FortiAP Series Deployment Guide
Secure Controller-managed Wireless LAN Solution
Overview

Large enterprises and campus deployments favor traditional controller-based WLAN solutions over emerging Cloud Wi-Fi alternatives, because they scale well for high-density deployments, and because there are many complex security integration requirements in corporate LANs and data centers. Fortinet’s controller-managed WLAN solution, addresses both requirements in a unique and elegant way, by combining WLAN control and network security into the WLAN controller platform.

Controller vs Cloud

In recent years, enterprise WLAN vendors have shifted their attention to cloud-based management, hoping to garner recurring revenues, and to better serve distributed enterprises who generally struggle with WLAN deployment. Yet despite heavy promotion, large enterprises have not taken the bait. They are reluctant to switch from controllers to the cloud.

The controller-managed WLAN architecture remains the preference for large enterprise and campus deployments for a number of reasons: AP adds, moves and changes are easier in controller-based WLANs compared to cloud because network addressing is simpler; roaming between APs and across domains is faster and more reliable; active/active controller fail-over and dual homing capabilities enables better session-level reliability than cloud Wi-Fi; and finally of the greatest importance, you can leverage enterprise security infrastructure such as firewalls, network IPS, antivirus scanning web-filtering and application controls and apply them to WLAN traffic.

Secure Controller Wi-Fi

Fortinet’s controller-based WLAN solution unifies the management of wired and wireless infrastructure and security on one platform, not a collection of separate appliances, and through a “single pane of glass” management interface. Together, this gives the WLAN solution an unfair advantage in security policy enforcement, operational efficiency and total cost of ownership.
Beyond Standard WLAN Security

How important is security beyond WLAN access control? Everyone recognizes strong authentication and encryption are important, and the standard bodies have seen to it that Wi-Fi access control is secure. However, over the last 10 to 15 years, threats have transformed from connection-based to content-based. Threats enter your network through common applications like email, web browsers, apps on mobile devices and social networking tools. With BYOD now the norm, the risk of corporate breaches from cyber-threats is at an all-time high.

Securing today's WLANs involves much more than Wi-Fi access control. It involves scanning for malware, preventing access to malicious websites, end-point integrity checking and controlling application usage. For complete protection, enterprises historically needed to tunnel all WLAN traffic through a variety of security appliances. But managing policies across multiple security systems gets complicated. This is where Fortinet's controller-managed WLAN solution has an unfair advantage with FortiGate.

Fortinet Secure Controller-managed WLAN

Fortinet's Secure WLAN solution for enterprise and campus deployments is based on the award winning FortiGate Wireless LAN controller and FortiAP access points in a classic coordinated AP architecture. What makes it unique is the level of security integration that comes with FortiGate.

Unlike other vendor's controller-based WLAN solutions, where content and application security requires a set of third party security appliances, FortiGate brings together network security and WLAN control on the same platform. WLAN traffic is passed through the various security measures in a single pass, without needing to map VLANs from one appliance to the next to the next. As a result, session layer detail is preserved, not obscured, and latency is minimized.

FortiGate WLAN Controller

The FortiGate is both a Wi-Fi controller and a network security platform. It consolidates the functions of more than seven individual security devices including: Firewall, VPN Gateway, Network IPS, DLP, Antimalware, Web Filtering and Application Control. Yet it out performs many single function appliances.

In its capacity as a Wi-Fi controller, it handles user authentication, radio resource management and forwarding of traffic. As a security platform, FortiGate provides complete protection against network, content, and application-level threats for both wired and wireless users.

FortiGate Wi-Fi Controller

IPS
Application Control
Web Filtering
WAN Acceleration
Anti-Malware
DLP
Firewall
VPN

Fig 1: FortiGate Appliance Consolidation

FortiGate platforms are equipped with custom FortiASIC™ processors which can detect malicious content at multi-gigabit speeds. FortiGate is a recognized network security appliance performance leader, with the flagship model clocking firewall throughput in excess of 300 Gbps. While the same platform, can handle over 100 Gbps of WLAN throughput, making it the world's fastest Wi-Fi controller as well.

FortiGate platforms incorporate sophisticated networking features, such as high availability (active/active, active/passive) for maximum network uptime, and virtual domain (VDOM) capabilities to provide multi-tenant support for subscriber-based environments or for greater internal segmentation of data for policy compliance in enterprises.
**FortiGate WLAN Highlights**

**BYOD Onboarding:** FortiGate has all the components to enable seamless self-service onboarding of users’ mobile devices. It offers branded captive portals, executes device integrity checks, virus scan, and authentication setup, with a variety of user authentication options to choose from, including Two-Factor Authentication. Until a user is properly authenticated and their device is checked, they are kept in walled garden. You can even specify how many devices an individual can onboard, rather than simply allowing them to onboard whatever they like.

**Guest Access:** You can create a separate SSID to grant access to groups of users who need temporary access to the network, such as long term contractors. This separation provides access to the necessary systems while keeping the back-office network and other critical systems completely segmented. Additionally, the fully customizable HTML Captive Portal login page allows visitors and contractors to gain access to the Internet without any risk to the LAN infrastructure. The Captive Portal is compatible with 3rd party RADIUS guest access provisioning platforms, like those found in hotel registration systems, should you wish to create a paid Hotspot and automatically debit the guests account.

When guest access is provisioned on the same WLAN and LAN infrastructure used for internal traffic, guest access must not impact performance for corporate users. Regardless of which backend authentication is used, the FortiGate policy engine maps guest users to a group associated with a guest policy, which rate-limits guest traffic to ensure that it does not affect business-critical corporate traffic. You also have the ability to control guest usage based on time of day, bandwidth consumption, and other criteria.

**Role and Identity-based Access:** Role-based access control lets IT staff configure separate access profiles for different groups within an organization (e.g. faculty, students and guests in a school or clinicians, nurses, admin and facilities in a hospital) using separate SSIDs with specific authentication options. Fortinet's identity-aware policy engine maps the user to an internal group based on its authentication information. Different polices can be assigned to different groups, allowing you to segment users or client devices based on unique business and compliance needs.

With identity-based security it is possible to place multiple groups of users on a single SSID/VLAN while still having separate access privileges for each functional group or user. This policy driven security also simplifies enabling access to less-secure legacy devices and headless devices such as VoWLAN handsets, bar code scanners, medical devices etc., without compromising regulatory compliance requirements such as PCI DSS and HIPAA.

**WIDS and Rogue AP Detection:** Industry policies such as PCI DSS mandate regular reporting on suspicious or unknown APs. The FortiGate Rogue AP detection engine automates the scanning process to provide continuous monitoring for Rogue APs, and provides a means to determine if unknown APs are on the network.

While dedicated or background air monitors scan for unknown APs and wireless client traffic, FortiGate uses various on-wire correlation techniques to determine how and where the unknown AP is physically connected to the network. It can even detect Layer-3 APs regardless of security settings and NAT configuration.

The Rogue AP list shows MAC address, manufacturer, security profile, speed, last seen and ‘on-wire’ status, enabling administrators to rapidly classify trusted or untrusted devices, and take corrective action to locate and remove rogues.

**Strong Authentication and Encryption:** As one might expect, all Fortinet wireless products support the full range of enterprise authentication types including WPA2-802.1X and standards-based encryption types including AES, TKIP. Extended user authentication against RADIUS servers is secured by EAP-MD5, EAP-TLS, EAP-TTLS, and PEAP. FortiGate also supports authentication against LDAP and Active Directory, without the need for extra software licenses.

Fortinet considers all these security protocols **Standard WLAN Security** – They are used for user authentication or they are needed to secure communication with backend directory services. Every vendor must support (most of) them, merely to achieve Wi-Fi certification.
FortiGate Security Highlights

Beyond Standard WLAN Security, Fortinet stands alone in providing network security integrated on the same platform as the WLAN controller. The FortiOS license for any sized FortiGate provides all of the following security capabilities and much more, as standard. All you need to do is enable the security services you need, when you need them. There are no extra hoops to jump through, no tricks and no hidden license fees for Firewall, IPS, Application Control or any other security measures.

**Firewall:** FortiGate is repeatedly proven one of the fastest firewall platforms in the industry, with flagship models outperforming all competitors by three times the throughput of actual application traffic.

**VPN Gateway:** No need for a separate VPN device or WAN accelerator to manage at head office or branch offices. FortiGate has high performance SSL and IPSec VPN services built in. Fortinet also provides a free remote access VPN client for PCs, tablets and smartphones on all major operating systems.

**IPS:** Fortinet Intrusion Prevention System (IPS) technology protects networks from both known and unknown threats, blocking attacks that might otherwise take advantage of network vulnerabilities and unpatched systems. You can enable IPS on any FortiGate at the edge of your network or within the network core to protect critical business applications from both external and internal attacks.

**DLP:** FortiGate can also be used to protect information privacy, and prevent unauthorized leaks. Sophisticated pattern matching is used to prevent unauthorized communication of sensitive or regulated data through the corporate perimeter.

**Antimalware:** Thanks to a combination of hardware assisted layer-7 deep packet inspection and a massive library of malware and exploit signatures, FortiGate provides real-time protection against viruses, bot-nets, web exploits, Trojans and other malicious software variants. Regular FortiGuard Labs updates ensure immediate protection against newly discovered zero-day vulnerabilities.

**Web URL Filtering:** FortiGate can block access to any known harmful websites that may contain phishing/pharming attacks or malware, or any other site you specify. Beyond reducing exposure to malware, this can also be used to control access to age-appropriate content in schools, or to disallow people from viewing potentially objectionable content in public areas.

**Application Control:** With signatures for over 3,300 applications FortiGate offers unrivalled control over application priority and bandwidth management. FortiGate distinguishes unique applications, not just broad Wi-Fi priority classes. You can treat YouTube, HD YouTube, Netflix, Facebook, LinkedIn, SIP, Skype all differently. When bandwidth is scarce, you can ensure mission-critical traffic prevails as low priority applications are throttled back.

---

Here is a more complete list of what is in FortiOS:

- Advanced Threat Protection
- Client Reputation Analysis
- Contextual Visibility
- Extended Single Sign-On
- Sandbox Integration
- Per-Device Security Policies
- Secure Guest Access
- Enterprise-class Firewall
- IPSec and SSL VPN
- SSL-encrypted Traffic Inspection
- Antivirus / Antispyware
- Antispam filtering
- Intrusion Prevention System (IPS)
- Data Loss Prevention (DLP)
- Flow-based Inspection Options
- Web Filtering
- Application Control
- Network Access Control (NAC)
- Vulnerability Management
- Monitoring, Logging and Reporting
- WAN Optimization
- Wireless Controller
- VoIP Security
- Central Management
- Virtual Domains
- High Availability
- Layer 2/3 Routing Services
Unified Management

Because Fortinet’s wireless controller is tightly integrated into FortiOS, each SSID appears just like any other interface on the FortiGate and provides IT staff a ‘single pane of glass’ management for wired and wireless traffic and security. The same deep packet inspection engine that filters malicious content on the wired network also filters traffic on the virtual wireless network. WLAN and security are truly unified.

FortiAP Access Points

The FortiAP family of controller-managed access points provides secure, high performance indoor and outdoor wireless access with a full range of APs from single radio 802.11n through to dual radio 3x3 MIMO 802.11ac, including plenum rated models. Smoke detector styling on indoor models allows for placement in aesthetically sensitive areas, while ruggedized outdoor models are suitable for the most extreme conditions.

Automatic radio resource provisioning and zero-touch deployment features let you roll out FortiAPs quickly, even in remote offices with no FortiGate at the premises. All enterprise features such as fast roaming, mesh and bridging support, air monitor, guest access, Rogue AP detection, WMM and QoS are supported as standard, without needing to purchase expensive feature licenses.

Standard POE support: Carefully designed for thermal efficiency to reduce power consumption during full operation of both radios and 3x3 MIMO, all indoor FortiAPs run on the earlier POE standard 802.3af which is rated at 12.9W. So there is no need to upgrade your LAN switches to support 802.3at.

Zero-touch Deployment: FortiAPs use a robust discovery mechanism to locate nearby FortiGate controllers over L2 or L3 connected networks. Simply select the discovered APs in the FortiOS GUI and assign them to a wireless profile, and that is it. The FortiAP will automatically download the configuration and start to act as an air monitor, or broadcast SSIDs as an AP, or both.

Auto Radio Optimization: Featuring automatic radio resource provisioning and spectrum sampling, FortiAPs automatically optimize channel and power settings for best performance when first installed. If interference occurs in future, the APs readjust their radio settings automatically. Or this feature can be disabled, if you prefer to control the channel plan manually.

Air Monitor: Individual radios can be assigned to perform channel scanning as a background air monitor, or as a dedicated air monitor. In PCI compliance applications, dual radio APs can be used to provide both client access and dedicated monitoring simultaneously.

Easy Policy Assignment: Each configured SSID appears to the FortiGate as a virtual network interface which can undergo Firewall policy, IPS checks, A/V scanning, Identity based segmentation, Application rate-limiting, Data Leakage Prevention, connect to other sites via VPN, or undergo Network Access Control functions. This allows security policies to be applied easily, whether a single set of policies apply all SSIDs or unique policies apply separately to each SSID.

No VLAN Mapping: Because traffic is normally tunneled to the FortiGate controller...
for forwarding, it is not necessary to map SSIDs to VLANs on switches. This allows for rapid adds, moves and changes of physical APs, and permits SSIDs to be enabled wherever you like without altering the wired network configuration in any way.

**FortiAP Tunnel Mode SSIDs**

FortiAPs are controller-managed. In their default configuration, SSIDs tunnel all traffic to the FortiGate wireless controller within CAPWAP DTLS or non-DTLS tunnels, where it undergoes security threat removal and policy examination before it is allowed on the Internet or corporate LAN. This is where the power of consolidated security on the FortiGate really offers a distinct performance advantage, as well as maximizing policy granularity and visibility of user and device behavior.

The first advantage is that traffic is subjected to all enabled security measures in one pass, it doesn’t need to get on-and-off the wire, or to be copied in-and-out of each system’s memory, as it does when security is implemented in multiple separate appliances. This significantly impacts latency and throughput. Latency through a FortiGate with IPS, Firewall, Antivirus, Application Control all enabled is significantly lower than for traffic passing sequentially through four separate appliances.

The second big difference is that traffic is processed at the session level, so you preserve total visibility of which user, on what device, is doing what. This is absolutely crucial when it comes to applying per-user or per-device policies for any one of these security functions. Compare this to multiple security appliances. To pass flows from one to another you need to map the appliances to VLANs, not sessions. Per-user policy granularity is lost, you can only apply security policies at the VLAN level, not at the user or device level.

![Fig 3: FortiAP SSID in Tunnel Mode](image-url)
FortiAP Local Bridge Mode SSIDs

It is also possible to configure FortiAP SSIDs to bridge traffic directly to the local LAN, bypassing the secure tunnel altogether. Many competitive WLAN vendors advocate this approach, especially when APs are deployed in remote branch offices and connect to the wireless controller over a WAN link. Fortinet considers this a high risk strategy however, as it leaves the network exposed to security threats.

Unlike other vendors, Fortinet’s extensive Secure WLAN solution portfolio provides two alternative approaches (using FortiWiFi or FortiAP-S series APs), to overcome this – providing the same security at the branch as in corporate, without overloading the WAN. These are described in more detail below.
FortiAP / FortiGate Deployment Architectures

From small offices and remote branch offices to headquarters for very large enterprises and campus deployments, there is a FortiGate with the capacity to match. Flexibility and rightsizing are important, you may prefer a distributed security model over centralized, or you may have a data center. FortiGate supports multiple deployment options to meet your needs and preferences. Here are some common deployment scenarios:

Enterprise Edge Gateway Deployment

Use FortiGate to secure your network edge and act as the wireless controller as well. In this deployment model, each FortiAP uses CAPWAP tunnels to connect to a (typically mid-range) FortiGate for policy processing and forwarding. FortiGate Firewall provides protection from network threats, whether they originate from the Internet or from wireless devices.

Fig 5: Enterprise Edge Gateway Deployment
Enterprise Campus / HQ Deployment

Distribute the security and controller capacity throughout your campus for very high density deployments, by putting FortiGate controllers at the access switching layer. This improves capacity scaling for high-density, especially as you migrate to 802.11ac, and spreads the WLAN and security processing load.

AP traffic is tunneled to the nearest controller, and optionally may be dual homed to allow failover to a second controller for resiliency. Entry-level FortiGate appliances with integrated POE ports are particularly suitable for this deployment model, since they can also power the APs using POE.

Fig 6: Enterprise Campus / HQ Deployment
Centralized Controller Deployment

Centralize a cluster of mid-range or high-end FortiGates in your data center or private cloud. High availability with active/active failover ensures continuous session-level availability.

This deployment model enables the aggregation of many APs deployed in remote locations that do not have a local FortiGate. Remote FortiAPs connect back to the FortiGate cluster via a CAPWAP tunnel over the internet and appear to the controller like any other connected AP. Each FortiGate maintains a secure CAPWAP control plane and data plane to the APs it controls. Remote Rogue AP detection functions enterprise-wide without needing controllers at each location.

Fig 7: Centralized Controller Deployment
Large Branch Office Deployment

Use an entry-level FortiGate acting as a wireless controller and security gateway, with FortiAPs deployed throughout the premises. Entry-level FortiGates support anywhere from 2 to 32 FortiAPs, providing ample indoor coverage for any sized branch office.

The onsite FortiGate provides policy enforcement and security threat inspection for all traffic, regardless of the destination. To reduce the traffic load heading to your HQ or data center, the onsite FortiGate can be configured using a hybrid-WAN approach with split routing. This enables corporate traffic only to be routed to the HQ or data center, with the rest of the traffic routing directly to the Internet.

Fig 8: Large Branch Office Deployment
Small Branch Office Deployment

In small branch offices or retail locations, it is not necessary to deploy a FortiGate onsite. One or more FortiAPs can be installed independently. Each AP discovers its remote controller and sets up a CAPWAP tunnel to it. Most of the traffic passes over the tunnel and terminates on the FortiGate for security processing and forwarding, however split tunneling allows traffic destined for the local LAN to still be bridged locally. This provides access to resources such as printers, without having to hairpin the traffic through the remote FortiGate.

When you have many remote locations, it is often preferable to avoid backhauling traffic through your HQ or data center at all. However this normally requires separate security appliances at the remote site, which can dramatically increase capital and operational costs. To meet this requirement, Fortinet has two deployment alternatives: Using FortiWIFI, enterprises can provide Wi-Fi access and implement the same centralized security policies, firewall and WAN access with a single appliance.

Fig 9: Small Branch Office Deployment – Tunneled FortiAP or Standalone FortiWiFi
Or if the remote site already has a WAN router or appliance, the FortiAP-S series offers a new way to secure all wireless data at the edge, without needing additional security appliances on premises or at the data center. Using specialized security processing on the AP hardware itself the FortiAP-S series can apply your security policies for local Internet traffic, at the network edge, while using local bridging to forward only corporate traffic over the WAN to HQ or the data center.

Fig 10: Small Branch Offices - FortiAP-S Series
Related Products and Services

**FortiGuard**

FortiGate is *Secured by FortiGuard*, meaning that it receives continual exploit, virus and application signature updates, ensuring immediate protection from zero-day cyber threats. FortiGuard Labs is a global team of over 200 threat researchers who continually research the latest attacks, and figure out how to neutralize them. Their work results in regular security updates which are downloaded to Fortinet products as a FortiGuard subscription service, to provide your network with the latest protection against new and emerging threats.

**FortiManager**

In large networks, management can be aggregated via the FortiManager appliance. This provides centralized management of multiple FortiGates spread across locations, and facilitates creating enterprise-wide SSIDs, and scheduling firmware updates for FortiAP and FortiWiFi appliances. WLAN administrators can activate global changes to FortiAP configurations such as changing authentication settings, SSIDs or radio profiles, quickly and seamlessly across the organization without causing disruption.

**FortiAnalyzer**

Another component of Fortinet's central management is FortiAnalyzer, a network security logging, analysis, and reporting appliance which aggregates log data from all Fortinet security appliances. A comprehensive suite of easily customizable reports allows you to quickly analyze and visualize network threats, inefficiencies and usage.

Among the standard reports are comprehensive auditor-friendly PCI compliance reports which ease the pain of PCI DSS compliance reporting. FortiAnalyzer provides IT with enterprise-wise dashboard level statistics about the overall health of the wireless network, and the ability to drill-down to determine root cause of any problems.

**Controller-managed WLAN Summary**

Controller-based WLANs have been around since 2004, that’s a long time for commoditization of standards and features to take place, and it certainly has. WLAN vendors can all lay claim to supporting all the Wi-Fi security standards and WLAN performance tricks (band steering, airtime fairness, etc.). So the tangible differences between vendors for speeds and feeds are small and mostly irrelevant. Not so in the areas of management and security. Here there are vast differences between vendors.

Fortinet’s approach is truly unique. Putting WLAN management and network security on the same platform delivers a quantum leap in management simplicity, user experience and reduced TCO. The combination of FortiGate and FortiAP access points gives enterprises a more secure, easier to manage WLAN than any other alternative.