

White Paper |

Government



## Requirements for Building Effective Government WLANs

CJ Mathias | Farpoint Group

**ARUBA**<sup>®</sup>  
ARUBA  
networks

---

## Introduction

With governments just now beginning the adoption of wireless LANs as a key component of their network connectivity strategy, the purpose of this White Paper is to enumerate the issues and solutions now available that lead to successful government WLAN installations. Government networks, given the nature of information they transport, demand an aggressive security posture. They are also characterized by stringent high-availability and performance requirements, which cannot compromise security requirements in any way.

Given that all of the security challenges that exist on wire are also present in wireless systems - including worms, viruses, software vulnerabilities, eavesdropping, break-ins (intrusions), unauthorized access, and denial-of-service attacks – along with new threats unique to wireless LANs, an appropriate security plan and implementation can be complex. This potential complexity is enhanced by the fact that wireless signals often propagate well beyond the building or intended coverage area where a given WLAN is installed. Special care must be taken to ensure that WLANs remain secure.

Fortunately, a vast amount of effort has been invested in identifying, understanding, and building systems and solutions that counter these challenges. Indeed, we even feel comfortable claiming that security on wireless LANs can *exceed* that usually implemented on wire.

## Core Federal Government Requirements

There are a number of key federal requirements for information security, as follows:

The Federal Information Security Management Act (FISMA) –FISMA requires all federal agencies “to develop, document, and implement an agency wide information security program”. The National Institute of Standards and Technology (NIST) develops standards and provides guidance to federal agencies on information security practice. Their *Wireless Network Security: 802.11, Bluetooth and Handheld Devices (Special Publication 800-48)* is an excellent place to start in understanding the risks and possibilities inherent in wireless security.

FIPS 140-2 Level 2 – This NIST developed standard specifies US Federal Government requirements for IT systems that are used for Sensitive But Unclassified (SBU) information. FIPS 140-2 specifies security requirements that must be met by a conforming product. Independent evaluators work with NIST and product vendors to validate a given product’s security functionality. Since early WLAN security schemes (those based on Wired Equivalent Privacy, or WEP) were proven insecure, the only way government agencies have been able to deploy WLANs to date has been by utilizing a proprietary Layer 2 encryption mechanism. These proprietary encryption overlays are very expensive and complex and do not provide the mobility and radio-management benefits of centralized WLAN mobility controllers.

---

DoD 8100.2 – This is the key DoD policy for the use of commercial wireless devices for non-classified communications within the DoD Global Information Grid. This policy requires that all DoD wireless infrastructure are both WPA2 certified and FIPS 140-2 certified for 802.11i. Such elements as layer 2 encryption, strong authentication, non-repudiation, personal identification, FIPS 140-2 compliance, addressing denial-of-service attacks, screening/sensing/monitoring, and other requirements are specified in this document.

The latest development in this space is NIST approval of the IEEE 802.11i standard for WLAN security as acceptable for FIPS validation and impending approval of 802.11i by DoD for non-classified deployments. With availability of FIPS-validated 802.11i products, the Federal Government can deploy commercially available 802.1X authentication and layer 2 AES encryption for securing their WLAN infrastructure.

Common Criteria – This is an internationally-adopted standard for information security. The creation of CC was lead by National Information Assurance Partnership (NIAP) program at NIST. Unlike FIPS, which provides a list of security requirements, Common Criteria provides a framework. Developers create their framework (referred to as a Security Target) and NIAP approved evaluators validate that a given product meets the claimed security functionality. When a particular framework for a class of product is widely accepted and approved by the NSA (National Security Agency), it is referred to as a Protection Profile (PP). In the Federal Government, Common Criteria validation is rapidly gaining acceptance as a key requirement.

## **Addressing Federal Requirements - Aruba's WLAN Product Strategy**

It is clear that switched (also called centralized) architectures are the preferred solution for enterprise- and government-class deployments, where centralized mobility controllers are primarily responsible for control, configuration and management of a WLAN. Centralized architectures vary, of course, with respect to specific implementations, but the core advantage to this approach is the very limited role played by access points (APs). APs in this case are “thin”; no state or other information is stored in the APs, enhancing security.

Aruba extends the centralized architecture with a number of key benefits, as follows:

### **Single Security Boundary**

While the definition of “thin” is still rather broad, Aruba believes that security processing should be centralized in the mobility controller, with not even security keys stored in the AP. While it has become popular in recent years to include security processing in the AP, there are at present no FIPS-certified WLAN chipsets that would allow a decentralized encryption architecture to gain FIPS approval. Moreover, the storage of security keys and certificates in the AP allows the possibility that this

---

information can be compromised. By moving all encryption and decryption processing to the mobility controller, the Aruba approach eliminates this possibility while providing both high-performance and end-to-end FIPS-compliant security.

## Future-Proof Architecture

A centralized architecture makes it much easier to apply updates and meet new requirements, for security or otherwise. By utilizing a high-performance programmable encryption chip in the controller, Aruba Mobility Controllers can be upgraded to new encryption algorithms centrally. Updating each access point individually for encryption is not only extremely cost-prohibitive, it is also often difficult because of the use of low-cost, non-programmable encryption chips that are typically used in APs. Thus the flexibility inherent in Aruba's centralized security architecture is critical to investment protection as federal security requirements continue to evolve, and clearly serves to minimize total cost of ownership (TCO) while maximizing return on investment (ROI).

## FIPS and Common Criteria Validation

Aruba Mobility Controllers are the only mobility controllers that are FIPS 140-2 Level 2 validated for 802.11i and that support all major encryption protocols in hardware, including AES. Aruba is the first and only vendor to achieve FIPS 140-2 for 802.11i systems, primarily as a result of the centralized programmable encryption architecture of the Aruba Mobility Controllers.

Aruba is already in evaluation for Common Criteria EAL-4 certification (as is noted on the NIAP web site). While there is no medium robustness Protection Profile for WLANs available today, Aruba has taken the initiative to work with NIAP and NSA on its own Security Target. This Security Target closely matches the draft WLAN Protection Profile published by the NSA and further adds Functional Security Requirements (FSRs) from the Firewall Protection Profile. In summary, Aruba is simultaneously defining and on a path to comply with the most stringent security standards for WLAN environments today.

## Integrated Security and Management

*Per-user, stateful firewalls* – Since wireless LANs represent a new edge for Federal and other networks, it's critical that the WLAN solution have an integrated (as opposed to add-on) stateful, per-user firewall. Aruba's firewall allows the definition of up to 512,000 simultaneous policies implemented on a per-user basis. The firewall is both bidirectional and dynamic; policies are role-based and can be easily modified as agency requirements change. Individual user permissions can also be set based upon their *location* at any moment in time, a capability unique to wireless.

---

*RF monitoring and management* – Aruba's Access Points are used for communications with clients, but they can also be used as air monitors, sniffing the air for potential security problems such as intruders and rogue (unauthorized) access points. Other threats include denial-of-service attacks, and a variety of network intrusion scenarios. Aruba's products are architected with these threats in mind. Aruba's patent-pending traffic classification algorithms are at the heart of the solutions set, allowing detailed analysis and immediate countermeasures against wireless threats. Jamming can be addressed via adjustments, made automatically, to AP channel and power settings. Similarly, man-in-the-middle, deauthentication, MAC-address spoofing, rogue APs, unintentional wireless bridges, and a huge range of other wireless-specific threats can all be addressed without compromising fundamental system integrity (redundant configurations and failover are integral capabilities as well).

*Identity-based security* – All Aruba security features can be tied to the identity of specific users, and, if desired, specific client devices. Two-factor authentication is supported as well. Mobile users have no fixed location so enforcing access control based on physical port (like a wired network) is not an option. Assigning VLAN membership based on SSID is not fully secure and is open to MAC address spoofing attacks. Being able to tie a user's identity to their location, device type, authentication method and encryption type is key to achieving robust security demanded by government WLAN installations. Aruba's products allow corporations to tie stateful security policies to users as they authenticate, then have those policies follow them as they move throughout the network—even when connecting from remote locations. This allows the implementation of a true "defense-in-depth" security framework that seamlessly overlays any existing IP data network while delivering mobility.

*xSec* – A joint development of Aruba and Juniper Networks (formerly Funk Software), xSec provides much-improved Layer-2 encryption (encrypting MAC addresses, for example), and also extends the capabilities similar to those of 802.11i/WPA2 to wired networks.. Implemented on clients, xSec can also be used to extend modern security to older access points. xSec is fully compliant with 802.1x, and has been approved under FIPS 140-2.

Hardware-based security acceleration makes these capabilities possible, and the Aruba architecture continues to provide a broad set of other important features, including location and tracking and mobility management with centralized control. This not only lowers total cost of ownership, but also makes it easier to audit the complete Agency security solution

## **Conclusions - Best Practices for Federal Security**

While civilian agencies have been deploying WLAN on an as-needed basis, the adoption rate within more sensitive agencies has been slow. Many defense agencies have simply not deployed any WLAN

---

because they have deemed them insecure. Aruba has taken a leadership role in addressing the barriers to further utilization of wireless LANs in all government-related missions.

Unfortunately, an ad-hoc strategy built on necessity will require a significant systems-integration workload and will include the risk of developing a less-than-optimal solution.

Given the expense and uncertainty associated with such a strategy, it is highly desirable to fully understand the requirements first and develop a solution prior to integration.

Aruba's products feature full compliance with all key Federal information security requirements, and minimize complexity and cost by integrating all requirements into a single, comprehensive product family. There is no need to obtain a wireless LAN mobility controller and APs from one vendor, a firewall from another, IDS/IPS from a third, and so on. Aruba's solution obviates the need for this effort and expense, providing a complete and secure mobile network for government applications.

## **About Aruba Networks**

Aruba securely delivers the enterprise network to users, wherever they work or roam, with user-centric networks that significantly expand the reach of traditional port-centric networks. User-centric networks integrate adaptive WLANs, identity-based security, and application continuity services into a cohesive, high-performance system that can be easily deployed as an overlay on top of existing network infrastructure. Adaptive WLANs deliver high-performance, follow-me connectivity so users are always within reach of mission-critical information. Identity-based security associates access policies with users, not ports, to enable follow-me security that is enforced regardless of access method or location. Application continuity services enable follow-me applications that can be seamlessly accessed across WLAN and cellular networks. The cost, convenience, and security benefits of user-centric networks are fundamentally changing how and where we work. Listed on the NASDAQ and Russell 2000® Index, Aruba is based in Sunnyvale, California, and has operations throughout the Americas, Europe, Middle East, and Asia Pacific regions. To learn more, visit Aruba at <http://www.arubanetworks.com>.

© 2007 Aruba Networks, Inc. All rights reserved. Aruba Networks, BlueScanner and RFprotect are trademarks of Aruba Networks, Inc. All other trademarks or registered trademarks are the property of their respective holders. All rights reserved. Specifications are subject to change without notice.



1322 Crossman Ave. Sunnyvale, CA 94089-1113  
Tel. +1.408.227.4500 | Fax. +1.408.227.4550 | [info@arubanetworks.com](mailto:info@arubanetworks.com)  
<http://www.arubanetworks.com>