In the Boxing Ring
APRIL 2020

Network Box Technical News
from Mark Webb-Johnson
Chief Technology Officer, Network Box

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

In light of the ongoing pandemic, this month, we will be talking about **Business Continuity in the time of COVID-19 Lockdowns**. During these difficult times, many of our customers are facing the inevitability of having to activate their *Business Continuity Plans*, in all likelihood for an extended period, or otherwise making work-from-home arrangements. The good news is that Internet technology has progressed rapidly in recent years and this is now very feasible for most. On pages 2 to 3, we discuss in detail how Network Box can support you with this, and we also outline our **Top Cybersecurity Tips for a Secure Remote Workplace.**

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, to support customers that may be working from home, Network Box has released an **SSL VPN Client Installation Guide**. Additionally, **NBSIEM+** is now live and available. In addition to the *Full Service*, Network Box is offering a *Free 90-day Basic Service* for existing customers. And in this month's Security Highlights, **Marriot** reveals another data breach, and vulnerabilities were found in **HP**, **Cisco**, and **Citrix** products.

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

In this month's issue:

BUSINESS CONTINUITY

in the time of COVID-19 Lockdowns

In these difficult times, many of our customers are facing the inevitability of having to activate their Business Continuity Plans, in all likelihood for an extended period, or otherwise making Work-from-Home arrangements. The good news is that Internet technology has progressed rapidly in recent years (in particular with respect to the available bandwidth in low latency connections), and this is now very feasible for most.

The Network Box Remote Access Approach

Remote Access should never be enabled by merely opening servers and ports to the Internet. Given recent vulnerability announcements, that is particularly true for Remote Desktop Protocol (RDP) and other administrative connections. You need to be able to differentiate between your authorized staff, and general Internet traffic; Virtual Private Network (VPN) technology is the right tool for that job. As well as robust authentication, VPNs provide for encryption of all traffic, and digital signing of that traffic for tamper-resistance. In addition, VPNs offer a network level connection (not application level), so a large number of applications can be run over them (not just web apps, for example).

In general, for 'road warrior' style remote access (laptops, etc.), Network Box recommends SSL VPNs. The SSL technology is exceptionally mature now, and certificates can be used at both ends to provide effective authentication at the device level. Also, a TLS secret can be configured to protect the SSL/TLS protocol channel itself from attack at the lowest level (in particular from brute-force and denial-of-service style attacks). Username+Password authentication can then be enabled on top of this device-level authentication, to provide authentication of individual connecting users.

For individual laptop connections, a small SSL VPN client (available for popular operating systems such as Windows, OSX, Linux, iOS, iPadOS, Android, and others) will need to be installed and configured via a single simple configuration file. The necessary certificate authority for issuing client and server certificates can be enabled on the Network Box itself, and Network Box can integrate with authentication providers such as Microsoft Active Directory or LDAP servers. Dual Factor Authentication is available as an option.

For network-to-network connections (e.g. branch offices, connections between offices, and multiple machines in one site accessing a central resource at another), the best solution is to install a small Network Box appliance such as the VPN-5Q at the remote site. Network Box engineers can then configure both ends to ensure a safe and secure network-level connection.

Once the VPN connection is established, the remote client/network becomes an extension of your own network. Restrictive firewall controls, as well as organizational policies, can be applied with the same fine-grained approach as for other connections protected by Network Box.

You should consider putting in place such networks and configurations NOW (assuming you still have time) before this becomes an urgent problem that you need to address without proper planning.

Network Box Security Response would like to re-assure you that we are here to support you with this. Even in usual times, our primary function is supporting clients and devices in remote locations. If you have any questions or concerns, please don't hesitate to contact your local Security Operation Centre for advice.

Top Cybersecurity Tips for a Secure Remote Workplace

1. All authorized personnel should have access to an individual (not shared) Virtual Private Network (VPN) account for secure access to office / Data Centre resources. Dual Factor Authentication (2FA) should be enabled on all such user accounts with remote access privileges. Strict password policies should be enforced (you might get away with a weak password in the office, but when open to the world that will be quickly discovered and exploited).

2. All traffic should be directed through the VPN, including Internet traffic, and you should ensure that the proxy and HTTP/HTTPS policies and protection you have in your office is also applied to remote workstations. You should not use split-tunnel arrangements (as they open the laptop to attack). You should consider source-NAT arrangements (as provided by most WiFi routers, and single IP home connectivity arrangements) to isolate laptops from direct attack from the Internet.

3. If VPN access is from the network (rather than an individual laptop), then the remote network comes into scope for protection. In such cases, remote networks should be suitably partitioned into the home and office LANs (or VLANs), for example. WiFi networks should be similarly separated and secured. Care should be taken when linking potentially insecure appliances to work-related equipment.

4. An uptick in the prevalence of malware and phishing related COVID-19 emails and website advertisements should be expected. Staff should be suitably trained to be suspicious and not to act on or spread such information.

5. Now, more than ever, it is vital that everyone keeps up to date with patches and updates to their systems (both local and remote).

6. Bear in mind that with all this new remote traffic coming into and out of your network, your bandwidth requirements may increase. Be flexible, but keep an eye on this. If necessary, implement restrictive policies, such as denial or quality of services constraints, against such bandwidth hogs as large downloads, non-work-related video and audio streaming.

7. Encourage video conferencing as a way to keep the team motivated and to help individuals feel less isolated. Encouraging your staff to adhere to a rigid schedule (can be flexible hours, so long as it is pre-defined and clear) will help productivity and avoid distractions.

Network Box 5.5

NEXT GENERATION MANAGED SECURITY

On Tuesday, 7th April 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
April 2020

This quarter, for Network Box 5, these include:

- Improvements in performance of the base configuration system
- Improvements in performance of configuration synchronisation (in particular for large clusters with large configurations)
- Extensions to cluster sync system, to support high availability and load balanced clusters
- Enhancements to support cloud reporting of device KPI statistics
- Improvements to VPN connection status tracking
- Support relay host authentication over non-standard ports
- Reliability and performance improvements to logging systems
- Enhanced auditing of admin and user portal authentication failures
- Improvements in network DDOS collections for WAF+
- Release support for proxying (and policy control) of DNS client protocol
- Release support for proxying (and policy control) of DNS server protocol
- Enhanced support for RDG_OUT_DATA and RDG_IN_DATA methods for HTTP protocol

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 Security Incident and Management System (NBSIEM+)

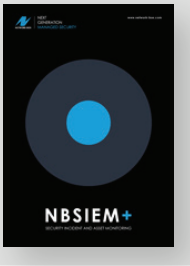
NBSIEM+ allows users to view all security incidents and events for all devices within their network. Delivered as a hybrid cloud/on-premises or pure cloud-based solution, NBSIEM+ integrates all the security logs and incidents into one centralized system. Thus, providing an overview of the entire network and allowing Integrated Security Intelligence, Digital Forensics, and Security Incident Management to be applied. Currently, Network Box is offering two options:

Free 90-day BASIC service

This service is available for existing Network Box customers for FREE. The service includes 90 days storage of non-audit Event Logs from Network Box devices. Audit logs, events from other non-Network Box devices, and cold archiving/retrieval are not included.

NBSIEM+ FULL Service

The service includes storage of ALL event logs (not just logs from denied and anomalous traffic) and logs from other non-Network Box devices.



For more information, you can download the NBSIEM+ brochure here:
https://www.network-box.com/sites/www.network-box.com/files/files/NBSIEM+_Brochure.pdf

To subscribe to any of the NBSIEM+ services, please download and fill in the Order Form:
https://www.network-box.com/sites/www.network-box.com/files/files/NBSIEM+_OrderForm.pdf

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 SSL VPN Client Installation Guide

As businesses and organizations are adopting a 'work from home' policy during these critical times, it is crucial to ensure that Internet traffic between your home and your office is encrypted and secured from hackers trying to intercept your communications.

If you are a Network Box customer working remotely, it is highly recommended that you use an SSL VPN client to ensure your traffic is protected. Please the link below to download the SSL VPN Client Installation Guide.

LINK:
https://www.network-box.com/sites/www.network-box.com/files/files/SSL_VPN-Client_InstallationGuide.pdf

Network Box Security Headlines

CBS News

Marriott reveals its second customer data breach in two years

LINK: https://bit.ly/2UJlQym

BleepingComputer

Windows PCs Exposed to Attacks by Critical HP Support Assistant Bugs

LINK: https://bit.ly/2V8WtSw

ThreatPost

Chinese Hackers Exploit Cisco, Citrix Flaws in Massive Espionage Campaign

LINK: hhttps://bit.ly/3dXrPUT