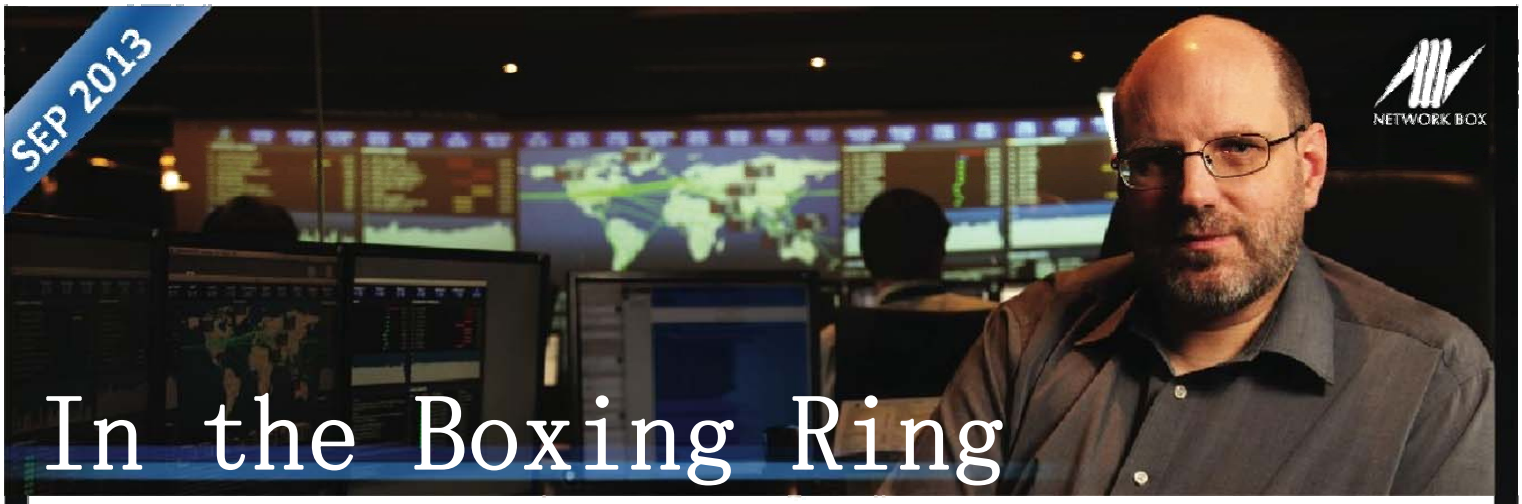


In the Boxing Ring

Network Box 技術資訊

from Mark Webb-Johnson, CTO Network Box

歡迎閱讀2013年9的月刊 In the Boxing Ring

這個月，我們首先發佈了NBRS-5.0的郵件掃描模組。爲進出BOX的SMTP資料提供了惡意軟體和垃圾郵件掃描。第2和第3頁也進一步的比較了NBRS-3.0和NBRS-5.0之間不同的掃描方法。

除了SMTP郵件掃描外，這個月我們還發佈了在Network Box NBRS-5.0上支援檔掃描的WAF+系統，這在第3頁會重點介紹。

在第4和第5頁裏我們闡述了這個月發佈的NBRS-5.0週二補丁的特徵，還包含了NBRS-5.0平臺的關鍵資訊。

最後，在8月份，Network Box參加了各種學術論壇和舉辦一系列標題爲“網路安全與你的業務”的講座，這些在第6頁會著重介紹。

Mark Webb-Johnson
Network Box技術總監
2013年9月

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
Google+ https://plus.google.com/u/0/107446804085109324633/posts

本 期 概 要

NBRS-5.0

郵件掃描

這個月，我們很高興的宣佈發行NBRS-5.0裏的第一個安全模組郵件掃描。這個模組爲進出BOX的SMTP資料提供了惡意軟體和垃圾郵件掃描。

透明代理

隨著nbrs-5.0代理是透明的(一般代理通信不改變源IP位址)，配置和部署通常是非常簡單的. 提供了兩個代理模組：

- smtpclient - 保護信任區域用戶端出站的SMTP連接。
- smtpserver - 保護信任區域的伺服器從非信任用戶端進來的SMTP連接。

這兩個模組主要的不同之處是smtpserver 模組執行第三方中繼保護，smtpclient不是。然而，不同模組也會有不同的報告。

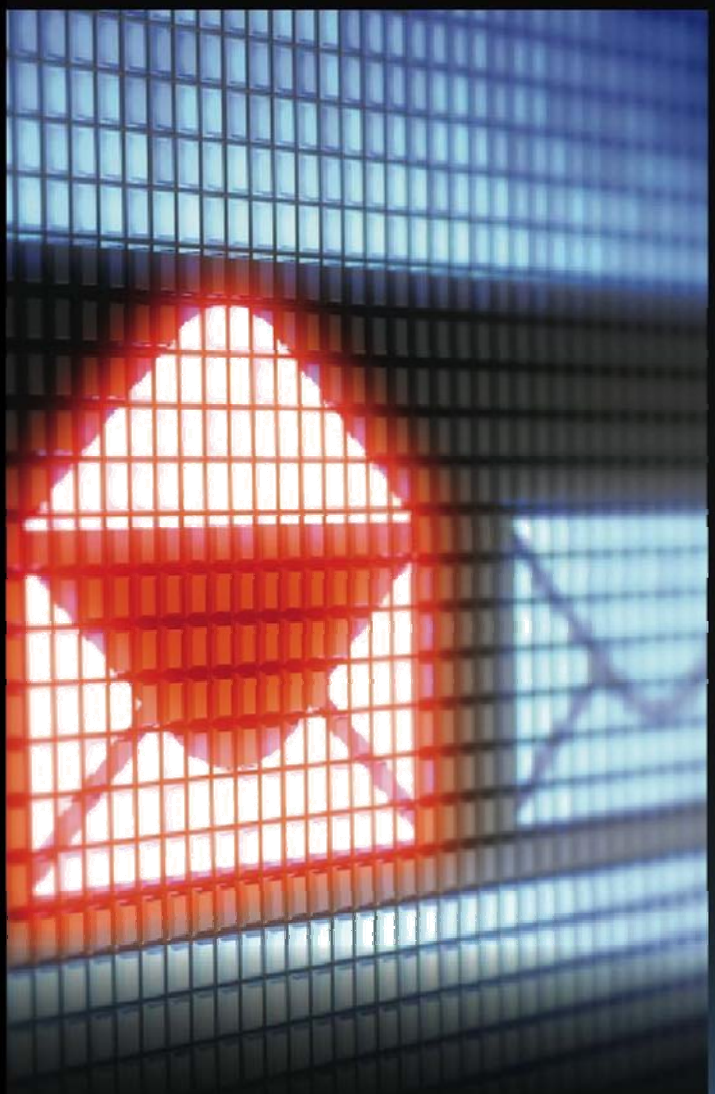
smtpserver 模組可以配置爲自動促進一個被smtpclient信任的客戶連接，有兩種情況：

1. 連接從一個源IP位址到達並配置爲受信任的。
2. SMTP用戶端成功的驗證到信任的SMTP伺服器。

同往常的NBRS-5.0模組一樣，SSL篩檢程式可以配置在傳入和傳出方向上，並支持IPv4和IPv6協定(包括IPv4和IPv6雙向轉換，SSL加密解密).

掃描

在NBRS-3.0的郵件掃描，一旦整封信件的信封 (發送者和接收者列表) 被收集，掃描後會返回一個單一的結果給所有的發送方和接收方。 類似的信件主體，會返回一個單一的結果給所有的收件者。如果這是一封垃圾郵件，會返回給所有人。

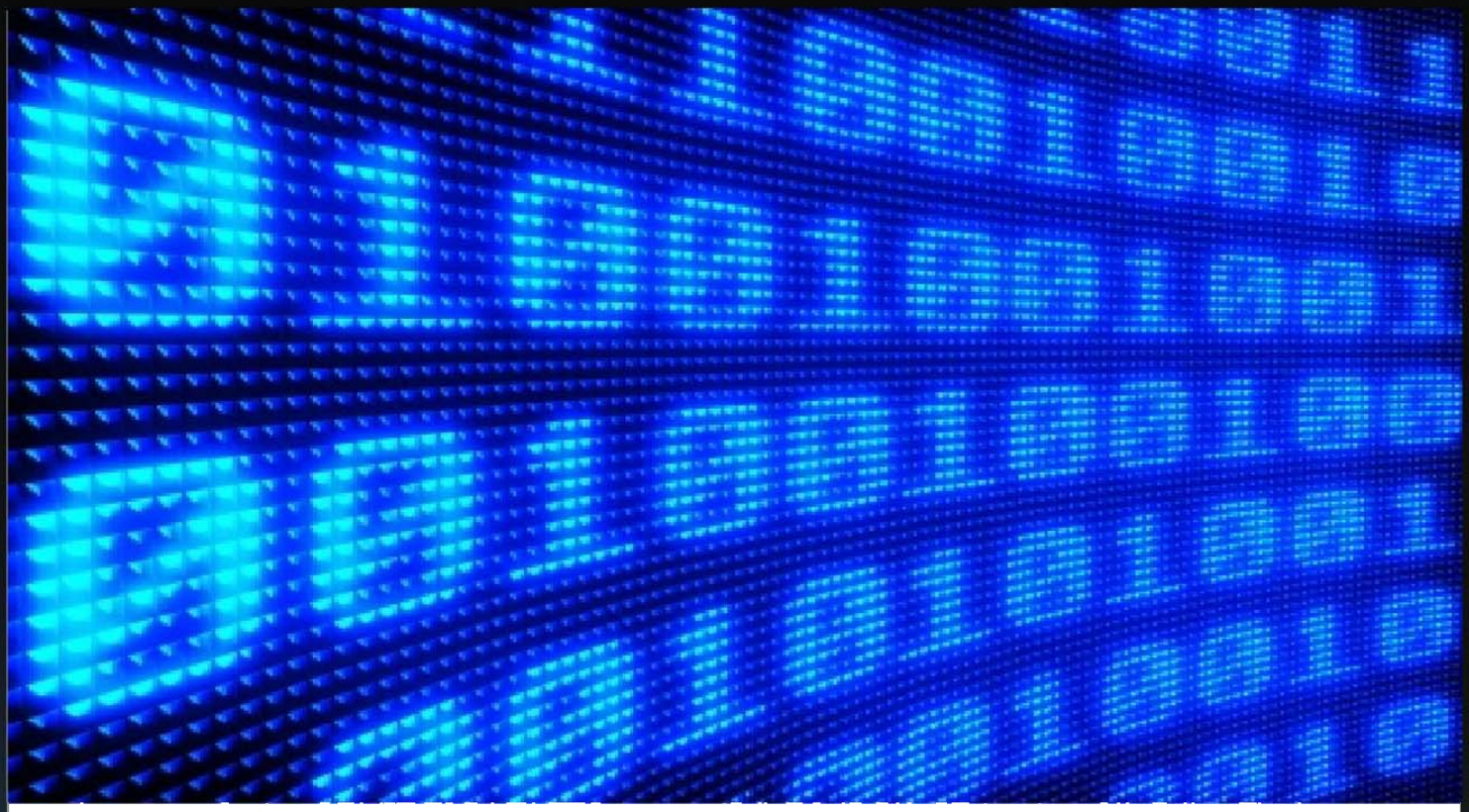


NBRS-5.0就大不相同。對於NBRS-5.0，消息傳輸的每個階段都是單獨掃描的，並單獨返回結果：

- 當 **HELO/EHLO** 消息已經接收，(按源IP位址和其他屬性)進行掃描。
- 當 **MAIL FROM** 發件者已經接收，(按結果和以前的 **HELO/EHLO** 屬性) 進行掃描.
- 當每個 **RCPT TO** 收件者已接收, (按結果和以前所有掃描階段的屬性)進行掃描。
- 當接收到消息主體 **DATA** 的掃描階段，(按結果和以前所有掃描階段的屬性)進行掃描。

在每個階段，策略規則在運行中可使單獨的收件者位址，或者整個郵件被攔截。

這個方法讓nbrs-5.0有能力非常精確的來控制接收電子郵件消息 - 減少帶寬使用情況並使設備性能最大化。尤其是，在早期的信封掃描階段(接收到消息主體之前)很多都著重放在增加掃描引擎的數量和能力上,在信封和信件掃描階段努力避免重複掃描。



類別

需要重點指出的是NBRS-5.0的核心，只是一個分類引擎。在掃描過程中，它能全面識別被掃描的物件(在這種情況下的信封或者消息）並返回一個分類列表，在這些分類和威脅識別中選取信任的，一旦掃描結果確定，然後由配置的策略來決定如何處理。

例如，不像NBRS-3.0，郵件掃描器在NBRS-5.0中不隔離郵件。替代的是，它僅僅表明使用代理發現一個威脅(例如惡意軟體)和分類物件。策略引擎在代理時可以允許或拒絕消息。例如：一個常見的配置：

```
config network proxy rule smtpclient deny

isthreat = TRUE with quarantine
```

這將禁止在給smtp用戶端進行掃描過程中攔截（禁止日誌）檢疫物件發現的威脅。

例如分類包括：

- malware - 確定爲惡意的對象
- spam - 確定爲垃圾郵件的物件
- bulk - 確定爲大批量的郵件
- testfile - 確定爲標準的測試檔

重要的是不但提供了分類，掃描引擎在分類的基礎上提供了信任度，以百分比表示。100%用於表示常規的推薦閾值來阻止一個威脅，但配置控制可以應用於更多（大於100%）或更少（少於100%）。這種方法工作在Network的多引擎掃描上特別能發揮作用。

從每個獨立的引擎通過允許信任級別後進行整體評分，與這些引擎一起工作能爲特定的分類提供一個清晰的資訊。

結論

2013年9月的NBRS-5.0的週二補丁發佈的郵件掃描系統將進入測試階段

Web 應用防火牆中的檔掃描

這個月，我們高興的宣佈Network Box NBRS-5.0 WAF+ 即將到來並支援檔掃描。這個可選的設備允許檔上傳到你的網站被當作是潛在的惡意內容，由nbrs-5.0反惡意軟體系統進行掃描。此外，作爲一個獨特的功能，你也可以選擇掃描出站流量（也許不是整個網站，但僅限於特定的路徑）。目前正在試驗的幾個網站都支持此功能，它將在10月的星期二補丁中正式發佈。

Network Box Version Five
NBRS-5.0

2013年9月3號，星期二
Network Box將發佈我們的星期二補丁對系統進行增強和修復，這些增強功能已經基本都支持新web用戶端的安全模組。

NBRS-5.0特徵
2013年9月

在接下來的7天裏各區域NOC將有計劃的進行新功能的發佈。這個月，NBRS-5.0的發佈包括：

- 發佈的7個新安全模組最終測試版：
  - scan-provider-policy-nb (Network Boxe郵件和檔掃描的策略引擎)
  - scan-provider-antispam-nb (Network Box郵件信封的病毒掃描引擎)
  - scan-mail (Network Box郵件信封和消息掃描框架)
  - proxy-mail-base (郵件代理支援)
  - proxy-mail-smtp-client (保護SMTP郵件用戶端的代理支援)
  - proxy-mail-smtp-server (保護SMTP郵件伺服器的代理支援)
- 爲客戶發佈的一個新的安全模組：
  - scan-provider-antimalware-clam (郵件和檔掃描的ClamAV防病毒引擎)
- 爲郵件、檔、url和認證掃描統一日誌系統。
- 爲郵件掃描提供Kaspersky防病毒引擎支援
- 報警基礎模組頁面，允許自定義的報警消息
- 提供一個可配置的設施避開所選擇的工作負載進行檔掃描。
- 提供一個可配置的設施避開所選擇的要求進行url掃描
- Web用戶端使用擴展的my.network-box.com和功能控制臺生成報告
- 統一‘isthreat’ ACL測試，作爲一個通用的指示可檢測到的威脅，應該阻止
- 增強的 my.network-box.com管理介面，爲分組表提供一個設備。
- 在my.network-box.com管理介面流覽器返回按鈕支援
- 爲隔離、報告、和其他這樣的物件統一裝載格式
- 各種（主要是內部）對Box Office增強和支援系統

在大多數情況下，上述變化不應影響運行服務或者會要求設備重啓，然而，在某情況下(根據配置)，可能要求設備重啓。如果有必要你當地的NOC將聯繫你安排處理。

如果你需要上述任何更進一步的資訊，請聯繫你當地的NOC，他們將聯繫你並做相關部署。

Network Box Version Five

NBRS-5.0

NBRS-5.0
路線圖

我們現在在NBRS-5.0路線圖的推進階段。大部分的開發工作已經完成，我們在進行最後的開發工作，爲剩餘的安全模組進行打包和測試。

去年7月的週二補丁我們發佈了SURF掃描產品，包括爲web用戶端提供反惡意軟體和內容過濾支援，並爲我們的web提供內容保護(客戶機和伺服器)。上個月的星期二補丁，我們發佈nbrs-5.0應用程式識別框架進行公測。這個月，我們將發佈我們的郵件掃描產品，接著就是nbrs-5.0剩下來的其他模組，到UTM+完備之後會等價於或者超過nbrs-3.0。現在我們已經達到這個里程碑，我們可以啓動從我們的現有客戶的nbrs-3.0升級到nbrs-5.0的過程。

Network Box主要的發佈版本 (NBRS-1.0, NBRS-3.0, NBRS-5.0等)包括進行至少長達5年的支持，所以這只是NBRS-5.0長途旅行的一個開始。我們有一些真正令人興奮的新產品，利用新基礎架構的支持, NBRS-5.0將幫助我們使你的線上網路保持安全。

1. 基礎平臺
回顧2012年夏天，我們完成了基礎平臺和支援NBRS-5.0的基礎結構。作爲產品的基礎代碼，並形成了NBRS-5.0產品的基礎。

2. WAF+
隨後我們開發了防Anti-DDoS的WAF+服務包。這個包提供了新的功能（是NBRS-3.0所沒有的）保護DMZ區域基礎雲的web基礎服務免受來自Internet的攻擊。它提供了網路防火牆，web應用防火牆，DDoS 防護，和IPv4與IPv6的協定轉換（IPv4-IPv6 / IPv6-IPv4橋接)功能，這個服務是單獨的。

3. SURF 掃描
要使web應用防火牆發揮作用，我們必須設計和建造一個代理能夠識別web的http協議。我們圍繞這個功能，結合我們先進的掃描技術，推出了我們下一代NBRS-5.0上的一個功能： SURF掃描。這將爲局域網內基礎的web用戶端在Internet上流覽web網站提供防護。它將支援病毒掃描，以及網站內容分類並進行策略控制。它也將支持更多的報告功能。

4. APP 掃描
根據這些，我們將發佈APP掃描，我們已經使用這個應用識別系統工作了一段時間。它可以獨立操作，也可以結合SURF掃描，它能夠在網路層識別應用並提取元資料和內容的資料流程。病毒掃描和策略控制技術都可以被應用。

5. MAIL 掃描
在這個階段，我們將全面的支援web伺服器和局域網用戶端，所以我們將發佈我們的郵件伺服器防護功能MAIL掃描。這將支援提供SMTP, POP3和IMAP郵件流量的掃描。

6. UTM+
最後，我們將完成UTM+的所有功能，發佈一組安全模組實現QoS（服務品質), VPNs, 群集, 高可用性，等。其中的一些服務將在前面的服務準備好之後一起發佈。

NBRS-3.0 特性

2013 9月

2013年9月3日，星期二， Network Box將發佈我們的週二補丁用以修復和增強系統相關功能。
各區域的NOCs在接下來的7天裏將有計劃的進行新功能的發佈。這個月針對NBRS-3.0的包括：

- 擴展了健康檢查功能允許精確控制網路錯誤報告
- 修改了在歐洲的檢測點
- 各種(主要是內部)針對Box Office的增強和系統支援

在大多數情況下，上述變化不應影響當前運行的服務或者要求重啓。然而，一些情況下（視具體配置），可能要求設備重啓。如果有必要你本地NOC將聯繫你安排處理。

Flock - Fedora 2013研討會

2013.8.9－2013.8.12

在南卡羅萊納州的查爾斯頓，Network Box的開發團隊參加了Fedora 2013的研討會。會議彙集了Fedora用戶和開發者分享和討論新的想法，並且努力使它們成爲現實。

Network Box USA

CompTIA ChannelCon 2013

2013.7.28－2013.8.1

Network Box參加了在美國佛羅里達州奧蘭多酒店舉行的CompTIA ChannelCon 2013。這是IT管道和高級別特性的頂級培訓和合作的機構進行的專題討論，以及強化執行證書培訓課程：雲計算、災難恢復、IT安全、移動、社會媒體等。

Network Box

網路安全和你的業務安全研討會

在8月，Network Box給一系列的網路安全研討會進行標題爲“網路安全與您的業務”的講座。參加這些會議簡要概述了最新的網路問題影響企業和Network Box的全面解決方案UTM+。

AUGUST 2013 NUMBERS

Key Metric	#	% difference (since last month)
PUSH Updates	495	-5.2
Signatures Released	614,277	+32.0
Firewall Blocks (/box)	916,560	+1.8
IDP Blocks (/box)	99,478	+2.0
Spams (/box)	19,138	+5.7
Malware (/box)	524	-31.5
URL Blocks (/box)	160,315	-4.0
URL Visits (/box)	3,147,924	-3.7

NEWSLETTER STAFF

Mark Webb-Johnson
Editor

Michael Gazeley
Nick Jones
Kevin Hla
Production Support

Network Box HQ
Network Box UK
Network Box USA
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