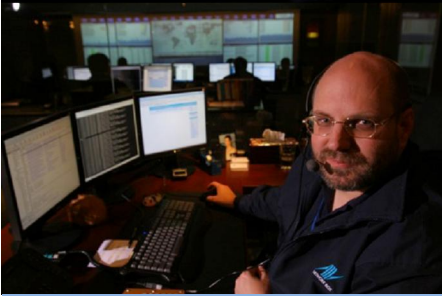


In The Boxing Ring



本期概要：

2. 2010年網路威脅概述總結

這部分，我們對關於2010年網路威脅有關資料以及威脅環境的性能指標進行了探討。

3. 2010年的提高

總結了一下2010年以來軟體的提高和功能特性上的改善。

3. 2011年的展望

對Network Box的2011年進行了未來的展望。

4. 2011年1月 新特性

一如往常，我們將對所有的NBRS-3.0 用戶進行我們持續不斷地增強、改善並部署，並進行相關的維護。

4. 2011年1月 提示

將帕雷托法則應用於頻寬控制。

來自 Network Box 首席技術官

Mark Webb-Johnson 的技術資訊

Welcome

歡迎閱讀 2011 年 1 月刊的《In The Boxing Ring》。在這次的月刊中，我們將主要針對 2010 年的總結以及 2011 年的未來展望進行了探討。

在第 2 頁，我們對 2010 年的威脅的有關資料進行了討論。Network Box 的安全回應監控並管理著全球數以千計的安全設備，這給予我們對威脅環境以極好的觀察依據。在 Network Box，我們堅信，只有在有能力清楚地觀察並分析問題的所在，才能夠拿出解決問題的最佳方案。

在第 3 頁，我們對 2010 年在軟體方面的增強和提升進行了歸納總結。在過去的一年裡，我們一直都有在致力於性能的提升、問題的解決、補丁的發佈、新特性的開發以及不斷的總結。

而且在第 3 頁中，我們對 2011 年進行了未來的展望。自從 2001 年，Network Box 推出了第一個 UTM 的安全管理服務，此服務運行於我們的 NBRS-1.1 版本固件的產品。

並且在接下來的 5 年之中一直致力於對其性能等各方面的提升。並且在 2006 年夏，我們又推出了一個新的 NBRS-3.0 版本的固件。這個版本的固件也經歷了 5 年的性能等各方面的提升，也保持了我們 5 年來的傳統，我們期望在 2011 年後期能發佈新版本 NBRS-5.0 的第一個版本。

第 4 頁是關於每個月的新特性和一月份的提示。

和往常一樣，如果您有任何寶貴的回饋、意見或者建議，我們都非常歡迎和感激不盡。您可以通過郵箱 (nbhq@network-box.com) 與我們總部取得聯繫，或者方便的話直接到我們辦公的地方來參觀指導。

您也可以訂閱我們的 Network Box 安全響應 Twitter 對我們保持關注，網址為：

twitter.com/networkboxhq

Mark Webb-Johnson

CTO, Network Box Corporation

2011 年 1 月



2010 年網路威脅概述總結

在 2010 年，Network Box 安全回應 PUSH (推送) 了 11,917 個更新，總計 3,083,018 個特徵碼 (相對於 2009 年分別下降了 21.7% 和上升了 6.1%)。

幾乎每 10.2 秒就發佈一個新特徵碼。

從 2010 年來看，每次更新的特徵碼數量逐次下降，而發佈的特徵碼總數量卻是增加；這也反映出向基於雲的特徵碼系統的不斷轉移 (比如 Network Box 的 Sentinel Z-Scan 系統，以及 NBCP 內容分類系統)。我們預計這一趨勢將繼續發展，因為傳統的特徵碼依然對更深度和廣泛的惡意軟體還是無濟於事，而基於雲的特徵碼正成為針對零日爆發的最有效的解決方案。

在 2010 年，每個 Network Box 平均攔截 471,304 封垃圾郵件和 25,089 個惡意軟體 (相對於 2009 年分別下降了 24.1% 和上升了 23.9%)。

垃圾郵件的總量在不斷地下降，緣於大規模的清除操作使有效地控制住了基於僵屍網路的垃圾郵件 (這是垃圾郵件最豐富的來源)。從 2010 年來看，垃圾郵件發送者依然還是更多地使用傳統的偉哥型垃圾郵件，而更加複雜的網路釣魚和騙局攻擊則相對要少些。

而惡意軟體相比於去年卻仍在不斷增長，這反映了更大一部分的垃圾郵件發送者的水準也在不斷提升。

2010 年內，每個 Network Box 平均每 63 秒攔截一封垃圾郵件或惡意軟體。

2010 年，每個 Network Box 使用防火牆技術平均攔截 8,129,674 次攻擊，使用 IDP 技術平均攔截 1,738,576 次攻擊 (相對於 2009 年分別上升了 38.9% 和 10.6%)。

主要以大量垃圾郵件和惡意軟體構成的網路威脅環境在不斷地向具有針對性的利用大量的漏洞的方式而轉變。IPv4 分配使用的不斷增長以及 IPv4 位址空間的消耗殆盡，使得壞人在 IP 掃描上更加有效。

而且這種情況將變得更糟，直到更巨大位址空間的 IPv6 正式啓用的那一天。IPv4 位址空間現在污染非常嚴重，這使得在 2010 年平均每個 Network Box 用戶每 3.2 秒就會產生一次防火牆或者 IDP 網路層的檢測攔截。

2010 年我們進行了 Network Box 的 NBIDPS 系統的部署。為使這個系統在網路層 IPv4 的保護功能得到進一步提升，我們為此而經歷了一段漫長的路程。但是，全面的防火牆政策 (特別是出站防火牆策略控制) 依然是用於控制網路層威脅的最有效機制。

在 2011 年期間，Network Box 將推出 Network Vulnerability Scanning 服務 (網路漏洞掃描服務)，這必將增強對我們使用者網路的保護。這還將可以積極主動地對網路中未授權的伺服器 and 服務進行掃描，這和我們的補丁和漏洞管理所提供的服務是類似的。

在 2010 全年，每個 Network Box 通過公司內容過濾策略的執行，平均攔截 1,143,378 個網站和 40,653,345 個網站 URL (相對於 2009 年分別上升了 39.1% 和 49.8%)。

頻寬的使用，特別是網頁內容方面的使用在不斷的增長，幾乎有 50% 的逐年增長率。基於雲的應用服務，社會媒體，行動電話的不斷發展，使得 IT 部門在頻寬和網頁內容使用方面的壓力逐漸加大。



那麼，2011 年會有哪些計畫展望呢？

今年是 Network Box 安全管理服務推出後的 10 周年，我們也一直看到行業最高的客戶保留率。10 年前，我們需要 30,000 個反病毒碼來保護我們的客戶網路，而今天，我們需要將近 5,000,000 個。這不僅僅是在覆蓋的廣度上大大的擴展。諸如入侵防禦、漏洞掃描和內容過濾等新技術的不斷發展，並整合進入我們的產品，從而也進一步更加深度地覆蓋。

互聯網威脅環境在不斷發展惡化，而我們的產品也在不斷地發展，以滿足應對這些新的挑戰，這一切，也進一步驗證了我們的不斷進步與提高的產品，全球管理的方式，還有服務 (而不僅僅只是靜態的一個產品) 都是符合發展趨勢的。

進入 2011 年以後，我們還將毫無疑問地看到更多類似的情況。互聯網環境在變化，而我們的 Network Box (包括產品和服務) 同樣也將繼續不遺餘力地為向客戶提供最有效的保護而不斷努力。

Network Box 威脅統計	2009	2010	變化比(%)
PUSH 更新	14,969	11,719	-21.7%
特徵碼發佈	2,905,697	3,083,018	+6.1%
防火牆攔截(/box)	5,854,972	8,129,674	+38.9%
IDP 攔截(/box)	1,572,211	1,738,576	+10.6%
垃圾郵件(/box)	621,302	471,304	-24.1%
惡意軟體(/box)	20,251	25,089	+23.9%
URL 攔截(/box)	821,983	1,143,378	+39.1%
URL 訪問(/box)	27,132,231	40,653,345	+49.8%

2010 年的提高

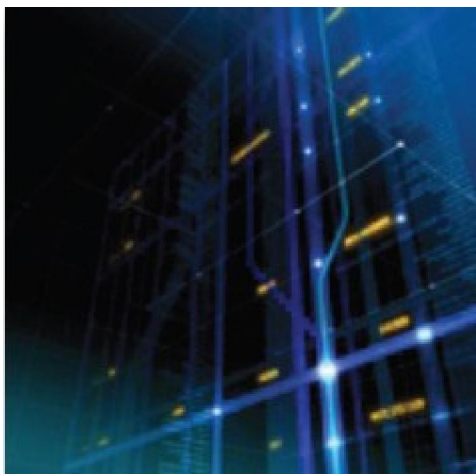
2010 年以來，Network Box 推出了 6 款新的 Box 產品（S-25, S-35, S-85, M-255, M-285 和 M-385），給用戶提供了更多的選擇，而這些 S/M 系列的 Box 在可靠性和性能表現上也更加優越。這一整個系列的 Network Box 現在都可以提供千兆網路介面和固態硬碟驅動器。

除了在硬體陣容上的變化之外，2010 年還有 100 多項各個方面的優化和提高進行了發佈，其中的亮點包括：

- 韓國語的支持
- GMS 的下層設備監控
- GMS 工單
- 對蘋果 iPad 的支持
- 反垃圾郵件的模糊指紋識別技術
- Box Office 的一系列增強
- PUSH 更新的改善
- 內容過濾的性能改善
- Box Office 的通知系統
- Sentinel Z-Scan 反病毒掃描
- Argus 內容過濾

還有 3,000,000 個以上新的防護特徵碼，通過 PUSH 技術推送更新多於 11,000 次。

進入 2011 年以後，我們還將繼續不遺餘力地向客戶提供最有效的保護而不斷努力，不斷提高，並做好安全回應的工作。



2011 年的展望

2011 年的上半年，值得期待的有 Network Vulnerability Scanning 服務（網路漏洞掃描服務），我們的資料洩漏防護功能方面的改進，還有就是 NBR5-3.0 平臺上常規性的增強改進和防護特徵碼的發佈。

2001 年，Network Box 推出了第一個 UTM 的安全管理服務，此服務運行於我們的 NBR5-1.1 版本固件的產品。並且在接下來的 5 年之中一直致力於對其性能等各方面的提升。並且在 2006 年夏，我們又推出了一個新的 NBR5-3.0 版本的固件。這個版本的固件也經歷了 5 年的性能等各方面的提升，也保持了我們 5 年來的傳統，我們期望在 2011 年後期能發佈新版本 NBR5-5.0 的第一個版本。

從 2011 年的第二季度開始，未來的 NBR5-5.0 版本的產品也將發佈更多的相關資訊，這些也將值得您的期待。我們還將繼續通過《In The Boxing Ring》月刊進行這些產品的資訊發佈。

NBR5-5.0 將是一個新的專業平臺，建立於現有的 NBR5-3.0 平臺，並大量吸收了基於用戶（包括現有的用戶和潛在的市場用戶）建議和要求而進行了功能和性能各方面的增強和提高。從 NBR5-3.0 遷移到 NBR5-5.0，這和從 NBR5-1.1 遷移到 NBR5-3.0 一樣，我們將在幾年內繼續支持 NBR5-3.0 的用戶使用。

當我們跟我們的客戶交流溝通並談及他們需要什麼的時候，他們經常提及到的有以下幾點：

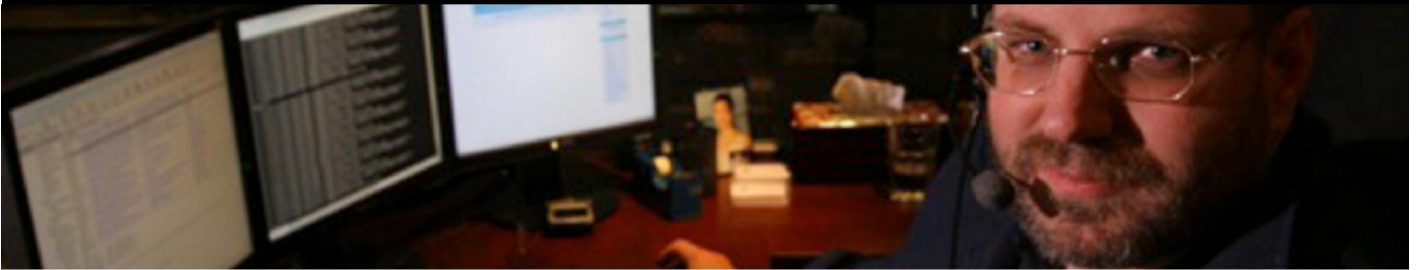
1. 透明度：您希望 Box 能夠部署起來更容易，並且能盡可能地對於現有的網路更具有透明性。
2. 性能表現：權衡取捨於掃描的全面性和網路輸送量表現，這二者而言，您可能會選擇最高的輸送量表現。

3. 入站過濾：您希望將垃圾 IP 阻斷在外面，保持內部 IP 乾淨。
4. 出站過濾與控制：您不僅僅希望對頻寬進行綜合性管理，還希望對用戶在行為上能進行控制（在應用層和協議層上）。
5. 可調節性：你希望根據不斷變化的工作負載能夠重新調節並平衡原有的解決方案。
6. 功能集成：您希望將閘道保護集成到您內部的系統（例如 DHCP，AD 域，LDAP 等等）。
7. 報告：您希望能有全面的控制和執行性報告。

在面對這些挑戰和不斷變化的網路威脅環境的時候，我們還希望：

1. IPv6：這將變得越來越重要，並且希望有一個明確的向 IPv6 的轉換方式，且能夠互相相容，以及 IPv4 和 IPv6 之間的 NAT 位址轉換。
2. SSL：您希望能對內部的 SSL 通道進行掃描，並且對在這些內部通道裡所發生的一切能進行控制。
3. 即時資訊：關於上面部分的第 4 點，出站過濾以及應用和協議的認證與授權，您希望能有效地對 IM，P2P，VOIP 等應用進行控制。

NBR5-5.0 就是旨在解決這些問題，並提供一個全面而整合化一的性能表現。充分利用雲端安全技術和 Box 安全技術的同時，我們還將為 Network Box 的下一個 5 年奠定堅實的基礎而不懈努力。



2011 年 1 月 新特性

在 2011 年 1 月 4 日的星期二這一天，Network Box 將發佈這次的 Patch Tuesday 的補丁包，各區域 NOC 將會在未來的 7 天內安排這些新的功能的發佈和更新工作。這個月的更新補丁包包括：

- V8 版本的卡巴斯基引擎的發佈。正如 2010 年 12 月刊的《In The Boxing Ring》中所探討的，新引擎和桌上出版以及伺服器版（Windows 和 Linux 上的）的卡巴斯基在使用上是完全一樣的，只是為在閘道上使用而做了一定的優化。不僅在性能表現上大受歡迎以及記憶體方面的提高之外，在啓發式檢測能力和沙箱技術的應用上也大有提高。

- 內容過濾策略引擎的優化，主要是關於 'everyone' 組的從屬關係。

- Box Office 合同管理系統也進行了改善，主要關於管理和顯示使用者的合同。

- 針對卡巴斯基 v8 引擎狀況監控的支援。

在多數情況下，以上的修改並不會影響到正在運行的服務，也不需要硬體重啓。但在某些情況下（取決於具體配置），可能需要重啓設備。必要時您當地的區域 NOC 將會與您取得聯繫。

如果您還需要要關於這些的更多的資訊，請與您當地的區域 NOC 取得聯繫。他們將會進行相關的諮詢和安排。

2011 年 1 月 提示

帕雷托法則（也被稱為 80/20 法則）表明，在大多數情況下，將近 80% 的影響來自於 20% 的因素。換句話說，您郵件的 80% 來自於您 20% 的用戶源，頻寬 80% 的使用率被您 20% 的用戶所佔用。

每個季度，Network Box 都會發佈一份關於 WEB 使用狀況的報告（2010 年第 4 季度的報告將會在下周發佈，同時 2010 年全年的報告也將一同發佈）。

當在查看頻寬使用情況的時候，也許您會主要關注於排前的幾個網站和用戶。2010 年的 Web 使用率報告表明，類似 YouTube 和 Facebook 等網站佔用了 Network Box 用戶的 Web 頻寬將近有 20%。單 Facebook 就有 10% 的 web URL 請求量，而 YouTube 則佔用了 13% 的頻寬。因此，針對這類網站的頻寬控制將會獲得最佳的效果。

在有威脅防護的情況下，帕雷托法則不幸地行不通了（沒有人會認為 80% 的保護就已經足夠了），但是針對於頻寬控制，帕雷托法則卻非常適用。

2011 年 1 月的提示就是，您有必要對您網路的那些數位進行關切。Network Box 的 my.network-box.com 裡面的報告，囊括了您所需要的所有的資料，不論發生了什麼，誰通過什麼佔用的頻寬。也許這很容易被其它個別事情所分心，那麼就應用帕雷托法則，將最大的罪魁禍首先揪出來吧。

Mark Webb-Johnson,
CTO, Network Box Corporation

2011 年 1 月份 資料表

關鍵指標	#	與上月 差值百分比
PUSH升級數	812	+2.4
特徵碼發佈數	409,998	-15.5
防火牆攔截數(每BOX)	753,356	-2.6
IDP 攔截數(每BOX)	110,749	-10.4
垃圾郵件數(每BOX)	26,943	-6.6
惡意軟體數(每BOX)	332	+19.0
URL攔截數(每BOX)	114,684	-21.2
URL訪問數(每BOX)	3,614,373	-17.2

月刊 工作人員

總編輯：
Mark Webb-Johnson

產品支援：
Michael Gazeley

Jason Law
Nick Jones

撰稿：
Network Box Australia
Network Box Hong Kong
Network Box UK

訂閱方式

寫電子郵件到以下郵箱位址：
Network Box Corporation
nbhq@network-box.com

或寫信到以下地址：
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 © 2011 Network Box Corporation Ltd.