Joint Solution Brief

Highlights

- Monitor massive volumes of network traffic more efficiently enabling improved threat intelligence at scale
- Target specific types of traffic to deliver high-value packets to the Stamus Probe for improved monitoring efficiency
- Optimize visibility into encrypted and streaming video traffic without expensive decryption
- Combine multiple monitoring points into a single Stamus Network Probe and scale capacity for higher-speed links
- Reduce instrumentation costs and enabling broader coverage for critical east-west network observation points
- Optimize traffic ingest efficiency and meet compliance requirements with intelligent packet and flow truncation

Optimizing Network Traffic Visibility to Scale Threat Detection and Response

The Problem

The scope, scale, and impact of cyberattacks continues to grow causing security operations teams and threat hunters to face unprecedented challenges defending against the increasing volume and complexity of cyberthreats. In today's hyperconnected world, everything crosses the network, and because the network interconnects everything it provides an unbridled pathway to reach the many attack surfaces to be protected. Consequently, the network sees everything and contains massive volumes of untapped intelligence that can be harnessed and mined to identify, understand, and stop threats and attacks as they emerge.

The challenge is that the volume of traffic crossing networks has reached unprecedented levels and continues to grow exponentially. With the growing adoption of 100G and higher network speeds, security and monitoring tools are easily overwhelmed by the massive amount of traffic to monitor. The need to monitor more traffic paths, such as east-west traffic flows to observe lateral movement, combined with the unrelenting data explosion forces the security and network operations teams to continually add incremental monitoring, analytics, and packet storage capacity just to keep up. This is not only excessively expensive, but in many cases futile, because an increasing amount of the network traffic being delivered to cyber tools has limited analytics value.

The reality is that the days of collecting 'everything' and letting the analytics tools 'sort it out' are no longer realistic or viable. To keep up with the massive volumes of network traffic to extract critical intelligence the security and network operations teams must now intelligently identify and deliver only relevant and monitorable traffic to security tools to optimize capacity, streamline analysis, and extend historical forensics capacity.

The Joint Solution

Virtually all cyber threats and attacks generate activity that can be observed from network traffic, so continuous network monitoring to identify threats and breaches has become mission critical. Security teams use the Stamus Security Platform (SSP) to tap into the inherent power of network traffic to uncover every possible threat for proactive threat hunting, automated detection, and incident investigation to protect their organization's most critical assets. The challenge is that not all network traffic flows are created equal and some traffic – such as streaming video – is less likely to contain indicators of malicious activity, causing valuable analysis resources to be consumed to assess irrelevant traffic.

The NetQuest Packet Services Broker adds significant value to the Stamus Networks monitoring architecture by intelligently assessing, conditioning, and optimizing network traffic to identify and deliver only high-value packets and discard low-value traffic. Depending on the network traffic profile, packet optimization can reduce network traffic volumes from 50 to 80 percent without compromising the integrity and value of the network traffic to be analyzed. Packet optimization allows the Stamus Network Probe to focus on analyzing the traffic that matters and off-loads valuable processing resources from analyzing irrelevant traffic, such as in the case of certain encrypted traffic packets that cannot be inspected.

Offloading encrypted packet payloads and reducing the inbound traffic volume allows a single Stamus Network Probe to be used to observe multiple network links. Intelligent traffic optimization also enables a lower speed Probe to monitor higher speed links, or higher speed Probes to monitor multiple network links. This reduces instrumentation costs while enabling broader network coverage for critical observation points such as east-west network links to gain much needed visibility into lateral traffic movement.

Combining the NetQuest Packet Services Broker with the Stamus Security Platform brings invaluable packet optimization capabilities that enable security operations teams to monitor massive volumes of network traffic more efficiently enabling improved threat intelligence at scale.

Stamus Security Platform

The Stamus Security Platform is a broad-spectrum and open Network Detection and Response (NDR) system that delivers response-ready threat detection from multiple intelligence sources, open interfaces, advanced lateral movement tracking, and Declarations of Compromise™. The Stamus Security Platform provides powerful threat hunting and incident investigation capabilities that uncovers subtle attack signals lurking in the network to identify serious and imminent threats – with a complete timeline for each host under attack and the necessary evidence to quickly respond and stop breaches before damage is done. The Platform performs the difficult work of automating event triage to identify the most serious threats that need immediate attention – empowering the security team to respond quickly, efficiently, and decisively with increased confidence.

The Stamus Security Platform consists of two components: Stamus Network Probes and Stamus Central Server – each playing a critical role in scaling the system. Stamus Central Server and Stamus Network Probes can be deployed in private cloud, public cloud, on-premises, or hybrid environments. The Stamus Network Probe passively monitors, inspects, and analyzes network traffic to capture network transactions, perform real-time threat detection, and enrich detected events with advanced metadata.

The Stamus Probe delivers the locally analyzed data to the Stamus Central Server for an additional layer of threat analysis leveraging machine learning and algorithmic threat detection, along with automated event triage.

NetQuest Packet Services Broker

The NetQuest Packet Services Broker delivers multi-terabit, wire-speed advanced packet processing services for high-performance security monitoring environments that rely on accurate and reliable network packets. The Packet Services Broker provides the density, performance and packet optimization capabilities needed to inspect and optimize Petabytes of network packets per hour for both clear and encrypted traffic.

Leveraging the NetQuest OMX platform's software-defined architecture enables feature flexibility and support for multiple operational modes on common hardware across high-density 10G, 25G, 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.

Intelligent Traffic Optimization

The NetQuest Packet Services Broker efficiently identifies, classifies, prioritizes, and optimizes packet-flow traffic at wire-speed to deliver only relevant packets to Stamus Network Probes. The traffic optimization services reduce the upstream processing burden enabling more efficient packet inspection to facilitate faster analysis and increase the traffic ingest capacity of the Stamus Probe. Depending on the network traffic profile and the monitoring and analysis goals, packet optimization can off-load from 50-80% of unwanted packet traffic to the Stamus Probe. This helps scale Stamus Probe capacity to enable the monitoring of higher speed links with lower speed probes while improving the integrity and increasing the value of monitored network traffic. Optimization services include:

- Target specific types of traffic to deliver only high-value packets to the Stamus Probe eliminating the processing burden and metadata creation cycles for low-value traffic
- Identify and optimize encrypted and streaming video traffic and deliver only relevant components for analysis by the Stamus Probe
- Perform packet slicing to remove unwanted elements from packets to improve traffic ingest efficiency and meet compliance requirements
- Apply adaptive flow slicing to optimize specific flow-types, such as encrypted or video traffic, to send initial and final handshakes and drop payload packets
- Removal of up to 7 layers of headers and encapsulation tunnels to deliver only the inner packets to the Stamus Probe making packets easier to ingest and analyze

High-Capacity Filtering

The cornerstone of the NetQuest Packet Services Broker is it's high-capacity, real-time traffic policy engine that performs advanced traffic classification and filtering services tailored specifically for security monitoring. Users can define policies to precisely identify high-value traffic that is to be forwarded to the Stamus Probe versus low-value traffic which can be discarded. Configurable rule-based priorities assure analysis resources are used efficiently without compromising traffic integrity. High-scale IP prefix lists, with over 1.2 million filters, enable sophisticated precision traffic prioritization for services, IP address, and IP CIDRs. This allows sending specific traffic classes or source IP addresses, such as traffic destined for critical services or traffic originating from suspect locations identified by threat intelligence feeds to the Stamus Probe for analysis.

Encrypted Traffic Optimization

Depending on the network environment as much as 80% of network traffic can be encrypted, presenting many challenges for the monitoring and analysis of network traffic. The NetQuest Packet Services Broker automatically recognizes encrypted packets without the need for slow and expensive decryption and applies user definable actions to drop or optimize this traffic for delivery to the Stamus Network Probe. User definable policies allow the automation of identification and actions including:

- Identify and truncate encrypted traffic to only forward header and handshake packets and discard the unusable encrypted payloads
- Drop all low-value encrypted traffic based on IP Prefix list or service type
- Forward only specific encrypted traffic types, such as SSH, and drop all other encrypted traffic

Eliminating low-value encrypted packets significantly reduces the traffic volume and packet processing burden on the Stamus Probe enabling more efficient and sophisticated threat hunting to accelerate identifying emerging threats and pinpointing indicators of compromise. Similar optimizations can be applied to commercial streaming video traffic, such as Netflix, AppleTV+, Amazon Prime, and others. The Packet Services Broker detects video traffic and can forward only session set-up packets and drop the remaining streaming video content packets, or simply drop all streaming video flow packets.

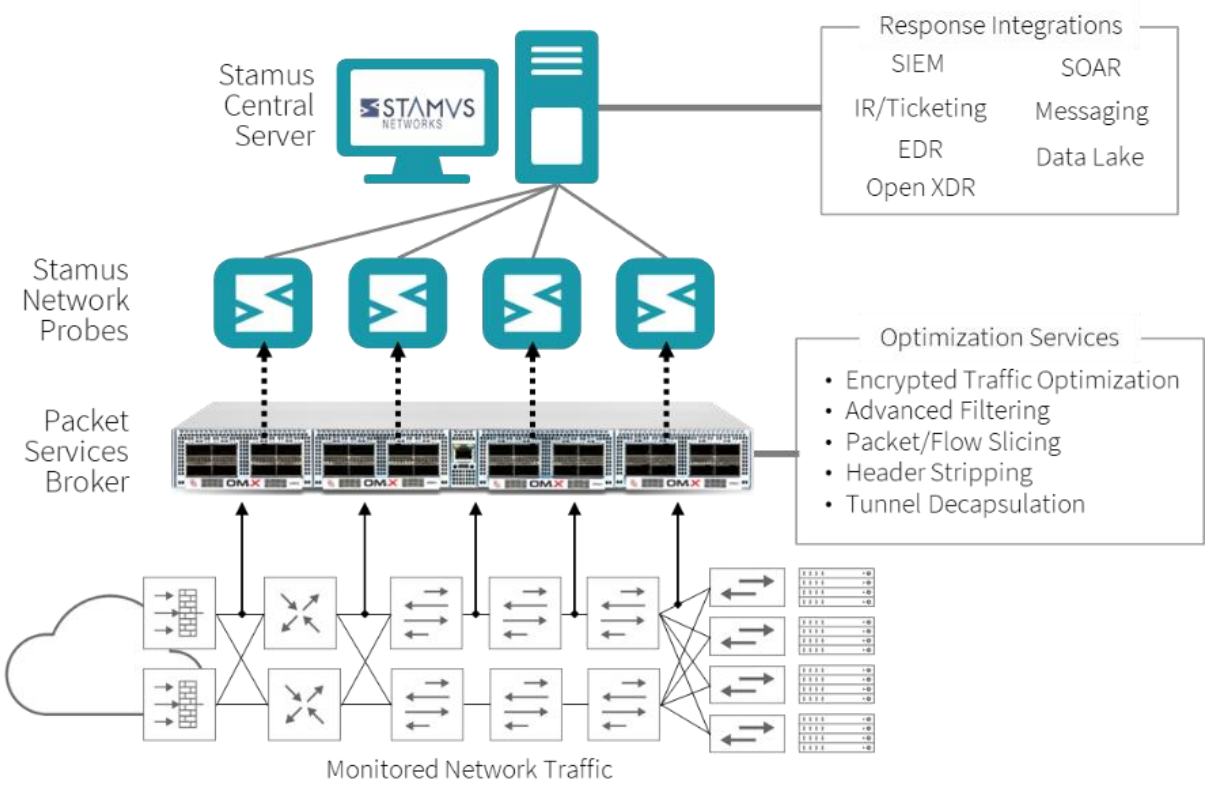

Figure 1: The joint Stamus Networks – NetQuest reference architecture shows a single monitored data center covering multiple network links including east-west traffic to collect and optimize network traffic feeding into Stamus Network Probes.

Joint Solution Brief

Simple to Integrate

The NetQuest Packet Services Broker quickly integrates with the Stamus Network Probe to add advanced packet optimization services for any monitoring environment. The Packet Services Broker is deployed in front of the Stamus Probe and collects packet traffic from key network TAP or SPAN points. All traffic is inspected and optimized at wire-speed and optimized packets are delivered to the Stamus Probe in real-time. The Packet Services Broker can also deliver the same collected packet traffic to other security and monitoring tools or packet collection and storage devices to leverage investments, reduce operational complexities and lower the TCO associated with operating multiple probes, sensors, and packet collection appliances.

Scaling the Monitoring Architecture

A single Packet Services Broker can support receiving traffic from many network links and can deliver the conditioned packets to many Stamus Network Probes. Optimized packet-flow traffic can be delivered to dedicated Stamus Probes or can be aggregated and delivered to multiple Stamus Probes to scale monitoring capacity for high volumes of traffic. When full-duplex link monitoring is required, both the TX and RX side of a monitored link can be combined for delivery to a single Stamus Probe input port.

To maintain the integrity of the source packet traffic the Packet Services Broker can tag the conditioned traffic to identify its traffic type or collection source. The interconnection link speed between the Packet Services Broker and the Stamus Probe is determined by the peak volume of traffic to be delivered to the Stamus Probe. The NetQuest Packet Services Broker features a modular architecture enabling port expansion as higher densities are required. Each interface module provides network-facing ports and Stamus Probe facing ports with a dedicated FPGA packet processing engine to assure 100% performance for every port at scale as port densities grow.

The Value Realized

The threat landscape is ever changing, so with today's hyperconnected world when defending against the increasing volume and complexity of cyberthreats rapid time to knowledge is essential. Together Stamus Networks and NetQuest deliver the highest scale network traffic collection and monitoring solution that empowers security operations teams to efficiently analyze high volumes of network traffic enabling unprecedented threat intelligence at scale. In addition, the joint solution reduces instrumentation costs removing barriers to the cost-efficient expansion of network coverage for critical observation points such as east-west network links to gain much needed visibility into lateral traffic movement to quickly spot emerging nefarious activity and support more comprehensive investigative activities.

About Stamus Networks

A global provider of high-performance network-based threat detection and response systems, Stamus Networks helps enterprise security teams accelerate their response to critical threats with solutions that uncover serious and imminent risk from network activity. Our advanced network detection and response (NDR) solutions expose threats to critical assets and empower rapid response.

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.

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