Better Security and Network Analytics with EndaceProbe™ and Scrutinizer™ from Plixer

plixer

Together Scrutinizer and EndaceProbes offer a uniquely powerful flow and packet analytics solution that speeds the identification, investigation and resolution of security threats and network and application performance problems.

Plixer's Scrutinizer is a highly scalable, enterprise-wide network traffic analysis and incident response system. It turns an existing multi-vendor network into a distributed sensor by centrally collecting all types of flows and metadata. Leveraging this data, it provides insight into 100% of all wired and wireless communications across the network. Scrutinizer can quickly and accurately identify network and security events such as malware, botnet communication, DNS abuse, low and slow data theft, and poor application performance.

Complementing the powerful monitoring, reporting and alerting capabilities of Scrutinizer, EndaceProbe Network Recorders provide 100% accurate recording of network traffic regardless of network speeds or loads. Recorded network packets are time-stamped with nanosecond-level accuracy allowing network events to be reconstructed with complete accuracy.

The high-fidelity network history recorded by EndaceProbes offers an unparalled source of evidence for analysts investigating the security or performance issues that Scrutinizer detects. Analysts can quickly and conclusively establish the root cause of issues and respond appropriately, dramatically reducing the time to investigate and resolve critical issues. False positives can be quickly identified and flagged so detection rules can be tuned.

PRODUCTS

- EndaceProbe Network Recorders
- Plixer Scrutinizer

BENEFITS

- Accurate, detailed and complete network history provides definitive evidence for investigations
- Streamlined investigation workflow improves SecOps and NetOps efficiency and reduces OPEX costs
- Faster, more conclusive investigations and quicker issue response and resolution
- More effective detection tuning reduces false-positives
- Network packets provide a definitive evidentiary trail

FURTHER INFORMATION

https://www.endace.com/plixer.html

Solution Details

Scrutinizer leverages the Pivot to Packets functionality on EndaceProbes to provide a streamlined investigation workflow for Network Operations (NetOps) and Security Operations (SecOps) teams. Analysts can click on an alert in the Scrutinizer console to quickly find and retrieve related packets from the network history recorded on EndaceProbes. Relevant packets can be downloaded as a packet capture file for analysis using Wireshark® or other tools, or archived for evidentiary purposes.

Conclusion

Scrutinizer's flow and metadata monitoring combined with the deep, contextual network history recorded by EndaceProbes delivers a powerful end-to-end monitoring and investigation solution for network and application performance and security. Integrating the two technologies gives SecOps and NetOps teams broader and deeper visibility into network activity and optimizes the detection, investigation and resolution of network security and performance issues.

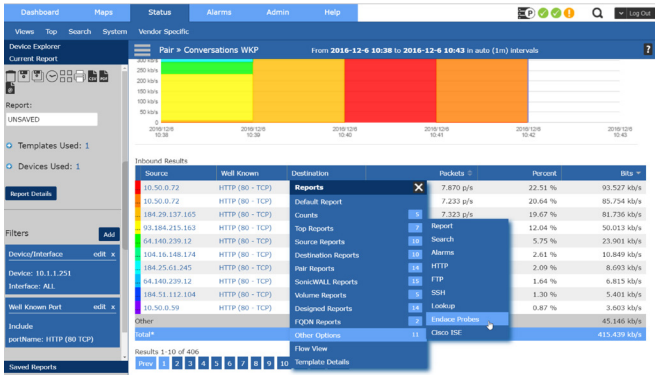

Figure 1. Retrieving the packets relating to an alert in the Scrutinizer console

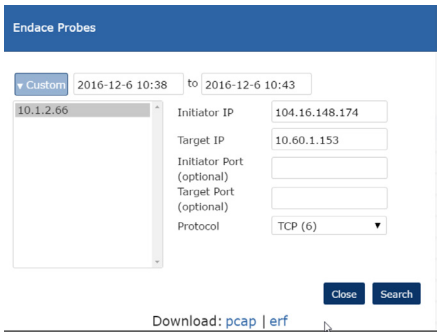

Figure 2. Search parameters are pre-filled, searching returns a packet capture file of related packets

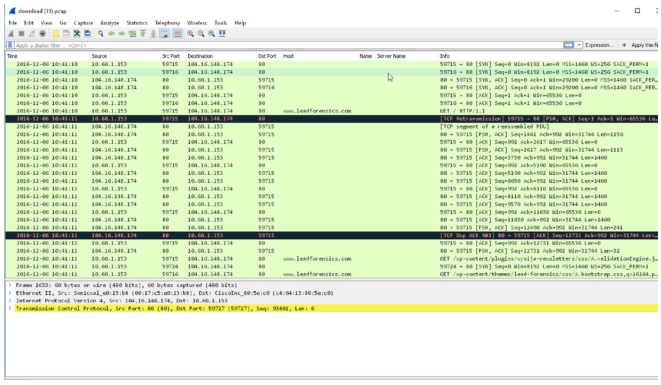

Figure 3. Packet capture file open in Wireshark for analysis

RoHS Compliant

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the Federal Communications Commission [FCC] Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction document, may cause harmful interference to radio communications.

Contact sales@endace.com to arrange a demonstration of the power that integrating EndaceProbe Network Recorders and Plixer Scrutinizer provides.