WIRED AND WIRELESS ROGUE DETECTION

AirWave® RAPIDS™ Rogue Detection automatically detects and locates unauthorized clients and access points, and utilizes a set of rules to highlight the most important threats to your organization.

RAPIDS uses existing, authorized APs to scan the RF environment for any unauthorized devices in range. It also scans your wired network to determine if the wirelessly detected rogues are physically connected to the local network, and to look for additional unauthorized devices in areas without wireless coverage.

In addition, RAPIDS captures and manages IDS events detected by wireless LAN controllers. RAPIDS then correlates all of this data and uses a set of customizable rules to highlight those devices that are truly a threat to the organization, greatly reducing false-positives and allowing you to work more efficiently.

RAPIDS works in conjunction with the Aruba Networks Mobility Controller RFProtect software module to correlate and consolidate rogue AP and client, wired and wireless attack data, delivering a comprehensive Wireless Intrusion Protection Solution (WIPS).

Customers can deploy this solution with “hybrid” APs serving as both APs and sensors or as an overlay architecture where Aruba APs act as dedicated sensors called air monitors (AMs). RAPIDS utilizes data from both the dedicated sensors and deployed APs to provide the most complete view of your wireless environment. The solution improves network security, manages compliance requirements and reduces the cost of manual security efforts.

HOW RAPIDS IS USED

As wireless LANs evolve into mission-critical infrastructure, organizations are becoming more concerned about managing network security in the most efficient manner. Most organizations implement strict policies banning the installation of unauthorized, or rogue, APs but often struggle with enforcing these policies.

In addition, a variety of compliance requirements such as those established by the Payment Card Industry (PCI) put greater pressure on organizations to reevaluate their WLAN strategy and operation. However, few enterprises have the tools or resources to adequately enforce their policies or follow up and resolve threats on a consistent basis.
RAPIDS provides an efficient, effective process for rogue detection, correlation, classification, alerting, reporting and containment.

KEY FEATURES

Wired network scans and AP identification
- Examines the MAC address of each device discovered by polling routers and switches and compares it to RAPIDS’ database of 12,000+ known MAC address ranges to identify likely rogue devices
- Examines the MAC address of each device discovered by polling routers and switches and compares it to RAPIDS’ database of 12,000+ known MAC address ranges to identify likely rogue devices
- Uses RAPIDS’ database of 1,700+ OS types to identify the device operating system to help you eliminate false-positive results

Wireless network scans
- Instructs authorized access points to scan the air for other wireless APs and clients
- Automatically builds a list of authorized APs to prevent them from being classified as rogues
- Allows you to distinguish between “true rogues” and “neighbor APs” that are in RF range but do not pose a threat to your network
- Displays valid and currently connected rogue clients, rogue client associations, and rogue client association history

Scan the airspace outside the coverage of your wireless network
- Turns your existing wireless-enabled Windows devices into additional RF sensors with the optional AirWave Management Client™ (AMC) software

Wireless intrusion detection system (WIDS) events
- Aggregates, correlates, alerts and logs wireless attacks that have been reported by your infrastructure, providing a full picture of your wireless network security

Comprehensive result correlation
- Correlates information from wired and wireless scans, including SSID, RF channel, security method, radio MAC address or BSSID, network type, LAN MAC address, IP address and operating system

- Compares wired and wireless scans to eliminate duplicates and refine threat assessment

Rules-based threat classification
- Classifies potential threats based on rules you customize to define what a rogue device is
- Reduces false-positives and lets your security team focus on the most significant threats first

Automated alerts and reports
- Assigns proper alert priority to each discovered AP and client depending on its classification
- Generates automated email alerts, syslog alerts, or SNMP traps containing all known information about rogue devices, including:
  - Radio MAC address
  - LAN MAC address
  - Discovery method
  - SSID
  - Channel
  - Security settings
  - Switch port
  - IP address
- Graphical dashboard displays real-time information on all suspected rogue APs and clients
- Pre-defined, customizable reports address common security and compliance information needs, such as rogue device tracking and PCI compliance

Visualization
- Integrates with AirWave VisualRF™ to display the likely location of each rogue device on a building floor plan

Automatic and manual containment
- Performs manual or automated rogue AP containment with Aruba and Cisco controllers
- Uses your customized rules-based classification scheme to determine when to automatically contain devices
- Can disable wired switch ports with rogue APs attached

www.arubanetworks.com
1344 Crossman Avenue. Sunnyvale, CA 94089
1-866-55-ARUBA | Tel. +1 408.227.4500 | Fax. +1 408.227.4550 | info@arubanetworks.com

© 2013 Aruba Networks, Inc. Aruba Networks’ trademarks include AirWave®, Aruba Networks®, Aruba Wireless Networks®, the registered Aruba the Mobile Edge Company logo, Aruba Mobility Management System®, Mobile Edge Architecture®, People Move, Networks Must Follow®, RFProtect®, and Green Island®. All rights reserved. All other trademarks are the property of their respective owners. The scale may vary depending upon the deployment scenario and features enabled. AB_AirWaveRAPIDS_081313