來自 Network Box 首席技術官

Mark Webb-Johnson 的技術資訊

Welcome

歡迎閱讀 2011 年 9 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，我們詳細介紹了防火牆功能。防火牆是任何 UTM+設備的核心部分，主要是負責企業和組織的策略規則在網路層的實現。NBRS-5.0 的防火牆功能是獨立的，但是與其它的安全模組（例如，應用識別、QoS 服務品質以及路由等）卻又集成於一個整體。

NBRS-5.0 的防火牆功能在內核採用了一種自動載入機制，使防火牆規則能在即時運行的情況下瞬間進行切換（不會造成任何網路連接的斷開）。存取控制清單和規則是 NBRS-5.0 的兩個關鍵特徵，當然這也不僅僅局限於防火牆功能本身，而且還貫穿並整合到整個系統的防火牆所有的的擴展模組之中。

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 9 月

本 刊 概 要

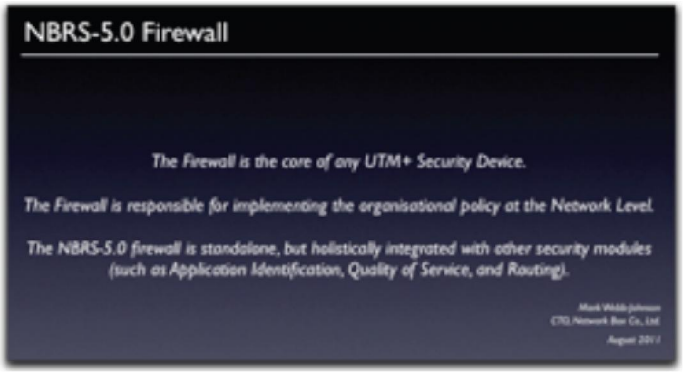
NBRS-5.0 的防火牆功能

這個月關於 NBRS-5.0 的話題，我們將就關於其防火牆功能進行詳細的描述。防火牆是任何 UTM+設備的核心部分，主要是負責企業和組織的策略規則在網路層的實現。NBRS-5.0 的防火牆功能是獨立的，但是與其它的安全模組（例如，應用識別、QoS 服務品質以及路由等）卻又集成於一個整體。

防火牆的可擴展性

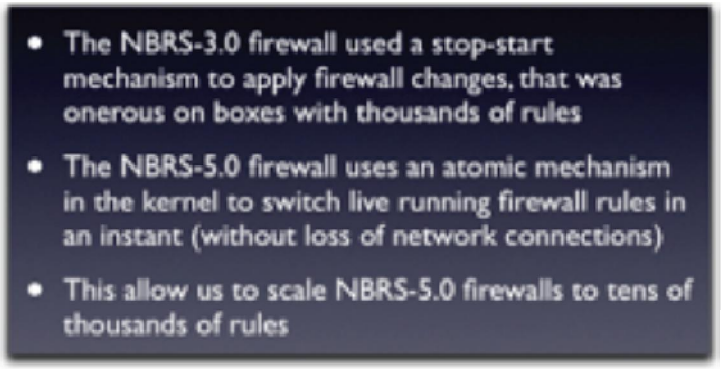
和其它競爭者一樣，NBRS-3.0 採用的是“關開”機制來實現防火牆策略的應用更新。這對於規則數量在合理範圍之內時，工作起來是沒有問題的，但是當規則達到數以千記時，工作起來就變得任務繁重了。其中所產生的問題就在於，防火牆在啓動時需要消耗過多的時間，而這個時間就與 Box 的運行速度以及需要載入的規則數量有著直接的關係。

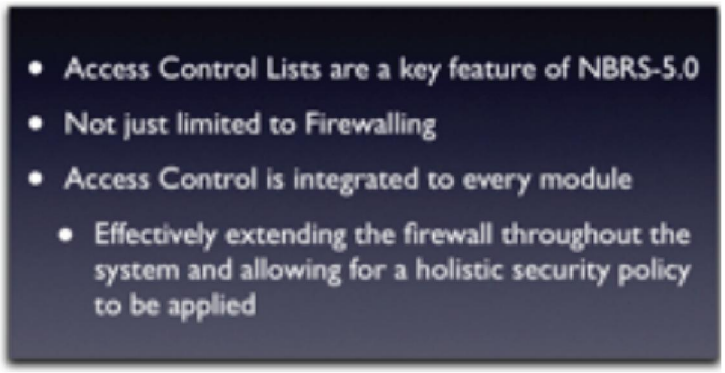
NBRS-5.0 的防火牆功能在內核採用了一種自動載入機制，使防火牆規則能在即時運行的情況下瞬間進行切換（不會造成任何網路連接的斷開）。而其實在內部，我們設立了兩個防火牆規則表（一個是當前運行的，另一個是保存最新的），而這之間在需要應用最新的規則時，是在瞬間自動完成切換的（不論是所有規則或者沒有任何規則需要載入，當然也取決於規則中是否存在錯誤）。這一特性，使得 NBRS-5.0 防火牆規則的數量可以達到數以萬計。



存取控制清單與規則

存取控制清單和規則是 NBRS-5.0 的兩個關鍵特徵，當然這也不僅僅局限於防火牆功能本身，而且還貫穿並整合到整個系統的防火牆所有的的擴展模組之中。





由於每一個安全模組實現了明確的策略定義，爲了防止重複，路由和代理的流量控制也是採用了相同的控制方式。

每一個存取控制清單（ACL）都是一個特定物件的清單。例如，IP 地址清單、使用者清單、設備 ID 清單，等等。在對這些列表進行歸類時，既可以是單個的條目（例如，10.8.2.301 是否是一個 IPv4 位址），也可以是擴展性的方式（例如 10.8.2.0/24 包括了 10.8.2.99）。

存取控制清單提供了最佳的性能（比起重複的規則要快很多）。例如以下的規則：

Permit LAN host 10.8.2.1 to call 10.8.9.99

Permit LAN host 10.8.2.65 to call 10.8.9.99

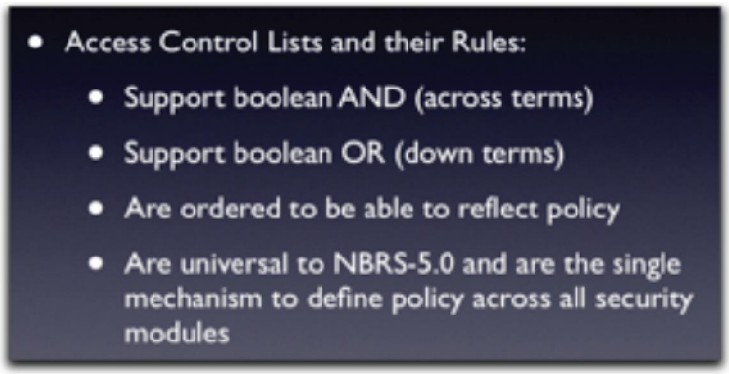
Permit LAN host 10.8.3.68 to call 10.8.9.99

（重複 100 個 LAN 用戶）

而將 100 個 LAN 用戶放入一個 ACL 列表且只需要一條規則。這樣做的話就會更加高效了：

Permit LAN hosts in ACL goodusers to call 10.8.9.99

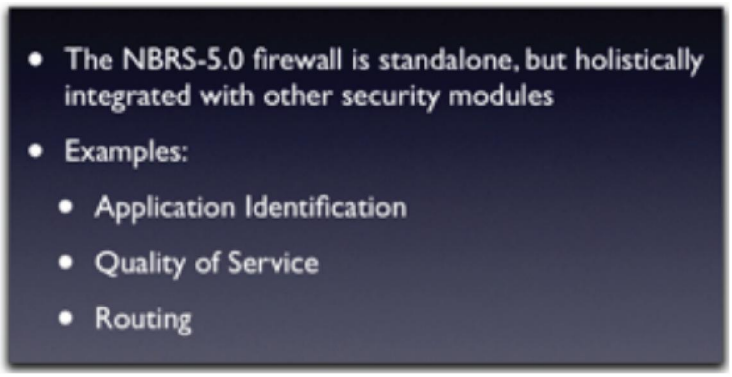
以 ACL 的方式建立和定義規則和策略。可以支援二進位“與”操作（類似上面例子中的“ LAN host ... call ...”格式的規範的格式），也支援二進位“或”操作（形如上面多條規則那樣上線有序的規則集）。這種排序的規則，以及允許/拒絕的結果動作，使得我們可以定義很多複雜的策略。



存取控制清單和規則普遍應用與 NBRS - 5.0 之中，同時也是用來定義所有安全模組策略的單一的機制。

模組化集成

NBRS-5.0 的防火牆功能是獨立的，但是與其它的安全模組卻又集成於一個整體。雖然防火牆在內核中運行（以提供最佳性能），但各方面都體現高層級的服務緊密集成到使用者空間。例如：



·連接和資料包標記（對於資料包和連接分類）

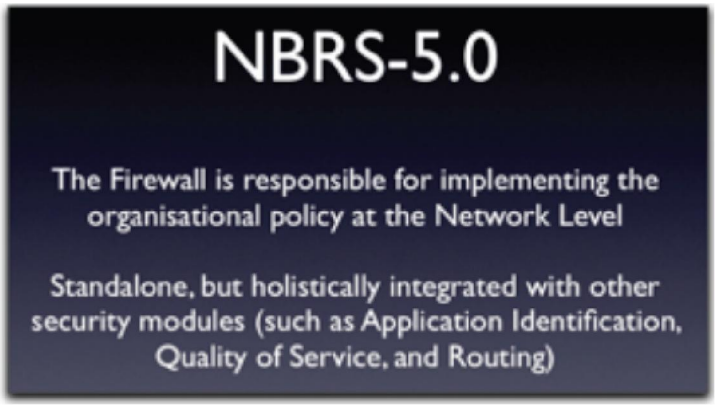
·應用識別（允許防火牆規則基於已識別的應用程式，而不是僅僅對協議或埠）

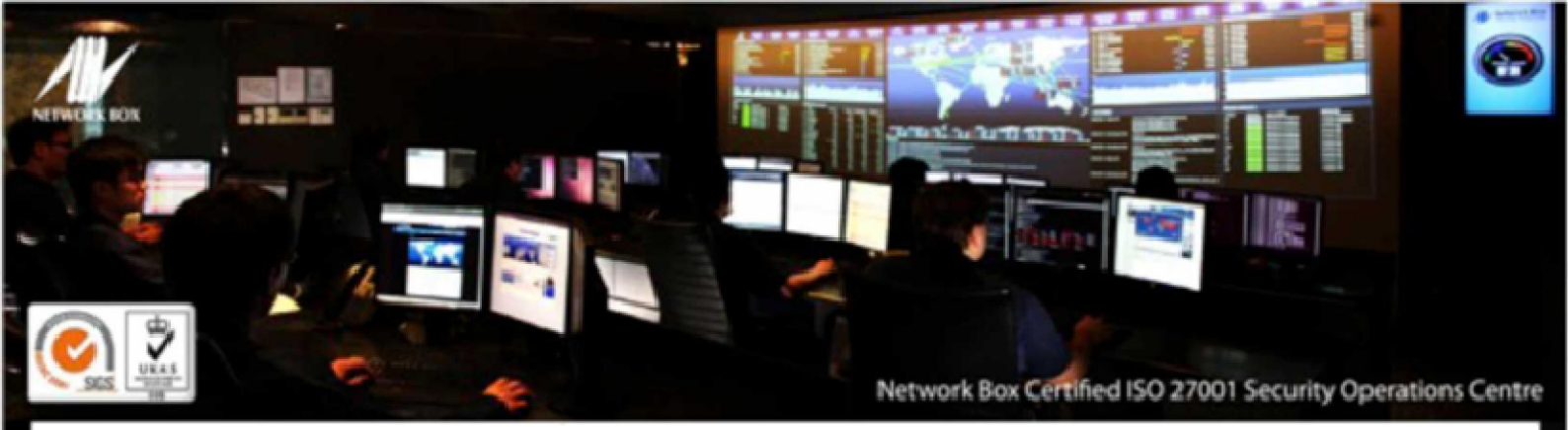
·IPS 資料流程（允許深層資料包分析的連接流的發送）

·條件（允許各種條件，如閘道斷開，高可用性模式等，在防火牆與其它提供或依靠這些條件的安全模組之間進行共用）

小結

NBRS-5.0 的防火牆功能主要是負責企業和組織的策略規則在網路層的實現。此功能是獨立的，但是與其它的安全模組（例如，應用識別、QoS 服務品質以及路由等）卻又集成於一個整體。這是在不犧牲配置的靈活性的同時，也對其性能進行優化的。





2011 年 9 月 新特性

在 2011 年 9 月 6 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：

·對各內部 NOC 系統有所增強。

· 修復了在 my.network-box.com 中自訂 LDAP 的 web 代理策略組中自訂群組和 LDAP 組存在顯示重名的情況。

·對交換分區記憶體使用情況的顯示的增強。

·修復了在 Box 人爲斷線的情況下全球監控系統中斷更新監控有關的不足。

·對全球監控系統中反病毒系統健康狀況監控有所增強。

·全球監控系統對 Box 重啓的警報的描述內容。

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。

S-Scan 內容過濾引擎

Network Box的S-Scan引擎是一個高速的Web內容過濾系統，主要是用於說明企業和組織阻斷其內部使用者對其所不受歡迎的網頁內容的訪問。

加入了“Google安全流覽”後，不良內容的類別就增加到16種，涵蓋了可能對企業電腦系統造成直接破壞的網站（含有惡意軟體），還包括含犯罪性質內容的（駭客），使人反感的（色情或仇恨），或者其它對用戶有害的網站（間諜軟體或欺詐）。

成人/色情	犯罪活動	賭博
偏執與仇恨	毒品	駭客
網路釣魚和欺詐	垃圾郵寄地址	間諜軟體
可疑網址	侮辱與誹謗	暴力
病毒/惡意軟體感染	武器	
谷歌安全流覽惡意軟體	谷歌安全流覽網路釣魚	

Network Box的S-Scan內容過濾引擎曾榮獲“電腦世界2011香港工商業獎 - 內容過濾/反間諜軟體”。“Network Box具有世界一流地位影響力。曾獲得40多個國際技術大獎，世界各地的客戶，包括超過150個在美國的銀行和信用社。Network Box在過去的10年上升到了一個在安全領域的的領導者。”“在內容過濾的問題 - 今年Network Box贏得了此項獲獎 - 一連串的安全駭客引出了如何保護資料的關注水準的問題。由於企業需要保護從企業流入流出的資料流程，內容過濾也是一個可墾地。” 香港《電腦世界》的首席主編Chee-Sing Chan如是說到。

更多內容，請參考：http://www.network-box.com/s-scan

2011 年 9 月份資料

關鍵指標	數據	與上月差比
PUSH 升級數	649	+14.3
特徵碼發包數	425,170	+14.0
防火牆攔截數(每 BOX)	823,945	+5.5
IDP 攔截數(每 BOX)	113,147	+4.2
垃圾郵件數(每 BOX)	12,591	-10.6
惡意軟體數(每 BOX)	1,047	+202.7
URL 攔截數(每 BOX)	163,582	+30.1
URL 訪問數(每 BOX)	4,234,015	+18.5

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