In The Boxing Ring

IN THIS ISSUE

2.
MY.NETWORK-BOX.COM
我們在管理界面里加入了查詢、報告和控制 Network Box 設備的新功能。

3.
垃圾郵件評分調整的改進
系統已經正式地發布，現在可以正常開始使用了。在第三頁會展示給您。

3.
用戶界面，開放公開測試
我們准備對這個項目進行大范圍的公開試用。

3.
代理服務器的漏洞
針對剛剛發布的關于 Web 代理服務器的漏洞，可能會影響到我們的客戶。

4.
Feb 2009 FEATURES
我們最近公布的增強性功能的部署情況

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 3 月版 'In The Boxing Ring'。在這一版，我將花一整頁來談論于本月已經發布的 my.network-box.com 管理系統的新功能。我也要更新一下目前我們正在進行測試的系統功能。

該 my.network-box.com 管理界面是用來查詢、報告和控制 Network Box 設備的。這種做法在業界可以說是獨樹一幟，它提供了一種混合式控制的管理服務架搆：客戶負責制定安全政策而網絡安全運維中心（NOC）負責執行它。它也提供客戶一個統一的界面來檢查其安全政策的執行效果。應大家的需求，我們在界面里增加了几個新的控制和診斷功能。翻到第 2 頁可以見到詳細的資料信息。

垃圾郵件評分調整系統也不負重望，2009 年 2 月 23 日它得到了正式地發布，現在可以正常使用了。要了解進一步資料，請翻到第 3 頁。

該 Network Box Office 客戶門戶測試已經持續了一段時間，現在我們准備迎接更大范圍的公開試用。申請試用的流程請見第 3 頁。

繼上個月關于出境政策執行的討論，一個剛剛發布的關于 Web 代理行爲的漏洞將再一次提到嚴格進行政策執行的必要性（見第 3 頁）。

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 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。

Mark Webb-Johnson
CTO, Network Box Corporation
March 2009

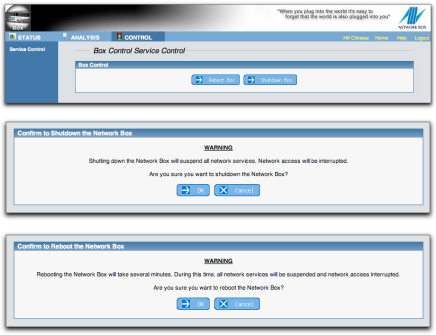
NETWORK BOX

my.network-box.com 大改進

和大量的小改進一起，這個月我們即將在全球范圍內發布了基于 NBRS-3.0 平台的有共四個關于 my.network-box.com 管理界面的新功能：

1、遠程關機 / 重新啓動
2、網絡地址信息
3、DHCP 租約
4、路由跟蹤和 Ping

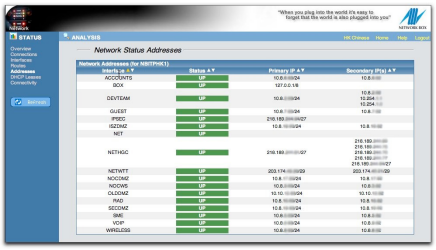
遠程關機 / 重新啓動



我們在 Box/ 控制 / 服務控制里增加了一個新的屏幕，允許管理員遠程關機或者重啓的 Network Box 設備。功能相當于之前從設備前端面板進行手工操作，目前加入到 my.network-box.com 管理界面。

在管理員選擇功能（關機或重新啟動）之后，會出現一個確認對話框。單擊確定執行行動。在訪問控制方面，也可以定義允許或拒絕管理員訪問此功能。

網絡地址信息

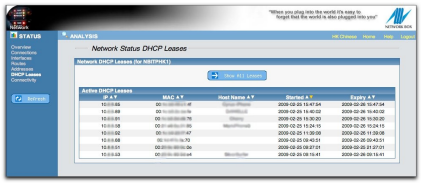


新增加了一個屏幕（網絡 / 狀態 / 地址）可以顯示出 Network Box 當前的 IP 地址分配情況。

這個信息對使用動態 IP 地址的 Box 顯得特別重要，該屏幕顯示每個已定義的網絡接口，它的狀態，它的主 IP 地址，以及所有的次要 IP 地址（如果有的話）。

該屏幕提供了一個簡單扼要的報告來顯示地址分配情況。

DHCP 租約



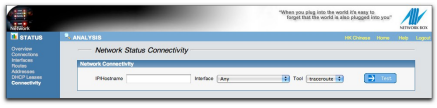
添加了一個新的屏幕到網絡 / 狀態 /DHCP 租約上，顯示出 Network Box 的 DHCP 服務器當前的和過去的 IP 地址租約信息。此功能只有當您的 Network Box 配置成 DHCP 服務器的時候才適用。

默認情況下，屏幕顯示的所有當前的 DHCP 租約信息（包括 IP 地址， MAC 地址，主機名稱，租賃期限等資料）。

點擊 “顯示所有租約” 的按鈕，可用于切換到所有的租約信息（包括目前活躍的，過期的，和曆史租約）。

過去，一些客戶一直不敢使用 Network Box 的 DHCP 服務器功能，原因是缺乏這方面的足夠的資料。我們希望，這一新功能能鼓勵大家使用這個強大的 DHCP 服務。

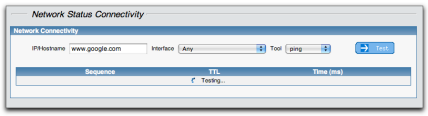
路由跟蹤和 Ping

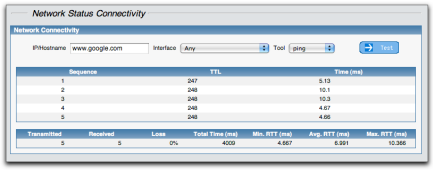


我們已經增加了一個屏幕（在網絡 / 狀態 / 連接），可以使系統管理員進行路由追蹤和 Ping 測試。雖然這些測試可以從 Network Box 后面的工作站 / 服務器中進行，但有時也有必要直接從網關上運行它們。

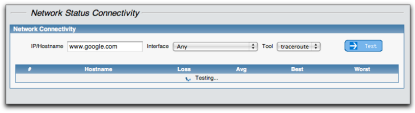
您需要輸入您想要測試的 IP 地址（或 DNS 主機名）開始使用，再選擇要使用的工具，然后點擊 “測試” 。測試結果將顯示在一個表中。

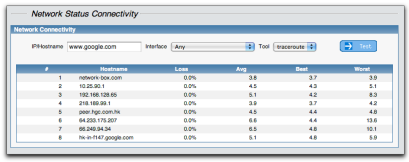
您也可以選擇更改您要測試的界面（特別是在使用 IPSec VPN 鏈接進行測試時，因爲它做了加密，也適用于如通過源 + 目的地址進行配置的高級選擇性路由情況下）。





Ping 連接測試的輸出結果將顯示您丟包和往返時間，用于測試的爲每次 5 個 ICMP 封包。它也將顯示出來一個簡單的報表（顯示最低，最高和平均值）。





路由跟蹤 Trace route 的連接測試輸出結果將顯示您的 Network Box 和目的地之間的網絡跳數。對于每一跳，它會顯示數據包丟失和往返時間（有最好，最壞和平均值），讓您可以看到究竟連接問題出在何處。

何時可用

所有這些新功能將在這個星期二補丁（ 2009 年 3 月 3 日）進行全球范圍內的發布，預計在一個星期內推廣到所有 NBRS-3.0 客戶 Box 中。

您也可以聯系您當地的網絡安全運維中心即 NOC 進行進一步的了解。

關系型垃圾郵件評分調整

我很高興能宣布， Network Box 電子郵件垃圾郵件分數關系調整制度已經在全球公開發布。

這種新系統基于關系的深度，采用關系數據庫來自動調整反垃圾分數。

它可以用來是： （ a ）更積極獲取已知垃圾郵件來源和（ b ）識辨出及親近已知的有良好來源的非垃圾郵件。

電子郵件與垃圾郵件分數調整制度對”邊境線“區內的垃圾郵件（一般調整前的分數在 5.0 至 9.0 之間）是非常有效的，并能給出相關的標示，以區分它們是垃圾郵件或非垃圾郵件。它會根據以前發送者和接收者的關系情況調整新郵件的垃圾郵件評分，并有試圖驗證發件人的信任挑戰機制，甚至在 SMTP 協議本身沒有啓用發件人身份驗證功能的狀態下也可行。

該系統有強大的可配置性，并且可進行微調，并可以配置為只調整分數上漲或下跌的配置的調整范圍。目前的工作正在取得積極的進展，在防病毒和政策執行方面也有提供同樣的技术。

這一新功能的代碼已成功地通過了所有測試，并在全球發行的 2009 年 2 月 23 日作爲一個 PUSHCODE 推進更新到了所有 NBRS-3.0 的客戶 BOX 中。

這個關系系統，必須針對每個 Network Box 進行單獨配置和調整。由于大量的客戶支持和咨詢工作都是由網絡安全運維中心 NOC 來進行的，我們將按照客戶一個一個地進行部署。

用戶門戶界面開放公開測試

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。 Network Box 的全球監測系統（ GMS ）是我們提供設備監控、事件及問題響應服務的一個關鍵組成部分。我們有一些全球運作的內部系統，這些內部系統包括：

•全球監控系統 (NBGMS) ，它是一個測試、記錄和報警着全球成千上萬個 Network Box 和互聯網網關系統健康狀態的矩陣式監控系統。

•資產信息系統，它記錄着哪個客戶在使用哪些 BOX ，這些 BOX 的硬件和軟件配置情況，是從哪個渠道伙伴銷售出去的等等。

•許可證，它記錄着 Network Box 和合作伙伴及客戶之間的合同、許可證和服務級別協議 SLA 。

•部署信息，它用于記錄和跟蹤新的 Network Box 的安裝及部署情況。

•工單系統，用來跟蹤客戶和 NOC 發起的一些事件或變更請求，通過它來確保服務能滿足 SLA 的要求，并且不斷提升服務管理質量。

•負載統計，它也是 Outbreak 系統的一部分，它用來跟蹤 Network Box 設備的負載情況，用來確保系統的可用性，并且以主動和積極的方式進行容量管理。

該系統已在測試階段，經過了一段時間的完善，我們現在准備在向全球發布之前將其開放給一個更廣泛的公開測試。

如果您希望參加試用，請聯系您當地的網絡安全運維中心 NOC ，他們將幫助您收集必要的資料和准備遷移您的 Box 。 Beta 版的 Boxoffice 客戶門戶和標准區域鏡會并行操作，因此您將能夠在測試階段隨時進行雙邊之間的切換。

代理服務器的嚴重安全漏洞

使用代理服務器的計算機網絡現在面臨着一個嚴重的架搆方面的安全漏洞，它會影響到瀏覽器的自動重定向連接，可能會讓攻擊者遠程無限制地訪問內部網和其他網站的資源，安全專家警告說。

美國計算機緊急反應小組已發出了警報漏洞 435052 來跟蹤這個問題。原文如下：

Transparent proxy servers intercept and redirect network connections without user interaction or browser configuration.

Some transparent intercepting proxy implementations make connection decisions based on the HTTP host-header value.

Browser plugins (Flash, Java, etc.) may enforce access controls on active content by limiting communication to the site or domain that the content originated from. An attacker may be able to forge the HTTP host-header (or other HTTP headers) via active content.

A proxy server running in intercepting ("transparent") mode that makes connection decisions based on HTTP header values instead of source and destination IP addresses is vulnerable due to the ability of a remote attacker to forge these values.

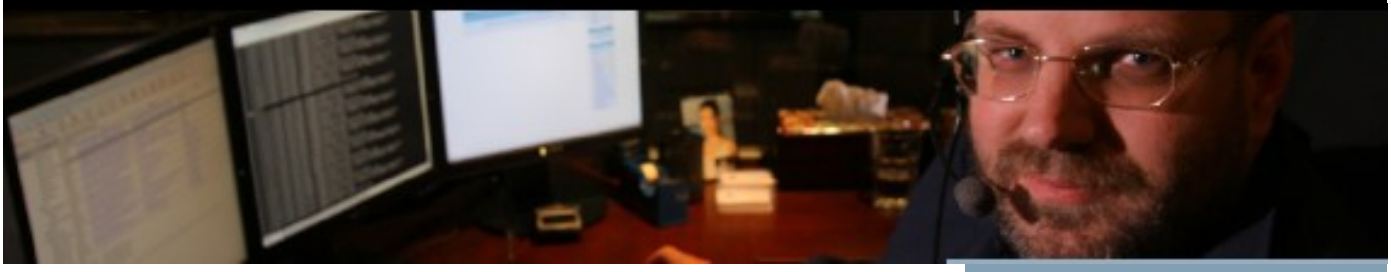
Network Box 安全響應中心目前建議客戶遵循最佳實踐做法，并確保

（ a ）代理服務器只應提供數量有限的常用的端口進行連接使用，以及

（ b ） CONNECT 方法應該只允許使用 tcp/443 的目標端口。

這個漏洞特別針對運行透明模式的代理服務器，不過最佳實踐建議對所有的代理服務器采取同樣的動作。

如果您有任何問題，請聯系您當地的網絡安全運維中心 NOC 提供與此有關的進一步的援助。



March 2009 Features

本月看點

2009 年 3 月的星期二補丁，我們將推出一些基于 NBRS-3.0 固件系統的錯誤和改進，包括如下工作：

•關于郵件掃描的大量系統增強功能，其中包括優化利用反垃圾郵件掃描中的白名單和黑名單功能來提升系統性能。我們也將開始部署關系垃圾分數調整制度。

•大批量的 my.network-box.com 管理界面的改進，以及新功能的添加比如遠程關機 / 重新啓動，網絡地址的信息顯示， DHCP 租約資料顯示，和路由追蹤 /Ping 連接測試。

•對 Network Box 健康監測系統和 GMS 系統進行較小的系統修正和改進（特別是在報告方面的改進，極大地方便已經將自己的網域加入到白名單中的客戶）。

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。

March Hint

本月小提示

你知道您的網絡里的哪些用戶天天在干什么嗎？網絡堵塞時您想知道誰占用了大部分的帶寬資源嗎？

我建議你看一下 my.network-box.com 中的網絡 / 簡要分析， IP 總結， IP 流量統計，所有協議和本地 IP 的報告。

這些報告是由一個復雜的軟件包叫做 NTOP 生成的。而不是把僅僅只關注帶寬（類似 MRTG 的功能，這是很容易做到的 ，它會檢查所有的網絡流量和記錄數據的總體使用（按照議議）和排列靠前的用戶（來源，目的地和協議）。

該報告可讓您精略地看到，誰和什么應用正在耗用大量帶寬，然后再轉到到細節。甚至有動態生成的網絡地圖（在網絡 / 分析 / 本地 IP / 網絡流量地圖）映射出在您的網絡上的所有用戶，服務器，設備和應用程序的網絡連接情況。

該系統是所有 Network Box NBRS-3.0 系統的標准配置，但并不一定都有啓用（尤其是負載量極高的 Box ）。

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的管理服務。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
March 2009

FEB 2009 NUMBERS

Key Metric	#
PUSH Updates	1,522
Signatures Released	270,180
Firewall Blocks (/box)	573,611
IDP Blocks (/box)	117,217
Spams (/box)	70,878
Malware (/box)	807
URL Blocks (/box)	60,489
URL Visits (/box)	2,389,984

NEWSLETTER STAFF

Mark Webb-Johnson
Editor

Pauline Chiu
Michael Gazeley
Jasmine Arif
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