

In The Boxing Ring



IN THIS ISSUE

2. NETWORK BOX INTRUSION DETECTION AND PREVENTION

The new Network Box Intrusion Detection & Prevention system now offers four operation modes.

3. NETWORK BOX OFFICE CUSTOMER PORTAL HINTS

Hints and tips for using a single simple powerful web-based user interface for the management of one or more Network Boxes.

3. PUSH TECHNOLOGY

Advantages of PUSH Technology are highlighted and the new, patented HQPUSH system is announced.

4. JUNE 2009 FEATURES

The ongoing deployment of our recently released features and enhancements.

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

Welcome

Welcome to the June 2009 edition of 'In the Boxing Ring'. In this edition, we focus on how the new Network Box Intrusion Detection & Prevention system operates in four modes: Frontline IPS, Passive IDS, Active IDS and Inline IPS. Turn to page 2 for details.

With the roll out of the Network Box Office Customer Portal, and technical details already covered in the previous issue of *In the Boxing Ring*, this issue looks at hints and tips for using the system. Page 3 provides further information.

Also on Page 3, we explain more about PUSH Technology and its advantages. We also announce the new, patented HQPUSH system that offers improved performance in delivering protection updates.

In our June features, we also have the usual allotment of updates to the

NBRS-3.0 system, enhancements to the scanning engine, further support for four more new spam signature types, and performance improvements to the system. Turn to Page 4.

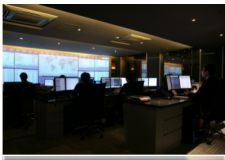
As usual, if you have any feedback, or comments, they are always appreciated. You can contact us here at HQ via email (nbhq@network-box.com). Or, drop by our office next time you are in town.

You can also keep in touch by following our new Network Box Security Response twitter feed at:

twitter.com/networkboxhq

Mark Webb-Johnson
CTO, Network Box Corporation
June 2009





Network Box Intrusion Detection & Prevention

In the May 2009 edition of *In The Boxing Ring*, I announced the start of a beta test of a new Intrusion Detection & Prevention System for Network Box. The beta testing is now ongoing, and excellent results are being shown with this new technology. So, this month, I would like to give you more information on what the technology does and where we are going with it.

Diagram (1) demonstrates the security architecture of Network Box for a typical system using this technology. Traffic passing between the three interfaces passes through the five layers of Network Box protection.

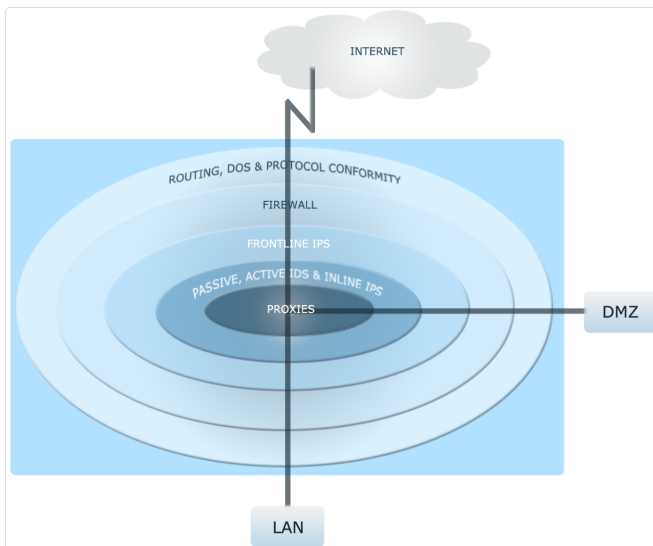


Diagram 1: Security Architecture of Network Box for a Typical System

- 1) The first protection layer provides basic routing, denial of service protection and protocol conformity. This layer is handled closest to the hardware and provides protection against routing, protocol obfuscation and load-orientated attacks.
- 2) The second protection layer is the firewall. At this layer, traffic that does not conform to firewall policies is blocked.
- 3) The third protection layer is the Frontline IPS system. This offers extremely lightweight, zero-latency, protection against worms, exploits and other such attacks.
- 4) The fourth protection layer is the new NBIDPS system. This offers passive IDS, active IDS and inline IPS protection using sophisticated rules and protocol / stream decoding engines.

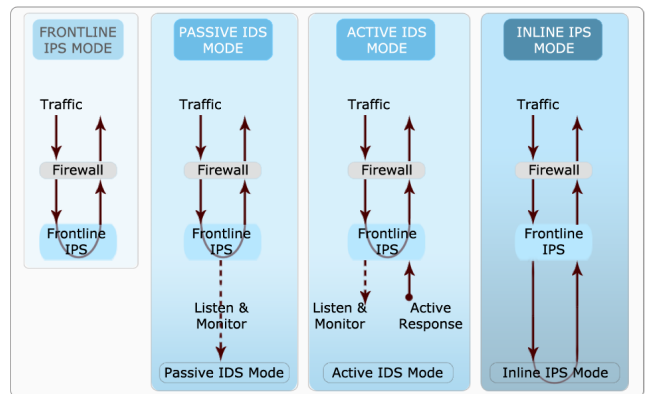


Diagram 2: New NBIDPS Engine - 3 Modes

- 5) The fifth protection layer consists of a set of Protected Services Proxies for specific protocols, such as POP3, IMAP4, SMTP, HTTP and FTP. These provide application-layer protection against malware, spam, protocol enforcement and policy violations.

By separating the protection into five highly-configurable, yet integrated, layers, Network Box is able to offer the best security given monetary and performance constraints.

At its foundation, the new NBIDPS system uses the open-source Snort engine. This is modified extensively to fit into the Network Box security model, logging and management framework. This allows us to use industry-standard format signatures and heuristics, and gives us a powerful rules language, as well as more stream and protocol decoders.

Diagram (2) represents the four modes that Network Box now provides. In passive and active IDS modes, the engine is run separately from the network traffic stream to minimise the performance impact and offer options to limit visibility of the monitoring on the network. The inline IPS mode allows the engine to run inline with the traffic stream and offers zero-latency response to attacks.

Intrusion Detection (passive and active IDS) and Intrusion Prevention (IPS) systems have their places in network security. An industry first, the new Network Box system combines the four approaches into a single unified platform and allows the technology and tools to be best applied on an individual device basis.

This will be a zero-cost addition to our offering to all NBRS-3.0 FW+ (or above) clients as part of our ongoing service and monitoring – performance willing. Beta testing has already started and we estimate that this new system will be available for full release during July 2009.



Network Box Office Customer Portal Hints

In last month's In the Boxing Ring, we covered an overview of the Network Box Office Customer Portal. As a quick recap, the Customer Portal provides a single, simple powerful web-based user interface for the management of one or more Network Boxes – at the country,

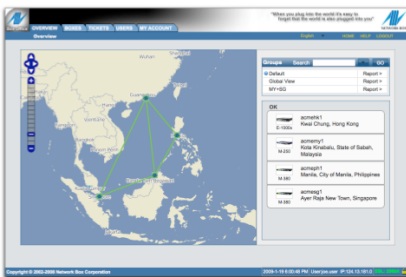


Fig. 1 – Overview Screen

regional and global levels. It went live globally on 12 May 2009.

Access to the Customer Portal is via <https://boxoffice.network-box.com>. After entering your User ID and Password, you will be greeted with the Overview screen which shows the network of your Network Boxes against a geographical background.

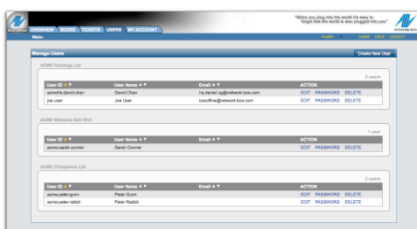


Fig. 2 – User Management

With the Customer Portal fully in use, I have provided three usage hints in this issue to improve user experience and help you make better use of the Portal:

1) The User Management Module: Permits designated client administrators to view and maintain Network Box Office users.

Selecting the *USERS* tab will display a list of users and their owners.

Use the *USERS* tab to create, delete and update Network Box Office user accounts for your users.

Each user has three options: *Edit* their preferences record, reset the user's *Password* and *Delete* user account.

You can also *Create New User*.

2) The Preferences Module: Users can edit their profile using the *MY ACCOUNT* tab and clicking the *Edit Profile* button.

Users are able to modify the following fields:

- User Name.
- eMail Address.
- Want Ticket eMail (tick if you want to receive email notification of ticket changes) and Preferred Ticket Template (the template format for email messages you require).
- Preferred Language (choose from the list of available languages).
- Preferred Portal (choose from the list of available regional mirrors).
- Newsletter Preferences (whether you want to receive newsletters from Network Box regarding security-related news, and technical and security announcements).

Users can also use the *Change Password* button to change their password.

3) Saving Custom Searches: The Customer Portal allows users to search for open and recently closed tickets and save your search query using the *TICKETS* module's Search function.

Search criteria allow you to specify any combination of *ticket number*, *boxid*, *status*, or *text*.

This function also gives you the opportunity to always display your saved search on the *TICKETS / OVERVIEW* page.

The Customer Portal provides many key functionalities enabling the user to effectively manage their Network Boxes.

There is similar functionality in *BOXES* to allow you to save common box reports.

Users can find further tips and hints in the User Guide.



PUSH Technology

Since its launch, Network Box has focused on optimising

its PUSH technology, as the best way to get security updates onto the devices providing the protection

PUSH Technology provides three primary advantages over PULL:

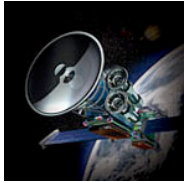
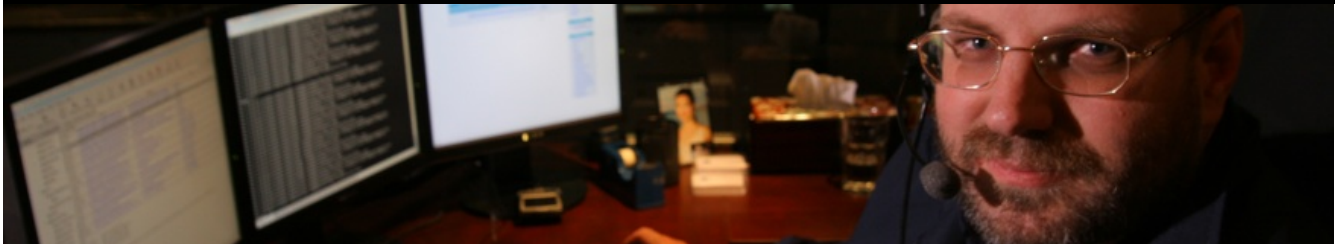
- 1) Speed – Reduces latency (the time from when the update is available until when delivery commences) to a minimum.
- 2) Acknowledgement – Allows for the provider to be certain that updates are installed and activated correctly.
- 3) Optimization – Provides for optimization of the update system, from the provider's point of view (making the most optimum use of the provider's network for delivery of updates, in both resource utilisation and source of updates).

Real world experience with PULL vs PUSH also backs up the clear statistical and mathematical analysis. PUSH Technology, quite simply, offers the best way to deliver updates to the signatures and code on protection devices.

We are pleased to announce that on 20 May 2009, we completed the migration of all our NOCs to our new patented HQPUSH system. This new system offers improved performance and optimisation of PUSH updates. It allows us to continuously, and concurrently, monitor all our sources of security signatures, and to PUSH out changes within seconds. With this new system, updates are currently being installed on regional NOCs within 3 seconds of their release, and on all end-user Network Boxes, globally, well within our targeted 45 seconds from release. This is orders of magnitudes faster than the industry standard.

For further information, please see our PUSH Technology white paper at:

<http://download.network-box.com/whitepapers/WP-PUSHTechnology.pdf>



June 2009 Features

On Tuesday, 2 June 2009, we will be releasing a number of bug fixes and enhancements for NBR3-3.0. These changes include:

- Enhancements to the scanning speed and control of scan times for our mail scanning engine.
- Support for four new spam signature types (backscatter, sender-id, from-to pair and message subject) for our mail scanning engine.
- Improved simplified Chinese translation for Box Office, and download link to User Guide (HELP menu).
- Minor cosmetic changes to my.network-box.com administrative interface.
- Performance improvement for health monitoring system on S-50, S-80 and M-250 models.

The above changes will not require any impacting service or device restarts, and should not cause any significant interruption to device operation. The regional NOCs will be conducting the rollouts of the new functionality in a phased manner.

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

June Hint

The newly released Network Box Office Customer Portal fully supports a hierarchy of ownership. If you have multiple boxes, in different, or the same, locations, owned (and controlled) by different parts of your organisation, that structure can be reflected in the Inventory records we keep and can be used to control the visibility of boxes and tickets.

For example, if you have boxes in the UK and the USA, it is possible for us to configure the system for you so that staff in your UK office have access to the UK boxes, staff in your USA office have access to the USA boxes, and staff who need global access can see all boxes (and tickets).

Talk to you local support NOC if you need assistance with this.

Conclusions

Thank you for your support of Network Box, and the continued entrustment of your network security to our managed service. I hope you find this communication useful – if you have any suggestions, they are most appreciated, and should be directed towards your local NOC or account manager. Please don't hesitate to contact us for assistance.

Mark Webb-Johnson
CTO, Network Box Corporation
June 2009

MAY 2009 NUMBERS

Key Metric)	#	% difference (since last month)
PUSH Updates	944	-22.1
Signatures Released	329,611	+58.2
Firewall Blocks (/box)	618,154	-1.9
IDP Blocks (/box)	139,190	+0.1
Spams (/box)	83,060	+27.7
Malware (/box)	1,725	+28.7
URL Blocks (/box)	70,199	+18.6
URL Visits (/box)	2,752,585	+5.4

NEWSLETTER STAFF

Mark Webb-Johnson
Editor

Pauline Chiu
Michael Gazeley
Jason Law
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