APPLICATION NOTE

High-Capacity NetFlow/IPFIX Generation for Securing Internet Peering Links

The Internet backbone is a high-capacity network of the world's largest Internet Service Providers (ISPs) peered together into a single seamless network. These Tier 1 ISPs also extend peering connections to other service providers and large content providers enabling universal connectivity around the globe. In any network, however, the most vulnerable point is often where traffic enters and exits the internal network, and this is particularly true for these public Internet peering connections. They represent a strategic location to instrument for security and most organizations inspect the traffic flowing on these links using technologies like NetFlow/IPFIX to help identify and mitigate threats.

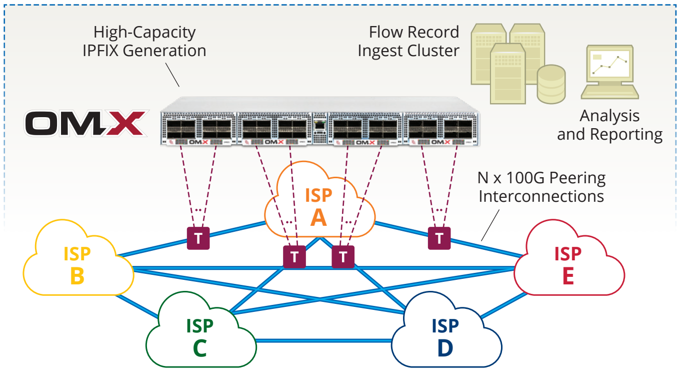
Security Visibility Challenge

Network traffic continues to grow at dramatic rates driven by the multitude of connected devices and the increasing array of services, and ISP peering connections are at the epicenter of this traffic growth. Tier 1 ISPs and their peering partners are embarking on network migrations to 100G peering links to meet this demand, but maintaining network visibility at these high speeds is increasingly difficult

The advancements in networking technologies to satisfy growing bandwidth demand is outpacing CPU performance gains making it more and more challenging to maintain acceptable visibility. Monitoring traffic directly in high-speed switches/routers can adversely impact network performance and often limits visibility. Continuing to utilize CPU-based probes or Network Packet Brokers through horizontal scaling to expand capacity is quickly becoming cost, rack space and power consumption prohibitive. Other approaches such as traffic sampling to reduce processing burden limits visibility and increases risk. As service providers rearchitect their monitoring infrastructures to support peering link migration to 100G and beyond, new approaches are required to offload and optimize traffic analysis.

The Solution

NetQuest's OMX Optical Monitoring Exchange leverages state of the art Field Programmable Gate Array (FPGA) technology in a purpose-built solution to scale a flow analysis architecture as links migrate to 100/200/400G.


High-Capacity IPFIX Generation
Flow Record Ingest Cluster
OMX
Analysis and Reporting
N x 100G Peering Interconnections
ISP A
ISP B
ISP C
ISP D
ISP E
T

- Passive Monitoring of High-Capacity Peering Interconnections
- N x 100G Unsampled Flow Metering
- Automatic Packet Header and Tunnel Preprocessing
- Compact Modular 1RU Platform Optimizes Space, Power, Cooling

The OMX delivers high-capacity IPFIX flow metering and flow record generation for network security that helps answer the who, what, when and where. The compact modular design supports up to four flow processing modules in a single rack unit, with each module supporting unsampled N x 100G flow processing. The OMX also supports targeting specific flows of interest and packet forwarding to other tools for deeper analysis.

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 Corporation

523 Fellowship Road
Mount Laurel, NJ 08054 USA
+1 856.866.0505

info@netquestcorp.com

NetQuest
Monitoring Access Solutions