

# In The Boxing Ring



## IN THIS ISSUE

### 1. A QUIET MONTH

This has been a quiet month, with lots of work going on behind the scenes in Box Office and NOC support systems (ready for new product feature launches in 2010Q3).

### 2. NETWORK BOX TRANSPARENCY

The Network Box is often configured as a transparent proxy. What exactly does this mean, and what impact does it have on your network?

### 3. JUNE 2010 FEATURES

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

### 3. JUNE 2010 HINT

All too often we find that configuration changes are delayed due to problems gathering information from our customers. We realise that such communication issues will always occur with a managed service such as ours, but continually strive to keep these to a minimum.

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

### Welcome

Welcome to the June 2010 edition of 'In the Boxing Ring'. May has been a relatively quiet month, with lots of work going on behind the scenes in Box Office and NOC support system (ready for new product feature launches in 2010Q3). More on this in the upcoming July and August newsletters.

As previously announced, we released the v3.2 iPhone/iPodTouch/iPad App, and Apple approved the App for release. It is now available on the Apple iTunes App store for upgrade/install.

On page 2, I discuss Network Box transparency. The Network Box is often configured as a transparent proxy. What exactly does this mean, and what impact does it have on your network? We always try to configure Network Boxes with minimal impact on your network, and transparency features keep this as flexible as possible. These features also allow for the Network Box to act as a client to customer servers for such things as authentication and email address verification - reducing duplication of information whilst also avoiding synchronisation, privacy and security issues.

On page 3, we present the usual monthly hint (this month regarding how best to work with the NOC for configuration changes and other support), 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

June 2010



## Network Box Transparency



The Network Box is often configured as a transparent proxy. What exactly does this mean, and what impact does it have on your network?

As defined by Wikipedia, *a proxy acts as an intermediary for requests from client seeking resources from other servers. A client connects to the proxy server, requesting some service, such as a file, connection, web page, or other resource, available from a different server. The proxy server evaluates the request according to its filtering rules.*

Network Boxes include proxies for services such as HTTP, FTP, SMTP, POP3 and IMAP4, and these can be configured as transparent (ie; operating transparently to the client/server, without any configuration changes required on either). In general, this is the preferred configuration (for simplicity purposes, as well as to minimise the impact on existing networks), although other configuration are possible (in particular when requiring the client to authenticate to the proxy so as to be able to define policies and track usage by user id rather than just source IP).

Network Box transparent proxies work by redirecting client connections to be answered by the proxy service (rather than the remote server). Once redirected, the proxy service itself makes a new connection to the remote server, transparently joins the two connections together, then passes the data back and forth between the two connections (whilst simultaneously applying filtering policies, protocol rules, and scanning of the data passing between the client and the server).

A common requirement for proxies is to be able to filter and authenticate based on a database or service not actually on the proxy itself. In such cases, the proxy acts as a client to some external service (passing on the role of authentication or database lookup to the remote service). The advantages of such an approach are that it reduces the duplication of information and avoids synchronisation, privacy and security issues. Network Box has excellent support for such services, and in particular:

- The SMTP proxy has the ability to either transparently pass through SMTP authentication (for third-party relay permission) to the remote smtp server, or to handle the authentication itself (via a large number of configurable authentication helpers).
- The SMTP mail scanner has the ability to perform envelope verification of recipient (and optionally sender) email addresses, either using a remote SMTP server's existing VRFY or RCPT-TO facility, or via LDAP directory lookup.
- Network Box has a generic LDAP retrieval facility that can be used to retrieve databases from remote LDAP servers, for local storage on the box. These databases can be used for such things as mail portal user lists, envelope verification email lists, policy mappings, etc.
- The Web Proxy has the ability to use the HTTP proxy protocol (not available in transparent mode) to request client user authentication from a variety of sources including LDAP server, Windows NTLM servers, etc. This authentication can either be via a pop-up dialog (using Basic

Authentication mode) or via three-way handshake between the client, the server and the proxy (in NTLM Authentication mode).

In all these modes, the authentication information or databases are not maintained on the network box itself, but are maintained on external servers by the customer or supplier. The network box merely acts as a client to such services. No authentication credentials need to be stored on the network box itself, and the authentication transaction is merely passed through to the remote server transparently.

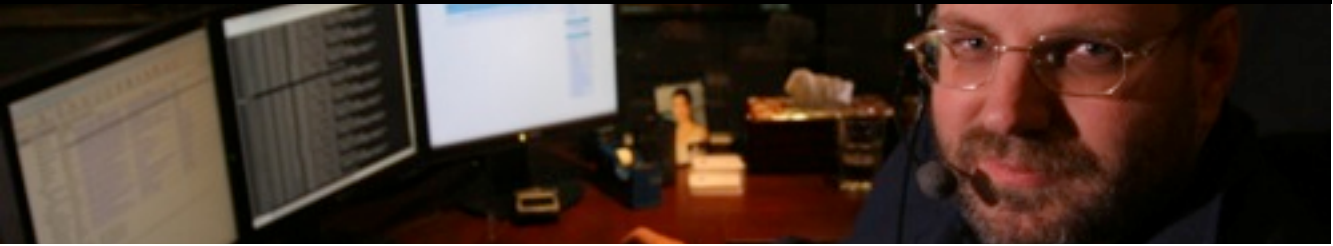
Such a facility is also available for the VPN services offered by Network Box. User authentication can be done via a selection of authentication methods (including LDAP, NTLM, Radius, etc).

While transparency offers its advantages, it also has limitations in the extent of services it can offer. For example, a transparent SMTP proxy cannot store incoming emails for you, while your email server is unreachable. For this reason, Network Box also offers a set of sophisticated non-transparent proxies able to offer more advanced services. Examples include:

- The Network Box Accelerated POP3 proxy offers the (patents pending) option to pre-connect to the remote server to download and scan emails prior to the client connecting to retrieve them. This has the dual advantage of offering the ability to quarantine spam and viruses for POP3, as well as greatly speed-up the email download time for the clients.
- The Network Box store-and-forward email proxy first receives emails from clients (while scanning them for adherence to filtering policies), then delivers them on behalf of the client. This offers the advantage of being able to receive incoming emails even if the mail server is unreachable, and deliver these when the mail server recovers.

In conclusion: we always try to configure Network Boxes with minimal impact on your network, and transparency features keep this as flexible as possible. These features also allow for the Network Box to act as a client to customer servers for such things as authentication and email address verification - reducing duplication of information and avoiding synchronisation, privacy and security issues. If you need further information on this, please contact your local support NOC for assistance.





**June 2010 Features**



On Tuesday, 1<sup>st</sup> June 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:

- Enhancements to the Box Office portal, to support the v3.2 iPhone/iPad application.
- Enhancements to the update logging system to improve granularity of logging of alerts and security enhancements.
- A fix to the my.network-box.com password change system, for changes to PPTP VPN accounts with fixed IP addresses.
- Improvements to the my.network-box.com charts for mail/overview and anti-spam/overview.
- Improvements to the my.network-box.com web proxy status overview screen.
- Enhancements to the Protected Service Proxy system, related to transparent SMTP proxy.
- Enhancements to the Protected Service Proxy system, related to transparent HTTP proxy and support for proxying of web transfers greater than 2GB in size.

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.

**June Hint: Let us know the background**

All too often we find that configuration changes are delayed due to problems gathering information from our customers. We realise that such communication issues will always occur with a managed service such as ours, but continually strive to keep these to a minimum.

We recommend that when asking for a configuration change, you don't just tell us what you need done, but also give us the background information on the request (ie; your requirements). The NOC engineers have an enormous amount of expertise in network security, and network boxes, and can often give you advise on how best to meet your needs using all the aspects of network box technology.

For example, when asking for a port to be opened to your new web server, it would be helpful if we could know what sort of server it is, and what applications will be running on it. That will allow us to best fine-tune the Intrusion Prevention System to protect the new server now reachable from the Internet.

And, when asking for a new mail server to be configured, we'll need to know how you intend both outbound and inbound mail to be routed, as well as aspects such as mail portal. Understanding exactly what the new mail server is will help us recommend the best configuration for you.

Please talk to your local support NOC to ensure that your configuration changes are as you require and take the time to explore the available options.

Mark Webb-Johnson,  
CTO, Network Box Corporation

**MAY 2010 NUMBERS**

Key Metric)	#	% difference (since last month)
PUSH Updates	1,086	-1.8
Signatures Released	250,660	+97.2
Firewall Blocks (/box)	669,637	-3.2
IDP Blocks (/box)	140,828	-20.4
Spams (/box)	45,514	+30.2
Malware (/box)	681	-95.0
URL Blocks (/box)	77,105	-10.5
URL Visits (/box)	3,439,503	+5.4

**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)