Cisco Secure Firewall Management Center 运行状况监控器收集的 Cisco Secure Firewall Threat Defense 设备指标，版本 7.2

首次发布日期: 2023 年 6 月 20 日

上次修改日期: 2024 年 1 月 17 日

Cisco Secure Firewall Management Center 运行状况监控器收集的 Cisco Secure Firewall Threat Defense 设备指标

设备运行状况监控器包括一系列用于预测和响应系统事件的关键威胁防御设备指标。任何威胁防御设备的运行状况都可以通过这些报告的指标来确定。本文档提供了有关所有运行状况监控控制面板和报告指标的列表。

CPU 组指标

运行状况监控器跟踪与CPU使用率相关的统计信息，包括按进程和物理核心划分的CPU使用情况。

表 *1: CPU* 组指标

指标	说明	格式
控制平面	控制平面过去一分钟的平均 CPU 使用率。	百分比
数据平面	数据平面过去一分钟的平均 CPU 使用率。	百分比
Snort	Snort 进程最近一分钟的平均 CPU 使用率。	百分比
系统	最近一分钟系统进程的平均 CPU 使用率。	百分比
物理核心	最后一分钟所有核心的平均 CPU 使用率。	%

内存组指标

运行状况监控器跟踪与设备内存使用率相关的统计信息，包括数据平面和 Snort 内存使用情况。

表 2: 内存组指标

指标	说明	格式
缓冲区缓存	缓冲区缓存。	字节
空闲	总可用内存。	字节
最大数据平面	数据平面使用的最大内存。	字节
最大 Snort	Snort 进程使用的最大内存。	字节
Snort 最大切换	Snort 进程使用的最大交换内存。	字节
剩余内存块 (1550)	1550 字节块中的可用内存。	数字
剩余内存块 (256)	256 字节块中的可用内存。	数字
已用系统	系统使用的总内存。	字节
总数	总可用内存。	字节
总计切换	可用于 swap 的总内存。	字节
数据平面	数据平面使用的总内存。	字节
数据平面使用百分比	数据平面使用内存百分比。	%
Snort 使用百分比	Snort 进程使用内存百分比。	%
用于交换的百分比	用于交换的内存百分比。	%
系统使用百分比	系统使用内存百分比。	%
系统和 Swap 使用百分比	系统和交换空间组合使用内存百分比。	%
Snort	Snort 进程使用的总内存。	字节
已使用切换	用于交换的总内存。	字节
Snort 已使用的切换	Snort 进程使用的总交换内存。	字节

接口组指标

运行状况监控器跟踪与设备接口相关的统计信息，包括接口状态和汇聚流量统计信息。

表 3: 接口组指标

指标	说明	格式
丢弃数据包	丢弃的数据包数。	数字

指标	说明	格式
平均输入数据包大小	传入数据包的平均大小。	字节
输入速率	总传入字节数。	字节
输入包数	总传入数据包数。	数字
平均输出数据包大小	传出数据包的平均大小。	字节
输出速率	传出总字节数。	字节
输出包数	传出数据包总数。	数字
状态	接口的状态； 1 表示开启，0 表示关闭。	1 或 0
CRC 错误数	收到的具有 CRC（循环冗余校验）错误的数据包总数。	数字
输入错误	输入错误的数量。	数字
输出错误	输出错误的数量	数字
溢出错误数	由于输入速率超出接收器处理输入数据的能力而丢弃的数据包数量。	数字
欠载错误数	由于发射器的运行速度超过路由器的处理能力而丢弃的数据包数量。	数字
L2 解码丢弃数	因未配置名称（nameif 命令）或接收到具有无效 VLAN ID 的帧而丢弃的数据包数。	数字
抖动	数据包流延迟的变化。	微秒
平均意见评分 (MOS)	连接质量的度量范围为 0 到 5，其中 5 表示质量最佳。	0 至 5
丢包	传输的数据包未到达目的地的百分比。	百分比
往返时间	ICMP 回应请求和响应之间的平均持续时间。	微秒

连接组指标

健康监控器跟踪与连接和 NAT 转换计数相关的统计。

表 *4:* 连接组指标

指标	说明	格式
活动大象流数	显示活动大象流数。 大象流是指大到足以影响整体系统性能的连接。默认情况下，大象流是速率大于每 10 秒 1GB 的流。您可以使用**系统支持大象流检测**命令调整字节和时间阈值，以在威胁防御 CLI 中识别大象流。 **注释** 仅当超过字节和时间阈值时，流才被视为大象流。	数字
活动连接	显示处于活动状态的连接数。	数字
峰值连接	显示最大同时连接数。	数字
每秒连接总数	所有连接类型的每秒连接数。	数字
每秒 TCP 连接数	TCP 连接类型的每秒连接数。	数字
每秒 UDP 连接数	UDP 连接类型的每秒连接数。	数字
保留已启用的连接	在 Snort 进程关闭时保留路由和透明接口上的现有 TCP/UDP 连接。	数字
保留的连接	当前启用了保留连接的连接。	数字
保留启用最多的连接	保留的最大连接数。	数字
保留的连接峰值	保留的最大高峰连接数。	数字
NAT 转换	显示转换计数。	数字
NAT 转换峰值	一次显示并发转换的历史最大值。	数字

Snort 组指标

运行状况监控器跟踪与 Snort 进程相关的统计信息。

表 *5: Snort* 组指标

指标	说明	格式
阻止的列表流	Snort 在策略配置中丢弃的流数。	数字
被阻止的数据包	被阻止的数据包的数量。	数字

指标	说明	格式
被拒绝的流	被拒绝的流事件的数量。当数据平面决定在将流发送到 Snort 之前丢弃流时，数据平面进程会向 Snort 发送拒绝流事件	数字
流结束	当快速路径流结束时，数据平面会向 Snort 发送流结束事件。	数字
快速转发的流	由策略快速转发并因此未检查的流的数量。	数字
已丢弃转发自数据平面的帧	已丢弃转发自数据平面的帧数。	数字
已丢弃注入数据包	Snort 添加到已丢弃的流量流的数据包数。	数字
注入的数据包	Snort 创建并添加到流量流的数据包数。例如，如果配置具有重置操作的阻止，Snort 会生成数据包以重置连接。	数字
实例 (Instances)	Snort 实例数（进程）。	数字
数据包接收队列的利用率百分比	数据平面接收队列的队列利用率。	%
由于 Snort 繁忙而绕过的数据包	当 Snort 太忙而无法处理数据包时，绕过检测的数据包的数量。	数字
由于 Snort 关闭而绕过的数据包	Snort 关闭时绕过检测的数据包数量。	数字
由于 RX 队列已满而绕过的数据包	由于接收队列已满而绕过的数据包数。	数字
由于 TX 队列已满而绕过的数据包	由于传输队列已满而绕过的数据包数。	数字
通过的流	从数据平面发送到 Snort 的数据包数。	数字
流开始	流开始事件的数量。这些事件有助于 Snort 跟踪连接并报告连接事件。	数字

ASP 丢弃指标

运行状况监控器跟踪与加速安全路径 (ASP) 丢弃的数据包或连接相关的统计信息。

表 *6: ASP* 丢弃指标

指标	说明	格式
超出连接限制	计算超出连接限制时关闭的流数。	数字

指标	说明	格式
达到连接限制	统计在超出连接限制或主机连接限制时被丢弃的数据包数。	数字
被访问规则拒绝的流	访问规则拒绝的连接数。	数字
被已配置规则拒绝的流	被已配置规则拒绝的连接数。	数字
L2 规则丢弃	统计由于第2层ACL而被拒绝的数据包的数量。	数字
L2 规则 VXLAN 丢弃	统计由于在应用第 2 层 ACL 检查时未能找到 VXLAN out_tag 而被拒绝的数据包数。	数字
NAT 逆向路径失败	统计拒绝尝试使用转换后的主机实际地址连接到转换后的主机的次数。	数字
NAT 失败	统计尝试创建 xlate 以转换 IP 或传输报头的失败次数。	数字
没有有效的 v4 邻接	对安全设备尝试获取邻接关系但无法获取下一跳 (IPv4) 的 MAC 地址时丢弃的数据包的数量进行计数。	数字
没有有效的 v6 邻接	对安全设备尝试获取邻接关系但无法获取下一跳 (IPv6) 的 MAC 地址时丢弃的数据包的数量进行计数。	数字
被 Snort 列入阻止列表的数据包；被 Snort 阻止的数据包	对 Snort 模块请求的数据包进行计数。	数字
丢帧 - Snort 繁忙；丢帧 - Snort down；丢帧 - Snort 丢弃	对由于 Snort 模块繁忙且无法处理帧而丢弃的帧进行计数； Snort模块已关闭； Snort模块请求丢弃。	数字
达到调度队列限制	计算设备的负载均衡ASP调度程序达到其队列限制的次数。当尝试更多数据包时，会发生尾部丢弃，并且此计数器递增。	数字
目标 MAC L2 查找失败	计算失败的第 2 层目的 MAC 地址查找的次数。一旦查找失败，设备将开始目标MAC发现过程，并尝试通过 ARP 和/或 ICMP 消息查找主机的位置。	数字
检测失败	计算设备未能启用网络处理器对连接执行的协议检测的次数。原因可能是内存分配失败，或者对于 ICMP 错误信息，设备无法找到与 ICMP 错误信息中嵌入的帧相关的任何已建立的连接。	数字

指标	说明	格式
NAT 无 PAT 池的 xlate	统计未找到目标与 PAT 池中的映射地址相匹配的连接的现存 xlate 的次数。	数字
无主机路由	计算安全设备尝试从接口发送数据包但未在路由表中找到该接口的路由的次数。	数字
超出 PDTS 转出限制	当数据路径将数据包转出到检查器，并且已排队等待 Snort 的数据包数超出最大限制时，此计数器会递增并且数据包会被丢弃。	数字
转出限制	由于排队等待检查的数据包达到上限而丢弃的数据包数量。	数字
Snort 静默丢弃	统计 Snort 模块请求的数据包被静默丢弃的次数。	数字
首个非 SYN 的 TCP 数据包	作为非拦截和非固定连接的首个数据包收到非 SYN 数据包的次数。	数字

硬件/环境状态指标

硬件/环境运行状况监控器跟踪统计信息并收集与威胁防御硬件实体相关的指标值。

表 *7:* 硬件/环境状态指标

指标	说明	格式
风扇速度	机箱风扇的速度。	RPM
入口温度	入口传感器的温度。	摄氏度
内部温度	内部传感器的温度。	摄氏度
出口温度	出口传感器的温度。	摄氏度
SSD1	SSD1 的状态。	数字
系统运行时间	系统处于活动状态的持续时间。	秒

硬件/环境状态指标的可用性可能会因威胁防御设备型号而异。下表介绍了每种设备型号的可用指标。

表 *8:* 每种设备型号的硬件/环境状态指标

指标	1000 系列	2100 系列	3100 系列	4100 系列	9300 系列	SSP
系统运行时间	是	是	是	是	是	是

指标	1000 系列	2100 系列	3100 系列	4100 系列	9300 系列	SSP
风扇速度	是	是	是	否	不支持	不支持
内部温度	是	是	是	否	不支持	不支持
入口温度	不支持	不支持	不支持	不支持	不支持	不支持
出口温度	不支持	不支持	不支持	不支持	不支持	不支持
SSD1 状态	是	是	是	否	不支持	不支持

已部署的配置组指标

运行状况监控器跟踪有关已部署配置的统计信息，例如 IPS 规则数和 ACE 数。

表 *9:* 已部署的配置组指标

指标	说明	格式
ACE 数	访问控制条目 (ACE) 数或规则。访问控制列表 (ACL) 由一个或多个 ACE 组成。	数字
规则数	入侵策略中的规则数量。	数字

磁盘组指标

运行状况监控器跟踪与设备磁盘使用情况相关的统计信息，包括每个分区的磁盘大小和磁盘利用率。

表 *10:* 磁盘组指标

指标	说明	格式
总数	设备磁盘的总大小。	字节
已使用	设备磁盘上使用的总空间。	字节
按 /ngfw 排列的已用百分比	/ngfw 分区使用的磁盘空间百分比。	百分比
按 /ngfw/Volume 排列的已用百分比	/ngfw/Volume 分区使用的磁盘空间百分比。	百分比
按 /dev/cgroups 排列的已用百分比	/dev/cgroups 分区使用的磁盘空间百分比。	百分比
按 /mnt/disk0 排列的已用百分比	/mnt/disk0 分区使用的磁盘空间百分比。	百分比

指标	说明	格式
按 /var/volatile 排列的已用百分比	/var/volatile 分区使用的磁盘空间百分比。	百分比

关键进程组指标

运行状况监控器跟踪与受管进程的进程重启相关的统计信息。此外，对于每个关键进程，运行状况监控器会跟踪 CPU 利用率、内存利用率、正常运行时间和状态。

表 *11:* 关键进程组指标

指标	说明	格式
CPU 利用率	进程自启动以来的 CPU 使用率。	%
重新启动计数	自威胁防御设备启动以来进程重新启动的次数。 请注意，如果进程重新启动太频繁，则重新启动计数指标可能无法反映确切的数量，因为此指标每分钟运行一次。	数字
意外重启计数	自威胁防御设备启动以来进程意外重启的时间。	数字
状态	进程状态。	以下项之一： • 已开始 • 应用类型 • 关闭 • 等待 • 已锁定 • 已禁用 已禁用用户
运行时间	进程运行的持续时间。	秒
已用内存	进程使用的 RSS 内存。	字节

NTP 服务器组指标

运行状态监控器会跟踪托管设备的 NTP 时钟同步状态相关的统计数据。

表 *12: NTP* 服务器组指标

指标	说明	格式
延迟	延迟到达 NTP 服务器。	毫秒
抖动	设备与 NTP 服务器之间的网络延迟。	毫秒
上次轮询时间	自设备上次轮询 NTP 服务器以来的时间。	秒
偏移	本地时钟与 NTP 服务器时钟之间的时间差异。	秒
覆盖范围	以八进制数表示的最近八次 NTP 更新。例如，8 次成功尝试用 377 表示。	数字

流分流统计信息组指标

运行状况监控会跟踪威胁防御 9300 和 4100 平台上的硬件流量分流统计信息。

表 *13:* 流分流统计信息组指标

指标	说明	格式
正在使用	当前分流的流数。	数字
最常用	截至目前看到的最大分流流数。	数字
冲突流数	同时匹配同一硬件分流位置的多个流的数量。	数字
分流百分比	目前已分流到硬件的总流的百分比。	百分比

路由统计信息组指标

运行状况监控器会跟踪来自威胁防御设备的 IPv4 和 IPv6 路由信息。

表 *14:* 路由统计信息组指标

指标	说明	格式
当前 IPv4 和 IPv6 路由数	当前 IPv4 和 IPv6 路由计数。	数字
全局 IPv4 路由数	全局 IPv4 路由数。	数字
全局 IPv6 路由数	全局 IPv6 路由数。	数字
峰值 IPv4 和 IPv6 路由数	IPv4 和 IPv6 的峰值路由计数。	数字
每 VRF 总 IPv4 路由数	每个 VRF 的 IPv4 路由总数。	数字

指标	说明	格式
每 VRF 总 IPv6 路由数	每个 VRF 的 IPv6 路由总数。	数字

VPN 组指标

运行状况监控会跟踪站点间和远程访问 VPN 隧道统计信息。

表 *15: VPN* 组指标

指标	说明	格式
活动 RA VPN 隧道数	活动远程访问 VPN 隧道的数量。	数字
活动 S2S VPN 隧道数	活动站点间 VPN 隧道的数量。	数字
累计 RA VPN 会话数	到目前为止处于活动状态的远程访问 VPN 隧道的总数。	数字
累计 S2S VPN 会话数	到目前为止处于活动状态的站点间 VPN 隧道总数。	数字
非活动 RA VPN 隧道数	非活动远程访问 VPN 隧道的数量。	数字
峰值并发 RA VPN 隧道数	到目前为止同时处于活动状态的远程访问 VPN 隧道的峰值数量。	数字
峰值并发 S2S VPN 隧道数	到目前为止同时处于活动状态的站点间 VPN 隧道的峰值数量。	数字

AMP 连接组指标

运行状况监控从威胁防御设备跟踪 AMP 云连接状态。

表 16:

指标	说明	格式
连接状态	AMP 云连接状态。	数字 0 到 5，其中： • 0 表示已禁用。 • 1 表示正在等待。 • 2 表示正在运行。 • 3 表示未配置。 • 4 表示 AMP 云连接已打开。 • 5 表示 AMP 云连接已关闭。

AMP 威胁网格连接组指标

运行状况监控从威胁防御设备跟踪 AMP Threat Grid 云连接状态。

表 17:

指标	说明	格式
连接状态	AMP Threat Grid 云连接状态。	数字 0 到 5，其中： • 0 表示已禁用。 • 1 表示正在等待。 • 2 表示正在运行。 • 3 表示未配置。 • 4 表示 AMP Threat Grid 云连接已打开。 • 5 表示 AMP Threat Grid 云连接已关闭。

设备运行状况指标的历史记录

功能	版本	详细信息
象流检测	7.1	运行状况警报包含以下增强功能： • 连接统计信息包括活动的象流。 • 连接组指标包括活动的象流数。
新的运行状况模块	7.0	我们添加了以下运行状况模块： • AMP 连接状态：从威胁防御监控 AMP 云连接。 • AMP Threat Grid 状态：从威胁防御监控 AMP Threat Grid 云连接。 • ASP 丢弃：监控数据平面加速安全路径所放弃的连接。 • 高级 Snort 统计信息：监控与数据包性能、流计数器和流事件相关的 Snort 统计信息。 • 硬件和环境状态：监控威胁防御设备的硬件和环境指标。 • 流量分流：监控威胁防御 9300 和 4100 平台上的硬件流量分流统计信息。 • NTP 状态：监控托管设备的 NTP 时钟同步状态。 • 路由统计信息：监控来自威胁防御的 IPv4 和 IPv6 路由信息。 • SSE 连接状态：从威胁防御监控 SSE 云连接。 • VPN 统计信息：监控站点间和远程访问 VPN 隧道统计信息。 • TLS 计数器：监控 xTLS/SSL 流、内存和缓存有效性。

功能	版本	详细信息
新的运行状况模块	6.7	新增了以下指标来跟踪 CPU 使用情况： • CPU 使用情况（每个核心）：监控所有核心上的 CPU 使用情况。 • CPU 使用率数据平面：监控设备上所有数据平面进程的平均 CPU 使用率。 • CPU 使用率 Snort：监控设备上 Snort 进程的平均 CPU 使用率。 • CPU 使用率系统：监控设备上所有系统进程的平均 CPU 使用率。 新增了以下指标组来跟踪设备运行状况统计数据： • 连接统计信息：监控连接统计信息和 NAT 转换计数。 • 关键进程统计信息：监控关键进程的状态、资源消耗和重新启动计数。 • 部署的配置统计信息：监控有关已部署配置的统计信息，例如 ACE 数、IPS 规则数。 • Snort 统计信息：监控事件、流和数据包的 Snort 统计信息。 新增了以下指标来跟踪内存使用情况： • 内存使用率数据平面：监控数据平面进程使用的已分配内存的百分比。 • 内存使用情况 Snort：监控 Snort 进程使用的已分配内存的百分比。

当地语言翻译版本说明

思科可能会在某些地方提供本内容的当地语言翻译版本。请注意，翻译版本仅供参考，如有任何不一致之处，以本内容的英文版本为准。