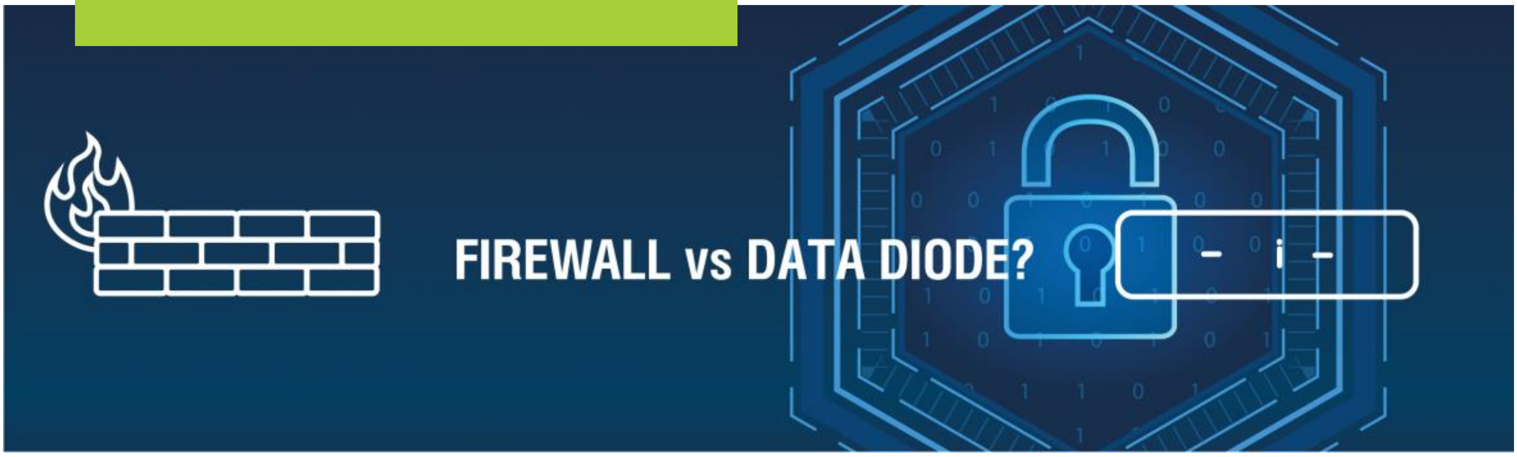
INFORMATION SECURITY



Firewall vs Data Diode: what’s the difference?

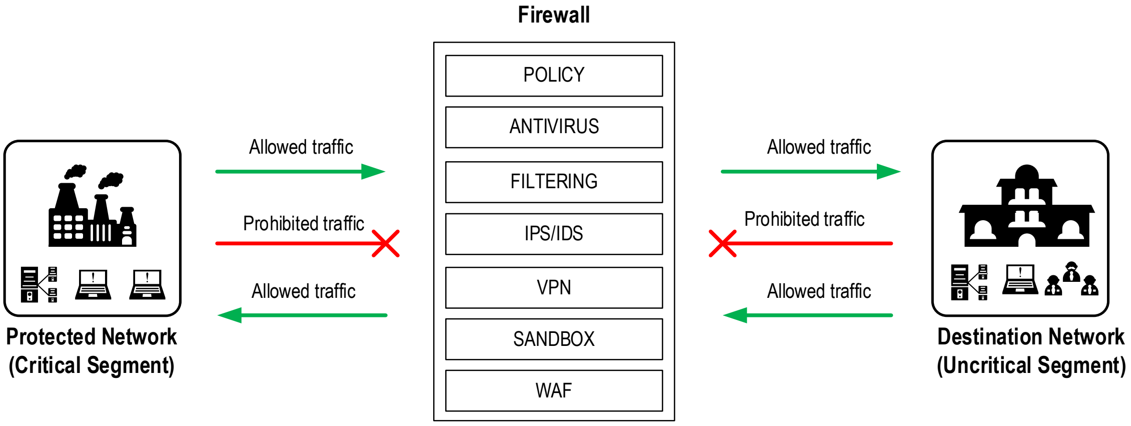
When evaluating the effectiveness of uni-directional data transmission devices of the «Data Diode» class, they are often compared with the widely used class of Firewall devices. Although both classes are designed to protect networks, they are fundamentally different in terms of both technology and application.

The term Firewall comes from the name of the physical barrier that is installed in buildings to prevent the spread of fire from one part to another. These barriers have fire resistance ratings in time and temperature that they will withstand before they inevitably fail. Neither the physical barrier nor the Firewall software is designed for long-term operation/protection under any conditions. Firewall software to protect against penetration into the protected segment of the network is also designed to deter certain types of attacks on the information infrastructure.

The «Data Diode» uni-directional data transmission devices were originally designed to ensure unauthorized access to nuclear weapons control systems. The introduction of devices of one-way data transmission provides physical separation or actually «air gap» between the network segments, while the possibility of data transmission in only one direction remains. Devices of «Data Diode» class isolate network segments, eliminating the possibility of physical backlinking and providing guaranteed protection based on physical principles.

«Data Diode» provides guaranteed segmentation of networks at physical level and due to applied physical principles of electroplating and optical isolation of network segments. Such devices are not subject to software errors, zero-day exploits, or configuration errors. The built-in physical security mechanism of this class of devices does not become less effective over time. Unidirectional data transmission devices are the basis for the construction of an integrated security and safety system for Critical Infrastructure (CI) facilities. They provide hardware protection for industrial and fuel and energy networks. Reference architecture is a set of solutions in which the integration of technological and corporate network is realized only through one-way gateways, not through firewalls. This architecture completely eliminates the possibility of remote access to a critical object.

Firewall



Modern Firewall provide flexible configuration, are effective for slowing down penetration into the protected segment and for limited prevention of certain classes of threats and attacks, but do not guarantee 100% penetration protection.

In practice, there is a large variety of attacks that allow you to overcome the protective mechanisms of the Firewall, and success is determined by the fundamental possibility of two-way interaction of segments.

For example:

- Phishing (sending specially formed emails, manipulating employees to obtain their credentials, downloading malware);
- Hacking of web applications (exploitation of vulnerabilities to gain unauthorized access to perimeter of protected networks);
- Compromise domain controller (attack on key nodes of IT infrastructure, creation of fake accounts with privileged access);
- Attack through client software (compromise at the level of client industrial software, including installed at third parties, in order to obtain unauthorized access to nodes of technological networks).

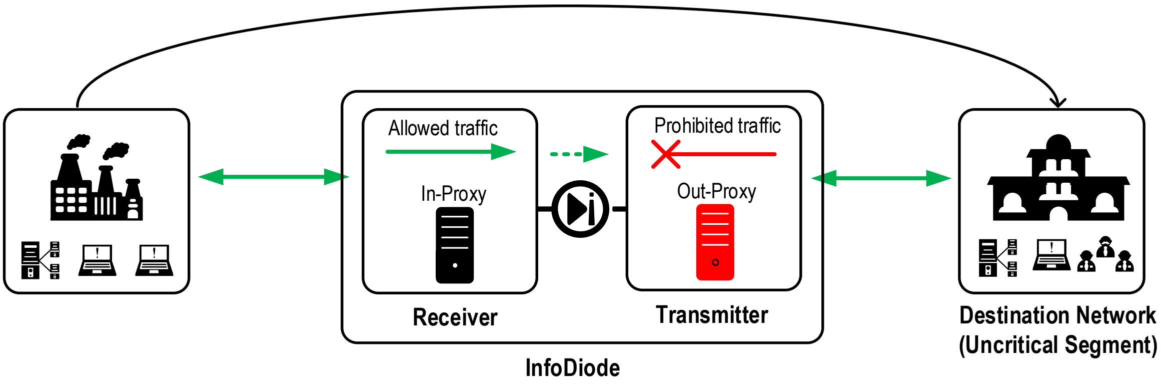
Modern and well-planned computer attacks of the above categories relatively easily overcome the means of protection in the form of software, including Firewall, cryptographic protection systems, intrusion detection systems, antiviruses, etc.

In addition, there is always the possibility of errors in the configuration of software solutions of the Firewall class by the maintenance personnel and technical support services, in this case, banal negligence can lead to huge damage.

Several years ago, Firewall was in fact the only available technology capable of protecting the most critical network objects and separating them from open networks. When, in practice, it was necessary to obtain information from the protected facility in real time, the only solution was to provide direct network connectivity, to use firewalls and similar security features and to believe in the reliability of the measures taken. However, modern computer attacks demonstrate the ability to systematically and effectively bypass many security tools, including firewalls.

CI objects can segment their technology networks using Firewall, ensuring their application in networks of the same level of trust and criticality. At the same time, interfaces with open and corporate networks are protected by Data Diode class unidirectional devices. Thus, by gaining layer-by-layer protection of the technological network, CI objects significantly improve their security, eliminating the possibility of computer attacks and the spread of viral activity from open networks and the Internet.

Unidirectional data gateway - Data Diode



The unidirectional data transmission devices — data diodes have been developed to ensure physical network separation, with the information transmission channel retained. As already mentioned above, the most complex attacks may utilize coherent tactics to break down the current security systems: password mining, hacking the multi-factor authentication and even social engineering methods. However, overcoming the «physical gap» in the data diode with the help of «information tools» remains impossible. The Data Diode-class devices have been designed to protect the most important and critical segments of information infrastructures and technological/military infrastructures. They remain one of the most effective tools for information security.

Devices for unidirectional data transfer ensure secure integration between technological and corporate networks and allow for continuous monitoring of the technological network operation out of other segments, including incident response capabilities from SOC and NOC. The use of unidirectional gateways to address information security challenges provides end-users with transparency of the required data without causing any significant network delays in accessing information. This eliminates the vulnerabilities that typically accompany building an architecture based on firewalls and security software solutions.

AMT GROUP Solution

AMT GROUP offers devices for unidirectional data transmission within its **InfoDiode** product line. The devices in this product line replace firewalls or add to Firewall-built solutions, ensuring reliable and secure integration of technological and corporate networks.

Today, Data Diode-class unidirectional data devices represent a popular security option widely used across the globe. In fact, these solutions are best practices recommended by leading information security experts, regulators and expert organizations.

In today’s world, we, having an effective security solution available in the Russian market also, should ask ourselves: “Which of our critical objects should be so accessible to the outside world that we can only afford to protect them with a firewall”?

InfoDiode products are available in various form factors and configurations: **InfoDiode PRO hardware and software solutions** in base and cluster configuration, **AK InfoDiode RACK single** hardware solutions, **AK InfoDiode RACK double** for mounting in 19" rack and **AK InfoDiode MINI** for mounting on DIN rail or in compact desktop configuration.

Applications for Data Diode

Technological & Corporate network integration

The most common scenario of unidirectional data devices use at CI objects is for assurance of a secure and efficient integration between technological and corporate networks. As a rule, a Data Diode replaces firewalls and applications at border points between technological and corporate networks in such cases.

Database replication and historical data transfer

Data Diode is often used to replicate various data sources from the technology network to the corporate network. Historical data replication and file delivery can be used in scenarios of reporting, sharing raw data and files that support debugging and monitoring processes. In case that the technological segment of the network collects data that must be made available for analysis to users of the corporate network, the installation of unidirectional data transmission devices ensures the transmission of such data to the corporate network, where relevant users and applications can access them without jeopardizing the technology network and critical infrastructure equipment.

Receiving of updates

In case it is necessary to periodically update antivirus databases, software and other updates and signature bases important for the security of the technological network, Data Diode, installed to transfer data from the open network segment to the technological segment (i.e., backwards), provides an efficient solution to this problem. This architectural solution reduces the risks associated with firewalls.

Integration with software solutions

Another scenario for transferring data through a unidirectional data transmission device is the transfer of Syslog traffic to specialized servers/security systems. This data is used to capture events in SIEM systems, specialized intrusion detection systems and network topology changes operating within corporate SOC, NOC centers.

Monitoring and control of the operation of the equipment of the protection object

Equipment operation monitoring

In a large number of CI objects and industries, there is a need for support for operational equipment from suppliers and manufacturers. For this purpose, specialized monitoring and diagnostic tools can be used, produced by the manufacturer / supplier.
Using Data Diode-class devices solves this problem by deploying a solution that can replicate management servers and data from a critical network segment to the vendor/manufacturer DMZ network. DMZ connects to the vendor’s central management system, most often via a VPN. Replicas transmitted to DMZ can be accurate copies of the plant systems and provide complete transparency to the supplier/manufacturer equipment.

Visual monitoring

There is often a need for visual monitoring of processes within the CI objects. This may be video surveillance or visual monitoring of operators in the external situation center.