來自 Network Box 首席技術官

Mark Webb-Johnson 的技術資訊

Welcome

歡迎閱讀 2011 年 10 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，我們詳細介紹了入侵防禦系統。Network Box 入侵防禦的六個系統，在網路模型的所有層中協同工作，使防護效能與性能之間達到平衡。這六個系統分別是，網路通訊協定驗證，拒絕服務保護，前端 IPS，被動/主動 IDS，內嵌 IPS 和應用層保護。

相比于傳統的網路級 IDS / IPS 系統，Network Box 的有所超越，在 OSI 的 7 層模型中，向下已擴展到第 2 層，向上已擴展到第 7 層。入站和出站的入侵防禦均有支援，並與 NBRS - 5.0 系統的其他模組緊密集成。

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

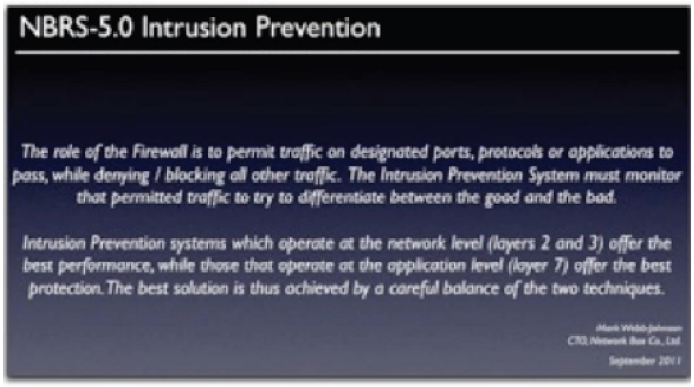
Mark Webb-Johnson
CTO, Network Box Corporation
2011 年 10 月

本 刊 概 要

NBRS-5.0 的入侵防禦功能

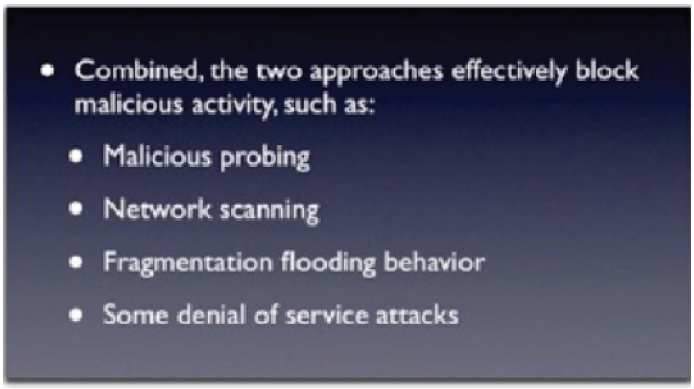
如果您詢問一個 UTM 供應商什麼是入侵防禦，他們通常會通過談論網路級的流量掃描、IDS、IDP、IPS 以及其它一下非常流行的詞語來回答您的問題。但如果您同樣的問題詢問網路管理人員時，他們通常多半會談論關於將網路威脅阻擋在他們網路的外面（同樣的，也包括使內網的網路威脅無法走出他們自己的網路）。而我們 Network Box，我們支援網路管理人員的說法。

防火牆的作用就是允許指定的埠、協議或者應用的流量通過，並且拒絕或者阻擋所有其它的流量。入侵防禦系統對允許通過的流量必須設法對其之好壞進行區分。防火牆是攔截指定的服務，而入侵防禦系統則是攔截由防火牆放行進來卻又可能存在威脅的流量。



運行於網路層（第 2 和第 3 層）的入侵防禦系統通常可以提供最佳的性能，而對於運行于應用層（第 7 層）的入侵防禦系統而言，則提供了最佳的保護。但最佳的解決方案則在於在這兩種技術之間達到一個最佳的平衡點。而 Network Box 的入侵防禦系統採用的方案也正是這種多層解決方案。

NBRS-5.0 的入侵防禦系統是由六個可供選擇但又互相協作的系統所組成。這六個系統互相協作且覆蓋了 OSI 網路模型的所有 7 個層。其作用就在於發現匿名的流量，並且盡可能早地將其進行攔截。讓我們一起來瞭解一下這六個系統。



1、網路通訊協定確認

網路通訊協定確認是在內核進行的，用於第 2 層和第 3 層。它涉及網路流量的確認，在核心協定層，基本協定的識別問題，以及盡可能接近硬體的解決方案。在這一層的攻擊檢測和攔截的實例包括 IP 碎片的漏洞，序號漏洞，對無效的 IP 選項或序列的掃描，以及無效的序列掃描。

結合核心防火牆（這使得 Network Box 可以對連接序列進行確認，並且利用無效的狀態對連接進行檢測）的連接跟蹤，這一層的技術的目的在於防止利用非常低級的 IP 協議以逃過偵察的入侵。

2、拒絕服務保護

NBRS-5.0 的網路 DDOS 安全模組提供了對拒絕服務（DOS）和分散式拒絕服務（DDOS）在網路層的保護的支援。緊密集成的防火牆，這個模組保護通過檢測潛在的惡意攻擊，並將它們在指定的將來的時期內的所有訪問列入黑名單。

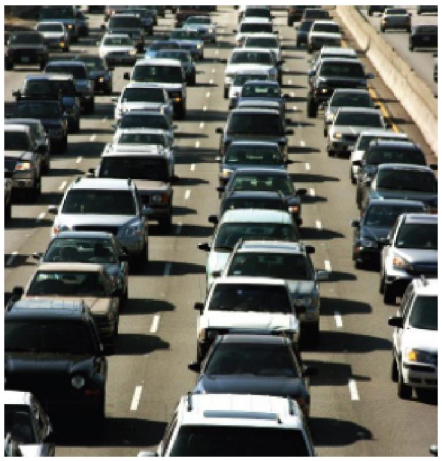
緩解源位址欺騙的方法有三種：a）總的連接速率限制；b）總的連接數限制；c）SYN cookies。前兩個對伺服器超載（例如 ICMP）提供某種程度的保護， 最後那個是對 SYN 洪攻擊提供保護的。

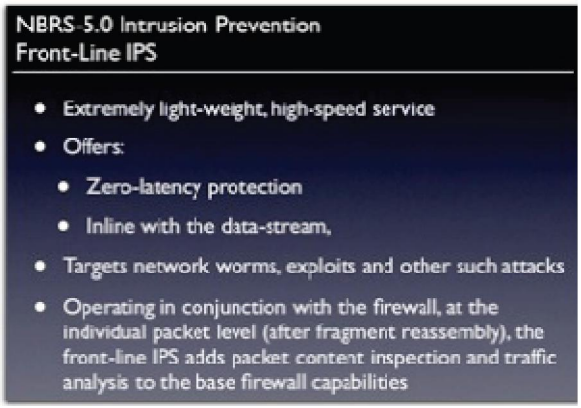
非欺騙性的源位址緩解使用兩個主要技術：a）每個源連接數限制，b）限制每個源的連接率。連接源超出任一限制，便會被判定爲惡意攻擊而丟棄連接。這些連接源將會被動態地添加如一個即時的黑名單，從而在未來再次發現這些源的連接請求時進行攔截。

在更高層的模組間的協作中（如代理相應的 DDOS ） ，動態特徵碼的生成需要採用啓發式方法，這樣，對流入的流量進行動態地生成特徵碼，以對惡意流量和攻擊源進行識別。這方面的例子包括在 HTTP 流量中 URL 方式的唯一標識，以及對源 IP 位址的即時信譽度查詢。這樣的一些動態的特徵碼，在往後可以用於對欺騙和非欺騙連接的惡意流量進行識別。

NBRS-5.0 的網路 DDOS 安全模組中包含了兩個已知爲安全源的白名單：a）期待應答的流出連接請求的動態清單；b）已知爲安全源的靜態清單。這兩個白名單均是用來避免將已知的安全源被列入黑名單的情況。

還有一個包含了已知攻擊源位址的基於時間的黑名單，用於在指定的時間段內對列表地址的流量列爲黑名單。這對於阻擋非欺騙源的 DDOS 攻擊是相當快速且特別有效的。一旦有一個惡意流量源被認定，其位址將被添加到這個動態的黑名單裡面，用於在預先指定的時間段內阻擋來自於此源地址的所有流量。





3、前置 IPS

前置 IPS 系統是一個非常羽量級、高速度的服務，用於提供零延遲的內嵌資料流程保護。它的防護目標物件是蠕蟲、漏洞攻擊以及其它類似此類的攻擊，結合 DDOS 防護模組進行防護。在與防火牆配合工作上，在單獨的資料包級別（在片段重組後），前置 IPS 增加了內容檢查和使用分析，給到基本的防火牆功能。

4、被動/主動 IDS

Network Box 的 IDS 系統工作在網路層，在資料流程的端側（對資料流程性能的影響不大）。它既可以配置爲純被動模式（可以進行警報和流量記錄，但不會有任何主動的執行動作）或者主動模式（可以主動地斷開被認定爲惡意的連接）。

5、內置 IPS

Network Box 的 IDS 系統工作在網路層，在資料流程的後端。每個連接的資料包都要經過這個系統，還有一個獨立的分組資料包的判決（來自於分組資料本身，以及作爲解碼應用層的資料流程），用於判決資料包是允許還是拒絕通過。與防火牆的緊密配合，可以在遠端系統發現之前對相關流量進行丟棄。

6、應用層防護

有效的應用層防護，要求能對連接進行攔截並且能夠完全地斷開用戶端與服務端之間的連接。一旦攔截，高層可以執行協議相關的動作（例如反病毒、策略執行、過濾等等）。

支援五種安全模型：1）漏洞防護（又名“補丁緩解” ）；2）出站保護；3）消極安全模式；4）DOS/DDOS 的安全模型；5）積極的安全模型。Network Box 的應用層防護，包含了請求和回應分析，廣泛的日誌記錄，協定驗證及策略，回應過濾，用戶端驗證等等諸如此類的更多的技術。

小結

Network Box 入侵防禦的這 6 個系統，在網路模型的所有層裡面協同工作，以平衡防護的性能表現。突破了傳統的只在網路層的 IDS/IPS 防護系統，Network Box 將此擴展延伸到 ISO 七層模型中，下至第二層，上至第七層。還支援入站和出站的入侵防禦，並且與 NBRS-5.0 系統的其它模組緊密結合於一體。

2011 年 10 月新特性

在 2011 年 10 月 4 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。

· 增加了對多條動態 IP 位址的 ADSL 的 Box 的 GMS 監控的支援。

·增強了 NBIDPS 系統的主動回應模式。

·增加了虛擬在雲端的 Network Box 的合同安排。

·對 Box Office 和支援系統的多個（多爲內部的）增強。

·修訂了對在不同的時間夏令時區的支持。

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。

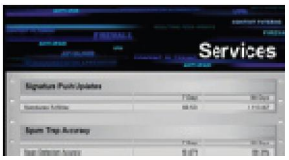
如果您還需要要關於這些的更多的資訊，請與您當地的區域 NOC 取得聯繫。他們將會進行相關的諮詢和安排。

Network Box 的安全回應

正如你可能知道，除了Network Box的主網站，我們還有一個安全響應網站，用於即時更新關於防火牆、入侵、惡意軟體以及垃圾郵件攻擊的最新資訊。

當你進入http://response.network-box.com/internet-health，您將看到一個動態的世界地圖，顯示了全球的網路健康狀況，不僅顯示了所有的攻擊源，還給出了攻擊源來源地的前十位排名列表。我們兩個部分的安全回應網站均已在最近進行了更新改版。

首先是保護頁，顯示了Network Box即時的保護統計概況。在此時刻，Network Box的系統運行多達78個保護引擎，其中包括一共有45818940個特徵碼。



其次是服務頁，顯示了垃圾郵件陷阱的精確度係數。這是一個特別引人注目的統計，也是我們全球各地很多客戶所要求的。目前，我們的垃圾郵件檢測精度是99.47%，而我們的電子郵件檢測準確度爲99.81%。這兩個指標係數在業內均是名列前茅的，且均爲在沒有定制策略，沒有反垃圾郵件學習，且沒有使用任何入侵反垃圾郵件技術（例如“挑戰應答”），使用的均是預設設置的情況下所獲得的資料結果。

當你登錄到Network Box的安全響應網站，您會發現，在頁面的左邊，有一個Facebook的連結。您可以點擊進入，以及時查看我們通過Facebook更新的安全資訊，以及給您任何您所應瞭解的特別重要的有關安全問題的提醒。

（http://www.facebook.com/networkboxresponse）

2011 年 10 月份資料

關鍵指標	數據	與上月差比
PUSH 升級數	620	+4.7
特徵碼發包數	328,676	+29.4
防火牆攔截數(每 BOX)	810,258	+1.7
IDP 攔截數(每 BOX)	116,355	-2.8
垃圾郵件數(每 BOX)	16,820	-25.1
惡意軟體數(每 BOX)	1,580	-33.8
URL 攔截數(每 BOX)	160,548	+1.9
URL 訪問數(每 BOX)	3,849,619	+9.9

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