



Wireless LAN Capabilities



Overview of Wireless LAN features for FortiWiFi, FortiAP, and FortiGate devices operating with FortiOS 4.0 MR2

Wireless Technology

Fortinet combines FortiGate security processing with IEEE 802.11 standards based radios into the FortiWiFi series of integrated security gateways that secure both wired and wireless traffic. In addition, Fortinet also offers a series of controller-managed FortiAP wireless access points. FortiAP access points are controlled and managed by FortiGate devices to add wireless capabilities to a wired network protected by those FortiGate devices.

Users operating devices such as laptops and mobile WiFi devices such as smartphones as well wireless security cameras, wireless VoIP handsets, point of sale devices, and scanners can all be connected to a wireless network and the Internet through an integrated FortiWiFi or FortiAP wireless Access Point (AP).

Thick and Thin Access Points

There are two methods of deploying a wireless network and the method to choose depends on your infrastructure and the amount of space that needs coverage. One is to use what the industry terms a Thick AP and the other option utilizes what is predictably called a Thin AP. A Thick AP refers to a wireless access point (or wireless termination point – WTP) that autonomously switches packets between wired and wireless domains. This Thick, or Fat AP is responsible for authentication and access control policies and has to be managed as an individual device. Thick AP installations are great for relatively small locations where only one or two access points are required.

FortiWiFi products are Thick APs and ideal for locations such as a small office or retail premise. Alternatively if coverage and capacity requirements are larger, a centralized wireless service with controlled and associated Thin APs employing FortiAP products becomes the best strategy to adopt.

Thick/Fat Access Points

Fortinet provides a number of FortiWiFi appliances with Thick AP functions that combine the management and wireless radio with FortiOS on a single device.

The table opposite provides a summary of the WiFi capabilities offered in FortiOS 4.0 MR2. Select the device that meets or exceeds your security performance needs as well as wireless needs. Please note that

Wireless Standards and Capabilities	FortiWiFi					FortiAP
	30B	50B	60B	60C	80C/81CM	220A
Thick AP	Yes	Yes	Yes	Yes	Yes	No
Thin AP	option	option	option	option	option	Yes
Number of WiFi radios	1	1	1	1	1	2
802.11a			Yes	Yes	Yes	Yes
802.11 b/g	Yes	Yes	Yes	Yes	Yes	Yes
802.11n	No	No	No	Yes 2x2 MiMo	Yes 2x2 MiMo	Yes 2x2 MiMo
High Throughput 40Mhz option	No	No	No	Yes	Yes	Yes
WME/WMM Multimedia Extensions	No	No	No	Yes	Yes	Yes
Max wireless speed	54Mbps	54Mbps	54Mbps	300Mbps	300Mbps	600Mbps
# simultaneous SSIDs	7	7	7	7	7	14
Background air monitor for Rogue AP detection	Yes	Yes	Yes	Yes	Yes	Yes
PoE power option	No	Yes	No	No	No	No
Ability to serve as wireless controller for FortiAP	No	No	No	No	No	N/A

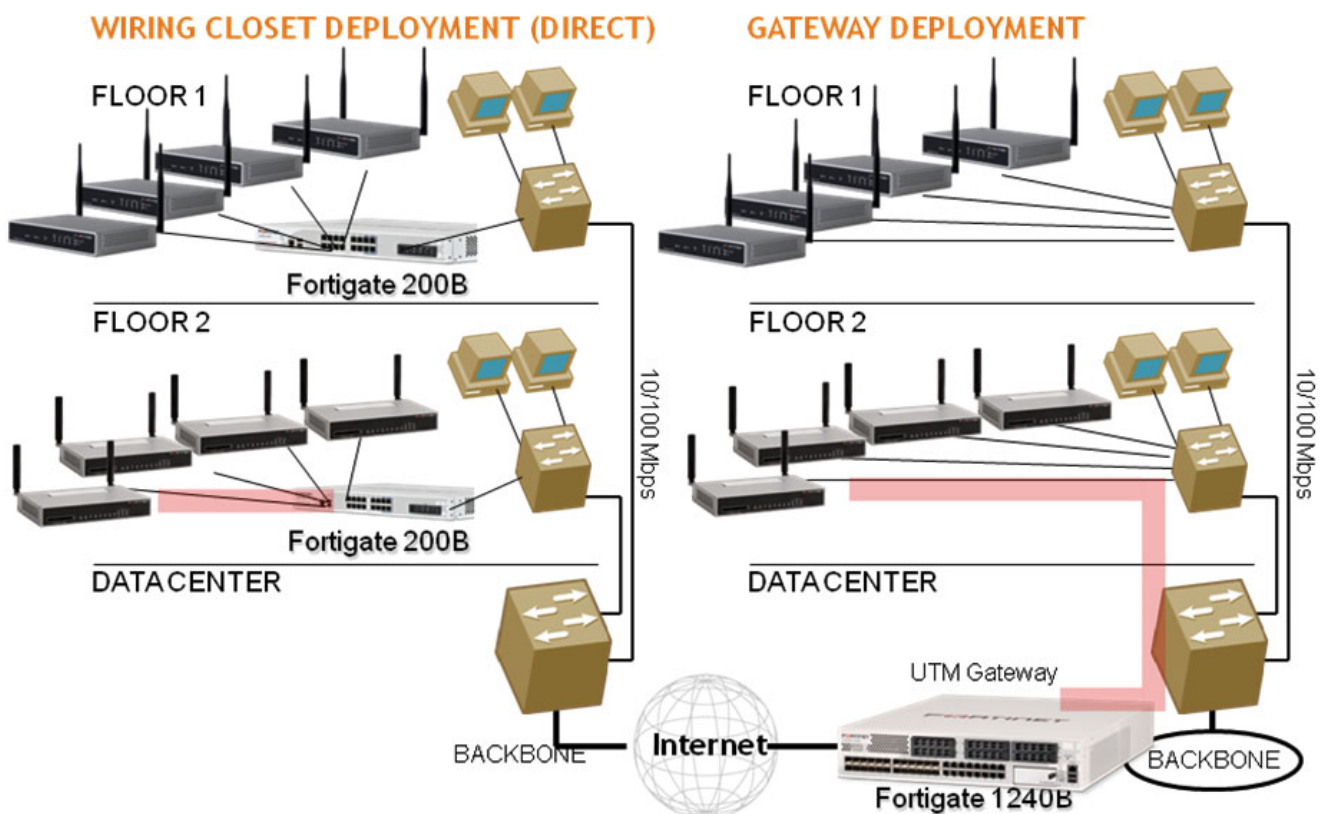
customers now have the option to deploy high performance 802.11n wireless to provide higher range or throughput. In this version of FortiOS, each physical AP is capable of beaconing up to seven Virtual Access Points.

Virtual Access Point (VAP)

A VAP appears to FortiOS as a separate interface, enabling standard firewall policies and user and application policies to be applied to this traffic. One best practice usage of VAPs is to setup separate guest and employee wireless networks with separate SSIDs, authentication options and QoS priorities. Since the wireless controller is combined with UTM functionality, this gives administrators the advantage of layer 7 application prioritization so that Guest traffic does not interfere with Employee traffic. Other VAPs can be setup for contractors and to service wireless voice traffic and infrastructure equipment like security cameras.

Thin/Lite Access Points

Thin APs provide the same wireless connectivity features as Thick APs, however Thin APs require a centralized wireless controller to function. The wireless controller allows a large number of Thin APs to be deployed together since the controller is the centralized decision point that automates the configuration and ongoing operation of the Thin APs. A Thin AP functions as the wireless RF radio and beacons a wireless AP SSID. The Thin AP also forwards all traffic using standards based CAPWAP tunnels directly to a FortiGate device configured as the wireless controller. The FortiAP is the newest addition to the Fortinet wireless family and operates as a Thin AP and provides the ability for FortiGate customers to take advantage of wireless capabilities via a software upgrade of their existing FortiGate equipment.



The distributed Thin AP deployment model enables FortiAP devices to delegate all the authentication, security processing, channel assignment, transmitter power level settings and rogue AP detection to the centralized wireless controller. FortiGate devices are typically used as gateway devices to the Internet and Thin APs can backhaul their traffic directly to a FortiGate device that is also configured as a wireless controller. In this overlay network, the wireless traffic bypasses the LAN and terminates at the FortiGate device for security processing and routing. Each Thin AP can also be connected directly to a FortiGate device placed in each wiring closet where the wireless CAPWAP tunnel is terminated and traffic enters the LAN.

Since FortiAP devices tunnel all packets to the FortiGate device, the path between the FortiAP device and the FortiGate device must allow traffic on UDP ports 5246 and 5247 (the ports used by CAPWAP tunnels). If required, the UDP ports used by the CAPWAP tunnels can be changed in the FortiGate configuration. Also note that only FortiGate devices can be wireless controllers for FortiAP devices and at this time FortiWiFi devices can only be configured as Thick APs and cannot control other FortiWiFi devices.

CAPWAP Standards Based Implementation

CAPWAP is a protocol initiated by the IETF standards body by a team of industry experts for Control And Provisioning of Wireless Access Points (CAPWAP) to provide interoperability among WLAN backend architectures. FortiOS 4.0 MR2 supports a number of CAPWAP RFC specifications to benefit Fortinet customers from the latest

security technologies and algorithms for a scalable wireless LAN infrastructure. For reference, these RFCs include: RFC 4118, RFC 4564, RFC 5418, RFC 5417, RFC 5416, and RFC 5415.

Inside the FortiAP-220A device



The FortiAP-220A device integrates two wireless radios in one enclosure and is perfect for applications that require simultaneous use of wireless on the 2.4Ghz and 5Ghz bands. This dual capability allows newer devices that support 802.11n to run separately on the 5Ghz 802.11n band avoiding interference sources such as microwave ovens and cordless phones, while still allowing older devices to use the 2.4 GHz band. The two independent radios require four internal antennas for high performance 802.11n communication.

The sleek design of the FortiAP enclosure includes the four concealed internal antennas in a white case that does not attract attention in public spaces because it blends into the background to reduce the potential for tampering and theft.

Flexible and Complete Authentication Options

Data Encryption and user authentication settings can be configured per VAP. This enables administrators to configure multiple SSIDs for guests, employees, voice and video traffic all with different authentication options and policies. In FortiOS 4.0 MR2 the authentication options are referred to as different Security Modes and offer the following capabilities.

Open/WEP64/ WEP128/ Shared

Used mainly for hotspot and guest APs where the traffic is to be routed directly to the Internet. With this option there is no authentication or link encryption. In this configuration, firewall policies should only allow traffic between the wireless interface and the WAN interface and all other traffic should be blocked. The open configuration should only be used for traffic where security is not a primary concern or where the clients use SSL or IPsec VPN.

Guest Captive Portal

Captive portal is an industry standard term for web authentication form. In this mode users can connect to the wireless AP similar to the open configuration above, however all traffic is blocked until the user opens a web browser. Once a browser is opened, all website addresses are intercepted by the FortiGate wireless controller or FortiWiFi device. Captive portal authentication is enabled by using identity based policies for the specific wireless virtual AP interfaces.

WPA /WPA2 802.11i Preshared key

Wifi Protect Access (WPA) is available for backward compatibility, but all users should migrate to WPA2 as it provides more secure encryption of data. The WAP preshared key allows a password to be shared among all users who connect to the wireless LAN. This type of security is useful for guest or home access, but enterprises should provide unique username and password combinations to employees and contractors using the WPA2 with RADIUS as described below.

WPA/WPA2 802.11i with RADIUS backend

In this mode user and password information is solicited from users and authenticated against a backend RADIUS server using 802.1x authentication. This is the most secure method of authentication for wireless deployments and is considered a best practice. The FortiGate and FortiWiFi RADIUS engine supports PAP, CHAP, MS-CHAP, and MS-CHAP-v2.

Fast Roaming

When a device connects to a wireless network it has to be authenticated. This authentication process can often take seconds to complete and this delay can impair wireless voice traffic and time sensitive applications. This delay is more important in a Thin AP deployment when users move between Thin APs. Fortinet has addressed this problem by enabling fast roaming using standards based authentication caching technology based on Pairwise Master Key (PMK) caching and pre-authentication. Fast roaming is available only between Thin AP deployments connected to the same FortiGate wireless controller.

PMK caching allows the client to associate with an AP and, upon doing a full RADIUS authentication, the FortiGate wireless controller stores a master key negotiated with that particular AP in a cache. Should the user roam away from that AP and back again, the client will not have to reauthenticate. This enables the 802.11i "fast roam-back" feature.

Pre-authentication or “fast-associate in advance” allows an 802.11 AP associated to a client to bridge to other APs and pre-authenticate the client to the “next” AP that the client might roam to. This enables the PMK to be derived in advance of a roam and cached. When the client does roam, it will already have negotiated authentication in advance and will use its cached PMK to quickly associate to the next AP. This capability ensures that wireless clients that support pre-authentication can continue wireless communication without noticeable connection delays or disruptions.

Rogue AP detection and on-wire correlation

Rogue APs can pose a threat to your internal network by creating a leakage point where data such as sensitive credit card information can be siphoned off the network by a malicious user. For this reason, PCI-DSS compliance mandates that this threat is regularly scanned for and any suspicious unknown AP be investigated to see if it is indeed on the network. The goal of the FortiGate Rogue AP detection engine is to automate this process and provide the ability for FortiWiFi and FortiAP system administrators to continuously monitor for unknown APs and also to determine if unknown APs are on the FortiWiFi or FortiAP network or are a neighboring AP. Rogue AP detection supports the following features:

- Dedicated or background Air Monitor scans for unknown APs and wireless client traffic.
- Unknown APs MAC address, BSSID, Manufacturer, Security profile of AP, speed, last seen and ‘on-wire’ status are all shown in the FortiOS Rogue AP detection table.
- The ‘on-wire’ detection engine uses various correlation techniques to determine whether the unknown AP is connected to the FortiWiFi or FortiAP wireless LAN. If the engine finds that AP is on the LAN, a log message is generated in real time to inform system administrators. This log message is stored in the FortiGate log files and can also be sent to a FortiAnalyzer unit.
 - The correlation engine constantly compares wireless client traffic to wireside client traffic to determine if a client using an unknown AP is communicating through a FortiGate device. This condition indicates that the unknown AP is indeed on the network. This technique can detect an AP operating as a bridge regardless of wireless security settings and encryption and authentication levels.
 - Another technique correlates wireless and wired MAC addresses to detect Layer-3 APs regardless of security settings and NAT configuration.
- Administrators can manually classify unknown APs as trusted or untrusted.

Range of WiFi and Coverage

Many wireless AP vendors claim the highest power output and correlate high power to being able to achieve a longer range. However, that would only be true if the WiFi communication was broadcast or uni-directional like an FM radio station tower. Since WiFi traffic is bidirectional, the wireless range is determined by capabilities of both the client and the AP. In today’s world where most WiFi enabled devices are battery powered (for example, laptops and other mobile devices). Limiting the transmission power of these devices can increase their battery life and decrease their size.

Therefore the weakest link that determines the range of the two way communication becomes the client. A good analogy is when you see 5-bars on your mobile phone, but the call still drops. Has this ever happened and you wondered why? It can happen when your phone can hear from the more powerful base station, but can’t transmit back to the base station because it doesn’t have enough power to cover the distance to the base station. WiFi networks can similar limitations and have to be designed with the weakest link in mind.

FortiWiFi and FortiAP products in general provide 17dBm or 50mW of power output which is optimized to meet or exceed the required power levels to close a two-way communication link with the clients on the wireless network. The typical WiFi range depends on obstructions and interference sources, but the general rule of thumb is that a wireless AP can cover a radius of 50-60 feet (18 meters). If greater coverage range is required, FortiAP devices can be deployed every 60 feet in a hexagonal or honeycomb pattern.

Conclusion

Fortinet today provides a range of Wireless LAN access points that can operate as standalone Thick AP mode devices or as Thin APs connected to a FortiGate wireless controller. This flexible architecture allows Fortinet to provide an end to end UTM capability for any wired and wireless environment.