



WIRELESS LANs AND THE SARBANES-OXLEY ACT

The Sarbanes-Oxley Act of 2002 has focused attention on the quality of public companies' financial data and the security of their data networks, including wireless LANs. Aruba's Enterprise Mobility Infrastructure helps your organization implement the proper controls over your WLAN infrastructure.

Section 404 of the Sarbanes-Oxley Act of 2002 makes corporate management responsible for "establishing and maintaining adequate internal control structures and procedures for financial reporting" and makes auditors responsible for assessing those controls. Most auditors are interpreting Section 404 broadly to require corporations to implement strict controls over access to data networks, including wireless LANs, to ensure the integrity and security of corporate data. Aruba's Enterprise Mobility Infrastructure ensures network administrators have the level of security and control they need over their WLANs. IT organizations at public corporations with wireless LANs need to be prepared to address key questions that are likely to be raised by their auditors, including many of the following.

How do you encrypt wireless data and control access to your WLAN?

Different corporations have adopted different policies and approaches to wireless data encryption and access control based on their particular requirements and budgets: utilizing WPA, requiring VPNs, segregating wireless traffic on separate VLANs, adopting RADIUS-based 802.1X authentication, using stateful user-aware firewalls, etc. For Aruba's best security practice recommendations, see the whitepaper entitled "Building Global Security for Wireless LANs," available from Aruba's website.

While different organizations have different security policies, your organization must be able to define these policies centrally and ensure that WLAN infrastructure complies with these policies. Aruba mobility controllers provide a central point of control for all Aruba access points, while Aruba's AirWave Management Platform™ (AMP) enables your network administrators to use a web-based UI to define exactly how all wireless access points – even non-Aruba access points – should be configured. It automatically applies those policies to every managed device on the network, and even enables efficient distribution of firmware to ensure that your entire WLAN infrastructure used the most recent, secure firmware from your hardware vendor. Centralized wireless control and management eliminates opportunities for human configuration error and ensures compliance with defined policies.

How do you audit your wireless infrastructure to ensure compliance?

Centralized mobility controllers ensure that the WLAN is configured properly. Through the mobility controller, there is one single view of the entire network, and one central location for all configuration data. In a multi-controller network, Aruba's master-local configuration system allows network-wide configuration on the master controller, with all local controllers pulling their configuration from the master. There is never any question as to how the WLAN is configured.

Best practice requires that you also continuously audit your WLAN infrastructure to ensure that no settings are misconfigured on any controller or AP due to human error or – worst case, the actions of a malicious intruder. AMP allows you to centrally define your own, specific configuration policies for each controller, access point, or group of access points on your network. AMP then continuously audits the configuration of these wireless access points, immediately alerting you and providing a detailed onscreen report whenever any AP's configuration does not match your policy. You can even instruct AMP to automatically 'repair' any misconfigured APs as soon as they are discovered, eliminating the possibility that a configuration error will allow an intruder to access your network.

How do you detect unauthorized 'rogue' access points?

Aruba's Enterprise Mobility Infrastructure delivers a unique, three-pronged approach to detecting unauthorized "rogue" access points connected to your network. Whenever rogues are detected via any of these mechanisms, you are automatically sent a high-priority alert.

RF Scans via Aruba Mobility Controllers

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 automatically classified as either "interfering" (non-threat) or "rogue" (threat) and can be automatically disabled over the air and over the wire. Administrators are notified of the presence of rogue devices, along with their precise physical location on a floorplan for mitigation purposes.

RF Scans via RFprotect Distributed

RFprotect Distributed is an infrastructure-based two-tier WIPS consisting of a network of sensors, built from Aruba's line of access points, and a centralized server running RFprotect Distributed software. This powerful wireless security solution incorporates the industry's only Wireless Threat Protection Framework for complete threat detection, attack prevention, "no wireless" policy enforcement and compliance reporting inside the enterprise. RFprotect Distributed secures your wireless network against intrusions that are perpetrated intentionally and from vulnerabilities caused unintentionally through misconfigured network equipment. The solution can be deployed standalone, with no wireless LAN present, or as an overlay to monitor any vendor's wireless LAN equipment.

Wired Network Scans via the AirWave Management Platform

The AirWave RAPIDS™ software module is designed for organizations that do not have wall-to-wall coverage with RF sensors, but still need to defend their networks against rogue APs. RAPIDS automatically detects and locates unauthorized access points through a combination of wireless and wired network scans. First, the RAPIDS software can use existing authorized APs and wireless LAN controllers to scan the airspace for any unauthorized devices in range. Second, RAPIDS queries wired switches and routers, and scans the wired network to determine whether any unknown devices that are likely rogue APs are connected. Even without an installed wireless LAN, RAPIDS can ensure no rogue APs are on the network. RAPIDS can also be combined with an Aruba or other third-party Wireless Intrusion Prevention System to increase their joint effectiveness.

Do you track who has connected to your network?

Your auditors will likely ask how your organization determines which users and devices have connected to your network. Aruba's Enterprise Mobility Infrastructure provides real-time monitoring of every access point, user and device connected to your network. For further visibility and long-term storage, AMP even correlates data from multiple network sources (including wireless access points, VPN servers, wireless gateways, RADIUS servers, and routers) to identify each WLAN user by username. This information is retained in AMP's database and is used to generate a daily Client Session Report with detailed information on every user session. This data can be exported via XHTML and stored externally to ensure that you have full records of who used your wireless network, where they connected, session length, authentication status, and more.

Is there an audit trail for administrative users?

Auditors are increasingly concerned with accountability and your ability to determine who made particular changes to your security and other network policies. Aruba's Enterprise Mobility Infrastructure provides a detailed log identifying exactly which administrative user took actions at specific times. This provides a complete audit trail for all major actions involving your wireless network. To supplement logs maintained on mobility controllers, AMP also provides long-term storage that can record data for several years.

To learn more about how Aruba's Enterprise Mobility Infrastructure solution can help provide the network controls required to comply with the Sarbanes-Oxley Act of 2002, please contact your Aruba Networks representative.



WWW.ARUBANETWORKS.COM

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