Proactively Monitoring Performance of WSA Using SNMP

Contents

Introduction

This document describes proactively monitoring performance of Cisco Web Security Appliance (WSA) with Simple Network Management Protocol (SNMP).

Which values can be observed through an SNMP monitoring tool in order to proactively monitor the performance of the Cisco WSA? At what level should threshold alerts be configured?

When you monitor the Cisco WSA, the most important items for SNMP polling are as follows:

- Client Requests / Second
  cacheThruputNow (.1.3.6.1.4.1.15497.1.2.3.7.1.1)Request throughput in the last minute
- Response Time
  cacheTotalRespTimeNow (.1.3.6.1.4.1.15497.1.2.3.7.9.1)Cache total response time in the last minute
- CPU Usage
  cacheBusyCpuUsage (.1.3.6.1.4.1.15497.1.2.3.1.5)Percentage busy time of the CPU

> **Note:** SNMP Management Information Base (MIB) files for WSA can be found on the Cisco Web Security Product Support Page.

Since every customer environment varies, it is recommended to gather baseline production statistics over a set period of time in order to see if there are any outliers during the baseline period. During this baseline, note periods when client requests/second where maximized. If there was a corresponding drastic increase in response time and potential CPU usage, this could represent the peak performance in this specific environment. Further testing and monitoring should be performed in order to confirm this maximum level.

After the baseline period has elapsed, and no specific maximum peaks have been observed in client requests /second, it is recommend to artificially set a threshold value of 10% to 25% of the highest observed client requests/second for alerting purposes.

Aside from monitoring performance and alerting on specific exceeded thresholds, the Cisco WSA can also be configured to send SNMP traps on these hardware conditions:

Enabled by Default

- RAID Status Change
- Fan Failure
- High Temperature
- Key Expiration
- Link Down
- Link Up
- Power Supply Status Change
- Update Failure
- Upstream Proxy Failure

Disabled by Default

- Connectivity Failure
- CPU Utilization Exceeded
- Memory Utilization Exceeded

If you need to check specific Proxy CPU usage, review Calculating Proxy CPU utilization on the WSA using SNMP.