



C Commands

cache-time

To specify in minutes how long to allow a CRL to remain in the cache before considering it stale, use the **cache-time** command in ca-crl configuration mode. To return to the default value, use the **no** form of this command.

cache-time *refresh-time*

no cache-time

Syntax Description

refresh-time Specifies the number of minutes to allow a CRL to remain in the cache. The range is 1 - 1440 minutes. If the NextUpdate field is not present in the CRL, the CRL is not cached.

Defaults

The default setting is 60 minutes.

Command Modes

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

	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple Context	System
CRL configuration	•	•	•	•	•

Command History

Release	Modification
7.0	This command was introduced.

Examples

The following example enters ca-crl configuration mode, and specifies a cache time refresh value of 10 minutes for trustpoint central:

```
hostname(configure)# crypto ca trustpoint central
hostname(ca-trustpoint)# crl configure
hostname(ca-crl)# cache-time 10
hostname(ca-crl)#
```

Related Commands

Command	Description
crl configure	Enters crl configuration mode.
crypto ca trustpoint	Enters trustpoint configuration mode.
enforcenextupdate	Specifies how to handle the NextUpdate CRL field in a certificate.

call-agent

To specify a group of call agents, use the **call-agent** command in MGCP map configuration mode, which is accessible by using the **mgcp-map** command. To remove the configuration, use the **no** form of this command.

call-agent *ip_address* *group_id*

no call-agent *ip_address* *group_id*

Syntax Description

<i>ip_address</i>	The IP address of the gateway.
<i>group_id</i>	The ID of the call agent group, from 0 to 2147483647.

Defaults

This command is disabled by default.

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
Global configuration	•	•	•	•	—

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

Use the **call-agent** command to specify a group of call agents that can manage one or more gateways. The call agent group information is used to open connections for the call agents in the group (other than the one a gateway sends a command to) so that any of the call agents can send the response. Call agents with the same *group_id* belong to the same group. A call agent may belong to more than one group. The *group_id* option is a number from 0 to 4294967295. The *ip_address* option specifies the IP address of the call agent.

Examples

The following example allows call agents 10.10.11.5 and 10.10.11.6 to control gateway 10.10.10.115, and allows call agents 10.10.11.7 and 10.10.11.8 to control both gateways 10.10.10.116 and 10.10.10.117:

```
hostname(config)# mgcp-map mgcp_inbound
hostname(config-mgcp-map)# call-agent 10.10.11.5 101
hostname(config-mgcp-map)# call-agent 10.10.11.6 101
hostname(config-mgcp-map)# call-agent 10.10.11.7 102
hostname(config-mgcp-map)# call-agent 10.10.11.8 102
hostname(config-mgcp-map)# gateway 10.10.10.115 101
hostname(config-mgcp-map)# gateway 10.10.10.116 102
```

```
hostname(config-mgcp-map)# gateway 10.10.10.117 102
```

Related Commands

Commands	Description
debug mgcp	Enables the display of debug information for MGCP.
mgcp-map	Defines an MGCP map and enables MGCP map configuration mode.
show mgcp	Displays MGCP configuration and session information.

capture

To enable packet capture capabilities for packet sniffing and network fault isolation, use the **capture** command. To disable packet capture capabilities, use the **no** form of this command (see the “Usage Guidelines” section for additional information about the **no** form of this command).

```
capture capture_name [access-list access_list_name] [buffer buf_size] [ethernet-type type]
[interface interface_name] [packet-length bytes] [circular-buffer]
```

```
capture capture_name type asp-drop all [drop-code] [buffer buf_size] [circular-buffer]
[packet-length bytes]
```

```
capture capture_name type isakmp [access-list access_list_name] [buffer buf_size]
[circular-buffer] [interface interface_name] [packet-length bytes]
```

```
capture capture_name type raw-data [access-list access_list_name] [buffer buf_size]
[circular-buffer] [ethernet-type type] [interface interface_name] [packet-length bytes]
```

```
capture capture_name type webvpn user webvpn-user [url url]
```

```
no capture capture_name
```

Syntax Description

access-list <i>access_list_name</i>	(Optional) Selects packets based on IP or higher fields for a specific access list identification.
all	Captures all the packets that the security appliance drops
buffer <i>buf_size</i>	(Optional) Defines the buffer size used to store the packet in bytes.
<i>capture_name</i>	Specifies the name of the packet capture.
circular-buffer	(Optional) Overwrites the buffer, starting from the beginning, when the buffer is full.
ethernet-type <i>type</i>	(Optional) Selects an Ethernet type to capture.
interface <i>interface_name</i>	(Optional) Specifies the interface on which to use packet capture, where <i>interface_name</i> is the name assigned to the interface by the nameif command.
packet-length <i>bytes</i>	(Optional) Sets the maximum number of bytes of each packet to store in the capture buffer.
type asp-drop <i>drop-code</i>	(Optional) Captures packets dropped for a reason. You can specify a particular reason by using the <i>drop-code</i> argument. Valid values for the <i>drop-code</i> argument are listed in the “Usage Guidelines” section, below.
type isakmp	(Optional) Captures encrypted and decrypted ISAKMP payloads.
type raw-data	(Optional) Captures inbound and outbound packets on one or more interfaces. This is the default.
type webvpn	(Optional) Captures WebVPN data for a specific WebVPN connection.
url <i>url</i>	(Optional) Specifies a URL for a WebVPN connection capture.
user <i>webvpn-user</i>	(Optional) Specifies a username for a WebVPN capture.

Defaults

The defaults are as follows:

- The capture type is raw data.
- The **buffer size** is 512 KB.
- All the Ethernet types are accepted.
- All the IP packets are matched.
- The **packet-length** is 1518 bytes.

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 mode	•	•	•	•	•

Command History

Release	Modification
6.2	Support for this command was introduced on the security appliance.
7.0	This command was modified to include several new keywords, most notably the type asp-drop , type isakmp , type raw-data , and type webvpn keywords.
7.2(4)	Added the all option to capture all packets that the security appliance drops.

Usage Guidelines

Capturing packets is useful when troubleshooting connectivity problems or monitoring suspicious activity. The security appliance can track packet information for traffic that passes through it, including management traffic and inspection engines. Packet information for all traffic that passes through the device can be captured.

With ISAKMP, the ISAKMP subsystem does not have access to the upper layer protocols. The capture is a pseudo capture, with the Physical, IP, and UDP layers combined together to satisfy a PCAP parser. The peer addresses are obtained from the SA exchange and are stored in the IP layer.

When selecting an Ethernet type to be included from capture, an exception occurs with the 802.1Q or VLAN type. The 802.1Q tag is automatically skipped and the inner Ethernet type is used for matching. By default, all the Ethernet types are accepted.

Once the byte buffer is full, packet capture stops.

To enable packet capturing, attach the capture to an interface with the *interface* optional argument. Multiple **capture** command statements attach the capture to multiple interfaces.

If you copy the buffer contents to a TFTP server in ASCII format, you will see only the headers, not the details and hexadecimal dump of the packets. To see the details and hexadecimal dump, you need to transfer the buffer in PCAP format and read it with TCPDUMP or Ethereal.

The **ethernet-type** and **access-list** optional keywords select the packets to store in the buffer. A packet must pass both the Ethernet and access list filters before the packet is stored in the capture buffer.

The **circular-buffer** keyword allows you to enable the capture buffer to overwrite itself, starting from the beginning, when the capture buffer is full.

Enter the **no capture** command with either the **access-list** or **interface** optional keyword unless you want to clear the capture itself. Entering **no capture** without optional keywords deletes the capture. If the **access-list** optional keyword is specified, the access list is removed from the capture and the capture is preserved. If the **interface** optional keyword is specified, the capture is detached from the specified interface and the capture is preserved.

**Note**

The **capture** command is not saved to the configuration, and the **capture** command is not copied to the standby module during failover.

Use the **copy capture:** *capture_name tftp://server/path [pcap]* command to copy capture information to a remote TFTP server.

Use the **https://securityappliance-ip-address/capture/capture_name[/pcap]** command to see the packet capture information with a web browser.

If you specify the **pcap** optional keyword, then a libpcap-format file is downloaded to the web browser and can be saved using the web browser. (A libcap file can be viewed with TCPDUMP or Ethereal.)

When you enable WebVPN capture, the security appliance creates a pair of matching files: *capture name_ORIGINAL.000* and *capture name_MANGLED.000*. For each subsequent capture, the security appliance generates additional matching pairs of files and increments the file extensions. *url* is the URL prefix to match for data capture. Use the URL *http://server/path* to capture HTTP traffic to the server. Use *https://server/path* to capture HTTPS traffic to the server.

**Note**

Enabling WebVPN capture affects the performance of the security appliance. Be sure to disable the capture after you generate the capture files that you need for troubleshooting.

type asp-drop Drop Codes

The following table lists valid values for the optional *drop-code* argument that can follow the **type asp-drop** keyword.

Drop Code	Description
acl-drop	Flow is denied by access rule.
all	All packet drop reasons.
bad-crypto	Bad crypto return in packet.
bad-ipsec-natt	Bad IPSEC NATT packet.
bad-ipsec-prot	IPSEC not AH or ESP.
bad-ipsec-udp	Bad IPSEC UDP packet.
bad-tcp-cksum	Bad TCP checksum.
bad-tcp-flags	Bad TCP flags.
buffer	Configure size of capture buffer, default is 512 KB.
circular-buffer	Overwrite buffer from beginning when full, default is non-circular.
conn-limit	Connection limit reached.
ctm-error	CTM returned error.
dns-guard-id-not-matched	DNS Guard id not matched.

Drop Code	Description
dns-guard-out-of-app-id	DNS Guard out of app id.
dst-l2_lookup-fail	Dst MAC L2 Lookup Failed.
flow-expired	Expired flow.
fo-standby	Dropped by standby unit.
host-move-pkt	FP host move packet.
ifc-classify	Virtual firewall classification failed.
inspect-dns-id-not-matched	DNS Inspect id not matched.
inspect-dns-invalid-domain-label	DNS Inspect invalid domain label.
inspect-dns-invalid-pak	DNS Inspect invalid packet.
inspect-dns-out-of-app-id	DNS Inspect out of app id.
inspect-dns-pak-too-long	DNS Inspect packet too long.
inspect-icmp-error-different-embedded-conn	ICMP Error Inspect different embedded conn.
inspect-icmp-error-no-existing-conn	ICMP Error Inspect no existing conn.
inspect-icmp-out-of-app-id	ICMP Inspect out of app id.
inspect-icmp-seq-num-not-matched	ICMP Inspect seq num not matched.
inspect-icmpv6-error-invalid-pak	ICMPv6 Error Inspect invalid packet.
inspect-icmpv6-error-no-existing-conn	ICMPv6 Error Inspect no existing conn.
intercept-unexpected	Intercept unexpected packet.
interface-down	Interface is down.
invalid-app-length	Invalid app length.
invalid-encap	Invalid encapsulation.
invalid-ethertype	Invalid ethertype.
invalid-ip-addr	Invalid IP address.
invalid-ip-header	Invalid IP header.
invalid-ip-length	Invalid IP length.
invalid-ip-option	IP option configured drop.
invalid-tcp-hdr-length	Invalid tcp length.
invalid-tcp-pak	Invalid TCP packet.
invalid-udp-length	Invalid udp length.
ip-fragment	IP fragment (unsupported).
ips-fail-close	IPS card is down.
ips-request	IPS Module requested drop.
ipsec-clearpkt-notun	IPSEC Clear Pkt w/no tunnel.
ipsec-ipv6	IPSEC via IPV6.
ipsec-need-sa	IPSEC SA Not negotiated yet.
ipsec-spoof	IPSEC Spoof detected.
ipsec-tun-down	IPSEC tunnel is down.

Drop Code	Description
ipsecpdp-keepalive	IPSEC/UDP keepalive message.
ipv6_fp-security-failed	IPv6 fastpath security checks failed.
ipv6_sp-security-failed	IPv6 slowpath security checks failed.
l2_acl	FP L2 rule drop.
l2_same-lan-port	L2 Src/Dst same LAN port.
large-buf-alloc-fail	FP fp large buffer alloc failed.
loopback-buffer-full	Loopback buffer full.
lu-invalid-pkt	Invalid LU packet.
natt-keepalive	NAT-T keepalive message.
no-adjacency	No valid adjacency.
no-mcast-entry	FP no mcast entry.
no-mcast-intrf	FP no mcast output intrf.
no-punt-cb	No registered punt cb.
no-route	No route to host.
non-ip-pkt-in-routed-mode	Non-IP packet received in routed mode.
np-sp-invalid-spi	Invalid SPI.
packet-length	Configure maximum length to save from each packet, default is 68 bytes.
punt-rate-limit	Punt rate limit exceeded.
queue-removed	Queued packet dropped.
rate-exceeded	QoS rate exceeded.
rpf-violated	Reverse-path verify failed.
security-failed	Early security checks failed.
send-ctm-error	Send to CTM returned error.
sp-security-failed	Slowpath security checks failed.
tcp-3whs-failed	TCP failed 3 way handshake.
tcp-ack-syn-diff	TCP ACK in SYNACK invalid.
tcp-acked	TCP DUP and has been ACKed.
tcp-bad-option-len	Bad option length in TCP.
tcp-bad-option-list	TCP option list invalid.
tcp-bad-sack-allow	Bad TCP SACK ALLOW option.
tcp-bad-winscale	Bad TCP window scale value.
tcp-buffer-full	TCP packet buffer full.
tcp-conn-limit	TCP Connection limit reached.
tcp-data-past-fin	TCP data send after FIN.
tcp-discarded-ooo	TCP packet out of order.
tcp-dual-open	TCP Dual open denied.
tcp-fo-drop	TCP replicated flow pak drop.

Drop Code	Description
tcp-invalid-ack	TCP invalid ACK.
tcp-mss-exceeded	TCP MSS was too large.
tcp-mss-no-syn	TCP MSS option on non-SYN.
tcp-not-syn	First TCP packet not SYN.
tcp-paws-fail	TCP packet failed PAWS test.
tcp-reserved-set	TCP reserved flags set.
tcp-rst-syn-in-win	TCP RST/SYN in window.
tcp-rstfin-ooo	TCP RST/FIN out of order.
tcp-seq-past-win	TCP packet SEQ past window.
tcp-seq-syn-diff	TCP SEQ in SYN/SYNACK.
tcp-syn-data	TCP SYN with data.
tcp-syn-ooo	TCP SYN on established conn.
tcp-synack-data	TCP SYNACK with data.
tcp-synack-ooo	TCP SYNACK on established conn.
tcp-tsopt-notallowed	TCP timestamp not allowed.
tcp-winscale-no-syn	TCP Window scale on non-SYN.
tcp_xmit_partial	TCP retransmission partial.
tfw-no-mgmt-ip-config	No management IP address configured for TFW.
unable-to-add-flow	Flow hash full.
unable-to-create-flow	Out of flow cache memory.
unimplemented	Slow path unimplemented.
unsupport-ipv6-hdr	Unsupported IPV6.
unsupported-ip-version	Unsupported IP version.

Examples

To enable packet capture, enter the following:

```
hostname(config)# capture captest interface inside
hostname(config)# capture captest interface outside
```

On a web browser, the capture contents for a capture named “mycapture” can be viewed at the following location:

<https://171.69.38.95/capture/mycapture/pcap>

To download a libpcap file (used in web browsers such as Internet Explorer or Netscape Navigator) to a local machine, enter the following:

<https://171.69.38.95/capture/http/pcap>

This example shows that the traffic is captured from an outside host at 171.71.69.234 to an inside HTTP server:

```
hostname(config)# access-list http permit tcp host 10.120.56.15 eq http host 171.71.69.234
hostname(config)# access-list http permit tcp host 171.71.69.234 host 10.120.56.15 eq http
hostname(config)# capture http access-list http packet-length 74 interface inside
```

This example shows how to capture ARP packets:

```
hostname(config)# capture arp ethernet-type arp interface outside
```

This example creates a WebVPN capture designated *hr*, which is configured to capture HTTP traffic for user2 visiting website *wwwin.abcd.com/hr/people*:

```
hostname# capture hr type webvpn user user2 url http://wwwin.abcd.com/hr/people  
WebVPN capture started.  
  capture name    hr  
  user name       user2  
  url             /http/0/wwwin.abcd.com/hr/people  
hostname#
```

Related Commands

Command	Description
clear capture	Clears the capture buffer.
copy capture	Copies a capture file to a server.
show capture	Displays the capture configuration when no options are specified.

cd

To change the current working directory to the one specified, use the **cd** command in privileged EXEC mode.

cd [**disk0:** | **disk1:** | **flash:**] [*path*]

Syntax Description

disk0:	Specifies the internal Flash memory, followed by a colon.
disk1:	Specifies the removable, external Flash memory card, followed by a colon.
flash:	Specifies the internal Flash memory, followed by a colon. In the ASA 5500 series, the flash keyword is aliased to disk0 .
<i>path</i>	(Optional) The absolute path of the directory to change to.

Defaults

If you do not specify a directory, the directory is changed to the root directory.

Command Modes

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

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

Command History

Release	Modification
7.0	This command was introduced.

Examples

This example shows how to change to the “config” directory:

```
hostname# cd flash:/config/
```

Related Commands

Command	Description
pwd	Displays the current working directory.

certificate

To add the indicated certificate, use the **certificate** command in crypto ca certificate chain mode. When you use this command, the security appliance interprets the data included with it as the certificate in hexadecimal format. A **quit** string indicates the end of the certificate.

To delete the certificate, use the **no** form of the command.

certificate [**ca** | **ra-encrypt** | **ra-sign** | **ra-general**] *certificate-serial-number*

no certificate *certificate-serial-number*

Syntax Description

<i>certificate-serial-number</i>	Specifies the serial number of the certificate in hexadecimal format ending with the word quit.
ca	Indicates that the certificate is a certificate authority (CA) issuing certificate.
ra-encrypt	Indicates that the certificate is a registration authority (RA) key encipherment certificate used in SCEP.
ra-general	Indicates that the certificate is a registration authority (RA) certificate used for digital signing and key encipherment in SCEP messaging.
ra-sign	Indicates that the certificate is an registration authority (RA) digital signature certificate used in SCEP messaging.

Defaults

This command has no default values.

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
Certificate chain configuration	•	•	•	•	•

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

A certificate authority (CA) is an authority in a network that issues and manages security credentials and public key for message encryption. As part of a public key infrastructure, a CA checks with a registration authority (RA) to verify information provided by the requestor of a digital certificate. If the RA verifies the requestor's information, the CA can then issue a certificate.

Examples

This example enters ca trustpoint mode for a trustpoint named central, then enters crypto ca certificate chain mode for central, and adds a CA certificate with a serial number 29573D5FF010FE25B45:

```
hostname(config)# crypto ca trustpoint central
hostname(ca-trustpoint)# crypto ca certificate chain central
hostname(ca-cert-chain)# certificate ca 29573D5FF010FE25B45
 30820345 308202EF A0030201 02021029 572A3FF2 96EF854F D0D6732F E25B4530
 0D06092A 864886F7 0D010105 05003081 8F311630 1406092A 864886F7 0D010901
 16076140 622E636F 6D310B30 09060355 04061302 55533116 30140603 55040813
 0D6D6173 73616368 75736574 74733111 300F0603 55040713 08667261 6E6B6C69
 6E310E30 0C060355 040A1305 63697363 6F310F30 0D060355 040B1306 726F6F74
 6F75311C 301A0603 55040313 136D732D 726F6F74 2D736861 2D30362D 32303031
 301E170D 30313036 32363134 31313430 5A170D32 32303630 34313430 3133305A
 30818F31 16301406 092A8648 86F70D01 09011607 6140622E 636F6D31 0B300906
 03550406 13025553 31163014 06035504 08130D6D 61737361 63687573 65747473
 3111300F 06035504 07130866 72616E6B 6C696E31 0E300C06 0355040A 13056369
 73636F31 0F300D06 0355040B 1306726F 6F746F75 311C301A 06035504 0313136D
 732D726F 6F742D73 68612D30 362D3230 3031305C 300D0609 2A864886 F70D0101
 01050003 4B003048 024100AA 3EB9859B 8670A6FB 5E7D2223 5C11BCFE 48E6D3A8
 181643ED CF7E75EE E77D83DF 26E51876 97D8281E 9F58E4B0 353FDA41 29FC791B
 1E14219C 847D19F4 A51B7B02 03010001 A3820123 3082011F 300B0603 551D0F04
 04030201 C6300F06 03551D13 0101FF04 05300301 01FF301D 0603551D 0E041604
 14E0D412 3ACC96C2 FBF651F3 3F66C0CE A62AB63B 323081CD 0603551D 1F0481C5
 3081C230 3EA03CA0 3A86386C 6461703A 2F2F7732 6B616476 616E6365 64737276
 2F436572 74456E72 6F6C6C2F 6D732D72 6F6F742D 7368612D 30362D32 3030312E
 63726C30 3EA03CA0 3A863868 7474703A 2F2F7732 6B616476 616E6365 64737276
 2F436572 74456E72 6F6C6C2F 6D732D72 6F6F742D 7368612D 30362D32 3030312E
 63726C30 40A03EA0 3C863A66 696C653A 2F2F5C5C 77326B61 6476616E 63656473
 72765C43 65727445 6E726F6C 6C5C6D73 2D726F6F 742D7368 612D3036 2D323030
 312E6372 6C301006 092B0601 04018237 15010403 02010130 0D06092A 864886F7
 0D010105 05000341 0056221E 03F377B9 E6900BF7 BCB3568E ADBA146F 3B8A71F3
 DF9EB96C BB1873B2 B6268B7C 0229D8D0 FFB40433 C8B3CB41 0E4D212B 2AEEDC77
 BEA3C1FE 5EE2AB6D 91
quit
```

Related Commands

Command	Description
clear configure crypto map	Clears all configuration for all crypto maps
show running-config crypto map	Displays the crypto map configuration.
crypto ca certificate chain	Enters certificate crypto ca certificate chain mode.
crypto ca trustpoint	Enters ca trustpoint mode.
show running-config crypto map	Displays all configuration for all the crypto maps

chain

To enable sending of a certificate chain, use the **chain** command in tunnel-group ipsec-attributes configuration mode. This action includes the root certificate and any subordinate CA certificates in the transmission. To return this command to the default, use the **no** form of this command.

chain

no chain

Syntax Description

This command has no arguments or keywords.

Defaults

The default setting for this command is disabled.

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
Tunnel-group ipsec attributes configuration	•	—	•	—	—

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

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

Examples

The following example entered in config-ipsec configuration mode, enables sending a chain for an IPSec LAN-to-LAN tunnel group with the IP address of 209.165.200.225, which includes the root certificate and any subordinate CA certificates:

```
hostname(config)# tunnel-group 209.165.200.225 type IPSec_L2L
hostname(config)# tunnel-group 209.165.200.225 ipsec-attributes
hostname(config-ipsec)# chain
hostname(config-ipsec)#
```

Related Commands	Command	Description
	clear configure tunnel-group	Clears all configured tunnel groups.
	show running-config tunnel-group	Shows the indicated certificate map entry.
	tunnel-group-map default-group	Associates the certificate map entries created using the crypto ca certificate map command with tunnel groups.

changeto

To change between security contexts and the system, use the **changeto** command in privileged EXEC mode.

changeto {**system** | **context** *name*}

Syntax Description

context <i>name</i>	Changes to the context with the specified name.
system	Changes to the system execution space.

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		
	Routed	Transparent	Single	Multiple Context	System
Privileged EXEC	•	•	—	•	•

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

If you log into the system execution space or the admin context, you can change between contexts and perform configuration and monitoring tasks within each context. The “running” configuration that you edit in configuration mode, or that is used in the **copy** or **write** commands, depends on which execution space you are in. When you are in the system execution space, the running configuration consists only of the system configuration; when you are in a context execution space, the running configuration consists only of that context. For example, you cannot view all running configurations (system plus all contexts) by entering the **show running-config** command. Only the current configuration appears.

Examples

The following example changes between contexts and the system in privileged EXEC mode:

```
hostname/admin# changeto system
hostname# changeto context customerA
hostname/customerA#
```

The following example changes between the system and the admin context in interface configuration mode. When you change between execution spaces, and you are in a configuration submode, the mode changes to the global configuration mode in the new execution space.

```
hostname(config-if)# changeto context admin
hostname/admin(config)#
```

Related Commands	Command	Description
	admin-context	Sets a context to be the admin context.
	context	Creates a security context in the system configuration and enters context configuration mode.
	show context	Shows a list of contexts (system execution space) or information about the current context.

checkheaps

To configure checkheaps verification intervals, use the **checkheaps** command in global configuration mode. To set the value to the default, use the **no** form of this command. Checkheaps is a periodic process that verifies the sanity of the heap memory buffers (dynamic memory is allocated from the system heap memory region) and the integrity of the code region.

checkheaps {**check-interval** | **validate-checksum**} *seconds*

no checkheaps {**check-interval** | **validate-checksum**} [*seconds*]

Syntax Description

check-interval	Sets the buffer verification interval. The buffer verification process checks the sanity of the heap (allocated and freed memory buffers). During each invocation of the process, the security appliance checks the entire heap, validating each memory buffer. If there is a discrepancy, the security appliance issues either an “allocated buffer error” or a “free buffer error.” If there is an error, the security appliance dumps traceback information when possible and reloads.
validate-checksum	Sets the code space checksum validation interval. When the security appliance first boots up, the security appliance calculates a hash of the entire code. Later, during the periodic check, the security appliance generates a new hash and compares it to the original. If there is a mismatch, the security appliance issues a “text checksum checkheaps error.” If there is an error, the security appliance dumps traceback information when possible and reloads.
<i>seconds</i>	Sets the interval in seconds between 1 and 2147483.

Defaults

The default intervals are 60 seconds each.

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
Global configuration	•	•	•	—	•

Command History

Release	Modification
7.0	This command was introduced.

Examples

The following example sets the buffer allocation interval to 200 seconds and the code space checksum interval to 500 seconds:

```
hostname(config)# checkheaps check-interval 200
hostname(config)# checkheaps validate-checksum 500
```

Related Commands	Command	Description
	show checkheaps	Shows checkheaps statistics.

check-retransmission

To prevent against TCP retransmission style attacks, use the **check-retransmission** command in tcp-map configuration mode. To remove this specification, use the **no** form of this command.

check-retransmission

no check-retransmission

Syntax Description

This command has no arguments or keywords.

Defaults

The default is disabled.

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
Tcp-map configuration	•	•	•	•	—

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

The **tcp-map** command is used along with the Modular Policy Framework infrastructure. Define the class of traffic using the **class-map** command and customize the TCP inspection with **tcp-map** commands. Apply the new TCP map using the **policy-map** command. Activate TCP inspection with **service-policy** commands.

Use the **tcp-map** command to enter tcp-map configuration mode. To prevent against TCP retransmission style attacks that arise from end-system interpretation of inconsistent retransmissions, use the **check-retransmission** command in tcp-map configuration mode.

The security appliance will make efforts to verify if the data in retransmits are the same as the original. If the data doesn't match, then the connection is dropped by the security appliance. When this feature is enabled, packets on the TCP connection are only allowed in order. For more details, see the **queue-limit** command.

Examples

The following example enables the TCP check-retransmission feature on all TCP flows:

```
hostname(config)# access-list TCP extended permit tcp any any
hostname(config)# tcp-map tmap
hostname(config-tcp-map)# check-retransmission
hostname(config)# class-map cmap
hostname(config-cmap)# match access-list TCP
hostname(config)# policy-map pmap
```

```
hostname(config-pmap)# class cmap
hostname(config-pmap)# set connection advanced-options tmap
hostname(config)# service-policy pmap global
```

Related Commands

Command	Description
class	Specifies a class map to use for traffic classification.
help	Shows syntax help for the policy-map , class , and description commands.
policy-map	Configures a policy; that is, an association of a traffic class and one or more actions.
set connection	Configures connection values.
tcp-map	Creates a TCP map and allows access to tcp-map configuration mode.

checksum-verification

To enable or disable TCP checksum verification, use the **checksum-verification** command in tcp-map configuration mode. To remove this specification, use the **no** form of this command.

checksum-verification

no checksum-verification

Syntax Description

This command has no arguments or keywords.

Defaults

Checksum verification is disabled by default.

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
Tcp-map configuration	•	•	•	•	—

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

The **tcp-map** command is used along with the Modular Policy Framework infrastructure. Define the class of traffic using the **class-map** command and customize the TCP inspection with **tcp-map** commands. Apply the new TCP map using the **policy-map** command. Activate TCP inspection with **service-policy** commands.

Use the **tcp-map** command to enter tcp-map configuration mode. Use the **checksum-verification** command in tcp-map configuration mode to enable TCP checksum verification. If the check fails, the packet is dropped.

Examples

The following example enables TCP checksum verification on TCP connections from 10.0.0.0 to 20.0.0.0:

```
hostname(config)# access-list TCP1 extended permit tcp 10.0.0.0 255.0.0.0 20.0.0.0
255.0.0.0
hostname(config)# tcp-map tmap
hostname(config-tcp-map)# checksum-verification

hostname(config)# class-map cmap
hostname(config-cmap)# match access-list TCP1

hostname(config)# policy-map pmap
hostname(config-pmap)# class cmap
```

```
hostname(config-pmap)# set connection advanced-options tmap
```

```
hostname(config)# service-policy pmap global
```

Related Commands

Command	Description
class	Specifies a class map to use for traffic classification.
help	Shows syntax help for the policy-map , class , and description commands.
policy-map	Configures a policy; that is, an association of a traffic class and one or more actions.
set connection	Configures connection values.
tcp-map	Creates a TCP map and allows access to tcp-map configuration mode.

class (policy-map)

To assign a class-map to a policy for traffic classification, use the **class** command in policy-map mode. To remove a class-map specification for a policy map, use the **no** form of this command.

class *classmap-name*

no class *classmap-name*

Syntax Description

classmap-name The name for the class-map. The name can be up to 40 characters long.

Defaults

By default, “class class-default” always exists at the end of a policy map.

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
Policy-map	•	•	•	•	—

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

Including the class-default, up to 63 class commands can be configured in a policy map.

The name “class-default” is a reserved name for default class, and it always exists; that is, you can include it in your configuration, but you cannot reconfigure or remove it using CLI. See the description of the **class-map** command for more information.

Use the **class** command to enter class mode, in which you can enter the following commands:

set connection

inspect

ips

priority

police

See the individual command descriptions for detailed information.

Examples

The following is an example of the class command in policy-map mode; note the change in the prompt:

```
hostname(config)# class-map localclass1
hostname(config-cmap)# match any
hostname(config-cmap)# exit
hostname(config)# policy-map localpolicy1
```

```
hostname(config-pmap)# class localclass1
hostname(config-pmap-c)# priority
hostname(config-pmap-c)# exit
```

The following is an example of a **policy-map** command, with its **class** commands, for a connection policy that limits connections to an HTTP server to a maximum of 256:

```
hostname(config)# access-list myhttp permit tcp any host 10.1.1.1
hostname(config)# class-map myhttp

hostname(config-cmap)# match access-list myhttp
hostname(config-cmap)# exit

hostname(config)# policy-map global-policy
hostname(config-pmap)# description This policy map defines a policy concerning connection
to http server.
hostname(config-pmap)# class myhttp
hostname(config-pmap-c)# set connection conn-max 256
```

The following is an example of a **policy-map** command, with its **class** commands, for the outside interface (defined in the **service-policy** command). The **class-map** command specifies a class of traffic that has a destination IP address of 192.168.10.10:

```
hostname(config)# class-map outside-voip
hostname(config-cmap)# match dscp af11
hostname(config-cmap)# exit

hostname(config)# policy-map outside-policy
hostname(config-pmap)# description This policy map defines policies for the outside
interface.
hostname(config-pmap)# class outside-voip
hostname(config-pmap-c)# priority
hostname(config-pmap-c)# exit
hostname(config-pmap)# exit
hostname(config)# service-policy outside-policy interface outside
```

Related Commands

Command	Description
clear configure policy-map	Removes all policy-map configuration, except for any policy-map that is in use in a service-policy command.
policy-map	Configures a policy; that is, an association of one or more traffic classes, each with one or more actions.
show running-config policy-map	Displays all current policy-map configurations.

class-map

To classify traffic for an interface when using Modular Policy Framework to configure a security feature, use the **class-map** command in global configuration mode. To delete a class map, use the **no** form of this command.

class-map *class_map_name*

no class-map *class_map_name*

Syntax Description

<i>class_map_name</i>	Text for the class map name; the text can be up to 40 characters in length. The name space for class-map is local to a security context. Therefore, the same name may be used in multiple security contexts. The maximum number of class-maps per security context is 255.
-----------------------	--

Defaults

The default class, class-default, always exists and cannot be configured or removed using the CLI. A default class, when used in a policy map, means “all other traffic.”. The definition of class-default is:

```
class-map class-default
  match any
```

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
Global configuration	•	•	•	•	—

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

The **class-map** command allows you to define a traffic class when using Modular Policy Framework to configure a security feature. Modular Policy Framework provides a consistent and flexible way to configure security appliance features in a manner similar to Cisco IOS software QoS CLI. Use the **class-map**, **policy-map**, and **service-policy** global configuration commands to configure a security feature using Modular Policy Framework.

Define a traffic class using the **class-map** global configuration command. Then create a policy map by associating the traffic class with one or more actions using the **policy-map** global configuration command. Finally, create a security policy by associating the policy map with one or more interfaces using the **service-policy** command.

A traffic class map contains, at most, one **match** command (with the exception of the **match tunnel-group** and **match default-inspection-traffic** commands). The **match** command identifies the traffic included in the traffic class. When a packet is matched against a class-map, the match result is either a match or a no match.

Use the **class-map** command to enter class-map configuration mode. From class-map configuration mode, you can define the traffic to include in the class using the **match** command. The following commands are available in class-map configuration mode:

description	Specifies a description for the class-map.
match access-list	Specifies the name of an access-list to be used as match criteria. When a packet does not match an entry in the access-list, the match result is a no-match. When a packet matches an entry in an access-list, and if it is a permit entry, the match result is a match. Otherwise, if it matches a deny access-list entry, the match result is no-match.
match port	Specifies to match traffic using a TCP/UDP destination port.
match precedence	Specifies to match the precedence value represented by the TOS byte in the IP header.
match dscp	Specifies to match the IETF-defined DSCP value in the IP header.
match rtp	Specifies to match an RTP port.
match tunnel-group	Specifies to match security related tunnel groups.
match flow ip destination-address	Specifies to match the IP destination address.
match default-inspection-traffic	Specifies to match default traffic for the inspect commands.

Examples

The following example shows how to define a traffic class of all TCP traffic to port 21 using a class map:

```
hostname(config)# class-map ftp-port
hostname(config-cmap)# match port tcp eq 21
```

Related Commands

Command	Description
clear configure class-map	Removes all of the traffic map definitions.
policy-map	Creates a policy map by associating the traffic class with one or more actions.
service-policy	Creates a security policy by associating the policy map with one or more interfaces.
show running-config class-map	Displays the information about the class map configuration.

clear aaa local user fail-attempts

To reset the number of failed user authentication attempts to zero without modifying the user's locked-out status, use the **clear aaa local user fail-attempts** command in privileged EXEC mode.

clear aaa local user authentication fail-attempts {username *name* | all}

Syntax Description

all	Resets the failed-attempts counter to 0 for all users.
<i>name</i>	Specifies a specific username for which the failed-attempts counter is reset to 0.
username	Indicates that the following parameter is a username, for which the failed-attempts counter is reset to 0.

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		
	Routed	Transparent	Single	Multiple Context	System
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

Use this command when a user fails authentication a few times, but you want to reset the counter to zero, for example, when the configuration has recently been modified.

After the configured number of failed authentication attempts, the user is locked out of the system and cannot successfully log in until either a system administrator unlocks the username or the system reboots.

The number of failed attempts resets to zero and the lockout status resets to No when the user successfully authenticates or when the security appliance reboots.

Locking or unlocking a username results in a syslog message.

A system administrator with a privilege level of 15 cannot be locked out.

Examples

The following example shows use of the **clear aaa local user authentication fail-attempts** command to reset the failed-attempts counter to 0 for the username anyuser:

```
hostname(config)# clear aaa local user authentication fail-attempts username anyuser
hostname(config)#
```

The following example shows use of the **clear aaa local user authentication fail-attempts** command to reset the failed-attempts counter to 0 for all users:

```
hostname(config)# clear aaa local user authentication fail-attempts all
hostname(config)#
```

Related Commands

Command	Description
aaa local authentication attempts max-fail	Configures a limit on the number of failed user authentication attempts allowed.
clear aaa local user logout	Resets the number of failed user authentication attempts to zero without modifying the user's locked-out status.
show aaa local user [locked]	Shows the list of usernames that are currently locked.

clear aaa local user logout

To clear the lockout status of the specified users and set their failed-attempts counter to 0, use the **clear aaa local user logout** command in privileged EXEC mode.

clear aaa local user logout {username *name* | all}

Syntax Description

all	Resets the failed-attempts counter to 0 for all users.
<i>name</i>	Specifies a specific username for which the failed-attempts counter is reset to 0.
username	Indicates that the following parameter is a username, for which the failed-attempts counter is reset to 0.

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		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

You can specify a single user by using the **username** option or all users with the **all** option.

This command affects only the status of users that are locked out.

The administrator cannot be locked out of the device.

Locking or unlocking a username results in a syslog message.

Examples

The following example shows use of the **clear aaa local user logout** command to clear the lockout condition and reset the failed-attempts counter to 0 for the username anyuser:

```
hostname(config)# clear aaa local user logout username anyuser
hostname(config)#
```

Related Commands	Command	Description
	aaa local authentication attempts max-fail	Configures a limit on the number of failed user authentication attempts allowed.
	clear aaa local user fail-attempts	Resets the number of failed user authentication attempts to zero without modifying the user's locked-out status.
	show aaa local user [locked]	Shows the list of usernames that are currently locked.

clear aaa-server statistics

To reset the statistics for AAA servers, use the **clear aaa-server statistics** command in privileged EXEC mode.

clear aaa-server statistics [**LOCAL** | *groupname* [**host** *hostname*] | **protocol** *protocol*]

Syntax Description

LOCAL	(Optional) Clears statistics for the LOCAL user database.
<i>groupname</i>	(Optional) Clears statistics for servers in a group.
host <i>hostname</i>	(Optional) Clears statistics for a particular server in the group.
protocol <i>protocol</i>	(Optional) Clears statistics for servers of the specified protocol: <ul style="list-style-type: none"> • kerberos • ldap • nt • radius • sdi • tacacs+

Defaults

Remove all AAA-server statistics across all groups.

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	•	•	•	•	—

Command History

Release	Modification
7.0	This command was modified to adhere to CLI guidelines. In the protocol values, nt replaces the older nt-domain , and sdi replaces the older rsa-ace .

Examples

The following command shows how to reset the AAA statistics for a specific server in a group:

```
hostname(config)# clear aaa-server statistics svrgrp1 host 1.2.3.4
```

The following command shows how to reset the AAA statistics for an entire server group:

```
hostname(config)# clear aaa-server statistics svrgrp1
```

The following command shows how to reset the AAA statistics for all server groups:

```
hostname(config)# clear aaa-server statistics
```

The following command shows how to reset the AAA statistics for a particular protocol (in this case, TACACS+):

```
hostname(config)# clear aaa-server statistics protocol tacacs+
```

Related Commands	Command	Description
	aaa-server protocol	Specifies and manages the grouping of AAA server connection data.
	clear configure aaa-server	Removes all non-default aaa server groups or clear the specified group
	show aaa-server	Displays AAA server statistics.
	show running-config aaa-server	Displays the current AAA server configuration values.

clear access-group

To remove access groups from all the interfaces, use the **clear access-group** command.

clear access-group

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values.

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

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

Command History	Release	Modification
	Preexisting	This command was preexisting.

Examples The following example shows how to remove all access groups:

```
hostname(config)# clear access-group
```

Related Commands	Command	Description
	access-group	Binds an access list to an interface.
	show running-config access-group	Displays the current access group configuration.

clear access-list

To clear an access-list counter, use the **clear access-list** command in global configuration mode.

clear access-list [*id*] **counters**

Syntax Description	counters	Clears access list counters.
	<i>id</i>	(Optional) Name or number of an access list.

Defaults All the access list counters are cleared.

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	•	•	•	•	—

Command History	Release	Modification
	Preexisting	This command was preexisting.

Usage Guidelines When you enter the **clear access-list** command, all the access list counters are cleared if you do not specify an *id*.

Examples The following example shows how to clear a specific access list counter:

```
hostname# clear access-list inbound counters
```

Related Commands	Command	Description
	access-list extended	Adds an access list to the configuration and configures policy for IP traffic through the firewall.
	access-list standard	Adds an access list to identify the destination IP addresses of OSPF routes, which can be used in a route map for OSPF redistribution.
	clear configure access-list	Clears an access list from the running configuration.
	show access-list	Displays the access list entries by number.
	show running-config access-list	Displays the access list configuration that is running on the security appliance.

clear arp statistics

To clear ARP statistics, use the **clear arp statistics** command in privileged EXEC mode.

clear arp statistics

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values.

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

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

Command History	Release	Modification
	Preexisting	This command was preexisting.

Examples The following example clears all ARP statistics:

```
hostname# clear arp statistics
```

Related Commands	Command	Description
	arp	Adds a static ARP entry.
	arp-inspection	For transparent firewall mode, inspects ARP packets to prevent ARP spoofing.
	show arp statistics	Shows ARP statistics.
	show running-config arp	Shows the current configuration of the ARP timeout.

clear asp drop

To clear accelerated security path drop statistics, use the **clear asp drop** command in privileged EXEC mode.

clear asp drop [*flow type* | *frame type*]

Syntax Description

flow	(Optional) Clears the dropped flow statistics.
frame	(Optional) Clears the dropped packet statistics.
<i>type</i>	(Optional) Clears the dropped flow or packets statistics for a particular process. See “ Usage Guidelines ” for a list of types.

Defaults

By default, this command clears all drop statistics.

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	•	•	•	•	•

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

Process types include the following:

```
acl-drop
audit-failure
closed-by-inspection
conn-limit-exceeded
fin-timeout
flow-reclaimed
fo-primary-closed
fo-standby
fo_rep_err
host-removed
inspect-fail
ips-fail-close
ips-request
ipsec-spoof-detect
loopback
mcast-entry-removed
mcast-intrf-removed
mgmt-lockdown
nat-failed
nat-rpf-failed
need-ike
```

```
no-ipv6-ipsec
non_tcp_syn
out-of-memory
parent-closed
pinhole-timeout
recurse
reinject-punt
reset-by-ips
reset-in
reset-ooout
shunned
syn-timeout
tcp-fins
tcp-intecept-no-response
tcp-intercept-kill
tcp-intercept-unexpected
tcpnorm-invalid-syn
tcpnorm-rexmit-bad
tcpnorm-win-variation
timeout
tunnel-pending
tunnel-torn-down
xlate-removed
```

Examples

The following example clears all drop statistics:

```
hostname# clear asp drop
```

Related Commands

Command	Description
show asp drop	Shows the accelerated security path counters for dropped packets.

clear asp table

To clear the hit counters either in asp arp or classify tables, or both, use the **clear asp table** command in privileged EXEC mode.

clear asp table [arp | classify]

Syntax Description

arp	clears the hits counters in asp arp table only.
classify	clears the hits counters in asp classify tables only

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		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	•	•	•	•	•

Command History

Release	Modification
7.2(4)	This command was introduced.

Usage Guidelines

There are only two options arp and classify having hits in the **clear asp table** command

Examples

The following example clears all drop statistics:

```
hostname# clear asp table
```

```
Warning: hits counters in asp arp and classify tables are cleared, which might impact the
hits statistic of other modules and output of other "show" commands! hostname#clear asp
table arp
```

```
Warning: hits counters in asp arp table are cleared, which might impact the hits statistic
of other modules and output of other "show" commands! hostname#clear asp table classify
```

```
Warning: hits counters in classify tables are cleared, which might impact the hits
statistic of other modules and output of other "show" commands! hostname(config)# clear
asp table
```

```
Warning: hits counters in asp tables are cleared, which might impact the hits statistics
of other modules and output of other "show" commands! hostname# sh asp table arp
```

```
Context: single_vf, Interface: inside 10.1.1.11 Active 00e0.8146.5212 hits 0
```

```
Context: single_vf, Interface: identity :: Active 0000.0000.0000 hits 0 0.0.0.0 Active
0000.0000.0000 hits 0
```


Related Commands

Command	Description
show asp table arp	Shows the contents of the accelerated security path, which might help you troubleshoot a problem.

clear blocks

To reset the packet buffer counters such as the low watermark and history information, use the **clear blocks** command in privileged EXEC mode.

clear blocks

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values.

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

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

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines Resets the low watermark counters to the current available blocks in each pool. Also clears the history information stored during the last buffer allocation failure.

Examples The following example clears the blocks:

```
hostname# clear blocks
```

Command	Description
blocks	Increases the memory assigned to block diagnostics
show blocks	Shows the system buffer utilization.

clear capture

To clear the capture buffer, use the **clear capture** *capture_name* command.

clear capture *capture_name*

Syntax Description

capture_name Name of the packet capture.

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 Mode	•	•	•	•	•

Command History

Release	Modification
2.2(1)	Support for this command was introduced on the security appliance.

Usage Guidelines

The shortened form of the **clear capture** (for example, **cl cap** or **clear cap**) is not supported to prevent accidental destruction of all the packet captures.

Examples

This example shows how to clear the capture buffer for the capture buffer “trudy”:

```
hostname(config)# clear capture trudy
```

Related Commands

Command	Description
capture	Enables packet capture capabilities for packet sniffing and network fault isolation.
show capture	Displays the capture configuration when no options are specified.

clear configure

To clear the running configuration, use the **clear configure** command in global configuration mode.

```
clear configure {primary | secondary | all | command}
```

Syntax Description	command	Clears the configuration for a specified command. For more information, see individual entries in this guide for each clear configure <i>command</i> command.
	primary	Clears commands related to connectivity, including the following commands: <ul style="list-style-type: none"> tftp-server shun route ip address mtu failover monitor-interface boot
	secondary	Clears commands not related to connectivity (that are cleared using the primary keyword).
	all	Clears the entire running configuration.

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		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	•	•	•	•	•

Command History	Release	Modification
	Preexisting	This command was preexisting.

Usage Guidelines When you enter this command in a security context, you clear only the context configuration. If you enter this command in the system execution space, you clear the system running configuration as well as all context running configurations. Because you cleared all context entries in the system configuration (see the **context** command), the contexts are no longer running, and you cannot change to a context execution space.

Before clearing the configuration, make sure you save any changes to the **boot config** command (which specifies the startup configuration location) to the startup configuration; if you changed the startup configuration location only in the running configuration, then when you restart, the configuration loads from the default location.

Examples

The following example clears the entire running configuration:

```
hostname(config)# clear configure all
```

Related Commands

Command	Description
configure http	Merges a configuration file from the specified HTTP(S) URL with the running configuration.
configure memory	Merges the startup configuration with the running configuration.
configure net	Merges a configuration file from the specified TFTP URL with the running configuration.
configure factory-default	Adds commands you enter at the CLI to the running configuration.
show running-config	Shows the running configuration.

clear configure aaa

To clear the aaa configuration, use the **clear configure aaa** command in global configuration mode. The **clear configure aaa** command removes the AAA command statements from the configuration.

clear configure aaa

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0	This command was modified for consistency within the CLI.

Usage Guidelines

This command also resets the AAA parameters to their default values, if any.

There is no undo.

Examples

```
hostname(config)# clear configure aaa
```

Related Commands

Command	Description
aaa accounting	Enable, disable, or view the keeping of records about which network services a user has accessed.
aaa authentication	Enable or view LOCAL, TACACS+, or RADIUS user authentication, on a server designated by the aaa-server command, or ASDM user authentication
aaa authorization	Enable or disable user authorization for a LOCAL or a TACACS+ server designated by the aaa-server command, or for ASDM user authentication.
show running-config aaa	Display the AAA configuration.

clear configure aaa-server

To remove all AAA server groups or to clear the specified group, use the **clear configure aaa-server** command in global configuration mode.

clear configure aaa-server [*server-tag*]

clear configure aaa-server [*server-tag*] **host** *server-ip*

Syntax Description

<i>server-ip</i>	The IP address of the AAA server.
<i>server-tag</i>	(Optional) Symbolic name of the server group to be cleared.

Defaults

Remove all AAA server groups.

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
Global configuration	•	•	—	—	•

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

You can specify a particular AAA server group or, by default, all AAA server groups.

Use the **host** keyword to specify a particular server within a server group.

This command also resets the AAA server parameters to their default values, if any.

Examples

```
hostname(config)# aaa-server svrgrp1 protocol sdi
hostname(config)# aaa-server svrgrp1 host 1.2.3.4
hostname(config-aaa-server)# timeout 9
hostname(config-aaa-server)# retry 7
hostname(config-aaa-server)# sdi-version sdi-5
hostname(config-aaa-server)# exit
```

Given the preceding configuration, the following command shows how to remove a specific server from a group:

```
hostname(config)# clear config aaa-server svrgrp1 host 1.2.3.4
```

The following command shows how to remove a server group:

```
hostname(config)# clear config aaa-server svrgrp1
```

The following command shows how to remove all server groups:

```
hostname(config)# clear config aaa-server
```

Related Commands

Command	Description
aaa-server host	Specifies and manages host-specific AAA server connection data.
aaa-server protocol	Allows you to configure AAA server parameters that are group-specific and common to all hosts.
show running-config aaa	Display the current maximum number of concurrent proxy connections allowed per user, along with other AAA configuration values.

clear configure access-group

To remove access groups from all the interfaces, use the **clear configure access-group** command.

clear configure access-group

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values.

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

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

Command History	Release	Modification
	7.0	Added keyword configure .

Examples The following example shows how to remove all access groups:

```
hostname(config)# clear configure access-group
```

Related Commands	Command	Description
	access-group	Binds an access list to an interface.
	show running-config access-group	Displays the current access group configuration.

clear configure access-list

To clear an access list from the running configuration, use the **clear configure access list** command in global configuration mode.

clear configure access-list [*id*]

Syntax Description

id (Optional) Name or number of an access list.

Defaults

All the access lists are cleared from the running configuration.

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
Global configuration	•	•	•	•	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

The **clear configure access-list** command automatically unbinds an access list from a **crypto map** command or interface. The unbinding of an access list from a **crypto map** command can lead to a condition that discards all packets because the **crypto map** commands referencing the access list are incomplete. To correct the condition, either define other **access-list** commands to complete the **crypto map** commands or remove the **crypto map** commands that pertain to the **access-list** command. Refer to the **crypto map client** command for more information.

Examples

This example shows how to clear the access lists from the running configuration:

```
hostname(config)# clear configure access-list
```

Related Commands

Command	Description
access-list extended	Adds an access list to the configuration and configures policy for IP traffic through the firewall.
access-list standard	Adds an access list to identify the destination IP addresses of OSPF routes, which can be used in a route map for OSPF redistribution.
clear access-list	Clears access list counters.

Command	Description
show access-list	Displays counters for an access list.
show running-config access-list	Displays the access list configuration running on the security appliance.

clear configure alias

To remove all **alias** commands from the configuration, use the **clear configure alias** command in global configuration mode.

clear configure alias

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values.

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

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

Release	Modification
Preexisting	This command was preexisting.

Examples This example shows how to remove all **alias** commands from the configuration:

```
hostname(config)# clear configure alias
```

Related Commands	Command	Description
	alias	Translates one address into another.
	show running-config alias	Displays the overlapping addresses with dual NAT commands in the configuration.

clear configure arp-inspection

To clear the ARP inspection configuration, use the **clear configure arp-inspection** command in global configuration mode.

clear configure arp-inspection

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values.

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

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

Release	Modification
7.0	This command was introduced.

Command History

Examples The following example clears the ARP inspection configuration:

```
hostname# clear configure arp-inspection
```

Related Commands	Command	Description
	arp	Adds a static ARP entry.
	arp-inspection	For transparent firewall mode, inspects ARP packets to prevent ARP spoofing.
	firewall transparent	Sets the firewall mode to transparent.
	show arp statistics	Shows ARP statistics.
	show running-config arp	Shows the current configuration of the ARP timeout.

clear configure asdm

To remove all **asdm** commands from the running configuration, use the **clear configure asdm** command in global configuration mode.

clear configure asdm [**location** | **group** | **image**]

Syntax Description

group	(Optional) Clears only the asdm group commands from the running configuration.
image	(Optional) Clears only the asdm image command from the running configuration.
location	(Optional) Clears only the asdm location commands from the running configuration.

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		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	•	•	•	•	•

Command History

Release	Modification
7.0	This command was changed from the clear pdm command to the clear configure asdm command.

Usage Guidelines

To view the **asdm** commands in the running configuration, use the **show running-config asdm** command.

Clearing the **asdm image** command from the configuration disables ASDM access. Clearing the **asdm location** and **asdm group** commands from the configuration causes ASDM to regenerate those commands the next time ASDM is accessed, but may disrupt active ASDM sessions.



Note

On security appliances running in multiple context mode, the **clear configure asdm image** command is only available in the system execution space, while the **clear configure asdm group** and **clear configure asdm location** commands are only available in the user contexts.

Examples

The following example clears the **asdm group** commands from the running configuration:

```
hostname(config)# clear configure asdm group
```

```
hostname(config)#
```

Related Commands

Command	Description
asdm group	Used by ASDM to associate object group names with interfaces.
asdm image	Specifies the ASDM image file.
asdm location	Used by ASDM to record IP address to interface associations.
show running-config asdm	Displays the asdm commands in the running configuration.

clear configure auth-prompt

To remove the previously specified authentication prompt challenge text and revert to the default value, if any, use the **clear configure auth-prompt** command in global configuration mode.

clear configure auth-prompt

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values.

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

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

Release	Modification
7.0	This command was modified to conform with CLI standards.

Usage Guidelines

After you clear the authentication prompt, the prompt users see when they log in depends on the protocol they use:

- Users who log in using HTTP see HTTP Authentication.
- Users who log in using FTP see FTP Authentication.
- Users who log in using Telnet see no prompt.

Examples

This example shows how to clear the auth-prompt:

```
hostname(config)# clear configure auth-prompt
```

Related Commands	auth-prompt	Sets the user authorization prompts.
	show running-config auth-prompt	Displays the user authorization prompts.

clear configure banner

To remove all the banners, use the **clear configure banner** command in global configuration mode.

clear configure banner

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values.

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

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

Command History	Release	Modification
	2.2(1)	This command was introduced.

Examples This example shows how to clear banners:

```
hostname(config)# clear configure banner
```

Related Commands	Command	Description
	banner	Configures the session, login, or message-of-the-day banner.
	show running-config banner	Displays all banners.

clear configure ca certificate map

To remove all certificate map entries or to remove a specified certificate map entry, use the **clear configure ca configure map** command in global configuration mode.

clear configure ca certificate map [*sequence-number*]

Syntax Description

sequence-number (Optional) Specifies a number for the certificate map rule you are removing. The range is 1 through 65535.

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		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	•	•	•	•	

Command History

Release	Modification
7.0	This command was introduced.

Examples

The following example removes all certificate map entries.

```
hostname(config)# clear configure ca certificate map
hostname(config)#
```

Related Commands

Command	Description
crypto ca certificate map	Enters CA certificate map mode.

clear configure class-map

To remove all class maps, use the **clear configure class-map** command in global configuration mode.

clear configure class-map

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values.

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

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

Release	Modification
7.0	Added keyword configure .

Usage Guidelines To clear the class map for a specific class map name, use the **no** form of the **class-map** command.

Examples The following example shows how to clear all configured class-maps:
hostname(config)# **clear configure class-map**

Related Commands	Command	Description
	class-map	Applies a traffic class to an interface.
	show running-config class-map	Displays the information about the class map configuration.

clear configure clock

To clear the clock configuration, use the **clear configure clock** command in global configuration mode.

clear configure clock

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values.

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

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

Command History	Release	Modification
	7.0	This command was changed from clear clock .

Usage Guidelines This command clears all **clock** configuration commands. The **clock set** command is not a configuration command, so this command does not reset the clock. To reset the clock, you need to set a new time for the **clock set** command.

Examples The following example clears all clock commands:

```
hostname# clear configure clock
```

Related Commands	Command	Description
	clock set	Manually sets the time.
	clock summer-time	Sets the date range to show daylight savings time.
	clock timezone	Sets the time zone.

clear configure command-alias

To remove all non-default command aliases, use the **clear configure command-alias** command in global configuration mode.

clear configure command-alias

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values.

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

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

Release	Modification
7.0	This command was introduced.

Usage Guidelines This command has no usage guidelines.

Examples The following example shows how to remove all non-default command aliases:

```
hostname(config)# clear configure command-alias
```

Command	Description
command-alias	Creates a command alias.
show running-config command-alias	Displays all non-default command aliases.

clear configure console

To reset the console connection settings to defaults, use the **clear configure console** command in global configuration mode.

clear configure console

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values.

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

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

Release	Modification
7.0	This command was introduced.

Examples The following example shows how to reset the console connection settings to defaults:

```
hostname(config)# clear configure console
```

Related Commands	Command	Description
	console timeout	Sets the idle timeout for a console connection to the security appliance.
	show running-config console timeout	Displays the idle timeout for a console connection to the security appliance.

clear configure context

To clear all context configurations in the system configuration, use the **clear configure context** command in global configuration mode.

clear configure context [noconfirm]

Syntax Description

noconfirm (Optional) Removes all contexts without prompting you for confirmation. This option is useful for automated scripts.

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		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	•	•	—	—	•

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

This command lets you remove all contexts, including the admin context. The admin context cannot be removed using the **no context** command, but can be removed using the **clear configure context** command.

Examples

The following example removes all contexts from the system configuration, and does not confirm the deletion:

```
hostname(config)# clear configure context noconfirm
```

Related Commands

Command	Description
admin-context	Sets the admin context.
changeto	Changes between contexts or the system execution space.
context	Creates a security context in the system configuration and enters context configuration mode.

Command	Description
mode	Sets the context mode to single or multiple.
show context	Shows a list of contexts (system execution space) or information about the current context.

clear configure crypto

To remove the entire crypto configuration, including IPsec, crypto maps, dynamic crypto maps, CA trustpoints, all certificates, certificate map configurations, and ISAKMP, use the **clear configure crypto** command in global configuration. To remove specific configurations, use this command with keywords as shown in the syntax. Take caution when using this command.

clear configure crypto [**ca** | **dynamic-map** | **ipsec** | **isakmp** | **map**]

Syntax Description

ca	Removes certification authority policy.
dynamic-map	Removes dynamic crypto map configuration.
ipsec	Removes IPsec configuration.
isakmp	Removes ISAKMP configuration.
map	Removes crypto map configuration.

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		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	•	—	•	—	—

Command History

Release	Modification
7.0	This command was introduced.

Examples

The following example issued in global configuration mode, removes all of the crypto configuration from the security appliance:

```
hostname(config)# clear configure crypto
hostname(config)#
```

Related Commands

Command	Description
clear configure crypto dynamic-map	Clears all or specified crypto dynamic maps from the configuration.
clear configure crypto map	Clears all or specified crypto maps from the configuration.
clear configure isakmp policy	Clears all ISAKMP policy configuration.
show running-config crypto	Displays the entire crypto configuration, including IPsec, crypto maps, dynamic crypto maps, and ISAKMP.

clear configure crypto ca trustpoint

To remove all trustpoints from the configuration, use the **clear configure crypto ca trustpoint** command in global configuration.

clear configure crypto ca trustpoint

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0	This command was introduced.

Examples

The following example entered in global configuration mode, removes all trustpoints from the configuration:

```
hostname(config)# clear configure crypto ca trustpoint
hostname(config)#
```

Related Commands

Command	Description
crypto ca trustpoint	Enters the trustpoint subconfiguration level for the indicated trustpoint.

clear configure crypto dynamic-map

To remove all or specified crypto dynamic maps from the configuration, use the **clear configure crypto dynamic-map** command in global configuration.

clear configure crypto dynamic-map *dynamic-map-name* *dynamic-seq-num*

Syntax Description

<i>dynamic-map-name</i>	Specifies the name of a specific crypto dynamic map.
<i>dynamic-seq-num</i>	Specifies the sequence number of the crypto dynamic map.

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		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	•	—	•	—	—

Command History

Release	Modification
7.0	This command was introduced.

Examples

The following example entered in global configuration mode, removes the crypto dynamic map mymaps with sequence number 3 from the configuration:

```
hostname(config)# clear configure crypto dynamic-map mymaps 3
hostname(config)#
```

Related Commands

Command	Description
clear configure crypto map	Clears the configuration of all or specified crypto maps.
show running-config crypto map	Displays all the active configuration for all dynamic crypto maps.
show running-config crypto map	Displays all the active configuration for all crypto maps.

clear configure crypto map

To remove all or specified crypto maps from the configuration, use the **clear configure crypto map** command in global configuration.

clear configure crypto map *map-name seq-num*

Syntax Description

<i>map-name</i>	Specifies the name of a specific crypto map.
<i>seq-num</i>	Specifies the sequence number of the crypto map.

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		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	•	—	•	—	—

Command History

Release	Modification
7.0	This command was introduced.

Examples

The following example entered in global configuration mode, removes the crypto map mymaps with sequence number 3 from the configuration:

```
hostname(config)# clear configure crypto map mymaps 3
hostname(config)#
```

Related Commands

Command	Description
clear configure crypto dynamic-map	Clears the configuration of all or specified crypto dynamic maps.
crypto map interface	Applies a crypto map to an interface.
show running-config crypto map	Displays the active configuration for all crypto maps.
	Displays the active configuration for all dynamic crypto maps.

clear configure dhcpd

To clear all of the DHCP server commands, binding, and statistics, use the **clear configure dhcpd** command in global configuration mode.

clear configure dhcpd

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values.

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

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

Release	Modification
7.0	This command was changed from clear dhcpd to clear configure dhcpd .

Usage Guidelines The **clear configure dhcpd** command clears all of the **dhcpd** commands, bindings, and statistical information. To clear only the statistic counters or binding information, use the **clear dhcpd** command.

Examples The following example shows how to clear all **dhcpd** commands:

```
hostname(config)# clear configure dhcpd
```

Related Commands	Command	Description
	clear dhcpd	Clears the DHCP server bindings and statistic counters.
	show running-config dhcpd	Displays the current DHCP server configuration.

clear configure dhcprelay

To clear all of the DHCP relay configuration, use the **clear configure dhcprelay** command in global configuration mode.

clear configure dhcprelay

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0	This command was changed from clear dhcprelay to clear configure dhcprelay .

Usage Guidelines

The **clear configure dhcprelay** command clears the DHCP relay statistics and configuration. To clear only the DHCP statistic counters, use the **clear dhcprelay statistics** command.

Examples

The following example shows how to clear the DHCP relay configuration:

```
hostname(config)# clear configure dhcprelay
```

Related Commands

Command	Description
clear dhcprelay statistics	Clears the DHCP relay agent statistic counters.
debug dhcprelay	Displays debug information for the DHCP relay agent.
show dhcprelay statistics	Displays DHCP relay agent statistic information.
show running-config dhcprelay	Displays the current DHCP relay agent configuration.

clear configure dns

To clear all DNS commands, use the **clear configure dns** command in global configuration mode.

clear configure dns

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values.

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

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

Command History	Release	Modification
	7.0	This command was introduced.

Examples The following example clears all DNS commands:

```
hostname(config)# clear configure dns
```

Related Commands	Command	Description
	show running-config dns-server-group	Shows the currently running DNS configuration.

clear configure established

To remove all established commands, use the **clear configure established** command in global configuration mode.

clear configure established

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values.

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

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

Release	Modification
7.0	The keyword configure was added.

Usage Guidelines To remove an established connection created by the **established** command, enter the **clear xlate** command.

Examples This example shows how to remove established commands:

```
hostname(config)# clear configure established
```

Command	Description
established	Permits return connections on ports that are based on an established connection.
show running-config established	Displays the allowed inbound connections that are based on established connections.
clear xlate	Clears the current translation and connection slot information.

clear configure failover

To remove **failover** commands from the configuration and restore the defaults, use the **clear configure failover** command in global configuration mode.

clear configure failover

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values.

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

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

Command History	Release	Modification
	7.0	Command was changed from clear failover to clear configure failover .

Usage Guidelines This command clears all **failover** commands from the running configuration and restores the defaults. If you use the **all** keyword with the **show running-config failover** command, you will see the default failover configuration.

The **clear configure failover** command is not available in a security context in multiple configuration mode; you must enter the command in the system execution space.

Examples The following example clears all failover commands from the configuration:

```
hostname(config)# clear configure failover
hostname(config)# show running-configuration failover
no failover
```

Related Commands	Command	Description
	show running-config failover	Displays the failover commands in the running configuration.

clear configure filter

To clear URL, FTP, and HTTPS filtering configuration, use the **clear configure filter** command in global configuration mode.

clear configure filter

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		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	•	•	•	•	•

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

The **clear configure filter** command clears the URL, FTP, and HTTPS filtering configuration.

Examples

The following example clears the URL, FTP, and HTTPS filtering configuration:

```
hostname# clear configure filter
```

Related Commands

Commands	Description
filter ftp	Identifies the FTP traffic to be filtered by a URL filtering server.
filter https	Identifies the HTTPS traffic to be filtered by a Websense server.
filter url	Directs traffic to a URL filtering server.
show running-config filter	Displays the filtering configuration.
url-server	Identifies an N2H2 or Websense server for use with the filter command.

clear configure fips

To clear the system or module FIPS configuration information stored in NVRAM, use the **clear configure fips** command.

clear configure fips

Syntax Description

fips FIPS-2 compliance information

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
Global configuration	—	—	•	—	—

Command History

Release	Modification
7.0(4)	This command was introduced.

Examples

```
sw8-ASA(config)# clear configure fips
```

Related Commands

Command	Description
crashinfo console disable	Disables the reading, writing and configuration of crash write info to flash.
fips enable	Enables or disablea policy-checking to enforce FIPS compliance on the system or module.
fips self-test poweron	Executes power-on self-tests.
show crashinfo console	Reads, writes, and configures crash write to flash.
show running-config fips	Displays the FIPS configuration that is running on the security appliance.

clear configure firewall

To set the firewall mode to the default routed mode, use the **clear configure firewall** command in global configuration mode.

clear configure firewall

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values.

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

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

Command History

Release	Modification
7.0	This command was introduced.

Examples The following example sets the firewall mode to the default:

```
hostname(config)# clear configure firewall
```

Related Commands

Command	Description
arp	Adds a static ARP entry.
firewall transparent	Sets the firewall mode to transparent.
show arp statistics	Shows ARP statistics.
show running-config arp	Shows the current configuration of the ARP timeout.

clear configure fixup

To clear the fixup configuration, use the **clear configure fixup** command in global configuration mode.

clear configure fixup

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		
	Routed	Transparent	Single	Multiple Context	System
Global configuration	•	•	•	•	•

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

The **clear configure fixup** command removes the fixup configuration.

Examples

The following example clears the fixup configuration:

```
hostname# clear configure fixup
```

Related Commands

Commands	Description
class-map	Defines the traffic class to which to apply security actions.
policy-map	Associates a class map with specific security actions.

clear configure fragment

To reset all the IP fragment reassembly configurations to defaults, use the **clear configure fragment** command in global configuration mode.

clear configure fragment [*interface*]

Syntax Description

interface (Optional) Specifies the security appliance interface.

Defaults

If an *interface* is not specified, the command applies to all interfaces.

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
Global configuration	•	•	•	•	—

Command History

Release	Modification
7.0	The configure keyword and optional <i>interface</i> argument were added. The command was also separated into two commands, clear fragment and clear configure fragment , to separate clearing of the configuration data from the operational data.

Usage Guidelines

The **clear configure fragment** command resets all the IP fragment reassembly configurations to defaults. In addition, the the **chain**, **size**, and **timeout** keywords are reset to their default values, which are as follows:

- **chain** is 24 packets
- **size** is 200
- **timeout** is 5 seconds

Examples

This example shows how to reset all the IP fragment reassembly configurations to defaults:

```
hostname(config)# clear configure fragment
```

Related Commands

Command	Description
clear fragment	Clears the operational data of the IP fragment reassembly module.
fragment	Provides additional management of packet fragmentation and improves compatibility with NFS.

Command	Description
show fragment	Displays the operational data of the IP fragment reassembly module.
show running-config fragment	Displays the IP fragment reassembly configuration.

clear configure ftp

To clear the FTP configuration, use the **clear configure ftp** command in global configuration mode.

clear configure ftp

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		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	•	•	•	•	•

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

The **clear configure ftp** command clears the FTP configuration.

Examples

The following example clears the FTP configuration:

```
hostname# clear configure filter
```

Related Commands

Commands	Description
filter ftp	Identifies the FTP traffic to be filtered by a URL filtering server.
filter https	Identifies the HTTPS traffic to be filtered by a Websense server.
filter url	Directs traffic to a URL filtering server.
show running-config filter	Displays the filtering configuration.
url-server	Identifies an N2H2 or Websense server for use with the filter command.

clear configure ftp-map

To clear the FTP map configuration, use the **clear configure ftp-map** command in global configuration mode.

clear configure ftp-map

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		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	•	•	•	•	•

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

The **clear configure ftp-map** command removes the FTP map configuration.

Examples

The following example clears the FTP map configuration:

```
hostname# clear configure ftp-map
```

Related Commands

Commands	Description
class-map	Defines the traffic class to which to apply security actions.
ftp-map	Defines an FTP map and enables FTP map configuration mode.
inspect ftp	Applies a specific FTP map to use for application inspection.
request-command deny	Specifies FTP commands to disallow.

clear configure global

To remove the **global** commands from the configuration, use the **clear configure global** command in global configuration mode.

clear configure global

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values.

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

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

Release	Modification
7.0	Added keyword configure .

Command History

Examples The following example shows how to remove the **global** commands from the configuration:

```
hostname(config)# clear configure global
```

Command	Description
global	Creates entries from a pool of global addresses.
show running-config global	Displays the global commands in the configuration.

Related Commands

clear configure group-policy

To remove the configuration for a particular group policy, use the **clear configure group-policy** command in global configuration mode, and append the name of the group policy. To remove all group-policy commands from the configuration except the default group policy, use this command without arguments.

clear configure group-policy [*name*]

Syntax Description

<i>name</i>	Specifies the name of the group policy.
-------------	---

Defaults

Remove all group-policy commands from the configuration, except the default group policy.

Command Modes

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

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
Global configuration	•	—	•	—	—

Command History

Release	Modification
7.0	This command was introduced.

Examples

The following example shows how to clear the configuration for the group policy named FirstGroup.

```
hostname(config)# clear configure group-policy FirstGroup
```

Related Commands

Command	Description
group-policy	Creates, edits, or removes a group policy.
group-policy attributes	Enters group-policy attributes mode, which lets you configure AVPs for a specified group policy.
show running-config group-policy	Displays the running configuration for a particular group policy or for all group policies.

clear configure gtp-map

To clear GTP map configuration, use the **clear configure gtp-map** command in global configuration mode.

clear configure gtp-map

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		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	•	•	•	•	•

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

The **clear configure gtp-map** command removes the GTP map configuration.

Examples

The following example clears GTP map configuration:

```
hostname# clear configure gtp-map
```

Related Commands

Commands	Description
clear service-policy inspect gtp	Clears global GTP statistics.
debug gtp	Displays detailed information about GTP inspection.
gtp-map	Defines a GTP map and enables GTP map configuration mode.
inspect gtp	Applies a specific GTP map to use for application inspection.
show service-policy inspect gtp	Displays the GTP configuration.

clear configure http

To disable the HTTP server and to remove configured hosts that can access the HTTP server, use the **clear configure http** command in global configuration mode.

clear configure http

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		
	Routed	Transparent	Single	Multiple Context	System
Global configuration	•	—	•	—	—

Command History

Release	Modification
7.0	This command was introduced.

Examples

The following example shows how to clear the HTTP configuration.

```
hostname(config)# clear configure http
```

Related Commands

Command	Description
http	Specifies hosts that can access the HTTP server by IP address and subnet mask. Specifies the security appliance interface through which the host accesses the HTTP server.
http authentication-certificate	Requires authentication via certificate from users who are establishing HTTPS connections to the security appliance.
http redirect	Specifies that the security appliance redirect HTTP connections to HTTPS.
http server enable	Enables the HTTP server.
show running-config http	Displays the hosts that can access the HTTP server, and whether or not the HTTP server is enabled.

clear configure http-map

To clear HTTP map configuration, use the **clear configure http-map** command in global configuration mode.

clear configure http-map

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		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	•	•	•	•	•

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

The **clear configure http-map** command removes the HTTP map configuration.

Examples

The following example clears the HTTP map configuration:

```
hostname# clear configure http-map
```

Related Commands

Commands	Description
class-map	Defines the traffic class to which to apply security actions.
debug http-map	Displays detailed information about traffic associated with an HTTP map.
http-map	Defines an HTTP map for configuring enhanced HTTP inspection.
inspect http	Applies a specific HTTP map to use for application inspection.
policy-map	Associates a class map with specific security actions.

clear configure icmp

To clear the configured access rules for ICMP traffic, use the **clear configure icmp** command in global configuration mode.

clear configure icmp

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		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	•	•	•	•	•

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

The **clear configure icmp** command clears the configured access rules for ICMP traffic.

Examples

The following example clears the clear configured access rules for ICMP traffic:

```
hostname# clear configure icmp
```

Related Commands

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

clear configure imap4s

To remove all IMAP4S commands from the configuration, reverting to default values, use the **clear configure imap4s** command in global configuration mode.

clear configure imap4s

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values.

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

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

Release	Modification
7.0	This command was introduced.

Examples The following example shows how to remove the IMAP4S configuration:

```
hostname(config)# clear configure imap4s
hostname(config)#
```

Command	Description
show running-config imap4s	Displays the running configuration for IMAP4S.
imap4s	Creates or edits an IMAP4S e-mail proxy configuration.

clear configure interface

To clear the interface configuration, use the **clear configure interface** command in global configuration mode.

clear configure interface [*physical_interface*[*.subinterface*] | *mapped_name* | *interface_name*]

Syntax Description

<i>interface_name</i>	(Optional) Identifies the interface name set with the nameif command.
<i>mapped_name</i>	(Optional) In multiple context mode, identifies the mapped name if it was assigned using the allocate-interface command.
<i>physical_interface</i>	(Optional) Identifies the interface ID, such as gigabitethernet0/1 . See the interface command for accepted values.
<i>subinterface</i>	(Optional) Identifies an integer between 1 and 4294967293 designating a logical subinterface.

Defaults

If you do not specify an interface, the security appliance clears all interface configuration.

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
Global configuration	•	•	•	•	•

Command History

Release	Modification
7.0	This command was changed from clear interface . This command was also modified to include the new interface numbering scheme.

Usage Guidelines

When you clear the interface configuration for main physical interfaces, the security appliance uses the default settings.

You cannot use the interface name in the system execution space, because the **nameif** command is only available within a context. Similarly, if you mapped the interface ID to a mapped name using the **allocate-interface** command, you can only use the mapped name in a context.

Examples

The following example clears the GigabitEthernet0/1 configuration:

```
hostname(config)# clear configure interface gigabitethernet0/1
```

The following example clears the inside interface configuration:

```
hostname(config)# clear configure interface inside
```

The following example clears the int1 interface configuration in a context. “int1” is a mapped name.

```
hostname/contexta(config)# clear configure interface int1
```

The following example clears all interface configuration.

```
hostname(config)# clear configure interface
```

Related Commands

Command	Description
allocate-interface	Assigns interfaces and subinterfaces to a security context.
clear interface	Clears counters for the show interface command.
interface	Configures an interface and enters interface configuration mode.
show interface	Displays the runtime status and statistics of interfaces.

clear configure ip

To clear all IP addresses set by the **ip address** command, use the **clear configure ip** command in global configuration mode.

clear configure ip

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
1.1(1)	Support for this command was introduced.

Usage Guidelines

In transparent firewall mode, this command clears the management IP address.

If you want to stop all current connections that use the old IP addresses, enter the **clear xlate** command. Otherwise, the connections time out as usual.

Examples

The following example clears all IP addresses:

```
hostname(config)# clear configure ip
```

Related Commands

Command	Description
allocate-interface	Assigns interfaces and subinterfaces to a security context.
clear configure interface	Clears all configuration for an interface.
interface	Configures an interface and enters interface configuration mode.
ip address	Sets the IP address for the interface.
show running-config interface	Displays the interface configuration.

clear configure ip audit

To clear the entire audit policy configuration, use the **clear configure ip audit** command in global configuration mode.

clear configure ip audit [**configuration**]

Syntax Description

configuration (Optional) You can enter this keyword, but the effect is the same without it.

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		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
7.0	This command was changed from clear ip audit .

Examples

The following example clears all **ip audit** commands:

```
hostname# clear configure ip audit
```

Related Commands

Command	Description
ip audit attack	Sets the default actions for packets that match an attack signature.
ip audit info	Sets the default actions for packets that match an informational signature.
ip audit interface	Assigns an audit policy to an interface.
ip audit name	Creates a named audit policy that identifies the actions to take when a packet matches an attack signature or an informational signature.
ip audit signature	Disables a signature.

clear configure ip local pool

To remove IP address pools, use the **clear configure ip local pool** command in global configuration mode.

clear ip local pool [*poolname*]

Syntax Description

poolname (Optional) Specifies the name of the IP address pool.

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		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	•	—	•	—	—

Command History

Release	Modification
7.0	This command was introduced.

Examples

The following example removes all IP address pools from the running configuration:

```
hostname(config)# clear config ip local pool
hostname(config)#
```

Related Commands

Command	Description
clear configure ip local pool	Removes all ip local pools.
ip local pool	Configures an IP address pool.

clear configure ip verify reverse-path

To clear the **ip verify reverse-path** configuration, use the **clear configure ip verify reverse-path** command in global configuration mode.

clear configure ip verify reverse-path

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0	This command was changed from clear ip verify reverse-path .

Examples

The following example clears the **ip verify reverse-path** configuration for all interfaces:

```
hostname(config)# clear configure ip verify reverse-path
```

Related Commands

Command	Description
clear ip verify statistics	Clears the Unicast RPF statistics.
ip verify reverse-path	Enables the Unicast Reverse Path Forwarding feature to prevent IP spoofing.
show ip verify statistics	Shows the Unicast RPF statistics.
show running-config ip verify reverse-path	Shows the ip verify reverse-path configuration.

clear configure ipv6

To clear the global IPv6 commands from the running configuration, use the **clear configure ipv6** command in global configuration mode.

clear configure ipv6 [**route** | **access-list**]

Syntax Description	route	(Optional) Clears the commands that statically define routes in the IPv6 routing table from the running configuration.
	access-list	(Optional) Clears the IPv6 access list commands from the running configuration.

Defaults Without keywords, this command clears all IPv6 commands from the running configuration.

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
Global configuration	•	—	•	•	—

Command History	Release	Modification
	7.0	This command was introduced.

Usage Guidelines This command only clears the global IPv6 commands from the running configuration; it does not clear the IPv6 commands entered in interface configuration mode.

Examples The following example shows how to clear statically defined IPv6 routes from the IPv6 routing table:

```
hostname(config)# clear configure ipv6 route
hostname(config)#
```

Related Commands	Command	Description
	ipv6 route	Defines a static route in the IPv6 routing table.
	show ipv6 route	Displays the contents of the IPv6 routing table.
	show running-config ipv6	Displays the IPv6 commands in the running configuration.

clear configure isakmp

To remove all of the ISAKMP configuration, use the **clear configure isakmp** command in global configuration mode.

clear configure isakmp

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values.

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

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

Release	Modification
7.0	This command was introduced.

Command History

Examples The following example issued in global configuration mode, removes all of the ISAKMP configuration from the security appliance:

```
hostname(config)# clear configure isakmp
hostname(config)#
```

Related Commands	Command	Description
	clear configure isakmp policy	Clears all ISAKMP policy configuration.
	isakmp enable	Enables ISAKMP negotiation on the interface on which the IPSec peer communicates with the security appliance.
	show isakmp stats	Displays runtime statistics.
	show isakmp sa	Displays IKE runtime SA database with additional information.
	show running-config isakmp	Displays all the active configuration.

clear configure isakmp policy

To remove all of the ISAKMP policy configuration, use the **clear configure isakmp policy** command in global configuration mode.

clear configure isakmp policy *priority*

Syntax Description

priority Specifies the priority of the ISAKMP priority to be cleared.

Defaults

No default behaviour or values.

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
Global configuration	•	—	•	—	—

Command History

Release	Modification
7.0	This command was introduced.

Examples

The following example removes the ISAKMP policy with priority 3 from the configuration:

```
hostname(config)# clear configure isakmp policy 3
hostname(config)#
```

Related Commands

Command	Description
isakmp enable	Enables ISAKMP negotiation on the interface on which the IPSec peer communicates with the security appliance.
show isakmp stats	Displays runtime statistics.
show isakmp sa	Displays IKE runtime SA database with additional information.
show running-config isakmp	Displays all the active configuration.

clear configure logging

To clear the logging configuration, use the **clear configure logging** command in global configuration mode.

clear configure logging [**disabled** | **level** | **rate-limit**]

Syntax Description

disabled	(Optional) Indicates that all disabled system log messages should be re-enabled. When you use this option, no other logging configuration is cleared.
level	(Optional) Indicates that the severity level assignments for system log messages should be reset to their default values. When you use this option, no other logging configuration is cleared.
rate-limit	(Optional) Resets the logging rate limit.

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		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	•	•	•	•	•

Command History

Release	Modification
7.0	This command was introduced.
7.0(4)	The rate-limit keyword was introduced.

Usage Guidelines

You can use the **show running-config logging** command to view all logging configuration. If you use the **clear configure logging** command without either the **disabled** or **level** keyword, all logging configuration is cleared.

Examples

The following example shows how to clear logging configuration. The output of the **show logging** command indicates that all logging features are disabled.

```
hostname(config)# clear configure logging
hostname(config)# show logging
Syslog logging: disabled
  Facility: 20
  Timestamp logging: disabled
  Standby logging: disabled
  Deny Conn when Queue Full: disabled
  Console logging: disabled
  Monitor logging: disabled
```

```
Buffer logging: disabled
Trap logging: disabled
History logging: disabled
Device ID: disabled
Mail logging: disabled
ASDM logging: disabled
```

Related Commands

Command	Description
show logging	Displays the enabled logging options.
show running-config logging	Displays the logging-related portion of the running configuration.

clear configure mac-address-table

To clear the **mac-address-table static** and **mac-address-table aging-time** configuration, use the **clear configure mac-address-table** command in global configuration mode.

clear configure mac-address-table

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values.

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

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

Release	Modification
7.0	This command was introduced.

Examples The following example clears the **mac-address-table static** and **mac-address-table aging-time** configuration:

```
hostname# clear configure mac-address-table
```

Related Commands	Command	Description
	firewall transparent	Sets the firewall mode to transparent.
	mac-address-table aging-time	Sets the timeout for dynamic MAC address entries.
	mac-address-table static	Adds static MAC address entries to the MAC address table.
	mac-learn	Disables MAC address learning for an interface.
	show mac-address-table	Shows the MAC address table, including dynamic and static entries.

clear configure mac-learn

To clear the **mac-learn** configuration, use the **clear configure mac-learn** command in global configuration mode.

clear configure mac-learn

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values.

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

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

Command History

Release	Modification
7.0	This command was introduced.

Examples The following example clears the **mac-learn** configuration:

```
hostname# clear configure mac-learn
```

Related Commands	Command	Description
	firewall transparent	Sets the firewall mode to transparent.
	mac-address-table static	Adds static MAC address entries to the MAC address table.
	mac-learn	Disables MAC address learning for an interface.
	show mac-address-table	Shows the MAC address table, including dynamic and static entries.

clear configure mac-list

To remove the indicated list of MAC addresses, previously specified the **mac-list** command, use the **clear configure mac-list** command in global configuration mode:

```
clear configure mac-list id
```

Syntax Description

id A MAC address list name.

Defaults

No default behaviors or values.

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
Global configuration	•	•	—	—	•

Command History

Release	Modification
7.0	This command was modified to conform with CLI standards.

Usage Guidelines

To remove a list of MAC addresses, use the **clear mac-list** command.

Examples

The following example shows how to clear a MAC address list:

```
hostname(config)# clear configure mac-list firstmaclist
```

Related Commands

Command	Description
mac-list	Adds a list of MAC addresses using a first-match search.
show running-config mac-list	Displays the MAC addresses in the MAC address list indicated by the <i>id</i> value.

clear configure management-access

To remove the configuration of an internal interface for management access of the security appliance, use the **clear configure management-access** command in global configuration mode.

clear configure management-access

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0	The keyword configure was added.

Usage Guidelines

The **management-access** command lets you define an internal management interface using the IP address of the firewall interface specified in *mgmt_if*. (The interface names are defined by the **nameif** command and displayed in quotes, “”, in the output of the **show interface** command.) The **clear configure management-access** command removes the configuration of the internal management interface specified with the **management-access** command.

Examples

The following example removes the configuration of an internal interface for management access of the security appliance:

```
hostname(config)# clear configure management-access
```

Related Commands

Command	Description
management-access	Configures an internal interface for management access.
show running-config management-access	Displays the name of the internal interface configured for management access.

clear configure mgcp-map

To clear the MGCP map configuration, use the **clear configure mgcp-map** command in global configuration mode.

clear configure mgcp-map

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		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	•	•	•	•	•

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

The **clear configure mgcp-map** clears the MGCP map configuration.

Examples

The following example clears clear the MGCP map configuration:

```
hostname# clear configure mgcp-map
```

Related Commands

Commands	Description
debug mgcp	Enables MGCP debug information.
mgcp-map	Defines an MGCP map and enables MGCP map configuration mode.
show conn	Displays the connection state for different connection types.
show mgcp	Displays information about MGCP sessions established through the security appliance.
timeout	Sets the maximum idle time duration for different protocols and session types.

clear configure mroute

To remove the **mroute** commands from the running configuration, use the **clear configure mroute** command in global configuration mode.

clear configure mroute

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0	This command was introduced.

Examples

The following example shows how to remove the **mroute** commands from the configuration:

```
hostname(config)# clear configure mroute
hostname(config)#
```

Related Commands

Command	Description
mroute	Configures a static multicast route.
show mroute	Displays IPv4 multicast routing table.
show running-config mroute	Displays the mroute commands in the running configuration.

clear configure mtu

To clear the configured maximum transmission unit values on all interfaces, use the **clear configure mtu** command in global configuration mode.

clear configure mtu

Syntax Description

This command has no arguments or keywords.

Defaults

Using the **clear configure mtu command** sets the maximum transmission unit to the default of 1500 for all ethernet interfaces.

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
Global configuration	—	•	•	•	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Examples

The following example clears the current maximum transmission unit values on all interfaces:

```
hostname(config)# clear configure mtu
```

Related Commands

Command	Description
mtu	Specifies the maximum transmission unit for an interface.
show running-config mtu	Displays the current maximum transmission unit block size.

clear configure multicast-routing

To remove the **multicast-routing** command from the running configuration, use the **clear configure multicast-routing** command in global configuration mode.

clear configure multicast-routing

Syntax Description

There are no keywords or arguments for this command.

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		
	Routed	Transparent	Single	Multiple Context	System
Global configuration	•	—	•	—	—

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

The **clear configure multicast-routing** command removes the **multicast-routing** from the running configuration. The **no multicast-routing** command also removes the multicast-routing command from the running configuration.

Examples

The following example shows how to remove the **multicast-routing** command from the running configuration:

```
hostname(config)# clear configure multicast-routing
```

Related Commands

Command	Description
multicast-routing	Enables multicast routing on the security appliance.

clear configure name

To clear the list of names from the configuration, use the **clear configure name** command in global configuration mode.

clear configure name

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values.

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

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

Release	Modification
7.0	The keyword configure was added.

Usage Guidelines This command has no usage guidelines.

Examples The following example shows how to clear the name list:

```
hostname(config)# clear configure name
```

Command	Description
name	Associates a name with an IP address.
show running-config name	Displays the list of names associated with IP addresses.

clear configure nat

To remove the NAT configuration, use the **clear configure nat** command in privileged EXEC mode.

clear configure nat

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0	Added keyword configure .

Usage Guidelines

The following applies to transparent firewall mode:



Note

In transparent firewall mode, only NAT id 0 is valid.

Examples

The following example shows how to remove the NAT configuration:

```
hostname(config)# clear configure nat
```

Related Commands

Command	Description
nat	Associates a network with a pool of global IP addresses.
show running-config nat	Displays a pool of global IP addresses that are associated with the network.

clear configure ntp

To clear the NTP configuration, use the **clear configure ntp** command in global configuration mode.

clear configure ntp

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values.

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

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

Release	Modification
7.0	This command was changed from clear ntp .

Command History

Examples The following example clears all **ntp** commands:

```
hostname# clear configure ntp
```

Command	Description
ntp authenticate	Enables NTP authentication.
ntp authentication-key	Sets the NTP authentication key.
ntp server	Identifies an NTP server to set the time on the security appliance.
ntp trusted-key	Specifies the NTP trusted key.
show running-config ntp	Shows the NTP configuration.

Related Commands

clear configure object-group

To remove all the **object group** commands from the configuration, use the **clear configure object-group** command in global configuration mode.

clear configure object-group [{**protocol** | **service** | **icmp-type** | **network**}]

Syntax Description

icmp-type	(Optional) Clears all ICMP groups.
network	(Optional) Clears all network groups.
protocol	(Optional) Clears all protocol groups.
service	(Optional) Clears all service groups.

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
Preexisting	This command was preexisting.

Examples

The following example shows how to remove all the **object-group** commands from the configuration:

```
hostname(config)# clear configure object-group
```

Related Commands

Command	Description
group-object	Adds network object groups.
network-object	Adds a network object to a network object group.
object-group	Defines object groups to optimize your configuration.
port-object	Adds a port object to a service object group.
show running-config object-group	Displays the current object groups.

clear configure passwd

To clear the login password configuration and restore the default setting of “cisco,” use the **clear configure passwd** command in global configuration mode.

clear configure {passwd | password}

Syntax Description

passwd | password You can enter either command; they are aliased to each other.

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		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	•	•	•	•	•

Command History

Release	Modification
7.0	This command was changed from clear passwd .

Examples

The following example clears the login password and restores it to the default of “cisco”:

```
hostname(config)# clear configure passwd
```

Related Commands

Command	Description
enable	Enters privileged EXEC mode.
enable password	Sets the enable password.
passwd	Sets the login 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.

clear configure pim

To clear all of the global **pim** commands from the running configuration, use the **clear configure pim** command in global configuration mode.

clear configure pim

Syntax Description

There are no keywords or arguments for this command.

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		
	Routed	Transparent	Single	Multiple Context	System
Global configuration	•	—	•	—	—

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

The **clear configure pim** command clears all of the **pim** commands from the running configuration. To clear PIM traffic counters and topology information, use the **clear pim counters** and the **clear pim topology** commands.

The **clear configure pim** command only clears the **pim** commands entered in global configuration mode; it does not clear the interface-specific **pim** commands.

Examples

The following example shows how to clear all **pim** commands from the running configuration:

```
hostname(config)# clear configure pim
```

Related Commands

Command	Description
clear pim topology	Clears the PIM topology table.
clear pim counters	Clears the PIM traffic counters.
show running-config pim	Displays the pim commands in the running configuration.

clear configure policy-map

To remove the policy-map specification from the configuration, use the **clear configure policy-map** command in global configuration mode.

clear configure policy-map

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0	This command was introduced.

Examples

This example shows the **clear configure policy-map** command:

```
hostname(config)# clear configure policy-map
```

Related Commands

Command	Description
policy-map	Configures a policy; that is, an association of a traffic class and one or more actions.
show running-config policy-map	Displays the entire policy configuration.

clear configure pop3s

To remove all POP3S commands from the configuration, reverting to default values, use the **clear configure pop3s** command in global configuration mode.

clear configure pop3s

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values.

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

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

Command History	Release	Modification
	7.0	This command was introduced.

Examples The following example shows how to remove the POP3S configuration:

```
hostname(config)# clear configure pop3s
hostname(config)#
```

Related Commands	Command	Description
	show running-config pop3s	Displays the running configuration for POP3S.
	pop3s	Creates or edits a POP3S e-mail proxy configuration.

clear configure port-forward

To remove a configured set of applications that WebVPN users access over forwarded TCP ports, use the **clear configure port-forward** command in global configuration mode. To remove all configured applications, use this command without the *listname* argument. To remove only the applications for a specific list, use this command with that *listname*.

clear configure port-forward [*listname*]

Syntax Description

<i>listname</i>	Groups the set of applications (forwarded TCP ports) WebVPN users can access. Maximum 64 characters.
-----------------	--

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
Global configuration	•	—	•	—	—

Command History

Release	Modification
7.0	This command was introduced.

Examples

The following example shows how to remove the portforwarding list called *SalesGroupPorts*.

```
hostname(config)# clear configure port-forward SalesGroupPorts
```

Related Commands

Command	Description
port-forward	Use this command in webvpn configuration mode to configure the set of applications that WebVPN users can access.
port-forward	Use this command in webvpn mode to enable WebVPN application access for a user or group policy.
show running-configuration port-forward	Displays the current set of configured port-forward commands.

clear configure prefix-list

To remove the **prefix-list** commands from the running configuration, use the **clear configure prefix-list** command in global configuration mode.

clear configure prefix-list [*prefix-list-name*]

Syntax Description

prefix-list-name (Optional) The name of a prefix list. When a prefix list name is specified, only the commands for that prefix list are removed from the configuration.

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		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	•	—	•	—	—

Command History

Release	Modification
7.0	This command was changed from clear prefix-list to clear configure prefix-list .

Usage Guidelines

The **clear configure prefix-list** command removes the **prefix-list** commands and the **prefix-list description** commands from the running configuration. If a prefix list name is specified, then the **prefix-list** command and **prefix-list description** command, if present, for that prefix list only are removed from the running configuration.

This command does not remove the **no prefix-list sequence** command from the running configuration.

Examples

The following example removes all **prefix-list** commands from the running configuration for a prefix list named MyPrefixList:

```
hostname# clear configure prefix-list MyPrefixList
```

Related Commands

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

clear configure priority-queue

To remove the priority queue specification from the configuration, use the **clear configure priority-queue** command in global configuration mode.

clear configure priority queue *interface-name*

Syntax Description

<i>interface-name</i>	Specifies the name of the interface for which you want to show the priority queue details
-----------------------	---

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0	This command was introduced.

Examples

This example shows the use of the **clear configure priority-queue** command to remove the priority-queue configuration on the interface named test:

```
hostname(config)# clear configure priority-queue test
```

Related Commands

Command	Description
priority-queue	Configures priority queueing on an interface.
show running-config priority-queue	Displays the current priority-queue configuration for the named interface.

clear configure privilege

To remove the configured privilege levels for commands, use the **clear configure privilege** command in global configuration mode.

clear configure privilege

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values.

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

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

Command History	Release	Modification
	7.0	This command was modified to conform to CLI guidelines.

Usage Guidelines There is no undo.

Examples This example shows how to reset the configured privilege levels for the commands:

```
hostname(config)# clear configure privilege
```

Related Commands	Command	Description
	privilege	Configures the command privilege levels.
	show curpriv	Displays current privilege level
	show running-config privilege	Displays privilege levels for commands.

clear configure rip

To clear the **rip** commands from the running configuration, use the **clear configure rip** command in global configuration mode.

clear configure rip

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0	This command was changed from clear rip to clear configure rip .

Usage Guidelines

The **clear configure rip** command removes all **rip** commands from the configuration. Use the **no** form of the commands to clear specific commands.

Examples

The following example clears all RIP commands from the running configuration:

```
hostname(config)# clear configure rip
```

Related Commands

Command	Description
debug rip	Displays debug information for RIP.
rip	Configures RIP on the specified interface.
show running-config rip	Displays the RIP commands in the running configuration.

clear configure route

To remove the **route** commands from the configuration that do not contain the **connect** keyword, use the **clear configure route** command in global configuration mode.

clear configure route [*interface_name* *ip_address* [*netmask* *gateway_ip*]]

Syntax Description

<i>gateway_ip</i>	(Optional) Specifies the IP address of the gateway router (the next hop address for this route).
<i>interface_name</i>	(Optional) Internal or external network interface name.
<i>ip_address</i>	(Optional) Internal or external network IP address.
<i>netmask</i>	(Optional) Specifies a network mask to apply to the <i>ip_address</i> .

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		
	Routed	Transparent	Single	Multiple Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
7.0	Added keyword configure .

Usage Guidelines

Use **0.0.0.0** to specify a default route. You can abbreviate the 0.0.0.0 IP address as **0** and the 0.0.0.0 *netmask* as **0**.

Examples

The following example shows how to remove the **route** commands from the configuration that do not contain the **connect** keyword:

```
hostname(config)# clear configure route
```

Related Commands

Command	Description
route	Specifies a static or default route for the an interface.
show route	Displays route information.
show running-config route	Displays configured routes.

clear configure route-map

To remove all of the route maps, use the **clear configure route-map** command in global configuration mode.

clear configure route-map

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

Use the **clear configure route-map** command in global configuration mode to remove all **route-map** commands in the configuration. The **route-map** command is used to configure conditions of redistributing the routes from one routing protocol into another routing protocol.

To remove individual **route-map** commands, use the **no route-map** command.

Examples

The following example shows how to remove the conditions of redistributing routes from one routing protocol into another routing protocol:

```
hostname(config)# clear configure route-map
```

Related Commands

Command	Description
route-map	Defines the conditions for redistributing routes from one routing protocol into another.
show running-config route-map	Displays the information about the route map configuration.

clear configure router

To clear all router commands from the running configuration, use the **clear configure router** command in global configuration mode.

clear configure router [*ospf id*]

Syntax Description

<i>id</i>	The OSPF process ID.
ospf	Specifies that only OSPF commands are removed from the configuration.

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		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	•	—	•	—	—

Command History

Release	Modification
7.0	This command was changed from the clear router command to the clear configure router command.

Examples

The following example clears all OSPF commands associated with OSPF process 1 from the running configuration:

```
hostname(config)# clear configure router ospf 1
hostname(config)#
```

Related Commands

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

clear configure service-policy

To clear the service policy configuration for enabled policies, use the **clear configure service-policy** command in privileged EXEC mode.

clear configure service-policy

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		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	•	•	•	•	•

Command History

Release	Modification
PIX Version 7.0	This command was introduced.

Examples

The following is an example of the **clear service-policy** command:

```
hostname(config)# clear configure service-policy
```

Related Commands

Command	Description
show service-policy	Displays the service policy.
show running-config service-policy	Displays the service policies configured in the running configuration.
service-policy	Configures the service policy.
clear service-policy	Clears service policy statistics.

clear configure smtps

To remove all SMTPS commands from the configuration, reverting to default values, use the **clear configure smtps** command in global configuration mode.

clear configure smtps

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values.

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

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

Command History	Release	Modification
	7.0	This command was introduced.

Examples The following example shows how to remove the SMTPS configuration:

```
hostname(config)# clear configure smtps
hostname(config)#
```

Related Commands	Command	Description
	show running-configuration smtps	Displays the running configuration for SMTPS.
	smtps	Creates or edits an SMTPS e-mail proxy configuration

clear configure snmp-map

To clear the SNMP map configuration, use the **clear configure snmp-map** command in global configuration mode.

clear configure snmp-map

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		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	•	•	•	•	•

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

The **clear configure snmp-map** command removes the SNMP map configuration.

Examples

The following example clears the SNMP map configuration:

```
hostname# clear configure snmp-map
```

Related Commands

Commands	Description
class-map	Defines the traffic class to which to apply security actions.
deny version	Disallows traffic using a specific version of SNMP.
inspect snmp	Enable SNMP application inspection.
snmp-map	Defines an SNMP map and enables SNMP map configuration mode.

clear configure snmp-server

To disable the Simple Network Management Protocol (SNMP) server, use the **clear configure snmp-server** command in global configuration mode.

clear configure snmp-server

Syntax Description

This command has no arguments or keywords.

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
Global configuration	•	•	•	•	•

Command History

Release	Modification
7.0	Support for this command was introduced on the security appliance.

Examples

This example shows how to disable the SNMP server:

```
hostname #clear snmp-server
```

Related Commands

Command	Description
snmp-server	Provides the security appliance event information through SNMP.
show snmp-server statistics	Displays information about the SNMP server configuration.

clear configure ssh

To clear all SSH commands from the running configuration, use the **clear configure ssh** command in global configuration mode.

clear configure ssh

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values.

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

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

Release	Modification
7.0	This command was changed from the clear ssh command to the clear configure ssh command.

Usage Guidelines This command clears all SSH commands from the configuration. To clear specific commands, use the **no** form of those commands.

Examples The following example clears all SSH commands from the configuration:

```
hostname(config)# clear configure ssh
```

Command	Description
show running-config ssh	Displays the current SSH commands in the running configuration.
ssh	Allows SSH connectivity to the security appliance from the specified client or network.
ssh scopy enable	Enables a secure copy server on the security appliance.
ssh timeout	Sets the timeout value for idle SSH sessions.
ssh version	Restricts the security appliance to using either SSH Version 1 or SSH Version 2.

clear configure ssl

To remove all SSL commands from the configuration, reverting to default values, use the **clear config ssl** command in global configuration mode.

clear config ssl

Defaults

By default:

- Both the SSL client and SSL server versions are **any**.
- SSL encryption is 3des-sha1 | des-sha1 | rc4-md5, in that order.
- There is no trust point association; the security appliance uses the default RSA key-pair certificate.

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
Global configuration	•	•	•	•	•

Command History

Release	Modification
7.0	This command was introduced.

Examples

The following example shows how to use the **clear config ssl** command:

```
hostname(config)# clear config ssl
```

Related Commands

Command	Description
show running-config ssl	Displays the current set of configured ssl commands.
ssl client-version	Specifies the SSL/TLS protocol version the security appliance uses when acting as a client.
ssl server-version	Specifies the SSL/TLS protocol version the security appliance uses when acting as a server
ssl trust-point	Specifies the certificate trust point that represents the SSL certificate for an interface

clear configure static

To remove all the **static** commands from the configuration, use the **clear configure static** command in global configuration mode.

clear configure static

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values.

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

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

Release	Modification
7.0	The keyword configure was added.

Command History

Examples This example shows how to remove all the **static** commands from the configuration:

```
hostname(config)# clear configure static
```

Command	Description
show running-config static	Displays all static commands in the configuration.
static	Configures a persistent one-to-one address translation rule by mapping a local IP address to a global IP address.

Related Commands

clear configure sunrpc-server

To clear the remote processor call services from the security appliance, use the **clear configure sunrpc-server** command in global configuration mode.

clear configure sunrpc-server [**active**]

Syntax Description	active (Optional) Identifies the SunRPC services that are currently active on the security appliance.
---------------------------	--

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		
	Routed	Transparent	Single	Multiple Context	System
Global configuration	•	•	•	•	•

Command History	Release	Modification
	Preexisting	This command was preexisting.

Usage Guidelines	The sunrpc-server command displays the configured router ospf commands.
-------------------------	---



Note

If the highest-level IP address on the security appliance is a private address, this address is sent in hello packets and database definitions. To prevent this action, set the **router-id** *ip_address* to a global address.

Examples	The following example shows how to clear the SunRPC services from the security appliance: hostname(config)# clear configure sunrpc-server active
-----------------	--

Related Commands	Command	Description
	sunrpc-server	Creates the SunRPC services table.
	show running-config sunrpc-server	Displays the information about the SunRPC configuration.

clear configure sysopt

To clear the configuration for all **sysopt** commands, use the **clear configure sysopt** command in global configuration mode.

clear configure sysopt

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0	This command was changed from clear sysopt .

Examples

The following example clears all **sysopt** command configuration:

```
hostname(config)# clear configure sysopt
```

Related Commands

Command	Description
show running-config sysopt	Shows the sysopt command configuration.
sysopt connection permit-ipsec	Permits any packets that come from an IPSec tunnel without checking any ACLs for interfaces.
sysopt connection tcpmss	Overrides the maximum TCP segment size or ensures that the maximum is not less than a specified size.
sysopt connection timewait	Forces each TCP connection to linger in a shortened TIME_WAIT state after the final normal TCP close-down sequence.
sysopt nodnsalias	Disables alteration of the DNS A record address when you use the alias command.

clear configure tcp-map

To clear tcp-map configuration, use the **clear configure tcp-map** command in global configuration mode.

clear configure tcp-map

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values.

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

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

Command History	Release	Modification
	7.0	This command was introduced.

Examples The following example shows how to clear the TCP map configuration:

```
hostname(config)# clear configure tcp-map
```

Related Commands	Command	Description
	tcp-map	Creates a TCP map and allows access to tcp-map configuration mode.
	show running-config tcp-map	Displays the information about the TCP map configuration.

clear configure telnet

To remove the Telnet connection and idle timeout from the configuration, use the **clear configure telnet** command in global configuration mode.

clear configure telnet

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values.

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

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

Release	Modification
7.0	The keyword configure was added.

Examples This example shows how to remove the Telnet connection and the idle timeout from the security appliance configuration:

```
hostname(config)# clear configure telnet
```

Related Commands	Command	Description
	show running-config telnet	Displays the current list of IP addresses that are authorized to use Telnet connections to the security appliance.
	telnet	Adds Telnet access to the console and sets the idle timeout.

clear configure terminal

To clear the terminal display width setting, use the **clear configure terminal** command in global configuration mode.

clear configure terminal

Syntax Description This command has no keywords or arguments.

Defaults The default display width is 80 columns.

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
Global configuration	•	•	•	•	•

Command History	Release	Modification
	7.0	The configure keyword was added.

Examples The following example clears the display width:

```
hostname# clear configure terminal
```

Related Commands	Command	Description
	terminal	Sets the terminal line parameters.
	terminal width	Sets the terminal display width.
	show running-config terminal	Displays the current terminal settings.

clear configure timeout

To restore the default idle time durations in the configuration, use the **clear configure timeout** command in global configuration mode.

clear configure timeout

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values.

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

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

Release	Modification
Preexisting	This command was preexisting.

Examples This example shows how to remove the maximum idle time durations from the configuration:

```
hostname(config)# clear configure timeout
```

Command	Description
show running-config timeout	Displays the timeout value of the designated protocol.
timeout	Sets the maximum idle time duration.

clear configure tunnel-group

To remove all or specified tunnel groups from the configuration, use the **clear config tunnel-group** command in global configuration.

clear config tunnel-group [*name*]

Syntax Description

name (Optional) Specifies the name of a tunnel group.

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		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	•	—	•	—	—

Command History

Release	Modification
7.0	This command was introduced.

Examples

The following example entered in global configuration mode, removes the toengineering tunnel group from the configuration:

```
hostname(config)# clear config tunnel-group toengineering
hostname(config)#
```

Related Commands

Command	Description
show running-config tunnel-group	Displays information about all or selected tunnel-groups.
tunnel-group	Enters tunnel-group subconfiguration mode for the specified type.

clear configure url-block

To clear clears URL pending block buffer and long URL support configuration, use the **clear configure url-block** command in global configuration mode.

clear configure url-block

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		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	•	•	•	•	•

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

The **clear configure url-block** command clears URL pending block buffer and long URL support configuration.

Examples

The following example clears URL pending block buffer and long URL support configuration:

```
hostname# clear configure url-block
```

Related Commands

Commands	Description
clear url-block block statistics	Clears the block buffer usage counters.
show url-block	Displays information about the URL cache, which is used for buffering URLs while waiting for responses from an N2H2 or Websense filtering server.
url-block	Manage the URL buffers used for web server responses.
url-cache	Enables URL caching while pending responses from an N2H2 or Websense server and sets the size of the cache.
url-server	Identifies an N2H2 or Websense server for use with the filter command.

clear configure url-cache

To clear the URL cache, use the **clear configure url-cache** command in global configuration mode.

clear configure url-cache

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		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	•	•	•	•	•

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

The **clear configure url-cache** command clears the URL cache.

Examples

The following example clears the URL cache:

```
hostname# clear configure url-cache
```

Related Commands

Commands	Description
clear url-cache statistics	Removes url-cache command statements from the configuration.
filter url	Directs traffic to a URL filtering server.
show url-cache statistics	Displays information about the URL cache, which is used for buffering URLs while waiting for responses from an N2H2 or Websense filtering server.
url-cache	Enables URL caching while pending responses from an N2H2 or Websense server and sets the size of the cache.
url-server	Identifies an N2H2 or Websense server for use with the scsc command.

clear configure url-list

To remove a configured set of URLs that WebVPN users can access, use the **clear configure url-list** command in global configuration mode. To remove all configured URLs, use this command without the *listname* argument. To remove only the URLs for a specific list, use this command with that *listname*.

clear configure url-list [*listname*]

Syntax Description

<i>listname</i>	Groups the set of URLs WebVPN users can access. Maximum 64 characters.
-----------------	--

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
Global configuration	•	—	•	—	—

Command History

Release	Modification
7.0	This command was introduced.

Examples

The following example shows how to remove the URL list called *Marketing URLs*.

```
hostname(config)# clear configure url-list Marketing URLs
```

Related Commands

Command	Description
show running-configuration url-list	Displays the current set of configured url-list commands.
url-list	Use this command in global configuration mode to configure the set of URLs that WebVPN users can access.
url-list	Use this command in webvpn mode that you access from group-policy or username mode to enable WebVPN URL access for a specific group policy or user.

clear configure url-server

To clear the URL filtering server configuration, use the **clear configure url-server** command in global configuration mode.

clear configure url-server

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		
	Routed	Transparent	Single	Multiple Context	System
Global configuration	•	•	•	•	•

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

The **clear configure url-server** command clears the URL filtering server configuration.

Examples

The following example URL filtering server configuration:

```
hostname# clear configure url-server
```

Related Commands

Commands	Description
clear url-server	Clears the URL filtering server statistics.
show url-server	Displays information about the URL cache, which is used for buffering URLs while waiting for responses from an N2H2 or Websense filtering server.
url-cache	Enables URL caching while pending responses from an N2H2 or Websense server and sets the size of the cache.
url-block	Manages the URL buffers used for web server responses while waiting for a filtering decision from the filtering server.
url-server	Identifies an N2H2 or Websense server for use with the filter command.

clear configure username

To clear the username database, use the **clear configure username** command. To clear the configuration for a particular user, use this command and append the username.

clear configure username [*name*]

Syntax Description

name (Optional) Provides the name of the user.

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		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	•	—	•	—	—

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

The internal user authentication database consists of the users entered with the username command. The login command uses this database for authentication.

Examples

The following example shows how to clear the configuration for the user named anyuser:

```
hostname(config)# clear configure username anyuser
```

Related Commands

Command	Description
show running-config username	Displays the running configuration for a particular user or for all users.
username	Adds a user to the security appliance database.
username attributes	Lets you configure AVPs for specific users.

clear configure virtual

To remove the authentication virtual server from the configuration, use the **clear configure virtual** command in global configuration mode.

clear configure virtual

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values.

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

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

Command History	Release	Modification
	7.0	This command was modified to conform to CLI guidelines.

Usage Guidelines There is no undo.

Examples This example shows the **clear configure virtual** command:

```
hostname(config)# clear configure virtual
```

Related Commands	Command	Description
	show running-config virtual	Displays the IP address for the authentication virtual server.
	virtual http	Allows separate authentication with the security appliance and with the HTTP server.
	virtual telnet	Authenticates users with the virtual Telnet server for traffic types for which the security appliance does not supply an authentication prompt.

clear configure vpn-load-balancing

To remove the previously specified VPN load-balancing configuration, thus disabling VPN load-balancing, use the **clear configure vpn load-balancing** command in global configuration mode.

clear configure vpn load-balancing

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values.

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

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

Release	Modification
7.0	This command was introduced

Usage Guidelines The **clear configure vpn load-balancing** command also clears the following related commands: **cluster encryption**, **cluster ip address**, **cluster key**, **cluster port**, **nat**, **participate**, and **priority**.

Examples The following command removes vpn load-balancing configuration statements from the configuration:

```
hostname(config)# clear configure vpn load-balancing
```

Related Commands	show running-config vpn load-balancing	Displays the current VPN load-balancing configuration.
	vpn load-balancing	Enters vpn load-balancing mode.

clear conn

To clear a specific connection or multiple connections, use the **clear conn** command in privileged EXEC mode. This command supports IPv4 and IPv6 addresses.

```
clear conn [all] [protocol {tcp | udp}] [address src_ip[-src_ip] [netmask mask]]
          [port src_port[-src_port]] [address dest_ip[-dest_ip] [netmask mask]]
          [port dest_port[-dest_port]]
```

Syntax Description		
address	(Optional) Clears connections with the specified source or destination IP address.	
all	(Optional) Clears all connections that are to the device or from the device, in addition to through-traffic connections.	
<i>dest_ip</i>	(Optional) Specifies the destination IP address (IPv4 or IPv6). To specify a range, separate the IP addresses with a dash (-). For example: 10.1.1.1-10.1.1.5	
<i>dest_port</i>	(Optional) Specifies the destination port number. To specify a range, separate the port numbers with a dash (-). For example: 1000-2000	
netmask <i>mask</i>	(Optional) Specifies a subnet mask for use with the given IP address.	
port	(Optional) Clears connections with the specified source or destination port.	
protocol { tcp udp }	(Optional) Clears connections with the protocol tcp or udp .	
<i>src_ip</i>	(Optional) Specifies the source IP address (IPv4 or IPv6). To specify a range, separate the IP addresses with a dash (-). For example: 10.1.1.1-10.1.1.5	
<i>src_port</i>	(Optional) Specifies the source port number. To specify a range, separate the port numbers with a dash (-). For example: 1000-2000	

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	•	•	•	•	—

Command History

Release	Modification
7.0(8)	This command was introduced.

Usage Guidelines

When the security appliance creates a pinhole to allow secondary connections, this is shown as an incomplete conn by the **show conn** command. To clear this incomplete conn use the **clear conn** command.

Examples

The following example shows all connections, and then clears the management connection between 10.10.10.108:4168 and 10.0.8.112:22:

```
hostname# show conn all
TCP mgmt 10.10.10.108:4168 NP Identity Ifc 10.0.8.112:22, idle 0:00:00, bytes 3084, flags
UOB
```

```
hostname# clear conn address 10.10.10.108 port 4168 address 10.0.8.112 port 22
```

Related Commandss

Commands	Description
clear local-host	Clears all connections by a specific local host or all local hosts.
clear xlate	Clears a NAT session, and any connections using NAT.
show conn	Shows connection information.
show local-host	Displays the network states of local hosts.
show xlate	Shows NAT sessions.

clear console-output

To remove the currently captured console output, use the **clear console-output** command in privileged EXEC mode.

clear console-output

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values.

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

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

Release	Modification
Preexisting	This command was preexisting.

Command History

Examples The following example shows how to remove the currently captured console output:

```
hostname# clear console-output
```

Command	Description
show console-output	Displays the captured console output.

Related Commands

clear counters

To clear the protocol stack counters, use the **clear counters** command in global configuration mode.

clear counters [**all** | **context** *context-name* | **summary** | **top** *N*] [**detail**] [**protocol** *protocol_name* [:*counter_name*]] [**threshold** *N*]

Syntax Description

all	(Optional) Clears all filter details.
context <i>context-name</i>	(Optional) Specifies the context name.
<i>:counter_name</i>	(Optional) Specifies a counter by name.
detail	(Optional) Clears detailed counters information.
protocol <i>protocol_name</i>	(Optional) Clears the counters for the specified protocol.
summary	(Optional) Clears the counter summary.
threshold <i>N</i>	(Optional) Clears the counters at or above the specified threshold. The range is 1 through 4294967295.
top <i>N</i>	(Optional) Clears the counters at or above the specified threshold. The range is 1 through 4294967295.

Defaults

clear counters summary detail

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
Global configuration	•	•	•	•	•

Command History

Release	Modification
7.0	This command was introduced.

Examples

This example shows how to clear the protocol stack counters:

```
hostname(config)# clear counters
```

Related Commands

Command	Description
show counters	Displays the protocol stack counters.

clear crashinfo

To delete the contents of the crash file in Flash memory, enter the **clear crashinfo** command in privileged EXEC mode.

clear crashinfo

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:

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

Release	Modification
Preexisting	This command was preexisting.

Command History

Usage Guidelines This command has no usage guidelines.

Examples The following command shows how to delete the crash file:

```
hostname# clear crashinfo
```

Related Commands	crashinfo force	Forces a crash of the security appliance.
	crashinfo save disable	Disables crash information from writing to Flash memory.
	crashinfo test	Tests the ability of the security appliance to save crash information to a file in Flash memory.
	show crashinfo	Displays the contents of the crash file stored in Flash memory.

clear crypto accelerator statistics

To clear the the global and accelerator-specific statistics from the crypto accelerator MIB, use the **clear crypto accelerator statistics** command in global configuration and privileged EXEC modes.

clear crypto accelerator statistics

Syntax Description

This command has no keywords or variables.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0	This command was introduced.

Examples

The following example entered in global configuration mode, displays crypto accelerator statistics:

```
hostname(config)# clear crypto accelerator statistics
hostname(config)#
```

Related Commands

Command	Description
clear crypto protocol statistics	Clears the protocol-specific statistics in the crypto accelerator MIB.
show crypto accelerator statistics	Displays the global and accelerator-specific statistics in the crypto accelerator MIB.
show crypto protocol statistics	Displays the protocol-specific statistics from the crypto accelerator MIB.

clear crypto ca crls

To remove the CRL cache of all CRLs associated with a specified trustpoint or to remove the CRL cache of all CRLs, use the **clear crypto ca crls** command in global configuration.

clear crypto ca crls [*trustpointname*]

Syntax Description

trustpointname (Optional) The name of a trustpoint. If you do not specify a name, this command clears all CRLs cached on the system.

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		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	•	•	•	•	

Command History

Release	Modification
7.0	This command was introduced.

Examples

The following example issued in global configuration mode, removes all of the CRL cache from all CRLs from the security appliance:

```
hostname(config)# clear crypto ca crls
hostname(config)#
```

Related Commands

Command	Description
crypto ca crl request	Downloads the CRL based on the CRL configuration of the trustpoint.
show crypto ca crls	Displays all cached CRLs or CRLs cached for a specified trustpoint.

clear [crypto] ipsec sa

To remove the IPsec SA counters, entries, crypto maps or peer connections, use the **clear [crypto] ipsec sa** command in global configuration mode. To clear all IPsec SAs, use this command without arguments.

clear [crypto] ipsec sa [**counters** | **entry** {*hostname* | *IP address*} {**esp** | **ah**} {*SPI*} | **map** {*map name*} | **peer** {*hostname* | *IP address*}]

Be careful when using this command.

Syntax Description

ah	Authentication header.
counters	Clears all IPsec per SA statistics.
entry	Deletes the tunnel that matches the specified IP address/hostname, protocol and SPI value.
esp	Encryption security protocol.
<i>hostname</i>	Identified a hostname assigned to an IP address.
<i>IP address</i>	Identifies an IP address.
map	Deletes all tunnels associated with the specified crypto map as identified by map name.
<i>map name</i>	An alphanumeric string that identifies a crypto map. Max 64 characters.
peer	Deletes all IPsec SAs to a peer as identified by the specified hostname or IP address.
<i>SPI</i>	Identifies the Security Parameters Index (a hexadecimal number).

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		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	•	—	•	—	—

Command History

Release	Modification
7.0	This command was introduced.

Examples

The following example, issued in global configuration mode, removes all of the IPsec SAs from the security appliance:

```
hostname(config)# clear ipsec sa
```



```
hostname(config)#
```

The next example, issued in global configuration mode, deletes SAs with a peer IP address of 10.86.1.1.

```
hostname(config)# clear ipsec peer 10.86.1.1
hostname(config)#
```

Related Commands

Command	Description
clear configure crypto map	Clears all or specified crypto maps from the configuration.
clear configure isakmp	Clears all ISAKMP policy configuration.
show ipsec sa	Displays information about IPSec SAs, including counters, entry, map name, peer IP address and hostname.
show running-config crypto	Displays the entire crypto configuration, including IPSec, crypto maps, dynamic crypto maps, and ISAKMP.

clear crypto protocol statistics

To clear the protocol-specific statistics in the crypto accelerator MIB, use the **clear crypto protocol statistics** command in global configuration or privileged EXEC modes.

clear crypto protocol statistics *protocol*

Syntax Description

protocol

Specifies the name of the protocol for which you want to clear statistics. Protocol choices are as follows:

ikev1—Internet Key Exchange version 1.

ipsec—IP Security Phase-2 protocols.

ssl—Secure Socket Layer.

other—Reserved for new protocols.

all—All protocols currently supported.

In online help for this command, other protocols may appear that will be supported in future releases.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0	This command was introduced.

Examples

The following example entered in global configuration mode, clears all crypto accelerator statistics:

```
hostname(config)# clear crypto protocol statistics all
hostname(config)#
```

Related Commands

Command	Description
clear crypto accelerator statistics	Clears the global and accelerator-specific statistics in the crypto accelerator MIB.

Command	Description
show crypto accelerator statistics	Displays the global and accelerator-specific statistics from the crypto accelerator MIB.
show crypto protocol statistics	Displays the protocol-specific statistics in the crypto accelerator MIB.

clear dhcpd

To clear the DHCP server bindings and statistics, use the **clear dhcpd** command.

clear dhcpd { **binding** [*IP_address*] | **statistics** }

Syntax Description

binding	Clears all the client address bindings.
<i>IP_address</i>	Clears the binding for the specified IP address.
statistics	Clears statistical information counters.

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		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

If you include the optional IP address in the **clear dhcpd binding** command, only the binding for that IP address is cleared.

To clear all of the DHCP server commands, use the **clear configure dhcpd** command.

Examples

The following example shows how to clear the **dhcpd** statistics:

```
hostname(config)# clear dhcpd statistics
```

Related Commands

Command	Description
clear configure dhcpd	Removes all DHCP server settings.
show dhcpd	Displays DHCP binding, statistic, or state information.

clear dhcprelay statistics

To clear the DHCP relay statistic counters, use the **clear dhcprelay statistics** command in privileged EXEC mode.

clear dhcprelay statistics

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values.

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

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

Command History	Release	Modification
	Preexisting	This command was preexisting.

Usage Guidelines The **clear dhcprelay statistics** command only clears the DHCP relay statistic counters. To clear the entire DHCP relay configuration, use the **clear configure dhcprelay** command.

Examples The following example shows how to clear the DHCP relay statistics:

```
hostname# clear dhcprelay statistics
hostname#
```

Related Commands	Command	Description
	clear configure dhcprelay	Removes all DHCP relay agent settings.
	debug dhcprelay	Displays debug information for the DHCP relay agent.
	show dhcprelay statistics	Displays DHCP relay agent statistic information.
	show running-config dhcprelay	Displays the current DHCP relay agent configuration.

clear dns-hosts cache

To clear the DNS cache, use the **clear dns-hosts cache** command in privileged EXEC mode. This command does not clear static entries you added with the **name** command.

clear dns-hosts cache

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values.

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

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

Release	Modification
7.0	This command was introduced.

Examples The following example clears the DNS cache:

```
hostname# clear dns-hosts cache
```

Related Commands	Command	Description
	dns domain-lookup	Enables the security appliance to perform a name lookup.
	dns name-server	Configures a DNS server address.
	dns retries	Specifies the number of times to retry the list of DNS servers when the security appliance does not receive a response.
	dns timeout	Specifies the amount of time to wait before trying the next DNS server.
	show dns-hosts	Shows the DNS cache.

clear failover statistics

To clear the failover statistic counters, use the **clear failover statistics** command in privileged EXEC mode.

clear failover statistics

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values.

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

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

Release	Modification
Preexisting	This command was introduced.

Command History

Usage Guidelines This command clears the statistics displayed with the **show failover statistics** command and the counters in the Stateful Failover Logical Update Statistics section of the **show failover** command output. To remove the failover configuration, use the **clear configure failover** command.

Examples The following example shows how to clear the failover statistic counters:

```
hostname# clear failover statistics
hostname#
```

Command	Description
debug fover	Displays failover debug information.
show failover	Displays information about the failover configuration and operational statistics.

Related Commands

clear fragment

To clear the operational data of the IP fragment reassembly module, enter the **clear fragment** command in privileged EXEC mode. This command clears either the currently queued fragments that are waiting for reassembly (if the **queue** keyword is entered) or clears all IP fragment reassembly statistics (if the **statistics** keyword is entered). The statistics are the counters, which tell how many fragments chains were successfully reassembled, how many chains failed to be reassembled, and how many times the maximum size was crossed resulting in overflow of the buffer.

clear fragment { **queue** | **statistics** } [*interface*]

Syntax Description

<i>interface</i>	(Optional) Specifies the security appliance interface.
queue	Clears the IP fragment reassembly queue.
statistics	Clears the IP fragment reassembly statistics.

Defaults

If an *interface* is not specified, the command applies to all interfaces.

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	•	•	•	•	—

Command History

Release	Modification
7.0	The command was separated into two commands, clear fragment and clear configure fragment , to separate clearing of the configuration data from the operational data.

Examples

This example shows how to clear the operational data of the IP fragment reassembly module:

```
hostname# clear fragment queue
```

Related Commands

Command	Description
clear configure fragment	Clears the IP fragment reassembly configuration and resets the defaults.
fragment	Provides additional management of packet fragmentation and improves compatibility with NFS.
show fragment	Displays the operational data of the IP fragment reassembly module.
show running-config fragment	Displays the IP fragment reassembly configuration.

clear gc

To remove the garbage collection process statistics, use the **clear gc** command in privileged EXEC mode.

clear gc

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:

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

Command History

Release	Modification
7.0	This command was introduced.

Examples

The following example shows how to remove the garbage collection process statistics:

```
hostname# clear gc
```

Related Commands

Command	Description
show gc	Displays the garbage collection process statistics.

clear igmp counters

To clear all IGMP counters, use the **clear igmp counters** command in privileged EXEC mode.

clear igmp counters [*if_name*]

Syntax Description

if_name The interface name, as specified by the **nameif** command. Including an interface name with this command causes only the counters for the specified interface to be cleared.

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0	This command was introduced.

Examples

The following example clears the IGMP statistical counters:

```
hostname# clear igmp counters
```

Related Commands

Command	Description
clear igmp group	Clears discovered groups from the IGMP group cache.
clear igmp traffic	Clears the IGMP traffic counters.

clear igmp group

To clear discovered groups from the IGMP group cache, use the **clear igmp** command in privileged EXEC mode.

clear igmp group [*group* | *interface name*]

Syntax Description

<i>group</i>	IGMP group address. Specifying a particular group removes the specified group from the cache.
<i>interface name</i>	Interface name, as specified by the namif command. When specified, all groups associated with the interface are removed.

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		
	Routed	Transparent	Single	Multiple Context	System
Privileged EXEC	•	—	•	—	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

If you do not specify a group or an interface, all groups are cleared from all interfaces. If you specify a group, only the entries for that group are cleared. If you specify an interface, then all groups on that interface are cleared. If you specify both a group and an interface, only the specified groups on the specified interface are cleared.

This command does not clear statically configured groups.

Examples

The following example shows how to clear all discovered IGMP groups from the IGMP group cache:

```
hostname# clear igmp
```

Related Commands

Command	Description
clear igmp counters	Clears all IGMP counters.
clear igmp traffic	Clears the IGMP traffic counters.

clear igmp traffic

To clear the IGMP traffic counters, use the **clear igmp traffic** command in privileged EXEC mode.

clear igmp traffic

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values.

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

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

Command History	Release	Modification
	7.0	This command was introduced.

Examples The following example clears the IGMP statistical traffic counters:

```
hostname# clear igmp traffic
```

Related Commands	Command	Description
	clear igmp group	Clears discovered groups from the IGMP group cache.
	clear igmp counters	Clears all IGMP counters.

clear interface

To clear interface statistics, use the **clear interface** command in privileged EXEC mode.

clear interface [*physical_interface* [, *subinterface*] | *mapped_name* | *interface_name*]

Syntax Description

<i>interface_name</i>	(Optional) Identifies the interface name set with the nameif command.
<i>mapped_name</i>	(Optional) In multiple context mode, identifies the mapped name if it was assigned using the allocate-interface command.
<i>physical_interface</i>	(Optional) Identifies the interface ID, such as gigabitethernet0/1 . See the interface command for accepted values.
<i>subinterface</i>	(Optional) Identifies an integer between 1 and 4294967293 designating a logical subinterface.

Defaults

By default, this command clears all interface statistics.

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	•	•	•	•	•

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

If an interface is shared among contexts, and you enter this command within a context, the security appliance clears only statistics for the current context. If you enter this command in the system execution space, the security appliance clears the combined statistics.

You cannot use the interface name in the system execution space, because the **nameif** command is only available within a context. Similarly, if you mapped the interface ID to a mapped name using the **allocate-interface** command, you can only use the mapped name in a context.

Examples

The following example clears all interface statistics:

```
hostname# clear interface
```

Related Commands	Command	Description
	clear configure interface	Clears the interface configuration.
	interface	Configures an interface and enters interface configuration mode.
	show interface	Displays the runtime status and statistics of interfaces.
	show running-config interface	Displays the interface configuration.

clear ip audit count

To clear the count of signature matches for an audit policy, use the **clear ip audit count** command in privileged EXEC mode.

clear ip audit count [**global** | **interface** *interface_name*]

Syntax Description

global	(Default) Clears the number of matches for all interfaces.
interface <i>interface_name</i>	(Optional) Clears the number of matches for the specified interface.

Defaults

If you do not specify a keyword, this command clears the matches for all interfaces (**global**).

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	•	•	•	•	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Examples

The following example clears the count for all interfaces:

```
hostname# clear ip audit count
```

Related Commands

Command	Description
ip audit interface	Assigns an audit policy to an interface.
ip audit name	Creates a named audit policy that identifies the actions to take when a packet matches an attack signature or an informational signature.
show ip audit count	Shows the count of signature matches for an audit policy.
show running-config ip audit attack	Shows the configuration for the ip audit attack command.

clear ip verify statistics

To clear the Unicast RPF statistics, use the **clear ip verify statistics** command in privileged EXEC mode. See the **ip verify reverse-path** command to enable Unicast RPF.

clear ip verify statistics [**interface** *interface_name*]

Syntax Description

interface Sets the interface on which you want to clear Unicast RPF statistics.
interface_name

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		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	•	—	•	•	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Examples

The following example clears the Unicast RPF statistics:

```
hostname# clear ip verify statistics
```

Related Commands

Command	Description
clear configure ip verify reverse-path	Clears the ip verify reverse-path configuration.
ip verify reverse-path	Enables the Unicast Reverse Path Forwarding feature to prevent IP spoofing.
show ip verify statistics	Shows the Unicast RPF statistics.
show running-config ip verify reverse-path	Shows the ip verify reverse-path configuration.

clear ipsec sa

To clear IPsec SAs entirely or based on specified parameters, use the **clear ipsec sa** command in global configuration and privileged EXEC modes. You can also use an alternate form: **clear crypto ipsec sa**.

clear ipsec sa [**counters** | **entry** *peer-addr protocol spi* | **peer** *peer-addr* | **map** *map-name*]

Syntax Description

counters	(Optional) Clears all counters.
entry	(Optional) Clears IPsec SAs for a specified IPsec peer, protocol and SPI.
map <i>map-name</i>	(Optional) Clears IPsec SAs for the specified crypto map.
peer	(Optional) Clears IPsec SAs for a specified peer.
<i>peer-addr</i>	Specifies the IP address of an IPsec peer.
<i>protocol</i>	Specifies an IPsec protocol: esp or ah .
<i>spi</i>	Specifies an IPsec SPI.

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		
	Routed	Transparent	Single	Multiple Context	System
Global configuration	•	•	•	—	—
Privileged EXEC	•	•	•	—	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Examples

The following example, entered in global configuration mode, clears all IPsec SA counters:

```
hostname(config)# clear ipsec sa counters
hostname(config)#
```

Related Commands

Command	Description
show ipsec sa	Displays IPsec SAs based on specified parameters.
show ipsec stats	Displays global IPsec statistics from the IPsec flow MIB.

clear ipv6 access-list counters

To clear the IPv6 access list statistical counters, use the **clear ipv6 access-list counters** command in privileged EXEC mode.

clear ipv6 access-list *id* **counters**

Syntax Description

id The IPv6 access list identifier.

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		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	•	—	•	•	—

Command History

Release	Modification
7.0	This command was introduced.

Examples

The following example shows how to clear the statistical data for the IPv6 access list 2:

```
hostname# clear ipv6 access-list 2 counters
hostname#
```

Related Commands

Command	Description
clear configure ipv6	Clears the ipv6 access-list commands from the current configuration.
ipv6 access-list	Configures an IPv6 access list.
show ipv6 access-list	Displays the ipv6 access-list commands in the current configuration.

clear ipv6 neighbors

To clear the IPv6 neighbor discovery cache, use the **clear ipv6 neighbors** command in privileged EXEC mode.

clear ipv6 neighbors

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

This command deletes all discovered IPv6 neighbor from the cache; it does not remove static entries.

Examples

The following example deletes all entries, except static entries, in the IPv6 neighbor discovery cache:

```
hostname# clear ipv6 neighbors
hostname#
```

Related Commands

Command	Description
ipv6 neighbor	Configures a static entry in the IPv6 discovery cache.
show ipv6 neighbor	Displays IPv6 neighbor cache information.

clear ipv6 traffic

To reset the IPv6 traffic counters, use the **clear ipv6 traffic** command in privileged EXEC mode.

clear ipv6 traffic

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values.

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

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

Release	Modification
7.0	This command was introduced.

Usage Guidelines Using this command resets the counters in the output from the show ipv6 traffic command.

Examples The following example resets the IPv6 traffic counters. The output from the **ipv6 traffic** command shows that the counters are reset:

```
hostname# clear ipv6 traffic
hostname# show ipv6 traffic
IPv6 statistics:
  Rcvd: 1 total, 1 local destination
        0 source-routed, 0 truncated
        0 format errors, 0 hop count exceeded
        0 bad header, 0 unknown option, 0 bad source
        0 unknown protocol, 0 not a router
        0 fragments, 0 total reassembled
        0 reassembly timeouts, 0 reassembly failures
  Sent: 1 generated, 0 forwarded
        0 fragmented into 0 fragments, 0 failed
        0 encapsulation failed, 0 no route, 0 too big
  Mcast: 0 received, 0 sent

ICMP statistics:
  Rcvd: 1 input, 0 checksum errors, 0 too short
        0 unknown info type, 0 unknown error type
        unreachable: 0 routing, 0 admin, 0 neighbor, 0 address, 0 port
        parameter: 0 error, 0 header, 0 option
        0 hopcount expired, 0 reassembly timeout, 0 too big
```

```

0 echo request, 0 echo reply
0 group query, 0 group report, 0 group reduce
0 router solicit, 0 router advert, 0 redirects
0 neighbor solicit, 1 neighbor advert
Sent: 1 output
  unreach: 0 routing, 0 admin, 0 neighbor, 0 address, 0 port
  parameter: 0 error, 0 header, 0 option
0 hopcount expired, 0 reassembly timeout, 0 too big
0 echo request, 0 echo reply
0 group query, 0 group report, 0 group reduce
0 router solicit, 0 router advert, 0 redirects
0 neighbor solicit, 1 neighbor advert

UDP statistics:
  Rcvd: 0 input, 0 checksum errors, 0 length errors
        0 no port, 0 dropped
  Sent: 0 output

TCP statistics:
  Rcvd: 0 input, 0 checksum errors
  Sent: 0 output, 0 retransmitted

```

Related Commands

Command	Description
show ipv6 traffic	Displays IPv6 traffic statistics.

clear isakmp sa

To remove all of the IKE runtime SA database, use the **clear isakmp sa** command in global configuration or privileged EXEC mode.

clear isakmp sa

Syntax Description

This command has no keywords or arguments.

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		
	Routed	Transparent	Single	Multiple Context	System
Global configuration	•		•		
Privileged EXEC	•		•		

Command History

Release	Modification
7.0	This command was introduced.

Examples

The following example removes the IKE runtime SA database from the configuration:

```
hostname(config)# clear isakmp sa
hostname(config)#
```

Related Commands

Command	Description
clear isakmp sa	Clears the IKE runtime SA database.
isakmp enable	Enables ISAKMP negotiation on the interface on which the IPSec peer communicates with the security appliance.
show isakmp stats	Displays runtime statistics.
show isakmp sa	Displays IKE runtime SA database with additional information.
show running-config isakmp	Displays all the active ISAKMP configuration.

clear local-host

To release network connections from local hosts displayed by entering the **show local-host** command, use the **clear local-host** command in privileged EXEC mode.

clear local-host [*ip_address*] [**all**]

Syntax Description

all	(Optional) Specifies to clear the local hosts state-made connections, including to the security appliance and from the security appliance.
<i>ip_address</i>	(Optional) Specifies the local host IP address.

Defaults

No default behaviors or values.

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	•	•	•	•	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

The **clear local-host** command releases the cleared hosts from the license limit. You can see the number of hosts that are counted toward the license limit by entering the **show local-host** command.



Caution

Clearing the network state of a local host stops all network connections and xlates that are associated with the local hosts.

Examples

The following example shows how the **clear local-host** command clears the information about the local hosts:

```
hostname# clear local-host 10.1.1.15
```

After the information is cleared, nothing more displays until the hosts reestablish their connections.

Related Commands

Command	Description
show local-host	Displays the network states of local hosts.

clear logging asdm

To clear the ASDM logging buffer, use the **clear logging asdm** command in privileged EXEC mode.

clear logging asdm

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values.

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

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

Command History	Release	Modification
	7.0	This command was changed from the show pdm logging command to the show asdm log command.

Usage Guidelines ASDM syslog messages are stored in a separate buffer from the security appliance syslog messages. Clearing the ASDM logging buffer only clears the ASDM syslog messages, it does not clear the security appliance system messages. To view the ASDM syslog messages, use the **show asdm log** command.

Examples The following example clears the ASDM logging buffer:

```
hostname(config)# clear logging asdm
hostname(config)#
```

Related Commands	Command	Description
	show asdm log_sessions	Displays the contents of the ASDM logging buffer.

clear logging buffer

To clear the logging buffer, use the **clear logging buffer** command in global configuration mode.

clear logging buffer

Syntax Description

This command has no arguments or keywords.

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
Global configuration	•	•	•	•	•

Command History

Release	Modification
7.0	Support for this command was introduced on the security appliance.

Examples

This example shows how to disable the SNMP server:

```
hostname #clear logging buffer
```

Related Commands

Command	Description
logging buffered	Configures logging.
show logging	Displays logging information.

clear mac-address-table

To clear dynamic MAC address table entries , use the **clear mac-address-table** command in privileged EXEC mode.

clear mac-address-table [*interface_name*]

Syntax Description

interface_name (Optional) Clears the MAC address table entries for the selected interface.

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		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	—	•	•	•	—

Command History

Release	Modification
7.0	This command was introduced.

Examples

The following example clears the dynamic MAC address table entries:

```
hostname# clear mac-address-table
```

Related Commands

Command	Description
arp	Adds a static ARP entry.
firewall transparent	Sets the firewall mode to transparent.
mac-address-table aging-time	Sets the timeout for dynamic MAC address entries.
mac-learn	Disables MAC address learning.
show mac-address-table	Shows MAC address table entries.

clear memory delayed-free-poisoner

To clear the delayed free-memory poisoner tool queue and statistics, use the **clear memory delayed-free-poisoner** command in privileged EXEC mode.

clear memory delayed-free-poisoner

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:

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

The **clear memory delayed-free-poisoner** command returns all memory held in the delayed free-memory poisoner tool queue to the system without validation and clears the related statistical counters.

Examples

The following example clears the delayed free-memory poisoner tool queue and statistics:

```
hostname# clear memory delayed-free-poisoner
```

Related Commands

Command	Description
memory delayed-free-poisoner enable	Enables the delayed free-memory poisoner tool.
memory delayed-free-poisoner validate	Forces validation of the delayed free-memory poisoner tool queue.
show memory delayed-free-poisoner	Displays a summary of the delayed free-memory poisoner tool queue usage.

clear memory profile

To clear the memory buffers held by the memory profiling function, use the **clear memory profile** command in privileged EXEC configuration mode.

clear memory profile [peak]

Syntax Description

peak (Optional) Clears the contents of the peak memory buffer.

Defaults

Clears the current “in use” profile buffer by default.

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	•	•	—	•	•

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

The **clear memory profile** command releases the memory buffers held by the profiling function and therefore requires that profiling stop before it is cleared.

Examples

The following example clears the memory buffers held by the profiling function:

```
hostname# clear memory profile
```

Related Commands

Command	Description
memory profile enable	Enables the monitoring of memory usage (memory profiling).
memory profile text	Configures a text range of memory to profile.
show memory profile	Displays information about the memory usage (profiling) of the security appliance.

clear memory tracking

To clear all currently gathered information, use the **clear memory tracking** command in privileged EXEC configuration mode.

clear memory tracking

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:

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

Command History

Release	Modification
7.0(8)	This command was introduced.

Usage Guidelines

The **clear memory tracking** command clears all currently gathered information.

Examples

The following example clears the memory tracking function:

```
hostname# clear memory tracking
```

Related Commands

Command	Description
memory tracking enable	Tracks heap memory request.
show memory tracking	Shows currently allocated memory.
show memory tracking address	Lists the size, location, and topmost caller function of each currently allocated piece memory tracked by the tool.
show memory tracking dump	This command shows the size, location, partial callstack, and a memory dump of the given memory address.

clear mfib counters

To clear MFIB router packet counters, use the **clear mfib counters** command in privileged EXEC mode.

clear mfib counters [*group* [*source*]]

Syntax Description

<i>group</i>	(Optional) IP address of the multicast group.
<i>source</i>	(Optional) IP address of the multicast route source. This is a unicast IP address in four-part dotted-decimal notation.

Defaults

When this command is used with no arguments, route counters for all routes are cleared.

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	•	—	•	—	—

Command History

Release	Modification
7.0	This command was introduced.

Examples

The following example clears all MFIB route counters:

```
hostname# clear mfib route counters
```

Related Commands

Command	Description
show mfib count	Displays MFIB route and packet count data.

clear module recover

To clear the AIP SSM recovery network settings set in the **hw-module module recover** command, use the **clear module recover** command in privileged EXEC mode.

clear module 1 recover

Syntax Description

1 Specifies the slot number, which is always 1.

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		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	•	•	•	—	•

Command History

Release	Modification
7.0	This command was introduced.

Examples

The following example clears the recovery settings for the AIP SSM:

```
hostname# clear module 1 recover
```

Related Commands

Command	Description
hw-module module recover	Recovers an AIP SSM by loading a recovery image from a TFTP server.
hw-module module reset	Shuts down an SSM and performs a hardware reset.
hw-module module reload	Reloads the AIP SSM software.
hw-module module shutdown	Shuts down the SSM software in preparation for being powered off without losing configuration data.
show module	Shows SSM information.

clear ospf

To clear OSPF process information, use the **clear ospf** command in privileged EXEC mode.

```
clear ospf [pid] { process | counters [neighbor [neighbor-intf] [neighbor-id]] }
```

Syntax Description

counters	Clears the OSPF counters.
neighbor	Clears the OSPF neighbor counters.
<i>neighbor-intf</i>	(Optional) Clears the OSPF interface router designation.
<i>neighbor-id</i>	(Optional) Clears the OSPF neighbor router ID.
<i>pid</i>	(Optional) Internally used identification parameter for an OSPF routing process; valid values are from 1 to 65535.
process	Clears the OSPF routing process.

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		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	•	—	•	—	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

This command does not remove any part of the configuration. Use the **no** form of the configuration commands to clear specific commands from the configuration or use the **clear configure router ospf** command to remove all global OSPF commands from the configuration.



Note

The **clear configure router ospf** command does not clear OSPF commands entered in interface configuration mode.

Examples

The following example shows how to clear the OSPF process counters:

```
hostname# clear ospf process
```

Related Commands

Command	Description
clear configure router	Clears all global router commands from the running configuration.

clear pim counters

To clear the PIM traffic counters, use the **clear pim counters** command in privileged EXEC mode.

clear pim counters

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values.

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

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

Command History	Release	Modification
	7.0	This command was introduced.

Usage Guidelines This command only clears the traffic counters. To clear the PIM topology table, use the **clear pim topology** command.

Examples The following example clears the PIM traffic counters:

```
hostname# clear pim counters
```

Related Commands	Command	Description
	clear pim reset	Forces MRIB synchronization through reset.
	clear pim topology	Clears the PIM topology table.
	show pim traffic	Displays the PIM traffic counters.

clear pim reset

To force MRIB synchronization through reset, use the **clear pim reset** command in privileged EXEC mode.

clear pim reset

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

All information from the topology table is cleared and the MRIB connection is reset. This command can be used to synchronize state between the PIM topology table and the MRIB database.

Examples

The following example clears the topology table and resets the MRIB connection:

```
hostname# clear pim reset
```

Related Commands

Command	Description
clear pim counters	Clears PIM counters and statistics.
clear pim topology	Clears the PIM topology table.
clear pim counters	Clears PIM traffic counters.

clear pim topology

To clear the PIM topology table, use the **clear pim topology** command in privileged EXEC mode.

clear pim topology [*group*]

Syntax Description	<i>group</i>	(Optional) Specifies the multicast group address or name to be deleted from the topology table.
---------------------------	--------------	---

Defaults	Without the optional <i>group</i> argument, all entries are cleared from the topology table.
-----------------	--

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	•	—	•	—	—

Command History	Release	Modification
	7.0	This command was introduced.

Usage Guidelines	This command clears existing PIM routes from the PIM topology table. Information obtained from the MRIB table, such as IGMP local membership, is retained. If a multicast group is specified, only those group entries are cleared.
-------------------------	---

Examples	The following example clears the PIM topology table:
-----------------	--

```
hostname# clear pim topology
```

Related Commands	Command	Description
	clear pim counters	Clears PIM counters and statistics.
	clear pim reset	Forces MRIB synchronization through reset.
	clear pim counters	Clears PIM traffic counters.

clear priority-queue statistics

To clear the priority-queue statistics counters for an interface or for all configured interfaces, use the **clear priority-queue statistics** command in either global configuration or privileged EXEC mode.

clear priority-queue statistics [*interface-name*]

Syntax Description

interface-name (Optional) Specifies the name of the interface for which you want to show the best-effort and low-latency queue details.

Defaults

If you omit the interface name, this command clears the priority-queue statistics for all configured interfaces.

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	•	•	•	•	—

Command History

Release	Modification
7.0	This command was introduced.

Examples

This example shows the use of the **clear priority-queue statistics** command in privileged EXEC mode to remove the priority queue statistics for the interface named “test”.

```
hostname# clear priority-queue statistics test
hostname#
```

Related Commands

Command	Description
clear configure priority-queue	Removes the priority-queue configuration from the named interface.
priority-queue	Configures priority queueing on an interface.
show priority-queue statistics	Shows the priority queue statistics for a specified interface or for all interfaces.
show running-config priority-queue	Shows the current priority-queue configuration on the named interface.

clear resource usage

To clear resource usage statistics, use the **clear resource usage** command in privileged EXEC mode.

clear resource usage [**context** *context_name* | **all** | **summary**] [**resource** {*resource_name* | **all**}]

Syntax Description

context <i>context_name</i>	(Multiple mode only) Specifies the context name for which you want to clear statistics. Specify all for all contexts.
resource <i>resource_name</i>	<p>Clears the usage of a specific resource. Specify all (the default) for all resources. Resources include the following types:</p> <ul style="list-style-type: none"> • conns—TCP or UDP connections between any two hosts, including connections between one host and multiple other hosts. • hosts—Hosts that can connect through the security appliance. • ipsec—(Single mode only) IPSec sessions • ssh—SSH sessions. • telnet—Telnet sessions. • xlates—NAT translations.
summary	(Multiple mode only) Clears the combined context statistics.

Defaults

For multiple context mode, the default context is **all**, which clears resource usage for every context. For single mode, the context name is ignored and all resource statistics are cleared.

The default resource name is **all**, which clears all resource types.

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	•	•	•	—	•

Command History

Release	Modification
7.0	This command was introduced.

Examples

The following example clears all resource usage statistics:

```
hostname# clear resource usage
```

Related Commands	Command	Description
	context	Adds a security context.
	show resource types	Shows a list of resource types.
	show resource usage	Shows the resource usage of the security appliance.

clear route

To remove dynamically learned routes from the configuration, use the **clear route** command in privileged EXEC mode.

clear route [*interface_name*]

Syntax Description

interface_name (Optional) Internal or external network interface name.

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		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Examples

The following example shows how to remove dynamically learned routes:

```
hostname# clear route
```

Related Commands

Command	Description
route	Specifies a static or default route for the an interface.
show route	Displays route information.
show running-config route	Displays configured routes.

clear service-policy

To clear operational data or statistics (if any) for enabled policies, use the **clear service-policy** command in global configuration mode.

clear service-policy [**global** | **interface** *intf* | **inspect**]

Syntax Description

global	(Optional) Clears the statistics of the global service policy.
interface	(Optional) Clears the service policy statistics of a specific interface.
<i>intf</i>	The interface name defined in the nameif command.
inspect	Clears inspect service policy statistics.

Defaults

By default, this command clears all the statistics for all enabled service policies.

Command Modes

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

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

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

If an interface name is specified, the policy-map only applies to the interface. The interface name is defined in the **nameif** command, and an interface policy-map overrides a global policy-map. Only one policy-map is allowed per interface.

Only one global policy is allowed.

Examples

The following example shows the syntax of the **clear service-policy** command:

```
hostname(config)# clear service-policy outside_security_map outside
```

Related Commands

Command	Description
show service-policy	Displays the service policy.
show running-config service-policy	Displays the service policies configured in the running configuration.

Command	Description
clear configure service-policy	Clears service policy configurations.
service-policy	Configures service policies.

clear service-policy inspect gtp

To clear global GTP statistics, use the **clear service-policy inspect gtp** command in privileged EXEC mode.

```
clear service-policy inspect gtp { pdp-context [all | apn ap_name | imsi IMSI_value | ms-addr IP_address | tid tunnel_ID | version version_num ] | requests | statistics [gsn IP_address] }
```

Syntax Description.

all	Clears all GTP PDP contexts.
apn	(Optional) Clears the PDP contexts based on the APN specified.
<i>ap_name</i>	Identifies the specific access point name.
gsn	(Optional) Identifies the GPRS support node, which is the interface between the GPRS wireless data network and other networks.
gtp	(Optional) Clears the service policy for GTP.
imsi	(Optional) Clears the PDP contexts based on the IMSI specified.
<i>IMSI_value</i>	Hexadecimal value that identifies the specific IMSI.
interface	(Optional) Identifies a specific interface.
<i>int</i>	Identifies the interface for which information will be cleared.
<i>IP_address</i>	IP address for which statistics will be cleared.
ms-addr	(Optional) Clears PDP contexts based on the MS Address specified.
pdp-context	(Optional) Identifies the Packet Data Protocol context.
requests	(Optional) Clears GTP requests.
statistics	(Optional) Clears GTP statistics for the inspect gtp command.
tid	(Optional) Clears the PDP contexts based on the TID specified.
<i>tunnel_ID</i>	Hexadecimal value that identifies the specific tunnel.
version	(Optional) Clears the PDP contexts based on the GTP version.
<i>version_num</i>	Specifies the version of the PDP context. The valid range is 0 to 255.

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		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	•	•	•	•	•

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

The Packet Data Protocol context is identified by the tunnel ID, which is a combination of IMSI and NSAPI. A GTP tunnel is defined by two associated PDP Contexts in different GSN nodes and is identified with a tunnel ID. A GTP tunnel is necessary to forward packets between an external packet data network and a mobile station (MS) user.

Examples

The following example clears GTP statistics:

```
hostname# clear service-policy inspect gtp statistics
```

Related Commands

Commands	Description
debug gtp	Displays detailed information about GTP inspection.
gtp-map	Defines a GTP map and enables GTP map configuration mode.
inspect gtp	Applies a GTP map to use for application inspection.
show service-policy inspect gtp	Displays the GTP configuration.
show running-config gtp-map	Shows the GTP maps that have been configured.

clear shun

To disable all the shuns that are currently enabled and clear the shun statistics, use the **clear shun** command in privileged EXEC mode.

clear shun [*statistics*]

Syntax Description

statistics (Optional) Clears the interface counters only.

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		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
1.1(1)	This command was introduced.

Examples

The following example shows how to disable all the shuns that are currently enabled and clear the shun statistics:

```
hostname(config)# clear shun
```

Related Commands

Command	Description
shun	Enables a dynamic response to an attacking host by preventing new connections and disallowing packets from any existing connection.
show shun	Displays the shun information.

clear sunrpc-server active

To clear the pinholes opened by Sun RPC application inspection, use the **clear sunrpc-server active** command in global configuration mode.

clear sunrpc-server active

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		
	Routed	Transparent	Single	Multiple Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

Use the **clear sunrpc-server active** command to clear the pinholes opened by Sun RPC application inspection that allow service traffic, such as NFS or NIS, to pass through the security appliance.

Examples

The following example shows how to clear the SunRPC services table:

```
hostname(config)# clear sunrpc-server
```

Related Commands

Command	Description
clear configure sunrpc-server	Clears the Sun remote processor call services from the security appliance.
inspect sunrpc	Enables or disables Sun RPC application inspection and configures the port used.
show running-config sunrpc-server	Displays information about the SunRPC services configuration.
show sunrpc-server active	Displays information about active Sun RPC services.

clear traffic

To reset the counters for transmit and receive activity, use the **clear traffic** command in privileged EXEC mode.

clear traffic

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values.

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

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

Release	Modification
Preexisting	This command was preexisting.

Command History

Usage Guidelines The **clear traffic** command resets the counters for transmit and receive activity that is displayed with the **show traffic** command. The counters indicate the number of packets and bytes moving through each interface since the last clear traffic command was entered or since the security appliance came online. And the number of seconds indicate the duration the security appliance has been online since the last reboot.

Examples The following example shows the **clear traffic** command:

```
hostname# clear traffic
```

Command	Description
show traffic	Displays the counters for transmit and receive activity.

Related Commands

clear uauth

To delete all the cached authentication and authorization information for a user or for all users, use the **clear uauth** command in privileged EXEC mode.

clear uauth [*username*]

Syntax Description

username (Optional) Specifies, by username, the user authentication information to remove.

Defaults

Omitting username deletes the authentication and authorization information for all users.

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	•	•	—	—	•

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

The **clear uauth** command deletes the AAA authorization and authentication caches for one user or for all users, which forces the user or users to reauthenticate the next time that they create a connection.

This command is used with the **timeout** command.

Each user host IP address has an authorization cache attached to it. If the user attempts to access a service that has been cached from the correct host, the security appliance considers it preauthorized and immediately proxies the connection. Once you are authorized to access a website, for example, the authorization server is not contacted for each image as it is loaded (assuming the images come from the same IP address). This process significantly increases performance and reduces the load on the authorization server.

The cache allows up to 16 address and service pairs for each user host.



Note

When you enable Xauth, an entry is added to the uauth table (as shown by the **show uauth** command) for the IP address that is assigned to the client. However, when using Xauth with the Easy VPN Remote feature in Network Extension Mode, the IPSec tunnel is created from network to network, so that the users behind the firewall cannot be associated with a single IP address. For this reason, a uauth entry cannot be created upon completion of Xauth. If AAA authorization or accounting services are required, you can enable the AAA authentication proxy to authenticate users behind the firewall. For more information on AAA authentication proxies, see the AAA commands.

Use the **timeout uauth** command to specify how long the cache should be kept after the user connections become idle. Use the **clear uauth** command to delete all the authorization caches for all the users, which will cause them to have to reauthenticate the next time that they create a connection.

Examples

This example shows how to cause the user “Lee” to reauthenticate:

```
hostname(config)# clear uauth lee
```

Related Commands

Command	Description
aaa authentication	Enable, disable, or view LOCAL, TACACS+ or RADIUS user authentication (on a server designated by the aaa-server command).
aaa authorization	Enable, disable, or view TACACS+ or RADIUS user authorization (on a server designated by the aaa-server command).
show uauth	Display current user authentication and authorization information.
timeout	Set the maximum idle time duration.

clear url-block block statistics

To clear the block buffer usage counters, use the **clear url-block block statistics** command in privileged EXEC mode.

clear url-block block statistics

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

The **clear url-block block statistics** command clears the block buffer usage counters, except for the `Current number of packets held (global) counter`.

Examples

The following example clears the URL block statistics and displays the status of the counters after clearing:

```
hostname# clear url-block block statistics
hostname# show url-block block statistics

URL Pending Packet Buffer Stats with max block 0
-----
Cumulative number of packets held: 0
Maximum number of packets held (per URL): 0
Current number of packets held (global): 38
Packets dropped due to
| exceeding url-block buffer limit: 0
| HTTP server retransmission: 0
Number of packets released back to client: 0
```

Related Commands

Commands	Description
filter url	Directs traffic to a URL filtering server.
show url-block	Displays information about the URL cache, which is used for buffering URLs while waiting for responses from an N2H2 or Websense filtering server.
url-block	Manage the URL buffers used for web server responses.
url-cache	Enables URL caching while pending responses from an N2H2 or Websense server and sets the size of the cache.
url-server	Identifies an N2H2 or Websense server for use with the filter command.

clear url-cache statistics

To remove **url-cache** command statements from the configuration, use the **clear url-cache** command in privileged EXEC mode.

clear url-cache statistics

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

The **clear url-cache** command removes **url-cache** statistics from the configuration.

Using the URL cache does not update the Websense accounting logs for Websense protocol Version 1. If you are using Websense protocol Version 1, let Websense run to accumulate logs so you can view the Websense accounting information. After you get a usage profile that meets your security needs, enter the **url-cache** command to increase throughput. Accounting logs are updated for Websense protocol Version 4 and for N2H2 URL filtering while using the **url-cache** command.

Examples

The following example clears the URL cache statistics:

```
hostname# clear url-cache statistics
```

Related Commands

Commands	Description
filter url	Directs traffic to a URL filtering server.
show url-cache statistics	Displays information about the URL cache, which is used for buffering URLs while waiting for responses from an N2H2 or Websense filtering server.
url-block	Manages the URL buffers used for web server responses while waiting for a filtering decision from the filtering server.

url-cache	Enables URL caching while pending responses from an N2H2 or Websense server and sets the size of the cache.
url-server	Identifies an N2H2 or Websense server for use with the filter command.

clear url-server

To clear URL filtering server statistics, use the **clear url-server** command in privileged EXEC mode.

clear url-server statistics

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values.

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

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

Command History	Release	Modification
	Preexisting	This command was preexisting.

Usage Guidelines The **clear url-server** command removes URL filtering server statistics from the configuration.

Examples The following example clears the URL server statistics:

```
hostname# clear url-server statistics
```

Related Commands	Commands	Description
	filter url	Directs traffic to a URL filtering server.
	show url-server	Displays information about the URL cache, which is used for buffering URLs while waiting for responses from an N2H2 or Websense filtering server.
	url-block	Manages the URL buffers used for web server responses while waiting for a filtering decision from the filtering server.
	url-cache	Enables URL caching while pending responses from an N2H2 or Websense server and sets the size of the cache.
	url-server	Identifies an N2H2 or Websense server for use with the filter command.

clear xlate

To clear current translation and connection information, use the **clear xlate** command in privileged EXEC mode.

```
clear xlate [global ip1[-ip2] [netmask mask]] [local ip1[-ip2] [netmask mask]]
               [gport port1[-port2]] [lport port1[-port2]] [interface if_name] [state state]
```

Syntax Description

global <i>ip1</i> [- <i>ip2</i>]	(Optional) Clears the active translations by global IP address or range of addresses.
gport <i>port1</i> [- <i>port2</i>]	(Optional) Clears the active translations by the global port or range of ports.
interface <i>if_name</i>	(Optional) Displays the active translations by interface.
local <i>ip1</i> [- <i>ip2</i>]	(Optional) Clears the active translations by local IP address or range of addresses.
lport <i>port1</i> [- <i>port2</i>]	(Optional) Clears the active translations by local port or range of ports.
netmask <i>mask</i>	(Optional) Specifies the network mask to qualify the global or local IP addresses.
state <i>state</i>	(Optional) Clears the active translations by state. You can enter one or more of the following states: <ul style="list-style-type: none"> • static—specifies static translations. • portmap—specifies PAT global translations. • norandomseq—specifies a nat or static translation with the norandomseq setting. • identity—specifies nat 0 identity address translations. When specifying more than one state, separate the states with a space.

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		
	Routed	Transparent	Single	Multiple Context	System
Privileged EXEC	•	•	•	•	•

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

The **clear xlate** command clears the contents of the translation slots (“xlate” refers to the translation slot). Translation slots can persist after key changes have been made. Always use the **clear xlate** command after adding, changing, or removing the **aaa-server**, **access-list**, **alias**, **global**, **nat**, **route**, or **static** commands in your configuration.

An xlate describes a NAT or PAT session. These sessions can be viewed with the **show xlate** command with the **detail** option. There are two types of xlates: static and dynamic.

A static xlate is a persistent xlate that is created using the **static** command. The **clear xlate** command does not clear for a host in a static entry. Static xlates can only be removed by removing the **static** command from the configuration; the **clear xlate** does not remove the static translation rule. If you remove a **static** command from the configuration, preexisting connections that use the static rule can still forward traffic. Use the **clear local-host** to deactivate these connections.

A dynamic xlate is an xlate that is created on demand with traffic processing (through the **nat** or **global** command). The **clear xlate** removes dynamic xlates and their associated connections. You can also use the **clear local-host** command to clear the xlate and associated connections. If you remove a **nat** or a **global** command from the configuration, the dynamic xlate and associated connections may remain active. Use the **clear xlate** or the **clear local-host** command to remove these connections.

Examples

The following example shows how to clear the current translation and connection slot information:

```
hostname# clear xlate global
```

Related Commands

Command	Description
clear local-host	Clears local host network information.
clear uauth	Clears cached user authentication and authorization information.
show conn	Displays all active connections.
show local-host	Displays the local host network information.
show xlate	Displays the current translation information.

client-access-rule

To configure rules that limit the remote access client types and versions that can connect via IPSec through the security appliance, use the **client-access-rule** command in group-policy configuration mode. To delete a rule, use the **no** form of this command.

To delete all rules, use the **no client-access-rule command** with only the priority argument. This deletes all configured rules, including a null rule created by issuing the **client-access-rule none** command.

When there are no client access rules, users inherit any rules that exist in the default group policy. To prevent users from inheriting client access rules, use the **client-access-rule none** command. The result of doing so is that all client types and versions can connect.

client-access-rule *priority* {**permit** | **deny**} **type** *type* **version** *version* | **none**

no client-access-rule *priority* [{**permit** | **deny**} **type** *type* **version** *version*]

Syntax Description

deny	Denies connections for devices of a particular type and/or version.
none	Allows no client access rules. Sets client-access-rule to a null value, thereby allowing no restriction. Prevents inheriting a value from a default or specified group policy.
permit	Permits connections for devices of a particular type and/or version.
<i>priority</i>	Determines the priority of the rule. The rule with the lowest integer has the highest priority. Therefore, the rule with the lowest integer that matches a client type and/or version is the rule that applies. If a lower priority rule contradicts, the security appliance ignores it.
type <i>type</i>	Identifies device types via free-form strings, for example VPN 3002. A string must match exactly its appearance in the show vpn-sessiondb remote display, except that you can use the * character as a wildcard.
version <i>version</i>	Identifies the device version via free-form strings, for example 7.0. A string must match exactly its appearance in the show vpn-sessiondb remote display, except that you can use the * character as a wildcard.

Defaults

By default, there are no access rules.

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
Global configuration	•	—	•	—	—

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

Construct rules according to these caveats:

- If you do not define any rules, the security appliance permits all connection types.
- When a client matches none of the rules, the security appliance denies the connection. This means that if you define a deny rule, you must also define at least one permit rule, or the security appliance denies all connections.
- For both software and hardware clients, type and version must match exactly their appearance in the **show vpn-sessiondb remote** display.
- The * character is a wildcard, which you can use multiple times in each rule. For example, **client-access-rule 3 deny type * version 3.*** creates a priority 3 client access rule that denies all client types running release versions 3.x software.
- You can construct a maximum of 25 rules per group policy.
- There is a limit of 255 characters for an entire set of rules.
- You can use n/a for clients that do not send client type and/or version.

Examples

The following example shows how to create client access rules for the group policy named FirstGroup. These rules permit VPN Clients running software version 4.1, while denying all VPN 3002 hardware clients:

```
hostname(config)# group-policy FirstGroup attributes  
hostname(config-group-policy)# client-access-rule 1 d t VPN3002 v *  
hostname(config-group-policy)# client-access-rule 2 p * v 4.1
```

client-firewall

To set personal firewall policies that the security appliance pushes to the VPN Client during IKE tunnel negotiation, use the **client-firewall** command in group-policy configuration mode. To delete a firewall policy, use the **no** form of this command.

When there are no firewall policies, users inherit any that exist in the default or other group policy. To prevent users from inheriting such firewall policies, use the **client-firewall none** command.

client-firewall none

client-firewall opt | req custom vendor-id *num* product-id *num* policy AYT | {CPP acl-in *ACL* acl-out *ACL*} [description *string*]

client-firewall opt | req zonelabs-zonealarm policy AYT | {CPP acl-in *ACL* acl-out *ACL*}

client-firewall opt | req zonelabs-zonealarmpro policy AYT | {CPP acl-in *ACL* acl-out *ACL*}

client-firewall opt | req zonelabs-zonealarmpro policy AYT | {CPP acl-in *ACL* acl-out *ACL*}

client-firewall opt | req cisco-integrated acl-in *ACL* acl-out *ACL*

client-firewall opt | req sygate-personal

client-firewall opt | req sygate-personal-pro

client-firewall opt | req sygate-security-agent

client-firewall opt | req networkice-blackice

client-firewall opt | req cisco-security-agent

Syntax Description

acl-in <ACL>	Provides the policy the client uses for inbound traffic
acl-out <ACL>	Provides the policy the client uses for outbound traffic
AYT	Specifies that the client PC firewall application controls the firewall policy. The security appliance checks to make sure the firewall is running. It asks, "Are You There?" If there is no response, the security appliance tears down the tunnel.
cisco-integrated	Specifies Cisco Integrated firewall type.
cisco-security-agent	Specifies Cisco Intrusion Prevention Security Agent firewall type
CPP	Specifies Policy Pushed as source of the VPN Client firewall policy
custom	Specifies Custom firewall type.
description <string>	Describes the firewall.
networkice-blackice	Specifies Network ICE Black ICE firewall type
none	Indicates that there is no client firewall policy. Sets a firewall policy with a null value, thereby disallowing one. Prevents inheriting a firewall policy from a default or specified group policy.
opt	Indicates an optional firewall type.
product-id	Identifies the firewall product
req	Indicates a required firewall type

sygate-personal	Specifies Sygate Personal firewall type
sygate-personal-pro	Specifies Sygate Personal Pro firewall type
sygate-security-agent	Specifies Sygate Security Agent firewall type
vendor-id	Identifies the firewall vendor
zonelabs-zonealarm	Specifies Zone Labs Zone Alarm firewall type
zonelabs-zonealarmorpro policy	Specifies Zone Labs Zone Alarm or Pro firewall type
zonelabs-zonealarmpro policy	Specifies Zone Labs Zone Alarm Pro firewall type

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		
	Routed	Transparent	Single	Multiple	
				Context	System
Group-policy	•	—	•	—	—

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

Only one instance of this command can be configured.

Examples

The following example shows how to set a client firewall policy that requires Cisco Intrusion Prevention Security Agent for the group policy named FirstGroup:

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# client-firewall req cisco-security-agent
```

client-update

To configure and change client update parameters, use the **client-update** command in tunnel-group ipsec-attributes configuration mode. If the client is already running a software version on the list of revision numbers, it does not need to update its software. If the client is not running a software version on the list, it should update. You can specify up to 4 of these client update entries.

To disable a client update, use the **no** form of this command.

client-update *type* {**url** *url-string*} {**rev-nums** *rev-nums*}

no client-update [*type*]

Syntax Description

rev-nums <i>rev-nums</i>	Specifies the software or firmware images for this client. Enter up to 4, separated by commas.
<i>type</i>	Specifies the operating systems to notify of a client update. The list of operating systems comprises the following: <ul style="list-style-type: none"> Windows: all windows-based platforms WIN9X: Windows 95, Windows 98, and Windows ME platforms WinNT: Windows NT 4.0, Windows 2000, and Windows XP platforms vpn3002: VPN 3002 hardware client
url <i>url-string</i>	Specifies the URL for the software/firmware image. This URL must point to a file appropriate for this client.

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		
	Routed	Transparent	Single	Multiple	
				Context	System
Tunnel-group ipsec attributes configuration	•	—	•	—	—

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

You can apply this attribute to IPSec remote-access tunnel-group type only.

Examples

The following example entered in config-ipsec configuration mode, configures client update parameters for the remote-access tunnel-group remotegrp. It designates the revision number, 4.6.1 and the URL for retrieving the update, which is https://support/updates.

```
hostname(config)# tunnel-group remotegrp type ipsec_ra
hostname(config)# tunnel-group remotegrp ipsec-attributes
hostname(config-ipsec)# client-update type windows url https://support/updates/ rev-nums
4.6.1
hostname(config-ipsec)#
```

Related Commands

Command	Description
clear configure tunnel-group	Clears all configured tunnel groups.
show running-config tunnel-group	Shows the indicated certificate map entry.
tunnel-group-map enable	Associates the certificate map entries created using the crypto ca certificate map command with tunnel groups.

clock set

To manually set the clock on the security appliance, use the **clock set** command in privileged EXEC mode.

clock set *hh:mm:ss {month day | day month} year*

Syntax Description

<i>day</i>	Sets the day of the month, from 1 to 31. You can enter the day and month as april 1 or as 1 april , for example, depending on your standard date format.
<i>hh:mm:ss</i>	Sets the hour, minutes, and seconds in 24-hour time. For example, set 20:54:00 for 8:54 pm.
<i>month</i>	Sets the month. Depending on your standard date format, you can enter the day and month as april 1 or as 1 april .
<i>year</i>	Sets the year using four digits, for example, 2004 . The year range is 1993 to 2035.

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		
	Routed	Transparent	Single	Multiple Context	System
Privileged EXEC	•	•	•	—	•

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

If you have not entered any **clock** configuration commands, the default time zone for the **clock set** command is UTC. If you change the time zone after you enter the **clock set** command using the **clock timezone** command, the time automatically adjusts to the new time zone. However, if you enter the **clock set** command after you establish the time zone with the **clock timezone** command, then enter the time appropriate for the new time zone and not for UTC. Similarly, if you enter the **clock summer-time** command after the **clock set** command, the time adjusts for daylight saving. If you enter the **clock set** command after the **clock summer-time** command, enter the correct time for daylight saving.

This command sets the time in the hardware chip, and does not save the time in the configuration file. This time endures reboots. Unlike the other **clock** commands, this command is a privileged EXEC command. To reset the clock, you need to set a new time for the **clock set** command.

Examples

The following example sets the time zone to MST, the daylight saving time to the default period in the U.S., and the current time for MDT to 1:15 p.m. on July 27, 2004:

```
hostname(config)# clock timezone MST -7
hostname(config)# clock summer-time MDT recurring
hostname(config)# exit
hostname# clock set 13:15:0 jul 27 2004
hostname# show clock
13:15:00.652 MDT Tue Jul 27 2004
```

The following example sets the clock to 8:15 on July 27, 2004 in the UTC time zone, and then sets the time zone to MST and the daylight saving time to the default period in the U.S. The end time (1:15 in MDT) is the same as the previous example.

```
hostname# clock set 20:15:0 jul 27 2004
hostname# configure terminal
hostname(config)# clock timezone MST -7
hostname(config)# clock summer-time MDT recurring
hostname# show clock
13:15:00.652 MDT Tue Jul 27 2004
```

Related Commands

Command	Description
clock summer-time	Sets the date range to show daylight saving time.
clock timezone	Sets the time zone.
show clock	Shows the current time.

clock summer-time

To set the date range for daylight saving time for the display of the security appliance time, use the **clock summer-time** command in global configuration mode. To disable the daylight saving time dates, use the **no** form of this command.

clock summer-time *zone* **recurring** [*week weekday month hh:mm week weekday month hh:mm*]
[*offset*]

no clock summer-time [*zone recurring [week weekday month hh:mm week weekday month hh:mm]*
[*offset*]]

clock summer-time *zone* **date** {*day month \ month day*} *year hh:mm {day month \ month day} year*
hh:mm [*offset*]

no clock summer-time [*zone date {day month \ month day} year hh:mm {day month \ month day}*
year hh:mm [*offset*]]

Syntax Description

date	Specifies the start and end dates for daylight saving time as a specific date in a specific year. If you use this keyword, you need to reset the dates every year.
<i>day</i>	Sets the day of the month, from 1 to 31. You can enter the day and month as April 1 or as 1 April , for example, depending on your standard date format.
<i>hh:mm</i>	Sets the hour and minutes in 24-hour time.
<i>month</i>	Sets the month as a string. For the date command, you can enter the day and month as April 1 or as 1 April , for example, depending on your standard date format.
<i>offset</i>	(Optional) Sets the number of minutes to change the time for daylight saving time. By default, the value is 60 minutes.
recurring	Specifies the start and end dates for daylight saving time, in the form of a day and time of the month, and not a specific date in a year. This keyword lets you set a recurring date range that you do not need to alter yearly. If you do not specify any dates, the security appliance uses the default date range for the United States: 2:00 a.m. on the first Sunday in April to 2:00 a.m. on the last Sunday in October.
<i>week</i>	(Optional) Specifies the week of the month as an integer between 1 and 4 or as the words first or last . For example, if the day might fall in the partial fifth week, then specify last .
<i>weekday</i>	(Optional) Specifies the day of the week: Monday , Tuesday , Wednesday , and so on.
<i>year</i>	Sets the year using four digits, for example, 2004 . The year range is 1993 to 2035.
<i>zone</i>	Specifies the time zone as a string, for example, PDT for Pacific Daylight Time. When the security appliance shows the daylight saving time according to the date range you set with this command, the time zone changes to the value you set here. See the clock timezone to set the base time zone to a zone other than UTC.

Defaults

The default offset is 60 minutes.

The default recurring date range is from 2:00 a.m. on the first Sunday in April to 2:00 a.m. on the last Sunday in October.

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
Global configuration	•	•	•	—	•

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

For the Southern Hemisphere, the security appliance accepts the start month to be later in the year than the end month, for example, from October to March.

Examples

The following example sets the daylight saving date range for Australia:

```
hostname(config)# clock summer-time PDT recurring last Sunday October 2:00 last Sunday
March 2:00
```

Some countries start daylight saving on a specific date. In the following example, daylight saving time is configured to start on April 1, 2004, at 3 a.m. and end on October 1, 2004, at 4 a.m.

```
hostname(config)# clock summer-time UTC date 1 April 2004 3:00 1 October 2004 4:00
```

Related Commands

Command	Description
clock set	Manually sets the clock on the security appliance.
clock timezone	Sets the time zone.
ntp server	Identifies an NTP server.
show clock	Shows the current time.

clock timezone

To set the time zone for the security appliance clock, use the **clock timezone** command in global configuration mode. To set the time zone back to the default of UTC, use the **no** form of this command. The **clock set** command or the time derived from an NTP server sets the time in UTC. You must set the time zone as an offset of UTC using this command.

clock timezone *zone* [-]*hours* [*minutes*]

no clock timezone [*zone* [-]*hours* [*minutes*]]

Syntax Description

<i>zone</i>	Specifies the time zone as a string, for example, PST for Pacific Standard Time.
[-] <i>hours</i>	Sets the number of hours of offset from UTC. For example, PST is -8 hours.
<i>minutes</i>	(Optional) Sets the number of minutes of offset from UTC.

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		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	•	•	•	—	•

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

To set daylight saving time, see the **clock summer-time** command.

Examples

The following example sets the time zone to Pacific Standard Time, which is -8 hours from UTC:

```
hostname(config)# clock timezone PST -8
```

Related Commands

Command	Description
clock set	Manually sets the clock on the security appliance.
clock summer-time	Sets the date range to show daylight saving time.

Command	Description
ntp server	Identifies an NTP server.
show clock	Shows the current time.

cluster encryption

To enable encryption for messages exchanged on the virtual load-balancing cluster, use the **cluster encryption** command in VPN load-balancing mode. To disable encryption, use the **no** form of this command.

cluster encryption

no cluster encryption



Note

VPN load balancing requires an active 3DES/AES license. The security appliance checks for the existence of this crypto license before enabling load balancing. If it does not detect an active 3DES or AES license, the security appliance prevents the enabling of load balancing and also prevents internal configuration of 3DES by the load balancing system unless the license permits this usage.

Syntax Description

This command has no arguments or variables.

Defaults

Encryption is disabled by default.

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
VPN load-balancing mode	•	—	•	—	—

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

This command turns encryption on or off for messages exchanged on the virtual load-balancing cluster.

Before configuring the **cluster encryption** command, you must have first used the **vpn load-balancing** command to enter VPN load-balancing mode. You must also use the **cluster key** command to configure the cluster shared-secret key before enabling cluster encryption.



Note

When using encryption, you must first configure 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 will get an error message when you try to configure cluster encryption.

Examples

The following is an example of a VPN load-balancing command sequence that includes a **cluster encryption** command that enables encryption for the virtual 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)# cluster key 123456789
hostname(config-load-balancing)# cluster encryption
hostname(config-load-balancing)# participate
```

Related Commands

Command	Description
cluster key	Specifies the shared-secret key for the cluster.
vpn load-balancing	Enters VPN load-balancing mode.

cluster ip address

To set the IP address of the virtual load-balancing cluster, use the **cluster ip address** command in VPN load-balancing mode. To remove the IP address specification, use the **no** form of this command.

cluster ip address *ip-address*

no cluster ip address [*ip-address*]

Syntax Description

ip-address The IP address that you want to assign to the virtual load-balancing cluster.

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		
	Routed	Transparent	Single	Multiple	
				Context	System
VPN load-balancing mode	•	—	•	—	—

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

You must first use the **vpn load-balancing** command to enter VPN load-balancing mode and configure the interface to which the virtual cluster IP address refers.

The cluster ip address must be on the same subnet as the interface for which you are configuring the virtual cluster.

In the **no** form of the command, if you specify the optional *ip-address* value, it must match the existing cluster IP address before the **no cluster ip address** command can be completed.

Examples

The following is an example of a VPN load-balancing command sequence that includes a **cluster ip address** command that sets the IP address of the virtual load-balancing cluster to 209.165.202.224:

```
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 Commands

Command	Description
interface	Sets the interfaces of the device.
nameif	Assigns a name to an interface.
vpn load-balancing	Enters VPN load-balancing mode.

cluster key

To set the shared secret for IPSec site-to-site tunnel exchanges on the virtual load-balancing cluster, use the **cluster key** command in VPN load-balancing mode. To remove this specification, use the **no** form of this command.

cluster key *shared-secret*

no cluster key [*shared-secret*]

Syntax Description

shared-secret A string defining the shared secret for the VPN load-balancing cluster.

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		
	Routed	Transparent	Single	Multiple Context	System
VPN load-balancing mode	•	—	•	—	—

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

You must first use the **vpn load-balancing** command to enter VPN load-balancing mode. The secret defined in the **cluster key** command is also used for cluster encryption.

You must use the **cluster key** command to configure the shared secret before enabling cluster encryption.

If you specify a value for *shared-secret* in the **no cluster key** form of the command, the shared secret value must match the existing configuration.

Examples

The following is an example of a VPN load-balancing command sequence that includes a **cluster key** command that sets the shared secret of the virtual load-balancing cluster to 123456789:

```
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)# cluster key 123456789  
hostname(config-load-balancing)# cluster encryption  
hostname(config-load-balancing)# participate
```

Related Commands

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

cluster port

To set the UDP port for the virtual load-balancing cluster, use the **cluster port** command in VPN load-balancing mode. To remove the port specification, use the **no** form of this command.

cluster port *port*

no cluster port [*port*]

Syntax Description

port The UDP port that you want to assign to the virtual load-balancing cluster.

Defaults

The default cluster port is 9023.

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
VPN load-balancing mode	•	—	•	—	—

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

You must first use the **vpn load-balancing** command to enter VPN load-balancing mode.

You can specify any valid UDP port number. The range is 1-65535.

If you specify a value for *port* in the **no cluster port** form of the command, the port number specified must match the existing configured port number.

Examples

The following is an example of a VPN load-balancing command sequence that includes a **cluster port address** command that sets the UDP port for the virtual load-balancing cluster to 9023:

```
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)# cluster port 9023
hostname(config-load-balancing)# participate
```

Related Commands

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

command-alias

To create an alias for a command, use the **command-alias** command in global configuration mode. To remove the alias, use the **no** form of this command. When you enter the command alias, the original command is invoked. You might want to create command aliases to provide shortcuts for long commands, for example.

command-alias *mode command_alias original_command*

no command-alias *mode command_alias original_command*

Syntax Description

<i>mode</i>	Specifies the command mode in which you want to create the command alias, for example exec (for user and privileged EXEC modes), configure , or interface .
<i>command_alias</i>	Specifies the new name you want for an existing command.
<i>original_command</i>	Specifies the existing command or command with its keywords for which you want to create the command alias.

Defaults

By default, the following user EXEC mode aliases are configured:

h for **help**

lo for **logout**

p for **ping**

s for **show**

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
Global configuration	•	•	•	•	•

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

You can create an alias for the first part of any command and still enter the additional keywords and arguments as normal.

When you use CLI help, command aliases are indicated by an asterisk (*), and displayed in the following format:

*command-alias=original-command

For example, the **lo** command alias displays along with other privileged EXEC mode commands that start with “lo,” as follows:

```
hostname# lo?
*lo=logout login logout
```

You can use the same alias in different modes. For example, you can use “happy” in privileged EXEC mode and configuration mode to alias different commands, as follows:

```
hostname(config)# happy?

configure mode commands/options:
*happy="username crichton password test"

exec mode commands/options:
*happy=enable
```

To list only commands and omit aliases, begin your input line with a space. Also, to circumvent command aliases, use a space before entering the command. In the following example, the alias happy is not shown, because there is a space before the happy? command.

```
hostname(config)# alias exec test enable
hostname(config)# exit
hostname# happy?
ERROR: % Unrecognized command
```

As with commands, you can use CLI help to display the arguments and keywords that can follow a command alias.

You must enter the complete command alias. Shortened aliases are not accepted. In the following example, the parser does not recognize the command hap as indicating the alias happy:

```
hostname# hap
% Ambiguous command: "hap"
```

Examples

The following example shows how to create a command alias named “save” for the **copy running-config startup-config** command:

```
hostname(config)# command-alias exec save copy running-config startup-config
hostname(config)# exit
hostname# save
```

```
Source filename [running-config]?
Cryptochecksum: 50d131d9 8626c515 0c698f7f 613ae54e
```

```
2209 bytes copied in 0.210 secs
hostname#
```

Related Commands

Command	Description
clear configure command-alias	Clears all non-default command aliases.
show running-config command-alias	Displays all non-default command aliases configured.

command-queue

To specify the maximum number of MGCP commands that are queued while waiting for a response, use the **command-queue** command in MGCP map configuration mode. To remove the configuration, use the **no** form of this command.

command-queue *limit*

no command-queue *limit*

Syntax Description

limit Specifies the maximum number of commands to queue, from 1 to 2147483647.

Defaults

This command is disabled by default.

The default for the MGCP command queue is 200.

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
MGCP map configuration	•	•	•	•	No

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

Use the **command-queue** command to specify the maximum number of MGCP commands that are queued while waiting for a response. The range of allowed values is from 1 to 4294967295. The default is 200. When the limit has been reached and a new command arrives, the command that has been in the queue for the longest time is removed.

Examples

The following example limits the MGCP command queue to 150 commands:

```
hostname(config)# mgcp-map mgcp_policy
hostname(config-mgcp-map)#command-queue 150
```

Related Commands

Commands	Description
debug mgcp	Enables the display of debug information for MGCP.
mgcp-map	Defines an MGCP map and enables MGCP map configuration mode.
show mgcp	Displays MGCP configuration and session information.

Commands	Description
timeout mgcp	Configures the idle timeout after which an MGCP media connection will be closed.
timeout mgcp-pat	Configures the idle timeout after which an MGCP PAT xlate will be removed.

compatible rfc1583

To restore the method that is used to calculate the summary route costs per RFC 1583, use the **compatible rfc1583** command in router configuration mode. To disable RFC 1583 compatibility, use the **no** form of this command.

compatible rfc1583

no compatible rfc1583

Syntax Description

This command has no arguments or keywords.

Defaults

This command is enabled by default.

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
Router configuration	•	—	•	—	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

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

Examples

The following example shows how to disable RFC 1583-compatible route summary cost calculation:

```
hostname(config-router)# no compatible rfc1583
hostname(config-router)#
```

Related Commands

Command	Description
router ospf	Enters router configuration mode.
show running-config router	Displays the commands in the global router configuration.

config-register

To set the configuration register value that is used the next time you reload the security appliance, use the **config-register** command in global configuration mode. To set the value back to the default, use the **no** form of this command. This command is only supported on the ASA 5500 adaptive security appliance. The configuration register value determines which image to boot from as well as other boot parameters.

config-register *hex_value*

no config-register

Syntax Description

hex_value

Sets the configuration register value as a hexadecimal number from 0x0 to 0xFFFFFFFF. This number represents 32 bits and each hexadecimal character represents 4 bits. Each bit controls a different characteristic. However, bits 32 through 20 are either reserved for future use, cannot be set by the user, or are not currently used by the security appliance; therefore, you can ignore the three characters that represent those bits, because they are always set to 0. The relevant bits are represented by 5 hexadecimal characters: 0xnnnnn.

You do not need to include preceding 0s. You do need to include trailing 0s. For example, 0x2001 is equivalent to 0x02001; but 0x10000 requires all the zeros. See [Table 3-1](#) for more information about available values for the relevant bits.

Defaults

The default value is 0x1, which boots from the local image and startup configuration.

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
Global configuration	•	•	•	—	•

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

The five characters are numbered from 0 to 4 from right to left, which is standard for hexadecimal and binary numbers. You can select one value for each character, and mix and match values as appropriate. For example, you can select either 0 or 2 for character number 3. Some values take priority if they conflict with other values. For example, if you set 0x2011, which sets the security appliance to both boot

from the TFTP server and to boot from the local image, the security appliance boots from the TFTP server. Because this value also stipulates that if the TFTP boot fails, the security appliance should boot directly into ROMMON, then the action that specifies to boot from the default image is ignored.

A value of 0 means no action unless otherwise specified.

Table 3-1 lists the actions associated with each hexadecimal character; choose one value for each character:

Table 3-1 Configuration Register Values

Prefix	Hexadecimal Character Numbers 4, 3, 2, 1, and 0				
0x	0	0	0 ¹	0 ²	0 ²
	1	2		1	1
	Disables the 10 second ROMMON countdown during startup. Normally, you can press Escape during the countdown to enter ROMMON.	If you set the security appliance to boot from a TFTP server, and the boot fails, then this value boots directly into ROMMON.		Boots from the TFTP server image as specified in the ROMMON Boot Parameters (which is the same as the boot system tftp command, if present). This value takes precedence over a value set for character 1.	Boots the image specified by the first boot system local_flash command. If that image does not load, the security appliance tries to boot each image specified by subsequent boot system commands until it boots successfully.
					3, 5, 7, 9
					Boots the image specified by a particular boot system local_flash command. Value 3 boots the image specified in the first boot system command, value 5 boots the second image, and so on.
					If the image does not boot successfully, the security appliance does not attempt to fall back to other boot system command images (this is the difference between using value 1 and value 3). However, the security appliance has a failsafe feature that in the event of a boot failure attempts to boot from any image found in the root directory of internal Flash memory. If you do not want the failsafe feature to take effect, store your images in a different directory than root.
				4³	2, 4, 6, 8
				Ignores the startup configuration and loads the default configuration.	From ROMMON, if you enter the boot command without any arguments, then the security appliance boots the image specified by a particular boot system local_flash command. Value 3 boots the image specified in the first boot system command, value 5 boots the second image, and so on. This value does not automatically boot an image.
				5	
				Performs both actions above.	

1. Reserved for future use.
2. If character numbers 0 and 1 are not set to automatically boot an image, then the security appliance boots directly into ROMMON.
3. If you disable password recovery using the **service password-recovery** command, then you cannot set the configuration register to ignore the startup configuration.

The configuration register value is not replicated to a standby unit, but the following warning is displayed when you set the configuration register on the active unit:

WARNING The configuration register is not synchronized with the standby, their values may not match.

You can also set the configuration register value in ROMMON using the **confreg** command.

Examples

The following example sets the configuration register to boot from the default image:

```
hostname(config)# config-register 0x1
```

Related Commands

Command	Description
boot	Sets the boot image and startup configuration.
service password-recovery	Enables or disables password recovery.

configure factory-default

To restore the configuration to the factory default, use the **configure factory-default** command in global configuration mode. The factory default configuration is the configuration applied by Cisco to new security appliances. This command is not supported on all platforms; see the CLI help for the **configure** command to confirm if the command is supported (enter **configure ?** at the global configuration prompt). The factory default configuration automatically configures an interface for management so you can connect to it using ASDM, with which you can then complete your configuration.

configure factory-default [*ip_address* [*mask*]]

Syntax Description

<i>ip_address</i>	Sets the IP address of the management interface, instead of using the default address, 192.168.1.1. If your platform includes a dedicated management interface, then this IP address applies to that interface. If your platform includes only data interfaces, then this address applies to the Ethernet 1 interface.
<i>mask</i>	Sets the subnet mask of the interface. If you do not set a mask, the security appliance uses the mask appropriate for the IP address class.

Defaults

The default IP address and mask are 192.168.1.1 and 255.255.255.0.

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
Global configuration	•		•		

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

The **configure factory-default** command configures the minimum commands required to connect to the security appliance using ASDM. This command is available only for routed firewall mode; transparent mode does not support IP addresses for interfaces, and setting the interface IP address is one of the actions this command takes. This command is also only available in single context mode; a security appliance with a cleared configuration does not have any defined contexts to automatically configure using this command.

This command clears the current running configuration and then configures several commands. The configured interface depends on your platform. For a platform with a dedicated management interface, the interface is named “management.” For other platforms, the configured interface is Ethernet 1 and named “inside.”

The following commands apply to the dedicated management interface, Management 0/0 (for a platform without a dedicated management interface, the interface is Ethernet 1):

```
interface management 0/0
  ip address 192.168.1.1 255.255.255.0
  nameif management
  security-level 100
  no shutdown
asdm logging informational 100
asdm history enable
http server enable
http 192.168.1.0 255.255.255.0 management
dhcpd address 192.168.1.2-192.168.1.254 management
dhcpd lease 3600
dhcpd ping_timeout 750
dhcpd enable management
```

If you set the IP address in the **configure factory-default** command, then the **http** command uses the subnet you specify. Similarly, the **dhcpd address** command range consists of addresses within the subnet that you specify.

After you restore the factory default configuration, save it to internal Flash memory using the **copy running-config startup-config** command. The **copy** command saves the running configuration to the default location for the startup configuration, even if you previously configured the **boot config** command to set a different location; when the configuration was cleared, this path was also cleared.



Note

This command also clears the **boot system** command, if present, along with the rest of the configuration. The **boot system** command lets you boot from a specific image, including an image on the external Flash memory card. The next time you reload the security appliance after restoring the factory configuration, it boots from the first image in internal Flash memory; if you do not have an image in internal Flash memory, the security appliance does not boot.

To configure additional settings that are useful for a full configuration, see the **setup** command.

Examples

The following example resets the configuration to the factory default, assigns the IP address 10.1.1.1 to the interface, and then saves the new configuration as the startup configuration:

```
hostname(config)# configure factory-default 10.1.1.1 255.255.255.0
Based on the inside IP address and mask, the DHCP address
pool size is reduced to 253 from the platform limit 256
```

```
WARNING: The boot system configuration will be cleared.
The first image found in disk0:/ will be used to boot the
system on the next reload.
Verify there is a valid image on disk0:/ or the system will
not boot.
```

```
Begin to apply factory-default configuration:
Clear all configuration
...
hostname(config)#
hostname(config)# copy running-config startup-config
```

Related Commands	Command	Description
	boot system	Sets the software image from which to boot.
	clear configure	Clears the running configuration.
	copy running-config startup-config	Copies the running configuration to the startup configuration.
	setup	Prompts you to configure basic settings for the security appliance.
	show running-config	Shows the running configuration.

configure http

To merge a configuration file from an HTTP(S) server with the running configuration, use the **configure http** command in global configuration mode. This command supports IPv4 and IPv6 addresses.

configure http[s]://[user[:password]@]server[:port]/[path/]filename

Syntax Description

:password	(Optional) For HTTP(S) authentication, specifies the password.
:port	(Optional) Specifies the port. For HTTP, the default is 80. For HTTPS, the default is 443.
@	(Optional) If you enter a name and/or a password, precedes the server IP address with an at sign (@).
filename	Specifies the configuration filename.
http[s]	Specifies either HTTP or HTTPS.
path	(Optional) Specifies a path to the filename.
server	Specifies the server IP address or name. For IPv6 server addresses, if you specify the port, then you must enclose the IP address in brackets so that the colons in the IP address are not mistaken for the colon before the port number. For example, enter the following address and port: [fe80::2e0:b6ff:fe01:3b7a]:8080
user	(Optional) For HTTP(S) authentication, specifies the username.

Defaults

For HTTP, the default port is 80. For HTTPS, the default port is 443.

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
Global configuration	•	•	•	•	•

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

A merge adds all commands from the new configuration to the running configuration, and overwrites any conflicting commands with the new versions. For example, if a command allows multiple instances, the new commands are added to the existing commands in the running configuration. If a command allows only one instance, the new command overwrites the command in the running configuration. A merge never removes commands that exist in the running configuration but are not set in the new configuration.

This command is the same as the **copy http running-config** command. For multiple context mode, that command is only available in the system execution space, so the **configure http** command is an alternative for use within a context.

Examples

The following example copies a configuration file from an HTTPS server to the running configuration:

```
hostname(config)# configure https://user1:pa$$w0rd@10.1.1.1/configs/newconfig.cfg
```

Related Commands

Command	Description
clear configure	Clears the running configuration.
configure memory	Merges the startup configuration with the running configuration.
configure net	Merges a configuration file from the specified TFTP URL with the running configuration.
configure factory-default	Adds commands you enter at the CLI to the running configuration.
show running-config	Shows the running configuration.

configure memory

To merge the startup configuration with the running configuration, use the **configure memory** command in global configuration mode.

configure memory

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

A merge adds all commands from the new configuration to the running configuration, and overwrites any conflicting commands with the new versions. For example, if a command allows multiple instances, the new commands are added to the existing commands in the running configuration. If a command allows only one instance, the new command overwrites the command in the running configuration. A merge never removes commands that exist in the running configuration but are not set in the new configuration.

If you do not want to merge the configurations, you can clear the running configuration, which disrupts any communications through the security appliance, and then enter the **configure memory** command to load the new configuration.

This command is equivalent to the **copy startup-config running-config** command.

For multiple context mode, a context startup configuration is at the location specified by the **config-url** command.

Examples

The following example copies the startup configuration to the running configuration:

```
hostname(config)# configure memory
```

Related Commands	Command	Description
	clear configure	Clears the running configuration.
	configure http	Merges a configuration file from the specified HTTP(S) URL with the running configuration.
	configure net	Merges a configuration file from the specified TFTP URL with the running configuration.
	configure factory-default	Adds commands you enter at the CLI to the running configuration.
	show running-config	Shows the running configuration.

configure net

To merge a configuration file from a TFTP server with the running configuration, use the **configure net** command in global configuration mode. This command supports IPv4 and IPv6 addresses.

configure net [*server:[filename]* | *:filename*]

Syntax Description

<i>:filename</i>	<p>Specifies the path and filename. If you already set the filename using the tftp-server command, then this argument is optional.</p> <p>If you specify the filename in this command as well as a name in the tftp-server command, the security appliance treats the tftp-server command filename as a directory, and adds the configure net command filename as a file under the directory.</p> <p>To override the tftp-server command value, enter a slash in front of the path and filename. The slash indicates that the path is not relative to the tftpboot directory, but is an absolute path. The URL generated for this file includes a double slash (//) in front of the filename path. If the file you want is in the tftpboot directory, you can include the path for the tftpboot directory in the filename path.</p> <p>If you specified the TFTP server address using the tftp-server command, you can enter the filename alone preceded by a colon (:).</p>
<i>server:</i>	<p>Sets the TFTP server IP address or name. This address overrides the address you set in the tftp-server command, if present. For IPv6 server addresses, you must enclose the IP address in brackets so that the colons in the IP address are not mistaken for the colon before the filename. For example, enter the following address:</p> <p>[fe80::2e0:b6ff:fe01:3b7a]</p> <p>The default gateway interface is the highest security interface; however, you can set a different interface name using the tftp-server command.</p>

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		
	Routed	Transparent	Single	Multiple Context	System
Global configuration	•	•	•	•	•

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

A merge adds all commands from the new configuration to the running configuration, and overwrites any conflicting commands with the new versions. For example, if a command allows multiple instances, the new commands are added to the existing commands in the running configuration. If a command allows only one instance, the new command overwrites the command in the running configuration. A merge never removes commands that exist in the running configuration but are not set in the new configuration.

This command is the same as the **copy tftp running-config** command. For multiple context mode, that command is only available in the system execution space, so the **configure net** command is an alternative for use within a context.

Examples

The following example sets the server and filename in the **tftp-server** command, and then overrides the server using the **configure net** command. The same filename is used.

```
hostname(config)# tftp-server inside 10.1.1.1 configs/config1
hostname(config)# configure net 10.2.2.2:
```

The following example overrides the server and the filename. The default path to the filename is /tftpboot/configs/config1. The /tftpboot/ part of the path is included by default when you do not lead the filename with a slash (/). Because you want to override this path, and the file is also in tftpboot, include the tftpboot path in the **configure net** command.

```
hostname(config)# tftp-server inside 10.1.1.1 configs/config1
hostname(config)# configure net 10.2.2.2:/tftpboot/oldconfigs/config1
```

The following example sets the server only in the **tftp-server** command. The **configure net** command specifies only the filename.

```
hostname(config)# tftp-server inside 10.1.1.1
hostname(config)# configure net :configs/config1
```

Related Commands

Command	Description
configure http	Merges a configuration file from the specified HTTP(S) URL with the running configuration.
configure memory	Merges the startup configuration with the running configuration.
show running-config	Shows the running configuration.
tftp-server	Sets a default TFTP server and path for use in other commands.
write net	Copies the running configuration to a TFTP server.

configure terminal

To configure the running configuration at the command line, use the **configure terminal** command in privileged EXEC mode. This command enters global configuration mode, which lets you enter commands that change the configuration.

configure terminal

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values.

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

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

Command History

Release	Modification
Preexisting	This command was preexisting.

Examples The following example enters global configuration mode:

```
hostname# configure terminal
hostname(config)#
```

Related Commands	Command	Description
	clear configure	Clears the running configuration.
	configure http	Merges a configuration file from the specified HTTP(S) URL with the running configuration.
	configure memory	Merges the startup configuration with the running configuration.
	configure net	Merges a configuration file from the specified TFTP URL with the running configuration.
	show running-config	Shows the running configuration.

config-url

To identify the URL from which the system downloads the context configuration, use the **config-url** command in context configuration mode.

config-url *url*

Syntax Description

<i>url</i>	<p>Sets the context configuration URL. All remote URLs must be accessible from the admin context. See the following URL syntax:</p> <ul style="list-style-type: none"> • disk0:<i>/[path/]filename</i> For the ASA 5500 series adaptive security appliance, this URL indicates the internal Flash memory. You can also use flash instead of disk0; they are aliased. • disk1:<i>/[path/]filename</i> For the ASA 5500 series adaptive security appliance, this URL indicates the external Flash memory card. • flash:<i>/[path/]filename</i> This URL indicates the internal Flash memory. • ftp:<i>//[user[:password]@]server[:port]/[path/]filename[;type=xx]</i> The type can be one of the following keywords: <ul style="list-style-type: none"> – ap—ASCII passive mode – an—ASCII normal mode – ip—(Default) Binary passive mode – in—Binary normal mode • http[s]:<i>//[user[:password]@]server[:port]/[path/]filename</i> • tftp:<i>//[user[:password]@]server[:port]/[path/]filename[;int=interface_name]</i> Specify the interface name if you want to override the route to the server address.
------------	---

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		
	Routed	Transparent	Single	Multiple	
				Context	System
Context configuration	•	•	—	—	•

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines**Note**

When you add a context URL, the system immediately loads the context so that it is running.

Enter the **allocate-interface** command(s) before you enter the **config-url** command. The security appliance must assign interfaces to the context before it loads the context configuration; the context configuration might include commands that refer to interfaces (**interface**, **nat**, **global**...). If you enter the **config-url** command first, the security appliance loads the context configuration immediately. If the context contains any commands that refer to interfaces, those commands fail.

The filename does not require a file extension, although we recommend using “.cfg”.

The admin context file must be stored on the internal Flash memory.

If you download a context configuration from an HTTP or HTTPS server, you cannot save changes back to these servers using the **copy running-config startup-config** command. You can, however, use the **copy tftp** command to copy the running configuration to a TFTP server.

If the system cannot retrieve the context configuration file because the server is unavailable, or the file does not yet exist, the system creates a blank context that is ready for you to configure with the command-line interface.

To change the URL, reenter the **config-url** command with a new URL.

The security appliance merges the new configuration with the current running configuration. Reentering the same URL also merges the saved configuration with the running configuration. A merge adds any new commands from the new configuration to the running configuration. If the configurations are the same, no changes occur. If commands conflict or if commands affect the running of the context, then the effect of the merge depends on the command. You might get errors, or you might have unexpected results. If the running configuration is blank (for example, if the server was unavailable and the configuration was never downloaded), then the new configuration is used. If you do not want to merge the configurations, you can clear the running configuration, which disrupts any communications through the context, and then reload the configuration from the new URL.

Examples

The following example sets the admin context to be “administrator,” creates a context called “administrator” on the internal Flash memory, and then adds two contexts from an FTP server:

```
hostname(config)# admin-context administrator
hostname(config)# context administrator
hostname(config-ctx)# allocate-interface gigabitethernet0/0.1
hostname(config-ctx)# allocate-interface gigabitethernet0/1.1
hostname(config-ctx)# config-url flash:/admin.cfg

hostname(config-ctx)# context test
hostname(config-ctx)# allocate-interface gigabitethernet0/0.100 int1
hostname(config-ctx)# allocate-interface gigabitethernet0/0.102 int2
hostname(config-ctx)# allocate-interface gigabitethernet0/0.110-gigabitethernet0/0.115
int3-int8
hostname(config-ctx)# config-url ftp://user1:passw0rd@10.1.1.1/configlets/test.cfg

hostname(config-ctx)# context sample
hostname(config-ctx)# allocate-interface gigabitethernet0/1.200 int1
hostname(config-ctx)# allocate-interface gigabitethernet0/1.212 int2
```

```
hostname(config-ctx)# allocate-interface gigabitethernet0/1.230-gigabitethernet0/1.235
int3-int8
hostname(config-ctx)# config-url ftp://user1:passw0rd@10.1.1.1/configlets/sample.cfg
```

Related Commands

Command	Description
allocate-interface	Allocates interfaces to a context.
context	Creates a security context in the system configuration and enters context configuration mode.
show context	Shows a list of contexts (system execution space) or information about the current context.

console timeout

To set the idle timeout for a console connection to the security appliance, use the **console timeout** command in global configuration mode. To disable, use the **no** form of this command.

console timeout *number*

no console timeout [*number*]

Syntax Description

number Specifies the idle time in minutes (0 through 60) after which the console session ends.

Defaults

The default timeout is 0, which means the console session will not time out.

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
Global configuration	•	•	•	•	•

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

The **console timeout** command sets the timeout value for any authenticated, enable mode, or configuration mode user session to the security appliance. The **console timeout** command does not alter the Telnet or SSH timeouts; these access methods maintain their own timeout values.

The **no console timeout** command resets the console timeout value to the default timeout of 0, which means that the console will not time out.

Examples

The following example shows how to set the console timeout to 15 minutes:

```
hostname(config)# console timeout 15
```

Related Commands

Command	Description
clear configure console	Restores the default console connection settings.
show running-config console timeout	Displays the idle timeout for a console connection to the security appliance.

content-length

To restrict HTTP traffic based on the length of the HTTP message body, use the **content-length** command in HTTP map configuration mode, which is accessible using the **http-map** command. To remove this command, use the **no** form of this command.

content-length { **min** *bytes* [**max** *bytes*] | **max** *bytes* } **action** { **allow** | **reset** | **drop** } [**log**]

no content-length { **min** *bytes* [**max** *bytes*] | **max** *bytes* } **action** { **allow** | **reset** | **drop** } [**log**]

Syntax Description

action	Specifies the action taken when a message fails this inspection.
allow	Allows the message.
bytes	Specifies the number of bytes. The permitted range is 1 to 65535 for the min option and 1 to 50000000 for the max option.
drop	Closes the connection.
log	(Optional) Generates a syslog.
max	(Optional) Specifies the maximum content length allowed.
min	Specifies the minimum content length allowed.
reset	Sends a TCP reset message to client and server.

Defaults

This command is disabled by default.

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
HTTP map configuration	•	•	•	•	—

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

After enabling the **content-length** command, the security appliance only allows messages within the configured range and otherwise takes the specified action. Use the **action** keyword to cause the security appliance to reset the TCP connection and create a syslog entry.

Examples

The following example restricts HTTP traffic to messages 100 bytes or larger and not exceeding 2000 bytes. If a message is outside this range, the security appliance resets the TCP connection and creates a syslog entry.

```
hostname(config)# http-map inbound_http
hostname(config-http-map)# content-length min 100 max 2000 action reset log
hostname(config-http-map)# exit
```

Related Commands

Commands	Description
class-map	Defines the traffic class to which to apply security actions.
http-map	Defines an HTTP map for configuring enhanced HTTP inspection.
debug appfw	Displays detailed information about traffic associated with enhanced HTTP inspection.
inspect http	Applies a specific HTTP map to use for application inspection.
policy-map	Associates a class map with specific security actions.

content-type-verification

To restrict HTTP traffic based on the content type of the HTTP message, use the **content-type-verification** command, in HTTP map configuration mode, which is accessible using the **http-map** command. To disable this feature, use the **no** form of the command.

content-type-verification [**match-req-rsp**] **action** {**allow** | **reset** | **drop**} [**log**]

no content-type-verification [**match-req-rsp**] **action** {**allow** | **reset** | **drop**} [**log**]

Syntax Description

action	Specifies the action taken when a message fails command inspection.
allow	Allows the message.
drop	Closes the connection.
log	(Optional) Generates a syslog message.
match-req-rsp	(Optional) Verifies that the content-type field in the HTTP response matches the accept field in the corresponding HTTP request message.
reset	Sends a TCP reset message to client and server.

Defaults

This command is disabled by default.

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
HTTP map configuration	•	•	•	•	—

Command History

Release	Modification
7.0	This command was introduced

Usage Guidelines

This command enables the following checks:

- Verifies that the value of the header content-type is in the internal list of supported content types,
- Verifies that the header content-type matches the actual content in the data or entity body portion of the message.
- The **match-req-rsp** keyword enables an additional check that verifies the content-type field in the HTTP response matches the **accept** field in the corresponding HTTP request message.

If the message fails any of the above checks, the security appliance takes the configured action.

The following is the list of supported content types.

audio/*	audio/basic	video/x-msvideo
audio/mpeg	audio/x-adpcm	audio/midi
audio/x-ogg	audio/x-wav	audio/x-aiff
application/octet-stream	application/pdf	application/msword
application/vnd.ms-excel	application/vnd.ms-powerpoint	application/postscript
application/x-java-arching	application/x-msn-messenger	application/x-gzip
image	application/x-java-xm	application/zip
image/jpeg	image/cgf	image/gif
image/x-3ds	image/png	image/tiff
image/x-portable-bitmap	image/x-bitmap	image/x-niff
text/*	image/x-portable-greymap	image/x-xpm
text/plain	text/css	text/html
text/xmcd	text/richtext	text/sgml
video/-flc	text/xml	video/*
video/sgi	video/mpeg	video/quicktime
video/x-mng	video/x-avi	video/x-fli

Some content-types in this list may not have a corresponding regular expression (magic number) so they cannot be verified in the body portion of the message. When this case occurs, the HTTP message will be allowed.

Examples

The following example restricts HTTP traffic based on the content type of the HTTP message. If a message contains an unsupported content type, the security appliance resets the TCP connection and creates a syslog entry.

```
hostname(config)# http-map inbound_http
hostname(config-http-map)# content-type-verification match-req-rsp reset log
hostname(config-http-map)# exit
```

Related Commands

Commands	Description
class-map	Defines the traffic class to which to apply security actions.
http-map	Defines an HTTP map for configuring enhanced HTTP inspection.
debug appfw	Displays detailed information about traffic associated with enhanced HTTP inspection.
inspect http	Applies a specific HTTP map to use for application inspection.
policy-map	Associates a class map with specific security actions.

context

To create a security context in the system configuration and enter context configuration mode, use the **context** command in global configuration mode. To remove a context, use the **no** form of this command. In context configuration mode, you can identify the configuration file URL and interfaces that a context can use.

context *name*

no context *name* [**noconfirm**]

Syntax Description

<i>name</i>	Sets the name as a string up to 32 characters long. This name is case sensitive, so you can have two contexts named “customerA” and “CustomerA,” for example. You can use letters, digits, or hyphens, but you cannot start or end the name with a hyphen. “System” or “Null” (in upper or lower case letters) are reserved names, and cannot be used.
noconfirm	(Optional) Removes the context without prompting you for confirmation. This option is useful for automated scripts.

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		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	•	•	—	—	•

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

If you do not have an admin context (for example, if you clear the configuration) then the first context you add must be the admin context. To add an admin context, see the **admin-context** command. After you specify the admin context, you can enter the **context** command to configure the admin context.

You can only remove a context by editing the system configuration. You cannot remove the current admin context using the **no** form of this command; you can only remove it if you remove all contexts using the **clear configure context** command.

Examples

The following example sets the admin context to be “administrator,” creates a context called “administrator” on the internal Flash memory, and then adds two contexts from an FTP server:


```

hostname(config)# admin-context administrator
hostname(config)# context administrator
hostname(config-ctx)# allocate-interface gigabitethernet0/0.1
hostname(config-ctx)# allocate-interface gigabitethernet0/1.1
hostname(config-ctx)# config-url flash:/admin.cfg

hostname(config-ctx)# context test
hostname(config-ctx)# allocate-interface gigabitethernet0/0.100 int1
hostname(config-ctx)# allocate-interface gigabitethernet0/0.102 int2
hostname(config-ctx)# allocate-interface gigabitethernet0/0.110-gigabitethernet0/0.115
int3-int8
hostname(config-ctx)# config-url ftp://user1:passw0rd@10.1.1.1/configlets/test.cfg

hostname(config-ctx)# context sample
hostname(config-ctx)# allocate-interface gigabitethernet0/1.200 int1
hostname(config-ctx)# allocate-interface gigabitethernet0/1.212 int2
hostname(config-ctx)# allocate-interface gigabitethernet0/1.230-gigabitethernet0/1.235
int3-int8
hostname(config-ctx)# config-url ftp://user1:passw0rd@10.1.1.1/configlets/sample.cfg

```

Related Commands

Command	Description
allocate-interface	Assigns interfaces to a context.
changeto	Changes between contexts and the system execution space.
config-url	Specifies the location of the context configuration.
join-failover-group	Assigns a context to a failover group.
show context	Shows context information.

copy

To copy a file from one location to another, use the **copy** command.

copy [/options] {url | local:[path] | running-config | startup-config} {running-config | startup-config | url | local:[path]}

no copy [/options] {url | local:[path] | running-config | startup-config} {running-config | startup-config | url | local:[path]}

Syntax Description	
<i>/options</i>	Options used for the copy command. <ul style="list-style-type: none"> • noconfirm Copies the file without a confirmation prompt. • pcap Specifies the defaults of the preconfigured TFTP server.
<i>url</i>	Sets the context configuration URL. All remote URLs must be accessible from the admin context. See the following URL syntax: <ul style="list-style-type: none"> • disk0:/[path]/filename This option is only available for the ASA platform, and indicates the internal Flash memory. You can also use flash instead of disk0; they are aliased. • disk1:/[path]/filename This option is only available for the ASA platform, and indicates the external Flash memory card. • flash:/[path]/filename This option indicates the internal Flash card. For the ASA platform, flash is an alias for disk0. • ftp://[user[:password]@]server[:port]/[path]/filename[;type=xx] The type can be one of the following keywords: <ul style="list-style-type: none"> – ap—ASCII passive mode – an—ASCII normal mode – ip—(Default) Binary passive mode – in—Binary normal mode • http[s]://[user[:password]@]server[:port]/[path]/filename • tftp://[user[:password]@]server[:port]/[path]/filename[;int=interface_name] Specify the interface name if you want to override the route to the server address.
<i>path</i>	Pathname that indicates the last component of the path to the file on the server.

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 mode	•	•	•	•	•

Command History

Release	Modification
7.0	Support for this command was introduced.

Usage Guidelines

The security appliance must know how to reach the location (specified by the *tftp_pathname* argument) through its routing table information. This information is determined by the **ip address** command, the **route** command, or the RIP, depending upon the configuration. The *tftp_pathname* can include any directory names in addition to the last component of the path to the file on the server.

The *pathname* can include any directory names in addition to the last component of the path to the file on the server. The pathname cannot contain spaces. If a directory name has spaces, set the directory in the TFTP server instead of in the **copy tftp flash** command

Examples

This example shows how to copy a file from the disk to a TFTP server:

```
hostname(config)# copy disk0:my_context/my_context.cfg
tftp://10.7.0.80/my_context/my_context.cfg
```

This example shows how to copy a file from one location on the disk to another location on the disk. The name of the destination file can be either the name of the source file or a different name.

```
hostname(config)# copy disk0:my_context.cfg disk0:my_context/my_context.cfg
```

This example shows how to copy an image or an ASDM file from the disk to the Flash partition:

```
hostname(config)# copy tftp://10.7.0.80/asa700.bin disk0:asa700.bin
hostname(config)# copy tftp://10.7.0.80/asdm700.bin disk0:asdm700.bin
```

This example shows how to copy a file from the disk to the startup configuration or a running configuration:

```
hostname(config)# copy disk:my_context/my_context.cfg startup-config
hostname(config)# copy disk:my_context/my_context.cfg running-config
```

Related Commands

Command	Description
copy capture	Copies a capture file to a TFTP server.

copy capture

To copy a capture file to a server, use the **copy capture** command in privileged EXEC mode.

copy [/noconfirm] [/pcap] **capture:** [context_name/]buffer_name url

Syntax Description	
/noconfirm	Copies the file without a confirmation prompt.
/pcap	Copies the packet capture as raw data.
<i>buffer_name</i>	Unique name that identifies the capture.
<i>context_name/</i>	Copies a packet capture defined in a security context.
<i>url</i>	Specifies the destination to copy the packet capture file. See the following URL syntax: <ul style="list-style-type: none"> • disk0:/[path/]filename This option is only available for the ASA 5500 series adaptive security appliance, and indicates the internal Flash card. You can also use flash instead of disk0; they are aliased. • disk1:/[path/]filename This option is only available for the ASA 5500 series adaptive security appliance, and indicates the external Flash card. • flash:/[path/]filename This option indicates the internal Flash card. For the ASA 5500 series adaptive security appliance, flash is an alias for disk0. • ftp://[user[:password]@]server[:port]/[path/]filename[;type=xx] The type can be one of the following keywords: <ul style="list-style-type: none"> – ap—ASCII passive mode – an—ASCII normal mode – ip—(Default) Binary passive mode – in—Binary normal mode • http[s]://[user[:password]@]server[:port]/[path/]filename • tftp://[user[:password]@]server[:port]/[path/]filename[;int=interface_name] Specify the interface name if you want to override the route to the server address. The pathname cannot contain spaces. If a pathname has spaces, set the path in the tftp-server command instead of in the copy tftp command.

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	•	•	•	—	•

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

The following example shows the prompts that are provided when you enter the **copy capture** command without specifying the full path:

```
hostname(config)# copy capture:abc tftp
Address or name of remote host [171.68.11.129]?
Source file name [username/cdisk]?
copying capture to tftp://171.68.11.129/username/cdisk:
[yes|no|again]? y
!!!!!!!!!!!!!!
```

You can specify the full path as follows:

```
hostname(config)# copy capture:abc tftp:171.68.11.129/tftpboot/abc.cap
```

If the TFTP server is already configured, the location or filename can be unspecified as follows:

```
hostname(config)# tftp-server outside 171.68.11.129 tftp/cdisk
hostname(config)# copy capture:abc tftp:/tftp/abc.cap
```

Related Commands

Command	Description
capture	Enables packet capture capabilities for packet sniffing and network fault isolation.
clear capture	Clears the capture buffer.
show capture	Displays the capture configuration when no options are specified.

crashinfo console disable

To read, write, and configure crash write to flash, use the **crashinfo console disable** command.

crashinfo console disable

[no] crashinfo console disable

Syntax Description

disable Suppresses console output in the event of a crash.

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
Global configuration	•	•	•	—	•

Command History

Release	Modification
7.0(4)	This command was introduced.

Usage Guidelines

This command lets you suppress crashinfo from being output to the console. The crashinfo may contain sensitive information that is not appropriate for viewing by all users connected to the device. In conjunction with this command, you should also ensure crashinfo is written to flash, which can be examined after the device reboots. This command effects output for crashinfo and checkheaps, which is saved to flash and should be sufficient for troubleshooting.

Examples

```
hostname(config)# crashinfo console disable
```

Related Commands

Command	Description
clear configure fips	Clears the system or module FIPS configuration information stored in NVRAM.
fips enable	Enables or disables a policy-checking to enforce FIPS compliance on the system or module.
fips self-test poweron	Executes power-on self-tests.

Command	Description
show crashinfo console	Reads, writes, and configures crash write to flash.
show running-config fips	Displays the FIPS configuration that is running on the FWSM.

crashinfo force

To force the security appliance to crash, use the **crashinfo force** command in privileged EXEC mode.

crashinfo force [**page-fault** | **watchdog**]

Syntax Description

page-fault	(Optional) Forces a crash of the security appliance as a result of a page fault.
watchdog	(Optional) Forces a crash of the security appliance as a result of watchdogging.

Defaults

The security appliance saves the crash information file to Flash memory by default.

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	•	•	•	—	•

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

You can use the **crashinfo force** command to test the crash output generation. In the crash output, there is nothing that differentiates a real crash from a crash resulting from the **crashinfo force page-fault** or **crashinfo force watchdog** command (because these are real crashes). The security appliance reloads after the crash dump is complete.



Caution

Do not use the **crashinfo force** command in a production environment. The **crashinfo force** command crashes the security appliance and forces it to reload.

Examples

The following example shows the warning that displays when you enter the **crashinfo force page-fault** command:

```
hostname# crashinfo force page-fault
WARNING: This command will force the XXX to crash and reboot.
Do you wish to proceed? [confirm]:
```

If you enter a carriage return (by pressing the Return or Enter key on your keyboard), “y”, or “Y” the security appliance crashes and reloads; any of these responses are interpreted as confirmation. Any other character is interpreted as a **no**, and the security appliance returns to the command-line prompt.

Related Commands

clear crashinfo	Clears the contents of the crash information file.
crashinfo save disable	Disables crash information from writing to Flash memory.
crashinfo test	Tests the ability of the security appliance to save crash information to a file in Flash memory.
show crashinfo	Displays the contents of the crash information file.

crashinfo save disable

To disable crash information from writing to Flash memory, use the **crashinfo save** command in global configuration mode.

crashinfo save disable

no crashinfo save disable

Syntax Description

This command has no default arguments or keywords.

Defaults

The security appliance saves the crash information file to Flash memory by default.

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
Global configuration	•	•	•	—	•

Command History

Release	Modification
7.0	The crashinfo save enable command was deprecated and is no longer a valid option. Use the no crashinfo save disable command instead.

Usage Guidelines

Crash information writes to Flash memory first, and then to your console.



Note

If the security appliance crashes during startup, the crash information file is not saved. The security appliance must be fully initialized and running first, before it can save crash information to Flash memory.

Use the **no crashinfo save disable** command to re-enable saving the crash information to Flash memory.

Examples

```
hostname(config)# crashinfo save disable
```

Related Commands

clear crashinfo	Clears the contents of the crash file.
crashinfo force	Forces a crash of the security appliance.

crashinfo test	Tests the ability of the security appliance to save crash information to a file in Flash memory.
show crashinfo	Displays the contents of the crash file.

crashinfo test

To test the ability of the security appliance to save crash information to a file in Flash memory, use the **crashinfo test** command in global configuration mode.

crashinfo test

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

If a previous crash information file already exists in Flash memory, that file is overwritten.



Note

Entering the **crashinfo test** command does not crash the security appliance.

Examples

The following example shows the output of a crash information file test.

```
hostname(config)# crashinfo test
```

Related Commands

clear crashinfo	Deletes the contents of the crash file.
crashinfo force	Forces the security appliance to crash.
crashinfo save disable	Disables crash information from writing to Flash memory.
show crashinfo	Displays the contents of the crash file.

crl

To specify CRL configuration options, use the **crl** command in **crypto ca trustpoint** configuration mode.

crl { required | optional | nocheck }

Syntax Description

required	The required CRL must be available for a peer certificate to be validated.
optional	The security appliance can still accept the peer certificate if the required CRL is not available.
nocheck	Directs the security appliance not to perform CRL checking.

Defaults

The default value is **nocheck**.

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
Crypto ca trustpoint configuration	•	•	•	•	•

Command History

Release	Modification
7.0	This command was introduced.

Examples

The following example enters **crypto ca trustpoint** configuration mode for **trustpoint central**, and requires that a CRL be available for a peer certificate to be validated for **trustpoint central**:

```
hostname(config)# crypto ca trustpoint central
hostname(ca-trustpoint)# crl required
hostname(ca-trustpoint)#
```

Related Commands

Command	Description
clear configure crypto ca trustpoint	Removes all trustpoints.
crypto ca trustpoint	Enters trustpoint submode.
crl configure	Enters crl configuration mode.

crl configure

To enter CRL configuration configuration mode, use the **crl configure** command in crypto ca trustpoint configuration mode.

crl configure

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0	This command was introduced.

Examples

The following example enters crl configuration mode within trustpoint central:

```
hostname<config># crypto ca trustpoint central
hostname<ca-trustpoint># crl configure
hostname<ca-crl>#
```

Related Commands

Command	Description
clear configure crypto ca trustpoint	Removes all trustpoints.
crypto ca trustpoint	Enters trustpoint submode.

crypto ca authenticate

To install and authenticate the CA certificates associated with a trustpoint, use the **crypto ca authenticate** command in global configuration mode. To remove the CA certificate, use the **no** form of this command.

crypto ca authenticate *trustpoint* [**fingerprint** *hexvalue*] [**nointeractive**]

no **crypto ca authenticate** *trustpoint*

Syntax Description

fingerprint	Specifies a hash value consisting of alphanumeric characters the security appliance uses to authenticate the CA certificate. If a fingerprint is provided, the security appliance compares it to the computed fingerprint of the CA certificate and accepts the certificate only if the two values match. If there is no fingerprint, the security appliance displays the computed fingerprint and asks whether to accept the certificate.
<i>hexvalue</i>	Identifies the hexadecimal value of the fingerprint.
nointeractive	Obtains the CA certificate for this trustpoint using no interactive mode; intended for use by the device manager only. In this case, if there is no fingerprint, the security appliance accepts the certificate without question.
<i>trustpoint</i>	Specifies the trustpoint from which to obtain the CA certificate. Maximum name length is 128 characters.

Defaults

This command has 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		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
7.0	This command was introduced

Usage Guidelines

If the trustpoint is configured for SCEP enrollment, the CA certificate is downloaded through SCEP. If not, the security appliance prompts you to paste the base-64 formatted CA certificate onto the terminal. The invocations of this command do not become part of the running configuration.

Examples

In the following example, the security appliance requests the certificate of the CA. The CA sends its certificate and the security appliance prompts the administrator to verify the certificate of the CA by checking the CA certificate fingerprint. The security appliance administrator should verify the fingerprint value displayed against a known, correct value. If the fingerprint displayed by the security appliance matches the correct value, you should accept the certificate as valid.

```
hostname(config)# crypto ca authenticate myca
Certificate has the following attributes:
Fingerprint: 0123 4567 89AB CDEF 0123
Do you accept this certificate? [yes/no] y#
hostname(config)#
```

In the next example, the trustpoint tp9 is configured for terminal-based (manual) enrollment. In this case the security appliance prompts the administrator to paste the CA certificate to the terminal. After displaying the fingerprint of the certificate, the security appliance prompts the administrator to confirm that the certificate should be retained.

```
hostname(config)# crypto ca authenticate tp9
Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself

MIIDjCCAvEgAwIBAgIQejIaQ3SJRIbMHcvDdgOsKTANBgkqhkiG9w0BAQUFADBA
MQswCQYDVQQGEwJVUzELMAkGA1UECBMCTUEuETAPBgNVBACTECEyYw5rbGluMREw
DwYDVQQDEwEhCm1hbnNDQTAeFw0wMjEwMTcxODE5MTJaFw0wNjEwMjEwMTcxODE5
MEACzAJBgNVBAYTA1VMTQswCQYDVQQLIEwJNQTERMA8GA1UEBxMIRnJhbmtsaW4x
ETAPBgNVBAMTCEJyaWwFuc0NBMIgfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCD
jXEPvNnkZD1bKzahbTHuRot1T8KRUBCP5aWkfQViKJENzI2GnAheArazaAcc4Eaz
LDnpuyyqa0j5LA3MI577MoN1/n1l018fbbpQOf9eVDPJdKYTvtZ/X3vJgnEjTOWyz
T0pXxhdU1b/jgqVE74OvKBzU7A2yoQ2hMYzwVbGkewIDAQABo4IBhzCCAYMwEwYJ
KwYBBAGCNxQCBAYeBABDAEEwCwYDVR0PBAQDAgFMA8GA1UdEwEB/wQFMAMBAf8w
HQYDVR0OBBYEFBhr3holowFDmniI3FBwKpSEucdtMIIBGwYDVR0fBIIBEjCCAQ4w
gcaggcOggcCGb1sZGFwOi8vL0NOPUJyaWFuc0NBLENOPWJyaWFuLXcyay1zdnIs
Q049Q0RQLENOPVB1YmxpYyUyMETleSUyMFN1cnZpY2VzLENOPVN1cnZpY2VzLENO
PUNvbmZpZ3VyYXRpb24sREM9YnJpYW5wZGMSREM9YmRzLERDPWNvbT9jZXJ0aWZp
Y2F0ZVJldm9jYXRpb25MaXN0P2Jhc2U/b2JqZWN0Y2xhc3M9Y1JMRGlzdHJpYnV0
aW9uUG9pbmQwQ6BBoD+GPWh0dHA6Ly9icm1hbn13Mmstc3ZyLmJyaWFwFucGRjLmJk
cy5jb20vQ2VydeVucm9sbC9Ccm1hbnNDQS5jcmmwEAYJKwYBBAGCNxUBBAMCAQEW
DQYJKoZIhvcNAQEFBQADgYEAdLhc4Za3AbMjRq66xH1qJWxKUZd4nE9wOrhGgA1r
j4B/Hv2K1gUie34xGqu9OpwqvJgpp/vCU12Ciykb1YdSDy/PxN4KtR9Xd1JDQMbu5
f20AYqCG5vpPWavCgmgtLcdwKa3ps1YSWGkhWmSCHHSiGgla3tevYVwhHNPA4mWo
7sQ=
```

```
Certificate has the following attributes:
Fingerprint: 21B598D5 4A81F3E5 0B24D12E 3F89C2E4
% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
% Certificate successfully imported
hostname(config)#
```

Related Commands

Command	Description
crypto ca enroll	Starts enrollment with a CA.
crypto ca import certificate	Installs a certificate received from a CA in response to a manual enrollment request. Also used to import PKS12 data to a trustpoint.
crypto ca trustpoint	Enters the trustpoint submode for the indicated trustpoint.

crypto ca certificate chain

To enter certificate chain configuration mode for the indicated trustpoint, use the **crypto ca certificate chain** command in global configuration mode. To return to global configuration mode, use the **no** form of the command or use the **exit** command.

crypto ca certificate chain *trustpoint*

Syntax Description

<i>trustpoint</i>	Specifies the trustpoint for configuring the certificate chain.
-------------------	---

Defaults

This command has no default values.

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
Global configuration	•	•	•	•	—

Command History

Release	Modification
7.0	This command was introduced.

Examples

The following example enters CA certificate chain submode for trustpoint central:

```
hostname<config># crypto ca certificate chain central
hostname<config-cert-chain>#
```

Related Commands

Command	Description
clear configure crypto ca trustpoint	Removes all trustpoints.

crypto ca certificate map

To enter CA certificate map mode, use the **crypto ca configuration map** command in global configuration mode. Executing this command places you in ca-certificate-map mode. Use this group of commands to maintain a prioritized list of certificate mapping rules. The sequence number orders the mapping rules.

To remove a crypto CA configuration map rule, use the **no** form of the command.

crypto ca certificate map *sequence-number*

no crypto ca certificate map [*sequence-number*]

Syntax Description

sequence-number Specifies a number for the certificate map rule you are creating. The range is 1 through 65535. You can use this number when creating a tunnel-group-map, which maps a tunnel group to a certificate map rule.

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		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

Issuing this command places the security appliance in CA certificate map configuration mode where you can configure rules based on the certificate's issuer and subject distinguished names (DNs). The general form of these rules is as follows:

DN match-criteria match-value

DN is either *subject-name* or *issuer-name*. DN's are defined in the ITU-T X.509 standard. For a list of certificate fields, see Related Commands.

match-criteria comprise the following expressions or operators:

attr <i>tag</i>	Limits the comparison to a specific DN attribute, such as common name (CN).
co	Contains
eq	Equal

nc	Does not contain
ne	Not equal

The DN matching expressions are case insensitive.

Examples

The following example enters CA certificate map mode with a sequence number of 1 (rule # 1) and specifies that the common name(CN) attribute of the subject-name must match Pat:

```
hostname(config)# crypto ca certificate map 1
hostname(ca-certificate-map)# subject-name attr cn eq pat
hostname(ca-certificate-map)#
```

The following example enters CA certificate map mode with a sequence number of 1 and specifies that the subject-name contain the value cisco anywhere within it:

```
hostname(config)# crypto ca certificate map 1
hostname(ca-certificate-map)# subject-name co cisco
hostname(ca-certificate-map)#
```

Related Commands+

Command	Description
issuer-name	Indicates that rule entry is applied to the issuer DN of the IPsec peer certificate.
subject-name (crypto ca certificate map)	Indicates that rule entry is applied to the subject DN of the IPsec peer certificate.
tunnel-group-map enable	Associates the certificate map entries created using the crypto ca certificate map command with tunnel groups.

crypto ca crl request

To request a CRL based on the configuration parameters of the specified trustpoint, use the **crypto ca crl request** command in Crypto ca trustpoint configuration mode.

crypto ca crl request *trustpoint*

Syntax Description

trustpoint Specifies the trustpoint. Maximum number of characters is 128.

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		
	Routed	Transparent	Single	Multiple	
				Context	System
Crypto ca trustpoint configuration	•	•	•	•	—

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

Invocations of this command do not become part of the running configuration.

Examples

The following example requests a CRL based on the trustpoint named central:

```
hostname(config)# crypto ca crl request central
hostname(config)#
```

Related Commands

Command	Description
crl configure	Enters crl configure mode.

crypto ca enroll

To start the enrollment process with the CA, use the **crypto ca enroll** command in global configuration mode. For this command to execute successfully, the trustpoint must have been configured correctly.

crypto ca enroll *trustpoint* [**noconfirm**]

Syntax Description

noconfirm	(Optional) Suppresses all prompts. Enrollment options that might have been prompted for must be pre-configured in the trustpoint. This option is for use in scripts, ASDM, or other such non-interactive needs.
<i>trustpoint</i>	Specifies the name of the trustpoint to enroll with. Maximum number of characters is 128.

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		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

When the trustpoint is configured for SCEP enrollment, the security appliance displays a CLI prompt immediately and displays status messages to the console asynchronously. When the trustpoint is configured for manual enrollment, the security appliance writes a base-64-encoded PKCS10 certification request to the console and then displays the CLI prompt.

This command generates interactive prompts that vary depending on the configured state of the referenced trustpoint.

Examples

The following example enrolls for an identity certificate with trustpoint tp1 using SCEP enrollment. The security appliance prompts for information not stored in the trustpoint configuration.

```
hostname(config)# crypto ca enroll tp1
%
% Start certificate enrollment ..
% Create a challenge password. You will need to verbally provide this
% password to the CA Administrator in order to revoke your certificate.
% For security reasons your password will not be saved in the configuration.
% Please make a note of it.
Password:
Re-enter password:
```

```
% The fully-qualified domain name in the certificate will be: xyz.example.com
% The subject name in the certificate will be: xyz.example.com
% Include the router serial number in the subject name? [yes/no]: no
% Include an IP address in the subject name? [no]: no
Request certificate from CA [yes/no]: yes
% Certificate request sent to Certificate authority.
% The certificate request fingerprint will be displayed.
% The 'show crypto ca certificate' command will also show the fingerprint.

hostname(config)#
```

The next command shows manual enrollment of a CA certificate.

```
hostname(config)# crypto ca enroll tp1

% Start certificate enrollment ..
% The fully-qualified domain name in the certificate will be: xyz.example.com
% The subject name in the certificate will be: wb-2600-3.example.com
if serial number not set in trustpoint, prompt:
% Include the router serial number in the subject name? [yes/no]: no
If ip-address not configured in trustpoint:
% Include an IP address in the subject name? [no]: yes
Enter Interface name or IP Address[]: 1.2.3.4
Display Certificate Request to terminal? [yes/no]: y
Certificate Request follows:
MIIBFTCBwAIBADA6MTgwFAYJKoZIhvcNAQkIEwcxLjIuMy40MCAGCSqGSIB3DQEEJ
AhYTd2ItMjYwMC0zLmNpc2NvLmNvbTBcMA0GCSqGSIB3DQEBAQUAA0sAMEgCQQDT
IdvHa4D5wXZ+40sKQV7Uek1E+CC6hm/LRN3p5ULW1KF6bxhA3Q5CQfh4jDxobn+A
Y8GoeceulS2Zb+mvgNvjAgMBAAGgITAfBgkqhkiG9w0BCQ4xEjAQM4GA1UdDwEB
/wQEAWIFoDANBgkqhkiG9w0BAQQFAANBACDhnrEGBVtltG7hp8x6Wz/dgY+ouWcA
1zy7QpdGhb1du2P81RYn+8pWRA43cikXMTem4yEkZhLjDUgv9t+R9c=

---End - This line not part of the certificate request---

Redisplay enrollment request? [yes/no]: no
hostname(config)#
```

Related Commands

Command	Description
crypto ca authenticate	Obtains the CA certificate for this trustpoint.
crypto ca import pkcs12	Installs a certificate received from a CA in response to a manual enrollment request. Also used to import PKS12 data to a trustpoint.
crypto ca trustpoint	Enters the trustpoint submode for the indicated trustpoint.

crypto ca export

To export in PKCS12 format the keys and certificates associated with a trustpoint configuration, use the **crypto ca export** command in global configuration mode.

crypto ca export *trustpoint* **pkcs12** *passphrase*

Syntax Description

passphrase	Specifies the passphrase used to encrypt the PKCS12 file for export.
pkcs12	Specifies the public key cryptography standard to use in exporting the trustpoint configuration.
trustpoint	Specifies the name of the trustpoint whose certificate and keys are to be exported. When you export, if the trustpoint uses RSA keys, the exported key pair is assigned the same name as the trustpoint.

Defaults

This command has no default 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	This command was introduced.

Usage Guidelines

Invocations of this command do not become part of the active configuration. The PKCS12 data is written to the terminal.

Examples

The following example exports PKCS12 data for trustpoint central using xxyyzz as the passcode:

```
hostname (config)# crypto ca export central pkcs12 xxyyzz
```

Exported pkcs12 follows:

```
[ PKCS12 data omitted ]
```

```
---End - This line not part of the pkcs12---
```

```
hostname (config)#
```

Related Commands	Command	Description
	crypto ca import pkcs12	Installs a certificate received from a CA in response to a manual enrollment request. Also used to import PKS12 data to a trustpoint.
	crypto ca authenticate	Obtains the CA certificate for this trustpoint.
	crypto ca enroll	Starts enrollment with a CA.
	crypto ca trustpoint	Enters the trustpoint submode for the indicated trustpoint.

crypto ca import

To install a certificate received from a CA in response to a manual enrollment request or to import the certificate and key pair for a trustpoint using PKCS12 data, use the **crypto ca import** command in global configuration mode. The security appliance prompts you to paste the text to the terminal in base 64 format.

crypto ca import *trustpoint* **certificate** [**nointeractive**]

crypto ca import *trustpoint* **pkcs12** *passphrase* [**nointeractive**]

Syntax Description

<i>trustpoint</i>	Specifies the trustpoint with which to associate the import action. Maximum number of characters is 128. If you import PKCS12 data and the trustpoint uses RSA keys, the imported key pair is assigned the same name as the trustpoint.
<i>certificate</i>	Tells the security appliance to import a certificate from the CA represented by the trustpoint.
pkcs12	Tells the security appliance to import a certificate and key pair for a trustpoint, using PKCS12 format.
<i>passphrase</i>	Specifies the passphrase used to decrypt the PKCS12 data.
nointeractive	(Optional) Imports a certificate using nointeractive mode. This suppresses all prompts. This option for use in scripts, ASDM, or other such non-interactive needs.

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		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
7.0	This command was introduced.

Examples

The following example manually imports a certificate for the trustpoint Main:

```
hostname (config)# crypto ca import Main certificate
% The fully-qualified domain name in the certificate will be:
securityappliance.example.com
```

```
Enter the base 64 encoded certificate.
End with a blank line or the word "quit" on a line by itself
[ certificate data omitted ]
```

```
quit
INFO: Certificate successfully imported
hostname (config)#
```

The following example manually imports PKCS12 data to trustpoint central:

```
hostname (config)# crypto ca import central pkcs12

Enter the base 64 encoded pkcs12.
End with a blank line or the word "quit" on a line by itself:
[ PKCS12 data omitted ]
quit
INFO: Import PKCS12 operation completed successfully
hostname (config)#
```

Related Commands

Command	Description
crypto ca export	Exports a trustpoint certificate and key pair in PKCS12 format.
crypto ca authenticate	Obtains the CA certificate for a trustpoint.
crypto ca enroll	Starts enrollment with a CA.
crypto ca trustpoint	Enters the trustpoint submode for the indicated trustpoint.

crypto ca trustpoint

To enter the trustpoint submode for the specified trustpoint, use the **crypto ca trustpoint** command in global configuration mode. To remove the specified trustpoint, use the **no** form of this command. This command manages trustpoint information. A trustpoint represents a CA identity and possibly a device identity, based on a certificate issued by the CA. The commands within the trustpoint sub mode control CA-specific configuration parameters which specify how the security appliance obtains the CA certificate, how the security appliance obtains its certificate from the CA, and the authentication policies for user certificates issued by the CA.

crypto ca trustpoint *trustpoint-name*

no crypto ca trustpoint *trustpoint-name* [**noconfirm**]

Syntax Description

noconfirm	Suppresses all interactive prompting
<i>trustpoint- name</i>	Identifies the name of the trustpoint to manage. The maximum name length is 128 characters.

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		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

Use the **crypto ca trustpoint** command to declare a CA. Issuing this command puts you in Crypto ca trustpoint configuration mode.

You can specify characteristics for the trustpoint using the following commands listed alphabetically in this command reference guide:

- **crl required | optional | nocheck**—Specifies CRL configuration options.
- **crl configure**—Enters CRL configuration submode (see **crl**).
- **default enrollment**—Returns all enrollment parameters to their system default values. Invocations of this command do not become part of the active configuration.
- **enrollment retry period**—Specifies a retry period in minutes for automatic (SCEP) enrollment.
- **enrollment retry count**—Specifies a maximum number of permitted retries for automatic (SCEP) enrollment.

- **enrollment terminal**—Specifies cut and paste enrollment with this trustpoint.
- **enrollment url** *url*—Specifies automatic enrollment (SCEP) to enroll with this trustpoint and configures the enrollment URL (*url*).
- **fqdn** *fqdn*—During enrollment, asks the CA to include the specified fully-qualified distinguished name (FQDN) in the Subject Alternative Name extension of the certificate.
- **email** *address*—During enrollment, asks the CA to include the specified email address in the Subject Alternative Name extension of the certificate.
- **subject-name** *X.500 name*—During enrollment, asks the CA to include the specified subject DN in the certificate.
- **serial-number**—During enrollment, asks the CA to include the security appliance's serial number in the certificate.
- **ip-addr** *ip-address*—During enrollment, asks the CA to include the IP address of the security appliance in the certificate.
- **password** *string*—Specifies a challenge phrase that is registered with the CA during enrollment. The CA typically uses this phrase to authenticate a subsequent revocation request.
- **keypair** *name*—Specifies the key pair whose public key is to be certified.
- **id-cert-issuer**—Indicates whether the system accepts peer certificates issued by the CA associated with this trustpoint.
- **accept-subordinates**—Indicates whether CA certificates subordinate to the CA associated with the trustpoint are accepted if delivered during phase one IKE exchange when not previously installed on the device.
- **support-user-cert-validation**—If enabled, the configuration settings to validate a remote user certificate can be taken from this trustpoint, provided that this trustpoint is authenticated to the CA that issued the remote certificate. This option applies to the configuration data associated with the subcommands **crl required** | **optional** | **nocheck** and all settings in the CRL sub mode.
- **exit**—Leaves the submode.

Examples

The following example enters CA trustpoint mode for managing a trustpoint named central:

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

Related Commands

Command	Description
clear configure crypto ca trustpoint	Removes all trustpoints.
crypto ca authenticate	Obtains the CA certificate for this trustpoint.
crypto ca certificate map	Enters crypto CA certificate map mode. Defines certificate-based ACLs.
crypto ca crl request	Requests a CRL based on configuration parameters of specified trustpoint.
crypto ca import	Installs a certificate received from a CA in response to a manual enrollment request. Also used to import PKS12 data to a trustpoint.

crypto dynamic-map match address

See the **crypto map match address** command for additional information about this command.

crypto dynamic-map *dynamic-map-name* *dynamic-seq-num* **match address** *acl_name*

no crypto dynamic-map *dynamic-map-name* *dynamic-seq-num* **match address** *acl_name*

Syntax Description

<i>acl-name</i>	Identifies the access-list to be matched for the dynamic crypto map entry.
<i>dynamic-map-name</i>	Specifies the name of the dynamic crypto map set.
<i>dynamic-seq-num</i>	Specifies the sequence number that corresponds to the dynamic crypto map entry.

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		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	•	—	•	—	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Examples

The following example shows the use of the **crypto dynamic-map** command to match address of an access list named **aclist1**:

```
hostname(config)# crypto dynamic-map mymap 10 match address aclist1
hostname(config)#
```

Related Commands

Command	Description
clear configure crypto dynamic-map	Clears all configuration for all the dynamic crypto maps.
show running-config crypto dynamic-map	Displays all configuration for all the dynamic crypto maps.

crypto dynamic-map set nat-t-disable

To disable NAT-T for connections based on this crypto map entry, use the **crypto dynamic-map set nat-t-disable** command in global configuration mode. To enable NAT-T for this crypto map entry, use the **no** form of this command.

crypto dynamic-map *dynamic-map-name* *dynamic-seq-num* **set nat-t-disable**

no crypto dynamic-map *dynamic-map-name* *dynamic-seq-num* **set nat-t-disable**

Syntax Description

<i>dynamic-map-name</i>	Specifies the name of the crypto dynamic map set.
<i>dynamic-seq-num</i>	Specifies the number you assign to the crypto dynamic map entry.

Defaults

The default setting is off.

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
Global configuration	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

Use the **isakmp nat-traversal** command to globally enable NAT-T. Then you can use the **crypto dynamic-map set nat-t-disable** command to disable NAT-T for specific crypto map entries.

Examples

The following command disables NAT-T for the crypto dynamic map named mymap:

```
hostname(config)# crypto dynamic-map mymap 10 set nat-t-disable
hostname(config)#
```

Related Commands

Command	Description
clear configure crypto dynamic-map	Clears all configuration for all the dynamic crypto maps.
show running-config crypto dynamic-map	Displays all configuration for all the dynamic crypto maps.

crypto dynamic-map set peer

See the **crypto map set peer** command for additional information about this command.

crypto dynamic-map *dynamic-map-name* *dynamic-seq-num* **set peer** *ip_address* | *hostname*

no crypto dynamic-map *dynamic-map-name* *dynamic-seq-num* **set peer** *ip_address* | *hostname*

Syntax Description

<i>dynamic-map-name</i>	Specifies the name of the dynamic crypto map set.
<i>dynamic-seq-num</i>	Specifies the sequence number that corresponds to the dynamic crypto map entry.
<i>ip_address</i>	Identifies the peer in the dynamic crypto map entry by IP address, as defined by the name command.
<i>hostname</i>	Identifies the peer in the dynamic crypto map entry by hostname, as defined by the name command.

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		
	Routed	Transparent	Single	Multiple Context	System
Global configuration	•	—	•	—	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Examples

The following example shows setting a peer for a dynamic-map named mymap to the IP address 10.0.0.1:

```
hostname(config)# crypto dynamic-map mymap 10 set peer 10.0.0.1
hostname(config)#
```

Related Commands

Command	Description
clear configure crypto dynamic-map	Clears all configuration for all the dynamic crypto maps.
show running-config crypto dynamic-map	Displays all configuration for all the dynamic crypto maps.

crypto dynamic-map set pfs

See the **crypto map set pfs** command for additional information about this command.

crypto dynamic-map *dynamic-map-name dynamic-seq-num* **set pfs** [**group1** | **group2** | **group5** | **group 7**]

no crypto dynamic-map *dynamic-map-name dynamic-seq-num* **set pfs** [**group1** | **group2** | **group5** | **group 7**]

Syntax Description

<i>dynamic-map-name</i>	Specifies the name of the dynamic crypto map set.
<i>dynamic-seq-num</i>	Specifies the sequence number that corresponds to the dynamic crypto map entry.
group1	Specifies that IPsec should use the 768-bit Diffie-Hellman prime modulus group when performing the new Diffie-Hellman exchange.
group2	Specifies that IPsec should use the 1024-bit Diffie-Hellman prime modulus group when performing the new Diffie-Hellman exchange.
group5	Specifies that IPsec should use the 1536-bit Diffie-Hellman prime modulus group when performing the new Diffie-Hellman exchange.
group7	Specifies that IPsec should use group7 (ECC) where the elliptical curve field size is 163-bits, for example, with the movianVPN client.
set pfs	Configures IPsec to ask for perfect forward secrecy (PFS) when requesting new security associations for this dynamic crypto map entry or configures IPsec to require PFS when receiving requests for new security associations.

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		
	Routed	Transparent	Single	Multiple Context	System
Global configuration	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was modified to add Diffie-Hellman group 7.

Usage Guidelines

The **crypto dynamic-map** commands, such as **match address**, **set peer**, and **set pfs** are described with the **crypto map** commands. If the peer initiates the negotiation and the local configuration specifies PFS, the peer must perform a PFS exchange or the negotiation fails. If the local configuration does not specify a group, the security appliance assumes a default of group2. If the local configuration does not specify PFS, it accepts any offer of PFS from the peer.

When interacting with the Cisco VPN Client, the security appliance does not use the PFS value, but instead uses the value negotiated during Phase 1.

Examples

The following example specifies that PFS should be used whenever a new security association is negotiated for the crypto dynamic-map mymap 10. The group specified is group 2:

```
hostname(config)# crypto dynamic-map mymap 10 set pfs group2
hostname(config)#
```

Related Commands

Command	Description
clear configure crypto dynamic-map	Clears all configuration for all the dynamic crypto maps.
show running-config crypto dynamic-map	Displays all configuration for all the dynamic crypto maps.

crypto dynamic-map set reverse route

See the **crypto map set reverse-route** command for additional information about this command.

crypto dynamic-map *dynamic-map-name* *dynamic-seq-num* **set reverse route**

no crypto dynamic-map *dynamic-map-name* *dynamic-seq-num* **set reverse route**

Syntax Description

<i>dynamic-map-name</i>	Specifies the name of the crypto map set.
<i>dynamic-seq-num</i>	Specifies the number you assign to the crypto map entry.

Defaults

The default value for this command is off.

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
Global configuration	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

The following command enables RRI for the crypto dynamic-map named mymap:

```
hostname(config)# crypto dynamic-map mymap 10 set reverse route
hostname(config)#
```

Related Commands

Command	Description
clear configure crypto dynamic-map	Clears all configuration for all the dynamic crypto maps.
show running-config crypto dynamic-map	Displays all configuration for all the dynamic crypto maps.

crypto map set security-association lifetime

To override (for a particular crypto map entry) the global lifetime value, which is used when negotiating IPSec security associations, use the **crypto map set security-association lifetime** command in global configuration mode. To reset a crypto map entry's lifetime value to the global value, use the **no** form of this command.

crypto map *map-name seq-num* **set security-association lifetime** {**seconds** *seconds* |
kilobytes *kilobytes*}

no crypto map *map-name seq-num* **set security-association lifetime** {**seconds** *seconds* |
kilobytes *kilobytes*}

Syntax Description

<i>kilobytes</i>	Specifies the volume of traffic (in kilobytes) that can pass between peers using a given security association before that security association expires. The default is 4,608,000 kilobytes.
<i>map-name</i>	Specifies the name of the crypto map set.
<i>seconds</i>	Specifies the number of seconds a security association will live before it expires. The default is 28,800 seconds (eight hours).
<i>seq-num</i>	Specifies the number you assign to the crypto map entry.

Defaults

The default number of kilobytes is 4,608,000; the default number of seconds is 28,800.

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
Global configuration	•	•	•	—	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

The crypto map's security associations are negotiated according to the global lifetimes.

IPSec security associations use shared secret keys. These keys and their security associations time out together.

Assuming that the particular crypto map entry has lifetime values configured, when the security appliance requests new security associations during security association negotiation, it specifies its crypto map lifetime values in the request to the peer; it uses these values as the lifetime of the new security associations. When the security appliance receives a negotiation request from the peer, it uses the smaller of the lifetime values proposed by the peer or the locally configured lifetime values as the lifetime of the new security associations.

There are two lifetimes: a “timed” lifetime and a “traffic-volume” lifetime. The session keys/security association expires after the first of these lifetimes is reached. You can specify both with one command.

**Note**

The security appliance lets you change crypto map, dynamic map, and ipsec settings on the fly. If you do so, the security appliance brings down only the connections affected by the change. If you change an existing access-list associated with a crypto map, specifically by deleting an entry within the access-list, the result is that only the associated connection is brought down. Connections based on other entries in the access-list are not affected.

To change the timed lifetime, use the **crypto map set security-association lifetime seconds** command. The timed lifetime causes the keys and security association to time out after the specified number of seconds have passed.

Examples

The following command, entered in global configuration mode, specifies a security association lifetime in seconds and kilobytes for crypto map mymap

```
hostname(config)# crypto map mymap 10 set security-association lifetime seconds 1400  
kilobytes 3000000  
hostname(config)#
```

Related Commands

Command	Description
clear configure crypto map	Clears all configuration for all crypto maps.
show running-config crypto map	Displays the crypto map configuration.


crypto dynamic-map set transform-set

See the **crypto map set transform-set** command for additional information about this command.

```
crypto dynamic-map dynamic-map-name dynamic-seq-num set transform-set
    transform-set-name1 [... transform-set-name9]

no crypto dynamic-map dynamic-map-name dynamic-seq-num set transform-set
    transform-set-name1 [... transform-set-name9]
```

Syntax Description	<i>dynamic-map-name</i>	Specifies the name of the dynamic crypto map set.
	<i>dynamic-seq-num</i>	Specifies the sequence number that corresponds to the dynamic crypto map entry.
	<i>transform-set-name1</i>	Identifies the transform set to be used with the dynamic crypt map entry (the names of transform sets defined using the crypto ipsec command).
	<i>transform-set-name9</i>	



Note

The **crypto map set transform-set** command is required for dynamic crypto map entries. All you need in the entry is a transform set.

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		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	•	—	•	—	—

Command History	Release	Modification
	Preexisting	This command was preexisting.

Examples

The following command specifies two transform sets (tfset1 and tfset2) for the crypto dynamic-map mymap:

```
hostname(config)# crypto dynamic-map mymap 10 set transform-set tfset1 tfset2
hostname(config)#
```

Related Commands

Command	Description
clear configure crypto dynamic-map	Clears all configuration for all the dynamic crypto maps.
show running-config crypto dynamic-map	Displays all configuration for all the dynamic crypto maps.

crypto ipsec df-bit

To configure DF-bit policy for IPSec packets, use the **crypto ipsec df-bit** command in global configuration mode.

crypto ipsec df-bit [**clear-df** | **copy-df** | **set-df**] *interface*

Syntax Description

clear-df	(Optional) Specifies that the outer IP header will have the DF bit cleared and that the security appliance may fragment the packet to add the IPSec encapsulation.
copy-df	(Optional) Specifies that the security appliance will look in the original packet for the outer DF bit setting.
set-df	(Optional) Specifies that the outer IP header will have the DF bit set; however, the security appliance may fragment the packet if the original packet had the DF bit cleared.
<i>interface</i>	Specifies an interface name.

Defaults

This command is disabled by default. If this command is enabled without a specified setting, the security appliance uses the **copy-df** setting as 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	This command was introduced.

Usage Guidelines

The DF bit with IPSec tunnels feature lets you specify whether the security appliance can clear, set, or copy the Don't Fragment (DF) bit from the encapsulated header. The DF bit within the IP header determines whether a device is allowed to fragment a packet.

Use the **crypto ipsec df-bit** command in global configuration mode to configure the security appliance to specify the DF bit in an encapsulated header.

When encapsulating tunnel mode IPSec traffic, use the **clear-df** setting for the DF bit. This setting lets the device send packets larger than the available MTU size. Also this setting is appropriate if you do not know the available MTU size.

Examples

The following example, entered in global configuration mode, specifies sets the IPSec DF policy to **clear-df**:

```
hostname(config)# crypto ipsec df-bit clear-df inside
hostname(config)#
```

Related Commands

Command	Description
crypto ipsec fragmentation	Configures the fragmentation policy for IPSec packets.
show crypto ipsec df-bit	Displays the DF-bit policy for a specified interface.
show crypto ipsec fragmentation	Displays the fragmentation policy for a specified interface.

crypto ipsec fragmentation

To configure the fragmentation policy for IPSec packets, use the **crypto ipsec fragmentation** command in global configuration mode.

crypto ipsec fragmentation {**after-encryption** | **before-encryption**} *interface*

Syntax Description

after-encryption	Specifies the security appliance to fragment IPSec packets that are close to the maximum MTU size after encryption (disables pre-fragmentation).
before-encryption	Specifies the security appliance to fragment IPSec packets that are close to the maximum MTU size before encryption (enables pre-fragmentation).
<i>interface</i>	Specifies an interface name.

Defaults

This feature is enabled by default.

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
Global configuration	•	•	•	—	—

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

When a packet is near the size of the MTU of the outbound link of the encrypting security appliance, and it is encapsulated with IPSec headers, it is likely to exceed the MTU of the outbound link. This causes packet fragmentation after encryption, which makes the decrypting device reassemble in the process path. Pre-fragmentation for IPSec VPNs increases the decrypting device's performance by letting it operate in the high performance CEF path instead of the process path.

Pre-fragmentation for IPSec VPNs lets an encrypting device predetermine the encapsulated packet size from information available in transform sets, which are configured as part of the IPSec SA. If the device predetermines that the packet will exceed the MTU of the output interface, the device fragments the packet before encrypting it. This avoids process level reassembly before decryption and helps improve decryption performance and overall IPSec traffic throughput.

Examples

The following example, entered in global configuration mode, enables pre-fragmentation for IPSec packets globally on the device:

```
hostname(config)# crypto ipsec fragmentation before-encryption inside
hostname(config)#
```

The following example, entered in global configuration mode, disables pre-fragmentation for IPSec packets on the interface:

```
hostname(config)# crypto ipsec fragmentation after-encryption inside  
hostname(config)#
```

Related Commands

Command	Description
crypto ipsec df-bit	Configures the DF-bit policy for IPSec packets.
show crypto ipsec fragmentation	Displays the fragmentation policy for IPSec packets.
show crypto ipsec df-bit	Displays the DF-bit policy for a specified interface.

crypto ipsec security-association lifetime

To configure global lifetime values, use the **crypto ipsec security-association lifetime** command in global configuration mode. To reset a crypto ipsec entry's lifetime value to the default value, use the **no** form of this command.

crypto ipsec security-association lifetime {seconds *seconds* | kilobytes *kilobytes*}

no crypto ipsec security-association lifetime {seconds *seconds* | kilobytes *kilobytes*}

Syntax Description

<i>kilobytes</i>	Specifies the volume of traffic (in kilobytes) that can pass between peers using a given security association before that security association expires. The range is 10 to 2147483647 kbytes. The default is 4,608,000 kilobytes.
<i>seconds</i>	Specifies the number of seconds a security association will live before it expires. The range is 120 to 214783647 seconds. The default is 28,800 seconds (eight hours).
<i>token</i>	Indicate a token-based server for user authentication is used.

Defaults

The default number of kilobytes is 4,608,000; the default number of seconds is 28,800.

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
Global configuration	•	•	•	—	—

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

The **crypto ipsec security-association lifetime** command changes global lifetime values used when negotiating IPSec security associations.

IPSec security associations use shared secret keys. These keys and their security associations time out together.

Assuming that the particular crypto map entry has no lifetime values configured, when the security appliance requests new security associations during negotiation, it specifies its global lifetime value in the request to the peer; it uses this value as the lifetime of the new security associations. When the security appliance receives a negotiation request from the peer, it uses the smaller of the lifetime value proposed by the peer or the locally configured lifetime value as the lifetime of the new security associations.

There are two lifetimes: a “timed” lifetime and a “traffic-volume” lifetime. The security association expires after the first of these lifetimes is reached.

The security appliance lets you change crypto map, dynamic map, and ipsec settings on the fly. If you do so, the security appliance brings down only the connections affected by the change. If you change an existing access-list associated with a crypto map, specifically by deleting an entry within the access-list, the result is that only the associated connection is brought down. Connections based on other entries in the access-list are not affected.

To change the global timed lifetime, use the **crypto ipsec security-association lifetime seconds** command. The timed lifetime causes the security association to time out after the specified number of seconds have passed.

To change the global traffic-volume lifetime, use the **crypto ipsec security-association lifetime kilobytes** command. The traffic-volume lifetime causes the security association to time out after the specified amount of traffic (in kilobytes) has been protected by the security associations' key.

Shorter lifetimes can make it harder to mount a successful key recovery attack, because the attacker has less data encrypted under the same key to work with. However, shorter lifetimes require more CPU processing time for establishing new security associations.

The security association (and corresponding keys) expires according to whichever occurs sooner, either after the number of seconds has passed or after the amount of traffic in kilobytes has passed.

Examples

The following example specifies a global timed lifetime for security associations:

```
hostname(config)# crypto ipsec-security association lifetime seconds 240
hostname(config)#
```

Related Commands

Command	Description
clear configure crypto map	Clears all IPSec configuration (i.e. global lifetimes and transform sets).
show running-config crypto map	Displays all configuration for all the crypto maps.

crypto ipsec transform-set

To define a transform set, use the **crypto ipsec transform-set** command in global configuration mode. With this command, you identify the IPSec encryption and hash algorithms to be used by the transform set. Use the **no** form of this command to remove a transform set.

crypto ipsec *map-name seq-num* **transform-set** *transform-set-name transform1 [transform2]*

no crypto ipsec *map-name seq-num* **transform-set** *transform-set-name*

Syntax Description

esp-aes	Specifying this option means that IPSec messages protected by this transform are encrypted using AES with a 128-bit key.
esp-aes-192	Specifying this option means that IPSec messages protected by this transform are encrypted using AES with a 192-bit key.
esp-aes-256	Specifying this option means that IPSec messages protected by this transform are encrypted using AES with a 256-bit key.
esp-des	Specifying this option means that IPSec messages protected by this transform with encryption using 56-bit DES-CBC.
esp-3des	Specifying this option means that IPSec messages protected by this transform are encrypted using the Triple DES algorithm.
esp-none	Specifying this option means that IPSec messages do not use HMAC authentication.
esp-null	Specifying this option means that IPSec messages are not encrypted using the IPSec security protocol (ESP) only.
esp-md5-hmac	Specifying this option means that IPSec messages protected by this transform are using MD5/HMAC-128 as the hash algorithm.
esp-sha-hmac	Specifying this option means that IPSec messages protected by this transform are using SHA/HMAC-160 as the hash algorithm.
<i>map-name</i>	Specifies the name of the crypto map set.
<i>seq-num</i>	Specifies the number you assign to the crypto map entry.
<i>transform1, transform2</i>	Specifies up to two transforms. Transforms define the IPSec security protocol(s) and algorithm(s). Each transform represents an IPSec security protocol (ESP), plus the algorithm to use, either [esp-aes esp-aes-192 esp-aes-256 esp-des esp-3des esp-null] or [esp-md5-hmac esp-sha-hmac] as defined in this syntax table.
<i>transform-set-name</i>	Specifies the name of the transform set to create or modify.
token	Indicate a token-based server for user authentication is used.

Defaults

The default encryption algorithm is esp-3des (Triple DES).

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
Global configuration	•	•	•	—	—

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

A transform set specifies one or two IPSec security protocols and specifies which algorithms to use with the selected security protocol. During the IPSec security association negotiation, the peers agree to use a particular transform set when protecting a particular data flow.

IPSec messages can be protected by a transform set using AES with a 128-bit key, 192-bit key, or 256-bit key.

Due to the large key sizes provided by AES, ISAKMP negotiation should use Diffie-Hellman group 5 instead of group 1 or group 2. To do this, use the **isakmp policy priority group 5** command.

You can configure multiple transform sets, and then specify one or more of these transform sets in a crypto map entry. The transform set defined in the crypto map entry in the IPSec security association negotiation protects the data flows specified by that crypto map entry's access list. During the negotiation, the peers search for a transform set that is the same at both peers. When the security appliance finds such a transform set, it applies it to the protected traffic as part of both peer's IPSec security associations.

Each transform-set represents an algorithm to use for encryption or authentication. When the particular transform set is used during negotiations for IPSec security associations, the entire transform set (the combination of protocols, algorithms, and other settings) must match a transform set at the remote peer.

In a transform set, you can specify just an ESP encryption transform or both an ESP encryption transform and an ESP authentication transform.

Examples of acceptable transform combinations are as follows:

- **esp-des**
- **esp-des** and **esp-md5-hmac**

If one or more transforms are specified in the **crypto ipsec transform-set** command for an existing transform set, the specified transforms replace the existing transforms for that transform set.

Examples

The following example configures two transform sets: one named t1, using DES for encryption and SHA/HMAC-160 as the hash algorithm, and the other named standard, using AES 192 for encryption and MD5/HMAC-128 as the hash algorithm:

```
hostname(config)# crypto ipsec transform-set t1 esp-des esp-sha-hmac
hostname(config)# crypto ipsec transform-set standard esp-aes-192 esp-md5-hmac
hostname(config)
```

Related Commands	Command	Description
	clear configure crypto	Clears all ipsec configuration (i.e. global lifetimes and transform sets).
	show running-config crypto map	Displays all configuration for all the crypto maps.

crypto ipsec transform-set mode transport

To specify IPSec transport mode for the transform set, use the **crypto ipsec transform-set mode transport** command in global configuration mode. Use the **no** form of this command to remove the IPSec transport mode from the transform set.

crypto ipsec transform-set *transform-set-name* **mode transport**

no crypto ipsec transform-set *transform-set-name* **mode transport**

Syntax Description

mode transport	Specifies the transform set to accept transport mode requests in addition to the tunnel mode request.
<i>transform-set-name</i>	Specifies the name of the transform set to create or modify.
token	Indicate a token-based server for user authentication is used.

Defaults

The default mode is tunnel mode.

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
Global configuration	•	—	•	—	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

This command specifies IPSec transport mode for a transform set. The default is tunnel mode. Tunnel mode is automatically enabled for a transform set.

Examples

The following example configures a transform set named transtet5 that uses Triple DES for encryption, MD5/HMAC-128 for a hash algorithm, and then specifies IPSec transport mode for the transform set transtet5:

```
hostname(config)# crypto ipsec transform-set transtet5 esp-3des esp-md5-hmac
hostname(config)# crypto ipsec transform-set transtet5 mode transport
hostname(config)#
```

Related Commands	Command	Description
	clear configure crypto	Clears all ipsec configuration (i.e. global lifetimes and transform sets).
	clear configure crypto map	Clears all crypto maps.
	show running-config crypto map	Displays all configuration for all the crypto maps.

crypto key generate dsa

To generate DSA key pairs for identity certificates, use the **crypto key generate dsa** command in global configuration mode.

crypto key generate dsa {**label** *key-pair-label*} [**modulus** *size*] [**noconfirm**]

Syntax Description

label <i>key-pair-label</i>	Specifies the name to be associated with the key pair(s); maximum label length is 128 characters. DSA requires a label.
modulus <i>size</i>	Specifies the modulus size of the key pair(s): 512, 768, 1024. The default modulus size is 1024.
noconfirm	Suppresses all interactive prompting.

Defaults

The default modulus size is 1024.

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
Global configuration	•	•	•	•	—

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

Use the **crypto key generate dsa** command to generate DSA key pairs to support SSL, SSH, and IPSec connections. The generated key pairs are identified by labels that you provide as part of the command syntax. If you do not provide a label, the security appliance displays an error message.



Note

When generating DSA keys, you may encounter a delay. On a Cisco PIX 515E Firewall, this delay may extend up to few minutes.

Examples

The following example, entered in global configuration mode, generates an DSA key pair with the label mypubkey:

```
hostname(config)# crypto key generate dsa label mypubkey
INFO: The name for the keys will be: mypubkey
hostname(config)#
```

The following example, entered in global configuration mode, inadvertently attempts to generate a duplicate DSA key pair with the label mypubkey:

```
hostname(config)# crypto key generate dsa label mypubkey
```

crypto key generate dsa

```
WARNING: You already have dSA keys defined named mypubkey
Do you really want to replace them? [yes/no] no
ERROR: Failed to create new DSA keys named mypubkey
hostname(config)#
```

Related Commands

Command	Description
crypto key zeroize	Removes the DSA key pairs.
show crypto key mypubkey	Displays the DSA key pairs.

crypto key generate rsa

To generate RSA key pairs for identity certificates, use the **crypto key generate rsa** command in global configuration mode.

crypto key generate rsa [**usage-keys** | **general-keys**] [**label** *key-pair-label*] [**modulus** *size*] [**noconfirm**]

Syntax Description	general-keys	Generates a single pair of general purpose keys. This is the default key-pair type.
	label <i>key-pair-label</i>	Specifies the name to be associated with the key pair(s). This key pair must be uniquely labeled. If you attempt to create another key pair with the same label, the security appliance displays an warning message. If no label is provided when the key is generated, the key pair is statically named <Default-RSA-Key>.
	modulus <i>size</i>	Specifies the modulus size of the key pair(s): 512, 768, 1024, and 2048. The default modulus size is 1024.
	noconfirm	Suppresses all interactive prompting.
	usage-keys	Generates two key pairs, one for signature use and one for encryption use. This implies that two certificates for the corresponding identity are required.

Defaults

The default key-pair type is **general key**. The default modulus size is 1024.

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
Global configuration	•	•	•	•	—

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

Use the **crypto key generate rsa** command to generate RSA key pairs to support SSL, SSH, and IPSec connections. The generated key pairs are identified by labels that you can provide as part of the command syntax. Trustpoints that do not reference a key pair can use the default one <Default-RSA-Key>. SSH connections always use this key. This does not affect SSL, since SSL generates its own cert/key dynamically, unless a trustpoint has one configured.

Examples

The following example, entered in global configuration mode, generates an RSA key pair with the label mypubkey:

```
hostname(config)# crypto key generate rsa label mypubkey
INFO: The name for the keys will be: mypubkey
Keypair generation process
hostname(config)#
```

The following example, entered in global configuration mode, inadvertently attempts to generate a duplicate RSA key pair with the label mypubkey:

```
hostname(config)# crypto key generate rsa label mypubkey
WARNING: You already have RSA keys defined named mypubkey
Do you really want to replace them? [yes/no] no
ERROR: Failed to create new RSA keys named mypubkey
hostname(config)#
```

The following example, entered in global configuration mode, generates an RSA key pair with the default label:

```
hostname(config)# crypto key generate rsa
INFO: The name for the keys will be: <Default-RSA-Key>
Keypair generation process begin. Please wait...
hostname(config)#
```

Related Commands

Command	Description
crypto key zeroize	Removes RSA key pairs.
show crypto key mypubkey	Displays the RSA key pairs.

crypto key zeroize

To remove the key pairs of the indicated type (rsa or dsa), use the **crypto key zeroize** command in global configuration mode.

crypto key zeroize {rsa | dsa} [label *key-pair-label*] [default] [noconfirm]

Syntax Description

default	Removes RSA key pairs with no labels. This keyword is legal only with RSA key pairs.
dsa	Specifies DSA as the key type.
label <i>key-pair-label</i>	Removes the key pairs of the indicated type (rsa or dsa). If you do not provide a label, the security appliance removes all key pairs of the indicated type.
noconfirm	Suppresses all interactive prompting.
rsa	Specifies RSA as the key type.

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		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Examples

The following example, entered in global configuration mode, removes all RSA key pairs:

```
hostname(config)# crypto key zeroize rsa
WARNING: All RSA keys will be removed.
WARNING: All router certs issued using these keys will also be removed.

Do you really want to remove these keys? [yes/no] y
hostname(config)#
```

Related Commands

Command	Description
crypto key generate dsa	Generates DSA key pairs for identity certificates.
crypto key generate rsa	Generate RSA key pairs for identity certificates.

crypto map interface

Use the **crypto map interface** command in global configuration mode to apply a previously defined crypto map set to an interface. Use the **no** form of this command to remove the crypto map set from the interface.

crypto map *map-name* **interface** *interface-name*

no crypto map *map-name* **interface** *interface-name*

Syntax Description

<i>interface-name</i>	Specifies the interface for the security appliance to use for establishing tunnels with VPN peers. If ISAKMP is enabled, and you are using a certificate authority (CA) to obtain certificates, this should be the interface with the address specified in the CA certificates.
<i>map-name</i>	Specifies the name of the crypto map set.

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		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	•	•	•	—	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

Use this command to assign a crypto map set to any active security appliance interface. The security appliance supports IPSec termination on any and all active interfaces. You must assign a crypto map set to an interface before that interface can provide IPSec services.

You can assign only one crypto map set to an interface. If multiple crypto map entries have the same *map-name* but a different *seq-num*, they are part of the same set and are all applied to the interface. The security appliance evaluates the crypto map entry with the lowest *seq-num* first.

**Note**

The security appliance lets you change crypto map, dynamic map, and ipsec settings on the fly. If you do so, the security appliance brings down only the connections affected by the change. If you change an existing access-list associated with a crypto map, specifically by deleting an entry within the access-list, the result is that only the associated connection is brought down. Connections based on other entries in the access-list are not affected.

**Note**

Every static crypto map must define three parts: an access list, a transform set, and an IPsec peer. If one of these is missing, the crypto map is incomplete and the security appliance moves on to the next entry. However, if the crypto map matches on the access-list but not on either or both of the other two requirements, this security appliance drops the traffic.

Use the **show running-config crypto map** command to ensure that every crypto map is complete. To fix an incomplete crypto map, remove the crypto map, add the missing entries, and reapply it.

Examples

The following example, entered in global configuration mode, assigns the crypto map set named mymap to the outside interface. When traffic passes through the outside interface, the security appliance evaluates it against all the crypto map entries in the mymap set. When outbound traffic matches an access list in one of the mymap crypto map entries, the security appliance forms a security association using that crypto map entry's configuration.

```
hostname(config)# crypto map mymap interface outside
```

The following example shows the minimum required crypto map configuration:

```
hostname(config)# crypto map mymap 10 ipsec-isakmp
hostname(config)# crypto map mymap 10 match address 101
hostname(config)# crypto map mymap set transform-set my_t_set1
hostname(config)# crypto map mymap set peer 10.0.0.1
```

Related Commands

Command	Description
clear configure crypto map	Clears all configuration for all crypto maps.
show running-config crypto map	Displays the crypto map configuration.

crypto map ipsec-isakmp dynamic

To require a given crypto map entry to refer to a pre-existing dynamic crypto map, use the **crypto map ipsec-isakmp dynamic** command in global configuration mode. Use the **no** form of this command to remove the cross reference.

Use the **crypto dynamic-map** command to create dynamic crypto map entries. After you create a dynamic crypto map set, use the **crypto map ipsec-isakmp dynamic** command to add the dynamic crypto map set to a static crypto map.

crypto map *map-name seq-num ipsec-isakmp dynamic dynamic-map-name*

no crypto map *map-name seq-num ipsec-isakmp dynamic dynamic-map-name*

Syntax Description

<i>dynamic-map-name</i>	Specifies the name of the crypto map entry that refers to a pre-existing dynamic crypto map.
ipsec-isakmp	Indicates that IKE establishes the IPSec security associations for this crypto map entry.
<i>map-name</i>	Specifies the name of the crypto map set.
<i>seq-num</i>	Specifies the number you assign to the crypto map entry.

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	This command was modified to remove the ipsec-manual keyword.

Usage Guidelines

After you define crypto map entries, you can use the **crypto map interface** command to assign the dynamic crypto map set to interfaces.

Dynamic crypto maps provide two functions: filtering/classifying traffic to protect, and defining the policy to apply to that traffic. The first use affects the flow of traffic on an interface; the second affects the negotiation performed (via IKE) on behalf of that traffic.

IPSec dynamic crypto maps identify the following:

- The traffic to protect
- IPSec peer(s) with which to establish a security association
- Transform sets to use with the protected traffic

- How to use or manage keys and security associations

A crypto map set is a collection of crypto map entries, each with a different sequence number (seq-num) but the same map name. Therefore, for a given interface, you could have certain traffic forwarded to one peer with specified security applied to that traffic, and other traffic forwarded to the same or a different peer with different IPsec security applied. To accomplish this you create two crypto map entries, each with the same map name, but each with a different sequence number.

The number you assign as the seq-num argument should not be arbitrary. This number ranks multiple crypto map entries within a crypto map set. A crypto map entry with a lower seq-num is evaluated before a map entry with a higher seq-num; that is, the map entry with the lower number has a higher priority.

**Note**

When you link the crypto map to a dynamic crypto map, you must specify the dynamic crypto map. This links the crypto map to an existing dynamic crypto map that was previously defined using the **crypto dynamic-map** command. Now any changes you make to the crypto map entry after it has been converted, will not take affect. For example, a change to the set peer setting does not take effect. However, the security appliance stores the change while it is up. When the dynamic crypto map is converted back to the crypto map, the change is effective and appears in the output of the **show running-config crypto map** command. The security appliance maintains these settings until it reboots.

Examples

The following command, entered in global configuration mode, configures the crypto map mymap to refer to a dynamic crypto map named test.

```
hostname(config)# crypto map mymap ipsec-isakmp dynamic test
hostname(config)#
```

Related Commands

Command	Description
clear configure crypto map	Clears all configuration for all crypto maps.
show running-config crypto map	Displays the crypto map configuration.

crypto map match address

To assign an access list to a crypto map entry, use the **crypto map match address** command in global configuration mode. Use the **no** form of this command to remove the access list from a crypto map entry.

crypto map *map-name seq-num match address acl_name*

no crypto map *map-name seq-num match address acl_name*

Syntax Description

<i>acl_name</i>	Specifies the name of the encryption access list. This name should match the name argument of the named encryption access list being matched.
<i>map-name</i>	Specifies the name of the crypto map set.
<i>seq-num</i>	Specifies the number you assign to the crypto map entry.

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		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	•	•	•	—	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

This command is required for all static crypto maps. If you are defining a dynamic crypto map (with the **crypto dynamic-map** command), this command is not required but is strongly recommended.

Use the **access-list** command to define the access lists.

The security appliance uses the access lists to differentiate the traffic to protect with IPSec crypto from the traffic that does not need protection. It protects outbound packets that match a permit ACE, and ensures that inbound packets that match a permit ACE have protections.

When the security appliance matches a packet to a deny statement, it skips the evaluation of the packet against the remaining access control entries (ACEs) in the crypto map, and resumes evaluation of the packet against the ACEs in the next crypto map in sequence. *Cascading ACLs* involves the use of deny ACEs to bypass evaluation of the remaining ACEs in an ACL, and the resumption of evaluation of traffic against the ACL assigned to the next crypto map in the crypto map set. Because you can associate each crypto map with different IPSec settings, you can use deny ACEs to exclude special traffic from further evaluation in the corresponding crypto map, and match the special traffic to permit statements in another crypto map to provide or require different security.

**Note**

The crypto access list does not determine whether to permit or deny traffic through the interface. An access list applied directly to the interface with the **access-group** command makes that determination.

**Note**

In transparent mode, the destination address should be the IP address of the security appliance, the management address. Only tunnels to the security appliance are allowed in transparent mode.

Related Commands

Command	Description
clear configure crypto map	Clears all configuration for all crypto maps.
show running-config crypto map	Displays the crypto map configuration.

crypto map set connection-type

To specify the connection type for the Backup Site-to-Site feature for this crypto map entry, use the **crypto map set connection-type** command in global configuration mode. Use the **no** form of this command to return to the default setting.

crypto map *map-name seq-num* **set connection-type** {**answer-only** | **originate-only** | **bidirectional**}

no crypto map *map-name seq-num* **set connection-type** {**answer-only** | **originate-only** | **bidirectional**}

Syntax Description

answer-only	Indicates that this peer can only respond to inbound IKE connections for Site-to-Site connections based on this crypto map entry. It cannot originate connection requests.
bidirectional	Indicates that this peer can accept and originate connections based on this crypto map entry. This is the default connection type for all Site-to-Site connections.
map-name	Specifies the name of the crypto map set.
originate-only	Indicates that this peer can only originate connections based on this crypto map entry. It cannot accept inbound connections.
seq-num	Specifies the number you assign to the crypto map entry.
set connection-type	Specifies the connection type for the Backup Site-to-Site feature for this crypto map entry. There are three types of connections: answer-only, originate-only, and bidirectional.

Defaults

The default setting is bidirectional.

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
Global configuration	•	—	•	—	—

*In transparent firewall mode, you can see this command but the answer-only value cannot be set to anything other than answer-only for crypto map entries that are part of a crypto map that has been attached to the interface.

Command History

Release	Modification
7.0	This command was introduced.

Examples

The following example, entered in global configuration mode, configures the crypto map mymap and sets the connection-type to bidirectional.

```
hostname(config)# crypto map mymap 10 set connection-type bidirectional
hostname(config)#
```

Related Commands

Command	Description
clear configure crypto map	Clears all configuration for all crypto maps.
show running-config crypto map	Displays the crypto map configuration.

crypto map set inheritance

To set the granularity (single or multiple) of security associations generated for this crypto map entry, use the **set inheritance** command in global configuration mode. To remove the inheritance setting for this crypto map entry, use the no form of this command.

crypto map *map-name seq-num set inheritance {data | rule}*

no crypto map *map-name seq-num set inheritance {data | rule}*

Syntax Description

data	Specifies one tunnel for every address pair within the address ranges specified in the rule.
<i>map-name</i>	Specifies the name of the crypto map set.
rule	Specifies one tunnel for each ACL entry associated with this crypto map. Default.
<i>seq-num</i>	Specifies the number you assign to the crypto map entry.
set inheritance	Specifies the type of inheritance: data or rule . Inheritance allows a single security association (SA) to be generated for each security policy database (SPD) rule or multiple security SAs for each address pair in the range.

Defaults

Default value is **rule**.

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	This command was introduced.

Usage Guidelines

This command works only when the security appliance is initiating the tunnel, not when responding to a tunnel. Using the data setting may create a large number of IPSec SAs. This consumes memory and results in fewer overall tunnels. You should use the data setting only for extremely security-sensitive applications.

Examples

The following example, entered in global configuration mode, configures the crypto map mymap and sets the inheritance type to data.

```
hostname(config)# crypto map mymap 10 set inheritance data
hostname(config)#
```


Related Commands	Command	Description
	clear configure crypto map	Clears all configuration for all crypto maps.
	show running-config crypto map	Displays the crypto map configuration.

crypto map set nat-t-disable

To disable NAT-T for connections based on this crypto map entry, use the **crypto map set nat-t-disable** command in global configuration mode. To enable NAT-T for this crypto map entry, use the **no** form of this command.

crypto map *map-name seq-num* **set nat-t-disable**

no crypto map *map-name seq-num* **set nat-t-disable**

Syntax Description

<i>map-name</i>	Specifies the name of the crypto map set.
<i>seq-num</i>	Specifies the number you assign to the crypto map entry.

Defaults

The default setting for this command is not on (therefore NAT-T is enabled by default).

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
Global configuration	•	•	•	—	—

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

Use the **isakmp nat-traversal** command to globally enable NAT-T. Then you can use the **crypto map set nat-t-disable** command to disable NAT-T for specific crypto map entries.

Examples

The following command, entered in global configuration mode, disables NAT-T for the crypto map entry named mymap.

```
hostname(config)# crypto map mymap 10 set nat-t-disable
hostname(config)#
```

Related Commands

Command	Description
clear configure crypto map	Clears all configuration for all crypto maps.
isakmp nat-traversal	Enables NAT-T for all connections.
show running-config crypto map	Displays the crypto map configuration.

crypto map set peer

To specify an IPSec peer in a crypto map entry, use the **crypto map set peer** command in global configuration mode. Use the **no** form of this command to remove an IPSec peer from a crypto map entry.

```
crypto map map-name seq-num set peer {ip_address | hostname}{...ip_address | hostname10}
```

```
no crypto map map-name seq-num set peer {ip_address | hostname}{...ip_address | hostname10}
```

Syntax Description

<i>hostname</i>	Specifies a peer by its host name as defined by the security appliance name command.
<i>ip_address</i>	Specifies a peer by its IP address.
<i>map-name</i>	Specifies the name of the crypto map set.
peer	Specifies an IPSec peer in a crypto map entry either by hostname or IP address.
<i>seq-num</i>	Specifies the number you assign to the crypto map entry.

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		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	•	•	•	—	—

Command History

Release	Modification
7.0	This command was modified to allow up to 10 peer addresses.

Usage Guidelines

This command is required for all static crypto maps. If you are defining a dynamic crypto map (with the **crypto dynamic-map** command), this command is not required, and in most cases is not used because, in general, the peer is unknown.

For LAN-to-LAN connections, you can use multiple peers only with originator-only connection type. Configuring multiple peers is equivalent to providing a fallback list. For each tunnel, the security appliance attempts to negotiate with the first peer in the list. If that peer does not respond, the security appliance works its way down the list until either a peer responds or there are no more peers in the list. You can set up multiple peers only when using the backup LAN-to-LAN feature (that is, when the crypto map is originate-only type).

Examples

The following example, entered in global configuration mode, shows a crypto map configuration using IKE to establish the security associations. In this example, you can set up a security association to either the peer at 10.0.0.1 or the peer at 10.0.0.2.

```
hostname(config)# crypto map mymap 10 ipsec-isakmp
hostname(config)# crypto map mymap 10 match address 101
hostname(config)# crypto map mymap 10 set transform-set my_t_set1
hostname(config)# crypto map mymap 10 set peer 10.0.0.1 10.0.0.2
```

Related Commands

Command	Description
clear configure crypto map	Clears all configuration for all crypto maps.
show running-config crypto map	Displays the crypto map configuration.

crypto map set pfs

Use the **crypto map set pfs** command in global configuration mode to set IPsec to ask for perfect forward secrecy (PFS) when requesting new security associations for this crypto map entry or that IPsec requires PFS when receiving requests for new security associations. To specify that IPsec should not request PFS, use the **no** form of this command.

crypto map *map-name seq-num set pfs* [**group1** | **group2** | **group5** | **group7**]

no crypto map *map-name seq-num set pfs* [**group1** | **group2** | **group5** | **group7**]

Syntax Description

group1	Specifies that IPsec should use the 768-bit Diffie-Hellman prime modulus group when performing the new Diffie-Hellman exchange.
group2	Specifies that IPsec should use the 1024-bit Diffie-Hellman prime modulus group when performing the new Diffie-Hellman exchange.
group5	Specifies that IPsec should use the 1536-bit Diffie-Hellman prime modulus group when performing the new Diffie-Hellman exchange.
group7	Specifies that IPsec should use group7 (ECC) where the elliptical curve field size is 163-bits, for example, with the movianVPN client.
<i>map-name</i>	Specifies the name of the crypto map set.
<i>seq-num</i>	Specifies the number you assign to the crypto map entry.

Defaults

By default PFS is not set.

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
Global configuration	•	•	•	—	—

Command History

Release	Modification
7.0	This command was modified to add Diffie-Hellman group 7.

Usage Guidelines

With PFS, every time a new security association is negotiated, a new Diffie-Hellman exchange occurs, which requires additional processing time. PFS adds another level of security because if one key is ever cracked by an attacker, only the data sent with that key is compromised.

During negotiation, this command causes IPsec to request PFS when requesting new security associations for the crypto map entry. If the **set pfs** statement does not specify a group, the security appliance sends the default (group2).

If the peer initiates the negotiation and the local configuration specifies PFS, the peer must perform a PFS exchange or the negotiation fails. If the local configuration does not specify a group, the security appliance assumes a default of group2. If the local configuration specifies group2, group5, or group7, that group must be part of the peer's offer or the negotiation fails.

For a negotiation to succeed PFS has to be set on both ends. If set, the groups have to be an exact match; The security appliance does not accept just any offer of PFS from the peer.

The 1536-bit Diffie-Hellman prime modulus group, group5, provides more security than group1, or group2, but requires more processing time than the other groups.

Diffie-Hellman Group 7 generates IPSec SA keys, where the elliptical curve field size is 163 bits. You can use this option with any encryption algorithm. This option is intended for use with the movianVPN client, but you can use it with any peers that support Group 7 (ECC).

When interacting with the Cisco VPN Client, the security appliance does not use the PFS value, but instead uses the value negotiated during Phase 1.

Examples

The following example, entered in global configuration mode, specifies that PFS should be used whenever a new security association is negotiated for the crypto map "mymap 10":

```
hostname(config)# crypto map mymap 10 ipsec-isakmp
hostname(config)# crypto map mymap 10 set pfs group2
```

Related Commands

Command	Description
clear isakmp sa	Deletes the active IKE security associations.
clear configure crypto map	Clears all configuration for all crypto maps.
show running-config crypto map	Displays the crypto map configuration.
tunnel-group	Configures tunnel-groups and their parameters.

crypto map set phase1 mode

To specify the IKE mode for phase 1 when initiating a connection to either main or aggressive, use the **crypto map set phase1mode** command in global configuration mode. To remove the setting for phase 1 IKE negotiations, use the **no** form of this command. Including a Diffie-Hellman group with aggressive mode is optional. If one is not included, the security appliance uses group 2.

```
crypto map map-name seq-num set phase1mode {main | aggressive [group1 | group2 | group5 |
group7]}
```

```
no crypto map map-name seq-num set phase1mode {main | aggressive [group1 | group2 | group5
| group7]}
```

Syntax Description

aggressive	Specifies aggressive mode for phase one IKE negotiations
group1	Specifies that IPsec should use the 768-bit Diffie-Hellman prime modulus group when performing the new Diffie-Hellman exchange.
group2	Specifies that IPsec should use the 1024-bit Diffie-Hellman prime modulus group when performing the new Diffie-Hellman exchange.
group5	Specifies that IPsec should use the 1536-bit Diffie-Hellman prime modulus group when performing the new Diffie-Hellman exchange.
group7	Specifies that IPsec should use group7 (ECC) where the elliptical curve field size is 163-bits, for example, with the movianVPN client.
main	Specifies main mode for phase one IKE negotiations.
<i>map-name</i>	Specifies the name of the crypto map set.
<i>seq-num</i>	Specifies the number you assign to the crypto map entry.

Defaults

Default phase one mode is **main**.

Command Modes

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

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

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

This command works only in initiator mode; not in responder mode.

Examples

The following example, entered in global configuration mode, configures the crypto map my map and sets the phase one mode to aggressive, using group 2.

```
hostname(config)# crypto map mymap 10 set phase1mode aggressive group2
hostname(config)#
```

Related Commands

Command	Description
clear isakmp sa	Delete the active IKE security associations.
clear configure crypto map	Clears all configuration for all crypto maps.
show running-config crypto map	Displays the crypto map configuration.

crypto map set reverse-route

To enable RRI for any connection based on this crypto map entry, use the **crypto map set reverse-route** command in global configuration mode. To disable reverse route injection for any connection based this crypto map entry, use the **no** form of this command.

crypto map *map-name seq-num set reverse-route*

no crypto map *map-name seq-num set reverse-route*

Syntax Description

<i>map-name</i>	Specifies the name of the crypto map set.
<i>seq-num</i>	Specifies the number you assign to the crypto map entry.

Defaults

The default setting for this command is off.

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
Global configuration	•	•	•	—	—

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

The security appliance can automatically add static routes to the routing table and announce these routes to its private network or border routers using OSPF.

Examples

The following example, entered in global configuration mode, enables RRI for the crypto map named mymap.

```
hostname(config)# crypto map mymap 10 set reverse-route
hostname(config)#
```

Related Commands

Command	Description
clear configure crypto map	Clears all configuration for all crypto maps.
show running-config crypto map	Displays the crypto map configuration.

crypto map set security-association lifetime

To override (for a particular crypto map entry) the global lifetime value, which is used when negotiating IPSec security associations, use the **crypto map set security-association lifetime** command in global configuration mode. To reset a crypto map entry's lifetime value to the global value, use the **no** form of this command.

crypto map *map-name seq-num* **set security-association lifetime** {seconds *seconds* |
kilobytes *kilobytes*}

no crypto map *map-name seq-num* **set security-association lifetime** {seconds *seconds* |
kilobytes *kilobytes*}

Syntax Description

<i>kilobytes</i>	Specifies the volume of traffic (in kilobytes) that can pass between peers using a given security association before that security association expires. The default is 4,608,000 kilobytes.
<i>map-name</i>	Specifies the name of the crypto map set.
<i>seconds</i>	Specifies the number of seconds a security association will live before it expires. The default is 28,800 seconds (eight hours).
<i>seq-num</i>	Specifies the number you assign to the crypto map entry.

Defaults

The default number of kilobytes is 4,608,000; the default number of seconds is 28,800.

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
Global configuration	•	•	•	—	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

The crypto map's security associations are negotiated according to the global lifetimes.

IPSec security associations use shared secret keys. These keys and their security associations time out together.

Assuming that the particular crypto map entry has lifetime values configured, when the security appliance requests new security associations during security association negotiation, it specifies its crypto map lifetime values in the request to the peer; it uses these values as the lifetime of the new security associations. When the security appliance receives a negotiation request from the peer, it uses the smaller of the lifetime values proposed by the peer or the locally configured lifetime values as the lifetime of the new security associations.

There are two lifetimes: a “timed” lifetime and a “traffic-volume” lifetime. The session keys/security association expires after the first of these lifetimes is reached. You can specify both with one command.

**Note**

The security appliance lets you change crypto map, dynamic map, and ipsec settings on the fly. If you do so, the security appliance brings down only the connections affected by the change. If you change an existing access-list associated with a crypto map, specifically by deleting an entry within the access-list, the result is that only the associated connection is brought down. Connections based on other entries in the access-list are not affected.

To change the timed lifetime, use the **crypto map set security-association lifetime seconds** command. The timed lifetime causes the keys and security association to time out after the specified number of seconds have passed.

Examples

The following command, entered in global configuration mode, specifies a security association lifetime in seconds and kilobytes for crypto map mymap

```
hostname(config)# crypto map mymap 10 set security-association lifetime seconds 1400  
kilobytes 3000000  
hostname(config)#
```

Related Commands

Command	Description
clear configure crypto map	Clears all configuration for all crypto maps.
show running-config crypto map	Displays the crypto map configuration.

crypto map set transform-set

To specify the transform sets to use with the crypto map entry, use the **crypto map set transform-set** command in global configuration mode. Use the **no** form of this command to remove the specified transform sets from a crypto map entry.

crypto map *map-name seq-num set transform-set transform-set-name1*
[... *transform-set-name9*]

no crypto map *map-name seq-num set transform-set transform-set-name1*
[... *transform-set-name9*]

Syntax Description

<i>map-name</i>	Specifies the name of the crypto map set.
<i>seq-num</i>	Specifies the number you assign to the crypto map entry.
<i>transform-set-name1</i> <i>transform-set-name9</i>	Specifies the name(s) of the transform set(s), defined using the crypto ipsec transform-set command, to use for the crypto map. For an ipsec-isakmp or dynamic crypto map entry, you can specify up to nine transform sets.

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		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	•	•	•	—	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

This command is required for all crypto map entries.

If the local security appliance initiates the negotiation, the transform sets are presented to the peer in the order specified in the **crypto map** command statement. If the peer initiates the negotiation, the local security appliance accepts the first transform set that matches one of the transform sets specified in the crypto map entry.

The first matching transform set that is found at both peers is used for the security association. If no match is found, IPSec does not establish a security association. The traffic is dropped because there is no security association to protect the traffic.

If you want to change the list of transform sets, respecify the new list of transform sets to replace the old list. This change is applied only to **crypto map** command statements that reference this transform set.

Any transform sets included in a **crypto map** command statement must previously have been defined using the **crypto ipsec transform-set** command.

Examples

The following example, entered in global configuration mode, specifies two transform sets (tfset1 and tfset2) for the crypto map mymap.

```
hostname(config)# crypto map mymap 10 set transform-set tfset1 tfset2
hostname(config)#
```

The following example, entered in global configuration mode, shows the minimum required crypto map configuration when the security appliance uses IKE to establish the security associations:

```
hostname(config)# crypto map mymap 10 ipsec-isakmp
hostname(config)# crypto map mymap 10 match address 101
hostname(config)# crypto map mymap set transform-set my_t_set1
hostname(config)# crypto map mymap set peer 10.0.0.1
hostname(config)#
```

Related Commands

Command	Description
clear configure crypto map	Clears all configuration for all crypto maps.
crypto ipsec transform-set	Configures a transform-set.
show running-config crypto map	Displays the crypto map configuration.

crypto map set trustpoint

To specify the trustpoint that identifies the certificate to send for authentication during Phase 1 negotiations for the crypto map entry, use the **crypto map set trustpoint** command in global configuration mode. Use the **no** form of this command to remove a trustpoint from a crypto map entry.

crypto map *map-name seq-num set trustpoint trustpoint-name [chain]*

no crypto map *map-name seq-num set trustpoint trustpoint-name [chain]*

Syntax Description

chain	(Optional) Sends a certificate chain. A CA certificate chain includes all CA certificates in a hierarchy of certificates from the root certificate to the identity certificate. The default value is disable (no chain).
<i>map-name</i>	Specifies the name of the crypto map set.
<i>seq-num</i>	Specifies the number you assign to the crypto map entry.
<i>trustpoint-name</i>	Identifies the certificate to be sent during Phase 1 negotiations. The default is none.

Defaults

The default value is none.

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
Global configuration	•	•	•	—	—

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

This crypto map command is valid only for initiating a connection. For information on the responder side, see the **tunnel-group** commands.

Examples

The following example, entered in global configuration mode, specifies a trustpoint named tpoint1 for crypto map mymap and includes the chain of certificates.

```
hostname(config)# crypto map mymap 10 set trustpoint tpoint1 chain
hostname(config)#
```

Related Commands

Command	Description
clear configure crypto map	Clears all configuration for all crypto maps.
show running-config crypto map	Displays the crypto map configuration.
tunnel-group	Configures tunnel groups.

