TECHNOLOGY BRIEF

Shunt Away Unwanted Suricata Traffic with Accolade Adapters

SUMMARY

Efficiently bypass traffic that Suricata doesn't need to examine, without dropping a single packet.

BENEFITS

- All traffic is fully processed with no dropped packets
- CPU resources are preserved for higher value features & functions
- Predictable performance

Suricata is a mature, open-source network threat detection engine. The software can be configured for real time intrusion detection (IDS), inline intrusion prevention (IPS), network security monitoring (NSM) and offline pcap processing. Suricata inspects network traffic using a powerful and extensive rules and signature language, and has powerful scripting support for detection of complex threats. With standard input and output formats like YAML and JSON, integration with external analytics tools such as Splunk, Logstash/Elasticsearch and Kibana is effortless.

The Suricata project and code is owned and supported by the Open Information Security Foundation (OISF), a non-profit foundation committed to ensuring Suricata's development and sustained success as an open source project. Accolade is a proud supporter of the project and sponsor of the annual Suricon user conference. More details about the project are on the foundation's website.

FLOW SHUNTING WITH SURICATA

Like many security applications, Suricata is CPU bound. This is clearly spelled out in the official Suricata User Guide as outlined in the quote below. In order to add additional capabilities or turn on specific features in Suricata, one must always be cognizant of the available CPU resources and often that requires upgrading to a more powerful server just to maintain acceptable levels of performance. Sometimes adding more CPUs is the right answer, but there is also an alternative: Adding an FPGA-based hardware adapter/NIC to offload the host CPU from intensive and repetitive tasks. There are many advantages to using a hardware adapter to solve the CPU resource problem, not the least of which is predictability. The hardware adapter will perform the same CPU intensive tasks over and over again in a very predictable and efficient manner—which greatly eases planning. A great example is flow processing.

> "...having additional CPUs available provides a greater performance boost than having more RAM available. That is, it would be better to spend money on CPUs instead of RAM when configuring a system."
>
> Source: Official Suricata User Guide rel 4.1.0 (pg. 119)

In Suricata release 3.2 (December, 2016) the concept of flow bypass was introduced. The idea is to let Suricata bypass or not process flows (based on 5-tuple) that are not of interest such as encrypted traffic; well-known traffic such as Netflix or YouTube; or any other non-interesting traffic. This is a very valuable Suricata feature, but it is also very CPU intensive and is an ideal candidate for offload to a hardware adapter. For example, with Accolade adapters, rather than have the Suricata software maintain a flow table and make bypass decisions the hardware takes care of all that processing. This in turn frees up the Suricata software to handle higher value tasks. In the next section we will show how effective the hardware is at flow processing.

Shunt Away Unwanted Suricata Traffic with Accolade Adapters

SURICATA SW BYPASS VS. ACCOLADE HW BYPASS

To test the relative efficacy of software versus hardware flow bypass an experiment was executed (with testing conducted by ntop, a leading network traffic analysis software company). Two identical servers were set up and configured with Suricata version 4.0.1 (test parameters are shown to the right). One server had an ANIC-40Ku adapter installed in it and the other relied entirely on Suricata's software implementation of flow bypass.

An identical 18 Gbps of Internet traffic was sent to each system. The traffic mix was the aggregate profile shown in figure 1. Roughly 70% (67.3% to be precise) of the traffic was entertainment which consisted of Netflix, YouTube , iTunes, Hulu, and other similar traffic. For the purposes of the experiment, this traffic was designated for flow bypass by Suricata, because it is from well-known sources and thus not worth examining for security purposes. The remaining roughly 30% of traffic was designated as traffic that Suricata should process and therefore not bypass.

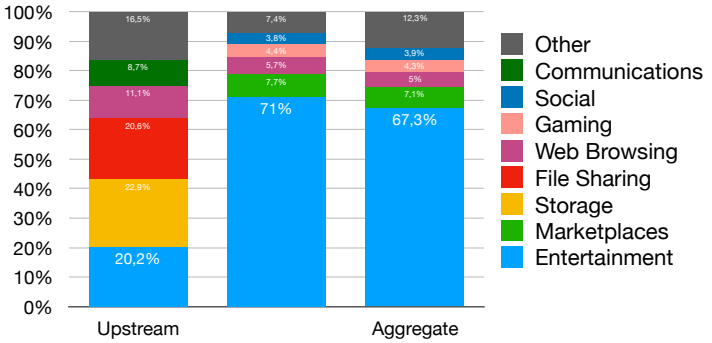

Fig 1: Internet Traffic Profile (Source: Sandvine)

TEST PARAMETERS

- Server Hardware: Intel Xeon E3 (single core)
- Suricata Version: 4.0.1
- Adapter Hardware: Accolade ANIC-40Ku (4 x 10G)
- Test Traffic Speed: 18 Gbps
- Test Traffic: Mixed Internet Traffic (see profile above)

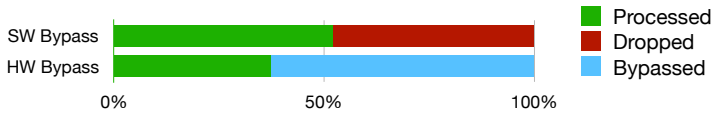

Fig 2: Hardware vs. Software Bypass Processing Performance

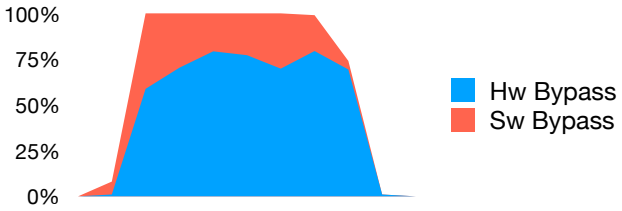

Fig 3: Hardware vs. Software Bypass CPU Utilization

The results are shown in figures 2 and 3. Figure 2 (HW Bypass) clearly shows that the server with the Accolade adapter successfully bypassed 70% of the traffic in hardware (onboard the adapter) which allowed Suricata to successfully process the remaining 30% of traffic. The server which relied purely on Suricata software to do all the work didn't fare as well. As figure 2 (SW Bypass) shows, Suricata only managed to process about 55% of the traffic (this includes both bypass and non-bypass traffic) and dropped around 45% of the overall traffic because it just didn't have enough CPU resources to handle it all. Figure 3 shows CPU load or utilization for each scenario. The system with hardware flow bypass peaked at about 75% CPU utilization which means it had significant spare capacity to perform other critical functions. The software only system, however, completely pegged the server at 100% CPU utilization and simply ran out of CPU capacity and therefore dropped critical traffic.

This experiment provides a very simple and compelling example of how a repetitive and CPU intensive task such as flow bypass is best done in hardware; so that software isn't burdened with this task and can therefore be used for higher value functionality which achieves the overall goal of processing all traffic to find security related problems.

ID:180603

Accolade Technology

Headquarters:
124 Grove Street, Suite 315
Franklin, MA 02038

phone: 877 653 1261
email: inquire@accoladetechnology.com
www.accoladetechnology.com