

# In The Boxing Ring



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

### Welcome

Welcome to the May 2010 edition of 'In the Boxing Ring'. In this edition, we'll be continuing our look at Network Vulnerability Scanning, as well as the problem of classification of Spam vs Malware. We'll also be presenting the new version of our App for the Apple iPad.

On page 2, I spend some time presenting a new service offering by Network Box. In the summer of 2010, we will be launching an optional service providing three types of Network Scanning, offered both externally and internally. We are very excited at the opportunities that this new technology will afford us.

On page 3, I discuss the problem of classification of blended threats (in particular, looking at the question of spam vs malware), and give insight into the longer-term direction Network Box is taking with regard to this problem.

Also on page 3, I announce the availability of v3.2 of the Network Box iPhone App, including support for the upcoming Apple iPad. The new v3.2 version (providing native resolution support on the iPad) is about to be released.

On page 4, we present the usual monthly hint (this month regarding alerting policy), and outline the software updates delivered as part of this month's software release.

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](mailto:nbhq@network-box.com)). Or, drop by our office next time you are in town.

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

[twitter.com/networkboxhq](https://twitter.com/networkboxhq)

Mark Webb-Johnson  
CTO, Network Box Corporation  
May 2010



### IN THIS ISSUE

#### 2. **NETWORK VULNERABILITY SCANNING**

The second in our two-part discussion on the state of Network Vulnerability Scanning. This month, we discuss Network Box's approach to the problem.

#### 3. **SPAM VS MALWARE**

We outline the difficulty in differentiating between spam and malware, and how blended threats are merging the two into one.

#### 3. **IPHONE AND IPAD APP**

The launch of v3.2 of the Network Box App, with native iPad support.

#### 4. **MAY 2010 FEATURES**

As usual, we will be deploying our on-going enhancements and improvements as well as maintenance features to all NBR3-3.0 customers.

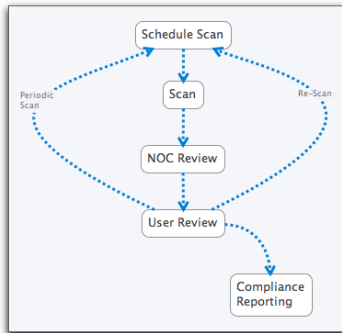
# Network Vulnerability Scanning



Last month I described what Network Vulnerability Scans are, and how they can be beneficially used for both compliance and pro-active protection of your network. This month, I'm proud to announce that starting in the summer of 2010, Network Box will begin to offer Network Vulnerability Scanning services, as an optional service to all our customers.

The Network Box approach adheres to the following flow:

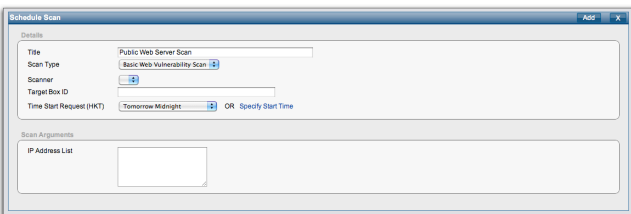
1. A scan is scheduled.
2. The scan is conducted.
3. The Network Box NOC reviews the scan, investigates the results, and comments, as appropriate.
4. The end-user reviews the scan results, and exports management and compliance reports (in both HTML and downloadable PDF format).
5. Facilities are provided for the end-user to classify each result for follow-up (including comparison of results from periodic scans, and re-scans to verify correctness of compliance actions).



At launch, Network Box will be offering three forms of scan:

- Network Mapping (identifying network equipment, and fingerprinting its identity).
- Comprehensive Vulnerability Scan (including identification of known vulnerabilities and suspicious applications).
- Comprehensive Web Server Scan (including scans targeted specifically at web servers and their unique vulnerabilities - such as SQL injection).

By offering the 'NOC Review' stage of the scan, Network Box experts review the results of each scan and can make recommendations unique to the client environment. This largely resolves the high false-positives problem experienced by users of automated scanners.



Network Box will offer these services both externally (via scanners located on the Internet, offering an external view of the network) and internally (via scanners placed inside the customers environment, offering an internal view of the network). Both types of scans, and the results produced, can be reviewed using the same Box Office interface.



Scan results are categorised on a six-point sliding scale ranging from 0 (Informational) though 5 (Urgent). This scale allows impacting results to be immediately targeted for remedial follow-up. A graphical drill-down user interface, within the Network Box Office framework, allows for quick and easy analysis of results. PDF reports can be downloaded, for full compliance and management reporting.

An important aspect of the Network Box approach is the inclusion of follow-up actions to allow for full integration into a compliance framework. Each scan result can have a follow-up action assigned, to allow compliance actions to be tracked through to incident closure. This mechanism is fully supported within the periodic and repeat scanning systems, allowing the system to automatically highlight discrepancies in the compliance follow-up system (such as items which have been marked as resolved, but still appear in subsequent periodic or repeat scans).



While the NOC teams maintaining the firewall and conducting the scans are separated (to allow for a clear delineation between maintenance and review functions, over and above those provided by the end-user), the close integration of the Network Box devices and scanning systems, allows the scan to be tuned to the environment being scanned. This provides for the best, most accurate, result with the least number of false-positives and misses.

Correctly used, and expertly handled, vulnerability scans are an invaluable tool for pro-active protection of your network. We here at Network Box are very excited with the capabilities that this new offering will give us (both for customers who require compliance reporting, as well as for those who merely desire it).

We expect to start public beta testing this new service offering during June/July 2010, with a full public release coming later in the summer.



## Spam vs Malware

A cursory glance at this month's statistics shows spam volumes down 23.7% and malware volumes up 1,798% - perhaps this needs some explanation!

Looking at the raw numbers:

- March 2010 saw 45,820 spams and 767 malwares per box, for a total of 46,587 unwanted messages per customer per box.
- April 2010 saw 34,944 spams and 13,791 malwares, totaling 48,735.
- So, while spams decreased 23.7% and malware increased 1,978%, the total difference is only +4.6% March -> April.

Early in April 2010, we started to see a massive eMail spam campaign advertising links to malware hosted on compromised servers (and in some cases directly attaching the malware to the eMail message). In co-operation with our partners, we immediately classified these servers as hosting malicious content (in some cases malware, in some cases spam, and in others phishing sites). As the same servers hosted all three types of content, it was hard to classify precisely the threat (as there were three threats involved), so Network Box and our partners had to take the approach of classifying them as the most-malicious (in some cases malware, and in others phishing). Our technology allows us to classify down to the URL path level, but often individual URLs were serving up all three types of unwanted content, depending on per-email parameters passed.

Irrespective of whether an eMail is a spam, porn, hoax, virus or phishing, it is 'unwanted'. The total volume of unwanted eMail did not change significantly throughout the month. What did change is the percentages of each type.

The core issue is that just as the threats have become blended, the difference in classification is also becoming blurred. A compromised web server is just as likely to serve up a spam site as it is a phishing site, or hosted malware.

Providing protection against such attacks is often only possible with multi-faceted technologies such as those offered by Network Box. The botnets spew out eMail malware and spam by the billions; the vast majority blocked by anti-spam and anti-malware engines at the gateway. Visiting a link in such an eMail gives the Network Box content filtering engines an opportunity to block the threat (either via policy against such sites, or engines such as Google Safe Browsing to block known malicious sites). Such sites host toolkits of automated vulnerability exploits, which the Network Box IDPS system has been designed to address. And, finally, the malware itself may be blocked by HTTP anti-virus systems. Only by operating a multi-layer and multi-protocol security system with all components working together, such as Network Box, can we achieve comprehensive protection against such threats.

Which leads us to the future. Where is this technology taking us and how can we maintain and improve our technological lead in protecting against such blended threats? Here at Network Box, we believe the core approach of content classification is correct. Our primary focus is on improving such classification, but also on introducing systems to provide for multi-categorisation of a single threat.

When you visit a web site which is a personal blog concerning shopping, should this be classified as 'Blogs' or 'Shopping'? We believe the correct answer is 'both', as such an approach offers the best granularity and support for precise policy control.

Introducing support for fine-grained multi-categorisation, will task the Network box device with accurately classifying a threat (eg; virus, phishing, spam, hoax, shopping, bulk email, executable attachment, etc), and then permit the individual customer policy to control how those categories are handled (eg; block and quarantine viruses, or deny access to Adult websites, as policy). This is the direction we are headed, and we will continue to deliver more and more systems adhering to this framework over the coming year.

## App v3.2

Version v3.2 of the Network Box iPhone / iPod Touch / iPad App is now ready and should be available on the Apple App Store early in May 2010.

This version is a "universal App" - meaning that one binary supports all the current Apple hardware (iPhone, iPod Touch and iPad) at native resolutions.

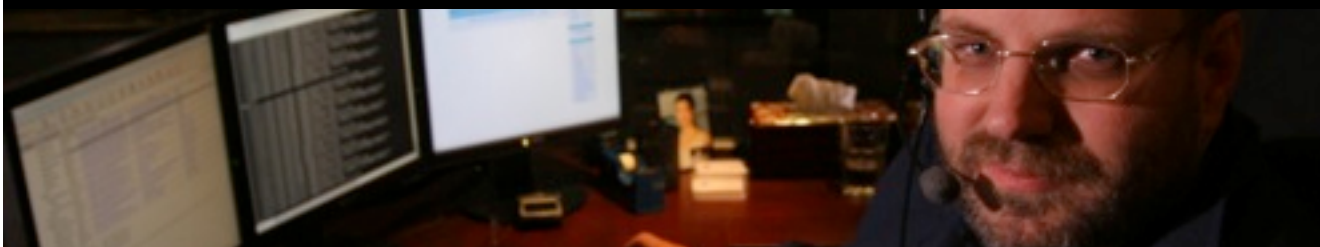
As well as support for the 1024x768 resolution of the iPad, the new version also adds support for the larger keyboard (as well as external/bluetooth keyboards).

- Compatibility with v3.2 of the Apple OS (as well as tested against v4.0 beta releases).
- Support for the Apple iPad at native 1024x768 resolution.
- Support for iPad-specific features (such as message pop-ups and message entry screens).
- Improvements to ticket entry/update screens, allowing for direct entry of the ticket text.
- Improvements in local caching for improved performance
- Auto-Refresh enhancements to main views (showing previous cached content, while retrieving the latest content from the server)
- Auto-Refresh enhancements to global map (showing previous cached map, while retrieving the last status from the server).
- Minor bug fixes

The v3.2 update will be delivered as a standard free-of-charge update through the Apple App store. We expect that this update will be available early in May 2010, but the approval and release schedule is dependent on Apple.



Network Box v3.2 iPhone/iPod Touch/iPad App



### May 2010 Features

On Tuesday, 4<sup>th</sup> May 2010, 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 firmware support for new box models.
- Enhancements to the Box Office portal, to support the v3.2 iPhone/iPad application.
- Mail scanning enhancement to support detection of broken ZIP archives and optionally block message containing them.
- Mail scanning enhancement to allow for per-box configuration of alert message suppression.
- Mail scanning enhancement to introduce a fuzzy fingerprint type for message structure and to allow that to be used for anti-spam and anti-malware systems.
- Improvements to the reliability of the IPSEC VPN service, to better cope with mis-matched negotiation parameters. Also includes enhancements to the health monitoring system to add additional checks regarding IPSEC VPN renegotiation health.
- Improvements to the Protected Service Proxy system, related to the transparent SMTP proxy.

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.

### April Hint: Alerting Policy

Each Network Box contains a sophisticated set of configurable policies related to how spam and malware should be treated. Quarantines can be enabled, and notification emails sent to combinations of the sender, recipient and/or administrator in the event of a malware block.

However, great care should be taken with this facility. The internet is under deluge from such notification eMails.

- Sender notifications are a nuisance when the sender is spoofed - inundating the sender with bounce messages for eMails he never sent.
- Recipient notifications, while useful in some cases (such as policy blocks) may overwhelm recipients in the event of a new outbreak.
- Mail Portal reports should be limited to known valid recipients (using a mechanism such as envelope verification to avoid generating non-deliverable bounces).

Network Box offers a Global Notification Suppression (GNS) system that can suppress these alerts for the most common types of mis-notification (for example suppressing sender notifications where we know the sender to be spoofed). This can be configured on a per-box basis (as well as having a global default).

Please talk to your local support NOC to ensure that your notifications are as you require and are not adding to the overall pollution on the Internet.

Mark Webb-Johnson,  
CTO, Network Box Corporation

### APRIL 2010 NUMBERS

Key Metric)	#	% difference (since last month)
PUSH Updates	1,106	+8.2
Signatures Released	127,140	-50.1
Firewall Blocks (/box)	692,125	+10.1
IDP Blocks (/box)	176,813	+9.3
Spams (/box)	34,944	-23.7
Malware (/box)	13,791	+1,798.0%
URL Blocks (/box)	86,141	+10.1
URL Visits (/box)	3,264,743	+0.2

### NEWSLETTER STAFF

**Mark Webb-Johnson**  
Editor

**Michael Gazeley**

**Jason Law**

**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)