

Security in SIP-Based Networks

This paper explores various network security threat models faced by today's Session Initiation Protocol (SIP)-based voice networks, and describes network security solutions based on Cisco SIP-enabled products.

SIP Security Overview

Cisco voice-over IP (VoIP) infrastructure solutions such as the Cisco Global Long Distance solution (see www.cisco.com/go/telephony) feature a voice-over-packet network design, using SIP to provide telephony services.

Figure 1
 SIP IP Telephony Network Components

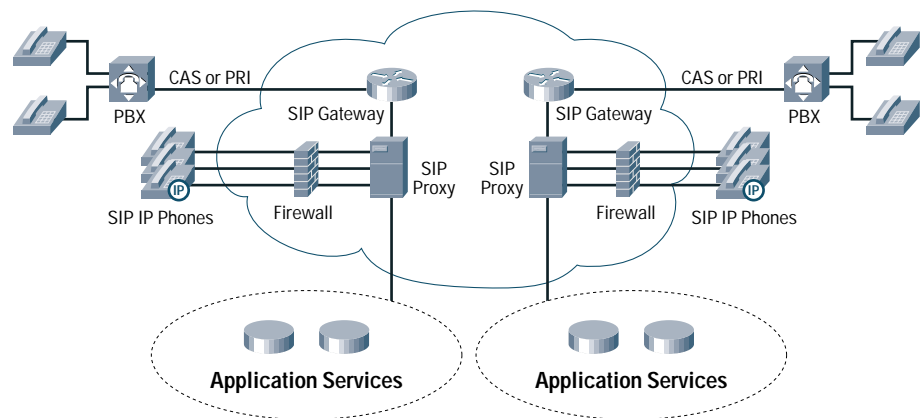


Figure 1 illustrates products that are used to implement SIP-based voice-over-packet networks. SIP-based solutions from Cisco include IP phones that support SIP (Cisco IP Phone 7960 and 7940), SIP-enabled gateways running Cisco IOS[®], Software (such as the Cisco AS5000 family of universal gateways and Cisco 1700, 2600, 3600, or 7200 series routers), a SIP proxy server (Cisco SIP Proxy Server), and a firewall (Cisco PIX[®] Firewall). These components work together to provide a SIP-based VoIP solution that can be integrated with existing telephony networks.

VoIP network security includes voice-packet security, which focuses on application issues, and IP security, which focuses on a network or transport problem. Securing a digitized bit stream is an example of a transport-level problem.

SIP deployments in a VoIP network are exposed to a wide range of network security threats and attacks. SIP may be deployed in relatively safe environments where the network equipment is trustworthy and physical security is agreeably sufficient, or into a potentially hostile Internet environment.

An Internet environment can be considered hostile for a number of reasons. Most important is that attacks are not traceable. There have never been enough safeguards and protection in an Internet environment for it to be considered safe, and the potential immunity to danger of devices communicating on the Internet make security threats commonplace.

There are two kinds of possible threats to a SIP-based network—external and internal. External threats are attacks launched by someone who is not participating in the message flow during a SIP-based call. External threats usually occur when the voice and signaling packets traverse untrustworthy boundaries, and may involve third-party networks when the call traffic is transferred from device to device, or participant to participant. Internal threats are much more complex because they are usually launched by a SIP call participant.

Because a SIP call participant launches internal attacks, the trust relationship is defied. Usually, endpoints within the enterprise are administratively controlled and secured behind firewall protection so they aren't expected to be capable of launching an attack. Once the trust relationship is defied and an endpoint acts hostile, it becomes very difficult to identify the source of the attack and to figure out the scope of the remedy.

Table 1 summarizes various threats including general network- and application-level security issues.

Table 1 Network Security Issues and Their Solutions

Issues	Solution
Denial-of-service (DoS) attacks: Prevention of access to a network service by bombarding SIP proxy servers or voice-gateway devices on the Internet with inauthentic packets	Configure devices to prevent such attacks
Eavesdropping: Unauthorized interception of voice packets or Real-Time Transport Protocol (RTP) media stream and decoding of signaling messages	Encrypt transmitted data using encryption mechanisms like Secure RTP.
Packet spoofing: Impersonation of a legitimate user transmitting data	Send address authentication (for example, endpoint IP addresses) between call participants.
Replay: The retransmission of a genuine message so that the device receiving the message reprocesses it	Encrypt and sequence messages; in SIP this is offered at the application-protocol level by using CSeq and Call-ID headers.
Message integrity: Ensuring that the message received is the same as the message that was sent	Authenticate messages by using HTTP Digest, an option supported on Cisco SIP-enabled phones and the Cisco SIP Proxy Server

SIP Security Mechanisms

The fundamental network-security services required for SIP are: preserving the confidentiality and integrity of messaging, preventing replay attacks or message spoofing, providing for the authentication and privacy of the participants in a session, and preventing DoS attacks.

SIP offers various security mechanisms for hop-by-hop and end-to-end encryption of certain sensitive header fields and the message body. Some of the mechanisms are built into the protocol, including different variations of HTTP authentication or secure attachments.

Transport- or network-layer security encrypts SIP signaling traffic, guaranteeing message confidentiality and integrity. IP security (IPSec) is a popular network-security mechanism that provides transport layer security. SIP RFC 2543 bis-09 further describes detailed security threats and mechanisms.

Authentication

During a call involving SIP user-agent clients, an attacker could masquerade as a user, forging the real identity of the client. Authentication provides a mechanism to verify that a user or client is legitimate.

In a SIP network, the authentication can take place between the user agent and the proxy, where the proxy server requires a user agent to authenticate itself before proceeding to process an “invite” message from it. Similarly, a user agent can request authentication of a proxy or redirect server.

SIP defines headers that are used for authentication. The *authorization* header contains a signature computed across components of the SIP message. This header does not change in transit between proxies and consists of: the nonce, the realm, the request method (the type of request message dispatched by a user-agent client), the request-method version, and the authorization type. There is also a *proxy-authorization* header, which is used by a SIP user agent to identify itself to a proxy. This contains the type of authentication, credentials of the user agent, or realm of the resource being requested.

Authorization

Once authentication is achieved, it must be determined whether that identity is authorized to use the services it is requesting. Despite being securely authenticated, a party may not have permission to use all or some of the services that are being requested, and may require further authorization.

IPSec

A framework of open standards, IPSec provides security functions, authentication, and encryption at the IP layer. Three protocols are used in IPSec implementation:

- *Encapsulating Security Payload (ESP) protocol*—A security protocol that provides data confidentiality and protection with optional authentication and replay-detection services. ESP completely encapsulates user data. ESP can be used either by itself or in conjunction with authentication header. For more information, refer to: [RFC 2406: IP Encapsulating Security Payload \(ESP\)](#).
- *Authentication Header (AH) protocol*—A protocol that can be used either by itself or with ESP, AH provides a packet authentication service. For more information, refer to: [RFC 2402](#).
- *Internet Key Exchange protocol*—A hybrid protocol that uses parts of Oakley and SKEME inside the Internet Security Association and Key Management Protocol (ISAKMP) framework, IKE is used to establish a shared security policy and authenticated keys for services (such as IPSec) that require keys. Before any IPSec traffic can be passed, each router, firewall, or host must be able to verify the identity of its peer. This can be done by manually entering preshared keys into both hosts, by a certification authority (CA) service, or via the forthcoming DNS secure (DNSSEC). This is the protocol formerly known as ISAKMP/Oakley, and is defined in: [RFC 2409: The Internet Key Exchange \(IKE\)](#).

IPSec creates secure tunnels through untrusted networks. Sites connected by these tunnels form virtual private networks (VPNs). Using IPSec or VPN prevents many attacks such as those described in Table 1.

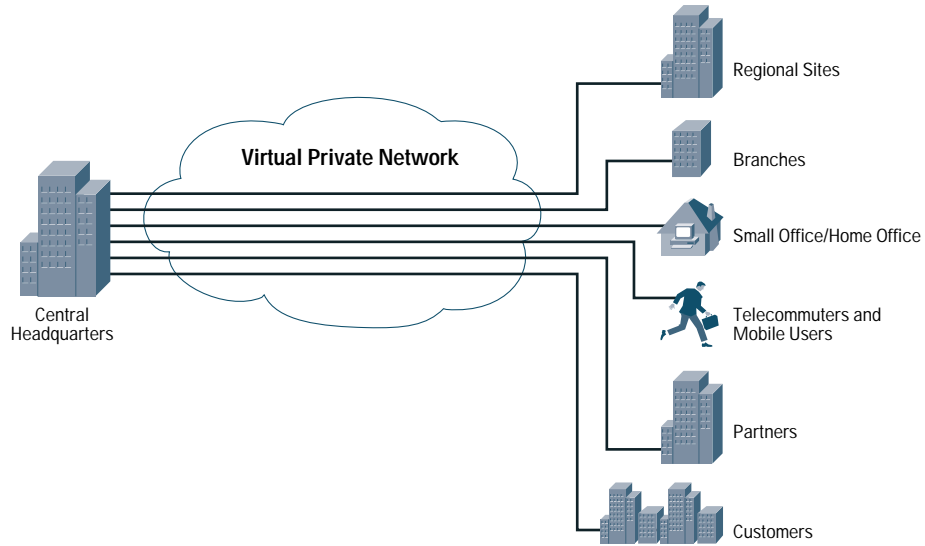
IPSec provides many options for performing network encryption and authentication. Each IPSec connection can provide encryption, integrity, and authenticity, or all three. When the security service is determined, the two communicating nodes must determine exactly which algorithms to use [for example, data-encryption standard (DES) or International Data Encryption Algorithm (IDEA) for encryption; Message Digest 5 (MD5) or Secure Hash Algorithm (SHA) for integrity]. After deciding on the algorithms, the two devices must share session keys. A security association (SA) is a relationship that is established between two VoIP entities.

Secure Voice and Video Enabled IPSec VPNs

In VPNs, VoIP traffic flowing across different network components on a shared network can be protected and secured as if it were on a private network. Cisco technology includes many robust security measures such as encrypting data, restricting access to authorized users, and tracking users once they are connected to the network.

VPNs are built around authentication and authorization capabilities, offering the users of the public VoIP network the privacy and authentication they would expect from a private network. A VPN tunnel is created as a logical, point-to-point connection in a connectionless VoIP network. An encrypted VPN tunnel provides network, data, and addressing privacy by scrambling data so that it is understood by the designated parties only. IPSec is a dominant standard in constructing VPNs. Figure 2 demonstrates VPN technology.

Figure 2
Virtual Private Network Technology



The following steps and diagrams (Figures 3 and 4) provide an overview of implementing a VPN for data, voice, and video using IPsec tunnels.

- Create generic routing encapsulation (GRE) tunnel endpoints.
- Establish security and authentication policies; define crypto maps.
- Associate crypto maps to GRE tunnels (encrypted voice traffic uses one of these tunnels, which terminates at a dedicated tunnel aggregation router).
- Identify and classify inbound voice (signaling and bearer) LAN traffic on access gateways.
- Use appropriate queuing strategies like Low Latency Queuing (LLQ) at the outbound WAN interface to assign higher priority to traffic across the voice tunnel.

Figure 3
Implementing a Multiservice VPN using IPsec Tunnels

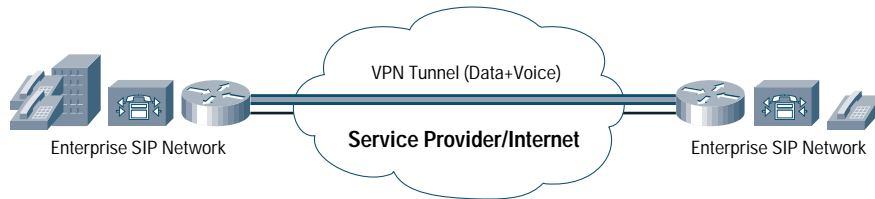
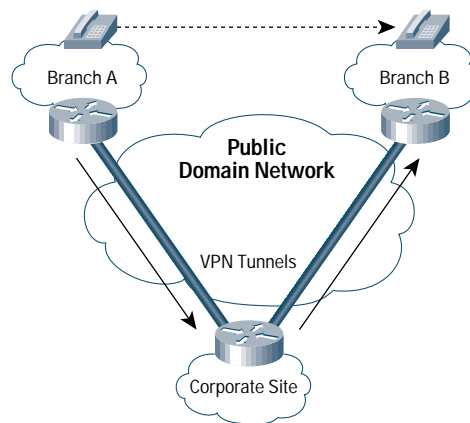


Figure 4
Public Domain Network



Firewalls

Endpoints such as SIP-based IP phones or other SIP-enabled devices in the enterprise private network that communicate with network components can be protected and secured by using firewalls. VoIP traffic can be routed to flow through policy-enforcement devices such as a firewall, where the traffic can be inspected before continuing.

A firewall is a part of a security policy in the VoIP network designed to safeguard the privacy of the enterprise or service-provider network. Firewalls allow administrators a single point of administration and control to police and filter traffic that keeps unauthorized users such as hackers or intruders from breaking in or leaving the protected network. Firewalls simplify security management—network security is consolidated on the firewall systems rather than having every SIP endpoint configured for security policies. A firewall also helps conserve precious IP addresses.

Since thousands of IPv4 addresses are registered each day and only a finite quantity of them are available to us, we are running out of public or globally recognizable Internet addresses. With this emerging space crisis in IP address domains, a firewall is a logical place to deploy Network Address Translation (NAT) to help alleviate this shortage. The Cisco PIX Firewall is implemented to serve both firewall and NAT functions.

Implementing Security Features on Cisco SIP-Enabled VoIP Products

Cisco SIP Proxy Server

The Cisco SIP Proxy Server supports authentication, authorization, and IPsec. A Cisco SIP Proxy Server can be configured to provide authentication either at an external RADIUS server or at the proxy itself. The proxy supports three types of authentication mechanisms in conjunction with the appropriate RADIUS server:

- Challenge Handshake Authentication Protocol (CHAP) Password Authentication
- HTTP Digest Authentication
- HTTP Basic Authentication

CHAP-Password Authentication depends upon a “secret” key known only to the authenticator and that peer. CHAP provides protection against playback attack by the peer through the use of an incrementally changing identifier and a variable challenge value. The use of repeated challenges is intended to limit the time of exposure to any single attack.

The proxy supports HTTP Digest Authentication and HTTP Basic Authentication. Both authentication mechanisms are performed as described in RFC 2617. RADIUS is an Internet Engineering Task Force (IETF) protocol that functions by exchanging attribute value pairs (AV pairs) between the client and the server. In conjunction with an external RADIUS server, CHAP-Password Authentication is supported. For example, a Cisco SIP Proxy Server acting as a RADIUS client exchanges AV pairs with a RADIUS server to provide authentication functions.

Using HTTP Digest Authentication, the password is never sent across the network in cleartext, but is always transmitted as an MD5 digest of the user's password. In this way, sniffing traffic on the network cannot identify the password.

For RADIUS-supported authentication, the SIP user-agent client (UAC) password is stored at the RADIUS server. For proxy-supported authentication, the UAC password is stored in a subscriber table in a MySQL database.

Authentication

The default authentication scheme is the HTTP Digest Authentication performed at the Cisco SIP Proxy Server. Though the Cisco SIP Proxy Server supports HTTP Basic Authentication, it is not recommended as a secure authentication mechanism. The authentication mechanisms performed at the proxy use the user name as found in the authorization header or the proxy-authorization header as the key to query the MySQL database.

If the RADIUS server is used to perform authentication, the user name is passed as one of the AV pairs from the Cisco SIP Proxy Server to the RADIUS server, where it can be used to key the user search before performing authentication.

Authorization

A user that has been authenticated is automatically authorized; there is no additional authorization step performed at the Cisco SIP Proxy Server.

Access Lists

The Cisco SIP Proxy Server Access Control directive in the configuration file determines access to the server. Access can be granted or denied based on a variety of criteria. The Allow and Deny directives in the Cisco SIP Proxy Server configuration file allow or deny access to the server based on host name or host address of the client.

- *Allow*—Determines which hosts can access an area of the server. Access can be controlled by hostname, IP address, IP address range, or by other characteristics of the client request captured in environment variables.
- The first argument to this directive is always the “from” hostname. The subsequent arguments can take two different forms (“all” and “host”). If “Allow from all” is specified, all hosts are allowed access. This is subject to the configuration of the Deny and Order directives (see below). To allow only particular hosts or groups of hosts to access the server, the host can be specified in any of the following formats:
 - A (partial) domain name
Example: Allow from company.com
In this example, hosts whose names match or end in this string are allowed access.
 - A full IP address
Example: Allow from 10.1.2.3
In this example, an IP address of a host is allowed access.
 - A partial IP address
Example: Allow from 10.1
This example shows the first 1 to 3 bytes of an IP address for subnet restriction.
 - A network/netmask pair
Example: Allow from 10.1.0.0/255.255.0.0
This example shows a network a.b.c.d, and a netmask w.x.y.z. for finer subnet restriction.
 - A network/nnn Classless Inter-Domain routing (CIDR) specification
Example: Allow from 10.1.0.0/16
This example is the same as the previous example, except the netmask consists of nnn high-order 1 bits.
- *Deny*—Allows access to the server with restrictions based on hostname, IP address, or environment variables. The arguments for the Deny directive are identical to the arguments for the Allow directive.

- *Satisfy*—Determines access policy for both types of access control (Allow and Deny) and authentication checks. The parameter can be either “all” or “any.” If “all” is specified, the sending host should be “allowed” and authenticated. If “any” is specified, the sending host can be granted access if it passes either the access control “allow” or authentication check. In either case, the authentication module must be turned on.
- *Order*—Controls the default access state and the order in which Allow and Deny directives are evaluated. Valid orders are:
 - Deny, Allow—The Deny directives are evaluated before the Allow directives. Access is allowed by default. Any client that does not match a Deny directive or does match an Allow directive will be allowed access to the server.
 - Allow, Deny—The Allow directives are evaluated before the Deny directives. Access is denied by default. Any client that does not match an Allow directive or does match a Deny directive will be denied access to the server.
 - Mutual-failure—Only hosts that appear on the Allow list and do not appear on the Deny list are granted access. This ordering has the same effect as the Allow, Deny order. The Allow, Deny configuration is recommended over the Mutual-failure configuration.

In the following example, all hosts in the company.com domain are allowed access, and all other hosts are denied access.

```
Order Deny, Allow
Deny from all
Allow from company.com
```

In the following example, all hosts in the company.com domain are allowed access, except for the hosts in the foo.company.com subdomain, who are denied access. All hosts not in the company.com domain are denied access because the default state is to deny access to the server.

```
Order Allow, Deny
Allow from company.com
Deny from foo.company.com
```

If the order in the last example is changed to “Deny, Allow,” all hosts will be allowed access. Regardless of the ordering of the directives in the configuration file, the “Allow from company.com” will be evaluated last and will override the “Deny from foo.company.com.” All hosts not in the company.com domain will also be allowed access because the default state will change to “Allow.”

IP Security

For transmission of sensitive information (VoIP traffic, for example) over unprotected or untrusted networks, IPSec acts as a network-layer security protocol that protects and authenticates IP packets exchanged between IPSec devices or peers (such as between a Cisco SIP Proxy Server and a UAC or another SIP proxy server).

IPSec offers two methods of key management for setting up security association between IPSec peer devices:

- *Manual keying*—The keys are manually installed or configured by the administrator. Manual keying is vulnerable to attacks where an attacker gains control of the proxy server or the gateway, can read the security configuration file, and can get access to the keys that are used in the traffic exchange.
- *Automatic keying*—In automatic keying, the keys are negotiated between devices that form a security association using IKE protocol. Security associations are automatically reconfigured and replenished periodically. Automatic keying is considerably more secure than manual keying. Automatic keys can be changed every few hours or even every few minutes without breaking the connection or requiring administrator intervention.

All IPSec combinations have been successfully tested and proven to secure traffic to and from the Cisco SIP Proxy Server on the following platforms:

- Solaris 8 Operating Environment (using manual key management method)
- RedHat Linux 6.2 (Kernel 2.2.14-5.0) with Linux Freeswan release 1.5 (using manual and IKE key management method)

IPSec in Cisco VoIP Gateways

The version of IPSec in Cisco VoIP gateways uses Cisco IOS Software that provides industry-leading capabilities while being fully interoperable with a wide range of devices from other vendors. Through the auspices of the Automotive Network Exchange (ANX), Cisco has demonstrated the interoperability of the IPSec feature in Cisco IOS Software. The IPSec feature offers the following advanced features:

- *Embedded solution*—Through a software-only upgrade, this does not require any modifications to the network, hosts, or applications.
- *Digital certificate support*—Cisco and VeriSign have developed the Certificate Enrollment Protocol (CEP), a protocol for communicating with certificate authorities. Several vendors, including VeriSign and Entrust Technologies, will support Cisco CEP and be interoperable with Cisco devices.
- *Flexible security policy*—Extended access lists are used to selectively encrypt or authenticate datagrams. IP packets can be selected by any combination of source or destination addresses, Layer 4 protocols, and ports. Each encrypted stream can be separately authenticated and encrypted. For example, if Alice is sending Web, e-mail, and Telnet traffic to Bob, Alice's router may encrypt the Web traffic with one key, the Telnet traffic with another key, and simply pass the e-mail traffic without encryption.
- *Part of a complete security solution*—Cisco IOS Software provides many security features in its Cisco Secure Integrated Software; authentication, authorization, and accounting (AAA); route authentication; and Kerberos Protocol.

IPSec in Cisco IOS Software supports the following standards:

- Current RFCs and Internet drafts for IPSec and IKE:
 - ESP is per RFC 2406
 - AH is per RFC 2402
 - IKE is per RFC 2409
 - Entire IPSec implementation is per RFC 2401 (Security Architecture for the Internet Protocol)
- IPSec and IKE DoS encryption algorithms, including:
 - DES-CBC as per RFC 2405
 - 3DES-CBC as per RFC 2451
 - 40-bit DES-CBC
 - DES-CBC with Derived IV as specified in RFC 1829
- Authentication algorithms:
 - HMAC-MD5 as per RFC 2403
 - HMAC-SHA as per RFC 2404
 - Keyed MD5 as per RFC 1828
- Remote access functionality:
 - Private address allocation as per draft-ietf-ipsec-isakmp-mode-cfg-04.txt
 - Legacy authentication as per draft-ietf-ipsec-isakmp-xauth-04.tx

Access Control Lists—Cisco gateways support configuring access control lists (ACLs) using standard Cisco IOS Software commands. ACLs should be used to provide a firewall type of security on the voice gateway to control the VoIP traffic in and out of the network.

Standard- and static-extended ACLs provide basic traffic filtering capabilities. Users set criteria that describe which packets should be forwarded and which packets should be dropped at an interface, based on each packet's network-layer information. For example, all User Datagram Protocol (UDP) packets from a specific source IP address or address range can be blocked. Some extended ACLs can also examine transport-layer information to determine whether to block or forward packets.

To define a standard IP ACL using numbers, the global “access-list” command is used. The ACLs default to an implicit “Deny” statement for blocking all traffic through it.

Cisco PIX Firewalls

Cisco PIX Firewalls provide full firewall protection that conceals the architecture of an internal network from the outside world. Cisco PIX Firewalls allow secure access to the Internet from within existing private networks, and the ability to expand and reconfigure TCP/IP networks without being concerned about a shortage of IP addresses.

With Cisco PIX Firewalls, users can take advantage of larger address classes than those they may have been assigned by the Internet’s Network Information Center (NIC). Cisco PIX Firewalls provide this access through its NAT facility, described by RFC 1631. Cisco PIX Firewall versions 6.0 and 6.1 offer SIP support that solves NAT traversal issues by acting as an application-layer gateway (ALG).

Cisco PIX Firewalls dynamically open and close UDP ports for secure SIP traffic to flow through. Other vendors must open a large range of UDP ports, which creates a security risk

Cisco PIX Firewall Features

Cisco Secure PIX Firewalls have the following features:

- Firewall capability that keeps intruders out of your internal network, while permitting regulated conduit access through the firewall for services such as electronic mail, Telnet, FTP, SNMP, and HTTP use.
- NAT services that allow a site to share one or more NIC-registered IP addresses among many users.
- An identity feature that allows NIC-registered IP addresses to pass through the firewall without address translation, while still retaining adaptive security.
- Better performance than competing firewalls. Cisco PIX Firewalls gain speed through a patent-pending process called Cut-Through proxies—the fastest way for a firewall to authenticate a user. Unlike a proxy server that must analyze every packet at LAYER 7 of the OSI model (a time- and process-intensive function), Cisco PIX Firewalls first query a TACACS+ or RADIUS server for authentication. Once approved, Cisco PIX Firewalls establish a data flow, and all subsequent traffic flows directly and quickly between the two parties. This Cut-Through capability allows Cisco PIX Firewalls to perform dramatically faster than proxy-based servers while maintaining a session state.
- Support for SNMP MIB-II gets and traps.
- Simplified configuration and system management with an HTML interface.
- Support for Telnet, FTP, and HTTP access using RADIUS and TACACS+ security systems. Cisco PIX Firewalls authenticate users in conjunction with the security systems that Cisco routers support. The security clients run on Cisco routers and send authentication requests to a central security server, which contains all user authentication and network service access information.
- Failover capability that permits a secondary Cisco PIX Firewall unit to take over firewall communications if the primary unit fails.
- Support for 10BASE-T and 100BASE-TX networking.
- SIP-aware ALG functionality.

SIP-Configuration Guidelines for Cisco PIX Firewalls

When using Cisco PIX Firewalls with SIP, be aware of the following:

- If a firewall proxy is placed outside the firewall in the demilitarized zone (DMZ) network with Record-Route enabled, the list of allowed IP addresses from the outside Cisco SIP Proxy Server’s IP address should be small, thus allowing for manageable security.
- Outside callers cannot make calls to end points inside the firewall unless they have been defined as an allowed device.

Cisco SIP-Enabled IP Phones

The best way to secure Cisco SIP-enabled IP phones is to put them on private, non-Internet-addressable addresses and to make sure there is good perimeter security for the LAN through the use of firewalls and intrusion detection systems, such as Cisco Intrusion Detection System Sensors (Cisco IDS). Cisco IDS Sensors monitor for attacks by examining packet flows for 'signatures' and generating alarms when attacks occur. A Cisco IDS Sensor should typically be placed in front of a Cisco PIX Firewall.

It is recommended that the IP phones and Cisco SIP Proxy Server be configured to use port 5060 for signaling and for phones and gateways to be configured to use a specific port range for media, and for all of these ports to be secured. Table 2 presents security concerns in administrating Cisco SIP-enabled IP phones.

Table 2 Network Security Issues in Cisco SIP-Enabled IP Phones

Security Concerns	Solutions
Trivial File Transfer Protocol (TFTP) eavesdropping: SIP phones make TFTP requests to download configuration files and firmware images. TFTP is inherently insecure since files are sent unencrypted.	Make FTP requests through Cisco PIX Firewalls using a TFTP server that is firewall protected.
Dynamic Host Configuration Protocol (DHCP) spoofing: SIP phones make DHCP requests to get an IP address, gateway, boot server, and so on.	Secure DHCP servers protected behind Cisco PIX Firewall. Static IP phone addressing is secure.
Unencrypted RTP media stream	Secure IPSec VPN tunneling.
Telnet	Disable Telnet in the phone configuration file or only allow this privilege on network admin workstations.
Authentication and authorization	HTTP Digest between phones and Cisco SIP Proxy Server. Cisco SIP IP phones can also authenticate methods such as INVITE, BYE, and CANCEL.

Conclusion

SIP-enabled products from Cisco offer a variety of industry-standard security mechanisms to help build a robust and secure SIP-based voice network. For more information about deploying SIP networks over a Cisco infrastructure, visit <http://www.cisco.com/go/telephony>.

CISCO SYSTEMS



Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems Europe
11 Rue Camille Desmoulins
92782 Issy-les-Moulineaux
Cedex 9
France
www-europe.cisco.com
Tel: 33 1 58 04 60 00
Fax: 33 1 58 04 61 00

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapore 068912
www.cisco.com
Tel: +65 317 7777
Fax: +65 317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the
Cisco Web site at www.cisco.com/go/offices

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia
Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland
Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland
Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden
Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe