

In The Boxing Ring

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

Welcome

Welcome to the January 2012 edition of 'In the Boxing Ring'. In this edition, I'll focus on a summary of 2011, and information on what to expect in 2012 and beyond.

On page 2, we discuss the threat numbers for 2011. Network Box Security Response monitors and manages thousands of devices around the world, and this gives us an excellent view on the threat landscape. Here at Network Box, we strongly believe that only by being able to clearly see and measure a problem is the solution achievable (and gains measurable).

In 2012 our focus is on NBR5-5.0, and the first customers will take delivery of it this year. After the upcoming base platform release, we'll be following up with a series of individual security modules, until we reach (and surpass) full UTM+ functionality. 2012 will be the year of NBR5-5.0.

The development of NBR5-5.0 has been an enormous undertaking for Network Box. Re-thinking solutions to the network security and control problems that plague you, our customers, day-by-day, is not an easy task - particularly in such a rapidly changing threat landscape. We are confident that you'll love NBR5-5.0, and we'll continue to release more information on this product, and on its component security modules, as we can.

Page 5 details the features and fixes to be released in this month's patch Tuesday for NBR5-3.0. We continue to develop, and will continue to support, NBR5-3.0 for the foreseeable future (several years), and this page will be used to keep you informed as to what is happening with our core product.

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 by several social networks:

Twitter: <http://twitter.com/networkbox>

Facebook: <http://www.facebook.com/networkbox>

<http://www.facebook.com/networkboxresponse>

LinkedIn: <http://www.linkedin.com/company/network-box-corporation-limited>

Mark Webb-Johnson
CTO, Network Box Corporation
January 2012

IN THIS ISSUE

2. 2011 THREAT ROUND-UP

We discuss the threat numbers for 2011 and performance metrics of the threat landscape.

3. 2011 ENHANCEMENTS

A look at the software enhancements and features delivered in 2011.

3-4. 2012 AND BEYOND

A look at the future of Network Box, 2012 and beyond.

5. NETWORK BOX WINS TWO CORPORATE CHOICE 2011 AWARDS

Network Box wins two Corporate Choice 2011 Awards from IT Pro Magazine. One award was for Network Box's Z-Scan zero day anti-virus system; while the other was for its S-Scan web content filtering system.

5. JANUARY 2012 FEATURES

The features and fixes to be released in this month's patch Tuesday for NBR5-3.0. We continue to develop, and will continue to support, NBR5-3.0 for the foreseeable future (several years), and this page will be used to keep you informed as to what is happening with our core product.



2011 Threat Round-Up

In 2011, Network Box Security Response PUSHed out 7,125 updates, totaling 3,880,267 signatures (down 39.2%, and up 25.9% respectively, compared with 2010).

That is approximately one new signature every 8.1 seconds. 2011 continued to see the number of signatures per-update fall, while the number of signatures released increase; reflecting the continued move to cloud-based signature systems (such as the Network Box Sentinel Z-Scan, and NBCP content categorisation systems). We expect this trend

to continue, as traditional signatures continue to be the most effective against the depth and breadth of malware, whilst cloud-based signatures are emerging as the most effective solution for zero-day outbreaks.

In 2011, the average Network Box blocked 208,081 spams and 8,008 malwares (down 55.8% and up 68.1% respectively, compared with 2010).

The reduction in overall spam volume continues, with large-scale take-down operations against botnets and their owners - the single biggest source of spam. However, the reduction in spam volume is somewhat masked by the increased use of pre-scan filtering (such as RBL blocks at the envelope stage and recipient address verification). Such envelope-stage blocks are effective against a huge amount of spam (currently estimated at around 35%, globally) and messages (both spam and malware) blocked at the envelope stage do not appear in our reported figures for 'messages blocked as spam and malware'. In 2012, with the release of NBRS-5.0, we hope to be able to better report on this. During 2010, the average Network Box blocked a spam or malware once every 146 seconds.



In 2011, the average Network Box blocked 9,191,536 attacks using firewall technology, and 1,420,534 attacks using IDP technology (up 13.1% and down 18.3% respectively, compared with 2010).

We continue to see such network-level attacks as mere 'background radiation' - an unavoidable consequence of being connected to the global Internet. The movement from a threat landscape primarily composed of mass-mailed spam and malware to one of targeted/mass vulnerability exploit continued during 2011. One worrying trend was the increase in relatively low-impact denial of service, and distributed denial of service, attacks - historically we have seen these use hundreds of megabits of bandwidth, but 2011 saw a large number of such attacks in the tens of megabit category. While the larger sites have deployed effective DDOS mitigation systems, the smaller sites are now faced with extortion and other such DDOS threats.

The IPv4 address space is now so polluted that during 2010, the average Network Box customer blocked a firewall/idp network-level probe once every 3 seconds. 2011 continued to see the deployment of the Network Box NBIDPS system, and benefits of our membership of Microsoft's MAPP program, which goes a long way to improving our protection offering for network-level IPv4. But, comprehensive firewall policies (in particular outbound firewall policy control) continue to be the most effective mechanism for controlling network-level threats.

In 2011, the average Network Box blocked 1,663,284 websites due to company content filtering policy enforcement, with 45,838,221 website URLs visited over the year (up 45.5% and 12.8% respectively, compared with 2010).

The growth in bandwidth, usage and in particular web usage continues. Fueled by cloud-based Apps, social media, and mobile, the pressure on IT departments with respect to bandwidth and web usage, continues to grow. We are pleased to see that the rate of policy enforcement blocks continues to outpace that of URL visits - implying that IT departments continue to take steps to impose policy on this major component of bandwidth consumption.

So, what is planned for 2012 and beyond?

We continue to see the threat landscape move with the users. As more and more systems move "into the cloud", web-based attacks (such as XSS, SQL injection, DDOS, etc) continue to gain in importance, and Network Box product announcements (the first of which will be in 2012Q1) will continue to address this evolving threat landscape.

As always, every month we see more and more threats, with faster and faster distribution times. Network Box will continue to invest in technologies (such as Z-Scan) to speed-up the protection release cycle, and will continue to leverage our excellent customer relationships so that we can all work together to co-ordinate an effective defense.

As with 2010, the threat landscape continues to grow, and our product continues to evolve to meet these new challenges; further validating our approach of providing a continually enhanced, globally managed, service (rather than a static product). In 2012, and beyond, we will undoubtedly see more of the same. The landscape will change, and Network Box (both the product and the service) will evolve to continue to provide the most effective protection to our customers.

Network Box Treat Statistics	2010	2011	% Change
PUSH Updates	11,719	7,125	-39.2%
Signatures Released	3,083,018	3,880,267	+25.9%
Firewall Blocks (/box)	8,129,674	9,191,536	+13.1%
IDP Blocks (/box)	1,738,576	1,420,534	-18.3%
Spams (/box)	471,304	208,081	-55.8%
Malware (/box)	25,089	8,008	-68.1%
URL Blocks (/box)	1,143,378	1,663,284	+45.5%
URL Visits (/box)	40,653,345	45,838,221	-12.8%

2011 Enhancements

We started 2011 with the release of the Kaspersky v8 engine. This is the same engine as used in Kaspersky's desktop and server products, but is optimised for use at the gateway. As well as welcome performance and memory improvements, the engine brought improved heuristic detection capabilities and application sand-boxing technologies. We then followed this with further releases of our award-winning Z-Scan zero-day protection for both Anti-Virus and Anti-Spam systems.

Throughout the year, more than 120 enhancements were released for NBR5-3.0, the highlights of which include:

- Enhancements to the Box Office contracts system, for better customer-visibility of contracts and their status
- Performance improvements in the policy URL categorisation engines
- Improved health monitoring
- Enhancements to the Global Monitoring System (GMS)
- DKIM support
- The new Security Response web site
- Extensions to message unpacking during scanning of mail
- Support for NTLM over PPTP
- Support for NBR5-5.0 in Box Office and internal systems
- ... and close to 4 million new protection signatures.

During 2011, we released a series of nine presentations on the next iteration of the Network Box firmware NBR5-5.0. This will continue during 2012, as the NBR5-5.0 product reaches customer hands.

2012 and Beyond



Our focus in 2012 is on NBR5-5.0, and the first customers will take delivery of it this year. After the upcoming base platform release, we'll be following up with a series of individual security modules, until we reach (and surpass) full UTM+ functionality. 2012 will be the year of NBR5-5.0.

As you should be aware by now, NBR5-5.0 is both a platform and a product. Made up of a large number of security modules, building upon the base platform, NBR5-5.0 provides comprehensive protection, without sacrificing the functionality of the individual security modules.

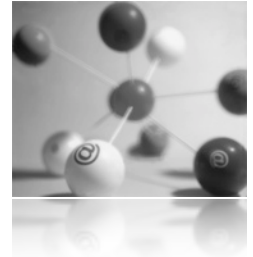
We've already started the deployment of the provisioning, monitoring, signature distribution and NOC operations infrastructure for NBR5-5.0. Before the end of Q1, we'll start deploying the first customer installations - based on the base platform plus the first set of 14 security modules. These first deployments will be for a series of products providing (a) base functionality, (b) NOC configuration and maintenance, (c) a network-level firewall, (d) a web-application firewall, (e) denial-of-service and distributed-denial-of-service protection, (f) load balancing, (g) command line administrative interface, (h) graphical web-based administrative interface, and (i) an IPv4-IPv6-SSL translation capability. The base NBR5-5.0 product will, at a minimum, be IPv6 Ready phase 2 certified at the core protocols level. Following on from this Q1 release, you will see the client-side web proxy release, and the rest of the year will see modules for mail scanning, vpns, and the other functionality.

NBR5-5.0 will be supported on all current hardware (the S- M- and E- class boxes that have been released for five years now), and should not require any hardware upgrades. However, as always, we must point out that extra functionality (if enabled and used) may require extra hardware capacity.

I'd like to take this opportunity to re-enforce the four main design goals of NBR5-5.0: transparency, holistic, scalable and modular.

NBRS-5.0 is Transparent

NBRS-5.0 applies transparency as a philosophical goal. The product is designed to have little impact on existing networks and to require as few changes as possible. Like a water filter, it is able to be installed in-line with the water (network traffic) and to filter out the dirt (viruses, spam, etc) without affecting other flows.



The connection between the box and NOCs is also simplified. NBRS-5.0 boxes connect back to their management NOCs (or other Network Boxes in a cluster) using single SSL-encrypted connections. The NOCs (and management boxes) then communicate with the box using these individual management links.

NBRS-5.0 is Holistic

Most UTM systems today are designed using a reductionist approach. They reduce the complex problem of network security to fundamental parts (such as anti-virus, anti-spam, firewall, etc) and deliver these as individual solutions. Although named 'Unified', in practice this approach does not lead to unification - other than that they are all running and maintained on the same appliance. To put it simply, the administrative interfaces are still broken apart by module.

NBRS-5.0 is designed, from the ground up, to provide a Holistic Security Management platform, and to extend that platform with security modules that both fit and work together in a holistic manner. We take several key technologies (including an entity model, unified logging and configuration) to provide a single Holistic User Interface.

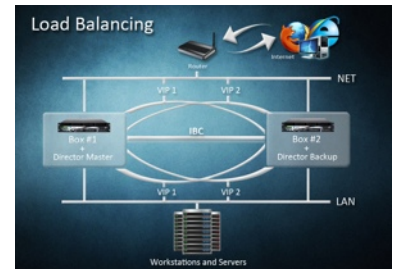


NBRS-5.0 is Scalable

The previous example of the water filter introduced the goal of transparency not interfering with the flow of network traffic. Capacity planning is a continuing problem for computer systems, as traffic and usage patterns continue to increase. Scalability is the key to meeting this goal.

NBRS-5.0 addresses scalability in two ways: in-the-box by supporting multi-core and multi-cpu appliances, and out-of-the-box with fundamental support for clustering of boxes into a single seamless solution.

With both high-availability and load-balanced approaches, the cluster can be centrally managed and traffic will be balanced both within the box (across CPU cores) and within available cluster devices. Unified logging and configuration systems make configuration seamless - a single change to a parameter is replicated and deployed across the cluster (either within an office, or across a globally dispersed organisation). Cluster configuration and log replication is automatic and can be flexibly deployed in a variety of configurations.



NBRS-5.0 is Modular

NBRS-5.0 is designed as a base platform, with security service components that can easily be installed and removed. The base platform consists of a kernel, a user space tool chain, a logging system and a configuration system - essentially an extremely sophisticated router. It is the security service components that provide the UTM+ functionality.

The advantages of this base platform approach are a reduction in firmware size (both in memory and on disk), no requirement for installation of services not required, simplification of deployment, and most importantly a clarity of thinking in what is being provided.

Not only does the entire UTM+ solution get to be best in class, but each individual component gets to stand up on its own and be compared to others. Individually, the components of NBRS-5.0 are best in class, and working together they combine to provide the most effective, affordable and comprehensive network security system.



Conclusions

The development of NBRS-5.0 has been an enormous undertaking for Network Box. Re-thinking solutions to the network security and control problems that plague you, our customers, day-by-day, is not an easy task - particularly in such a rapidly changing threat landscape. We are confident that you'll love NBRS-5.0, and we'll continue to release more information on this product, and on its component security modules, as we can.



Network Box Certified ISO 27001 Security Operations Centre

January 2012 Features

On Tuesday, 3rd January 2012, 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 various internal NOC systems
- Internal changes to Box Office related to migration from LICENSES to CONTRACTS and exposure of contract information to customer view
- Further support for NBR5-5.0 in Box Office systems
- 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 wins two Corporate Choice 2011 Awards

Network Box wins two Corporate Choice 2011 Awards from IT Pro Magazine. One award was for Network Box's Z-Scan zero day anti-virus system; while the other was

for its S-Scan web content filtering system. The Award Ceremony takes place at the Intercontinental Grand Stanford Hong Kong, on 14th December, 2011.

Network Box's new "Z-Scan" anti-malware technology focuses on reducing the time taken to obtain malware samples, and to produce anti-malware signatures. The purpose of "Z-Scan" is to bring that timeframe down from the current industry standard of several hours, to less than one minute. Indeed, best times of just 3 seconds are being seen in the field.



The Network Box "S-Scan" engine is a high speed web content filtering system, designed to help organizations block undesirable web content from reaching their users. When combined with 'Google Safe Browsing,' there are sixteen categories of undesirable content, covering websites which might directly harm an organization's computer systems (websites compromised by malware), as well as websites which include subject matter that may be criminal in nature (hacking sites), cause offence (sexually explicit or hate sites), or otherwise harm users (spyware or fraud).



For more information on ITPro Corporate Choice 2011, please see <http://choice.itpromag.com/>.

DECEMBER 2011 NUMBERS

Key Metric	#	% difference (since last month)
PUSH Updates	507	-1.17
Signatures Released	423,324	+13.4
Firewall Blocks (/box)	826,753	-4.47
IDP Blocks (/box)	184,043	+55.3
Spams (/box)	15,130	-3.28
Malware (/box)	322	-38.67
URL Blocks (/box)	158,708	-19.04
URL Visits (/box)	3,836,156	-14.98

NEWSLETTER STAFF

Mark Webb-Johnson
Editor

Michael Gazeley

Jasmine Arif

Nick Jones

Production Support

Network Box Australia

Network Box Hong Kong

Network Box UK

Contributors

SUBSCRIPTION

Network Box Corporation

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

Copyright © 2012 Network Box Corporation Ltd.