



clear console-output through clear xlate Commands

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.

Examples The following example shows how to remove the currently captured console output:

```
hostname# clear console-output
```

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

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(1)	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.

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(1)	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

<i>trustpointname</i>	(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(1)	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:

	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 example, issued in global configuration mode, removes all of the IPSec SAs from the security appliance:

```
hostname(config)# clear ipsec sa
```

■ clear [crypto] 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

<i>protocol</i>	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(1)	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 dhcp** 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	•	—	•	•	—

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#
```

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(1)	This command was introduced.

Examples The following example clears the DNS cache:

```
hostname# clear dns-hosts cache
```

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.

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.

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(1)	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	•	•	•	—	•

Release	Modification
7.0(1)	This command was introduced.

Examples The following example shows how to remove the garbage collection process statistics:

```
hostname# clear gc
```

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

<i>if_name</i>	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(1)	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:

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 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

The **clear interface** command clears all interface statistics except the number of input bytes. See the **show interface** command for detail about interface statistics.

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:

Command Mode	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(1)	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	•	—	•	•	—

Release	Modification
7.0(1)	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#
```

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	•	—	•	•	—

Command History	Release	Modification
	7.0(1)	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
  hopcount expired, 0 reassembly timeout, 0 too big
```

■ clear ipv6 traffic

```

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(1)	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	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	•	•	•	•	•

Release	Modification
7.0(1)(1)	This command was changed from the show pdm logging command to the show asdm log command.

Usage Guidelines

ASDM system log messages are stored in a separate buffer from the security appliance system log messages. Clearing the ASDM logging buffer only clears the ASDM system log messages; it does not clear the security appliance system log messages. To view the ASDM system log messages, use the **show asdm log** command.

Examples

The following example clears the ASDM logging buffer:

```
hostname(config)# clear logging asdm
hostname(config)#
```

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

Examples This example shows how to clear the contents of the log buffer:

```
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	<i>interface_name</i> (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(1)	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	•	•	•	—	•

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(1)	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 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(1)	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(1)	This command was introduced.

Examples	<p>The following example clears the recovery settings for the AIP SSM:</p> <pre>hostname# clear module 1 recover</pre>
----------	--

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
```

 clear ospf**Related Commands**

Command	Description
clear configure router	Clears all global router commands from the running configuration.

clear pc

To clear connection, xlate, or local-host information maintained on PC, use the **clear pc** command in global configuration mode.

clear pc

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(1)	This command was introduced.

Examples

The following example clears PC information:

```
hostname(config)# clear pc
```

Related Commands

Command	Description
clear pclu	Clears PC logical update statistics.

clear pclu

To clear PC logical update statistics, use the **clear pclu** command in global configuration mode.

clear pclu

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(1)	This command was introduced.

Examples The following example clears PC information:

```
hostname(config)# clear pclu
```

Command	Description
clear pc	Clears connection, xlate, or local-host information maintained on PC.

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(1)	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	•	—	•	—	—

Release	Modification
7.0(1)	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
```

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

group (Optional) Specifies the multicast group address or name to be deleted from the topology table.

Defaults

Without the optional *group* 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(1)	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	<i>interface-name</i>	(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(1)	This command was introduced.

Examples	<p>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”.</p> <pre>hostname# clear priority-queue statistics test hostname#</pre>	
----------	---	--

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(1)	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(1)	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(1)	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
	7.0(1)	This command was introduced.

Examples	<p>The following example shows how to disable all the shuns that are currently enabled and clear the shun statistics:</p> <pre>hostname(config)# clear shun</pre>
----------	---

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 startup-config errors

To clear configuration error messages from memory, use the **clear startup-config errors** command in privileged EXEC mode.

clear startup-config errors

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(1)	This command was introduced.

Usage Guidelines To view configuration errors generated when the security appliance loaded the startup configuration, use the **show startup-config errors** command.

Examples The following example clears all configuration errors from memory:

```
hostname# clear startup-config errors
```

Related Commands	Command	Description
	show startup-config errors	Shows configuration errors generated when the security appliance loaded the startup configuration.

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	•	•	•	•	—

Command History	Release	Modification
	Preexisting	This command was preexisting.

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
```

Related Commands	Command	Description
	show traffic	Displays the counters for transmit and receive activity.

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	•	•	•	•	•

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	•	•	•	•	•

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
```

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	•	•	•	•	•

Release	Modification
Preexisting	This command was preexisting.

Command History

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[-ip2]</i>	(Optional)	Clears the active translations by global IP address or range of addresses.
gport <i>port1[-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[-ip2]</i>	(Optional)	Clears the active translations by local IP address or range of addresses.
lport <i>port1[-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. 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.