Scaling Network Flow Analysis for Cyber Security

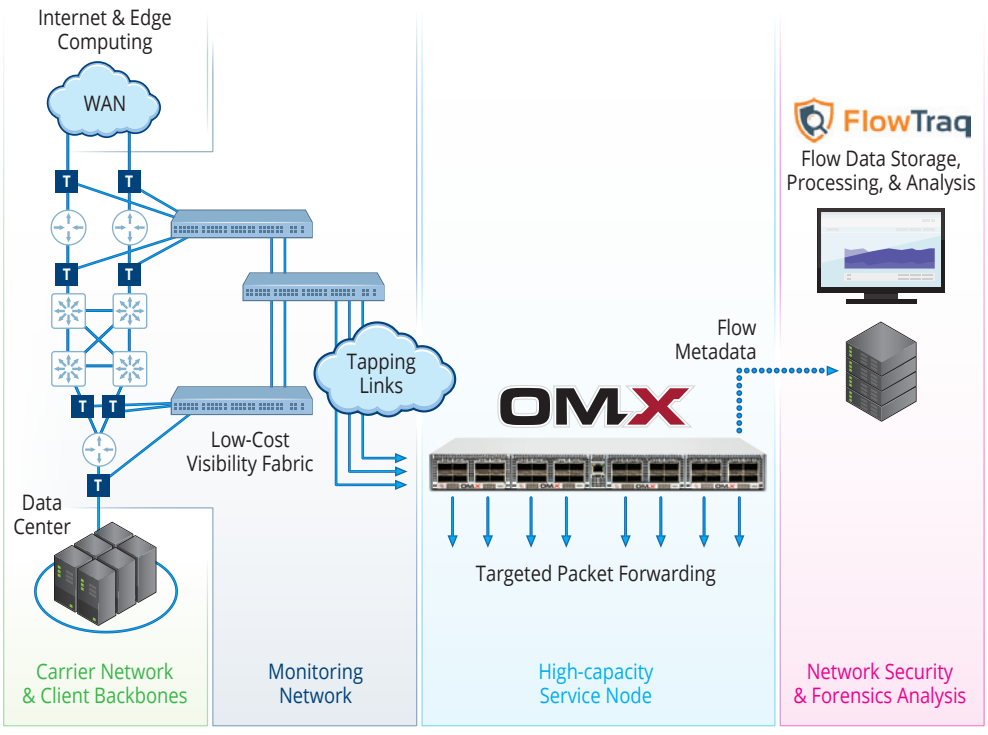
The geographic expansion of the Internet, the multitude of connected devices, and the growing array of services and content continue to fuel network traffic growth. Tier 1 Internet Service Provider (ISP) peering connections are at the epicenter of this traffic growth and are embarking on network migrations to N X 10G and 100G peering links to meet this demand. Maintaining security visibility at these higher speeds is increasingly difficult.

Other providers of remote compute and network access such as Enterprise Public Internet Links, Cloud Direct Connect, and Edge Connect Providers are similarly having to build out N X 10G and 100G infrastructure – as well as manage and secure those environments for their customers.

Oversubscribed or bursty traffic links can create visibility outages for monitoring solutions that rely on standard high-speed switches/routers to forward packets or generate flow metadata. This effectively lowers visibility when it is needed most. Utilizing CPU-based probes or Network Packet Brokers to inspect traffic, with horizontal scaling to expand capacity, is quickly becoming cost prohibitive as these architectures do not scale with increasing backbone speeds. Other approaches, such as traffic sampling to reduce processing burden, limit analytical tool efficacy as lower sampling rates lead to fewer security incidents detected.

NetQuest OMX / Riverbed FlowTraq Network Security Solution

A NetFlow/IPFIX unsampled flow metering solution for today's higher capacity, at risk, links must support forensically accurate, line-rate flow metering of traffic at rates ranging from N X 10G up to 100Gbps per port. In order to ensure full visibility, the solution must also support processing of up to 50 million active flows per 100G of traffic.



Who We Are

NetQuest is a trusted and longstanding supplier of high-performance Cyber Surveillance solutions to government agencies around the globe.

With the introduction of the OMX Optical Monitoring Exchange we have built upon our 30+ years of network monitoring experience and applied the indepth cyber knowledge we have gained to offer an optimized solution for complex network infrastructures, such as fixed line/mobile service providers and large-scale enterprise networks.

NetQuest
Monitoring Access Solutions

Instrumentation Architecture

Given the challenges of trying to detect security threats on high-capacity traffic links, an optimal monitoring architecture should complement any packet inspection with analysis of unsampled flow metadata. The diagram (page 1) details a qualified high-performance network metadata extraction and collection architecture for network security analysis.

- 10/100G Monitoring Network that provides tapping and aggregated packet access.
- High-Capacity Service Node optimized for unsampled flow metadata generation & targeted packet forwarding.
- Network Security & Forensics Platform purpose-built for high volume flow metadata analysis and cyber threat hunting.

The NetQuest OMX3200 Service Node receives network traffic from the Monitoring Network, performs line-rate unsampled flow metering, and exports the resulting IPFIX flow records to a cluster of bare metal commercial-off-the-shelf (COTS) servers running FlowTraq software that performs flow metadata collection, storage, and security analysis.

Monitoring Network

Several leading switch/router vendors have introduced visibility fabric solutions leveraging their merchant silicon switches combined with management software to enable flexible packet access for a cost-effective visibility fabric. When compared to traditional network packet broker offerings, the price-per-port advantage and broader networking technology options of this approach increase as port speeds migrate to 100/400G.

NetQuest OMX3200 High-Capacity Service Node

The NetQuest OMX3200 High-Capacity Service Node is a multi-terabit traffic flow visibility platform supporting metadata generation and advanced packet processing in a compact modular 1RU hardware platform. Each of the 4 OMX3200 hot-swappable modules support line-rate packet processing on 8 configurable QSFP28 interfaces (100G or 4x10G) for a total port density of up to 32x100G. The OMX3200 supports:

- Unsampled Network Metadata Generation transforming packets to flow-based metadata (IPFIX) for highly scalable N x 10/100G Flow Analysis.
- Advanced Packet Processing providing header/tunnel stripping, port labeling, MAC tagging and intelligent packet forwarding to downstream packet analysis tools.
- Automated WAN network discovery and targeting of traffic within Packet Optical Network hierarchy.

FlowTraq Network Security and Forensics Platform

The FlowTraq Network Security and Forensics Platform gives network operators, security professionals and cyber hunters a high-speed, highly scalable solution to detect and generate real-time alerts on changing traffic patterns, suspicious activity such as Distributed Denial of Service (DDoS) and brute force attacks, malware, zero-day threats, malicious botnets, new viruses, and other threat vectors. FlowTraq is optimized to collect and store large volumes of unsampled flow data to analyze network traffic with a powerful network behavioral engine that "learns" various patterns of behavior on your network. Key capabilities of the FlowTraq architecture include:

- Big Data Database – Built upon modern parallel architectures, with distributed load balancing clusters.
- Triple-Split Storage Architecture –
  - Most recent flow data is quickly accessed directly from the RAM database.
  - Longer queries are serviced from a local SSD database.
  - Historical flow data is archived in spinning RAID or remote SAN/NAS solutions.
- Long-Term Trends & Baselines – The behavioral engine learns patterns of behavior on your network and stores long-term trends for all interfaces and network traffic groups to quickly evaluate peering relationships and link utilization.
- Automated Traffic & Security Alerts – Detects a complete range of network anomalies including simple traffic threshold alerts, deviations from established baseline behavior, DDoS events and user-defined security policy violations.

Demonstrated Visibility and Performance

- Using unsampled IPFIX to monitor and secure a Tier 1 ISP 100G peering connection.
- *NetQuest* OMX3200 IPFIX IPv4/IPv6 flow record interworking with *FlowTraq* collection and analysis.
- *NetQuest* OMX3200 generating unsampled flow data and exporting standards-based IPFIX flow records for a 100G peering link (peak traffic).
- *Riverbed FlowTraq* collecting unsampled IPFIX flow records for analysis of a 100G peering link (peak traffic).

Results

A single OMX3200 module supported unsampled IPFIX flow generation (250 KFPS) for a 100G full-duplex ISP Peering link (2 inputs), with average (66 GbE) and peak (109 GbE) loads with no drops. **The NetQuest OMX3200 supports flow metadata generation on up to 16 X 100G inputs in a 1RU footprint!**

FlowTraq running on a single dual-socket server performed unsampled IPFIX collection and analysis for the 100G full-duplex link with no drops. **FlowTraq can be extended with multiple processors, multiple nodes, and multiple clusters!**

More detailed information on the High-capacity Flow Generation & Analysis from Riverbed FlowTraq – NetQuest is available as a white paper from your NetQuest Sales associate.

NetQuest Corporation • 523 Fellowship Road • Mount Laurel, NJ 08054 USA • +1.856.866.0505 • Email: info@netquestcorp.com