

Cisco IOS Firewall

Networks are exposed to an increasingly hostile environment when connected to the public Internet and private WAN. This can introduce security breaches, malware outbreaks, and unwanted application traffic, which can result in lost revenues, productivity, and damage to corporate reputation.

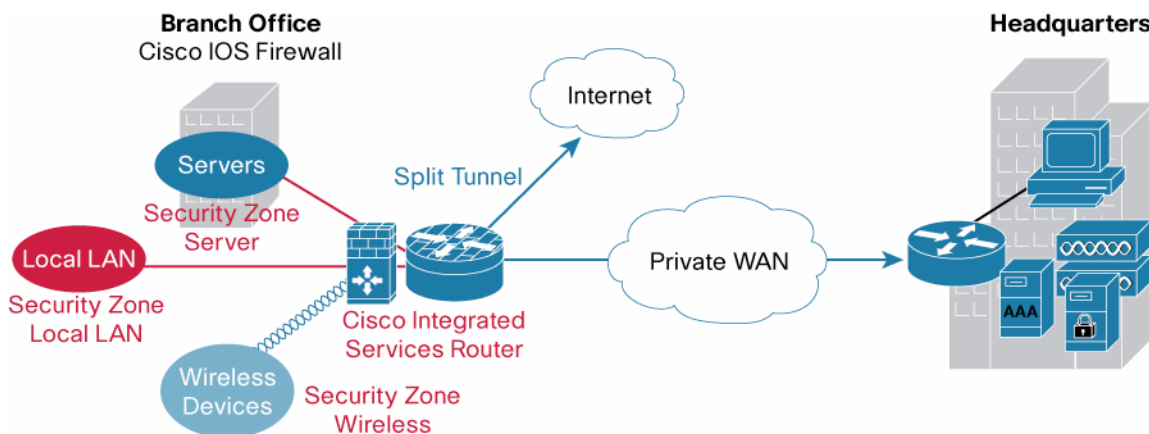
Today there is increased pressure to comply with industry regulations as well as state and federal regulations, created to enhance privacy, national security, and in many cases corporate accountability. Examples of these regulations include the Payment Card Industries (PCI) Data Security Standard, which affects all vendors who receive, store, or transmit cardholder data. In the United States, other examples include the Health Insurance Portability and Accountability Act (HIPAA) in the healthcare industry, the Gramm Leach Bliley Act (GLBA) in the financial services industry, and the Sarbanes-Oxley Act in the accounting field. The European Union's privacy legislation, called the Directive on Data Protection, requires that transfers of personal data to non-EU countries take place with only those organizations that provide acceptable levels of privacy protection. Fines, penalties, and lawsuits are just some of what a company might undergo if a security breach occurs and the company is out of compliance.

Cisco IOS® Firewall offers the threat defense required for today's changing threat environment. With more dangerous targeted attacks and the growth of the mobile workforce, the perception of network borders and where the office starts and stops has changed significantly to anywhere there is connectivity.

Deployed extensively at branch locations and home offices, Cisco IOS Firewall provides broad security coverage with deployment flexibility and the cost benefits that are fundamental to an integrated security approach (Figure 1).

It is the simple-to-use, certified, cost-effective firewall solution.

Figure 1. Typical Cisco IOS Firewall Deployment



Cisco IOS Firewall runs on the Cisco® integrated services router at the branch office and head office, protecting branch office resources and segmenting the network with security zone policies.

Cisco IOS Firewall Features and Benefits

The Cisco IOS Firewall is Common Criteria EAL4 certified and provides the following benefits:

- **Application protection:** Block unwanted applications such as instant messaging traffic, peer-to-peer file-sharing traffic, and HTTP-tunneling applications to reduce bandwidth usage and increase employee productivity.
- **Network border enforcement:** Recommended at all network entry points, secure the “front line,” and prevent illegal access to sensitive resources.
- **Unmatched return on investment:** Perform routing, perimeter security, intrusion detection, VPN functionality, and per-user authentication and authorization on your router while addressing regulatory compliance.
- **Easy provisioning and management:** Enable rapid deployment of Cisco Technical Assistance Center (TAC)-approved firewall policies, monitor firewall activity, and dynamically configure mitigation policies with Cisco Configuration Professional, the Unified Firewall MIB, and Cisco Security Manager.

Table 1 describes Cisco IOS Firewall features.

Table 1. Feature and Benefits

Feature	Benefit
Network zone segmentation PCI Requirement 3: Protect stored cardholder data	Precise zone segmentation capabilities facilitate deploying security for internal, external and DMZ subgroups on the network to prevent unauthorized access.
Management options and flexibility	Enable management access from Cisco Configuration Professional, Cisco Security Manager, Unified Firewall MIB, and audit trail and logging.
Application traffic rate and session control	Policy-map policing applies rate limits to firewall policies to control network bandwidth usage. Session policing limits connection rates to network hosts and helps protect against denial-of-service (DoS) attacks.
High availability*	Stateful Failover provides for active and standby failover between two routers for most TCP-based services. Firewall session state is maintained such that active sessions continue even during a router or circuit failure.
Virtual (VRF-aware) firewall	VRF-aware firewall functions offer virtual firewalls for isolated route space and overlapping addresses.
Authentication proxy PCI Requirement 10: Track and monitor all access to network resources and cardholder data	Network administrators can authenticate and authorize each user's access to network resources with Cisco IOS Firewall Authentication Proxy using HTTP, Telnet, FTP, and HTTPS interfaces.
Transparent firewall	A transparent firewall facilitates insertion of a stateful Layer 2 firewall within an existing network, without readdressing statically defined devices. It provides the same Layer 3-7 filtering as "routed" mode, but offers the simplicity of bump-in-the-wire deployment.
Policy-map policing and session control	Policy-map policing applies rate limits to firewall policies to control network bandwidth usage. Session policing limits connection rates to network hosts and helps protect against DoS attacks.
Instant messenger blocking	Instant messenger blocking offers per-service control to block or allow MSN Messenger, Yahoo! Messenger, Windows Messenger and AOL Instant Messenger. It allows service restriction to text-chat only, blocking voice and video chat, and file transfer.
Peer-to-peer control	Peer-to-peer control individually blocks access to BitTorrent, Gnutella, KaZaA, and eDonkey file-sharing networks. Service-specific improvements were introduced in Cisco IOS Software Release 12.4(9)T to limit certain activities supported by certain peer-to-peer networks.
Protocol conformance checking	This feature enforces protocol conformance for HTTP, Simple Mail Transfer Protocol (SMTP), Extended SMTP (ESMTP), Internet Mail Access Protocol (IMAP), and Post Office Protocol 3 (POP3). It facilitates detection and prevention of unwanted traffic on desired application service ports. HTTP inspection offers Java applet filtering to block malicious content in HTTP traffic. Cisco IOS Software Release 12.4(9)T introduced capabilities to configure regular expression matching for policy enforcement, as well as a granular application inspection and control of various HTTP objects, such as HTTP methods, URLs and URIs, and header names; and values such as maximum URI length, maximum header length, maximum number of headers, maximum header-line length, non-ASCII headers, or duplicate header fields. This feature allows you to limit buffer overflows, HTTP header vulnerabilities, binary or non-ASCII character injections, and exploits such as Structured Query Language (SQL) injection, cross-site scripting, and worm attacks.

Feature	Benefit
Integrates with Cisco IOS Software Intrusion Prevention System (IPS) PCI Requirement 6: Develop and maintain secure systems and applications	Prevent application level attacks from flooding the network.
Integrates with Cisco IOS Software Content Filtering	Controls and blocks access to malicious and inappropriate websites.

* Current support for the Cisco 1841 Integrated Services Router, Cisco 2800 and 3800 Series Integrated Services Routers, Cisco 3700 Series Multiservice Access Routers, Cisco 7200 Series Routers, and the Cisco 7301 Router.

* Only on Classic IOS Firewall, not Zone Based Policy Firewall.

Beyond Data Threats: Securing Unified Communications

Voice and video are also targets of security attacks. Concerns such as toll fraud remain the same in the unified communications environment as in traditional telephone networks. Today's organizations also face increased regulatory requirements for conversation privacy, message confidentiality, and user and device authentication. Therefore, unified communications strategies must address the security aspects of Sarbanes-Oxley, GLB, HIPAA, PCI Data Security Standard, European Basel II, and other mandates affecting global organizations directly within the unified communications architecture. Integrating security within the underlying infrastructure also thwarts DoS attacks, worms, and other malicious activity that are usually aimed at the data network, but, when successful, have ramifications for the voice network, too.

Taking a comprehensive, systemic approach, incorporating all unified communications layers, means looking at applications, endpoints, call control, and the network infrastructure. Especially at branch offices, securing unified communications is easy to address because Cisco integrated services routers can incorporate voice as well as security functions, all in the same device. Table 2 describes specific support for securing unified communications.

Table 2. Features for Securing Unified Communications

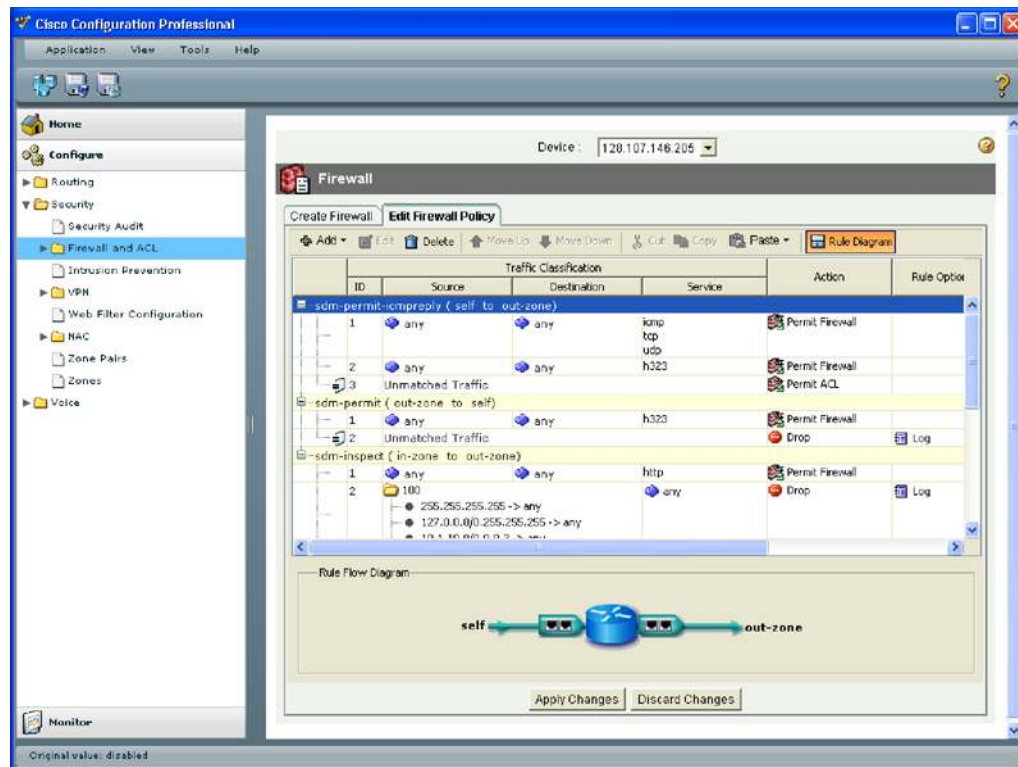
Feature	Benefit
Session Initiation Protocol (SIP) application layer gateway (ALG) Inspection	SIP ALG inspection provides the ability to prevent unauthorized calls, call hijacking, and other SIP exploits and related DoS attacks. This protection helps ensure protocol conformance and application security, giving more granular control over what policies and security checks to apply to SIP traffic and what messages or users to filter out.
Voice protocol and media streams inspection support	Cisco IOS Firewall configured with Cisco Communications Manager Express offers granular local inspection support for all voice protocols such as skinny local inspection (Skinny Client Control Protocol [SCCP]), which requires Cisco IOS Software Release 12.4(20)T and higher. Cisco IOS Firewall also supports inspection for media streams such as MS NetMeeting, RealMedia, and MS Netshow.
H.323v3 and v4 support	Cisco IOS Firewall supports H.323v3 and v4 such as Annex E, Annex G, and Annex D; it also supports fax and call transfer.
Instant messaging voice control support	Cisco IOS Firewall supports permit, deny, and alert policies and logging operations within instant messaging, including general text chat, SIP Live Communication Server support, and other services such as file transfers and attachments, white boarding, application sharing, games, video and audio conferencing, URLs, advertisements, tickers, and pop-ups.
Trusted firewall control	Trusted firewall control builds intelligence into the firewall so that it can open a pinhole (a port that is opened through a firewall to allow a particular application access to the protected network) dynamically when it receives a Simple Traversal of User Datagram (STUN) Protocol request for a media flow. This request is authenticated/authorized by the firewall to make sure that it opens pinholes only for genuine calls.

Cisco IOS Firewall Management

Cisco Configuration Professional

Cisco Configuration Professional is a GUI device management tool for Cisco integrated services routers and Cisco 7200 Series and 7301 Routers running Cisco IOS Software. It offers smart wizards and advanced configuration support for LAN and WAN interfaces, Network Address Translation (NAT), and stateful and application firewall policy. The firewall wizard allows a single-step deployment of high, medium, or low firewall policy settings. Cisco Configuration Professional also offers a one-click router lockdown and an innovative security auditing capability to check and recommend changes to router configuration based on Cisco TAC recommendations. Figures 2 and 3 provide examples of the UI.

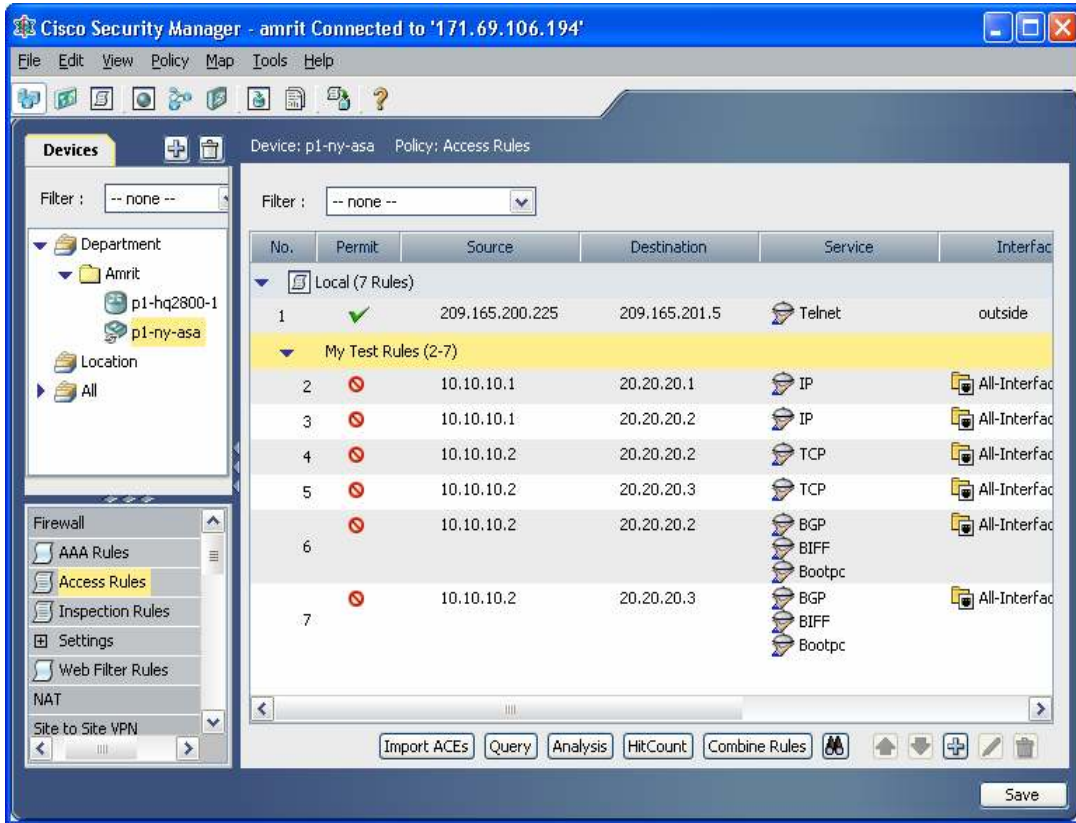
Figure 2. Defining Firewall Policies with Cisco Configuration Professional GUI



Cisco Security Manager

Cisco Security Manager is an enterprise-class management application that is Cisco device-independent designed to configure firewall, VPN, and IPS security services on Cisco network and security devices. It's a unified interface for managing firewall rules across different Cisco devices supporting the Cisco Firewall family of products, with its flexible rule specification methods for improved productivity and organization of rules; powerful toolset to identify configuration errors and optimize firewall rules.

Figure 3. Defining Firewall Policies with Cisco Security Manager GUI



Cisco IOS Firewall product specifications are described in Tables 3 through 11. Tests were completed using Cisco IOS Software Releases 12.4(15)T6 and *12.4(22)T1

Table 3. Performance and Capacity

Platforms	Cisco IOS Software Release Tested	Traffic Load	Throughput
3845	12.4(15)T6	6700 connections/sec	729 Mbps*
		176000 connections	
3825	12.4(15)T6	3800 connections/sec	564 Mbps*
		146000 connections	
2851	12.4(15)T6	2000 connections/sec	452 Mbps*
		98000 connections/sec	
2821	12.4(15)T6	1500 connections/sec	352 Mbps*
		94000 connections	
1861*	12.4(22)T1	710 connections/sec	90 Mbps*
		75000 connections	

*Max throughput with 64K HTTP object size with stateful HTTP traffic.

Table 4. Firewall Services Support

User group firewall support
Intra-zone firewall support
Stateful inspection engine
Secure network posture by default
Packet tracer for debugging*
Packet capture capabilities for packet sniffing*
Independent inspection parameters on a per-flow basis
VRF/VLAN aware NAT
Bidirectional NAT
Policy NAT
VPN NAT transparency
Ability to capture drops
Stateless SYN flood protection
TCP session timeout (specify configurable options)
UDP session timeout (specify configurable options)

*Cisco IOS Software 12.4(20)T or later release is required.

Table 5. Access Control Support

Inbound access control lists (ACLs)
Outbound ACLs
Layer 2 (transparent mode) ACLs
Time of day based policies
ACL editing (insert/delete individual rules in existing ACL)
Able to add comments to ACLs
Object grouping support for simplified firewall policy definition*
Ability to match on "no type" with service object group
Time-based ACLs
Add/remove ACL entry by ACL entry line number
Ability to rename an ACL
Enabling/disabling of ACL entries

*Cisco IOS Software 12.4(20)T or later release is required.

Table 6. Table 6 Routing Network Integration Support

Security contexts (virtual firewalls)
Transparent firewall (Layer 2 transparent firewall)
Mixed mode (L2/L3 firewall on same box)
Static route
Open Shortest Path First (OSPF) routing
RIP routing
EIGRP routing
IS-IS routing (multiple contexts)
BGP routing (multiple contexts)
Multicast sparse-dense mode
Multicast PIM bidir mode
Multicast PIM sparse mode

Static multicast route (mroute)
QoS (traffic shaping)

Table 7. Advanced Inspection Services Support

HTTP
Port 80 Misuse prevention: HTTP tunnel prevention
RFC compliance checking for protocol anomaly detection
HTTP command filtering: filter any HTTP command
MIME type filtering
Regex filtering on HTTP messages
SMTP/ESMTP Control
RFC compliance checking for protocol anomaly detection*
Permit/deny/log or rate limit email messages based on sender*
Permit/deny/log or rate limit email messages based on recipient*
Permit/deny/log or rate limit email messages based on attachment file names/extensions*
Permit/deny/log or rate limit email messages based on content within headers or bodies of messages*
Combat spam by denying/rate-limit/log email messages with a large number of recipients or an excessive number of invalid email addresses*
Combat spam by controlling usage of email relays*
IM and p2p Control
Filtering Windows Messenger instant messaging
Filtering AIM instant messaging
Filtering Yahoo instant messaging
Filtering MSN instant messaging
Filtering Kazaa peer-to-peer services
Filtering Gnutella peer-to-peer services
Permit/deny/log file transfers
Permit/deny/log video conferencing
Permit/deny/log voice chat
Control direction services can be initiated
Content/URL Filtering
Support for multiple URL filtering servers (primary/backup)
Long URL filtering (greater than ~1024 bytes)
HTTP server response buffering
URL auditing (admin see URLs user are attempting to access)
Local URL filtering exception policy (based on IP address/local policy)
Java blocking
Antispyware
Antispam
Antiphishing
Automatic updates

* Cisco IOS Software 12.4(20)T or later release is required.

Table 8. Unified Communications Support

Session Initiation Protocol (SIP)
RFC 3262 (PRACK)*
RFC 3265 (SUBSCRIBE/NOTIFY)*
RFC 3311 (UPDATE)*
RFC 3515 (REFER)*
RFC 3428 (MESSAGE)*
RTP and RTCP connection inspection*
Rate-limiting*
PAT with SIP*
Enforcement of mandatory header fields (From, To, Call-Id, CSeq, Via, Max-Forwards) presence and validity*
Enforcement of forbidden header fields*
Enforcement of SIP dialog and SIP transaction*
Check URL in Header fields against permit/deny list of callers/callee*
Check Max-Forwards header field; action on Max-Forwards =0 configurable by user*
Recognition of non-SIP packet on SIP signaling port*
Permit/deny third -arty registrations/deregistrations and if permit, ability to specify users allowed to do that*
Protection against buffer overflows*
Protection against DDOS attacks*
User configurable allowable SIP commands/extensions*
Skinny Client Control Protocol Control (SCCP)
Translation of embedded IP addresses and ports*
Dynamic pinholing*
Protocol conformance*
Configurable timeouts for skinny signaling and media channel*
H.323 Control
H.323 (v1 and v2) (NAT/PAT) *
H.323 (v3 and v4) (NAT/PAT) *
H.225: RAS*
H.323: direct call signaling*
H.323: T.38 (fax over IP) *

* Cisco IOS Software 12.4(20)T or later release is required.

Table 9. Table 9 Monitoring and Management Support

SSHv2
SNMPv3*
Cisco Configuration Professional
Cisco Security Manager*
Netflow
Class-map (MPF) for management traffic

* Supported on Classic Cisco IOS Firewall only.

Table 10. Table 10 IPv6 Support

IPv6 inspection, access control, and management*
IPv6 Firewall*

* Supported on Classic Cisco IOS Firewall only.

Table 11. Table 11 Platform Support

Product	Platforms Supported
Cisco 800 Series Routers	Cisco 831*, 836*, 837*, 851, 857, 860, 871, 876, 877, 878, 881, and 888
Cisco 1700* Series Modular Access Routers	Cisco 1701, 1702, 1711, 1712, 1721, 1751, 1751-V, and 1760
Cisco 1800 Series Integrated Services Routers	Cisco 1801, 1802,1803,1811,1812, 1841 and 1861
Cisco 1900 Series Integrated Services Routers	Cisco 1941 and 1941W
Cisco 2600* Series Multiservice Platforms	Cisco 2610XM, 2611XM, 2620XM, 2621XM, 2650XM, 2651XM, and 2691
Cisco 2800 Series Integrated Services Routers	Cisco 2801, 2811, 2821, and 2851
Cisco 2900 Series Integrated Services Routers	Cisco 2901, 2911, 2921, and 2951
Cisco 3600* Series Multiservice Platforms	Cisco 3660
Cisco 3700* Series Multiservice Access Routers	Cisco 3725 and 3745
Cisco 3800 Series Integrated Services Routers	Cisco 3825 and 3845
Cisco 3900 Series Integrated Service Routers	Cisco 3925 and 3945
Cisco 7200 Series Routers	Cisco 7201, 7204VXR, and 7206VXR
Cisco 7300 Series Routers	Cisco 7301
Cisco ASR 1000 Series Aggregation Services Routers	Cisco ASR 1002, 1004, and 1006

*End-of-life router platforms.

Cisco and Partner Services for the Branch

Services from Cisco and our certified partners can help you transform the branch experience and accelerate business innovation and growth in the Borderless Network. We have the depth and breadth of expertise to create a clear, replicable, optimized branch footprint across technologies. Planning and design services align technology with business goals and can increase the accuracy, speed, and efficiency of deployment. Technical services help improve operational efficiency, save money, and mitigate risk. Optimization services are designed to continuously improve performance and help your team succeed with new technologies.

Additional Resources

For more information about Cisco IOS Firewall and other router security technologies, visit the following webpages:

- Cisco IOS Firewall: www.cisco.com/go/iosfirewall
- Cisco IOS Software IPS: www.cisco.com/go/iosips
- Cisco IOS content filtering: www.cisco.com/go/ioscontentfiltering
- Cisco Configuration Professional: www.cisco.com/go/ccp
- Cisco Router and Security Device Manager: www.cisco.com/go/sdm
- Cisco Integrated Services Routers: www.cisco.com/go/isr
- Cisco information on how to be PCI compliant: www.cisco.com/go/pci



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.

CCDE, CCSI, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Stackpower, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCI, CCNA, CCNP, CCSP, CCVP, 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, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, 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. (0903R)