Tenix Data Diode Based Solutions from HP

White Paper

Introduction.................................................................................................................................................. 2
Components.................................................................................................................................................. 2
Data Diode .................................................................................................................................................. 2
Uni-Directional Network Bridge .............................................................................................................. 2
Data Pump Applications ............................................................................................................................ 2
  File Transfer Application......................................................................................................................... 3
  Email Transfer Application....................................................................................................................... 3
  Data Forwarding Application.................................................................................................................... 3
  Clipboard File Transfer Application....................................................................................................... 3
Content and Anti-Virus checking................................................................................................................ 4
Interactive Link.......................................................................................................................................... 4
Multiple Computer Switch....................................................................................................................... 5
Conclusion.................................................................................................................................................. 6
For more information................................................................................................................................ 7
Call to action.............................................................................................................................................. 7
Introduction

Originally developed to meet the security requirements of the Australian Defence community, the Tenix Data Diode allows data to be transferred from a lower security network to a higher one while guaranteeing the confidentiality of data stored on the higher security network, or provides an outbound connection to a lower security network, while ensuring no connection can be made to the secure network.

The Tenix Data Diode device is certified to ITSEC E6 - the highest level of assurance obtainable under the Information Technology Security Evaluation Criteria.

Used with the Interactive Link Keyboard Switch or Multiple Computer Switch (both of which are also certified to ITSEC E6), users can be given full Interactive access to two different networks, and allowed Cut and Paste functionality from the lower security network to the higher one.

All data transferred can be Content and Anti Virus checked before and/or after transfer across the Data Diode.

Components

Data Diode

The Data Diode is a 100 Mbit/s Fibre optic network device providing a guaranteed one way connection between two networks, with hardware enforced prevention of reverse data flow.

The Data Diode is implemented between two dedicated servers which run the necessary software to route data through the device.

Uni-Directional Network Bridge

The Uni-Directional Network Bridge (UNB) provides the low level connectivity across the Data Diode. UNB software is installed on dedicated servers on either side of the Data Diode.

Data Pump Applications

Data Pump Applications (DPA) provide functionality to transfer data between a source and destination network using the File Transfer Application (FTA) for files and folders; Email Transfer Application (ETA) for Email; Data Forwarding Application (DFA) for Uni-Directional (UDP) Network traffic; or Clipboard File Transfer application and client software (CFT) to transfer Microsoft Clipboard data.

In a basic configuration the DPA is installed and configured on the same dedicated servers as the UNB, however for larger implementations they can be installed on separate servers, leaving the dedicated Data Diode servers to run the UNB.
# File Transfer Application

The FTA DPA allows the administrator to configure any number of source areas on the low side network for automatic transfer to a corresponding area on the high side network. Each of these transfer paths can be configured independently, allowing the administrator to define the period between scans of the source areas and for different priorities to be assigned. Individual transfer paths can be stopped and started either together or independently of each other.

Files and folders can be either transferred, removing the source files in the process; Replicated, leaving the source files in place following transfer; or mirrored, maintaining a mirror of the source area on the destination network.

An archive option also allows a copy of all files and folders transferred across the specified transfer path to be kept on the low side network.

The FTA DPA can also be used to provide a secure means of publishing data either to the internet or business partners, ensuring that no connection can be made into the secure network.

# Email Transfer Application

The ETA DPA allows Email to be routed from the low or source network to the high or destination network.

Used with HP ProtectTools Email Release Manager to provide an assured Email policy release mechanism, and Clearswift content checker, a two way email gateway can also be configured using two separate inbound and outbound ETA DPA systems.

# Data Forwarding Application

The DFA DPA allows UniDirectional network traffic to be routed from the low or source network to the high or destination network.

Data may come from the internet, financial data feeds, news feeds or meteorological data for example, or customer specific applications or devices on the source network.

# Clipboard File Transfer Application

The CFT DPA is used to transfer Microsoft Clipboard data between a PC or Terminal server session on the lower security network to a PC or Terminal server session on the higher one.

The CFT DPA client software provides the user with a ‘drop target’ on their low side desktop, into which files, folders and the clipboard can be dropped. The data is routed to the low side CFT DPA server, transferred through the Data Diode and on to the high side desktop, where it is made available on the clipboard or in the folder configured to receive it.
Content and Anti-Virus checking

Optional Content and Anti-Virus checking, using commercial products, can be configured on both or either side of the Data Diode to check all, or just some transfer paths.

Interactive Link

The Interactive Link utilises the Interactive Link Keyboard Switch (KBS) to allow users of a secure network to access data, applications and services on an insecure network from a single PC or Workstation.

The KBS is a Desktop switch which enables the Keyboard and Mouse input to be switched between a connected PC or Workstation and a lower classification network. The switch has a direct connection to the lower network as well as PS/2 connection to the PC or workstation.

When switched to High, all keyboard and mouse input is passed to the high side PC or Workstation which operates as normal.

When switched to Low, all keyboard and mouse input is routed over the low network to the Interactive Link server on the low side of the Data Diode. Configuration of Interactive Link software on this server, allows the keyboard and mouse input to be directed to a Terminal server or other system on the low network, with the display from that system being transmitted through the Data Diode to the high side PC where it is displayed in an X-Window. The user can switch between low and high, keeping the low side X-Window display on the desktop if desired.

Used with the CFT DPA, the user can also cut and paste data from the lower security session to the higher security desktop.
Multiple Computer Switch

The Multiple Computer Switch (MCS) is a Keyboard, Video and Mouse switch (KVM) which allows users to access two systems of different classifications using a single keyboard, mouse and monitor.

Used with the CFT DPA, the user can also cut and paste data from the lower classification desktop to the higher classification desktop.
Conclusion

HP’s Tenix Data Diode based solutions provide Government, Defence or Commercial customers with the ability to allow users to access physically separated domains from a single desktop or, securely switch between systems on different networks with full Cut & Paste functionality from the lower classification to the higher one.

The solutions can also provide the means to transfer data, Email and network traffic from one network to another, either for data import to a secure network or to publish data from a secure or corporate network to an in-secure or external network.
For more information

www.hp.com/hps/security/products
HP ProtectTools Security Team, 2004

Call to action

www.hp.com/hps/security/products
email: protecttools@hp.com
Tel: +44 (0) 1925 841881