Multinational Telecom Provider Delivers Visibility and Security on Internet Peering Links

OMX3200 enables 10/100G backbone security with delivery of packets, flow metadata and investment protection

Peering links are the unknown connections that most end-users do not know exist - but enable the operation of the world’s Internet and telephony carriers. Peering links are the connections that knit together the fabric of remote, long haul, and regional data providers so that your message can reach any corner of the globe.

NEXT GENERATION PROTECTION

The Company realized that in order to protect their customers from the storm of attacks that are growing yearly, they needed a new method of protection.

The solution was created by building a monitoring, analysis, and filtering infrastructure at their primary linkage points – peering links. This new architecture could serve as a monitoring overlay to protect their local loop, mobile, data, and long-haul networks while eliminating bottlenecks in their customer network.

The solution could scale, had a defined number of traffic visualization points, and could roll-up to a 24/7 monitoring framework.

GRANULAR VISIBILITY

With all the technology available to The Company, their best data for tracking network traffic and security threats were the packets flowing over the fibers. Sampled metadata flows were of little use for detecting subtle attacks such as low and slow scans, worm propagation, advanced persistent threats (APT), exfiltration events, and botnets. Full unsampled flow records are required as well as having the ability to see the original packets if more detail is required.

Solutions were available for Enterprise networks, but capturing data on multiple 10G links, 10G Link Aggregation Groups (LAGs), and 100G carrier-grade backbones required a different toolset.
NetQuest OMX3200 enables The Company 10/100G to provide backbone security with optimized packet streams and unsampled flow metadata

HIGH BANDWIDTH VISIBILITY

HIGH CAPACITY

The Company needed a way to handle a variety of link speeds and feeds from a visibility fabric through optical taps. The NetQuest OMX3200 provides 4 separate modules which plug into a 1 RU system. Each of the modules provides 4 X 100G inputs with 4 full packet streams capable of generating full unsampled metadata records for all links. Standard IPFIX data records are output through a separate 10G port while full targeted packets are also forwarded for detailed forensics.

Each OMX module can also be provisioned to ingest 16 X 10G links for high-density data extraction on high-capacity 10G LAG bundles.

FILTERING AND TUNNEL REMOVAL

Just being able to create flows and packet streams is not enough. The Company also took advantage of the OMX’s capability of stripping MPLS labels, VLANs, and IP tunnels to reduce processing required of downstream packet analysis tools. The OMX’s filtering toolkit offered further options to offload downstream tools by providing The Company the option to remove packets associated with low-risk applications.

FLOW METADATA FOR SECURITY

In order to make sense of the flow data extracted from a large number of peering links, The Company devised a method whereby downstream tools can read the flow records and through data analysis and the link records (i.e. Observation Domain) provided in the metadata, pinpoint the exact location of where an individual flow was created. This is significant because with unidirectional backbone links and hot potato routing techniques, the return portion of the conversation is typically located on another link. It also enables them to point their security tools to the proper Peering Links and determine attack locality, whether inside or outside The Company’s network.

The Company used automated analysis functions to find anomalies in flow metadata and trigger protective measures.

INVESTMENT PROTECTION

The Company requires that their Peering Link monitoring solutions have the flexibility to handle multiple generations of backbone technologies without having to replace their architecture. Fiber optic technology increase link speeds by a factor of 2 to 10 times every 5 years. The OMX supports their 10G and 100G requirements and if needed, can be upgraded to different capability with an easy 5-minute module update.

The OMX platform does not lock customers into a particular architecture and can grow with speeds and the number of links through a flexible licensing and provisioning structure.