來自 Network Box 首席技術官

Mark Webb-Johnson 的技術資訊

Welcome

歡迎閱讀2012年5月刊的《In The Boxing Ring》。在這一期當中，重點的內容是Network Box NBRS-5.0 的安全套接協議層（SSL）。

在第2、3頁，我們詳細描述了 Network Box NBRS-5.0 的安全套接協議層（SSL）。其根本的缺陷在於， SSL 應用（如 Web 流覽器）通常取決於用戶接受或拒絕證書的問題。

NBRS-5.0 可以工作與兩種模式之一來爲使用者提供保護：SSL 旁路模式和透明的 SSL 攔截模式。大多數行業競爭者的系統都只能工作於第一種模式，並且對 SSL 加密的流量無法提供保護。而那些提供了第二種模式的也只是提供了有限的方式。Network Box 完全支援這兩種模式，並允許一個非常精細的基礎上作出選擇的模式。

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
2012 年 5 月

本 刊 概 要

Network Box NBRS-5.0 的安全套接協議層（SSL）

Network Box NBRS-5.0 包括了廣泛的對安全通訊端層（SSL ）協定的支援。該協定是安全互聯網通訊的核心，用於許多更高級別的協定（如使用 HTTPS， SMTPS ， POP3S 等），但大多數實現起來卻存在根本性的缺陷。

有關“用戶”的問題

其根本的缺陷在於， SSL 應用（如 Web 流覽器）通常取決於用戶接受或拒絕證書的問題。例如，當用戶訪問一台遠端的 Web 伺服器，而此伺服器的 SSL 證書卻已經過期了，那麼用戶就會被詢問是否接收或拒絕連接。或者，當遠端 Web 伺服器名稱與證書簽名授權的名稱不相符時，用戶同樣會被詢問是否接收或拒絕連接。

多項研究表明，用戶將忽略這些警告，並按下任何按鈕，他們認爲他們想去的地方。現實世界的結果還表明，眾多的用戶在他們遇到選擇時，甚至無法確定哪一個是安全的流覽器連接，而且大多數人連看都不看這些用於幫助防止釣魚攻擊的擴展驗證（EV ）證書的資訊。

在一篇名爲《狼來了：SSL 警告有效性的實證研究》的研究報告中，可以找到一個很好的情況總結。訪問位址：http://lorrie.cranor.org/pubs/sslwarnings.pdf

NBRS-5.0 的方法

NBRS-5.0 可以工作於爲使用者提供兩種保護模式中的一種：

1、SSL 旁路模式 —— SSL 通訊都留下完整和旁路保護機制。

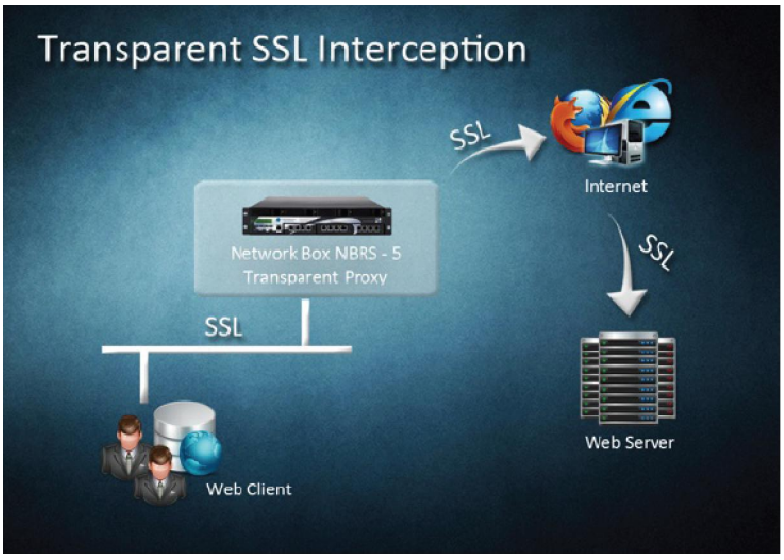
2、透明 SSL 攔截模式 —— SSL 通信將被截獲下來並且進行透明代理，以使 Network Box 能對加密流量進行保護並強制執行證書策略的規則。

大多數行業競爭者的系統都只能工作於第一種模式，並且對 SSL 加密的流量無法提供保護。而那些提供了第二種模式的也只是提供了有限的方式。Network Box 完全支援這兩種模式，並允許一個非常精細的基礎上作出選擇的模式（例如，基於每用戶、每網站分類、每網站等）。這樣的政策是一種有效的機制，用來在 SSL 會話保護的情況下處理隱私問題。

讓我們具體地來看看 NBRS-5.0 的透明 SSL 攔截模式是如何對流量進行保護的。

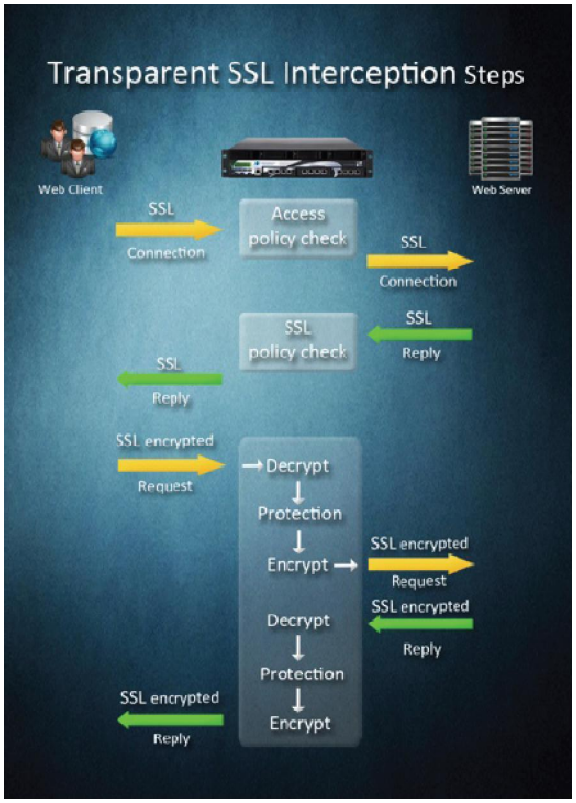
NBRS-5.0 的 SSL 透明攔截模式

第一個圖顯示，當在訪問一個 SSL 保護的互聯網伺服器時，通過 Network Box 來對一個 web 用戶端進行保護的典型的流覽器會話的示例。在局域網的 web 用戶端的連接源，在閘道處由 Network Box 進行透明代理，並且指向互聯網的 web 伺服器。這種通信通常由 tcp/443 埠發起，但是通過應用程式識別，最初的 SSL 協商可以自動識別爲透明的攔截，然後協議自行從加密的資料流程中做出判決。



第二個圖顯示了通信的資料流程。首先，Network Box 對出站的 tcp/443 埠的請求進行攔截，並且透明代理到目標伺服器。通常的策略審核都可以在這個階段進行應用。通過對用戶端和伺服器之間的通信進行審查，Network Box 確定這是一個 SSL 通信。如果配置的是第二種模式的透明 SSL 攔截模式的話，那麼 Network Box 將會先對伺服器端提供的證書與自身的 SSL 策略進行審查驗證。如果證書是可接受的，那麼 Network Box 就會生成自身匹配的證書呈現給用戶端，這種證書是由 Network Box 自身的憑證授權簽名頒發的，並且被用戶端所信任。

在這裡，有兩個 SSL 流——一個是 Web 用戶端與 Network Box 之間的，由 Network Box 自身來進行加密和認證，另一個是 Network Box 與遠端 Web 伺服器之間的。這樣一來，當已加密的資料流程從用戶端傳輸到 Network Box 時，Network Box 有能力進行解密並對資料進行安全保護，然後再將其進行加密並傳輸到伺服器上。同樣的，對伺服器的回應資料 Network Box 也能對其進行解密並進行安全保護，然後重新加密並傳輸給用戶端。



最終的結果是：

a · 是否接受遠端伺服器憑證的驗證和決定就取決於 Network Box——根據行政需要所定義的策略而定。

b · 高級證書驗證技術可以作爲一個集中實施政策。

c · 是否執行透明 SSL 攔截的第 2 中模式也是由 Network Box 來決定——同樣也是根據行政需要所定義的策略而定。

d · 去到/來自遠端伺服器的請求/回應，都將被當作未加密的流量和物件進行完全應用程式識別檢查。

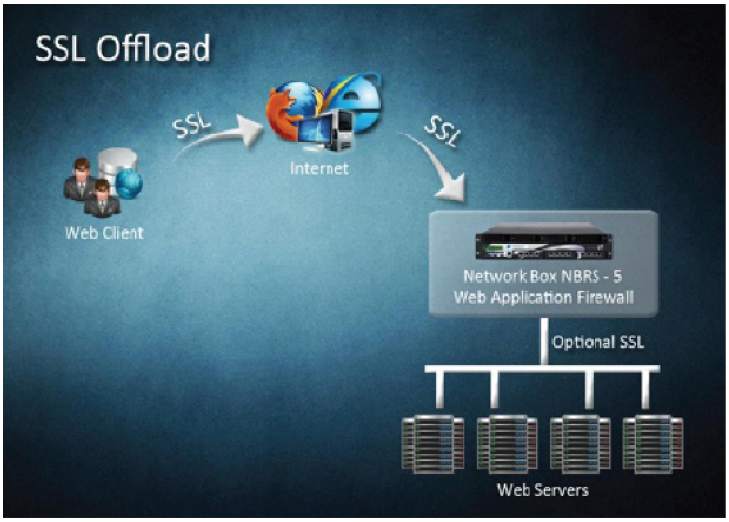
e · 提供充分的保護（包括反病毒保護等），甚至對 SSL 加密的流量，以及策略/保護規則的應用。

特別需要注意的是，應用程式識別在容器（SSL）和內容（被保護的 SSL 會話的解密明文流量）兩個層級上都可能發生。但這些對於經過該網路的安全不會產生任何影響。

NBRS-5.0 對 DMZ 區 Web 伺服器的保護

針對互聯網上 SSL Web 伺服器上惡意的內容將內網 Web 用戶端保護起來，同樣的，NBRS-5.0 也支持 Web 應用防火牆（WAF）中的 SSL 功能，用於針對來自互聯網或內網 Web 用戶端的惡意攻擊將 DMZ 區的 Web 伺服器保護起來。這是通過 SSL Offload 來實現的，正如第三個圖中所示。

SSL Offload 是通過將 SSL 伺服器憑證放在 Network Box 的 WAF 功能中來進行工作的。這樣 Network Box 就可以接受來自用戶端發起的 SSL 連接，然後解密進來的請求資料，以在將之提交到受保護的 Web 伺服器之前進行安全保護。同樣的，來自 DMZ 區 Web 伺服器的回應資料，在進行加密和發送給請求用戶端之前，也會通過策略匹配以及其它的保護機制對之進行審查。



管理人員可以針對是否對 DMZ 區的 Web 伺服器與 Network Box 之間的資料鏈使用 SSL 進行選擇。這可以基於安全、性能與管理負荷來進行權衡決定。因此，完全功能的 WAF 功能就達成了哪怕是 SSL 安全連接，也不會對其資料在互聯網上傳輸的安全性產生任何影響的目標。

用戶端的證書問題

這種 SSL 攔截的方法（不論是透明 SSL 攔截，還是 SSL Offload）所存在的問題就在於，SSL 用戶端證書需要進行特殊的處理。這是由於 SSL 協議本身的設計所決定的。

對於 SSL Offload，Network Box 可以配置爲繞過攔截用戶端證書的 SSL 連接，或者在將請求的詳細資料傳送到 Web 伺服器之前，Box 自身對用戶端的證書進行接受並驗證。

對於透明 SSL 攔截，Network Box 可以配置爲繞過攔截用戶端證書的 SSL 連接。

在現實世界裡，SSL 用戶端證書 SSL 用戶端證書通常用於密切的業務合作夥伴之間的信任載體，而對於上述的一些限制也是在極少數情況下所需要考慮的。

總結

Network Box NBRS-5.0 包括了 SSL 協定的廣泛支援。它支援管理人員對 SSL 通信實施策略控制，並提供了有效的機制，對 SSL 流量進行識別、保護以及策略的執行。

2012 年 5 月 新特性

在 2012 年 5 月 1 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 中對 NBRS-5.0 的進一步支持；
- 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 榮獲多項大獎

2012 年 PC3 白金品牌獎

2012 年 4 月 17 日，Network Box 在統一威脅管理類別中贏得 2012 年白金品牌獎。這是一個很具權威的獎項，它是由 PC3 雜誌、APPS 雜誌和 IP Pro 雜誌的讀者通過線上的投票方式所評選決定的。

2011 年 BQJ 超級品牌獎

4 月 14 日，Network Box 贏得商業商雜誌的最佳超級品牌獎。該獎項是在資訊和通信技術博覽會上頒發的。

2012 年 Linux Pilot Editor 的最佳選擇

4 月 14 日，Network Box 在最佳的安全管理服務方面贏得了 2012 年 Linux 及 OSS 獎，該獎項也是在資訊和通信技術博覽會上頒發的。

香港貿發局國際資訊和通信技術博覽會（2012.4.13-16）

今年在香港 ICT 博覽會已經結束了。非常感謝大家前來參觀我們的展位。同時也非常的榮幸，能通過這個機會向大家展示我們全新的 Web 應用防火牆、IPv6 橋接器以及零日反病毒技術。

2012 年 5 月份資料

關鍵指標	數據	與上月差比
PUSH 升級數	599	+4.7
特徵碼發包數	424,446	-6.4
防火牆攔截數(每 BOX)	896,789	+6.1
IDP 攔截數(每 BOX)	129,261	-11.3
垃圾郵件數(每 BOX)	14,276	-10.5
惡意軟體數(每 BOX)	580	+174.9
URL 攔截數(每 BOX)	160,154	+5
URL 訪問數(每 BOX)	4,045,348	-1.3

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