In The Boxing Ring

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

Welcome

Welcome to the June 2011 edition of 'In the Boxing Ring'. Continuing on from April's format changes, we have a new look this month, 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 base platform. consisting of a kernel, a user space tool chain, configuration and logging systems - essentially, an extremely sophisticated router. It serves as the platform upon which we build our security appliances and higher-level functionality.

The NBRS-5.0 base provides a foundation for our security products, but is not a security product itself. Building on the base, highly-granular Security Modules will be offered to provide the security functionality itself.

By focusing each security module on the task it is designed for, and designing security modules to work together (taking advantage of facilities offered), we can optimise and maximise the security capabilities of the product. An example of this is Web Client vs Web Server protection. While you can look at this as just HTTP protection, the requirements for the two sides are very different, and optimising the protection support to the particular problem offers tremendous benefits to the protection that can be deployed (as well as minimising side-effects).

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), 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

June 2011

IN THIS ISSUE

The NBRS-5.0 Base Platform

For this month's topic on NBRS-5.0, we'll be presenting information on the 'Base Platform' design concept, and how we are using it to provide a modular, but holistic, security platform.

Firstly, let's answer the question 'What is the Base Platform'? It consists of a kernel, a user space tool chain, configuration and logging systems - essentially, an extremely sophisticated router. It serves as the platform upon which we build our security appliances and higher-level functionality.

The NBRS-5.0 Kernel

The kernel is a customised version of Linux 2.6 and is primarily responsible for process, memory and I/O management - in particular network I/O. Operating in a combination of bridged, routed and NAT modes, the kernel is responsible for moving network traffic between network interfaces on the box, as well as internally directing that traffic to the appropriate security modules, to apply security and organisational policies. A combination or kernel (for high performance) and user space (for in-depth inspection) approaches are used.

- Native IPv4 and IPv6 Support
  - Fully standards-compliant IPv4 and IPv6 stacks
  - Uses a dual stack approach
  - NAT support within IPv4
  - Translation capability for IPv4 <-> IPv6 traffic
  - Full IPv6 support at all layers

As with NBRS-3.0, sophisticated policy-based routing is available, with both static and dynamic routing protocols supported (for both IPv4 and IPv6). Multi-link, Multi-home and Multi-route configurations are supported, and a kernel-based route-cache approach is used to optimise performance.

The NBRS-5.0 User Space Tool Chain

The user space tool chain is used for basic system operations, and is responsible for system startup and shutdown. A parallelised control system is used in order to minimise startup times by initialising the many parts of the system in parallel (using multiple CPU cores and disk subsystems).

The NBRS-5.0 Configuration System

- A configuration system
  - A single unified configuration store, including:
    - Revision Control
    - Auditing
    - Clustered Replication
    - Bi-Directional Sync

In the May 2011 edition of In The Boxing Ring we spent some time presenting the configuration system coming with NBRS-5.0. How we've taken all the customer feedback from the past ten years of providing a managed service, and built it into a system capable of meeting the needs of our customers (as well as the regulatory and compliance requirements of their security auditors). Combined with full access control and auditing - securing the configuration, both on the box and on the cluster.

By unifying the configuration into a single store, and providing support for revision control, auditing, cluster replication and bi-directional sync, we've extended what we had with NBRS-3.0 from the NOC to the BOX.

The NBRS-5.0 Logging System

The NBRS-5.0 logging system is called NBSYSLOG. It is a single unified logging system, fully compatible with (but greatly extended from) the SYSLOG standard. At its core, it provides a highly-optimised switch capable of receiving, filtering, switching and sending/storing log messages via a selection of delivery agents. It is transactional by design, to ensure reliable in-order delivery of log messages, with automatic recovery from link/storage failure.

- The NBRS-5.0 logging system is called NBSYSLOG
  - It is a single unified logging system, including:
    - Rich, complete, logging messages
    - A switch to distribute these messages
    - Delivery agents to transmit these messages
    - A database store to permanently record logs

We will be providing a large selection of delivery agents, including: SYSLOG, NBSYSLOG (via NBSYNC protocol between a cluster of boxes), log file output, database output, data export reporting, and email alerts.

The database used to record the logs is a transactional ACID compliant database, offering row-level locking and concurrency control. This allow us to provide a highly-optimised storage model for the transactional logs, real-time summary capability, and the important ability to continue to insert new logs and summary information into the database at the same time that analytical reports are being produced. An object-based approach towards messages, and rich message structure, dramatically reduces the number of messages required to contain a piece of information.

NBRS-5.0 Security Modules - Building on the Base

The NBRS-5.0 base provides a foundation for our security products, but is not a security product itself. Building on the base, highly-granular Security Modules will be offered to provide the security functionality itself.

By focusing each security module on the task it is designed for, and designing security modules to work together (taking advantage of facilities offered), we can optimise and maximise the security capabilities of the product. An example of this is Web Client vs Web Server protection. While you can look at this as just HTTP protection, the requirements for the two sides are very different, and optimising the protection support to the particular problem offers tremendous benefits to the protection that can be deployed (as well as minimising side-effects).

Service packages will continue to be offered, and customers given the choice between 'à la carte' and the current 'buffet' offerings.

We plan to release a suite of security products, all built on the same secure base platform and all operating seamlessly together. The modules can operate either on the same appliance, or across a cluster, depending on performance and architectural requirements.

- The NBRS-5.0 Base
  - Provides a foundation for our security products
  - Is built using secure coding principles
  - Is maintain using secure practices
  - But is not a security product itself

- Service Packages (FW+, CF+, AV+, UTM+)
  - Will continue to be offered
  - But will now be augmented with a selection of optional security modules
  - This will allow us to expand the product (building on the base in a structured, expandable manner)
  - It will also allow customers to choose 'à la carte' as well as the current 'buffet' offering

Security Modules Offered

While the full list of available security modules, pricing, service packages and availability will be released later this year, the table below should give you some idea of the sorts of modules we will be offering, and how they are designed to be granular and stand-alone, yet capable of inter-operating to produce a highly customised security solution.

NBRS-5.0 Security Modules (*preliminary information, subject to change*)	
Router (IPv4, IPv6, NAT, Bridged, Routed modes)	Scanning, Policy and Control for FTP clients
High Availability	Scanning, Policy and Control for FTP servers
Load Balancing	Scanning, Policy and Control for Mail
Clustering	Scanning, Policy and Control for Web Clients
Quality of Service	Scanning, Policy and Control for Web Servers
Application Identification and Policy Control	Scanning, Policy and Control for IM Clients
Firewall (including IPv4 and IPV6)	Internet Acceleration and Cache
Intrusion Detection System	Intranet Web Portal
Intrusion Prevention System (both active and inline modes)	Encryption Services
Virtual Private Networking	PCI Compliance
Web Server Application Firewall	Data Leakage Prevention
Anti-Spam	Network Vulnerability Scanning
Anti-Virus	NOC Services
Web Filtering	... *and many more*

Modularity is often the result of a reductionist approach to systems development. However, modular and holistic approaches are not mutually exclusive.

NBRS-5.0 is the first Holistic Security Management 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.

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

June 2011 Features

On Tuesday, 7th June 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:

- Continuation of the phased deployment for configurable heuristic support in the Kaspersky anti-virus scanning engine. Support for this has been in internal beta for some time now, and we will be continuing the rollout of this to all customers. The new configurable heuristic support allows the heuristic level within the Kaspersky anti-virus engine to be set, on a per-box basis, to Off, Shallow, Medium or Detailed (with individual settings for mail and http scanning).
- Minor enhancements to the health monitoring system.
- Enhancements to the kernel-level ethernet drive for Intel ethernet chipsets.
- 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.

Tolly Group

Tolly Group, in conjunction with AV-Test GmbH, a leading IT security testing laboratory from Germany, just issued a report, showing that Network Box is 100% effective against Extended WildList Malware, for POP3, HTTP, and SMTP.

As one of the world's leading Managed Security Services, Network Box has long said that the best protection against hackers, malware, and undesirable content, is to use a multi-engine approach, augmented by real-time PUSH updates, and real-time in-the-cloud technology.

Network Box's award winning Z-Scan zero day anti-malware system for example, uses state- of-the-art in-the-cloud technology, to help ensure new viruses are blocked in as little as 3 seconds from the time they are launched.

It is one thing to talk about effectiveness however, and another to prove it.

Network Box recently commissioned The Tolly Group (USA), in conjunction with AV-Test (Germany), to test Network Box's anti-malware technology against their Extended WildList. Malware samples included viruses, worms, root kits, and back doors. These malicious files were all tested across HTTP, POP3, and SMTP protocols. Network Box proved 100% effective.

For more information, please see
http://www.network-box.com/tolly_nb_malware_report_2011

MAY 2011 NUMBERS

Key Metric	#	% difference (since last month)
PUSH Updates	612	-3.3
Signatures Released	163,935	-31.7
Firewall Blocks (/box)	767,402	-1.0
IDP Blocks (/box)	106,661	-24.9
Spams (/box)	16,183	-17.7
Malware (/box)	687	-26.3
URL Blocks (/box)	134,081	+15.9
URL Visits (/box)	3,985,257	+4.7

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