NOV 2016

In the Boxing Ring

Network Box Technical News

from Mark Webb-Johnson, CTO Network Box

Welcome to the November 2016 edition of In the Boxing Ring

This month, we discuss the issue of **PUSH vs PULL vs Online Signatures**. One of the key technologies that distinguishes Network Box from other security vendors is that Network Box offers true realtime PUSH updates, which allows every device to updated in an average time of less than 45 seconds. On pages 2–3 we highlight the latest enhancements to the system.

Also this month, we are releasing an update to the **Admin and User Portal** that will allow end users easier access to the Dashboard. This is highlighted on page 3.

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

Finally, Network Box Singapore was at **Cloud Asia Expo 2016**, held at the Marina Bay Sands Convention and Exhibition Centre; Network Box Germany participated at the largest IT Security Event in Germany, **IT-SA 2016**; and Network Box Managing Director, Michael Gazeley was interview by various news outlets.

Mark Webb-Johnson
CTO, Network Box Corporation Ltd.
November 2016

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:

PUSH VS PULL VS Online signatures

Network Box has always pioneered the use of the PUSH, as opposed to PULL, method of signature distribution. It is quite simply the better way of doing the job.

Most other security vendors configure their devices to poll (PULL) for updates once an hour or so, while Network Box SOCs deliver updated signatures in real time as soon as we get them, and within 45 seconds globally. Then, once we've downloaded the signature updates, we install them, and check that they are working and up-to-date; all automatically and in real time.

With the Network Box 5 platform, we've improved our PUSH update technology even further by introducing record-based, in addition to file-based, updates for incredibly granular delivery of new protection signatures.

However, there are times when even this is not fast enough - especially for cases where the size of the signature database is massive and cloud based. For that, we have the Network Box 5 reputation services which offer online real-time lookup of the reputation of file hashes, IP addresses, email addresses, URLs, etc. This month, we're proud to announce the release of three new reputation services for Network Box 5 customers:

1. **NBL** - The Network Box IP address reputation service
2. **EBL** - The Network Box email address reputation service
3. **UBL** - The Network Box URL reputation service

Each of those databases is updated in real-time from the Network Box Security Response OUTBREAK system - tracking the status of millions of threat metrics from both our own as well as partner systems. Each system provides reputation confidence scores for malware, spam and policy classifications. The reputation scores themselves are distributed to the Network Box Cloud DNS system; typically once every 3 seconds. Network Box 5 boxes access these reputation scores over the public DNS system, in real-time.

It is our Security Response Team and the Managed Services we provide that continue to differentiate Network Box from other security providers. Not relying on just PUSHing the latest threat protection signatures to managed devices, we continue to expand on our online reputation services where appropriate.

ADMIN and USER web portal access via names

The admin and user web portals are typically accessed via the IP address of the box, using the ports 4242 & 4244 (for HTTP), and 4243 & 4245 (for HTTPS), respectively.

With the November 2016 release of Network Box 5 firmware, we are also now offering an optional automatic re-direct to allow access to the web portals, for users behind Network Box protection, using the DNS names admin.network-box.com and user.network-box.com. The access URLs offered are now:

Admin Web Portal

- http://admin.network-box.com/
- https://admin.network-box.com/
  (for TLS/SSL secure access)

User Web Portal

- http://user.network-box.com/
- https://user.network-box.com/
  (for TLS/SSL secure access)

This is in addition to the existing kiosk.network-box.com (for Captive Portal kiosk mode authentication).

Network Box 5

NEXT GENERATION MANAGED SECURITY

On Tuesday, 1st November 2016, 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
November 2016

This month, for Network Box 5, these include:

- Introduction of a facility for system ACLs (ACLs whose contents are PUSHed from Network Box Security Response)
  - ❖ **“automated"** system acl for automated domains
  - ❖ **“ocsp”** system acl for domains used to serve Certificate Revocation Lists, or OCSP, for SSL/TLS
  - ❖ **“sslpinned”** system acl for domains that use SSL pinning technology
- Support DNS zone (domain) forwarding in the base security module (moved from dns-server security module)
- Provide a facility for reboot/shutdown of device from admin web portal
- Provide a facility for scheduling of automatic shutdown/ reboot at user-defined time
- Introduce an optional hardware watchdog facility
- Introduce a restriction to not permit personal whitelisting (where sender and recipient is the same)
- Enhancement to the Global Monitoring System (GMS) to allow granular control of each sub-sensor in a GMS sensor
- Introduction of a facility to allow the suppression of a GMS fault for a defined period of time
- Improvements to IKE2 support in IPSEC VPNs
- Admin Web Portal support for admin.network-box.com
- User Web Portal support for user.network-box.com
- Mail scanning support for EBL reputation service
- Mail scanning support for NBL reputation service
- Mail scanning support for UBL reputation service
- Improved support for unpacking of RAR archives in mail scanning
- Mail scanning anti-spam support for whitelist/ blacklist based on either envelope or message header senders/recipients
- Performance improvements in URL scanning on E-4000i, E-8000i and E-16000i class devices
- Introduce a facility to run Web Client policy rules at SNI bypass stage for SSL/TLS connections (provides a facility to deny connections in HTTPS protocol, for policy enforcement, even without decoding SSL traffic)

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 Singapore
Cloud Expo Asia 2016

Network Box Singapore was at this year's Cloud Expo Asia, held at the Marina Bay Sands Expo and Convention Centre, Singapore. During the event, attendees were introduced to Network Box's Managed Cloud Protection.

Newsletter Staff

Mark Webb-Johnson
Editor

Michael Gazeley
Nick Jones
Kevin Hla
Production Support

Network Box HQ
Network Box UK
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

Network Box Germany
IT-SA 2016

Network Box Germany, in association with TAROX, participated at IT-SA 2016, the largest IT Security Exhibition and Conference in the German speaking world, and certainly one of the most important IT Security Events anywhere across the globe.

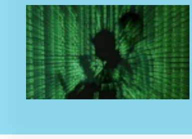
Network Box
Media Coverage

Due to the recent surge in cyber security issues, Network Box Managing Director, Michael Gazeley, was interview by various news outlets.

RTHK 香港電台

LINK:
http://programme.rthk.hk/channel/radio/programme.php?name=radio3%2Fbackchat&d=2016-10-26&p=514&e&m=episode

South China Morning Post



LINK:
http://www.scmp.com/tech/article/2039584/chinas-xiongmai-tech-admits-product-flaws-contributed-cyberattack-us-sites