In The Boxing Ring

IN THIS ISSUE

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

Welcome

Welcome to the January 2011 edition of 'In the Boxing Ring'. In this edition, I'll focus on a summary of 2010, and information on what to expect in 2011 and beyond.

On page 2, we discuss the threat numbers for 2010. 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).

On page 3, we turn to look at the software enhancements and features delivered in 2010. For the past year, we've been hard at work delivering enhancements, fixes, patches and new features, and summarize them here.

Also on page 3, we present the features planned for 2011 and beyond. In 2001, Network Box launched the first managed UTM security service, based on a product running our NBRS-1.1 firmware. We enhanced that over the following five years, and in the summer of 2006 launched a new firmware NBRS-3.0. This firmware has now received five years of enhancements, and continuing our five year tradition, we expect to release the first versions of a new NBRS-5.0 firmware late in 2011.

Page 4 details the usual monthly features summary and January hint.

You can contact us here at HQ via eMail (nbhq@network-box.com). Or, drop by our office next time you are in town. You can also keep in touch by following our Network Box Security Response twitter feed at:

twitter.com/networkboxhq

Mark Webb-Johnson
CTO, Network Box Corporation
January 2011

NETWORK BOX

2010 Threat Round-Up

In 2010, Network Box Security Response PUSHed out 11,719 updates, totaling 3,083,018 signatures (down 21.7%, and up 6.1% respectively, compared with 2009).

That is approximately one new signature every 10.2 seconds.

2010 saw 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 2010, the average Network Box blocked 471,304 spams and 25,089 malwares (down 24.1% and up 23.9% respectively, compared with 2009).

The reduction in overall spam volume continues, as large-scale take-down operations are effective in controlling botnet-based spam (which is the most prolific source of spam). 2010 saw the spammers continued migration away from traditional Viagra-type spam to more sophisticated phishing and hoax attacks.

The increase in malware over the year has continued, and reflects this greater level of sophistication on the part of the spammers.

During 2010, the average Network Box blocked a spam or malware once every 63 seconds.

In 2010, the average Network Box blocked 8,129,674 attacks using firewall technology, and 1,738,576 attacks using IDP technology (up 38.9% and 10.6% respectively, compared with 2009).

The movement from a threat landscape primarily composed of mass-mailed spam and malware to one of targeted/mass vulnerability exploit continues during 2010. The growth in IPv4 allocation and exhaustion of IPv4 address space fuels the continued effectiveness of IP-scanning by black hats; and this situation is likely to only get worse until the enormous address space offered by IPv6 takes a hold. 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 3.2 seconds.

2010 saw the deployment of the Network Box NBIDPS system, which goes a long way to improving out 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.

During 2011, Network Box will launch a Network Vulnerability Scanning service that will also improve the protection we can offer to our customers; pro-actively scanning networks for unauthorized servers/services, as well as assisting with patch and vulnerability management processes.

In 2010, the average Network Box blocked 1,143,378 websites due to company content filtering policy enforcement, with 40,653,345 website URLs visited over the year (up 39.1% and 49.8% respectively, compared with 2009).

The growth in bandwidth, usage and in particular web usage continues; nearing 50% growth year-on-year. Fueled by cloud-based Apps, social media, and mobile, the pressure on IT departments with respect to bandwidth and web usage, continues to grow.

So, what is planned for 2011 and beyond?

This year sees the 10th anniversary for Network Box Managed Security Services, and we continue to see the industries highest customer retention rates. 10 years ago, we needed 30,000 anti-virus signatures to protect our customers; today, we need close to 5 million. And it is not just the breadth of coverage that has increased. New technologies such as Intrusion Prevention, Vulnerability Scanning and Content Filtering continue to evolve and are integrated to our product; so increasing our depth of coverage.

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 2011, 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 Threat Statistics	2009	2010	% Change
PUSH Updates	14,969	11,719	-21.7%
Signatures Released	2,905,697	3,083,018	+6.1%
Firewall Blocks (/box)	5,854,972	8,129,674	+38.9%
IDP Blocks (/box)	1,572,211	1,738,576	+10.6
Spams (/box)	621,302	471,304	-24.1%
Malware (/box)	20,251	25,089	+23.9%
URL Blocks (/box)	821,983	1,143,378	+39.1%
URL Visits (/box)	27,132,231	40,653,345	+49.8%

2010 Enhancements

During 2010, Network Box launched 6 new box models (S-25, S-35, S-85, M-255, M-285 and M-385); the new models provided increased choice, reliability and performance across the entire S and M ranges of boxes. The complete Network Box range now offers gigabit network ports and solid state drives.

As well as the hardware lineup changes, more than 100 enhancements were released during 2010, the highlights of which include:

- Korean language support
- GMS Sub-device monitoring
- GMS Ticketing
- Support for Apple's iPad
- Anti-Spam Fuzzy-Fingerprints
- Box Office enhancements
- PUSH update improvements
- Content Filtering performance
- Box Office Notifications
- Sentinel Z-Scan Anti-Virus
- Argus Content Filtering

... and more than 3 million new protection signatures, delivered by more than 11 thousand PUSH updates.

Throughout 2011, we intend to continue our enhancement and security response work, to evolve with the security threat landscape and deliver the most effective protection to our customers.

2011 and Beyond

During the first half of 2011, you can expect to see releases for Network Vulnerability Scanning services, improvements to our Data Leakage Prevention capabilities, plus the usual enhancements and protection signatures for the NBRS-3.0 platform.

In 2001, Network Box launched the first managed UTM security service, based on a product running our NBRS-1.1 firmware. We enhanced that over the following five years, then in the summer of 2006 launched a new firmware NBRS-3.0. That firmware has now received five years of enhancements, and continuing our five year tradition, we expect to release the first versions of a new NBRS-5.0 firmware late in 2011.

You can expect to see the release of more information on the future NBRS-5.0 product, starting in 2011Q2. We will continue to use this In the Boxing Ring newsletter to get the news out about these new products.

NBRS-5.0 will be a major new platform, building on the existing NBRS-3.0 and incorporating enhancement requests from our customer base (both current and potential new markets). As with NBRS-1.1 to NBRS-3.0, we will provide an upgrade migration path from NBRS-3.0 to NBRS-5.0, as well as continue to support NBRS-3.0 customers for several years.

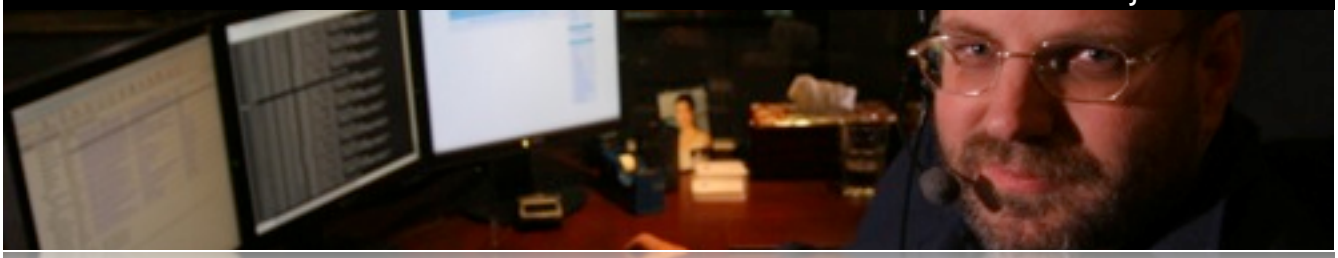
When we talk to our customers about what they want, the following key points repeatedly come up:

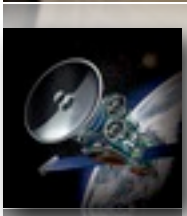
1. Transparency: you want the boxes to be easily deployed and as transparent as possible to the existing network.
2. Performance: balancing the trade-off between completeness of the scan, and throughput, you want the highest throughput possible.
3. Inbound filtering: you want dirty IP outside, clean IP inside.
4. Outbound filtering and control: you want control (at the application and protocol levels) of what your users are doing, as well as comprehensive management of bandwidth.
5. Scalability: you want to be able to scale and re-balance the solution depending on a changing workload.
6. Integration: you want the gateway protection to be integrated to your internal systems (such as DHCP, Active Directory, LDAP, etc).
7. Reporting: you want comprehensive reporting, for both control and compliance purposes.

Looking at the challenging and changing threat landscape, we also anticipate:

1. IPv6: this will become increasingly important, and you need a clear migration path to IPv6, with dual-stack support and NAT between IPv4 and IPv6.
2. SSL: you need to scan inside SSL tunnels, and control what happens inside these tunnels.
3. Instant Messaging: a subset of point [4], outbound filtering and application/protocol identification; you need effective control over IM, P2P and VOIP applications.

NBRS-5.0 is designed to address these concerns and deliver this in both a unified and a holistic manner. Utilizing and leveraging both in-the-cloud and on-the-box technologies, we're busy laying the foundation for the next five years of Network Box.





January 2011 Features

On Tuesday, 4th January 2011, 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:

- Release of Kaspersky v8 engine. As discussed in the December 2010 Boxing Ring newsletter, this new engine is the same engine as used in Kaspersky desktop and server products (on Windows and Linux), but is optimized for use at the gateway. As well as welcome performance and memory improvements, the engine brings improved heuristic detection capabilities and application sand-boxing technologies.
- Optimizations to the content filtering policy engine, related to membership of the 'everyone' group.
- Enhancements to the Box Office Contracts system, for managing and displaying customer contracts.
- Health monitoring support for Kaspersky v8 engine.

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.

January 2011 Hint

The Pareto principle (also known as the 80-20 rule), states that, for many events, roughly 80% of the effects come from 20% of the causes. In other words, 80% of your mail comes from 20% of your sources, and 80% of your bandwidth is used by 20% of your users.

Every quarter, Network Box releases a report on the state of Web Usage (the 2010Q4 report will be released next week, along with the 2010 yearly report).

When looking at bandwidth usage, you should be concentrating on the top sites and top users. The 2010 Web Usage report shows that sites like YouTube and Facebook take up close to 20% of all the web bandwidth of Network Box customers. Facebook alone is 10% of web URL requests, and YouTube is 13% of bandwidth. Concentrating on control of these sites will have the biggest impact on bandwidth.

In the case of threat protection, the Pareto principle is unfortunately unworkable (few would argue that 80% protection is good enough), but for bandwidth control Pareto works well.

The January 2011 hint is that you have a look at the numbers for your network. The Network Box my.network-box.com reports have all the information you need to see what is going on and who is using what bandwidth. It is easy to be distracted by individual events, so apply the Pareto principle and go after the biggest culprits first.

Mark Webb-Johnson,

CTO, Network Box Corporation

DECEMBER 2010 NUMBERS

Key Metric)	#	% difference (since last month)
PUSH Updates	812	+2.4
Signatures Released	409,998	-15.5
Firewall Blocks (/box)	753,356	-2.6
IDP Blocks (/box)	110,749	-10.4
Spams (/box)	26,943	-6.6
Malware (/box)	332	+19.0
URL Blocks (/box)	114,684	-21.2
URL Visits (/box)	3,614,373	-17.2

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