Introduction:

Using a ForiGate 40F, we paired it up with a Fortinet FAP-221c. We configured it to broadcast 2 SSIDs, one running WPA2 PSK and one running WPA2 Enterprise. Our 40F firewall acted as a Wireless Lan Controller (WLC) for the AP allowing for the WPA2 Enterprise to work.

Background information:

Wi-Fi Protection Access (WPA) are security certification protocol that uses encryption methods like Terminal Key Integration Protocol (TKIP) and AES to encrypt packets that travel across the network. Each packet has its own encryption key which ensures that even if one, or a few, packets are decrypted, other packets being sent are still protected from any malicious users.

WPA was originally released in 2003 to replace Wired Equivalent Privacy (WEP). It used TKIP as its encryption method that used a unique key for each packet, preventing the types of attacks that plagued WEP in the past. WPA also included Message Integrity Check (MIC) that prevents hackers from altering packets on the network and resending it as if it is the same packets. MIC replaced Cyclic Redundancy Check (CRC) that was used in WEP. CRC did not provide a sufficient data integrity check on the packets it handled and proved to be venerable requiring a replacement.

WPA2 is what we used in this lab. Released in 2004 in order to replace WPA, WPA2 implemented elements of the IEEE 802.11i like Counter-Mode/CBC-Mac Protocol (CCMP) encryption, an Advanced Encryption Standard (AES) based encryption protocol. WPA 2 utilizes a 4-way handshake that involves the AP and client sending each other random number, then based on this number a PTK is made, and an encrypted message is sent by the AP and decrypted by the client. This allows encryption and authentication method has ensured WPA2 remained a robust security standard for wireless networks for 14 years till it was replaced by WPA3.

WPA3 was announced to be replacing WPA2 in January of 2018. WPA3 mode Enterprise mode more secure as it now uses a 192-bit cryptographic strength opposed to the old 128-bit standard in WPA2. WPA3 also replaced the PSK exchange with a Simultaneous Authentication of Equals (SAE) exchange which allows for a more secure initial key exchange (4 way handshake).

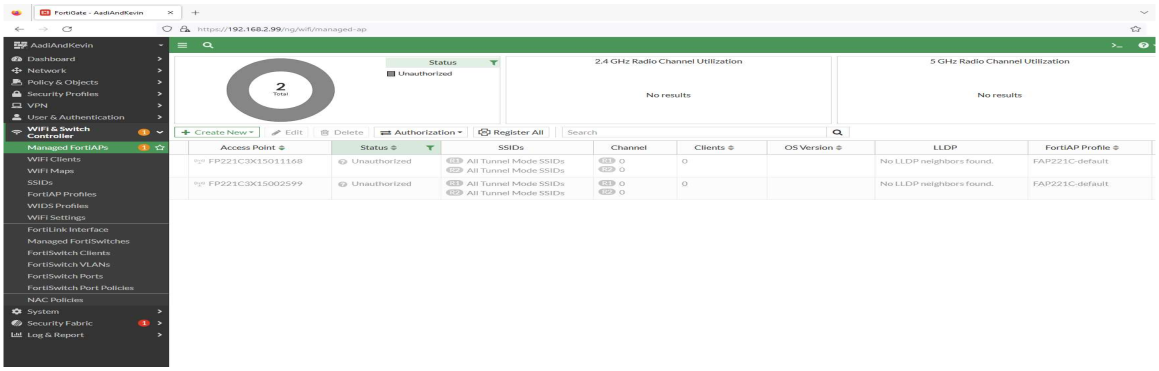
WPA Enterprise differs from normal WPA as it uses a radius server to set up user IDs. These unique user IDs require a Username and Password when initially signing into the network. This ensures everyone on a network running WPA Enterprise uses a different login credential. The network can be set up to only allow a certain number of sessions per user ID on the network ensuring that users can't share their login with coworkers or friends. This allows for a more secure and safter network, specifically design for business environment.

Tunnel and Bridge mode differ as Bridge Mode works by creating a virtual bridge between the wireless and wired networks. This allows wired and wireless traffic to be on the same local network. Tunnel mode on the other hand creates a separate network for wireless traffic (a tunnel). All wireless traffic is then encapsulated and sent to the FortiGate firewall for processing. This creates a new virtual interface on the FortiGate with the SSID name specifically designed for the tunneled wireless traffic.

Lab Summary:

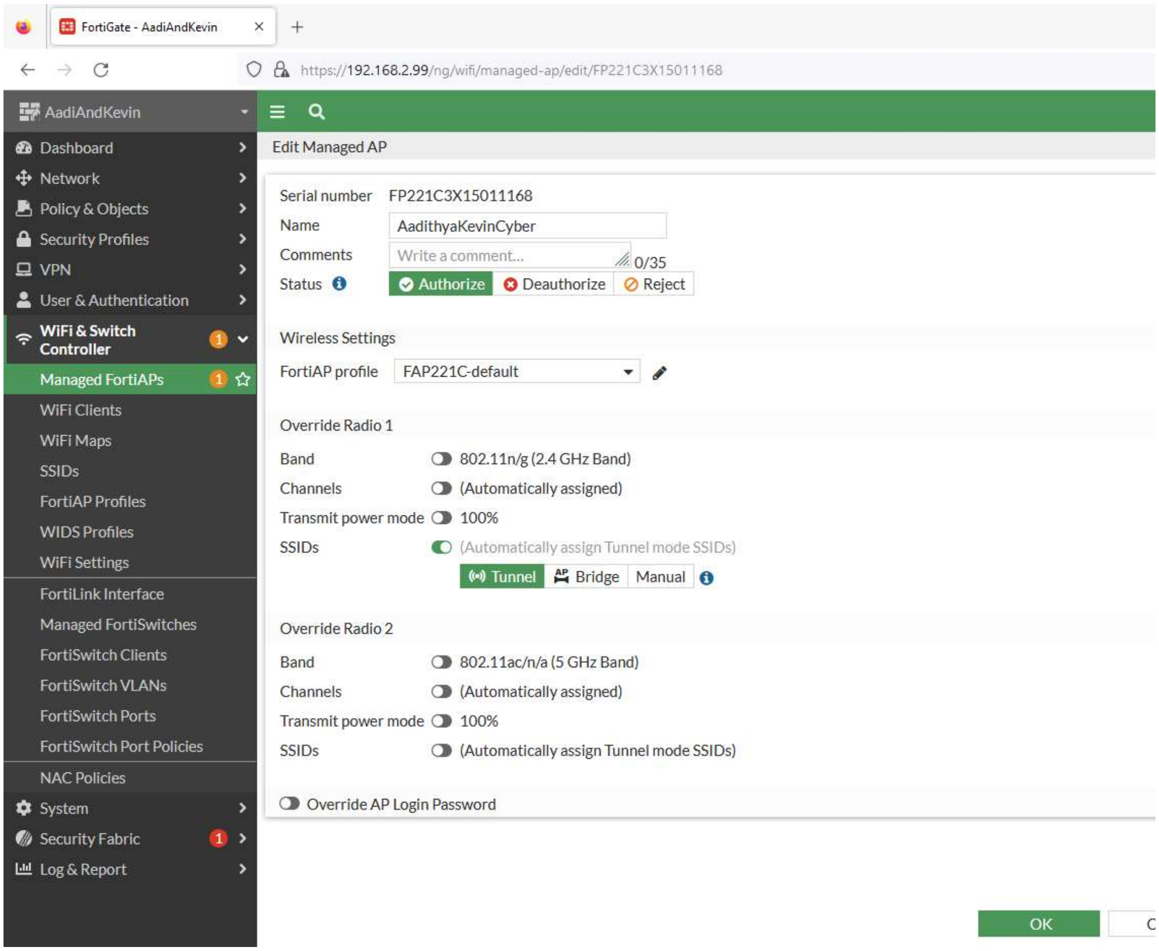
All of this Fortinet AP lab can be done within the FortiGate 40F GUI which made this process much simpler and more time efficient. First going to Managed FortiAPs, we set up our connected AP to have its SSIDs in tunnel mode. We then go to SSIDs and create 2 new SSIDs, one for WPA2 Personal and one for WPA2 Enterprise. Ensure these SSIDs have NAT and DHCP running. In order for WPA2 Enterprise to work we need to set up users on a radius server, however the 40F firewall will be able to act as the radius server in this case. Set up local users in User Definition all with unique usernames and passwords. Finally we just need to go to Firewall Policy in order to create 4 different policies that will allow for traffic to route from the Internet Wan (outside network) to our FortiAP SSIDs. 4 policies are needed as each policy only deals with incoming traffic OR outgoing, not both.

Step-by-step:



Access Point	Status	SSIDs	Channel	Clients	OS Version	LLDP	FortiAP Profile
FP221C3X15011168	Unauthorized	R1 All Tunnel Mode SSIDs R2 All Tunnel Mode SSIDs	R1 0 R2 0	0		No LLDP neighbors found.	FAP221C-default
FP221C3X15002599	Unauthorized	R1 All Tunnel Mode SSIDs R2 All Tunnel Mode SSIDs	R1 0 R2 0	0		No LLDP neighbors found.	FAP221C-default

1: Go to WiFi & Switch Controller > Managed FortiAPs, select your AP’s Serial Number shown on the bottom of the AP, and click Edit.



https://192.168.2.99/ng/wifi/managed-ap/edit/FP221C3X15011168

Edit Managed AP

Serial number FP221C3X15011168
Name AadithyaKevinCyber
Comments Write a comment... 0/35
Status Authorize Deauthorize Reject

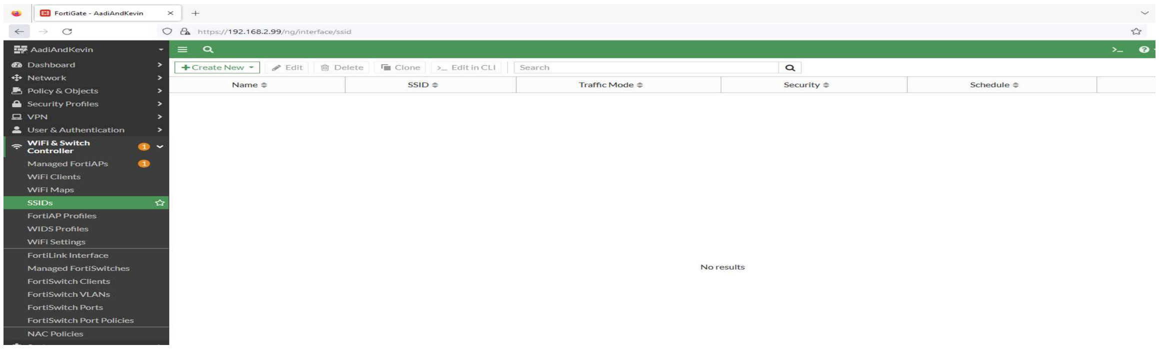
Wireless Settings
FortiAP profile FAP221C-default

Override Radio 1
Band 802.11n/g (2.4 GHz Band)
Channels (Automatically assigned)
Transmit power mode 100%
SSIDs (Automatically assign Tunnel mode SSIDs)
Tunnel Bridge Manual

Override Radio 2
Band 802.11ac/n/a (5 GHz Band)
Channels (Automatically assigned)
Transmit power mode 100%
SSIDs (Automatically assign Tunnel mode SSIDs)

Override AP Login Password

2: Under the AP manager, configure as shown above, ensure the AP SSID is in Tunnel Mode. Click OK.

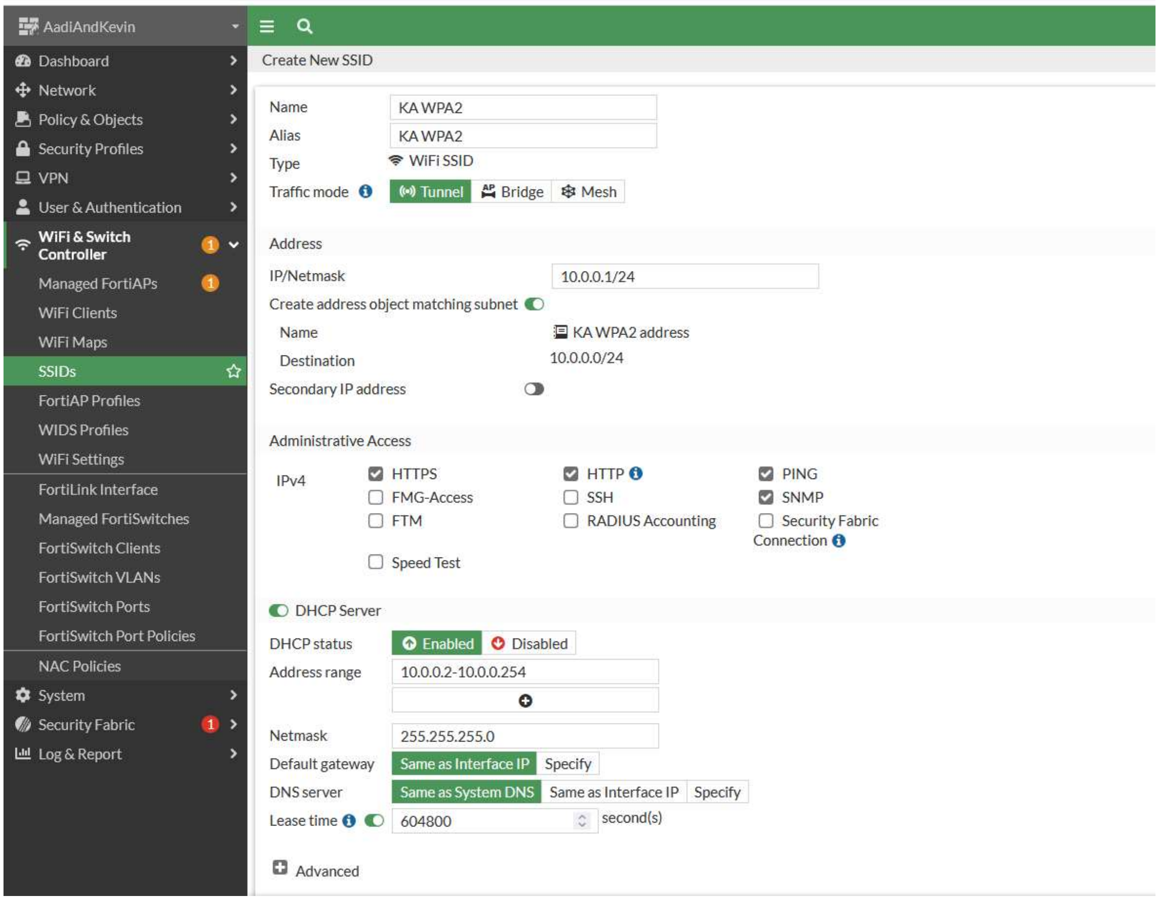


https://192.168.2.99/ng/interface/ssid

Name	SSID	Traffic Mode	Security	Schedule

No results

3: WiFi & Switch Controller > SSIDs, click Create New.



Create New SSID

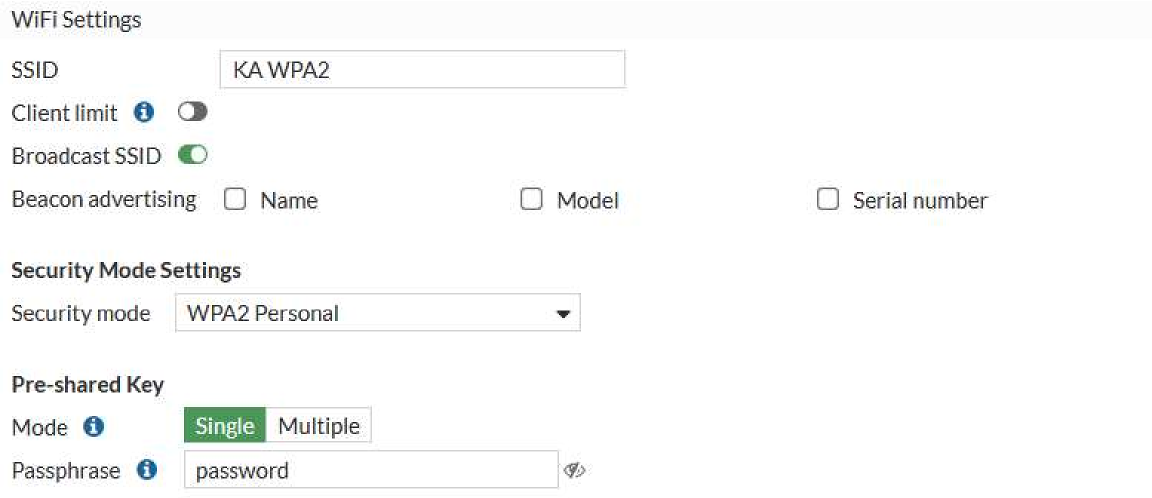
Name: KA WPA2
Alias: KA WPA2
Type: WiFi SSID
Traffic mode: [✓ Tunnel] Bridge Mesh

Address
IP/Netmask: 10.0.0.1/24
Create address object matching subnet: ●
Name: KA WPA2 address
Destination: 10.0.0.0/24
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: 10.0.0.2-10.0.0.254
Netmask: 255.255.255.0
Default gateway: [✓ Same as Interface IP] Specify
DNS server: [✓ Same as System DNS] Same as Interface IP Specify
Lease time ● 604800 second(s)

4: Configure your SSID with a Name and Alias. Ensure the SSID is in Traffic Mode. Enter an IP address + Netmask. Set up the DHCP server as shown above.



WiFi Settings

SSID: KA WPA2

Client limit ○

Broadcast SSID ●

Beacon advertising □ Name □ Model □ Serial number

Security Mode Settings

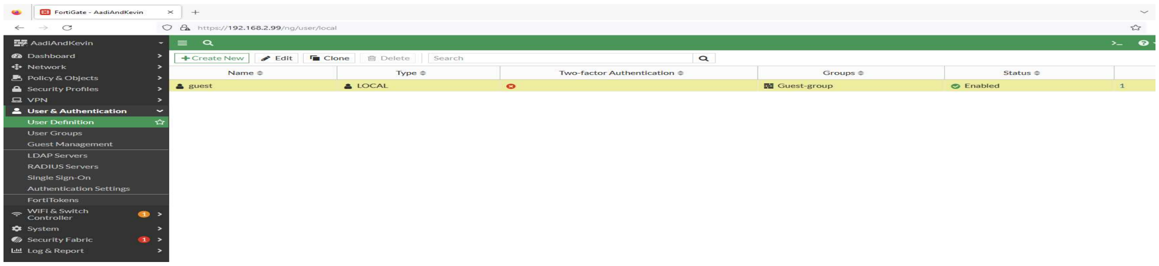
Security mode: WPA2 Personal

Pre-shared Key

Mode: [✓ Single] Multiple

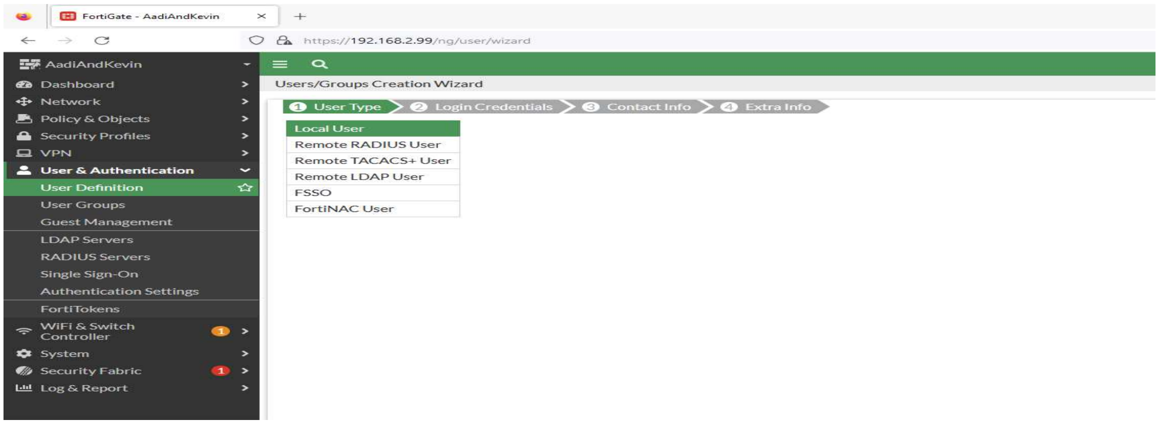
Passphrase: password

5: Scroll down to WiFi Settings and configure as the following shown above, we recommend a stronger password than what we used



Name	Type	Two-factor Authentication	Groups	Status	
guest	LOCAL	✗	Guest-group	Enabled	1

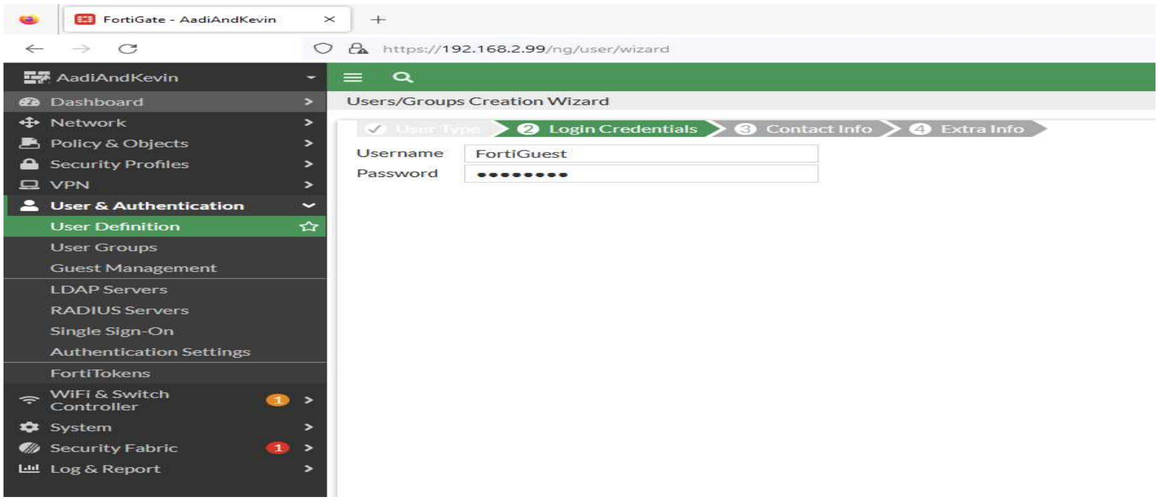
6: Go to User & Authentication > User Definition, Create New.



Users/Groups Creation Wizard

Local User

7: Select the User Type as Local User

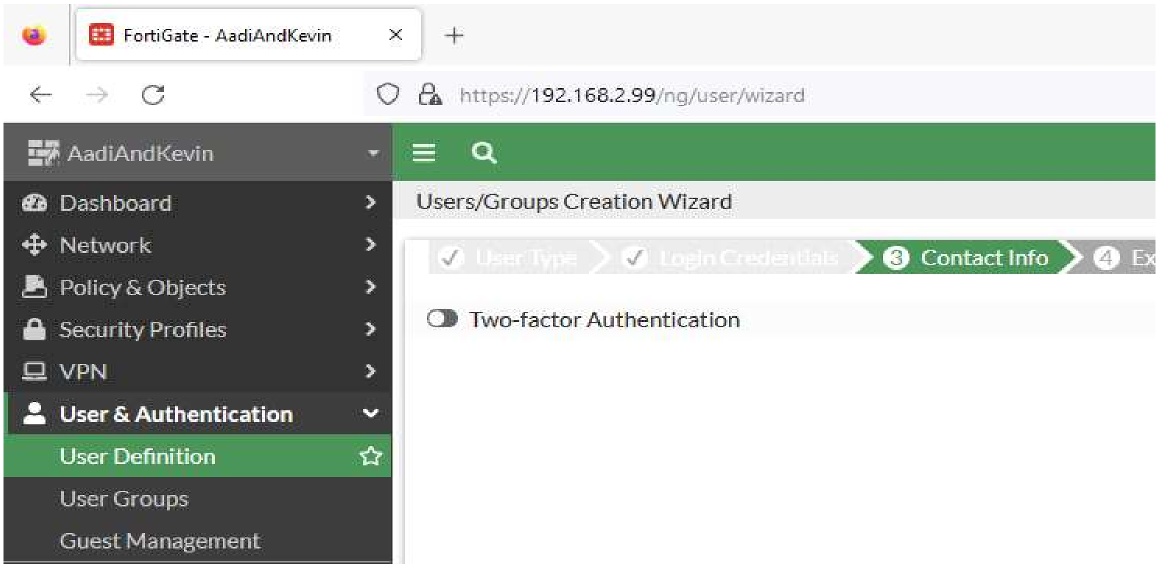


Users/Groups Creation Wizard

Username FortiGuest

Password ••••••••

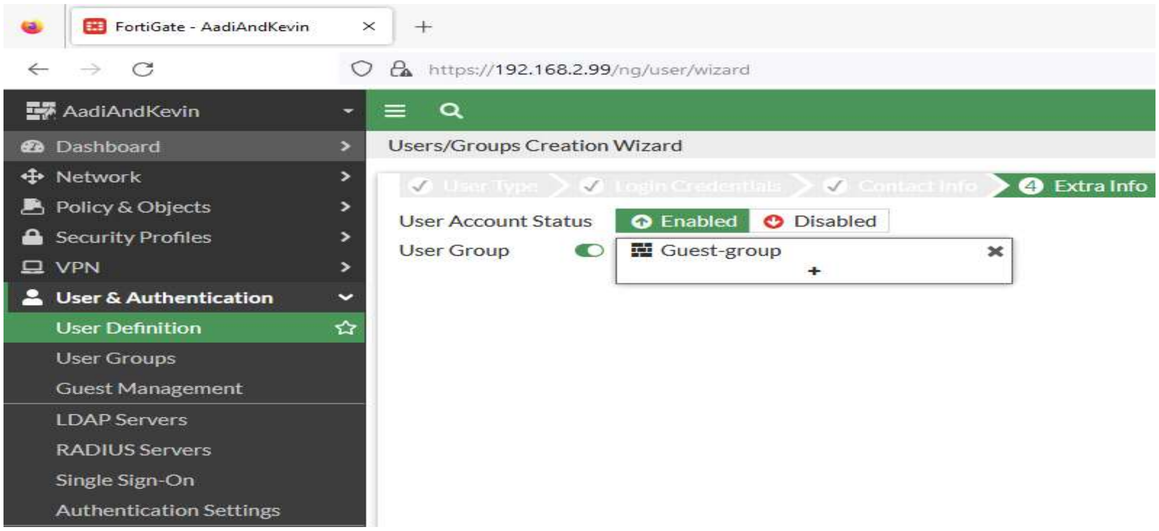
8: Enter a Username and Password, this will be used to login into the WPA2 Enterprise network later.



Users/Groups Creation Wizard

○ Two-factor Authentication

9: Keep Two-factor Authentication off.

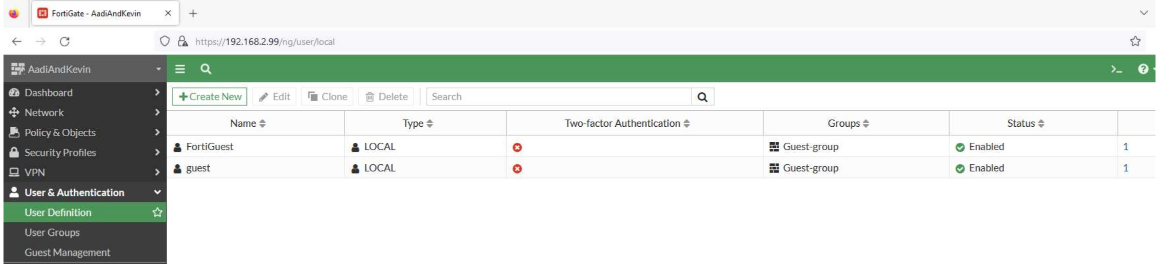


Users/Groups Creation Wizard

User Account Status [✓ Enabled] Disabled

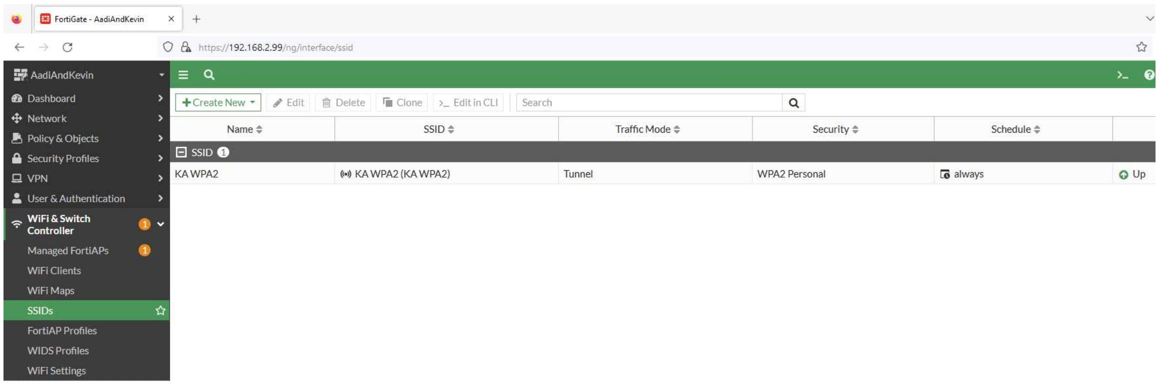
User Group ● Guest-group

10: Enable User Account Status and select your User Group.



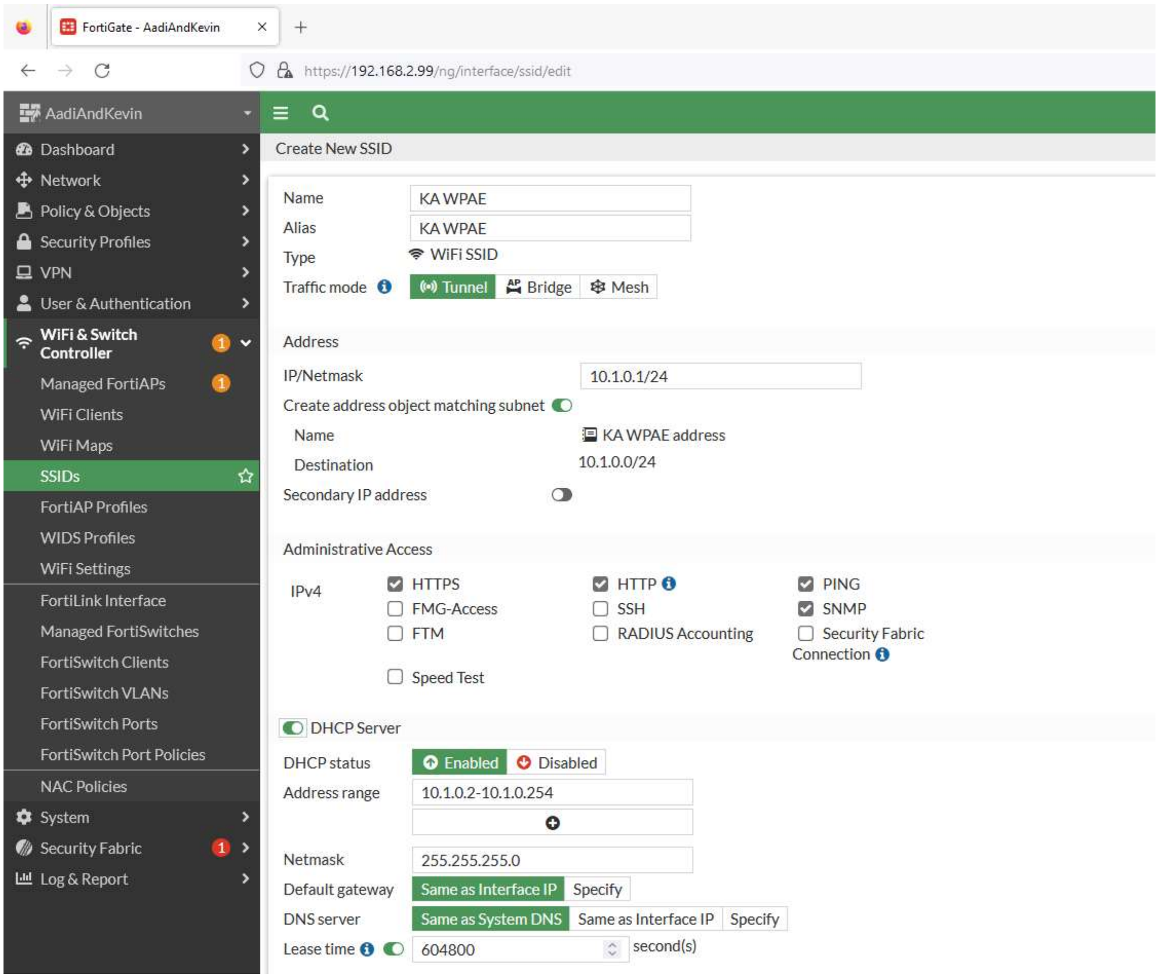
Name	Type	Two-factor Authentication	Groups	Status	
FortiGuest	LOCAL	✗	Guest-group	✓ Enabled	1
guest	LOCAL	✗	Guest-group	✓ Enabled	1

11: The FortiGuest user has now been created



Name	SSID	Traffic Mode	Security	Schedule	
SSID 1					
KA WPA2	KA WPA2 (KA WPA2)	Tunnel	WPA2 Personal	always	Up

12: Go to WiFi & Switch Controller > SSIDs and create a new SSID.



Create New SSID

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

Address

IP/Netmask: 10.1.0.1/24
Create address object matching subnet ●
Name: KA WPAE address
Destination: 10.1.0.0/24
Secondary IP address ○

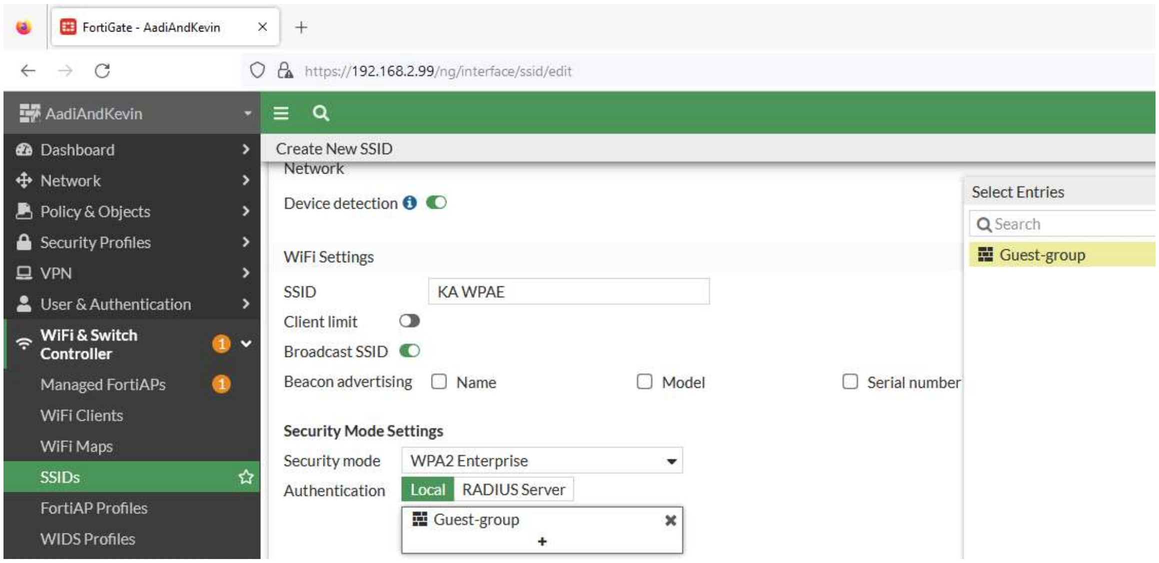
Administrative Access

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

● DHCP Server

DHCP status: [✓ Enabled] Disabled
Address range: 10.1.0.2-10.1.0.254
Netmask: 255.255.255.0
Default gateway: [✓ Same as Interface IP] Specify
DNS server: [✓ Same as System DNS] Same as Interface IP Specify
Lease time ● 604800 second(s)

13: In order to create a WPA2 Enterprise SSID, first add a Name and Allis. Ensure the Traffic Mode is Tunnelling. Create your IP address + Netmask. Create your DHCP Server with a pool (Address Range).



Create New SSID

Network

Device detection: on

WiFi Settings

SSID: KA WPAE

Client limit: off

Broadcast SSID: on

Beacon advertising: ☐ Name ☐ Model ☐ Serial number

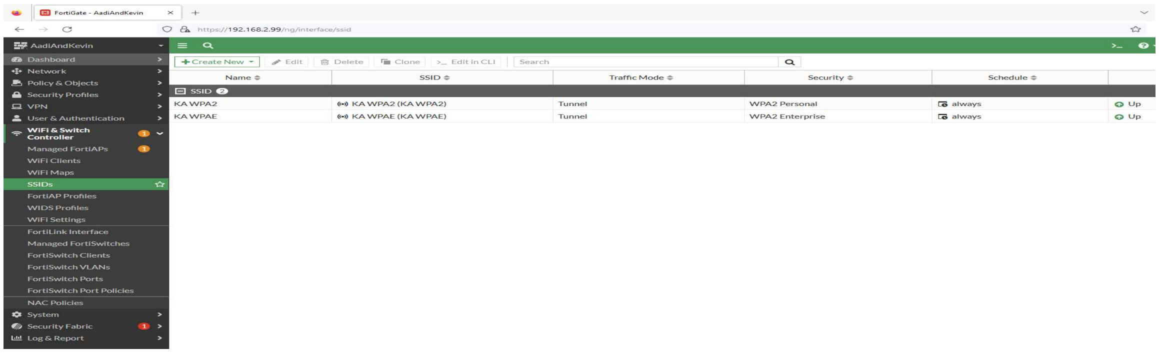
Security Mode Settings

Security mode: WPA2 Enterprise

Authentication: Local | RADIUS Server

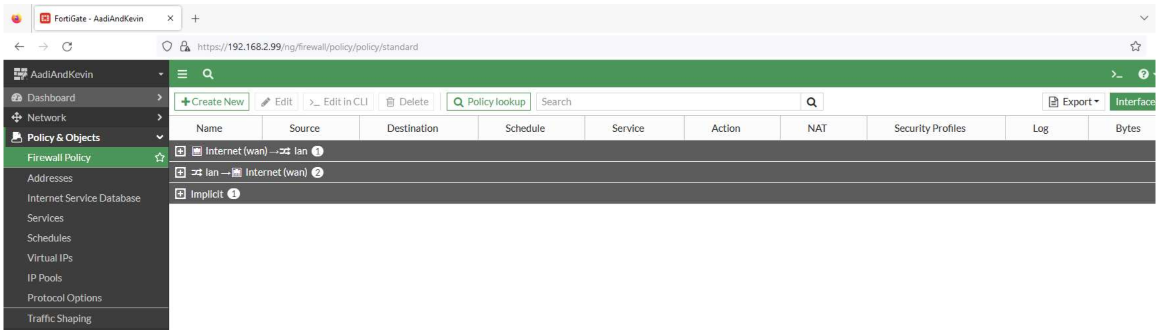
Guest-group

14: Scroll down to WiFi Settings and configure as shown above. Make sure your Security mode is WPA2 Enterprise.



Name	SSID	Traffic Mode	Security	Schedule	
SSID 2					
KA WPA2	KA WPA2 (KA WPA2)	Tunnel	WPA2 Personal	always	Up
KA WPAE	KA WPAE (KA WPAE)	Tunnel	WPA2 Enterprise	always	Up

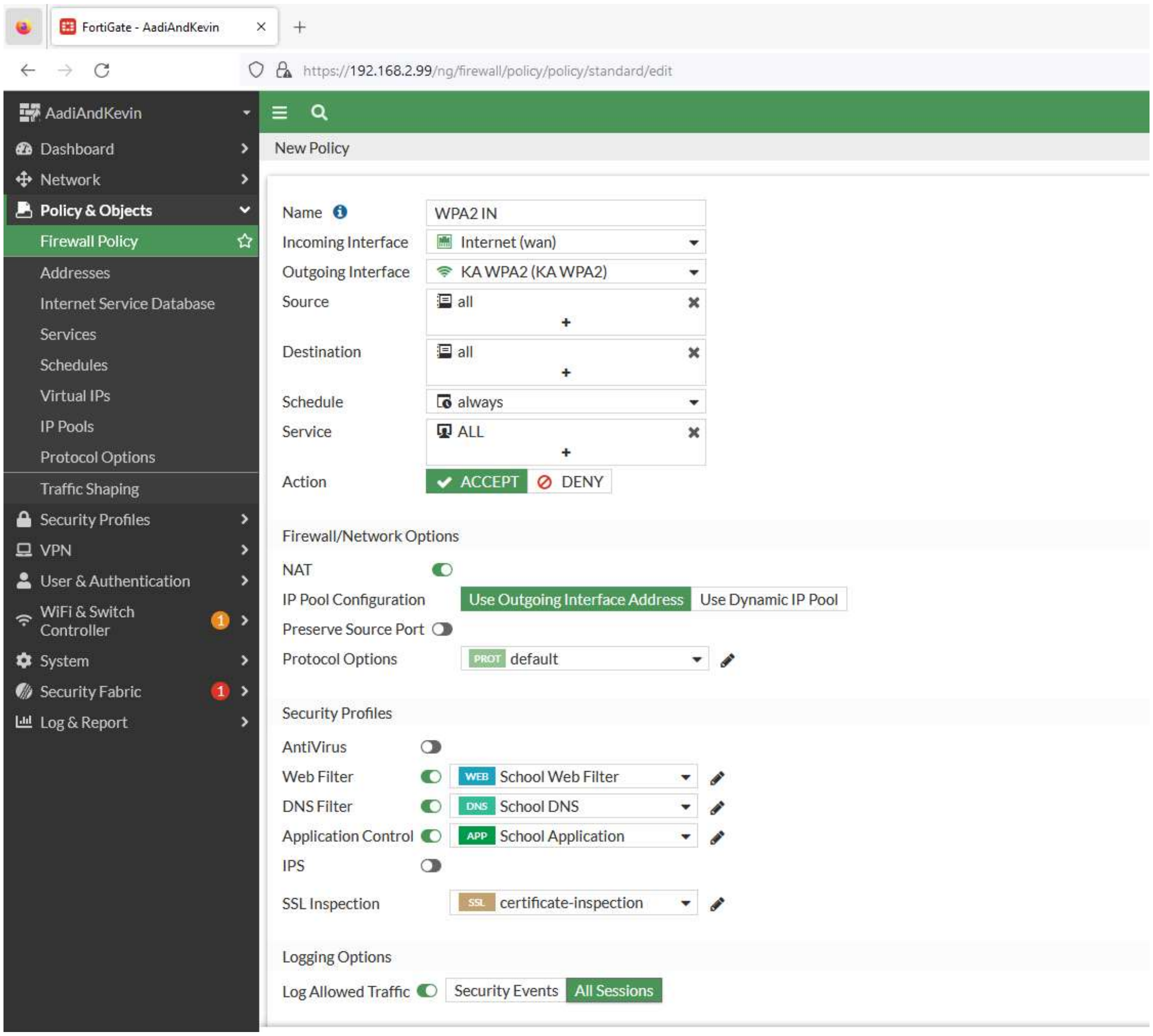
15: There are now the two required SSIDs, one WPA2 PSK and one WPA2 Enterprise.



https://192.168.2.99/ng/firewall/policy/policy/standard

Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log	Bytes
Internet (wan) → lan 1									
lan → Internet (wan) 2									
Implicit 1									

16: Go to Policy & Objects > Firewall Policy. Create New.



New Policy

Name: WPA2 IN
Incoming Interface: Internet (wan)
Outgoing Interface: KA WPA2 (KA WPA2)
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

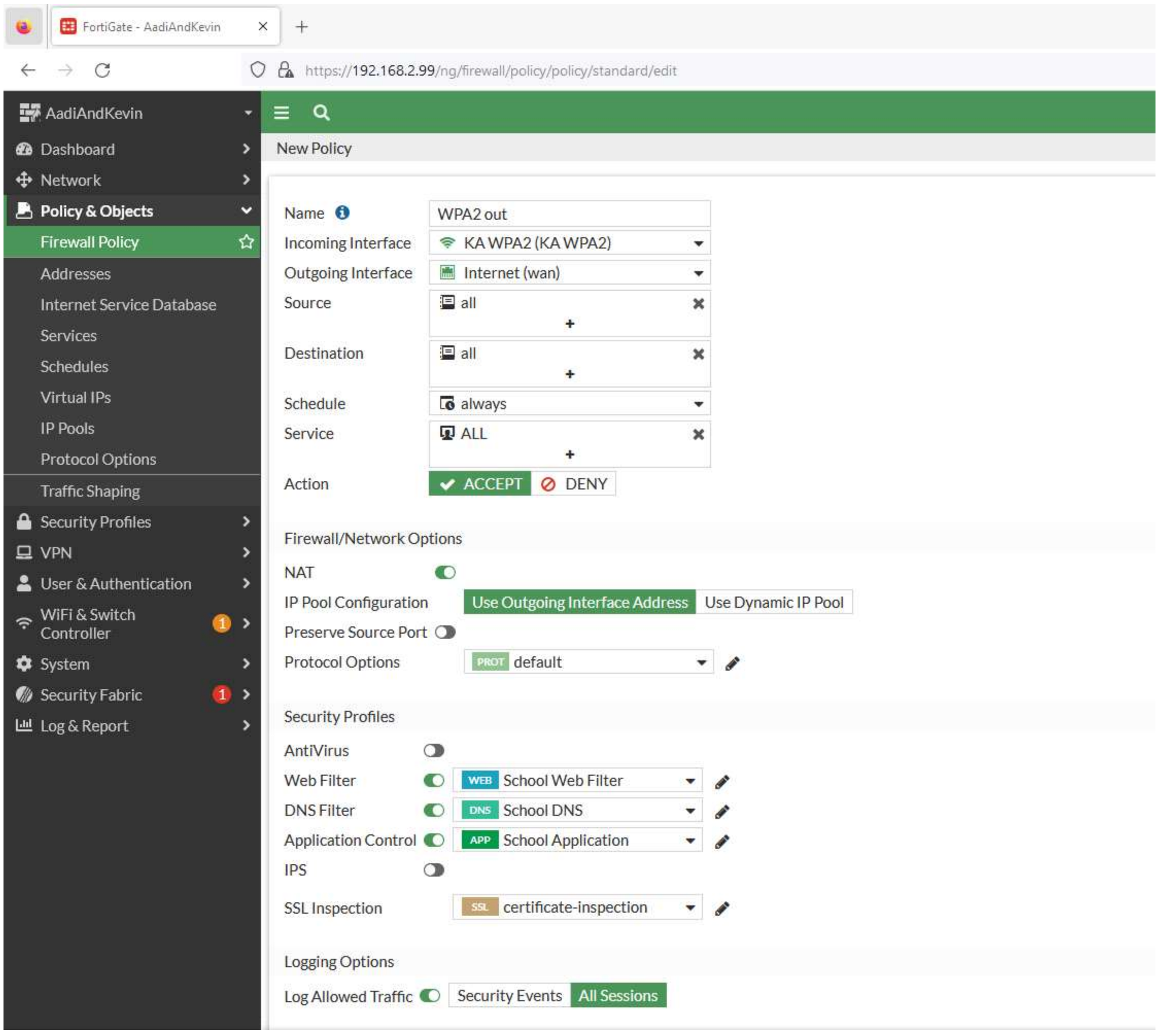
Security Profiles

AntiVirus: ○
Web Filter: ● WEB School Web Filter
DNS Filter: ● DNS School DNS
Application Control: ● APP School Application
IPS: ○
SSL Inspection: SSL certificate-inspection

Logging Options

Log Allowed Traffic: ● Security Events [✓ All Sessions]

17: Create a new policy that sets the Incoming Interface as the Internet Wan and Outgoing Interface as your WPA2 SSID. Ensure NAT is on and apply any Security Profiles you have created and want applied to this SSID.



New Policy

Name: WPA2 out

Incoming Interface: KA WPA2 (KA WPA2)

Outgoing Interface: Internet (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: ● WEB School Web Filter

DNS Filter: ● DNS School DNS

Application Control: ● APP School Application

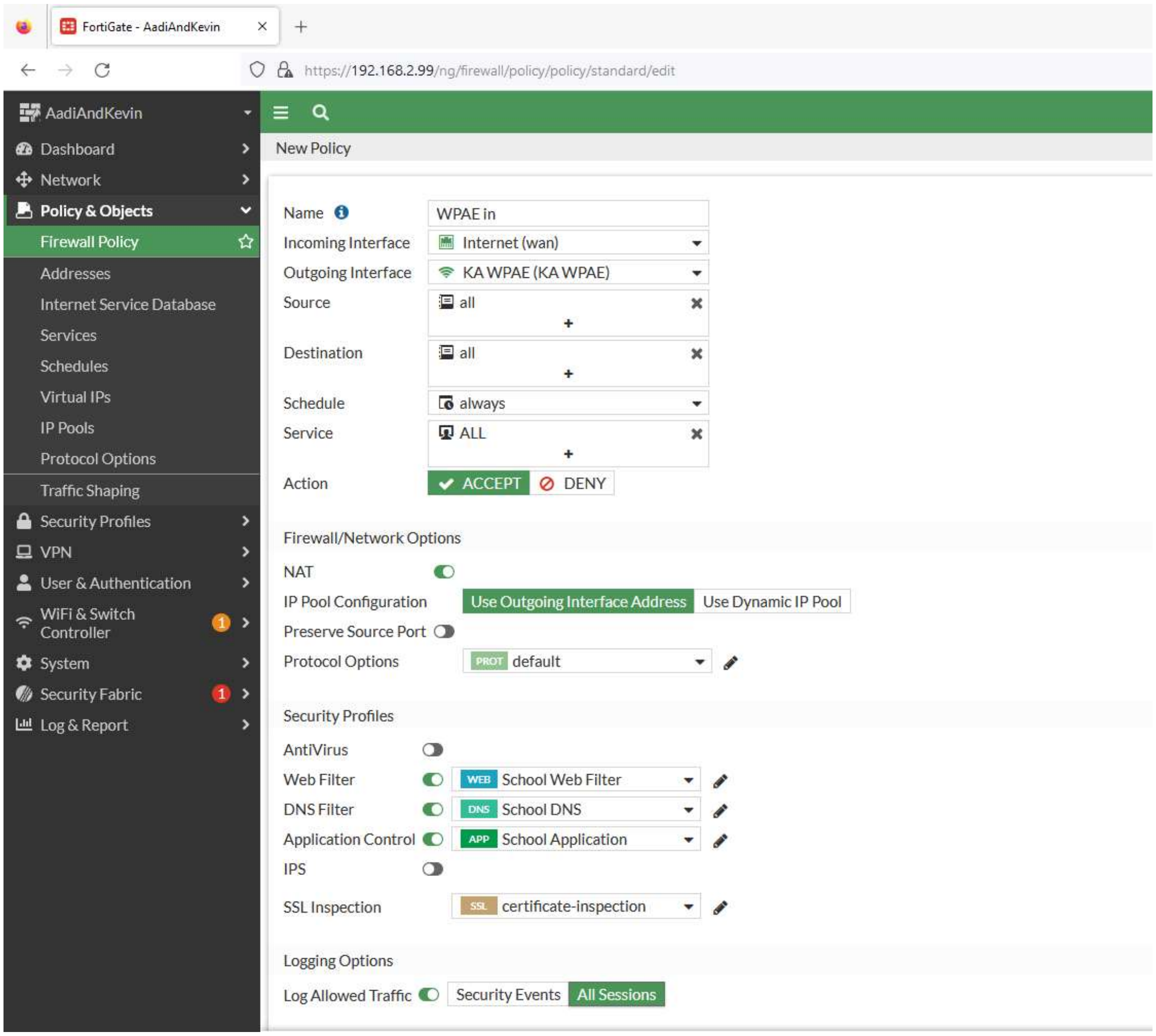
IPS: ○

SSL Inspection: SSL certificate-inspection

Logging Options

Log Allowed Traffic: ● Security Events [✓ All Sessions]

18: Repeat step 17 but swap the interfaces, Incoming as your WPA2 SSID and Outgoing as the Internet Wan.



New Policy

Name: WPAE in
Incoming Interface: Internet (wan)
Outgoing Interface: KA WPAE (KA WPAE)
Source: all
Destination: all
Schedule: always
Service: ALL
Action: ACCEPT | DENY

Firewall/Network Options

NAT: on
IP Pool Configuration: Use Outgoing Interface Address | Use Dynamic IP Pool
Preserve Source Port: off
Protocol Options: PROT default

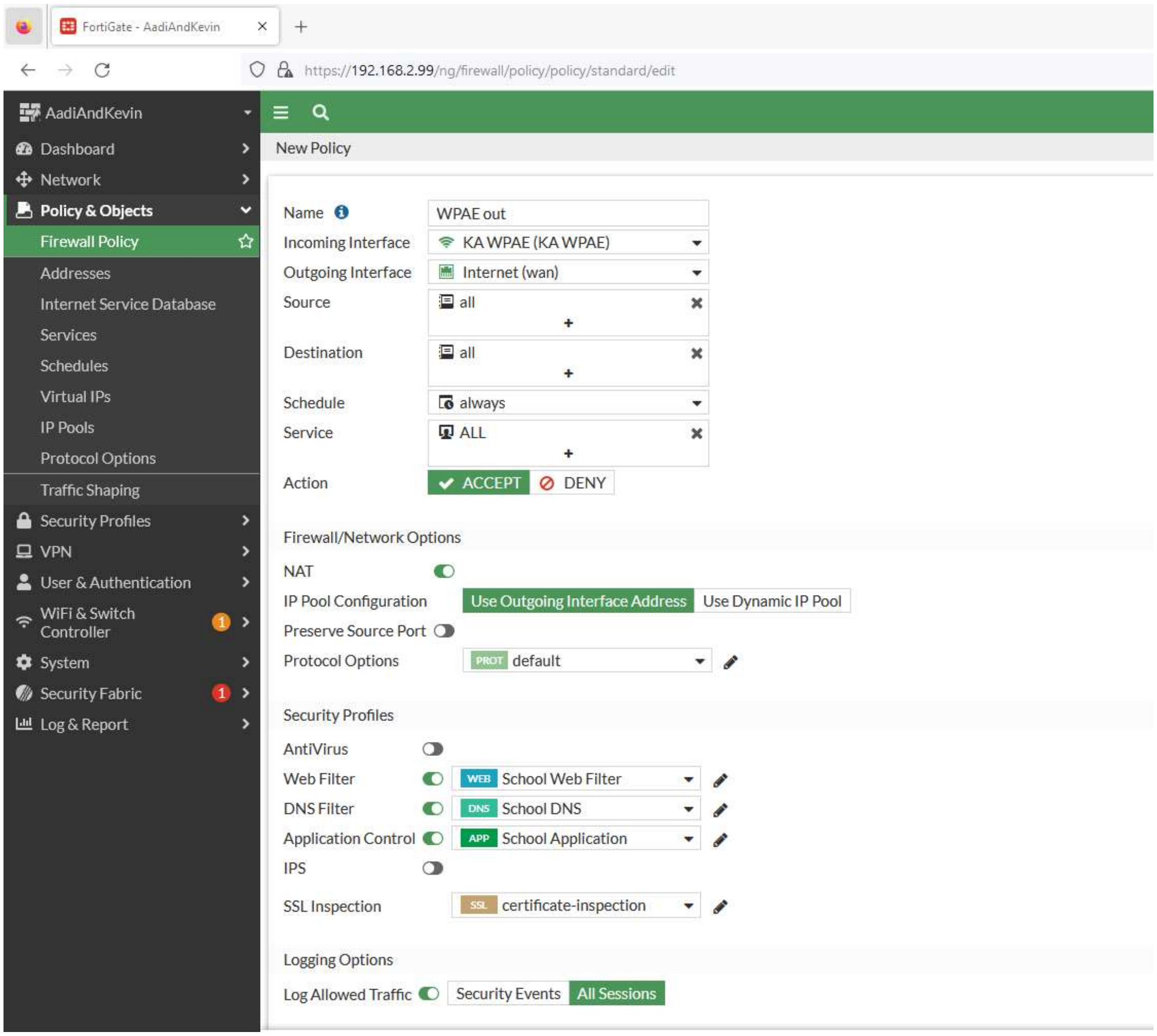
Security Profiles

AntiVirus: off
Web Filter: on, WEB School Web Filter
DNS Filter: on, DNS School DNS
Application Control: on, APP School Application
IPS: off
SSL Inspection: SSL certificate-inspection

Logging Options

Log Allowed Traffic: on, Security Events | All Sessions

19: Create another Firewall policy for your WPA2 Enterprise SSID. Select the Incoming Interface as the Internet Wan and Outgoing Interface as your WPA2 Enterprise SSID. Ensure NAT is on and apply any Security Profiles you have created and want applied to this SSID.



New Policy

Name: WPAE out

Incoming Interface: KA WPAE (KA WPAE)

Outgoing Interface: Internet (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 ● WEB School Web Filter

DNS Filter ● DNS School DNS

Application Control ● APP School Application

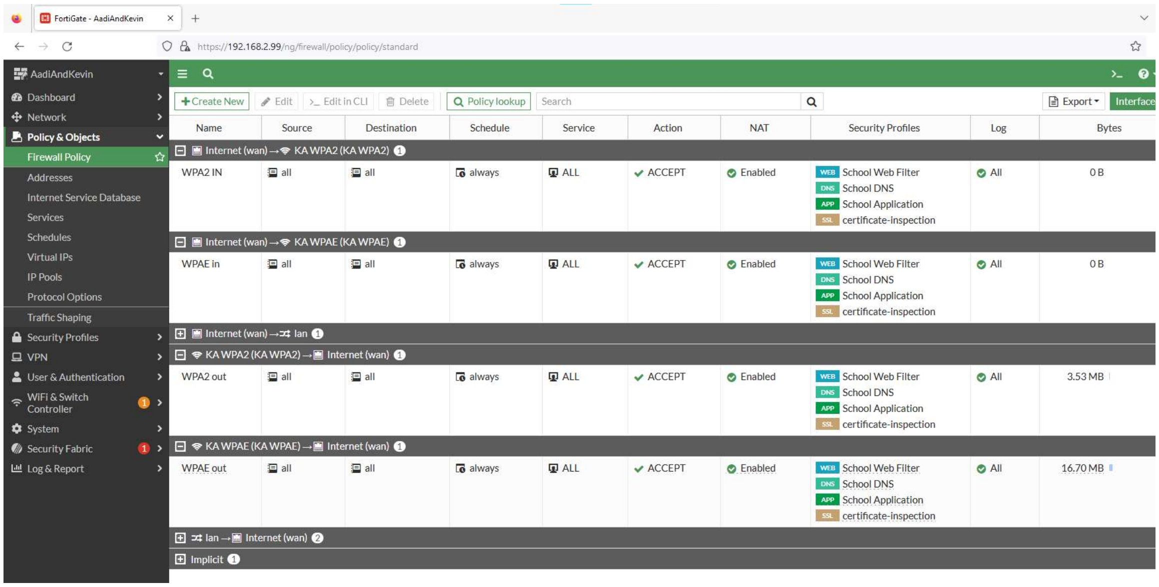
IPS ○

SSL Inspection: SSL certificate-inspection

Logging Options

Log Allowed Traffic ● Security Events [✓ All Sessions]

20: Repeat Step 19 but with the Interfaces swapped. Incoming as the WPA2 Enterprise SSID and Outgoing as the Interface Wan



Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log	Bytes
⊟ Internet (wan) → KA WPA2 (KA WPA2) 1									
WPA2 IN	all	all	always	ALL	✓ ACCEPT	Enabled	WEB School Web Filter DNS School DNS APP School Application SSL certificate-inspection	All	0 B
⊟ Internet (wan) → KA WPAE (KA WPAE) 1									
WPAE in	all	all	always	ALL	✓ ACCEPT	Enabled	WEB School Web Filter DNS School DNS APP School Application SSL certificate-inspection	All	0 B
⊞ Internet (wan) → lan 1									
⊟ KA WPA2 (KA WPA2) → Internet (wan) 1									
WPA2 out	all	all	always	ALL	✓ ACCEPT	Enabled	WEB School Web Filter DNS School DNS APP School Application SSL certificate-inspection	All	3.53 MB
⊟ KA WPAE (KA WPAE) → Internet (wan) 1									
WPAE out	all	all	always	ALL	✓ ACCEPT	Enabled	WEB School Web Filter DNS School DNS APP School Application SSL certificate-inspection	All	16.70 MB
⊞ lan → Internet (wan) 2									
⊞ Implicit 1									

21: All 4 Firewall policies should be up now, this will ensure that traffic will flow through your firewall from your WAP to the outside network connected to your Internet Wan.

Issues:

No issues were encountered when doing this lab. Due to the simplicity of the FortiOS, setup for creating SSIDs using even WPA2 Enterprise was very straight forward and only required 20 minutes at the most.

Conclusion:

This lab initially seems more difficult than it turned out to be due to Fortinet a having straightforward and intuitive OS. The ability to use the Firewall as a radius server by just setting up users made this lab very easy when creating a WPA2 Enterprise SSID. The knowledge of WPA2 Personal vs WPA2 Enterprise and how to set them up will be a useful skill in the future. Even if we don’t end up in a security/IT field of work, this knowledge can be useful at home to set up secure home networks as we continue towards a more technology focused future.