# Secure Firewall Threat Defense Device Metrics Collected by the Secure Firewall Management Center Health Monitor, Version 7.4.x

**First Published:** 2023-09-07

**Last Modified:** 2023-12-13

## Secure Firewall Threat Defense Device Metrics Collected by the Secure Firewall Management Center Health Monitor

The device health monitor includes an array of key threat defense device metrics that serve to predict and respond to system events. The health of any threat defense device can be determined by these reported metrics. This document provides a list of all the health monitor dashboards and the reported metrics.

## CPU Group Metrics

The health monitor tracks statistics related to the CPU utilization, including the CPU usage by process and by physical cores.

***Table 1: CPU Group Metrics***

| Metric | Description | Format |
|---|---|---|
| Control Delegate Plane | The average CPU usage by the control delegate plane. | percentage |
| Control Plane | The average CPU utilization for the control plane, for the last one minute. | percentage |
| Data Plane | The average CPU utilization for the data plane, for the last one minute. | percentage |
| Snort | The average CPU utilization for the Snort process, for the last one minute. | percentage |
| System | The average CPU utilization for the system processes, for the last one minute. | percentage |
| Physical cores | The average CPU utilization for all the cores, for the last one minute. | percent |

# Memory Group Metrics

The health monitor tracks statistics related to the device memory utilization, including data plane and Snort memory usage.

***Table 2: Memory Group Metrics***

| Metric | Description | Format |
|---|---|---|
| Buffer cache | The buffer cache memory used. | bytes |
| Free | The free memory available. | bytes |
| Maximum Data Plane | The maximum memory used by the data plane. | bytes |
| Maximum Snort | The maximum memory used by the Snort process. | bytes |
| Maximum Swap for Snort | The maximum swap memory used by the Snort process. | bytes |
| Remaining Memory Block (1550) | The free memory in a 1550 byte block. | number |
| Remaining Memory Block (256) | The free memory in a 256 byte block. | number |
| Remaining Memory Block (4) | The free memory in a 4 byte block. | number |
| Remaining Memory Block (80) | The free memory in a 80 byte block. | number |
| Remaining Memory Block (2048) | The free memory in a 2048 byte block. | number |
| Remaining Memory Block (2560) | The free memory in a 2560 byte block. | number |
| Remaining Memory Block (4096) | The free memory in a 4096 byte block. | number |
| Remaining Memory Block (8192) | The free memory in a 8192 byte block. | number |
| Remaining Memory Block (9344) | The free memory in a 9344 byte block. | number |
| Remaining Memory Block (16384) | The free memory in a 16384 byte block. | number |
| Remaining Memory Block (65664) | The free memory in a 65664 byte block. | number |
| System Used | The average memory used by the system. | bytes |
| Total | The total memory available. | bytes |
| Total Swap | The total swap memory available. | bytes |
| Data Plane | The total memory used by the data plane. | bytes |
| Percent Used by Data Plane | The percent of memory used by the data plane. | percent |
| Percent Used by Snort | The percent of memory used by the Snort process. | percent |
| Percent Used for Swap | The percent of swap memory used. | percent |

| Metric | Description | Format |
|---|---|---|
| Percent Used by System | The percent of memory used by the system. | percent |
| Percent Used by System and Swap | The percent of memory used by the system and swap combined. | percent |
| Snort | The total memory used by the Snort process. | bytes |
| Used Swap | The total swap memory used. | bytes |
| Used Swap by Snort | The total swap memory used by the Snort process. | bytes |

# Interface Group Metrics

The health monitor tracks statistics related to the device interfaces, including the interface status and aggregate traffic statistics.

*Table 3: Interface Group Metrics*

| Metric | Description | Format |
|---|---|---|
| Drop Packets | The number of packets dropped. | number |
| Average Input Packet Size | The average size of incoming packets. | bytes |
| Input Rate | The total incoming bytes. | bytes |
| Input Throughput | The total incoming bytes processed per second. | bytes |
| Input Packets | The total incoming packets. | number |
| Average Output Packet Size | The average size of outgoing packets. | bytes |
| Output Rate | The total outgoing bytes. | bytes |
| Output Throughput | The total outgoing bytes processed per second. | bytes |
| Output Packets | The total outgoing packets. | number |
| Status | The status of an interface; 1 for up and 0 for down. | 1 or 0 |
| CRC Errors | Total number of packets received with CRC (Cyclic Redundancy Check) errors. | number |
| Input Error | Number of input errors. | number |
| Output Error | Number of output errors. | number |
| Overrun Errors | Number packets dropped due to input rate exceeded the receiver's capability to handle the incoming data. | number |
| Underrun Errors | Number packet dropped due to the transmitter is running faster than the router can handle. | number |

| Metric | Description | Format |
|---|---|---|
| L2 Decode Drops | Number of packets dropped due to name is not configured (nameif command) or a frame with an invalid VLAN id is received. | number |
| Jitter | Variation in latency of packet flow. | microseconds |
| Mean Opinion Score (MOS) | The measure of the quality of a connection, ranges from 0 to 5, where 5 is the best. | 0 to 5 |
| Packet Loss | Percentage of the transmitted packets not reaching the destination. | percentage |
| Round Trip Time | Average duration between ICMP echo request and response. | microseconds |

# Connection Group Metrics

The health monitor tracks statistics related to the connections and NAT translation counts.

***Table 4: Connection Group Metrics***

| Metric | Description | Format |
|---|---|---|
| Active Elephant Flows | Shows the number of active elephant flows.<br>Elephant flows are connections that are large enough to affect overall system performance. By default, elephant flows are those larger than 1GB/10 seconds. You can adjust the byte and time thresholds for identifying elephant flows in the threat defense CLI using the **system support elephant-flow-detection** command.<br>**Note** A flow is considered an elephant flow only when both the byte and time thresholds are surpassed. | number |
| Active connections | Shows the number of active connections. | number |
| Peak Connections | Shows the maximum number of simultaneous connections. | number |
| Total Connections per second | The connections-per-second for all connection types. | number |
| TCP Connections per second | The connections-per-second for TCP connection types. | number |
| UDP Connections per second | The connections-per-second for UDP connection types. | number |

| Metric | Description | Format |
|---|---|---|
| Preserve Connections Enabled | Preserves existing TCP/UDP connections on routed and transparent interfaces in case the Snort process goes down. | number |
| Connections Preserved | Connections for which preserve-connection is currently enabled. | number |
| Preserve Connections Most Enabled | The most number of connections ever preserved. | number |
| Peak Connections Preserved | The most number of peak connections ever preserved. | number |
| NAT Translations | Displays the translation count. | number |
| Peak NAT Translations | Displays the historic maximum of concurrent translations at a time. | number |

# Snort Group Metrics

The health monitor tracks statistics related to the Snort process.

*Table 5: Snort Group Metrics*

| Metric | Description | Format |
|---|---|---|
| Blocked list flows. | The number of flows from policy configuration that were dropped by Snort. | number |
| Blocked packets. | The number of blocked packets. | number |
| Denied flows. | The number of denied flow events. The data plane sends denied flow events to Snort when it decides to drop a flow before sending it to Snort. | number |
| End of flows. | The data plane sends end-of-flow events to Snort when a fast path flow ends. | number |
| Fast forwarded flows. | The number of flows that were fast forwarded by policy, and thus not inspected. | number |
| Packets forwarded to snort before drop. | The number of to-be-dropped packets forwarded to snort. | number |
| Injected packets dropped. | The number of packets that Snort added to the traffic stream that were dropped. | number |
| Injected packets. | The number of packets Snort created and added to the traffic stream. For example, if you configure a block with reset action, Snort generates packets to reset the connection. | number |

| Metric | Description | Format |
|---|---|---|
| Instances. | The number of snort instances (processes). | number |
| Packet receive queue utilization percentage. | The queue utilization percentage for the data-plane receive queue. | percent |
| Packet Transmit queue utilization percentage. | The queue utilization percentage for the data-plane transmit queue. | percent |
| Packets bypassed due to Snort busy. | The number of packets that bypassed inspection when Snort was too busy to handle the packets. | number |
| Packets bypassed due to Snort down. | The number of packets that bypassed inspection when Snort was down. | number |
| Packets bypassed due to RX queue full. | The number of packets bypassed due to a receive queue full. | number |
| Packets bypassed due to TX queue full. | The number of packets bypassed due to a transmit queue full. | number |
| Passed packets. | The number of packets sent to Snort from the data plane. | number |
| Start of flows. | The number of start-of-flow events. These events help Snort keep track of the connections and report the connection events. | number |

# ASP Drop Metrics

The health monitor tracks statistics related to the accelerated security path (ASP) dropped packets or connections.

Following table describes the list of general ASP drop dashboard metrics. For more information about the list of all the ASP drop dashboard metrics, see the Show ASP Drop Command Usage document.

*Table 6: ASP Drop Metrics*

| Metric | Description | Format |
|---|---|---|
| Connection limit exceeded | Counts the number of flows closed when the connection limit has been exceeded. | number |
| Connection limit reached | Counts the number of dropped packets when the connection limit or host connection limit has been exceeded. | number |
| Flow denied by access rule | Number of connections that are denied by access rule. | number |
| Flow denied by configured rule | Number of connections that are denied by configured rule. | number |

| Metric | Description | Format |
|---|---|---|
| L2 rule drop | Counts the number of denied packets due to a Layer 2 ACL. | number |
| L2 rule VXLAN drop | Counts the number of denied packets due to a failure to locate a VXLAN out_tag when applying Layer 2 ACL checks. | number |
| NAT reverse path failed | Counts the number of rejected attempts to connect to a translated host using the translated host's real address. | number |
| NAT failed | Counts the number of failed attempts to create an xlate to translate an IP or transport header. | number |
| No valid v4 adjacency | Counts the number of dropped packets when the security appliance has tried to obtain an adjacency and could not obtain mac-address for next hop (IPv4). | number |
| No valid v6 adjacency | Counts the number of dropped packets when the security appliance has tried to obtain an adjacency and could not obtain mac-address for next hop (IPv6). | number |
| Packet blocklisted by Snort; Packet blocked by Snort | Counts the number of packets dropped as requested by the Snort module. | number |
| Frame drops – Snort busy; Frame drops – Snort down; Frame drops – Snort drop | Counts the number of frames dropped as the Snort module is busy and unable to handle the frame; the Snort module is down; the Snort module requests the drop. | number |
| Dispatch queue limit reached | Counts the number of times a device's load balance ASP dispatcher reaches its queue limit. When more packets are attempted, tail drop occurs and this counter is incremented. | number |
| Destination MAC L2 lookup failed | Counts the number of Layer 2 destination MAC address lookups which fail. Upon the lookup failure, the appliance will begin the destination MAC discovery process and attempt to find the location of the host via ARP and/or ICMP messages. | number |
| Inspection failure | Counts the number of times the appliance fails to enable protocol inspection carried out by the network processor for the connection. The cause could be memory allocation failure, or for ICMP error message, the appliance not being able to find any established connection related to the frame embedded in the ICMP error message. | number |

| Metric | Description | Format |
|---|---|---|
| NAT no xlate to PAT pool | Counts no pre-existing xlate found for a connection with a destination matching a mapped address in a PAT pool. | number |
| No routes to host | Number of times the security appliance tries to send a packet out of an interface and does not find a route for it in routing table. | number |
| PDTS punt limit exceeded | Number of packet dropped when datapath punts packets to inspectors and the no. of packets queued to snort exceeded the maximum limit. | number |
| Punt limit | Number of packets dropped due to packets queued for the inspection reached the limit. | number |
| Snort silent drop | Number of times a packet is dropped silently as requested by the Snort module. | number |
| First TCP packet not in SYN | Number of times a non SYN packet is received as the first packet of a non intercepted and non nailed connection. | number |

# Hardware/Environment Status Metrics

The Hardware / Environment health monitor tracks statistics and collects metric values that are related to the threat defense hardware entities.

*Table 7: Hardware / Environment Status Metrics*

| Metric | Description | Format |
|---|---|---|
| Fan Speed | Speed of chassis fan(s). | RPM |
| Inlet Temperature | Temperature of the inlet sensor. | Celsius |
| Internal Temperature | Temperature of the internal sensor. | Celsius |
| Outlet Temperature | Temperature of the outlet sensor(s). | Celsius |
| Power Supply Unit Temperature | Temperature of the Power Supply Unit(s). | Celsius |
| Power Supply Unit Fan Speed | Speed of Power Supply Unit fan(s). | RPM |
| Power Supply Unit Input Current | Input current of the Power Supply Unit(s). | Ampere |
| Power Supply Unit Input Voltage | Input voltage of the Power Supply Unit(s). | Volt |
| Power Supply Unit Input Power | Input power of the Power Supply Unit(s). | Watt |
| Power Supply Unit Input Status | Input status of the Power Supply Unit(s). | Boolean |

| Metric | Description | Format |
|---|---|---|
| Power Supply Unit Output Power | Output power of the Power Supply Unit(s). | Watt |
| Power Supply Unit Fan Status | Status of the Power Supply Unit fans(s). | Boolean |
| SSD1 | Status of SSD1. | number |
| System Uptime | Duration for which the system is active. | seconds |
| Thermal Status | Power supply status of the device, where 1 represents up-state and 0 represents down-state. | 1 or 0 |

The availability of Hardware / Environment status metrics can vary depending on the model of the threat defense device. The following table describes the metrics available for each device model.

*Table 8: Hardware / Environment Status Metrics per Device Model*

| Metric | 1000 Series | 2100 Series | 3100 Series | 4100 Series | 4200 Series | 9300 Series | SSP |
|---|---|---|---|---|---|---|---|
| System Uptime | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| Fan Speed | Yes | Yes | Yes | No | Yes | No | No |
| Power Supply Unit Temperature | No | No | Yes | No | Yes | No | No |
| Power Supply Unit Fan Speed | No | No | Yes | No | Yes | No | No |
| Power Supply Unit Fan Status | Yes | No | Yes | No | Yes | No | No |
| Power Supply Unit Input Current | No | No | Yes | No | Yes | No | No |
| Power Supply Unit Input Voltage | No | No | Yes | No | Yes | No | No |
| Power Supply Unit Input Power | No | No | Yes | No | Yes | No | No |
| Power Supply Unit Input Status | Yes | Yes | Yes | No | Yes | No | No |
| Power Supply Unit Output Power | No | No | Yes | No | Yes | No | No |
| Internal Temperature | Yes | Yes | Yes | No | Yes | No | No |
| Inlet Temperature | No | No | No | No | No | No | No |
| Outlet Temperature | No | No | No | No | No | No | No |
| SSD1 Status | Yes | Yes | Yes | No | Yes | No | No |
| Thermal Status | No | No | No | Yes | No | Yes | Yes |

# Deployed Configuration Group Metrics

The health monitor tracks statistics related to the deployed configuration, such as the number of IPS rules and the number of ACEs.

*Table 9: Deployed Configuration Group Metrics*

| Metric | Description | Format |
|---|---|---|
| Number of ACEs | The number of access control entries (ACE), or rules. An access control list (ACL) is composed of one or more ACEs. | number |
| Number of rules | The number of rules in an intrusion policy. | number |

# Disk Group Metrics

The health monitor tracks statistics related to the device disk usage, including the disk size and disk utilization per partition.

*Table 10: Disk Group Metrics*

| Metric | Description | Format |
|---|---|---|
| Total | The total size of the device disk. | bytes |
| Used | The total space used on the device disk. | bytes |
| Used Percentage by /ngfw | The percent of disk space used by the /ngfw partition. | percentage |
| Used Percentage by /ngfw/Volume | The percent of disk space used by the /ngfw/Volume partition. | percentage |
| Used Percentage by /dev/cgroups | The percent of disk space used by the /dev/cgroups partition. | percentage |
| Used Percentage by /mnt/disk0 | The percent of disk space used by the /mnt/disk0 partition. | percentage |
| Used Percentage by /var/volatile | The percent of disk space used by the /var/volatile partition. | percentage |

# Critical Process Group Metrics

The health monitor tracks statistics related to process restarts for managed processes. In addition, for each critical process, the health monitor tracks CPU utilization, memory utilization, uptime, and status.

*Table 11: Critical Process Group Metrics*

| Metric | Description | Format |
|---|---|---|
| CPU utilization | The CPU utilization for the process since the start of the process. | percent |
| Restart count | Number of times the process has restarted since the threat defense device boot up.<br>Note that if the process restarts too frequently, the restart count metric may not reflect the exact number as this metric runs for every minute. | number |
| Unexpected Restart Count | Number of time the process has restarted unexpectedly, since the threat defensedevice boot up. | number |
| Status | Status of the process. | One of the following:<br>• Started<br>• Running<br>• Down<br>• Waiting<br>• Locked<br>• Disabled<br>User Disabled |
| Uptime | Duration for which the process is running. | seconds |
| Memory used | RSS memory used by the process. | bytes |

# Cluster Metrics

The cluster health monitor tracks statistics that are related to a cluster and its nodes, and aggregate of load distribution, performance, and CCL traffic statistics.

*Table 12: Cluster Metrics*

| Metric | Description | Format |
|---|---|---|
| CPU | Average of CPU metrics on the nodes of a cluster (individually for data plane and snort). | percentage |
| Memory | Average of memory metrics on the nodes of a cluster (individually for data plane and snort). | percentage |

| Metric | Description | Format |
|---|---|---|
| Data Throughput | Incoming and outgoing data traffic statistics for a cluster. | bytes |
| CCL Throughput | Incoming and outgoing CCL traffic statistics for a cluster. | bytes |
| Connections | Count of active connections in a cluster. | number |
| NAT Translations | Count of NAT translations for a cluster. | number |
| Distribution | Connection distribution count in the cluster for every second. | number |
| Packets | Packet distribution count in the cluster for every second. | number |

# NTP server group metric

The health monitor tracks statistics related the NTP clock synchronization status of the managed device.

***Table 13: NTP Server Group Metrics***

| Metric | Description | Format |
|---|---|---|
| Delay | Delay in reaching the NTP server. | milliseconds |
| Jitter | Network latency between the device and the NTP server. | milliseconds |
| Last polled | Time since the device's last poll to the NTP server. | seconds |
| Offset | Time difference between the local clock and the NTP server's clock. | seconds |
| Reach | Most recent eight NTP updates in octal number. For example, eight successful attempts is represented by 377. | number |

# Flow Offload Statistics Group Metrics

Health monitoring tracks the hardware flow offload statistics on the Threat Defense 9300 and 4100 platforms.

***Table 14: Flow Offload Statistics Group Metrics***

| Metric | Description | Format |
|---|---|---|
| In Use | Number of flows that are offloaded at the moment. | number |
| Most Used | Maximum number of offloaded flows seen up to now. | number |

| Metric | Description | Format |
|---|---|---|
| Number of Collision Flows | Number of multiple flows matching the same hardware offload location at the same time. | number |
| Offload Percentage | Percentage of total flows offloaded to the hardware at the moment. | percentage |

# Route Statistics Group Metrics

Health monitor tracks both the IPv4 and IPv6 route information from the threat defense device.

*Table 15: Route Statistics Group Metrics*

| Metric | Description | Format |
|---|---|---|
| Current IPv4 and IPv6 routes | Count of current IPv4 and IPv6 routes. | number |
| Global IPv4 routes | Global IPv4 routes. | number |
| Global IPv6 routes | Global IPv6 routes. | number |
| Peak IPv4 and IPv6 routes | Peak route count for IPv4 and IPv6. | number |
| Per VRF Total IPv4 routes | Total number of IPv4 routes per VRF. | number |
| Per VRF Total IPv6 routes | Total number of IPv6 routes per VRF. | number |

# VPN Group Metrics

Health monitoring tracks site-to-site and remote access VPN tunnel statistics.

*Table 16: VPN Group Metrics*

| Metric | Description | Format |
|---|---|---|
| Active RA VPN Tunnels | Number of active remote access VPN tunnels. | number |
| Active S2S VPN Tunnels | Number of active site-to-site VPN tunnels. | number |
| Cumulative RA VPN Sessions | Total number of remote access VPN tunnels which were active until now. | number |
| Cumulative S2S VPN Sessions | Total number of site-to-site VPN tunnels which were active until now. | number |
| Inactive RA VPN Tunnels | Number of inactive remote access VPN tunnels. | number |
| Peak Concurrent RA VPN Tunnels | Peak number of remote access VPN tunnels which were simultaneously active until now. | number |

| Metric | Description | Format |
|---|---|---|
| Peak Concurrent S2S VPN Tunnels | Peak number of site-to-site VPN tunnels which were simultaneously active until now. | number |

# TLS Counters Group Metric

The health monitoring tracks the XTLS flows, memory, and cache effectiveness.

*Table 17: Connection Group Metrics*

| Metric | Description | Format |
|---|---|---|
| Allocation failures. | Shows the number of allocation failures due to decryption or re-encryption running out of DMA memory per second. | number |
| Cache effectiveness. | The rate of overall cache hits to the cache look-ups. | percentage |
| Cache entries. | Cache entries of the total cache summary per second. | number |
| Cache evictions. | Cache evictions of the total cache summary per second. | number |
| Cache hits. | Cache look-up hits for all caches per second. | number |
| Cache miss. | Cache look-up misses for all caches per second. | number |
| Cache added. | Number of items added to all caches per second. | number |
| Certificate validation cache. | The ratio of certificate validation cache hits to cache look-ups. | percentage |
| Client hello digest cache. | The ratio of client hello digest cache hits to cache look-ups. | percentage |
| Original certificate cache. | The ratio of original certificate cache hits to cache look-ups. | percentage |
| Replaced key certificate cache. | The ratio of replaced key cache hits to cache look-ups. | percentage |
| Resigned certificate cache. | The ratio of resigned key cache hits to cache look-ups. | percentage |
| Session ID cache. | The ratio of session ID cache hits to cache look-ups. | percentage |
| Session ticket cache. | The ratio of session ticket cache hits to cache look-ups. | percentage |
| RSA SCB allocation failures. | The number of allocation failures due to crypto operations running out of resources for an RSA key operation per second. | number |

| Metric | Description | Format |
|---|---|---|
| SCB allocation failures. | The number of allocation failures due to crypto operations running out of resources for payload decryption per second. | number |
| SNI cache. | The ratio of SNI cache hits to cache look-ups. | percentage |
| Upstream record check errors. | Number of bad TLS records from the client or server received by the device per second. | number |

## AMP Connectivity Group Metrics

Health monitoring tracks the AMP cloud connectivity status from the threat defense device.

*Table 18:*

| Metric | Description | Format |
|---|---|---|
| Connection Status | AMP cloud connection status. | number ranging from 0 to 5 where:<br>• 0 indicates Disabled.<br>• 1 indicates Waiting.<br>• 2 indicates Running.<br>• 3 indicates Not configured.<br>• 4 indicates AMP cloud connection ON.<br>• 5 indicates AMP cloud connection OFF. |

## AMP Threat Grid Connectivity Group Metrics

Health monitoring tracks the AMP Threat Grid cloud connectivity status from the threat defense device.

*Table 19:*

| Metric | Description | Format |
|---|---|---|
| Connection Status | AMP Threat Grid cloud connection status. | number ranging from 0 to 5 where:<br>• 0 indicates Disabled.<br>• 1 indicates Waiting.<br>• 2 indicates Running.<br>• 3 indicates Not configured.<br>• 4 indicates AMP Threat Grid cloud connection ON.<br>• 5 indicates AMP Threat Grid cloud connection OFF. |

# History for Device Health Metrics

| Feature | Version | Details |
|---|---|---|
| New memory metrics. | 7.41 | Added new metrics to track the free memory in blocks of 4, 80, 2048, 2560, 4096, 8192, 9344, 16384, and 65664 bytes. |
| ASP drop visibility improvement. | 7.4.0 | Added new health metrics to the ASP Drop dashboard, which provides enhanced visibility of ASP drops. The new metrics enable you to monitor additional reasons for packet and connection drops. |
| New cluster health monitor dashboard. | 7.3 | A new dashboard to view the cluster health monitor metrics was introduced with the following components:<br>• Overview—Displays information about the cluster topology, cluster statistics, and metric charts.<br>• Load Distribution—Displays load distribution across the cluster nodes.<br>• Member Performance—Displays current metrics of all the member nodes of the cluster.<br>• CCL—Displays, graphically, the cluster control link data namely, the input, and output rate.<br>**Note** These features are applicable only for a cluster. Hence, you must select the cluster under the **Devices** list on the **Monitoring** pane to view and use the cluster dashboard.<br>New/modified screens: **System** > **Health** > **Monitor**. |

| Feature | Version | Details |
|---|---|---|
| Monitor fans speed and temperature for the hardware power supply units (PSU). | 7.3 | The custom metric group, **Hardware / Environment Status** now includes metrics to monitor the power supply units. The new metrics included PSU fan speed, PSU fan status, PSU temperature, and PSU input and output metrics.<br>**Note** These features are applicable only for the threat defense hardware. Hence, you must select the appropriate device under the **Devices** list on the **Monitoring** pane.<br>New/modified screens: **System** > **Health** > **Monitor**. |
| Elephant Flow Detection<br>. | 7.1 | The health monitor includes the following enhancements:<br>• The Connection statistics includes active elephant flows.<br>• The Connection Group Metrics includes the number of active elephant flows. |
| New health modules. | 7.0 | We added the following health modules:<br>• AMP Connection Status: Monitors AMP cloud connectivity from the threat defense.<br>• AMP Threat Grid Status: Monitors AMP Threat Grid cloud connectivity from the threat defense.<br>• ASP Drop: Monitors the connections dropped by the data plane accelerated security path.<br>• Advanced Snort Statistics: Monitors Snort statistics related to packet performance, flow counters, and flow events.<br>• Hardware and Environment Status: Monitors device hardware and environmental metrics from the threat defense device.<br>• Flow Offload: Monitors hardware flow offload statistics on the threat defense 9300 and 4100 platforms.<br>• NTP Status: Monitors the NTP clock synchronization status of the managed device.<br>• Routing Statistics: Monitors both IPv4 and IPv6 route information from the threat defense.<br>• SSE Connection Status: Monitors SSE cloud connectivity from the threat defense.<br>• VPN Statistics: Monitors site-to-site and remote access VPN tunnel statistics.<br>• TLS Counters: Monitors xTLS/SSL flows, memory and cache effectiveness. |

| Feature | Version | Details |
|---|---|---|
| New health modules. | 6.7 | The following metrics are added to track CPU usage:<br>• CPU Usage (per core): Monitors the CPU usage on all of the cores.<br>• CPU Usage Data Plane: Monitors the average CPU usage of all data plane processes on the device.<br>• CPU Usage Snort: Monitors the average CPU usage of the Snort processes on the device.<br>• CPU Usage System: Monitors the average CPU usage of all system processes on the device.<br>The following metric groups are added to track device health statistics:<br>• Connection Statistics: Monitors the connection statistics and NAT translation counts.<br>• Critical Process Statistics: Monitors the state of critical processes, their resource consumption, and the restart counts.<br>• Deployed Configuration Statistics: Monitors statistics about the deployed configuration, such as the number of ACEs and IPS rules.<br>• Snort Statistics: Monitors the Snort statistics for events, flows, and packets.<br>The following metrics are added to track memory usage:<br>• Memory Usage Data Plane: Monitors the percentage of allocated memory used by the Data Plane processes.<br>• Memory Usage Snort: Monitors the percentage of allocated memory used by the Snort process. |