

In The Boxing Ring



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

Welcome

Welcome to the October 2009 edition of 'In the Boxing Ring'. In this edition, we focus on the New NBIDPS system as it emerges from private development and heads straight for public beta. With the October Patch Tuesday, it has been integrated into the MY.NETWORK-BOX.COM administrative interface, so that now the IDP module shows the top types of attacks detected and deflected. The system will be rolled out in two phases. Turn to Page 2 for details.

Last month, we mentioned that Network Box joined the Microsoft Active Protections Program. Joining MAPP means we can provide you with even more comprehensive protection earlier and more effectively. For an exact explanation as to how this partnership works, turn to Page 3.

Page 4 details the usual monthly features summary and hints.

As usual, if you have any feedback, or comments, they are always appreciated. 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 new Network Box Security Response twitter feed at:

twitter.com/networkboxhq

Mark Webb-Johnson
CTO, Network Box Corporation
October 2009

IN THIS ISSUE

2. NEW NBIDPS SYSTEM ENTERS PUBLIC BETA

On 13 October 2009, the new NBIDPS system is rolled out for your use. Deployed in two phases, the first phase uses passive IDS mode and phase two switches the mode to IPS. The most noticeable difference will be the increased number of attacks detected and deflected.

3. NETWORK BOX AND MAPP

Network Box has joined the Microsoft Active Protections Program. Hinted at last month, more details are provided in this month's *In the Boxing Ring*.

4. OCTOBER 2009 FEATURES

As usual, we will be deploying our on-going enhancements and improvements as well as maintenance features.

4. OCTOBER 2009 HINT

Tips on how to speed up your queries are provided here to help facilitate your work and keep you updated efficiently and effectively.





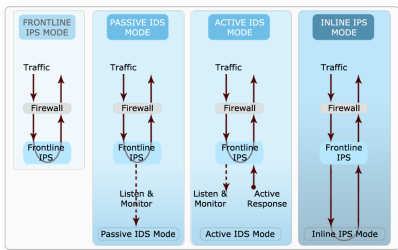
New NBIDPS System Enters Public Beta

On Tuesday, October 13, 2009, the new

NBIDPS system leaves private development and testing to enter its public beta phase. On that date, we are starting our first large-scale deployments of the technology. This system is offered to all clients.

Back in the June 2009 edition of *In the Boxing Ring*, we described how IDPS works and the type of system architecture that it, ideally, uses:

The Network Box Intrusion Detection and Prevention System (NBIDPS) offers four modes of Intrusion Detection and Prevention:



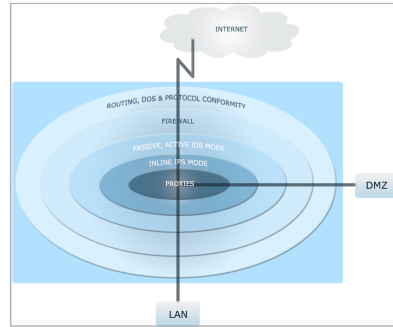
- Front-line IPS is an extremely lightweight, high-speed service, offering zero-latency protection, inline with the data stream, against network worms, exploits and other such attacks.
- Passive IDS alerts and logs traffic side-by-side with the data stream; this is useful for policy enforcement and more aggressive rules.
- Active IDS also alerts and logs traffic along side the data stream, but has the ability to actively tear down malicious connections (once malicious traffic has been identified).
- Inline IPS alerts and logs traffic inline with the data stream, as well. Inline IPS is tightly coupled to the firewall, enabling it to drop traffic before the remote system sees it.

The system architecture of Network Box for a typical system using this technology can be represented as a series of concentric circles.

Each layer provides different protections. From the most basic (routing,

DOS and protocol conformity) to Proxies.

The inner-most layer comprises a set of Protected Services Proxies for specific protocols, e.g., POP3, IMAP4, SMTP, HTTP and FTP. These provide application-layer protection against malware, spam, protocol enforcement and policy violations.



The NBIDPS system is designed to apply the second-inner layer of protection: passive IDS, active IDS and inline IPS protection using sophisticated rules and protocol / stream decoding engines.

With the Network Box October Patch Tuesday, NBIDPS has been integrated into the MY.NETWORK-BOX.COM administrative interface. The overview page of the IDP module shows the top types of attacks and an overview description.

Type	Count	Percentage
ICMP	1	0%
IDS-116.55	1	0%
IDS-1.200000476	1	0%
IDS-1.200000483	1	0%
IDS-1.200000499	2	0%
IDS-1.200001616	2	0%
IDS-1.200002003	1	0%
IDS-1.200002050	1	0%
IDS-1.200002590	1	0%
IDS-1.200003634	1	0%
IDS-1.202000537	126	10%
IDS-1.202000545	126	10%
IDS-1.202002911	1	0%
IDS-1.202009584	6	0%
NETBIOS	2	0%
SOBIG-F	24	2%

Type	In
IDS-1:200000499	IPS
IDS-1:20000499	IPS
NETBIOS	NETHGC
IDS-1:200001616	IPS
NETBIOS	NETHGC
IDS-1:200001616	IPS
IDS-1:200001616	IPS
IDS-1:20000545	IPS
IDS-1:202000537	IPS
IDS-1:202000537	IPS
IDS-1:202000545	IPS
IDS-1:202000537	IPS
IDS-1:202000545	IPS
IDS-1:202000537	IPS
IDS-1:200000499	IPS
IDS-1:200000483	IPS
IDS-1:200000499	IPS
IDS-1:200000499	IPS
IDS-1:200000499	IPS
IDS-1:200000499	IPS

Type	Count	Percentage
ICMP	1	0%
IDS-116.55	1	0%
IDS-1.200000476	1	0%
IDS-1.200000483	1	0%
IDS-1.200000499	2	0%
IDS-1.200001616	2	0%
IDS-1.200002003	1	0%
IDS-1.200002050	1	0%
IDS-1.200002590	1	0%
IDS-1.200003634	1	0%
IDS-1.202000537	126	10%
IDS-1.202000545	126	10%
IDS-1.202002911	1	0%
IDS-1.202009584	6	0%
NETBIOS	2	0%
SOBIG-F	24	2%

Clicking *Live Watch* in the left-hand menu offers detailed real-time information. And placing the mouse cursor over the link in the *Type* column brings up a tag describing the threat.

Type	In
IDS-1:200000499	IPS
IDS-1:20000499	IPS
NETBIOS	NETHGC
IDS-1:200001616	IPS
NETBIOS	NETHGC
IDS-1:200001616	IPS
IDS-1:200001616	IPS
IDS-1:20000545	IPS
IDS-1:202000537	IPS
IDS-1:202000537	IPS
IDS-1:202000545	IPS
IDS-1:202000537	IPS
IDS-1:202000545	IPS
IDS-1:202000537	IPS
IDS-1:200000499	IPS
IDS-1:200000483	IPS
IDS-1:200000499	IPS
IDS-1:200000499	IPS
IDS-1:200000499	IPS
IDS-1:200000499	IPS

Type	In
IDS-1:200000499	IPS
IDS-1:20000499	IPS
NETBIOS	NETHGC
IDS-1:200001616	IPS
NETBIOS	NETHGC
IDS-1:200001616	IPS
IDS-1:200001616	IPS
IDS-1:20000545	IPS
IDS-1:202000537	IPS
IDS-1:202000537	IPS
IDS-1:202000545	IPS
IDS-1:202000537	IPS
IDS-1:202000545	IPS
IDS-1:202000537	IPS
IDS-1:200000499	IPS
IDS-1:200000483	IPS
IDS-1:200000499	IPS
IDS-1:200000499	IPS
IDS-1:200000499	IPS
IDS-1:200000499	IPS

Deployment of the NBIDPS system is typically conducted in two phases to assess loading impact and reduce the possibility of false positives affecting business continuity.

- Phase 1: the NOC deploys the system in passive IDS mode to monitor the loading impact and determine which signatures are firing and what traffic would be blocked. Over one to two weeks, the NOC fine-tunes the system on an individual Box basis.
- Phase 2: After Phase 1 is successfully completed, the NOC switches the mode to IPS to enable active enforcement.

The most noticeable difference you will see after switching to the new system is an increase in the number of attacks detected and blocked. As well as new protocol and stream decoders, the new system offers over 20 times the number of signatures. This is reflected in the breadth and depth of attacks it can detect.

Additionally, to ensure the system is as comprehensive as possible, Network Box has joined the Microsoft Active Protections Program (MAPP). This new program provides vulnerability information in advance of Microsoft's monthly security update release. More on this on the following page.

Network Box and the Microsoft Active Protections Program

Microsoft Security Response Center Partners



- » Microsoft Malware Protection Center
- » Active Protections: <http://www.microsoft.com/security/portal/>



- » Network-Box Security Web site
- » Active Protections: <http://www.network-box.com/support/mapp>

Network Box has joined the Microsoft Active Protections Program (MAPP). MAPP is a programme from the Microsoft Security Response Center (MSRC).

MAPP will provide us with vulnerability information in advance of Microsoft's monthly security update release to offer protection to customers efficiently and effectively. By receiving vulnerability information earlier, our clients benefit from additional possible improvements that provide security protection, such as Active Intrusion Detection and Prevention, as part of the Network Box managed UTM+ services.

Commenting on the partnership, Mark Miller, director of Microsoft's Trustworthy Computing product management stated: "Our partners share our passion for industry collaboration to protect a world full of Internet users. No one company can accomplish this by itself. That is why we are partnering with Network Box to advance and improve security."

So, what does this mean for our clients?

Firstly, it means that Network Box Security Response is now working in partnership with Microsoft to release active protection vulnerabilities in Microsoft software. Our protection release is synchronised with Microsoft's Patch Tuesday. So, in most cases, the protection is released at the same time the vulnerability is publicly announced.

Secondly, this means, even if our client does not, or cannot, immediately apply Microsoft's patches, the Network Box active protection signatures and heuristics will provide some protection against exploit of these vulnerabilities.

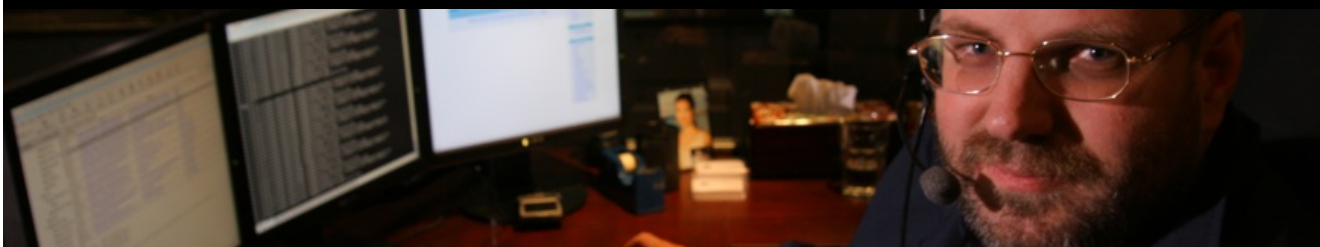
And, finally, it means that every Microsoft Patch Tuesday (the second Tuesday of each month), Network Box will release a report on the Microsoft Patch Tuesday fixes. This report details each vulnerability, the active protection that we have released, and our recommendations regarding each vulnerability. The latest reports can be found at <http://www.network-box.com/support/mapp>. As well as detailed

information on Network Box protection, you should also find these a useful summary of the Microsoft announcements.

But, most important is how this fits in with Network Box's Managed Security model. By maintaining such a close relationship with our customers, as well as having detailed technical knowledge of customer configurations and network arrangements, Network Box NOCs are in an ideal position to be able to assess the possible impact of each vulnerability, on an individual customer basis. We are then able to offer recommendations tailored both to our overall customer base and on an individual case basis.

Network Box, in cooperation with our OEM partners, utilises a whole range of technologies to implement these active protections — including anti-virus, anti-spam, firewall and Intrusion Prevention systems depending on the actual vulnerability. However, the majority of these vulnerabilities are network-based and often require real-time detailed analysis and scanning of network traffic. The Network Box NBIDPS system, entering public beta on 13 October 2009, forms the core technology to enable us to deploy these active protections.

Security is an industry challenge. With the Microsoft Active Protections Program, Network Box and Microsoft continue to show each company's commitment to industry partnership to help protect customers. Enhanced protection at both the application and network layers, means customers have improved defence-in-depth protection while testing and deploying Microsoft security updates.



October 2009 Features

On Tuesday, 6 October 2009, we will globally release the enhancement features to our systems. These improvements provide both performance and usability, as well as facilitate the interface for key administrative functions.

The release of the new NBIDPS system is on 13 October 2009. Large-scale deployment will also begin that Tuesday. On the same date, we shall also be releasing MAPP vulnerability notes for the Microsoft Patch Tuesday releases.

We will also be releasing some further refinements and minor bug fixes to the MY.NETWORK-BOX.COM and Mail Portal web systems, including:

- Fixes to Mail / Status / Trace for searches of ‘clean’ messages.
- Integration of NBIPDS information into the IDP module, status and analysis tabs — these revisions provide both summary and detailed documentation on the different types of IDP blocks.

We have also made enhancements to the POP3 Acceleration system, to support a server keep-alive facility.

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. The regional NOCs will be conducting the rollouts of the new functionality in a phased manner.

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

October 2009 Hint

One of the things NOCs frequently get asked is how to speed up queries on the MY.NETWORK-BOX.COM administrative interface. Here are some suggestions (in order of impact):

- Narrow down the search date / time range (using the “Period” option). With some boxes recording millions of records a day, narrowing the date / time range of the search to the smallest possible denominator will have the biggest impact on performance.
- Don’t do complex searches / reports during peak periods. It is preferable to run these off-peak to avoid slowing down other tasks the box is handling.
- Don’t use “contains” unless absolutely necessary. the indexed searches (“is” and “starts with”) are hundreds of times faster than “contains” searches.
- Complete as many search terms as you can. They are all combined together, and that narrows down the number of records that must be searched.”

Your searches and reports should appear within a couple of seconds from your MY.NETWORK-BOX.COM. If not, then please try the above techniques.

Mark Webb-Johnson
 CTO, Network Box Corporation
 October 2009

SEPTEMBER 2009 NUMBERS

Key Metric)	#	% difference (since last month)
PUSH Updates	1,551	+4.3
Signatures Released	226,861	-45.3
Firewall Blocks (/box)	638,485	+0.8
IDP Blocks (/box)	190,456	-2.3
Spams (/box)	59,439	-6.7
Malware (/box)	3,404	+60.3
URL Blocks (/box)	123,777	+6.1
URL Visits (/box)	3,319,291	+4.3

NEWSLETTER STAFF

Mark Webb-Johnson
 Editor

Pauline Chiu

Michael Gazeley

Jason Law

Nick Jones

Production Support

Network Box Australia

Network Box Hong Kong

Network Box UK

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