NEOX NETWORKS

NEXT GENERATION NETWORK VISIBILITY

# NEOXPacketWolf 100G-400G Advanced Packet Processor

## Hardware accelerated through FPGA architecture | Performance up to 400Gbps

PACKETWOLF

SecurITy made in Germany

Trust Seal www.teletrust.de/itsmig

The NEOXPacketWolf is the ideal platform for advanced packet processing of network data up to 400Gbps per appliance thanks to its FPGA-based architecture.

Our PacketWolf solutions belong to the family of Advanced Packet Processing Appliances and can be deployed as a complement to a Network Packet Broker (NPB) - or stand-alone in an existing network monitoring infrastructure.

The data traffic for processing usually comes from a Network Packet Broker, but can also originate from other sources, such as a SPAN port or Network TAP, and after processing is forwarded by PacketWolf on the same or a separate port to a monitoring/security tool or sent back to the original data source.

### PRODUCT HIGHLIGHTS

- Small form factor (1U, only 40cm deep)
- Supports lossless processing of network data up to 400Gbps
- Reliable and low latency due to FPGA architecture
- Up to 4x 100G QSFP28 interfaces or 4x 40G QSFP+ / 8x 25G (fan-out) / 16x10G (fan-out)
- Supports individual configurations for 10G, 25G, 40G, 50G or 100G
- Supports nanosecond timestamping according to IEEE 1588v2 PTP
- Scalable and easy to commission
- Replaceable fans and redundant power supplies

The use of an Advanced Packet Processing Appliance offers several advantages worth mentioning.
On the one hand, it is possible to granularly reduce the data load for the monitoring system through the advanced packet processing functions. For example, duplicate packets can be removed from SPAN sessions by means of deduplication (see whitepaper „TAPs vs SPAN Port"), or unwanted packets can be removed by means of various packet filtering options.
On the other hand, functions such as Packet Slicing and Packet Masking can ensure compliance with legal and compliance requirements. Particularly in connection with the GDPR, it may be necessary to use Packet Slicing to remove the user data, as the metadata is often sufficient for an analysis.

- 4x 100G QSFP28 — Up to 4x 100G QSFP28
- Very low latency
- FPGA design very high configurability
- FPGA based Nanosecond Timestamping
- FPGA based Deduplication
- FPGA based Packet Slicing
- Protocol Header Stripping
- D — Developed & QA in Germany

Using packet masking, it would also be possible to overwrite or „black out" personal information such as voice data, GEO data, IMSI or IMEI information in the user data and thus hide sensitive and/or personal information from the eyes of third parties.

The processing of the network packets takes place on the high-performance FPGA in hardware and is carried out loss-free up to 400Gbps by the PacketWolf.

# // NEOX**PacketWolf**

## KEY FEATURES

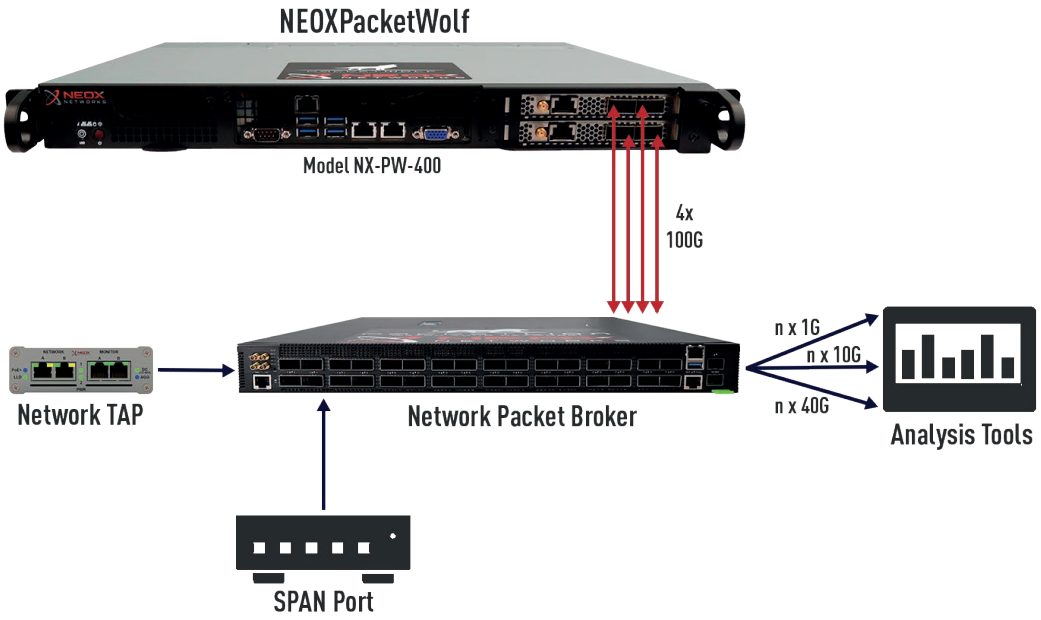
- **Line-rate FPGA features/functionalities:**
  - Advanced filtering
    - Frame length, header length or payload length
    - Frame errors
    - L2 Protocol/Encapsulation
    - L3 IPversion/Protocol/Encapsulation
    - L4 Protocol (Ports)/Tunnel
    - Pattern compare
    - Complex expressions via logical operators (NOT,AND,OR)
    - Advanced Deduplication (customizable packet signatures to meet the unique requirements of each network.)
    - Masking (for sensitive information in the packets)
    - Slicing (to remove the sensitive or heavy payloads from the packets)
    - Decapsulation MPLS, VLAN, VNTAG, PPTP, ERSPAN, VxLAN, GRE, GENEVE, NVGRE, CFP, EoMPLS, IP-in-IP, MAC-in-MAC and custom/user defined encapsulations
  - De-tunneling (Tunnel Termination) for traffic generated by vTAPs, ERSPAN,VxLAN
  - GTP filtering
  - Timestamping (where the time is being synchronized externally by PTP IEEE-1588 v2 or PPS)
  - High precision PCAP Replay at original rate and at any desired rates
  - Source port labeling and VLAN tagging
  - Load-balancing on multiple VLAN tags
- **FPGA accelerated features/functionalities:**
  - Loopback (shuffling the L2,L3,L4 sources and destinations)
  - Entire payload masking
- **Host features/functionalities:**
  - Highly secure UI
  - GUI (coming very soon)
  - PCAP viewer
  - PCAP composer/editor
- **Optional features/functionalities:**
  - IPv4/IPv6 subnets/addresses list filtering (based on TCAM/CAM technology for ultra-low latency filtering)
  - Custom/user defined field list filtering (based on TCAM/CAM technology for ultra-low latency filtering)
  - GTP Correlation
  - IPFIX, NetFlow generation
  - Intelligent dynamic packet slicing
  - Full packet capture
  - Anonymizing MAC, IP addresses, source/destination or custom/User defined fields

| VALUE ADDED FUNCTIONS | |
|---|---|
| **Advanced Packet Processing** | Optimisation of tool efficiency through Header Stripping, Deduplication, Packet Slicing (trimming) without packet loss. |
| **Line Rate Filtering** | e.g. protocol-based, IP match list-based and/or by means of logical links. |
| **Layer 2 based Filtering** | Packet lengths, packet errors, frame types (PPPoE Discovery/Session, LLC, SNAP), EtherType, Encapsulation (CFP Cisco Fabric Path, ISL, VLAN (3 Levels), MPLS (7 Levels), VN-Tag), VLAN Tag Value, TPID , MPLS label, MAC addresses, Broadcasts. |
| **Layer 3 based Filtering** | IPv4 or IPV6 version, source/destination addresses (up to 36,000 IPv4 addresses or 8000 IPv6 for exact match and 864 IPv4 or 216 IPv6 subnet match), (ICMP packets), DSCP,ECN/Traffic Class, Protocol/Next Header, TTL/Hop Limit, Flow Label, Fragments (First, Mid, Last), IPv4 header checksum error. |
| **Layer 4 based Filtering** | TCP, UDP, SCTP or other, source/destination ports, TCP flags, TCP/UDP checksum errors. |
| **Fragment Filtering** | Filtering of IP4 and IP6 fragments. |
| **Data Pattern Matching** | Dynamic offset data pattern matching. Based on the start or end of L2, L3, L4 headers or payloads. |
| **Timestamping** | A timestamp with nanosecond accuracy is applied to each processed packet using a PTP time server. Locally or via external PTP grandmaster according to IEEE 1588v2. |
| **Deduplication** | Removal of duplicate packets with a programmable deduplication window of 10 milliseconds to 2 seconds. Configurable packet signatures (masking of variable fields e.g. TTL/Hoplimit, DSCP/TraffType, exclusion of Outer Encapsulations, and others). |
| **Dynamic Packet Slicing/Trimming** | Payload removal so that the Ethernet packet contains only the desired number of bytes or information, including a programmable number of bytes offset. Including FCS recalculation. Metadata is preserved. Enables, among other things, to ensure GDPR compliance. |
| **Protocol Header Stripping** | Remove protocol headers (e.g. VxLAN, MPLS, FabricPath, VNTag, GTP, GRE, ERSPAN, GENEVE, LISP, PPPoE, etc) and extract IP packet payloads for the benefit of analysis tools that cannot process them via decapsulation and de-tunnelling. |
| **Source Port Labeling** | VLAN tagging and untagging or VLAN tag management with ingress tagging and egress stripping. |
| **Aggregation** | Consolidation of incoming network traffic to optimise port usage. 1:1, 1:Many, Many:1, Many:Many |
| **Traffic Tunneling** | Supports L2, L3, L4 filters (see above). Tunnel types: GRE_v0, GRE_v1, EtherIP, GTPv0U, GTPv1v2-C, GTPv1-U_signaling, GTPv1-U_GPDU, IPinIP; VXLAN, GENEVE and others. |
| **Native Tunnel Termination** | L2GRE and VxLAN tunnel termination, including header stripping. |
| **Load Balancing** | Intelligent distribution (uni- and bi-directional flows) of traffic to the ports being monitored to preserve traffic integrity and maximise uptime through failover protection. Wide range of hashing algorithms (e.g. 5 tuple, 2 tuple, VLAN, MPLS, etc). |
| **Asymetric Hashing** | Asymmetric and individual hashing supports common use cases, e.g. lawful interception |

| FURTHER FUNCTIONS (optionally available on request) | |
|---|---|
| **Netflow Export** | Generate metadata and flow records in standard NetFlow formats such as NetFlow v5, v9 and IPFIX. |
| **IP List Filtering** | Enables to control what kind of IP traffic will be allowed into and out of the network. |

# // NEOX**PacketWolf**

## EXAMPLE SCENARIO




## TECHNICAL SPECIFICATIONS & ITEM NUMBERS

| HARDWARE |
|---|
| 1x Intel XEON Scalable |
| 2x 10G LAN management port |
| Redundant and hot-swappable AC power supplies |
| 64GB DDR4 RAM |
| NVMe SSD storage for the operating system |

| DIMENSIONS (HxWxD) | WEIGHT |
|---|---|
| 43 mm x 437 mm x 399 mm | ca. 16 kg |
| 1.7" x 17.2" x 15.7" | ca. 29 lb |

| OPERATING TEMPERATURE |
|---|
| 10° to 35° C (50° to 95° F) at sea level |

| POWER SUPPLY |
|---|
| 2 power supply units with 500W each |
| Input: 100 to 120 VAC - or - 200 to 240 VAC |
| Output: 500W each at 100 VAC or 240 VAC |

| RELATIVE HUMIDITY | |
|---|---|
| Operation | 8% to 90% relative humidity (Rh), 28°C (82.4°F) maximum temperature, non-condensing |
| Storage | 5% to 95% relative humidity (Rh), 38.7°C (101.7°F) maximum temperature, non-condensing |

## MODELS

| ITEM NO. | DESCRIPTION |
|---|---|
| NX-PW-100 | 4x 25G SFP28 interfaces with 100G data throughput, or 4x 1G SFP / 4x 10G SFP+ |
| NX-PW-200 | 2x 100G QSFP28 interfaces with 200G data throughput, or 2x 40G QSFP+ / 4x 25G (fan-out) / 8x10G (fan-out) |
| NX-PW-400 | 4x 100G QSFP28 interfaces with 400G data throughput, or 4x 40G QSFP+ / 8x 25G (fan-out) / 16x10G (fan-out) |



NEOX NETWORKS GmbH
Monzastr. 4 · 63225 Langen · Germany
+49 6103 / 37 215 910 · solutions@neox-networks.com · www.neox-networks.com