



Fortinet SOHO and WPA2-PSK/Enterprise Setup

Andrew Pai

Period 5 Cybersecurity



paloalto[®]
NETWORKS

Purpose:

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

Background Information:

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

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

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

Access points are wireless network devices that essentially allow devices to connect to a LAN without actually being plugged into it. They allow for an increase in the number of devices that can be on the network if all the physical slots are taken up, and extend any existing wireless coverage on a network. For this lab, our group used the security protocols of WPA2-Pre-Shared Key (WPA2-PSK) and WPA2-Enterprise. Security protocols are used

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

Lab Summary:

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

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

```
FortiGate-40F login:
System is resetting to factory default...

Please stand by while rebooting the system.
Restarting system.

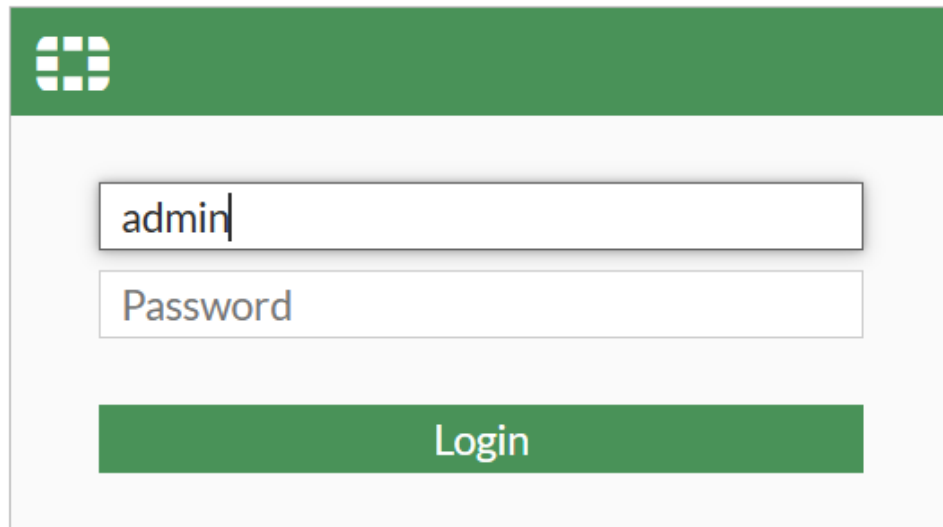
FortiGate-40F (00:32-03.17.2023)
Ver:05000030
Serial number: FGT40FTK23099156
CPU: 1200MHz
Total RAM: 2 GB
Initializing boot device...
Initializing MAC... NP6XLITE#0
Please wait for OS to boot, or press any key to display configuration menu.....

Booting OS...
Initializing firewall...

System is starting...
```

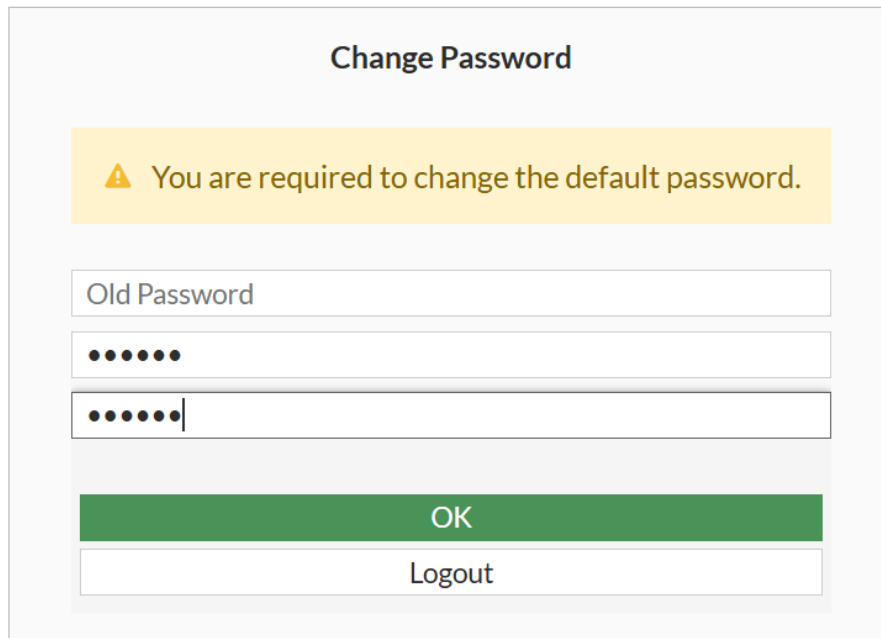
After the firewall has been reset, enter the management IP address of the firewall, which should be 192.168.1.99. This will get you into the GUI of the

firewall. From there, you can enter the default credentials of admin and no password.



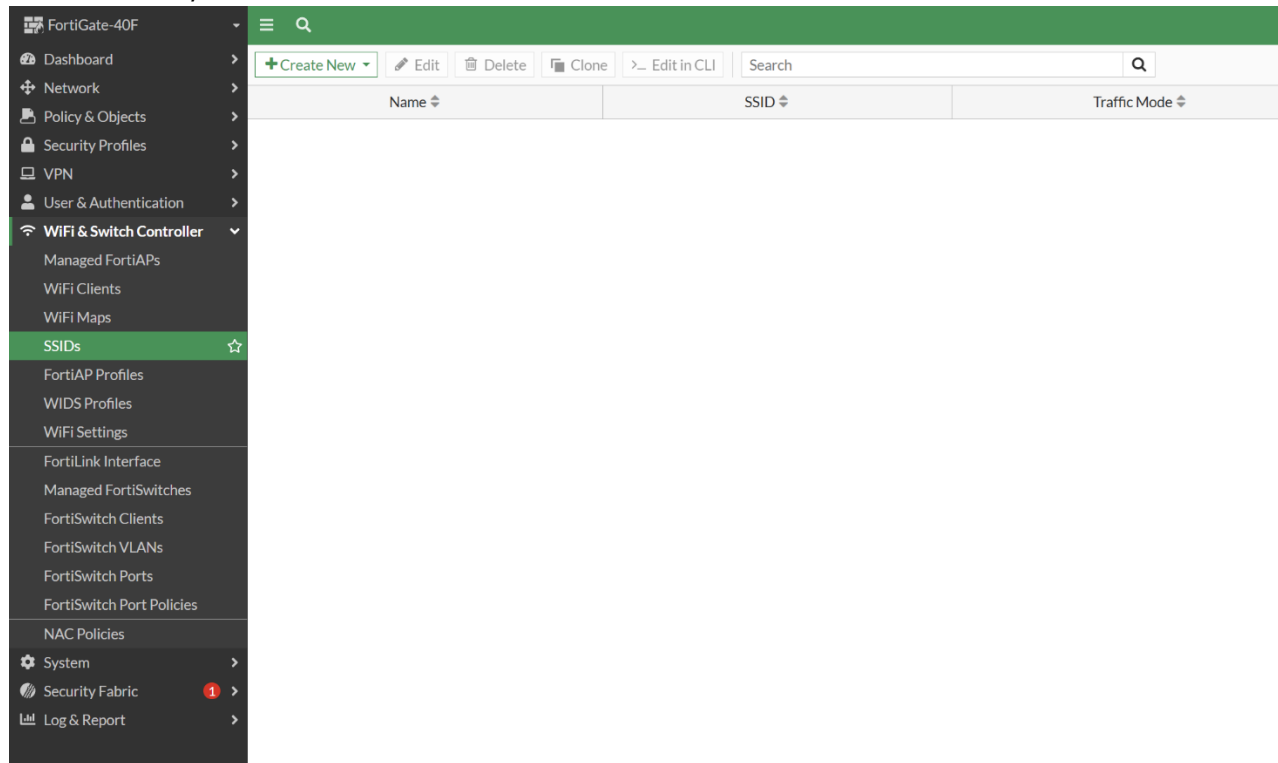
The image shows a login interface. At the top is a green header with a white icon consisting of a 3x3 grid of squares. Below the header is a light gray box containing two input fields. The first input field has the text 'admin' and a cursor at the end. The second input field is empty and has the placeholder text 'Password'. Below these fields is a green button with the text 'Login' in white.

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

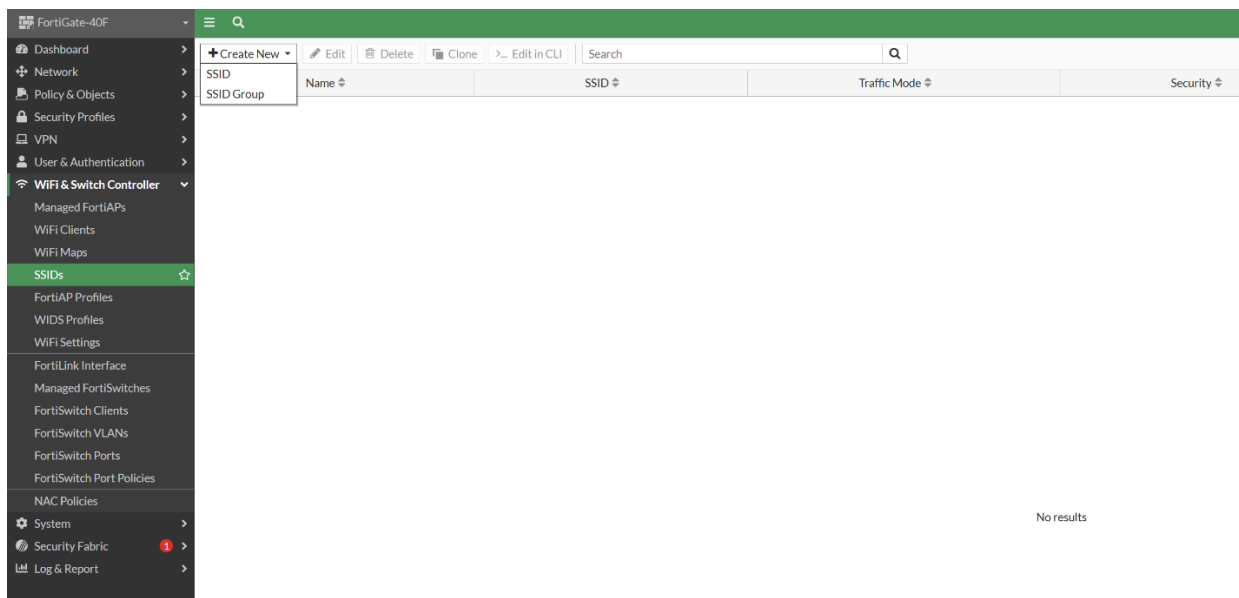


The image shows a 'Change Password' form. At the top is a title 'Change Password'. Below the title is a yellow warning box with a triangle icon and the text 'You are required to change the default password.' Below the warning box are three input fields. The first input field is labeled 'Old Password'. The second input field contains six dots. The third input field contains six dots and a cursor at the end. Below these fields are two buttons: a green button labeled 'OK' and a white button labeled 'Logout'.

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



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



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

FortiGate-40F

Dashboard

Network

Policy & Objects

Security Profiles

VPN

User & Authentication

WiFi & Switch Controller

Managed FortiAPs

WiFi Clients

WiFi Maps

SSIDs

FortiAP Profiles

WIDS Profiles

WiFi Settings

FortiLink Interface

Managed FortiSwitches

FortiSwitch Clients

FortiSwitch VLANs

FortiSwitch Ports

FortiSwitch Port Policies

NAC Policies

System

Security Fabric

Log & Report

Create New SSID

NamePSK

Alias

TypeWiFi SSID

Traffic modeTunnelBridgeMesh

Address

IP/Netmask192.168.2.1/27

Create address object matching subnet

NamePSK address

Destination192.168.2.0/27

Secondary IP address

Administrative Access

IPv4

HTTPS

HTTP

PING

FMG-Access

SSH

SNMP

FTM

RADIUS Accounting

Security Fabric Connection

Speed Test

DHCP Server

DHCP statusEnabledDisabled

Address range192.168.2.2-192.168.2.30

Netmask255.255.255.224

Default gatewaySame as Interface IPSpecify

DNS serverSame as System DNSSame as Interface IPSpecify

Lease time604800second(s)

Advanced

Network

Device detection

WiFi Settings

SSIDfortinet

Client limit

Broadcast SSID

Beacon advertisingNameModelSerial number

Security Mode Settings

Security modeWPA2 Personal

OKCancel

FortiGate-40F

Dashboard

Network

Policy & Objects

Security Profiles

VPN

User & Authentication

WiFi & Switch Controller

Managed FortiAPs

WiFi Clients

WiFi Maps

SSIDs

FortiAP Profiles

WIDS Profiles

WiFi Settings

FortiLink Interface

Managed FortiSwitches

FortiSwitch Clients

FortiSwitch VLANs

FortiSwitch Ports

FortiSwitch Port Policies

NAC Policies

System

Security Fabric

Log & Report

Create New SSID

Advanced

Network

Device detection

WiFi Settings

SSIDandrewjoshpsk

Client limit

Broadcast SSID

Beacon advertisingNameModelSerial number

Security Mode Settings

Security modeWPA2 Personal

Pre-shared Key

ModeSingleMultiple

Passphrase

Client MAC Address Filtering

RADIUS server

Address group policyDisableAllowDeny

Additional Settings

Schedulealways

Block intra-SSID traffic

Optional VLAN ID0

Broadcast suppression

ARPs for known clients

DHCP unicast

DHCP uplink

Quarantine host

VLAN pooling

NAC profile

Traffic Shaping

Outbound shaping profile

Miscellaneous

Comments0/255

StatusEnabledDisabled

OKCancel

The screenshot displays the 'Create New SSID' configuration window in the FortiGate-40F management interface. The configuration is as follows:

- Name:** enterprise
- Alias:** WIFI SSID
- Type:** WIFI SSID
- Traffic mode:** Tunnel, Bridge, Mesh
- Address:**
 - IP/Netmask:** 192.168.2.100/27
 - Create address object matching subnet:**
 - Name:** enterprise address
 - Destination:** 192.168.2.96/27
 - Secondary IP address:** (empty)
- Administrative Access:**
 - IPv4:**
 - ☐ HTTPS
 - ☐ HTTP
 - ☐ PING
 - ☐ FMG Access
 - ☐ SSH
 - ☐ SNMP
 - ☐ FTM
 - ☐ RADIUS Accounting
 - ☐ Security Fabric Connection
 - ☐ Speed Test
- DHCP Server:**
 - DHCP status:** Enabled
 - Address range:** 192.168.2.98-192.168.2.126
 - Netmask:** 255.255.255.224
 - Default gateway:** Same as Interface IP
 - DNS server:** Same as System DNS
 - Lease time:** 60:00:00
- Advanced:**
 - Network:**
 - Device detection:** Enabled
 - WiFi Settings:**
 - SSID:** fortinet
 - Client limit:** Enabled
 - Broadcast SSID:** Enabled
 - Beacon advertising:** Name, Model, Serial number
- Security Mode Settings:**
 - Security mode:** WPA2 Enterprise

The right sidebar shows the 'FortiGate-40F' header, 'Additional Information' (API Preview), 'SSID' section (GUID, FortiAP-S and FortiAP-U Bridge Mode Security Profiles), 'Online Guides' (Retrieved Documentation, Video Tutorials), and 'Fortinet Community' (Link, Events, Multiples SSIDs with RADIUS FortiAuthenticator, Multiples SSIDs with RADIUS FortiAuthenticator + EAP-TLS, FortiAP Tunnel Mode: FortiSwitch VLAN, See More).

New User Group

NameCisco

TypeFirewall

Fortinet Single Sign-On (FSSO)
RADIUS Single Sign-On (RSSO)
Guest

Members

guest

OK

Cancel

Select Entries

Search

+ Create

USER (1)

Local (1)

guest

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

The screenshot shows the 'Users/Groups Creation Wizard' window. At the top, there is a progress bar with four steps: 1 User Type, 2 Login Credentials, 3 Contact Info, and 4 Extra Info. Step 1 is currently active and highlighted in green. Below the progress bar, there is a list of user types: Local User, Remote RADIUS User, Remote TACACS+ User, Remote LDAP User, FSSO, and FortiNAC User. The 'Local User' option is selected and highlighted in green.

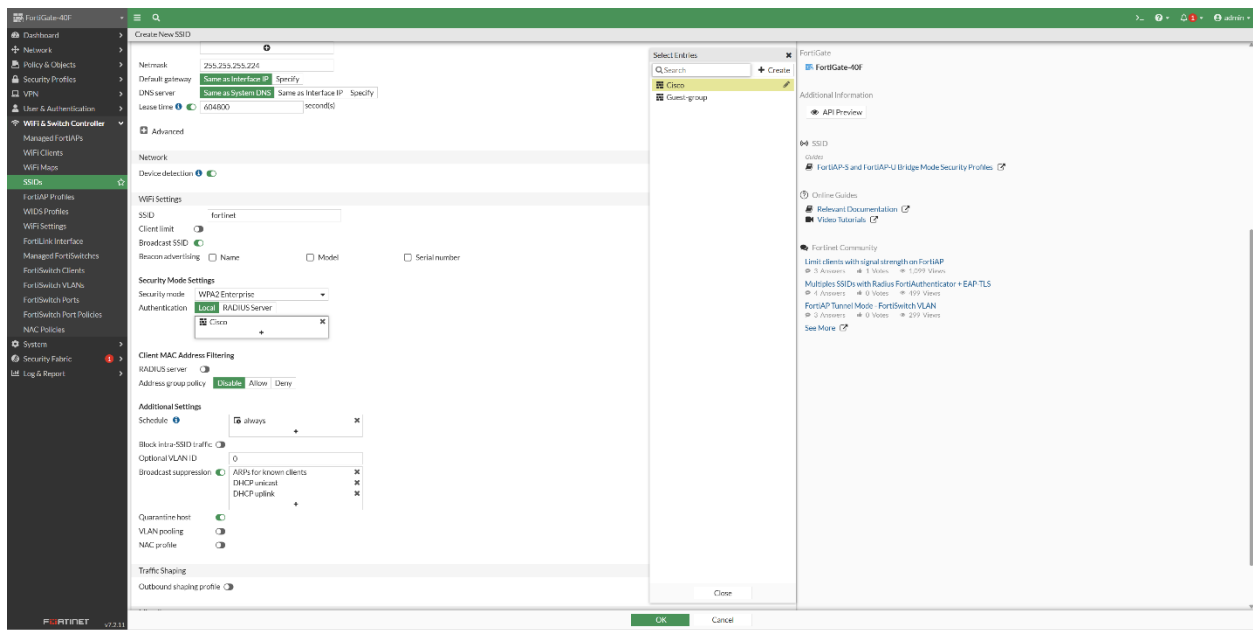
Input your chosen login credentials and click through contact info and extra info, making sure two factor authentication is off and user account status is enabled.

The first screenshot shows the 'Users/Groups Creation Wizard' window at Step 2: Login Credentials. The progress bar shows Step 1 as completed (checked) and Step 2 as active (green). The 'Username' field contains 'admin' and the 'Password' field is masked with dots.

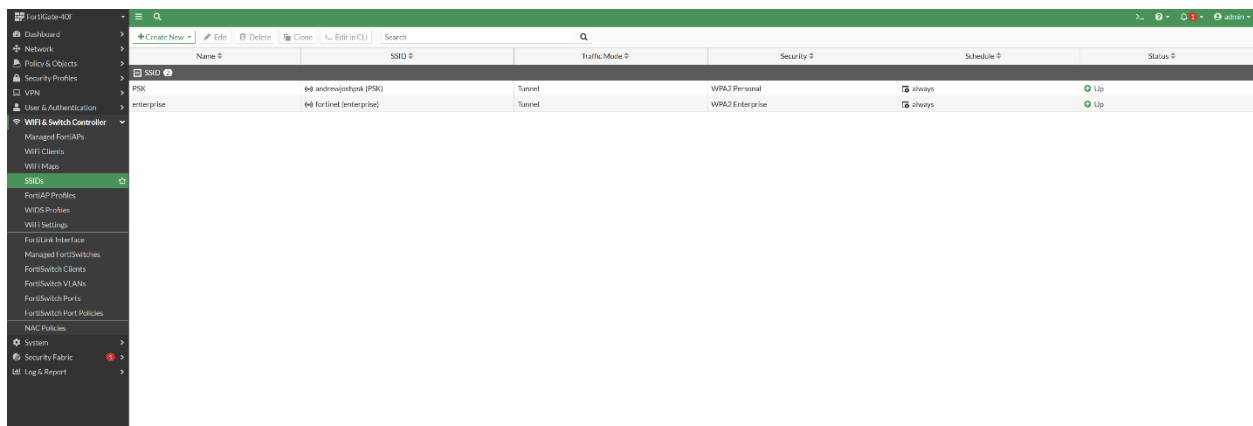
The second screenshot shows the 'Users/Groups Creation Wizard' window at Step 3: Contact Info. The progress bar shows Steps 1 and 2 as completed (checked) and Step 3 as active (green). Below the progress bar, there is a toggle switch for 'Two-factor Authentication', which is currently turned off.

The third screenshot shows the 'Users/Groups Creation Wizard' window at Step 4: Extra Info. The progress bar shows Steps 1, 2, and 3 as completed (checked) and Step 4 as active (green). Below the progress bar, there is a 'User Account Status' section with two options: 'Enabled' (selected with a green arrow) and 'Disabled' (with a red arrow). Below that, there is a 'User Group' section with a toggle switch that is currently turned off.

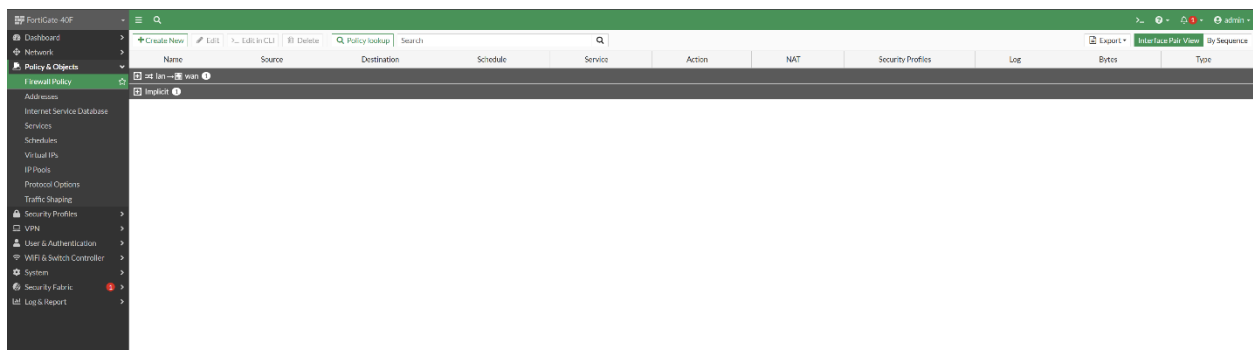
Finish creating your enterprise SSID by clicking "Ok" on the bottom of the screen.



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



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



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

The screenshot shows the 'New Policy' configuration page for Policy 1. The left sidebar contains the navigation menu with 'Policy & Objects' selected. The main configuration area is divided into several sections:

- Name:** 1
- Incoming Interface:** wan
- Outgoing Interface:** fortinet (enterprise)
- Source:** all
- Destination:** all
- Schedule:** always
- Service:** ALL
- Action:** ACCEPT (checked), DENY

Firewall/Network Options:

- NAT:** ☒
- IP Pool Configuration:** Use Outgoing Interface Address, Use Dynamic IP Pool
- Preserve Source Port:** ☐
- Protocol Options:** PROXY default

Security Profiles:

- AntiVirus:** ☐
- Web Filter:** ☐
- DNS Filter:** ☐
- Application Control:** ☐
- IPS:** ☐
- SSL Inspection:** SSL no-inspection

Logging Options:

- Log Allowed Traffic:** ☒ Security Events All Sessions

Comments: Write a comment... 0/1023

Enable this policy: ☒

Buttons: OK, Cancel

The screenshot shows the 'New Policy' configuration page for Policy 2. The left sidebar contains the navigation menu with 'Policy & Objects' selected. The main configuration area is divided into several sections:

- Name:** 2
- Incoming Interface:** fortinet (enterprise)
- Outgoing Interface:** wan
- Source:** all
- Destination:** all
- Schedule:** always
- Service:** ALL
- Action:** ACCEPT (checked), DENY

Firewall/Network Options:

- NAT:** ☒
- IP Pool Configuration:** Use Outgoing Interface Address, Use Dynamic IP Pool
- Preserve Source Port:** ☐
- Protocol Options:** PROXY default

Security Profiles:

- AntiVirus:** ☐
- Web Filter:** ☐
- DNS Filter:** ☐
- Application Control:** ☐
- IPS:** ☐
- SSL Inspection:** SSL no-inspection

Logging Options:

- Log Allowed Traffic:** ☒ Security Events All Sessions

Comments: Write a comment... 0/1023

Enable this policy: ☐

Buttons: OK, Cancel

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

The screenshot shows the FortiGate-40F web interface for configuring a new firewall policy. The left sidebar lists various configuration categories, with 'Policy & Objects' and 'Firewall Policy' selected. The main panel is titled 'New Policy' and contains the following fields:

- Name:** 3
- Incoming Interface:** wan
- Outgoing Interface:** andrewjoshpsk (PSK)
- Source:** all
- Destination:** all
- Schedule:** always
- Service:** ALL
- Action:** ACCEPT (checked), DENY

Below these fields are several sections for additional options:

- Firewall/Network Options:**
 - NAT:** enabled
 - IP Pool Configuration:** Use Outgoing Interface Address, Use Dynamic IP Pool
 - Preserve Source Port:** disabled
 - Protocol Options:** default
- Security Profiles:**
 - AntiVirus, Web Filter, DNS Filter, Application Control, IPS: all disabled
 - SSL Inspection:** no-inspection
- Logging Options:**
 - Log Allowed Traffic:** Security Events, All Sessions
- Comments:** Write a comment... (0/1023)
- Enable this policy:** checked

At the bottom right, there are 'OK' and 'Cancel' buttons.

The screenshot shows the FortiGate-40F web interface for configuring a new firewall policy, similar to the one above but for Policy 4. The left sidebar is the same. The main panel is titled 'New Policy' and contains the following fields:

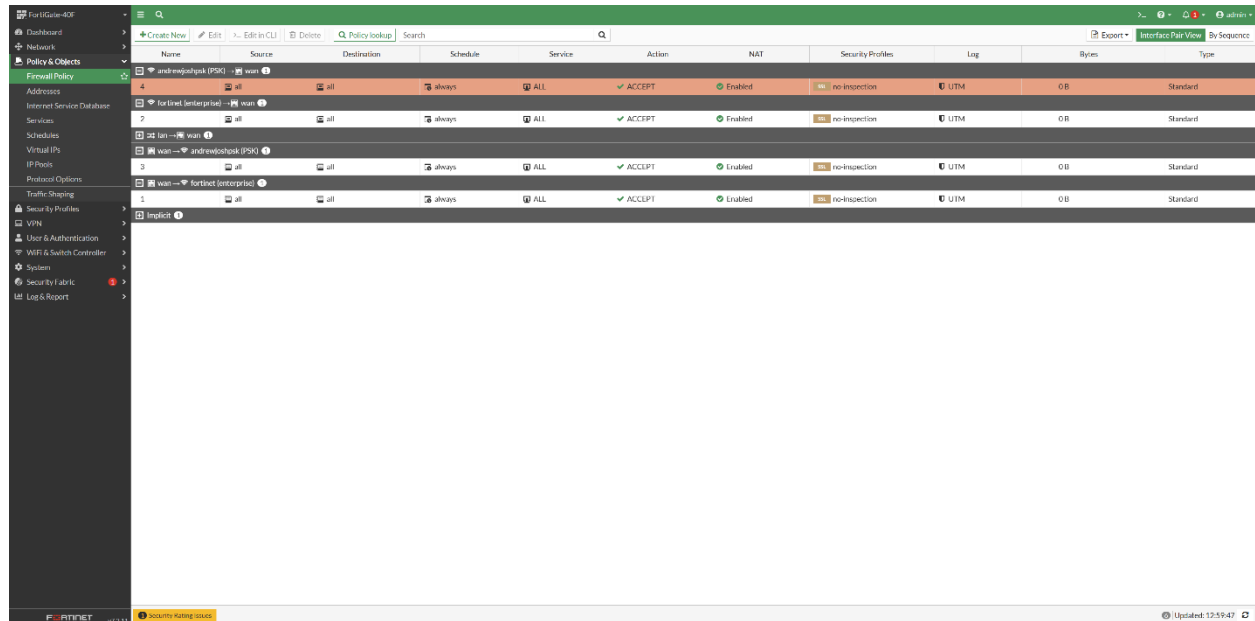
- Name:** 4
- Incoming Interface:** andrewjoshpsk (PSK)
- Outgoing Interface:** wan
- Source:** all
- Destination:** all
- Schedule:** always
- Service:** ALL
- Action:** ACCEPT (checked), DENY

Below these fields are several sections for additional options:

- Firewall/Network Options:**
 - NAT:** enabled
 - IP Pool Configuration:** Use Outgoing Interface Address, Use Dynamic IP Pool
 - Preserve Source Port:** disabled
 - Protocol Options:** default
- Security Profiles:**
 - AntiVirus, Web Filter, DNS Filter, Application Control, IPS: all disabled
 - SSL Inspection:** no-inspection
- Logging Options:**
 - Log Allowed Traffic:** Security Events, All Sessions
- Comments:** Write a comment... (0/1023)
- Enable this policy:** checked

At the bottom right, there are 'OK' and 'Cancel' buttons.

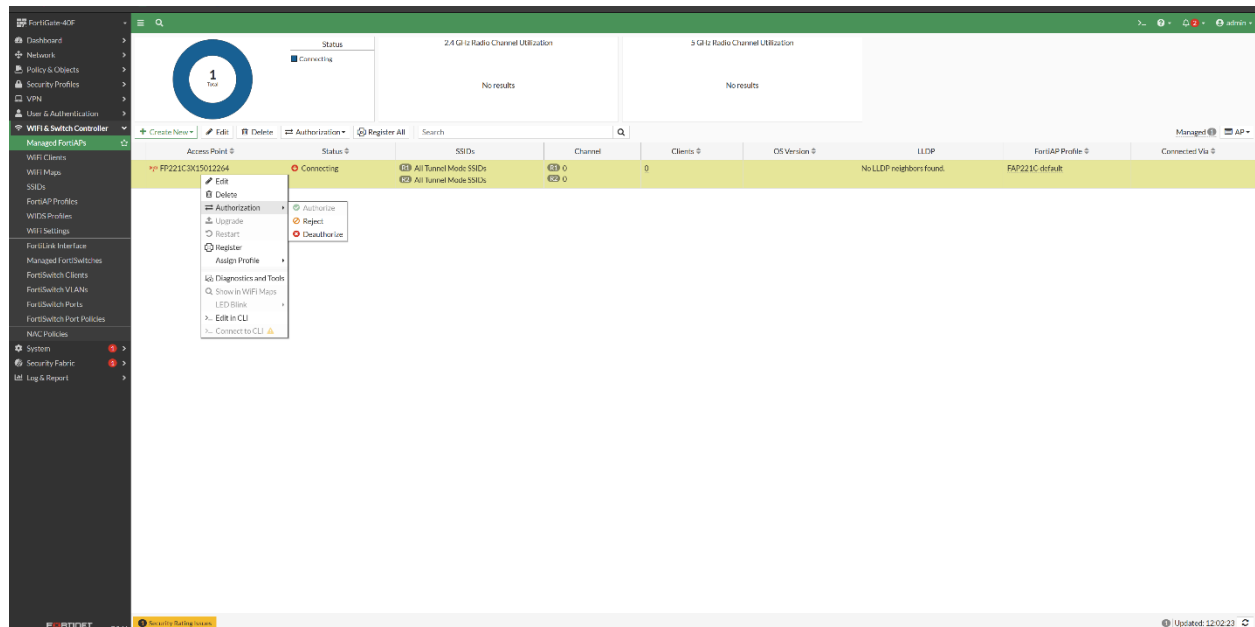
Verify that all 4 of these new policies have been created on your GUI.



The screenshot shows the FortiGate GUI with the Firewall Policy list. The table contains the following data:

Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log	Bytes	Type
4	andrew@psk (PSK)	all	always	ALL	ACCEPT	Enabled	no-inspection	UTM	0 B	Standard
7	fortinet (interperiod) → wan	all	always	ALL	ACCEPT	Enabled	no-inspection	UTM	0 B	Standard
3	wan → andrew@psk (PSK)	all	always	ALL	ACCEPT	Enabled	no-inspection	UTM	0 B	Standard
5	wan → fortinet (interperiod)	all	always	ALL	ACCEPT	Enabled	no-inspection	UTM	0 B	Standard
Implicit										

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



The screenshot shows the FortiGate GUI with the Managed FortiAPs section. The table contains the following data:

Access Point	Status	SSIDs	Channel	Clients	OS Version	LLDP	FortiAP Profile	Managed Via
FP221C3K15012264	Connecting	All Tunnel Mode SSIDs All Tunnel Mode SSIDs	0 0	0		No LLDP neighbors found	FAP221C default	Connected Via

Problems:

One of the problems that our team came across was an error in the physical wiring of the devices. By miswiring our firewall, switches, and ISP, our group

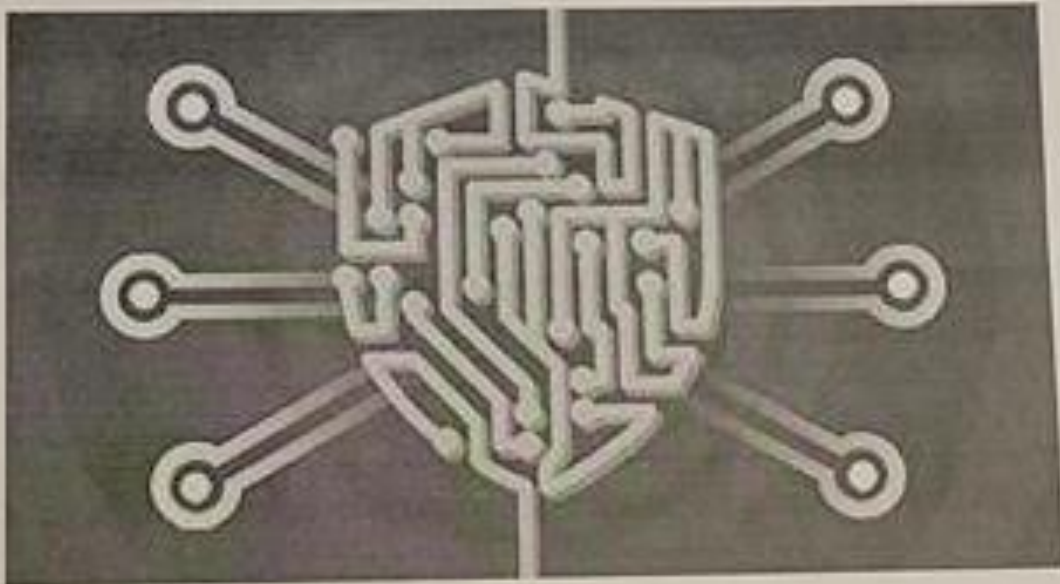
stopped ourselves from logging into the GUI of the firewall even after having reset the firewall. This prevented us from making further progress on the lab until we found our error in wiring and fixed it.

Conclusion:

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

Lab Signoff:

Fortinet SOHO with Wireless WPA2-PSK and WPA2-Enterprise



Name: Andrew Poi

