Firewall Stateful Inspection of ICMP

The Firewall Stateful Inspection of ICMP feature categorizes Internet Control Management Protocol Version 4 (ICMPv4) messages as either malicious or benign. The firewall uses stateful inspection to *trust* benign ICMPv4 messages that are generated within a private network and permits the entry of associated ICMP replies into the network. The Firewall Stateful Inspection of ICMP feature helps network administrators to debug network issues by using ICMP so that intruders cannot enter the network.

This module provides an overview of the firewall stateful inspection of ICMPv4 messages and describes how to configure the firewall to inspect ICMPv4 messages.

- Prerequisites for Firewall Stateful Inspection of ICMP, on page 1
- Restrictions for Firewall Stateful Inspection of ICMP, on page 1
- Information About Firewall Stateful Inspection of ICMP, on page 2
- How to Configure Firewall Stateful Inspection of ICMP, on page 3
- Configuration Examples for Firewall Stateful Inspection of ICMP, on page 8
- Additional References for Firewall Stateful Inspection of ICMP, on page 8
- Feature Information for Firewall Stateful Inspection of ICMP, on page 9

Prerequisites for Firewall Stateful Inspection of ICMP

- You must configure the Cisco firewall before you can configure the Firewall Stateful Inspection of ICMP feature.
- The network must allow all ICMP traffic to pass through security appliance interfaces.
- Access rules must be configured for ICMP traffic that terminates at a security appliance interface.

Restrictions for Firewall Stateful Inspection of ICMP

This feature does not work with the UDP traceroute utility, in which UDP datagrams are sent instead of ICMP packets. UDP traceroute is the default for UNIX systems. For a UNIX host to generate ICMP traceroute packets that are inspected by the firewall, use the “-I” option with the **traceroute** command.

Information About Firewall Stateful Inspection of ICMP

Overview of the Firewall Stateful Inspection of ICMP

Internet Control Management Protocol (ICMP) is a network protocol that provides information about a network and reports errors in the network. Network administrators use ICMP to debug network connectivity issues. To guard against potential intruders using ICMP to discover the topology of a private network, ICMPv4 messages can be blocked from entering a private network; however, network administrators may then be unable to debug the network.

You can configure Cisco routers to use access control lists (ACLs) to either completely allow or deny ICMPv4 messages. When using ACLs for ICMPv4 messages, message *inspection* has precedence over the configured allow or deny actions.

ICMPv4 messages that use the IP protocol can be categorized into the following two types:

- Informational messages that utilize a simple request/reply mechanism.
- Error messages that indicate that some sort of error has occurred while delivering an IP packet.

Note To prevent ICMP attacks from using the Destination Unreachable error message, only one Destination Unreachable message is allowed per session by the firewall.

A host that is processing a UDP session that is traversing the firewall may generate an ICMP error packet with a Destination Unreachable message. In such cases, only one Destination Unreachable message is allowed through the firewall for that session.

The following ICMPv4 packet types are supported:

Table 1: ICMPv4 Packet Types

Packet Type	Name	Description
0	Echo Reply	Reply to an echo request (type 8).
3	Unreachable	Possible reply to any request.
8	Echo Request	Ping or a traceroute request.
11	Time Exceeded	Reply if the time-to-live (TTL) size of a packet is zero.
13	Timestamp Request	Request.
14	Timestamp Reply	Reply to a timestamp request (type 13).

ICMPv4 packet types 0 and 8 are used to ping a destination; 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 ICMPv4 traceroute (that is, Echo Request packets that are sent start with a TTL size of 1) and the TTL size is incremented for

each hop. Intermediate hops respond to the Echo Request packet with a Time Exceeded packet and the final destination responds with an Echo Reply packet.

If an ICMPv4 error packet is an embedded packet, the embedded packet is processed according to the protocol and the policy configured for the packet. For example, if the embedded packet is a TCP packet, and a drop action is configured for the packet, the packet is dropped even if ICMPv4 has configured a pass action.

The following scenario describes how ICMPv4 packets pass through the firewall:

1. An ICMPv4 packet arrives at the source interface. The firewall uses the source and destination addresses of the packet without any change for packet inspection. The firewall uses IP addresses (source and destination), the ICMP type, and the protocol for session key creation and lookup.
2. The packet passes the firewall inspection.
3. Return traffic comes from the destination interface and, based on the ICMPv4 message type, the firewall creates the session lookup key.
4. **a.** If the reply message is an informational message, the firewall uses the source and destination addresses from the packet without any change for packet inspection. Here, the destination port is the ICMPv4 message request type.
   b. If the reply message is an ICMPv4 error message, the firewall uses the payload packet present in the ICMP error packet to create the session key for session lookup.
5. If the firewall session lookup is successful, the packet passes the firewall inspection.

ICMP Inspection Checking

ICMP return packets are checked by the inspect code, and not by access control lists (ACLs). The inspect code tracks destination address from each outgoing packet 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.

How to Configure Firewall Stateful Inspection of ICMP

Configuring Firewall Stateful Inspection of ICMP

Perform this task to configure the firewall stateful inspection of ICMP, which includes the following:

- A class map that matches the ICMP traffic.
- A policy map with the inspect action.
- Security zones and zone pairs (to attach a firewall policy map to the zone pair).

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **access-list** *access-list-number* {**deny** | **permit**} **icmp** *source source-wildcard destination destination-wildcard*

4. **class-map type inspect** *class-map-name*
5. **match protocol** *protocol-name*
6. **exit**
7. **policy-map type inspect** *policy-map-name*
8. **class** *class-map-name*
9. **inspect**
10. **exit**
11. **exit**
12. **zone security** *zone-name*
13. **exit**
14. **zone-pair security** *zone-pair-name* **source** *source-zone* **destination** *destination-zone*
15. **service-policy type inspect** *policy-map-name*
16. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**access-list** *access-list-number* {**deny** | **permit**} **icmp** *source source-wildcard destination destination-wildcard* **Example:** `Device(config)# access-list 102 permit icmp 192.168.0.1 255.255.255.0 192.168.2.22 255.255.255.0`	Defines an extended IP access list.
Step 4	**class-map type inspect** *class-map-name* **Example:** `Device(config)# class-map type inspect c1`	Defines the class on which an action is to be performed and enters QoS class-map configuration mode.
Step 5	**match protocol** *protocol-name* **Example:** `Device(config-cmap)# match protocol icmp`	Configures a match criterion for a class map on the basis of the specified protocol.
Step 6	**exit** **Example:** `Device(config-cmap)# exit`	Exits QoS class-map configuration mode and enters global configuration mode.

	Command or Action	Purpose
Step 7	**policy-map type inspect** *policy-map-name* **Example:** `Device(config)# policy-map type inspect p1`	Creates a protocol-specific inspect type policy map and enters QoS policy-map configuration mode.
Step 8	**class** *class-map-name* **Example:** `Device(config-pmap)# class c1`	Defines the class on which an action is to be performed and enters QoS policy-map class configuration mode.
Step 9	**inspect** **Example:** `Device(config-pmap-c)# inspect`	Enables stateful packet inspection.
Step 10	**exit** **Example:** `Device(config-pmap-c)# exit`	Exits QoS policy-map class configuration mode and enters QoS policy-map configuration mode.
Step 11	**exit** **Example:** `Device(config-pmap)# exit`	Exits QoS policy-map configuration mode and enters global configuration mode.
Step 12	**zone security** *zone-name* **Example:** `Device(config)# zone security z1`	Creates a security zone and enters security zone configuration mode. • Your configuration must have two security zones to create a zone pair: a source zone and a destination zone. • In a zone pair, you can use the default zone as either the source or the destination zone.
Step 13	**exit** **Example:** `Device(config-sec-zone)# exit`	Exits security zone configuration mode and enters global configuration mode.
Step 14	**zone-pair security** *zone-pair-name* **source** *source-zone* **destination** *destination-zone* **Example:** `Device(config)# zone-pair security inout source z1 destination z2`	Creates a zone pair to which interfaces can be assigned and enters security zone-pair configuration mode.
Step 15	**service-policy type inspect** *policy-map-name* **Example:** `Device(config-sec-zone-pair)# service-policy type inspect p1`	Attaches a firewall policy map to a zone pair.

	Command or Action	Purpose
Step 16	**end** **Example:** `Device(config-sec-zone-pair)# end`	Exits security zone-pair configuration mode and enters privileged EXEC mode.

Verifying Firewall Stateful Inspection of ICMP

You can use the following **show** commands in any order.

SUMMARY STEPS

1. **enable**
2. **show ip access-lists**
3. **show policy-map type inspect** *policy-map-name*
4. **show policy-map type inspect zone-pair** *zone-pair-name*
5. **show zone security** *zone-name*
6. **show zone-pair security** [**source** *source-zone* **destination** *destination-zone*]

DETAILED STEPS

Step 1 **enable**

Example:

```
Device> enable
```

Enables privileged EXEC mode.

- Enter your password if prompted.

Step 2 **show ip access-lists**

Example:

```
Device# show ip access-lists
```

Displays information about the specified policy map.

Step 3 **show policy-map type inspect** *policy-map-name*

Example:

```
Device# show policy-map type inspect p1
```

Displays information about the specified policy map.

Step 4 **show policy-map type inspect zone-pair** *zone-pair-name*

Example:

```
Device# show policy-map type inspect zone-pair inout
```

Displays the runtime inspect type policy-map statistics for the zone pair.

Step 5 **show zone security** *zone-name*

Example:

```
Device# show zone security z1
```

Displays zone security information.

Step 6 **show zone-pair security** [**source** *source-zone* **destination** *destination-zone*]

Example:

```
Device# show zone-pair security source z1 destination z2
```

Displays source and destination zones and the policy attached to the zone pair.

Example:

The following sample output from the **show ip access-lists** command shows how ACLs are created for an ICMP session for which only ping packets were issued from the host:

```
Device# show ip access-lists

 Extended IP access list 102
     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)
```

The following is sample output from the **show policy-map type inspect p1** command:

```
Device# show policy-map type inspect p1

 Policy Map type inspect p1
  Class c1
   Inspect
```

The following is sample output from the **show policy-map type inspect zone-pair inout** command:

```
Device# show policy-map type inspect zone-pair inout

 Zone-pair: inout
  Service-policy : p1
   Class-map: c1 (match-all)
    Match: protocol icmp
    Inspect
     Session creations since subsystem startup or last reset 0
     Current session counts (estab/half-open/terminating) [0:0:0]
     Maxever session counts (estab/half-open/terminating) [0:0:0]
     Last session created never
     Last statistic reset never
     Last session creation rate 0
     half-open session total 0
   Class-map: class-default (match-any)
    Match: any
    Drop
     0 packets, 0 bytes
```

The following is sample output from the **show zone security** command:

```
Device# show zone security
```

```
zone self
Description: System defined zone
```

The following is sample output from the **show zone-pair security** command:

```
Device# show zone-pair security source z1 destination z2

zone-pair name inout
  Source-Zone z1  Destination-Zone z2
  service-policy p1
```

Configuration Examples for Firewall Stateful Inspection of ICMP

Example: Configuring Firewall Stateful Inspection of ICMP

```
Device# configure terminal
Device(config)# access-list 102 permit icmp 192.168.0.1 255.255.255.0 192.168.2.22
255.255.255.0
Device(config)# class-map type inspect c1
Device(config-cmap)# match protocol icmp
Device(config-cmap)# exit
Device(config)# policy-map type inspect p1
Device(config-pmap)# class c1
Device(config-pmap-c)# inspect
Device(config-pmap-c)# exit
Device(config-pmap)# exit
Device(config)# zone security z1
Device(config-sec-zone)# exit
Device(config)# zone security z2
Device(config-sec-zone)# exit
Device(config)# zone-pair security inout source z1 destination z2
Device(config-sec-zone-pair)# service-policy type inspect p1
Device(config-sec-zone-pair)# end
```

Additional References for Firewall Stateful Inspection of ICMP

Related Documents

Related Topic	Document Title
Cisco IOS commands	Master Command List, All Releases
Security commands	• Security Command Reference: Commands A to C • Security Command Reference: Commands D to L • Security Command Reference: Commands M to R • Security Command Reference: Commands S to Z

Standards & RFCs

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

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	Cisco IOS XE Release 2.1 Cisco IOS XE Release 3.2S	The Firewall Stateful Inspection of ICMP feature categorizes ICMPv4 messages as either malicious or benign. The firewall uses stateful inspection to *trust* benign ICMP messages that are generated within a private network and permits the entry of associated ICMP replies.