

AirTight

NETWORKS

WLAN Security— Why Your Firewall, VPN, and IEEE 802.11i Aren't Enough to Protect Your Network

| 339 N. Bernardo Avenue, Suite 200 • Mountain View, CA 94043
| www.airtightnetworks.net

The Importance of Proper Planning and Security Monitoring for Voice over Wi-Fi Networks

Executive Summary

Wireless Local Area Networks based on the IEEE 802.11 standard (also called 'Wi-Fi', and referred to as 'WLAN' in this white paper) have proliferated in enterprises, homes, and public places. IEEE 802.11 a, b, and g are now considered as a de facto standard for WLANs. Embedding of wireless technology into laptops, personal digital assistants (PDAs), and phones has significantly increased the user base of WLAN devices. It is anticipated that majority of the laptops and notebook computers will have embedded WLAN capability. In addition, the mobile user base is anticipated to grow manifold in the coming years with many of them being WLAN users.

While WLANs are known for convenience, flexibility, productivity, and low cost, enterprise networks are vulnerable due to security threats posed by the presence of these devices, irrespective of whether the enterprise has an officially deployed WLAN or not. Conventional firewalls, VPNs, and security mechanisms in the 802.11 standard are unable to alleviate these threats. This white paper describes these new security threats from WLANs and desirable features of a new type of security system—a Wi-Fi Firewall—to prevent them.

A New Class of Security Threats to Enterprise Networks

The prevailing model of enterprise network security is rooted in the axiom that being "physically inside is safe and outside is unsafe". Connecting to a network point within the enterprise premises is generally considered safe and is subject to weaker security controls. On the other hand, tight security controls are enforced at the network traffic entry and exit points using firewalls and Virtual Private Networks (VPNs).

A WLAN breaks the barrier provided by the building perimeter as the physical security envelope for a wired network. This is because invisible radio signals used by the WLAN cannot be confined within the physical perimeter of a building, and usually cut through walls and windows. This creates a backdoor for unauthorized devices to connect to the enterprise network. Some specific security threats from WLANs are described below.

Rogue APs: WLAN Access Points (APs) are inexpensive, easy to install, and small enough to be carried by a person. Unauthorized WLAN APs can be connected to an enterprise network unwittingly or with malicious intention without the knowledge of the IT administration. All it takes is to carry the device inside the enterprise premises, and connect it to an Ethernet port on the network.

Since Rogue APs are typically deployed by employees looking for quick wireless access, they are usually installed without any WLAN security controls (such as Access Control Lists, Wired Equivalent Protocol, 802.1x, 802.11i etc). As they can be connected to virtually any Ethernet port on the network, they can bypass existing WLAN security control points such as Wi-Fi switches and firewalls. The radio coverage of Rogue APs cannot be confined within the building perimeter of the enterprise. Unauthorized users can now connect to the enterprise net-



The Importance of Proper Planning and Security Monitoring for Voice over Wi-Fi Networks

work through these Rogue APs using their radio spillage. The invisibility of wireless medium makes it difficult to prevent this undesirable activity.

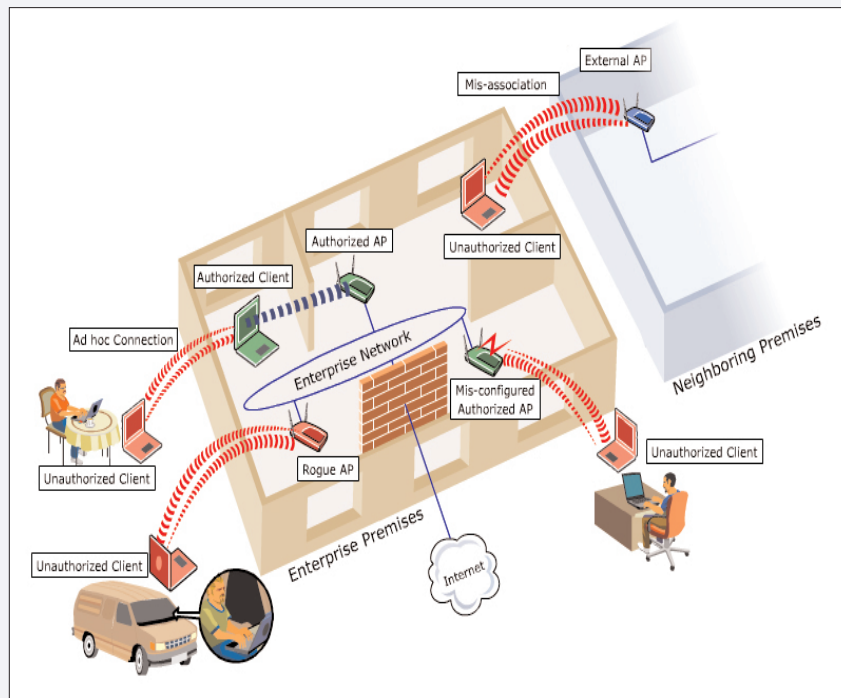
Mis-configured APs: APs support a variety of security features and configuration settings. In many cases, the IT administration may have left the authorized APs to their factory default setting or may not set the configuration properly. This may result in no encryption

or a weak form of encryption such as WEP on the wireless link. It is also possible that the AP does not perform any authentication on the client devices seeking to connect to it, and hence the enterprise network, over the wireless link.

Mis-configured APs can pose a variety of security threats. For example, intruders can eavesdrop on the wireless communication between a mis-configured authorized AP and an authorized client in the enterprise WLAN. The intruder can read this communication if encryption is weak. If the mis-configured AP does not perform proper authentication of clients, the unauthorized user will be able to connect to the enterprise network through this AP. A recent hacking fad, called 'war-driving', involves using freely available tools on the Internet to discover and publicize APs whose signals spill in public places. Various reconnaissance tools such as Netstumbler, Wellenreiter, and others are freely available on the Internet.

Soft APs: With client cards and embedded WLAN radios in PDAs and laptops, a threat called 'soft AP' is on the rise. A soft AP functions as an AP under software control and can be lunched inadvertently or through a virus program; unauthorized users can now connect to the enterprise network through soft APs using their radio spillage.

MAC Spoofing: APs in a WLAN transmit beacons (or probe responses) to advertise their presence in the air. The beacons of an AP contain information about its MAC address, which is its identity, and SSID, which is the identity of the network it supports. Wireless clients listen to beacons from different APs in the vicinity. Clients typically connect to an AP that advertises



New Security Threats from WLAN

The Importance of Proper Planning and Security Monitoring for Voice over Wi-Fi Networks

the desired SSID and transmits a strong beacon signal. A number of WLAN AP models available in the market allow their MAC addresses and SSIDs to be user defined. APs as well as many software tools are also available that enable setting of MAC addresses and SSIDs of AP devices to virtually any user defined values.

In MAC Spoofing, the attacker programs the AP to advertise exactly the same identity information as that of the victim AP. A MAC spoofing AP can also launch disruptive attacks such as packet dropping and packet corruption and modification. A MAC Spoofing AP can even connect to the wired enterprise network as a Rogue AP and evade detection by conventional site survey tools.

A MAC Spoofing AP can lure authorized wireless clients in the enterprise WLAN into establishing a connection and providing confidential information to it. It can insert itself as a man-in-the-middle (described in more detail in the next paragraph) of an authorized communication.

Honeypot APs: Multiple wireless networks can coexist in the same space enabling users to connect to any available network, whether it is one's own network or some other network in the vicinity with overlapping radio coverage. This feature can be exploited by intruders who can set up an unauthorized wireless network with overlapping radio coverage with the enterprise wireless network. It requires powering on an AP in the vicinity (e.g. street or parking lot) of the enterprise wireless network. These APs can attract authorized enterprise clients into connecting to them by transmitting a stronger beacon signal and MAC spoofing. Such APs are called 'Honeypot' APs or 'Evil Twins'. An authorized user unwittingly connecting to a Honeypot AP creates security vulnerability by inadvertently providing sensitive information such as its identity to the Honeypot AP. The intruder can also act as a man-in-the-middle of a communication of an authorized client using Honeypot APs.

Authorized wireless clients in the enterprise WLAN can also accidentally connect to non-malicious neighboring APs (called 'client mis-associations'). Nonetheless, this creates security vulnerability as the wireless clients may inadvertently provide confidential information to such APs. This can happen due to mis-configuration on clients and/or on neighboring APs.

Denial of Service: WLANs are being increasingly entrusted with carrying mission-critical applications such as database access, VoIP, e-mail and Internet access. These applications can be disrupted with a DOS attack causing network downtime, user frustration, and loss of productivity.

As 802.11 WLAN transmissions are a shared medium, they are easily susceptible to DOS attacks. Additionally, 'soft spots' in the 802.11 MAC protocol can be easily exploited to launch DOS attacks. To name a few, DOS attacks such as authentication, association, de-authentication or disassociation flood, NAV attack, CTS flood, and EAP and EAPOL message floods are easy to launch and have the potential of bringing down the entire enterprise WLAN. Unfortunately, a variety of DOS tools are freely available on the Internet including AirJack, FataJack, Void11 and Fake AP

The Importance of Proper Planning and Security Monitoring for Voice over Wi-Fi Networks

Ad Hoc Networks: The 802.11 WLAN standard has provisions for establishing peer-to-peer wireless connections between wireless clients. The wireless clients can therefore form an ad hoc network among themselves using this provision. However, the ad hoc networks can create security vulnerability. For example, an intruder on the street, parking lot, or neighboring premises can form a peer-to-peer ad hoc wireless connection with an authorized laptop in the enterprise premises. The intruder can then launch security attacks on the laptop using this wireless connection. For example, if the laptop has a setting to share certain resources (files, directories, etc.) with other authorized laptops in the enterprise, the intruder can also get access to these resources over the ad hoc wireless connection.

The seriousness of threats to enterprise network security from Rogue APs, Mis-configured APs, Soft APs and ad hoc networks cannot be underestimated. Unauthorized devices connecting to the enterprise network through such APs can engage in data theft, data rerouting, data corruption, impersonation, denial of service, virus injection, and many other types of attacks on the computer systems in the (wired) enterprise network. This vulnerability exists in organizations that have official WLAN deployments, as well as those which have banned wireless on their premises.

Protecting Enterprise Networks from WLAN Threats

The emergence of WLANs has created a new breed of security threats to enterprise networks, which cannot be mitigated by traditional firewall technologies and VPNs. The firewall is similar to a lock on the front door to block unauthorized wired traffic from reaching the internal trusted enterprise network. A VPN protects enterprise data traveling beyond the boundaries of the enterprise network into the public Internet. However, these technologies as well as the encryption and authentication mechanisms such as WEP, WPA, 802.1x, and 802.11i cannot plug the security holes created by Rogue APs, Mis-configured APs, and Soft APs. Conventional enterprise network security systems are not designed to detect and prevent threats from MAC spoofing, Honeypots, DOS, and ad hoc wireless networks.

A new security solution called Wi-Fi Firewall is therefore needed that:

- Monitors the wireless activity within and in the vicinity of the enterprise premises.
- Classifies WLAN transmissions into harmful and harmless.
- Prevents transmissions that pose a security threat to the enterprise network.
- Locates participating devices for physical remediation.

The Wi-Fi Firewall comprises of wireless sensor devices for wireless monitoring that are placed

The Importance of Proper Planning and Security Monitoring for Voice over Wi-Fi Networks

spatially to cover the enterprise premises. These sensors keep a constant vigil on the 'enterprise air' and create an RF shield to alleviate security threats from WLANs.

The five key features of the Wi-Fi Firewall are planning, detecting, classifying, protecting, and locating. These features are described below.

1. Planning WLAN RF Coverage:

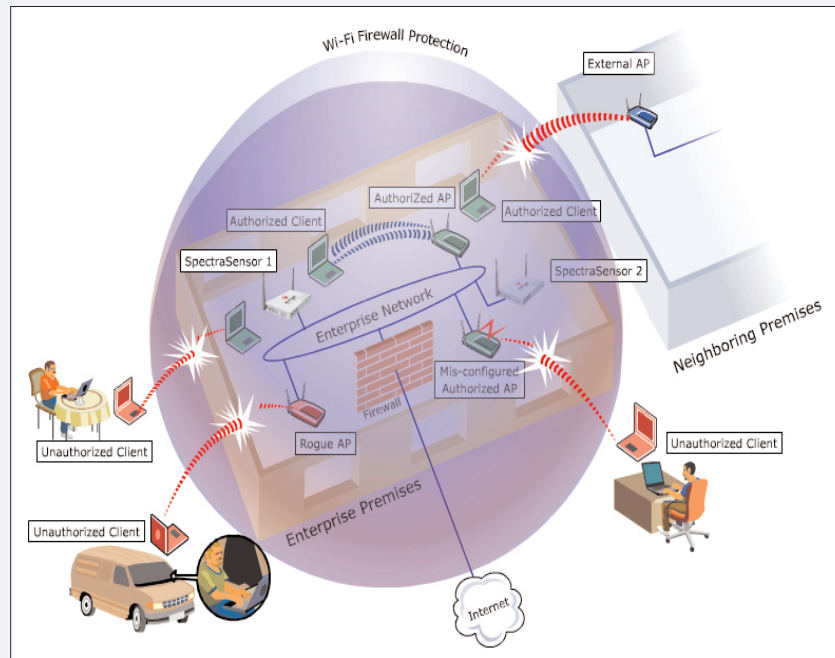
The spatial layout as well as materials within the enterprise

(walls, columns, windows, furniture, etc.) interacts with the radio coverage of the sensor in a complex way creating a gap between rule-of-thumb for placing APs and reality. A systematic, scientific, and scalable RF planning process is therefore required for determining the right placement of access points and wireless sensors. This process must account for the spatial layout of the premises and indoor RF signal propagation characteristics. This ensures that there are no holes in the Wi-Fi Firewall coverage through which undesirable wireless activity can go unabated.

2. **Detecting WLAN Transmissions:** The Wi-Fi Firewall needs to scan radio channels and capture any wireless activity detected on these channels using spatially distributed sensors. It is necessary to scan all the channels in the 2.4 GHz (b, b/g) and 5 GHz (a) band. It needs to analyze, aggregate, and correlate information reported by different sensors.

3. **Classifying WLAN Transmissions:** With increasing penetration of WLANs, there is a need to accurately and automatically sort harmful activity from the harmless activity in the shared wireless medium. For example, in organizations with no official WLAN deployment, either any wireless activity detected in the air is due to a Rogue AP or it could be emanating from an external (neighbor's) WLAN. The Wi-Fi Firewall must categorize it accordingly. In organizations with official WLAN infrastructure, the Wi-Fi Firewall must be able to differentiate between authorized, rogue, and external wireless activities.

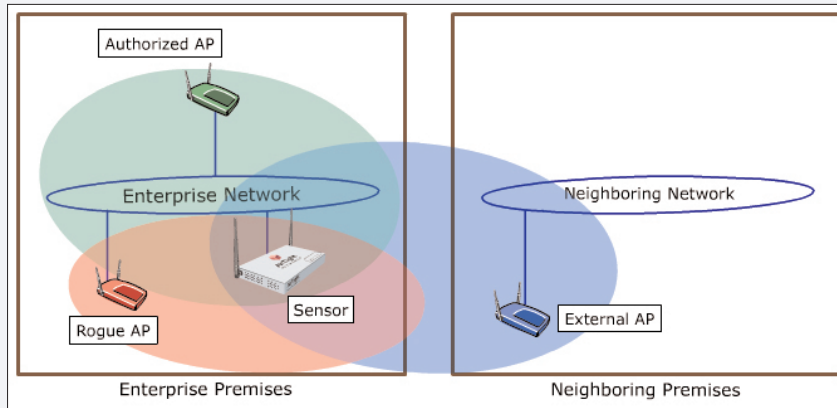
This type of classification minimizes annoying false alarms and volumes of irrelevant alerts from the security standpoint, both of which make the security system unusable. The automat-



Wi-Fi Firewall Protection

The Importance of Proper Planning and Security Monitoring for Voice over Wi-Fi Networks

ic classification also facilitates automatic intrusion prevention as described in the following paragraph.



Classification of WLAN Transmission

4. Protecting Against Intrusion: The Wi-Fi Firewall must automatically and instantaneously block harmful wireless activity detected by its wireless sensors until remediation. For example, the Wi-Fi Firewall must block any client from connecting to a Rogue AP or a MAC spoofing AP, prohibit formation of ad-hoc networks, and mitigate any type of DOS attack. Further, it must block harmful wireless activity until physical remediation has taken place.

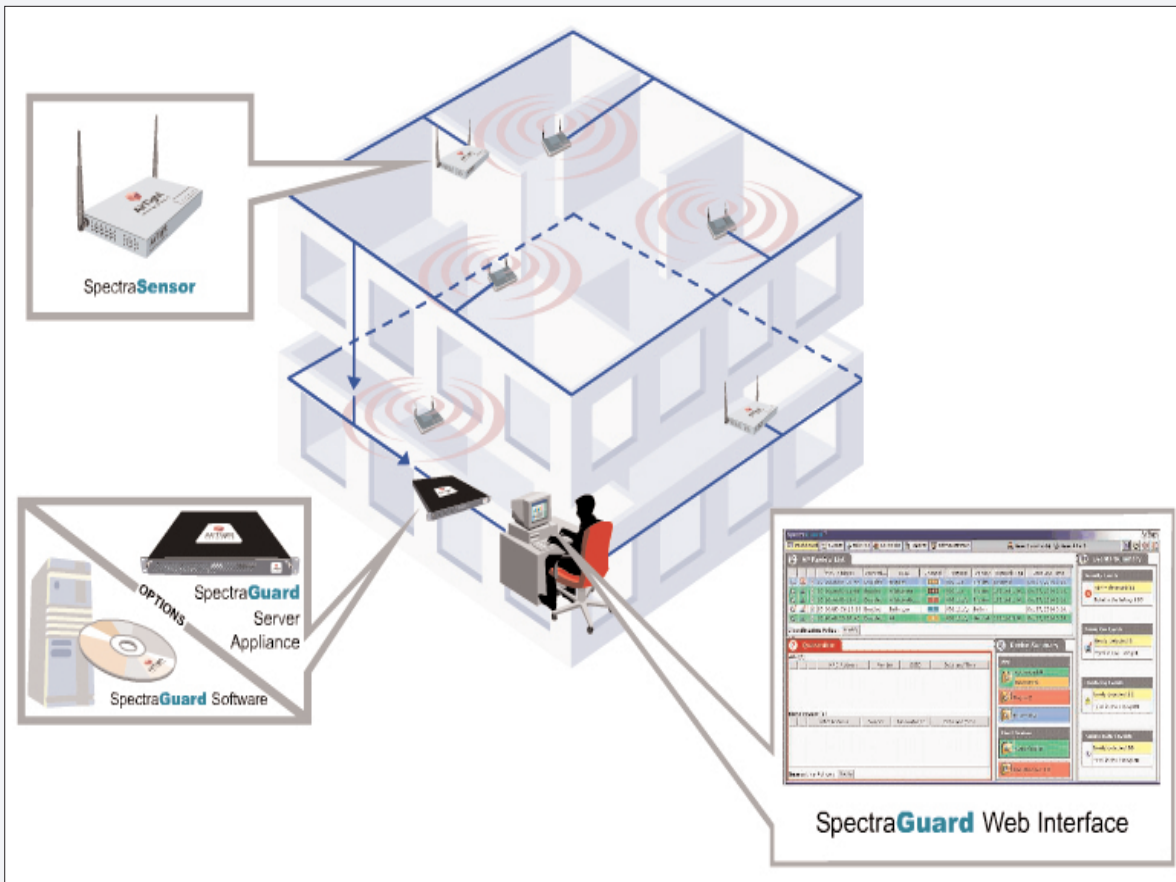
Prevention of harmful WLAN transmission must be carried out with surgical precision without disturbing legitimate WLAN activities. It should not bring down the entire wireless network like some brute force methods such as radio jamming would do. The prevention should also be reliable to minimize false alarms and block every single unauthorized activity.

5. Locating WLAN Devices: Physical remediation i.e. disconnecting and powering off the WLAN device(s) taking part in harmful activity requires knowledge of the physical location of these devices. The Wi-Fi Firewall must provide the location co-ordinates of such a device inside and around the perimeter of the enterprise premises. There should be no need for any specialized client side software or hardware.

SpectraGuard: Industry's First Wi-Fi Firewall

SpectraGuard from AirTight Networks is the industry's first comprehensive Wi-Fi Firewall that effectively tackles security threats from WLANs. SpectraGuard provides RF planning, detection, accurate classification automatic prevention, and location tracking. It comprises an overlay network of RF sensors, called SpectraSensors that are dedicated to the monitoring of wireless activity in the enterprise air. The SpectraSensors communicate with a centralized high availability SpectraGuard Server. This client-server architecture is well suited for medium to large enterprise installations. The system architecture of SpectraGuard is illustrated below.

The Importance of Proper Planning and Security Monitoring for Voice over Wi-Fi Networks



SpectraGuard System Architecture

Summary

1. WLANs are being rapidly adopted due to the convenience and flexibility they provide. However, WLANs create a new set of security threats to enterprise networks such as Rogue APs, Mis-configured APs, Soft APs, MAC Spoofing, Honey-pot APs, DOS, and Ad hoc Networks.
2. Neither traditional firewalls and VPNs nor IEEE 802.11 security standards such as WEP, WPA, 802.1x, and 802.11i can protect enterprise networks against over-the-air attacks from WLANs.
3. A new and comprehensive security solution in the form of a Wi-Fi Firewall is required to alleviate these new security threats. The Wi-Fi Firewall must be able to provide RF planning, detection of RF activity, accurate classification of WLAN networks, automatic and reliable prevention from harmful WLAN transmissions, and precision location tracking of WLAN devices.
4. The SpectraGuard solution from AirTight Networks is industry's first comprehensive Wi-Fi Firewall that can effectively protect enterprise networks against over-the-air attacks from WLANs.