來自 Network Box 首席技術官

Mark Webb-Johnson 的技術資訊

Welcome

歡迎閱讀 2011 年 7 月刊的《In The Boxing Ring》。延續自 4 月份來本月刊的格式變化，自從 6 月以來我們也有了一個新的外觀排版，這是因爲我們正繼續著手於 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）。每月的提示版塊將會去除，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 的配置架構。我們也談到 NBRS-5.0 部署的 6 個關鍵點。

我們的目標是在盡可能少的影響現有網路的情況下部署所有的安全服務。和現有網路並存，爲現有的流量提供一個安全的過濾。NBRS-5.0 達到了透明代理和安全服務的目標。NBRS-5.0 配置架構在透明方式下允許我們去部署，監控和管理我們的安全過濾設備。

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 7 月

本 刊 概 要

NBRS-5.0 的配置架構

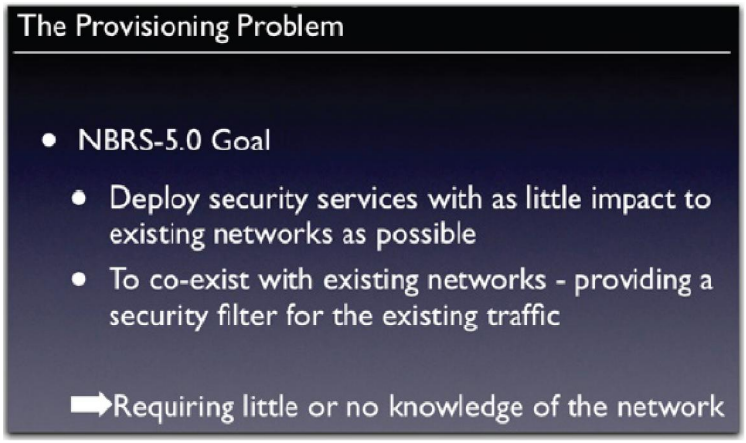
這個月關於 NBRS-5.0 的主題是，我們將介紹配置架構的相關資訊。我們的目標是在盡可能少的影響現有網路的情況下部署所有的安全服務。和現有網路並存，爲現有的流量提供一個安全的過濾。NBRS-5.0 達到了透明代理和安全服務的目標。這種配置架構允許我們在透明模式下，部署、監控和管理我們的安全過濾設備。

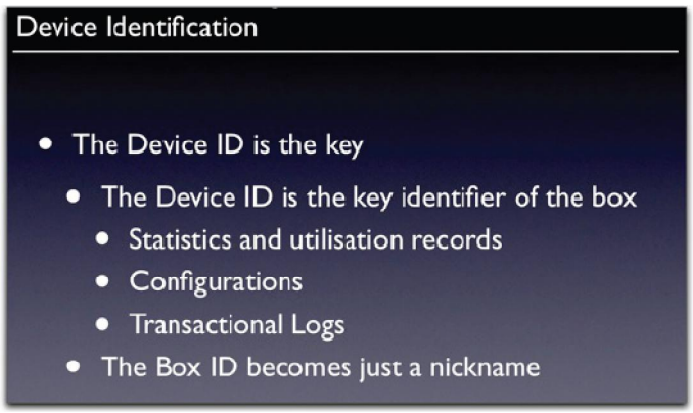
NBRS-3.0 與 NBRS-5.0 部署對比

在 NBRS-3.0 平臺下，BOX 通過 NOC 去配置。BOX 發送它的外網介面 IP 位址給 NOC，NOC 應答 BOX 下達更新指令。這需要詳細的瞭解客戶網路和具有網路許可權來允許 NOC 請求 BOX。通過各種埠和位址在兩個反向上建立大量的連接，在 BOX 和 NOC 之間的任何安全設備需要被配置來允許這些流量。

NBRS-5.0 的目標是部署盡可能少的影響客戶網路的安全服務， 在不需要瞭解客戶網路架構的情況下，和現有網路並存，爲現有的流量提供一個安全的過濾。

這需要一個新的途徑去部署我們的 BOX 和保持它們 7x24 小時的更新和監控。





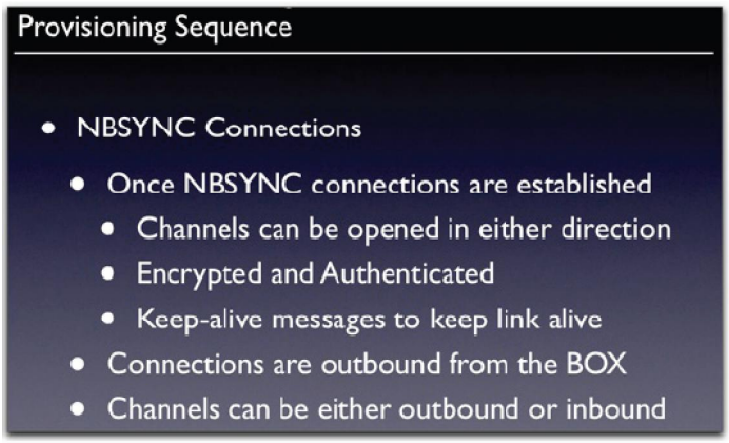
設備角色與 ID

NBRS-3.0 使用 BOXID 作爲其主要的標識。現在，在 NBRS-5.0 平臺上，我們使用了一個設備角色的新概念（類似於設備 ID），每一個設備角色都有一個伴隨其全部使用生命的唯一設備 ID。BOXID 是可以改變的，但設備 ID 卻是固定不變的且是一個全球唯一標識，這樣的話創建起來也不會受到集中分配服務的影響。當硬體被替換時，原設備的 ID 保持不變（在不同設備之間遷移時）且始終取決於設備本身的特殊用途。

在 NBRS-5.0 平臺下，設備 ID 是 BOX 的主要識別字。它是對所有的統計和使用率記錄的關鍵字，也包括配置和事務日誌在內。而 BOXID 也變成爲一個別名。

部署過程

有一個系統叫做 NBSYNC，它是建立 BOX 之間通信的閘道。它在設備之間通過 IP 傳輸來構建鏈路，類似如動態 VPN，用 SSL 作爲 ZF 技術去傳遞安全認證和加密的通信通道。NBSYNC 運行在每一個 NBRS-5.0 的 Network Box 上，以及集中服務（例如統計，全球監控系統和 NOC）。NBSYNC 被用於 BOX 與 BOX（例如：集群）和 BOX 與 NOC 的通信，並提供了一個單一的安全通信鏈路，在這個鏈路上每一個單獨的通信通道均可被雙向建立。



配置工作是通過在 BOX 指令 NBSYNC 上的一個用戶端去連接到一個全球可用的配置和註冊服務。這是一個從 BOX 到 Network Box HQ 的出站請求，這種請求可以嘗試在很多的埠和很多的後備目的地址，因此它能嘗試解決任何上游過濾或阻塞。一旦一個連接成功，BOX 提供它的設備 ID 和認證給配置和註冊服務，配置和註冊服務回應給 Box 後續連接列表,這些連接清單包括詳細的後續服務。這清單被緩存在 BOX 本地（用於網路加速，以及避免配置和註冊服務不可達的情況。）

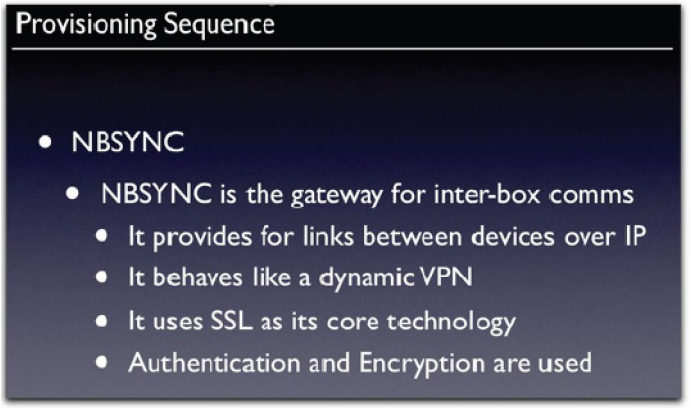
可提供的後續服務包括：

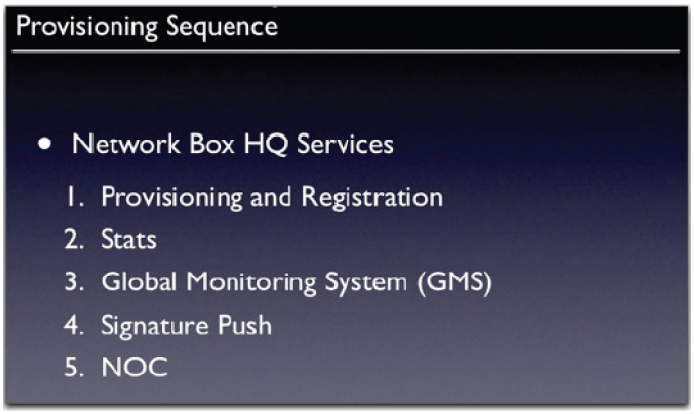
1.統計和利用率服務（一個可選的服務對於從 BOX 接收統計，存儲每個 BOX、每個行業和全球範圍允許匿名趨勢報告）。

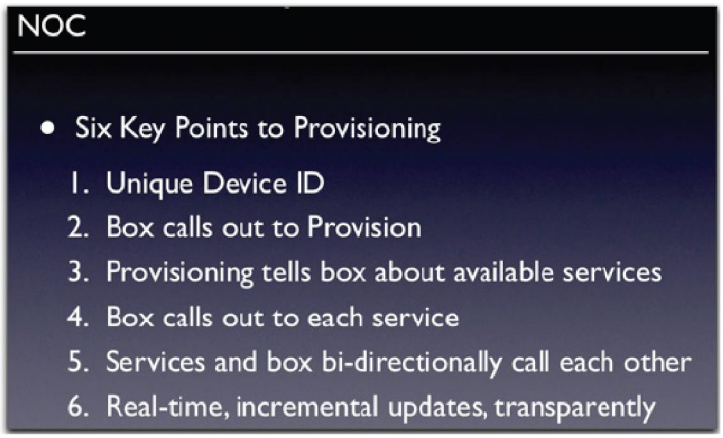
2.全球監控系統（即時的從 BOX 收到健康資訊，允許快速通告 BOX 連接問題無需 ICMP 或 SNMP 偵測）。

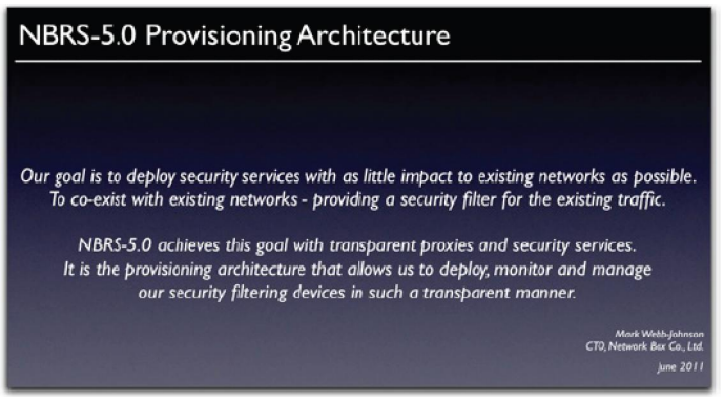
3.特徵碼 PUSH（一個全球分發網路的特徵碼 PUSH 伺服器傳遞簽名的特徵碼包和即時的週期性更新，允許按需重傳這些包）。

4.NOC（配置雙向同步改變，提供 BOX 配置的備份和允許從一個或多個允許的 NOC 對 BOX 的遠端維護）









安全考慮

NBSYNC 協定是建立在 SSL 安全標準之上。這意味著它繼承了同樣的驗證模式，以及加密和認證功能，向大多數的安全系統一樣。這項核心技術已經獲得了許多嚴格的安全審計和評估，被認爲是安全的。此系統當前自身用了 4096 位 RSA 驗證和 256 位 AES 加密。

結論

有 6 個關鍵點去部署 NBRS-5.0：

1.每個設備角色分配一個唯一設備 ID（不再依賴 Boxid）

2.每個 box 請求配置服務

3.配置服務回應 box 可用的服務

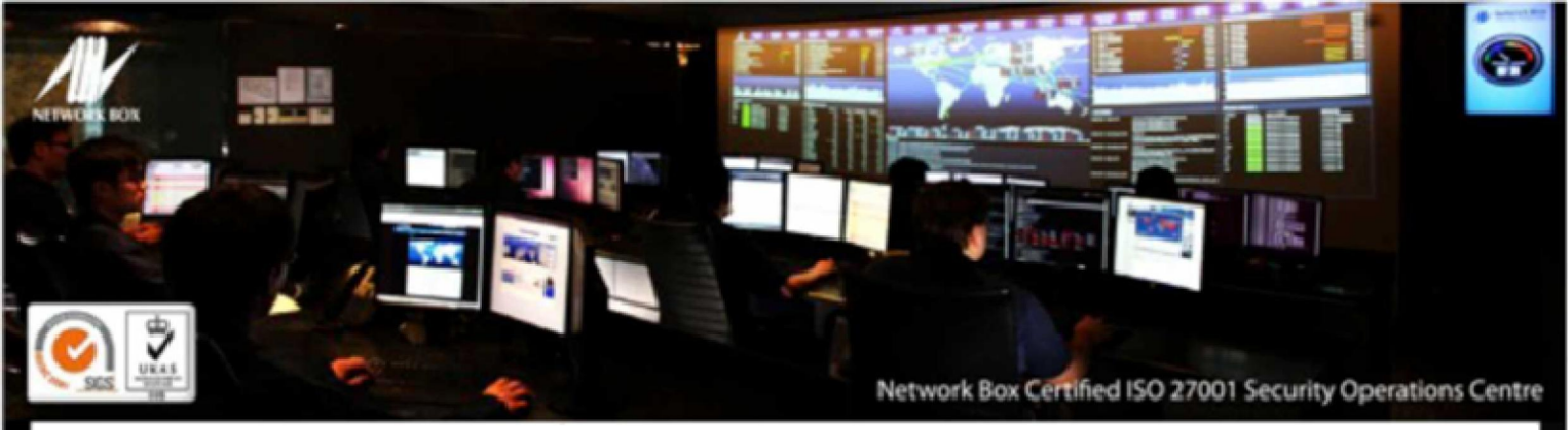
4.box 請求每個可用服務

5.服務和 box 雙向互連

6.即時，增量更新，透明傳遞

通過使用 NBSYNC 提供一個單向出站（BOX 到 NOC）通信鏈路，然而建立在這個單向鏈路裡的後續通信是雙向的，這個通信極其簡單（與 NBRS-3.0 相比）。這使得 Box 一直得到配置，更新，監控和維護而不需知道 Box 的 IP 位址以及不需要改變網路策略去增加從 NOC 到 Box 的存取權限。

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 7 月 新特性

在 2011 年 7 月 5 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：

·統計摘要中自訂威脅名稱的支持 (改進了 response.network-box.com 網站的內容、統計和 Network Box 安全回應工程師的趨勢分析)。

·針對健康狀況監控系統的局部增強。

·對 my.network-box.com 管理介面的各種增強以及小修復。

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。

Z-Scan 反病毒引擎

Z-Scan 反病毒系統關注于開發和發佈它自身的特徵碼去查殺剛面世的緊急病毒，而非等待反病毒協會發佈的新特徵碼，反病毒協會發佈新特徵碼經常需要將近一天的時間。

該引擎的運作是通過不斷地分析所有威脅資訊，這些資訊是即時從超過 200000 多個在雲中的陷阱獲得，該引擎 7x24 小時防護病毒攻擊，這些病毒包括：垃圾郵件、病毒、郵件統計、http 統計、可疑樣本。一年 365 天、一周 7 天、一天 24 小時的得到防護。

Z-Scan 是一種新的方法，它能查殺不少於 40000 種新的'零日'病毒，這些病毒可能在 internet 的特定時間爆發。在大多數情況下僅有 3 秒的反應時間，而傳統的殺毒軟體廠商保護他們的客戶時需要發 3 小時到 12 小時、或者甚至 20 小時才能做出反應，這是相差甚遠的。

Network Box Z-Scan 反病毒引擎在 2011 年 6 月 30 日獲得 HKAI 200－技術成就大獎。這一尖端技術專門設計用於加強世界各地 Network Box 的保護等級。Z-Scan 正在保護世界各地的跨國公司，組織，和政府部門，僅在美國就超過 150 個銀行和信用社。

香港工商業獎 2011 HONG KONG AWARDS FOR INDUSTRIES
科技成就大獎 TECHNOLOGICAL ACHIEVEMENT GRAND AWARD

2011 年 7 月份資料

關鍵指標	數據	與上月差比
PUSH 升級數	622	+1.6
特徵碼發包數	273,323	+66.7
防火牆攔截數(每 BOX)	801,198	+4.4
IDP 攔截數(每 BOX)	103,696	-2.9
垃圾郵件數(每 BOX)	17,434	+7.7
惡意軟體數(每 BOX)	407	-40.7
URL 攔截數(每 BOX)	148,005	+10.4
URL 訪問數(每 BOX)	4,098,720	+2.8

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