Intrusion Prevention System (IPS)

The Cisco® Intrusion Prevention System (IPS) software is an inline, network-based solution, designed to accurately identify, classify, and stop malicious traffic, including worms, spyware/adware, network viruses, and application abuse, before they affect business continuity.

The Cisco IPS Sensor software v5 combines inline prevention services with innovative technologies to improve accuracy. The result is total confidence in the provided protection of your IPS solution, without the fear of legitimate traffic being dropped. As well, the Cisco IPS solution, utilizing Cisco IPS Sensor software v5, offers comprehensive protection of your network through its unique ability to collaborate with other network security resources, providing a proactive approach to protecting your network.

The Cisco IPS Sensor software v5 helps users stop more threats with greater confidence through the use of the following elements:

- **Accurate inline prevention technologies**—Provides unparalleled confidence to take preventive action on a broader range of threats without the risk of dropping legitimate traffic. These unique technologies offer intelligent, automated, contextual analysis of your data and help ensure you are getting the most out of your intrusion prevention solution.
- **Multivector threat identification**—Protects your network from policy violations, vulnerability exploitations, and anomalous activity through detailed inspection of traffic in Layers 2 through 7.
- **Unique network collaboration**—Enhances scalability and resiliency through network collaboration, including efficient traffic capture techniques, load-balancing capabilities, and visibility into encrypted traffic.
- **Comprehensive deployment solutions**—Provides solutions for environments ranging from small and medium-sized businesses (SMBs) and branch office locations to large enterprise and service provider installations.
- **Powerful management, event correlation, and support services**—Enables a complete solution, including configuration, management, data correlation, and advanced support services. In particular, the Cisco Security Monitoring, Analysis, and Response System (MARS) identifies, isolates, and recommends precision removal of offending elements, for a networkwide intrusion prevention solution. And the Cisco Incident Control System prevents new worm and virus outbreaks by enabling the network to rapidly adapt and provide a distributed response.

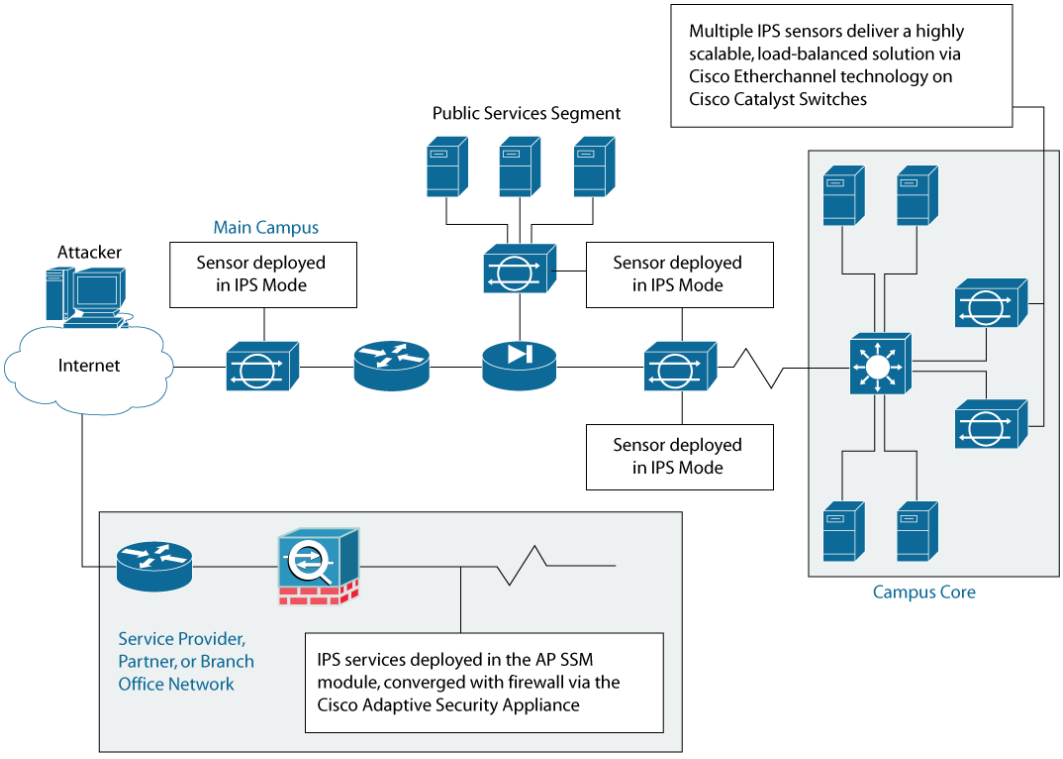
Features and Benefits

Intrusion Prevention System Services to Stop Worms and Viruses

Cisco IPS Sensor software Version 5 delivers inline IPS capabilities to Cisco IPS 4200 Series sensors; Cisco Catalyst® 6500 Series IPSM-2 modules and the AIP SSM Module for the Cisco Adaptive Security Appliance, which offers full IPS features within a converged appliance, all allowing effective worm and virus mitigation at strategic points across the network. IPS services:

- Provide support for hybrid intrusion detection system (IDS)/IPS services that allow a single sensor to operate simultaneously as an IDS sensor and an IPS sensor. Figure 1 shows how single IPS devices can be strategically deployed to deliver IDS and IPS services concurrently, using a single device. This considerably lowers total cost of ownership by alleviating the need to deploy multiple devices across the network.
- Deliver a wide array of inline packet drop actions, including the ability to drop single malicious packets, all packets within a flow that contains multiple malicious packets, and all packets from the attacker's IP address. These inline response actions complement existing response actions such as connection resets and access control list (ACL) modifications on switches, routers, and firewalls, delivering a rich set of attack mitigation techniques that work in unison to effectively stop worms and viruses.

Figure 1. Cisco IPS Sensor Software Version 5.0 Delivers Converged Code Across the IPS Product Line



Accurate Prevention Technologies

Cisco Meta Event Generator provides “on-box” correlation to deliver accurate worm classification. Cisco IPS Sensor software Version 5.0 incorporates advanced sensor-level event correlation that gives security administrators an automated method for enhancing the confidence level in the classification of malicious activity detected by the IPS sensor. This provides a mechanism that

allows for corresponding actions to deliver networkwide containment of worm and virus injection vectors, as well as worm propagation.

This classification is accomplished through the following techniques:

- **Correlation of alarms pertaining to worms that exploit multiple vulnerabilities**—Figure 2 demonstrates how multiple alarms triggered within a short time interval can be correlated, in real time, to deliver a single metaevent that delivers greater visibility into worm activity.
- **Correlation of a sequence of actions that lead up to worm infestation**—Historical trend analyses performed to characterize the lifecycle of worms often reveal a certain sequence of actions that are detected just prior to penetration. These actions occur in the "probing phase," when a chain of reconnaissance activities is performed against the target network. Cisco Meta Event Generator allows the user to define the precursors to worm penetration by specifying a logical algorithm that triggers when a particular sequence of events occurs. Such correlations lead to metaevents that give the user a greater level of confidence that the malicious activity has actually taken place.
- **Correlation of multiple events at low severity levels to result in a single event of higher severity**—As worms propagate through the network, they generate alarms of varying degrees of severity. Cisco Meta Event Generator links seemingly unrelated lower-severity alarms into a high-severity, high-risk event, enabling the user to confidently drop the associated packets (Figure 3).
- **Enhancement of alarm fidelity through simultaneous triggers based on hybrid detection algorithms**—For example, if a denial-of-service (DoS) activity is detected through the triggering of a traffic anomaly algorithm and a classical "flood" type of signature, Cisco Meta Event Generator can be used to corroborate one event with the other, thereby delivering a single metaevent that indicates a higher likelihood that the DoS activity has actually occurred. These added levels of security offer the confidence needed to deploy inline intrusion prevention without the fear of dropping legitimate traffic, as well as identifying and stopping worms in the network.

Figure 2. Cisco Meta Event Generator Correlates Multiple Events to Indicate the Presence of a Worm

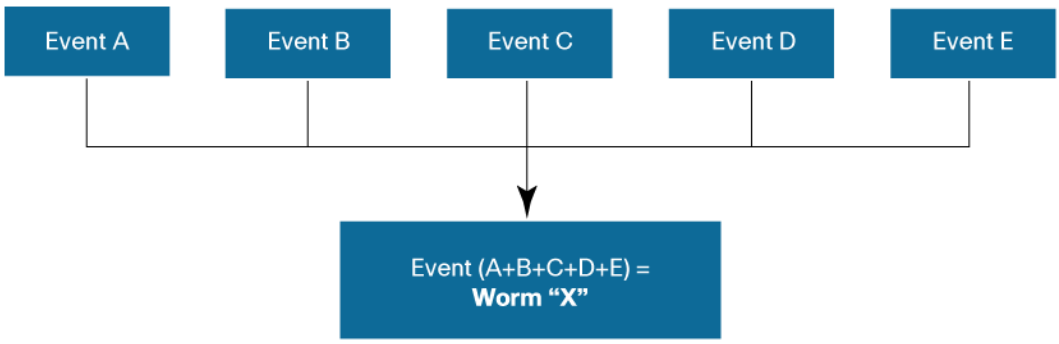
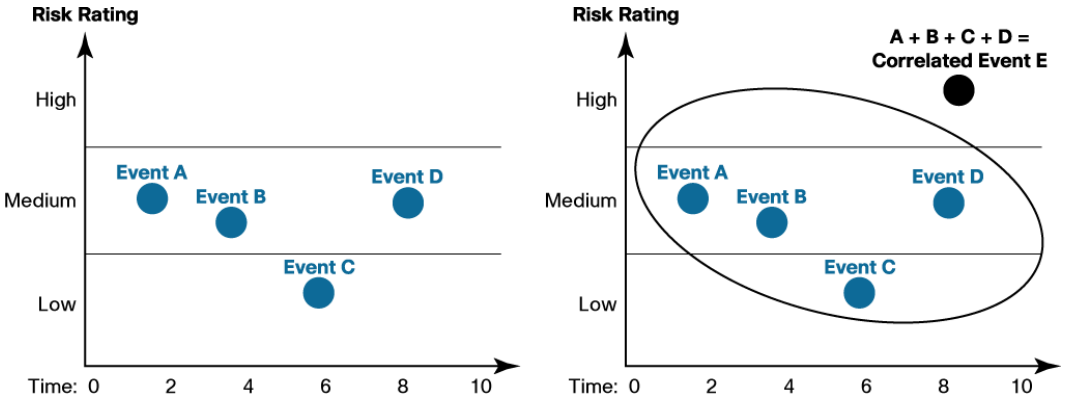


Figure 3. Cisco Meta Event Generator Correlates Multiple Events at Low Severity Levels to a Single Worm Event at a High Severity Level

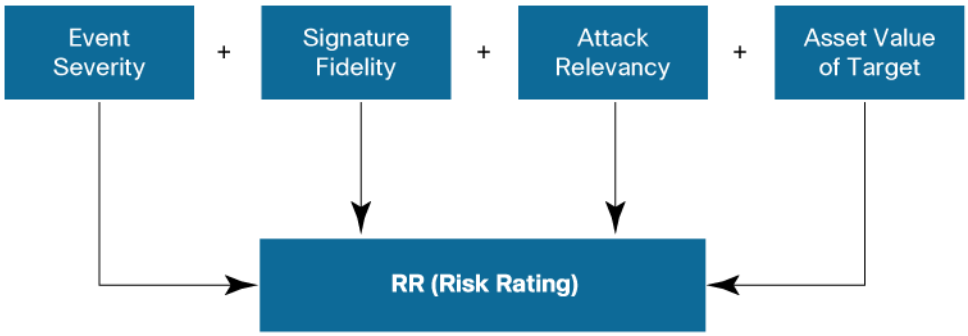


Risk rating increases the accuracy and confidence of IPS packet drop actions by delivering a risk-balanced approach to classifying threats (Figure 4). In an automated fashion, risk rating employs a unique multidimensional algorithm that takes into account several terms, including:

- **Event severity**—A user-modifiable weighted value that characterizes the damage potential of the suspect traffic
- **Signature fidelity**—A user-modifiable weighted value that characterizes the fidelity of the signature that has detected the suspect activity
- **Asset value**—A user-defined value that represents the user's perceived value of the target host
- **Attack relevancy**—An internal weighted value that characterizes any additional knowledge that the sensor may have about the target of the event

The resulting risk rating is an integer value that is dynamically applied to every IPS signature, policy, or anomaly detection algorithm. The higher the value, the greater the security risk of the trigger event for the associated alert. The result is a mechanism that allows the user to develop policies for the prevention of network attacks or to better characterize events for prioritization of further investigation. The user is empowered to make more intelligent decisions on inline IPS actions while virtually eliminating the possibility of dropping valid traffic.

Figure 4. Risk Rating Enhances the Accuracy of IPS Actions



Multivector Threat Identification

At the core of Cisco IPS Sensor software are numerous methods for the inspection and analysis of traffic in Layers 2 through 7. These methods provide comprehensive threat identification, often supporting the development of signatures to a vulnerability prior to the release of an exploit to provide you with day-zero protection. Threat identification methods include:

- **Rate limiting**—New with Version 5.1. Allows the IPS device to limit certain types of traffic by preventing them from utilizing an excessive amount of bandwidth. This feature can also signal external devices such as Cisco IOS® Software routers to perform rate limiting to accomplish the same function.
- **IPv6 detection**—New with Version 5.1. Enhanced visibility into IPv6 traffic to identify malicious traffic.
- **IP in IP detection**—New with Version 5.1. Identifies malicious traffic within mobile IP traffic.
- Stateful pattern recognition—Identifies vulnerability-based attacks through the use of multipacket inspection across all protocols, thwarting attacks that hide within a data stream.
- **Protocol analysis**—Provides protocol decoding and validation for network traffic. Cisco IPS Sensor software Version 5.0 monitors all of the major TCP/IP protocols, including but not limited to IP, Internet Control Message Protocol (ICMP), TCP, and User Datagram Protocol (UDP). It also provides stateful decoding of application-layer protocols such as FTP, Simple Mail Transfer Protocol (SMTP), HTTP, Domain Name System (DNS), remote procedure call (RPC), NetBIOS, Network News Transfer Protocol (NNTP), generic routing encapsulation (GRE), and Telnet.
- **Traffic anomaly detection**—Provides anomaly identification for attacks that may cover multiple sessions and connections, using techniques based on identifying changes in normal network traffic patterns. An example would be an ICMP flood with a predefined number of ICMP packets within a certain amount of time.
- **Protocol anomaly detection**—Identifies attacks based on observed deviations in the normal RFC behavior of a protocol or service (an HTTP response without an HTTP request, for example).
- **Layer 2 detection**—Identifies Layer 2 Address Resolution Protocol (ARP) attacks and man-in-the-middle attacks, which are prevalent in switched environments.
- **Application policy enforcement**—Provides deep analysis and control of a broad set of applications, including control of peer-to-peer, instant messaging (IM), and tunneled applications over port 80. This allows the user to make policy decisions about various traffic types and Multipurpose Internet Mail Extensions (MIME) types to help ensure that malicious traffic is disallowed from traversing the network.
- **Anti-IPS evasion techniques**—Provides traffic normalization, IP defragmentation, TCP stream reassembly, and deobfuscation for comprehensive protection against hackers attempting to evade IPSs.
- **Customizable policies**—Gives users the flexibility to create new policies or modify existing policies to meet their unique security objectives, using the innovative Cisco Threat Analysis Micro Engine (TAME) policy language.

These techniques allow Cisco IPS Sensor software to address both known and unknown attack types, including:

- **Policy violations**—Reconnaissance activity, misuse activity, and file-sharing threats.
- **Anomalous activities**—DoS activity, where an attempt is made to consume bandwidth or computing resources, resulting in the disruption of normal operations. Examples include Trinoo, TFN, and SYN floods.
- **Vulnerability exploitation**—Back Orifice, failed login attempts, and TCP hijacking.

Comprehensive Deployment Solutions

Cisco offers a wide range of network IPS deployment solutions, giving customers the ability to implement intrusion prevention in the ways that are the most effective for their environments. All solutions are designed for high availability and backed by outstanding customer support and are available in a range of performance levels, from 45 Mbps up to multiple Gbps. Deployment options include dedicated appliances, switch and router modules, and software-based solutions. The solutions are:

- Cisco IPS 4200 Series sensors—Deliver intrusion prevention using dedicated, purpose-built devices that protect multiple network segments through the use of up to eight interfaces and support dual operation simultaneously, in both passive and inline modes. These appliances provide a range of performance, from 80 Mbps up to 8 Gbps, when used in collaboration with Cisco EtherChannel® load balancing on Cisco Catalyst 6500 Series switches. The appliance models and their base performance levels are:
  - Cisco IDS 4215 Sensor: 80 Mbps
  - Cisco IPS 4240 Sensor: 250 Mbps
  - Cisco IPS 4255 Sensor: 600 Mbps
  - Cisco IDS 4250 XL Sensor: 1000 Mbps

Performance numbers are for tested intrusion detection throughput.

- **Cisco IDSM-2 Module for the Cisco Catalyst 6500 Series**—Integrates full IPS capabilities into Cisco Catalyst 6500 Series switches using a dedicated module, providing integrated protection at 600 Mbps.
- **Cisco IDS Network Module for Cisco access routers**—Integrates traditional intrusion detection into the router using Cisco IPS Sensor software Version 5.0. This provides added detection, correlation, and identification technology to effectively mitigate against and isolate threats at up to 45 Mbps.
- **Cisco Advanced Inspection and Prevention Security Services Module for Cisco ASA 5500 Series adaptive security appliances**—Provides IPS capabilities as part of the ASA 5500 Series multifunction threat mitigation solution.
- **Cisco IOS Software IPS**—Provides a focused set of IPS capabilities using Cisco IOS Software on the router.

Powerful Management, Event Correlation, and Services

Cisco uses a range of management and correlation tools and support services to provide an effective and complete IPS solution regardless of deployment size or environment.

Management Solutions

- **Command-line interface (CLI)**—A full-featured Cisco IOS Software–like CLI that provides device configuration over a Secure Shell (SSH) Protocol connection.
- **Cisco IPS Device Manager**—A single device manager, providing a secure, browser-based GUI for configuration and alarm viewing. Cisco IPS Device Manager can be easily accessed from practically any desktop, regardless of the operating system being used. The result is rapid access to data from systems throughout the enterprise. The familiar browser interface enhances ease of use, and with Secure Sockets Layer (SSL), data security is maintained.
- **CiscoWorks VPN/Security Management Solution (VMS)**—A multidevice configuration and alarm management tool offering a unified, scalable view of all security events. With CiscoWorks VMS, events from all types of security devices, including firewalls, VPNs, and IPSs, can be viewed from a single console in a browser-based GUI. Multiple security devices can be configured and managed, making it easier to manage security across the enterprise.

Additionally, CiscoWorks VMS provides enhanced security management through the inclusion of flexible reporting and notification, automated updates, and event correlation.

- **Cisco Router and Security Device Manager (SDM)**—An intuitive, Web-based device manager that provides easy and reliable deployment and management of Cisco access routers, including the Cisco IOS Software IPS feature set and Cisco IDS network modules.

Event Correlation Solutions

- **Cisco Security Monitoring, Analysis, and Response System (MARS)**—An appliance-based solution that correlates data from across the enterprise and uses your existing network and security investments to identify, isolate, and recommend precision removal of offending elements. MARS, when used in conjunction with the Cisco IPS Sensor software v5, provides a total collaborative solution, protecting your entire network infrastructure from attacks, viruses, worms, and other malicious traffic.
- **CiscoWorks Security Information Management Solution (SIMS)**—An event management solution that collects, analyzes, and correlates security event data from across the enterprise. The award-winning CiscoWorks SIMS 3.1 can help you identify and respond to more threats, more effectively, without adding additional staff.

Services

- **Cisco Services for IPS**—As a part of the Cisco Technical support services portfolio, Cisco Services for IPS combines deliverables of Cisco SMARTnet® services with access to IPS signatures into one comprehensive service program and features the following deliverables:
  - Access to Cisco IPS signatures for broad range of threats with standard release intervals
  - Access to operating system software updates such as IPS Version 5.x
  - Access to the Cisco Technical Assistance Center, any time, anywhere in the world
  - Access to Cisco.com and knowledge base
  - Options for advanced hardware replacement with or without a field engineer to replace failed hardware

For IPS-enabled mitigation devices, this service is required to process signature updates. It is also a prerequisite for the premium service Cisco Incident Control System. For more information about Cisco Services for IPS and Q&A documents, please visit http://www.cisco.com/en/US/products/ps6076/serv_group_home.html.

Other Features

- **Auto and manual sensor bypass configuration**—High availability can be achieved through numerous mechanisms for Cisco IPS sensors. Resiliency and redundancy can be delivered through unique network collaboration—for example, Hot Standby Router Protocol (HSRP) configuration and Cisco EtherChannel load balancing on Cisco Catalyst switches to divert traffic to a secondary IPS device upon the failure of a primary device. Cisco IPS Sensor software Version 5.0 also delivers on-box bypass mechanisms that allow the IPS sensor to automatically assume a fail-open condition upon certain types of sensor failure. This bypass mechanism can also be configured manually. The manual configuration requires the user to switch the sensor into bypass mode to achieve the fail-open condition. The result is increased reliability of the IPS device.
- **Support for Security Device Event Exchange (SDEE)**—SDEE is a standardized IPS communications protocol developed by Cisco for the IDS Consortium at ICSA. Through SDEE, Cisco IPS Sensor software Version 5.0 delivers a flexible, standardized API to the IPS sensor, facilitating the integration of third-party management and monitoring solutions with the Cisco IPS solution. This gives users a choice of third-party solutions to monitor events generated by Cisco IPS sensors.
- **Extensions to monitoring and notification mechanisms through the delivery of sensor alerts using Simple Network Management Protocol (SNMP) traps**—In addition to existing alarm formats, Cisco IPS Sensor software Version 5.0 offers users a tool for transmitting IPS alarms from the sensor to monitoring tools that require alarms to be generated in SNMP format. SNMP can also be used to poll the IPS sensor for critical diagnostic and status information that gives the user vital signs of the sensor's health.

System Requirements

Inline IPS services require more than one monitoring interface on Cisco IPS 4200 Series sensors. For information on upgrade options, please refer to the Cisco IPS 4200 Series data sheet at http://www.cisco.com/go/ips.

Cisco IPS Sensor software Version 5.0 is supported on the Cisco IDS 4215, 4235, 4240, 4255, and 4250 XL sensors; the IDSM-2 module for Cisco Catalyst 6500 Series switches; and the Advanced Inspection and Prevention Security Services Module for Cisco ASA 5500 Series adaptive security appliances. It is supported in promiscuous-based IDS mode only for the Cisco IDS 4210 Sensor and the Cisco IDS Network Module (NM-CIDS).

Ordering Information

Table 1 lists ordering information for Cisco IPS Sensor software Version 5.0.

Table 1. Ordering Information for Cisco IPS Sensor software Version 5.0

Part Number	Description
IPS-SW-K9-U	Cisco IPS Sensor software Version 5.0

To place an order, visit the Cisco Ordering Home Page.

For More Information

For more information about Cisco IPS Sensor software Version 5.0, contact your local account representative or visit http://www.cisco.com/go/ips.

Resources

Cisco IPS Alert Center—Provides instant access to specific information about threats, including potential countermeasures and related vulnerabilities. For more information, visit http://www.cisco.com/go/ipsalert.

For ordering details or more information about Cisco IPS solutions, visit http://www.cisco.com/go/ips.

For more information about Cisco ASA 5500 Series adaptive security appliances, visit http://www.cisco.com/go/asa.

For more information about Cisco Security MARS, visit http://www.cisco.com/go/mars or http://www.cisco.com/en/US/products/ps6241/.

For more information about Cisco IOS Software IPSs, visit http://www.cisco.com/warp/public/732/Tech/security/intrusion.

For more information about the CiscoWorks VMS, visit http://www.cisco.com/go/vms.

For more information about the CiscoWorks SIMS, visit http://www.cisco.com/en/US/products/sw/cscowork/ps5209/index.html.

For more information about Cisco SDM, visit http://www.cisco.com/en/US/products/sw/secursw/ps5318/index.html.

For more information about the Cisco Incident Control System, visit http://www.cisco.com/go/ics.

Americas 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: 408 527-0883

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Europe Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: +31 0 800 020 0791
Fax: +31 0 20 357 1100

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

C78-440386-00 11/07