Monitoring the System

The ASA FirePOWER module provides many useful monitoring features to assist you in the daily administration of your system, all on a single page. For example, on the Host Statistics page you can monitor basic host statistics.

Viewing Host Statistics

License: Any

The **Statistics** page lists the current status of the following:

- general host statistics; see the Table 1: Host Statistics , on page 1 table for details
- intrusion event information (requires Protection); see Viewing Events or details

The following table describes the host statistics listed on the Statistics page.

Table 1: Host Statistics

Category	Description
Time	The current time on the system.
Uptime	The number of days (if applicable), hours, and minutes since the system was last started.
Memory Usage	The percentage of system memory that is being used.
Load Average	The average number of processes in the CPU queue for the past 1 minute, 5 minutes, and 15 minutes.
Disk Usage	The percentage of the disk that is being used. Click the arrow to view more detailed host statistics. See Monitoring System Status and Disk Space Usage, on page 2 for more information.

Category	Description
Processes	A summary of the processes running on the system. See Monitoring System Status and Disk Space Usage, on page 2 for more information.

To view the Statistics page:

Select **Monitoring** > **ASA FirePOWER Monitoring** > **Statistics**.

The **Statistics** page appears.

Monitoring System Status and Disk Space Usage

License: Any

The **Disk Usage** section of the Statistics page provides a quick synopsis of disk usage, both by category and by partition status. If you have a malware storage pack installed on a device, you can also check its partition status. You can monitor this page from time to time to ensure that enough disk space is available for system processes and the database.

To access disk usage information:

Step 1 Select **Monitoring** > **ASA FirePOWER Monitoring** > **Statistics**.

The **Statistics** page appears.

For more information on the disk usage categories, see Understanding the Disk Usage Widget.

Step 2 Click the down arrow next to **Total** to expand it.

The **Disk Usage** section expands, displaying partition usage. If you have a malware storage pack installed, the /var/storage partition usage is also displayed.

About System Process Status

License: Any

The **Processes** section of the Host Statistics page allows you to see the processes that are currently running on an appliance. It provides general process information and specific information for each running process.

The following table describes each column that appears in the process list.

Table 2: Process Status

Column	Description
Pid	The process ID number

Column	Description
Username	The name of the user or group running the process
Pri	The process priority
Nice	The *nice* value, which is a value that indicates the scheduling priority of a process. Values range between -20 (highest priority) and 19 (lowest priority)
Size	The memory size used by the process (in kilobytes unless the value is followed by m , which indicates megabytes)
Res	The amount of resident paging files in memory (in kilobytes unless the value is followed by m , which indicates megabytes)
State	The process state: • D — process is in uninterruptible sleep (usually Input/Output) • N — process has a positive nice value • R — process is runnable (on queue to run) • S — process is in sleep mode • T — process is being traced or stopped • W — process is paging • X — process is dead • Z — process is defunct • < — process has a negative nice value
Time	The amount of time (in hours:minutes:seconds) that the process has been running
Cpu	The percentage of CPU that the process is using
Command	

Viewing System Process Status

The executable name of the process

To expand the process list:

Step 1 Select **Monitoring** > **ASA FirePOWER Monitoring** > **Statistics**.

The **Statistics** page appears.

Step 2 Click the down arrow next to **Processes**.

The process list expands, listing general process status information that includes the number and types of running tasks, the current time, the current system uptime, the system load average, CPU, memory, and swap information, and specific information about each running process.

Cpu(s) lists the following CPU usage information:

- user process usage percentage
- system process usage percentage
- nice usage percentage (CPU usage of processes that have a negative nice value, indicating a higher priority)

Nice values indicate the scheduled priority for system processes and can range between -20 (highest priority) and 19 (lowest priority).

- idle usage percentage

Mem lists the following memory usage information:

- total number of kilobytes in memory
- total number of used kilobytes in memory
- total number of free kilobytes in memory
- total number of buffered kilobytes in memory

Swap lists the following swap usage information:

- total number of kilobytes in swap
- total number of used kilobytes in swap
- total number of free kilobytes in swap
- total number of cached kilobytes in swap

Note For more information about the types of processes that run on the appliance, see Understanding Executables and System Utilities, on page 6.

What to do next

To collapse the process list:

Click the up arrow next to **Processes**.

The process list collapses.

Understanding Running Processes

License: Any

There are two different types of processes that run on an appliance: daemons and executable files. Daemons always run, and executable files are run when required.

Understanding System Daemons

License: Any

Daemons continually run on an appliance. They ensure that services are available and spawn processes when required. The following table lists daemons that you may see on the Process Status page and provides a brief description of their functionality.

Note The table below is not an exhaustive list of all processes that may run on an appliance.

Table 3: System Daemons

Daemon	Description
crond	Manages the execution of scheduled commands (cron jobs)
dhclient	Manages dynamic host IP addressing
httpd	Manages the HTTP (Apache web server) process
httpsd	Manages the HTTPS (Apache web server with SSL) service, and checks for working SSL and valid certificate authentication; runs in the background to provide secure web access to the appliance
keventd	Manages Linux kernel event notification messages
klogd	Manages the interception and logging of Linux kernel messages
kswapd	Manages Linux kernel swap memory
kupdated	Manages the Linux kernel update process, which performs disk synchronization
mysqld	Manages ASA FirePOWER module database processes
ntpd	Manages the Network Time Protocol (NTP) process
pm	Manages all Cisco processes, starts required processes, restarts any process that fails unexpectedly
reportd	Manages reports
safe_mysqld	Manages safe mode operation of the database; restarts the database daemon if an error occurs and logs runtime information to a file
sfmgr	Provides the RPC service for remotely managing and configuring an appliance using an sftunnel connection to the appliance
sftroughd	Listens for connections on incoming sockets and then invokes the correct executable (typically the Cisco message broker, sfmb) to handle the request
sftunnel	Provides the secure communication channel for all processes requiring communication with a remote appliance
sshd	Manages the Secure Shell (SSH) process; runs in the background to provide SSH access to the appliance
syslogd	Manages the system logging (syslog) process

Understanding Executables and System Utilities

License: Any

There are a number of executables on the system that run when executed by other processes or through user action. The following table describes the executables that you may see on the Process Status page

Table 4: System Executables and Utilities

Executable	Description
awk	Utility that executes programs written in the awk programming language
bash	GNU Bourne-Again SHell
cat	Utility that reads files and writes content to standard output
chown	Utility that changes user and group file permissions
chsh	Utility that changes the default login shell
cp	Utility that copies files
df	Utility that lists the amount of free space on the appliance
echo	Utility that writes content to standard output
egrep	Utility that searches files and folders for specified input; supports extended set of regular expressions not supported in standard grep
find	Utility that recursively searches directories for specified input
grep	Utility that searches files and directories for specified input
halt	Utility that stops the server
httpsdctl	Handles secure Apache Web processes
hwclock	Utility that allows access to the hardware clock
ifconfig	Indicates the network configuration executable. Ensures that the MAC address stays constant
iptables	Handles access restriction based on changes made to the Access List page. See Configuring the Access List for Your Appliance for more information about access configuration.
iptables-restore	Handles iptables file restoration
iptables-save	Handles saved changes to the iptables
kill	Utility that can be used to end a session and process
killall	Utility that can be used to end all sessions and processes
ksh	Public domain version of the Korn shell

Executable	Description
logger	Utility that provides a way to access the syslog daemon from the command line
md5sum	Utility that prints checksums and block counts for specified files
mv	Utility that moves (renames) files
myisamchk	Indicates database table checking and repairing
mysql	Indicates a database process; multiple instances may appear
openssl	Indicates authentication certificate creation
perl	Indicates a perl process
ps	Utility that writes process information to standard output
sed	Utility used to edit one or more text files
sh	Public domain version of the Korn shell
shutdown	Utility that shuts down the appliance
sleep	Utility that suspends a process for a specified number of seconds
smtpclient	Mail client that handles email transmission when email event notification functionality is enabled
snmptrap	Forwards SNMP trap data to the SNMP trap server specified when SNMP notification functionality is enabled
snort(requires Protection)	Indicates that Snort is running
ssh	Indicates a Secure Shell (SSH) connection to the appliance
sudo	Indicates a sudo process, which allows users other than admin to run executables
top	Utility that displays information about the top CPU processes
touch	Utility that can be used to change the access and modification times of specified files
vim	Utility used to edit text files
wc	Utility that performs line, word, and byte counts on specified files