Firewalls for Secure Unified Communications

Positioning Guide

Firewall protection for call control and unified communications applications is an increasingly common security requirement for unified communications deployments. Firewall platforms are sometimes dictated as a mandatory requirement in corporate security policies and are becoming established as a best practice. Firewall platforms can provide security services that enhance security without impacting the performance and availability of the unified communications system.

Cisco offers a range of firewall platforms to deliver additional security to unified communications deployments, with each platform positioned to provide key security services for differing deployments. It is important to understand the positioning for each of the firewall platforms and the specific security services they can provide.

Firewall Platform Security Services for Unified Communications

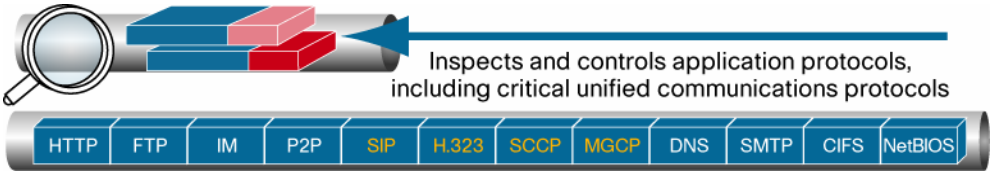
Security services for unified communications deployments can be broken down into four main categories: access control and Network Address Translation (NAT), protocol conformance, application inspection and control, and encryption services.

Access Control and NAT

A key function of firewall platforms is to provide stateful, network-based access control to application servers. In the unified communications context, this includes Cisco® Unified Communications Manager and application servers such as Cisco Unity®, Cisco Unified MeetingPlace®, and Cisco Unified Presence. By controlling access from clients to these servers, the firewall can prevent malicious or unauthorized network connections from being initiated to these critical servers, which could impact performance or availability. By inspecting the connections to ensure that they meet the access control policy and that the connection conforms to expected behavior, firewalls provide a first line of defense for a secure unified communications deployment.

Although most firewall platforms are able to deal with data applications that use consistent static ports to communicate, unified communications protocols such as Session Initiation Protocol (SIP), Skinny Client Control Protocol (SCCP), and H.323 have special requirements that not all available firewall platforms can support. SIP, SCCP, and H.323 signal to Cisco Unified Communications Manager using well-known ports that the firewall is able to inspect and apply policy to. However, associated media traffic (Real-Time Transport Protocol and Secure Real-Time Transport Protocol [RTP/SRTP]) does not use a static port that the firewall can anticipate for media traffic inspection. Instead, these protocols negotiate the media port that will be used for the stream, which for audio alone could be any even-numbered port between 16384 and 32767. This means either configuring the firewall to allow traffic on all the possible ports, or the firewall must be able to dynamically inspect the signaling traffic to identify that port if the media is expected to pass through the platform. Opening all the possible RTP media ports on the firewall dilutes the access control capability and exposes the unified communications system to a range of attacks and reconnaissance.

Figure 1. Unified Communications-Aware Firewalls



Unified-communications-aware firewalls are able to inspect the signaling channel and dynamically open only the port that has been negotiated (Figure 1). The port remains open only as long as the firewall does not see signaling that suggests the call is over, or until the connection times out. Dynamically opening a pinhole minimizes the access control exposure and affords a tighter first line of defense.

Although strongly discouraged, there are occasions when there is a requirement to provide NAT to the signaling and media packets. In the case of signaling in particular, this requires the platform to translate not only the external IP header but also the embedded address held within the payload of the signaling packet. Unified-communications-aware NAT functions, often deployed in firewall platforms, need to be able to provide this advanced capability. Without unified-communications-aware NAT translation, the call processing system will reject the request because of the inconsistency between the external and embedded IP addresses.

Protocol Conformance

Firewalls have evolved to understand and enforce conformance of the protocols that applications use to communicate. This is critical, because in the unified communications context, protocols such as SIP and SCCP can be used to attack call processing systems, such as Cisco Unified Communications Manager. The attacks, sometimes referred to as protocol fuzzing, are based upon sending malformed SIP or SCCP packets to the call processing system. This can include incorrect data formats, data that exceeds the length of the expected data field, and other distortions of the expected packet header. Although the call processor will usually reject the malformed packet, there have some cases where the malformed packets have impacted the Communications Manager's ability to process other calls. It is therefore beneficial to provide a first line of defense: Cisco firewall platforms are able to check the conformance of signaling packets to the expected standards. If malformed packets are detected, they can be silently dropped and the offending client's details logged.

For details of some of the known protocol fuzzing issues that relate to Cisco platforms, please refer to the security advisory services available at http://www.cisco.com/en/US/products/products_security_advisories_listing.html.

Application Inspection and Control

Network-based policy enforcement often requires firewalls to have greater awareness of the applications whose traffic traverses the platform. Preventing unregistered phones from initiating call requests to the Cisco Unified Communications Manager and denying the use of SIP-based instant messenger activity are two examples of application policy enforcement enabled by firewall inspection and control. If advanced policy enforcement is required for the unified communications deployment, you will need to verify the control features available on the platforms, as support will vary.

Encryption Services

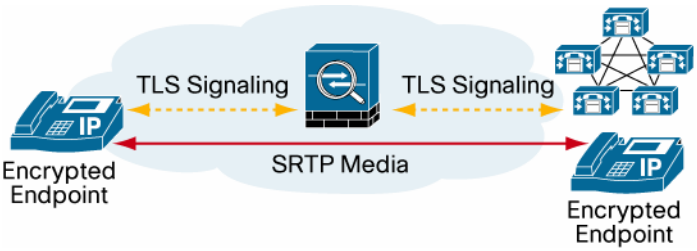
Encryption for the Internal Network

To mitigate internal eavesdropping and to achieve corporate and regulatory compliance, some unified communications deployments employ encryption (Transport Layer Security [TLS] and SRTP) within the internal network. Although this service is usually a function employed between the endpoints and the call control platform, it does have security implications for firewall deployments. In many vendor solutions, encryption and firewalling are not interoperable, leaving enterprises forced to choose between security mechanisms.

The problem lies with the requirement for the signaling to be encrypted. In most unified communications platforms, the call processing agent, for reasons of performance and scalability, determines the encryption keys the endpoints will use to encrypt their media. These keys are passed to the phones in the signaling messages; therefore, it is critical to ensure that the signaling is encrypted to protect those keys from being read by an attacker. By encrypting the signaling, the firewalls that are employed to protect the communications manager and other applications no longer have access to the information to function as a unified-communications-aware firewall. Unified-communications-aware NAT, the dynamic opening of pinholes for the media, and the application of policy and protocol conformance are all lost if the firewall is unable to decrypt the signaling.

Cisco has developed a unique feature called TLS Proxy on the Cisco ASA 5500 Series platform to address this specific integration issue (Figure 2). With TLS Proxy, the firewall is added to the Certificate Trust List (CTL) used by the IP phone. The trust list determines which devices the phone is allowed to establish a TLS encrypted signaling session with. In effect, the Cisco ASA appliance, as a trusted device within the Cisco Unified Communications Manager system, is able to intercept the encrypted signaling, mutually authenticate with the endpoint, and decrypt the signaling. Once the signaling is decrypted, the ASA appliance is able to retrieve all the necessary signaling information and apply all the inspection and policy enforcement actions. To maintain secure connectivity from end to end, the ASA appliance then initiates a secondary TLS session back to the Cisco Unified Communications Manager. The signaling and communications between endpoint and Communications Manager remain functionally the same and the firewall is able to deliver its unified communications security services

Figure 2. TLS Proxy on the Cisco ASA 5500 Series Platform



Encryption for Remote Access

As organizations continue to expand remote and mobile unified communications services, the combination of firewall and secure connectivity services within a single device are becoming a common platform requirement. Many firewall platforms have evolved to support remote-access encryption in addition to the core firewalling services. IP Security (IPsec) and Secure Sockets Layer (SSL) are commonly supported encryption standards, and can be used to provide secure connectivity services for remote or mobile soft phone clients. These solutions provide security

services for voice and data applications with the security client largely independent of the unified communications client.

More recently, a number of third-party phones have embedded VPN technology to provide an integrated VPN phone capability. Typically, the Datagram TLS standard has been adopted to offer encryption that is optimized for delay-sensitive traffic, such as media, due to its use of User Datagram Protocol (UDP) rather than TCP.

For endpoints such as desk phones, encryption is typically provided by TLS for signaling traffic and SRTP for the media. For existing Cisco IP phones, there is no means to take advantage of IPsec and SSL services for remote access. To address this, the Cisco ASA has been developed to support an ASA Phone Proxy feature that enables organizations to use the native phone encryption technology (TLS/SRTP) in order to allow remote Cisco IP phones to securely connect to a Cisco Unified Communications Manager enterprise system.

The ASA Phone Proxy builds upon the TLS Proxy functionality but has been enhanced to provide key interoperability features. These features enable the remote phones to be seamlessly deployed without needing to re-configure the Cisco UC Manager and internal network phones to support encryption.

More details on the TLS Proxy and ASA Phone Proxy are available in the technology guides available at http://www.cisco.com/go/secureuc.

VPN and Encryption Positioning for Unified Communications

The range of options available for providing encryption for customer confidentiality is covered in more detail in a related positioning guide titled “Cisco Unified Communication Confidentiality: VPN and Encryption Solutions”, available at http://www.cisco.com/go/secureuc.

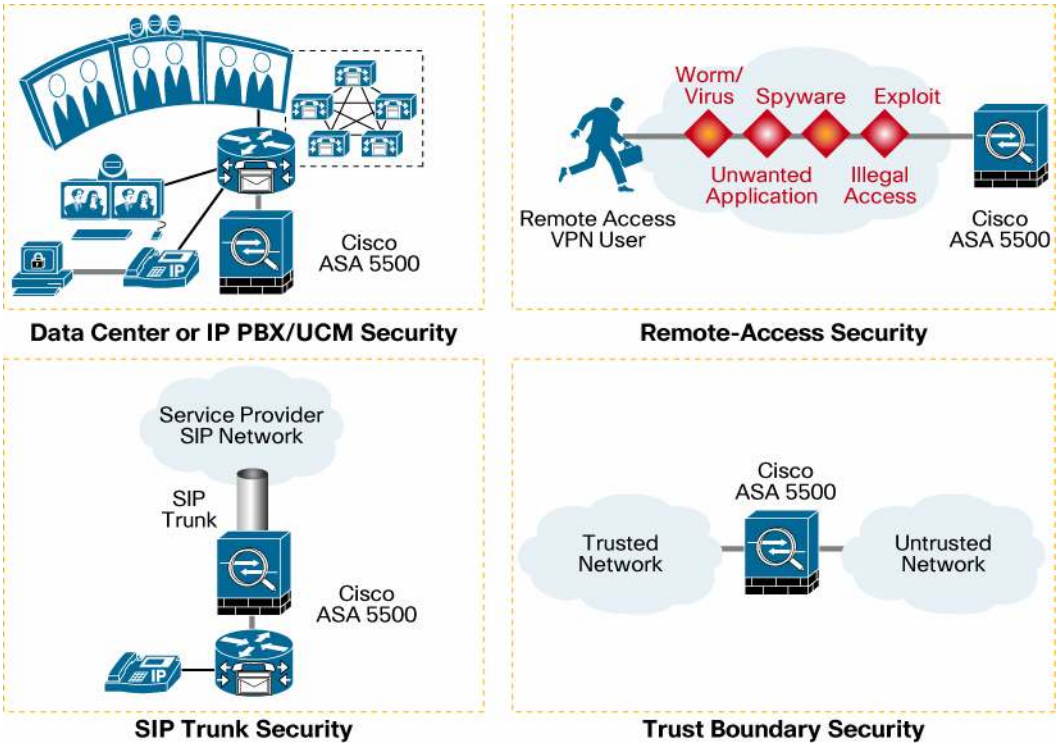
Cisco Firewall Platforms

Cisco ASA 5500 Series

Cisco ASA 5500 Series Adaptive Security Appliances are easy-to-deploy solutions that integrate world-class firewall, unified communications (voice/video) security, SSL and IPsec VPN, intrusion prevention (IPS), and content security services in a flexible, modular product family. Designed as a key component of the Cisco Self-Defending Network, the Cisco ASA 5500 Series provides intelligent threat defense and secure communications services that stop attacks before they impact business continuity. Designed to protect networks of all sizes, the Cisco ASA 5500 Series enables organizations to lower their overall deployment and operations costs while delivering comprehensive multilayer security.

The Cisco ASA 5500 Series is Cisco’s premier enterprise platform for unified communications firewall services and is deployed in a range of unified communication topologies (Figure 3). With the most advanced application inspection and control features, combined with unique encryption solutions such as TLS Proxy, the ASA appliance is well suited to campus firewalling for Cisco Unified Communications Manager, as well as perimeter deployments for remote-access solutions. As enterprises begin to adopt SIP trunking for their external voice services, the deployment of a firewall in conjunction with popular enterprise session border controllers, such as the Cisco Unified Border Element (CUBE), is becoming more common. In some cases, organizations have also used the Cisco ASA to provide a demarcation point between trusted and untrusted unified communications networks.

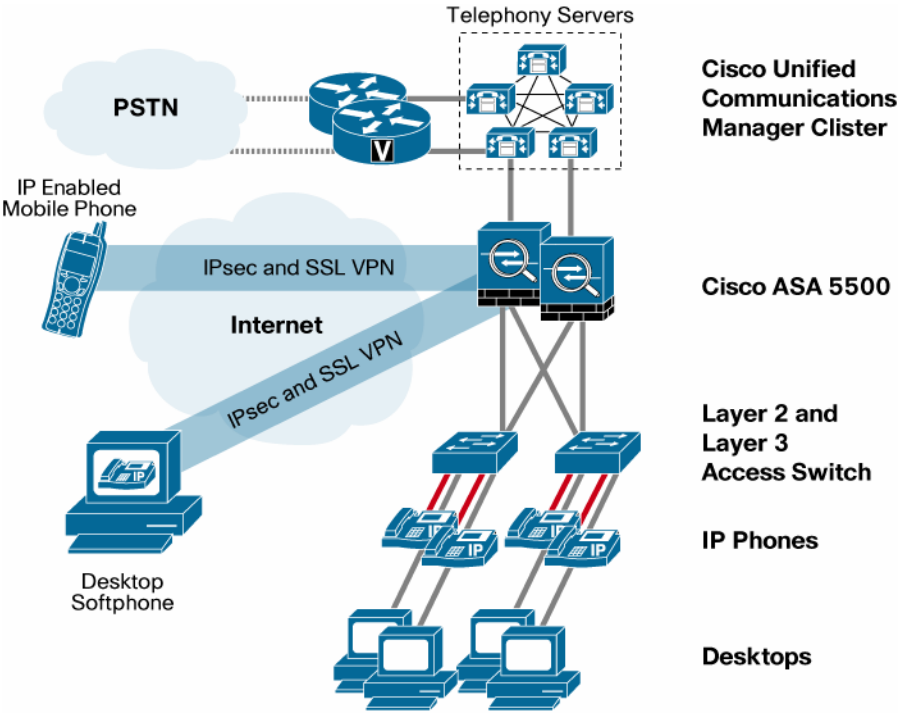
Figure 3. Unified Communications Deployment Topologies for the Cisco ASA 5500 Series



Within the campus, the optimal deployment for the ASA appliance is either within the data center or in front of Cisco Unified Communications Manager clusters (Figure 4). For remote-access services, the ASA appliance is optimally deployed at the enterprise's Internet edge, often behind the service provider customer premises equipment (CPE).

For detailed design guidance, please refer to the security chapter of the Cisco Solutions Reference Network design guide available at http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/srnd/7x/security.html.

Figure 4. Campus Deployment of the Cisco ASA 5500 Series



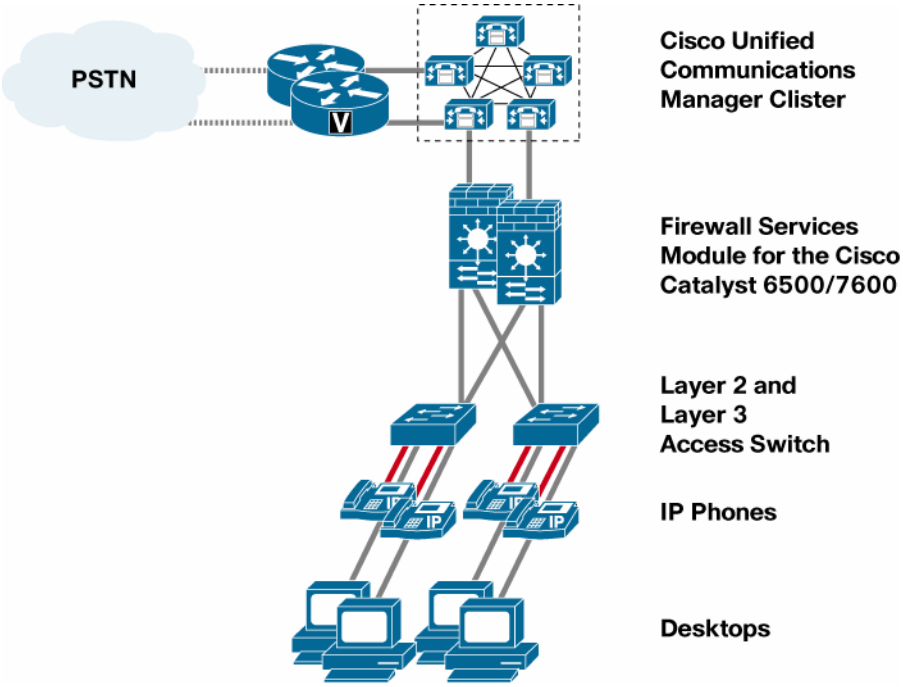
For detailed deployment guidance on the best practices for deploying Cisco ASA 5500 Series Adaptive Security Appliances, please refer to the Cisco ASA Unified Communications application note available at http://www.cisco.com/go/secureuc.

More general information on the Cisco ASA platform is available here http://www.cisco.com/go/asa.

Cisco Firewall Services Module for the Catalyst 6500/7600 Platforms

The Cisco Firewall Services Module (FWSM)—a high-speed, integrated firewall module for Cisco Catalyst® 6500 Series switches and Cisco 7600 Series routers—provides the fastest firewall data rates in the industry: 5-Gbps throughput, 100,000 CPS, and 1M concurrent connections. Up to four FWSMs can be installed in a single chassis, providing scalability to 20 Gbps per chassis. Based on Cisco PIX® technology, the Cisco FWSM offers large enterprises and service providers unmatched security, reliability, and performance (Figure 5).

Figure 5. The Cisco Firewall Services Module



The FWSM is a high-performance, firewall-only platform designed for deployment in data center environments. Integrated into Cisco's premier data center switching platform, the Catalyst 6500/7600 Series, the FWSM is positioned for unified communications deployments that are hosted in a shared environment with data applications. In enterprises that have standardized on the Catalyst 6500/7600 Series within a data center architecture, their core unified communications application inspection functions can enable the seamless deployment of unified communications application servers in the existing environment. Although not as feature-rich as the ASA appliance, the FWSM is firmly positioned in the multimedia data center environment.

The FWSM does not support any encryption for application traffic and is therefore not suited to any secure connectivity requirements. For enterprises that require internal integration services such as TLS Proxy, the ASA 5500 Series would be the preferred platform.

For detailed design guidance, please refer to the security chapter of the Cisco Solutions Reference Network design guide at

http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/srnd/7x/security.html

More general information on the Cisco Firewall Services Module is available here

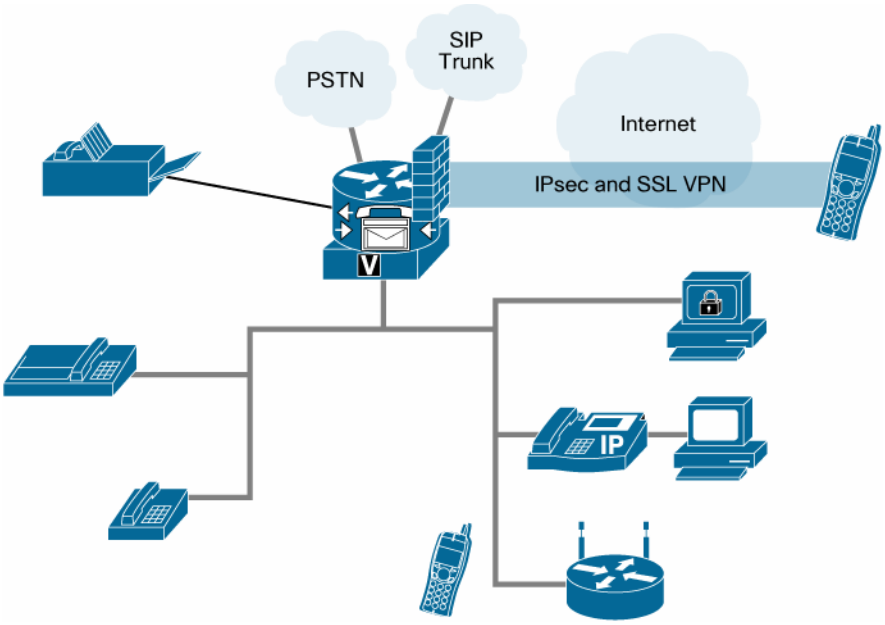
http://www.cisco.com/go/fwsm

Cisco IOS Firewall Feature Set

The Cisco IOS® Firewall is a stateful-inspection firewall option available for Cisco routers. Built from market-leading Cisco PIX Firewall technologies, Cisco IOS Firewall is supported on all the integrated services routers with the Cisco IOS Software Advanced Security or higher feature sets. Cisco IOS Firewall is an ideal single-box security and routing solution for protecting the WAN entry point into the network. The primary features of Cisco IOS Firewall include stateful firewall with denial of service (DoS) protection, and enhanced application, traffic, and user awareness to identify, inspect, and control applications. Packaged as part of a suite of software security services

on the routers, Cisco IOS Firewall can be combined with other security services such as URL filtering, IPS, and VPN to provide a complete solution for branch or commercial office.

Figure 6. Cisco IOS Firewall Secures Unified Communications Deployments



With the release of Cisco IOS Software Release 12.4.20(T), the Cisco IOS Firewall feature set provides a robust set of firewalling capabilities for the branch office or for commercial customer unified communications deployments (Figure 6). The feature set supports a range of unified communications protocols, providing cost-effective protection for both the firewall and for Cisco Unified Communications Manager Express. Deployed either on a separate router platform or co-resident with Cisco Unified Communications Manager Express, Cisco IOS Firewall applies services to traffic going to and from Cisco Unified Communications Manager Express to provide a secure, single-box unified communications solution. For commercial customers, the application of IPsec and SSL VPN provides a flexible, low-cost remote-access solution for remote soft phone clients, allowing remote users to make and receive calls from their office number as well as access message stores such as voicemail. All of this is possible within a single software feature set applied to a single device.

For detailed design guidance, please refer to the security chapter of the Cisco Solutions Reference Network design guide at http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/srnd/7x/security.html.

For detailed deployment guidance on the best practices for deploying the Cisco IOS Firewall, please refer to the Cisco IOS Firewall Unified Communications application note, available at http://www.cisco.com/go/secureuc.

More general information on Cisco IOS Security feature set is available here http://www.cisco.com/go/iossecurity.

Positioning and Feature Comparison Overview

Table 1.

	Cisco ASA 5500 Series Adaptive Security Appliance	Cisco Firewall Services Module	Cisco IOS Firewall
Stateful Inspection (Access Control)	• Yes • SIP UDP • SIP TCP • SCCP • RTP/RTCP • H.323 v1-4 • H.323 RAS • H.323 T.38 • MGCP • TAPI/JTAPI • CTI-QBE	• Yes (with FWSM 4.0) • SIP UDP • SIP TCP • SCCP • RTP/RTCP • H.323 v1-4 • H.323 RAS • H.323 T.38 • MGCP	• Yes (with Cisco IOS Software Release 12.5 and later) • SIP UDP • SIP TCP • SCCP • RTP/RTCP • H.323 v1-4 • H.323 RAS • H.323 T.38
Unified-Communications-Aware NAT	Yes	Yes	No
Protocol Conformance	Yes	Yes	Yes
Application Inspection and Control	Yes (SIP and SCCP)	Yes (FWSM 4.0)	On the roadmap
Remote Access/ Secure Connectivity	Yes (IPsec, SSL, DTLS)	No (firewall only)	Yes (IPsec and SSL in the Cisco IOS Advanced Security feature set)
Phone Proxy	Yes (Cisco ASA Software Release 8.0.4)	No (use Cisco ASA Phone Proxy)	No (use Cisco ASA Phone Proxy)
TLS Proxy	Yes (Cisco ASA Software Release 8.0)	No (firewall only)	No (on the roadmap)
Positioning	Campus and enterprise Internet edge for remote access	Data center: Unified communications and data applications	Branch office and commercial customers (Cisco Unified Communications Manager Express + Cisco IOS Firewall)

For a broader comparison of the enterprise-class firewall platforms available from Cisco, please review the comparison posted at http://www.cisco.com/en/US/prod/collateral/vpndevc/ps5708/ps5710/ps1018/C78-345384-04_CiscoIntegratedFirewallSolutions.html.

The Key to a Successful Unified Communications Firewall Deployment

A common perception is that applying firewalling to unified communications deployments is likely to lead to service interruption and other operational issues. The complexity of firewalling IP voice protocols, compounded by the impact of unified communications vendors altering signaling messages to add additional functionality, can result in compatibility issues between the firewalls and the unified communications system. Even if a firewall vendor claims its product supports the various voice protocols that will be used in the unified communications system, this is by no means a guarantee of interoperability. To ensure a successful firewall deployment, it is important to consult design guidance that is based upon a tested, validated solutions architecture.

The Cisco Solutions Reference Network Design (SRND) provides Cisco's recommendations for deploying security within a Cisco Unified Communications deployment. These guidelines are based upon extensive compatibility testing performed by the Cisco solutions testing teams who ensure that Cisco firewall platforms are interoperable and compatible with each release of Cisco Unified Communications Manager.

The SRND can be located here http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/srnd/7x/security.html.

The results of recent Cisco Unified Communications Manager system releases and the tested versions of code for each platform are listed here http://www.cisco.com/en/US/docs/voice_ip_comm/uc_system/unified/communications/system/ucstart.htm.

For a detailed guide on the available resources for deploying security within a Cisco Unified Communications system, please refer here http://www.cisco.com/go/secureuc.

Summary

There is clear value in the addition of firewalling services to supplement security within a unified communications system; this is becoming an increasingly common best practice. Cisco offers a comprehensive range of firewalling solutions for unified communications deployments, covering a number of common customer topologies.

The Cisco ASA 5500 Series provides multifunction security services for unified communications. Advanced firewall services that are tuned to provide protection for the demands of unified communications systems, combined with a range of encryption solutions, makes the ASA 5500 Series the premier Cisco firewall for enterprise campus and remote-access unified communications deployments. When protecting Cisco Unified Communications Manager clusters and providing a secure gateway for remote or mobile devices, the ASA 5500 Series would be the first choice.

The Cisco Firewall Services Module (FSWM) is optimally deployed in shared data center architectures that are based on the Cisco Catalyst 6500/7600 Series switches. Although not as feature-rich as the ASA appliance and not positioned for encryption services, the FWSM is an acceptable alternative for enterprises that require a common firewall platform to support voice and data in a single device.

The Cisco IOS Firewall provides protection for voice gateways and for Cisco Unified Communications Manager Express deployments. The cost-effective, integrated firewall and voice solution is commonly positioned in commercial and midrange enterprise solutions. Within larger deployments, Cisco IOS Firewall would play a complementary role to the other firewall platforms by providing firewalling services at the enterprise branch and for SIP trunk 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 C07-494658-00 09/08