AutoSecure

Last Updated: January 26, 2012

The AutoSecure feature secures a router by using a single CLI command to disable common IP services that can be exploited for network attacks, enable IP services and features that can aid in the defense of a network when under attack, and simplify and harden the security configuration of the router.

AutoSecure enhances secure access to the router by configuring a required minimum password length to eliminate common passwords that can be common on many networks, such as “lab” and “company name.” Syslog messages are generated after the number of unsuccessful attempts exceeds the configured threshold.

AutoSecure also allows a router to revert (roll) back to its pre-AutoSecure configuration state if the AutoSecure configuration fails.

When AutoSecure is enabled, a detailed audit trail of system logging messages capture any changes or tampering of the AutoSecure configuration that may have been applied to the running configuration.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Restrictions for AutoSecure

The AutoSecure configuration can be configured at run time or setup time. If any related configuration is modified after AutoSecure has been enabled, the AutoSecure configuration may not be fully effective.

Information About AutoSecure

Securing the Management Plane

The management plane is secured by turning off certain global and interface services that can be potentially exploited for security attacks and turning on global services that help mitigate the threat of attacks. Secure access and secure logging are also configured for the router.

Caution If your device is managed by a network management (NM) application, securing the management plane could turn off some services like the HTTP server and disrupt the NM application support.

The following subsections define how AutoSecure helps to secure the management plane:

Disabling Global Services

After enabling this feature (through the **auto secure** command), the following global services are disabled on the router without prompting the user:

- Finger--Collects information about the system (reconnaissance) before an attack. If enabled, the information can leave your device vulnerable to attacks.
- PAD--Enables all packet assembler and disassembler (PAD) commands and connections between PAD devices and access servers. If enabled, it can leave your device vulnerable to attacks.
- Small Servers--Causes TCP and User Datagram Protocol (UDP) diagnostic port attacks: a sender transmits a volume of fake requests for UDP diagnostic services on the router, consuming all CPU resources.
- Bootp Server--Bootp is an insecure protocol that can be exploited for an attack.
- HTTP Server--Without secure-http or authentication embedded in the HTTP server with an associated ACL, the HTTP server is insecure and can be exploited for an attack. (If you must enable the HTTP server, you are prompted for the proper authentication or access list.)

Note If you are using Cisco Configuration Professional (CCP), you must manually enable the HTTP server through the **ip http server** command.

- Identification Service--An insecure protocol, defined in RFC 1413, that allows one to query a TCP port for identification. An attacker can access private information about the user from the ID server.
- CDP--If a large number of Cisco Discovery Protocol (CDP) packets are sent to the router, the available memory of the router can be consumed, causing the router to crash.

Caution NM applications that use CDP to discover network topology are not able to perform discovery.

- NTP--Without authentication or access-control, Network Time Protocol (NTP) is insecure and can be used by an attacker to send NTP packets to crash or overload the router. (If you want to turn on NTP, you must configure NTP authentication using Message Digest 5 (MD5) and the **ntp access-group** command. If NTP is enabled globally, disable it on all interfaces on which it is not needed.)
- Source Routing--Provided only for debugging purposes, so source routing should be disabled in all other cases. Otherwise, packets may slip away from some of the access control mechanisms that they should have gone through.

Disabling Per Interface Services

After enabling this feature, the following per interface services are disabled on the router without prompting the user:

- ICMP redirects--Disabled on all interfaces. Does not add a useful functionality to a correctly configured to network, but it could be used by attackers to exploit security holes.
- ICMP unreachables--Disabled on all interfaces. Internet Control Management Protocol (ICMP) unreachables are a known cause for some ICMP-based denial of service (DoS) attacks.
- ICMP mask reply messages--Disabled on all interfaces. ICMP mask reply messages can give an attacker the subnet mask for a particular subnetwork in the internetwork.
- Proxy-Arp--Disabled on all interfaces. Proxy-Arp requests are a known cause for DoS attacks because the available bandwidth and resources of the router can be consumed in an attempt to respond to the repeated requests that are sent by an attacker.
- Directed Broadcast--Disabled on all interfaces. Potential cause of SMURF attacks for DoS.
- Maintenance Operations Protocol (MOP) service--Disabled on all interfaces.

Enabling Global Services

After AutoSecure is enabled, the following global services are enabled on the router without prompting the user:

- The **service password-encryption** command--Prevents passwords from being visible in the configuration.
- The **service tcp-keepalives-in** and **service tcp-keepalives-out** commands--Ensures that abnormally terminated TCP sessions are removed.

Securing Access to the Router

Caution If your device is managed by an NM application, securing access to the router could turn off vital services and may disrupt the NM application support.

After enabling this feature, the following options in which to secure access to the router are available to the user:

- If a text banner does not exist, users are prompted to add a banner. This feature provides the following sample banner:

```
Authorized access only
This system is the property of ABC Enterprise
Disconnect IMMEDIATELY if you are not an authorized user!
Contact abc@xyz.com +99 876 543210 for help.
```

- The login and password (preferably a secret password, if supported) are configured on the console, AUX, vty, and tty lines. The **transport input** and **transport output**commandsare also configured on all of these lines. (Telnet and secure shell (SSH) are the only valid transport methods.) The **exec-timeout** command is configured on the console and AUX as 10.
- When the image on the device is a crypto image, AutoSecure enables SSH and secure copy (SCP) for access and file transfer to and from the router. The **timeout** *seconds* and **authentication-retries** *integer* options for the **ip ssh** command are configured to a minimum number. (Telnet and FTP are not affected by this operation and remain operational.)
- If the AutoSecure user specifies that their device does not use Simple Network Management Protocol (SNMP), one of the following functions occur:
  - In interactive mode, the user is asked whether to disable SNMP regardless of the values of the community strings, which act like passwords to regulate access to the agent on the router.
  - In non-interact mode, SNMP is disabled if the community string is “public” or “private.”

Note After AutoSecure has been enabled, tools that use SNMP to monitor or configure a device is unable to communicate with the device through SNMP.

- If authentication, authorization, and accounting (AAA) is not configured, configure local AAA. AutoSecure prompts users to configure a local username and password on the router.

Security Logging

The following logging options are available after AutoSecure is enabled. These options identify security incidents and provide ways to respond to them.

- Sequence numbers and time stamps for all debug and log messages. This option is useful when auditing logging messages.
- Logging messages can be generated for login-related events; for example, the message “Blocking Period when Login Attack Detected” is displayed when a login attack is detected and the router enters “quiet mode.” (Quiet mode means that the router does not allow any login attempts through Telnet, HTTP, or SSH.)

For more information on login system messages, see the Cisco IOS Release 12.3(4)T feature module Cisco IOS Login Enhancements .

- The **logging console critical**command, which sends system logging (syslog) messages to all available TTY lines and limits messages based on severity.
- The **logging buffered** command, which copies logging messages to an internal buffer and limits messages logged to the buffer based on severity.
- The **logging trap debugging** command, which allows all commands with a severity higher than debugging to be sent to the logging server.

Securing the Forwarding Plane

To minimize the risk of attacks on the router forward plane, AutoSecure provides the following functions:

- Cisco Express Forwarding (CEF)--AutoSecure enables CEF or distributed CEF (dCEF) on the router whenever possible. Because there is no need to build cache entries when traffic starts arriving for new destinations, CEF behaves more predictably than other modes when presented with large volumes of traffic addressed to many destinations. Thus, routers configured for CEF perform better under SYN attacks than routers using the traditional cache.

Note CEF consumes more memory than a traditional cache.

- If the TCP intercept feature is available, it can be configured on the router for connection timeout.
- If strict Unicast Reverse Path Forwarding (uRPF) is available, it can be configured on the router to help mitigate problems that are caused by the introduction of forged (spoofed) IP source addresses. uRPF discards IP packets that lack a verifiable IP source address.
- If the router is being used as a firewall, it can be configured for context-based access control (CBAC) on public interfaces that are facing the Internet.

Note At the beginning of the AutoSecure dialogue, you are prompted for a list of public interfaces.

How to Configure AutoSecure

Configuring AutoSecure

Caution Although the **auto secure**command helps to secure a router, it does not guarantee the complete security of the router.

SUMMARY STEPS

1. **enable**
2. auto secure [management | forwarding] [no-interact | full] [ntp | login | ssh | firewall | tcp-intercept]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables higher privilege levels, such as privileged EXEC mode. Enter your password if prompted.

Step 2	auto secure [management | forwarding] [no-interact | full] [ntp | login | ssh | firewall | tcp-intercept]
	
	Example:
	
	`Router#`
	`auto secure`
		A semi-interactive dialogue session begins to secure either the management or forwarding planes on the router when the **management** or **forwarding** keyword is selected. If neither option is selected, then the dialogue asks for both planes to be configured. If the **management** keyword is selected, then the management plane is secured only. If the **forwarding keyword is selected, then**the forwarding plane is secured only.
		
		If the **no-interact** keyword is selected, then the user is not prompted for any interactive configurations.
		
		If the **full** keyword is selected, then user is prompted for all interactive questions, which is the default.

Configuring Enhanced Security Access to the Router

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **security passwords min-length** *length*
4. **enable password** {*password* | [*encryption-type*] *encrypted-password* }
5. **security authentication failure rate** *threshold-rate* **log**
6. **exit** *threshold-rate* **log**
7. **show auto secure config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables higher privilege levels, such as privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**security passwords min-length** *length* **Example:** `Router(config)# security passwords min-length 6`	Ensures that all configured passwords are at least a specified length. • *length* --Minimum length of a configured password.
Step 4	**enable password** {*password* | [*encryption-type*] *encrypted-password* } **Example:** `Router(config)# enable password elephant`	Sets a local password to control access to various privilege levels.
Step 5	**security authentication failure rate** *threshold-rate* **log** **Example:** `Router(config)# security authentication failure rate 10 log`	Configures the number of allowable unsuccessful login attempts. • *threshold-rate* --Number of allowable unsuccessful login attempts. • **log** --Syslog authentication failures if the rate exceeds the threshold.
Step 6	**exit** *threshold-rate* **log** **Example:** `Router(config)# exit`	Exits configuration mode and enters privileged EXEC mode.
Step 7	**show auto secure config** **Example:** `Router# show auto secure config`	(Optional) Displays all configuration commands that have been added as part of the AutoSecure configuration.

Configuration Example for AutoSecure

The following example is a sample AutoSecure dialogue. After you enable the **auto secure** command, the feature automatically prompts you with a similar dialogue unless you enable the **no-interact** keyword. (For information on which services are disabled and which features are enabled, see the sections, "Securing the Management Plane, page 2" and "Securing the Forwarding Plane, page 5" earlier in this document.)

```
Router# auto secure
               --- AutoSecure Configuration ---
*** AutoSecure configuration enhances the security of the router but it will not make
router absolutely secure from all security attacks ***
All the configuration done as part of AutoSecure will be shown here. For more details of
why and how this configuration is useful, and any possible side effects, please refer to
Cisco documentation of AutoSecure.
At any prompt you may enter '?' for help.
Use ctrl-c to abort this session at any prompt.
Gathering information about the router for AutoSecure
Is this router connected to internet? [no]:y
Enter the number of interfaces facing internet [1]:
Interface                  IP-Address OK? Method Status
Protocol
FastEthernet0/1/0          10.1.1.1  YES NVRAM  up down
FastEthernet1/0/0            10.2.2.2  YES NVRAM  up down
FastEthernet1/1/0            10.0.0.1  YES NVRAM  up up
Loopback0                  unassigned YES NVRAM  up up
FastEthernet0/0/0            10.0.0.2  YES NVRAM  up down
Enter the interface name that is facing internet:FastEthernet0/0/0
Securing Management plane services..
Disabling service finger
Disabling service pad
Disabling udp & tcp small servers
Enabling service password encryption
Enabling service tcp-keepalives-in
Enabling service tcp-keepalives-out
Disabling the cdp protocol
Disabling the bootp server
Disabling the http server
Disabling the finger service
Disabling source routing
Disabling gratuitous arp
Enable secret is either not configured or is same as enable password
Enter the new enable secret:abc123
Configuring aaa local authentication
Configuring console, Aux and vty lines for
local authentication, exec-timeout, transport
Configure SSH server? [yes]:
Enter the domain-name:example.com
Configuring interface specific AutoSecure services
Disabling the following ip services on all interfaces:
 no ip redirects
 no ip proxy-arp
 no ip unreachables
 no ip directed-broadcast
 no ip mask-reply
Disabling mop on Ethernet interfaces
Securing Forwarding plane services..
Enabling CEF (it might have more memory requirements on some low end
platforms)
Enabling unicast rpf on all interfaces connected to internet
Configure CBAC Firewall feature? [yes/no]:yes
This is the configuration generated:
no service finger
no service pad
no service udp-small-servers
no service tcp-small-servers
service password-encryption
service tcp-keepalives-in
service tcp-keepalives-out
no cdp run
```

```
no ip bootp server
no ip http server
no ip finger
no ip source-route
no ip gratuitous-arps
no ip identd
security passwords min-length 6
security authentication failure rate 10 log
enable secret 5 $1$CZ6G$GkGOnHdNJCO3CjNHHyTUA.
aaa new-model
aaa authentication login local_auth local
line console 0
 login authentication local_auth
 exec-timeout 5 0
 transport output telnet
line aux 0
 login authentication local_auth
 exec-timeout 10 0
 transport output telnet
line vty 0 4
 login authentication local_auth
 transport input telnet
ip domain-name example.com
crypto key generate rsa general-keys modulus 1024
ip ssh time-out 60
ip ssh authentication-retries 2
line vty 0 4
 transport input ssh telnet
service timestamps debug datetime localtime show-timezone msec
service timestamps log datetime localtime show-timezone msec
logging facility local2
logging trap debugging
service sequence-numbers
logging console critical
logging buffered
interface FastEthernet0/1/0
 no ip redirects
 no ip proxy-arp
 no ip unreachables
 no ip directed-broadcast
 no ip mask-reply
 no mop enabled
interface FastEthernet1/0/0
 no ip redirects
 no ip proxy-arp
 no ip unreachables
 no ip directed-broadcast
 no ip mask-reply
 no mop enabled
interface FastEthernet1/1/0
 no ip redirects
 no ip proxy-arp
 no ip unreachables
 no ip directed-broadcast
 no ip mask-reply
 no mop enabled
interface FastEthernet0/0/0
 no ip redirects
 no ip proxy-arp
 no ip unreachables
 no ip directed-broadcast
 no ip mask-reply
 no mop enabled
ip cef
interface FastEthernet0/0/0
 ip verify unicast reverse-path
ip inspect audit-trail
ip inspect dns-timeout 7
ip inspect tcp idle-time 14400
ip inspect udp idle-time 1800
ip inspect name autosec_inspect cuseeme timeout 3600
ip inspect name autosec_inspect ftp timeout 3600
ip inspect name autosec_inspect http timeout 3600
```

```
ip inspect name autosec_inspect rcmd timeout 3600
ip inspect name autosec_inspect realaudio timeout 3600
ip inspect name autosec_inspect smtp timeout 3600
ip inspect name autosec_inspect tftp timeout 30
ip inspect name autosec_inspect udp timeout 15
ip inspect name autosec_inspect tcp timeout 3600
access-list 100 deny ip any any
interface FastEthernet0/0/0
 ip inspect autosec_inspect out
 ip access-group 100 in
!
end
Apply this configuration to running-config? [yes]:yes
Applying the config generated to running-config
The name for the keys will be:ios210.example.com
% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys ...[OK]
Router#
```

Additional References

Related Documents

Related Topic	Document Title
Login functionality (such as login delays and login blocking periods)	Cisco IOS Login Enhancements module
Additional information regarding router configuration	*Cisco IOS XE Configuration Fundamentals Configuration Guide* , Release 2
Additional router configuration commands	*Cisco IOS Configuration Fundamentals Command Reference*

RFCs

RFCs	Title
RFC 1918	Address Allocation for Private Internets
RFC 2267	*Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing*

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for AutoSecure

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 1 Feature Information for AutoSecure

Feature Name	Releases	Feature Information
AutoSecure Manageability	Cisco IOS XE Release 2.3	This feature was introduced on the Cisco ASR 1000 Series Aggregation Services Routers. By using a single command-line interface (CLI), the AutoSecure feature allows a user to perform the following functions: • Disable common IP services that can be exploited for network attacks • Enable IP services and features that can aid in the defense of a network when under attack This feature also simplifies the security configuration of a router and hardens the router configuration. The following commands were introduced or modified: **auto secure**, **security passwords min-length**, and **show auto secure config**

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned 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. (1110R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

© 2012 Cisco Systems, Inc. All rights reserved.