



# Real-Time Network Protection for the Enterprise Wireless LAN

## White Paper

*July 2003*

### *Abstract*

Wireless LANs have experienced tremendous growth since the introduction of the 802.11x wireless networking standard spurred development of a wide range of solutions developed by traditional network equipment vendors. Flexibility, ease of deployment and low components costs constitute three major drivers for the popularity of WLANs. However, the same flexibility and mobility provided by wireless networking also introduces new security vulnerabilities in addition to those that threaten conventional LANs. 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 LAN security solutions, and describes how Fortinet's FortiGate™ Antivirus Firewall systems enable enterprises and service providers to successfully navigate the constantly changing landscape of network threats to wireless LANs.

---

## **Wireless LANs: New Freedoms, New Risks**

The wireless LAN (WLAN) market is poised to take off. By 2005, Gartner projects that over 80 percent of corporate PCs will be wireless LAN-enabled<sup>1</sup>. According to Gartner, various security and capacity planning challenges will confront enterprises as they adopt and try to manage WLANs. These issues include:

- Rogue and foreign stand-alone access points installed by those unaware of the security impact of such practices. *Rogue access points* are connected into enterprise Ethernet ports, but have their security turned off, thereby broadcasting Ethernet traffic into unsecured areas. *Stand-alone access points* are not connected directly to any enterprise Ethernet port, but can become a threat when enterprise users accidentally connect to them wirelessly, thereby exposing their PCs.
- Concerns about managing enterprise airspace as a resource. Wireless bandwidth is a shared resource that needs to be appropriately managed and allocated in accordance with key business priorities.

Current wireless LAN standards are not security-hardened for the enterprise. For example 802.11a/b both include the WEP (Wired Equivalent Privacy) security standard but as is universally acknowledged WEP is relatively easy to crack, and presents a major challenge for administrators to manage encryption keys for each user. The newest emerging standard, 802.11g, which contains stronger authentication and AES (Advanced Encryption Standard) capabilities, has only recently been approved, will not be available in new WLAN systems for some time, and will not be retrofit-able into much of the WLAN infrastructure that has already been deployed by users.

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.

---

<sup>1</sup> "Public Wireless LAN Hot Spots: Worldwide, 2002-2008," Gartner, May 15, 2003

- 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) attack and interruption. 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” (P2P) mode to communicate directly with people outside of the company.

### **Conventional WLAN Security Offers Limited Protection**

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 patches rather than complete solutions. 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. The weakness of the SSID is that it’s a relatively simple password, common to all devices on the WLAN, and once the SSID is compromised, any device with the SSID can gain unrestricted access to the WLAN. Further, the default setting of SSID is often not changed in WLAN deployments, and access points are typically configured to broadcast their SSID, further degrading security since intruders can get the SSID through easily obtainable tools.

*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. In addition, MAC

---

address filtering merely verifies the identity of the WLAN interface card, and not the identity of the PC into which it's inserted or the person using the PC. Finally, MAC authentication complicates support for roaming between different access points, and since MAC addresses can be spoofed, it is not regarded as a strong authentication method.

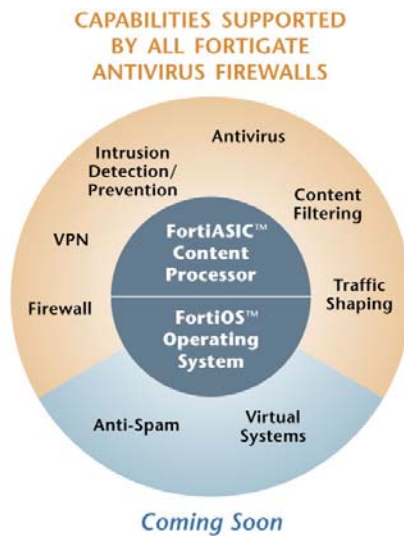
*Wired Equivalent Privacy:* Using WEP, communications between mobile terminals and access points are scrambled using a symmetrical encryption technique called RC4 on the data link layer. This prevents eavesdropping and also prevents unauthorized access by users that have not been configured with the necessary encryption key. WEP offers both 40-bit and 128-bit encryption strengths; however, WEP suffers from a number of drawbacks. For example, as with the SSID, all users within a service area have the same encryption key; if one user's encryption key is compromised the entire network is jeopardized. Moreover, unless the highest strength (128-bit) is used, WEP can be decrypted within a few hours, and many of the initial WLAN access points and interface cards shipping do not support 128-bit encryption.

Another important area of concern for wireless LANs is protection against content-based attacks. Wireless LAN users who are browsing the Internet can be exposed to viruses and worms in Web (HTTP) downloads and applications that are not scanned by conventional firewalls or email-based antivirus software. To prevent these attacks, real-time antivirus scanning at the network gateway should be applied at all WLAN access points to prevent infection and rapid spread of content-based attacks.

## **Fortinet Wireless LAN Security Solutions Provide Real Time Network Protection**

FortiGate Antivirus Firewalls are based on a groundbreaking architecture designed specifically to deliver application-layer security and content processing services in

addition to network-layer services in real time. All models in the 10-member FortiGate product family employ Fortinet's unique FortiASIC™ content processing chip and the powerful, secure, FortiOS™ operating system to achieve breakthrough price/performance. The unique, 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 wireless LANs. FortiGate systems can be deployed in conjunction with wireless access points from any vendor, and used to detect and eliminate content-based threats from email and Web traffic such as 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.

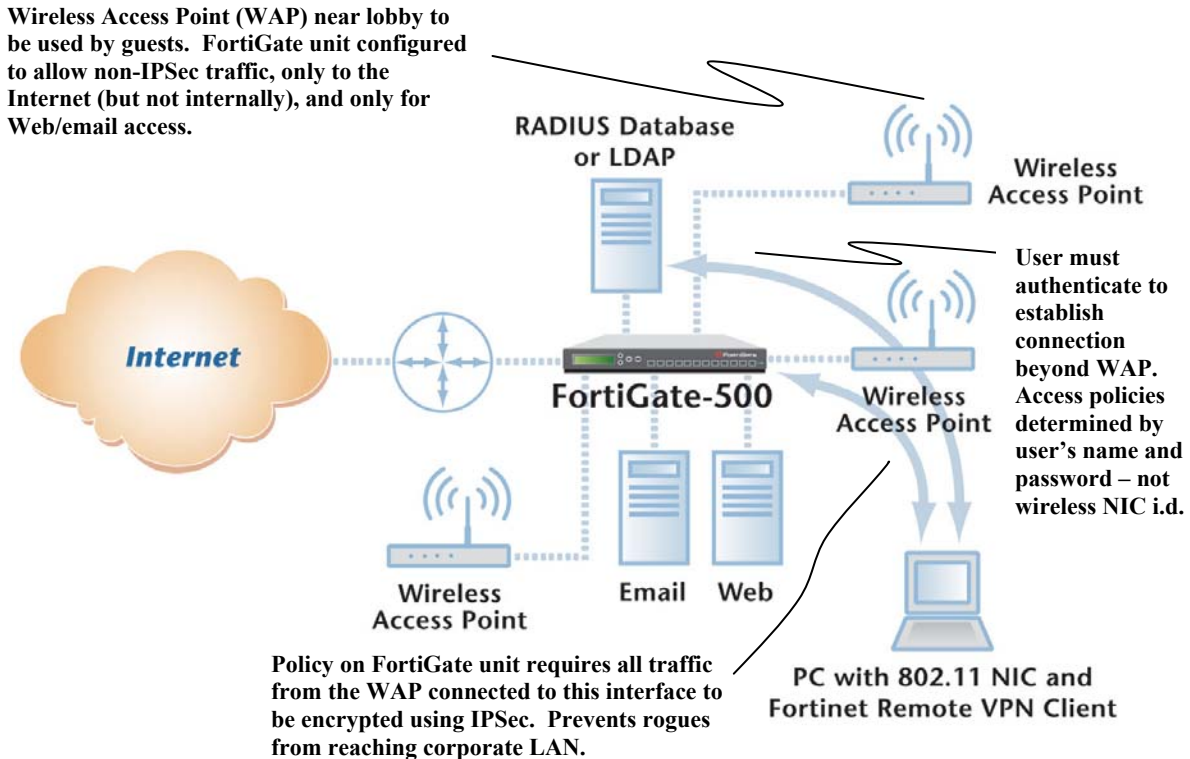
In particular, the VPN encryption, user authentication and directory integration capabilities of FortiGate systems make it possible to mitigate the security weaknesses of current generation WLAN products and to retrofit complete, high-performance security into any WLAN deployment.

The FortiGate platform uniquely solves key issues and concerns currently holding back rapid adoption of wireless LANs in the enterprise, including:

<b>Security Problem with WLAN Deployment . . .</b>	<b>Addressed by the FortiGate Platform</b>
No native support to enable a wireless access point to distinguish an employee's WLAN NIC from that of a friendly visitor or malicious rogue . . .	User-level authentication and user/group policies that enable, for example, employees to have access to specific data resources and services, provides Internet access to guests for mail and Web access only, and denies service to rogues
Limited support for directory integration . . .	User authentication through internal database, Radius server or LDAP directory
No native support for terminal device authentication . . .	IP/MAC binding to enable physical authentication of access terminals
Weakness of WEP encryption . . .	Strong encryption and authentication of wireless links using IPSec VPN with a choice of triple-DES and AES encryption, and SHA1 or MD5 for packet-level authentication
No built in mechanism to detect or stop content-based attacks such as virus scanning, script filtering and intrusion detection/prevention . . .	Complete wireless network protection with AV, intrusion detection/prevention and content filtering
No native support for QoS to ensure appropriate allocation of shared wireless bandwidth . . .	Policy-based traffic shaping to allocate bandwidth based on user identity and type of application

## **Fortinet Wireless LAN Security Deployment**

FortiGate Antivirus Firewalls deploy easily in conjunction with existing WLAN systems and enterprise directory systems. The 10-member FortiGate family includes units that are cost effective for SOHO/telecommuter deployment, branch offices and large-scale, multi-gigabit applications. A typical enterprise application is shown below.



## **Conclusion**

Wireless LANs provide a tremendous amount of freedom and flexibility and support the increasing desire for always-on, always-available connectivity. 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 untethered connectivity without compromising security. Fortinet’s FortiGate family of Antivirus Firewalls add a critical layer of protection to wireless LANs, extending the life and improving the security of existing systems and providing a foundation for expanded implementations even as wireless standards evolve and mature.

## **For More Information**

Please visit our web site at [www.fortinet.com](http://www.fortinet.com) or email us at [info@fortinet.com](mailto:info@fortinet.com)