NEOX NETWORKS
NEXT GENERATION NETWORK VISIBILITY

NEOX**PacketShark TLS/SSL Visibility Layer**

PROVIDING NETWORK TRANSPARENCY INTO TLS/SSL TRAFFIC

packetshark

PacketShark offers an all-in-one solution to improve SSL infrastructure, providing security devices with visibility into TLS/SSL encrypted traffic and optimizing existing security investments. It supports policy-based traffic management and easily integrates with current architectures, while centralizing SSL decryption and encryption using the latest technologies across the security framework.

Multi-Layered Security

To effectively protect an enterprise network from both internal and external threats, a range of security devices is essential. Traditionally, addressing security challenges has involved administrators manually linking various point products to form a „security stack". PacketShark integrates with leading security vendors, allowing deployment within a „secure decrypt zone" to safeguard the entire network against encrypted threats. PacketShark works seamlessly with:

- Firewalls
- Intrusion Prevention Systems (IPS)
- Unified Threat Management (UTM) platforms
- Data Loss Prevention (DLP) tools
- Network Detection and Response (NDR)
- Web Application Firewall
- Threat prevention platforms
- Network forensics and web monitoring solutions

Dynamic Visibility Plane

Dynamic service chaining offers a more flexible approach by routing traffic based on the Security Policy context. This enables specific types of traffic to flow through tailored chains of services, such as layer 2 and layer 3 inline services, receive-only services, ICAP, and HTTP web proxy services, optimizing security based on traffic needs.

- **TLS 1.3 Support**
- **Compliance & Privacy**
- **Maintain 5-Tuple**
- **Bypass**
- **URL Filtering**
- **Certificate Distribution & Control**
- **SSL Decryption on all L4 Ports**
- **Supports Forward Proxy & Reverse Proxy**

// NEOX**PacketShark**

PacketShark uses advanced URL classification to categorize traffic from domains, allowing selective bypass of decryption to protect sensitive data such as medical or financial records, ensuring compliance with standards like HIPAA. Additionally, its URL filtering feature boosts employee productivity and mitigates risks by blocking access to malicious websites, including those linked to malware, spam, and phishing.

Modular and Flexible

The PacketShark is a modular solution that keeps up with the process of ever-growing networks with its possibility to utilize NMC modules to increase the port density if required. To add more protection to the solution these NMC modules are also available with integrated Bypass functionality, handing over full control of the network links to the user.
In combination with an external PacketHawk Inline Bypass and PacketLion Network Packet Brokers one can scale their security design to an unlimited degree.

KEY FEATURES

- **Inbound and Outbound Decryption**
  - Ability to decrypt/encrypt both incoming and outgoing TLS/SSL traffic to provide visibility to Security tools such as IDS, NDR, WAF, Forensics etc.

- **TLS 1.3 Support**
  - Can handle multiple encryption protocols, such as SSL 3.0, TLS 1.0, 1.1, 1.2, and TLS 1.3

- **URL Classification**
  - PacketShark's URL classification system categorizes traffic, enabling selective decryption bypass to protect privacy. This ensures sensitive data, like medical or financial records, stays encrypted and complies with regulations such as HIPAA.

- **URL Filtering**
  - URL filtering enhances employee productivity and mitigates risks by blocking access to malicious websites, such as those hosting malware, spam, or phishing attacks.

- **Policy-Based Traffic Control**
  - Policies to control what types of traffic should be decrypted and inspected, ensuring flexibility in managing different traffic flows.

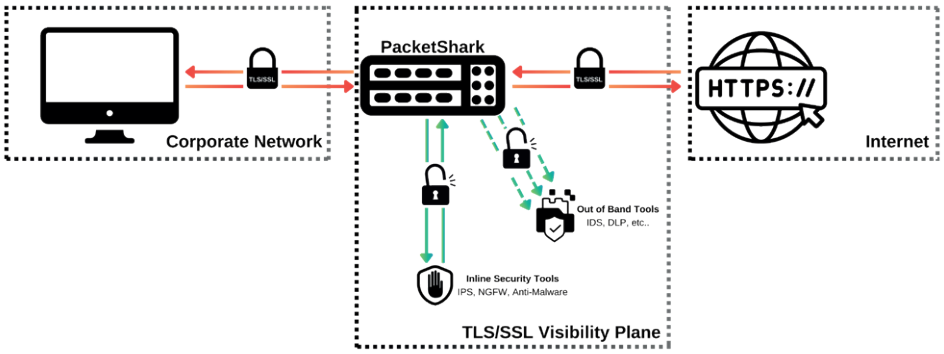
- **Inline and Out-of-Band Deployment**
  - Enables real-time decryption of network traffic and offers the option to mirror or copy traffic for inspection without adding latency.

- **Integration with Security Ecosystems**
  - Integrates seamlessly with NGFWs, IDS/IPS, DLP, and other security tools to share decrypted traffic for inspection.

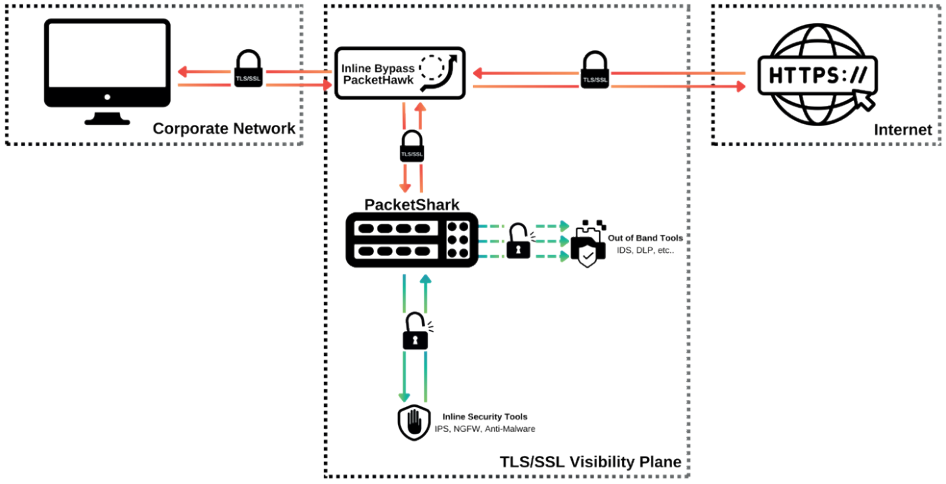
- **Logging and Auditing**
  - Full audit trail and logging capabilities to comply with regulatory requirements (e.g., GDPR, HIPAA, PCI DSS).

DEPLOYMENT SCENARIOS

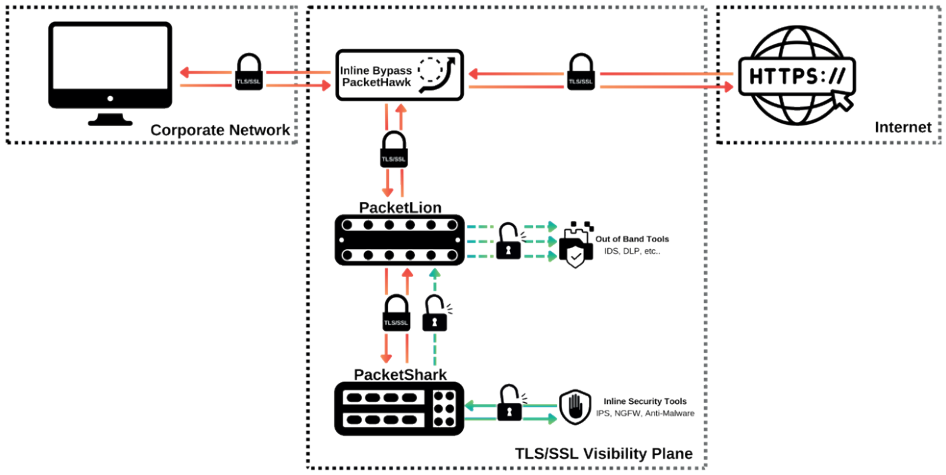
PacketShark - Inline Deployment



PacketHawk & PacketShark - Secured Deployment



PacketHawk & PacketLion & PacketShark - Orchestrated Deployment



// NEOX**PacketShark**

TECHNICAL SPECIFICATIONS

DIMENSIONS (HxWxD)	WEIGHT
438mm x 760mm x 88mm	ca. 21 kg

POWER SUPPLY
1600W 1+1 ATX Redundant PSUs

TEMPERATURES & RELATIVE HUMIDITY	
Operation	0°C - 40°C, 5% to 90% relative humidity (Rh)
Storage	-20°C - 70°C, 5% to 95% relative humidity (Rh)

MODELS

ITEM NO.	THROUGHPUT TOTAL TRAFFIC*	THROUGHPUT SSL TRAFFIC*	NMC SLOTS	HEIGHT
NX-PS-DC-1M	15 Gbit/s	7 Gbit/s	8	2U
NX-PS-DC-1L	25 Gbit/s	13 Gbit/s	8	2U
NX-PS-DC-1XL	50 Gbit/s	25 Gbit/s	8	2U

** Minimum*

NMC MODULES

ITEM NO.	PORTS	INTER-FACE	BYPASS	NMC SLOT REQUIREMENT
NX-PS-DC-8PC	8x 10/100/1000Base-T	RJ45	✓ 4 Pairs	1
NX-PS-DC-4P1ML	4x 1G Multimode	LC	✓ 2 Pairs	1
NX-PS-DC-4P1SL	4x 1G Singlemode	LC	✓ 2 Pairs	1
NX-PS-DC-4P10ML	4x 10G Multimode	LC	✓ 2 Pairs	1
NX-PS-DC-4P10SL	4x 10G Singlemode	LC	✓ 2 Pairs	1
NX-PS-DC-2P40MM	2x 40G Multimode	MTP	✓ 1 Pair	1
NX-PS-DC-2P40SL	2x 40G Singlemode	LC	✓ 1 Pair	1
NX-PS-DC-2P100MM	2x 100G Multimode	MTP	✓ 1 Pair	2
NX-PS-DC-2P100SL	2x 100G Singlemode	LC	✓ 1 Pair	2

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