

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 6 月刊的《In The Boxing Ring》。延續自 4 月份來本月刊的格式變化，我們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，主要概述本刊的新內容。

本月刊中，在第 2、3 頁，我們詳細介紹了 NBRS-5.0 的基礎平臺。這個平臺包含了一個內核、一個使用者空間工具鏈、配置和日誌系統。從本質上說，可以說是一個極其複雜的路由器。作為一個平臺，我們將我們的安全性群組件和高級功能都在此平臺的基礎上建立的。

NBRS-5.0 平臺為我們的安全產品提供了一個很好的基礎，但它本身並不是一個安全產品。建立於此基礎之上，高精細的安全性群組件將由其自身提供各種安全功能。

通過將各個安全模組集中專注於設計好的工作任務，以及將各安全模組協同工作的設計方法（利用所提供的設施優勢），我們可以對產品進行最大限度的優化。WEB 用戶端與 WEB 伺服器的保護就是一個這樣的例子。雖然您可以將此看成為簡單的 HTTP 保護，但是兩端對此的要求卻是非常迥異的，並且對特殊問題也提供了特殊防護的優化，對所部署的防護也提供了極大的好處（同時也減少了負面的影響）。

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

本刊概要

2 - 3.

NBRS-5.0 基礎平臺

我們詳細介紹了NBRS-5.0的基礎平臺。這個平臺包含了一個內核、一個使用者空間工具鏈、配置和日誌系統。從本質上說，可以說是一個極其複雜的路由器。作為一個平臺，我們將我們的安全性群組件和高級功能都在此平臺的基礎上建立的。

4.

美國TOLLY GROUP實驗室

Tolly Group 實驗室 測試 驗證 Network Box對POP3, HTTP及SMTP 中的現有病毒攔截有效率達到100%。

4.

2011年6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 基礎平臺

這個月就關於 NBR5-5.0 的話題，我們將講一講關於“基礎平臺”在設計理念上的一些資訊，以及我們是如何使用它來提供一個模組化的，但卻是一個整體的安全平臺的。

首先，讓我們來回答一下這個問題，“什麼是基礎平臺？”。這個平臺包含了一個內核、一個使用者空間工具鏈、配置和日誌系統。從本質上說，可以說是一個極其複雜的路由器。作為一個平臺，我們將我們的安全性組件和高級功能都在此平臺的基礎上建立的。

NBR5-5.0 的內核

內核是 Linux 2.6 的一個定制版本，主要負責資料處理、記憶體及 I/O 管理，尤其是網路 I/O 管理。由於可以在橋接器、路由和 NAT 多種模式下結合作，內核主要負責將 Box 裡面的網路流量在各個介面之間進行傳輸，以及將這些流量內部引導到相應的安全模組，再應用安全和組織策略進行過濾。需要應用到內核（鑒於高性能）及使用者空間（鑒於深入掃描）各種方法相結合。

正如 NBR5-3.0 一樣，可以支援先進的基於策略的路由的配置，也支援靜態和動態的路由式通訊協定（包括 IPv4 和 IPv6），支援多連接，多家庭，多路由配置，還使用了基於內核的路由緩存方法來進行性能的優化。

NBR5-5.0 的用戶空間工具鏈

使用者空間工具鏈主要用於基本的系統操作，以及負責系統的啟動和關閉。通過一個並行的控制系統，儘量使得並行系統的各個部分的初始化時間最小化（使用多 CPU 內核和磁片子系統）。

- Native IPv4 and IPv6 Support
- Fully standards-compliant IPv4 and IPv6 stacks
- Uses a dual stack approach
- NAT support within IPv4
- Translation capability for IPv4 <-> IPv6 traffic
- Full IPv6 support at all layers

- A configuration system
- A single unified configuration store, including:
 - Revision Control
 - Auditing
 - Clustered Replication
 - Bi-Directional Sync

NBR5-5.0 的配置管理系統

在 2011 年 5 月刊的 In The Boxing Ring 裡面，我們也用了一些篇幅來說明伴隨 NBR5-5.0 而來的配置管理系統。在過去的十年裡，我們是如何從提供託管服務中吸取了所有客戶的回饋，並且將之建立起來了一個機制，以使得能夠滿足我們客戶的需求（以及他們安全審計師在監管和法規上的監管的要求）。結合完整的存取控制和審計，使得單個 Box 和 Box 集群的配置均得以安全保護。

通過將配置資訊統一到一個單一的存儲庫，以及提供版本修改控制的支援，資料審計，集群複製以及雙向同步，我們已經將 NBR5-3.0 中在 NOC

所能做的一切延伸到了 BOX 上。

NBR5-5.0 的日誌管理系統

在 NBR5-5.0 中，日誌管理系統被稱之為 NBSYSLOG。它是一個統一的日誌系統，與 SYSLOG 標準完全相容（但也有所擴展）。在其內核，提供了一個高優化的開關，使其通過一個傳送代理的選擇能夠接收，過濾，交換以及發送/保存日誌資訊。採用了事務型的設計思路，是為了可靠地按順序傳送日誌資訊，並且能從連接或存儲錯誤中自動恢復過來。

我們提供了大量的傳送代理的選擇，包括：SYSLOG，NBSYSLOG（通過集群 Box 之間的 NBSYNC 協定），日誌檔輸出，資料庫輸出，資料匯出報告，以及郵件預警。

用於記錄日誌的資料庫是事務性的 ACID（原子性 Atomicity、一致性 Consistency、隔離性 Isolation、持久性 Durability）的相容資料庫，提供行級鎖定和併發控制。這使我們能夠提供一個高優化的事務型日誌存儲模組，即時匯總分析功能，以及一個很重要的功能，那就是繼續將新的日誌條目和匯總資訊插入到資料庫，並且分析報告也在同時間進行生成。一種基於物件的面向資訊的方法，加上豐富的資訊結構，就可以大大減少所需包含的資料片消息的數量。

- The NBR5-5.0 logging system is called NBSYSLOG
- It is a single unified logging system, including:
 - Rich, complete, logging messages
 - A switch to distribute these messages
 - Delivery agents to transmit these messages
 - A database store to permanently record logs

NBRS-5.0 建立於基礎平臺的安全模組

NBRS-5.0 平臺為我們的安全產品提供了一個很好的基礎平臺，但它本身並不是一個安全產品。而提供各種安全功能的是建立於此基礎平臺之上，高精細的各種安全性群組件。

通過將各個安全模組集中專注於已設計好的工作任務，以及將各安全模組協同工作的設計方法（利用所提供的各種工具設施的優勢），我們可以對產品進行最大限度的優化。WEB 用戶端與 WEB 伺服器的保護就是一個這樣的例子。雖然您可以將此看成為簡單的 HTTP 保護，但是兩端對此的要求卻是非常迥異的，並且對特殊問題也提供了特殊防護的優化，對所部署的防護也提供了極大的好處（同時也減少了負面的影響）。

升級服務包還將繼續為您提供，作為客戶的您只需要在“服務功能表選項”與“特定服務套餐”之間做出選擇即可。

我們計畫發佈一系列的安全產品，且所有產品均建立于同一個安全基礎平臺之上，並且讓其均能進行無縫協同工作。不論是在同一設備上，或者是在一個 Box 集群上，這些產品模組根據性能要求和結構要求均能無縫地協同工作。

安全模組新特徵表

雖然包含可用的安全模組、價格、服務包以及可用性的完整清單還需要等到今年的晚些時候才能夠發佈出來，但是在下表中，也許可以給到您一些關於我們所提供的各個模組的相關資訊，以及為何將它們設計成為輕量型而獨立的，還可以跨作業系統的各種模組，使其能夠制定一個高度定制性的安全解決方案。

NBRS-5.0 的安全模組（初步資訊，將有變更）

路由功能（IPv4，IPv6，NAT，橋接器，路由模式）	FTP 用戶端的掃描、策略與控制
高可用性	FTP 服務端的掃描、策略與控制
負載均衡	郵件的掃描、策略與控制
集群	Web 用戶端的掃描、策略與控制
服務品質（QoS）	Web 伺服器的掃描、策略與控制
應用識別和策略控制	IM 用戶端的掃描、策略與控制
防火牆（包括 IPv4 和 IPv6）	網路加速與緩存
入侵偵測系統	內部 Web 介面
入侵防禦系統（主動模式和內聯模式）	加密服務
虛擬私人網路（VPN）	PCI 相容
Web 伺服器應用防火牆	數據洩漏防禦
反垃圾郵件	網路漏洞掃描
反病毒	NOC 服務
Web 內容過濾	以及更多.....

- The NBRS-5.0 Base
 - Provides a foundation for our security products
 - Is built using secure coding principles
 - Is maintain using secure practices
 - But is not a security product itself

- Service Packages (FW+, CF+, AV+, UTM+)
 - Will continue to be offered
 - But will now be augmented with a selection of optional security modules
 - This will allow us to expand the product (building on the base in a structured, expandable manner)
 - It will also allow customers to choose 'à la carte' as well as the current 'buffet' offering

Modularity is often the result of a reductionist approach to systems development. However, modular and holistic approaches are not mutually exclusive.

NBRS-5.0 is the first Holistic Security Management Platform. Modular, but integrated in a way never before seen, to provide a single holistic view both of the network and of the entities using it.

Mark Webb-Johnson
CTO, Network Box Co., Ltd.
May 2011



Network Box Certified ISO 27001 Security Operations Centre

2011年6月新特性

在2011年6月7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：

將繼續卡斯基的支援可配置啓發式的反病毒掃描引擎的階段性的部署。這一項的支持已經在內部進行了一段時間的測試，我們將此版本繼續對所有客戶發佈，這項新功能可配置的啓發式支援允許在卡斯基反病毒引擎內設置啓發式等級，針對單個 Box，可以設置為關閉，初級，中級或高級（可單獨對郵件和 HTTP 掃描進行設置）。

- 針對健康狀況監控系統的局部增強。
- 針對 Intel 乙太網晶片組增強了內核級乙太網驅動。
- 對 my.network-box.com 管理介面的各種增強以及小修復。

在大多數情況下，以上這些改變不會影響到正在運行的服務或不需對 Box 重啓。然而，在一些情況中（由於對 Box 進行了配置），可能需要重啓 Box。如果需重啓 Box，當地 NOC 將會聯繫你去安排此事。

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。

Facebook 上的安全回應

美國 Tolly Group 實驗室聯合德國知名的 IT 安全測試實驗室 AV-Test GmbH 剛發佈了一個報告，報告顯示 Network Box 能 100%有效阻擋 POP3、HTTP 和 SMTP 上的病毒。

作為全球知名的網路安保管理服務公司的其中一員，Network Box 一直被認為是採用了最好的方法阻擋駭客、惡意程式和不良網站內容，是使用多引擎掃描，再以即時的 PUSH 更新和即時的雲計算技術去加強配合。

以 Network Box 屢獲殊榮的 Z-Scan 防零日病毒系統為例，透過尖端的雲端技術，在發現新病毒後 3 秒內能有效地被阻擋。

然而上面是談到了 Network Box 強大功能，下面是一個有力的證明。

Network Box 最近委託 Tolly Group（美國），聯同 AV-Test（德國）一起測試 Network Box 的反病毒功能模組，使用這個模組來查殺 WildList 病毒庫中最新病毒變種的樣本，包括：病毒、蠕蟲、root kits 和後門程式，這些惡意檔都通過了 HTTP、POP3 和 SMTP 協議測試。此次測試已經證明 Network Box 能 100%有效的清除這些病毒。



更多內容請參考：

http://www.network-box.com/tolly_nb_malware_report_2011

2011年6月份數據

關鍵指標	數據	與上月差比 (%)
PUSH 升級數	612	-3.3
特徵碼發包數	163,935	-31.7
防火牆攔截數(每 BOX)	767,402	-1.0
IDP 攔截數(每 BOX)	106,661	-24.9
垃圾郵件數(每 BOX)	16,183	-17.7
惡意軟體數(每 BOX)	687	-26.3
URL 攔截數(每 BOX)	134,081	+15.9
URL 訪問數(每 BOX)	3,985,257	+4.7

月刊 工作成員

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

Copyright © 2011 Network Box Corporation Ltd.