WHITE PAPER

COMBATANT COMMAND (COCOM) NEXT-GENERATION SECURITY ARCHITECTURE USING NSA SUITE B

aruba NETWORKS

TABLE OF CONTENTS

COMBATANT COMMAND (COCOM) NEXT-GENERATION SECURITY ARCHITECTURE USING NSA SUITE B

The local site classified networking team at a COCOM was faced with several challenges resulting from the use of legacy encryption systems on clients that connect to its classified networks.

These networks were being underutilized as a result of several inherent technical and financial issues associated with the existing architecture including:

- The huge expense of installing and maintaining classified networks that are policy compliant and accredited.
- Usability issues with government-sponsored proprietary cryptology systems such as a high-assurance Type 1 system.
- Low performance when using these cryptosystems for network access.
- Keying and rekeying issues associated with Type 1 systems.

Working with the NSA and COCOM G2/G6, the local site classified networking team responsible for network operations and policy compliance was tasked with designing and accrediting a vastly improved next-generation security architecture to replace legacy Type 1 systems.

This new architecture uses NSA-approved Suite B cryptographic capabilities that provide:

- Easier and more affordable deployment and management.
- Better operational performance.
- An inexpensive way to provide secure site and remote access to authorized users.

In addition to the cost savings afforded by commercial technologies, the solution delivers a variety of strategic benefits, including:

- Improved classified network access for authorized personnel.
- A high-performance network that supports and operates without physical-hardened network connections.
- Secure access for a larger user population at much lower expense.
- Lower costs to deploy and operate.
- Faster network performance prompting higher user adoption and satisfaction.
- Elimination of the issues associated with operating Controlled Cryptographic Items (CCIs) and securing them when not in use. With expanded access, users have more flexibility to contribute to their agency missions.
- Facilitation of interagency and intergovernmental collaboration.

Since Suite B systems are based on commercially available technology, they are approximately 10% of the purchase cost of a Type 1-certified solution and cost far less to operate. The result of the local site networking team's effort produced an accredited, lower cost and better performing solution for deploying IPsec VPNs, which provide site-to-site and remote connections for the U.S. and coalition forces.

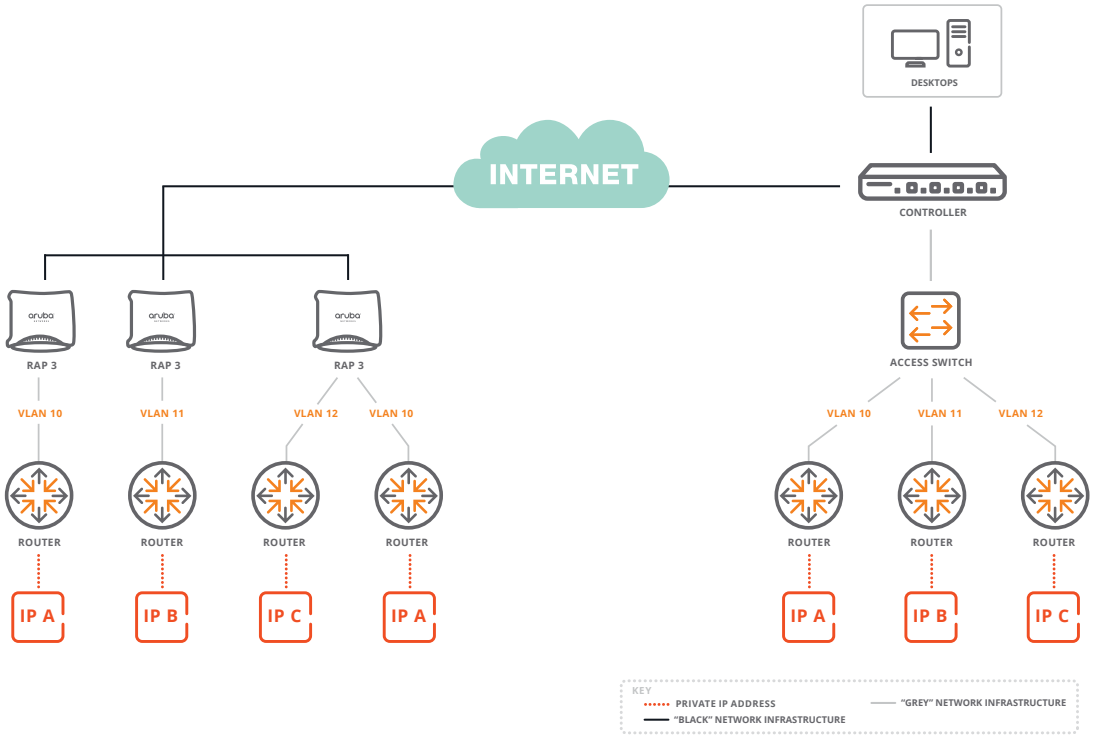
This solution utilizes a multivendor, dual-encryption tunnel architecture. The key elements of the architecture consist of an Aruba Networks® Mobility Controller at the central facility, which terminates an outer Suite B encryption tunnel sourced from Aruba Remote Access Points (RAPs) at the coalition site.

A second inner tunnel at the central facility utilizes a router paired to another router located at the coalition site. Together, the combined strength of the dual-tunnel approach meets conditions of the NSA Commercial Solutions for Classified program for safeguarding classified networks.

As depicted in the diagram below, the Aruba Mobility Controller and RAPs attach to a "black" network infrastructure. They utilize Suite B X.509 certificates issued by the COCOM certificate authority (CA).

On the back of the Aruba Mobility Controller and RAPs are defined "gray" VLANs that connect to routers. Firewall rules are defined on Aruba devices and the routers to only allow IKEv2 connections between statically-defined addresses on the "gray" network interfaces of the routers.

On the back of the routers at the remote and headquarters sites is a private IP addressing/VLAN defined for the "red" network device/application access. Additionally, Aruba Mobility Controllers feature a management interface that provides secure administrative control over Mobility Controllers and RAPs.



COCOM Next-Generation Security Architecture

As a result of this architcture, COCOMs and other government agencies now have access to a fully-accredited solution for deploying their next-generation security architecture using NSA-approved Suite B cryptography on classified networks.

NSA COMMERCIAL SOLUTION FOR CLASSIFIED (CSFC) PROGRAM OVERVIEW

The secure sharing of information among Department of Defense, coalition forces, and first-responders is driving the need for widespread cryptographic interoperability and for NSA-approved information assurance products that meet appropriate security standards to protect classified information.

Due to these challenges, there is a desire to use commercial technology cryptosystems to provide classified network access. The advantages of using commercial solutions include high performance, lower acquisition and operations costs, and a more rapid cycle of feature and product innovation.

But the strength of the underlying crypto algorithms traditionally has simply not been robust enough to meet strict government communications security requirements. In addition, several older and widely deployed cryptology methods found within commercial solutions are scheduled for government use decertification due to the increased likelihood of exploitation.

Ultimately, what is needed is a solution that features the characteristics of a commercial technology augmented with stronger underlying cryptography algorithms. Aruba Networks, in conjunction with the NSA, through its CSfC program, has developed an alternative network access architecture for classified network connectivity.

This alternative architecture uses Suite B protocols and methods. Suite B is a stronger, faster set of encryption protocols and methods that enable commercial cryptography to be used in classified government networks or even in unclassified networks where a stronger level of security is required.

Suite B is easier to deploy and manage, has better operational performance, and offers multiple access methods, including wired, wireless and remote access. This solution delivers a wide range of additional benefits:

Improved classified network access to authorized personnel

- Enables mobility through high-performance, classified-capable wireless LANs (WLANs).
- Avoids the time and expense of physical-hardened network connections.
- Expands classified network and application usage to a larger user population.
- Lower cost to purchase.
- Lower cost to operate.

Enhanced user adoption and satisfaction

- Improves individual user performance and overall classified network capacity.
- Reduces or eliminate use of CCIs that must be physically secured when not in use.
- Increases the number and flexibility of use cases and classified access mission profiles.

Future-proofing the network architecture

- Elevates the overall communications security posture of new unclassified networks in anticipation of the deprecation of older crypto methods.
- Utilizes classified-capable solutions when building new unclassified networks while anticipating their elevation to classified status at a later date.
- Operates truly unclassified networks at a classified level by using commercial technology.

Classified and other high-value networks must be protected from brute force attacks and other attack vectors. Suite B achieves this by replacing or augmenting asymmetric cryptography algorithms commonly used during key exchanges and symmetric crypto algorithms used for unique user-session data encryption.

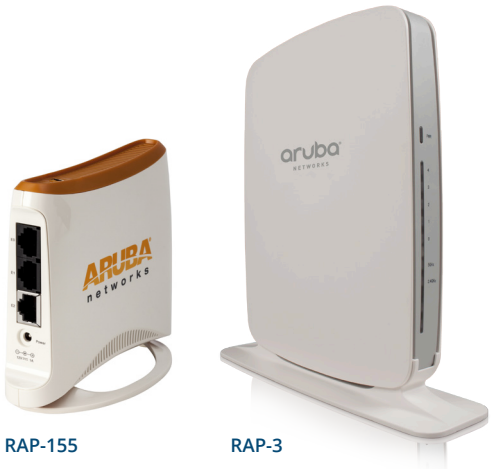
The Suite B algorithms have better overall crypto strength and their underlying computation methods are more efficient, making them more appropriate for high-performance applications. Briefly, the Suite B protocols and methods required are:

- SHA-256/SHA-384 secure hash.
- Elliptical Curve Digital Signature Algorithm certificates/signatures (ECDSA 256/384).
- Elliptical Curve Diffie-Hellman for key exchange (ECDH 256/384).
- AES-128 and AES-256 user-data symmetrical cryptography, with the AES-GCM mode.

Aruba 7000, 6000, 3000 and 600 series Mobility Controllers address classified network access requirements by supporting Suite B.

Aruba Remote Access Points (RAPs) are provisioned to establish a secure IPsec tunnel to the Aruba Mobility controller using Suite-B algorithms. ECDSA Certificate credentials are stored either on a secure USB key or directly on the RAP itself. These ECDSA certificates are used for authentication, while the encrypting of payload data is accomplished using AES-128-GCM or AES-256-GCM. The RAP is capable of allowing a Certificate Signing Request (CSR) to be generated for signing by the appropriate Certificate Authority. While the RAPs have 802.11 a/b/g/n radios that support Wi-Fi capabilities, these radios are typically disabled and the wired ports are utilized.

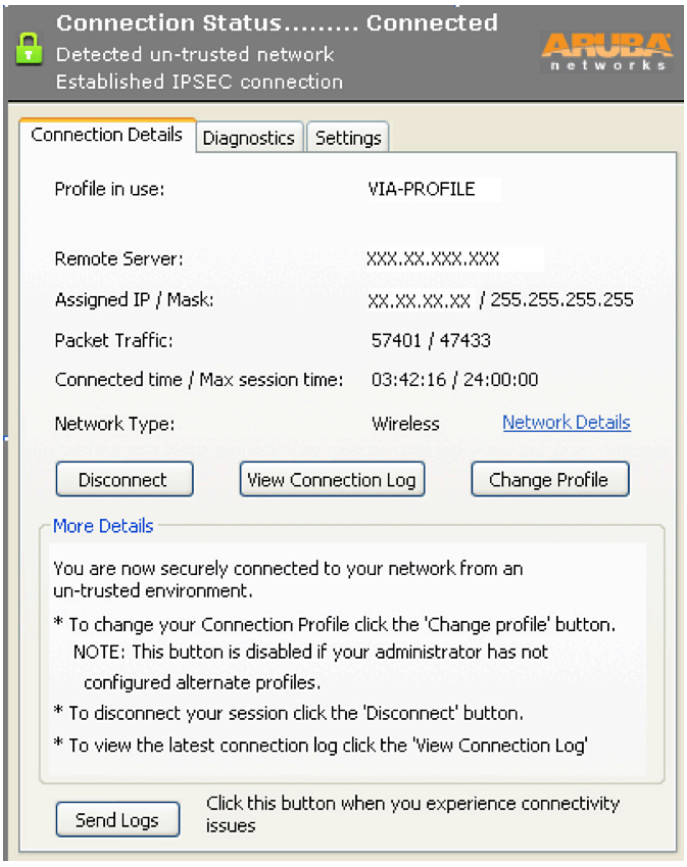
The RAPs provide a "WAN" port for connecting to the network and "LAN" ports for connecting client or "inner" tunnel VPN/routing devices. The RAP-3 provides two LAN ports while the RAP-155 provides 4. If ECDSA certificates are stored directly on the RAP, a 3G or 4G USB modem can be used to provide the "WAN" backhaul transport over a private or public carrier cellular network. The RAP is an approved NSA CSfC component that provides CPU separation between the two Suite-B layers while forming one layer of the "rule of two" IPsec tunnels.



RAP-155 RAP-3

Aruba VIA client on Android and iOS tablets and smartphones.

The Aruba Virtual Intranet Access™ (VIA) IPsec VPN client also supports Suite B. The VIA client is a soft-installable NIC client driver/IP stack shim that detects whether the client device is connected to a trusted or untrusted network, and then uses a combination of authentication and encryption to create a secure tunnel connection to its home Mobility Controller.



Windows version of the Aruba VIA client.

VIA is available for Windows (32-bit and 64-bit), Android, iOS, Mac OS X, and Linux (Ubuntu and Red Hat), and is in-process for FIPS 140-2 and Common Criteria. VIA also appears on the CSfC Approved Product List.

Additional certifications will be achieved through other agencies in order to deploy this solution as part of a classified access network architecture. When combined with other appropriate networking and security technologies, they are intended to provide classified-capable network access to LANs, WLANs and remote networks.

Because this solution is based on commercial crypto technology, it will be available to U.S. government agencies as well as other defense, government and critical infrastructure organizations worldwide. The advantages of this solution include:

- **Enabling technology for new mission profiles:** Suite B will fundamentally transform mobility-oriented communications due to a lack of CCI issues.
- **Support for all access modes:** High-performance Aruba Mobility Controllers manage classified wireless and wired users, thereby simplifying network design and increasing overall security through strict access controls and user firewalling.
- **Multiple services on the same WLAN:** Unclassified and classified access is possible in different or same coverage areas using a single WLAN network architecture. Physical separation of user traffic based on advertised network availability and logical separation of user traffic through Mobility Controller crypto and user-firewall functions prevent comingling of classified and unclassified traffic.

- **Support for local and remote users:** The ability to rapidly deploy secure access locally (using WLAN) and remotely (using remote WLAN) using a single network architecture.
- **High performance:** Aruba 7200 series Mobility Controllers provide up to 40 Gbps of AES-256 encrypted throughput and support thousands of concurrent users.
- **Lower acquisition and operational costs:** Commercial solutions offer lower capital and operating costs compared to government/proprietary solutions.

Aruba classified mobile networks with Suite B cryptography have gained NSA approval within the first overall NSA CSfC approved package. In addition, Aruba classified mobile networks have been tested as part of the NSA CSfC Campus IEEE 802.11 WLAN Capability Package.

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