w

**Fortinet SOHO Firewall Configuration on**

**FortiGate 40F**

Ryan Chen

3/24/2025

**Purpose:**

This lab is primarily used as a starter for familiarization to the Fortinet interface as well as FortiGate configurations. Given that SOHO is a relatively easy task to setup, this is a good time to understand how Fortinet configurations work at a basic level.

Aside from Fortinet, SOHO itself is a simple lab that provides wireless connectivity to clients at a small scale, hence the name “Small Office Home Office”. This style of configuration is common for personal networks and small enterprise networks. The primary purpose of this lab is to complete basic configuration of this type of network by setting up two SSIDs: one running WPA2 Personal, and the other running WPA2 Enterprise.

**Background Information:**

Barebones configuration is commonly referred to as a SOHO or Small Office/Home Office setup. Traditionally, this means that the network will be used at a small scale for a limited number of clients. As a result, the config is robust at a small scale, and easy to setup. Despite these advantages, SOHO networks are often limited in future growth and must be upgraded to support anything larger scale.

Before utilizing a firewall, configuration must be done in order to prepare the device for use by clients. This involves setting up Dynamic Host Configuration Protocol (DHCP) to automatically provide client machines with IP addresses, which ensures that all devices can reach to the internet.

Our lab makes use of an upstream internet provider that already has DHCP leasing system set up for its clients. Thus, as a client, we can configure the firewall to receive a DHCP address on a specified interface, and then internally host a DHCP server to provide local clients with internet access. This would mimic a normal scenario where an ISP gives out a DHCP address for your upstream connection.

Leasing addresses is the act of giving out a specific IP address from a pool of addresses for clients connected. These addresses have a “lifespan” attribute attached to them, and after the time is up, they will need to renew another address. This ensures addresses are always moving in circulation, which is optimal in a network where devices are constantly connecting and disconnecting to the internet, such as a SOHO network.

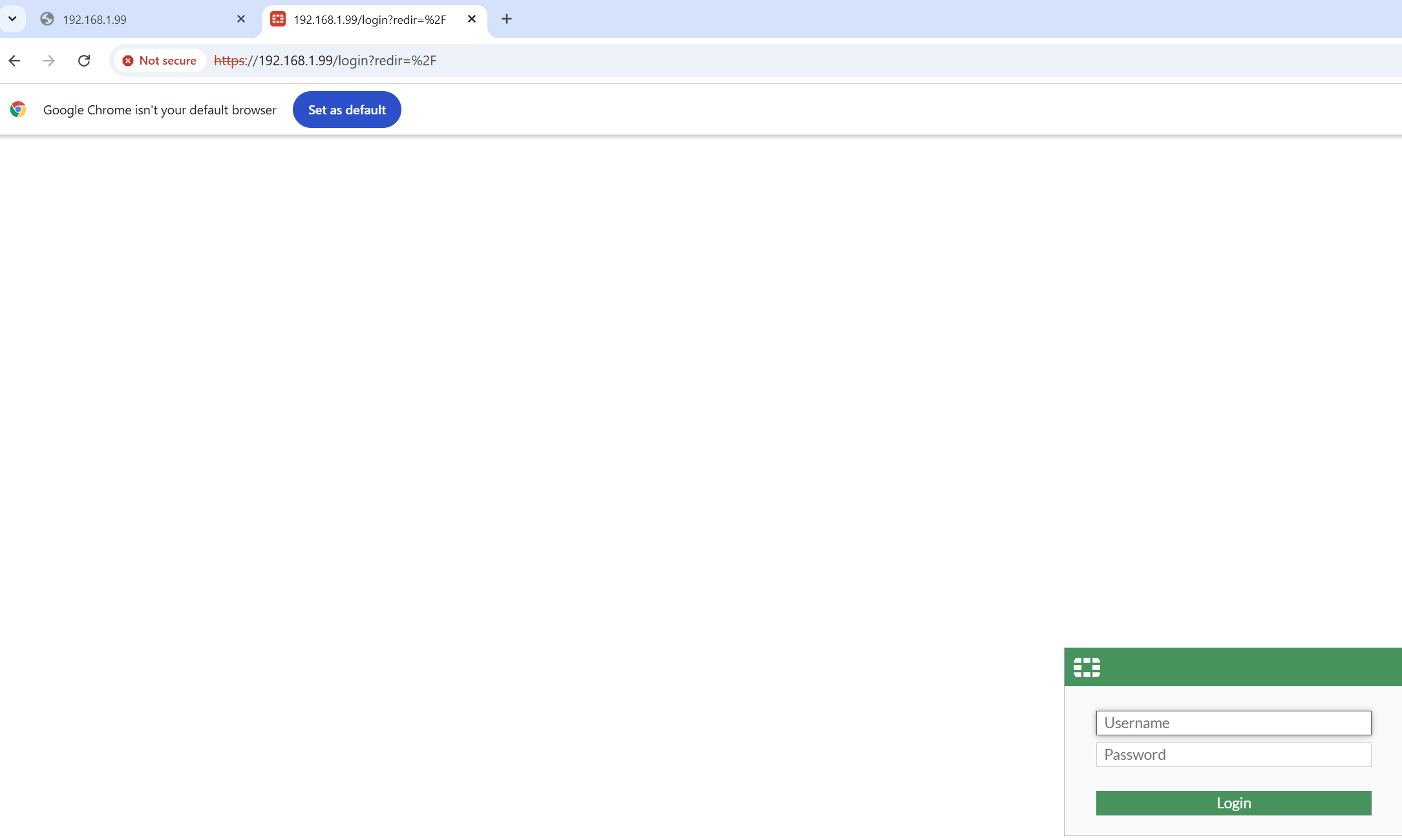
To follow best practices, we should also configure our zones accordingly, as we would have done on Palo Alto. Like configuring Security Zones on PA220 firewalls, Fortinet offers a Firewall Policy section in its configuration that allows us to set rules for SSIDs, interfaces, and much more. For the purposes of this lab, we all traffic to flow bidirectionally.

One of the primary differences between Fortinet access points and other traditional access points like Cisco ones is the ease of configuration. On Fortinet devices, access points can be configured directly by accessing the GUI of the main firewall. This provides much more accessibility because when a WAP is connected into the network of a Fortinet firewall, the firewall will be automatically detected and available for configuration. This means that instead of having to manage each AP individually over webpages, the APs can all be managed through a central firewall and GUI.

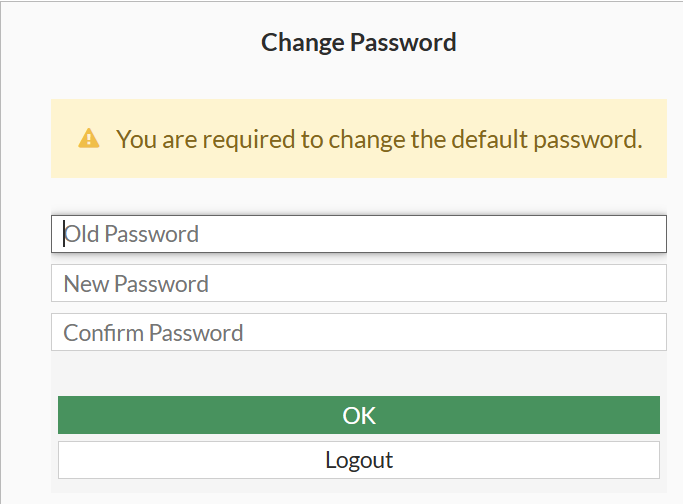
Finally, we use a local authentication setup instead of RADIUS for the WPA2 Enterprise setup used. This reduces a lot of the configuration overhead necessary for getting WPA2 Enterprise up and running, making the process a lot more simple.

**Lab Summary:**

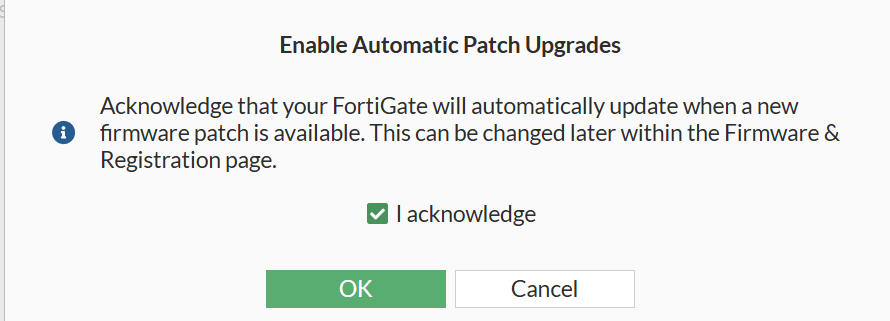
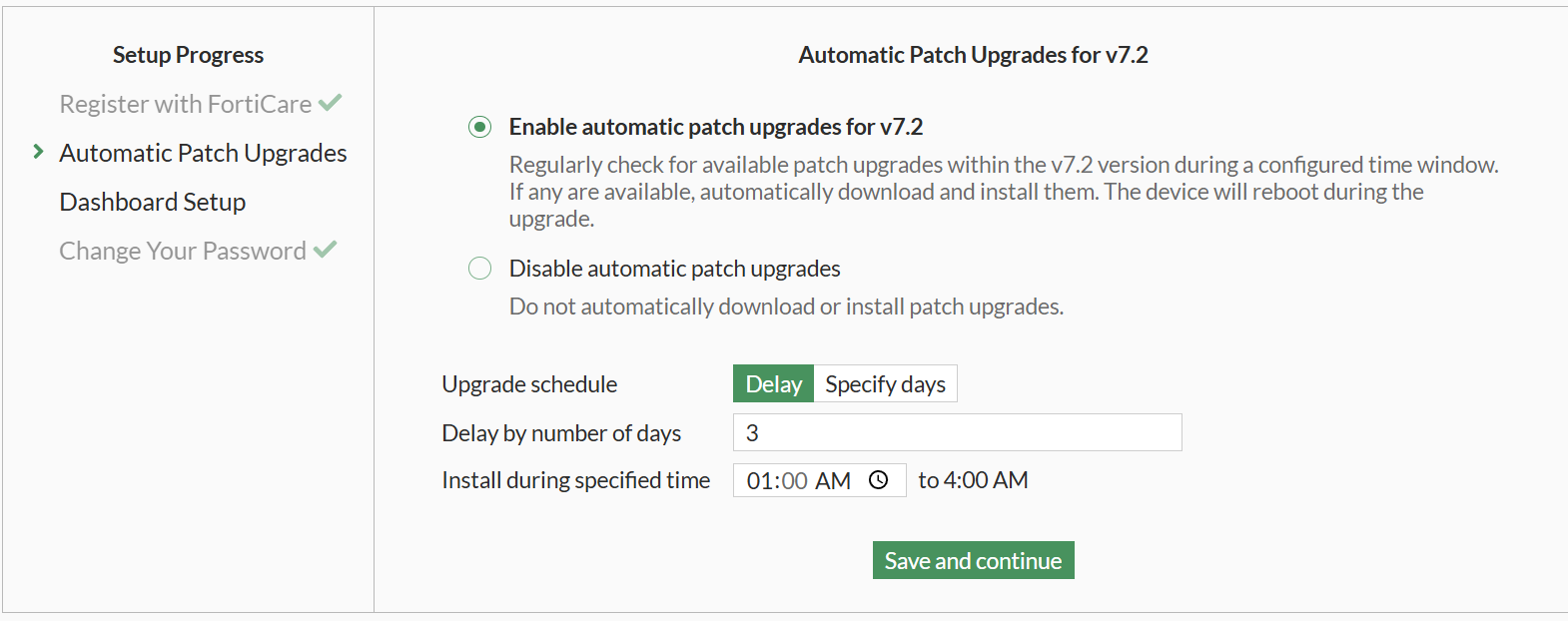
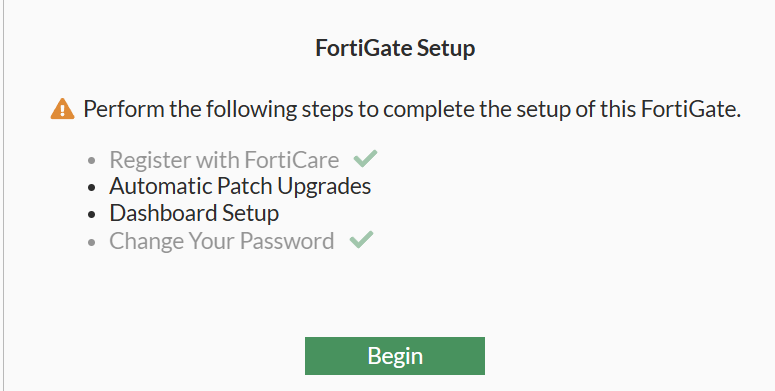
1. Head to <https://192.168.1.99> to access the firewall GUI.



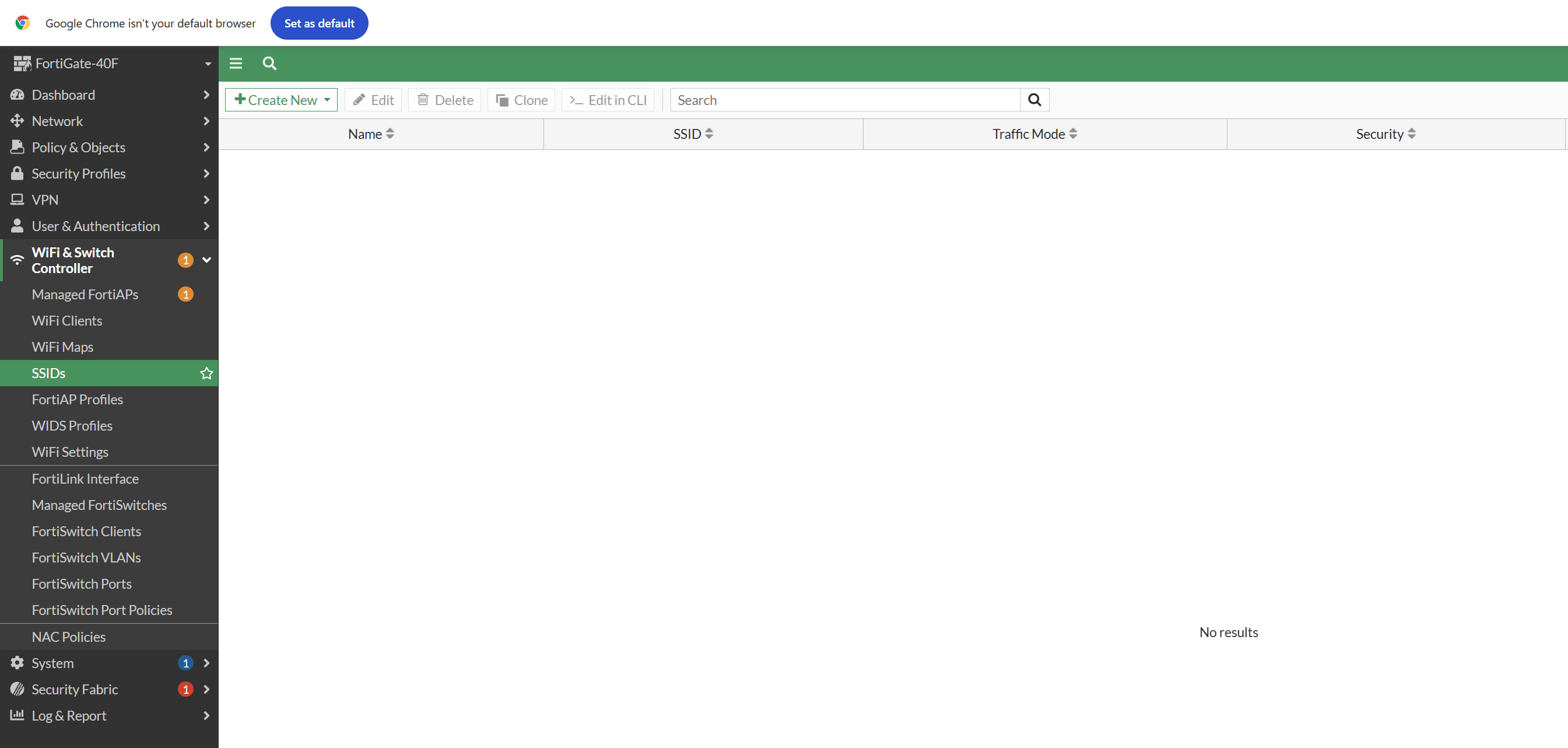
1. Enter “admin” for the username and press enter. The firewall should be wiped meaning that everything is fresh. Now, we can set our password.



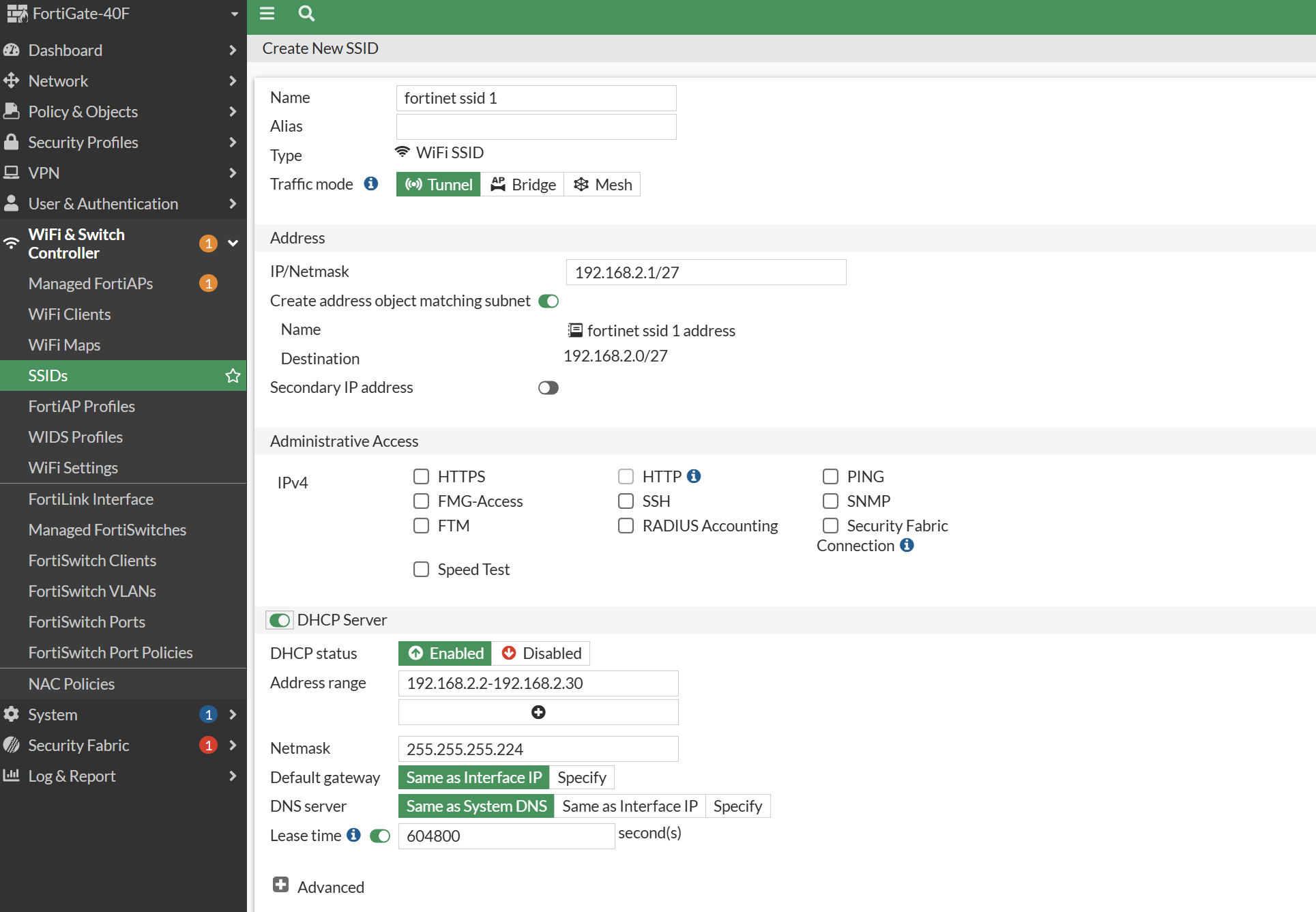
1. After setting a password, begin basic setup. This will take care of initialization of the device and other housekeeping items.



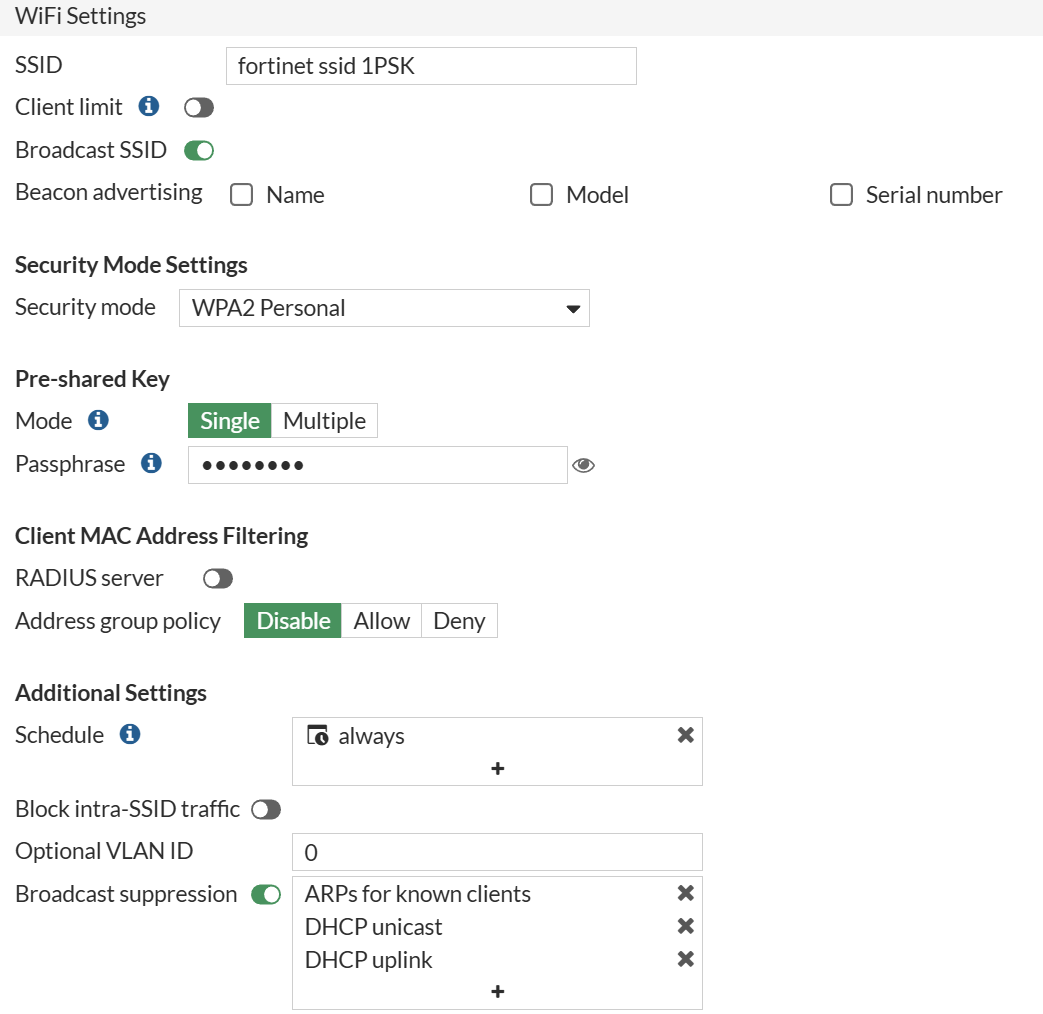
1. Once logged into the GUI, go to “Wifi & Switch Controller > SSIDs”



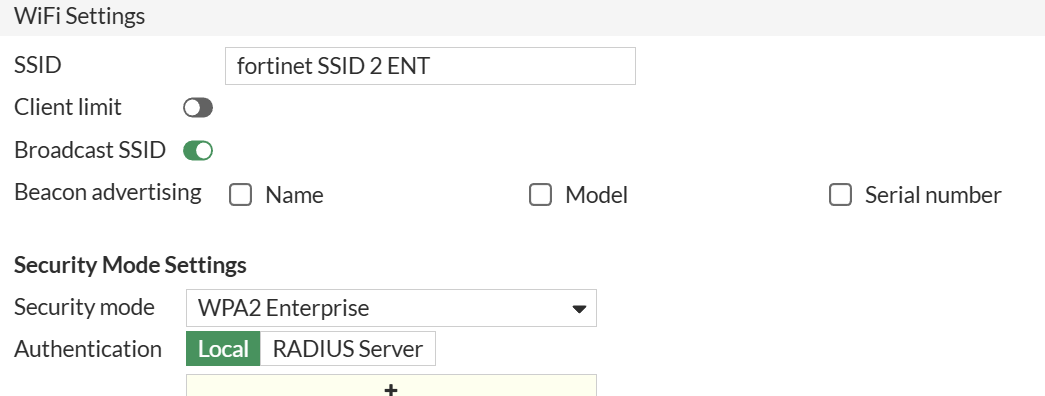
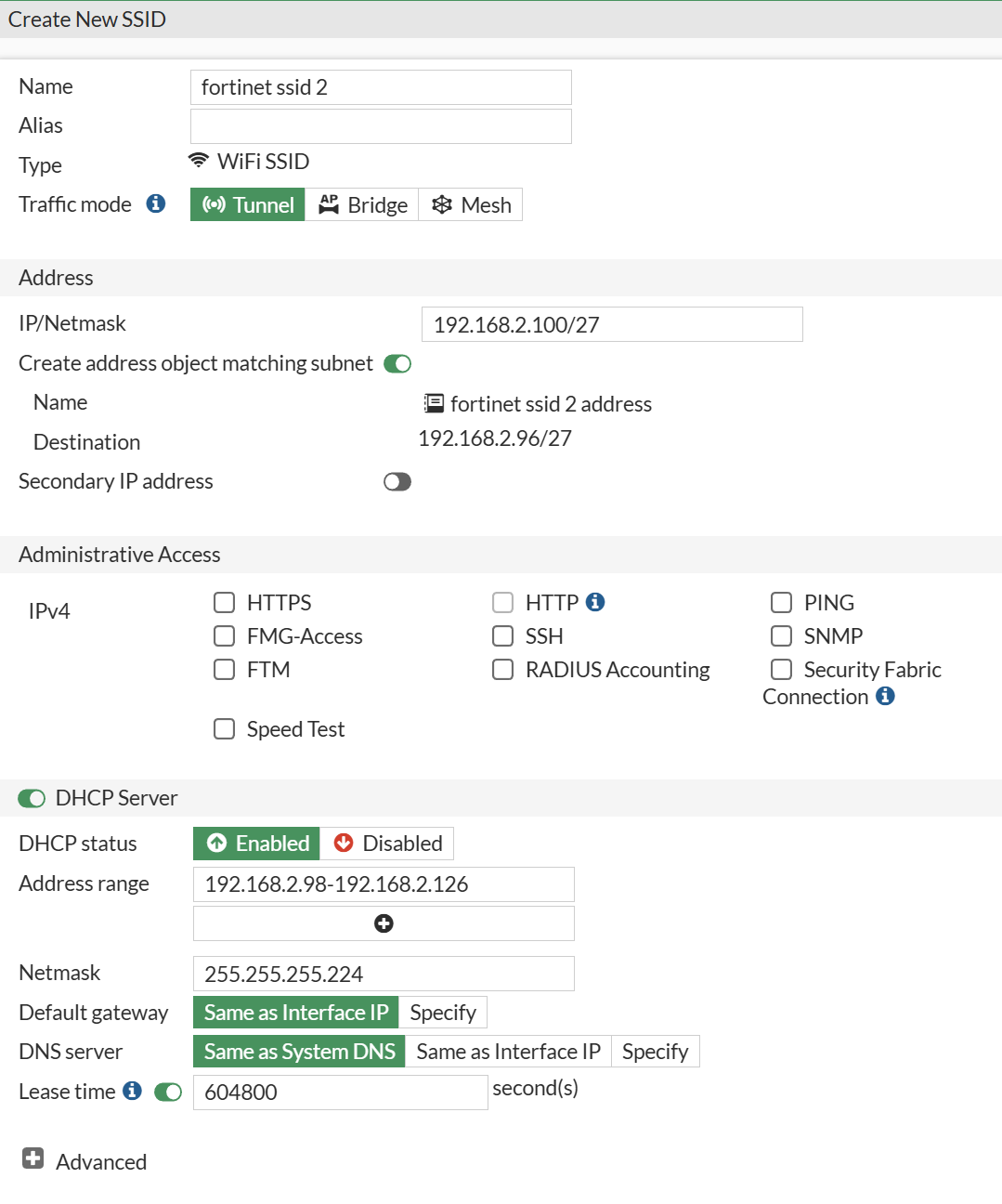
1. Create the first SSID. Add a name, and an IP/netmask that is different from the LAN IP address. This is to prevent overlapping ranges that will render the device unreachable. Also, make sure to turn on the DHCP server in order to automatically assign host IP addresses.



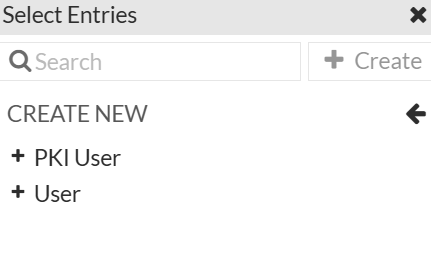
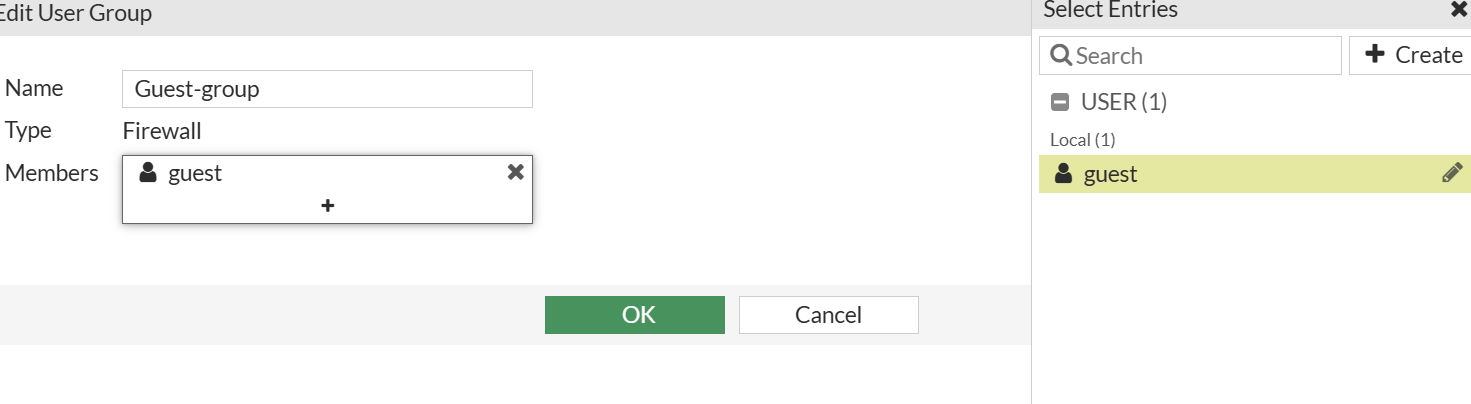
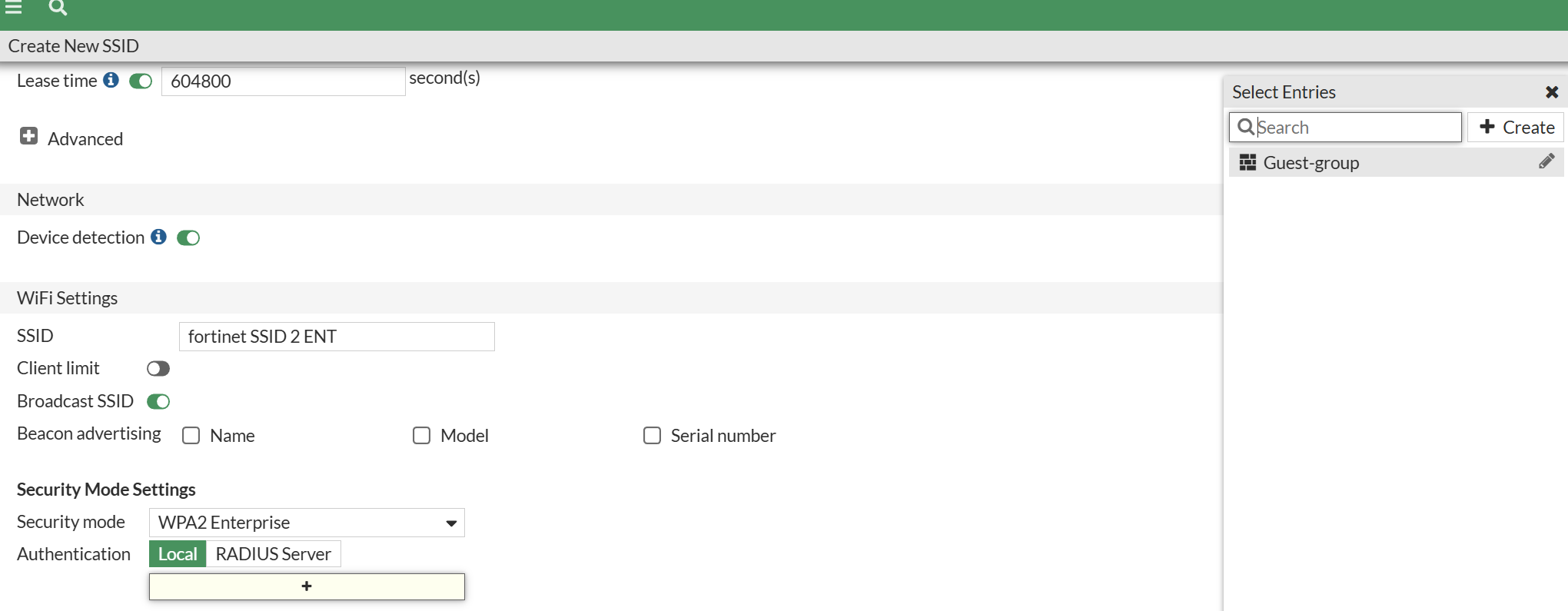
1. Set the SSID name, as well as the passphrase. Our first SSID will be WPA2 Personal, so select that item.



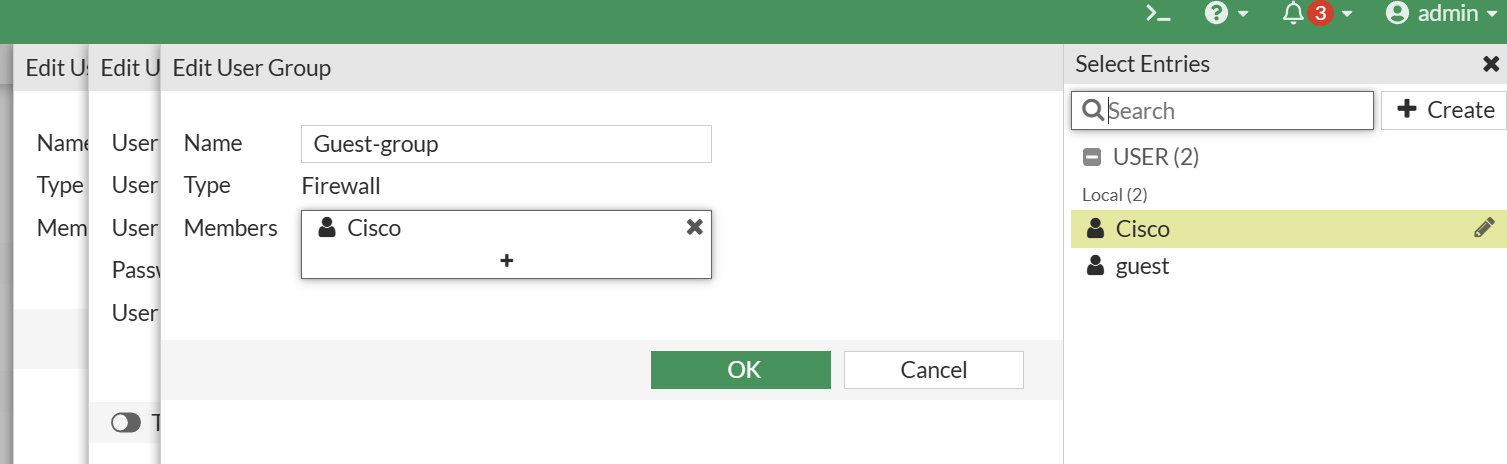
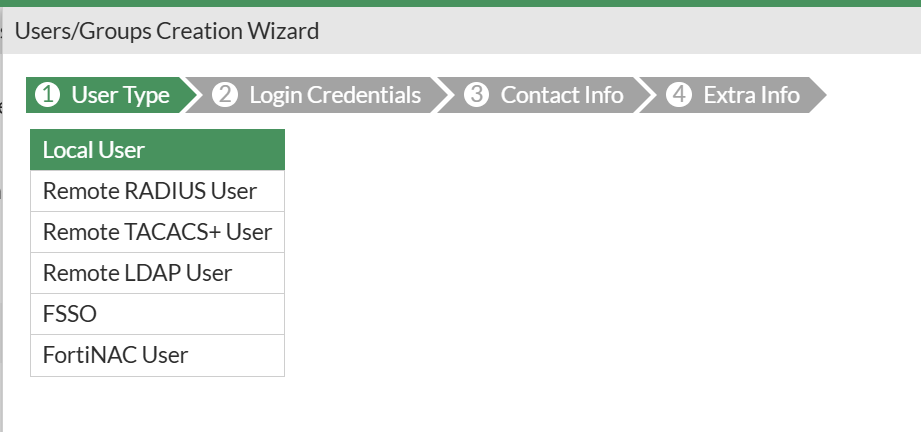
1. Now, we want to create the WPA2 Enterprise. Create another SSID and fill out the same boxes. This time, select Enterprise as the security mode.



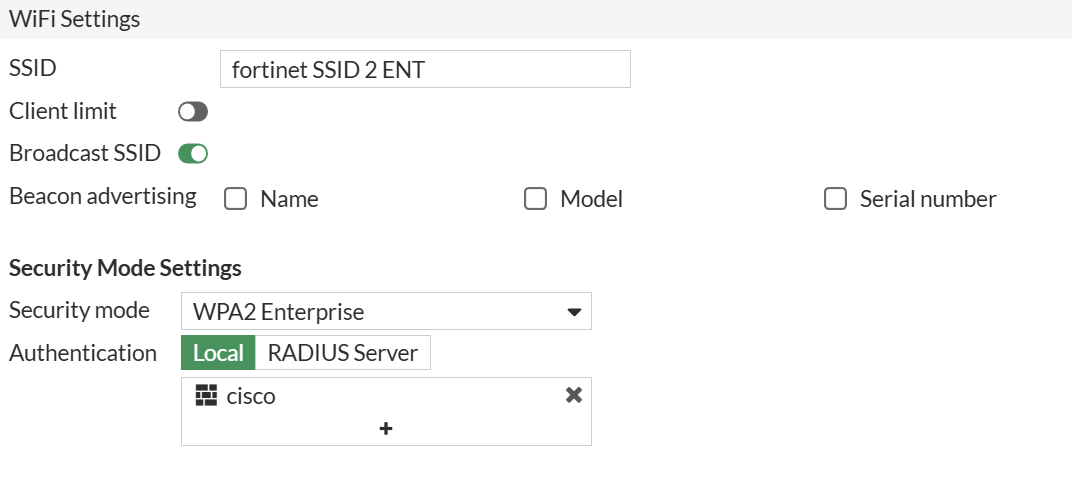
1. Now, we have to create a user for authentication purposes. Click the plus icon in order to create a new user, and create a new user group.

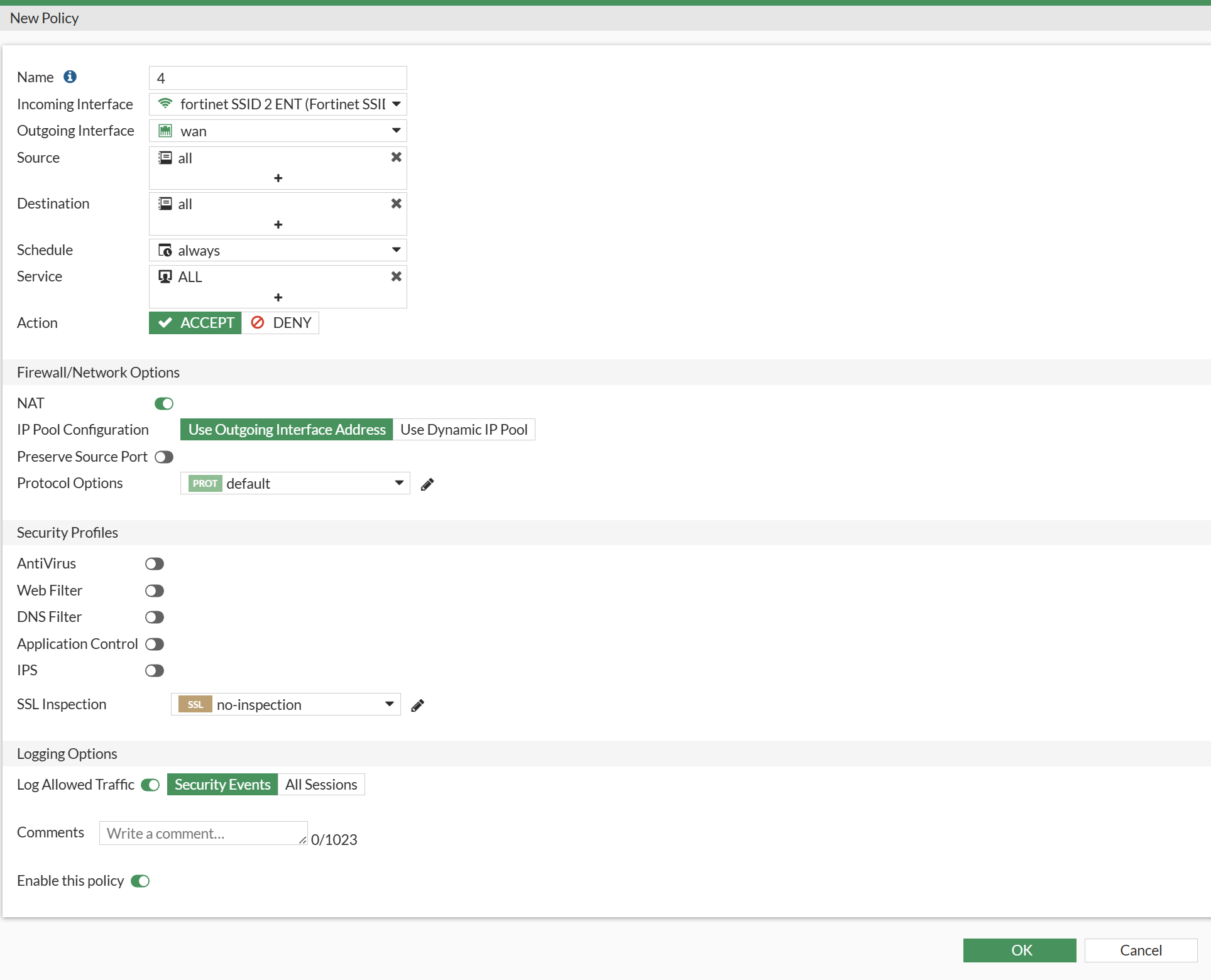
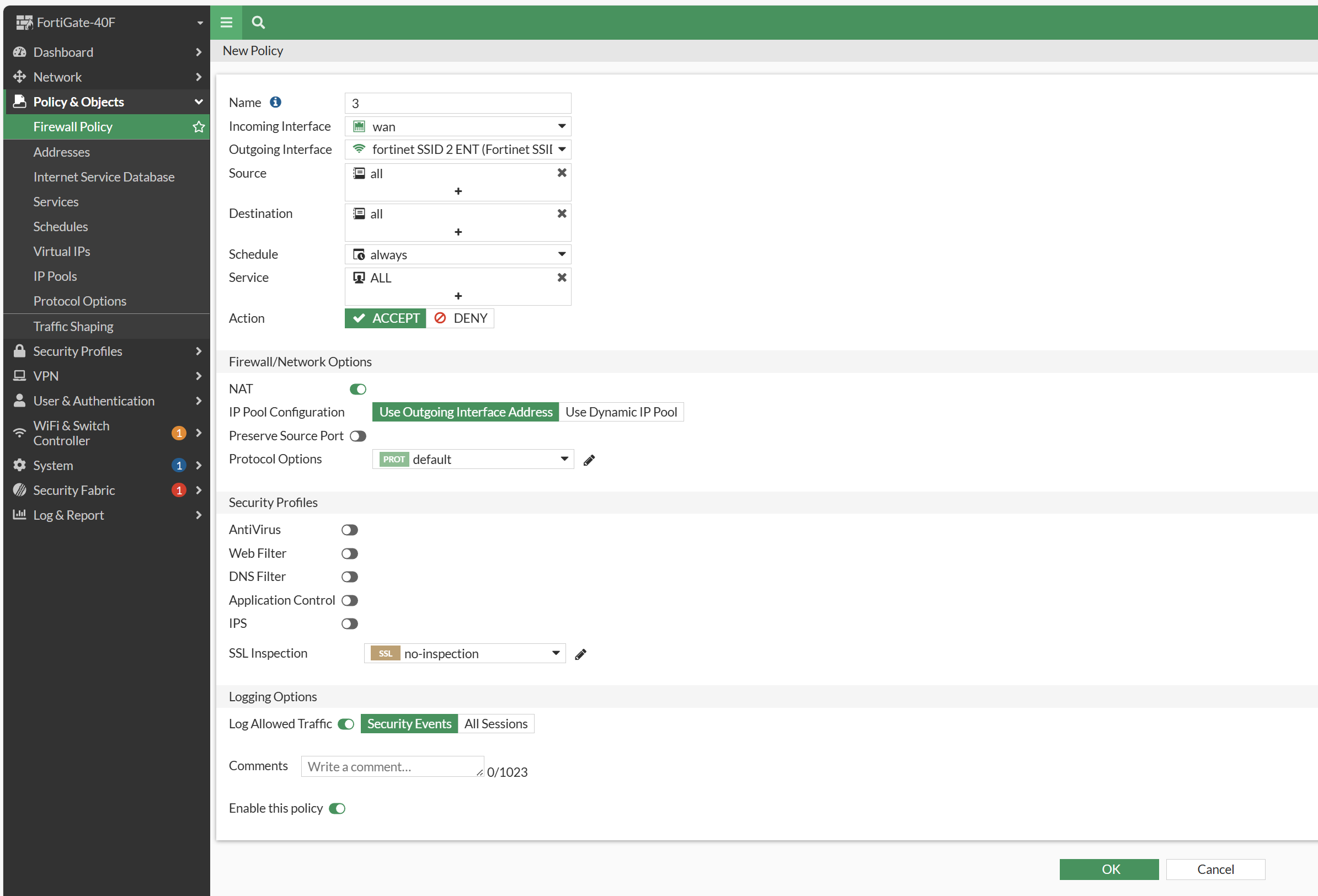
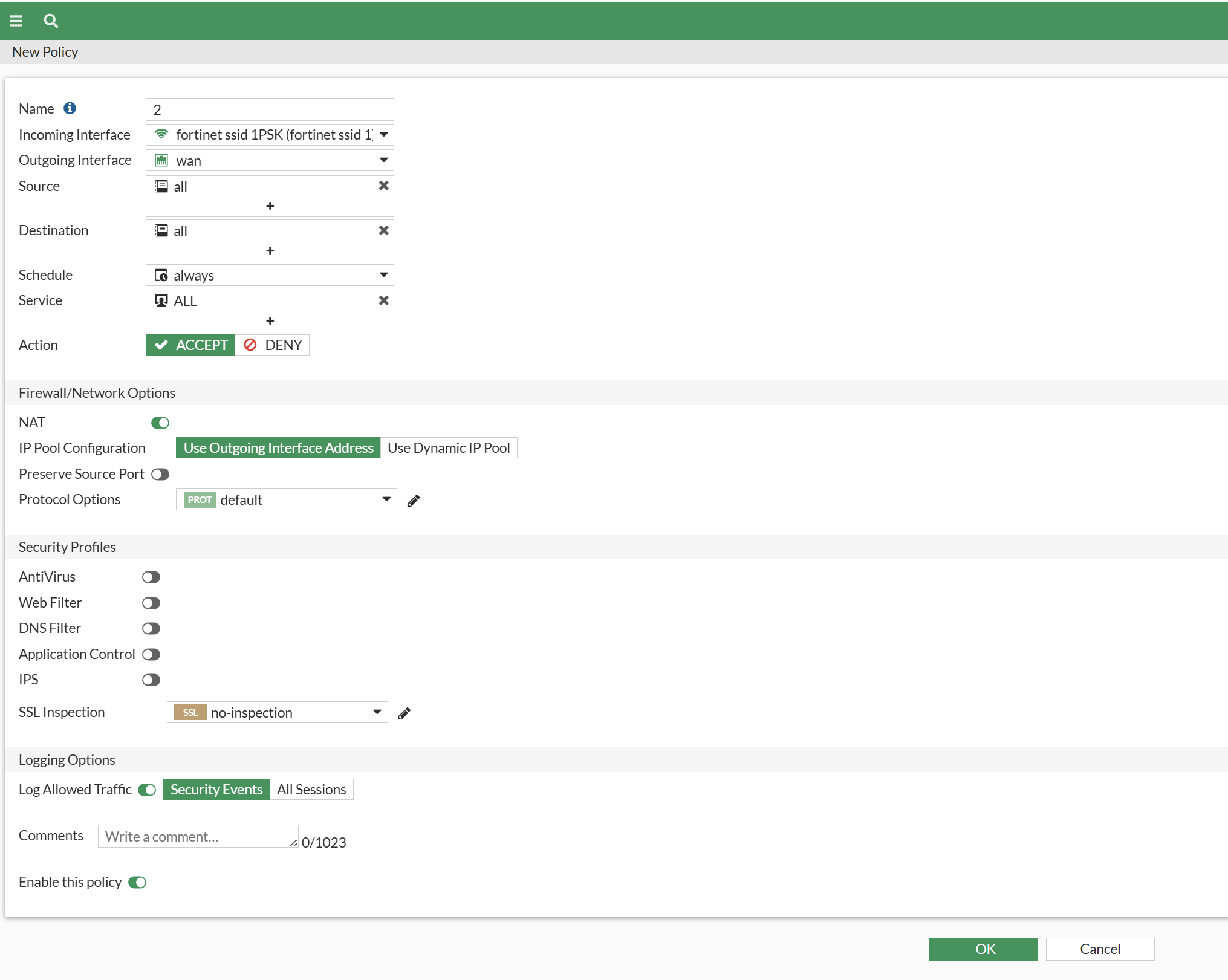
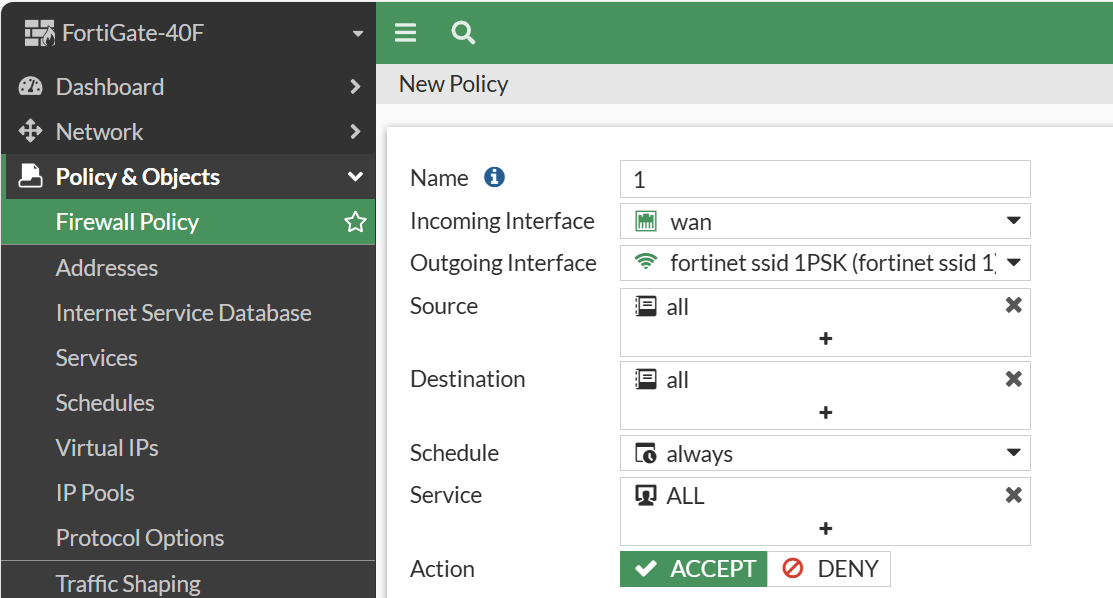


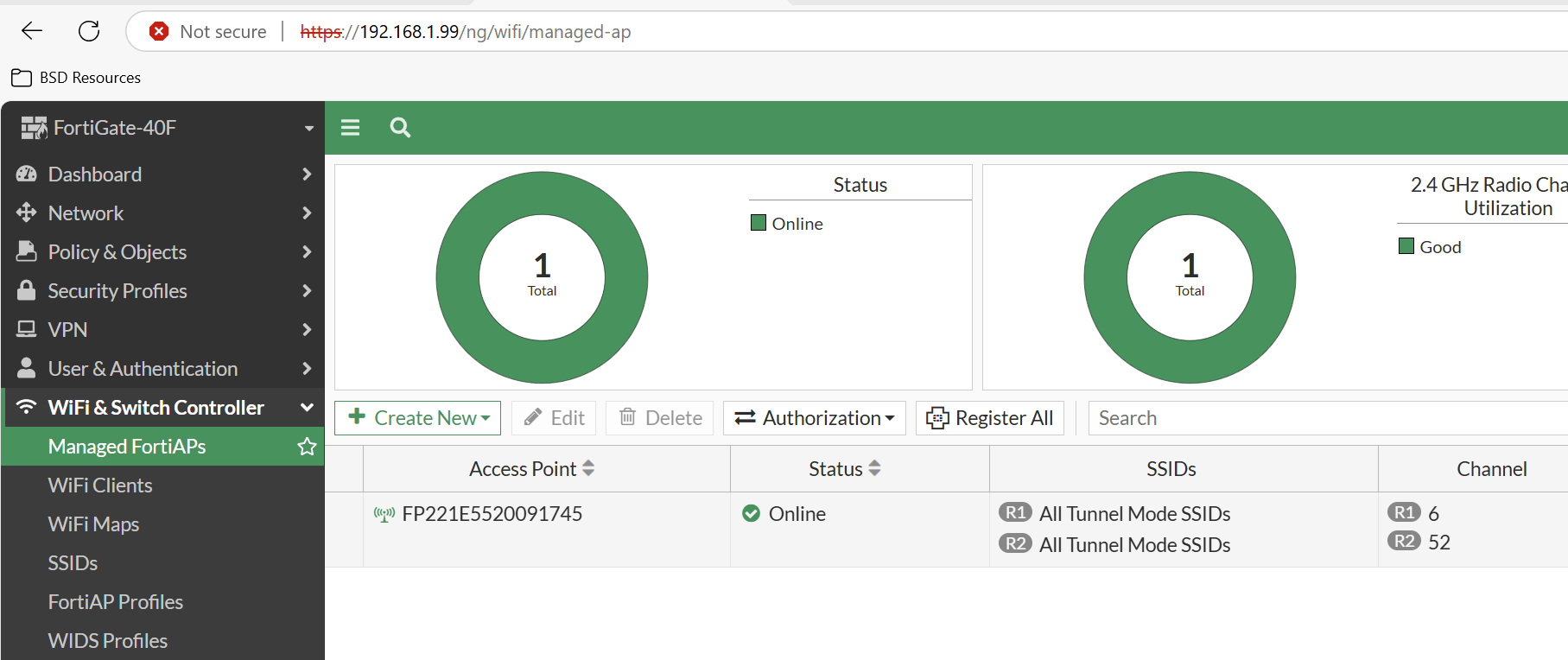
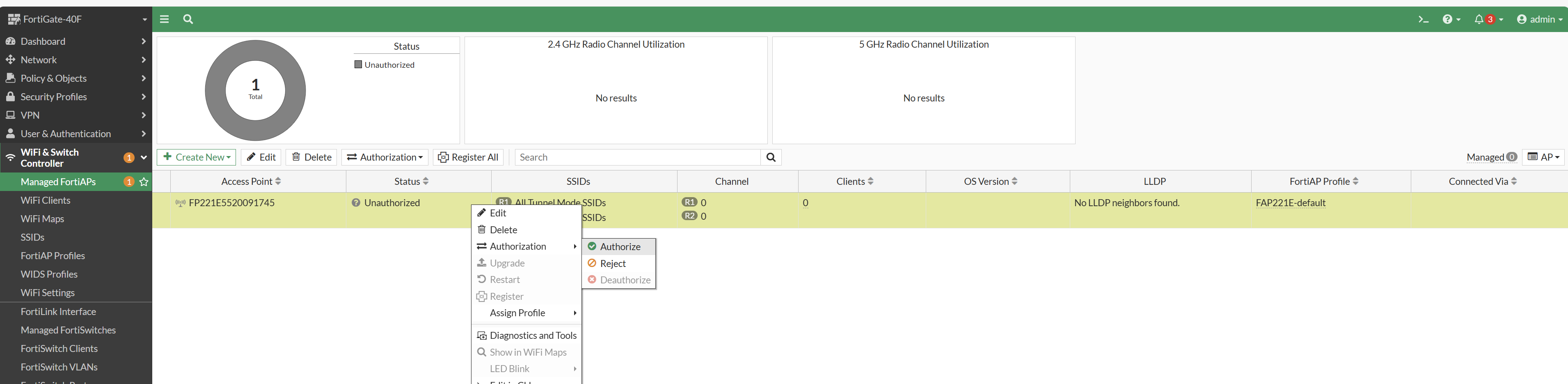
1. We want to create a locally authenticated user, so select “Local”. Now, input a username and password.



1. Upon successfully creating the User Group and local authentication user, we can assign it to the Enterprise network. This will ensure that only that user’s credentials can be used to sign in.



1. Now, all we have to do is add a firewall policy to allow traffic to flow through our network. This is important, as traffic is typically blocked for security reasons. Navigate to “Policy & Object > Firewall Policy” and create a new policy. 
2. After creating the necessary firewall policies, our last step is to authroize the Fortigate AP. Navigate to “Wifi & Switch controller > Managed Fortinet APs”, and right click on the connected AP to authorize. If you haven’t connected an AP at this stage, connect it to one of the firewall’s ethernet ports and wait for it to show up.



1. After our firewall shows up as “Online”, our network should be up and running. Get on a device near the access point and try and connected.



1. Success! We have configured our WPA2 Personal and WPA2 Enterprise networks.

**Network Diagram:**

A diagram of a diagram of a cell

Description automatically generated

**Problems:**

1. **SSID Networks Requiring Firewall Policy**

At first, we were not aware that both networks require firewall policies in order to allow network traffic to flow through. Because of this, we mistakenly thought that our configuration was entirely wrong, causing us to debug for quite a while.

Furthermore, we had an issue where our WPA2 Personal network was running smoothly with a correctly configured firewall policy, but our WPA2 Enterprise network could not access any internet. This was fixed by changing our firewall policy to the appropriate values.

1. **FortiGate AP Load Times/Auto Configuration**

Though we knew that the AP would automatically negotiate a connection with the access point, we thought that it would be quite fast. For some reason, our access point took a long time to connect, and as a result left us confused. We initially believed it was a configuration issue, only to later see that the access point was up and running with no issues.

1. **FortiGate AP POE Connector**

Because of our unique rack setup with the ground racks, we were assigned a rack that only had normal Layer 2 ethernet switches. Unfortunately, the FortiGate AP’s only ran over barrel jack connections or POE. Due to a limited supply of barrel jack connections, we were forced to try and use POE. However, with the lack of POE on our rack’s switch, we needed to use a POE injector in order to supply power, and then route the ethernet connection back to our Layer 2 switch and into our firewall. This was the only way to get power to the AP, as well as connect it to the firewall.

**Conclusion:**

Overall, this lab was a great introduction to the utilities and GUI of Fortinet and its FortiGate firewall/AP combination network setup. We were able to successfully configure an introductory SOHO network that can be practically used in all small-scale enterprise or home network situations. This was also a good refresher on basic network configuration and best security practices for firewalls.

Fortinet SOHO Configuration Signoff Sheet

Ryan Chen, P3-4 Cisco Cybersecurity, Mr. Mason

