Building the Fortified Wireless LAN
Consolidated, integrated security for wired and wireless networks
Contents
Introduction to Wireless Security ...................................................................................................................................................... 3
Fortinet Wireless Solutions ............................................................................................................................................................... 3
Key Criteria to Consider Before Deploying Wireless Technology ..................................................................................................... 6
  Coverage and Speed.................................................................................................................................................................... 6
  User Segmentation and Guest Access......................................................................................................................................... 6
  Strong Authentication and Encryption .......................................................................................................................................... 7
  Rogue AP Detection and On-wire Correlation .............................................................................................................................. 7
  Flexible Deployment Options ........................................................................................................................................................ 8
  Ease of Implementation ................................................................................................................................................................ 9
  Centralized Management ........................................................................................................................................................... 10
User Case Studies .......................................................................................................................................................................... 11
  Case One: K-12 Education ......................................................................................................................................................... 11
  Case Two: Distributed Retail Industry ........................................................................................................................................ 11
  Case Three: Healthcare Clinic/ Hospital Industry ....................................................................................................................... 13
Summary ......................................................................................................................................................................................... 14
Appendix 1 – FortiWiFi Platforms ................................................................................................................................................... 16
Appendix 2 – Wireless Controller Scalability of FortiGate Platforms .............................................................................................. 17
Appendix 3 – The Fortinet Advantage ............................................................................................................................................ 18
Introduction to Wireless Security

Growth of Wireless LANs

The increasing popularity of mobile devices and the need for cost reduction are driving Wireless LAN (WLAN) adoption. In-stat research forecasts that mobile handset shipments with Wi-Fi capability will achieve 50% CAGR from 2009 to 2013. In addition, organizations have embraced a wireless edge design to drive down the cost associated with edge switches and wiring. The ratification of the IEEE 802.11n wireless standard is the catalyst for new enterprise adoption since the new standard provides better coverage and fivefold performance increase over legacy wireless outperforming wired Fast Ethernet LANs.

Choice of Architectures

There are two leading Wi-Fi architectures today. One is called “Thick APs” and the other is referred to as “Thin APs.” The use of Thick or Thin AP Wi-Fi architecture depends on the service needs.

- **Thick AP** refers to a wireless access point or Wireless Termination Point (WTP) that autonomously switches packets between wired and wireless domains. Each Thick AP is a standalone device responsible for authentication, encryption and applying access control policies. Each Thick AP requires independent management, or management via a centralized network management application. All-in-one Thick APs are ideal for locations such as small office or retail shops requiring smaller service area.

- **Thin AP** provides the same features as a Thick AP, but in a distributed fashion to provide greater service area. The Thin AP simply passes wireless network traffic to the switch/controller, performing few complex tasks locally. This capability will enable all the Thin APs to delegate all the authentication, security processing, channel assignment, transmitter power level and rogue AP detection to the centralized wireless LAN controller which decreases management complexity and reduces overall cost of deployment. As the size of service area increases, you can deploy additional Thin APs and connect them to the existing Controller. Thin APs require a centralized wireless controller for management, and are ideal for locations requiring greater coverage and capacity than a single Thick AP can deliver.

The Need for Comprehensive Wireless LAN Security

Independent of the type of architecture used for access points, WLANs face many threats that strong authentication and link encryption do not address. Because wireless is a shared medium, it is subject to malicious attacks such as de-authentication broadcasts, evil twin access point (AP) / Honeypot. Also, it is possible for one user’s high usage of application traffic to reduce the bandwidth available to all other users. Therefore you need to implement the same protection mechanisms that you deploy ubiquitously on your WAN gateway, on your wireless LAN as well. Also, in response to these threats, regulators and standards bodies like the PCI Security Standards Council have created wireless data protection requirements. Failure to comply with those standards can result in significant penalties and/or loss of customer trust due to exposure of protected data.

Fortinet Wireless Solutions

Fortinet offers both Thick and Thin APs, as well as Wireless Controllers, to address your need for flexibility in deploying a secure wireless solution. This range of options gives you the choice you need to consolidate your security strategy to deliver integrated, comprehensive protection for both your wired and wireless networks.

**FortiWiFi (Thick AP)**

Fortinet provides five models of FortiWiFi security appliances with Thick AP capabilities, ranging from the FortiWiFi-30B to the FortiWiFi-81CM. These Thick AP devices offer a range of performance and features, including high-speed 802.11n support and WAN communications via optional wireless broadband access and dial-up modems.

The FortiWiFi consolidated security platforms deliver comprehensive enterprise-class protection for smaller locations at an affordable price. They make it easy to protect smaller locations, branch offices, customer
premise equipment (CPE) and retail networks. With the FortiWiFi platforms’ integrated set of essential security technologies, you can deploy a single device that protects all of your applications and data. The simple per-device pricing, integrated management console, and remote management capabilities significantly reduce the costs associated with deploying and managing complete content protection.

Each FortiWiFi model is capable of broadcasting up to seven SSIDs or Virtual Access Points (VAPs) enabling multi-tenant environments in a single device. Each VAP appears a separate virtual interface on the FortiWiFi device, enabling the application of separate firewall and user policies to the traffic. Appendix 1 includes a summary of the wireless features offered in FortiWiFi platforms.

**FortiAP (Thin AP)**

Fortinet’s FortiAP 200-series Access Points are affordable, indoor, IEEE 802.11n capable Thin APs that provide concurrent security and Wi-Fi client access on both the 2.4 GHz and 5 GHz spectrums. The FortiAP series utilize industry-leading wireless chip technology that takes advantage of 2x2 MIMO technology with dual transmit streams. This MIMO technology enables the FortiAP to reach wireless association rates as high as 300Mbps per radio and also allows the coverage to extend twice as far as legacy 802.11a/b/g.

Designed for use exclusively with Fortinet’s FortiGate series, FortiAP tunnels all traffic to the FortiGate Controller for added security and ease of management, eliminating the need for a separate Wireless Controller. Each FortiAP can support up to seven SSIDs per radio and these SSIDs show up as separate interfaces on the FortiGate, enabling multi-tenant environments in an AP. This architecture allows for the easy application of security policies from a single FortiGate platform, whether a single set of policies applied all SSIDs or unique policies applied separately to each SSID.

Table 1 describes the primary features and applications of the two models in the FortiAP family.

<table>
<thead>
<tr>
<th>Model</th>
<th>Target Applications</th>
</tr>
</thead>
</table>
| FortiAP-220B | • Designed for PCI Compliance applications, this AP provides a dual band (2.4/5 GHz) security monitoring radio and a second client access radio enabling full time wireless scanning without affecting client traffic.  
• Data rates of up to 600 Mbps (dual radio operation)  
• Can be powered by IEEE 802.3af POE for flexible installation  
• a/b/g/n bands |
| FortiAP-210B | • This single radio dual-band AP is designed for high performance client access with background air monitoring option or a dedicated air monitor for rogue AP detection.  
• Data rates of up to 300 Mbps  
• Can be powered by IEEE 802.3af PoE for flexible installation  
• a/b/g/n bands |

Table 1 - FortiAP Features and Applications
Wireless Controller – FortiGate Platforms

The FortiGate consolidated security platforms can act as wireless controllers, significantly reducing the cost and complexity of deploying secure WLANs. FortiGate platforms enable the integration of both wired and wireless traffic into a single management console, giving you a “single pane of glass” management interface of your network.

FortiGate platforms provide complete content protection against network, content, and application-level threats. These high-performance, low-latency devices ensure that your network security does not become a network bottleneck. 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 greater internal segmentation of data for policy compliance. (For more information on the FortiGate consolidated security platforms, see Appendix 3 – The Fortinet Advantage.)

Deploying FortiAPs with a FortiGate gateway acting as a wireless controller enables FortiAPs to “homerun” their client traffic directly to the FortiGate device. In this overlay network the wireless traffic bypasses the LAN and terminates at the FortiGate for security processing and routing which ensures that traffic undergoes threat removal and policy examination before its allowed back on the LAN. Figure 1 illustrates this architecture.
Fortinet is the only company to provide wireless controller options for any size environment and use case, from small offices and remote branch offices to headquarters for very large enterprises, as well as service providers and telecommunications carriers. FortiGate platforms protect a majority of the Fortune Global 500, as well as tens of thousands of smaller organizations around the world.

Key Criteria to Consider Before Deploying Wireless Technology

Coverage and Speed
Many wireless AP vendors claim the highest power output and correlate high power to a longer range. However, that would only be true if the Wi-Fi communication was broadcast or unidirectional like an FM radio station tower. Since Wi-Fi traffic is bidirectional, the wireless range is determined by capabilities of both the client and the AP. Because most Wi-Fi enabled devices are battery powered (for example, laptops and other mobile devices), they become the weakest link to the Wi-Fi range, not the AP.

FortiWiFi and FortiAP products generally 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 a wireless network. The typical Wi-Fi range depends on obstructions and interference sources, but the rule of thumb is that a wireless AP can cover a radius of 50-60 feet (approximately 15-18 meters). Deploying APs every 60 feet in a hexagonal or honeycomb pattern can increase the coverage.

Historically, enterprises have not adopted WLANs due to the lower speed of wireless compared to that of wired networks. The adoption of the IEEE 802.11n technology standard has enabled wireless speeds to surpass wired Fast Ethernet.

Fortinet’s FortiAP product family is 802.11n-capable and employs 2x2 MIMO technology that is able to provide 300 Mbps association rate for clients. Thus, it is able to provide over five times the performance and twice the range of legacy IEEE 802.11 a/b/g technology. The FortiAP device’s advanced signal processing ability is due to the use of dual antennas that maximize signal fidelity and data reconstruction.

User Segmentation and Guest Access
Organizations deploying WLANs want to have the ability to segment their users based on SSID as well as user role. Role-based access control gives employees on the same SSID different access privileges, which reduces risk of unauthorized access to confidential or regulated data by insiders. In addition, role-based access ensures guests, contractors and temporary workers instant access to timely business information without compromising corporate traffic.

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. This feature allows your IT organization to create rules to segment users or machines based on your unique business and compliance needs.

Since guest access is provisioned on the same WLAN and LAN infrastructure that is carrying internal traffic, it must not compromise corporate traffic at the expense of guest traffic. Regardless of which backend authentication is used, the FortiGate firewall policy engine maps users to a user group associated with a guest policy, which rate-limits guest traffic to ensure that it does not affect business-critical corporate traffic. Malicious content, such as rogue applications and viruses are kept off the guest network by FortiGate’s application control and IPS engines. You can enable additional security technologies built into every FortiGate, such as web filtering and antispam protection to further secure guest traffic. You also have the ability to enforce granular control of the guest network based on time of day, bandwidth consumption, and other criteria.
Strong Authentication and Encryption
Since WLANs are shared medium, encryption is a critical consideration. The following are authentication and encryption standards that have been widely adopted and supported.

- **Open/ WEP64/ WEP128/ Shared** – Used mainly for hotspot and guest access point where the traffic is to be routed directly to the Internet. With this option there is no authentication or link encryption. The open option should only be used for traffic that its security is not of concern or SSL or VPN communication will be used at application layer to secure the communication.

- **Guest Captive Portal** – Captive portal is an industry standard term for a web authentication form. In this mode the user 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 gateway.

- **WPA /WPA2 802.11i Preshared key** – Wi-Fi Protect Access WPA is available for backward compatibility, but all users should migrate to WPA2 as it provides more secure encryption of data. The Preshared key allows a password to be shared among all users to connect to the wireless LAN. This type of security is useful for guest or home access, but enterprises should provide unique username and password 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 the 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 best practice. The Radius engine supports PAP, CHAP, MS-CHAP, MS-CHAP-v2.

Fortinet Wireless products support the full range of Authentication types including WPA, WPA2 and newest standards based encryption types, including AES, TKIP, and WEP for wireless and SSL for captive portal. For Extended Authentication Protocol (EAP) Fortinet supports the full set of standard protocols to be compatible with your company user database. Extended user Authentication against Radius servers is secured by EAP-MD5, EAP-TLS, EAP-TTLS, and PEAP. The FortiOS operating system which powers the FortiGate and FortiWiFi devices supports authentication against LDAP and Active Directory, without the need for extra software licenses.

Rogue AP Detection and On-wire Correlation
Rogue APs can pose a threat to your internal network by creating a leakage point where a malicious user can steal confidential, regulated, or proprietary data. For this reason, industry policies such as PCI-DSS mandate the regular scanning for suspicious or unknown APs.

The goal of the FortiGate Rogue AP detection engine is to automate this scanning 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 network. Fortinet’s Rogue AP detection capability supports the following features:

- Dedicated or background Air Monitor scans for unknown APs and wireless client traffic.

- Unknown APs MAC address, 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.

- The correlation engine constantly compares wireless client traffic to wired client traffic to determine if a client using an unknown AP is communicating through a FortiGate device. 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.
Flexible Deployment Options

It is important for wireless vendors to provide flexible deployment options to meet your needs. Distributed retail customers could benefit from centralization and aggregation of a single Wireless Controller in the cloud, and Enterprises may benefit from a distributed controller deployment which allows for higher wireless throughputs. Fortinet wireless solution provides multiple deployment options to meet these needs.

- **Wiring closet deployment** allows the traffic to get services quickly at the first point of entry into the network. This allows greater bandwidth, since there are more FortiGate controllers servicing the wireless traffic. A FortiGate-200-POE is ideal in this situation since it can directly power up to 8 FortiAPs using its built-in POE ports (Figure 2).

- **Gateway deployment** allows customers to use their existing FortiGate device that is servicing the WAN-LAN boundary to act as the wireless controller as well. In this deployment model, each FortiAP forwards its traffic in a tunnel (illustrated by the blue paths in each deployment example) to the FortiGate for policy processing and forwarding (Figure 2).

- **Data center or cloud deployment** allows many remote locations to forward their traffic over the private network to a centralized FortiGate controller. This deployment model can be used for retailers to provide remote Rogue AP detection capability without the need to run independent wireless LAN controllers at each location. This model is also suitable for smaller locations that don’t have a dedicated FortiGate device. (Figure 3)
Ease of Implementation

Ease of deployment and implementation are essential considerations when you plan to deploy a wireless network. Your IT organization needs a solution that it can install with ease and low cost, and with an easy and intuitive setup process, while leveraging its existing infrastructure.

Fortinet provides all the components you need to achieve fast and low-cost deployment of WLANs. First, existing FortiGate users can simply upgrade their existing FortiGate consolidated security device listed in Appendix 1 with FortiOS 4.0 MR2 to take advantage of this new wireless controller capability. There are no additional license fees to run the wireless controller, just add some FortiAPs and you have an integrated wireless and wired network security architecture.

Second, the FortiAP setup is simplified so that each AP uses a robust discovery mechanism to locate nearby FortiGate controllers over L2 or L3 connected network. IT will simply select the discovered APs in the same familiar FortiOS GUI and assigns them to a wireless profile, and that is. The FortiAP will automatically download the configuration and start to act as air monitors, or Broadcast SSIDs as an AP, or provides both functions simultaneously.

Third, each configured SSID appears as a virtual network interface, and can be managed in the same way as a physical interface on the Fortinet appliance is managed and policed. The traffic on this interface can undergo FW policy, IPS checks, A/V scanning, Identity based segmentation, Application rate-limiting, Data leakage prevention, or connect to other sites via VPN, or undergo Network Access Control functions.

Last but not least, the FortiAP-210/220B devices have the option of using POE, eliminating the need to run extra AC outlet for the wireless AP. This not only reduces installation costs, but also gives you the flexibility to move the AP
without the need of an electrician. The FortiAP products comply with lower cost 802.3af specification and can be powered by existing POE switches or power injectors.

Centralized Management
Any viable wireless management solution for the enterprise should have the ability to manage both Thick and Thin APs. Fortinet provides centralized management of FortiGate and FortiWiFi devices via the FortiManager™, thereby eliminating the need to configure each and every discrete controller and Thick AP, reducing any chance of user error while setting up redundant systems. Software updates are also coordinated via this central approach.

Each FortiGate also centrally manages and performs software updates to its associated FortiAPs. FortiGate’s profile-based management allows IT to make global changes to all physical FortiAP by simply making a profile change. This allows authentication settings, SSIDs or radio management changes to take place across your organization seamlessly thereby reducing overall cost of operations and total cost of ownership.

Figure 4: AP Profile Based Central Management and Upgrade via FortiGate

Another component of central management is the FortiAnalyzer data mining and reporting. FortiAnalyzer centralizes all the logs from all FortiGates and allows IT to receive dashboard level statistics about the overall health of the wireless network, and to drill-through the information to determine root cause of any problems. This in turn helps managed service providers or large enterprises to provide monthly status reports and for helpdesk to quickly resolve any network connectivity or security issues.
User Case Studies

Case One: K-12 Education

Common issues to address:
- Separate students and faculty traffic to prevent potential attacks on Faculty PCs
- Provide access to grading system and other privileged servers
- Reduce costs by providing network access to all computers without a network switch
- URL Filtering of inappropriate Internet content
- Guest access to Internet

Deployment Example: Synapse Institute, San Mateo, CA.

Fortinet solutions:
- **Coverage**: This kindergarten through grade 12 facility required full wireless access. As it is larger than 3000 ft² (300 m²), it required the use of Thin AP products for optimum coverage. The same FortiGate-80C that secured the WAN communications also centrally managed three FortiAP Thin APs.

  At the pre-deployment planning stage, the Ekahau Site Survey Professional application was able to provide a clear picture of the coverage the school could expect with this three Thin AP design. A post-deployment survey showed that the school achieved full network coverage at 300Mbps throughout the facility.

- **Role-Based Access**: The IT staff is able to configure separate access profiles for faculty, students and guests using separate SSIDs with specific authentication options to a backend directory. The fully customizable HTML Captive Portal login page allows visitors and contractors to gain access to the Internet through without any risk to the LAN infrastructure.

- **Single Pane of Glass Management**: Because Fortinet’s Wireless Controller is tightly integrated into FortiOS, each SSID appears as a virtual interface on the FortiGate and provides the IT staff the ‘single pane of glass’ management for wired and wireless traffic. The same rich deep packet inspection engine that filters malicious content on the wired interfaces also filters traffic on the virtual wireless interfaces. Role-based policy and deep packet inspection engine allows the IT staff to rate-limit or block student traffic that is not education-related. Standard firewall policies keep student and faculty traffic separate from each other and ensure that only faculty members have access to the grading servers and the color printer. Also, the FortiGate enforces time-based access policies to limit network access for specific times during the school day.

Case Two: Distributed Retail Industry

Common issues to address:
- Encrypted connectivity of multiple distributed stores to headquarters
- Secure wireless coverage for different size store fronts from 1,000 ft² (100 m²) in some locations to 40,000 ft² (4,000 m²) in warehouses
- Wireless monitoring with rogue AP detection and reporting to achieve PCI DSS compliance
- Separation Point of Sale (POS) registers from wireless network, back office computers and inventory contractors
- Wireless voice roaming throughout the store
Fortinet solutions:

- **Secure connectivity of remote retail locations to the headquarters and separate regulated data:**
  
  - Both FortiGate and FortiWiFi platforms run the FortiOS operating system, delivering a wide range of consolidated security and networking technologies, including the ability to establish a secure IPsec VPN tunnel between HQ and the retail locations. This allows all POS transactions and voice conversations to traverse this secure tunnel to HQ before it is routed.
  
  - Split routing is also possible via the onsite FortiGate/FortiWiFi, enabling policy enforcement of local traffic before being routed to the Internet, eliminating the need to first traverse the IPsec tunnel to HQ.
  
  - The FortiGate and FortiWiFi devices also offer multiple ports that allow for the physical separation of network segments. This enables you to meet regulatory requirements for segmentation of systems handling card data from other users and devices.

- **Complete coverage of any size retail location:** FortiGate/FortiWiFi and FortiAP solutions can cover any location, from small kiosks to very large destination retail locations.
  
  - Retail locations that are less than 3000 ft² can provide coverage for their store using the FortiWiFi gateway.
  
  - Larger locations can use a FortiGate acting as a wireless controller with multiple FortiAP Thin APs deployed every 100-120 ft (32-40 m), to provide constant wireless connectivity. For instance, a FortiGate-80C can service 16 FortiAP devices that provide service to an area of 48,000 ft² (4,500 m²) with high obstructions. If there are fewer obstructions the coverage increases to 150,000 ft² (14,000 m²) and if the space is open the coverage expands to approximately 500,000 ft² (46,500 m²). This enables checkout personnel to be mobile throughout the store to provide pricing for merchandise, electronic coupons and information research information on products to achieve higher sales conversion ratios.

- **PCI DSS compliance with WLANS:** Retailers can use FortiGate/FortiWiFi and FortiAPs to address the requirement to mitigate the threat that rogue APs pose to the integrity of their credit card transaction system. The simplest and most cost effective method to address this risk is to use an automated monitoring system. For example, both FortiWiFi-60C platforms and FortiAP devices provide dual band radios that operate on both the 2.4 GHz and 5 GHz bands to seek out other APs. After identifying the APs by MAC address and manufacturer type, the Fortinet devices use an ‘on-wire’ correlation technique to seek out wireless devices connected to the retail network. The Fortinet devices flag these APs with a high severity ‘on-wire’ syslog message and transmits it to an upstream log aggregation device and/or the FortiAnalyzer centralized analysis and reporting system. Once alerted of the presence of the device at the retail location, the IT staff can physically remove the rogue AP from the network.

- **Temporary access:** You can create a separate SSID to grant access to groups of users who need temporary access to the network, such as inventory personnel. This separation provides access to the necessary systems keeping the back-office network and POS systems completely segmented.

**Deployment Example:** Large super market chain, New England region, USA

Fortinet has been securely connecting the multiple locations of this growing super market chain. This customer saw the need to abide by the PCI DSS standards and the benefit of providing wireless access throughout the store for business efficiency.

Wired Ethernet was not an option due to the large and disparate location of the clients and the higher cost of wired ports and cabling. This customer was able to upgrade its existing FortiGate devices to wireless controllers via an update on the FortiOS operating system. Since the customer had maintained their support contract, there were no additional software costs or licenses to manage.

The customer deployed FortiAP Thin APs and connected them directly to the FortiGate in the back office. The automatic discovery protocol simplified installation and the FortiGate was able to provision the wireless service
throughout the store after a few configuration clicks. The customer used firewall policies to segment the SSIDs from each other and allow only necessary access between zones.

As the customer was already familiar with the FortiOS ‘single pane of glass’ management console, it was very easy for the IT staff to consolidate its wired and wireless policies. The customer was also able to detect the presence of a rogue AP in one of their locations immediately after deployment, yielding immediate ROI to the customer.

Case Three: Healthcare Clinic/ Hospital Industry

Common issues to address:

- HIPAA and similar regulations around the world require that healthcare providers ensure the confidentiality of patient information. These regulations require the segmentation of network traffic from patient data with along with access audit trails to ensure patient health data is not compromised.

- To provide better care for patients and better tracking of treatments, the industry is rapidly adopting the Electronic Medical Record (EMR) management of data. Since this data needs to be accessed and manipulated at the bedside, the equivalent of a ‘digital clipboard’ is required. The iPad is the ‘ultimate thin client’ and this digital clipboard enables EMR access for doctors and nurses, and is being well embraced by the industry. The thin client requires fast mobility and good signal-to-noise ratio for greater coverage and response time.

- Much of the medical equipment in the industry runs off of a PC operating system, such as Microsoft Windows, and they suffer from the same vulnerabilities that our desktops face. However, due to the life critical nature of medical equipment, IT staff is not allowed to load A/V clients or install Microsoft patches on medical devices. Unfortunately, there have been incidents where a doctor connected his personal laptop to the network and unknowingly spread malware to the medical equipment on that network.

- For larger facilities, asset tracking is an issue that can increase operations costs due to misplaced equipment. A system of locating each piece of equipment and hospital staff members at any time can improve the efficiency of the hospital and increase the turnover of patients and beds, leading to increased profits.

- Visitors and patients hotspot access to Internet is desired and may be additional source of revenue.

Fortinet solutions:

- Reliability and Security: The critical nature of medical processes requires a highly reliable and secure wireless infrastructure to deliver high-speed access to all corners of the facility. Medical professionals require high data transfer rates to download medical images and large files. The FortiAP thin access points can be deployed in numbers to blanket the facility each servicing large pool of clients with high performance IEEE 802.11n performance to meet this stringent coverage requirement. The Automatic Radio Resource Provisioning feature ensures that the FortiAPs are operating on non-interfering channels and identifies other APs that may be interference sources. Since the FortiAP operates on concurrently both the 5 GHz and 2.4 GHz bands, you can move much of the mission-critical traffic to the more open 5 GHz band, freeing up precious bandwidth on 2.4 GHz.

- Confidentiality of Data: The Fortinet integrated network security and wireless solution gives your IT staff powerful tools for ensuring patient confidentiality throughout the healthcare system (such as hospitals, clinics, and doctors’ offices). Since all users must authenticate with the wireless network, the FortiGate
Wireless Controller can use this information as an identity-based policy enforcement tool. Identity-based enforcement ensures that only medical personnel have access to patient records and medical devices, and can segment staff traffic from guest/visitor traffic. The ICSA-certified identity-aware firewall security policies follow users as they move from the hospital, to clinics, and even to their home office.

- Legacy WLAN solutions tie policies to specific SSID/VLANs, making network designs unnecessarily complex.
- With identity-based security, hospitals can place nurses, doctors, operations, and management on a single SSID/VLAN while having separate access privileges for each functional group or user. The policy driven security also simplifies providing access to less-secure legacy devices (e.g. old Voice over WLAN handsets, bar code scanners, etc.) without compromising HIPAA requirements.

- **Network Segmentation:** You can protect your medical devices from malware by using the FortiGate consolidated security platform for your wireless and wired infrastructure. The FortiGate 1240B for example provides 48 1-Gbps ports to segment medical equipment and other user PCs as well as removing malicious content from both the wireless and wired networks. All traffic will pass through the FortiOS inspection engine, where it cleanses the traffic prior to being routed to another segment of the network.

- **Guest Access:** The built-in Captive Portal page provides patient and visitor access, giving you the ability to authenticate guests with separate individual passwords. This system is compatible with 3rd party RADIUS guest access provisioning systems to provide a paid hot-spot feature to meet business requirements.

- **Location Awareness:** Precise location-tracking is often achieved by placing small Wi-Fi tags on mobile assets or in badges of personnel. These Wi-Fi tags beacon the location of the mobile devices through the FortiAP to a backend positioning engine installed on a separate server. FortiAP is compatible with Wi-Fi tags enabling the location engine from partners such as Ekahau Real-Time Location System to identify the location of assets and personnel. The site survey data from Ekahau tells the location engine the Wi-Fi characteristics at every location in the building and helps in accurately triangulating assets or personnel in real time, as well as monitoring the wireless network coverage area.

**Deployment example: Radiation Oncology Center, Central Florida, USA**
The doctors and staff in this medical institution gravitated to using the iPad as the method to access medical records at the patients’ bed side, therefore necessitating an overnight Wi-Fi deployment. This multi-site oncology center uses a MPLS backbone to connect all sites together over a private cloud.

The Center is using a FortiGate platform at the larger facility to provide secure WAN access to the Internet and URL filtering. By simply upgrading the OS of this device, the IT staff was able to use it as the Wireless LAN controller and deploy FortiAPs in all locations. Since there is IP connectivity between the sites, the FortiAPs connect through the MPLS cloud back to the FortiGate controller at the main facility. Multiple FortiAPs are deployed at each remote location to provide high performance 802.11n connectivity and edge-to-edge coverage of the facility. This Datacenter / Cloud deployment model was the least expensive and least complex method for wireless deployment with performance and security advantage but without any need for license upgrades or additional Wireless Controllers.

**Summary**

Fortinet wireless technology delivers the integrated, consolidated security every organization needs to fortify their wireless network security. FortiGate, FortiWiFi and FortiAP security platforms add layers of security to wireless traffic without affecting performance or increasing costs. You can quickly and easily add core security services such as application control, antivirus, intrusion prevention (IPS), web filtering, antispam, and traffic shaping to your network, which reduce your risk of unauthorized access, data loss, or damage to critical systems.
FortiGate and FortiWiFi platforms provide the ‘single pane of glass’ management you need for increased control and visibility of all network traffic. Our robust reporting and analysis tools also help you demonstrate policy compliance and satisfy audit requests. Fortinet delivers complete, end-to-end security, from the mobile endpoint to the network core. Our solutions scale for any size environment, from the SOHO to Headquarters to a global telecommunications provider.

For more information or to find your nearest reseller, please visit www.fortinet.com.
Appendix 1 – FortiWiFi Platforms

Table 2 below shows the wireless standards and features included in each model of the FortiWiFi consolidated security platforms.

<table>
<thead>
<tr>
<th>Wireless Standards and capabilities</th>
<th>FortiWiFi Platforms</th>
</tr>
</thead>
<tbody>
<tr>
<td>802.11a</td>
<td>Yes</td>
</tr>
<tr>
<td>802.11 b/g</td>
<td>Yes</td>
</tr>
<tr>
<td>802.11n</td>
<td>Yes</td>
</tr>
<tr>
<td>High-Throughput 40 MHz Option</td>
<td>Yes</td>
</tr>
<tr>
<td>WME / WMM Multimedia Extensions</td>
<td>Yes</td>
</tr>
<tr>
<td>Max Wireless association rate</td>
<td>54 Mbps</td>
</tr>
<tr>
<td>Number of simultaneous SSIDs</td>
<td>7</td>
</tr>
<tr>
<td>Background Rogue AP detection</td>
<td>Yes</td>
</tr>
<tr>
<td>Rogue AP on-wire correlation</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Table 2: FortiWiFi Family Features
Appendix 2 – Wireless Controller Scalability of FortiGate Platforms

Table 3 below summarizes the number of FortiAPs that specific models of FortiGate platforms can service. Note: in version 4.0MR2 special release only the FortiGate family can function as the Wi-Fi Controller for FortiAP devices. FortiWiFi products are Thick APs, and are managed as stand-alone devices or centrally managed by FortiManager centralized management platform for centralized management of multiple FortiGate/FortiWiFi platforms.

<table>
<thead>
<tr>
<th>FortiGate Platform</th>
<th>Number of Supported FortiAPs (Thin APs)</th>
</tr>
</thead>
<tbody>
<tr>
<td>60B/C</td>
<td>4</td>
</tr>
<tr>
<td>80C Series</td>
<td>16</td>
</tr>
<tr>
<td>110C/111C</td>
<td>32</td>
</tr>
<tr>
<td>200B/200B-POE</td>
<td>32</td>
</tr>
<tr>
<td>310B/311B</td>
<td>32</td>
</tr>
<tr>
<td>800</td>
<td>64</td>
</tr>
<tr>
<td>1240B</td>
<td>64</td>
</tr>
<tr>
<td>3016B</td>
<td>256</td>
</tr>
<tr>
<td>3040B</td>
<td>256</td>
</tr>
<tr>
<td>3140B</td>
<td>256</td>
</tr>
<tr>
<td>3600A</td>
<td>256</td>
</tr>
<tr>
<td>3810A</td>
<td>512</td>
</tr>
<tr>
<td>3950B/3951B</td>
<td>512</td>
</tr>
<tr>
<td>5001A</td>
<td>512</td>
</tr>
</tbody>
</table>

Table 3: FortiGate Scalability as a Wireless Controller
Appendix 3 – The Fortinet Advantage

Complete Content Protection
Fortinet delivers complete content protection for today's evolving networks. Over the last 10 to 15 years, threats have transformed from connection-based to content-based. Traditional security technologies have not kept up with this evolution and cannot tell the difference between malicious and legitimate content.

Threats can enter your network from common applications like email and web browsers as well as the latest social networking tools. Today's threats require complete content protection, which is more than simply identifying applications and allowing or denying the traffic. It is application control coupled with identity-based policy enforcement of all content.

Our high-performance unified threat management solutions provide the visibility you need to detect hidden threats within legitimate content, even from trusted sources and authorized applications. This unmatched protection means you can allow new applications into your network, but automatically block any malicious content or behavior.

Market Leadership
Fortinet is the market leader in unified threat management, delivering purpose-built solutions that improve performance, increase protection, and reduce costs. We secure the networks of more than 100,000 customers worldwide, including the majority of the Fortune Global 500. Many of the largest and most successful organizations and service providers in the world rely on Fortinet technology to protect their networks and data, including:

- 7 of the top 10 Fortune companies in Americas
- 8 of the top 10 Fortune companies in EMEA
- 8 of the top 10 Fortune companies in APAC
- 10 of the top 10 Fortune telecommunications companies
- 9 of the top 10 Fortune banking companies
Certified Protection
Fortinet is the only unified threat management vendor to earn certifications across all core security technologies. These independent certifications demonstrate our ability to consolidate multiple security technologies into a single device while still meeting the highest standards of performance and accuracy. Our certifications include:

- 7 ICSA Labs security certifications
- NSS UTM certification
- ISO 9001 certification
- 12 Virus Bulletin (VB) 100% awards
- IPV6 certification and Common Criteria Evaluation Assurance Level 4 Augmented (EAL 4+) for FortiOS 3.0

Unmatched Performance
Fortinet’s purpose built hardware and software provide industry-leading performance for the most demanding networking environments. We developed our integrated architecture specifically to provide extremely high throughput and exceptionally low latency. Our unique approach minimizes packet processing while accurately scanning the data for threats. Custom FortiASIC™ processors deliver the power you need to detect malicious content at multi-Gigabit speeds. Other security technologies cannot protect against today’s wide range of content- and connection-based threats because they rely on general-purpose CPUs, causing a dangerous performance gap. FortiASIC processors provide the performance needed to block emerging threats, meet rigorous third-party certifications, and ensure that your network security solution does not become a network bottleneck.
Global Threat Research and Support

Our FortiGuard® Labs’ global team of threat researchers continuously monitors the evolving threat landscape. The team of over 125 FortiGuard Labs researchers provides around the clock coverage to ensure your network stays protected. It delivers rapid product updates and detailed security knowledge, providing protection from new and emerging threats. Our FortiCare customer support organization provides global technical support for all Fortinet products, with support staff in the Americas, Europe, and Asia.