Welcome to the June 2013 edition of In the Boxing Ring

Starting this month, we are bringing NBRS-5.0 into our patch Tuesday release cycle along side NBRS-3.0. For NBRS-5.0 this month, there are more than 50 enhancements/fixes including these new security modules: network-highavailability, network-dhcp-server and portal-web-client-base, which are summarized on page 2.

As we countdown to the launch of the NBRS-5.0 UTM+ platform, we will be providing monthly progress reports as illustrated on the NBRS-5.0 Roadmap featured on page 3.

On Page 4, Network Box’s Head of R&D, Nick Jones, continues his series on Secure Socket Layer (SSL) Security Strategy. This month, we take a look at Web Client SSL Protection and how NBRS-5.0 can help Network Administrators enforce security policies on SSL transactions.

Finally, we are proud to announce that Network Box won the Network Products Guide Gold Award 2013, published out of Silicon Valley. Other notable Network Products Guide Gold Award 2013 winners from various other categories included: Red Hat, NET-GEAR, HP, Cisco Systems, Varonis, and Qosmos.

Mark Webb-Johnson
CTO, Network Box Corporation
June 2013

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 with us by several social networks:

- [twitter](http://twitter.com/networkbox)
- [facebook](http://www.facebook.com/networkbox)
- [http://www.facebook.com/networkboxresponse](http://www.facebook.com/networkboxresponse)
- [Linked In](http://www.linkedin.com/company/network-box-corporation-limited)
- [Google+](https://plus.google.com/u/0/107446804085109324633/posts)

IN THIS ISSUE

2-3
NBRS-5.0 Features and Roadmap

The features and fixes to be released in this month’s patch Tuesday for NBRS-5.0.

NBRS-5.0 roadmap, which gives a clear overview of what we have recently released, as well as the final milestones.

4
SSL Security Strategy (part iv)

Network Box’s Head of Research & Development, Nick Jones, talks about Web Client SSL Protection, which is for the protection of Web Clients, namely web browsers.

5
Awards & Events

Network Box won the Network Products Guide Gold Award 2013

5
NBRS-3.0 Features

The features and fixes to be released in this month’s patch Tuesday for NBRS-3.0. We continue to develop, and will continue to support, NBRS-3.0 for the foreseeable future (several years).
Network Box Version Five
NBRS-5.0

On Tuesday, 4th June 2013, 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.

The following three new security modules have also been released this month:

1. network-highavailability
The Network Box High Availability Security module provides a VRRP based network-level high availability foundation. A VRRP service co-ordinates between MASTER and BACKUP high availability nodes and switches roles (using a priority-based election mechanism) should a master node fail. The module provides a facility for a group of network boxes to be treated as a high availability set - with one member having the role of MASTER and being responsible for the network traffic. Should the master fail, an automated electronic election will take place, and one of the backup nodes will be promoted to be the new master.

2. network-dhcp-server
The Network DHCP Server security module provides a DHCP server. The service is integrated to the entity database, and will update and maintain entity attributes based on DHCP activity.

3. portal-web-client-base
The Network Box Proxy Web Client security module provides a proxy for protection and control of web clients using the HTTP protocol. The module implements support for both directed (listening on a particular port, the client browser is specifically directed to connect to the proxy port for web traffic) and transparent (traffic is transparently intercepted) modes. Note that this is a foundational component, to be extended in the upcoming July Patch Tuesday to include anti-virus and content-filtering support (finalizing the NBRS-5.0 SURF SCAN product release).

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.

Note also that this month we are bringing NBRS-5.0 into our Patch Tuesday release cycle. Starting this month (June), we will be reporting NBRS-5.0 features and enhancements alongside those for NBRS-3.0.

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

NBRS-5.0 Features
This month, for NBRS-5.0, there are more than 50 enhancements / fixes, including:

- base: Support for tab-expansion in raid disk creation
- base: Improvements to security module dependency system, to speed-up system boot time
- base: Introduce warning messages for package updates that require a reboot
- base: Improve reconnection of console client after service restart
- base: Support automatic loading of optional kernel modules
- base: Add support for bonded network interfaces
- network-firewall: Improvements to policy routing rule support for IPv6
- network-firewall: Add ICMPv6 policy control for IPv6
- reporting-base: Fixes to csv export
- portal-base: Fixes for HTTPS support over slow Internet links
- portal-base: Add support for gzip compression
- proxy-web-server-waf: Add support for geolocation of caller source IP in signature rules

In the Boxing Ring - June 2013
Network Box Version Five
NBRS-5.0

NBRS-5.0 Roadmap

We are now well into the ramp-up phase of our road-map for NBRS-5.0. The majority of development work has been completed, and we are now conducting final development, packaging and beta tests for the remaining security modules.

We intend to release our SURF SCAN product with the July 2013 patch tuesday, and this will include anti-malware and content-filtering support for web clients - rounding-out our web content protection offering (both client and server). Then, in August 2013 we will release our mail scanning product, and that will be followed by the remaining miscellaneous modules to bring NBRS-5.0 up to, and beyond, full UTM+ equivalence to NBRS-3.0. Once we have reached those milestones, we can start the process of offering NBRS-5.0 upgrades to our existing NBRS-3.0 clients.

The NBRS major releases for Network Box (NBRS-1.0, NBRS-3.0, NBRS-5.0, etc) include long-term support, of 5+ years, so this is just the start of a long journey with NBRS-5.0. We have some truly exciting new product offerings, taking advantage of the new foundational support architecture of NBRS-5.0 that will help us to help you to keep your online networks secure.

1. BASE PLATFORM
Back in the summer of 2012, we completed and released the base platform and support infrastructure for NBRS-5.0. This made up the bulk of the product’s code base, and forms the foundation for all our NBRS-5.0 product offerings.

2. WAF+
We followed that up with the Anti-DDoS WAF+ service package. This package provide new functionality (not previously available with NBRS-3.0) to protect DMZ/cloud based web servers from Internet-based attackers. It provides network firewall, web application firewall, DDoS protection, and protocol translation (IPv6-IPv4 bridging) functionality, into a single service offering.

3. SURF SCAN
To produce a web application firewall, we had to design and build a proxy capable of understanding the web’s HTTP protocol. We’re now turning that around, and combining it with our advanced scanning technology, to make up our next NBRS-5.0 offering: SURF SCAN. This will provide for protection of web based clients on the LAN, browsing web servers on the Internet. It will support anti-virus scanning, as well as web site and content classification - for comprehensive policy control. It will also support extensive reporting capabilities.

4. APP SCAN
Following on from that, we will be releasing APP SCAN - the application identification system that we have been working on for some time. This, operating standalone, or combined with SURF SCAN, is capable of identifying applications at the network level, and extracting meta data and content from the data streams. Both anti-virus scanning and policy control technology can then be applied.

5. MAIL SCAN
At that point, we will have comprehensive web server, and LAN client support, so we will be releasing our mail server protection MAIL SCAN. This will provide support for scanning mail traffic using the SMTP, POP3 and IMAP4 protocols.

6. UTM+
Finally, we will round-out the UTM+ equivalence, with the release of a set of security modules implementing such functionality as QoS (Quality of Service), VPNs, Clustering, High Availability, etc. Some of these will actually be released alongside the earlier service offerings, as and when they are ready.
Web Client SSL Protection

A typical tactic for internet fraudsters is to use an authentic looking email to lead victims to a fake version of a reputable website that the victim is familiar with. The fake website is visually identical to the original, often using the original design and layout assets from the real website, so the user is fooled into submitting personal information into the fake website, namely their username and password, as there may be no visual cues in the website content that give away its inauthenticity.

There will however be one important clue, which is the fact that the SSL Certificate of this reputable website is invalid. SSL Certificate validity is an issue that reputable websites take very seriously, so the fact that such a website has an invalid certificate should raise alarm bells to the potential fraud victim, or any internet user.

Unfortunately, the urge to settle the sense of alarm instilled in the victim by the fraudulent email is strong enough to cause them to ignore the SSL Certificate Validity Warnings raised by their web browser. The victim will bypass the security warning, and carry on right into the trap of the fraudster.

With NBRS-5.0 Client SSL Protection, another component of SSL Security Strategy, the browser transaction at the SSL protocol layer is analyzed in addition to the standard HTTP protocol layer. This information is made available for the Network Administrator to create Security Policy rules. For example, the Network Administrator may demand that the NBRS-5.0 device prevent a network user from bypassing a SSL Certificate warning.

Because the NBRS-5.0 device is able to interpret the SSL transaction and is aware of such a violation, it will block a user attempting to bypass the certificate warning. Alternatively, the Network Administrator may allow users to carry out this action, but occurrences will be logged as non-disruptive alerts that may be analyzed at a later time.

One significant outcome of the SSL Certificate bypass protections provided by NBRS-5.0 is that bypass decisions are moved to the Network Gateway, where the Network Administrator is able to apply security policies that are enforceable network wide, and traceable through event logging.

Monthly SSL Housekeeping

In May 2013 the Network Box platform development team released a software update for a foundational component in the NBRS-5.0 SSL Software Ecosystem. The purpose of the upgrade was to address a number of security vulnerabilities in cryptographic algorithms that had been discovered in recent months.

Because one of the goals of the Network Box SSL Strategy is to move SSL execution to the network gateway, with the Network Box SSL Protocol Upgrade feature being a classic example, an update to the NBRS-5.0 SSL software ecosystem is an update to the SSL ecosystem for the whole network.

In June 2013, the Network Box platform development team will again be busy updating the Root Certificate Authority Database in NBRS-5.0. This database contains the lists and Public Certificates of the highest level SSL authorities and it is by these authorities that the SSL Certificate of public websites must be signed, for the reason that the same authorities are also trusted by applications that use SSL, such as web browsers.

A future issue of In the Boxing Ring will go into more detail about SSL Certificate Authorities and how they are a part of the NBRS-5.0 SSL Security Strategy.
Network Box won the Network Products Guide Gold Award 2013, in the Unified & Integrated Security category, for Network Box UTM+ (NBRS-5.0). Cyberoam Technologies Pvt Ltd., took home the Silver Award 2013, for their 2500iNG, in the same category.

Other notable Network Products Guide Gold Award 2013 winners from various other categories included: Red Hat, NET-GEAR, HP, Cisco Systems, Varonis, and Qosmos.

Network Box was recognized in three categories: Security Services (New or Upgrade Version) and Security Software (New or Upgrade Version) Categories for Anti-DDoS WAF+; and Unified & Integrated Security Category for UTM+ (NBRS5.0).

Note also that this month is the first month we are bringing NBRS-5.0 into our Patch Tuesday release cycle. Starting this month (June), we will be reporting NBRS-5.0 features and enhancements alongside those for NBRS-3.0.

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