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12月刊的《In The Boxing Ring》

這個月，我們感覺非常的欣喜與自豪，我們最新的Anti-DDoS WAF+系統（反分散式拒絕服務Web應用防火牆增強版系統）WAF-Scan正式發佈了。這是後續幾個月裡即將發佈的Network Box 第五版本的產品和服務的第一個版本。

在第2至4頁，Network box 的研究和開發主管尼克·鐘斯（Nick Jones）對這個系統在技術層面上進行了介紹，並重點介紹了所涉及到的攔截、分類、動作以及轉換方法等內容。

作爲一項特殊的功能，它是Network Box自從有了原來的統一威脅管理Plus（UTM+）的12年來，絕對是最重要的一次發佈。在第5頁中我們也貼上了一些現場的圖片。

在第6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
December 2012

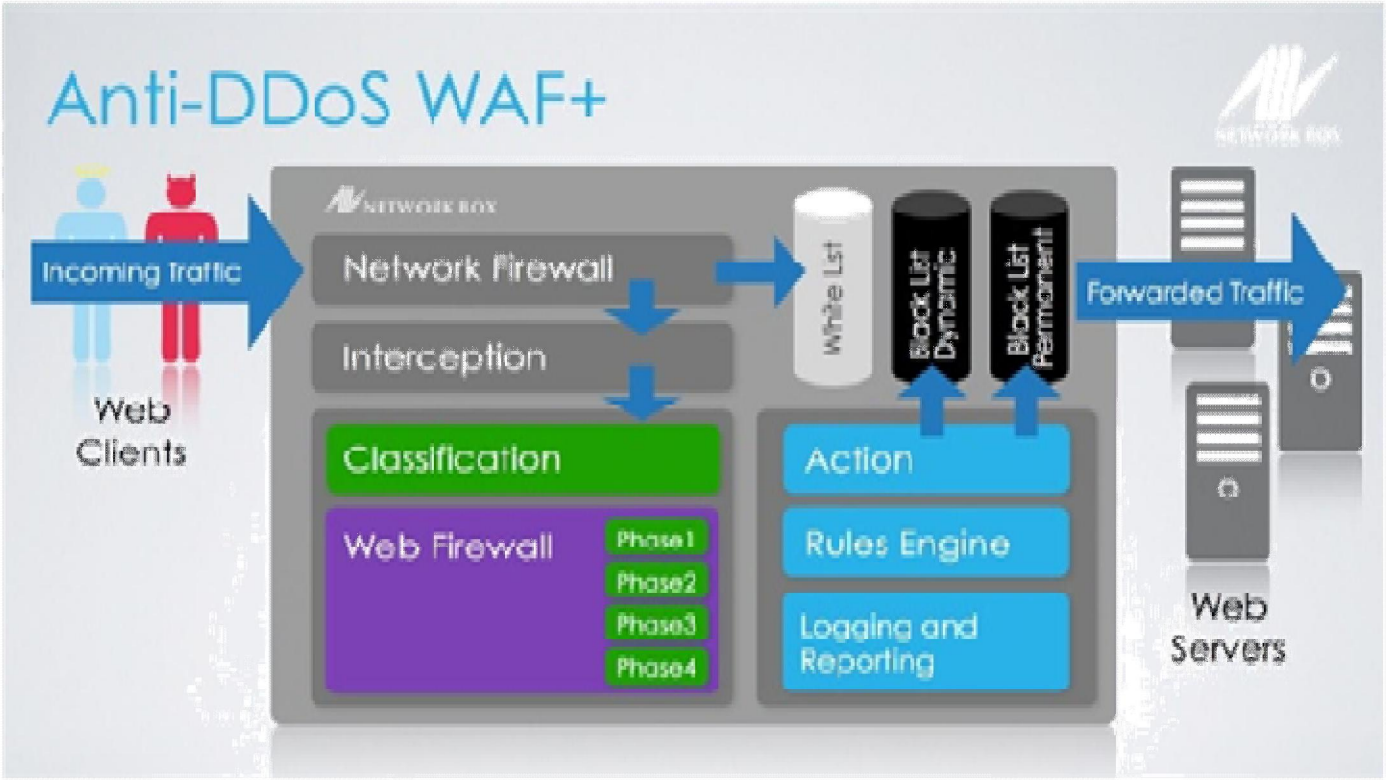
您可以通過郵箱（nbhq@network-box.com）與我們總部取得聯繫，或者到我們的辦公地點親臨參觀指導。您還可以通過以下幾個對外網站對我們保持關注：

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

本刊概要

Anti-DDoS WAF+ 概述

2012年11月30日這一天，我們的Anti-DDoS WAF+系統WAF-Scan已經正式發佈了。並在這次的正式的發佈會上將這一系統向我們的一部分重要的客戶進行介紹。



介紹

Anti-DDoS WAF+ 是一個多層次的安全解決方案，主要針對Web應用的保護，包括應用程式所部署在的伺服器，以及這些伺服器所連接的網路的安全的防護。

它是從多個層面來處理一個安全問題的，因爲攻擊者會結合多種攻擊技術，包括精准的Web應用與伺服器漏洞攻擊，以及大量的暴力性的分散式拒絕服務攻擊等。

Anti-DDoS WAF+ 產品提供了對HTTP傳播的Web應用程式攻擊的保護功能，可以通過規則對常見的攻擊類型進行檢測，例如：跨站腳本、SQL注入、網路爬蟲以及惡意軟體的檢測等。並且針對客戶的Web應用可以建立更多的特殊而獨立的安全規則。同時還提供了針對DoS防護的IP位址黑名單，並且當Anti-DDoS WAF+定義了一個新的DoS攻擊後，還可以對黑名單進行動態更新。

另外，Network Box的這一混合型防火牆裝置，其中針對安全分析的流量捕獲元件，可以完成傳輸與會話協議的轉換，並且可以將NBRS-5.0設備用作一個IPv6和SSL的連接終端。

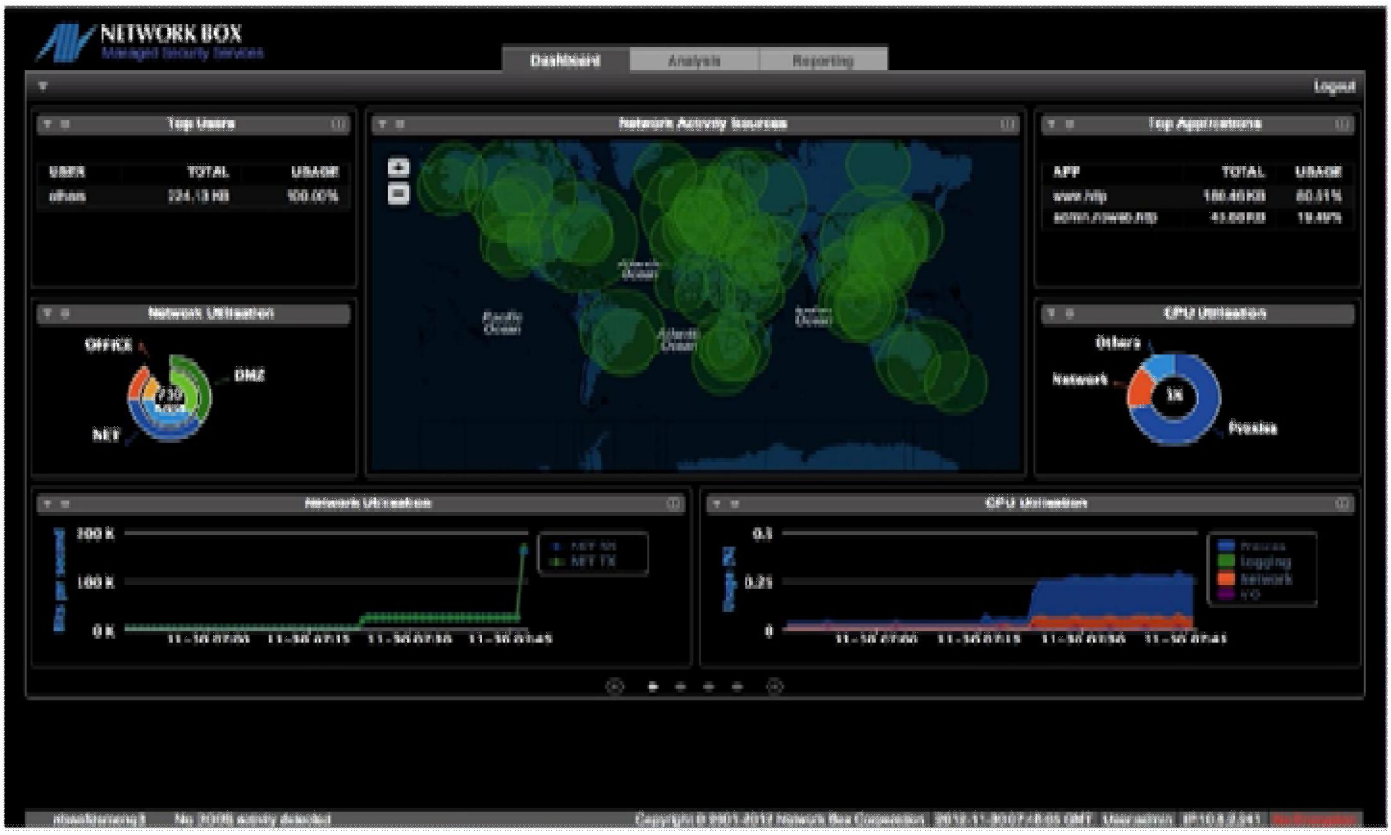
作爲In The Boxing Ring中課題的一部分，Anti-DDoS WAF+的一些關鍵體系結構元件以及他的非常重要的一些特性和好處都將在這裡進行描述。

資料攔截偵聽

Anti-DDoS WAF+設備最理想的部署方式，是串列連接方式，並對流量進行透明攔截偵聽，安裝在外部的不被信任的Web終端與客戶的Web伺服器之間的位置。

在這裡，Anti-DDoS WAF+設備通常會遵循Network Box的安全功能的設計理念，那就是“不傷害、不影響”。對於用戶端的原有IP地址，在Web伺服器看來是被隱匿了的，而對於Web用戶端看來，Web伺服器的IP位址也是被隱匿的，給雙方都產生一種直接的錯覺。

然而，“不傷害、不影響”的指導原則是針對正常良性流量而言的，而不是說對惡意流量也執行這樣的安全政策。針對



這樣一些流量所採取的的動作，包括協議性的具體重整和去除，其範圍包括從所有IP流量的完全阻止，到列入黑名單的Web用戶端位址，再到被認爲違反了安全性原則的傳輸資料和中繼資料。

首先，來自Web用戶端的流量在首次進入Anti-DDoS WAF+設備的網路棧時，在第一時間需要經過IPv4和IPv6位址黑名單的檢查。這些黑名單包含了在之前被Anti-DDoS WAF+安全性原則（尤其是DDoS保護策略）認爲是惡意的用戶端位址。

這一過濾處理是在一個非常接近於設備物理硬體的層面上運行的，處在於NBRS-5.0主機系統所要執行的其它重要的處理過程之前，因此在這一層面所進行的處理是非常快速的，甚至類似Network Box的M系列的中檔設備在每秒鐘就可以處理幾十萬個資料包。

在此之後，流量來到截取層，這是NBRS-5.0混合型防火牆的應用層代理元件。應用層代理掛接到下層作業系統的網路堆疊，並且提供了一個“兩全其美”的服務，通過允許協定層資料流程的完全訪問進行分類，但同時又保留同類原IP位址在IP層的橋接。

翻譯功能，這樣也是作爲Anti-DDoS WAF+產品的一項關鍵功能，是由應用層代理進行處理的。他們將在翻譯中的部分細節進行討論，概況地說，剝去Web用戶端的流量傳輸層和工作階段層的封裝，然後提取出資料流程給到Anti-DDoS WAF+的分類層。

分類

NBRS-5.0的一個基本設計原理是分類和動作的分離。

NBRS-5.0的分類處理過程只有個簡單的目的：“盡可能多地對給定的流量進行確認“。NBRS-5.0中的每一個安全模組的目的是在一個獨特的環境中，執行其執行相關功能，以確認一個給定的資料庫的特性，不論是所提取和編目在列的具體的協議的中繼資料，或者是被識別爲病毒或惡意軟體的傳輸載荷。因此，在分類層的通用目標要求的背後，是更多的需要執行的細節的實現。

作爲一款Anti-DDoS WAF+安全產品分類元件的網頁防火牆，其目的在於完全並徹底地將流入的HTTP協定的資料分解爲最基本的資料元。對中繼資料進行提取，並對其行爲進行觀

察，記錄日誌以備日後參考，並對所建造的HTTP協定資訊採用特定Web應用程式防火牆規則語言的規則引擎。

由於其複雜性和綜合性，Anti-DDoS WAF+ Web防火牆是一個自成體系的安全子系統，具有多層次HTTP協定解析和提取引擎，以及採用了一個獨特的特徵碼庫的且以規則爲基礎的分析引擎，其特徵碼庫由Network Box進行專門的維護並進行週期性更新。

分類階段的結果，將由下一階段的動作執行階段讀取解釋。

動作執行

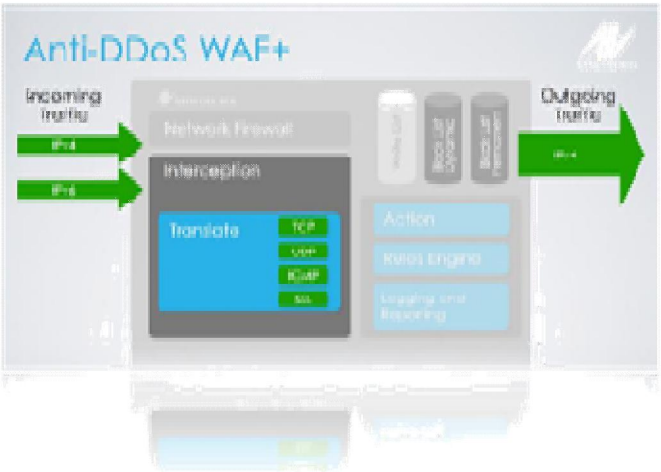
動作執行階段涉及到多個NBRS-5.0基本架構層，包括從NBCONFIG和NBCONSOLE提供的統一配置管理，到特定環境下的相關元件，例如Anti-DDoS WAF+等。

第一階段的動作環節實際上是發生在Web用戶端與Web服務端資料傳輸開始之前的。它也就是在通過NBCONSOLE系統所定義的安全性原則規則之所在。Anti-DDoS WAF+ 插入到NBCONSOLE系統之中，以利用龐大的資料類型庫以及在NBRS-5.0中所定義的網路管理和安全的相關概念，同時添加Web應用防火牆所特有的資料類型和概念。

Anti-DDoS WAF+ 中NBCONSOLE模組爲管理人員提供了一整套安全性原則和規則的定義，用於對中繼資料的處理和特定的Anti-DDoS WAF+防火牆的分析判決，並將其解釋爲行爲動作，以展開對改資料傳輸的深入分析。

Anti-DDoS WAF+產品在安全防護方面，在NBCONSOLE環境中也提供了非常豐富的內容，增加了一些獨特的網路管理概念。

DDoS防護模組還爲管理人員提供了分析說明和HTTP傳輸的中繼資料作爲DDoS攻擊的證據。這種DDoS攻擊的判決將會使Anti-DDoS WAF+系統進一步採取具體的動作。也就是對動態IP位址黑名單的更新，以使能夠對之後的DDoS擁護短的連接進行快速的拒絕回應動作。



資料翻譯

Anti-DDoS WAF+產品的翻譯層爲核心的分類元件提供了一個重要的功能，那就是，那就是對無論是低層級傳輸層還是安全封裝層（SSL）的協定資料都會進行隔離操作。

通過讓網路管理人員能夠訪問這些對入站的資料的翻譯功能，並且讓他們也能夠對出站的資料進行類似的翻譯，這些使得Anti-DDoS WAF+設備成爲了一款強大的資料翻譯工具。對於這一特性的兩個非常關鍵的使用案例，那就是IPv6與IPv4兩種網路之間的有效而近乎透明的翻譯，以及作爲資料傳輸到達內部Web伺服器之前的SSL加密終端。

IP翻譯服務的一個關鍵重要的好處就在於，消除了內部Web伺服器作業系統直接參與到IPv6互聯網或者IPv6內部網路，爲客戶節省了成本並消除了其複雜性。然而，客戶的Web應用和Web伺服器軟體最好還是應該升級到能夠合理處理IPv6的用戶端位址，特別是對其進行日誌記錄。

對於SSL的翻譯和終端，有兩方面的好處：首先，通過消除內部Web伺服器由於解密而擔負的CPU和記憶體的消耗，客戶可以享受到更加優越的性能表現，因爲這些工作都將被Anti-DDoS WAF+設備所代勞。但是有一點需要注意的是，Anti-DDoS WAF+設備與內部Web伺服器之間的通信必須盡可能直接地在互相信任的內部網路之間進行，以減少因爲之前加密傳輸以明文形式所消耗的大量的時間。

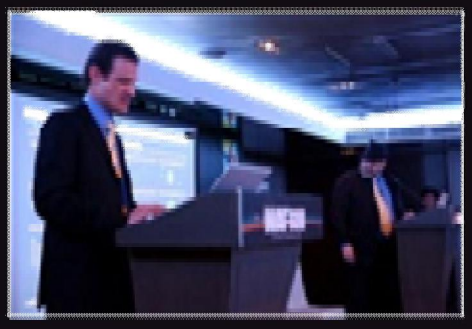
其次，使用了Anti-DDoS WAF+ 作爲SSL終端的的客戶，將享受到更加優越的SSL透明協議的保護，目前達到了最高的TLS 1.2的版本，並且Network Box將使之作爲我們SSL安全戰略的一部分而繼續不懈地努力。

這一項計畫將是一個長期的安全戰略規劃，也是Network Box的一項承諾，將爲客戶提供一系列基於SSL的且在閘道上執行的產品和服務。我們將在未來的 “In The Boxing Ring” 期刊上，更加深入地詳細介紹Network Box的SSL安全戰略。

Anti-DDoS WAF+ 全球發佈

2012年11月30日

Network Box正式發佈了最新的Anti-DDoS WAF+（Anti-Distributed Denial of Service Web Application Firewall Plus）系統，WAF-SCAN。這也是基於Network Box版本5這一平臺所即將在未來幾個月發佈的一系列系統中的第一個。謝謝所有支持和參加此次活動的你們。



活動期間，董事總經理Michael Gazeley簡要概述了Network Box具有關鍵里程碑的事件。緊接著是由首席技術總監Mark Webb-Johnson 和R&D主管 Nick Jones進行了詳細的解釋和現場演示。

2012年12月 新特性

在2012年11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：

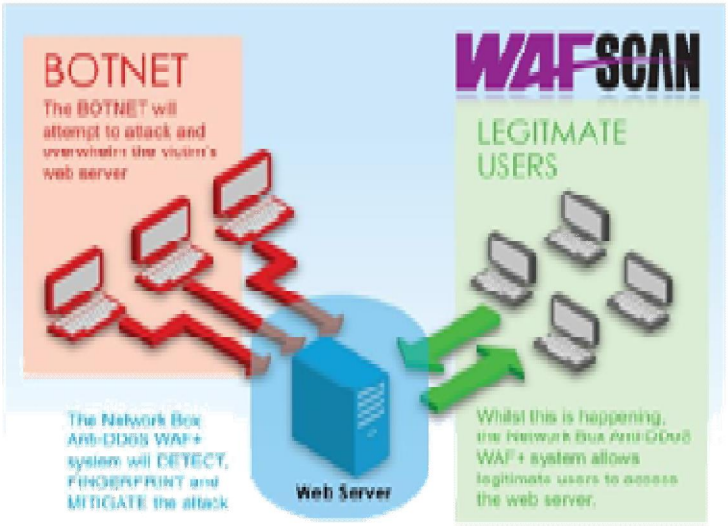
- 各種內部NOC系統的改進；
- 針對管理介面my.network-box.com的一些小修改
- 對每週報告PDF文檔排版佈局的一些小修改；
- NBRS-5.0在Box Office系統中的進一步支援；
- 一系列針對Box Office和支援系統的（主要是內部）功能增強。

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

Network Box的Anti-DDoS WAF+ (Anti-Distributed Denial of Service Web Application Firewall Plus) 系統, **WAF-SCAN**, 是一款具有高可制訂性安全管理設備（或可選的虛擬/基於雲端的設備），可以針對HTTP/HTTPS會話應用一整套嚴格的預配置的規則，以使Web伺服器免於受到外部攻擊。



幾個關鍵的功能：**Anti-DDoS攻擊防護**, **Web應用防護**以及**IPv4到IPv6 / IPv6到IPv4跨協議橋接器**。這也是基於Network Box版本5這一平臺所即將在未來幾個月發佈的一系列系統中的第一個。

NOVEMBER 2012 NUMBERS

Key Metric	#	% difference (since last month)
PUSH Updates	534	+13.1
Signatures Released	382,104	+0.4
Firewall Blocks (/box)	961,385	+6.2
IDP Blocks (/box)	121,483	-13.5
Spams (/box)	11,448	-10.9
Malware (/box)	1,441	+43.7
URL Blocks (/box)	195,584	+21.5
URL Visits (/box)	4,880,160	+11.1

NEWSLETTER STAFF

Mark Webb-Johnson
Editor

Michael Gazeley
Nick Jones
Kevin Hla
Production Support

Network Box HQ
Network Box Australia
Network Box UK
Network Box USA
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