

Enterprise



**Using AirWave RAPIDS Rogue Detection
to Implement Your Wireless Security
and PCI Compliance Strategy**

Table of Contents

Introduction.....	2
Using AirWave RAPIDS to Detect All Rogues on Your Network.....	3
Rogue Device Detection and Attack Signature Tracking.....	3
Wireless Discovery	3
Result Correlation.....	4
Threat Classification	4
Automated Alerts and Reports	5
Rogue Remediation and Containment Mechanisms	5
Summary.....	8

1. Introduction

Wireless LANs (WLANs) are quickly becoming the connectivity platform of choice across all types of organizations because of their flexibility, convenience and ability to improve productivity. As WLANs evolve from best-effort to mission-critical infrastructure, organizations find that the operational aspects of network security take on much greater importance. They discover that technical requirements are only one part of the equation. Regulatory requirements relating to wireless networks consume a significant amount of time and resources. As a result, many organizations are rethinking their approach to security in their network operations.

Effectively managing wireless security presents many challenges. Because wireless networks are based on RF spectrum, they are inherently hard to control and allow malicious attacks much more easily than with wired networks. Attackers can execute wireless attacks, such as denial-of-service and man-in-the-middle, using simple, off-the-shelf hardware and free software.

Another security issue involves well-meaning users who set up rogue (or unauthorized) consumer-grade access points (APs) in the workplace. These users, unaware of the security implications of their actions, can easily compromise the corporate network's security. Related problems occur when laptops in dense urban settings or open, public Wi-Fi networks connect to the organization's wired network.

Regulatory compliance is a key motivator that drives many organizations to implement stringent security processes for their enterprise wireless networks. The most common regulations are Payment Card Industry (PCI) Data Security Standard, Health Insurance Portability and Accountability Act (HIPAA) and Sarbanes-Oxley (SOX).

Despite setting strict policies that ban the installation of unauthorized APs, few enterprises have the tools or resources to adequately enforce these guidelines and to follow up and resolve threats consistently. Some organizations try to get by with periodic manual scans by security or network engineering teams using handheld scanners. This method is time-consuming and random, and thus provides little return on a significant investment.

Still other companies use their authorized Wi-Fi access points to detect rogue APs. This approach is a cost-effective way to detect the presence of possible rogues, but without proper management tools to classify the devices found, using authorized APs to find rogues can potentially identify thousands of potential threats with no follow-up mechanism. In addition, this approach is only effective in detecting rogues within RF range of the authorized APs. In organizations without comprehensive wireless coverage, this approach potentially leaves a great deal of space exposed. It is precisely these uncovered areas where employees and hackers are most likely to install their own access points. Further, wireless networks may have inadvertent coverage holes that create blind spots.

Another strategy is to install a complete overlay infrastructure, which provides dedicated sensors that locate rogue wireless devices, monitor for attacks and shield clients from attaching to rogue devices. Overlay solutions bring the benefits of full-time scanning to bear, but add complexity. Network operations teams must manage yet another system. In addition, overlay systems must be updated constantly to keep them synchronized with the APs deployed on the network, which frequently change or are swapped out for maintenance. Too frequently, the overlay system does not recognize valid APs and contains them as rogues, which cuts off service to users. Overlay architectures are the most costly approach in terms of capital expenditure and operating costs.

AirWave RAPIDS™ Rogue Detection provides organizations with a practical, cost-effective solution for enforcing security policies and managing compliance. RAPIDS is a feature of AirWave Wireless Management Suite™ from Aruba Networks that delivers the core capabilities needed to manage service quality for mobile users.

Using a patented combination of wireless and wired network scans, RAPIDS automatically detects and locates unauthorized access points using the existing, authorized APs and air monitors to scan the RF

environment for any unauthorized devices in range. Unlike many other wireless security solutions, RAPIDS scans your wired network to determine whether any unknown devices have been connected. An additional software client allows Wi-Fi enabled Windows devices to act as auxiliary RF sensors with the optional AirWave Management Client™ (AMC) software. RAPIDS then correlates all of this data and uses a set of rules to highlight only those devices that are truly a threat to your organization, which greatly reduces false-positives and allows IT staff to focus on the most important issues.

RAPIDS works in conjunction with the wireless intrusion prevention module available with Aruba routers to offer customers a comprehensive wireless intrusion protection solution (WIPS). Customers can deploy this solution with hybrid APs that serve the dual purpose of providing access to users while scanning for wireless threats. Or, when implemented as an overlay architecture, Aruba APs can serve as dedicated sensors called air monitors (AMs). RAPIDS uses data from both the deployed APs and the dedicated AMs to provide a complete view of your wireless environment. In the event that your organization does not yet have an authorized wireless LAN, you can use RAPIDS and AMC to detect rogues on the network using both wired and wireless detection methods.

This white paper discusses how RAPIDS works to vastly improve network security, manage compliance requirements such as PCI, and reduce the cost of maintaining wireless security.

2. Using AirWave RAPIDS to Detect All Rogues on Your Network

To provide a practical, effective defense against rogues and other forms of wireless intrusion, a solution must offer both wired and wireless scans, accurately analyze and prioritize the threat levels of potential rogues, and alert staff of threats based on the enterprise's security policies and requirements. To accomplish these objectives, RAPIDS supports the five-step process outlined below:

1. Performs multiple types of wired and wireless scans.
2. Correlates the results of the various scans to consolidate all available information about identified devices.
3. Classifies the discovered devices based on rules that are customized to an organization's security needs.
4. Generates automated alerts and reports for IT containing key known information about unauthorized devices, including the physical location and switch port whenever possible.
5. Deploys containment mechanisms to neutralize potential threats.



Figure 1: AirWave RAPIDS Rogue Detection automatically detects and locates unauthorized access points and utilizes a set of rules to highlight the most important threats to your organization.

3. Rogue Device Detection and Attack Signature Tracking

RAPIDS uses a patented combination of discovery techniques across both your wireless and wired network infrastructure to find every potential rogue access point, whether it is connected to your network or not.

3.1.1 Wireless Discovery

For wireless discovery, RAPIDS uses your existing authorized access points and/or dedicated sensors to scan the airspace for IDS events or any unauthorized devices broadcasting within range. These infrastructure devices handle the scanning of the wireless environment, and in some systems they take care of correlating wireless and wired traffic. All data is reported to RAPIDS.

Optional AirWave Management Client software allows you to use existing Wi-Fi-enabled PCs for rogue detection where no wireless coverage is provided. AMC software acts as a passive sensor that listens to the surrounding environment and reports back to the RAPIDS. This enhances the wireless discovery process without having to deploy additional sensors or APs, which can be costly.

3.1.2 Wired Discovery

To find rogue APs that cannot be discovered via RF scans and to provide richer information on those APs that have been discovered wirelessly, RAPIDS polls the routers and switches on the network to obtain a full list of devices physically connected to the wired infrastructure. RAPIDS compares the MAC address of each device to AirWave's database of more than 12,000 MAC address ranges to identify devices that fall within the ranges used by manufacturers of consumer-grade wireless access points. Since these devices are rarely used by enterprise IT departments, they are the most common devices to be identified as rogues.

As an additional procedure for rogue detection, RAPIDS uses SNMP and HTTP fingerprint scans, which allows the system to scan every IP address in a specified range. Since false-positive identifications are costly and time-consuming for IT to investigate, RAPIDS can interrogate a suspected rogue device to determine its operating system, and that information can weed out devices that are less likely to be rogues. Armed with this supplementary information, network security personnel have a greater confidence level when confirming a device as a rogue, even if it wasn't identified wirelessly.

3.2 Result Correlation

As RAPIDS runs its scans, it uses a series of algorithms to correlate and aggregate the data into a single device record that:

- Provides comprehensive information to assess and locate a potential rogue.
- Shows wireless scan result details, which includes SSID, number of discovering radios, encryption information, vendor, RF channel, radio MAC address or BSSID, and network type.
- Displays wireline scan data, including LAN MAC address, IP address, vendor and operating system.
- Uses wireless discovery information to link BSSIDs together, allowing RAPIDS to accurately identify a single rogue that is broadcasting multiple BSSIDs.
- Compares the wired and wireless information to detect devices on the physical LAN, which avoids duplicate reports on a single rogue.

The correlation process permits a more accurate threat assessment for the organization. The comprehensive device record is passed to the classification engine, where RAPIDS makes a determination about the device's threat level.

3.3 Threat Classification

For many companies, rogue scans produce an overwhelming number of devices to investigate. RAPIDS' classification capabilities help network staff quickly rank potential threats, reduce false-positives and accurately prioritize their risk mitigation activities within the context of the organization's unique definitions of what constitutes a threat.

RAPIDS provides an easy-to-use framework with a customizable rules engine that uses rankings to determine if a device is a rogue or simply a nearby AP. The rules engine is pre-populated with common default classifications that are completely configurable to meet the organization's policy requirements. These classifications include Valid, Neighbor, Suspected Neighbor, Suspected Rogue and Rogue.

Unlike wireless security products, RAPIDS seamlessly integrates with AirWave Wireless Management Suite, which enables it to automatically identify all valid APs



Figure 2: RAPIDS classifications make device investigations more efficient.

during the course of network operations. As a result, RAPIDS does not mistakenly see valid devices as potential rogues, even if they have just been added to the network or if they are legacy WLAN infrastructure with different operational parameters from the organization's current architecture.

3.4 Automated Alerts and Reports

Once RAPIDS classifies devices, it generates alerts and reports according to user-definable triggers. Most organizations configure RAPIDS to issue high-priority alerts via email, SNMP trap, syslog or console

whenever devices with a threat classification of Suspected Rogue or greater are detected. Potential rogues that have been assigned lower scores may generate lower-priority alerts or be logged in a report for later investigation.

All RAPIDS alerts and log files incorporate links to the RAPIDS detail screen, which contains all known data about the potential rogue device to assist IT in finding and removing the device as quickly as possible.

Organizations can define triggers to act on wireless attack data reported by the network infrastructure. Most modern Wi-Fi controller architectures can detect wireless network attacks and report them through SNMP traps. RAPIDS adds a layer of management by acquiring the traps, linking them to the detecting device and aggregating them across the network. By linking and aggregating the traps, RAPIDS adds useful context about what is happening on the network.

This information is powerful. While a single attack might not warrant an investigation, emerging patterns might tell a different story. For example, if your baseline is 100 attacks in one day, RAPIDS can alert you that "Today, this controller had 150 attacks."

RAPIDS offers a customizable dashboard that provides the network security team with an at-a-glance view into the current state of the entire network. The dashboard displays all pertinent details of the network, including current IDS activity, detected devices, OS versions used and a complete security change log. It includes graphical charts that enable staff to quickly assess current situations and determine if action is required.

RAPIDS creates a full report that lists all suspected rogues for more efficient management and compliance reporting. Reports can run automatically on a scheduled basis and be customized to meet the organization's specific security requirements. AirWave includes a PCI compliance report designed specifically to speed up the PCI auditing process and help organizations track ongoing network compliance.

3.5 Rogue Remediation and Containment Mechanisms

When a device is classified as a rogue, its information and classification pass through to AirWave VisualRF™ Location and Mapping feature. This graphical tool calculates the rogue's location and displays this information on a building floor plan. In most cases, the location can be identified within a few meters, so IT can take immediate action to eliminate the threat.

If physical remediation is not immediately possible, network administrators can remotely disable the switch port to which it is connected, thereby denying the rogue device access to the wired network. In addition, IT has several manual and configurable rules-based options to contain rogues wirelessly. As an

Summary

IDS Events for devices in folder Top and subfolders

Attack	Last 2 Hours	Last 24 Hours	Total
AP Impersonation	0	19	88
Deauth-Broadcast	0	2	2
Disconnect Station Attack (AP)	55	728	1925
Disconnect Station Attack (Station)	2	11	49
Null-Probe-Response	0	0	2
Station Associated to Rogue AP	71	1198	2927
Station Unassociated from Rogue AP	74	1156	2636
7 Attack Types	202	3114	7629

Rogue Data

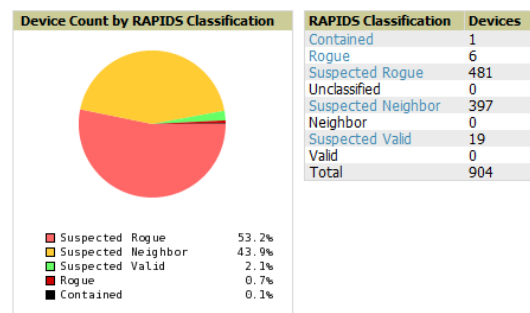


Figure 3: The RAPIDS dashboard displays real-time information on all suspected rogues and on IDS events.

example, the organization may want to contain all rogues automatically so that when they are discovered after normal business hours, the network security team has time to investigate.

The result is a two-pronged containment approach. First, it prevents users from associating with rogue devices, and second, it ensures that rogue devices do not have access to the wired network. Once a device has been removed from the network, RAPIDS remembers it so that it is automatically rejected even if it is moved to another location. In addition, RAPIDS provides reports to identify which APs have been blacklisted and to display a history of their use.

4. Using RAPIDS to Ensure PCI Compliance

Developed by the Payment Card Industry Security Standards Council, which includes American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa Inc., PCI Data Security Standard (DSS) is a set of comprehensive requirements intended to help organizations proactively protect customer account data. PCI DSS¹ requires that all organizations accepting credit or debit cards for purchases protect their networks from attacks via rogue or unauthorized wireless APs and clients. This applies even if the merchant has not deployed a wireless network for its own use.



¹ PCI Security Standards Council Wireless Special Interest Group Implementation Team, "Information Supplement: PCI DSS Wireless Guideline," July 2009

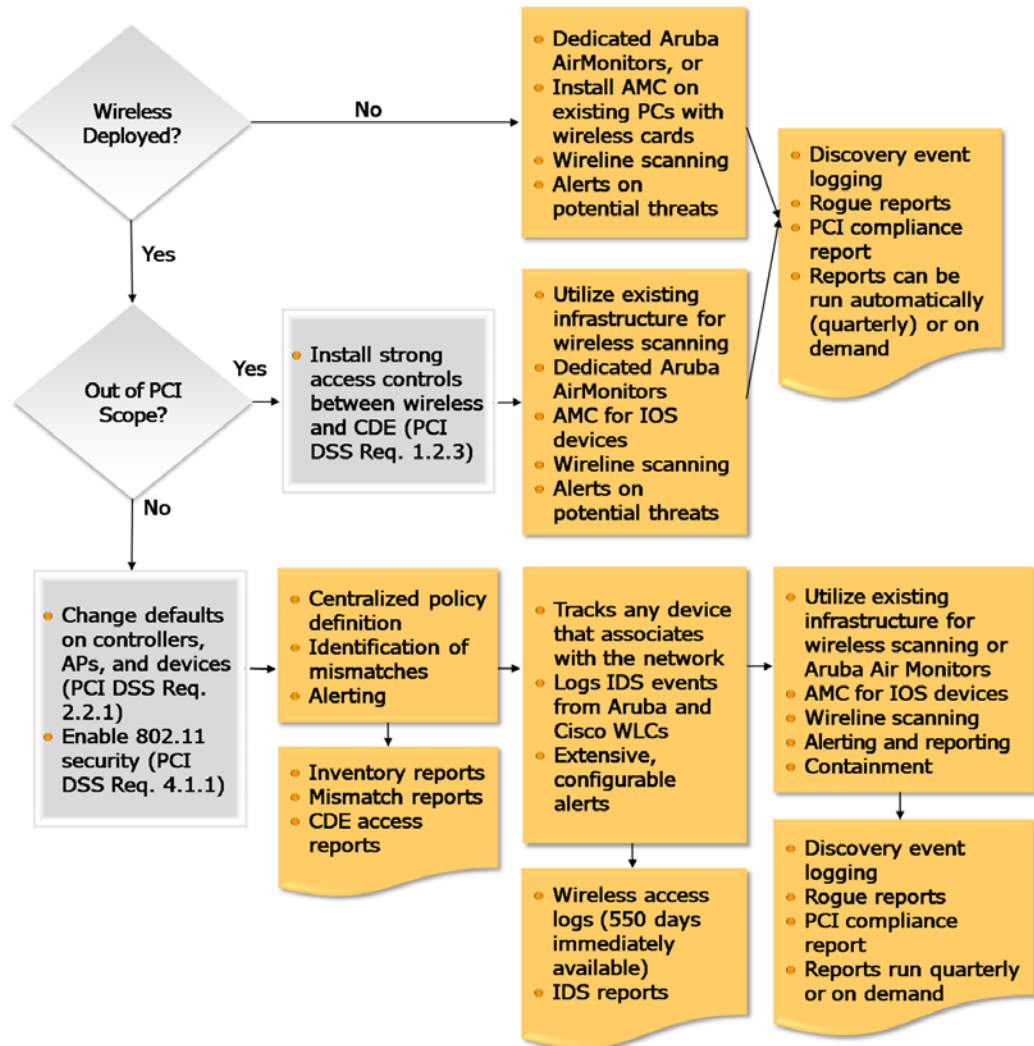


Figure 4: Key requirements from PCI DSS Wireless Guidelines.

PCI compliance mandates that merchants:

- Change defaults on all wireless APs, controllers and devices and generate audit reports proving such changes have been implemented.
- Log wireless access centrally, review access logs daily and archive these access logs for one year.
- Test for the presence of wireless access points by using a wireless analyzer at least quarterly or deploying a wireless IDS/IPS to identify all wireless devices in use. For large organizations with multiple locations, a centrally managed wireless IDS/IPS to detect and contain unauthorized or rogue wireless devices is recommended.
- Enable automatic alerts and containment mechanisms on the wireless IPS to eliminate rogues and unauthorized wireless connections into the network environment.
- Create an incident response plan to physically eliminate rogue devices immediately from the network.
- Perform audits on a regular basis for compliance and provide reports on the security of the network.

The AirWave RAPIDS Rogue Detection feature helps retailers and other covered organizations comply with these requirements. RAPIDS can leverage existing access points to automatically detect, locate and display the location of any rogue devices on both the wireless and wireline networks. RAPIDS also enables companies to set up automated, prioritized alerts that can be emailed to a specified distribution list the instant that rogues are detected.

PCI auditing features in RAPIDS allow organizations to monitor, audit and demonstrate real-time PCI compliance on the network. The system can alert network staff whenever a configuration error is detected, providing complete information as to how the configuration violates defined policy. Because RAPIDS seamlessly integrates with AirWave, it has a complete view into a wide range of requirements, including default password enablement and wireless association information. RAPIDS provides detailed user tracking and session history, showing who is connected to your network, when they connected and where they've roamed.

RAPIDS creates a full report listing all suspected rogues for compliance reporting. Reports can be run on a scheduled or ad hoc basis to meet your specific requirements. As staff investigates potential rogues, RAPIDS provides an Acknowledge Yes/No flag for every device to aid in workflow management. RAPIDS provides a pass/fail grade for the network for each PCI requirement, which allows security teams and auditors to quickly confirm compliance in an easy-to-use report.

Daily PCI Report for Groups Ethersphere-lms3, Aruba HQ, Cisco Gear

11/5/2009 11:00 PM to 11/6/2009 11:00 PM
Generated on 11/6/2009 11:02 PM

This report covers sections of the Payment Card Industry (PCI) Data Security Standard (DSS) Version 1.2 requirements that are relevant to security in your network. PCI DSS standard requirements are available at <https://www.pcisecuritystandards.org>.

Disclaimer: The PCI Compliance Report must be completed by an authorized QSA. The sole purpose of this report is to provide IT administrators with an on-demand internal audit of components that are visible to AirWave Wireless Management Suite.

Summary

PCI Requirement ▲	Description	Status
1.1	Configuration standards for routers. A device fails if there are mismatches between the desired configuration and the configuration on the device.	Fail
1.2.3	Install firewalls between any wireless networks and the cardholder data environment. A device passes if it can function as a stateful firewall.	Pass
2.1	Always change vendor-supplied defaults. A device fails if the usernames, passwords or SNMP credentials being used by AWMS to communicate with the device are on a list of forbidden credentials. The list includes common manufacturer defaults.	Pass
2.1.1	Change vendor-supplied defaults for wireless environments. A device fails if the passphrases, SSIDs or other security-related settings are on a list of forbidden values. The list includes common manufacturer defaults.	Pass
4.1.1	Use strong encryption in wireless networks.	Pass

Figure 5: The PCI Report provides an at-a-glance view of compliance status, along with detailed information about what issues need to be addressed.

5. Summary

Network security is only as strong as the weakest point in the infrastructure, and unfortunately, well-meaning employees and malicious attackers to create security gaps. Wireless scans alone cannot defend organizations against all threats from rogue access points. The combination of integrated wired and wireless scans is the most effective approach to detection and containment of rogue devices. To be successful at both goals, solutions must be able to accurately assess the threat levels of devices, provide a framework for prioritizing risk mitigation tasks and alert staff of threats based on the enterprise's specific security policies and requirements.

AirWave RAPIDS delivers highly accurate, extremely flexible, and cost-effective rogue detection and containment for any organization.

Feature	Benefit
Wireless scanning that	Time and cost savings. Eliminates the need to perform walk-arounds

leverages existing APs points and sensors	or to purchase additional RF sensors or dedicated servers.
Wireline scanning	Improved security. Enables a more accurate threat assessment, improving the efficiency of network staff. Allows organizations to detect rogues in remote offices and locations without wireless APs.
Rules-based threat classification	Time and resource savings. Allows staff to focus on the most important risk mitigation tasks. Comprehensive device classification that's tailored to the organization means less time spent investigating false-positives.
Automated alerts	Faster response times. Alerts staff the instant a rogue is detected, reducing reaction times and further improving security.
Rogue AP location and discovered device switch/port information	Faster threat mitigation. Greatly simplifies the task of securing rogue devices and removing potential threats.
Reporting	Reduced regulatory expense. Comprehensive rogue and audit reports helps companies comply with various industry standards and regulatory requirements.
IDS event management	Single point of control. Provides you with a full picture of network security. Improves security by aggregating data for pattern detection.
Manual and automated containment	Continuous security. Improves security by enabling immediate action even when network staff is not present

About Aruba Networks

Aruba is the global leader in distributed enterprise networks. Its award-winning portfolio of campus, branch/teleworker, and mobile solutions simplify operations and secure access to all corporate applications and services - regardless of the user's device, location, or network. This dramatically improves productivity and lowers capital and operational costs.

Listed on the NASDAQ and Russell 2000® Index, Aruba is based in Sunnyvale, California, and has operations throughout the Americas, Europe, Middle East, and Asia Pacific regions. To learn more, visit Aruba at arubanetworks.com. For real-time news updates follow Aruba on twitter.com/ArubaNetworks, or greenislandnews.blogspot.com.



1344 Crossman Ave. Sunnyvale, CA 94089-1113
Tel. 408.227.4500 | Fax. 408.227.4550 | 1-866-55-ARUBA
info@arubanetworks.com | <http://www.arubanetworks.com>