

In The Boxing Ring

來自 Network Box 首席技術官

Mark Webb-Johnson 的技術資訊

Welcome

歡迎閱讀 2011 年 8 月刊的《In The Boxing Ring》。延續自 4 月份來本月刊的格式調整，我們自 6 月份以來也有了一個新的外觀排版，這是因為我們正繼續著手於 NBRS-5.0 發佈前的準備階段。在今年接下來的時間裡，每個月我們都將針對 NBRS-5.0 的一個話題展開探討（接下來的主要是關於 Network Box 的固件發佈的話題）。每月的提示板塊將會去除，取而代之的將是整個版面的關於現有產品 NBRS-3.0 的發佈更新的資訊。這個版頭將依然保留，主要概述本刊值得關注的新內容。

本月刊中，在第 2、3 頁，我們詳細介紹了 NBRS-5.0 的網路架構。透明性是 NBRS-5.0 的四個目標之中的第一位。設計以“無損害”的理念為指導，試圖盡可能少地對網路流量產生影響，同時繼續完善我們的安全功能，使其成爲一個適合於 NBRS-5.0 建立透明模式的網路架構。

NBRS-5.0 還包括了對橋接、路由以及網路位址轉譯部署模式的關鍵支援。這三種模式均能極好地對 IPv4 和 IPv6 網路通訊協定的支持。不僅僅只是對 IPv6 的支持，還能協助我們的客戶遷移到 IPv6 網路（協定轉換相結合的雙重堆疊）。

在第 4 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
2011 年 8 月

本刊概要

2-3.

NBRS-5.0 網路架構

我們詳細介紹了NBRS-5.0的網路架構。透明性是NBRS-5.0的四個目標之第一位。設計以“無損害”的理念為指導，試圖盡可能少地對網路流量產生影響，同時繼續完善我們的安全功能，使其成爲一個適合於NBRS-5.0建立透明模式的網路架構。

4.

Z-scan零日雲端保護

Network Box的零日技術現在已經也瞄準了垃圾郵件。屢獲殊榮的Z-Scan雲端保護就是用於抵禦零日病毒和垃圾郵件威脅的利器。

4.

2011年8月 新特性

這個月的補丁星期二將會對NBRS-3.0的新特性和補丁修復進行發佈。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。



NBR5-5.0 的網路架構

這個月關於 NBR5-5.0 的話題，我們將就關於其網路架構進行詳細的描述。透明性是 NBR5-5.0 的四個目標之中的第一位。設計以“無損害”的理念為指導，試圖盡可能少地對網路流量產生影響，同時繼續完善我們的安全功能，使其成爲一個適合於 NBR5-5.0 建立透明模式的網路架構。

NBR5-5.0 網路基礎平臺

NBR5-5.0 還包括了對橋接、路由以及網路位址轉譯部署模式的關鍵支援。這三種模式均能極好地對 IPv4 和 IPv6 網路通訊協定的支持。

每種模式都可以單獨操作，或者在更複雜的網路中組合配置。例如，透明橋接網路可以同時使用 NAT，使某些流量可以復位向到安全的 DMZ 區域，再通過路由將流量傳輸過去。

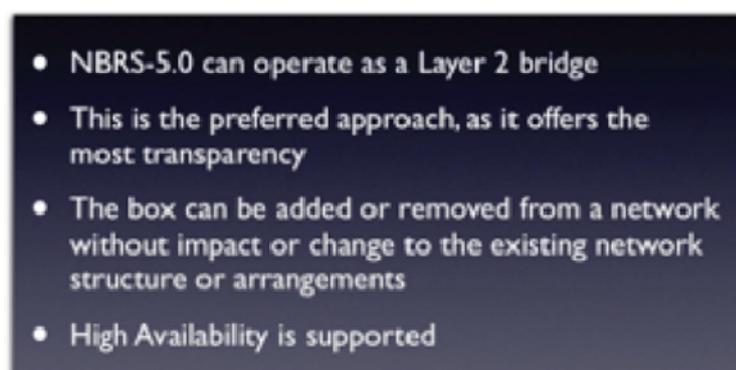
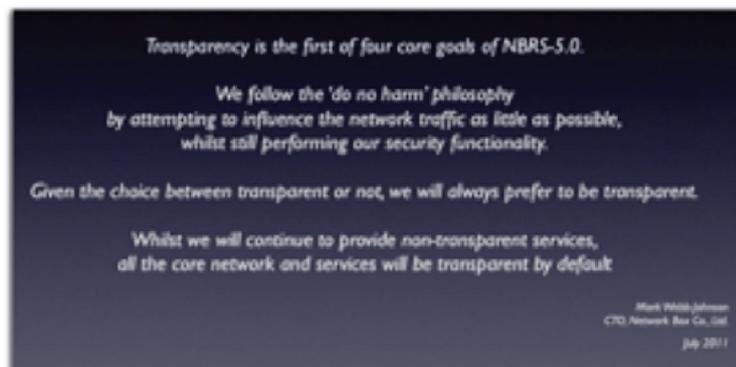
安全模組擴展提供了以下基本的網路功能：

- 虛擬私人網路；
- 防火牆功能；
- 應用識別；
- QoS（服務品質）；
- 高可用性；
- 代理和應用層過濾/控制；
- 入侵偵測和預防；
- 其它功能。

NBR5-5.0 的橋接器模式

橋接器模式是 NBR5-5.0 Box 的首選部署模式，因爲這種模式最透明。

要部署橋接器模式，至少需要 2 個物理介面。猶如是一個 HUB 集線器那樣，流量從其中一個介面流入，並根據安全性原則進行透明的過濾，然後再傳輸到其它的介面上。而實際上，每個 Box 均含有 2 個以上的介面，這就意味著，可以配置多個橋接器。



NBRS-5.0 的路由模式

NBRS-5.0 可以支援路由模式，並且在基於目的地址以及其它更複雜的策略規則能夠很好地規範流量。

路由表保存了很多的路由，而策略規則則可以對特殊的流量選擇合適的路由表選擇路由。還設有一個路由緩存區，用於優化路由選擇的性能。

我們可以靜態地或者動態地對這些路由表進行路由添加，而且也可以支持各種類型的高層路由式通訊協定。

NBRS-5.0 的 NAT 模式

NBRS-5.0 可以支援 IPv4 下的 NAT 模式。NAT (Network Address Translation, 網路位址轉譯) 最初是用於延長 IPv4 的使用期限，但是其在服務遷移或者重定向的情況下也是非常有用的。Network Box 可以同時支援源位址轉換 (多台設備共用同一個公網源位址) 和目的地址轉換 (請求的目的地址被復位向到另一個位址)。還可以支援雙向位址映射。

由於 IPv4 和 IPv6 兩種協議之間的巨大差異，因此這兩種協議之間在全球互聯網上的簡單 NAT 位址轉換是不可能的。然而，NBRS - 5.0 提供了這種轉換服務，以協助這兩個協議之間的共存和遷移。通過使用路由器層級的技術，結合高層級的代理和服務，NBRS - 5.0 將可以支援 IPv4 和 IPv6 之間的雙向位址轉換。

我們還提供了靈活的連接選項，即便客戶的網路服務提供商不能提供直接的 IPv6 連接，我們也可以為他們建立 IPv6 在 IPv4 上的 IPv6 通道連接。

雖然 NBRS-3.0 對 IPv6 已經有了基本的支持，但是 NBRS-5.0 則對 IPv6 進行了全面的支援，並且更重要的是，還可以支援 IPv4 與 IPv6 之間的資料傳輸。其目的是協助我們的客戶解決關於遷移到 IPv6 網路的問題，而不是僅僅作為一個在網路上支援 IPv6 的設備。

小結

NBRS-5.0 提供了一個既支援當前的 IPv4 互聯網的網路架構，同時也支持未來的 IPv6 的網路架構。不僅僅只是為了支持 IPv6，更重要的是，協助我們的客戶解決關於遷移到 IPv6 網路的問題 (協定轉換相結合的雙重堆疊)。

- Static and Dynamic Routing Tables
- Routes can be added either statically or dynamically
- High-level routing protocols supported:
 - RIP v1 and v2 for IPv4
 - RIPng for IPv6
 - OSPFv2 for IPv4
 - OSPFv3 for IPv6
 - BGP for both IPv4 and IPv6
 - and others to follow...

- For IPv6 NBRS-5.0 also offers Translation
- Using router-level technologies, combined with high-level proxies and services, NBRS-5.0 will support bi-directional translation between IPv4 and IPv6
- Examples:
 - IPv4 DMZ, IPv4 and IPv6 dual-stack Internet
 - IPv4 LAN and DMZ, IPv6 Internet
 - IPv6 LAN and DMZ, IPv4 Internet
 - IPv4 LAN and DMZ, IPv4 Internet with connectivity via IPv6-in-IPv4 tunnel to provider



Network Box Certified ISO 27001 Security Operations Centre

2011年8月 新特性



在 2011 年 8 月 2 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：

- 增加了郵件掃描系統對包含 Microsoft Excel 附件的拆包功能的改善。
 - 增加了郵件掃描系統對包含 Microsoft Word 附件的拆包功能的改善。
 - 增加了反垃圾郵件系統對最新的 Word 和 Excel 的拆包器的支持。
 - 增加了資料洩漏防禦系統對最新的 Word 和 Excel 的拆包器的支持。
 - 增加了 Sentinel Z-Scan 關於反垃圾郵件的描述內容。
- 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。



Z-Scan 零日雲端防護

Network Box 已經對 Z-Scan 的零日反病毒系統進行了增強，現在也已經可以對垃圾郵件進行病毒掃描了。同樣屢獲殊榮的零日反惡意軟體技術也正在參與到針對垃圾郵件的永無止境的鬥爭當中。

這種新的 Z-Scan 反垃圾郵件引擎為 Network Box 提供了總數為 25 個的反垃圾郵件引擎，並提供了超過 1960 萬的反垃圾郵件的特徵碼。

Z-Scan 的零日防護

Z-Scan 防垃圾郵件是一種適用於 Network Box 的屢獲殊榮的零日防病毒解決方案。利用最先進的雲端技術，Z-Scan 對零日病毒所作出的反應速度比傳統的防病毒系統要快將近 4200 倍。通過在同一個反垃圾郵件的系統環境中進行對比，Network Box 對某些類型垃圾郵件的零日病毒爆發所作出的反應，僅需要幾秒鐘。

Z-Scan 系統的威脅資訊的獲得是來源於 20 萬個以上的陷阱，這些陷阱均可以即時不間斷地對病毒資訊進行捕獲。這些 Z-Scan 陷阱包括垃圾郵件陷阱、病毒陷阱、內部規則、客戶規則、郵件統計、HTTP 統計以及嫌疑樣本。Z-Scan 的陷阱網路可以一天 24 小時，每週 7 天，每年 365 天持續工作。

2011年8月份資料

月刊工作人員

訂閱方式

關鍵指標	數據	與上月差比
PUSH 升級數	568	-8.7
特徵碼發包數	373,197	+36.5
防火牆攔截數(每 BOX)	781,004	-2.5
IDP 攔截數(每 BOX)	108,595	+4.7
垃圾郵件數(每 BOX)	14,081	-19.2
惡意軟體數(每 BOX)	346	-15.0
URL 攔截數(每 BOX)	125,707	-15.1
URL 訪問數(每 BOX)	3,571,601	-12.9

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

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

Copyright © 2011 Network Box Corporation Ltd.