In The Boxing Ring

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

IN THIS ISSUE

Welcome

歡迎您閱讀2009年10月版的In the Boxing Ring。在這一版中，我們著眼於最近新改進的NBIDPS入侵檢測與防禦系統，因爲它即將從開發階段過渡到目前的公開測試階段。伴隨著10月份的週二補丁一起，它已被納入了MY.NETWORK-BOX.COM管理介面中，所以現在IDP顯示模組可以以排序的方式顯示出業已檢測出的和已經被清除的攻擊。該系統將分兩個階段逐步推出。請轉到第2頁瞭解更多的細節內容。

上個月，我們提到，Network Box已經加入了微軟的積極防禦計畫（簡稱MAPP）。成功地加入MAPP意味著我們能夠提供給您更全面、更有效的安全保護。關於這種夥伴關係是如何工作的，請轉到第3頁瞭解詳細的內容。

第4頁的細節內容你照慣例是關於月度總結和使用技巧提示。

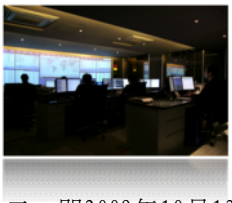
和以往一樣，如果您有任何的回饋，意見或者建議，我們都歡迎您隨時提出來。您也可以通過發送郵件到我們的郵件列表：nbhq@network-box.com聯繫我們。或者當您下次在香港市區的話來隨時來我公司辦公室進行參觀指導。

您也可以通過加入或訂閱我們的安全響應Twitter 和我們保持聯繫，網址是：

twitter.com/networkboxhq

Mark Webb-Johnson
CTO, Network Box Corporation
October 2009

NETWORK BOX

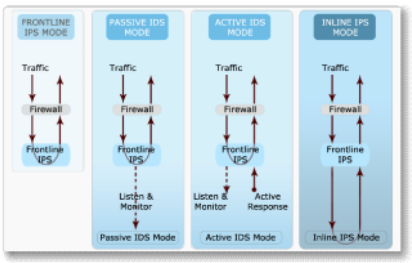


新的NBIPDS系統進入公開測試階段

在這個星期二，即2009年10月13日，新的NBIDPS系統將終結前期開發和內部測試，從而進入它的公開測試階段。從這一天開始，我們開始對我們的這一技術進行第一輪大規模部署。這個系統將提供給所有的客戶。

回想起在2009年6月版的In the Boxing Ring中，我們描述了IDPS是怎麼運作的，以及使用系統架構的種類，理想情況如下：

Network Box新的網路入侵檢測與預防系統提供四種模式下的入侵檢測與預防：

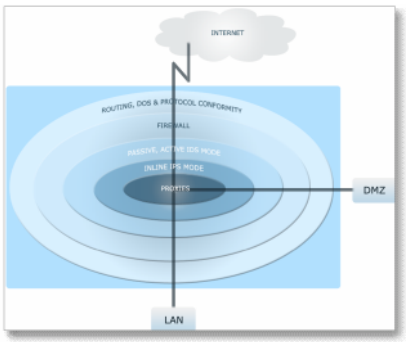


- 前端IPS系統。它可以非常輕便的，零延遲，防止蠕蟲，漏洞和其他此類的攻擊。
- 被動入侵檢測系統-報警和記錄相關流量，旁路方式部署獲取資料流程——方便執行政策和發放更具攻擊性的規則。
- 積極的入侵檢測系統-報警和記錄相關流量，側路方式部署獲取資料流程，當發現惡意網路流量時，它可以使用積極的方式中斷連接會話。
- 串聯的IPS -報警和記錄相關流量，資料流程將穿透經過系統；串聯的IPS可以和防火牆緊密地結合，它可以使遠端入侵流量在進入內部系統之前就被丟棄（拒絕）。

包含這一技術的Network Box的網路安全系統架構可以用一系列的同心圓來展示。

每個層次提供不同的防護。這些層次從最基本（路由，拒絕服務保護和協定一致性檢查）到安全代理服務。

最核心的保護層包含一組受保護的服務代理，具體的協定，如POP3，IMAP4，SMTP，HTTP和FTP。它們用來提供應用層保護，防止惡意軟體及垃圾郵件，以及對安全政策的嚴格執行。



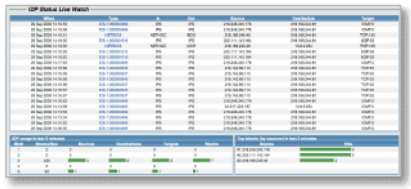
NBIDPS系統被設計在靠內的第二層進行安全保護：被動IDS、主動IDS和串聯IPS使用先進的規則和協定/流解碼引擎。

同Network Box10月份的補丁星期二一起，NBIDPS將集成於MY.NETWORK-BOX.COM管理介面中。IDP模組的概要頁而將顯示排名靠前的攻擊及這些攻擊的簡單描述。

Top Type

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 %

點擊在左手菜單的即時觀看將得到詳細的即時資訊。 並且當您講滑鼠游標放置在類型專欄的鏈結上時，會看到有標記威脅的詳細描述。



Type	In
IDS-1:200000499	IPS
IDS-1:200000499	IPS
NETBIOS	NETHGC
IDS-1:200001616	IPS
NETBIOS	NETHGC
IDS-1:200001616	IPS
IDS-1:200001616	IPS
IDS-1:20(DNS named version attempt	
IDS-1:202000545	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

部署NBIDPS系統將分爲兩個典型的階段，包含評估系統負載影響及減少可能會影響業務連續性的假陽性反應。

- 第一階段： NOC將系統部署爲被動IDS模式，用來監測負載影響並且確定哪些入侵代碼可以使用，哪些攻擊流量將被阻攔。這個過程要持續一到二個星期，在這期間NOC將根據每一個單獨的箱子爲依據進行系統優化。
- 第二階段： 在第一階段順利地完成以後，NOC將切換系統工作在IPS模式下以確保開始執行針對攻擊的主動防禦。

換成新的系統以後，您將體會到的最大的變化在於檢測和封鎖的攻擊的數量的會有大幅增加。 再加上新的協議和流解碼器，新的系統將提供超過此前20倍的簽名的數量。這可使它可能檢測出更有廣度和深度的攻擊。

另外，爲了保證系統的功能盡可能的全面，Network Box加入了微軟的主動防護計畫(MAPP)。這個新的計畫將使微軟在每月度安全更新發行前提供給我們漏洞或弱點的資訊。 要瞭解更多的內容請翻看下頁。

Network Box and the Microsoft Active Protections Program

Network Box已經加入了微軟主動保護計畫(MAPP)。MAPP是微軟安全回應中心(MSRC)的一個項目。

MAPP將使我們在微軟每月爲客戶發佈補丁更新之前獲得漏洞的詳細資訊，以便能提供給客戶相關的安全更新並使客戶獲得高效、有效的保護。由於我們可以更早些地收到相關的漏洞資訊，客戶可以從中得到附加的安全主動保護改進方面的收益，諸如主動入侵檢測和防範，它是Network Box UTM+管理服務的一部分。

馬克·米勒，微軟的可信計算產品管理評論說：“我們的合作夥伴分享我們的激情，以達到業界協作共同保護世界上的互聯網用戶。沒有一家公司可以獨自做到這一點。這就是爲什麼我們通過與Network Box合作，共同提高和改進安全的原因。”

因此，這對我們的客戶來講意味著什麼呢？

首先，意味著Network Box安全響應團隊現在與微軟合作，發佈針對微軟公司軟體漏洞的主動保護。我們的保護代碼與微軟的星期二補丁同步發放。因此，在許多情況下，保護在漏洞弱點被公開宣佈的同時已經成效。

第二，這意味著，即使我們的客戶尚未，或者不可能馬上安裝微軟的補丁，Network Box的主動保護簽名代碼以及啓發式學習法就可以提供一些防護措施，以阻止利用這些漏點的溢出攻擊。

最後，它也意味著在每個微軟星期二補丁(每個月的第二個星期二)發放時，Network Box將公佈關於微軟星期二補丁的一個報告。這個報告會詳述列出發佈了的每個弱點、我們已經發放的主動保護以及我們對於每個弱點的建議。最新的報告可以在http://www.network-box.com/support/mapp 中找到。

關於Network Box主動保護的更詳細資訊，您也可以在微軟公告中發現它們這些非常有用的總結。

但是，最重要的是它是如何適應Network Box可管理的安全模型的。通過維護與我們顧客的密切關係，並且擁有對顧客的配置和網路安排更深入的技術知識，Network Box的安全運維中心NOC處在一個能幫忙估計每個弱點帶來的潛在影響的理想位置，對每一個單獨顧客都是這樣。然後我們能提供針對我們的整體用戶和在單個用戶的專業建議。

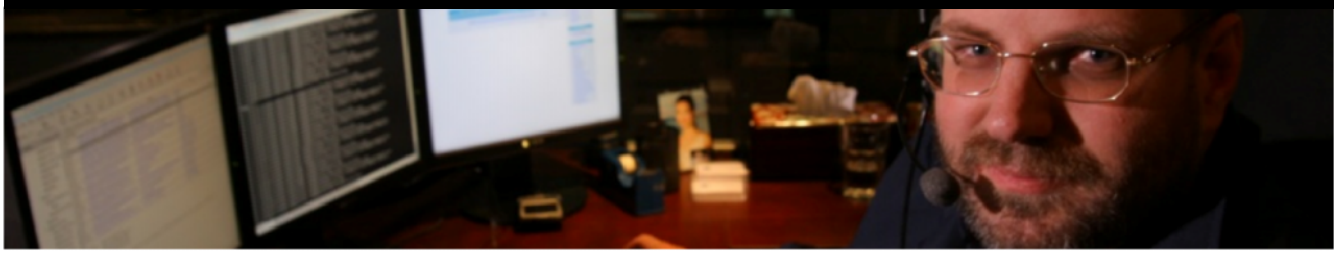
Network Box和我們的OEM合作夥伴一起，使用一系列的技術來執行這些積極防禦——包括利用系統真實漏洞的防病毒，反垃圾郵件，防火牆和入侵防禦系統。

然而，大多數這些漏洞是基於網路的，往往需要即時地進行詳細的資料分析和對網路流量的掃描。

Network Box NBIDPS新系統即將於2009年10月13日進入公共測試階段，這將建立新的核心技術，允許我們部署這些積極的保護。

安全是一個行業的挑戰。在微軟主動保護計畫，Network Box和微軟公司繼續我們的承諾——致力於通過業界合作來保障客戶的安全。

加強應用層和網路層的保護，也意味著客戶在在測試和部署微軟安全更新時已經啓用和改進了深層防禦體系。



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

近期網路運維中心NOC常常得到的要求之一是如何加速在MY.NETWORK-BOX.COM管理的查詢。下面這兒有些建議(按照可帶來的影響爲序) ：

- 縮小查尋日期/時間範圍 (使用"期間"選項)。對每天記錄成千上萬條紀錄的那些箱子，縮小查詢的日期/時間範圍，到盡可能最小的限度將大幅提高性能的改進。
- 不要在高峰期，做複雜的查尋/報告指令。 建議在非高峰期處理，以防止對Box正在處理的其他任務速度變慢。
- 不要使用“包含”，除非絕對有必要。索引搜索(“是”和“開始與”)可以比“包含”查尋有數百倍的快速。
- 輸入更可能多的查尋條件。他們全部被結合在一起，並且那樣做可縮小必須搜尋的結果紀錄數。

正常情況下，您的查尋和報告應該在兩三秒鐘內就在您的MY.NETWORK-BOX.COM介面中出現。否則，請嘗試上面所講的這些技術。

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