COMBINING DATA DIODES WITH NETWORK FIREWALLS FOR ENHANCED DATA SECURITY

SAMI ADVANCED ELECTRONICS
شركة الإلكترونيات المتقدمة

www.aecl.com

technology developed with

أرامكو السعودية
saudi aramco

CONTENT

EXECUTIVE
SUMMARY

Businesses, government agencies, and other key sectors are rigorously investing in cybersecurity infrastructure as cyber losses are projected to reach a staggering $6 trillion per annum in 2021.[1] The ongoing digital revolution has led to an increase in use of cloud services, cloud service security, smartphones, and the Internet of Things (IoT).[2] This has created a myriad of sophisticated cybersecurity threats that didn't exist a few decades ago. In recent times, the Middle East has witnessed an increase in cyberattacks and hacking activity, owing to increased adoption of digital and smart solutions across banks, financial institutions, and other critical infrastructure.[3]

As part of its Vision 2030, the Kingdom of Saudi Arabia (KSA) is tirelessly working towards accomplishing various localization and digitalization initiatives. The Kingdom has prioritized its cybersecurity initiatives to develop a net of protection around control systems, digital infrastructure, smart devices, and other mission-critical operations. [4]

The current cybersecurity posture is more critical than ever as cyberattacks become increasingly aggressive and powerful. Increased usage of IoT devices has also led to expansion of the attack surface. It is, therefore, crucial for leading sectors and critical industries to adopt cyber technologies that can offer foolproof protection against attacks, breaches, and intrusions. Advanced Electronics Company (AEC), with its core competencies in cybersecurity, developed its local data diode technology for rapid data protection and information transfer. AEC Data Diodes are optimized to protect the Kingdom's critical infrastructure, diverse industrial landscape, and growing digital technologies.

It is worthwhile to note that firewalls have remained an important component of data security. However, firewalls need to be patched and updated on a regular basis to eliminate the possibility of error and misconfiguration. AEC Data Diodes are scaled to work in conjunction with firewalls by overcoming underlying issues with firewalls. Data diodes use physical separation between the host and the destination to prevent external malware to enter the network. Besides, the technology is optimized for unidirectional data transfer to facilitate secure flow of data from secure to insecure networks, and vice versa.[5] With increasing number of networks exposed to vulnerabilities each day, data diodes provide a valuable potential addition to the current cybersecurity toolbox.[5]

FLOW OF

INFORMATION IN THE DIGITAL WORLD

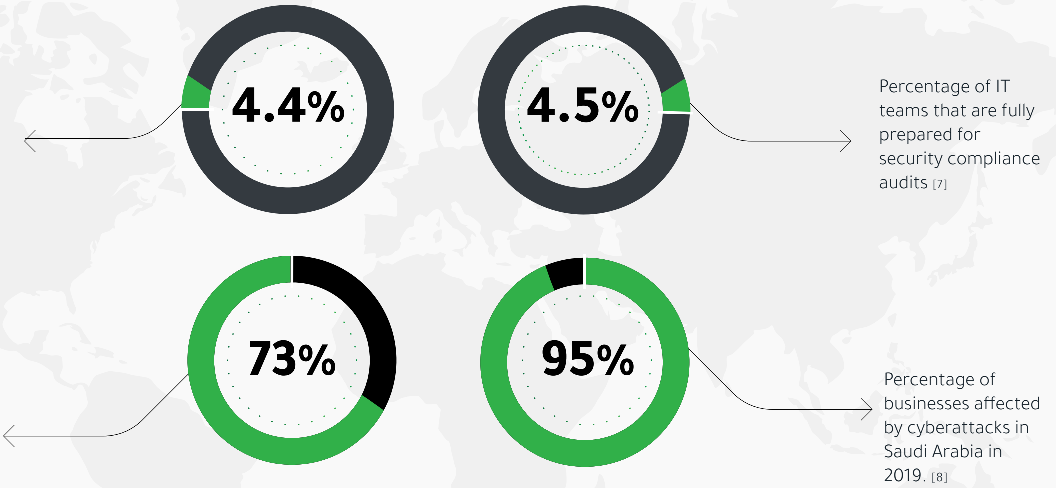
Digital transformation has resulted in an increase in Industrial IoT and the flow of information across business networks.[5] These networks include process control networks and enterprise networks that collectively monitor industrial control systems.[6]

The use of standard communication protocols across high-value networks exposes critical infrastructure components to cyberattacks. [6] These networks store critical data that must be protected from unauthorized access, while also ensuring that proper data flows enable authorized users to receive this data. [2]

A number of attack vectors such as email attachments, malware, viruses, web pages, instant messages, social engineering, and remote access can enter the network to disrupt operations, embezzle data, or initiate illegal usage. Therefore, it is crucial for businesses and organizations to maintain the integrity, confidentiality, and safety of high-value networks. [5]

Protection of security networks makes it crucial for data traffic to pass through network-firewalls. [3] However, vulnerabilities of firewalls have raised concerns related to network security. In this scenario, data diodes can be combined with firewall security to ensure optimal protection against external attacks and data breaches.

STATE OF DATA AND NETWORK
SECURITY ACROSS ORGANIZATIONS



Percentage of IT teams with 100% real-time visibility into network security.[7]

Percentage of IT teams that are fully prepared for security compliance audits [7]

Percentage of black-hat hackers who consider firewalls inadequate [9]

Percentage of businesses affected by cyberattacks in Saudi Arabia in 2019. [8]

The aforementioned numbers are suggestive of the need for more robust and secure technologies for protection of data networks. Businesses can complement their firewall security with flexible, intelligent, and resilient data diodes that can increase network visibility and security.

COMBINING FIREWALLS

AND DATA DIODES FOR FLAWLESS DATA SECURITY

Network firewalls combine complex rule sets to filter incoming information and restrict potential threats.[10] However, despite the proven effectiveness of network firewalls in multiple industries, their two-way communication mechanism exposes security networks to several threat vectors.

To address the aforementioned issues, businesses are combining the synergies of firewalls with unidirectional data diodes that completely isolate the network from external threats, malware, and intrusions.

Data Diodes- Going a Notch Higher with Data Security

The vulnerabilities of network firewalls can be effectively managed through the use of hardware-based data diodes that complement the former.

Firewalls

Data Diodes

Firewall misconfigurations can allow spyware and malware to bypass the firewalls and intrude the network.

Traffic through a firewall can be routed to other computers within a trusted network.[11]

Firewalls have a complex software ruleset to implement and can introduce network latency.[10]

Firewalls require diligent patching, constant monitoring, and assessment of rules to maintain security.[13]

Long-term operating costs for maintaining and auditing Firewall rules and firmware over time is high.[10]

Easily accessible to hackers to develop exploits.[14]

Data diodes can address the anomaly by ensuring physical separation of host and destination, and blocking malware. There have been no reported cases of data diodes being bypassed or exploited to enable two-way transmission.[10]

Traffic through these fiber optic channels is a non-routable proprietary protocol that does not implement the TCP/IP stack.[10]

Data Diodes allow the data to flow in real-time without introducing latency. [12]

Data diodes work without a software rule set, are hard to implement incorrectly, rarely require changes, and are relatively easy to audit.[10]

Businesses can install lesser number of firewalls while investing in data diode technology for improved security compliance.

Difficult for hackers to get a hold of an industrial grade data diode, which makes it very challenging to develop exploits.[10]

ADDING A NEW TIER OF

PROTECTION FOR FIREWALL MISCONFIGURATIONS

Despite the evident complexities of firewalls, organizations across the world confide in the security posture of this software-based technology. With proper compliance, monitoring, and configuration, firewalls can indeed prove to be a strong data protection technology. However, firewall misconfigurations are common across several critical business networks.

99% of firewall breaches will be caused by firewall misconfigurations through 2023.[7]

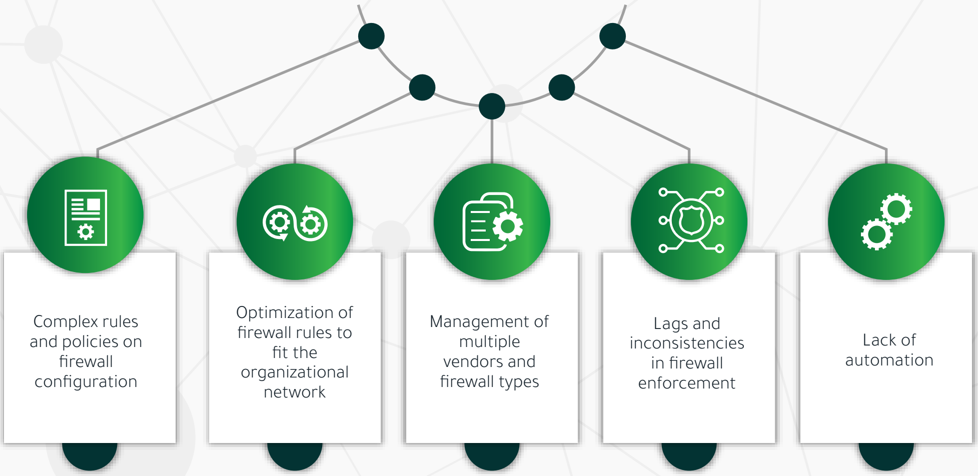
Only 3 out of 10 enterprises have over 80% visibility into their firewall networks.[7]

30% of enterprises use over 100 firewalls.[7]

78% of enterprises use over 3 vendors for enforcing firewalls.[7]

The increasing number of firewalls used across organizational networks, coupled with their vulnerability to misconfiguration, has reduced visibility into network security. In this scenario, use of data diodes for foolproof protection against data breaches has emerged as a parallel security avenue alongside firewalls.

The leading challenges faced by organizations in managing firewalls are:



Complex rules and policies on firewall configuration

Optimization of firewall rules to fit the organizational network

Management of multiple vendors and firewall types

Lags and inconsistencies in firewall enforcement

Lack of automation

Several security experts concur with the idea of using firewalls in conjunction with data diodes in order to ensure optimal data security. As a matter of evaluation, there have been no reported cases of data diodes being bypassed or exploited to enable two-way transmission.[10]

PROGRESSION FROM

AIR GAPS TO FIREWALLS AND DATA DIODES

Attack vectors across the cyberspace are constantly changing, giving hackers greater power in controlling and intruding security networks. Business networks need to map their cyber security journey, and adequately balance the use of air gaps, firewalls, and data diodes.

Traditional Air Gap Security Blocks Information Exchange

Air gaps are physical barriers that completely isolate security networks from the outside world. Therefore, high-security systems are disconnected from low-security systems, protecting the former against malware or data breaches. However, air gaps only offer a half-baked solution by eliminating risks without facilitating utility across the network. Due to complete network isolation, it becomes impossible to transfer real-time information or data across the channel.[15]

◆ **Less than 10% industrial control systems use air gaps as a cybersecurity hack.**[5]

Firewalls follow a more utilitarian approach by managing the connections of various networks through software-based communication protocols. In theory, firewalls offer a secure channel for data exchange and information transfer. However, their software configuration exposes them to a number of vulnerabilities in the form of backdoor attacks, bugs, and misconfigurations.

◆ **36% security teams believe firewall inaccuracies and misconfigurations increase rework time.**[7]

Data diodes offer improved functionality to cybersecurity networks by ensuring secure transfer of data and information. Overcoming the limitations of both air gaps and firewalls, data diodes use hardware separation for protecting networks while using one-way communication to transfer information.

◆ **Considered to be 100% secure, data diodes have not reported any cases of data breach or bypass.**[10]

Air Gaps

- Physical barriers for protection
- No scope for information transfer

Firewalls

- Software-based protection barriers
- Vulnerabilities to threats and malware

Data Diodes

- Physical separation combined with one-way data transfer protocols for information transfer

BUSINESS NETWORK

SECURITY WITH AEC's CROSS DOMAIN SOLUTION

Lack of protocol breaks in firewalls allows all the service functions to work during network communication. However, networks with incompatible security classifications require certain restrictions when data is being transferred to or from sensitive and trusted domains.
AEC's Cross Domain Solution (CDS) imposes these strategic network restrictions to uphold the integrity of proprietary data.

Decoding AEC's Cross Domain Solution: CD-S-E-001

AEC's Cross Domain Solution, CD-S-E-001, enforces two distinct and isolated unidirectional network connections to increase the security level of the company network, while also providing the capability to control and filter the data flow on cross domain networks.

Protection against Infiltration

When data is transferred from high security environment to low security environment

Protection against Exfiltration

When data is transferred from low security environment to high security environment

Upholding the Integrity of Business Networks

- CD-S-E-001 utilizes the principle of bidirectional data flow by enabling two isolated unidirectional streams of data travelling in opposite directions.
- The CDS software accepts/initiates the connection requests as per the protocol functionality and terminates full duplex protocols by permitting only one-way traffic through, in each data flow direction.
- CD-S-E-001 is designed to handle simultaneous high-speed data flows and secure transfer of the data to the specified destination.

AEC's Cross Domain Solution paves the way for transfers that are prohibited by other rigorous data security approaches. Complemented by firewalls, it provides added safety for high security environments. Evolving constantly to meet and defeat equally-evolving cyber threats, CD-S-E-001 continually assures designated levels of information-sharing to support multi-level collaborations across different domains.

CONCLUSION

Organizations are developing and adopting new technologies to share valuable information in an interconnected world. Parallel to this, the threat landscape of business and information networks is also evolving both in volume and complexity. Standard security solutions alone are not enough to avert multifaceted cyber threats. Resilient cybersecurity programs that consist of varying measures for improving the security posture are the need of the hour.

One such proactive and adaptive approach is using firewalls and data diodes together. Firewalls will likely always be an indispensable part of network security. Data diodes, on the other end, overcome the capability gap and provide a more reliable unhackable network. Each have their own strengths, and are suitable in different settings and scenarios. In recent times, the increased vulnerability of software-based firewalls to external attacks has brought data diodes to the fore of the cybersecurity industry. As attacks get craftier, using different tools to work in harmony is the best play to prevent cyberattacks and reduce the resulting loss.

Saudi Arabia's Vision 2030 focuses on building a sophisticated digital infrastructure for advanced industrial activities, while facilitating localization of manufacturing, research, development, and other services. AEC has diversified its offerings in accordance to this vision. Data diodes are one such product that supports the digital transformation journey of KSA by guarding data networks from external threats. With their fundamental qualities, data diodes provide an opportunity to be at the forefront of cybersecurity.

REFERENCES

1. Cybercrime Magazine. 2019. 2019 Cybersecurity Almanac: 100 Facts, Figures, Predictions And Statistics. [online] Available at: <https://cybersecurityventures.com/cybersecurity-almanac-2019/>

2. Upguard.com. 2020. Why Is Cybersecurity Important?. [online] Available at: <https://www.upguard.com/blog/cybersecurity-important>

3. Naseba. 2020. Companies In The Middle East Highly Vulnerable To Cyber Attacks, Says Pwc Study - Naseba. [online] Available at: <https://naseba.com/content-hub/topic/cyber-security-topic/companies-middle-east-highly-vulnerable-cyber-attacks-says-pwc-study/>

4. Arab News. 2020. Aramco, AEC To Develop Kingdom`S First Data Diode. [online] Available at: <https://www.arabnews.com/node/1635101/corporate-news>

5. The Hague Security Delta 2019. Understanding the Strategic and Technical Significance of Technology for Security The Case of Data Diodes for Cybersecurity [ebook] Available at: <https://www.thehaguesecuritydelta.com/media/com_hsd/report/246/document/HSD-Rapport-Data-Diodes.pdf>

6. Web.mit.edu. 2020. [online] Available at: <http://web.mit.edu/ha22286/www/papers/CSIIRW10.pdf>

7. https://www.firemon.com/state-of-the-firewall-report-2019/. 2019. State Of The Firewall. [online] Available at: <https://3hggz2ftdz41fqjfc37yqew1-wpengine.netdna-ssl.com/wp-content/uploads/2019-FireMon-State-of-the-Firewall-Report.pdf>

8. Arab News. 2020. Cyberattacks Hit 95% Of Saudi Businesses Last Year, Says Study. [online] Available at: <https://www.arabnews.com/node/1718596/saudi-arabia>

9. HostingTribunal. 2020. 40 Scary Hacking Statistics That Concern Us All In 2020. [online] Available at: <https://hostingtribunal.com/blog/hacking-statistics/#gref>

10. Sans.org. 2015. SANS Institute: Reading Room - Firewalls & Perimeter Protection. [online] Available at: <https://www.sans.org/reading-room/whitepapers/firewalls/tactical-data-diodes-industrial-automation-control-systems-36057>

11. Watchguard.com. 2020. Positioning Your Firewall. [online] Available at: <http://www.watchguard.com/training/fireware/82/archite8.htm>

12. ROI4CIO. 2020. Data Diode Review, Comparison, Best Products, Implementations, Suppliers. | ROI4CIO. [online] Available at: <https://roi4cio.com/en/categories/category/data-diode/>

13. FireMon. 2017. Misconfigurations: The Firewalls Greatest Threat - Firemon. [online] Available at: <https://www.firemon.com/misconfigurations-firewalls-greatest-threat/>

14. Netsparker.com. 2017. Vulnerable Web Applications On Developers, Computers Allow Hackers To Bypass Corporate Firewalls. [online] Available at: <https://www.netsparker.com/blog/web-security/vulnerable-web-applications-developers-target/>

15. PCMag India. 2018. Black Hat Researcher Shows Why Air Gaps Won't Protect Your Data. [online] Available at: <https://in.pcmag.com/news/124706/black-hat-researcher-shows-why-air-gaps-wont-protect-your-data>

SAMI
ADVANCED
ELECTRONICS
شركة الإلكترونيات المتقدمة

Advanced Electronics Company
King Khalid International Airport Industrial Estate
P.O. Box 90916,
Riyadh 11623, Saudi Arabia

☎ +966112201350 Email - info@aecl.com

/AECSaudiArabia