

In The Boxing Ring



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

Welcome

Welcome to the April 2011 edition of 'In the Boxing Ring'. This month, you'll find the format of the newsletter has been changed, as we start 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 NBR3-3.0 product. This front page will remain, and summarise what is new and notable.

This month, on pages 2 and 3, we present an overview of NBR5-5.0. We talk about its four fundamental goals of Transparency, Holistic approach, Scalability and Modularity; and how each of those goals will be used to help us to continue to deliver the leading security service for protection of customer networks.

Page 4 details the features and fixes to be released in this months patch Tuesday for NBR3-3.0. We continue to develop, and will continue to support, NBR3-3.0 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
April 2011



IN THIS ISSUE

2-3.

NBR5-5.0 FIRMWARE

We present an overview of NBR5-5.0. We talk about its four fundamental goals of Transparency, Holistic approach, Scalability and Modularity; and how each of those goals will be used to help us to continue to deliver the leading security service for protection of customer networks.

4.

SECURITY RESPONSE WEBSITE

This month, we have released a new Security Response website that you can find at:

<http://response.network-box.com/>

4.

APRIL 2011 FEATURES

The features and fixes to be released in this months patch Tuesday for NBR3-3.0. We continue to develop, and will continue to support, NBR3-3.0 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.



NBR5 Background

The Network Box product development cycle is to regularly issue incremental releases (as a standard part of our service) on the foundation of relatively infrequent major releases - rather than mimic our competitors who have (and charge for) frequent major releases and infrequent updates. We see that our approach better suits the requirements of protecting the security of our customer base, and gives us the ability to release new protection capabilities without waiting for a major new software release (with associated complexities of deployment).

The first Network Box firmware (NBR5-1.1) was released in the year 2001, and this was followed in the summer of 2006 by NBR5-3.0 (which is the version of our firmware that all our customers today are using). These base firmwares are kept up-to-date by frequent incremental updates of both protection signatures and new features, as part of our managed service.

Five years has now passed since the release of NBR5-3.0, and it is time to start to talk about the next major release of Network Box firmware - to be known as NBR5-5.0.

NBR5-5.0 Overview

During the second half of 2011, we intend to start releasing the first versions of NBR5-5.0. Starting with a base platform, followed by FW+, then higher-level services such as content filtering, anti-virus, anti-spam, and ending with the full UTM+ product (most likely early in 2012).

NBR5-5.0 will be supported on all current hardware (the S- M- and E- class boxes that have been released for five years now), and should not require any hardware upgrades. However, as always, we must point out that extra functionality (if enabled and used) may require extra hardware capacity.

NBR5-5.0 is designed, from the ground-up, to be Transparent, Holistic, Scalable and Modular. Let's talk about these four main design goals, to give you some idea of the approach taken in NBR5-5.0.



- **Transparency as a Philosophical Goal**
 - We will follow the 'do no harm' philosophy by attempting to influence the network traffic as little as possible, whilst still performing our security functionality
 - Given the choice between transparent or not, we will always prefer to be transparent
 - Whilst we will continue to provide non-transparent services (such as store-and-forward, acceleration by web caching and content acceleration, etc), all the core network and services will be transparent by default

NBR5-5.0 is Transparent

NBR5-5.0 applies transparency as a philosophical goal. The product is designed to have little impact on existing networks and to require as few changes as possible. Like a water filter, it is able to be installed in-line with the water (network traffic) and to filter out the dirt (viruses, spam, etc) without affecting other flows.

The connection between the box and NOCs is also simplified. NBR5-5.0 boxes connect back to their management NOCs (or other Network Boxes in a cluster) using single SSL-encrypted connections. The NOCs (and management boxes) then communicate with the box using these individual management links.

NBR5-5.0 is Holistic

Most UTM systems today are designed using a reductionist approach. They reduce the complex problem of network security to fundamental parts (such as anti-virus, anti-spam, firewall, etc) and deliver these as individual solutions. Although named 'Unified', in practice this approach does not lead to unification - other than that they are all running and maintained on the same appliance. To put it simply, the administrative interfaces are still broken apart by module.

NBR5-5.0 is designed, from the ground up, to provide a Holistic Security Management platform, and to extend that platform with security modules that both fit and work together in a holistic manner. We take several key technologies (including an entity model, unified logging and configuration) to provide a single Holistic User Interface.



NBR5-5.0 is the first Holistic Security Platform

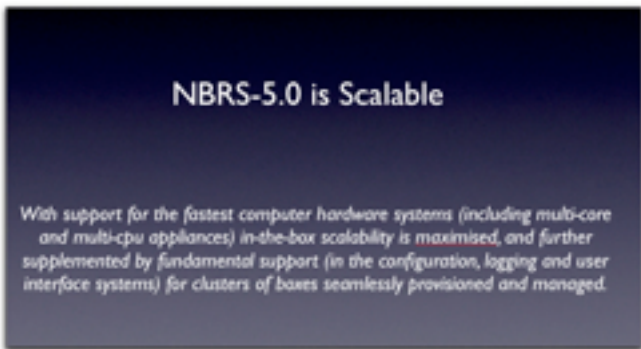
Modular, but integrated in a way never before seen, to provide a single holistic view both of the network and of the entities using it.

NBRS-5.0 is Scalable

The previous example of the water filter introduced the goal of transparency not interfering with the flow of network traffic. Capacity planning is a continuing problem for computer systems, as traffic and usage patterns continue to increase. Scalability is the key to meeting this goal.

NBRS-5.0 addresses scalability in two ways: in-the-box by supporting multi-core and multi-cpu appliances, and out-of-the-box with fundamental support for clustering of boxes into a single seamless solution.

With both high-availability and load-balanced approaches, the cluster can be centrally managed and traffic will be balanced both within the box (across CPU cores) and within available cluster devices. Unified logging and configuration systems make configuration seamless - a single change to a parameter is replicated and deployed across the cluster (either within an office, or across a globally dispersed organisation). Cluster configuration and log replication is automatic and can be flexibly deployed in a variety of configurations.



NBRS-5.0 is Modular

NBRS-5.0 is designed as a base platform, with security service components that can easily be installed and removed. The base platform consists of a kernel, a user space tool chain, a logging system and a configuration system - essentially an extremely sophisticated router. It is the security service components that provide the UTM+ functionality.

The advantages of this base platform approach are a reduction in firmware size (both in memory and on disk), no requirement for installation of services not required, simplification of deployment, and most importantly a clarity of thinking in what is being provided.

Not only does the entire UTM+ solution get to be best in class, but each individual component gets to stand up on its own and be compared to others. Individually, the components of NBRS-5.0 are best in class, and working together they combine to provide the most effective, affordable and comprehensive network security system.

Conclusions

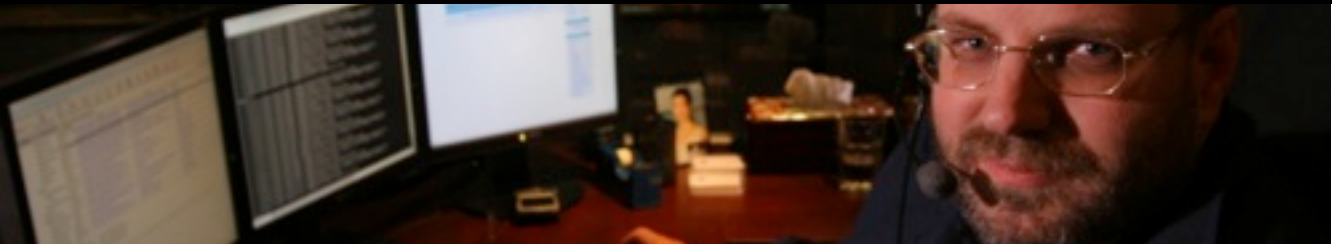
NBRS-5.0 is designed to be Transparent, Holistic, Scalable and Modular.

- Transparency will minimise the impact on existing networks, requiring as few network changes as possible.
- A holistic design will ensure that the individual components of the security system work together in the same way, to provide a seamless management experience. Deployment of additional components will extend the security capabilities of the product, without needlessly extending the complexity.
- Scalability will ensure that the flow of traffic through an individual appliance is as optimised as it can be - fully making use of all available resources (cpu cores, memory, disk and bandwidth). And, should the capacity of a single appliance be exceeded, or the customer require further resilience to hardware failure, scalability can be further extended across a cluster of appliances.
- The modular approach, will ensure both best-in-class components as well as a best overall security solution.

The first versions of NBRS-5.0 are targeted to be released in the second half of 2011. Starting with a base platform, closely followed by FW+, then higher-level services such as content filtering, anti-virus, anti-spam, and ending with the full UTM+ product (early in 2012).

Over the coming months, each month we will be presenting one aspect of the NBRS-5.0 product in this Boxing Ring newsletter, to keep you informed as to progress and to explain what NBRS-5.0 means to you and how we intend to meet our goal of continuing to deliver the leading security service for protection of customer networks.





April 2011 Features



On Tuesday, 5th April 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:

- Further enhancements to the Global Monitoring System (GMS), and improved performance and functionality in the ticketing of GMS issues.
- Performance enhancements to the Network Box web proxy policy engine (in particular for sites with large numbers of users and/or rules).
- A change to the quarantine release eMail message to better support Outlook 2007/2010 mail clients.
- Enhancements to the protected service proxy system to better handle configurations with multiple redundant connections.
- 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.

Security Response Website

This month, we have released a new Security Response website that you can find at:

<http://response.network-box.com/>

The new site is designed to showcase our network and protection services - backed by real numbers. Under 'network' you can see the health of our network, globally, and find our regional security operation centres. Under 'protection' you can find the details on the protection engines running under the five main classes of protection we offer. Under 'Services' you can see our key service metrics. Finally, the Internet Health and Statistics tabs show you the current health and key statistical metrics for the Internet. We hope you like it.



MARCH 2011 NUMBERS

Key Metric)	#	% difference (since last month)
PUSH Updates	472	-22.7
Signatures Released	287,830	+2.3
Firewall Blocks (/box)	710,068	-3.9
IDP Blocks (/box)	131,447	+31.3
Spams (/box)	21,230	-15.8
Malware (/box)	747	+6.0
URL Blocks (/box)	114,955	-3.9
URL Visits (/box)	3,905,495	-0.8

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

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