

www.neox-networks.com

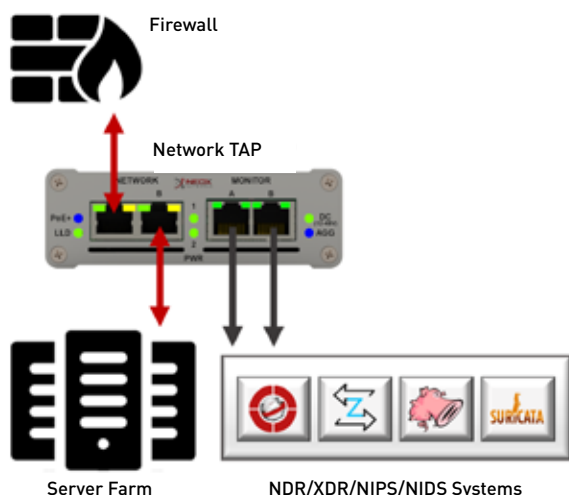
PRODUCT BROCHURE

SOLUTION PROVIDER
FOR NETWORK MONITORING AND SECURITY SOLUTIONS

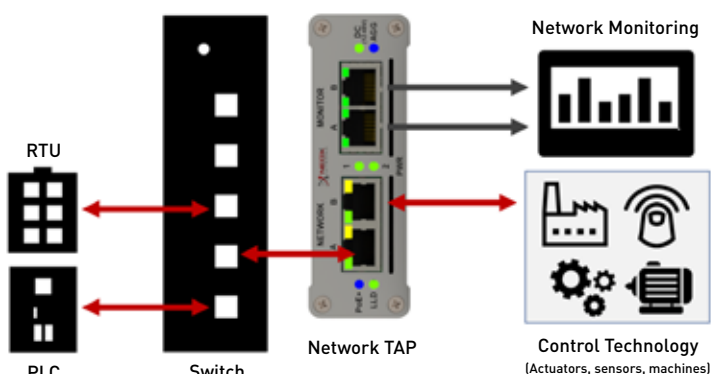
Network TAPs Deployment Scenarios

SINCE THE USE OF A SPAN/MIRROR PORT CAN FALSIFY RESULTS, THE USE OF A NETWORK TAP IS INDISPENSABLE IN A WIDE VARIETY OF AREAS

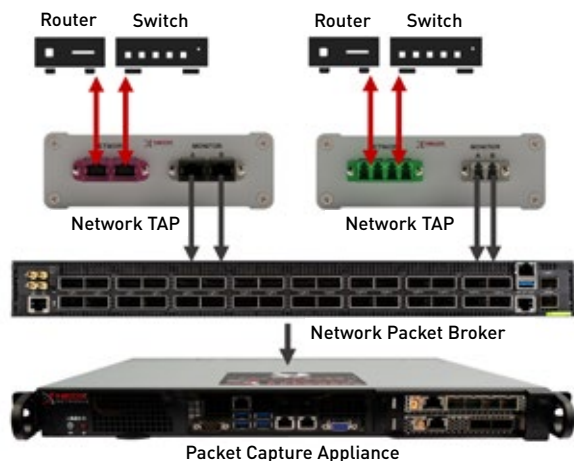
For the implementation of a security system:



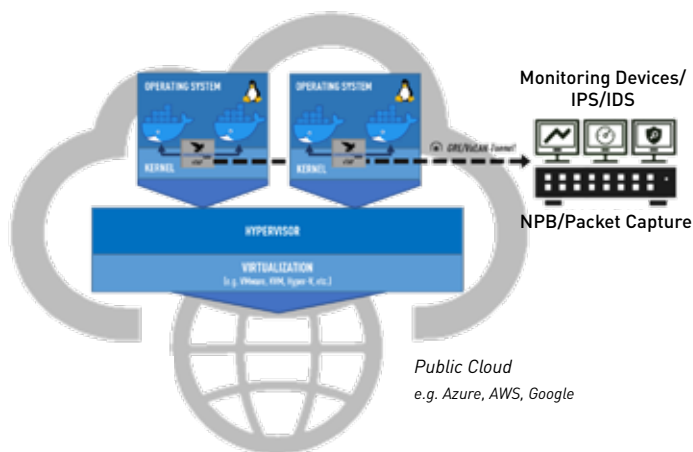
For the implementation of a monitoring system:



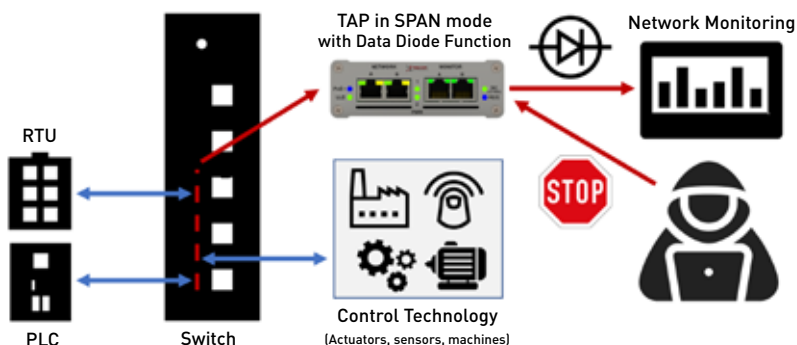
For the implementation of a network forensics solution:



Implementation of a Virtual NEOX TAP:



For implementing a Data Diode Function in combination with a Mirror Port:



NEOXPacketRaven Portable Network TAPs

FULL NETWORK VISIBILITY FROM 10M TO 400G | FPGA CHIPSET
DATA DIODE FUNCTION | REDUNDANT POWER SUPPLY



Network TAPs are decoupling elements for the secure and reliable tapping of network data in optical and copper-based networks. These TAPs are looped into the network line to be monitored and forward the entire data traffic without interruption and without packet loss.

Our Network TAPs do not have a MAC or IP address, but work entirely on OSI Layer 1 and cannot be traced in the network without special and expensive measuring equipment. Hackers and attackers therefore have no chance. As the integrity of the outgoing data remains unaltered due to this tapping method, our Network TAPs are increasingly used in the areas of network forensics, security and monitoring.

All our TAPs with an active monitoring port (RJ45/copper, SFP or M12) work like a Data Diode. This means that the monitoring ports are physically isolated from the network ports and access to the network via the monitoring ports is prevented on the hardware side.

In order to ensure the highest possible reliability, all our Network TAPs with active monitoring ports have redundant power supplies, but can also be additionally operated or protected with 12-48V DC voltage and in some cases also by means of PoE. Our Fiber TAPs, on the other hand, do not require any power supply.

These models of the PacketRaven Network TAPs product family were designed as portable TAPs, but can also be installed in a 19" mounting frame in data centers using a rack mounting kit or on a DIN hat rail using a DIN rail clip.

Our portable TAPs are also available in a specially hardened version for high-security areas according to IEC 62443. They also have secure and encrypted firmware, security seals against unnoticed opening, security screws against unwanted opening and are optimally preconfigured.

Our TAPs with passive monitoring port (LC, MTP®/MPO) are also available in an extra-secure version. These Secure Fiber TAPs have both an additional optical isolator (Data Diode functionality) and an optical filter to ensure that unwanted incoming light signals are blocked at the monitoring port to protect the network from compromise.

The supported network speeds of our TAPs range from 10Mbps up to 400Gbps.

With PacketRaven Network TAPs you get permanent network access without risk and provide e.g. your monitoring tools with 100% reliable network data, including FCS/CRC of errored packets, without introducing a single point of failure.

-  Up to 400 Gbps
-  Full Network Transparency
-  No impairment of Data Traffic
-  100% Network Data
-  Invisible for Attackers
-  No Network Access via Monitoring Port
-  Flexible to Use
-  Plug-n-Play
-  Failure Protection on Power Loss
-  PoE+ Power over Ethernet
-  Redundant Power Supply
-  Various Split Ratios
-  Fast and Precise
-  Support Jumbo Frames
-  Hardened & Secure models available
-  Made in Germany



Learn more at: www.neoxn.eu/ptap

NEOXPacketRaven Portable Hardened TAPs

HIGH SECURITY NETWORK TAP | CRITIS & IEC 62443 APPROVED
SECUREBOOT FIRMWARE | OPTIONALLY PRECONFIGURED | UP TO 1G



PacketRaven Network TAPs are therefore already in the standard version (see page 3) among the network components via which an attack vector is excluded.

For high-security areas according to IEC 62443 and critical infrastructures (CRITIS), however, even this is sometimes not sufficient, which is why NEOX NETWORKS now also offers a specially hardened version of its TAPs.

These TAPs can be delivered pre-configured, if desired, and then do not allow any subsequent configuration changes.

In addition, they are secured against unwanted or unnoticed opening by special screws and security seals.

And to top it all off, these TAPs also have specially secured and encrypted firmware. Secureboot checks each time the TAP is started whether the firmware to be executed has a valid signature and an authorized public key.

If this is not the case, the TAP cannot be put into operation.

Our portable Hardened Network TAPs are available as copper TAPs as well as active Fiber TAPs and support network speeds of 10Mbps, 100Mbps and 1Gbps.

Certifications:

- CE, FCC, RoHS, WEEE, EN 55032 KL. A/B, EN 55035, EN 61000-3-2, EN 61000-3-3, EN 61000-6-2, EN 50121-4:2016, EN 50129

Hardened PacketRaven Advanced Features:

- Optionally preconfigured – do not allow subsequent configuration changes
- Secureboot Firmware – at every start of the TAP it is checked if the firmware to be executed has a valid signature and an authorized public key
- Security seals – cannot be removed unnoticed
- Safety screws – special tool required
- IEC 62443 and CRITIS approved



Portable
PacketRaven
Standard Features



(Optional)
Fix preconfigured



Secured and
encrypted firmware



Security seal
against unnoticed
opening



Safety screws
against unwanted
opening



Learn more at: www.neoxn.eu/htap

NEOXPacketRaven Modular Fiber TAPs

FULL NETWORK VISIBILITY FROM 100M TO 400G | 100% PASSIVE
EXTRA SECURE MODELS AVAILABLE



Fiber TAPs are passive decoupling elements for the secure and reliable tapping of network data in optical networks. These TAPs are looped into the fibre optic line to be monitored and transmit the entire data traffic without interruption and without packet loss.

Our optical TAPs do not require power and are purely passive components. They have no MAC or IP address, but work entirely on OSI Layer 1 and cannot be detected in the network without special and expensive measuring equipment. Hackers and attackers therefore have no chance.

As the integrity of the outgoing data remains unaltered due to this tapping method, our Network TAPs are increasingly used in the areas of network forensics, security and monitoring.

Even in their standard version, Fiber TAPs are among the most secure network components. However, even this is not enough for high-security areas and CRITIS infrastructures. That is why we have developed the Secure Modular TAPs, which are also available.

Due to their optical isolator and optical filter, these TAPs offer a Data Diode functionality which additionally ensures that unwanted incoming light signals are blocked at the monitoring port in order to protect the network from compromise. A very high insertion loss on the return channel from the monitoring port to the network provides an additional security layer.

Some of our TAPs support tapping connections with bidirectional (BiDi) technology based on WDM (Wavelength Division Multiplexing) and are suitable for both Singlemode and Multimode configurations.

PacketRaven Fiber TAPs are designed for data centres and allow you to fit up to 30 network segments with TAPs using our innovative modular 1U chassis. The supported network speeds range from 100Mbps to 400Gbps. Our modular Fiber TAPs are available with LC and MTP connectors, as well as singlemode and multimode variants.

With PacketRaven Network TAPs you get permanent network access without risk and provide e.g. your monitoring tools with 100% reliable network data, including FCS/CRC of errored packets, without introducing a single point of failure.

-  Up to 400 Gbps
-  Full Network Transparency
-  No Impairment of Data Traffic
-  100% Network Data
-  Invisible for Attackers
-  No Network Access via Monitoring Port
-  Plug-n-Play
-  No Power Supply necessary
-  Various Split Ratios
-  Color Coded Connectors
-  Scalable and Modular
-  Extra secure models available
-  Made in Germany



Learn more at: www.neoxn.eu/mtap

NEOXPacketRaven Secure Fiber Network TAPs

FOR HIGH SECURITY AREAS AND CRITIS | DATA DIODE FUNCTIONALITY
FOR MODULAR OR PORTABLE PASSIVE TAPS | FROM 100M TO 400G



Our passive modular and portable Secure Fiber TAPs from the PacketRaven product family feature both an additional optical isolator (Data Diode functionality) and an optical filter that ensures unwanted incoming light signals are blocked at the monitoring port to protect the network from compromise. This adds another layer of security, providing increased protection against attackers and faulty configurations.

Our optical TAPs do not require power, they are purely passive components and therefore cannot be detected on the network without expensive measuring equipment. Hackers and other attackers therefore don't stand a chance, and because the integrity of outgoing data remains unchanged due to this tapping method, Network TAPs are increasingly used in network forensics, security and surveillance.

Passive PacketRaven Secure Fiber TAPs are available in 2 variants. Our modular Fiber TAPs are designed for data centers and allow you to fit up to 30 network segments with TAPs using our innovative 1U modular enclosure.

Our portable Fiber TAPs are developed for mobile use, but can also be installed in a 19" mounting frame in data centres using a mounting kit or on a DIN rails using a DIN rail mounting clip.

Modular PacketRaven Secure TAPs are 100% compatible with our standard modular TAPs without data diode function and can be installed together in the same enclosure. They are also protocol agnostic and compatible with all monitoring systems from leading vendors.

Our Secure TAPs support network speeds from 100Mbps up to 400Gbps, and are available as Singlemode and Multimode models. Without risk, you get permanent network access and provide your surveillance and security tools with 100% reliable network data without introducing a single point of failure. This makes our Secure TAPs particularly suitable for business-critical applications and high-security areas as well as CRITIS infrastructures with high requirements for securing sensitive data.



Passive PacketRaven
Standard Features



Data Diode Functionality
against undesired light injections

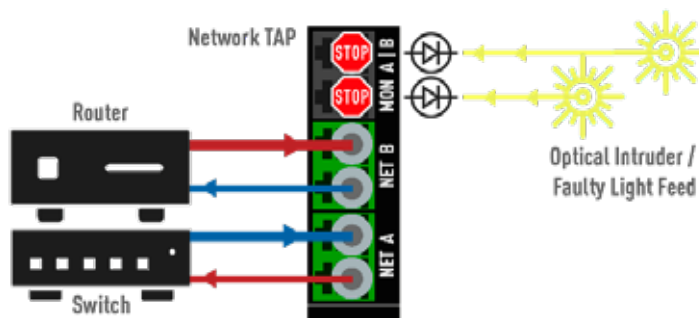


Security seal
against unnoticed opening



Safety screws
against unwanted opening*

Secure TAP with Data Diode functionality:



Learn more at: www.neoxn.eu/stap

* Portable TAPS

NEOXPacketRavenVirtual - Virtual Network TAP

100% NETWORK ACCESS IN VIRTUAL ENVIRONMENTS & THE CLOUD



Our Virtual Network TAPs (vTAPs) are designed to provide secure and reliable access to network data in virtual and cloud environments. With the increase in the use of virtual, cloud-based and hybrid environments in the enterprise space, there has also been an increase in the number of blind spots on the network that make a much-needed, 100% view of network traffic impossible.

But without visibility into your East-West traffic, how do you know if danger is currently looming or that you haven't already been compromised?

NEOXPacketRavenVirtual is a virtual Network TAP and provides physical and virtual security and monitoring tools with complete network visibility in virtualised private, public and hybrid cloud environments.

Simply installed using a Debian package or Docker image, you instantly gain full visibility of virtual machine (VM) traffic (including traffic between VMs) for monitoring security, availability and performance in native Linux systems and cloud environments without impacting performance or architectures and without having to make changes to your network infrastructure.

The often used and already existing (virtual) SPAN/mirror port is unsuitable for professional purposes, as it lacks some important features that the TAP offers. While with port mirroring the entire data traffic to be mirrored is sent to all destinations (security/monitoring tools), with the virtual NEOX TAP a much more granular, such as an n:1 (aggregation) or a 1:n (regeneration) allocation is possible. Furthermore, with the TAP it is also possible to mirror the traffic per direction, i.e. the incoming, the outgoing or the complete network traffic.

Furthermore, the NEOX-TAP offers the possibility to connect to physical devices via GRE/VxLAN tunneling, which is difficult or impossible with port mirroring.

Another feature is the use of stateful filtering (connection-oriented filtering) to copy out only the data that is relevant and to relieve the connected tools. Filter criteria on OSI layers 2-4 are supported. And last but not least, there is the danger that cloud providers can restrict mirrored port mirror traffic according to their terms and conditions. This would result in partial or even total loss of network transparency.

Therefore, our virtual Network TAPs guarantee reliable network analysis or security investigation without compromise. With PacketRavenVirtual Network TAPs you get permanent network access without risk and provide e.g. your monitoring tools with 100% reliable network data.

	Full Network Transparency
	No impairment of data traffic
	100% network data
	For different environments
	Unrestricted network speed
	Flexible deployable
	Alternative to virtual Port Mirroring
	Easy to install & configure
	GRE/VxLAN Tunneling
	OSI Layer 2-4 Stateful Filtering
	Aggregation n:1
	Regeneration/ Replication 1:n
	Developed & programmed in Germany



Learn more at: www.neoxn.eu/vtap

NEOXPacketLion Packet Broker Product Family

SMART AND HIGH PERFORMANCE NETWORK PACKET BROKERS WITH HIGH PORT DENSITY



With a Network Packet Broker, also known as a Data/Network Monitoring Switch or Matrix Switch, you are able to provide your analysis and monitoring systems with all data streams of the Network TAPs distributed in the network or other data sources reliably and in aggregated form.

The Network Packet Broker acts as a link between the access point in your network and, for example, your security tool and, depending on the version, supports all common transceiver standards, from 1 Gigabit SFP slots to the widespread 10 Gigabit SFP+ interfaces to the high-performance QSFP-DD connections, which allow bandwidths of up to 400 Gigabit per interface.

Using dedicated ASIC hardware, which is used in every Network Packet Broker, both simple and complicated filter rules can be created to ensure an optimised data flow towards the analysis systems.

Here, you can filter out unwanted data packets or data packets not required for analysis, or even entire data streams, thus reducing the overall load. This enables you to filter incoming data volumes from measuring points, which may be distributed over several 10G, 100G or even 400G lines, almost latency-free in real time.














This allows you to continue to make optimal use of your existing 1G or 10G monitoring infrastructure and directly discard data that is not of interest without creating additional load on your monitoring systems.

FEATURES

- Flexible port assignment (1:1, N:N, N:1, 1:N)
- Aggregation of 1G, 2.5G, 10G, 25G, 40G, 50G, 100G, 200G and 400G network ports
- Support for filtering rules (MAC, VLAN, IPv4/IPv6, TCP/UDP, DSCP, TCP Flags, MPLS)
- Filtering within a tunnel (GTP, L2TP, MPLS, GRE, and PPPoE)
- Equipped with 8GB Deep Buffer to eliminate packet loss because of micro bursts
- Aggregation and regeneration of any network traffic
- Support for User-Defined Filter rules (UDF)
- Multiple management options (CLI, SSH, SNMP V2/V3, WEB UI, Net CONF and REST API)
- Configure all PacketLion (and PacketTiger) Brokers via a Single-Pane-Of-Glass with our PacketDirector*

* Available soon

SecurITy
made in Germany
Trust Seal
www.certtrust.de/germany

-  Up to 400 Gbps
-  Port Splitting & Port Labeling
-  L3GRE Tunneling Protocol
-  Clustering possible
-  Dig. Diagnostics Monitoring
-  Radius & TACACS
-  Flexible port allocation
-  Tunnel Filtering
-  Aggregation & Regeneration
-  User Defined Filter rules
-  MPLS Stripping
-  Timestamping
-  Packet Slicing
-  8GB Deep Buffer
-  Development & QA in Germany



Learn more at: www.neoxn.eu/lion

NEOXPacketTiger Packet Broker Product Family

NEXT GENERATION NETWORK PACKET BROKER WITH ADVANCED FEATURES



Network Packet Brokers (Data/Network Monitoring Switches) are used to provide the network analysis tools with the network data packets (e.g. via Network TAP) reliably and in optimised form.

New network protocols and tunnel methods lead to changes in the format and length of the packet structure. To gain real insight into network traffic, the payload of the packets must also be analysed. Such changes push the parsing capabilities of switch-based NPBs to their limits and reveal a growing need for more sophisticated methods to process the network data.

NEOXPacketTiger Next Generation Advanced Network Packet Brokers (ANPBs) allow full flexibility in parsing headers and processing payloads, and provide advanced technology for modifying and optimising these packets.

Advanced features such as IPv6 filtering in GTP tunneling, regex and DPI or application-based metadata extraction using CPU-based NPBs are available.

NEOXPacketTiger ANPBs use modern, high-performance, modular and scalable COTS hardware that can be configured for the desired processing capacity. This unique approach removes hardware performance constraints and enables better scaling and matching between hardware and performance requirements.

Media type and speed of your network do not matter, as our PacketTigers are equipped with RJ45/SFP/SFP+/QSFP+/QSFP28 ports depending on the configuration.

The PacketTiger's Next Gen Advanced Packet Processing allows you to work even more granularly and look deeper into the individual packets of the data load than you are used to with regular Network Packet Brokers.

Even resource-intensive scenarios such as removing duplicates in the network or masking or blacking out content in the individual packets are no problem for PacketTiger!

All in all, an Next Gen Advanced Network Packet Broker has significantly more functionalities to optimally distribute network data than a conventional NPB.

NEOXPacketTiger ANPBs are available in different categories: Desktop Appliances, Network Appliances and Servers, enabling a wide range of solutions, from stand-alone solutions with lower data capacity for small businesses and small remote sites to multi-Gbps processing clusters for service providers.



Up to
8x 100Gbps



PacketLion
Features



GTP
Correlation



Data Masking



Deduplication



Advanced Filtering



Netflow/IPFIX
Support



Deep Packet
Inspection



Tunnel
Support



Packet Capturing
& Replay



GTP Tunneling
& IMSI Filtering



Development &
QA in Germany

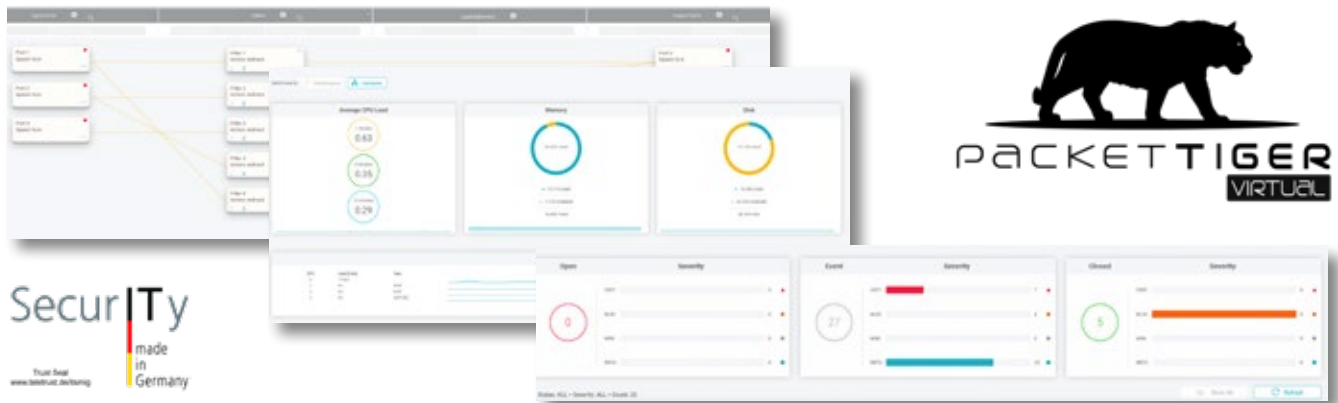


Learn more at: www.neoxn.eu/tiger

NEOXPacketTigerVirtual Packet Broker

MAXIMIZE YOUR NETWORK TRANSPARENCY

IN VIRTUAL ENVIRONMENTS WITH OUR INNOVATIVE PACKET BROKER PLATFORM!



With our Network Packet Broker product family NEXPacketTiger you do not compromise on security, performance and end-to-end quality of service. Today's network infrastructure has to do a lot, while operating 24x7 without interruption and providing critical applications with the necessary data connections.

The benefits of virtual data centres, cloud solutions and SD-WAN technologies are obvious. Due to higher complexity of communication paths, you often lack visibility in both physical and virtual networks. But without visibility, threats can go undetected and reduce the performance of your security and monitoring tools.

The increased shift from physical systems to virtual and hybrid environments presents network managers with unprecedented challenges when it comes to performance and enterprise security.

Because of this migration to the cloud and virtual environments, your existing physical monitoring, analytics and security tools are losing access to your critical network traffic, further degrading visibility. In addition, new solutions are currently deployed in virtual form, adding another challenge to the network infrastructure.

With NEXPacketTiger, we provide a Network Packet Broker solution to meet the need for increased visibility and transparency in both physical and virtual network environments.

This provides SecOps and NetOps with the comprehensive and necessary functions of a hybrid Network Packet Broker that you need for your security and monitoring tools.

KEY FEATURES

- Providing network visibility for virtual network traffic
- Redirecting virtual network traffic to monitoring tools in physical and/or virtual environments
- Leverage physical monitoring tools when migrating to virtual environments
- Optimise virtual and physical monitoring tools by filtering data
- Balance physical and virtual monitoring tools

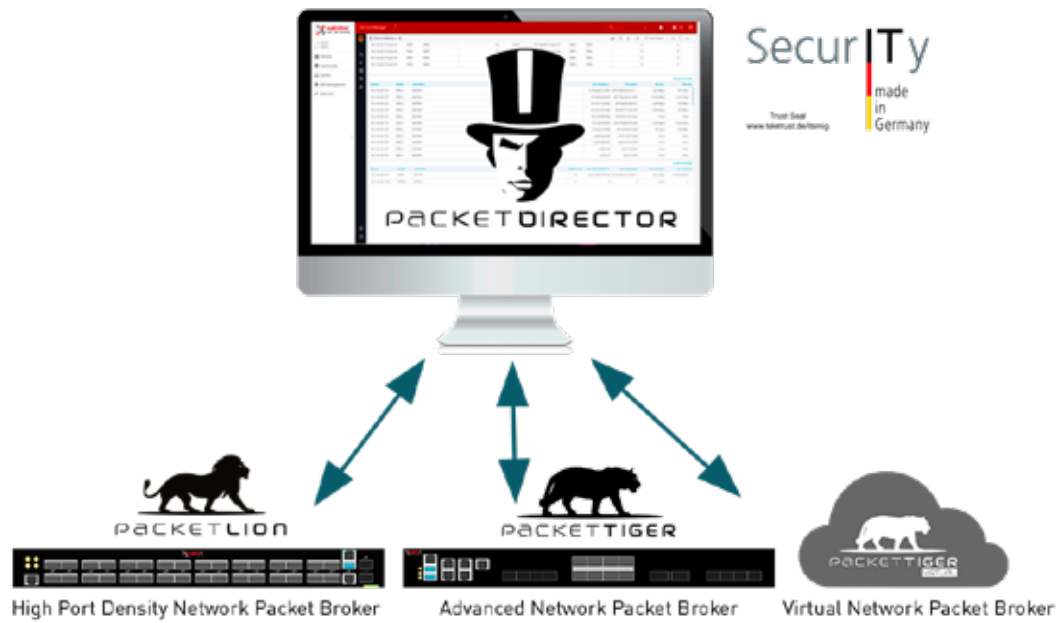
-  For different environments
-  GTP Correlation & Filtering
-  Inner IP LB & Tunnel Filtering
-  OSI L2-L4 & RegEx Filtering
-  User Defined Filters
-  Header Stripping & Editing
-  Deduplication
-  Data Masking
-  Packet Slicing
-  Metadata Extraction
-  Timestamping
-  Capture & Replay
-  IPFIX/NetFlow
-  NEXDevice-Manager



Learn more at: www.neoxn.eu/vtiger

NEOXPacketDirector Network Management

SOFTWARE-BASED | CLUSTERING OF UP TO 100 PACKET BROKERS
FOR PHYSICAL & VIRTUAL BROKERS | CENTRALIZED | BULK OPERATIONS



NEOXPacketDirector is a centralized management system, a single pane of glass which provides users with a holistic view of the devices across the network topology and helps them configure, monitor, manage and operate the Network Visibility deployment.

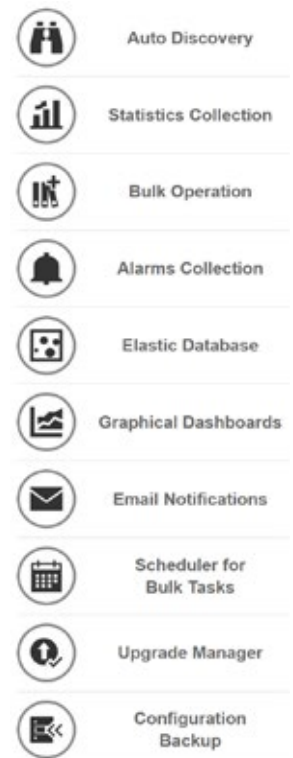
The centralized NEOXPacketDirector software enhances the productivity of network operations and DevOps teams and helps them maximize the ROI from the network visibility equipment in their organization.

NEOXPacketDirector enables auto discovery and management of hundreds of virtual and physical Network Packet Brokers. It collects network statistics and traffic telemetry stored in elastic databases and displayed with real-time graphic visualization utilizing Kibana and Grafana dashboards.

Alarms and events from managed devices trigger email notifications from the PacketDirector, and users can define different events and triggers per device according to cross devices events.

Unique Advantages

- Software based solution that is available on both VM and containers
- Single tool for centralized management of both physical and virtual visibility devices
- Scheduler for bulk operations and tasks for multiple devices (configuration, backup, upgrade, reboot, scripting)
- Centralized filter management per device rules and across devices rules via clustering
- Clustering of up to 100 Network Packet Brokers into a single unit, allowing for policy definition between cross-connected devices



Learn more at: www.neoxn.eu/dir

NEOXPacketWolf

FPGA-BASED ADVANCED PACKET PROCESSING APPLIANCE



SecurITy
made
in
Germany



The NEXPacketWolf 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.

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.

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.



Up to 4x
100G QSFP28



Up to
400Gbps



FPGA design



FPGA based
Nanosecond
Timestamping



FPGA based
Deduplication



FPGA based
Packet Slicing



Protocol Header
Stripping



Developed & QA
in Germany



Learn more at: www.neoxn.eu/wolf

NEOXPacketFalcon - 100G Packet Capture Appliance

PORTABLE 100G NETWORK FORENSICS APPLIANCE

FOR ULTRA-FAST CAPTURING, INDEXING, SEARCHING AND ANALYSING NETWORK DATA



SecurITy
made in Germany

The speed of networks and their complexity continue to increase. And attacks on network infrastructure will also evolve in terms of complexity and stealth. Business operations will continue to be network-heavy, and for optimal and secure IT service delivery, IT security teams must have constant access to detailed traffic analysis. Network forensics provides this essential access and insight that security analysts need.

Our PacketFalcon products are powerful recorders for all types of network speeds, enabling IT organisations to analyse, monitor and accurately record traffic without compromise.

PacketFalcon provides permanent 24 x 7 access to 1G, 10G, 25G, 40G and 100G networks for detailed analysis, including forensic analysis of past events.

PacketFalcon assists security teams with analysis by recording data at key network points while minimising the traffic this data collection can generate. By indexing the data and providing simple and complex filters (Berkeley Packet Filter), PacketFalcon enables security teams to quickly investigate and thus stop attacks - even when they occur in state-of-the-art high-speed networks such as 40G or 100G network topologies.

Linux is used as the operating system and LiveAction's award-winning network forensics software LiveCapture is used for analysis and evaluation. This makes it possible to remotely analyse network traffic across locations and quickly find errors, which drastically reduces MTTR time.

With its robust construction and Linux as operating system, optional 24 TB, 51 TB, 102 TB or 240 TB disk storage and 1G/10G/25G/40G/100G high-performance Gigabit capture adapter, it is the ideal companion for the mobile network analysis and forensics specialist.

-  Lossless recording up to 100G
-  Up to 3 FPGA Capture Cards
-  Storage Capacity up to 240 TB
-  HW Encrypted Capture Storage
-  FPGA based Nanosecond Timestamping
-  FPGA based Packet Slicing & Capture Filter
-  FPGA based Deduplication
-  Hardware RAID 0,5,6,00,50,60
-  PCAP & PCAPNG Support
-  Optional transport case
-  Developed & QA in Germany



Learn more at: www.neoxn.eu/falcon

NEOXPacketFalcon Compact

COMPACT LIGHTWEIGHT 100G NETWORK FORENSICS APPLIANCE
FOR ULTRA-FAST CAPTURING, INDEXING, SEARCHING AND ANALYSING NETWORK DATA



Our PacketFalcon products are powerful recorders for all types of network speeds, enabling IT organisations to analyse, monitor and accurately record traffic without compromise.

PacketFalcon provides permanent 24 x 7 access to 1G, 10G, 25G, 40G and 100G networks for detailed analysis, including forensic analysis of past events.

PacketFalcon supports security teams by accurately and losslessly recording network traffic at key nodes using Network TAPs, indexing and analysing it in real time, enabling rapid investigation of anything happening on the network.

By indexing the data and providing simple and complex hardware and software filters (Berkeley Packet Filter), PacketFalcon enables security teams to quickly investigate and thus stop attacks - even when they occur in state-of-the-art high-speed networks such as 40G or 100G network topologies.

On the hardware side, the PacketFalcon impresses with its robust design, a choice of 31 TB or 61 TB disk storage, a high-performance gigabit capture card from Napatech and an optionally available hard-shell transport case.

Linux is used as the operating system and LiveAction's award-winning network forensics software LiveWire is used for analysis and evaluation.

This makes it possible to analyse network traffic remotely from any location and quickly find errors, which drastically reduces MTTR time.

Its high flexibility in terms of mobile and stationary applications makes it the ideal companion for every network analysis and forensics specialist.



Learn more at: www.neoxn.eu/falconc

-  Lossless Recording up to 100Gbps
-  High-End FPGA Capture Cards
-  For 1G - 100G Networks
-  Storage Capacity up to 61 TB
-  IEEE 1588v2 Precision Time Protocol
-  Portable & Rackmountable
-  FPGA based Packet Slicing & Capture Filter
-  FPGA based Nanosecond Timestamping
-  FPGA based Deduplication
-  PCAP & PCAPNG Support
-  Cascading possible
-  Optional Transport Case
-  Developed & QA in Germany

NEOXPacketFalcon Mini

PORTABLE AND COMPACT 1G/10G/25G NETWORK FORENSICS APPLIANCE
FOR ULTRA-FAST CAPTURING, INDEXING, SEARCHING AND ANALYSING NETWORK DATA



The speed of networks and their complexity continue to increase. And attacks on the network infrastructure will also evolve in terms of complexity and stealth.

Thus, for optimal and secure IT service delivery, IT security teams must have permanent access to detailed traffic analysis. Network forensics provides this essential access and insight that security analysts need.

Our PacketFalcon products are powerful recorders for all types of network speeds, enabling IT organisations to analyse, monitor and accurately record traffic without compromise.














The PacketFalcon Mini provides permanent 24 x 7 access to 1G, 10G and 25G networks for detailed analysis, including forensic analysis of past events.

PacketFalcon assists security teams with analysis by recording data at key network points while minimising the traffic this data collection can generate.

By indexing the data and providing simple and complex filters (Berkeley Packet Filter), PacketFalcon enables security teams to quickly investigate and thus stop attacks.

Linux is used as the operating system and LiveAction's award-winning network forensics software LiveWire is used for analysis and evaluation. This makes it possible to analyse network traffic remotely from any location and quickly find errors, which drastically reduces MTTR time.

With its robust and compact design, optional 8TB, 16TB or 32TB disk storage and a 1G/10G/25G or 1G high performance Gigabit capture adapter, it is the ideal companion for the mobile network analysis and forensics specialist.

-  Lossless recording up to 25Gbps
-  High Speed FPGA Capture Card
-  Storage up to 32 TB
-  Portable, compact and robust
-  Flexible due to SFP/SFP+/SFP28
-  FPGA based Nanosecond Timestamping
-  FPGA based Packet Slicing & Capture Filter
-  FPGA based Deduplication
-  Lossless Full Packet Capturing
-  PCAP & PCAPNG Support
-  IPFIX/NetFlow Export
-  Cascading possible
-  Developed & QA in Germany



Learn more at: www.neoxn.eu/falconm

NEOXPacketGrizzly

MODULAR AND SCALABLE NETWORK FORENSICS SOLUTION
FOR ULTRA-FAST CAPTURING, INDEXING, SEARCHING & ANALYSING NETWORK DATA



Write to Disk Full Packet Capture Performance up to 100Gbps

There is more data than ever before on corporate networks, but the accuracy of network analysis usually leaves much to be desired. Companies rely on their networks more than ever, but have little confidence in network monitoring and troubleshooting.



How can network monitoring and troubleshooting be made more practical without losing sight of the essentials?

PacketGrizzly, an industry-leading modular packet capture and analysis solution, enables real-time and post-event analysis on networks running at speeds up to 100Gbps.

PacketGrizzly gives network administrators the ability to identify network and application performance issues in 1G/10G/25G/40G/100G Gigabit Ethernet, 802.11ac WLAN, VoIP and Video over IP networks.

PacketGrizzly provides a powerful network capture solution that records up to multiple petabytes of traffic without packet loss, as well as award-winning Omnipcap software for real-time analysis of live network traffic and forensic network analysis of recorded traffic.

PacketGrizzly consists of a capture appliance for packet capture and, depending on the storage space required, internal storage in the capture appliance or up to four storage units on which the captured packet data is recorded.

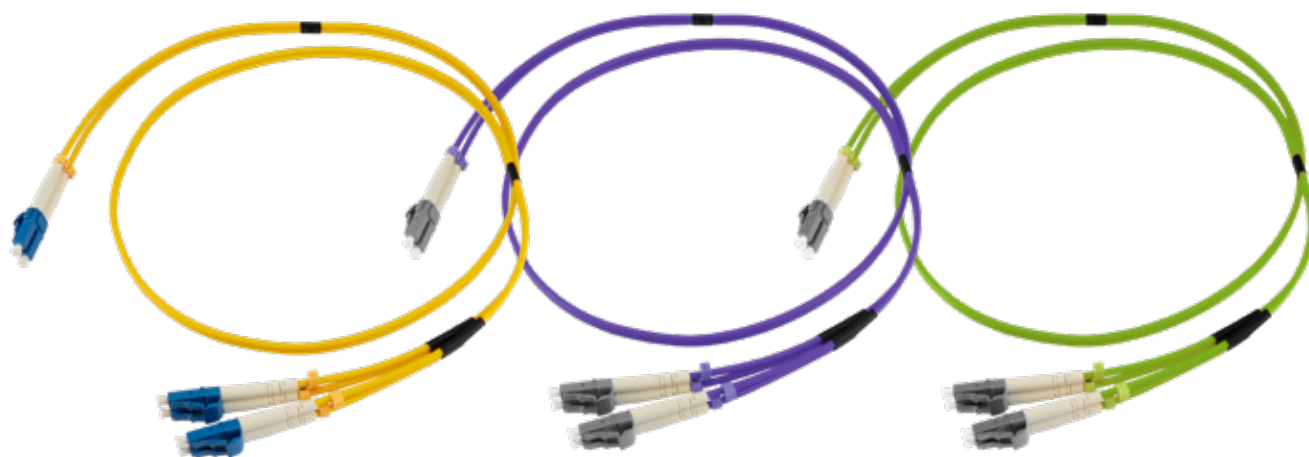
-  Up to 100 Gbps
-  High-End FPGA Capture Cards
-  Storage Capacity up to 6.7 Petabyte
-  HW Encrypted Capture Storage
-  IEEE 1588v2 Precision Time Protocol
-  FPGA based Nanosecond Timestamping
-  FPGA based Packet Slicing & Capture Filter
-  FPGA based Deduplication
-  Hardware RAID or ADAPT
-  PCAP & PCAPNG Support
-  Supports SSL Decryption
-  Developed & QA in Germany



Learn more at: www.neoxn.eu/grizzly

Y-Kabel für Fiber-Netzwerk-TAPs

FOR FIBER NETWORKS & LC CONNECTORS

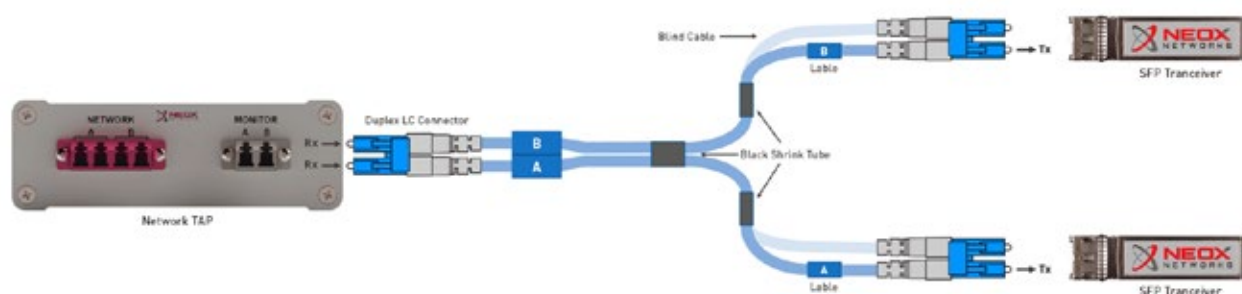


A Network TAP equipped with LC connectors has three duplex connectors, two of which are needed for looping through the network traffic to be analysed and one duplex connector for passively tapping the mirrored data for forwarding to, for example, a Network Packet Broker (NPB), an analysis system, an Intrusion Detection System (IDS) or an Intrusion Prevention System (IPS).

This is the so-called monitoring port at which both the left and the right data traffic is present. These two outputs must be fed into two monitoring ports using two transceivers in order to fully receive the bi-directional traffic, as only the receive side (Rx) of the transceivers can be used for recording.

This presents a challenge because the output of the TAP is a duplex port and yet two separate ports are needed on the receive side for two individual transceivers.

To avoid this problem, it is best to use one of our special Y-cables that convert one duplex connector into two duplex connectors oriented so that the light is fed exclusively into the receiving side of the transceivers.



Learn more at: www.neoxn.eu/ycable

Optical Transceiver

E.G. FOR NETWORK TAPS, PACKET BROKERS, PACKET CAPTURE APPLIANCES

Our optical transceivers are universally applicable and meet the highest quality requirements. Available for networks and media types from 1G to 400G, they provide a cost-effective and flexible solution for devices with integrated SFP, SFP+, SFP28, QSFP+, QSFP28, QSFP56 or QSFP-DD ports.

They can be used in some of our PacketRaven Network TAPs models, our Network Packet Broker product families PacketLion and PacketTiger, as well as in some PacketFalcon Packet Capture Appliances. All our transceivers are of course MSA compliant and can therefore not only be used in our own products, but also in devices from other manufacturers.



Other Accessories

NETWORK TAP MOUNTING KITS FOR SERVER RACKS & DIN HAT RAILS

NETWORK TAP MOUNTING FRAMES AND COVER PLATES



HIGH PERFORMANCE CAPTURE CARDS



TRANSPORT CASES

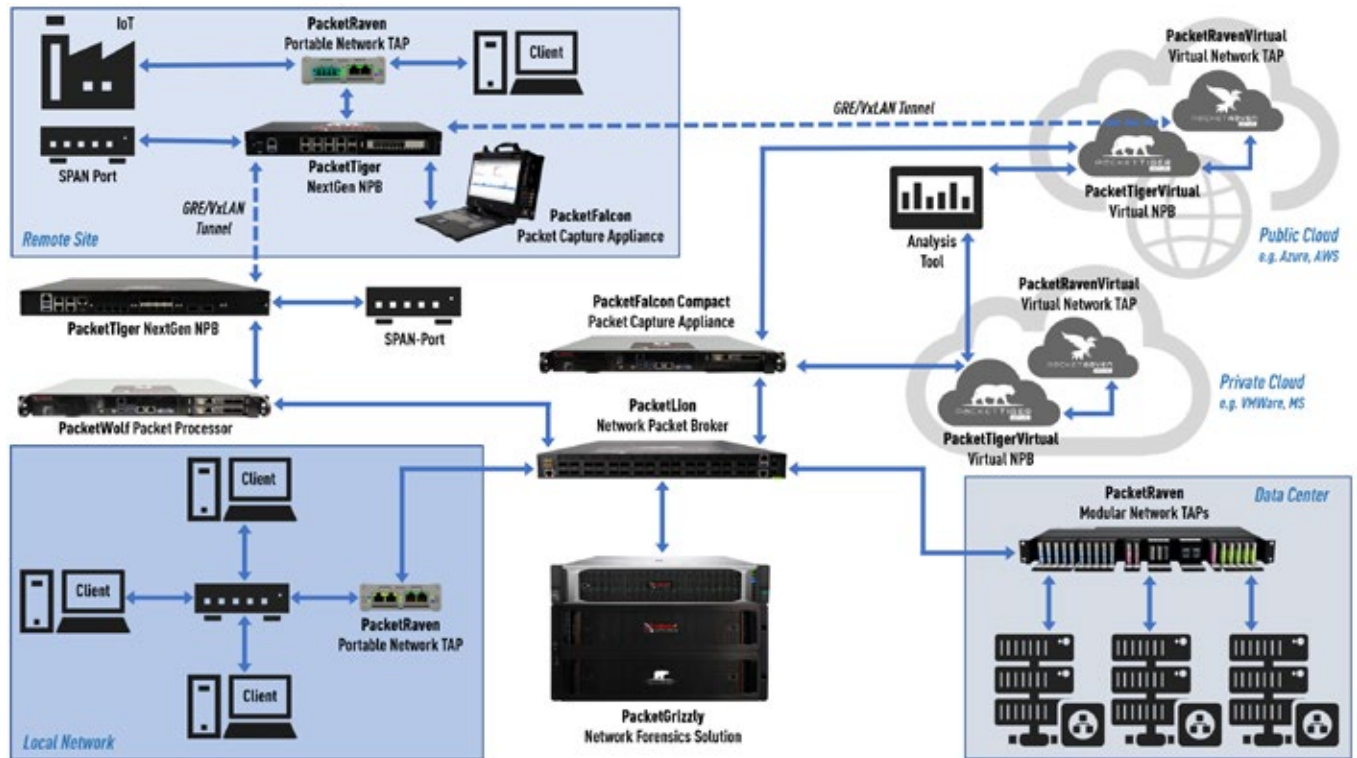


AS WELL AS
STANDARD FIBER OPTIC CABLES, M12 CABLES, FAN-OUT CABLES,
FIBER LOOPBACK ADAPTER, HAT RAIL KITS, ETC.

[illegible]

NEOXUseCases

FOR PHYSICAL & VIRTUAL NETWORK TAPS, NETWORK PACKET BROKERS, PACKET CAPTURE & ADVANCED PACKET PROCESSOR APPLIANCES



NEOX NETWORKS GmbH

Monzastr. 4
63225 Langen
Germany

Tel.: +49 6103 / 37 215 910

Mail: solutions@neox-networks.com

URL: www.neox-networks.com