

# Provide Secure Unified Communications with Cisco IOS Firewall Session Initiation Protocol

Help Enhance the Integrity and Availability of Cisco Unified Communications

## Abstract

Many organizations have discovered that unified communications—the convergence of data, voice, and video onto a single network infrastructure—can enhance employee productivity and mobility, while dramatically reducing communications costs. What is crucial to attaining these advantages is securing unified communications systems to maintain service availability and system integrity. To increase protection, Cisco® recommends an approach in which multiple layers of security are integrated throughout Cisco Unified Communications applications and systems. The four primary components of a unified communications system include the endpoints; call control; applications; and, perhaps most critically, the converged IP network infrastructure. Cisco router-based security solutions provide a solid foundation toward building a secure unified communications architecture that can secure each of these four critical components. Cisco IOS® Firewall provides perimeter security and policy control to maintain the integrity and availability of unified communications components.

## Benefits

With Cisco Secure Unified Communications, your organization can:

- Mitigate Cisco Unified Communications security threats: Identify attempts to exploit security vulnerabilities and deviations from your corporate security policy and industry best practices.
- Improve the integrity of Cisco Unified Communications: Protect the primary elements of the unified communications system by validating communications requests.
- Maintain the highest availability of the system: Help ensure that critical unified communications services, such as communications gateways and the underlying network infrastructure, remain highly available and resistant to attempts at service disruption.
- Increase your network administration and IT staff productivity: Enable your organization to enforce consistent, efficient Cisco Unified Communications security policies and procedures.
- Lower your total cost of ownership (TCO) for Cisco Unified Communications: Improve your unified communications system operating procedures through the consistent deployment of security controls, such as a common security and unified communications footprint in remote locations.

## Session Initiation Protocol

Session Initiation Protocol (SIP) is an application-layer control (signaling) protocol for creating, modifying, and terminating sessions with one or more participants. These sessions could include Internet telephone calls, multimedia distribution, and multimedia conferences. SIP is based on an

HTTP-like request/response transaction model. Each transaction consists of a request that invokes a particular method, or function, on the server and at least one response.

SIP makes use of elements called proxy servers to help route requests to the user's current location, authenticate and authorize users for services, implement provider call-routing policies, and provide features to users. SIP runs on top of several different transport protocols.

### **How Does Cisco IOS Firewall Provide Enhanced Voice Security?**

Cisco IOS Firewall SIP protection enhances Cisco IOS Firewall to provide RFC 3261-conformant inspection and control of SIP traffic. This protects valid SIP endpoints and call-control resources against the negative effects of malformed SIP signaling and requests that can be used to exploit potential vulnerabilities in important system resources. Malformed packets, also known as protocol fuzzing, are one of the most common means to exploit unified communications systems. By filtering these malformed packets, the Cisco IOS Firewall can provide an effective first line of defense.

Cisco IOS Firewall SIP inspection goes beyond protocol conformance and can enable an organization to apply fine-grained application policies. This provides organizations with the tools to help ensure that only authorized services are enabled and, with an array of filtering options available, enables policy to be applied based on user or phone number, not just network addresses, making Cisco IOS Firewall SIP Inspection a truly unified communications-aware security platform.

Cisco IOS Firewall SIP Protection accommodates SIP security requirements and improves support for new capabilities in the Cisco Unified Communications product line by:

- Restricting irrelevant or malicious traffic: By enforcing mandatory header fields, restricting forbidden header fields, checking header-parameter validity in the context of each message, discarding non-SIP traffic on SIP signaling channels, and applying configurable policy on unknown SIP methods, Cisco IOS Firewall SIP Protection greatly diminishes the likelihood of a successful attack that applies malformed or invalid traffic.
- Assuring manageability; Cisco IOS Firewall SIP Inspection provides the ability to configure and dynamically add new methods and extensions as configuration modifications are needed and by offering syslog messages on various SIP events and messages.
- Adding support for recent standards that extend SIP's capabilities, such as SIP-TCP, Session Description Protocol (SDP) grouping (RFC 3388), sip-outbound (draft-ietf-sip-outbound), alternative network address types (RFC 4091), symmetric routing support/rport (RFC 3581), and SIP multipart Multipurpose Internet Mail Extensions (MIME).
- Upgrading Cisco CallManager and IP-IP gateway version support: Updates SIP support to that required by Cisco Unified CallManager Version 5 and Cisco Unified CallManager Express Version 4.0 as well as providing interoperability with the Cisco IP-IP gateway version consistent with Cisco CallManager Express v3.x and Cisco CallManager v4.x and above.

Cisco IOS Firewall SIP Protection defends against denial of service (DoS) attacks which can disrupt unified communications voice systems through depletion of resources by:

- Rate-limiting SIP INVITE and REGISTER messages
- Rate-limiting total number of SIP messages
- Limiting the number of active calls

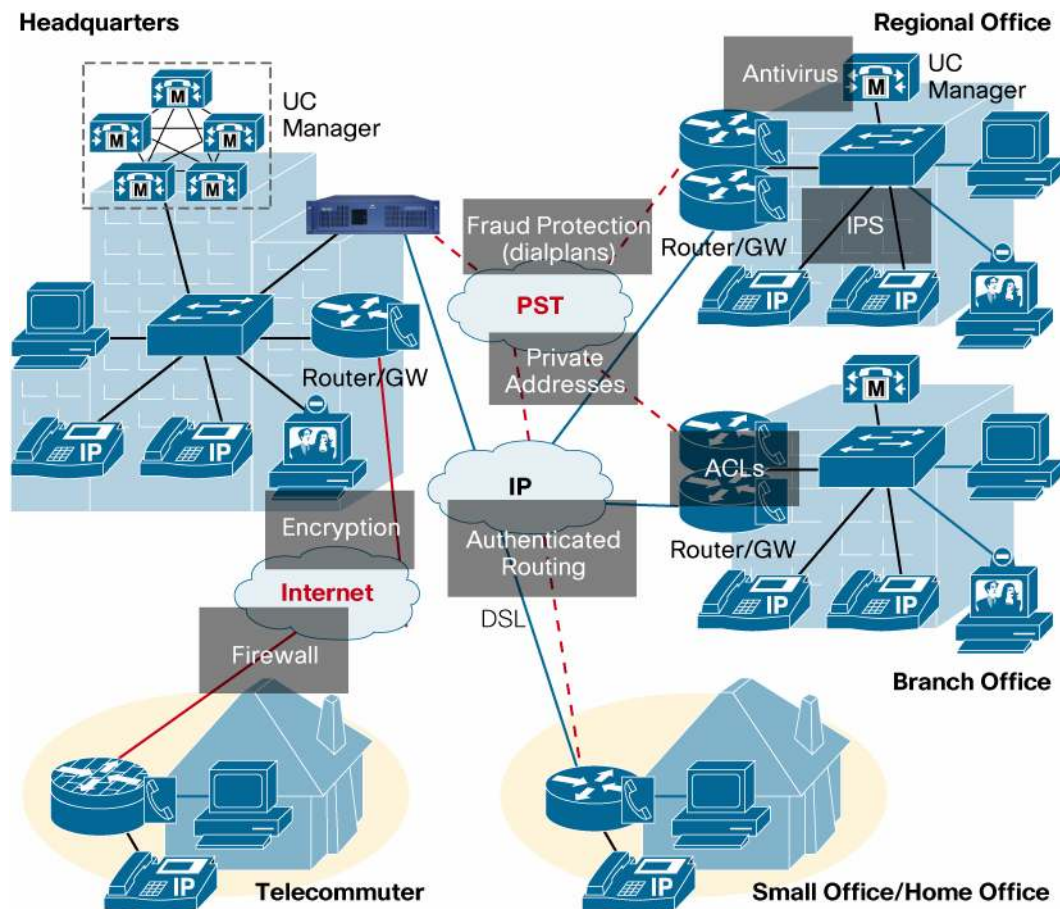
SIP Application and Inspection Control provides granular control over SIP application activity (Table 1).

**Table 1.** Granular Control over SIP Application Activity with SIP Application and Inspection Control

Feature	Benefit
Blacklist/whitelist of callers and callees	Restricts dialing destinations to reduce the likelihood of toll fraud
Filtering for SIP messages based on: <ul style="list-style-type: none"> <li>• Methods (or a group of methods)</li> <li>• Uniform Resource Identifiers (URI)'s or a group of URIs</li> <li>• SIP version</li> <li>• SIP header fields</li> </ul>	Limits SIP messages to known-good content to stifle attacks on call-control resources and end hosts
Ability to filter SIP messages based on the Via headers IP address or names	Limits exposure to specific DoS attacks and efforts to mask originating or destination end hosts
Hide endpoint software version	Reduces exposure to network reconnaissance where potential attackers "fingerprint" hosts to find vulnerabilities
Cross check of content length and actual packet size	Reduces potential of buffer overrun/underrun attacks
Ability to specify: <ul style="list-style-type: none"> <li>• SIP message based on total message length</li> <li>• Min/max content length</li> <li>• Min/max lengths for various fields such as Methods, URIs, Via-headers, total header, and so on</li> </ul>	Limits buffer overflow and DoS attacks and provides granular application control
Ability to filter messages based on content type	Controls type of content carried by SIP to filter unwanted content types that might carry undesired or malicious material
Ability to disable instant messaging	Blocks undesired SIP instant messaging application activity

Figure 1 shows the recommended multilayer architecture for secure unified communications.

**Figure 1.** Multilayer Architecture for Secure Unified Communications Recommended by Cisco



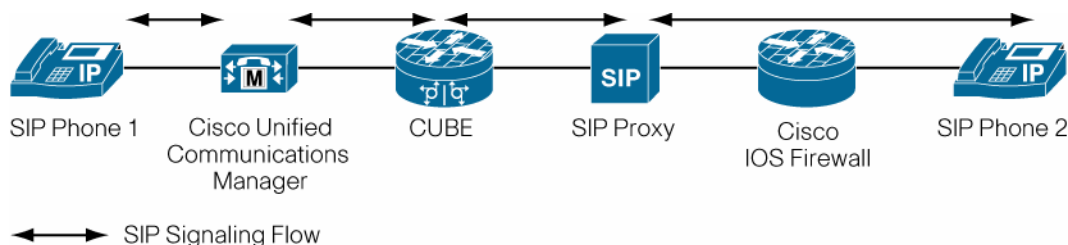
**Use Case Scenarios**

The following are some typical deployment scenarios where Cisco IOS Firewall plays a primary role in protecting unified communications components such as Cisco Unified Communications Manager, Cisco Unified Border Element, and the endpoints.

**Deployment 1: SIP Trunk-Based Connectivity**

This is a typical enterprise deployment that utilizes the service provider SIP trunk to provide access to remote branch sites (Figure 2). Cisco Unified Border Element is providing SIP trunk interworking for Cisco Unified Communications Manager at the headquarters site, with SIP trunk services provided by the service provider. The remote site, with Cisco IP phones deployed, is protected by Cisco IOS Firewall, enabling the remote site to securely connect to the service provider network.

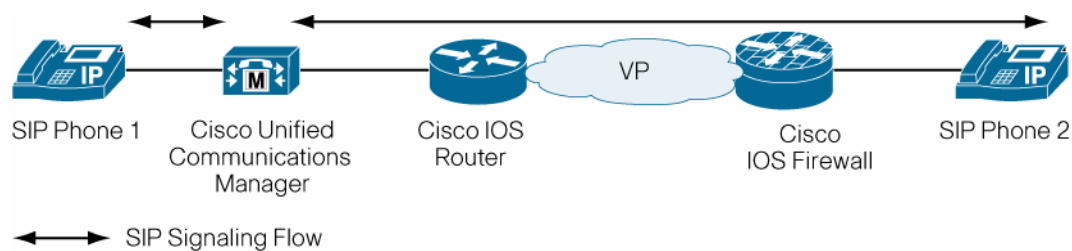
**Figure 2.** SIP Trunk-Based Connectivity Deployment



**Deployment 2: Enterprise-Class Telecommuter Deployment**

This deployment case illustrates a remote enterprise-class telecommuter site that connects to the headquarters through a VPN tunnel (Figure 3). The WAN, either a leased-line or an Internet connection, provides the basic transport. The remote phone registers to the centralized communications manager, but to protect the remote site from the untrusted WAN connection, Cisco IOS Firewall is able to protect the communications between the phone and the centralized unified communications resources.

**Figure 3.** Enterprise-Class Telecommuter Deployment



### Summary

The Cisco IOS Firewall SIP Inspection and Control feature greater control over network traffic to protect the data network; unified communications infrastructure resources such as Cisco Unified Communications Manager and Cisco Unified Communications Manager Express; and IP telephony endpoints and resources such as IP phones, Cisco Unity<sup>®</sup>, and Cisco TelePresence resources. Increased protection for these resources helps ensure that voice and data resources offer reliability, performance, and security to provide an effective environment to meet business needs.

### Additional Resources

NIST recommendations for securing voice-over-IP systems

<http://csrc.nist.gov/publications/nistpubs/800-58/SP800-58-final.pdf>.

Cisco Secure Unified Communications <http://www.cisco.com/go/secureuc>.

Cisco IOS Firewall <http://www.cisco.com/go/iosfw>.



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](http://www.cisco.com/go/offices).

CCDE, CCVP, Cisco Eze, Cisco StadiumField, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play and Learn is a service mark; and Access Registrar, Altran, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSF, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS IPPhone, IP/TV, IQ Expertise, the IQ logo, IQ Net Readiness Scorecard, iQuickStudy, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MIM, Networker, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. ©2007