer you're trying to access on the other firewall's network and enter user credentials.





Once you enter your credentials, you should be able to access the other computer through RDP.



Problems:

One of the problems that our group had was that our VPN wasn't working with Ryan and Ethan's group's firewall. Despite being able to ping each other's firewalls, our PCs couldn't ping each other even if we allowed all traffic through. This meant that the VPN couldn't work. To solve this, I set up site to site with Colin's firewall instead.

We also had the same problem as last lab where we forgot to DHCP our PC and had a static IP, meaning no default gateway. We caught it much earlier on this time around though, leading to us simply setting our PC's IP to be from a DHCP server and working.

Conclusion:

In conclusion, this lab has familiarized our group with creating and setting up an IPSec VPN. We gained skills relating to how to set up firewall policies on the Fortigate, how to create IPSec VPN Tunnels on the Fortigate using the VPN Wizard, how to set up static routes, and how to successfully use RDP for site to site VPNs.