Whitepaper

Fox DataDiode

A Preferred Solution for High-Security Real-time Electronic Unidirectional Data Transfer between Networks

FOX-IT
EXPERTS IN IT SECURITY

Summary
The Fox DataDiode has been designed to avoid problems that are inherent to the conventional air gap solution of data transfer. It provides a fast and secure way to send data to a high security network, guaranteeing that no data will ever leak back, just like a diode in the field of electronics is used for its unidirectional current property.

The Fox DataDiode has been approved to connect a network that handles SECRET data and has been certified as follows:

- NATO (Secret)
- Common Criteria EAL4+
- NL-NCSA (Secret)
- BSI (Secret)

Introduction

Every network needs to be updated at some point with data from an external source. In case of high security environments, security measures do not permit physical connections to an external source such as another network, although this would be convenient for data transfers.

Conventional Approach

Since secure networks cannot be connected to other networks, data have to be transferred manually, using portable data storage mediums like USB sticks, CDs or comparable devices. The data are copied onto the storage medium, then the medium is transported to the high security network, and there the data are transferred onto this network. This way a unidirectional data transfer is secured, so data leakage is impossible.

However, there are some major disadvantages to this way of dealing with data transfers. It is not real time, but more important than that: high security risks are being introduced through the possible loss of these portable storage media or through incorrect disposal after they have been used. Apart from that, this way of data transfer is time intensive and costs much.

A Preferred Solution

A more straightforward way of unidirectional data transfer between networks would be possible if a data diode were used. A diode is a device that allows an electric current to flow in one direction and blocks it in the opposite direction. Similar, a data diode allows data transfer in one direction and blocks it in the opposite direction.

This is exactly what the Fox DataDiode does. This hardware-based data security solution has been specifically designed for transferring data unidirectionally between two networks, where the receiving network has a high security level and cannot be allowed to leak information to any other network.

Although developed primarily for security-conscious government authorities like defence organizations, intelligence agencies and the police, the Fox DataDiode is also well suited for deployment by commercial organizations or anyone seeking a secure, one-way data link between two physically separated networks.

The Fox DataDiode is currently deployed in multiple agencies in numerous countries. It ensures a 100% secure unidirectional network connection, certified and approved by multiple independent organisations.

Philosophy
The Fox DataDiode philosophy derives from the field of electronics, where a diode is a device that allows an electric current to flow in one direction and that blocks it in the opposite direction. Instead of an electric current, the data diode allows data to flow in one direction, while blocking it in the opposite direction.

This is done by the Fort Fox Hardware Data Diode, a unique, hardware based communication device, which makes use of a gigabit optical data link to transfer data in a single direction.

Reliability
Besides providing unidirectional data flow, the Fox DataDiode also offers data integrity by means of error detection and correction.

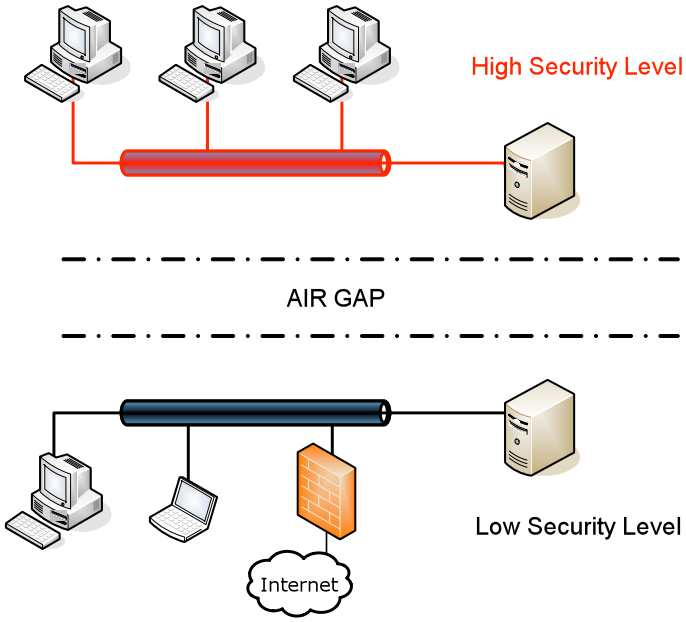
An easy-to-use web interface allows authorized users to specify and initiate data transfers. Not only data files, but also backup mirror images of frequently used websites and servers, and anything else that can be sent using FTP can be sent through the data diode. The data diode also supports SMTP, so incoming email can be sent through the diode to the secure network. One-way UDP is also supported, which makes it possible to send e.g. real-time video and audio streaming through the diode.

This hugely increases the functionality and the flexibility of the still highly secure network, and these advantages come with a reduced time, cost and effort of transferring data manually on data-storage mediums.

Security

How secure is the Data Diode concept? Some investigation must be done to answer that important question.

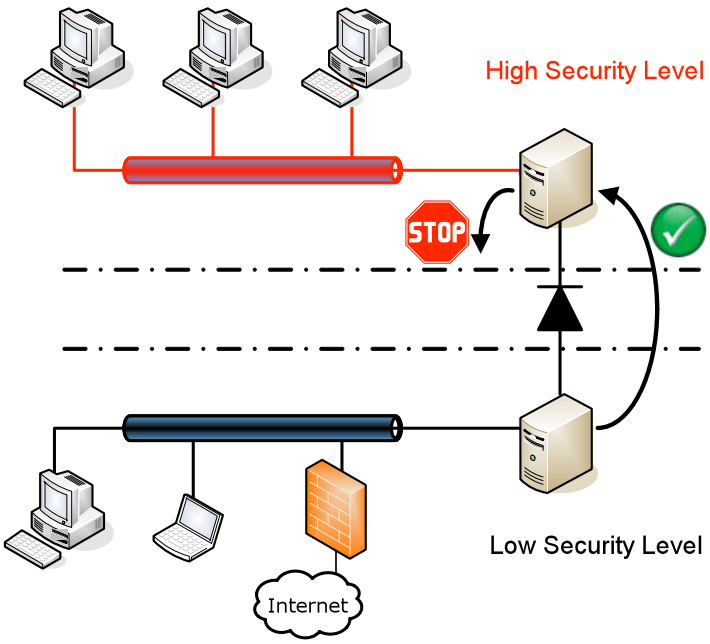
Let's first look at the conventional setup, in which a so called air gap solution is implemented.



'Air gap' refers to the physical separation of two networks, where the only means of transferring data is through a portable data-storage device, such as a USB stick, CD or DVD, combined with human intervention. For a long time, this was the most common approach to securing highly confidential data. However, strictly separating a high security network from other networks still does not ensure data security, because it cannot prevent data leakage. Data has to be physically copied to the storage medium, transported and then copied to the receiving network. This introduces a security risk: data storage devices can be lost, or they can be disposed of incorrectly. Apart from that, it is a process that involves a considerable amount of time, effort and cost, and it cannot be automated or performed remotely.

Deployment of a hardware-based, one-way connection between networks is a secure solution that avoids all of these problems. Such a connection prevents any data leakage, while at the same time a continuous data stream is provided to the secure network.
Implementation in hardware means there is no chance that a software malfunction (through a bug, virus or tampering) will ever occur in the data diode. No decision logic,

software or firmware is present in the Hardware Data Diode, so the security of the red network cannot be compromised.

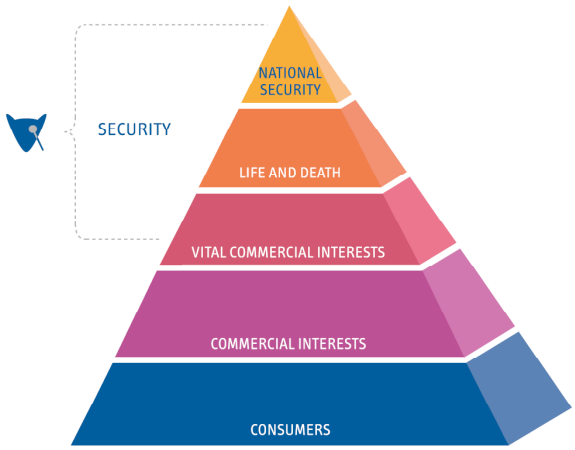


Data integrity is maintained by using a custom-developed, proprietary communications protocol that has intelligent error correcting codes. Logging all transfer activities on both sides of the transaction ensures that all 'events' during a transfer are tracked and timed, and abnormal activities are detected and reported.

Not a single new technical threat or vulnerability is being introduced by using a data diode; the disadvantages of the conventional approach are avoided, while at the same time a much higher level of security for the protected network is achieved. This makes a data diode a very attractive alternative to the air gap solution.

Positioning

The Fox DataDiode was primarily developed for use by governmental organisations, especially those that have to maintain a certain security level. It is typically used in environments that require 'state-secret security' solutions.



However, commercial organizations can also make excellent use of the Fox DataDiode, when they need to perform one-way transfers between two physically separated networks. Based on user requirements (custom made) 'connectors' for other (proprietary) protocols can be implemented, which guarantee a one-way data flow under all circumstances.

Typical Deployment

Some real-life examples will help to better understand the typical deployment of data diodes.

Linking a Defence network to the Internet

In order to work effectively, a secret defence network requires gathering information from around the world via the Internet, and transferring this information to the secret network to be properly aggregated, filtered and used. In order to guarantee 24/7 information transfer, the process should be fully automated and without human intervention. Of course, security is paramount; no information should leak from the secret network.

Securing emails holding tax data

To facilitate the tax-return process, the tax authority requires citizens to digitally fill out their tax forms and email them to the tax office, using the Internet. These forms are subsequently transferred automatically to the back office where they are processed. Internally, the tax administration is split into two separate networks: a network connected

to the Internet and the back office network that handles all national tax data and which is therefore deemed highly secure. Once in the hands of the tax authority, the tax data are to be protected and any leakage at this point is therefore totally unacceptable.

Again, the Fox DataDiode offers an elegant solution. A 'normal' email gateway is used to receive email from the Internet, and scan it for viruses and similar threats.

The Fox DataDiode is then deployed to transfer these emails from the unsecured network to the protected network in the back-office, this guarantees 100% security against leakage of confidential back-office information. In addition, this also allows for a 24/7 operation, which was not possible or practical with the original air gap method of using magnetic tapes to transfer digital tax forms.

Protecting telephone interceptions

Another scenario involves the mobile telecom industry. Mobile telephone service providers are frequently required to intercept telecom traffic data. This data needs to be subsequently transmitted digitally, in real time and without risk of data leakage, to a high-security network for analysis by the police or intelligence agencies.

Intercepted signals are transformed into digital data and packaged in low-level UDP network packets for secure transfer to the high-security network, using the Fort Fox Hardware Data Diode. It should be noted that in this case no Data Diode servers are deployed. The interception system is connected to the Fort Fox Hardware Data Diode through the underlying network and router; on the receiving side, data is received directly and in real-time by the high-security network.

Linking two high security networks

It goes without saying that the Fox DataDiode can also be used in secure data transfer between two secure networks. A good example would be the data link between NATO's secret network and a member government's high-security network. In this case, NATO-oriented data may be sent to the national network, but no national data may be sent in the reverse direction.

In Conclusion

High security networks are deployed widely by government authorities and the military and intelligence communities, as well as in business and R&D. A breach of data security in these cases could have wide-ranging repercussions, involving national security, financial fraud and other criminal activities, industrial espionage or breach of personal privacy – affecting national, commercial and personal interests. That is why security must be taken most seriously.

The Fox DataDiode successfully combines secure data transfer with efficient, easy to use and cost-effective data transfer. It is superior to the conventional air gap solution, because less risks are involved, it is less time consuming and it allows for more types of data transfer.

The Fox DataDiode, with its wide selection of application areas, offers the best of all worlds: a watertight-secure data transfer, which is also affordable, efficient, and user-friendly; and which comes with extra functionality for network administrators and users.

The Fox DataDiode has been approved to connect a network that handles SECRET data and has been certified as follows:

- NATO (Secret)
- Common Criteria EAL4+
- NL-NCSA (Secret)
- BSI (Secret)

Contact Information
For more information about the Fox DataDiode, please contact:

Fox-IT
Olof Palmestraat 6
2616 LM Delft
The Netherlands

Email: datadiode@fox-it.com
Phone: +31 (0)15 284 79 99
Fax: +31 (0)15 284 79 90

Or access our website at: http://www.datadiode.eu