NEOX NETWORKS
NEXT GENERATION NETWORK VISIBILITY

Data Sheet

NEOX**PacketHawk** Inline-Bypass Switch & TAP

High-Performance, High-Availability, Security Service-Chaining and Visibility with 10/25/40/100Gbps Network and Inline Security Devices

PacketHawk enables you to:

- Assure highest availability for security service chaining and inline security devices at the network edge for up to 100Gbps north-south traffic
- Add or remove security devices for strenthening the security stack, or for maintenance, without any network downtime, guaranteeing business continuity
- Provision complete north-south network visibility through breakout and aggregated mirroring along with bypass switching
- Connect network and inline devices for versatile speed of 10, 25, 40, and 100Gbps with up to 2 inline devices per module
- Use advanced filtering along with multiple operational modes for full control: cascade, high-availability, load balancing, bypass, and visibility modes along with controlled failover conditions

NEOX Solution

The NEOX PacketHawk Inline-Bypass Switch and TAP is engineered to safeguard mission critical network links while enabling full operational continuity for inline security and monitoring devices/tools such as Firewalls, IPS, DDoS, DLP, WAF, SSL/TLS, and threat-prevention platforms. As networks evolve toward high bandwidth 10/25/40/100Gbps environments, inline devices introduce potential points of failure. PacketHawk eliminates this risk through intelligent, data center and carrier-grade bypass protection that keeps north-south traffic flowing—no matter what happens downstream.

PacketHawk sits transparently between north-south mainstream production links (traffic) and inline devices, continuously monitoring devices' health via heartbeat packets and link-loss detection (LLD). If an inline device becomes unresponsive, loses power, or requires maintenance, PacketHawk instantly switches to load-balancing, standby, or bypass mode, as configured, to maintain uninterrupted traffic flow and service. Once the inline device recovers, PacketHawk can automatically restore the original traffic path without manual intervention. Designed with a modular architecture, redundant hardware, and ultra-low latency processing, PacketHawk delivers the performance, reliability, and flexibility required for today's mission-critical networks in enterprise data centers, telecom environments, carrier networks, and industrial infrastructures.

NEOX PacketHawk enables network and security teams to provision:

- **Business Continuity**
  Automatically bypass inline security devices during power loss, hardware failure, or software crash, ensuring traffic continues to flow and preventing outages.
- **Eliminate Single Points of Failure**
  Decouple network availability from the health of inline security tools, allowing maintenance or failures without taking applications offline.
- **Non-Disruptive Maintenance**
  Enable hot insertion, removal, upgrades, and reboots of inline security devices without requiring network downtime or traffic reconfiguration—ideal for 24/7 operational environments.

- **Preserve SLAs and Uptime Guarantees**
  Prevent security device failures from cascading into application or service outages.
- **Support Disaster Recovery and Incident Response**
  Allow rapid isolation or removal of compromised or malfunctioning devices
- **Improve Operational Resilience**
  Enable testing, tuning, and policy changes on inline devices/tools without impacting production
- **High-Availability Network Designs**
  Deploy in active-active or active-standby architectures to enhance resilience in data centers, telecom central offices, and service provider backbones.
- **Hybrid Visibility & TAP Deployments**
  Use PacketHawk in bypass or TAP/mirror mode for combined inline inspection and out-of-band monitoring—maximizing tool investment and visibility across complex networks.
- **Tool Testing & "Sandboxing"**
  Insert, test, validate, or benchmark new security or monitoring tools inline without risk, then remove them instantly using bypass mode.

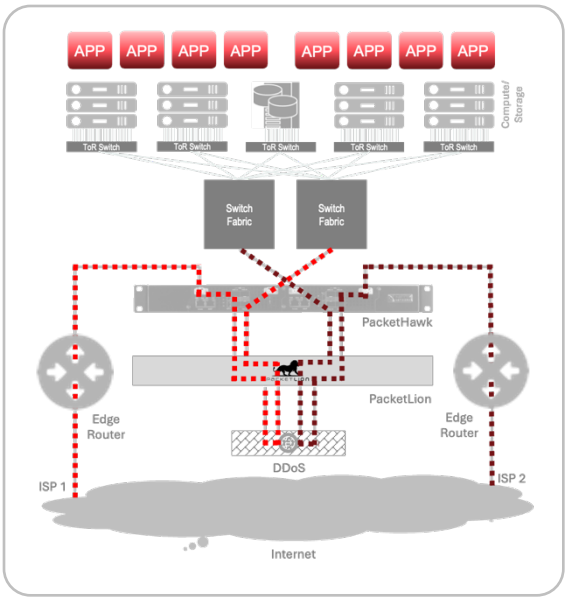

Diagram-1: PacketHawk at DC Edge

Designed for flexible inline visibility and control, PacketHawk is available in a compact (1U rackmount) modular form factor to support a wide range of deployment scenarios to deliver high-throughput inline bypass switching with advanced traffic monitoring, making it ideal for data centers, cloud on-ramps, service providers, and large-scale enterprise networks. Its energy-efficient and redundant IO and power design provides tactical network monitoring without compromising availability or fail-safe operation.

Diagram-2: PacketHawk Front and Back View

Modes of Operation

The PacketHawk supports multiple deployment and operation modes to address a wide range of network architectures, security toolchains, and visibility requirements. Whether protecting critical inline devices or aggregating monitoring traffic, PacketHawk adapts to your infrastructure with precision.

PacketHawk supports both inline-bypass and visibility (TAP/mirror) modes within the same platform—allowing a single appliance to protect inline devices while simultaneously aggregating flows for in-depth monitoring and observability. This makes it a versatile choice for converged traffic-visibility architectures that combine inline security and out-of-band analysis.

By deploying PacketHawk in these configurations, organizations gain the reliability of uninterrupted production traffic, the flexibility to scale across link rates and locations, and the operational freedom to manage, upgrade, or replace inline tools without impacting service availability.

Service-Chain Mode

PacketHawk is designed to support service-chaining of two inline devices through a single bypass module (or four devices per chassis)—ideal for layered security stacks. For example, traffic can flow through inline device 1 (e.g., IPS), cascade into inline device 2 (e.g., WAF), with PacketHawk managing failover and path integrity across the chain. The without disruption of unaffected segments, simplifying upgrades and maintenance.

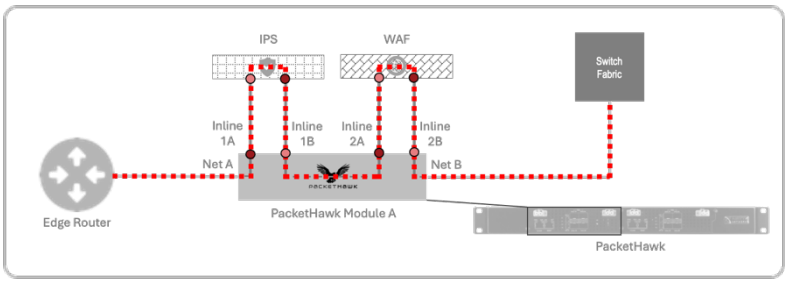

Diagram-3(a): PacketHawk Service Chain Mode

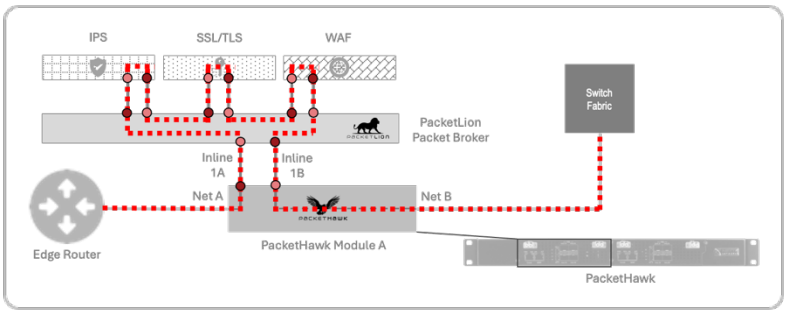

Diagram-3(b): PacketHawk Extended Service

Extended Service-Chain with a Packet Broker

PacketHawk can extend to many more inline devices in a service chain through a NEOX PacketLion Network Packet Broker. PacketLion provides high-density 10/25/40/100/400Gbps aggregation along with local heartbeat and advanced filtering capabilities in addition to many other features.

It also leaves ample room (ports) for futureproofing and expansion of the tool rail, without any disruption to the production network. In this case, three inline devices such as IPS, SSL/TLS, and WAF are connected to a PacketHawk through a PacketLion.

High Availability Mode

For ultra-high-availability deployments, PacketHawk supports dual-redundancy configurations: dual inline devices chained through a single link or dual bypass modules in parallel. Additionally, the architecture supports both Active Bypass (software-controlled failover) and Passive Bypass (physical relay fallback in case of power loss). This dual-layer protection ensures traffic continuity even if the bypass switch itself suffers a power or module failure. In this case, if the inline device 1 (WAF A) fails, the traffic is failed over and routed through inline device 2 (WAF 2) connected to the same module.

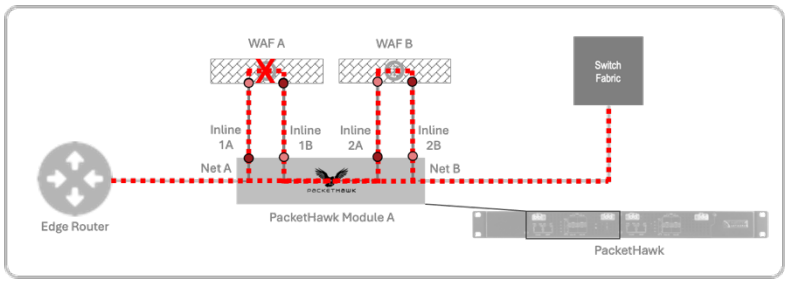

Diagram-4: PacketHawk High Availability Mode

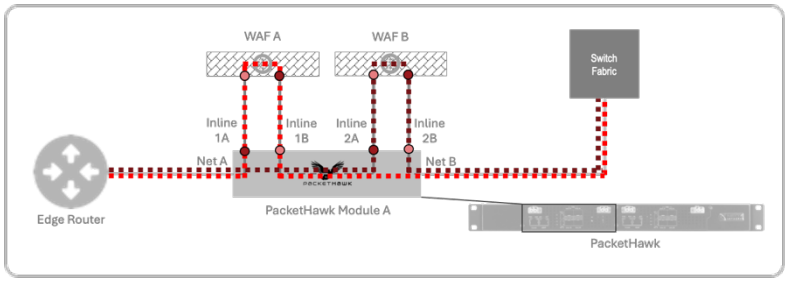

Diagram-5: PacketHawk Load Balancing Mode

Load Balancing Mode

Load balancing mode distributes traffic across multiple inline devices simultaneously to increase processing capacity and prevent bottlenecks. PacketHawk uses flow-aware hashing (odd/even IP addresses) to ensure session-consistent forwarding, making it ideal for Firewalls, IDS/IPS, WAF, DDoS or SSL/TLS inspection devices. If one tool becomes unavailable, network traffic is automatically redistributed to maintain service continuity. This mode enables scalable performance and flexible tool expansion in high-bandwidth environments.

Bypass Mode

In typical deployment, PacketHawk is placed directly inline on the production network link such as north-south WAN/LAN border. The production network traffic flows through the PacketHawk inline-bypass module, then onward to one or two inline devices. PacketHawk continuously monitors both the inline devices (via heartbeat packets) and network link status (via link-loss detection or LLD). On detection of one or more inline device failure, as configured, PacketHawk instantly switches the link into bypass (protected path) mode—directing traffic straight through the network path and temporarily excluding the devices—ensuring uninterrupted service. Once the devices recover or get replaced, traffic flows are re-instated. This mode supports both Active/Passive and Active/Active service-chaining of inline devices. In this example, if WAF A and WAG B go down, the traffic is bypassed straight.

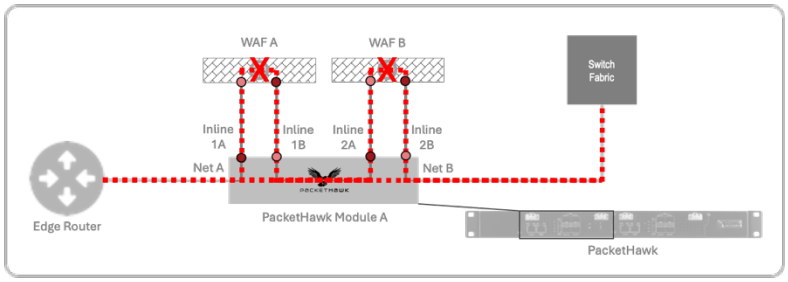

Diagram-6: PacketHawk Bypass Mode

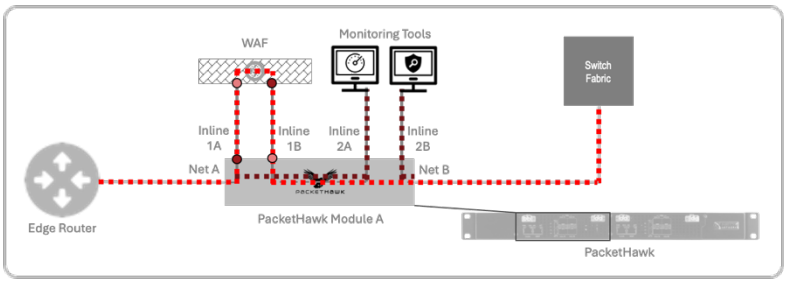

Diagram-7(a): PacketHawk TAP-Breakout Mode

Visibility or Mirror Mode

In scenarios where out-of-band monitoring is required (for example NDR, forensics, or analytics tools), PacketHawk can operate in Visibility (TAP or Mirroring) mode. In this configuration, the PacketHawk module aggregates or breaks out traffic from the network links, and forwards copies to monitoring devices while optionally also protecting inline devices.

The available modes include “Tap-Breakout” (each monitoring tool receives its own dedicated feed) and “Tap-Aggregate” (tools share aggregated streams). This flexibility optimizes tool usage and supports hybrid inline + out-of-band topologies.

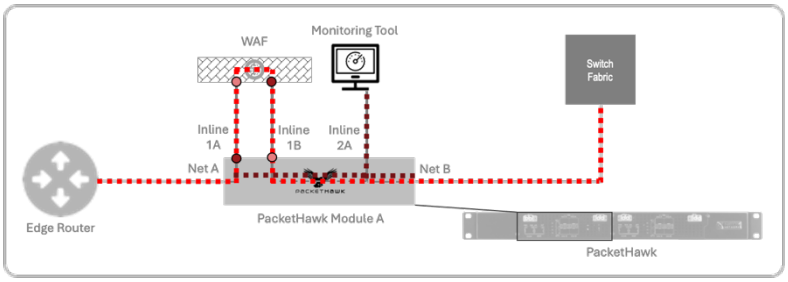

Diagram-7(b): PacketHawk TAP-Aggregate Mode

Failover Condition Modes

Forced & Semi-Auto Condition Modes (Flexible Failover Control)

NEOX PacketHawk inline-bypass switch includes four selectable failover condition modes in addition to the operational modes described above: Auto, Semi-Auto, Forced-Inline, and Forced-Bypass. These failover conditions determine how the network should behave in case of network or inline device failures. These modes assure a non-disruptive operation where network redundancy is provisioned through dual homing.

In Auto mode, the system dynamically chooses inline or bypass path based on real-time health status. Semi-Auto mode allows an operator to define a preferred primary path, with automatic failover enabled. Forced Inline locks the link through the appliance (bypass disabled); Forced Bypass keeps traffic flowing directly through the network, bypassing the appliance altogether. These modes give administrators full control over maintenance scenarios, testing, and risk posture.

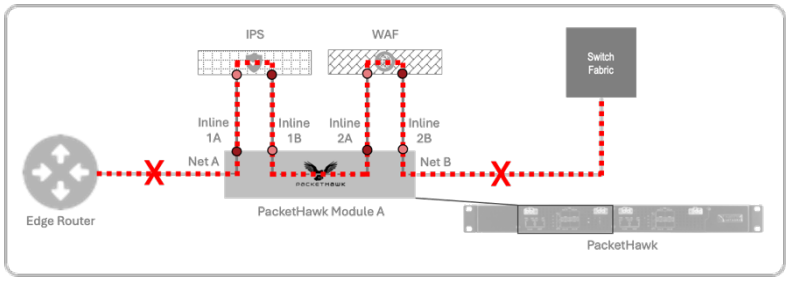

Diagram-8(a): PacketHawk Link Drop Condition

Link Loss Detection (LLD) ensures correct traffic handling during network switches or edge router failures by propagating link-down conditions across the inline path connected to PacketHawk. When the link to the outside network drops due to a router, switch, or carrier failure, the corresponding link to the inside network is also automatically brought down. This prevents the inline device chain from receiving traffic in only one direction and eliminates the risk of asymmetric flows or traffic black holing. The same behavior applies in reverse: if the inside network link fails, the outside link is dropped as well. By ensuring both directions of the traffic path remain synchronized, LLD maintains network stability, preserves proper failover behavior, and prevents inline security or monitoring devices from seeing incomplete or stale traffic flows.

When a Link-Drop Network condition is configured, if a link to any inline device fails and heartbeat is lost from the device, the corresponding links to both the outside and inside networks are automatically brought down to maintain traffic symmetry and prevent black-holing.

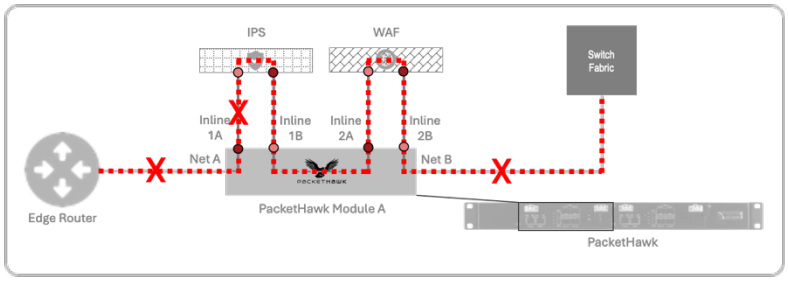

Diagram-8(b): PacketHawk Link Drop Network Condition

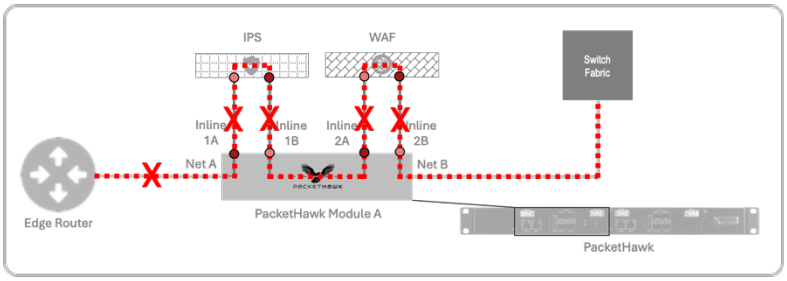

Diagram-8(c): PacketHawk Link Drop Inline Condition

When Link-Drop Inline condition is configured, if the link to either the outside or inside network fails, Link Loss Detection (LLD) automatically drops all inline device links to prevent asymmetric traffic and maintain path integrity.

Inline and Bypass Filtering

PacketHawk inline filtering provides granular, high-performance traffic control across Layers-2 through 4, allowing traffic to be included or excluded based on MAC address, VLAN, IP address, protocol, and port. Supporting up to 940 hardware-based filters with no performance impact, PacketHawk ensures deterministic, line-rate operation even in high-throughput environments. In inline filtering mode, packets that do not meet defined filter criteria continue to pass inline through the network, while trusted or non-relevant traffic can be safely bypassed.

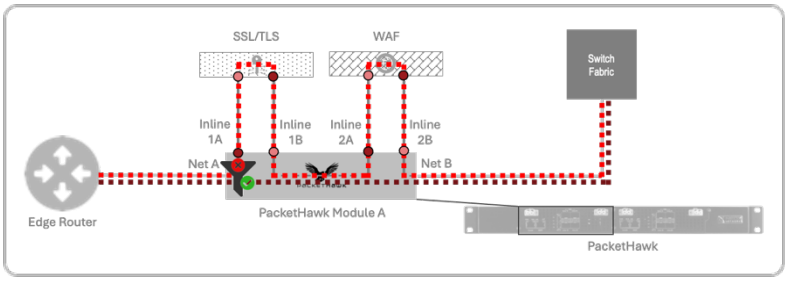

Diagram-9: PacketHawk Inline Filtering

Bypass filtering reverses this behavior, enabling only selected traffic flows to traverse the inline security or monitoring devices, while all other packets are automatically bypassed. This selective steering ensures critical traffic receives full inspection while preserving network performance, reducing tool load, and maintaining high availability.

Deployment

The PacketHawk Inline Bypass Switch is engineered for flexible, high-availability deployment across a variety of network environments—from enterprise data centers to telecom central offices, remote industrial sites, and distributed branch networks. Data center deployment: Mount PacketHawk in a 1RU rack space between core switches and edge routers with inline security or monitoring appliances connected. In this configuration, PacketHawk protects high-speed north–south links (e.g., 25/40/100Gbps) by diverting traffic into bypass mode when inline tools fail, ensuring continuous service.

Telecom / service-provider central office: Install PacketHawk alongside inline devices such as firewalls, SSL/TLS decryptors or next-gen intrusion prevention systems (IPS). Its hot-swappable modules and dual-power architecture make it ideal for carrier-grade operations, allowing seamless maintenance of inline tools without interrupting subscriber traffic.

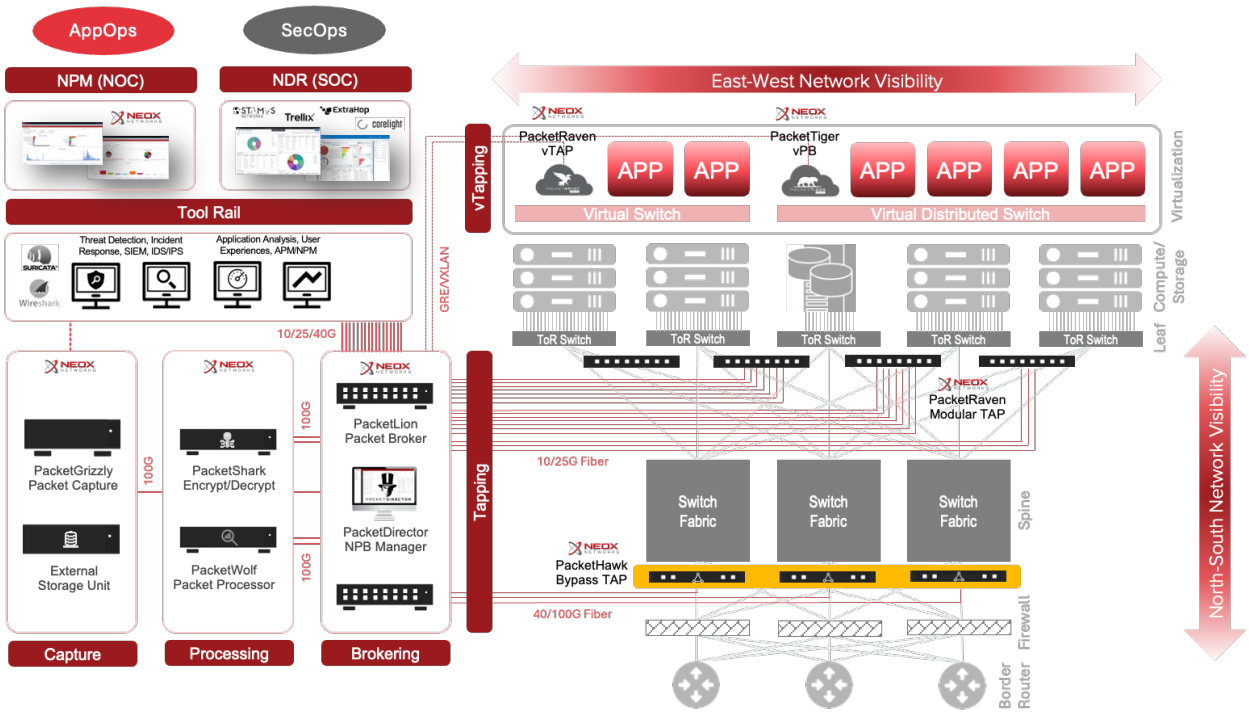

Diagram-10: NEOX PacketHawk Deployment in the Data Center

Key Benefits

Guaranteed Traffic Continuity

The PacketHawk Inline Bypass Switch is designed to ensure that network traffic always remains up, even when inline security or monitoring tools fail or require attention. By intelligently monitoring the health of connected appliances and automatically switching into bypass mode, when necessary, PacketHawk eliminates the downtime typically associated with inline deployments. This fail-safe "always-on" design ensures critical business operations continue without disruption, protecting productivity, revenue, and customer experience. Whether a tool loses power, crashes, or is simply undergoing maintenance, PacketHawk keeps traffic flowing reliably through the network link.

Inline Tool Resilience & Intelligent Health Monitoring

PacketHawk continuously verifies the availability and responsiveness of inline tools using advanced heartbeat packets and link-loss detection mechanisms. These real-time checks allow the system to instantly detect tool degradation or failure and take corrective action in microseconds. Once the inline tool recovers, PacketHawk can automatically reinstate the traffic path back through the device without manual intervention. This intelligent orchestration maximizes tool uptime while preventing tool instability from becoming a network-wide issue. By effectively isolating failures, PacketHawk enhances the resilience of your entire security and monitoring ecosystem.

Modular, Scalable High-Performance Architecture

Built for modern multi-gigabit networks, PacketHawk features a modular chassis that supports a wide range of interface types and speeds—including 1/10/25/40/100Gbps modules. Each module operates as an independent bypass segment, allowing you to deploy multiple protected links in a single compact system. With hot-swappable cards, redundant power supplies, and field-replaceable fans, PacketHawk delivers the reliability required for mission-critical operations. As your network grows or transitions to higher link speeds, PacketHawk scales seamlessly, ensuring long-term investment protection.

Flexible Deployment Modes & Multi-Tool Integration

PacketHawk adapts to virtually any network architecture thanks to its wide range of configurable modes, including inline, bypass, forced-bypass, forced-inline, TAP breakout, TAP aggregate, and mirror modes. This flexibility enables operators to protect inline tools, provide out-of-band monitoring, feed multiple analytics systems, or perform hybrid visibility and security functions from a single

platform. Whether you need to support a single appliance or orchestrate a complex multi-vendor toolchain, PacketHawk simplifies integration and ensures consistent, predictable traffic handling across all connected equipment.

Enhanced Operational Control, Visibility & Automation

The PacketHawk platform brings extensive management capabilities designed for modern operations teams. A user-friendly web interface, full CLI, and remote management options (SSH, Telnet, API) streamline configuration and monitoring tasks. With support for SNMPv2/v3, Syslog, NTP and granular access control lists, PacketHawk integrates easily into enterprise management frameworks. Built-in filtering capabilities at Layer 3 and Layer 4 enable selective forwarding and optimized tool utilization, while jumbo-frame support ensures complete visibility across high-performance environments. The result is a device that not only protects your inline tools, but also provides the operational clarity and control needed to manage them efficiently.

Technical Specifications

Key Features

Rack-mountable 2-slots modular chassis	1RU
Inline devices per module	2
Network and inline device port speeds	1/10/25/40/100Gbps
Supported packet sizes	64-9,000 Byte
Hot-swappable redundant power supply & fan modules	Yes
Inline device heartbeat health check: Unidirectional, Bidirectional	Yes
Supported heartbeat packet: ICMP, IPX, UDP (*TCP) and Firewall health check (*special feature)	Yes
Traffic auto-refresh statistics per port	Yes
Inline device port(s) operation modes	Service-Chain, High Availability, Load Balance, Bypass, Visibility
Network port(s) operation modes	Auto, Semi-Auto, Force Inline, Force Bypass
Visibility (In-line port TAP/mirror) mode support • Net A, Net B traffic any-to-any mapping • Combine Inline and TAP mode: “2 x Inline” or “1 x Inline + 1 x TAP” or “2 x TAP	Breakout, Aggregation
Redundant bypass operation in case of Bypass TAP failure	Active Bypass, Passive Bypass
LLD (Link Loss Detection) operation in case of network link failure	Yes
Link-Drop operation: Inline device failure or network link failure	Yes
Inline port L3/L4 filtering: include or exclude	Yes
Syslog (internal: logging & viewer, external – up to 3 Syslog servers)	Yes
SNMP v2/3, NTP	Yes
RADIUS, TACACS+, LDAP	Yes
2 x Management ports: serial console, Ethernet	Yes
Management access: Telnet, SSH, HTTP, HTTPS (enable/disable, Service Port Custom)	Yes
ACL (Access Control List) on management port (based on host & network address)	Yes
Port DDM (Digital Diagnostic Monitoring)	Yes
System health monitoring LED indicator: power, fan, port link/activity, operation mode	Yes
Configuration export/import	Yes
Mean Time between Failure (MTBF)	Min 12+ Years (105,000 Hours)

Connectivity

Link Speed (Options)	Network Ports	Inline Device Ports	Supported Transceiver
100G Ports	4	8	QSFP28
40G Ports	4	8	QSFP+
25G Ports	4	8	SFP28
10G Ports	4	8	SFP+
1G Ports	4	8	SFP
Management Interface	2	N/A	RJ45 / SFP+
Console Interface	1	N/A	RS323

Dimensions and Weight

Rack Mount	Yes
Rack Unit	1 RU
Height	1.73" (4.4 cm)
Width	17.32" (44 cm)
Depth	16.14" (41 cm)
Weight	12.13 lb (5.5 Kg)

Power and Cooling

Airflow	Front-to-Back
Fan Redundancy	4+0
Power Redundancy	1+1 AC/DC
Power Supplies	100 to 240 VAC, 2A, 50/60Hz
Max. Power Consumption	Chassis with 2 modules (SR4): Typical 100W, Max 130W Chassis with 2 modules (LR4): Typical 110W, Max 160W
Heat Dissipation	< 307 BTU/Hour

Operating Conditions

Operating Temperature	32°F–104°F (0°C–40°C)
Storage Temperature	-49°F–158°F (-40°C–70°C)
Operating Humidity	10% – 90%
Storage Humidity	10% - 90% Non-condensing

Certifications

Safety	CE
EMC	Class A FCC/CE
RoHS	CE

Ordering Information

Ordering Guide

Pick one of the options in each category below to provide to NEOX to quote the right product SKU:
Example: PacketFalcon Mini X with 25G Capture + 15TB Packet Storage + 3 Year Software Subscription & Silver Support

Product SKU	Description	Support Level	
		Silver	Gold
NX-PH-BS-CH	NEOX PacketHawk Inline-Bypass Switch and TAP Modular Chassis, 1U, with 2 Slots for TAP Modules. Does not include any NEOX hardware/software support or maintenance and must be added.	Default	Upgrade
NX-PH-BS-M10S	NEOX PacketHawk Inline-Bypass Switch and TAP 10G-SR Interface Module. Does not include any NEOX hardware/software support or maintenance or optics and must be added.	Default	Upgrade
NX-PH-BS-M10L	NEOX PacketHawk Inline-Bypass Switch and TAP 10G-LR Interface Module. Does not include any NEOX hardware/software support or maintenance or optics and must be added.	Default	Upgrade
NX-PH-BS-M40S	NEOX PacketHawk Inline-Bypass Switch and TAP 40G-SR Interface Module. Does not include any NEOX hardware/software support or maintenance or optics and must be added.	Default	Upgrade
NX-PH-BS-M40L	NEOX PacketHawk Inline-Bypass Switch and TAP 40G-LR Interface Module. Does not include any NEOX hardware/software support or maintenance or optics and must be added.	Default	Upgrade
NX-PH-BS-M100S	NEOX PacketHawk Inline-Bypass Switch and TAP 100G-SR Interface Module. Does not include any NEOX hardware/software support or maintenance or optics and must be added.	Default	Upgrade
NX-PH-BS-M100L	NEOX PacketHawk Inline-Bypass Switch and TAP 100G-LR Interface Module. Does not include any NEOX hardware/software support or maintenance or optics and must be added.	Default	Upgrade

Note: 3-Year Silver Support is default for all NEOX PacketHawk products and can be upgraded to Gold and available with 1-Year, 3-Year, or 5-Year option under each support level. Learn about NEOX Service and Support.
1 Year @ 15% of the product cost 3 Year @ 30% of the product cost 5 Year @ 45% of the product cost

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