SECURE FILES TRANSFER SOLUTIONS

Creating Secure Segregated Networks

ST Engineering

Contents

Importance of Network Segration

Cities around the world are leveraging smart technologies to better operate and manage municipal services. Internet-of-Things (IoT) solutions have been developed to help city service providers manage multiple city services while optimising operational efficiency as well as reducing manpower and maintenance costs.

However, we are also witnessing an exponential increase in cyberattacks resulting in data lost, system downtime, etc. Network segregation is thus extremely important for mission-critical, or sensitive network to counteract network-based cyberattacks. Network-based cyberattacks refer to any form of attacks that enters a secured network via a network or application connection. Many cyberattacks are instrumented through malware embedded in files, and these files may infiltrate the enterprise network via thumb drives, emails, or downloaded from web surfing.

Adopting Data Diodes for Network Segregation

Data Diode is one solution that can be used for data transfer while maintaining the air-gap between the separated networks. In general, Data Diodes work by allowing unidirectional transfer of data while any transfer in the opposite direction is prevented. Data Diodes however, being a unidirectional data transfer solution, may inevitably have issues with data integrity, due to the lack of feedback path. This means that if there is an error during the data transfer process, data packets may be dropped without any retransmission, leading to corrupted files. In addition, like many network solutions, Data Diodes can be challenging to configure or maintain. It is thus important that these are deliberated before the solution is implemented.

ST Engineering Data Diode

High Assurance and Reliability for Files Transfer

ST Engineering Data Diode is designed specifically for data transfer while maintaining the air-gap between the separated networks, i.e. allowing whitelisted network connections to transfer data across the air-gap networks. Any data leakage (or back flow of data) is prevented due to its hardware enforced unidirectional data transfer. ST Engineering Data Diode is CC EAL 4+ certified by Cyber Security Agency of Singapore.

Within the ST Engineering Data Diode, a pair of specially engineered SFP+ (T-module and R-module) ensures that data is transmitted unidirectionally. On the Data Diode Sender, the T-module SFP+ only contains a laser diode, while on the Data Diode Receiver; the R-module SFP+ only contains an optical sensor. This ensures that physically, data will only flow from the Sender to the Receiver, and it is physically impossible for data to flow in the reverse direction, even if the Data Diode malfunctions.

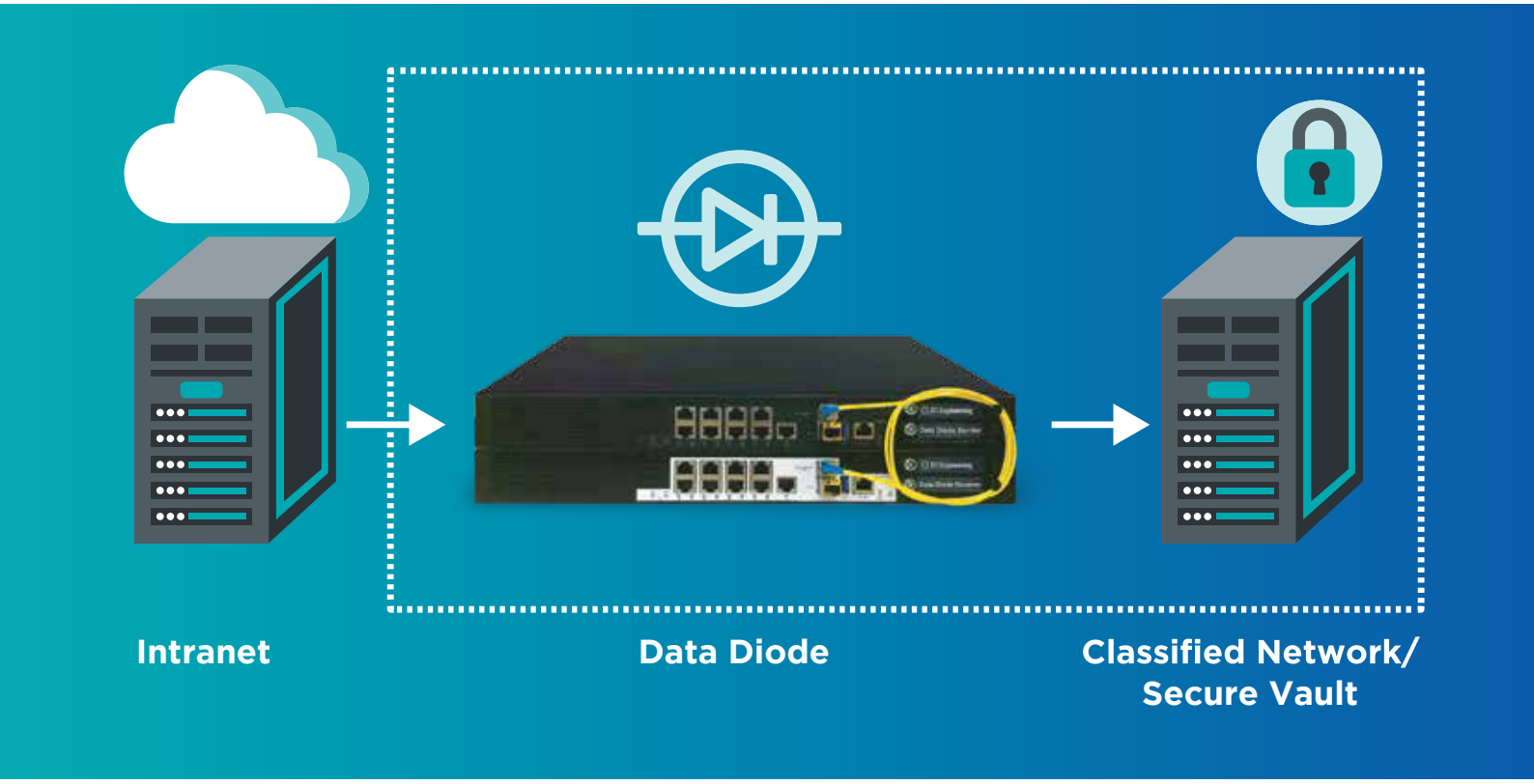

Figure 1 - Deployment of ST Engineering Data Diode for Files Transfer

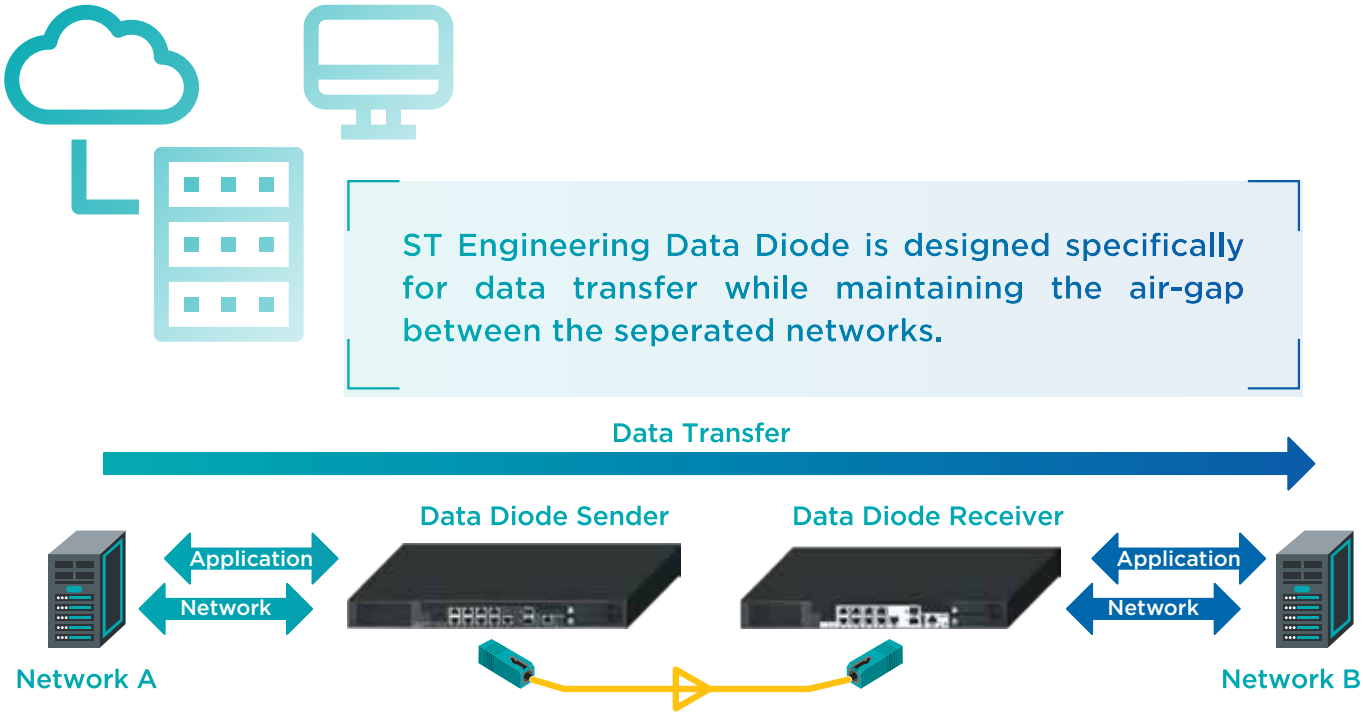

Figure 2 - ST Engineering Data Diode

To verify unidirectional transmission, a simple test using a commercial off-the-shelf SFP+ tester can be performed. Typically, when a pair of regular two-way SFP+ is connected to the SFP+ tester, both ends will show the Transmitted Power and Received Power readings.

However, if the same test is done using a pair of the T-module and R-module SFP+, the R-module SFP+ will return a Transmitted Power reading corresponding to near zero value. Without any output from the R-module SFP+, the transmission can only be unidirectional.

The control of data flow is also enforced at both the application layer (by elective implementation of appropriate data communication protocols) and network layer (by elective implementation of appropriate communication protocols and whitelisting of IP addresses/ports).

When a sending network is connected to the receiving network using the ST Engineering Data Diode, both networks remain independent and isolated. The network scan can only terminate at the Data Diode Sender or Receiver, depending on where the scan is performed. There will not be an instance where a network scan returns a result where both Data Diode Sender and Receiver is shown. Hence, all network-based activities, or attacks, will terminate at the ST Engineering Data Diode.

ST Engineering Data Diode is engineered with high reliability in mind to meet the most stringent operational requirements. It can achieve a minimum end-to-end throughput of at least 500 Mbps for file transfer, with no more than 1 file loss in 5 million files and can transfer files of varying sizes (ranging from a few bytes to more than 50GB). It also has a built-in self-monitoring capability to notify users in the rare event of a file or packet loss.

COMMON CRITERIA CERTIFIED EAL 4+ FC CE UL IPOS INTELLECTUAL PROPERTY OFFICE OF SINGAPORE

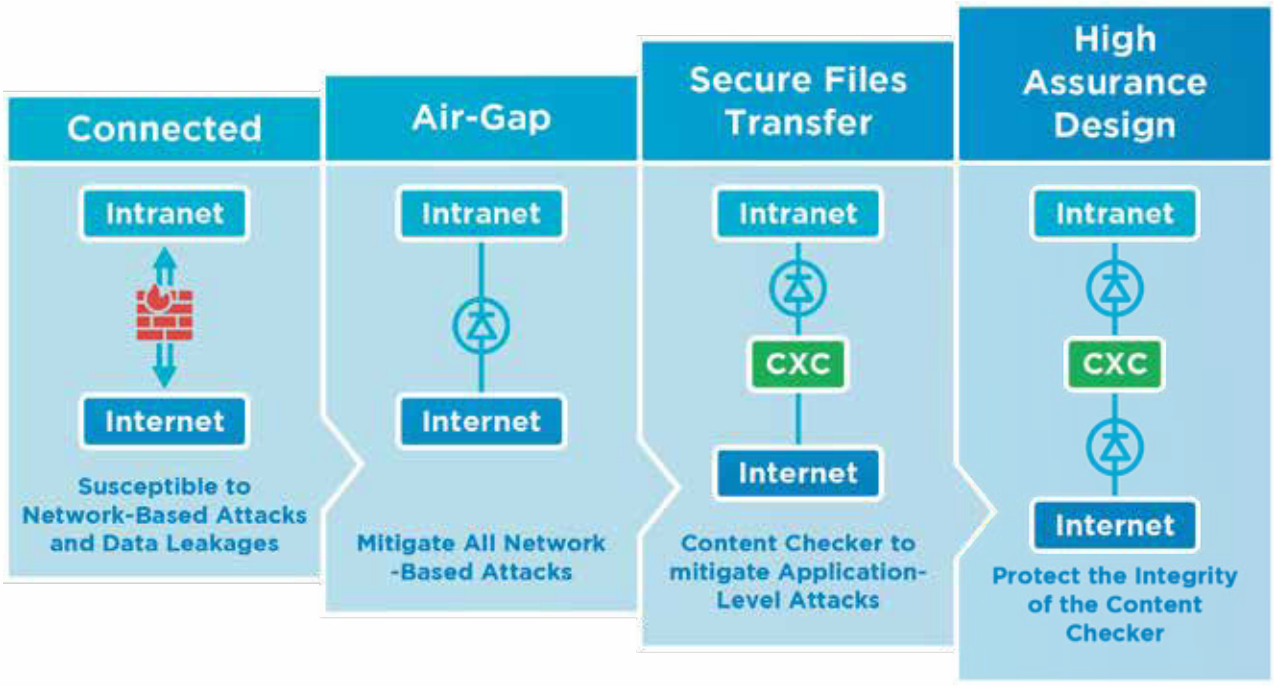

Figure 3 - ST Engineering Data Diode in a High Assurance Guard (HAG) Configuration

From Appliance to Scalable System Solutions

Traditionally, IT professionals deploy firewalls to connect the Enterprise Intranet to the Internet (Figure 3). However, hackers often exploit these firewalls' vulnerabilities and misconfigurations to launch cyberattacks into the Enterprise IT systems.

While ST Engineering Data Diode focuses on high throughput and lossless transmission, it does not ensure that the data being transferred are free of embedded malware or malicious code. The Data Diode mitigates all network-based cyberattacks because all networks and applications protocols are terminated at the Data Diode Sender or Receiver, and only the payload is transferred one-way over the fibre optic connection.

As such, a complementary Files Cleansing (FCS) or Content Checker (CXC) solution is necessary to check the payload for malicious content or data leakages. These solutions can consist of traditional Anti-Virus software, Content Disarm and Reconstruction modules, or Static Code Analysis engines.

For incoming traffic, the FCS needs to be deployed before the Data Diode so that only "safe" content enters the Classified Networks. Another set of Data Diode is instrumented before the FCS to protect its integrity. For outgoing traffic, the CXC will ensure that unauthorized content does not leave and similarly, another set of Data Diode can be deployed to ensure its integrity.

This integrated solution, deployed in a High Assurance Guard configuration, will not only enable trusted networks to be protected from both malware intrusion and information leakage, but also ensure the integrity of the content checker.

As requirements become more demanding or stringent, the solutions transit to scalable system solutions. For example, for enterprises that are required to transfer more than 10 or 100 terabytes of data a day, multiple Data Diodes can be deployed, together with load balancing components. Together, they will ensure that extremely high amount of data can be transferred efficiently and effectively.

Additionally, for extremely sensitive operational requirement where a single file loss cannot be tolerated, a secure feedback path can be engineered, in order to trigger the "retransmission" commands back to the sending system automatically. Similarly, if the throughput needs to be scaled, transmission controllers will be added for load balancing, etc.

These solutions have been widely deployed in organizations, such as intelligence agencies, financial institutes and defence or homeland security agencies, where huge amount of data is required to be transferred between networks of different domains.

A High Assurance Guard (HAG) configuration will enable trusted networks to be protected from malware intrusion & information leakage and ensure the integrity of the content checker.

MITRE ATT&CK

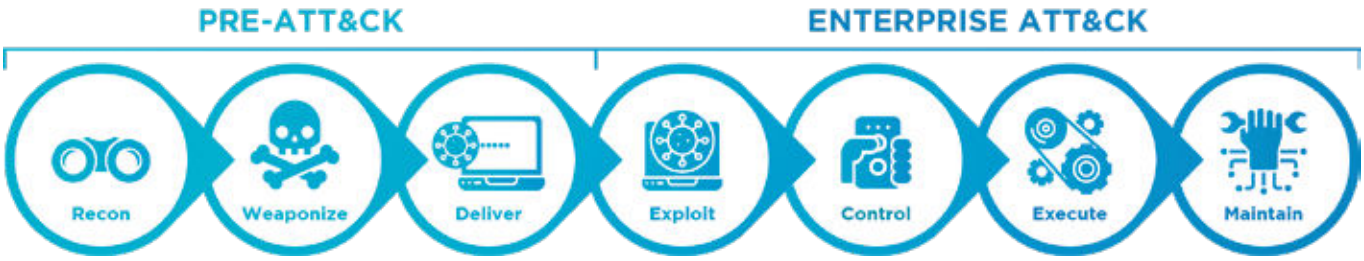

Figure 4 - MITRE ATT&CK Framework

We can follow a hacker tactical activities using the MITRE ATT&CK[1] framework (Figure 4), and analyse how the Secure Files Transfer Gateway can defeat the cyberattacks (Figure 5).

S/No	MITRE ATT&CK	Tactical Activities	Mitigation by Data Diode & Content Checker Module
1	**Recon**	Researching and gathering information about the target bank, e.g. IP addresses, domain names, email addresses, system vulnerabilities, etc.	Data Diode breaks both network (IP, Ports, SSL, etc) and application (SMB, SFTP, etc) layers communication protocols. Hence, hackers can only scan those internet-facing ports and services.
2	**Weaponize & Deliver**	Infiltrating further into the network by acquiring access privileges and upgrading access to penetrate back-office and operational networks	Only whitelisted end-points, and file types can be transferred across the Secure File Transfer Gateway. Any malicious content will be removed by the FCS or CXC.
3	**Exploit & Control**	Infiltrating the network (lateral movement), establishing C&C links back to Mothership, and injecting malware into critical systems.	In the event that the Intranet or Classified Network has been compromised, the hacker will not be able to establish C2 linkages back to the "*mothership*" through Data Diode.
4	**Execute & Maintain**	Exfiltration of data, or detonate ransomware.	Without any access or control, hackers would not be able to execute their objectives, such as detonating ransomware. The CXC conducts deep inspection on all outbound traffic so as prevent any leakage of data.

Figure 5 - Defeating the Cyber Attacks

[1] *https://attack.mitre.org/*

Configuration Made Easy

In summary, ST Engineering Secure Files Transfer Gateways secures and protects the Classified Networks from being exposed to cyber threats from external networks. At the same time, it enables files to be transferred between the networks securely without adding any significant inconveniences or latency. Enterprises will be able to transfer large amount of files efficiently while keeping the cyber threats at bay.

ST Engineering Data Diode is also designed with ease of operation in mind. Each Data Diode Sender and Receiver comes with its own management portal, which allows users to view the status of the Data Diode and the various services at a glance. Configurations such as setting IP addresses, ports or alerts can all be done within the management portal, which makes maintaining the appliance and systems effortless.

ST Engineering Cybersecurity Solutions

As more cities and corporations around the world continue to leverage on improving technologies to better operate and manage services, the amount of data generated will only continue to increase. ST Engineering Data Diode not only allows real time movement of data, it does so while eliminating cyber threats and maintaining the segregation between these networks. ST Engineering Data Diode complements the suite of cybersecurity solutions offered by ST Engineering.

ST Engineering's cybersecurity arm is a pioneering and leading provider of cybersecurity solutions with almost two decades of comprehensive future-ready cybersecurity solutions, forming trust with their customers in national, government, critical information infrastructures, and commercial enterprises. Backed by indigenous capabilities and deep domain expertise in cybersecurity, we offer robust cyber-secure products and services in cryptography, cybersecurity engineering, cross domain solutions, SCADA protection, audit and compliance.

Our team of cybersecurity expertise have designed, built, operated and maintained up to 18 cybersecurity operations centres globally. We also provide cybersecurity professional and managed security services to empower organisations with cyber resilience and increase operational efficiency. To-date, our cybersecurity academy have certified and trained cybersecurity professionals in more than 150 organisations.

References

The MITRE Corporation (2015-2020).
ATT&CK Matrix for Enterprise.
Retrieved from MITRE Web Site:
https://attack.mitre.org

100 Jurong East Street 21
Singapore 609602

(65) 6914 5959

cybersecurity@stengg.com

ST Engineering Info-Security Pte. Ltd.
www.stengg.com/cybersecurity
cybersecurity@stengg.com

V0620