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

Welcome to the August 2013 edition of In the Boxing Ring

This month, we release our NBRS-5.0 application identification framework to public beta test. The system identifies web applications and by extracting meta data from the data stream, it allows comprehensive reporting and policy control to be enabled.

On page 3, following on from last month's In the Boxing Ring Newsletter, we discuss how NBRS-5.0 addresses the issue of real-time detection and blocking of outbound trojan activities.

On pages 4 and 5 we feature the fixes to be released in this month’s NBRS-5.0 patch Tuesday; and cover the key milestones of the NBRS-5.0 platform.

Finally, Network Box participated in variety of seminars in July. Network Box was at the Hotel Technology Next Generation (HTNG) Asia-Pacific Conference and a recent ebay PayPal partnership event.

Mark Webb-Johnson
CTO, Network Box Corporation Ltd.
August 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
- LinkedIn: http://www.linkedin.com/company/network-box-corporation-limited
- Google+: https://plus.google.com/u/0/107446804085109324633/posts

IN THIS ISSUE

2
NBRS-5.0
Application Identification Framework
There will two versions of this system: ‘lite’ and ‘full’. The key features of the system are highlighted here.

3
Real-Time Detection and Blocking of Outbound Trojan Activity
We discuss the key technologies that NBRS-5.0 uses to address this issue.

4-5
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.

6
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).
This month, we release our NBRS-5.0 application identification framework to public beta test.

This framework includes a proxy type called 'applicationid' capable of automatically analysing network traffic and determining the application responsible for such traffic. The system will then label the connection appropriately (for reporting and policy control). In this way, you can detect traffic such as Skype, QQ, FTP, HTTP, Facebook, and more than 1,000 other recognised applications - all based on the traffic itself and not just the network port / address it is on.

For protocols supported natively by the proxy (for example, HTTP supported by the web client proxy module), once the application has been identified, the session can be seamlessly upgraded from the applicationid proxy module to the protocol-specific proxy module. So, for example, HTTP traffic on an open port tcp/80 can be detected and moved into the webclient module for higher-level protocol control (such as authentication, policy control and anti-virus scanning).

This is a very exciting offering for us, as it provides a foundation for a lot of capabilities. Once the application has been identified, meta data can be extracted from the data stream and options for comprehensive reporting and policy control enabled.

We will be offering licenses for two versions of this system:

**Lite**
A 'free of charge' light version, capable of identifying 10 common applications, and included with every service package with proxy services. The applications detected are our core protocols, SSL, plus several voice/video services. In addition, custom policy rules can be used to manually identify other applications using such criteria as addresses, ports, urls, etc. The 10 applications identified are:

HTTP, SMTP, POP3, IMAP, FTP (incl. FTPCRD and FTPDATA), SSL, SIP, H.323, Facetime, GTALK (incl. GTALKAUD and GTALKVID)

**Full**
The full version of the system, capable of identifying more than

1,000 applications.

---

For protocols supported natively by the proxy (for example, HTTP supported by the web client proxy module), once the application has been identified, the session can be seamlessly upgraded from the applicationid proxy module to the protocol-specific proxy module. So, for example, HTTP traffic on an open port tcp/81 can be detected and moved into the webclient module for higher-level protocol control (such as authentication, policy control and anti-virus scanning).

This is a very exciting offering for us, as it provides a foundation for a lot of capabilities. Once the application has been identified, meta data can be extracted from the data stream and options for comprehensive reporting and policy control enabled.
Real-Time Detection and Blocking of Outbound Trojan Activity for NBRS-5.0

NBRS-5.0 has a specific framework for detecting, and policy control of, botnet infections in internal network segments as well as connected VPN networks. This is delivered as an optional security module called "Infected LAN". The framework uses three main technologies to detect anomalous internal client behavior:

1. Connections to know compromised command and control centres.
2. Signature-based and heuristic detection of network traffic from botnet clients to command and control centres.
3. Rate based and anomalous response exceptions.

If such traffic is detected from a client on the internal network, the client can be automatically isolated and administrators notified of the event.

This month we have released the base network framework for this system, and next month we will follow-up with the proxy level framework.
Network Box Version Five
NBRS-5.0

On Tuesday, 6th August 2013, Network Box will release our patch Tuesday set of enhancements and fixes. These enhancements have been primarily made to support the new web client security modules.

NBRS-5.0 Features
August 2013

The regional NOCs will be conducting the rollouts of the new functionality in a phased manner over the next 7 days. This month, for NBRS-5.0, these include:

- Release of 4 new security modules to final beta testing:
  - network-infectedlan (Botnet protection base framework at network level)
  - proxy-appid-base (Application Identification framework)
  - proxy-appid-navlite ('lite' application identification for 10+ common applications)
  - proxy-appid-navl ('full' application identification for 1000+ applications)
- Full customer release of 2 new security modules:
  - scan-auth (Base authentication framework)
  - proxy-auth (Proxy authentication for web clients)
- Improve reporting on raid resync status.
- New DHCP server commands, for Network Boxes acting as DHCP servers.
- Improvements to administrative web portal.
- Various (mostly internal) enhancements to Box Office and support systems

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.

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

**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.

With last month's patch Tuesday we released our SURF SCAN product, and included anti-malware and content-filtering support for web clients - rounding-out our web content protection offering (both client and server). In this month's patch Tuesday, we will release our NBRS-5.0 application identification framework to public beta test. At the end of August, 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. Now that we have reached these 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 (IPv4-IPv6 / 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.
Key Metric | # | % difference (since last month)
--- | --- | ---
PUSH Updates | 522 | -18.7
Signatures Released | 465,232 | -18.2
Firewall Blocks (/box) | 900,291 | -2.9
IDP Blocks (/box) | 97,518 | -9.1
Spams (/box) | 18,105 | +0.5
Malware (/box) | 765 | +26.9
URL Blocks (/box) | 167,010 | -10.4
URL Visits (/box) | 3,268,582 | -0.9

Network Box
Hotel Technology Next Generation

On Tuesday, 6th August 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. This month, for NBRs-3.0, these include:

- Revisions to Kaspersky Anti-Virus to optimize resource usage.
- Various (mostly internal) enhancements to Box Office and support systems

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.

Network Box was invited as a guest speaker at the Hotel Technology Next Generation (HTNG) Asia-Pacific Conference, held in Hong Kong this year. Network Box CTO, Mark Webb-Johnson gave a seminar titled ‘Protecting your Hotel from Global Cyber Threats.’

In the Boxing Ring - August 2013