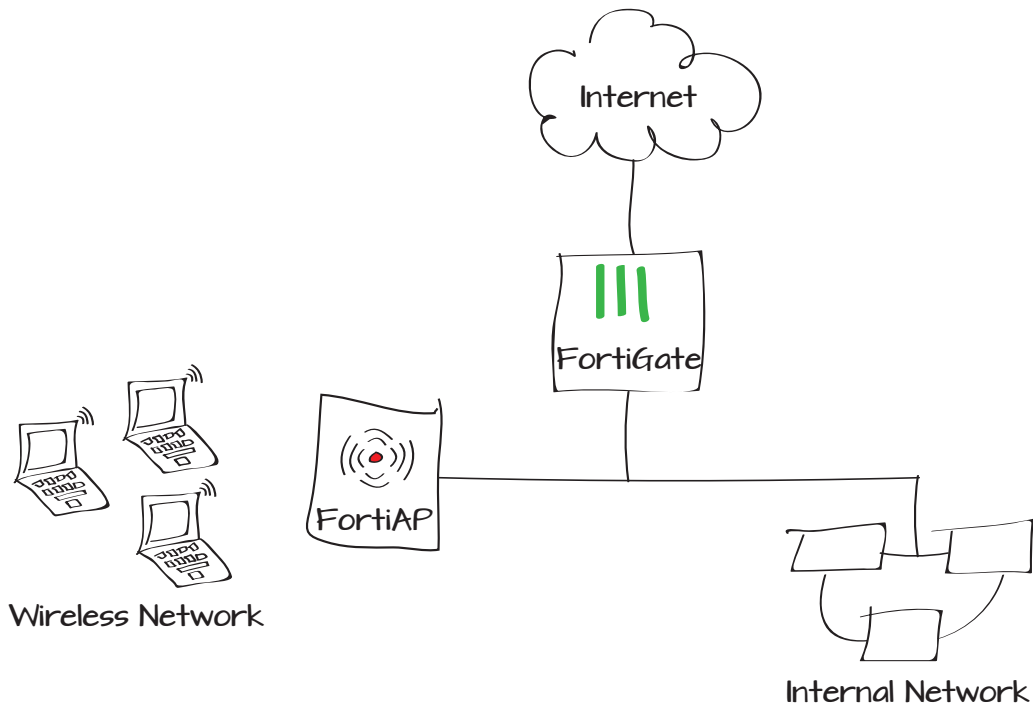


Setting up a network using a FortiGate unit and a FortiAP unit

This example sets up a wired network and a wireless network that are in the same subnet. This will allow wireless and wired users to share network resources.

1. Configuring the internal wired network to use DHCP
2. Creating the internal wireless network
3. Results



Configuring the internal wired network to use DHCP

Edit the internal interface.

Set **Addressing mode** to **Manual** and enable **DHCP server**. Take note of the IP range.

Go to **Firewall Objects > Address > Addresses**.

Set **Type** to **IP Range** and set **Subnet/IP Range** to use the IP range from the DHCP server.

The screenshot shows the configuration page for an interface named 'internal (00:09:0F:7E:88:26)'. The interface is a Physical Interface and is currently 'Up'. The addressing mode is set to 'Manual' with a sub-net/mask of '192.168.1.99/255.255.255.0'. The IPv6 address is set to '::/0'. Administrative access is disabled for all protocols (HTTPS, PING, HTTP, SSH, SNMP, TELNET, FMG-Access, FCT-Access, CAPWAP, Auto IPsec Request). The DHCP server is enabled, and a table shows a single address range from 192.168.1.100 to 192.168.1.254 with a netmask of 255.255.255.0. The default gateway and DNS server are both set to 'Same as Interface IP' and 'Same as System DNS' respectively.

Starting IP	End IP
192.168.1.100	192.168.1.254

Go to **Policy > Policy > Policy**.

Create a security policy allowing users on the wired network to access the Internet.

Creating the internal wireless network

Connect the FortiAP to the internal interface. Go to **WiFi Controller > Managed Access Points > Managed FortiAPs** and right-click on the FortiAP unit. Select **Authorize**.



It may take a few minutes for the FortiAP unit to appear on the **Managed FortiAPs** list.

Policy Type: Firewall SSL-VPN

Policy Subtype: Address User Identity Device Identity

Incoming Interface: internal

Source Address: Internal network

Outgoing Interface: wan1

Destination Address: all

Schedule: always

Service: ALL

Action: ACCEPT

Enable NAT

- Use Destination Interface Address
- Use Dynamic IP Pool
- Use Central NAT Table

Fixed Port

Click to add...

Logging Options

- No Log
- Log Security Events
- Log all Sessions

Mesh	Access Point	State	Connected Via	SSIDs	Chann
-	FAP22B3U11022065	?	192.168.1.110	Radio 1: All Radio 2: All	Radio 1: 0 Radio 2: 0

Context menu for FAP22B3U11022065:

- Edit
- Delete
- Authorize
- Restart
- Upgrade

Go to **WiFi Controller > WiFi Network > SSID** and create a new SSID.

Ensure the **Traffic Mode** is set to **Local** bridge with FortiAP's Interface.



Bridge mode is more efficient than Tunnel mode, as it uses the CAPWAP tunnel for authentication only. Bridge mode is also required in order to have a wired and wireless network be on the same subnet.

Go to **WiFi Controller > WiFi Network > Custom AP Profiles**. Select **Create New**.

Set **SSID** for both **Radio 1** and **Radio 2** to the new SSID.

Name: WLAN
Type: WiFi SSID
Traffic Mode: Local bridge with FortiAP's Inter...

WiFi Settings
SSID: My_SSID
Security Mode: WPA/WPA2-Personal
Data Encryption: AES TKIP TKIP-AES
Pre-shared Key: (8 - 63 characters)
Maximum Clients:

Comments: Write a comment... 0/255

Radio 1
Mode: Disable Access Point Dedicated Monitor
Background Scan: Disable Enable
WIDS Profile:
Radio Resource Provision:
Client Load Balancing: Frequency Handoff AP Handoff
Band: 802.11an_5G
20/40 MHz Channel Width:
Channel: 36 40 44 48 149 153 157 161 165
Auto TX Power Control: Disable Enable
TX Power: 100 %

SSID
Available: fortinet.mesh.root (Mest...
Selected: My_SSID

Go to **WiFi Controller > Managed Access Points > Managed FortiAPs**. Edit the FortiAP unit.

Under **Wireless Settings**, set **AP Profile** to use the new profile.

Results

Users connected to the new SSID will be able to access the Internet. The wireless devices will be in the same subnet as the internal wired network.

Go to **WiFi Controller > Monitor > Client Monitor** to see WiFi users and their IP addresses.

Go to **Log & Report > Traffic Log > Forward Traffic** to verify that the same policy controls both wired and wireless traffic.

Serial Number

Name

Description [\[Change\]](#)

Managed AP Status

Status Online

Connected Via Ethernet (192.168.1.110)

Base MAC Address 00:09:0f:35:6d:40

Join Time 03/22/13 10:38

Clients 0

FortiAP OS Version FAP22B-v5.0-build031 [\[Upgrade\]](#)

State Authorized

Wireless Settings

AP Profile [\[Apply\]](#)

Radio 1

Mode Access Point

Band 802.11an_5G

Channel 36, 40, 44, 48, 149, 153, 157, 161, 165

Radio 2

Mode Access Point

Band 802.11bgn_2.4G

Channel 1, 6, 11

SSID	FortiAP	IP	Device	Auth	Channel	Bandwidth Tx/Rx
My_SSID	FAP22B3U11022065 (1)	192.168.1.111	84:29:99:be:54:dc	Pass	36	560 bps

[Total: 1]

Src Interface	Dst Interface	Src	Dst	Policy ID	Service	Sen
lan	wan1	192.168.1.111	74.121.50.17	1	HTTP	1.02 KB
lan	wan1	192.168.1.111	184.28.198.224	1	HTTP	940 B /
lan	wan1	192.168.1.112	208.91.112.132	1	HTTP	964 B /
lan	wan1	192.168.1.112	208.91.112.132	1	HTTP	924 B /
lan	wan1	192.168.1.112	8.8.8.8	1	DNS	62 B / 1
lan	wan1	192.168.1.112	208.91.112.133	1	HTTP	3.14 KB
lan	wan1	192.168.1.112	208.91.112.133	1	HTTP	924 B /
lan	wan1	192.168.1.112	173.194.64.147	1	HTTPS	1.59 KB
lan	wan1	192.168.1.111	192.168.110.9	1	DNS	71 B / 5
lan	wan1	192.168.1.111	17.164.0.8	1	HTTPS	2.68 KB