Cisco Secure Communications: Address Government Security Requirements with Off-the-Shelf Solutions

What You Will Learn

Secure communications requires two types of protections: privacy and safeguards against outside attacks or insider threats that could impede continuity of operations (COOP).

This white paper, intended for civilian and defense personnel planning the transition to unified communications, briefly summarizes how Cisco® Unified Communications solutions meet all government security requirements, off the shelf. Cisco solutions provide:

- End-to-end security, for defense in depth
- Compliance with all federal and National Security Agency (NSA) requirements
- Security technology that is integrated, not an add-on that can be removed
- Security for other collaboration activities accompanying voice, such as video and web sharing
- A large partner ecosystem to meet specific agency needs

End-to-End Security, for Defense in Depth

Every element in a Cisco Unified Communications solution helps to protect privacy and prevent attacks. These elements include Cisco Unified Communications Manager, Cisco routers, gateways, and Ethernet switches, Cisco Unified IP Phones, and application servers for voicemail, contact center, and so on. Figure 1 maps each component to the security threats it helps to prevent. A Cisco end-to-end solution eliminates the risk and expense of integrating multiple vendors' security systems. Solutions from Cisco ecosystem partners are preintegrated and tested.

Figure 1. The Most Common Government Security Settings Are Preconfigured

	Phones	Switches	Routers	Network/ Firewall	Cisco Unified Communications Manager	Servers
Eavesdropping	X	X	X		X	
Denial of Service	X	X	X	X	X	X
Impersonation	X	X		X	X	
UC Applications Security					X	X
Soft Client				X	X	
Toll Fraud			X		X	

The components of Cisco Unified Communications solutions work collaboratively to prevent external or insider threats that could compromise privacy or take down communications[1]. Consider eavesdropping, for example. A sampling of the many technologies to prevent eavesdropping includes:

- Default settings in Cisco Unified Communications Manager keep Cisco Unified IP Phones from displaying information that a hacker could use to eavesdrop.

[1] Fifty percent of all attacks are internal, according to CIS/FBI Computer Crime and Security Survey, 2008.

- Cisco Unified IP Phones stop traffic from PCs masquerading as other phones, preventing intruders from accessing the VLAN.
- Cisco Unified IP phones protect voice traffic from “man-in-the-middle” attacks that users would not ordinarily notice.
- The phone software image is digitally signed at the Cisco factory, preventing someone from replacing that image to remotely control the phone or listen in on conversations.
- Cisco Catalyst® switches stop hackers from impersonating a router to intercept voice streams, a technique known as Dynamic Host Configuration Protocol (DHCP) snooping.
- Cisco Catalyst switches also prevent hackers from sending Address Resolution Protocol (ARP) packets to snoop, modify, or stop packets.

Other Cisco Unified Communications security technologies help prevent denial-of-service (DoS) and distributed DoS (DDoS) attacks. For example:

- Cisco Unified IP Phones resist network-based attacks such as runts, shorts, giants, and malformed packets.
- The phones do not accept invitations from devices other than Cisco Unified Communications Manager.
- Basic quality-of-service (QoS) policies in Cisco Catalyst switches protect application servers and gateways from being overrun.
- Adding a scavenger-class QoS category limits the total amount of data that an attacker can send before the traffic is remarked for less-than-best effort. The result is that agency voice and video traffic continues to receive adequate bandwidth during DoS attacks.
- Cisco firewalls check packets as they flow through the firewall, blocking them if they do not meet specifications. The firewall also imposes a rate limit on most of protocols that flow through the firewall.

Field Tested and Certified

Cisco Unified Communications is accredited by every branch of the U.S. intelligence community. In addition, the solutions have been field tested in every industry and around the world since their introduction in the late 1990s, giving Cisco engineers the opportunity to fine-tune the security design. Cisco Unified Communications is the most popular communications system of any type, either IP or time-division multiplexed (TDM). As of June 2010, Cisco Unified Communications solutions were deployed in more than 100,000 organizations that collectively use more than 30 million phones and 66 million gateway ports. More than 400 customers have very large deployments with more than 5000 phones.

Cisco invests heavily in product certification to help ensure that Cisco Unified Communications solutions meet or exceed Department of Defense (DoD) mission requirements, including security. Cisco Unified Communications solutions support the following standards:

- Interoperability I/O and Information Assurance (IA)
- Assured Service Voice Application LAN (ASVALAN) for Cisco switches and routers
- Support for secure devices: Certified Secure Telephone Unit (STU) and Secure Terminal Equipment (STE) support
- Federal Information Process Standard (FIPS) 140.2

Integrated Security, Not an Add On

Every hardware and software element of Cisco Unified Communications has security built in. Therefore, hackers and insiders cannot turn off or remove security, either deliberately or unintentionally. Built-in security also relieves agency IT groups from having to research security options and find budget for add-ons. Furthermore, every new security feature that Cisco introduces is available to every customer in the next software release, giving government access to

innovations introduced in the private sector. The result is that each government agency's system is as secure as the systems of other agencies, enabling secure interagency collaboration.

Security for All Collaboration Activities, Not Just Voice

Increasingly, voice conversations are part of multimedia collaboration sessions that also include video and web sharing. Security is integrated into all Cisco collaboration solutions, including Cisco Unified Communications Manager and Cisco Unified IP Phones, as well as Cisco TelePresence® systems, Cisco WebEx™, and Cisco videoconferencing solutions such as TANDBERG Movi software for high-definition video on a PC.

All security in Cisco collaboration solutions is standards-based. Therefore, an agency that implements a Cisco Unified Videoconferencing Multipoint Control Unit (MCU) can continue to use existing videoconferencing equipment from other vendors that also uses standards-based security.

Large Ecosystem of Partners for Specialized Government Security Needs

Off-the-shelf Cisco solutions meet the vast majority of government needs. For specialized requirements, Cisco has a large ecosystem of partners that provide customized solutions. A few examples include:

- **Phones for airplanes:** A partner provides Cisco Unified IP Phones with the aluminum casing required in airplanes.
- **Black phones in Secure Compartmentalized Information Facilities (SKIFs):** Cisco partners API and CIS Secure Computing provide a modified Cisco Unified IP Phone that includes a positive disconnect circuit and an activation button.
- **Type 1 encrypted phones:** General Dynamics Viper and L-3 Communications Secure Terminal Equipment (STE) phones work out of the box with Cisco Unified Communications Manager and Cisco routers.

Conclusion

Cisco Unified Communications solutions meet all federal government security requirements without requiring extra expense or effort by government IT teams. An end-to-end Cisco solution provides defense in depth, increasing protection against attacks that otherwise might expose sensitive information or interrupt agency voice services. As agencies provide business video tools to the workforce to enable collaboration and comply with the 2010 Telework Enhancement Act, secure Cisco Unified Communications solutions will integrate with other secure Cisco Collaboration solutions without expensive or time-consuming integration efforts.

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 a Cisco Center of Excellence, 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 C11-634233-00 11/10