JUN 2018

In the Boxing Ring

Network Box Technical News

from Mark Webb-Johnson

Chief Technology Officer, Network Box

Welcome to the June 2018 edition of In the Boxing Ring

This month, we are proud to announce, as of the 31st of May 2018, Network Box HQ and HK Security Operations Centres have achieved compliance with the latest **PCI-DSS v3.2** standard. Thus, customers seeking to obtain and maintain PCI-DSS v3.2 compliance can now explicitly list Network Box as a compliant service provider. On pages 2 to 3, we discuss in further detail how Network Box can assist you with your compliance, and also highlight the twelve major requirements for PCI-DSS.

On page 4, we highlight the features and fixes to be released in this month's patch Tuesday for Network Box 5.

Finally, Guardforce has partnered with Network Box to introduce a first-in-the-market solution combining cyber protection and crisis management: **GRID**. Following on from that, Network Box HQ welcomed the Guardforce Global Management Team for a **Cyber Security Seminar**. In addition, Network Box USA was at the **2018 Texas Regional HIMSS Conference**, held at the Hyatt Regency Dallas, in Texas, USA.

Mark Webb-Johnson
CTO, Network Box Corporation Ltd.
June 2018

Stay Connected

You can contact us here at Network Box HQ by email: **nbhq@network-box.com**, or drop by our office next time you are in town. You can also keep in touch with us by several social networks:

https://twitter.com/networkbox

https://www.facebook.com/networkbox
https://www.facebook.com/networkboxresponse

https://www.linkedin.com/company/network-box-corporation-limited/

https://plus.google.com/u/0/107446804085109324633

In this month's issue:

NETWORK BOX

PCI DSS COMPLIANCE

Payment Card Industry Data Security Standard

Network Box HQ and HK Security Operations Centers are proud to announce that, as of 31st May 2018, both have achieved compliance with the latest **PCI DSS v3.2** standard. This means Managed Security Services can now be provided to Network Box customers within the PCI DSS v3.2 framework.

In particular, customers seeking to obtain and maintain PCI DSS compliance can now explicitly list Network Box as a compliant service provider for the following requirements:

- **8.1.5** - Remote Access
- **12.8.1** - Service Provider Listing
- **12.8.2** - Service Provider Responsibilities
- **12.8.4** - Service Provider PCI DSS Compliance Monitoring
- **12.8.5** - Service Provider PCI DSS Requirements

This is in addition to all the other PCI DSS requirements that Network Box has always been able to assist with, including aspects such as:

- Segmentation Control
- Strict Policy Control
- Intrusion Prevention
- Web Application Firewalling
- PCI Compliant TLS Data Protection
- Dual Factor Authentication
- etc.

All this without the requirement for compensating controls.

NETWORK BOX

For those customers subject to PCI compliance requirements, Network Box now have available **PCI DSS v3.2 SAQ-D** compliance information packs for both HQ and HK Security Operation Centers; and are ready to discuss with you, how Network Box can help with your own PCI compliance programs.

As per our PCI charter, Network Box is committed to preserving the confidentiality, integrity and availability of all the physical and electronic information assets throughout Network Box in order to comply with the PCI DSS. Information and information security requirements (specifically those within the PCI DSS) will continue to be aligned with Network Box's goals and the PCI DSS compliance program. The PCI compliance program is intended to enable continued compliance and to reduce information-related risks to acceptable levels. This is in addition to, and complementary with, Network Box's existing triple ***ISO 9001: 2008***, ***ISO/IEC 20000:2011***, and ***ISO/IEC 27001:2013*** certifications.

Over the coming few months Network Box intends to continue the work with the PCI framework, to further simplify the use of the managed security services by PCI compliant customers. We will be producing templated compliance worksheets, as well as testing guidance, to be used by customers and their PCI auditors. We will also be migrating the existing dual-factor authorized PCI Box Office system to our upcoming **NBSIEM+** system (in particular to assist with requirement 8 identification and authentication policies, but also to integrate asset management and vulnerability scanning options). And we will be extending this program out to our other global regional Security Operation Centres.

With 12 primary requirements, and hundreds of sub-requirements, achieving and maintaining PCI compliance is often a huge undertaking for many organizations. It is Network Box's goal to provide our security services in a PCI compliant framework. To lighten the PCI workload on our customers by making it easier to see and test specifically which requirements are met.

The PCI Data Security Standard defines six goals, and 12 specific major requirements to meet those goals:

I) Build and Maintain a Secure Network

1. Install and maintain a firewall configuration to protect cardholder data
2. Do not use vendor-supplied defaults for system passwords and other security parameters

II) Protect Cardholder Data

3. Protect stored cardholder data
4. Encrypt transmission of cardholder data across open, public networks

III) Maintain a Vulnerability Management Program

5. Use and regularly update anti-virus software or programs
6. Develop and maintain secure systems and applications

IV) Implement Strong Access Control Measures

7. Restrict access to cardholder data by business need-to-know
8. Assign a unique ID to each person with computer access
9. Restrict physical access to cardholder data

V) Regularly Monitor and Test Networks

10. Track and monitor all access to network resources and cardholder data
11. Regularly test security systems and processes

VI) Maintain an Information Security Policy

12. Maintain a policy that addresses information security for employees and contractors

By simply replacing the words **'cardholder data'** with **'sensitive data'**, these standards and requirements can apply to any industry and provide a clearly defined framework of best security practices to follow. Network Box Security Response recommends all customers follow this, or similar, security frameworks.

NETWORK BOX

Network Box 5.5

NEXT GENERATION MANAGED SECURITY

On Tuesday, 5th June 2018, Network Box will release our patch Tuesday set of enhancements and fixes. The regional SOCs will be conducting the rollouts of the new functionality in a phased manner over the next 14 days.

Network Box 5 Features
June 2018

This month, for Network Box 5, these include:

- Improve logging for 'base striker' URL extraction in text/HTML email messages
- Enhanced caching support in proxy services (particularly for SSL certificates)
- Improvements to GMS sensor for SCAN services
- New screens to show mail server queue on admin web portal
- Mail server queue force flush and delete actions on admin web portal
- New directed proxy option for FTP client proxy protection
- Improved performance in KIOSK mode authentication
- General release of Network Box 5.5 to all customers
- IDS and IPS engine updates for improved performance and protection capabilities

In most cases, the above changes should not impact running services or require a device restart. However, in some cases (depending on configuration), a device restart may be required. Your local SOC will contact you to arrange this if necessary.

Should you need any further information on any of the above, please contact your local SOC. They will be arranging deployment and liaison.

NETWORK BOX

Network Box
Guardforce Partnership

Guardforce, a leading physical security service provider, has partnered with Network Box to introduce a first-in-the-market solution combining cyber protection and crisis management: GRID. Guardforce Real-time Insured Defense (GRID), augments Network Box's UTM hardware and Managed Security Services, with Guardforce's current security solutions, to provide complete security protection on both physical and virtual levels.

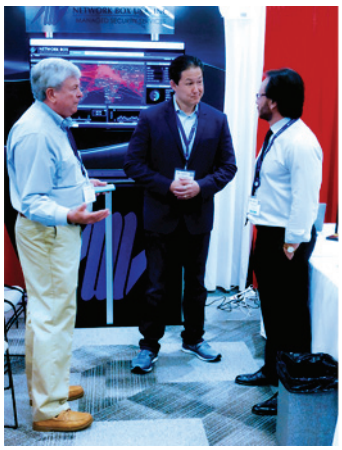
"GRID is a revolutionary product integrating physical and cyber security. GRID is backed by Network Box's exceptional cyber security technology proven over the years to provide all-rounded defence for individual and corporate customers."

Michael Gazeley
Managing Director
Network Box Corporation Limited

LINK: http://www.guardforce.com.hk/en/news/detail/Stay-One-Step-Ahead-of-Hackers_1999

Network Box USA
HIMSS Texas Regional Conference 2018

Network Box USA was at the **2018 Texas Regional HIMSS Conference**, held at the Hyatt Regency Dallas, Texas. During the event, Network Box USA's Chief Technology Officer, Pierluigi Stella, gave a talk titled, "Managed Security in Healthcare: Actual Case Studies," highlighting cyber security concerns specific to the healthcare sector, and case studies with clients who have both been with Network Box USA for over 10 years.



HIMSS TEXAS REGIONAL CONFERENCE

Network Box
Guardforce Cyber Security Seminar

Network Box welcomed the Guardforce Global Management Team to Network Box HQ, for a briefing on the current cyber-security landscape, as well as an in-depth look at the Network Box 5.5 Managed Security platform.

Newsletter Staff	Subscription
Mark Webb-Johnson Editor **Michael Gazeley** **Kevin Hla** Production Support **Network Box HQ** **Network Box USA** Contributors	Network Box Corporation nbhq@network-box.com or via mail at: **Network Box Corporation** 16th Floor, Metro Loft, 38 Kwai Hei Street, Kwai Chung, Hong Kong Tel: +852 2736-2083 Fax: +852 2736-2778 www.network-box.com