networktest

Protect the Air:

Testing Aruba Networks' RFProtect AirWave Capabilities to Detect and Repel WLAN Attacks

January 2011

Table of Contents

1 Executive Summary

It's a common misconception: Enterprise network managers too often assume strong encryption equals strong security for wireless LAN (WLAN) traffic.

Certainly, WPA2 Enterprise offers better authentication and encryption options than many organizations deploy in their wired networks. But WLANs involve many other potential vulnerabilities: Rogue access points (APs); denial-of-service attacks against clients; and targeted attacks against WLAN infrastructure all can lead to leakage of sensitive data. The threat to enterprise WLANs is real and growing[1].

The **RFProtect** capabilities in Aruba Networks' **ArubaOS** operating system for Mobility Controllers, along with the company's **AirWave Management System,** use deep knowledge of 802.11 WLAN protocols, correlated with information from the wired network, to detect, classify, and block attacks and wireless vulnerabilities.

Aruba commissioned Network Test and Brad "RenderMan" Haines, a widely known wireless penetration tester and speaker at security conferences, to assess the effectiveness of its network security products. Tests involved a battery of published and unpublished attacks, all conducted on a 20,000-square-foot over-the-air test bed.

Among the key findings of the security tests:

- ✓ ArubaOS and AirWave correctly detected 11 different forms of rogue APs
- ✓ In all cases attempted, multiple wireless intrusion detection (WIP) sensors – both Access Points and Air Monitors – simultaneously detected unauthorized devices and actions.
- ✓ In all cases attempted, the Aruba system effectively contained unauthorized clients and rogue APs, thus preventing leakage of enterprise data. Containment used wired as well as wireless methods to block attack traffic
- ✓ The AirWave RAPIDS intrusion detection software allowed quick, simple definition of custom rules, making it possible to match on multiple attack conditions
- ✓ ArubaOS correctly detected multiple forms of attack against wireless clients and wireless management infrastructure, including denial-of-service attacks

[1] While hard data on wireless LAN security incidents is difficult to come by, it's safe to say the size of the attack surface continues to expand. The Computer Security Institute's 2009 and 2010 enterprise security surveys report increases in malware infection, denial-of-service attacks, password sniffing, and targeted attacks. And IDC forecasts robust growth in WLAN equipment sales even under challenging economic circumstances.

- ✓ ArubaOS effectively correlated wired and wireless information to detect and block attacks. Correlation requires close integration with WLAN management infrastructure, and is not possible with standalone appliance-based approaches to WLAN security

This document is organized as follows. This section introduces the test project. Section 2 describes the features in ArubaOS and the AirWave Management Suite. Section 3 introduces the test bed. Section 4 describes rogue AP detection tests, while Section 5 describes rogue containment tests. Section 6 discusses penetration testing against WLAN clients, while Section 7 describes attacks against wireless infrastructure. An appendix at the end of this document describes the test bed infrastructure.

2 Introducing RFProtect and AirWave

Defense in depth – the use of multiple mechanisms to detect and repel attackers – is a best practice in network security. Enterprise network architects rely on multiple types of devices to protect the enterprise, including firewalls, virtual private network (VPN) concentrators, and intrusion detection/prevention systems (IDS/IPS), among others.

While these devices all have their place, they don't necessarily understand or integrate well with the wireless network. Given an ever-growing number of attacks that attempt to exploit 802.11 protocols, wireless-specific countermeasures are clearly needed.

Aruba extends the defense-in-depth concept with **RFProtect** capabilities **in ArubaOS** and with the **AirWave Management Suite.** Both leverage deep 802.11 protocol knowledge to detect, classify, block, and manage wireless security threats throughout the enterprise.

As the wireless security module for ArubaOS, **RFProtect** is the primary engine for detecting and classifying wireless attacks in real time. A key component is **RFProtect WIP,** discussed throughout this report.

Among other features, WIP continually observes the 2.4-GHz and 5-GHz bands using TotalWatch Air Monitoring; detects, classifies and contains rogue APs; and protects against denial-of-service (DoS) and client attacks. RFProtect also includes a built-in spectrum analyzer, discussed in Network Test's previous *Own the Air* report.

Tight integration with the ArubaOS controller platform makes it possible for RFProtect to detect some attacks, such as AP spoofing, that overlays and standalone appliance-based WIP solutions cannot effectively match.

The **AirWave Management Suite** accepts data from ArubaOS and other sources to provide a comprehensive picture of wired and wireless network security.

AirWave's software modules include VisualRF for location and mapping, including heat maps that show signal strength and rogue AP locations. For example, Figure 1 shows an AirWave VisualRF heat map that locates three rogue APs, indicated as triangles, along with eight legitimate APs and Air Monitors. Seen graphically, identification of rogue APs is quick and easy.

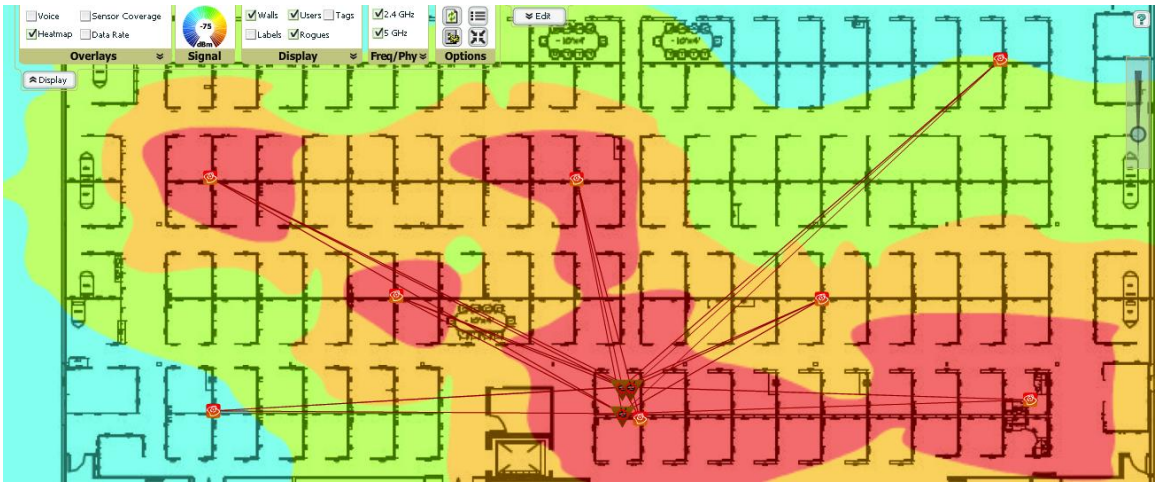
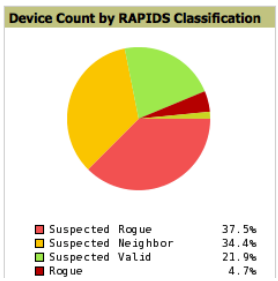


FIGURE 1: ROGUE AP LOCATION USING VISUALRF

IDS Events

Attack ▲	Last 2 Hours	Last 24 Hours	Total
Adhoc Network Detected	5	15	101
AP Flood Attack	0	0	32
AP Impersonation	0	0	29
AP Spoofing Detected	0	0	48
Block ACK Attack	24	123	987
Channel Rate Anomaly	0	0	6
Client Associating On Wrong Channel	2	5	21
Client Flood Attack	0	0	24
CTS Packets Rate Anomaly	7	21	41
Deauth Broadcast	0	0	173
Disassoc Broadcast Attack	0	0	46
Disconnect Station Attack	0	0	2
Hotspotter Attack	22	394	464
HT Greenfield support	0	0	36
Information Element Overflow	0	0	2
Invalid Address Combination	0	2	28
Invalid MAC OUI	4	65	215
Malformed Frame Wrong Channel Detected	2	16	38
Malformed HT Information Element	0	0	7
Node Rate Anomaly	3	20	68
RTS Packets Rate Anomaly	6	20	28
Station Associated to Rogue AP	114	2175	2465
Station Unassociated from Rogue AP	153	3243	3480
WEP Misconfiguration	2	2	12
Wireless Bridge Detected	1	1	1
25 Attack Types	345	6102	8354

Rogue Data



RAPIDS Classification	Devices
Contained Rogue	0
Rogue	3
Suspected Rogue	24
Unclassified	0
Suspected Neighbor	22
Neighbor	1
Suspected Valid	14
Valid	0
Total	64

FIGURE 2: RAPIDS OVERVIEW

Another AirWave module, RAPIDS, offers comprehensive wireless intrusion detection using relevant information from both the wired and wireless sides of the enterprise network. AirWave RAPIDS combines input from RFProtect WIP with data from the wired network, continually correlating data sets to report on threats using custom-defined rules. (AirWave RAPIDS also can correlate APs' wired MAC addresses and wireless BSSIDs, a useful capability in detecting rogue AP attachments.)

AirWave RAPIDS offers comprehensive and intuitive reporting on network security events. Figure 2 shows the AirWave RAPIDS overview screen, which reports on attacks and rogue data at a glance. Much more detailed reporting also is possible via custom report definitions, configurable alerting, and the detailed logging stored in the product.

Custom classification is a key feature in AirWave RAPIDS, helping to identify specific security issues. For example, as discussed below in the "Rogue AP Detection" section, a network manager may wish to define rules to match only a particular vendor of possible rogues, or only a specific SSID pattern (perhaps using wildcards), or some combination of these.

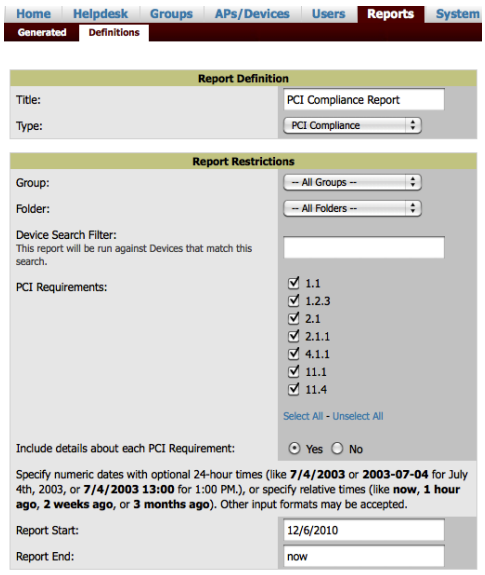


FIGURE 3: PCI COMPLIANCE REPORTING

AirWave RAPIDS' custom report definition also can be helpful in ensuring regulatory compliance. Enterprises that handle credit card transactions, for example, are obligated to follow the Payment Card Industry Data Security Standard (PCI DSS) standards. PCI compliance is a complex topic, with different requirements depending on whether an organization holds, processes, or exchanges cardholder information. Enterprises face many additional requirements when performing any of these tasks over WLANs; at least seven different sections of PCI apply just to wireless intrusion prevention. Regular security auditing is one of these requirements, and AirWave RAPIDS has custom rules to help fulfill that requirement.

Figure 3 shows the AirWave RAPIDS custom reporting screen for PCI compliance. Rather than defining custom conditions for every PCI requirement (a task that could involve hundreds of steps), the custom report generator uses check boxes for each section of PCI. Simply by checking the relevant sections, the network manager can produce a report on current PCI compliance.

3 The Aruba Security Test Bed

Network Test assessed the ability of ArubaOS RFProtect and AirWave RAPIDS to detect, classify, and block a wide range of rogue AP attempts. We also conducted penetration tests targeting both wireless clients and the wireless infrastructure.

Figure 4 illustrates the physical layout used for security testing. Aruba leased an empty 40,000-square-foot office building with many of the conditions faced by organizations deploying 802.11 networks – dozens of cubicles, carpeting, brick-on-steel construction, and occasional intermittent signals from outside sources.

Network Test and Aruba conducted all tests on the building's first floor, show in Figure 4. Into this space of roughly 20,000 square feet, Aruba deployed eight Aruba AP-105 802.11n APs, and configured two of these to function as Air Monitors (labeled AM). The other six access points (labeled AP) offered connectivity in both the 2.4- and 5-GHz bands and performed wireless

security scanning as well. Engineers also used up to five rogue access points (not shown) in rogue containment testing.

FIGURE 4: THE ARUBA SECURITY TEST BED

The building's data center was on the second floor. It housed an Aruba 3400 controller; an AirWave management server; a Layer 2/3 Ethernet switch; and patch panels connected to Ethernet drops throughout the building. Network Test also assessed Aruba's Remote AP (RAP) in one test case, discussed below; RAP functionality is identical to that of the AP-105.

The Aruba controller, AirWave server, and Aruba APs were the only authorized networking devices in use. **No other equipment was needed for secure connectivity** (such as firewalls, VPNs, IDS/IPS, or 802.11 management appliances).

Also, unless otherwise noted, test engineers used the same setup with six APs and two air monitors in all tests. Again, **no special configuration beyond the intuitive WIP Wizard was required to repel the various attempted attacks and security scans. Figure 5 shows the WIP wizard, with guided templates for defining intrusion detection policies.**

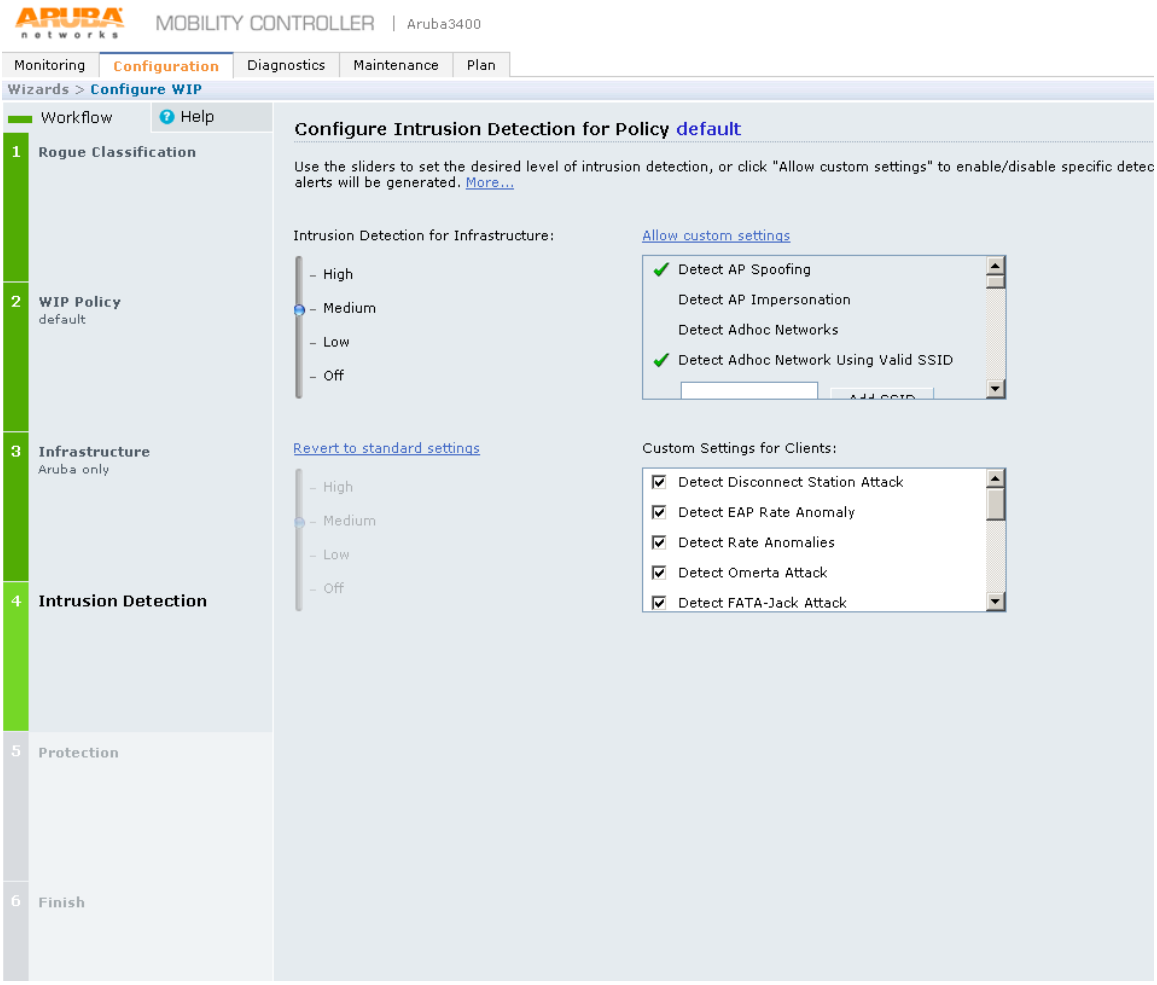


FIGURE 5: DEFINING INTRUSION DETECTION POLICIES WITH THE WIP WIZARD

As usual in open-air testing, engineers began with baseline measurements to determine whether the test environment was “clean” from an RF perspective. Measurements from the spectrum analyzer in RFProtect confirmed that the test bed was relatively free from outside interference. As noted, the SSIDs of APs outside the building appeared, but typically with a weak signal strength of -80 dBm or less. Thus, test engineers were confident they had control of the RF spectrum for all tests.

4 Rogue Detection in Depth

Rogue AP testing is often too simple: Just put up an unauthorized AP, log whether the system under test saw the rogue's SSID, and call the test a success.

In fact, enterprise-grade rogue detection is far more complex and nuanced, involving numerous variations: Does the rogue AP use a valid or invalid SSID? Is the rogue AP attached to the enterprise Ethernet network, or not? What if multiple rogues appear on the same channel or on a channel between or outside those allowed in a given regulatory domain? Can spoofing of a legitimate AP be detected?

ArubaOS RFProtect and AirWave RAPIDS defend the enterprise infrastructure against these and other attacks with a variety of detection mechanisms. Aruba does not simply classify all non-valid APs as rogues, but instead uses a more intelligent classification algorithm. ArubaOS RFProtect will discover all APs in the RF neighborhood at a basic level as interfering. Depending on the threat they pose, the Aps get classified into different levels such as rogues or suspected rogues. There is even a more granular concept of "confidence level" to assess the threat level presented by each device.

Network Test and Aruba identified 11 different rogue AP scenarios, and verified the Aruba system's ability to detect rogue APs in each case.

Rogue Detection With Invalid SSID

Rogue APs with invalid SSIDs represent the most common problem when it comes to protecting enterprise networks. The intent isn't necessarily malicious in such cases: Often an employee may attach an off-the-shelf wireless router to the enterprise network without realizing that doing so with an unmanaged, unauthorized AP violates security policy.

Not all invalid-SSID uses are benign, however. An attacker might use a wireless router in the hopes of luring authorized client PCs to associate to the rogue AP, leading to a compromise of confidential data. Either way, **the enterprise network manager must be made aware whenever an invalid SSID appears on the enterprise network.**

Aruba RFProtect WIP and AirWave RAPIDS detect interfering APs by correlating the BSSIDs in frames seen over the air with traffic seen on the wired network. If no correlation occurs, the access point may belong to a neighbor; for example, imagine a situation where a neighboring restaurant and book store each offer wireless access for customers. If there is a correlation between frames seen on the wired and wireless networks, the Aruba WLAN system classifies the AP as a suspected rogue. (More fine-grained control is also possible, as discussed in later scenarios.)

Network Test validated the ability of the Aruba WLAN system to detect a rogue AP by attaching a consumer-grade wireless router to the enterprise network. **Detection was nearly instantaneous, with detection occurring within one second of the rogue AP becoming operational.**

Figure 6 shows the status message from RFProtect WIP, noting the presence of a rogue AP on the enterprise network. Since the SSID of "NETGEAR" was invalid, the Aruba WLAN system classified the AP as a rogue.

Note also in the figure that "Marked to Contain" is enabled. As discussed below in the "Rogue Containment" section, the Aruba WLAN system offers multiple mechanisms to ensure no client will be able to associate with rogue APs. We'll discuss rogue containment in more detail below, but note here that the client count is zero: No client could associate with the AP once the Aruba WLAN system classified it as a rogue.

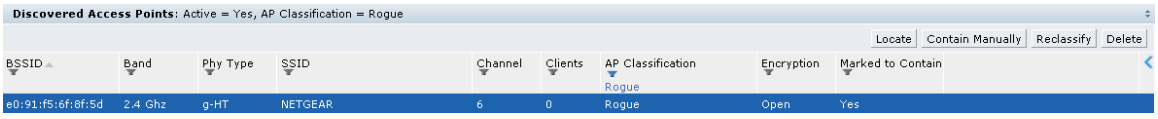


FIGURE 6: DETECTION OF ROGUE AP WITH INVALID SSID

Rogue Detection With Valid SSID

Rogue APs with valid SSIDs pose a special challenge for wireless users: How can they tell which AP is legitimate?

RFProtect WIP mitigates this problem by monitoring the BSSID of each beacon frame advertising a valid SSID. Since APs send beacons every 100 milliseconds by default, and since the Aruba WLAN system knows which BSSIDs are legitimate, it can quickly determine when a rogue AP appears.

As in the test case with an invalid SSID, **RFProtect WIP detected a rogue AP using a valid SSID within one second** of its becoming operational. Here again, no client association was possible because rogue containment was enabled.

In this case, the system classified the rogue AP because test engineers configured the Aruba WLAN system to do so. RFProtect WIP automatically generates an alert whenever a rogue AP uses a valid SSID. However, the system does not automatically classify the AP as a rogue or suspected rogue. For that, users can define custom classification rules using AirWaveRAPIDS – the topic of our next scenario.

Rogue Detection With Custom Classification

It is often desirable to classify APs that match multiple conditions. For example, network managers may notice a recurring problem with APs that use variations on a given SSID *and* operate within a given range of signal strengths *and* appear only on the wireless but not the wired LAN.

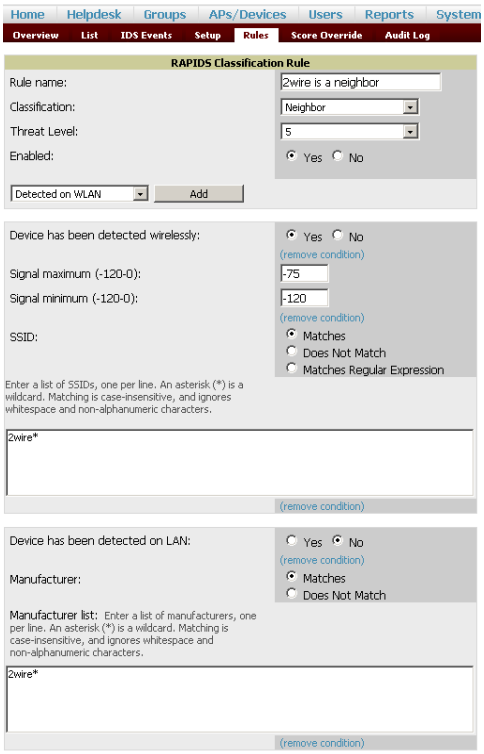


FIGURE 7: CUSTOM RULE DEFINITION

AirWave RAPIDS offers classification menus that make it simple to define custom detection and containment rules. Rule definition is straightforward, and can rely on combinations of up to 13 wired and wireless conditions.

As shown in Figure 7, rule definition involves a series of menus. In this case, a custom rule defines a case where any 2wire AP should be classified as a neighbor based on four conditions: It is detected only on the wireless network; its signal strength is between -75 and -120 dBm; its SSID matches a pattern beginning with "2wire" (note the use of a wildcard search pattern); and the rogue AP's BSSID uses an organizationally unique identifier (OUI) that shows 2wire to be its manufacturer.

Once a custom classification rule is defined, AirWave RAPIDS displays it alongside existing rules, as shown in Figure 8. In this case, different rules trigger different actions. RAPIDS classifies an unauthorized AP detected on wired and wireless networks as a rogue; classifies those with signal strength of greater than -75 dBm as suspected rogues; and as in our example above, classifies 2wire APs as neighbors.

As with many other access-control systems, rule order is important. AirWave RAPIDS operates on a "first-match" basis, where classification is based on the first rule that applies. Aruba recommends that rules be ordered from highest to lowest threat levels (e.g., with rules for rogues placed before rules for neighbors). If a device hits multiple rules, it will be classified by the first rule it matches. Subsequent rule matches may move a device upward in classification, but not lower. For example, a neighbor may be reclassified as a rogue, but not vice-versa.

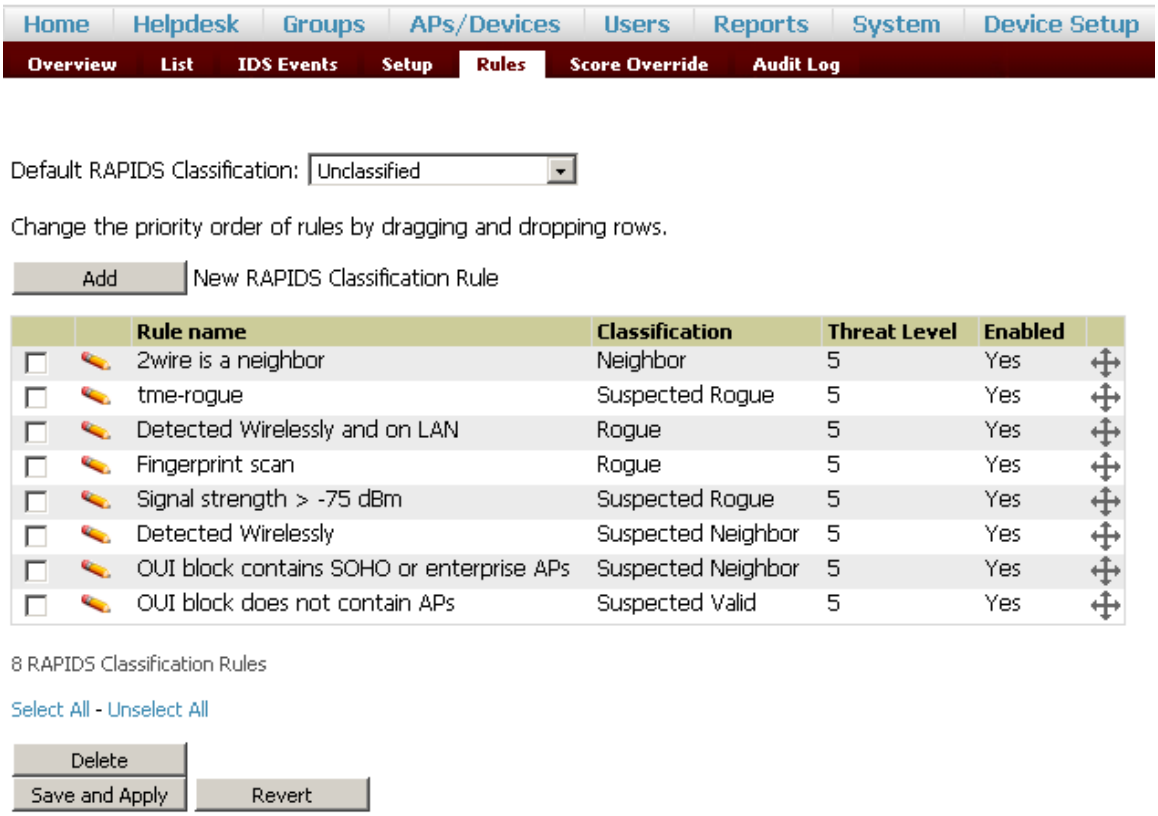


FIGURE 7: CUSTOM CLASSIFICATION RULE LIST

As in the previous tests, **detection was nearly instantaneous for an AP matching the 2wire rule**. RFProtect and RAPIDS correctly identified a 2wire AP and classified it as a neighbor, all in less than one second after its discovery by an Aruba RFProtect WIP sensor.

Mid-Channel AP Interference

A comprehensive rogue detection service must work not only *on* the expected 802.11 channels but also *between* channels. While regulatory domains define a set number of channels in the 2.4- and 5-GHz bands, it's trivially easy for an attacker to set up a rogue AP on a nearby channel, where it would not be detected by most WIP solutions, and then pull data from the wired network.

ArubaOS RFProtect WIP defends against this form of rogue attack by monitoring the entire spectrum in the 2.4- and 5-GHz bands. If RFProtect WIP detects a correlation between wired traffic and an AP operating on a "mid" channel, it will classify the offending AP as a rogue.

Network Test observed the ability of the system not only to classify a mid-channel rogue but also to locate it. As seen in Figure 9, the Aruba 3400 controller detected and classified a rogue AP operating on Channel 164, which isn't part of any regulatory domain, but is adjacent to Channel 165, which is valid.

Discovered Access Points: Active = Yes, AP Classification = Rogue

BSSID	Band	Phy Type	SSID	Channel	Clients	AP Classification
						Rogue
00:11:f5:43:b2:7f	5 Ghz	a	Sensor Coverage Survey	164	0	Rogue

FIGURE 8: MID-CHANNEL ROGUE AP DETECTION

By triangulating data received from the Aruba Air Monitors, AirWave RAPIDS also reported on the location on the mid-channel interference source, as shown in Figure 10. The red circle in the diagram accurately pinpoints the location of the mid-channel rogue AP.

Discovery Events

1-10 of 10 Discovery Events Page 1 of 1 Choose Columns CSV Export

RSSI	Signal	Channel	SSID	WEP	WPA	BSSID	Network Type	IP Address	Time	Discovery Method	Discovery Agent
			- All -	- All -	- All -	- All -	- All -	- All -		- All -	- All -
42	-70	164	Sensor Coverage Survey	No	No	00:11:F5:43:B2:7F	AP	-	12/6/2010 4:50 PM	Wireless AP scan	ap105-7
41	-71	164	Sensor Coverage Survey	No	No	00:11:F5:43:B2:7F	AP	-	12/6/2010 4:50 PM	Wireless AP scan	ap105-3

FIGURE 9: LOCATING MID-CHANNEL INTERFERENCE

Rare Channel AP Interference

Devices operating in the 4.9-GHz public-safety band represent another potential interference source. Devices in this band can pose a threat to APs operating on valid lower 5-GHz channels. An attacker armed with this knowledge could affect connectivity for clients with 5-GHz radios.

In the recently released ArubaOS 6.0 **RFProtect introduces TotalWatch, a capability that allows AMs to scan around as well as between regulatory domain channels.** In this case, that means detecting devices in the 4.9-GHz band and correlating those signals with any traffic seen on the wired network.

To verify the Aruba system's ability to detect rare-channel traffic, test engineers used a specially constructed AP capable of generating traffic in the 4.9-GHz band. Engineers also attached this AP to the wired network.

As shown in Figure 11 below, **RFProtect immediately identified the rogue AP operating on the rare channel.** The system detected an AP operating on channel 184, which is at 4.920 GHz, below the lowest 5-GHz regulatory channel in most countries[2].

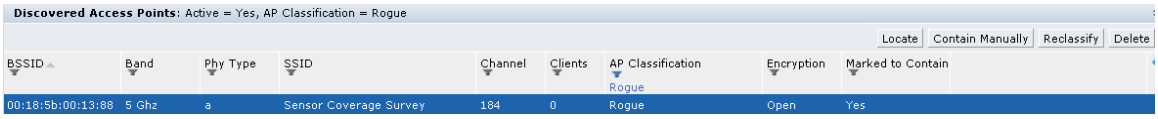


FIGURE 10: RARE CHANNEL AP DETECTION

In such cases, where the WIP cannot transmit outside regulatory domain channels and hence cannot contain such rogues, Aruba RFProtect and AirWave RAPIDS offer the invaluable ability to contain such devices on the wired network. Wired containment is not bound by the regulatory domain constraints APs and AMs face, and thus offers a more effective containment solution.

Multiple Rogue APs on the Same Channel

At the very least, the appearance of multiple rogue APs on the same channel will unfairly consume bandwidth. A benign example of this is the attachment of multiple unauthorized wireless routers, all set to the default channel. A less benign example occurs when an attacker seeks to confuse the wireless intrusion prevention system or tie up channel bandwidth by putting multiple rogue APs on a single channel.

ArubaOS RFProtect WIP can protect clients against multiple rogue APs using the same channel. As in previous rogue detection cases, RFProtect WIP will detect each rogue AP by correlating its wired and wireless traffic. (If necessary, another ArubaOS feature called band steering will move clients away from heavily utilized channels as needed.)

Network Test validated the ability to detect multiple rogue APs on the same channel by attaching two off-the-shelf wireless routers to the test network. ArubaOS **RFProtect WIP detected both rogue APs on the same channel, while AirWave VisualRF pinpointed their locations.**

Figure 12 below shows the rogue detection messages from RAPIDS[3], with the rogue APs using SSIDs of “tme-linksys” and “tme-gr-netgear.”

[2] Channel 184 is permitted in Japan, but is not permitted in other countries.

[3] Sharp-eyed readers will note a five-minute gap between detection times in the AirWave RAPIDS screen. These indicate initial detection times for a test run multiple times, and not a five-minute delay in identifying a second rogue. In practice, rogue detection was nearly instantaneous after each rogue AP booted up on the test network.

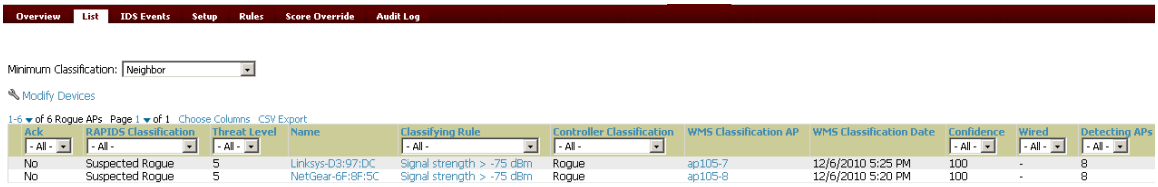


FIGURE 11: AIRWAVE RAPIDS IDENTIFIES 2 ROGUE APS

Multiple Rogue APs on Multiple Channels

As should be abundantly obvious by now, **rogue APs can appear anywhere, anytime. An intrusion detection system (IDS) that scans only one channel may miss the introduction of multiple rogue APs on multiple channels.**

ArubaOS RFProtect WIP and AirWave RAPIDS guard against that possibility by correlating data from multiple input sources. In addition to the two dedicated Air Monitors that continuously scanned all channels, the six AP105s on the test bed periodically scanned for interference sources as well. Since scan cycles of the APs were independent of one another, **the APs were able to find rogue APs on any channel relatively fast.**

To evaluate detection of multiple rogue APs on different channels, test engineers configured off-the-shelf wireless routers on channels 1, 6, and 11 in the 2.4-GHz band. As shown in Figure 13 below, AirWave **RAPIDS detected the three rogue APs on multiple channels.** Note the use of different SSIDs and channels at the right of the figure.

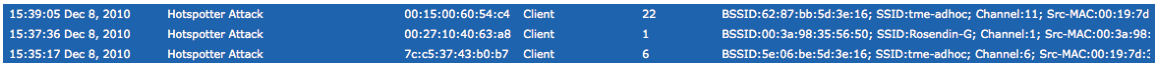


FIGURE 12: DETECTION OF MULTIPLE ROGUE APS ON MULTIPLE CHANNELS

Ad-hoc Rogue APs With Invalid SSIDs

While all detection tests thus far have involved rogue APs operating in infrastructure mode, rogue APs acting in ad-hoc mode also can pose a security threat. Thus, **an enterprise-grade rogue detection system must be able to detect and classify rogue APs operating in ad-hoc as well as infrastructure modes.**

Ad hoc rogues may represent benign accidents (e.g., a user unwittingly enabling ad-hoc mode on a notebook PC using an invalid SSID) rather than a targeted attack. Even so, a benign accident can induce client PCs to roam away from authorized APs, leading to potential data leakage.

To verify the ability of the Aruba WLAN system to detect and classify rogue APs, test engineers configured two Windows laptops to operate in ad-hoc mode, with one using an invalid SSID and

the other a valid SSID. (The next section discusses detection of ad-hoc mode rogue APs using valid SSIDs.)

The Aruba WLAN system detected the ad-hoc rogue APs nearly instantaneously, just as with infrastructure-mode rogue APs. Figure 14 shows the rogue detection messages from AirWave RAPIDS.

1-172 of 172 IDS Events Page 1 of 1 Choose Columns CSV Export

Severity	Category	Scope	Attack	Detail	Count	Attacker	Target	Time	AP/Device
- All -	- All -	- All -	- All -			- All -	- All -		- All -
Low	Policy Compliance Issue	Client	Adhoc Network Detected	Adhoc Network Detected	-	CE:F9:13:81:4C:21	90:27:E4:F8:EB:C3	12/6/2010 6:02 PM	ap105-2
Low	Policy Compliance Issue	Client	Adhoc Network Detected	Adhoc Network Detected	-	CE:F9:13:81:4C:21	90:27:E4:F8:EB:C3	12/6/2010 6:02 PM	ap105-2
Low	Policy Compliance Issue	Client	Adhoc Network Detected	Adhoc Network Detected	-	CE:F9:13:81:4C:21	90:27:E4:F8:EB:C3	12/6/2010 6:02 PM	ap105-5
Low	Policy Compliance Issue	Client	Adhoc Network Detected	Adhoc Network Detected	-	CE:F9:13:81:4C:21	90:27:E4:F8:EB:C3	12/6/2010 6:02 PM	ap105-5
Low	Policy Compliance Issue	Client	Adhoc Network Detected	Adhoc Network Detected	-	CE:F9:13:81:4C:21	90:27:E4:F8:EB:C3	12/6/2010 6:02 PM	ap105-8
Low	Policy Compliance Issue	Client	Adhoc Network Detected	Adhoc Network Detected	-	CE:F9:13:81:4C:21	90:27:E4:F8:EB:C3	12/6/2010 6:02 PM	ap105-8
Low	Policy Compliance Issue	Client	Adhoc Network Detected	Adhoc Network Detected	-	CE:F9:13:81:4C:21	90:27:E4:F8:EB:C3	12/6/2010 6:01 PM	ap105-4
Low	Policy Compliance Issue	Client	Adhoc Network Detected	Adhoc Network Detected	-	CE:F9:13:81:4C:21	90:27:E4:F8:EB:C3	12/6/2010 6:01 PM	ap105-4
Low	Policy Compliance Issue	Client	Adhoc Network Detected	Adhoc Network Detected	-	00:39:94:E6:81:F5	00:C0:CA:21:9D:FB	12/6/2010 6:01 PM	ap105-2
Low	Policy Compliance Issue	Client	Adhoc Network Detected	Adhoc Network Detected	-	00:39:94:E6:81:F5	00:C0:CA:21:9D:FB	12/6/2010 6:01 PM	ap105-2

FIGURE 13: AIRWAVE RAPIDS IDENTIFIES AD-HOC ROGUE APS

Ad-hoc Rogue APs With Valid SSIDs

An ad-hoc rogue AP may represent something less benign than an authorized user's accidental misconfiguration. For example, an attacker could attempt to lure clients to associate by using a valid SSID in ad-hoc mode. **With both invalid and valid SSIDs, the rogue detection system must be able to detect, classify, and act on ad-hoc mode rogue APs as they appear.**

As noted in the previous section, test engineers put two rogue APs into ad-hoc mode, and one of these used a valid SSID of "tme-gr." As shown in Figure 14, **the ArubaOS RFProtect WIP system correctly detected and classified the ad-hoc rogue AP using a valid SSID. Detection was nearly instantaneous after the rogue AP's appearance on the network.**

Spoof Detection

Attackers can impersonate legitimate APs by spoofing both SSIDs and BSSID(s). **Because it is so difficult to detect, AP spoofing is the most insidious rogue attack.** Spoof detection requires comparison and correlation of many parameters, including beacon rates for each BSSID, sequence numbers in data frames, signal strengths, and various driver-level heuristics.

Detecting spoofed APs requires 802.11 management and intrusion detection to be performed on the same platform, since neither overlay management systems nor appliance-based IDS systems alone receive all necessary information. **ArubaOS RFProtect WIP and AirWave RAPIDS easily detected a spoofed AP,** as shown in Figure 15.

1-114 of 114 IDS Events Page 1 of 1 Choose Columns CSV Export

	Severity	Category	Scope	Attack	Detail	Count	Attacker	Target	Time	AP/Device
	- All -	- All -	- All -	- All -			- All -	- All -		- All -
	Highest	Vulnerability	AP	AP Spoofing Detected	AP Spoofing Detected	-	00:24:6C:B7:B4:C0	00:24:6C:B7:B4:C0	12/6/2010 5:53 PM	ap105-1
	Highest	Vulnerability	AP	AP Spoofing Detected	AP Spoofing Detected	-	00:24:6C:B7:B4:C0	00:24:6C:B7:B4:C0	12/6/2010 5:53 PM	ap105-1
	Highest	Vulnerability	AP	AP Spoofing Detected	AP Spoofing Detected	-	00:24:6C:B7:B4:C0	00:24:6C:B7:B4:C0	12/6/2010 5:51 PM	ap105-1
	Highest	Vulnerability	AP	AP Spoofing Detected	AP Spoofing Detected	-	00:24:6C:B7:B4:C0	00:24:6C:B7:B4:C0	12/6/2010 5:51 PM	ap105-1
	Low	Exploit	AP	AP Impersonation	AP Impersonation	-	-	00:24:6C:B7:B4:C0	12/6/2010 5:51 PM	ap105-1
	Low	Exploit	AP	AP Impersonation	AP Impersonation	-	-	00:24:6C:B7:B4:C0	12/6/2010 5:51 PM	ap105-1
	Low	Exploit	AP	AP Impersonation	AP Impersonation	-	-	00:24:6C:B7:B4:C0	12/6/2010 5:51 PM	ap105-6
	Low	Exploit	AP	AP Impersonation	AP Impersonation	-	-	00:24:6C:B7:B4:C0	12/6/2010 5:51 PM	ap105-6

FIGURE 14: RAPIDS REPORTS AP SPOOFING

802.11n Rogue APs

Comprehensive wireless security includes the ability to detect any type of rogue AP, including newer 802.11n devices. **Only 802.11n-capable APs and Air Monitors can detect 802.11n headers and modulation schemes. Older 802.11a/b/g devices will not detect 802.11n-capable rogue APs.**

In testing, ArubaOS **RFProtect WIP detected and located an 802.11n rogue AP using an invalid SSID.** As shown in Figure 16, RFProtect WIP correctly discovered the rogue AP as using 802.11n (indicated by its use of g-HT [2.4-GHz high throughput] PHY and MAC enhancements).

In Figure 17, VisualRF shows the location of the 802.11n rogue AP (indicated by a red ID tag and the invalid SSID of “NETGEAR”).

Discovered Access Points: Active = Yes, AP Classification = Rogue

Locate | Contain Manually | Reclassify | Delete

BSSID	Band	Phy Type	SSID	Channel	Clients	AP Classification	Encryption	Marked to Contain
						Rogue		
e0:91:f5:6f:8f:5d	2.4 Ghz	g-HT	NETGEAR	6	0	Rogue	Open	Yes

FIGURE 15: DETECTION OF 802.11N ROGUE AP

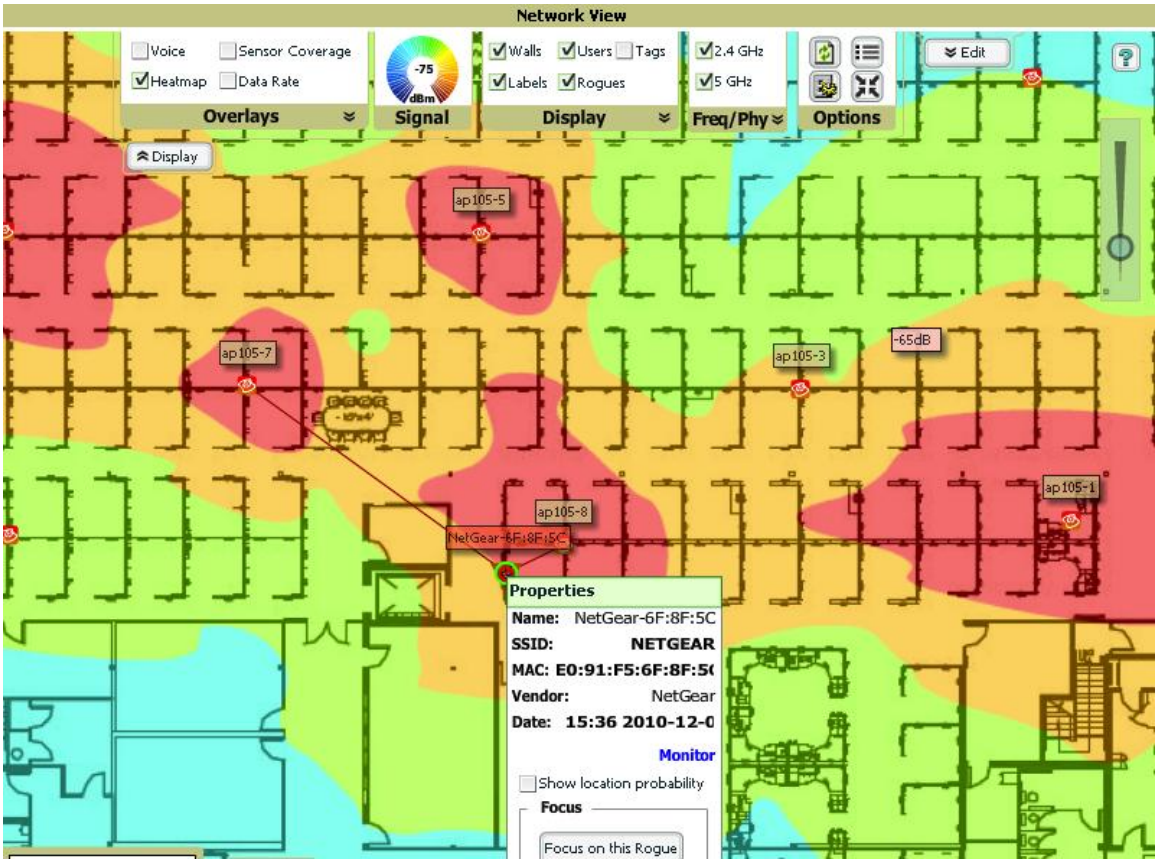


FIGURE 16: LOCATION OF 802.11N ROGUE AP

5 Rogue Containment: Stopping Attackers in Their Tracks

Detecting and classifying various types of rogue APs is important, but it's only half the battle. **An effective wireless defense system also must contain attackers, preventing them from gaining network access once a rogue AP is detected.**

Most detection scenarios discussed thus far classified unauthorized APs as rogues, and acted to contain any traffic matching that classification. But it's worth considering what "containment" actually does. **ArubaOS RFProtect offers multiple mechanisms to repel attackers,** including deauthentication, tarpitting, and two forms of wired containment. **Containment also can extend to remote offices,** as validated by tests using the Aruba Remote AP (RAP).

Deauthentication

The simplest form of client containment is deauthentication. Here, the Aruba APs transmit 802.11 deauthentication frames to clients, effectively preventing them from associating with a rogue AP (once it's been detected and classified).

Tarpit Containment

Tarpitting is an innovative containment method that uses rogue methods to fight rogue APs. Here, instead of sending a continuous stream of deauthentication frames, an Aruba AP either uses a fake BSSID for the rogue AP, or uses the rogue AP's SSID but advertises it on a different channel. Either way, clients are enticed to associate with a safe (quarantined) AP faked by an Aruba AP rather than the rogue AP.

Tarpit containment may prove more efficient in terms of bandwidth utilization in some scenarios. Tarpitting makes sense, for example, in settings where rogue APs are spread across channels and there are more clients to be contained than legitimate APs can handle. In such settings, tarpitting is likely to use less channel capacity than deauthentication.

Wired Containment

ArubaOS RFProtect WIP and AirWave RAPIDS offer two mechanisms that thwart rogue APs from an unexpected front – the wired network.

The first wired containment mechanism detects a rogue AP's MAC address on the wired network and then poisons the Ethernet switch's ARP cache with a fake entry for rogue AP's port, thus preventing traffic from reaching the rogue AP. Detection is possible because of ArubaOS RFProtect's ability to correlate wired and wireless traffic patterns.

The second mechanism is even more comprehensive: Upon detection of a rogue AP's attachment to the wired network, AirWave RAPIDS can issue a command to disable the rogue AP's switch port. No further communication is possible.

Putting It All Together

Network Test verified the effectiveness of all four containment mechanisms in separate tests. **ArubaOS RFProtect successfully contained rogue APs in all four test cases.**

Figure 18 shows the Aruba controller's report for containment using three of those mechanisms: wired containment using ARP poisoning; tarpit containment; and deauthentication.

14:48:51 Dec 8, 2010	AP Wired Containment	00:1d:7e:d3:97:dc	Infrastructure	21	MAC:00:1d:7e:d3:97:dc; Spoof-IP:168297657; Src-MAC:00:1d:7e:d3:97:db
14:41:01 Dec 8, 2010	Tarpit Containment	00:1d:7e:d3:97:dc	Infrastructure	335360	Channel:6; Channel:5; Src-MAC:00:1d:7e:d3:97:dc; MAC:00:13:e8:f8:aa:f1
14:40:59 Dec 8, 2010	AP Deauth Containment	00:1d:7e:d3:97:dc	Infrastructure	1768	SSID:tme-linksys; Channel:6; MAC:00:13:e8:f8:aa:f1

FIGURE 17: MULTIPLE FORMS OF ROGUE AP CONTAINMENT AT WORK

For the final form of containment, involving the shutdown of an Ethernet switch port, a Network Test engineer inspected the switch's configuration file before and after ArubaOS RFProtect WIP issued a command to disable the port. As expected, the switch configuration indicated that the rogue AP's port had been shut down.

6 Protecting Wireless Clients

ArubaOS RFProtect not only blocks rogue APs, but also offers safeguards for wireless clients. Using its knowledge of WLAN status and client associations, ArubaOS **RFProtect ensures valid clients do not inadvertently connect to unauthorized or unsecured networks.**

Network Test validated ArubaOS RFProtect's ability to protect clients in two sets of tests. The first tests involved a valid client attempting to associate with a rogue AP, using both invalid and valid SSIDs. In both cases, we assessed the ability of ArubaOS RFProtect's "Protect Valid Stations" feature to prevent unauthorized associations.

The second set of tests involved penetration attacks launched against clients, and gauged ArubaOS RFProtect's ability to thwart these attacks.

Valid Client on Unencrypted SSID

A valid client inadvertently associating to an unsecured, open SSID can cause leakage of confidential data. Although the SSID may not necessarily be malicious (and hence should not be completely contained), it's still essential to take steps to ensure that valid clients do not stray.

To evaluate this scenario, test engineers attached a rogue AP with an invalid SSID to the test network. Engineers ran the scenario multiple times, looking to determine whether the Aruba RFProtect system would detect each roaming event to a rogue AP. As shown in Figure 19, **ArubaOS RFProtect immediately reported that a client had associated to a rogue AP** using an invalid SSID of "tme-linksys."

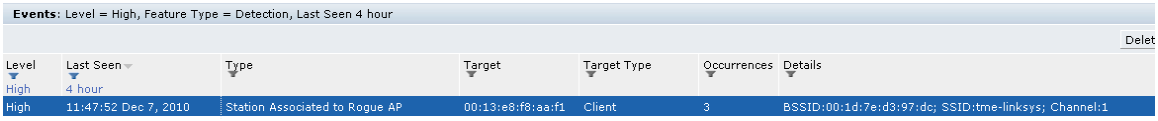


FIGURE 18: CLIENT ASSOCIATES TO ROGUE AP

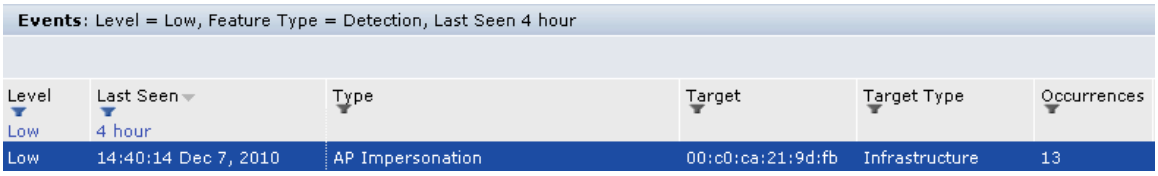
Detection and containment was possible because the Aruba WLAN system could correlate authorized clients and APs. This is another case where it's essential to integrate WLAN management and intrusion prevention onto one platform so the WIP can distinguish between valid and invalid clients.

Valid Client on Rogue AP With Valid SSID

So-called "honeypot" attacks can be very dangerous. Here, an attacker uses a valid SSID with the intent of luring clients to associate with a rogue AP. Obtaining the valid SSID is easy to do:

It's contained in every probe request that clients transmit. The attacker then sends probe responses to those clients, which in turn may associate with the rogue AP. The honeypot attack can be thwarted by checking valid and invalid BSSIDs and client associations.

Test engineers validated the ability to identify a honeypot attack by configuring an off-the-shelf wireless router to use a valid SSID seen on the test network. As shown in Figure 20, **the Aruba WLAN system correctly detected the invalid AP as a rogue. Because the Aruba controller and ArubaOS RFProtect WIP work together, it's possible to construct rules that will contain the rogue, as described above in the "Rogue Containment" discussion.**



Events: Level = Low, Feature Type = Detection, Last Seen 4 hour

Level	Last Seen	Type	Target	Target Type	Occurrences
Low	4 hour				
Low	14:40:14 Dec 7, 2010	AP Impersonation	00:c0:ca:21:9d:fb	Infrastructure	13

FIGURE 19: HONEYPOT DETECTION

Penetration Attacks Against Valid Clients

In addition to using rogue APs, attackers may also directly target wireless clients. **There are a number of DoS attacks specific to wireless clients. Wired network security appliances may be unable to detect such attacks.**

To determine the ability of the Aruba WLAN system to safeguard clients against such attacks, wireless security consultant Bradley Haines developed a series of attacks for this test targeting both wireless clients and infrastructure.

Disconnect Station Attacks

An attacker can use FakeAP, a widely used penetration testing tool, to flood the airwaves with arbitrarily large numbers of SSIDs and/or BSSIDs. The intent is not always malicious; the penetration tester may be looking to determine how readily clients will roam to neighboring APs not attached to the enterprise network. Benign or not, the effect is that clients may disconnect from the enterprise network, potentially leading to data leakage.

As shown in Figure 21 below, **AirWave RAPIDS detected the appearance of multiple rogue APs as they appeared.**

1-32 of 32 IDS Events Page 1 of 1 Choose Columns CSV Export

Severity	Category	Scope	Attack	Detail	Count	Attacker	Target	Time	AP/Device	Radio	Controller
- All -	- All -	- All -	AP Flood Attack			- All -	- All -		- All -	- All -	- All -
Low	Exploit	Probe	AP Flood Attack	AP Flood Attack	-	-	-	12/7/2010 1:12 PM	ap105-4	802.11bgn	Aruba3400
Low	Exploit	Probe	AP Flood Attack	AP Flood Attack	-	-	-	12/7/2010 1:12 PM	ap105-4	802.11an	Aruba3400
Low	Exploit	Probe	AP Flood Attack	AP Flood Attack	-	-	-	12/7/2010 1:12 PM	ap105-4	802.11bgn	Aruba3400
Low	Exploit	Probe	AP Flood Attack	AP Flood Attack	-	-	-	12/7/2010 1:12 PM	ap105-4	802.11an	Aruba3400
Low	Exploit	Probe	AP Flood Attack	AP Flood Attack	-	-	-	12/7/2010 1:12 PM	ap105-2	802.11bgn	Aruba3400
Low	Exploit	Probe	AP Flood Attack	AP Flood Attack	-	-	-	12/7/2010 1:12 PM	ap105-2	802.11an	Aruba3400
Low	Exploit	Probe	AP Flood Attack	AP Flood Attack	-	-	-	12/7/2010 1:12 PM	ap105-2	802.11bgn	Aruba3400
Low	Exploit	Probe	AP Flood Attack	AP Flood Attack	-	-	-	12/7/2010 1:12 PM	ap105-2	802.11an	Aruba3400
Low	Exploit	Probe	AP Flood Attack	AP Flood Attack	-	-	-	12/7/2010 1:12 PM	ap105-3	802.11bgn	Aruba3400
Low	Exploit	Probe	AP Flood Attack	AP Flood Attack	-	-	-	12/7/2010 1:12 PM	ap105-3	802.11an	Aruba3400

FIGURE 20: RAPIDS SEES DISCONNECT ATTACKS

Client Flooding Attacks

The opposite of a disconnect station attack is a client flood. Here, **an attacker injects traffic from arbitrarily large numbers of fake clients, all looking to gain access to the enterprise network.** Given enough fake clients, channel capacity will become constrained and valid clients may lose connectivity.

Network Test verified that the Aruba WLAN system successfully defended against client flooding attacks. As shown in Figure 22, the Aruba system correctly identified each instance of a fake client. This is yet another example where AirWave and ArubaOS RFProtect work together to distinguish between valid and invalid clients.

1-20 of 20 IDS Events Page 1 of 1 Choose Columns CSV Export

Severity	Category	Scope	Attack	Detail	Count	Attacker	Target	Time	AP/Device	Radio	Controller
- All -	- All -	- All -	Client Flood Attack			- All -	- All -		- All -	- All -	- All -
Low	Exploit	Probe	Client Flood Attack	Client Flood Attack	-	-	-	12/7/2010 1:16 PM	ap105-6	802.11an	Aruba3400
Low	Exploit	Probe	Client Flood Attack	Client Flood Attack	-	-	-	12/7/2010 1:16 PM	ap105-6	802.11bgn	Aruba3400
Low	Exploit	Probe	Client Flood Attack	Client Flood Attack	-	-	-	12/7/2010 1:16 PM	ap105-6	802.11bgn	Aruba3400
Low	Exploit	Probe	Client Flood Attack	Client Flood Attack	-	-	-	12/7/2010 1:16 PM	ap105-6	802.11an	Aruba3400
Low	Exploit	Probe	Client Flood Attack	Client Flood Attack	-	-	-	12/7/2010 1:15 PM	ap105-7	802.11bgn	Aruba3400
Low	Exploit	Probe	Client Flood Attack	Client Flood Attack	-	-	-	12/7/2010 1:15 PM	ap105-7	802.11an	Aruba3400
Low	Exploit	Probe	Client Flood Attack	Client Flood Attack	-	-	-	12/7/2010 1:15 PM	ap105-7	802.11bgn	Aruba3400
Low	Exploit	Probe	Client Flood Attack	Client Flood Attack	-	-	-	12/7/2010 1:15 PM	ap105-7	802.11an	Aruba3400
Low	Exploit	Probe	Client Flood Attack	Client Flood Attack	-	-	-	12/7/2010 1:15 PM	ap105-3	802.11bgn	Aruba3400

FIGURE 21: AIRWAVE RAPIDS SEES CLIENT FLOOD

Block ACK Attacks

Attackers may exploit the "Block ACK" feature new to 802.11n, forcing a receiver to drop frames. While Block ACK conserves bandwidth compared with the older method of transmitting one acknowledgment for each data frame received, an attacker could manipulate Block ACK messages to force frame loss.

The 802.11n specification allows a transmitter to send an Add Block Acknowledgment (ADDBA) to a recipient, indicating a starting frame sequence number and a window size of frame sequence numbers that the receiver should expect.

The receiver silently accepts frames with sequence numbers inside the current window and delivers a Block ACK message once the window's sequence numbers have all been successfully received. The receiver then drops any frames received outside of the current window – and that's exactly what an attacker can exploit.

By spoofing the source (the victim in this case) and transmitting a fake ADDBA frame to the recipient, an attacker can advertise a window of sequence numbers not currently in use by the victim.

The result: The receiver will drop all frames from the victim. While ADDBAs are a type of management action frame, they are not protected with the management frame protection mechanisms introduced in IEEE 802.11w.

While no IDS will prevent a Block ACK attack, since any attacker can send any frame, it is nonetheless important to determine when they occur. Armed with knowledge such as the source of the attack, other measures such as containment can then protect clients.

Test engineers verified the ability of the Aruba WLAN system to detect Block ACK attacks by generating ADDBA frames with modified window sizes and ACK bitmaps. As shown in Figure 23, **AirWave RAPIDS successfully detected a Block ACK attack and identified its source.**

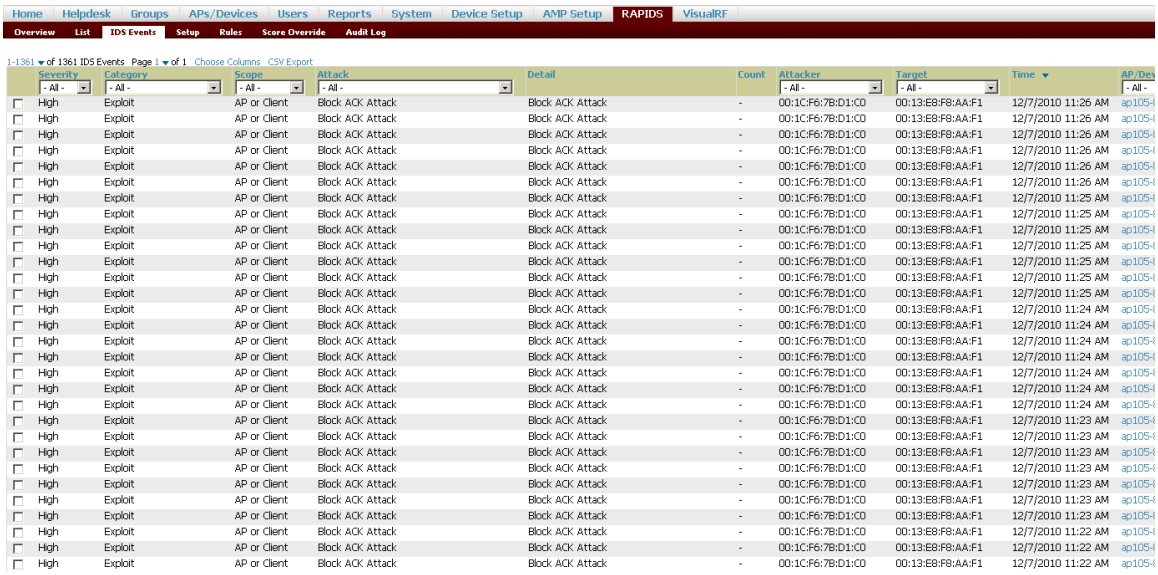


FIGURE 22: RAPIDS DETECTS BLOCK ACK DOS ATTACK

7 Protecting Wireless Infrastructure

Attackers may target wireless infrastructure components such as controllers and APs, putting both infrastructure and clients at risk. These attacks are often wireless-specific, and thus require specialized knowledge of 802.11 protocols on the part of the IDS.

To validate the ability of the Aruba WLAN system to detect and repel such attacks, Network Test and Aruba engineers used four penetration attacks targeting WLAN infrastructure: Broadcast attacks using deauthentication and disassociation messages; frame rate anomalies; and malformed 802.11n header contents. **In all four cases, the Aruba WLAN system correctly detected attacks against infrastructure, making it possible to identify and contain an attacker's station.**

Deauthentication and Disassociation Broadcast Attacks

As their names suggest, these attacks involve a concerted attempt to confuse the WLAN management infrastructure through spurious broadcasting of deauthentication and disassociation management frames.

Network Test targeted the test network with both types of frames. **In both cases, the Aruba WLAN infrastructure correctly detected the nature of these broadcast attacks.** Figures 24 shows the attacks as detected by AirWave RAPIDS.

☐	Highest	Exploit	AP	Deauth Broadcast	Deauth Broadcast	-	00:24:6C:B7:B4:C0	-	12/7/2010 10:54 AM
☐	Highest	Exploit	AP or Client	Deauth Broadcast	Deauth Broadcast	-	00:24:6C:B7:B4:C0	FF:FF:FF:FF:FF:FF	12/7/2010 10:54 AM
☐	Highest	Exploit	AP or Client	Disassoc Broadcast Attack	Disassoc Broadcast Attack	-	00:24:6C:B7:B4:C0	FF:FF:FF:FF:FF:FF	12/7/2010 10:54 AM
☐	Highest	Exploit	AP	Deauth Broadcast	Deauth Broadcast	-	00:24:6C:B7:B4:C0	-	12/7/2010 10:54 AM

FIGURE 23: AIRWAVE RAPIDS SEES DISASSOCIATION AND DEAUTHENTICATION BROADCAST ATTACKS

Frame Rate Anomaly Attacks

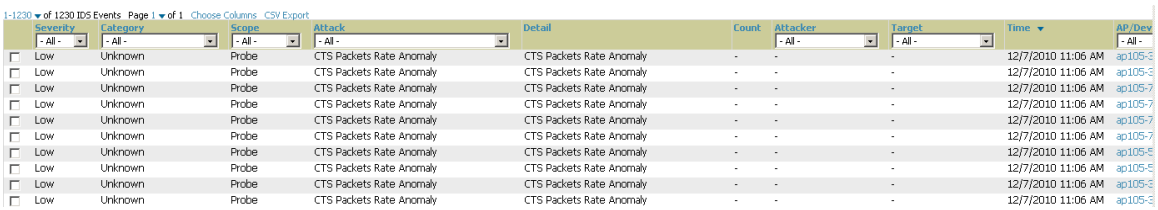
An intruder can exploit timing information carried in 802.11 frame headers to conduct DoS attacks. Ironically, although timing information is intended to ensure fair access for all stations even in mixed 802.11n/legacy settings, frame headers can be manipulated to tie up the medium.

Network Test verified that ArubaOS RFProtect WIP can detect frame-rate anomaly attacks. This specific exploit involves the RTS/CTS (ready to send/clear to send) messages used by 802.11 stations to reserve access to the medium. Among other things RTS/CTS signaling works especially well for legacy clients, which cannot decode the modulation schemes used in 802.11n frame headers.

However, this method works only if stations reserve time on the medium in a fair way. **An attacker could reserve the medium indefinitely by flooding the network with RTS and CTS**

frames. As a result, other stations would be denied access to the medium, and thus would be unable to transmit data.

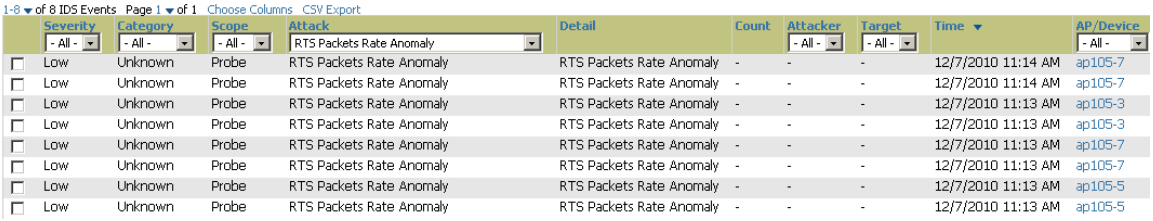
Network Test validated the ability of ArubaOS RFProtect WIP and AirWave RAPIDS to detect frame rate anomalies by injecting floods of CTS and RTS frames. ArubaOS **RFProtect WIP detected both types of frame-rate attacks,** as shown in Figures 25 and 26.



1-1230 of 1230 IDS Events Page 1 of 1 Choose Columns CSV Export

Severity	Category	Scope	Attack	Detail	Count	Attacker	Target	Time	AP/Dev
- All -	- All -	- All -	- All -			- All -	- All -		- All -
Low	Unknown	Probe	CTS Packets Rate Anomaly	CTS Packets Rate Anomaly	-	-	-	12/7/2010 11:06 AM	ap105-3
Low	Unknown	Probe	CTS Packets Rate Anomaly	CTS Packets Rate Anomaly	-	-	-	12/7/2010 11:06 AM	ap105-3
Low	Unknown	Probe	CTS Packets Rate Anomaly	CTS Packets Rate Anomaly	-	-	-	12/7/2010 11:06 AM	ap105-7
Low	Unknown	Probe	CTS Packets Rate Anomaly	CTS Packets Rate Anomaly	-	-	-	12/7/2010 11:06 AM	ap105-7
Low	Unknown	Probe	CTS Packets Rate Anomaly	CTS Packets Rate Anomaly	-	-	-	12/7/2010 11:06 AM	ap105-7
Low	Unknown	Probe	CTS Packets Rate Anomaly	CTS Packets Rate Anomaly	-	-	-	12/7/2010 11:06 AM	ap105-7
Low	Unknown	Probe	CTS Packets Rate Anomaly	CTS Packets Rate Anomaly	-	-	-	12/7/2010 11:06 AM	ap105-5
Low	Unknown	Probe	CTS Packets Rate Anomaly	CTS Packets Rate Anomaly	-	-	-	12/7/2010 11:06 AM	ap105-5
Low	Unknown	Probe	CTS Packets Rate Anomaly	CTS Packets Rate Anomaly	-	-	-	12/7/2010 11:06 AM	ap105-3
Low	Unknown	Probe	CTS Packets Rate Anomaly	CTS Packets Rate Anomaly	-	-	-	12/7/2010 11:06 AM	ap105-3

FIGURE 24: CTS RATE ANOMALY DETECTION



1-8 of 8 IDS Events Page 1 of 1 Choose Columns CSV Export

Severity	Category	Scope	Attack	Detail	Count	Attacker	Target	Time	AP/Device
- All -	- All -	- All -	RTS Packets Rate Anomaly			- All -	- All -		- All -
Low	Unknown	Probe	RTS Packets Rate Anomaly	RTS Packets Rate Anomaly	-	-	-	12/7/2010 11:14 AM	ap105-7
Low	Unknown	Probe	RTS Packets Rate Anomaly	RTS Packets Rate Anomaly	-	-	-	12/7/2010 11:14 AM	ap105-7
Low	Unknown	Probe	RTS Packets Rate Anomaly	RTS Packets Rate Anomaly	-	-	-	12/7/2010 11:13 AM	ap105-3
Low	Unknown	Probe	RTS Packets Rate Anomaly	RTS Packets Rate Anomaly	-	-	-	12/7/2010 11:13 AM	ap105-3
Low	Unknown	Probe	RTS Packets Rate Anomaly	RTS Packets Rate Anomaly	-	-	-	12/7/2010 11:13 AM	ap105-7
Low	Unknown	Probe	RTS Packets Rate Anomaly	RTS Packets Rate Anomaly	-	-	-	12/7/2010 11:13 AM	ap105-7
Low	Unknown	Probe	RTS Packets Rate Anomaly	RTS Packets Rate Anomaly	-	-	-	12/7/2010 11:13 AM	ap105-5
Low	Unknown	Probe	RTS Packets Rate Anomaly	RTS Packets Rate Anomaly	-	-	-	12/7/2010 11:13 AM	ap105-5

FIGURE 25: RTS RATE ANOMALY DETECTION

Malformed Frame Attacks

A final form of interfering with client connectivity involves corrupted fields in 802.11n beacon frames, while also injecting multiple beacons per beacon interval. ArubaOS **RFProtect WIP can safeguard the network against malformed frame attacks because of its ability to determine correct timing and to distinguish between valid and invalid 802.11 frame header contents.**

Network Test verified detection of malformed frames by "fuzzing" 802.11n beacon frames, injecting illegal or unexpected values into four fields in the frame headers. **Such an attack prevented clients from associating with the network,** both because of the high frequency of beacons and invalid contents of beacon frames.

ArubaOS RFProtect WIP correctly detected the malformed frames, as shown in Figure 27. Note that RAPIDS displays the type of attack ("HT" stands for "high throughput," indicating 802.11n beacons are involved) and also the attacker's MAC address. Armed with this knowledge, the system can be configured to take automatic countermeasures such as containing the attacker.

1-7 of 7 IDS Events Page 1 of 1 Choose Columns CSV Export

	Severity	Category	Scope	Attack	Detail	Count	Attacker	Target
	- All -	- All -	- All -	Malformed HT Information Element			- All -	- All -
☐	Low	Exploit	AP or Client	Malformed HT Information Element	Malformed HT Information Element	-	00:13:E8:F8:AA:F1	FF:FF:FF:FF:FF:FF
☐	Low	Exploit	AP or Client	Malformed HT Information Element	Malformed HT Information Element	-	00:13:E8:F8:AA:F1	FF:FF:FF:FF:FF:FF
☐	Low	Exploit	AP or Client	Malformed HT Information Element	Malformed HT Information Element	-	00:13:E8:F8:AA:F1	FF:FF:FF:FF:FF:FF
☐	Low	Exploit	AP or Client	Malformed HT Information Element	Malformed HT Information Element	-	00:13:E8:F8:AA:F1	FF:FF:FF:FF:FF:FF
☐	Low	Exploit	AP or Client	Malformed HT Information Element	Malformed HT Information Element	-	00:13:E8:F8:AA:F1	FF:FF:FF:FF:FF:FF
☐	Low	Exploit	AP or Client	Malformed HT Information Element	Malformed HT Information Element	-	00:13:E8:F8:AA:F1	FF:FF:FF:FF:FF:FF
☐	Low	Exploit	AP or Client	Malformed HT Information Element	Malformed HT Information Element	-	00:13:E8:F8:AA:F1	FF:FF:FF:FF:FF:FF

FIGURE 26: MALFORMED FRAME DETECTION

8 Conclusion

WLAN traffic is subject to special security considerations. Strong authentication and encryption is necessary but not sufficient. Other vulnerabilities exist, such as rogue APs (in many varieties) and attacks against wireless clients and infrastructure.

Defending against such attacks requires intrusion detection systems with deep knowledge of 802.11 protocols and timing behavior, including protection for 802.11n stations. An effective defense also involves strong correlation between wired and wireless networks, which in turn requires tight integration between WLAN management and intrusion detection systems.

ArubaOS RFProtect and AirWave Management Suite demonstrated the ability to repel multiple forms of wireless-specific attacks in this project. The Aruba WLAN system successfully detected 11 commonly observed forms of rogue APs used in testing[4]; contained all rogue APs, preventing disclosure of sensitive data; and detected and contained various 802.11-specific attacks against wireless clients and infrastructure.

Defense in depth involves comprehensive coverage of both wired and wireless networks. The Aruba system provided both in these tests.

[4] ArubaOS RFProtect and AirWave RAPIDS have signatures to detect many other types of attacks. Network Test and Aruba chose a relatively small representative sample for this project.

Appendix A: Hardware and Software Releases Tested

This appendix describes the software versions used on test bed infrastructure.

Component	Version
Controller	Aruba 3400
Access Points / Air Monitors	Aruba AP-105
Remote Access Points	Aruba RAP5wn
ArubaOS software release	6.0.0.1
AirWave Wireless Management Suite software release	7.2.1202

Appendix B: Disclaimer

Network Test Inc. has made every attempt to ensure that all test procedures were conducted with the utmost precision and accuracy, but acknowledges that errors do occur. Network Test Inc. shall not be held liable for damages which may result for the use of information contained in this document. All trademarks mentioned in this document are property of their respective owners.

Network Test Inc.
31324 Via Colinas, Suite 113
Westlake Village, CA 91362-6761
USA
+1-818-889-0011
info@networktest.com