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*

{ | } *ip_address net_mask* [*icmp_type*] *if_name*

Syntax Description

	Deny access if the conditions are matched.
	(Optional) ICMP message type (see Table 3).
	The interface name.
	The IP address of the host sending ICMP messages to the interface.
	The mask to be applied to .
	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 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 command disables pinging to an interface, and the 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.

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 statement is assumed.

Table 3 lists the supported ICMP type values.

Table 14-1 ICMP Types and Literals

ICMP Type	Literal
	echo-reply
3	unreachable
8	echo
11	time-exceeded

Examples

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

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

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

```
icmp permit host 172.16.2.15 echo-reply outside
icmp permit 172.22.1.0 255.255.0.0 echo-reply outside
icmp permit any unreachable outside
```

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 unreachable

icmp unreachable **no**

icmp unreachable rate-limit **burst-size** *size*

no icmp unreachable rate-limit *rate* **burst-size** *size*

					—

7.2(2)	This command was introduced.

icmp

set connection decrement-ttl

```
hostname(config-pmap)# class local_server
hostname(config-pmap-c)# set connection decrement-ttl
hostname(config-pmap-c)# exit
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
hostname(config)# icmp unreachable rate-limit 50 burst-size 1
```

	Clears the ICMP configuration.
	Enables the display of debug information for ICMP.
	Decrements the time to live value for a packet.
	Displays ICMP configuration.
	Configures the idle timeout for ICMP.

icmp-object

To add icmp-type object groups, use the **icmp-object**

no

icmp-object

no group-object

Syntax Description

	Specifies an icmp-type name.

Defaults

No default behavior or values.

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

Icmp-type configuration					—

Preexisting	This command was preexisting.

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
	echo-reply
	unreachable
	source-quench
	redirect
	alternate-address
	echo
	router-advertisement
	router-solicitation
	time-exceeded
	parameter-problem

	address-mask-request
	address-mask-reply
	conversion-error
	mobile-redirect

Examples

icmp-object

```
                    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
```

clear configure object-group	**object-group**
network-object	
object-group	Defines object groups to optimize your configuration.
	Adds a port object to a service object group.
	Displays the current object groups.

id-cert-issuer

Syntax Description

Defaults

Command Modes

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

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)#
hostname(ca-trustpoint)#
hostname(ca-trustpoint)#
```

Related Commands

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

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

id-mismatch

To enable logging for excessive DNS ID mismatches, use the command in parameters configuration mode. To disable this feature, use the form of this command.

[*number* *seconds*

number *seconds*

Syntax Description

number

seconds

Defaults

Command Modes

					—

Command History

Usage Guidelines

Examples

```
hostname(config)# policy-map type inspect dns preset_dns_map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# id-mismatch action log
```

class	
class-map type inspect	
policy-map	Creates a Layer 3/4 policy map.
show running-config policy-map	Display all current policy map configurations.

id-randomization

To randomize the DNS identifier for a DNS query, use the command in parameters configuration mode. To disable this feature, use the form of this command.

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled by default. The DNS identifier from the DNS query does not get modified.

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
Parameters configuration	•	•	•	•	

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

ID randomization helps protect against cache poisening attacks.

Examples

The following example shows how to enable ID randomization in a DNS inspection policy map:

```
hostname(config-pmap-p)# id-randomization
```

Related Commands

Command	Description
	Identifies a class map name in the policy map.
	Creates an inspection class map to match traffic specific to an application.
	Creates a Layer 3/4 policy map.
	Display all current policy map configurations.

igmp

To reinstate IGMP processing on an interface, use the command in interface configuration mode. To disable IGMP processing on an interface, use the form of this command.

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 form of this command appears in the running configuration.

Examples

The following example disables IGMP processing on the selected interface:

```
hostname(config-if)#
```

Related Commands

Command	Description
	Displays the multicast groups with receivers that are directly connected to the security appliance and that were learned through IGMP.
	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 command in interface configuration mode. To disable groups on the interface, use the form of this command.

acl

acl

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 for the source.

All groups are allowed to join on an interface.

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

Interface configuration				—	

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.

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

```
interface gigabitethernet 0/0
   igmp access-group 1
```

	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 command in interface configuration mode. To remove the forwarding, use the form of this command.

if-name

if-name

Syntax Description

if-name

Defaults

Command Modes

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
	•		•		

Command History

Release	Modification

Usage Guidelines

Examples

Related Commands

Command	Description

igmp join-group

group-address

group-address

Syntax Description

group-address

Defaults

Command Modes

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
	•		•		

Command History

Release	Modification

Usage Guidelines

Examples

Related Commands

Command	Description

igmp limit

number

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 and commands) are still permitted.

Defaults

Command Modes

Interface configuration				—	

Command History

7.0(1)	This command was introduced. It replaced the command.

Examples

Related Commands

	Reinstates IGMP processing on an interface.
	Configure an interface to be a locally connected member of the specified group.
	Configure the interface to be a statically connected member of the specified multicast group.

igmp query-interval

seconds

seconds

Syntax Description

seconds

Defaults

Command Modes

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
	•		•		

Command History

Release	Modification

Usage Guidelines

-
-

Caution

Examples

```
igmp query-interval 120
```

Related Commands

Command	Description

igmp query-max-response-time

Syntax Description

Defaults

Command Modes

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
	•		•		

Command History

Release	Modification

Usage Guidelines

Examples

```
interface gigabitethernet 0/0
   igmp query-max-response-time 8
```

Related Commands

Command	Description

igmp query-timeout

]

		—			—

```
interface gigabitethernet 0/0
   igmp query-timeout 200
```

igmp query-interval

igmp query-max-response-time

igmp static-group
no

igmp static-group

no igmp static-group

		—			—

igmp static-group

igmp

join-group **igmp join-group**
igmp static-group **igmp join-group**

```
interface gigabitethernet 0/0
   igmp static-group 239.100.100.101
```

igmp join-group

igmp version

no

igmp version 1 2

no igmp version 1 2

1	
2	

		—			—

igmp query-max-response-time **igmp query-timeout**

```
interface gigabitethernet 0/0
   igmp version 1
```

igmp **query-max-response-time**
igmp query-timeout

ignore lsa mospf
no

ignore lsa mospf

no ignore lsa mospf

		—			—

ignore lsa mospf

show running-config
router ospf

im

no

im

no im

					—

class
class-map type inspect
policy-map
show running-config policy-map

imap4s

imap4s

no

imap4s

no imap4s

Syntax Description

Defaults

Command Modes

Command History

Examples

imap4s

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