CHAPTER 14

icmp through imap4s Commands

icmp

To configure access rules for ICMP traffic that terminates at a security appliance interface, use the **icmp** command. To remove the configuration, use the **no** form of this command.

icmp {**permit** | **deny**} *ip_address net_mask* [*icmp_type*] *if_name*

no icmp {**permit** | **deny**} *ip_address net_mask* [*icmp_type*] *if_name*

Syntax Description

deny	Deny access if the conditions are matched.
icmp_type	(Optional) ICMP message type (see Table 14-1).
if_name	The interface name.
ip_address	The IP address of the host sending ICMP messages to the interface.
net_mask	The mask to be applied to *ip_address*.
permit	Permit access if the conditions are matched.

Defaults

The default behavior of the security appliance is to allow all ICMP traffic *to* the security appliance interfaces. However, by default the security appliance does not respond to ICMP echo requests directed to a broadcast address. The security appliance also denies ICMP messages received at the outside interface for destinations on a protected interface.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	**Routed**	**Transparent**	**Single**	**Context**	**System**
Global configuration	•	•	•	•	•

Command History

Release	Modification
6.0	This command was introduced.

Usage Guidelines

The **icmp** command controls ICMP traffic that terminates on any security appliance interface. If no ICMP control list is configured, then the security appliance accepts all ICMP traffic that terminates at any interface, including the outside interface. However, by default, the security appliance does not respond to ICMP echo requests directed to a broadcast address.

The security appliance only responds to ICMP traffic sent to the interface that traffic comes in on; you cannot send ICMP traffic through an interface to a far interface.

The **icmp deny** command disables pinging to an interface, and the **icmp permit** command enables pinging to an interface. With pinging disabled, the security appliance cannot be detected on the network. This is also referred to as configurable proxy pinging.

Use the **access-list extended** or **access-group** commands for ICMP traffic that is routed *through* the security appliance for destinations on a protected interface.

We recommend that you grant permission for the ICMP unreachable message type (type 3). Denying ICMP unreachable messages disables ICMP Path MTU discovery, which can halt IPSec and PPTP traffic. See RFC 1195 and RFC 1435 for details about Path MTU Discovery.

If an ICMP control list is configured for an interface, then the security appliance first matches the specified ICMP traffic and then applies an implicit deny for all other ICMP traffic on that interface. That is, if the first matched entry is a permit entry, the ICMP packet continues to be processed. If the first matched entry is a deny entry or an entry is not matched, the security appliance discards the ICMP packet and generates a syslog message. An exception is when an ICMP control list is not configured; in that case, a **permit** statement is assumed.

Table 14-1 lists the supported ICMP type values.

Table 14-1 ICMP Type Literals

ICMP Type	Literal
0	echo-reply
3	unreachable
4	source-quench
5	redirect
6	alternate-address
8	echo
9	router-advertisement
10	router-solicitation
11	time-exceeded
12	parameter-problem
13	timestamp-request
14	timestamp-reply
15	information-request
16	information-reply
17	mask-request
18	mask-reply
31	conversion-error
32	mobile-redirect

Examples

The following example denies all ping requests and permits all unreachable messages at the outside interface:

```
hostname(config)# icmp permit any unreachable outside
```

Continue entering the **icmp deny any** *interface* command for each additional interface on which you want to deny ICMP traffic.

The following example permits host 172.16.2.15 or hosts on subnet 172.22.1.0/16 to ping the outside interface:

```
hostname(config)# icmp permit host 172.16.2.15 echo-reply outside
hostname(config)# icmp permit 172.22.1.0 255.255.0.0 echo-reply outside
hostname(config)# icmp permit any unreachable outside
```

Related Commands

Commands	Description
clear configure icmp	Clears the ICMP configuration.
debug icmp	Enables the display of debug information for ICMP.
show icmp	Displays ICMP configuration.
timeout icmp	Configures the idle timeout for ICMP.

icmp-object

To add icmp-type object groups, use the **icmp-object** command in icmp-type configuration mode. To remove network object groups, use the **no** form of this command.

icmp-object *icmp_type*

no group-object *icmp_type*

Syntax Description

icmp_type	Specifies an icmp-type name.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Icmp-type configuration	•	•	•	•	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

The **icmp-object** command is used with the **object-group** command to define an icmp-type object. It is used in icmp-type configuration mode.

ICMP type numbers and names include:

Number	ICMP Type Name
0	**echo-reply**
3	**unreachable**
4	**source-quench**
5	**redirect**
6	**alternate-address**
8	**echo**
9	**router-advertisement**
10	**router-solicitation**
11	**time-exceeded**
12	**parameter-problem**

Number	ICMP Type Name
13	**timestamp-request**
14	**timestamp-reply**
15	**information-request**
16	**information-reply**
17	**address-mask-request**
18	**address-mask-reply**
31	**conversion-error**
32	**mobile-redirect**

Examples

The following example shows how to use the **icmp-object** command in icmp-type configuration mode:

```
hostname(config)# object-group icmp-type icmp_allowed
hostname(config-icmp-type)# icmp-object echo
hostname(config-icmp-type)# icmp-object time-exceeded
hostname(config-icmp-type)# exit
```

Related Commands

Command	Description
clear configure object-group	Removes all the **object-group** commands from the configuration.
network-object	Adds a network object to a network object group.
object-group	Defines object groups to optimize your configuration.
port-object	Adds a port object to a service object group.
show running-config object-group	Displays the current object groups.

id-cert-issuer

To indicate whether the system accepts peer certificates issued by the CA associated with this trustpoint, use the **id-cert-issuer** command in crypto ca trustpoint configuration mode. Use the **no** form of this command to disallow certificates that were issued by the CA associated with the trustpoint. This is useful for trustpoints that represent widely used root CAs.

id-cert-issuer

no id-cert-issuer

Syntax Description

This command has no arguments or keywords.

Defaults

The default setting is enabled (identity certificates are accepted).

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Crypto ca trustpoint configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

Use this command to limit certificate acceptance to those issued by the subordinate certificate of a widely used root certificate. If you do not allow this feature, the security appliance rejects any IKE peer certificate signed by this issuer.

Examples

The following example enters crypto ca trustpoint configuration mode for trustpoint central, and lets an administrator accept identity certificates signed by the issuer for trustpoint central:

```
hostname(config)# crypto ca trustpoint central
hostname(ca-trustpoint)# id-cert-issuer
hostname(ca-trustpoint)#
```

Related Commands

Command	Description
crypto ca trustpoint	Enters trustpoint submode.
default enrollment	Returns enrollment parameters to their defaults.
enrollment retry count	Specifies the number of retries to attempt to send an enrollment request.

Command	Description
enrollment retry period	Specifies the number of minutes to wait before trying to send an enrollment request.
enrollment terminal	Specifies cut and paste enrollment with this trustpoint.

igmp

To reinstate IGMP processing on an interface, use the **igmp** command in interface configuration mode. To disable IGMP processing on an interface, use the **no** form of this command.

igmp

no igmp

Syntax Description

This command has no arguments or keywords.

Defaults

Enabled.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Interface configuration	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

Only the **no** form of this command appears in the running configuration.

Examples

The following example disables IGMP processing on the selected interface:

```
hostname(config-if)# no igmp
```

Related Commands

Command	Description
show igmp groups	Displays the multicast groups with receivers that are directly connected to the security appliance and that were learned through IGMP.
show igmp interface	Displays multicast information for an interface.

igmp access-group

To control the multicast groups that hosts on the subnet serviced by an interface can join, use the **igmp access-group** command in interface configuration mode. To disable groups on the interface, use the **no** form of this command.

igmp access-group *acl*

no igmp access-group *acl*

Syntax Description

acl	Name of an IP access list. You can specify a standard or and extended access list. However, if you specify an extended access list, only the destination address is matched; you should specify **any** for the source.

Defaults

All groups are allowed to join on an interface.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Interface configuration	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was moved to interface configuration mode. Earlier versions required you to enter multicast interface configuration mode, which is no longer available.

Examples

The following example limits hosts permitted by access list 1 to join the group:

```
hostname(config)# interface gigabitethernet 0/0
hostname(config-if)# igmp access-group 1
```

Related Commands

Command	Description
show igmp interface	Displays multicast information for an interface.

igmp forward interface

To enable forwarding of all IGMP host reports and leave messages received to the interface specified, use the **igmp forward interface** command in interface configuration mode. To remove the forwarding, use the **no** form of this command.

igmp forward interface *if-name*

no igmp forward interface *if-name*

Syntax Description

if-name	Logical name of the interface.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Interface configuration	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was moved to interface configuration mode. Earlier versions required you to enter multicast interface configuration mode, which is no longer available.

Usage Guidelines

Enter this command on the input interface. This command is used for stub multicast routing and cannot be configured concurrently with PIM.

Examples

The following example forwards IGMP host reports from the current interface to the specified interface:

```
hostname(config)# interface gigabitethernet 0/0
hostname(config-if)# igmp forward interface outside
```

Related Commands

Command	Description
show igmp interface	Displays multicast information for an interface.

igmp join-group

To configure an interface to be a locally connected member of the specified group, use the **igmp join-group** command in interface configuration mode. To cancel membership in the group, use the **no** form of this command.

igmp join-group *group-address*

no igmp join-group *group-address*

Syntax Description

group-address	IP address of the multicast group.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Interface configuration	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was moved to interface configuration mode. Earlier versions required you to enter multicast interface configuration mode, which is no longer available.

Usage Guidelines

This command configures a security appliance interface to be a member of a multicast group. The **igmp join-group** command causes the security appliance to both accept and forward multicast packets destined for the specified multicast group.

To configure the security appliance to forward the multicast traffic without being a member of the multicast group, use the **igmp static-group** command.

Examples

The following example configures the selected interface to join the IGMP group 255.2.2.2:

```
hostname(config)# interface gigabitethernet 0/0
hostname(config-if)# igmp join-group 225.2.2.2
```

Related Commands

Command	Description
igmp static-group	Configure the interface to be a statically connected member of the specified multicast group.

igmp limit

To limit the number of IGMP states on a per-interface basis, use the **igmp limit** command in interface configuration mode. To restore the default limit, use the **no** form of this command.

igmp limit *number*

no igmp limit [*number*]

Syntax Description

number	Number of IGMP states allowed on the interface. Valid values range from 0 to 500. The default value is 500. Setting this value to 0 prevents learned groups from being added, but manually defined memberships (using the **igmp join-group** and **igmp static-group** commands) are still permitted.

Defaults

The default is 500.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Interface configuration	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced. It replaced the **igmp max-groups** command.

Examples

The following example limits the number of hosts that can join on the interface to 250:

```
hostname(config)# interface gigabitethernet 0/0
hostname(config-if)# igmp limit 250
```

Related Commands

Command	Description
igmp	Reinstates IGMP processing on an interface.
igmp join-group	Configure an interface to be a locally connected member of the specified group.
igmp static-group	Configure the interface to be a statically connected member of the specified multicast group.

igmp query-interval

To configure the frequency at which IGMP host query messages are sent by the interface, use the **igmp query-interval** command in interface configuration mode. To restore the default frequency, use the **no** form of this command.

igmp query-interval *seconds*

no igmp query-interval *seconds*

Syntax Description

seconds	Frequency, in seconds, at which to send IGMP host query messages. Valid values range from 1 to 3600. The default is 125 seconds.

Defaults

The default query interval is 125 seconds.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Interface configuration	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was moved to interface configuration mode. Earlier versions required you to enter multicast interface configuration mode, which is no longer available.

Usage Guidelines

Multicast routers send host query messages to discover which multicast groups have members on the networks attached to the interface. Hosts respond with IGMP report messages indicating that they want to receive multicast packets for specific groups. Host query messages are addressed to the all-hosts multicast group, which has an address of 224.0.0.1 TTL value of 1.

The designated router for a LAN is the only router that sends IGMP host query messages:

- For IGMP Version 1, the designated router is elected according to the multicast routing protocol that runs on the LAN.
- For IGMP Version 2, the designated router is the lowest IP-addressed multicast router on the subnet.

If the router hears no queries for the timeout period (controlled by the **igmp query-timeout** command), it becomes the querier.

Caution Changing this value may severely impact multicast forwarding.

Examples

The following example changes the IGMP query interval to 120 seconds:

```
hostname(config)# interface gigabitethernet 0/0
hostname(config-if)# igmp query-interval 120
```

Related Commands

Command	Description
igmp query-max-response-time	Configures the maximum response time advertised in IGMP queries.
igmp query-timeout	Configures the timeout period before the router takes over as the querier for the interface after the previous querier has stopped querying.

igmp query-max-response-time

To specify the maximum response time advertised in IGMP queries, use the **igmp query-max-response-time** command in interface configuration mode. To restore the default response time value, use the **no** form of this command.

igmp query-max-response-time *seconds*

no igmp query-max-response-time [*seconds*]

Syntax Description

seconds	Maximum response time, in seconds, advertised in IGMP queries. Valid values are from 1 to 25. The default value is 10 seconds.

Defaults

10 seconds.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Interface configuration	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was moved to interface configuration mode. Earlier versions required you to enter multicast interface configuration mode, which is no longer available.

Usage Guidelines

This command is valid only when IGMP Version 2 or 3 is running.

This command controls the period during which the responder can respond to an IGMP query message before the router deletes the group.

Examples

The following example changes the maximum query response time to 8 seconds:

```
hostname(config)# interface gigabitethernet 0/0
hostname(config-if)# igmp query-max-response-time 8
```

Related Commands

Command	Description
igmp query-interval	Configures the frequency at which IGMP host query messages are sent by the interface.
igmp query-timeout	Configures the timeout period before the router takes over as the querier for the interface after the previous querier has stopped querying.

igmp query-timeout

To configure the timeout period before the interface takes over as the querier after the previous querier has stopped querying, use the **igmp query-timeout** command in interface configuration mode. To restore the default value, use the **no** form of this command.

igmp query-timeout *seconds*

no igmp query-timeout [*seconds*]

Syntax Description

seconds	Number of seconds that the router waits after the previous querier has stopped querying and before it takes over as the querier. Valid values are from 60 to 300 seconds. The default value is 255 seconds.

Defaults

The default query interval is 255 seconds.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Interface configuration	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

This command requires IGMP Version 2 or 3.

Examples

The following example configures the router to wait 200 seconds from the time it received the last query before it takes over as the querier for the interface:

```
hostname(config)# interface gigabitethernet 0/0
hostname(config-if)# igmp query-timeout 200
```

Related Commands

Command	Description
igmp query-interval	Configures the frequency at which IGMP host query messages are sent by the interface.
igmp query-max-response-time	Configures the maximum response time advertised in IGMP queries.

igmp static-group

To configure the interface to be a statically connected member of the specified multicast group, use the **igmp static-group** command in interface configuration mode. To remove the static group entry, use the **no** form of this command.

igmp static-group *group*

no igmp static-group *group*

Syntax Description

group	IP multicast group address.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Interface configuration	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

When configured with the **igmp static-group** command, the security appliance interface does not accept multicast packets destined for the specified group itself; it only forwards them. To configure the security appliance both accept and forward multicast packets for a speific multicast group, use the **igmp join-group** command. If the **igmp join-group** command is configured for the same group address as the **igmp static-group** command, the **igmp join-group** command takes precedence, and the group behaves like a locally joined group.

Examples

The following example adds the selected interface to the multicast group 239.100.100.101:

```
hostname(config)# interface gigabitethernet 0/0
hostname(config-if)# igmp static-group 239.100.100.101
```

Related Commands

Command	Description
igmp join-group	Configures an interface to be a locally connected member of the specified group.

igmp version

To configure which version of IGMP the interface uses, use the **igmp version** command in interface configuration mode. To restore version to the default, use the **no** form of this command.

igmp version {**1** | **2**}

no igmp version [**1** | **2**]

Syntax Description

1	IGMP Version 1.
2	IGMP Version 2.

Defaults

IGMP Version 2.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	**Routed**	**Transparent**	**Single**	**Context**	**System**
Interface configuration	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was moved to interface configuration mode. Earlier versions required you to enter multicast interface configuration mode, which is no longer available.

Usage Guidelines

All routers on the subnet must support the same version of IGMP. Hosts can have any IGMP version (1 or 2) and the security appliance will correctly detect their presence and query them appropriately.

Some commands require IGMP Version 2, such as the **igmp query-max-response-time** and **igmp query-timeout** commands.

Examples

The following example configures the selected interface to use IGMP Version 1:

```
hostname(config)# interface gigabitethernet 0/0
hostname(config-if)# igmp version 1
```

Related Commands

Command	Description
igmp query-max-response-time	Configures the maximum response time advertised in IGMP queries.
igmp query-timeout	Configures the timeout period before the router takes over as the querier for the interface after the previous querier has stopped querying.

ignore lsa mospf

To suppress the sending of syslog messages when the router receives link-state advertisement (LSA) Type 6 Multicast OSPF (MOSPF) packets, use the **ignore lsa mospf** command in router configuration mode. To restore the sending of the syslog messages, use the **no** form of this command.

ignore lsa mospf

no ignore lsa mospf

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Router configuration	•	—	•	—	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

Type 6 MOSPF packets are unsupported.

Examples

The following example cause LSA Type 6 MOSPF packets to be ignored:

```
hostname(config-router)# ignore lsa mospf
```

Related Commands

Command	Description
show running-config router ospf	Displays the OSPF router configuration.

imap4s

To enter IMAP4S configuration mode, use the **imap4s** command in global configuration mode. To remove any commands entered in IMAP4S command mode, use the **no** form of this command.

IMAP4 is a client/server protocol in which your Internet server receives and holds e-mail for you. You (or your e-mail client) can view just the heading and the sender of the letter and then decide whether to download the mail. You can also create and manipulate multiple folders or mailboxes on the server, delete messages, or search for certain parts or an entire note. IMAP requires continual access to the server during the time that you are working with your mail. IMAP4S lets you receive e-mail over an SSL connection.

imap4s

no imap4s

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	—	—	•

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

The following example shows how to enter IMAP4S configuration mode:

```
hostname(config)# imap4s
hostname(config-imap4s)#
```

Related Commands

Command	Description
clear configure imap4s	Removes the IMAP4S configuration.
show running-config imap4s	Displays the running configuration for IMAP4S.