WHITE PAPER

aruba
a Hewlett Packard Enterprise company

Classified Networking Solutions

Policy-compliant commercial mobility technology with lower costs and higher performance

TABLE OF CONTENTS

GOVERNMENT AGENCIES RECOGNIZE THE BENEFITS OF MOBILITY AND BYOAD

Government agencies are experiencing tremendous pressure from their end users to BYOAD - bringing your own approved devices like smartphones, tablets and laptops that have been validated by government IT departments.

Just as in the corporate world, workers in the public sector have become accustomed to the productivity enhancements that these mobile devices bring to their lives and understand the value they could offer both in the workplace and through Commercial Virtual Remote (CVR) options.

Some end users, in attempts to fulfill their communication requirements, consider using these commercial-grade devices in an unsecured manner to conduct classified voice and data communications – which can put their agencies at risk.

THE DEMAND FOR CLASSIFIED NETWORK ACCESS IS INCREASING

Over the past decade, military, intelligence community and civilian agencies have been transitioning to network-centric applications to support their operations.

The most important applications used by these agencies reside on tactically secret networks, such as the U.S. Department of Defense SIPRNET. As a result, classified networks have experienced a dramatic increase in importance and usage.

At the same time, these networks tend to be underutilized because of:

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

> With the rollout of CVR and the success of CVR users and the fact that users are working differently with CVR, it is driving us more quickly to BYOAD

Steve Wallace, systems innovation specialist for DISA's Emerging Technologies Directorate

Source: January 2021 AFCEA DC virtual event

CONVERGENCE OF COMMERCIAL MOBILITY AND CLASSIFIED ACCESS

The need to increase classified access, support personal mobility and reduce costs for taxpayers has prompted government agencies to find ways to utilize commercial technology in their networks. Commercial technology delivers important advantages, including:

> To appreciate the scope and scale of our task, our work is to enable productive collaboration for over four million military and civilian worldwide teleworkers with innovative tools that are both cutting-edge and secure, often with overnight demands.

Source: April 2020 Briefing, U.S. DOD

- Higher performance.
- Lower purchase and operations costs.
- Increased productivity and rapid innovation.

To meet the converged needs of classified access and mobility, the U.S. National Security Agency (NSA) instituted the Commercial Solutions for Classified (CSfC) program, which defines a series of end-to-end architectures to provide commercial off-the-shelf (COTS) mobile devices with secure connectivity to classified networks and applications over untrusted networks like the Internet. The primary underlying information assurance technology defined in this program involves CNSA cryptographic algorithms.

CNSA Suite cryptography modernizes the communications infrastructure for highly sensitive environments while improving the strength and performance of cryptographic algorithms for key exchange, digital signatures and hashing.

In order to protect classified or other high-value networks from brute-force and other attack vectors, it replaces or augments both the asymmetric cryptography algorithms used during key exchanges and symmetric cryptography algorithms used for unique user-session data encryption.

The CNSA algorithms have better overall cryptographic strength and utilize more efficient underlying computation methods, making them more appropriate for high-performance applications.

The required CNSA protocols and methods are:

- SHA2-384 secure hash algorithms.
- Elliptical Curve Digital Signature Algorithm certificates/signatures (ECDSA p384).
- Elliptical Curve Diffie-Hellman for key exchange (ECDH p384).
- AES-256 user-data symmetrical cryptography, with the AES-GCM mode.

THE LEADING COMMERCIAL SOLUTION FOR CLASSIFIED WIRED, WIRELESS AND REMOTE ACCESS

Aruba, a Hewlett Packard Enterprise company, now offers government agencies a significantly improved approach.

Using Aruba's Edge Services Platform (Aruba ESP), agencies can utilize a mobile-first, BYOAD-compliant network security architecture to automate infrastructure-wide performance optimization and trigger security actions that used to require manual IT intervention.

Aruba ESP provides the mechanisms to control the dynamic mobility environment by correlating real-time data about users, devices, apps and location. Self-healing and self-optimization functions dramatically reduce helpdesk tickets and protect enterprise data.

Aruba employs a software approach that extends mobility intelligence across wired and wireless networks all the way to users, devices and apps. This makes Aruba ESP architecture amazingly easy to deploy without any changes to the existing infrastructure.

Working with various government agencies responsible for network security technology and policy compliance, Aruba has developed a vastly improved access architecture for networks that handle sensitive but unclassified, confidential and classified information.

This new architecture uses NSA-approved CNSA Suite cryptographic capabilities to deliver a variety of strategic benefits to every government agency, including:

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

FEDRAMP AND OTHER KEY BENEFITS

In addition to the cost savings afforded by commercial technology, Aruba solution includes Aruba Central, which has received a formal "In Process" designation with FedRAMP. As Aruba's cloud-native network management and analytics platform, Aruba Central is the first AI-powered solution for unified WLAN, switching, VPN, and WAN cloud infrastructure to undergo FedRAMP Authorization. For more information, refer to our Federal blog website: https://blogs.arubanetworks.com/series/Aruba-Federal/

> "Smartphones and PDAs are gaining traction among a range of federal audiences as agencies and departments seek to enable greater mobility..."
>
> Source: Washington Technology

A variety of additional strategic benefits include:

- Improved classified network access for authorized personnel. A high-performance WLAN that supports mobility and operates without physical hardwired network connections enables secure access for a larger user population at much lower expense.
- Lower costs of deployment and operations. The Aruba solution is as little as 10% of the purchase cost of a Type 1-certified solution and also costs less to operate.
- FedRAMP Authorization of Aruba Central in process: As the first
- Higher user adoption and satisfaction. The Aruba solution offers faster performance and increased battery life for mobile devices. It also removes the challenge of operating Controlled Cryptographic Items (CCIs) and securing them when not in use. With expanded mobile access, users have more flexibility to contribute to their agency missions. The advantages include:
  - Using commercial mobile devices in classified environments.
  - Using the same mobile devices while connected to 3G/4G carrier networks for classified activities.
  - Enabling cross-agency and cross-government collaboration by connecting interoperable networks for first responders or coalition governments.
  - Secure access to multiple services, both unclassified and classified, over the same WLAN infrastructure.
- A network architecture that's ready for the future. Aruba's CNSA Suite implementation makes it possible to utilize classified-capable solutions when building new unclassified networks, in anticipation of elevating them to classified status at a later date.

In addition, it improves security on new unclassified networks in anticipation of the deprecation of older cryptographic methods. Finally, it allows unclassified networks to operate at a classified level without deploying government-proprietary technology.

- An affordable way to provide secure wired, wireless and remote access to authorized users. Using a single group of Aruba solution elements, users can be offered any combination of mobile and fixed network access in a variety of policy-compliant deployment scenarios. Access to applications in each scenario is provided in exactly the same manner without requiring different client configurations, ensuring end user satisfaction and ease of use.

AFFORDABLE CLASSIFIED MOBILITY USING CNSA SUITE

The advanced cryptography capabilities available in ArubaOS brings CNSA Suite cryptography to government agencies of all sizes.

Aruba's advanced cryptography capabilities are available on all 9000, 7200, and 7000 Series Gateways and Controllers, and include the following capabilities:

- SHA2-256 and SHA2-384 secure hash algorithms.
- ECDSA certificates/signatures during user/device authentication.
- ECDH for key exchange.
- AES-128-GCM and AES-256-GCM for symmetric cryptography.
- AES-128-CBC, AES-128-CCMP legacy modes.
- WLAN mode: bSec (802.11i enhanced with CNSA Suite) using EAP-TLS 1.2
- VPN mode: IPSec + CNSA Suite using IKEv2
- Seamless PKI integration with OCSP and CRL support, and with TPM hardware in Aruba Mobility Controllers and Access Points (APs).

Additionally, the Aruba Virtual Intranet Access™ (VIA™) software agent, available for a variety of mobile and laptop devices, provides an end-to-end secure CNSA Suite tunnel from the device to the Mobility Controller. The VIA client is an installable NIC/IP stack client driver shim that detects whether the client device is connected to a trusted or untrusted network and can connect automatically.

Figure 1: Aruba Virtual Intranet Access (VIA) software agent connection status screen.

It then uses a combination of authentication and encryption to create a secure CNSA Suite-enhanced connection to its Gateway or Mobility Controller. It can operate as a WLAN client supplicant, Ethernet LAN IPSec mode, or remote access IPSec mode.

Aruba Gateways and Mobility Controllers, APs, ArubaOS and VIA continue to be validated through the U.S. National Institute of Standards and Technology (NIST), U.S. National Information Assurance Partnership (NIAP) Common Criteria, NSA and other agencies for deployment as part of a classified access network architecture.

Figure 2: The Aruba Gateway and Mobility Controller

When combined with other appropriate networking and security technologies, Aruba solutions provide a policy-compliant, classified-capable access network connection for LAN, WLAN and remote access requirements.

Using Aruba's innovative MultiZone feature, logical separation of user traffic through the AP and to the physically separated Gateways and Mobility Controllers ensure that classified and unclassified traffic are not co-mingled.

Because this solution is based on commercial cryptographic technology, it is available to U.S. government agencies as well as defense, government and also to enterprise organizations worldwide.

CONSISTENT ACCESS VIA NETWORK ON-RAMPS

As part of the common network services at the core of Aruba Mobility-Defined Networks, CNSA Suite support is available to networks accessible through a variety of on-ramps:

- Wireless APs. Aruba APs provide high-performance connectivity to mobile and fixed wireless devices, while providing best-in-class RF control using Adaptive Radio Management (ARM) and patented ClientMatch™ technologies.
- Aruba CX switching portfolio. Aruba has extended the user-centric, services-based approach of the MOVE architecture to a new class of access, aggregation, and core switches. Designed to provide network access in wiring closets and aggregation at the distribution and core, the Aruba CX family of switches connect wired Ethernet devices such as virtual desktops, video surveillance cameras and wireless APs.
- Remote APs. An alternative operating mode for Aruba APs, Aruba Remote APs (RAPs™) automatically extend centralized resources to branch and remote locations using site-to-site VPN tunnels to the central data center. Using zero-touch configuration, personnel at these sites can easily set up their own RAPs with no IT assistance.
- Outdoor APs. Aruba outdoor APs combine a unique multi-radio, multi-frequency architecture, Adaptive Radio Management and hardened enclosures to bring high-performance networking to outdoor or deployable environments. Using the ArubaOS mesh features, they can connect to the backbone network wirelessly as an alternative to a wired AP connection.

THE BENEFITS OF SIMPLIFIED MANAGEMENT

With Aruba ESP architecture, services are defined once via a centralized Aruba Gateway or Mobility Controller in the data center. This eliminates the need to keep up with a profusion of wiring closets, firewalls, network access control (NAC) solutions, management systems and reporting tools that operate in separate domains.

As a result, network operations are consistent across the entire organization, regardless of user location, access method, mobile device or applications. This is critical especially during challenging times like the pandemic. Aruba easily accommodates users with multiple devices, including both legacy devices and commercial mobile technology, including smartphones, tablets and laptops.

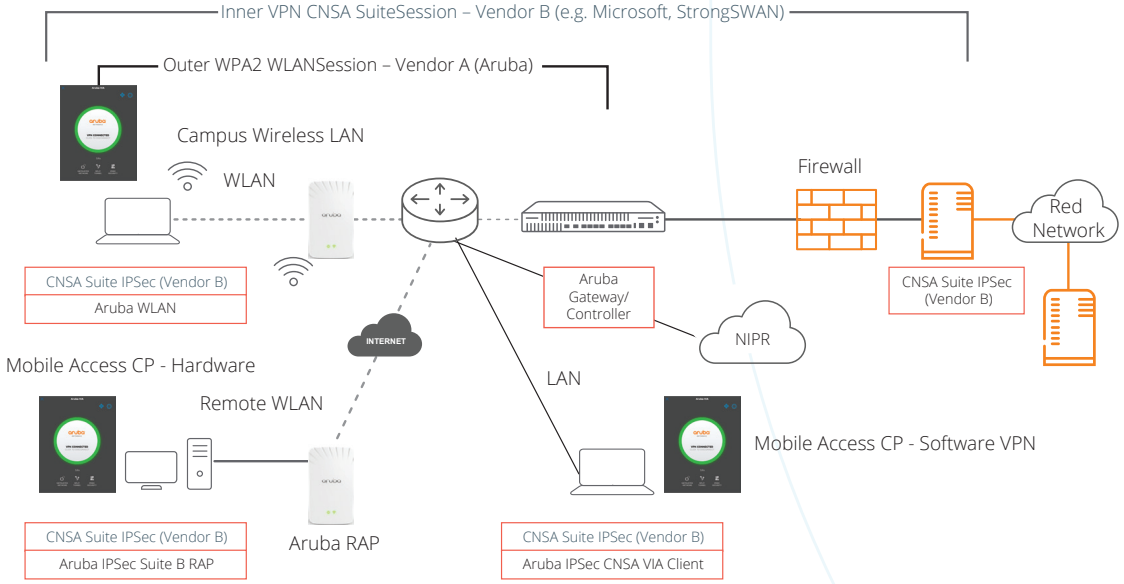

Figure 3: Example of the Department of Defense SIPRNET access architecture using Aruba Suite B encryption.

With its user-centric approach, Aruba ESP architecture also eliminates the need to maintain VLANs at the edge and manually configure user additions and changes.

> Organizations will have to figure out what's important to them: what has to be accomplished inside a physical facility and what can be done remotely

Source: Essye Miller, principal deputy in the office of the DoD chief information officer

THE BUSINESS CASE FOR ARUBA

With tight budgets and mobility at a critical juncture, Aruba ESP present a very compelling business case for government, civilian and military agencies:

- Significantly lower purchase costs compared to proprietary solutions. The Aruba medium-assurance solution is as little as 10% of the purchase cost of a high-assurance Type 1-certified solution. Additional operational savings come from:
  - Eliminating cumbersome CCI checkout and handling processes.
  - Accelerating the move from wired to multi-gigabit Wi-Fi, thereby reducing the number of Ethernet switches needed in favor of more cost-effective Wi-Fi access.
  - Moving to thin on-ramps at the edge that are easier to install and operate.
- Additional savings by operating multiple services on the same WLAN. Aruba supports unclassified and classified access using a single AP infrastructure, while maintaining physical and cryptographic boundaries.
- Easier support for both local and remote users. Because it utilizes a single architecture and network design for local (using WLAN, WLAN mesh and wired) and remote (using remote wired and WLAN) access, it is simpler to manage.

Instead of employing a complex, legacy approach to network management and operations, IT administrators can deploy a simpler, mobile-first solution with Aruba:

- **Improved security by supporting all access modes.** Aruba Mobility Controllers manage classified WLAN users and classified wired users to simplify network design and strengthen the overall security posture by adding access control and user firewalling.
- **A higher performance network.** Aruba Gateways and Mobility Controllers support up to 40 Gbps of AES-256 encrypted throughput for tens of thousands of concurrent users.
- **Lower end-user support costs and higher satisfaction.** Aruba gives the entire workforce – employees with and without clearance as well as contractors and guests – a single, consistent way to access the appropriate agency resources.

Role-based access policies allow IT to control users and devices, so that personnel can switch effortlessly between desktops, laptops, tablets, smartphones and other mobile devices. By cutting down on the confusion and saving time for users, Aruba reduces IT service desk calls and increases user satisfaction.

Finally, employees accessing classified information via mobile devices gain significant benefits in terms of usability, application performance and battery life.

CONCLUSION

Aruba ESP architecture give government IT organizations the technology they need to realize their vision to embrace mobility and cloud services in a meaningful way. It does so by securely unifying disparate computing infrastructures into one seamless network access solution – for government employees, contractors, visitors, and military personnel in garrison or in deployment.

For the first time, government agencies that handle sensitive but unclassified, confidential and classified information can benefit from the lower purchase costs, lower operational costs and faster pace of innovation available through COTS solutions.

With Aruba ESP architecture, access privileges are linked to a user's identity. That means government personnel have consistent, secure access to classified and non-classified network resources based on who they are – no matter where they are, what devices they're using or how they're connected.

ABOUT ARUBA, A HEWLETT PACKARD ENTERPRISE COMPANY

Aruba, a Hewlett Packard Enterprise company, is the global leader in secure, intelligent edge-to-cloud networking solutions that use AI to automate the network, while harnessing data to drive powerful business outcomes. With Aruba ESP (Edge Services Platform) and as-a-service options, Aruba takes a cloud-native approach to helping customers meet their connectivity, security, and financial requirements across campus, branch, data center, and remote worker environments, covering all aspects of wired, wireless LAN, and wide area networking (WAN).

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 the Airheads Community at community.arubanetworks.com.

WP_CNSASuite_ClassifiedNetworkingSolutions_SK_032321 a00112198enw