
## 來自 Network Box 首席技術官

## Mark Webb-Johnson 的技術資訊

### Welcome

歡迎閱讀 2012 年 3 月刊的《In The Boxing Ring》。在本期中，我們的重點內容是 WAF（Web 應用防火牆）。

本月刊中，在第 2、3 頁，我們詳細介紹了 Network Box NBRS-5.0 的 WAF。WAF 可以被認爲是一個非常特別的一種入侵防禦系統和/或防火牆，專門用於針對 Web 伺服器及其運行的通過 HTTP 協定進行訪問的應用程式提供保護。

它是通過對不可信（不乾淨的）的 Web 用戶與可信（乾淨的）Web 伺服器之間的交互流量進行診斷。它通過完全地解碼 6 個階段的 HTTP 協議交互，以及在每個階段執行保護策略：入站連接，請求頭，請求主體（適用於某些請求），出站連接，回應頭，回應主體。

第 4 頁詳細公佈了本月 NBRS-3.0 的星期二補丁的特徵和修正。爲了可預見的未來（幾年之內）我們將繼續發展和支持 NBRS-3.0，這一頁是用來讓你瞭解我們的核心產品發生了什麼。

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 3 月

## 本 刊 概 要

**2-3.**
**Web應用防火牆**
WAF可以被認爲是一個非常特別的一種入侵防禦系統和/或防火牆，專門用於針對Web伺服器及其運行的通過HTTP協定進行訪問的應用程式提供保護。

**4.**
**2012年全球資訊安全優秀獎**
Network Box 於2012年第八屆全球資訊安全優秀獎中，以我們的Z-Scan零日反病毒系統榮獲“金融及銀行業安全產品與解決方案”類獎項。

**4.**
**2012年3月 新特性**
這個月的補丁星期二將會對NBRS-3.0的新特性和補丁修復進行發佈。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。


## Web 應用防火牆

幾乎每個禮拜，在與客戶提及 Network Box 前景時，都會就關於他們面向互聯網的 Web 伺服器上運行的應用程式方面給予關注。通常來講，安全掃描或者 PCI 脆弱性評估顯示了傳統應用中存在的突出問題，而要通過它們自身來解決修復應用程式中所存在的問題，也是非常困難和不經濟的。

雖然 NBIDPS 入侵防禦系統（以及其它類似的技術）本身可以在保護 Web 伺服器方面有一定的顯著效果，但是在保護伺服器上自訂應用程式方面的能力卻是非常有限的。雖然普遍的攻擊類型可以被檢測並抵禦，但是在針對自訂的應用程式的自訂攻擊，大部分的入侵防禦系統卻依然是無能爲力的。

然而，現在另外一種類型的保護便應運而生了——Web 應用防火牆。在這兩個部分的文章中，我將談論這項技術以及如何應用到現實網路環境中。在本期當中，我會大概講一下技術本身的概述，在下期月刊中，我將進行細節的描述。

## 什麼是 Web 應用防火牆？

WAF 可以被認爲是一個非常特別的一種入侵防禦系統和/或防火牆，專門用於針對 Web 伺服器及其運行的通過 HTTP 協定進行訪問的應用程式提供保護。

Firewall 可以被看成是 Web 訪問 tcp/80 埠的開關，而入侵偵測系統是對通過 tcp/80 埠的資料流程量進行普遍性的缺陷與漏洞檢測，而 Web 應用防火牆則超越了前面兩者，它通過完全的解碼 HTTP 協議以及通過應用策略來進行協議請求與回應。

## 爲何不能只啓用 HTTP 入站的反病毒功能？

這是一個會經常被問及的一個問題。尤其是對上傳到伺服器上的檔的掃描。

將“乾淨的”web 用戶（通常是 LAN 和 DMZ 的用戶）針對互聯網上“不乾淨的”惡意 web 伺服器保護起來，這是 Network Box 的 HTTP 反病毒代理所需要做到的功能，並且其一直表現優越。而要將您 LAN 和 DMZ 區“乾淨的”web 伺服器針對 NET 區“不乾淨的”web 訪問用戶的攻擊中保護起來，如果使用同樣的基本的 HTTP 協議，那麼這將帶來一個結果完全不同的挑戰。從技術上來說，這被稱爲“反向代理”，但遺憾的是，由於其需要去請求而並不是那麼容易實現的。

即使我們可以克服正向代理和反向代理所存在的問題，而其實反病毒只是這些問題中的一小部分而已。

## 那麼，Web 應用防火牆是如何工作的？

是通過對不可信（不乾淨的）的 Web 用戶與可信（乾淨的）Web 伺服器之間的交互流量進行診斷。它通過完全地解碼 6 個階段的 HTTP 協議交互，以及在每個階段執行保護策略：

**1、 入站連接**

來自 Web 訪問用戶端的連接到達之後，被路由到 Web 伺服器。在這個階段，入站連接的詳細資訊（例如源位址和目標位址）將被獲得，然後會將之與此源位址的統計歷史相關聯，再決定是否允許此源發起請求或者拒絕其建立連接。

**2、 請求頭**

在這個階段，來自 Web 訪問用戶端的請求被接收並且解碼和分析。報頭內容將被進行分析並且受到規則保護，然後將會被決定是否允許此源發送其請求主體（如果需要的話）。

**3、 請求主體（適用於某些請求）**

在這個階段，整個的請求均已被接收並且解碼和分析。報頭內容及其請求主體將被分析和受到規則保護，然後將會被決定是否允許此源可以繼續與 Web 伺服器建立連接。

**4、 出站連接**

在這個階段，連接詳情已被獲知並且受到規則保護，這樣將會就否允許此源與目標伺服器建立連接，並且繼續發送請求報頭和主體到目標伺服器做出決定。

一些 Web 應用防火牆可以配置推遲出站連接階段，直到請求包頭和主體被接受，或者在入站連接已被接受的情況下立即建立連接（因此，在階段 1 之後和階段 2 之前，就可以立即進入階段 4）。

**5、 回應頭**

被保護的 Web 伺服器將會對請求報頭和主體進行回應並發出回應報頭。這些報頭將會被解碼、分析並且受到規則保護，然後被決定是否允許伺服器發送這些報頭給到此用戶端。

**6、 回應主體（適用於某些回應）**

受保護的伺服器在發出響應報頭後將會發出響應主體。該主體將會被解碼、分析並受到規則保護，然後被決定是否允許伺服器向該用戶端發送此回應主體。

## 安全模式

Web 應用防火牆一般會提供多種安全模式以供選擇。以下列舉了比較常用的五種：

**1、漏洞防護**

Web 應用防火牆有強大的規則語言，並且會針對最新發現的漏洞和技術不斷地進行更新，以提供漏洞補救並支援客戶的內部補丁發佈週期。保護系統其實可以在防火牆上進行修補，而不需要在相關影響到的系統自身上安裝補丁包；保證被保護系統的安全，直到生產廠家的補丁包發佈並被應用。

**2、出站保護**

Web 應用防火牆可以對出站流量執行策略。這通常用於防止資料洩漏，塗改檢測以及其它類似的一些功能。再與其它的一些模組（例如 Web 伺服器反病毒模組以及防 LAN 網路感染等）相結合，這就組成了一套有效的出站防禦。

**3、被動安全模式**

被動安全模式是一種掃描入站請求以及應用保護標準（包括特徵碼、規則以及啓發式）的方法，以檢測協議異常，異常行爲，漏洞和其他常見的攻擊。攻擊源可能需要集成其它安全模組（例如網路 DDOS 防護）以應對這些惡意流量，或者這些流量本身能夠簡單地被記錄、丟棄或者殺毒。

**4、DDOS/DOS 模式**

DDOS/DOS 模式通常跟蹤使用模式，以確定攻擊源抑制方法並加入黑名單。使用的技術範例包括連接速率限制，請求速率限制，被動回應速率限制，重複請求限制以及請求時間限制。

**5、主動安全模式**

主動安全模式需要一系列的規則定義，以明確哪些應用和流量允許通過，而所有其它不合格的流量則被拒絕掉。

## 日誌記錄

最現代的 Web 伺服器的日誌記錄功能，也只是主要關注於記錄足夠的資訊以達到統計分析的目的。尤其是 POST 請求的報頭和主體，通常是不被記錄的，這樣就做到攻擊行爲的法理分析。

Web 應用防火牆包括了廣泛的、可配置的日誌記錄功能。它通常可以將整個的請求和回應各自的報頭和主體完整地進行記錄。

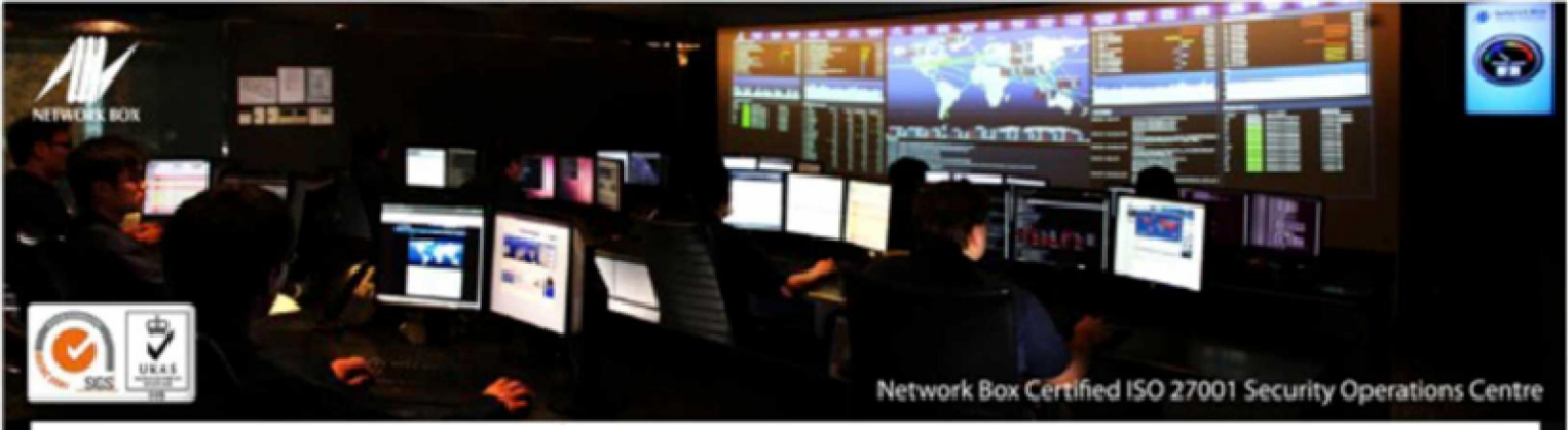
## 協議驗證與策略

Web 應用防火牆通常都有驗證和執行 HTTP 協議的技術，以說明管理員定義全面的協議策略。例如包括參數的數量、參數的長度、大小限制、Cookie 的限制等等。

網路防火牆可以允許或禁止 tcp/80 埠，而 Web 應用防火牆則可以基於對 HTTP 協議的深度理解以及強大的配置語言，允許或禁止請求和回應。

## 協議驗證與策略

我希望以上關於 Web 應用防火牆的介紹能給您很好的認識，並且真正給您帶來幫助。下個月，我們將給您帶來 NBRS-5.0 的一個特別的 Network Box 的 Web 應用防火牆，以及它是如何給您的實際網路解決安全方面的問題。




## 2012 年 3 月 新特性

在 2012 年 3 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：

·多個內部 NOC 系統的提升；

·my.network-box.com 中 email 地址對個人的白名單和黑名單驗證的增強；

·對在 my.network-box.com 的郵件跟蹤資訊頁面中影響到一些病毒郵件檢疫發佈的問題的一個修復；

·在 my.network-box.com 中 SSL 證書續期；

·功能變數名稱解析服務的安全修復；

·在 Box Office 系統中對 NBRS-5.0 的支援；

· 多個（多是內部的）針對 Box Office 和支援系統的提升。

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 年全球資訊安全卓越獎

Network Box 於 2012 年第八屆全球資訊安全卓越獎中，以我們的 Z-Scan 零日反病毒系統榮獲“金融及銀行業安全產品與解決方案”類獎項。

2012 年 2 月 29 日，許多來自全球在安全行業領先的專家們參加了 2012 年第八屆全球資訊安全卓越獎入圍及獲勝頒獎慶典。這是在安全領域載譽全球的一個獎項，專門對在安全領域各個方面取得成就進行表彰。

資訊安全產品指南贊助商領導會議與全球博覽會，在保證終端使用者在針對數位資源保護方面做出選擇提供參考，並發揮了至關重要的作用。對於那些堅持保持安全威脅通報以及能夠採取防禦措施的安全產品提供商均會被明確入圍。在這個指南中，你會發現非常豐富的資訊，包括現在及以後的技術、最好的部署方案、人與技術所形成的資訊安全以及便於做出最相關安全決策的獨立產品評估。資訊安全產品指南獎項對在資訊安全的所有方面做出卓越成就的給予認可和榮譽。

想要獲得更多的關於資訊安全產品指南的相關資訊，請登錄 http://www.infosecurityproductsguide.com/index.html。

### 2012 年 3 月份資料

| 關鍵指標 | 數據 | 與上月差比 |
|---|---|---|
| PUSH 升級數 | 393 | -29.8 |
| 特徵碼發佈數 | 466,192 | -11.0 |
| 防火牆攔截數(每 BOX) | 872,356 | +6.7 |
| IDP 攔截數(每 BOX) | 163,190 | -26.8 |
| 垃圾郵件數(每 BOX) | 15,660 | +8.4 |
| 惡意軟體數(每 BOX) | 293 | 13.8 |
| URL 攔截數(每 BOX) | 168,697 | +17.8 |
| URL 訪問數(每 BOX) | 4,303,241 | +27.8 |


### 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