Secure Wireless Architecture Type-1: Reduce Costs with a Common Infrastructure for Classified and Unclassified Traffic

Abstract

Until now, defense, intelligence, and civilian agencies that wanted to transmit classified voice, video, and data over wireless networks had to deploy a purpose-built National Security Agency (NSA)-certified Type-1 wireless solution. But purchasing and operating separate wireless networks for classified and unclassified clients increases equipment and operational costs. It also prevents the Type-1 wireless clients from taking advantage of the built-in capabilities of enterprise-class wireless infrastructure, such as intrusion detection, location tracking, and network management. Now agencies can support a multilevel security architecture for classified, unclassified, and guest clients on a converged wireless LAN infrastructure that meets all federal and NSA security requirements. This white paper explains the Secure Wireless Architecture Type-1 solution from Cisco and Harris, which combines the Cisco® Unified Wireless Architecture, Harris SecNet 54 inline network encryptor (INE), and professional services from Harris IT Services.

The Role of Secure Wireless Networks in Agency Missions

Wireless networks can increase productivity, facilitate collaboration, and reduce physical infrastructure costs, helping agencies achieve their mission objectives. Agency employees and contractors are more productive when they can securely access data and mission-related applications from any workspace, including a Secure Compartmented Information Facility (SCIF) and tactical environments. And infrastructure costs decrease when temporary communities of interest or rapidly deployable tactical units can access voice, video, and data over a secure wireless connection, sparing their agencies the expense of installing Protected Distribution System (PDS) conduit for classified data communications.

Security Requirements

A wireless mission fabric designed for a multilevel security environment must comply with federal requirements that apply to both the infrastructure and clients:

- National Institute of Standards Federal Information Processing Standards (FIPS) 140-2
- National Information Assurance Partnership (NIAP) Common Criteria validation against a government-approved protection profile
- Department of Defense (DoD) Directive 8100.2, 8500.01E, DoD Instruction 8500.02, and certification and accreditation in accordance with DoD Instruction 5200.40
- NSA Type-1 certification for client devices sending up to top-secret traffic

Previous secure wireless solutions were useful for specific applications but could not take advantage of enterprise services available from the agency’s existing, enterprise-class wireless infrastructure, such as intrusion detection, location tracking, and spectrum intelligence. In addition, previous Type-1 solutions had to be deployed as a parallel infrastructure, separate from the agency’s wired and wireless enterprise infrastructure, which increased operational expense.
Solution from Cisco and Harris

The Secure Wireless Architecture Type-1 solution from Cisco and Harris is the first solution to enable federal government agencies to use a common wireless infrastructure for all enclaves—from unclassified to top secret—in a multilevel security architecture that meets all federal and NSA security requirements. The solution also simplifies deployment and support because all technology and services are available from a single source, Harris IT Services. The joint solution from Cisco and Harris provides the following capabilities:

- 802.11 standards compliance
- Data confidentiality:
  - WLAN infrastructure: FIPS 140-2 Wi-Fi Protected Access Version 2 (WPAv2)-Enterprise and Pre-Shared Key (PSK)
  - SecNet 54: High-Assurance Internet Protocol Encryptor (HAIPE) Type 1 for Layer 3 security and WPAv2 for Layer 2 security
- Location tracking of all wireless devices, including SecNet 54 clients, within the wireless LAN
- Spectrum Intelligence Integration with Cognio Spectrum Expert for visibility into the entire 2.4- and 5-GHz spectrum
- Wireless intrusion detection:
  - Rogue access points and clients
  - Location-based alarms
- Integration with Cisco Wired Intrusion Prevention System (IPS)
- Fast, secure roaming
- Wireless QoS (802.11e) prioritization of HAIPE traffic on the wireless LAN
- End-to-end enterprise-class wireless network management
- Transparent extension of enclave data center applications

Cisco Unified Wireless Architecture

The Secure Wireless Architecture Type-1 solution comprises the Cisco Unified Wireless Architecture, Harris SecNet 54 device, and professional services from Harris IT Services. The Cisco Unified Wireless Architecture in conjunction with the Harris SecNet 54 cryptographic client extends the security perimeter of the agency’s existing wireless network up to top secret. As a result, agencies can use a single, virtualized wireless infrastructure to provide services for all levels of classification, including guest traffic, FIPS-validated unclassified client traffic, and classified traffic up to top secret. Having a single virtualized infrastructure eliminates the capital and operational costs of building and supporting parallel infrastructures for classified and unclassified traffic.

Cisco solution components include FIPS-validated wireless LAN controllers, FIPS-validated wireless access points, the Cisco Secure Access Control Server for Authentication, Authorization, and Accounting (AAA) services, the Cisco Enterprise Wireless Control Software and Location Appliance, and the Cisco Secure Services Client for unclassified devices.
Harris SecNet 54 Cryptographic Device
SecNet 54 is a highly portable, modular, standards-based Type-1 inline network encryptor (INE) that provides the highest levels of data protection for mobile unified communications (Figure 2). The only NSA-certified, wireless, Type-1 secure INE, SecNet 54 delivers speeds up to 54 Mbps for 802.11a/b/g and complies with NSA HAIPE standards. Its modular design supports multiple transmission media in use in federal government: 802.11, wired Ethernet, and emerging wireless media.
Harris IT Services

Harris IT Services provides all services needed to design, deploy, and support the Secure Wireless Architecture Type-1:

- **Site survey:** At the beginning of the engagement, Harris IT Services performs a spectrum analysis at the 2.4- and 5-GHz range to verify that the noise floor is acceptable to implement a successful WLAN. The spectrum analysis allows Harris IT Services to detect, classify, locate, and mitigate sources of wireless interference. Typical sources include Bluetooth, cordless phones, microwave ovens, and video recorders. Next, Harris IT Services performs a passive survey to detect existing authorized or unauthorized wireless LANs and identify channels in use that might cause interference. In the final phase of the site survey, Harris IT Services verifies the design by staging wireless access points to measure network performance and radio frequency coverage.

- **Design:** Harris IT Services engineers who have a wireless certification from Cisco develop a wireless design that meets the agency’s classified security needs and follows commercial best practices. Design criteria include integration into the existing network infrastructure, high performance, high availability, and a single point of control for the wired and wireless environments. The latter is achieved using the Cisco Wireless Control System.

- **Installation:** Harris IT Services employs several hundred cleared network engineers who are trained to install the Cisco Unified Wireless Architecture and SecNet 54 INEs.

- **Support and maintenance:** Harris IT Services engineers can be deployed throughout the continental United States, enabling them to respond quickly to outage situations or requests for additional services.

- **Onsite training:** Harris IT Services trains agency employees, IT staff, and Information Assurance (IA) staff on using and supporting SecNet 54 devices.

**Solution Benefits for Federal Agencies**

**Lower Total Cost of Ownership**
The Secure Wireless Architecture Type-1 solution from Cisco and Harris eliminates the equipment and operational costs of supporting separate wireless networks for classified and unclassified traffic. Instead, a single Type-1 infrastructure supports all enclaves.

**Support for Temporary Communities of Interest**
Used in temporary environments in place of a wired network, the Secure Wireless Architecture Type-1 from Cisco and Harris eliminates the high costs of laying PDS conduit. This is especially useful during Base Reduction, Realignment, and Closure (BRAC) projects and disaster relief efforts because personnel can immediately begin accessing voice, video, and data over a Type-1 wireless network.

**Compliance with Federal and NSA Security Requirements**
The Cisco and Harris solution is the first to meet strict federal and NSA security requirements.

**Flexible Usage, for Higher ROI**
The solution can be used in campus or military base network infrastructures as well as in rapidly deployable communications kits provided for temporary command posts. (The SecNet 54 device weighs less than one pound.) An agency that purchases the solution for one purpose can later use it for another, as mission needs change. The solution provides investment protection because Cisco and Harris are committed to supporting new standards.
Why Cisco and Harris
Cisco and Harris lead the industry in networking and encryption, respectively, and have combined their expertise to provide an all-in-one solution for Type-1 wireless networks based on commercial, off-the-shelf (COTS) technology.

Cisco Communications Expertise
As the leading provider of IP networking for government, Cisco is committed to helping agencies use their wired and wireless IP networks to increase mission effectiveness despite limited resources and increasing threats worldwide. Cisco networking solutions deliver information, applications, and services across geographic and organizational boundaries, helping to achieve the goal of connected government. Agency officials can take advantage of Cisco wired and wireless networks to collaborate from any location, using any device.

Harris Lifecycle Services Expertise
Harris IT Services is a leading provider of mission-critical IT and communications services and support to defense, intelligence, homeland security, and civil customers. With 3000 global professionals, Harris IT Services supports large-scale IT programs that span the full technology lifecycle. The company is chartered to provide high-quality, cost-effective operation, maintenance, engineering, and technical support services to the U.S. government. Harris IT Services has a superior record with performance-based contracts, value-oriented services and solutions, and a multi-skilled, trained, and certified workforce with security clearances. Harris IT Services is a Cisco Gold Partner and has earned the Advanced Wireless Certification.

Financing
Through a wholly owned subsidiary, Harris IT Services holds the FirstSource and United States Air Force Network-Centric Solutions (NETCENTS) contracts. Department of Homeland Security agencies can take advantage of FirstSource to purchase the hardware, software, and professional services included in the Secure Wireless Architecture Type-1 solution from Cisco and Harris. The solution also qualifies for NETCENTS.

Conclusion
Defense, intelligence, and civilian agencies can increase productivity and enhance collaboration by providing wireless access to mission-related applications and data. The Secure Wireless Architecture Type-1 solution from Cisco and Harris meets all federal and NSA security requirements for agencies to transmit classified, unclassified, and guest traffic on the same infrastructure, reducing costs. Harris IT Services acts as a single point of contact for all technology and services related to the Secure Wireless Architecture Type-1 solution, simplifying and accelerating deployment and support.

For more information or a personal meeting, e-mail: Ask_The_COE@external.cisco.com.
