Welcome to the September 2013 edition of In the Boxing Ring

This month, we release the first NBRS-5.0 mail scanning modules. These provide anti-malware and anti-spam scanning for both incoming and outgoing SMTP email envelopes and messages. This is expanded further on pages 2 and 3 and we also compare the different scanning methodology between NBRS-3.0 and NBRS-5.0.

In addition to SMTP mail scanning, this month, we are releasing support for file scanning in Network Box NBRS-5.0 WAF+. This is highlighted in page 3.

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, in August, Network Box participated in a variety of conferences and hosted a series of seminars title ‘Cyber Security and Your Business’. This is covered in page 6.

Mark Webb-Johnson
CTO, Network Box Corporation Ltd.
September 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)
This month, we’re pleased to announce the first releases of security modules for mail scanning in NBRS-5.0. These first modules provide for anti-malware and anti-spam scanning of SMTP eMail envelopes and messages, both inbound and outbound.

Transparency

As the NBRS-5.0 proxies are transparent (typically proxying traffic without changing the source IP address), configuration and deployment is typically very simple. Two proxy modules are provided:

- `smtpclient` - for protection of trusted SMTP clients, typically connecting outbound
- `smtpserver` - for protection of trusted SMTP servers from untrusted clients, typically connecting inbound

The primary difference between the two modules is that the `smtpserver` module performs third-party relay protection, while the `smtpclient` module does not. However, the different modules are also accounted for differently in reporting.

The `smtpserver` module can be configured to automatically promote a connecting client to be a trusted `smtpclient`, in each of two cases:

1. The connection arrives from a source IP address configured as trusted.
2. The SMTP client successfully authenticates to the trusted SMTP server.

Scanning

With mail scanning in NBRS-3.0, once the entire message envelope (sender and list of recipients) had been collected, it was scanned and a single result returned for all of that sender and recipients. Similarly for the message body, a single result was returned for all recipients. If the mail was SPAM for one, it was SPAM for all.

NBRS-5.0 does this very differently. With NBRS-5.0, each stage of the message transmission is scanned individually, and individual results returned:

- When the HELO/EHLO message is received, that (along with the source IP address and other attributes) is scanned.
- When the MAIL FROM sender is received, that (along with the results and attributes from the previous HELO/EHLO scan) is scanned.
- When each RCPT TO recipient is received, that (along with the results and attributes from all previous stages of the scan) is scanned.
- When the message itself is received at the DATA stage of the scan, that (along with the results and attributes from all previous stages of the scan) is scanned.

At each stage, policy rules are run and the individual recipient, or entire message, can be blocked.

This approach gives NBRS-5.0 a very fine-grained capability to control the reception of eMail messages, minimizing bandwidth usage and maximizing the performance of the appliance. In particular, a lot of emphasis has been placed in increasing the number and capability of scanning engines at the early envelope stage (before message body reception), as well as avoiding duplication of scanning effort at both envelope and message scan stages.
Classification

It is important to point out that NBRS-5.0, at its core, is merely a classification engine. During the scanning process, it identifies aspects of the object being scanned (envelope, or message, in this case) and returns a list of classifications, confidence in those classifications, and threats identified. It is then up to the policy to be configured to determine the disposition, once the scan results have been determined.

For example, unlike in NBRS-3.0, the mail scanner in NBRS-5.0 does not quarantine mail. Instead, it merely indicates back to the proxy that a threat (malware, for example) has been discovered, and classifies the object. The policy engine in the proxy can then be used to permit or deny the message, and to quarantine as necessary. For example, a common configuration would be:

```
config network proxy rule smtpclient deny
if isthreat = TRUE with quarantine
```

That would deny (block and log) as well as quarantine any objects found to be a threat during smtp client scanning.

Example classifications include:

- **malware** - the object is determined to be malicious
- **spam** - the object is determined to be spam
- **bulk** - the object is determined to be bulk email
- **testfile** - the object is determined to be a standardized test file

Importantly, as well as providing the classification, the scanning engine provides the confidence in its classification, expressed as a percentage. 100% would indicate the normal recommended threshold to block a threat, but configuration control can be applied to be more (>100%) or less (<100%) conservative. This approach works particularly well with the multi-engine scanning approach taken by Network Box. By allowing the confidence levels from each individual engine to affect the overall score, the engines work together to provide a clear indication of the likelihood of a particular classification.

Conclusion

The NBRS-5.0 mail scanning system enters beta testing with the September 2013 NBRS-5.0 Patch Tuesday.

File scanning in Web Application Firewall

This month, we’re pleased to announce upcoming support for file scanning in Network Box NBRS-5.0 WAF+. This optional facility allows files being uploaded to your websites to be scanned for potentially malicious content by the NBRS-5.0 anti-malware systems. In addition, as a unique feature, you can also optionally enable scanning of outbound traffic (perhaps not for the entire website, but only for certain paths). Support for this functionality is currently under trial on several sites, and will be formally released in the October patch Tuesday.
Network Box Version Five
NBRS-5.0

On Tuesday, 3rd September 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
September 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 7 new security modules to final beta testing:
  - scan-provider-policy-nb (Network Box policy engine for mail and file scanning)
  - scan-provider-antispam-nb (Network Box anti-spam engine for mail and envelope scanning)
  - scan-mail (Network Box mail envelope and message scanning framework)
  - proxy-mail-base (Proxy support for eMail)
  - proxy-mail-smtp-client (Proxy support for protection of SMTP eMail clients)
  - proxy-mail-smtp-server (Proxy support for protection of SMTP eMail servers)
- Full customer release of 1 new security module:
  - scan-provider-antimalware-clam (ClamAV anti-virus engine for mail and file scanning)
- Unified logging system for mail, file, url and authentication scanning
- Mail scanning support for Kaspersky anti-virus engine
- Template-based alert pages, to allow for customization of alert messages
- Provide a configurable facility to bypass selected workloads from file scanning
- Provide a configurable facility to bypass selected requests from url scanning
- Extensions to the my.network-box.com and engineering consoles for reporting on web client usage
- Unified 'isthreat' ACL test, as a generic indication of a detected threat that should be blocked
- Enhancements to my.network-box.com administrative interface, to provide a facility for grouped table
- Support for BACK browser button in my.network-box.com administrative interface
- Unified container format for quarantine, reports, and other such objects
- 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

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 July’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 last month’s patch Tuesday, we released our NBRS-5.0 application identification framework to public beta test. This month, 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.
NBRS-3.0 Features
September 2013

On Tuesday, 3rd September 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:

- Extensions to health checks to permit fine-grained control over reporting of network errors
- Revisions to GMS test points in Europe
- 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.

Flock - Fedora Contribution Conference 2013

9th to 12th August 2013

Network Box’s development team attended the Fedora Contribution Conference 2013, Flock; in Charleston, South Carolina. The conference brings together Fedora users and developers to share and discuss new ideas, and work to make them a reality.

Network Box USA
CompTIA ChannelCon 2013

28th July to 1st August 2013

Network Box USA was at the CompTIA ChannelCon 2013, held at the Peabody Orlando Hotel in Orlando, Florida. It is the premier training and partnering event for the IT channel and features high-level executive panel discussions, as well as intensive executive certificate training courses on: cloud computing, disaster recovery, IT security, mobility, social media and more.

Flock Cyber Security and Your Business Seminars

In August, Network Box gave a series of cyber security seminars titled ‘Cyber Security and Your Business’. Those that attended were given a brief overview of the latest cyber issues affecting businesses and were introduced to Network Box’s comprehensive UTM+ solution.