DATA SHEET

ArubaOS Wireless Intrusion Protection

ARUBAOS WIRELESS INTRUSION PROTECTION MODULE

Aruba's Wireless Intrusion Protection (WIP) module protects the network against wireless threats to network security by incorporating wireless intrusion protection into the network infrastructure and eliminating the need for a separate system of RF sensors and security appliances. The WIP module provides unmatched wireless network visibility to administrators, and thwarts malicious wireless attacks, impersonations, and unauthorized intrusions.

ROGUE AP PREVENTION

- Rogue AP detection, classification, location and automatic containment

DENIAL OF SERVICE (DOS) ATTACK DETECTION

- Management frame floods
- Deauthentication 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

CLIENT INTRUSION PREVENTION

- Honeypot AP protection
- Valid station protection

NETWORK INTRUSION DETECTION

- Wireless bridges
- ASLEAP attacks

SURVEILLANCE

- Detection of weak encryption implementation

IMPERSONATION DETECTION AND PREVENTION

- MAC address spoofing
- AP impersonations
- Man-in-the-middle attacks
- Sequence number anomaly detection

Detection is only one step in securing the corporate environment from unwanted wireless access. Adequate measures to quickly shut down intrusions are critical to protect sensitive information and network resources. To do this, you need accurate means of classifying APs and stations (e.g., valid, rogue, or neighbor), and providing an automated response to possible intrusion attempts.

Aruba access points constantly scan all channels of the RF spectrum, capturing all 802.11 traffic and locally examining captured data. Only policy violations are sent to the Aruba Mobility Controller to minimize the impact on wired network performance. During scanning, the system learns about all wireless APs and stations, and classifies these devices based on traffic flows seen on the wire and over the air. Traffic data are collected and correlated on the Mobility Controller.

Aruba's WIP module provides both detection and prevention capabilities, so administrators can react to both unintentional and malicious WLAN access.

Accurately detect and stop rogue access points

DETECTING AND DISABLING ROGUE APS

Aruba's adaptive WLAN infrastructure allows APs to service WLAN clients while monitoring the air for intrusion events, or can be optionally configured to serve only one function. Air monitoring detects unauthorized APs and devices, including those with MIMO or pre-802.11n radios. Detected devices are classified as rogues and can be automatically disabled. Administrators are also notified of the presence of rogue devices, along with their precise physical location on a floorplanfor mitigation purposes.

ARUBAOS WIRELESS INTRUSION PROTECTION MODULE

UNIQUE STATION AND USER CLASSIFICATION

Aruba's patented system automatically identifies and classifies all APs and stations connected to the network to minimize false positives. The system works using innovative logic that includes traffic pattern analysis, comparison of wired- and wireless-side traffic, and device location information. Using this logic, devices and APs found are accurately classified as real threats or rogues vs. devices that belong to neighboring networks.

DENIAL OF SERVICE AND IMPERSONATION PROTECTION

Due to their open medium, wireless networks make attractive targets for denial of service attacks. Such attacks include software that floods the network with association requests, attacks that make a laptop look like thousands of APs, and deauthentication floods. Aruba Mobility Controllers equipped with the ArubaOS WIP module maintain signatures of many different wireless attacks and are able to block them so service is not disrupted.

Advanced Denial of Service (DoS) protection keeps enterprises safe against a variety of wireless attacks, including association and deauthentication floods, honeypots and AP and station impersonations. Based on location signatures and client classification, Aruba access points will drop illegal requests and generate alerts to notify administrators of the attack.

MAN-IN-THE-MIDDLE PROTECTION

One of the common wireless networks attacks is the "man-in-the-middle" attack. During such an attack, a hacker masquerades as a legitimate AP, and acting as a relay point, fools users and other APs into sending data through the unauthorized device. The attacker can then modify or corrupt data, or run password-cracking routines.

Aruba access points monitor the air to detect other wireless stations masquerading as valid APs. When masquerading is detected, appropriate defense mechanisms are put into place. Aruba Mobility Controllers also track unique "signatures" for each wireless client in the network, and if a new station is introduced claiming to be a particular client, but lacks a proper signature, a station impersonation attack is declared.

POLICY DEFINITION AND ENFORCEMENT

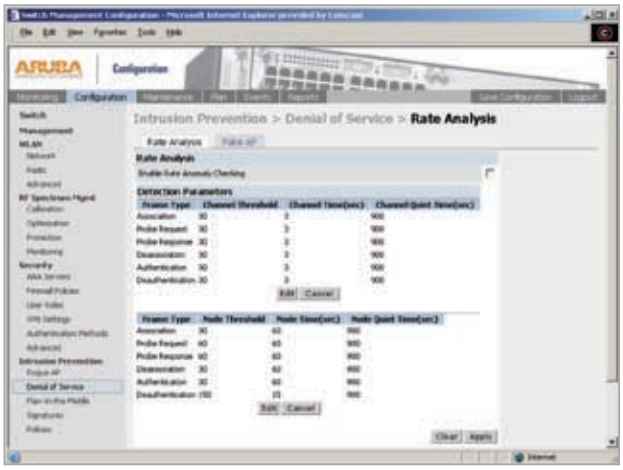
The ArubaOS WIP module uses a number of policies that can be configured to act automatically when a policy is violated. Examples of wireless policies include weak WEP implementation detection, AP misconfiguration protection, ad-hoc network detection and protection, unauthorized NIC type detection, and wireless bridge detection.

USING WIRELESS TO PROTECT YOUR WIRED NETWORK

Even if wireless LANs are not used, Aruba's WIP will stop wireless traffic from flowing into the wired network through rogue APs unknowingly attached to a network port. This capability protects the network against wireless security breaches. Once the enterprise is ready to deploy wireless LANs, the Aruba system can be easily reconfigured to provide a scalable, secure wireless LAN infrastructure.

USING WIRELESS TO PROTECT YOUR EXISTING WIRELESS NETWORK

ArubaOS WIP complements and enhances any existing WLAN deployment, including Cisco deployments, by providing advanced RF security and control features not found in first-generation wireless produd\cts.



Wireless Intrusion Protection detects entire range of RF threats

ARUBA networks

WWW.ARUBANETWORKS.COM

1322 Crossman Avenue. Sunnyvale, CA 94089 | Tel. +1 408.227.4500 | Fax. +1 408.227.4550

DS_WIP_US_071112