Fortinet Access Point SSID Configuration Lab

Emma Matsuda

Advanced Cisco Cybersecurity

**Purpose**

In this lab, we configured WPA2 PSK and Enterprise SSIDs on a FortiGate Access Point. This exercise illustrated the distinction between WPA2-PSK, which relies on a shared password for authentication, and WPA2-Enterprise, which utilizes an authentication server to manage individual user credentials.

**Background Info**

Fortinet access points are a key component of Fortinet's wireless networking solutions. They are designed to provide secure, high-performance wireless connectivity in various environments, ranging from small businesses to large enterprises.

|  |  |
| --- | --- |
| Key features/concepts | In detail |
| Security | * integrate security features such as intrusion prevention, rogue AP detection, and role-based access control * ensure that wireless networks remain secure against various threats |
| Wireless Standards Support | * support latest wireless standards   + 802.11ac   + 802.11ax (Wi-Fi) * Deliver high performance wireless connectivity and increased capacity/efficiency |
| Unified Management | * Can be centrally managed and monitored through Fortinet’s network management platform * Provides admins with a single interface to configure, monitor, and troubleshoot the entire wireless network |
| Dynamic Radio Management | * Utilize dynamic radio management techniques to:   + Optimize wireless coverage   + Minimize interference   + Maximize performance in dynamic RF environments |
| Mesh Networking | * Support mesh networking capabilities * Allows them to extend wireless coverage to areas where running Ethernet cables is not feasible |
| Quality of Service | * QoS features to prioritize network traffics based on application requirements * Ensures optimal performance for critical applications |
| Guest Access | * Built-in support for guest access   + Captive portal authentication   + Guest isolation   + Bandwidth management * Provides secure guest Wi-Fi services |
| Fortinet Security Fabric | * Integrate the Fortinet Security Fabric * Enables enhances security and visibility across the entire network infrastructure |
| Cloud Management | * Can be managed from the cloud using Fortinet’s cloud-based management platform * Provides flexibility and scalability for managing distributed wireless networks |
| PoE Support | * Supports Power over Ethernet * Allows them to be powers over the Ethernet cable * Simplifies deployment * Reduces the need for additional power outlets |

**Lab Summary**

1. Set up topology
2. Create the SSIDs
3. Configure the network interfaces
4. Authorize and configure the Access Point
5. Create the firewall policy
6. Create the user and user group
7. Test the connectivity

**Lab Commands**

Because every configuration was done in the Web GUI, there were no new commands used.

**Network Diagram/Topology**

A diagram of a firewall

Description automatically generated

**Configurations** – screenshots of the process

|  |  |
| --- | --- |
| 1. Connect the FortiGate firewall to a switch with internet access. |  |
|  | 1. Connect the FortiGate access point (AP) to the firewall, use the ethernet cable.  * Check that the lights on the AP is on. |
| 1. Log into the Fortinet GUI using the “admin” and “Cisco123” password set in previous labs. |  |
| 1. Wi-Fi & Switch Controller > SSIDs > New |  |
|  | 1. Enter the same settings on the left to configure the Bridge Mode SSID. 2. Click OK |
|  | 1. Click “New” to create a new PSK SSID, and configure the SSID with the following settings on the left. 2. The password and SSID can be changed to its convenience. 3. Click OK |
|  | 1. Click New to create an enterprise SSID 2. The enterprise SSID should have the following settings on the left 3. Click OK to confirm the creation |
|  | 1. The SSIDs homepage should be like the image on the left |
| 1. Network > Interfaces > New |  |
|  | 1. Configure the following settings – it should be the same as the screenshots on the left 2. Click OK |
| 1. Managed FortiAPs > homepage |  |
|  | 1. The homepage should look like the screenshot on the left |
| 1. Right click on the gray AP option > Authorize |  |
|  | 1. After the authorization, the homepage should look like the left. |
|  | 1. Right click on Edit > configure with the same settings on the left 2. Click OK |
|  | 1. Managed APs should look like the left.  * The SSIDs should be visible under the SSIDs tab |
| 1. Policy & Objects > Firewall Policy > Create New |  |
|  | 1. To configure the policy for the PSK SSID, configure the same settings on the left. 2. Click OK |
|  | 1. The Firewall Policy homepage should look something like the one on the left |
|  | 1. To create the Snterprise SSID, click New and configure the same settings at the left image. 2. Click OK |
| 1. Policy & Objects > Firewall Policy  * Check that you can see both of the firewall policies here |  |
| 1. User & Authentication > User definition > New  * This is to create the user that we will use to log into our SSIDs |  |
| 1. Local User > Next |  |
|  | 1. Set the username and password of your user, and then click OK to confirm |
| 1. Make sure the user account statues in enabled under the Extra Info tab |  |
| 1. Click on the + sign under the user group |  |
|  | 1. Create a new user group for the user, and click OK |
| 1. User & Authentication > User Definition  * Check that the new user is visible there |  |
| 1. Repeat the steps above to create a user to use for the Enterprise SSID |  |
| 1. In the bottom right corner, click on the WiFi button to show the options.  * The name of the SSID should be shown as an option |  |
|  | 1. Connec to each SSID using the username and password that you set previously. |
| 1. You should be able to connect to the internet. |  |

**Problems**

* We didn’t have internet connection, even though we were able to connect our pre shared key SSID. The internet browsers were not working. One solution is that we tried factory resetting our firewall to see if that will fix the problem, but it didn’t. We then realized that there is a hardware wiring problem – our firewall was plugged into a different group’s firewall instead of our switch that provided the internet connection. With the correct wiring, our configurations were working normally.

**Conclusion**

In our lab, we began by setting up each SSID (both PSK and Enterprise) using the FortiGate GUI. Following this, we configured a network interface, established firewall policies for each SSID, and authorized the access point. We also created a user and a user group to manage internet access, and then connected to each SSID using these credentials. Initially, we encountered an issue where we could connect to the SSID but couldn't access the internet. Upon investigation, we discovered it was a Layer 1 issue caused by our firewall not being connected to the switch with internet access. After correcting our network topology, we were able to access the internet within a few minutes.