CASE STUDY

Corelight, Arista & Accolade Deliver Worldclass Bro Solution

SUMMARY

Corelight integrates the ANIC-40Ku adapter into BroBox One appliance

KEY CHALLENGES

- Guarantee 100% lossless packet capture across all ports
- Require merging of data streams in timestamp order to recreate bi-directional traffic flows
- Require high performance, cost effective adapter with full service support

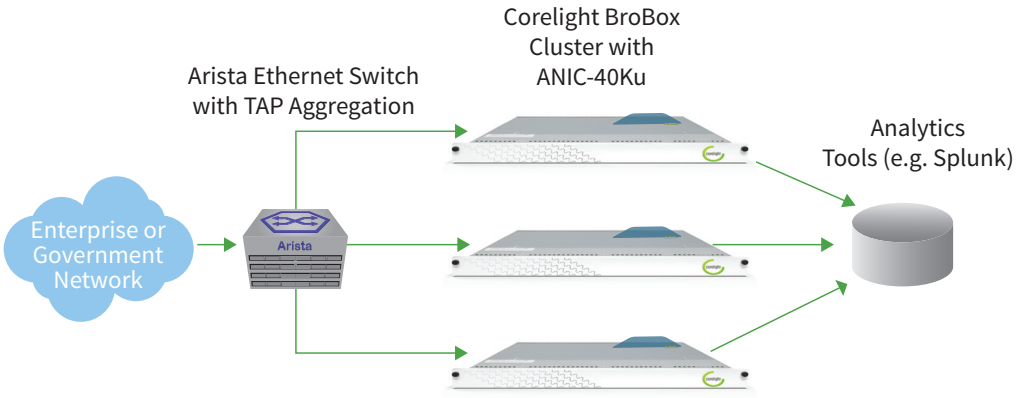
WHY ACCOLADE?

- Worked closely with Corelight to rapidly integrate ANIC-40Ku into BroBox One
- Provide full line of packet capture adapters from 4 x 1G to 2 x 100G with common feature set
- Willingness to develop custom features tailored to BroBox

ANIC FEATURES USED

- 100% packet capture
- Timestamping
- Packet Merging
- Flow Classification
- Packet Steering

Corelight (formerly Broala) is the market leading provider of enterprise class Bro solutions. Corelight brings the power of open-source Bro to the Global 2000 enterprise with a fully supported, highly efficient and scalable network monitoring framework. Corelight's flagship BroBox One appliance transforms raw network traffic into rich data streams for real-time analysis, intrusion detection and forensics. BroBox One provides a carefully tailored subset of Bro functionality. The graphic below depicts an optimal Bro architecture; beginning with a wire speed, Arista Ethernet switch with TAP Aggregation distributing traffic to a cluster of BroBoxes which focus on sending Bro's renowned network logs to external analytics tools or pipelines such as Splunk, Kafka, Syslog, or even an external file server.



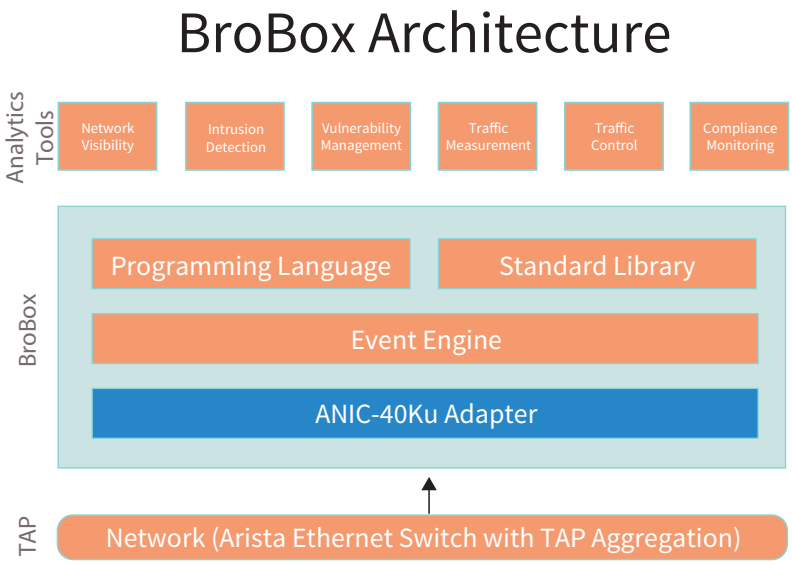
TECHNICAL CHALLENGE

Corelight engineers have deep software expertise and possess intricate knowledge of the inner workings of Bro. In addition to providing the most optimal Bro implementation they are also focused on offering additional value-added capabilities with BroBox such as intuitive configuration, secure operation, automated updates, comprehensive REST APIs and more. However, in order to provide a large-scale Bro implementation Corelight engineers knew that software alone is not enough. So they turned to Accolade to help integrate the FPGA-based packet processing features and horsepower required to meet and exceed the expectations of the most demanding enterprise information and security professionals. The ANIC-40Ku adapter enables lossless 10G performance and key packet processing features such as merging of incoming data streams in timestamp order.

Corelight, Arista and Accolade Deliver Worldclass Bro Solution

THE SOLUTION

Although Bro is an immensely powerful platform, its basic architecture can be depicted with a simple block diagram. At the base layer is the network from which packets are replicated via a wire speed, Arista Ethernet switch with TAP Aggregation and sent to the BroBox for processing and analysis. The ANIC-40Ku adapter gracefully accepts all incoming network traffic with zero packet loss, and performs hardware-based packet processing functions such as flow classification. The BroBox benefits significantly from the ANIC-40Ku because it allows the Bro application to focus on analysis functions. The resulting network traffic is forwarded to the Bro event engine which produces rich and highly-structured data. Finally the data can be further processed by scripts written in the Bro programming language and/or fed into external analytics tools (e.g. Splunk, SIEM) for intrusion detection, traffic measurement, compliance monitoring and other purposes. In addition, many organizations use Bro to re-assemble and extract files, in real time, directly from network traffic streams.



ANIC-40Ku

CORELIGHT PROFILE

Corelight provides enterprise solutions for network security. Founded by the creator and key technologists behind Bro, the widely deployed network monitoring platform, Corelight helps companies answer urgent cybersecurity questions in real time, understand what happened in the past, and detect and prevent attacks. Corelight: illuminate your network. For further information please visit: www.corelight.com

ARISTA PROFILE

Arista Networks was founded to pioneer and deliver software-driven cloud networking solutions for large data center storage and computing environments. Arista's award-winning platforms, ranging in Ethernet speeds from 10 to 100 gigabits per second, redefine scalability, agility and resilience. Arista has shipped more than 10 million cloud networking ports worldwide with CloudVision and EOS, an advanced network operating system. Committed to open standards, Arista is a founding member of the 25/50GbE consortium. Arista Networks products are available worldwide directly and through partners. www.arista.com

ID:170301

Accolade Technology

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

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