ARUBAOS RFPROTECT MODULE

The ArubaOS RFProtect™ module is an optional software module installed on Aruba Mobility Controllers. RFProtect safeguards the network infrastructure against wireless security threats as well as provides a critical layer of visibility into sources of radio frequency (RF) interference and their effect on wireless LAN (WLAN) performance.

RFProtect provides the industry's only integrated wireless security and spectrum analysis system for enterprise WLANs. Aruba's WLAN infrastructure allows access points (APs) to service WLAN clients while monitoring the air for interference sources and rogue devices. Aruba APs may also be turned into dedicated air monitors to focus on detecting and containing unauthorized APs and devices. Dedicated air monitors are used for containment only and do not broadcast SSIDs or other information over the air.

Additionally, Aruba 802.11ac and 802.11n APs may be configured as a spectrum analyzer to remotely scan 2.4 and 5-GHz radio bands, identify RF interference, classify the source and provide real-time analysis. With RFProtect, no specialized hardware or client software is required for RF spectrum analysis, eliminating the need for a separate network of RF sensors and security appliances.

Used in conjunction with RFProtect, Aruba's AirWave provides event history, event correlation, spectrum visibility, location tracking and security reports to meet compliance requirements, such as those defined by the Payment Card Industry (PCI).

SPECTRUM ANALYSIS

RF interference in WLANs is inevitable and unpredictable. It can originate from neighboring Wi-Fi networks or non-Wi-Fi sources, such as 2.4-GHz cordless phones, microwave ovens, analog video cameras, gaming consoles and wireless telemetry systems. The characteristics and severity of RF interference varies based on the type and location of the device and may have an impact on client access and performance of the WLAN.

Aruba 802.11ac and 802.11n APs utilize Wi-Fi chipsets with integrated high-definition spectrum analysis capabilities, enabling always-on, simultaneous spectrum analysis, client serving and wireless security monitoring. Simultaneous scanning of the RF spectrum for interference and intrusion protection eliminates the cost and complexity of separate dedicated hardware or handheld analyzers with client software. As a result, the Aruba solution is less than half the cost of other products and reduces the time spent by IT staff to manually capture RF interference events.

Aruba's Adaptive Radio Management (ARM) features, which are part of the base controller operating system, allow Aruba APs to avoid interference. The ArubaOS RFProtect module enhances ARM functionality by including spectrum analysis capabilities which identifies and classifies interference sources in up to 13 categories, then provides administrator analysis of the interference via 12 graphical charts, including FFT and spectrogram graphs.

WIRELESS INTRUSION PROTECTION

Wireless networks make attractive targets for denial-of-service (DoS) and man-in-the-middle attacks. Aruba Mobility Controllers with RFProtect maintain signatures to identify and block wireless attacks so service is not disrupted. Based on location signatures and client classification, Aruba access points will drop illegal requests and generate alerts to notify administrators of an attack.

Aruba APs monitor the air to detect other wireless stations masquerading as valid APs. Dedicated Aruba 802.11ac and 802.11n AP sensors can detect and contain over 250 Rogue access points simultaneously. RFProtect tracks unique signatures for each wireless client in the network. If a newly-introduced station claims to be a particular client but lacks a proper signature, a station impersonation or man-in-the-middle attack is declared. When a man-in-the-middle or invalid/masquerading AP is detected, defense mechanisms are put in place to contain the unauthorized device and prevent the corruption or loss of confidential data.

CLASSIFYING AND DISABLING ROGUE ACCESS POINTS

Classification is the first step in securing the corporate environment from unauthorized wireless access. Adequate measures to quickly shut down intrusions are critical to protect sensitive information and network resources. APs and stations must be accurately classified to determine whether they are valid, rogue or neighboring APs, and an automated response must be implemented to prevent possible intrusion attempts.

With RFProtect, Aruba 802.11ac and 802.11n APs support TotalWatch™ – the ability to scan all channels of the RF spectrum, including 2.4- and 5-GHz bands as well as the 4.9-GHz public safety band. TotalWatch also provides 5-MHz granular channel scanning of bands for rogue devices, and dynamic scanning dwell times to focus on those channels with traffic. TotalWatch provides an advanced set of features to detect unauthorized wireless devices and a set of customizable rules are utilized to highlight devices that truly pose a threat to the network.

Detected devices classified as rogues may be contained using both wireless and wired means. Wireless Tarpitting provides an efficient method of containing rogues over the air without impacting neighboring devices. This method of tarpitting is more efficient than rogue containment via repeated de-authorization requests. Network administrators are notified of rogue devices, and the physical location of the rogue may be determined with the use of AirWave.

RFProtect will stop wireless traffic from flowing into the wired infrastructure via rogue APs, protecting the wired network against wireless security breaches.

POLICY DEFINITION AND ENFORCEMENT

RFProtect enables the configuration and dynamic enforcement of network policies. Examples of wireless policies include valid station protection, AP misconfiguration protection, ad-hoc network detection and protection, unauthorized network interface card (NIC) detection, and wireless bridge detection. RFProtect includes a policy-configuration wizard, simplifying the creation of an organization's wireless security policies.

RFPROTECT FEATURES

Spectrum Analyzer
- Simultaneous RF spectrum analysis, client serving and security scanning
- Integrated into Aruba 802.11ac and 802.11n APs
- Scales like APs on a controller (up to 1024 RAP monitors on an M3)
- Scans 2.4- and 5-GHz bands
- Classification of interference in up to 13 categories including:
  - Bluetooth devices
  - Cordless phone, network and base station devices
  - Fixed-frequency video and audio devices
  - Microwaves
- Visualization via 12 spectrum analysis charts including:
  - FFT Duty Cycle
  - Real-time FFT
  - Swept Spectrogram
- Integration with Aruba AirWave to display, aggregate and display intereferer Classification, location and RF information

TOTALWATCH AIR MONITORING
- Automatic rule-based classification
- Wireless containment via tarpitting
- Location tracking via AirWave

IMPERSONATION DETECTION AND PREVENTION*
- Hotspotter attack detection
- MAC address spoofing
- AP impersonations
- Man-in-the-middle attacks
- Sequence number anomaly detection

CLIENT INTRUSION PREVENTION*
- Honeypot AP protection
- Valid station protection

DENIAL OF SERVICE ATTACK DETECTION*
- Auto immune attacks Power save attacks Management frame floods De-authentication attacks Authentication floods Probe request floods
- Fake AP floods
- Null probe responses
- EAP handshake floods

PROBING AND NETWORK DISCOVERY*

- Detection of NetStumbler and broadcast probes

NETWORK INTRUSION DETECTION*

- Wireless bridges
- ASLEAP attacks

ORDERING INFORMATION

- RFProtect is available as a license for mobility controllers and is ordered based on the number of APs supported by the controller.
- LIC-RFP-xx   RFProtect Module License

* Representative list of features – for a complete list of all wireless intrusion detection and prevention (WIDS/WIPS) features please see the ArubaOS users guide.