As a recognized leader in network security, Fortinet provides a comprehensive, secure wireless solution for uninterrupted clinical applications at any facility, with the best performance and broadest set of capabilities in the industry.

Fortinet Wi-Fi for Healthcare

Secure Wireless LAN for Uninterrupted Clinical Applications

Healthcare professionals are the epitome of a mobile workforce: Constantly on the move, yet highly dependent on fast, accurate information. They need a secure wireless solution that delivers flawless performance on an array of devices they rely on every day.

Hospitals, clinics, and elderly care facilities have countless ways to exploit wireless technology for better patient care and operational efficiency. Whether they use computers on wheels, handheld tablets, or Wi-Fi enabled medical devices, the growing security threat arising from BYOD, and the competition for bandwidth, make network security and application control a critical success factor.

Equipped with industry-leading network security services delivering line-rate deep packet inspection, Fortinet's secure wireless LAN (WLAN) solution addresses the security and performance requirements for uninterrupted clinical applications, with the least amount of administrative complexity.

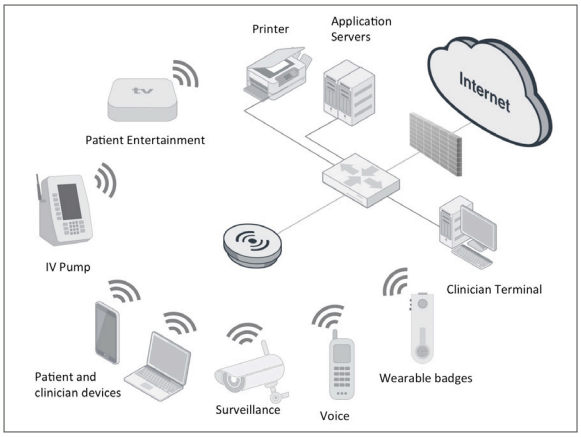

Figure 1: Fortinet Secure Wireless LAN Solution for Clinical Applications

- Advanced BYOD: Simplified device onboarding and integrity checks
- Integrated Security: Industry-leading security effectiveness
- Application Control: Policy-based control over any application usage
- Functional Consolidation: Right-sized platforms for every size facility
- No Feature Gouging: Enterprise feature-set without hidden license fees

Healthcare WLAN Challenges

Plethora of Mobile Devices: Today's caregivers have a veritable arsenal of mobile devices at their disposal, many of which are personal devices. From smartphones to Wi-Fi VoIP phones and voice badges, a typical clinician may carry three or four mobile devices, and use any number of other Wi-Fi enabled medical devices, from tablets to infusion pumps.

Securely onboarding the myriad devices and preserving network integrity is imperative. Dealing with the different operating systems and user interfaces – some of them headless – can quickly drain IT resources without the right security framework in place. Adding to the complexity, some devices are personal, while others are shared, requiring different policies depending on the identity of the user.

Escalating Mobile Threats: The introduction of so many personal mobile devices in patient care delivery has resulted in a growing reliance on the Internet and cloud services. This poses a major security threat to the healthcare network, since this is where malware and viruses originate.

Due to their relative immaturity, mobile platforms are now a prime target for attack. This puts the network at risk and endangers patient privacy. In May 2015 Forrester surveyed 150 IT pros using Next Generation Firewalls, asking what factors impacted their organization's vulnerability to security breaches and attacks. 87% of respondents said increased use of mobile devices significantly impacted their vulnerability.

Wireless network security has always been an important factor for HIPAA compliance, and all wireless LAN vendors have delivered robust solutions to neutralize wireless protocol and RF threats such as Rogue APs, DDoS attacks, man-in-the-middle, and many more. However, the growing exposure to malware, resulting from BYOD and increased Internet use, is something new and ever changing, requiring wholly different L3-L7 security strategies that most WLAN vendors are not equipped for.

Competition for Bandwidth: Beyond mobile access to EMR/EHR, which is now commonplace, video and imaging applications are becoming more widespread. And as the resolution of imaging systems shoots upward, so too spirals wireless bandwidth demand. Meanwhile, other mission-critical applications such as wireless voice services, mobile patient monitors and telemedicine, demand guaranteed bandwidth and priority to function properly.

Healthcare has more than its fair share of mission-critical applications; some are life-critical. Wireless LANs are now expected to deliver those applications without a glitch at the point of care, be it bedside, in examination rooms and hallways, or even in the most RF-hostile environments such as elevators.

As if all the clinical applications were not enough, they must vie for bandwidth with patients and visitors who might be watching movies on their smartphones while connected as guests on your Wi-Fi infrastructure. Effective bandwidth and application management is therefore crucial to a successful wireless deployment. No amount of investment in 802.11ac access points will satiate the thirst for bandwidth, as this is a scarce resource that must be managed with scalpel precision – lives can truly depend on it.

Rural and Community Clinics: The recent growth in remote clinics and community health centers is helping to reduce the cost of medical delivery in local communities short on medical practitioners. However, to be effective, these facilities must provide access to centralized medical records and support applications such as telemedicine to allow specialists at other locations to consult remotely.

Clinicians demand a consistent experience every time. Regardless whether they are at a hospital or at a small clinic, they must be able to connect to the WLAN and access the applications and resources they need, just as they do at their main place of work, without changing anything. The clinic WLAN should be an extension of their normal workplace, with the same utility-like performance and reliability.

For remote care delivery to make economic sense, the CAPEX and OPEX costs of provisioning and maintaining Wi-Fi access and secure VPN connectivity over the Internet must be minimized.

Solution Overview

With advanced application management capabilities and world-class security protection effectiveness, Fortinet's secure WLAN solution is unique in its ability to fully address the security, bandwidth, and application performance challenges that can so easily derail healthcare WLAN deployments.

Healthcare IT infrastructure and applications are diverse enough. Why add more complexity with an incomplete mobile security framework? With Fortinet you don't have to. It is not

necessary to integrate an array of point security products from different vendors and run the risk of leaving gaps, or making it so complex that only a security mastermind can manage the network.

Fortinet's consolidated security solution embodied in FortiGate combines WLAN controller functions, network security, and application control on a single, easy-to-manage platform, allowing network administrators to manage users, devices, security, and applications holistically through a "single pane of glass" management interface, while ensuring user-centric mobility for clinicians.

With Fortinet, hospitals, clinics, and long-term care facilities can embrace the latest mobile clinical applications with confidence that they will perform as they should, and with the assurance that patient data is completely secure from all types of security threats, from Wi-Fi hackers to viruses and malware.

By unifying L3-L7 security and application control with WLAN and VPN management, Fortinet's secure WLAN solution saves network administrators enormous amounts of time, and removes the complexity and risk of using multiple point security products.

From large campus WAN aggregation or data center firewall applications to distributed clinics and elderly care facilities, the FortiGate, FortiWiFi, and FortiAP product families can match the price, performance, and scale requirements of any venue.

Medium to Large Facilities

In hospital campus deployments, retirement villages, and large assisted-living communities, a WLAN solution based on FortiGate and coordinated FortiAP access points provides unlimited scalability for extended coverage areas, supporting many thousands of client devices.

The FortiGate provides unified security and WLAN control by consolidating all the functions of Firewall, Intrusion Prevention, Anti-malware, VPN, WAN Optimization, Web Filtering and Application Control in a single platform. This enables effortless support BYOD, compliance with PCI DSS and HIPAA, and the industry's most comprehensive protection for all manner of wireless and Internet threats, while providing the benefits of centrally administered security policies through "single pane of glass" management.

FortiAP access points provide secure, high performance indoor and outdoor wireless access from a broad family of 802.11n and 802.11ac devices. The FortiAP family includes models with dual Ethernet ports for resiliency against switch failure, plenum ratings as well as EN-60601-1-1 and EN-60601-1-2 certifications for use in medical environments. Featuring automatic radio resource provisioning and spectrum sampling, they automatically optimize channel and power settings to ensure optimum performance, amid the ever-changing RF conditions typical of large healthcare facilities. All enterprise features, such as guest access, Rogue AP detection, and QoS, are supported as standard, without needing to purchase expensive feature licenses.

Small Locations

The FortiWiFi series takes the FortiGate consolidation theme one step further. They are compact, all-in-one appliances that combine a wireless access point and an entry-level FortiGate, providing coverage for locations up to 200 square meters (2,000 square feet), making it an ideal one-box solution.

With a single device that covers everything from Wi-Fi access, BYOD onboarding, and guest portal to Unified Threat Management and WAN connectivity, it couldn't be easier to deploy secure Wi-Fi access and mission-critical clinical applications in small locations such as clinics, community health centers, and assisted living facilities.

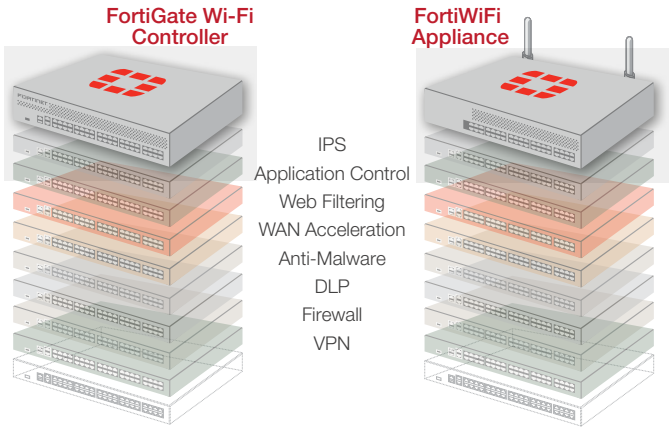

Figure 2: FortiGate/FortiWiFi Functional Consolidation

Crucial Security Features in Healthcare Facilities

No matter how large or small the location, a common security framework is required across the entire health network. Fortinet's experience in unified threat management, coupled with its commitment to functional consolidation, brings right-sized security and Wi-Fi control to every facility.

BYOD Onboarding: FortiGate and FortiWiFi provide seamless self-service onboarding, with device integrity checking, virus scanning, and authentication setup, keeping devices off the network until they have been fully screened. Guest portals and Social Wi-Fi features allow a variety of options for enabling and controlling patient and visitor access through branded ports.

Threat Protection: FortiGate and FortiWiFi provide complete protection from wireless threats such as Rogue APs or MAC spoofing, to all types of malware, meeting HIPAA regulatory requirements, and ensuring patient data is safe and network integrity is preserved. Backed by FortiGuard Labs, which continually researches the latest attacks, the platforms receive real-time updates, providing your network with immediate protection against newly discovered virus and malware threats.

Web URL Filtering: FortiGate and FortiWiFi can block access to any known harmful websites that may contain phishing/pharming attacks or malware, or any other site. Beyond reducing exposure to malware, this can also be used to prevent patients and visitors from viewing potentially objectionable content in public areas, or at all, or to reduce potential bandwidth abuse or noise from videos and gaming.

Application Control: Signatures for thousands of applications, combined with high-performance, ASIC-assisted packet inspection, give FortiGate/FortiWiFi platforms unrivalled granularity for application priority and bandwidth management. When bandwidth is scarce, mission-critical clinical applications run without interruption or degraded performance, as low-priority applications are throttled to ensure priority apps get what is prescribed for them.

Unified Management: Functional consolidation simplifies management and provides tremendous time savings. You can administer the same (or different) policies to the wired and wireless network and monitor everything through a "single pane of glass," not a collection of disconnected management consoles. This removes complexity and eliminates the risk of leaving gaps in your security policies.

Summary

Healthcare networks are classic "distributed enterprises," requiring everything from all-in-one appliances at small clinics to VPN aggregation and centralized security services at the nerve center. As a recognized leader in network security, Fortinet is able to provide a comprehensive, secure wireless solution for uninterrupted clinical applications at any facility, with the best performance and broadest set of capabilities at the best value.

Mobility is paramount. Caregivers roam both within and between multiple facilities. Therefore, healthcare WLANs must not only be fast and secure, but they must also be convenient. Wherever clinicians roam, with a Fortinet secure wireless LAN they can connect instantly and feel right at home without changing a thing. They'll have access to all the same resources they are used to, completely segregated from patients and visitors whose access is controlled through a branded guest portal. Regardless of the size of the location, wherever they are, they'll have the same L3-L7 protection and application priorities as they have at a large hospital campus.

Fortinet transcends basic Wi-Fi access, enabling unified wired and wireless security policies, application service profiles, and L1-L7 security measures on every device at every point of care – all managed through a "single pane of glass." Only Fortinet's secure wireless LAN solution delivers the low total cost of ownership that comes from its unique combination of consolidated functionality, unified management, and a fair AP pricing strategy that is free of feature licenses.

GLOBAL HEADQUARTERS
Fortinet Inc.
899 Kifer Road
Sunnyvale, CA 94086
United States
Tel: +1.408.235.7700
www.fortinet.com/sales

EMEA SALES OFFICE
120 rue Albert Caquot
06560, Sophia Antipolis,
France
Tel: +33.4.8987.0510

APAC SALES OFFICE
300 Beach Road 20-01
The Concourse
Singapore 199555
Tel: +65.6513.3730

LATIN AMERICA SALES OFFICE
Paseo de la Reforma 412 piso 16
Col. Juarez
C.P. 06600
México D.F.
Tel: 011-52-(55) 5524-8428

July 29, 2015