



clear conn through clear xlate Commands

clear conn

To clear through-the-box connections based on the IP address, use the **clear conn** command in privileged EXEC mode.



Note

We recommend that you use the **clear xlate** command instead of **clear conn**; **clear xlate** has finer control of the connections cleared (including port specification), and is more reliable. The **clear xlate** command clears all connections, not just those with active translation sessions.

```
clear conn [{local | foreign} ip_address [netmask mask]]
```

Syntax Description

local	(Optional) Clears connections with the specified local IP address. “Local” means that the IP address is on a higher security interface than its peer for a given connection. If you clear all local connections for a given IP address, then connections where the specified IP address is on a <i>lower</i> security level than its peer are not affected. For example, for a connection between Host A on the DMZ interface (security level 50) and Host B on the outside interface (security level 0), Host A is the local address. But for a connection between Host A and Host C on the inside interface (security level 0), Host A is the foreign IP address.
foreign	(Optional) Clears connections with the specified foreign IP address. “Foreign” means that the IP address is on a lower security interface than its peer for a given connection. If you clear all foreign connections for a given IP address, then connections where the specified IP address is on a <i>higher</i> security level than its peer are not affected. See the description for local for an example.
<i>ip_address</i>	(Optional) Specifies the IPv4 IP address.
netmask mask	(Optional) Specifies a subnet mask for use with the given IP address.

Defaults

Without any arguments, all through-the-box connections 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
1.1(1)	This command was introduced.

Usage Guidelines

You cannot clear management (to-the-box) connections with this command.

When you make security policy changes to the configuration, *do not use* the **clear conn** command to ensure that all connections use the new security policy. The **clear conn** command causes the teardown of all connections established in the network processors (NPs); it does not affect the xlates and it does not clean up the connection database in the control plane. As a result, it may cause the NPs and PC to get out of sync. When you make a security policy change, all existing connections continue to use the policy that was configured at the time of the connection establishment. To ensure that all connections use the new policy, you need to disconnect the current connections so they can reconnect using the new policy. Use the **clear xlate** command to clear all connections (**clear xlate** clears all connections, not just those with translation sessions). **clear xlate** also enforces the PC side to flush its databases allowing the system to remain in sync. You can alternatively use the **clear local-host** command to clear connections per host.

Examples

The following example shows all connections, and then clears the connections where 10.61.98.215 is the foreign address:

```
hostname# show conn
0 in use, 0 most used
  Network Processor 1 connections
TCP out 10.61.98.215:1935 in 172.23.204.14:443 idle 0:00:00 Bytes 60536 FLAGS - UBOI
TCP out 10.61.98.215:1938 in 172.23.204.14:443 idle 0:00:05 Bytes 61240 FLAGS - UBOI
TCP out 10.61.98.215:1961 in 172.23.204.14:443 idle 0:00:00 Bytes 3058 FLAGS - UBOI
  Network Processor 2 connections
Multicast sessions:
  Network Processor 1 connections
  Network Processor 2 connections
IPv6 connections

hostname# clear conn foreign 10.61.98.215
```

Related Commandss

Commands	Description
clear local-host	Clears all connections by a specific local host or all local hosts.
clear xlate	Clears all connections.
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	•	•	•	•	•

Command History	Release	Modification
	1.1(1)	This command was introduced.

Usage Guidelines The FWSM automatically captures output destined for the internal console port. Do not use the internal console port unless you are advised to do so by Cisco TAC.

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

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

Related Commands	Command	Description
	show console-output	Displays the captured console output.

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	(Multiple mode only) Clears counters for all contexts.
context <i>context-name</i>	(Multiple mode only) Clears counters for the specified context name.
:counter_name	(Optional) Clears the specified counter.
detail	(Optional) Clears detailed counter information.
protocol <i>protocol_name</i>	(Optional) Clears the counters for the specified protocol.
summary	(Multiple mode only) Clears counters for all contexts.
threshold <i>n</i>	(Optional) Clears the counters at or above the specified threshold. The range is 1 through 4294967295.
top <i>n</i>	(Multiple mode only) Clears a counter for the contexts that are the top <i>n</i> users of the counter. You must specify a counter name with this option. The range is 1 through 4294967295.

Defaults

By default, the FWSM clears all counters.

Command Modes

The 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 the protocol stack counters:

```
hostname(config)# clear counters
```

Related Commands

Command	Description
show counters	Displays the protocol stack counters.
show counters description	Shows a list of protocol 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
3.1(1)	This command was introduced.

Command History

Usage Guidelines This command has no usage guidelines.

Examples The following example shows how to delete the crash file:

```
hostname# clear crashinfo
```

clear crashinfo force	Forces a crash of the FWSM.
clear crashinfo save disable	Disables crash information from writing to Flash memory.
clear crashinfo test	Tests the ability of the FWSM to save crash information to a file in Flash memory.
show crashinfo	Displays the contents of the crash file stored in Flash memory.

Related Commands

clear crypto accelerator statistics

To clear the global and accelerator-specific statistics from the crypto accelerator MIB, use the **clear crypto accelerator statistics** command in 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
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
3.1(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 mode.

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
3.1(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 FWSM:

```
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 protocol statistics

To clear the protocol-specific statistics in the crypto accelerator MIB, use the **clear crypto protocol statistics** command in 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 Sockets 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
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
3.1(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 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
	2.2(1)	This command was introduced.

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	•	•	•	•	—

Command History	Release	Modification
	3.1(1)	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 FWSM 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 FWSM 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	•	•	•	•	•

Command History	Release	Modification
	3.1(1)	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#
```

Related Commands	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 FWSM 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
1.1(1)	This command was introduced.
3.1(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.

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 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
	1.1(1)	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

<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.
----------------	--

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
3.1(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	group	IGMP group address. Specifying a particular group removes the specified group from the cache.
	interface name	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
	3.1(1)	This command was introduced.

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
	3.1(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 [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.

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
1.1(1)	This command was introduced.

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 FWSM clears only statistics for the current context. If you enter this command in the system execution space, the FWSM 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 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. <i>interface_name</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
Privileged EXEC	•	—	•	•	—

Command History	Release	Modification
	3.1(1)	This command was introduced.

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 privileged EXEC mode. 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
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
3.1(1)	This command was introduced.

Examples

The following example clears all IPsec SA counters:

```
hostname# clear ipsec sa counters
hostname#
```

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
3.1(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	•	—	•	•	—

Command History	Release	Modification
	3.1(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#
```

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	•	—	•	•	—

Command History	Release	Modification
	3.1(1)	This command was introduced.

Usage Guidelines 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 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
Privileged EXEC	•	•	•	•	—

Command History	Release	Modification
	3.1(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 sa	Clears the IKE runtime SA database.
	isakmp enable	Enables ISAKMP negotiation on the interface on which the IPsec peer communicates with the FWSM.
	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 remove network connections, use the **clear local-host** command in privileged EXEC mode.

```
clear local-host [ip_address] [all]
```



Note

When you specify the IP address of 0.0.0.0, all local-host entries will be matched and cleared. This special IP address is treated as a wildcard mask for all addresses. Therefore, there is no way to clear just the local-host entries involving 0.0.0.0 IP address (such as DHCP).

Syntax Description

all	(Optional) Clears all connections, except for those directly to the FWSM and from the FWSM.
<i>ip_address</i>	(Optional) Specifies the host IP address for which you want to clear connections.

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
1.1(1)	This command was introduced.

Examples

The following example clears all connections from 10.1.1.15:

```
hostname# clear local-host 10.1.1.15
```



Note

If you enter the **clear local 10.1.1.15** command then the uauth of the IP address 10.1.1.15 is also cleared. If you enter the **clear local** or **clear local all** commands then the uauth is not cleared.

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
	3.1(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 FWSM system log messages. Clearing the ASDM logging buffer only clears the ASDM system log messages, it does not clear the FWSM system 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)#
```

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
	3.1(1)	This command was introduced.

Examples The following example shows how to remove all system log messages from the internal log buffer:

```
hostname #clear logging buffer
```

Related Commands	Command	Description
	logging buffered	Specifies the log buffer as an output destination, enabling event messages to be written to the log buffer as they occur.
	show logging	Displays the enabled logging options.

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
	2.2(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	•	•	•	—	•

Command History

Release	Modification
3.1(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
	3.1(1)	Support for 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: <pre>hostname# clear memory profile</pre>
-----------------	--

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 FWSM.

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	group	(Optional) IP address of the multicast group.
	source	(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
	3.1(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 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
3.1(1)	This command was introduced.

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
	3.1(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	•	—	•	—	—

Command History	Release	Modification
	3.1(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
```

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

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
3.1(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 prompt

To clear the configured prompt, enter the **clear prompt** command in global configuration mode (P_CONF), replicated (P_REP) and in single mode, and in the system context in multi-mode. This command clears all the prompts that have been configured. Only an administrator can view the configured prompt. If you are in user context, you can see the default hostname/context (config-mode) prompt.

```
clear prompt [<keyword> [keyword] ...]
```

Syntax Description

Keyword	Description
<i>context</i>	Configures the prompt to display the current context (multimode only).
<i>domain</i>	Configures the prompt to display the domain.
<i>hostname</i>	Configures the prompt to display the hostname.
<i>priority</i>	Configures the prompt to display the 'failover lan unit' setting.
<i>slot</i>	Configures the prompt to display the slot location (when applicable).
<i>state</i>	Configures the prompt to display the current traffic handling state.

Defaults

The default is hostname/context (config-mode) prompt.

Command Modes

The 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
3.1(1)	This command was introduced.

Usage Guidelines

The ability to add information to a prompt allows you to see at-a-glance which module you are logged into when you have multiple modules. During a failover, this is important where both modules have the same hostname.

Examples

The following example shows how to clear prompts with the hostname, domain, context, priority, slot and state keywords:

```
fwsn(config)# clear prompt hostname context priority slot state
```

Related Commands

Command	Description
prompt	Configures the sessioned prompt display.
show prompt	Displays the configured prompt.

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>	Clears the usage of a specific resource. Specify all (the default) for all resources. Resources include the following types: <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 FWSM. • 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
2.2(1)	This command was introduced.

Examples

The following example clears all resource usage statistics:

```
hostname# clear resource usage
```

■ 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 FWSM.

clear route

To remove dynamically learned routes from the routing table, use the **clear route** command in privileged EXEC mode.

clear route [statistics]

Syntax Description

statistics (Optional) Clears route statistical 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
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
1.1(1)	This command was introduced.

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:

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

Command History

Release	Modification
3.1(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 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
3.1(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	<i>statistics</i> (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
2.2(1)	Support for this command was introduced.
3.1(1)	This command was changed from clear rpc-server .

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 FWSM.

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 FWSM.
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.
sunrpc-server	Creates entries in the SunRPC services table.

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
1.1(1)	This command was introduced.

Command History

Usage Guidelines The **clear traffic** command resets the counters for transmit and receive activity that is displayed with the **show traffic** command.

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
1.1(1)	This command was introduced.

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 FWSM 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 rlee to reauthenticate:

```
hostname(config)# clear uauth rlee
```

Related Commands

Command	Description
aaa authentication	Enable or disable user authentication.
aaa authorization	Enable or disable user authorization.
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
1.1(1)	The clear url-block command was introduced.
3.1(1)	This command was changed from clear url-block .

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
1.1(1)	The clear url-cache command was introduced.
3.1(1)	This command was changed from clear url-cache .

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 that 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
1.1(1)	The clear url-server command was introduced.
3.1(1)	This command was changed from clear url-server .

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, and to clear all connections, not just those that have active xlates, 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:

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.

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.

The **clear xlate** command clears all connections, even when xlate-bypass is enabled and when a connection does not have an xlate.

When you make security policy changes to the configuration, use the **clear xlate** command to ensure that all connections use the new security policy. When you make a security policy change, all existing connections continue to use the policy that was configured at the time of the connection establishment. To ensure that all connections use the new policy, you need to disconnect the current connections so they can reconnect using the new policy. **clear xlate** also enforces the PC side to flush its databases allowing the system to remain in sync. You can alternatively use the **clear local-host** command to clear connections per host. Do not use the clear conn command to clear all connections; it can cause the network processors (NPs) to get out of sync with with the PC.

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. A dynamic xlate is an xlate that is created on demand with traffic processing (through the **nat** or **global** command).

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.

