Solution Brief

Highlights

- Terabytes of scalable traffic optimization reduces unmonitorable traffic enabling improved threat intelligence at scale
- Target specific traffic types to deliver only high-value packets to Suricata Sensors
- Optimize visibility into encrypted and streaming services traffic without expensive decryption
- Combine multiple monitoring points into a single Suricata Sensor to scale capacity
- Enable cost-effective visibility into East-West traffic to analyze lateral movements
- Reduce packet capture volume to optimize storage requirements and increase packet retention times
- Reduce instrumentation costs, rack space requirements and extend security tool life
- Meet compliance requirements with intelligent packet and flow truncation

Optimizing Traffic Monitoring for Suricata to Increase Scale and Capacity

Suricata is a powerful open-source security tool that combines high-performance threat detection, intrusion detection, intrusion prevention, network security monitoring and packet capture capabilities. Since network traffic represents an essential vantage point to identify emerging threats and active intrusions, the Suricata Network Sensor is at the heart of a successful deployment.

However, the speed and velocity of network traffic has grown by many orders of magnitude and will continue to grow exponentially. This traffic growth presents many challenges for most security platforms. One challenge is that one hour of raw network traffic on a single 100G link can reach 45 terabytes. As a result, the Suricata Sensor is easily overwhelmed by the massive amount of traffic to monitor and analyze. Another challenge is that not all network traffic flows are created equal. Some traffic, such as encrypted traffic, cannot always be analyzed, while some other traffic types are less likely to contain indicators of malicious activity and is not useful to monitor. Analyzing this lower-priority traffic consumes valuable Suricata Sensor processing, analysis, and storage resources to assess irrelevant traffic.

Since Suricata Sensors are 'do-it-yourself' appliances, it is important to optimize capacity to ingest the network traffic for the links to be monitored. Impaired Sensor performance can lead to critical gaps in network visibility, which can result in attacks going undetected – enabling them to dwell longer and propagate deeper across the network.

Optimize Traffic to Scale Suricata Capacity

Evaluating every packet in real time against thousands of attack signatures for hundreds or thousands of concurrent flows requires significant processing power. To scale performance and get the most from a Suricata deployment, network and security operators should optimize network traffic to deliver only high-value traffic to the Suricata Sensor since not all network traffic needs to be processed and analyzed. Intelligent traffic optimization reduces unwanted packets from reaching the Sensor and storage layers, which can significantly increase the scale and capacity of the Suricata Sensor and other packet collection tools.

Consequently, traffic optimization enables achieving more pervasive network coverage while needing fewer physical Sensors and reducing instrumentation costs and complexity. It also extends the useable life of existing lower speed 10G and 40G Sensors and delays the need to upgrade Sensors to support the ever-growing network traffic footprint.

NetQuest Packet Services Broker

The NetQuest Packet Services Broker delivers multi-terabit, advanced packet processing services for high-performance security monitoring environments that rely on accurate network packets. The Packet Services Broker efficiently identifies, prioritizes, and optimizes packet traffic at wire-speed to deliver only relevant packets to reduce the upstream processing burden. This facilitates faster analysis and enables more efficient packet recording to reduce storage requirements and extend packet retention time.

The NetQuest Packet Services Broker brings significant value to Suricata deployments by intelligently assessing, conditioning, and optimizing network traffic to automate the delivery of only high-value packets to the Suricata Sensor. In addition to traditional 'smart' packet optimization services, the NetQuest Packet Services Broker advanced optimization services enable:

- Optimize Suricata analysis resources by targeting specific types of traffic to deliver eliminating the processing burden for low-value traffic
- Optimize specific flow-types, such as encrypted or streaming traffic, and drop undesirable packets with adaptive flow slicing
- Remove unwanted packet elements with packet slicing to improve traffic ingest efficiency and meet privacy and compliance requirements
- Header stripping and protocol de-encapsulation to deliver only the inner packets to the Sensor making packets easier to ingest and analyze

These intelligent optimizations enable the Suricata Sensor to more efficiently monitor massive volumes of network traffic enabling improved network visibility and threat intelligence at scale. A single Packet Services Broker can support multiple Suricata Sensors and 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.

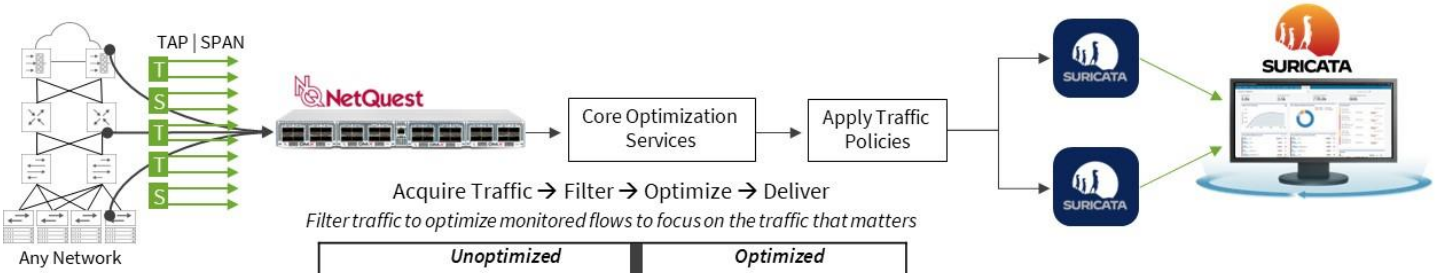
Result: Up to 80% Traffic Reduction

Depending on the monitored network traffic profile, intelligent packet optimization can reduce monitored network traffic volumes by 80% or more without compromising the integrity and value of the network traffic to be analyzed. Consequently, packet optimization allows the Suricata Sensor to focus on analyzing the traffic that matters and frees up valuable processing resources from analyzing irrelevant traffic, such as encrypted traffic packets that cannot be inspected, or unwanted streaming traffic. Traffic optimizations enable a lower speed Sensor to monitor higher speed links, or higher speed Sensors 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.

Ultra-Scale Filtering

The cornerstone of the NetQuest Packet Services Broker is its 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 the high-value traffic that is to be forwarded to the Suricata Sensor versus low-value traffic which can be discarded. User configurable rule-based priorities assure Suricata analysis resources are used efficiently without compromising traffic integrity. Filters can be applied to outer IP headers for tunneled flows, or on inner IP headers, or both as may be required for the specific monitoring environment and traffic profile. Users can change the filtering rules on-demand to adapt to changing traffic characteristics, threat activity and updated threat intelligence.

High-scale IP prefix lists enable sophisticated precision traffic prioritization for services, IP addresses, and IP CIDRs. This allows sending specific traffic classes or source IP addresses, such as traffic destined for critical services, or by targeting specific traffic originating from suspect locations identified by threat intelligence feeds. APIs enable the automation of real-time filtering rule adjustments between security platforms and threat intelligence feeds to change the parameters on-demand as new threat vectors or high-risk sources are identified.



	Unoptimized		Optimized	
	10G Sensor	40G Sensor	10G Sensor	40G Sensor
25G	5x	2x	2x	1x
40G	8x	2x	2x	1x
100G	20x	5x	4x	1x

- Assumes 80% traffic optimization
- TX/RX monitoring requires 2x capacity

Encrypted Traffic Optimization

Depending on the network environment, as much as 80% of network traffic is now encrypted. Eliminating low-value encrypted packets significantly reduces the packet processing burden on the Suricata Sensor to accelerate identifying emerging threats and enabling more efficient and sophisticated threat hunting.

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 Suricata Sensor. User-definable traffic policies allow the identification and automation of actions to drop or optimize this traffic for delivery to the Suricata Sensor including:

- Truncate encrypted traffic to only forward headers and handshake packets and discard the unusable encrypted payloads
- Drop low-value encrypted traffic based on IP Prefix list or service type
- Forward only encrypted traffic with specific algorithms, such as SSH, TLS and QUIC, and drop all other encrypted traffic
- Flow-based metadata can be provided for optimized or discarded traffic to maintain 100% flow accounting

Similar optimizations can be applied to streaming services traffic, such as voice or video. The Packet Services Broker detects streaming traffic and can forward only session set-up packets and drop the remaining streaming content payload packets, or simply drop all streaming services packets.

East-West Traffic Visibility

Increasingly cyberattacks are using lateral movement to travel across the network and infiltrate as many devices as possible. Consequently, early detection of abnormal lateral activities and reducing dwell times is critical as many high-profile attacks have evaded traditional security protections and moved laterally over multiple months.

The NetQuest Packet Services Broker enables expanding network traffic visibility to more places by enabling cost-effective access to, and optimization of, critical East-West network traffic and efficiently delivering only the relevant packets to the Suricata Sensor. This reveals lateral connectivity patterns and reconnaissance anomalies and the usage of ports, protocols, applications, file sharing, login failures and other suspicious activities no matter what phase of the attack.

Unsampled Flow Metadata Generation

The Packet Services Broker can simultaneously act as a high-scale Network Flow Sensor to deliver 1:1 unsampled IPFIX metadata from the same packet traffic. When activated, metadata is created at the same time the packet traffic is processed and can include standard layer 2/3/4 NetFlow metadata or can be enriched with layer 4-7 advanced application, protocol, and encrypted traffic details.

The Flow metadata is delivered as a separate IPFIX output stream and can be distributed, and load balanced to up to 32 different flow collectors to support multiple monitoring platforms and use cases. The optional metadata generation capabilities further extend the operational value of the NetQuest Packet Services Broker platform while reducing TCO and operational complexities associated with managing multiple probes and sensors.

Scaling Traffic Monitoring Coverage

A single Packet Services Broker can support receiving traffic from many TAP or SPAN observation points and can deliver and load balance the conditioned packets to one or many Suricata Sensors to scale monitoring capacity for high volumes of traffic. Optimized packet traffic from multiple slower-speed links can be aggregated, optimized, and delivered to a single Sensor, or traffic from higher speed 100G links can be optimized and delivered to multiple Sensors. Since the monitored traffic is optimized, fewer Sensors are required, thus reducing instrumentation costs and optimizing rack space utilization while enabling pervasive visibility.

Conclusion

Today's traffic complexity and growing volumes continually challenge security monitoring. To keep up with the massive volumes of network traffic to extract critical intelligence, the security and network operations teams must intelligently identify and deliver only relevant and monitorable traffic to the Suricata Sensor to optimize traffic monitoring capacity, streamline analysis, and extend historical forensics capacity. The NetQuest Packet Services Broker helps organizations overcome the challenges of collecting and ingesting high volumes of network traffic to enable the highest scale network traffic collection and monitoring that empowers security operations teams to achieve unprecedented threat intelligence at scale. In addition, optimizing traffic reduces instrumentation costs and removes barriers to the cost-efficient expansion of network coverage for critical observation points, such as East-West network links, to quickly spot emerging nefarious activity and support comprehensive investigative missions.

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