

Protect the Network Infrastructure with Enhanced Cisco IOS Security Services

In today's complex network environment, networking devices offer a robust set of configuration options to meet the requirements of different businesses. These services also include a rich set of perimeter security services that protect the network from hostile intentions, as well as security services that protect the networking device itself. To address the increasing complexity of the attacks in a heightened security environment, Cisco has enhanced Cisco IOS® Security Services for both perimeter and device protection, thus ensuring the availability of the device.

The following services, designed to protect the networking device, are recent enhancements to Cisco IOS Software that compliment its already rich set of services.

Cisco AutoSecure

Security configuration necessitates a detailed understanding of the security implications of each set parameter. An error or omission in configuring these parameters could jeopardize network security with an easily-exploited hole, compromising the availability, integrity, and privacy of the network information. Many network administrators have limited technical knowledge in terms of understanding the security implication of every Cisco IOS Software feature.

Cisco AutoSecure provides vital security requirements to Enterprise and Service Provider networks by incorporating a straightforward “one touch” device

lockdown process. It simplifies the security process by enabling the rapid implementation of security policies and procedures without requiring extensive knowledge of Cisco IOS Software features or the manual execution of the Command Line Interface (CLI). This feature offers a single CLI command that instantly configures the security posture of routers and disables non-essential system processes and services, thereby eliminating potential security threats.

Cisco AutoSecure can be deployed in one of its two modes, depending on customer deployment scenario:

- Interactive mode: prompts the user with options to enable and disable services and other security features
- Non-interactive mode: automatically executes the Cisco AutoSecure command with the recommended Cisco default settings

For additional information about Cisco AutoSecure, please visit:

<http://www.cisco.com/go/autosecure>

Control Plane Policing

Even the most robust software implementations and hardware architectures are vulnerable to Denial of Service (DoS) attacks. DoS attacks are malicious acts designed to cause failures in a network infrastructure by flooding it with worthless traffic camouflaged as specific types of control packets directed at the



control plane processor. Distributed DoS attacks multiply the amount of worthless IP traffic, sometimes by as much as many gigabytes per second, by involving hundreds of sources. These IP streams contain packets that are destined for processing by the control plane of Cisco route processors. Based on the high rate of rogue packets presented to the route processor, the control plane is forced to spend an inordinate amount of time processing and discarding the DoS traffic.

To counter these and similar threats directed towards the heart of the system, the processor, Control Plane Policing can employ a programmable policing functionality on routers that rate limit (or police) traffic to the control plane. In conjunction with Cisco IOS Quality of Service (QoS) classification mechanisms, this policing functionality can be configured to identify and limit certain traffic types completely, or target only those that exceed a specified threshold level.

For additional information about Control Plane Policing, please visit:

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122s18/gtrtlmt.htm>

Silent Mode

One requirement for hacking a system is reconnaissance: gaining information about the network. Hackers conduct reconnaissance by listening to system messages, such as the status of packet delivery, which provide information (ie: IP addresses of devices).

Silent Mode is a new Cisco IOS Software feature designed to reduce the amount of information that a hacker can gather about a network. It stops the router from generating certain informational packets. For example, it suppresses the Internet Control Message Protocol (ICMP) Messages and Simple Network Management Protocol (SNMP) traps that are normally generated by the router. Like Control Plane Policing, Silent Mode leverages the familiar Modular QoS CLI (MQC) interface.

For more information about Silent Mode, please visit:

http://www.cisco.com/en/US/products/sw/iosswrel/ps1838/products_feature_guide09186a00801afad4.html

Cisco IOS Software Login Enhancements

To control accessibility to the networking device, Cisco IOS Software requires that users login to the device with a username and password; unfortunately, hackers can exploit this requirement with dictionary attacks. This is an attack in which a hacker gains access to the device by programmatically trying all combinations of username and password.

Cisco IOS Software Login Enhancements offer a new time-based dimension to user login. Network administrators can use this feature to specify a time period between retries, alleviating dictionary attacks. User account lockout can now include a time period during which a user must succeed in order to logon to the device.

For more information about Login Enhancements, please visit:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_4/gt_login.htm



CPU and Memory Thresholding Notification

CPU and memory are critical resources that mitigate the potential availability impact of the networking device. SNMP MIBs currently enable a monitoring application to inquire as to the availability of a given resource. Due to the dynamic nature of these resources, scheduled polling of these variables often delays the action necessary to maximize network availability.

Memory Thresholding Notification enables users to manage the amount of memory consumed by various resource groups. Users can specify the maximum amount of memory in bytes, or as a percentage of total processor resources. They receive notification when a resource group approaches its specified memory threshold.

With CPU Thresholding Notification, users can configure CPU utilization thresholds, which trigger a notification when exceeded. Cisco IOS Software supports two CPU utilization thresholds:

- Rising Threshold: percentage of CPU resources that trigger a CPU threshold notification when exceeded for a configured period of time
- Falling Threshold: percentage of CPU resources that trigger a CPU threshold notification when CPU usage falls below this level for a configured period of time

For more information about CPU and Memory Thresholding Notification, please visit:

- http://www.cisco.com/en/US/products/sw/iosswrel/ps1838/products_feature_guide09186a00801b1bee.html
- http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_4/gt_cput.htm

Cisco IOS Software Image Verification

Cisco currently uses MD5 hash coding to verify the integrity of Cisco IOS Software images. While the MD5 hash code is available on Cisco.com, users must go through a series of manual steps to perform image verification.

Cisco IOS Software Image Verification simplifies this process by embedding the MD5 hash coding in the image and by offering automatic MD5 hash checksum during copy, reload, and manual verification.

For more information about Image Verification, please visit:

http://www.cisco.com/en/US/products/sw/iosswrel/ps1838/products_feature_guide09186a00801afa4b.html

RAW IP Traffic Export

To perform a detailed security analysis of network traffic, many network administrators must attach a tool, such as protocol analyzers or mitigation servers. However, connection of these tools to the router currently requires inline insertion, which is operationally difficult.

RAW IP Traffic Export feature is a lightweight Cisco IOS Software feature that exports IP packets as they arrive at or leave the networking device. A designated LAN interface exports captured IP packets out of the device. The objective is to export raw IP packets in their unaltered form to a designated device (ie: packet analyzer or intrusion detection systems (IDS) device).

- Filter capability (using ACL) to help focus on exporting only interested traffic
- Sampling option reduces the traffic output volume



- User specifies an Ethernet port for exportation utilizing either a MAC/802.1q/ISL address associated with the destination host instead of an IP address.
- Syslog information is provided when the feature is activated or de-activated

For more information on Silent Mode, please visit:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_4/gt_rawip.htm

ACL IP Options Selective Drop

On most Cisco routers, a packet with IP Options is filtered and switched in software, because it requires control plane software processing. This is primarily due to the need to process the options and rewrite the IP header. This poses potential security threats, as malformed packets containing IP Options can adversely affect the performance of the device.

ACL IP Options Selective Drop allows Cisco routers to filter packets that contain IP options or to mitigate the effects of IP options on a router by dropping these packets or ignoring the processing of the IP options.

For more information on ACL IP Options Selective Drop, please visit:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s23/sel_drop.htm

Table 1 Key Cisco IOS Security Infrastructure Enhancements

Cisco IOS Software Feature	Description	Cisco IOS Software Availability
Cisco AutoSecure	<ul style="list-style-type: none"> • Automatically disables exploitable IP services and activates IP services that help defend a device or network under attack 	<ul style="list-style-type: none"> • 12.3 • 12.2(18)S
Control Plane Policing	<ul style="list-style-type: none"> • Protects the route processor from unnecessary or malicious levels of traffic, including DoS attacks 	<ul style="list-style-type: none"> • 12.3(4)T • 12.2(18)S
Silent Mode	<ul style="list-style-type: none"> • Suppresses response messages from the router's control plane, limiting network reconnaissance information available to hackers 	<ul style="list-style-type: none"> • 12.3(4)T
Raw IP Traffic Export	<ul style="list-style-type: none"> • Allows copies of inbound and outbound packets to efficiently capture packets with analysis or IDS tools by sending them out a LAN interface 	<ul style="list-style-type: none"> • 12.3(4)T • 12.2(22)S
Login Enhancements—Password Retry Delay	<ul style="list-style-type: none"> • Delays potential dictionary attacks and provides other methods of thwarting unwanted device access 	<ul style="list-style-type: none"> • 12.3(4)T • 12.2(22)S
Image Verification	<ul style="list-style-type: none"> • Replaces the manual process of validating the integrity of all downloaded Cisco IOS Software images with an automated method 	<ul style="list-style-type: none"> • 12.3(4)T • 12.2(18)S • 12.0(26)S
Memory Threshold Notifications	<ul style="list-style-type: none"> • Mitigates low-memory router conditions by sending alerts when the amount of available memory has fallen below a configured threshold 	<ul style="list-style-type: none"> • 12.3(4)T • 12.2(22)S • 12.0(26)S

Table 1 Key Cisco IOS Security Infrastructure Enhancements (Continued)

Cisco IOS Software Feature	Description	Cisco IOS Software Availability
CPU Threshold Notifications	<ul style="list-style-type: none"> Triggers a syslog notification when a specified percentage of CPU resources for a given process exceeds or falls below a certain threshold for a configured time period 	<ul style="list-style-type: none"> 12.3(4)T 12.2(22)S 12.0(26)S
Secure Shell Version 2 (SSHv2)	<ul style="list-style-type: none"> Enhances previous versions of SSH for remote network management by concealing password length, making dictionary attacks more difficult. Resolves SSHv1 vulnerability to man-in-the-middle attacks during user authentication 	<ul style="list-style-type: none"> 12.3(4)T 12.1(19)E



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

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
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
Tel: 408 526-7660
Fax: 408 527-0883

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

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

All contents are Copyright © 1992–2004 Cisco Systems, Inc. All rights reserved. CCIP, CCSP, the Cisco Arrow logo, the Cisco Powered Network mark, Cisco Unity, Follow Me Browsing, FormShare, 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 Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, the Cisco IOS logo, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherSwitch, Fast Step, GigaStack, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, MGX, MICA, the Networkers logo, Networking Academy, Network Registrar, Packet, PIX, Post-Routing, Pre-Routing, RateMUX, Registrar, ScriptShare, SlideCast, SMARTnet, StrataView Plus, Stratm, 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 U.S. and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company.
(0304R) ETMG 203153—SH 02.04