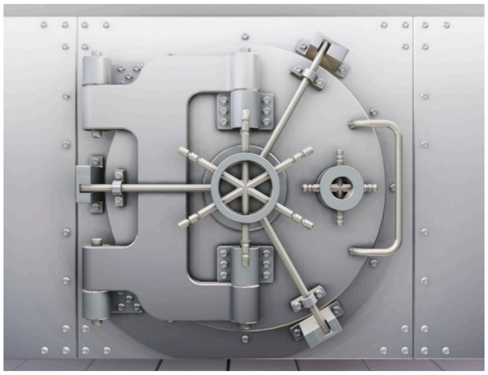
Commercial Solution for Classified (CSfC) Programs

Secure Network Architecture for Classified Networks

Over the past decade, military, intelligence and civilian agencies have transitioned to "network-centric" applications to support their operations. The most important applications used by these agencies reside on tactically secret networks (for example, the U.S. Department of Defense SIPRNET); thus these classified networks have experienced a dramatic increase in importance and usage. Unfortunately, these enterprises don't provide classified network access to all possible authorized users and there are limitations on where this technology can be used – severely hampering personal mobility. The under-utilization of classified resources is typically blamed on the expense of installing certified classified network connections; the usability challenges of government-specific proprietary crypto systems (e.g., the US TYPE-1 system); and reports of low performance when using these cryptosystems for network access.



More recently, agencies have experienced significant pressure from their end-users to support classic personal mobility products for both classified and non-classified uses. Consumer-oriented mobility products including RIM Blackberry, Apple iPhones and iPads, along with just netbooks and laptops, have been fielded by the end-users themselves. These end users want local WLAN support when on-premise for local mobility and want 3G support for global mobility. Some Government end-users, in desperate moves to fulfill their communications requirements, are utilizing these commercial grade devices in an insecure manner to conduct classified voice and data communications – thereby putting their agencies at risk.

Due to these new requirements and subsequent challenges, there is a desire from agencies to use commercial solutions to provide classified network access, via the traditional advantages associated with using commercial solutions: 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 that are typically fielded today are simply not good enough to meet the more strict government communications security requirements. In addition, several of the older and widely deployed underlying cryptology methods found within commercial solutions are scheduled for government de-certification due to the increased likelihood of exploitation.

Aruba Networks Introduction of CSfC for Classified Wired, Wireless and Remote Access

Aruba Networks, in conjunction with various government agencies responsible for government network security technology and policy, has developed an alternative access network architecture for classified network connectivity. This alternative architecture uses the collection of protocols and methods referred to as CSfC and is intended to be easier to deploy and manage, have better operational performance, and offer multiple access methods including wired, wireless and remote access.

Advantages

- Support for All Access Modes: High performance management for both classified wireless and wired networks
- Multiple Services on the Same WLAN: Crypto and user-firewall functions ensure classified and unclassified traffic is not co-mingled
- Support for Both Local and Remote Users: Rapid deployment of secure access both local and remote, using single architecture and network design
- High Performance: Supports 4Gb/s of AES-256 encrypted throughput, supporting thousands of users simultaneously

Integrio Technologies, an SBA-designated small business headquartered in Herndon, Va., is an IT integration and engineering company that offers reliable, cost-effective, secure solutions for organizations seeking to develop new capabilities and optimize legacy systems. Our company collaborates with its customers, partners and employees to provide outstanding cutting-edge solutions for network performance, secure wireless infrastructure, software application lifecycle support, and physical cyber security that support the missions of federal, state and local government agencies.

2355 Dulles Corner Blvd.
Suite 600
Herndon, VA 20171

703 961 1125
1 800 929 3871

salesinfo@Integrio.com

Integrio.com

Key Benefits

Improved classified network access to authorized personnel:

- Enables mobility through a high performance, classified-capable WLAN
- Avoids the time and expense of physical hardened network connections
- Expands classified network and application usage to larger user populations
- Lowers Cost to Purchase – as little as 10% of the cost of a traditional TYPE-1 solution
- Lowers Cost to Operate – reduces or eliminates manual re-keying

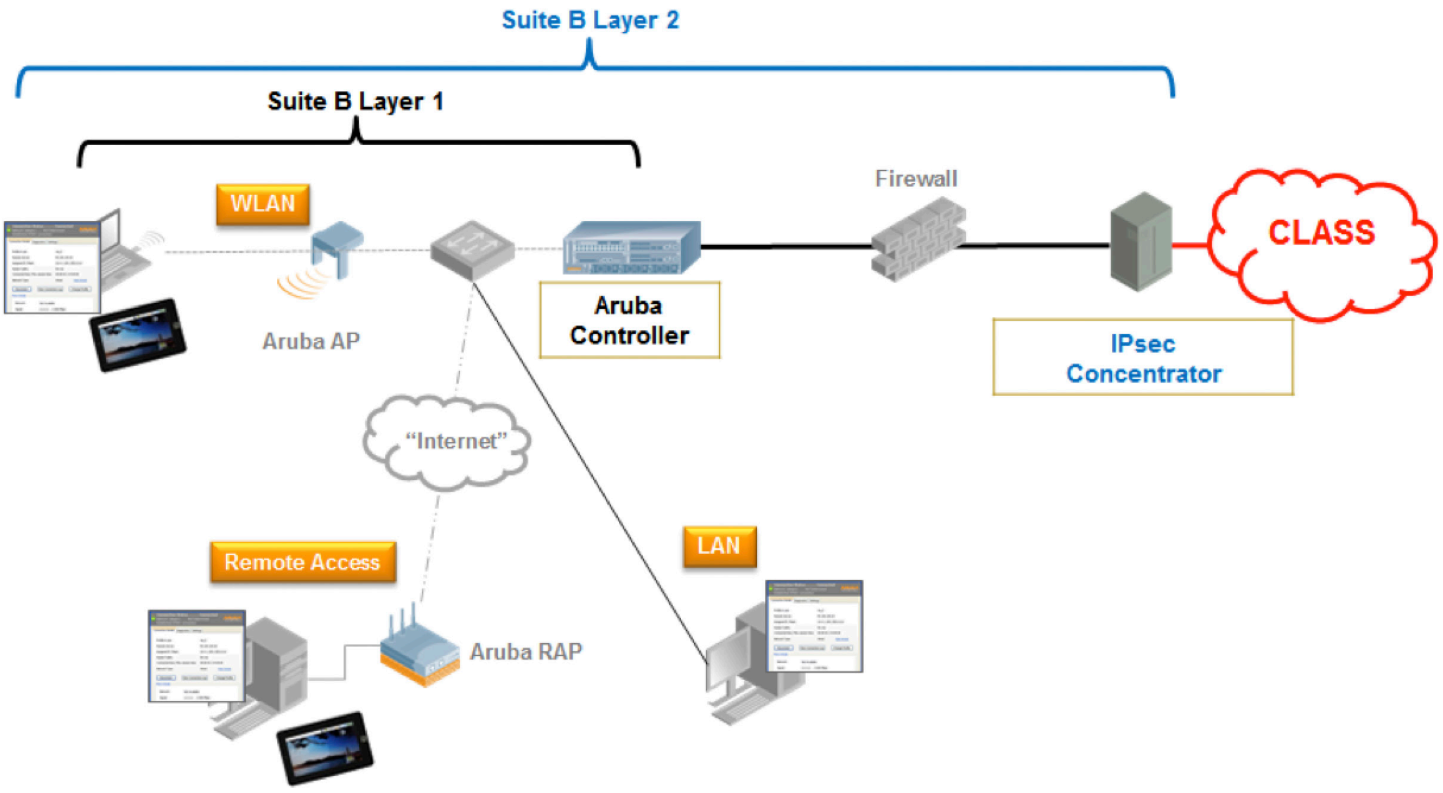
Enhanced user adoption and satisfaction:

- Improves individual user performance and overall classified network capacity
- Reduces reliance on Controlled Cryptographic Items that must be secured when not in use
- Increases the number of and the flexibility of use cases, and classified access mission profiles

Future-proof the network architecture:

- Elevates the overall communications security posture of new unclassified networks in anticipation of the deprecation of older crypto methods
- Similarly, utilizes classified-capable solutions when building new unclassified networks, in anticipation of elevating them to classified status at a later date
- Realizes additional peace of mind by operating truly unclassified networks at a classified level via commercial technology

In order to protect these classified, or other high-value networks, from brute force attacks and other attack vectors, CSfC replaces or augments both the asymmetric cryptography algorithms (used, for example, during key exchanges) and symmetric crypto algorithms (used for unique user-session data encryption). The CSfC algorithms not only have a better overall crypto strength, but the underlying computation methods are more efficient, making them more appropriate for high-performance applications.


Suite B Layer 2
Suite B Layer 1
WLAN
Aruba AP
Aruba Controller
Firewall
IPsec Concentrator
CLASS
"Internet"
Remote Access
Aruba RAP
LAN