

Cisco AutoSecure

Overview

In today's complex network environment, networking devices offer a robust set of configuration options to meet the requirements of different businesses. Choosing the appropriate configuration parameters for a network is a multifaceted process: setting the proper parameters, creating the appropriate filters, and enabling and disabling an assortment of services in order to secure the networking environment and device.

Security configuration necessitates a detailed understanding of the security implications of each set parameter. An error or omission in configuring these parameters has the potential to jeopardize network security, as it could create a security hole, which can be exploited, compromising the availability, integrity, and privacy of the information connected to or through the network.

Remote workers, partners, and customers depend on networks for access to vital information, outside of traditional corporate boundaries. By incorporating a "one touch" device lockdown process, Cisco AutoSecure enables rapid implementation of security policies and procedures to ensure secure networking services. This new Cisco IOS®



Software feature simplifies the security process, thus lowering barriers to the deployment of critical security functionality.

Feature Description

Cisco AutoSecure is a new Cisco IOS Security Command Line Interface (CLI) command. Customers can deploy one of its two modes, depending on their individual needs:

- *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

Software Availability

Cisco AutoSecure is available in Cisco IOS Software Major Release 12.3 and subsequent 12.3 T releases for the Cisco 800, 1700, 2600, 3600, 3700, 7200, and 7500 Series Routers.

For additional information about Release 12.3, please visit: <http://www.cisco.com/go/release123/>

Technical Specification

Cisco AutoSecure performs the following functions:¹

1. Disables the following Global Services
 - Finger
 - PAD
 - Small Servers
 - Bootp

1. Prior to deploying Cisco AutoSecure, please check your network management application requirements. Some applications require services that may be disabled by Cisco AutoSecure.

- HTTP service
 - Identification Service
 - CDP
 - NTP
 - Source Routing
2. Enables the following Global Services
- Password-encryption service
 - Tuning of scheduler interval/allocation
 - TCP synwait-time
 - TCP-keepalives-in and tcp-keepalives-out
 - SPD configuration
 - No ip unreachable for null 0
3. Disables the following services per interface
- ICMP
 - Proxy-Arp
 - Directed Broadcast
 - Disables MOP service
 - Disables icmp unreachable
 - Disables icmp mask reply messages.
4. Provides logging for security
- Enables sequence numbers & timestamp
 - Provides a console log
 - Sets log buffered size
 - Provides an interactive dialogue to configure the logging server ip address.
5. Secures access to the router
- Checks for a banner and provides facility to add text to automatically configure:
- Login and password
 - Transport input & output
 - Exec-timeout
 - Local AAA
 - SSH timeout and ssh authentication-retries to minimum number
 - Enable only SSH and SCP for access and file transfer to/from the router
 - Disables SNMP If not being used
6. Secures the Forwarding Plane
- Enables Cisco Express Forwarding (CEF) or distributed CEF on the router, when available
 - Anti-spoofing
 - Blocks all IANA reserved IP address blocks
 - Blocks private address blocks if customer desires
 - Installs a default route to NULL 0, if a default route is not being used
 - Configures TCP intercept for connection-timeout, if TCP intercept feature is available and the user is interested
 - Starts interactive configuration for CBAC on interfaces facing the Internet, when using a Cisco IOS Firewall image,
 - Enables NetFlow on software forwarding platforms

Additional Information

Cisco IOS Security:

<http://www.cisco.com/warp/public/732/Tech/security/>

Cisco IOS Software Release 12.3:

<http://www.cisco.com/go/release123/>

Cisco Feature Navigator: <http://www.cisco.com/go/fn/>



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 © 1992–2003 Cisco Systems, Inc. All rights reserved. Catalyst, Cisco, Cisco Systems, Cisco IOS, the Cisco Systems logo, Cisco Unity, and EtherSwitch are registered trademarks or 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.
(0303R) 202925.B/ETMG 05/03