Joint Solution Brief

Improving Network Intelligence with Intelligent Traffic Aggregation and Optimization

Highlights

- Terabytes of aggregation and scalable packet-flow traffic optimization
- Reduce unwanted and unmonitorable traffic to optimize monitoring efficiency
- Maximize security and monitoring tool performance for more efficient processing
- Extend monitoring and security tool life and defer future upgrades
- Reduce packet capture volume to speed forensic analysis, reduce storage requirements and increase packet retention times
- Gain optimized visibility into encrypted traffic without expensive decryption
- Optimize packet-flow backhaul traffic to increase transport capacity and reduce WAN costs

The Problem

As network traffic grows exponentially and 100G and higher network speeds proliferate, security and monitoring tools are overwhelmed and continually challenged by the massive amount of traffic to monitor. This unrelenting data explosion forces the security and network operations teams to add incremental monitoring, analytics, and packet storage capacity just to keep up. This is not only excessively expensive, but in many cases futile as an increasing amount of network traffic being delivered to upstream tools is unwanted and has low analytics value.

Consequently, the days of collecting “everything” and letting the analytics layer “sort it out” are no longer viable. To keep up with critical network traffic intelligence, the security and network operations teams still need to collect everything, but now must intelligently identify and deliver only relevant and monitorable traffic to the upstream tools to streamline analysis and optimize historical storage resources.

Optimizing network traffic not only reduces unwanted packets from reaching the analysis and storage layers it enables organizations to extend the useable life of existing lower speed 10G and 40G tools and delay the need to upgrade the monitoring infrastructure to support 100G links and ever-growing traffic volumes. In addition, for organizations with a multi-site monitoring infrastructure, traffic optimization is now an essential requirement to reduce the volume of packets to be backhauled to centralized collection points to lower WAN bandwidth requirements and better control transport costs.

The Joint Solution

The network packet broker (NPB) has become an essential and ubiquitous tool for both network and security operations teams to gain always-on visibility into everything flowing across the network. By combining the Aviz Open Packet Broker™ (OPB) with the NetQuest OMX™ Intelligent Service Node™, SecOps and NetOps teams can create an Intelligent Aggregation Layer™ that more efficiently collects, aggregates, and optimizes network traffic based upon granular user-definable policies for delivery to upstream tools and packet storage.

The Intelligent Aggregation Layer off-loads the burden of prioritizing traffic for analysis and storage at the lower cost traffic collection layer by automating the identification and delivery of only relevant packets for analysis and forensic activities. This enables organizations to improve the value and integrity of monitored network traffic to maximize security and network visibility which extends the deployment life of existing tools, thereby delaying the need to add additional resources and storage capacity.

Together the joint Aviz and NetQuest Intelligent Aggregation Layer empowers organizations to break-through the performance barriers, packet processing limitations and the high costs of smart packet broker systems. By combining cost-effective Open Network switches with ultra-scale packet processing, the combined solution delivers higher capacity with more optimization services at a lower cost than comparable products from alternative vendors.

Aviz Open Packet Broker

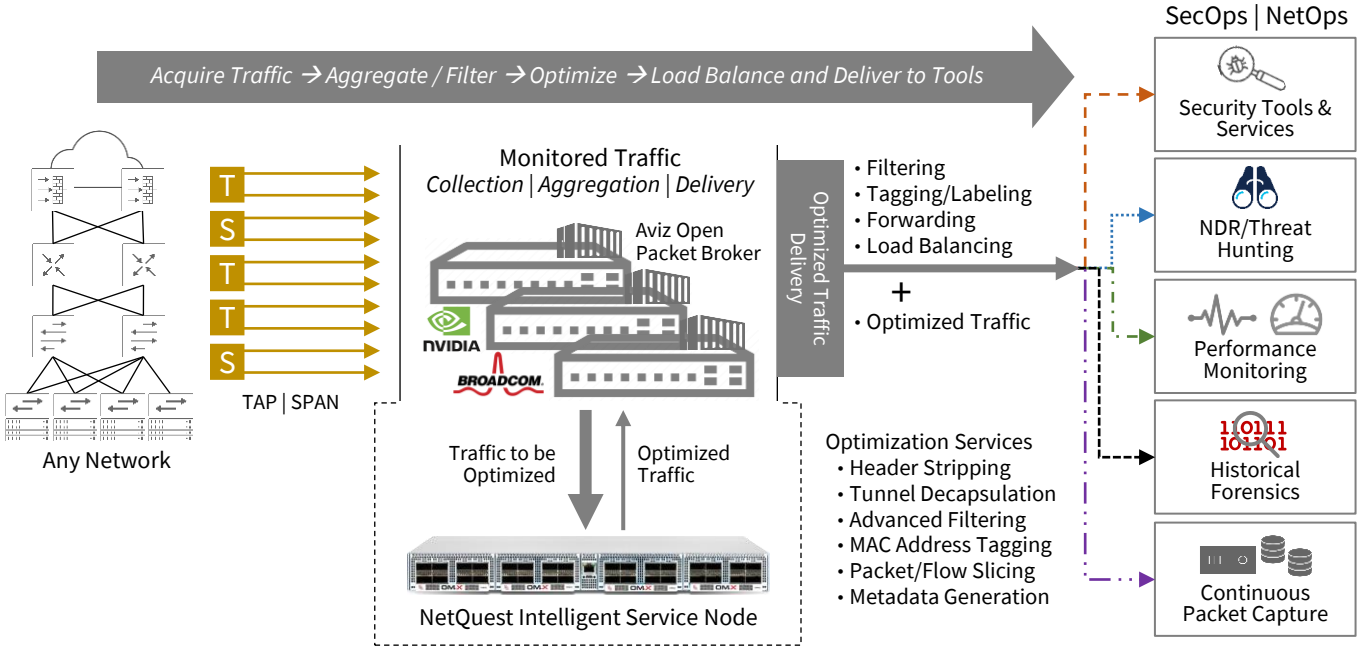
The Aviz Open Packet Broker is the industry's first containerized network packet broker built on top of the SONiC Operating System. Unlike other "whitebox" packet broker platforms, the Aviz OPB delivers on the unfulfilled promise of open networking by running on virtually any OCP compliant Open Network switch that supports SONiC – enabling a truly disaggregated hardware and software operational model. Supporting physical network TAP or SPAN connection points from 1G, 10G, 25G, 40G, 100G and 400G links, and virtualized taps from within Aviz SONiC powered network switches in a data center fabric, the Aviz OPB collects, aggregates, and distributes network traffic to virtually any monitoring tool, analytics or packet storage platform.

NetQuest OMX Platform

NetQuest OMX is a specialized FPGA-based appliance purpose-built to deliver multi-terabit-scale, wire-speed advanced packet processing services and metadata creation for high-performance security and monitoring environments. Its software-defined architecture enables feature flexibility with multiple operational modes on the same hardware across high-density 10G, 40G, 100G and 400G ports. The OMX platform's unique distributed pipeline processing architecture allows all packet optimization services to be activated simultaneously at wire-speed, with sustained performance at scale for the most demanding packet processing requirements. The OMX, when deployed as an Intelligent Service Node, delivers more than 4x higher density, throughput, and packet processing power per rack unit (RU) than alternative smart packet service brokers at a significantly lower cost with a smaller footprint and measurably lower power consumption.

Plug-and-Play Integration

The OMX Intelligent Service Node quickly and easily integrates with the Aviz OPB platform adding Advanced Packet Optimization services to any monitoring environment. The Aviz OPB collects and aggregates network traffic and, based upon user-defined policies, feeds the targeted traffic to be optimized to OMX. OMX performs the desired optimization services and returns the conditioned traffic back to the OPB to redistribute to targeted tools. OMX can retain or drop any tagging added by the Aviz OPB, and if needed, OMX can further tag the conditioned traffic to identify a source port, a specific tool destination or traffic type.



Intelligent Traffic Optimization

The OMX Intelligent Service Node efficiently identifies, prioritizes, and optimizes packet flow traffic at wire-speed to deliver only relevant packets to reduce the upstream tool processing burden, facilitating faster analysis, and enable more efficient packet recording to reduce storage requirements and extend packet retention time. Depending on the network traffic profile and analysis goals, intelligent optimization can eliminate up to 80-90% of unwanted packet-flow traffic. OMX Intelligent Service Node optimization services include:

- **Header stripping and protocol de-encapsulation** – Remove headers and tunnels to deliver inner packets to tools
- **Multi-stage adaptive filtering** – enables granular control over traffic to be sent
- **High-Scale Black/White/Grey list filtering** – high-scale prioritization of traffic classes and IP address filtering to send and traffic classes to drop
- **Packet slicing** – remove unwanted elements from packets for better tool efficiency or compliance
- **Adaptive flow slicing** – truncate specific flow-types, such as encrypted traffic, to remove payloads that are unmonitorable
- **Encrypted traffic optimization** – identify and optimize encrypted traffic without expensive decryption
- **Packet deduplication** – remove duplicate packets collected from different monitoring points
- **Time stamping** – add time stamps to traffic for upstream tools
- **Source labeling** – identify source of optimized traffic, including preserving or removing tags inserted by the Aviz OPB
- **Flow metadata generation** – High scale IPFIX metadata generated from the same optimized traffic (pre- or post-optimization)

High-Capacity Filtering

OMX Intelligent Service Node provides high-scale, real-time traffic classification with advanced packet parsing and filtering capabilities for creating customizable rules to precisely identify traffic that is to be discarded or forwarded. Configurable rule-based priorities assure visibility integrity is not compromised, and analysis resources are efficiently used. Advanced Deep Packet Inspection algorithms step-through each packet to analyze and account for all relevant parameters including beyond protocol headers and when packets are encapsulated within transport tunneling protocols. Up to 7 layers of headers and tunnels can be stripped before the traffic is forwarded, enabling tools to receive the desired inner traffic for analysis.

Encrypted Traffic Optimization

As much as 80% of network traffic is now encrypted, presenting many challenges for monitoring and analysis activities. The OMX Intelligent Service Node recognizes encrypted traffic and enables flexible user definable actions to eliminate or optimize encrypted traffic for upstream tools. Configurable policies allow OMX to identify and drop all traffic classified as encrypted. Alternatively, OMX can identify, and forward only encrypted traffic with specific algorithms, such as SSH, TLS and QUIC, and drop all other encrypted traffic. To support sophisticated threat hunting missions, Adaptive Flow Slicing allows forwarding only packet header and handshake details and discarding the encrypted payloads. This enables advanced threat hunting and NDR tools to quickly recognize fingerprints, signatures, and heuristics to identify emerging threats and pinpoint indicators of compromise without the need for slow and expensive decryption.

Simultaneous Flow Metadata Generation

The OMX Intelligent Service Node can simultaneously act as a high-scale Network Flow Sensor to generate and deliver 1:1 unsampled IPFIX Metadata for non-packet-based tools from the same packet-flow traffic. When activated, contextual Metadata is created at the same time as packet traffic is processed. Flow Metadata is delivered as a separate IPFIX output stream and can be distributed, and load balanced to up to 16 different flow collectors. OMX high-scale Metadata generation capabilities range from standard five-tuple network-level metadata, to enriched application, protocol, and encrypted traffic metrics. OMX Metadata generation capabilities extend the value of the OMX platform while reducing TCO and operational complexities associated with managing multiple probes and sensors.

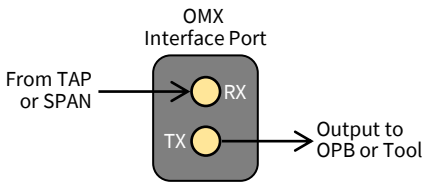
High-Scale Single-Pass Processing

All OMX Intelligent Service Node optimization services are applied in a single pipeline process for each input packet flow – so there is no need for recirculating traffic back and forth when multiple optimization services are needed. This significantly increases throughput and performance and eliminates undesirable packet service latency. Multiple Aviz OPB platforms can be connected directly into the same physical OMX system while maintaining the integrity of the source data. The interconnection link speed between the OMX and Aviz OPB is determined by the peak volume of traffic to be processed – so, a single 10, 40 or 100G link or multiple links can be used to support higher volumes of traffic for conditioning.

Joint Solution Brief

Half-Duplex Ports Double Port Capacity

The OMX Intelligent Service Node receives, processes, and returns optimized packets on the same physical port allowing each physical port to be operated as two distinct and separate interfaces. Consequently, each physical port is receiving traffic to be optimized on the RX side and is using the TX side to send optimized traffic back to the Aviz OPB or directly to upstream tools. This doubles the OMX Intelligent Service Node capacity to up to 32x 40/100G input ports (ingress traffic) and 32x 40/100G conditioned traffic output ports (egress traffic) – providing up to 64x 40/100G ports with 6.4 Tbps of aggregate bi-directional wire-speed throughput in a single rack unit (RU).



High-Scale Optical WAN Monitoring

OMX can be tasked with monitoring high-speed WAN links such as OTN or SONET/SDH by connecting to the optical fiber pair and identifying all traffic traversing the fiber. OMX auto-discovers WAN traffic and converts this traffic to IP Packets suitable for traditional monitoring tools – eliminating the need for expensive and specialized WAN monitoring tools. The WAN traffic, now converted to standards-based IP packets, can be conditioned in the same manner as native IP packets, and delivered to the Aviz OPB for aggregation and distribution to security and performance monitoring tools. OMX WAN-to-IP packet translation retains details on the WAN transport characteristics and delivers these metrics within the transformed IP packet.

The Value Realized

The combined Aviz-NetQuest solution integrates two industry-leading platforms to provide organizations with an ultra-high-scale, lower-cost approach enabling the construction of a truly flexible and powerful Intelligent Aggregation Layer. When compared to other well-known smart packet broker systems, the combined Aviz and NetQuest solution delivers significantly higher density with more capacity and functionality and greater performance at scale than alternative solutions in its class to meet the most demanding monitoring requirements.

About Aviz Networks

Aviz Networks enables SONiC deployments in data center & edge networks by delivering platform and ASIC agnostic, easy-to-use applications for network observability, orchestration, and assurance. The Aviz Open Packet Broker is the industry's first containerized Network Packet Broker application built on top of SONiC NOS to collect and aggregate network traffic and feed the data to any network or security tool.

About NetQuest

NetQuest provides market-leading Ethernet and WAN Flow and Packet-Based traffic monitoring solutions that deliver the highest levels of accuracy, capacity, and performance at scale. Monitoring solutions from NetQuest are deployment-proven across thousands of network segments in enterprise, carrier, government, and defense agency networks across the globe, empowering security operations teams with high-scale visibility and actionable traffic intelligence.

NQ-ISN-JSB-0523

NetQuest Corporation
523 Fellowship Road, Suite 205
Mount Laurel, NJ 08054 USA
+1-856-866-0505 | sales@netquestcorp.com
www.netquestcorp.com