

White paper

Fort Fox Data Diode:

A Preferred Solution For High-Security
Real-time Electronic Data Transfer
Between Networks



Table of contents

Executive Summary & Introduction	3
What Is The Fort Fox Data Diode?	5
Figure 1: A typical Fort Fox Data Diode configuration	6
Security Aspects	8
THE AIR GAP SOLUTION	8
THE ONE-WAY CONNECTION	9
WHY IS THE FORT FOX DATA DIODE SO SECURE?	10
Positioning	12
Typical Deployment Scenarios	13
LINKING A DEFENSE NETWORK TO THE INTERNET	13
SECURING E-MAILS HOLDING TAX DATA	13
PROTECTING TELEPHONE INTERCEPTIONS	14
LINKING TWO HIGH SECURITY NETWORKS	15
Concluding Remarks	16
Appendix 1: Specifications Summary	17
Contact Information	18



Executive Summary & Introduction

Every network needs to be updated at some point with electronic data from an external source, like another network. This is a relatively straightforward task. However, in the case of high security environments, physical connections to other networks are not allowed for security reasons. The transfer of electronic data therefore has to take place manually, using a USB stick, CD or similar device. It involves copying data from one network or system onto the portable data storage medium, transferring the medium to the receiving network and subsequently importing the data. Unfortunately, this form of data transfer is never real-time and more important introduces security risks through the loss of the portable storage medium or its incorrect disposal. This is indeed a critical issue when considering high-security, confidential data.

This is where the Fort Fox Data Diode really comes into its own, as this white paper will further explain. This hardware-based data security solution from Fox-IT is ideal for transferring data optically between two networks, where the receiving network has a high security level and cannot, or should not, be connected to another network.

Central to the Fort Fox Data Diode solution is the Fort Fox Hardware Data Diode, which operates in a unidirectional mode and deploys a light source and corresponding photocell to conduct the actual data transfer.

A Fort Fox Data Diode configuration can also have two optional server computers connected to the transmitting and receiving networks to provide additional user and network-administration functionality. This enables users of the receiving network to receive e-mail from outside their network, print locally or access frequently used websites. This is done without exposing their high-security network to outside threats.



[Fort Fox Data Diode](#)

Security and data integrity are also further enhanced through the use of encryption, and error detection and correction.

Developed primarily for security-conscious government authorities, such as defense organizations, intelligence agencies and the police, the Fort Fox Data Diode is also well suited for deployment by commercial organizations seeking a secure, one-way data link between two physically separated networks. Typically, these organizations could be financial institutions or highly competitive R&D environments.

Secure data-transfer applications range from transmitting tax returns to a tax authority's back-office network; transferring intercepted telecom data to a police or intelligence network for analysts to examine; to transferring data between NATO's secret network and a member government's own high-security network.

The Fort Fox Data Diode's proven technology, currently deployed in several countries and within multiple agencies, ensures a hundred-percent-secure, one-way network connection between two networks of varying security levels, without compromising the security of the receiving network. Equally important, the transfer—automated or manual—of data is easy and user-friendly to perform, offering network owners and administrators savings in time, effort and cost.



What Is The Fort Fox Data Diode?

The Fort Fox Data Diode is an elegant solution for the high-security transfer of data between networks.

Central to the Fort Fox Data Diode solution is 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 (hence the term 'diode'), between a low-security network and a network with a high-security level. Needless to say, this solution can also be used where both networks have the same level of security.

The Fox Hardware Data Diode can be deployed on its own, or in combination with two optional Intel-based servers, where one is connected to the low-security (black) network, and the other to the high-security (red) network (see Figure 1).



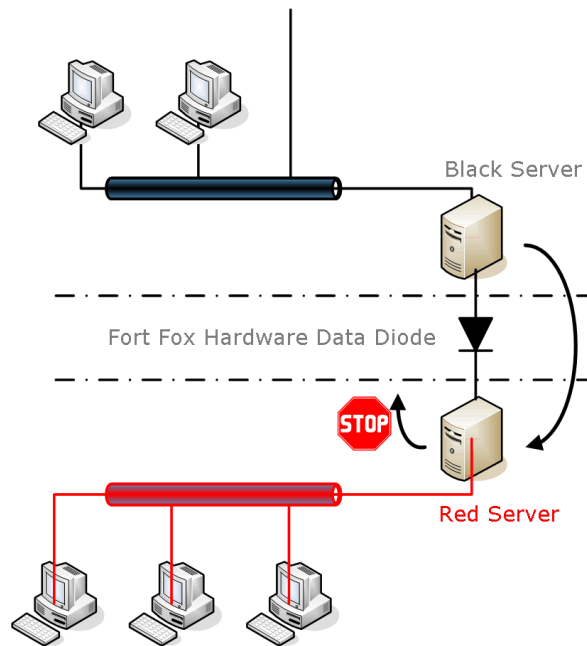


Figure 1: A typical Fort Fox Data Diode configuration

The Fort Fox Data Diode also can also provide added protection through encryption (optional), as well as data integrity by means of error detection and correction. Each server comes with an easy-to-use web interface, which allows authorized users to specify and initiate a data transfer.

A Fort Fox Data Diode transfer is not limited to data files. It can also contain a backup mirror image of frequently used websites and servers, a print job or even incoming email. This provides red network-users with added functionality and flexibility. For example, they can receive (although not send) e-mail from outside their network¹. Frequently used websites and FTP servers can also be mirrored and accessed locally. Furthermore, print jobs from the black network can be received on the red network and printed locally.

¹ Fox-IT is currently developing a new solution that also allows a user to send signed e-mail messages from the red network as well. Please contact Fox-IT for more information and the release date.



[Fort Fox Data Diode](#)

Most of all, network administrators are saved the effort, time and cost of transferring data manually on data-storage media.



Security Aspects

To appreciate how secure the Fort Fox Data Diode really is, it is worth investigating and analyzing certain security aspects of data transfer between highly secured networks.

The air gap solution

An 'air gap' refers to a 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.

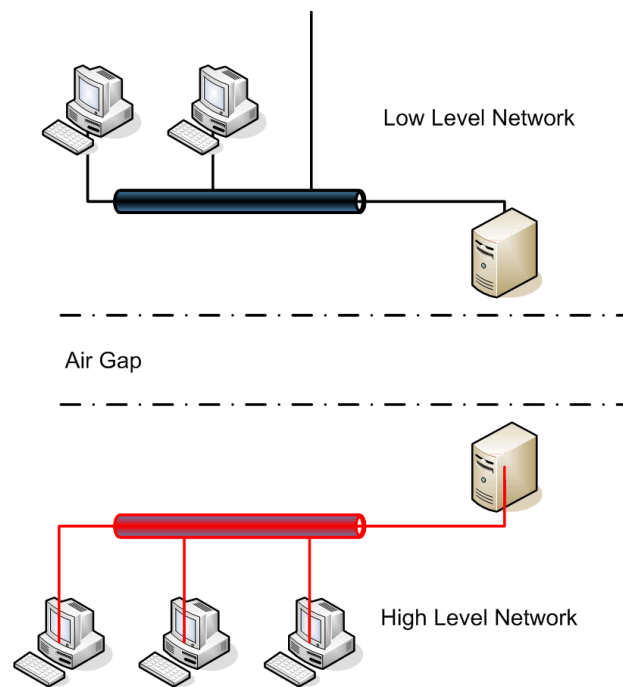


Figure 2: Using an Air Gap to secure inter-network data transfer

The use of an air gap to transfer data between high- and low-security networks has long since been the most common approach to securing highly confidential data.



Strictly separating the two networks ensures data security and critically prevents any data leakage from the high security network. However, this solution also comes with considerable disadvantages.

Data has to be physically copied to the storage medium, transported and then copied to the receiving network. This is an ongoing process, which usually involves a considerable amount of time, effort and cost, and which cannot be automated or performed remotely. Moreover, there is still a security risk. Data storage devices could be lost, or disposed of incorrectly, where confidential data is not or only partially deleted (inadvertently or deliberately). In both cases, confidential information could fall in the wrong hands.

The one-way connection

The other solution is the deployment of a hardware-based, one-way connection between the networks (see Figure 3). Such a connection prevents data from flowing in the opposite direction—from the high-security to the low-security network—while providing a continuous, data stream to the secure network. Implementing this connection in hardware (instead of firmware or software) has its benefits, as explained in the following section. All of this means real-time access to the data, but without the risk of losing or leaking any of it. It also means manpower, time and cost savings.

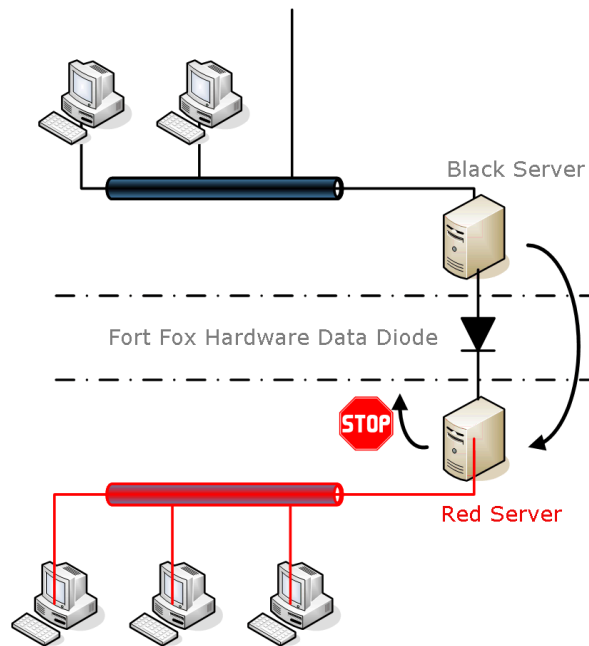


Figure 3: A secure data transfer using the Fort Fox Data Diode

Why is the Fort Fox Data Diode so secure?

Firstly, the physical connection—the Fort Fox Hardware Data Diode—between the red and black networks is single-directional and fully implemented in hardware. Importantly, no decision logic, software or firmware is present in the Hardware Data Diode (although there is software in the optional Data Diode servers). This means that no error or malfunction can take place that could result in data leakage on the red network’s end. This also means that a software malfunction (through a bug, virus or tampering, for instance) will never occur in the Hardware Data Diode. Critically, the security of the red network will never be compromised.

Furthermore, data transmitted from the black to the red Data Diode servers can be optionally encrypted to prevent data injection, data tampering and data eavesdropping. The use of a custom-developed, proprietary communications protocol with intelligent error correcting codes means that data integrity is also maintained at all times.



[Fort Fox Data Diode](#)

Moreover, all transfer activities are logged on both sides of the transaction, ensuring that all 'events' during a transfer are tracked and timed, and abnormal activities are detected and reported.

The Fort Fox Data Diode does not introduce any new technical threats or vulnerabilities. What is more, it provides a much higher level of security in managing and administering a secret network than an air gap solution (which can still present a security risk, as explained earlier).



Positioning

The Fort Fox Data Diode was primarily developed for use by governmental organizations, especially those that have to maintain a certain security level. It is typically used in environments that require 'state-secret security' solutions (see Figure 4).

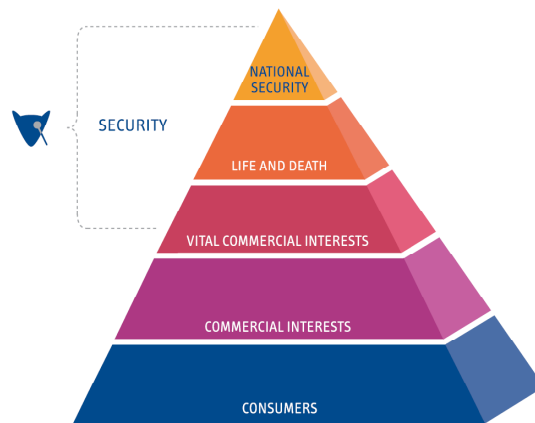


Figure 4: The Fort Fox Data Diode security pyramid

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



Typical Deployment Scenarios

Here are some typical examples of where and how the Fort Fox Data Diode can be used effectively.

Linking a defense network to the Internet

Consider the following situation. In order to work effectively, a secret defense 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.

The solution is to deploy the Fort Fox Data Diode and its automated features to link the Internet to the secret network, using a standard file-transfer communications protocol, FTP.

Securing e-mails holding tax data

To facilitate the tax-return process, the tax authority requires citizens to digitally fill in their tax forms and e-mail 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: an unprotected 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, this tax data has to be secured and any leakage at this point is therefore totally unacceptable.

Again, the Fort Fox Data Diode offers an elegant solution. A 'normal' e-mail gateway is used to receive e-mail from the Internet, and scan it for viruses and similar threats.



The Fort Fox Data Diode is then deployed to transfer these e-mails from the unsecured network to the protected back-office one, thus guaranteeing 100% security against leakage of confidential back-office information. In addition, this also allows for a 24/7 operation, something that was not possible or practical with the previous 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.

Using the Fort Fox Hardware Data Diode (as Figure 5 illustrates), intercepted signals are transformed into digital data and packaged in low-level UDP network packets for secure transfer to the high-security network.

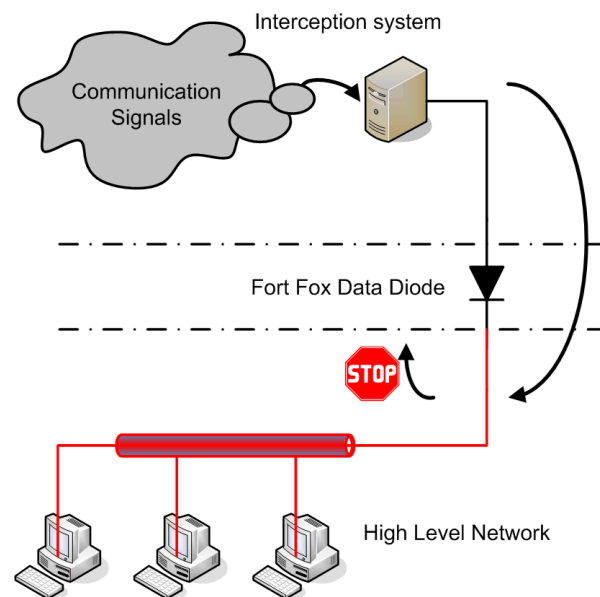


Figure 5: Using the Fort Fox Hardware Data Diode to transfer intercepted data securely



It should be noted that no Data Diode servers are deployed in this case. The interception system is connected to the Fort Fox Hardware Data Diode through the underlying network and router; and 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 Fort Fox Data Diode 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 sent in the reverse direction.



Concluding Remarks

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 owners and administrators of such networks take security threats and risks most seriously.

However, while data security is of paramount importance, it should be balanced, where possible, with means and methods that are efficient, easy to use and cost-effective. It is obvious that the use of portable data-storage media is not the best answer, not least because it comes with risks and is cumbersome and time-consuming.

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



Appendix 1: Specifications Summary

Fort Fox Data Diode: Fort Fox Hardware Data Diode	
Physical interfaces:	Gigabit optical (SC)
Throughput:	1 Gbit/s
Approvals:	Stg. Geheim (Dutch information security accreditation body) AMSG720B approved
Dimensions:	19" 1U rack
Power usage:	Double 75-230V 12W and other international standards
Temperature:	Operating: 5°C - 50°C (non-condensing) Storage: -10°C - 60°C (non condensing)

Fort Fox Data Diode: Data Diode Servers	
Physical interfaces:	100BaseT (RJ45) or Gigabit optical (SC) towards the black and red network.
Protocols supported	
Black server:	SMTP (server), FTP (server). (Planned: HTTP (client), Microsoft Windows print server) Others can be implemented upon request.
Red server:	SMTP forwarder, FTP forwarder. (Planned: HTTP local cache, Printer forwarder) Others can be implemented upon request.
Between servers:	Proprietary protocol with strong error detection and correction algorithms to prevent data corruption.
Servers:	Intel compatible hardware (according to hardware compatibility list)
Operating system:	FoxBSD (proprietary)
Encryption:	256 bit AES between servers (optional)
Configuration:	Stored locally on each server for optimal security
Dimensions:	Black & Red server: industry standard 19" 1U or 2U housing
Power usage:	Servers: double PSU 230V 200W and other international standards
Temperature:	Operating: 5°C - 50°C (non-condensing) Storage: -10°C - 60°C (non condensing)



Contact Information

For more information about the Fort Fox Data Diode, please contact:

Fox-IT

Olof Palmestraat 6

2616 LM Delft

The Netherlands

E-mail: datadiode@fox-it.com

Phone: +31 (0)15 284 79 99

Fax: +31 (0)15 284 79 90

Or access our website at www.datadiode.eu