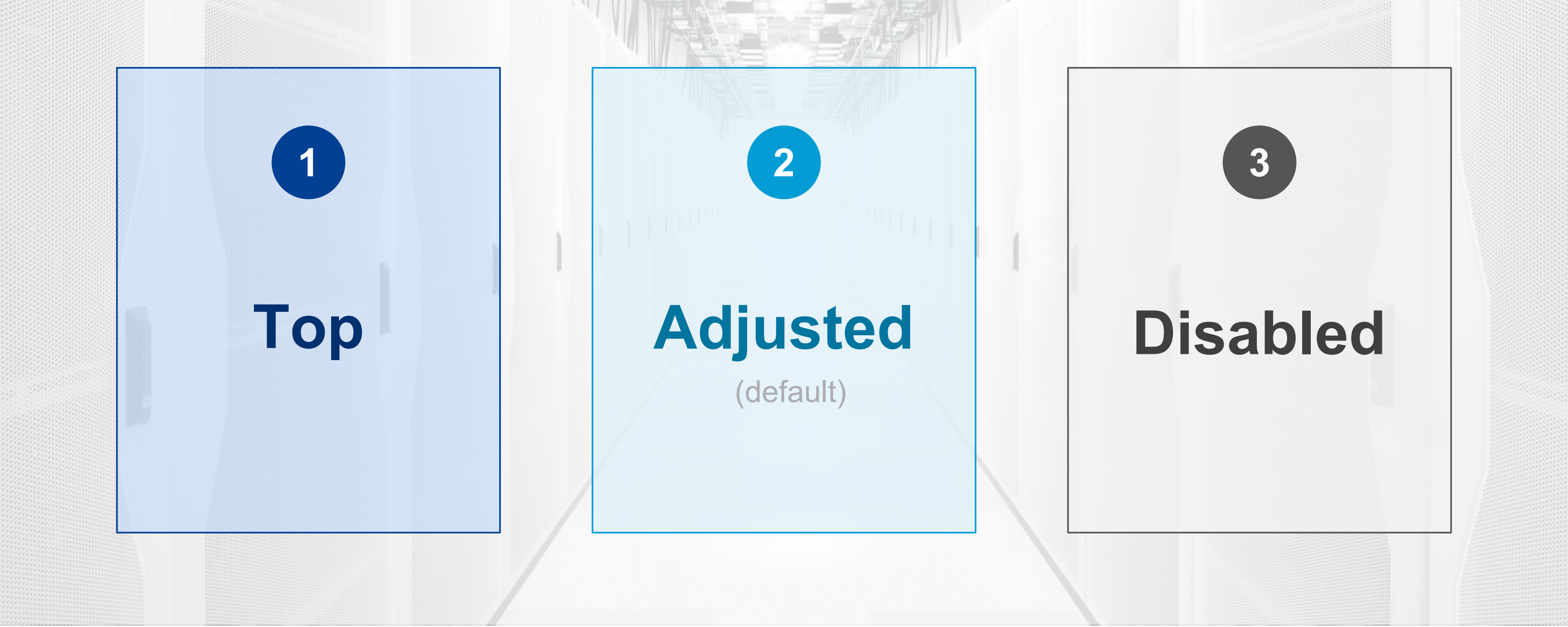
Cisco Secure Workload Sensors

Rate Limiting

Tim Garner - Technical Marketing Engineer

Secure Workload Has Three Rate Limiting Modes



1

Top

2

Adjusted

(default)

3

Disabled

Operating System Terminology

- Operating systems measure CPU usage in a quirky fashion

- Each logical core presented to the system provides 100%

- The total available amount of CPU percentage is added together

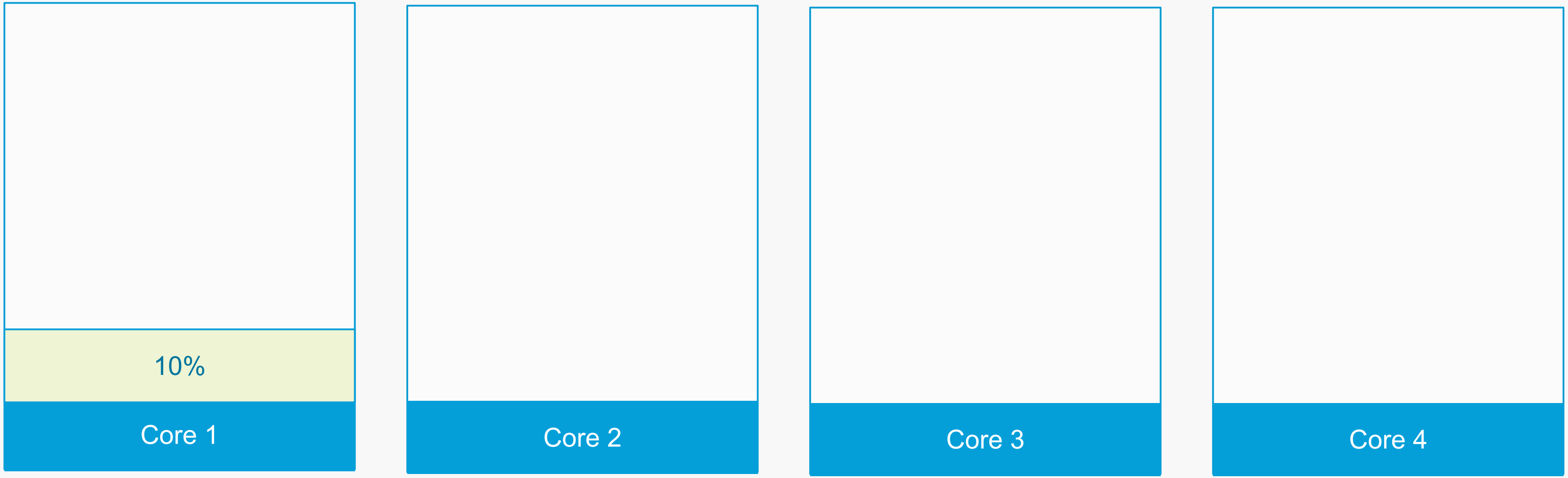
- 2 core system = 200%
- 4 core system = 400%

Top Limit

- “What you see is what you get”
- Uses no more CPU % than the given limit on any single core
- For example, 3% limit on a 10 core system = 3% out of total 1,000% available
- *This is a fairly restrictive mode and would be suggested only when necessary*

Top

Take 4 CPU cores - apply a 10% policy – 10% total (out of 400%)



10%

Core 1

Core 2

Core 3

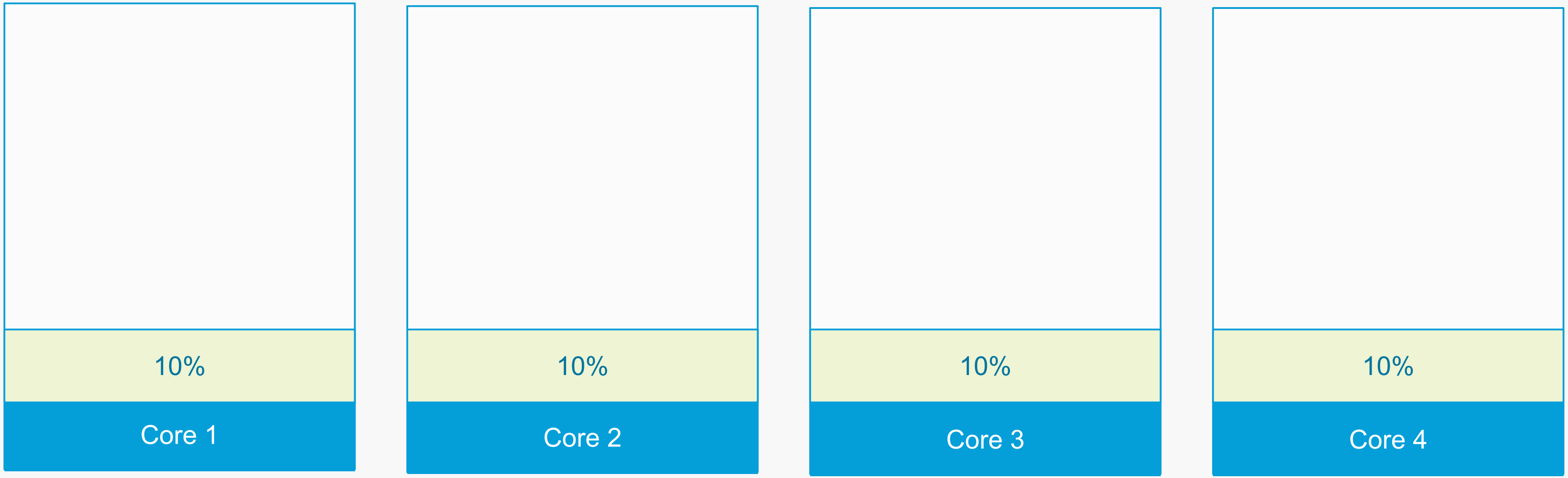
Core 4

Adjusted Limit

- Designed to account for multi-processor and multi-core systems
- Takes the provided limit and multiplies it by the amount of cores available to the system
- For example, 3% limit on a 10 core system = 30% out of total 1,000% limit
- **Important note:** “top” could display up to 30% CPU usage (on one or spread across cores) Don’t be surprised!
- *This is the default profile (set to 3%) – and it’s recommended to use this profile unless necessary*

Adjusted

Take 4 CPU cores - apply a 10% policy – 40% total (out of 400%)



10%

Core 1

10%

Core 2

10%

Core 3

10%

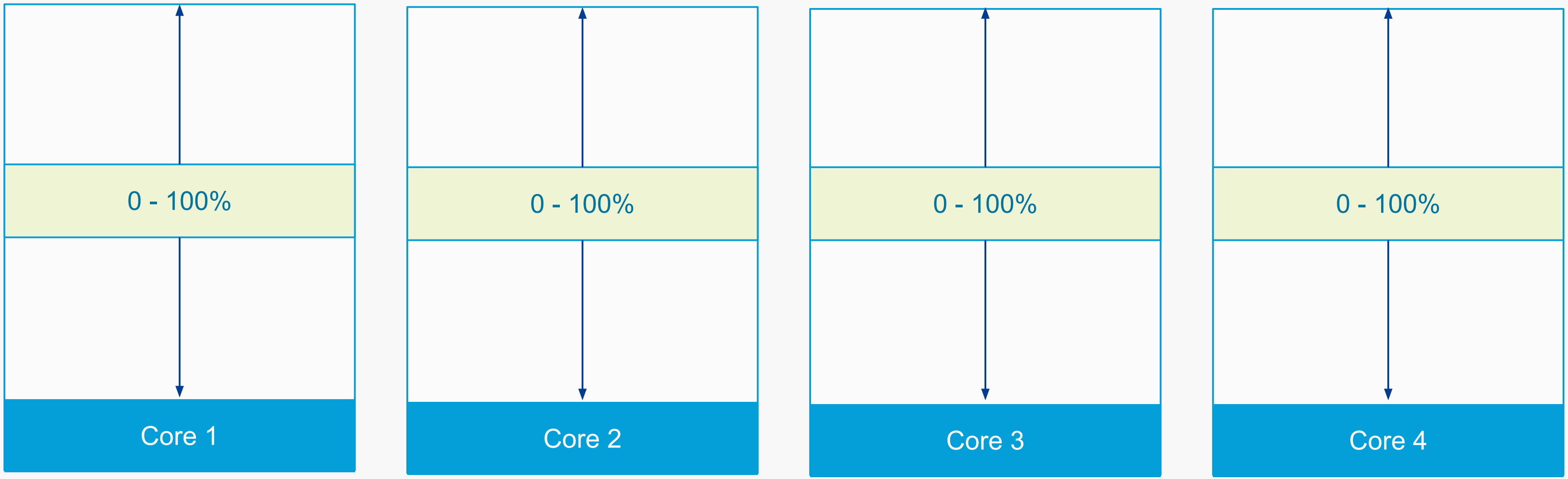
Core 4

Disabled

- *Use in hosts where telemetry MUST be collected*
- No CPU % limit, will take as much as necessary to capture each and every packet

Disabled

Take 4 CPU cores - apply a disabled policy – no limit (out of 400%)



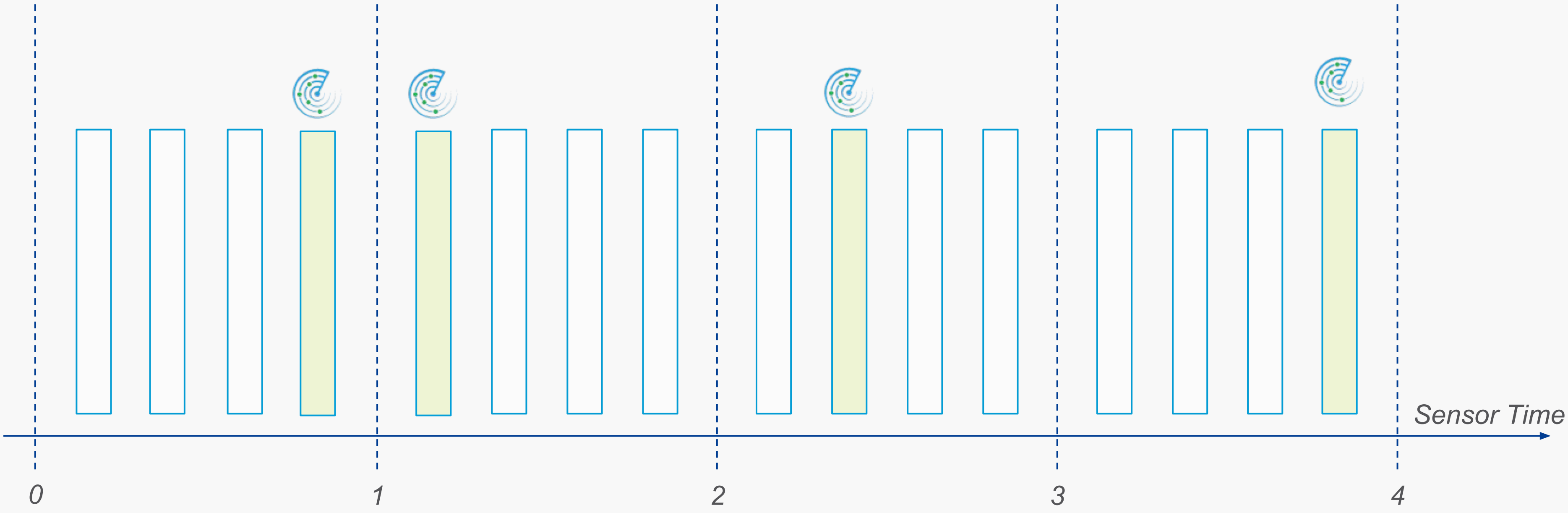
How does it work?

- CPU profile limit is specified in percentage of CPU time - the default limit is 3% CPU adjusted (limit * amount of cores)
- Sensor uses no more than the given amount of limit in a 1 second interval (as seen by the sensor)
- The process is self limiting – it monitors itself and does not require operating system intervention (cgroups, etc.)

Time Slicing

In one second – we will use a given amount of microseconds

Slices will not necessarily be evenly distributed at the one second boundary

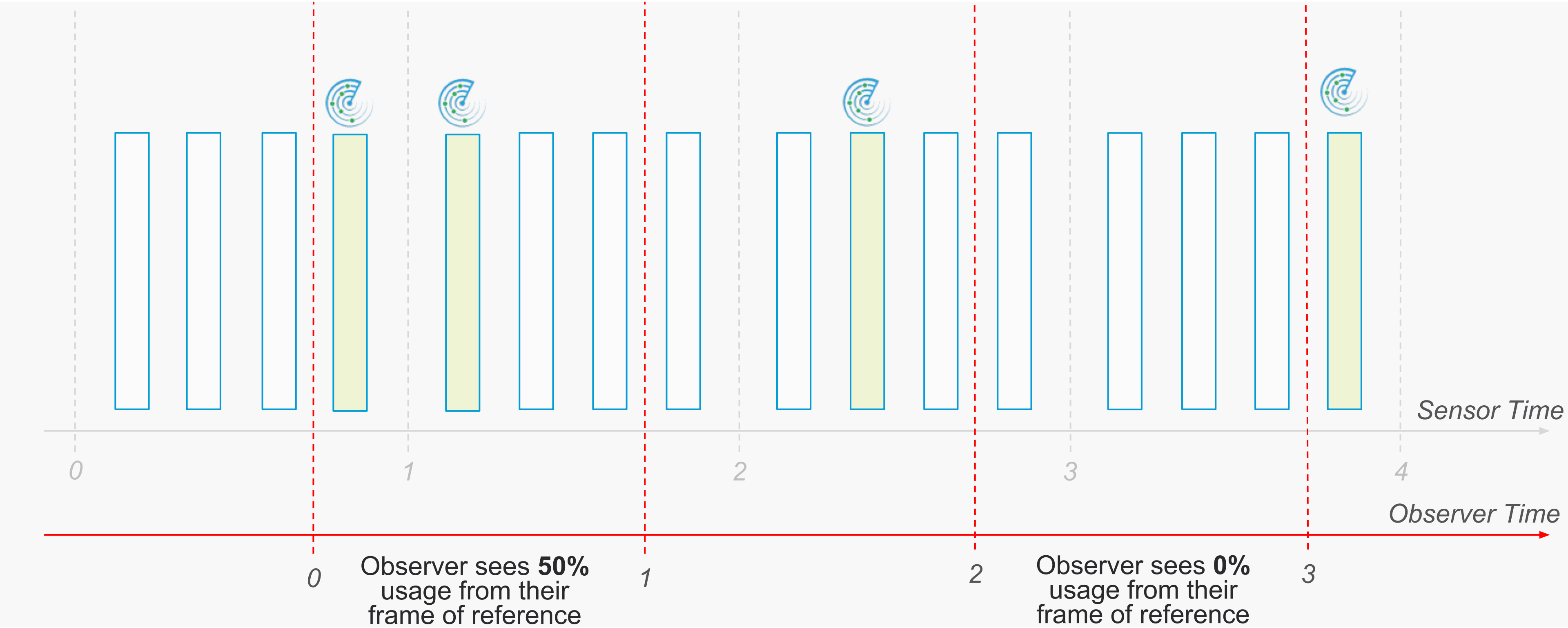


250,000 microsecond (25%) top profile

Observation

“top shows the Secure Workload sensor going over the limit I set!!”

Observer time and sensor time boundaries will not always match



Observer sees **50%** usage from their frame of reference

Observer sees **0%** usage from their frame of reference

Memory Utilisation (Flow Records)

- The sensor allocates enough memory for 65,536 flow records at launch
- A flow record is 360 bytes
- That equals about 23.59 megabytes statically allocated
- Accounting for other overhead (20,904 bytes), the entire static memory footprint is around 12.82 megabytes

Memory Utilisation (Per Connection)

- Per unique connection dynamic memory is allocated
- 25 bytes + ~200 byte headers + protocol receive buffer
- Multiply this factor by the amount of unique connections to the host

Memory Utilisation (Queuing)

- The sensor will queue up to 100,000 packets if rate limiting is in effect
- That equals about 22.50 megabytes that will be allocated
- If the 100,000 limit is reached, tail drop will be performed for incoming packets
- Queue will continue to be processed in FIFO order when/if CPU time is available again
- Packet drop count will be reported to the Secure Workload cluster