NEOX NETWORKS
NEXT GENERATION NETWORK VISIBILITY

Data Sheet

NEOX**Packet**Dragon

High-Performance Threat IP-Blocker - blocks up to 10 million threat IPs

PacketDragon Highlights:

- **Purpose-Built IP Blocking Engine**: Utilizes a dedicated hardware-accelerated engine engineered specifically for ultra-fast, large-scale IP rule processing — optimized for perimeter defense use cases.
- **Consistent Line-Rate Performance**: Maintains full throughput even under extreme conditions (e.g. small-packet 64-byte UDP traffic), with no performance degradation. Designed to deliver maximum CPS (Connections Per Second) and Concurrent Connections (CC) without relying on session-based inspection.
- **Wire-Speed Filtering with Zero Latency**: Ensures real-time IP blocking at full line rate, even in multi-10Gbps network environments—delivering consistent protection without delay.
- **Rapid System Reboot**: Reboots in under 3 minutes, regardless of the size or complexity of active rule sets—enabling fast recovery and minimized downtime in critical environments.
- **Ultra-High Capacity Filtering**: Capable of enforcing up to 10 million IP block rules simultaneously, allowing for broad threat coverage without compromising system responsiveness.
- **Live Policy Enforcement**: All IP rule updates and policy changes are applied instantly and without disrupting active services, ensuring continuous operation and uninterrupted protection.

NEOX Solution

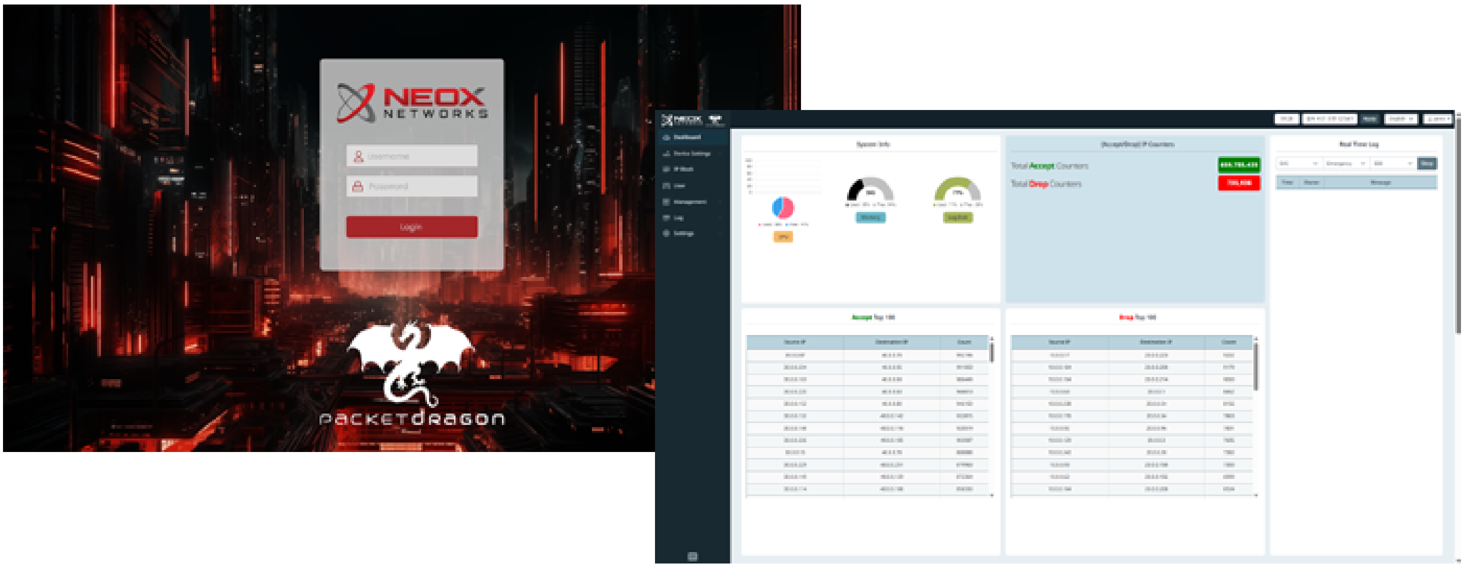
Traditional network firewalls are often overwhelmed by modern traffic volumes and complex rule sets. In many environments, they must manage hundreds of thousands of access control rules and track vast numbers of stateful sessions—pushing CPU, memory, and software limitations to their edge.

These bottlenecks not only degrade performance but also increase latency and introduce potential points of failure in security-critical infrastructures. Moreover, frequent policy updates—such as blocking newly identified malicious IPs—can take several minutes to apply, creating critical windows of vulnerability during which attackers can penetrate defenses or exfiltrate data undetected.

As digital infrastructures scale and threats become more dynamic and distributed, relying solely on traditional firewall technology introduces unacceptable risk. Perimeter defenses must be able to react instantly, scale horizontally, and operate without compromising performance.

PacketDragon by NEOX NETWORKS is engineered to meet these demands. It acts as a first-line defense system at the network edge—intercepting and filtering traffic at wire speed before it reaches internal firewalls, routers, or load balancers. Operating as a dedicated high-performance IP filtering appliance, PacketDragon continuously blocks malicious or unauthorized traffic in real time.

By eliminating superfluous and malicious traffic at the perimeter, PacketDragon not only enhances security posture but also offloads the processing burden from downstream security systems. This results in significantly improved firewall performance, faster response times, and increased network stability—allowing your core infrastructure to focus on what it does best: protecting business-critical applications and data.



Features

- **Automated Threat IP Blocking**

Instantly blocks IP addresses associated with botnets, phishing campaigns, malware distribution, and other threat categories

- **Low-Latency Real-Time Filtering**

Applies IP block rules in real-time at wire speed without introducing measurable impact on network performance or throughput.

- **Massive IP Blocking Capacity**

Designed for scale—supports up to 10 million concurrent IP block rules, far exceeding traditional firewall limitations.

- **Ultra-Fast Rule Deployment**

Imports up to 3 million threat IPs within 3 minutes, with new or updated policies enforced in under 1 second—ideal for rapid incident response.

- **Bulk IP Rule Import via CSV**

Simplifies large-scale policy updates by enabling the upload of extensive IP blocklists using standard CSV file formats.

- **Flexible IP Rule Format Support**

Accepts IP entries in single address, IP range, and CIDR/bitmask format—ensuring compatibility with diverse threat data sources.

- **Advanced Search & Filtering Functions**

Includes multi-criteria search options such as bulk IP lookup, expiration-date filtering, and user-specific IP rule tracking.

- **Hierarchical Management & Integration**

PacketDragon features an intuitive built-in web interface along with a centralized Manager system for streamlined multi-device control.

- **Advanced IP Policy Control**

Supports comprehensive IP policy enforcement through customizable whitelists and blacklists, along with compatibility for external Threat Intelligence databases to enhance detection and response capabilities.

- **RESTful API for Seamless Integration**

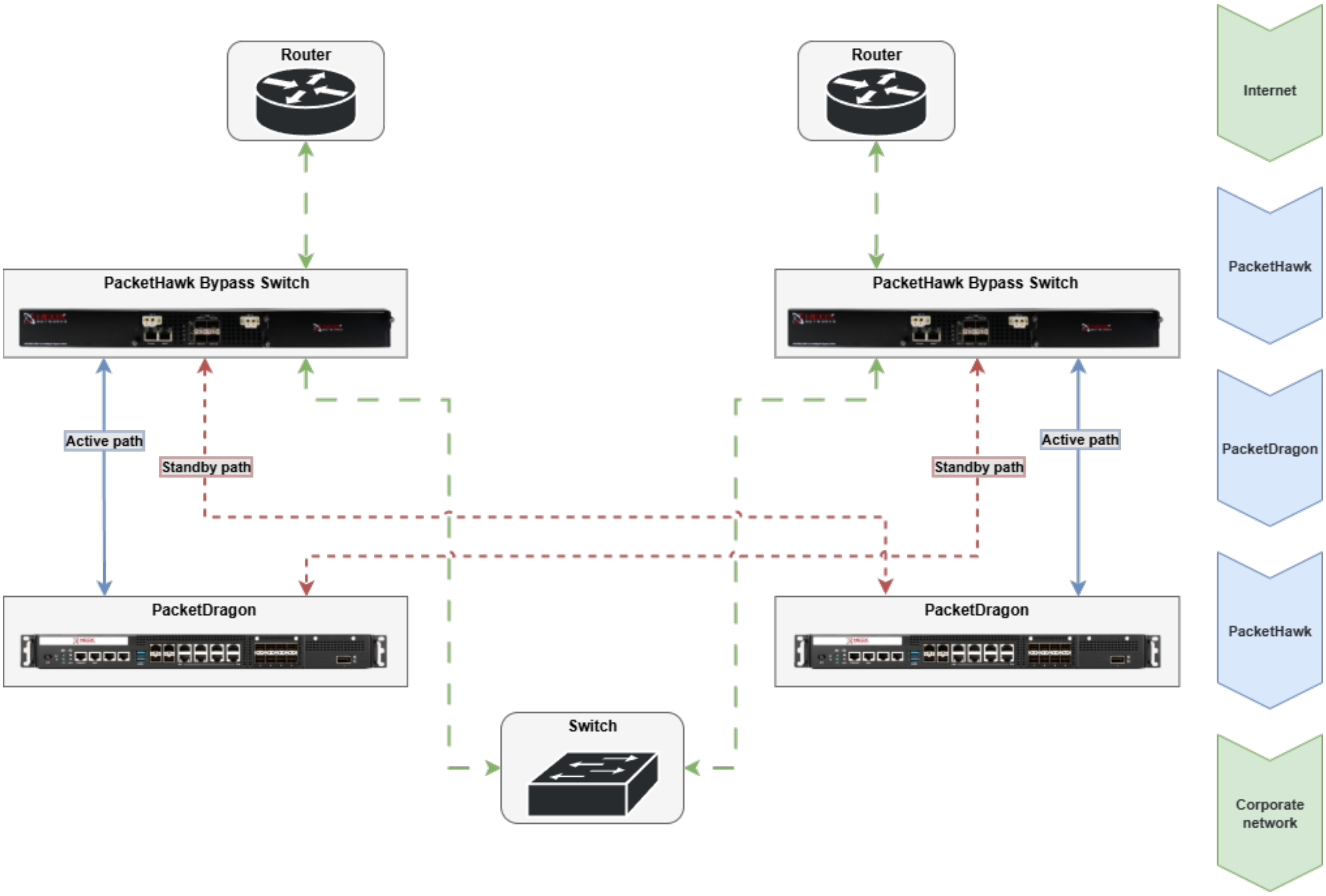
Provides a secure, standards-based API for easy integration with SIEM, SOAR, and other threat detection or automation platforms.

- **High Availability (HA) Architecture**

Supports full active-passive HA configuration with PacketHawk Bypass functionality, ensuring uninterrupted operation even during failover or maintenance scenarios.

HA Setup

PacketDragon supports high availability configurations through seamless integration with PacketHawk Bypass TAPs. In the event of a failure in the active unit, traffic is automatically redirected to a standby unit to ensure continuous protection. Should both units become unavailable, the system engages a fail-safe bypass mode, allowing traffic to flow uninterrupted and preserving critical network connectivity. This setup is ideal for mission-critical environments where uptime and reliability are essential.



Technical Specifications

Hardware

CPU	Intel® Xeon® D-2832NT, 8 Cores / 16 Threads @ 2.1Gh
Memory	16GB DDR4
Management	2x 10/100/1000Base-T RJ45
Internal HDD (for OS)	1TB
Removable ext. HDD (for logfiles)	2TB

Network

4x 10/100/1000Base-T RJ45	With integrated Bypass (2x Bypass Pairs)
4x 10/100/1000Base-T RJ45	No Bypass
4x 1G/10G SFP+	No Bypass

Power Supply

Power Type	AC Redundant CRPS, (Optional: DC Redundant CRPS)
Watts	300W
Input	AC: 100-240V~, 50-60Hz, (Optional: DC -48V, 800W)

Mechanical

Dimensions (HxWxD)	Weight	Consumed Rackspace
438 x 44 x 420 mm	8,23 kg	1RU
17.2" x 1.7" x 16.5"	18.14 lbs	1RU

Environmental

Operating Temperature	0 ~ 40 °C (32 ~ 104 °F)
Non-operating Temperature	-40 ~ 70 °C (-40 ~ 158 °F), 60 °C@95% Non-Condensing Humidity
Vibration Resistance (Operation)	5-500 Hz, 0.3 Grms, 3 axes, 1 hr/per axis
Shock Protection (Operation)	10 G, 11 ms

Ordering Information

SKU	Description
NX-PD-S	1G/10G Threat IP Blocker. Includes 8x 10/100/1000Base-T RJ45 (including 4x Bypass pairs) and 4x 1G/10G SFP+ interfaces. Blocks up to 10 million Threat IPs, ultra-fast sync and commit of Threat IP database. **Maximum throughput 100Mbit/s**
NX-PD-M	1G/10G Threat IP Blocker. Includes 8x 10/100/1000Base-T RJ45 (including 4x Bypass pairs) and 4x 1G/10G SFP+ interfaces. Blocks up to 10 million Threat IPs, ultra-fast sync and commit of Threat IP database. **Maximum throughput 1Gbit/s**
NX-PD-L	1G/10G Threat IP Blocker. Includes 8x 10/100/1000Base-T RJ45 (including 4x Bypass pairs) and 4x 1G/10G SFP+ interfaces. Blocks up to 10 million Threat IPs, ultra-fast sync and commit of Threat IP database. Operates at full line rate. **Maximum throughput 10Gbit/s.**

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