



DATA DIODES **vs.** UNIDIRECTIONAL GATEWAYS

**The Architect's Guide to
Modern OT Security**



waterfall

Data Diodes vs. Unidirectional Gateways

The Architect's Guide to Modern OT Security

Introduction: The Need for Secure Data Transfer in a Digital World

In today's interconnected industrial landscape, the security of operational technology (OT) networks and systems has become paramount. High-profile attacks like Stuxnet, Triton, and Colonial Pipeline have demonstrated that when bi-directional communication channels are compromised, the consequences can be very serious.

The fundamental security challenge lies in the nature of bi-directional data transfer itself. Every channel that allows information to flow can also allow attack information to flow. All incoming information flows are potential attack vectors. This reality has driven organizations to seek solutions that can physically enforce one-way data transfer.

Two technologies have emerged as leading solutions: **data diodes** and **unidirectional gateways**. While data diodes have served as the traditional approach in military and government facilities for decades, unidirectional gateways represent the evolution of this technology – offering the same physical security guarantees while incorporating advanced industrial connectivity to simplify deployment of the technology in complex industrial networks.

In this guide, we'll explore why organizations seeking to secure their critical infrastructure should look beyond basic data diodes to more comprehensive unidirectional gateway solutions, examining how these technologies differ and why those differences matter for both security and operational efficiency.

Chapter 1: Data Diodes – The Foundation of One-Way Communication

The concept of a data diode is straightforward: information can flow in only one direction, making it impossible for any data – malicious or otherwise – to travel in the reverse direction. This one-way transfer is sometimes enforced at the physical layer, typically using fiber optic components where a transmitter is present on one side and only a receiver on the other.

The technology traces its origins to high-security military and government facilities, where the need to maintain absolute separation between networks while still allowing some data transfer was paramount. Some data diodes achieve this unidirectional flow through hardware mechanisms such as cutting wires in an effort to achieve unidirectionality. (Note: this practice is dangerous.)

Where the Rubber Meets the Road

While data diodes are often considered a secure solution for isolating critical networks, they come with significant challenges that can undermine their effectiveness:

Inconsistent Hardware

- **Ethernet Connections:** Single-pair, twisted-pair ethernet connections may appear to enforce one-way communication, but modern ethernet hardware negotiates half-duplex bi-directional communications when it detects the presence of only a single pair in the connecting cable.
- **One-Way Electrical Signaling:** Data diodes that rely on only electrical isolation face a fundamental physics challenge: electrical circuits are inherently circular in nature, making true unidirectional flow physically impossible to guarantee.
- **Optical Isolation:** Even optical data diodes, while more secure than their electrical counterparts, can present verification challenges when transmit and receive optical and electronic circuitry share the same circuit board, as internal electrical routing could potentially create hidden return channels.

Limited Software Support

- **Limited Functionality:** Many data diodes are basic network appliances that only transmit UDP/IP and other broadcast packets, a format used by almost no common communications protocols. This means custom software is generally required for useful data transfer.
- **Primitive Software:** The software that accompanies data diodes is often minimal, with some models lacking software entirely, requiring custom solutions to integrate with modern IT and OT systems.
- **Basic TCP Proxying:** While some data diodes offer basic TCP proxying or simple file transfers, these capabilities are often insufficient for complex data transfer needs, as most TCP-based protocols rely on two-way, query-response communication.
- **Limited Integration:** Due to poor software support, data diodes struggle to integrate with modern IT and OT ecosystems, including standard operating systems and applications. This complicates their use in most environments.

With these challenges in mind, customers must carefully assess whether the data diode offerings they are considering are truly unidirectional. Not all products marketed as data diodes provide the required level of security, and customers must verify that the solution adheres to strict unidirectional communication principles.



What About Unidirectional Firewalls?

Practitioners who are new to the concept of unidirectional communications sometimes mistakenly believe they can create the effect of a true data diode with a “unidirectional firewall.” While it is generally possible to configure a firewall to initiate TCP connections from only one side or the other, once initiated, all TCP connections are bi-directional. Once a firewall allows a connection, data can flow in

both directions — a direct contradiction to the fundamental idea of unidirectional communication.

The concept of a “unidirectional firewall” is a misnomer, and any attempt to use firewalls for this purpose will fall short of delivering the robust, one-way protection that true data diodes and unidirectional gateways provide.

Chapter 2: Unidirectional Gateways – The Next Generation of Secure Data Transfer

As the demand for more secure and adaptable data transfer solutions has grown, unidirectional gateways (UGWs) have emerged as a next-generation evolution of data diodes. While data diodes were designed to enforce one-way data transfer, they were often limited by their rigid functionality and lack of integration with modern systems.


Unidirectional gateways, on the other hand, are engineered to overcome these challenges, offering a more flexible and versatile approach to secure data transfer.

What is a Unidirectional Gateway?

In the US National Institute of Standards and Technology SP 800-82 (r3) standard, a unidirectional gateway is defined as a combination of hardware and software. The hardware enforces one-way data transfer between networks. The software replicates servers and emulates devices. Together, the hardware and software enable safe IT/OT integration.

Unlike traditional data diodes, unidirectional gateways provide simple IT/OT integration, replicating servers and data to IT networks to enable predictive maintenance, real-time inventory management and other business automation, without risk to operations.

Caution: just like data diode vendors, some unidirectional gateway vendors claim more than they deliver:



“Unidirectional gateways are a combination of hardware and software. The hardware permits data to flow from one network to another but is physically unable to send any information at all back to the source network. The software replicates databases and emulates protocol servers and devices.”

- Some vendors call all-software solutions unidirectional gateways, when in fact the NIST definition demands hardware-enforced unidirectionality.
- Some unidirectional gateway vendors use electrical isolation rather than optical isolation, or optical isolation in a complex circuit board, both of which practices make verification of true unidirectionality difficult or impossible.
- Some vendors call all-hardware solutions unidirectional gateways, without any ability to replicate servers or emulate devices.

Again, customers must carefully assess whether the unidirectional gateway offerings they are considering are truly unidirectional and are truly unidirectional gateways. Not all products marketed as unidirectional gateways provide hardware-enforced security nor software-enabled ease of integration.

Benefits of Unidirectional Gateways over Data Diodes

- **Real-Time Server Replication:** Unidirectional gateways enable replication of databases, servers, and devices across networks, ensuring that reliable and efficient physical operations remain intact while providing users and applications with natural interaction with replica servers in IT environments.
- **Device Emulation:** UGWs generally support some degree of device emulation for devices using industrial protocols, simplifying integration with IT-based historians and other consumers of device data.

How UGWs Replicate Servers and Emulate Devices

Unidirectional gateway software replicates servers by:

- Logging into source servers, such as a historian or SQL Server, on the OT network and asking those servers for all data, or all new data – new since the last time the software asked.
- The software pushes that data through the one-way hardware to the gateway software on the receiving network.
- There, the gateway software logs into an identical receiving server, such as a historian or SQL Server, and updates that server with the data received from the one-way hardware.

In this way, the unidirectional software maintains a real-time copy of the source OT server on the destination IT network. IT users and applications log into and use the IT replica server normally.







Similarly, unidirectional gateway software emulates devices by:

- Logging into source devices, such as Modbus PLCs or OPC servers, on the OT network and asking those devices for all their data – all tags/registers and their values.
- The software pushes that device state snapshot through the one-way hardware to the gateway software on the receiving network.
- There, the gateway software holds the snapshot and emulates the original device, responding to IT queries the same way as the original OT device would have.

For example, when emulating Modbus PLC's or OPC servers, the unidirectional gateway's receiving software implements a compliant Modbus TCP slave or OPC server, responding to Modbus or OPC queries the same way as the original device would have, respectively.

These replicas are the defining difference between data diodes and unidirectional gateways, according to the NIST definition. Replicating servers and emulating devices to the IT network means that neither IT nor OT applications need to be aware of the unidirectional data transfer. In most cases, the unidirectional gateway manifests as an application or device client on the OT network, and as an application client or device emulator on the IT network. All IT and OT devices, users and applications interact with the IT replicas normally and bi-directionally.

NIST Unidirectional Gateway vs. Data Diode

	Data Diode	Unidirectional Gateway
One-Way Hardware	 Yes	 Yes
Files & Syslog Replication	 Varies by vendor	 Generally, yes
Industrial Server & Device Replications	 Generally, not	 Generally, yes, but which servers and devices varies by vendor

Chapter 3: How Waterfall UGWs Put You on the Right Track

In the unidirectional arena, Waterfall's Unidirectional Security Gateway products are the gold standard for OT network protection. What truly distinguishes Waterfall's UGWs is their unparalleled versatility and comprehensive approach to industrial network security.

Designed for maximum clarity in unidirectional communication, Waterfall's UGWs are built with superior hardware and software that runs

on Waterfall's own purpose-designed proprietary operating system and offered as a comprehensive, off-the-shelf solution that integrates seamlessly with existing technology stacks. This integration delivers exceptional performance, with throughput capabilities ranging from 1Gbps to 10Gbps, adapting to any network's demands, and with no need to install any unidirectional or other software on other OT or IT hosts to enable the functionality of the gateway.



Waterfall's Unidirectional Gateway is the gold standard for OT network protection.

What truly distinguishes Waterfall's UGWs is their unparalleled versatility and comprehensive approach to industrial network security.

Waterfall's Unidirectional Gateway:



Hardware is designed for easily-verified unidirectionality



Software and hardware is designed and built by Waterfall



Software runs in the gateway appliance – not on other hosts



The widest available unidirectional connector library



Comprehensive, easy to use web-based user interface



Standard 1Gbps throughput, 10Gbps optional



High availability options, if needed

At the heart of Waterfall's superiority lies its extensive connector library – the most comprehensive in the industry.

While other unidirectional gateways offer basic connectivity options, Waterfall's solution seamlessly integrates with virtually any OT network configuration. This vast ecosystem of connectors, battle-proven across thousands of deployments worldwide, enables unprecedented enterprise visibility into physical operations, while maintaining absolute security.

A Waterfall hardware-enforced Unidirectional Security Gateway for OT networks creates an

impenetrable shield against remote attacks, malware, DOS attacks, ransomware, and remote human error.

Waterfall's Unidirectional Gateways also uniquely enable OT networks to gain access to cloud connectivity for advanced automation and analytics without compromising security, protecting operations from the growing threat of ransomware while maintaining full access to cloud-based capabilities. The intuitive web-based interface further sets Waterfall apart, offering straightforward configuration, management, and troubleshooting tools that reduce operational complexity.

Chapter 4: Real-World Applications of Waterfall's Unidirectional Gateways

While data diodes have long been the traditional choice for creating physical network segmentation, unidirectional gateways have emerged as an easier-to-deploy alternative, and Waterfall's Unidirectional Security Gateways have emerged as the market leaders for features,

connectors, ease of use, and clear unidirectional engineering.

In this chapter we'll explore how Waterfall's Unidirectional Gateways have been successfully deployed to protect vital assets in diverse sectors.

Case Study 1: An Oil & Gas Refinery in the UAE

An oil & gas refinery in Dubai, UAE, needed to maintain secure access to plant data while facing increased cyber threats to their industrial control systems (ICS). While their legacy Wonderware Historian (AVEVA System Platform) was out of support, Waterfall's AVEVA System Platform connector product supports a wide range of WW / AVEVA product versions, including the customer's version.

Thus, the refinery turned to Waterfall's Unidirectional Gateway solution as it offered them native integration with Wonderware AVEVA System Platform and provided a continuously updated replica of the Historian server on their commercial IT network. This ensured that the actual production server remained isolated and that data flowed one-way (from OT to IT).

The results:

100% secure OT network:

unbreachable by online cyber threats from external networks.

Real-time data visibility:

full and secure access to real-time production data.

Scalability: The refinery's success lead them to order additional Waterfall Unidirectional Gateways for further applications, without the need to continuously pay to maintain custom code in perpetuity.

Legacy systems unaltered:

no modifications were required to the customer's legacy systems.

Case Study 2: A European Pharmaceutical Manufacturer

A leading pharmaceutical manufacturer in Europe was looking to provide enterprise-wide access to real-time data while protecting manufacturing operations and intellectual property from cyberattacks.

Knowing that modern industrial attacks routinely defeat firewalls, encryption, anti-virus systems, security updates, intrusion detection systems and other software protections, the customer was aware that protecting pharmaceutical critical assets with such software security measures was not enough.

A Waterfall Unidirectional Gateway was installed as the sole connection between the OT network and any external network, replicating the control system historian database to an enterprise historian. Unidirectional Gateway hardware makes online attacks on ICS networks from external networks physically impossible. To protect product recipes and other trade secrets, the Gateway was configured to replicate only those historian tags that were safe to share with the enterprise network. Tags containing recipes, formulas and other intellectual property remained exclusively in the control system historian.

The results:

100% security:

production processes and intellectual property are now physically protected from any attacks originating on external networks.

100% visibility:

enterprise users and applications have access to all permitted real-time data via the enterprise historian.

100% compliance:

Waterfall's Unidirectional Gateways simplify compliance with global regulations, standards and best practice guidance for industrial cybersecurity.

Conclusion: Making the Right Choice

Protecting critical industrial networks requires careful consideration of security solutions. While data diodes have served as a traditional approach to network segmentation, unidirectional gateways have emerged as the more sophisticated and practical choice for protecting modern OT environments.

Unlike data diodes, which often require extensive custom engineering and ongoing maintenance, Waterfall's Unidirectional Security Gateways offer seamless integration with existing systems. They provide robust protocol support, comprehensive monitoring capabilities, and simplified user interfaces and management interfaces – all while maintaining the same level of security as the best data diodes.

The best data diode and unidirectional gateway technologies both offer powerful solutions depending on the use case. Waterfall's Unidirectional Security Gateways also offer industry-leading unidirectional security and throughput and are far superior when it comes to important considerations such as ease of auditing, ease of integration, management, and providing remote access to industrial data.

Waterfall's Unidirectional Gateway products stand alone as the only solution that offers all these advantages as an off-the-shelf, no-custom-engineering-required platform.

**Want a free consultation about your security needs with one of our experts?
Contact us on info@waterfall-security.com**

Waterfall's products are covered by U.S. Patents 7,649,452, 8,223,205, and by other pending patent applications in the US and other countries. "Waterfall", the Waterfall Logo, "Stronger than Firewalls", "In Logs We Trust", "Unidirectional CloudConnect", and "CloudConnect, and "One Way to Connect" are trademarks of Waterfall Security Solutions Ltd. All other trademarks mentioned above are the property of their respective owners. Waterfall Security reserves the right to change the content at any time without notice. Waterfall Security makes no commitment to update content and assumes no responsibility for any mistakes in this document. Copyright © 2022, Waterfall Security Solutions Ltd. All Rights Reserved. www.waterfall-security.com