

In The Boxing Ring

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

Welcome

Welcome to the August 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 NBR5-5.0. For the rest of this year, each month we will present one topic on NBR5-5.0 (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 NBR5-3.0 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 NBR5-5.0 Networking Architecture. Transparency is the first of our four goals for NBR5-5.0. Following the 'do no harm' philosophy by attempting to influence the network traffic as little as possible, whilst still performing our security functionality, it is the networking architecture that allows a NBR5-5.0 box to be transparent.

NBR5-5.0 includes core support for Bridging, Routing and Network Address Translation modes of deployment. All three have excellent support for both the IPv4 and IPv6 Internet protocols. Not merely supporting IPv6, but assisting our customers with their migration to IPv6 (combining dual-stack with protocol translation).

Page 4 details the features and fixes to be released in this months patch Tuesday for NBR5-3.0. We continue to develop, and will continue to support, NBR5-3.0 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), 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
August 2011

IN THIS ISSUE

2-3. NBR5-5.0 NETWORKING ARCHITECTURE

We present details on the NBR5-5.0 Networking Architecture. Transparency is the first of our four goals for NBR5-5.0. Following the 'do no harm' philosophy by attempting to influence the network traffic as little as possible, whilst still performing our security functionality, it is the networking architecture that allows a NBR5-5.0 box to be transparent.

4. Z-SCAN ZERO-DAY IN-THE-CLOUD PROTECTION

Network Box Zero-Day Technology Now Targets Spam. Award winning Z-Scan in-the-cloud protection against zero-day virus and spam threats.

This new Z-Scan powered Anti-Spam engine brings the total number of Anti-Spam engines used by Network Box to 25, and the number of Anti-Spam signatures to over 19.6 million.

4. AUGUST 2011 FEATURES

The features and fixes to be released in this month patch Tuesday for NBR5-3.0. We continue to develop,



The NBR5-5.0 Network Architecture

For this month's topic on NBR5-5.0, we'll be presenting information on the network architecture. Transparency is the first of our four goals for NBR5-5.0. Following the 'do no harm' philosophy by attempting to influence the network traffic as little as possible, whilst still performing our security functionality, it is the networking architecture that allows a NBR5-5.0 box to be transparent.

NBR5-5.0 Networking in the Base Platform

NBR5-5.0 includes core support for Bridging, Routing and Network Address Translation modes of deployment. All three have excellent support for both the IPv4 and IPv6 Internet protocols.

Each mode can operate individually, or be combined in more sophisticated network configurations. For example, a transparently bridged network can use NAT for some traffic to be re-directed to a secure DMZ, and routing to deliver that traffic.

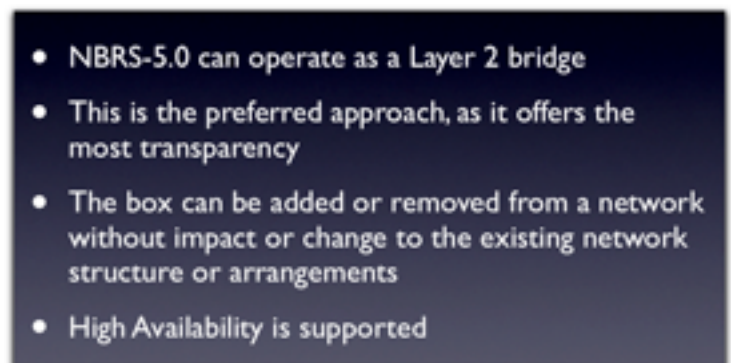
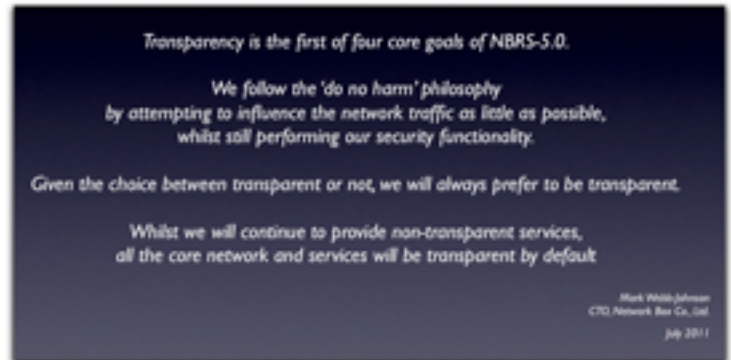
Security Modules extend the base networking capabilities to provide:

- Virtual Private Networking,
- Firewalling,
- Application Identification,
- Quality of Service,
- High Availability,
- Proxying and Application Level filtering/control,
- Intrusion Detection and Prevention,
- and others.

NBR5-5.0 Bridging

Bridge-mode is the preferred approach for deployment of NBR5-5.0 boxes, as it offers the most transparency.

Bridging deployments operate over a minimum of 2 physical interfaces. Acting similarly to a network hub, traffic on one interface is transparently filtered according to security policies and then passed through to the other interfaces. More than 2 interfaces are supported, as are configurations with more than one bridge per box.



NBRS-5.0 Routing

NBRS-5.0 can operate in router-mode, and is able to direct traffic based on destination address or other more complex policy rules.

Routing tables store the routes, and policy rules select the routing table to use for particular traffic. A routing cache is used to optimise performance.

Routes can be added to these tables either statically or dynamically, and a variety of high-level routing protocols are supported.

- Static and Dynamic Routing Tables
 - Routes can be added either statically or dynamically
 - High-level routing protocols supported:
 - RIP v1 and v2 for IPv4
 - RIPng for IPv6
 - OSPFv2 for IPv4
 - OSPFv3 for IPv6
 - BGP for both IPv4 and IPv6
 - and others to follow...

NBRS-5.0 Network Address Translation

NBRS-5.0 can operate in an IPv4 NAT mode. NAT (Network Address Translation) was originally used to extend the life of IPv4, but is also useful in cases of service migration and redirection. Network Box supports both Source (multiple machines sharing the same usually-public source address) and Destination (calls to one destination address being redirected to another) translation. Bi-directional mappings are also supported.

Due to the dramatic differences between the protocols, it is not possible to simply NAT between IPv4 and IPv6 on the global Internet. However, NBRS-5.0 offers translation services to assist with the co-existence and migration between these two protocols. Using router-level technologies, combined with high-level proxies and services, NBRS-5.0 will support bi-directional translation between IPv4 and IPv6.

Flexible connectivity options are offered, including IPv6-in-IPv4 tunnels to provide IPv6 connectivity to those customers whose ISPs cannot offer direct IPv6 connectivity.

While NBRS-3.0 had basic support for IPv6, NBRS-5.0 offers full support for IPv6 and (most importantly) translation between IPv4 and IPv6 traffic. It is designed to assist our customers with their migration to IPv6, not merely to act as an IPv6 device on the network.

- For IPv6 NBRS-5.0 also offers Translation
 - Using router-level technologies, combined with high-level proxies and services, NBRS-5.0 will support bi-directional translation between IPv4 and IPv6
 - Examples:
 - IPv4 DMZ, IPv4 and IPv6 dual-stack Internet
 - IPv4 LAN and DMZ, IPv6 Internet
 - IPv6 LAN and DMZ, IPv4 Internet
 - IPv4 LAN and DMZ, IPv4 Internet with connectivity via IPv6-in-IPv4 tunnel to provider

Conclusion

NBRS-5.0 offers a network architecture designed for the present (IPv4) as well as the future (IPv6) Internet. Not merely supporting IPv6, but assisting our customers with their migration to IPv6 (combining dual-stack with protocol translation).



Network Box Certified ISO 27001 Security Operations Centre

August 2011 Features



On Tuesday, 2nd August 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:

- Extensions to the mail scanning system to support improved unpacking of messages containing Microsoft Excel attachments.
- Extensions to the mail scanning system to support improved unpacking of messages containing Microsoft Word attachments.
- Extensions to the anti-spam system to support the new Word and Excel unpackers.
- Extensions to the Data Leakage Prevention system to support the new Word and Excel unpackers.
- Introduction of Sentinel Z-Scan for Anti-Spam.

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 ZERO-DAY IN-THE-CLOUD PROTECTION

Network Box, has enhanced their Z-Scan zero-day Anti-Virus system, so it can now target spam as well. The same multi-award winning zero-day Anti-Malware technology is now helping in the never ending fight against spam.

This new Z-Scan powered Anti-Spam engine brings the total number of anti-spam engines used by Network Box to 25, and the number of anti-spam signatures to over 19.6 million.

Z-SCAN zero-day protection

Z-Scan for Anti-Spam is an adaptation of Network Box's multi-award winning zero day anti-virus solution. Utilizing state-of-the-art in-the-cloud technology, Z-Scan can react to zero day malware up to 4,200 times faster than traditional Anti-Virus systems. By adapting the same system to the fight against spam, Network Box is responding to zero-day outbreaks of certain types of spam in just seconds as well.

The Z-Scan system operates by continually analysing all the threat information obtained in real time from more than 200,000 traps. These Z-Scan traps include spam-traps, virus traps, in-house submissions, customer submissions, mail statistics, http statistics, and suspect samples. The network of Z-Scan traps works 24 hours a day, 7 days a week, 365 days a year.

JULY 2011 NUMBERS

Key Metric	#	% difference (since last month)
PUSH Updates	568	-8.7
Signatures Released	373,197	+36.5
Firewall Blocks (/box)	781,004	-2.5
IDP Blocks (/box)	108,595	+4.7
Spams (/box)	14,081	-19.2
Malware (/box)	346	-15.0
URL Blocks (/box)	125,707	-15.1
URL Visits (/box)	3,571,601	-12.9

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

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

Copyright © 2011 Network Box Corporation Ltd.