

Government



FIPS Validated 802.11i WLAN
Meeting Government Requirements
for Secure Mobile Data

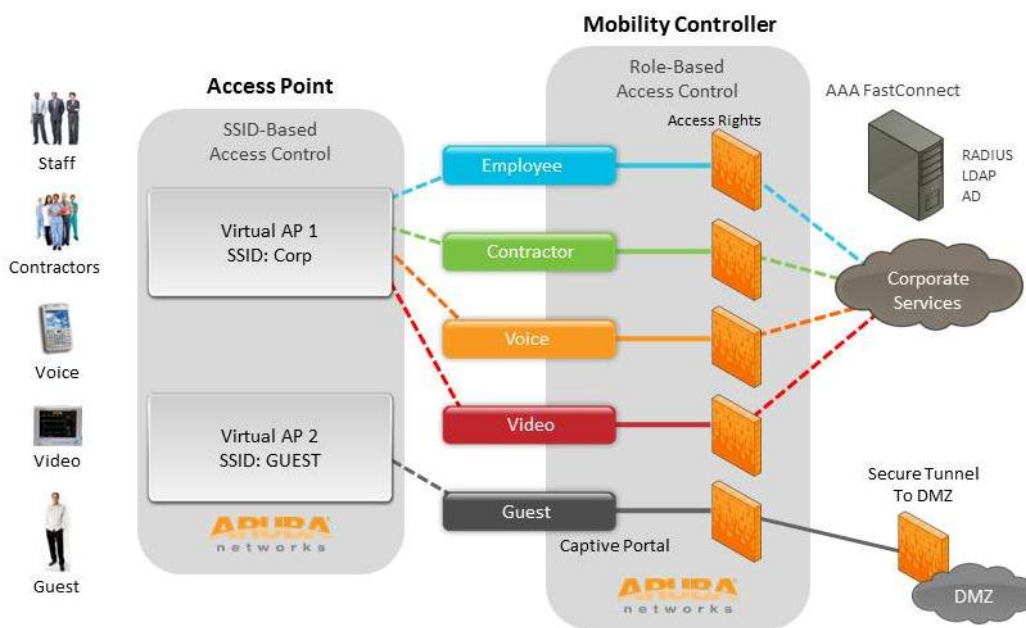
Situation

From the boardroom to the battlefield, no entity has a greater need for mobile communications than the Government. Until recently, however, WLAN technology has been a trade off between increased productivity and security. To take advantage of wireless technologies, the only option for government agencies, per Department of Defense Directive (DoDD) 8100.2, was to deploy a Layer 2 encryption overlay on top of their wireless infrastructure.

While this solution provided encryption, it was still not sufficient for securing wireless networks carrying sensitive information, lacking key components such as secure authentication, access control and wireless intrusion detection. In addition these networks were extremely cumbersome to manage as they lacked centralized management (for the Access Points and the security overlay) and automated RF management. Access Points (AP's) on a distributed architecture simply can't deliver the degree of security and manageability necessary for Government agencies.

Solution

Aruba Networks took a fundamentally different approach to WLAN security by centralizing the architecture and delivering a user centric solution. Aruba utilizes a centralized architecture to maintain a single point of security control thereby integrating the multiple disparate components a user would utilize to access their network. Where traditional thin-AP architecture of a distributed network offloads wireless traffic at the access point, the Aruba solution aggregates all encrypted traffic and is therefore able to monitor all wireless activity for all stations at the mobility controller while ensuring complete encryption from one end of the network to the other.



Key Benefits

- Single Point of Security Control
- Universal Authentication
- Role-based Access Control
- Stateful Firewalls
- High-Speed Encryption
- Hardware-based Processing
- Automatic Client Blacklisting
- Flexible Policy Creation

Equally important to Government agencies, the Aruba User Centric network, as the name implies, is based on user identity, not Access Point or device IP addresses. Mobile users and devices, by definition, do not connect to the network through a fixed port. For this reason, the network must identify every user and device that joins the network. Once this identity is known, custom security policies may be applied to the network so that only appropriate access is provided based on specific departments or groups, security clearance, or the actual position of a user. This “follow-me” security based on user roles drastically improves network security by eliminating excess privileges on the network while providing identity-based auditing.

The Ideal Solution for the Federal Government’s Robust Network Security Requirements

The Aruba solution offers a comprehensive FIPS validated 802.11i solution today. For wireless clients that do not support 802.11i protocols yet, an interim step to 802.11i is provided by xSec, an Aruba – Juniper Networks jointly developed, standards-based Layer 2 encryption protocol. xSec also provides FIPS 140-2 validated security for wired clients, legacy access points, and legacy mobile devices that do not currently support 802.11i.

Because of its centralized architecture, Aruba’s mobility controller delivers unmatched encryption processing power and a design where no encryption keys are stored anywhere outside the controller. The Aruba mobility platform delivers a complete FIPS 140-2 validated solution that meets the Federal government’s stringent requirements as defined in the DoD policy 8100.2 and its addendum, while addressing 802.11i and non-802.11i compliant devices alike.

Key Features / Benefits

Superior Architecture

- A centralized and programmable encryption architecture ensures scalability and unmatched security. As new encryption protocols emerge, the mobility infrastructure can be upgraded with minimum disruption.
- The contained encryption boundary offered by Aruba’s mobility controller architecture sets the standard for best practices in security key distribution and management in wireless networks.
- Government organizations can leverage commercial off-the-shelf (COTS) technologies available for the 802.11i wireless security standard for their wireless deployments, keeping purchasing costs low.
- The adoption of COTS technologies for wireless security by the Federal government also significantly lowers costs associated with user training, administration, and updates, while increasing a user’s familiarity with the products.
- Legacy wireless clients that do not support 802.11i can be secured with xSec, a FIPS validated Layer 2 encryption technology, leveraging existing equipment.

Solution Components

Aruba Mobility Controllers:

Aruba mobility controllers are the centralized intelligence behind the Aruba User Centric mobility solution. Mobility controllers provide a single point of management and control for all the components needed to deploy a secure WLAN solution including a stateful identity based policy enforcement firewall, Wireless IDS, Client integrity, Layer 2 encryption and remote access. Aruba mobility controllers are available for a range of applications from small office to large data centers. Aruba mobility controllers are FIPS 140-2 validated for 802.11i and xSec.

Aruba Access Points:

Aruba access points are designed to maximize coverage and throughput for dense deployments in a range of environments. Access points do not terminate encrypted traffic to maintain information integrity over the wireless and wired connection so they do not require FIPS certification. Aruba access points are self-configuring, self-healing and remotely managed. Aruba access points can be deployed across a Layer 2/3 network and even across a public network to connect to the centrally located mobility controller. They can also act as a standalone Air Monitors for Wireless IDS applications and perform remote packet-capture for troubleshooting.

About Aruba Networks

Aruba is the global leader in distributed enterprise networks. Its award-winning portfolio of campus, branch/teleworker, and mobile solutions simplify operations and secure access to all corporate applications and services - regardless of the user's device, location, or network. This dramatically improves productivity and lowers capital and operational costs.

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>. For real-time news updates follow Aruba on [Twitter](#), [Facebook](#), or the [Green Island News Blog](#).



1344 Crossman Ave. Sunnyvale, CA 94089-1113
Tel. 408.227.4500 | Fax. 408.227.4550 | 1-866-55-ARUBA
info@arubanetworks.com | <http://www.arubanetworks.com>