

What's the Difference *Between Firewalls & Data Diodes?*



VS



When evaluating data diodes, the first point of comparison is often a software firewall. Firewalls are ubiquitous, and generally seen as “checking the box” for most network security requirements, so they make for a natural touchstone for users unfamiliar with other network security technologies like data diodes. However, the comparison doesn’t usually extend beyond the shared trait that they both secure networks. So how do data diodes actually compare to firewalls?

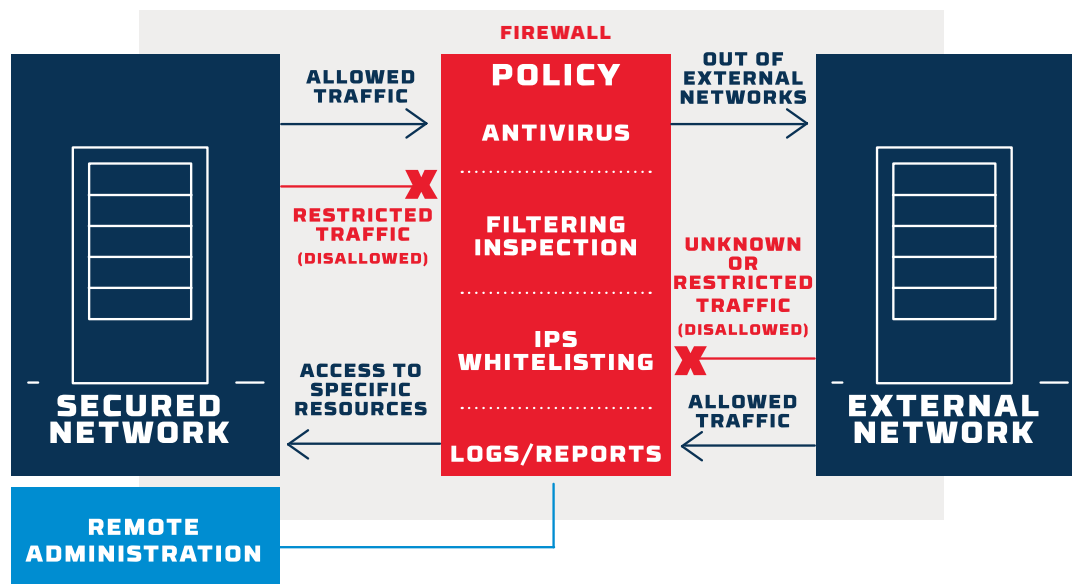
Background

As you may know, the word “firewall” actually comes from a physical barrier that is installed in buildings and vehicles to impede the spread of literal fire from one room or section to the next. These firewalls have Time/Temperature fire resistance ratings that are measured in hours, meaning the hours they will hold up at a certain temperature before they inevitably fail. Neither physical nor software firewalls are designed to hold up forever. Of course, if the fire or threat is stopped before they fail, they will have done their job in protecting the other sections of the structure or network.

Data diodes were designed on uncompromising technology intended to stop all unauthorized access to nuclear weapons systems. They enforce a physical separation or “air-gap” between network segments that is enforced by the laws of physics, which are immutable and absolute – data will never be able to flow in the opposite direction, and therefore attackers will never be able to access networks through a data diode. There’s no hourly rating, no number of brute-force attempts that will overcome them, and their failure state is equally as secure – no connection at all.

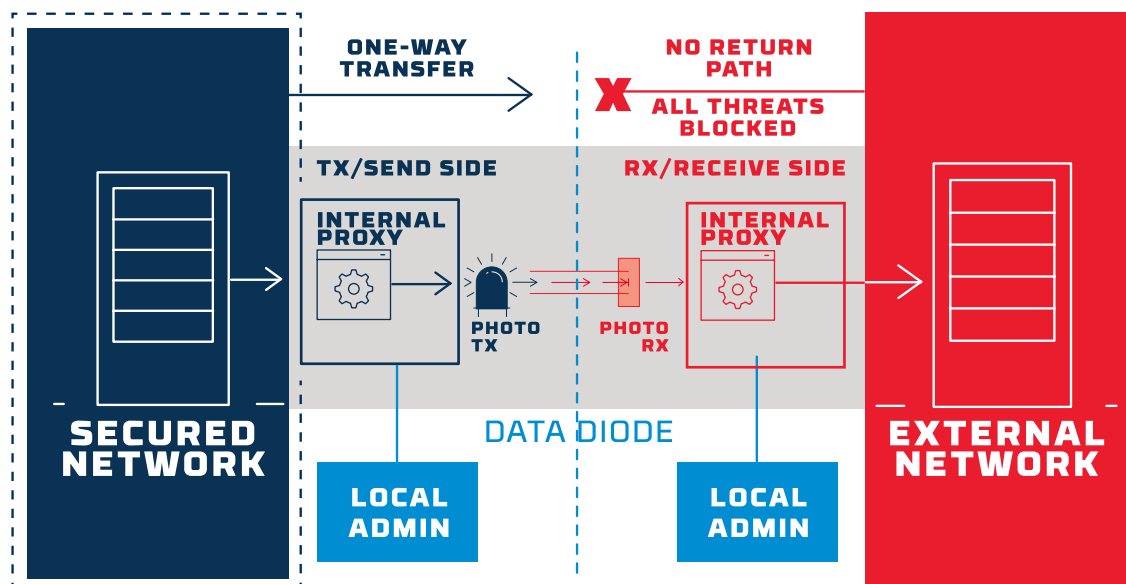
Firewalls

Firewalls are enforced by flexible code and configuration that, like the physical firewall, is effective at slowing threats, but not necessarily at stopping them. In many cases, especially with additional inspection capabilities, the software barrier provided by a firewall is enough to stop minor threats, much as a physical firewall would hold back a small fire. However, modern cyber threats are more akin to taking a flamethrower to every wall of the house simultaneously, with complex, coordinated attacks from multiple angles all at once. Firewalls were never designed to completely stop these kinds of threats, nor should anyone expect them to.



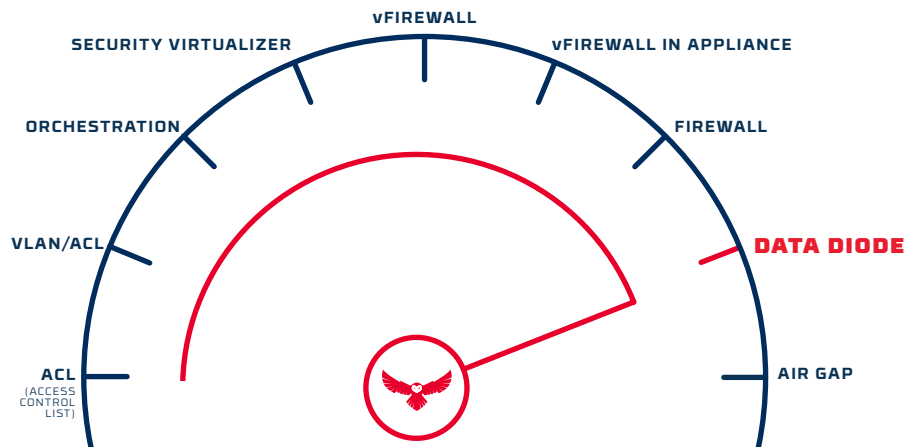
Data Diodes

In contrast, hardware-enforced data diodes were designed to physically separate networks from external threats via an effective air-gap between them. Their lack of routable, configurable connectivity reduces their flexibility to a degree, but it also adds to their security profile. Sophisticated threats can use coordinated, persistent tactics to overcome advanced RBAC, passwords, multi-factor authentication, and even biometrics, but jumping the physical gap in a data diode with electronic tools remains impossible. Data diodes were intended to secure that which must never be compromised, and they remain one of the strongest cybersecurity tools available today.



Security

There is really no debate over whether data diodes are more secure than software firewalls – they are. Owl data diodes are physically enforced with a hardware-based security mechanism and provide 100% confidentiality and segmentation between networks, while firewalls are enforced by configurable code and policy. Data diodes are not vulnerable to the software bugs, zero-day exploits, or misconfiguration that plague firewall solutions. Hardware-enforced data diodes also provide something firewalls and other software-based security cannot: protection from the unknown. They do not need regular patching or maintenance to stay secure, and the enforcement mechanism never becomes less effective over time.



Why Hardware-Based Security



Software

- » Configuration-enforced
- » Zero-day exploits
- » Malware / Ransomware
- » Heavy ongoing management



Hardware

- » Physics-enforced
- » No zero-day exploits
- » Invulnerable to malware
- » Little to no ongoing management

Virtual vs. Physical Segmentation

Like a physical firewall, software firewalls do not provide a true separation between sections or network segments, but rather act as a virtual impediment to potential threats. Fire, or in this case, cyber threats, will eventually break through given enough time and severity. They both also have holes or pathways built in to allow certain things through. If you know where the holes are, you could break through even faster.



Firewall

Designed to withstand for a while, but will fail eventually





Data Diode

Unless someone physically brings the fire to the other side of the air gap, it will never spread to the other segment

Capabilities

Rather than security, the question has been whether data diodes can meet all of the same sophisticated communication capabilities which have made firewalls the traditional network security solution. Owl has invested decades of engineering and intelligent design into the communication facilitation software layer built on top of its patented hardware platform. This sophisticated layer of connectivity, compatibility, and functionality is really what sets Owl data diodes above other unidirectional networking products and finally provides a solution that has both far superior security compared to firewalls, and comparable communication capabilities.

|  FIREWALLS | VS. |  OWL DATA DIODES | COMPARISON |
|---|------------------------------------|---|---|
| Software-Enforced (Configured) | Enforcement Mechanism | Hardware-Enforced (Physical) | Software-based policy in firewalls is configurable and corruptible with known and unknown exploits. Owl data diode components and circuitry cannot be altered by malware or code to enable unauthorized access or open an attack vector. |
| One-Way or Two-Way | Connection | One-Way | While firewalls can be configured to operate in only one direction, they are inherently two-way. Data diodes can provide a two-way capability with a parallel connection in the opposite direction. |
| Varies Widely Based on # of Rules | Latency | Very Low to Moderate | Software security controls (rules) in firewalls inherently add overhead to the transfer – More Rules = More Lag. Owl data diodes can be virtually real-time without affecting air-gap level security. |
| Very High | Reliability & Assurance | Very High | As “pass-through” devices, firewalls are highly reliable in data transfer accuracy. Owl data diodes utilize packetized transfer with sequenced headers for near absolute data assurance and integrity. |
| Masking with Proxies | Network IP Information Security | Protocol Break | While software proxies in firewalls can help to mask network information, the protocol break in Owl data diodes makes network information completely invisible to each side of the device. Any probing or pinging of data diode protected networks is impossible through the diode. |
| Network-Based Single Point | Administration | Local Dual-Authenticated | Network-based firewall administration is often only as strong as a single password. Owl data diodes are locally administrated on each side of the device, requiring both sides to agree for the system operate. |
| Routable | Routability | Deterministic | Firewalls protocols can be re-routed to any other destination. Owl data diode transfers are designed to be deterministic, configured in advance by local administration on both sides of the device. |
| Heavy Ongoing Requirements | Maintenance | Little to None Required | Firewalls require specialized expertise to configure and heavy ongoing maintenance/patching. Owl data diodes arrive pre-configured, ready to install, and operate securely with little to no maintenance. |

Summary

Cutting edge data diode technology from Owl has bridged the capability gap with firewalls, enabling air-gap level hardware-enforced security with full-featured solutions with a lower total cost of ownership. Owl data diodes are far simpler to install and maintain than firewalls, are available in a wide range of options, including two-way solutions, and are available at a competitive price point. While firewalls will likely always be a staple of network security to “check the box,” Owl data diodes go well beyond to enable reliable, undefeated security today and into the future.



Owl Cyber Defense Solutions, LLC leads the world in data diode and cross domain network cybersecurity. With a constant focus on customers in the military, government, critical infrastructure, and commercial communities, Owl develops market-first, one-way data transfer products to meet a variety of operational needs, from entry level to enterprise.

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