White Paper

Cisco and EADS-North America Secure Communications Cross-Domain Solution

Executive Summary

The Department of Defense (DoD), North Atlantic Treaty Organization (NATO), the Intelligence Communities (IC), as well as the international Ministry of Defense (MoD) have long had the requirement to conduct secure voice communications across multiple security domains. The secure communications solution developed by Cisco Systems and EADS-North America (EADS-NA) provides a scalable, IP-based, cross-domain solution that can meet both enterprise and tactical operational voice requirements in a form factor that was built with size, weight, and power (SWaP) constraints in mind.

Challenge

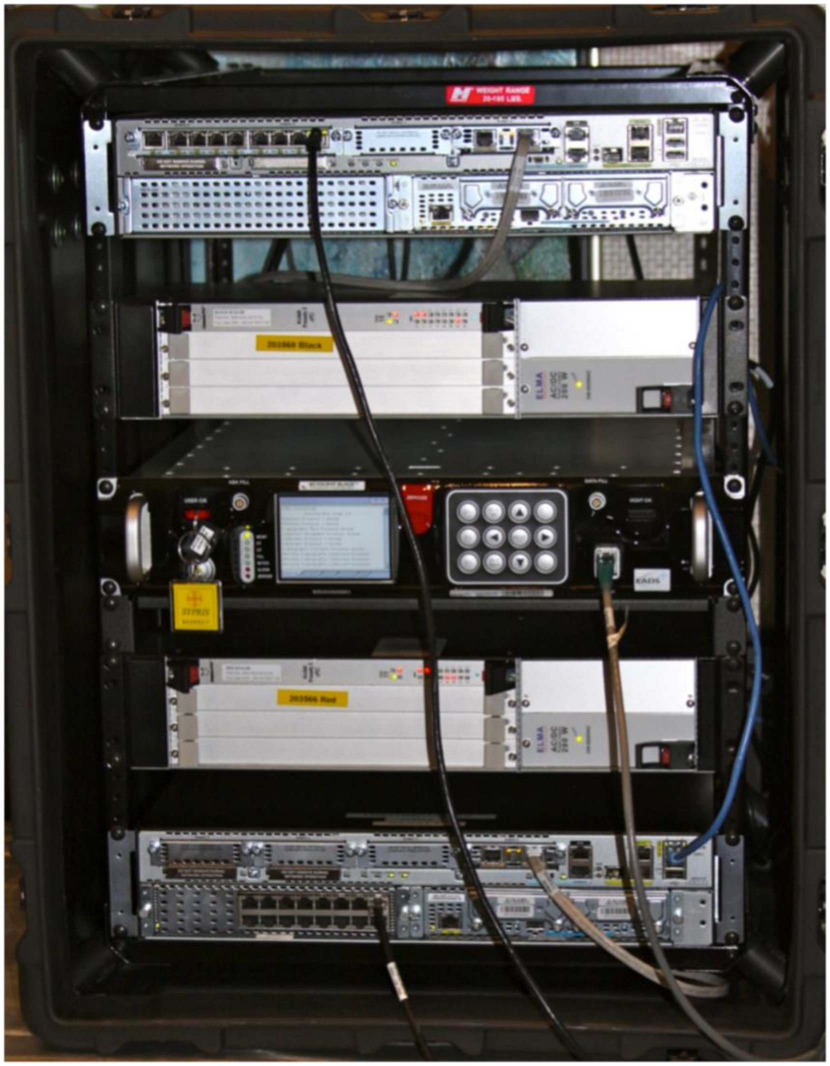
Over the last 10 years, the adoption of Internet Protocol Telephony (IPT) across the U.S. DoD, NATO, and IC, as well as in the international MoD communities has led to the requirement for a secure cross-domain IP voice capability. In addition, in providing a critical operational capability, this approach also facilitates the transition from expensive circuit-based technology to the more cost-effective IP-based solutions.

Until recently, the challenge had been the lack of certified systems that could replace the large Time-Division Multiplexing (TDM) Channel Encryption Units (CEUs) that were both costly and cumbersome to maintain. With the further enhancement and broad adoption of the Secure Communications Interoperability Protocol (SCIP), formerly known as Future Narrow Band Digital Terminal (FNBDT), industry has been able to move beyond the development of TDM-based devices that were initially fielded under the FNBDT program, to the development of new IP-based solutions.

Solution

The EADS-NA certified SCIP cryptographic solution (ECTOCRYP® Black), when combined with the Cisco® virtualized call-control solution (Cisco Unified Communications Manager) on a router, provides a secure cross-domain voice communications solution that is scalable from the tactical to enterprise environments. Figure 1 depicts the SWaP architectural solution for tactical implementations that was successfully demonstrated at both the Defense Information Systems Agency (DISA)-sponsored Coalition Warrior Interoperability Demonstration (CWID) event at U.S. Joint Forces Command in June 2011 and the National Security Agency (NSA)-sponsored 19th International-Interoperability Control Working Group (I-ICWG) SCIP event at Annapolis, Maryland, in October 2011.

Figure 1. Architecture 1: Tactical Classified Voice-Video over IP (CVVoIP) Service

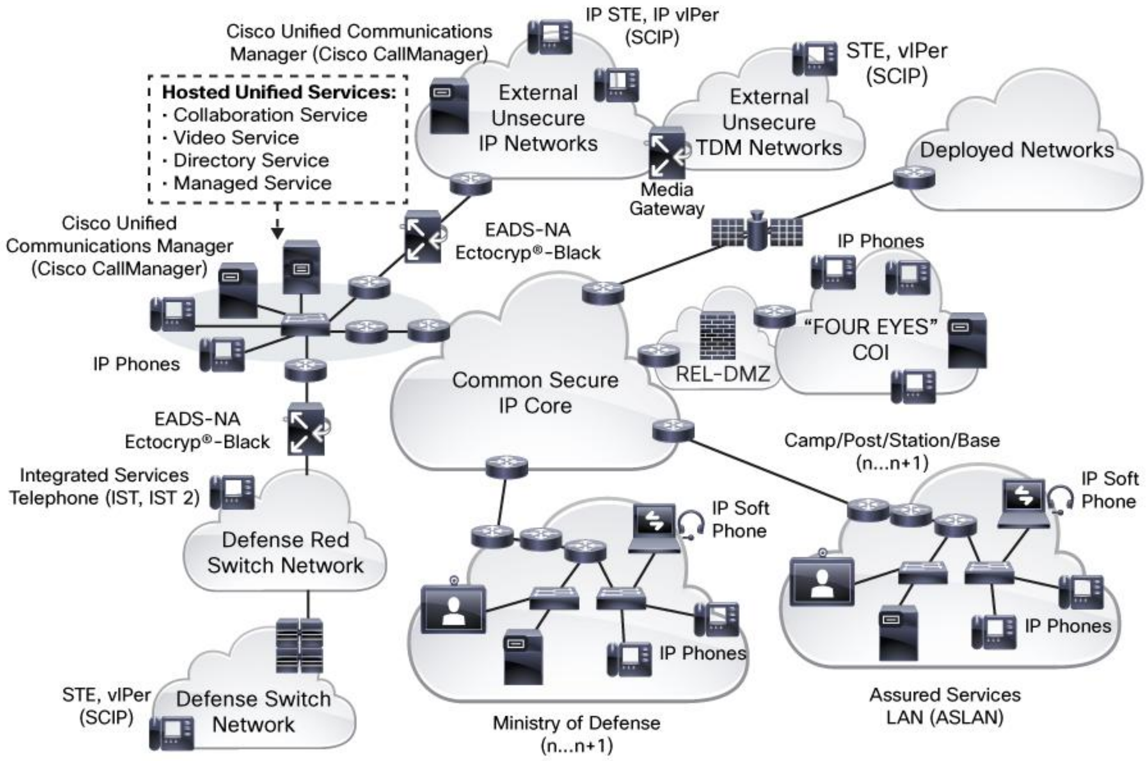


By simplifying the architecture and packaging this tactical configuration in this fashion, the solution can scale to deliver non-blocking voice services across two security domains. Successful bidirectional calls were completed between Cisco IP-based endpoints on the secure domain (Red) and General Dynamics' IP-based vIPer secure terminals on the unsecure domain (Black). The figure illustrates the EADS-NA ECTOCRYP® Black (in the middle) packaged between controller blades and Cisco 2951 Integrated Services Router (ISR) platforms with the unsecure (Black) domain on top and the secure (Red) domain on the bottom. Both platforms were configured with Power over Ethernet (PoE) switches for LAN voice, video, and data services while also housing virtualized call-control images (Cisco Unified Communications Manager) mounted within a Cisco Services-Ready Engine (SRE) - 910 module. With voice services delivered in this small form factor, the complete tactical package using Cisco Unified Communications Manager Version 8.6(1) supporting the SCIP-216 standard, and the ECTOCRYP® Black supporting the SCIP-210, 215, and 216 certified standards is able to conduct secure voice communications efficiently, economically, and effectively between two established and separate security domains.

In a larger enterprise architecture, the Cisco Unified Communications Manager and EADS-NA ECTOCRYP® Black solution can grow to support upward of 30,000 users in a distributed, redundant, yet survivable, non-blocking unified services architecture. If required, this scalable architecture growth can be accomplished in a single call-control construct.

Whether it is the ability to provision small office, branch office, tactical, or enterprise unified services the tested Joint Interoperability Test Center (JITC) solution by Cisco and EADS-NA can scale to meet those needs. As Figure 2 illustrates, the notional architecture view shows how multiple Communities of Interest (COI) (for example, nations, MoDs, DoD, and the IC) are able to complete secure cross-domain voice communications by using a single, common, secure IP architectural backbone that continues to provide domain separation where and when needed.

Figure 2. Architecture 2: Notional View of a CVVoIP (aka Voice over Secure IP [VoSIP]) Service



Summary

By using the multi-nationally adopted Secure Communications Interoperability Protocol, Cisco and EADS-NA have developed a cross-domain voice solution that provides critical mission capability for IP telephony solutions being deployed across defense and intelligence communities today in both the enterprise and tactical environments.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

Printed in USA

C11-698311-00 02/12