Fortinet SOHO and WPA2-PSK/Enterprise Setup

Andrew Pai

Period 5 Cybersecurity

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.

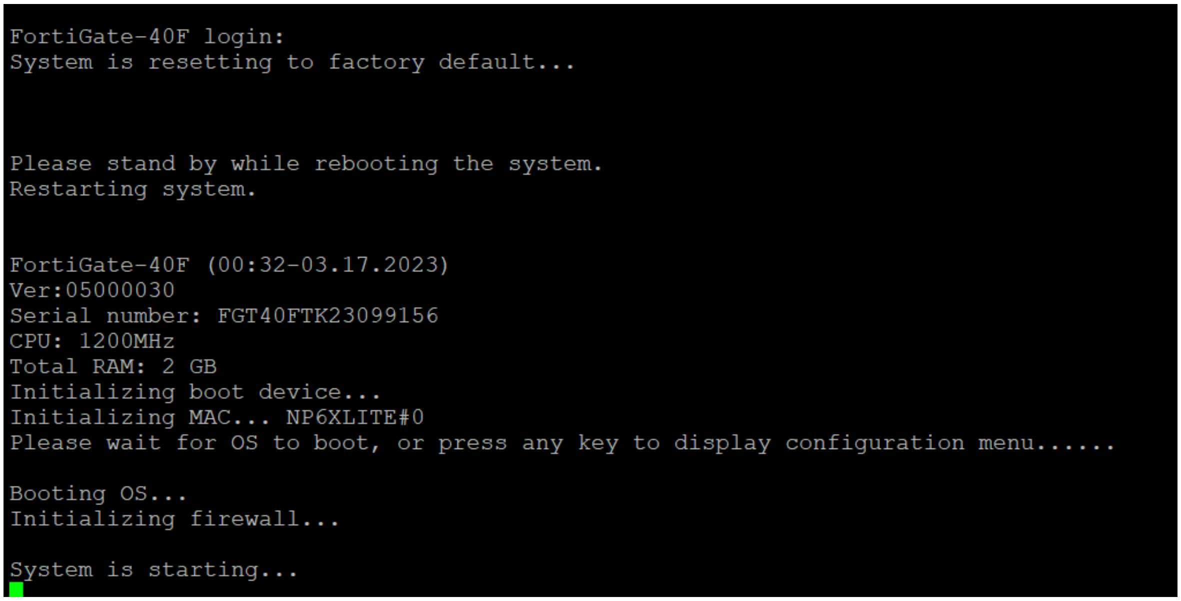
For this SOHO network that our lab is going to be setting up, we will be using a Fortigate 40F firewall from Fortinet. Based in Sunnyvale, California and founded by Ken Xie and Michael Xie, Fortinet is a cybersecurity company that creates security solutions like firewalls and intrusion detection systems. 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:

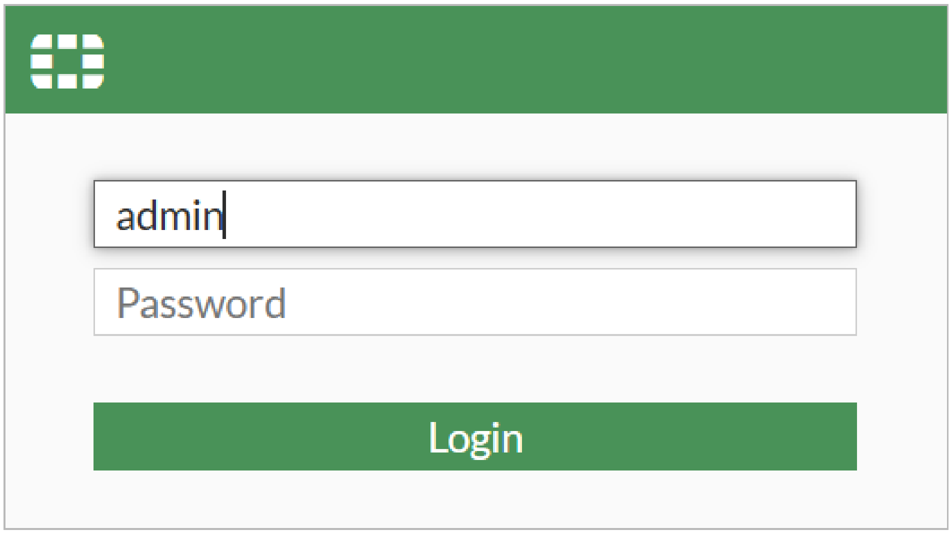
Since we're starting with a brand new Fortigate firewall, one thing that we have to do is reset the firewall to enter in new credentials. To do this, unplug the device for 10 seconds, replug it in and hold the reset button until the status light blinks.

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.



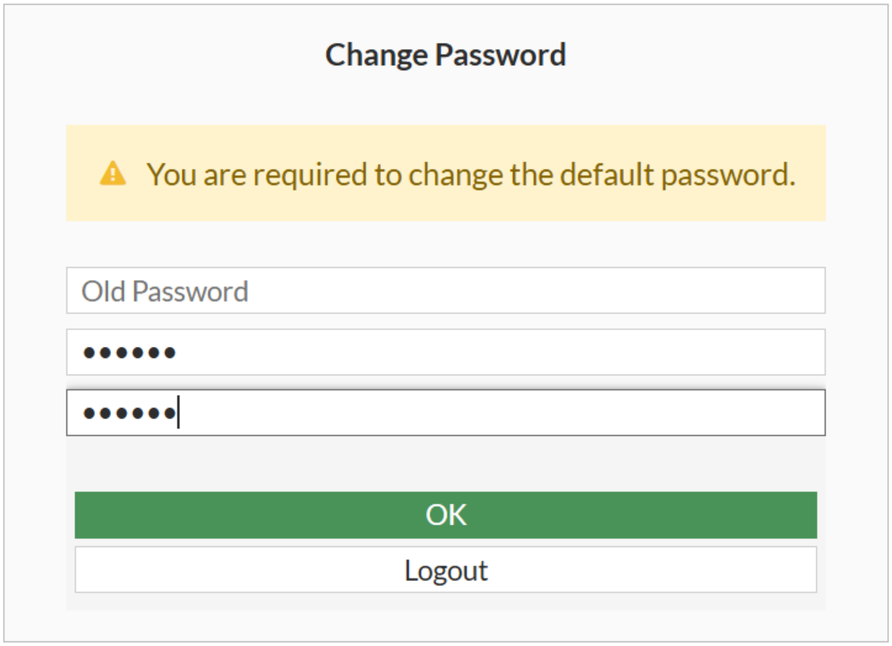
```
FortiGate-40F login:
System is resetting to factory default...



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.



admin

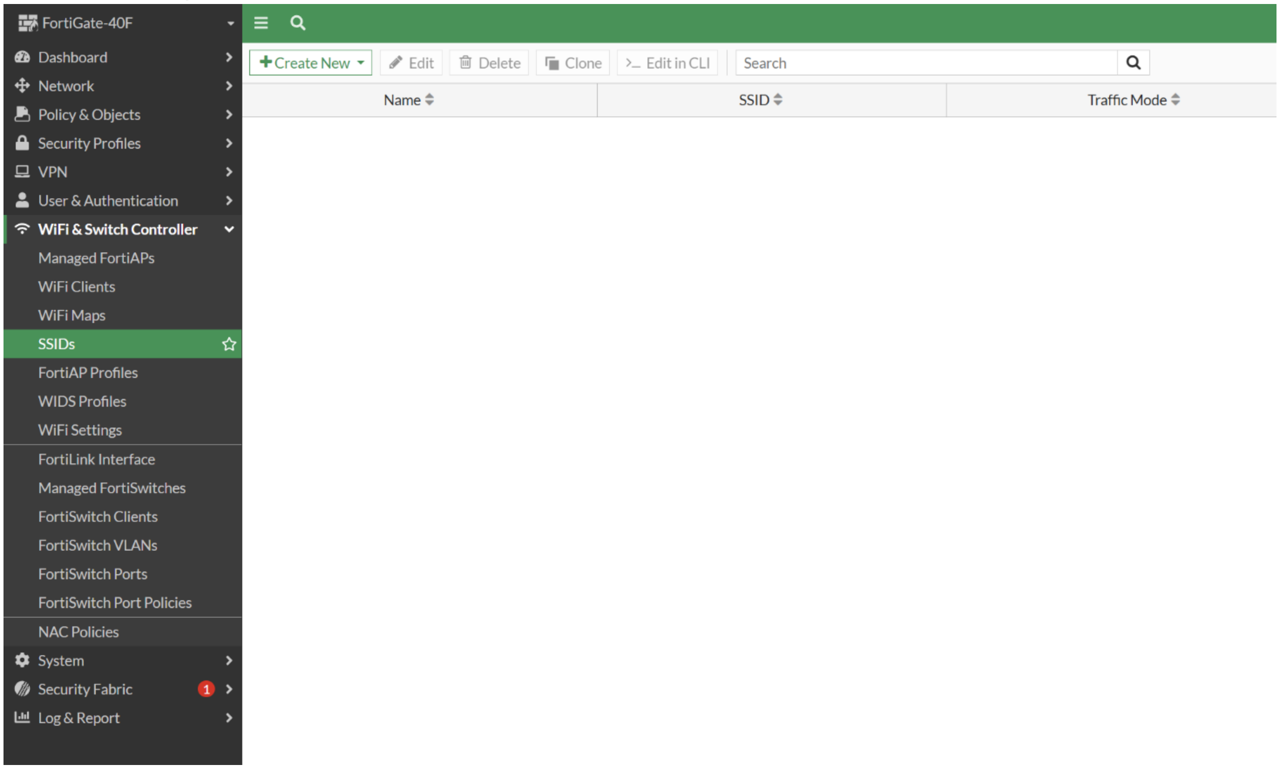
Once you've logged in with default credentials, you should be able to enter your own password and device hostname.



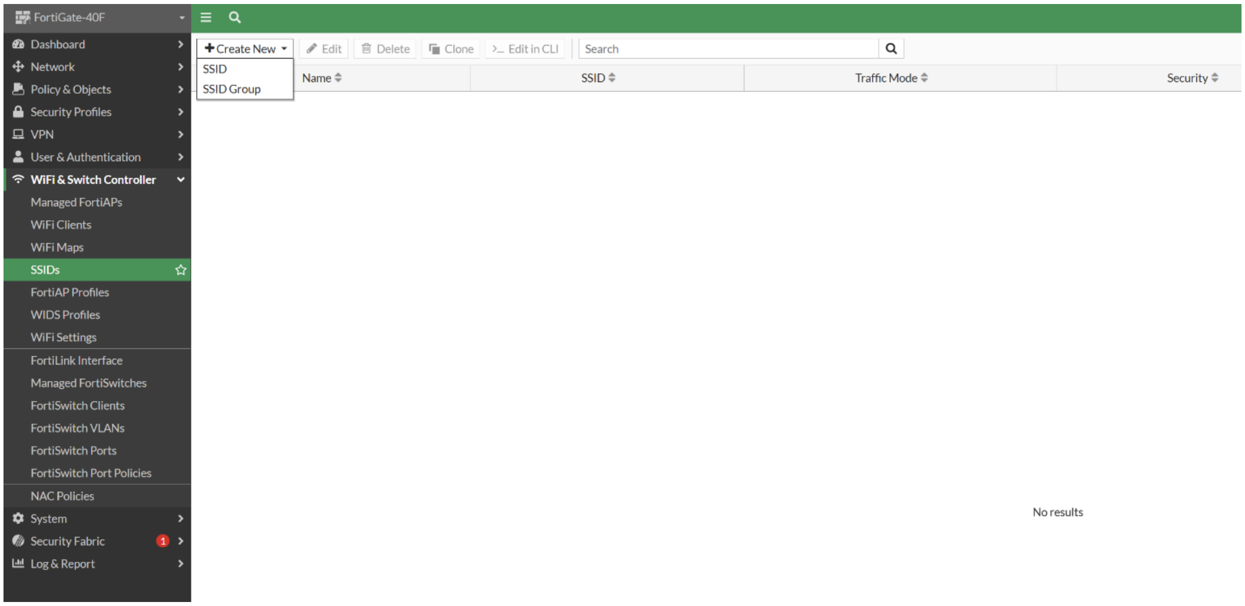
Change Password

⚠ You are required to change the default password.

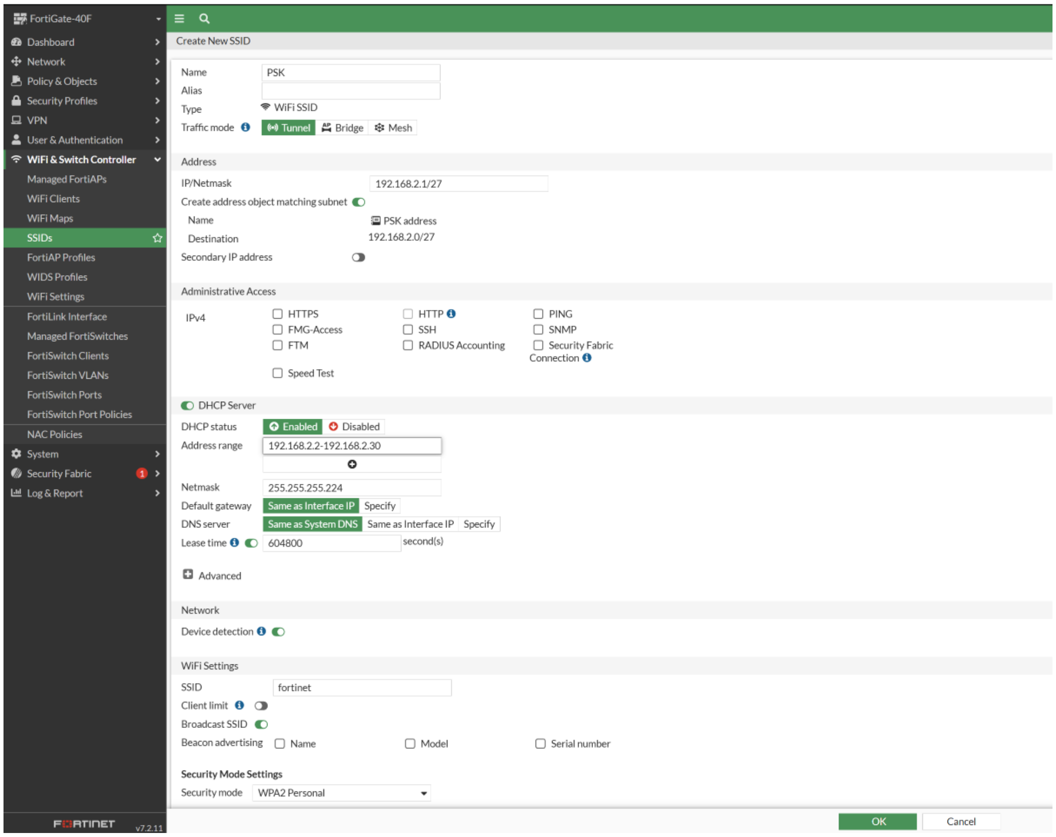
In the GUI, navigate to the "WiFi and Switch Controller" section on the left of the taskbar, and then "SSIDs" under it.



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.



Create New SSID

Name: PSK
Alias:
Type: WiFi SSID
Traffic mode: [✓ Tunnel] Bridge Mesh

Address
IP/Netmask: 192.168.2.1/27
Create address object matching subnet: ●
Name: PSK address
Destination: 192.168.2.0/27
Secondary IP address: ○

Administrative Access
IPv4
□ HTTPS □ HTTP □ PING
□ FMG-Access □ SSH □ SNMP
□ FTM □ RADIUS Accounting □ Security Fabric Connection
□ Speed Test

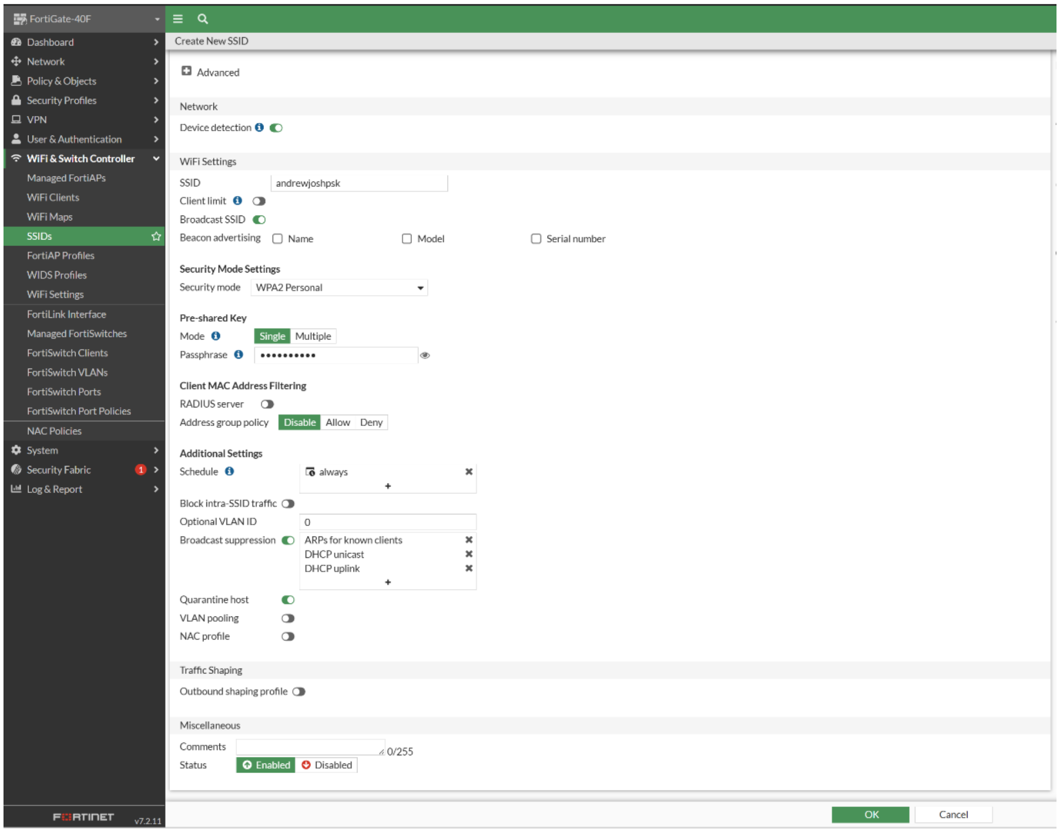
● DHCP Server
DHCP status: [✓ Enabled] Disabled
Address range: 192.168.2.2-192.168.2.30
Netmask: 255.255.255.224
Default gateway: [✓ Same as Interface IP] Specify
DNS server: [✓ Same as System DNS] Same as Interface IP Specify
Lease time: ● 604800 second(s)

Advanced

Network
Device detection: ●

WiFi Settings
SSID: fortinet
Client limit: ○
Broadcast SSID: ●
Beacon advertising: □ Name □ Model □ Serial number

Security Mode Settings
Security mode: WPA2 Personal



Create New SSID

Advanced

Network
Device detection: ●

WiFi Settings
SSID: andrewjoshpsk
Client limit: ○
Broadcast SSID: ●
Beacon advertising: □ Name □ Model □ Serial number

Security Mode Settings
Security mode: WPA2 Personal

Pre-shared Key
Mode: [✓ Single] Multiple
Passphrase: ••••••••••

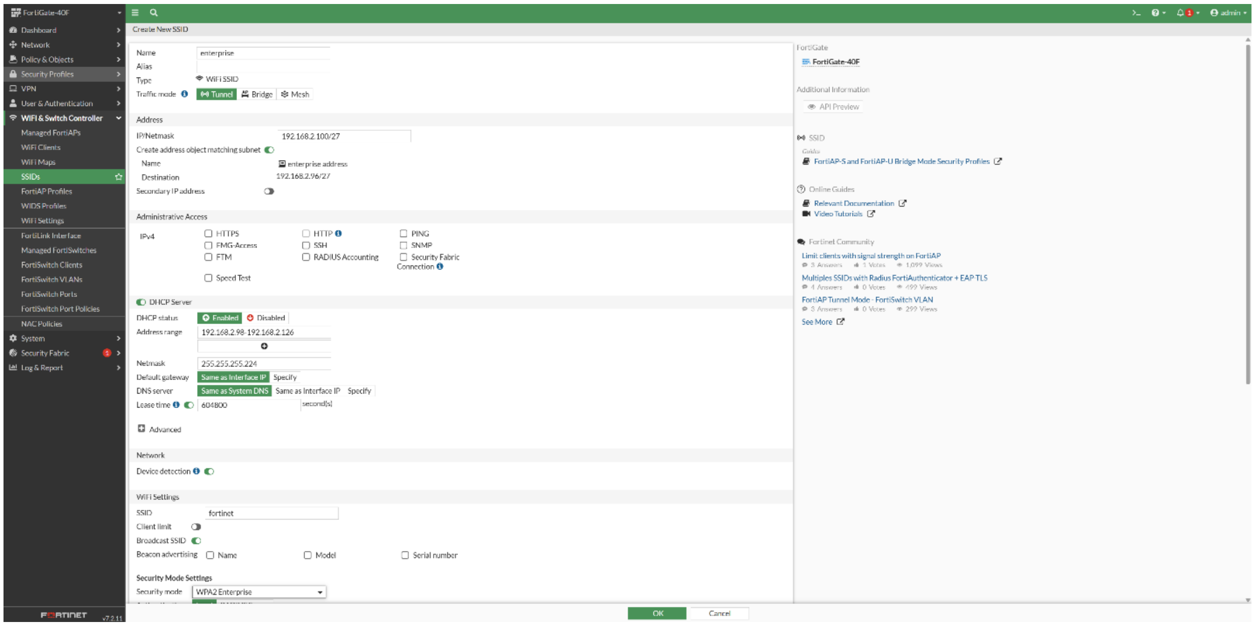
Client MAC Address Filtering
RADIUS server: ○
Address group policy: [✓ Disable] Allow Deny

Additional Settings
Schedule: always
Block intra-SSID traffic: ○
Optional VLAN ID: 0
Broadcast suppression: ● ARPs for known clients
DHCP unicast
DHCP uplink
Quarantine host: ●
VLAN pooling: ○
NAC profile: ○

Traffic Shaping
Outbound shaping profile: ○

Miscellaneous
Comments: 0/255
Status: [✓ Enabled] Disabled

Create another new SSID for the WPA2-Enterprise protocol now, choosing enterprise as the security mode.



Create New SSID

Name: enterprise
Alias:
Type: WiFi SSID
Traffic mode: [✓ Tunnel] Bridge Mesh

Address
IP/Netmask: 192.168.2.100/27
Create address object matching subnet: on
Name: enterprise address
Destination: 192.168.2.96/27
Secondary IP address: off

Administrative Access
IPv4: □ HTTPS □ HTTP □ PING □ FMG-Access □ SSH □ SNMP □ FTM □ RADIUS Accounting □ Security Fabric Connection □ Speed Test

DHCP Server: on
DHCP status: [✓ Enabled] Disabled
Address range: 192.168.2.98-192.168.2.126
Netmask: 255.255.255.224
Default gateway: [✓ Same as Interface IP] Specify
DNS server: [✓ Same as System DNS] Same as Interface IP Specify
Lease time: on 604800 second(s)

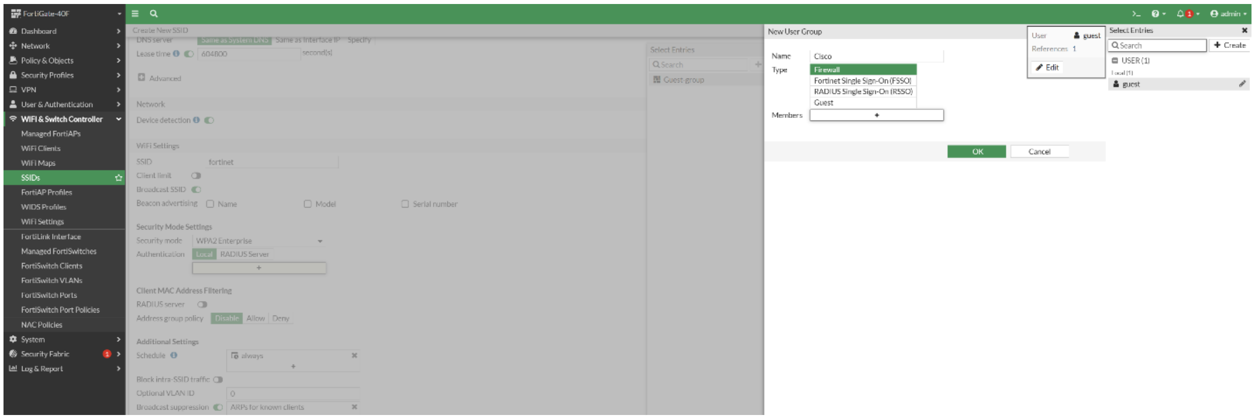
Network
Device detection: on

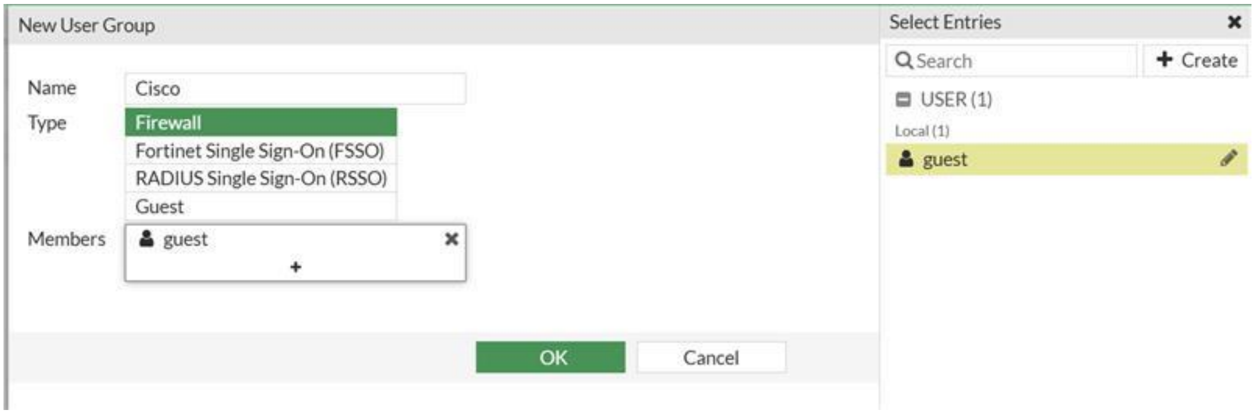
WiFi Settings
SSID: fortinet
Client limit: off
Broadcast SSID: on
Beacon advertising: □ Name □ Model □ Serial number

Security Mode Settings
Security mode: WPA2 Enterprise

OK Cancel

Create a new User Group with the “Firewall” type on the side of the Enterprise SSID creation.





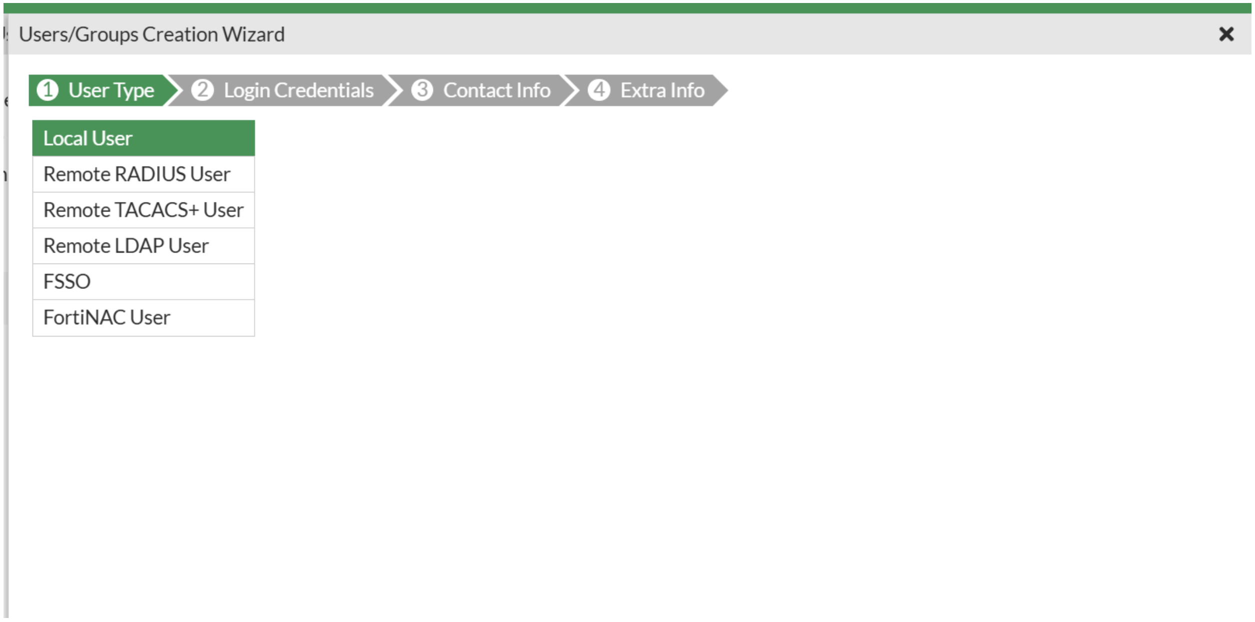
New User Group

Name: Cisco
Type: [✓ Firewall] Fortinet Single Sign-On (FSSO) RADIUS Single Sign-On (RSSO) Guest
Members: guest

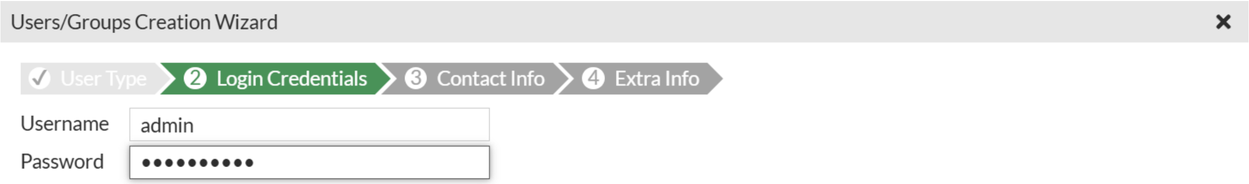
OK Cancel

Select Entries
Search + Create
USER (1)
Local (1)
guest

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

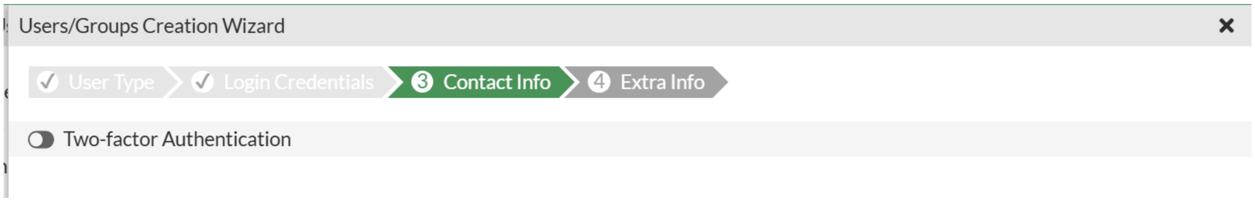


Input your chosen login credentials and click through contact info and extra info, making sure two factor authentication is off and user account status is enabled.

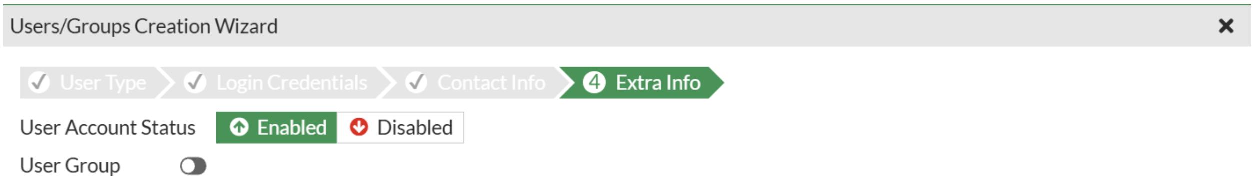


Username admin

Password ••••••••••



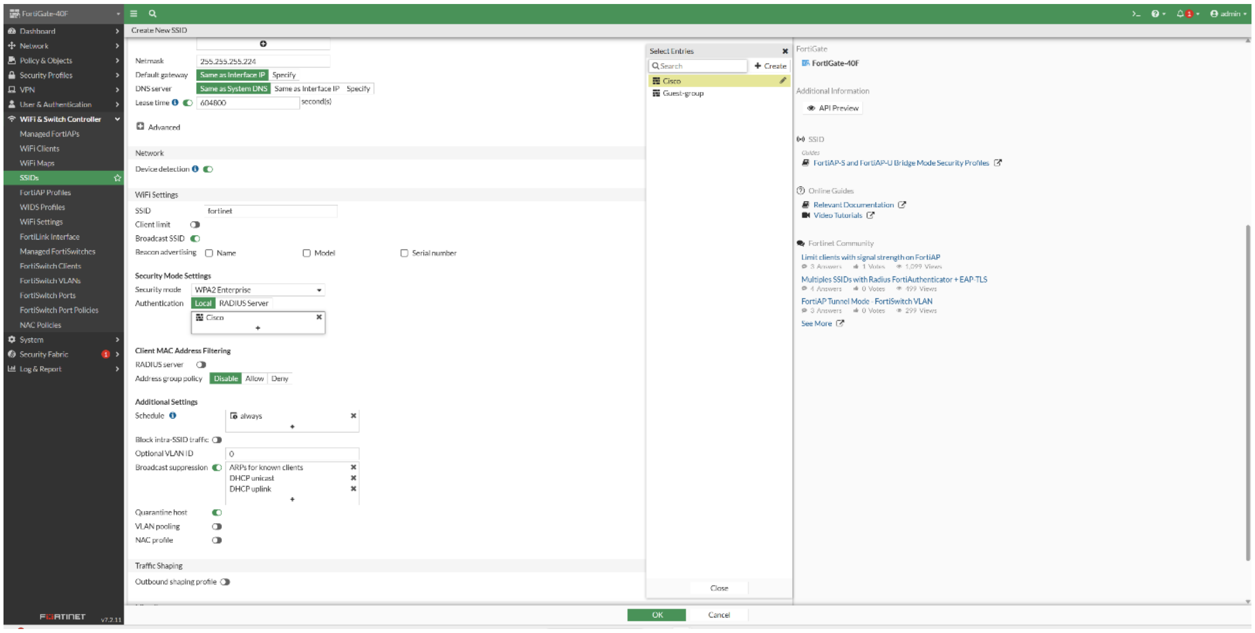
○ Two-factor Authentication



User Account Status [✓ Enabled] Disabled

User Group ○

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


Create New SSID

Netmask: 255.255.255.224
Default gateway: Same as Interface IP
DNS server: Same as System DNS
Lease time: 604800 second(s)

Network
Device detection: enabled

WiFi Settings
SSID: fortinet
Client limit: disabled
Broadcast SSID: enabled
Beacon advertising: ☐ Name ☐ Model ☐ Serial number

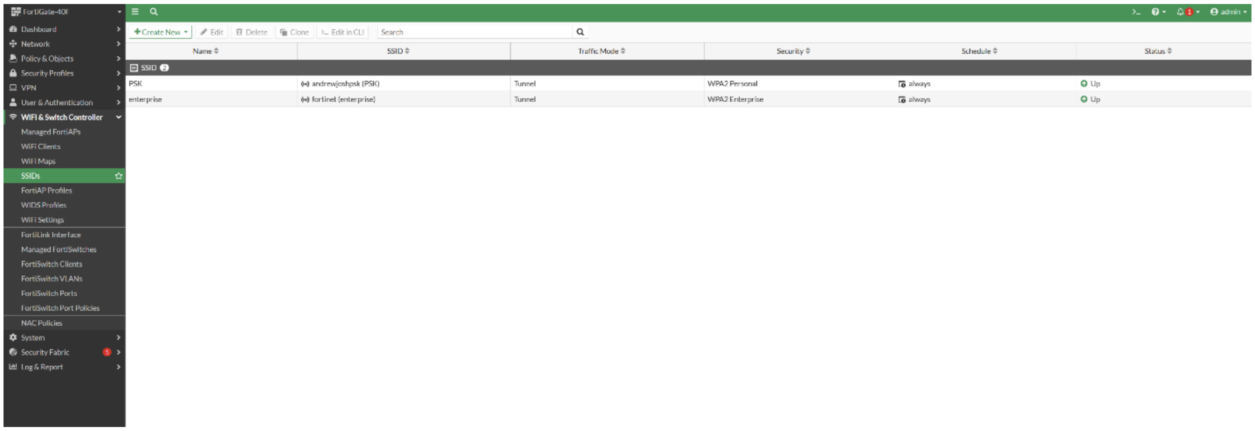
Security Mode Settings
Security mode: WPA2 Enterprise
Authentication: Local
Cisco

Client MAC Address Filtering
RADIUS server: disabled
Address group policy: Disable

Additional Settings
Schedule: always
Block intra-SSID traffic: disabled
Optional VLAN ID: 0
Broadcast suppression: enabled — ARPs for known clients, DHCP unicast, DHCP uplink
Quarantine host: enabled
VLAN pooling: disabled
NAC profile: disabled

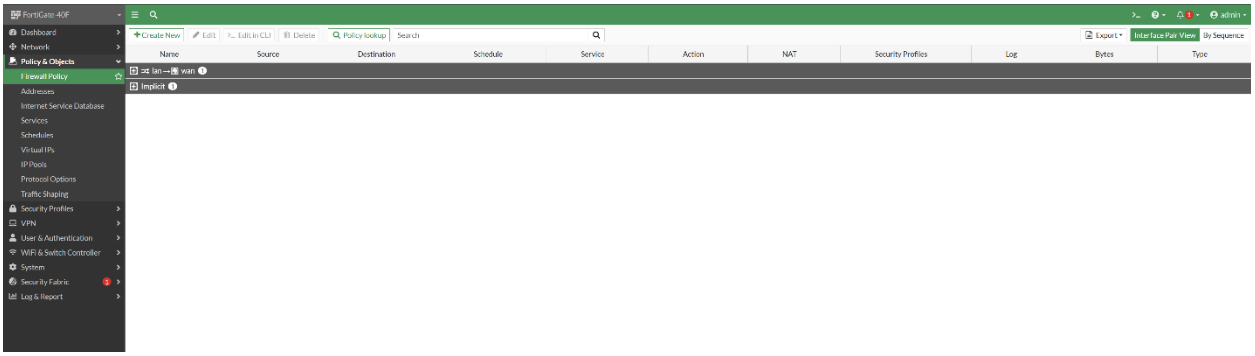
Traffic Shaping
Outbound shaping profile: disabled

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



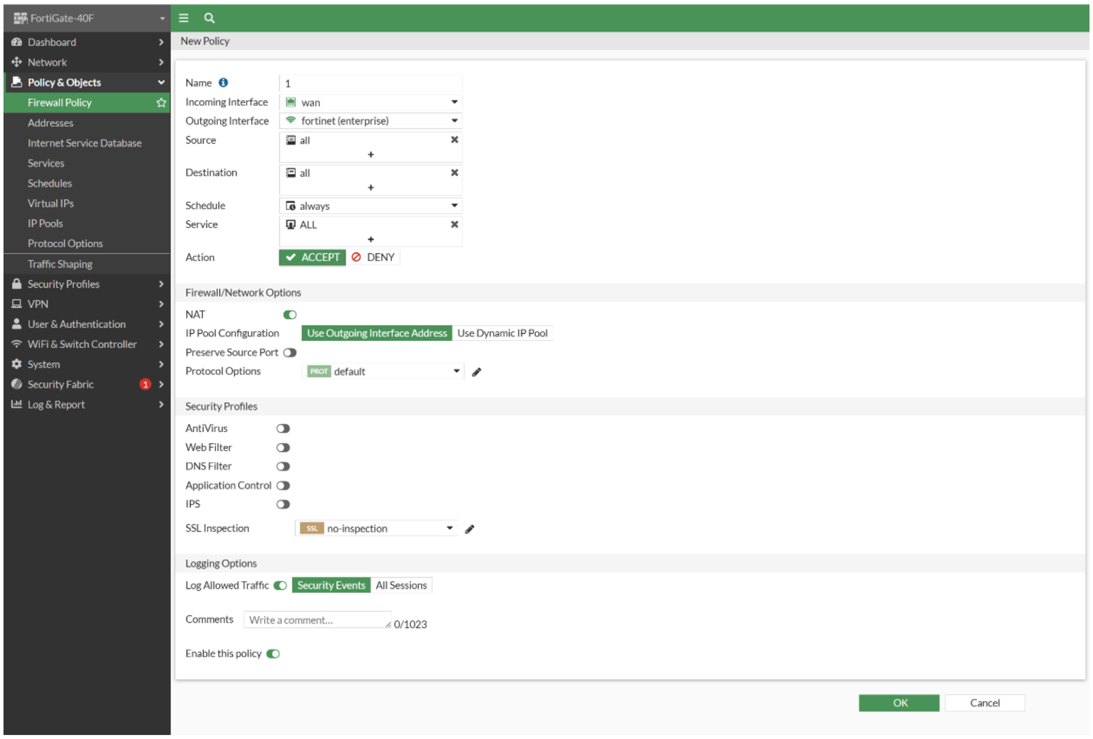
Name	SSID	Traffic Mode	Security	Schedule	Status
SSID 2					
PSK	andrewjoshpsk (PSK)	Tunnel	WPA2 Personal	always	Up
enterprise	fortinet (enterprise)	Tunnel	WPA2 Enterprise	always	Up

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



Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log	Bytes	Type
lan → wan										
Implicit										

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”.



New Policy

Name: 1
Incoming Interface: wan
Outgoing Interface: fortinet (enterprise)
Source: all
Destination: all
Schedule: always
Service: ALL
Action: ✓ ACCEPT | DENY

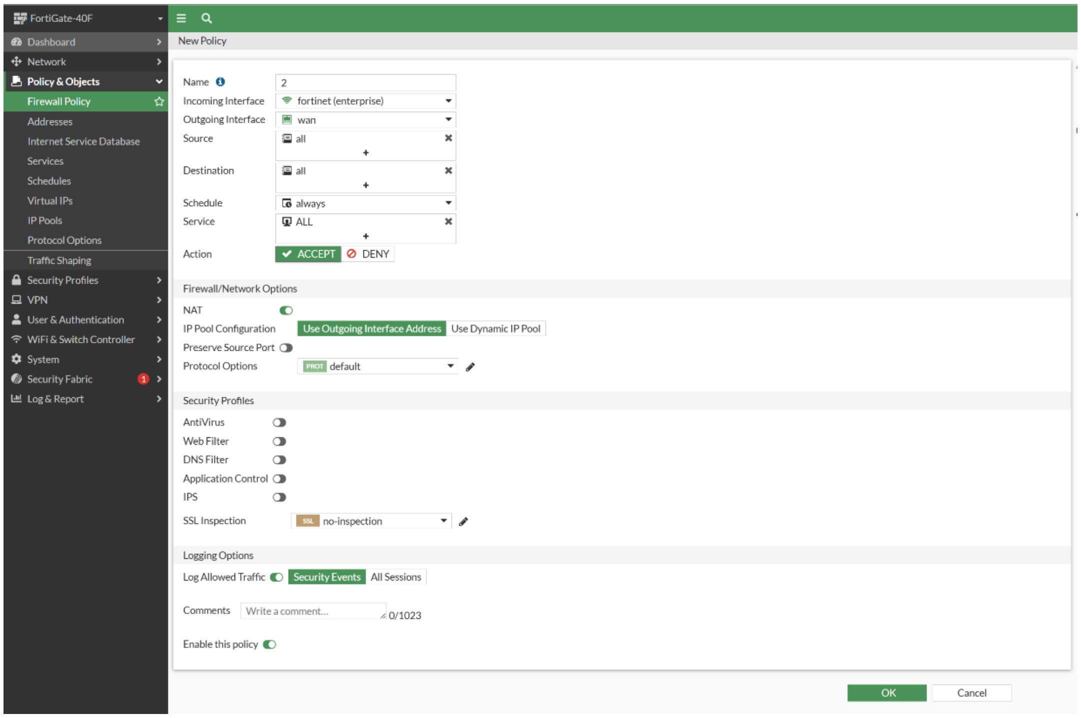
Firewall/Network Options
NAT: ●
IP Pool Configuration: Use Outgoing Interface Address | Use Dynamic IP Pool
Preserve Source Port: ○
Protocol Options: PROT default

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: ●



New Policy

Name: 2
Incoming Interface: fortinet (enterprise)
Outgoing Interface: wan
Source: all
Destination: all
Schedule: always
Service: ALL
Action: ✓ ACCEPT | DENY

Firewall/Network Options
NAT: ●
IP Pool Configuration: Use Outgoing Interface Address | Use Dynamic IP Pool
Preserve Source Port: ○
Protocol Options: PROT default

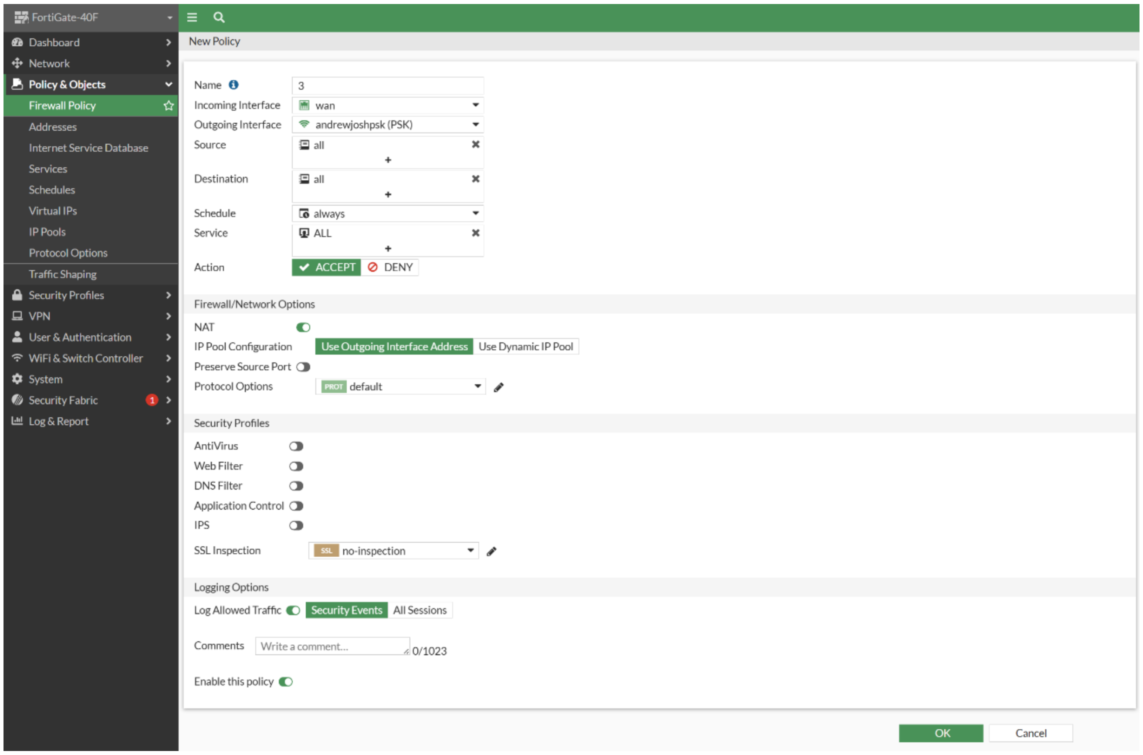
Security Profiles
AntiVirus: ○
Web Filter: ○
DNS Filter: ○
Application Control: ○
IPS: ○
SSL Inspection: SSL no-inspection

Logging Options
Log Allowed Traffic: ● Security Events | All Sessions

Comments: Write a comment... 0/1023

Enable this policy: ●

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.



New Policy

Name 3
Incoming Interface wan
Outgoing Interface andrewjoshpsk (PSK)
Source all
Destination all
Schedule always
Service ALL
Action ✓ ACCEPT DENY

Firewall/Network Options

NAT ●
IP Pool Configuration [✓ Use Outgoing Interface Address] Use Dynamic IP Pool
Preserve Source Port ○
Protocol Options PROT default

Security Profiles

AntiVirus ○
Web Filter ○
DNS Filter ○
Application Control ○
IPS ○
SSL Inspection SSL no-inspection

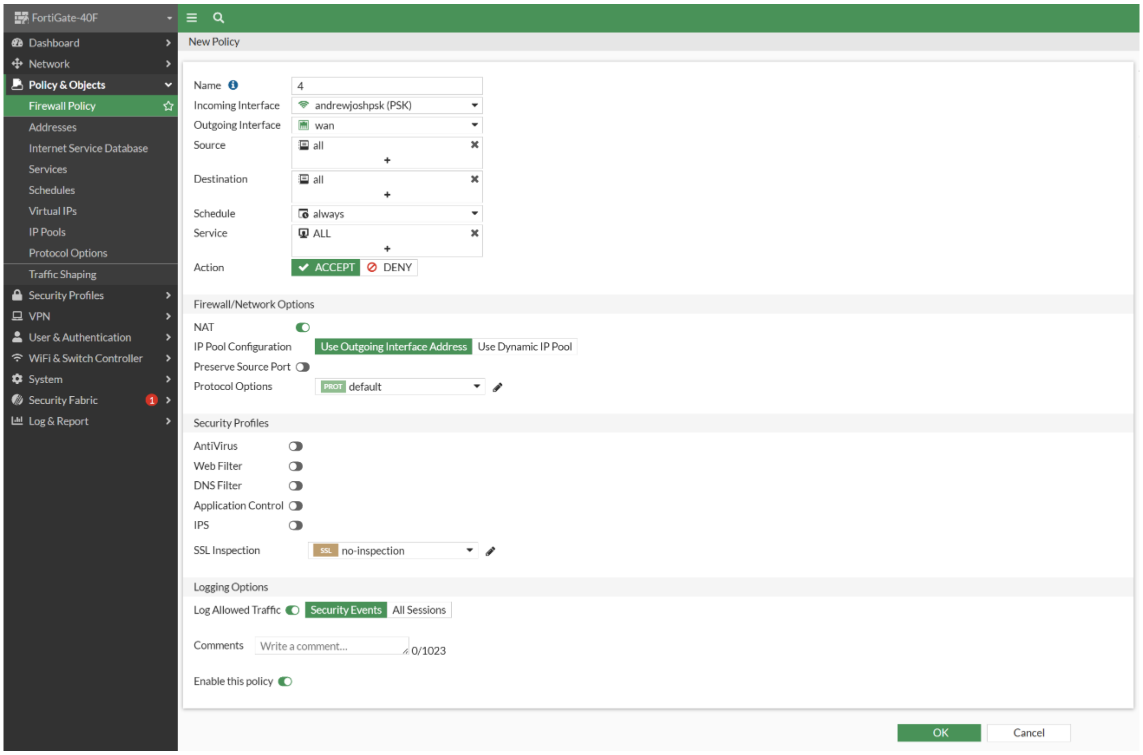
Logging Options

Log Allowed Traffic ● [✓ Security Events] All Sessions

Comments Write a comment... 0/1023

Enable this policy ●

OK Cancel



New Policy

Name 4
Incoming Interface andrewjoshpsk (PSK)
Outgoing Interface wan
Source all
Destination all
Schedule always
Service ALL
Action ✓ ACCEPT DENY

Firewall/Network Options

NAT ●
IP Pool Configuration [✓ Use Outgoing Interface Address] Use Dynamic IP Pool
Preserve Source Port ○
Protocol Options PROT default

Security Profiles

AntiVirus ○
Web Filter ○
DNS Filter ○
Application Control ○
IPS ○
SSL Inspection SSL no-inspection

Logging Options

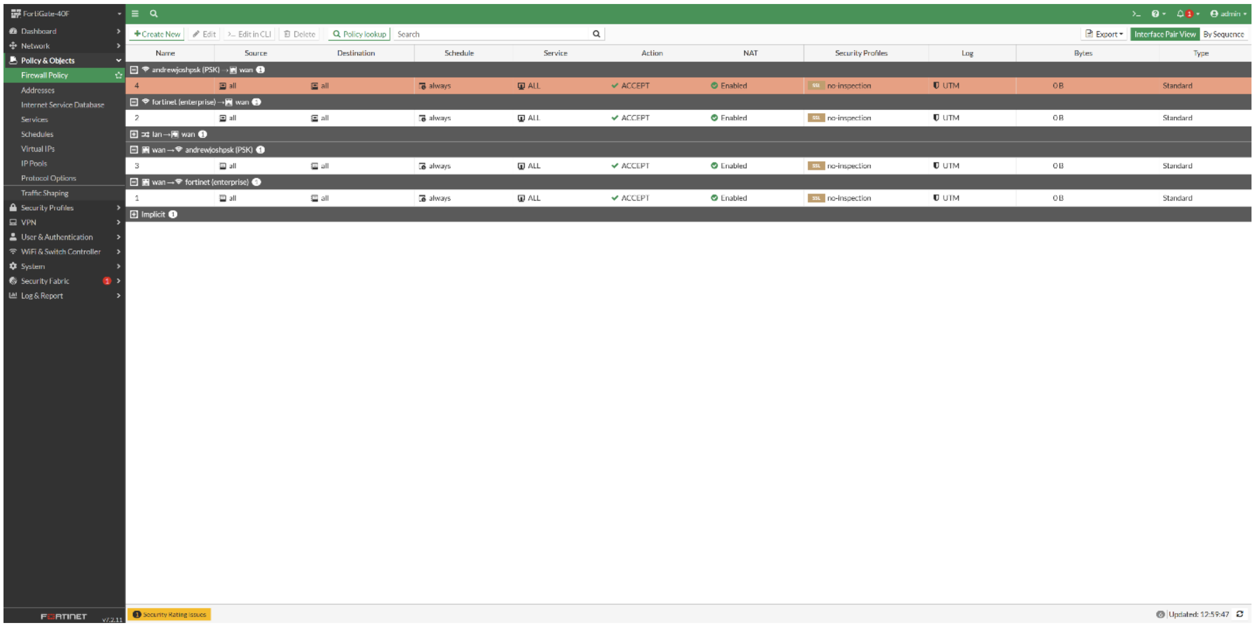
Log Allowed Traffic ● [✓ Security Events] All Sessions

Comments Write a comment... 0/1023

Enable this policy ●

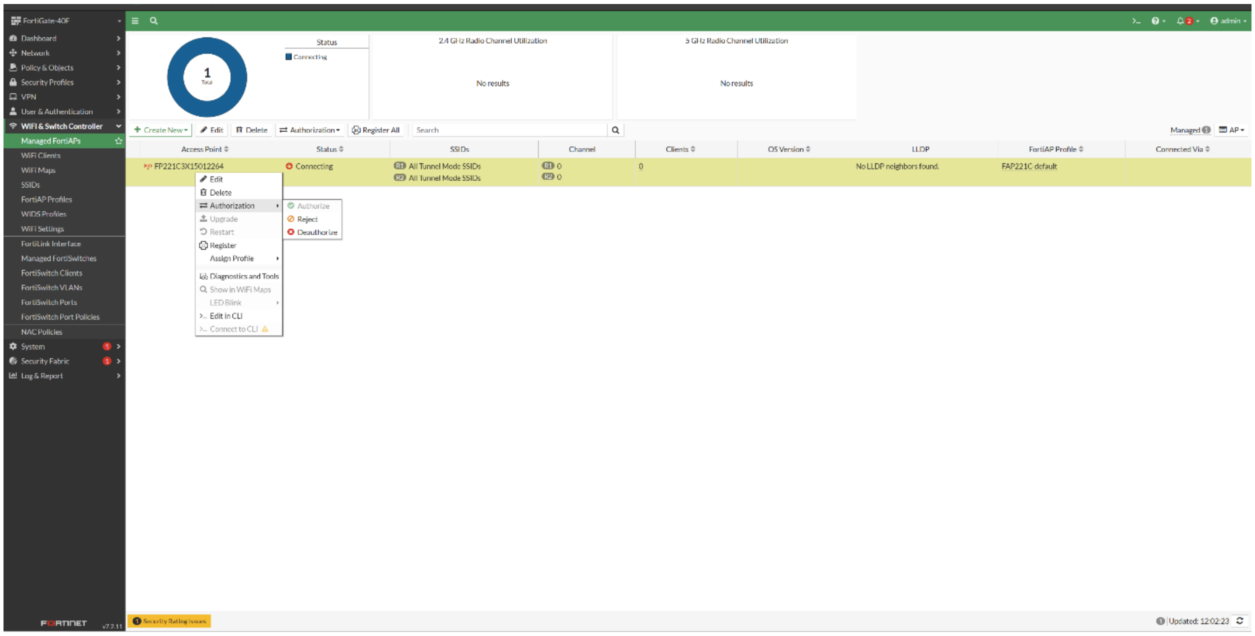
OK Cancel

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



Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log	Bytes	Type
andrewjoshpsk (PSK) → wan 1										
4	all	all	always	ALL	✓ ACCEPT	Enabled	SSL no-inspection	UTM	0 B	Standard
fortinet (enterprise) → wan 1										
2	all	all	always	ALL	✓ ACCEPT	Enabled	SSL no-inspection	UTM	0 B	Standard
lan → wan 1										
wan → andrewjoshpsk (PSK) 1										
3	all	all	always	ALL	✓ ACCEPT	Enabled	SSL no-inspection	UTM	0 B	Standard
wan → fortinet (enterprise) 1										
1	all	all	always	ALL	✓ ACCEPT	Enabled	SSL no-inspection	UTM	0 B	Standard
Implicit 1										

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



Access Point	Status	SSIDs	Channel	Clients	OS Version	LLDP	FortiAP Profile	Connected Via
FP221C3X15012264	Connecting	R1 All Tunnel Mode SSIDs R2 All Tunnel Mode SSIDs	R1 0 R2 0	0		No LLDP neighbors found.	FAP221C default	

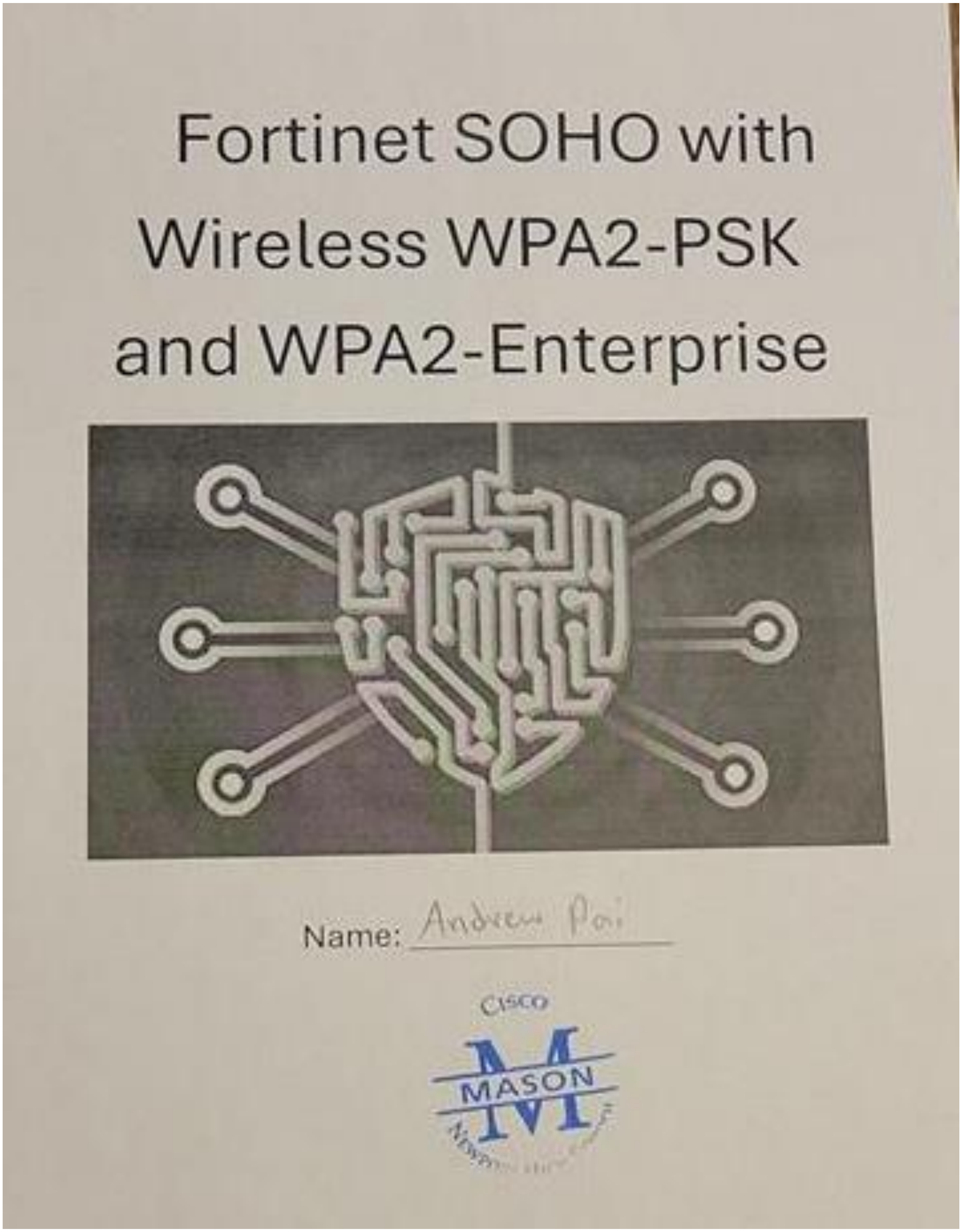
Problems:

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

CISCO

MASON