In The Boxing Ring

Network Box Technical News from Mark Webb-Johnson, CTO Network Box

IN THIS ISSUE

2.
NETWORK BOX VIRTUAL PRIVATE NETWORK (VPN)
What a true SSL VPN is and how to deploy it. With the July 2009 Patch Tuesday firmware update, Network Box has fully integrated our SSL VPN to the Network Box Certificate Authority.

3.
NETWORK BOX SQL INJECTION ADVICE
Fighting SQL Injection is tough; this article provides some insights.

3.
BING.COM AND SAFE SEARCH
SafeSearch for Bing.com (beta) appears too good to be true.

4.
JULY 2009 FEATURES
The ongoing deployment of our recently released features and enhancements.

Welcome

歡迎您到 2009 年 7 月版的 'In the Boxing Ring'。在此版本，我們把重點放在如何最好地保護您的虛擬專用網路（VPN）。請轉到第 2 頁瞭解的詳細資訊。

我們還解決日益關注針對網站的通過 SQL 注入的一種安全威脅，它永遠不能 100%地在閘道處被攔截。讓我們看看 SQL 注入是什麼以及你可以做些什麼來保護自己。在第 3 頁會提供給您進一步的資訊。

又在第 3 頁，我們將檢視一下 Bing.com 試用版，它是微軟公司新推出的'必應'引擎，和談論一下安全搜索。

在 7 月的特別欄目中，我們也有通常的針對 NBRS-3.0 系統的分配更新，增強的掃描引擎，對全球監控系統的進一步支援，和性能方面的改進。轉到第 4 頁瞭解詳情。

和以往一樣，如果您有任何的回饋，意見或者建議，我們都歡迎您隨時提出來。您也可以通過發送郵件到我們的郵件列表：nbhq@network-box.com 聯繫我們。或者當您下次在香港市區的話來隨時來我公司辦公室進行參觀指導。

您也可以通過加入或訂閱我們的安全響應 Twitter 和我們保持聯繫，網址是：

twitter.com/networkboxhq

Mark Webb-Johnson

CTO, Network Box Corporation

July 2009

NETWORK BOX

Network Box Virtual Private Network (VPN)

虛擬專用網路（VPN）是一個不同網路節點之間的虛擬鏈路，它可以跨越一些較大的網路（如Internet ），而不是運行在一個單一的專用網路。虛擬網路的鏈路層協定被認爲是通過傳輸網路的隧道。

VPN是站點到站點的隧道，這樣它們運作在ISO堆疊的最底層。

現在業界有一種誤解（至於是有意的或以其他方式，要看你自己如何來看待），將真正的SSL VPN和具有SSL功能的WEB伺服器和代理伺服器混爲一談。

關於SSL只能在應用層加密流量的說法也是不正確的。

真正的SSL VPN在ISO棧的最底層加密流量，因此，它可以以透明的方式來保護所有網路（和應用）的流量。SSL代理和埠轉發只是在一個時間爲個別指定的應用加密流量。這些都不是真正的VPN，他們的保護作用受到很大的限制。

在很好地支援PPTP及IPSec協定的同時，Network Box還包含一個開放源碼的SSL VPN伺服器和用戶端，即所謂的“Open VPN ”（詳見http://www.openvpn.org/）。

這是一個真正的SSL VPN，它建立了鏈路級別的加密，並提供隧道兩個端點之間的認證以保護所有通過它（和應用無關）的流量 。因此，它需要安裝用戶端軟體，目前用戶端軟體可用於Microsoft Windows ，蘋果OSX和Unix系統。

從安全角度來看，使用SSL證書（一種基於PKI的公鑰基礎架構）可以提供最高等級的安全。但是，管理這些SSL證書，以及用戶端軟體和配置檔，已被證明需要大量的管理工作，並限制這一技術的部署。

隨著2009年7月份週二補丁的發佈和固件的安裝，Network Box已解決了管理SSL VPN證書，用戶端軟體和配置檔的問題，並且充分整合我們的SSL VPN到Network Box證書頒發機構。這樣就可自動分發用戶端證書（以及安裝說明，自定義配置檔，和其他輔助檔），分發的管道可以通過電子郵件或通過基於Web介面的Network Box Mail Portal郵件門戶網站系統。

Network Box也提供一套完整的證書吊銷列表（CRL），以便即時撤銷用戶端訪問許可權（以每個用戶端爲基礎），以及一個強大的範本系統，它可以用於自動生成每個用戶的配置檔和安裝指示。

要給SSL VPN用戶端簽發證書，授權管理員使用MY.NETWORK-BOX.COM管理門戶。輸入用戶的電子郵件位址，並選擇分發管道是通過電子郵件或郵寄門戶網站，系統會爲最終用戶設置自己的SSL VPN用戶端自動生成和分發一切必要的檔。證書的延續和證書的撤銷處理也使用相同的集成機制。

可選的郵件門戶分配機制（在郵件門戶網站的主頁上和電子郵件報告中）允許用戶獲得證書下載，並允許下載先前發出的證書。

Network Box建議針對站點到站點和用戶端遠端接入這兩種方式都選用SSL VPN。該議議對通過NAT設備有很好的支援並且有非常靈活和強大的配置選項。

Network Box SQL Injection Advice

在我們的第一期In The Boxing Ring通訊中（是一年前的2008年7月發佈的），我們談到了SQL注入的問題，在此周年之際，我認爲是有必要再次談論它一下，因爲我們仍然看到有大量的這類攻擊氾濫（無論是在新聞和在互聯網中）。

想在閘道處停止SQL注入攻擊是極難的，由於攻擊對應用程式無依賴性，因此，通用入侵檢測系統/入侵防禦規則只可以提供有限的防禦。雖然 Network Box中有許多的IDS和IPS的規則，應用層安全（通過嚴格的輸入資料驗證）才是最終能阻止這些類型的攻擊的唯一途徑。

讓我舉一個針對這種攻擊的一個例子。比方說，Web伺服器運行的應用程式（稱爲news.cgi ）採用單一的參數爲' id '來檢索新聞故事：

http://target.com/news.cgi?id=22

通過下面這個 SQL 表單來抓取故事：

"select article from news where id=" . $id

接著生成如下SQL申明語句（示例）：

select article from news where id=22

現在，如果一個攻擊者出於某種目的修改' id '參數的話會怎樣呢？舉例來說，如果他發出：

http://target.com/news.cgi?id=22;truncate%20table%news

由此產生的SQL語句將成爲：

select article from news where id=22;truncate table news

其結果將刪除掉所有的新聞故事。

所以，你將如何阻止這種攻擊呢？主要有三種方法：

1) 使用帶參數的SQL語句（如上述聲明變成"select article from news where id=?" 並且'id'要作爲參數傳遞）。
2) 執行嚴格的參數驗證（例如，檢查'id'參數的值，以確保它是一個數字）。
3) 在插入SQL申明之前加入退出參數的語句（用以解決刪除的問題，如通過嵌入';'和引用——在這種情況下，SQL語句就變成爲" select article from news where id='22;truncate table news' " ）。

這僅僅是一個例子，SQL注入攻擊可以借助很多種變數。這些Web應用程式的脆弱性漏洞（如上述news.cgi所表明的）可以造成嚴重破壞，包括重要資料的丟失或篡改。

對於那些通用的，眾所周知的Web應用程式，已知的漏洞已經被公佈，閘道或邊界保護（如Network Box）系統可以應用入侵檢測/入侵防禦規則來檢測和阻止利用已知的漏洞的攻擊。但對私有或客戶自定制的Web應用程式，一般來講是無法防禦的。

所有NBRS-3.0 Network Box設備都有兩個IDP模組（命名爲HTTP-S-SQLINJECT和HTTP-S-SQLINJWORM）提供針對特定應用和特定蠕蟲的SQL注入 攻擊防範，早在2008年7月我們已經將這些新的保護模組釋放給我們的所有客戶Box之中。然而，如前所述，通用入侵檢測系統/入侵防禦規則只可以提供有 限的防禦，應用層的安全（通過進行嚴格的輸入驗證）才是最終能阻止這些類型攻擊的唯一途徑。

我們建議有提供公共Web伺服器的客戶（特別是那些在互聯網上開放使用的）進行腳本和Web伺服器上應用程式的審查，以確保它們安裝了最新的補丁，以免受到這類型的攻擊。

Bing.com (beta) and Safe Search

在2008年9月發行的*In the Boxing Ring*中，我們講到了穀歌和雅虎的安全搜索SafeSearch。今天，一種新的搜索引擎，Bing.com（必應），已經加入到了搜索引擎巨頭行列中。它的創作者是微軟公司，作爲其"決策引擎"，Bing.com提供的搜索引擎會提供非常簡化明瞭的搜索結果。除此這外，它還提供了如下安全搜索SafeSearch功能：

*嚴格-從您的搜尋結果中過濾色情文字，圖像和視頻。

*中度-從您的搜尋結果中過濾色情圖片和視頻，但不過濾文字。

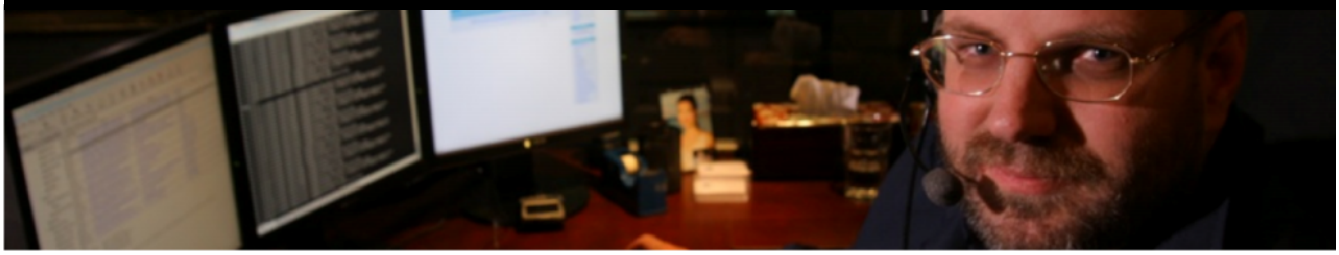
*關閉-從您的搜尋結果不過濾任何露骨的文字，影像或影片。

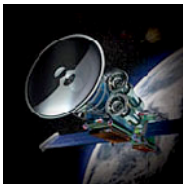
雖然標準的SafeSearch篩選水準相當不錯，但是像其宣稱的那樣，Bing.com的安全功能似乎離中度設置太遠。

隨著增加搜尋關鍵字的細度，應該引起預警，儘管這些關鍵字有多重意義，例如，當我們搜索"mature adult" （高齡成人，表示年紀更大一些的成人）時，Bing.com回應是："我們沒有返回結果，因爲您的安全設置被設置爲嚴格。"

和從搜索結果中（如穀歌和雅虎的做法）消除不安全結果不同 ，Bing.com則會自己停止整個不安全的搜索請求。這是一個關鍵的差異，並且嚴重限制了Bing.com作爲一種安全的搜索引擎的可用性。然而，Network Box現在已經擴展了政策引擎中集成的安全搜索，不僅包括穀歌和雅虎，也新加入了Bing.com。通過集成這三個搜索引擎來提高搜索結果的安全水準和貫徹執行SafeSearch功能，進而使得企業安全政策的規定得到強制執行。

但迄今爲止，Bing.com安全搜索的成績，還是令人失望，和其他搜索引擎相比缺乏可操作性和控制力度。





July 2009 Features

On Tuesday, 7 July 2009, we will be releasing a number of improvements to the mail scanning system, primarily to further improve anti-spam performance. And also new GMS health metrics for the correct operation of envelope verification and the customer LDAP server will be released.

Revisions to the MY.NETWORK-BOX.COM administrative interface and Mail Portal have been made to restrict users from whitelisting themselves, or administrators from whitelisting their own domain, by accident.

Additionally, we also release support for SSL Certificate bundles (including template configurations, instructions and software clients) in the Network Box Certificate Authority, MY.NETWORK-BOX.COM and Mail Portal systems.

And as always, we will be releasing general performance improvements and functionality enhancements.

The above changes will not require any impacting service or device restarts, and should not cause any significant interruption to device operation. The regional NOCs will be conducting the rollouts of the new functionality in a phased manner.

Should you need any further information on any of the above, please contact your local NOC. They will be arranging deployment and liaison.

July Hint

對於任何公司來講，尋求客戶，資訊是關鍵。要訪問此資訊，尤其是在虛擬的商業世界中， Web流覽器是使用最廣泛的工具。但大多數人們不知道默認提供的Web流覽器還有可替代的選擇。例如，Firefox、Safari和Opera。

所有這些流覽器都可以免費下載和使用；每種還提供了大致相同的功能。更重要的是，每種流覽器提供了一些略微不同的用戶體驗，這將可以讓每個人以不同的方式利用。

爲了幫助您擴展您的業務工具，最近的Safari 4和穀歌Chrome已經可用了，另外最新的Firefox 3.5也剛剛被發佈。這些流覽器提供的Javascript性能大大超過其對手IE7和IE8。

結束語

感謝您支援Network Box，並繼續將您的網路安全託付給我們進行管理服務。我希望這份通訊月刊對您有用。如果您有任何建議，我們都非常歡迎，您可以向當地的NOC或客戶經理反映；如果您有其他需求，也請別猶豫，馬上與我們聯繫，尋求協助。

Mark Webb-Johnson
CTO, Network Box Corporation
July 2009

JUNE 2009 NUMBERS

Key Metric)	#	% difference (since last month)
PUSH Updates	1,083	+14.7
Signatures Released	204,873	-38.7
Firewall Blocks (/box)	637,305	+3.1
IDP Blocks (/box)	157,576	+13.2
Spams (/box)	73,136	-11.9
Malware (/box)	2,216	+22.8
URL Blocks (/box)	82,445	+17.4
URL Visits (/box)	3,080,726	+11.9

NEWSLETTER STAFF

Mark Webb-Johnson
Editor

Pauline Chiu
Michael Gazeley
Jason Law
Nick Jones
Production Support

Network Box Australia
Network Box Hong Kong
Network Box UK

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