In the Boxing Ring

Network Box 技術資訊

Network Box 技術總監 Mark Webb-Johnson編輯

歡迎閱讀2012年10月刊的《In The Boxing Ring》

在本期的略加長版當中，我們從第二到第四頁裡面詳細探討了拒絕服務（DoS）以及分散式拒絕服務（DDoS）攻擊。

在這些天已成爲一個重大的問題，因爲最近發生的越來越多的這方面的攻擊。這在我們的技術資訊發佈中正從中間頁的位置上升到排前頁的凸顯位置。

然而，通常來講是沒有什麼辦法可以完全阻止這些攻擊的。唯一的解決辦法就是，盡可能地減小攻擊所帶來的影響，以使您的服務在其可用性上對相關用戶的影響達到很小甚至沒有，這樣的話，攻擊者就會自然而然地停止攻擊或者轉攻他處。

有兩種不同形式的拒絕服務攻擊：欺騙性源地址攻擊和真實源地址攻擊。我們將從如何防禦這些類型的攻擊以及NBRS-3.0和NBRS-5.0的防禦技術兩方面著重探討。

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。

Mark Webb-Johnson
CTO, Network Box Corporation
October 2012

You can contact us here at HQ by eMail (nbhq@network-box.com), or drop by our office next time you are in town. You can also keep in touch with us by several social networks:

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
Google+: https://plus.google.com/u/0/107446804085109324633/posts

本 刊 概 要

拒絕服務與
分散式拒絕服務

在電腦領域，拒絕服務攻擊（DoS攻擊）或者分散式拒絕服務攻擊（DDoS攻擊）是一種企圖使伺服器或其網路無法爲其相關使用者提供服務的這麼一類攻擊（維琪百科）。

相當於在現實生活中，在一個商店的門前，聚集了大量的人群，但其中大部分人都不是要買東西的顧客，從而導致真正的顧客都無法步入門前，進而阻礙了商店的正常經營。

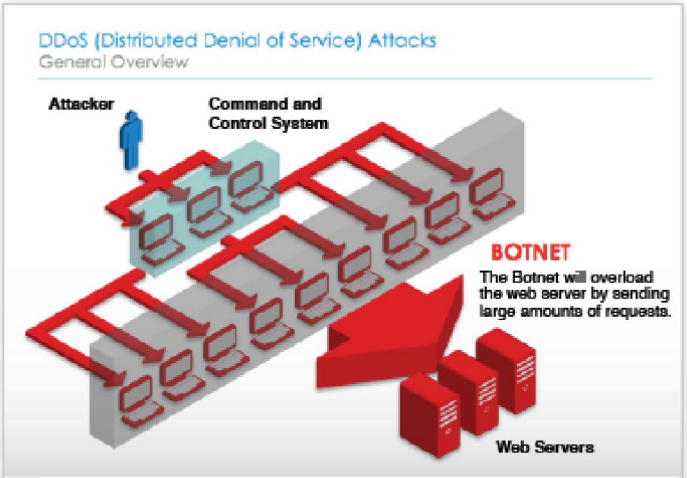
如何有效地防禦
DoS/DDoS 攻擊

首先要指出的是，通常來講是沒有什麼辦法可以完全阻止這些攻擊的。唯一的解決辦法就是，盡可能地減小攻擊所帶來的影響，以使您的服務在其可用性上對相關用戶的影響達到很小甚至沒有，這樣的話，攻擊者就會自然而然地停止攻擊或者轉攻他處。簡單地說，防禦就是讓你自己成爲比別人更難攻擊的目標。形象地說就是，你不需要比獅子跑得更快，但你只需要比你旁邊的那個傢伙跑得更快一點就可以了。

那麼，如何減少這種攻擊呢？好了，第一步是要掌握對這樣一個術語性非常強的“拒絕服務”概念的認知，它有兩種不同的形式：

1. 欺騙性源地址攻擊 在發生時，攻擊者的攻擊機器的身份是僞裝隱藏的。他所使用的僞裝的源位址是隨機生成的，然後企圖通過洪攻擊堵塞你的入站頻寬或者耗盡你處理併發連接的資源。

2. 真實源地址攻擊 在發生時，攻擊者並不嘗試要將直接攻擊的機器的身份進行僞裝隱藏。攻擊者自身的攻擊機器也混入在所有的攻擊機器（通常大部分的攻擊機器並不屬於攻擊者的）裡面。這種情況下，攻擊者會使用真實源位址，通過成百上千（甚至成千上萬）的真實機器（形成一個僵屍網路）通過洪攻擊堵塞你的入站和出站頻寬或者耗盡你處理併發連接的資源。



一個典型的 DDoS 攻擊示意圖

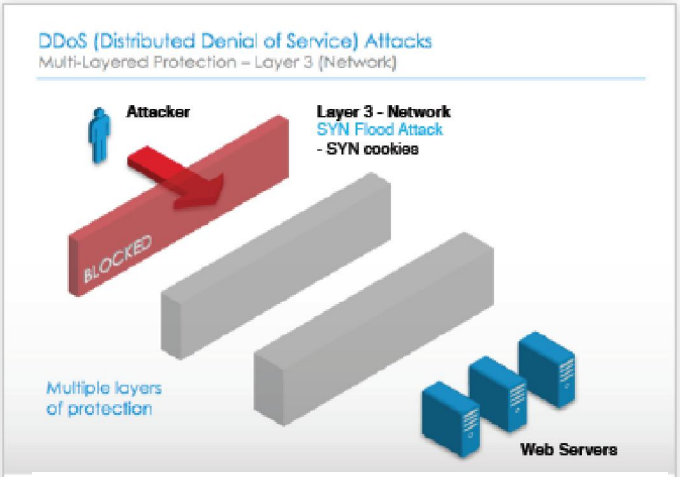
從歷史上來看，第一種（欺騙性源地址）是最普遍的一種DoS/DDoS攻擊，但這些攻擊的範圍是極其有限的，所以我們現在很少看到這些類型的攻擊。這是由於源位址都是僞裝的，TCP/IP的三次握手無法完成，所以高級的TCP/IP服務就具有固有的保護。那麼這裡的漏洞就在於入站頻寬容量本身，以及被攻擊伺服器處理併發連接的資源容量。

現如今，第二種（真實源地址）是迄今爲止最普遍的，而Web伺服器（通常是TCP/80埠）是遭受攻擊最多的目標物件。攻擊者通常會利用由數以萬計的傀儡機所組成的僵屍網路，對伺服器進行小的HTTP GET請求檢索大型網頁的洪水攻擊。這樣的洪水攻擊將有效地占滿出站頻寬以及伺服器的資源。

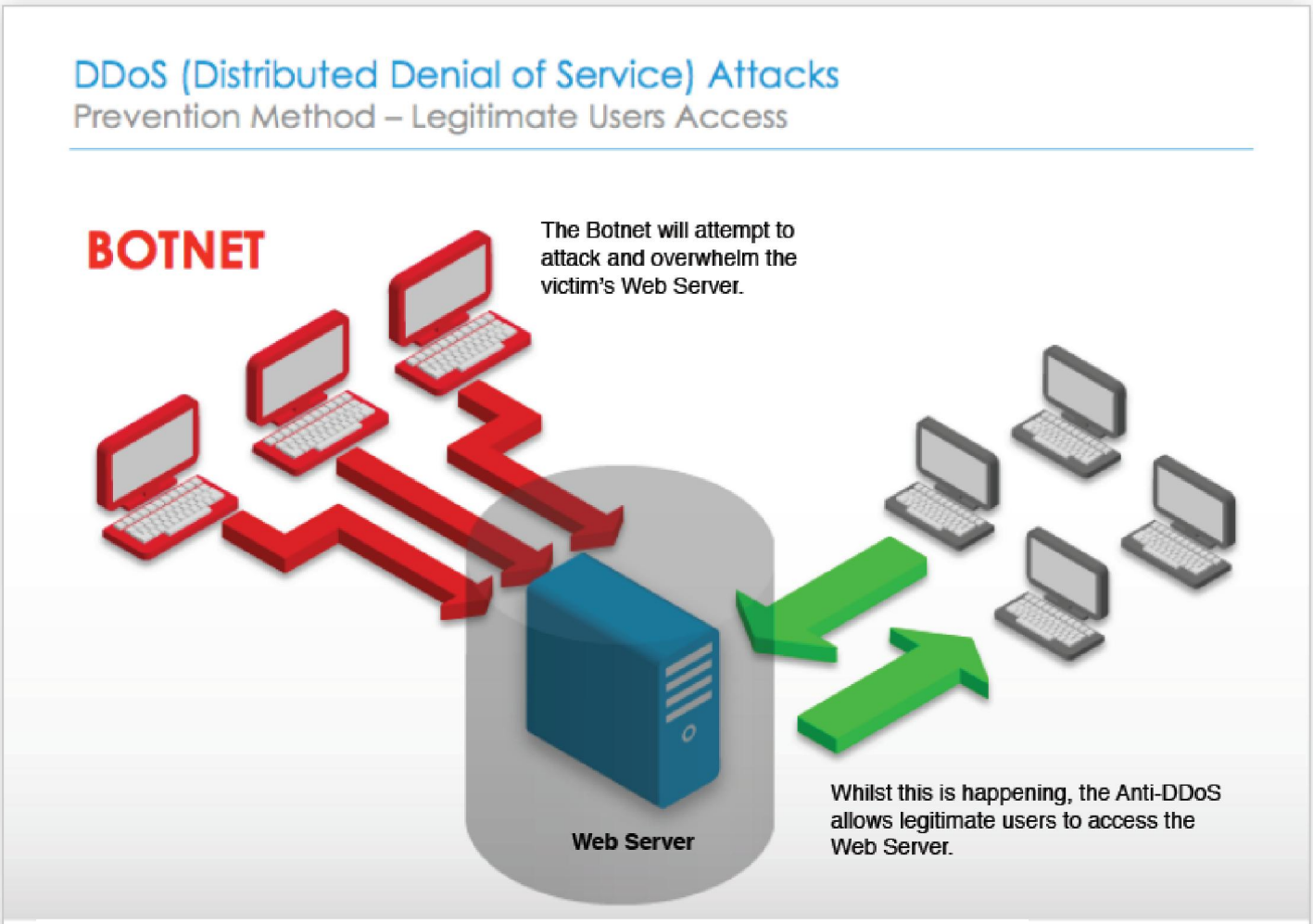
如何有效地防禦
欺騙性源地址攻擊

對攻擊者的源IP是僞造的這樣一類的攻擊進行防禦，涉及到一個關於Internet與被攻擊伺服器之間的嚴格區分的問題。Network Box上處在去到互聯網的閘道上的防護模組，對來自互聯網的初始連接進行處理，並且應用防護技術對攻擊流量進行識別，然後在其到達被保護的伺服器之前丟棄掉。相關的技術包括SYN cookies（主要TCP/IP等協定），速率限制以及攻擊資料包指紋識別。

只有合法的驗證爲非欺騙性的源位址，才能被允許繼續與內部的伺服器進行連接，這種方式可以防禦絕大多數這一類的攻擊（只要入站頻寬足以有效地處理這些攻擊的流量）。



第三層的保護——通過 SYN Cookie 技術攔截攻擊



在受到 DDoS 攻擊期間，採用多種技術以緩解攻擊者的攻擊，同時合法用戶也可以正常訪問。

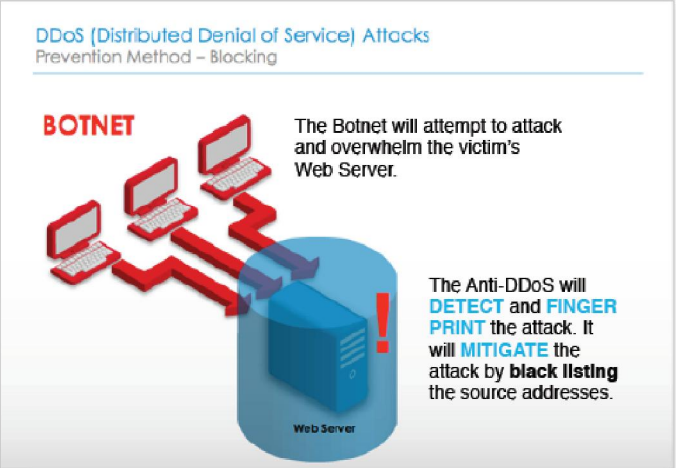
如何有效地防禦
真實源地址攻擊

Network Box一旦識別某個特別連接的源IP位址不是僞造的，我們就可以允許這個連接進入客戶的伺服器，並且會繼續監控該連接的活動情況，以查看使用者在做些什麼。在這個時候，我們就會對合法的請求與來自於惡意攻擊者的請求進行區分開來。

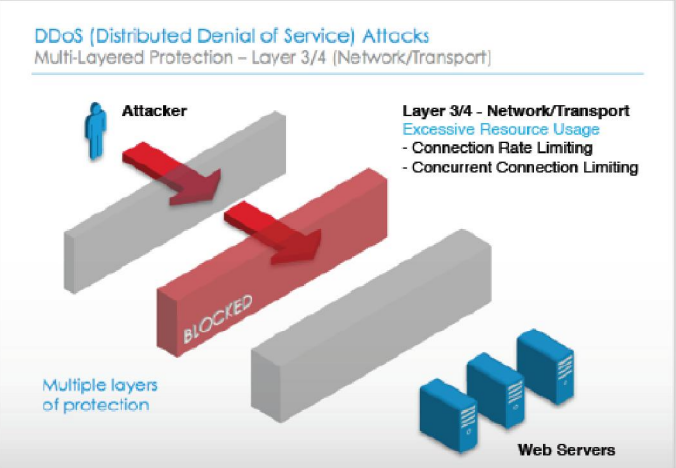
Network Box採用行爲分析，流量簽名，速率限制，以及其它用於識別惡意流量的源地址的類似技術。一旦我們確定了一個惡意流量來源，我們便會將其列入黑名單。

Network Box的網路通訊協定棧由許多層的保護組成，從第一層的實體層的保護，一直到第7層的應用層保護。IP地址的白名單和黑名單都被保持在協議棧的較低層，這樣，來自於黑名單（但不是白名單）裡面的這地址的源流量就會非常高效地被攔截掉。一旦一個攻擊源被確定，它將被加入到黑名單中，那麼其之後的流量將在一定時間內（動態黑名單）或無法確定的時間內（永久黑名單）被攔截掉。

通過對攻擊源的識別，並將其列入黑名單，Network Box從遭受攻擊開始在幾秒鐘內即可得到緩解，避免了內部伺服器的超載，並且可以對具體的攻擊源及其數量進行準確記錄和計量。



▸ 一般的 DDoS 攻擊防護——攻擊的指紋識別和黑名單處理

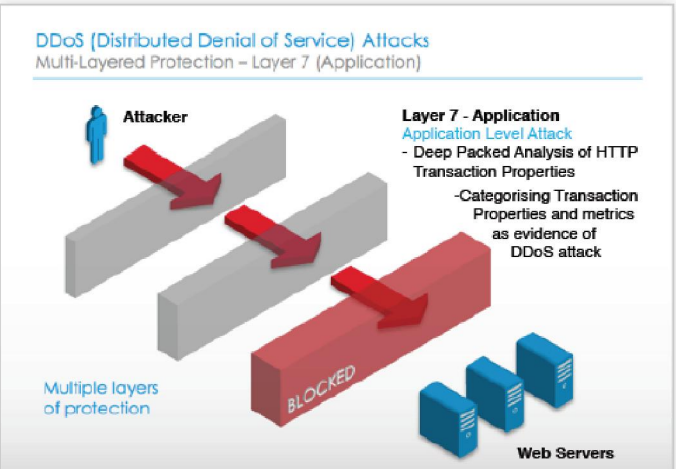


▸ 第三、四層的保護——通過連接速率限制進行封鎖

NBRS-3.0
以及 NBRS-5.0

這一防護技術已經植入到所有的Network Box。區別就在於，在NBRS-5.0中，我們對其防護結構在性能上進行了更多的提升，並且緊密地集成到我們的Web應用防火牆和Web代理系統之中。這樣，NBRS-5.0就可以通過自動啓發式和演算法，再結合大量的簽名特徵碼和已知的Web攻擊的規則資料庫，對攻擊源進行識別以及黑名單處理。

正是由於Network Box擁有了Web應用防火牆以及DoS/DDoS的防禦能力，才使得NBRS-5.0成爲Web伺服器防護方面的領導者。



▸ 第七層的保護——通過深包裝分析和分類處理

Network Box Certified ISO 9001 / ISO 20000 / ISO 27001 Security Operations Centre

2012 年10月
新特性

在2012年10月2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：

- 各種內部NOC系統的改進；
- 即將推出的S-Scan內容過濾引擎的支援方面的改進；
- NBRS-5.0在Box Office系統中的進一步支援；
- Box健康檢測系統的一些小修改以提高對Box的監控能力；
- 一系列針對Box Office和支援系統的（主要是內部）功能增強。

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 |
Anti-DDoS WAF+ 全球發佈在即

Network Box的Anti-DDoS WAF+（反分散式拒絕服務Web應用防火牆增強版）系統，是一個高度可定制性的安全管理設備（或者說是虛擬的或者基於雲的設備），它可以針對HTTP/HTTPS會話進行一系列嚴格的預配置策略的處理，爲Web伺服器提供針對攻擊的保護。

WAF SCAN

其關鍵的特性包括：

- 頻寬與網路的優化
- 分散式拒絕服務（DDoS）攻擊的防禦
- Web應用防火牆
- IPv4 - IPv6 / IPv6 - IPv4 的互相轉換
- 性能的優化
- Adobe PDF 格式的報告

這是Network Box的NBRS 5.0爲基礎的第一個版本的系統，它將在未來數月內推出。

SEPTEMBER 2012 NUMBERS

Key Metric	#	% difference (since last month)
PUSH Updates	529	-7.7
Signatures Released	326,411	+12.14
Firewall Blocks (/box)	927,429	+0.3
IDP Blocks (/box)	147,920	+4.9
Spams (/box)	14,006	+0.3
Malware (/box)	755	+5.6
URL Blocks (/box)	179,202	+0.9
URL Visits (/box)	4,476,589	-1.9

NEWSLETTER STAFF

Mark Webb-Johnson
Editor

Michael Gazeley
Jasmine Arif
Nick Jones
Production Support

Network Box Australia
Network Box Hong Kong
Network Box UK
Contributors

SUBSCRIPTION

Network Box Corporation
nbhq@network-box.com
or via mail at:

Network Box Corporation
16th Floor, Metro Loft,
38 Kwai Hei Street,
Kwai Chung, Hong Kong

Tel: +852 2736-2078
Fax: +852 2736-2778

www.network-box.com