Supercharging the Security of Your Cisco Aironet Wireless LAN

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

Application Note: Supercharging the Security of Your Cisco Aironet Wireless LAN

Executive Summary

Wireless LAN security issues were first addressed by Cisco well before new IEEE 802.11i standards were put in place to help enterprises maintain confidence in and productivity gains from their Cisco wireless network. However new Wi-Fi threats endanger not just the wireless LAN, but also the wireline corporate infrastructure, leading Cisco to team with AirTight Networks to deliver a world class wireless intrusion prevention system (IPS) to their Cisco Aironet customers.

Cisco has effectively solved the encryption and authentication security issues between the client and the access point, however, new security holes from Wi-Fi threats have emerged that the current solution does not address. As a Wireless Alliance member of the Cisco Technology Development Partnership Program, AirTight Networks integrates seamlessly with the Cisco Aironet solution extending its useful life and value while maintaining state-of-the art security. This application note will discuss how adding AirTight Networks SpectraGuard Enterprise to your existing Cisco Aironet wireless LAN installation will provide the following capabilities:

- Complete wireless threat identification
- Automatic wireless intrusion prevention against all known wireless threat categories
- Streamlined, calibrated location tracking
- Accurate visualization of RF security coverage and defenses
- Comprehensive compliance reporting for Sarbanes-Oxley, HIPAA, Gramm-Leach-Bliley and DoD 8100.2

Cisco Aironet Wireless Security Measures

With all the positive press and analyst coverage of Cisco Aironet security, you may wonder what the issues are. The Cisco Aironet solution does an excellent job of over-the-air encryption and mutual authentication between the client and network. However, this is just a portion of the security needed to protect today’s enterprises against wireless threats.

Cisco Aironet Access Points combined with an appropriate RADIUS server provide strong over-the-air encryption and mutual authentication between the wireless client and the network as the following Cisco diagram illustrates.

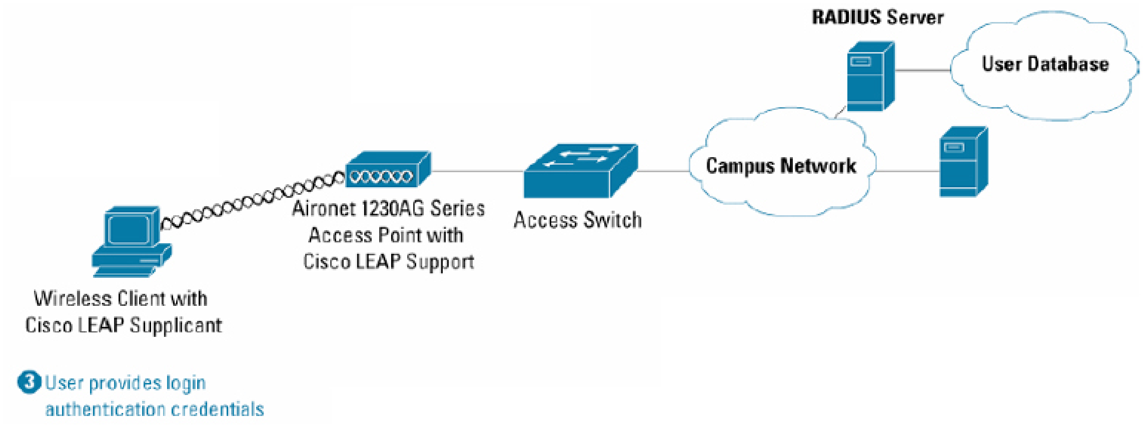
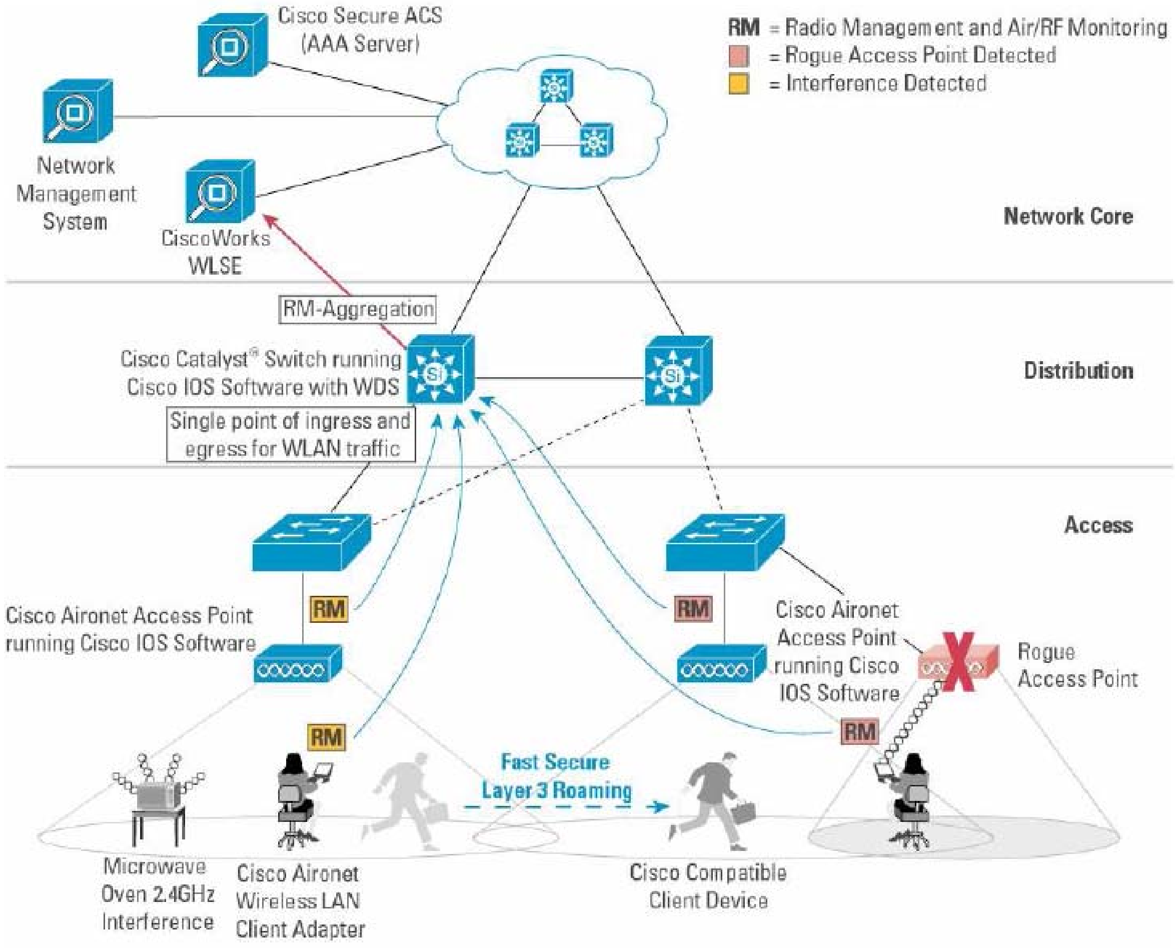

RADIUS Server
User Database
Campus Network
Access Switch
Aironet 1230AG Series Access Point with Cisco LEAP Support
Wireless Client with Cisco LEAP Supplicant
3 User provides login authentication credentials

Figure 1: Over-the-air encryption and strong mutual authentication using IEEE 802.11i built into the Cisco Aironet wireless LAN provide strong protection against eavesdropping or hacking of the encryption key.

With the addition of the Cisco Wireless LAN Solution Engine to the network, the enterprise further enhances security by ensuring that all authorized Cisco access points remain under management control, maintaining up-to-date authorized security and radio policies. In addition, Cisco Access Points can provide the WLSE with a rudimentary ability to detect some, but not all, types of rogue access points. And if the switch network consists of end-to-end Cisco switches, the solution can provide the ability to shut down rogues via wired-side support suppression. A Cisco wireless LAN network with the WLSE is shown below.


Cisco Secure ACS (AAA Server)
RM = Radio Management and Air/RF Monitoring
🟥 = Rogue Access Point Detected
🟨 = Interference Detected
Network Management System
CiscoWorks WLSE
Network Core
RM-Aggregation
Cisco Catalyst® Switch running Cisco IOS Software with WDS
Si
Si
Distribution
Single point of ingress and egress for WLAN traffic
Access
RM
RM
Cisco Aironet Access Point running Cisco IOS Software
Cisco Aironet Access Point running Cisco IOS Software
Rogue Access Point
RM
RM
Fast Secure Layer 3 Roaming
Microwave Oven 2.4GHz Interference
Cisco Aironet Wireless LAN Client Adapter
Cisco Compatible Client Device

1. Clients and Access Points (AP) send their Radio Management (RM) data to the Cisco AP, switch or router running wireless-aware Cisco IOS Software with Wireless Domain Services (WDS).

2. Cisco AP, switch or router running wireless-aware Cisco IOS Software with WDS uses RM-Aggregation to remove redundant RM data received from the access points and client devices. The WDS device then forwards the aggregated data to the CiscoWorks WLSE.

Figure 2: The addition of the Cisco Wireless LAN Services Engine (WLSE) adds additional security capabilities such as protection against certain types of rogue access points. However, it is not a comprehensive solution against the majority of wireless threats.

Security Holes in the Cisco Wireless LAN Solution

While the Cisco Aironet and WLSE solution may look comprehensive, it is lacking in two critical areas. Specifically, the Cisco solution does **NOT**:

- Automatically identify and classify all categories of wireless threats over-the-air. It identifies a subset of the universe of possible rogue access points.
- Use over-the-air prevention to stop wireless threats. Many wireless threats cannot be prevented by shutting down a switch port.

The following explains the dangers of not protecting against these threats in more detail.

Rogue Access Points – More Than Just One Type

Rogue access points are the most well known category of wireless threat. Typically brought in by unknowing employees, they can be plugged into the Ethernet network behind the corporate firewalls and provide an open door to outsiders. What the Cisco solution does not protect against are all types of rogue access points. The following table shows the rogue access point categories and the ones that Cisco Aironet with the WLSE can reliably detect.

Rogue Access Point Type		**Cisco Aironet and WLSE Detection Capabilities**
Bridging Access Point	Non-encrypted	Yes
	Encrypted	No
NATing Access Point	Non-encrypted	No
	Encrypted	No

As you can see from the table above, only one out of the four types of rogue access points are protected against with the Cisco Aironet solution. Most rogue access points are typically the low cost consumer or SOHO versions that employ NATing to support multiple clients. Given this, it is highly likely that the most common type of rogue access point will not be detected at all! If it is connected to the network and is not encrypted, it leaves an open port to the enterprise network for any wireless client within radio range.

Additional Wireless Threats Cisco Does Not Protect Against

The second most common wireless threat is from mis-associated clients. A mis-associated client is an authorized client that connects to a non-authorized access point.

- A sales laptop that connects wirelessly to the Starbucks hot spot next door.
- A marketing laptop that connects wirelessly to a Linksys access point in the same office park.

This can happen quite easily in environments where Windows XP laptops with wireless clients are plugged into docking stations to directly connect to the Ethernet network. In this scenario, the wireless client will still be on unless actively disabled by the user. Windows XP will search for the strongest wireless signal. At the same time, wireless signals from external, neighboring access points can broadcast within the building, and if the client connects, provide a direct link into the corporation's wireline network. Unauthorized users or malicious hackers can now access confidential information.

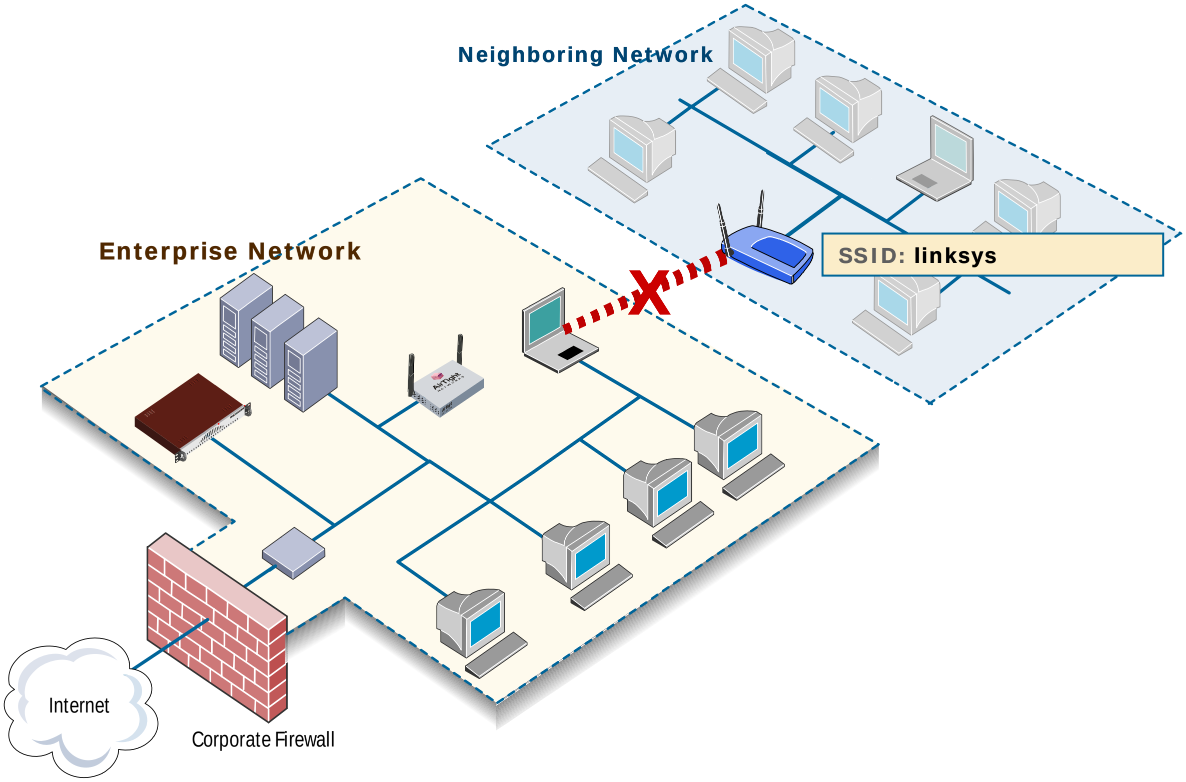


Figure 3: A mis-associated client can provide a direct link to the corporate enterprise network without the knowledge of the end user.

In addition to mis-associated clients, additional threats that Cisco Aironet does not protect against include:

- Ad hoc networks – an authorized client that connects directly to another Wi-Fi client not through an access point.

- Mis-configured access points – an authorized access point that has its authorized security policies changed to potentially allow insecure access.

- MAC AP spoofing – an access point that mimics the SSID and MAC address of an authorized access point in an attempt to have authorized clients connect. It can insert itself as a "man-in-the-middle" of authorized communication.

- Evil Twin/Honey Pot APs – building on a MAC AP spoofing attack, the Evil Twin AP further tries to lure the client in by mimicking a log in page to capture confidential log in information or credit card.

- Denial of Service attacks - a device flooding a channel or channels with deauthentication or similar packets that terminate all current and attempted client associations to APs.

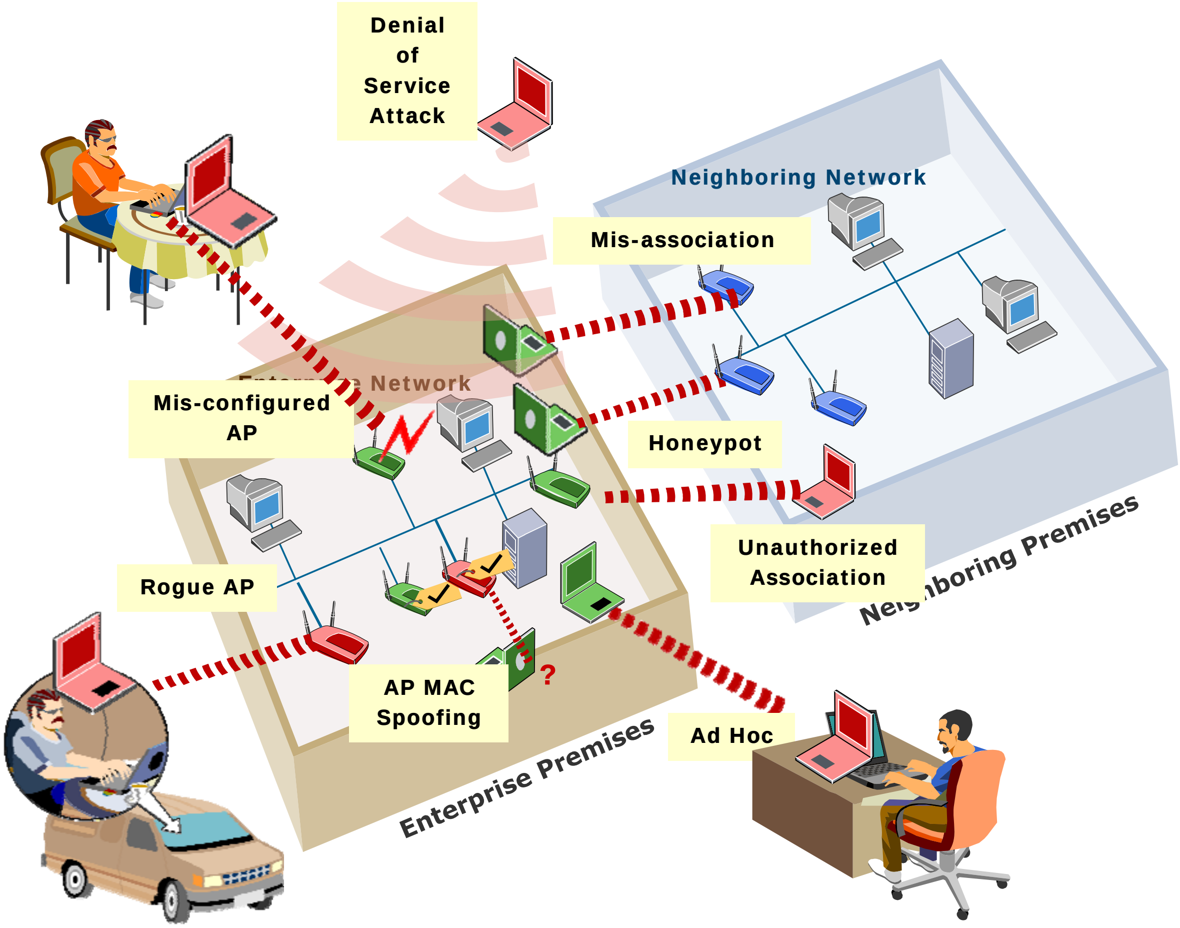


Figure 4: In addition to rogue APs, enterprises need to be concerned about protecting against the seven other major categories of Wi-Fi threats.

A New Solution to Complement Wireline Network Security – A Wireless IPS Firewall

As has been discussed, the Cisco Aironet and WLSE wireless LAN solution even with the latest IEEE 802.11i security does not protect against the majority of wireless threats to corporate security. Neither do conventional network firewalls or VPNs. These traditional wireline security measures only monitor wired traffic and have no visibility into the wireless traffic that is flowing in the air. Until recently no solutions were available that adequately protected both wireless and wireline networks by providing automatic and reliable prevention against "rogue" intruders and neighboring unauthorized Wi-Fi clients. A new class of solution, the Wireless Intrusion Prevention System (WIPS) Firewall, is now available to complement wired security solutions such as VPNs and firewalls, providing complete protection of an enterprise's air space and thus their trusted wire-line network.

Components of a Wireless IPS

AirTight Networks provides a world class wireless IPS solution – SpectraGuard Enterprise - comprised of a Server and wireless Sensors. Functionality of the two major components is described in detail below.

AirTight SpectraGuard Enterprise Server

The SpectraGuard Enterprise Server provides correlation and analysis of the RF information collected by the SpectraGuard Sensors. Information from the Sensors is also analyzed in context of their location. Using information and policies set up by the administrator, the Server automatically classifies the wireless devices 'seen' by the sensors. Patent pending technology ensures that classification is nearly foolproof to all categories of wireless threats. Automatic prevention, again based on policies set up by the administrator, is initiated by the Server to the appropriate Sensors to use over-the-air techniques to stop the threat. With all of the Wi-Fi information available to it, SpectraGuard Enterprise Server also provides needed wireless LAN monitoring for performance issues. Unique Knowledge Based Troubleshooting can even help administrators or help desk personnel pinpoint client performance issues and resolve them quickly. Pre-defined or custom reports on the performance of the system or compliance to specific regulations such as Sarbanes-Oxley, HIPAA, Gramm-Leach-Bliley and DoD 8100.2 can be scheduled to be delivered automatically to a variety of personnel. All management of the entire solution is done through a simple web-based GUI.

AirTight SpectraGuard Enterprise Sensors

SpectraGuard Sensors connect to the wireline network and provide round-the-clock scanning of the airwaves. SpectraGuard Sensors support two separate radios, covering both the 2.4 GHz (802.11b/g) and the 5 GHz (802.11a) bands. Sensors detect all Wi-Fi activity within range. Multiple Sensors can be placed around the building site to ensure complete protection of the enterprise. Sensor placement is dependent upon the type of building materials and the level of prevention and location tracking that is required.[1]

Each AirTight Sensor can block devices on multiple channels simultaneously while they continue to scan for new threats. On each of these channels, multiple devices can be blocked. The collected RF information is sent back to the SpectraGuard Enterprise Server for analysis and collation. If a wireless threat is detected, the Server will provide instructions to the Sensor(s) to implement the over-the-air prevention per the policies set up by the administrator.

Benefits of the Combined AirTight Networks SpectraGuard Enterprise Wi-Fi IPS and Cisco Aironet Wireless LAN

Using the SpectraGuard Enterprise as the wireless IPS with a Cisco Aironet wireless LAN infrastructure delivers the following benefits:

- Comprehensive threat prevention using wireless and wired techniques
    - Complete wireless threat identification
    - Automatic wireless intrusion prevention against all wireless threat categories
    - Automatic wired-side port blocking through Cisco WLSE
- Industry's best location tracking for quick permanent removal of rogues
- Easier administration of authorized Cisco access points
- Lower total cost of ownership of the wireless LAN
    - Accurate visualization of RF security coverage and defenses
    - Comprehensive compliance reporting for Sarbanes-Oxley, HIPAA, Gramm-Leach-Bliley and DoD 8100.2

A sample architecture using the two solutions is shown in the diagram below.

[1] For more details on the placement of sensors, please see the AirTight Networks whitepaper "Planning IEEE 802.11 Wireless Networks for Security and Coverage."

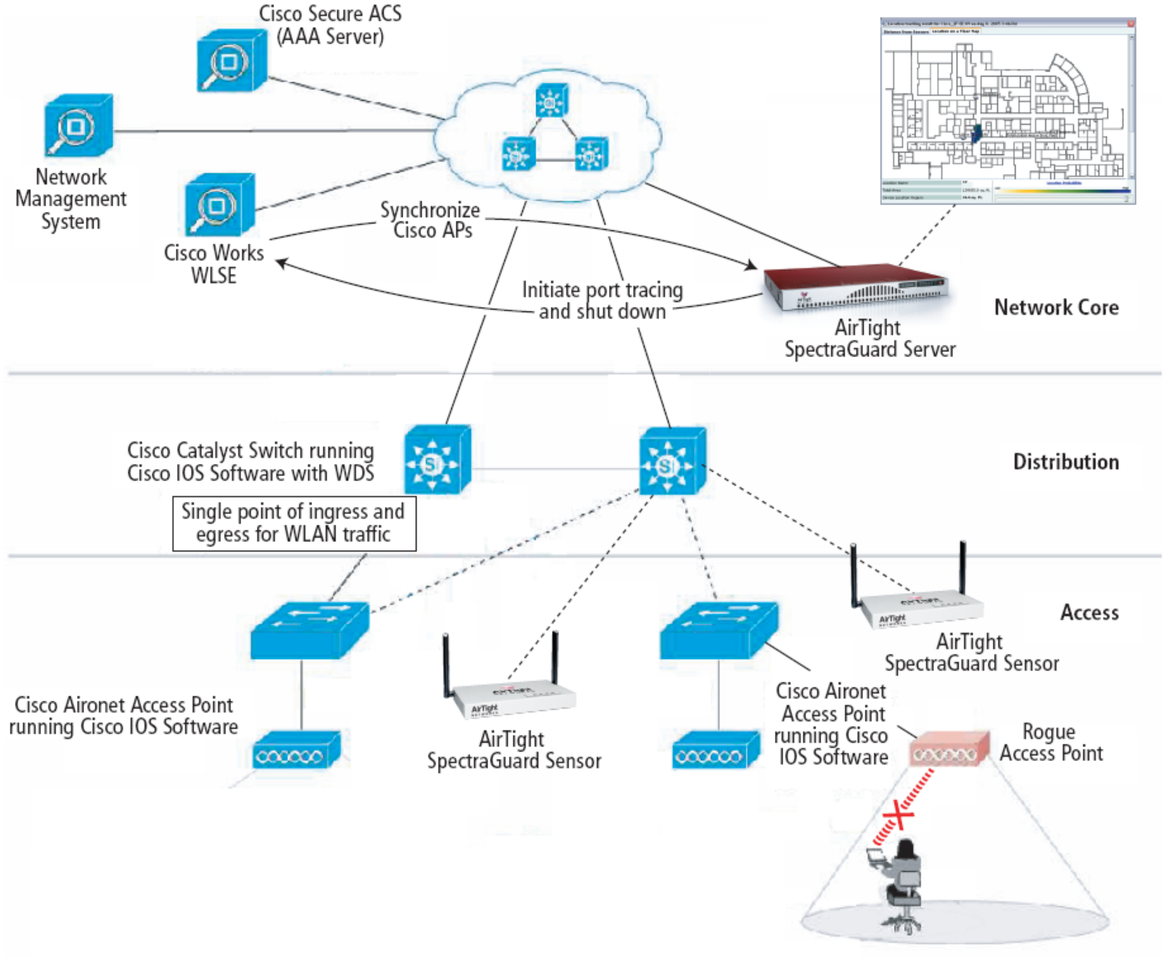

Cisco Secure ACS (AAA Server)
Network Management System
Cisco Works WLSE
Synchronize Cisco APs
Initiate port tracing and shut down
AirTight SpectraGuard Server
Network Core
Cisco Catalyst Switch running Cisco IOS Software with WDS
Single point of ingress and egress for WLAN traffic
Distribution
Access
AirTight SpectraGuard Sensor
Cisco Aironet Access Point running Cisco IOS Software
AirTight SpectraGuard Sensor
Cisco Aironet Access Point running Cisco IOS Software
Rogue Access Point

Figure 5: AirTight Networks SpectraGuard Enterprise easily integrates with the Cisco Aironet WLSE and access points, providing best-in-class wireless intrusion prevention.

Deploying SpectraGuard Enterprise with the Cisco Aironet Wireless LAN Solution

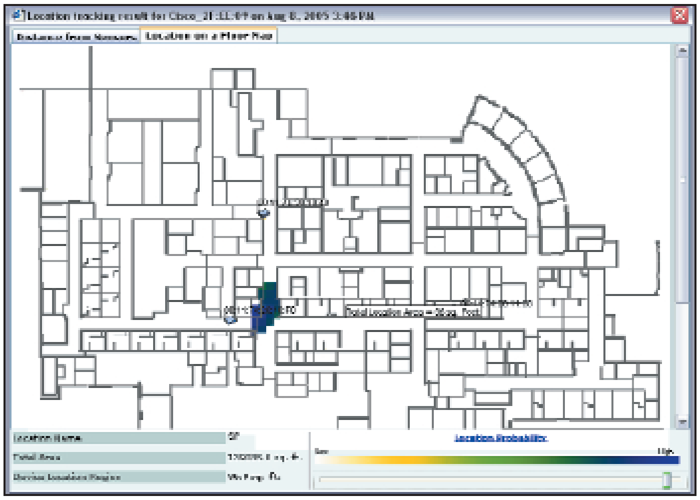
SpectraGuard Enterprise integrates seamlessly with Cisco Aironet wireless LANs and the WLSE. Simply connect SpectraGuard Sensors to the Ethernet network to provide automatic detection and prevention coverage throughout the enterprise. Placing Sensors is as simple as deploying Access Points. SpectraGuard Planner can provide a detailed map of where sensors should be placed for your specific site based on the specific building layout and materials in your facility. SpectraGuard Enterprise Server can be placed in any wiring closet and does not need a direct connection to the Sensors. Sensors can be a Layer 2 or Layer 3 network away from the Server. Sensors will automatically relay information back to the Server for correlation and analysis. In version 4.0 of SpectraGuard Enterprise, complete integration with Cisco WLSE is available. This delivers the following benefits.

Comprehensive Threat Prevention Using Over-the-Air and Wired Side Port Blocking Techniques

RF information about clients and access points discovered by Cisco Access Points is fed to SpectraGuard Enterprise through Cisco WLSE. This information enhances that discovered by the sensors. For rogue access points, in addition to using precise over-the-air prevention techniques, SpectraGuard Enterprise can initiate port tracing and wired side port blocking through Cisco WLSE. This delivers the most comprehensive threat prevention against rogue access points. For all other wireless threats such as client mis-association, unauthorized APs not connected to the network and Denial of Service attacks, SpectraGuard Enterprise delivers full protection through over-the-air prevention techniques.

Industry's Best Location Tracking

Patent pending techniques allow SpectraGuard Enterprise to deliver the industry's most precise location tracking of any Wi-Fi device. This eliminates the time consuming walk arounds needed with other systems to physically remove the rogue device.

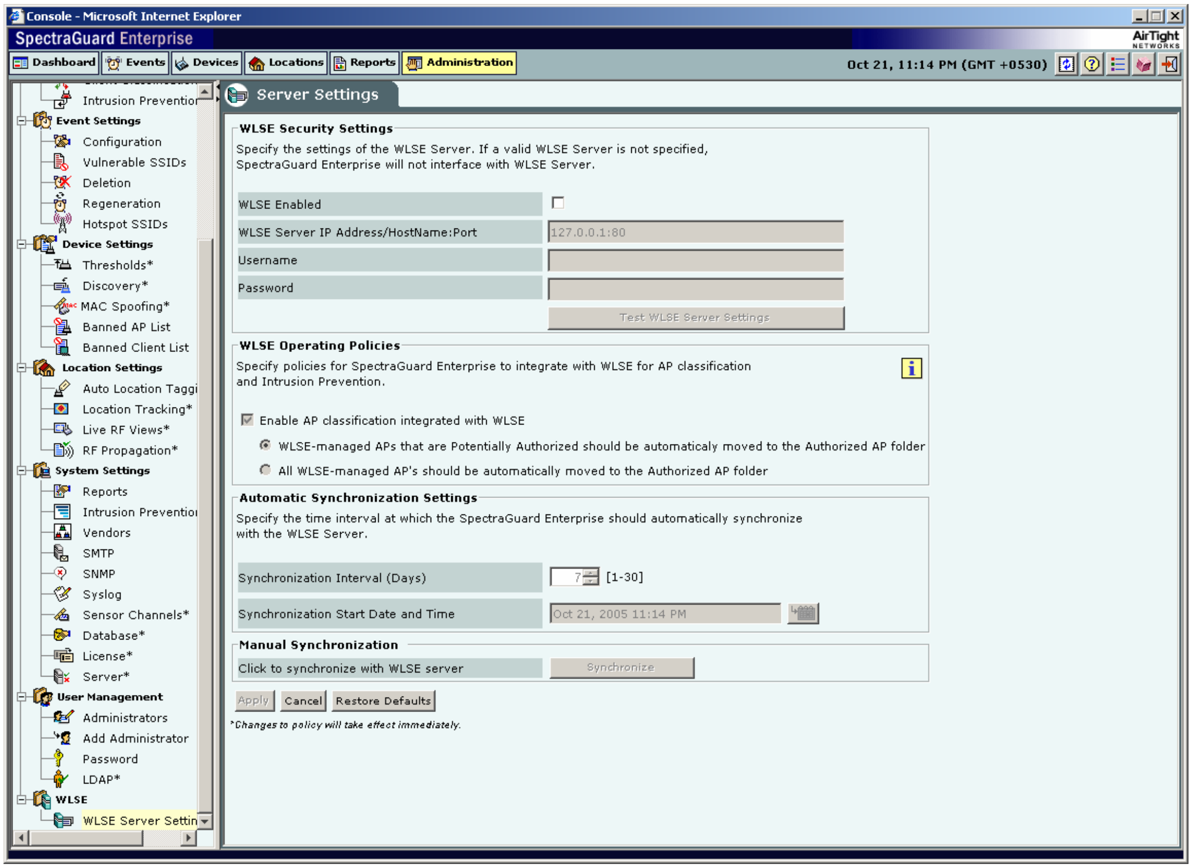

Location tracking result for Cisco_21:11:09 on Aug 8, 2005 3:46 PM
Distance from Sensors
Location on a Floor Map
Total Location Area = 35 sq. feet
Location Probability
Low
High

Location Name	2F
Total Area	170208 sq. ft.
Device Location Region	[illegible] sq. ft.

Figure 6: Precisely locate any access point or client.

Easier Administration

Integration with Cisco WLSE allows all managed Cisco APs to be automatically entered into the SpectraGuard Enterprise Server. This eliminates the need for manual authorization upon set up of the wireless IPS. Ongoing additions to the wireless LAN network continue to be updated automatically as well. With a few simple keystrokes in the administration screen shown below, SpectraGuard Enterprise is integrated with Cisco WLSE.



WLSE Security Settings

Specify the settings of the WLSE Server. If a valid WLSE Server is not specified, SpectraGuard Enterprise will not interface with WLSE Server.

WLSE Enabled	□
WLSE Server IP Address/HostName:Port	127.0.0.1:80
Username	
Password	

Test WLSE Server Settings

WLSE Operating Policies

Specify policies for SpectraGuard Enterprise to integrate with WLSE for AP classification and Intrusion Prevention.

☑ Enable AP classification integrated with WLSE

● WLSE-managed APs that are Potentially Authorized should be automaticaly moved to the Authorized AP folder

○ All WLSE-managed AP's should be automatically moved to the Authorized AP folder

Automatic Synchronization Settings

Specify the time interval at which the SpectraGuard Enterprise should automatically synchronize with the WLSE Server.

Synchronization Interval (Days)	7 [1-30]
Synchronization Start Date and Time	Oct 21, 2005 11:14 PM

Manual Synchronization

Click to synchronize with WLSE server — Synchronize

Apply Cancel Restore Defaults

**Changes to policy will take effect immediately.*

Figure 7: A simple one page screen quickly configures SpectraGuard Enterprise to integrate with Cisco WLSE. This allows automatically updates of new Cisco APs eliminating manual configuration.

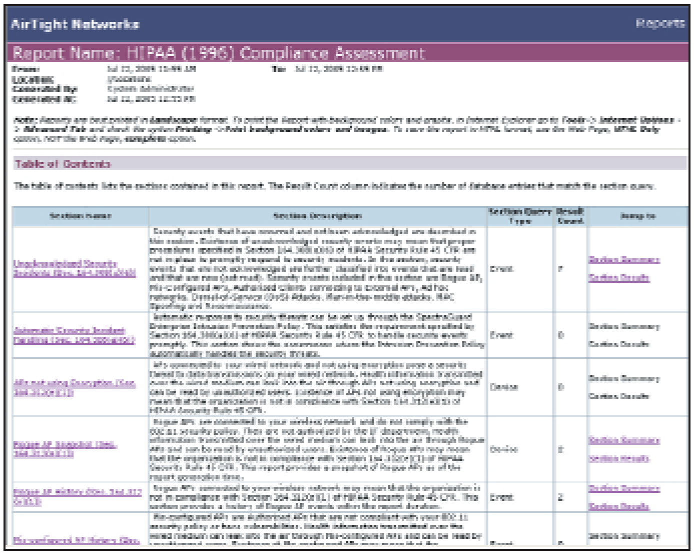
Lower Total Cost of Ownership

With automatic classification and prevention of all wireless threats, precise location tracking and built-in compliance reporting, the overall cost of deploying a wireless LAN securely is significantly lowered. Manual walk throughs for:

- Site calibration for location tracking
- Precise location of wireless threats

is now removed, saving valuable man hours.

Built-in compliance reporting of wireless LAN security and wireless threats eases the regulatory burden on the IT administrator.



AirTight Networks

Reports

Report Name: HIPAA (1996) Compliance Assessment

From: Jul 13, 2009 [illegible] To: Jul 13, 2009 [illegible]
Location: [illegible]
Generated By: System Administrator
Generated At: [illegible]

Note: Reports are best printed in Landscape format. To print the Report with background colors and graphs, in Internet Explorer go to Tools -> Internet Options -> Advanced Tab and check the option Printing -> Print background colors and images. To save the report in HTML format, use the Web Page, MHTML Only option, not the Web Page, complete option.

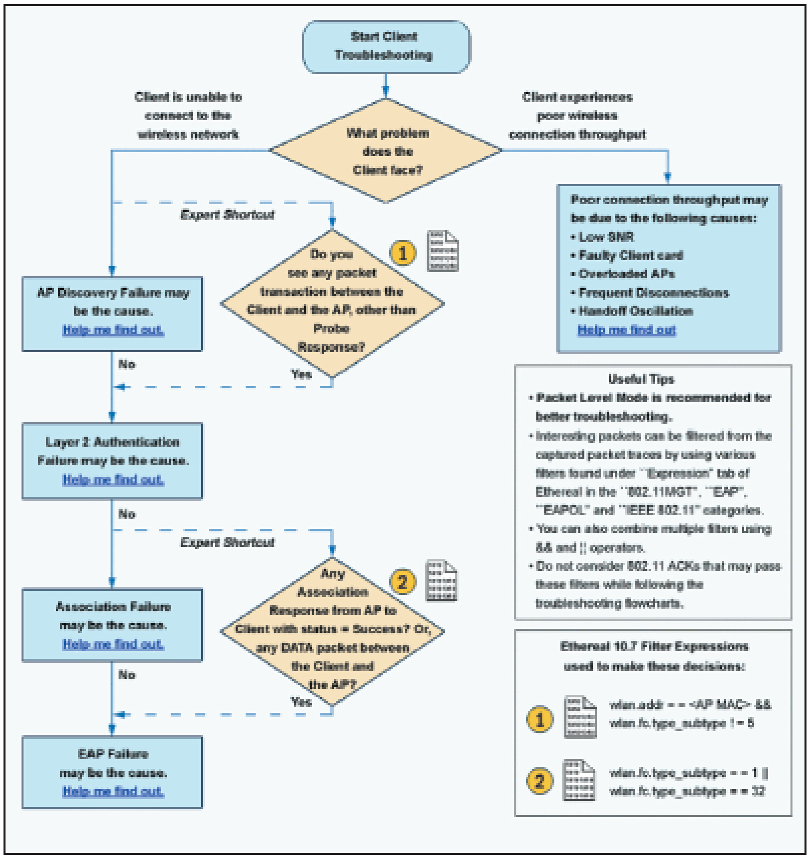
Table of Contents

The table of contents lists the sections contained in this report. The Result Count column indicates the number of database entries that match the section query.

Section Name	Section Description	Section Query Type	Result Count	Jump to
Unacknowledged Security Incidents (Sec. 164.308(a)(6))	Security events that have occurred and not been acknowledged are described in this section. Existence of unacknowledged security events may mean that proper procedures specified in Section 164.308(a)(6) of HIPAA Security Rule 45 CFR are not in place to promptly respond to security incidents. In this section, security events that are not acknowledged are further classified into events that are read and that are new (unread). Security events included in this section are Rogue AP, Mis-configured APs, Authorized clients connecting to external APs, Ad hoc networks, Denial-of-Service (DoS) Attacks, Man-in-the-middle attacks, MAC Spoofing and Reconnaissance.	Event	7	Section Summary Section Results
Automatic Security Incident Handling (Sec. 164.308(a)(6))	Automatic responses to security threats can be set up through the SpectraGuard Enterprise Intrusion Prevention Policy. This satisfies the requirement specified by Section 164.308(a)(6) of HIPAA Security Rule 45 CFR to handle security events promptly. This section shows the occurrences where the Intrusion Prevention Policy automatically handled the security threats.	Event	0	Section Summary Section Results
APs not using Encryption (Sec. 164.312(e)(1))	APs connected to your wired network and not using encryption pose a security threat to data transmissions on your wired network. Health information transmitted over the wired medium can leak into the air through APs not using encryption and can be read by unauthorized users. Existence of APs not using encryption may mean that the organization is not in compliance with Section 164.312(e)(1) of HIPAA Security Rule 45 CFR.	Device	0	Section Summary Section Results
Rogue AP Snapshot (Sec. 164.312(e)(1))	Rogue APs are connected to your wireless network and do not comply with the 802.11 security policy. They are not authorized by the IT department. Health information transmitted over the wired medium can leak into the air through Rogue APs and can be read by unauthorized users. Existence of Rogue APs may mean that the organization is not in compliance with Section 164.312(e)(1) of HIPAA Security Rule 45 CFR. This report provides a snapshot of Rogue APs as of the report generation time.	Device	2	Section Summary Section Results
Rogue AP History (Sec. 164.312(e)(1))	Rogue APs connected to your wireless network may mean that the organization is not in compliance with Section 164.312(e)(1) of HIPAA Security Rule 45 CFR. This section provides a history of Rogue AP events within the report duration.	Event	2	Section Summary Section Results
Misconfigured AP History (Sec.	Mis-configured APs are Authorized APs that are not compliant with your 802.11 security policy or have vulnerabilities. Health information transmitted over the wired medium can leak into the air through Mis-configured APs and can be read by unauthorized users. Existence of Mis-configured APs may mean that the	Event	0	Section Summary

Figure 8: Easily schedule customized compliance reports to ease the reporting function.

And, Knowledge Based Troubleshooting provides a simple, flowchart analysis for troubleshooting wireless LAN client performance issues that plague help desks.


Start Client Troubleshooting
Client is unable to connect to the wireless network
What problem does the Client face?
Client experiences poor wireless connection throughput
Expert Shortcut
Do you see any packet transaction between the Client and the AP, other than Probe Response?
1
AP Discovery Failure may be the cause.
Help me find out.
No
Yes
Poor connection throughput may be due to the following causes:
• Low SNR
• Faulty Client card
• Overloaded APs
• Frequent Disconnections
• Handoff Oscillation
Help me find out
Layer 2 Authentication Failure may be the cause.
Help me find out.
No
Expert Shortcut
Any Association Response from AP to Client with status = Success? Or, any DATA packet between the Client and the AP?
2
Association Failure may be the cause.
Help me find out.
No
Yes
EAP Failure may be the cause.
Help me find out.
Useful Tips
Ethereal 10.7 Filter Expressions used to make these decisions:
1
2

Useful Tips

- **Packet Level Mode is recommended for better troubleshooting.**
- Interesting packets can be filtered from the captured packet traces by using various filters found under ``Expression'' tab of Ethereal in the ``802.11MGT'', ``EAP'', ``EAPOL'' and ``IEEE 802.11'' categories.
- You can also combine multiple filters using && and || operators.
- Do not consider 802.11 ACKs that may pass these filters while following the troubleshooting flowcharts.

Ethereal 10.7 Filter Expressions used to make these decisions:

1
```
wlan.addr = = <AP MAC> &&
wlan.fc.type_subtype ! = 5
```

2
```
wlan.fc.type_subtype = = 1 ||
wlan.fc.type_subtype = = 32
```

Figure 9: Simple Knowledge-Based Troubleshooting Wizard allows help desk or remote administrators to quickly solve client performance problems.

Last, Cisco Aironet Access Points may act as Sensors, allowing a lower overall total number of Sensors to completely protect the enterprise's air space.

Conclusion

This document describes a sample architecture for deploying wireless IPS using the AirTight Networks SpectraGuard Enterprise Wi-Fi IPS Firewall and the Cisco Aironet wireless LAN solution as depicted in Figure 4. Interoperability amongst the products has been tested and validated ensuring customers that the combined solution will provide superior wireless threat prevention keeping the Cisco Aironet network safe as well as protecting the enterprise wireline network from wireless breaches. In addition, AirTight Networks adds comprehensive monitoring and troubleshooting tools, compliance reporting and the industry's best location tracking, further enhancing the value of the Cisco wireless LAN. Together, the two solutions deliver the industry's most secure and robust wireless LAN solution.