NEOX NETWORKS
NEXT GENERATION NETWORK VISIBILITY

Feature Brief

Simplify Network Monitoring With Granular Filtering

In today's dynamic network environments, visibility alone is not enough—precision is key. As networks expand in scale and complexity, the ability to filter and analyze only the most relevant traffic becomes critical for performance optimization, security monitoring, and efficient resource utilization. At NEOX, we understand that Granular Filtering is not just about reducing noise and unwanted traffic—it's about delivering focused, actionable intelligence to your monitoring and security tools, so you are spot on.

What is Granular Filtering

Granular or Advanced Filtering refers to the selective processing and forwarding of network traffic based on granular criteria, ensuring that only the most relevant data reaches monitoring, analytics, and security tools. Unlike basic filtering, which may rely on simple rules (e.g., IP or port-based), Granular Filtering leverages deep packet inspection (DPI), metadata enrichment, and dynamic rule sets to classify and filter traffic with surgical precision.

Why Granular Filtering Matters

NEOX's Granular Filtering capabilities transform raw network traffic into high-value intelligence, ensuring that tools operate efficiently and security teams focus on genuine threats. Here's why it's indispensable:

1. **Reduced Tool Overload & Improved Efficiency**
   Monitoring tools often drown in irrelevant traffic, reducing effectiveness. NEOX's Granular Filtering solves this by delivering only high-priority traffic to security systems, cutting latency and storage costs while improving threat detection. By intelligently discarding redundant or low-risk data, NEOX ensures your security stack operates at peak performance—maximizing ROI on existing tools and reducing alert fatigue.

2. **Enhanced Security Detection**
   Advanced traffic filtering improves threat detection by eliminating benign network noise and prioritizing analysis of suspicious encrypted communications, enabling security teams to concentrate on high-risk activities such as lateral movement and command-and-control traffic. By focusing resources on truly malicious behavior, NEOX increases detection accuracy while reducing false positives—helping security teams detect real threats faster and with greater confidence.

3. **Optimized Bandwidth & Resource Utilization**
   Boost network efficiency by eliminating redundant traffic like backup streams while prioritizing mission-critical flows such as VoIP and transactions. This intelligent filtering optimizes bandwidth usage and ensures monitoring resources focus on high-value data. The result is a leaner, more responsive network infrastructure where critical applications never compete with non-essential traffic for bandwidth or analysis resources.

4. **Compliance & Data Privacy Alignment**
   Strengthen compliance and reduce risk by automatically filtering out sensitive data (PHI, financial records, PII) before traffic reaches monitoring tools—ensuring adherence to GDPR, HIPAA, and other regulations. NEOX's granular filtering also restricts monitoring to authorized traffic only, minimizing legal exposure while maintaining essential visibility for security teams

5. **Proactive Threat Intelligence & Incident Response**
   NEOX's Granular Filtering doesn't just reduce noise—it actively enhances threat intelligence by surfacing high-risk traffic

patterns and anomalies. By prioritizing critical indicators of compromise (IoCs) and attack signatures, security teams gain faster, more accurate insights for proactive threat hunting and rapid incident response. This ensures organizations stay ahead of adversaries, minimizing dwell time and mitigating potential breaches before they escalate.

How NEOX Delivers Granular Filtering

NEOX PacketWolf, PacketLion, and PacketTiger series of Packet Brokers & Processors integrate hardware-accelerated filtering to maximize precision without compromising performance.

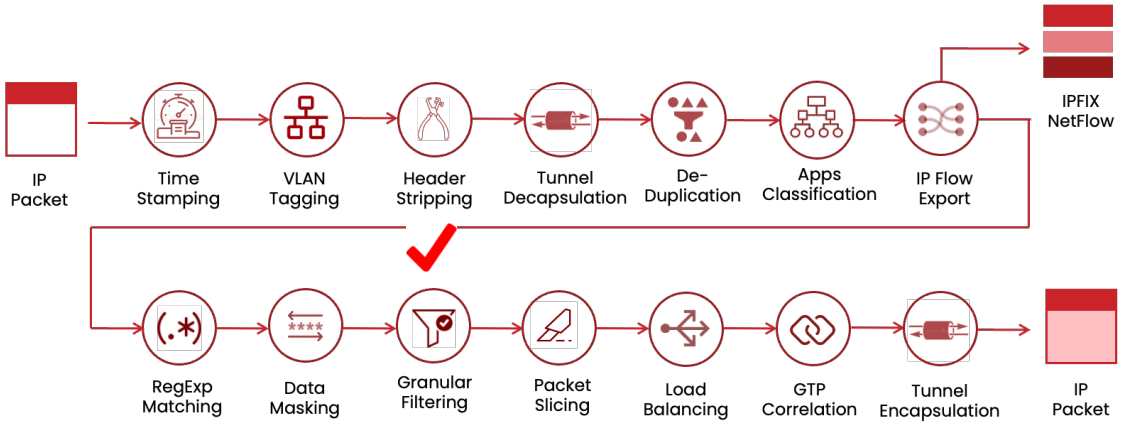
1. **Dynamic Rule-Based Filtering**
   NEOX enables precision traffic control through real-time rule enforcement—leveraging ACLs, regex patterns, and flow attributes to instantly isolate critical network traffic. Our stateful filtering goes beyond simple packet inspection, maintaining complete session awareness to enforce intelligent, context-driven policies that adapt dynamically to your network environment.

2. **Deep Packet Inspection (DPI)**
   NEOX's Deep Packet Inspection (DPI) goes beyond basic filtering, identifying applications, malware signatures, and encrypted traffic anomalies by analyzing Layer 7 metadata (HTTP headers, DNS queries, API calls). Combined with behavioral and anomaly-driven filtering, our machine learning-powered baselining detects and isolates suspicious patterns—like port scanning or data exfiltration—before they reach security tools, ensuring proactive threat prevention without overwhelming your monitoring infrastructure.

3. **Tool-Specific Optimization**
   NEOX enables intelligent traffic distribution by customizing filters for each monitoring tool—sending only NetFlow data to analytics platforms while routing malware traffic exclusively to NDR solutions. Our technology automatically load-balances processed traffic across multiple tools, ensuring scalable analysis without overwhelming any single system. This precision filtering maximizes tool efficiency while maintaining complete visibility across your security stack.

4. **Hardware-Accelerated Performance & Scalability**
   NEOX's PacketWolf, PacketLion, and PacketTiger series leverage custom FPGA/ASIC-powered processing to deliver line-rate filtering at scale—ensuring zero packet drops even under heavy traffic loads. By offloading filtering, deduplication, and packet slicing to hardware, NEOX eliminates bottlenecks and maintains sub-microsecond latency, critical for high-speed networks (100G+/400G+). This architecture future-proofs deployments, allowing seamless scaling from enterprise to service provider environments without sacrificing precision or performance.

5. **Cloud & Hybrid Network Support**
   NEOX delivers seamless cloud and hybrid network support, extending Granular Filtering policies to cloud workloads (AWS/Azure/GCP) through PacketTigerVirtual. Maintain uniform security monitoring across multi-cloud and hybrid environments while reducing cloud egress costs—ensuring enterprise-grade visibility without infrastructure limitations.



Feature	PacketWolf	PacketLion	PacketTiger	PacketTigerVirtual
Granular Filtering	✓	✓	✓	✓

Best Practices for Granular Filtering with NEOX

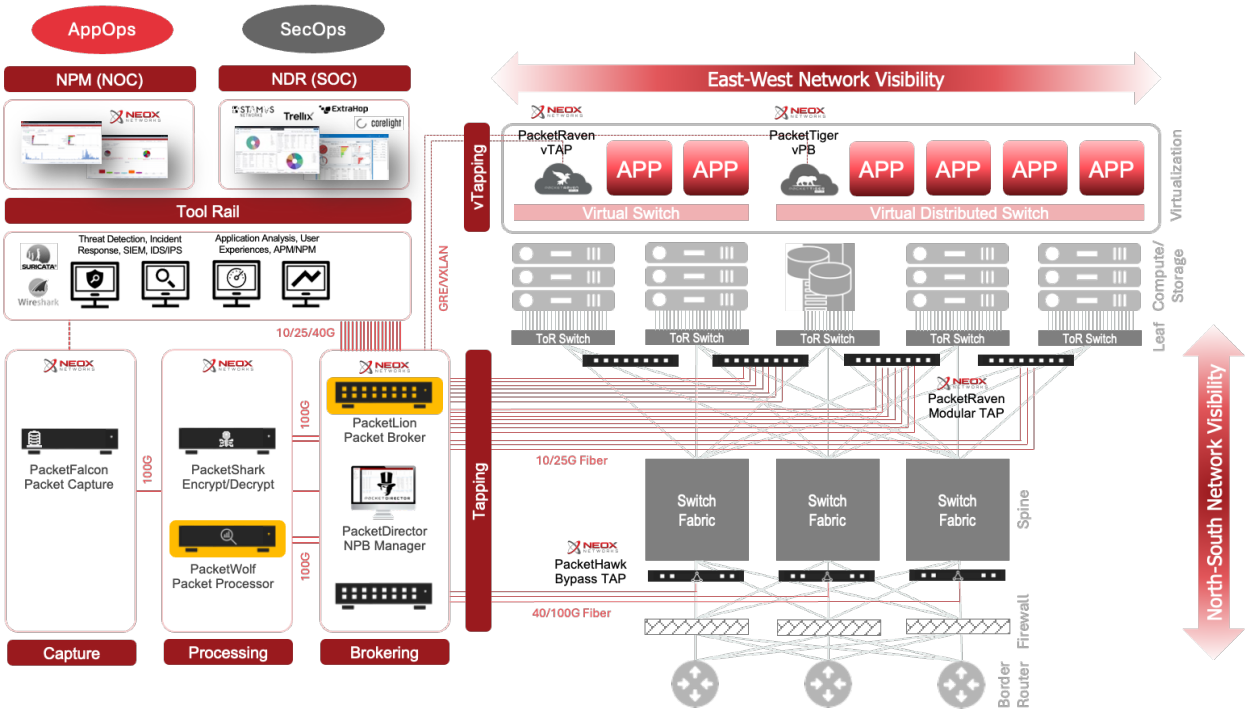
To maximize the value of your network observability and security stack, we recommend:

- ✓ Deploy NEOX Packet Brokers inline or via TAP/SPAN to filter traffic before it reaches monitoring tools.
- ✓ Use a two-tier architecture (PacketLion for aggregation + PacketWolf for filtering) in high-speed networks.
- ✓ Continuously update filtering rules based on threat intelligence and application changes.
- ✓ Combine with Advance Filtering for a dual-layer visibility approach (metadata + filtered packets).

To help you get the most out of your network, we recommend the following best practices to funnel, consolidate, and process all network traffic to be monitored through one of the two NEOX Packet Broker approaches:

- For better hardware performance, lower latency network, or for a future-proofed scalable visibility approach, deploy a **two-tier visibility architecture**. Use NEOX PacketLion Packet Broker for high-density TAP and tool aggregation, and use NEOX PacketWolf Packet Broker for faster Data Masking and other packet services operations.

- For a lighter or software-driven approach, consolidate all network traffic to be monitored through a NEOX PacketTiger, and then from there to the tool rail. Same can be achieved in the cloud with PacketTigerVirtual before forwarding traffic to cloud-native monitoring or security tools.



The Future of Network Traffic Brokering Starts Here

As networks grow in complexity and speed, the importance of Granular Filtering will only continue to rise. At NEOX we're committed to helping you stay ahead of the curve with innovative solutions that deliver precision, reliability, and performance

Ready to Transform Your Network?

Discover how NEOX can elevate your Network Traffic Brokering with advanced Granular Filtering technology. Contact Us today or Request a Demo to learn more about our solutions and take the first step toward a smarter, faster, and more secure network.
NEOX – Precision. Performance. Perfected.

About NEOX Networks

NEOX Networks provides Next Generation Network Visibility for IT & OT Observability and Security. The result is strengthened cybersecurity, hybrid-cloud application observability, and business continuity, by integrating the network intelligence and real-time data-in-motion. Learn more at neoxnetworks.com