CHAPTER 38

packet-tracer through ping Commands

packet-tracer

To enable packet tracing capabilities for troubleshooting by specifying the 5-tuple to test firewall rules, use the **packet-tracer** command in privileged EXEC mode.

packet-tracer input [**1-255**] [**A.B.C.D**] [*ifc_name*] [**icmp** [*sip* | **user** *username* | **security-group** [**name** *name* | **tag** *tag*] **fqdn** *fqdn-string*] *type code ident* [*dip* **security-group** [**name** *name* | **tag** *tag*] | **fqdn** *fqdn-string*]] | [**tcp** [*sip* | **user** *username* | **fqdn** *fqdn-string*] *sport* [*dip* | **fqdn** *fqdn-string*] *dport*] | [**udp** [*sip* | **user** *username* | **fqdn** *fqdn-string*] *sport* [*dip* | **fqdn** *fqdn-string*] *dport*] | [**rawip** [*sip* | **user** *username* | **fqdn** *fqdn-string*] [*dip* | **fqdn** *fqdn-string*]] [**detailed**] [**xml**]

Syntax Description

1-255	Specifies the IP protocol ID or next header range.
A.B.C.D	Specifies the IPv4 source address.
code	Specifies the ICMP code.
detailed	(Optional) Provides detailed trace results information.
dip	Specifies the destination IP address for the packet trace.
dport	Specifies the destination port for the packet trace.
fqdn *fqdn-string*	Specifies the fully qualified domain name of the host, which can be both the source and destination IP address. Supports the FQDN for IPv4 only.
icmp	Specifies the protocol to use is ICMP.
ident	Specifies the ICMP identifier.
input *ifc_name*	Specifies the name of the source interface on which to trace the packets.
name *name*	Specifies the security group name.
rawip	Specifies the protocol to use is raw IP.
security-group	Specifies the source and destination security groups.
sip	Specifies the source IP address for the packet trace.
sport	Specifies the source port for the packet trace.
tag *tag*	Specifies the security group tag.
tcp	Specifies the protocol to use is TCP.
type	Specifies the ICMP type.
udp	Specifies the protocol to use is UDP.
user *username*	Specifies the user identity in the format of [domain\user] if the user is identified as the source IP address. The domain can be a maximum of 32 characters. The user can be a maximum of 64 characters. Only the most recent logon IP address for a user is used for testing.
xml	(Optional) Displays the trace results in XML format.
X:X:X:X::X	Specifies the IPv6 source address.

Defaults

This command has no default settings.

Command Modes

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

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC mode	•	—	•	•	•

Command History

Release	Modification
7.2(1)	This command was introduced.
8.4(2)	Added two keyword-argument pairs: **user** *username* and **fqdn** *fqdn string*. Renamed and redefined several keywords. Added support for IPv6 source addresses.
9.0(1)	Support for user identity was added. Only IPv4 fully qualified domain names (FQDNs) are supported.

Usage Guidelines

In addition to capturing packets, it is possible to trace the lifespan of a packet through the ASA to see if it is behaving as expected. The **packet-tracer** command enables you to do the following:

- Debug all packet drops in production network.
- Verify the configuration is working as intended.
- Show all rules applicable to a packet along with the CLI lines that caused the rule addition.
- Show a time line of packet changes in a data path.
- Inject tracer packets into the data path.
- Search for an IPv4 or IPv6 address based on the user identity and the FQDN.

The **packet-tracer** command provides detailed information about the packets and how they are processed by the ASA. If a command from the configuration did not cause the packet to drop, the **packet-tracer** command provides information about the cause in an easily readable format. For example if a packet was dropped because of an invalid header validation, the following message appears: “packet dropped due to bad ip header (reason).”

You can specify a user identity in the format of domain\user in the source part of this command. The ASA searches for the user's IP address and uses it in packet trace testing. If a user is mapped to multiple IP addresses, the most recent login IP address is used and the output shows that more IP address-user mapping exists. If user identity is specified in the source part of this command, then the ASA searches for the user's IPv4 or IPv6 address based on the destination address type that the user entered.

This command supports a FQDN, which means that you can also specify a FQDN as both the source and destination address. The ASA performs DNS lookup first, then retrieves the first returned IP address for packet construction. If multiple IP addresses are resolved, the output shows that more DNS resolved IP addresses exist. Only an IPv4 FQDN is supported.

Examples

To enable packet tracing from inside host 10.2.25.3 to external host 209.165.202.158 with detailed information, enter the following:

```
hostname# packet-tracer input inside tcp 10.2.25.3 www 209.165.202.158 aol detailed
```

The following example shows how to enable packet tracing from inside host 10.0.0.2 to outside host 20.0.0.2 with the username of CISCO\abc:

```
hostname# packet-tracer input inside icmp user CISCO\abc 0 0 1 20.0.0.2

Source: CISCO\abc 10.0.0.2

Phase: 1
Type: ROUTE-LOOKUP
Subtype: input
Result: ALLOW
Config:
Additional Information:
in 20.0.0. 255.255.255.0 outside
...
Result:
input-interface: inside
input-status: up
input-line-status: up
output-interfce: outside
output-status: up
output-line-status: up
Action: allow
```

The following example shows how to enable packet tracing from inside host 20.0.0.2 with the username of CISCO\abc and map this username to IP address 10.0.0.2:

```
hostname# packet-tracer input inside tcp user CISCO\abc 1000 20.0.0.2 23

Mapping user CISCO\abc to IP address 10.0.0.2
(More mappings exist. Please run "show user-identity ip-of-user <username>" to check.)

Phase: 1
Type: ROUTE-LOOKUP
Subtype: input
Result: ALLOW
Config:
Additional Information:
in 20.0.0. 255.255.255.0 outside
...
```

The following example shows how to enable packet tracing from inside host 20.0.0.2 with the username of CISCO\abc, map this username to IP address 10.0.0.2, and display the trace results in XML format:

```
<Source>
<user>CISCO\abc</user>
<user-ip>10.0.0.2</user-ip>
<more-ip>1</more-ip>
</Source>

<Phase>
<id>1</id>
<type>ROUTE-LOOKUP</type>
<subtype>input</subtype>
<result>ALLOW</result>
<config>
</config>
<extra>
in 20.0.0.0 255.255.255.0 outside
</extra>
</Phase>
```

The following example shows the error message that results from a packet trace from inside host 1000::123 in a search for the destination IPv6 address for the username of CISCO\abc:

```
hostname# packet-tracer input inside tcp user CISCO\abc 1000 1000::123
ERROR: No active IPv6 address found for user cisco.com\abc
```

The following example shows the results in XML format from a packet trace from inside host 1000::123 in a search for the destination IPv6 address for the username of CISCO\abc after this username has been mapped to an IPv6 address:

```
hostname# user-i s user CISCO\abc 2000::2
hostname# packet-tracer input inside tcp user CISCO\abc 1000 1000::123 xml

<Source>
<user>CISCO\abc</user>
<user-ip>2000::2</user-ip>
<more-ip>0</more-ip>
</Source>

<Result>
<input-interface>inside</input-interface>
<input-status>up</input-status>
```

The following example shows the error message that results from a packet trace from inside host 1000::123 when the username of CISCO\ancdef has not yet been created on the ASA:

```
hostname# packet-tracer input inside tcp user CISCO\ancdef 1000 1000::123
ERROR: User CISCO\ancdef does not exist
```

The following example shows how to enable a packet trace from inside host example.com to external host abc.idfw.com, in which the inside host has been identified as the FQDN of the source IP address, and the external host has been identified as the FQDN of the destination IP address:

```
hostname# packet-tracer input inside tcp fqdn xyz.example.com 1000 fqdn abc.example.com 23
Mapping FQDN xyz.example.com to IP address 10.0.0.2
(More IP addresses resolved. Please run "show dns-host" to check.)

Mapping FQDN abc.example.com to IP address 20.0.0.2
(More IP addresses resolved. Please run "show dns-host" to check.)

Phase: 1
Type: ROUTE-LOOKUP
Subtype: input
Result: ALLOW
Config:
Additional Information:
```

The following example shows how to enable a packet trace from inside host xyz.example.com to external host abc.example.com, in which the inside host has been identified as the FQDN of the source IP address and the external host has been identified as the FQDN of the destination IP address, and display the input in XML format:

```
hostname# packet-tracer input inside tcp fqdn xyz.example.com 1000 fqdn abc.example.com 23
xml
<Source>
<fqdn>xyz.example.com</user>
<fqdn-ip>10.0.0.2</fqdn-ip>
<more-ip>1</more-ip>
</Source>

<Destination>
<fqdn>abc.example.com</user>
<fqdn-ip>20.0.0.2</fqdn-ip>
<more-ip>1</more-ip>
</Destination>
```

```
Phase: 1
Type: ROUTE-LOOKUP
Subtype: input
Result: ALLOW
Config:
Additional Information:
```

The following example shows the error message that results from a packet trace in which the FQDN of the source IP address cannot be resolved:

```
hostname# packet-tracer input inside icmp fqdn ns10.example.com 0 0 2 20.0.0.2
ERROR: Cannot resolve ns10.example.com
```

Related Commands

Command	Description
capture	Captures packet information, including trace packets.
show capture	Displays the capture configuration when no options are specified.

page style

To customize the WebVPN page displayed to WebVPN users when they connect to the security appliance, use the **page style** command in webvpn customization configuration mode. To remove the command from the configuration and cause the value to be inherited, use the **no** form of this command.

page style *value*

[**no**] **page style** *value*

Syntax Description

value	Cascading Style Sheet (CSS) parameters (maximum 256 characters).

Defaults

The default page style is background-color:white;font-family:Arial,Helv,sans-serif

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
Webvpn customization configuration	•	—	•	—	—

Command History

Release	Modification
7.1(1)	This command was introduced.

Usage Guidelines

The **style** option is expressed as any valid Cascading Style Sheet (CSS) parameters. Describing these parameters is beyond the scope of this document. For more information about CSS parameters, consult CSS specifications at the World Wide Web Consortium (W3C) website at www.w3.org. Appendix F of the CSS 2.1 Specification contains a convenient list of CSS parameters, and is available at www.w3.org/TR/CSS21/propidx.html.

Here are some tips for making the most common changes to the WebVPN pages—the page colors:

- You can use a comma-separated RGB value, an HTML color value, or the name of the color if recognized in HTML.
- RGB format is 0,0,0, a range of decimal numbers from 0 to 255 for each color (red, green, blue); the comma separated entry indicates the level of intensity of each color to combine with the others.
- HTML format is #000000, six digits in hexadecimal format; the first and second represent red, the third and fourth green, and the fifth and sixth represent blue.

Note To easily customize the WebVPN pages, we recommend that you use ASDM, which has convenient features for configuring style elements, including color swatches and preview capabilities.

Examples

The following example customizes the page style to large:

```
F1-asa1(config)# webvpn
F1-asa1(config-webvpn)# customization cisco
F1-asa1(config-webvpn-custom)# page style font-size:large
```

Related Commands

Command	Description
logo	Customizes the logo on the WebVPN page.
title	Customizes the title of the WebVPN page

pager

To set the default number of lines on a page before the "---More---" prompt appears for Telnet sessions, use the **pager** command in global configuration mode.

pager [**lines**] *lines*

Syntax Description

[**lines**] *lines*	Sets the number of lines on a page before the "---More---" prompt appears. The default is 24 lines; 0 means no page limit. The range is 0 through 2147483647 lines. The **lines** keyword is optional and the command is the same with or without it.

Defaults

The default is 24 lines.

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 changed from a privileged EXEC mode command to a global configuration mode command. The **terminal pager** command was added as the privileged EXEC mode command.

Usage Guidelines

This command changes the default pager line setting for Telnet sessions. If you want to temporarily change the setting only for the current session, use the **terminal pager** command.

If you Telnet to the admin context, then the pager line setting follows your session when you change to other contexts, even if the **pager** command in a given context has a different setting. To change the current pager setting, enter the **terminal pager** command with a new setting, or you can enter the **pager** command in the current context. In addition to saving a new pager setting to the context configuration, the **pager** command applies the new setting to the current Telnet session.

Examples

The following example changes the number of lines displayed to 20:

```
hostname(config)# pager 20
```

Related Commands

Command	Description
clear configure terminal	Clears the terminal display width setting.
show running-config terminal	Displays the current terminal settings.
terminal	Allows system log messsages to display on the Telnet session.
terminal pager	Sets the number of lines to display in a Telnet session before the "`---more---`" prompt. This command is not saved to the configuration.
terminal width	Sets the terminal display width in global configuration mode.

parameters

To enter parameters configuration mode to set parameters for an inspection policy map, use the **parameters** command in policy-map configuration mode.

parameters

Syntax Description

This command has no arguments or keywords.

Defaults

No default behaviors 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
Policy-map configuration	•	•	•	•	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

Modular Policy Framework lets you configure special actions for many application inspections. When you enable an inspection engine using the **inspect** command in the Layer 3/4 policy map (the **policy-map** command), you can also optionally enable actions as defined in an inspection policy map created by the **policy-map type inspect** command. For example, enter the **inspect dns dns_policy_map** command where dns_policy_map is the name of the inspection policy map.

An inspection policy map may support one or more **parameters** commands. Parameters affect the behavior of the inspection engine. The commands available in parameters configuration mode depend on the application.

Examples

The following example shows how to set the maximum message length for DNS packets in the default inspection policy map:

```
hostname(config)# policy-map type inspect dns preset_dns_map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# message-length maximum 512
```

Related Commands

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

participate

To force the device to participate in the virtual load-balancing cluster, use the **participate** command in VPN load-balancing configuration mode. To remove a device from participation in the cluster, use the **no** form of this command.

participate

no participate

Syntax Description

This command has no arguments or keywords.

Defaults

The default behavior is that the device does not participate in the vpn load-balancing cluster.

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
VPN load-balancing configuration	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

You must first configure the interface using the **interface** and **nameif** commands, and use the **vpn load-balancing** command to enter VPN load-balancing mode. You must also have previously configured the cluster IP address using the **cluster ip** command and configured the interface to which the virtual cluster IP address refers.

This command forces this device to participate in the virtual load-balancing cluster. You must explicitly issue this command to enable participation for a device.

All devices that participate in a cluster must share the same cluster-specific values: ip address, encryption settings, encryption key, and port.

Note When using encryption, you must have previously configured the command **isakmp enable** *inside*, where *inside* designates the load-balancing inside interface. If isakmp is not enabled on the load-balancing inside interface, you get an error message when you try to configure cluster encryption.

If isakmp was enabled when you configured the **cluster encryption** command, but was disabled before you configured the **participate** command, you get an error message when you enter the **participate** command, and the local device will not participate in the cluster.

Examples

The following is an example of a VPN load-balancing command sequence that includes a **participate** command that enables the current device to participate in the vpn load-balancing cluster:

```
hostname(config)# interface GigabitEthernet 0/1
hostname(config-if)# ip address 209.165.202.159 255.255.255.0
hostname(config)# nameif test
hostname(config)# interface GigabitEthernet 0/2
hostname(config-if)# ip address 209.165.201.30 255.255.255.0
hostname(config)# nameif foo
hostname(config)# vpn load-balancing
hostname(config-load-balancing)# interface lbpublic test
hostname(config-load-balancing)# interface lbprivate foo
hostname(config-load-balancing)# cluster ip address 209.165.202.224
hostname(config-load-balancing)# participate
```

Related Commandsh

Command	Description
vpn load-balancing	Enter VPN load-balancing mode.

passive-interface (RIP)

To disable the transmission of RIP routing updates on an interface, use the **passive-interface** command in router configuration mode. To reenable RIP routing updates on an interface, use the **no** form of this command.

passive-interface {**default** | *if_name*}

no passive-interface {**default** | *if_name*}

Syntax Description

default	(Optional) Set all interfaces to passive mode.
if_name	(Optional) Sets the specified interface to passive mode.

Defaults

All interfaces are enabled for active RIP when RIP is enabled.

If an interface or the **default** keyword is not specified, the commands defaults to **default** and appears in the configuration as passive-interface default.

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
7.2(1)	This command was introduced.
9.0(1)	Multiple context mode is supported.

Usage Guidelines

Enables passive RIP on the interface. The interface listens for RIP routing broadcasts and uses that information to populate the routing tables, but does not broadcast routing updates.

Examples

The following example sets the outside interface to passive RIP. The other interfaces on the security appliance send and receive RIP updates.

```
hostname(config)# router rip
hostname(config-router)# network 10.0.0.0
hostname(config-router)# passive-interface outside
```

Related Commands

Command	Description
clear configure rip	Clears all RIP commands from the running configuration.
router rip	Enables the RIP routing process and enters rip router configuration mode.
show running-config rip	Displays the RIP commands in the running configuration.

passive-interface (EIGRP)

To disable the sending and receiving of EIGRP routing updates on an interface, use the **passive-interface** command in router configuration mode. To reenable routing updates on an interface, use the **no** form of this command.

passive-interface {**default** | *if_name*}

no passive-interface {**default** | *if_name*}

Syntax Description

default	(Optional) Set all interfaces to passive mode.
if_name	(Optional) The name of the interface, as specified by the **nameif** command, to passive mode.

Defaults

All interfaces are enabled for active routing (sending and receiving routing updates) when routing is enabled for that 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**
Router configuration	•	—	•	—	—

Command History

Release	Modification
7.2(1)	This command was introduced.
8.0(2)	Support for EIGRP routing was added.

Usage Guidelines

Enables passive routing on the interface. For EIGRP, this disables the transmission and reception of routing updates on that interface.

You can have more than one **passive-interface** command in the EIGRP configuration. You can use the **passive-interface default** command to disable EIGRP routing on all interfaces, and then use the **no passive-interface** command to enable EIGRP routing on specific interfaces.

Examples

The following example sets the outside interface to passive EIGRP. The other interfaces on the security appliance send and receive EIGRP updates.

```
hostname(config)# router eigrp 100
hostname(config-router)# network 10.0.0.0
hostname(config-router)# passive-interface outside
```

The following example sets all interfaces except the inside interface to passive EIGRP. Only the inside interface will send and receive EIGRP updates.

```
hostname(config)# router eigrp 100
hostname(config-router)# network 10.0.0.0
hostname(config-router)# passive-interface default
hostname(config-router)# no passive-interface inside
```

Related Commands

Command	Description
show running-config router	Displays the router configuration commands in the running configuration.

passive-interface (OSPFv3)

To suppress the sending and receiving of routing updates on an interface or across all interfaces that are using an OSPFv3 process, use the **passive-interface** command in router configuration mode. To reenable routing updates on an interface or across all intterfaces that are using an OSPFv3 process, use the **no** form of this command.

passive-interface [*interface_name*]

no passive-interface [*interface_name*]

Syntax Description

interface_name	(Optional) Specifies the interface name on which the OSPFv3 process is running.

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
9.0(1)	This command was introduced.

Usage Guidelines

This command enables passive routing on an interface.

Examples

The following example suppresses the sending and receiving of routing updates on the inside interface.

```
hostname(config)# ipv6 router ospf 10
hostname(config-rtr)# passive-interface interface
hostname(config-rtr)#
```

Related Commands

Command	Description
show running-config router	Displays the router configuration commands in the running configuration.

passwd, password

To set the login password for Telnet, use the **passwd** or **password** command in global configuration mode. To reset the password, use the **no** form of this command.

{**passwd** | **password**} *password* [**encrypted**]

no {**passwd** | **password**} *password*

Syntax Description

encrypted	(Optional) Specifies that the password is in encrypted form. The password is saved in the configuration in encrypted form, so you cannot view the original password after you enter it. If for some reason you need to copy the password to another ASA but do not know the original password, you can enter the **passwd** command with the encrypted password and this keyword. Normally, you only see this keyword when you enter the **show running-config passwd** command.
passwd | **password**	You can enter either command; they are aliased to each other.
password	Sets the password as a case-sensitive string of up to 80 characters. The password must not contains spaces.

Defaults

9.1(1): The default password is “cisco.”

9.1(2): 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.
8.4(2)	The SSH default username is no longer supported; you can no longer connect to the ASA using SSH with the **pix** or **asa** username and the login password.
9.0(2), 9.1(2)	The default password, “cisco,” has been removed; you must actively set a login password. Using the **no passwd** or **clear configure passwd** command removes the password; formerly, it reset it to the default of “cisco.”

Usage Guidelines

When you enable Telnet with the **telnet** command, you can log in with the password set by the **passwd** comamnd. After you enter the login password, you are in user EXEC mode. If you configure CLI authentication per user for Telnet using the **aaa authentication telnet console** command, then this password is not used.

This password is also used for Telnet sessions from the switch to the ASASM (see the **session** command).

Examples

The following example sets the password to Pa$$w0rd:

```
hostname(config)# passwd Pa$$w0rd
```

The following example sets the password to an encrypted password that you copied from another ASA:

```
hostname(config)# passwd jMorNbK0514fadBh encrypted
```

Related Commands

Command	Description
clear configure passwd	Clears the login password.
enable	Enters privileged EXEC mode.
enable password	Sets the enable password.
show curpriv	Shows the currently logged in username and the user privilege level.
show running-config passwd	Shows the login password in encrypted form.

password encryption aes

To enable password encryption , use the password encryption aes command in global configuration mode. To disable password encryption, use the **no** form of this command.

password encryption aes

no password encryption aes

Syntax Description

This command has no arguments or keywords.

Defaults

No default behaviors 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
8.3(1)	This command was introduced.

Usage Guidelines

As soon as password encryption is turned on and master pass phrase is available all the user passwords will be encrypted. The running configuration will show the passwords in the encrypted format. If the pass phrase is not configured at the time of enabling password encryption the command will succeed in anticipation that the pass phrase will be available in future. This command will be automatically synchronized between the failover peers.

The **write erase** command when followed by the **reload** command will remove the master passphrase if it is lost.

Examples

The following example enables password encryption:

```
Router (config)# password encryption aes
```

Related Commands

Command	Description
key config-key password-encryption	Sets the passphrase used for generating the encryption key.
write erase	Removes the master passphrase if it is lost when followed by the **reload** command.

password (crypto ca trustpoint)

To specify a challenge phrase that is registered with the CA during enrollment, use the **password** command in crypto ca trustpoint configuration mode. To restore the default setting, use the **no** form of this command.

password *string*

no password

Syntax Description

string	Specifies the name of the password as a character string. The first character cannot be a number. The string can contain any alphanumeric characters, including spaces, up to 80 characters. You cannot specify the password in the format number-space-anything. The space after the number causes problems. For example, "hello 21" is a legal password, but "21 hello" is not. The password checking is case sensitive. For example, the password "Secret" is different from the password "secret".

Defaults

The default setting is to not include a password.

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

This command lets you specify the revocation password for the certificate before actual certificate enrollment begins. The specified password is encrypted when the updated configuration is written to NVRAM by the ASA.

The CA typically uses a challenge phrase to authenticate a subsequent revocation request.

If this command is enabled, you will not be prompted for a password during certificate enrollment.

Examples

The following example enters crypto ca trustpoint configuration mode for trustpoint central, and includes a challenge phrase registered with the CA in the enrollment request for trustpoint central:

```
hostname(config)# crypto ca trustpoint central
hostname(ca-trustpoint)# password zzxxyy
```

Related Commands

Command	Description
crypto ca trustpoint	Enters trustpoint configuration mode.
default enrollment	Returns enrollment parameters to their defaults.

password-management

To enable password management, use the **password-management** command in tunnel-group general-attributes configuration mode. To disable password management, use the **no** form of this command. To reset the number of days to the default value, use the **no** form of the command with the **password-expire-in-days** keyword specified.

password-management [**password-expire-in-days** *days*]

no password-management

no password-management password-expire-in-days [*days*]

Syntax Description

days	Specifies the number of days (0 through 180) before the current password expires. This parameter is required if you specify the **password-expire-in-days** keyword.
password-expire-in-days	(Optional) Indicates that the immediately following parameter specifies the number of days before the current password expires that the ASA starts warning the user about the pending expiration. This option is valid only for LDAP servers. See the Usage Notes section for more information.

Defaults

The default is no password management. If you do not specify the **password-expire-in-days** keyword for an LDAP server, the default length of time to start warning before the current password expires is 14 days.

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
Tunnel-group general-attributes configuration	•	—	•	—	—

Command History

Release	Modification
7.1(1)	This command was introduced.

Usage Guidelines

The ASA supports password management for the RADIUS and LDAP protocols. It supports the "password-expire-in-days" option for LDAP only.

You can configure password management for IPsec remote access and SSL VPN tunnel-groups.

When you configure the password-management command, the ASA notifies the remote user at login that the user's current password is about to expire or has expired. The ASA then offers the user the opportunity to change the password. If the current password has not yet expired, the user can still log in using that password.

This command is valid for AAA servers that support such notification; that is, natively to LDAP servers and RADIUS proxied to an NT 4.0 or Active Directory server. The ASA ignores this command if RADIUS or LDAP authentication has not been configured.

Note Some RADIUS servers that support MSCHAP currently do not support MSCHAPv2. This command requires MSCHAPv2 so please check with your vendor.

The ASA, releases 7.1 and later, generally supports password management for the following connection types when authenticating with LDAP or with any RADIUS configuration that supports MS-CHAPv2:

- AnyConnect VPN Client (ASA software version 8.0 and higher)
- IPsec VPN Client
- Clientless SSL VPN (ASA software version 8.0 and higher)WebVPN (ASA software versions 7.1 through 7.2.x)
- SSL VPN Client full tunneling client

These RADIUS configurations include RADIUS with LOCAL authentication, RADIUS with Active Directory/Kerberos Windows DC, RADIUS with NT/4.0 Domain, and RADIUS with LDAP.

Password management is *not* supported for any of these connection types for Kerberos/Active Directory (Windows password) or NT 4.0 Domain. The RADIUS server (for example, Cisco ACS) could proxy the authentication request to another authentication server. However, from the ASA perspective, it is talking only to a RADIUS server.

Note For LDAP, the method to change a password is proprietary for the different LDAP servers on the market. Currently, the ASA implements the proprietary password management logic only for Microsoft Active Directory and Sun LDAP servers.

Native LDAP requires an SSL connection. You must enable LDAP over SSL before attempting to do password management for LDAP. By default, LDAP uses port 636.

Note that this command does not change the number of days before the password expires, but rather, the number of days ahead of expiration that the ASA starts warning the user that the password is about to expire.

If you do specify the **password-expire-in-days** keyword, you must also specify the number of days.

Specifying this command with the number of days set to 0 disables this command. The ASA does not notify the user of the pending expiration, but the user can change the password after it expires.

Note Radius does not provide a password change, or provide a password change prompt.

Examples

The following example sets the days before password expiration to begin warning the user of the pending expiration to 90 for the WebVPN tunnel group "testgroup":

```
hostname(config)# tunnel-group testgroup type webvpn
hostname(config)# tunnel-group testgroup general-attributes
hostname(config-tunnel-general)# password-management password-expire-in-days 90
hostname(config-tunnel-general)#
```

The following example uses the default value of 14 days before password expiration to begin warning the user of the pending expiration for the IPsec remote access tunnel group “QAgroup”:

```
hostname(config)# tunnel-group QAgroup type ipsec-ra
hostname(config)# tunnel-group QAgroup general-attributes
hostname(config-tunnel-general)# password-management
hostname(config-tunnel-general)#
```

Related Commands

Command	Description
clear configure passwd	Clears the login password.
passwd	Sets the login password.
radius-with-expiry	Enables negotiation of password update during RADIUS authentication (Deprecated).
show running-config passwd	Shows the login password in encrypted form.
tunnel-group general-attributes	Configures the tunnel-group general-attributes values.

password-parameter

To specify the name of the HTTP POST request parameter in which a user password must be submitted for SSO authentication, use the **password-parameter** command in aaa-server-host configuration mode. This is an SSO with the HTTP Forms command.

password-parameter *string*

Note To configure SSO with HTTP correctly, you must have a thorough working knowledge of authentication and HTTP exchanges.

Syntax Description

string	The name of the password parameter included in the HTTP POST request. The maximum password length is 128 characters.

Defaults

No default value or behavior.

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
Aaa-server-host configuration	•	—	•	—	—

Command History

Release	Modification
7.1(1)	This command was introduced.

Usage Guidelines

The WebVPN server of the ASA uses an HTTP POST request to submit a single sign-on authentication request to an authenticating web server. The required command **password-parameter** specifies that the POST request must include a user password parameter for SSO authentication.

Note At login, the user enters the actual password value, which is entered into the POST request and passed on to the authenticating web server.

Examples

The following example, entered in aaa-server-host configuration mode, specifies a password parameter named user_password:

```
hostname(config)# aaa-server testgrp1 host example.com
hostname(config-aaa-server-host)# password-parameter user_password
```

Related Commands

Command	Description
action-uri	Specifies a web server URI to receive a username and password for single sign-on authentication.
auth-cookie-name	Specifies a name for the authentication cookie.
hidden-parameter	Creates hidden parameters for exchange with the authenticating web server.
start-url	Specifies the URL at which to retrieve a pre-login cookie.
user-parameter	Specifies the name of the HTTP POST request parameter in which a username must be submitted for SSO authentication.

password-policy authenticate enable

To determine whether users are allowed to modify their own user account, use the **password-policy authenticate enable** command in global configuration mode. To set the corresponding password policy attribute to its default value, use the **no** form of this command.

password-policy authenticate enable

no password-policy authenticate enable

Syntax Description

This command has no arguments or keywords.

Defaults

Authentication is disabled by default.

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
9.1(2)	This command was introduced.

Usage Guidelines

If authentication is enabled, the **username** command does not allow users to change their own password or delete their own account. In addition, the **clear configure username** command does not allow users to delete their own account.

Examples

The following example shows how to enable users to modify their user account:

```
hostname(config)# password-policy authenticate enable
```

Related Commands

Command	Description
password-policy minimum-changes	Sets the minimum number of characters that must be changed between new and old passwords.
password-policy minimum length	Sets the minimum length of passwords.
password-policy minimum-lowercase	Sets the minimum number of lower case characters that passwords may have.

password-policy lifetime

To set password policy for the current context and the interval in days after which passwords expire, use the **password-policy lifetime** command in global configuration mode. To set the corresponding password policy attribute to its default value, use the **no** form of this command.

password-policy lifetime *value*

no password-policy lifetime *value*

Syntax Description

value	Specifies the password lifetime. Valid values range from 0 to 65535 days.

Defaults

The default lifetime value is 0 days.

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
9.1(2)	This command was introduced.

Usage Guidelines

Passwords have a specified maximum lifetime. A lifetime interval of 0 days specifies that local user passwords never expire. Note that passwords expire at 12:00 a.m. of the day following lifetime expiration.

Examples

The following example specifies a password lifetime value of 10 days:

```
hostname(config)# password-policy lifetime 10
```

Related Commands

Command	Description
password-policy minimum-changes	Sets the minimum number of characters that must be changed between new and old passwords.
password-policy minimum length	Sets the minimum length of passwords.
password-policy minimum-lowercase	Sets the minimum number of lower case characters that passwords may have.

password-policy minimum-changes

To set the minimum number of characters that must be changed between new and old passwords, use the **password-policy minimum-changes** command in global configuration mode. To set the corresponding password policy attribute to its default value, use the **no** form of this command.

password-policy minimum-changes *value*

no password-policy minimum-changes *value*

Syntax Description

value	Specifies the number of characters that must be changed between new and old passwords. Valid values range from 0 to 64 characters.

Defaults

The default number of changed characters is 0.

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
9.1(2)	This command was introduced.

Usage Guidelines

New passwords must include a minimum of 4 character changes from the current password and are considered changed only if they do not appear anywhere in the current password.

Examples

The following example specifies a minimum number of character changes between old and new passwords of 6 characters:

```
hostname(config)# password-policy minimum-changes 6
```

Related Commands

Command	Description
password-policy lifetime	Sets the password lifetime in days after which passwords expire.
password-policy minimum-length	Sets the minimum length of passwords.
password-policy minimum-lowercase	Sets the minimum number of lowercase characters that passwords may have.

password-policy minimum-length

To set the minimum length of passwords, use the **password-policy minimum-length** command in global configuration mode. To set the corresponding password policy attribute to its default value, use the **no** form of this command.

password-policy minimum-length *value*

no password-policy minimum-length *value*

Syntax Description

value	Specifies the minimum length for passwords. Valid values range from 0 to 64 characters.

Defaults

The default minimum length is 0.

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
9.1(2)	This command was introduced.

Usage Guidelines

If the minimum length is less than any of the other minimum attributes (changes, lower case, upper case, numeric, and special), an error message appears and the minimum length is not changed. The recommended password length is 8 charcters.

Examples

The following example specifies a minimum number of characters for passwords as 8:

```
hostname(config)# password-policy minimum-length 8
```

Related Commands

Command	Description
password-policy lifetime	Sets the password lifetime value in days after which passwords expire.
password-policy minimum-changes	Sets the minimum number of changed characters allowed between old and new passwords.
password-policy minimum-lowercase	Sets the minimum number of lower case characters that passwords may have.

password-policy minimum-lowercase

To set the minimum number of lower case characters that passwords may have, use the **password-policy minimum-lowercase** command in global configuration mode. To set the corresponding password policy attribute to its default value, use the **no** form of this command.

password-policy minimum-lowercase *value*

no password-policy minimum-lowercase *value*

Syntax Description

value	Specifies the minimum number of lower case characters for passwords. Valid values range from 0 to 64 characters.

Defaults

The default number of minimum lower case characters is 0, which means there is no minimum.

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
9.1(2)	This command was introduced.

Usage Guidelines

This command sets the minimum number of lower case characters that passwords may have. Valid values range from 0 to 64 characters.

Examples

The following example specifies the minimum number of lower case characters that passwords may have as 6:

```
hostname(config)# password-policy minimum-lowercase 6
```

Related Commands

Command	Description
password-policy lifetime	Sets the password lifetime value in days after which passwords expire.
password-policy minimum-changes	Sets the minimum number of characters that must be changed between new and old passwords.
password-policy minimum-length	Sets the minimum length of passwords.

password-policy minimum-numeric

To set the minimum number of numeric characters that passwords may have, use the **password-policy minimum-numeric** command in global configuration mode. To set the corresponding password policy attribute to its default value, use the **no** form of this command.

password-policy minimum-numeric *value*

no password-policy minimum-numeric *value*

Syntax Description

value	Specifies the minimum number of numeric characters for passwords. Valid values range from 0 to 64 characters.

Defaults

The default number of minimum numeric characters is 0, which means there is no minimum.

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
9.1(2)	This command was introduced.

Usage Guidelines

This command sets the minimum number of numeric characters that passwords may have. Valid values range from 0 to 64 characters.

Examples

The following example specifies the minimum number of numeric characters that passwords may have as 8:

```
hostname(config)# password-policy minimum-numeric 8
```

Related Commands

Command	Description
password-policy lifetime	Sets the password lifetime value in days after which passwords expire.
password-policy minimum-changes	Sets the minimum number of characters that must be changed between new and old passwords.
password-policy minimum-length	Sets the minimum length of passwords.

password-policy minimum-special

To set the minimum number of special characters that passwords may have, use the **password-policy minimum-special** command in global configuration mode. To set the corresponding password policy attribute to its default value, use the **no** form of this command.

password-policy minimum-special *value*

no password-policy minimum-special *value*

Syntax Description

value	Specifies the minimum numer of special characters for passwords. Valid values range from 0 to 64 characters.

Defaults

The default number of minimum special characters is 0, which means there is no minimum.

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
9.1(2)	This command was introduced.

Usage Guidelines

This command sets the minimum number of special characters that passwords may have. Special characters include the following: !, @, #, $, %, ^, &, *, '(‘ and ‘)’.

Examples

The following example specifies the minimum number of special characters that passwords may have as 2:

```
hostname(config)# password-policy minimum-special 2
```

Related Commands

Command	Description
password-policy lifetime	Sets the password lifetime value in days after which passwords expire.
password-policy minimum-changes	Sets the minimum number of characters that must be changed between new and old passwords.
password-policy minimum-length	Sets the minimum length of passwords.

password-policy minimum-uppercase

To set the minimum number of upper case characters that passwords may have, use the **password-policy minimum-uppercase** command in global configuration mode. To set the corresponding password policy attribute to its default value, use the **no** form of this command.

password-policy minimum-uppercase *value*

no password-policy minimum-uppercase *value*

Syntax Description

value	Specifies the minimum number of upper case characters for passwords. Valid values range from 0 to 64 characters.

Defaults

The default number of minimum upper case characters is 0, which means there is no minimum.

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
9.1(2)	This command was introduced.

Usage Guidelines

This command sets the minimum number of upper case characters that passwords may have. Valid values range from 0 to 64 characters.

Examples

The following example specifies the minimum number of upper case characters that passwords may have as 4:

```
hostname(config)# password-policy minimum-uppercase 4
```

Related Commands

Command	Description
password-policy lifetime	Sets the password lifetime value in days after which passwords expire.
password-policy minimum-changes	Sets the minimum number of characters that must be changed between new and old passwords.
password-policy minimum-length	Sets the minimum length of passwords.

password-prompt

To customize the password prompt of the WebVPN page login box that is displayed to WebVPN users when they connect to the security appliance, use the **password-prompt** command from webvpn customization mode:

password-prompt {**text** | **style**} *value*

[**no**] **password-prompt** {**text** | **style**} *value*

To remove the command from the configuration and cause the value to be inherited, use the **no** form of the command.

Syntax Description

text	Specifies you are changing the text.
style	Specifies you are changing the style.
value	The actual text to display (maximum 256 characters), or Cascading Style Sheet (CSS) parameters (maximum 256 characters).

Defaults

The default text of the password prompt is “PASSWORD:”.

The default style of the password prompt is color:black;font-weight:bold;text-align:right.

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
Webvpn customization	•	—	•	—	—

Command History

Release	Modification
7.1(1)	This command was introduced.

Usage Guidelines

The **style** option is expressed as any valid Cascading Style Sheet (CSS) parameters. Describing these parameters is beyond the scope of this document. For more information about CSS parameters, consult CSS specifications at the World Wide Web Consortium (W3C) website at www.w3.org. Appendix F of the CSS 2.1 Specification contains a convenient list of CSS parameters, and is available at www.w3.org/TR/CSS21/propidx.html.

Here are some tips for making the most common changes to the WebVPN pages—the page colors:

- You can use a comma-separated RGB value, an HTML color value, or the name of the color if recognized in HTML.
- RGB format is 0,0,0, a range of decimal numbers from 0 to 255 for each color (red, green, blue); the comma separated entry indicates the level of intensity of each color to combine with the others.

- HTML format is #000000, six digits in hexadecimal format; the first and second represent red, the third and fourth green, and the fifth and sixth represent blue.

Note To easily customize the WebVPN pages, we recommend that you use ASDM, which has convenient features for configuring style elements, including color swatches and preview capabilities.

Examples

In the following example, the text is changed to "Corporate Password:", and the default style is changed with the font weight increased to bolder:

```
hostname(config)# webvpn
hostname(config-webvpn)# customization cisco
hostname(config-webvpn-custom)# password-prompt text Corporate Username:
hostname(config-webvpn-custom)# password-prompt style font-weight:bolder
```

Related Commands

Command	Description
group-prompt	Customizes the group prompt of the WebVPN page
username-prompt	Customizes the username prompt of the WebVPN page

password-storage

To let users store their login passwords on the client system, use the **password-storage enable** command in group-policy configuration mode or username configuration mode. To disable password storage, use the **password-storage disable** command.

To remove the password-storage attribute from the running configuration, use the **no** form of this command. This enables inheritance of a value for password-storage from another group policy.

password-storage {enable | disable}

no password-storage

Syntax Description

disable	Disables password storage.
enable	Enables password storage.

Defaults

Password storage is disabled.

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**
Group-policy configuration	•	—	•	—	—
Username configuration	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

Enable password storage only on systems that you know to be in secure sites.

This command has no bearing on interactive hardware client authentication or individual user authentication for hardware clients.

Examples

The following example shows how to enable password storage for the group policy named FirstGroup:

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# password-storage enable
```

peer-id-validate

To specify whether to validate the identity of the peer using the peer's certificate, use the **peer-id-validate** command in tunnel-group ipsec-attributes mode. To return to the default value, use the **no** form of this command.

peer-id-validate *option*

no peer-id-validate

Syntax Description

option	Specifies one of the following options: • **req**: required • **cert**: if supported by certificate • **nocheck**: do not check

Defaults

The default setting for this command is **req**.

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
Tunnel-group ipsec attributes	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

You can apply this attribute to all IPsec tunnel-group types.

Examples

The following example entered in config-ipsec configuration mode, requires validating the peer using the identity of the peer's certificate for the IPsec LAN-to-LAN tunnel group named 209.165.200.225:

```
hostname(config)# tunnel-group 209.165.200.225 type IPsec_L2L
hostname(config)# tunnel-group 209.165.200.225 ipsec-attributes
hostname(config-tunnel-ipsec)# peer-id-validate req
hostname(config-tunnel-ipsec)#
```

Related Commands

Command	Description
clear-configure tunnel-group	Clears all configured tunnel groups.
show running-config tunnel-group	Shows the tunnel group configuration for all tunnel groups or for a particular tunnel group.
tunnel-group ipsec-attributes	Configures the tunnel-group ipsec-attributes for this group.

perfmon

To display performance information, use the **perfmon** command in privileged EXEC mode.

perfmon {**verbose** | **interval** *seconds* | **quiet** | **settings**} [*detail*]

Syntax Description

verbose	Displays performance monitor information at the ASA console.
interval *seconds*	Specifies the number of seconds before the performance display is refreshed on the console.
quiet	Disables the performance monitor displays.
settings	Displays the interval and whether it is quiet or verbose.
detail	Displays detailed information about performance.

Defaults

The *seconds* is 120 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**
Privileged EXEC	•	•	•	•	

Command History

Release	Modification
7.0	Support for this command was introduced on the ASA.
7.2(1)	Support for the **detail** keyword was added.

Usage Guidelines

The **perfmon** command allows you to monitor the performance of the ASA. Use the **show perfmon** command to display the information immediately. Use the **perfmon verbose** command to display the information every 2 minutes continuously. Use the **perfmon interval** *seconds* command with the **perfmon verbose** command to display the information continuously every number of seconds that you specify.

An example of the performance information is displayed as follows:

PERFMON STATS:	Current	Average
Xlates	33/s	20/s
Connections	110/s	10/s
TCP Conns	50/s	42/s
WebSns Req	4/s	2/s
TCP Fixup	20/s	15/s
HTTP Fixup	5/s	5/s

FTP Fixup	7/s	4/s
AAA Authen	10/s	5/s
AAA Author	9/s	5/s
AAA Account	3/s	3/s

This information lists the number of translations, connections, Websense requests, address translations (called “fixups”), and AAA transactions that occur each second.

Examples

This example shows how to display the performance monitor statistics every 30 seconds on the ASA console:

```
hostname(config)# perfmon interval 120
hostname(config)# perfmon quiet
hostname(config)# perfmon settings
interval: 120 (seconds)
quiet
```

Related Commands

Command	Description
show perfmon	Displays performance information.

periodic

To specify a recurring (weekly) time range for functions that support the time-range feature, use the **periodic** command in time-range configuration mode. To disable, use the **no** form of this command.

periodic *days-of-the-week time* **to** [*days-of-the-week*] *time*

no periodic *days-of-the-week time* **to** [*days-of-the-week*] *time*

Syntax Description

days-of-the-week	(Optional) The first occurrence of this argument is the starting day or day of the week that the associated time range is in effect. The second occurrence is the ending day or day of the week the associated statement is in effect. This argument is any single day or combinations of days: Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, and Sunday. Other possible values are: • daily—Monday through Sunday • weekdays—Monday through Friday • weekend—Saturday and Sunday If the ending days of the week are the same as the starting days of the week, you can omit them.
time	Specifies the time in the format HH:MM. For example, 8:00 is 8:00 a.m. and 20:00 is 8:00 p.m.
to	Entry of the **to** keyword is required to complete the range "from start-time to end-time."

Defaults

If a value is not entered with the **periodic** command, access to the ASA as defined with the **time-range** command is in effect immediately and always on.

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
Time-range configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

To implement a time-based ACL, use the **time-range** command to define specific times of the day and week. Then use the with the **access-list extended time-range** command to bind the time range to an ACL.

The **periodic** command is one way to specify when a time range is in effect. Another way is to specify an absolute time period with the **absolute** command. Use either of these commands after the **time-range** global configuration command, which specifies the name of the time range. Multiple **periodic** entries are allowed per **time-range** command.

If the end days-of-the-week value is the same as the start value, you can omit them.

If a **time-range** command has both **absolute** and **periodic** values specified, then the **periodic** commands are evaluated only after the **absolute start** time is reached, and are not further evaluated after the **absolute end** time is reached.

The time-range feature relies on the system clock of the ASA; however, the feature works best with NTP synchronization.

Examples

Some examples follow:

If you want:	Enter this:
Monday through Friday, 8:00 a.m. to 6:00 p.m. only	**periodic weekdays 8:00 to 18:00**
Every day of the week, from 8:00 a.m. to 6:00 p.m. only	**periodic daily 8:00 to 18:00**
Every minute from Monday 8:00 a.m. to Friday 8:00 p.m.	**periodic monday 8:00 to friday 20:00**
All weekend, from Saturday morning through Sunday night	**periodic weekend 00:00 to 23:59**
Saturdays and Sundays, from noon to midnight	**periodic weekend 12:00 to 23:59**

The following example shows how to allow access to the ASA on Monday through Friday, 8:00 a.m. to 6:00 p.m. only:

```
hostname(config-time-range)# periodic weekdays 8:00 to 18:00
hostname(config-time-range)#
```

The following example shows how to allow access to the ASA on specific days (Monday, Tuesday, and Friday), 10:30 a.m. to 12:30 p.m.:

```
hostname(config-time-range)# periodic Monday Tuesday Friday 10:30 to 12:30
hostname(config-time-range)#
```

Related Commands

Command	Description
absolute	Defines an absolute time when a time range is in effect.
access-list extended	Configures a policy for permitting or denying IP traffic through the ASA.
default	Restores default settings for the **time-range** command **absolute** and **periodic** keywords.
time-range	Defines access control to the ASA based on time.

permit errors

To allow invalid GTP packets or packets that otherwise would fail parsing and be dropped, use the **permit errors** command in GTP map configuration mode, which is accessed by using the **gtp-map** command. To return to the default behavior, where all invalid packets or packets that failed, during parsing, are dropped. use the **no** form of this command.

permit errors

no permit errors

Syntax Description

This command has no arguments or keywords.

Defaults

By default, all invalid packets or packets that failed, during parsing, are dropped.

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
GTP map configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

Use the **permit errors** command in GTP map configuration mode to allow any packets that are invalid or encountered an error during inspection of the message to be sent through the ASA instead of being dropped.

Examples

The following example permits traffic containing invalid packets or packets that failed, during parsing:

```
hostname(config)# gtp-map qtp-policy
hostname(config-gtpmap)# permit errors
```

Related Commands

Commands	Description
clear service-policy inspect gtp	Clears global GTP statistics.
gtp-map	Defines a GTP map and enables GTP map configuration mode.
inspect gtp	Applies a specific GTP map to use for application inspection.

Commands	Description
permit response	Supports load-balancing GSNs.
show service-policy inspect gtp	Displays the GTP configuration.

permit response

To support load-balancing GSNs, use the **permit response** command in GTP map configuration mode, which is accessed by using the **gtp-map** command. Use the **no** form of this command to allow the ASA to drop GTP responses from GSNs other than the host to which the request was sent.

permit response to-object-group *to_obj_group_id* **from-object-group** *from_obj_group_id*

no permit response to-object-group *to_obj_group_id* **from-object-group** *from_obj_group_id*

Syntax Description

from-object-group *from_obj_group_id*	Specifies the name of the object-group configured with the **object-group** command which can send responses to the set of GSNs in the object-group specified by the *to_obj_group_id* argument. The ASA supports only object-groups containing network-objects with IPv4 addresses. IPv6 addresses are currently not supported with GTP.
to-object-group *to_obj_group_id*	Specifies the name of the object-group configured with the **object-group** command which can receive responses from the set of GSNs in the object-group specified by the *from_obj_group_id* argument. The ASA supports only object-groups containing network-objects with IPv4 addresses. IPv6 addresses are currently not supported with GTP.

Defaults

By default, the ASA drops GTP responses from GSNs other than the host to which the request was sent.

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**
GTP map configuration	•	•	•	•	—

Command History

Release	Modification
7.0(4)	This command was introduced.

Usage Guidelines

Use the **permit response** command in GTP map configuration mode to support load-balancing GSNs. The **permit response** command configures the GTP map to allow GTP responses from a different GSN than the response was sent to.

You identify the pool of load-balancing GSNs as a network object. Likewise, you identify the SGSN as a network object. If the GSN responding belongs to the same object group as the GSN that the GTP request was sent to and if the SGSN is in a object group that the responding GSN is permitted to send a GTP response to, the ASA permits the response.

Examples

The following example permits GTP responses from any host on the 192.168.32.0 network to the host with the IP address 192.168.112.57:

```
hostname(config)# object-group network gsnpool32
hostname(config-network)# network-object 192.168.32.0 255.255.255.0
hostname(config)# object-group network sgsn1
hostname(config-network)# network-object host 192.168.112.57
hostname(config-network)# exit
hostname(config)# gtp-map gtp-policy
hostname(config-gtpmap)# permit response to-object-group sgsn1 from-object-group gsnpool32
```

Related Commands

Commands	Description
clear service-policy inspect gtp	Clears global GTP statistics.
gtp-map	Defines a GTP map and enables GTP map configuration mode.
inspect gtp	Applies a specific GTP map to use for application inspection.
permit errors	Allow invalid GTP packets.
show service-policy inspect gtp	Displays the GTP configuration.

pfs

To enable PFS, use the **pfs enable** command in group-policy configuration mode. To disable PFS, use the **pfs disable** command. To remove the PFS attribute from the running configuration, use the **no** form of this command.

pfs {enable | disable}

no pfs

Syntax Description

disable	Disables PFS.
enable	Enables PFS.

Defaults

PFS is disabled.

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**
Group-policy configuration	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

The PFS setting on the VPN Client and the ASA must match.

Use the **no** form of this command to allow the inheritance of a value for PFS from another group policy.

In IPsec negotiations, PFS ensures that each new cryptographic key is unrelated to any previous key.

Examples

The following example shows how to set PFS for the group policy named FirstGroup:

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# pfs enable
```

phone-proxy

To configure the Phone Proxy instance, use the **phone-proxy** command in global configuration mode.

To remove the Phone Proxy instance, use the **no** form of this command.

phone-proxy *phone_proxy_name*

no phone-proxy *phone_proxy_name*

Syntax Description

phone_proxy_name	Specifies the name of the Phone Proxy instance.

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
8.0(4)	The command was introduced.

Usage Guidelines

Only one Phone Proxy instance can be configured on the ASA.

If NAT is configured for the HTTP proxy server, the global or mapped IP address of the HTTP proxy server with respect to the IP phones is written to the Phone Proxy configuration file.

Examples

The following example shows the use of the **phone-proxy** command to configure the Phone Proxy instance:

```
hostname(config)# phone-proxy asa_phone_proxy
hostname(config-phone-proxy)# tftp-server address 128.106.254.8 interface outside
hostname(config-phone-proxy)# media-termination address 192.0.2.25 interface inside
hostname(config-phone-proxy)# media-termination address 128.106.254.3 interface outside
hostname(config-phone-proxy)# tls-proxy asa_tlsp
hostname(config-phone-proxy)# ctl-file asactl
hostname(config-phone-proxy)# cluster-mode nonsecure
hostname(config-phone-proxy)# timeout secure-phones 00:05:00
hostname(config-phone-proxy)# disable service-settings
```

Related Commands

Command	Description
ctl-file (global)	Specifies the CTL file to create for Phone Proxy configuration or the CTL file to parse from Flash memory.
ctl-file (phone-proxy)	Specifies the CTL file to use for Phone Proxy configuration.
tls-proxy	Configures the TLS proxy instance.

pim

To re-enable PIM on an interface, use the **pim** command in interface configuration mode. To disable PIM, use the **no** form of this command.

pim

no pim

Syntax Description

This command has no arguments or keywords.

Defaults

The **multicast-routing** command enables PIM on all interfaces by default.

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

The **multicast-routing** command enables PIM on all interfaces by default. Only the **no** form of the **pim** command is saved in the configuration.

Note PIM is not supported with PAT. The PIM protocol does not use ports and PAT only works with protocols that use ports.

Examples

The following example disables PIM on the selected interface:

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

Related Commands

Command	Description
multicast-routing	Enables multicast routing on the ASA.

pim accept-register

To configure the ASA to filter PIM register messages, use the **pim accept-register** command in global configuration mode. To remove the filtering, use the **no** form of this command.

pim accept-register {**list** *acl* | **route-map** *map-name*}

no pim accept-register

Syntax Description

list *acl*	Specifies an access list name or number. Use only extended host ACLs with this command.
route-map *map-name*	Specifies a route-map name. Use extended host ACLs in the referenced route-map.

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.

Usage Guidelines

This command is used to prevent unauthorized sources from registering with the RP. If an unauthorized source sends a register message to the RP, the ASA will immediately send back a register-stop message.

Examples

The following example restricts PIM register messages to those from sources defined in the access list named “no-ssm-range”:

```
hostname(config)# pim accept-register list no-ssm-range
```

Related Commands

Command	Description
multicast-routing	Enables multicast routing on the ASA.

pim bidir-neighbor-filter

To control which bidir-capable neighbors can participate in the DF election, use the **pim bidir-neighbor-filter** command in interface configuration mode. To remove the filtering, use the **no** form of this command.

pim bidir-neighbor-filter *acl*

no pim bidir-neighbor-filter *acl*

Syntax Description

acl	Specifies an access list name or number. The access list defines the neighbors that can participate in bidir DF elections. Use only standard ACLs with this command; extended ACLs are not supported.

Defaults

All routers are considered to be bidir capable.

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
7.2(1)	This command was introduced.

Usage Guidelines

Bidirectional PIM allows multicast routers to keep reduced state information. All of the multicast routers in a segment must be bidirectionally enabled for bidir to elect a DF.

The **pim bidir-neighbor-filter** command enables the transition from a sparse-mode-only network to a bidir network by letting you specify the routers that should participate in DF election while still allowing all routers to participate in the sparse-mode domain. The bidir-enabled routers can elect a DF from among themselves, even when there are non-bidir routers on the segment. Multicast boundaries on the non-bidir routers prevent PIM messages and data from the bidir groups from leaking in or out of the bidir subset cloud.

When the **pim bidir-neighbor-filter** command is enabled, the routers that are permitted by the ACL are considered to be bidir-capable. Therefore:

- If a permitted neighbor does not support bidir, the DF election does not occur.
- If a denied neighbor supports bidir, then DF election does not occur.
- If a denied neighbor does not support bidir, the DF election can occur.

Examples

The following example allows 10.1.1.1 to become a PIM bidir neighbor:

```
hostname(config)# access-list bidir_test permit 10.1.1.1 255.255.255.55
hostname(config)# access-list bidir_test deny any
hostname(config)# interface GigabitEthernet0/3
hostname(config-if)# pim bidir-neighbor-filter bidir_test
```

Related Commands

Command	Description
multicast boundary	Defines a multicast boundary for administratively-scoped multicast addresses.
multicast-routing	Enables multicast routing on the ASA.

pim dr-priority

To configure the neighbor priority on the ASA used for designated router election, use the **pim dr-priority** command in interface configuration mode. To restore the default priority, use the **no** form of this command.

pim dr-priority *number*

no pim dr-priority

Syntax Description

number	A number from 0 to 4294967294. This number is used to determine the priority of the device when determining the designated router. Specifying 0 prevents the ASA from becoming the designated router.

Defaults

The default value is 1.

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

The device with the largest priority value on an interface becomes the PIM designated router. If multiple devices have the same designated router priority, then the device with the highest IP address becomes the DR. If a device does not include the DR-Priority Option in hello messages, it is regarded as the highest-priority device and becomes the designated router. If multiple devices do not include this option in their hello messages, then the device with the highest IP address becomes the designated router.

Examples

The following example sets the DR priority for the interface to 5:

```
hostname(config-if)# pim dr-priority 5
```

Related Commands

Command	Description
multicast-routing	Enables multicast routing on the ASA.

pim hello-interval

To configure the frequency of the PIM hello messages, use the **pim hello-interval** command in interface configuration mode. To restore the hello-interval to the default value, use the **no** form of this command.

pim hello-interval *seconds*

no pim hello-interval [*seconds*]

Syntax Description

seconds	The number of seconds that the ASA waits before sending a hello message. Valid values range from 1 to 3600 seconds. The default value is 30 seconds.

Defaults

The interval default is 30 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.

Examples

The following example sets the PIM hello interval to 1 minute:

```
hostname(config-if)# pim hello-interval 60
```

Related Commands

Command	Description
multicast-routing	Enables multicast routing on the ASA.

pim join-prune-interval

To configure the PIM join/prune interval, use the **pim join-prune-interval** command in interface configuration mode. To restore the interval to the default value, use the **no** form of this command.

pim join-prune-interval *seconds*

no pim join-prune-interval [*seconds*]

Syntax Description

seconds	The number of seconds that the ASA waits before sending a join/prune message. Valid values range from 10 to 600 seconds. 60 seconds is the default.

Defaults

The default interval is 60 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.

Examples

The following example sets the PIM join/prune interval to 2 minutes:

```
hostname(config-if)# pim join-prune-interval 120
```

Related Commands

Command	Description
multicast-routing	Enables multicast routing on the ASA.

pim neighbor-filter

To control which neighbor routers can participate in PIM, use the **pim neighbor-filter** command in interface configuration mode. To remove the filtering, use the **no** form of this command.

pim neighbor-filter *acl*

no pim neighbor-filter *acl*

Syntax Description

acl	Specifies an access list name or number. Use only standard ACLs with this command; extended ACLs are not supported.

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
7.2(1)	This command was introduced.

Usage Guidelines

This command defines which neighbor routers can participate in PIM. If this command is not present in the configuration then there are no restrictions.

Multicast routing and PIM must be enabled for this command to appear in the configuration. If you disable multicast routing, this command is removed from the configuration.

Examples

The following example allows the router with the IP address 10.1.1.1 to become a PIM neighbor on interface GigabitEthernet0/2:

```
hostname(config)# access-list pim_filter permit 10.1.1.1 255.255.255.55
hostname(config)# access-list pim_filter deny any
hostname(config)# interface gigabitEthernet0/2
hostname(config-if)# pim neighbor-filter pim_filter
```

Related Commands

Command	Description
multicast-routing	Enables multicast routing on the ASA.

pim old-register-checksum

To allow backward compatibility on a rendezvous point (RP) that uses old register checksum methodology, use the **pim old-register-checksum** command in global configuration mode. To generate PIM RFC-compliant registers, use the **no** form of this command.

pim old-register-checksum

no pim old-register-checksum

Syntax Description

This command has no arguments or keywords.

Defaults

The ASA generates PIM RFC-compliant registers.

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.

Usage Guidelines

The ASA software accepts register messages with checksum on the PIM header and only the next 4 bytes rather than using the Cisco IOS method—accepting register messages with the entire PIM message for all PIM message types. The **pim old-register-checksum** command generates registers compatible with Cisco IOS software.

Examples

The following example configures the ASA to use the old checksum calculations:

```
hostname(config)# pim old-register-checksum
```

Related Commands

Command	Description
multicast-routing	Enables multicast routing on the ASA.

pim rp-address

To configure the address of a PIM rendezvous point (RP), use the **pim rp-address** command in global configuration mode. To remove an RP address, use the **no** form of this command.

pim rp-address *ip_address* [*acl*] [**bidir**]

no pim rp-address *ip_address*

Syntax Description

acl	(Optional) The name or number of a standard access list that defines which multicast groups the RP should be used with. Do not use a host ACL with this command.
bidir	(Optional) Indicates that the specified multicast groups are to operate in bidirectional mode. If the command is configured without this option, the specified groups operate in PIM sparse mode.
ip_address	IP address of a router to be a PIM RP. This is a unicast IP address in four-part dotted-decimal notation.

Defaults

No PIM RP addresses are configured.

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.

Usage Guidelines

All routers within a common PIM sparse mode (PIM-SM) or bidir domain require knowledge of the well-known PIM RP address. The address is statically configured using this command.

Note The ASA does not support Auto-RP; you must use the **pim rp-address** command to specify the RP address.

You can configure a single RP to serve more than one group. The group range specified in the access list determines the PIM RP group mapping. If the an access list is not specified, the RP for the group is applied to the entire IP multicast group range (224.0.0.0/4).

Note The ASA always advertises the bidir capability in the PIM hello messages regardless of the actual bidir configuration.

Examples

The following example sets the PIM RP address to 10.0.0.1 for all multicast groups:

```
hostname(config)# pim rp-address 10.0.0.1
```

Related Commands

Command	Description
pim accept-register	Configures candidate RPs to filter PIM register messages.

pim spt-threshold infinity

To change the behavior of the last hop router to always use the shared tree and never perform a shortest-path tree (SPT) switchover, use the **pim spt-threshold infinity** command in global configuration mode. To restore the default value, use the **no** form of this command.

pim spt-threshold infinity [**group-list** *acl*]

no pim spt-threshold

Syntax Description

group-list *acl*	(Optional) Indicates the source groups restricted by the access list. The *acl* argument must specify a standard ACL; extended ACLs are not supported.

Defaults

The last hop PIM router switches to the shortest-path source tree by default.

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.

Usage Guidelines

If the **group-list** keyword is not used, this command applies to all multicast groups.

Examples

The following example causes the last hop PIM router to always use the shared tree instead of switching to the shortest-path source tree:

```
hostname(config)# pim spt-threshold infinity
```

Related Commands

Command	Description
multicast-routing	Enables multicast routing on the ASA.

ping

To test connectivity from a specified interface to an IP address, use the **ping** command in privileged EXEC mode.

ping {**tcp**] [*if_name*] [*host*] [*port*] [**repeat** *count*] [**timeout** *seconds*][**source** *host ports*] [**data** *pattern*] [**size** *bytes*] [**validate**]}

Note The **source** and *port* options are only available with the **tcp** option; the **data**, **size**, and **validate** options are not available with the **tcp** option.

Syntax Description

data *pattern*	(Optional) Specifies the 16-bit data pattern in hexidecimal format.
host	Specifies the IPv4 or IPv6 address or name of the host to ping. The name can be a DNS name or a name assigned with the **name** command. The maximum number of characters for DNA names is 128, and the maximum number of characters for names created with the **name** command is 63.
if_name	(Optional) For ICMP, this is the interface name, as configured by the **nameif** command, by which the *host* is accessible. If not supplied, then the *host* is resolved to an IP address and the routing table is consulted to determine the destination interface. For TCP, this is the input interface through which the source sends SYN packets.
pattern	(Optional) Specifies the 16-bit data pattern in hexidecimal format.
port	(Optional) Specifies the associated port number from 1-65535.
repeat *count*	(Optional) Specifies the number of times to repeat the ping request.
size *bytes*	(Optional) Specifies the datagram size in bytes.
source	(Optional) Specifies a certain IP address and port to send from (Use port = 0 for a random port).
tcp	(Optional) Tests a connection over TCP (the default is ICMP). The available interfaces are the following: • DMZ—Name of interface GigabitEthernet0/2 • Hostname or A.B.C.D—Ping destination IPv4 address or hostname • Hostname or X:X:X:X::X—Ping destination IPv6 address or hostname • internal—Name of interface GigabitEthernet0/3 • management—Name of interface Management0/0 • outside—Name of interface GigabitEthernet0/0 • publicl4tm—Name of interface GigabitEthernet0/1 **Note** TCP does not use the source interface address for pings.
timeout *seconds*	(Optional) Specifies the number of seconds of the timeout interval.
validate	(Optional) Validates reply data.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.
7.2(1)	Support for DNS names added.
8.4(1)	Added the **tcp** option.

Usage Guidelines

The **ping** command allows you to determine if the ASA has connectivity or if a host is available on the network. If the ASA has connectivity, make sure that the **icmp permit any** *interface* command is configured. This configuration is required to allow the ASA to respond and accept messages generated from the **ping** command. The **ping** command output shows if the response was received. If a host is not responding after you enter the **ping** command, a message similar to the following appears:

```
hostname(config)# ping 10.1.1.1
Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:
?????
Success rate is 0 percent (0/5)
```

Use the **show interface** command to ensure that the ASA is connected to the network and is passing traffic. The address of the specified *if_name* is used as the source address of the ping.

If you want internal hosts to ping external hosts over ICMP, you must do one of the following:

- Create an ICMP **access-list** command for an echo reply; for example, to give ping access to all hosts, use the **access-list acl_grp permit icmp any any** command and bind the **access-list** command to the interface that you want to test using the **access-group** command.
- Configure the ICMP inspection engine using the **inspect icmp** command. For example, adding the **inspect icmp** command to the **class default_inspection** class for the global service policy allows echo replies through the ASA for echo requests initiated by internal hosts.

You can also perform an extended ping, which allows you to enter the keywords one line at a time.

If you are pinging through the ASA between hosts or routers, but the pings are not successful, use the **capture** command to monitor the success of the ping.

The ASA **ping** command does not require an interface name. If you do not specify an interface name, the ASA checks the routing table to find the address that you specify. You can specify an interface name to indicate through which interface the ICMP echo requests are sent.

The **ping tcp** command requires the **enable** password and allows a maximum of two users to initiate simultaneous ping requests. In addition, this command does not support IPv6.

Examples

The following example shows how to determine if other IP addresses are visible from the ASA:

```
hostname# ping 171.69.38.1
Sending 5, 100-byte ICMP Echos to 171.69.38.1, timeout is 2 seconds:
```

```
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms
```

The following example specifies a host using a DNS name:

```
hostname# ping www.example.com
Sending 5, 100-byte ICMP Echos to www.example.com, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms
```

The following is an example of an extended ping:

```
hostname# ping
Interface: outside
Target IP address: 171.69.38.1
Repeat count: [5]
Datagram size: [100]
Timeout in seconds: [2]
Extended commands [n]:
Sweep range of sizes [n]:
Sending 5, 100-byte ICMP Echos to 171.69.38.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms
```

The following are examples of the **ping tcp** command:

```
hostname# ping
TCP [n]: yes
Interface: dmz
Target IP address: 10.0.0.1
Target IP port: 21
Specify source? [n]: y
Source IP address: 192.168.2.7
Source IP port: [0] 465
Repeat count: [5]
Timeout in seconds: [2] 5
Type escape sequence to abort.
Sending 5 TCP SYN requests to 10.0.0.1 port 21
from 192.168.2.7 starting port 465, timeout is 5 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms

hostname# ping tcp
Interface: dmz
Target IP address: 10.0.0.1
Target IP port: 21
Specify source? [n]:
Repeat count: [5] 3
Timeout in seconds: [2]
Type escape sequence to abort.
No source specified. Pinging from identity interface.
Sending 3 TCP SYN requests to 10.0.0.1 port 21
from 10.0.0.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms

hostname# ping tcp 10.0.0.1 21
Type escape sequence to abort.
No source specified. Pinging from identity interface.
Sending 5 TCP SYN requests to 10.0.0.1 port 21
from 10.0.0.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

```
hostname# ping tcp 10.0.0.1 21 source 192.168.1.1 2002 repeat 10
Type escape sequence to abort.
Sending 10 TCP SYN requests to 10.0.0.1 port 21
from 192.168.1.1 starting port 2002, timeout is 2 seconds:
!!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 1/2/2 ms

hostname(config)# ping tcp www.example.com 80
Type escape sequence to abort.
No source specified. Pinging from identity interface.
Sending 5 TCP SYN requests to 74.125.19.103 port 80
from 171.63.230.107, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 3/4/4 ms

hostname# ping tcp 192.168.1.7 23 source 192.168.2.7 24966
Type escape sequence to abort.
Source port 24966 in use! Using port 24967 instead.
Sending 5 TCP SYN requests to 192.168.1.7 port 23
from 192.168.2.7 starting port 24967, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms

hostname(config)# ping tcp www.example.com 80
Type escape sequence to abort.
No source specified. Pinging from identity interface.
Error! Too many concurrent TCP ping sessions. Please wait...
```

Related Commands

Command	Description
capture	Captures packets at an interface.
icmp	Configures access rules for ICMP traffic that terminates at an interface.
show interface	Displays information about the VLAN configuration.