WHITE PAPER

A GUIDE TO IMPLEMENTING THE DOD MOBILITY STRATEGY

aruba NETWORKS

TABLE OF CONTENTS

INTRODUCTION

The U.S. Department of Defense (DoD) leads the world in the deployment of mobile information, communication, and computing systems, and has held that leadership position for decades.

In that context, it can be a bit puzzling to hear that mobility is now being looked at as something new. Yet there are countless hours now being spent on the strategy and tactics around adoption of mobility in the DoD. What has changed?

For the most part, it is the widespread availability of low-cost consumer-oriented mobile devices such as tablets and smartphones, along with commercial wireless networks that connect those devices to applications and information.

In the past, the DoD has deployed custom military-grade solutions to solve mobility requirements. Today, the DoD leadership sees tremendous cost, productivity and usability advantages to adopting the same mainstream mobile technology.

However, as with any new technology, there are a host of technical and policy obstacles to navigate. This paper describes the Aruba Networks perspective on what it all means and how it can be done.

It is important to put context around mobility and mobile device. In the broader context, mobility is about much more than just smartphones. A smartphone is really a mobile, battery-operated computing platform with voice communication capabilities – something that could easily be applied to laptop computers as well.

When considering a mobility strategy, it is vital to take a holistic look at the domain to see where technologies can support multiple mission requirements. For example, a Wi-Fi network that supports logistics for cargo can also support iPad applications for accessing weather data. At its core, mobility is really about secure access to information anywhere, anytime, and using the appropriate device for the task at hand.

Still, the current focus on mobility in the DoD is decidedly biased toward smartphones and tablets. There is already a strong precedent for use of laptop computers and specialized handheld devices connected to DoD-operated Wi-Fi networks.

In order to avoid confusion with these existing types of devices, DoD policy has defined the term Commercial Mobile Device (CMD) to mean:

"A subset of portable electronic devices (PED) as defined in DoDD 8100.02 that provide one or more commercial wireless interfaces along with a compact user input interface (touch screen, miniature keyboard) and exclude PEDs running a multi-user operating system (Windows OS, Mac OS). This definition includes, but is not limited to smartphones, tablets, and e-readers."[1]

This paper will continue to use the CMD term as defined in the referenced DoD memorandum.

ABOUT ARUBA NETWORKS

Aruba Networks is a leading provider of next-generation network access solutions for the mobile enterprise. Aruba's expertise is rooted in its intimate understanding of how to provision, securely connect and manage mobile devices.

As a vendor who builds the infrastructure to connect mobile devices to their applications, Aruba is in a unique position to see the mobility solution's big picture. Aruba solutions include secure wireless LAN (WLAN), remote access, outdoor mesh networks, guest and contractor access, classified communication using commercial devices, and network access control (NAC).

The Aruba mobility architecture enables government agencies to easily scale networks to accommodate the latest commercial smartphones and tablets and support both unclassified and classified services on the same infrastructure. Offering purpose-built solutions, Aruba allows government agencies to securely meet the demands of their users, who require anywhere and anytime access to enterprise information.

With Aruba, context-aware access privileges are linked based on user identity, their device, and location, along with providing application awareness capabilities. That means your agency's workforce has consistent, secure access to network resources – no matter where they are, what devices they use or how they connect.

THE DOD MOBILITY VISION

In May 2012, the office of the DoD chief information officer published the Department of Defense Mobility Device Strategy to provide a high-level vision of the department's goals and objectives surrounding mobility.

"The DoD Mobile Device Strategy identifies information technology (IT) goals and objectives to capitalize on the full potential of mobile devices. It focuses on improving three areas critical to mobility: wireless infrastructure, the mobile device itself, and mobile applications. It allows mobile activities across the Department to converge toward a common vision and approach. Although mobile devices are the new and popular item in today's commercial market, this strategy is not simply about embracing the newest technology – it is about keeping the DoD workforce relevant in an era when information and cyberspace play a critical role in mission success."[2]

The first of these areas, the infrastructure area, is where DoD IT managers can have the greatest impact. Within the infrastructure goal are three objectives:

1. Evolve spectrum management
2. Expand infrastructure to support wireless capabilities
3. Establish a mobile device security architecture

Objective 1: Evolve spectrum management

The DoD is not unique in the need to deal efficiently with electromagnetic spectrum, particularly in the unlicensed bands. In the early days of Wi-Fi, manual site surveys were performed to measure sources of interference, impediments to signals, and site conditions in order to determine optimal access point (AP) placement, channel assignment, and transmit power levels.

Unfortunately, manual site surveys measured only a snapshot in time, and given the dynamic nature of enterprise and government facilities, conditions could change at any moment. Aruba Networks was the pioneer of Adaptive Radio Management™ (ARM), a technology that was first developed to automate channel assignment and power control. Today, millions of Aruba APs use ARM™ daily to maintain maximum performance.

APs are only one part of the equation, however. Wireless client devices also play a major role in overall network performance, and this is where the introduction of CMDs must be carefully controlled. CMDs are often designed for consumer environments where a single Wi-Fi AP is available. The CMD connects and remains connected to that AP, no matter what.

CMD hardware and software are often not optimized for enterprise environments that are characterized by multiple APs, frequent roaming and widespread interference from other client devices. At best, CMDs are variable in their performance and behavior – and variability is not a welcome trait for a mission-critical application.

For that reason, Aruba developed ClientMatch™, an extension to ARM, which takes away much of the client variability by putting controls in the network infrastructure. Using ClientMatch, neighboring Aruba APs compare signal strength, load conditions, RF band saturation, and non-Wi-Fi sources of interference in the spectrum.

This information is used to steer a client device to the optimal AP on the optimal channel, which improves network performance and reduces overall RF interference. While client devices support advanced control technologies like 802.11k, Aruba APs signal the client to adjust transmit power levels, further reducing interference. The result is maximum performance, minimum interference, and predictability throughout the Wi-Fi environment.

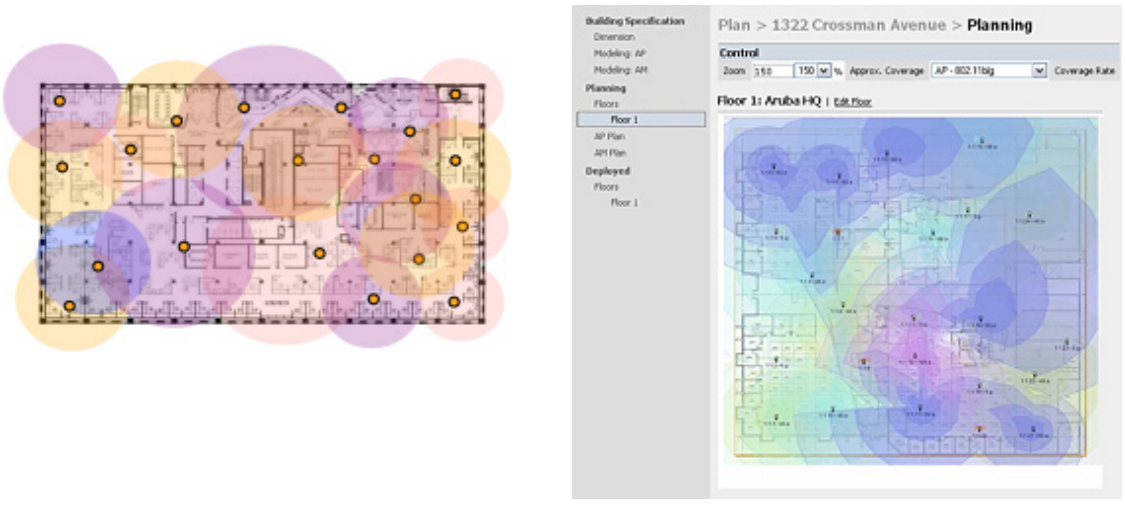

Figure 1: Adaptive Radio Management

The latest generation of Aruba 802.11ac APs offers further spectrum management tools through Aruba RFProtect™ spectrum visibility. Using this technology, APs provide real-time monitoring and classification of interference sources in the 2.4-GHz and 5-GHz bands where Wi-Fi operates.

RFProtect can classify and locate common sources of interference, such as cordless phones, video cameras, Bluetooth, and microwave ovens. Armed with this information, government network managers can quickly solve wireless performance problems without the guesswork often inherent in wireless troubleshooting.

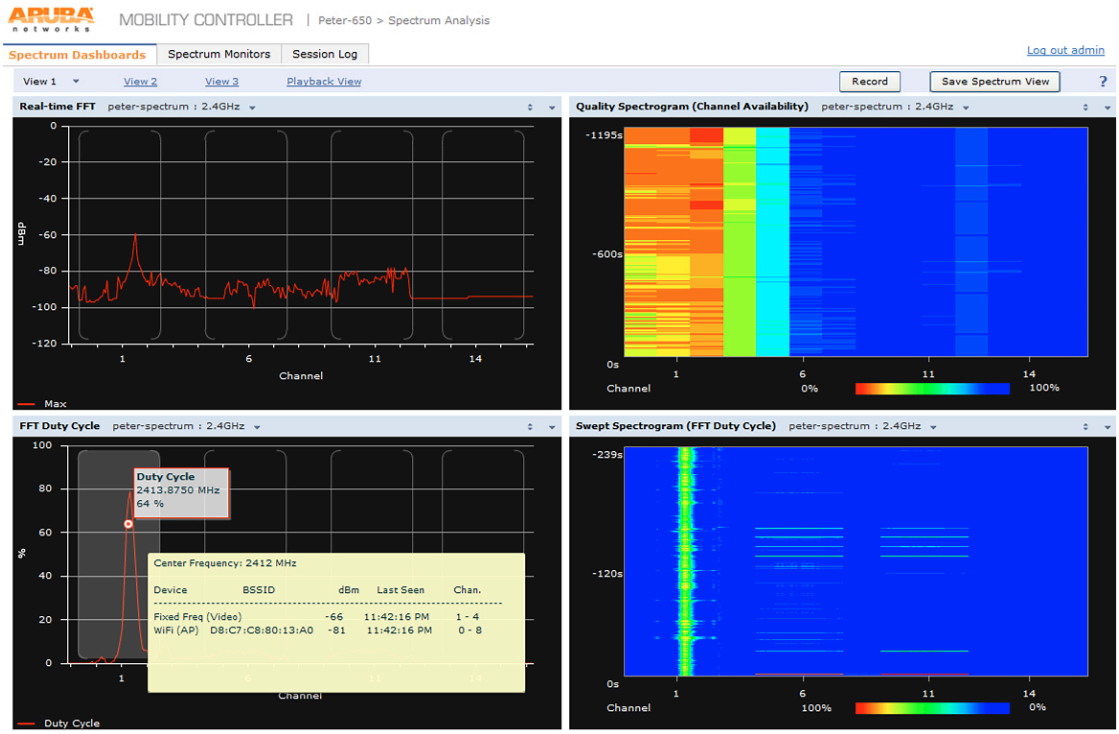

Figure 2: Integrated Spectrum Monitoring and Management

Through the use of ARM and RFProtect, government network managers can ensure they are getting the maximum possible utilization of precious RF spectrum while minimizing waste. As more IT devices become wireless, spectrum management will become increasingly vital.

Objective 2: Expand infrastructure to support wireless capabilities

Aruba is already a major supplier of enterprise-grade Wi-Fi infrastructure for the DoD. Today, Aruba has tens of thousands of wireless APs and Mobility Controllers operating under Approvals to Operate (ATOs) on the unclassified side and a growing number of deployments on the classified side.

These deployments began in 2005 with previous-generation 802.11a/b/g WLANs, and have steadily evolved to increase Wi-Fi client density, performance, and the number of devices supported. Today's 802.11n networks, which support throughput of up to 300 Mbps per radio, commonly deliver wire-like performance for client devices.

The next generation of wireless technology, 802.11ac, promises to improve aggregate throughput up to 1 Gbps and greater once it becomes widely adopted over the next several years. The progress within the Wi-Fi industry over the past decade has been remarkable, and technological advances continue to be made.

Unclassified Wi-Fi is divided into two categories – those that connect to a Non-classified IP Router Network (NIPRNet) and those that provide only commercial Internet service. Internet-only networks are simpler to accredit, have dramatically lower security requirements, and, importantly, permit CMDs to connect with few conditions.

The process for connecting client devices to a NIPRNet is much more stringent. NIPRNet-connected wireless deployments must meet several DoD directives and Security Technical Information Guides (STIGs). The final section of this paper reviews many of these requirements.

Classified wireless networks using CMDs must conform to guidance from the NSA Commercial Solutions for Classified (CSfC) program. Products must be selected from the CSfC Approved Product List, and two independent layers of Suite B cryptography must be deployed to protect classified information.

Despite this complexity, the enablement of CMDs like smartphones and tablets on a CSfC architecture – instead of legacy Type I encryption equipment – allows the use of new classified applications that embrace mobility at a much lower cost. Click here for more information about Aruba wireless technology for classified environments.

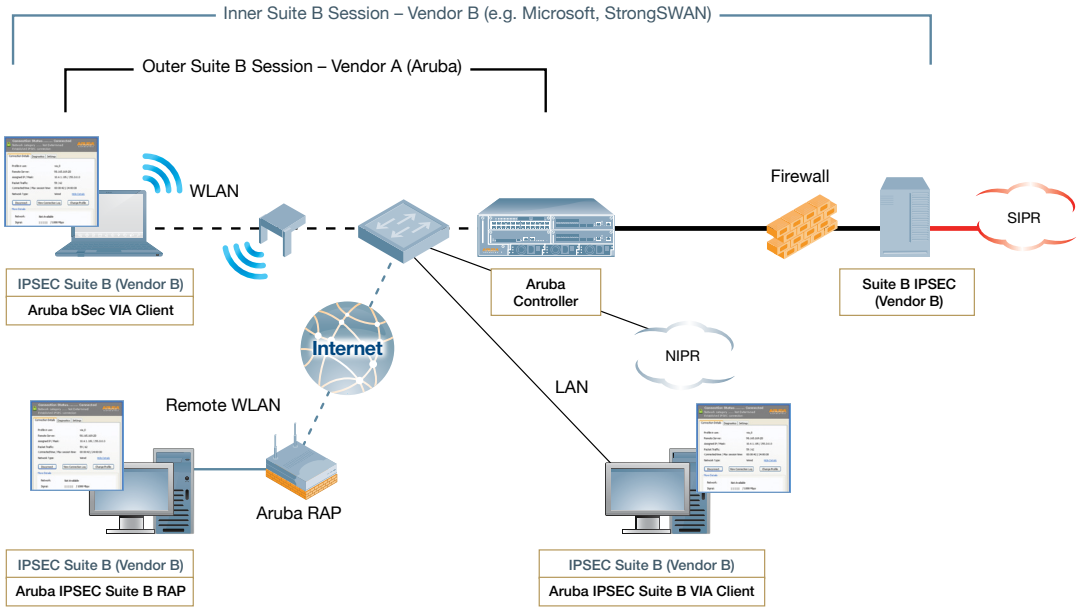

Figure 3: Commercial Solutions for Classified Architecture

In addition to Wi-Fi, the DoD Mobility Device Strategy calls for "persistent VPN technologies to ensure that mission-critical mobile applications experience continuous connectivity through the use of advanced commercial and DoD network technologies."

This part of the strategy would allow a CMD to establish a secure encrypted connection to a DoD network across Wi-Fi and 3G/4G infrastructures, no matter where the user roams. Security context stays with the user, rather than requiring the user to understand the wireless connectivity mode and adjust the security context to match.

The Aruba Virtual Intranet Access™ (VIA) client software is built for just such a requirement. Available for most popular CMDs as well as multi-user operating systems, VIA™ automatically detects when it is connected to a trusted network versus an untrusted network, and establishes a persistent VPN connection automatically when needed.

This frees up valuable resources and conserves battery life when the VPN is not necessary, but ensures that a secure connection is always available when needed without requiring the user to interact with the application.

VIA's head-end termination point is the Aruba Mobility Controller. This can be the same Mobility Controller used for WLAN operations, but typically a dedicated controller is placed in an Internet DMZ. VIA supports Suite B cipher suites, making it suitable for deployment in classified environments.

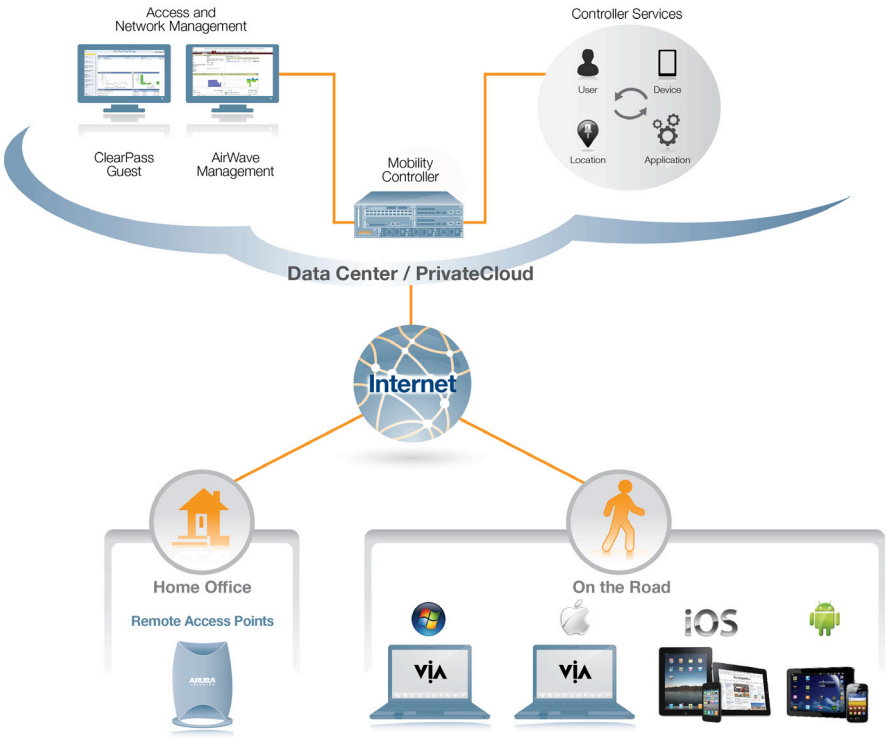

Figure 4: Aruba's Virtual Internet Access (VIA) Client

Secure wireless connectivity necessarily involves an authentication and authorization process. Whether using common access cards (CACs) for wireless authentication, Elliptic Curve Digital Signature Algorithm (ECDSA) software certificates for Suite B, or simple username/password authentication, the Aruba ClearPass Policy Manager serves as a centralized point of control for network access.

Implementing standard protocols such as RADIUS and TACACS+, and with a rich policy-definition language that understands multiple sources of authentication and authorization information, Aruba ClearPass ensures that mobile devices and users obtain network access at the correct level of security.

Aruba ClearPass is not only for wireless or for use exclusively with Aruba WLANs. ClearPass supports nearly all popular wired, wireless and remote access infrastructures, and has the intelligence to instantiate policies differently, depending on the capabilities of the equipment.

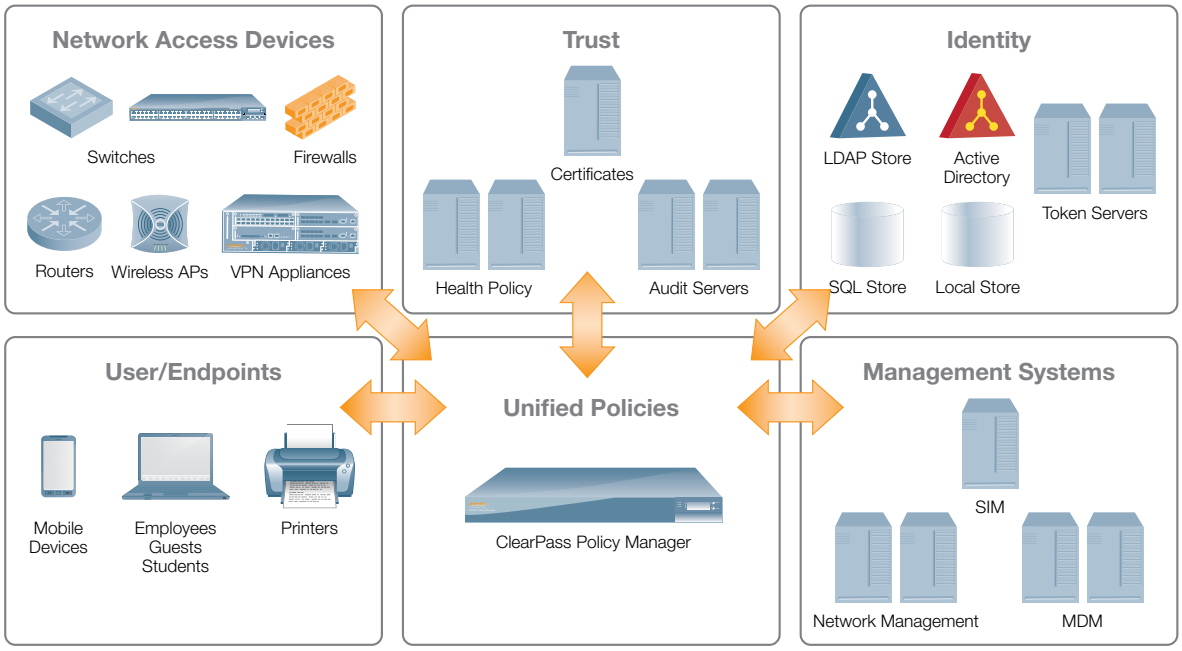

Figure 5: ClearPass Policy Manager

ClearPass can also be deployed in a guest/visitor management role, where it controls credentials, policies and provisioning of non-enterprise devices that attempt to connect to a wired or wireless network. Part of this functionality involves the familiar captive portal capability used by thousands of Wi-Fi hotspots around the world to authenticate users through a standard web browser.

To manage an enterprise bring-your-own-device (BYOD) strategy, ClearPass authenticates users, authorizes them for BYOD, and securely provisions their CMDs for network access. Once provisioned, the level of network access granted to a personal device is managed by the ClearPass AAA capabilities in conjunction with an Aruba Mobility Controller.

Objective 3: Establish a mobile device security architecture

MDM permits central control over parameters like authentication credentials, wireless settings, camera and Bluetooth settings, and application policies. Information about device compliance with MDM policies is valuable when making network access control decisions.

For this reason, ClearPass Policy Manager includes MDM Connector – middleware that integrates with popular MDM systems to enable MDM status information to be used as a policy input for network access control. ClearPass Policy Manager with MDM Connector provides full linkage between a mobile device security architecture and a network access control architecture.

Click here for more information on Aruba ClearPass.

DEPLOYING MOBILE DEVICES WITHIN DOD POLICIES

Meeting the general goals and objectives of a vision is one thing, but the rubber meets the road when it comes to complying with DoD policies. This section summarizes key DoD requirements around mobile device deployments and provides techniques and ideas that will prove beneficial during the accreditation process.

The Defense Information Systems Agency (DISA) Unified Capabilities Requirements (UCR)[3] section 5.3.6.2 defines two use cases for mobile devices. Use Case 1, which is known as a CMD, has no connectivity to a DoD network. Use Case 2 supports connectivity to a DoD network such as NIPRNet. There is a dramatic difference in requirements between these two use cases.

Use Case 1: CMDs not connected to DoD networks

In 2012, the policy governing non-connected CMDs is the DoD Commercial Mobile Device Interim Policy.[4] Attachment 2 of that Policy spells out specific requirements that must be met in order to use CMDs. The most important of these are:

- Connection to DoD networks is prohibited.
- Processing, storing, transmitting or receiving any information other than that which is publicly releasable is prohibited.
- Internet access must occur through a commercial Internet service provider (ISP).
- Access to DoD email is prohibited.
- CMDs used for this purpose must be listed on the DoD Unified Capabilities Approved Product List (UC-APL).

One implementation challenge for Use Case 1 involves areas where a DoD-connected WLAN is already present. It is impractical and expensive to setup a second WLAN in the same physical location, given the potential for RF interference and the need to install a second parallel network of APs.

Fortunately, Aruba Networks provides a mechanism that allows a single AP to supply wireless service for multiple disparate networks by isolating traffic between those networks, a technical means permitted by the January 2012 DoD Interim Policy:

"Non-sensitive information shall only be transferred to and from non-enterprise activated CMDs using the public Internet or a CIO designated workstation that only connects to a demilitarized zone (DMZ) that meets the DoD requirement that such contacts are isolated from other DoD systems by physical or technical means."

First, Aruba's centralized encryption technology isolates wireless traffic from the client device all the way to the Mobility Controller. Once traffic is decrypted and processed inside the Mobility Controller, the Common Criteria EAL4-evaluated firewall in the Mobility Controller continues to provide traffic separation and prevents traffic from Use Case 1 devices from reaching DoD networks.

If desired, Use Case 1 traffic can be immediately encapsulated into IP-in-IP or IPsec tunnels for transport to an Internet-connected router located at a commercial ISP, ensuring that IP address space for this service comes from an ISP rather than a DoD pool.

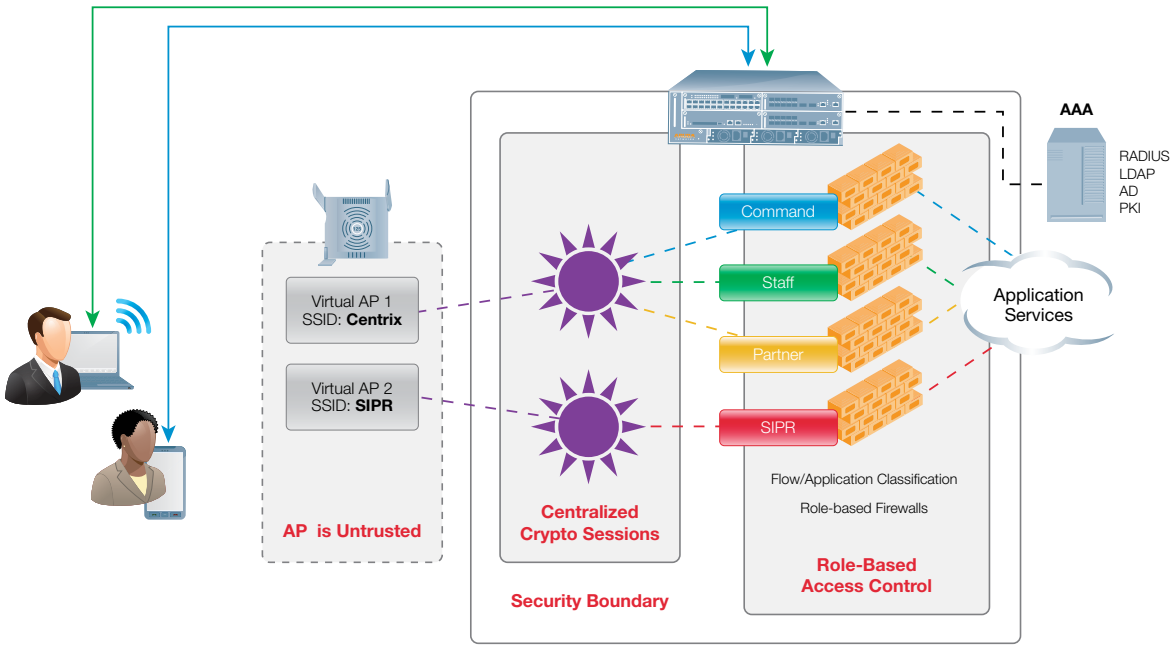

Figure 6: Role-based Access Control

Use Case 2: CMDs connected to DoD networks

This use case is far more challenging to implement. A CMD connected to a DoD network must meet the same requirements that a PC, laptop or other device must meet, including compliance with all relevant STIGs. Two requirements are particularly challenging for CMDs:

- Data in transit and data at rest must be protected using FIPS 140-2 validated encryption.
- Access to a DoD network must be CAC-authenticated.

For Apple iOS devices, an interim STIG4 has been published. While this STIG is specific to iOS, it highlights issues that will be present in other operating systems like Android. Note that while FIPS 140-2 validation of some cryptographic components is in process for iOS, this validation does not include data-in-transit components such as Wi-Fi.

In 2012, the same is true of other CMDs. As a result, it is not be possible to directly connect a CMD to a DoD WLAN and rely on Wi-Fi encryption to protect government data. And while smart card readers like Tactivo from Precise Biometrics are available for iOS devices, the native iOS 802.1X supplicant cannot make use of these readers – making CAC authentication impossible.

Aruba offers a potential solution through its VIA client. Available for Windows, Mac OS X, Android, iOS and Linux, VIA provides IPsec and/or SSL VPN connections to an Aruba Mobility Controller. FIPS 140-2 validation is underway for this product and a Common Criteria evaluation against the VPN Client Protection Profile is planned in the near future.

In addition, because VIA is application software and not tied to the operating system, it is possible to integrate smart card readers into the application. Using VIA, requirements for FIPS validation and CAC authentication can be fulfilled.

SUMMARY

The use of CMDs in the DoD will be in the forefront of information and communication over the next several years. Technology and operational requirements are new and continue to evolve. Consequently, a close partnership between DoD and industry is needed to ensure that DoD requirements are integrated into future products and that deployments become standardized – in the same way that Windows laptops are connected to DoD Wi-Fi networks. Aruba Networks will continue to lead the industry in solving DoD mobility challenges.

Figure 7. Integrating iPhone CAC Reader with VIA client allowing policy compliant access to DoD networks

[1] DoD Commercial Mobile Device (CMD) Interim Policy, 17 January 2012. http://www.hsdl.org/?view&did=712435
[2] DoD Mobile Device Strategy, 8 June 2012. http://www.defense.gov/news/dodmobilitystrategy.pdf
[3] Unified Capabilities Requirements Change 3 http://www.disa.mil/_large_files/DOD_UCR_2008_Change_3.pdf
[4] Apple iOS 6 Interim STIG. http://iase.disa.mil/stigs/net_perimeter/wireless/smartphone.html#iOS6

ABOUT ARUBA NETWORKS, INC.

Aruba Networks is a leading provider of next-generation network access solutions for the mobile enterprise. The company's Mobile Virtual Enterprise (MOVE) architecture unifies wired and wireless network infrastructures into one seamless access solution for corporate headquarters, mobile business professionals, remote workers and guests. This unified approach to access networks enables IT organizations and users to securely address the Bring Your Own Device (BYOD) phenomenon, dramatically improving productivity and lowering 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, Africa and Asia Pacific regions. To learn more, visit Aruba at www.arubanetworks.com. For real-time news updates follow Aruba on Twitter and Facebook, and for the latest technical discussions on mobility and Aruba products visit Airheads Social at http://community.arubanetworks.com.

aruba NETWORKS

1344 CROSSMAN AVE | SUNNYVALE, CA 94089
1.866.55.ARUBA | T: 1.408.227.4500 | FAX: 1.408.227.4550 | INFO@ARUBANETWORKS.COM

www.arubanetworks.com