White Paper

Cisco AutoSecure

Globally networked businesses rely on their networks to communicate with employees, customers, partners, and suppliers. While organizations recognize the advantage of instant communication and immediate access to information advantage, many are also concern about security, and protecting access to critical network resources. The deployment and management of security solutions requires a highly skilled technical staff and sufficient time to implement a focused, disciplined, and consistent approach.

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, that can be exploited, which compromises the availability, integrity, and privacy of the network information. Many smaller customers do not have the personnel and equipment necessary to support network protection.

CISCO AUTOSECURE

Cisco® AutoSecure provides vital security requirements to Enterprise and Service Provider networks by incorporating a straightforward “one touch” device lockdown process. Cisco AutoSecure enables rapid implementation of security policies and procedures to simplify the security process, without having to understand all the Cisco® Software IOS features and execute each of the many Command Line Interface (CLI) commands manually. This feature uses a single command that instantly configures the security posture of routers and disables non-essential system processes and services thereby eliminating potential security threats.

PLATFORM SUPPORT

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at http://www.cisco.com/go/fn. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

CISCO AUTOSECURE IN-DEPTH

Cisco AutoSecure provides a variety of mechanisms that enhance security to the router itself, while also helping make users more efficient at securing Cisco routers. In general, Cisco AutoSecure focuses on two areas of network security; security of the management plane and security of the forwarding plane.

Security Relative to the Management Plane

Cisco AutoSecure addresses services and features that can help to manage the router and/or network. These services are often unneeded or go unused; as such, they should be disabled. Cisco AutoSecure helps secure the management plane by:

- Disabling often unnecessary, and potentially insecure global services
- Enabling certain services that help further secure often necessary global services
- Disabling often unnecessary, and potentially insecure interface services, which can be configured on a per interface level
- Securing administrative access to the router
- Enabling appropriate security-related logging

Security Relative to the Forwarding Plane

Cisco AutoSecure additionally helps minimize attacks on the router forwarding plane.

It enables Cisco Express Forwarding (CEF) a scalable, distributed, advanced Layer 3 IP switching technology designed to meet the performance requirements of the Internet and Enterprise networks.

CISCO AUTOSECURE MODES

Cisco AutoSecure allows two modes of operation; interactive and non-interactive.

- **Interactive Mode—**prompts users to select their own configuration of router services and other security-related features.
- **Non-Interactive Mode—**configures the router's security-related features based on a set of Cisco defaults.

Interactive mode provides for greater control over the router security-related features than the non-interactive mode. However, when a user needs to quickly secure a router without much human intervention, the non-interactive mode is appropriate.

CISCO AUTOSECURE COMMAND

Cisco AutoSecure is a single privileged EXEC command that quickly and easily eliminates many potential security threats.

The **`auto secure`** command guides users through a semi-interactive session (also known as the AutoSecure dialogue) to secure the management and forwarding planes. This command gives users the option to secure the management or forwarding plane; if neither is selected, the dialogue will ask the user to configure both planes.

This command also allows you to go through all noninteractive configuration portions of the dialogue before the interactive portions. The noninteractive portions of the dialogue can be enabled by selecting the optional no-interact keyword.

The syntax for this command is as follows:

`auto secure [management | forwarding] [no-interact]`

Command Option	Description
management	(Optional.) Only the management plane will be secured.
forwarding	(Optional.) Only the forwarding plane will be secured.
no-interact	(Optional.) The user will not be prompted for any interactive configurations. It will automatically apply the changes to running-config. **Note:** No interactive configurations will be configured, including username or passwords.

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

Restrictions

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

USING CISCO AUTOSECURE

Cisco routers support many network services that may not be required in certain networks. Turning off or restricting access to these services greatly improves network security. One of the most basic rules of router security is to provide only those services the network requires. Enabling unused network services increases the possibility of malicious attacks.

The following section explains how to use Cisco AutoSecure to lockdown a router. Included are screen shot examples with explanations of the configurable settings. The screens are organized by function in the sequence presented to the user; explanations follow each screen.

Getting Started with Cisco AutoSecure

After you enter the **`auto secure`** EXEC command, the feature will automatically prompt you with a similar dialogue unless you enable the **`no interact`** keyword. You can abort the session anytime by pressing **`Ctrl-C`**, or press **"?"** to get help.

Cisco AutoSecure begins by gathering information about the router.

```
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
```

Cisco AutoSecure—Interface Selection

Cisco AutoSecure first asks questions directly related to how the router is connected to the Internet.

```
Is this router connected to internet? [no]: y
Enter the number of interfaces facing internet [1]: 1
Interface     IP-Address      OK? Method Status  Protocol
Ethernet0/0   10.0.2.2        YES NVRAM  up      up
Ethernet0/1   172.30.2.2      YES NVRAM  up      up

Enter the interface name that is facing internet: Ethernet0/1
```

Cisco AutoSecure needs to know the following:

- Is the router going to be connected to the Internet?
- How many interfaces are connected to the Internet?
- What are the names of the interfaces connected to the Internet?

Cisco AutoSecure—Securing Management Plane Services

Next, Cisco AutoSecure automatically secures management plane services.

```
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
```

The following list describes router global services.

Global Services	Description
Finger	• The Finger protocol (port 79) allows users throughout the network to get a list of the users currently using a particular routing device. The information displayed includes the processes running on the system, the line number, connection name, idle time, and terminal location. This information is provided through the Cisco IOS Software **show users** EXEC command. Unauthorized persons can use this information to plan malicious damage. This service should be disabled if not used. • Cisco AutoSecure disables this service to keep intruders from seeing who is logged into the router and from what location. • If this service is desired for your environment, enter the **service finger** command.
PAD	• This service is used to enable X.25 packet assembler and disassembler (PAD) commands and connections between the routers and other network devices. One example of where the PAD service is used is when a router must process traffic between a remote IP user and an X.25 host. The PAD service should be disabled when not required for X.25 network operations. • Cisco AutoSecure disables this service to prevent intruders from accessing the X.25 PAD command set on the router. • If this service is desired for your environment, enter the **service pad** command.
UDP and TCP Small Servers	• The TCP and UDP protocol standard includes a recommended list of simple services that hosts should provide. When enabled, it can leave the router vulnerable to TCP and User Datagram Protocol (UDP) diagnostic port attacks; where a sender transmits a volume of fake requests for UDP diagnostic services on the router, consuming all CPU resources. Although most abuses of the small services can be avoided or made less dangerous by using anti-spoofing access lists, the services should almost always be disabled in any router that is part of a firewall or lies in a security-critical part of the network. Since the services are rarely used, the best policy is usually to disable them on all routers. • Cisco AutoSecure disables the UDP and TCP small servers' service to prevent attackers from using those services in DoS attacks. • If this service is desired for your environment, enter the **service tcp-small-servers** and/or **service udp-small-servers** commands.
Password Encryption	• Cisco AutoSecure automatically encrypts passwords preventing them from being visible in the configuration. This feature should always be enabled. • Cisco AutoSecure uses the **service password-encryption** command to encrypt the password.
TCP Keepalives	• Idle logged-in user sessions can be susceptible to unauthorized access and hijacking attacks. • By default, Cisco routers do not continually test whether a previously connected TCP endpoint is still reachable. If one end of a TCP connection idles out or terminates abnormally (crashes, reloads, etc.), the opposite end of the connection may still believe the session is available. These "orphaned" sessions use up valuable router resources. Attackers have been known to take advantage of this weakness to attack Cisco routers. • To remedy this situation, Cisco routers can be configured to send periodic keepalive messages to ensure that the remote end of a session is still available. If the remote device fails to respond to the keepalive message, the sending router will clear the connection. This immediately frees router resources for other more important tasks. Keepalives are important because they help guard against orphaned sessions. • Cisco AutoSecure enables TCP keepalives in/out. Doing this ensures that abnormally terminated TCP sessions are removed which allows the router to quickly cleanup idle TCP sessions. • Cisco AutoSecure uses global configuration commands **service tcp-keepalives-in** and **service tcp-keepalives-out**.

Global Services	Description
CDP	• Cisco Discovery Protocol is a Cisco proprietary device discovery protocol that runs over Layer 2 (the data link layer) on all Cisco-manufactured devices (routers, bridges, access servers, and switches) and allows network management applications to discover Cisco devices that are neighbors of already known devices. This service is enabled by default. • With Cisco Discovery Protocol network management applications can learn the device type and the simple network management protocol (SNMP) agent address of neighboring devices running lower-layer, transparent protocols. This feature enables applications to send SNMP queries to neighboring devices. If a router has SNMP enabled and has used Cisco Discovery Protocol to discover its neighbors, an attacker may be able to access important routing information using an SNMP server. • Cisco Discovery Protocol is useful in specialized situations, but can be detrimental to security if left enabled. It can be disabled entirely or at an interface level. • Cisco AutoSecure disables this service to prevent attackers from exploiting a recently discovered Cisco Discovery Protocol security threat or DoS attacks. • If this service is desired for your environment, enter the **cdp run** command. If you need to use Cisco Discovery Protocol, restrict its use to only those interfaces that require it. In this case globally re-enable Cisco Discovery Protocol by entering the **cdp run** global configuration command, and then use the **no cdp enable** command in interface configuration mode to turn off Cisco Discovery Protocol interfaces.
Bootp Server	• Bootp is a user datagram protocol (UDP) that can be used by Cisco routers to access copies of Cisco IOS Software on another Cisco router running the Bootp service. In this scenario, one Cisco router acts as an Cisco IOS Software server that can download the software to other Cisco routers acting as Bootp clients. In reality, this service is rarely used and can allow an attacker to download a copy of a router's Cisco IOS Software. It is recommended to disable this service. • Cisco AutoSecure disables this service to prevent attackers from using it to generate DoS attacks. • If this service is desired for your environment, enter the **ip bootp server** global configuration command.
HTTP Server	• Hypertext Transfer Protocol (HTTP) is used for retrieving web pages and many related tasks. Most recent Cisco IOS Software releases support remote configuration and monitoring using the World Wide Web's HTTP protocol. In general, HTTP access is equivalent to interactive access to the router. The authentication protocol used for HTTP is equivalent to sending a cleartext password across the network, and, unfortunately, there is no effective provision in HTTP for challenge-based or one-time passwords. This makes HTTP a relatively risky choice for use across the public Internet. The default setting for this service is Cisco device dependent. • If Web-based administration is not required, disable the HTTP service. • If you choose to use HTTP for management, you should restrict access to appropriate IP addresses using the **ip http access-class** command. You should also configure authentication using the **ip http authentication** command. As with interactive logins, the best choice for HTTP authentication is probably to use a TACACS+ or RADIUS server. It is advisable to avoid using the "enable" password as an HTTP password. • Cisco AutoSecure disables this service to prevent attackers from accessing the HTTP router administrative access interface. **Note:** If you are using Security Device Manager (SDM), you must manually enable the HTTP server via the **ip http server** command. Otherwise SDM will not work for this router.

Global Services	Description
Source Routing	• The IP protocol supports source routing options that allow the sender of an IP datagram to control the route that a datagram will take toward its ultimate destination, and generally the route that any reply will take. These options are rarely used for legitimate purposes in real networks. Some older IP implementations do not process source-routed packets properly, and it may be possible to crash machines running these implementations by sending datagrams to them with source routing options. Unless a network depends on source routing, Cisco recommends disabling this service. • Cisco AutoSecure disables this service to prevent packets from slipping away from the access control mechanisms that they should have normally go through. • If this service is desired for your environment, enter the **ip source-route** command.
Gratuitous ARPs	• Most Cisco routers (by default) will send out a gratuitous Address Resolution Protocol (ARP) message whenever a client connects and negotiates an IP address over a PPP connection. Gratuitous ARP is the main mechanism used in ARP poisoning attacks. You should disable gratuitous ARPs unless otherwise needed. • Cisco AutoSecure disables gratuitous ARPs to prevent the router from granting the broadcast request for the IP address of its interfaces. • If this service is desired for your environment, enter the **ip gratuitous-arps** command in global configuration.

Essentially, Cisco AutoSecure disables the most common attack vectors by shutting down their associated global router services. The global services listed in this figure have been designated as high risk attack vectors.

Cisco AutoSecure—Creating a Security Banner

Next, Cisco AutoSecure prompts you to create a banner to be shown every time someone accesses the router.

The login banner serves as a legal notice, such as “no trespassing” or a “warning” statement. A proper legal notice protects the ability of the owning organization to pursue legal actions against the attackers. Consult your legal staff for suitable language to use in your notice applied to the banner.

This is the same as using the **`banner motd`** command in global configuration mode. The following is an example of how this portion of the Cisco AutoSecure dialogue appears.

```
Here is a sample Security Banner to be shown at every access
to device. Modify it to suit your enterprise requirements.

Authorized Access only

  This system is the property of So-&-So-Enterprise.

  UNAUTHORISED ACCESS TO THIS DEVICE IS PROHIBITED.

  You must have explicit permission to access this

  device. All activities performed on this device

  are logged and violations of this policy result

  in disciplinary action.

Enter the security banner {Put the banner between

k and k, where k is any character}:

#This system is the property of Cisco Systems, Inc.

UNAUTHORIZED ACCESS TO THIS DEVICE IS PROHIBITED.#
```

Customize the banner by editing between the two delimiting characters of your choice. In this example, pound (#) characters are used as delimiters.

Cisco AutoSecure—Configuring Passwords, AAA, SSH Server, and Domain Name

Next, Cisco AutoSecure prompts you to configure local authentication, SSH server, router hostname, and the domain name.

```
Enable secret is either not configured or is same as enable
password
Enter the new enable secret:sU@c1cs0!


Configuration of local user database
Enter the username:aDm198736
Enter the password:sHm9$n3p#
Configuring aaa local authentication
Configuring console, Aux and vty lines for
local authentication, exec-timeout, transport


Configure SSH server? [yes]: y
Enter the hostname:Ralb9f4
Enter the domain-name: cisco.com
```

The following list describes these settings.

Global Services	Description
Enable Secret	• Cisco AutoSecure checks the router to determine if the enable secret password is the same as the enable password or if it has not been configured at all. If either is true, you are prompted to enter a new enable secret password. • Avoid using dictionary words, names, phone numbers, and dates. Better passwords are greater than 8 characters and include at least one of each of the following: lowercase letters, uppercase letters, digits, and special characters. • Cisco AutoSecure verifies the minimum password length is compliant with the settings of the **security passwords min-length** command.

Global Services	Description
AAA Local Authentication	Cisco AutoSecure determines whether a user account and password exists for local Authentication, Authorization, and Accounting (AAA). If neither is true, you are prompted to enter a new username/password combination and then, AAA local authentication is enabled. Cisco AutoSecure also configures the routers console, Auxiliary, and VTY lines for local authentication, EXEC timeouts, and transport. Many commands are executed, some include: • Cisco AutoSecure creates the **username** *login_name* **password** *login_password* specified by the user. • Console Line—**line con 0** • Auxiliary Line—**line aux 0** • VTY Lines—**line vty 0 4** • **login local** is used on all lines
SSH Server	• Secure Shell (SSH) provides secure login sessions and other communications between two untrusted hosts over an insecure network by encrypting the entire session. SSH provides support for password and RSA authentication. SSH is a secure replacement for classic telnet, rsh, rlogin and rcp. • Cisco AutoSecure asks you if you want to configure the router to act as a SSH server. If you answer “yes”, the SSH timeout (**ip ssh time-out**) will automatically be configured to 60 seconds and the SSH authentication retries (**ip ssh authentication-retries**) to 2. • To act as an SSH server, the router must possess a RSA key for authentication. The RSA key is generated from the router hostname and domain name combination. Therefore the hostname and domain name must be defined. Cisco AutoSecure prompts for these settings next when SSH server is configured; otherwise these fields are not displayed in the Cisco AutoSecure dialogue. • Cisco AutoSecure uses **crypto key generate rsa** command to generate the RSA key. It will display the name of the key. By default, the SSH service will be present on the router whenever an RSA key pair exists.
Hostname	• When you answer “yes” to SSH server and the default “Router” hostname exists, this interactive prompt is displayed. • This is a required entry for the SSH server. Cisco AutoSecure prompts for a unique hostname for this router. It will not accept “Router” to generate RSA keys for an SSH server. **Note:** Change the hostname of the router to a name that does not give away that it is a Cisco router. Make it hard for hackers. Use the **hostname** command if you do not configure a SSH server.
Domain-Name	• When you answer “yes” to SSH server, this interactive prompt displays. • This is a required entry for SSH server. Cisco AutoSecure prompts for the domain in which this router belongs. This is a requirement in order to generate RSA keys for an SSH server. Use the **ip domain name** command if you do not configure a SSH server, but need to configure the domain name.

Cisco AutoSecure—Configuring Interface Specific Services

Next, Cisco AutoSecure automatically disables specific IP services on all interfaces.

```
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
```

The following list describes these settings.

Global Services	Description
IP Redirects	• An ICMP redirect message instructs hosts on a network to use a specific router as its path to a particular destination. In a properly functioning IP network, a router will send redirects only to hosts on its own local subnets, no host will ever send a redirect, and no redirect will ever be sent more than one network hop away. These messages are useful for diagnosis. An attacker may use this as a method to map the network. • It can be beneficial to filter out incoming ICMP redirects messages at the input interfaces of any router that lies at an untrusted border. For better security, disable these messages at all interfaces. • Cisco AutoSecure disables IP redirects on each interface using the **no ip redirect** interface configuration command.
IP Proxy ARP	• Network hosts use the Address Resolution Protocol (ARP) to translate network addresses into media access control (MAC) addresses A router act as an intermediary for ARP, by responding to ARP queries. This service is called proxy ARP. • When proxy ARP is enabled on a Cisco router, it allows that router to extend the network (at Layer 2) across multiple interfaces (LAN segments). Because proxy ARP allows hosts from different LAN segments to look like they are on the same segment, proxy ARP is only safe when used between trusted LAN segments. • Attackers can leverage the trusting nature of proxy ARP by spoofing a trusted host and then intercepting packets. You should always disable proxy ARP on router interfaces that do not require it, unless the router is being used as a LAN bridge. • Cisco AutoSecure disables IP proxy ARP to prevent Ad-hoc routing. It uses the **no ip proxy-arp** interface configuration command on each interface.
IP Unreachables	• This service notifies senders via messages of incorrect IP addresses. These messages are useful for diagnosis. Attackers can use ICMP unreachable messages to map your network. • It can be beneficial to filter out incoming ICMP unreachable messages at the input interfaces of any router that lies at an untrusted border. For better security, disable these messages at all interfaces. • Cisco AutoSecure disables IP unreachables by using the no ip unreachable interface configuration command on each interface.

Global Services	Description
IP Directed-Broadcast	• An IP directed broadcast is a datagram sent to the broadcast address of a subnet that is not directly attached to the sending machine. The directed broadcast is routed through the network as a unicast packet until it arrives at the target subnet, where it is converted into a link-layer broadcast. Because of the nature of the IP addressing architecture, only the last router in the chain, which is connected directly to the target subnet, can conclusively identify a directed broadcast. • IP directed broadcasts are used in the extremely common and popular smurf Denial of Service (DoS) attacks. In a smurf attack, the attacker sends ICMP echo requests from a falsified source address to a directed broadcast address, causing all the hosts on the target subnet to send replies to the falsified source. By sending a continuous stream of such requests, the attacker can create a much larger stream of replies, which can completely inundate the host whose address is being falsified. • This service should be disabled on all interfaces when not needed to prevent smurf and DoS attacks. • Cisco AutoSecure disables IP directed broadcasts using the **no ip directed-broadcast** command in interface configuration mode on each interface.
IP Mask Replies	• This service tells the router to respond to ICMP mask requests by sending ICMP Mask Reply messages containing the interface's IP address mask. These messages are useful for diagnosis. Attackers can use IP mask reply messages to map the network. • It is beneficial to filter out IP mask reply messages at the input interfaces of any router that lies at an untrusted border. For better security, disable these messages at all interfaces. • Cisco AutoSecure disables IP mask replies using the **no ip mask-reply** command in interface configuration mode on each interface.

Cisco AutoSecure—Securing Forwarding Plane Services

Next, Cisco AutoSecure secures the router forwarding plane.

```
Securing Forwarding plane services..

Enabling CEF (it might have more memory requirements on some
low end platforms)
```

The following list describes these settings.

Forwarding Services	Description
CEF	Cisco Express Forwarding is an advanced Layer 3 IP switching technology that defines the fastest method a Cisco router can forward packets from ingress to egress interfaces. Routers configured for Cisco Express Forwarding perform better under SYN flood attacks (directed at hosts, not the routers themselves) than routers configured using a standard cache. Cisco AutoSecure enables Cisco Express Forwarding if the router platform supports this type of caching using the **ip cef** global configuration command.

Cisco AutoSecure—Configuring Ingress Filtering

Next, Cisco AutoSecure performs several steps to continue configuring ingress filtering.

```
Enabling unicast rpf on all interfaces connected to internet


Configure CBAC Firewall feature? [yes/no]: y
```

The following list describes these settings.

Forwarding Services	Description
Unicast RFP	• Unicast Reverse Path Forwarding (RPF) is an input function on an interface that can be set to check if the source address is reachable by the interface that received it, or is reachable by any interface. Unicast RFP is a defense against spoofing and DoS attacks. • Unicast RFP depends on Cisco Express Forwarding. If the router does not support Cisco Express Forwarding, then you cannot use Unicast RFP. Unicast RFP is best suited for routers that act as a boundary between two networks (i.e filtering edge router between a LAN and the Internet). When used properly, it can provide a better performance than an access list for ingress and egress filtering. • Cisco AutoSecure automatically configures strict Unicast RPF if the router platform supports this function. It configures all interfaces connected to the Internet by using the **ip verify source reachable-via interface** command. This helps drop any source-spoofed packets.
CBAC Firewall	Context-based Access Control (CBAC) Firewall is an optional Cisco IOS Software feature set. When installed and configured, it prevents unauthorized external individuals to access the internal network, while providing internal users with secure access control and for all traffic across network perimeters. CBAC enhances security by scrutinizing both source and destination addresses and by tracking each application's connection status. Cisco AutoSecure asks if you want to enable generic CBAC inspection rules on all interfaces connected to the Internet. If you answer “yes”, a set of generic inspect rules are assigned to Internet facing router interfaces. Cisco AutoSecure configures the following for CBAC: • “autosec_inspect” inspection rules set. • “autosec_firewall_acl” extended-named ACL. • Applies the CBAC “autosec_inspect” inspection rule set to the outbound side of all Internet-facing router interfaces. • It also enables audit-trail logging to provide a record of network access through the Cisco IOS Firewall, including illegitimate access attempts, and inbound and outbound services.

Checking Configuration and Running-Config

Finally, Cisco AutoSecure displays the changes as they will be applied to the router running configuration. The output displayed in the picture below does not show the entire output. Refer to the “Configuration Generated Output” section for a complete listing of the changes.

After the output is displayed you are prompted as to whether you wish to apply these changes now.

- If the configuration is acceptable, answer “yes” to the “Apply this configuration to running-config?”
- If the configuration is not acceptable, answer “no” and AutoSecure aborts with no changes made to running-config.

```
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
.
.
.
Apply this configuration to running-config? [yes]: y
```

Configuration Generated Output

The following is an example of how this portion of the AutoSecure dialogue appears:

Note: Notes have been inserted into this example to help you understand what AutoSecure is doing at various points. These notes are not part of the router AutoSecure CLI output.

This is the configuration generated.

Note: Here AutoSecure disables several router global services that are considered possible attack vectors, and enables other global services that help protect the router and the network.

```
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
```

Note: Next, AutoSecure creates a banner to be displayed upon any access to the router. This banner message contains the text you provided during the AutoSecure script.

```
banner #This system is the property of Cisco Systems, Inc.
UNAUTHORIZED ACCESS TO THIS DEVICE IS PROHIBITED.#
```

Note: Here AutoSecure sets a minimum password length of 6 characters. You are not prompted to do this in the AutoSecure script. This is performed automatically by AutoSecure.

```
security passwords min-length 6
```

Note: Next, AutoSecure configures an authentication failure rate of 10. This allows a user 10 failed log in attempts before the router sends an authentication failure event to the logger (router log or Syslog server). You are not prompted to do this in the AutoSecure script. This is performed automatically by AutoSecure.

```
security authentication failure rate 10 log
```

Note: Next , AutoSecure configures the enable secret password you specified during the AutoSecure script. Enable secret uses a MD-5 hashing mechanism (denoted by the number “5”).

```
enable secret 5 $1$D5gC$4X79guFOe4rTOTqJgngZ0
```

Note: Next, AutoSecure configures the local user account you specified during the AutoSecure script. Notice that this password is encrypted using a Cisco proprietary Vigenere-based cipher (denoted by the number “7”). This is the result of AutoSecure automatically running the **service password-encryption** command earlier.

```
username aDm198736 password 7 0832585B0D1C0B0343
```

Note: Next, AutoSecure enables AAA local authentication.

```
aaa new-model
aaa authentication login local_auth local
```

Note: Next, AutoSecure configures console line 0 for local authentication, an EXEC session timeout after 5 minutes of idle time, and outgoing Telnet connections.

```
line console 0
 login authentication local_auth
 exec-timeout 5 0
 transport output telnet
```

Note: Next, AutoSecure configures auxiliary line 0 for local authentication, an EXEC session timeout after 10 minutes of idle time, and outgoing Telnet connections.

```
line aux 0
 login authentication local_auth
 exec-timeout 10 0
 transport output telnet
```

Note: Next, AutoSecure configures VTY lines 0-4 for local authentication and incoming Telnet connections.

```
line vty 0 4
 login authentication local_auth
 transport input telnet
```

Note: Next, AutoSecure configures the router hostname that you specified in the AutoSecure script.

```
hostname Ralb9f4
```

Note: Next, AutoSecure configures the router domain that you specified in the AutoSecure script.

```
ip domain-name cisco.com
```

Note: Next, AutoSecure generates a pair of general-purpose RSA keys. These keys will are used by SSH.

```
crypto key generate rsa general-keys modulus 1024
```

Note: Next, AutoSecure sets the SSH time-out timer to 60 seconds. This setting applies to the SSH negotiation phase and determines how long the router waits for a SSH client to respond. Once the EXEC session starts, the standard timeouts configured for the VTY lines apply.

```
ip ssh time-out 60
```

Note: Next, AutoSecure configures the SSH authentication-retries for 2 failed attempts, after which the interface will be reset.

```
ip ssh authentication-retries 2
```

Note: Next, AutoSecure configures VTY lines 0-4 to support both SSH and Telnet incoming connections. Note that Telnet was previously configured for the VTY lines. This step simply adds SSH to the possible list of incoming connection types.

```
line vty 0 4
 transport input ssh telnet
```

Note: Next, AutoSecure configures the router logging facility for more detailed security logging than is typically found in Cisco routers.

```
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
```

Note: Next, AutoSecure disables services that are considered security threats on all router interfaces.

```
int Ethernet0/0
no ip redirects
 no ip proxy-arp
 no ip unreachables
 no ip directed-broadcast
 no ip mask-reply

int Ethernet0/1
 no ip redirects
 no ip proxy-arp
 no ip unreachables
 no ip directed-broadcast
 no ip mask-reply
```

Note: Next, AutoSecure enables Cisco Express Forwarding to aid in router performance during SYN flood attacks.

```
ip cef
```

Note: Next, AutoSecure creates an extended-numbered ACL (100). This ACL permits UDP bootstrap protocol client (bootpc) packets from any source to any destination. This ACL is used by Unicast Reverse Path Forwarding on Internet-facing router interfaces.

```
ip access-list extended 100
 permit udp any any eq bootpc
```

Note: Next, AutoSecure enables Unicast Reverse Path Forwarding (URPF) strict checking mode using ACL 100 on all Internet-facing router interfaces. Because ACL 100 permits bootpc packets, spoofed bootpc packets will be forwarded to the destination address. The forwarded bootpc packets are counted in the interface statistics.

```
interface Ethernet0/1
 ip verify unicast source reachable-via rx 100
```

Note: Next, AutoSecure enables CBAC audit-trail logging to provide a record of network access through the IOS Firewall, including illegitimate access attempts, and inbound and outbound services.

```
ip inspect audit-trail
```

Note: Next, AutoSecure configures the DNS idle timeout for 7 seconds.

```
ip inspect dns-timeout 7
```

Note: Next, AutoSecure configures the TCP idle timeout for 14400 seconds (240 minutes).

```
ip inspect tcp idle-time 14400
```

Note: Next, AutoSecure configures the UDP idle timeout to 1800 seconds (30 minutes)

```
ip inspect udp idle-time 1800
```

Note: Next, AutoSecure configures the CBAC "autosec_inspect" inspection rules set.

```
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
```

Note: Next, AutoSecure creates the "autosec_firewall_acl" extended-named ACL. This ACL permits UDP bootpc packets from any source to any destination while denying all other packets.

```
ip access-list extended autosec_firewall_acl
 permit udp any any eq bootpc
 deny ip any any
```

Note: Next, AutoSecure applies the CBAC "autosec_inspect" inspection rule set to the outbound side of all Internet-facing router interfaces. Here the inspection rule set is applied on the outbound side of Ethernet0/1.

```
interface Ethernet0/1
 ip inspect autosec_inspect out
end
```

Note: Finally, AutoSecure asks you if you want to apply these changes to the router running-configuration. Roll-back of the AutoSecure configuration is currently unavailable; thus, you should always save the running configuration before committing to the AutoSecure configuration.

```
Apply this configuration to running-config? [yes]: y
```

Note: If SSH server is configured, AutoSecure generates RSA keys from the hostname and domain name settings. The default "Router" hostname will cause an error when trying to generate keys.

```
Applying the config generated to running-config
The name for the keys will be: Ralb9f4.cisco.com
% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys ...[OK]
```

VERIFYING AUTOSECURE

There are two ways to verify the router security configuration is running; an IOS command and performing a security audit using Cisco Security Device Manager (SDM).

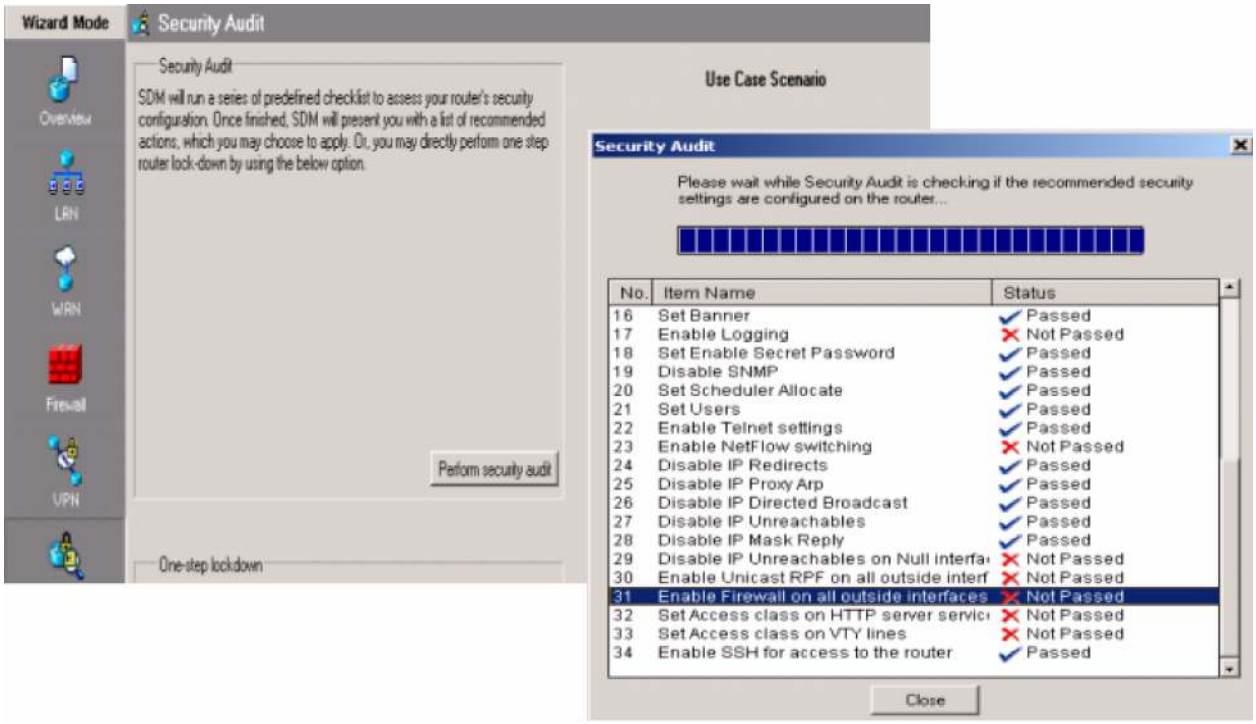
IOS Command

Use the IOS EXEC command **show auto secure config** to verify that the AutoSecure feature is working successfully. It displays all the configuration commands that have been added as part of the AutoSecure configuration. The output is the same as the configuration generated output (displayed in the previous section).

Security Device Manager (SDM) Audit Tool

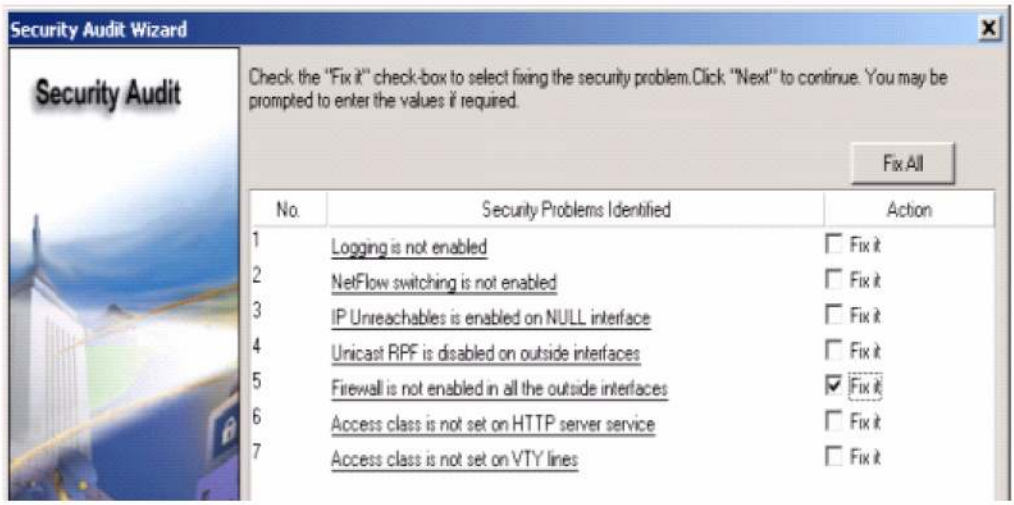
SDM comes free with many Cisco router platforms and is supported by the same software releases that support AutoSecure. It is a browser-based GUI management tool for the router. It has many wizards to simplified router and security configuration. It has a Security Audit wizard.

The SDM Security Audit feature examines router configuration just like AutoSecure. Then the Security Audit wizard tests your router configuration to determine which possible security vulnerabilities may exist. A screen showing the progress of this action appears, listing all of the configuration options being tested for, and whether or not the current router configuration passes those tests.



Vulnerable items found by SDM audit are marked in red as “Not Passed”.

Next the Security Audit Report Card screen appears. It shows a list of possible security problems.



You can click on the security problem identified to learn more about the vulnerability. You can check the “Fix it” boxes next to any problems that you want SDM to fix or elect to “fix all”. It will automatically secure all vulnerabilities found that the user selected to fix (or all of them). It uses same logic as AutoSecure to lock down vulnerabilities.

To learn more about SDM refer to http://www.cisco.com/go/sdm/.

CONFIGURATION EXAMPLES

Sample Configuration: Typical Router Configuration Pre-AutoSecure

The following example shows the router configuration just prior to applying the AutoSecure configuration changes:

```
version 12.3
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Router
!
no logging console
enable password cisco
!
memory-size iomem 15
ip subnet-zero
!
no ip domain lookup
!
ip audit notify log
ip audit po max-events 100
!
```

```
no voice hpi capture buffer
no voice hpi capture destination
!
interface Ethernet0/0
 ip address 10.0.2.2 255.255.255.0
 half-duplex
!
interface Ethernet0/1
 ip address 172.30.2.2 255.255.255.0
 half-duplex
!
router eigrp 1
 network 10.0.0.0
 network 172.30.0.0
 no auto-summary
!
no ip http server
no ip http secure-server
ip classless
ip route 10.1.2.0 255.255.255.0 10.0.2.102
!
line con 0
line aux 0
line vty 0 4
 password cisco
 login
!
end
```

Sample Configuration: Typical Router Configuration Post-AutoSecure

The following example shows the result of applying the AutoSecure configuration to the running configuration:

```
version 12.3
no service pad
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
service password-encryption
service sequence-numbers
!
hostname Ralb9f4
!
security authentication failure rate 10 log
```

```
security passwords min-length 6
logging buffered 4096 debugging
logging console critical
enable secret 5 1$yccL$kyqS8mWlVz3IPZlUPC8PC.
enable password 7 120A301443180F546B
!
username aDm198736 password 7 13163F1F52480A793B67
memory-size iomem 15
aaa new-model
!
aaa authentication login local_auth local
aaa session-id common
ip subnet-zero
no ip source-route
no ip gratuitous-arps
!
no ip domain lookup
ip domain name cisco.com
!
no ip bootp server
ip cef
ip inspect audit-trail
ip inspect udp idle-time 1800
ip inspect dns-timeout 7
ip inspect tcp idle-time 14400
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
ip audit notify log
ip audit po max-events 100
ip ssh time-out 60
ip ssh authentication-retries 2
no ftp-server write-enable
!
no voice hpi capture buffer
no voice hpi capture destination
!
```

```
interface Ethernet0/0
 ip address 10.0.2.2 255.255.255.0
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 half-duplex
!
interface Ethernet0/1
 ip address 172.30.2.2 255.255.255.0
 ip verify unicast source reachable-via rx 100
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 ip inspect autosec_inspect out
 half-duplex
!
router eigrp 1
 network 10.0.0.0
 network 172.30.0.0
 no auto-summary
!
no ip http server
no ip http secure-server
ip classless
ip route 10.1.2.0 255.255.255.0 10.0.2.102
!
ip access-list extended autosec_firewall_acl
 permit udp any any eq bootpc
 deny  ip any any
!
logging trap debugging
logging facility local2
access-list 100 permit udp any any eq bootpc
no cdp run
!
radius-server authorization permit missing Service-Type
!
banner motd ^C This system is the property of Cisco Systems, Inc.
UNAUTHORIZED ACCESS TO THIS DEVICE IS PROHIBITED.^C
!
line con 0
 exec-timeout 5 0
 login authentication local_auth
```

```
 transport output telnet
line aux 0
 login authentication local_auth
 transport output telnet
line vty 0 4
 password 7 14141B180F0B
 login authentication local_auth
 transport input telnet ssh
!
end
```

ADDITIONAL INFORMATION

- **Cisco IOS Security:** http://www.cisco.com/warp/public/732/Tech/security/
- **Cisco IOS Software Release 12.3:** http://www.cisco.com/warp/public/732/releases/release123/major/
- **AutoSecure Document:** http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123_1/ftatosec.htm
- **Cisco Feature Navigator:** http://www.cisco.com/go/fn/
- **Cisco AutoSecure Datasheet:** http://www.cisco.com/en/US/netsol/ns340/ns394/ns171/ns336/networking_solutions_white_paper09186a0080183b83.shtml

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.
168 Robinson Road
#28-01 Capital Tower
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 Website at www.cisco.com/go/offices.**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Cyprus 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

205233.CL_ETMG_KL_12.05

Printed in the USA