



## Using Troubleshooting Tools

---

This chapter describes the troubleshooting tools that are available for the Cisco Virtual Security Gateway (VSG).

This chapter includes the following sections:

- [Commands, page 2-1](#)
- [Ping, page 2-1](#)
- [Traceroute, page 2-2](#)
- [Monitoring Processes and CPUs, page 2-2](#)
- [Syslog, page 2-7](#)
- [CLI Configuration, page 2-8](#)
- [show Commands, page 2-14](#)

### Commands

Use the CLI from a local console or remotely use the CLI through a Telnet or Secure Shell (SSH) session. The CLI provides a command structure that is similar to the Cisco NX-OS software, with context-sensitive help, **show** commands, multi-user support, and role-based access control.

Each feature has **show** commands that provide information about the feature configuration, status, and performance. Additionally, you can use the following commands for more information:

- **show system**—Provides information on system-level components, including codes, errors, and exceptions. Use the **show system error-id** command to find details on error codes:

```
vsg# show system error-id 0x401e0008
Error Facility: sysmgr
Error Description: request was aborted, standby disk may be full
```

### Ping

The ping utility generates a series of echo packets to a destination across a TCP/IP internetwork. When the echo packets arrive at the destination, they are rerouted and sent back to the source. Using ping, you can verify connectivity and latency to a particular destination across an IP routed network.

Ping allows you to ping a port or end device. By specifying the IPv4 address, you can send a series of frames to a target destination. When these frames reach the target, they are looped back to the source and a time stamp is taken. Ping helps you to verify the connectivity and latency to a destination.

## Traceroute

Use traceroute to do the following tasks:

- Trace the route followed by the data traffic.
- Compute inter switch (hop-to-hop) latency.

The **traceroute** command identifies the path taken on a hop-by-hop basis and includes a time stamp at each hop in both directions. This command tests the connectivity of ports along the path between the generating switch and the switch closest to the destination.

If the destination cannot be reached, the path discovery starts, which traces the path up to the point of failure.

## Monitoring Processes and CPUs

This section includes the following topics:

- [Identifying Running Processes and Their States, page 2-2](#)
- [Displaying CPU Usage, page 2-5](#)
- [Displaying CPU and Memory Information, page 2-6](#)

## Identifying Running Processes and Their States

The **show processes** command identifies the running processes and the status of each process as follows:

- PID—Process ID.
- State—Process state.
- PC—Current program counter in hex format.
- Start\_cnt—How many times a process has been started (or restarted).
- TTY—Terminal that controls the process. A dash (-) usually means a daemon that is not running on any particular TTY.
- Process—Name of the process.

Process states are as follows:

- D—Uninterruptible sleep (usually I/O).
- R—Runnable (on run queue).
- S—Sleeping.
- T—Traced or stopped.
- Z—Defunct zombie process.
- NR—Not-running.

- ER—Should be running but is currently not running. The ER state typically designates a process that has been restarted too many times, which causes the system to classify it as faulty and disable it.

This example shows how to identify the available options for the **show processes** command:

```
vsg# show processes ?
<CR>
>      Redirect it to a file
>>    Redirect it to a file in append mode
cpu    Show processes CPU Info
log    Show information about process logs
memory Show processes Memory Info
vdc    Show processes in vdc
|      Pipe command output to filter
```

This example shows how to display the complete output from the Cisco VSG:

```
vsg# show processes
```

PID	State	PC	Start_cnt	TTY	Process
1	S	b7f8a468	1	-	init
2	S	0	1	-	ksoftirqd/0
3	S	0	1	-	desched/0
4	S	0	1	-	events/0
5	S	0	1	-	khelper
10	S	0	1	-	kthread
18	S	0	1	-	kblockd/0
35	S	0	1	-	khubd
188	S	0	1	-	pdflush
189	S	0	1	-	pdflush
190	S	0	1	-	kswapd0
191	S	0	1	-	aio/0
776	S	0	1	-	kseriod
823	S	0	1	-	kide/0
833	S	0	1	-	ata/0
837	S	0	1	-	scsi_eh_0
1175	S	0	1	-	kjournald
1180	S	0	1	-	kjournald
1743	S	0	1	-	kjournald
1750	S	0	1	-	kjournald
1979	S	b7f6c18e	1	-	portmap
1992	S	0	1	-	nfsd
1993	S	0	1	-	nfsd
1994	S	0	1	-	nfsd
1995	S	0	1	-	nfsd
1996	S	0	1	-	nfsd
1997	S	0	1	-	nfsd
1998	S	0	1	-	nfsd
1999	S	0	1	-	nfsd
2000	S	0	1	-	lockd
2001	S	0	1	-	rpciod
2006	S	b7f6e468	1	-	rpc.mountd
2012	S	b7f6e468	1	-	rpc.statd
2039	S	b7dd1468	1	-	sysmgr
2322	S	0	1	-	mping-thread
2323	S	0	1	-	mping-thread
2339	S	0	1	-	stun_kthread
2340	S	0	1	-	stun_arp_mts_kt
2341	S	0	1	-	stun_packets_re
2376	S	0	1	-	redun_kthread
2377	S	0	1	-	redun_timer_kth
2516	S	0	1	-	sf_rdn_kthread
2517	S	b7f37468	1	-	xinetd

2518	S	b7f6e468	1	-	tftpd
2519	S	b79371b6	1	-	syslogd
2520	S	b7ecb468	1	-	sdwrapd
2521	S	b7d6c468	1	-	platform
2526	S	0	1	-	ls-notify-mts-t
2539	S	b7eaabe4	1	-	pfm_dummy
2548	S	b7f836be	1	-	klogd
2555	S	b7c07be4	1	-	vshd
2556	S	b7e4e468	1	-	stun
2557	S	b7af2f43	1	-	smm
2558	S	b7ea0468	1	-	session-mgr
2559	S	b7cb2468	1	-	psshelper
2560	S	b7f75468	1	-	lmgrd
2561	S	b7e69be4	1	-	licmgr
2562	S	b7eb4468	1	-	fs-daemon
2563	S	b7e96468	1	-	feature-mgr
2564	S	b7e44468	1	-	confcheck
2565	S	b7ea8468	1	-	capability
2566	S	b7cb2468	1	-	psshelper_gsvc
2577	S	b7f75468	1	-	cisco
2580	S	b777d40d	1	-	clis
2586	S	b76a340d	1	-	port-profile
2588	S	b7cf9468	1	-	xmlma
2589	S	b7e59497	1	-	vnm_pa_intf
2590	S	b7e6c468	1	-	vmm
2591	S	b7b7d468	1	-	vdc_mgr
2592	S	b7e72468	1	-	ttyd
2593	R	b7eda5f5	1	-	sysinfo
2594	S	b7d06468	1	-	sksd
2596	S	b7e82468	1	-	res_mgr
2597	S	b7e48468	1	-	plugin
2598	S	b7bb7f43	1	-	npacl
2599	S	b7e93468	1	-	mvsh
2600	S	b7e01468	1	-	module
2601	S	b78fb40d	1	-	fwm
2602	S	b7e92468	1	-	evms
2603	S	b7e8c468	1	-	evmc
2604	S	b7ec3468	1	-	core-dmon
2605	S	b7e10468	1	-	bootvar
2606	S	b767040d	1	-	ascii-cfg
2607	S	b7ce4be4	1	-	securityd
2608	S	b77bf40d	1	-	cert_enroll
2609	S	b7ce1468	1	-	aaa
2612	S	b7aecf43	1	-	l3vm
2613	S	b7adff43	1	-	u6rib
2614	S	b7adff43	1	-	urib
2615	S	b7dce468	1	-	ExceptionLog
2616	S	b7da8468	1	-	ifmgr
2617	S	b7ea4468	1	-	tcap
2621	S	b75e140d	1	-	snmpd
2637	S	b7f03896	1	-	PMon
2638	S	b7be1468	1	-	ac1mgr
2662	S	b7af0f43	1	-	adjmgr
2670	S	b7aecf43	1	-	arp
2671	S	b791c896	1	-	icmpv6
2672	S	b7993f43	1	-	netstack
2746	S	b778d40d	1	-	radius
2747	S	b7f3ebe4	1	-	ip_dummy
2748	S	b7f3ebe4	1	-	ipv6_dummy
2749	S	b789840d	1	-	ntp
2750	S	b7f3ebe4	1	-	pktmgr_dummy
2751	S	b7f3ebe4	1	-	tcpudp_dummy
2755	S	b782740d	1	-	cdp
2756	S	b7b6240d	1	-	dcos-xinetd

```

2758      S  b7b8d40d          1    -  ntpd
2869      S  b7dd9468          1    -  vsim
2870      S  b797440d          1    -  ufdm
2871      S  b796740d          1    -  sal
2872      S  b793840d          1    -  pltfm_config
2873      S  b782f40d          1    -  monitor
2874      S  b7d80468          1    -  ipqosmgr
2875      S  b7a2827b          1    -  igmp
2876      S  b7a4340d          1    -  eth-port-sec
2877      S  b7b29468          1    -  copp
2878      S  b7ad740d          1    -  eth_port_channel
2879      S  b7b05468          1    -  vlan_mgr
2880      S  b767240d          1    -  ethpm
2921      S  b7d1e468          1    -  msp
2924      S  b7e8c468          1    -  vsn_service_mgr
2925      S  b7e25497          1    -  sp
2926      S  b7832497          1    -  policy_engine
2927      S  b7e3d497          1    -  inspect
3064      S  b7f836be          1    1  getty
3066      S  b7f806be          1    S0  getty
3091      S  b7f1deee          1    -  pa-httpd.sh
3092      S  b73da4c7          1    -  svc_sam_vsnAG
3096      S  b7db7b49          1    -  httpd
3098      S  b7476be4          1    -  svc_sam_commonA
3103      S  b70254c7          1    -  svc_sam_dme
3108      S  b7f1deee          1    -  sam_cores_mon.s
3150      S  b7db6dcc          1    -  httpd
25835    S  b7b4f40d          1    -  dcos_sshd
25850    S  b78e7eee          1    0  vsh
26766    S  b7f5d468          1    -  sleep
26768    S  b7f5d468          1    -  sleep
26769    R  b7f426be          1    0  more
26770    R  b790ebe4          1    0  vsh
26771    R  b7f716be          1    -  ps
-        NR  -                  0    -  tacacs
-        NR  -                  0    -  dhcp_snoop
-        NR  -                  0    -  installer
-        NR  -                  0    -  private-vlan
-        NR  -                  0    -  scheduler
-        NR  -                  0    -  vbuilder

```

## Displaying CPU Usage

You can use the **show processes cpu** command to display CPU usage. The command output includes the following information:

- **Runtime#(ms)**—CPU time that the process has used, expressed in milliseconds.
- **Invoked**—Number of times that the process has been invoked.
- **uSecs**—Microseconds of CPU time as an average for each process invocation.
- **1Sec**—CPU usage as a percentage for the last one second.

This example shows how to display all CPU processes:

```
vsg# show processes cpu
```

PID	Runtime (ms)	Invoked	uSecs	1Sec	Process
1	1519	14917	101	0.0%	init
2	555	16391	33	0.0%	ksoftirqd/0
3	96	59084	1	0.0%	desched/0

```

 4          1469      36858      39      0.0%  events/0
 5           35       2901      12      0.0%  khelper
10           0         14       3      0.0%  kthread
18           1        193       9      0.0%  kblockd/0
35           0         1       3      0.0%  khubd
188          0         3       0      0.0%  pdflush
189          95      13678       6      0.0%  pdflush
190          0         1       0      0.0%  kswapd0
191          0         2       1      0.0%  aio/0
776          0         1       3      0.0%  kseriod
823          3        138      28      0.0%  kide/0
833          0         2       2      0.0%  ata/0
837          0         1       4      0.0%  scsi_eh_0
1175         0         5      12      0.0%  kjournald
1180         0         1       5      0.0%  kjournald
1743         5        194      29      0.0%  kjournald
1750         0         21      21      0.0%  kjournald
1979         0         21      25      0.0%  portmap
1992         0         32      23      0.0%  nfsd
1993         0         20       4      0.0%  nfsd
1994         0         20       2      0.0%  nfsd
1995         0         20       2      0.0%  nfsd
1996         0         20       1      0.0%  nfsd
1997         0         20       9      0.0%  nfsd
1998         0         22       3      0.0%  nfsd
1999         0         22       3      0.0%  nfsd
2000         0         2      18      0.0%  lockd
2001         0         1       1      0.0%  rpciod
2006         0         1      53      0.0%  rpc.mountd
2012         1         5     341      0.0%  rpc.statd
2039         906     148314       6      0.0%  sysmgr
2322         0         1       9      0.0%  mping-thread
2323         0         1       3      0.0%  mping-thread
...

```

## Displaying CPU and Memory Information

You can use the **show system resources** command to display system-related CPU and memory statistics as follows:

- The load is defined as the number of running processes. The average reflects the system load over the past 1, 5, and 15 minutes.
- The Processes field displays the number of processes in the system and how many processes currently are running.
- The CPU state field shows the CPU usage percentage in the user mode, kernel mode, and idle time in the last one second.
- The memory usage field lists the total memory, used memory, free memory, memory used for buffers, and memory used for the cache in kilobytes. The memory used for buffers and cache is also included in the used memory statistics.

This example shows how to display statistics about available system resources:

```

vsg# show system resources
Load average:  1 minute: 0.00   5 minutes: 0.00   15 minutes: 0.02
Processes   :  321 total, 1 running
CPU states  :  0.0% user,   0.0% kernel, 100.0% idle
Memory usage: 1944668K total, 1114044K used, 830624K free
              62340K buffers, 479040K cache

```

# Syslog

The system message logging software saves messages in a log file or directs messages to other devices. This feature provides the following capabilities:

- Logging information for monitoring and troubleshooting.
- Selecting the types of logging information for capture.
- Selecting the destination of the captured logging information.

A syslog can store a chronological log of system messages locally or send the messages to a central syslog server. Syslog messages can also be sent to the console for immediate use. These messages can vary in detail depending on the configuration.

Syslog messages are categorized into seven severity levels from debug to critical events. Severity levels that are reported can be limited for specific services within the switch.

Log messages are not saved across system reboots. However, a maximum of 100 log messages with a severity level of critical and below (levels 0, 1, and 2) can be logged and saved to a local file or server.

This section includes the following topics:

- [Logging Levels, page 2-7](#)
- [Enabling Logging for Telnet or SSH, page 2-7](#)

## Logging Levels

The Cisco VSG supports the following logging levels:

- 0—Emergency
- 1—Alert
- 2—Critical
- 3—Error
- 4—Warning
- 5—Notification
- 6—Informational
- 7—Debugging

By default, the switch logs normal but significant system messages to a log file and sends these messages to the system console. Users can specify which system messages are saved, based on the type of facility and the severity level. Messages are time stamped to enhance real-time debugging and management.

## Enabling Logging for Telnet or SSH

System logging messages are sent to the console based on the default or configured logging facility and severity values.

Users can disable logging to the console or enable logging to a given Telnet or Secure Shell (SSH) session.

- To disable console logging, use the **no logging console** command in interface configuration mode.
- To enable logging for Telnet or SSH, use the **terminal monitor** command in EXEC mode.

**Note**

When logging to a console session is disabled or enabled, that state is applied to all future console sessions. If you exit and log in again to a new session, the state is preserved. When logging to a Telnet or SSH session that is enabled or disabled, that state applies only to that session. The state is not preserved after you exit the session.

The **no logging console** command is enabled by default. Use this command to disable console logging.

The **terminal monitor** command is disabled by default. Use this command to enable logging for Telnet or SSH.

For more information about configuring syslog, see the *Cisco Prime Network Services Controller GUI Configuration Guide*.

## CLI Configuration

This section includes the following topics:

- [Event Log, page 2-8](#)
- [Configuration and Restrictions, page 2-9](#)

## Event Log

This section describes event logs.

This section includes the following topics:

- [Event Log Configuration Format, page 2-8](#)
- [Viewing the Event Log Configuration, page 2-8](#)
- [Viewing Event Logs, page 2-9](#)
- [Event Log Configuration Persistence, page 2-9](#)

## Event Log Configuration Format

The configuration is displayed using this format:

```
[no] event-log inspect {{error | info} | {{ftp {error | info | warn | pkt_trace} | {rsh {error | info | pkt_trace} | {tftp {error | info }}}} {terminal}}
```

You can configure event logs for either the inspection process or one of its modules. For example, you can use the **event-log inspect error terminal** command to enable error events for the inspection process and to display these messages on the terminal where the command was entered.

## Viewing the Event Log Configuration

You can display the event log configuration by using the **show event-log all** command. This example shows how to display the event logs for all the processes and their modules:

```
vsg# show event-log all
event-log inspect tftp error
event-log inspect rsh error
event-log inspect ftp error terminal
```



```
event-log policy_engine attr-mgr error
event-log service-path sp pkt-error terminal
```

## Viewing Event Logs

Event logs are always logged in a process that is specific to the message buffer. Process logging in the event log buffer does not incur any overhead. In addition to using the **show event-log** command, you can display messages on a terminal where the event logs are enabled by using the terminal option, which is useful for reproducing a certain behavior.

The **show** command shows all the processes that are integrated with the event log Cisco VSG infrastructure. You can display inspection event logs using the **show system internal event-log inspect** command. The Cisco VSG event log infrastructure is a layer on top of the Cisco NX-OS event log infrastructure. Event logs can be redirected to a file and exported.

To display event logs on the terminal, use the **terminal** option while configuring the event. Different terminals can view different event logs. For example, use the **event-log inspect ftp info terminal** command to enable the information event logs for the inspection FTP module and to display the logs on the terminal. Use the **event-log inspect rsh error terminal** command to display only the error logs that are related to the RSH module. This command helps to debug various modules at the same time.

## Event Log Configuration Persistence

You can save the event log configuration by using the **event-log save config** command. This command allows you to save all of the currently enabled event logs in a file. This file is read at the time of the module/process initialization with the event log infrastructure. The event log configuration that is relevant to the process is reapplied during initialization, which makes the event log configuration persistent across the process/system reboot. Some important things about the event log configuration are as follows:

- Terminal information is not reapplied for process or system restarts because that information might not be applicable.
- The event log configuration is independent of the other Cisco NX-OS configurations. The **copy running-config startup-config** and **show running-config** commands do not save and display the event log configuration.
- The event log configuration is specific to the individual system. In a high-availability setup, the configuration must be set up on both systems.

## Configuration and Restrictions

Event logs CLIs for the Cisco VSG are classified based on the process and its modules. This section describes event log commands.

This section includes the following topics:

- [VNS Agent, page 2-10](#)
- [Inspection Process, page 2-11](#)
- [Service Path Process, page 2-12](#)
- [Policy Engine Process, page 2-13](#)
- [Restrictions, page 2-14](#)

## VNS Agent

Virtual Network Service (VNS) agent-related event logs are maintained on the Virtual Supervisor Module (VSM), not on the Cisco VSG.

This section includes the following topics:

- [Core Module, page 2-10](#)
- [VPath Module, page 2-10](#)
- [License Module, page 2-10](#)

### Core Module

Core events are those events that are related to the port attach, port detach, Internet Protocol Database (IPDB), and port-profile CLI.

This example shows how to enable/disable error messages for the vns\_agent core module:

```
vsm# event-log vns-agent core-error [terminal] ----->enable messages to the terminal
vsm# no event-log vns-agent core-error [terminal] ----->disable messages to the terminal
```

This example shows how to enable/disable informational messages for the vns\_agent core module:

```
vsm# event-log vns-agent core-info [terminal] ----->enable messages to the terminal
vsm# no event-log vns-agent core-info [terminal] ----->disable messages to the terminal
```

This example shows how to enable/disable notice event messages for the vns\_agent core module:

```
vsm# event-log vns-agent core-notice [terminal] ----->enable messages to the terminal
vsm# no event-log vns-agent core-notice [terminal] ----->disable messages to the terminal
```

### VPath Module

Because the vPath module works based on core-module events, you should always enable core module event logs before you enable the vPath module events.

This example shows how to enable/disable error messages for the vns\_agent vPath module:

```
vsm# event-log vns-agent vpath-error [terminal] ----->enable messages to the terminal
vsm# no event-log vns-agent vpath-error [terminal] ----->disable messages to the terminal
```

This example shows how to enable/disable informational messages for the vns\_agent vPath module:

```
vsm# event-log vns-agent vpath-info [terminal] ----->enable messages to the terminal
vsm# no event-log vns-agent vpath-info [terminal] ----->disable messages to the terminal
```

This example shows how to enable/disable notice event messages for the vns\_agent vPath module:

```
vsm# event-log vns-agent vpath-notice [terminal] ----->enable messages to the terminal
vsm# no event-log vns-agent vpath-notice [terminal] ----->disable messages to the terminal
```

### License Module

Because the license module works based on core-module events, you should always enable the core module event logs before enabling the license module.

This example shows how to enable/disable error messages for the vns\_agent license module:

```
vsm# event-log vns-agent license-error [terminal] ----->enable messages to the terminal
vsm# no event-log vns-agent license-error [terminal] ----->disable messages to the terminal
```

This example shows how to enable/disable informational messages for the vns\_agent license module:

```
vsm# event-log vns-agent license-info [terminal] ----->enable messages to the terminal
vsm# no event-log vns-agent license-info [terminal] ----->disable messages to the terminal
```

## Inspection Process

The inspection process uses event log commands for the inspection process and the File Transfer Protocol (FTP), Remote Shell (RSH), and Trivial File Transfer Protocol (TFTP) modules. These processes are all available on the Cisco VSG.

Use the **event-log inspect error** command to display configuration errors, process initialization errors, and so forth. This example shows how to enable/disable error messages for the inspection process:

```
vsg# event-log inspect error [terminal] ----->enable messages to the terminal
vsg# no event-log inspect error [terminal] ----->disable messages to the terminal
```

This example shows how to enable/disable informational messages for the inspection process:

```
vsg# event-log inspect info [terminal] ----->enable messages to the terminal
vsg# no event-log inspect info [terminal] ----->disable messages to the terminal
```

Use the **event-log inspect ftp error** command to display FTP packet processing errors. This example shows how to enable/disable error messages for the inspection FTP module:

```
vsg# event-log inspect ftp error [terminal] ----->enable messages to the terminal
vsg# no event-log inspect ftp error [terminal] ----->disable messages to the terminal
```

The command output is as follows:

```
Mon Oct 4 15:12:14 2010 ie_ftp: flow (->(ING), 6912), Bad ftp command.
Mon Oct 4 15:12:14 2010 ie_ftp: flow (->(ING), 6912), invalid PORT request / PASV reply.
```

This example shows how to enable/disable informational event log messages for the inspection FTP module:

```
vsg# event-log inspect ftp info [terminal] ----->enable messages to the terminal
vsg# no event-log inspect ftp info [terminal] ----->disable messages to the terminal
```

The command output is as follows:

```
Mon Oct 4 15:12:18 2010 ie_ftp: embryonic connection request (ip, port, proto, pfid, cid,
action, offload) = (192.168.1.20, 40074, tcp, 13569, 6912, 3,1).
Mon Oct 4 15:17:11 2010 ie_ftp: flow (<-(ING), 6912), more reply expected in cmd-reply.
```

This example shows how to enable/disable warning messages for the inspection FTP module:

```
vsg# event-log inspect ftp warn [terminal] ----->enable messages to the terminal
vsg# no event-log inspect ftp warn [terminal] ----->disable messages to the terminal
```

The command output is as follows:

```
Mon Oct 4 15:19:03 2010 ie_ftp: flow (<-(ING), 8192), ftp reply not terminated properly.
```

This example shows how to enable/disable packet trace messages for the inspection FTP module:

```
vsg# event-log inspect ftp pkt_trace [terminal] ----->enable messages to the terminal
vsg# no event-log inspect ftp pkt_trace [terminal] ----->disable messages to the terminal
```

The command output is as follows:

```
Mon Oct 4 15:31:46 2010 ie_ftp: flow (->(ING), 17152), flags(S:)
```

```
Mon Oct 4 15:31:54 2010 ie_ftp: flow (->(ING), 17152), cmd (USER)
```

This example shows how to enable/disable error messages for the inspection RSH module:

```
vsg# event-log inspect rsh error [terminal] ----->enable messages to the terminal
vsg# no event-log inspect rsh error [terminal] ----->disable messages to the terminal
```

This example shows how to enable/disable informational messages for the inspection RSH module:

```
vsg# event-log inspect rsh info [terminal] ----->enable messages to the terminal
vsg# no event-log inspect rsh info [terminal] ----->disable messages to the terminal
```

The command output is as follows:

```
Mon Oct 4 15:21:29 2010 ie_rsh: emryonic connection request (ip, port, proto, pfid, cid,
action, offload) = (192.168.1.10, 1021, tcp, 22529, 11264, 3, 1).
```

This example shows how to enable/disable packet trace messages for the inspection RSH module:

```
vsg# event-log inspect rsh pkt_trace [terminal] ----->enable messages to the terminal
vsg# no event-log inspect rsh pkt_trace [terminal] ----->disable messages to the terminal
```

The command output is as follows:

```
Mon Oct 4 15:25:26 2010 ie_rsh: flow (->(ING), 15872), rsh inspect action stop punt
```

This example shows how to enable/disable error messages for the inspection TFTP module:

```
vsg# event-log inspect tftp error [terminal] ----->enable messages to the terminal
vsg# no event-log inspect tftp error [terminal] ----->disable messages to the terminal
```

This example shows how to enable/disable informational messages for the inspection TFTP module:

```
vsg# event-log inspect tftp info [terminal] ----->enable messages to the terminal
vsg# no event-log inspect tftp info [terminal] ----->disable messages to the terminal
```

The command output is as follows:

```
Mon Oct 4 15:27:42 2010 ie_tftp: emryonic connection request (ip, port, proto, pfid, cid,
action, offload) = (192.168.1.10, 32771, udp, 33281, 16640, 3, 1)
```

## Service Path Process

This section includes the following topics:

- [Service Path Module, page 2-12](#)
- [Service Path Flow Manager, page 2-13](#)
- [AC Module, page 2-13](#)

The service path process exposes event log output for the VSN service path, flow manager, and AC infrastructure modules.

### Service Path Module

The **event-log service-path sp error** command can display a failure to initialize the FE, and so forth. This example shows how to enable/disable error messages for the service path module:

```
vsg# event-log service-path sp error [terminal] ----->enable messages to the terminal
vsg# no event-log service-path sp error [terminal] ----->disable messages to the terminal
```

Use the **event-log service-path sp info** command to display FE initialization messages, control path messages, and so forth. This example shows how to enable/disable informational messages for the service path module:

```
vsg# event-log service-path sp info [terminal] ----->enable messages to the terminal
vsg# no event-log service-path sp info [terminal] ----->disable messages to the terminal
```

The **event-log service-path sp pkt-error** command can display failures to read or write a packet, a corrupted packet, and so forth.

This example shows how to enable/disable packet error messages for the service path module:

```
vsg# event-log service-path sp pkt-error [terminal] ----->enable messages to the terminal
vsg# no event-log service-path sp pkt-error [terminal] ----->disable messages to the terminal
```

The **event-log service-path sp pkt-info** command can display the field description of a packet, where the packet arrived from or going to, decisions taken on the packet, and so forth.

This example shows how to enable/disable packet informational messages for the service path module:

```
vsg# event-log service-path sp pkt-info [terminal] ----->enable messages to the terminal
vsg# no event-log service-path sp pkt-info [terminal] ----->disable messages to the terminal
```

The **event-log service-path sp pkt-detail** command can display the first few 100 bytes of the incoming packets.

This example shows how to enable/disable detailed packet messages for the service path module:

```
vsg# event-log service-path sp pkt-detail [terminal] ----->enable messages to the terminal
vsg# no event-log service-path sp pkt-detail [terminal] ----->disable messages to the terminal
```

## Service Path Flow Manager

This example shows how to enable/disable the packet messages for the service path flow manager module:

```
vsg# event-log service-path fm error [terminal] ----->enable messages to the terminal
vsg# no event-log service-path fm error [terminal] ----->disable messages to the terminal
```

## AC Module

The **event-log service-path ac error** command can display failures to initialize the AC, timer, FD, pending queue, and so forth.

This example shows how to enable/disable error messages for the AC module:

```
vsg# event-log service-path ac error [terminal] ----->enable messages to the terminal
vsg# no event-log service-path ac error [terminal] ----->disable messages to the terminal
```

The **event-log service-path ac info** command can display AC initialization messages, control path messages, and so forth.

This example shows how to enable/disable informational messages for the AC module:

```
event-log service-path ac info [terminal] ----->enable messages to the terminal
no event-log service-path ac info [terminal] ----->disable messages to the terminal
```

## Policy Engine Process

This section includes the following topic:

- [Restrictions, page 2-14](#)

## Restrictions

The event log configuration has the following restrictions:

- Terminal information is not reapplied in case of process restart/system restart because it may or may not be applicable.
- Event log configuration is independent of the other Cisco NX-OS configurations. The Cisco NX-OS **copy running-config startup-config** and **show running-config** commands do not save and display event log configuration.
- Event log configuration is specific to the individual system. In the high-availability setup, this configuration must be done on both of the systems.

## show Commands

This section includes the following topics:

- [VSM show Commands, page 2-14](#)
- [Cisco VSG show Commands, page 2-18](#)

## VSM show Commands

This section includes the following topics:

- [show nsc-pa status, page 2-14](#)
- [show vservice node mac brief, page 2-14](#)
- [show vservice node detail, page 2-15](#)
- [show vservice port brief, page 2-15](#)
- [show vservice connection, page 2-16](#)
- [show vservice statistics \[ip ip-addr\] \[module module-num\], page 2-16](#)
- [clear vservice statistics \[ip ip-addr\] \[module module-num\], page 2-17](#)

### show nsc-pa status

You can display the NSC policy agent status by entering the **show nsc-pa status** command.

This example shows how to display the NSC policy agent installation status:

```
vsm# show nsc-pa status
NSC Policy-Agent status is - Installed Successfully. Version 2.1(1e)-vsm
```

### show vservice node mac brief

You can display a consolidated view of all VSNs in use by using the **show vservice node mac brief** command.

This example shows how to display all VSNs in use:

```
VSM-hpv# sh vservice node mac brief
-----
```

```

                                Node Information
-----
ID Type   IP-Address   MAC-Addr           Mode   Fail State  Module
 3 vsg     10.1.0.150   00:00:00:00:00:00 13     close Alive   4

```

The MAC address is shown as 0 for L3 mode since the VSG is configured behind a router that can perform proxy ARP.

## show vservice node detail

You can display detailed information for all VSNs in use by using the **show vservice node detail** command. Information is displayed for each of the associated VEMs. The command output displays the port profile, security profile, organization, and list of Cisco Nexus 1000V Series Switch ports that have inherited this configuration. Also displayed are any configuration mismatches between the VSM and VEM missing ports for a given port profile, all ports of a port profile that are not configured with the same security profile, and so forth.

This example shows how to display all VSNs in use:

```
VSM-hpv# show vservice node detail
```

```

                                Node Information
-----
Node ID:3      Name:VSG-Root
Type:vsg      IPAddr:10.1.0.150   Fail:close L3
Mod  State     MAC-Addr           VVer
 4  Alive     --                  2

```

## show vservice port brief

You can display information for each virtual Ethernet (vEth) interface by using the **show vservice port brief** command. By default, all attached vEths are listed. Use the **Module** option for output of vEth interfaces from specific module.

This example shows how to display the vEth interfaces from specific module:

```
vsm# show vservice port brief module 3
```

```

                                Port Information
-----
PortProfile:PP-VM-VNS1
Org:root
Node:VSG-Node1(90.1.0.79) Profile(Id):SP13(7)
Veth Mod VM-Name vNIC IP-Address
 1 3  lin1 80.1.0.11,
 5 3  lin2 80.1.0.22,
 6 3  vm-11 80.1.0.52,

```

Ensure that the VM Name value matches the name of the VM associated with this vNIC. For VSN Data IP in the brackets in the Node, Profile Name, and Org values, ensure that correct values for this VM are displayed. The Profile ID value should never be zero. For IP addresses, ensure that the list of IP addresses matches the IP addresses configured for the specific vNIC for that VM.

## show vservice connection

You can display VSN connections by using the **show vservice connection** command.

This example shows how to display VSN connections:

```
vsm-hpv# show vservice connection
Actions(Act):
d - drop s - reset
p - permit t - passthrough
r - redirect e - error
_ - not processed yet upper case - offloaded
Flags:
A - seen ack for syn/fin from src a - seen ack for syn/fin from dst
E - tcp conn established (SasA done)
F - seen fin from src f - seen fin from dst
R - seen rst from src r - seen rst from dst
S - seen syn from src s - seen syn from dst
T - tcp conn torn down (FafA done) x - IP-fragment connection

#Port-Profile:PP-VM-VNS1 Node:VSG-Node1
#Module 3
Proto SrcIP[:Port] SAct DstIP[:Port] DAct Flags Bytes
icmp 80.1.0.52 P 80.1.0.53 888
```

## show vservice statistics [ip ip-addr] [module module-num]

You can display VSN statistics by using the **show vservice statistics** command.

This example shows how to display the VSN statistics:

```
VSM-hpv# show vservice statistics module 4
#VSN VLAN: 0, IP-ADDR: 10.1.0.150
Module: 4
#VPath Packet Statistics      Ingress      Egress      Total
Total Seen                    2             2             4
Policy Redirects              2             2             4
No-Policy Passthru            0             0             0
Policy-Permits Rcvd           1             2             3
Policy-Denies Rcvd            0             0             0
Permit Hits                    0             0             0
Deny Hits                     0             0             0
Decapsulated                   1             2             3
Fail-Open                      0             0             0
Badport Err                    0             0             0
VSN Config Err                 0             0             0
VSN State Down                 228           1288          1516
Encap Err                      0             0             0
Version Mismatch               0             0             0
V1 In svcPath                  0             0             0
All-Drops                      228           1288          1516
Flow Notificns Sent            0
Total Rcvd From VSN            5
Non-Cisco Encap Rcvd           0
VNS-Port Drops                 2
Policy-Action Err              0
Decap Err                      0
L2-Frag Sent                    0
L2-Frag Rcvd                    0
L2-Frag Coalesced              0
Encap exceeded MTU             0
ICMP Too Big Rcvd              0
```



```

#VPath Flow Statistics
Active Flows                0  Active Connections                0
Forward Flow Create        1  Forward Flow Destroy              1
Reverse Flow Create        1  Reverse Flow Destroy              2
Flow ID Alloc              3  Flow ID Free                      3
Connection ID Alloc        1  Connection ID Free                1
L2 Flow Create             1  L2 Flow Destroy                   1
L3 Flow Create             0  L3 Flow Destroy                   0
L4 TCP Flow Create         0  L4 TCP Flow Destroy               0
L4 UDP Flow Create         2  L4 UDP Flow Destroy               2
L4 Oth Flow Create         0  L4 Oth Flow Destroy               0
Embryonic Flow Create      0  Embryonic Flow Bloom              0
L2 Flow Timeout           2  L2 Flow Offload                   3
L3 Flow Timeout           0  L3 Flow Offload                   0
L4 TCP Flow Timeout        0  L4 TCP Flow Offload               0
L4 UDP Flow Timeout        5  L4 UDP Flow Offload               0
L4 Oth Flow Timeout        0  L4 Oth Flow Offload               0
Flow Lookup Hit           5  Flow Lookup Miss                  3
Flow Dual Lookup           8  L4 TCP Tuple-reuse                0
TCP chkfail InvalACK      0  TCP chkfail SeqPstWnd             0
TCP chkfail WndVari        0
Flow Classify Err          0  Flow ID Alloc Err                 0
Conn ID Alloc Err          0  Hash Alloc Err                    0
Flow Exist                 0  Flow Entry Exhaust                0
Flow Removal Err           0  Flow Entry Miss                   0
Flow Full Match Err        0  Bad Action Receive                0
Invalid Flow Pair          3  Invalid Connection                 0
Hash Alloc                 0  Hash Free                          0
InvalFID Lookup Err        0  Deferred Delete                    0

```

## clear vservice statistics [ip ip-addr] [module module-num]

You can clear the VSN statistics by using the **clear vservice statistics** command.

This example shows how to clear VSN statistics:

```

VSM# clear vservice statistics ip 200.1.1.67 module 3
Cleared statistics successfully for specified VSN in module 3
VSM#show vservice statistics ip 200.1.1.67 module 3
#VSN VLAN: 756, IP-ADDR: 200.1.1.67
Module: 3
#VPath Packet Statistics      Ingress      Egress      Total
Total Seen                    0             0            0
Policy Redirects              0             0            0
No-Policy Passthru            0             0            0
Policy-Permits Rcvd           0             0            0
Policy-Denies Rcvd            0             0            0
Permit Hits                   0             0            0
Deny Hits                     0             0            0
Decapsulated                  0             0            0
Fail-Open                     0             0            0
Badport Err                   0             0            0
VSN Config Err                0             0            0
ARP Resolve Err               0             0            0
Encap Err                     0             0            0
All-Drops                     0             0            0
Total Rcvd From VSN           0
Non-Cisco Encap Rcvd          0
VNS-Port Drops                0
Policy-Action Err             0
Decap Err                     0
L2-Frag Sent                   0

```

```

L2-Frag Rcvd                                0
L2-Frag Coalesced                            0

#VPath Flow Statistics
Active Flows                                0 Active Connections                        0
Forward Flow Create                          0 Forward Flow Destroy                      0
Reverse Flow Create                          0 Reverse Flow Destroy                      0
Flow ID Alloc                                0 Flow ID Free                              0
Connection ID Alloc                          0 Connection ID Free                        0
L2 Flow Create                               0 L2 Flow Destroy                           0
L3 Flow Create                               0 L3 Flow Destroy                           0
L4 TCP Flow Create                           0 L4 TCP Flow Destroy                       0
L4 UDP Flow Create                           0 L4 UDP Flow Destroy                       0
L4 Oth Flow Create                           0 L4 Oth Flow Destroy                       0
Embryonic Flow Create                        0 Embryonic Flow Bloom                     0
L2 Flow Timeout                              0 L2 Flow Offload                           0
L3 Flow Timeout                              0 L3 Flow Offload                           0
L4 TCP Flow Timeout                          0 L4 TCP Flow Offload                       0
L4 UDP Flow Timeout                          0 L4 UDP Flow Offload                       0
L4 Oth Flow Timeout                          0 L4 Oth Flow Offload                       0
Flow Lookup Hit                              0 Flow Lookup Miss                         0
Flow Dual Lookup                             0 L4 TCP Tuple-reuse                       0
Flow Classify Err                            0 Flow ID Alloc Err                         0
Conn ID Alloc Err                            0 Hash Alloc Err                           0
Flow Exist                                   0 Flow Entry Exhaust                       0
Flow Removal Err                             0 Bad Flow ID Receive                       0
Flow Entry Miss                              0 Flow Full Match Err                       0
Bad Action Receive                           0 Invalid Flow Pair                         0
Invalid Connection                           0
Hash Alloc                                   0 Hash Free                                 0
InvalFID Lookup                              0 InvalFID Lookup Err                       0
Deferred Delete                              0

```

## Cisco VSG show Commands

The attribute manager maintains a set of tables and does a lookup that is based on the fields in the packet. The VNISP table is the main table. Use the **show vsg security-profile** command to display runtime information for the VNISP table.

Hash tables are maintained based on IP addresses (IP address to DV port entry) and the VNISP ID (VNISP ID to VNISP entry). An IP address is used to determine which policy set to evaluate for a given traffic type. The VNISP ID is used (the valid VNISP ID in the packet header) to determine which policy set to evaluate.

This section details the following commands:

- [show nsc-pa status, page 2-19](#)
- [show service-path statistics, page 2-19](#)
- [clear service-path statistics, page 2-20](#)
- [show service-path connection, page 2-20](#)
- [clear service-path connection, page 2-21](#)
- [show vsg security-profile {\[vnsp-name \]| detail | table}, page 2-21](#)
- [show vsg zone, page 2-22](#)
- [clear policy-engine, page 2-23](#)
- [show ac-driver statistics, page 2-23](#)

- [clear ac-driver statistics, page 2-24](#)
- [show system internal ac ipc-stats fe \[process-name\], page 2-24](#)
- [clear system internal ac ipc-stats fe \[process-name\], page 2-24](#)
- [show inspect ftp statistics, page 2-25](#)
- [clear inspect ftp statistics, page 2-26](#)

## show nsc-pa status

Enter the **show nsc-pa status** command to display the Cisco Prime NSC policy agent status.

This example shows how to display the Cisco Prime NSC policy agent status:

```
vsg# show nsc-pa status
NSC Policy-Agent status is - Installed Successfully. Version 2.1(1e)-vsg
```

## show service-path statistics

You can display the following statistics that pertain to one vPath by using the **show service-path statistics** command:

- The packets seen by the service path from the vPath.
- Flows created by the service path due to these packets.
- Packets dropped in the service path due to various errors.



### Note

If no module is given, the command displays the aggregate statistics of all the modules in the given SVS domain.

This command provides the following keyword filters:

- **svs-domain-id** *domain-id*—Displays only the Cisco VSG connections that are associated to the sv-domain specified by the *domain-id* argument.
- **module** *module-num*—Displays only the Cisco VSG connections that are associated to the sv-domain and VEM module specified by the *domain-id* and the *module-num* argument. Use this keyword filter only with the **svs-domain-id** filter.

This example shows how to display the statistics using the **svs-domain-id** keyword filter:

```
vsg# show service-path statistics svs-domain-id 118 module 5
Input Packet          161359233  Output Packet          161359220
Vpath Ingress Packet  7608059   Vpath Egress Packet   153751174
Vpath Frag            0         VSN Offload Packet    0
ARP Packet            0         Unknown L2 Packet     0
802.3 Packet         0         Vpath Jumbo Frame     0
IPV4 Packet          161359233  IPV4 options Packet   0
IPV4 Frag            0         Unknown L3Proto Packet 0
ICMP Packet           66        IGMP Packet           0
TCP Packet            161359095  UDP Packet             72
Policy Lookup Packet  160669149  Inspect FTP Packet    0
Inspect RSH Packet    0         Inspect TFTP Packet   0
Policy Lookup Fail    0         Policy Lookup Drop    0
Inspect FTP Fail      0         Inspect FTP Drop      0
Inspect RSH Fail      0         Inspect RSH Drop      0
Inspect TFTP Fail     0         Inspect TFTP Drop     0
Malformed Packet      0         Output Fail           0
Active Flows          473278    Active Connections    379521
```

Forward Flow Create	8690219	Forward Flow Destroy	3008524
Reverse Flow Create	3362016	Reverse Flow Destroy	8570433
Flow ID Alloc	12052235	Flow ID Free	11578957
Connection ID Alloc	3362016	Connection ID Free	2982495
L2 Flow Create	0	L2 Flow Destroy	0
L3 Flow Create	66	L3 Flow Destroy	66
L4 TCP Flow Create	12052097	L4 TCP Flow Destroy	11578819
L4 UDP Flow Create	72	L4 UDP Flow Destroy	72
L4 Other Flow Create	0	L4 Other Flow Destroy	0
Embryonic Flow Create	0	Embryonic Flow Bloom	0
L2 Flow Timeout	0	L2 Flow Offload	0
L3 Flow Timeout	99	L3 Flow Offload	66
L4 TCP Flow Timeout	25158984	L4 TCP Flow Offload	160668998
L4 UDP Flow Timeout	108	L4 UDP Flow Offload	72
L4 Other Flow Timeout	0	L4 Other Flow Offload	0
Flow Lookup Hit	157997217	Flow Lookup Miss	12052235
Flow Dual Lookup	138932556	L4 TCP Tuple-reuse	151978861
Flow Classify Err	0	Flow ID Alloc Err	0
Conn ID Alloc Err	0	Hash Alloc Err	0
Flow Exist	0	Flow Entry Exhaust	0
Flow Removal Err	0	Bad Flow ID receive	0
Flow Entry Missing	0	Flow Full Match Err	0
Bad Action Received	0	Invalid Flow Pair	0
Invalid Connection	0		

## clear service-path statistics

You can clear the service path statistics globally by using the **clear service-path statistics** command when no option is given. When the SVS domain ID and the module are provided, entering the command clears the statistics of the specified module.

This command provides the following keyword filters:

- **svs-domain-id** *domain-id*—Displays only the Cisco VSG connections that are associated to the svs-domain specified in the *domain-id*.
- **module** *module-num*—Displays only the Cisco VSG connections that are associated to the svs-domain and VEM module specified in the *domain-id* and the *module-num*. Use this only with the **svs-domain-id** filter.

This example shows how to clear the service path statistics:

```
vsg# clear service-path statistics
```

## show service-path connection

You can display the connections (flow-table) maintained in the Cisco VSG by using the **show service-path connection** command. These connections are provided per VEM module per SVS domain.

This command provides the following keyword filters:

- **svs-domain-id** *domain-id*—Displays only the Cisco VSG connections that are associated to the svs-domain specified in the *domain-id*.
- **module** *module-num*—Displays only the Cisco VSG connections that are associated to the svs-domain and VEM module specified in the *domain-id* and the *module-num*. Use this keyword filter only with the **svs-domain-id** keyword filter.

This example shows how to display the connections in the Cisco VSG:

```
vsg# show service-path connection
Flags:
```

```

P - policy at src                p - policy at dst
O - conn offloaded to ser-path at src  o - conn offloaded to ser-path at dst
S - seen syn from src           s - seen syn from dst
A - seen ack for syn/fin from src    a - seen ack for syn/fin from dst
F - seen fin from src            f - seen fin from dst
R - seen rst from src            r - seen rst from dst
E - tcp conn established (SasA done)  T - tcp conn torn down (FafA done)

#SVS Domain 2007  Module  3
Proto SrcIP[:Port]          DstIP[:Port]          VLAN Action  Flags

#SVS Domain 2007  Module  4
Proto  SrcIP[:Port]          DstIP[:Port]          VLAN  Action  Flags
icmp   10.100.201.176        10.100.201.185        160   permit  PpOo

```

## clear service-path connection

You can clear the connections (flow-table) maintained in the Cisco VSG by using the **clear service-path connection** command.

This example shows how to clear the flow-table connection output:

```
vsg# clear service-path connection
```

## show vsg vm uuid {vm\_uuid}

You can display relevant information for a particular VM by using the **show vsg vmuuid** command. The attribute manager looks up the VM attributes for the VM based on this association before doing a policy evaluation.

When debugging issues, such as when the wrong VM attributes are fetched, check the output of this command as well as the IP address to DV port mapping.

This example shows how to display the relevant information for a VM:

```

firewall1# show vsg vm uuid c42067b5-4533-43c5-8f2f-a3766d4cff4e
VM uuid : c42067b5-4533-43c5-8f2f-a3766d4cff4e
VM attributes :
name : vm-11
os-fullname : windows server 2012 r2 datacenter
os-hostname : windows123

DV Port(s) :
DV Port : c42067b5-4533-43c5-8f2f-a3766d4cff4e--75650fec-3694-49f0-b3
4c-f843d0d0fb88::542e5b16-694f-4bcb-ba2e-f7cb484cfc9b
Security Profile : SP13@root
Port Profile : pp-vm-vns1
IP Addresses :
80.1.0.52

Zone(s) :

```

## show vsg security-profile {[vnsn-name]} detail | table}

You can display information for a specific VNSP or all VNSPs by using the **show vsg security-profile** command. The attribute manager looks up custom attributes for a particular VNSP that is based on this association before doing a policy evaluation. By default, information is displayed for all VNSPs. You can specify a particular VNSP by using the *vnsn-name* argument.

When debugging issues such as the wrong policy set, check if the correct policy set is associated with the VNSP. If custom attribute values are not correct, this command displays some details.

The detailed version of this command includes names of the VMs that are using the security profile in addition to their security-profile information. A VNSP name can be specified to get details of a specific security profile.

This example shows how to display detailed information about a specific Cisco VSG security profile with the name `sp_deny@root`:

```
firewall-1# show vsg security-profile sp_deny@root detail
VNSP                : sp_deny@root
VNSP id             : 5
Policy Name         : ps_deny@root
Policy id           : 3
Custom attributes   :
  Name              : vnsporg
  Value             : root
  Name              : profile1
  Value             : eng
Virtual Machines:
  sg-pg-vm206
  sg-pg-redhat
```

You can display the associated VNSP ID and policy for all VNSPs by using the **show vsg security-profile** command. The attribute manager uses this association when looking up a VNSP and associated policy from the packet that reaches the data0 interface of the Cisco VSG. When vPath redirects the packets to the Cisco VSG, the VNSP ID is added in the packet header.

This example shows how to display brief tabular information for the Cisco VSG security profile:

```
firewall-tenant-aa# show vsg security-profile table
-----
Security-Profile Name      VNSP ID      Policy Name
-----
default@root               1            default@root
sec-profile-AB@root/Tenant-A/Data-Center-B 30
sec-profile-AA@root/Tenant-A/Data-Center-A 31
policyset-AA@root/Tenant-A/Data-Center-A
```

## show vsg zone

You can display VM to zone mappings on a Cisco VSG by using the **show vsg zone** command.

This example shows how to display the VM to zone mappings on a Cisco VSG:

```
vsg# show vsg zone
Zone : vzone2@root/T1
Virtual Machines :
-----
Zone : zone1@root/T1
Virtual Machines :
```

## show policy-engine stats

You can display statistics on the policy engine by using the **show policy-engine stats** command.

This example shows how to display the statistics for the Cisco VSG policy engine:

```
firewall-1# show policy-engine stats
```

```

Policy Match Stats:

default@root          :          0
  default/default-rule@root :      0 (Drop)
  NOT_APPLICABLE       :          0 (Drop)

policyset-one@root/Tenant-one      : 844935064
  policy-one/rule-z1@root/Tenant-one : 808288619 (Permit)
  policy-one/rule-one@root/Tenant-one : 366464445 (Permit)
  NOT_APPLICABLE                   :          0 (Drop)

```

This example shows how to use the help (?) feature of the command to display command options:

```

firewall-1# show policy-engine ?
WORD  Enter policy-name to show its stats
stats Show the Stats

firewall-1# show policy-engine policyset-one@root/Tenant-one stats

Policy Match Stats:

policyset-one@root/Tenant-one      : 844935064
  policy-one/rule-z1@root/Tenant-one : 808288619 (Permit)
  policy-one/rule-one@root/Tenant-one : 366464445 (Permit)
  NOT_APPLICABLE                   :          0 (Drop)

```

## clear policy-engine

You can clear the policy-engine statistics by using the **clear policy-engine** command.

This example shows how to see the options for clearing the policy-engine statistics:

```

firewall-1# clear policy-engine ?
WORD  Enter policy-name to clear its stats
stats Clear the Stats

```

When the **stats** argument is used, the statistics are cleared and the only response for a successful action is a return to the prompt. This example shows how to clear the policy engine statistics:

```

firewall-1# clear policy-engine stats

```

## show ac-driver statistics

You can display statistics that are collected in the AC driver module by using the **show ac-driver statistics** command. These statistics indicate how many packets are received, how many of those received packets are from vPath, how many packets are passed up to the service path, how many packets are passed as a response to the vPath, and any error statistics, and so on.

This example shows how to display the AC driver module statistics:

```

firewall-1# show ac-driver statistics
#Packet Statistics:
Rcvd Total          852079858  Buffers in Use          3190
Rcvd VPath Pkts    848148272  Sent to VPath          846621771
Sent to Service-Path 848148272  Sent to Control-Path   3931586
All Drops           0          Invalid LLC              0
Invalid OUI         0          Invalid VNS Hdr         0
Invalid VNS PDU     1          Service-Path not Inited 0
Service-Path Down   0          Rcvd Bad Descriptor     0
Send to Service-Path Err 0          Packet Offset Err       0
Send Bad Descriptor 0          Send NIC Err            0

```

## clear ac-driver statistics

You can clear the statistics that are collected in the AC driver module by using the **clear ac-driver statistics** command.

This example shows how to clear the statistics collected in the AC driver module:

```
vsg# clear ac-driver statistics
Cleared statistics successfully.
```

## show system internal ac ipc-stats fe [process-name]

You can display internal statistics of the following processes by using the **show system internal ac ipc-stats fe** command:

- attribute-manager
- inspection-ftp
- inspection-rsh
- inspection-tftp
- service-path

This example shows how to display the statistics for the inspection-ftp process:

```
firewall-1# show system internal ac ipc-stats fe inspection-ftp
=====
Instance:                1
IPC Type:                MTS(SAP 1326)
  Async requests sent:   0
  Async responses received: 0
  Async requests received: 764364
  Async responses sent:  764364
  Sendto requests sent:  32485
  Sendto requests received: 32485
  Async send errors:     0
  Async receive errors:  0
  Async response errors: 0
  Sendto send errors:    0
  Sendto receive errors: 0
  Receive errors:       0
  Token errors :        0
  Destination not found errors: 0
  Sendto response errors: 0
  Timer Errors :        0
  Timouts :             0
  Recv Queue Len:       11
  Queue Length High:    0
  Reciever Busy Errors: 0
=====
```

## clear system internal ac ipc-stats fe [process-name]

You can clear the internal statistics for the following processes by using the **clear system internal ac ipc-stats fe** command:

- attribute-manager
- inspection-ftp
- inspection-rsh



- inspection-tftp
- service-path

This example shows how to clear the statistics for the inspection-ftp process:

```
firewall-1# clear system internal ac ipc-stats fe inspection-ft
```

## show inspect ftp statistics

You can display the following inspect FTP statistics pertaining to one vPath by using the **show inspect ftp statistics** command:

- The packets seen by the inspect FTP path from the vPath.
- Flows created by the inspect FTP path due to these packets.
- Packets dropped in the inspect FTP path due to various errors.

This example shows how to display FTP statistics:

```
firewall-1# show inspect ftp statistics
```

```
Input packets          764364
Dropped packets        0
Reset-drop packets     0
New connections        32485
Deleted connections    31064
IPC errors             0
IPC allocation errors  0
```

```
SVS Domain 131 Module 4
```

```
Input packets          764364
Dropped packets        0
Reset-drop packets     0
New connections        32485
Deleted connections    31064
```

```
firewall-1# show inspect ftp statistics svs-domain-id 131 module 4
```

```
Input packets          764364
Dropped packets        0
Reset-drop packets     0
New connections        32485
Deleted connections    31064
Port zero drops        0
Invalid port drops     0
No port drops          0
Port command long drops 0
Rx port mismatch drops 0
Command not port command drops 0
Embryonic connections 32485
Embryonic connection failures 0
Memory allocations     64970
Memory de-allocations 63549
Memory allocation failures 0
Command in reply mode drops 0
Invalid command drops  0
Un-supported command drops 0
Command not terminated drops 0
Unexpected reply drops  0
Command too short drops 0
Reply code invalid drops 0
Reply length negative drops 0
Reply unexpected drops  0
Rx command in command mode drops 0
```

## clear inspect ftp statistics

Use the **clear inspect ftp statistics** command to clear the inspect FTP statistics globally when no option is given. When the SVS domain ID and the module are provided, the command clears the statistics of the specified module.

This command provides the following keyword filters:

- **svs-domain-id** *domain-id*—Displays only the Cisco VSG connections that are associated to the svcs-domain specified in the *domain-id*.
- **module** *module-num*—Displays only the Cisco VSG connections that are associated to the SVS domain and VEM module specified in the *domain-id* and the *module-num*. Use this keyword filter only with the **svs-domain-id** filter.

This example shows how to clear the inspect FTP statistics:

```
firewall-1# clear inspect ftp statistics
firewall-1# clear inspect ftp statistics svcs-domain-id 131 module 4
```