

# In The Boxing Ring



## IN THIS ISSUE

### 2. **MY.NETWORK-BOX.COM ENHANCEMENTS**

We've added several new control and diagnostic features to our administrative interface.

### 3. **RELATIONSHIP SPAM SCORE ADJUSTMENTS**

This system has now been released, and is available for use (along with a large number of more minor mail scanning functional enhancements).

### 3. **CUSTOMER PORTAL: BETA TEST OPEN**

The beta test for this project is now ready to be opened to a wider audience.

### 3. **PROXY VULNERABILITY**

A vulnerability in web proxy servers has been discovered, which may have implications for Network Box customers. We present our recommendations.

### 4. **FEB 2009 FEATURES**

The ongoing deployment of our recently released features.

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

### Welcome

Welcome to the March 2009 edition of 'In The Boxing Ring'. In this edition, I'll be devoting a whole page to talk about a set of new functions released this month for the [my.network-box.com](http://my.network-box.com) administrative system. I also have a status update on the systems we currently have undergoing beta test.

The [my.network-box.com](http://my.network-box.com) administrative interface is used to query, report on and control a Network Box appliance. Unique in the industry, it offers hybrid control of the managed service: The customer is responsible for setting the security policy and the NOC is responsible for enforcing it. It also offers the customer full visibility of the policy as it is in effect. And by popular demand, we have added several new control and diagnostic features to the interface. Turn to page 2 for details.

As targeted, the relationship spam score adjustment system was released on 23<sup>rd</sup> February 2009 - and is now available

for use. Turn to page 3 for further information.

The Network Box Office Customer Portal beta has been ongoing for some time now, and we are ready to open it up to a wider audience. Application procedures are on page 3.

Further to last month's discussion on outbound policy enforcement, a vulnerability in web proxy behavior has just been announced that re-enforces this requirement (page 3).

As usual, if you have any feedback, or comments, it is 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.

Mark Webb-Johnson  
CTO, Network Box Corporation  
March 2009



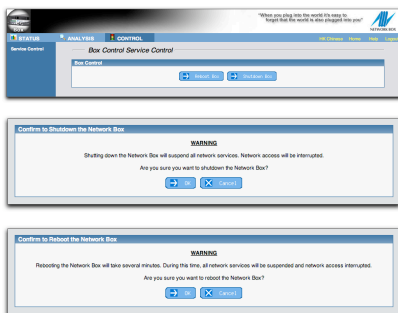


**my.network-box.com Enhancements**

As well as a large number of minor enhancements, this month we are globally releasing four new functions in the NBR3-3.0 my.network-box.com administrative interface:

1. Remote Shutdown/Reboot
2. Network Address Information
3. DHCP Leases
4. Trace Route and Ping

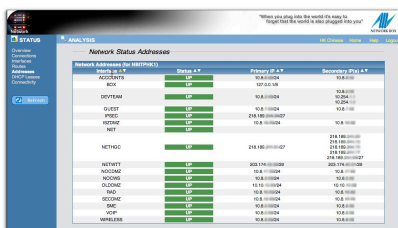
**Remote Shutdown/Reboot**



We added a screen (at Box / Control / Service Control) to permit the administrator to remotely shutdown or reboot a Network Box appliance. The functionality is equivalent to that already from the front-panel, but works over the my.network-box.com web interface.

After the administrator chooses the function (shutdown or reboot), a confirmation dialogue appears. Clicking OK performs the action. Access control to permit / deny access to this functionality is also available.

**Network Address Information**

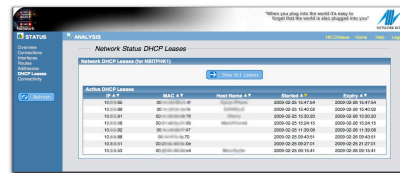


An additional screen (at Network / Status / Addresses) shows the current IP address assignments on the Network Box.

Of particular importance for boxes configured to use dynamic IP addresses, this screen shows each defined network interface, it's status, it's primary IP address, and all it's secondary IP addresses (if any).

The screen provides a simple succinct report for the administrator to report on address assignments.

**DHCP Leases**



A new screen, at Network / Status / DHCP Leases, shows active and historical IP address leases from the DHCP server on the Network Box. This function is only available if you have specified a DHCP server to be configured and enabled on your Network Box.

By default, the screen shows all active DHCP leases (including IP address, MAC address, Host Name, and lease duration information).

The button, "Show All Leases", can be used to switch to a view of all leases (including currently active, expired, and historical leases).

In the past, some clients have been reluctant to use the DHCP server available on the Network Box because of a lack of visibility of this information. Hopefully, this new functionality will encourage the use of this powerful facility.

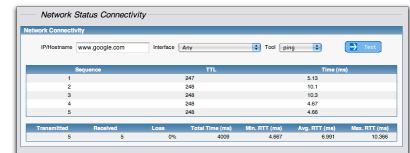
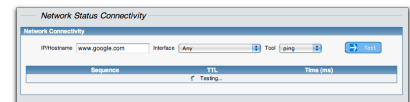
**Trace Route and Ping**



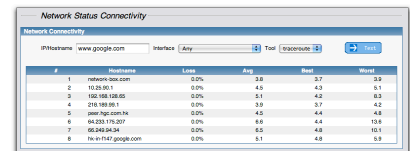
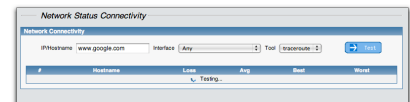
We have added a screen (at Network / Status / Connectivity) to allow the administrator to conduct trace route and ping tests. While these tests can be done from workstations / servers behind

the Network Box, at times it is useful to run them directly from the gateway.

To use the function, you enter the IP address (or DNS host name) of the address you want to test, choose the tool you want to use, and click "Test". The results are displayed in a table. You can optionally change the interface you want to test from (of particular use when testing IPSEC VPN links - which encrypt and route via source+destination address pairs).



The output results of the ping connectivity test will show you packet loss and round-trip times for each of the 5 ICMP packets used for the test. It will also display a summary table (with minimum, maximum and average).



The output results of the trace route connectivity test will show you the network hops between the Network Box and the destination. For each hop, it shows packet loss and round-trip times (best, worst and average) to allow you to see exactly where the connectivity problem is.

**Availability**

All of this new functionality will be globally released on patch Tuesday (3rd March 2009) and should be rolled out to all NBR3-3.0 clients within a week. Please contact your local support NOC for further information.



## Relationship Spam Score Adjustments

I am pleased to announce that the Network Box eMail Relationship Spam Score Adjustment system has now been globally released.

This new system uses the relationship database to automatically adjust anti-spam scores based on relationship strength.

It can be used to be (a) more aggressive towards known spam sources and (b) kinder to known good sources of non-spam mail.

The eMail Relationship Spam Score Adjustment system is exceptionally effective with messages in the 'border-line' zone (typically scoring between 5.0 and 9.0 before adjustment) and can 'tip the scale' to mark them spam / not spam. It adjusts the spam score of new messages by taking into account the previous relationship history of that sender and recipient pair. It also has a confidence mechanism to attempt to authenticate the sender - even if the SMTP protocol itself does not have sender authentication capability.

The system is extremely configurable and tunable. It can be configured to only adjust scores up or down by configuration of the adjustment range. Work is in progress to offer the same techniques for anti-virus and policy enforcement.

The code for this new feature has successfully passed all testing, and was globally released on February 23rd 2009 as a PUSHCODE update. It is a free-of-charge update to all Network Box NBR3-3.0 customers.

The relationship system must be individually configured and tuned on each Network Box. Due to the large number of customers and consultancy work for the NOCs to undertake to enable this system, we will be deploying this on a customer-by-customer basis.



## Customer Portal: Beta Test Open

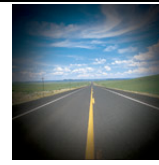
While our customers' organisational structures may be centralised, distributed or individualised (and any combination of the three), Network Box has always been concerned with the global view. We have several internal systems that operate globally, including:

- Global Monitoring System (NBGMS) - a global network of monitoring stations.
- Inventory - the system that records which customers own which boxes, resold through which partner.
- Licensing - recording the contractual, licensing and SLA arrangements.
- Deployment - tracking the deployment of Network Boxes.
- Ticketing - tracking customer and NOC initiated issues and ensuring we meet our SLA targets.
- Workload Statistics - tracks the workload that Network Box devices are handling.

The Network Box Office Customer Portal gives our customers a window into these systems and provides real-time status of Network Box devices under our management. It allows for formalised two-way communication with the Network Box Network Operation Centres (NOCs) responsible for monitoring and configuration of the equipment and network.

This system has been under beta testing and refinement for some time, and we are now ready to open it up to a wider audience, prior to global release.

Should you wish to participate in the beta, please contact your local support NOC who will assist you with gathering the necessary information and preparing you boxes for the transition. Both the Beta Box Office Customer Portal and standard Regional Mirrors operate side-by-side - so you will be able to switch between both during the testing phase.



## Proxy Vulnerability

Computer networks that use proxy servers to automatically redirect browser connections should be on the lookout for a serious architectural flaw that could allow attackers to remotely access intranets and other website resources that are normally off limits, security experts are warning.

The US Computer Emergency Response Team has issued [alert vulnerability 435052](#) to track this problem, and summarises it thus:

*Transparent proxy servers intercept and redirect network connections without user interaction or browser configuration. Some transparent intercepting proxy implementations make connection decisions based on the HTTP host-header value. Browser plugins (Flash, Java, etc.) may enforce access controls on active content by limiting communication to the site or domain that the content originated from. An attacker may be able to forge the HTTP host-header (or other HTTP headers) via active content. A proxy server running in intercepting ("transparent") mode that makes connection decisions based on HTTP header values instead of source and destination IP addresses is vulnerable due to the ability of a remote attacker to forge these values.*

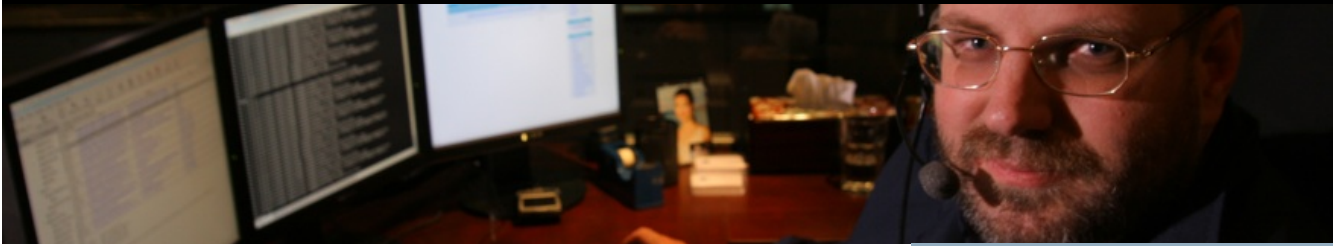
Network Box Security Response is currently recommending that customers follow best practices and ensure that:

(a) Proxy servers should only be able to connect to a limited number of well known ports.

(b) The CONNECT method should only be allowed for traffic that uses destination port 443/tcp.

This is particularly important for proxies configured to operate in transparent mode, but the best practices recommendation is applicable to all proxies.

Should you have any questions on this, please contact your local support NOC for assistance.



## March 2009 Features



On Tuesday 3<sup>rd</sup> March 2009, we will be releasing several bug fixes and enhancements to the NBR3-3.0 firmware.

These changes include:

- A large number of minor enhancements to mail scanning. These include performance enhancements to optimise the use of whitelists and blacklists in anti-spam scanning. We will also start deploying the Relationship Spam Score Adjustment system.
- A large number of minor enhancements to the [my.network-box.com](http://my.network-box.com) administrative interface, as well as the new functions of remote shutdown / reboot, network address information display, DHCP lease information display, and trace route / ping connectivity tests.
- Minor system revisions and enhancements to the on-box health monitoring and GMS systems (in particular to better report problems with whitelisting of customer's own / popular domains).

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 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.

## March Hint

How much do you know about what the users on your network are really up to? I suggest you have a look at the [my.network-box.com](http://my.network-box.com) NETWORK / ANALYSIS Summary, IP Summary, IP Traffic Directions, All Protocols and Local IP reports.

These reports are produced from a sophisticated software package called NTOP. Rather than looking at just bandwidth (which is easily done with something like MRTG), it examines all network traffic and records data on both overall usage (by protocol) and top users (by source, destination and protocol). The reports allow you to see, at a glance, who and what is using the bandwidth, and then to drill-down into the detail. There is even a dynamically-generated network map (at NETWORK / ANALYSIS / Local IP / Network Traffic Map) that maps out the connections of all the users, servers, devices and applications on your network.

The system is available, as standard, on all Network Box NBR3-3.0 boxes, but may not be enabled on your box (especially for boxes under extremely high workloads).

## 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  
 March 2009

## FEB 2009 NUMBERS

Key Metric	#
PUSH Updates	1,522
Signatures Released	270,180
Firewall Blocks (/box)	573,611
IDP Blocks (/box)	117,217
Spams (/box)	70,878
Malware (/box)	807
URL Blocks (/box)	60,489
URL Visits (/box)	2,389,984

## NEWSLETTER STAFF

**Mark Webb-Johnson**  
 Editor

**Pauline Chiu**  
**Michael Gazeley**  
**Jasmine Arif**  
**Jason Law**  
 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)

Copyright © 2009  
 Network Box Corporation Ltd.