NEOXPacketWolf 100G-400G Advanced Packet Processor

Hardwarebeschleunigt durch FPGA-Architektur | Performance bis zu 400Gbps

PACKETWOLF

Secur ITy made in Germany

Der NEOXPacketWolf ist dank seiner FPGA-basierten Architektur die ideale Plattform für die fortschrittliche Paketbearbeitung von Netzwerkdaten bis 400Gbps pro Appliance.

Unsere PacketWolf Lösungen gehören zur Familie der Advanced Packet Processing Appliances und können als Ergänzung zu einem Network Packet Broker (NPB) - oder auch Stand-Alone in einer bereits vorhandenen Netzwerkmonitoring-Infrastruktur eingesetzt werden.

Der Datenverkehr zur Verarbeitung kommt üblicherweise von einem Network Packet Broker, kann aber auch von anderen Quellen stammen, wie bspw. einem SPAN-Port oder Netzwerk TAP und wird nach Bearbeitung vom PacketWolf auf demselben oder aber auch gerne einem separaten Port zu einem Monitoring/Security-Tool weitergeleitet bzw. zur ursprünglichen Datenquelle zurückgeschickt.

Der Einsatz einer Advanced Packet Processing Appliance bietet mehrere nennenswerte Vorteile. Zum einen ist es möglich, durch die erweiterten Funktionen zur Paketverarbeitung die Datenlast für das Monitoring-System granular zu reduzieren. So können mittels Deduplication doppelte Pakete aus z.B. SPAN-Sessions (s. Whitepaper „TAPs vs SPAN-Port"), oder mittels vielfältiger Packet Filtering Optionen anderweitig unerwünschte Pakete entfernt werden.

PRODUKT HIGHLIGHTS

- Kleiner Formfaktor (1HE, nur 40cm tief)
- Unterstützt die verlustfreie Verarbeitung von Netzwerkdaten bis 400Gbps
- Zuverlässig und geringe Latenz durch FPGA-Architektur
- Bis zu 4x 100G QSFP28 Interfaces oder 4x 40G QSFP+ / 8x 25G (Fan-out) / 16x10G (Fan-out)
- Unterstützt individuelle Konfigurationen für 10G, 25G, 40G, 50G oder 100G
- Unterstützt nanosekundengenaues Timestamping nach IEEE 1588v2 PTP
- Skalierbar und einfache Inbetriebnahme
- Austauschbare Lüfter und redundante Stromversorgungen

Zum anderen können Funktionen wie z.B. Packet Slicing und Packet Masking die Einhaltung rechtlicher bzw. Compliance Anforderungen sicherstellen. Insbesondere im Zusammenhang mit der DSGVO kann es erforderlich sein, mittels Packet Slicing die Nutzdaten zu entfernen, da oftmals für eine Analyse die Metadaten zur Auswertung ausreichen.

Mittels Packet Masking wäre es zudem möglich persönliche Informationen wie Sprachdaten, GEO-Daten, IMSI oder IMEI Informationen in den Nutzdaten zu überschreiben bzw. zu „schwärzen" und somit sensible und/oder personenbezogene Informationen vor den Augen Dritter zu verbergen.

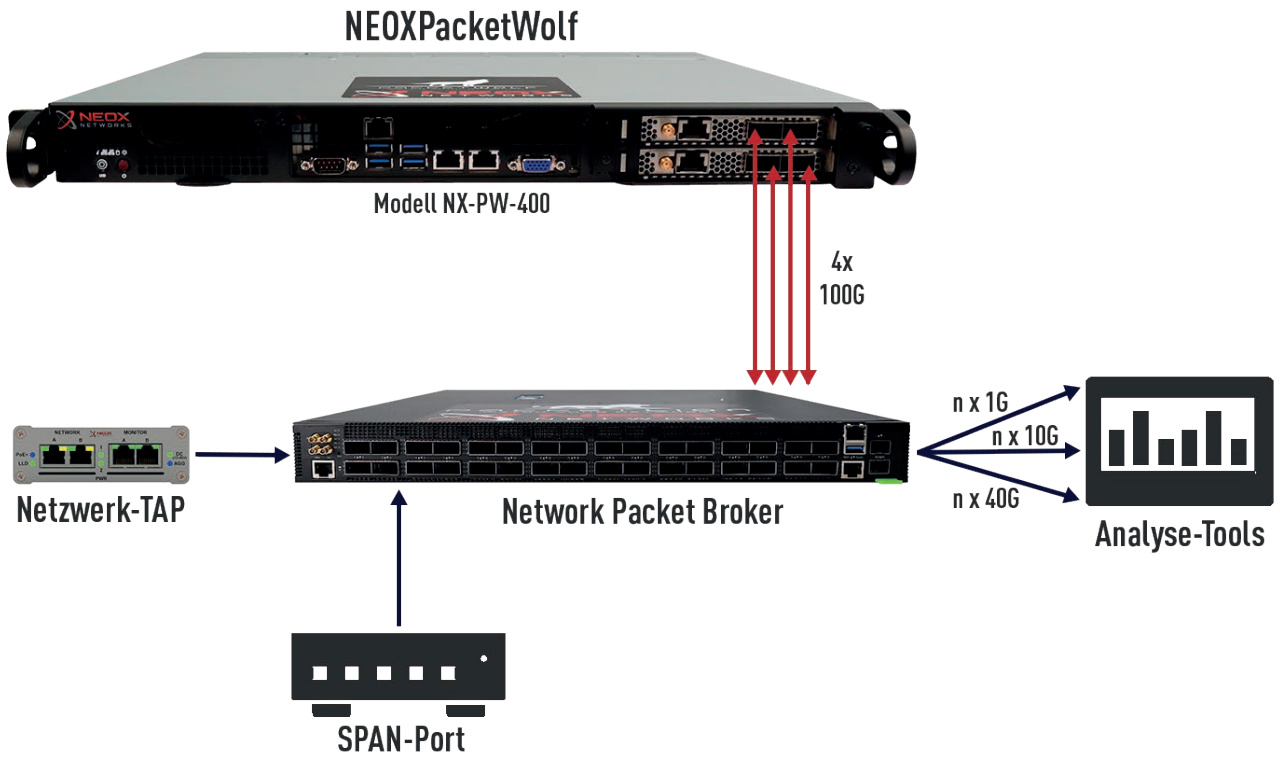
Die Verarbeitung der Netzwerkpakete erfolgt in dem hoch-performanten FPGA in Hardware und wird verlustfrei bis 400Gbps durch den PacketWolf durchgeführt.

VALUE ADDED FUNKTIONEN	
Advanced Packet Processing	Optimierung der Tool-Effizienz durch Header Stripping, Deduplication,Packet Slicing (Trimming) ohne Paketverluste.
Line Rate Filtering	z.B. Protokoll-basiert, IP-Match-List-basiert und/oder mittels logischer Verknüpfungen.
Layer 2 based Filtering	Paketlängen, Paketfehler, Frame-Typen (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-Adressen, Broadcasts.
Layer 3 based Filtering	Version IPv4 oder IPV6, Source/Destination-Adressen (bis zu 36.000 IPv4 Adressen oder 8000 IPv6 für Exact-Match und 864 IPv4 oder 216 IPv6 Subnet-Match), (ICMP packets), DSCP,ECN/Traffic Class, Protocol/Next Header, TTL/Hop Limit, Flow Label, Fragmente (First, Mid, Last), IPv4 Header Checksummen-Fehler.
Layer 4 based Filtering	TCP, UDP, SCTP oder Andere, Source/Destination-Ports, TCP FLags, TCP/UDP Checksummen-Fehler.
Fragment Filtering	Filterung von IP4 und IP6-Fragmenten.
Data Pattern Matching	Dynamischer Offset-Daten-Musterabgleich. Basierend auf dem Beginn oder dem Ende von L2, L3, L4 Headern oder Payloads.
Timestamping	Auf jedes verarbeitete Paket wird mithilfe eines PTP-Zeitservers ein Zeitstempel mit einer Genauigkeit von einer Nanosekunde aufgebracht. Lokal oder via externem PTP-Grandmaster nach IEEE 1588v2.
Deduplication	Entfernung von doppelten Paketen mit einem programmierbaren Deduplizierungsfenster von 10 µs bis 2 Sekunden. Konfigurierbare Paketsignaturen (Maskierung variabler Felder z.B. TTL/Hoplimit, DSCP/TraffType, Ausschluss von Outer Encapsulations, und weitere).
Dynamic Packet Slicing/Trimming	Entfernen der Nutzdaten (Payload), so dass das Ethernet-Paket nur die gewünschte Anzahl von Bytes oder Informationen enthält, einschließlich einer programmierbaren Anzahl von Bytes Offset. Inklusive FCS-Recalculation. Metadaten bleiben erhalten. Ermöglicht u.a. DSGVO-Konformität sicherzustellen.
Protocol Header Stripping	Protokoll-Header (z. B. VxLAN, MPLS, FabricPath, VNTag, GTP, GRE, ERSPAN, GENEVE, LISP, PPPoE, etc) entfernen und IP-Paket-Nutzdaten zugunsten von Analysetools extrahieren, die diese nicht verarbeiten können, mittels Decapsulation und De-Tunneling.
Source Port Labeling	VLAN-Tagging und Untagging bzw. VLAN Tag Management mit Ingress-Tagging und Egress-Stripping.
Aggregation	Konsolidierung des eingehenden Netzwerkverkehrs zur Optimierung der Port-Nutzung. 1:1, 1:Many, Many:1, Many:Many
Traffic Tunneling	Unterstützt L2, L3, L4 Filter (s.o.). Tunneltypen: GRE_v0, GRE_v1, EtherIP, GTPv0U, GTPv1v2-C, GTPv1-U_signaling, GTPv1-U_GPDU, IPinIP; VXLAN, GENEVE und andere
Native Tunnel Termination	L2GRE und VxLAN-Tunnel-Terminierung, inklusive Header Stripping.
Load Balancing	Intelligente Verteilung (Uni und Bi-Directional Flows) des Datenverkehrs auf die zu überwachenden Ports, um die Integrität des Datenverkehrs zu bewahren und die Betriebszeit durch Failover-Schutz zu maximieren. Große Auswahl an Hashing-Algorithmen (z.B. 5 Tuple, 2 Tuple, VLAN, MPLS, etc)
Asymetric Hashing	Asymmetrisches und individuelles Hashing unterstützt gängige Anwendungsfälle bspw. Lawful Interception

WEITERE FUNKTIONEN (Optional auf Anfrage erhältlich)	
Netflow Export	Generierung von Metadaten und Flow Records in Standard-Netflow-Formate wie NetFlow v5, v9 und IPFIX
Packet Masking	Überschreiben persönlich identifizierbarer Informationen (PII) wie Sprachdaten, GEO-Daten, IMSI, IMEI, etc. und dergleichen
GTP Filtering	Filterung innerhalb des GTP Protokolls (GTP-C, GTP-U, etc.)

// NEOX**PacketWolf**

BEISPIELSZENARIO



TECHNISCHE SPEZIFIKATIONEN & ARTIKELNUMMERN

HARDWARE
1x Intel XEON Scalable
2x 10G LAN Management-Port
Redundante und austauschbare AC-Stromversorgungen
64GB DDR4 RAM
NVMe SSD-Speicher für das Betriebssystem

STROMVERSORGUNG
2 Stromversorgungsnetzteile mit je 500W
Input: 100 bis 120 VAC - oder - 200 bis 240 VAC
Output: je 500W bei 100 VAC oder 240 VAC

BETRIEBSTEMPERATUR
10° bis 35° C (50° bis 95° F) auf Meereshöhe

RELATIVE LUFTFEUCHTIGKEIT	
In Betrieb	8% bis 90% relative Luftfeuchtigkeit (Rh), 28°C (82,4°F) maximale Temperatur, nicht kondensierend
Lagerung	5% bis 95% relative Luftfeuchtigkeit (Rh), 38,7°C (101,7°F) maximale Temperatur, nicht kondensierend

ARTIKELNUMMER	BESCHREIBUNG
NX-PW-100	4x 25G SFP28 Interfaces mit 100G Datendurchsatz, bzw. 4x 1G SFP / 4x 10G SFP+
NX-PW-200	2x 100G QSFP28 Interfaces mit 200G Datendurchsatz, bzw. 2x 40G QSFP+ / 4x 25G (Fan-out) / 8x10G (Fan-out)
NX-PW-400	4x 100G QSFP28 Interfaces mit 400G Datendurchsatz bzw. 4x 40G QSFP+ / 8x 25G (Fan-out) / 16x10G (Fan-out)

ABMESSUNGEN (HxBxT)	GEWICHT
43 mm x 437 mm x 399 mm	ca. 16 kg
1.7" x 17.2" x 15.7"	ca. 29 lb

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