In the Boxing Ring JULY 2020

Network Box Technical News

from Mark Webb-Johnson
Chief Technology Officer, Network Box

Welcome to the July 2020 edition of In the **Boxing Ring**

This month, we are talking about **Core Engine Upgrades**. As part of this quarter's Patch Tuesday, we are releasing updates to three of our core security engines: *IDS/IPS*, *Anti-Malware*, and *SSL VPN*. On pages 2 to 3, we discuss these upgrades in greater detail and how they improve the performance of the Network Box 5 platform.

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

In other news, Network Box is excited to announce our latest revision to the **M-255i** hardware unit. Additionally, Network Box has published an executive summary video of our Security Incident and Event Management (**NBSIEM+**) system. And finally, Network Box gave a cybersecurity talk titled, *'Managing your cyber risk for remote working,'* for members of the **HK Institute of Human Resource Management**.

Mark Webb-Johnson
CTO, Network Box Corporation Ltd.
July 2020

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

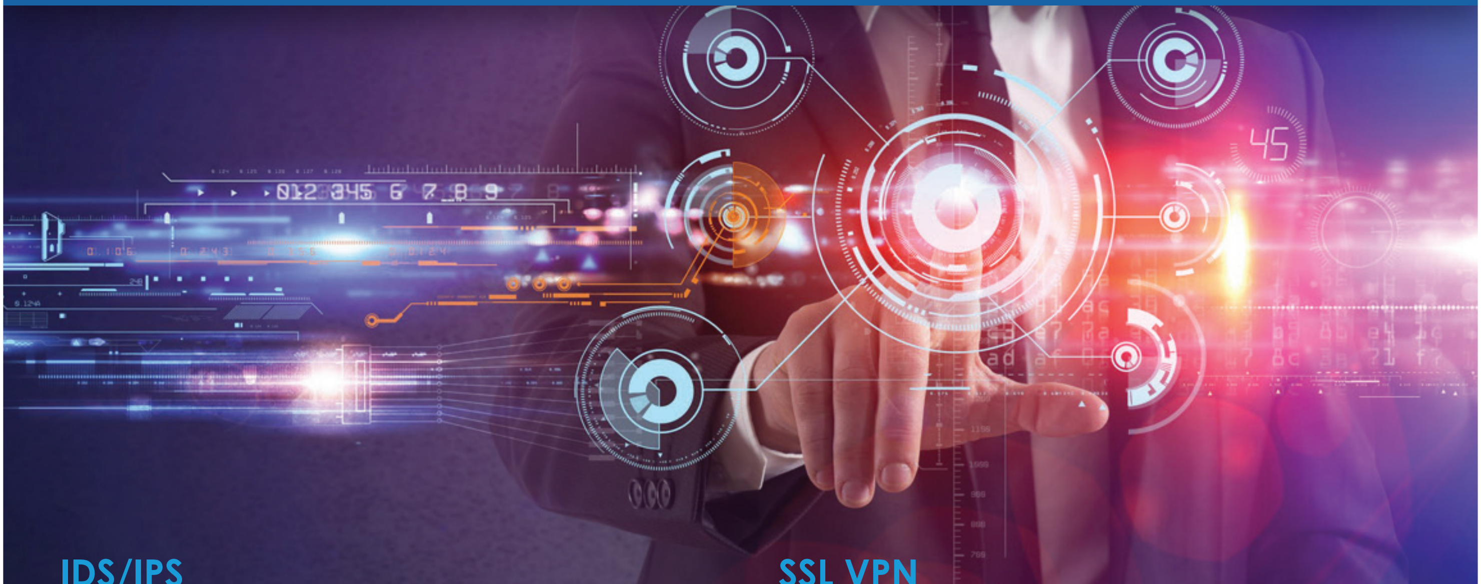
https://www.facebook.com/networkbox
https://www.facebook.com/networkboxresponse

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

https://www.youtube.com/user/NetworkBox

Network Box CORE ENGINE UPGRADES

As part of our ongoing improvements to the Network Box 5 platform, in this month's Patch Tuesday, we are releasing updates to three of our core security engines.



IDS/IPS

Our Anti-Intrusion Detection and Prevention (IDP) engine can operate in one of three modes: Detect+Alert, In-line Prevention, and Active-Response Prevention. All three methods share a core set of intrusion signatures, and heuristics, with more the more aggressive signatures enabled in the Detect+Alert mode (where false positives are more tolerated).

The engine operates between layers 2 and 7 of the ISO model, including full stream reassembly, and high-level protocol decodes for protocols such as HTTP, SSL/TLS, SMB, SMTP, FT, DNS, NFS, DHCP, SSH, IKEv2, RDP, and many more.

This latest update improves on and further expands the capabilities of this protection. It enables new types of signatures and continues our support for this vital base security technology.

Anti-Malware

This month, we have also updated our core anti-malware engine. The primary enhancement here is to expand our support for cloud-based detection signatures. We are now so confident in the system's capabilities that we are starting to offer the option of reducing the size of the signature database on the Network Box device itself, and instead access those signatures as required using real-time lookups to the cloud. This option saves both disk space and RAM, which is particularly beneficial for the smaller S-series devices. It allows us to continue expanding our protection database without increasing on-device disk and RAM.

We have also introduced a feature that the anti-malware engine now returns a heuristic indication to the policy engines. So, even though the sample being scanned is not a known threat, it is executable and should be subject to a more thorough analysis in a sandbox or other similar environments. This can be used for policy control.

SSL VPN

Our core SSL VPN engine is based on the industry-standard OpenVPN technology, and this month's update brings the latest security and performance improvements.

Our security model for OpenVPN connections is:

- At the lowest level, a TLS key is used to protect against DDoS, or unauthorized connections, at the lowest TLS packet level. This is a shared secret between the client and the server.
- TLS certificates are used at both the client and server, so both sides can mutually authenticate each other. This authentication protects the devices themselves and forms the core of the protection offered by the VPN. These certificates can be thought of as authenticating devices (not necessarily the users of those devices).
- Optionally, user authentication (via username, password, and optionally Dual Factor Authentication TOTP PIN) can be enabled to perform authentication at the user level.

OpenVPN introduced a feature (with their v2.4 clients) that will also allow a fourth layer of the client to provide information to the server regarding the hardware identification of the workstation/server that the client itself is running on. This may be the MAC address of the Ethernet card or some other unique identifying token that we call the '**clientid**.' This month we have extended the entity system to allow recording of **clientid** attributes for entities. We have also extended the authentication framework to allow **clientid** matches to be optionally enforced. Using the 'push-peer-info' option on OpenVPN clients, users can now be restricted from logging in from particular devices.

The above enhancements, alongside the other Patch Tuesday work, are being released this month and will be deployed by our regional SOCs in phases. Should you need more information on any of these features, please don't hesitate to ask.

Network Box 5.5

NEXT GENERATION MANAGED SECURITY

On Tuesday, 7th July 2020, 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

July 2020

This quarter, for Network Box 5, these include:

- Enhancements to KPI system to support upcoming cloud based centralised KPI reporting feature
- Support recent changes to NOC IP address allocations
- Enhancements to cluster sync, adding optional support for TLS session tickets
- Enhancements to cluster sync, adding optional support for multi-threading (for improved performance)
- Enhancements to support updated version of core IDS and IPS engine
- Improvements to eMail disclaimer addition, supporting more malformed eMail types
- Introduce new entity attribute type ‘clientid’, reflecting a hardware identifier associated with each entity
- Improved authentication support, locking entities by listed clientid attributes
- OpenVPN version upgrade to latest v2.4.8
- Add support for clientid (period) in openvpn - allowing VPN clients to be locked to particular hardware
- Enhanced VPN reporting
- Kaspersky anti-malware engine upgrade to latest
- Support for new options in Kaspersky anti-malware, including KSN, sandbox, and reduced database size option
- Improvements to GMS report for anti-malware, reflecting cloud singature connectivity and status

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 HIGHLIGHTS

Network Box M-255i
Hardware platform for small offices

Network Box is excited to announce our latest revision to the **M-255i** hardware unit, for small offices that require a high volume of storage. Built on a 64bit dual-core processor, this model is equipped with 8GB RAM and a 1TB hard disk. Additionally, it offers six independent 1Gb ethernet ports for high-speed Internet connections.

Technical Specifications

Processor	64bit, 1.6GHz, 2 physical cores
RAM	8GB, 1600MHz DDR3L
Storage	1 x 1TB 3.5" HDD
Networking	6 x 1Gb RJ45
Power Supply	50w
Chassis	1u rackmount – ½ depth
I/O Interface	1 x reset button 1 x RJ-45 Management Console 2 x USB 3.0
Physical Dimensions	440mm(w) x 44.5mm(h) x 250mm(d)
Weight	3.4Kg
Approvals/Compliance	CE Class B, FCC Class B, RoHS

Newsletter Staff

Mark Webb-Johnson
Editor

Michael Gazeley
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

Network Box Security Incident and Event Management (NBSIEM+)

Video Link: https://youtu.be/BDrEyyxd118

The IT network of companies today is more complex than ever before. With so many devices actively connecting to the Internet, it is crucial to continually monitor your systems and assets to ensure your network is protected, and you can detect a breach.

Once you subscribe to the NBSIEM+ service, event data from assets across your company's multiple networks are logged and stored in the one unified system. Thus, providing a real-time, high-level view of your network and assets from one centralized system.

For more information: http://www.network-box.com/NBSIEM

HK Institute of Human Resource Management Cybersecurity Seminar

Network Box, in association with the **HK Institute of Human Resource Management**, gave a cybersecurity talk titled, *'Managing your cyber risk for remote working.'* Covering key aspects of the dangers for a company's remote workforce, and security policies and best practices.