Contents

Introduction

This document describes the issue on sessmgr going to WARN state due to huge number of HTTP flows. This issue is reported on Cisco Aggregrated Service Routers (ASR) 5x00.

Problem

Sessmgr status is WARN and high memory utilization.

These Error logs are generated in the process.There is no subscriber impact due to this error log. As per design once the call is rejected from sessmgr which is in **WARN** state, system tries at different sessmgrs and call goes through.

Troubleshoot

Capture **s** output and check for the command outputs to troubleshoot further.

The memory problem is related with the amount of flows that the sessmgr handles. The correlation can be seen between sessmgr having high memory consumption and high amount of flows.

For affected sessmgrs (and for one unaffected), collect these command outputs, where *x* is the Sessmgr instance.

Check if unoptimized rules and group of ruledefs consume lot of memory.

The highest memory consumption is due to these functions based on the command outputs.

You can also check Max No of Simultaneous HTTP Flows attained by Call lines

You can conclude that there are huge number of HTTP sessions being allocated and this could be due to the heavy HTTP traffic. Also there are almost 1044671491 Calllines, which have greater than 10000 HTTP flows at a time. This leads to high memory usage.

Solution

You have the CLI to limit the number of flows per subscriber

Cisco would recommend to configure **flow limit-across-applications** to **5000** as recommended under all affected Rule-bases where huge number of HTTP Traffic can be seen.

This is the procedure to configure the command

More information about this command.

flow limit-across-applications

This command allows you to limit the total number of simultaneous flows per Subscriber/APN sent to a rulebase regardless of the **flow** type, or limit flows based on the protocol type under the Session Control feature.

Product:

ACS

Privilege:

Security Administrator, Administrator

Mode:

Syntax

If previously configured, deletes the **flow limit-across-applications** configuration from the current rulebase.

flow limit-across-applications limit

Specifies the maximum number of flows across all applications for the rulebase.

limit must be an integer from 1 through 4000000000.

Default: No limits

non-tcp limit

Specifies the maximum limit of non-TCP type flows.

limit must be an integer from 1 through 4000000000.

Default: No limits

tcp limit

Specifies the maximum limit of TCP flows.

limit must be an integer from 1 through 4000000000.

Default: No limits

Usage:

Use this command to limit the total number of flows allowed for a rulebase regardless of **flow** type, or limit flows based on the protocol—non-TCP (connection-less) or TCP (connection-oriented).

If a subscriber attempts to exceed these limits system discards the packets of new **flow**. This limit processing of this command has following aspects for UDP, TCP, ICMP and some of the exempted flows:

- UDP/ICMP: System waits for the **flow** timeout before updating the counter and removing it from the count of number of flows.
- TCP: After a TCP **flow** ends, system waits for a short period of time to accommodate the retransmission of any missed packet from one end. TCP flows those are ended, but are still in wait period for timeout are exempted for this limit processing.
- Exempted flows: System exempts all the other flows specified with the **flow limit-for-flow-type** command in the ACS Charging Action Configuration Mode set to **no**.

Example:

This command defines the maximum number of 200000 flows for the rulebase: