In The Boxing Ring

IN THIS ISSUE

Network Box 技术新聞

作者： **Mark Webb-Johnson**，首席技术官

致辭

歡迎您來到 2009 年 5 月版 'In The Boxing Ring' 。

在這一版，我首先會和大家講一講 Network Box Office 客戶門戶。它的主要功能是可以讓用戶在國家，地區和全球等各種級別下管理一個或多個 Network Box 。該系統計划于今年 5 月份的頭兩個星期正式上線，詳情請見第 2 頁。

在 2009 年 4 月的下旬， Network Box 被授予 UTM 類的 PC3 白金至尊品牌大獎， PC3 大獎也授予給了一些其它的全球性品牌。請轉到第 2 頁查看詳細信息。

在第 3 頁，我將提供有關 Network Box 對 SMTPS 和 STARTTLS 的支持情況，及討論 SMTP 郵件加密——后者我建議我們所有的客戶考慮，如果你還沒有這樣做的話。

我也將向您來介紹我們的入侵檢測和預防的新方法，其中包括四個解决方案，及我們即將進行系統全面發布的日期。

本月我們再次有非常多的一批關于 NBRS - 3.0 的重大改進。我們也有關于 my.network-box.com 管理界面的小的改動，以便更好的用來查詢，報告和控制 Network Box 設備。

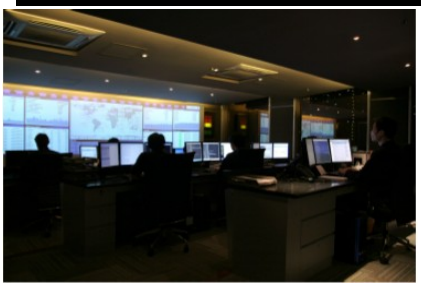
和以往一樣，如果您有任何的反饋，意見或者建議，我們都歡迎您隨時提出來。您也可以通過發送郵件到我們的郵件列表： nbhq@network-box.com 聯系我們。或者當您下次在香港市區的話來隨時來我公司辦公室進行參觀指導。

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

twitter.com/networkboxhq

Mark Webb-Johnson
CTO, Network Box Corporation
May 2009

NETWORK BOX



NETWORK BOX Office 客戶門戶（用戶界面）

我們的客戶的組織架搆可以是集中式、分布式或者個性化的（也包含三者之間的任意組合）， Network Box 的全球化視野包括全球支持功能是客戶非常關注的。

我們的分支機搆和網絡安全運維中心已經遍布全球。它們都會提供給我們的叫做 Outbreak 的集中管理系統相關回饋信息。

Network Box Outbreak 系統目前可以在每分鐘處理大約 60,000 個安全事件（每秒鐘處理 1000 個或者每天處理 8 千 6 百萬個），一個名叫 WOPR 的大型電腦系統會實時的對這些安全事件進行實時動態地采集、整理和進行關聯分析；測算出未來的安全趨勢并且告知我們的網絡安全工程師全球的安全威脅狀況。

Network Box 客戶門戶爲客戶提供一個通向這個（和其他）內部系統的窗口。它提供 Network Box 設備在我們管理之下的實時狀態，并允許同 Network Box 網絡運維中心（ NOC ）進行正式雙向的溝通，他們負責監測和配置 Network Box 設備和網絡。系統提供下列主要的功能：

* 概貌頁面提供一個有着全球地圖背景的包含 BOX 、 VPN 和管理鏈路連接狀況的網絡接入拓撲圖。它提供一個客戶所托管的網絡安全的簡單概貌。

* 一個工單模塊顯示用戶或者 NOC 創建的工單和它們的狀態。這就爲客戶和 NOC 之間建立了一個重要的溝通渠道，它可以提供正式的問題事件跟蹤，遵從服務級別協定，授權訪問控制，變更和配置管理等等）。這個模塊也包括：

  * 一個部署調查模塊，用來跟蹤在 BOX 的安裝和部署期間的信息（包括必要的信息收集、使用在線協同工作工具）。

* 一個資產模塊，用來顯示 BOX 的所有者信息及狀態。這個模塊也包括：

  * BOX 健康狀態模塊，它也嵌入全球監控系統（ GMS ），顯示 BOX ，網關和 VPN 的狀態。

* 許可證模塊，顯示合同信息，以及服務級別協議 SLA 信息。

* 負載模塊，顯示 BOX 的工作負載及趨勢分析。

* 一個用戶管理模塊，允許客戶中的指定特權用戶自己查看和維護 Box Office 的用戶賬號信息，而不需 NOC 的參與。這個模塊允許客戶更好地控制和管理支持全球部署的團隊。

這個系統提供了一個簡單、單一而強大的基于 WEB 的用戶界面，它可以在國家、地區和全球等級別管理一台或多台 Network Box 。

我們很高興地宣布，該系統現定于 2009 年 5 月 12 號進行（全球）正式發布。

2008 年度 PC3 至尊品牌大獎

在 2009 年 4 月， Network Box 被授予統一威脅管理（ UTM ）類別的白金至尊品牌大獎。

Network Box 和它的一些主要競爭對手獲得了 PC3 優質品牌獎 UTM 類的提名，并參與了競爭的過程。

處于技术發展最前沿，抵御日益增長的互聯網威脅是一項非常艱難的工作，并且行業競爭非常激烈。然而，盡管其他的 UTM 類參選者是 Network Box 的競爭對手，大家都努力，以保持各種規模的企業客戶免受日益擴大的數字安全威脅。

其中有不少相關的互聯網安全部門也獲得提名及獲獎，包括我們的合作伙伴卡巴斯基防病毒軟件，與提名者 NOD32 ，趨勢科技和其他企業安全軟件，其中包括 Sophos 公司，賽門鐵克公司及其他機搆。

其他獎項組包括快閃記憶體，科技教育和網上商店解決方案。進一步類別集中在互聯網安全，移動硬槃，投影機和文件解決方案等等。

總體而言，共有 45 個獎項由兩個團體通過兩個類別頒發。獲獎的還有三星電子， Acronis ，卡巴斯基，索尼，華碩和許多其他知名品牌。主辦機搆在香港九龍塘的創新中心簡短地舉辦了頒發儀式，但是很專業和正規。

加密 SMTP 郵件

由于標准的 SMTP 發送郵件時，并不使用加密或認證，所以您所傳送的每封郵件都以明文文件被轉發。針對這一問題，有郵件客戶端解決方案（如 S/MIME 和 PGP ）可以供采用。它們可以非常有效地解決這一問題，但需要終端用戶的參與并且非常復雜。現在有一個更加好的方法可以提供基本的 SMTP 保護，它就是在郵件服務器 / 網關進行郵件加密。

為什么要這么做呢？答案主要是為了避免對你的通訊受到不必要的竊聽。和 SMTP 協議類似的一個真實世界中的例子就是傳遞不密封信封口的公開信件：您的郵遞員，前台工作人員，清潔員，或任何可以接觸到這封信的人都可以打開和閱讀，甚至修改它并繼續傳遞。最終在你一點兒都未覺察的情況下，你的“私人”通訊被攔截了。如果您信任您的郵差（如：運營商），通訊的隱私或許并不那么重要，那么您不必擔心保護您的 SMTP 郵件。

如果您擔心這一點，那么你應該先開始考察使用加密的 SMTP 或一個客戶端解決方案（如 S/MIME 和 PGP ）。

Network Box 已花費一些時間增加對 SMTPS 和 STARTTLS 協議的支持，對象包括我們的傳入（入站）和傳出（出站）的 SMTP 網關。
在 2009 年 5 月份的星期二補丁更新中，我們將向 SMTP 軟件中增加這種支持，而且我們將開始在 5 月中下旬對這一技朮進行公開測試，預估會在 2009 年 6 月達到完全支持的目標。

該 SMTPS 和 STARTTLS 協議建立于 SMTP 和標准的 SSL/TLS 之上。因此，它們需在鏈接的服務器端使用加密證書（也提供可選的客戶端加密選項）。

配置出站郵件，使其支持 SMTPS （或 STARTTLS ）非常簡單。該 Network Box 可配置爲在“隨機加密”模式（這樣它就可以自動檢測，看服務器是否支持 STARTTLS ，如果不行就切換到 SSL/TLS ，進而自動加密所有這些服務器的流量）。 Network Box 也可以配置成只針對指定的網域或服務器應用 SMTPS 。

配置入站郵件支持 SMTPS （或 STARTTLS ）需要在 Network Box 上安裝一個 SSL 證書。這些證書可以在線購買，并且可以很簡單地取得它。通常情況下，您購買的證書將包括您的發布 DNS MX 記錄的名稱（因爲協議會使用這些名稱來驗證服務器是誰及是否屬實），人們通常會按每年一次支付費用。

該 Network Box 能坐在一個加密的 SMTP 連接的中間。這樣，加密郵件可以通過網絡傳送到 Network Box ，接着郵件被解密和掃描以發現惡意 / 垃圾郵件及執行公司政策，然后被重新加密，最后傳遞給目標服務器。

加密 SMTP 協議（ SMTPS 和 STARTTLS ）并不適合每一個人。但是，他們會爲那些需要這種保護水平的客戶提供有效的 SMTP 協議的保護支持。該協議是標准化的，而且有非常好的互操作性。

NETWORK BOX 入侵偵測及防御系統

一段時間以來， Network Box 提供的 IDP 系統是其可管理 UTM+ 韌體（固件）的一部分。這是一個非常輕量級的，高速的服務，專門提供針對網絡蠕蟲，緩沖區溢出和其他此類攻擊的零延遲保護。

我們正處于開發一套全新的入侵偵測及防御系統的最后階段。這套新辦法，將提供四種運行模式（ 1 個舊的和 3 個新的）：

。目前 NBIDS 系統 - 輕量級，零延時，非常快的高性能。

。新 NBIDPS 引擎，使用全面流和協議解碼。能夠運行在混雜模式（使用交換機的監聽口，或集線器），只需使用很少的 IP 地址，并有三種模式：

。被動入侵檢測系統 - 報警和記錄相關流量，旁路方式部署獲取數據流——方便執行政策和發放更具攻擊性的規則。

。積極的入侵檢測系統 - 報警和記錄相關流量，側路方式部署獲取數據流，它可以使用積極的方式中斷連接會話。

。串聯的 IPS - 報警和記錄相關流量，數據流將穿透經過系統；好處是可以減少流量。

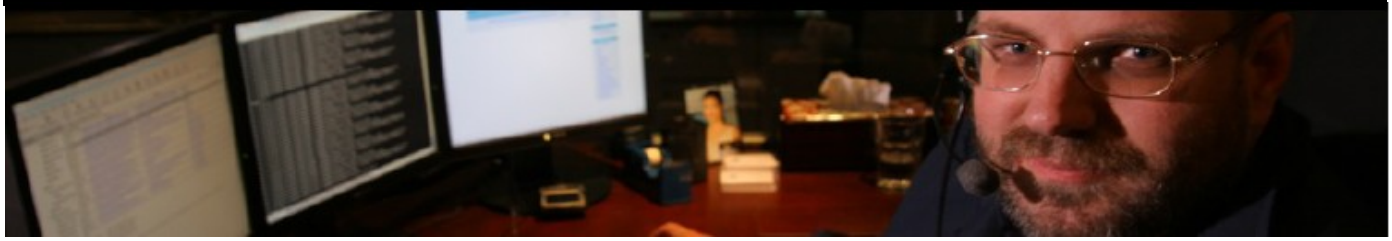
上述几種模式可以結合起來，以適應客戶的需求，鑒于性價比的限制，我們通過靈活地部署達到盡可能高的保護水平。

新引擎的簽名按照行業標准的 Snort 格式，并可以按全球，按 NOC ，按每個客戶等不同層面來建立自己的規則。在每個設備的基礎上也可以按需要定義所需的簽名和獨特的配置。每個規則有一個記錄和檢索幫助頁，以幫助進行報告和分析之目的。我們目前的新系統已經有超過 10000 個簽名。

新的引擎提供了一個更強大的規則語言，及更好的流和協議解碼支持。這是好的消息，但是它也會影響性能。該解決方案提供四種運作模式，以用來在保護水平（和延遲）和性能取得平衡。可以將不同的接口設定運行在在不同的模式下（例如，在內部網絡接口部署積極的入侵檢測系統，在外網接口部署串聯的 IPS ）。或者，我們可以簡單地對所有流量使用同一個模式運行。

日志記錄將合并到我們的 NOC 的統計資料 / 報告 / 監測系統，以及定期的 PDF 報告和 my.network-box.com 管理界面。

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。我們估計將于 2009 年 5 月下旬開始公開的測試，正式的發布會在 6 、 7 月份。



May 2009 Features

2009 年 5 月 5 日的星期二補丁，我們將爲 NBRS-3.0 系統發布大量的錯誤修復和改進工作。這些變化包括如下：

•將在 2009 年 5 月 12 日進行全球發布的 Network Box Office 客戶門戶。
•改進了 NOC 進行系統維護，診斷和控制的功能——包括更好地對 NOC 及客戶更改配置進行集中審計的制度（如防垃圾郵件白名單 / 黑名單的制定） 。
•新的健康狀態監督和檢查，針對 DNS 服務器以及谷歌安全瀏覽，新功能會定期檢查這些系統和報警（通過全球監控系統）發現的問題。
•支持 SMTPS 和 STARTTLS 議定書我們存儲轉發 SMTP 代理。
•支持 NBIDPS 和定期報告有關 IDPS 的警告。
•關于 my.network-box.com 管理界面的一些小改動。

上述變化將不會對正在運行的服務產生任何影響，也不需要設備重新啟動，所以不會造成任何設備運作的重大中斷事故。您當地的網絡安全運維中心 NOC 將以分階段的方式進行新功能的推出。

如果您需要關于任何上述情況的進一步的資料，請聯系您當地的網絡安全運維中心 NOC ，他們將會安排補丁的安裝部署及在必要時同您聯絡。

May Hint

Network Box 利用行業標准協議和服務爲您提供各種實時信息。我建議你充分利用它以便及早了解全球范圍內的安全事件，以及 Network Box 正在幫您做什么。通過這樣您可以隨時做到更好的准備。
您可以隨時通過我們的網站或 my.network-box.com 主頁看到新聞故事。但是，您是否知道您可以通過您的瀏覽器 / RSS 閱讀器得到這些新聞的 RSS 種子？請訪問： http://www.network-box.com/aboutus/news/feed 來訂閱我們的簡易信息聚合種子吧。
我們也提供更快的最尖端的新聞，提示和警示，請跟隨我們的安全反應 RSS 種子 http://twitter.com/networkboxhq 或 http://tinyurl.com/c49s7v 。

結束語

感謝您的支持 Network Box ，并繼續將您的網絡安全托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；如果您有其它需求，也請別猶豫，馬上與我們聯系，尋求協助。

Mark Webb-Johnson
CTO, Network Box Corporation
May 2009

MAY 2009 NUMBERS

Key Metric	#	% difference (since last month)
PUSH Updates	1,213	-12.5
Signatures Released	2,083,850	-14.0
Firewall Blocks (/box)	618,154	+8.8
IDP Blocks (/box)	139,060	+12.8
Spams (/box)	35,025	+18.5
Malware (/box)	1,340	+63.2
URL Blocks (/box)	59,193	+9.8
URL Visits (/box)	2,611,502	+3.0

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