

# In The Boxing Ring

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

### Welcome

Welcome to the July 2011 edition of 'In the Boxing Ring'. Continuing on from April's format changes, we have had a new look since June, as we continue the run-up to the release of NBRS-5.0. For the rest of this year, each month we will present one topic on NBRS-5.0 (the upcoming major Network Box firmware release). The monthly hint will go, and is replaced with an entire back page on the updates being released to the existing NBRS-3.0 product. This front page will remain, and summarise what is new and notable.

This month, on pages 2 and 3, we present details on the NBRS-5.0 Provisioning Architecture. We talk about the six key points to provisioning NBRS-5.0.

Our goal is to deploy security services with as little impact to existing networks as possible. To co-exist with existing networks - providing a security filter for the existing traffic. NBRS-5.0 achieves this goal with transparent proxies and security services. The NBRS-5.0 Provisioning Architecture allows us to deploy, monitor and manage our security filtering devices in such a transparent manner.

Page 4 details the features and fixes to be released in this months patch Tuesday for NBRS-3.0. We continue to develop, and will continue to support, NBRS-3.0 for the foreseeable future (several years), and this page will be used to keep you informed as to what is happening with our core product.

You can contact us here at HQ by eMail ([nbhq@network-box.com](mailto:nbhq@network-box.com)), or drop by our office next time you are in town. You can also keep in touch 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>

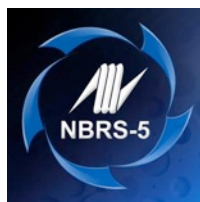
Mark Webb-Johnson  
CTO, Network Box Corporation  
July 2011

### IN THIS ISSUE

**2-3. NBRS-5.0 PROVISIONING ARCHITECTURE**  
We present details on the NBRS-5.0 Provisioning Architecture. We talk about the six key points to provisioning NBRS-5.0.

**4. Z-SCAN ANTI-MALWARE ENGINE**  
Network Box Z-Scan Anti-Malware engine won HKA I 2011 - Technological Achievement Grand Award on 30th Jun 2011.  
Network Box Z-Scan focuses on focuses on developing and releasing its own signatures to protect against emerging viruses within seconds of a threat being seen.

**4. JULY 2011 FEATURES**  
The features and fixes to be released in this month patch Tuesday for NBRS-3.0. We continue to develop, and will continue to support, NBRS-3.0 for the foreseeable future (several years), and this page will be used to keep you informed as to what is happening with our core product.



### The NBR5-5.0 Provisioning Architecture

For this month's topic on NBR5-5.0, we'll be presenting information on the provisioning architecture. Our goal is to deploy security services with as little impact to existing networks as possible. To co-exist with existing networks - providing a security filter for the existing traffic. NBR5-5.0 achieves this goal with transparent proxies and security services. It is the provisioning architecture that allows us to deploy, monitor and manage our security filtering devices in such a transparent manner.

### NBR5-3.0 vs NBR5-5.0 Provisioning

Under NBR5-3.0, the box is provisioned from the NOC. The box informs the NOC of its public IP address, and the NOC calls out to the box to update it. This requires detailed knowledge of the customer network, and network permissions to allow the NOC to call the box. There are a large number of connections in both directions, over a variety of ports and addresses, and any security devices between the box and the NOC needs to be configured to permit this traffic.

The goals of NBR5-5.0 are to deploy security services with as little impact to existing networks as possible, to co-exist with existing networks - providing a security filter for the existing traffic while requiring little or no knowledge of the customer network.

This requires a new approach to provisioning our boxes, and to keeping them updated and monitored 24x7.

#### Device Identification

- The Device ID is the key
  - The Device ID is the key identifier of the box
    - Statistics and utilisation records
    - Configurations
    - Transactional Logs
  - The Box ID becomes just a nickname

### Provisioning Sequence

A system called NBSYNC is the gateway for inter-box communications. It provides for links between devices over IP, behaving like a dynamic VPN; using SSL as its zf technology to deliver secure authenticated and encrypted communication channels. NBSYNC runs on every NBR5-5.0 Network Box, as well as the centralised services (such as statistics, global monitoring system and NOCs). NBSYNC is used for both intra-box (eg; cluster) and box-to-noc communications, and provides a single secure communication circuit over which individual communication channels may be bi-directionally established.

#### The Provisioning Problem

- NBR5-5.0 Goal
  - Deploy security services with as little impact to existing networks as possible
  - To co-exist with existing networks - providing a security filter for the existing traffic

➔ Requiring little or no knowledge of the network

### Devices Roles and IDs

With NBR5-3.0, the boxid was the primary key. Now, in NBR5-5.0, we introduce a new concept of Device Role (and associated Device ID). Each device role is given a unique Device ID that exists for its lifetime. The boxid may change, but the Device ID is fixed, and is a globally unique identifier (a UUID) so that it can be created on the box without reference to any centralised allocation service. As hardware is swapped, the Device ID remains constant (moving between different hardware) and always refers to the particular role of the device.

Under NBR5-5.0, the Device ID is the key identifier of the box. It is the key to all statistics and utilisation records, as well as configurations and transactional logs. The boxid becomes just a nickname.

#### Provisioning Sequence

- NBSYNC Connections
  - Once NBSYNC connections are established
    - Channels can be opened in either direction
    - Encrypted and Authenticated
    - Keep-alive messages to keep link alive
  - Connections are outbound from the BOX
  - Channels can be either outbound or inbound

Provisioning works by a client on the box instructing NBSYNC to connect to a globally available provisioning and registration service. This is an outbound call from the box to Network Box HQ. The call may be attempted over many ports and to many fallback destination addresses, so that it can try to work around any upstream filtering or blocking. Once a connection is successful, the box provides its Device ID and identification to the Provisioning and Registration Service, and the service replies with a list of subsequent connections to make for detailed services. The list is cached locally on the box (for speed, as well as to protect against the case of the provisioning and registration service being unreachable).

The subsequent services provided include:

1. Statistics and Utilisation (an optional service to receive statistics from boxes, storing per-box, per-industry and globally to allow anonymous trend reporting).
2. Global Monitoring System (receives health information from the boxes in real-time, and allows for fast notification of box connectivity problems without requiring ICMP or SNMP polling).
3. Signature Push (a globally distributed network of signature PUSH servers delivering subscribed signature packages and periodic updates in real-time, and allowing for on-demand retransmission of these packages).
4. NOCs (bi-directional syncing of configuration changes, providing a backup of the box configuration and allowing for remote maintenance of the boxes from one or more permitted NOCs).

## NOC

- Six Key Points to Provisioning
  1. Unique Device ID
  2. Box calls out to Provision
  3. Provisioning tells box about available services
  4. Box calls out to each service
  5. Services and box bi-directionally call each other
  6. Real-time, incremental updates, transparently

## NBRS-5.0 Provisioning Architecture

*Our goal is to deploy security services with as little impact to existing networks as possible. To co-exist with existing networks - providing a security filter for the existing traffic.*

*NBRS-5.0 achieves this goal with transparent proxies and security services. It is the provisioning architecture that allows us to deploy, monitor and manage our security filtering devices in such a transparent manner.*

Mark Webb-Johnson  
CTO, Network Box Co., Ltd.  
June 2011

## Provisioning Sequence

- NBSYNC
  - NBSYNC is the gateway for inter-box comms
    - It provides for links between devices over IP
    - It behaves like a dynamic VPN
    - It uses SSL as its core technology
    - Authentication and Encryption are used

## Provisioning Sequence

- Network Box HQ Services
  1. Provisioning and Registration
  2. Stats
  3. Global Monitoring System (GMS)
  4. Signature Push
  5. NOC

## Security Considerations

The NBSYNC protocol is built on top of the SSL security standard. This means it inherits the same certificate model, as well as encryption and authentication capabilities, as the most secure systems. The core technology has received many thorough security audits, evaluations, and is considered secure. The system itself currently uses 4096 byte RSA certificates and 256 byte AES encryption.

## Conclusions

There are six key points to provisioning NBRS-5.0:

1. Each device role is assigned a unique Device ID (no longer dependent on the boxid)
2. Each box calls out to Provision itself
3. Provisioning tells the box about the services available to the box
4. The box calls out to each service
5. Services and boxes bi-directionally call each other
6. Real-time, incremental updates, are delivered transparently

By the use of NBSYNC to provide a single outbound (box to NOC) communication link, and then routing subsequent communications bi-directionally within that single link, the communications requirements are vastly simplified (when compared to NBRS-3.0). This allows boxes to be seamlessly provisioned, updated, monitored and maintained without having to know the IP address of the box or requiring changes to the network to be able to make a call from the NOC to the box.



## July 2011 Features

On Tuesday, 5th July 2011, Network Box will release our patch Tuesday set of enhancements and fixes. The regional NOCs will be conducting the rollouts of the new functionality in a phased manner over the next 7 days. This month, these include:

- Support for custom threat names in statistical summaries (for improved presentation on response.network-box.com website and statistical and trend analysis by Network Box Security Response engineers.
- Minor enhancements to the health monitoring system.
- Various enhancements and minor fixes to the my.network-box.com administrative interface.

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 NOC will contact you to arrange this if necessary.

Should you need any further information on any of the above, please contact your local NOC. They will be arranging deployment and liaison.



## Z-SCAN ANTI-MALWARE ENGINE

Z-Scan Anti-Malware system focuses on developing and releasing its own signatures to protect against emerging viruses within seconds of a threat being seen, rather than waiting for the antivirus industry to release a new signature which can often take nearly a day.

The engine operates by continually analysing all the threat information obtained in real time from more than 200,000 traps in the cloud, poised 24/7 for virus attacks to occur, which includes spam-traps, virus traps, in-house submissions, customer submissions, mail statistics, http statistics, and suspect samples. This is done 24 hours a day, 7 days a week, 365 days a year.

'Z-Scan' is a new approach which deals with the less than 40,000 brand new 'zero day' viruses, which may be making the rounds on the Internet at any given time. With a reaction time of just 3 seconds in many cases, this is a far cry from the 3, 12, or even 20 hours, traditional anti-virus vendors are often taking to protect their customers.

Network Box Z-Scan Anti-Malware engine won HKAI 2011 - Technological Achievement Grand Award on 30th Jun 2011. This cutting edge technology was designed specifically to enhance the level of protection available to existing Network Box clients around the world. 'Z-Scan' is already protecting multi-national companies, organizations, and government departments across the globe, including over 150 banks and credit unions in the USA alone.



## JULY 2011 NUMBERS

Key Metric	#	% difference (since last month)
PUSH Updates	622	+1.6
Signatures Released	273,323	+66.7
Firewall Blocks (/box)	801,198	+4.4
IDP Blocks (/box)	103,696	-2.9
Spams (/box)	17,434	+7.7
Malware (/box)	407	-40.7
URL Blocks (/box)	148,005	+10.4
URL Visits (/box)	4,098,720	+2.8

## NEWSLETTER STAFF

### Mark Webb-Johnson

Editor

### Michael Gazeley

### Jasmine Arif

### Nick Jones

Production Support

### Network Box Australia

### Network Box Hong Kong

### Network Box UK

Contributors

## SUBSCRIPTION

Network Box Corporation

[nbhq@network-box.com](mailto: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 2736-2078

Fax: +852 2736-2778

[www.network-box.com](http://www.network-box.com)

Copyright © 2011 Network Box Corporation Ltd.