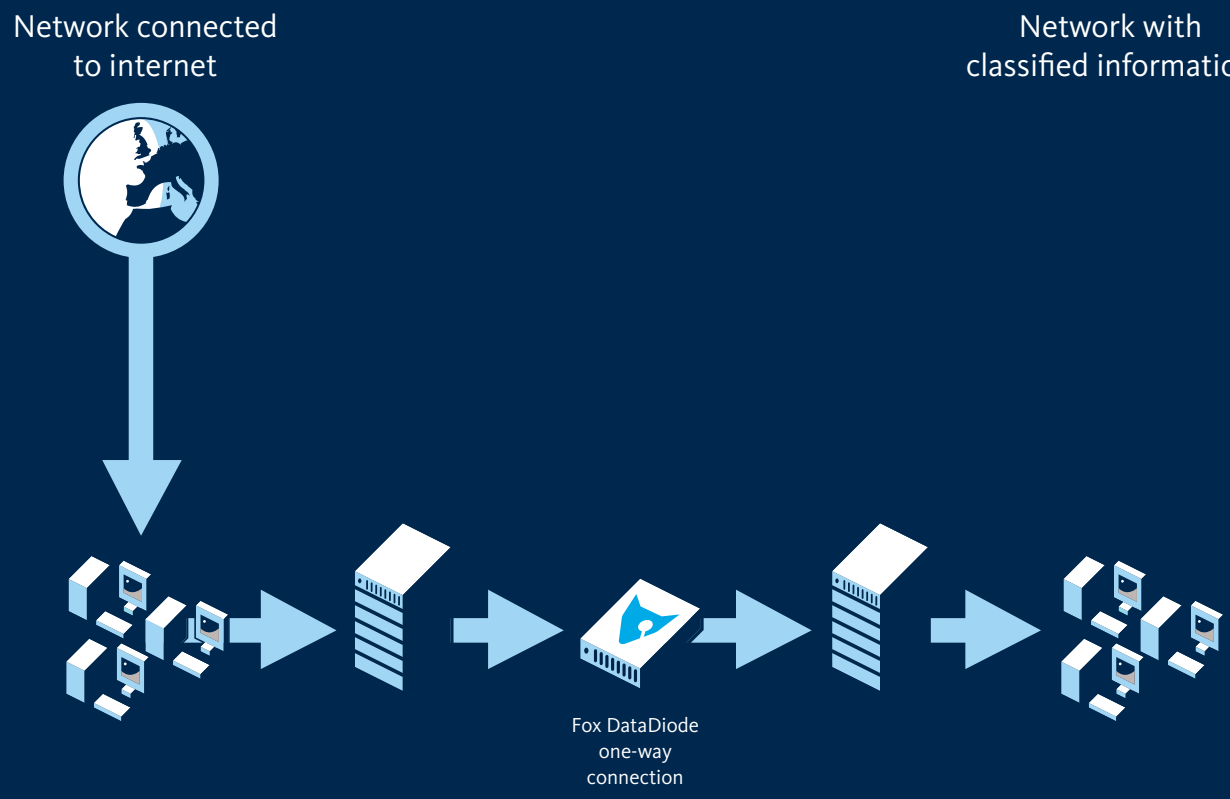


Fox DataDiode makes outgoing network traffic impossible

One-way traffic keeps secrets secret

There is widespread belief that the only foolproof and guaranteed way to prevent classified information leaks via a network is by making sure there is no physical connection. This is a misconception. Moreover, it would be unwise to isolate a network entirely from the outside digital world: after all, it needs to be able to receive incoming traffic.

FOX IT
part of nccgroup

fox-it.com/datadiode

The solution that meets both requirements – no leaks, while allowing incoming traffic – is a so-called data diode: a physical device without IP address, software, firmware, or FPGAs (programmable chips) that allows network traffic to flow in one direction, but impossible to let traffic flow in the other way. This article is based on the presentation Protecting Secrets from Cyber Crime, held by Peter C. Geytenbeek, International Sales Director at Fox-IT.

National governments have always been interested in learning each other's defense secrets and of ways to undermine each other's infrastructures. They deploy a wide array of resources – including digital weapons – for this purpose. The online threats currently facing defense organizations are already well-known. Less well-known, however, is that the instigation of digital resources has been around a lot longer than many people think. One of the oldest examples dates from the pre-Internet era.

Sabotage

In 1982, a Russian pipeline exploded in the Siberian city of Urengoy. It was the largest-ever non-nuclear explosion that was visible from space. The cause was – allegedly – sabotage by the CIA. Not by agents on the spot, but by a Trojan horse planted by the CIA in the pipeline's operating software, which had been developed by a Canadian company. Since then, malware – supposedly developed by 'state actors' – has surfaced on a regular basis, with Stuxnet being the most famous. Terrorists and hacktivists are also increasing their targeting of secrets and infrastructures of 'unsympathetic countries.'

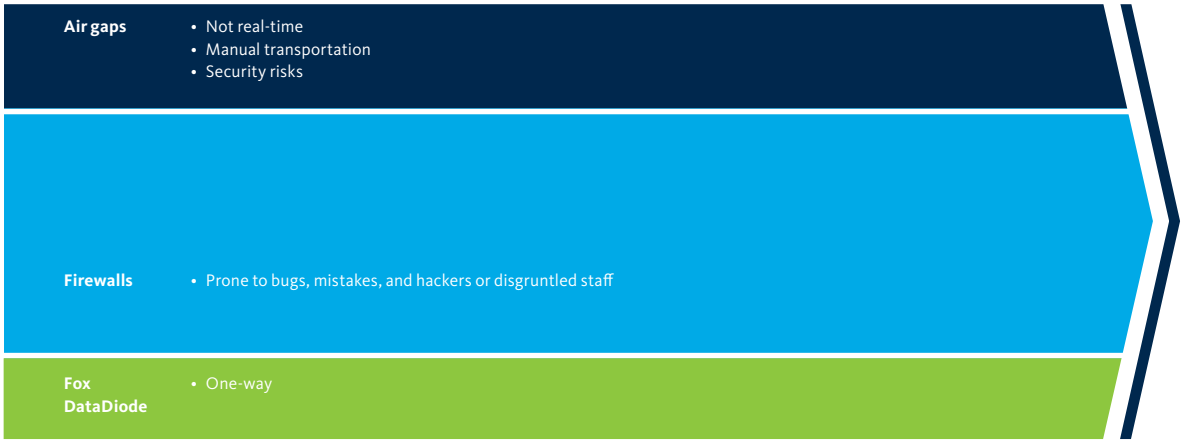
Vulnerable

These trends are mounting pressure put on the defense networks that house secrets. Network design (architecture), security policy (e.g. enforcing passwords that meet specific requirements), network software and communication protocols are particularly vulnerable. A single blindspot in one of these areas can expose the network to infiltration.

Measures

One well-known way to rigorously isolate a network is to create an 'air gap.' The network would then stand alone

Network boundary options



and information would only be able to enter or leave via a USB stick, CD-ROM, or another medium. Critics of this method say that it is not real-time, it is a tedious process, and, most importantly, that it is unsafe because malware can still enter the network through the media, and sensitive information can, in effect, leave by the same route.

Another option is to shield the network with a firewall, preferably a 'next generation'. However these are IP solutions that can be hacked, cannot guarantee faultless operation (bugs, backdoors), and are sensitive to configuration and administration errors, intentional or otherwise. And finally, there is the Fox DataDiode, which can make all outgoing – or incoming – network traffic impossible, but in a different way from the 'air gap.'

Hardware-Only

Like its electronic namesake, a DataDiode is a device that enables one-way traffic. Current (data) can flow in one direction, but not in the other. The Fox DataDiode is based on this principle (see cover picture). It is a hardware-only device with no software, programmable components, or IP address. This ensures that the Fox DataDiode cannot be hacked from the outside, and thus makes it absolutely impervious to online attacks.

However, the electronic disabling of (data)traffic in one direction is not sufficient. A solid solution requires more.

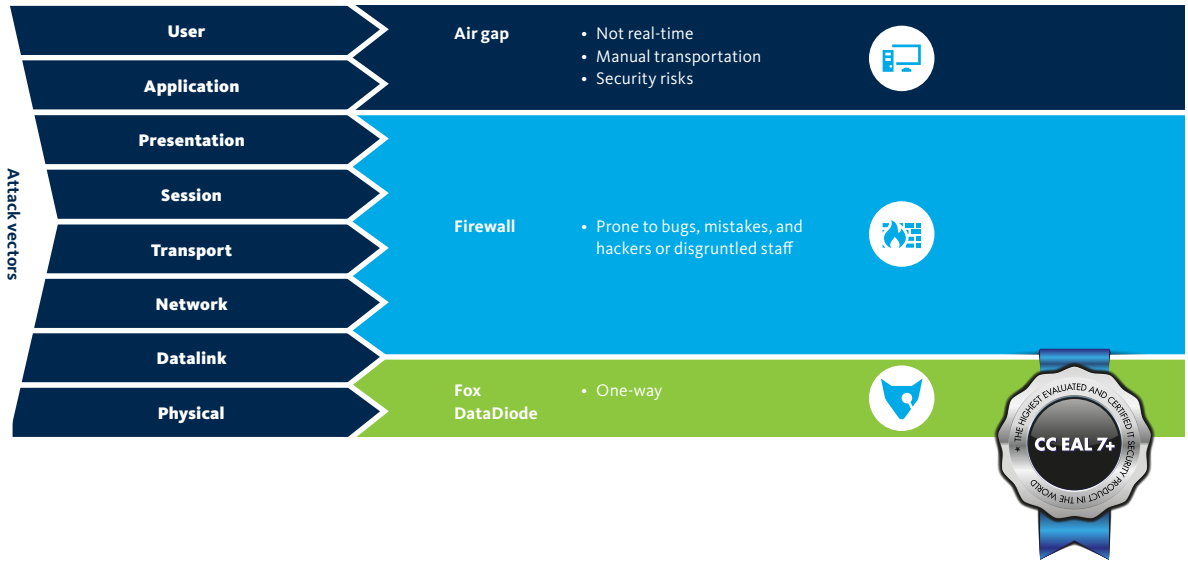
Most protocols are designed for and require two-way traffic and will be broken if traffic is blocked in one direction. If IP traffic in one direction is impossible, then there is no flow control either. For this too a solution is needed.

In principle

A DataDiode can ensure that outbound traffic is impossible. It can prevent leakages of confidential and classified information, but it does not stop incoming traffic which potentially can undermine a protected network. In practice, incoming traffic is first guided through a network with all the necessary security measures, ranging from antivirus to IPS and SIEM. Also, additional techniques are used, such as file format conversion (for example, Word to pdf), to neutralize potentially harmful content. The odds of this happening are minimal, but it is still theoretically possible that, despite all the measures, malware finds its way into a protected network. That said, it is of primary importance to prevent any information from leaving the network.

Proxy Servers for Flow Control

Two proxy servers are used for flow control: one between the incoming traffic and the Fox DataDiode and one between the Fox DataDiode and the shielded network. This allows the data traffic flow to be controlled up to the diode and from the diode to the network. Bridging via the diode goes through a dedicated protocol with the ability to transfer data reliably without receiving feedback.



Extensive testing and actual experience have shown this very short route to be error-free.

Certification
Because the complete Fox DataDiode solution renders outbound traffic impossible, it guarantees against network leaks of confidential and classified information. The Fox DataDiode has the highest certification possible: it is the only CC EAL 7+ certified device in the world and it has received defense certifications from The Netherlands, Germany, the United States, Russia, and India.

Blocking Incoming Traffic
A DataDiode can of course also be set up to work in the other direction: meaning outbound traffic is allowed and incoming traffic blocked. This configuration is common in companies and organizations in the energy, oil & gas, and nuclear sectors, whom demand absolute guarantees that nothing can be disrupted by external traffic. Outbound traffic is used, for example, to send oil rig production data and the like to corporate headquarters. This configuration can also prove useful for defense organizations. Take, for example, cases in which it is necessary to prevent external influences via a network (impacting launchers, for instance), but which harbor no secret information and require outbound traffic.

No Management, Low Cost
As the Fox DataDiode itself is made up entirely of hardware, without software and programmable chips, there is no need for regular updates or device management. This has a very positive impact on the reliability of the device. The savings in maintenance and administration costs alone make the Fox DataDiode a very attractive solution for guaranteed physical shielding of a network.

Fortify and secure your network connections
A wealth of information on the different applications and scenarios for the Fox DataDiode is available on our website. The Fox DataDiode is delivered through a global network of certified and trained partners who are knowledgeable in handling confidential information. For more details, including partner information, please go to www.foxdatadiode.com.

Fox-IT
Fox-IT prevents, solves and mitigates the most serious threats caused by cyber attacks, data leaks, or fraud with innovative solutions for governments, defense agencies, law enforcement, critical infrastructure and banking and commercial enterprise clients worldwide. Fox-IT combines smart ideas with advanced technology to create solutions that contribute to a more secure society. We develop products and custom solutions for our clients to guarantee the safety of sensitive and critical government systems, to protect industrial networks, to defend online banking systems, and to secure confidential data.

FOX IT
part of nccgroup

fox-it.com

Fox-IT B.V.
Olof Palmestraat 6, Delft
P.O. Box 638, 2600 AP Delft
The Netherlands

T +31 (0)15 284 7999
F +31 (0)15 284 7990
fox@fox-it.com

Fox-IT is part of NCC Group.