Cisco Services for Intrusion Prevention Systems Customer Q&A

Contents

Introduction to Cisco Services for IPS

Q. What is an intrusion prevention system (IPS)?

A. IPS is a technology used to detect and prevent suspected malicious network traffic or behavior. Cisco® IPS devices are installed at critical points in the network to perform real-time analysis of network traffic. Cisco IPS devices include IPS appliances (IPS42xx), ASA 5500-AIP series with IPS modules, routers or Cisco Catalyst® switches with IPS modules, and routers with Cisco IOS® Software–based IPS. For more information, visit www.cisco.com/go/ips.

Q. What are Cisco Services for IPS?

A. Cisco Services for IPS provide essential, ongoing support for Cisco IPS devices, including:

- Keeping your Cisco IPS devices current on the latest threats so that malicious traffic is accurately identified, classified, and stopped in real time. This includes delivering signature updates on the latest threats and providing global correlation threat updates from Cisco Security Intelligence Operations (SIO). Cisco SIO is the world's largest threat monitoring network and includes a 500-person team of security engineers and analysts who monitor security traffic and rapidly respond to new threats through multiple remediation techniques. Cisco SIO uses a broad set of sources and methods to make sure that the protection updates provided by Cisco are timely, accurate, and effective.
- Providing ongoing hardware support and operating system updates and around-the-clock global access to the Cisco Technical Assistance Center (TAC).

Q. Why do I need Cisco Services for IPS?

A. Unwanted network intrusions are not static events, and new threats constantly emerge. Without IPS signature and global correlation updates, network protection quickly degrades, and your business becomes increasingly vulnerable. Just like the antivirus software on your desktop, you need the most recent virus signatures for the software to protect you from the latest virus. Cisco Services for IPS include:

- Proactive delivery or access to the signature library and new signature updates for each registered Cisco IPS solution
- Cisco global correlation and reputation updates delivered to enabled IPS devices throughout the day, usually every five minutes
- Access to Cisco IntelliShield search access for detailed research on the latest threats and vulnerabilities correlated with IPS signatures for each Cisco IPS solution
- Notification of availability of updated signatures (requires subscription to the Cisco Threat Defense Bulletin)
- Updates and version upgrades on licensed operating system software, including bug fixes; service packs; and maintenance, minor, and major updates
- Around the clock global access to Cisco TAC
- Access to the extensive Cisco.com knowledge base and tools for easy access to online technical information and service request management
- Advance hardware replacement options including:
  - 24x7x2 advance replacement parts, with or without a field engineer
  - 24x7x4 advance replacement parts, with or without a field engineer
  - 8x5x4 advance replacement parts, with or without a field engineer
  - Next business day (NBD) advance replacement parts, with or without a field engineer

Table 1 shows CIPS service program options.

Table 1. Available Services for IPS Programs

Service Program Name: CIPS **IPS Service Program: Enterprise**		
IPS Svc, AR NBD	SU1	CON-SU1
IPS Svc, AR 8X5X4	SU2	CON-SU2
IPS Svc, AR 24X7X4	SU3	CON-SU3
IPS Svc, AR 24X7X2	SU4	CON-SU4
IPS Svc, Onsite NBD	SUO1	CON-SUO1
IPS Svc, Onsite 8X5X4	SUO2	CON-SUO2
IPS Svc, Onsite 24X7X4	SUO3	CON-SUO3
IPS Svc, Onsite 24X7X2	SUO4	CON-SUO4

Q. Is my IPS solution less effective without a Cisco Services for IPS contract?

A. The effectiveness of your IPS solution will quickly degrade without the frequent security updates included with Cisco Services for IPS. Your IPS solution will continue to operate with the existing library of signatures and reputation updates, but it will process only signature and reputation updates downloaded prior to the expiration of your Cisco Services for IPS contract.

Q. Do I need both a Cisco SMARTnet® Service and a Cisco Services for IPS contract?

A. No. Cisco Services for IPS also includes Cisco SMARTnet Service deliverables. In fact, only Cisco Services for IPS is available for IPS appliances.

Q. Will Cisco SMARTnet Service coverage still be available for routers integrating IPS functionality in Cisco IOS Software?

A. Yes. Both Cisco SMARTnet Service and Cisco Services for IPS are available for routers running operating system images with integrated IPS functionality. If you turn on IPS functionality in Cisco IOS Software or use the IPS router module, Cisco Services for IPS is the appropriate service.

Signature Updates

Q. What is an IPS signature?

A. Cisco IPS signatures are used to identify and block attacks against specific vulnerabilities or certain types of threats. Because new threats and vulnerabilities are constantly being discovered, the signature database needs to be constantly updated to make sure that the protection provided by the IPS stays current.

Q. How do I update my signatures?

A. Cisco investigates and creates signatures for new threats as they are discovered and publishes new signatures regularly. When a new signature update is available, Cisco notifies you that it is available. Signature updates can be installed manually or downloaded and installed automatically using native Cisco IPS capabilities or management tools such as Cisco Security Manager.

Q. Why is updating signatures important?

A. Network security threat levels are common and have escalated in severity. The scope of damage has grown from individual computers and networks to regional networks and even global infrastructures. Vulnerabilities can be exploited within hours. Without constant updates, the IPS solution cannot provide protection against new threats and attacks. The results of undetected, uncontained security breaches are well known, including expensive repair and restoration, lost revenue, compromise and loss of vital data, disruption of business, and damage to your company's reputation.

Q. How often can I expect to be notified of a signature update?

A. Cisco typically publishes lower priority IPS signature updates on a weekly basis. Depending on the severity of a threat, Cisco publishes signature updates within hours of identifying a threat.

Q. Can I obtain signature updates without a Cisco Services for IPS contract?

A. No. Signature updates are available only to customers with a Cisco Services for IPS service contract. Each IPS solution must be under contract.

Q. Am I entitled to signature updates during the warranty period of a product?

A. No. Cisco warranty does not include signature updates.

Global Correlation and Reputation Updates

Q. What is Cisco global correlation and reputation?

A. Cisco global correlation for IPS is a security capability deployed with Cisco IPS Sensor Software Release 7.0. Global correlation harnesses the power of Cisco Security Intelligence Operations (SIO), to achieve unprecedented threat management efficacy. Global threat information is turned into actionable intelligence, such as reputation scores, and pushed out to all enabled Cisco IPS systems. Real-world customer feedback is that global correlation makes Cisco IPS Sensor Software Release 7.0 twice as effective in stopping legitimate attacks, in a shorter amount of time, than traditional signature-only IPS technologies.

Q. When did global correlation and reputation updates become available?

A. Global correlation and reputation updates became available with the release of IPS 7.0.

Q. What IPS technologies and platforms are supported in IPS 7.0?

A. Global correlation is enabled in Cisco IPS Sensor Software Release 7.0. All Cisco IPS sensors that are able to support new IPS Sensor Software releases will be able to run global correlation. Cisco IOS Software IPS currently does not support global correlation and reputation updates. Installed base customers with valid Cisco Services for IPS contracts are entitled to upgrade their IPS products under their service agreement. Supported devices include:

- Cisco IPS 4200 Series appliances
- Cisco ASA 5500 Series with IPS modules
- IPS modules (IDSM-2) for Cisco Catalyst switches
- IPS modules (AIM-IPS and NME-IPS) for ISR routers

Cisco IOS Software-based IPS devices (IPS on Cisco IOS Software) and ASA-5505-AIP5 do not take advantage of global correlation and reputation updates at this time.

Q. How do global correlation and reputation updates work?

A. Cisco IPS sensors continually receive threat updates from the Cisco SensorBase Network that contain detailed information about the known threats on the Internet. Powerful reputation filters can block the worst attackers outright. Cisco IPS 7.0 incorporates global threat data into its inspection algorithms, providing earlier and more accurate detection and prevention of malicious intrusions.

Q. How often will the IPS be updated by Cisco SensorBase Network and vice versa?

A. SensorBase provides global correlation updates generally as frequently as every five minutes. Participating Cisco IPS devices retrieve these updates and can also send threat information back to Cisco SensorBase. This creates a feedback loop that helps improve the SensorBase analysis and improves the effectiveness of your network security.

Q. What is network participation?

A. In addition to receiving updates on global threat conditions, a Cisco IPS sensor might also contribute threat information back into the Cisco SensorBase Network. When a participating IPS detects an attack, it anonymously sends back information on that attack. This data can then be correlated with all other security intelligence that Cisco SensorBase receives to provide early warning of emerging Internet threats.

Q. How does Cisco protect my data when I opt in to network participation?

A. All threat information shared with Cisco is anonymous and encrypted. The information that is most useful in identifying emerging global threats is information about the threats themselves. As such, participation data does not include any information about the victims of attacks, just the identity of the attacker and the type of attack detected. To protect your privacy, participation data does not include any information about internal addresses. So, even if attack activity originates from your network, it will not be communicated back to Cisco, only attacks that target your resources.

Cisco IntelliShield Search Access

Q. What is Cisco IntelliShield Search Access?

A. The Cisco IntelliShield database is a multivendor compilation of new security threats and remediation information. Customers with Cisco Service for IPS can register to get access this database and save time researching threats and vulnerabilities by:

- Finding and confirming emerging vulnerabilities and threats
- Accessing the latest vulnerabilities and threats with correlated signature information
- Viewing updates to existing Cisco IntelliShield alerts with new information as it becomes available (alerts are living documents)
- Getting access to actionable intelligence, such as expertise and methodology through Cisco IntelliShield analysis and safeguards

Q. Does IntelliShield Search Access give me access to the full Cisco Security IntelliShield Alert Manager Service?

A. No. The Cisco Security IntelliShield Alert Manager Service is sold as a separate subscription. The Cisco Security IntelliShield Alert Manager Service provides a comprehensive, cost-effective solution for delivering the intelligence that organizations need to identify, prevent, and mitigate IT attacks. For more information about the full IntelliShield Alert Manager Service, contact your authorized Cisco reseller or Cisco account representative or visit www.cisco.com/en/US/products/ps6834/serv_group_home.html.

Cisco IPS Threat Defense Bulletin

Q. What is the Cisco IPS Threat Defense Bulletin?

A. The Cisco IPS Threat Defense Bulletin is included with every signature update. The bulletin provides detailed information on new protections provided for Cisco IPS as well as the threats and vulnerabilities to which they apply. Information in the bulletin is linked to additional content from Cisco Security Intelligence Operations as well as third-party sources to provide a comprehensive single source solution for security intelligence information.

Operating System Software Updates

Q. Are Cisco operating system software updates included with the Cisco Services for IPS contract?

A. Yes. For Cisco operating systems, such as Cisco IPS Version 6.0 and Cisco IOS Software, all software updates for the licensed feature set are part of the service. Software updates include bug fixes and maintenance, minor, and major releases within a feature set. There are no additional charges for updates as long as the product remains under Cisco Services for IPS coverage.

- Major release (version or main line): Consolidates previous bug fixes, maintenance and previous early deployment releases, and new capabilities into a single release; for example: Cisco IOS Software Release 12.0 or 12.0M or IPS version 6.x to 7.x
- Minor release: Internal to Cisco for Cisco IOS Software; for example: Cisco IOS Software Release 12.3 or 12.3M to 12.4 or IPS version 6.0 to 6.1
- Maintenance release: Includes bug fixes, patches, and service packs; for example: Cisco IOS Software Releases 12.2.3 or 12.2(3) or IPS Operating System release 6.0 to 6.0.6

Q. Why does Cisco only offer OS software "updates" with Cisco Services for IPS? Other vendors say they offer software upgrades.

A. It is only a difference in terminology. Cisco uses the term "upgrade" when a customer moves from one software feature set to another. Major updates or major releases within a software feature set are the Cisco equivalent to what other vendors call software upgrades (for example, an upgrade from version 6.0 to 7.0).

Q. What is a feature set upgrade? Is it included in Cisco Services for IPS?

A. A feature set upgrade is a separately licensed and priced software release that contains enhanced configurations or features that provide additional capabilities. For example, to upgrade from the IP to IP/Internetwork Packet Exchange (IPX) feature set or IP Base to IP Advance Security, you must purchase the upgrade. However, just like Cisco SMARTnet Service, feature set upgrades are not available as part of a Cisco Services for IPS offering.

Q. Is support for Cisco applications software products, such as IP telephony and network management, included in the Cisco Services for IPS offering?

A. No. Cisco has three software application service offerings that support Cisco application software products such as IP telephony, network management, and CiscoWorks VPN Security Management Software (VMS). The three programs are Unified Communication Essential Operate Services for voice products; Cisco Software Application Support (SAS); and Cisco Software Application Support plus Upgrades (SASU) for network management, security, and other software applications.

Availability, Ordering, Registration, and Entitlement

Q. Where is Cisco Services for IPS support available?

A. Cisco Services for IPS support is available globally. Service levels might vary. The Cisco Service Finder tool can be used to verify the available product services. This tool includes information for Cisco Services for IPS support as well as other technical services. Information is available at www.cisco-servicefinder.com.

Q. How do I buy Cisco Services for IPS?

A. You can purchase Cisco Services for IPS from Cisco or its certified partners. Cisco service providers can also resell Cisco Services for IPS. You can find a Cisco certified partner in your area by searching in the partner locator at www.cisco.com/go/partnerlocator.

Q. Do Cisco Services for IPS include remote or onsite software update installation services?

A. No. Cisco Services for IPS do not include software installation. You are responsible for software installation, or you can purchase these services from a Cisco channel partner. However, the service does allow you to call the Cisco TAC for help during this process.

Q. Can I purchase Cisco Services for IPS for an IPS product that has not been covered previously by a Cisco service contract?

A. Yes, but you must have purchased a license for the current version of operating system software. If the software is one or more releases old, then you must purchase the current release before you can purchase Cisco Services for IPS for each IPS product. Cisco inspects all hardware, components, and software to certify the product before approving coverage. For applicable certification fees, contact your Cisco sales team.

Q. Why is the price of Cisco Services for IPS generally higher than that for Cisco SMARTnet Service?

A. Cisco Services for IPS includes all of the deliverables of Cisco SMARTnet Service plus the additional value elements needed for essential coverage for IPS, including signature updates, global correlation and reputation updates, and IntelliShield Alert Manager Search Access.

Q. Is there a registration process to acquire a license for my IPS solution?

A. Cisco IPS appliances, ASA5500 IPS bundles, ASA IPS modules, IPS router modules, and Cisco Catalyst IPS service modules running IPS Version 5.0 or later software require registration and licensing.

With IOS version 15.0(1)M or later, both the feature set license for the security images with IPS and the ability to get IPS on IOS signature file updates require registration. The feature set license for the security features including IPS is a one-time (perpetual) license.

Registration for IPS on IOS signature file updates is the same as IPS appliance registration today and applies to most ISR routers that run IOS version 15.0.(1)M or later. To register for IPS on IOS signature file updates, make sure the IPS solution is supported by a valid Cisco Services for IPS contract, then visit the Cisco licensing site at www.cisco.com/go/license. (Cisco.com login credentials required for access.) Re-registration is required when the Cisco service for IPS contract is renewed.

For ISR routers with earlier versions of IPS integrated in Cisco IOS Software, registration is not required.

Q. Why do I need to know about the registration process?

A. Registration includes validation that the serial number for IPS exists in an eligible contract type between you and Cisco. If registration fails because a serial number is incorrect or the serial number is in an ineligible contract type, it might delay implementing IPS signature updates. To get a license key, contact your sales organization.

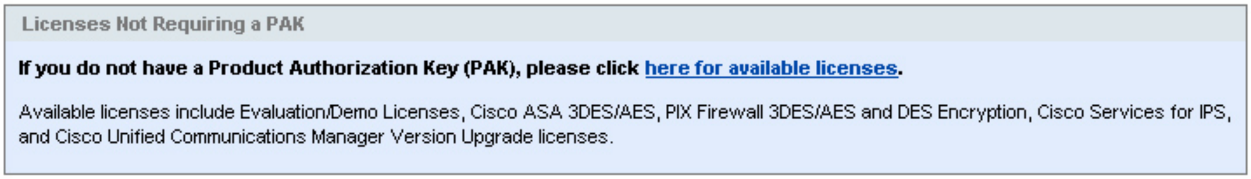
Q. Why is it important that the IPS product and serial numbers on each Cisco Services for IPS contract be accurate?

A. Cisco service entitlement is based on serial number validation. Customers using IPS appliances, IPS router modules, or Cisco Catalyst service modules running IPS version 5.0 or higher must complete online serial number registration in order for their IPS solution to process signature updates. Registration includes validation that the serial number for IPS solution exists in an eligible contract type. If registration fails because a serial number is incorrect or that serial number is in an ineligible contract type, you should contact your Cisco sales team or your Cisco reseller for assistance in obtaining a license key.

Q. How do I register my intrusion prevention system to get signature updates through Cisco Services for IPS?

A. To register, follow these five steps:

1. Make sure the IPS solution is supported by a valid Cisco Services for IPS contract.
2. Visit the Cisco licensing site at www.cisco.com/go/license. This requires your Cisco.com login credentials.
3. Select “if you do not have a Product Authorization Key (PAK), please click here for available licenses.”

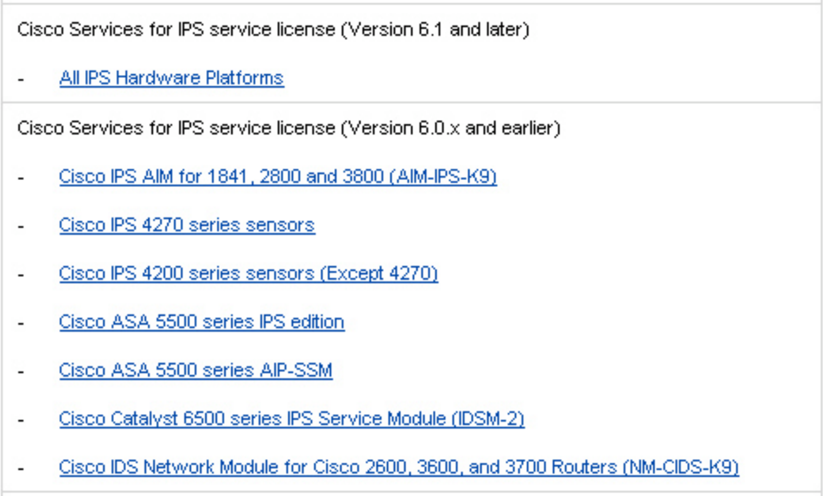


Licenses Not Requiring a PAK

If you do not have a Product Authorization Key (PAK), please click here for available licenses.

Available licenses include Evaluation/Demo Licenses, Cisco ASA 3DES/AES, PIX Firewall 3DES/AES and DES Encryption, Cisco Services for IPS, and Cisco Unified Communications Manager Version Upgrade licenses.

4. Choose the appropriate IPS version and product:



Cisco Services for IPS service license (Version 6.1 and later)

- All IPS Hardware Platforms

Cisco Services for IPS service license (Version 6.0.x and earlier)

- Cisco IPS AIM for 1841, 2800 and 3800 (AIM-IPS-K9)
- Cisco IPS 4270 series sensors
- Cisco IPS 4200 series sensors (Except 4270)
- Cisco ASA 5500 series IPS edition
- Cisco ASA 5500 series AIP-SSM
- Cisco Catalyst 6500 series IPS Service Module (IDSM-2)
- Cisco IDS Network Module for Cisco 2600, 3600, and 3700 Routers (NM-CIDS-K9)

5. Enter the requested serial number or serial number and part number. The IPS system lookup/show UDI command should have the correct PID identified. For IPS modules, use the part number and serial number of the module. Examples: IPS-4255-K9 uses product ID IPS4255, ASA5510-AIP10-K9 uses the SSM module (ASA-AIP-10-INC-K9) part number SSM10.

Q. How do I register for Cisco IntelliShield Alert Manager Search Access?

A. IntelliShield Alert Manager Search Access is available to Cisco Services for IPS customers at no additional cost. Registration requires a valid IPS license file or serial number of a Cisco IPS device currently entitled to Cisco Services for IPS (only one user account per IPS license file or serial number is allowed).

IntelliShield Search Access support is available from 7 a.m. to 8 p.m. Eastern Time by sending an email to IntelliShieldsearch-support@cisco.com.

IntelliShield Alert Manager Search Access is not associated with Cisco.com credentials.

Q. How do I register for network participation?

A. Global correlation ships with network participation turned off by default. Customers must opt in (turn it on) using the management application to start sending threat data back to Cisco. This makes sure that no customer will send data to Cisco without intending to.

Q. How do I subscribe to the Cisco Threat Defense Bulletin?

A. You can subscribe to Cisco Threat Defense Bulletin (formerly Cisco IPS Active Update Bulletin) on Cisco.com to receive emails when signature updates and service pack updates occur by following these steps:

1. Log in to Cisco.com.
2. Using the Search function on the right side of the window, enter Security Center. Choose the first entry.
3. Scroll down, and under Products and Service Updates, choose Cisco IPS Threat Defense Bulletins.
4. Click one of the Cisco IPS Threat Defense Bulletins.
5. Under In this Issue, click Subscription Information.
6. Under Subscription Information, click Subscribe Now.
7. Fill out the required information.

Q. If my IPS solution is already covered under the Cisco warranty, why should I buy Cisco Services for IPS support during the warranty duration?

A. Signature updates are not included in warranty coverage. Cisco Services for IPS provide more robust levels of support than what is available under a Cisco warranty. For most IPS products, Cisco warranties are limited to 90 days, whereas Cisco Services for IPS can be purchased in renewable annual and multiyear increments. To take full advantage of all the investment protection benefits provided by Cisco Services for IPS, it is important that you purchase service on the day you purchase your Cisco IPS solution. Services available under a Cisco Services for IPS contract that are not covered under warranty include the following:

- Notification or delivery of signature updates when they are posted to Cisco.com
- Cisco global correlation and reputation updates on enabled IPS products
- Cisco IntelliShield Search Access
- Entitlement to Cisco OS and IPS engine updates
- Continuous technical support through Cisco TAC
- Registered access to Cisco.com support tools and applications
- Rapid replacement of hardware in next business day, 4-hour, or 2-hour dispatch options, where available

Table 2 shows a comparison between warranty and Cisco Services for IPS deliverables.

Table 2. Comparison of Warranty Coverage and Cisco Services for IPS

Feature	Warranty	Cisco Services for IPS
Notification of signature updates	No	Yes
Signature updates	No	Yes
Operating system updates	No	Yes
Registered access to Cisco.com security knowledge base	No	Yes
Access to technical support (TAC)	No	Yes
Options for advance hardware replacement	No	Yes
Global correlation updates	No	Yes

Q. Are Cisco Services for IPS contracts transferable from customer to customer?

A. No. Cisco service contracts are not transferable.

Q. What do I do if the licensing process fails?

A. Contact your sales organization and explain the situation and ask the sales organization to verify that the serial number for the IDS or IPS you want to register is under a Cisco Services for IPS contract. If it is, your sales agent will work with the Cisco licensing team to resolve the problem. You can also request a one-time license key (valid for 30 days only) by visiting the licensing website at www.cisco.com/go/license. (Cisco.com login credentials required for access.)

Q. How do I enable the Cisco Services for IPS for entitlement through the pending process?

A. Customer service resolves all pending process issues.

Q. How am I notified of available signature updates?

A. Cisco automatically generates email messages when new or updated signatures are posted to Cisco.com. In accordance with Cisco privacy policy, you must elect to receive this notification and product news by subscribing to Cisco IPS Threat Defense Bulletin email notifications.

Q. How do I obtain signature updates?

A. Downloading signature updates is simple. Make sure the IPS device is supported by a valid Cisco Services for IPS contract.

- Signature updates can be updated from the Software Download Center at http://tools.cisco.com/support/downloads/go/Redirect.x?mdfid=268438162. (Log in required.)
- With IPS version 6.1 and later, new auto update functionality has been added to the IPS device operating system that allows you to configure your IPS devices to automatically pull new signature updates from Cisco.com. You can also configure auto updates of operating system and IPS engine updates.
- Cisco Security Manager can also be configured to automatically download signature updates and push the new files to the deployed IPS devices. For more information, visit www.cisco.com/en/US/products/ps6498/index.html.

Q. How do I obtain Cisco operating system software updates?

A. Visit the Cisco Software Center at http://tools.cisco.com/support/downloads/go/Redirect.x?mdfid=268438162 and select Intrusion Prevention System (IPS). (Log in required.)

Q. Can I obtain support from the Cisco TAC if I do not have a service contract?

A. Yes, but you might be asked to pay a per-incident fee or to purchase a service contract. Signature updates are not available on a one-time basis.

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 C67-554954-00 08/09