PACKET LOSS COMPROMISES PCAP ANALYSIS

STORAGE ACCESS IS RESOURCE CONSTRAINED

VALUABLE BUT COMPLEX:

Capturing and recording network packets for analysis has been essential for forensic and root cause analysis to secure networks and ensure their operation. However, despite the value and insight it provides, many organizations only employ this selectively and reactively after an event has been detected – often too late to capture the actual incident. It is time to rethink this approach.

Today's packet capture appliances are complex, inflexible, expensive, and only provide limited access to the data they capture. As storage access is resource constrained, most resources are assigned to capturing the traffic. This process however competes with its ability to index the incoming traffic for easier extraction later on. Reading packets off disk is often slow and selective to not impact capture performance. The challenge for any operator is to balance those processes to ensure that no packets are lost during capture, as this would be devastating for later analysis.

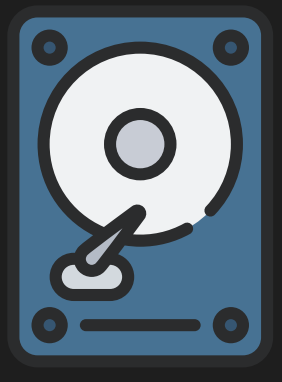
CURRENT TRAFFIC RECORDERS ARE COMPLEX, INFLEXIBLE, EXPENSIVE, AND ONLY ALLOW FOR LIMITED DATA ACCESS – THIS RESULTS IN TOO MANY TRADEOFFS:

TRAFFIC RECORDING IS EXPENSIVE – SO WE LIMIT ITS USAGE OR OUR VISIBILITY AT THE RISK OF NOT BEING ABLE TO ANALYZE THE NEXT INCIDENT:

- Reduce number of links to monitor – but which ones are used for the next attack?
- Reduce traffic through selective filtering –which traffic is important for the next incident?
- Use Packet Brokers to distribute incoming traffic across multiple appliances - which is costly and complex.
- Selective deployment after an event – will the same event happen again?

CAPTURE TAKES PRIORITY AND CAN BE OPTIMIZED AT THE COST OF GETTING TO THE DATA:

- Limit traffic indexing - this slows down data access and limits search options.
- Utilize less expensive SATA drives – however they limit intake and read rates.



THE CURRENT APPROACH TO TRAFFIC RECORDING LEADS TO INCOMPLETE DATA – AND UNRESOLVED THREATS AND INFRASTRUCTURE ISSUES

A new approach is needed that accelerates time-to-resolution through faster reconstruction of events at significantly reduced complexity, size & costs:

- High-speed intake, processing, and storage – at 100 Gbps with zero packet loss.
- Simultaneous, high-speed read and write at intake speed – No need to wait for data with high-speed analysis while not impacting data capture performance.
- Extract based on any information – extract based on any search criteria, not just the one you had to foresight to index.

CONTACT US!

www.Axellio.com
(800) 463-0297
2375 Telstar Dr. Suite 150 Colorado Springs, CO 80920