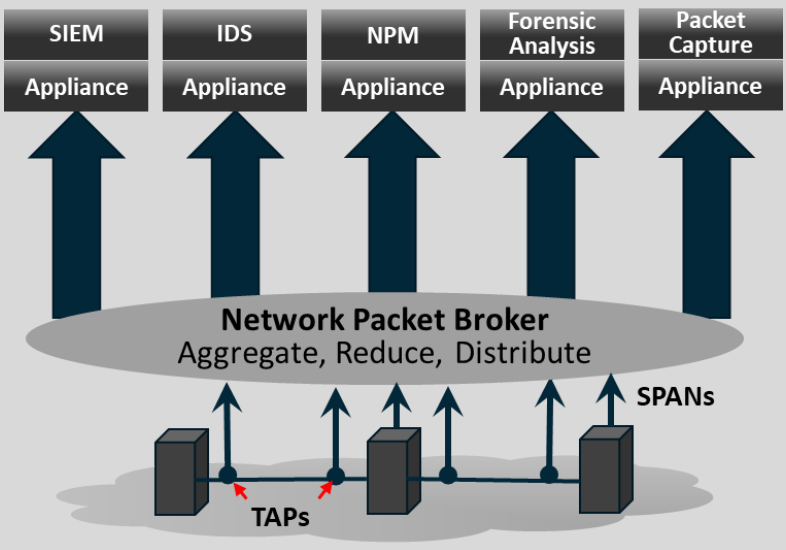
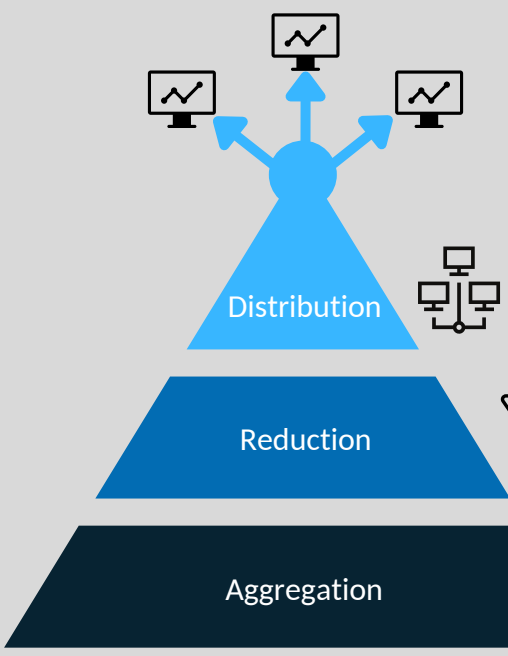
NETWORK & SECURITY MONITORING INFRASTRUCTURE IS COMPLEX AND INCOMPLETE

Monitoring network traffic is the best way to get a complete picture of the security threats as well as network and application problems. However, today's solutions are often costly, complex, difficult to maintain, and are prone to overload situations that result in incomplete information.



Network Visibility Fabrics (NVFs) collect and aggregate network traffic, which is then distributed across the many IT monitoring applications. Based on a combination of network TAPs, SPANs, and network packet brokers, they provide network and security operations teams with the ability to monitor and analyze their network traffic.

In order to have fast, effective issue detection and response, and to maximize the insight those monitoring solutions provide, NVFs need to provide reliable access to all information and cannot allow for any blind spots in the network.



NETWORK PACKET BROKER PRIMARY SERVICES:

Replicates and load balances traffic for the specific needs of each monitoring application

Select, deduplicate, decrypt, and filter relevant data to reduce monitoring application loading

Collect and consolidate network traffic to share across multiple monitoring applications

TODAY'S NETWORK MONITORING APPROACH IS REAL-TIME CENTRIC AND HARDWARE INTENSIVE

Security, network, and application monitoring solutions benefit from the traffic management but struggle to keep up with traffic spikes and a continuing increase in traffic that sometimes exceeds its processing ability, resulting in lost information:

- **Network Packet Brokers** - Can offload traffic from analysis applications but are difficult to configure and maintain in an environment where application infrastructures are dynamically changing
- **SPAN ports** - In high-load situations, SPAN ports stop forwarding traffic or only provide sampled traffic
- **Network and security monitoring solutions** - Unable to keep up with traffic spikes and increasing traffic loads

The only way to respond to today's resource processing challenges is to grow the proprietary hardware for both network visibility and monitoring infrastructure, which is costly and complex:

- Apply **more real-time processing capacity** to the proprietary monitoring appliances
- Apply **more capture and distribution capacity** to your network visibility fabric

Furthermore, packets that could provide further insight for critical forensic and root cause analysis are often discarded after being analyzed. Today's dedicated network packet capture solutions are mostly reactive, which often further delays resolutions, root-cause, and incident analysis. A new approach is needed to increase network visibility and reduce complexity. Network visibility hubs such as Axellio's PacketXpress® can simplify, virtualize, and streamline your network monitoring for critical security, network, and application analysis.

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