Brit Stevens 4/17/24

Fortinet AP Configuration

**Purpose:**

The purpose of this lab was to expand our knowledge of Fortinet’s FortiGate capabilities and understand how an access point functions with the different WPA2 security modes. It demonstrates to us how a network may be set up in a professional environment where we must choose whether our wireless network needs to have access to the wired network or be entirely separate. It also taught us the advantages and disadvantages of using pre-shared keys or enterprise mode for SSIDs.

**Background Information on lab concepts:**

* **Forti-AP**
  + A Wireless Access Point that is fully integrated with Fortinet hardware that can be managed from devices like FortiGates.
  + **WPA2**
    - **Enterprise:** This mode of the network security protocol WPA2, uses a RADIUS server to authenticate users in a secure way suitable for an enterprise network. Each end device who wants to log in will need to use unique credentials, username, and password, to use this RADIUS server.
    - **PSK:** This mode of WPA2 uses a shared password for all users who want to access this network. It is less secure than WPA2 Enterprise but is more efficient for networks with many users who come and go, making it very commonly used in places like local establishments.
  + **frequency bands**
    - Newgen Access Points utilize three different bands of frequency – 2.4 GHz, 5 GHz, and 6 GHz. Our Forti-AP is not capable of 6GHz I will not cover that here.
    - **2.4Ghz** has the biggest range out of the three bands but cannot transmit data as fast and has fewer available channels.
      * When you set your AP’s radios in a certain frequency you can either set a channel or choose automatically to select open channels. For 2.4Ghz the channel width is 20MHz or 40MHz making there very few options for channel selection. Because of this, the channels can become crowded if many others use 2.4GHz when users simultaneously transmit data, slowing down everyone’s bandwidth.
    - **The 5Ghz** band is much faster than 2.4Ghz but has less range and does not go through things like walls as easily. It has a good range of frequency channels of 20MHz, 40MHz, 80MHz, and 160MHz, ensuring it does not congest as easily. This is why we only used 5GHz in the lab as there would be many APs running at the same time in close proximity.
  + **SSID types (hidden or broadcast)**
    - When an SSID is hidden, an end device will have to manually input all details about the SSID like the name, security protocol, etc. This SSID will not show up like broadcasted SSIDs do when they are in range. This is more user-friendly than the prior type.
  + **Tunnel vs. Bridge Mode**
    - **Tunnel Mode:** In this mode, all wireless traffic is encapsulated and sent through a secure tunnel to the FortiGate, making a new network separate from the physical network directly connected to it. This enhances the security of the network as a whole by separating wireless from wired.
    - **Bridge Mode:** In this mode, the wireless and wired networks are fully connected and are in the same subnet. This is typically used to integrate wireless devices into existing networks without creating a separate subnet which would be necessary.
* **Cisco vs. Fortinet APs**
  + **Cisco Access Points** are generally **CLI favored**, a command line interface used for typing commands directly into the access point, due to its greater precision and control for configurations and troubleshooting compared to GUIs. For **Fortinet Access Points, F-APs,** are **GUI favored** due to the company's ease of use and variety of features present in their GUIs. This way is more intuitive but is not necessarily better than using a CLI which is why both ways of configuring are available.

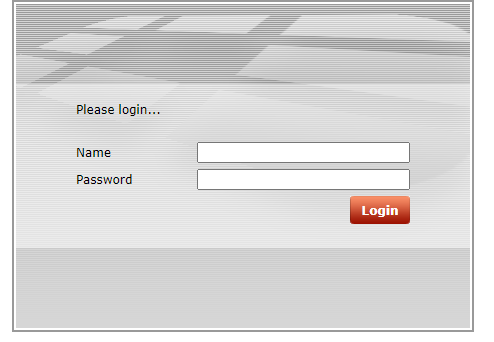
**Required Resources:**

* ***Forti-AP221E.***
* ***PoE switch (Catalyst 3560 series PoE-24).***
* ***Access to the Internet through a switch.***
* ***Desktop with an Ethernet NIC.***
* ***FortiGate 40-F Firewall.***

**Lab Summary:**

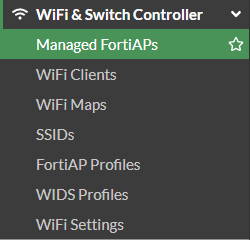
****

Connect your Forti-AP to a power-over ethernet device that is connected to your preconfigured FortiGate. This will give power to the F-AP.

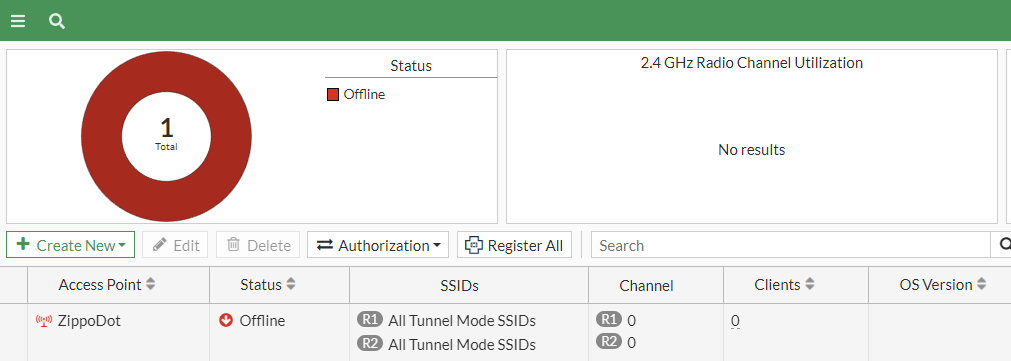


One way you can access the GUI of the Forti-AP using the default IP found online. Our AP did not have the default login credentials so we used the other simpler method.

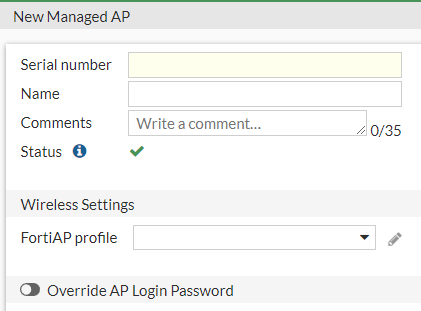
Next, go to your **Fortigate** Firewall and log into it.

****

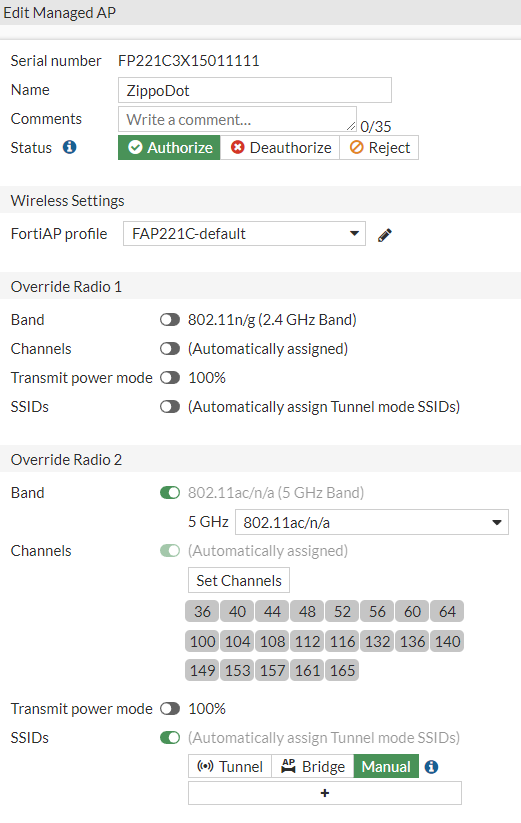
Once logged in head to the navigation panel on the left and select **Wi-Fi & Switch Controller** then go to **Managed Forti-APs**.

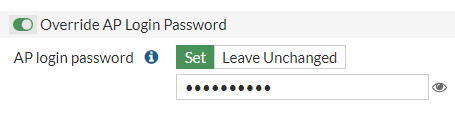
****

Click Create new managed AP to start adding your connected AP to your managed devices.

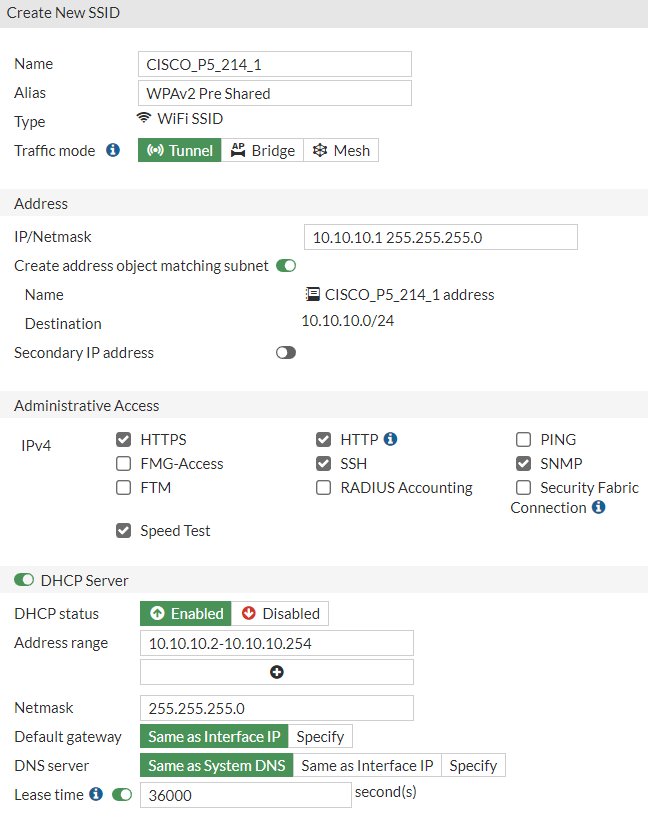
****

Once in the AP configuration, enter the serial number found on the back of your AP that is connected and name it what you want. Select OK. Your AP should now be connected to the FortiGate.

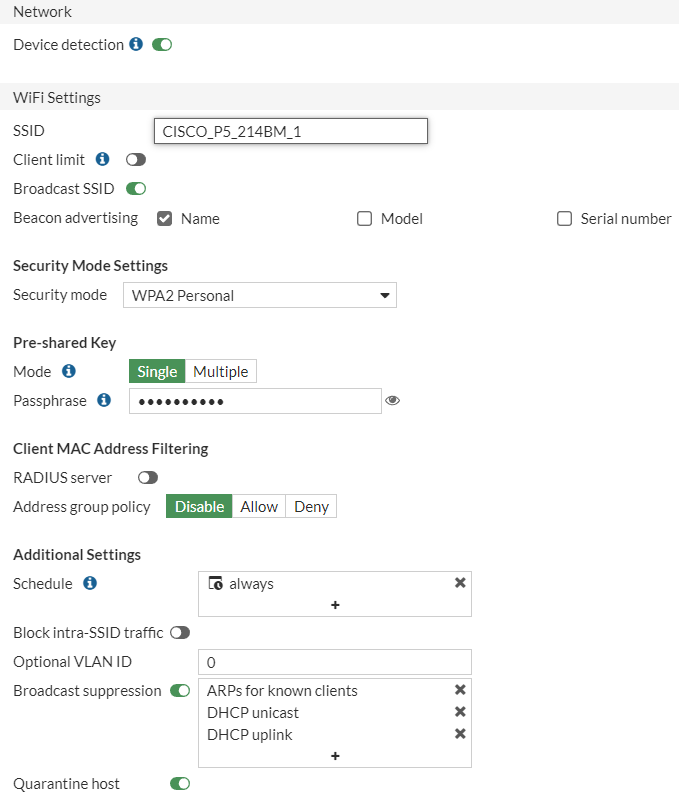




Right-click and select **Edit** to configure the AP for use. For our lab we’re using only the **5GHz** band so fully **disabled** radio 1 which is **2.4GHz** and **enabled** radio 2. Set the AP login password to a memorable password and set **SSIDs** to **manual** then create a new SSID.

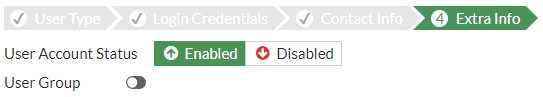
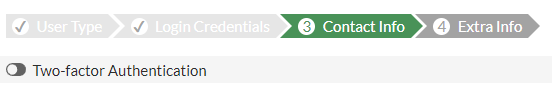
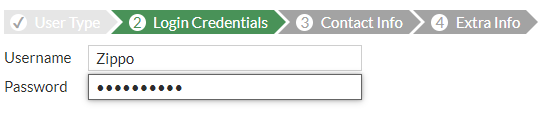


First, we are configuring our **WPA2 PSK** SSID. Give it a name and select **Tunnel** mode or **Bridge** mode depending on what kind of SSID you want to configure it as. Set an address that will be in the same range as the DHCP pool you configure. Permit whatever protocols you feel are necessary. Toggle the DHCP pool on, select enable, and give it an IP range to distribute to connections. Leave **Default gateway** and **DNS server** as the defaults. You can set the lease time to anything you want depending on how often users are expected to connect and disconnect from the network. We used ten hours because we will be connecting and disconnecting from this SSID often as we leave and enter the lab often.

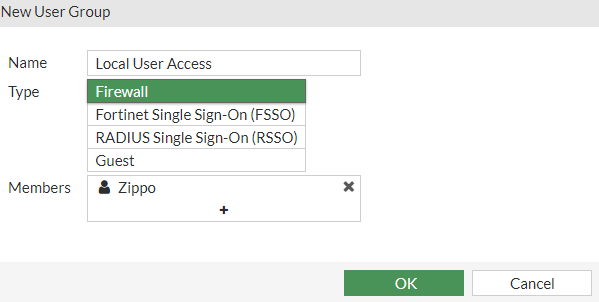


Toggle **Device Detection** to on so you can tell what end devices join the network for security purposes and logging. Enter an SSID again and set to **Broadcast** which will allow end devices like a desktop to see and be able to connect to that SSID. Select **WPA2 Personal** for the Security Mode and set your **PSK** that will be entered to join the network. Leave additional settings as the default unless you only want your SSID to accept join requests during a certain time frame using the Schedule feature.

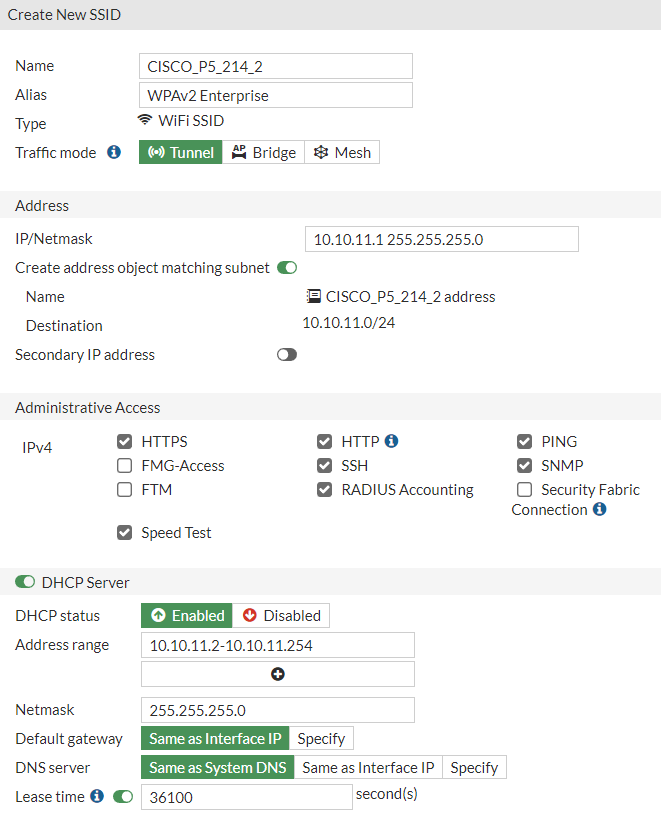
Now we will make a **User Group** for the **WPA2 Enterprise** SSID.



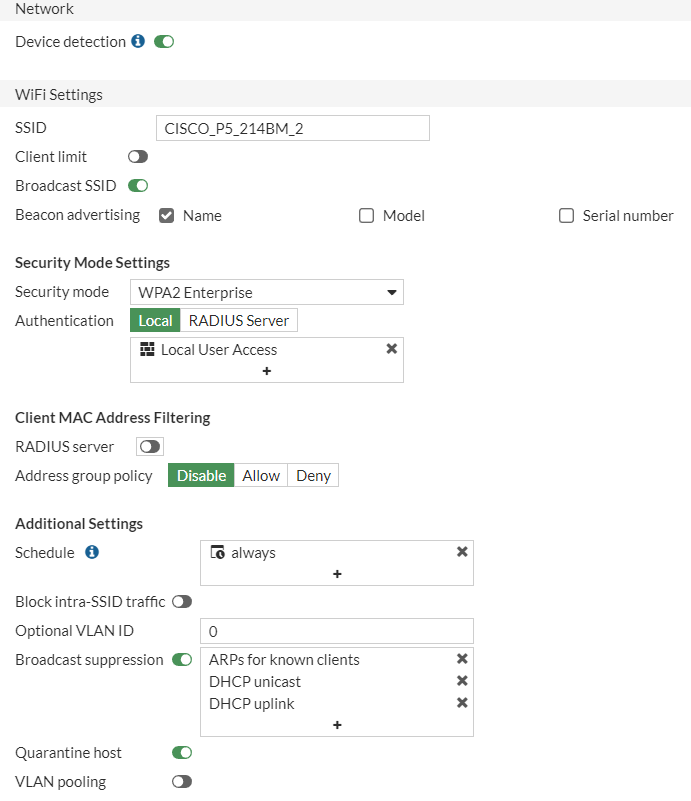
Navigate to **User & Authentication** -> **Users Definition** and create new. Go through the process of making a new user setting the login to **Local User**.



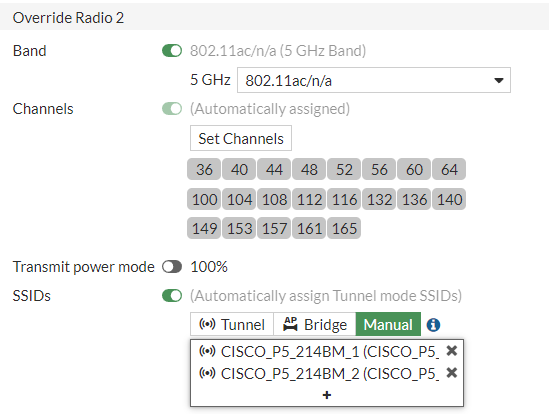
Next, make a user group for the User created. From the same category navigate to **User Groups** and create new. Name it, set it to **Firewall**, and add the user you just created to the group as a **Member**. This will put the user in the group.



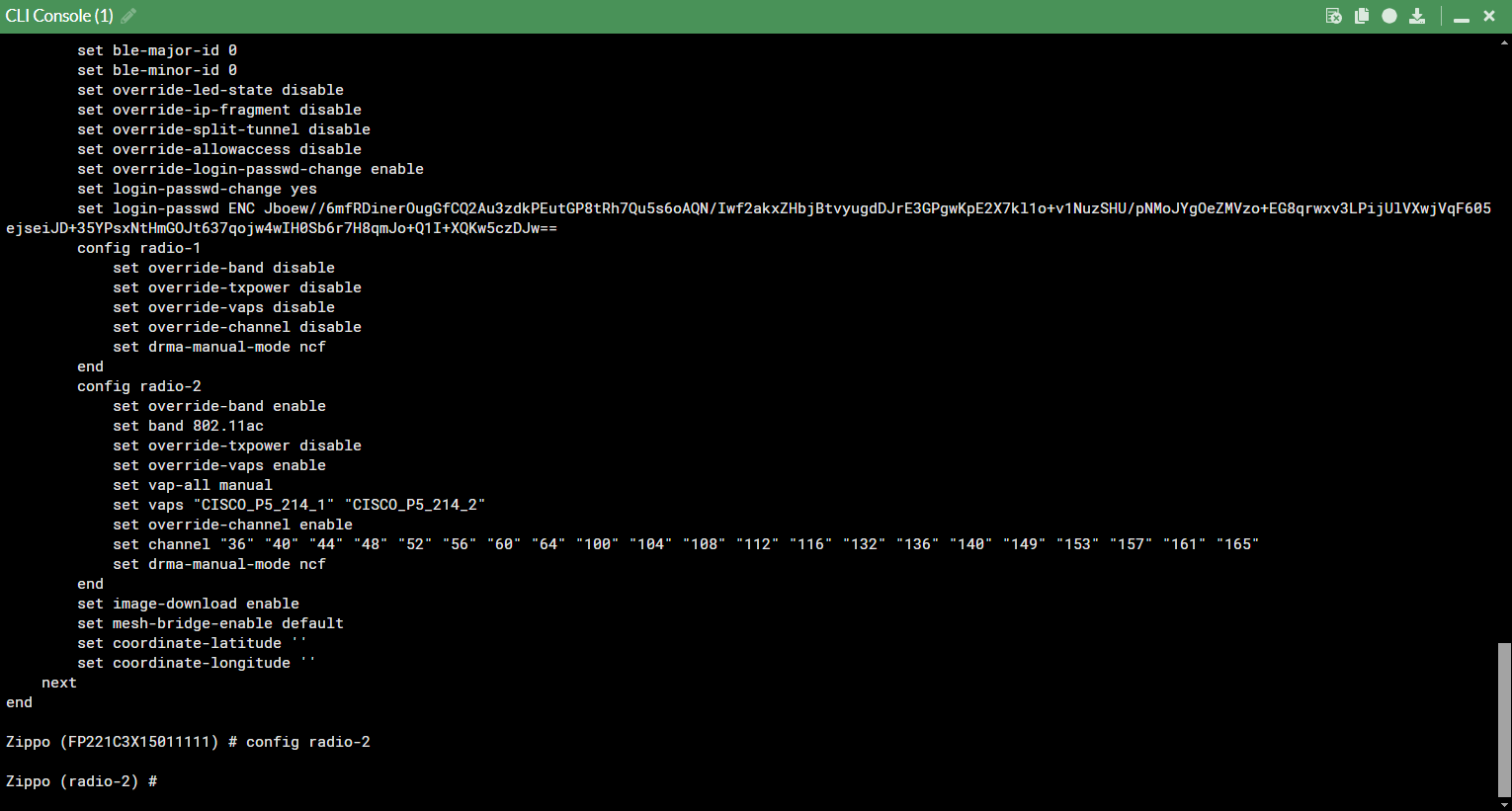
Navigate back to your F-AP configuration and create another SSID, this time we will configure it for WPA2 Enterprise. Most of the settings will be the same as the PSK SSID with some differences. Change the name of the SSID so it is recognizable as the Enterprise SSID. Change the IP of the DHCP server and SSID IP so they are a different subnet than the other SSID. Ensure **RADIUS Accounting** is enabled as you will be using a local radius server.



Once again make sure the broadcasted SSID is recognizable as the Enterprise SSID. Under **Security Mode** select **WPA2 Enterprise** and Local Mode. Add the user group previously created to the Local Authentication method. This will ensure that when the WPA2 SSID looks for a radius server to authenticate a user attempting to join with a User and Password, it will look at the Local User Group we had created.

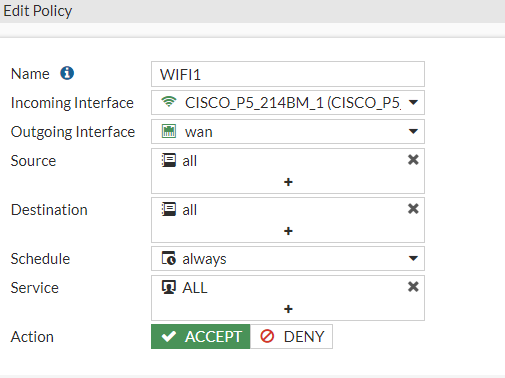


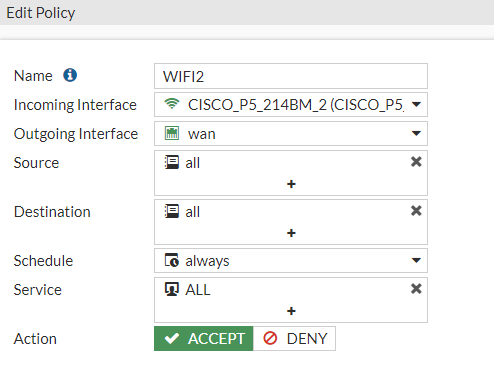
Now that we have the SSIDs created, navigate back to the F-AP configuration and add the SSIDs.



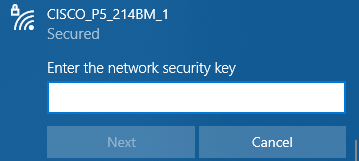
In the CLI of the F-AP, you can see that Radio-2 is configured correctly.

Next, navigate to **Policy & Objects ->** **Firewall Policy** to allow our SSIDs internet access through the FortiGate.



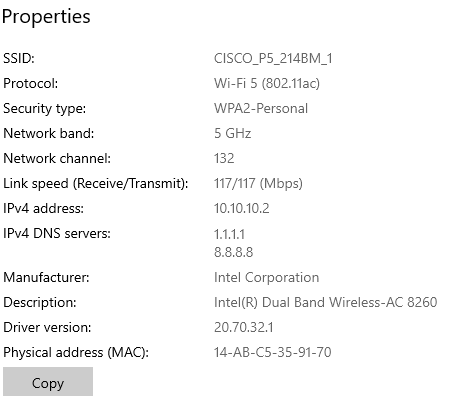


Create a new policy for both the PSK and Enterprise network with the **Incoming Interface** set to their respective SSIDs and the **Outgoing Interface** set to **WAN**. The source IPs can be all which is less secure or set to the IP range of the SSID. The destination IP must be all to ensure your SSIDs can access any address on the internet. Make sure the Policy is set to **Accept.,**

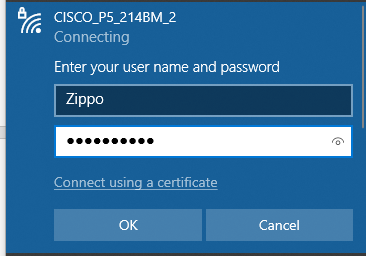


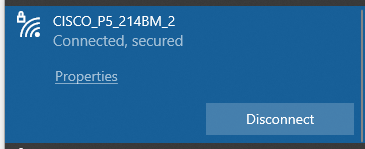


Entering in the PSK we configured you can log into the PSK SSID.



Going into the **properties** of the SSID, you can see that the IP is in the range we set on the SSID and the **Security Type** is WPA2-Personal as we set.

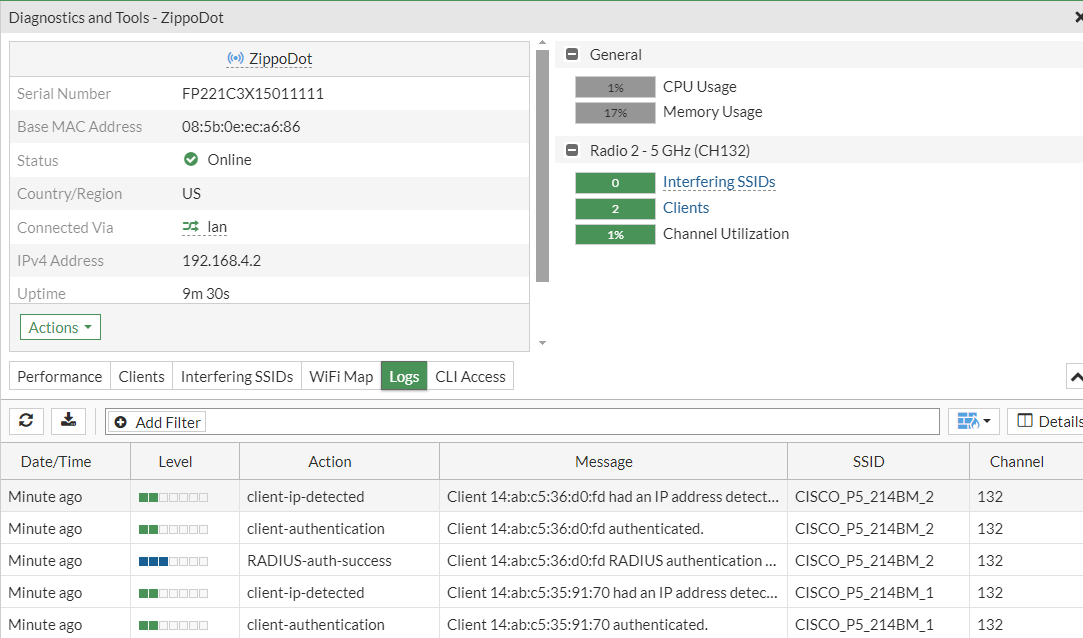




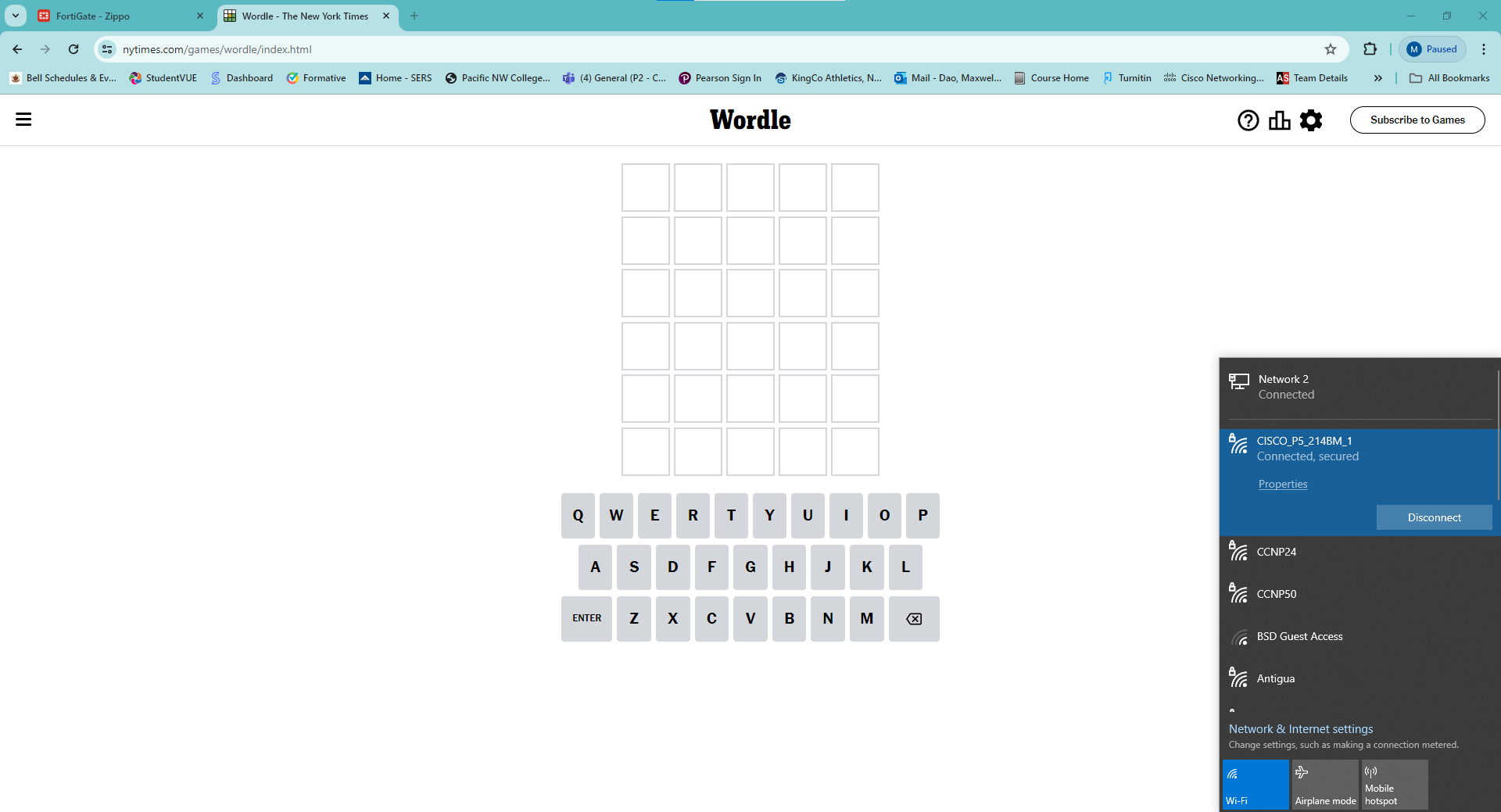
Entering the User and Password configured for the Enterprise SSID, you should be able to log into the SSID. Entering in an unknown will not work.



You can also confirm in the **properties** with WPA2-Enterprise as the **Security Type** and the IP is in the range we set for the SSID.



If you navigate to **Manage Forti-AP,** you can right-click your F-AP and look at the diagnostics log showing that RADIUS is being used and confirmed with the respective SSID. You can also see that the PSK SSID was authenticated confirming it was being used.



You can confirm internet access but searching on a browser.

**Problems:**

* We didn’t know how to access the F-AP so attempted to ARP to find the IP address of its port.
  + ARP results did not include the F-AP’s serial number.
    - Searched for the default IP of F-AP in an attempt to access the GUI.
    - Credentials to log in were not the default even though the IP was.
      * We realized that we could configure the F-AP from our FortiGate once they are connected by a switch.
* We had to export the configuration of our FortiGate to our partnering group so they could do the F-AP lab off their firewall and AP now that one of the group members was back.
  + To export the configuration, we needed to click on profile in the top right -> configuration -> backup -> confirm to a location on the desktop and export.
* We could not attach the F-AP to the Firewall due to the necessity of PoE which the FortiGate could not provide.
  + Physical topology was set up in a way that the AP could not connect.
    - Had to set up the FortiGate to have its LAN port connected to a PoE switch and then connect the AP to the PoE switch.
* SSIDs did not have a Wi-Fi connection.
  + At first we tried to change the subnets of the SSIDs to be in the range of the of the FortiGate’s inside network. No success.
    - We realized we need a policy to permit Forti WIFI traffic to the internet and added such.

**Conclusion:**

Overall, this lab was relatively easy to configure due to the simplicity of the FortiGate GUI and its compatibility with the Forti-AP but gave us important takeaways for decisions professionals need to make when creating or expanding a network. Compared to our Cisco AP lab, this one was more straightforward covering nearly the same topics with a few key differences like deciding to use tunnel mode or bridge mode. This was an interesting thing to learn as to when to use each mode of the SSID for different purposes. The lab also highlighted the importance of a Radius server to increase the security of a network as it ensures greater authentication. My biggest takeaway from this lab is how convenient but effective the GUI of the FortiGate is when you are learning how to configure things like access points. The Cisco AP was very hard to get introduced to but Forti-AP was user-friendly with its compatibility with the familiar FortiGate.

