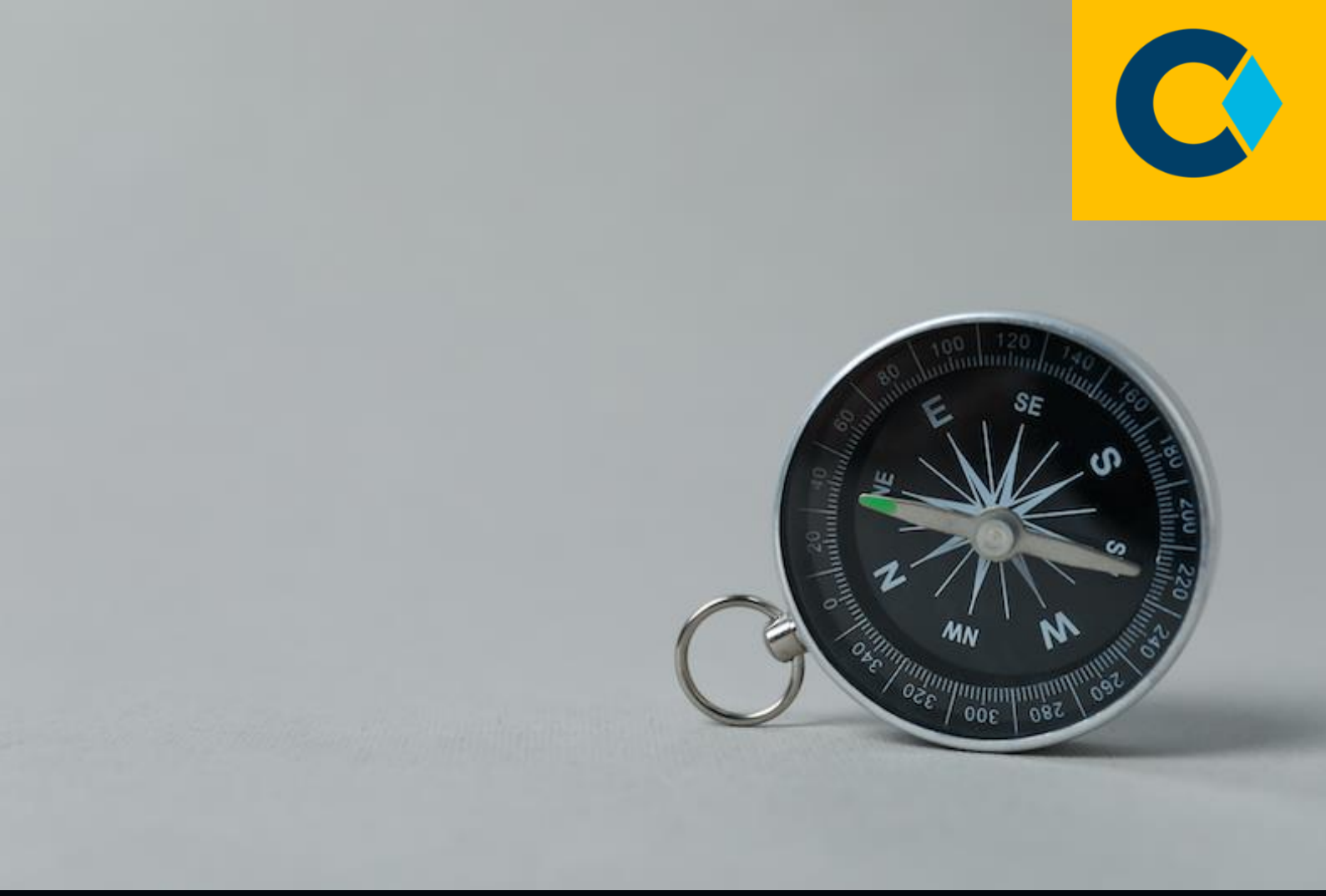


A GUIDE TO DATA DIODES

CONNEXONE

CONNEXITE

TABLE OF CONTENTS

1. INTRODUCTION TO DATA DIODES

1.1. What is Data Diode

A data-diode (also referred to as a unidirectional gateway) is a network device (appliance) that allows data to flow in only one direction. Unidirectional data flow feature guarantees information security (e.g. database) and protection of critical digital systems (such as industrial control systems) from inbound cyber-attacks. Data-diodes are commonly used in high security environments (such as defense, security, energy, finance, manufacturing), where they serve as connections between two or more networks of differing security classifications.

An advanced data-diode is not only a network device which allows raw data to flow only in one direction; it is also a combination of hardware and software running acting as protocol proxies. The hardware enforces physical unidirectionality, and the software replicates databases and emulates protocol servers to handle bi-directional communication that source and destination devices require.

New generation data diodes are now capable of transferring multiple protocols and data types simultaneously.

1.2. Two Way Data Diode

Secure two-way communication can be achieved using two independent data-diodes installed in opposite directions. A high level of security can be achieved with enabling commands and controls to flow in one direction and data to flow in the other direction.

1.3. Applications of Data Diode

- Real time monitoring of safety critical networks
- Secure OT - IT bridge
- Database replication
- Database disaster backup
- Secure printing from a less secure network to a high secure network
- Transferring application and operating system updates from a less secure network to a high secure network
- Transferring data between a less secure network and a high secure network
- File transfer
- Streaming video
- Sending/receiving alerts or alarms from open to critical/confidential networks
- Sending/receiving emails from open to critical/confidential networks

2. Firewall

2.1. What is Firewall

A firewall is a network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules. They act as a barrier between trusted networks and untrusted and usally external networks, such as the internet.

Firewalls can be hardware, software, or a combination of both and are used to prevent unauthorized access to or from private networks. They come in various types, including packet-filtering, stateful inspection, proxy, and next-generation firewalls, each offering different levels of security and functionality. Firewalls are versatile and widely used in a variety of network environments, from personal home networks to large corporate settings, making them a fundamental part of network security.

Roles of the firewalls are more related to protect the exchange of two-way communication such as access control, versatile threat prevention, monitoring traffic and adapting to new threads. Some details would be good to understand more quickly.

2.2. Data Diode vs. Firewall

Although these technologies provide a common purpose which is to protect data exchange between two isolated networks, the main difference between a Data Diode and a Firewall is physical unidirectional data flow.

Data Diode physically enforce a one-way flow of data, making it impossible for data to be sent back in the opposite direction, due to the lack of physical return path.

Data diodes are typically used in high-security environments where the utmost confidentiality and integrity of data are required, such as military, government, or industrial control systems. They are particularly valued in scenarios where information must leave a secure network without any possibility of external threats infiltrating the network via the same path.

Since firewall does not have unidirectional interfaces, it is designed to achieve blocking unwanted data flow with a set of rules. But this method has its weaknesses, such as

- Zero-day attacks
- Operator errors

2.2.1. Zero-Day Attacks

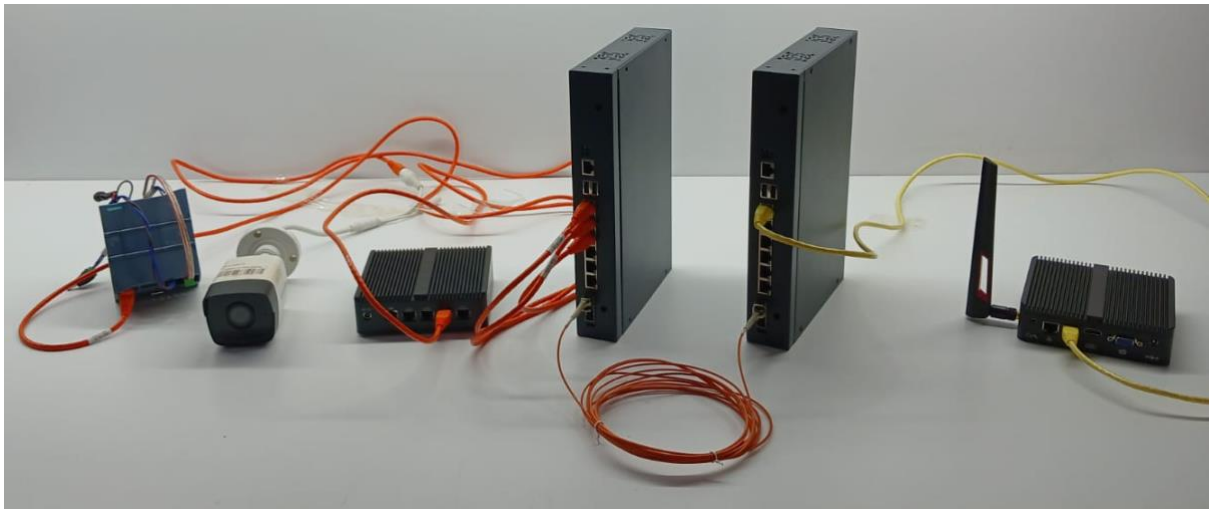
A zero-day attack is a vulnerability or security hole in a computer system unknown to its developers and owners. This type of attack is made through flaws in firewall's software or firmware design. This flaw can only be prevented after it occurs. Thus, by the time it was patched, it has already caused a security breach for some users.

2.2.2. Operator Errors

Most common vulnerability of firewall use is caused by its operators. Weak management interface password and weak configuration (rules set) can be exploited by attackers.

3. ConnexOne SOLUTION

ConnexOne is an advanded data diode system.



3.1. Hardware

ConnexOne consists of two devices. Transmit only device is ConnexOne-Tx, and receive only device is ConnexOne-Rx. Transmit device is paired with a transmit only SFP, and receive device is paired with a receive only SFP.

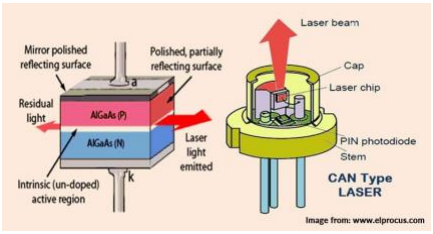
Data can flow only from ConnexOne-Tx to ConnexOne-Rx.

3.1.1. ConnexOne-Tx

The transmit device contains an embedded processor, capable of conducting upto 10Gps of data transmission.

This device is connected to the network through its copper RJ45 interfaces.

The transmit device is connected to the receive device through its optical interface with a single core LC fiber cable. Transmit only for ConnexOne-Tx is realized by an optical transmitter, which contains only a laser diode (TOSA). This circuitry ensures only tranmission of optical signal.

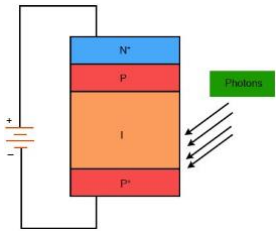


3.1.2. ConnexOne-Rx

Receive device contains an embedded processor, capable of conducting upto 10Gps of data transmission.

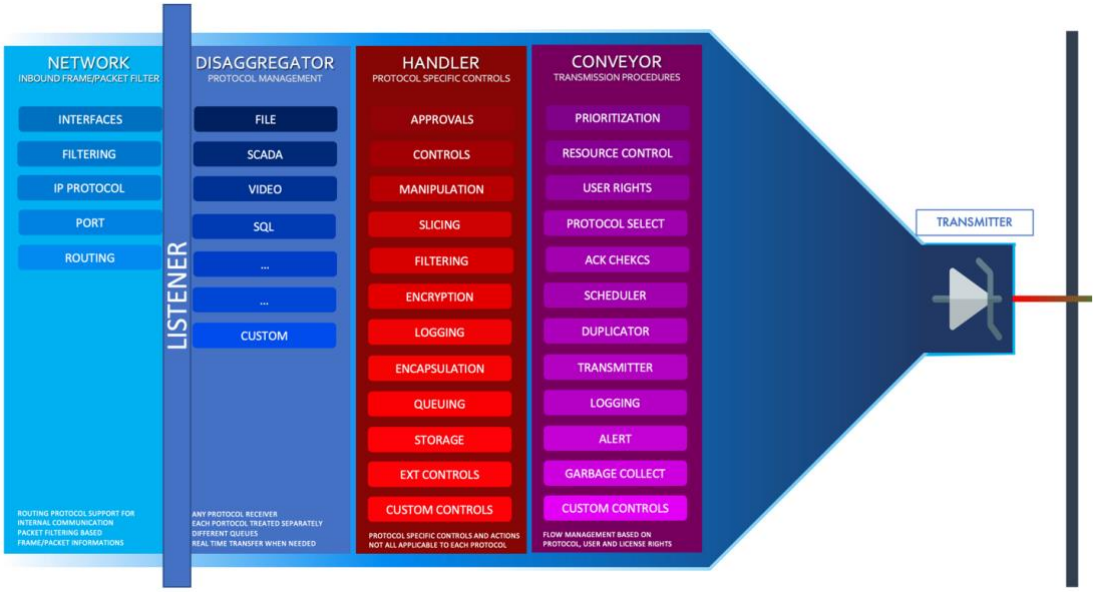
This device is connected to the network through its copper RJ45 interfaces.

The receive device is connected to the transmit device through its optical interface with a single core LC fiber cable. Receive only for ConnexOne-Rx is realized by an optical receiver, which contains only an avalanche photodiode (ROSA). This circuitry ensures only reception of optical signal.



3.2. Software

ConnexOne uses a layered packet processing that allows different protocols to be implemented without affecting any other functionality. The flexible architecture makes any new protocol addition possible. Following is an illustration of how flow processing is handled by ConnexOne:



All processes defined in different layers are running separately and adding new functions and features are possible. ConnexOne limit, filter, manipulate or block any data based on application and payload.

Each protocol flow is handled with different set of controls. An SQL schema delivery is subject to schema controls and any unwanted query can be denied and dropped. A file transfer would require user approvals, before sending out from critical network.

4. USE CASES

Data-diode shall be part of the IT infrastructure of the following industries:

- Power
- Oil & Gas
- Manufacturing
- Transportation
- Finance
- Security
- Defense
- Engineering / Design services

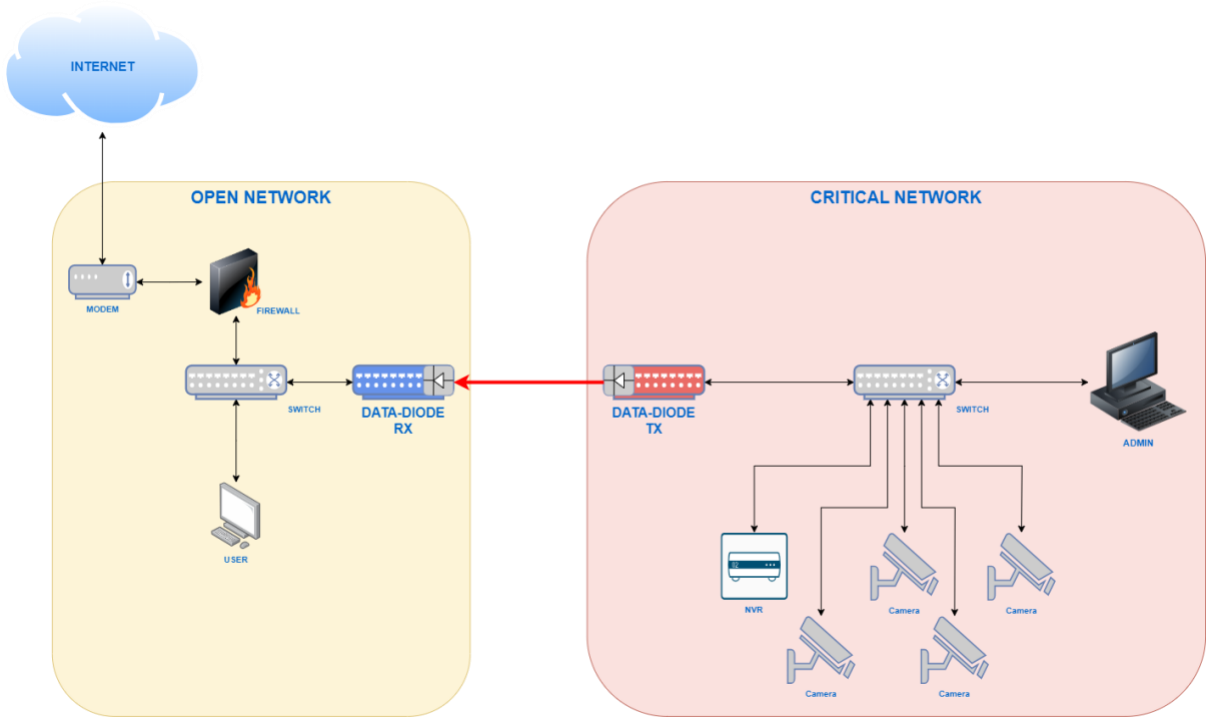
Any company generating proprietary data shall protect it with data diode.

Following use cases of ConnexOne are briefly explained:

- Camera streaming
- Data transfer of industrial control systems (OT)
- Database replication
- Database disaster recovery backup
- File transfer

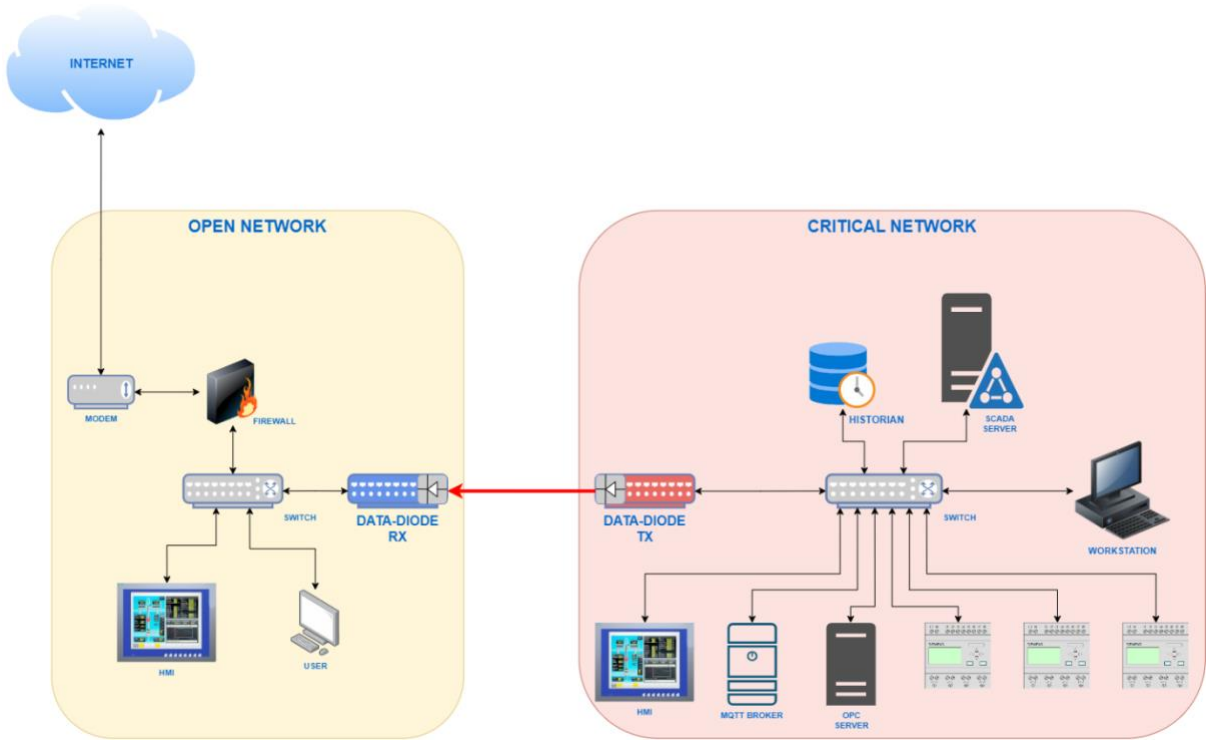
4.1. CAMERA STREAMING

a. ConnexOne-Tx starts RTSP streams from all cameras.
b. Collected streams are buffered, encrypted, and sent out to ConnexOne-Rx.
c. ConnexOne-Rx acts as a RTSP server. Registered users can watch camera streams from their PCs and smartphones.



4.2. Data Transfer of Industrial Control System (OT)

a. ConnexOne-Tx requests data from Scada, PLC, MQTT Broker, OPC Server, and/or Historian.
b. Collected data are buffered, encrypted, and sent out to ConnexOne-Rx.
c. ConnexOne-Rx can act as a Modbus server, Profinet server, OPC server, MQTT Broker. Registered users can request intended data in standard OT protocols.
Or, ConnexOne-Rx can send collected data through e-mail, sql query, and/or web request.

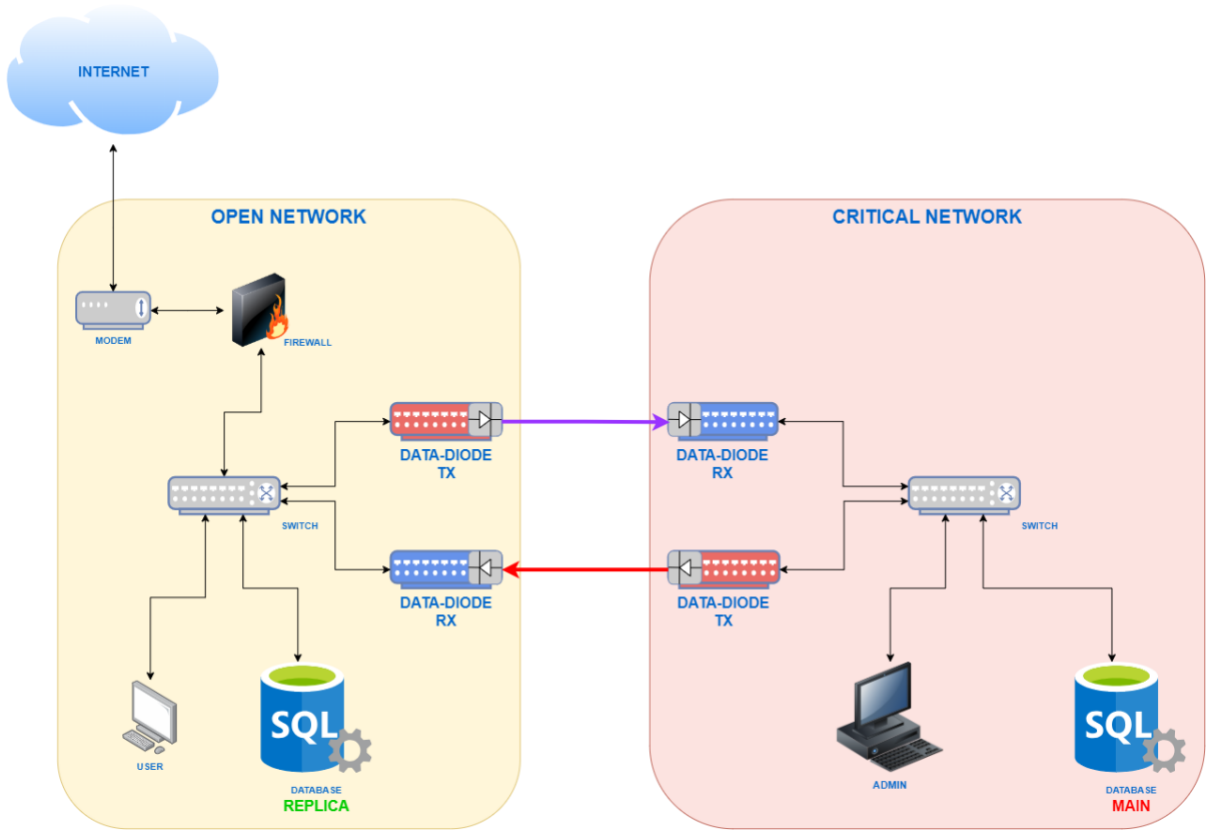


4.3. Database Replication

In this configuration two independent data-diodes are positioned between open and critical network. This configuration consists of 4 appliances.

Only SQL ports are enabled in all ConnexOne appliances. And all data flowing between open and critical networks are encrypted.

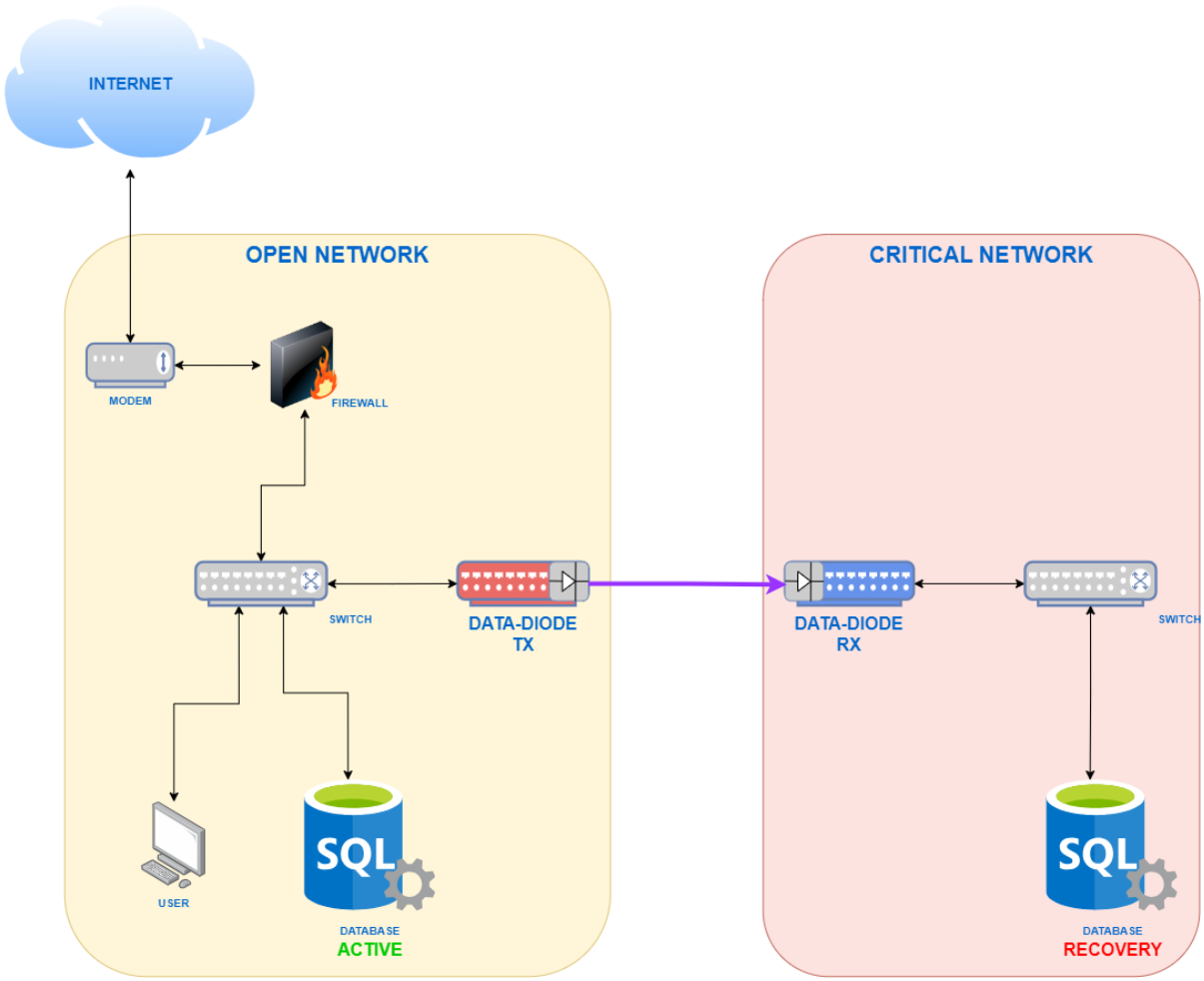
Since 2 appliances of (connected to Critical Network) have one way connections through their fiber interfaces, these 2 appliances cannot be penetrated by inbound cyber-attacks. Since cyber-attacks are impossible to conduct, port rules cannot be bypassed.



For this topology, ConnexOne devices located in the “open network” are vulnerable to cyber-attacks. Even if somehow the attacker manages to control two devices in the “open network,” it is impossible for the attacker to infiltrate other ConnexOne devices (since there is no two way communication) located in the “critical network.” Thus, the “critical network” is always protected.

4.4. DataBase Disaster Recovery Backup

a. Database backup is initiated by Database-Active.
b. Collected data by ConnexOne-Tx is buffered, encrypted, and sent to ConnexOne-Rx.
c. ConnexOne-Rx acts as database server and sends backup data to Database-recovery server



4.5. File Transfer

a. File transfer is initiated by User computer in critical network through ConnexOne-Tx https user interface.
b. Once the file is uploaded, ConnexOne-Tx starts review cycle. Data transfer request notice e-mails are sent to predetermined users (e.g. project manager, data security specialist, IT specialist). Each user must login to ConnexOne-Tx https user interface, inspect uploaded data, and approve data transfer.
c. Once all approvals are done, data will be encrypted and transferred to ConnexOne-Rx.
d. ConnexOne-Rx sends an e-mail to user in open network to notify for reception of file. User then can login to ConnexOne-Rx https user interface to download the file.

ConnexOne-Rx can also be programmed to transfer this file through an e-mail or to an ftp server.