來自 Network Box 首席技術官

Mark Webb-Johnson 的技術資訊

Welcome

歡迎閱讀 2012 年 4 月刊的《In The Boxing Ring》。在這一期當中，我們的重點是關於 Network Box NBRS-5.0 的 Web 應用防火牆的內容。

在第 2、3、4 頁當中，我們詳細介紹了 Network Box NBRS-5.0 的 Web 應用防火牆。這是一種最新發展水準的防火牆，它結合了路由、協議翻譯、加密和解壓縮、以及 DDOS 保護等技術和功能。它超越了一般的防火牆功能，不僅僅只是通過普通地對 tcp/80 埠的開或者關，來爲在開放的 tcp/80 埠上經過的 web 流量提供保護和翻譯服務。

那麼，Network Box NBRS-5.0 的 Web 應用防火牆（WAF）又有哪些特別之處呢？而在這一領域的眾多競爭者當中，又爲何要選擇 Network Box 呢？最基本的答案就在於，正如 Network Box 在 UTM 方面的設計方法，新增更多的服務和功能而達到我們的 UTM+，而在保護 Web 伺服器方面，Network Box 採用了所有必要的關鍵安全性群組件，並將這些元件與其它相關的服務一起放入一個整體的管理設備。這便是我們的 WAF+。

在第 5 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
2012 年 4 月

本 刊 概 要

Network Box NBRS-5.0 Web 應用防火牆

Network Box NBRS-5.0 的 Web 應用防火牆是一種最新發展水準的防火牆，它結合了路由、協議翻譯、加密和解壓縮、以及 DDOS 保護等技術和功能。它超越了一般的防火牆功能，不僅僅只是通過普通地對 tcp/80 埠的開或者關，來爲在開放的 tcp/80 埠上經過的 web 流量提供保護和翻譯服務。

上個月我們大概地講解了一下 Web 應用防火牆。這個月，我們主要講解 Network Box 的思路方法。

入站網路流量

網路流量（通常是與 tcp/80 埠的連接的一個 Web 應用防火牆環境）從以下示意圖的左邊流入。進入網路輸入層進行處理，執行基本 IP 協議一致性判斷，並結合可能在最低層出現的類似 synflood 之類的 DDOS/DOS 攻擊、碎片攻擊以及協議異常等的處理。尤其是在這一層對可能出現的源位址欺騙攻擊進行處理，以使在隨後的各層確保源地址是真實的。

然後，被放行的連接進入到網路 DDOS 保護模組。這個模組包含了一個 IP 位址白名單，DDOS 保護模組將會對這些 IP 地址放行通過。白名單通常用於防止對組織自身的位址拒絕服務，也包括一些重要的合作夥伴的地址。通過白名單後，兩個黑名單用於連接的主動攔截。（a）一個動態黑名單用於在短期內保留對攻擊源位址進行攔截，（b）還有一個永久性的黑名單用於長期地對攻擊源位址進行攔截。動態黑名單中的條目通常會過期，短短幾分鐘後可能就會自動刪除，而永久性黑名單中的條目將會一直保留到管理人員將之刪除爲止。所有三個黑名單均使用基於散列的匹配查詢，以應付每秒鐘數百數千連接個連接的攻擊。

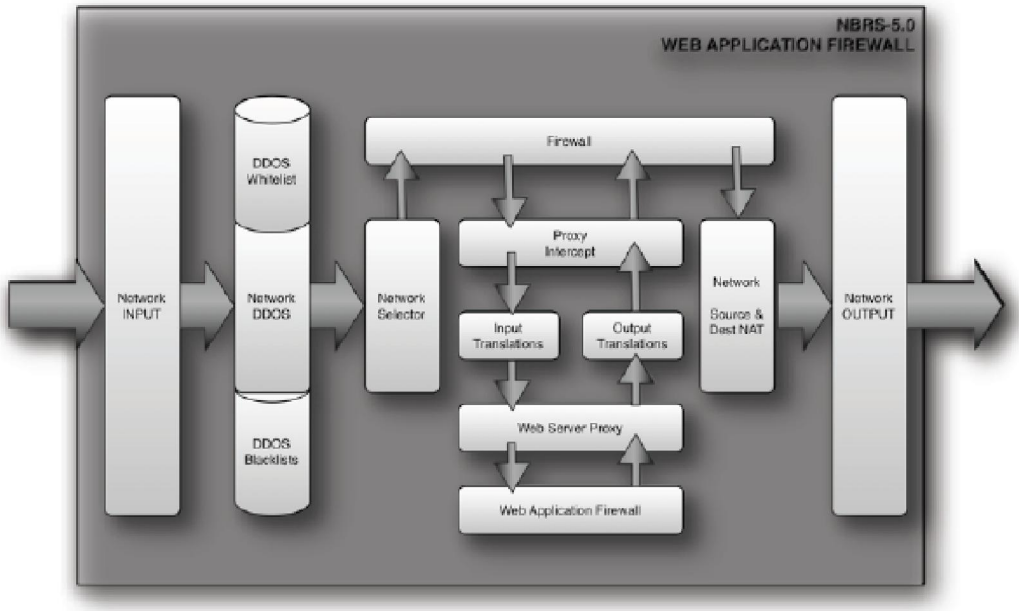
網路選擇

一旦一個入站連接通過了輸入層與 DDOS 保護模組，下一步將進入網路選擇階段。在這裡，流量將會被分類，在網路防火牆層將決定是否放行流量通過，或者將其攔截下來進入更深層次的處理。而在 Web 流量的情況下，它通常會被配置爲被攔截下來，並且直接通過防火牆進入代理攔截系統。

代理攔截和 Web 應用防火牆

代理攔截模組是一個高性能的代理網路流量的模組。一個入站的連接被接受並與相關而獨立的出站伺服器連接進行安全隔離。這種隔離可以對請求頭、請求主體、回應頭和回應主體進行獨立分析以便策略的執行。

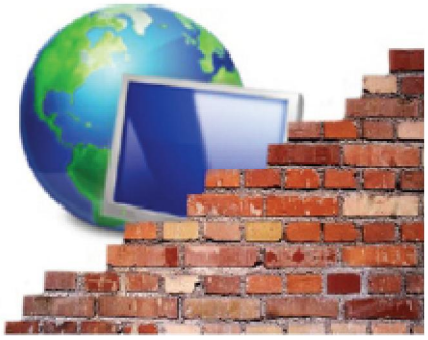
之後，入站流量（來自 Web 用戶端）進入輸入翻譯模組，以處理高層協定的翻譯，例如 SSL 代理以及 IPv4 與 IPv6 協定的支援。SSL 連接可被代理攔截系統終止，並進行流量解密以作進一步的分析。



然後，Web 伺服器代理將流入和流出 Web 應用防火牆的連接進行處理， 將 HTTP 協議（透明支援至 HTTP/1.1）解碼爲其組成部分，並且在網上交易的這些部分的策略執行上與 Web 應用防火牆進行即時地協同工作，猶如流量即時通過 Box 一樣。

之後，出站流量（來自 Web 用戶端，已經成功通過 Web 應用防火牆）放行進入輸出翻譯模組，此模組用於處理高層協定翻譯，例如 SSL 用戶端連接，以及 IPv4 和 IPv6 協定的支援。連接在這個階段會被 SSL 加密（不管它們原本是否被 SSL 加密過）。

出站網路流量



流量的最後一部分就是流量通過防火牆模組傳回到網路源/宿 NAT 模組。在這個階段，網路流的源位址可以被轉換（通常是私有的多對一的 NAT），目的地址也可以被轉換（通常是服務重定向或者負載均衡），或者只是被透明代理（不需要做任何的源位址或目的地址轉換）。

由此之後，流量便通過網路輸出模組到達內部被保護的 Web 伺服器。

Network Box WAF 的方法與好處

那麼，Network Box NBRS-5.0 的 Web 應用防火牆（WAF）又有哪些特別之處呢？而在這一領域的眾多競爭者當中，又爲何要選擇 Network Box 呢？

最基本的答案就在於，正如 Network Box 在 UTM 方面的設計方法，新增更多的服務和功能而達到我們的 UTM+，而在保護 Web 伺服器方面，Network Box 採用了所有必要的關鍵安全性群組件，並將這些元件與其它相關的服務一起放入一個整體的管理設備。這便是我們的 WAF+。

那麼，讓我們一起來看看這種方法的一些關鍵點。

1、拒絕服務保護

通過在盡可能最底層的網路棧使用 DOS/DDOS 保護，NBRS-5.0 在針對 DOS 和 DDOS 類型攻擊方面提供了第一級緩解。但是，除此之外，DDOS 系統也整合進 WAF 裡面，允許對掃描、其它暴力攻擊以及有如網站抄襲智慧財產權盜竊等不良競爭活動的積極回應。

2、協定轉換

支援 IPv4、IPv6 以及 SSL 協定，NBRS-5.0 的代理攔截系統可以支援由這些協定所組合的所有協定進行轉換。例如，Box 可以配置爲同時支援 IPv4 和 IPv6 的連接，純文字 HTTP（TCP/80）和 SSL 的 HTTPS（tcp/443），然後將這些連接以單一的 IPv4 資料流程發送到僅支援 IPv4 的做了負載均衡的集群 web 伺服器。這就大大簡化了 DMZ 區需要維護的 web 伺服器的網路結構。

NBRS-5.0 還可以執行 IPv4 與 IPv6 協議之間的源位址和目的地址 NAT 映射，可以達到無縫服務遷移以及在系統的部署和維護方面更加不可思議的方便靈活。

3、內部和外部的負載均衡

NBRS5 WAF 通過使用大量的多核 CPU 的優勢，包含了最新的 Intel 的 Sandy Bridge 架構的 CPU，實現並承載著一個高度多執行緒的代理伺服器。NBRS5 WAF 軟體架構設計用於內部多個 CPU 內核之間平衡其連接負載，從而使其能夠實現在一個硬體單一的基礎上安裝多個 WAF 的技術水準。再加上先進的網路通信硬體的支撐，例如 Intel i350 網路介面卡晶片，縮短了網路與系統記憶體之間的資料路徑的長度，NBRS5 WAF 在伺服器硬體方面也做了很大的提升。

另外，NBRS5 WAF 也有能力做到多個物理伺服器實例之間連接的負載均衡。

4、代理計算

NBRS5 WAF 提供了一些降低 Web 伺服器 CPU 負載的方法，通過採用一系列的策略，使其有能力爲 Web 伺服器擔當起一些昂貴的計算任務。

5、代理壓縮

內容壓縮是 HTTP 協定的一個標準的功能，旨在通過即時地壓縮，或者可逆的萎縮流覽器與 Web 伺服器之間的通信流量，以提高感知頻寬。對於流覽器與一台 Web 伺服器進行通信，CPU 資源的消耗是微不足道的，但對於一台 Web 伺服器與非常非常多的用戶端進行通信時，即使對頻寬的使用進行了優化，這對於 CPU 負載消耗也是無濟於事的，尤其在當前情況下頻寬的費用有所下降。

6、代理加密

安全的網路通信或 HTTPS 是互聯網安全的基石。其最主要的用途就是確保流覽器與 Web 伺服器之間的通信的私密性，這也特別是線上商貿和線上銀行的根本所在。但其不足之處在於加密演算法需要進行大量的計算，從而使得流覽器與 Web 伺服器的 CPU 的負擔達到更高的程度。同樣，對於一台爲眾多用戶端提供服務的 Web 伺服器，維持安全連接所消耗的 CPU 資源也是非常重要的。

當 NBRS5 WAF 扮演代表 Web 伺服器的角色並且直接接受用戶端流覽器的請求時，其可疑執行對流入和流出到互聯網的流量的加密和解密，而在內部安全網路與 Web 伺服器進行通信時卻不需要有加密的負擔了。通過利用硬體輔助加密，NBRS5 WAF 將有能力可以代替受保護的 Web 伺服器進行重要的加密負載的處理。

好處不僅於此，由於 NBRS5 一直不斷地對其加密軟體套件進行維護，使其保持最新最安全並進行功能修復，因此通過“代理”的方式也保證了受保護的 Web 伺服器的最新最安全特性。

7、Web 應用防火牆

以上多有的功能的運用並不會對 Web 應用防火牆的有效性產生任何的影響。Network Box NBRS-5.0 的 WAF 不僅支持在入站連接、請求包頭、請求主體、出站連接、回應包頭以及回應主體階段提供保護和策略執行，還可以通過使用被動、主動以及 DDOS 安全模組擔當並提供漏洞保護和出站保護。

總結

NBRS-5.0 代理 Web 伺服器 WAF 通常是安裝在攻擊源與 Web 伺服器之間來提供保護。去到被保護的 Web 伺服器的 Web 請求將被 NBRS-5.0 WAF 透明攔截並代理，並受到保護策略的過濾，然後再轉發到 Web 伺服器。被保護的 Web 伺服器的回應資料也是同樣被攔截並且通過保護策略的過濾，再返回到請求的發起者。

經過 2012 年 4 月 3 日週二的最終 Beta 測試版的發佈，Network Box NBRS-5.0 WAF 便具有了針對 Web 應用攻擊的全面而有效的安全保護。

2012 年 4 月 新特性

在 2012 年 4 月 3 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：

·一系列內部 NOC 系統的功能增強；

· 在 Box Office 工單更新郵件中包含了 Box 類型和 SLA；

· 修正了針對 GMS 健康監控系統在 IDPS 服務監控的提高；

· 針對 SMTP 驗證服務的性能提高；

· NBRS-5.0 在 Box Office 系統中的進一步支援；

· 一系列（多爲內部的）針對 Box Office 和支援系統的增強與提高。

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。

2012 年資本雜誌優秀企業獎

Network Box 贏得 2012 年資本雜誌優秀企業獎的“最佳網路安全提供商”獎項。

頒獎儀式於 2012 年 3 月 13 日在港島香格里拉大酒店的宴會大廳隆重舉行。

資本雜誌是大中國著名的商業雜誌。資本傑出企業成就獎旨在表彰那些在本年度內具有出色的業績和成就的企業所做出的貢獻和努力。所有獲獎企業均經過了專業評審團隊、資本雜誌編委會以及公眾網上投票的嚴格評估評審。

公開選拔標準包括以下內容：企業的信譽、行銷策略、產品的創新與發展、社會責任和環保專案、員工培訓計畫以及對商業合作夥伴所提供的客戶服務。

Network Box 爲能贏得如此高的殊榮而感到非常的榮幸與自豪。我們想感謝大家，特別是我們的客戶，能爲我們在此次評審中投下了您非常重要的贊成票。

2012 年 4 月份資料

關鍵指標	數據	與上月差比
PUSH 升級數	572	+45.5
特徵碼發包數	453,202	-2.8
防火牆攔截數(每 BOX)	845,384	-3.1
IDP 攔截數(每 BOX)	145,742	-10.7
垃圾郵件數(每 BOX)	15,952	-1.86
惡意軟體數(每 BOX)	211	+28
URL 攔截數(每 BOX)	152,521	-9.6
URL 訪問數(每 BOX)	4,098,951	-4.8

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