



## PARTNER Q & A

# CISCO SERVICES FOR INTRUSION PREVENTION SYSTEM

### **A secure network infrastructure is critical to the success of your business.**

Without the proper protection, your network is vulnerable to viruses, worms, denial-of-service attacks, and other internal and external threats that could degrade network performance, compromise the integrity and privacy of sensitive data, or disrupt business continuity. The challenge is to implement a security solution that actively blocks this deviant network traffic while simultaneously allowing authorized traffic to flow freely so your users can access data and applications as needed.

Cisco® Services for Intrusion Prevention System (IPS) provides essential, ongoing support for Cisco Systems® IPS solutions and helps ensure that a Cisco IPS product and the signature files that it uses to protect the network are current. Together, Cisco IPS solutions and the Cisco Services for IPS are components of the Cisco Self-Defending Network, which can proactively identify known issues and respond to and contain many emerging threats.

Delivering timely information, signature-file updates, and comprehensive support, Cisco Services for IPS helps your Cisco IPS solution stay current on the latest threats so that malicious or damaging traffic is accurately identified, classified, and stopped in real time.

## **GENERAL**

**Q.** What does Cisco deliver with its “integrated security solutions?”

**A.** Security staffs must ensure free flow of authorized information through the network and at the same time protect its integrity and confidentiality. Cisco Integrated Security solutions help IT and security staff meet this challenge by embedding security in network infrastructure elements, security platforms and applications, and security applications for endpoints such as desktops and servers.

Cisco Integrated Security solutions offer a broad and in-depth network defense that meets the needs of both security operations (SecOps) and network operations (NetOps) staff.

**Q.** What is an intrusion detection system (IDS) or intrusion prevention system (IPS)?

**A.** A Cisco Intrusion Detection System (IDS) is a technology used to detect suspected malicious network traffic or behavior. Intrusion prevention systems (IPSS) evolve from IDSs to not only detect, but also prevent malicious network traffic or behavior.

Cisco products which feature IPS functionality such as an IPS appliance, router or Catalyst switch are installed at critical points in the network to perform real-time analysis of network traffic. They monitor for anomalies and misuse based on a “signature file.” When the system detects unauthorized activity, it can automatically terminate the specific connection, permanently block the attacking host, log the incident, and send an alarm to the management console.

**Q.** What is a signature?

**A.** Like a fingerprint, the signature uniquely identifies a specific worm, virus, protocol anomaly, or malicious traffic.

**Q.** What is a signature file?

**A.** A signature file comprises a package of network signatures that is intended as an update to the signature database resident in a Cisco product with IDS or IPS functions. This signature database is used by the IPS solution to compare network traffic against data patterns within the signature-file library. The IPS solution uses this comparison to detect suspected malicious network traffic behavior. The signature file, therefore, when installed in an IPS solution becomes the signature database that the product uses to detect suspicious behavior.

**Q.** What is a signature-file update?

**A.** Because new threats and malicious behavior are discovered continually, Cisco investigates and creates signatures for threats around the clock and publishes new signatures regularly. A signature-file update simply means replacing the most recent signature file with one that has newer signatures and posting it to Cisco.com. Each update includes new signatures and all those that were in the previous version. For example, signature file 124 includes all signatures in file 123 plus signatures created for threats discovered after file 123. When the signature file is available, Cisco notifies your customer that the new file is available and can be downloaded.

**Q.** How am I or my customer notified of available signatures?

**A.** Cisco automatically generates e-mail messages to customers when updated signature files are posted to Cisco.com. In accordance with Cisco privacy policy, customers must elect to receive this notification and product news by subscribing to Cisco IDS Active Update Bulletin e-mail notifications. Their e-mail address is not used for any other purposes. To sign up, they should go to: <http://www.cisco.com/pgi-bin/front.x/ipsalerts/ipsalertsHome.pl> and click on “Subscribe to Active Update Notifications.”

**Q.** What is Cisco Services for IPS?

**A.** Cisco Services for IPS has two variations. The first, Cisco Services for IPS, combines Cisco SMARTnet® support with signature-file updates and notifications about their availability. The second, Cisco Services for IPS Standalone, delivers only signature-file updates and notification about their availability. This service is available for sale only on top of a Cisco Shared Support or Cisco Systems Integrator Support (SIS) service, where available.

**Q.** What is included with Cisco Services for IPS?

**A.** Cisco Services for IPS includes:

- Notification of availability of new or updated signature files
- Access to signature-file library and new signature files for each registered IPS
- Support for licensed operating system software for each registered IPS; software updates include maintenance, minor, and major releases
- Access to the Cisco Technical Assistance Center (TAC) 24 hours a day, 7 days a week
- Registered access to Cisco.com and its online technical information and service request management tools
- Advance Replacement of hardware parts, depending on the customer need and the coverage selected:
  - – 24 x 7 x 4—Advance Replacement parts are delivered within 4 hours of determining that part replacement is required during a standard work week (24 hours per day, 7 days per week).
  - – 8 x 5 x 4—Advance Replacement parts are delivered on a 4-hour response basis between 9 a.m. and 5 p.m. local time the same business day, provided both the call and the Cisco diagnosis and determination of the failed hardware has been made before 1 p.m. local time. For calls placed after 1 p.m. local time, Cisco delivers the Advance Replacement part the morning of the next business day.
  - – Next Business Day (NBD)—Advance Replacement parts are delivered the next business day between 9 a.m. and 5 p.m. provided the request is received before 3 p.m. local depot time.

**Q.** Why should I (my customer) buy Cisco Services for IPS support?

**A.** The extent of network protection is related to the currency of the signature files. Cisco Services for IPS proactively alerts customers when the latest signature files are available. In doing so, this service may help customers as they focus to:

- Increase business productivity through reduced disruptions to the enterprise, and efficient and intelligent tools, applications, and processes
- Improve business resiliency by proactively detecting and preventing security threats
- Protect their network investment through reduced capital expense and lower operating costs, providing the market’s lowest total cost of ownership (TCO)
- Preserve integrity and privacy of sensitive business, employee, and customer information by protecting your network from security intrusions

**Q.** What benefits does Cisco Services for IPS provide?

**A.** Cisco Services for IPS can help customers as they focus to:

- Ensure network security and maximize network availability, reliability, and stability
- Reduce total cost of network ownership by using Cisco security expertise, knowledge, and availability
- Increase return on investment (ROI) by having access to Cisco operating system software enhancements
- Expedite time to repair with the right parts at the right time
- Supplementing the customer's network support organization to ensure the availability of the knowledge and skills necessary to address rapidly changing technologies
- Better manage limited internal expert resources at all locations
- Improve productivity and revenue per employee with access to tools and technical support documentation that can increase self-sufficiency and technical knowledge

**Q.** Cisco Services for IPS does not seem to significantly affect my customer's current business initiatives. Is it just break-and-fix insurance?

**A.** Only a small portion of service requests deal with failures and defects. Most service requests help customers handle complex network operation and management issues such as:

- Advanced software configuration
- Interoperability and upgrade questions
- Hardware and software information
- 24-hour monitoring of new threats and intrusions and delivery of new signatures

**Q.** Will Cisco SMARTnet coverage still be available for IPS appliances, IPS network modules for routers and Catalyst IPS service modules?

**A.** No. Cisco Services for IPS replaces SMARTnet coverage for IPS appliances, IPS switch modules, and IPS router modules. Cisco SMARTnet support is suitable to protect most networking products that must operate at optimum performance. Cisco SMARTnet support, however, does not include all the service components suitable to ensure that an IPS appliance, IPS switch module, or IPS router module operates at peak performance.

Since Cisco Services for IPS replaces Cisco SMARTnet support for IPS appliances, IPS switch modules, and IPS router modules, you will no longer be able to resell Cisco SMARTnet for these products.

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

**A.** Yes. Both Cisco SMARTnet and Cisco Services for IPS support are available for routers running operating system images with integrated IPS functionality. If a customer selects to turn on IPS functionality in IOS, Cisco Services for IPS provides the appropriate service since Cisco SMARTnet support does not include all the service components suitable to support IPS functionality.

**Q.** How will upgrading from Cisco IPS Version 4.0 to the new Cisco IPS Version 5.0 software impact my customers' IPS solution?

**A.** IPS appliances, IPS router modules, and Catalyst IPS service modules running IPS version 5.0 will not be able to process updated signatures. They will continue to process the signature shipped at time of purchase or the last signature file downloaded before contract expired.

**Q.** How does my customer or I start downloading signature files for their IPS solution?

**A.** Downloading signature files is simple. Ensure the IPS solution is supported by a valid Cisco Services for IPS services. Then visit the IPS Alert Center at <http://www.cisco.com/pcgi-bin/front.x/ipalerts/ipalertsHome.pl> and click on "Software Center" on the right hand side of the page. Scroll through the list of updates and select the update for the appropriate IPS solution.

**Q.** How do I register to acquire a license for an IPS solution?

**A.** Routers running IPS integrated in IOS do not require registration. Cisco IPS appliances, IPS router modules, and Catalyst IPS service modules running IPS Version 5.0 software require licensing. Licensing uses a registration process to generate tokens with an expiration date.

The registration process checks the Cisco contract database (CIBER) for existence of a serial number in a valid Cisco Services for IPS contract. If a match is found, it issues a license key that expires on that date. This allows the IPS software to process signatures during a contract period only.

To register, visit: <http://www.cisco.com/go/license> .

**Q.** Will a customer’s IPS solution continue to operate if the customer does not renew this service?

**A.** Yes. Your customers IPS solution will continue to operate but it will be able to process only signature-file versions downloaded prior to the expiration of their Cisco Services for IPS contract. Caution: Processing the latest signatures is critical in detecting exploits. Products processing old signatures will provide inadequate detection.

**Q.** Can my customer obtain signature-file updates without a Cisco Service for IPS contract?

**A.** No. Signature-file updates are not available to customers without a Cisco Services for IPS service contract. Each IPS solution must be under contract.

**Q.** Which Cisco service offerings include signature-file updates?

**A.** Both Cisco Services for IPS and Cisco Services for IPS Standalone provide signature updates. Cisco Services for IPS Standalone, however, is available as Cisco Brand Resale (CBR) on top of Cisco Shared Support or Cisco SIS (where available) contract for the same device (based on serial number).

### CISCO WARRANTY COMPARED TO CISCO SERVICE CONTRACT

**Q.** If a product is already covered under the standard Cisco warranty, why should a customer buy Cisco Services for IPS support during the warranty duration?

**A.** Signature files are not included in warranty coverage. To receive coverage beginning on the date of purchase, customers must enroll on that date. Cisco Services for IPS provides more robust levels of support than what is available under a Cisco warranty. For all IPS solutions, Cisco warranties are limited to 90 days, whereas Cisco Services for IPS can be purchased in renewable annual and multiyear increments.

Services available under a Cisco Services for IPS contract that are not covered under a warranty include the following:

- Notification of signature-file updates as they are developed
- Alerts for recently available signature-file updates
- Rapid replacement of hardware in NBD, 4-hour, or 2-hour dispatch options, where available
- Continuous technical support through Cisco TAC
- Latest Cisco operating system software updates
- Registered access to Cisco.com

**Table 1.** Comparison of Warranty Coverage and Cisco Services for IPS

Feature	Warranty	Cisco Services for IPS	Cisco Services for IPS Standalone *
Notification of signature-file updates	N	Y	Y
Signature-file updates	N	Y	Y
Operating system updates	N	Y	N
Registered access to Cisco.com security knowledge base	N	Y	N

Feature	Warranty	Cisco Services for IPS	Cisco Services for IPS Standalone *
Access to technical support	N	Y	N
Options for advance hardware replacement	N	Y	N

\* Requires the product serial number to exist in a shared support or Cisco SIS contract

To take full advantage of all investment protection benefits offered by Cisco Services for IPS, customers must begin coverage on the day they purchase Cisco hardware.

**Q.** Is Cisco liable for damages to customer assets if a virus, worm, or other malicious attack occurs while they have Cisco Services for IPS coverage for their IPS solutions?

**A.** Any liability of Cisco is defined in the executed agreement between the parties.

### SIGNATURE-FILE SUPPORT

**Q.** When does a customer receive notification of a signature-file update?

**A.** Cisco and its partner Trend Micro are monitoring and investigating threats and exploits around the clock. When a new signature file is created, tested, and released, Cisco alerts the customer by e-mail that the signature file is available. The alert includes a URL for downloading the appropriate signature file. To receive the alerts, visit the IPS Alert Center at <http://www.cisco.com/pcgi-bin/front.x/ipsalerts/ipsalertsHome.pl> click on “Subscribe to Active Update Notifications” on the right of the page and complete the form.

**Q.** How often can a customer expect to be notified of a signature-file update?

**A.** Cisco typically publishes lower-priority IPS signature files biweekly. However, depending on the severity of a threat, Cisco publishes signature files within hours of identifying and prioritizing a threat.

**Q.** Why is updating signature files important?

**A.** Network security threat levels are escalating. There were 6.6 times more virus alerts in the first quarter of 2004 compared to the first quarter of 2003. At the same time, the target of these attacks and the scope of damage they create has grown from individual computers and networks to regional networks and global infrastructures. In addition, these attacks are occurring more frequently and spreading more quickly.

All these factors combined lead to the greater likelihood of network compromise. Networks deploying the latest signature files are better protected against network intrusions.

**Q.** How is this service different from Cisco SMARTnet only coverage?

Cisco Services for IPS adds a preventive component. It combines Cisco SMARTnet deliverables with timely notification and availability of signatures and policies for IPS solutions.

**Q.** Why is it important that serial-number information on each Cisco Services for IPS contract is accurate?

Cisco service entitlement is based on serial number validity.

Furthermore, customers using IPS appliances, IPS router modules, or Catalyst service modules running IPS version 5.0 must complete online serial number registration in order for their IPS solution to process signature file 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 will have to work with Cisco licensing to help customers get their license key as well as explain how the process works.

## TECHNICAL SUPPORT

**Q.** How does Cisco.com help customers support their networks?

**A.** Cisco.com empowers customers to open service requests online and to solve problems more quickly, increasing self-sufficiency and productivity. Access to Cisco.com provides productivity and software support tools:

- Software Advisor—This single, convenient interface helps customers resolve the common question, “What Cisco IOS® Software release do I need?”
- Software Bug toolkit—This tool helps customers make informed decisions about which specific software versions to use. Customers can sign up to receive proactive bug notification, based on their network profiles, which will inform them of software bugs that could affect their networks.
- Interactive software management tools—These tools provide patch information and error notifications to help customers address network issues more efficiently.
- Cisco IOS Software Planner—This tool helps customers determine the correct software version to use.
- Product Alert tool—This tool is used to set up a customer profile to receive e-mail updates about reliability, safety, network security, and end-of-sale issues for specific Cisco products.

Internet commerce tools:

- Allow customers to purchase Cisco products and services, check order status, and use the enhanced Web-based configuration tool
- Offer peer-to-peer online forums—Extend customer access to industry peers and allow them to have technical discussions with engineers (many with CCIE® certification)

Automated troubleshooting tools and support:

- Cisco TAC Case Collection—This tool allows customers to interactively identify and troubleshoot common hardware, configuration, and performance issues.

Cisco Software Center:

- The Cisco Software Center is a comprehensive library of software updates and signature files. This service allows customers to quickly access and download the updates they need directly to their network.

**Q.** My customer has asked me about the out-tasking of Cisco TAC services under a Cisco Services for IPS contract. How will this affect the handling of my customer’s network issues?

**A.** There should not be a change in technical support you or your customer receives from Cisco TAC. The Cisco TAC uses a network of partners and third-party vendors who work under the supervision of Cisco TAC management. Cisco TAC employs a highly skilled staff that offers years of networking experience—more than 1200 customer support engineers on staff, more than 390 CCIE certified staff, and access to 13,000 research and development engineers. In addition, the Cisco TAC sophisticated call-routing system promptly routes the customer to the correct technology expert to quickly address the problem at hand.

**Q.** How do I talk to customers about our competitors’ service offerings, and how do our offerings compare to competitors’ offerings?

**A.** For information about how to respond to customer questions about specific competitors and how Cisco services offerings compare, visit: <http://www.in.cisco.com/competitive/security/index.shtml>.

## OPERATING SYSTEM SOFTWARE SUPPORT

**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 5, Cisco IOS Software, and the Cisco Catalyst® Operating System software, all software updates for licensed feature sets for the customer’s covered platform are part of the basic program. Software updates include bug

fixes and maintenance, minor, and major releases within a feature set. No additional charge for updates is warranted 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, or new capabilities into a single release; for example: Cisco IOS Software Release 12.0 or 12.0M
- Minor release—Internal to Cisco for Cisco IOS Software; synonymous with a major release; for example: Cisco IOS Software Release 12.3 or 12.3M
- Maintenance release—Includes bug fixes; for example: Cisco IOS Software Release 12.2(16), 12.2(16a), 12.2.16, or 12.2.16a; also includes new point features or early-deployment releases; for example: Cisco IOS Software Release 12.2(8)T, 12.2.(8)T1, 12.2.8T, or 12.2.8T1

**Q.** Other vendors say they offer software upgrades. My customer wants to know why Cisco offers only software “updates” with Cisco Services for IPS.

**A.** It is only a difference in terminology. Cisco has chosen to attribute the term “upgrade” to when a customer moves from one software feature set to another. “Major releases” within a software feature set are the Cisco equivalent to what other vendors call software upgrades (an upgrade from 2.0 to 3.0, for example).

**Q.** What, then, 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 (new feature sets for Cisco 1700, 2600, and 3700 series routers), customers must purchase the upgrade. However, these 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 Software Application Services provides support for Cisco application software products such as IP telephony, network management, and CiscoWorks VPN/Security Management Software (VMS). Two programs are available to support these applications—Software Application Support (SAS) and Software Application Support plus Upgrades (SASU). Cisco SAS includes 24-hour Cisco TAC support, registered access to Cisco.com, and application software updates (maintenance and minor releases). Cisco SASU includes all the components of Cisco SAS, plus access to major releases of application software.

**Q.** Does Cisco Services for IPS include entitlement to remote or onsite software upgrade installation services?

**A.** No. Cisco Services for IPS does not include software installation. The customer is responsible for software installation or can purchase these services from a Cisco channel partner. However, the services do allow the company to call the Cisco TAC for help in this process.

## **PRICING**

**Q.** My customer is not necessarily against a price increase but would like to understand why the Cisco Services for IPS price is different from the Cisco SMARTnet price. How do I explain this?

**A.** Cisco Services for IPS and Cisco SMARTnet support are equally valuable to you because they provide the “right” level of support for the appropriate products.

With regard to IPS solutions, Cisco Services for IPS combines a new service deliverable, signature-file updates, with standard Cisco SMARTnet deliverables to ensure the latest signature files are within your reach to mitigate threats, in addition to providing support for software and hardware.

Current signature files are critical for network protection. Identifying, preventing, and responding to network security threats depends on timely delivery of up-to-date signature files. This service helps you minimize network intrusions that would result in disruption in your business and lower productivity with the same or reduced staff, and it results in reduced TCO.

**Q.** My customer wants to pay on a time-and-materials (T&M) basis rather than purchasing a service contract. What should I do?

**A.** Signature updates are not available on a T&M basis. Inform your customer that the T&M method can be costly. Each telephone support call incurs minimum charges, regardless of the complexity of the problem. Do you or your customer really want to issue purchase orders or manage payments on a weekly or biweekly cycle? In addition, T&M customers:

- Are served only on an “as available” basis—Customers with contracts have priority.
- Have no assurance that spare parts will be available where and when they need them
- Are not entitled to registered access to Cisco.com and the advantages of software downloads, online tools, and other technical resources that can help keep their staff up-to-date and self-reliant
- Do not have the network investment protection and risk-minimization advantages that Cisco Services for IPS provides, and may possibly require more services than anticipated, increasing their cost burdens

### **PROCESSES AND RESPONSIBILITIES**

**Q.** How does Cisco prioritize support service requests?

Cisco requests that customers provide the severity of every service request reported. To ensure that all problems are reported in a standard format, Cisco has established the following problem severity definitions:

- Severity 1—An existing network is down or there is a critical impact to the customer’s business operations. Cisco and the customer will commit necessary resources around the clock to resolve the situation.
- Severity 2— Operation of an existing network is severely degraded or significant aspects of the customer’s business operation are being negatively affected by unacceptable network performance. Cisco and the customer will commit full-time resources during normal business hours to resolve the situation.
- Severity 3—Operational performance of the network is impaired, while most business operations remain functional. Cisco and the customer are willing to commit resources during normal business hours to restore service to satisfactory levels.
- Severity 4—Customer requires information or assistance on Cisco product capabilities, installation, or configuration. There is clearly little or no impact to the customer’s business operation. Cisco and the customer are willing to provide resources during normal business hours to provide information or assistance as requested.

Note: Customers should understand that they set the severity of the service request they open.

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

**A.** Yes. The Cisco TAC will provide support to companies that do not have a current Cisco service contract, but there is a per-incident fee, or the customer may be asked to purchase a service contract.

Note: Signature updates are not available on a one-time basis. Providing a signature-file update by Cisco TAC does not ensure that IPS will be able to process it.

**Q.** Is there a registration process to enable processing of new signatures?

**A.** Yes. Customers installing Cisco IPS Version 5 on their IPS appliances, IPS router modules, Catalyst IPS service modules must access the Cisco licensing website at <http://www.cisco.com/go/license> to register the serial number and receive a key before their IPS solution can process signature updates.

**Q.** I have a service organization offering my own brand of service. How do I provide services for Cisco IPS solutions?

**A.** You can and should continue to renew and sell your brand of service to your customers. You can continue to deliver ongoing support for the operating system software and advance hardware replacement.

For customers to receive signature files, you must resell Cisco Services for IPS, Standalone. You may resell this contract under your Cisco Brand Resale agreement.

To support your brand of maintenance service, excluding signature updates, purchase a Cisco Shared Support contract for the IPS appliance or Cisco Catalyst services module, ensuring the correct serial number is recorded in the contract. Then resell Cisco Services for IPS Standalone to the customer. Work with your Cisco sales support team to ensure the serial number in the second contract matches the one in shared support. The Cisco Services for IPS Standalone allows product licensing to process signatures, and provides signature updates and e-mail notification to end users about the availability of new signatures.

- Q.** How does Cisco Services for IPS align with existing partner brand support programs such as Cisco Shared Support and Cisco SIS98 (where still available)
- A.** Cisco Services for IPS is available for resale by Shared Support and SIS98 partners under the terms of their Cisco Brand Resale agreement.
- Q.** What happens to existing Cisco SMARTnet contracts covering IPS appliances, IPS router modules, Catalyst IPS service modules?
- A.** All Cisco SMARTnet contracts for these products are grandfathered into a Cisco Services for IPS contract that expires at same date as the existing Cisco SMARTnet contract.
- Q.** Are Cisco Services for IPS contracts transferable from customer to customer?
- A.** No. Cisco service contracts are not transferable. Customers must purchase a contract from Cisco or an authorized Cisco support reseller.

#### **AVAILABILITY**

- Q.** Can a customer purchase Cisco Services for IPS for an IPS solution that has not been covered previously by a Cisco service contract?
- A.** Yes, but customers must be licensed to use the current version of operating system software. If the operating system software is one or more releases old, customers must purchase the current release before they can purchase Cisco Services for IPS for each IPS solution.

Additionally, Cisco inspects all hardware, components, and software before approving coverage.

- Q.** Where is Cisco Services for IPS support available?
- A.** Cisco Services for IPS support is available in North America, Western Europe, New Zealand, Mexico, Australia, and select countries in Asia and South America. Cisco is continually expanding its service areas. In addition, the Cisco Service Availability Matrix (SAM) tool can be used to verify the available product services worldwide. This tool includes information for Cisco Services for IPS support, Cisco SP Base, and the Cisco SmartSpares (where available) program. Information is available at: [http://www.cisco.com/cgi-bin/front.x/agents/SAM/cca\\_sam\\_main.cgi](http://www.cisco.com/cgi-bin/front.x/agents/SAM/cca_sam_main.cgi)
- Q.** What kind of service will my customers receive on equipment that is heavy or oversized?
- Refer to the Cisco Heavy/Oversized Equipment Service Policy and Procedures at: [http://www.in.cisco.com/cmcc/serv/mkt/sup/tsssv/opmsup/smton/sssre\\_in.pdf](http://www.in.cisco.com/cmcc/serv/mkt/sup/tsssv/opmsup/smton/sssre_in.pdf)
- Q.** Can I resell Cisco Services for IPS?
- A.** Yes. Cisco partners can resell Cisco Services for IPS if they have signed a Cisco Brand Services Resale Agreement.
- Q.** Can service providers resell Cisco Services for IPS for support?
- A.** Yes. Service providers can resell Cisco Services for IPS if they have signed a Cisco Brand Services Resale Agreement.
- Q.** Is Cisco Services for IPS support available through the Cisco Shared Support program?
- A.** No. Signature updates are not available through Cisco Shared Support. Cisco Shared Support contracts provide coverage for service deliverables equivalent to Cisco SMARTnet support.

For example, purchase of CON-CSSP-IDS4215K9 entitles partners to IPS operating system software updates, technical support, and access to Cisco.com. Customers must purchase a Cisco Services for IPS Standalone contract, part number CON-SUSA-IDS4215K9, to receive signature file updates.

- Q.** Is the Cisco Services for IPS offering available through two-tier distributors?

**A.** Yes. Resellers who purchase Cisco products through two-tier distributors can purchase and resell packaged Cisco Services for IPS. Packaged Cisco Services for IPS support provides the same deliverables as standard Cisco Services for IPS and support. Distributors stock Cisco Services for IPS packages, which are provided to the reseller with each sale. The package contains mandatory contract registration instructions for the end user.

## **ORDERING AND ENTITLEMENT**

**Q.** What is the process to order Cisco Services for IPS at the point of product sale?

**A.** If you are creating a quote or order that contains only IDS products, you can use the service-level default function in the Cisco Ordering tool. When creating your order, select the IPS SVC service with desired hardware response level from the service-level drop-down menu on the “Create an Order” page. When you add and configure IDS products to your order, the service is automatically added for you.

**Q.** What is the process to order Cisco Services for IPS at the point of product sale?

**A.** If you are creating a quote or order that contains only IPS/IDS solutions, you can use the service-level default function in the Cisco Ordering tool. When creating your order, select the IPS SVC service with desired hardware response level from the service-level drop-down menu on the “Create an Order” page. When you add and configure IPS/IDS solutions to your order, the service is automatically added for you.

If you are creating a quote or order that contains IPS/IDS solutions as well as other Cisco products or services, select the desired level of service to cover the other products on your order (for example, Cisco SMARTnet 8x5x4, Software Application Support, etc.). After you have ordered and configured the IPS/IDS solutions, you will notice that no service has been added by default to your order for this product. To add service, go to the “Line Details” screen for the IPS/IDS solution and select the IPS SVC for the product from the service-level drop-down menu at the top of the page. Then “add” the additional required service information and save your order.

**Q.** How do I order Cisco Services for IPS for my IDS-enabled blade configured within a Cisco core product (router, Cisco Catalyst switch, etc.)?

**A.** Because Cisco Services for IPS replaces Cisco SMARTnet or Cisco SP Base as a service option for IPS/IDS appliances, IPS router modules, Catalyst IPS service modules, you will notice that when you configure a router or Cisco Catalyst switch that contains an IPS/IDS product, the service program ordered for the chassis does not cascade to any IDS product(s) you have added to the chassis. To ensure signature-file coverage for each IDS product, you need to add a separate service line on your quote or order for the IPS SVC service level using the part number that corresponds to the IDS-enabled card you are ordering. In the line notes of the service line you have added, be sure to note the line number and product number of the IDS-enabled card for which you are requesting service. This ensures prompt and accurate assignment of this product to a service contract—critical for the product to be able to access and install signature files.

**Note:** If you order the IPS router modules or Catalyst IPS service module as a spare item instead of a configured item within a router or Cisco Catalyst product, you can select the “Cisco Services for IPS” service from the service-level drop-down menu at the top of the “Main Order Form” as you are adding the spare IPS router modules or Catalyst IPS service module to your order.

**Q.** As a sales person, how do I know if my customer is purchasing the correct coverage?

**A.** It is simple. When purchasing support, customers have two options:

- They may purchase your brand of maintenance service (Cisco SMARTnet equivalent deliverable) plus Cisco brand Cisco Services for IPS Standalone

or

- They may purchase Cisco Services for IPS that combines Cisco SMARTnet deliverables and signature updates

**Q.** How do I support customers who are contacting me because their IPS solutions are failing the licensing process?

A. If you have verified that your customer does not have a current Cisco Services for IPS contract you should advise them that a valid IPS contract is required and encourage them to purchase one. If your customer has a current IPS contract, then route them to the Licensing Support Team. You should also advise your customer that they can request a one time licensing key (valid for 30 days only), providing them the appropriate URL, <http://www.cisco.com/go/license>



#### Corporate Headquarters

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

#### European Headquarters

Cisco Systems International  
BV  
Haarlerbergpark  
Haarlerbergweg 13-19  
1101 CH Amsterdam  
The Netherlands  
[www-europe.cisco.com](http://www-europe.cisco.com)  
Tel: 31 0 20 357 1000  
Fax: 31 0 20 357 1100

#### Americas Headquarters

Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
USA  
[www.cisco.com](http://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](http://www.cisco.com)  
Tel: +65 6317 7777  
Fax: +65 6317 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](http://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

Copyright © 2005 Cisco Systems, Inc. All rights reserved. CCSP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, IQ Expertise, the IQ logo, IQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, Packet, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StrataView Plus, SwitchProbe, TeleRouter, The Fastest Way to Increase Your Internet Quotient, TransPath, and VCO 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 is the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0411R)