TECHNOLOGY GUIDE

WIRELESS INTRUSION PROTECTION (WIP)

aruba NETWORKS

TABLE OF CONTENTS

INTRODUCTION

This document outlines the configuration and features of the Wireless Intrusion Protection solution available from Aruba Networks. For simplicity, this document assumes that the Controller, RFProtect license and AirWave are being used. In most cases, functionality similar to what is in the Controller is available in Aruba Instant. The concepts discussed with the controller can be applied to an Instant based solution.

Table 1 lists the current software versions for this guide.

TABLE 1. ARUBA SOFTWARE VERSIONS

Product	Version
ArubaOS™ (Mobility Controllers)	6.4
AirWave®	8.0

REFERENCE MATERIAL

- This guide assumes a working knowledge of Aruba products. This guide is based on the network detailed in the Aruba Campus Wireless Networks VRD and the Base Designs Lab Setup for Validated Reference Design. These guides are available for free at http://www.arubanetworks.com/vrd.
- The complete suite of Aruba technical documentation is available for download from the Aruba support site. These documents present complete, detailed feature and functionality explanations. The Aruba support site is located at: https://support.arubanetworks.com/. This site requires a user login and is for current Aruba customers with support contracts.

DETERMINE YOUR SECURITY NEEDS

An effective security solution must be monitored and updated on a regular basis. It should alert the security team of critical issues that merit a response without overwhelming them with information. It is important that the critical issues do not get lost in a flood of general information. Because of that we recommend turning on only the IDS events that are deemed worthy of investigation and follow up.

One of the first steps in deploying a security solution is determining the security policy that needs to be enforced by your enterprise. Preferably this would be done before choosing a security solution and would determine the evaluation criteria when choosing a solution.

The three main wireless security areas to keep in mind when evaluating a WIDS system are rogue detection, rogue containment and wireless intrusion detection needs. Once those base wireless security requirements are established and met, other general criteria come into play like ease of use, notification options, reporting depth, and data retention.

UNDERSTANDING THE PIECES OF THE ARUBA SOLUTION

The Aruba solution can seem overwhelming at first. There are a number of different optional pieces. But they really boil down to the type of Aruba network you deploy (controller based or Instant), the radio performing RF scanning (AM, AP or SM) and AirWave (long term data storage).

Controller or Instant? In general, this question will be answered by the WLAN requirements of your network. Both the controller and Instant provide a secure network with a wealth of IDS features. The controller gives you a few more features on the automatic containment side. The differences on the WIDS side are negligible.

What are the required pieces of the solution? If the answer above was a controller, then the RFProtect license may be necessary to get the most out of the WIP solution. RFProtect enables a lot of advanced features including spectrum analysis, IDS attack detection, and advanced wireless containment. The table below outlines what is provided by the base ArubaOS vs the RFProtect license for the controller. This guide will assume that the RFProtect license has been applied.

Feature	ArubaOS Base	RFProtect License
Air monitor (2.4 and 5 GHz)	✓	✓
Wireless rogue scanning and identification	✓	✓
Wired rogue containment	✓	✓
Wireless rogue containment via de-authorization	✓	✓
Wi-Fi interference detection	✓	✓
Spectrum analysis (Hybrid and Spectrum monitor)		✓
Wi-Fi interference classification		✓
Wi-Fi interference visualization		✓
Wireless IDS attack signatures detection		✓
Security threat management visualization		✓
Wireless intrusion configuration wizard		✓
Total Watch enhanced air monitoring		✓
Air monitoring of all bands (2.4, 4.9 and 5 GHz)		✓
Dynamic channel dwell times		✓
In-between channels rogue scanning		✓
Advanced wireless rogue containment via tar-pitting		✓
Detect and contain Windows Bridge		✓
Security events correlation		✓

Wireless detection happens at the radio level and then gets fed upstream. Aruba radios can be deployed in a few different modes to fit the needs of the environment. These include AP mode, Air Monitor (AM) mode and Spectrum Monitor (SM) mode. Only the AP mode will serve clients. AP mode will perform wireless rogue scans in 2.4 and 5 GHz, IDS detection and opportunistic wireless containment. AP mode prioritizes client traffic over other functions. AM mode focuses on security. AMs are strongly recommended if wireless containment is to be enabled. SM mode focuses on gathering spectrum data. SMs will perform basic IDS while they scan, but their scanning is focused on classifying interferers. They cannot perform containment because of how they need to scan to classify non-Wi-Fi interferers. More details on containment can be found in the containment chapter. More details on scanning algorithms can be found in the chapter on detection.

Most customers will only need standard AP mode devices for security. High security customers like financial customers and federal institutions may need AMs depending on their requirements. Anyone planning on deploying wireless containment should deploy AMs. Please see the chapter on containment for more information.

Finally there is AirWave. AirWave is a required piece of any security solution from Aruba. Unlike the controller or instant, AirWave has a hard drive. This allows it to store a great deal of data and add a lot of value to the security solution. AirWave can poll wired devices for additional wired rogue detection. AirWave has highly flexible classification rules that can and should be customized to your environment. AirWave also provides alerting and reporting on security issues. However, information on configuring the controller to communicate with AirWave is outside of the scope of this document. At a high level, ensure that SNMP monitoring, SNMP traps and AMON are enabled between the controller and AirWave.

DETECTION

Wireless scanning

Radios in an Aruba AP can be configured to run in different modes: AP mode, Air Monitor (AM) mode, or Spectrum Monitor (SM) mode. Each mode is designed to prioritize different tasks but will perform some level of all of them.

Radio Mode	Serve Clients	IDS/Rogue detection	IDS/Rogue Channels Scanned	Channels scanned	Wireless Containment	Spectrum analysis
AP mode	Yes	Yes	All regulatory channels	All regulatory channels	Best effort	Client serving channel only
Air Monitor	No	Yes	All regulatory + Rare channels	All regulatory + Rare	Yes	No
Spectrum Monitor	No	Yes	All regulatory channels	All regulatory channels	No	All channels

AP mode radios focus on serving clients and pushing wireless traffic but they also perform IDS detection, Rogue detection and spectrum analysis. The information provided by the APs provides the base for detection. Most customers only need APs and do not need to deploy any AMs or SMs. IDS detection occurs 100% of the time that the AP is serving clients. This means you have full IDS attack detection against your deployed network. The off channel scanning will find rogue devices and IDS attacks outside of your network.

Typically an AP will perform off channel scanning every 10 seconds for slightly less than 100 milliseconds. This allows the AP to see what is occurring around it, without missing beacons and causing problems for clients. A lot of logic has been built into the Aruba scanning algorithm. It will pause scanning for any detected voice or video on a particular radio to ensure the best quality for the clients. These settings can be configured using the VoIP Aware Scan, Video Aware Scan and Power Save Aware Scan options in the ARM profile. PEF firewall rules can also be defined to pause scanning based on a type of traffic running through the network. This typically isn't needed but can be useful to ensure QoS for specific latency sensitive applications. It is important to note that the off channel scanning is used for more than just WIP. It is also a key piece of Aruba's Adaptive Radio Management (ARM). All Aruba APs ship with scanning enabled by default. All published Aruba performance numbers have scanning enabled unless otherwise noted.

The AP can be configured to scan different sets of channels by changing the 'Scan Mode' setting in the scanning section of the ARM profile. Scanning all regulatory domain channels is recommended. That will include any channel valid in any regulatory domain, not just the regulatory domain of the AP. This is recommended since attackers typically don't feel the need to follow the law. Please note that the AP cannot perform containment on the channels outside of its regulatory domain. The set of channels can be restricted to use those within the AP's regulatory domain but that is not recommended for security conscious customers.

The AP uses a bucketing based algorithm for channel scanning. When the AP boots, all channels are divided into 2 different buckets, regulatory channels and non-regulatory channels. The regulatory channels are scanned more frequently than the non-regulatory channels. The third channel bucket, active channels, is populated as the AP scans and detects channels with wireless traffic. The active bucket is scanned more frequently than all of the others. This allows the AP to spend most of its time on channels where a threat is likely and the least amount of time on channels that are not likely to see attacks.

Because of the adaptive nature of the scanning algorithm it is very difficult to give an answer to the question 'how long does it take to scan all channels'. Typically all channels will be scanned at least once in less than an hour with active channels getting scanned much more frequently. Starting in AOS 6.4.3, the 2xx series APs will scan 80 MHz in the 5 GHZ spectrum when possible. This significantly decreases the amount of time it takes for an AP to detect rogue devices in the 5 GHz band.

APs can perform wireless containment but they will prioritize pushing client traffic over containment. This is a very important distinction and the reason why AMs are recommended if wireless containment is enabled. If the AP is serving clients on channel 1 and the rogue is on channel 6, the AP will not change channels to contain the rogue. If the rogue happens to be on channel 1, the AP will perform wireless containment while serving clients. If there are no clients on the AP, it can be configured to change channel to contain the rogue device by enabling the 'Rogue AP Aware' setting in the ARM profile.

APs can also perform spectrum analysis on the channel where they are serving clients. This gives the AP the ability to detect and classify non-Wi-Fi interferers that are impacting the deployed wireless network. APs are not able to scan and process spectrum data off of the home channel due to the short dwell times and relatively infrequent visits to other channels. Spectrum Monitors are designed to scan every channel within 1 second.

AMs are dedicated to wireless security. They do not serve clients. AMs typically do not need to be deployed at the same density an AP would since they do not serve clients. In most cases a 4 to 1 or 5 to 1 ratio of APs to AMs is recommended, but that varies heavily based on AP density and environment.

AMs use a channel scanning algorithm that is similar to an AP but has an extra bucket for 'Rare' channels. In raw MHz that is 2412-2484 and 4900 through 5895 in 5 MHz increments. Rare channels include the 4.9 GHz spectrum which is a licensed public safety band in many countries. AMs will also scan the 5 GHz spectrum in 5 MHz increments. Due to the analogue nature of wireless, we have found that the natural bleed through of RF signals will allow us to find rogues that are configured in between channels by scanning every 5 MHz. The channels scanned by an AM are configured in the AM scanning profile which is part of the radio profile.

Scan dwell times are based on the bucketing system. When in AP mode, the off channel's dwell time is quite short so that the AP doesn't miss a beacon. Since the AM is not serving clients, it does not send beacons and hence does not need to be on any particular channel. The AM will spend ~500 milliseconds on active channels, ~250 on channels in the regulatory domain, ~200 in any regulatory domain and ~100 on rare channels. Channels will be promoted to the active channel list at any time based on the detection of Wi-Fi activity. If no activity is seen for a significant period of time, the channel will be demoted back to its original bucket.

AMs will scan the active channels bucket more frequently than the regulatory channels which will be scanned more frequently than the all regulatory channels which will be scanned more frequently than the rare channels. The exact channel that is scanned will be chosen randomly and will not increment exactly. The dwell times listed above are slightly randomized to ensure that a rogue cannot predict exactly when it can and cannot transmit to avoid detection.

AMs are very effective at wireless containment. They will alter their scanning algorithm when containing to make sure they visit the channel where containment is occurring frequently. They will continue to scan for additional threats on other channels.

SMs are designed for spectrum classification. They will perform IDS detection and rogue detection while they are scanning for spectrum analysis, but they do not follow the bucketing system used by APs and AMs. They rapidly cycle through all of the channels making sure they are all visited every second. SMs will not perform any wireless containment since the time spent containing a rogue would impact the accuracy of the spectrum classifications. Typically, SMs are used as a point troubleshooting. A full spectrum monitor overlay is not needed in most cases since the APs can perform hybrid spectrum analysis.

While we generally don't recommend single radio APs, a single radio AM or SM can make sense. An AP-93, which is a single radio 11n device, provides a low cost option for an AM or SM. All of the Aruba single radio APs can be tuned to both 2.4 GHz and 5 GHz. Using a single radio will slightly increase the amount of time it takes to detect a rogue, but it can still effectively detect and contain them. If a single radio device is deployed as an AM, be sure to verify that 'Multi Band Scan' is enabled in the ARM profile. Multi Band Scan tells the single radio AP to scan both the 2.4 GHz and 5 GHz band. Multi Band Scan can enable a single radio device in AP mode to scan both bands, but isn't recommended since a robust wireless network will simultaneously support 2.4 and 5 GHz clients.

You can verify which channels are scanned and how frequently they are getting scanned by running the 'Show ap arm scan times ap-name' command, or by using AirWave to run the command on the controller. You will see an output that looks like:

```
Channel Scan Time
-----------------
```

channel	assign-time(ms)	scans-attempted	scans-rejected	dos-scans	flags	timer-tick
34	55220	502	0	0	D	2736027
36	311642310	6421	198	0	DVACL	2737453
38	53680	488	0	0	D	2736283
40	101052240	14084	519	0	DVACLU	2737476
42	53680	488	0	0	D	2736628
44	52562480	14368	514	0	DVACLU	2737505
46	54340	494	13	0	D	2736969
48	494459940	11954	482	0	DVACLU	2737597
52	491920	4472	160	0	DCLUX	2737196
56	1125520	10232	316	0	DCLUX	2737444
60	1394470	12677	432	0	DACLUX	2737554
64	730400	6640	272	0	DACLUX	2737565
100	584650	5315	162	0	DACLX	2737575
104	1014420	9222	351	0	DCLUX	2737084
108	1391830	12653	443	0	DACLUX	2737588

```
112      1164460          10586          362            0          DACLUX   2737314
116      1502600          13660          478            0          DACLUX   2737433
120      1575860          14326          493            0          DACLUX   2737546
124      1026960          9336           278            0          DACLUX   2737175
128      1074920          9772           368            0          DACLUX   2737218
132      915200           8320           323            0          DACLUX   2737239
136      1071400          9740           359            0          DACLUX   2737280
140      1268960          11536          414            0          DACLUX   2737304
149      511740690        5979           192            0          DVACL    2737341
153      31289180         14438          518            0          DVACLU   2737359
157      18712460         14586          0              0          DVACLU   2737387
161      3579540          14614          548            0          DVACLU   2737414
165      1223614570       4087           0              0          DVACU    2737426
1        722995340        14494          473            0          DVACL    2737498
2        2142140          19474          695            0          DACL     2737514
3        2088570          18987          652            0          DACL     2737526
4        2111670          19197          690            0          DACL     2737548
5        4269100          38810          1410           0          DVACLU   2737565
6        1148002050       21955          0              0          DVACLU   2737584
7        4261840          38744          1404           0          DVACLU   2737433
8        2106500          19150          657            0          DACU     2737445
9        2080650          18915          659            0          DACU     2737460
10       2113210          19211          641            0          DACU     2737491
11       872092550        13505          507            0          DVACU    2737597
12       460790           4189           165            0          D        2737106
13       297110           2701           109            0          D        2737229
14       162470           1477           0              0          D        2737354

Channel Flags: D: All-Reg-Domain Channel, C: Reg-Domain Channel, A: Activity Present
               L: Scan 40MHz Lower, U: Scan 40MHz Upper, Z: Rare Channel
               V: Valid, T: Valid 20MHZ Channel, F: Valid 40MHz Channel,
               O: DOS Channel, K: DOS 40MHz Upper, H: DOS 40MHz Lower
               R: Radar detected in last 30 min, X: DFS required
```

The scanning configuration of an AP or AM can be confirmed by running the 'show ap monitor scan-info ap-name' command. It will give you a view of how the radio is configured for scanning and a little information about the scans. The output will look similar to:

```
WIF Scanning State: wifi0: 6c:f3:7f:a9:e2:b0
-----------------------------------------
Parameter                      Value
---------                      -----
Probe Type                     sap
Phy Type                       80211a-HT-20
Scan Mode                      all-reg-domain
Scan Channel                   no
```

```
Disable Scanning                yes
RegDomain Scan Completed        yes
DOS Channel Count               0
Current Channel                 48
Current Scan Channel            124+
Current Channel Index           18
Current Scan Start Milli Tick   -1787802966
Current Dwell Time              110
Current Scan Type               active

Scan-Type-Info
---------------
Info-Type          Active  Reg-domain  All-reg-domain  Rare  DOS
---------          ------  ----------  --------------  ----  ---
Dwell Times        500     250         200             100   500

Last Scan Channel  124+    124-        60-
0     0
```

Wired Rogue AP Detection

The controller has a few different methods for determining that an AP is connected to the wire. The most basic is a +/- 1 MAC address check of traffic that has been on the wire and seen wirelessly. If wired traffic is observed with a MAC address that is within 1 of wireless traffic, that device will be tagged as a wired connected rogue.

There are a few more sophisticated methods as well. The APs and AMs will monitor all the traffic heard over the air to see if any of it is originating on the wired network. It is determined that the traffic originated on the wire if the from_ds field of the wireless traffic matches any of the known wired gateway MAC addresses. The list of known wired gateway MAC addresses is built up by the controller, APs and AMs. All client facing VLANs should be trunked to either the controller or an AP or AM. The traffic only needs to be trunked to 1 AP or AM for the detection to work. It doesn't hurt to trunk the VLANs to all of the APs or AMs that are deployed. That is actually required for wired containment which is discussed in the chapter regarding containment.

AirWave should be configured to poll routers and switches on the network via SNMP. AirWave will poll the bridge forwarding tables and the ARP tables to gather rogue information about the network. The bridge forwarding table gives AirWave a mapping of wired MAC addresses to switch ports. The ARP table gives a mapping of wired MAC addresses and IP addresses. AirWave will then correlate the list of wired MAC addresses with everything that has been heard over the air. If two MAC addresses are within a configurable offset, they will be considered the same device and linked together. The size of the correlation window can be configured in RAPIDS→Setup page in the 'wired to wireless MAC address correlation' setting. There is also a wired to wireless correlation window that can be configured on the RAPIDS→Setup page. It defaults to 6 hours. This can help limit false positives for devices that have similar MAC addresses but are not on the network at the same time.

If AirWave is able to get an IP address for a rogue, it can perform an NMAP scan on the device to determine the operating system. While the scan isn't able to classify 100% of the operating systems, it does give valuable insight into the type of device on the network. It is worth noting that there is also a wireless BSSID correlation window. That window will link wireless BSSIDs that are numerically close together into the same device. This means that neighboring networks that are broadcasting multiple SSIDs from the same AP will be linked into a single rogue record.

All of the information gathered by AirWave can be used to classify a rogue device. More information on that is included in the section detailing classification.

Adding switches to AirWave has additional value outside of the security realm. AirWave can perform upstream event correlation to identify wired causes to AP problems. It can also provide visibility into the switch ports that are serving APs so wired problems can be easily identified.

802.11ac Rogue Detection

802.11ac devices are backwards compatible with 802.11a/b/g/n devices. For 11ac devices to be backwards compatible, the management frames, like beacons, will go out at 20 MHz. That way non-11ac clients can detect the AP and connect to them. This means that legacy a/b/g/n APs can also wirelessly detect rogue 11ac access points. But the legacy APs won't necessarily have visibility into the data coming out of a rogue 11ac AP.

If the rogue is communicating with an 11ac client, the data frames may have a channel that is too wide, or a modulation that the legacy AP cannot decode. That means legacy APs are unable to always determine if a client is associated to the rogue. That detection is critical for more advanced features such as wireless containment and wired rogue detection. If an AP can't hear the client on the rogue, then it cannot contain it.

Earlier it was mentioned that the wired rogue detection was based on looking at the source MAC address of frames coming out of the rogue AP. Those are the data frames. With an 11ac rogue and an 11ac client, they may not be visible to 11a/b/g/n devices. If a legacy client connects to the 11ac rogue, then it can be detected by the legacy AP since the legacy radio can understand the traffic.

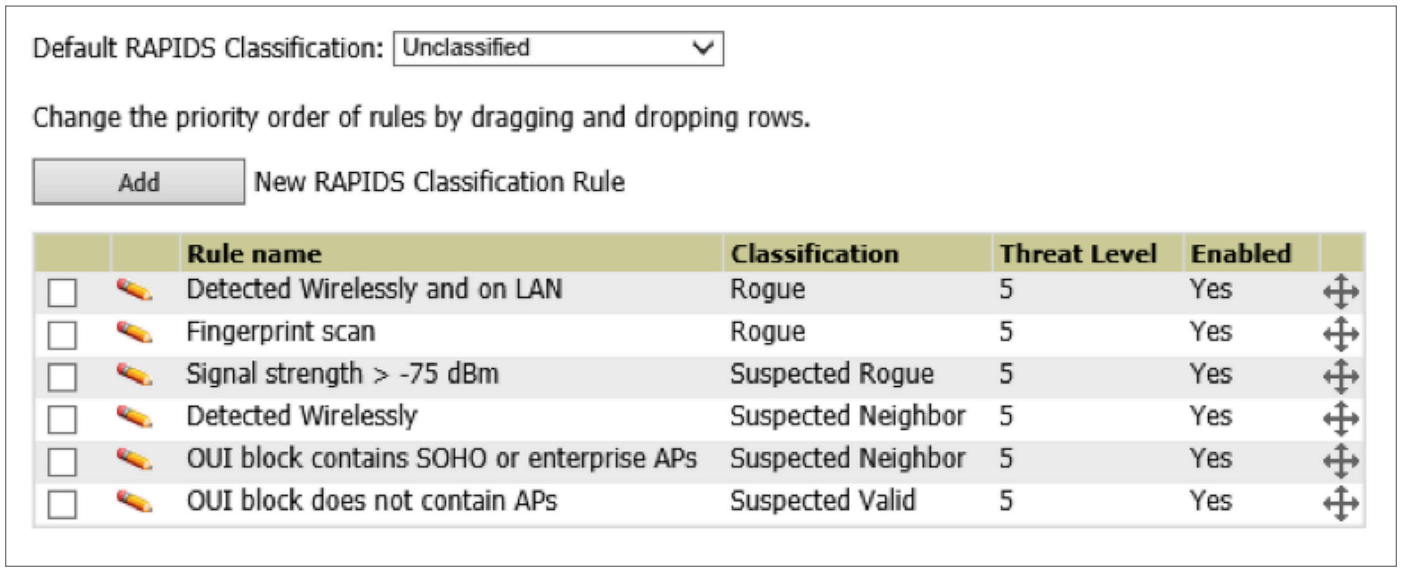
Because of these limitations, an 11ac overlay or 11ac network is recommended for high security customers. 11ac is required to make sure that all potential threats are detected.

Feature	Legacy Network	11ac Overlay	11ac Network
Wireless rogue detection	Supported	Supported	Supported
Basic wired rogue detection	Supported	Supported	Supported
Advanced wired rogue detection	Vulnerable	Supported	Supported
Basic IDS attack detection	Supported	Supported	Supported
Advanced IDS attack detection	Vulnerable	Supported	Supported
Custom IDS signature detection	Vulnerable	Supported	Supported
Full IDS attack detection	Vulnerable	Supported	Supported
Wired containment	Supported	Supported	Supported

CLASSIFYING ROGUE APS

Rogue classification should happen in AirWave. The controller can perform some basic device classification but AirWave provides a more robust and configurable solution. The heart of the Aruba classification system is configured on the Rapids→Rules page in AirWave.

The rules are displayed in a list form. They act similar to firewall rules. The first rule in the list that is matched, is the classification a device will receive. If a device does not match any rule, it will get the default classification specified in the drop down above the rules list.



		Rule name	Classification	Threat Level	Enabled	
☐		Detected Wirelessly and on LAN	Rogue	5	Yes	
☐		Fingerprint scan	Rogue	5	Yes	
☐		Signal strength > -75 dBm	Suspected Rogue	5	Yes	
☐		Detected Wirelessly	Suspected Neighbor	5	Yes	
☐		OUI block contains SOHO or enterprise APs	Suspected Neighbor	5	Yes	
☐		OUI block does not contain APs	Suspected Valid	5	Yes	

Devices will get continuously reclassified as new information comes in about them. But they will only be reclassified up the list into a more specific rule. It is important that more specific and detailed rules are at the top of the list and that generic catch-all rules are at the bottom.

If a neighboring AP is heard with a weak signal strength it would fall to the 'Detected wirelessly' rule and get classified as a suspect neighbor. If a week later the device suddenly had a strong signal strength of -60 dBm, it would be promoted up to a suspect rogue. At that point an alert could fire, but more on alerts in the alerting and reporting chapter. Now if that device were to be detected on the wire a day later, it would be classified by the 'Detected Wirelessly and on LAN' rule and reclassified as a rogue.

Threat level is an optional additional bucketing system within a single classification. It has no set definition. A threat level of 1 or 10 can be considered the most dangerous. However, be sure to keep the rules in sync so that a specific threat level is always considered the most dangerous. The threat level can be used to change the alerting options within AirWave.

The rules above are pretty much the default rules you will see in RAPIDS. The rules should be customized for your unique environment. They should be updated based on the security policies implemented by your enterprise. It is a recommended best practice to make sure that anything classified into the 'Rogue' classification is considered a significant security threat and will be investigated by the security team right away. It is important to focus that classification down into things that need to be investigated so that the true threats don't get lost in a flood of neighboring devices.

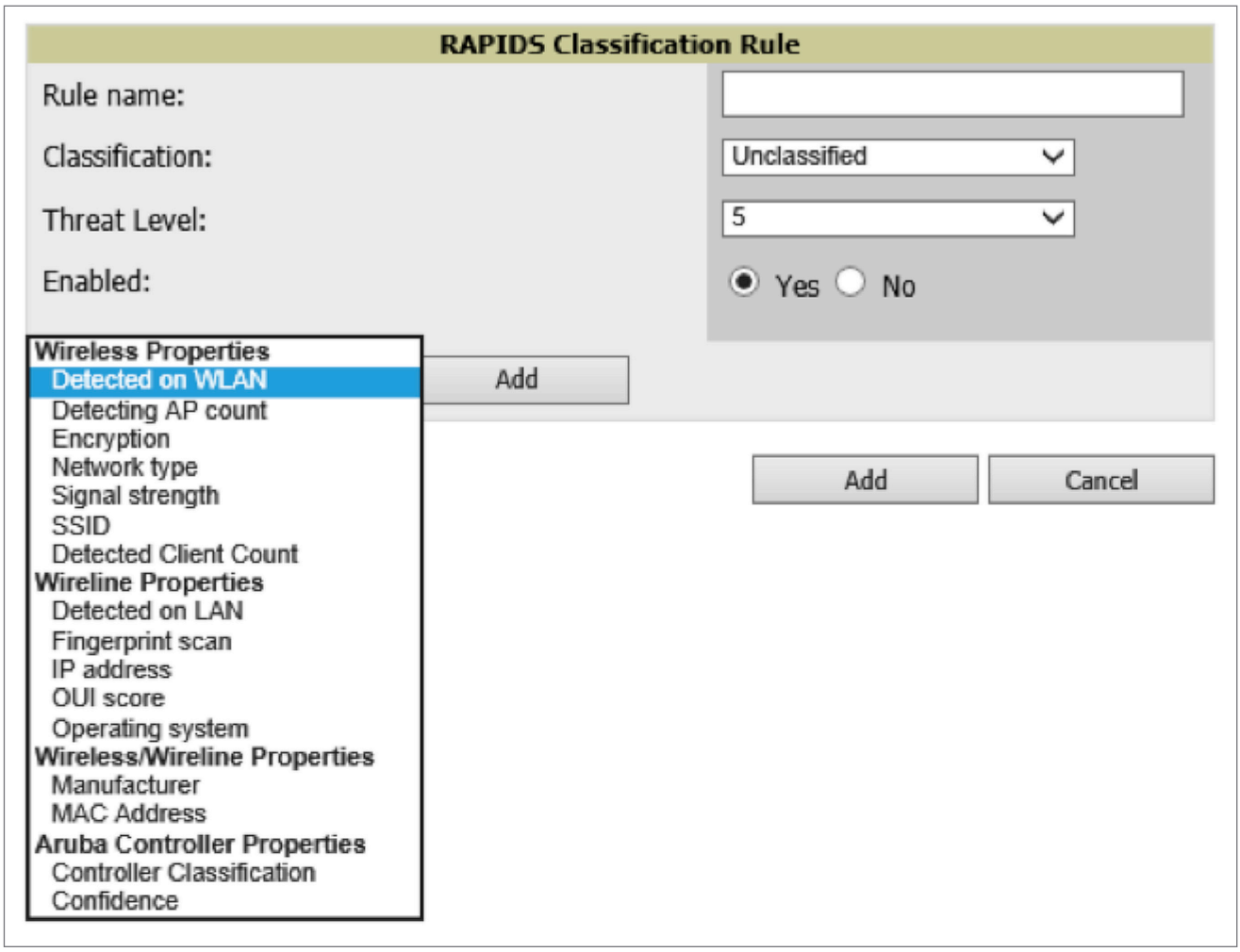
Once the customized security policy rules are in place, it is recommended that you take a look at the classified devices. You can often find sets of devices that can be reclassified into the neighbor classification without creating any security risk. It is both common and recommended to create general rules to match neighboring devices so that they can be pushed down the danger meter into less threatening classifications.

A common example are 2Wire APs. 2Wire makes home DSL routers that are often used by AT&T or SBC for wireless. If you have a campus near an apartment building or residential area, you will see a lot of 2Wire devices. Within RAPIDS you can create a rule that will reclassify any 2Wire device to be a neighbor without manually inspecting it. This can save a great deal of time and make it much easier to keep up with the wirelessly detected devices in your RF environment. The common 2Wire rule is to classify any device manufactured by 2Wire with a 2Wire SSID, running encryption, heard with a weak signal strength and not connected to the LAN as a neighbor.

CONFIGURING IDS ATTACK DETECTION

How you choose to configure your controllers is a larger discussion than WIP. The easiest way to configure IDS attack detection is to use the WIP wizard in the controller. Once you have gone through the wizard, you can have AirWave pull the configuration from the controller and use that as the golden sample.

The wizard is straight forward and will prompt for which IDS attacks and automatic containment should be enabled as part of step 4. It is recommended to start with a small list of serious threats, and slowly grow that list. A lot of teams make the mistake of turning on everything they can detect. Then they get overwhelmed by the number of alerts and fail to follow up on any of it.



It is recommended that you only turn on attack detection that is worth investigating. High security customers should choose the 'High' option. The high option does not enable every event that can be detected by the Aruba system. For example, Netstumbler detection isn't turned on by default. Netstumbler detection means that a client device is running an old scanning system. It doesn't necessarily mean they are trying to break into the network. Custom settings can be chosen that allow you to enable or disable every attack detection individually if you wish to see everything.

If you prefer, the IDS detection can be configured through the profiles but correct configuration requires a deeper knowledge of AOS and the profile structure. Please see the User Guide for more information.

ROGUE CONTAINMENT

Not all customers are comfortable running rogue containment. Some types of rogue containment may impact neighboring networks while others will only protect your network and pose no threat to neighbors.

Just like IDS, containment is most easily configured through the wizard. Containment may also be referred to as shielding or mitigation. They all mean the same thing. Breaking the rogue's or client's ability to connect to the network. There are two main types of containment, wired and wireless.

Wired containment is performed by ARP poisoning the default gateway of a rogue device connected to the wire. The detecting AP or AM will perform the containment. The wirelessly detecting device needs to be on the same VLAN as the rogue for the wired containment to be successful.

There are two types of wireless containment, deauth and tar-pitting. Both of them start out the same way. The Aruba AP will send de-authentication packets to the AP and the client device. Most client devices will automatically try to reconnect to the network. When deauth is selected, the AP will send another deauth packet once the client is connected to the network. With modern clients that can happen as quickly as every 15 milliseconds.

Tar-pitting will behave a little differently. When the client device attempts to reconnect to the network, the Aruba AP will respond with a probe response that has some fake data in it to induce the client device to connect to the Aruba AP rather than the rogue device. The client device then takes some time to realize the connection isn't going anywhere. At that point it disconnects and starts over. The important thing is that realization can take anywhere from 500 milliseconds to requiring user intervention. This makes tar-pitting a significantly more efficient mechanism to contain rogue devices.

AMs are always recommended when wireless containment is enabled. APs will perform containment, but only if the rogue device or client is on the same channel as the AP. APs may change channel to contain a rogue if there are no clients on the AP and 'Rogue AP Aware' is enabled in the ARM profile. AMs will mark a channel for DOS and will alternate between it and the channels it is scanning. This allows an AM to spend a lot more time containing rogues.

There are a lot of automatic rogue containment options that go beyond 'contain if the device is classified as a rogue'. The safest and most common options are 'Protect Valid Stations' and 'Protect SSID'. Any station that has authenticated to the Aruba network with encryption will be automatically classified as valid. Once this happens, the Aruba network will not allow them to connect to any other network if Protect Valid Stations is enabled. This protects the network by preventing users with sensitive data from connecting to neighboring networks that may be snooping the data.

Protect SSID will automatically contain any non-valid APs that are broadcasting the SSIDs on the controller. This can be very effective and preventing honey pot attacks and poor network experience caused by connecting to non-approved APs.

ALERTING AND REPORTING

Alerting and reporting are critical pieces of any security system. Security team members can't spend time every day logging into the system and looking for issues. Alerts and reports provide quick and easy visibility into the system. The Alerting and Reporting is run from AirWave.

In AirWave, triggers are defined for the thresholds that should cause an alert to get created. Alerts are the events that are created. Triggers are defined on the System→Triggers page. As an NMS system, AirWave supports a very large set of network health and troubleshooting triggers. On the security side there are a few key triggers to be aware of, IDS events, Rogue device classified and Client on Rogue AP.

All of the triggers can be configured to be logged locally on AirWave, send an email to a specified address or mailing list, sent as an SNMP trap or as a syslog message. There aren't a lot of best practices around which alerting system is best. They all work well and it really depends on what will fit best in your environment. It is strongly recommended that only the highest threat alerts are sent as emails. Otherwise recipients tend to create filters in their email client and miss the threat entirely.

Triggers can also be restricted to specific groups or folders. Because of that, different sites can alert differently. Typically we find that remote sites often have reduced alerting. That may be due to a lack of resources to investigate the issue, a lack of sensitive material on the remote networks or lack of control over the remote site if it is a home office.

APPENDIX: CONTACTING ARUBA NETWORKS

WEB SITE SUPPORT	
Main Site	http://www.arubanetworks.com
Support Site	https://support.arubanetworks.com
Software Licensing Site	http://www.arubanetworks.com/support/wsirt.php
Wireless Security Incident Response Team (WSIRT)	http://www.arubanetworks.com/support/wsirt.php
Support Emails	
Americas and APAC	support@arubanetworks.com
EMEA	emea_support@arubanetworks.com
WSIRT Email Please email details of any security problem found in an Aruba product.	wsirt@arubanetworks.com

VALIDATED REFERENCE DESIGN CONTACT AND USER FORUM	
Validated Reference Designs	http://www.arubanetworks.com/vrd
VRD Contact Email	referencedesign@arubanetworks.com
Airheads Online User Forum	http://airheads.arubanetworks.com

TELEPHONE SUPPORT	
Aruba Corporate	+1 (408) 227-4500
FAX	+1 (408) 227-4550
Support	
United States	+1-800-WI-FI-LAN (800-943-4526)
Universal Free Phone Service Numbers (UIFN)	
Australia	Reach: 11 800 494 34526
United States	1 800 9434526 1 650 3856589
Canada	1 800 9434526 1 650 3856589
United Kingdom	BT: 0 825 494 34526 MCL: 0 825 494 34526
Japan	IDC: 10 810 494 34526 * Select fixed phones IDC: 0061 010 812 494 34526 * Any fixed, mobile and payphone KDD: 10 813 494 34526 * Select fixed phones JT: 10 815 494 34526 * Select fixed phones JT: 0041 010 816 494 34526 * Any fixed, mobile and payphone
Korea	DACOM: 2 819 494 34526 KT: 1 820 494 34526 ONSE: 8 821 494 34526
Singapore	Singapore Telecom: 1 822 494 34526
Taiwan (U)	CHT-I: 0 824 494 34526
Belgium	Belgacom: 0 827 494 34526
Israel	Bezeq: 14 807 494 34526 Barack ITC: 13 808 494 34526
Ireland	EIRCOM: 0 806 494 34526
Hong Kong	HKTI: 1 805 494 34526
Germany	Deutsche Telkom: 0 804 494 34526
France	France Telecom: 0 803 494 34526

TELEPHONE SUPPORT	
Universal Free Phone Service Numbers (UIFN)	
China (P)	China Telecom South: 0 801 494 34526 China Netcom Group: 0 802 494 34526
Saudi Arabia	800 8445708
UAE	800 04416077
Egypt	2510-0200 8885177267 * within Cairo 02-2510-0200 8885177267 * outside Cairo
India	91 044 66768150

ABOUT ARUBA NETWORKS, INC.

Aruba Networks is a leading provider of next-generation network access solutions for the mobile enterprise. The company's Mobile Virtual Enterprise (MOVE) architecture unifies wired and wireless network infrastructures into one seamless access solution for corporate headquarters, mobile business professionals, remote workers and guests. This unified approach to access networks enables IT organizations and users to securely address the Bring Your Own Device (BYOD) phenomenon, dramatically improving productivity and lowering 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, Africa and Asia Pacific regions. To learn more, visit Aruba at www.arubanetworks.com. For real-time news updates follow Aruba on Twitter and Facebook, and for the latest technical discussions on mobility and Aruba products visit Airheads Social at http://community.arubanetworks.com.

aruba NETWORKS

1344 CROSSMAN AVE | SUNNYVALE, CA 94089
1.866.55.ARUBA | T: 1.408.227.4500 | FAX: 1.408.227.4550 | INFO@ARUBANETWORKS.COM

www.arubanetworks.com