Owl Protocol Filtering Diodes

Eliminate protocol blind spots left open by simple diodes & firewalls

Summary

Key Features & Benefits

→ Hardware-enforced one-way transfer with FPGA protocol break

→ Deep inspection blocks out-of-policy, or malicious content in hardware

→ Eases accreditation against HTN and Zero Trust-aligned U.S. Government requirements

→ Owl PFD suite scales from 1 Gbps single-PCIe card to 100 Gbps enterprise platforms

Challenge: Achieving True Assurance in One-Way Data Flows

Defense and critical infrastructure teams must move mission, log, and sensor data from OT or other sensitive networks into IT or lower-side networks for analysis and sharing—without exposing command-and-control systems or internal services to attack. Traditional data diodes reliably enforce unidirectional flow via hardware but still depend on mutable software to determine what gets sent across the boundary and treating most traffic as opaque, trusting anything that looks like the right protocol. That software-centric control limits assurance that the traffic which actually leaves the secure side fully matches the sender's intent and is free of corrupted, spoofed, or weaponized payloads hiding inside otherwise "approved" protocols.

Solution: Protocol Filtering Diodes, Because "One-Way" Alone Isn't Enough

A **Protocol Filtering Diode (PFD)**, like Owl Talon One and Owl Talon Torrent, combines the reliable hardware-enforced one-way transfer of a simple diode with an additional layer of FPGA-based protocol break, validation, and reconstruction, so only specific, mission-required data flows are permitted while malformed, unexpected, or malicious traffic is blocked at line rate. This multilayer control aligns with U.S. Government High Threat Network mandates, Raise-the-Bar style expectations, and Zero Trust guidance for the most sensitive domains.

Use Case: One-Way Analytic Feeds That Don't Expose Control Systems

An agency/organization needs to move high-value telemetry, operational logs, and security events from a classified or OT network into an HTN, IT, or cloud analytics environment without exposing control systems to inbound risk. Deploying an Owl Protocol Filtering Diode enables continuous one-way streaming with hardware-enforced protocol inspection, so only intended data crosses the boundary while hidden threats remain trapped on the untrusted side.

How Owl Protocol Filtering Diodes Work
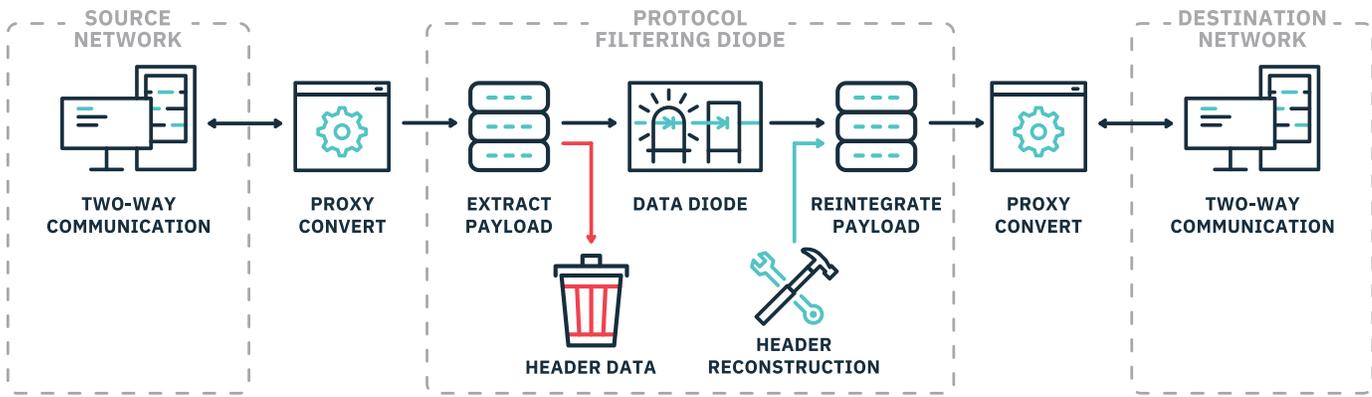
A PFD guarantees data moves only one way between networks, creating a physical barrier to inbound attacks or data theft. Owl pairs send/receive modules with proxy hosts that translate two-way protocols into one-way flows and reconstitute them on the destination side. Inside the diode, FPGAs enforce a protocol break, normalize messages, and ensure that only data payloads are allowed to transit the diode. Only valid, policy-compliant traffic is re-created on the receive side; malformed, out-of-policy, or suspicious content is discarded by hardware. The result is physical one-way separation with deep protocol inspection that firewalls and software filters alone cannot match.

Owl Protocol Filtering Diodes

Owl Talon One

Compact, PCIe-based PFD that delivers up to 1 Gbps of hardware enforced one way transfer with FPGA protocol filtering, ideal for securing individual servers, gateways, and edge platforms without adding significant latency or complexity.

Owl Talon Torrent

Next-gen high-performance PFD platform that scales up to 100 Gbps, combining FPGA protocol filtering, ideal for low-latency, high-speed and high-volume mission, OT, AI/ML, etc. data.

Owl Cyber Defense Solutions, LLC, headquartered in Columbia, MD, leads the industry in data diode and cross-domain network cybersecurity solutions for faster, safer and smarter decision making. We create solutions tailored for high-risk sectors including the military, government and critical infrastructure. Our advanced technologies enable secure, near-instantaneous collaboration, bridging network barriers to protect critical missions. With a focus on scalability and interoperability, Owl ensures that organizations can maintain secure, reliable, and compliant communication channels against evolving cyber threats.

For more information on Owl, or to schedule a demo, visit **www.owlcyberdefense.com.**