Alcatel-Lucent OmniAccess Wireless Intrusion Protection Module

WIRELESS LAN SOFTWARE

The Alcatel-Lucent OmniAccess™ Wireless Intrusion Protection (WIP) module is an optional module that protects the network against wireless threats by incorporating wireless intrusion protection into the wireless infrastructure and eliminating the need for a separate system of radio frequency (RF) sensors and security appliances. The WIP module provides unmatched wireless network visibility to administrators and thwarts malicious wireless attacks, impersonations and unauthorized intrusions.

Key features

Ability to detect and protect against the following:

- Management frame floods
- De-authentication attacks
- Authentication floods
- Probe request floods
- Fake access point (AP) floods
- Null probe responses
- EAP handshake floods

- Detection of NetStumbler and broadcast probes

- Protects against client configured with windows wireless bridging active
- Protects against clients or AP configured in bridge mode.
- Defends from ASLEAP attacks
- Support for customizable wireless attack signature

- Detection of weak encryption implementation

Key benefits

- Keeps enterprises safe against wireless denial of service (DoS) attacks.

- Detection of discovery attacks that typically precede a hacking attempt.

- Protects against attacks with set pattern / signature.

- Enforcement of wireless security policies with monitoring of access Points (APs) security configuration

Key features

Detection and protection against:

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

Key benefits

- Protects against client or access point impersonation including man-in-the-middle attacks.

Detection is only one step in securing the corporate environment from unwanted wireless access. Adequate measures to quickly shut down intrusions are critical to protecting sensitive information and network resources. OmniAccess wireless 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 OmniAccess wireless switch 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 is collected and correlated on the wireless switch. The OmniAccess WIP module provides both detection and prevention capabilities, so administrators can react to both unintentional and malicious WLAN access.

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 de-authentication floods. OmniAccess Wireless switches equipped with a 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 de-authentication floods, and AP and station impersonations. Based on location signatures and client classification, OmniAccess Wireless 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.

OmniAccess Wireless 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. OmniAccess Wireless switches 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 OmniAccess 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.

Alcatel·Lucent