JAN 2018

In the Boxing Ring

Network Box Technical News

from Mark Webb-Johnson, CTO Network Box

Welcome to the January 2018 edition of In the Boxing Ring

Season's Greeting and Happy New Year to you all. This month, we discuss **Network Box Managed Security in 2018 and beyond**. When Network Box was first formed, our goal was to move organizations from simple firewalls to managed UTM+ devices at the network perimeter. However, with the increased use of cloud services, and the evolution of security threats, Network Box has developed new technologies to comprehensively secure our customers' networks. These new features are highlighted on pages 2 to 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 Hong Kong welcomed the **HKSTP** team to see the Network Box Security Operations Centre in action and discuss future collaboration. In addition, Network Box Germany was at **IT-Sicherheitstag NRW**, and Network Box was a guest panelist on **RTHK Radio 3**, to discuss the issue of China's installation of a national camera surveillance network. Furthermore, the **Network Box Technology Review 2017**, is now available, and can be downloaded using the link on page 5.

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

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

Network Box MANAGED SECURITY IN 2018 and Beyond

Since our formation more than 18 years ago, Network Box has been the trusted Managed Security Services Provider for some of the world's leading organizations, small and large. We pioneered the concept of managed UTM+, and remain the leader in our field; with thousands of devices under management from a global network of Security Operation Centres distributed across the world.

Back then, our goal was to move organizations from simple firewalls, to managed UTM+ devices at the network perimeter. At the time, 80% of network intrusions were caused by missing security protection components; we addressed that by including all the key security applications in one single UTM+ appliance and updating protection signatures in real time with our patented PUSH technology. The remaining 20% of intrusions were caused by incorrectly configured or maintained protection; an issue we solved by delivering a managed security service with 24x7x365 maintenance by our security professionals.

Now, in 2018, organizational perimeters have expanded. With the increased use of cloud services, leased data centre racks and virtual machines, as well as home and roaming workers, there is no longer a single perimeter to be defended. The threats themselves have similarly evolved; in addition to the viruses and spams of old, we're now defending against outbound data leakage threats, spyware, keyloggers, and ransomware.

This requires a new way of thinking about network security; a new Security Architecture. The release of Network Box 5.0 introduced a holistic approach to managing our UTM+ appliances, and we followed that up with 5.1 and 5.3 releases to further develop our core security services and cloud offerings. We now expand on this framework, our cloud platforms, and Security Operation Centres, to provide a holistic overview of the entire network and its security incidents. This means managing security and availability incidents not just on Network Box appliances, but on customer networking equipment, servers, workstations and software systems. Such a new architecture encompasses a multi-level network based approach:

Cloud Platform Integration

Network Box will continue to integrate with, and run on, public cloud services (offering delivery of our security platform and services in clouds such as Rackspace, Amazon AWS, Microsoft Azure, and others), and expand on the list of supported services used for platform delivery. This is in addition to the existing on-premise physical hardware offerings.

Asset Tracking

Integrated to services such as DHCP and Active Directory, as well as active network probing, this provides for baseline discovery and auditing of network assets; in particular concentrating on new and changed assets and displaying these in clear easy-to-use reporting.

Vulnerability Scanning

Asset based scanning of the network (both internally and externally) for known vulnerabilities and weaknesses. Correlation of discovered vulnerabilities in change management systems, and tracking through to resolution. We'll continue to offer the classic periodic scanning for audit compliance, but prefer and recommend to move to a continuous scanning approach.

Global Monitoring System Incidents

Up until now we've offered our Global Monitoring System for Network Box devices only. This system monitors availability and dozens of core metrics, across Europe, Asia and US reachability zones. In 2018, we'll start to offer this monitoring and availability notification to customer equipment (either externally or internally reachable), as well as the high-level services that they provide. We'll be able to alert when an incoming mail server becomes unreachable (not just when the mail queue on the Network Box starts to grow, or backup MX systems become active).

Security Incident and Event Management

Delivered as cloud based and/or on-premises solutions, Network Box appliances will operate both as a source of incident logs to industry standard SIEM products, as well as collectors for customer equipment (routers, switches, servers, workstations, etc). We are integrating both with client based (such as workstation based Host IDS and blacklist/whitelist systems) as well as server based SIEMs. The goal here is to integrate all the security logs and incidents into one centralized system, to provide an overview of the entire network, and to be able to apply Integrated Security Intelligence, Digital Forensics, and Security Incident Management.

Integrated Security Intelligence

Built on top of our SIEM support, Security Intelligence will automate handling of security incidents and implement escalation and notification logic; correlating logs across equipment, and providing a single holistic incident report for each event.

Application Services

Network Box will continue to provide our high level application services, as well as expand on these offerings. We'll be offering gateway based eMail encryption, DKIM outbound signing support, DMARC policy enforcement, and other such application services. We'll continue to offer our own cloud application services (such as cloud DNS, cloud reputation, cloud Mail backup, etc), and expand on these offerings.

Penetration, Scanning, and Audit Services

In 2018, Network Box will start offering penetration testing, scanning, and audit services (both via our own SOCs, as well as with certified industry partners to provide an independent service).

Audit and Security Standard Compliance

Network Box will continue to provide our solutions to support the latest PCI standards, and certifications. Our focus will be on the PCI standard as a framework for security (not just for organizations which require PCI regulatory compliance, but also as a generally recommended platform).

All the above operate not just at the perimeter but at all levels of the organization (internal, in the cloud, and on portable devices out on the road), with the architecture delivered via on-premises and in the cloud options. Further information on these offerings will be provided in a roadmap to be released 2018 Q1.

NETWORK BOX

Network Box 5

NEXT GENERATION MANAGED SECURITY

On Tuesday, 2nd January 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
January 2018

This month, for Network Box 5, these include:

- Support "." characters in DHCP host names
- Improvements in ACL rule evaluation performance (via caching support for ACL metadata)
- Standardized object download framework
- New network address ranges for New Zealand SOC
- Support optional domain appending for mail server
- Display protocol name in network IPS logs
- Improvements to loopback protection in proxy web client
- Improvements to enforcement in security module enablement
- Remove duplicate threat IDs in mail logs
- Support optional disabling of mail scanning in proxy IMAP4 and POP3 protocols
- Support recommended guidelines for high security DH group announcements in SSL connections
- Support cipher preference (default) order in SSL server side proxied connections
- Improved content 'tickling' for upload proxy connections
- General reduction in latency for proxy HTTP requests
- Improvements to NTLM v2 support for Firefox browser
- Improvements to proxy authentication support for Chrome browser

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 Hong Kong
HKSTP Visit

The marketing team of the Hong Kong Science and Technology Parks (HKSTP), visited Network Box HQ, to observe the Network Box Security Operations Centre in action, as well as to brainstorm on how Network Box and HKSTP could cooperate to promote Information Technology Development and Cyber Security adoption in Hong Kong.

Network Box Germany
IT-Sicherheitstag NRW

Network Box Germany participated at IT-Sicherheitstag NRW, organized by the the Chambers of Commerce and Industry in North Rhine-Westphalia, to connect businesses with leading security solution providers.

Network Box Hong Kong
RTHK Radio 3

Network Box Managing Director, Michael Gazeley, was a guest panelist in RTHK Radio 3's current affairs programme, *Backchat*. With China installing what's being described as "the world's biggest camera surveillance network", backed by artificial intelligence and facial recognition technology, Michael was asked to share his opinions on the subject, and the global implications of it all.

RTHK 香港電台

http://www.rthk.hk/radio/radio3/programme/backchat/episode/475880

Network Box
Technology Review 2017

As a special end-of-year review, Network Box has complied the key *In the Boxing Ring* articles and technology news of 2017. Please use the link below to download the **Network Box Tech Review 2017**.

http://www.network-box.com/sites/www.network-box.com/files/files/Technology_Review_2017.pdf

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

Copyright © 2018 Network Box Corporation Ltd.