Government Use Cases for Secure Communications: Transition from TDM Telephony to IP Telephony

What You Will Learn

Transitioning from time-division multiplexing (TDM) voice systems to unified communications, also called IP communications, reduces government costs and provides new collaboration capabilities to accelerate speed to decision, knowledge exchange, and responsiveness. Cisco® Unified Communications solutions meet all government security requirements for communications, either off the shelf or in combination with solutions from Cisco ecosystem partners.

This white paper, intended for federal government personnel planning agency communications solutions, describes common use cases for Cisco Unified Communications in government:

- Migrating from TDM telephony to IP telephony
- Deploying phones in a Secure Compartmentalized Information Facility (SCIF)
- Encrypting voice traffic
- Migrating to voice-over-secure-IP (VoSIP) in military organizations

Migrating to Unified Communications

Situation

A civilian agency is migrating from a private branch exchange (PBX) system or Centrex service to unified communications. The agency's security requirements include:

- Complying with all federal regulations for communications security
- Protecting privacy by preventing eavesdropping
- Supporting continuity of operations (COOP) plans by preventing denial of service (DoS) attacks or distributed DoS (DDoS) attacks
- Preventing loss of information through impersonation
- Protecting unified communications applications such as voicemail, contact centers, or presence from infection or outsider control, including revealing employee names or locations
- Securing soft phones used for voice, video, and instant messaging
- Preventing toll fraud

Solution

Cisco Unified Communications meets all federal and National Security Agency (NSA) security requirements. Security is not an add-on that can be turned off or removed, but rather is built into all solution components off the shelf. Examples of the many Cisco Unified Communications security capabilities include:

- Voice traffic is kept separate from data traffic on its own virtual LAN (VLAN). This helps prevent a hacker who gains access to a government data network from also accessing the voice network. Furthermore, an intruder cannot access the voice VLAN by connecting a PC to a Cisco Unified IP Phone.
- All voice traffic is encrypted, including phone-to-phone, the audio portion of multimedia conferences, and voicemail playback.

- Cisco switches, routers, firewalls, and phones all have features to prevent DoS attacks from interrupting voice services. For example, Cisco Unified IP Phones resist malformed packets, and basic quality-of-service (QoS) policies in Cisco Catalyst® switches protect application servers and gateways from being overrun.
- Cisco Security Agent software resides on application servers to detect and stop anomalous application behavior before harm occurs. Default settings allow only those processes required for the specific application, such as Cisco Unified Communications Manager or Cisco Unity® Connection voicemail.
- Cisco firewall solutions recognize voice and video traffic, dynamically opening and closing the firewall port as each call starts and ends. Because the port does not have to be kept open, the time in which an attack can get through is minimized.

Many other security capabilities work in combination to provide defense in depth, protecting information privacy and preventing attacks from interrupting government voice services.

Deploying Phones in a Secure Compartmentalized Information Facility

Situation

A civilian or military intelligence agency needs two types of secure phones in a Secure Compartmentalized Information Facility (SCIF). Phones connected to classified networks (“red phones”) are used only for calls within the agency. Phones attached to unclassified networks (“black phones”) can also access the public switched telephone network (PSTN).

Solution

Cisco Unified IP Phones are certified for use as red phones in SCIFs, with no modification required. Agencies that need black phones can obtain them from Cisco ecosystem partners, including API and CIS Secure Computing. These partners modify Cisco Unified IP Phones by adding a positive disconnect circuit and an activation button. When not in use, the phone is disconnected, preventing its use as a clandestine listening device that transmits audio from the room to an outside party. Before making a call, users press the button to connect the circuit and allow audio transmission.

Using Cisco Unified IP Phones for both black and red communications in a SCIF reduces management overhead. Although the phones connect to separate networks, a single administrator can manage all phones using the same Cisco Unified Communications Manager interface, reducing training requirements. Telecore also provides a phone that connects to classified as well as unclassified networks and is compatible with Cisco Unified Communications Manager.

Encrypting Voice Traffic

Situation

Certain personnel need Type 1 phones, which are certified by the NSA for encrypting classified information. The phones perform encryption and decryption internally. Traditionally, Type 1 phones could only connect to traditional time-division-multiplexed (TDM) voice systems. Therefore, even if only a handful of users needed Type 1 phones, the agency could not take advantage of unified communications for collaboration and cost savings without also operating a separate TDM network.

Solution

Cisco ecosystem partners General Dynamics and L-3 Communications provide Type 1 phones that are compatible work with Cisco Unified Communications Manager and Cisco routers. Communications to and from these phones - the General Dynamics vIPer and L-3 Communications Secure Terminal Equipment (STE) - are encrypted even if the network connection itself is not inherently secure. Therefore, agencies can transition to unified communications by providing Cisco Unified IP Phones for users who do not need encryption, and Type 1 phones to users that do need

encryption. The Cisco phones and Type 1 phones both receive services through the same Cisco Unified Communications Manager, simplifying management.

Migrating to Voice over Secure IP in Military Organizations

Situation

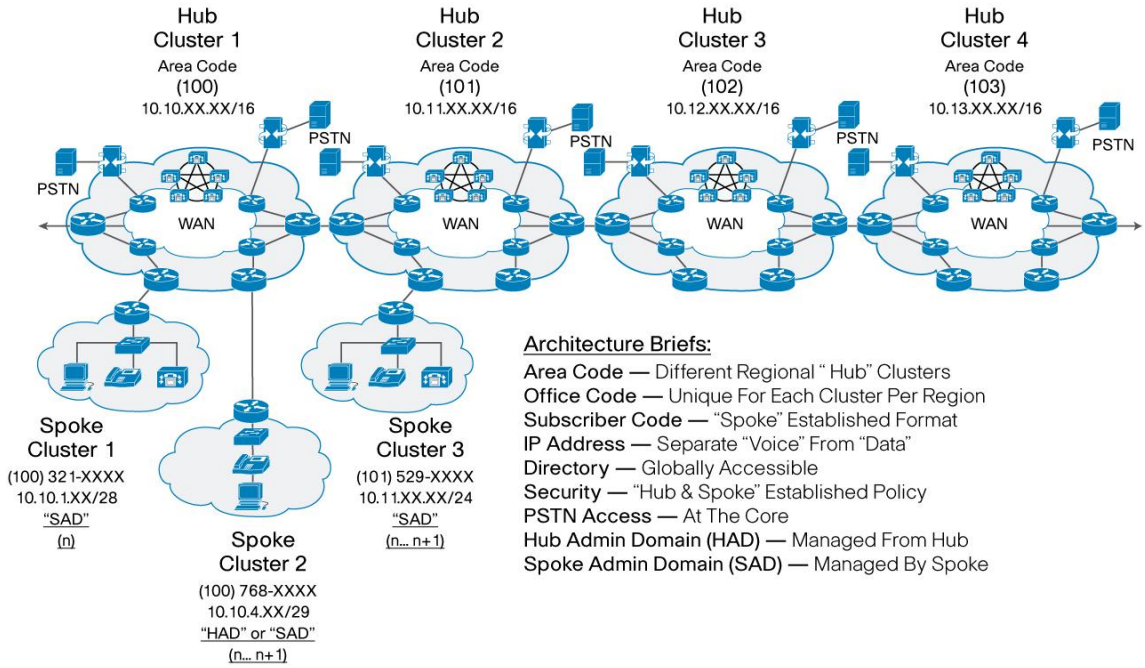
Military organizations have begun integrating their IP telephony enclaves into the Defense Information Systems Agency (DISA) Information Systems Network (DISN). The intent of joining the DISN is to increase the speed of command, more effectively link knowledgeable entities in and between theaters, enable simpler and improved communications across coalition forces, and align with the Department of Defense Network-Centric Operations (NCO) strategy.

Solution

DISA has implemented a Voice-over-Secure-IP (VoSIP) architecture to provide low-cost, stable, and secure communications transport across an encrypted data network (Figure 1). The VoSIP architecture currently supports more than 151 different federal government organizations in a hub-and-spoke, tandem-switched architecture. Designed for civilian as well as Department of Defense organizations, this specialized command and control (Special C2) telephony system uses Cisco Unified Communications technology to provide the following operational benefits:

- Reduce the demand on the circuit-switched network
- Scale with little effort because of a standardized, global dial plan including directory services
- Provide redundancy and survivability with a distributed, regional and localized voice architecture
- Centralize administration, security, control, and management with no single point of failure
- Help to ensure availability and high quality by providing scalable bandwidth and call admission control

Figure 1. Enterprise Hub-and-Spoke Architecture for VoSIP



Conclusion

Cisco Unified Communications solutions meet all government security requirements, off the shelf. The built-in security capabilities plus partner solutions for specific mission requirements enable civilian and defense agencies to migrate confidently to unified communications. Major benefits include better support for collaboration within and between agencies, lower costs, and simplified management.

For More Information

To read about Cisco solutions for federal government, visit: http://www.cisco.com/go/federal.

To arrange a demonstration of Cisco technologies at the Public Sector Center of Excellence in Herndon, Virginia, contact your local Cisco account team.

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 C11-631468-00 10/10