show d – show e

show data-plane quick-reload status

To view the state of the data plane reload, use the **show data-plane quick-reload status** command in privileged EXEC mode.

show data-plane quick-reload status

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:

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

Command History

Release	Modification
9.20(2)	This command was added.

Usage Guidelines

This command displays the quick reload status of the data path for the current context.

Examples

The following is sample output for the **show data-plane quick-reload status** command when the data plane quick reload is enabled:

```
ciscoasa# show data-plane quick-reload status
data-plane reloaded!
```

The following is sample output for the **show data-plane quick-reload status** command when the data plane quick reload is disabled:

```
ciscoasa# show data-plane quick-reload status
device reloaded
```

Related Commands

Command	Description
data-plane quick-reload	Enables data-plane quick-reload.

show ddns update interface

To display the DDNS methods assigned to ASA interfaces, use the **show ddns update interface** command in privileged EXEC mode.

show ddns update interface [*interface-name*]

Syntax Description

interface-name	(Optional) The name of a network interface.

Command Default

Omitting the *interface-name* string displays the DDNS method assigned to each interface.

Command Modes

The 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	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
7.2(1)	This command was added.
9.15(1)	For the Web update method, the output of this command includes the last successful updated FQDN/IP address mapping.

Examples

The following example displays the DDNS method assigned to the inside interface:

```
ciscoasa# show ddns update interface inside
Dynamic DNS Update on inside:
  Update Method Name            Update Destination
  ddns-2                        not available
ciscoasa#
```

The following example shows a successful web type update:

```
ciscoasa# show ddns update interface outside

Dynamic DNS Update on outside:
  Update Method Name            Update Destination
  test                          not available

Last Update attempted on 09:01:52.729 UTC Mon Mar 23 2020
Status : Success
FQDN : asa1.example.com
IP addresses(s): 10.10.32.45,2001:DB8::1
```

The following example shows a web type failure:

```
ciscoasa# show ddns update interface outside

Dynamic DNS Update on outside:
  Update Method Name            Update Destination
  test                          not available

Last Update attempted on 09:01:52.729 UTC Mon Mar 23 2020
Status : Failed
Reason : Could not establish a connection to the server
```

The following example shows that the DNS server returned an error for the web type update:

```
ciscoasa# show ddns update interface outside

Dynamic DNS Update on outside:
  Update Method Name            Update Destination
  test                          not available

Last Update attempted on 09:01:52.729 UTC Mon Mar 23 2020
Status : Failed
Reason : Server error (Error response from server)
```

The following example shows that a web update was not yet attempted due to the IP address unconfigured or the DHCP request failed, for example:

```
ciscoasa# show ddns update interface outside

Dynamic DNS Update on outside:
  Update Method Name            Update Destination
  test                          not available

Last Update Not attempted
```

Related Commands

Command	Description
ddns	Specifies the standard DDNS update method type.
ddns update	Associates a DDNS method with an interface.
ddns update method	Creates a DDNS update method.
interval maximum	Configures the update interface between DNS requests.
show ddns update method	Displays the type and interval for each configured DDNS method. a DHCP server to perform DDNS updates.
show running-config ddns	Displays the type and interval of all configured DDNS methods in the running configuration.
web update-type	Specifies the address types (IPv4 or IPv6) that you want to update.
web update-url	Sets the DDNS update method to Web and sets the update URL.

show ddns update method

To display the DDNS update methods in the running configuration, use the **show ddns update method** command in privileged EXEC mode.

show ddns update method [*method-name*]

Syntax Description

method-name	(Optional) The name of a configured DDNS update method.

Command Default

Omitting the *method-name* string displays all configured DDNS update methods.

Command Modes

The 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	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
7.2(1)	This command was added.
9.15(1)	Output for the Web update method was added.
9.18(1)	Output for the Web update method was enhanced to display the configured reference-identity.

Examples

The following example displays the DDNS method named ddns-2:

```
ciscoasa(config)# show ddns update method ddns-2
 Dynamic DNS Update Method: ddns-2
 IETF standardized Dynamic DNS 'A' and 'PTR' records update
 Maximum update interval: 0 days 0 hours 10 minutes 0 seconds
 ciscoasa(config)#
```

The following example shows details about the web update method:

```
 ciscoasa# show ddns update method web1
Dynamic DNS Update Method: web1
Dynamic DNS updated via HTTP(s) protocols
  URL used to update record:
pwd@10.x.x.x/update?hostname=<>https://admin:pwd@10.x.x.x/update?hostname=<;h>&myip=<a>
  Update type configured: ipv4
  Configured reference-identity name: dyndns
  Maximum update interval: 0 days 0 hours 2 minutes 0 seconds
```

Related Commands

Command	Description
ddns	Specifies a DDNS update method type for a created DDNS method.
ddns update	Associates a ASA interface with a Dynamic DNS (DDNS) update method or a DDNS update hostname.
ddns update method	Creates a method for dynamically updating DNS resource records.
show ddns update interface	Displays the interfaces associated with each configured DDNS method.
show running-config ddns	Displays the type and interval of all configured DDNS methods in the running configuration.

show debug

To show the current debugging configuration, use the **show debug** command.

show debug [*command* [*keywords*]]

Syntax Description

command	(Optional) Specifies the **debug** command whose current configuration you want to view.
keywords	(Optional) For each *command* , the *keywords* following the *command* are identical to the *keywords* supported by the associated **debug** command.

Command Default

This command has no default settings.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was added.
8.0(2)	The **eigrp** keyword was added to the list of possible command values.
8.4(1)	The **route** keyword was added to the list of possible command values.
9.2(1)	The **event manager** keyword was added to the list of possible command values.
9.5(2)	The output has been modified to include any debug persistent settings.
9.5(2)	The ability to show debug logs by filtering, based on the filter condition sets was added.

Usage Guidelines

For each *command* , the *keywords* following the *command* are identical to the *keywords* supported by the associated **debug** command. For information about the supported syntax, see the associated **debug** command.

Note The availability of each *command* depends on the command modes that support the applicable **debug** command.

The valid *command* values are as follows:

- **aaa**

- **appfw**
- **arp**
- **asdm**
- **context**
- **crypto**
- **ctiqbe**
- **ctm**
- **cxsc**
- **debug eigrp parser**
- **dhcpc**
- **dhcpd**
- **dhcprelay**
- **disk**
- **dns**
- **eigrp**
- **email**
- **entity**
- event manager
- **fixup**
- **fover**
- **fsm**
- **ftp**
- **generic**
- **gtp**
- **h323**
- **http**
- **http-map**
- **icmp**
- **igmp**
- **ipv6 eigrp**
- **ipv6 eigrp neighbor**
- **ipv6 eigrp notifications**

- **ipv6 eigrp summary**
- **ils**
- **imagemgr**
- **ipsec-over-tcp**
- **ipv6**
- **iua-proxy**
- **kerberos**
- **ldap**
- **mfib**
- **mgcp**
- **mmp**
- **mrib**
- **ntdomain**
- **ntp**
- **ospf**
- **parser**
- **pim**
- **pix**
- **pptp**
- **radius**
- **rip**
- **route**
- **rtsp**
- **sdi**
- **sequence**
- **sfr**
- **sip**
- **skinny**
- **smtp**
- **sqlnet**
- **ssh**
- **ssl**

- **sunrpc**
- **tacacs**
- **timestamps**
- **vpn-sessiondb**
- **webvpn**
- **xdmcp**
- **xml**

Examples

You can use the **show debug** command to view all debugging configurations, a debugging configuration for a specific feature, and a debugging configuration for a portion of a feature.

The following commands enable debugging for authentication, accounting, and flash memory:

```
ciscoasa# debug aaa authentication

debug aaa authentication enabled at level 1
ciscoasa# debug aaa accounting
debug aaa accounting enabled at level 1
ciscoasa# debug disk filesystem
debug disk filesystem enabled at level 1
ciscoasa# show debug
debug aaa authentication enabled at level 1
debug aaa accounting enabled at level 1
debug disk filesystem enabled at level 1
ciscoasa# show debug aaa
debug aaa authentication enabled at level 1
debug aaa authorization is disabled.
debug aaa accounting enabled at level 1
debug aaa internal is disabled.
debug aaa vpn is disabled.
ciscoasa# show debug aaa accounting
debug aaa accounting enabled at level 1
ciscoasa#
```

Related Commands

Command	Description
debug	Displays all **debug** commands.

show dhcpd

To view DHCP binding, state, and statistical information, use the **show dhcpd** command in privileged EXEC or global configuration mode.

show dhcpd { **binding** [*IP_address*] **| state | statistics** }

Syntax Description

binding	Displays binding information for a given server IP address and its associated client hardware address and lease length.
IP_address	Shows the binding information for the specified IP address.
state	Displays the state of the DHCP server, such as whether it is enabled in the current context and whether it is enabled on each of the interfaces.
statistics	Displays statistical information, such as the number of address pools, bindings, expired bindings, malformed messages, sent messages, and received messages.

Command Default

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	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

If you include the optional IP address in the **show dhcpd binding** command, only the binding for that IP address is shown.

The **show dhcpd binding | state | statistics** commands are also available in global configuration mode.

Examples

The following is sample output from the **show dhcpd binding** command:

```
ciscoasa# show dhcpd binding
IP Address Client-id         Lease  Expiration  Type
10.0.1.100 0100.a0c9.868e.43 84985 seconds automatic
```

The following is sample output from the **show dhcpd state** command:

```
ciscoasa# show dhcpd state
```

```
Context Not Configured for DHCP
Interface outside, Not Configured for DHCP
Interface inside, Not Configured for DHCP
```

The following is sample output from the **show dhcpd statistics** command:

```
ciscoasa# show dhcpd statistics
DHCP UDP Unreachable Errors: 0
DHCP Other UDP Errors: 0
Address pools        1
Automatic bindings   1
Expired bindings     1
Malformed messages   0
Message              Received
BOOTREQUEST          0
DHCPDISCOVER         1
DHCPREQUEST          2
DHCPDECLINE          0
DHCPRELEASE          0
DHCPINFORM           0
Message              Sent
BOOTREPLY            0
DHCPOFFER            1
DHCPACK              1
DHCPNAK              1
```

Related Commands

Command	Description
clear configure dhcpd	Removes all DHCP server settings.
clear dhcpd	Clears the DHCP server bindings and statistic counters.
dhcpd lease	Defines the lease length for DHCP information granted to clients.
show running-config dhcpd	Displays the current DHCP server configuration.

show dhcprelay state

To view the state of the DHCP relay agent, use the **show dhcprelay state** command in privileged EXEC or global configuration mode.

show dhcprelay state

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:

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

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

This command displays the DHCP relay agent state information for the current context and each interface.

Examples

The following is sample output from the **show dhcprelay state** command:

```
ciscoasa# show dhcprelay state
Context  Configured as DHCP Relay
Interface outside, Not Configured for DHCP
Interface infrastructure, Configured for DHCP RELAY SERVER
Interface inside, Configured for DHCP RELAY
```

Related Commands

Command	Description
show dhcpd	Displays DHCP server statistics and state information.
show dhcprelay statistics	Displays the DHCP relay statistics.
show running-config dhcprelay	Displays the current DHCP relay agent configuration.

show dhcprelay statistics

To display the DHCP relay statistics, use the **show dhcprelay statistics** command in privileged EXEC mode.

show dhcprelay statistics

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:

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

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

The output of the **show dhcprelay statistics** command increments until you enter the **clear dhcprelay statistics** command.

Examples

The following shows sample output for the **show dhcprelay statistics** command:

```
ciscoasa# show dhcprelay statistics
DHCP UDP Unreachable Errors: 0
DHCP Other UDP Errors: 0
Packets Relayed
BOOTREQUEST          0
DHCPDISCOVER         7
DHCPREQUEST          3
DHCPDECLINE          0
DHCPRELEASE          0
DHCPINFORM           0
BOOTREPLY            0
DHCPOFFER            7
DHCPACK              3
DHCPNAK              0
ciscoasa#
```

Related Commands

Command	Description
clear configure dhcprelay	Removes all DHCP relay agent settings.

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

show diameter

To display state information for each Diameter connection, use the **show diameter** command in privileged EXEC mode.

show diameter

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:

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

Command History

Release	Modification
9.5(2)	This command was added.

Usage Guidelines

To display Diameter connection state information, you must inspect Diameter traffic.

Examples

The following shows sample output for the **show diameter** command:

```
ciscoasa# show diameter

Total active diameter sessions: 5
Session 3638
       ==========
       ref_count: 1 val = .; 1096298391; 2461;
           Protocol : diameter Context id : 0
           From inside:211.1.1.10/45169 to outside:212.1.1.10/3868
...
```

Related Commands

Command	Description
clear service-policy	Clears service policy statistic.
inspect diameter	Inspects Diameter traffic.

show disk

To display the contents of the flash memory for the ASA only, use the **show disk** command in privileged EXEC mode.

show disk [**0 | 1**] [**filesys | all**] **controller**

Syntax Description

0 | **1**	Specifies the internal flash memory (0, the default) or the external flash memory (1).
all	Shows the contents of flash memory plus the file system information.
controller	Specifies the flash controller model number.
filesys	Shows information about the compact flash card.

Command Default

By default, this command shows the internal flash memory.

Command Modes

The 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	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
7.0(1)	This command was added.

Examples

The following is sample output from the **show disk** command:

```
ciscoasa# show disk
-#- --length-- -----date/time------ path
 11 1301       Feb 21 2005 18:01:34 test.cfg
 12 1949       Feb 21 2005 20:13:36 test1.cfg
 13 2551       Jan 06 2005 10:07:36 test2.cfg
 14 609223     Jan 21 2005 07:14:18 test3.cfg
 15 1619       Jul 16 2004 16:06:48 test4.cfg
 16 3184       Aug 03 2004 07:07:00 old_running.cfg
 17 4787       Mar 04 2005 12:32:18 test5.cfg
 20 1792       Jan 21 2005 07:29:24 test6.cfg
 21 7765184    Mar 07 2005 19:38:30 test7.cfg
 22 1674       Nov 11 2004 02:47:52 test8.cfg
 23 1863       Jan 21 2005 07:29:18 test9.cfg
 24 1197       Jan 19 2005 08:17:48 test10.cfg
 25 608554     Jan 13 2005 06:20:54 backupconfig.cfg
 26 5124096    Feb 20 2005 08:49:28 cdisk1
```

```
 27 5124096    Mar 01 2005 17:59:56 cdisk2
 28 2074       Jan 13 2005 08:13:26 test11.cfg
 29 5124096    Mar 07 2005 19:56:58 cdisk3
 30 1276       Jan 28 2005 08:31:58 lead
 31 7756788    Feb 24 2005 12:59:46 asdmfile.dbg
 32 7579792    Mar 08 2005 11:06:56 asdmfile1.dbg
 33 7764344    Mar 04 2005 12:17:46 asdmfile2.dbg
 34 5124096    Feb 24 2005 11:50:50 cdisk4
 35 15322      Mar 04 2005 12:30:24 hs_err.log
10170368 bytes available (52711424 bytes used)
```

The following is sample output from the **show disk filesys** command:

```
ciscoasa# show disk filesys
******** Flash Card Geometry/Format Info ********
COMPACT FLASH CARD GEOMETRY
   Number of Heads:            4
   Number of Cylinders       978
   Sectors per Cylinder       32
   Sector Size               512
   Total Sectors          125184
COMPACT FLASH CARD FORMAT
   Number of FAT Sectors      61
   Sectors Per Cluster         8
   Number of Clusters      15352
   Number of Data Sectors 122976
   Base Root Sector          123
   Base FAT Sector             1
   Base Data Sector          155
```

The following is sample output from the **show disk controller** command:

```
ciscoasa# show disk:1 controller
Flash Model: TOSHIBA THNCF064MBA
```

Related Commands

Command	Description
dir	Displays the directory contents.

show dns

To show the current resolved DNS addresses for fully qualified domain name (FQDN) hosts, and the trusted DNS source configuration, use the **show dns** command in privileged EXEC mode.

show dns [**host** *fqdn_name* | **ip-cache** [**count**] | **trusted-source** [**detail**]]

Syntax Description

host*fqdn_name*	(Optional) Limits the command to show information about the specified fully-qualified domain name (FQDN) only.
ip-cache [**count**]	(Optional.) Show the contents of the IP cache created by snooping DNS responses for network-service object domain specifications. Include the **count** keyword if you only want to see the number of items in the cache.
trusted-source [**detail**]	(Optional.) Show the configuration for trusted DNS servers, which are snooped for network-service object domain resolution. Include the **detail** keyword to show the IP addresses of all trusted DNS servers.

Command Default

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	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
9.17(1)	Without parameters, the **show dns** command and **show dns-hosts** commands provide the same information. We also added the **ip-cache** and **trusted-source** keywords.

Examples

The following is sample output from the **show dns** command. If no FQDN host has not been activated yet, this command shows no output.

```
ciscoasa# show dns
Name:   www.example1.com
  Address: 10.1.3.1                              TTL 00:03:01
  Address: 10.1.3.3                              TTL 00:00:36
  Address: 10.4.1.2                              TTL 00:01:01
Name: www.example2.com
  Address: 10.2.4.1                              TTL 00:25:13
  Address: 10.5.2.1                              TTL 00:25:01
```

```
Name: server.ddns-exampleuser.com
  Address: fe80::21e:8cff:feb5:4faa             TTL 00:00:41
  Address: 10.10.10.2                           TTL 00:25:01
```

The following is sample output from the **show dns host** command:

```
ciscoasa# show dns host www.example.com
Name:   www.example.com
Address: 10.1.3.1 TTL 00:03:01
Address: 10.1.9.5 TTL 00:00:36
Address: 10.1.1.2 TTL 00:01:01
```

Starting with 9.17(1), the command without parameters shows the same information as the **show dns-hosts** command, and includes information on the trusted DNS sources used for network-service object domain resolution, and the IP cache.

```
ciscoasa# show dns
Host                     Flags      Age Type   Address(es)
sngdc01-ucs-dcz01n-gslb1-(temp, OK) 0    IP    173.39.112.230
alln01-ucs-dcz03n-gslb1-s(temp, OK) 0    IP    173.37.151.38
rcdn9-ucs-dcz05n-gslb1-sn(temp, OK) 0    IP    72.163.7.198
aer01-ucs-dcz01n-gslb1-sn(temp, OK) 0    IP    173.38.213.70
rtp5-ucs-dcz01n-gslb1-sni(temp, OK) 0    IP    64.101.37.118
mtv5-ucs-dcz06n-gslb1-sni(temp, OK) 0    IP    173.36.225.38
www.cisco.com            (temp, OK) 0    IP    72.163.4.161
       origin-www.cisco.com
DNS Trusted Source enabled for DHCP Server Configured
DNS Trusted Source enabled for DHCP Client Learned
DNS Trusted Source enabled for DHCP Relay Learned
DNS Trusted Source enabled for DNS Server Configured
DNS Trusted Source not enabled for Trust-any
DNS Trusted Source: Type: IPs : Interface : Idle/Timeout (sec)
    DNS Server Configured: 72.163.47.11: management : N/A
    DNS Server Configured: 173.37.137.85: management : N/A
    DNS Server Configured: 173.37.142.73: management : N/A
DNS snooping IP cache: 0 in use, 0 most used
Address                              Idle(sec) Timeout(sec) Hit-count          Branch(es)
```

Related Commands

Command	Description
clear dns-hosts	Clears the DNS cache.
clear ip-cache	Clears the cache built by snooping DNS responses for network-service object domain specifications.
dns domain-lookup	Enables the ASA to perform a name lookup.
dns name-server	Configures a DNS server address.
dns trusted-source	Identifies the trusted DNS servers.

show dns-hosts

To show the DNS cache, use the **show dns-hosts** command in privileged EXEC mode. The DNS cache includes dynamically learned entries from a DNS server and manually entered names and IP addresses.

show dns-hosts

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:

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

Command History

Release	Modification
7.0(1)	This command was added.

Examples

The following is sample output from the **show dns-hosts** command:

```
ciscoasa# show dns-hosts
Host                      Flags      Age Type   Address(es)
ns2.example.com           (temp, OK) 0    IP    10.102.255.44
ns1.example.com           (temp, OK) 0    IP    192.168.241.185
snowmass.example.com      (temp, OK) 0    IP    10.94.146.101
server.example.com        (temp, OK) 0    IP    10.94.146.80
```

Related Commands

Command	Description
clear dns-hosts	Clears the DNS cache.
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.

Table 11 shows each field description.

Table 1: show dns-hosts Fields

Field	Description
Host	Shows the hostname.
Flags	Shows the entry status as a combination of the following: • temp—This entry is temporary because it comes from a DNS server. The ASA removes this entry after 72 hours of inactivity. • perm—This entry is permanent because it was added with the name command. • OK—This entry is valid. • ??—This entry is suspect and needs to be revalidated. • EX—This entry is expired.
Age	Shows the number of hours since this entry was last referenced.
Type	Shows the type of DNS record; this value is always IP.
Address(es)	The IP addresses.

Related Commands

Command	Description
clear dns-hosts	Clears the DNS cache.
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 dynamic-filter data

To show information about the Botnet Traffic Filter 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, use the **show dynamic-filter data** command in privileged EXEC mode.

show dynamic-filter data

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:

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

Command History

Release	Modification
8.2(1)	This command was added.

Usage Guidelines

To view dynamic database information, first enable use and download of the database with the **dynamic-filter use-database** and **dynamic-filter updater-client enable** commands.

Examples

The following is sample output from the **show dynamic-filter data** command:

```
ciscoasa# show dynamic-filter data
Traffic filter is using downloaded database version '907'
Fetched at 18:00:16 UTC Jan 22 2009, size: 674381
Sample names from downloaded database:
  example.com, example.net, example.org,
cisco.example, cisco.invalid, bad.example.com
bad.example.net, bad.example.org, bad.cisco.example
bad.cisco.ivalid
Total entries in Dynamic Filter database:
  Dynamic data: 40909 domain names , 1080 IPv4 addresses
  Local data: 0 domain names , 0 IPv4 addresses
Active rules in Dynamic Filter asp table:
  Dynamic data: 0 domain names , 1080 IPv4 addresses
  Local data: 0 domain names , 0 IPv4 addresses
```

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 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.
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 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.

Command	Description
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.

show dynamic-filter dns-snoop

To show the Botnet Traffic Filter DNS snooping summary, or the actual IP addresses and names, use the **show dynamic-filter dns-snoop** command in privileged EXEC mode.

show dynamic-filter dns-snoop [**detail**]

Syntax Description

detail	(Optional) Shows the IP addresses and names snooped from DNS responses.

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
8.2(1)	This command was added.

Usage Guidelines

All inspected DNS data is included in this output, and not just matching names in the blacklist. DNS data from static entries are not included.

To clear the DNS snooping data, enter the **clear dynamic-filter dns-snoop** command.

Examples

The following is sample output from the **show dynamic-filter dns-snoop** command:

```
ciscoasa# show dynamic-filter dns-snoop
DNS Reverse Cache Summary Information:
75 addresses, 124 names, 997 dnsrc address buckets
```

The following is sample output from the **show dynamic-filter dns-snoop detail** command:

```
ciscoasa# show dynamic-filter dns-snoop detail
DNS Reverse Cache Summary Information:
75 addresses, 124 names, 997 dnsrc address buckets
DNS reverse Cache Information:
[10.67.22.34] flags=0x22, cat=2, unit=0 b:g:w=3:0:0, cookie=0xda148218
    [www3.example.com] cat=2, ttl=3
    [www.bad.example.com] cat=2, ttl=3
    [www.example.com] cat=2, ttl=3
[10.6.68.133] flags=0x2, cat=2, unit=0 b:g:w=1:0:0, cookie=0xda13ed60
    [cisco.example] cat=2, ttl=73
```

```
[10.166.226.25] flags=0x2, cat=2, unit=0 b:g:w=1:0:0, cookie=0xda608cb8
    [cisco.invalid] cat=2, ttl=2
```

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 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.
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 reports	Generates reports of the top 10 botnet sites, ports, and infected hosts.

Command	Description
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.

show dynamic-filter reports infected-hosts

To generate reports about infected hosts classified by the Botnet Traffic Filter, use the **show dynamic-filter reports infected-hosts** command in privileged EXEC mode.

show dynamic-filter reports infected-hosts [**max-connections | latest-active | highest-threat |subnet** *ip_address netmask* **| all**]

Syntax Description

all	Shows all buffered infected-hosts information. This display might include thousands of entries. You might want to use ASDM to generate a PDF file instead of using the CLI.
highest-threat	Shows the 20 hosts that connected to the malware sites with the highest threat level.
latest-active	Shows the 20 hosts with the most recent activity. For each host, the display shows detailed information about 5 visited malware sites.
max-connections	Shows the 20 infected hosts with the most number of connections.
subnet *ip_address netmask*	Shows up to 20 hosts within the specified subnet.

Command Default

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	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
8.2(2)	This command was added.

Usage Guidelines

These reports contain detailed history about infected hosts, showing the correlation between infected hosts, visited malware sites, and malware ports.

To clear the report data, enter the **clear dynamic-filter reports infected-hosts** command.

Examples

The following is sample output from the **show dynamic-filter reports infected hosts all** command:

```
ciscoasa#
                show
```

dynamic-filter reports infected-hosts all

```
Total 2 infected-hosts in buffer

Host (interface)                        Latest malicious conn time, filter action  Conn
logged, dropped

=============================================================================================================

192.168.1.4 (internal)                  15:39:40 UTC Sep 17 2009, dropped
   3      3

Malware-sites connected to (not ordered)

Site                        Latest conn port, time, filter action   Conn logged, dropped
Threat-level Category

-------------------------------------------------------------------------------------------------------------

10.73.210.27 (bad.example.com)     80, 15:39:31 UTC Sep 17 2009, dropped      2   2
very-high Malware

10.65.2.119 (bad2.example.com)     0, 15:39:40 UTC Sep 17 2009, dropped       1   1
very-high admin-added

=============================================================================================================

192.168.1.2 (internal)                  15:39:01 UTC Sep 17 2009, dropped
   5      5

Malware-sites connected to (not ordered)

Site                        Latest conn port, time, filter action   Conn logged, dropped
Threat-level Category

-------------------------------------------------------------------------------------------------------------

10.131.36.158 (bad.example.com)    0, 15:37:46 UTC Sep 17 2009, dropped      1    1
very-high admin-added

10.65.2.119 (bad2.example.com)     0, 15:37:53 UTC Sep 17 2009, dropped      1    1
very-high  admin-added

20.73.210.27 (bad3.example.com)   80, 15:39:01 UTC Sep 17 2009, dropped      3    3
very-high  Malware

=============================================================================================================


Last clearing of the infected-hosts report: Never
```

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 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.
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 statistics	Shows how many connections were monitored with the Botnet Traffic Filter, and how many of those connections match the whitelist, blacklist, and greylist.

Command	Description
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.

show dynamic-filter reports top

To generate reports of the top 10 malware sites, ports, and infected hosts classified by the Botnet Traffic Filter, use the **show dynamic-filter reports top** command in privileged EXEC mode.

show dynamic-filter reports top [**malware-sites | malware-ports | infected-hosts**]

Syntax Description

malware-ports	(Optional) Shows a report for the top 10 malware ports.
malware-sites	(Optional) Shows a report for the top 10 malware sites.
infected-hosts	(Optional) Shows a report for the top 10 infected hosts.

Command Default

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	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
8.2(1)	This command was added.
8.2(2)	The **botnet-sites** and **botnet-ports** keywords were changed to **malware-sites** and **malware-ports**. The malware-sites report now includes the number of connections dropped, and the threat level and category of each site. A last clear timestamp was added. For threat events, the severity level was changed from a warning to a notification. Threat events can be triggered every five minutes.

Usage Guidelines

This report is a snapshot of the data, and may not match the top 10 items since the statistics started to be collected.

To clear the report data, enter the **clear dynamic-filter reports top** command.

Examples

The following is sample output from the **show dynamic-filter reports top malware-sites** command:

```
ciscoasa# show dynamic-filter reports top malware-sites
Site                                Connections logged dropped Threat Level Category
-------------------------------------------------------------------------------------
bad1.example.com (10.67.22.34)                    11     0          2      Botnet
bad2.example.com (209.165.200.225)                 8     8          3      Virus
bad1.cisco.example(10.131.36.158)                  6     6          3      Virus
bad2.cisco.example(209.165.201.1)                  2     2          3      Trojan
```

```
horrible.example.net(10.232.224.2)                    2     2          3      Botnet
nono.example.org(209.165.202.130)                     1     1          3      Virus
Last clearing of the top sites report: at 13:41:06 UTC Jul 15 2009
```

The following is sample output from the **show dynamic-filter reports top malware-ports** command:

```
ciscoasa# show dynamic-filter reports top malware-ports
Port                                        Connections logged
------------------------------------------------------------------------
tcp 1000                                                  617
tcp 2001                                                  472
tcp 23                                                     22
tcp 1001                                                   19
udp 2000                                                   17
udp 2001                                                   17
tcp 8080                                                    9
tcp 80                                                      3
tcp >8192                                                   2
Last clearing of the top ports report: at 13:41:06 UTC Jul 15 2009
```

The following is sample output from the **show dynamic-filter reports top infected-hosts** command:

```
ciscoasa# show dynamic-filter reports top infected-hosts
Host                                        Connections logged
------------------------------------------------------------------------
10.10.10.51(inside)                                     1190
10.12.10.10(inside)                                       10
10.10.11.10(inside)                                        5
Last clearing of the top infected-hosts report: at 13:41:06 UTC Jul 15 2009
```

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 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.
dynamic-filter database purge	Manually deletes the Botnet Traffic Filter dynamic database.
dynamic-filter drop blacklist	Automatically drops blacklisted traffic.

Command	Description
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 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.

show dynamic-filter statistics

To show how many connections were classified as whitelist, blacklist, and greylist connections using the Botnet Traffic Filter, use the **show dynamic-filter statistics** command in privileged EXEC mode.

show dynamic-filter statistics [**interface** *name*] [**detail**]

Syntax Description

detail	(Optional) Shows how many packets at each threat level were classified or dropped.
interface *name*	(Optional) Shows 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:

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

Command History

Release	Modification
8.2(1)	This command was added.
8.2(2)	The **detail** keyword was added to show how many packets at each threat level were classified or dropped. For threat events, the severity level was changed from a warning to a notification. Threat events can be triggered every five minutes.

Usage Guidelines

The greylist includes addresses that are associated with multiple domain names, but not all of these domain names are on the blacklist.

To clear the statistics, enter the **clear dynamic-filter statistics** command.

Examples

The following is sample output from the **show dynamic-filter statistics** command:

```
ciscoasa# show dynamic-filter statistics
Enabled on interface outside
 Total conns classified 11, ingress 11, egress 0
 Total whitelist classified 0, ingress 0, egress 0
 Total greylist classified 0, dropped 0, ingress 0, egress 0
 Total blacklist classified 11, dropped 5, ingress 11, egress 0
Enabled on interface inside
 Total conns classified 1182, ingress 1182, egress 0
 Total whitelist classified 3, ingress 3, egress 0
```

```
 Total greylist classified 0, dropped 0, ingress 0, egress 0
 Total blacklist classified 1179, dropped 1000, ingress 1179, egress 0
```

The following is sample output from the **show dynamic-filter statistics interface outside detail** command:

```
ciscoasa# show dynamic-filter statistics interface outside detail
Enabled on interface outside
 Total conns classified 2108, ingress 2108, egress 0
 Total whitelist classified 0, ingress 0, egress 0
 Total greylist classified 1, dropped 1, ingress 0, egress 0
   Threat level 5 classified 1, dropped 1, ingress 0, egress 0
   Threat level 4 classified 0, dropped 0, ingress 0, egress 0
   ...
Total blacklist classified 30, dropped 20, ingress 11, egress 2
   Threat level 5 classified 6, dropped 6, ingress 4, egress 2
   Threat level 4 classified 5, dropped 5, ingress 5, egress 0
```

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 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.
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.

Command	Description
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 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.

show dynamic-filter updater-client

To show information about the Botnet Traffic Filter updater server, including the server IP address, the next time the ASA will connect with the server, and the database version last installed, use the **show dynamic-filter updater-client** command in privileged EXEC mode.

show dynamic-filter updater-client

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:

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

Command History

Release	Modification
8.2(1)	This command was added.

Examples

The following is sample output from the **show dynamic-filter updater-client** command:

```
ciscoasa# show dynamic-filter updater-client
Traffic Filter updater client is enabled
Updater server url is https://10.15.80.240:446
Application name: trafmon, version: 1.0
Encrypted UDI:
0bb93985f42d941e50dc8f022350d1a8de96ba6c1f6d45f4bc0ead02a7d5990be32f483b
5715cd80a215cedadd4e5ffe
Next update is in 00:02:00
Database file version is '907' fetched at 22:51:41 UTC Oct 16 2006,
size: 521408
```

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 reports	Clears Botnet Traffic filter report data.

Command	Description
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	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 running-config dynamic-filter	Shows the Botnet Traffic Filter running configuration.

show eigrp events

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

show eigrp [*as-number*] **events** [{ *start end* } | **type**]

Syntax Description

as-number	(Optional) Specifies the autonomous system number of the EIGRP process for which you are viewing the event log. Because the ASA only supports one EIGRP routing process, you do not need to specify the autonomous system number.
end	(Optional) Limits the output to the entries with starting with the *start* index number and ending with the *end* index number.
start	(Optional) A number specifying the log entry index number. Specifying a start number causes the output to start with the specified event and end with the event specified by the *end* argument. Valid values are from 1 to 4294967295.
type	(Optional) Displays the events that are being logged.

Command Default

If a *start* and *end* is not specified, all log entries are shown.

Command Modes

The 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	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
8.0(2)	This command was added.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

The **show eigrp events** output displays up to 500 events. Once the maximum number of events has been reached, new events are added to the bottom of the output and old events are removed from the top of the output.

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

The **show eigrp events type** command displays the logging status of EIGRP events. By default, neighbor changes, neighbor warning, and DUAL FSM messages are logged. You can disable neighbor change event logging using the **no eigrp log-neighbor-changes** command. You can disable neighbor warning event logging using the **no eigrp log-neighbor-warnings** command. You cannot disable the logging of DUAL FSM events.

Examples

The following is sample output from the **show eigrp events** command:

```
ciscoasa# show eigrp events
Event information for AS 100:
1    12:11:23.500 Change queue emptied, entries: 4
2    12:11:23.500 Metric set: 10.1.0.0/16 53760
3    12:11:23.500 Update reason, delay: new if 4294967295
4    12:11:23.500 Update sent, RD: 10.1.0.0/16 4294967295
5    12:11:23.500 Update reason, delay: metric chg 4294967295
6    12:11:23.500 Update sent, RD: 10.1.0.0/16 4294967295
7    12:11:23.500 Route install: 10.1.0.0/16 10.130.60.248
8    12:11:23.500 Find FS: 10.1.0.0/16 4294967295
9    12:11:23.500 Rcv update met/succmet: 53760 28160
10   12:11:23.500 Rcv update dest/nh: 10.1.0.0/16 10.130.60.248
11   12:11:23.500 Metric set: 10.1.0.0/16 4294967295
```

The following is sample output from the **show eigrp events** command with a start and stop number defined:

```
ciscoasa# show eigrp events 3 8
Event information for AS 100:
3    12:11:23.500 Update reason, delay: new if 4294967295
4    12:11:23.500 Update sent, RD: 10.1.0.0/16 4294967295
5    12:11:23.500 Update reason, delay: metric chg 4294967295
6    12:11:23.500 Update sent, RD: 10.1.0.0/16 4294967295
7    12:11:23.500 Route install: 10.1.0.0/16 10.130.60.248
8    12:11:23.500 Find FS: 10.1.0.0/16 4294967295
```

The following is sample output from the **show eigrp events** command when there are no entries in the EIGRP event log:

```
ciscoasa# show eigrp events
Event information for AS 100:  Event log is empty.
```

The following is sample output from the **show eigrp events type** command:

```
ciscoasa# show eigrp events type
EIGRP-IPv4 Event Logging for AS 100:
      Log Size          500
      Neighbor Changes  Enable
      Neighbor Warnings Enable
      Dual FSM          Enable
```

Related Commands

Command	Description
clear eigrp events	Clears the EIGRP event logging buffer.
eigrp log-neighbor-changes	Enables the logging of neighbor change events.
eigrp log-neighbor-warnings	Enables the logging of neighbor warning events.

show eigrp interfaces

To display the interfaces participating in EIGRP routing, use the **show eigrp interfaces** command in privileged EXEC mode.

show eigrp [*as-number*] **interfaces** [*if-name*] [**detail**]

Syntax Description

as-number	(Optional) Specifies the autonomous system number of the EIGRP process for which you are displaying active interfaces. Because the ASA only supports one EIGRP routing process, you do not need to specify the autonomous system number.
detail	(Optional) Displays detail information.
if-name	(Optional) The name of an interface as specified by the **nameif** command. Specifying an interface name limits the display to the specified interface.

Command Default

If you do not specify an interface name, information for all EIGRP interfaces is displayed.

Command Modes

The 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	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
8.0(2)	This command was added.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

Use the **show eigrp interfaces** command to determine on which interfaces EIGRP is active, and to learn information about EIGRP relating to those interfaces.

If an interface is specified, only that interface is displayed. Otherwise, all interfaces on which EIGRP is running are displayed.

If an autonomous system is specified, only the routing process for the specified autonomous system is displayed. Otherwise, all EIGRP processes are displayed.

Examples

The following is sample output from the **show eigrp interfaces** command:

```
ciscoasa# show eigrp interfaces
EIGRP-IPv4 interfaces for process 100
                    Xmit Queue    Mean   Pacing Time   Multicast   Pending
```

```
Interface    Peers    Un/Reliable    SRTT    Un/Reliable    Flow Timer  Routes
mgmt           0          0/0          0       11/434           0          0
outside        1          0/0        337        0/10            0          0
inside         1          0/0         10        1/63          103          0
```

Table 6-2 describes the significant fields shown in the display.

Table 2: show eigrp interfaces Field Descriptions

Field	Description
process	Autonomous system number for the EIGRP routing process.
Peers	Number of directly-connected peers.
Xmit Queue Un/Reliable	Number of packets remaining in the Unreliable and Reliable transmit queues.
Mean SRTT	Mean smooth round-trip time interval (in seconds).
Pacing Time Un/Reliable	Pacing time (in seconds) used to determine when EIGRP packets should be sent out the interface (unreliable and reliable packets).
Multicast Flow Timer	Maximum number of seconds in which the ASA will send multicast EIGRP packets.
Pending Routes	Number of routes in the packets in the transmit queue waiting to be sent.

Related Commands

Command	Description
network	Defines the networks and interfaces that participate in the EIGRP routing process.

show eigrp neighbors

To display the EIGRP neighbor table, use the **show eigrp neighbors** command in privileged EXEC mode.

show eigrp [*as-number*] **neighbors** [**detail** | **static**] [*if-name*]

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.
detail	(Optional) Displays detail neighbor information.
if-name	(Optional) The name of an interface as specified by the **nameif** command. Specifying an interface name displays all neighbor table entries that were learned through that interface.
static	(Optional) Displays EIGRP neighbors that are statically defined using the **neighbor** command.

Command Default

If you do not specify an interface name, the neighbors learned through all interfaces are displayed.

Command Modes

The 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	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
8.0(2)	This command was added.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

You can use the **clear eigrp neighbors** command to clear the dynamically learned neighbors from the EIGRP neighbor table.

Static neighbors are not included in the output unless you use the **static** keyword.

Examples

The following is sample output from the **show eigrp neighbors** command:

```
ciscoasa# show eigrp neighbors
EIGRP-IPv4 Neighbors for process 100
Address                 Interface     Holdtime Uptime   Q      Seq  SRTT  RTO
                                      (secs)   (h:m:s)  Count  Num  (ms)  (ms)
172.16.81.28            Ethernet1     13       0:00:41  0      11   4     20
```

```
172.16.80.28            Ethernet0     14        0:02:01  0      10    12    24
172.16.80.31            Ethernet0     12        0:02:02  0      4     5     20
```

Table 6-2 describes the significant fields shown in the display.

Table 3: show eigrp neighbors Field Descriptions

Field	Description
process	Autonomous system number for the EIGRP routing process.
Address	IP address of the EIGRP neighbor.
Interface	Interface on which the ASA receives hello packets from the neighbor.
Holdtime	Length of time (in seconds) that the ASA waits to hear from the neighbor before declaring it down. This hold time is received from the neighbor in the hello packet, and begins decreasing until another hello packet is received from the neighbor. If the neighbor is using the default hold time, this number will be less than 15. If the peer configures a non-default hold time, the non-default hold time will be displayed. If this value reaches 0, the ASA considers the neighbor unreachable.
Uptime	Elapsed time (in hours:minutes: seconds) since the ASA first heard from this neighbor.
Q Count	Number of EIGRP packets (update, query, and reply) that the ASA is waiting to send.
Seq Num	Sequence number of the last update, query, or reply packet that was received from the neighbor.
SRTT	Smooth round-trip time. This is the number of milliseconds required for an EIGRP packet to be sent to this neighbor and for the ASA to receive an acknowledgment of that packet.
RTO	Retransmission timeout (in milliseconds). This is the amount of time the ASA waits before resending a packet from the retransmission queue to a neighbor.

The following is sample output from the **show eigrp neighbors static** command:

```
ciscoasa# show eigrp neighbors static
EIGRP-IPv4 neighbors for process 100
Static Address                Interface
192.168.1.5                   management
```

Table 6-4 describes the significant fields shown in the display.

Table 4: show ip eigrp neighbors static Field Descriptions

Field	Description
process	Autonomous system number for the EIGRP routing process.
Static Address	IP address of the EIGRP neighbor.
Interface	Interface on which the ASA receives hello packets from the neighbor.

Examples

The following is sample output from the **show eigrp neighbors detail** command:

```
ciscoasa# show eigrp neighbors detail
EIGRP-IPv4 neighbors for process 100
H   Address                 Interface       Hold Uptime   SRTT   RTO  Q Seq Tye
                                            (sec)         (ms)       Cnt Num
3   1.1.1.3                 Et0/0             12 00:04:48 1832  5000  0  14
   Version 12.2/1.2, Retrans: 0, Retries: 0
   Restart time 00:01:05
0   10.4.9.5                Fa0/0             11 00:04:07  768  4608  0  4   S
   Version 12.2/1.2, Retrans: 0, Retries: 0
2   10.4.9.10               Fa0/0             13 1w0d        1  3000  0  6   S
   Version 12.2/1.2, Retrans: 1, Retries: 0
1   10.4.9.6                Fa0/0             12 1w0d        1  3000  0  4   S
   Version 12.2/1.2, Retrans: 1, Retries: 0
```

Table 5: show ip eigrp neighbors details Field Descriptions describes the significant fields shown in the display.

Table 5: show ip eigrp neighbors details Field Descriptions

Field	Description
process	Autonomous system number for the EIGRP routing process.
H	This column lists the order in which a peering session was established with the specified neighbor. The order is specified with sequential numbering starting with 0.
Address	IP address of the EIGRP neighbor.
Interface	Interface on which the ASA receives hello packets from the neighbor.
Holdtime	Length of time (in seconds) that the ASA waits to hear from the neighbor before declaring it down. This hold time is received from the neighbor in the hello packet, and begins decreasing until another hello packet is received from the neighbor. If the neighbor is using the default hold time, this number will be less than 15. If the peer configures a non-default hold time, the non-default hold time will be displayed. If this value reaches 0, the ASA considers the neighbor unreachable.
Uptime	Elapsed time (in hours:minutes: seconds) since the ASA first heard from this neighbor.
SRTT	Smooth round-trip time. This is the number of milliseconds required for an EIGRP packet to be sent to this neighbor and for the ASA to receive an acknowledgment of that packet.
RTO	Retransmission timeout (in milliseconds). This is the amount of time the ASA waits before resending a packet from the retransmission queue to a neighbor.
Q Count	Number of EIGRP packets (update, query, and reply) that the ASA is waiting to send.
Seq Num	Sequence number of the last update, query, or reply packet that was received from the neighbor.
Version	The software version that the specified peer is running.
Retrans	The number of times that a packet has been retransmitted.

Field	Description
Retries	The number of times an attempt was made to retransmit a packet.
Restart time	Elapsed time (in hours:minutes:seconds) since the specified neighbor has restarted.

Related Commands

Command	Description
clear eigrp neighbors	Clears the EIGRP neighbor table.
debug eigrp neighbors	Displays EIGRP neighbor debugging messages.
debug ip eigrp	Displays EIGRP packet debugging messages.

show eigrp topology

To display the EIGRP topology table, use the **show eigrp topology** command in privileged EXEC mode.

show eigrp [*as-number*] **topology** [*ip-addr* [*mask*]] **active | all-links | pending | summary | zero-successors**]

Syntax Description

active	(Optional) Displays only active entries in the EIGRP topology table.
all-links	(Optional) Displays all routes in the EIGRP topology table, even those that are not feasible successors.
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.
ip-addr	(Optional) Defines the IP address from the topology table to display. When specified with a mask, a detailed description of the entry is provided.
mask	(Optional) Defines the network mask to apply to the *ip-addr* argument.
pending	(Optional) Displays all entries in the EIGRP topology table that are waiting for an update from a neighbor or are waiting to reply to a neighbor.
summary	(Optional) Displays a summary of the EIGRP topology table.
zero-successors	(Optional) Displays available routes in the EIGRP topology table.

Command Default

Only routes that are feasible successors are displayed. Use the **all-links** keyword to display all routes, including those that are not feasible successors.

Command Modes

The 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	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
8.0(2)	This command was added.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

You can use the **clear eigrp topology** command to remove the dynamic entries from the topology table.

Examples

The following is sample output from the **show eigrp topology** command:

Command History

```
EIGRP-IPv4 Topology Table for AS(100)/ID(192.168.1.1)
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - Reply status
P 10.2.1.0 255.255.255.0, 2 successors, FD is 0
          via 10.16.80.28 (46251776/46226176), Ethernet0
          via 10.16.81.28 (46251776/46226176), Ethernet1
P 10.2.1.0 255.255.255.0, 1 successors, FD is 307200
          via Connected, Ethernet1
          via 10.16.81.28 (307200/281600), Ethernet1
          via 10.16.80.28 (307200/281600), Ethernet0
```

Table 6-6 describes the significant fields shown in the displays.

Table 6: show eigrp topology Field Information

Field	Description
Codes	State of this topology table entry. Passive and Active refer to the EIGRP state with respect to this destination; Update, Query, and Reply refer to the type of packet that is being sent.
P - Passive	The route is known to be good and no EIGRP computations are being performed for this destination.
A - Active	EIGRP computations are being performed for this destination.
U - Update	Indicates that an update packet was sent to this destination.
Q - Query	Indicates that a query packet was sent to this destination.
R - Reply	Indicates that a reply packet was sent to this destination.
r - Reply status	Flag that is set after the software has sent a query and is waiting for a reply.
address mask	Destination IP address and mask.
successors	Number of successors. This number corresponds to the number of next hops in the IP routing table. If “successors” is capitalized, then the route or next hop is in a transition state.
FD	Feasible distance. The feasible distance is the best metric to reach the destination or the best metric that was known when the route went active. This value is used in the feasibility condition check. If the reported distance of the router (the metric after the slash) is less than the feasible distance, the feasibility condition is met and that path is a feasible successor. Once the software determines it has a feasible successor, it need not send a query for that destination.
via	IP address of the peer that told the software about this destination. The first *n* of these entries, where *n* is the number of successors, is the current successors. The remaining entries on the list are feasible successors.
(*cost* /*adv_cost*)	The first number is the EIGRP metric that represents the cost to the destination. The second number is the EIGRP metric that this peer advertised.

Field	Description
interface	The interface from which the information was learned.

Command History

The following is sample output from the **show eigrp topology** used with an IP address. The output shown is for an internal route.

```
ciscoasa# show eigrp topology 10.2.1.0 255.255.255.0
EIGRP-IPv4 (AS 100): Topology Default-IP-Routing-Table(0) entry for entry for 10.2.1.0
255.255.255.0
 State is Passive, Query origin flag is 1, 1 Successor(s), FD is 281600
 Routing Descriptor Blocks:
  0.0.0.0 (Ethernet0/0), from Connected, Send flag is 0x0
   Composite metric is (281600/0), Route is Internal
   Vector metric:
    Minimum bandwidth is 10000 Kbit
    Total delay is 1000 microseconds
    Reliability is 255/255
    Load is 1/255
    Minimum MTU is 1500
    Hop count is 0
```

The following is sample output from the **show eigrp topology** used with an IP address. The output shown is for an external route.

```
ciscoasa# show eigrp topology 10.4.80.0 255.255.255.0
EIGRP-IPv4 (AS 100): Topology Default-IP-Routing-Table(0) entry for entry for 10.4.80.0
255.255.255.0
 State is Passive, Query origin flag is 1, 1 Successor(s), FD is 409600
 Routing Descriptor Blocks:
  10.2.1.1 (Ethernet0/0), from 10.2.1.1, Send flag is 0x0
   Composite metric is (409600/128256), Route is External
   Vector metric:
    Minimum bandwidth is 10000 Kbit
    Total delay is 6000 microseconds
    Reliability is 255/255
    Load is 1/255
    Minimum MTU is 1500
    Hop count is 1
   External data:
    Originating router is 10.89.245.1
    AS number of route is 0
    External protocol is Connected, external metric is 0
    Administrator tag is 0 (0x00000000)
```

Related Commands

Command	Description
clear eigrp topology	Clears the dynamically discovered entries from the EIGRP topology table.

show eigrp traffic

To display the number of EIGRP packets sent and received, use the **show eigrp traffic** command in privileged EXEC mode.

show eigrp [*as-number*] **traffic**

Syntax Description

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

Command Default

No default behaviors or values.

Command Modes

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

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

Command History

Release	Modification
8.0(2)	This command was added.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

You can use the **clear eigrp traffic** command to clear the EIGRP traffic statistics.

Examples

The following is sample output from the **show eigrp traffic** command:

```
ciscoasa# show eigrp traffic
EIGRP-IPv4 Traffic Statistics for AS 100
  Hellos sent/received: 218/205
  Updates sent/received: 7/23
  Queries sent/received: 2/0
  Replies sent/received: 0/2
  Acks sent/received: 21/14
  Input queue high water mark 0, 0 drops
  SIA-Queries sent/received: 0/0
  SIA-Replies sent/received: 0/0
  Hello Process ID: 1719439416
  PDM Process ID: 1719439824
```

Table 6-4 describes the significant fields shown in the display.

Table 7: show eigrp traffic Field Descriptions

Field	Description
process	Autonomous system number for the EIGRP routing process.
Hellos sent/received	Number of hello packets sent and received.
Updates sent/received	Number of update packets sent and received.
Queries sent/received	Number of query packets sent and received.
Replies sent/received	Number of reply packets sent and received.
Acks sent/received	Number of acknowledgment packets sent and received.
Input queue high water mark/drops	Number of received packets that are approaching the maximum receive threshold and number of dropped packets.
SIA-Queries sent/received	Stuck-in-active queries sent and received.
SIA-Replies sent/received	Stuck-in-active replies sent and received.

Related Commands

Command	Description
debug eigrp packets	Displays debugging information for EIGRP packets sent and received.
debug eigrp transmit	Displays debugging information for EIGRP messages sent.

show environment

To display system environment information for system components, use the **show environment** command in privileged EXEC mode.

show environment [**alarm-contact | driver | fans | power-consumption | power-supply | temperature**] [**chassis | cpu | voltage**]

Syntax Description

alarm-contact	(Optional) Displays the operational status of the input alarm contacts on an ISA 3000 device.
chassis	(Optional) Limits the temperature display to the chassis.
cpu	(Optional) Limits the temperature display to the processors.
driver	(Optional) Displays the environment monitoring (IPMI) driver status. The driver status can be one of the following: • RUNNING—The driver is operational. • STOPPED—An error has caused the driver to stop.
fans	(Optional) Displays the operational status of the cooling fans. The status is one of the following: • OK—The fan is operating normally. • Failed—The fan has failed and should be replaced. When you remove dual fan module, to view the actual status of the fan, use the **show environment basic** and **show environment expand** FXOS commands.
power-consumption	(Optional) Shows the power consumption for PoE interfaces.

power-supply	(Optional) Displays the operational status of the power supplies. The status for each power supply is one of the following: • OK—The power supply is operating normally. • Failed—The power supply has failed and should be replaced. • Not Present—The specified power supply is not installed. The power supply redundancy status also displays. The redundancy status is one of the following: • OK—The unit is operating normally with full resources. • Lost—The unit has lost redundancy but is operating normally with minimum resources. Any further failures will result in a system shutdown. • N/A—The unit is not configured for power supply redundancy.
temperature	(Optional) Displays the temperature and status of the processors and chassis. The temperature is given in celsius. The status is one of the following: • OK—The temperature is within normal operating range. • Critical—The temperature is outside of normal operating range.
voltage	(Optional) Displays the values for CPU voltage channels 1-24. Excludes the operational status.

Command Default

All operational information, except for the driver, is displayed if no keywords are specified.

Command Modes

The 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	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
8.1(1)	This command was added.
8.4(2)	The output for an ASA 5585-X SSP was added. In addition, support for a dual SSP installation was added.
8.4.4(1)	Displayed power supply temperature values for the ASA 5515-X, ASA 5525-X, 5545-X, and ASA 5555-X have been changed in the output.
8.6(1)	The output for CPU voltage regulator thermal events in the ASA 5545-X and ASA 5555-X was added. The output for power supply input status was added. The output for voltage sensors was added.
9.7(1)	We added the **alarm-contact** keyword for the ISA 3000.
9.13(1)	We added the **power-consumption** keyword for the Firepower 1010 PoE interfaces.

Usage Guidelines

You can display operating environment information for the physical components in the device. This information includes the operational status of the fans and power supplies, and temperature and status of the CPUs and chassis. For ISA 3000 devices, it includes information about the input alarm contacts.

Note For a dual SSP installation, only the sensors for the chassis master show output for the cooling fans and power supplies.

Examples

The following is sample generic output from the **show environment** command:

```
ciscoasa# show environment

Cooling Fans:
---------------------------------
   Power Supplies:
   --------------------------------
   Left Slot (PS0): 6900 RPM - OK  (Power Supply Fan)
   Right Slot (PS1): 7000 RPM - OK  (Power Supply Fan) Power Supplies:
---------------------------------
   Power Supply Unit Redundancy: OK
   Temperature:
   --------------------------------
   Left Slot (PS0): 26 C - OK  (Power Supply Temperature)
   Right Slot (PS1): 27 C - OK  (Power Supply Temperature)
   Cooling Fans:
   --------------------------------
   Left Slot (PS0): 6900 RPM - OK  (Power Supply Fan)
   Right Slot (PS1): 7000 RPM - OK  (Power Supply Fan)
Temperature:
---------------------------------
   Processors:
   --------------------------------
   Processor 1: 44.0 C - OK  (CPU1 Core Temperature)
   Processor 2: 45.0 C - OK  (CPU2 Core Temperature)
   Chassis:
   --------------------------------
   Ambient 1: 28.0 C - OK  (Chassis Front Temperature)
```

```
   Ambient 2: 40.5 C - OK  (Chassis Back Temperature)
   Ambient 3: 28.0 C - OK  (CPU1 Front Temperature)
   Ambient 4: 36.50 C - OK  (CPU1 Back Temperature)
   Ambient 5: 34.50 C - OK  (CPU2 Front Temperature)
   Ambient 6: 43.25 C - OK  (CPU2 Back Temperature)
   Power Supplies:
   --------------------------------
   Left Slot (PS0): 26 C - OK  (Power Supply Temperature)
   Right Slot (PS1): 27 C - OK  (Power Supply Temperature)
```

The following is sample output from the **show environment driver** command:

```
ciscoasa# show environment driver
Cooling Fans:
-----------------------------------
   Chassis Fans:
   --------------------------------
   Cooling Fan 1: 5888 RPM - OK
   Cooling Fan 2: 5632 RPM - OK
   Cooling Fan 3: 5888 RPM - OK
   Power Supplies:
   --------------------------------
   Left Slot (PS0): N/A
   Right Slot (PS1): 8448 RPM - OK
Power Supplies:
-----------------------------------
   Left Slot (PS0): Not Present
   Right Slot (PS1): Present
   Left Slot (PS0): N/A
   Right Slot (PS1): 33 C - OK
   Left Slot (PS0): N/A
   Right Slot (PS1): 8448 RPM - OK
Temperature:
-----------------------------------
   Processors:
   --------------------------------
   Processor 1: 70.0 C - OK
   Chassis:
   --------------------------------
   Ambient 1: 36.0 C - OK  (Chassis Back Temperature)
   Ambient 2: 31.0 C - OK  (Chassis Front Temperature)
   Ambient 3: 39.0 C - OK  (Chassis Back Left Temperature)
   Power Supplies:
   --------------------------------
   Left Slot (PS0): N/A
   Right Slot (PS1): 33 C - OK
Voltage:
-----------------------------------
   Channel 1:  1.168 V -  (CPU Core 0.46V-1.4V)
   Channel 2: 11.954 V -  (12V)
   Channel 3:  4.998 V -  (5V)
   Channel 4:  3.296 V -  (3.3V)
   Channel 5:  1.496 V -  (DDR3 1.5V)
   Channel 6:  1.048 V -  (PCH 1.5V)
```

The following is sample output from the **show environment** command for an ASA 5555-X:

```
ciscoasa# show environment
Cooling Fans:
-----------------------------------
   Chassis Fans:
   --------------------------------
   Power Supplies:
```

```
   --------------------------------
   Left Slot (PS0): 9728 RPM - OK
   Right Slot (PS1): 0 RPM - OK
Power Supplies:
 ---------------------------------

    Left Slot (PS0): Present
    Right Slot (PS1): Present

    Power Input:
    --------------------------------
    Left Slot (PS0): OK
    Right Slot (PS1): Failure Detected
    Temperature:
    --------------------------------
    Left Slot (PS0): 29 C - OK
    Right Slot (PS1): N/A
   Processors:
   --------------------------------
   Processor 1: 81.0 C - OK
   Chassis:
   --------------------------------
   Ambient 1: 39.0 C - OK  (Chassis Back Temperature)
   Ambient 2: 32.0 C - OK  (Chassis Front Temperature)
   Ambient 3: 47.0 C - OK  (Chassis Back Left Temperature)
   Power Supplies:
   --------------------------------
   Left Slot (PS0): 33 C - OK
   Right Slot (PS1): -128 C - OK
```

The following is sample output from the **show environment** command for an ASA 5585-X chassis master in a dual SSP installation:

```
ciscoasa(config)# show environment
Cooling Fans:
---------------------------------
   Power Supplies:
   --------------------------------
   Left Slot (PS0): 7000 RPM - OK  (Fan Module Fan)
   Right Slot (PS1): 6900 RPM - OK  (Power Supply Fan)
Power Supplies:
---------------------------------
   Power Supply Unit Redundancy: N/A
   Power Supplies:
   --------------------------------
   Left Slot (PS0): 64 C - OK  (Fan Module Temperature)
   Right Slot (PS1): 64 C - OK  (Power Supply Temperature)
   Power Supplies:
   --------------------------------
   Left Slot (PS0): 7000 RPM - OK  (Fan Module Fan)
   Right Slot (PS1): 6900 RPM - OK  (Power Supply Fan)
Temperature:
---------------------------------
   Processors:
   --------------------------------
   Processor 1: 48.0 C - OK  (CPU1 Core Temperature)
   Processor 2: 47.0 C - OK  (CPU2 Core Temperature)
   Chassis:
   --------------------------------
   Ambient 1: 25.5 C - OK  (Chassis Front Temperature)
   Ambient 2: 37.5 C - OK  (Chassis Back Temperature)
   Ambient 3: 31.50 C - OK  (CPU1 Back Temperature)
   Ambient 4: 27.75 C - OK  (CPU1 Front Temperature)
```

```
   Ambient 5: 38.25 C - OK  (CPU2 Back Temperature)
   Ambient 6: 34.0 C - OK  (CPU2 Front Temperature)
   Power Supplies:
   --------------------------------
   Left Slot (PS0): 64 C - OK  (Fan Module Temperature)
   Right Slot (PS1): 64 C - OK  (Power Supply Temperature)
Voltage:
-----------------------------------
   Channel 1:  3.310 V -  (3.3V (U142 VX1))
   Channel 2:  1.492 V -  (1.5V (U142 VX2))
   Channel 3:  1.053 V -  (1.05V (U142 VX3))
   Channel 4:  3.328 V -  (3.3V_STDBY (U142 VP1))
   Channel 5: 11.675 V -  (12V (U142 VP2))
   Channel 6:  4.921 V -  (5.0V (U142 VP3))
   Channel 7:  6.713 V -  (7.0V (U142 VP4))
   Channel 8:  9.763 V -  (IBV (U142 VH))
   Channel 9:  1.048 V -  (1.05VB (U209 VX2))
   Channel 10:  1.209 V -  (1.2V (U209 VX3))
   Channel 11:  1.109 V -  (1.1V (U209 VX4))
   Channel 12:  0.999 V -  (1.0V (U209 VX5))
   Channel 13:  3.324 V -  (3.3V STDBY (U209 VP1))
   Channel 14:  2.504 V -  (2.5V (U209 VP2))
   Channel 15:  1.799 V -  (1.8V (U209 VP3))
   Channel 16:  1.899 V -  (1.9V (U209 VP4))
   Channel 17:  9.763 V -  (IBV (U209 VH))
   Channel 18:  2.048 V -  (VTT CPU0 (U83 VX2))
   Channel 19:  2.048 V -  (VTT CPU1 (U83 VX3))
   Channel 20:  2.048 V -  (VCC CPU0 (U83 VX4))
   Channel 21:  2.048 V -  (VCC CPU1 (U83 VX5))
   Channel 22:  1.516 V -  (1.5VA (U83 VP1))
   Channel 23:  1.515 V -  (1.5VB (U83 VP2))
   Channel 24:  8.937 V -  (IBV (U83 VH))
```

If the ASA was shut down because of a CPU voltage regulator thermal event, the following warning message appears:

```
WARNING: ASA was previously shut down due to a CPU Voltage Regulator running beyond the max
 thermal operating temperature. The chassis and CPU need to be inspected immediately for
ventilation issues.
```

For more information, see syslog message 735024 in the syslog messages guide.

The following is a sample output from the show environment alarm-contact command:

```
ciscoasa> show environment alarm-contact
ALARM CONTACT 1
   Status:      not asserted
   Description: external alarm contact 1
   Severity:    minor
   Trigger:     closed
ALARM CONTACT 2
   Status:      not asserted
   Description: external alarm contact 2
   Severity:    minor
   Trigger:     closed
```

The following is a sample of driver error statistics.

```
Driver Error Statistics:
-------------------------
I2C I/O Errors          : 0
GPIO Errors             : 0
Ioctl Null Ptr Errors   : 0
```

```
Poll Errors             : 0
Invalid Ioctl Errors    : 0
PECI Errors             : 3
Unknown Errors          : 0
```

The PECI Errors indicate that there is an issue when retrieving the CPU temperature data. The error count number is the number of times it failed retrieving the temperature data.

Related Commands

Command	Description
clear facility-alarm output	De-energizes the output relay and clears the alarm state of the LED.
show facility-alarm relay	Displays status information for triggered alarms.
show version	Displays the hardware and software version.

show event manager

To show information about each configured event manager applet, use the **show event manager** command in privileged EXEC mode.

show event manager

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:

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

Command History

Release	Modification
9.2(1)	This command was added.

Examples

The following is sample output from the **show event manager** command:

```
ciscoasa# show event manager
event manager applet 21, hits 1, last 2014/01/19 06:47:46
  last file disk0:/eem-21-20140119-064746.log
  event countdown 21 secs, left 0 secs, hits 1, last 2014/01/19 06:47:47
  action 1 cli command "sh ver", hits 1, last 2014/01/19 06:47:46
```

Related Commands

Command	Description
show running-config event manager	Shows the event manager running configuration.