



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.

Send document comments to vsg-docfeedback@cisco.com.

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

You can monitor and the CPU status and usage.

This section includes the following topics:

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

Identifying the 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.

Send document comments to vsg-docfeedback@cisco.com.

- 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
vsg#
```

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

Send document comments to vsg-docfeedback@cisco.com.

```

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  b7addf43          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    -  aclmgr
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

```

Send document comments to vsg-docfeedback@cisco.com.

```

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
vsg#

```

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 of the CPU processes:

```
vsg# show processes cpu
```

```

PID      Runtime(ms)   Invoked   uSecs   1Sec   Process
-----  -
1        1519         14917    101     0.0%   init

```

Send document comments to vsg-docfeedback@cisco.com.

```

 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
...
vsg#
```

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.
- Processes display the number of processes in the system and how many processes are running when the command is issued.
- The CPU states show the CPU usage percentage in the user mode, kernel mode, and idle time in the last one second.
- The memory usage provides the total memory, used memory, free memory, memory used for buffers, and memory used for the cache in kilobytes. Buffers and cache are also included in the used memory statistics.

This example shows how to display the results of 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
```

Send document comments to vsg-docfeedback@cisco.com.

```
Memory usage: 1944668K total, 1114044K used, 830624K free
               62340K buffers, 479040K cache
vsg#
```

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.

Send document comments to vsg-docfeedback@cisco.com.

- 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 Virtual Network Management Center 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
```


Send document comments to vsg-docfeedback@cisco.com.

```
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
vsg#W
```

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](#)

Send document comments to vsg-docfeedback@cisco.com.

- [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 port attach, port detach, Internet Protocol Database (IPDB), and to 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
```

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
```

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
```

Send document comments to vsg-docfeedback@cisco.com.

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:

Send document comments to vsg-docfeedback@cisco.com.

```
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

The service path processes are available on the Cisco VSG.

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, 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:

Send document comments to vsg-docfeedback@cisco.com.

```
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 failure 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 failure 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

The policy engine processes are available on the Cisco VSG.

This section contains the following topic:

- [Attribute Manager Module, page 2-14](#)

Send document comments to vsg-docfeedback@cisco.com.

Attribute Manager Module

This section describes the attribute manager-related errors.

You can use the **event-log policy-engine attr-mgr error** command to display the policy ID for a PE evaluation lookup based on the VNSP ID, IP address, zone name resolution, attribute fetched, and so forth.

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

```
vsg# event-log policy-engine attr-mgr error [terminal] ----->enable messages to the
terminal
vsg# no event-log policy-engine attr-mgr error [terminal] ----->disable messages to the
terminal
```

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

```
vsg# event-log policy-engine attr-mgr info [terminal] ----->enable messages to the
terminal
vsg# no event-log policy-engine attr-mgr info [terminal] ----->disable messages to the
terminal
```

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 (HA) 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 2-20](#)

VSM Show Commands

This section includes the following topics:

- [show vnm-pa status, page 2-15](#)
- [show vsn brief, page 2-15](#)
- [show vsn detail \[port\] \[vlan vlan-num ip ip-addr\] \[module module-num\], page 2-15](#)
- [show vsn port \[vethernet veth-num\], page 2-16](#)
- [show vsn connection, page 2-16](#)
- [show vsn statistics \[vlan vlan-num ip ip-addr\] \[module module-num\], page 2-17](#)

Send document comments to vsg-docfeedback@cisco.com.

- `clear vsn statistics [vlan vlan-num ip ip-addr] [module module-num]`, page 2-19

show vnm-pa status

You can display the VNM policy agent status by entering the **show vnm-pa status** command.

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

```
vsm2# show vnm-pa status
VNM Policy-Agent status is - Installed Successfully. Version 1.0(1j)-vsm
vsm2#
```

show vsn brief

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

This example shows how to display all VSNs in use:

```
vsm2# show vsn brief
VLAN          IP-ADDR          MAC-ADDR          FAIL-MODE          STATE          MODULE
78            10.0.0.1         00:50:56:9c:04:28  Close              Up             3
vsm2#
```

FAIL-MODE specifies the behavior when the Virtual Ethernet Module (VEM) has no connectivity to the Cisco VSG. The default is Close (packets are dropped). Open means packets are forwarded.

The MAC-ADDR column lists the MAC address of the data0 interface that corresponds to that Cisco VSG (if the VEM can resolve it). If the VEM does not resolve the MAC address, it cannot redirect packets to the Cisco VSG. If a valid MAC address is not shown, check if the Cisco VSG data0 is reachable from the VEM. If there is no valid MAC-ADDR, these are possible reasons:

- The data0 interface on the Cisco VSG is not configured
- The VLAN is not up
- A mismatch has occurred in the VLAN specified in the **vn-service** command and the port profile used for the Cisco VSG VM.

The STATE can be Up, Down, or No Licenses. If Down, the MAC-ADDR is not resolved or the module is not up. If multiple VEM modules inherit the same VM port profile, those interfaces must pass all checks before the state can be Up. If No Licenses appears, install the Cisco VSG license on the VSM.

The MODULE column lists the VEM numbers whose interfaces have inherited this configuration.

show vsn detail [port] [vlan vlan-num ip ip-addr] [module module-num]

You can display detailed information for all VSNs in use by using the **show vsn detail** command. Information is displayed for each of the associated VEM modules. The command output displays the port profile, security profile, organization, and list of Cisco Nexus 1000V 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 same security profile, and so forth.

This example shows how to display all VSNs in use:

```
vsm# show vsn detail
#VSN VLAN: 756, IP-ADDR: 200.1.1.67
MODULE          VSN-MAC-ADDR          FAIL-MODE          VSN-STATE
3 00:50:56:83:03:1c    Close              Up
4 00:50:56:83:03:1c    Close              Up
```

Send document comments to vsg-docfeedback@cisco.com.

```
#VSN Ports, Port-Profile, Org and Security-Profile Association:
#VSN VLAN: 756, IP-ADDR: 200.1.1.67
  Port-Profile: profile-data, Security-Profile: sec-profile-stress1, Org:
root/Tenant-Stress1
  Module Vethernet
    3 9, 7, 8
    4 5, 6
vsm#
```

The Vethernet column shows the virtual Ethernet (vEth) interfaces that are bound to the appropriate VEM listed in the Module column and that they inherit the correct port profile.

Possible red flags include notations (* or ??) against the security profile or organization (the Org column).

show vsn port [vethernet veth-num]

You can display information for each vEth interface by using the **show vsn port** command. By default, all attached vEths are listed. Use the **vethernet** option for output of a specific vEth interface.

This example shows how to display the vEth interfaces:

```
vsm2# show vsn port
Veth          : Veth4
VM Name       : win2k3
VM uuid      : 42 1c 5a e4 51 c3 5d d9-60 fa a5 0c b0 4e d0 ea
DV Port      : 576
DVS uuid     : bc aa 1c 50 87 47 8d 08-fe 7e a9 aa 89 24 bf 8e
Flags        : 0x48
VSN Data IP   : 10.0.0.1
Security Profile : spcustom
Org          : orgroot
VNSP id      : 1
IP addresses:
  100.1.1.20
vsm2#
```



Note

- Any field with a value of Not set is an improper port configuration.
- For the VM Name value, make sure the VM name matches name of the VM associated with this vNIC.
- For VSN Data IP, Security Profile, and Org values, ensure that correct values for this VM are displayed.
- The VNSP ID 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. If not, use the **vemcmd show learnt** command on all VEM modules to display the Internet Protocol Database (IPDB) table.

show vsn connection

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

This example shows how to display VSN connections:

```
VSM-207-1# show vsn connection vlan 159 ip 15.15.15.15 module 4
Flags:
A - seen ack for syn/fin from src   a - seen ack for syn/fin from dst
```


Send document comments to vsg-docfeedback@cisco.com.

```

E - tcp conn established (SasA done)
F - seen fin from src          f - seen fin from dst
O - conn offloaded to vPath at src  o - conn offloaded to vPath at dst
P - policy at src              p - policy at 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

VSG IP 15.15.15.15 VLAN 159
#Module 4
Proto      SrcIP[:Port]  DstIP[:Port]  VLAN   Action   Flags   Bytes
icmp       10.100.201.176 10.100.201.185 160    permit  PpOo    53312

```

show vsn statistics [vlan vlan-num ip ip-addr] [module module-num]

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

This example shows how to display the VSN statistics:

```

vsm# show vsn statistics
#VSN VLAN: 756, IP-ADDR: 200.1.1.67
Module: 3
#VPath Packet Statistics      Ingress      Egress      Total
Total Seen                    381295      622662      1003957
Policy Redirects              0            120681      120681
No-Policy Passthru           14830       14835       29665
Policy-Permits Rcvd          0            120681      120681
Policy-Denies Rcvd           0            0            0
Permit Hits                   366465     487146      853611
Deny Hits                    0            0            0
Decapsulated                  0            120681      120681
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                                120681
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            120681 Forward Flow Destroy         120681
Reverse Flow Create            120681 Reverse Flow Destroy         120681
Flow ID Alloc                  241362 Flow ID Free                  241362
Connection ID Alloc            120681 Connection ID Free           120681
L2 Flow Create                 0 L2 Flow Destroy              0
L3 Flow Create                 0 L3 Flow Destroy              0
L4 TCP Flow Create             241362 L4 TCP Flow Destroy          241362
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            249934 L4 TCP Flow Offload          120681
L4 UDP Flow Timeout            0 L4 UDP Flow Offload          0

```

Send document comments to vsg-docfeedback@cisco.com.

```

L4 Oth Flow Timeout                0 L4 Oth Flow Offload                0
Flow Lookup Hit                    853611 Flow Lookup Miss                    241362
Flow Dual Lookup                    998732 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

Module: 4

#VPath Packet Statistics            Ingress          Egress           Total
Total Seen                          9886             9890             19776
Policy Redirects                     0                0                0
No-Policy Passthru                   9886             9890             19776
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                0                0
Non-Cisco Encap Rcvd                 0                0                0
VNS-Port Drops                       0                0                0
Policy-Action Err                     0                0                0
Decap Err                             0                0                0
L2-Frag Sent                          0                0                0
L2-Frag Rcvd                          0                0                0
L2-Frag Coalesced                    0                0                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

```

Send document comments to vsg-docfeedback@cisco.com.

```

Hash Alloc                0 Hash Free                0
InvalFID Lookup          0 InvalFID Lookup Err      0
Deferred Delete          0
vsm#

```

clear vsn statistics [vlan vlan-num ip ip-addr] [module module-num]

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

This example shows how to clear VSN statistics:

```

vsm# clear vsn statistics vlan 756 ip 200.1.1.67 module 3
Cleared statistics successfully for specified VSN in module 3
vsm-fcs# show vsn statistics vlan 756 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

```

Send document comments to vsg-docfeedback@cisco.com.

```

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
vsm#

```

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. There are three main tables: DV port table, VM table, and VNSP table. Use the **show vsg dvport** command to display runtime information for the DV port table. For the other two tables, use the **show vsg vm** and **show vsg vnsp** commands.

Hash tables are maintained based on IP addresses (IP address to DV port entry) and VNSP ID (VNSP ID to VNSP entry). An IP address is used when fetching attributes (custom and VM attributes) that are based on the source or destination IP address. It is also used to determine which policy set to evaluate for a given traffic type. The VNSP ID is used (valid VNSP ID in the packet header) to determine which policy set to evaluate. Custom attributes can also be fetched.

This section includes the following topics:

- [show vnm-pa status, page 2-20](#)
- [show service-path statistics, page 2-21](#)
- [clear service-path statistics, page 2-22](#)
- [show service-path connection, page 2-22](#)
- [clear service-path connection, page 2-23](#)
- [show vsg ip-binding, page 2-23](#)
- [show vsg dvport {dvport_id}, page 2-24](#)
- [show vsg vm name {name}, page 2-26](#)
- [show vsg security-profile \[{vnsp-name}\] detail | table, page 2-28](#)
- [show vsg zone, page 2-29](#)
- [clear policy-engine, page 2-30](#)
- [show ac-driver statistics, page 2-30](#)
- [clear ac-driver statistics, page 2-30](#)
- [show system internal ac ipc-stats fe \[process-name\], page 2-30](#)
- [clear system internal ac ipc-stats fe \[process-name\], page 2-31](#)
- [show inspect ftp statistics, page 2-31](#)
- [clear inspect ftp statistics, page 2-32](#)

show vnm-pa status

Enter the **show vnm-pa status** command to display the VNMC policy agent status.

This example shows how to display the VNMC policy agent status:

```

vsg# show vnm-pa status
VNMC Policy-Agent status is - Installed Successfully. Version 1.0(1j)-vsg

```

Send document comments to vsg-docfeedback@cisco.com.

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 svcs-domain specified in the *domain-id*.
- **module** *module-num*—Displays only the Cisco VSG connections that are associated to the svcs-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 display the statistics using the **svs-domain-id** keyword filter:

```
vsg# show service-path statistics svcs-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
```

Send document comments to vsg-docfeedback@cisco.com.

```

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
vsg#

```

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 svcs-domain specified in the *domain-id*.
- **module** *module-num*—Displays only the Cisco VSG connections that are associated to the svcs-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
vsg#

```

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 svcs-domain specified in the *domain-id*.
- **module** *module-num*—Displays only the Cisco VSG connections that are associated to the svcs-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 the output for the command:

```

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
icmp   10.100.201.176          10.100.201.185        160  permit  PpOo

#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

```

Send document comments to vsg-docfeedback@cisco.com.

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
vsg#
```

show vsg ip-binding

You can display a list of VM IP addresses and associated Virtual Network Service Profiles (VNSPs) with the associated policy set by using the **show vsg ip-binding** command. This information helps you to troubleshoot data path issues. The attribute manager determines which policy set to evaluate for a given packet (source IP address is the key for the lookup).

When debugging issues (for example, the wrong policy set or no policy), use this command to ensure that IP bindings (IP address to VNSP association) are correct. This association can also affect VNSP and VM attributes fetched by the attribute manager.

This example shows how to display the list of VM IP addresses and associated VNSPs:

```
vsn# show vsg-ip-binding
-----
VM IP address      Security-Profile Name      Policy Name
-----
100.1.246.6        sec-profile-one@root/Tenant-one  policysset-one@root/Tenant-one
100.1.246.5        sec-profile-one@root/Tenant-one  policysset-one@root/Tenant-one
100.1.246.4        sec-profile-one@root/Tenant-one  policysset-one@root/Tenant-one
100.1.246.3        sec-profile-one@root/Tenant-one  policysset-one@root/Tenant-one
100.1.246.2        sec-profile-one@root/Tenant-one  policysset-one@root/Tenant-one
100.1.246.1        sec-profile-one@root/Tenant-one  policysset-one@root/Tenant-one
100.1.246.10       sec-profile-one@root/Tenant-one  policysset-one@root/Tenant-one
100.1.246.9        sec-profile-one@root/Tenant-one  policysset-one@root/Tenant-one
100.1.246.8        sec-profile-one@root/Tenant-one  policysset-one@root/Tenant-one
100.1.246.7        sec-profile-one@root/Tenant-one  policysset-one@root/Tenant-one
vsn#
```

You can use the **show vsg ip-binding vm** command to show all IP VM bindings.

This example shows how to display all IP VM bindings:

```
vsg# show vsg ip-binding vm
-----
VM IP address      VM Name      Port Profile Name
-----
10.100.201.185     linux-206-185  profile_test2
10.100.201.176     linux-206-176  profile_test2
```

You can use the **show vsg ip-binding vm detail** command to see more details about the IP VM bindings.

This example shows how to display the details of the IP VM bindings:

```
vsg# show vsg ip-binding vm detail
VM IP address      : 10.100.201.185
VM Name           : linux-206-185
VM uuid           : 421cefd6-29d1-4c8e-e563-2c3a4d58cd31
DV Port           : 1209::1c7b1c50-f1b7-9a71-259d-820f4713a4b1
Port Profile      : profile_test2
```

Send document comments to vsg-docfeedback@cisco.com.

```
VM IP address   : 10.100.201.176
VM Name        : linux-206-176
VM uuid       : 421c44f9-91e0-b063-4fb0-ff3f4d736c3b
DV Port       : 1208::1c7b1c50-f1b7-9a71-259d-820f4713a4b1
Port Profile   : profile_test2
```

show vsg dvport {*dvport_id*}

You can display relevant information for a DV port by using the **show vsg dvport** command. A DV port is a logical representation of a vNIC. By default, this displays information for all DV ports. Specify a particular DV port with the *dvport id* parameter.

This example shows how to display the DV port information:

```
vsg# show vsg dvport

DV Port           : 576::bcaa1c50-8747-8d08-fe7e-a9aa8924bf8e
Security Profile  : spcustom
VM uuid          : 421c5ae4-51c3-5dd9-60fa-a50cb04ed0ea
Port Profile     : vm_data
IP Addresses     :
                  100.1.1.20
                  100.1.1.10
```

show vsg vm

You can display information for all VMs on a VSG by using the **show vsg vm** command. In addition to the existing VM information, zone names are displayed in the command output. DV port information is not display to limit verbosity.

This example shows how to display all VMs on a VSG:

```
firewall-1# show vsg vm
VM uuid          : 42031129-65af-976b-5c5c-509966ffdede
VM attributes :
  name           : gentoo-246-2
  vapp-name      :
  os-fullname    : other 2.6x linux (64-bit)
  tools-status   : not-installed
  host-name      : 10.193.77.246
  cluster-name   :

VM uuid          : 4203326d-91d1-2fba-838a-3a551e5bcce1
VM attributes :
  name           : gentoo-246-8
  vapp-name      :
  os-fullname    : other 2.6x linux (64-bit)
  tools-status   : not-installed
  host-name      : 10.193.77.246
  cluster-name   :

VM uuid          : 420392dd-1146-f8eb-f0cb-363fb999a02d
VM attributes :
  name           : gentoo-246-10
  vapp-name      :
  os-fullname    : other 2.6x linux (64-bit)
  tools-status   : not-installed
  host-name      : 10.193.77.246
  cluster-name   :

VM uuid          : 42036819-f763-342a-8833-c24f9c55261f
VM attributes :
```


Send document comments to vsg-docfeedback@cisco.com.

```
name : gentoo-246-4
vapp-name :
os-fullname : other 2.6x linux (64-bit)
tools-status : not-installed
host-name : 10.193.77.246
cluster-name :

VM uuid : 420374a0-a81d-fe72-1dd8-f7b4ece9194c
VM attributes :
name : gentoo-246-5
vapp-name :
os-fullname : other 2.6x linux (64-bit)
tools-status : not-installed
host-name : 10.193.77.246
cluster-name :

VM uuid : 4203625c-d9d0-1dde-228e-a2aaa97ad7c2
VM attributes :
name : gentoo-246-1
vapp-name :
os-fullname : other 2.6x linux (64-bit)
tools-status : not-installed
host-name : 10.193.77.246
cluster-name :

VM uuid : 42034686-db79-478a-920f-2dd2cce07151
VM attributes :
name : gentoo-246-7
vapp-name :
os-fullname : other 2.6x linux (64-bit)
tools-status : not-installed
host-name : 10.193.77.246
cluster-name :

VM uuid : 4203ac4a-a7f6-3320-436d-29a49c1c73e8
VM attributes :
name : gentoo-246-9
vapp-name :
os-fullname : other 2.6x linux (64-bit)
tools-status : not-installed
host-name : 10.193.77.246
cluster-name :

VM uuid : 42033483-18b1-a89f-2f24-ae142365f061
VM attributes :
name : gentoo-246-6
vapp-name :
os-fullname : other 2.6x linux (64-bit)
tools-status : not-installed
host-name : 10.193.77.246
cluster-name :

VM uuid : 420360fb-cfcc-21f0-b3dd-f3650ff37a6d
VM attributes :
name : gentoo-246-3
vapp-name :
os-fullname : other 2.6x linux (64-bit)
tools-status : not-installed
host-name : 10.193.77.246
cluster-name :
firewall-1#
```

Send document comments to vsg-docfeedback@cisco.com.

show vsg vm name {name}

You can display information of one or more VMs by entering the **show vsg vm name** command. The VM name should be specified as a parameter and can be the name or the first few characters of the name. The information for the VM includes the details of each DV port used by the VM and zones that the VM belongs to.

The following example shows how to display information for the VM with a name that starts with linux-204.

```
firewall-1# show vsg vm name linux-204
VM uuid      : 421ceac2-3b3f-67f9-b71c-3755d2c8cabe
VM attributes :
  cluster-name      : cluster23
  host-name         : 10.193.77.204
  name              : linux-204-184
  os-fullname       : red hat enterprise linux 4 (32-bit)
  os-hostname       :
  res-pool          : resources
  tools-status      : not-installed
  vapp-name         :
DV Port(s) :
  DV Port           : 272::1c7b1c50-f1b7-9a71-259d-820f4713a4b1
  Security Profile  : SP-DC1@root/Cisco-Tenant1
  Port Profile      : profile_App2
  IP Addresses     :
    20.100.201.184
  DV Port           : 240::1c7b1c50-f1b7-9a71-259d-820f4713a4b1
  Security Profile  : SP-App1@root/Cisco-Tenant1
  Port Profile      : profile_App1
  IP Addresses     :
    10.100.201.184
Zone(s) :
  zone_linux_204@root/Cisco-Tenant1

firewall-1#
```

show vsg vm uuid {vm_uuid}

You can display relevant information for a particular VM by using the **show vsg vm uuid** 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:

```
firewall-1# show vsg vm uuid
VM uuid      : 42031129-65af-976b-5c5c-509966ffdede
VM attributes :
  name            : gentoo-246-2
  vapp-name       :
  os-fullname     : other 2.6x linux (64-bit)
  tools-status    : not-installed
  host-name       : 10.193.77.246
  cluster-name    :
VM uuid      : 4203326d-91d1-2fba-838a-3a551e5bccel
VM attributes :
```

Send document comments to vsg-docfeedback@cisco.com.

```
name : gentoo-246-8
vapp-name :
os-fullname : other 2.6x linux (64-bit)
tools-status : not-installed
host-name : 10.193.77.246
cluster-name :

VM uuid : 420392dd-1146-f8eb-f0cb-363fb999a02d
VM attributes :
name : gentoo-246-10
vapp-name :
os-fullname : other 2.6x linux (64-bit)
tools-status : not-installed
host-name : 10.193.77.246
cluster-name :

VM uuid : 42036819-f763-342a-8833-c24f9c55261f
VM attributes :
name : gentoo-246-4
vapp-name :
os-fullname : other 2.6x linux (64-bit)
tools-status : not-installed
host-name : 10.193.77.246
cluster-name :

VM uuid : 420374a0-a81d-fe72-1dd8-f7b4ece9194c
VM attributes :
name : gentoo-246-5
vapp-name :
os-fullname : other 2.6x linux (64-bit)
tools-status : not-installed
host-name : 10.193.77.246
cluster-name :

VM uuid : 4203625c-d9d0-1dde-228e-a2aaa97ad7c2
VM attributes :
name : gentoo-246-1
vapp-name :
os-fullname : other 2.6x linux (64-bit)
tools-status : not-installed
host-name : 10.193.77.246
cluster-name :

VM uuid : 42034686-db79-478a-920f-2dd2cce07151
VM attributes :
name : gentoo-246-7
vapp-name :
os-fullname : other 2.6x linux (64-bit)
tools-status : not-installed
host-name : 10.193.77.246
cluster-name :

VM uuid : 4203ac4a-a7f6-3320-436d-29a49c1c73e8
VM attributes :
name : gentoo-246-9
vapp-name :
os-fullname : other 2.6x linux (64-bit)
tools-status : not-installed
host-name : 10.193.77.246
cluster-name :

VM uuid : 42033483-18b1-a89f-2f24-ae142365f061
VM attributes :
name : gentoo-246-6
```

Send document comments to vsg-docfeedback@cisco.com.

```

vapp-name          :
os-fullname        : other 2.6x linux (64-bit)
tools-status       : not-installed
host-name          : 10.193.77.246
cluster-name       :

VM uuid           : 420360fb-cfcc-21f0-b3dd-f3650ff37a6d
VM attributes :
  name            : gentoo-246-3
  vapp-name       :
  os-fullname     : other 2.6x linux (64-bit)
  tools-status    : not-installed
  host-name       : 10.193.77.246
  cluster-name    :
firewall-1#

```

show vsg security-profile *[[vnsf-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 *vnsf-name* argument.

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

The detail 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.

The following 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

```

```
firewall-1#
```

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

```

Send document comments to vsg-docfeedback@cisco.com.

```
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

firewall-tenant-aa#
```

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 : zone2@root/test34
Virtual Machines :
linux-206-185
-----
Zone : zone1@root/test34
Virtual Machines :
linux-206-176
-----
```

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)

firewall-1#
```

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)

firewall-1#
```

Send document comments to vsg-docfeedback@cisco.com.

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
firewall-1#
```

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
firewall-1#
```

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.
vsg#
```

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

Send document comments to vsg-docfeedback@cisco.com.

- 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
=====

firewall-1#
```

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-ftp
firewall-1#
```

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 the FTP statistics:

Send document comments to vsg-docfeedback@cisco.com.

```

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

firewall-1#

```

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:

Send document comments to vsg-docfeedback@cisco.com.

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

Send document comments to vsg-docfeedback@cisco.com.