Firepower Threat Defense Device Metrics Collected by the Firepower Management Center Health Monitor, Version 7.0

First Published: 2023-06-20

Last Modified: 2023-06-27

Firepower Threat Defense Device Metrics Collected by the Firepower Management Center Health Monitor

The device health monitor includes an array of key FTD device metrics that serve to predict and respond to system events. The health of any FTD 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 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.	bytes
Free	The total free memory.	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
System Used	The total memory used by the system.	bytes
Total	The total memory available.	bytes
Total Swap	The total memory available for swap.	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 memory used for swap.	percent
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 memory used for swap.	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

Metric	Description	Format
Average Input Packet Size	The average size of incoming packets.	bytes
Input Rate	The total incoming bytes.	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 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
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

Connection Group Metrics

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

Table 4: Connection Group Metrics

Metric	Description	Format
Connections in use	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
Dropped frames forwarded from the data plane	The number of dropped frames forwarded from the data plane.	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 receiving queue utilization percentage	The queue utilization rate for the data plane receive 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 the accelerated security path (ASP) dropped packets or connections.

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
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

Metric	Description	Format
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
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	Counts the 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
Packet dropped as number of packet queued	Counts the number of packets dropped when the appliance receives a retransmitted data packet that is already in the out of order packet queue.	number

Metric	Description	Format
Number of segments queued to an inspection reached limit	For a flow, the number of packets queued to the inspector has reached the limit, thus terminating the flow.	number
Blocked or blocklisted by Snort	Counts the number of times a packet is dropped as requested by the Snort module.	number
Packet drop silently by Snort	Counts the number of times a packet is dropped silently as requested by the Snort module.	number
Un-synced first TCP packet	Counts the 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
SSD1	Status of SSD1.	number
System Uptime	Duration for which the system is active.	seconds

The availability of Hardware / Environment status metrics can vary depending on the model of the FTD 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
Internal Temperature	Yes	Yes	Yes	No	Yes	No	No
Inlet Temperature	No	No	No	No	No	No	No

Metric	1000 Series	2100 Series	3100 Series	4100 Series	4200 Series	9300 Series	SSP
Outlet Temperature	No	No	No	No	No	No	No
SSD1 Status	Yes	Yes	Yes	No	Yes	No	No

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 FTD device boot up. 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
Status	Status of the process.	One of the following: • Started • Running • Down • Waiting • Locked • Disabled User Disabled
Uptime	Duration for which the process is running.	seconds
Memory used	RSS memory used by the process.	bytes

NTP server group metric

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

Table 12: 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

Metric	Description	Format
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 FTD 9300 and 4100 platforms.

Table 13: 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
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 FTD device.

Table 14: 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 15: 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
Peak Concurrent S2S VPN Tunnels	Peak number of site-to-site VPN tunnels which were simultaneously active until now.	number

AMP Connectivity Group Metrics

Health monitoring tracks the AMP cloud connectivity status from the FTD device.

Table 16:

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

AMP Threat Grid Connectivity Group Metrics

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

Table 17:

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

History for Device Health Metrics

Feature	Version	Details
New health modules	7.0	We added the following health modules: • AMP Connection Status: Monitors AMP cloud connectivity from the FTD. • AMP Threat Grid Status: Monitors AMP Threat Grid cloud connectivity from the FTD. • ASP Drop: Monitors the connections dropped by the data plane accelerated security path. • Advanced Snort Statistics: Monitors Snort statistics related to packet performance, flow counters, and flow events. • Hardware and Environment Status: Monitors device hardware and environmental metrics from the FTD device. • Flow Offload: Monitors hardware flow offload statistics on the FTD 9300 and 4100 platforms. • NTP Status: Monitors the NTP clock synchronization status of the managed device. • Routing Statistics: Monitors both IPv4 and IPv6 route information from the FTD. • SSE Connection Status: Monitors SSE cloud connectivity from the FTD. • VPN Statistics: Monitors site-to-site and remote access VPN tunnel statistics. • 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: • CPU Usage (per core): Monitors the CPU usage on all of the cores. • CPU Usage Data Plane: Monitors the average CPU usage of all data plane processes on the device. • CPU Usage Snort: Monitors the average CPU usage of the Snort processes on the device. • CPU Usage System: Monitors the average CPU usage of all system processes on the device. The following metric groups are added to track device health statistics: • Connection Statistics: Monitors the connection statistics and NAT translation counts. • Critical Process Statistics: Monitors the state of critical processes, their resource consumption, and the restart counts. • Deployed Configuration Statistics: Monitors statistics about the deployed configuration, such as the number of ACEs and IPS rules. • Snort Statistics: Monitors the Snort statistics for events, flows, and packets. The following metrics are added to track memory usage: • Memory Usage Data Plane: Monitors the percentage of allocated memory used by the Data Plane processes. • Memory Usage Snort: Monitors the percentage of allocated memory used by the Snort process.