



Securing the Wireless Network in Enterprise Branch Offices & Small Businesses

White Paper

February, 2004

Abstract

Wireless LANs (WLANs) have experienced tremendous growth since the introduction of the 802.11x wireless networking standard. Flexibility, ease of deployment and administration, and the resulting low total cost of ownership constitute three of the major incentives accounting for the popularity of WLANs. These factors encourage the deployment of WLANs in small businesses and remote offices, where elimination of cabling and ease of administering the network can result in significant savings to the organization.

However, the same flexibility and mobility enabled by wireless networking also introduces new security vulnerabilities in addition to those faced by conventional, wired networks today. For real-time communications enabled by wireless LANs, a comprehensive real-time network protection strategy is required to enable pervasive, widespread deployment.

This paper reviews the challenges confronting wireless LANs and their associated security solutions, and how Fortinet's FortiGate™ Antivirus Firewall systems enable enterprises with remote offices and small businesses to successfully navigate the constantly changing landscape of network threats to wireless LANs.

© Fortinet, Inc. All rights reserved.

The information contained in this document represents the current view of Fortinet, Inc. on the issues discussed as of the date of publication.

This document is for informational purposes only. FORTINET MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS DOCUMENT.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording or otherwise) or for any purpose, without the express written permission of Fortinet Corporation.

Fortinet may have patents, patent applications, trademarks, copyrights or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Fortinet, the furnishing of this document does not give you any license to these patents, trademarks, copyrights or other intellectual property.

Fortinet, FortiGate and FortiContent are either registered trademarks or trademarks of Fortinet, Inc., in the United States and/or other countries.

*Fortinet, Inc.
920 Stewart Drive
Sunnyvale, CA 94085
USA*

Contents

| | |
|--|----|
| The Growing Wireless Opportunity..... | 4 |
| Wireless LANs: New Freedoms, New Risks..... | 4 |
| Fortinet Solutions Provide Complete Content Protection | 7 |
| Secure Wireless Access with the FortiWiFi-60..... | 8 |
| Summary | 10 |
| More Information | 10 |

The Growing Wireless Opportunity

The convenience of mobile data access is driving adoption of wireless networking across all types of organizations, from small and medium sized businesses to the largest enterprises. As a result we are rapidly entering an environment in which we will simply expect to have wireless connectivity wherever we are – in our homes, in our businesses, and in public locations. Wireless LANs (WLANs) enable new mobile data applications and also reduce the costs associated with installing and managing cabling. WLANs free employees to contribute at any location, increasing productivity. As a result, InfoTech predicts that WLAN penetration will reach 80% in the US by 2008,”¹

Small and medium-sized businesses continue to increase as economies move to more emphasis on services. Price sensitivity sways decision-makers toward ease of installation, administration and use for equipment and technologies used for networking. Additionally, the need for mobility within the Enterprise has increased. Travel among business users continues to rise, leading to information that no longer resides centrally, but has become distributed and portable. Laptops, Personal Digital Assistants (PDAs) and built-in connectivity such as 802.11, have become popular because of their ease of implementation, allowing users to create and break connections to the Enterprise network at will, often without notice, increasing access and productivity, but introducing security exposures as well.

For any small or medium-sized site, the choice of wireless connectivity is compelling but is not without risk, and requires both careful planning and thought. New, additional exposures introduced by wireless networking such as the demand-based connectivity mentioned above compound the threats already facing more traditional wired infrastructures.

Wireless LANs: New Freedoms, New Risks

According to Gartner, various security and capacity planning challenges will confront businesses as they adopt and try to manage WLANs². These issues include:

- *Rogue access points* that are connected into enterprise Ethernet ports, but have their security turned off, thereby extending Ethernet access and broadcasting traffic into unsecured areas.
- *Stand-alone access points* are not connected directly to any enterprise Ethernet port, and can become a threat when enterprise users accidentally connect to them wirelessly, thereby exposing their PCs.

¹ Mixed fortunes for enterprise WLANs, By Wireless Watch, November 21, 2003

²“Public Wireless LAN Hot Spots: Worldwide, 2002-2008,” Gartner, May 15, 2003

Because WLANs use publicly available radio spectrum as the medium to carry data, unauthorized access and eavesdropping are key concerns. Major security threats to WLANs include:

- WLAN access points can be probed by anyone within reach of the network’s radio signal, thus constituting physically unbounded entry points from which to launch intrusions, viruses and all other types of attacks that threaten landline networks.
- WLAN access points are often deployed inside corporate networks “behind” conventional firewalls, making these access points even more attractive as points for launching attacks.
- WLANs are extremely vulnerable to Denial of Service (DoS) attacks and service interruptions. Any malicious hacker with a laptop and wireless NIC card can transmit wireless signal interrupters in close proximity to company sites where WLANs are deployed and effectively “jam” a WiFi signal.
- Internal employees can set up their WLAN interface cards to operate in “peer-to-peer” (Adhoc) mode to communicate directly with people outside of the company.

Naturally, the framers of the 802.11b wireless standards were aware of these vulnerabilities and designed a number of security features into the technology to address them, most of which are minor patches rather than a complete solution addressing the previous issues. These include the following:

- *The use of Service Set Identifier (SSID):* The SSID is a common shared secret (typically an ASCII string) that has to be configured by network administrators into all access points and wireless terminals (e.g., PCs) that share a common WLAN.
- *Media Access Control (MAC) address filtering:* Since every WLAN terminal’s network card has a unique MAC address, it is possible to manually maintain a set of allowed MAC addresses for physical address filtering. Using a MAC address access control list, the system administrator needs to update the list constantly to accommodate changes, including when users get a new or replacement WLAN interface card.
- *Wired Equivalent Privacy:* Using WEP, communications between mobile terminals and access points are scrambled using a symmetrical encryption technique called RC4 on the data link layer. This prevents eavesdropping and also prevents unauthorized access by users that have not been configured with the necessary encryption key. WEP offers both 40-bit and 128-bit encryption strengths

However, as is demonstrated by the regular exercise known as the World Wide War Drive (wherein participants cruise metropolitan streets with WiFi-enabled devices, looking for unsecured Access Points – Table 1), exposures to unauthorized network access are numerous and range from the simple to the complex.

IEEE standards 802.11a & b

both include the Wired Equivalent Privacy (WEP) security standard. However, it has been acknowledged that WEP presented an administrative challenge in managing

| Conventional WLAN Security Offers Limited Protection | | | |
|---|-------|---------|----------------|
| Category | Total | Percent | Percent Change |
| Total AP Found | 88122 | 100 | +71.68 |
| WEP Enabled | 28427 | 32.26 | +4.34 |
| No WEP Enabled | 59695 | 67.74 | -4.34 |
| Default SSID | 24525 | 27.83 | -7.44 |
| Default SSID and No WEP | 21822 | 24.76 | -6.68 |

Table 1 – Results from World Wide War Drive [The Third WWWD took place from 28 June thru 5 July 2003]³

3. “WWD3 Statistics,” <http://www.worldwidewardrive.org/>

encryption keys for each user. The IEEE undertook the newer standard, 802.11g, with the intent of providing stronger authentication as well as Advanced Encryption Standard (AES).

Proposed jointly by the IEEE and Wi-Fi Alliance, WiFi Protected Access (WPA) is a specification of standards based, interoperable security enhancements that increase the level of data protection and access control for existing WiFi networks. WPA has been designed to be forward compatible with the IEEE 802.11i specification. It utilizes the enhanced data encryption TKIP (Temporal Key Integrity Protocol) in addition to user authentication using 802.1X and EAP (Extensible Authentication Protocol).

The IEEE is close to completing the 802.1X standard. Within this standard is a stronger security mechanism known as the robust security network (RSN) feature. RSN defines two security networks: the legacy method is hardware based on RC4 (along the lines of WEP), while; the newer hardware method is based on the advanced encryption standard (AES). The AES standard has an open format that will allow new methodologies to be incorporated as they are developed.

In the last ten years, applications have become much more complex, and protocol changes have been made to carry much richer content. These changes are being exploited by attackers in creating more effective, content-based threats that circumvent traditional, connection-oriented security. New threats have the ability to reproduce and spread automatically. Content-based threats bypass connection-oriented Stateful Inspection firewalls because they are typically delivered via connections that are inherently “trusted”. Content-based threats include viruses, Trojans, worms, banned content and spam. Newer threats containing elements of all are readily propagated through email, web pages and other real-time communications applications.

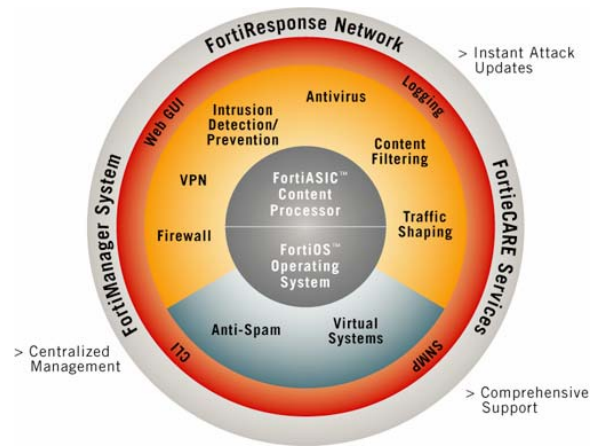
While RSN uses port authentication to authenticate wireless devices and to provide dynamic keys for encryption, wireless LAN users who are authorized and get connected still share the same vulnerabilities as those users who share a physical connection: WiFi users browsing the Internet can be exposed to viruses and worms in email, file transfers and Web (HTTP) downloads and applications that are not scanned by conventional firewalls or email-based antivirus software. ***Perhaps of greater concern, wireless users who’s laptops have become infected with a virus or worm while at a remote location can easily introduce that threat into their own (or other) company network, because no wireless security standard includes protections against content-based threats: Once a user is authenticated and allowed to connect to a wireless access point, the wireless channel can be used to deliver viruses and worms into the wired network, from “behind” the organization’s typical perimeter defenses (firewall, etc.).***

Given all the above risks, a secure WLAN then will need protection against unauthorized access at the link levels, but also at network, user and application layers. A secure wireless platform must include mechanisms for securing physical-layer access, prohibiting undesirable network-layer connections between clients, and protection at the application-layer from malicious code, and against unauthorized use of network resources (e.g.: worms, Trojans or blocking access to banned URLs).

Fortinet Solutions Provide Complete Content Protection

FortiGate Antivirus Firewalls are based on a groundbreaking architecture designed specifically to deliver application-layer security and network-layer security in real time. All models in the product family employ Fortinet's unique FortiASIC™ content processing chip and the powerful, secure, FortiOS™ operating system to achieve breakthrough price/performance. The ASIC-based architecture analyzes content and behavior in real time, and delivers a combination of services and performance that cannot be matched using conventional layer 3/layer 4 networking architectures or by deploying software applications on conventional computer systems.

FortiGate Antivirus Firewalls offer a comprehensive set of capabilities that address the key challenges to deploying secure wired and wireless LANs. FortiGate systems can be deployed in small and medium businesses and in remote offices and used to detect and eliminate content-based threats from email and Web traffic (e.g.: viruses, worms, intrusions, inappropriate Web content and more in real time) without degrading network performance. In addition to providing application-level protection, the FortiGate systems deliver a full range of network-level services — firewall, VPN, intrusion detection and traffic shaping — delivering a complete network protection services in dedicated, easily managed platforms.



FortiGate antivirus firewalls address the limitations of traditional firewalls by using a more sophisticated approach to network security called Complete Content Protection. Complete Content Protection involves the reassembly of packet payloads into application-level objects, such as files, documents, and programs, followed by the scanning and analysis of the objects to detect content-based threats. To prevent the new attacks, the same real-time Complete Content Protection can be applied at all WLAN access points much as they are at internal, physical network gateways (e.g.: the distribution zone, or workgroup zone) to prevent infection and the rapid spread of content-based attacks.

Secure Wireless Access with the FortiWiFi-60



The FortiWiFi™-60 is an integrated wireless access security solution that provides complete, real-time network protection at the wireless access point. The FortiWiFi-60 provides secure mobile connectivity by combining a wireless access point with a full suite of standards-based wireless security features, and also includes a complete set of network security functions including network-based antivirus, firewall, content filtering, VPN, intrusion detection and prevention, and traffic shaping. Providing default support for Wired Equivalent Privacy (WEP), and upgradeable to WiFi Protected Access (WPA) the FortiWiFi-60 ensures standards compatibility as they evolve to 802.11i.

Implemented in the small- or medium-size business, these features work together to ensure that wireless users enjoy worry free, high performance access without compromising the integrity of company networks. Implemented in the remote- or branch-office, the FortiWiFi-60 extends internal security beyond the traditional Enterprise boundary.

The FortiWiFi-60 unit features an integrated 802.11b and 802.11g WLAN access point and allows administrators to apply antivirus, firewall, VPN, and intrusion detection and prevention services to wireless connections. The FortiWiFi-60 also provides dual WAN link support for redundant Internet connections, and an integrated 4-port switch that eliminates the need for an external hub or switch, giving networked devices a direct connection to the FortiWiFi-60. Two USB ports offer support for connections to dial-up modems. Ideally suited for small businesses and remote offices, as well as retail stores and broadband telecommuter sites, the FortiWiFi-60 is unmatched in capabilities, speed, and price/performance. The FortiWiFi-60 is kept up to date automatically by Fortinet's FortiProtect Network, which provides continuous updates that ensure protection against the latest viruses, worms, Trojans, and other threats — around the clock, and around the world.

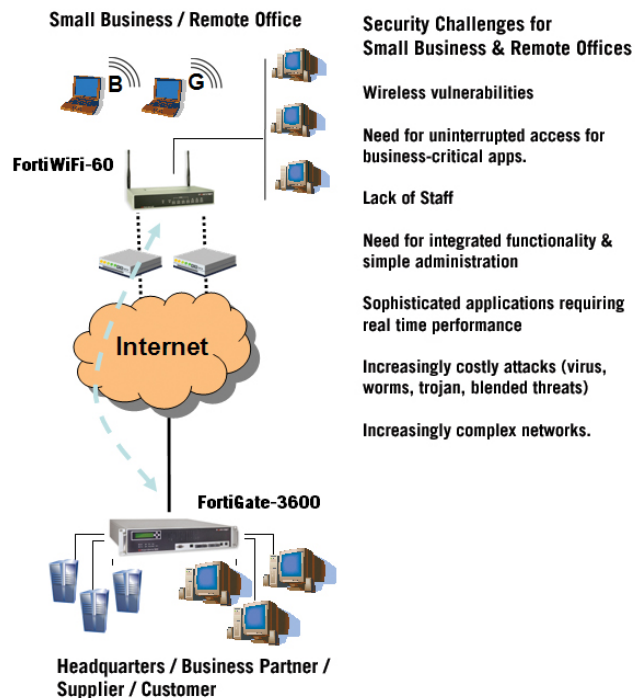


Table 2 summarizes the features and benefits of the FortiWiFi-60 solution.

| Feature | Function | Benefit |
|------------------------------|---|---|
| Complete Content Protection | <ul style="list-style-type: none"> Eliminates viruses and worms from email, file transfer, and real-time (Web) traffic without degrading network performance | <p>Increased user satisfaction while maximizing internal threat containment</p> <p>MAXIMUM THREAT ELIMINATION</p> |
| FortiOS | <ul style="list-style-type: none"> Underlying FortiOS™ operating system is ICASA-certified for Antivirus, Firewall, IPSec VPN, and Intrusion Detection | <p>Guaranteed security</p> <p>BEST OF BREED SECURITY</p> |
| FortiASIC Chip | <ul style="list-style-type: none"> Fortinet-designed custom chip, accelerates scanning and elimination of content-based threats. | <p>Real-time performance, no degradation in performance even when scanning broadband wireless connections for viruses, worms and other content-based threats.</p> <p>FASTER PERFORMANCE</p> |
| WiFi | <ul style="list-style-type: none"> Integrated wireless access point with industry standard 802.11b and 802.11g WLAN support | <p>Standards-compliant implementation guaranteeing ease-of-use network integration</p> <p>INTEROPERABILITY WITH ALL STANDARDS-BASED PRODUCTS</p> |
| FortiManager System | <ul style="list-style-type: none"> Centralized management system that can manage dozens, hundreds or thousands of FortiWiFi and FortiGate units. | <p>Scalability of administration contributing to lowest total cost of ownership in the Industry</p> <p>REDUCED MANAGEMENT COSTS</p> |
| WEP and IPSec support | <ul style="list-style-type: none"> Implements Wireless Encryption Protocol over WLAN connections Provides enterprise level wireless security through enforced IPSec encryption for WLAN connections Upgradeable to WiFi Protected Access (WPA) | <p>Standards-compliant implementation guaranteeing ease-of-use network integration, and maximum-strength security</p> <p>STANDARDS-BASED ENCRYPTION</p> |
| Rogue Access Point Discovery | <ul style="list-style-type: none"> Automatically detects rogue access points by scanning all radio frequency (RF) channels for any access points in range | <p>Industry-benchmark WiFi network awareness and reporting guaranteeing topology integrity</p> <p>MAXIMUM PROTECTION</p> |
| FortiProtect Network | <ul style="list-style-type: none"> Automatically downloads the latest virus and attack database and can accept instant “push” updates from the FortiProtect Network | <p>Lowest possible latency between discovery and elimination of contemporary threats</p> <p>REDUCED VULNERABILITY TO ATTACKS</p> |

The table below compares today’s conventional wireless access points with Fortinet’s FortiWiFi-60 solution:

| Feature | Conventional Wireless Access Points | Fortinet’s Solution FortiWiFi-60 |
|------------------------------|--|--|
| Connectivity 802.11x | Varies by Manufacturer, most have a/b or just b or b/g | 802.11b/g |
| Security (WEP/WPA) | Varies by Manufacturer, most have WEP, WPA support possible with few manufacturers | WEP (Yes) WPA (Planned and Upgradeable) |
| Rogue Access Point Detection | Varies by Manufacturer, mostly wireless networking vendors | Yes |
| VPN (IPSec) | Varies by Manufacturer, mostly security vendors | Yes |
| Antivirus | No | Yes |
| Firewall | Yes | Yes |
| Content filtering | Additional Fee, if available | Yes |
| IDS | No | Yes |
| IDP | No | Yes |

Summary

Wireless LANs provide a tremendous amount of freedom and flexibility and support the increasing desire for always-on, always-available mobile connectivity. Wireless LANs can also provide significantly lower Total-Cost-of-Ownership to small businesses and in remote or branch offices with their elimination of cabling and ease of administration.

However, wireless LANs also break down the notion of a definable “network edge,” and bring significant new challenges for maintaining network security. With proper augmentation, the security deficiencies of wireless LANs can be mitigated, enabling the benefits of un-tethered connectivity without compromising security.

Fortinet’s FortiASIC technology in conjunction with the FortiOS brings Complete Content Protection beyond that of traditional firewalls to add a critical layer of protection to wireless LANs, extending the life and improving the security of existing systems. Implemented in all FortiGate units including the FortiWiFi 60, small businesses and enterprises can deploy with confidence the 802.11b/g technology – enabling cost effective connectivity at all their locations, as well as deriving maximum threat reduction while lowering their total administrative costs.

More Information

Please visit our web site at www.fortinet.com or email us at info@fortinet.com.