TECHNOLOGY BRIEF

Native Suricata Integration with Accolade, FPGA-Based Hardware

SUMMARY

Seamless and native integration of the Suricata, open-source network threat detection engine with Accolade CPU offload hardware

BENEFITS

- Increased scalability, performance and throughput
- Native integration with zero software modification
- Cost savings

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 Suricata conference. More details about the project are on the foundation's website.

HOST CPU OFFLOAD

Like most networking and security applications, Suricata performance and throughput can be scaled tremendously with some assistance from underlying hardware. Accolade offers two distinct FPGA-based, hardware options as shown in the figures below. Both of these options provide the same host CPU offload features and functions such as lossless packet capture, flow classification, deduplication, packet filtering and more.

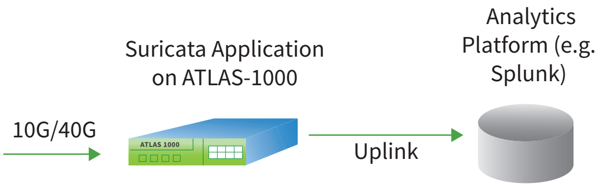

Suricata Application on ATLAS-1000
Analytics Platform (e.g. Splunk)
10G/40G
ATLAS 1000
Uplink

Fig 1: Suricata Application deployed on ATLAS-1000

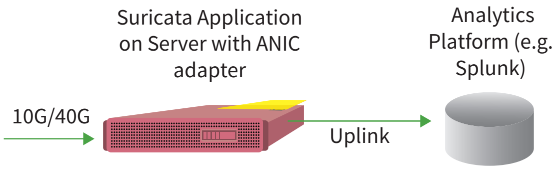
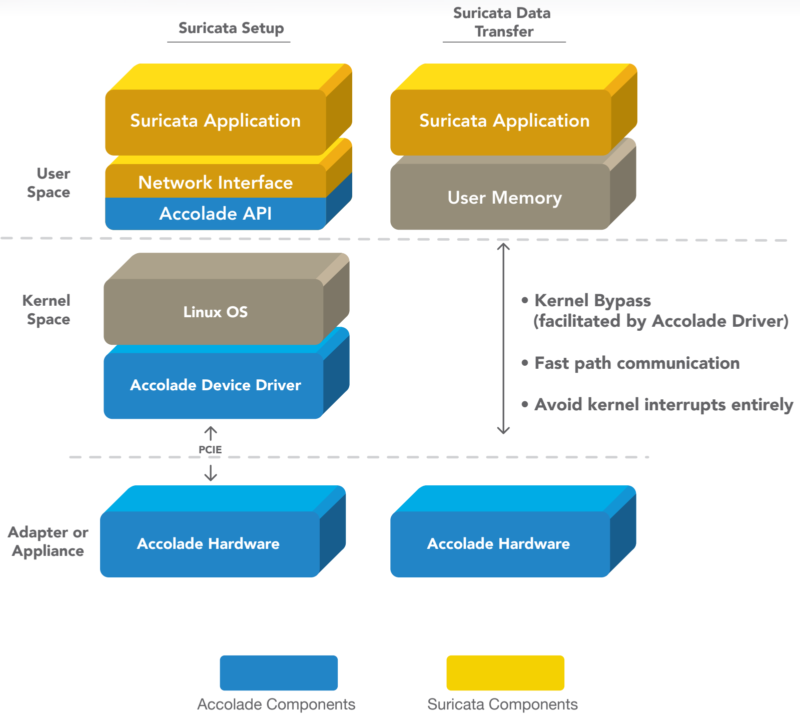

Suricata Application on Server with ANIC adapter
Analytics Platform (e.g. Splunk)
10G/40G
Uplink

Fig 2: Suricata Application deployed with ANIC Adapter

Suricata can be deployed on the Accolade, ATLAS-1000 appliance which is a fully integrated, 1U platform that provides all the standard features and functions of an industry standard server with the added benefit of an onboard CPU offload engine in the form of an FPGA. As an alternative to the ATLAS-1000, Accolade offers a complete line of host CPU offload adapters/NICs that can be plugged into the PCIe slot of any industry standard server. The adapters are available in various configurations with 1G, 10G, 40G or 100G network interfaces.

Native Suricata Integration with Accolade Hardware

NATIVE INTEGRATION



The Suricata application must be able to communicate directly with the Accolade hardware, in order to take advantage of the valuable host CPU offload features and functions. Communication with Accolade hardware is accomplished via a lightweight, C language API (shown on the left side of the diagram) which is typically linked to the user application as a shared library. Via this API the application can control the Accolade hardware and perform various functions such as policy configuration, reading port status and retrieving flow table entries. Normally the application would have to be modified in order to make API calls, however in the case of Suricata, no modification is required. Accolade has natively integrated the appropriate API calls into Suricata's standard network interface. Therefore all interaction with Accolade hardware is transparent to the Suricata application, which most importantly means the user does not have to make any modifications to the application at all. The only actions required by the user are a few configuration steps when initially deploying the application, in order to inform Suricata that it will be utilizing Accolade hardware.

FAST PATH COMMUNICATION

After the Suricata application natively performs setup procedures at system startup, almost all the ensuing interaction between Suricata and Accolade hardware is performed in kernel bypass mode as fast path communication. As shown on the right side of the diagram above, Accolade hardware transfers network data (after performing CPU offload functions) directly into user memory. The Suricata application in turn fetches the pre-processed data from user memory and performs its myriad security and network monitoring functions.

ACCOLADE TECHNOLOGY PROFILE

Accolade is the technology leader in FPGA-based Host CPU Offload and 100% Packet Capture PCIe Adapter/NIC's and Scalable 1U Platforms. Accolade's line of 1-100GE products enable 100% packet capture, flow classification, deduplication, packet filtering and more. Our customers are global leaders in network monitoring & cybersecurity applications as well as in the network test and measurement, telecom and video stream monitoring markets.