來自 Network Box 首席技術官

Mark Webb-Johnson 的技術資訊

Welcome

歡迎閱讀 2012 年 1 月刊的《In The Boxing Ring》。在這一期當中，我會將重點放在對 2011 年的總結與 2012 年及以後的內容上的展望。

在第 2 頁，我們對 2011 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 2012 年我們的工作重點仍是即將推出的 NBRS-5.0，第一批客戶將在今年可以使用到。在即將到來的基礎平臺發佈以後，我們會跟進一系列的網路安全模組，直到達到（或超越）完全的 UTM＋功能。2012 年將是 NBRS-5.0 的一年。

NBRS-5.0 的開發已經是 Network Box 的一個重大工程計畫。重新思考每天給您帶來困擾的網路安全和控制問題的解決方案不是一個簡單的任務——特別是在這樣一個威脅快速變種的環境之下。我們很有信心你會對 NBRS-5.0 產生興趣，我們將盡可能地公佈更多有關這個產品和其元件安全模組的資訊。

在第 5 頁，是這個月對 NBRS-3.0 的發佈的新特性和新修復的補丁的詳情。在可預見的未來幾年，我們將繼續 NBRS-3.0 的開發和提高技術支援。這一頁將讓您瞭解到我們核心產品的動態資訊。

您可以通過郵箱（nbhq@network-box.com）與我們總部取得聯繫，或者到我們的辦公地點親臨參觀指導。您還可以通過以下幾個對外網站對我們保持關注：

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
2012 年 1 月

本 刊 概 要

2011 年的威脅指數

在 2011 年，Network Box 安全回應通過 PUSH 推送了 7,125 個更新，總共發佈了 3,880,267 個特徵碼（與 2010 年相比，分別下降 39.2%和上升 25.9%）。

大約每 8.1 秒鐘就有一個新的特徵碼產生。2011 年依然看到，雖然發佈的特徵碼數量是增加的，但每次更新的特徵碼數量卻是下降的。這反映出基於雲端的特徵碼系統所產生的效用（例如 Network Box 的 Sentinel Z-Scan 系統和 NBCP 的內容分類系統）。我們預計這種趨勢會繼續發展下去，因爲傳統特徵碼依然是對抗惡意軟體深度和廣度的最有效方法，而同時基於雲端的特徵碼卻是針對最新零日爆發最有效的解決方案。

在 2011 年，Network Box 平均攔截了 208,081 個電子郵件和 8,008 個惡意軟體（與 2010 年相比，分別下降 55.8%和上升 68.1%）。整體的垃圾郵件數量在縮減，這得益於大範圍的針對僵屍網路及其所有者（也即垃圾郵件的唯一最大來源）的阻擋操作。當然，垃圾郵件數量減少也或多或少得益於預先掃描過濾的增加使用（例如 RBL 限制了在信封階段和收信者地址的驗證）。這種信封掃描階段限制有效地抵擋了大量的垃圾郵件（全球範圍內，目前估計大約爲 35%），並且在信封掃描階段限制的郵件（垃圾郵件和惡意郵件）不顯示在我們的統計報告中“被限制疑爲垃圾郵件和惡意郵件資訊”的數位當中。2012 年，隨著 NBRS-5.0 的公佈，我們希望能夠更好地報告這部分內容。2010 年期間，Network Box 平均每 146 秒攔截一個垃圾郵件或惡意郵件。

2011 年，Network Box 使用防火牆技術平均阻止了 9,191,536 次攻擊，使用 IDP 技術平均阻止了 1,420,534 次攻擊（與 2010 年相比，分別上升了 13.1%和下降了 18.3%）。

我們繼續看到這樣的網路層面的攻擊只是“背景輻射”——這是連接到全球的互聯網所不可避免的。2011 年，從大量的垃圾郵件和惡意病毒構成的威脅環境到一個被鎖定有大量漏洞利用的目標，都在不斷地變化發展。一個令人擔憂的趨勢是相對較低影響服務拒絕，分散式服務拒絕，攻擊的增加——根據歷史記錄，我們已經看到這些使用數百兆比特的頻寬，但 2011 年在幾十兆一類的攻擊中，看到有大量這樣的攻擊。儘管較大的網站已經部署了有效的 DDOS 防禦系統，小型網站現在仍面對勒索和其他此類 DDOS 威脅。

Ipv4 位址空間現在已被嚴重污染，以至於 2010 年期間，Network Box 客戶中平均每 3 秒鐘，就能通過防火牆或者 IDP 攔截到一次網路層的探測攻擊。2011 年繼續看到 Network Box NBIDPS 系統的部署，以及我們作爲微軟的 MAPP 成員的好處所在，當然，這也是我們需要堅持不懈地努力來提高所提供的針對網路層 IPv4 的保護能力。但是，綜合的防火牆策略（特別是出站防火牆策略控制）依然是用於控制網路層威脅最有效的機制。

2011 年，Network Box 平均攔截了 1,663,284 個執行公司內容過濾政策的網站，全年中有 45,838,221 個 URLs 訪問網站（與 2010 年相比，分別上升了 45.5%和 12.8%）。

頻寬及其使用率尤其是網站的使用率在不斷地增長。隨著基於雲端的應用程式、社會性媒體以及移動手機的不斷發展，IT 部門在頻寬及其網站使用率方面的壓力也在不斷地增長。我們高興地看到，政策執行的阻止率繼續超過了 URL 訪問增長率——這意味著 IT 部門一直在採取利於主要頻寬消費群政策的措施。

Network Box 威脅統計	2010	2011	變化%比
PUSH 升級數	11,719	7,125	-39.2%
特徵碼發包數	3,083,018	3,880,267	+25.9%
防火牆攔截數(每 BOX)	8,129,674	9,191,536	+13.1%
IDP 攔截數(每 BOX)	1,738,576	1,420,534	-18.3%
垃圾郵件數(每 BOX)	471,304	208,081	-55.8%
惡意軟體數(每 BOX)	25,089	8,008	-68.1%
URL 攔截數(每 BOX)	1,143,378	1,663,284	+45.5%
URL 訪問數(每 BOX)	40,653,345	45,838,221	-12.8%

那麼，2012 年以後的計畫是什麼呢？

我們看到威脅狀況隨著用戶而變動。當越來越多的系統轉入到“雲端”，基於網站的攻擊（例如 XSS，SQL 注入，DDOS 等等）依然是很重要的一部分，Network Box 產品發佈（第一個版本將在 2012 年第一季度發佈）將會不斷爲解決這種不斷發展的威脅狀況而努力。

和往常一樣，每個月我們看到的威脅越來越多，發佈也越來越快。Network Box 將繼續加大技術投入（例如 Z—Scan）來加快保護發佈的週期，並且繼續充分利用我們與優秀客戶的關係，共同協作來尋求更加有效的防禦措施。

與 2010 年一樣，威脅狀況在不斷地變化發展，我們的產品也在不斷地發展以應對這些新的挑戰；進一步驗證了我們所提供的這樣一個不斷增強，全球管理，服務（而不是一個靜態產品）的思路的正確性。在 2012 年及以後，我們將毫無疑問地看到更多的類似情況。威脅狀況也將會不斷變化，Network Box（產品和服務）將繼續完善和發展，以成爲我們提供給客戶最有效的保護和防禦。

2011 年的增強功能

伴隨著卡巴斯基 v8 引擎版本的公佈，我們拉開了 2011 年的序幕。與原來卡巴斯基桌面使用的引擎和伺服器產品是一樣的，但優化了針對閘道的使用。不僅在性能和記憶體方面得到了提高，也在啓發式檢測功能和沙箱技術應用方面也大有增強。接著來我們就公佈了獲獎無數的專爲防病毒和防垃圾郵件而設計開發的 Z—Scan 零日保護系統。

縱觀全年，NBRS-3.0 已經公佈了超過 120 個增強功能，主要包括：

- Box Office 合同系統的增強，更好地爲顧客提供合同的可見性及其狀況
- 策略 URL 分類引擎的性能的改進
- 健康狀況監控的改進
- 全球監控系統（GMS）的改進
- 增加了對 DKIM 的支持
- 發佈了新的安全響應網站
- 擴展了在郵件掃描的過程中對壓縮包的解壓掃描功能
- PPTP 對 NTLM 的支持
- Box Office 和內部系統對 NBRS-5.0 的支援
- 接近 4 百萬新的保護特徵碼等等

2011 年期間，我們發佈了關於下一代的 Network Box 固件 NBRS-5.0 的一系列的共九個專題介紹。在 2012 年期間，當客戶真正使用上 NBRS-5.0 這個新產品的同時，我們將繼續做這方面的專題介紹。

2012 年及以後的展望

在 2012 年我們的工作重點仍是即將推出的 NBRS-5.0，第一批客戶將在今年可以使用到。在即將到來的基礎平臺發佈以後，我們會跟進一系列的網路安全模組，直到達到（或超越）完全的 UTM＋功能。2012 年將是 NBRS-5.0 的一年。

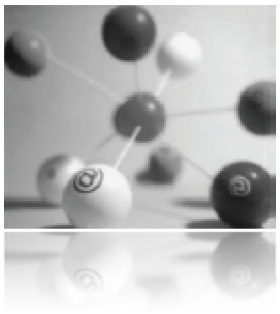
現在您應該知道，NBRS-5.0 既是一個平臺，也是一個產品。由大量的安全模組組成，建立在這個基礎平臺的基礎之上，NBRS-5.0 提供全面的保護，而又不犧牲個人安全模組的功能。

我們已經開始了對資源管理、監控系統、特徵碼的分發及 NBRS-5.0 的 NOC 操作基礎設施的部署工作。在第一季度結束之前，我們將開始第一個客戶安裝的部署——基於基礎平臺，加上 14 個安全性模組的第一個套裝。這些首次的部署將會提供一系列的產品：（a）基本功能，（b）NOC 配置和維護，（c）一個網路層的防火牆模組，（d）一個 WEB 應用的防火牆模組，（e）DOS 與 DDOS 保護模組，（f）負載均衡，（g）命令列管理介面，（h）視覺化 WEB 圖形管理介面，（i）IPv4 IPv6 SSL 翻譯功能。基本的 NBRS-5.0 產品中，至少在核心協議層會有認證 IPv6 Ready phase 2。在這第一季度發佈之後，您將看到 web 代理用戶端的發佈，在今年剩下的時間裡，將會陸續發佈郵件掃描模組、 VPN 相關模組和其它的功能模組。

NBRS 5.0 將支援所有當前的硬體 （S-M-E 系列的 Box 至今已發佈 5 年了），並且不要求任何硬體升級。但是，一般來說，我們必須指出的是額外的功能 （如果已啓用並使用） 可能需要額外的硬體支援。

我想藉此機會再次強調 NBRS-5.0 的四個主要設計目標： 透明性、整體性、可擴展性和模組化。

NBRS-5.0 的透明性



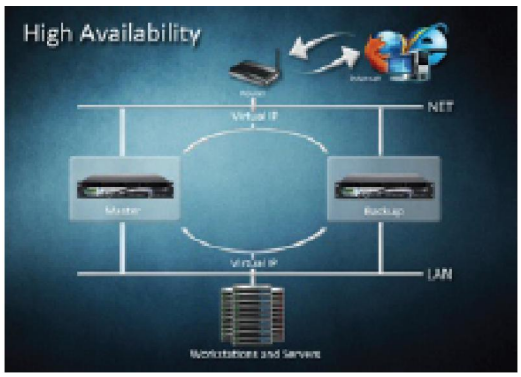
NBRS-5.0 應用了作爲哲學理論目標的透明性。在產品的設計上，將對現有網路沒有影響，且儘量不對網路進行改變。就像是一個水篩檢程式，可將其安裝在水流（好比是網路流量）的方向上，並且可以將污垢（好比是病毒、垃圾郵件等）過濾出來，而不會影響其它的水流。

Box 和區域 NOC 的連接也非常的簡單方便。NBRS-5.0 的 Box 連接到它們的管理 NOC（或者其它 Network Box 集群）採用的是 SSL 加密連接。那麼 NOC（以及管理的 Box）與客戶 box 之間的通信就是使用這些獨享的管理連接進行的。

NBRS-5.0 的整體性

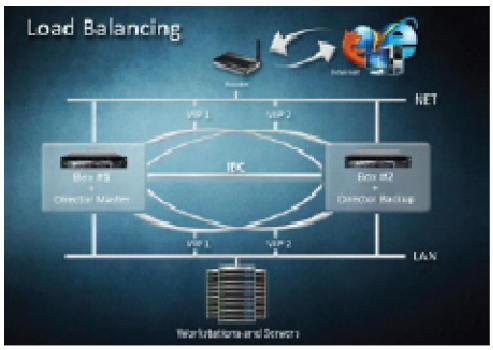
當前大多數的 UTM 系統設計採用的是分解法。他們將複雜的網路安全問題分解爲多個基本的部分（比如反病毒、反垃圾郵件、防火牆等），並且個性化地單獨提供這些解決方案。雖然稱之爲“統一”，而在實踐中，這並不能達到所謂“統一”的要求。除此之外，他們的都是在同一個設備上運行以及維護。簡單地說，管理的介面依然被那些模組分解得支離破碎。

NBRS-5.0 從最基本的開始設計，並提供了一個整體的安全管理平臺，然後對此平臺進行安全模組擴展，並使各個模組能整體地相容並協同工作。我們採用了幾個關鍵的技術（包括實體模型，統一日誌記錄和配置），用於提供一個單一的整體使用者介面。



NBRS-5.0 的可擴展性

前面所提到的關於水篩檢程式的用於介紹對網路流量沒有干擾的透明性的例子。容量規劃是一項持續的電腦系統問題，因爲流量和使用量狀況是在不斷增加變化的。可擴展性是完成這個目標的關鍵。



NBRS-5.0 處理可擴展性有兩種途徑：在 Box 裡面，採用支持多核心和多 CPU 的方式，而在 Box 外部，採用對集群的各 Box 間組成一個無縫的解決方案的支持。

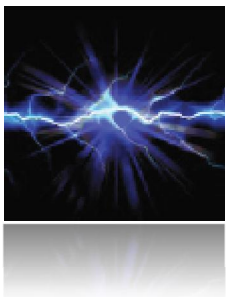
採用高可用性和負載均衡的方式，Box 集群可以集中進行管理，並且其流量可以通過此 Box（通過各 CPU 核心）以及通過集群中其它可用的 Box 進行均衡分流。統一日誌和配置系統可以進行無縫配置。只需要對一個參數進行修改，那就是“通過集群複製和部署”（無論是在辦公室，還是在全球分散的各組織）。群集配置和日誌的複製是自動的，可通過多種配置進行靈活部署。

NBRS-5.0 的模組化

NBRS-5.0 是設計爲一個基礎平臺，在此平臺上可以非常容易地安裝或者卸載不同的安全服務元件。此基礎平臺由一個內核、一個用戶層工具鏈、一個日誌系統和一個配置系統構成。本質上是一個極其複雜的路由器。

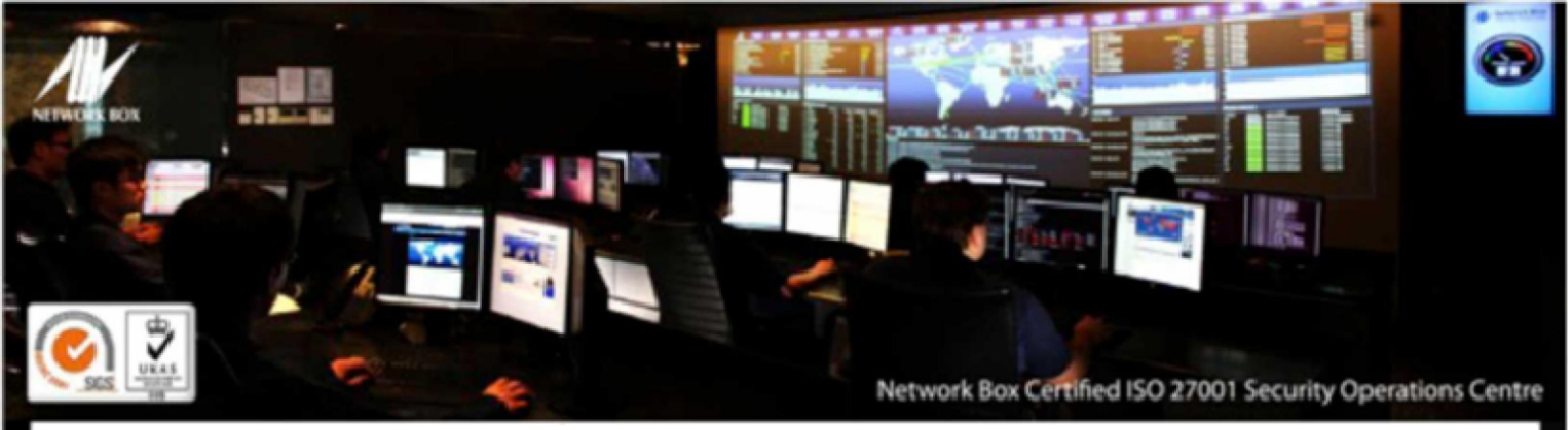
這種基礎平臺方式的優點是減少了固件的大小（包括記憶體佔用和硬碟佔用），對不需要的服務不進行安裝，按需以最簡化部署，最重要的是所提供的一切都是清晰明瞭的。

在同類產品中，我們的整體 UTM+解決方案不但是最好的，而且每個元件與其它產品相比較而言，都是有其獨樹一幟的地方。單獨而言，NBRS-5.0 版本的元件又是其中最好的，這些元件協同工作時，可以提供最有效的、最經濟並且最全面的網路安全系統。



總結

NBRS-5.0 的開發已經是 Network Box 的一個重大工程計畫。重新思考每天給您帶來困擾的網路安全和控制問題的解決方案不是一個簡單的任務——特別是在這樣一個威脅快速變種的環境之下。我們很有信心你會對 NBRS-5.0 產生興趣，我們將盡可能地公佈更多有關這個產品和其元件安全模組的資訊。



2012 年 1 月 新特性

在 2012 年 1 月 3 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 將會在此之後的 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：

·一系列內部 NOC 系統的功能增強；

· 關於在 Box Office 中從 LICENESES 遷移到 CONTRACTS 以及在客戶介面合同資訊的可視性的的內部修改；

· 在 Box Office 中對 NBRS-5.0 的進一步支持；

· 一系列針對 Box Office 和支援系統的（主要是內部）功能增強。

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。

Network Box 榮獲 Corporate Choice2011 年的兩項大獎

Network Box 從資訊技術專業雜誌上榮獲 Corporate Choice2011 年兩項大獎。一個是 Network Box 的 Z-Scan 零日防病毒系統；另一個是 S-Scan 的 WEB 內容過濾系統。頒獎儀式於 2011 年 12 月 14 日在香港海景嘉福洲際大酒店舉行。

Network Box 的新"Z-Scan"防病毒技術的重點是縮短獲得惡意軟體樣本，並產生反惡意軟體特徵碼所需的時間。“Z-Scan”的目的是把當前行業標準時限爲幾個小時減少到不到 1 分鐘。實際上，從實際檢驗中可以看到最快的時間爲僅僅 3 秒。

Network Box 的“S-Scan”引擎是一個高速的網路內容過濾系統，作用是說明企業阻止不良的 web 內容到達他們的使用者。在增加了“Google 安全流覽”類之後，就達到了十六個不良內容的類別，覆蓋可能會直接損害企業電腦系統（含惡意軟體的網站）的網站，也含有一些犯罪性質的（駭客網站），會導致犯罪的（色情或仇恨網站）或以其它方式傷害使用者（間諜軟體或欺詐）的網站。

獲取更多關於 2011 IT Pro Corporate Choice 的資訊，請流覽 http://choice.itpromag.com 。

2012 年 1 月份資料

關鍵指標	數據	與上月差比
PUSH 升級數	507	-1.17
特徵碼發包數	423,324	+13.4
防火牆攔截數(每 BOX)	826,753	-4.47
IDP 攔截數(每 BOX)	184,043	+55.3
垃圾郵件數(每 BOX)	15,130	-3.28
惡意軟體數(每 BOX)	322	-38.67
URL 攔截數(每 BOX)	158,708	-19.04
URL 訪問數(每 BOX)	3,836,156	-14.98

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

您可以些電子郵件到：
Network Box Corporation
nbhq@network-box.com
或者寫信到以下地址：
Network Box Corporation
16th Floor, Metro Loft,
38 Kwai Hei Street,
Kwai Chung, Hong Kong
Tel: +852 2736-2078
Fax: +852 2736-2778