In The Boxing Ring

IN THIS ISSUE

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

Welcome

歡迎您來到2009年6月版'In The Boxing Ring'。

在這一版，我們將要把重點放在Network Box新的網路入侵檢測與預防系統是如何運作在四個模式下的：前端IPS ，被動IDS，主動IDS和串聯的IPS。轉到第2頁瞭解詳細資訊。

隨著Network Box Office客戶門戶的推出，前幾期In the Boxing Ring中提供了相關的技術細節，本版將提供給您使用該系統的提示和小技巧。第3頁提供進一步的資訊。

還是在第3頁，我們將提供更多的關於PUSH技術的解釋和它的優勢。我們還宣佈了新的專利技術即HQPUSH系統，它在提供保護更新方面有更高的性能。

在6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4個新的垃圾郵件簽名類型的進一步支援，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

June 2009

NETWORK BOX

Network Box Intrusion Detection & Prevention

在2009年5月版In The Boxing Ring中我們宣佈開始測試一種新的入侵檢測和預防系統。我們的測試一直在進行，到目前這種新技術已經顯示出良好的效果。所以，這個月，我想給你更多關於它是什麼樣的技術以及我們將在哪里使用它的詳細資訊。

圖（1）表明，使用這種技術的一個典型的Network Box網路安全系統架構。資料流程量通過三個網路介面，接受五層Network Box的保護。

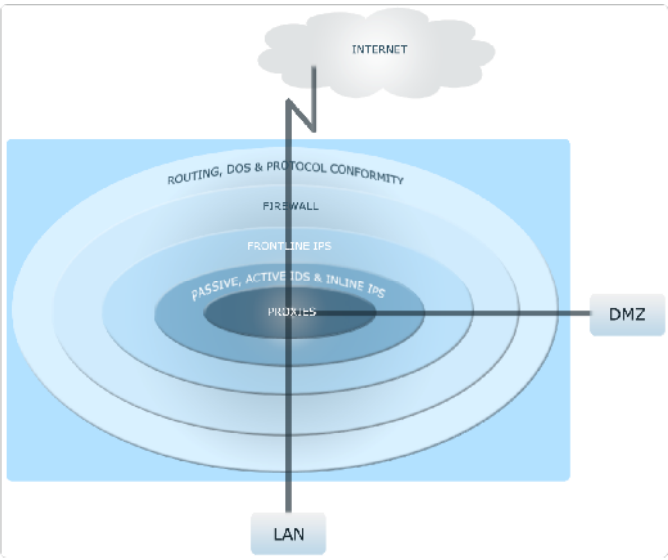


Diagram 1: Security Architecture of Network Box for a Typical System

1 ）第一層保護提供基本的路由，拒絕服務保護和協定一致性檢查。這一層的處理最接近硬體和提供針對路由、協定混淆和負載攻擊方面的保護。

2 ）第二個保護層是防火牆。在這一層，不符合安全策略的流量被防火牆封鎖。

3 ）第三個保護層是前端IPS系統。它可以非常輕便的，零延遲，防止蠕蟲，漏洞和其他此類的攻擊。

4 ）第四個保護層是新的NBIDPS系統。這一層包括被動入侵檢測系統，積極的入侵檢測系統和串聯的IPS，它使用先進的規則和協定/流解碼引擎。

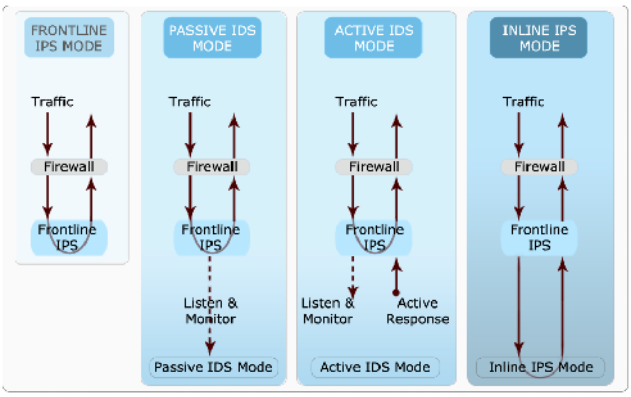


Diagram 2: New NBIDPS Engine – 3 Modes

5 ）第五保護層包含一組受保護的服務代理，具體的協定，如POP3，IMAP4，SMTP，HTTP和FTP。它們用來提供應用層保護，防止惡意軟體及垃圾郵件，以及對安全政策的嚴格執行。

通過將安全保護分開爲五個高度可配置的，但又可綜合應用的層次，Network Box能夠在預算有限的情況下提供最佳的安全和性能平衡。

在此基礎上，新NBIDPS系統採用開放源碼的Snort引擎。我們對它進行了大量的修改，以適應Network Box的安全模型，日誌記錄和管理框架。這樣，我們就可以使用行業標準格式的簽名代碼和啓發引擎，並爲我們提供了強大的規則語言，以及更多流和協議解碼器。

圖（2）展示了Network Box目前支援的四個模式。在被動和主動的入侵檢測系統模式中，引擎和網路通信流量分開運行，以儘量減少對性能的影響，並提供選項來限制監測網路的能見度。串聯的IPS模式允許網路通信流量以穿透引擎的方式運行，它提供應對攻擊的零延遲回應。

入侵檢測（被動和主動IDS）和入侵阻斷（IPS）系統在網路安全體系中有它們不同的位置。做爲業內第一，新的Network Box系統結合了四種辦法並將它們納入一個統一的平臺，可以使技術和工具以最好的方式適用於單個的設備。

這將是我們提供的一個不用另外花錢的增值服務，所有NBRS-3.0 FW+（或以上）的客戶都可以享用，也將成爲我們持續不斷地服務和監測性能的一部分，當然是在性能允許的情況下。Beta測試已經開始，我們估計將於2009年7月正式的發佈這個系統。

Network Box Office Customer Portal Hints

在上個月的In the Boxing Ring中，我們的討論包含有Network Box Office客戶門戶系統。這個快速概括的客戶門戶提供了一個單一，簡單而又強大的基於Web的用戶介面來管理一台或多台Network Box——在國家，區域和全球各個級別。

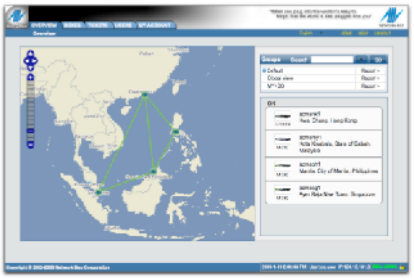


Fig. 1 – Overview Screen

它在全球正式的發佈時間是09年5月12日。

訪問客戶門戶的位址是：https://boxoffice.network-box.com。在輸入您的用戶名和密碼之後，你將看到綜覽畫面，它根據地理背景顯示出您的Network Box的網路連接圖。

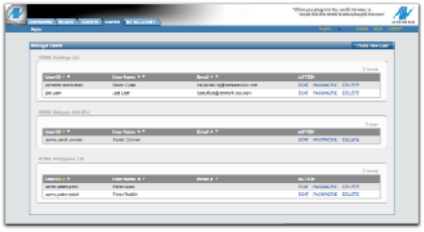


Fig. 2 – User Management

隨著客戶門戶網站的深入使用，我們想要提供給您在這個問題上的三個使用提示，以改善用戶體驗，並幫助您更好地利用門戶網站：

1）用戶管理模組：允許客戶預先指定的管理員，進行查看和維護Box Office用戶帳戶。

選擇用戶標籤將顯示用戶列表和它們的所有者。

使用用戶標籤，您可以爲您的用戶創建，刪除和更新Network Box Office用戶帳戶。

每個用戶有三種選擇：編輯偏好記錄，重置用戶的密碼和刪除用戶的帳戶。

您還可以創建新用戶。

2）偏好模組：用戶可以修改他們的個人資料，方法是通過使用我的帳戶標籤，然後點擊編輯個人資料按鈕。

用戶可以修改以下領域：:

- 用戶名。
- 電子郵件位址。
- 是否需要工單郵件（如果你想接收電子郵件通知工單變化）和推薦的工單範本（您想要的電子郵件範本格式）。
- 首選語言（從列表中可用的語言）。
- 首選門戶（從列表中選擇現有的區域鏡相）。
- 郵件列表首選項（是否要收到關於網路安全的新聞，技術和安全通告的電子郵件）。

使用者也可使用更改密碼按鈕來更改他們的密碼。

3）保存自定義搜索：客戶門戶網站允許用戶可以正在打開的和最近關閉的工單，並且通過使用工單模組的搜索功能進而保存搜索查詢的條件設置。

搜索標準使您可以指定任意組合的工單號碼，箱子編號 ，狀態，或文字。

此功能也可以總是顯示給您保存的搜索工單/概要頁面。

客戶門戶網站提供了許多關鍵功能，使用戶能夠更有效地管理Network Box。

有類似的功能在BOXES裏，讓您保存通用的BOX報告。

用戶也可以在用戶指南裏找到進一步的提示和技巧。

PUSH Technology

自推出以來，Network Box售中精力不斷地優化其PUSH推進式更新技術，作爲使設備獲得安全更新以提供及時安全保護的最好的方式——PUSH推進式更新技術相對於PULL下拉式技術有三個主要的優勢：

1）高速-減少延遲時間（時間從有更新出現到更新的發送過程開始）到最低限度。

2）準確-允許供應商確認更新的安裝和啓動的正確性。

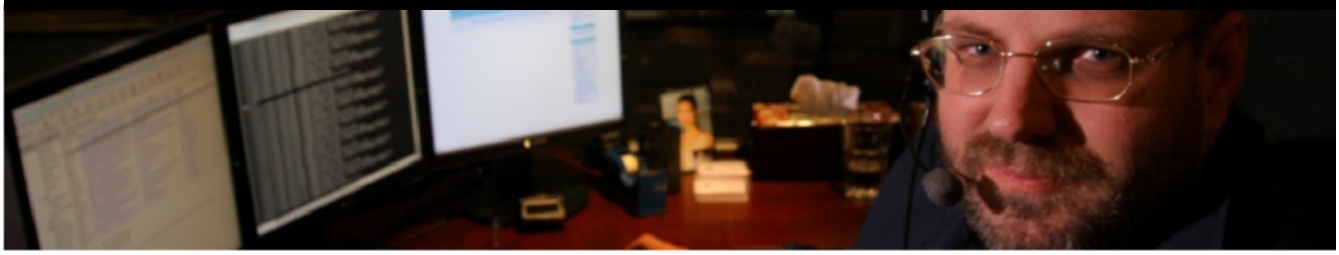
3）優化-提供優化的更新系統，從供應商的角度來看（最優化使用該供應商的網路來提供更新，在資源利用率和更新來源這兩個方面可以體現出來） 。

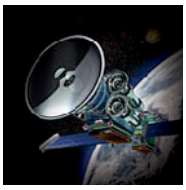
實地的對比測驗結果，通過明確的統計和數學分析也顯示出PULL與PUSH推送的明顯差別。 PUSH技術，非常簡便地提供了最好的方式，來使系統裝置獲得更新的簽名和保護代碼。

我們很高興地宣佈， 在2009年5月20日，我們完成了所有NOC到我們的新專利HQPUSH系統的遷移過程。這一新系統提供更高的性能和推進更新的優化。它使我們能夠持續不斷地，即時地監測我們的所有安全簽名的來源，並在幾秒鐘內推出這些變化。有了這個新系統，目前的最新更新只需3秒鐘就會被釋放安裝到地區NOC，更新到所有最終用戶的Network Box，在全球範圍內，仍在我們的目標範圍即45秒鐘內完成更新。這種更新的速度遠遠高於行業標準。

如需進一步資訊，請參閱我們的PUSH技術白皮書：

http://download.network-box.com/whitepapers/WP-PUSHTechnology.pdf





June 2009 Features

On Tuesday, 2 June 2009, we will be releasing a number of bug fixes and enhancements for NBRS-3.0. These changes include:

- Enhancements to the scanning speed and control of scan times for our mail scanning engine.
- Support for four new spam signature types (backscatter, sender-id, from-to pair and message subject) for our mail scanning engine.
- Improved simplified Chinese translation for Box Office, and download link to User Guide (HELP menu).
- Minor cosmetic changes to my.network-box.com administrative interface.
- Performance improvement for health monitoring system on S-50, S-80 and M-250 models.

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.

June Hint

新發佈的Network Box Office客戶門戶完全支援許可權分級管理。如果您有多台箱子，在不同或相同的地點，屬於（和被控制於）組織的不同部門，該結構可以反映在我們保存的資產庫存記錄中，並可用於對箱子和工單的能見度的控制。

例如，如果您在英國和美國有箱子，我們能夠配置系統，以便您在英國的辦事處的工作人員訪問英國的箱子，美國辦事處的工作人員訪問美國的箱子，需要訪問全球許可權的工作人員可以看到所有的箱子和工單。

如果您需要支援，請同您當地的NOC聯繫，告訴他們您的需求。

結束語

感謝您支持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
June 2009

MAY 2009 NUMBERS

Key Metric)	#	% difference (since last month)
PUSH Updates	944	-22.1
Signatures Released	329,611	+58.2
Firewall Blocks (/box)	618,154	-1.9
IDP Blocks (/box)	139,190	+0.1
Spams (/box)	83,060	+27.7
Malware (/box)	1,725	+28.7
URL Blocks (/box)	70,199	+18.6
URL Visits (/box)	2,752,585	+5.4

NEWSLETTER STAFF

Mark Webb-Johnson
Editor

Pauline Chiu
Michael Gazeley
Jason Law
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