

Solution Summary

Introduction

Organizations often are unwilling to accept the risk of connecting networks operating at different classifications for fear of leaking sensitive or classified data to uncleared and perhaps malicious users. You only have to look in the news to see the latest incidents involving breaches in network security to know that the threat is real. This aversion to connecting networks, however, is in complete contrast to the need for organizations to share information.

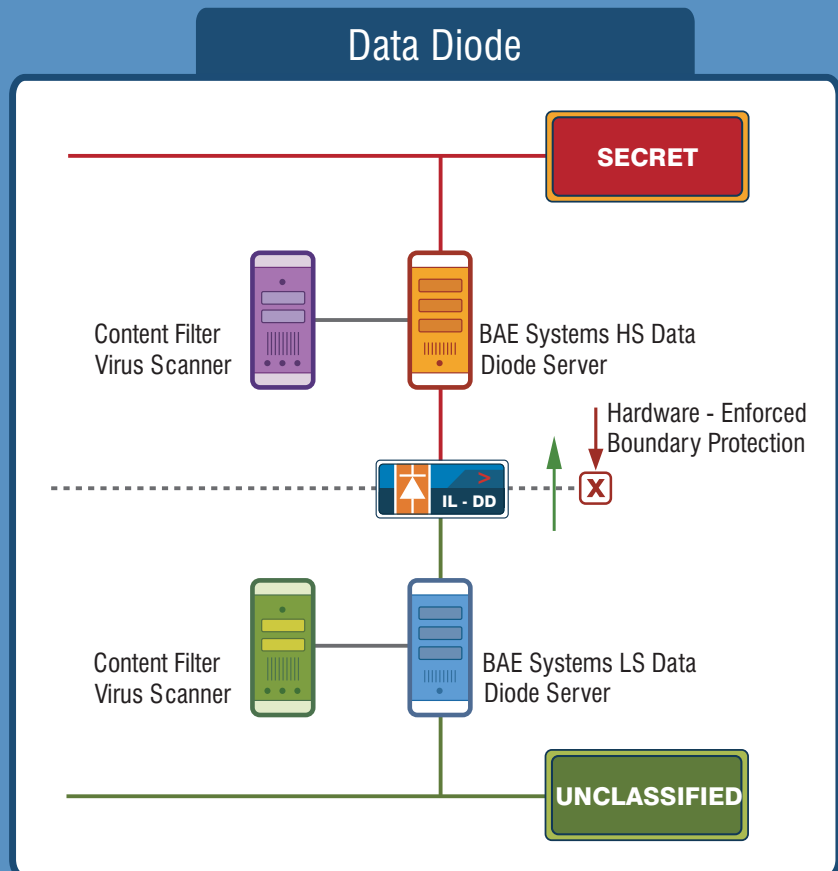
BAE Systems offers a simple solution to overcome this dilemma. Using the Data Diode and Data Pump Applications, an organization can create a system that allows the movement of lower-classification data into higher classifications, yet prevents the flow of data in the opposite direction. This enables the efficiency of real-time data transfers, with absolutely no risk of compromising the confidentiality of sensitive data.

Data Diode

The 100-Mbps and 1-Gbps Data Diode are multimode fiber optic hardware devices that are connected between two servers attached to their respective security domains. Data Pump Applications, installed on these servers, provide a unidirectional mechanism for transmitting different data types through the Data Diode. BAE Systems provides four basic Data Pump Applications that can be adapted for any organization's specific data transfer requirements.

Data Forwarding Application

The Data Forwarding Application (DFA) is a Data Pump Application used for the real-time transfer of IP packets from lower to higher classifications. It is used in environments where an organization needs to transfer streaming data such as video, audio, and sensor data in real time with minimal latency. The DFA works by redirecting IP packets addressed to specific IP addresses and ports on the lower classification and sending them through the Diode to the higher classification. The DFA can support multiple UDP- and TCP-IP streams.



Solution Summary

General product requirements and technical specifications

File Transfer Application

The File Transfer Application (FTA) is a Data Pump Application used for the automated transfer of files from lower to higher classifications. Files placed into a specific source directory on the lower classification are automatically transferred to a corresponding destination directory on the higher classification. The FTA can be configured to support multiple source and destination directories and can operate in four different modes of operation, including "Transfer (Move)", "Replicate (Copy)", "Archive," and "Mirror". Files of any size can be sent through the Diode, although the FTA can be configured with a maximum file size if required. The FTA also can interface with third-party content filters and virus scanners to ensure that no files contain malicious content.

E-mail Transfer Application

The Email Transfer Application (ETA) is a Data Pump Application used for the automated transfer of e-mail from lower to higher classifications. It interfaces with SMTP mail servers such as MS Exchange to allow users on the higher classification to receive e-mail from users on the lower classification. For example, users working within a classified environment can receive both classified and unclassified e-mail in the same inbox, thereby removing the need for the user to monitor both security domains. The ETA also can interface with third-party content filters and virus scanners to ensure that e-mail attachments contain no malicious content.

Keyboard switch

The interactive link-keyboard switch (KBS) operates in conjunction with the Data Diode and allows a user to access two security domains from a single workstation at the push of a button.

Like the Diode, the keyboard switch is a hardware device with its security enforced at the hardware layer.

The KBS connects to a high-side workstation, a low-side network, and a standard keyboard and mouse. Using a session server hosted on the low side, the KBS provides the user with a low-side window that is displayed on the high-side workstation through the Data Diode. The user can switch the keyboard and mouse between classifications by selecting the appropriate button on the KBS. To the user, it appears as though he is operating on a multi-level-security workstation, when in fact the system maintains the separation of the classifications through hardware.

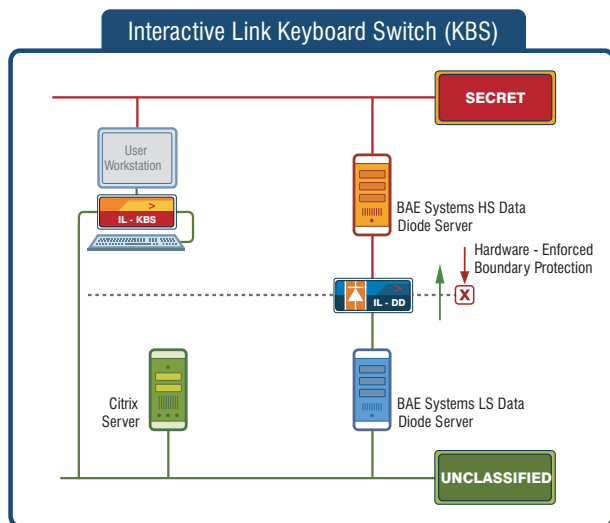
Clipboard and File Transfer Application

The Clipboard and File Transfer Application (CFT) is a Data Pump Application that allows user-initiated transfers of data from a lower-classification session to a higher-classification session. By interfacing with a session's operating system clipboard, the CFT can seamlessly transfer text, images, and files among security enclaves in real time. The CFT can also be configured to allow specific types of clipboard data to be transferred. For example, if only text is to be transferred, the system can be configured to move text data only, stripping out all other formatting. The CFT is best suited to environments where a user has access to multiple security enclaves either through a multi-Level-security system or separate workstations connected via a KVM (keyboard-video-mouse) switch.

Security certification

The BAE Systems Data Diode is the first and only product in the world to be awarded the highest security certification of EAL 7+ under the NIAP Common Criteria scheme.

The BAE Systems interactive link-keyboard switch and Data Diode solution has been awarded the security certification of EAL 5+ under the NIAP Common Criteria scheme.



FOR MORE INFORMATION, CONTACT:

BAE Systems.
1595 Spring Hill Road
Suite 330
Vienna, Virginia 22182
Office: 703 413 6680
Fax: 703 413 6684
www.baesystems.com