Product Brief

Packet Services Broker

Optimized Packet Forwarding for Telco-Scale Network Visibility

Highlights

- Dramatically reduce costs of network security solutions for packet capture, analysis and backhaul
- High-scale customizable Traffic Policy Engine optimizes packet forwarding by identifying specific traffic components to forward or drop
- Process 5G mobile network and other transport protocols for subscriber-level insights
- Scale network visibility to monitor 100G links with up to 1.6 Tbps throughput in a single rack unit.

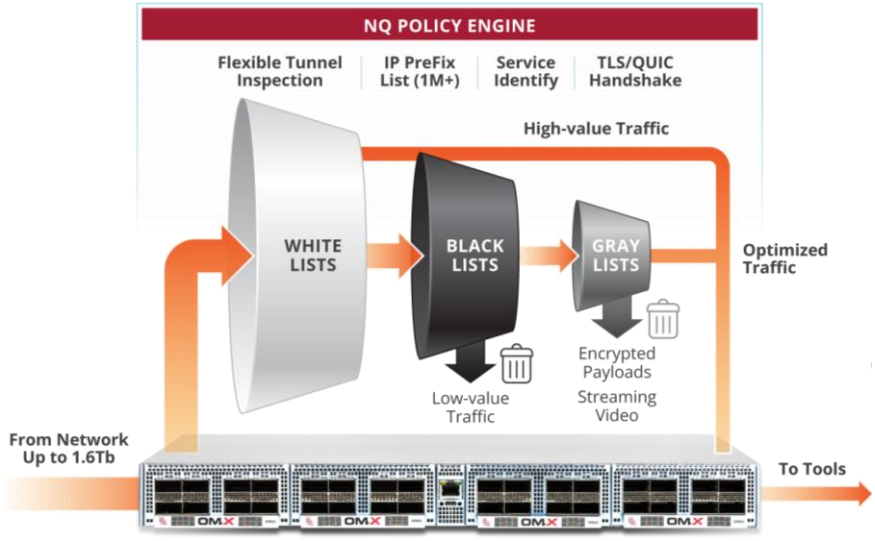
Cyber threat hunters and network security teams are facing a massive challenge defending against increasingly complex cyber threats. A continuous rise in traffic volume combined with an increasing percentage of encrypted traffic is forcing CISOs to exhaust their budget to maintain visibility and protect their network. This challenge is magnified for telco security and government defense applications where the attack surface is truly global.

Security Monitoring Optimization

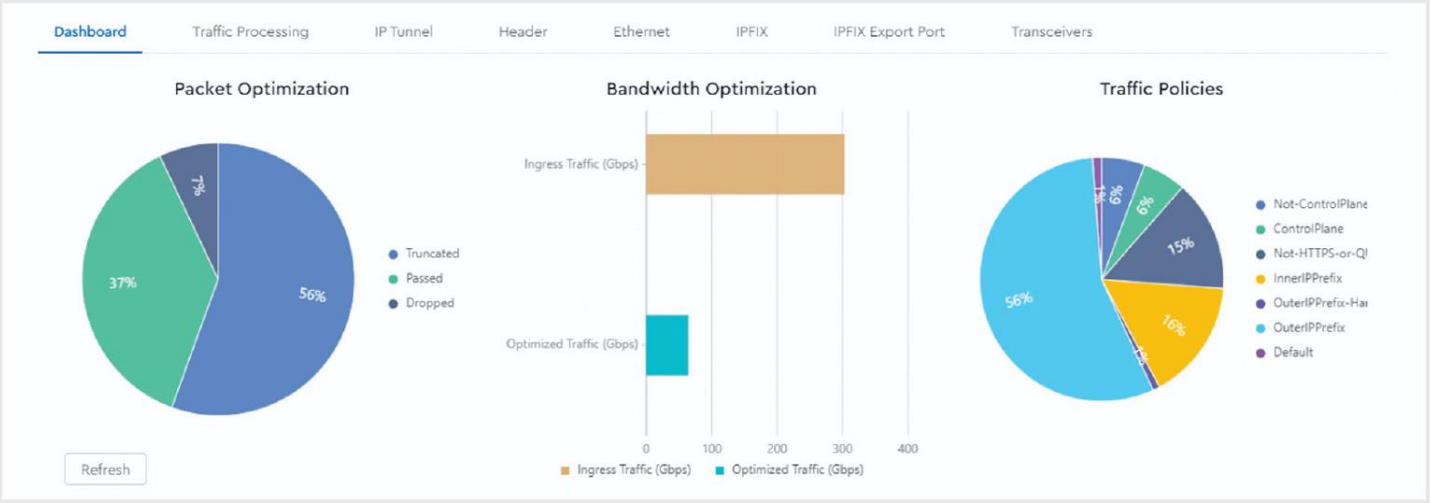
Purpose-built for network security teams, the NetQuest Packet Services Broker is an easy-to-deploy bump-in-the-wire between network TAPs and security tools. The Packet Services Broker can help to dramatically reduce threat hunting costs by intelligently removing traffic that provides little value to the cyber mission. This is done by identifying the following for each packet:

- Traffic payloads encrypted with increasingly hard to break algorithms such as TLS 1.3 and IETF QUIC
- Streaming services like voice and video such as Netflix™, Hulu, Disney+, YouTube, Amazon, etc.

The Packet Services Broker can conditionally drop these packets completely or truncate the packet payloads while only passing valuable headers that can be used by threat hunting tools to pinpoint anomalous traffic or other Indicators of Compromise. The Packet Services Broker can also apply custom filters using large IP prefix lists to identify exceptions to be passed to security tools. These exceptions are typically used to forward high-value traffic such as 5G control plane, or suspect traffic identified by threat intelligence feeds.



Product Brief



Configurable Traffic Policy Engine

Advanced packet parsing and filtering capabilities for creating customizable rules dictating the precise traffic that is discarded or forwarded to security tools. Traffic policies assign configurable rule-based priority to assure no visibility is compromised and cyber threat hunting resources are used most efficiently.

Terabit-Scale Packet Processing

Designed for mobile operators and government defense agencies, the Packet Services Broker packs DPI-based processing for up to 16x 100G interfaces into a compact 1RU footprint. To maximize efficiency of network security tools, traffic can be intelligently reduced by 50 to 80 percent and remaining optimized packets can be load balanced to local or remote tools via GRE.

High-Capacity IP Address Filtering

the Traffic Policy Engine supports massive IP prefix lists to ensure proper visibility is maintained. Support for lists containing 1M+ IP address prefixes for identifying high-value traffic from sources such as threat intelligence feeds, and low-value traffic such as popular streaming voice or video services such as Netflix™, Disney+, Hulu and others.

The NetQuest Packet Services Broker includes the following capabilities to optimize packet forwarding to security tools:

- **Traffic Gray Listing** goes beyond standard white and black-listing to provide an additional dimension to standard traffic policies. As blacklisted traffic is dropped and whitelisted traffic forwarded intact, the Traffic Policy Engine gray listing can go deeper into each packet-flow to intelligently forward just the most critical packet information to the network security tools.
  - Drop traffic classified as encrypted but forward all packets carrying TLS and QUIC handshake messages
  - Forward key IP packet header information but truncate encrypted IP payloads using a configurable slicing length
  - Detect and drop packets carrying popular streaming video services while forwarding just enough information for security tools to account for each session
- **Advanced Packet Inspection Algorithms** step thru each packet to analyze and account for all relevant parameters. 5-tuple information and TLS/QUIC handshake details can be identified including when packets are encapsulated within VLAN, MPLS, GTP, GRE, IP-in-IP, PWE3, VXLAN and other transport tunneling protocols.

Processing Throughput	Tunneling Inspection	IP Prefix Filtering	Packet Payload Truncation	Handshake Detection	Load Balancing	Remote SOC Forwarding	Metadata Generation
1.6Tbps	GTP, GRE, IP-in-IP, etc	1M+ Prefixes	Configurable Length	TLS, IETF QUIC	Session-Based or Equal Distribution	GRE Encapsulation	1:1 or Sampled IPFIX

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