CHAPTER 6

clear conn through clear xlate Commands

clear conn

To clear a specific connection or multiple connections, use the **clear conn** command in privileged EXEC mode. This command supports IPv4 and IPv6 addresses.

clear conn [**all**] [**protocol** {**tcp** | **udp**}] [**address** *src_ip*[**-***src_ip*] [**netmask** *mask*]]
[**port** *src_port*[**-***src_port*]] [**address** *dest_ip*[**-***dest_ip*] [**netmask** *mask*]]
[**port** *dest_port*[**-***dest_port*]]

Syntax Description

address	(Optional) Clears connections with the specified source or destination IP address.
all	(Optional) Clears all connections, including to-the-box connections. Without the **all** keyword, only through-the-box connections are cleared.
dest_ip	(Optional) Specifies the destination IP address (IPv4 or IPv6). To specify a range, separate the IP addresses with a dash (-), For example: `10.1.1.1-10.1.1.5`
dest_port	(Optional) Specifies the destination port number. To specify a range, separate the port numbers with a dash (-), For example: `1000-2000`
netmask *mask*	(Optional) Specifies a subnet mask for use with the given IP address.
port	(Optional) Clears connections with the specified source or destination port.
protocol {tcp | udp}	(Optional) Clears connections with the protocol **tcp** or **udp**.
src_ip	(Optional) Specifies the source IP address (IPv4 or IPv6). To specify a range, separate the IP addresses with a dash (-), For example: `10.1.1.1-10.1.1.5`
src_port	(Optional) Specifies the source port number. To specify a range, separate the port numbers with a dash (-), For example: `1000-2000`

Command Modes

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

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

Command History

Release	Modification
7.0(8)/7.2(4)/8.0(4)	This command was introduced.

Usage Guidelines

When you make security policy changes to the configuration, all *new* connections use the new security policy. 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 using the **clear conn** command. You can alternatively use the **clear local-host** command to clear connections per host, or the **clear xlate** command for connections that use dynamic NAT.

When the adaptive security appliance creates a pinhole to allow secondary connections, this is shown as an incomplete conn by the **show conn** command. To clear this incomplete conn use the **clear conn** command.

Examples

The following example shows all connections, and then clears the management connection between 10.10.10.108:4168 and 10.0.8.112:22:

```
hostname# show conn all
TCP mgmt 10.10.10.108:4168 NP Identity Ifc 10.0.8.112:22, idle 0:00:00, bytes 3084, flags
UOB

hostname# clear conn address 10.10.10.108 port 4168 address 10.0.8.112 port 22
```

Related Commandss

Commands	Description
clear local-host	Clears all connections by a specific local host or all local hosts.
clear xlate	Clears a dynamic NAT session, and any connections using NAT.
show conn	Shows connection information.
show local-host	Displays the network states of local hosts.
show xlate	Shows NAT sessions.

clear console-output

To remove the currently captured console output, use the **clear console-output** command in privileged EXEC mode.

clear console-output

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
Preexisting	This command was preexisting.

Examples

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

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

Related Commands

Command	Description
console timeout	Sets the idle timeout for a console connection to the adaptive 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 adaptive security appliance.

clear coredump

To remove coredump filesystem contents and clear the coredump log, enter the **clear coredump** command.

clear coredump

Syntax Description

This command has no arguments or keywords.

Defaults

By default, coredumps are not enabled.

Command Modes

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

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

Command History

Release	Modification
8.2(1)	This command was introduced.

Usage Guidelines

This command removes the coredump filesystem contents and the coredump log. The coredump filesystem remains intact. Current coredump configuration remains unchanged.

Examples

The following example removes the coredump filesystem contents and the coredump log:

```
hostname(config)# clear coredump
Proceed with removing the contents of the coredump filesystem on 'disk0:' [confirm]
```

Related Commands

Command	Description
coredump enable	Enables the coredump feature.
clear configure coredump	Removes the coredump filesystem and it's contents from your system. Also clears the coredump log. This disables coredump and changes the configuration, you must save the configuration after performing this operation.
show coredump filesystem	Displays files on the coredump filesystem, also gives a clue as to how full it might be.
show coredump log	Shows the coredump log.

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 *context-name*	(Optional) Specifies the context name.
:*counter_name*	(Optional) Specifies a counter by name.
detail	(Optional) Clears detailed counters information.
protocol *protocol_name*	(Optional) Clears the counters for the specified protocol.
summary	(Optional) Clears the counter summary.
threshold *N*	(Optional) Clears the counters at or above the specified threshold. The range is 1 through 4294967295.
top *N*	(Optional) Clears the counters at or above the specified threshold. The range is 1 through 4294967295.

Defaults

The **clear counters summary detail** is the default.

Command Modes

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

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

Command History

Release	Modification
7.0	This command was introduced.

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, use 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:

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

Command History

Release	Modification
Preexisting	This command was preexisting.

Examples

The following command shows how to delete the crash file:

```
hostname# clear crashinfo
```

Related Commands

crashinfo force	Forces a crash of the adaptive security appliance.
crashinfo save disable	Disables crash information from writing to Flash memory.
crashinfo test	Tests the ability of the adaptive 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 privileged EXEC mode.

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:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
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 privileged EXEC 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:

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

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 adaptive security appliance:

```
hostname# clear crypto ca crls
hostname#
```

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 privileged EXEC 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.
hostname	Identified a hostname assigned to an IP address.
ip_address	Identifies an IP address.
map	Deletes all tunnels associated with the specified crypto map as identified by map name.
map name	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.
spi	Identifies the Security Parameters Index (a hexidecimal number). This must be the inbound spi. We do not support this command for the outbound spi.

Defaults

No default behavior or values.

Command Modes

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

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

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 adaptive security appliance:

```
hostname# clear crypto ipsec sa
hostname#
```

The next example, issued in global configuration mode, deletes SAs with a peer IP address of 10.86.1.1.

```
hostname# clear crypto ipsec peer 10.86.1.1
hostname#
```

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 privileged EXEC mode.

clear crypto protocol statistics *protocol*

Syntax Description

protocol	Specifies the name of the protocol for which you want to clear statistics. Protocol choices are as follows: • **ikev1**—Internet Key Exchange version 1. • **ipsec**—IP Security Phase-2 protocols. • **ssl**—Secure Socket Layer. • **other**—Reserved for new protocols. • **all**—All protocols currently supported. In online help for this command, other protocols may appear that will be supported in future releases.

Defaults

No default behavior or values.

Command Modes

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

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
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# clear crypto protocol statistics all
hostname#
```

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 in privileged EXEC mode.

clear dhcpd {**binding** [*ip_address*] | **statistics**}

Syntax Description

binding	Clears all the client address bindings.
ip_address	(Optional) 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:

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

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# 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:

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

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

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

Examples

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

```
hostname# clear dhcprelay statistics
hostname#
```

Related Commands

Command	Description
clear configure dhcprelay	Removes all DHCP relay agent settings.
debug dhcprelay	Displays debug information for the DHCP relay agent.
show dhcprelay statistics	Displays DHCP relay agent statistic information.
show running-config dhcprelay	Displays the current DHCP relay agent configuration.

clear dns-hosts cache

To clear the DNS cache, use the **clear dns-hosts cache** command in privileged EXEC mode. This command does not clear static entries you added with the **name** command.

clear dns-hosts cache

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(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 adaptive 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 adaptive 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 dynamic-filter dns-snoop

To clear Botnet Traffic Filter DNS snooping data, use the **clear dynamic-filter dns-snoop** command in in privileged EXEC mode.

clear dynamic-filter dns-snoop

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
8.2(1)	This command was introduced.

Examples

The following example clears all Botnet Traffic Filter DNS snooping data:

```
hostname# clear dynamic-filter dns-snoop
```

Related Commands

Command	Description
address	Adds an IP address to the blacklist or whitelist.
clear configure dynamic-filter	Clears the running Botnet Traffic Filter configuration.
clear dynamic-filter reports	Clears Botnet Traffic filter report data.
clear dynamic-filter statistics	Clears Botnet Traffic filter statistics.
dns domain-lookup	Enables the adaptive security appliance to send DNS requests to a DNS server to perform a name lookup for supported commands.
dns server-group	Identifies a DNS server for the adaptive security appliance.
dynamic-filter ambiguous-is-black	Treats greylisted traffic as blacklisted traffic for action purposes.
dynamic-filter blacklist	Edits the Botnet Traffic Filter blacklist.
dynamic-filter database fetch	Manually retrieves the Botnet Traffic Filter dynamic database.
dynamic-filter database find	Searches the dynamic database for a domain name or IP address.

Command	Description
dynamic-filter database purge	Manually deletes the Botnet Traffic Filter dynamic database.
dynamic-filter drop blacklist	Automatically drops blacklisted traffic.
dynamic-filter enable	Enables the Botnet Traffic Filter for a class of traffic or for all traffic if you do not specify an access list.
dynamic-filter updater-client enable	Enables downloading of the dynamic database.
dynamic-filter use-database	Enables use of the dynamic database.
dynamic-filter whitelist	Edits the Botnet Traffic Filter whitelist.
inspect dns dynamic-filter-snoop	Enables DNS inspection with Botnet Traffic Filter snooping.
name	Adds a name to the blacklist or whitelist.
show asp table dynamic-filter	Shows the Botnet Traffic Filter rules that are installed in the accelerated security path.
show dynamic-filter data	Shows information about the dynamic database, including when the dynamic database was last downloaded, the version of the database, how many entries the database contains, and 10 sample entries.
show dynamic-filter dns-snoop	Shows the Botnet Traffic Filter DNS snooping summary, or with the **detail** keyword, the actual IP addresses and names.
show dynamic-filter reports	Generates reports of the top 10 botnet sites, ports, and infected hosts.
show dynamic-filter statistics	Shows how many connections were monitored with the Botnet Traffic Filter, and how many of those connections match the whitelist, blacklist, and greylist.
show dynamic-filter updater-client	Shows information about the updater server, including the server IP address, the next time the adaptive security appliance will connect with the server, and the database version last installed.
show running-config dynamic-filter	Shows the Botnet Traffic Filter running configuration.

clear dynamic-filter reports

To clear report data for the Botnet Traffic Filter, use the **clear dynamic-filter reports** command in privileged EXEC mode.

clear dynamic-filter reports {**top** [**malware-sites** | **malware-ports** | **infected-hosts**] | **infected-hosts**}

Syntax Description

malware-ports	(Optional) Clears report data for the top 10 malware ports.
malware-sites	(Optional) Clears report data for the top 10 malware sites.
infected-hosts (top)	(Optional) Clears report data for the top 10 infected hosts.
top	Clears report data for the top 10 malware sites, ports, and infected hosts.
infected-hosts	Clears report data for infected hosts.

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
8.2(1)	This command was introduced.
8.2(2)	The **botnet-sites** and **botnet-ports** keywords were changed to **malware-sites** and **malware-ports**. The **top** keyword was added to differentiate clearing the top 10 reports and the new infected-hosts reports. The **infected-hosts** keyword was added (without **top**).

Examples

The following example clears all Botnet Traffic Filter top 10 report data:

```
hostname# clear dynamic-filter reports top
```

The following example clears only the top 10 malware sites report data:

```
hostname# clear dynamic-filter reports top malware-sites
```

The following example clears all infected hosts report data:

```
hostname# clear dynamic-filter reports infected-hosts
```

Related Commands

Command	Description
address	Adds an IP address to the blacklist or whitelist.
clear configure dynamic-filter	Clears the running Botnet Traffic Filter configuration.
clear dynamic-filter dns-snoop	Clears Botnet Traffic Filter DNS snooping data.
clear dynamic-filter statistics	Clears Botnet Traffic filter statistics.
dns domain-lookup	Enables the adaptive security appliance to send DNS requests to a DNS server to perform a name lookup for supported commands.
dns server-group	Identifies a DNS server for the adaptive security appliance.
dynamic-filter ambiguous-is-black	Treats greylisted traffic as blacklisted traffic for action purposes.
dynamic-filter blacklist	Edits the Botnet Traffic Filter blacklist.
dynamic-filter database fetch	Manually retrieves the Botnet Traffic Filter dynamic database.
dynamic-filter database find	Searches the dynamic database for a domain name or IP address.
dynamic-filter database purge	Manually deletes the Botnet Traffic Filter dynamic database.
dynamic-filter drop blacklist	Automatically drops blacklisted traffic.
dynamic-filter enable	Enables the Botnet Traffic Filter for a class of traffic or for all traffic if you do not specify an access list.
dynamic-filter updater-client enable	Enables downloading of the dynamic database.
dynamic-filter use-database	Enables use of the dynamic database.
dynamic-filter whitelist	Edits the Botnet Traffic Filter whitelist.
inspect dns dynamic-filter-snoop	Enables DNS inspection with Botnet Traffic Filter snooping.
name	Adds a name to the blacklist or whitelist.
show asp table dynamic-filter	Shows the Botnet Traffic Filter rules that are installed in the accelerated security path.
show dynamic-filter data	Shows information about the dynamic database, including when the dynamic database was last downloaded, the version of the database, how many entries the database contains, and 10 sample entries.
show dynamic-filter dns-snoop	Shows the Botnet Traffic Filter DNS snooping summary, or with the **detail** keyword, the actual IP addresses and names.
show dynamic-filter reports infected-hosts	Generates reports of infected hosts.
show dynamic-filter reports top	Generates reports of the top 10 malware sites, ports, and infected hosts.
show dynamic-filter statistics	Shows how many connections were monitored with the Botnet Traffic Filter, and how many of those connections match the whitelist, blacklist, and greylist.
show dynamic-filter updater-client	Shows information about the updater server, including the server IP address, the next time the adaptive security appliance will connect with the server, and the database version last installed.
show running-config dynamic-filter	Shows the Botnet Traffic Filter running configuration.

clear dynamic-filter statistics

To clear Botnet Traffic Filter statistics, use the **clear dynamic-filter statistics** command in in privileged EXEC mode.

clear dynamic-filter statistics [**interface** *name*]

Syntax Description

interface *name*	(Optional) Clears statistics for a particular interface.

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
8.2(1)	This command was introduced.

Examples

The following example clears all Botnet Traffic Filter DNS statistics:

```
hostname# clear dynamic-filter statistics
```

Related Commands

Command	Description
dynamic-filter ambiguous-is-black	Treats greylisted traffic as blacklisted traffic for action purposes.
dynamic-filter drop blacklist	Automatically drops blacklisted traffic.
address	Adds an IP address to the blacklist or whitelist.
clear configure dynamic-filter	Clears the running Botnet Traffic Filter configuration.
clear dynamic-filter dns-snoop	Clears Botnet Traffic Filter DNS snooping data.
clear dynamic-filter reports	Clears Botnet Traffic filter report data.
dns domain-lookup	Enables the adaptive security appliance to send DNS requests to a DNS server to perform a name lookup for supported commands.
dns server-group	Identifies a DNS server for the adaptive security appliance.
dynamic-filter blacklist	Edits the Botnet Traffic Filter blacklist.
dynamic-filter database fetch	Manually retrieves the Botnet Traffic Filter dynamic database.

Command	Description
dynamic-filter database find	Searches the dynamic database for a domain name or IP address.
dynamic-filter database purge	Manually deletes the Botnet Traffic Filter dynamic database.
dynamic-filter enable	Enables the Botnet Traffic Filter for a class of traffic or for all traffic if you do not specify an access list.
dynamic-filter updater-client enable	Enables downloading of the dynamic database.
dynamic-filter use-database	Enables use of the dynamic database.
dynamic-filter whitelist	Edits the Botnet Traffic Filter whitelist.
inspect dns dynamic-filter-snoop	Enables DNS inspection with Botnet Traffic Filter snooping.
name	Adds a name to the blacklist or whitelist.
show asp table dynamic-filter	Shows the Botnet Traffic Filter rules that are installed in the accelerated security path.
show dynamic-filter data	Shows information about the dynamic database, including when the dynamic database was last downloaded, the version of the database, how many entries the database contains, and 10 sample entries.
show dynamic-filter dns-snoop	Shows the Botnet Traffic Filter DNS snooping summary, or with the **detail** keyword, the actual IP addresses and names.
show dynamic-filter reports infected-hosts	Generates reports of infected hosts.
show dynamic-filter reports top	Generates reports of the top 10 malware sites, ports, and infected hosts.
show dynamic-filter statistics	Shows how many connections were monitored with the Botnet Traffic Filter, and how many of those connections match the whitelist, blacklist, and greylist.
show dynamic-filter updater-client	Shows information about the updater server, including the server IP address, the next time the adaptive security appliance will connect with the server, and the database version last installed.
show running-config dynamic-filter	Shows the Botnet Traffic Filter running configuration.

clear eigrp events

To clear the EIGRP event log, use the **clear eigrp events** command in privileged EXEC mode.

clear eigrp [*as-number*] **events**

Syntax Description

as-number	(Optional) Specifies the autonomous system number of the EIGRP process for which you are clearing the event log. Because the adaptive security appliance only supports one EIGRP routing process, you do not need to specify the autonomous system number (process ID).

Defaults

No default behaviors or values.

Command Modes

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

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

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

You can use the **show eigrp events** command to view the EIGRP event log.

Examples

The following example clears the EIGRP event log:

```
hostname# clear eigrp events
```

Related Commands

Command	Description
show eigrp events	Displays the EIGRP event log.

clear eigrp neighbors

To delete entries from the EIGRP neighbor table, use the **clear eigrp neighbors** command in privileged EXEC mode.

clear eigrp [*as-number*] **neighbors** [*ip-addr* | *if-name*] [**soft**]

Syntax Description

as-number	(Optional) Specifies the autonomous system number of the EIGRP process for which you are deleting neighbor entries. Because the adaptive security appliance only supports one EIGRP routing process, you do not need to specify the autonomous system number (process ID).
if-name	(Optional) The name of an interface as specified by the **nameif** command. Specifying an interface name removes all neighbor table entries that were learned through this interface.
ip-addr	(Optional) The IP address of the neighbor you want to remove from the neighbor table.
soft	Causes the adaptive security appliance to resynchronize with the neighbor without resetting the adjacency.

Defaults

If you do not specify a neighbor IP address or an interface name, all dynamic entries are removed from the neighbor table.

Command Modes

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

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

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

The **clear eigrp neighbors** command does not remove neighbors defined using the **neighbor** command from the neighbor table. Only dynamically-discovered neighbors are removed.

You can use the **show eigrp neighbors** command to view the EIGRP neighbor table.

Examples

The following example removes all entries from the EIGRP neighbor table:

```
hostname# clear eigrp neighbors
```

The following example removes all entries learned through the interface named “outside” from the EIGRP neighbor table:

```
hostname# clear eigrp neighbors outside
```

Related Commands

Command	Description
debug eigrp neighbors	Displays debug information for EIGRP neighbors.
debug ip eigrp	Displays debug information for EIGRP protocol packets.
show eigrp neighbors	Displays the EIGRP neighbor table.

clear eigrp topology

To delete entries from the EIGRP topology table, use the **clear eigrp topology** command in privileged EXEC mode.

clear eigrp [*as-number*] **topology** *ip-addr* [*mask*]

Syntax Description

as-number	(Optional) Specifies the autonomous system number of the EIGRP process. Because the adaptive security appliance only supports one EIGRP routing process, you do not need to specify the autonomous system number (process ID).
ip-addr	The IP address to clear from the topology table.
mask	(Optional) The network mask to apply to the *ip-addr* argument.

Defaults

No default behaviors or values.

Command Modes

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

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

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

This command clears existing EIGRP entries from the EIGRP topology table. You can use the **show eigrp topology** command to view the topology table entries.

Examples

The following example removes entries in the 192.168.1.0 network from EIGRP topology table:

```
hostname# clear eigrp topology 192.168.1.0 255.255.255.0
```

Related Commands

Command	Description
show eigrp topology	Displays the EIGRP topology table.

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:

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

Command History

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#
```

Related Commands

Command	Description
debug fover	Displays failover debug information.
show failover	Displays information about the failover configuration and operational statistics.

clear flow-export counters

To reset runtime counters that are associated with NetFlow data to zero, use the **clear flow-export counters** command in privileged EXEC mode.

clear flow-export 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:

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

Command History

Release	Modification
8.1(1)	This command was introduced.

Usage Guidelines

The runtime counters include statistical data as well as error data.

Examples

The following example shows how to reset runtime counters that are associated with NetFlow data:

```
hostname# clear flow-export counters
```

Related Commands

Commands	Description
flow-export destination *interface-name ipv4-address | hostname udp-port*	Specifies the IP address or hostname of the NetFlow collector, and the UDP port on which the NetFlow collector is listening.
flow-export template timeout-rate *minutes*	Controls the interval at which the template information is sent to the NetFlow collector.
logging flow-export-syslogs enable	Enables syslog messages after you have entered the **logging flow-export-syslogs disable** command, and the syslog messages that are associated with NetFlow data.
show flow-export counters	Displays all runtime counters in NetFlow.

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

interface	(Optional) Specifies the adaptive 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:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	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:

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

Command History

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
```

Related Commands

Command	Description
show gc	Displays the garbage collection process statistics.

clear igmp counters

To clear all IGMP counters, use the **clear igmp counters** command in privileged EXEC mode.

clear igmp counters [*if_name*]

Syntax Description

if_name	The interface name, as specified by the **nameif** command. Including an interface name with this command causes only the counters for the specified interface to be cleared.

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

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

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	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

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:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	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 group
```

Related Commands

Command	Description
clear igmp counters	Clears all IGMP counters.
clear igmp traffic	Clears the IGMP traffic counters.

clear igmp traffic

To clear the IGMP traffic counters, use the **clear igmp traffic** command in privileged EXEC mode.

clear igmp traffic

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

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

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	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

interface_name	(Optional) Identifies the interface name set with the **nameif** command.
mapped_name	(Optional) In multiple context mode, identifies the mapped name if it was assigned using the **allocate-interface** command.
physical_interface	(Optional) Identifies the interface ID, such as **gigabitethernet0/1**. See the **interface** command for accepted values.
subinterface	(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:

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

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

If an interface is shared among contexts, and you enter this command within a context, the adaptive security appliance clears only statistics for the current context. If you enter this command in the system execution space, the adaptive 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 *interface_name*	(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:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	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 *interface_name*	Sets the interface on which you want to clear Unicast RPF statistics.

Defaults

No default behavior or values.

Command Modes

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

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
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 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 *map-name*	(Optional) Clears IPSec SAs for the specified crypto map.
peer	(Optional) Clears IPSec SAs for a specified peer.
peer-addr	Specifies the IP address of an IPSec peer.
protocol	Specifies an IPSec protocol: **esp** or **ah**.
spi	Specifies an IPSec SPI.

Defaults

No default behavior or values.

Command Modes

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

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
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# 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:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	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 mld traffic

To clear the IPv6 Multicast Listener Discovery (MLD) traffic counters, use the **clear ipv6 mld traffic** command in privileged EXEC mode.

clear ipv6 mld traffic

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.2(4)	This command was introduced.

Usage Guidelines

The **clear ipv6 mld traffic** command allows you to reset all the Multicast Listener Discovery traffic counters.

Examples

The following example shows how to clear the traffic counters for the IPv6 Multicast Listener Discovery:

```
hostname# clear ipv6 mld traffic
hostname#
```

Related Commands

Command	Description
debug ipv6 mld	Displays all debug messages for Multicast Listener Discovery.
show debug ipv6 mld	Displays the **ipv6** Multicast Listener Discovery 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:

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

Command History

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#
```

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:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	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
        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
  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:

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

Command History

Release	Modification
7.0(1)	This command was introduced.
7.2(1)	The **clear isakmp sa** command was changed to **clear crypto isakmp sa**.

Examples

The following example removes the IKE runtime SA database from the configuration:

```
hostname# clear isakmp sa
hostname#
```

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 adaptive 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 reinitalize per-client run-time states such as connection limits and embryonic limits, use the **clear local-host** command in privileged EXEC mode. As a result, this command removes any connection that uses those limits.

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

Syntax Description

all	(Optional) Clears all connections, including to-the-box traffic. Without the **all** keyword, only through-the-box traffic is cleared.
ip_address	(Optional) Specifies the local host IP address.

Defaults

Clears all through-the-box run-time states.

Command Modes

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

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

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

When you make security policy changes to the configuration, all *new* connections use the new security policy. 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 using the **clear local-host** command. You can alternatively use the **clear conn** command for more granular connection clearing, or the **clear xlate** command for connections that use dynamic NAT.

The **clear local-host** command releases the hosts from the host license limit. You can see the number of hosts that are counted toward the license limit by entering the **show local-host** command.

Examples

The following example clears the run-time state and assocaited connections for the host at 10.1.1.15:

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

Related Commands

Command	Description
clear conn	Terminates connections in any state.
clear xlate	Clears a dynamic NAT session, and any connections using NAT.
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:

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

Command History

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

Usage Guidelines

ASDM system log messages are stored in a separate buffer from the adaptive security appliance system log messages. Clearing the ASDM logging buffer only clears the ASDM system log messages; it does not clear the adaptive 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)#
```

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 privileged EXEC mode.

clear logging buffer

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

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

```
hostname# clear logging buffer
```

Related Commands

Command	Description
logging buffered	Configures the logging buffer.
show logging	Displays logging information.

clear logging queue bufferwrap

To clear the saved logging buffers (ASDM logging buffer, internal logging buffer, FTP logging buffer, and flash logging buffer), use the **clear logging queue bufferwrap** command in privileged EXEC mode.

clear logging queue bufferwrap

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
8.2(1)	This command was introduced.

Examples

The following example shows how to clear the contents of the saved logging buffers:

```
hostname# clear logging queue bufferwrap
```

Related Commands

Command	Description
logging buffered	Configures the logging buffer.
show logging	Displays logging information.

clear mac-address-table

To clear dynamic MAC address table entries, use the **clear mac-address-table** command in privileged EXEC mode.

clear mac-address-table [*interface_name*]

Syntax Description

interface_name	(Optional) Clears the MAC address table entries for the selected interface.

Defaults

No default behavior or values.

Command Modes

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

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	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:

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

The **clear memory delayed-free-poisoner** command returns all memory held in the delayed free-memory poisoner tool queue to the system without validation and clears the related statistical counters.

Examples

The following example clears the delayed free-memory poisoner tool queue and statistics:

```
hostname# clear memory delayed-free-poisoner
```

Related Commands

Command	Description
memory delayed-free-poisoner enable	Enables the delayed free-memory poisoner tool.
memory delayed-free-poisoner validate	Forces validation of the delayed free-memory poisoner tool queue.
show memory delayed-free-poisoner	Displays a summary of the delayed free-memory poisoner tool queue usage.

clear memory profile

To clear the memory buffers held by the memory profiling function, use the **clear memory profile** command in privileged EXEC 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:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	**Routed**	**Transparent**	**Single**	**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 adaptive 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

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:

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

The following example clears all MFIB router packet counters:

```
hostname# clear mfib 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:

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

The following example clears the recovery settings for the AIP SSM:

```
hostname# clear module 1 recover
```

Related Commands

Command	Description
hw-module module recover	Recovers an AIP SSM by loading a recovery image from a TFTP server.
hw-module module reset	Shuts down an SSM and performs a hardware reset.
hw-module module reload	Reloads the AIP SSM software.
hw-module module shutdown	Shuts down the SSM software in preparation for being powered off without losing configuration data.
show module	Shows SSM information.

clear nac-policy

To reset NAC policy usage statistics, use the **clear nac-policy** command in global configuration mode.

clear nac-policy [*nac-policy-name*]

Syntax Description

nac-policy-name	(Optional) Name of the NAC policy for which to reset usage statistics.

Defaults

If you do not specify a name, the CLI resets the usage statistics for all NAC policies.

Command Modes

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

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

Command History

Release	Modification
8.0(2)	This command was introduced.

Examples

The following command resets the usage statistics for the NAC policy named framework1:

```
hostname(config)# clear nac-policy framework1
```

The following command resets all NAC policy usage statistics:

```
hostname(config)# clear nac-policy
```

Related Commands

Command	Description
show nac-policy	Displays NAC policy usage statistics on the adaptive security appliance.
show vpn-session_summary.db	Displays the number IPSec, WebVPN, and NAC sessions.
show vpn-session.db	Displays information about VPN sessions, including NAC results.

clear nat counters

To clear NAT policy counters, use the **clear nat counters** command in global configuration mode.

clear nat counters [*src_if* [*src_ip* [*src_mask*]] [*dst_ifc* [*dst_ip* [*dst_mask*]]]]

Syntax Description

dst_ifc	(Optional) Specifies destination interface to filter.
dst_ip	(Optional) Specifies destination IP address to filter.
dst_mask	(Optional) Specifies mask for destination IP address.
src_ifc	(Optional) Specifies source interface to filter.
src_ip	(Optional) Specifies source IP address to filter.
src_mask	(Optional) Specifies mask for source IP address.

Defaults

This command has no default settings.

Command Modes

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

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

Command History

Release	Modification
7.0 (4)	This command was introduced.

Examples

This example shows how to clear the NAT policy counters:

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

Related Commands

Command	Description
nat	Identifies addresses on one interface that are translated to mapped addresses on another interface.
nat-control	Enables/disables NAT configuration requirement.
show nat counters	Displays the protocol stack counters.

clear ospf

To clear OSPF process information, use the **clear ospf** command in privileged EXEC mode.

clear ospf [*pid*] {**process** | **counters** [**neighbor** [*neighbor-intf*] [*neighbr-id*]]}

Syntax Description

counters	Clears the OSPF counters.
neighbor	Clears the OSPF neighbor counters.
neighbor-intf	(Optional) Clears the OSPF interface router designation.
neighbr-id	(Optional) Clears the OSPF neighbor router ID.
pid	(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:

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

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

This command does not remove any part of the configuration. Use the **no** form of the configuration commands to clear specific commands from the configuration or use the **clear configure router ospf** command to remove all global OSPF commands from the configuration.

Note The **clear configure router ospf** command does not clear OSPF commands entered in interface configuration mode.

Examples

The following example shows how to clear the OSPF process counters:

```
hostname# clear ospf process
```

Related Commands

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

clear pc

To clear connection, xlate, or local-host information maintained on the PC, use the **clear pc** command in privileged EXEC 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:

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

The following example clears PC information:

```
hostname# 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 privileged EXEC 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:

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

The following example clears PC information:

```
hostname# clear pclu
```

Related Commands

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

clear phone-proxy secure-phones

To clear the secure-phone entries in the phone proxy database, use the **clear phone-proxy secure-phones** command in privileged EXEC mode.

clear phone-proxy secure-phones [*mac_address* **| noconfirm]**

Syntax Description

mac_address	Removes the IP phone from the phone proxy database with the specified MAC address.
noconfirm	Removes all the secure-phone entries in the phone proxy database without prompting for confirmation. If you do not specify the **noconfirm** keyword, you are prompted to confirm whether to remove all the secure-phone entries.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
8.2(1)	This command was introduced.

Usage Guidelines

Since secure phones always request a CTL file upon bootup, the phone proxy creates a database that marks the phone as secure. The entries in the secure phone database are removed after a specified configured timeout (via the **timeout secure-phones** command). Alternatively, you can use the **clear phone-proxy secure-phones** command to clear the phone proxy database without waiting for the configured timeout.

Examples

The following example clears PC information:

```
hostname# clear phone-proxy secure-phones 001c.587a.4000
```

Related Commands

Command	Description
timeout secure-phones	Configures the idle timeout after which the secure-phone entry is removed from the phone proxy database.

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:

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

Command History

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
```

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:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	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

interface-name	(Optional) Specifies the name of the interface for which you want to show the best-effort and low-latency queue details.

Defaults

If you omit the interface name, this command clears the priority-queue statistics for all configured interfaces.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

This example shows the use of the **clear priority-queue statistics** command in privileged EXEC mode to remove the priority queue statistics for the interface named “test”.

```
hostname# clear priority-queue statistics test
hostname#
```

Related Commands

Command	Description
clear configure priority queue	Removes the priority-queue configuration from the named interface.
priority-queue	Configures priority queueing on an interface.
show priority-queue statistics	Shows the priority queue statistics for a specified interface or for all interfaces.
show running-config priority-queue	Shows the current priority-queue configuration on the named interface.

clear resource usage

To clear resource usage statistics, use the **clear resource usage** command in privileged EXEC mode.

clear resource usage [**context** *context_name* | **all** | **summary** | **system**] [**resource** {[**rate**] *resource_name* | **all**}]

Syntax Description

context *context_name*	(Multiple mode only) Specifies the context name for which you want to clear statistics. Specify **all** (the default) for all contexts.
resource [**rate**] *resource_name*	Clears the usage of a specific resource. Specify **all** (the default) for all resources. Specify **rate** to clear the rate of usage of a resource. Resources that are measured by rate include **conns**, **inspects**, and **syslogs**. You must specify the **rate** keyword with these resource types. The conns resource is also measured as concurrent connections; only use the **rate** keyword to view the connections per second. Resources include the following types: • **asdm**—ASDM management sessions. • **conns**—TCP or UDP connections between any two hosts, including connections between one host and multiple other hosts. • **inspects**—Application inspections. • **hosts**—Hosts that can connect through the adaptive security appliance. • **mac-addresses**—For transparent firewall mode, the number of MAC addresses allowed in the MAC address table. • **ssh**—SSH sessions. • **syslogs**—System log messages. • **telnet**—Telnet sessions. • **xlates**—NAT translations.
summary	(Multiple mode only) Clears the combined context statistics.
system	(Multiple mode only) Clears the system-wide (global) usage 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	Multiple System
Privileged EXEC	•	•	•	—	•

Command History

Release	Modification
7.2(1)	This command was introduced.

Examples

The following example clears all resource usage statistics for all contexts, but not the system-wide usage statistics:

```
hostname# clear resource usage
```

The following example clears the system-wide usage statistics:

```
hostname# clear resource usage system
```

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 adaptive 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:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	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 privileged EXEC mode. To clear service policy startistics for inspection engines, see the **clear service-policy inspect** commands.

clear service-policy [**global** | **interface** *intf*]

Syntax Description

global	(Optional) Clears the statistics of the global service policy.
interface *intf*	(Optional) Clears the service policy statistics of a specific interface.

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

The following example shows the syntax of the **clear service-policy** command:

```
hostname# clear service-policy outside_security_map interface outside
```

Related Commands

Command	Description
clear service-policy inspect gtp	Clears service policy statistics for the GTP inspection engine.
clear service-policy inspect radius-accounting	Clears service policy statistics for the RADIUS accounting inspection engine.
show service-policy	Displays the service policy.
show running-config service-policy	Displays the service policies configured in the running configuration.
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.
ap_name	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.
IMSI_value	Hexadecimal value that identifies the specific IMSI.
interface	(Optional) Identifies a specific interface.
int	Identifies the interface for which information will be cleared.
IP_address	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.
tunnel_ID	Hexadecimal value that identifies the specific tunnel.
version	(Optional) Clears the PDP contexts based on the GTP version.
version_num	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:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	**Routed**	**Transparent**	**Single**	**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 service-policy inspect radius-accounting

To clear RADIUS accounting users, use the **clear service-policy inspect radius-accounting** command in privileged EXEC mode.

clear service-policy inspect radius-accounting users {**all** | *ip_address* | *policy_map*}

Syntax Description.

all	Clears all users.
ip_address	Clears a user with this IP address.
policy_map	Clears users associated with this policy map.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.2(1)	This command was introduced.

Examples

The following example clears all RADIUS users:

```
hostname# clear service-policy inspect radius-accounting users all
```

clear shared license

To reset shared license statistics, shared license client statistics, and shared license backup server statistics to zero, use the **clear shared license** command in privileged EXEC mode.

clear shared license [**all** | **backup** | **client** [*hostname*]]

Syntax Description

all	(Optional) Clears all statistics. This is the default setting.
backup	(Optional) Clears statistics for the backup server.
client	(Optional) Clears statistics for all participants.
hostname	(Optional) Clears statistics for a particular participant.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
8.2(1)	This command was introduced.

Usage Guidelines

The shared license counters include statistical data as well as error data.

Examples

The following example shows how to reset all shared license counters:

```
hostname# clear shared license all
```

Related Commands

Command	Description
activation-key	Enters a license activation key.
clear configure license-server	Clears the shared licensing server configuration.
license-server address	Identifies the shared licensing server IP address and shared secret for a participant.
license-server backup address	Identifies the shared licensing backup server for a participant.
license-server backup backup-id	Identifies the backup server IP address and serial number for the main shared licensing server.

Command	Description
license-server backup enable	Enables a unit to be the shared licensing backup server.
license-server enable	Enables a unit to be the shared licensing server.
license-server port	Sets the port on which the server listens for SSL connections from participants.
license-server refresh-interval	Sets the refresh interval provided to participants to set how often they should communicate with the server.
license-server secret	Sets the shared secret on the shared licensing server.
show activation-key	Shows the current licenses installed.
show running-config license-server	Shows the shared licensing server configuration.
show shared license	Shows shared license statistics.
show vpn-sessiondb	Shows license information about VPN sessions.

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:

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

Command History

Release	Modification
7.0(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 snmp-server statistics

To clear SNMP server statistics (SNMP packet input and output counters), use the **clear snmp-server statistics** command in privileged EXEC mode.

clear snmp-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:

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

The following example shows how to clear SNMP server statistics:

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

Related Commands

Command	Description
clear configure snmp-server	Clears the SNMP server configuration.
show snmp-server statistics	Displays SNMP server configuration 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:

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

To view configuration errors generated when the adaptive 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 adaptive 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 privileged EXEC 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:

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

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 adaptive security appliance.

Examples

The following example shows how to clear the SunRPC services table:

```
hostname# clear sunrpc-server
```

Related Commands

Command	Description
clear configure sunrpc-server	Clears the Sun remote processor call services from the adaptive 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 threat-detection rate

When you enable basic threat detection using the **threat-detection basic-threat** command, you can clear statistics using the **clear threat detection rate** command in privileged EXEC mode.

clear threat-detection rate

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
8.0(2)	This command was introduced.

Examples

The following example clears the rate statistics:

```
hostname# clear threat-detection rate
```

Related Commands

Command	Description
show running-config all threat-detection	Shows the threat detection configuration, including the default rate settings if you did not configure them individually.
show threat-detection rate	Shows basic threat detection statistics.
threat-detection basic-threat	Enables basic threat detection.
threat-detection rate	Sets the threat detection rate limits per event type.
threat-detection scanning-threat	Enables scanning threat detection.

clear threat-detection scanning-threat

If you enable scanning threat detection with the **threat-detection scanning-threat** command, then clear the attackers and targets using the **clear threat-detection scanning-threat** command in privileged EXEC mode.

clear threat-detection scanning-threat [attacker [*ip_address* [*mask*]] |
target [*ip_address* [*mask*]]

Syntax Description

ip_address	(Optional) Clears a specific IP address .
mask	(Optional) Sets the subnet mask.
attacker	(Optional) Clears only attackers.
target	(Optional) Clears only targets.

Defaults

If you do not specify an IP address, all hosts are released.

Command Modes

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

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

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

To view current attackers and targets, use the **show threat-detection scanning-threat** command.

Examples

The following example shows targets and attackers with the **show threat-detection scanning-threat** command, and then clears all targets:

```
hostname# show threat-detection scanning-threat
Latest Target Host & Subnet List:
    192.168.1.0
    192.168.1.249
   Latest Attacker Host & Subnet List:
    192.168.10.234
    192.168.10.0
    192.168.10.2
    192.168.10.3
    192.168.10.4
    192.168.10.5
    192.168.10.6
```

```
    192.168.10.7
    192.168.10.8
    192.168.10.9
hostname# clear threat-detection scanning-threat target
```

Related Commands

Command	Description
show threat-detection shun	Shows currently shunned hosts.
show threat-detection statistics host	Shows the host statistics.
show threat-detection statistics protocol	Shows the protocol statistics.
show threat-detection statistics top	Shows the top 10 statistics.
threat-detection scanning-threat	Enables scanning threat detection.

clear threat-detection shun

If you enable scanning threat detection with the **threat-detection scanning-threat** command, and you automatically shun attacking hosts, then release the currently shunned hosts using the **clear threat-detection shun** command in privileged EXEC mode.

clear threat-detection shun [*ip_address* [*mask*]]

Syntax Description

ip_address	(Optional) Releases a specific IP address from being shunned.
mask	(Optional) Sets the subnet mask for the shunned host IP address.

Defaults

If you do not specify an IP address, all hosts are released.

Command Modes

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

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

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

To view currently shunned hosts, use the **show threat-detection shun** command.

Examples

The following example views currently shunned hosts with the **show threat-detection shun** command, and then releases host 10.1.1.6 from being shunned:

```
hostname# show threat-detection shun
Shunned Host List:
10.1.1.6
198.1.6.7
hostname# clear threat-detection shun 10.1.1.6 255.255.255.255
```

Related Commands

Command	Description
show threat-detection shun	Shows currently shunned hosts.
show threat-detection statistics host	Shows the host statistics.
show threat-detection statistics protocol	Shows the protocol statistics.

Command	Description
show threat-detection statistics top	Shows the top 10 statistics.
threat-detection scanning-threat	Enables scanning threat detection.

clear threat-detection statistics

If you enable TCP Intercept statistics with the **threat-detection statistics tcp-intercept** command, then clear the statistics using the **clear threat-detection scanning-threat** command in privileged EXEC mode.

clear threat-detection statistics [tcp-intercept]

Syntax Description

tcp-intercept	(Optional) Clears TCP Intercept statistics. This is the default.

Defaults

Clears TCP Intercept statistics.

Command Modes

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

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

Command History

Release	Modification
8.0(4)	This command was introduced.

Usage Guidelines

To view TCP Intercept statistics, enter the **show threat-detection statistics top** command.

Examples

The following example shows TCP Intercept statistics with the **show threat-detection statistics top tcp-intercept** command, and then clears all statistics:

```
hostname# show threat-detection statistics top tcp-intercept

Top 10 Protected Servers under Attack (sorted by average rate)
Monitoring Window Size: 30 mins    Sampling Interval: 30 secs
<Rank> <Server IP:Port> <Interface> <Ave Rate> <Cur Rate> <Total> <Source IP (Last Attack
Time)>
------------------------------------------------------------------------------
1    192.168.1.2:5000 inside 1249 9503 2249245 <various> Last: 10.0.0.3 (0 secs ago)
2    192.168.1.3:5000 inside 10 10 6080 10.0.0.200 (0 secs ago)
3    192.168.1.4:5000 inside 2 6 560 10.0.0.200 (59 secs ago)
4    192.168.1.5:5000 inside 1 5 560 10.0.0.200 (59 secs ago)
5    192.168.1.6:5000 inside 1 4 560 10.0.0.200 (59 secs ago)
6    192.168.1.7:5000 inside 0 3 560 10.0.0.200 (59 secs ago)
7    192.168.1.8:5000 inside 0 2 560 10.0.0.200 (59 secs ago)
8    192.168.1.9:5000 inside 0 1 560 10.0.0.200 (59 secs ago)
9    192.168.1.10:5000 inside 0 0 550 10.0.0.200 (2 mins ago)
10   192.168.1.11:5000 inside 0 0 550 10.0.0.200 (5 mins ago)
```

```
hostname# clear threat-detection statistics
```

Related Commands

Command	Description
show threat-detection statistics top	Shows the top 10 statistics.
threat-detection statistics	Enables threat detection statistics.

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:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	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 adaptive security appliance came online. And the number of seconds indicate the duration the adaptive 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:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	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 adaptive 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 to reauthenticate:

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

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:

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

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

The **clear url-block block statistics** command clears the block buffer usage counters, except for the `Current number of packets held (global)` counter.

Examples

The following example clears the URL block statistics and displays the status of the counters after clearing:

```
hostname# clear url-block block statistics
hostname# show url-block block statistics

URL Pending Packet Buffer Stats with max block  0
-----------------------------------------------------
Cumulative number of packets held: | 0
Maximum number of packets held (per URL): | 0
Current number of packets held (global): | 38
Packets dropped due to
| exceeding url-block buffer limit: | 0
| HTTP server retransmission: | 0
Number of packets released back to client: | 0
```

Related Commands

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

clear url-cache statistics

To remove **url-cache** command statements from the configuration, use the **clear url-cache** command in privileged EXEC mode.

clear url-cache statistics

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

The **clear url-cache** command removes **url-cache** statistics from the configuration.

Using the URL cache does not update the Websense accounting logs for Websense protocol Version 1. If you are using Websense protocol Version 1, let Websense run to accumulate logs so you can view the Websense accounting information. After you get a usage profile that meets your security needs, enter the **| url-cache** command to increase throughput. Accounting logs are updated for Websense protocol Version 4 and for N2H2 URL filtering while using the **url-cache** command.

Examples

The following example clears the URL cache statistics:

```
hostname# clear url-cache statistics
```

Related Commands

Commands	Description
filter url	Directs traffic to a URL filtering server.
show url-cache statistics	Displays information about the URL cache, which is used for buffering URLs while waiting for responses from an N2H2 or Websense filtering server.
url-block	Manages the URL buffers used for web server responses while waiting for a filtering decision from the filtering server.

url-cache	Enables URL caching while pending responses from an N2H2 or Websense server and sets the size of the cache.
url-server	Identifies an N2H2 or Websense server for use with the **filter** command.

clear url-server

To clear URL filtering server statistics, use the **clear url-server** command in privileged EXEC mode.

clear url-server statistics

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

The **clear url-server** command removes URL filtering server statistics from the configuration.

Examples

The following example clears the URL server statistics:

```
hostname# clear url-server statistics
```

Related Commands

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

clear wccp

To reset WCCP information, use the **clear wccp** command in privileged EXEC mode.

clear wccp [**web-cache** | *service_number*]

Syntax Description

web-cache	Specifies the web-cache service.
service-number	A dynamic service identifier, which means the service definition is dictated by the cache. The dynamic service number can be from 0 to 254 and up to 255. There is a maximum allowable number of 256 that includes the web-cache service specified with the **web-cache** keyword.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.2(1)	This command was introduced.

Examples

The following example shows how to reset the WCCP information for the web-cache service:

```
hostname# clear wccp web-cache
```

Related Commands

Command	Description
show wccp	Displays the WCCP configuration.
wccp redirect	Enables support of WCCP redirection.

clear webvpn sso-server statistics

To reset the statistics from the webvpn Single Sign-On (SSO) server, use the **clear webvpn sso-server statistics** command in privileged EXEC mode.

clear webvpn sso-server statistics *servername*

Syntax Description

servername	Specifies the name of the SSO server to be revoked.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

This does not reset the "pending requests" statistic.

Examples

The following example entered in privileged EXEC mode, displays crypto accelerator statistics:

```
hostname # clear webvpn sso-server statistics
hostname #
```

Related Commands

Command	Description
clear crypto accelerator statistics	Clears the global and accelerator-specific statistics in the crypto accelerator MIB.
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 xlate

To clear current dynamic 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 *ip1*[**-***ip2*]	(Optional) Clears the active translations by global IP address or range of addresses.
gport *port1*[*-port2*]	(Optional) Clears the active translations by the global port or range of ports.
interface *if_name*	(Optional) Displays the active translations by interface.
local *ip1*[**-***ip2*]	(Optional) Clears the active translations by local IP address or range of addresses.
lport *port1*[*-port2*]	(Optional) Clears the active translations by local port or range of ports.
netmask *mask*	(Optional) Specifies the network mask to qualify the global or local IP addresses.
state *state*	(Optional) Clears the active translations by state. You can enter one or more of the following states: • **static**—specifies **static** translations. • **portmap**—specifies PAT global translations. • **norandomseq**—specifies a **nat** or **static** translation with the **norondomseq** 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		
				Multiple	
Command Mode	Routed	Transparent	Single	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 **global** or **nat** commands in your configuration.

An xlate describes a NAT or PAT session. These sessions can be viewed with the **show xlate** command with the **detail** option. There are two types of xlates: static and dynamic.

A static xlate is a persistent xlate that is created using the **static** command. The **clear xlate** command does not clear for a host in a static entry. Static xlates can only be removed by removing the **static** command from the configuration; the **clear xlate** command 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** or **clear conn** command 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** or **clear conn** 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** 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.