CHAPTER 8

# clear conn through clear isakmp sa Commands

# clear conn

To clear a specific connection or multiple connections, use the **clear conn** command in privileged EXEC mode.

**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*] [**user** [*domain_nickname*\]*user_name* | **user-group** [*domain_nickname*\\]*user_group_name*]]

## 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:<br>`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:<br>`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:<br>`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:<br>`1000-2000` |
| **user** [*domain_nickname*\]*user_name* | (Optional) Clears connections that belong to the specified user. When you do not include the *domain_nickname* argument, the ASA clears connections for the user in the default domain. |
| **user-group** [*domain_nickname*\\]*user_group_name* | (Optional) Clears connections that belong to the specified user group. When you do not include the *domain_nickname* argument, the ASA clears connections for the user group in the default domain. |

## 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. |
| 8.4(2) | Added the **user** and **user-group** keywords to support the Identity Firewall. |

## Usage Guidelines

This command supports IPv4 and IPv6 addresses.

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 ASA creates a pinhole to allow secondary connections, this is shown as an incomplete connection in the **show conn** command output. To clear this incomplete connection, use the **clear conn** command.

## Examples

The following example shows how to remove all connections and then clear 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 |
|---|---|
| 7.0(1) | This command was introduced. |

## 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 ASA. |
| **show console-output** | Displays the captured console output. |
| **show running-config console timeout** | Displays the idle timeout for a console connection to the ASA. |

# clear coredump

To clear the coredump log, use the **clear coredump** command in global configuration mode.

**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 file system contents and the coredump log. The coredump file system remains intact. The current coredump configuration remains unchanged.

## Examples

The following example removes the coredump file system 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 file system and its contents from your system. |
| **show coredump filesystem** | Displays files on the coredump filesystem. |
| **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** command 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(1) | This command was introduced. |

## Examples

The following 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 |
|---|---|
| 7.0(1) | This command was introduced. |

## Examples

The following example shows how to delete the crash file:

```
hostname# clear crashinfo
```

## Related Commands

| | |
|---|---|
| **crashinfo force** | Forces a crash of the ASA. |
| **crashinfo save disable** | Disables crash information from writing to flash memory. |
| **crashinfo test** | Tests the ability of the ASA 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 arguments or keywords.

## 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. |
| 9.0(1) | Support for multiple context mode was added. |

## 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 empty the CRL cache of all CRLs associated with a specified trustpoint, all CRLs associated with the trustpool from the cache, or the CRL cache of all CRLs, use the **clear crypto ca crls** command in privileged EXEC mode.

**clear crypto ca crls** [**trustpool** | trustpoint *trustpointname*]

## Syntax Description

| | |
|---|---|
| *trustpointname* | The name of a trustpoint. If you do not specify a name, this command clears all CRLs cached on the system. If you give the trustpoint keyword without a trustpointname, the command fails. |
| **trustpool** | Indicates that the action should be applied only to the CRLs that are associated with certificates in the trustpool. |

## 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 |
|---|---|
| 9.0(1) | This command was introduced. |

## Examples

The following independent examples issued in privileged EXEC configuration mode clear all of the trustpool CRLs, clears all of the CRLs associated with trustpoint123, and removes all of the cached CRLs from the ASA:

```
hostname# clear crypto ca crl trustpool
hostname# clear crypto ca crl trustpoint trustpoint123
hostname# clear crypto ca crl
```

## Related Commands

| Command | Description |
|---|---|
| **crypto ca crl request** | Downloads the CRL based on the CRL configuration of the trustpoint. |
| **show crypto ca crl** | Displays all cached CRLs or CRLs cached for a specified trustpoint. |

# clear crypto ca trustpool

To remove all certificates from the trustpool, use the **clear crypto ca trustpool** command in global configuration mode.

**clear crypto ca trustpool** [**noconfirm**]

## Syntax Description

| | |
|---|---|
| **noconfirm** | Suppresses user confirmation prompts, and the command will be processes as requested. |

## 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 |
|---|---|
| 9.0(1) | This command was introduced. |

## Usage Guidelines

The user is asked to confirm this action before carrying it out.

## Examples

```
hostname# clear crypto ca trustpool
You are about to clear the trusted certificate pool. Do you want to continue? (y/n)
hostname#
```

## Related Commands

| Command | Description |
|---|---|
| **crypto ca trustpool export** | Exports the certificates that constitute the PKI trustpool. |
| **crypto ca trustpool import** | Imports the certificates that constitute the PKI trustpool. |
| **crypto ca trustpool remove** | Removes a single specified certificate from the trustpool. |

# clear crypto ikev1

To remove the IPsec IKEv1 SAs or statistics, use the **clear crypto ikev1** command in privileged EXEC mode. To clear all IKEv1 SAs, use this command without arguments.

**clear crypto ikev1** {**sa** *IP_address_hostname* | **stats**}

## Syntax Description

| | |
|---|---|
| **sa** | Clears the SA. |
| *IP_address_hostname* | An IP address or hostname. |
| **stats** | Clears the IKEv1 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 |
|---|---|
| 8.4(1) | This command was introduced. |
| 9.0(1) | Support for multiple context mode was added. |

## Usage Guidelines

To clear all IPsec IKEv1 SAs, use this command without arguments.

## Examples

The following example, issued in global configuration mode, removes all of the IPsec IKEv1 statistics from the ASA:

```
hostname# clear crypto ikev1 stats
hostname#
```

The following example, entered in global configuration mode, deletes SAs with a peer IP address of 10.86.1.1:

```
hostname# clear crypto ikev1 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 ikev2

To remove the IPsec IKEv2 SAs or statistics, use the **clear crypto ikev2** command in privileged EXEC mode. To clear all IKEv2 SAs, use this command without arguments.

**clear crypto ikev2** {**sa** *IP_address_hostname* | **stats**}

## Syntax Description

| | |
|---|---|
| **sa** | Clears the SA. |
| *IP_address_hostname* | An IP address or hostname. |
| **stats** | Clears the IKEv2 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 |
|---|---|
| 8.4(1) | This command was introduced. |
| 9.0(1) | Support for multiple context mode was added. |

## Usage Guidelines

To clear all IPsec IKEv2 SAs, use this command without arguments.

## Examples

The following example, issued in global configuration mode, removes all of the IPsec IKEv2 statistics from the ASA:

```
hostname# clear crypto ikev2 stats
hostname#
```

The following example, entered in global configuration mode, deletes SAs with a peer IP address of 10.86.1.1:

```
hostname# clear crypto ikev2 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 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*}**]**

## 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* | Identifies 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. The maximum is 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. |
| 9.0(1) | Support for multiple context mode was added. |

## Usage Guidelines

To clear all IPsec SAs, use this command without arguments.

## Examples

The following example, issued in global configuration mode, removes all of the IPsec SAs from the ASA:

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

The following example, entered 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:<br>• **all**—All protocols currently supported.<br>• **ikev1**—Internet Key Exchange (IKE) version 1.<br>• **ikev2**—Internet Key Exchange (IKE) version 2.<br>• **ipsec-client**—IP Security (IPsec) Phase-2 protocols.<br>• **other**—Reserved for new protocols.<br>• **srtp**—Secure RTP (SRTP) protocol<br>• **ssh**—Secure Shell (SSH) protocol<br>• **ssl-client—**Secure Socket Layer (SSL) protocol. |

## 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. |
| 8.4(1) | The **ikev1** and **ikev2** keywords were added. |
| 9.0(1) | Support for multiple context mode was added. |

## 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. |
| **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 cts

To clear data used by the ASA when integrated with Cisco TrustSec, use the **clear cts** command in global configuration mode:

**clear cts** {**environment-data** | **pac**}

## Syntax Description

| | |
|---|---|
| **environment-data** | Clears all CTS environment data. |
| **pac** | Clears the stored CTS PAC. |

## Defaults

No default behavior or values.

## Command Modes

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

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

## Command History

| Release | Modification |
|---|---|
| 9.0(1) | This command was introduced. |

## Usage Guidelines

Using the **environment-data** keyword with the **clear cts** command clears the Cisco TrustSec environment data downloaded from the Cisco ISE. You can trigger the next environment data refresh manually or the ASA will refresh the data when the refresh timer expires. Running the **clear cts environment-data** does not remove the Cisco TrustSec PAC from the ASA. Because running the **clear cts nvironment-data** command impacts traffic policy, you are prompted to confirm the action.

Using the **pac** keyword with the **clear cts** command clears the PAC information stored in NVRAM on the ASA. Without a PAC, the ASA cannot download Cisco TrustSec environment data. However, environment data that is already on the ASA remains in use. Because running the **clear cts pac** command renders the ASA unable to retrieve environment data updates, you are prompted to confirm the action.

### Restrictions

- HA: This command is not supported on the standby device in an HA configuration. Running the **clear cts** [**environment-data** | **pac**] on the standby device displays the following error message:

  This command is only permitted on the primary device.

- Clustering: This command is only supported on the master device. Running the **clear cts** [**environment-data** | **pac**] on the slave device displays the following error message:

  This command is only permitted on the master device.

## Examples

The following examples show how to clear data from the ASA used for the ASA integration with Cisco TrustSec:

```
hostname# clear cts pac
Are you sure you want to delete the cts PAC? (y/n)

hostname# clear cts environment-data
Are you sure you want to delete the cts environment data? (y/n)
```

## Related Commands

| Command | Description |
|---|---|
| **clear configure all** | Clears the entire running configuration on the ASA. |
| **clear configure cts** | Clears the configuration for integrating the ASA with Cisco TrustSec. |
| **cts sxp enable** | Enables the SXP protocol on the ASA. |

# 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 |
|---|---|
| 7.0(1) | This command was introduced. |

## 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:

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

## Command History

| Release | Modification |
|---|---|
| 7.0(1) | This command was introduced. |

## 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 debugging 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

To clear all IP addresses associated with the specified fully qualified domain name (FQDN) host, use the **clear dns** command in privileged EXEC mode.

**clear dns** [**host** *fqdn_name*]

## Syntax Description

| | |
|---|---|
| *fqdn_name* | (Optional) Specifies the fully qualified domain name of the selected host. |
| **host** | (Optional) Indicates the IP address of the specified host. |

## 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 |
|---|---|
| 8.4(2) | This command was introduced. |

## Examples

The following example clears the IP address associated with the specified FQDN host:

```
hostname# clear dns 10.1.1.2 www.example.com
```

**Note** The setting of the **dns expire-entry** keyword is ignored for this command. New DNS queries are sent for each activated FQDN host.

## Related Commands

| Command | Description |
|---|---|
| **dns domain-lookup** | Enables the ASA 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 ASA 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 dns-hosts cache

To clear the DNS cache, use the **clear dns-hosts cache** command in privileged EXEC mode.

**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. |

## Usage Guidelines

This command does not clear static entries that you added with the **name** command.

## Examples

The following example clears the DNS cache:

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

## Related Commands

| Command | Description |
|---|---|
| **dns domain-lookup** | Enables the ASA 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 ASA 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 ASA 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 ASA. |
| **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 ASA 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 ASA 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 ASA. |
| **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 ASA 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 ASA 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 ASA. |
| **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 ASA 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 ASA 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. |
| 9.0(1) | Multiple context mode is supported. |

## 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 ASA only supports one EIGRP routing process, you do not need to specify the autonomous system number (AS), which is the 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 ASA 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. |
| 9.0(1) | Multiple context mode is supported. |

## 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 debugging information for EIGRP neighbors. |
| **debug ip eigrp** | Displays debugging 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 ASA only supports one EIGRP routing process, you do not need to specify the autonomous system number (AS), which is the 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. |
| 9.0(1) | Multiple context mode is supported. |

## 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 |
|---|---|
| 7.0(1) | This command was introduced. |

## Usage Guidelines

This command clears the statistics displayed with the **show failover statistics** command and the counters in the Stateful Failover Logical Update Statistics section of the **show failover** command output. To remove the failover configuration, use the **clear configure failover** command.

## Examples

The following example shows how to clear the failover statistic counters:

```
hostname# clear failover statistics
hostname#
```

## Related Commands

| Command | Description |
|---|---|
| **debug fover** | Displays failover debugging 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.

**clear fragment** {**queue** | **statistics**} [*interface*]

## Syntax Description

| | |
|---|---|
| *interface* | (Optional) Specifies the ASA 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. |

## Usage Guidelines

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.

## Examples

The following 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 the NFS. |

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

# clear gc

To remove the garbage collection (GC) 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 GC process statistics:

```
hostname# clear gc
```

## Related Commands

| Command | Description |
|---|---|
| **show gc** | Displays the GC 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. |

## 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 |
|---|---|
| 7.0(1) | This command was introduced. |

## Usage Guidelines

If you do not specify a group or an interface, all groups are cleared from all interfaces. If you specify a group, only the entries for that group are cleared. If you specify an interface, then all groups on that interface are cleared. If you specify both a group and an interface, only the specified groups on the specified interface are cleared.

This command does not clear statically configured groups.

## Examples

The following example shows how to clear all discovered IGMP groups from the IGMP group cache:

```
hostname# clear igmp 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 |
|---|---|
| 7.0(1) | This command was introduced. |

## Usage Guidelines

If an interface is shared among contexts, and you enter this command within a context, the ASA clears only statistics for the current context. If you enter this command in the system execution space, the ASA 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 |
|---|---|
| 7.0(1) | This command was introduced. |

## 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.

**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 |
|---|---|
| 7.0(1) | This command was introduced. |

## Usage Guidelines

See the **ip verify reverse-path** command to enable unicast RPF.

## 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 RPF 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.

**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. |
| **inactive** | (Optional) Clears IPsec SAs that are unable to pass traffic. |
| **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 |
|---|---|
| 7.0(1) | This command was introduced. |
| 9.0(1) | Support for multiple context mode was added. |

## Usage Guidelines

You can also use an alternate form of this command to perform the same function: **clear crypto ipsec sa**.

## 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 dhcprelay binding

To clear the IPv6 DHCP relay binding entries, use the **clear ipv6 dhcprelay binding** command in privileged EXEC mode.

**clear ipv6 dhcprelay binding** [**ip**]

## Syntax Description

| | |
|---|---|
| **ip** | (Optional) Specifies the IPv6 address for the DHCP relay binding. If the IP address is specified, only the relay binding entries associated with that IP address are cleared. |

## 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 |
|---|---|
| 9.0(1) | This command was introduced. |

## Examples

The following example shows how to clear the statistical data for the IPv6 DHCP relay binding:

```
hostname# clear ipv6 dhcprelay binding
hostname#
```

## Related Commands

| Command | Description |
|---|---|
| **show ipv6 dhcprelay binding** | Shows the relay binding entries created by the relay agent. |
| **show ipv6 dhcprelay statistics** | Shows the IPv6 DHCP relay agent information. |

# clear ipv6 dhcprelay statistics

To clear the IPv6 DHCP relay agent statistics, use the **clear ipv6 dhcprelay statistics** command in privileged EXEC mode.

**clear ipv6 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 |
|---|---|
| 9.0(1) | This command was introduced. |

## Examples

The following example shows how to clear the statistical data for the IPv6 DHCP relay agent:

```
hostname# clear ipv6 dhcprelay statistics
hostname#
```

## Related Commands

| Command | Description |
|---|---|
| **show ipv6 dhcprelay binding** | Shows the relay binding entries created by the relay agent. |
| **show ipv6 dhcprelay statistics** | Shows the DHCP relay agent information for IPv6. |

# 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 MLD traffic counters.

## Examples

The following example shows how to clear the traffic counters for IPv6 MLD:

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

## Related Commands

| Command | Description |
|---|---|
| **debug ipv6 mld** | Displays all debugging messages for MLD. |
| **show debug ipv6 mld** | Displays the MLD commands for IPv6 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 neighbor discovery cache. |
| **show ipv6 neighbor** | Displays IPv6 neighbor cache information. |

# clear ipv6 ospf

To clear OSPFv3 routing parameters, use the **clear ipv6 ospf** command in privileged EXEC mode.

**clear ipv6** [*process_id*] [**counters**] [**events**] [**force-spf**] [**process**] [**redistribution**] [**traffic**]

## Syntax Description

| | |
|---|---|
| **counters** | Resets the OSPF process counters. |
| **events** | Clears the OSPF event log. |
| **force-ospf** | Clears the SPF for OSPF processes. |
| **process** | Resets the OSPFv3 process. |
| *process_id* | Clears the process ID number. Valid values range from 1 to 65535. |
| **redistribution** | Clears OSPFv3 route redistribution. |
| **traffic** | Clears traffic-related 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 |
|---|---|
| 9.0(1) | This command was introduced. |

## Usage Guidelines

This command removes all OSPFv3 routing parameters.

## Examples

The following example shows how to clear all OSPFv3 route redistribution:

```
hostname# clear ipv6 ospf redistribution
hostname#
```

## Related Commands

| Command | Description |
|---|---|
| **show running-config ipv6 router** | Shows the running configuration of OSPFv3 processes. |
| **clear configure ipv6 router** | Clears OSPFv3 routing processes. |

# 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 have been 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 | • | — | • | • | — |
| Global configuration | • | — | • | • | — |

## 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**. |
| 9.0(1) | Support for multiple context mode was added. |

## 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 ASA. |
| **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. |