APR 2017

In the Boxing Ring

Network Box Technical News

from Mark Webb-Johnson, CTO Network Box

Welcome to the April 2017 edition of In the Boxing Ring

This month, we will be releasing a new security enhancement to the Box Office portal, to include **Dual Factor Authentication**. Traditionally, only a username and password was necessary for authentication, however, standard bodies, such as PCI v3.1 standard, are now enforcing more secured methods for authentication. In pages 2 to 3 we highlight the changes that we have implemented to comply with these new standards.

Also this month, the US-CERT released a note questioning the process of **TLS/SSL Interception**. Whilst they made some valid points, they failed to address the benefits of TLS/SSL interception and the dangers of leaving it to the end-user to make the correct choice. In pages 4 to 5, we present our case for HTTPS Interception and how, if done correctly, can strengthen TLS Security.

On page 6, we highlight the features and fixes to be released in this month's patch Tuesday for Network Box 5.

Finally, Network Box Germany, in association with technology partner Tarox, was at CeBIT 2017, held in Hannover, Germany. In addition, Network Box Managing Director, Michael Gazeley, was interviewed by RTHK about the latest IT-related issues.

Mark Webb-Johnson
CTO, Network Box Corporation Ltd.
April 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

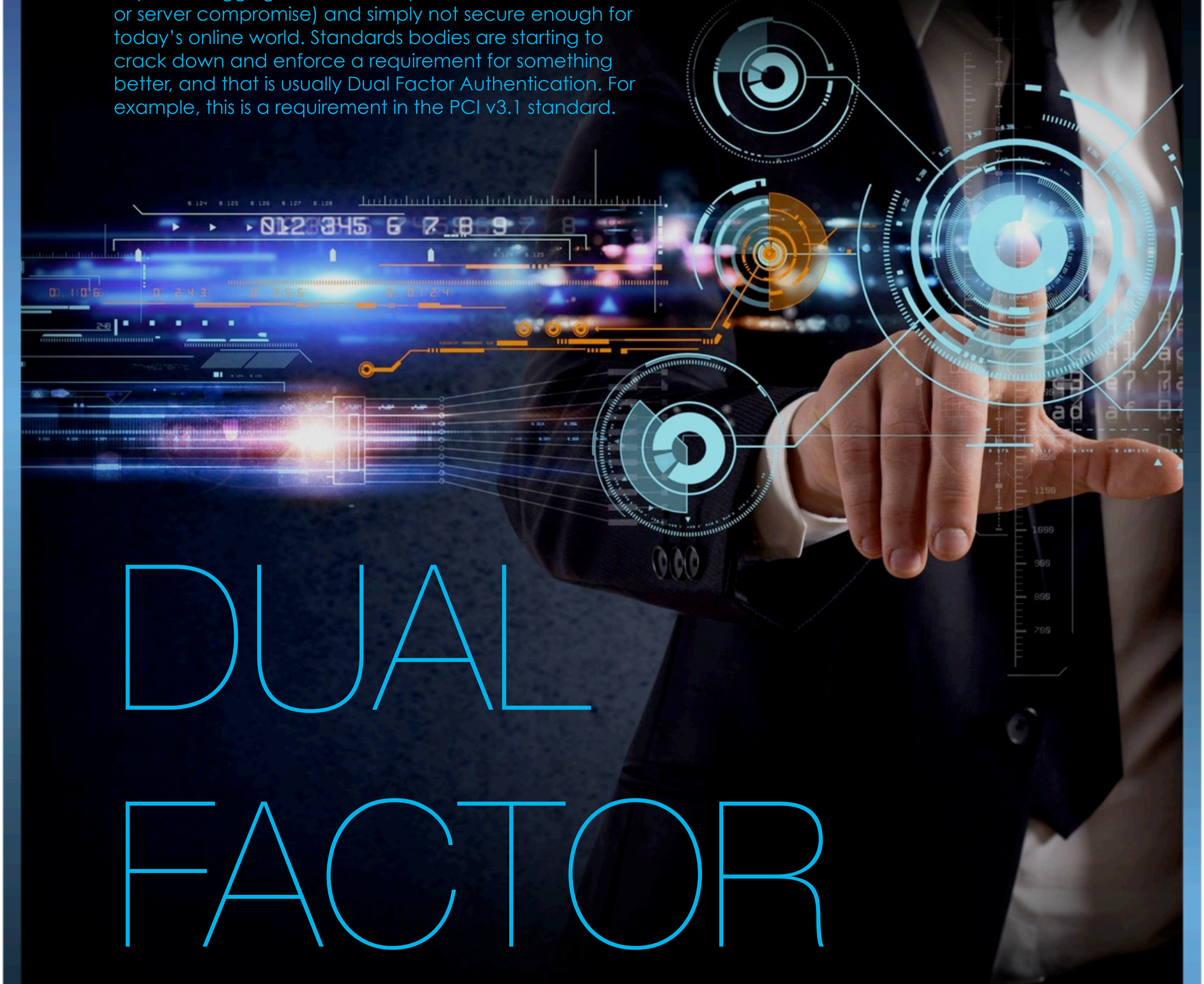
LinkedIn http://www.linkedin.com/company/network-box-corporation-limited

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

In this month's issue:

NETWORK BOX

Over the years, we've become accustomed to traditional username + password authentication. However, this has been shown to be too simple to compromise (via keystroke logging, traffic interception, brute force attacks, or server compromise) and simply not secure enough for today's online world. Standards bodies are starting to crack down and enforce a requirement for something better, and that is usually Dual Factor Authentication. For example, this is a requirement in the PCI v3.1 standard.



DUAL FACTOR BOX OFFICE

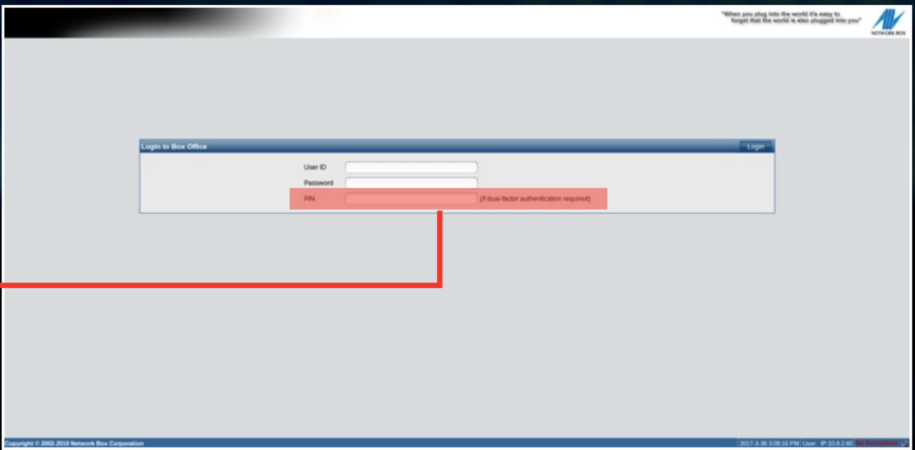
Recently, an open standard RFC6238 has emerged for the TOTP (Time-Based One-Time Password Algorithm) Dual Factor Authentication mechanism. This is simple to implement, and provides excellent enhanced security on top of the usual username+password. There are a number of freely available smartphone apps (the most popular perhaps being Google Authenticator) that support RFC6238 TOTP authentication.

Along with our work for PCI v3.1 and v3.2 compliance, Network Box introduced our own RFC6238 compliant TOTP support in our Network Box 5 product. Dual Factor Authentication can now optionally be used for Admin Web Portal access to Network Box 5 boxes, as well as for services such as VPN access. Today, we bring that work to Box Office and announce Dual Factor Authentication support for Box Office using RFC6238 compliant TOTP.

The following is a summary of changes to the Network Box Box Office portal:

Login Screen

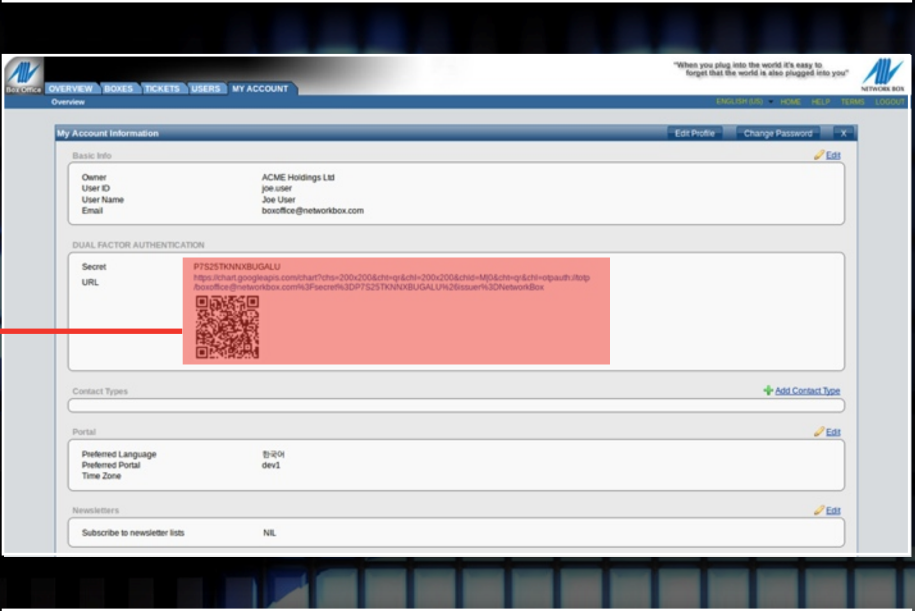
The Box Office login screen has been changed to show a Dual Factor Authentication entry field, in addition to the usual username and password. For accounts with Dual Factor Authentication required, that must be used during login. For others, it can simply be ignored.


"When you plug into the world it's easy to forget that the world is also plugged into you"
NETWORK BOX
Login to Box Office
Login
Copyright © 2002-2010 Network Box Corporation

User ID
Password
PIN (if dual-factor authentication required)

My Account

The My Account screen has been extended to show the TOTP secret so that the user can put that into their smartphone TOTP application.



Basic Info

Owner	ACME Holdings Ltd
User ID	joe.user
User Name	Joe User
Email	boxoffice@networkbox.com

DUAL FACTOR AUTHENTICATION

Secret	P7S25TKNNXBUGALU
URL	https://chart.googleapis.com/chart?chs=200x200&cht=qr&chl=200x200&chld=M|0&cht=qr&chl=otpauth://totp/boxoffice@networkbox.com%3Fsecret%3DP7S25TKNNXBUGALU%26issuer%3DNetworkBox

Contact Types

Portal

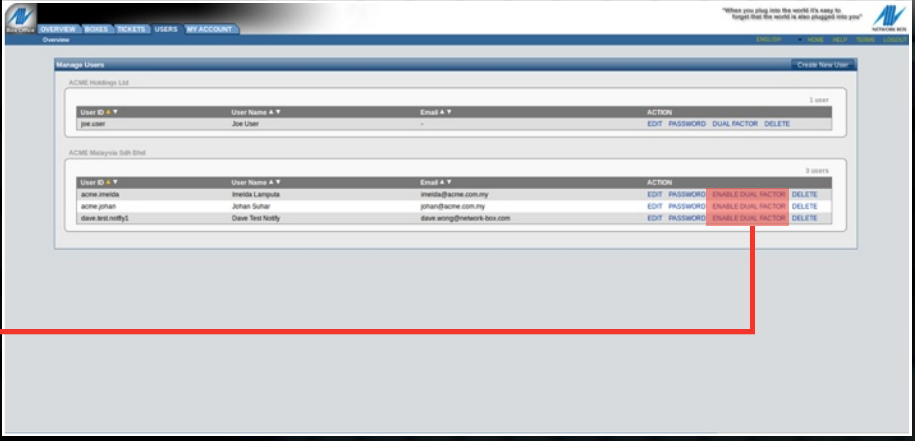
Preferred Language	한국어
Preferred Portal	dev1
Time Zone	

Newsletters

Subscribe to newsletter lists	NIL

User Module

The USERS account maintenance screen has been extended to provide customer administrators the capability of enabling dual factor authentication for their users.



ACME Holdings Ltd

1 user

User ID ▲▼	User Name ▲▼	Email ▲▼	ACTION
joe.user	Joe User	-	EDIT PASSWORD DUAL FACTOR DELETE

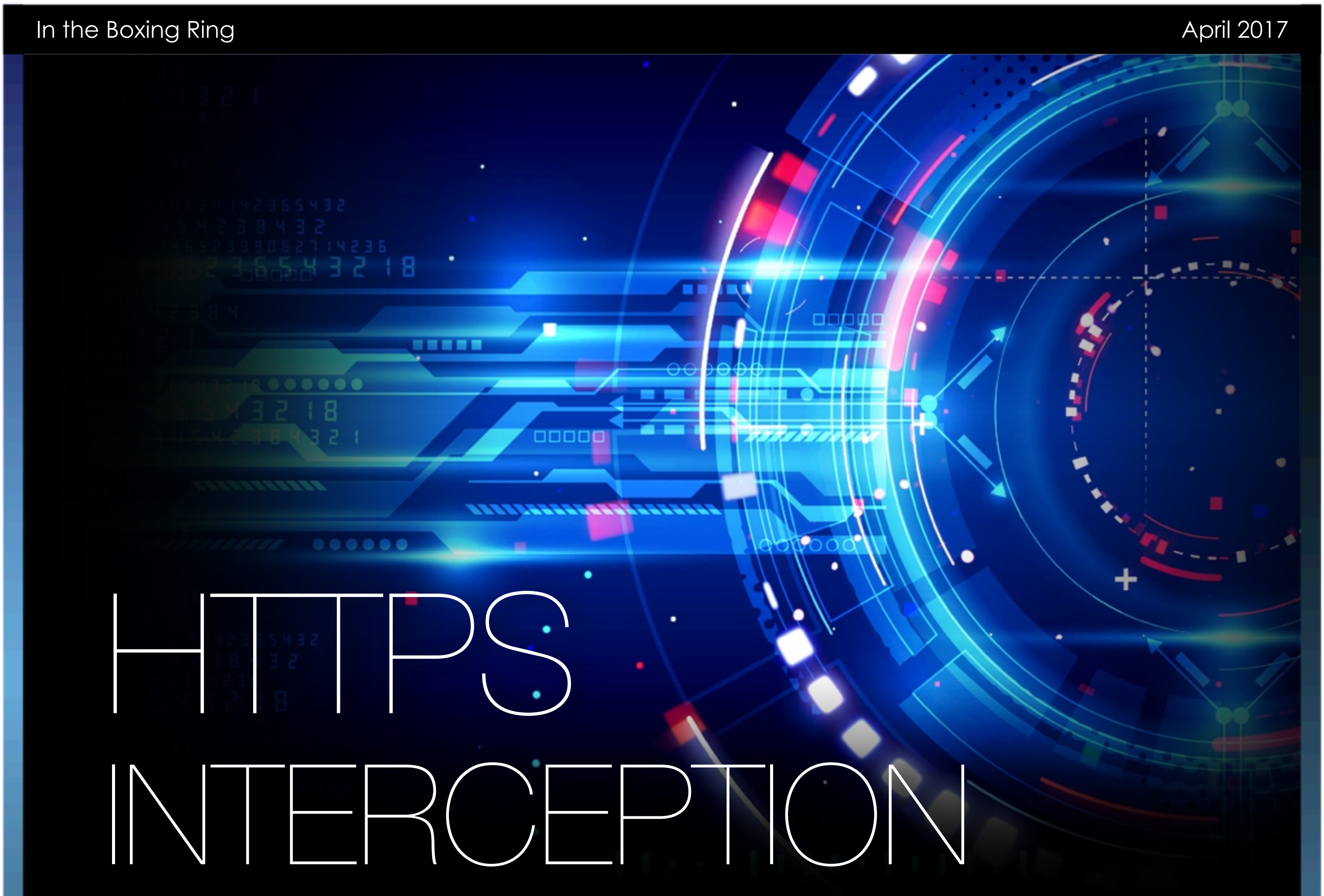
ACME Malaysia Sdn Bhd

3 users

User ID ▲▼	User Name ▲▼	Email ▲▼	ACTION
acme.imelda	Imelda Lamputa	imelda@acme.com.my	EDIT PASSWORD ENABLE DUAL FACTOR DELETE
acme.johan	Johan Suhar	johan@acme.com.my	EDIT PASSWORD ENABLE DUAL FACTOR DELETE
dave.test.notify1	Dave Test Notify	dave.wong@network-box.com	EDIT PASSWORD ENABLE DUAL FACTOR DELETE

The usual workflow for this would be that a NOC engineer, or customer administrator, would ask a new user to login to Box Office. Once the user has confirmed they are logged in, the engineer/administrator would then enable Dual Factor Authentication on that user's account. The user would then go to My Account to see his TOTP secret that can then be scanned (as a QR code) into their smartphone TOTP application. The user then logs out, and tries to login again (this time using their smartphone to generate the TOTP PIN code that they enter into the login screen).

This functionality will be deployed globally to all Box Office mirrors on Thursday 6th April 2017.



HTTPS INTERCEPTION

(when done right) strengthens TLS security

The US-CERT recently released a note (TA17-075A) raising questions about the process of TLS/SSL interception. While many of the points raised in that document are valid, both the benefits of TLS/SSL interceptions and the dangers of relying on end-users to make the correct choices were left out. So, here we present the case for TLS/SSL interception, and 5 reasons it may be suitable for your organization.

1. Without interception at the gateway, there is little protection at the gateway

TSL/SSL is, by definition, strongly encrypted. Without interception, and decoding of that traffic, there is very little that a gateway protection device can do to protect you from malicious traffic in these TLS/SSL encrypted streams. No anti-malware. No content filtering. No anti-spam. No intrusion detection or prevention. etc.

Last year, a study by the GeorgiaTech Institute for Information Security and Privacy showed that 49 percent of Internet traffic is encrypted (up from just 13 percent in 2014). 24 of the top 50 web sites encrypted their traffic by default, and that number rises to 42 out 50 after login to those sites. Without TLS/SSL interception at the gateway, none of that traffic can be protected to ensure that it conforms to organizational policy and is free of malware or intrusions.

2. Relying on end-users to make security decisions is a very bad idea

Study after study has shown that end-users cannot be relied upon to make security decisions. When presented with a security violation dialog box, end-users will choose the option that allows them access to what they want, with little regard for the security implications. Perhaps the issue is lack of education in network security, or simply a lack of understanding of the implications, but the results are clear.

For example, in a study conducted by Carnegie Mellon University among 409 participants, the researchers found that the majority of respondents would ignore warnings about an expired SSL certificate. The more tech-savvy the user, the more likely they would be to ignore it. Of the 50 percent of users polled who could identify the term "expired security certificate," 71 percent said they would ignore the warning. Of the 59 percent of users who understood the significance of a "domain mismatch" warning, 19 percent said they would ignore the hazard.

3. Centralized policy control is an appropriate solution to the problem

Policy control at the gateway is performing an admirable job for unencrypted traffic. Organizations using such systems can define a central policy and control the categories of websites their users visit (both for security, as well as acceptable behaviour reasons), and they can implement effective front-line control against malware, spam, intrusions, and other such malicious activity.

To extend such control to encrypted TLS/SSL traffic requires TLS/SSL interception. Once intercepted, and decrypted, the traffic becomes subject to the same policy control as unencrypted traffic.

4. Security upgrades at the gateway to the Internet

Often an organization cannot upgrade to the latest security technology on each and every workstation, server, and IoT device in their network. Network Box 5 SSL Proxy offers an effective mechanism to upgrade such traffic as it enters/leaves the network. For example, low-security ciphers can be used by devices on the internal network, but that traffic is upgraded to high-security ciphers at the Network Box 5 gateway before it reaches the public Internet.

In other cases, a new security vulnerability is announced and protection can be effectively implemented at the gateway, without having to urgently upgrade the TLS/SSL protocol stacks on hundreds of devices in the network. TLS/SSL exploits such as BEAST, CRIME, FREAK, HEARTBLEED, etc, have all been effectively protected against by such gateway level security upgrades.

5. Not all web browsers and TLS/SSL clients are created equal

While the TLS/SSL certificate verification, ciphers, and protocol support in the latest Chrome or Safari browser may be wonderful, our networks today also have a large number of devices on them running TLS/SSL clients / servers that are not so up-to-date. This is particularly true for IoT style devices and custom applications. When was your conference room smart TV last updated or included in a security audit?

Unifying the TLS/SSL security policy and implementing it at the gateway offers the identical leading TLS/SSL protection to all devices.

The Problem of Testing

The problem of testing a TLS/SSL interception product, as described by US-CERT, is however not so easy.

When a client connects directly to a server, it is simple to see the protocols and ciphers chosen, as well as protection afforded. It is simple to test.

However, when a TLS/SSL interception product is used, the connections client->interceptor and interceptor->server are separate. Without access to both ends of the connection (both client and server) and a clear understanding of the effect of the interception, it is much harder to test.

For example, a cipher negotiation problem on a direct client->server connection is simple to see as it occurs during the TLS/SSL negotiation phase. But, how would such a problem be seen with interception? Would the interceptor reflect the error during TLS/SSL client side negotiation, or would it delay it until after server negotiation had completed, simply shut down the connection, reflect the error back as a layer 7 protocol message, or simply silently upgrade the ciphers according to policy?

Conclusions

Intercepting TLS/SSL can be a great way to improve security and implement effective policy control for this encrypted traffic. Network Box is committed to providing the most complete and effective TLS/SSL policy control at the gateway. We talked about this in detail back in the summer of 2015, and suggest you read these two articles, for more background information on the issue and how TLS/SSL interception can improve the security of your organization:

Proxying SSL (part 1 of 2)

Proxying SSL (part 2 of 2)

Network Box 5

NEXT GENERATION MANAGED SECURITY

On Tuesday, 4th April 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

April 2017

This month, for Network Box 5, these include:

- Improvements to identification of specific disk at fault, by GMS sensor
- Introduction of a policy rule to control console client connections
- Improvements to database optimisation and performance on transactional tables
- Performance improvements in database tracking of static data
- Improvements to identification and allocation of logging vs proxy CPU utilisation
- Provide a configurable control for option of cipher suite preference
- Improvement to reliability of UDP syslog logger output, particularly in non-switched networks
- Optional TCP support for syslog logger output
- Improved support for CDN distribution of threat signatures and updates
- Change section title of KPI Report "Mail Classifications" from "Mail Classification"
- Introduce an administrative console command to help in identification of spam trap candidates
- Extensions to KPI for spam traps
- Introduce policy control for customisation of SSL/TLS certificate verification behaviour
- Enhanced proxy support for cipher preference (as part of SSL profile)
- Performance improvement in SSL proxy, via introduction of a SSL context cache
- Improved PDF unpacker for text and images, as part of mail scanning
- Enhancement to envelope verification of empty username portion of recipient eMail addresses

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 Germany
CeBIT 2017

Network Box Germany, in association with Technology partner, Tarox, was at CeBIT 2017. Over 200,000 participants attended the five day expo held at the Hannover Exhibition Grounds Messegelände, in Germany.

During the conference, Network Box Germany's General Manager, Dariush Ansari, participated in a forum, hosted by CRN TV, to discuss the latest technology trends and innovations. To view the video, please use the link below:
http://www.crn.de/videos/video-a3d7f44caada901324f79faf20b2ddf1.html

Network Box Hong Kong
Media Coverage: RTHK

Network Box Managing Director, Michael Gazeley, was interviewed by Radio Television Hong Kong (RTHK), a public broadcasting service of Hong Kong, about the latest security-related issues. Please click on the links below to listen:

WikiLeaks and Role of CIA

In RTHK Radio 3's current affairs program, Back Chat, Michael Gazeley discusses the implications of the latest WikiLeaks revelations, regarding the cyber-monitoring capabilities of the CIA. The bottom line is simple, get your networks, computers, and devices, properly secured today.

LINK:
http://www.rthk.hk/radio/radio3/programme/backchat/episode/417077

Loss of Voter's Data

Michael Gazeley discusses the theft of two laptops, containing Hong Kong's 3.7 million voters' information. Much of this voter data included: ID Card number, address, mobile phone number, etc., is exactly what's used by banks and credit card companies, to 'prove' a 'customer' is who they say they are. This incident highlights the need of people in Hong Kong needs to be extremely vigilant about the increased possibility of identity theft.

LINK:
http://www.rthk.hk/radio/radio3/programme/backchat/episode/417101

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