CHAPTER 46

show blocks through show cpu Commands

show blocks

To show the packet buffer utilization, use the **show blocks** command in privileged EXEC mode.

show blocks [{**address** *hex* | **all** | **assigned** | **free** | **old** | **pool** *size* [**summary**]} [**diagnostics** | **dump** | **header** | **packet**] | **queue history** [**detail**]]

Syntax Description

address *hex*	(Optional) Shows a block corresponding to this address, in hexadecimal.
all	(Optional) Shows all blocks.
assigned	(Optional) Shows blocks that are assigned and in use by an application.
detail	(Optional) Shows a portion (128 bytes) of the first block for each unique queue type.
dump	(Optional) Shows the entire block contents, including the header and packet information. The difference between dump and packet is that dump includes additional information between the header and the packet.
diagnostics	(Optional) Shows block diagnostics.
free	(Optional) Shows blocks that are available for use.
header	(Optional) Shows the header of the block.
old	(Optional) Shows blocks that were assigned more than a minute ago.
packet	(Optional) Shows the header of the block as well as the packet contents.
pool *size*	(Optional) Shows blocks of a specific size.
queue history	(Optional) Shows where blocks are assigned when the ASA runs out of blocks. Sometimes, a block is allocated from the pool but never assigned to a queue. In that case, the location is the code address that allocated the block.
summary	(Optional) Shows detailed information about block usage sorted by the program addresses of applications that allocated blocks in this class, program addresses of applications that released blocks in this class, and the queues to which valid blocks in this class belong.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	The **pool summary** option was added.
8.0(2)	The dupb block uses 0 length blocks now instead of 4 byte blocks. An additional line was added for 0 byte blocks.

Usage Guidelines

The **show blocks** command helps you determine if the ASA is overloaded. This command lists preallocated system buffer utilization. A full memory condition is not a problem as long as traffic is moving through the ASA. You can use the **show conn** command to see if traffic is moving. If traffic is not moving and the memory is full, there may be a problem.

You can also view this information using SNMP.

The information shown in a security context includes the system-wide information as well as context-specific information about the blocks in use and the high water mark for block usage.

See the "Examples" section for a description of the display output.

Examples

The following is sample output from the **show blocks** command in single mode:

```
hostname# show blocks
  SIZE    MAX    LOW    CNT
     0    100     99    100
     4   1600   1598   1599
    80    400    398    399
   256   3600   3540   3542
  1550   4716   3177   3184
 16384     10     10     10
  2048   1000   1000   1000
```

Table 46-1 shows each field description.

Table 46-1 show blocks Fields

Field	Description
SIZE	Size, in bytes, of the block pool. Each size represents a particular type. Examples are shown below.
0	Used by dupb blocks.
4	Duplicates existing blocks in applications such as DNS, ISAKMP, URL filtering, uauth, TFTP, and TCP modules. Also, this sized block can be used normally by code to send packets to drivers, etc.
80	Used in TCP intercept to generate acknowledgment packets and for failover hello messages.

Table 46-1 show blocks Fields (continued)

Field	Description
256	Used for Stateful Failover updates, syslogging, and other TCP functions. These blocks are mainly used for Stateful Failover messages. The active ASA generates and sends packets to the standby ASA to update the translation and connection table. In bursty traffic, where high rates of connections are created or torn down, the number of available blocks might drop to 0. This situation indicates that one or more connections were not updated to the standby ASA. The Stateful Failover protocol catches the missing translation or connection the next time. If the CNT column for 256-byte blocks stays at or near 0 for extended periods of time, then the ASA is having trouble keeping the translation and connection tables synchronized because of the number of connections per second that the ASA is processing. Syslog messages sent out from the ASA also use the 256-byte blocks, but they are generally not released in such quantity to cause a depletion of the 256-byte block pool. If the CNT column shows that the number of 256-byte blocks is near 0, ensure that you are not logging at Debugging (level 7) to the syslog server. This is indicated by the logging trap line in the ASA configuration. We recommend that you set logging at Notification (level 5) or lower, unless you require additional information for debugging purposes.
1550	Used to store Ethernet packets for processing through the ASA. When a packet enters an ASA interface, it is placed on the input interface queue, passed up to the operating system, and placed in a block. The ASA determines whether the packet should be permitted or denied based on the security policy and processes the packet through to the output queue on the outbound interface. If the ASA is having trouble keeping up with the traffic load, the number of available blocks will hover close to 0 (as shown in the CNT column of the command output). When the CNT column is zero, the ASA attempts to allocate more blocks, up to a maximum of 8192. If no more blocks are available, the ASA drops the packet.
16384	Only used for the 64-bit, 66-MHz Gigabit Ethernet cards (i82543). See the description for 1550 for more information about Ethernet packets.
2048	Control or guided frames used for control updates.
MAX	Maximum number of blocks available for the specified byte block pool. The maximum number of blocks are carved out of memory at bootup. Typically, the maximum number of blocks does not change. The exception is for the 256- and 1550-byte blocks, where the ASA can dynamically create more when needed, up to a maximum of 8192.
LOW	Low-water mark. This number indicates the lowest number of this size blocks available since the ASA was powered up, or since the last clearing of the blocks (with the **clear blocks** command). A zero in the LOW column indicates a previous event where memory was full.
CNT	Current number of blocks available for that specific size block pool. A zero in the CNT column means memory is full now.

The following is sample output from the **show blocks all** command:

```
hostname# show blocks all
Class 0, size 4
     Block   allocd_by    freed_by  data size    alloccnt     dup_cnt  oper location
0x01799940  0x00000000  0x00101603          0           0           0 alloc not_specified
0x01798e80  0x00000000  0x00101603          0           0           0 alloc not_specified
0x017983c0  0x00000000  0x00101603          0           0           0 alloc not_specified
```

```
...

    Found 1000 of 1000 blocks
    Displaying 1000 of 1000 blocks
```

Table 46-2 shows each field description.

Table 46-2 show blocks all Fields

Field	Description
Block	The block address.
allocd_by	The program address of the application that last used the block (0 if not used).
freed_by	The program address of the application that last released the block.
data size	The size of the application buffer/packet data that is inside the block.
alloccnt	The number of times this block has been used since the block came into existence.
dup_cnt	The current number of references to this block if used: 0 means 1 reference, 1 means 2 references.
oper	One of the four operations that was last performed on the block: alloc, get, put, or free.
location	The application that uses the block, or the program address of the application that last allocated the block (same as the allocd_by field).

The following is sample output from the **show blocks** command in a context:

```
hostname/contexta# show blocks
  SIZE    MAX    LOW    CNT  INUSE   HIGH
     4   1600   1599   1599      0      0
    80    400    400    400      0      0
   256   3600   3538   3540      0      1
  1550   4616   3077   3085      0      0
```

The following is sample output from the **show blocks queue history** command:

```
hostname# show blocks queue history
Each Summary for User and Queue_type is followed its top 5 individual queues
Block Size: 4
Summary for User "http", Queue "tcp_unp_c_in", Blocks 1595, Queues 1396
Blk_cnt Q_cnt Last_Op Queue_Type        User      Context
    186     1 put                               contexta
     15     1 put                               contexta
      1     1 put                               contexta
      1     1 put                               contextb
      1     1 put                               contextc
Summary for User "aaa", Queue "tcp_unp_c_in", Blocks 220, Queues 200
Blk_cnt Q_cnt Last_Op Queue_Type        User      Context
     21     1 put                               contexta
      1     1 put                               contexta
      1     1 put                               contexta
      1     1 put                               contextb
      1     1 put                               contextc
Blk_cnt Q_cnt Last_Op Queue_Type        User      Context
    200     1 alloc   ip_rx             tcp       contexta
    108     1 get     ip_rx             udp       contexta
     85     1 free    fixup             h323_ras  contextb
     42     1 put     fixup             skinny    contextb

Block Size: 1550
```

```
Summary for User "http", Queue "tcp_unp_c_in", Blocks 1595, Queues 1000
Blk_cnt Q_cnt Last_Op Queue_Type        User      Context
    186     1 put                               contexta
     15     1 put                               contexta
      1     1 put                               contexta
      1     1 put                               contextb
      1     1 put                               contextc
...
```

The following is sample output from the **show blocks queue history detail** command:

```
hostname# show blocks queue history detail
History buffer memory usage: 2136 bytes (default)
Each Summary for User and Queue type is followed its top 5 individual queues
Block Size: 4
Summary for User "http", Queue_Type "tcp_unp_c_in", Blocks 1595, Queues 1396
Blk_cnt Q_cnt Last_Op Queue_Type        User      Context
    186     1 put                               contexta
     15     1 put                               contexta
      1     1 put                               contexta
      1     1 put                               contextb
      1     1 put                               contextc
 First Block information for Block at 0x.....
  dup_count 0, flags 0x8000000, alloc_pc 0x43ea2a,
  start_addr 0xefb1074, read_addr 0xefb118c, write_addr 0xefb1193
  urgent_addr 0xefb118c, end_addr 0xefb17b2
  0efb1150: 00 00 00 03 47 c5 61 c5 00 05 9a 38 76 80 a3 00  |  ....G.a....8v...
  0efb1160: 00 0a 08 00 45 00 05 dc 9b c9 00 00 ff 06 f8 f3  |  ....E...........
  0efb1170: 0a 07 0d 01 0a 07 00 50 00 17 cb 3d c7 e5 60 62  |  .......P...=..`b
  0efb1180: 7e 73 55 82 50 18 10 00 45 ca 00 00 2d 2d 20 49  |  ~sU.P...E...-- I
  0efb1190: 50 20 2d 2d 0d 0a 31 30 2e 37 2e 31 33 2e 31 09  |  P --..10.7.13.1.
  0efb11a0: 3d 3d 3e 09 31 30 2e 37 2e 30 2e 38 30 0d 0a 0d  |  ==>.10.7.0.80...

Summary for User "aaa", Queue "tcp_unp_c_in", Blocks 220, Queues 200
Blk_cnt Q_cnt Last_Op Queue_Type        User      Context
     21     1 put                               contexta
      1     1 put                               contexta
      1     1 put                               contexta
      1     1 put                               contextb
      1     1 put                               contextc
 First Block information for Block at 0x.....
  dup_count 0, flags 0x8000000, alloc_pc 0x43ea2a,
  start_addr 0xefb1074, read_addr 0xefb118c, write_addr 0xefb1193
  urgent_addr 0xefb118c, end_addr 0xefb17b2
  0efb1150: 00 00 00 03 47 c5 61 c5 00 05 9a 38 76 80 a3 00  |  ....G.a....8v...
  0efb1160: 00 0a 08 00 45 00 05 dc 9b c9 00 00 ff 06 f8 f3  |  ....E...........
  0efb1170: 0a 07 0d 01 0a 07 00 50 00 17 cb 3d c7 e5 60 62  |  .......P...=..`b
  0efb1180: 7e 73 55 82 50 18 10 00 45 ca 00 00 2d 2d 20 49  |  ~sU.P...E...-- I
  0efb1190: 50 20 2d 2d 0d 0a 31 30 2e 37 2e 31 33 2e 31 09  |  P --..10.7.13.1.
  0efb11a0: 3d 3d 3e 09 31 30 2e 37 2e 30 2e 38 30 0d 0a 0d  |  ==>.10.7.0.80...
...

total_count: total buffers in this class
```

The following is sample output from the **show blocks pool summary** command:

```
hostname# show blocks pool 1550 summary
Class 3, size 1550

================================================
         total_count=1531    miss_count=0
Alloc_pc        valid_cnt       invalid_cnt
0x3b0a18        00000256        00000000
         0x01ad0760 0x01acfe00 0x01acf4a0 0x01aceb40 00000000 0x00000000
```

```
0x3a8f6b        00001275        00000012
         0x05006aa0 0x05006140 0x050057e0 0x05004520 00000000
0x00000000

================================================
         total_count=9716    miss_count=0
Freed_pc        valid_cnt       invalid_cnt
0x9a81f3        00000104        00000007
         0x05006140 0x05000380 0x04fffa20 0x04ffde00 00000000 0x00000000
0x9a0326        00000053        00000033
         0x05006aa0 0x050057e0 0x05004e80 0x05003260 00000000 0x00000000
0x4605a2        00000005        00000000
         0x04ff5ac0 0x01e8e2e0 0x01e2eac0 0x01e17d20 00000000 0x00000000
...
================================================
         total_count=1531    miss_count=0
Queue   valid_cnt       invalid_cnt
0x3b0a18        00000256        00000000  Invalid Bad qtype
         0x01ad0760 0x01acfe00 0x01acf4a0 0x01aceb40 00000000 0x00000000
0x3a8f6b        00001275        00000000  Invalid Bad qtype
         0x05006aa0 0x05006140 0x050057e0 0x05004520 00000000
0x00000000

================================================
free_cnt=8185  fails=0  actual_free=8185  hash_miss=0
   03a8d3e0  03a8b7c0  03a7fc40  03a6ff20  03a6f5c0  03a6ec60 kao-f1#
```

Table 46-3 shows each field description.

Table 46-3 show blocks pool summary Fields

Field	Description
total_count	The number of blocks for a given class.
miss_count	The number of blocks not reported in the specified category due to technical reasons.
Freed_pc	The program addresses of applications that released blocks in this class.
Alloc_pc	The program addresses of applications that allocated blocks in this class.
Queue	The queues to which valid blocks in this class belong.
valid_cnt	The number of blocks that are currently allocated.
invalid_cnt	The number of blocks that are not currently allocated.
Invalid Bad qtype	Either this queue has been freed and the contents are invalid or this queue was never initialized.
Valid tcp_usr_conn_inp	The queue is valid.

Related Commands

Command	Description
blocks	Increases the memory assigned to block diagnostics
clear blocks	Clears the system buffer statistics.
show conn	Shows active connections.

show boot device (IOS)

To view the default boot partition, use the **show boot device** command.

show boot device [*mod_num*]

Syntax Description

mod_num	(Optional) Specifies the module number. Use the **show module** command to view installed modules and their numbers.

Defaults

The default boot partition is cf:4.

Command Modes

Privileged EXEC.

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

The following is sample output from the **show boot device** command that shows the boot partitions for each installed ASA on Cisco IOS software:

```
Router# show boot device
[mod:1 ]:
[mod:2 ]:
[mod:3 ]:
[mod:4 ]: cf:4
[mod:5 ]: cf:4
[mod:6 ]:
[mod:7 ]: cf:4
[mod:8 ]:
[mod:9 ]:
```

Related Commands

Command	Description
boot device (IOS)	Sets the default boot partition.
show module (IOS)	Shows all installed modules.

show bootvar

To show the boot file and configuration properties, use the **show bootvar** command in privileged EXEC mode.

show bootvar

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
9.0(1)	This command was introduced.

Usage Guidelines

The BOOT variable specifies a list of bootable images on various devices. The CONFIG_FILE variable specifies the configuration file used during system initialization. Set these variables with the **boot system** command and **boot config** command, respectively.

Examples

The BOOT variable contains disk0:/f1_image, which is the image booted when the system reloads. The current value of BOOT is disk0:/f1_image; disk0:/f1_backupimage. This value means that the BOOT variable has been modified with the **boot system** command, but the running configuration has not been saved with the **write memory** command. When the running configuration is saved, the BOOT variable and current BOOT variable will both be disk0:/f1_image; disk0:/f1_backupimage. Assuming that the running configuration is saved, the boot loader will try to load the contents of the BOOT variable, starting with disk0:/f1image, but if that is not present or invalid, the boot loader will try to boot disk0:1/f1_backupimage.

The CONFIG_FILE variable points to the system startup configuration. In this example it is not set, so the startup configuration file is the default specified with the **boot config** command. The current CONFIG_FILE variable may be modified with the **boot config** command and saved with the **write memory** command.

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

```
hostname# show bootvar
BOOT variable = disk0:/f1_image
Current BOOT variable = disk0:/f1_image; disk0:/f1_backupimage
```

```
CONFIG_FILE variable =
Current CONFIG_FILE variable =
hostname#
```

Related Commands

Command	Description
boot	Specifies the configuration file or image file used at startup.

show bridge-group

To show bridge group information such as interfaces assigned, MAC addresses, and IP addresses, use the **show bridge-group** command in privileged EXEC mode.

show bridge-group *bridge-group-number*

Syntax Description

bridge-group-number	Specifies the bridge group number as an integer between 1 and 100.

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
8.4(1)	We introduced this command.

Examples

The following is sample output from the **show bridge-group** command with IPv4 addresses:

```
hostname# show bridge-group 1
 Interfaces: GigabitEthernet0/0.101, GigabitEthernet0/0.201
 Management System IP Address: 10.0.1.1 255.255.255.0
 Management Current IP Address: 10.0.1.1 255.255.255.0
 Management IPv6 Global Unicast Address(es):
    N/A
 Static mac-address entries: 0
 Dynamic mac-address entries: 2
```

The following is sample output from the **show bridge-group** command with IPv4 and IPv6 addresses:

```
hostname# show bridge-group 1
 Interfaces: GigabitEthernet0/0.101, GigabitEthernet0/0.201
 Management System IP Address: 10.0.1.1 255.255.255.0
 Management Current IP Address: 10.0.1.1 255.255.255.0
 Management IPv6 Global Unicast Address(es):
    2000:100::1, subnet is 2000:100::/64
    2000:101::1, subnet is 2000:101::/64
    2000:102::1, subnet is 2000:102::/64
 Static mac-address entries: 0
 Dynamic mac-address entries: 2
```

Related Commands

Command	Description
bridge-group	Groups transparent firewall interfaces into a bridge group.
clear configure interface bvi	Clears the bridge group interface configuration.
interface	Configures an interface.
interface bvi	Creates a bridge virtual interface.
ip address	Sets the management IP address for a bridge group.
show running-config interface bvi	Shows the bridge group interface configuration.

show call-home

To display the configured Call Home information, use the **show call-home** command in privileged EXEC mode.

[**cluster exec**] **show call-home** [**alert-group** | **detail** | **events** | **mail-server status** | **profile** {*profile _name* | **all**} | **statistics**]

Syntax Description

alert-group	(Optional) Displays the available alert group.
cluster exec	(Optional) In a clustering environment, enables you to issue the **show call-home** command in one unit and run the command in all the other units at the same time.
detail	(Optional) Displays the Call Home configuration in detail.
events	(Optional) Displays current detected events.
mail-server status	(Optional) Displays the Call Home mail server status information.
profile *profile _name* **all**	(Optional) Displays configuration information for all existing profiles.
statistics	(Optional) Displays the Call Home statistics.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
8.2(2)	This command was introduced.
9.1(3)	A new type of Smart Call Home message has been added to include the output of the **show cluster history** command and **show cluster info** command.

Examples

The following is sample output from the **show call-home** command and displays the configured Call Home settings:

```
hostname# show call-home
Current Smart Call-Home settings:
Smart Call-Home feature : enable
Smart Call-Home message's from address: from@example.com
Smart Call-Home message's reply-to address: reply-to@example.com
contact person's email address: example@example.com
contact person's phone: 111-222-3333
street address: 1234 Any Street, Any city, Any state, 12345
customer ID: ExampleCorp
```

```
contract ID: X123456789
site ID: SantaClara
Mail-server[1]: Address: smtp.example.com Priority: 1
Mail-server[2]: Address: 192.168.0.1 Priority: 10
Rate-limit: 60 message(s) per minute
Available alert groups:
Keyword                  State
------------------------ -------
Syslog Enable
diagnostic Enable
environmental Enable
inventory Enable
configuration Enable
firewall Enable
troubleshooting Enable
report Enable
Profiles:
Profile Name: CiscoTAC-1
Profile Name: prof1
Profile Name: prof2
```

The following is sample output from the **show call-home detail** command and displays detailed Call Home configuration information:

```
hostname# show call-home detail
Description: Show smart call-home configuration in detail.
Supported Modes: single mode and system context in multi mode, routed/transparent.
Output:
Current Smart Call-Home settings:
Smart Call-Home feature : enable
Smart Call-Home message's from address: from@example.example.com
Smart Call-Home message's reply-to address: reply-to@example.example.com
contact person's email address: abc@example.com
contact person's phone: 111-222-3333
street address: 1234 Any Street, Any city, Any state, 12345
customer ID: 111111
contract ID: 123123
site ID: SantaClara
Mail-server[1]: Address: example.example.com Priority: 1
Mail-server[2]: Address: example.example.com Priority: 10
Rate-limit: 60 message(s) per minute
Available alert groups:
Keyword State
------------------------ -------
syslog Enable
diagnostic Enable
environmental Enable
inventory Enable
configuration Enable
firewall Enable
troubleshooting Enable
report Enable
Profiles:
Profile Name: CiscoTAC-1
Profile status: ACTIVE Preferred Message Format: xml
Message Size Limit: 3145728 Bytes
Email address(es): anstage@cisco.com
HTTP address(es): https://tools.cisco.com/its/service/oddce/services/DDCEService
Periodic inventory message is scheduled monthly at 01:00
Alert-group Severity
------------------------ ------------
inventory n/a
```

```
Profile Name: prof1
Profile status: ACTIVE Preferred Message Format: xml
Message Size Limit: 3145728 Bytes
Email address(es): example@example.com
HTTP address(es): https://kafan-lnx-01.cisco.com:8443/sch/sch.jsp
Periodic configuration message is scheduled daily at 01:00
Periodic inventory message is scheduled every 60 minutes
Alert-group Severity
------------------------ ------------
configuration n/a
inventory n/a
Profile Name: prof2
Profile status: ACTIVE Preferred Message Format: short-text
Message Size Limit: 1048576 Bytes
Email address(es): example@example.com
HTTP address(es): https://example.example.com:8443/sch/sch.jsp
Periodic configuration message is scheduled every 1 minutes
Periodic inventory message is scheduled every 1 minutes
Alert-group Severity
------------------------ ------------
configuration n/a
inventory n/a
```

The following is sample output from the **show call-home events** command and displays available Call Home events:

```
hostname# show call-home events
Description: Show current detected events.
Supported Modes: single mode and system context in multi mode, routed/transparent.
Output:
Active event list:
Event client alert-group severity active (sec)
-------------------------------------------------------------------
Configuration Client configuration none 5
Inventory inventory none 15
```

The following is sample output from the **show call-home mail-server status** command and displays available Call Home mail-server status:

```
hostname# show call-home mail-server status
Description: Show smart call-home configuration, status, and statistics.
Supported Modes: single mode and system context in multi mode, routed/transparent.
Output:
Mail-server[1]: Address: example.example.com Priority: 1 [Available]
Mail-server[2]: Address: example.example.com Priority: 10 [Not Available]
```

The following is sample output from the **show call-home alert-group** comand and displays the available alert groups:

```
hostname# show call-home alert-group
Description: Show smart call-home alert-group states.
Supported Modes: single mode and system context in multi mode, routed/transparent.
Output:
Available alert groups:
Keyword State
------------------------ -------
syslog Enable
diagnostic Enable
environmental Enable
inventory Enable
configuration Enable
firewall Enable
troubleshooting Enable
report Enable
```

The following is sample output from the **show call-home profile profile-name | all** command and displays information for all predefined and user-defined profiles:

```
hostname# show call-home profile {profile-name | all}
Description: Show smart call-home profile configuration.
Supported Modes: single mode and system context in multi mode, routed/transparent.
Output:
Profiles:
Profile Name: CiscoTAC-1
Profile status: ACTIVE Preferred Message Format: xml
Message Size Limit: 3145728 Bytes
Email address(es): anstage@cisco.com
HTTP address(es): https://tools.cisco.com/its/service/oddce/services/DDCEService
Periodic inventory message is scheduled monthly at 01:00
Alert-group Severity
------------------------ ------------
inventory n/a
Profile Name: prof1
Profile status: ACTIVE Preferred Message Format: xml
Message Size Limit: 3145728 Bytes
Email address(es): example@example.com
HTTP address(es): https://example.example.com:8443/sch/sch.jsp
Periodic configuration message is scheduled daily at 01:00
Periodic inventory message is scheduled every 60 minutes
Alert-group Severity
------------------------ ------------
configuration n/a
inventory n/a
Profile Name: prof2
Profile status: ACTIVE Preferred Message Format: short-text
Message Size Limit: 1048576 Bytes
Email address(es): example@example.com
HTTP address(es): https://example.example.com:8443/sch/sch.jsp
Periodic configuration message is scheduled every 1 minutes
Periodic inventory message is scheduled every 1 minutes
Alert-group Severity
------------------------ ------------
configuration n/a
inventory n/a
```

The following is sample output from the **show call-home statistics** command and displays the call-home statistics:

```
hostname# show call-home statistics
Description: Show smart call-home statistics.
Supported Modes: single mode and system context in multi mode, routed/transparent.
Output:
Message Types Total Email HTTP
-------------------- ---------------- ---------------- ----------------
Total Success 0 0 0
Total In-Queue 0 0 0
Total Dropped 5 4 1
Tx Failed 5 4 1
inventory 3 2 1
configuration 2 2 0
Event Types Total
-------------------- ----------------
Total Detected 2
inventory 1
configuration 1
Total In-Queue 0
Total Dropped 0
Last call-home message sent time: 2009-06-17 14:22:09 GMT-07:00
```

The following is sample output from the **show call-home status** command and displays the call-home status:

```
hostname# show call-home mail-server status
Description: Show smart call-home configuration, status, and statistics.
Supported Modes: single mode and system context in multi mode, routed/transparent.
Output:
Mail-server[1]: Address: kafan-lnx-01.cisco.com Priority: 1 [Available]
Mail-server[2]: Address: kafan-lnx-02.cisco.com Priority: 10 [Not Available]

37. ciscoasa# show call-home events
Description: Show current detected events.
Supported Modes: single mode and system context in multi mode, routed/transparent.
Output:
Active event list:
Event client alert-group severity active (sec)
-------------------------------------------------------------------
Configuration Client configuration none 5
Inventory inventory none 15
```

The following is sample output from the **cluster exec show call-home statistics** command and displays call-home statistics for a cluster:

```
hostname(config)# cluster exec show call-home statistics
A(LOCAL):*************************************************************
Message Types           Total             Email             HTTP
--------------------   ---------------- ---------------- ----------------
       Total Success                  3                3                0
                test                  3                3                0

 Total In-Delivering                  0                0                0

      Total In-Queue                  0                0                0

Total Dropped                         8                8                0
           Tx Failed                  8                8                0
        configuration                 2                2                0
                test                  6                6                0


Event Types             Total
--------------------   ----------------
      Total Detected                10
       configuration                 1
                test                 9

 Total In-Processing                 0

      Total In-Queue                 0

Total Dropped                        0

Last call-home message sent time: 2013-04-15 05:37:16 GMT+00:00

B:*************************************************************
Message Types           Total             Email             HTTP
--------------------   ---------------- ---------------- ----------------
       Total Success                  1                1                0
                test                  1                1                0

 Total In-Delivering                  0                0                0
```

```
      Total In-Queue                  0                0                0

Total Dropped                         2                2                0
           Tx Failed                  2                2                0
       configuration                  2                2                0

Event Types             Total
--------------------   ----------------
      Total Detected                  2
       configuration                  1
                test                  1

 Total In-Processing                  0

      Total In-Queue                  0

Total Dropped                         0

Last call-home message sent time: 2013-04-15 05:36:16 GMT+00:00

C:**********************************************************************
Message Types           Total            Email             HTTP
--------------------   ---------------- ---------------- ----------------
       Total Success                  0                0                0

 Total In-Delivering                  0                0                0

      Total In-Queue                  0                0                0

Total Dropped                         2                2                0
           Tx Failed                  2                2                0
       configuration                  2                2                0

Event Types             Total
--------------------   ----------------
      Total Detected                  1
       configuration                  1

 Total In-Processing                  0

      Total In-Queue                  0

Total Dropped                         0

Last call-home message sent time: n/a

D:**********************************************************************
Message Types           Total            Email             HTTP
--------------------   ---------------- ---------------- ----------------
       Total Success                  1                1                0
                test                  1                1                0

 Total In-Delivering                  0                0                0

      Total In-Queue                  0                0                0

Total Dropped                         2                2                0
           Tx Failed                  2                2                0
       configuration                  2                2                0

Event Types             Total
--------------------   ----------------
      Total Detected                  2
       configuration                  1
```

```
                test                    1
 Total In-Processing                    0
      Total In-Queue                    0
Total Dropped                           0
Last call-home message sent time: 2013-04-15 05:35:34 GMT+00:00
hostname(config)#
```

Related Commands

Command	Description
call-home	Enters call home configuration mode.
call-home send alert-group	Sends a specific alert group message.
service call-home	Enables or disables Call Home.

show call-home registered-module status

To display the registered module status, use the **show call-home registered-module status** command in privileged EXEC mode.

show call-home registered-module status [**all**]

Note The [**all**] option is only valid in system context mode.

Syntax Description

all	Displays module status based on the device, not per context. In multiple context mode, if a module is enabled in at least one context, it is displayed as enabled if the "**all**" option is included.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
8.2(2)	This command was introduced.

Examples

The following example displays the **show call-home registered-module status all** output:

```
Output:
Module Name Status
---------------------------------------- --------------------
Smart Call-Home enabled
Failover Standby/Active
```

Related Commands

Command	Description
call-home	Enters call-home configuration mode.
call-home send alert-group	Sends a specific alert group message.
service call-home	Enables or disables Call Home.

show capture

To display the capture configuration when no options are specified, use the **show capture** command in privileged EXEC mode.

[**cluster exec**] **show capture** [*capture_name*] [**access-list** *access_list_name*] [**count** *number*] [**decode**] [**detail**] [**dump**] [**packet-number** *number*]

Syntax Description

access-list *access_list_name*	(Optional) Displays information for packets that are based on IP or higher fields for the specific access list identification.
capture_name	(Optional) Specifies the name of the packet capture.
cluster exec	(Optional) In a clustering environment, enables you to issue the **show capture** command in one unit and run the command in all the other units at the same time.
count *number*	(Optional) Displays the number of packets specified data.
decode	This option is useful when a capture of type isakmp is applied to an interface. All ISAKMP data flowing through that interface will be captured after decryption and shown with more information after decoding the fields.
detail	(Optional) Displays additional protocol information for each packet.
dump	(Optional) Displays a hexadecimal dump of the packets that are transported over the data link.
packet-number *number*	Starts the display at the specified packet number.

Defaults

This command has no default settings.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.
8.4(2)	Added detailed information in the output for IDS.
9.0(1)	The **cluster exec** option was added.

Usage Guidelines

If you specify the *capture_name*, then the capture buffer contents for that capture are displayed.

The **dump** keyword does not display MAC information in the hexadecimal dump.

The decoded output of the packets depend on the protocol of the packet. In Table 46-4, the bracketed output is displayed when you specify the **detail** keyword.

Table 46-4 Packet Capture Output Formats

Packet Type	Capture Output Format
802.1Q	*HH:MM:SS.ms* [ether-hdr] *VLAN-info encap-ether-packet*
ARP	*HH:MM:SS.ms* [ether-hdr] *arp-type arp-info*
IP/ICMP	*HH:MM:SS.ms* [ether-hdr] *ip-source* > *ip-destination:* icmp: *icmp-type icmp-code* [checksum-failure]
IP/UDP	*HH:MM:SS.ms* [ether-hdr] *src-addr.src-port dest-addr.dst-port*: [checksum-info] udp *payload-len*
IP/TCP	*HH:MM:SS.ms* [ether-hdr] *src-addr.src-port* d*est-addr.dst-port*: *tcp-flags* [header-check] [checksum-info] *sequence-number ack-number tcp-window urgent-info tcp-options*
IP/Other	*HH:MM:SS.ms* [ether-hdr] *src-addr dest-addr*: *ip-protocol ip-length*
Other	*HH:MM:SS.ms ether-hdr*: *hex-dump*

Examples

This example shows how to display the capture configuration:

```
hostname(config)# show capture
capture arp ethernet-type arp interface outside
capture http access-list http packet-length 74 interface inside
```

This example shows how to display the packets that are captured by an ARP capture:

```
hostname(config)# show capture arp
2 packets captured
19:12:23.478429 arp who-has 171.69.38.89 tell 171.69.38.10
19:12:26.784294 arp who-has 171.69.38.89 tell 171.69.38.10
2 packets shown
```

The following example shows how to display the packets that are captured on a single unit in a clustering environment:

```
hostname(config)# show capture
capture 1 cluster type raw-data interface primary interface cluster [Buffer Full - 524187
bytes]
capture 2 type raw-data interface cluster [Capturing - 232354 bytes]
```

The following example shows how to display the packets that are captured on all units in a clustering environment:

```
hostname(config)# cluster exec show capture
mycapture (LOCAL):------------------------------------------------------------

capture 1 type raw-data interface primary [Buffer Full - 524187 bytes]
capture 2 type raw-data interface cluster [Capturing - 232354 bytes]

yourcapture:------------------------------------------------------------------
capture 1 type raw-data interface primary [Capturing - 191484 bytes]
capture 2 type raw-data interface cluster [Capturing - 532354 bytes]
```

The following example shows the packets that are captured on the cluster control link in a clustering environment after the following commands are entered:

```
hostname (config)# capture a interface cluster
hostname (config)# capture cp interface cluster match udp any eq 49495 any
hostname (config)# capture cp interface cluster match udp any any eq 49495
hostname (config)# access-list cc1 extended permit udp any any eq 4193
hostname (config)# access-list cc1 extended permit udp any eq 4193 any
hostname (config)# capture dp interface cluster access-list cc1
hostname (config)# capture lacp type lacp interface gigabitEthernet 0/0

hostname(config)# show capture
capture a type raw-data interface cluster [Capturing - 970 bytes]
capture cp type raw-data interface cluster [Capturing - 26236 bytes]
  match udp any eq 49495 any
capture dp type raw-data access-list cc1 interface cluster [Capturing - 4545230 bytes]
capture lacp type lacp interface gigabitEthernet0/0 [Capturing - 140 bytes]
```

Related Commands

Command	Description
capture	Enables packet capture capabilities for packet sniffing and network fault isolation.
clear capture	Clears the capture buffer.
copy capture	Copies a capture file to a server.

show chardrop

To display the count of characters dropped from the serial console, use the **show chardrop** command in privileged EXEC mode.

show chardrop

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
9.0(1)	This command was introduced.

Examples

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

```
hostname# show chardrop
Chars dropped pre-TxTimeouts: 0, post-TxTimeouts: 0
```

Related Commands

Command	Description
show running-config	Shows the current operating configuration.

show checkheaps

To show the checkheaps statistics, use the **show checkheaps** command in privileged EXEC mode. Checkheaps is a periodic process that verifies the sanity of the heap memory buffers (dynamic memory is allocated from the system heap memory region) and the integrity of the code region.

show checkheaps

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

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

```
hostname# show checkheaps

Checkheaps stats from buffer validation runs
--------------------------------------------
Time elapsed since last run     : 42 secs
Duration of last run            : 0 millisecs
Number of buffers created       : 8082
Number of buffers allocated     : 7808
Number of buffers free          : 274
Total memory in use             : 43570344 bytes
Total memory in free buffers    : 87000 bytes
Total number of runs            : 310
```

Related Commands

Command	Description
checkheaps	Sets the checkheap verification intervals.

show checksum

To display the configuration checksum, use the **show checksum** command in privileged EXEC mode.

show checksum

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

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

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

Command History

Release	Modification
9.0(1)	We introduced this command.

Usage Guidelines

The **show checksum** command allows you to display four groups of hexadecimal numbers that act as a digital summary of the configuration contents. This checksum is calculated only when you store the configuration in flash memory.

If a dot (“.”) appears before the checksum in the **show config** or **show checksum** command output, the output indicates a normal configuration load or write mode indicator (when loading from or writing to the ASA flash partition). The “.” shows that the ASA is preoccupied with the operation but is not “hung up.” This message is similar to a “system processing, please wait” message.

Examples

This example shows how to display the configuration or the checksum:

```
hostname(config)# show checksum
Cryptochecksum: 1a2833c0 129ac70b 1a88df85 650dbb81
```

show chunkstat

To display the chunk statistics, use the **show chunkstat** command in privileged EXEC mode.

show chunkstat

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

This example shows how to display the chunk statistics:

```
hostname# show chunkstat
Global chunk statistics: created 181, destroyed 34, siblings created 94, siblings
destroyed 34

Per-chunk statistics: siblings created 0, siblings trimmed 0
Dump of chunk at 01edb4cc, name "Managed Chunk Queue Elements", data start @ 01edbd24, end
@ 01eddc54
next: 01eddc8c, next_sibling: 00000000, prev_sibling: 00000000
flags 00000001
maximum chunk elt's: 499, elt size: 16, index first free 498
# chunks in use: 1, HWM of total used: 1, alignment: 0
Per-chunk statistics: siblings created 0, siblings trimmed 0
Dump of chunk at 01eddc8c, name "Registry Function List", data start @ 01eddea4, end @
01ede348
next: 01ede37c, next_sibling: 00000000, prev_sibling: 00000000
flags 00000001
maximum chunk elt's: 99, elt size: 12, index first free 42
# chunks in use: 57, HWM of total used: 57, alignment: 0
```

Related Commands

Command	Description
show counters	Displays the protocol stack counters.
show cpu	Displays the CPU utilization information.

show class

To show the contexts assigned to a class, use the **show class** command in privileged EXEC mode.

show class *name*

Syntax Description

name	Specifies the name as a string up to 20 characters long. To show the default class, enter **default** for the name.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.2(1)	This command was introduced.

Examples

The following is sample output from the **show class default** command:

```
hostname# show class default

Class Name           Members    ID   Flags
default                All       1    0001
```

Related Commands

Command	Description
class	Configures a resource class.
clear configure class	Clears the class configuration.
context	Configures a security context.
limit-resource	Sets the resource limit for a class.
member	Assigns a context to a resource class.

show clock

To view the time on the ASA, use the **show clock** command in user EXEC mode.

show clock [**detail**]

Syntax Description

detail	(Optional) Indicates the clock source (NTP or user configuration) and the current summer-time setting (if any).

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

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

```
hostname> show clock
12:35:45.205 EDT Tue Jul 27 2004
```

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

```
hostname> show clock detail
12:35:45.205 EDT Tue Jul 27 2004
Time source is user configuration
Summer time starts 02:00:00 EST Sun Apr 4 2004
Summer time ends 02:00:00 EDT Sun Oct 31 2004
```

Related Commands

Command	Description
clock set	Manually sets the clock on the ASA.
clock summer-time	Sets the date range to show daylight saving time.
clock timezone	Sets the time zone.
ntp server	Identifies an NTP server.
show ntp status	Shows the status of the NTP association.

show cluster

To view aggregated data for the entire cluster or other information, use the **show cluster** command in privileged EXEC mode.

show cluster {**access-list** [*acl_name*] | **conn** [**count**] | **cpu** [**usage**] | **history** | **interface-mode** | **memory** | **resource usage** | **traffic** | **xlate count**}

Syntax Description

access-list [*acl_name*]	Shows hit counters for access policies. To see the counters for a specific ACL, enter the *acl_name*.
conn [**count**]	Shows the aggregated count of in-use connections for all units. If you enter the **count** keyword, only the connection count is shown.
cpu [**usage**]	Shows CPU usage information.
history	Shows cluster switching history.
interface-mode	Shows the cluster interface mode, either spanned or individual.
memory	Shows system memory utilization and other information.
resource usage	Shows system resources and usage.
traffic	Shows traffic statistics.
xlate count	Shows current translation information.

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
9.0(1)	We introduced this command.

Usage Guidelines

See also the **show cluster info** and **show cluster user-identity** commands.

Examples

The following is sample output from the **show cluster access-list** command:

```
hostname#  show cluster access-list
hitcnt display order: cluster-wide aggregated result, unit-A, unit-B,  unit-C, unit-D
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096) alert-interval
300
access-list 101; 122 elements; name hash: 0xe7d586b5
```

```
access-list 101 line 1 extended permit tcp 192.168.143.0 255.255.255.0 any eq www
(hitcnt=0, 0, 0, 0, 0) 0x207a2b7d
access-list 101 line 2 extended permit tcp any 192.168.143.0 255.255.255.0 (hitcnt=0, 0,
0, 0, 0) 0xfe4f4947
access-list  101 line 3 extended permit tcp host 192.168.1.183 host 192.168.43.238
(hitcnt=1, 0, 0, 0, 1) 0x7b521307
access-list 101 line 4 extended permit tcp host 192.168.1.116 host 192.168.43.238
(hitcnt=0, 0, 0, 0, 0) 0x5795c069
access-list 101 line 5 extended permit tcp host 192.168.1.177 host 192.168.43.238
(hitcnt=1, 0, 0, 1, 0) 0x51bde7ee
access list 101 line 6 extended permit tcp host 192.168.1.177 host 192.168.43.13
(hitcnt=0, 0, 0, 0, 0) 0x1e68697c
access-list 101 line 7 extended permit tcp host 192.168.1.177 host 192.168.43.132
(hitcnt=2, 0, 0, 1, 1) 0xc1ce5c49
access-list 101 line 8 extended permit tcp host 192.168.1.177 host 192.168.43.192
(hitcnt=3, 0, 1, 1, 1) 0xb6f59512
access-list 101 line 9 extended permit tcp host 192.168.1.177 host 192.168.43.44
(hitcnt=0, 0, 0, 0, 0) 0xdc104200
access-list 101 line 10 extended permit tcp host 192.168.1.112 host 192.168.43.44
(hitcnt=429, 109, 107, 109, 104)
0xce4f281d
access-list 101 line 11 extended permit tcp host 192.168.1.170 host 192.168.43.238
(hitcnt=3, 1, 0, 0, 2) 0x4143a818
access-list 101 line 12 extended permit tcp host 192.168.1.170 host 192.168.43.169
(hitcnt=2, 0, 1, 0, 1) 0xb18dfea4
access-list 101 line 13 extended permit tcp host 192.168.1.170 host 192.168.43.229
(hitcnt=1, 1, 0, 0, 0) 0x21557d71
access-list 101 line 14 extended permit tcp host 192.168.1.170 host 192.168.43.106
(hitcnt=0, 0, 0, 0, 0) 0x7316e016
access-list 101 line 15 extended permit tcp host 192.168.1.170 host 192.168.43.196
(hitcnt=0, 0, 0, 0, 0) 0x013fd5b8
access-list 101 line 16 extended permit tcp host 192.168.1.170 host 192.168.43.75
(hitcnt=0, 0, 0, 0, 0) 0x2c7dba0d
```

To display the aggregated count of in-use connections for all units, enter:

```
hostname# show cluster conn count
Usage Summary In Cluster:*********************************************
  200 in use (cluster-wide aggregated)
     cl2(LOCAL):*************************************************************
  100 in use, 100 most used

  cl1:*************************************************************
  100 in use, 100 most used
```

Related Commands

Command	Description
show cluster info	Shows cluster information.
show cluster user-identity	Shows cluster user identity information and statistics.

show cluster info

To view cluster information, use the **show cluster info** command in privileged EXEC mode.

show cluster info [**clients | conn-distribution | goid** [*options*] **| health | incompatible-config | loadbalance | old-members | packet-distribution | trace** [*options*] **| transport {asp | cp}**]

Syntax Description

clients	(Optional) Shows the version of register clients.
conn-distribution	(Optional) Shows the connection distribution in the cluster.
goid [*options*]	(Optional) Shows the global object ID database. Options include: • **classmap** • **conn-set** • **hwidb** • **idfw-domain** • **idfw-group** • **interface** • **policymap** • **virtual-context**
health	(Optional) Shows health monitoring information.
incompatible-config	(Optional) Shows commands that are incompatible with clustering in the current running configuration. This command is useful before you enable clustering.
loadbalance	(Optional) Shows load balancing information.
old-members	(Optional) Shows former members of the cluster.
packet-distribution	(Optional) Shows packet distribution in the cluster.
trace [*options*]	(Optional) Shows the clustering control module event trace. Options include: • **latest** [*number*]—Displays the latest *number* events, where the number is from 1 to 2147483647. The default is to show all. • **level** *level*—Filters events by level where the *level* is one of the following: **all**, **critical**, **debug**, **informational**, or **warning**. • **module** *module*—Filters events by module where the *module* is one of the following: **ccp**, **datapath**, **fsm**, **general**, **hc**, **license**, **rpc**, **or transport**. • **time** {[*month day*] [*hh*:*mm*:*ss*]}—Shows events before the specified time or date.
transport {asp | cp}	(Optional) Show transport related statistics for the following: • **asp**—Data plane transport statistics. • **cp**—Control plane transport statistics.

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	•	•	•	—	•

Command History

Release	Modification
9.0(1)	We introduced this command.

Usage Guidelines

If you do not specify any options, the **show cluster info** command shows general cluster information including the cluster name and status, the cluster members, the member states, and so on.

Clear statistics using the **clear cluster info** command.

See also the **show cluster** and **show cluster user-identity** commands.

Examples

The following is sample output from the **show cluster info** command:

```
hostname# show cluster info
Cluster stbu: On
  This is "C" in state SLAVE
      ID        : 0
      Version   : 100.8(0.52)
      Serial No.: P3000000025
      CCL IP    : 10.0.0.3
      CCL MAC   : 000b.fcf8.c192
      Last join : 17:08:59 UTC Sep 26 2011
      Last leave: N/A
Other members in the cluster:
  Unit "D" in state SLAVE
      ID        : 1
      Version   : 100.8(0.52)
      Serial No.: P3000000001
      CCL IP    : 10.0.0.4
      CCL MAC   : 000b.fcf8.c162
      Last join : 19:13:11 UTC Sep 23 2011
      Last leave: N/A
  Unit "A" in state MASTER
      ID        : 2
      Version   : 100.8(0.52)
      Serial No.: JAB0815R0JY
      CCL IP    : 10.0.0.1
      CCL MAC   : 000f.f775.541e
      Last join : 19:13:20 UTC Sep 23 2011
      Last leave: N/A
  Unit "B" in state SLAVE
      ID        : 3
      Version   : 100.8(0.52)
      Serial No.: P3000000191
      CCL IP    : 10.0.0.2
      CCL MAC   : 000b.fcf8.c61e
      Last join : 19:13:50 UTC Sep 23 2011
      Last leave: 19:13:36 UTC Sep 23 2011
```

The following is sample output from the **show cluster info incompatible-config** command:

```
hostname(cfg-cluster)# show cluster info incompatible-config
INFO: Clustering is not compatible with following commands which given a user's
confirmation upon enabling clustering, can be removed automatically from running-config.
policy-map global_policy
 class scansafe-http
  inspect scansafe http-map fail-close
policy-map global_policy
 class scansafe-https
  inspect scansafe https-map fail-close

INFO: No manually-correctable incompatible configuration is found.
```

The following is sample output from the **show cluster info trace** command:

```
hostname# show cluster info trace
 Feb 02 14:19:47.456 [DBUG]Receive CCP message: CCP_MSG_LOAD_BALANCE
 Feb 02 14:19:47.456 [DBUG]Receive CCP message: CCP_MSG_LOAD_BALANCE
 Feb 02 14:19:47.456 [DBUG]Send CCP message to all: CCP_MSG_KEEPALIVE from 80-1 at MASTER
```

Related Commands

Command	Description
show cluster	Displays aggregated data for the entire cluster.
show cluster user-identity	Shows cluster user identity information and statistics.

show cluster user-identity

To view cluster-wide user identity information and statistics, use the **show cluster user-identity** command in privileged EXEC mode.

show cluster user-identity {**statistics** [**user** *name* | **user-group** *group_name*] | **user** [**active** [**domain** *name*] | **user** *name* | **user-group** *group_name*] [**list** [*detail*] | **all** [**list** [*detail*] | **inactive** {**domain** *name* | **user-group** *group_name*] [**list** [*detail*]]}

Syntax Description

active	Shows users with active IP-user mappings.
all	Shows all users in the user database.
domain *name*	Shows user info for a domain.
inactive	Shows users with inactive IP-user mappings.
list [*detail*]	Shows a list of users.
statistics	Shows cluster user identity statistics.
user	Shows the user database.
user *name*	Show information for a specific user.
user-group *group_name*	Shows information for each user of a specific group.

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
9.0(1)	We introduced this command.

Usage Guidelines

See also the **show cluster info** and **show cluster** commands.

Related Commands

Command	Description
show cluster	Displays aggregated data for the entire cluster.
show cluster info	Shows cluster information.

show compression svc

To view compression statistics for SVC connections on the ASA, use the **show compression svc** command from privileged EXEC mode.

show compression svc

Defaults

There is no default behavior for this command.

Command Modes

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

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

Command History

Release	Modification
7.1(1)	This command was introduced.

Examples

The following example shows the output of the **show compression svc** command:

```
hostname# show compression svc
Compression SVC Sessions                    1
Compressed Frames                      249756
Compressed Data In (bytes)            0048042
Compressed Data Out (bytes)           4859704
Expanded Frames                             1
Compression Errors                          0
Compression Resets                          0
Compression Output Buf Too Small            0
Compression Ratio                        2.06
Decompressed Frames                    876687
Decompressed Data In                279300233
```

Related Commands

Command	Description
compression	Enables compression for all SVC and WebVPN connections.
svc compression	Enables compression of http data over an SVC connection for a specific group or user.

show configuration

To display the configuration that is saved in flash memory on the ASA, use the **show configuration** command in privileged EXEC mode.

show configuration

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was modified.

Usage Guidelines

The **show configuration** command displays the saved configuration in flash memory on the ASA. Unlike the **show running-config** command, the **show configuration** command does not use many CPU resources to run.

To display the active configuration in memory (including saved configuration changes) on the ASA, use the **show running-config** command.

Examples

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

```
hostname# show configuration
: enable password 8Ry2YjIyt7RRXU24 encrypted
names
dns-guard
!
interface Ethernet0/0
 nameif inside
 security-level 100
 ip address 192.168.2.5 255.255.255.0
!
interface Ethernet0/1
 nameif outside
 security-level 0
 ip address 10.132.12.6 255.255.255.0
!
interface Ethernet0/2
 nameif dmz
```

```
 security-level 50
 ip address 10.0.0.5 255.255.0.0
!
interface Ethernet0/3
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Management0/0
 nameif management
 security-level 100
 ip address 192.168.1.1 255.255.255.0
 management-only
!
passwd 2KFQnbNIdI.2KYOU encrypted
boot system disk0:/newImage
ftp mode passive
access-list acl1 extended permit ip any any
access-list mgcpacl extended permit udp any any eq 2727
access-list mgcpacl extended permit udp any any eq 2427
access-list mgcpacl extended permit udp any any eq tftp
access-list mgcpacl extended permit udp any any eq 1719
access-list permitIp extended permit ip any any
pager lines 25
logging enable
logging console debugging
logging buffered debugging
logging asdm informational
mtu inside 1500
mtu outside 1500
mtu dmz 1500
mtu management 1500
icmp unreachable rate-limit 1 burst-size 1
icmp permit any inside
icmp permit any outside
icmp permit any dmz
asdm image disk0:/pdm
no asdm history enable
arp timeout 14400
global (outside) 1 10.132.12.50-10.132.12.52
global (outside) 1 interface
global (dmz) 1 interface
nat (inside) 1 0.0.0.0 0.0.0.0
access-group permitIp in interface inside
access-group permitIp in interface outside
access-group mgcpacl in interface dmz
!
router ospf 1
 network 10.0.0.0 255.255.0.0 area 192.168.2.0
 network 192.168.2.0 255.255.255.0 area 192.168.2.0
 log-adj-changes
 redistribute static subnets
 default-information originate
!
route outside 0.0.0.0 0.0.0.0 10.132.12.1 1
route outside 10.129.0.0 255.255.0.0 10.132.12.1 1
route outside 88.0.0.0 255.0.0.0 10.132.12.1 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout uauth 0:05:00 absolute
dynamic-access-policy-record DfltAccessPolicy
```

```
aaa authentication ssh console LOCAL
http server enable
http 10.132.12.0 255.255.255.0 outside
http 192.168.2.0 255.255.255.0 inside
http 192.168.1.0 255.255.255.0 management
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart
telnet 192.168.2.0 255.255.255.0 inside
telnet 10.132.12.0 255.255.255.0 outside
telnet timeout 5
ssh 192.168.2.0 255.255.255.0 inside
ssh timeout 5
console timeout 0
dhcpd address 192.168.1.2-192.168.1.254 management
dhcpd enable management
!
threat-detection basic-threat
threat-detection statistics access-list
!
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum 512
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect rsh
  inspect rtsp
  inspect esmtp
  inspect sqlnet
  inspect skinny
  inspect sunrpc
  inspect xdmcp
  inspect sip
  inspect netbios
  inspect tftp
  inspect mgcp
policy-map type inspect mgcp mgcpapp
 parameters
  call-agent 150.0.0.210 101
  gateway 50.0.0.201 101
  gateway 100.0.0.201 101
  command-queue 150
!
service-policy global_policy global
webvpn
 memory-size percent 25
 enable inside
 internal-password enable
 onscreen-keyboard logon
username snoopy password /JcYsjvxHfBHc4ZK encrypted
prompt hostname context
Cryptochecksum:62bf8f5de9466cdb64fe758079594635:
end
```

Related Commands

Command	Description
configure	Configures the ASA from the terminal.

show conn

To display the connection state for the designated connection type, use the **show conn** command in privileged EXEC mode. This command supports IPv4 and IPv6 addresses.

show conn [**count** | [**all**] [**detail**] [**long**] [**state** *state_type*] [**protocol** {**tcp** | **udp**}] [**scansafe**]
[**address** *src_ip*[**-***src_ip*] [**netmask** *mask*]] [**port** *src_port*[**-***src_port*]]
[**address** *dest_ip*[**-***dest_ip*] [**netmask** *mask*]] [**port** *dest_port*[**-***dest_port*]]
[**user-identity** | **user** [*domain_nickname*\]*user_name* | **user-group**
[*domain_nickname*\\]*user_group_name*] | **security-group**]

Syntax Description

address	(Optional) Displays connections with the specified source or destination IP address.
all	(Optional) Displays connections that are to the device or from the device, in addition to through-traffic connections.
count	(Optional) Displays the number of active connections.
dest_ip	(Optional) Specifies the destination IP address (IPv4 or IPv6). To specify a range, separate the IP addresses with a dash (-). For example: `10.1.1.1-10.1.1.5`
dest_port	(Optional) Specifies the destination port number. To specify a range, separate the port numbers with a dash (-). For example: `1000-2000`
detail	(Optional) Displays connections in detail, including translation type and interface information.
long	(Optional) Displays connections in long format.
netmask *mask*	(Optional) Specifies a subnet mask for use with the given IP address.
port	(Optional) Displays connections with the specified source or destination port.
protocol {**tcp** | **udp**}	(Optional) Specifies the connection protocol, which can be **tcp** or **udp**.
scansafe	(Optional) Shows connections being forwarded to the Cloud Web Security server.
security-group	(Optional) Specifies that all connections displayed belong to the specified security group.
src_ip	(Optional) Specifies the source IP address (IPv4 or IPv6). To specify a range, separate the IP addresses with a dash (-). For example: `10.1.1.1-10.1.1.5`
src_port	(Optional) Specifies the source port number. To specify a range, separate the port numbers with a dash (-). For example: `1000-2000`
state *state_type*	(Optional) Specifies the connection state type. See Table 46-5 for a list of the keywords available for connection state types.
user [*domain_nickname*\] *user_name*	(Optional) Specifies that all connections displayed belong to the specified user. When you do not include the *domain_nickname* argument, the ASA displays information for the user in the default domain.

user-group [*domain_nickname*\\] *user_group_name*	(Optional) Specifies that all connections displayed belong to the specified user group. When you do not include the *domain_nickname* argument, the ASA displays information for the user group in the default domain.
user-identity	(Optional) Specifies that the ASA display all connections for the Identity Firewall feature. When displaying the connections, the ASA displays the user name and IP address when it identifies a matching user. Similarly, the ASA displays the host name and an IP address when it identifies a matching host.

Defaults

All through connections are shown by default. You need to use the **all** keyword to also view management connections to the device.

Command Modes

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

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

Command History

Release	Modification
7.0(8)/7.2(4)/8.0(4)	The syntax was simplified to use source and destination concepts instead of “local” and “foreign.” In the new syntax, the source address is the first address entered and the destination is the second address. The old syntax used keywords like **foreign** and **fport** to determine the destination address and port.
7.2(5)/8.0(5)/8.1(2)/8.2(4)/ 8.3(2)	The **tcp_embryonic** state type was added. This type shows all TCP connections with the i flag (incomplete connections); i flag connections for UDP are not shown.
8.2(1)	The b flag was added for TCP state bypass.
8.4(2)	Added the **user-identity**, **user**, and **user-group** keywords to support the Identity Firewall.
9.0(1)	Support for clustering was added. We added the **scansafe** and **security-group** keywords.

Usage Guidelines

The **show conn** command displays the number of active TCP and UDP connections, and provides information about connections of various types. Use the **show conn all** command to see the entire table of connections.

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

The connection types that you can specify using the **show conn state** command are defined in Table 46-5. When specifying multiple connection types, use commas without spaces to separate the keywords.

Table 46-5 Connection State Types

Keyword	Connection Type Displayed
up	Connections in the up state.
conn_inbound	Inbound connections.
ctiqbe	CTIQBE connections
data_in	Inbound data connections.
data_out	Outbound data connections.
finin	FIN inbound connections.
finout	FIN outbound connections.
h225	H.225 connections
h323	H.323 connections
http_get	HTTP get connections.
mgcp	MGCP connections.
nojava	Connections that deny access to Java applets.
rpc	RPC connections.
service_module	Connections being scanned by an SSM.
sip	SIP connections.
skinny	SCCP connections.
smtp_data	SMTP mail data connections.
sqlnet_fixup_data	SQL*Net data inspection engine connections.
tcp_embryonic	TCP embryonic connections.
vpn_orphan	Orphaned VPN tunneled flows.

When you use the **detail** option, the system displays information about the translation type and interface information using the connection flags defined in Table 46-6.

Table 46-6 Connection Flags

Flag	Description
a	awaiting outside ACK to SYN
A	awaiting inside ACK to SYN
b	TCP state bypass
B	initial SYN from outside
C	Computer Telephony Interface Quick Buffer Encoding (CTIQBE) media connection
d	dump
D	DNS

Table 46-6 Connection Flags (continued)

Flag	Description
E	outside back connection. This is a secondary data connection that must be initiated from the inside host. For example, using FTP, after the inside client issues the PASV command and the outside server accepts, the ASA preallocates an outside back connection with this flag set. If the inside client attempts to connect back to the server, then the ASA denies this connection attempt. Only the outside server can use the preallocated secondary connection.
f	inside FIN
F	outside FIN
g	Media Gateway Control Protocol (MGCP) connection
G	connection is part of a group[1]
h	H.225
H	H.323
i	incomplete TCP or UDP connection
I	inbound data
k	Skinny Client Control Protocol (SCCP) media connection
K	GTP t3-response
m	SIP media connection
M	SMTP data
O	outbound data
p	replicated (unused)
P	inside back connection. This is a secondary data connection that must be initiated from the inside host. For example, using FTP, after the inside client issues the PORT command and the outside server accepts, the ASA preallocates an inside back connection with this flag set. If the outside server attempts to connect back to the client, then the ASA denies this connection attempt. Only the inside client can use the preallocated secondary connection.
q	SQL*Net data
r	inside acknowledged FIN
R	outside acknowledged FIN for TCP connection
R	UDP RPC[2]
s	awaiting outside SYN
S	awaiting inside SYN
t	SIP transient connection[3]
T	SIP connection[4]
U	up
V	VPN orphan
W	WAAS
X	Inspected by the service module, such as a CSC SSM.
y	For clustering, identifies a backup owner flow.
Y	For clustering, identifies a director flow.

Table 46-6 Connection Flags (continued)

Flag	Description
z	For clustering, identifies a forwarder flow.
Z	Cloud Web Security

1. The G flag indicates the connection is part of a group. It is set by the GRE and FTP Strict fixups to designate the control connection and all its associated secondary connections. If the control connection terminates, then all associated secondary connections are also terminated.
2. Because each row of **show conn** command output represents one connection (TCP or UDP), there will be only one R flag per row.
3. For UDP connections, the value t indicates that it will timeout after one minute.
4. For UDP connections, the value T indicates that the connection will timeout according to the value specified using the **timeout sip** command.

Note For connections using a DNS server, the source port of the connection may be replaced by the *IP address of DNS server* in the **show conn** command output.

A single connection is created for multiple DNS sessions, as long as they are between the same two hosts, and the sessions have the same 5-tuple (source/destination IP address, source/destination port, and protocol). DNS identification is tracked by *app_id*, and the idle timer for each app_id runs independently.

Because the app_id expires independently, a legitimate DNS response can only pass through the ASA within a limited period of time and there is no resource build-up. However, when you enter the **show conn** command, you will see the idle timer of a DNS connection being reset by a new DNS session. This is due to the nature of the shared DNS connection and is by design.

Note When there is no TCP traffic for the period of inactivity defined by the **timeout conn** command (by default, 1:00:00), the connection is closed and the corresponding conn flag entries are no longer displayed.

If a LAN-to-LAN/Network-Extension Mode tunnel drops and does not come back, there might be a number of orphaned tunnel flows. These flows are not torn down as a result of the tunnel going down, but all the data attempting to flow through them is dropped. The **show conn** command output shows these orphaned flows with the **V** flag.

When the following TCP connection directionality flags are applied to connections between same-security interfaces (see the **same-security permit** command), the direction in the flag is not relevant because for same-security interfaces, there is no “inside” or “outside.” Because the ASA has to use these flags for same-security connections, the ASA may choose one flag over another (for example, f vs. F) based on other connection characteristics, but you should ignore the directionality chosen.

- B—Initial SYN from outside
- a—Awaiting outside ACK to SYN
- A—Awaiting inside ACK to SYN
- f—Inside FIN
- F—Outside FIN
- s—Awaiting outside SYN
- S—Awaiting inside SYN

To display information for a specific connection, include the **security-group** keyword and specify a security group table value or security group name for both the source and destination of the connection. The ASA displays the connection matching the specific security group table values or security group names.

When you specify the **security-group** keyword without specifying a source and destination security group table value or a source and destination security group name, the ASA displays data for all SXP connections.

The ASA displays the connection data in the format *security_group_name* (*SGT_value*) or just as the *SGT_value* when the security group name is unknown.

Note Security group data is not available for stub connections because stub connection do not go through the slow path. Stub connections maintain only the information necessary to forward packets to the owner of the connection.

You can specify a single security group name to display all connections in a cluster; for example, the following example displays connections matching security-group mktg in all units of the cluster:

```
hostname# show cluster conn security-group name mktg
```

Examples

When specifying multiple connection types, use commas without spaces to separate the keywords. The following example displays information about RPC, H.323, and SIP connections in the Up state:

```
hostname# show conn state up,rpc,h323,sip
```

The following is sample output from the **show conn count** command:

```
hostname# show conn count
54 in use, 123 most used
```

The following is sample output from the **show conn** command. This example shows a TCP session connection from inside host 10.1.1.15 to the outside Telnet server at 10.10.49.10. Because there is no B flag, the connection is initiated from the inside. The “U”, “I”, and “O” flags denote that the connection is active and has received inbound and outbound data.

```
hostname# show conn
54 in use, 123 most used
TCP out 10.10.49.10:23 in 10.1.1.15:1026 idle 0:00:22, bytes 1774, flags UIO
UDP out 10.10.49.10:31649 in 10.1.1.15:1028 idle 0:00:14, bytes 0, flags D-
TCP dmz 10.10.10.50:50026 inside 192.168.1.22:5060, idle 0:00:24, bytes 1940435, flags
UTIOB
TCP dmz 10.10.10.50:49764 inside 192.168.1.21:5060, idle 0:00:42, bytes 2328346, flags
UTIOB
TCP dmz 10.10.10.51:50196 inside 192.168.1.22:2000, idle 0:00:04, bytes 31464, flags UIB
TCP dmz 10.10.10.51:52738 inside 192.168.1.21:2000, idle 0:00:09, bytes 129156, flags UIOB
TCP dmz 10.10.10.50:49764 inside 192.168.1.21:0, idle 0:00:42, bytes 0, flags Ti
TCP outside 192.168.1.10(20.20.20.24):49736 inside 192.168.1.21:0, idle 0:01:32, bytes 0,
flags Ti
TCP dmz 10.10.10.50:50026 inside 192.168.1.22:0, idle 0:00:24, bytes 0, flags Ti
TCP outside 192.168.1.10(20.20.20.24):50663 inside 192.168.1.22:0, idle 0:01:34, bytes 0,
flags Ti
TCP dmz 10.10.10.50:50026 inside 192.168.1.22:0, idle 0:02:24, bytes 0, flags Ti
TCP outside 192.168.1.10(20.20.20.24):50663 inside 192.168.1.22:0, idle 0:03:34, bytes 0,
flags Ti
TCP dmz 10.10.10.50:50026 inside 192.168.1.22:0, idle 0:04:24, bytes 0, flags Ti
TCP outside 192.168.1.10(20.20.20.24):50663 inside 192.168.1.22:0, idle 0:05:34, bytes 0,
flags Ti
```

```
TCP dmz 10.10.10.50:50026 inside 192.168.1.22:0, idle 0:06:24, bytes 0, flags Ti
TCP outside 192.168.1.10(20.20.20.24):50663 inside 192.168.1.22:0, idle 0:07:34, bytes 0,
flags Ti
```

The following is sample output from the **show conn** command, whcih includes the "X" flag to indicate that the connection is being scanned by the SSM.

```
hostname# show conn address 10.0.0.122 state service_module
TCP out 10.1.0.121:22 in 10.0.0.122:34446 idle 0:00:03, bytes 2733, flags UIOX
```

The following is sample output from the **show conn detail** command. This example shows a UDP connection from outside host 10.10.49.10 to inside host 10.1.1.15. The D flag denotes that this is a DNS connection. The number 1028 is the DNS ID over the connection.

```
hostname# show conn detail
54 in use, 123 most used
Flags: A - awaiting inside ACK to SYN, a - awaiting outside ACK to SYN,
       B - initial SYN from outside, b - TCP state-bypass or nailed, C - CTIQBE media,
       D - DNS, d - dump, E - outside back connection, F - outside FIN, f - inside FIN,
       G - group, g - MGCP, H - H.323, h - H.225.0, I - inbound data,
       i - incomplete, J - GTP, j - GTP data, K - GTP t3-response
       k - Skinny media, M - SMTP data, m - SIP media, n - GUP
       O - outbound data, P - inside back connection, p - Phone-proxy TFTP connection,
       q - SQL*Net data, R - outside acknowledged FIN,
       R - UDP SUNRPC, r - inside acknowledged FIN, S - awaiting inside SYN,
       s - awaiting outside SYN, T - SIP, t - SIP transient, U - up,
       V - VPN orphan, W - WAAS,
       X - inspected by service module
TCP outside:10.10.49.10/23 inside:10.1.1.15/1026,
    flags UIO, idle 39s, uptime 1D19h, timeout 1h0m, bytes 1940435
UDP outside:10.10.49.10/31649 inside:10.1.1.15/1028,
    flags dD, idle 39s, uptime 1D19h, timeout 1h0m, bytes 1940435
TCP dmz:10.10.10.50/50026 inside:192.168.1.22/5060,
    flags UTIOB, idle 39s, uptime 1D19h, timeout 1h0m, bytes 1940435
TCP dmz:10.10.10.50/49764 inside:192.168.1.21/5060,
    flags UTIOB, idle 56s, uptime 1D19h, timeout 1h0m, bytes 2328346
TCP dmz:10.10.10.51/50196 inside:192.168.1.22/2000,
    flags UIB, idle 18s, uptime 1D19h, timeout 1h0m, bytes 31464
TCP dmz:10.10.10.51/52738 inside:192.168.1.21/2000,
    flags UIOB, idle 23s, uptime 1D19h, timeout 1h0m, bytes 129156
TCP outside:10.132.64.166/52510 inside:192.168.1.35/2000,
    flags UIOB, idle 3s, uptime 1D21h, timeout 1h0m, bytes 357405
TCP outside:10.132.64.81/5321 inside:192.168.1.22/5060,
    flags UTIOB, idle 1m48s, uptime 1D21h, timeout 1h0m, bytes 2083129
TCP outside:10.132.64.81/5320 inside:192.168.1.21/5060,
    flags UTIOB, idle 1m46s, uptime 1D21h, timeout 1h0m, bytes 2500529
TCP outside:10.132.64.81/5319 inside:192.168.1.22/2000,
    flags UIOB, idle 31s, uptime 1D21h, timeout 1h0m, bytes 32718
TCP outside:10.132.64.81/5315 inside:192.168.1.21/2000,
    flags UIOB, idle 14s, uptime 1D21h, timeout 1h0m, bytes 358694
TCP outside:10.132.64.80/52596 inside:192.168.1.22/2000,
    flags UIOB, idle 8s, uptime 1D21h, timeout 1h0m, bytes 32742
TCP outside:10.132.64.80/52834 inside:192.168.1.21/2000,
    flags UIOB, idle 6s, uptime 1D21h, timeout 1h0m, bytes 358582
TCP outside:10.132.64.167/50250 inside:192.168.1.35/2000,
    flags UIOB, idle 26s, uptime 1D21h, timeout 1h0m, bytes 375617
```

The following is sample output from the **show conn** command when an orphan flow exists, as indicated by the **V** flag:

```
hostname# show conn
16 in use, 19 most used
TCP out 192.168.110.251:7393 in 192.168.150.252:21 idle 0:00:00, bytes 1048, flags UOVB
TCP out 192.168.110.251:21137 in 192.168.150.252:21 idle 0:00:00, bytes 1048, flags UIOB
```

To limit the report to those connections that have orphan flows, add the **vpn_orphan** option to the **show conn state** command, as in the following example:

```
hostname# show conn state vpn_orphan
14 in use, 19 most used
TCP out 192.168.110.251:7393 in 192.168.150.252:5013, idle 0:00:00, bytes 2841019, flags
UOVB
```

For clustering, to troubleshoot the connection flow, first see connections on all units by entering the **cluster exec show conn** command on the master unit. Look for flows that have the following flags: director (Y), backup (y), and forwarder (z). The following example shows an SSH connection from 172.18.124.187:22 to 192.168.103.131:44727 on all three ASAs; ASA 1 has the z flag showing it is a forwarder for the connection, ASA3 has the Y flag showing it is the director for the connection, and ASA2 has no special flags showing it is the owner. In the outbound direction, the packets for this connection enter the inside interface on ASA2 and exit the outside interface. In the inbound direction, the packets for this connection enter the outside interface on ASA 1 and ASA3, are forwarded over the cluster control link to ASA2, and then exit the inside interface on ASA2.

```
hostname/ASA1/master# cluster exec show conn
ASA1(LOCAL):**********************************************************
18 in use, 22 most used
Cluster stub connections: 0 in use, 5 most used
TCP outside  172.18.124.187:22 inside  192.168.103.131:44727, idle 0:00:00, bytes
37240828, flags z


ASA2:****************************************************************
12 in use, 13 most used
Cluster stub connections: 0 in use, 46 most used
TCP outside  172.18.124.187:22 inside  192.168.103.131:44727, idle 0:00:00, bytes
37240828, flags UIO


ASA3:****************************************************************
10 in use, 12 most used
Cluster stub connections: 2 in use, 29 most used
TCP outside  172.18.124.187:22 inside  192.168.103.131:44727, idle 0:00:03, bytes 0, flags
Y
```

The output of **show conn detail** on ASA2 shows that the most recent forwarder was ASA1:

```
hostname/ASA2/slave# show conn detail
12 in use, 13 most used
Cluster stub connections: 0 in use, 46 most used
Flags: A - awaiting inside ACK to SYN, a - awaiting outside ACK to SYN,
       B - initial SYN from outside, b - TCP state-bypass or nailed, C - CTIQBE media,
       D - DNS, d - dump, E - outside back connection, F - outside FIN, f - inside FIN,
       G - group, g - MGCP, H - H.323, h - H.225.0, I - inbound data,
       i - incomplete, J - GTP, j - GTP data, K - GTP t3-response
       k - Skinny media, M - SMTP data, m - SIP media, n - GUP
       O - outbound data, P - inside back connection, p - Phone-proxy TFTP connection,
       q - SQL*Net data, R - outside acknowledged FIN,
       R - UDP SUNRPC, r - inside acknowledged FIN, S - awaiting inside SYN,
       s - awaiting outside SYN, T - SIP, t - SIP transient, U - up,
       V - VPN orphan, W - WAAS, Z - Scansafe redirection,
       X - inspected by service module
       Y - director stub flow
       y - backup stub flow
       z - forwarder stub flow
TCP outside: 172.18.124.187/22 inside: 192.168.103.131/44727,
```

```
    flags UIO , idle 0s, uptime 25s, timeout 1h0m, bytes 1036044, cluster sent/rcvd bytes
0/1032983, cluster sent/rcvd total bytes 0/1080779, owners (1,255)
Traffic received at interface outside
        Locally received: 0 (0 byte/s)
        From most recent forwarder ASA1: 1032983 (41319 byte/s)
Traffic received at interface inside
        Locally received: 3061 (122 byte/s)
```

The following examples show how to display connections for the Identity Firewall feature:

```
hostname# show conn user-identity ?
exec mode commands/options:
  all       Enter this keyword to show conns including to-the-box and from-the-box
  detail    Enter this keyword to show conn in detail
  long      Enter this keyword to show conn in long format
  port      Enter this keyword to specify port
  protocol  Enter this keyword to specify conn protocol
  state     Enter this keyword to specify conn state
  |         Output modifiers

hostname# show conn user-identity
1219 in use, 1904 most used
UDP inside (www.yahoo.com))10.0.0.2:1587 outside (user1)192.0.0.2:30000, idle 0:00:00, bytes 10, flags -
UDP inside (www.yahoo.com)10.0.0.2:1586 outside (user2)192.0.0.1:30000, idle 0:00:00, bytes 10, flags –
UDP inside 10.0.0.34:1586 outside 192.0.0.25:30000, idle 0:00:00, bytes 10, flags –
…
hostname# show conn user user1
2 in use
UDP inside (www.yahoo.com))10.0.0.2:1587 outside (user1)192.0.0.2:30000, idle 0:00:00, bytes 10, flags –
```

Related Commands

Commands	Description
clear conn	Clears connections.
inspect ctiqbe	Enables CTIQBE application inspection.
inspect h323	Enables H.323 application inspection.
inspect mgcp	Enables MGCP application inspection.
inspect sip	Removes Java applets from HTTP traffic.
inspect skinny	Enables SCCP application inspection.

show console-output

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

show console-output

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

The following is sample output from the **show console-output** command, which displays the following message when there is no console output:

```
hostname# show console-output
Sorry, there are no messages to display
```

Related Commands

Command	Description
clear configure console	Restores the default console connection settings.
clear configure timeout	Restores the default idle time durations in the configuration.
console timeout	Sets the idle timeout for a console connection to the ASA.
show running-config console timeout	Displays the idle timeout for a console connection to the ASA.

show context

To show context information including allocated interfaces and the configuration file URL, the number of contexts configured, or from the system execution space, a list of all contexts, use the **show context** command in privileged EXEC mode.

show context [*name* | **detail** | **count**]

Syntax Description

count	(Optional) Shows the number of contexts configured.
detail	(Optional) Shows additional detail about the context(s) including the running state and information for internal use.
name	(Optional) Sets the context name. If you do not specify a name, the ASA displays all contexts. Within a context, you can only enter the current context name.

Defaults

In the system execution space, the ASA displays all contexts if you do not specify a name.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.
8.0(2)	Information about assigned IPS virtual sensors was added.

Usage Guidelines

See the “Examples” section for a description of the display output.

Examples

The following is sample output from the **show context** command. The following sample display shows three contexts:

```
hostname# show context

Context Name      Interfaces                  URL
*admin            GigabitEthernet0/1.100      flash:/admin.cfg
                  GigabitEthernet0/1.101
contexta          GigabitEthernet0/1.200      flash:/contexta.cfg
                  GigabitEthernet0/1.201
contextb          GigabitEthernet0/1.300      flash:/contextb.cfg
                  GigabitEthernet0/1.301
Total active Security Contexts: 3
```

Table 46-7 shows each field description.

Table 46-7 show context Fields

Field	Description
Context Name	Lists all context names. The context name with the asterisk (*) is the admin context.
Interfaces	The interfaces assigned to the context.
URL	The URL from which the ASA loads the context configuration.

The following is sample output from the **show context detail** command in the system execution space:

```
hostname# show context detail

Context "admin", has been created, but initial ACL rules not complete
  Config URL: flash:/admin.cfg
  Real Interfaces: Management0/0
  Mapped Interfaces: Management0/0
  Real IPS Sensors: ips1, ips2
  Mapped IPS Sensors: highsec, lowsec
  Flags: 0x00000013, ID: 1

Context "ctx", has been created, but initial ACL rules not complete
  Config URL: ctx.cfg
  Real Interfaces: GigabitEthernet0/0.10, GigabitEthernet0/1.20,
     GigabitEthernet0/2.30
  Mapped Interfaces: int1, int2, int3
  Real IPS Sensors: ips1, ips3
  Mapped IPS Sensors: highsec, lowsec
  Flags: 0x00000011, ID: 2

Context "system", is a system resource
  Config URL: startup-config
  Real Interfaces:
  Mapped Interfaces: Control0/0, GigabitEthernet0/0,
     GigabitEthernet0/0.10, GigabitEthernet0/1, GigabitEthernet0/1.10,
     GigabitEthernet0/1.20, GigabitEthernet0/2, GigabitEthernet0/2.30,
     GigabitEthernet0/3, Management0/0, Management0/0.1
  Flags: 0x00000019, ID: 257

Context "null", is a system resource
  Config URL: ... null ...
  Real Interfaces:
  Mapped Interfaces:
  Flags: 0x00000009, ID: 258
```

Table 46-8 shows each field description.

Table 46-8 Context States

Field	Description
Context	The context name. The null context information is for internal use only. The system context represents the system execution space.
State Message:	The context state. See the possible messages below.
Has been created, but initial ACL rules not complete	The ASA parsed the configuration but has not yet downloaded the default ACLs to establish the default security policy. The default security policy applies to all contexts initially, and includes disallowing traffic from lower security levels to higher security levels, enabling application inspection, and other parameters. This security policy ensures that no traffic can pass through the ASA after the configuration is parsed but before the configuration ACLs are compiled. You are unlikely to see this state because the configuration ACLs are compiled very quickly.
Has been created, but not initialized	You entered the **context** *name* command, but have not yet entered the **config-url** command.
Has been created, but the config hasn't been parsed	The default ACLs were downloaded, but the ASA has not parsed the configuration. This state might exist because the configuration download might have failed because of network connectivity issues, or you have not yet entered the **config-url** command. To reload the configuration, from within the context, enter **copy startup-config running-config**. From the system, reenter the **config-url** command. Alternatively, you can start configuring the blank running configuration.
Is a system resource	This state applies only to the system execution space and to the null context. The null context is used by the system, and the information is for internal use only.
Is a zombie	You deleted the context using the **no context** or **clear context** command, but the context information persists in memory until the ASA reuses the context ID for a new context, or you restart.
Is active	This context is currently running and can pass traffic according to the context configuration security policy.
Is ADMIN and active	This context is the admin context and is currently running.
Was a former ADMIN, but is now a zombie	You deleted the admin context using the **clear configure context** command, but the context information persists in memory until the ASA reuses the context ID for a new context, or you restart.
Real Interfaces	The interfaces assigned to the context. If you mapped the interface IDs in the **allocate-interface** command, this display shows the real name of the interface.
Mapped Interfaces	If you mapped the interface IDs in the **allocate-interface** command, this display shows the mapped names. If you did not map the interfaces, the display lists the real names again.
Real IPS Sensors	The IPS virtual sensors assigned to the context if you have an AIP SSM installed. If you mapped the sensor names in the **allocate-ips** command, this display shows the real name of the sensor.

Table 46-8 Context States (continued)

Field	Description
Mapped IPS Sensors	If you mapped the sensor names in the **allocate-ips** command, this display shows the mapped names. If you did not map the sensor names, the display lists the real names again.
Flag	For internal use only.
ID	An internal ID for this context.

The following is sample output from the **show context count** command:

```
hostname# show context count
Total active contexts: 2
```

Related Commands

Command	Description
admin-context	Sets the admin context.
allocate-interface	Assigns interfaces to a context.
changeto	Changes between contexts or the system execution space.
config-url	Specifies the location of the context configuration.
context	Creates a security context in the system configuration and enters context configuration mode.

show controller

To view controller-specific information of all interfaces present, use the **show controller** command in privileged EXEC mode.

show controller [**slot**] [*physical_interface*] [**pci** [**bridge** [*bridge-id* [*port-num*]]]] [**detail**]

Syntax Description

bridge	(Optional) Displays PCI bridge-specific information for the ASA 5585-X.
bridge-id	(Optional) Displays each unique PCI bridge identifier for the ASA 5585-X.
detail	(Optional) Shows additional detail about the controller.
pci	(Optional) Displays a summary of PCI devices along with their first 256 bytes of PCI configuration space for the ASA 5585-X.
physical_interface	(Optional) Identifies the interface ID.
port-num	(Optional) Displays the unique port number within each PCI bridge for the ASA 5585-X adaptive ASA.
slot	(Optional) Displays PCI-e bus and slot information for the ASA 5580 only.

Defaults

If you do not identify an interface, this command shows information for all interfaces.

Command Modes

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

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

Command History

Release	Modification
7.2(1)	This command was introduced.
8.0(2)	This command now applies to all platforms, and not just the ASA 5505. The **detail** keyword was added.
8.1(1)	The **slot** keyword was added for the ASA 5580.
8.2(5)	The **pci**, **bridge**, *bridge-id,* and *port-num* options were added for the ASA 5585-X with an IPS SSP installed. In addition, support for sending pause frames to enable flow control on 1 GigabitEthernet interfaces has been added for all ASA models.
8.6(1)	Support was added for the **detail** keyword for the ASA 5512-X through ASA 5555-X Internal-Control0/0 interface, used for control traffic between the ASA and the software module, and for the Internal-Data0/1 interface used for data traffic to the ASA and the software module.

Usage Guidelines

This command helps Cisco TAC gather useful debug information about the controller when investigating internal and customer found defects. The actual output depends on the model and Ethernet controller. The command also displays information about all the PCI bridges of interest in the ASA 5585-X with an IPS SSP installed. For the ASA Services Module, the **show controller** command output does not show any PCIe slot information.

Examples

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

```
hostname# show controller

Ethernet0/0:
   Marvell 88E6095 revision 2, switch port 7
     PHY Register:
         Control:       0x3000  Status:        0x786d
         Identifier1:   0x0141  Identifier2:   0x0c85
         Auto Neg:      0x01e1  LP Ability:    0x40a1
         Auto Neg Ex:   0x0005  PHY Spec Ctrl: 0x0130
         PHY Status:    0x4c00  PHY Intr En:   0x0400
         Int Port Sum:  0x0000  Rcv Err Cnt:   0x0000
         Led select:    0x1a34
         Reg 29:        0x0003  Reg 30:        0x0000
     Port Registers:
         Status:        0x0907  PCS Ctrl:      0x0003
         Identifier:    0x0952  Port Ctrl:     0x0074
         Port Ctrl-1:   0x0000  Vlan Map:      0x077f
         VID and PRI:   0x0001  Port Ctrl-2:   0x0cc8
         Rate Ctrl:     0x0000  Rate Ctrl-2:   0x3000
         Port Asc Vt:   0x0080
         In Discard Lo: 0x0000  In Discard Hi: 0x0000
         In Filtered:   0x0000  Out Filtered:  0x0000

     Global Registers:
         Control:       0x0482

--------------------------------------------------------------------------
Number of VLANs: 1
--------------------------------------------------------------------------
Vlan[db]\Port|  0 |  1 |  2 |  3 |  4 |  5 |  6 |  7 |  8 |  9 | 10 |
--------------------------------------------------------------------------
  <0001[01]> | EUT| EUT| EUT| EUT| EUT| EUT| EUT| EUT| EUM| NM | NM |
--------------------------------------------------------------------------

....

Ethernet0/6:
   Marvell 88E6095 revision 2, switch port 1
     PHY Register:
         Control:       0x3000  Status:        0x7849
         Identifier1:   0x0141  Identifier2:   0x0c85
         Auto Neg:      0x01e1  LP Ability:    0x0000
         Auto Neg Ex:   0x0004  PHY Spec Ctrl: 0x8130
         PHY Status:    0x0040  PHY Intr En:   0x8400
         Int Port Sum:  0x0000  Rcv Err Cnt:   0x0000
         Led select:    0x1a34
         Reg 29:        0x0003  Reg 30:        0x0000
     Port Registers:
         Status:        0x0007  PCS Ctrl:      0x0003
         Identifier:    0x0952  Port Ctrl:     0x0077
         Port Ctrl-1:   0x0000  Vlan Map:      0x07fd
         VID and PRI:   0x0001  Port Ctrl-2:   0x0cc8
         Rate Ctrl:     0x0000  Rate Ctrl-2:   0x3000
```

```
        Port Asc Vt:   0x0002
        In Discard Lo: 0x0000  In Discard Hi: 0x0000
        In Filtered:   0x0000  Out Filtered:  0x0000
   ----Inline power related counters and registers----
   Power on fault: 0  Power off fault: 0
   Detect enable fault: 0  Detect disable fault: 0
   Faults: 0
   Driver counters:
   I2C Read Fail: 0   I2C Write Fail: 0
   Resets: 1  Initialized: 1
   PHY reset error: 0
   LTC4259 registers:
   INTRPT STATUS = 0x88  INTRPT MASK   = 0x00  POWER EVENT   = 0x00
   DETECT EVENT  = 0x03  FAULT EVENT   = 0x00  TSTART EVENT  = 0x00
   SUPPLY EVENT  = 0x02  PORT1 STATUS  = 0x06  PORT2 STATUS  = 0x06
   PORT3 STATUS  = 0x00  PORT4 STATUS  = 0x00  POWER STATUS  = 0x00
   OPERATE MODE  = 0x0f  DISC. ENABLE  = 0x30  DT/CLASS ENBL = 0x33
   TIMING CONFIG = 0x00  MISC. CONFIG  = 0x00

...

Internal-Data0/0:
   Y88ACS06 Register settings:
    rap                          0xe0004000 = 0x00000000
    ctrl_status                  0xe0004004 = 0x5501064a
    irq_src                      0xe0004008 = 0x00000000
    irq_msk                      0xe000400c = 0x00000000
    irq_hw_err_src               0xe0004010 = 0x00000000
    irq_hw_err_msk               0xe0004014 = 0x00001000
    bmu_cs_rxq                   0xe0004060 = 0x002aaa80
    bmu_cs_stxq                  0xe0004068 = 0x01155540
    bmu_cs_atxq                  0xe000406c = 0x012aaa80

   Bank 2: MAC address registers:

....
```

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

```
hostname# show controller gigabitethernet0/0 detail

GigabitEthernet0/0:
   Intel i82546GB revision 03

     Main Registers:
         Device Control:             0xf8260000 = 0x003c0249
         Device Status:              0xf8260008 = 0x00003347
         Extended Control:           0xf8260018 = 0x000000c0
         RX Config:                  0xf8260180 = 0x0c000000
         TX Config:                  0xf8260178 = 0x000001a0
         RX Control:                 0xf8260100 = 0x04408002
         TX Control:                 0xf8260400 = 0x000400fa
         TX Inter Packet Gap:        0xf8260410 = 0x00602008
         RX Filter Cntlr:            0xf8260150 = 0x00000000
         RX Chksum:                  0xf8265000 = 0x00000300

     RX Descriptor Registers:
         RX Descriptor 0 Cntlr:      0xf8262828 = 0x00010000
         RX Descriptor 0 AddrLo:     0xf8262800 = 0x01985000
         RX Desccriptor 0 AddrHi:    0xf8262804 = 0x00000000
         RX Descriptor 0 Length:     0xf8262808 = 0x00001000
         RX Descriptor 0 Head:       0xf8262810 = 0x00000000
         RX Descriptor 0 Tail:       0xf8262818 = 0x000000ff
         RX Descriptor 1 Cntlr:      0xf8262828 = 0x00010000
```

```
        RX Descriptor 1 AddrLo:     0xf8260138 = 0x00000000
        RX Descriptor 1 AddrHi:     0xf826013c = 0x00000000
        RX Descriptor 1 Length:     0xf8260140 = 0x00000000
        RX Descriptor 1 Head:       0xf8260148 = 0x00000000
        RX Descriptor 1 Tail:       0xf8260150 = 0x00000000

    TX Descriptor Registers:
        TX Descriptor 0 Cntlr:      0xf8263828 = 0x00000000
        TX Descriptor 0 AddrLo:     0xf8263800 = 0x01987000
        TX Descriptor 0 AddrHi:     0xf8263804 = 0x00000000
        TX Descriptor 0 Length:     0xf8263808 = 0x00001000
        TX Descriptor 0 Head:       0xf8263810 = 0x00000000
        TX Descriptor 0 Tail:       0xf8263818 = 0x00000000

    RX Address Array:
        Ethernet Address 0:         0012.d948.ef58
        Ethernet Address 1:         Not Valid!
        Ethernet Address 2:         Not Valid!
        Ethernet Address 3:         Not Valid!
        Ethernet Address 4:         Not Valid!
        Ethernet Address 5:         Not Valid!
        Ethernet Address 6:         Not Valid!
        Ethernet Address 7:         Not Valid!
        Ethernet Address 8:         Not Valid!
        Ethernet Address 9:         Not Valid!
        Ethernet Address a:         Not Valid!
        Ethernet Address b:         Not Valid!
        Ethernet Address c:         Not Valid!
        Ethernet Address d:         Not Valid!
        Ethernet Address e:         Not Valid!
        Ethernet Address f:         Not Valid!

    PHY Registers:
        Phy Control:                0x1140
        Phy Status:                 0x7969
        Phy ID 1:                   0x0141
        Phy ID 2:                   0x0c25
        Phy Autoneg Advertise:      0x01e1
        Phy Link Partner Ability:   0x41e1
        Phy Autoneg Expansion:      0x0007
        Phy Next Page TX:           0x2801
        Phy Link Partnr Next Page:  0x0000
        Phy 1000T Control:          0x0200
        Phy 1000T Status:           0x4000
        Phy Extended Status:        0x3000

    Detailed Output - RX Descriptor Ring:

    rx_bd[000]: baddr      = 0x019823A2, length = 0x0000, status  = 0x00
                pkt chksum = 0x0000,     errors = 0x00,   special = 0x0000
    rx_bd[001]: baddr      = 0x01981A62, length = 0x0000, status  = 0x00
                pkt chksum = 0x0000,     errors = 0x00,   special = 0x0000

   ........
```

The following is sample output from the **show controller detail** command for the Internal interfaces on the ASA 5512-X through ASA 5555-X:

```
hostname# show controller detail

Internal-Control0/0:
   ASA IPS/VM Back Plane TunTap Interface , port id 9
     Major Configuration Parameters
         Device Name           : en_vtun
         Linux Tun/Tap Device  : /dev/net/tun/tap1
```

```
        Num of Transmit Rings : 1
        Num of Receive Rings  : 1
        Ring Size             : 128
        Max Frame Length      : 1550
        Out of Buffer         : 0
        Reset                 : 0
        Drop                  : 0
    Transmit Ring [0]:
        tx_pkts_in_queue      : 0
        tx_pkts               : 176
        tx_bytes              : 9664
    Receive Ring [0]:
        rx_pkts_in_queue      : 0
        rx_pkts               : 0
        rx_bytes              : 0
        rx_drops              : 0

Internal-Data0/1:
   ASA IPS/VM Management Channel TunTap Interface , port id 9
     Major Configuration Parameters
        Device Name           : en_vtun
        Linux Tun/Tap Device  : /dev/net/tun/tap2
        Num of Transmit Rings : 1
        Num of Receive Rings  : 1
        Ring Size             : 128
        Max Frame Length      : 1550
        Out of Buffer         : 0
        Reset                 : 0
        Drop                  : 0
    Transmit Ring [0]:
        tx_pkts_in_queue      : 0
        tx_pkts               : 176
        tx_bytes              : 9664
    Receive Ring [0]:
        rx_pkts_in_queue      : 0
        rx_pkts               : 0
        rx_bytes              : 0
        rx_drops              : 0
```

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

```
Slot  Card Description                              PCI-e Bandwidth Cap.
----  ----------------                             ---------------------
3.    ASA 5580 2 port 10GE SR Fiber Interface Card   Bus: x4, Card: x8

4.    ASA 5580 4 port GE Copper Interface Card       Bus: x4, Card: x4

5.    ASA 5580 2 port 10GE SR Fiber Interface Card   Bus: x8, Card: x8

6.    ASA 5580 4 port GE Fiber Interface Card        Bus: x4, Card: x4

7.    empty                                          Bus: x8

8.    empty                                          Bus: x8
```

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

```
hostname# show controller pci

PCI Evaluation Log:
  ------------------------------------------------------------------------------
    Empty

  PCI Bus:Device.Function (hex): 00:00.0 Vendor ID: 0x8086 Device ID: 0x3406
```

```
-------------------------------------------------------------------------

  PCI Configuration Space (hex):
  0x00: 86 80 06 34 00 00 10 00 22 00 00 06 10 00 00 00
  0x10: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x20: 00 00 00 00 00 00 00 00 00 00 00 00 86 80 00 00
  0x30: 00 00 00 00 60 00 00 00 00 00 00 00 05 01 00 00
  0x40: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x50: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x60: 05 90 02 01 00 00 00 00 00 00 00 00 00 00 00 00
  0x70: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x80: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x90: 10 e0 42 00 20 80 00 00 00 00 00 00 41 3c 3b 00
  0xa0: 00 00 41 30 00 00 00 00 c0 07 00 01 00 00 00 00
  0xb0: 00 00 00 00 3e 00 00 00 09 00 00 00 00 00 00 00
  0xc0: 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0xd0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0xe0: 01 00 03 c8 08 00 00 00 00 00 00 00 00 00 00 00
  0xf0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

  Link Capabilities: x4, Gen1
  Link Status: x4, Gen1
```

Related Commands

Command	Description
show interface	Shows the interface statistics.
show tech-support	Shows information so Cisco TAC can diagnose problems.

show coredump filesystem

To show the contents of the coredump filesystem, enter the **show coredump filesystem** command.

show coredump filesystem

Syntax Descriptionn

This command has no arguments or keywords.

Defaults

By default, coredumps are not enabled.

Command Modes

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

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

Command History

Release	Modification
8.2(1)	This command was introduced.

Usage Guidelines

This command shows the contents of the coredump filesystem.

Examples

To show the contents of any recent coredumps generated, enter the **show coredump filesystem** command.

```
hostname(config)# show coredump filesystem
Coredump Filesystem Size is 100 MB
Filesystem type is FAT for disk0
Filesystem 1k-blocks Used Available Use% Mounted on
/dev/loop0 102182 75240 26942 74% /mnt/disk0/coredumpfsys
Directory of disk0:/coredumpfsys/
246 -rwx 20205386 19:14:53 Nov 26 2008 core_lina.2008Nov26_191244.203.11.gz
247 -rwx 36707919 19:17:27 Nov 26 2008 core_lina.2008Nov26_191456.203.6.gz
```

Related Commands

Command	Description
coredump enable	Enables the coredump feature.
clear configure coredump	Removes any coredumps currently stored on the coredump filesystem and clears the coredump log. Does not touch the coredump filesystem itself and does not change or affect the coredump configuration.

Command	Description
clear coredump	Removes any coredumps currently stored on the coredump filesystem and clears the coredump log. Does not touch the coredump filesystem itself and does not change/effect the coredump configuration.
show coredump log	Shows the coredump log.

show coredump log

To show the contents of the coredump log, newest first, enter the **show coredump log** command. To show the contents of the coredump log, oldest first, enter the **show coredump log reverse** command.

show coredump log

show coredump log [**reverse**]

Syntax Description

reverse	Shows the oldest coredump log.

Defaults

By default, coredumps are not enabled.

Command Modes

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

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

Command History

Release	Modification
8.2(1)	This command was introduced.

Usage Guidelines

This command displays the contents of the coredump log. The logs should reflect what is currently on the disk.

Examples

The following example shows the output from these commands:

```
hostname(config)# show coredump log
[ 1 ] Wed Feb 18 22:12:09 2009: Coredump completed for module 'lina', coredump file
'core_lina.2009Feb18_221032.203.6.gz', size 971722752 bytes, compressed size 21293688
[ 2 ] Wed Feb 18 22:11:01 2009: Filesystem full on 'disk0', removing module coredump
record 'core_lina.2009Feb18_213558.203.11.gz'
[ 3 ] Wed Feb 18 22:10:32 2009: Coredump started for module 'lina', generating coredump
file 'core_lina.2009Feb18_221032.203.6.gz' on 'disk0'
[ 4 ] Wed Feb 18 21:37:35 2009: Coredump completed for module 'lina', coredump file
'core_lina.2009Feb18_213558.203.11.gz', size 971722752 bytes, compressed size 21286383
[ 5 ] Wed Feb 18 21:35:58 2009: Coredump started for module 'lina', generating coredump
file 'core_lina.2009Feb18_213558.203.11.gz' on 'disk0'
```

Note The older coredump file is deleted to make room for the new coredump. This is done automatically by the ASA in the event the coredump filesystem fills and room is needed for the current coredump. This is why it is imperative to archive coredumps as soon as possible, to insure they don't get overwritten in the event of a crash.

```
hostname(config)# show coredump log reverse
[ 1 ] Wed Feb 18 21:35:58 2009: Coredump started for module 'lina', generating coredump
file 'core_lina.2009Feb18_213558.203.11.gz' on 'disk0''
[ 2 ] Wed Feb 18 21:37:35 2009: Coredump completed for module 'lina', coredump file
'core_lina.2009Feb18_213558.203.11.gz', size 971722752 bytes, compressed size 21286383
[ 3 ] Wed Feb 18 22:10:32 2009: Coredump started for module 'lina', generating coredump
file 'core_lina.2009Feb18_221032.203.6.gz' on 'disk0'
[ 4 ] Wed Feb 18 22:11:01 2009: Filesystem full on 'disk0', removing module coredump
record 'core_lina.2009Feb18_213558.203.11.gz'
[ 5 ] Wed Feb 18 22:12:09 2009: Coredump completed for module 'lina', coredump file
'core_lina.2009Feb18_221032.203.6.gz', size 971722752 bytes, compressed size 21293688
```

Related Commands

Command	Description
coredump enable	Enables the coredump feature.
clear configure coredump	Removes any coredumps currently stored on the coredump filesystem and clears the coredump log. Does not touch the coredump filesystem itself and does not change/effect the coredump configuration.
clear coredump	Removes any coredumps currently stored on the coredump filesystem and clears the coredump log. Does not touch the coredump filesystem itself and does not change or affect the coredump configuration.
show coredump filesystem	Shows the contents of the coredump filesystem.

show counters

To display the protocol stack counters, use the **show counters** command in privileged EXEC mode.

show counters [all | context *context-name* **| summary | top** *N* **] [detail] [protocol** *protocol_name* **[:***counter_name***]] [threshold** *N***]**

Syntax Description

all	Displays the filter details.
context *context-name*	Specifies the context name.
:*counter_name*	Specifies a counter by name.
detail	Displays additional counters information.
protocol *protocol_name*	Displays the counters for the specified protocol.
summary	Displays a counter summary.
threshold *N*	Displays only those counters at or above the specified threshold. The range is 1 through 4294967295.
top *N*	Displays the counters at or above the specified threshold. The range is 1 through 4294967295.

Defaults

show counters summary detail threshold 1

Command Modes

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

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

Command History

Release	Modification
9.0(1)	This command was introduced.

Examples

The following example shows how to display all counters:

```
hostname# show counters all
Protocol     Counter           Value   Context
IOS_IPC      IN_PKTS               2   single_vf
IOS_IPC      OUT_PKTS              2   single_vf

hostname# show counters
Protocol     Counter           Value   Context
NPCP         IN_PKTS            7195   Summary
NPCP         OUT_PKTS           7603   Summary
IOS_IPC      IN_PKTS             869   Summary
IOS_IPC      OUT_PKTS            865   Summary
IP           IN_PKTS             380   Summary
IP           OUT_PKTS            411   Summary
IP           TO_ARP              105   Summary
IP           TO_UDP                9   Summary
UDP          IN_PKTS               9   Summary
UDP          DROP_NO_APP           9   Summary
FIXUP        IN_PKTS             202   Summary
UAUTH        IPV6_UNSUPPORTED     27   Summary
IDFW         HIT_USER_LIMIT        2   Summary
```

The following example shows how to display a summary of counters:

```
hostname# show counters summary
Protocol     Counter           Value   Context
IOS_IPC      IN_PKTS               2   Summary
IOS_IPC      OUT_PKTS              2   Summary
```

The following example shows how to display counters for a context:

```
hostname# show counters context single_vf
Protocol     Counter           Value   Context
IOS_IPC      IN_PKTS               4   single_vf
IOS_IPC      OUT_PKTS              4   single_vf
```

Related Commands

Command	Description
clear counters	Clears the protocol stack counters.

show cpu

To display the CPU utilization information, use the **show cpu** command in privileged EXEC mode.

[**cluster exec**] **show cpu** [**usage** *core-id* | **profile** | **dump** | **detailed**]

From the system configuration in multiple context mode:

[**cluster exec**] **show cpu** [**usage**] [**context** {**all** | *context_name*}]

Syntax Description

all	Specifies that the display show all contexts.
cluster exec	(Optional) In a clustering environment, enables you to issue the **show cpu** command in one unit and run the command in all the other units at the same time.
context	Specifies that the display show a context.
context_name	Specifies the name of the context to display.
core-id	Specifies the number of the processor core.
detailed	(Optional) Displays the CPU usage internal details.
dump	(Optional) Displays the dump profiling data to the TTY.
profile	(Optional) Displays the CPU profiling data.
usage	(Optional) Displays the CPU usage.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.
8.6(1)	The *core-id* option was added to support the ASA 5512-X, 5515-X, 5525-X, 5545-X, and 5555-X.
9.1(2)	The output was updated for the **show cpu profile** and **show cpu profile dump** commands.

Usage Guidelines

The CPU usage is computed using an approximation of the load every five seconds, and by further feeding this approximation into two, following moving averages.

You can use the **show cpu** command to find process related loads (that is, activity on behalf of items listed by the output of the **show process** command in both single mode and from the system configuration in multiple context mode).

Further, you can request, when in multiple context mode, a breakdown of the process related load to CPU consumed by any configured contexts by changing to each context and entering the **show cpu** command or by entering the **show cpu context** command.

While process related load is rounded to the nearest whole number, context related loads include one additional decimal digit of precision. For example, entering the **show cpu** command from the system context produces a different number than from entering the **show cpu context system** command. The former is an approximate summary of everything that appears in the **show cpu context all** command, and the latter is only a portion of that summary.

You can use the **show cpu profile dump** command in conjunction with the **cpu profile activate** command to collect information for TAC use in troubleshooting CPU issues. The **show cpu profile dump** command output is in hexadecimal format.

If the CPU profiler is waiting for a starting condition to occur, the **show cpu profile** command displays the following output:

```
CPU profiling started: 12:45:57.209 UTC Wed Nov 14 2012
CPU Profiling waiting on starting condition.
Core 0: 0 out of 10 samples collected.
Core 1: 0 out of 10 samples collected.
Core 2: 0 out of 10 samples collected.
Core 3: 0 out of 10 samples collected.
CP
0 out of 10 samples collected.
```

Examples

The following example shows how to display the CPU utilization:

```
hostname# show cpu usage
CPU utilization for 5 seconds = 18%; 1 minute: 18%; 5 minutes: 18%
```

The following example shows how to display detailed CPU utilization information:

```
hostname# show cpu detailed
Break down of per-core data path versus control point cpu usage:
Core         5 sec            1 min            5 min
Core 0       0.0 (0.0 + 0.0)  3.3 (0.0 + 3.3)  2.4 (0.0 + 2.4)

Current control point elapsed versus the maximum control point elapsed for:
      5 seconds = 99.0%; 1 minute: 99.8%; 5 minutes: 95.9%

CPU utilization of external processes for:
      5 seconds = 0.2%; 1 minute: 0.0%; 5 minutes: 0.0%

Total CPU utilization for:
      5 seconds = 0.2%; 1 minute: 3.3%; 5 minutes: 2.5%
```

Note The “Current control point elapsed versus the maximum control point elapsed for” statement means that the current control point load is compared to the maximum load seen within the defined time period. This is a ratio instead of an absolute number. The figure of 99% for the 5-second interval means that the current control point load is at 99% of the maximum load that is visible over this 5-second interval. If the load continues to increase all the time, then it will always remain at 100%. However, the actual CPU may still have a lot of free capacity because the maximum absolute value has not been defined.

The following example shows how to display the CPU utilization for the system context in multiple mode:

```
hostname# show cpu context system
CPU utilization for 5 seconds = 9.1%; 1 minute: 9.2%; 5 minutes: 9.1%
```

The following example shows how to display the CPU utilization for all contexts:

```
hostname# show cpu usage context all
5 sec  1 min  5 min  Context Name
9.1%   9.2%   9.1%  system
0.0%   0.0%   0.0%  admin
5.0%   5.0%   5.0%  one
4.2%   4.3%   4.2%  two
```

The following example shows how to display the CPU utilization for a context named “one”:

```
hostname/one# show cpu usage
CPU utilization for 5 seconds = 5.0%; 1 minute: 5.0%; 5 minutes: 5.0%
```

The following example activates the profiler and instructs it to store 1000 samples.

```
hostname# cpu profile activate
Activated CPU profiling for 1000 samples.
Use "show cpu profile" to display the progress or "show cpu profile dump" to interrupt
profiling and display the incomplete results.
```

The following examples show the status of the profiing (in-progress and completed):

```
hostname# show cpu profile
CPU profiling started: 13:45:10.400 PST Fri Nov 16 2012
CPU profiling currently in progress:
Core 0: 209 out of 1000 samples collected.
Use "show cpu profile dump" to see the results after it is complete or to interrupt
profiling and display the incomplete results.

hostname# show cpu profile dump
Cisco Adaptive Security Appliance Software Version 9.1(2)
Hardware:   ASA5555
CPU profiling started: 09:13:32.079 UTC Wed Jan 30 2013
No CPU profiling process specified.
No CPU profiling trigger specified.
cores: 2

Process virtual address map:
---------------------------
…
---------------------------
End of process map
Samples for core 0 - stopped
{0x00000000007eadb6,0x000000000211ee7e} ...
```

Copy this information and provide it to the TAC for decoding.

Related Commands

Command	Description
show counters	Displays the protocol stack counters.
cpu profile activate	Activates CPU profiling.