FORTINET

DEPLOYMENT GUIDE

Secure Wireless LAN

Complete Wi-Fi Security for Any Network Technology

Secure Wireless LAN

Overview

The simple requirement of any access layer, be it wired or wireless, is to allow simple and secure client access. This can be a challenge, but Fortinet has a wide range of solutions. The Fortinet Secure WLAN portfolio comprises three separate Wi-Fi product lines. This document deals with the two security-focused product lines, the Integrated solution, where APs are part of the fabric controlled by the FortiGate, and the Cloud solution, where the FortiGuard security can be deployed at the edge of the network. Fortinet's more traditional controller solution can of course be secured with the addition of a FortiGate, but this is more akin to the rest of the industry as separate solutions working together. The purpose of this document is to focus on the full integrated solution where UTM is built into the solution from the ground up. Solutions in this document are designed to meet the needs of different market segments with complete focus on comprehensive security, no matter which topology and network management model is best suited to the business.

Secure Wireless Lans

You can enjoy the industry's most comprehensive wireless security, regardless of the size of your business, your network topology, and your choice of integrated or cloud-based Wi-Fi management.

Introduction

With 6.5 million Wi-Fi certified devices shipping every day, Wi-Fi has become the network of choice in every type of business large and small, public venues, and hundreds of millions of homes. Wi-Fi has become ubiquitous, from home and workplace to coffee shop and on aircraft, Wi-Fi can keep you connected. The days of one-size-fits-all enterprise

Wi-Fi are over. The wide range of different use cases, deployment models, security requirements, and budgets dictate that vendors deliver different Wi-Fi solutions for different markets and deployment topologies. Some vendors have been slower to adapt than others.

Controller-managed WLAN solutions designed for large enterprise are a poor fit for SMBs and distributed enterprises because managing them is too complex and costly. Yet, established cloud-managed Wi-Fi offerings targeted at these underserved markets fall short on another dimension. They lack the comprehensive security found in corporate networks, which leaves cloud-managed Wi-Fi users exposed to a growing number of cyber threats.

In contrast, the Fortinet Secure WLAN portfolio meets the needs of these different market segments without sacrificing comprehensive security, no matter which deployment model is selected.

Commoditization of Wi-Fi Speeds and Feeds

Throughout its evolution, Wi-Fi has faced numerous deployment challenges, which have driven vendor innovation and new standards. New standards have largely taken care of the performance limitations: 802.11n, and MIMO, channel bonding, 802.11ac, MU-MIMO and these continue to evolve. Standards also solved roaming, QoS, device power drain, and many more issues. Vendor innovation took care of the rest, including band steering, AP load balancing, and bandwidth management, to name a few.

As is the way with technology, speeds and feeds and performance-enhancing features quickly get commoditized. Soon everyone has them. Management and security, however, remain perennial concerns that are very much in the limelight today. And unlike the speeds and feeds, vast differences exist between vendors.

Cloud Management vs. Security Tradeoffs

Since the first Wi-Fi security crisis in 2005, when a team at the FBI demonstrated how WEP security could be cracked in less than three minutes, wireless security has remained a top-ranking CIO concern. It began with requirements to let visitors and guests access the Internet while on your premises. Now with BYOD the accepted norm, the need for complete mobile security has never been more acute.

It's generally accepted that WPA2 Enterprise using 802.1X is a secure way for users to access a Wi-Fi network. But as the device landscape shifts from corporate-owned to employee-owned, and as network usage shifts to an ever-greater reliance on cloud services, the security challenge has also morphed. Access control is no longer the problem. The vulnerability is now your applications, content, and devices, which are continually exposed to cyber threats via the Internet.

Wireless security must go far beyond Wi-Fi access control of the past. In addition to facilitating BYOD, it must secure sessions, prevent users from visiting inappropriate websites, ensure the integrity of connected devices, and more. Large enterprises handle these complex security requirements in a variety of ways, with centralized firewalls, intrusion prevention systems (IPS), webfiltering and antivirus appliances, and so on, and by tunneling branch office traffic though the corporate network.

Not so for education and distributed enterprises such as retail chains, health clinics, hospitality, and transportation providers. They don't have the infrastructure, IT resources, or the networks to emulate the large enterprise hub-andspoke security model. No wonder they have been slow to adopt enterprise-grade Wi-Fi, unless it is managed by a service provider, and they have sometimes had to make do with consumer-grade products.

This dichotomy has given rise to cloud-managed Wi-Fi and cloud Wi-Fi vendors focused on these underserved markets, and it has created a flourishing market for managed security service providers. But as vendors have shifted their focus from controller-managed to cloud-managed Wi-Fi, they've taken one step forward and two steps back. Security above Layer 2 is more about reporting than actual control and focuses on the known and easily recognized applications rather than any real threat.

Fortinet Wi-Fi Security Without Compromises

Fortinet WLANs are different. Security is at the core of these Wi-Fi offerings. Fortinet Secure Wireless LAN solutions are designed to provide the same award-winning and third-party-validated security in every type of deployment, from a stand-alone AP in an isolated office to a handful of APs in a retail store to hundreds of APs deployed across a large enterprise campus. Our Wi-Fi product families enable any business to choose the topology and network management that best suits them, without having to compromise on security protection.

Securing business communications, personal information, financial transactions, and the mobile devices of your users involves much more than Wi-Fi access control. It requires scanning for malware, preventing access to malicious websites, endpoint integrity, checking and controlling application usage. But typical cloud Wi-Fi solutions don't cater to these requirements. Fortinet has a novel approach that completely addresses this shortcoming in all existing cloud Wi-Fi offerings.v

	Integrated Mary APs per site	Cloud Managed Few APs per site
Enterprise Campus / HQ	FortiGate + FortiAPs	
Large Branch	FortiGate + FortiAPs	FortiAP-S
Small Branch	FortiAPs tunneled or FortiWiFi [+FortiAPs]	FortiAP-S
Small Business	FortiWiFi [+FortiAPs]	FortiAP-S

Figure 1: Fortinet's Wi-Fi solutions for different requirements.

Enterprise Cloud Wi-Fi Migration Fears

Certain hypersensitive verticals (federal, financial, etc.) simply don't want any traffic to leave their network, not even AP management traffic, for fear of possible security breaches. But in general, large enterprises have been reluctant to move to cloud-managed Wi-Fi solutions. There are several reasons for this. The first is the per-AP subscription fees typical of cloud Wi-Fi offerings. For a large network, these recurring fees can, within a few years, eclipse the cost of local management servers and the staff to run them. Second, they already have a substantial investment in controller and management infrastructure. Third, while it may no longer be true, there is a general perception that cloud management provides less control and more limited reporting.

But above all, the biggest barrier is the disruption to the security framework that moving to the cloud would entail. Some network topologies are better suited than others for migration to cloud-managed Wi-Fi. However, for the majority of hub-and-spoke deployments and large enterprise campuses, there is more to lose than there is to gain because security enforcement beyond basic authentication becomes all the more complicated. For distributed, enterprises cloud-managed Wi-Fi can make sense, provided the equivalent security found in corporate networks can be replicated.

Gaps in Typical Cloud Wi-Fi Security

All cloud Wi-Fi vendors' solutions claim to be secure. And they are, up to a point. If the scope of your security is limited to access control or wireless intrusion detection, this is an easy checkbox to fill. However, on a broader scope there are significant gaps. No other vendor matches the comprehensive security available with Fortinet's integrated or cloud-managed Wi-Fi solutions. The comparison table below illustrates the voids found in typical cloud Wi-Fi offerings.

	Typical Management	Fortinet Cloud Wi-Fi
Configuration management	●	●
Bandwidth & traffic analysis	◑	●
Connected client analysis	◕	●
Guest access management	●	●
Access Control - WPA2, 802.1X	●	●
WIDS & Rogue AP detection	●	●
Network IPS	○	●
Web filtering	○	●
Antivirus	○	●
Application control	◕	●
Private Cloud for MSPs	○	●

Figure 2: Comparison of Fortinet vs. typical cloud Wi-Fi.

Fortinet Secure WLAN Solution Portfolio

Fortinet has different Wi-Fi hardware platforms optimized for different use cases. The same security protection is available across these product families, which allows businesses to choose the topology and management model that suits them best, without giving up important security capabilities.

FortiAP-S Series

The FortiAP-S Series is a family of singleand dual-radio 802.11ac access points designed for deployment in SMBs and distributed enterprise sites. They contain advanced security functions embedded in the AP hardware. Equipped with extra memory and twice the processing power of typical thin APs, they can perform real-time security processing at the network edge, not in the cloud or on the corporate LAN.

By implementing IPS, application controls, web filtering, and malware protection on the AP hardware itself, precious network bandwidth is conserved, and infected devices and applications are stopped in their tracks. SMBs and distributed enterprises get the simplicity of cloud management through FortiCloud and the protection of enterprise-class security without needing the collection of expensive security appliances normally required in large enterprise network deployments.

The APs receive regular exploit, malware, and application signature updates from Fortinet's award-winning FortiGuard security service, providing immediate protection against newly discovered virus and malware threats. And with over 3,300 application signatures, versus a few hundred at best from the nearest rival, FortiAP-S Series APs have the granularity to enforce laser-precision prioritization and bandwidth management far superior to crude WMM priority classes. Together, this means corporate content and application policies can now extend beyond the corporate network to any size location, without backhauling all traffic over the corporate WAN.

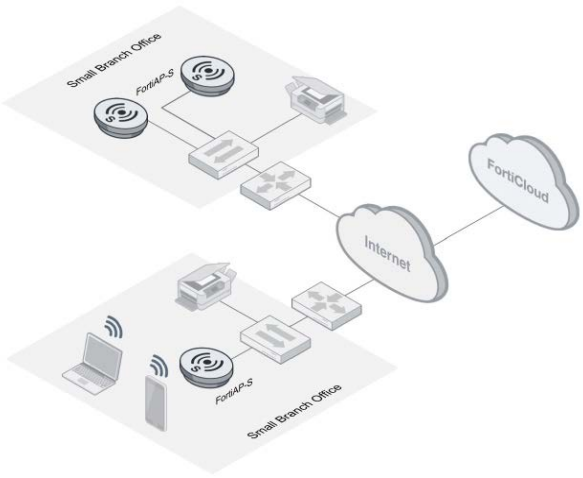

Figure 3: Distributed offices using FortiAP-S series.

Complete Security at the Network Edge

Because of the sheer volume of Internet traffic, some enterprises prefer to avoid tunneling Internet traffic from branches through the corporate network. This is especially true when the number of locations is large or when guest traffic predominates, as it does in hospitality, retail, and restaurants. Tunneling traffic through the corporate WAN is inefficient for cloud applications and it adds latency, not to mention the cost of needing bigger pipes. No one wants to backhaul a guest's highbandwidth videos and Facebook traffic through the corporate network, only to be able to provide application-level security in the remote site. But until now, enterprises have not have much choice. The alternative is to directly connect each site to the Internet which leaves these sites with limited control of application usage and leaves them exposed to all manner of cyber threats.

The FortiAP-S Series overcomes this deficiency, allowing distributed enterprise sites to connect to the Internet directly, without sacrificing security. Corporate users can still be authenticated against corporate RADIUS servers over the WAN if desired, or via FortiCloud, while all traffic from employees or guests is protected by enterprise-class Layer 7 security directly at the AP, without squandering WAN bandwidth.

The FortiAP-S Series allows distributed enterprises to benefit from superior security at all remote sites, without altering their existing security infrastructure at corporate or backhauling traffic through the corporate network, and without needing anything more than FortiAP-S Series APs at these locations.

FortiAP Series

The FortiAP Series is a family of integrated access points that function in cooperation with a FortiGate Wi-Fi Integrated Controller. The FortiGate is much more than just a Wi-Fi controller. It combines comprehensive network security and WLAN control by consolidating all the functions of Firewall, IPS, Anti-malware, VPN, WAN Optimization, Web Filtering, and Application Control in a single platform.

Recognized as a leader in Gartner's Magic Quadrant for Unified Threat Management since 2009, FortiGate enforces the most stringent access control and enables effortless BYOD onboarding. Complete PCI-DSS and HIPAA compliance is assured, along with the industry's most comprehensive protection for all manner of wireless and Internet threats. Enterprises can centrally administer security policies through a "single-pane-of-glass" management interface. Like other Fortinet security products, FortiGate is Secured by FortiGuard and receives regular signature updates, ensuring immediate protection from zero-day cyber threats.

The combination of FortiGate security and coordinated FortiAPs gives large enterprises, hospitals and schools scalability for thousands of APs and tens of thousands of clients, without the complexity of adding an assortment of point security products in order to provide complete threat protection.

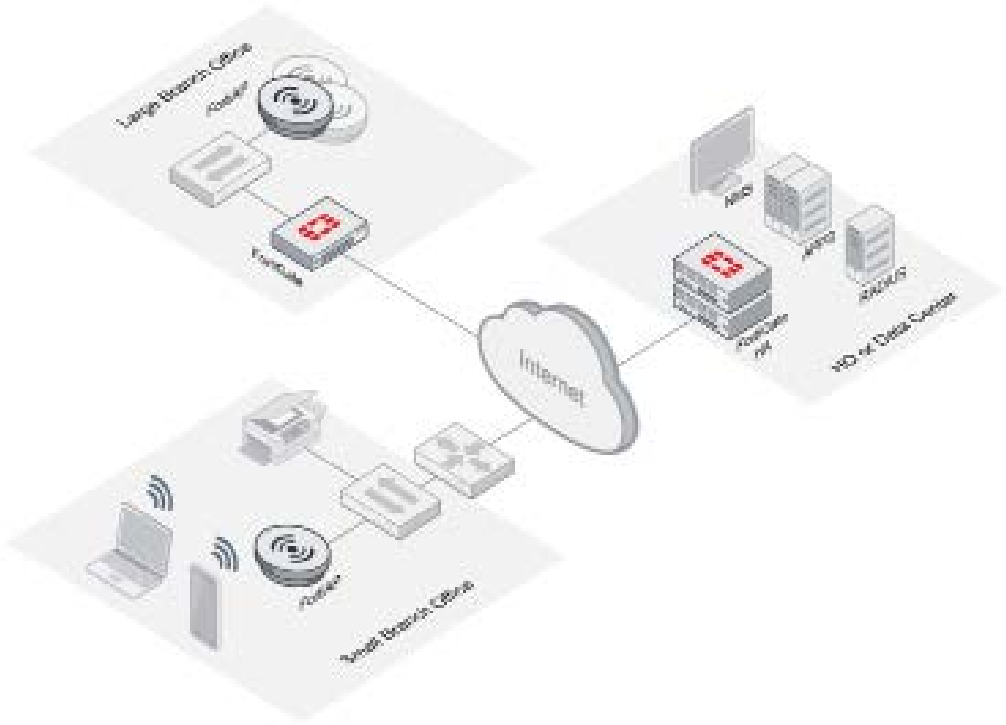

Figure 4: Large and small branch offices using FortiAP.

FortiWifi Series

The FortiWiFi Series are compact, stand-alone appliances that combine, in one platform, a full-featured wireless access point, a LAN switch, and an entry-level FortiGate equipped with WAN features and all the same security and WLAN functionality as its bigger brothers.

Ideal for branch offices and small businesses, a single FortiWiFi appliance provides everything from wired and wireless access, BOYD onboarding, and guest portal to unified threat management and WAN connectivity. It even supports backup broadband access over a 3G/4G/ LTE network. Remotely managed from the corporate network, FortiWiFi appliances provide complete threat protection locally in branch offices, while inheriting centralized corporate security policies.

Corporate traffic can be routed or bridged to the corporate network, while Internet traffic is bridged locally, fully protected by the FortiWiFi appliance implementing the same or different security policies as those at corporate.

With up to 3.5 Gbps firewall throughput, FortiWiFi appliances have the capacity to handle security for wired and wireless clients without becoming a performance bottleneck. A single FortiWiFi appliance provides wireless coverage for locations up to 3,000 square feet, making it an ideal onebox solution for small locations including retail establishments, clinics, and assisted living facilities. In larger sites, wireless coverage and capacity can be expanded with up to 32 additional FortiAP access points, enabling support for hundreds of mobile devices.

Equipped with world-class unified threat management and WAN connectivity, FortiWiFi makes an ideal entry-level Wi-Fi solution for managed service providers targeting SMBs. With one device they can cover network access and security requirements in one fell swoop, and they can easily extend Wi-Fi coverage with FortiAPs as needed.

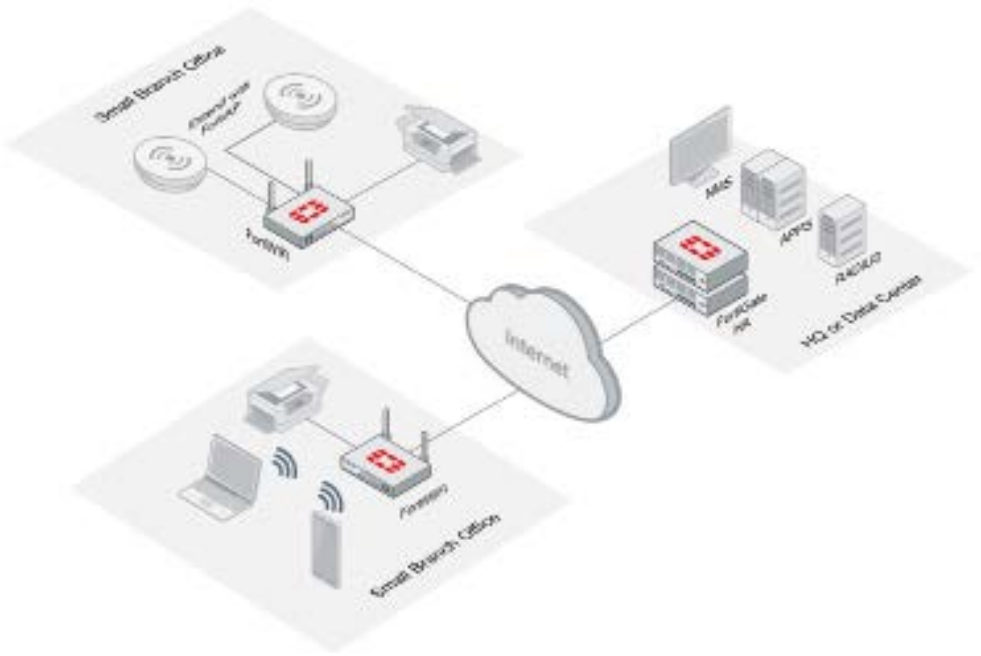

Figure 5: Small office using FortiWifi.

FortiCloud Provisioning and Management Service

FortiCloud offers a free, cloud-based provisioning, configuration management, and analytics service for FortiGate, FortiWiFi, FortiAP, and FortiAP-S Series product lines. It lets you quickly get up and running with Fortinet products and maintain centralized control and visibility of your network, all from the cloud, avoiding the cost of centralized management gear. FortiCloud eases provisioning of wireless and security devices at remote sites where on-site configuration expertise is unavailable.

FortiWiFi, FortiAP, FortiAP-S Series and FortiGate all include FortiCloud registration functionality in their firmware, enabling zero-touch provisioning with minimal on-premise expertise. From Rogue AP detection to guest access management to custom reporting, FortiCloud gives you everything you need to manage the complete Wi-Fi security environment at all enterprise locations and maintain full visibility of wireless health and the quality of experience for clients. FortiCloud also can be upgraded to a multi-tenant solution, which allows MSPs to offer a managed service with no significant investment.

FortiPortal for MSPs

MSPs can manage their clients' wireless, WAN, and security remotely through FortiPortal. FortiPortal is a feature-rich VM software platform designed specifically for MSPs, which enables them to deploy managed services on their own hosted services infrastructure. Designed with multi-tier, multi-tenant capabilities, it allows MSPs to manage all their customers' networks through one console, while also providing management access to their customers, allowing different privileges for different users.

Same Security on All Wi-Fi Platforms

To provide the same level of security as Fortinet, all competing WLAN vendors need a variety of different supplementary security products, depending on the WLAN solution architecture deployed. This adds to the operational complexity and TCO of their solutions. Lacking integrated security of their own, their cloud-managed Wi-Fi solutions must sacrifice the additional security measures often found in controllermanaged deployments.

In contrast, the Fortinet Secure WLAN portfolio offers the same comprehensive security across all its Wi-Fi platforms, whether integrated or cloud-managed. This makes it easy for businesses to mix and match deployment models for different use cases, without giving up critical security protection.

	FortiAP with FortiGate	FortiWifi	FortiAP-S with FortiCloud
WPA2, 802.1X, Captive Portal	√	√	√
WIDS	√	√	√
Rogue AP Detection	√	√	√
Network IPS	√	√	√
WAN / VPN	√	√	
Web Filtering	√	√	√
Antivirus	√	√	√
Application Control	√	√	√

Figure 6: Comparison of Fortinet wireless platform.

Presence Analytics Solution

Among the distributed enterprises most interested in deploying secure cloud Wi-Fi are retailers. Retail industry leaders recognize that Wi-Fi is about more than guest access these days. Naturally they want PCI compliance and stringent security, with the full benefit of fast Wi-Fi for their guests. But they also need value-added security and analytics services such as social Wi-Fi, web filtering, and presence analytics.

Complementing the industry's most secure wireless portfolio, Fortinet's Presence Analytics solution gives retailers much-needed consumer intelligence by combining presence information and big data. FortiPresence gathers presence data from access points distributed in a store and processes it in real time in the cloud, empowering retailers with the ability to instantly measure consumer footfall, connect to customers through social Wi-Fi, and influence them directly while they are in the store.

Complete Wi-Fi Security, No Compromise

As a global leader in network security, Fortinet provides complete and comprehensive security for wired and wireless users, no matter how large or small your business, on the network deployment model you prefer. Campus, large office, branch office, corner shop…controller-managed, cloud-managed, service provider managed…tunneled traffic, bridged traffic, both…The Fortinet Secure Wireless LAN solution portfolio delivers the same enterprise-class security in every scenario, without compromises.

January 24, 2020 9:28 AM

D:\Fortinet\Minor Changes\Re-color existing assets\dg-red-FA-secure-wireless-lan-solution-guide-1242020

485439-A-0-EN