JUN 2015

In the Boxing Ring

Network Box Technical News
from Mark Webb-Johnson, CTO Network Box

Welcome to the June 2015 edition of In the Boxing Ring

This month, Network Box is launching two major features: 1) the Network Box *VPN-5 hardware appliance*, and 2) *VPN Reporting* enhancements. The VPN-5 hardware appliance is intended for VPN and Firewall only, and specifically targeted at remote branch offices requiring VPN connectivity back to head office (in either a hub-spoke or mesh style network environment using VPN or MPLS technology). Key specifications and details are highlighted in page 2.

With the VPN reporting system, Network Box has released a significant number of enhancements which can be accessed via the administrative web portal in Network Box 5. We now offer reporting based on four levels, which is discussed in detail in page 3.

On pages 4–5, we highlight the features and fixes to be released in this month's patch Tuesday for Network Box 5 and Network Box 3. We continue to develop, and will continue to support, Network Box 3 for the foreseeable future (several years).

Finally, Network Box Australasia General Manager, Howard Nicholls, was profiled in *CIO Magazine*. In addition, Network Box Managing Director, Michael Gazeley, was interviewed by *Capital Magazine*, and was also profiled in *Security Asia*.

Mark Webb-Johnson
CTO, Network Box Corporation Ltd.
June 2015

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
Linked in 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
VPN-5 Model

When it comes to large mesh or hub-and-spoke networks, using VPN/MLPS connections to branch offices, the choice of devices to deploy at the remote stations has always been difficult.

Until today, there have been two options:

Option (a):

Very cheap and simple devices, with little effective centralised management, poor performance, and limited protection capabilities.

Option (b):

More expensive devices, which can be fully integrated to your managed infrastructure, and offer the capability of perform effective protection at the network edges.

Up until now, the Network Box S-series appliances have addressed option (b), and we have been forced to work with less-than-optimal devices to address the requirement for option (a).

Today, Network Box is proud to release our VPN-5 appliance to provide another option at the lower end, without sacrificing protection capabilities.

The VPN-5 appliance is specifically targeted at remote branch offices requiring VPN connectivity back to head office (in either a hub-spoke or mesh style network environment using VPN or MPLS technology).

The appliance itself is not based on a low power, low memory, low performance, single core CPU like most of its competitors. Instead, it uses a dual core 1.6GHz CPU, 2GB RAM, and offers 16GB (4GB system, 12GB user) flash storage. Coupled with 4x 1Gbps ethernet interfaces, this provides performance to handle even the most high bandwidth remote office connections. All three VPN types are supported (PPTP, SSL and IPSEC), and the device can be fully managed and integrated with the rest of your managed network.

It is intended for firewall and VPN only, and the price is significantly less than S or M series units.

VPN Reporting

This month, we're proud to release a number of significant enhancements to our VPN reporting system, as accessed via the administrative web portal in Network Box 5. We now offer reporting based on 4 levels, as described below.

Level 0 - Current Status

The current status of connected VPNs can be seen in most VPN devices. This simple display shows you each VPN, when it was connected, and (in some appliances) how long it has been connected for.

Network Box 5 has offered this report for some time now (Network / VPN / Status). It is updated in real-time, and goes a step further than most VPN devices by also showing a real-time updated global map of the status of your VPN connections.

Level 1 - Events

Most VPN devices on the market today offer an event based reporting system. They'll tell you events such as when a VPN was connected, when it was disconnected, or details of when an error occurred on the link.

This is a pretty basic report. It doesn't tell you how long a VPN has been up, or even which VPNs were up at a particular date/time, but you can manually process the events to try to determine that for yourself.

Network Box 5 has always tracked these events, but this month we're releasing a basic report (under Network / VPN / Events) to allow you to see the raw underlying data yourself.

Level 2 - Sessions

A small number of VPN devices available today attempt to correlate the VPN events to track VPN sessions. A session is a continuous period of connectivity of a particular VPN connection. For example, a VPN connecting at 11am on 10th April, and disconnecting at 10am on 13th April, could be said to have a session lasting for duration 2 days 23 hours.

The problem comes when you report on these sessions. You typically want to produce a report saying 'show me all VPNs connected on 10th April', and the VPN device will show you any VPN sessions that started on that day. Some will even show you VPN sessions that completed on that day. But, it is rare to find one that will report on sessions established on that day without starting/ending.

Level 3 - In Progress Sessions

To show sessions that were already connected on a specific day (but didn't start or end on that day) requires tracking the *In Progress* sessions on a daily basis. This report is the most useful, is surprisingly rare to see offered by VPN devices, and is precisely what we have released for Network Box 5 this month. You can find this new report at Network / VPN / Connections.

The report shows VPN sessions that either started, completed, or were in progress, for a specified time range. For each session, it shows the duration the session was up during that specified time range, as well as the total uptime so far for the session.

Using the above example, and asking for a connection report for time period 11th April, the report would show the connection as having duration 24 hours (the entire day) and uptime 37 hours (from 11am on 10th April to midnight 11th April - the end of the reporting period). Such reports are extremely useful to immediately see VPN connections experiencing downtimes, repeated reconnections, or other such issues.

Conclusions

The three VPN reports are being released this month to all Network Box 5 customers. They are available for all three types of supported VPN (IPSEC, SSL and PPTP), and we hope that you find them useful.

Our work on VPN reporting continues during June, and a second batch of improvements is scheduled to be released in the July patch tuesday. These include:

- Configurability of VPN persistent type. VPNs will be able to be configured as permanent (expected to be up 100% of the time) or ephemeral (disconnecting and connecting at will, with no expected up time).

- Reporting on persistent VPN availability. A report showing the percentage of uptime for each permanent type VPN.

- VPN KPIs will also be released for each of the three main VPN types.

NETWORK BOX

Network Box 5
NEXT GENERATION MANAGED SECURITY

On Tuesday, 2nd June 2015, 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 7 days.

Network Box 5 Features
June 2015

This month, for Network Box 5, these include:

- Support for S-SCAN URL categorisation on 32bit Network Box models
- Improvements to logging of smtp header/body timings and sizes in SMTP client and server
- Migration of Kaspersky anti-malware engine to new ACL system
- Migration of Scanning service to new ACL system
- Migration of URL categorisation engine to new ACL system
- Re-organisation of admin web portal menu to better reflect holistic system:
  - Modules/Mail -> Activity/Mail/Overview
  - Modules/Web Client/Utilisation Summary -> Activity/ Web Client/Overview
  - Modules/Web Client/Utilisation Detail -> Activity/Web Client/Tops
  - Modules/Web Client/Categorise URL -> Activity/Web Client/Categorise URL
  - Modules/DDoS -> Attacks/DDoS
  - Modules/High-availability -> Network/High-Availability
  - Modules/VPN/Status -> Network/VPN/Overview

- Improvements to VPN tracking and reporting
- Introduction of new Network/VPN/Events report
- Introduction of new Network/VPN/Connections report
- Improvements to handling of UTF-8 internationally encoded eMail
- Improvements to text fingerprinting for anti-spam eMail scanning
- Improvements to ZIP decode handling for corrupted, but partially unpackable, ZIP archives in eMail scanning
- Enhanced support for source address selection in directed proxy mode
- Enhanced support for source address selection in mail server
- Make LDAP server basedn an optional parameter (previously required)
- Support importation of custom CRL in SSL VPN server
- Improved support for handling routes in the event one or more routes fail to be applied
- Symmetric Outbound support for gateway load balancing
- Improvements to handling of control-C in admin command line console

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

Network Box 3 Features
June 2015

On Tuesday, 2nd June 2015, 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 7 days. This month, for Network Box 3, these include:

- Enhancements to Box Office and Response web sites, related to display of MAPP partnership information

- Optional configuration for mail scanning, to treat broken RAR archives as encrypted

- Various (mostly internal) enhancements to several internal support systems

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.

Newsletter Staff	Subscription
Mark Webb-Johnson Editor	Network Box Corporation nbhq@network-box.com or via mail at:
Michael Gazeley **Nick Jones** **Kevin Hla** Production Support	**Network Box Corporation** 16th Floor, Metro Loft, 38 Kwai Hei Street, Kwai Chung, Hong Kong
Network Box HQ **Network Box UK** **Network Box USA** Contributors	Tel: +852 2736-2083 Fax: +852 2736-2778 www.network-box.com

Network Box Hong Kong
Capital Magazine

Network Box Managing Director, Michael Gazeley, was interviewed by Capital Magazine, in an article which highlighted the future trends in cyber-security, the latest features offered by Network Box 5, and also the fact that Network Box recently won a Capital Outstanding Enterprise Award 2015, where Network Box received the award for *'Best Network Security Provider.'*

Network Box Australasia
CIO Magazine

Howard Nicholls, the General Manager of Network Box Australasia, was featured in CIO magazine.

LINK: hhttp://www.cio.co.nz/article/575152/doing-business-howard-nicholls-network-box/

Network Box Hong Kong
Security Asia

Network Box's Managing Director, Michael Gazeley, was featured in a Personality Profile interview in Security Asia. In the interview, Michael shared his experience and opinions on the challenges and the future of the cyber security industry.

LINK: http://www.security-asia.net/uploads/1/1/8/7/11871079/sa_issue_8.pdf

NETWORK BOX