Portfolio

I S H A A N
M A K A M

2024-2025

CYBERSECURITY

Cybersecurity Portfolio

Table of Contents

Palo Alto 220 Factory Reset and Reboot

1. Purpose

The aim of this lab was to provide hands-on experience in rebooting and performing a factory reset on a Palo Alto PA 220 firewall. Knowing this is important for network administrators, especially when solving configuration issues or preparing a device for deployment. In the process of this lab, we became familiar on the basics of accessing the firewall from a state where the log in credentials are unknown.

2. Background Information on Lab Concepts

Palo Alto Networks is based in Santa Clara, California, and is a well-established leader in the field of cybersecurity. This company creates top of the line firewalls that have many features like traffic monitoring, threat prevention, and application-level filtering. Palo Alto Networks claims to be a 10x Network Security Leader with over 70,000 customers and growing. In business for 30 years, Palo Alto Networks are starting to use machine learning and artificial intelligence to make the security even stronger. In this lab, we worked with the PA 220, a compact firewall designed for small businesses or SOHOs .

The PA 220 has several exterior components:

- MGT (Management) Port: Used for administrative purposes, this port allows access to the firewall's interface for management security and system configs.
- Console Port: This port enables direct access to the firewall and is frequently used for consoling in with a PC.
- USB & Micro-USB Ports: These ports are used for system recovery, updates, or backups.
- 8 Ethernet Ports: These ports connect the firewall to both internal and external networks, allowing traffic to be filtered and routed.
- Power Inputs 1 & 2: The device has two power inputs, ensuring that if one goes down, there is another.

Physical firewalls like the PA 220 provide several advantages over cloud-based solutions. First, they give administrators full control over the network's security configurations. Second, they ensure reliability by operating locally without depending on anything outside of physical, thus reducing latency and potential points of failure. Finally, they help maintain data privacy, as sensitive data remains within the organization's infrastructure rather than passing through online.

In this lab, we accessed the PA 220 through its console port using an RJ45 Console Cable. This allowed us to enter maintenance mode and perform a factory reset, which is needed to remove all existing configurations and have a fresh start.

3. Lab Summary

The steps to perform a factory reset and reboot of the PA 220 were straightforward but required precise timing. The process began by connecting to the firewall using the console port. I used a console RJ45 cable to establish the connection on my laptop via PuTTY.

Here's what I did next:

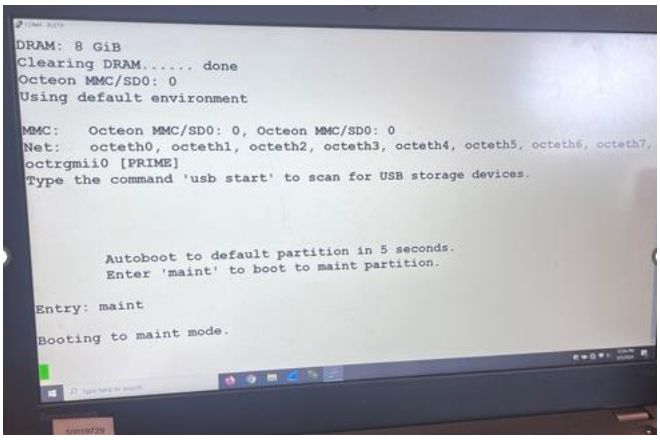
- After rebooting the firewall, I interrupted the boot sequence within 5 seconds by typing maint at the prompt. This timing was weird because missing the 5-second window would result in the firewall booting in the default setup, which would require starting the process over.
- Once in maintenance mode, I navigated through the menu using the arrow keys to select the Factory Reset option. This is where Mr. Mason checked our work and approved.
- I confirmed the reset, which wiped all previous configurations and returned the firewall to its factory settings.
- After completing the reset, I logged in with the default information which is admin for username and admin for password.

The reset was successful, restoring the firewall to its original state, with all previous configurations and user data erased. I can check this using show config.

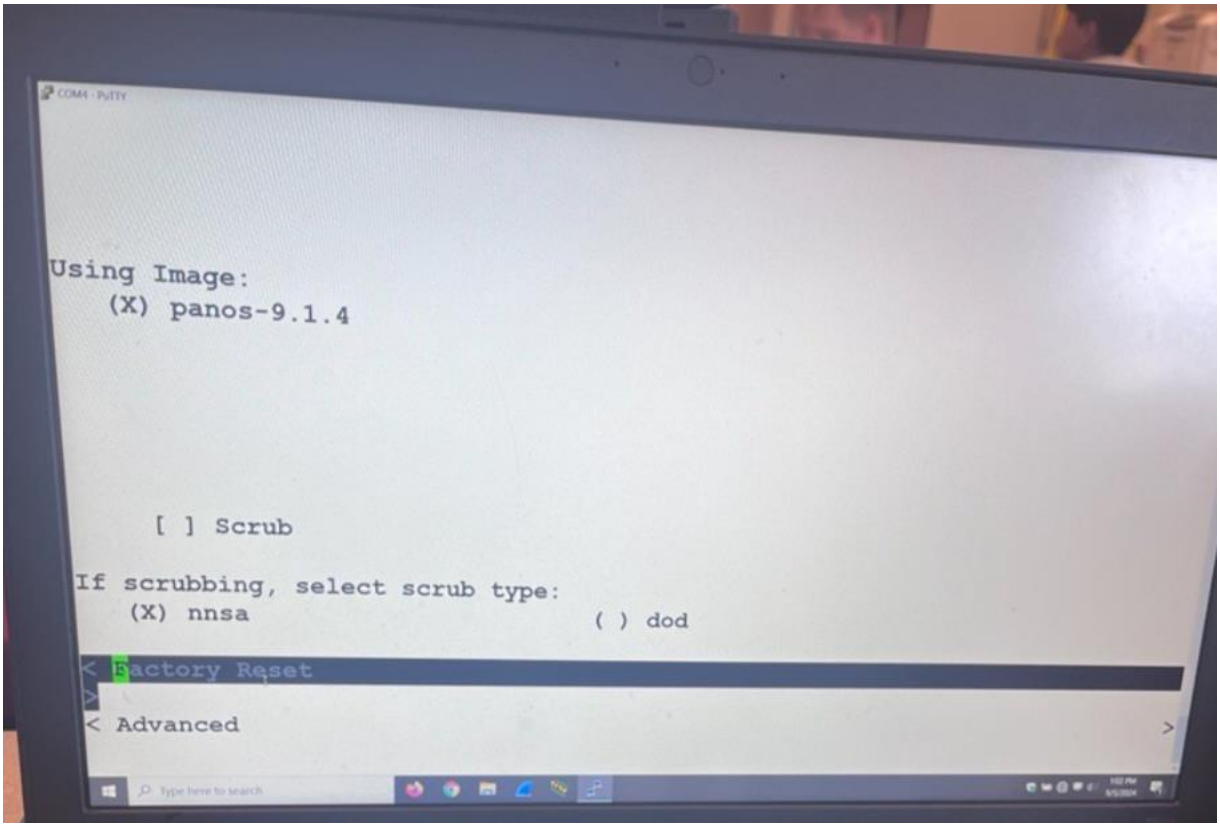
4. Lab Commands

Several commands and actions were essential during this lab:

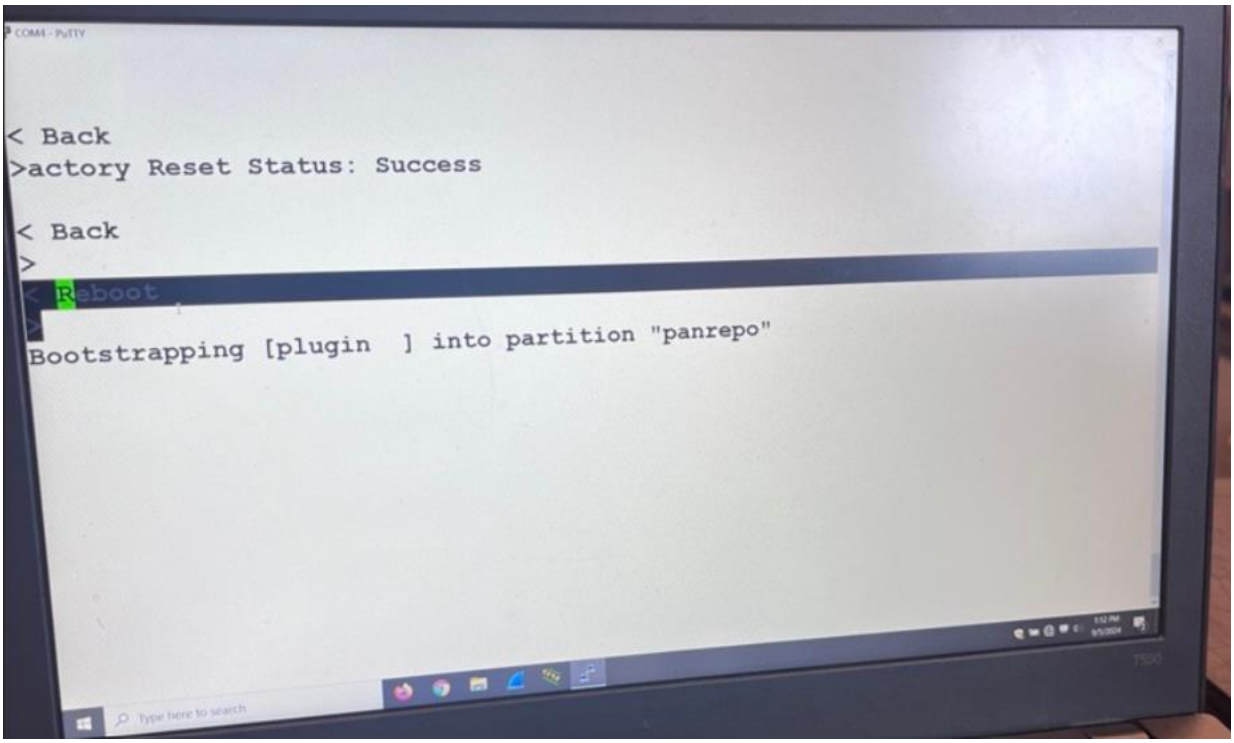
- Access Maintenance Mode: After rebooting, I interrupted the boot process by typing maint within the first 5 seconds.

- 

- Factory Reset: Once in maintenance mode, I used the arrow keys to select the Factory Reset option and initiated the process by pressing Enter.



- Reboot: After the factory reset, I navigated with arrow keys and I rebooted the system.

- 

- Check Configurations: Finally, I ran show commands to verify that the firewall had reverted to its default configuration, confirming that all previous settings had been wiped.

5. Problems

We faced a couple of issues during the lab:

1. Connectivity Issue: First, we had trouble turning on the firewall because we had the wrong cables. After some troubleshooting, we realized the issue was due to the power cable not being properly inserted and a missing adaptor. Once the power was fully connected, we were able to establish communication with the firewall.
2. Timing to Enter Maintenance Mode: Entering maintenance mode was tricky because we had only a 5-second window to type maint during the boot sequence. Missing this window required restarting the firewall, which delayed the process since we had to wait for the device to fully boot before trying again. Restarting the process was so tedious.

6. Conclusion

This lab provided valuable experience in resetting and rebooting a physical firewall, which is a critical task for network administrators. In the CCNA class, this is similar because we had to factory reset a router in case, we did not know the passwords for config T. By following the steps to access maintenance mode through the console port and performing a factory reset, I learned how to restore a device to its default settings, a key skill for troubleshooting and preparing hardware for redeployment. The challenges we encountered, particularly with connectivity and timing, show how important each step is when working with network security equipment. Overall, this lab was engaging and a good start for the cybersecurity class showing how even basic steps can require a whole lab and multiple errors.

Palo Alto 220 Firewall SOHO Configuration

1. Purpose

The aim of this lab was to provide hands-on experience in configuring and setting up the GUI for the Palo Alto PA 220 firewall. Knowing this is important for network administrators when they are implementing security in a network. In the process of this lab, we became familiar with all 30 steps including security zones, applying them to interfaces, DHCP for the firewall, and so much more.

2. Background Information on Lab Concepts

Palo Alto Networks is based in Santa Clara, California, and is a well-established leader in the field of cybersecurity. This company creates top of the line firewalls that have many features like traffic monitoring, threat prevention, and application-level filtering. Palo Alto Networks claims to be a 10x Network Security Leader with over 70,000 customers and growing. In business for 30 years, Palo Alto Networks are starting to use machine learning and artificial intelligence to make the security even stronger. In this lab, we worked with the PA 220, a compact firewall designed for small businesses or SOHOs .

The PA 220 has several exterior components:

- MGT (Management) Port: Used for administrative purposes, this port allows access to the firewall's interface for management security and system configs.
- Console Port: This port enables direct access to the firewall and is frequently used for consoling in with a PC.
- USB & Micro-USB Ports: These ports are used for system recovery, updates, or backups.
- 8 Ethernet Ports: These ports connect the firewall to both internal and external networks, allowing traffic to be filtered and routed.
- Power Inputs 1 & 2: The device has two power inputs, ensuring that if one goes down, there is another.

Physical firewalls like the PA 220 provide several advantages over cloud-based solutions. First, they give administrators full control over the network's security configurations. Second, they ensure reliability by operating locally without depending on anything outside of physical, thus reducing latency and potential points of failure. Finally, they help maintain

data privacy, as sensitive data remains within the organization's infrastructure rather than passing through online.

In this lab, we accessed the PA 220 through its console port using an RJ45 Console Cable. This allowed us to enter maintenance mode and perform a factory reset, which is needed to remove all existing configurations and have a fresh start.

3. Lab Summary

To set up the PA 220 firewall required lots of time and a great learning curve especially working with its Web GUI the whole time. The goal of the lab was to access the internet on another host by just connecting to the firewall. This entailed having the firewall be part of DHCP, and also have security zones which connected to everything. The firewall was configured through a console cable from MGT port to host number 2 which was how the GUI connected. The ethernet ports on the firewall were connected directly connected to the ISP.

After configuring the basic cable configuration, here is what I did next in a general overview:

We began by setting the IP address of Host 2 as 192.168.1.2, and then we accessed the Web GUI by going to HTTPS://192.168.1.1 and we logged in with default credentials, admin/Cisco123. (We created new password).

To properly segment and secure network traffic, we created three security zones: Untrust-L3 for external or untrusted traffic, and then Trust-L3, for internal layer 3 traffic, and Trust-L2 for trusted Layer 2 traffic. These zones helped because they were applied in multiple steps following this. We configured ethernet 1/1 as a Layer 3 interface and connected it to the ISP and this was set to obtain an ISP dynamically using Dynamic Host Configuration Protocol (DHCP). For the internal network, ethernet 1/1-4 were configured as Layer 2 interfaces and assigned to VLANS.

Then we created a VLAN interface which served as the gateway for the internal devices with the IP: 192.168.1.254. Then the firewall served as a DHCP host to provide the PC's and other devices on the network IP addresses.

To control and secure outbound internet traffic, we created a security policy that allowed traffic from Trust-L3 zone to the Untrust-L3 zone. NAT was configured to translate internal IP's to firewall's public addresses for the internet because private IP's are not allowed on the internet. NAT stands for network address translations.

After configuring everything, we verified and committed the changes to make them active. This process saved the configuration to the firewall's running state, ensuring the changes would stay.

4. Lab Commands

Here is the password change using PuTTY on Com4:

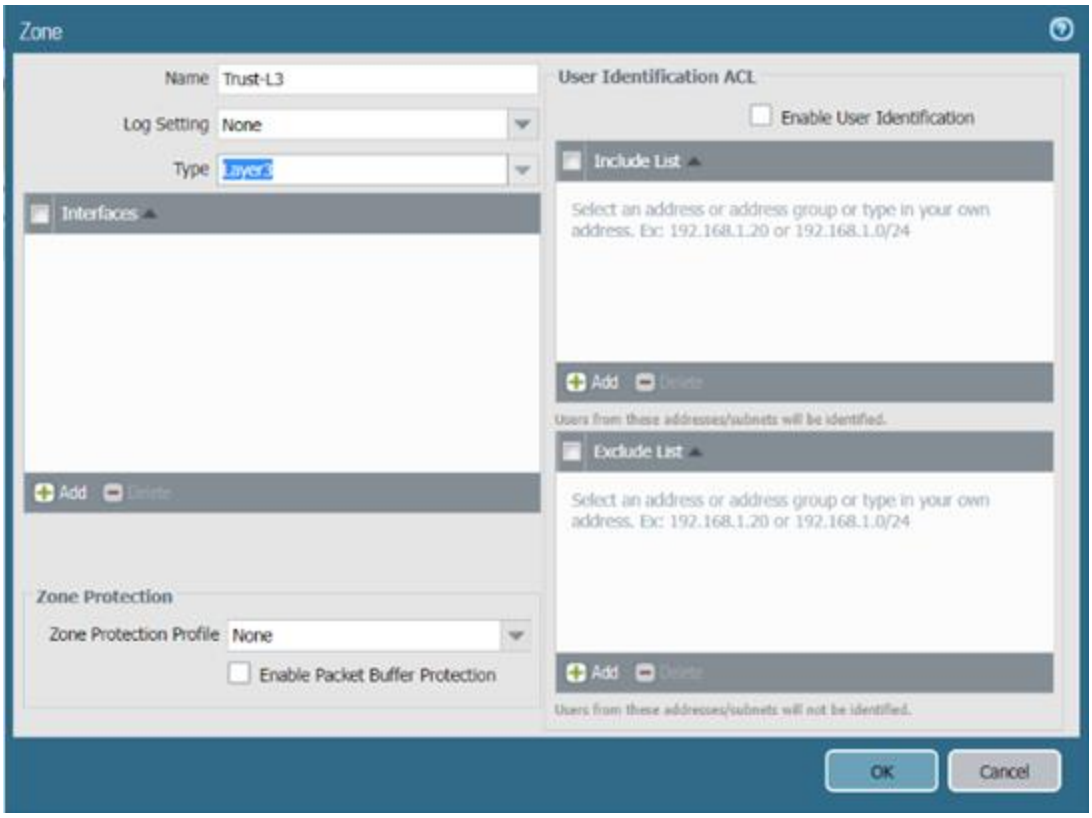
```
PA-220 login: admin
Password:
Last login: Fri Sep  6 12:08:54 on ttyS0
Enter old password :
Enter new password :
Confirm password   :
Password changed
```

This is an ARP table on Host 2:

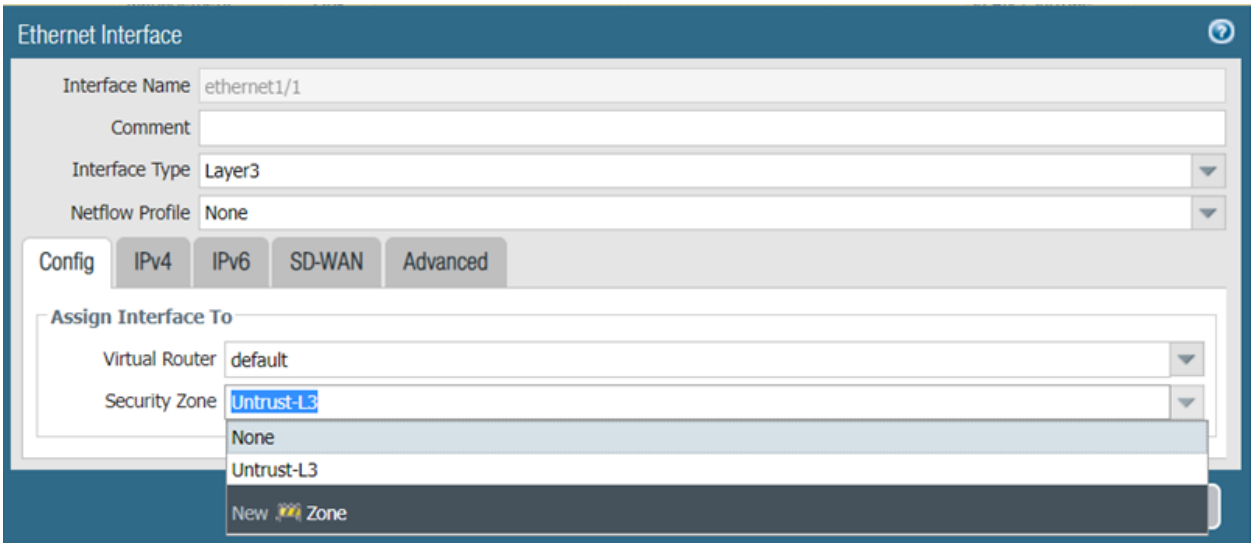
```
Microsoft Windows [Version 10.0.18362.449]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\Cisco>arp a

C:\Users\Cisco>arp -a

Interface: 169.254.30.59 --- 0xd
  Internet Address      Physical Address      Type
  169.254.255.255       ff-ff-ff-ff-ff-ff     static
  224.0.0.2             01-00-5e-00-00-02     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

Interface: 169.254.20.164 --- 0x13
  Internet Address      Physical Address      Type
  169.254.255.255       ff-ff-ff-ff-ff-ff     static
  224.0.0.2             01-00-5e-00-00-02     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

Interface: 172.28.128.230 --- 0x14
  Internet Address      Physical Address      Type
  172.28.128.1          a0-36-9f-4e-8b-2c     dynamic
  172.28.128.17         b8-ca-3a-70-ba-82     dynamic
```

This is what the login for the WebGUI is with [admin/Cisco123]:

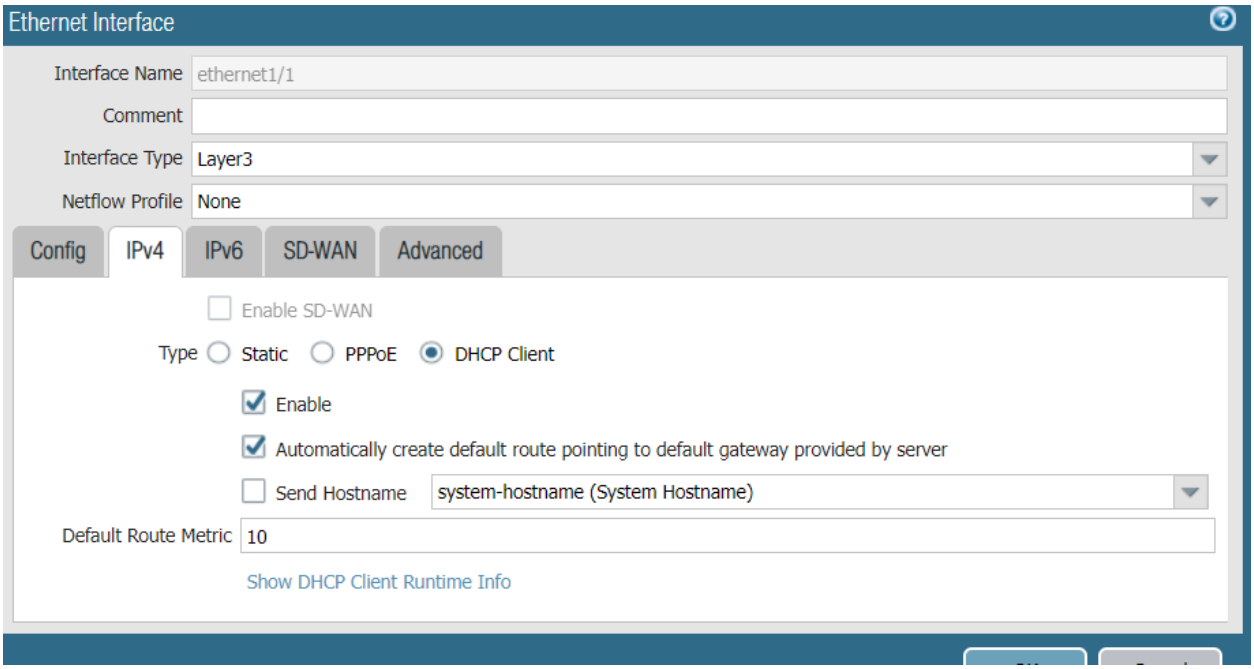
Here is a sample of how to create one of the 3 zones, this is the Trust in Layer 3:



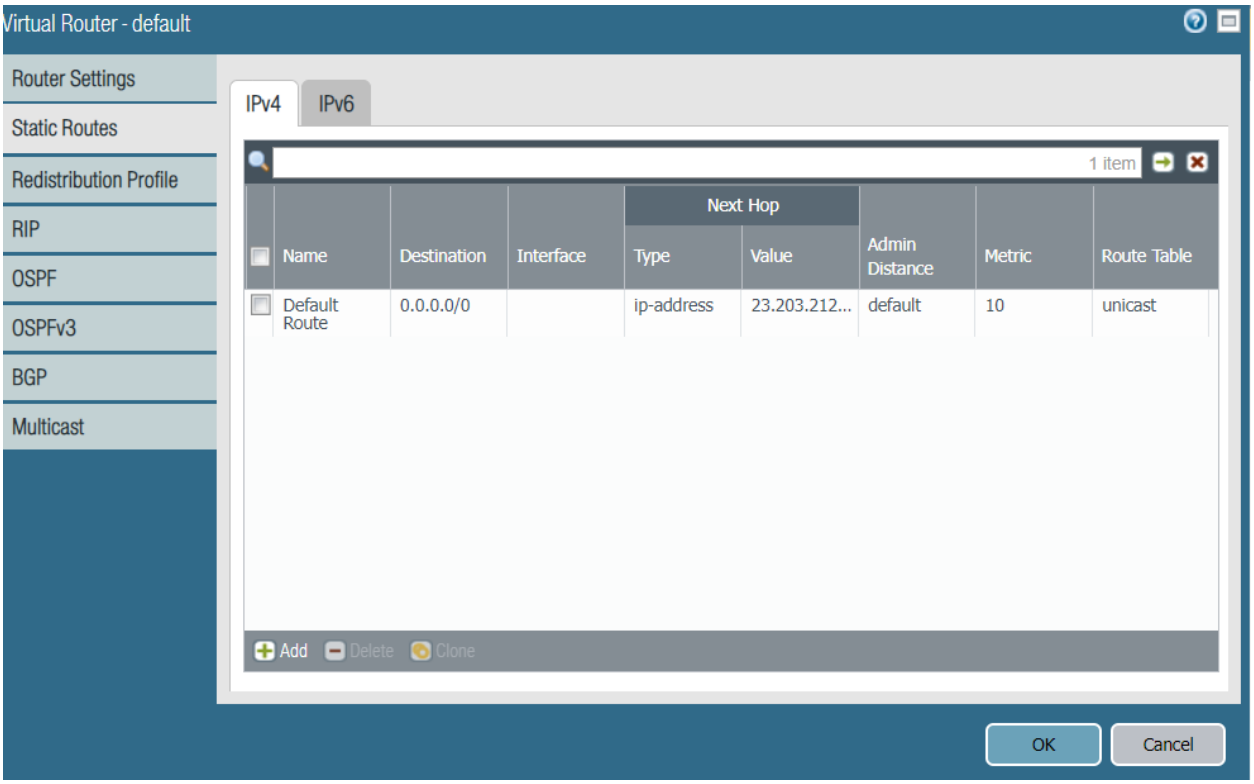
Here is applying a zone to one of the ethernet ports on the firewall:



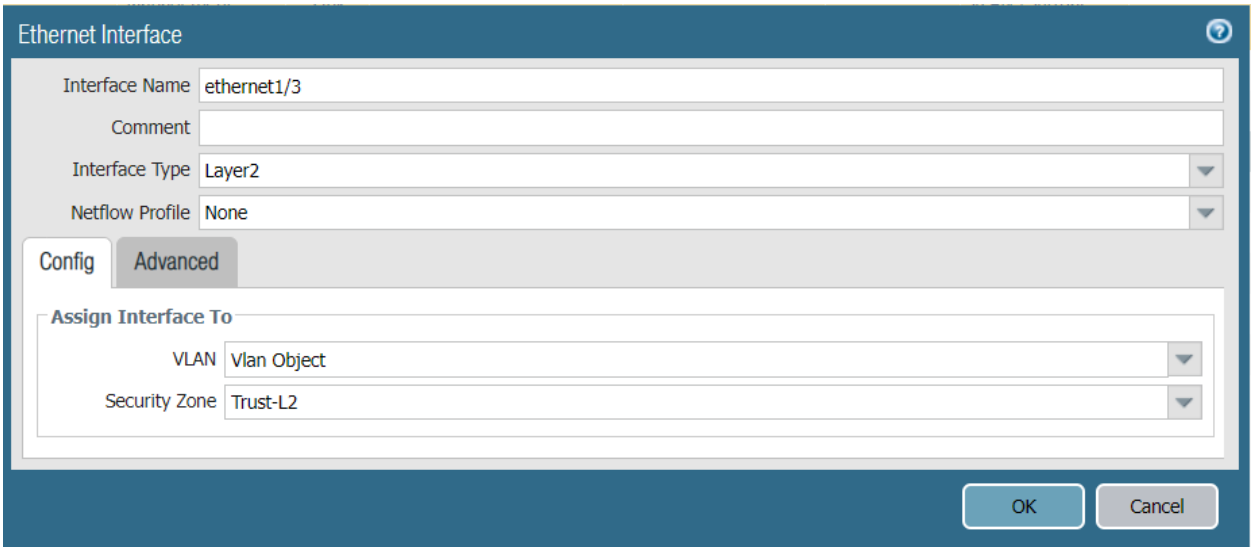
In the same configuration panel, we also made the IPV4 a DHCP client for the interface:



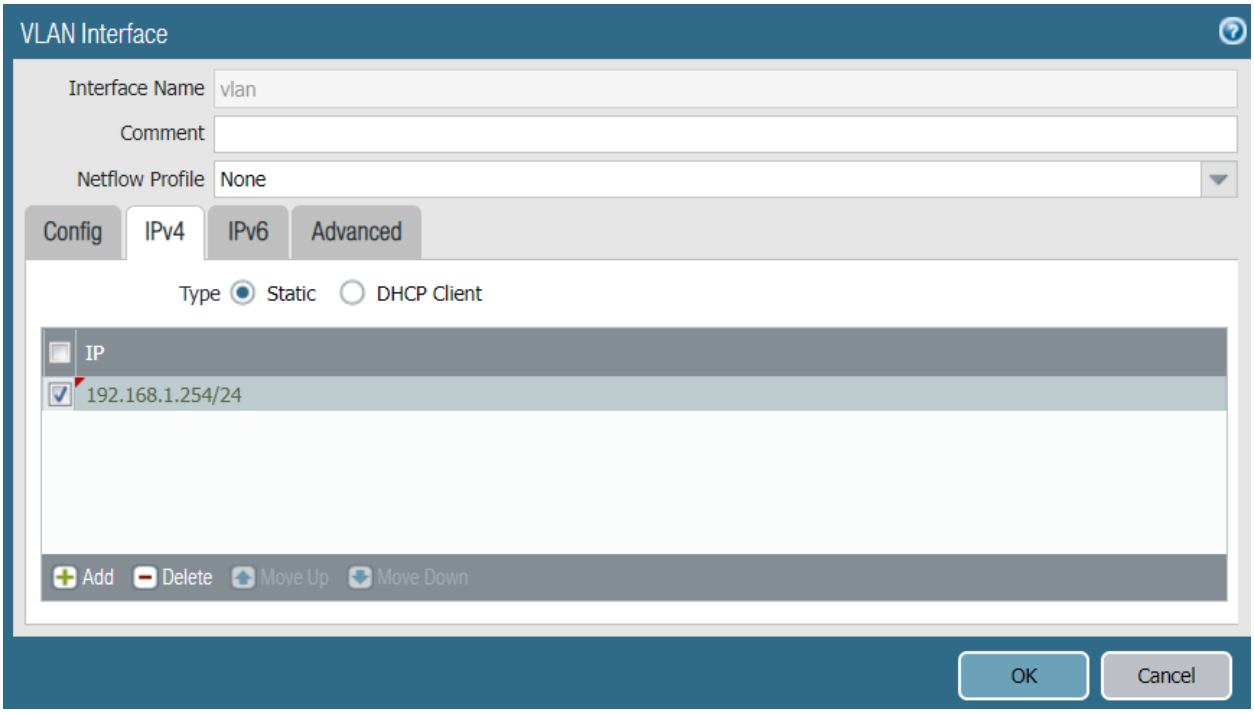
After doing that for all the interface, this is a default route pointing to the ISP next hop:



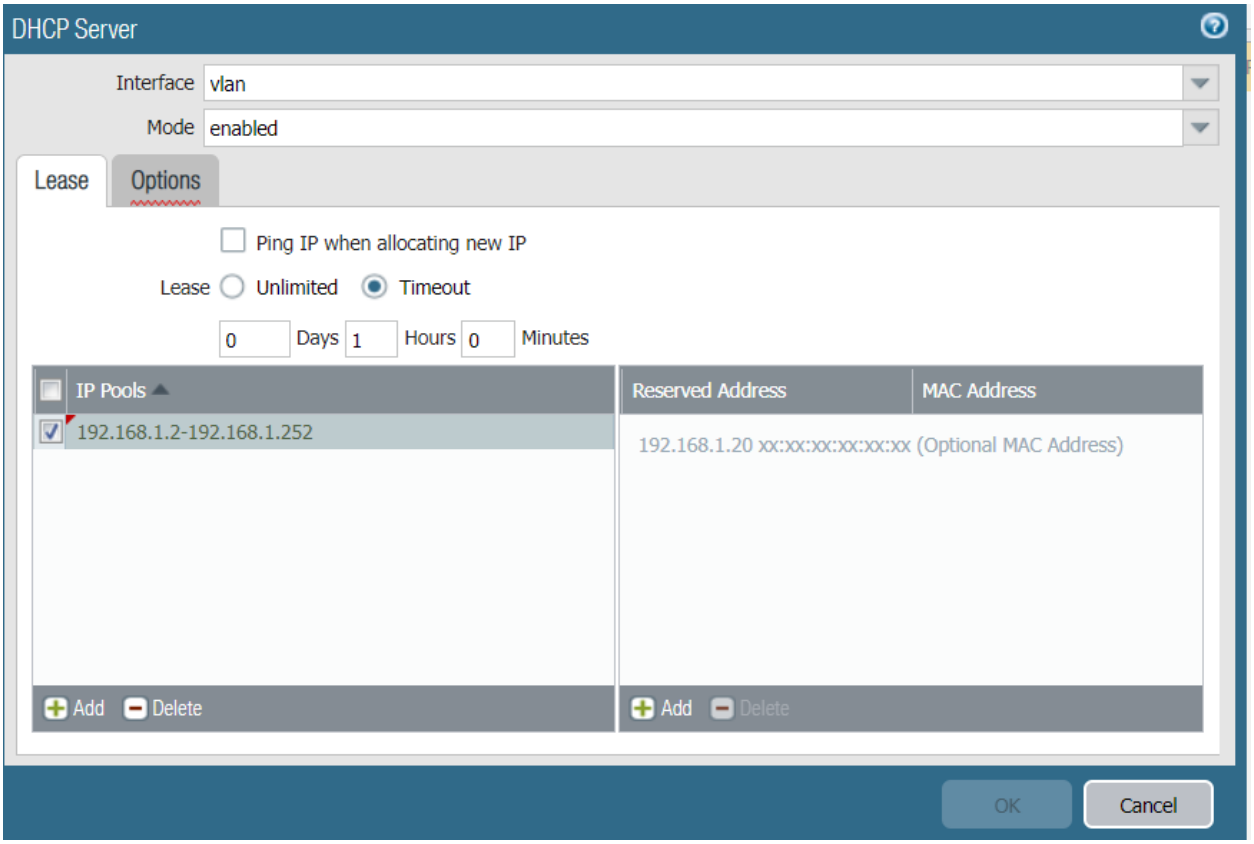
This next step was repeated 4 times for E1/1-4 with Trust L2 as security zone:



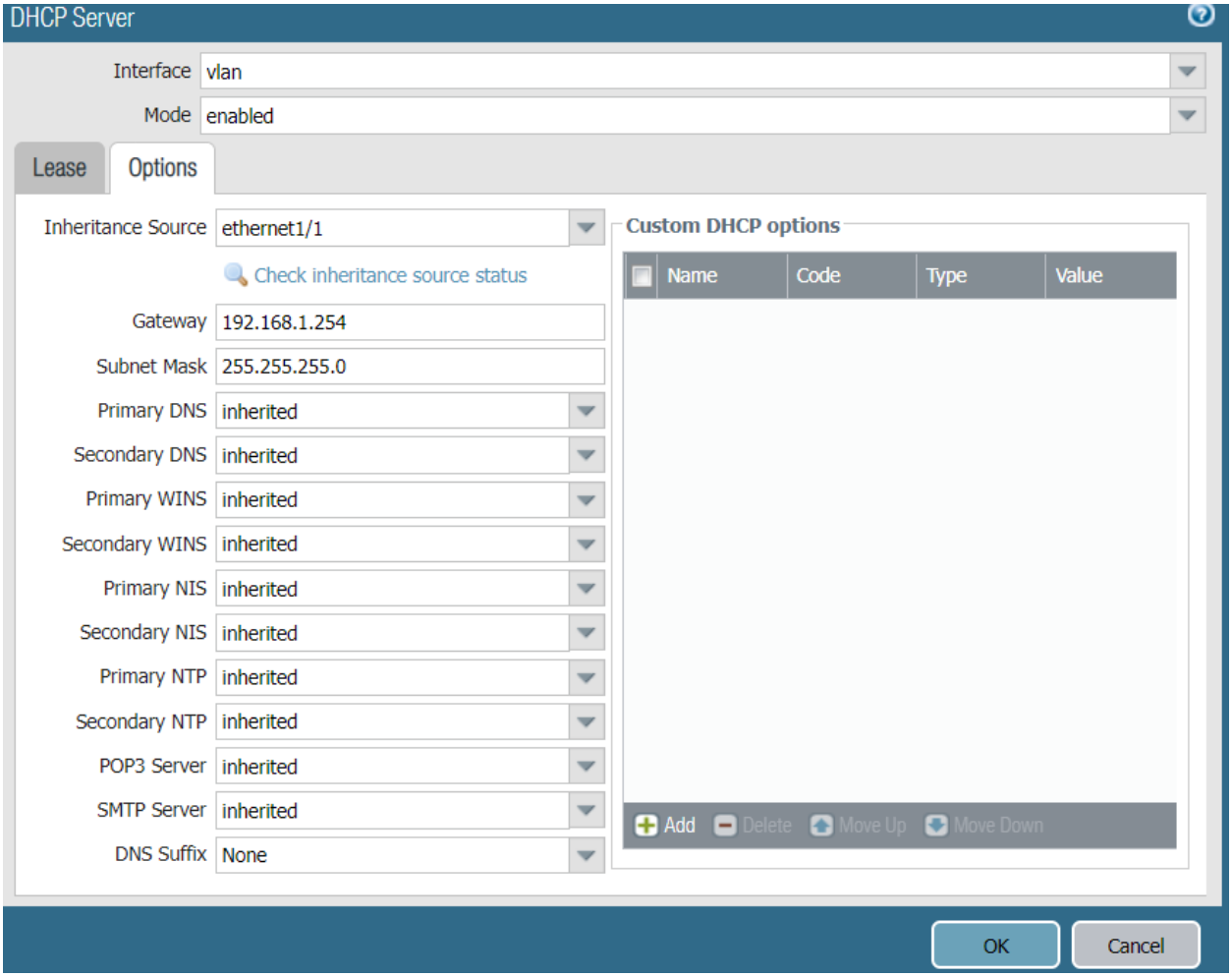
This is configuring a VLAN interface with the virtual router as default and security zone as Trust-L3 and we added the IP address for the static IP of the interface.



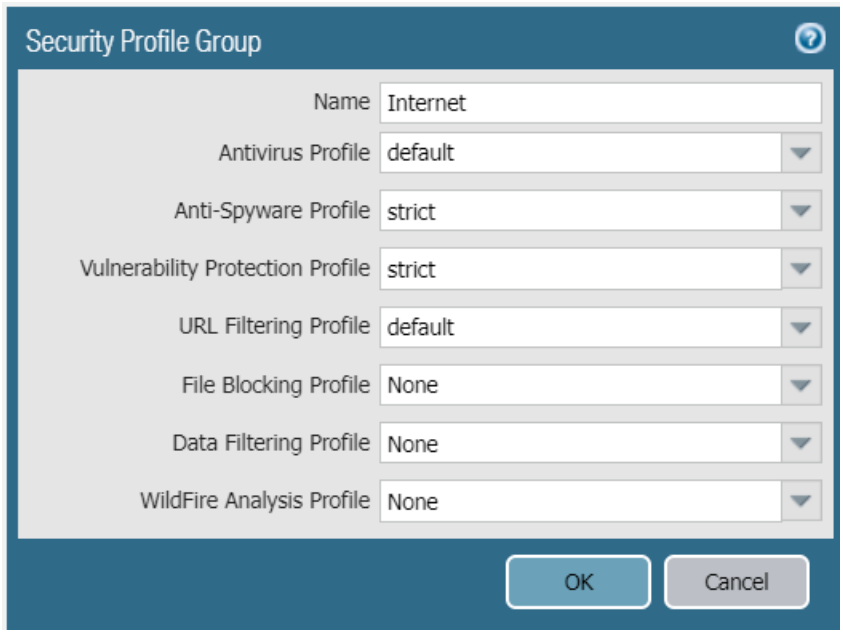
Here is one of the most crucial steps where the firewall was configured as a DHCP server for the devices on the network. In this picture, we assigned an IP address pool of private addresses. The timeout of 1 hour means the borrowed IP address will only work for 1 hour and 0 minutes.



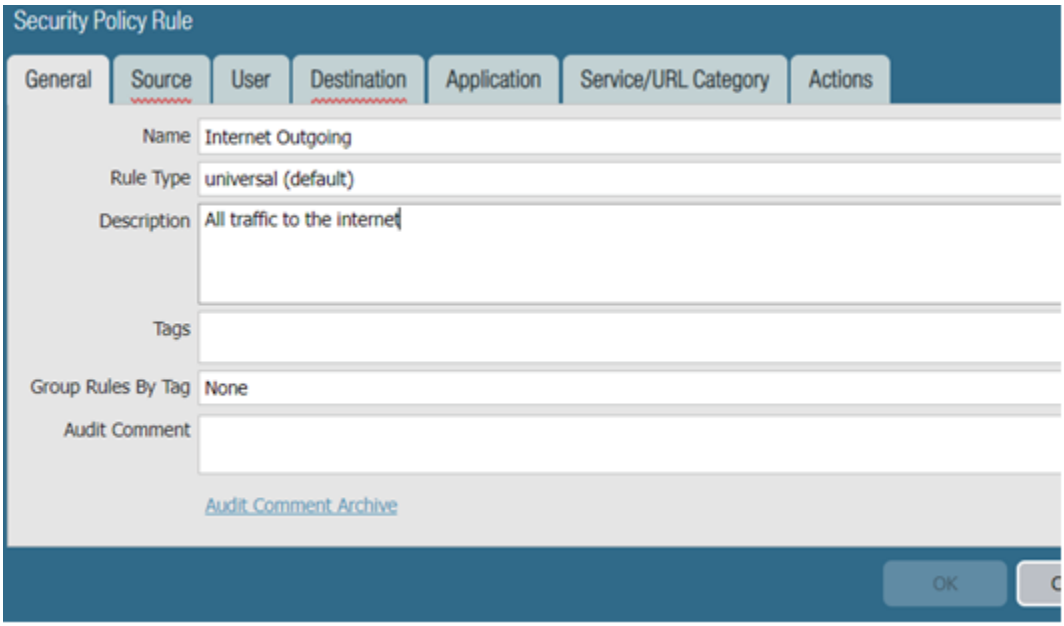
Here is additional steps when configuring DHCP for the VLAN:



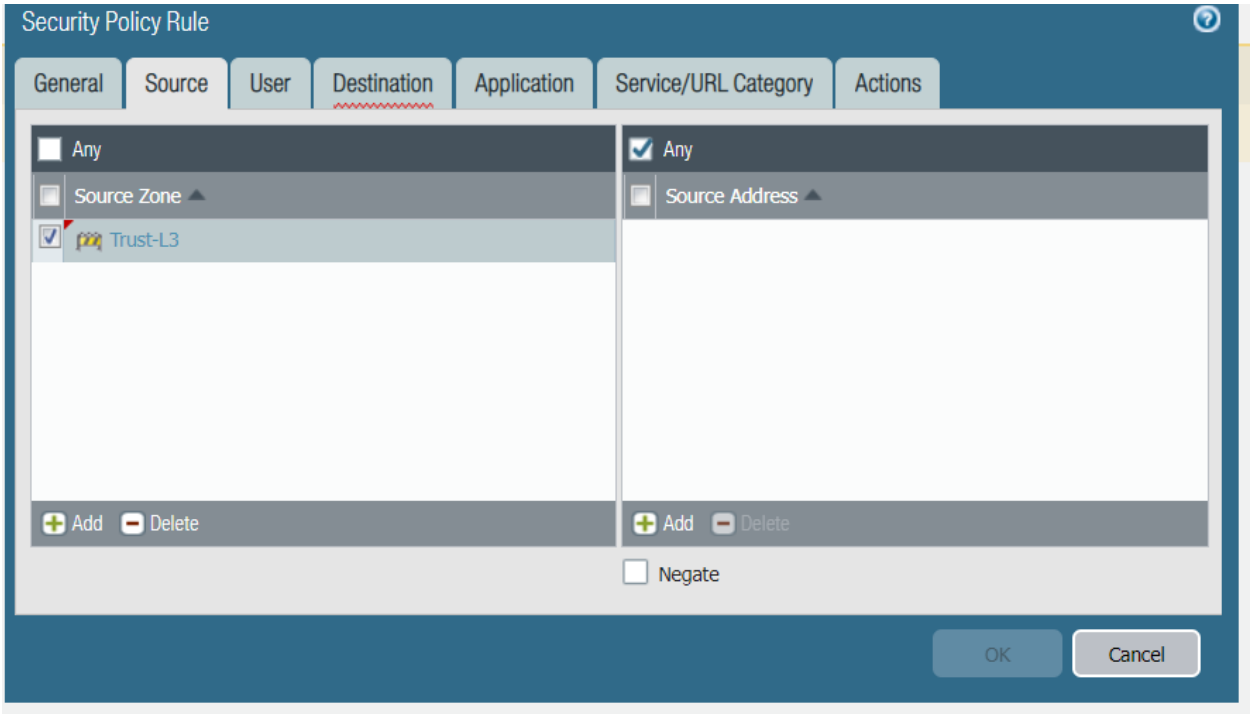
These configurations are personal preferences for the most benefit of the network:



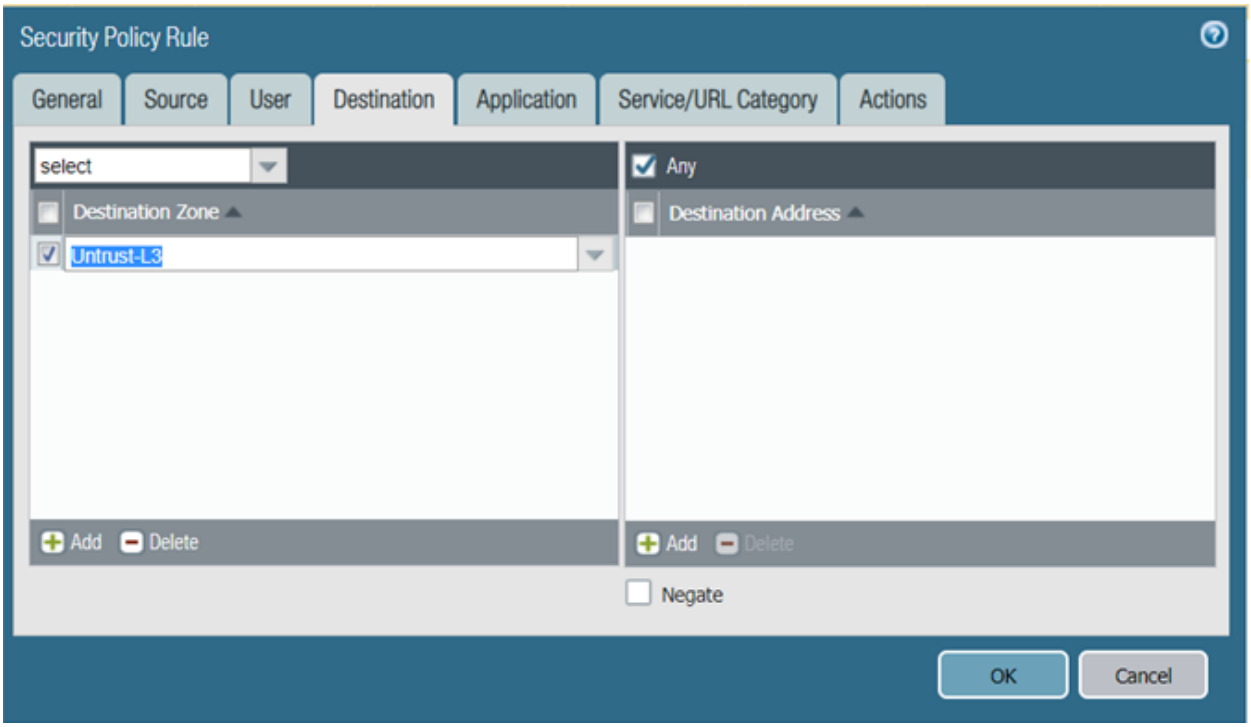
For the outbound Internet Security this is the rule for it:



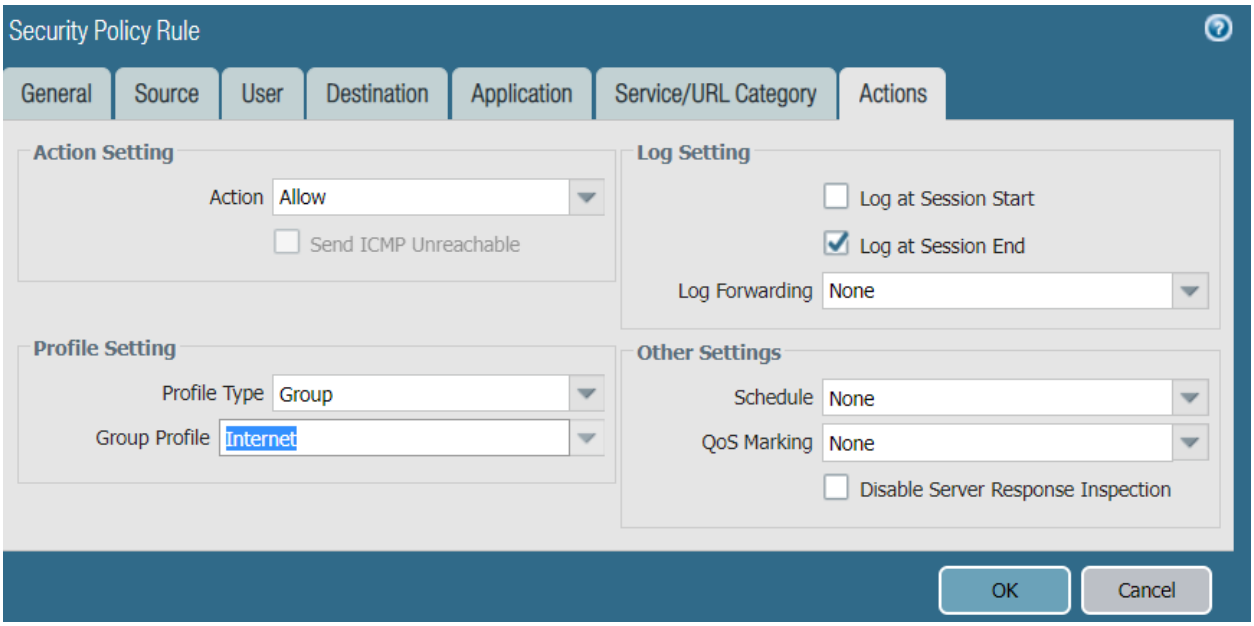
Here is the source zone so it knows that it is part of the WAN (Layer 3):



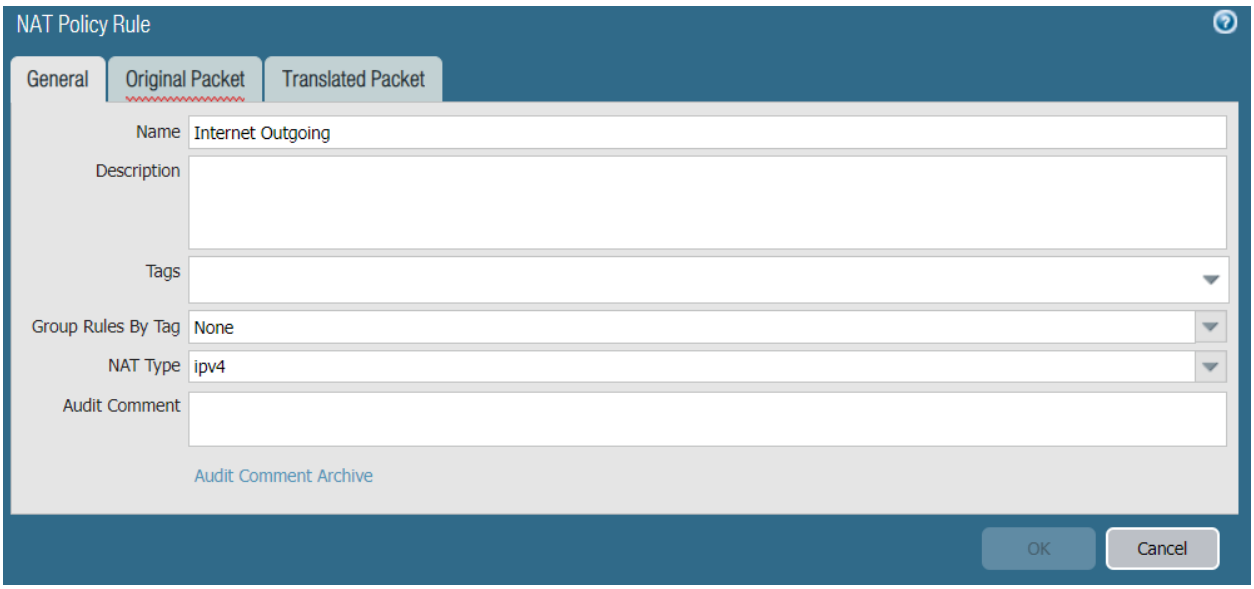
The next one is the destination for the policy. Combined, there is security on L3, and security in between Trust L3, and Untrust L3:



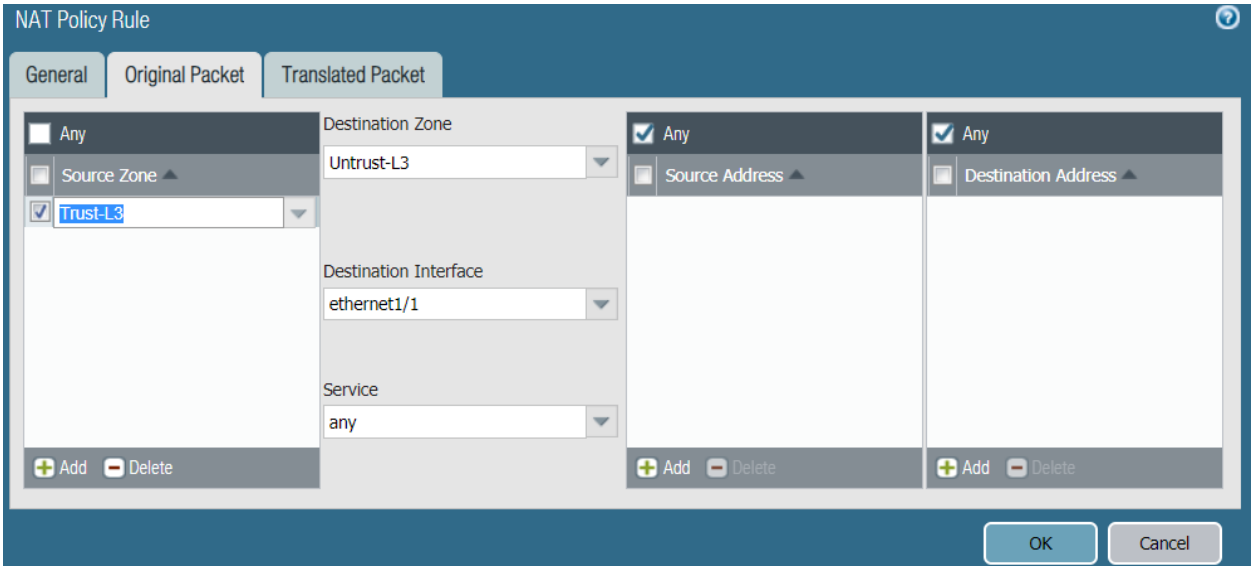
This is some of the actions for it, as you can see, we skipped over URL category which is an optional filtering method:



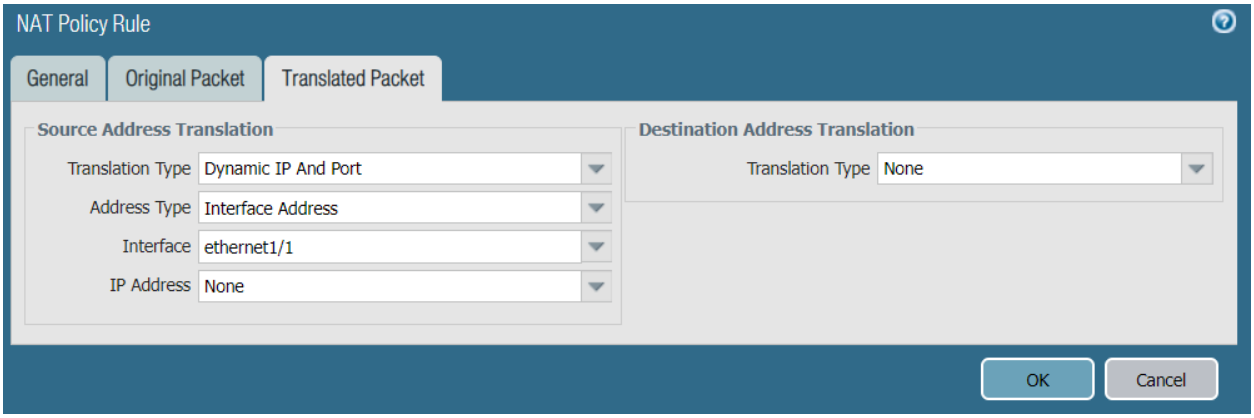
Outbound Network Address Translations for the IPV4 is for the outgoing network:



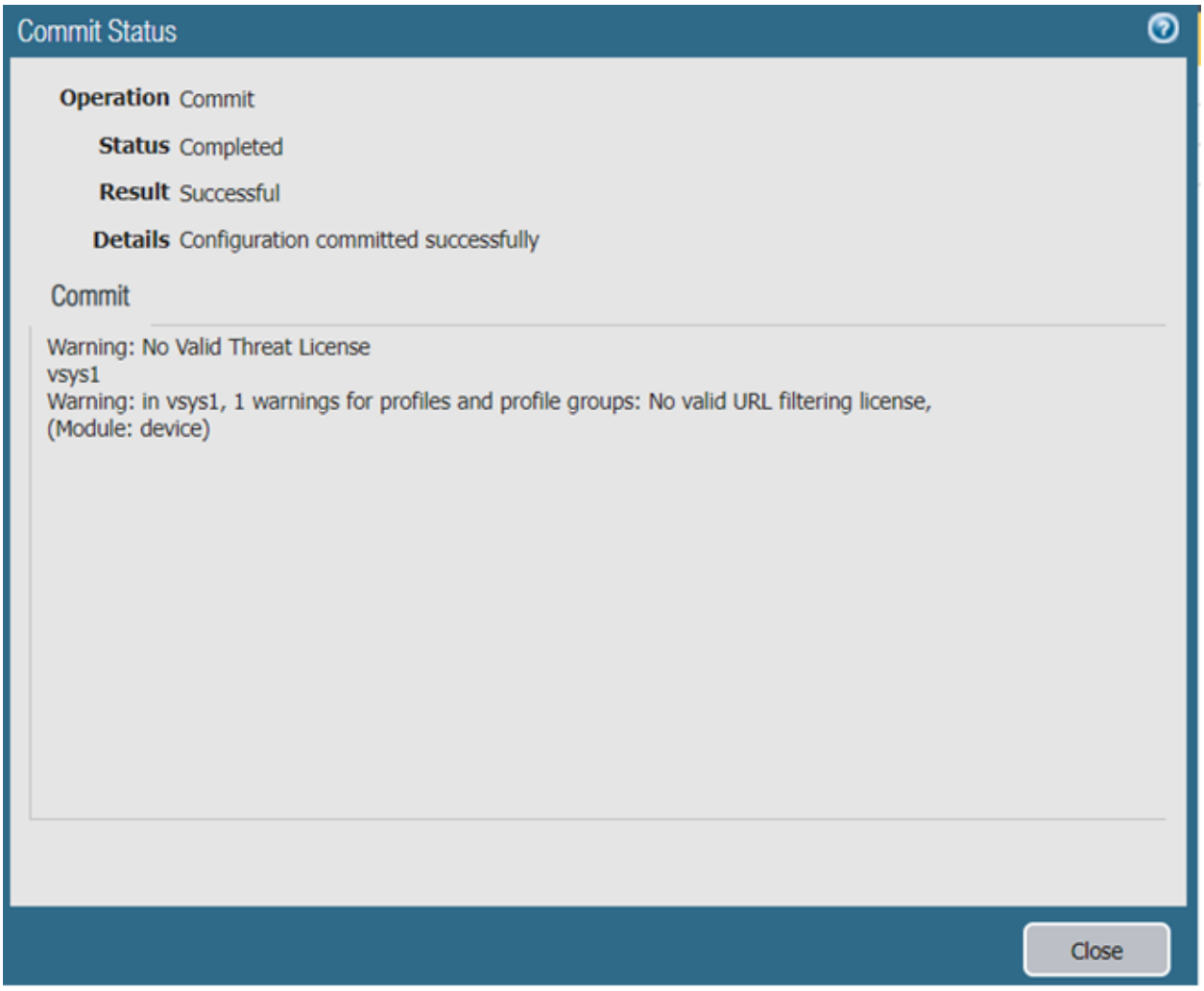
On the original packet for NAT, this is for address translated from inside to the destination of the outside which is Untrusted on the e1/1 interface. The service of any means any address on the inside can be translated from Trust L3 which is the source zone:



On the translated packet, we set translation type as IP and port which signifies the use of Port Address Translation also on ethernet 1/1 interface.



If all the steps were done 100% correctly, the commit status will return successful which means that the whole configuration was complete.



5. Problems

Due to the amount of steps for configuring the PA220 for SOHO, there were countless mistakes that we made. Firstly, the cable configuration between the ISP and hosts had to match the exact ports that were configured with the GUI, if they were different, no filtering would occur. Another error we faced is that the DNS servers that were said to be previously configured were actually not set up at all. This problem led us to go in circles countless times looking for false errors. Finally, once we went through the whole process again, we checked DNS, and we clicked enable and set it up.

6. Conclusion

Overall, throughout this lab, I learned so much throughout the entire process of how a basic firewall works. The screen shots that I collected are detailed steps of how to recreate the GUI for SOHO setup for the PA220 Firewall. Additionally, all the work I learned in CCNA

which involved OSI model layers, DHCP, DNS, and NAT all came together one hands-on assignment where the PA220 Firewall was fully configured for SOHO use.

Palo Alto 220 URL Filtering

1. Purpose

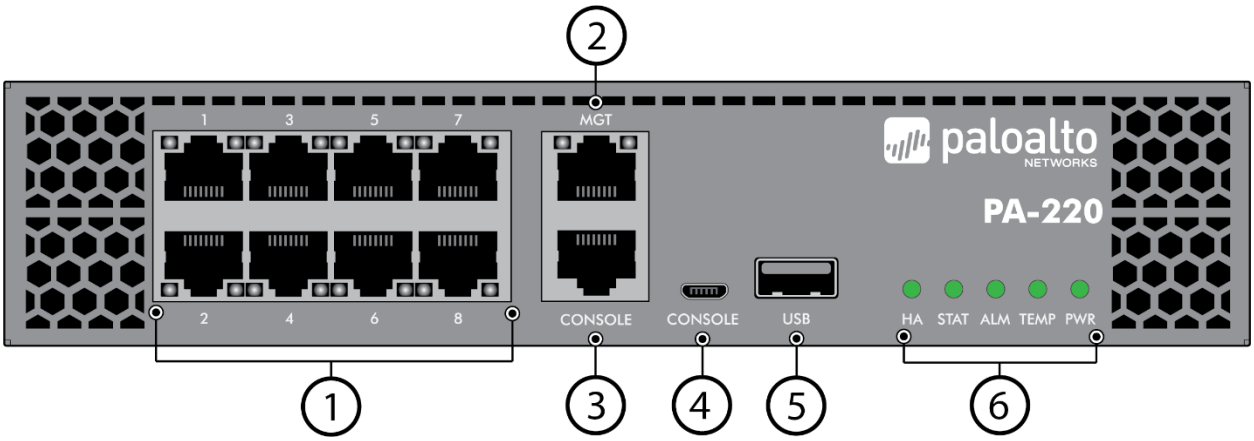
The purpose of this lab was to gain hands-on experience in configuring URL filtering and URL override features on a Palo Alto PA 220 firewall. This configuration was tailored for elementary schoolers to block inappropriate or unsafe websites while allowing an administrator to override blocks if necessary. Completing this lab provided valuable insights into managing and securing network traffic, which is a critical skill for network administrators.

2. Background Information on Lab Concepts

Palo Alto Networks is one of the most trusted names in cybersecurity, protecting over 70,000 organizations across 150 countries, including 85 of the Fortune 100 companies. Their next-generation firewalls (NGFWs) are designed to block both known and unknown cyber threats while giving administrators advanced control over network traffic. Unlike traditional firewalls that rely on ports and IP addresses, Palo Alto firewalls allow policies based on specific applications, so you can allow access to tools like YouTube but block games like Fortnite. Their global threat intelligence system ensures that if one customer encounters a new threat, all other customers are automatically updated to defend against it. In this lab, I worked with the PA 220, a compact firewall designed for small businesses or SOHOs.

The PA 220 has several exterior components, labeled on the diagram:

- **MGT (Management) Port (2)**: Used for administrative purposes, this port allows access to the firewall's interface for managing security and system configurations.
- **Console Port (3)**: This port enables direct access to the firewall and is frequently used for consoling in with a PC.
- **USB & Micro-USB Ports (4,5)**: These ports are used for system recovery, updates, or backups.
- **8 Ethernet Ports (1)**: These ports connect the firewall to both internal and external networks, allowing traffic to be filtered and routed.



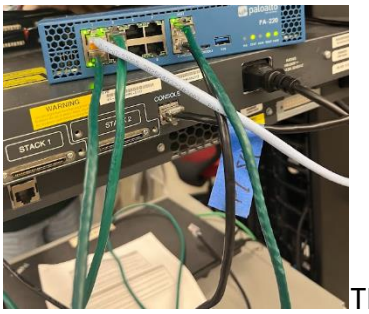
- **Power Inputs 1 & 2**: The device has two power inputs, ensuring that if one goes down, there is another.

Recently, Palo Alto firewalls were targeted in **Operation Lunar Peek**, where attackers exploited two vulnerabilities (**CVE-2024-0012** and **CVE-2024-9474**) to bypass authentication and gain admin privileges. Hackers used this access to install malware and make unauthorized changes. The attack primarily affected devices with **exposed management interfaces** on the internet. Palo Alto responded by releasing patches and recommending restricting management access to **trusted internal IPs**.

Palo Alto quickly released updates to patch the vulnerabilities and advised customers to secure the management interface by limiting access to internal, trusted IPs. They emphasized that regular updates and best practices are critical to keeping networks safe. Even with these challenges, Palo Alto firewalls remain one of the most trusted tools for protecting networks because of their ability to adapt and share real-time threat intelligence across customers.

Physical firewalls like the PA 220 provide several advantages over cloud-based solutions. First, they give administrators full control over the network's security configurations. Second, they ensure reliability by operating locally without depending on external factors, thus reducing latency and potential points of failure. Finally, they help maintain data privacy, as sensitive data remains within the organization's infrastructure rather than passing through the cloud.

3. Lab Summary



The lab began with setting up the hardware. The image shows the physical connections made on the PA 220:

- **Port 1** was connected to the internet.
- **Port 2** was connected back into the management interface to extend management functionality to other ports.
- **Port 3** and the **console port** were connected to the PC for accessing and managing the GUI.

Once the cables were connected, I configured the PC with an IP address of **192.168.1.2** and a subnet mask of **/24**. I accessed the GUI by entering https://192.168.1.1 into Firefox and logged in with the default credentials (**admin/admin**). The first step was to change the default password to **admin/Cisco123** for security purposes.

Next, I updated the firewall. This process required upgrading incrementally from version **9.0.0** to **10.2.0**, following a sequence like **9.0.0 → 9.0.9 → 9.1.0 → 9.1.9** and so on. Each update took approximately 20 minutes, making this step time-consuming but necessary for accessing the latest features.

After updating, I manually synchronized the firewall's clock with real-world time. While I didn't encounter issues here, having an accurate clock is important for update validation, log accuracy, and overall functionality.

The next step was configuring the URL filtering profile. I created a profile named **ElementaryBlocked** (Image 2) to block categories such as:

- Malware
- Phishing
- Spyware
- Adult Content
- Nudity
- Gambling

- Drugs
- Alcohol
- Games
- Shopping

I made sure these categories were set to **Block**. After this, I went to the **Policies → Security** menu to create a new security policy. I configured the policy with **any to any** source/destination settings for simplicity during testing and linked the **ElementaryBlocked** profile in the URL Filtering section.

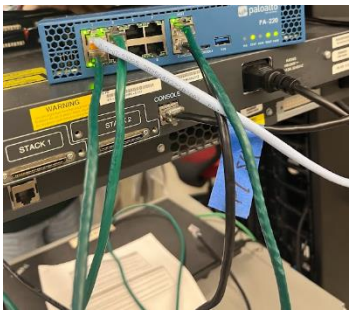
Finally, I configured the **URL Admin Override** feature under **Device → Setup → Content-ID**. I set the mode to **Transparent** and created a password that allowed administrators to override blocked content when necessary. I chose **Shopping** because when I was testing the links for the override password, **Amazon** was an easy website to use because it is defaulted unblocked whereas the majority of those filters were already pre-blocked.

To test the setup, I used Palo Alto's provided **URL filtering test link** (Image 6). When visiting a blocked page, the override password worked seamlessly without additional steps or delays, confirming that the configuration was successful.

4. Lab Commands

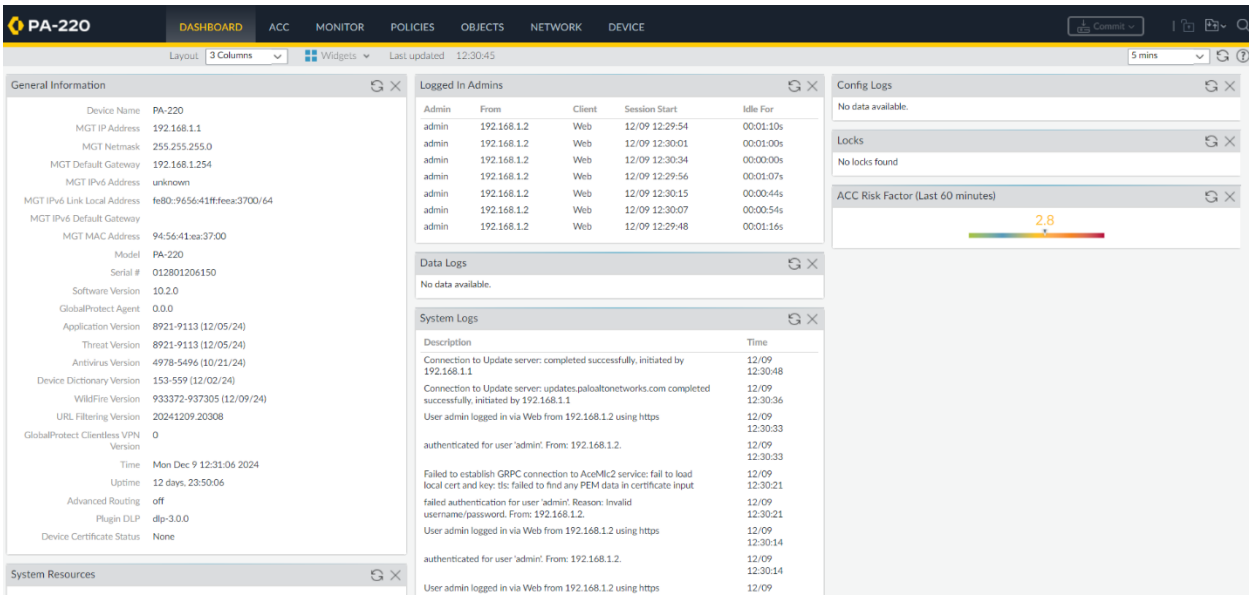
Several actions and configurations were critical during this lab:

- **Cable Setup**: Ensured proper physical connections to the firewall.

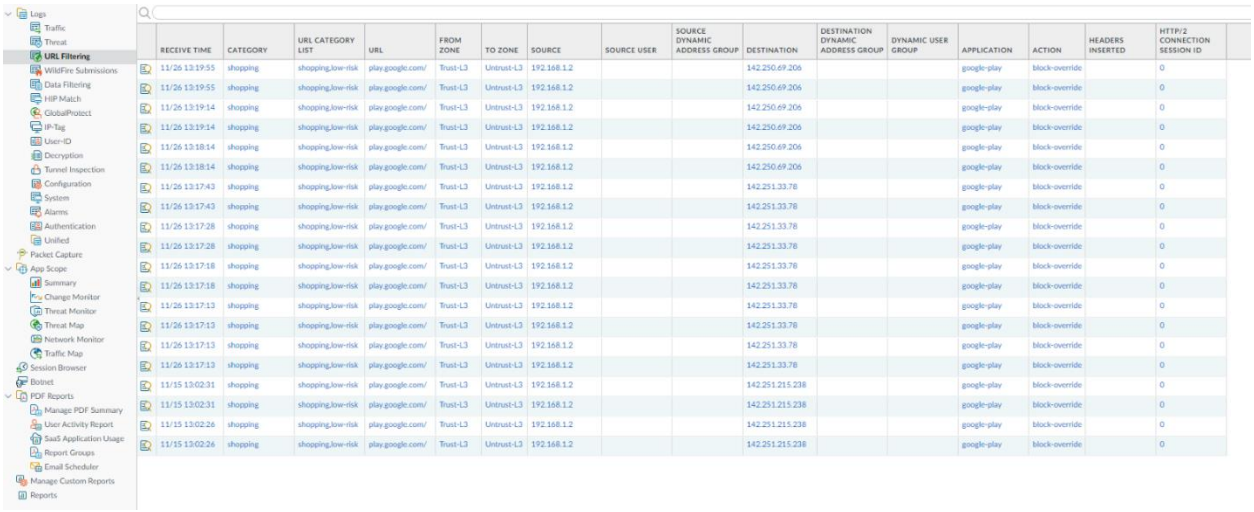


Here, in this image, it shows the console cable connected into the console port which is consoled into the PC. The **ethernet** on port 3 is also connected into the PC and is located above the console port. The **MGT** port is connected back into port 2 for extended management. Port 1 is connected directly to the **internet**.

- **GUI Access**: Logged into the GUI using https://192.168.1.1.

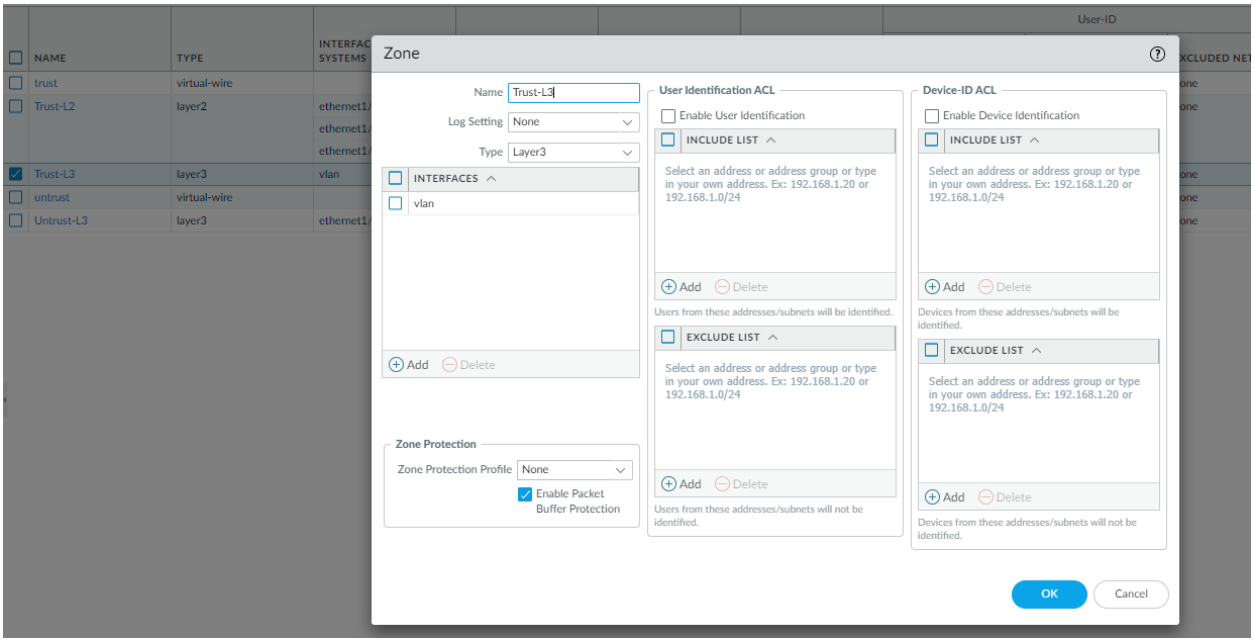
- 

Here is the main dashboard of the GUI, this is the **dashboard** page and it has the MGT IP address and subnet in the top left in general information. The logged in admins are the same every time because I configured a **static** IP address in the control panel for the PC.



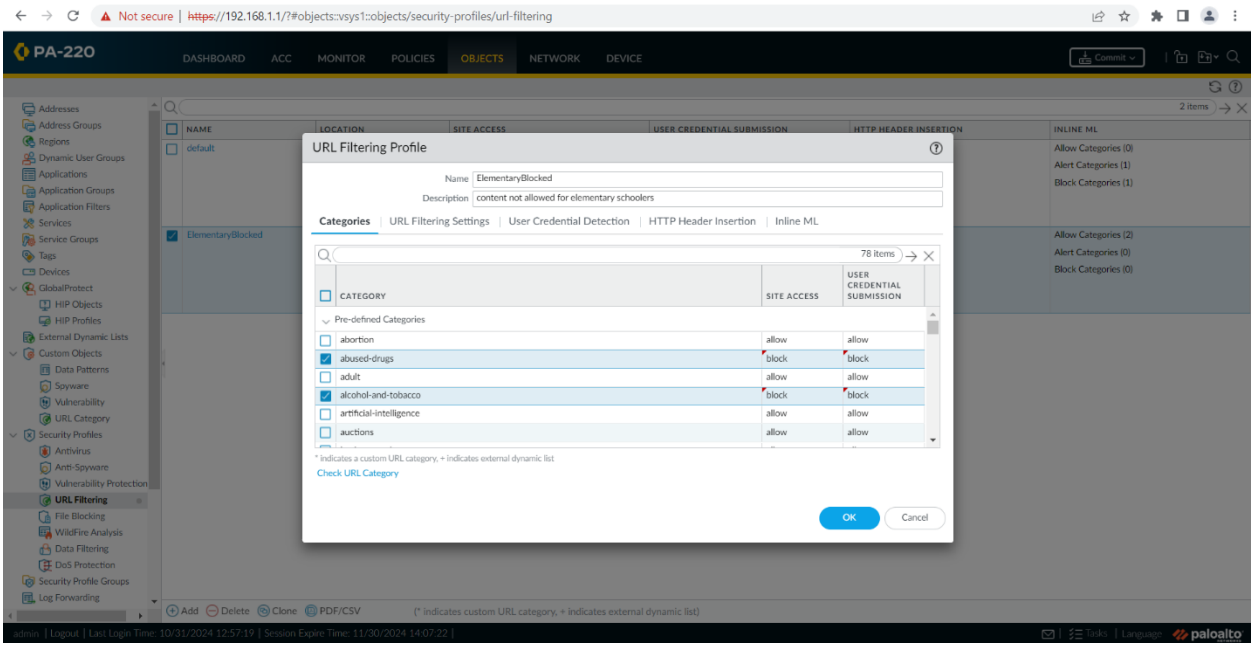
Here are all the IP addresses that are blocked, for this I blocked shopping category and therefore Amazon was unable to be reached by the PC.

Zone creation: Create the **zones** for internet outgoing on the layers.



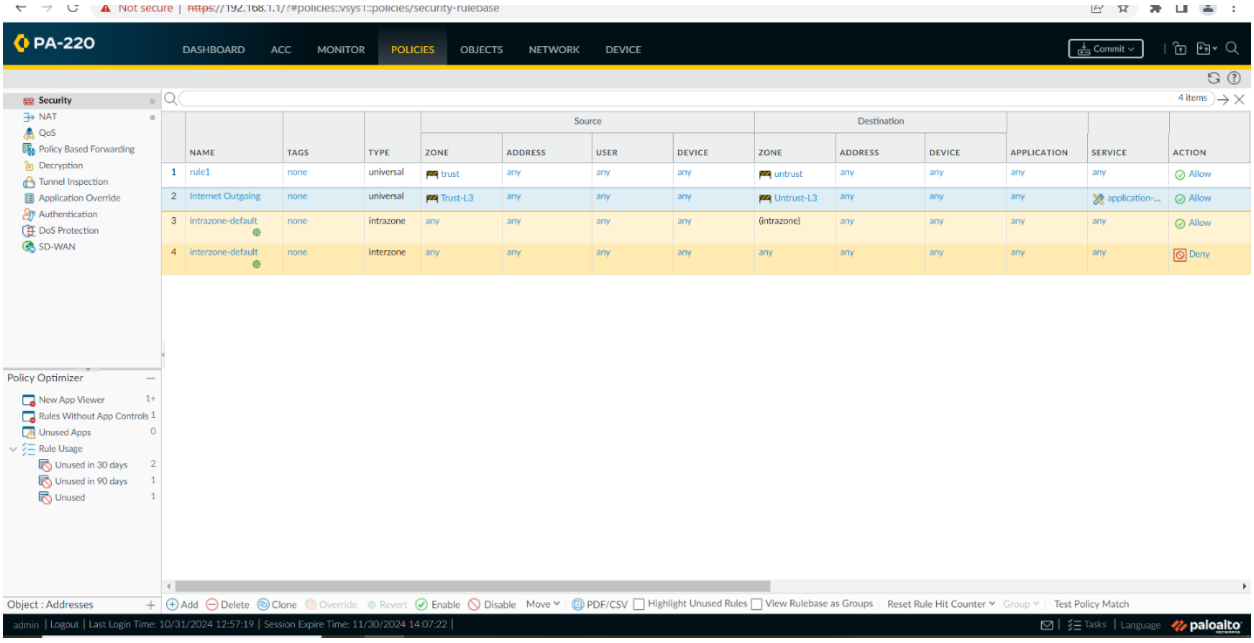
Here is the name of the zone on layer 3.

- **URL Filtering Profile**: Created the **ElementaryBlocked** list to define blocked categories.

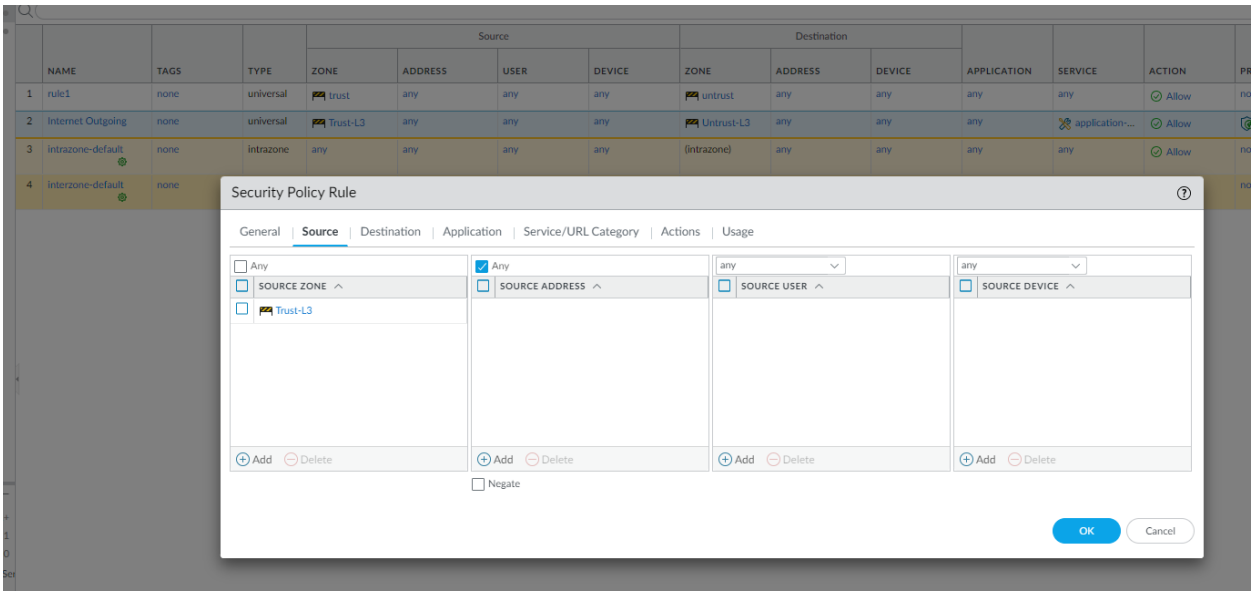


-

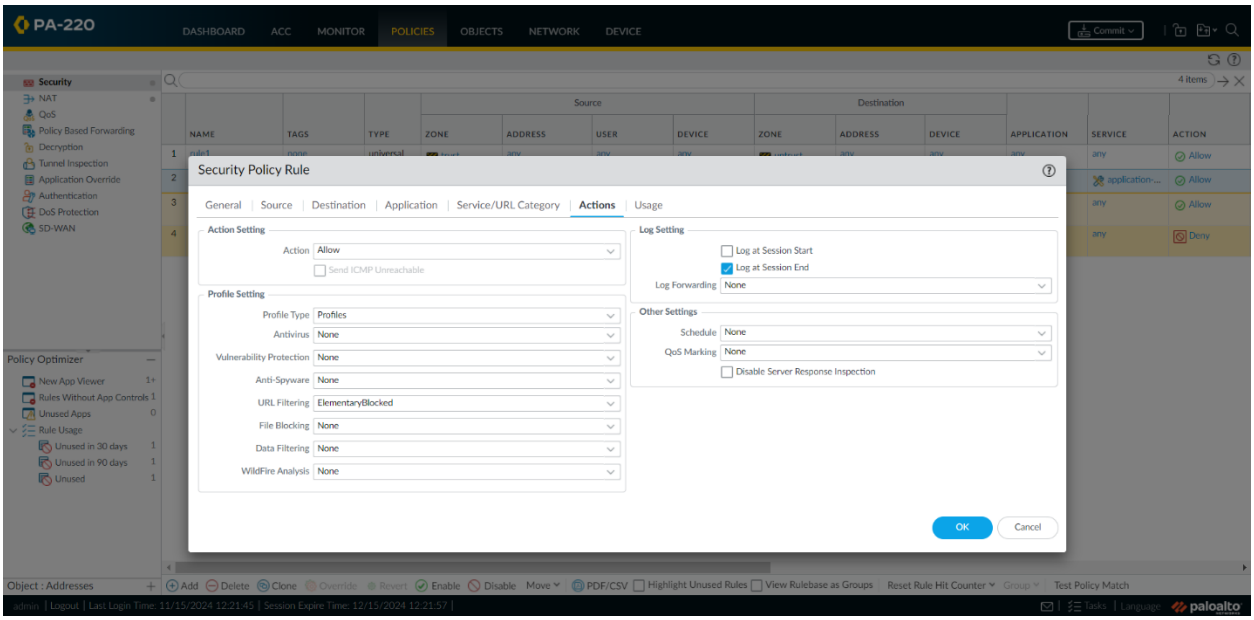
This picture is going into objects then URL filtering in the left menu. After pressing add, we get a new url filtering profile and can name it anything, then, the most crucial part, is choosing all the categories that align with the network security goals and set site access to block and credential submission block.



Once the profile is created, head into the policies tab and in the security tab in the left menu, all of the zones and policies will be there.

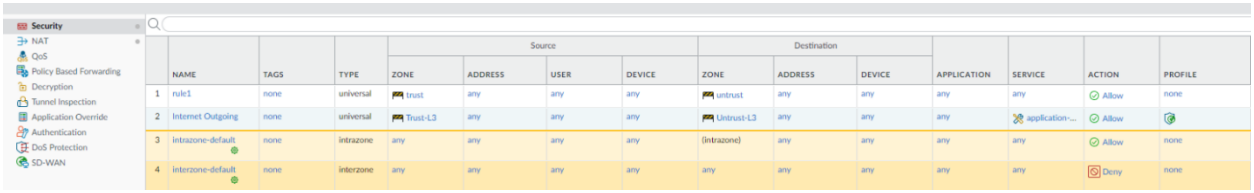


Now here, I clicked the zone policy that I wanted the url filtering profile to be configured on and set source zone to the one created in the previous step.



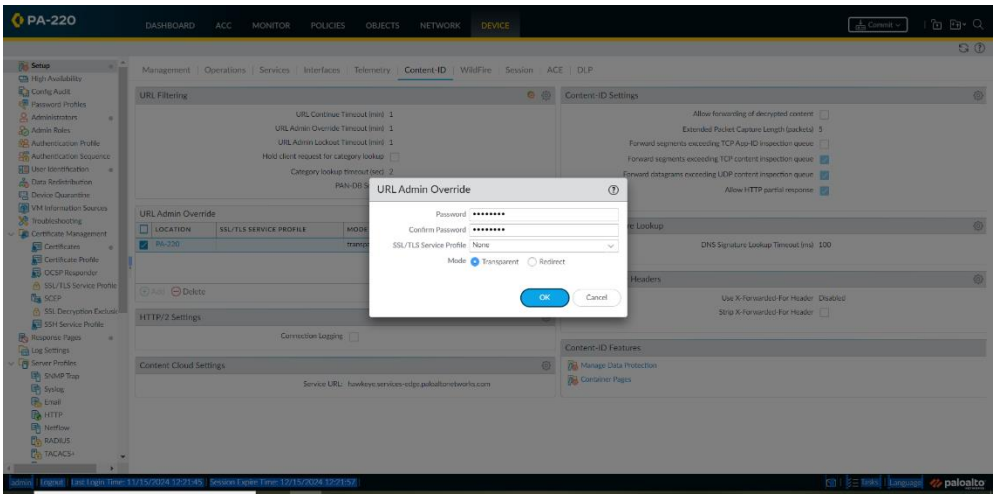
Then, click the zone that one prefers the url filtering list on, I chose the internet outgoing because of the guidelines for blocking url for elementary schoolers.

Security Policy: Linked the URL filtering profile to a new security policy with universal settings.



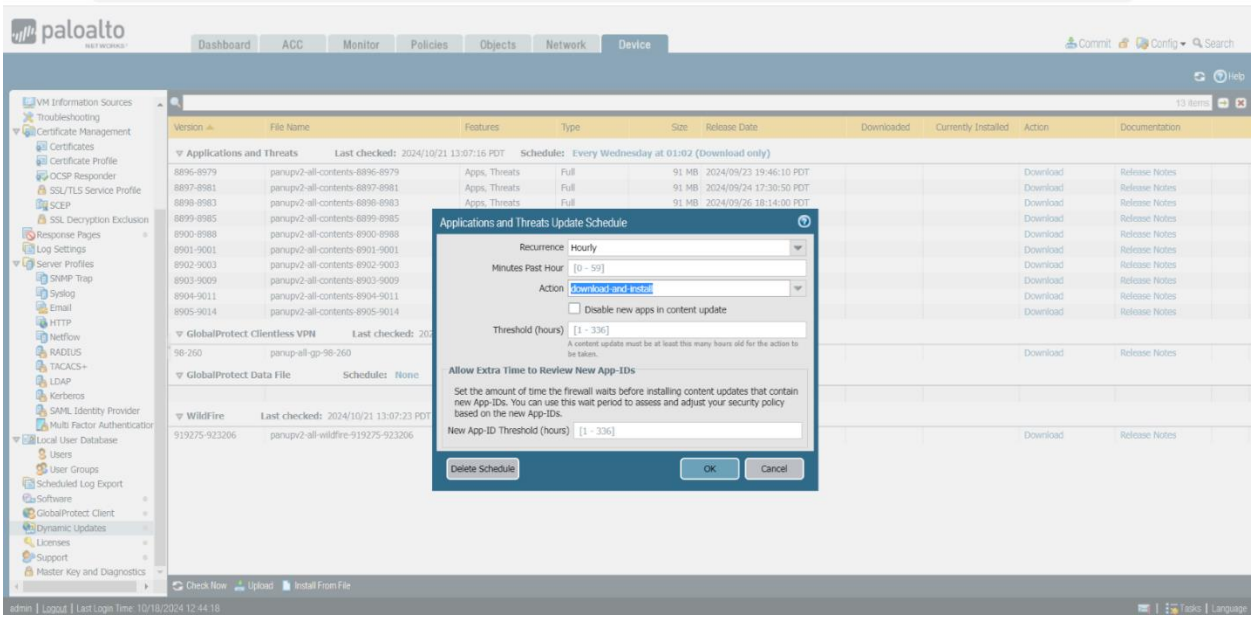
Here is the final internet outgoing security policy with the blocked profile configured on it.

URL Admin Override: Configured an override password for bypassing blocked pages.

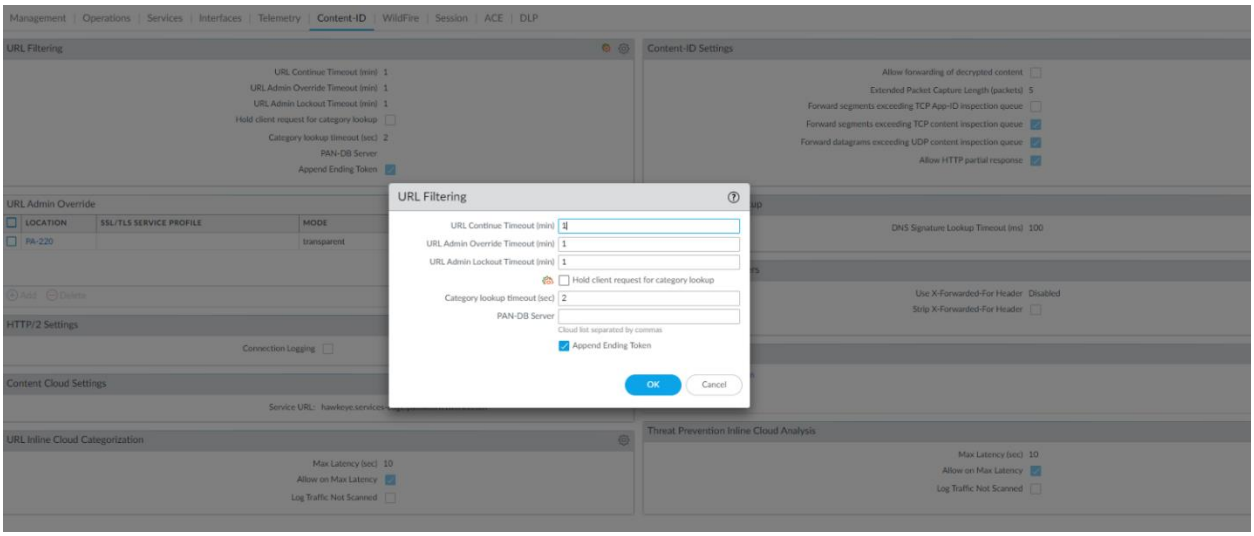


Here this image is configuring the URL admin Override password for “parents” to manually access the website.

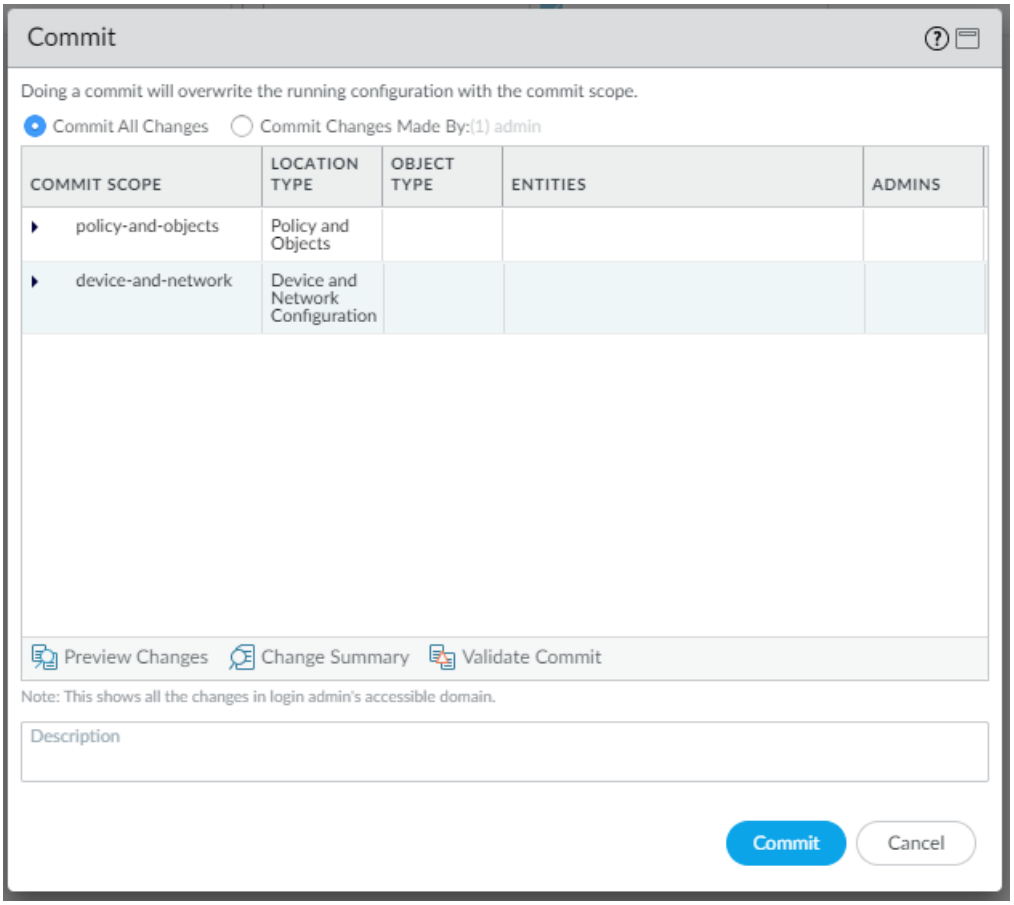
Time and Settings:



This picture illustrates default setting of hourly checking for threat updates and updating the firewall if needed. This is located in device tab on the top menu.

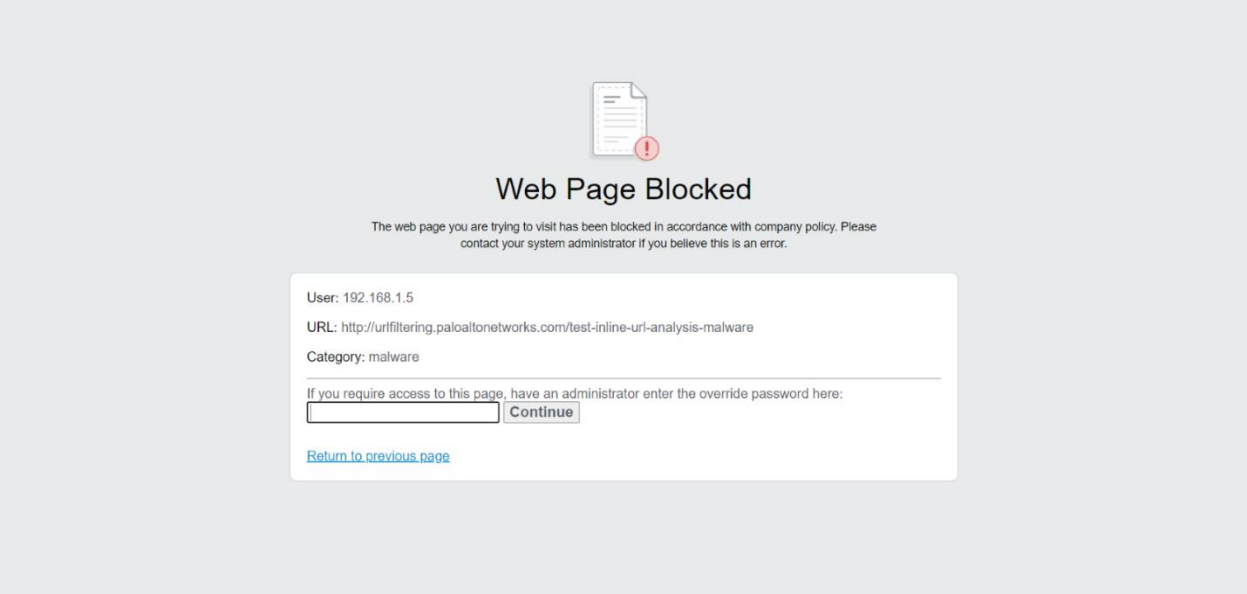


Here is the timeout for the override password if they guess the password wrong, it is 1 minute configured for mine.
Lastly, the most important part is committing all changes so saves are updated and ready for future access into the firewall:



This commit is in the top right corner and this is what it looks like.

Here is what it looks like when everything is configured and committed when one wants to visit a blocked URL:



5. Problems

I faced a few challenges during the lab:

1. **Port 2 Connection**: Initially, I struggled to understand why the management interface needed to connect to port 2. This caused delays until I realized it was necessary to extend management functionality.
2. **IP Configuration Mix-Ups**: Sometimes, I accidentally used **.1** in the control panel and **.2** in the browser, but this was a minor issue.
3. **Commit Times**: Changes had to be committed before testing, and each commit took about 10 minutes, making the process time-consuming.
4. **Updates**: Incremental updates took nearly 20 minutes each, which added up significantly during the upgrade process.

5. **Time Setting**: One classic issue I faced was making sure the manual clock on the firewall matched with the clock on the PC so that the updates sync at the same time because some actions are configured time based.

6. Conclusion

This lab provided practical experience in configuring URL filtering and override features on a physical firewall. I learned how to block inappropriate content effectively while enabling administrator override when needed. Despite challenges like cable setup and long update times, the lab was successful and highlighted the importance of attention to detail when working with network security equipment. This exercise further developed my skills in managing Palo Alto firewalls and reinforced my understanding of cybersecurity principles.

Palo Alto 220 GlobalProtect Site-to-Site VPN

1. Purpose

The purpose of this lab was to gain hands-on experience in configuring GlobalProtect VPN on a Palo Alto PA-220 firewall for secure site-to-site and remote desktop connectivity. This included creating security zones, managing tunnel interfaces, and implementing security policies for controlled access to different zones. The lab also covered the creation and deployment of certificates for authentication and configuring GlobalProtect portals and gateways to ensure encrypted communication between clients and the network. The objective was to build a secure and functional remote access environment while understanding the configuration process for real-world application.

What I learned/problems:

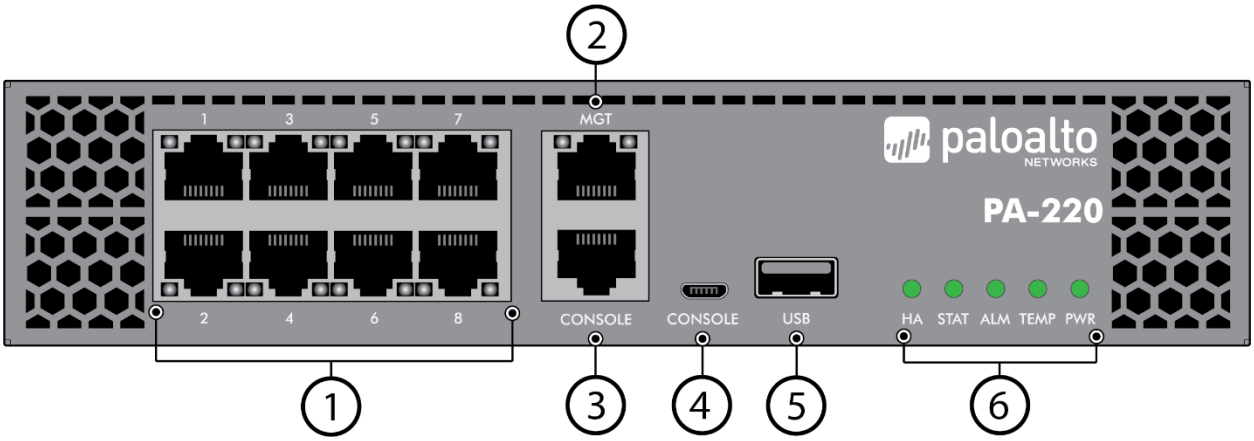
The skills I learned in this lab are concrete and expandable. The problems we faced and how we fixed them:

- No Global Protect – We downloaded this software on the PCs for the VPN
- Bad VLAN – We did not create NEW VLAN which had a number in the top right corner such as 10 which created problems for everything associated with the original VLAN so all of those had to change to the new one we created. Mr. Mason warned us.
- Laptop Malfunction – We came to class and all the IPs and control panel and GUI stopped working for the firewall, we tried for a week to debug this by replacing cables and reorganizing the topology. Following our OWN labs for the reboot firewall, we did that and did the reboot sequence by typing MAINT in 5 seconds; our firewall started working again.

2. Background Information on Lab Concepts

Palo Alto Networks is one of the most trusted names in cybersecurity, protecting over 70,000 organizations across 150 countries, including 85 of the Fortune 100 companies. Their next-generation firewalls (NGFWs) are designed to block both known and unknown cyber threats while giving administrators advanced control over network traffic. Unlike traditional firewalls that rely on ports and IP addresses, Palo Alto firewalls allow policies based on specific applications, so you can allow access to tools like YouTube but block games like Fortnite. Their global threat intelligence system ensures that if one customer encounters a new threat, all other customers are automatically updated to defend against it. In this lab, I worked with the PA 220, a compact firewall designed for small businesses or SOHOs.

The PA 220 has several exterior components, labeled on the diagram:

- **MGT (Management) Port (2)**: Used for administrative purposes, this port allows access to the firewall's interface for managing security and system configurations.
- **Console Port (3)**: This port enables direct access to the firewall and is frequently used for consoling in with a PC.
- **USB & Micro-USB Ports (4,5)**: These ports are used for system recovery, updates, or backups.
- **8 Ethernet Ports (1)**: These ports connect the firewall to both internal and external networks, allowing traffic to be filtered and routed.
- 

  Power Inputs 1 & 2: The device has two power inputs, ensuring that if one goes down, there is another.

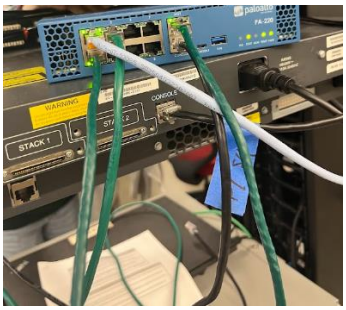
Recently, Palo Alto firewalls were targeted in **Operation Lunar Peek**, where attackers exploited two vulnerabilities (**CVE-2024-0012** and **CVE-2024-9474**) to bypass authentication and gain admin privileges. Hackers used this access to install malware and make unauthorized changes. The attack primarily affected devices with **exposed management interfaces** on the internet. Palo Alto responded by releasing patches and recommending restricting management access to **trusted internal IPs**.

Palo Alto quickly released updates to patch the vulnerabilities and advised customers to secure the management interface by limiting access to internal, trusted IPs. They emphasized that regular updates and best practices are critical to keeping networks safe. Even with these challenges, Palo Alto firewalls remain one of the most trusted tools for protecting networks because of their ability to adapt and share real-time threat intelligence across customers.

Physical firewalls like the PA 220 provide several advantages over cloud-based solutions.

First, they give administrators full control over the network's security configurations. Second, they ensure reliability by operating locally without depending on external factors, thus reducing latency and potential points of failure. Finally, they help maintain data privacy, as sensitive data remains within the organization's infrastructure rather than passing through the cloud.

3. Lab Summary



The lab began with setting up the hardware. The image shows the physical connections made on the PA 220: Once the cables were connected, I configured the PC with an IP address of **192.168.1.2** and a subnet mask of **/24**. I accessed the GUI by entering https://192.168.1.1 into Firefox and logged in with the default credentials (**admin/admin**). The first step was to change the default password to **admin/Cisco123** for security purposes.

Next, I updated the firewall. This process required upgrading incrementally from version **9.0.0** to **10.2.0**, following a sequence like **9.0.0 → 9.0.9 → 9.1.0 → 9.1.9** and so on. Each update took approximately 20 minutes, making this step time-consuming but necessary for accessing the latest features.

After updating, I manually synchronized the firewall's clock with real-world time. While I didn't encounter issues here, having an accurate clock is important for update validation, log accuracy, and overall functionality.

1. **Initial Configuration:**
    a. The firewall was accessed through the MGT port using its default IP (192.168.1.1). The PC was configured with a static IP (192.168.1.2) and a subnet mask (/24) to access the firewall's GUI.
    b. Default credentials (admin/admin) were changed to improve security.
2. **Security Zones and Interfaces:**
    a. Security zones such as *Trust*, *Untrust*, and *VPN Tunnel* were created.
    b. Interfaces were assigned to the appropriate zones to control traffic flow. For example, tunnel interfaces were tied to the VPN zone, while external-facing interfaces were connected to the Untrust zone.
3. **GlobalProtect VPN Configuration:**
    a. A GlobalProtect portal was created to handle VPN client connections. The portal was configured with an SSL/TLS certificate for secure communication.

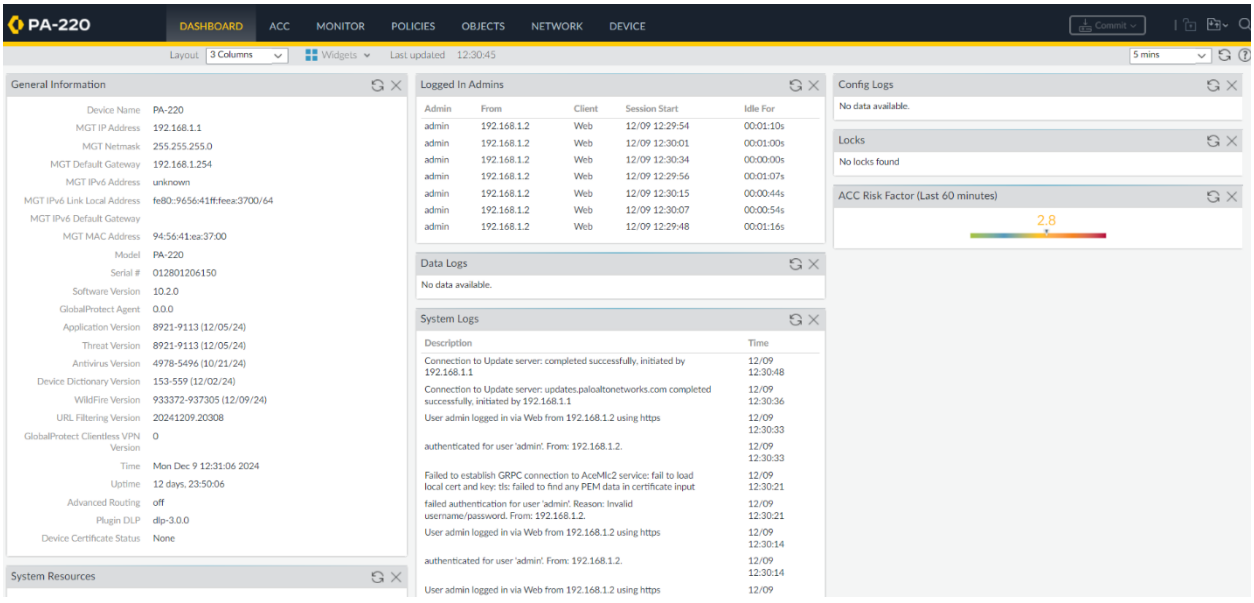
    b. A GlobalProtect gateway was created to enable secure data tunneling between remote clients and the internal network.
    c. Certificates were generated using the Certificate Management feature to authenticate users and encrypt data.
4. **Policy Implementation:**
    a. Security policies were created to control access between zones. Examples include:
        i. *Interzone traffic policies:* Allowed limited access between internal zones and restricted access from the Untrust zone.
        ii. *Tunnel-specific policies:* Enabled traffic from the VPN zone to access the Trust zone for remote desktop purposes.
    b. Policies were tested to ensure they matched the intended flow of traffic, with rules like "Trust to Tunnel" or "Tunnel to Untrust."
5. **Testing the Configuration:**
    a. After committing all configurations, connectivity was tested by connecting to the VPN using GlobalProtect.
    b. Policies were validated by monitoring traffic logs, ensuring only authorized traffic passed between zones.
6. **Troubleshooting and Observations:**
    a. Issues such as certificate errors and misconfigured policies were identified and resolved.
    b. Time synchronization between the firewall and client devices was manually adjusted to ensure certificate validation.

4. Lab Commands

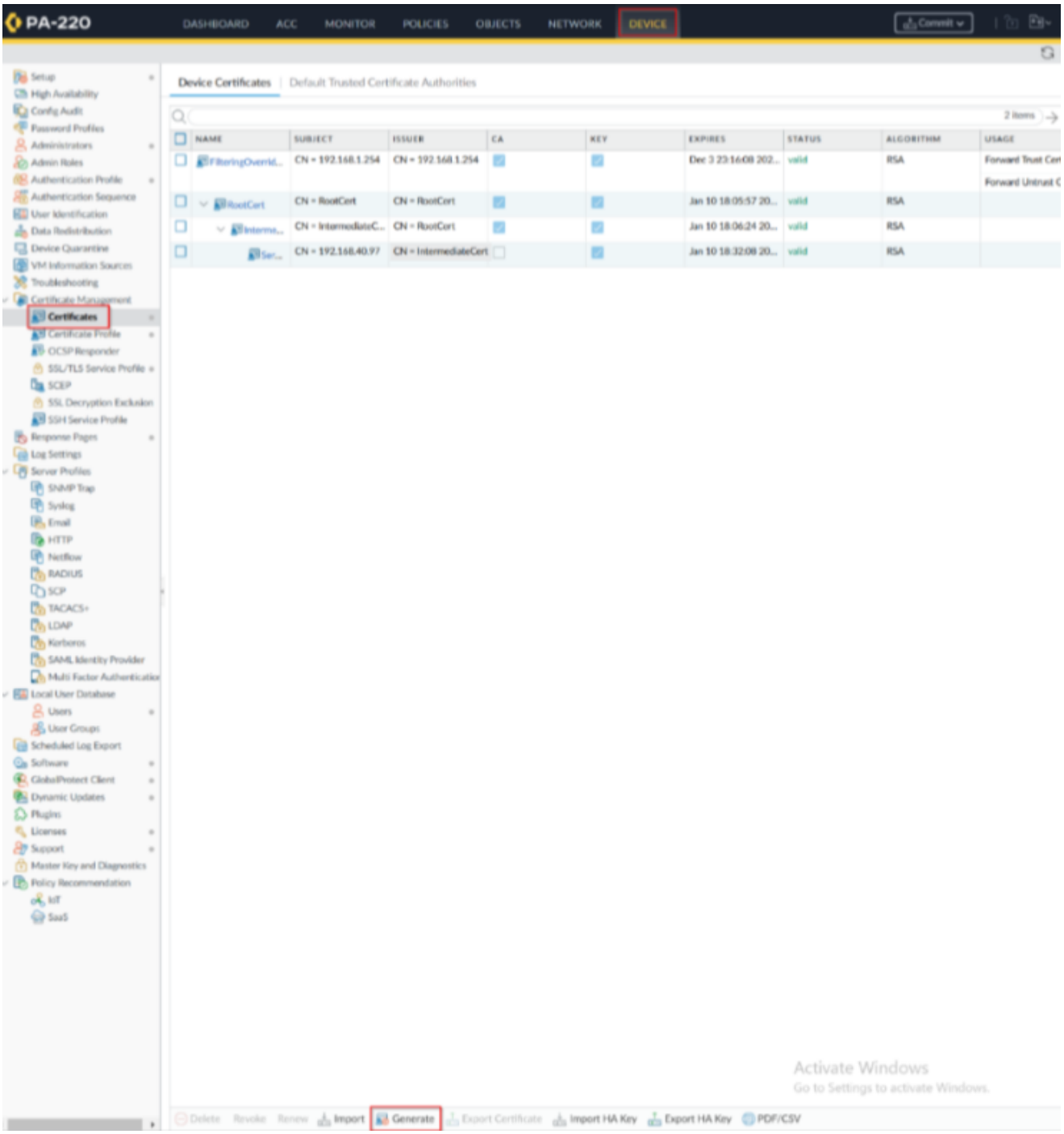
Several actions and configurations were critical during this lab:

- **Cable Setup**: Ensured proper physical connections to the firewall.

Here, in this image, it shows the console cable connected into the console port which is consoled into the PC. The **ethernet** on port 3 is also connected into the PC and is located above the console port. The **MGT** port is connected back into port 2 for extended management. Port 1 is connected directly to the **internet**.

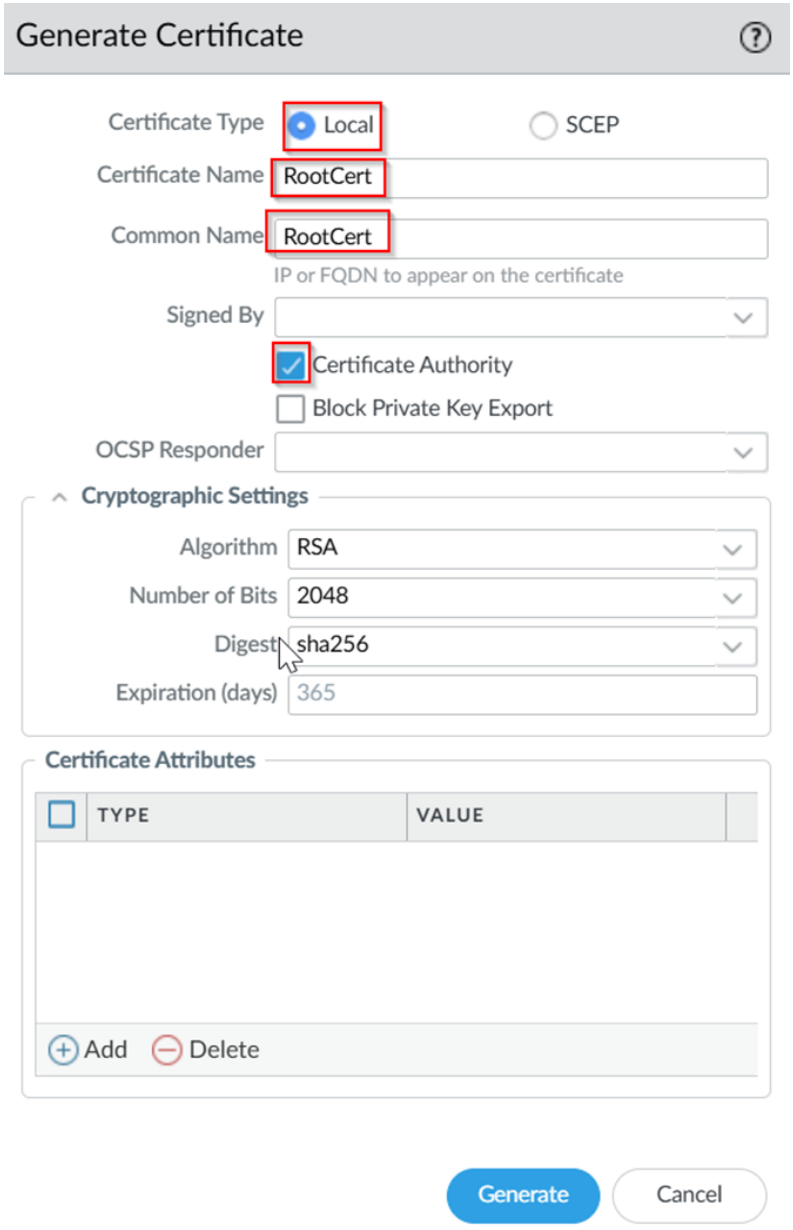
- **GUI Access**: Logged into the GUI using https://192.168.1.1.
- 

Here is the main dashboard of the GUI, this is the **dashboard** page and it has the MGT IP address and subnet in the top left in general information. The logged in admins are the same every time because I configured a **static** IP address in the control panel for the PC.



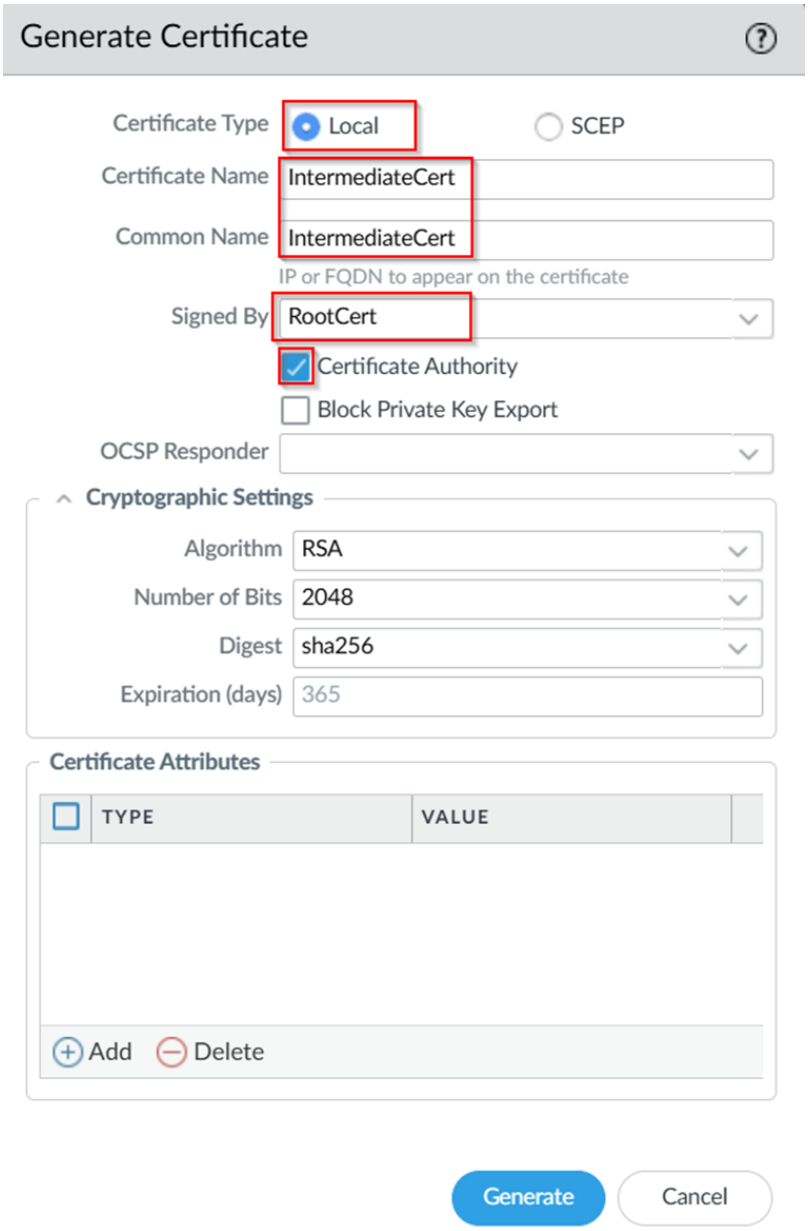
The image above shows the generation of certificates. We made 3 different certificates: Root, Intermediate, and Server, these were in a stack respectively. This was created by

going into the GUI, then Device tab, then certificate, then generate.

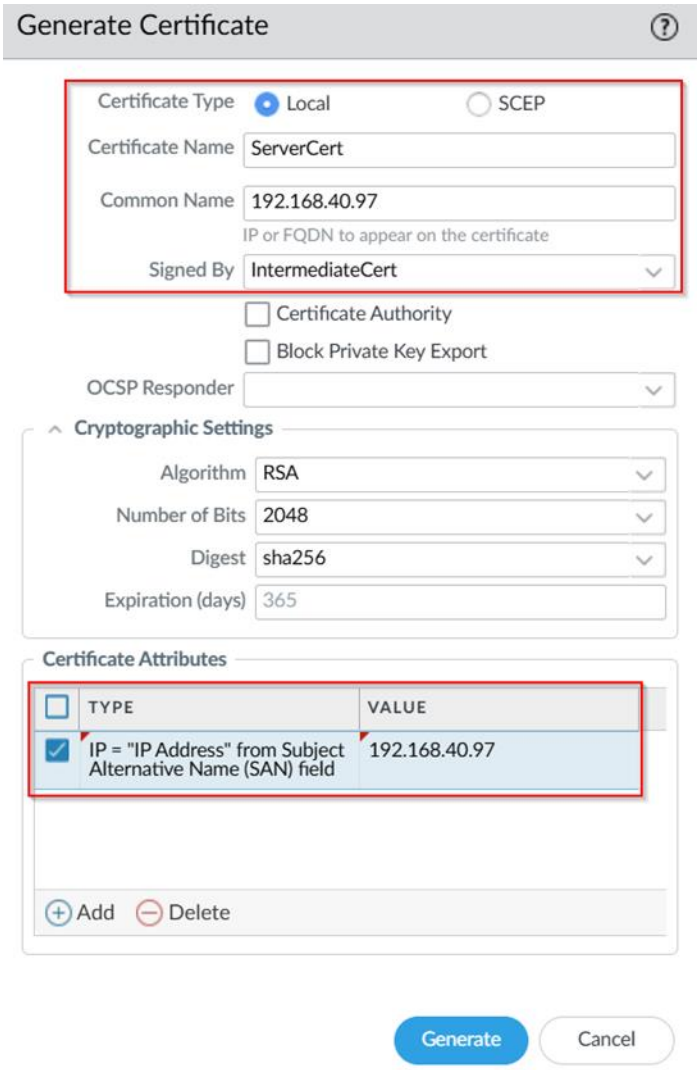


The first certificate to create is the Root Cert. This is a local certificate signed off by Root, and this is certificate authority. Now create an intermediate certificate which is signed off

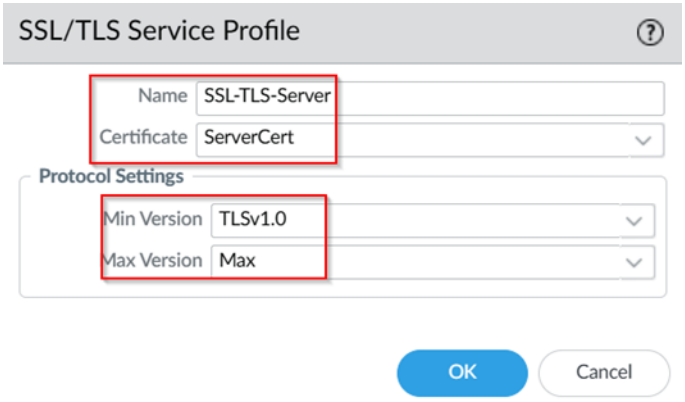
by the Root Certificate we just made:



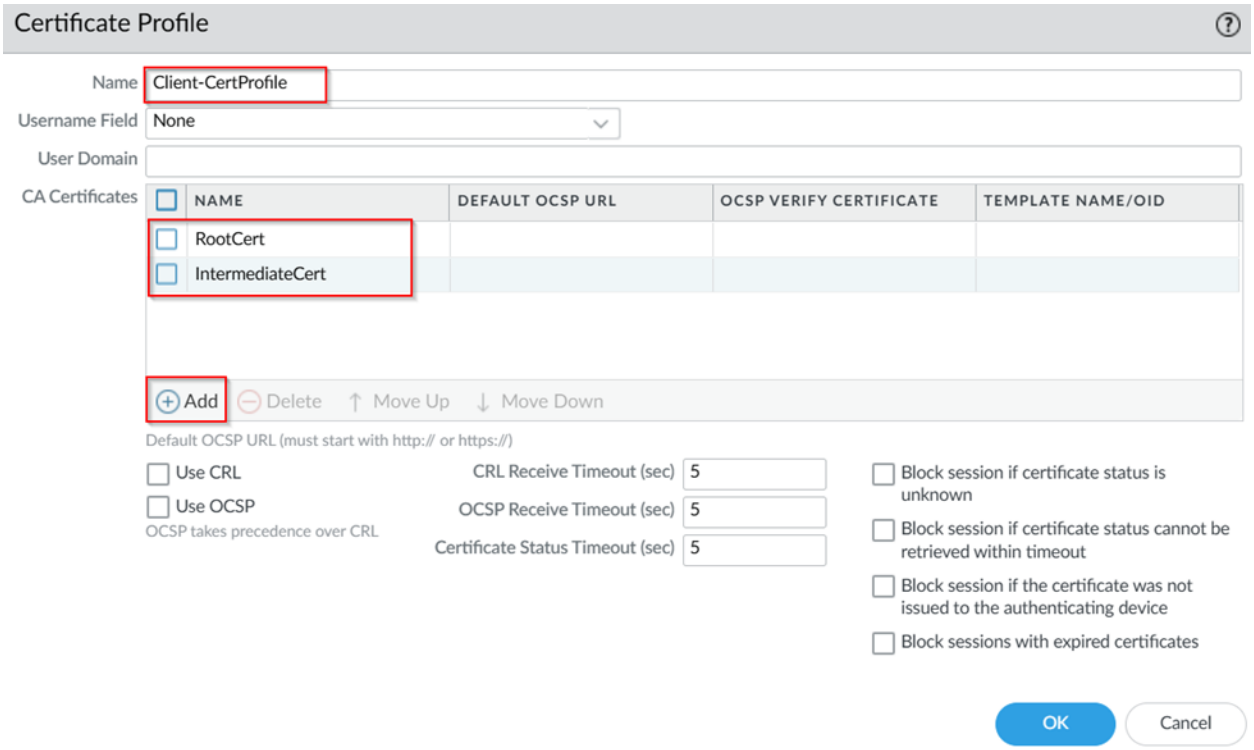
Lastly, create the server certificate. The common name is the IP address of your Global Protect Portal:



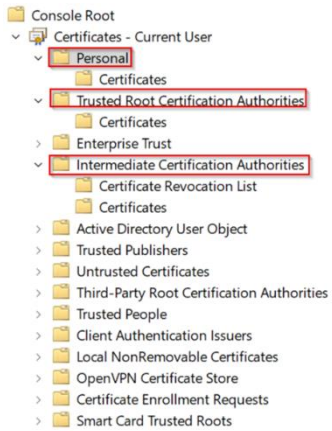
Then create a TLS-SSL Service Profile using the Server Certificate that was just created. Follow the image below:



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.

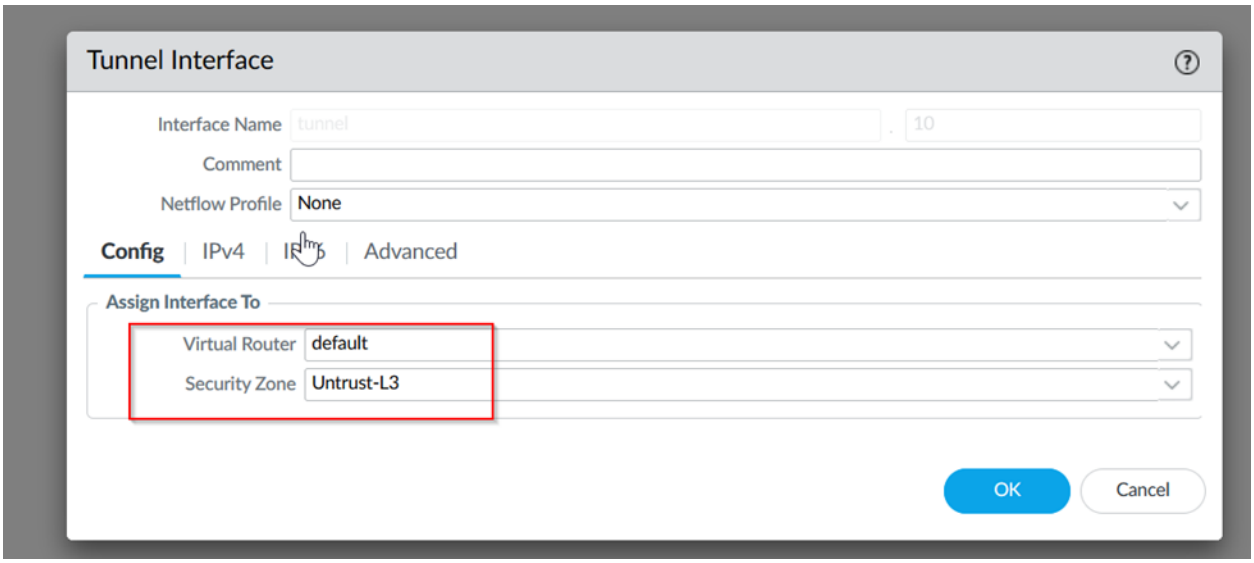


Now all the certificates are created so they must be downloaded on the first device of the VPN, then transferred with a flash drive to the other site where the VPN will be using remote desktop. Hit WIN+R and then type ”mmc.” Then click file, and then add/remove and choose my user account. Select certificates, then add, then ok. Follow those steps to include all the certificates into the authorities folder.

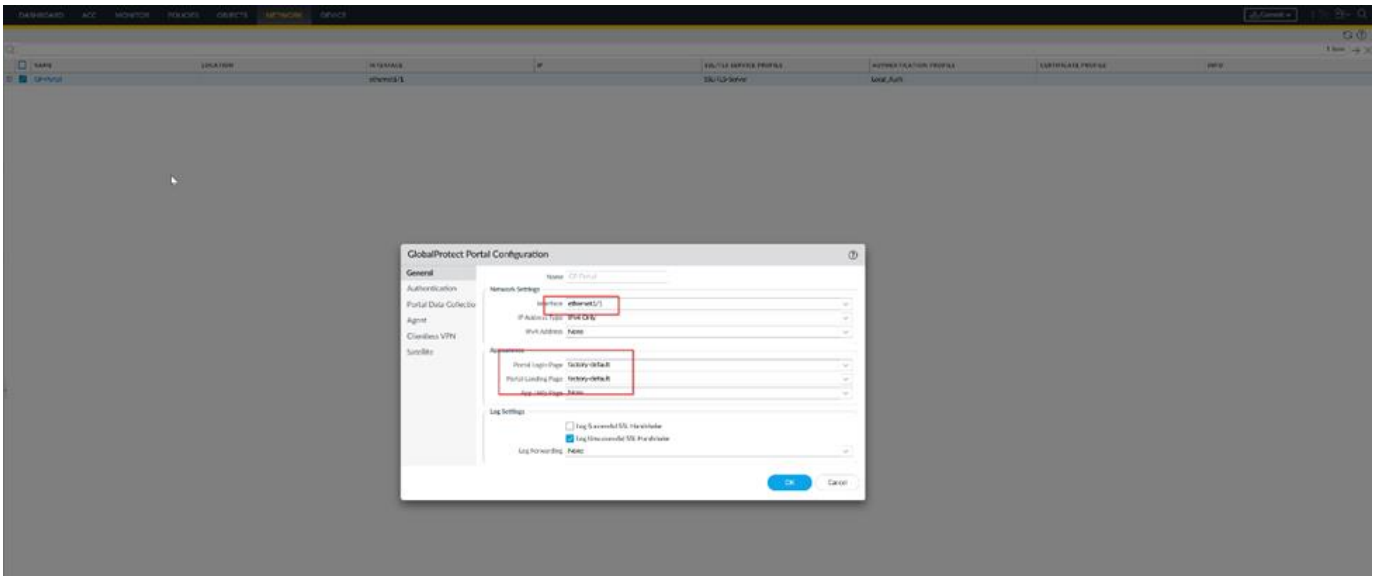


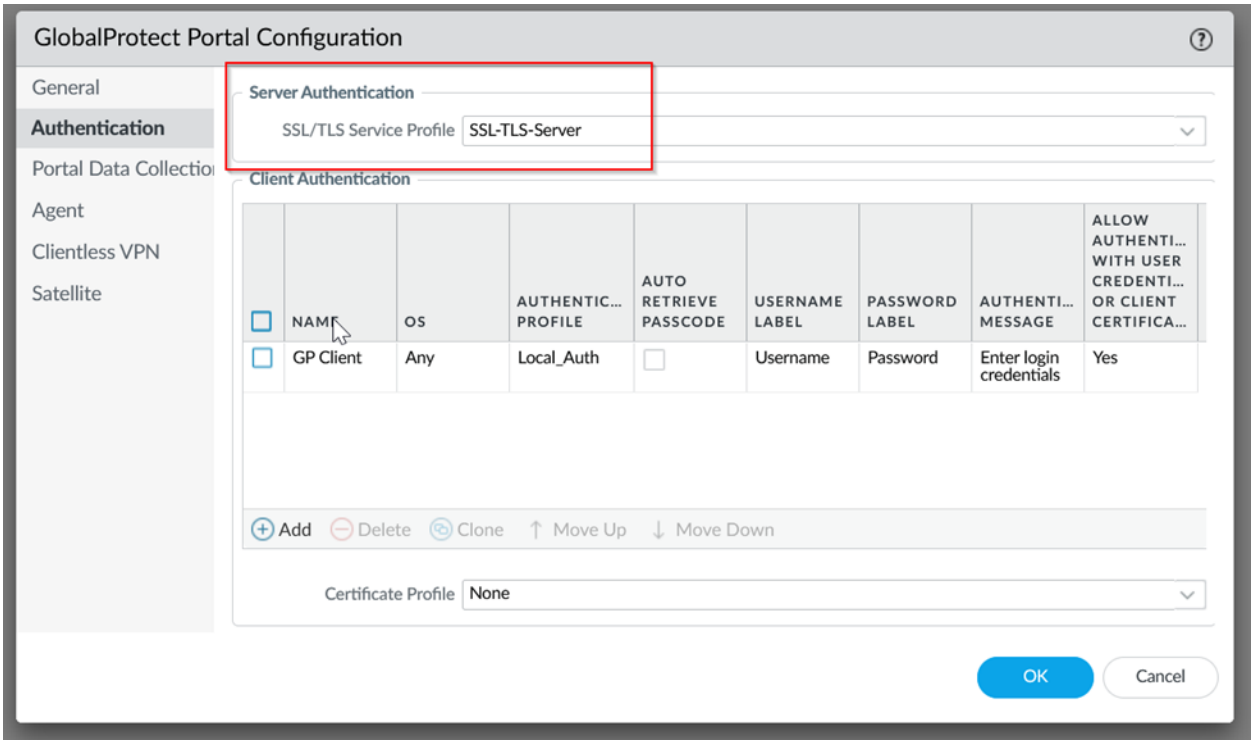
Now go back to the GUI, go to authentication profile, and the type is a local database.

Now we need to create a tunnel in the network tab under interfaces and then security zone is usually untrust L3 or whichever your outwards interface is.

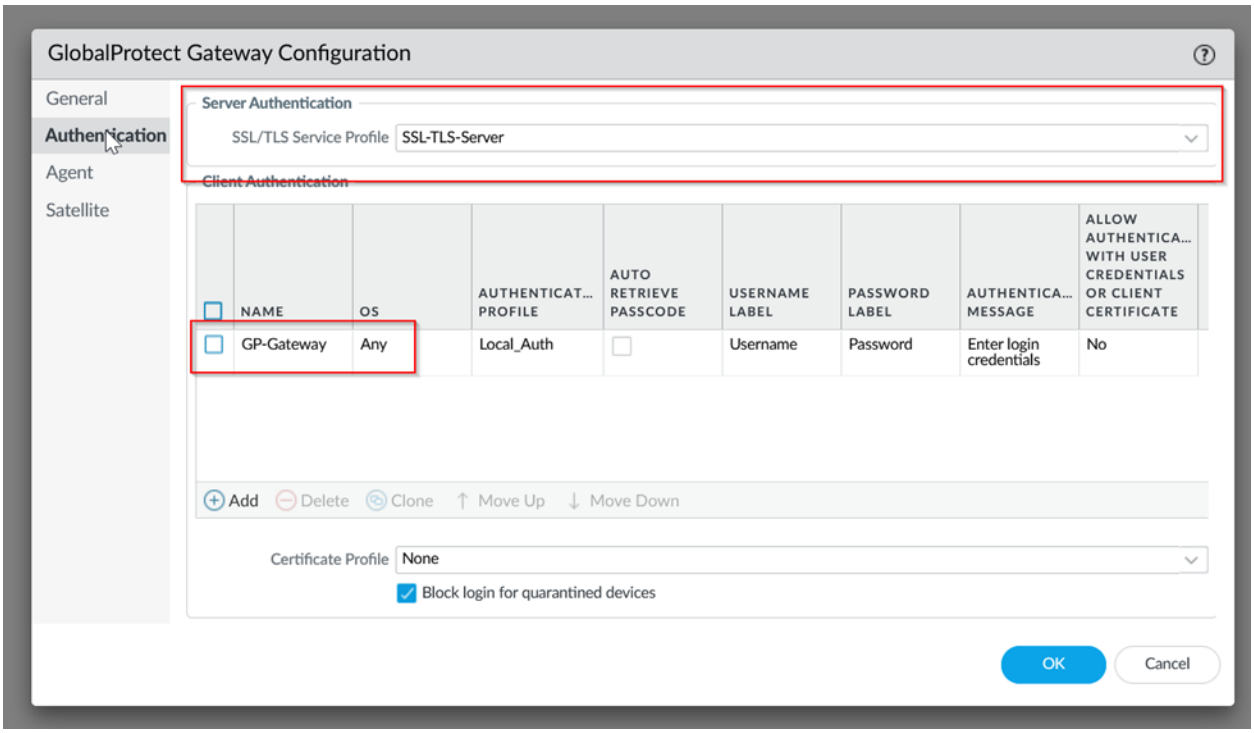


Then in global protect and portals, add a new portal, the interface is the outwards facing one again. Once done with the name and interface, click on “Authentication” and make sure the Service Profile is set to “SSL-TLS-Server.” OS is Any, and Auth Profile is Local_Auth.

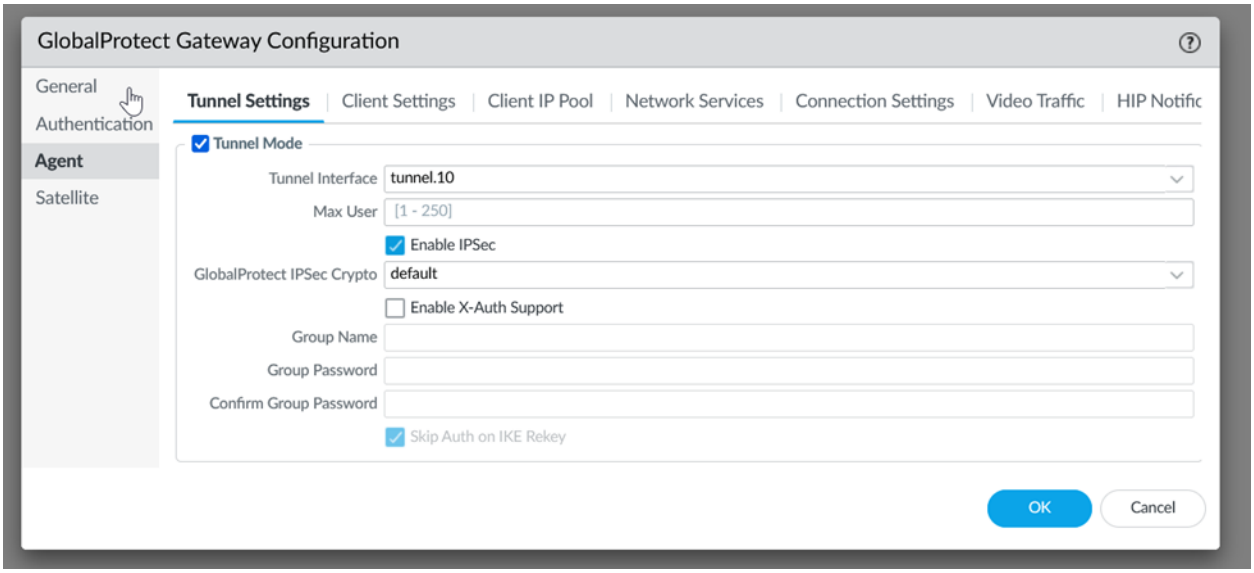




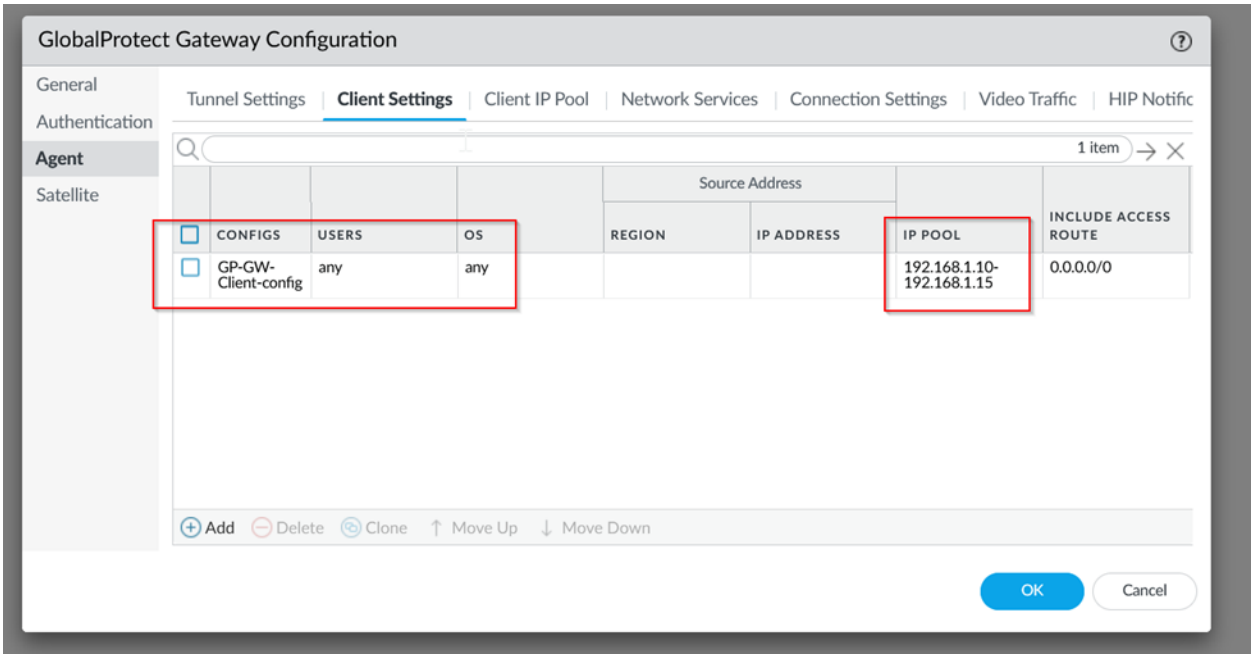
Then in Network go to gateways and create one with the name of the portal created above. Click authentication and select the SSL server. Add a new authentication with the OS any.



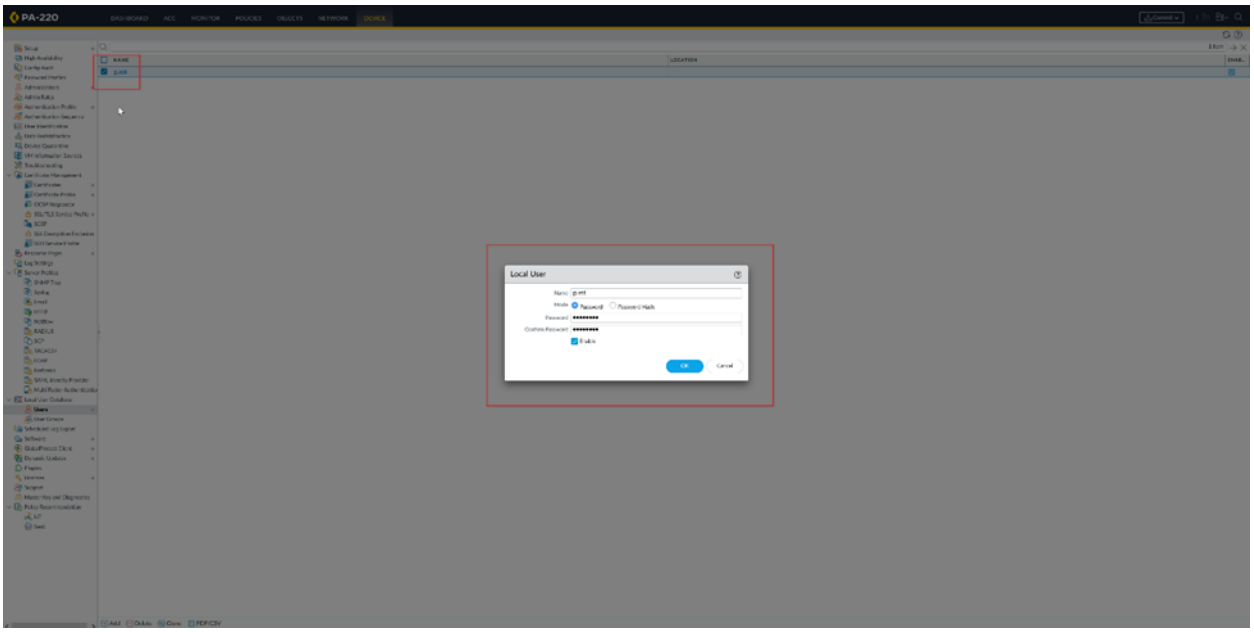
Then in the same section go to the agent tab and enable IPSec.



In client settings add an IP pool in the range of IPs we have.

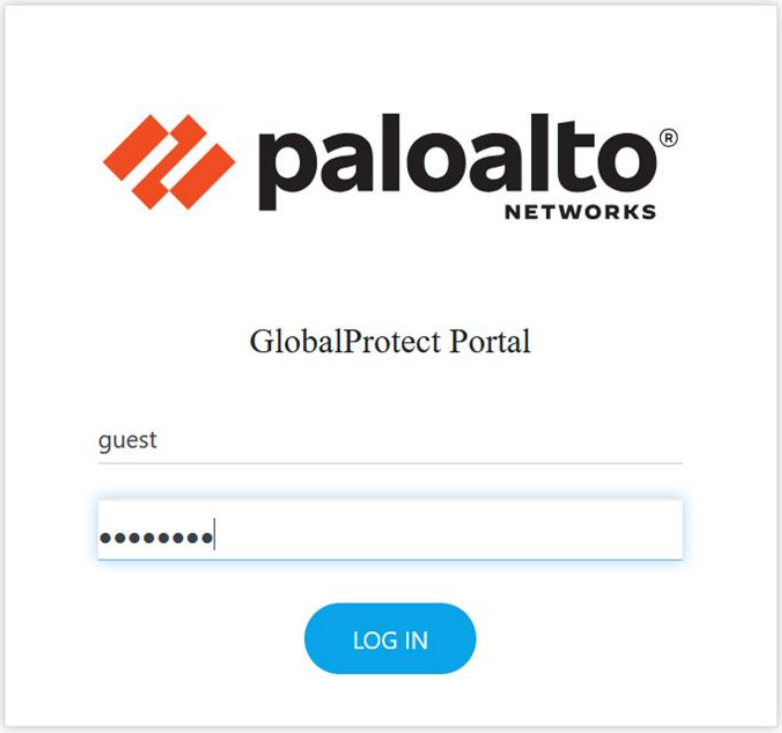


In the device tab now, create a local user.



Finally, commit all the changes.

On the other PC where the remote desktop is, enter the IP address of the outward interface. For us it was 192.168.40.14.



Conclusion: This lab provided valuable experience in configuring a Palo Alto PA-220 firewall for secure site-to-site and remote desktop VPN connectivity. By creating security zones, configuring GlobalProtect portals and gateways, and implementing detailed security policies, I gained practical skills in managing remote access and securing network traffic.

Fortinet Firewall SOHO Configuration

1. Purpose

The purpose of this lab was to gain hands-on experience setting up a small office/home office (SOHO) wireless network using a Fortinet firewall. The lab covered both the CLI and GUI sides of configuration, firmware upgrades, and creating wireless SSIDs for different types of network access. The final step involved verifying successful connectivity using mobile devices. This lab provided a complete overview of wireless deployment on Fortinet devices, including both administrative configuration and real-world testing.

Problems:

The first major issue came right at the beginning, when we connected to the Fortinet firewall, it still had a username and password set from the previous group. We couldn't log in through the GUI at all, so we had to connect through the console using PuTTY and perform a full factory reset. This step took a bit of troubleshooting since we had to make sure we were connected properly through the console cable and navigate the CLI to wipe the config and restore it to default settings. Once it was reset, we were able to get into the GUI using the default credentials.

After getting into the GUI, we ran into our second issue: the firewall wasn't running FortiOS 7.4.0. We had to manually update the firmware by downloading the latest version and then uploading it to the firewall. That process took a little while, but once the firewall was on 7.4.0, everything we needed became available.

Lastly, during the wireless setup, we accidentally overlapped the DHCP IP pools between the two SSIDs. That caused some address conflicts that made it seem like one of the networks wasn't working at all. Once we caught the mistake and changed one of the address ranges, both SSIDs started assigning addresses correctly and everything functioned like it was supposed to.

2. Background Information on Lab Concepts

Fortinet is a huge player in the network security space, especially when it comes to delivering an all-in-one solution. While people often think of firewalls like Palo Alto when they think "enterprise security," Fortinet does things a bit differently. Their approach is more about building out an ecosystem where everything works together under one management system: switches, firewalls, access points, and even endpoint security. They call this the **Security Fabric**, and it really shows in labs like this one.

The firewall used in this lab, the **FortiGate 40F**, is meant for small businesses or branch offices. But don't let the size fool you, it comes packed with features that would normally

be spread across multiple devices. In this one lab, it handled DHCP, Wi-Fi controller duties, NAT, security inspection, firmware management, and policy enforcement — all from the same GUI. Compared to Palo Alto's PA-220, which is strong in deep packet inspection and app control, the 40F feels a little more user-friendly and way faster to set up for a full wireless deployment.

One of Fortinet's biggest strengths is how seamless the Wi-Fi side of things is. You don't need an extra wireless controller , you just connect a FortiAP and everything shows up under the same dashboard. You can configure SSIDs, assign static IPs, monitor bandwidth per device, and set up NAT and security profiles, all in one place. The wireless features even include tunnel and bridge modes, so you can route traffic exactly how you want.

This lab also involved some basic CLI work with PuTTY, which is important for recovery scenarios or low-level changes. But most of the heavy lifting happened in the GUI. What makes Fortinet different is that it's built to support both open networks (just a password) and enterprise networks (username + password with WPA2-Enterprise) without needing a RADIUS server or separate gear.

3. Lab Summary

This lab began by building out the full SOHO topology using a Fortinet firewall, FortiAP, PC, internet cable, and multiple Ethernet connections. The setup started with assigning a static IP to the PC and connecting to the firewall over console using PuTTY. After logging in with default credentials and resetting, the GUI was accessed through the management IP (192.168.1.99).

From the GUI, a new admin password was set, and the system was upgraded from FortiOS v7.0.15 to v7.4.0.

Two wireless SSIDs were created: ISFortiGate (open access) and ISFortiGate2 (enterprise authentication). For each SSID, IP addresses and subnet masks were configured manually, and DHCP servers were enabled where needed. These SSIDs were broadcasted through a connected FortiAP, and mobile devices were used to connect and test access.

Both phones successfully connected, one with just a password and the other with enterprise-style credentials, illustrating how Fortinet can support multiple types of Wi-Fi access on the same device. Finally, traffic was allowed between interfaces through clearly defined firewall policies that used NAT and SSL profile settings.

4. Lab Commands (The captions reference the image ABOVE)

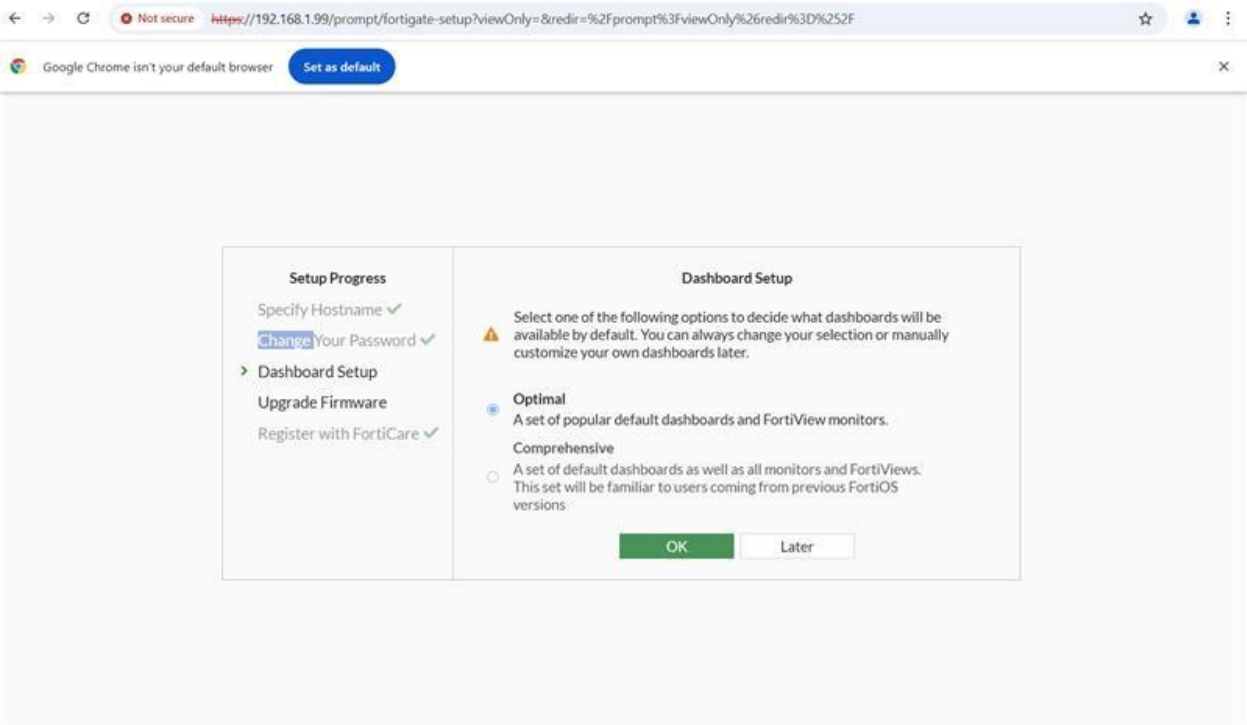


Image 1 (Dashboard Setup GUI - Initial Screen)

After assigning the static IP 192.168.1.2/24 to the PC, the first login to the firewall GUI at https://192.168.1.99 brought up the setup wizard. This is where the hostname and password were configured, and the GUI offered an “Optimal” vs. “Comprehensive” dashboard view.

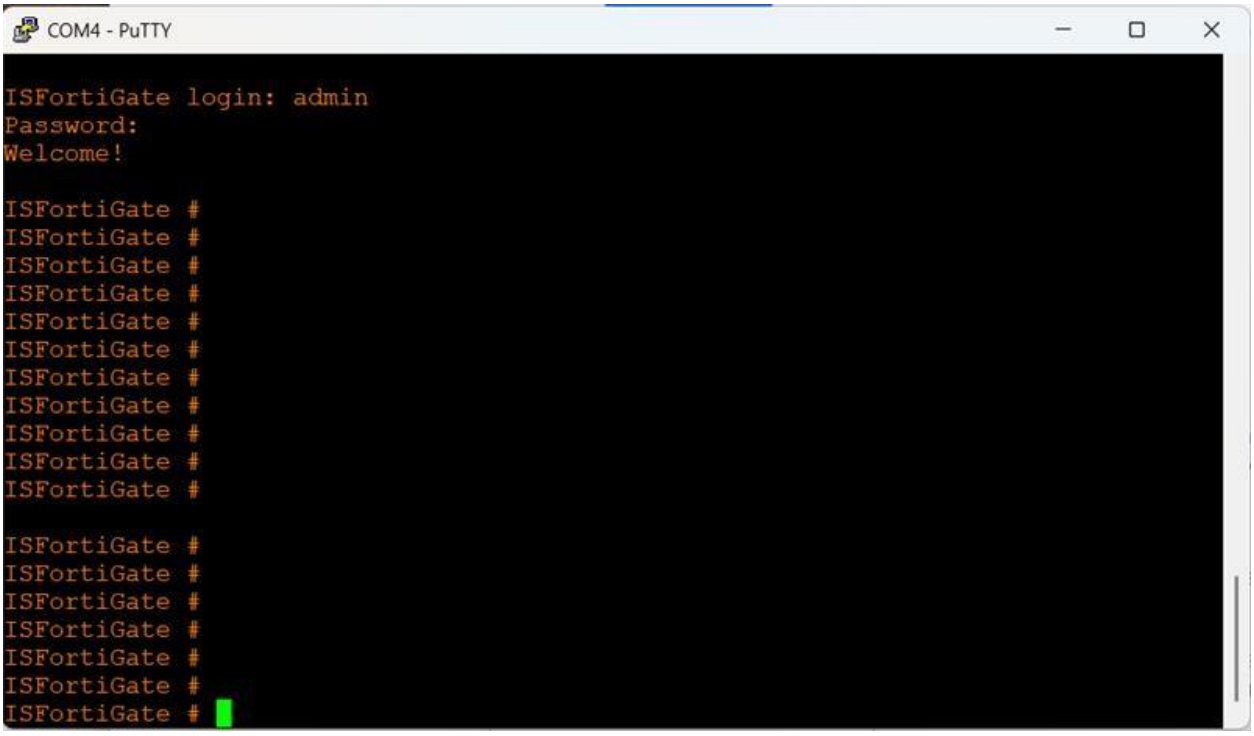


Image 2 (CLI - PuTTY Login)

Using the console cable, the firewall was accessed via PuTTY and logged into with default credentials. The password was changed through the CLI interface, and a reset was performed before moving on to GUI work.

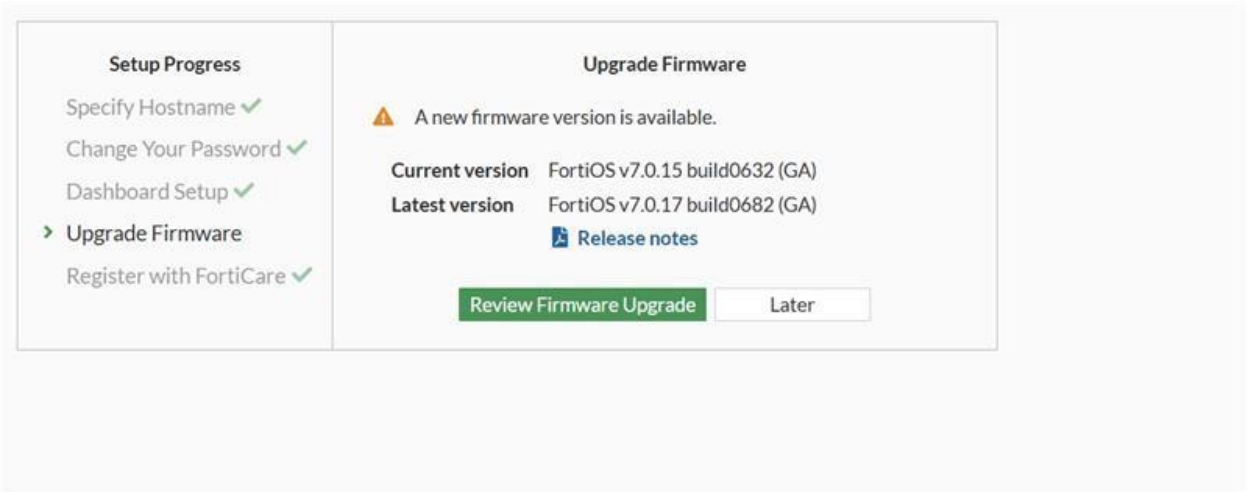


Image 3 (Firmware Upgrade Prompt)

After logging into the GUI again, FortiOS notified that a newer firmware version (v7.0.17) was available. The upgrade process from v7.0.15 was done through the web interface.

Afterwards however, the upgrade process was completed even further and updated to v7.4.0 which required a new access point.

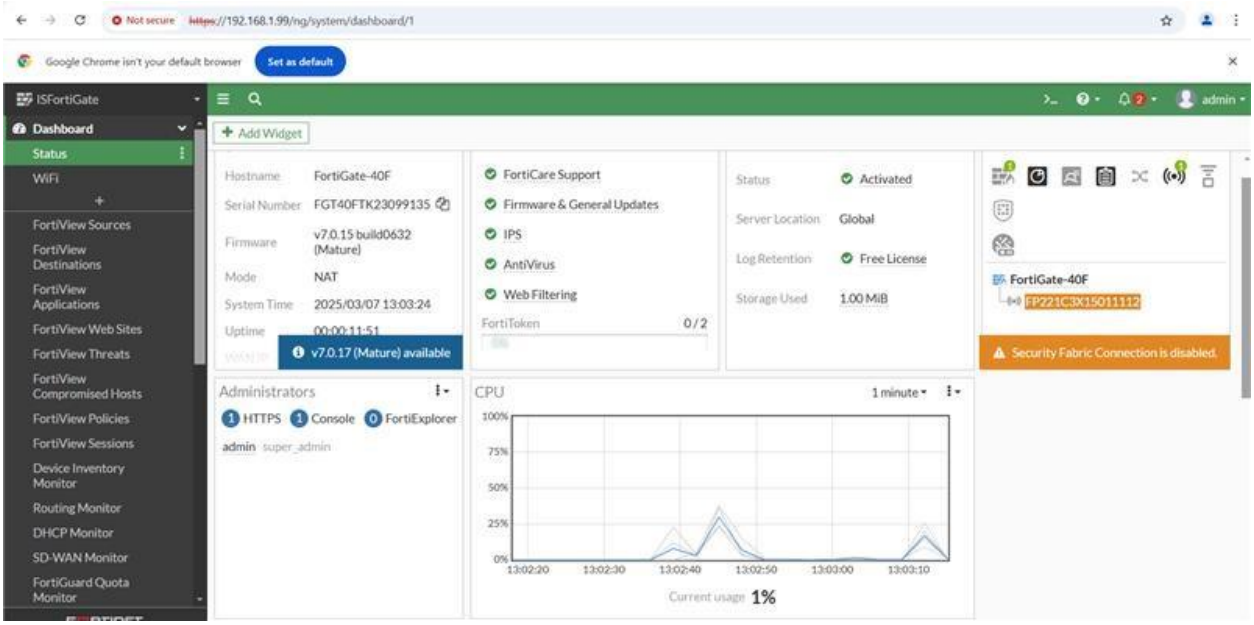


Image 4 (Main Dashboard)

This is the main screen showing the firewall's operational status post-update. Information like firmware version, NAT mode, uptime, CPU usage, and admin access methods are all visible here. The firewall also shows that the Security Fabric Connection is disabled at this point.

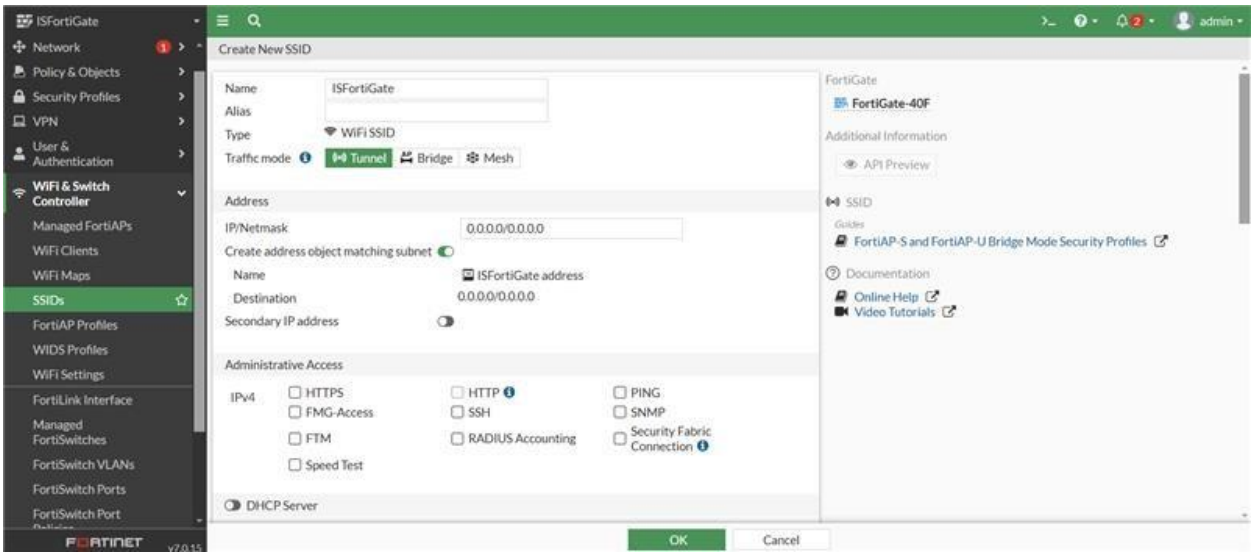


Image 5 (Creating New SSID - ISFortiGate)

The first Wi-Fi SSID was configured with tunnel mode and no IP address set manually yet. It was named ISFortiGate and prepped for administrative access via selected protocols.

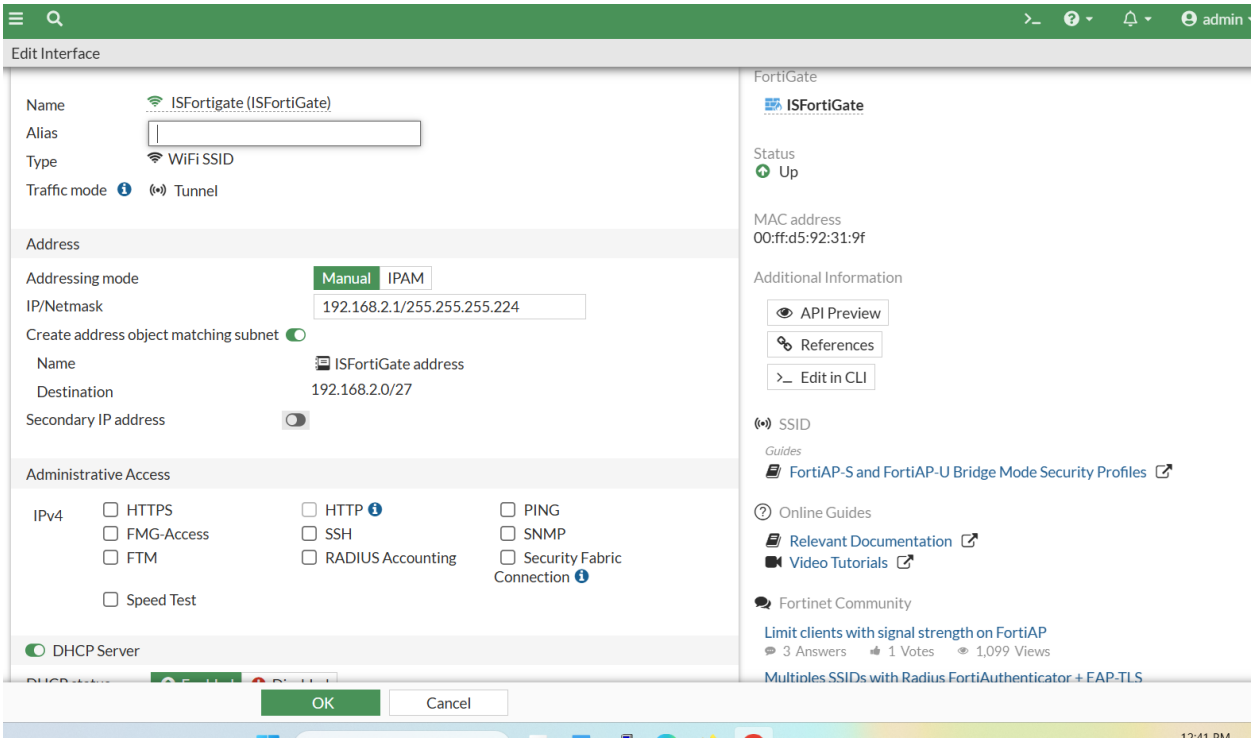


Image 6 (SSID with Static IP - ISFortiGate)

This is the same ISFortiGate SSID but this time with its IP manually set to 192.168.2.1/27. This was for open network access where only a password is required to connect.

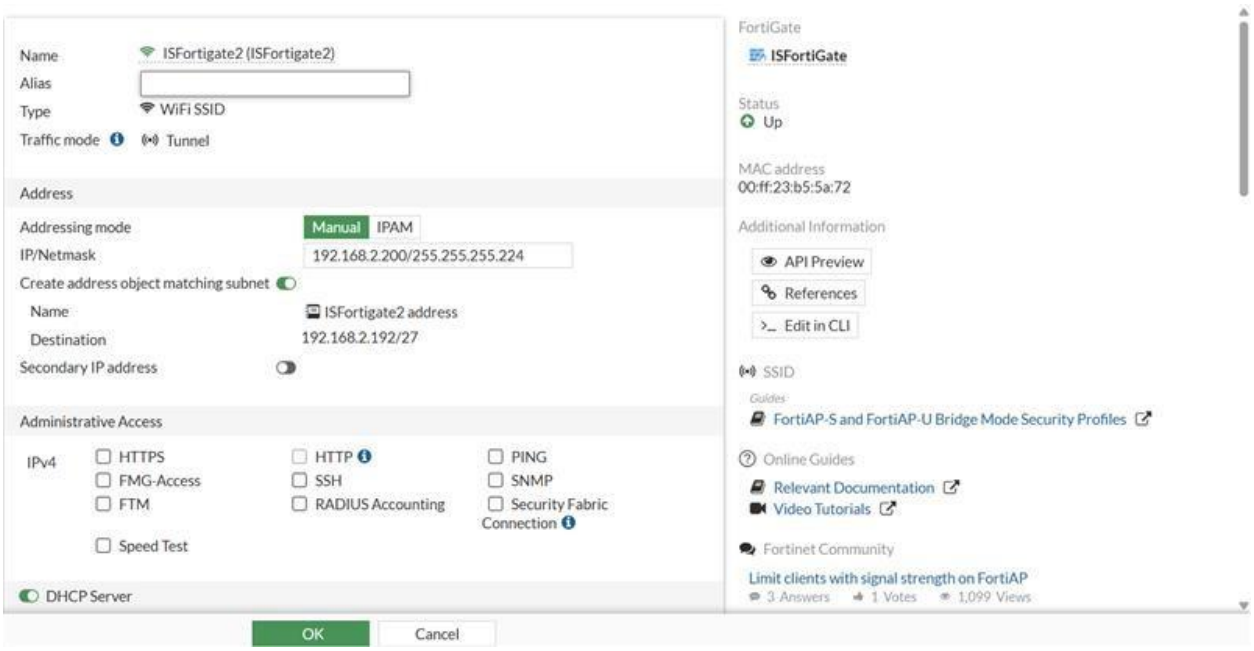


Image 7

(SSID with Static IP - ISFortiGate2)

A second SSID named ISFortiGate2 was created with the IP address 192.168.2.200/27. This was for enterprise-style access where users authenticate with both a username and password. DHCP was enabled here.

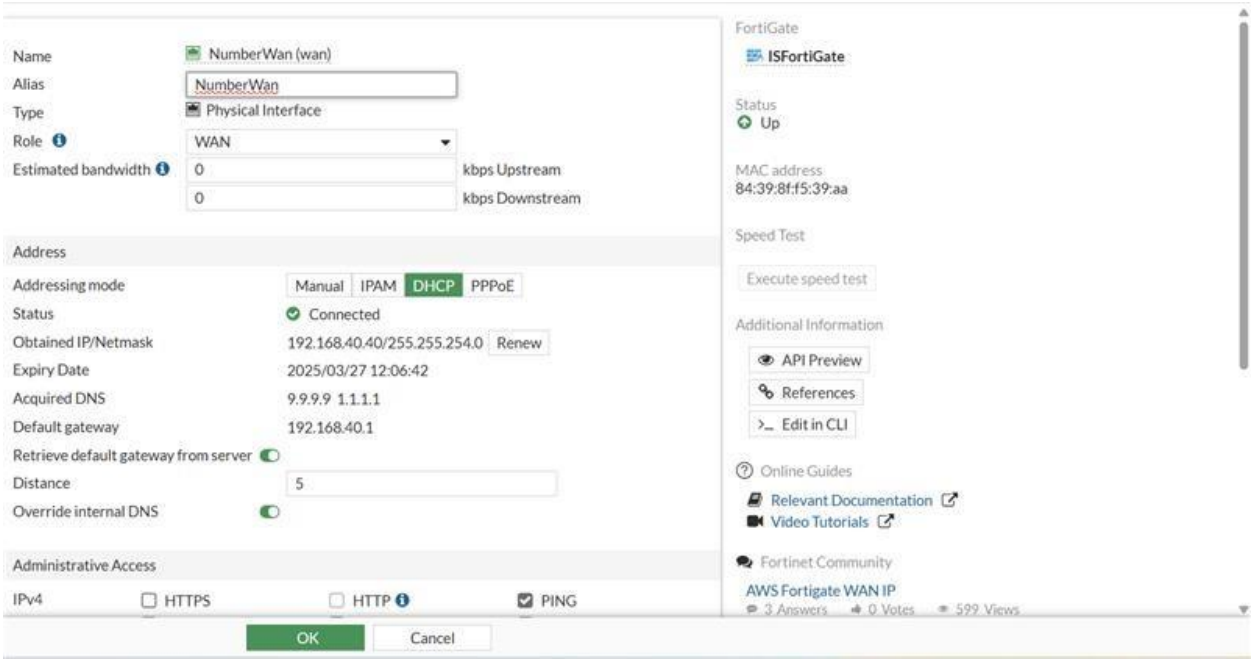


Image 8 (WAN Interface Settings)

The WAN interface named NumberWan was configured with DHCP. The device successfully pulled IP 192.168.40.40 and used public DNS servers 9.9.9.9 and 1.1.1.1.

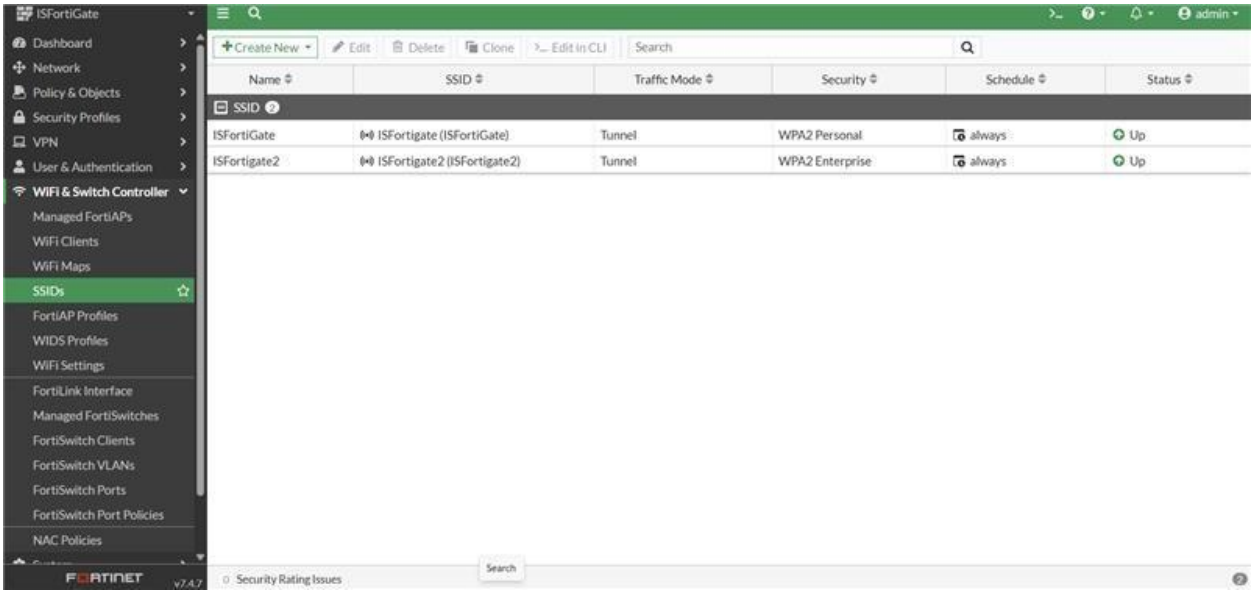


Image 9 (Overview of Wireless Networks)

This SSID page under WIFI and Switch Controllers shows both networks ISFortiGate and ISFortigate2, person and enterprise respectively. Both of the status's are up.

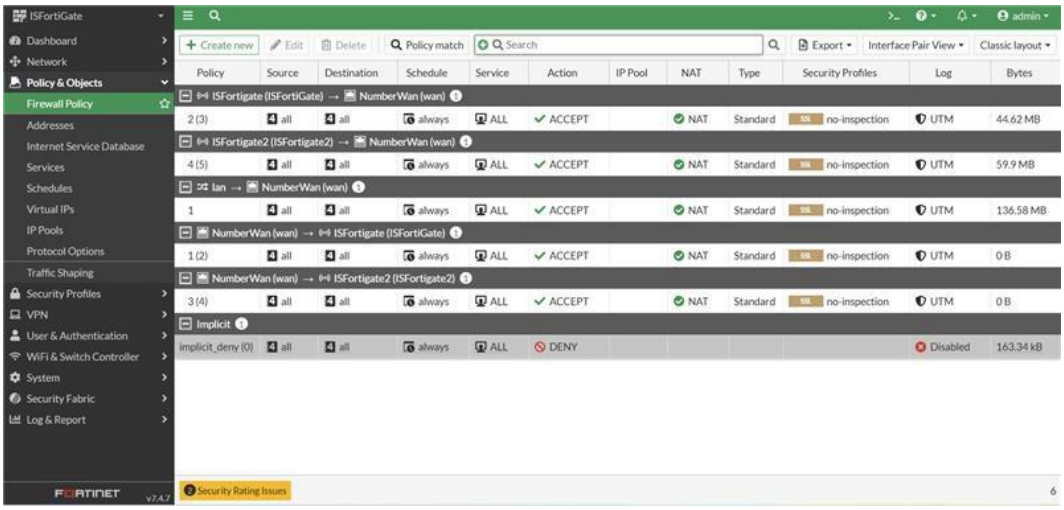


Image 10 (Firewall Policies)

Finally, firewall policies were created to allow traffic between interfaces. For example,

policies were made to allow both ISFortiGate and ISFortiGate2 to communicate to the WAN and vice versa. NAT was enabled, and SSL inspection was set to no-inspection.

Image 11 (Wireless Client Overview)

Here, the two iPhones are connected to the Wi-Fi networks are visible. The dashboard shows the SSID each is connected to, their IPs, and how much bandwidth each is using. Signal strength and frequency bands (5 GHz, 802.11ac) are also shown.

Conclusion:

This lab gave a complete overview of deploying wireless access in a Fortinet firewall environment. From CLI work to SSID creation and live mobile testing, it covered both back-end configuration and front-end validation. The experience showed how simple yet powerful Fortinet can be for small office wireless setups.

Fortinet Firewall RDP Configuration

Purpose:
The purpose of this lab was to remote into another PC through the VPN tunnel that was configured in the previous lab. The idea was to build off the VPN site-to-site by using Remote Desktop Protocol (RDP) to fully control another system in a different LAN. This lab was more focused on Windows settings, IP addressing, and user creation. It showed how to use a private IP address inside a VPN to connect across networks without using a public IP. We created a new user on the remote PC, gave them admin permissions, and then used the built-in RDP app to fully remote in. This was the second part of the two-part VPN lab and made it feel real because we could actually control the other PC.

Background Information on Lab Concepts:

Fortinet is a huge player in the network security space, especially when it comes to delivering an all-in-one solution. While people often think of firewalls like Palo Alto when they think “enterprise security,” Fortinet does things a bit differently. Their approach is more about building out an ecosystem where everything works together under one management system: switches, firewalls, access points, and even endpoint security. They call this the Security Fabric, and it really shows in labs like this one.

The firewall used in this lab, the FortiGate 40F, is meant for small businesses or branch offices. But don’t let the size fool you, it comes packed with features that would normally be spread across multiple devices. In this one lab, it handled DHCP, Wi-Fi controller duties, NAT, security inspection, firmware management, and policy enforcement, all from the same GUI. Compared to Palo Alto’s PA-220, which is strong in deep packet inspection and app control, the 40F feels a little more user-friendly and way faster to set up for a full wireless deployment.

One of Fortinet’s biggest strengths is how seamless the Wi-Fi side of things is. You don’t need an extra wireless controller , you just connect a FortiAP and everything shows up under the same dashboard. You can configure SSIDs, assign static IPs, monitor bandwidth per device, and set up NAT and security profiles, all in one place. The wireless features even include tunnel and bridge modes, so you can route traffic exactly how you want.

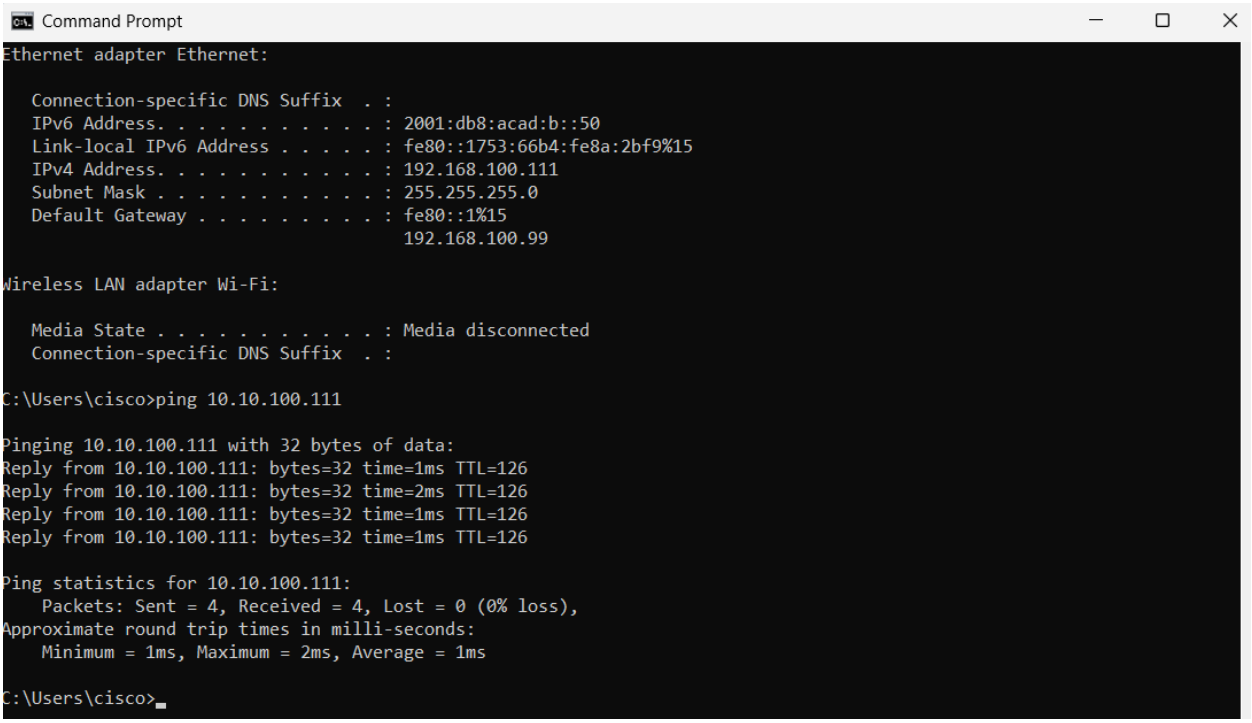
Problems:
The first problem we ran into was that Remote Desktop wasn’t enabled on the target PC. Even though everything with the VPN was working and the firewall allowed traffic, we couldn’t connect until we went into the system settings and turned on Remote Desktop manually. That step took a little while to figure out because it wasn’t a networking issueit was a setting inside the settings of the PC.
The second issue was that there wasn’t a user profile created for the person we were trying to remote in as. We had to go into user settings, create a new account named "advik," and then give

that user administrator privileges. Without that, the RDP login wouldn't accept the credentials. Once both of those were fixed, the connection went through instantly.

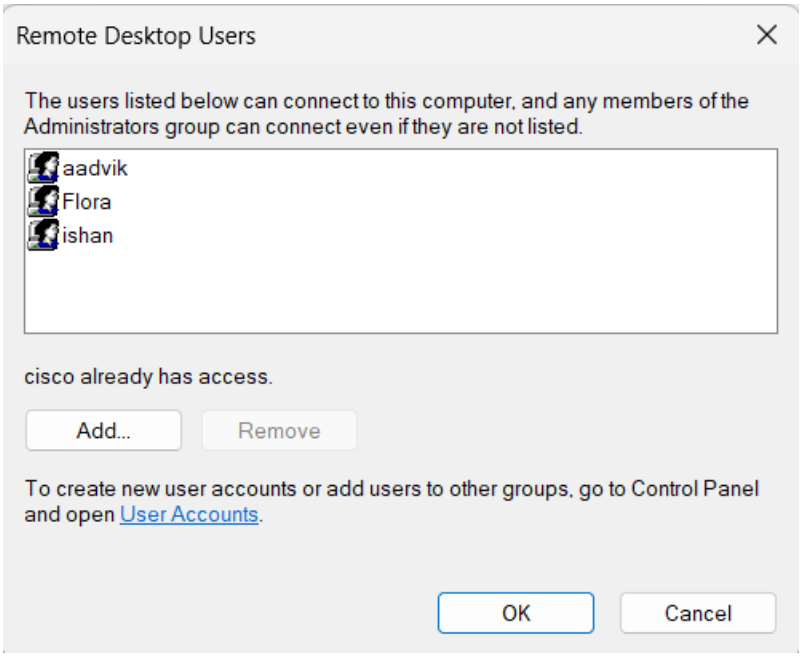
Lab Summary:
This lab was focused on setting up Remote Desktop over a working VPN tunnel. On Advik's PC, we created a user account named "test" and made sure Remote Desktop was enabled in settings. We gave the account a password and made it an admin. Then, from Advik's PC, we opened Remote Desktop Connection and typed in our private IP address (192.168.100.111). After entering the username and password, we accepted the connection on our end and it successfully logged in.

Lab Commands (The captions reference the image ABOVE)

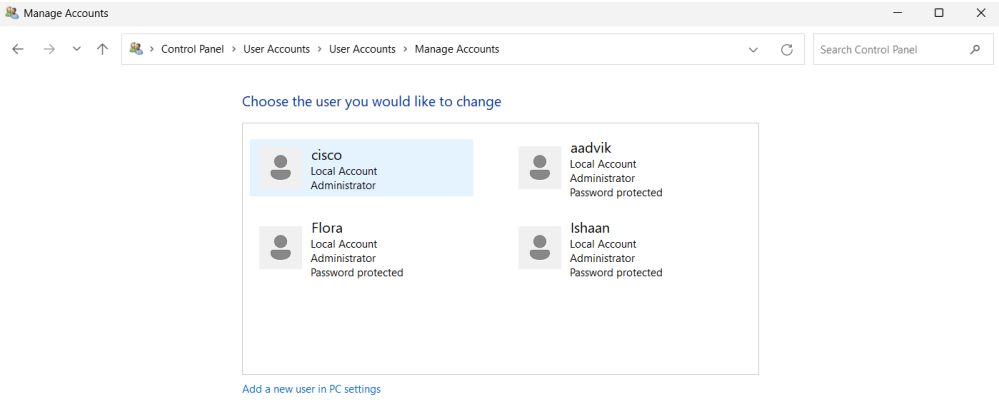
This screenshot shows the ping from our PC at 192.168.100.111 to Advik's PC at 10.10.100.111. All packets were received with 0% loss, TTL was 126 and average time was 1ms, showing that the VPN tunnel was working and the machines could talk before trying Remote Desktop.



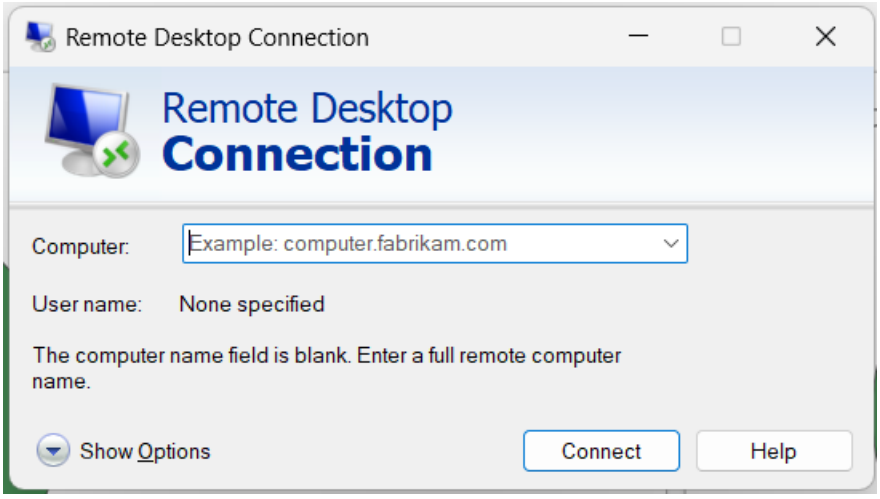
This screenshot is from Advik's PC, under remote desktop user settings. It shows that aadvik, Flora, and Ishaan are added as users who can connect. This step was one of the problems we faced, Advik had to add himself as a remote desktop user before we could connect.



This is the user account panel in Control Panel. It shows all local accounts created on Advik's machine. We used this to confirm that the aadvik user account was active and had administrator access.



This is the Remote Desktop client on our PC. Advik typed our IP address into this window to connect. Once all settings were fixed (RDP enabled, user profile created), the connection worked. 192.168.100.111 was our PC address that was typed into the box. This RDP connection was on advik's computer.



Fortinet Firewall Inter-VLAN VPN

Purpose:

The purpose of this lab was to establish a site-to-site Virtual Private Network (VPN) between two PCs located on separate Local Area Networks (LANs) but within the same Wide Area Network (WAN). The goal was to create a secure, encrypted communication channel between the two systems using Fortinet firewalls. This setup enables secure data transfer, improved network segmentation, and supports remote collaboration, key principles in modern network engineering. The lab covered GUI-based VPN configuration using FortiGate's IPSec Wizard, static routes, address objects, and firewall policies, along with basic validation using command-line tools like ping. This exercise reinforced networking concepts learned in CCNA and served as the first half of a two-part lab, with remote desktop access built on top of the VPN in the second part.

Background Information on Lab Concepts:

Fortinet is a huge player in the network security space, especially when it comes to delivering an all-in-one solution. While people often think of firewalls like Palo Alto when they think "enterprise security," Fortinet does things a bit differently. Their approach is more about building out an ecosystem where everything works together under one management system: switches, firewalls, access points, and even endpoint security. They call this the Security Fabric, and it really shows in labs like this one.

The firewall used in this lab, the FortiGate 40F, is meant for small businesses or branch offices. But don't let the size fool you, it comes packed with features that would normally be spread across multiple devices. In this one lab, it handled DHCP, Wi-Fi controller duties, NAT, security inspection, firmware management, and policy enforcement, all from the same GUI. Compared to Palo Alto's PA-220, which is strong in deep packet inspection and app control, the 40F feels a little more user-friendly and way faster to set up for a full wireless deployment.

One of Fortinet's biggest strengths is how seamless the Wi-Fi side of things is. You don't need an extra wireless controller , you just connect a FortiAP and everything shows up under the same dashboard. You can configure SSIDs, assign static IPs, monitor bandwidth per device, and set up NAT and security profiles, all in one place. The wireless features even include tunnel and bridge modes, so you can route traffic exactly how you want.

Problems:

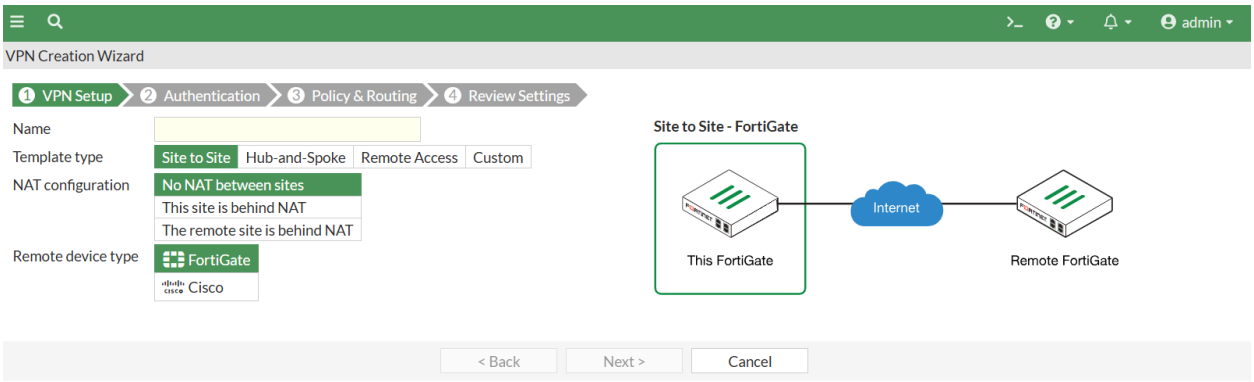
The first major issue we encountered was with subnet configuration. Initially, both of the PCs were set within the same subnet range of 10.10.100.blank, so then we had to change one of the sides. To resolve this, we changed our PC in control panel to 192.168.100.blank so that the subnets were overlapping.

Also, another problem that we faced was we forgot to reverse the initial firewall policy from LAN to the remote subnet (To_Advik). After, when we tried pings, they were not working and that was because the tunnel was not bidirectional. It was a simple fix that took a little bit of troubleshooting; on the firewall policy tab under policies, just right click “Reverse Firewall Policy”. This automatically generated the return policy so that the tunnel worked both ways, immediately after, the pings across the board worked.

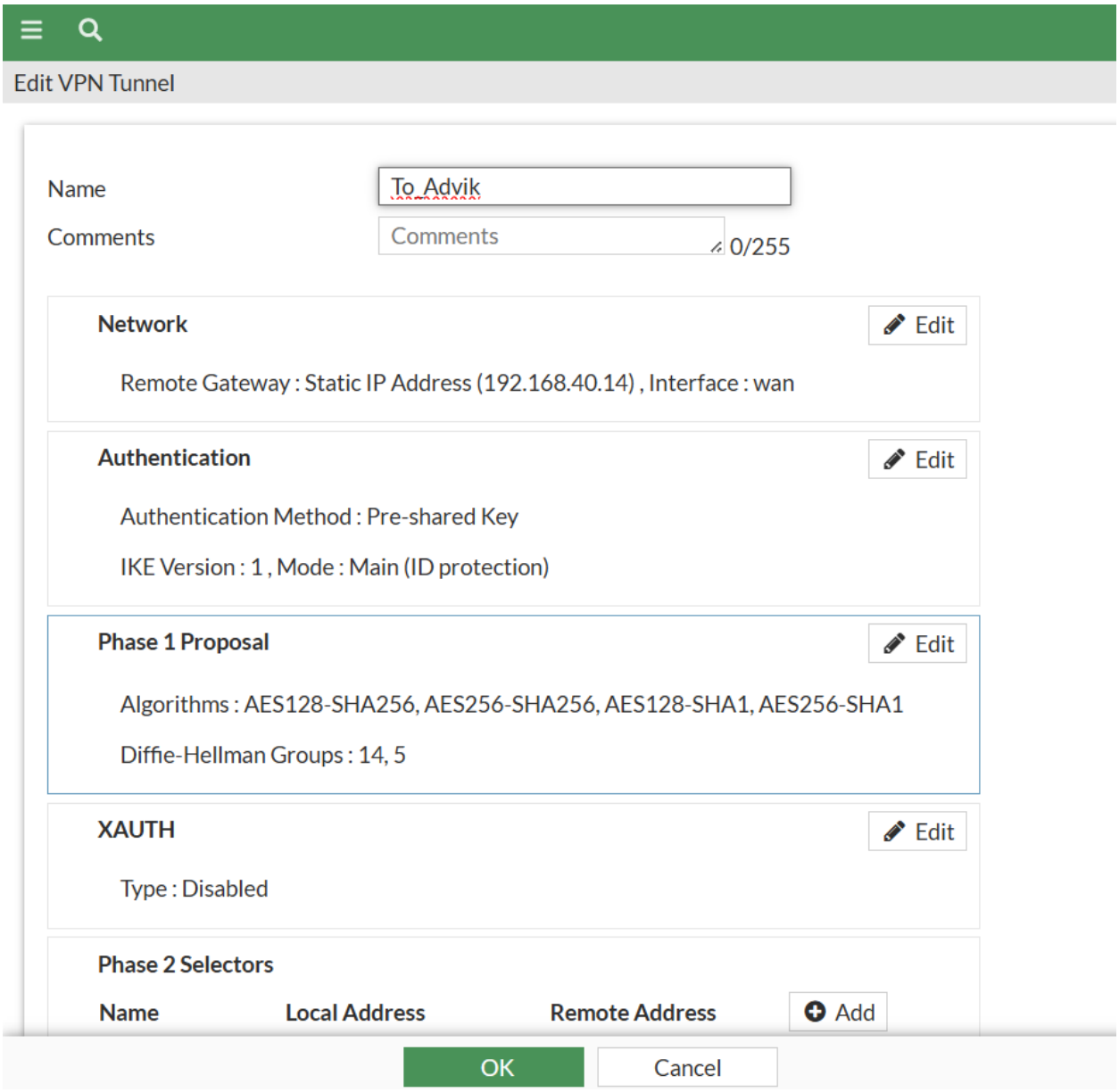
Lab Summary:
This lab focused on setting up a site-to-site VPN between two Fortinet firewalls on the same WAN. I configured tunnels using the IPsec wizard, set static routes, and created firewall policies to allow traffic. Subnets were changed to avoid overlap and policies were reversed to enable bidirectional communication. The connection was verified using ping.

Lab Commands (The captions reference the image ABOVE)

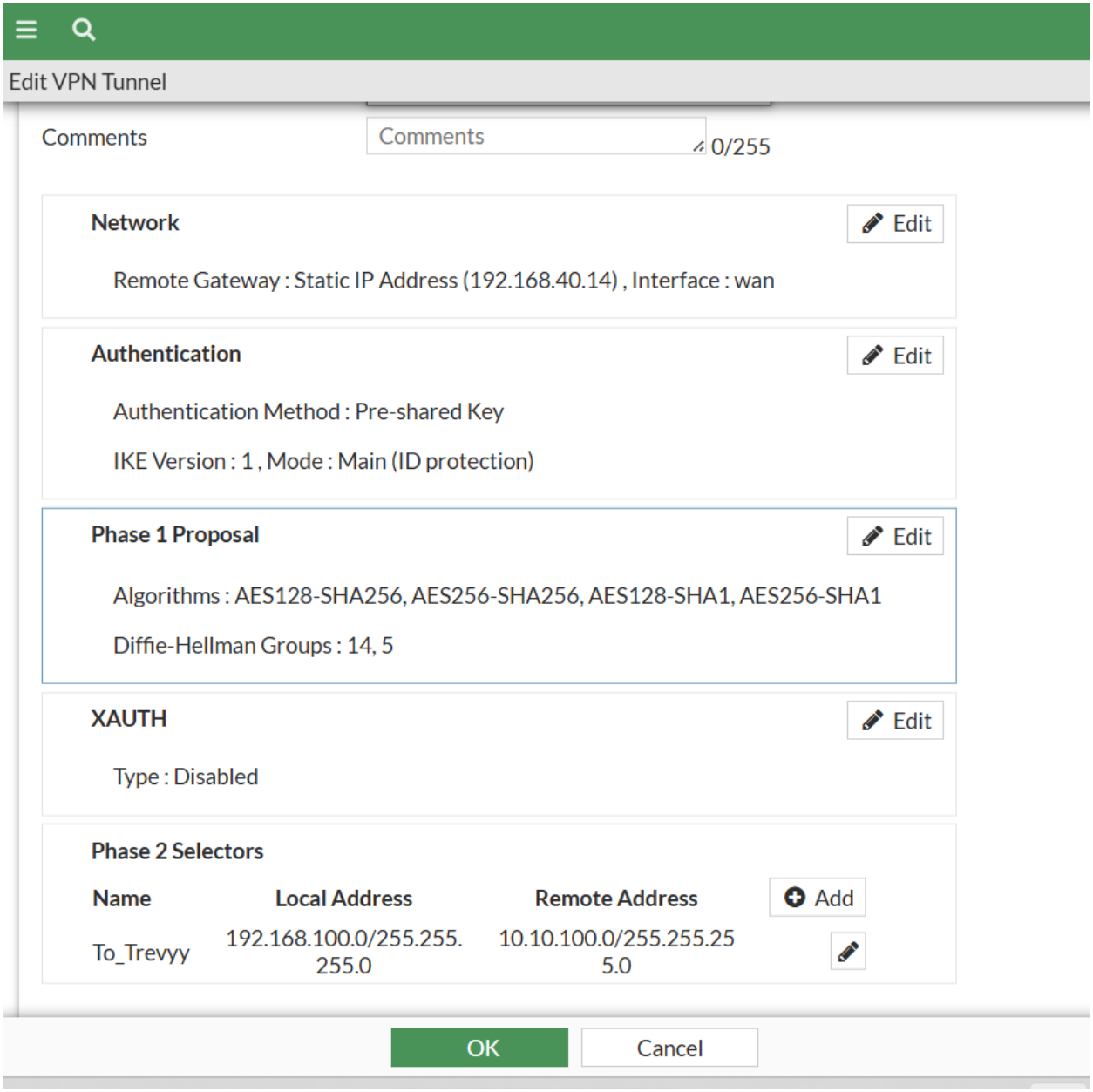
Initial VPN setup using the built-in Fortinet wizard. Custom and "No NAT between sites" are selected with FortiGate as the remote device. As the steps go through, it just clicking next through authentication, policy and routing, and review.



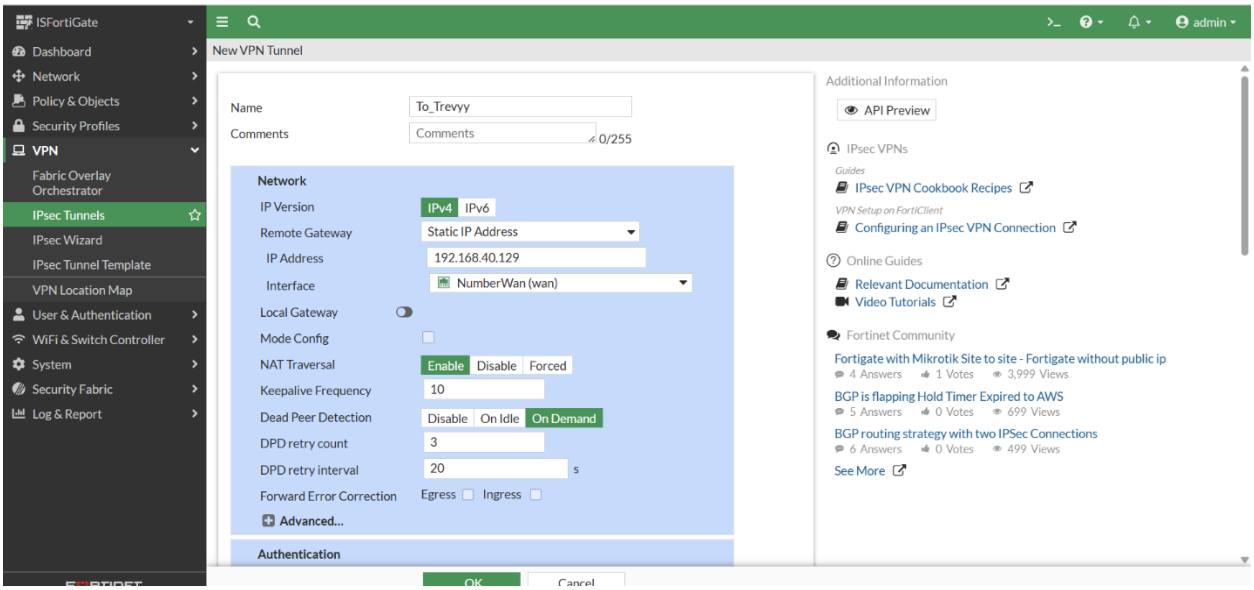
This screenshot is crucial. This is after finishing the steps for the VPN wizard; this is the VPN tunnel and creating it. Configuring this IPSec VPN Tunnel named To_Advik with a static IP Gateway, AES encryption algorithms, and Diffie-Hellman groups. Also, the static IP address is the interface address on OUR firewall, (the WAN interface).



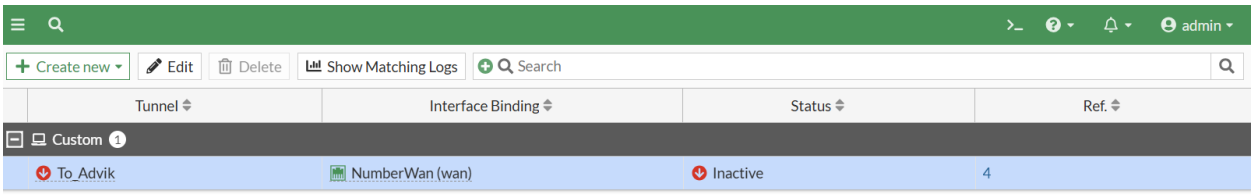
This is the second phase of creating the VPN Tunnel. This screenshot includes both the local address subnet and the remote address subnet. As stated earlier, the subnet for our LAN is 192.168.100.x and the remote is 10.10.100.0, specifically, our PC used DHCP as set in the control panel to be 192.168.100.111, the remote address was 10.10.100.111.



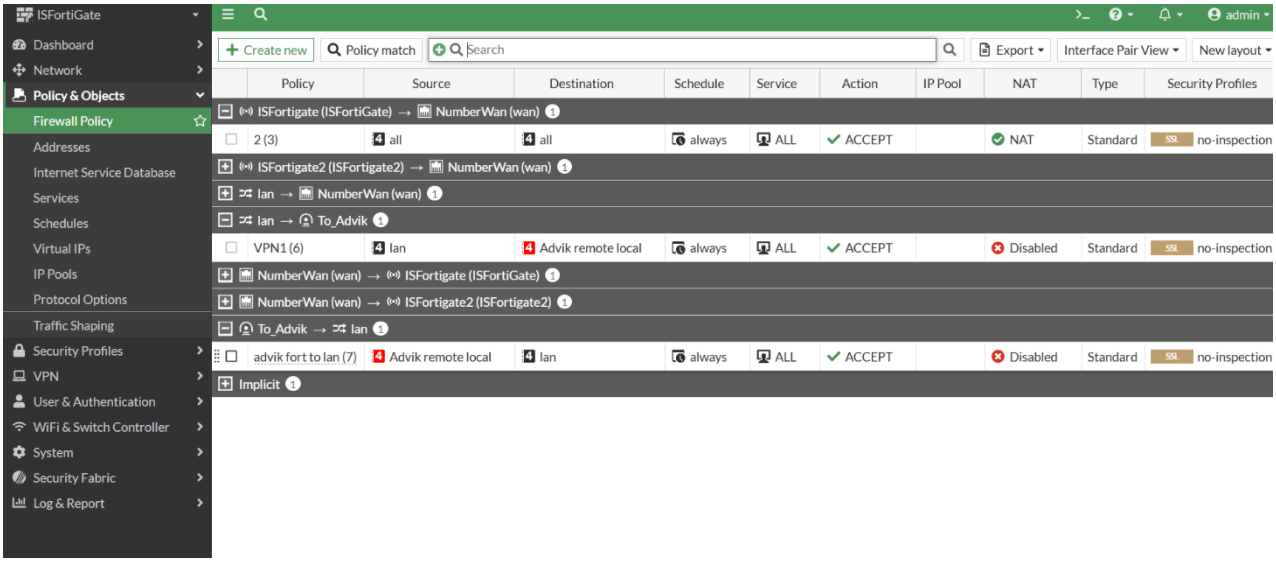
This next screenshot is creating a New VPN Tunnel that was configured in the last 2 screenshots. The IP address of the remote gateway is the IP on the WAN interface of the other PC's LAN's firewall. In this case it was 192.168.40.129. All of the IP's in the room are on the same WAN. The interface that it leaves our firewall is NumberWan which was configured in the SOHO lab. NAT traversal is automatic for any address translations, dead peer detection is on as well to find any PC's or devices that are down in the network.



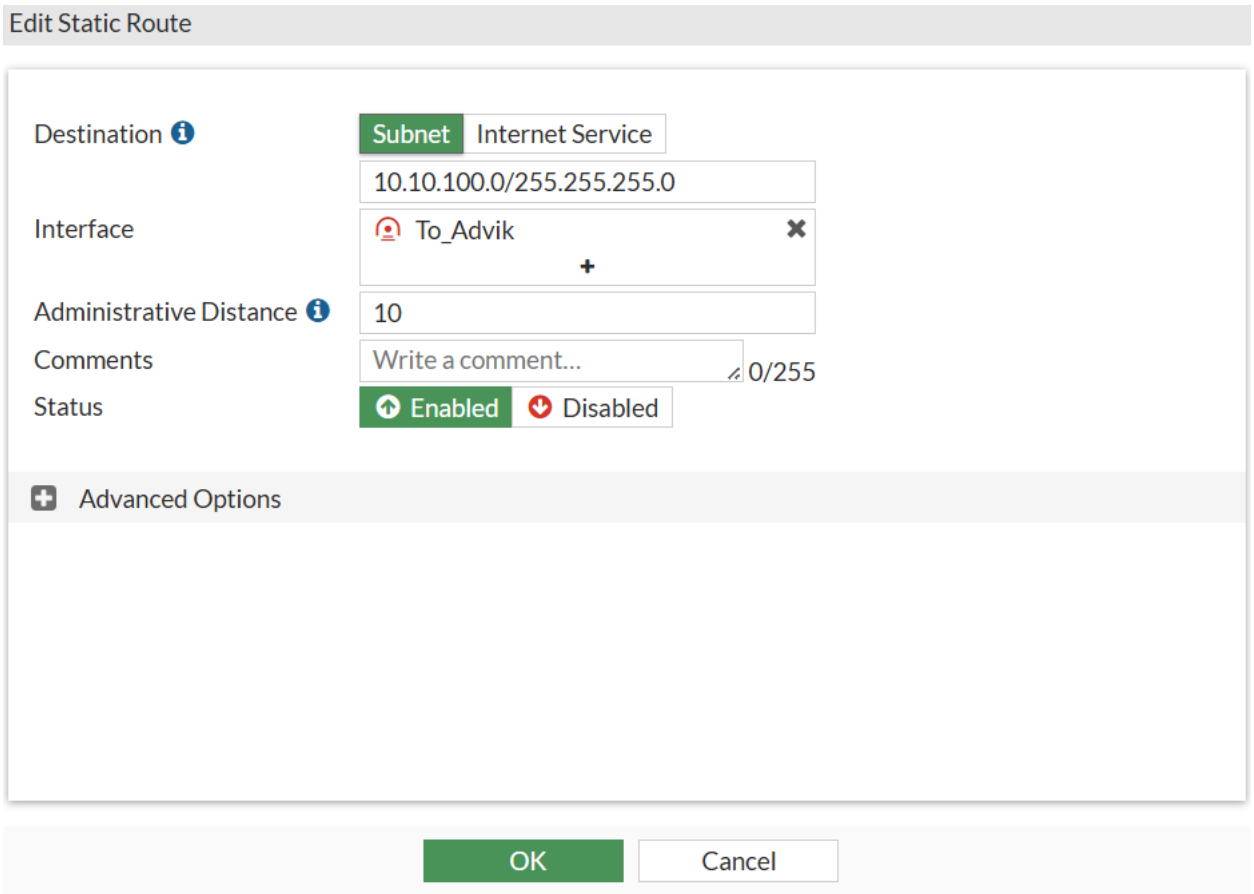
This screenshot is the tunnels that are finally created. It is currently inactive in this screenshot but after right clicking and clicking enable, it goes up and becomes active. This screenshot is the end result of the VPN Tunnel created in the last screenshot from the interface NumberWan to To_Advik which is 192.168.40.129.



This screenshot is probably the most important step. The firewall policies is what enables communication between both VPN's and clearly show what data get transferred. Here, there are 3 firewall policies that are important. Firstly, ISFortigate to NumberWan, this policy grants access to the WAN port of the firewall and sends data through there. The next policy is from our LAN to Advik's PC, this is a finished VPN tunnel that was created previously. The last one is the problem that we encountered in the problems section, it just confirms that data is bidirectional between the firewalls. To create it, just reverse the firewall policy that was created before.



This is the last step, once the static route is created from our firewall to Advik's personal LAN subnet/interface, the data can then be sent.



Here is the confirmation of working pings across the board to Advik's PC with 10.10.100.111.

TTL is time to live and that shows how long between hops it took.