

# FIPS VALIDATED 802.11i SECURITY FOR GOVERNMENT LANS

## Challenge

The rapid proliferation of mobile devices increases security risks as users and devices traverse networks and locales, some secure, some not. IT organizations are challenged to preserve user access rights and privileges while fully validating each client every time new access is requested.

## Solution

This combination of Aruba's powerful mobility controllers with Juniper Networks Odyssey Access Client FIPS Edition delivers a complete FIPS 140-2 validated secure mobile solution that meets the governments' most stringent requirements, while addressing both 802.11i and non-802.11i compliant devices.

## Benefits

- Provides a centralized and programmable encryption architecture that ensures scalability and unmatched security.
- Leverages commercial off-the-shelf (COTS) technologies.
- Significantly lowers costs associated with user training, administration and updates.
- Supports legacy wireless clients that do not support 802.11i, leveraging existing equipment.

With a fast-growing mobile workforce and significant increases in the number of mobile devices being used by employees, contractors, guests and others attempting to access their networks, government agencies have a strong need and desire to define a robust wireless security policy—particularly in light of the vast amounts of sensitive, classified information they have under their control.

Until recently, the only wireless option available to government agencies had been to deploy a Layer 2 encryption overlay on top of their wireless infrastructure (per Department of Defense Directive (DoDD) 8100.2). Not only cumbersome and costly, this option also does not provide the radio frequency (RF) management and intrusion detection system (IPS) capabilities of today's centralized mobility systems.

While there is a mandate to use Federal Information Processing Standards (FIPS) validated 802.11i solutions for non-classified government networks, there lacks a comprehensive solution for the government's many legacy clients and access points that do not support 802.11i.

Today, enterprise alliance partners Aruba Networks and Juniper Networks® offer a FIPS validated 802.11i solution with a clear migration path for existing clients, legacy clients and access points.

## The Challenge

Mobility and the increased need for security are dramatically changing today's networking landscape for government agencies. Rapid proliferation of mobile devices increases security risks as these devices move through a variety of networks and connect to an agency's network from various locations—some secure, some not. As these devices traverse networks and locales, user access rights and privileges need to be preserved, and each client must be fully validated every time new access is requested.

Organizations have been forced to perform this integration with limited success. Now, Aruba Networks and Juniper Networks have partnered to create joint solutions that solve these integration and management challenges and ease the deployment of seamless, secure mobile connectivity.

## The Juniper Networks and Aruba Networks FIPS Validated 802.11i Security Solution

Through the Juniper enterprise alliance technology partnership program, Juniper and Aruba have co-developed solutions that provide a comprehensive, validated offering that meets strict government IT and network security requirements.

Aruba and Juniper are the only partners that can offer a comprehensive FIPS validated 802.11i solution today. A modified driver is needed to run 802.11i in a FIPS-compliant configuration, but these drivers are not available for all devices and platforms. Juniper and Aruba have jointly developed the xSec protocol to address this problem. xSec is a standards-based, Layer 2 protocol that can provide FIPS-compliant Advanced Encryption Standard (AES) encryption over off-the-shelf 802.11 adapters and drivers. The selected adapter does not need to support 802.11i; xSec also provides AES encryption over 802.1X wired connections.

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. Only Aruba's mobility controller needs to be FIPS validated. Juniper Networks Odyssey Access Client FIPS Edition is compatible with the Department of Defense (DoD) Common Access Card (CAC) standard, and supports both the Aruba/Juniper jointly developed xSec and 802.11 standards through its own embedded FIPS 140-2 Level 1, which has been validated by the National Institute of Standards and Technology (NIST) cryptographic module and meets the most rigorous government encryption standards. OAC FIPS Edition also offers the advanced management features needed by large government organizations with multiple facilities and sites.

This combination of Aruba's powerful mobility controllers with Juniper's robust OAC FIPS Edition delivers a complete FIPS 140-2 validated solution that meets the government's most stringent requirements, while addressing both 802.11i and non-802.11i compliant devices.

### Features and 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.

#### Investment Protection

Government organizations can finally leverage commercial off-the-shelf (COTS) technologies available for the 802.11i wireless security standard in their wireless deployments, keeping purchasing costs low.

The adoption of COTS technologies for wireless security by the 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 standards-based, Layer 2 protocol that provides FIPS-compliant AES encryption, leveraging existing equipment.

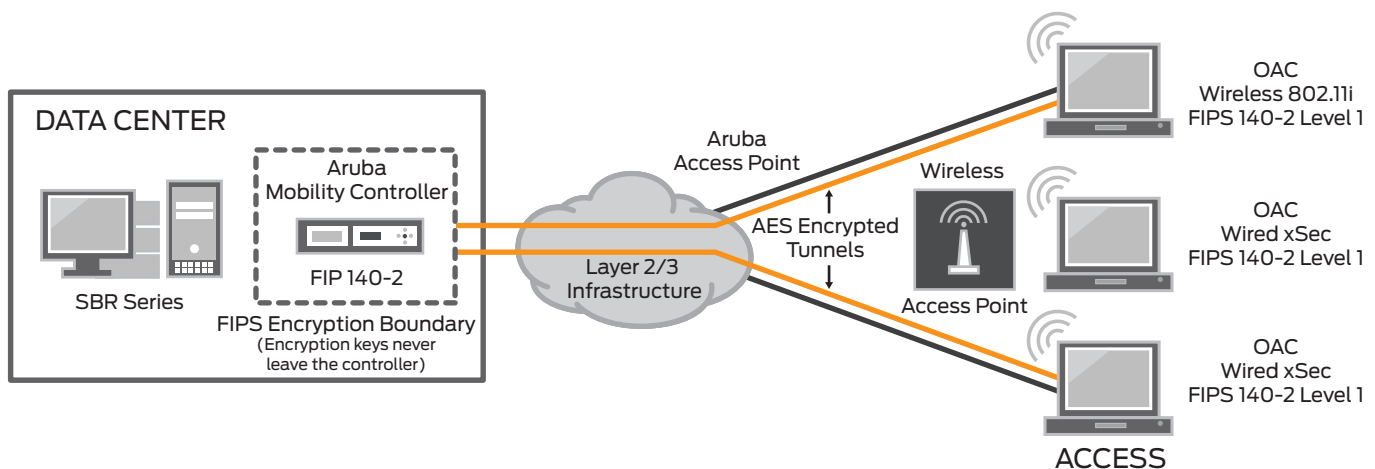


Figure 1: Juniper Networks Unified Access Control Solution with Aruba WLAN

## Solution Components

### Aruba Mobility Controllers

Aruba mobility controllers are the centralized intelligence behind the Aruba Networks mobility overlay. Mobility controllers integrate all of the components needed to deploy a secure wireless local area network (WLAN) solution including an identity-based policy enforcement engine, wireless IPS, 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.

### Aruba Access Points

Aruba access points are designed for dense deployments in a range of environments to maximize coverage and throughput. Access points do not terminate any encryption 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 standalone Air Monitors for Wireless IPS applications and perform remote packet-capture for troubleshooting.

### Juniper Networks SBR Series Steel-Belted Radius Servers

Juniper Networks SBR Series Steel-Belted Radius Servers empower enterprises with complete control over how users access their networks. The SBR Series enhances the security and manageability of any network—centralizing user authentication, configuring the appropriate access level, and controlling who's authorized to access the network. SBR Series Steel-Belted Radius Servers can manage the busiest networks and easily scale to accommodate a growing network. A complete, standards-based implementation of the RADIUS protocol, the SBR Series performs three crucial access control functions: Authentication, Authorization and Accounting (AAA). The SBR Series enables enterprises to centrally and uniformly enforce network access and security policies, and configure restrictions or special requirements for user access. The SBR Series supports nearly all access technologies, user authentication stores, and authentication protocols. Already in use in the world's busiest networks managing millions of user transactions daily, SBR Series Steel-Belted Radius Servers are the gold standard for AAA/RADIUS servers.

### Juniper Networks Odyssey Access Client

Juniper Networks Odyssey Access Client is a complete family of secure 802.1X access clients purpose-built for enterprises and government agencies. OAC delivers strong security capable of fully protecting network data and user credentials, and can be easily and quickly deployed and managed enterprise-wide for the lowest total cost of ownership (TCO). An enterprise-class 802.1X supplicant/

access client with full support for advanced network protocols and identity-based connections, OAC secures user authentication and connections, ensuring that login credentials will not be compromised, and that data privacy will be maintained.

The OAC product line includes a specialized edition of OAC—OAC FIPS Edition—that incorporates the Odyssey Security Component, a cryptographic module that has been FIPS 140-2 Level 1 validated (by NIST and the Canada Communications Security Establishment). OAC FIPS Edition is compatible with U.S. Department of Defense (DoD) Common Access Card (CAC) standards and supports the xSec protocol, which utilizes AES encryption. All client-side cryptographic xSec operations are performed using its integrated cryptographic module. OAC FIPS Edition also supports the 802.11i standards, and operates with FIPS certified access points.

OAC FIPS Edition supports Windows 2000 and Windows XP. OAC FIPS Edition requires a modified driver to enable wireless adapters to run 802.11i in FIPS mode. OAC FIPS Edition supports FIPS compliance with Atheros chipsets for Peripheral Component Interconnect (PCI), Cardbus, mPC, PCIe, and mPCIe (AR5001, AR5002, AR5004, AR5005, AR5006); the Intel® PRO/Wireless 3945ABG and Intel® Wireless WiFi Link 4965AGN chipsets; and any Broadcom chipset (including, but not limited to BCM2050, BCM2060, BCM4306, BCM4309, BCM4311, BCM4312, BCM4318, BCM4321). Please note that USB WLAN network interface cards (NICs) are not supported by the FIPS modified drivers in OAC FIPS Edition. Also, please note that there are no special adapter or driver requirements needed to run xSec in FIPS mode.

## Summary

Aruba's powerful mobility controllers with Juniper's robust Odyssey Access Client FIPS Edition deliver a complete FIPS 140-2 validated solution that meets the government's most stringent requirements, while addressing both 802.11i and non-802.11i compliant devices. This solution provides a centralized and programmable encryption architecture that ensures scalability and unmatched security while leveraging commercial off-the-shelf (COTS) technologies, significantly lowering costs associated with user training, administration and updates.

## Next Steps

Please contact Juniper Networks for additional information about the Juniper Networks/Aruba joint security solution.

For more information on and a 30-day FREE trial of the SBR Series, please go to [www.juniper.net/sbr-series](http://www.juniper.net/sbr-series).

For more information on and a 30-day FREE trial of OAC, please go to [www.juniper.net/oac](http://www.juniper.net/oac).

## About Juniper Networks

Juniper Networks, Inc. is the leader in high-performance networking. Juniper offers a high-performance network infrastructure that creates a responsive and trusted environment for accelerating the deployment of services and applications over a single network. This fuels high-performance businesses. Additional information can be found at [www.juniper.net](http://www.juniper.net).

## About Aruba Networks

The business drivers and application requirements for mobility vary considerably across vertical markets. These disparate needs require a dedicated focus on each industry to serve the unique complexities and nuances that exist. Aruba offers a comprehensive mobility solution that serves applications for all industries as well as targeted products, features and technology partnerships that provide a focused solution for vertical markets.

Aruba Networks is headquartered in Sunnyvale, CA. More information can be found at: [www.arubanetworks.com/company/contact\\_us.php](http://www.arubanetworks.com/company/contact_us.php).

---

### Corporate and Sales Headquarters

Juniper Networks, Inc.  
1194 North Mathilda Avenue  
Sunnyvale, CA 94089 USA  
Phone: 888.JUNIPER (888.586.4737)  
or 408.745.2000  
Fax: 408.745.2100  
[www.juniper.net](http://www.juniper.net)

### APAC Headquarters

Juniper Networks (Hong Kong)  
26/F, Cityplaza One  
1111 King's Road  
Taikoo Shing, Hong Kong  
Phone: 852.2332.3636  
Fax: 852.2574.7803

### EMEA Headquarters

Juniper Networks Ireland  
Airside Business Park  
Swords, County Dublin, Ireland  
Phone: 35.31.8903.600  
EMEA Sales: 00800.4586.4737  
Fax: 35.31.8903.601

To purchase Juniper Networks solutions, please contact your Juniper Networks representative at 1-866-298-6428 or authorized reseller.

Copyright 2010 Juniper Networks, Inc. All rights reserved. Juniper Networks, the Juniper Networks logo, Junos, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered marks, or registered service marks are the property of their respective owners. Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.