Firewall Stateful Inspection of ICMP

Last Updated: March 26, 2012

The Firewall Stateful Inspection of ICMP feature addresses the limitation of qualifying Internet Control Management Protocol (ICMP) messages into either a malicious or benign category by allowing the Cisco IOS firewall to use stateful inspection to "trust" ICMP messages that are generated within a private network and to permit the associated ICMP replies. Thus, network administrators can debug network issues by using ICMP without concern that possible intruders may enter the network.

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.

Restrictions for Firewall Stateful Inspection of ICMP

- To enable this feature, your Cisco IOS image must contain the Cisco IOS firewall.
- This feature does not work for the User Datagram Protocol (UDP) traceroute, in which UDP datagrams are sent instead of ICMP packets. The UDP traceroute is typically the default for UNIX systems. To use ICMP inspection with a UNIX host, use the "I" option with the traceroute command.

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

This functionality will cause the UNIX host to generate ICMP traceroute packets, which will be inspected by the Cisco IOS firewall ICMP.

Information About Firewall Stateful Inspection of ICMP

Feature Design of Firewall Stateful Inspection of ICMP

ICMP is used to report errors and information about a network. It is a useful tool for network administrators who are trying to debug network connectivity issues. Unfortunately, intruders can also use ICMP to discover the topology of a private network. To guard against a potential intruder, ICMP messages can be blocked from entering a private network; however, a network administrator may then be unable to debug the network. Although a Cisco IOS router can be configured using access lists to selectively allow certain ICMP messages through the router, the network administrator must still guess which messages are potentially malicious and which messages are benign. With the introduction of this feature, a user can now configure a Cisco IOS firewall for stateful inspection to “trust” that the ICMP messages are generated within the private network and to permit the associated ICMP replies.

Note Access lists can still be used to allow unsolicited error messages along with Cisco IOS firewall inspection. Access lists complement Cisco IOS firewall ICMP inspection.

Stateful inspection of ICMP packets is limited to the most common types of ICMP messages that are useful to network administrators who are trying to debug their networks. That is, ICMP messages that do not provide a valuable tool for the internal network administrator will not be allowed. For the Cisco IOS firewall-supported ICMP message request types, see the table below.

Table 1 ICMP Packet Types Supported by CBAC

ICMP Packet Type	Name	Description
0	Echo Reply	Reply to Echo Request (Type 8)
3	Destination Unreachable	Possible reply to any request **Note** This packet is included because it is a possible response to any ICMP packet request.
8	Echo Request	Ping or traceroute request
11	Time Exceeded	Reply to any request if the time to live (TTL) packet is 0
13	Timestamp Request	Request

ICMP Packet Type	Name	Description
14	Timestamp Reply	Reply to Timestamp Request (type 13)

Note ICMP packet types 0 and 8 are used for pinging: the source sends out an Echo Request packet, and the destination responds with an Echo Reply packet. Packet types 0, 8, and 11 are used for ICMP traceroute: Echo Request packets are sent out starting with a TTL packet of 1, and the TTL is incremented for each hop. The intermediate hops respond to the Echo Request packet with a Time Exceeded packet; the final destination responds with an Echo Reply packet.

ICMP Inspection Checking

Return packets are checked by the inspect code, not by ACLs. The inspect code tracks each destination address from outgoing packets and checks each return packet. For ECHO REPLY and TIMESTAMP REPLY packets, the return address is checked. For UNREACHABLE and TIME EXCEEDED packets, the intended destination address is extracted from the packet data and checked.

For more information, see "Example Checking for ICMP Inspection".

How to Use Firewall Stateful Inspection of ICMP

Configuring Firewall Stateful Inspection for ICMP

To enable the Cisco IOS Firewall to start inspection ICMP messages, perform the following steps:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip inspect name** *inspection-name* **icmp alert** {**on** | **off**}] [**audit-trail on** |**off**}] [**timeout** *seconds*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

Step 3	**ip inspect name** *inspection-name* **icmp alert** {**on** | **off**}] [**audit-trail on** |**off**}] [**timeout** *seconds*
	
	Example:
	`Router(config)#`
	`ip inspect name test icmp alert on audit-trail on timeout 30`
		Turns on inspection for ICMP.
		• **alert** --Alert messages are generated. This function is **on** by default.
		• **audit-trail** --Audit trail messages are generated. This function is **off** by default.
		• **timeout** --Overrides the global channel inactivity timeout value. The default value of the *seconds* argument is 10.

Verifying Firewall and ICMP Session Information

To display active ICMP session and IP access list information, perform the following optional steps:

SUMMARY STEPS

1. **enable**
2. **show ip inspect session detail**
3. **show ip access-list**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show ip inspect session detail** **Example:** `Router# show ip inspect session`	(Optional) Displays existing sessions that are currently being tracked and inspected by the Cisco IOS firewall. • The optional **detail** keyword causes additional details about these sessions to be shown.
Step 3	**show ip access-list** **Example:** `Router# show ip access-list`	(Optional) Displays the contents of all current IP access lists. For a sample output example, see the section “Example ICMP Session Verification.”

Monitoring Firewall and ICMP Session Information

To monitor debugging messages related to ICMP inspection, perform the following optional steps:

Note Effective with Cisco IOS Release 12.4(20)T, the **debug ip inspect** command is replaced by the **debug policy-firewall** command. See the Cisco IOS Debug Command Reference for more information.

SUMMARY STEPS

1. **enable**
2. **debug ip inspect icmp**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**debug ip inspect icmp** **Example:** `Router# debug ip inspect icmp`	(Optional) Displays the operations of the ICMP inspection engine for debugging purposes. For an example of sample output, see the command debug ip inspect in the Command Reference section.

Configuration Examples for Stateful Inspection of ICMP

Example Firewall Stateful Inspection for ICMP Configuration

The default ICMP timeout is deliberately short (10 seconds) due to the security hole that is opened by allowing ICMP packets with a wild-carded source address back into the inside network. The timeout will occur 10 seconds after the last outgoing packet from the originating host. For example, if you send a set of 10 ping packets spaced 1 second apart, the timeout will expire in 20 seconds or 10 seconds after the last outgoing packet. However, the timeout is not extended for return packets. If a return packet is not seen within the timeout window, the hole will be closed and the return packet will not be allowed in. Although the default timeout can be made longer if desired, it is recommended that this value be kept relatively short.

The following example shows how to configure a firewall for stateful inspection of ICMP packets:

```
no service pad
service timestamps debug uptime
service timestamps log uptime
service password-encryption
!
hostname UUT
!
ip subnet-zero
no ip domain lookup
!
ip inspect audit-trail
ip inspect name test icmp alert on audit-trail on timeout 30
!
interface Ethernet0
ip address 192.168.10.2 255.255.255.0
ip inspect test in
!
interface Ethernet1
ip address 192.168.20.2 255.255.255.0
ip access-group 101 in
!
ip classless
ip route 0.0.0.0 0.0.0.0 192.168.20.3
no ip http server
!
access-list 101 deny ip any any
!
line con 0
exec-timeout 0 0
!
end
```

Example Checking for ICMP Inspection

In the following example, three destinations were pinged. The example shows that the inspect code tracked each destination address in the inspect session information.

```
fw_1751#sh ip insp sess detail
Established Sessions
 Session 813A1808 (192.168.156.5:0)=>(0.0.0.0:0) icmp SIS_OPEN
   Created 00:04:20, Last heard 00:00:00
   Destinations: 3
       Dest addr [192.168.131.3]
       Dest addr [192.168.131.7]
       Dest addr [192.168.131.31]
   Bytes sent (initiator:responder) [8456:5880] acl created 4
   Inbound access-list 102 applied to interface Ethernet0/0
   Inbound access-list 102 applied to interface Ethernet0/0
   Inbound access-list 102 applied to interface Ethernet0/0
   Inbound access-list 102 applied to interface Ethernet0/0
```

Example ICMP Session Verification

The following example is sample output from the **show ip access-list** command. In this example, Access Control Lists (ACLs) are created for an ICMP session on which only ping packets were issued from the host.

```
Router# show ip access-list 101
Extended IP access list 101
     permit icmp any host 192.168.133.3 time-exceeded
     permit icmp any host 192.168.133.3 unreachable
     permit icmp any host 192.168.133.3 timestamp-reply
     permit icmp any host 192.168.133.3 echo-reply (4 matches)
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
CBAC information and configuration tasks	"Configuring Context-based Access Control"
Additional CBAC commands	*Cisco IOS Security Command Reference*

Standards

Standards	Title
None	--

MIBs

MIBs	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFCs[1]	Title
RFC 792	*Internet Control Message Protocol*
RFC 950	*Internet Standard Subnetting Procedure*
RFC 1700	*Assigned Numbers*

1 **Not all supported RFCs are listed.**

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 Firewall Stateful Inspection of ICMP

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 2 Feature Information for Firewall Stateful Inspection of ICMP

Feature Name	Releases	Feature Information
Firewall Stateful Inspection of ICMP	12.2(11)YU 12.2(15)T	The Firewall Stateful Inspection of ICMP feature addresses the limitation of qualifying Internet Control Management Protocol (ICMP) messages into either a malicious or benign category by allowing the Cisco IOS firewall to use stateful inspection to "trust" ICMP messages that are generated within a private network and to permit the associated ICMP replies. Thus, network administrators can debug network issues by using ICMP without concern that possible intruders may enter the network. The following commands were introduced or modified: **debug ip inspect**, **ip inspect name**.

Glossary

ACL --access control list. An ACL is a list kept by routers to control access to or from the router for a number of services (for example, to prevent packets with a certain IP address from leaving a particular interface on the router).

CBAC --Context-Based Access Control. CBAC is the name given to the Cisco IOS Firewall subsystem.

firewall --A firewall is a networking device that controls access to the network assets of your organization. Firewalls are positioned at the entrance points into your network. If your network has multiple entrance points, you must position a firewall at each point to provide effective network access control.

The most basic function of a firewall is to monitor and filter traffic. Firewalls can be simple or elaborate, depending on your network requirements. Simple firewalls are usually easier to configure and manage. However, you might require the flexibility of a more elaborate firewall.

ICMP --Internet Control Message Protocol. An ICMP is a network layer Internet protocol that reports errors and provides other information relevant to IP packet processing.

RPC --remote-procedure call. A RPC is the technological foundation of client or server computing. RPCs are procedure calls that are built or specified by clients and are executed on servers, with the results returned over the network to the clients.

RTSP --Real Time Streaming Protocol. RTSP enables the controlled delivery of real-time data, such as audio and video. Sources of data can include both live data feeds, such as live audio and video, and stored content, such as prerecorded events. RTSP is designed to work with established protocols, such as RTP and HTTP.

SIP --Session Initiation Protocol. SIP is a protocol developed by the IETF MUSIC Working Group as an alternative to H.323. SIP features are compliant with IETF RFC 2543, published in March 1999. SIP equips platforms to signal the setup of voice and multimedia calls over IP networks.

SMTP --simple mail transfer protocol. SMTP is an Internet protocol providing e-mail services.

UDP --User Datagram Protocol. A UDP is a connectionless transport layer protocol in the TCP/IP protocol stack. UDP is a simple protocol that exchanges datagrams without acknowledgments or guaranteed delivery, requiring that error processing and retransmission be handled by other protocols. UDP is defined in RFC 768.

Note Refer to the *Internetworking Terms and Acronyms* for terms not included in this glossary.