5 Practical Steps to Secure Your Wireless LAN

The mobility and productivity benefits of 802.11 wireless local-area networks do not have to put your information assets at risk. While the many risks associated with wireless LANs have made headlines in the last year, security conscious enterprises are deploying secure wireless LANs by implementing a few practical steps to protect their information assets, identify vulnerabilities, and protect the network from wireless-specific attacks.

Overview of Wireless LAN Risks

The benefits of 802.11 wireless LANs are easy to see from the mobility of untethered workers connecting to the network from a conference room, retailers easily running cash registers throughout a store, or manufacturers wirelessly connecting operations throughout a plant. However, the risks of wireless LANs are still being identified as hackers become more familiar with the technology and develop more creative ways to compromise wireless security.

5 Practical Steps for Securing WLANs

1 Discovery & Vulnerability Assessment
2 Access Point Security
3 Encryption & Authentication -- VPN
4 Security Policy Enforcement
5 Intrusion Protection

Over the last year, analysts and media have documented and publicized vulnerabilities of wireless LANs that have been identified, such as encryption that can be broken and rogue access points that allow anyone within 1,000 feet to access your network.

> *Networks Without a Safety Net*
>
> – **InformationWeek, June 2002**

> *Holes Expose Retail Data … White-hat hackers last week discovered vulnerabilities in the wireless networks of two major retailers—holes that they claimed exposed data that appeared to include customer information.*
>
> – **Computerworld, May 2002**

> *Wireless LAN Install Leaves Corporate Nets Wide Open*
>
> – **Computerworld, May 2002**

> *Researchers Crack New Wireless Security Specs*
>
> – **InfoWorld, February 2002**

> *At least 20 percent of enterprises already have rogue WLANs attached to their corporate networks, installed by users looking for convenience of wireless and unwilling to wait for the IS organization to take the lead.*
>
> – **Gartner Group, August 2001**

These reports focus on breaking encryption, the risk of unauthorized access points connected to the wired network, and the failure of enterprises to incorporate security into their wireless LANs. However, network and security managers must be aware of all wireless risks as they develop, including:

Ad hoc networks – Peer-to-peer wireless networking between laptops without an access point opens up a laptop to be directly attacked and used as a conduit to the network.

Policy violations – Authorized users who violate network policies against rogue access points, file sharing, and turning off security measures circumvent your investment in network security.

Identity theft – Intruders can pick off Service Set Identifiers (SSIDs) and Media Access Control (MAC) addresses to steal the identity of an authorized user.

Man-in-the-Middle attacks – Hackers can force a rogue station between an authorized station and an access point where all traffic between the authorized station and access point is routed through the rogue station.

Denial-of-Service – Outsiders who cannot gain access to a WLAN can none-the-less pose security threats by jamming or flooding the airwaves with static noise that causes WLAN signals to collide or simply force stations to continuously disconnect from access points.

> *Wireless LANs are a breeding ground for new attacks because the technology is young and organic growth creates the potential for a huge payoff for hackers.*
>
> – **Pete Lindstrom, Hurwitz Group, Sept. 2002**

Wireless LAN Security

The attention on the pitfalls of wireless LANs has inspired some enterprises to ban wireless LANs altogether. However, security conscious enterprises are fortifying their wireless LANs with a layered approach to security that includes: 1.) Discovery of rogue access points and vulnerabilities; 2.) Access point security; 3.) Encryption & authentication (which may include a virtual private network); 4.) Establishment and enforcement of wireless network policies; and 5.) Proactive security with intrusion protection.

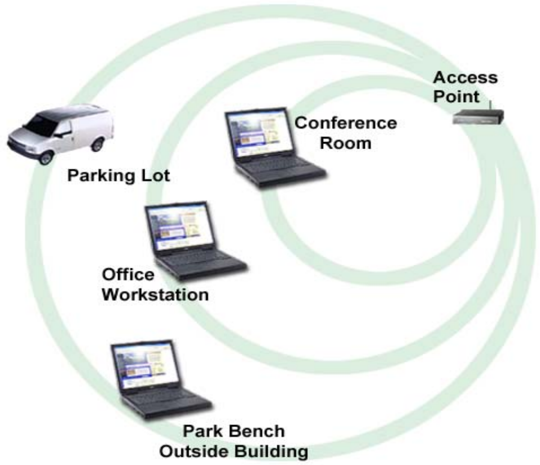
1. Discovery of Rogue Access Points & Vulnerabilities

The basis for all wireless LAN security should start by understanding the environment in which your wireless LAN operates.

Because a simple wireless LAN can be easily installed by attaching a $150 access point to a wired network and a $70 wireless LAN card to a laptop, employees are deploying unauthorized WLANs when IT departments are slow to adopt the new technology. These rogue access points generally lack standard security and thus circumvent an enterprise's investment in network security.

The same insecurity can come from network vulnerabilities originating from improperly configured wireless LANs. Upon a power surge or after a power failure, some access points restart in their default modes that do not include encryption, authentication, or other security measures with which they were configured.

Neighboring wireless LANs located in the same vicinity as your wireless LAN also pose risks of the neighboring stations accessing your network and interfering on wireless channel.



Discovery of rogue access points and vulnerabilities can be accomplished with two approaches: 1.) Physically walking the network area with scanners; or 2.) Statefully monitoring the wireless LAN with remote sensors.

Freeware, such as Netstumbler and Kismet, and other commercial scanners can survey the airwaves for rogue access points and some network vulnerabilities. This process requires a network administrator to physically walk through the wireless LAN coverage area for the scanner to pick up data that the network administrator interprets to identify all access points and wireless LAN traffic. The network administrator then sorts through the access points to determine which are unauthorized and analyzes the wireless LAN traffic to determine if the network is properly configured without interference from other networks.

A September 2002 research brief from META Group questioned the viability of scanners.

> *Current radio frequency scanning tools such as Sniffer Wireless and AirMagnet are limited in their ability to perform scalable and repeatable audits.*
>
> – **META Group, September 2002**

While this process requires the physical presence and valuable time of a network manager, the effectiveness is limited because it only samples the airwaves for threats. New rogue access points and other vulnerabilities can arise after a scan and will not be detected until the next time a network administrator surveys the network.

This approach is particularly unreasonable for enterprises operating dozens of offices around the country or retailers with hundreds of stores. Even if these organizations could feasibly devote a network administrator's full attention to survey each site on a monthly basis, rogue access points and other vulnerabilities can pop up the minute the survey is completed.

Wireless security experts recommend 24x7 monitoring of the airwaves to discover rogues access point and identify network vulnerabilities as they happen. AirDefense's distributed architecture with remote sensors placed in proximity of wireless LANs enables AirDefense to statefully monitor wireless LAN traffic to discover these security risks the minute they arise.

2. Lock Down All Access Points

The next step of wireless LAN security involves the basics of configuring all access points to implement the best practices of wireless LAN security and requires little or no additional cost other than a little time and effort.

> *A firewall costing thousands of dollars can be completely compromised by a single incorrectly configured access point, even when the access point is behind a brick wall.*
>
> – **Network Computing, October 2001**

Enterprises should change the default Service Set Identifiers (SSIDs), which are essentially the names of each access point. Cisco access points come with the default SSID of "tsunami", Linksys defaults to "linksys," and both Intel and Symbol access points default to "101." These default SSIDs alert hackers to vulnerable wireless LANs.

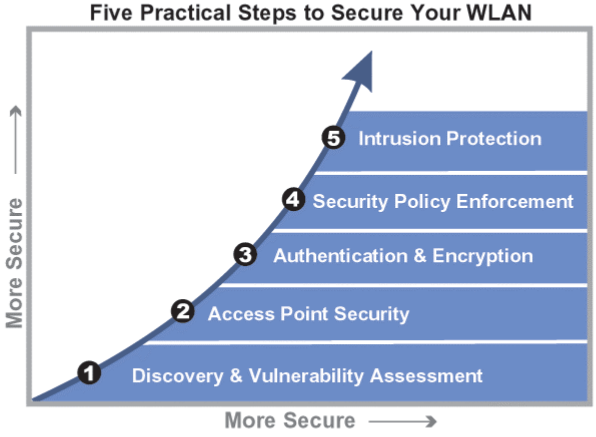
The SSIDs should be changed to names that are meaningless to outsiders. An SSID of "CEO Office" or "East Cash Register" only calls attention to valuable information that a hacker would like to get into.

Enterprises should also configure access points to disable the broadcast mode where the access point constantly broadcasts its SSID as a beacon in search for stations with which to connect. By turning this default feature off, stations must know the SSID in order to connect to the access point.

Most enterprise-class access points allow you to limit which stations can connect to it based on filtering of Media Access Control (MAC) addresses of authorized stations. While this is not foolproof, MAC address filtering provides basic control over which stations can connect to your network. Larger enterprises with more complex wireless LANs that allow hundreds of stations to roam between access points may require more complex filtering from remote authentication dial-in service (RADIUS) servers.

To eliminate the threat of intruders connecting to your wireless LAN from the parking lot or the floor above you where connection speeds will be greatly reduced, access points should be configured to not allow the slower connection speeds.

Five Practical Steps to Secure Your WLAN


5 Intrusion Protection
4 Security Policy Enforcement
3 Authentication & Encryption
2 Access Point Security
1 Discovery & Vulnerability Assessment
More Secure
More Secure

3. Encryption & Authentication – VPN

Encryption and authentication provide the core of security for wireless LANs. However, fail-proof encryption and authentication standards have yet to be implemented.

In 2001, researchers and hackers demonstrated their ability to crack Wired Equivalency Policy (WEP), the standard encryption for 802.11 wireless LANs. Soon after, hackers published freeware tools, such as WEPCrack, which allow anyone to crack the encryption after observing enough traffic over the network to figure out the encryption "key." WEP comes in two variations with 64-bit keys and 128-bit keys. While the longer key takes longer to crack, both remain vulnerable.

After reports showed the vulnerability of WEP and standard authentication, many enterprises were discouraged from implementing WEP into their wireless LAN deployments, which left their networks totally exposed.

Electronics retailer Best Buy Co. ran into trouble in the spring of 2002 when customers who had purchased wireless LAN cards from Best Buy installed the cards in their laptops before they left the parking lot. The customers noticed unencrypted wireless LAN traffic that contained customer information and possibly credit card numbers. The Best Buy case gives an example of why enterprises should at a minimum encrypt their wireless LAN traffic with WEP.

> *By year-end 2002, 30 percent of enterprises will suffer serious security exposures from deploying WLANs without implementing the proper security.*
>
> – **Gartner Group, August 2001**

With authentication vulnerabilities stemming from WEP, the wireless LAN standards group introduced 802.1x as strengthened authentication for all 802.11 networks. However, 802.1x also has shown to be vulnerable to hackers. (See "An Initial Security Analysis of the IEEE 802.1X Standard" a paper by University of Maryland professor William Arbaugh.)

Because these encryption and authentication standards are vulnerable, stronger encryption and authentication methods should be deployed to more completely secure a wireless LAN with wireless virtual private networks and RADIUS servers.

VPNs can employ strong authentication and encryption mechanisms between the access points and the network, and RADIUS systems can be used to manage authentication, accounting, and access to network resources.

While VPNs are touted as a secure solution for wireless LANs, one-way authentication VPNs are still vulnerable to exploitation. Deployment of wireless LANs in large organizations can create a nightmare of distributing and maintaining client software to all clients. One-way authentication VPNs are also vulnerable to Man-in-the Middle attacks and a number of other known attacks. Mutual authentication wireless VPNs offer strong authentication and overcome weaknesses in WEP.

Despite these vulnerabilities, encryption and authentication remain essential elements of wireless LAN security.

4. Set & Enforce Wireless LAN Policies

Every enterprise network needs a policy for uses and security. Wireless LANs are no different. While policies will vary based on individual security and management requirements of each wireless LAN, a thorough policy – and enforcement of the policy – can protect an enterprise from unnecessary security breaches and performance degradation.

Wireless LAN policies should begin with the basics of forbidding unauthorized access points and ad hoc networks that can circumvent network security. Because many security features, such as the use of WEP or VPNs and open broadcast of SSIDs, are controlled on the access points and stations, policies should be in place to forbid the reconfiguration of access points and wireless LAN cards to alter these features.

Wireless LAN security is greatly increased with policies that limit wireless LAN traffic to operate on set channels, at connection speeds of 5.5 Mbps and 11 Mbps, and only during select hours. By establishing a set channel for each access point, all traffic on the other channels can be identified as suspicious activities. A policy that all stations connect at the higher speeds protects a wireless LAN from intruders in the parking lot or neighboring office who are likely too far away to connect at 5.5 Mbps and 11 Mbps. A policy that limits wireless LAN traffic to select hours of operation protects a network from late night attacks of an intruder in the parking lot connecting to the network or an unscrupulous employee sending sensitive files from the wired network to a wireless network while no one else is around.

In addition to securing a wireless LAN, policies can assist in the overall performance of wireless LANs. Network abuses, such as downloading of MP3 files and playing bandwidth-intensive online games, can drain the performance of wireless LANs and affect everyone on the network. Policies banning such activity boost productivity for everyone on the network.

While policies are necessary, they can be useless paper weights without effective enforcement. Similar to the effective discovery of network vulnerabilities, policy enforcement requires 24x7 monitoring of a wireless LAN. AirDefense provides the stateful monitoring to alert you to policy violations that degrade network performance or put your information assets at risk.

5. Intrusion Detection & Protection

Security mangers rely on intrusion detection and protection to ensure that all components of 802.11 wireless LANs are secure and protected from wireless threats and attacks. While many organizations have already deployed intrusion detection systems for their wired networks, only a wireless LAN-focused intrusion detection system can protect your network from attacks in the airwaves before the traffic reaches the wired network.

The growing number of attacks on wireless LANs is best seen in a study of wireless LAN activity at the DefCon X hacker convention in August 2002. AirDefense surveyed the wireless LAN at the Las Vegas convention for two hours and identified more than 10 previously undocumented wireless attacks from new creative ways in which hackers are learning to manipulate 802.11 protocols to launch new forms of Denial-of-Service attacks, identity theft, and Man-in-the-Middle attacks.

During the two hours monitoring the confernce's wireless LAN, AirDefense identified 8 sanctioned access points, 35 rogue access points, and more than 800 different station addresses. AirDefense's 802.11 security experts estimate that 200 to 300 of the station addresses were fakes because roughly 350 people were in the wireless LAN network room at a single time.

AirDefense discovered 115 peer-to-peer ad hoc networks and identified 123 stations that launched a total of 807 attacks during the 2 hours.

Among the 807 attacks:

- 490 were wireless probes from tools such as Netstumbler, which were used to scan the network and determine who was most vulnerable to greater attacks;
- 190 were identity thefts, such as when MAC addresses and SSIDs were spoofed to assume the identity of another user;
- 100 were varying forms Denial-of-Service attacks that either (1) jammed the airwaves with noise to shut down an access point, (2) targeted specific stations by continually disconnecting them from an access point, or (3) forced stations to route their traffic through other stations that ultimately did not connect back to the network; and
- 27 attacks came from out-of-specification management frames where hackers launched attacks that exploited 802.11 protocols to take over other stations and control the network.

> *The wireless LAN at DefCon was probably the best place to learn about these new attacks and threats to wireless LANs because DefCon is one of few places where the focus is on breaking things. Enterprises should be aware of these threats and learn what they can do to combat them.*
>
> – **Pete Lindstrom, Hurwitz Group, September 2002**

AirDefense provides the industry's only wireless LAN intrusion detection and protection system. By statefully monitoring the airwaves and analyzing all wireless LAN traffic before it reaches the wired network, AirDefense identifies and responds to these continuously developing wireless attacks.

5 Practical Steps Summary

Practical security measures can overcome the risks and threats associated with wireless LANs. AirDefense can assist enterprises with the three of the five steps: 1.) Discovery of rogue access points and vulnerabilities; 4.) Enforcement of wireless LAN policies; and 5.) Intrusion protection and detection.

For more information about AirDefense, please read the following section that focuses exclusively on AirDefense.

The AirDefense Solution

AirDefense provides the industry's only security appliance for wireless LANs to discover wireless LAN vulnerabilities, enforce security policies, and detect and respond to intruders.

More simply put, AirDefense is a wireless LAN intrusion protection and management system that discovers network vulnerabilities, detects and protects a wireless LAN from intruders and attacks, and assists in the management of a wireless LAN.

AirDefense: (i) Discovers vulnerabilities and threats – such as rogue APs and ad hoc networks – as they happen; (ii) Secures a wireless LAN by detecting intruders and attacks and eliminating those threats; and (iii) Provides a robust wireless LAN management functionality that allows users to understand their network, monitor network performance, and enforce network policies.

Remote Sensors & Server Appliances

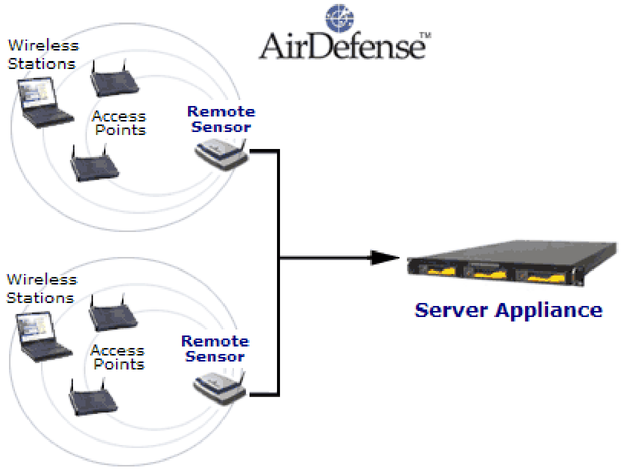
The AirDefense solution consists of distributed sensors and server appliances. The remote sensors sit near 802.11 Access Points to monitor all wireless LAN activities and report back to the server appliance, which analyzes the traffic in real time.

The remote sensors:

- Are deployed near access points;
- Provide 24x7 monitoring of all wireless LAN activities;
- Capture wireless traffic from access points and stations; and
- Report to a back-end server where they are centrally managed.

The server appliances:

- Analyze traffic in real time;
- Discover wireless LANs and rogue deployments;
- Detect intrusions and impending threats;
- Disconnect intruders and protect against attacks;
- Enforce wireless LAN policies;
- Monitor wireless LAN performance and troubleshoot network issues;
- Offer a secure web-based interface; and
- Provide comprehensive reporting.



AirDefense Functionality

The State-Analysis Engine and Multi-Dimensional Detection Engine power AirDefense's core functionality to discover wireless LAN vulnerabilities, protect against intruders and attacks, and manage the wireless network.

Discovery & Vulnerability Assessment

Because new risks can arise with the easy deployment of unauthorized access points or an intruder driving into the parking lot, wireless LANs should be routinely surveyed to track traffic patterns, ensure network fidelity, and identify security vulnerabilities. AirDefense provides and identifies:

- Site Surveys
- Rogue Deployments
- Unauthorized Use
- Security Vulnerabilities

Intrusion Detection & Protection

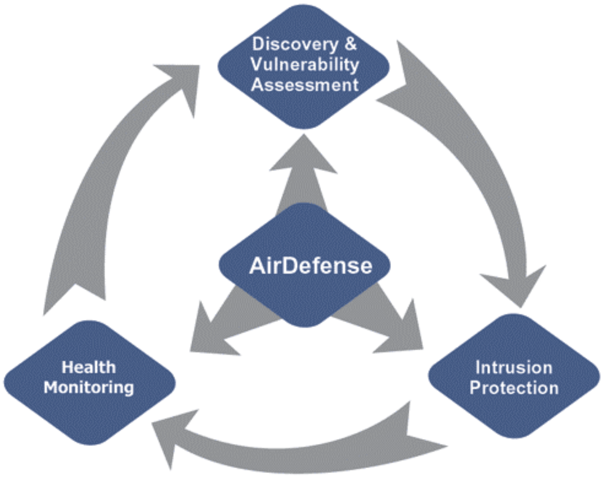
AirDefense provides the greatest level of wireless LAN security with effective measures that include 24x7, real-time monitoring of wireless networks, intrusion detection, attack prevention, and forensic auditing.

By statefully monitoring WLANs in real time, AirDefense provides critical information regarding suspicious or late night activities, unauthorized stations scanning your network, and signal strength; an uncharacteristically weak signal could indicate that a station is accessing the network from the parking lot or other covert location outside the building.

AirDefense is designed to accurately detect:

- Identity theft
- Denial-of-Service (DoS) attacks
- Man-in-the-Middle.

AirDefense recognizes these and other attacks and can be configured to eliminate any threat by disconnecting the intruder or blocking the attacking station from associating with all authorized access points and stations.



AirDefense provides a forensic database to audit a WLAN with a minute-by-minute report on the status of each access point and wireless station. AirDefense documents all information it gathers into a relational database that becomes a source of detailed traffic history. The database can pinpoint which systems were targeted with what type of attack and can provide the play-by-play detail of how the attack occurred and can track if the attacker had previously visited the network for reconnaissance or a prior attack.

Health Monitoring

By constantly monitoring wireless activity, AirDefense provides a comprehensive tool to manage the entire wireless LAN. Network administrators are given a complete survey of the network to troubleshoot problems, make better decisions, and plan for future implantations and upgrades.

AirDefense's wireless LAN health monitoring functionality is based upon:

- Wireless LAN network view & characteristics – AirDefense gives network managers a real-time view of a wireless LAN with detail into network usage and inventory of access points and stations.
- Fault diagnostics – A key management feature includes fault diagnostics that track CRC errors from failed connections, interference from neighboring wireless LANs, network misconfigurations, and a complete history of network and station failures.
- Performance monitoring – Information gathered allows network administrators to monitor performance of wireless LANs by identifying usage characteristics and bandwidth hogs who tie-up the network with capacity-draining activities.
- Capacity planning – With historical data of network usage related to individual access points and the overall wireless LAN, administrators can plan for appropriate network capacity by monitoring network usage over time to make better decisions for adding additional access points or wired-end capacity.

Policies, Alarms & Reports

AirDefense provides network administrators with easy-to-use tools to manage network policies, set alarms, and receive detailed status reports.

The policy manager is used to define, monitor, and enforce business rules for wireless LANs such as off-hours traffic, ad hoc networking, unauthorized channels, open broadcasts of SSIDs, and encryption usage.

The alarm manager intelligently filters and aggregates events to notify management of security threats based upon policy. The relational database provides detailed and summary reports of user information for each access point and mobile station.

For more information, please contact:

AirDefense, Inc.
11475 Great Oaks Way
Suite 200
Alpharetta, GA 30022
www.AirDefense.net
phone: 770.663.8115
email: info@airdefense.NET