SmartSilc
Solutions by Silicom Ltd.

Silicom SPDK-1.1 Snort DAQ

Quick Overview

Snort DAQ (Data AcQuisition) component is a software interface between platform's data path and Snort engine. SPDK offer an efficient DAQ of intel® DPDK and Snort engine.

Compared to standard Linux based implementation, where data path is interrupt based and is implemented in kernel, SPDK breaks free of this paradigm and brings packet processing ever close to wire speed.

Two important advantages are offered by SPDK compared to standard DPDK. First, **smart and easy buffers managemen**t that makes more stable and scalable application. Second, is **threaded clustering** capability with software based **processing load balancing**, that enable ultimate optimization of packet processing.

Testing SPDK DAQ was performed in order to reveal the extent in which it both:

1) Enhances Snort performance
2) Scales up linearly, using SPDK threads cluster

Table 1 - Summary of Performence Number of SPDK DAQ

Setup Type	Rule	Mbps	MBps	pps	Average Paket Size	Latency
HW RSS 16 Instances	Community	2840	355	441000	800	5-6ms
HW RSS 16 Instances	VRT	1910	239	295000	810	6-8ms
Cluster 16 Instances	Community	2740	342	436000	780	3-4ms
Cluster 16 Instances	VRT	1830	229	291300	780	2-3ms
Cluster 32 Instances	Community	4500	560	730000	760	5-6ms
Cluster 32 Instances	VRT	3250	405	520000	770	5-6ms

Testing real life scenario with Snort is an important aspect of the work carried out here in these tests. Having client and server installation, along with VRT rules, brings the test setup as close to actual production grade Snort as can be, with true reflection of results expected in the field.