JAN 2017

In the Boxing Ring

Network Box Technical News

from Mark Webb-Johnson, CTO Network Box

Welcome to the January 2017 edition of In the Boxing Ring

Season's Greetings and Happy New Year to you all! 2016 was another great year for Network Box. In addition to winning multiple international awards, which takes our total number of awards to over 130; Network Box participated in various IT and Security events, was featured in numerous media outlets, and hosted many security seminars. This, and other key milestones of 2016 are highlighted on page 6, together with a link to **Year in Focus 2016**, our end of year summary of Network Box news and events.

Also this month, we discuss **PCI Security Standards**. The Payment Card Industry Data Security Standard *(PCI DSS)* is a proprietary information security standard for organizations that handle branded credit cards. On pages 2 to 4, we discuss in detail the various approaches that Network Box has taken to ensure PCI DSS compliance.

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

Finally, Network Box is proud to announce that Network Box USA was listed in CIO Review's **20 Most Promising DDoS Solutions Provider** for 2016.

Mark Webb-Johnson
CTO, Network Box Corporation Ltd.
January 2017

You can contact us here at 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:

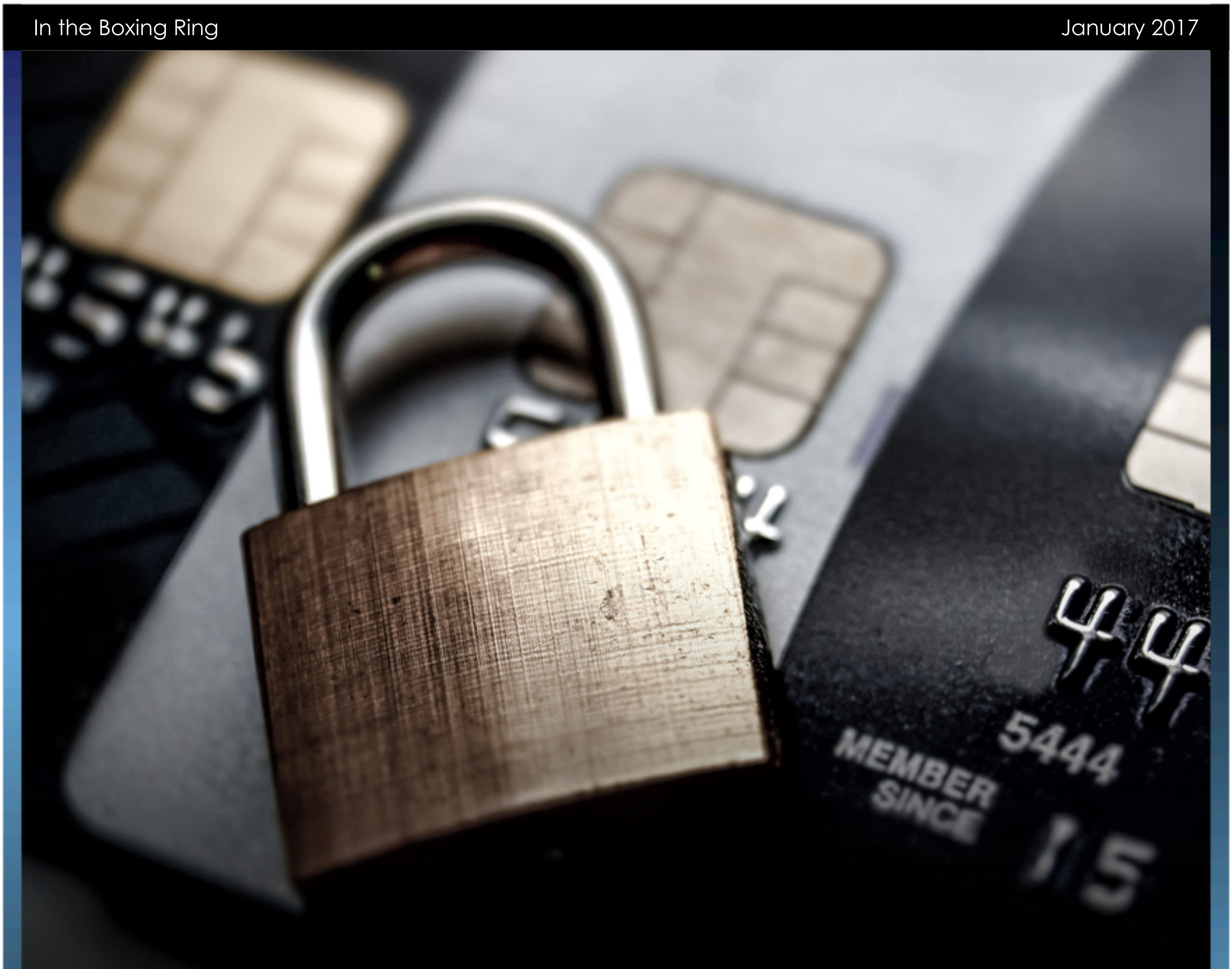
twitter http://twitter.com/networkbox

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

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

Google+ https://plus.google.com/u/0/107446804085109324633/posts

In this month's issue:

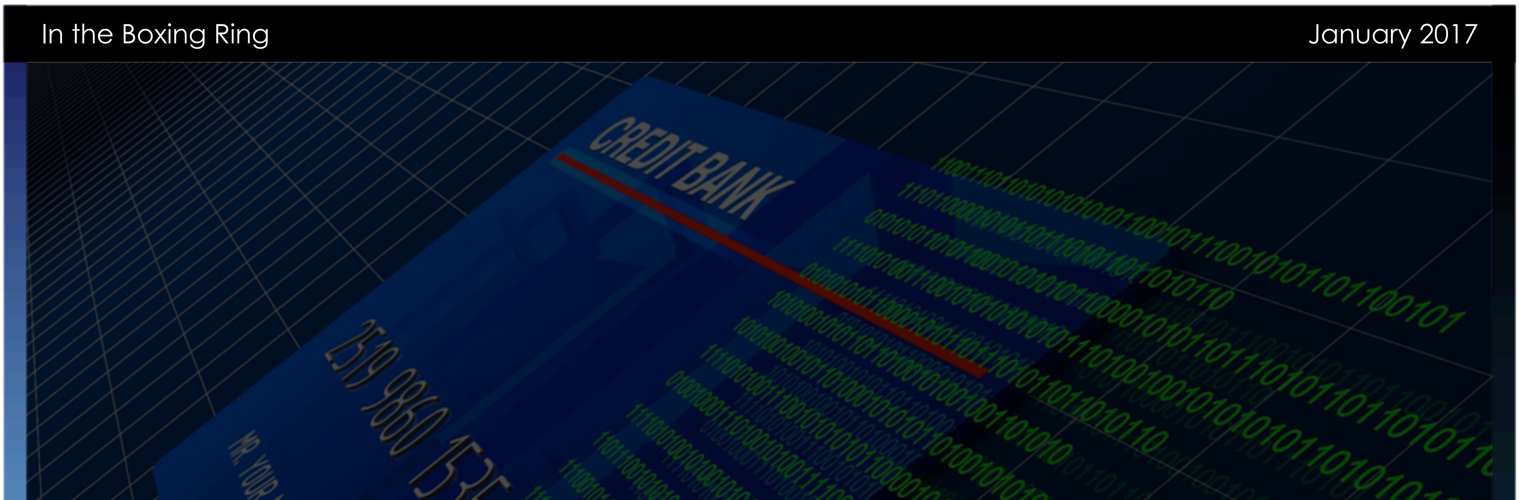


PCI Security Standards

While Network Box does not directly store or process credit card information, a large number of our customers do, and that brings them under the PCI Security Standard. Network Box, as service provider, seeks to assist our customers with gaining and maintaining their PCI compliance.

Since the release of the PCI Data Security Standard (DSS) v3.1, emphasis has been made on the use of SSL/TLS encryption technology and of obsoleting older cryptographic protocols. The PCI Security Standards Council has been leading the way in this respect. In particular, current standards obsolete the use of all versions of the SSL protocol, as well as early versions of the TLS standard. The latest PCI DSS v3.2 has similar requirements.

With effect from January 2017 Patch Tuesday, Network Box is making available a set of tools and standard configurations to ease conformance with PCI DSS standards.



Box Office

We recognize that some customers are listing us as a Service Provider for their PCI DSS documentation, and despite the absence of processing of credit card information, that brings our Box Office support systems into the PCI framework. However, we have to balance this requirement with the problem that Box Office is a public service and we have little control over the web browsers our customers are using to access the service. In particular, the PCI v3.1 requirement for disabling of TLS 1.0 on such public services in onerous. Google, Facebook, Department of Homeland Security, US CERT, to name just a few; all currently enable TLS 1.0 on their public web services.

What we have arranged, can be summarized as follows:

- All Network Box public services available today use SHA256 certificates.
- Our Intranet service (used by NOC staff) uses a PCI v3.1 and v3.2 compliant profile of only secure ciphers with forward secrecy. SSL, TLS 1.0, and TLS 1.1 are all disabled.
- For customers requiring a PCI v3.1/v3.2 compliant support system today, we offer a portal https://pci.boxoffice.network-box.com/ that uses a PCI v3.1 and v3.2 compliant profile of only secure ciphers with forward secrecy. SSL, TLS 1.0 and TLS 1.1 are disabled. This portal can be configured as required on a per-user basis (see My Account, under Box Office). Using this portal will meet PCI v3.1 and v3.2 requirements.
- Our Box Office main portal https://boxoffice.network-box.com/ uses a PCI v3.1 and v3.2 mitigating profile of only secure ciphers with forward secrecy. SSL disabled, but TLS 1.0 1.1 and 1.2 are enabled. Our regional mirrors (ap, us, and eu) will be migrated to this same system early in 2017.
- We anticipate disabling TLS 1.0 and 1.1 completely on all Box Office mirrors later in the first half of 2017. At that point, only modern browsers will be able to access these services. This matches the plans of most major public services.

Network Box 5

Today, Network Box 5 offers two on-the-box web accessible services using SSL/TLS technology; the Admin and User web portals:

- Both portals use SHA256 certificates.
- Up until now, both admin and user web portals have used a PCI v3.1 and v3.2 mitigating profile of only secure ciphers with forward secrecy, SSL disabled, but TLS 1.0, 1.1 and 1.2 enabled.
- In this month's January 2017 patch tuesday, we will be migrating all customers by default to a PCI v3.1 and v3.2 compliant profile of only secure ciphers with forward secrecy. SSL, TLS 1.0 and TLS 1.1 will be disabled. This can still be changed on a per-box, per-service, basis; but the default will be full compliance with PCI v3.1 and v3.2 standards.
- To ensure the highest level of security, all customers should ensure that they are using modern browsers when accessing these admin and user web portal services.

In addition, Network Box 5 offers several SSL/TLS enabled functions (such as VPNs, SSL Proxy, SSL CA, etc):

- Since 2015-04 patch Tuesday, all Network Box SSL CA certificates have used SHA256.
- Since 2016-06 patch Tuesday, all Network Box SSL proxy CA certificates have used SHA256.
- Network Box certificates issued before that date, can simply be renewed on the Network Box console, to upgrade to SHA256.
- The security profile for services using SSL/TLS is individual configured at service creation time, according to customer requirements. For simplicity of configuration, we include two default profiles:
  - pci31: a PCI v3.1 and v3.2 compliant profile of only secure ciphers with forward secrecy. SSL, TLS 1.0 and TLS 1.1 are disabled.
  - pci31m: a PCI v3.1 and v3.2 mitigating profile of only secure ciphers with forward secrecy. SSL is disabled, but TLS 1.0, 1.1 and 1.2 are enabled.

Network Box 3

Organizations subject to PCI compliance, and conforming to PCI DSS v3.1 or later, should not be using the Network Box 3 platform. Network Box 5 has been designed specifically to protect the SSL/TLS protocols, and provides a much more effective platform for compliance with the latest PCI DSS standards.

Today, Network Box 3 offers two on-the-box web accessible services using SSL/TLS technology: The my.network-box.com and Mail Portal systems:

- Both portals use SHA256 certificates (valid until April 2019).
- Today, both portals use TLS profiles with SSL disabled, and only TLS v1.0 offered. We mitigate with a restrictive cipher list of only medium and high security ciphers, to provide the best browser compatibility.

For Network Box 3, we suggest the following:

- The SSL/TLS use in Network Box 3 is limited to the my.network-box.com administrative and user portals. These systems are typically used only within a LAN environment (protected by firewall from external access). It is not usual for the user portal system to be used in a PCI environment.
- There should be no credit card information stored or accessed from these systems. The systems merely provide access to statistical and other log information for the network itself.
- We recommend that the my.network-box.com administrative system be firewalled to only accessible from a defined set of workstation source IP addresses. In addition, we have configured a restrictive set of TLS ciphers to be available on these interfaces.
- The Network Box 3 end-of-sale date was 1st February 2016, and no new systems should be installed after that date.
- All existing Network Box 3 systems should be migrated to Network Box 5 before the end-of-support date in 2018.

Mitigation and Migration Plan

For Network Box 5, given the January 2017 patch tuesday change to default to a PCI v3.1 and v3.2 compliant SSL/TLS profile, there should be no need for mitigation. If required, the following can be used:

- All Network Box 5 systems should be updated, by default, to use a PCI v3.1 and v3.2 compliant SSL/TLS profile, in January 2017.
- If further mitigation is required, we recommend that the admin web portal be firewalled to only accessible from a defined set of workstation source IP addresses.

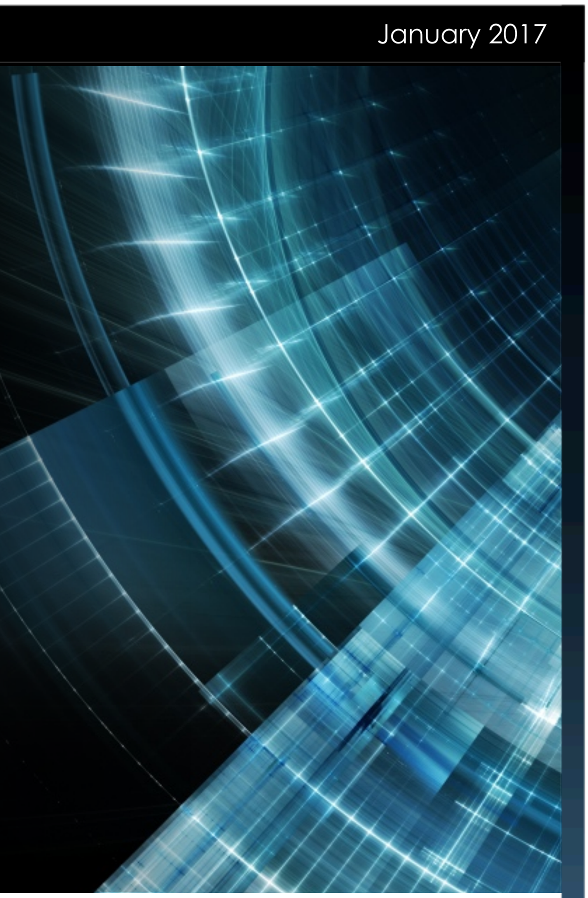
Conclusion

Network Box is committed to supporting our customers with their PCI DSS compliance activities. We regularly audit our systems to ensure our own compliance with the standards, and now offer standard profiles for one-click compliance.

As of the January 2017 patch Tuesday, by default all Network Box 5 services will be configured as PCI DSS v3.1 and v3.2 compliant. For those customers listing Network Box as a service provider, we also offer the PCI v3.1 and v3.2 compliant portal https://pci.boxoffice.network-box.com/ for ticketing and support.

Network Box 5

NEXT GENERATION MANAGED SECURITY



On Tuesday, 3rd January 2017, 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

January 2017

This month, for Network Box 5, these include:

- Improvements to software update procedure following hard drive replacement
- Support disabling of IPv6 protocol for DNS name server (for deployments not requiring IPv6)
- A new GMS sensor to track mail queue levels, for those using the mail-server security module
- PCI v3.1/v3.2 SSL/TLS profiles, for ease of deployment into PCI environments
- Enhancement to VPN tunnels to permit configuration of MTU size
- Improved validation of eMail address in admin and user web portals
- Improvements to calculation method for KPI "Top SPAM Recipient" related to messages with multiple classifications
- Admin portal now, by default, complies with PCI v3.1 and v3.2 (modern browsers supporting TLS v1.2 now required)
- User portal now, by default, complies with PCI v3.1 and v3.2 (modern browsers supporting TLS v1.2 now required)
- Minor improvements to admin web portal related to widget scrolling and window sizing
- Improvements to layout of KPI report
- Fix to re-scheduling of reports straddling daylight saving time changes
- New configurable behaviour for sender/ recipient as envelope, message header, or both

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.

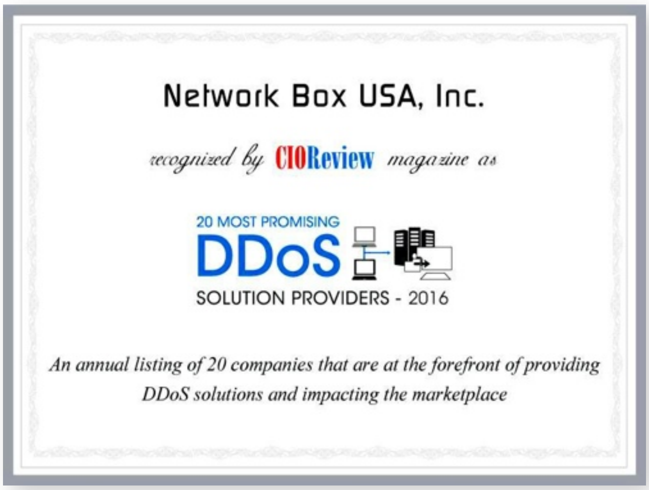
Should you need any further information on any of the above, please contact your local SOC. They will be arranging deployment and liaison.

Network Box ISO 9001 / ISO 20000 / ISO 27001 certified Security Operations Centre, ensures that customers' networks are protected against cyber threats, 24x7x365.

Network Box USA

20 Most Promising DDoS Solution Providers for 2016

Network Box USA was named in CIO Review's 20 Most Promising DDoS Solution Providers for 2016. A select panel of CEOs, CIOs, VCs, and CIO Review's editorial team analyzed offerings from numerous DDoS solutions providers in the USA, to determine the listing. Criterion for the list was based on offerings, competence, customer testimonials, achievements and recognition.



Network Box USA, Inc.

recognized by CIOReview *magazine as*

20 MOST PROMISING DDoS SOLUTION PROVIDERS - 2016

An annual listing of 20 companies that are at the forefront of providing DDoS solutions and impacting the marketplace

Network Box

Year in *Focus* 2016

2016 was another great year for Network Box. Over the past twelve months, Network Box 5 won numerous awards around the globe. These included the **Cybersecurity Excellence Award** from the USA, the **IT Innovation Award** from Germany, and at the Silicon Valley Communications **Info Security Global Excellence Awards**, Network Box received the Grand Trophy and two Gold awards.

Network Box also participated in various international IT and Security events including the **China IT Expo (CITE) 2016**, **Cloud Expo Asia 2016** in Singapore, the **ITx 2016 Expo** in New Zealand, **Microsoft – Deloitte Cyber Security Event** held in Indonesia, and **it-sa 2016** in Germany.

In addition to the many awards and events, Network Box was featured in various media outlets, and held numerous cyber security seminars throughout the year. And finally, 2016 also saw the launch of the new **Network Box Mobile App**, which is available as a free download in the Apple iTunes AppStore and Google Play Store.

For all the highlights of 2016, please click the link below to view Network Box's *Year in Focus 2016*:

http://www.network-box.com/sites/www.network-box.com/files/files/Year_in_Focus_2016.pdf

YEAR in FOCUS 2016
Network Box highlights and events in 2016
NEXT GENERATION MANAGED SECURITY

Newsletter Staff

Mark Webb-Johnson
Editor

Michael Gazeley
Nick Jones
Kevin Hla
Production Support

Network Box HQ
Network Box USA
Contributors

Subscription

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