

You have chosen to display **errors** **warnings** general information, and helpful references. Headings are displayed for all supported commands that you submitted.

[SHOW RUNNING-CONFIG SECURITY Analysis](#)
[SHOW RUNNING-CONFIG - FW Analysis](#)

[Back to top](#)

=====
SHOW RUNNING-CONFIG SECURITY NOTIFICATIONS (if any)
=====

This process will suggest enhancements to an IP network's first line of defense, the router. Please note the following:

1. This is NOT a substitute for an overall network security policy. Responsible network security management requires careful research, planning, as well as continued vigilance. It is important to develop, document, and maintain standards for appropriate network access and utilization.
2. While a guide to your first steps in securing the TCP/IP operations within a Cisco router running IOS, this process is NO substitute for expertise in IP network security and exploit reduction. It is crucial for network support personnel to cultivate and maintain a base of knowledge in these areas.
3. DO NOT deploy any proposed configuration changes without thorough testing in a non-critical environment. You will want to research any commands with which you are not very familiar. Cisco's web-site has many outstanding resources, documents, templates, and links for further information, to assist you in this effort. Also, the Cisco Technical Assistance Center (TAC) is always available.

[Product Security Incident Response Team\(PSIRT\) advisories.](#)

SECURING INTERACTIVE SESSIONS:

WARNING: Interactive sessions initiated to and from this router are not as secure as they can be.

TRY THIS: Consider introducing the following configuration command(s):

['banner login'](#)

INFO: In some jurisdictions, civil and/or criminal prosecution of unauthorized users is much easier when you provide a banner warning them that their access is unauthorized. Legal notification requirements are complex and these should be discussed with your own legal counsel. Once the appropriate login warning has been developed for your router, you may incorporate it into your unit for display before all interactive logins with the 'banner login' configuration command.

PORT/LINE SECURITY:

WARNING: This router's ports/lines are not as secure as they can be.

TRY THIS: Consider introducing the following configuration command(s):

'line con 0'

['transport input none'](#)

INFO: This command guards against anyone initiating a reverse-telnet session to the router's console port.

'line aux 0'

['transport input none'](#)

INFO: This command guards against anyone initiating a reverse-telnet session to the router's aux port.

['exec-timeout'](#)

INFO: This command will end an interactive session if it remains inactive for a specified number of minutes.

'line vty 0 4'

['transport input ssh'](#)

INFO: This command restricts the session protocols that can be used to only SSH, in order to initiate a session to the router. Using SSH is preferable to TELNET since sessions are encrypted. SSH has been supported since IOS 12.0.5.S.

REFERENCE: [Configuring SSH on Cisco IOS routers](#)

['exec-timeout'](#)

INFO: This command will end an interactive session if it remains inactive

for a specified number of minutes.

'access-class ... in'

INFO: This command, in conjunction with an access-list, restricts interactive sessions to a specific list of source hosts. This parameter can be added to all vty ports or just the last. The later case will allow access to the router from anywhere on the network but holds the last port in reserve for a trusted host should the others 'fill-up' for any reason.

ROUTE/PATH INTEGRITY:

WARNING: This router does not show any filter against ICMP redirects.

INFO: An ICMP redirect is a message to a host to use a specific router as its path to a particular destination. In a properly functioning network, these messages will be sent within a local segment only. If this rule is violated, however, ICMP redirects can become the basis of attack.

TRY THIS: Consider the introduction of or addition to an access-list applied to externally facing interfaces to prevent these messages from crossing network segments. Use the 'access-list 100 deny icmp any any redirect' configuration command.

REFERENCE: See Extended Access List Examples for more information.

WARNING: This router does not show protection against commonly 'spoofed' IP addresses.

INFO: Spoofing is the practice of falsifying the source-address of an IP packet so as to disguise it's origin and/or intent.

TRY THIS: Consider the introduction of OR addition to an IP access-list applied to incoming packets on all active interfaces. The LAN interface should block all IP source-addresses not specifically permitted to exist on that network segment. The WAN interface should block any traffic attempting to represent itself as from the WAN interface itself, the internal LAN segment, a private network (impossible from the Internet), a loopback address (not permitted on the Internet), or from multicast/experimental address-space (invalid under most circumstances).

INFO: Private network addresses are within these ranges:

10.0.0.0 - 10.255.255.255

172.16.0.0 - 172.31.255.255

192.168.0.0 - 192.168.255.255

INFO: Loopback and multicast addresses exist within these ranges:

127.0.0.0 - 127.255.255.255

224.0.0.0 - 255.255.255.255

NOTE: Research the anti-spoofing requirements of your own network before applying this protection.

SERVICE-EXPLOIT REDUCTION:

WARNING: One or more services are running that can be exploited.

TRY THIS: To reduce possible service-based exploits that may be attempted against this router, consider disabling these services using the following configuration command(s):

'no ip finger'

'no ip domain-lookup'

These services are rarely used for legitimate purposes and can be co-opted to launch a denial-of-service as well as other types of attacks.

WARNING: NTP (Network Time Protocol) has not been secured.

INFO: While not particularly dangerous, can be used to subvert certain security protocols (those that use a time-base) and foul the time-stamps on the router's log messages.

TRY THIS: To disable NTP on a per interface basis, use the 'ntp disable' interface configuration command. To use NTP more securely, consider the following configuration command(s):

'ntp server'

'ntp authenticate'

TRAFFIC-FLOOD MANAGEMENT:

INFO: Many denial-of-service (DOS) attacks are based on sending a flood of useless packets to vulnerable units.

WARNING: This router may not respond well in the face of a flood-based attack.

TRY THIS: To improve this router's response, consider introducing the following configuration command(s):

'scheduler allocate'

INFO: This command guarantees that the router's CPU will respond to

interactive sessions regardless of heavy traffic loads.

'ip verify unicast reverse-path'

INFO: This interface command examines each packet received as input on that interface. If the source IP address does not have a route in the CEF tables that points back to the same interface on which the packet arrived, the router drops the packet. The feature should be applied to internet facing interfaces and CEF (Cisco Express Forwarding) should be enabled on the router.

REFERENCE: [Configuring Unicast Reverse Path Forwarding](#)

INFO: If this router is a 2600 series or higher (this includes Catalyst 5000 series units configured with an RSM), you may wish to investigate the TCP Intercept feature introduced in IOS Version 11.2. This is a powerful feature designed to protect selected hosts from SYN-flood attacks common to the Internet. There is some cost, however, with regard to the router's performance.

REFERENCE: For more information, see [Cisco IOS TCP Intercept](#) and [TCP Intercept](#)

INFO: You may consider enabling the 'committed access rate' (CAR) feature to limit the bandwidth consumed by certain traffic types such as ICMP, TCP 'SYN', UDP and multicast packets. These should be applied to internet facing interfaces using the 'rate-limit' interface configuration command and an appropriate access-list. This can be helpful in limiting the effect of denial of service attacks. CAR is a functionality that works with Cisco Express Forwarding, found in 11.1CC and releases from 12.0.

REFERENCE: For more information, see [Configuring Committed Access Rate](#)

LOGGING:

WARNING: This router is not taking full advantage of its logging capabilities.

INFO: The router is capable of logging accesses and other significant events using a variety of methods. These logs, when detailed over a significant interval, are invaluable in identifying/responding to attacks and other abuses.

TRY THIS: To take advantage of these logging activities consider introducing the following configuration command(s):

'logging (IP address of syslog server)'

'logging trap'

INFO: These commands set up communication between the router's logging process and a syslog server. A syslog server is an inexpensive and widely available application/agent that stores log entries from network devices. This facility allows you permanent storage for logging information, which is especially valuable when physical access to the router is impractical. A syslog server also affords greater detail within the logs themselves (less reliance on the router's logging buffer). The level of 'urgency' (detail) of the syslog server-stored logs is set via the 'logging trap' command. There is minimal performance impact to the router, regardless of the level of logging detail. Like any component of a network-management system, the syslog server application should be run only from a secured, trusted host.

'no logging console'

INFO: This command disables all logging to the console terminal. Excessive debugs to the console port of a router can cause it to hang. This is because the router automatically prioritizes console output ahead of other router functions. Hence, if the router is processing a large debug output to the console port, it may hang. Hence, if the debug output is excessive, use the vty (telnet) ports or the log

buffers

to obtain your debugs.

REFERENCE: [Important Information on Debug Commands](#)

'aaa accounting'

INFO: The best, most detailed logging is done in conjunction with a TACACS+ or RADIUS server. While this option would require some setup, configuration, and ongoing support, the benefits to your overall network security are considerable and extend well beyond logging functions.

'exception dump'

INFO: When a router crashes, a copy of the core memory is kept. Before the memory is erased on reboot, the router can be set up to copy the core dump out to a UNIX server. These dumps can be extremely useful in identifying the cause of a crash. An account (ftp, tftp, or rcp) and sufficient disk space (equal to the amount of memory on the router per dump) needs to be set up and allocated. One example, using FTP to export the dump:

```
!  
ip ftp source-interface Loopback0  
ip ftp username [enter username here]
```



```
ip ftp password [enter password here]
!
exception protocol ftp
exception dump [enter IP address of FTP Server here]
!
```

REFERENCE: For more information on configuring core dumps, see: [Configuring Core](#)

Dumps

'ip ftp source-interface Loopback0'

INFO: The commands above will enable services on your router to send messages sourced from a loopback interface (Loopback0 in these examples). Using a loopback address as a source interface will keep your messages consistent and simplify access-list statements for security purposes.

'ip accounting access-violations'

INFO: This command enables IP accounting on an interface with the ability to identify IP traffic that fails IP access lists. The following interfaces could benefit from this:

```
FastEthernet0/0
FastEthernet0/1
```

Once enabled, violations may be viewed with the 'show ip accounting access-violations' command.

REFERENCE: For additional information see:

Practical Reading:

[Improving Security on Cisco Routers](#)

[Characterizing and Tracing Packet Floods Using Cisco Routers](#)

Cisco Security Solutions:

[Security Solutions](#)

[Back to top](#)

```
=====
SHOW RUNNING-CONFIG - FW NOTIFICATIONS (if any)
=====
```

LOCK AND KEY:

Lock and Key is not configured.

For additional information, visit: [Configuring Lock-and-Key Security](#)

IP SESSION FILTERING (REFLEXIVE ACCESS LISTS):

IP Session Filtering (Reflexive Access Lists) is not configured.

For additional information, visit: [Configuring IP Session Filtering](#)

TCP INTERCEPT:

TCP Intercept is not configured.

For additional information, visit: [Configuring TCP Intercept](#)

CONTEXT-BASED ACCESS CONTROL (CBAC):

WARNING: The following protocols are not being inspected by their respective firewalls.

autosec_inspect(Inbound):

h323	H.323 Protocol (e.g, MS NetMeeting, Intel Video Phone)
netshow	Microsoft NetShow Protocol
rpc	Remote Procedure Call Protocol
rtsp	Real Time Streaming Protocol
sqlnet	SQL Net Protocol
streamworks	StreamWorks Protocol
vdolive	VDOLive Protocol

TRY THIS: Ensure that the proper protocols are being inspected. While inspecting TCP and UDP allows connections for non-inspected protocols, TCP and UDP inspection does not recognize application-specific commands, and therefore might not permit all return packets for an application, particularly if the return packets have a different port number than the previous exiting packet.

If any of above the protocols should be inspected, use the respective 'ip inspect name {fw_name} {protocol}' global configuration command.

If these protocols should be inspected, packets for that protocol should be permitted to exit the firewall (by configuring the correct ACL), and packets for that protocol will only be allowed back in through the firewall if they belong to a valid existing session. Each protocol packet is inspected to maintain information about the session state.

WARNING: The following timeouts have been changed from their defaults:

Inspection rule autosec_inspect:

UDP Timeouts (default 30 seconds):

udp User Datagram Protocol

TRY THIS: Ensure that the timeout values for these protocols are the desired values. If they are too low, sessions will be closed too quickly. If they are too high, sessions may never end. Use the 'ip inspect name {inspection_name} {protocol} timeout {timeout_value}' global configuration command to alter these values (if desired).

ERROR: The 'http' protocol is being inspected by the autosec_inspect firewall, but a java-list is not defined.

The 'http' protocol does not inspect web traffic but rather is used for Java applet blocking.

TRY THIS: Define a standard IP access-list to be used for Java applet inspection. Then use the 'ip inspect name autosec_inspect http java-list {standard_acl}' global configuration command to allow Java applets to be inspected.

WARNING: The following access-list lines may be permitting traffic they should not be:

Access-List autosec_complete_bogon

permit ip any any

TRY THIS: Ensure that these access-lists are configured properly. Since this is an inbound access-list on an external interface, only specific connections should be permitted while more general traffic is denied. The inspection rule will create temporary access-list entries that will allow inbound traffic from sessions originating internally. Reconfigure these access-lists as necessary.

WARNING: Using CBAC uses less than approximately 600 bytes of memory per connection. There is also a slight amount of additional processing that occurs whenever packets are inspected.

TRY THIS: Because of the memory and processor usage, CBAC should only be used when needed.

WARNING: CBAC does not provide intelligent filtering for all protocols; it only works for the protocols that are specified. If a protocol is not specified for CBAC, the existing access lists will determine how that protocol is filtered. No temporary openings will be created for protocols not specified for CBAC inspection.

TRY THIS: Ensure that CBAC has been configured for the proper protocols.

INFO: CBAC does not protect against attacks originating from within the protected network. CBAC only detects and protects against attacks that travel through the firewall.

INFO: CBAC protects against certain attacks but should not be considered a perfect, impenetrable defense. Determined, skilled attackers might be able to launch effective attacks. While there is no such thing as a perfect defense, CBAC detects and prevents most of the popular attacks on your network.

INFO: Use the following show commands to monitor CBAC operation:

show ip inspect name inspection-name

show ip inspect config

show ip inspect interfaces

show ip inspect session [detail]

show ip inspect all