In The Boxing Ring

IN THIS ISSUE

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

Welcome

歡迎您閱讀2009年11月版的In the Boxing Ring。在這一版中，我們將專門來討論電子郵件這一課題。

翻到第2頁我們將向您講述互聯網電子郵件，它的的核心標準及SMTP，POP3和IMAP4協議（這些Network Box都已經全面支持）。這個介紹是爲了使大家對這些核心協議有一個基礎的認知、及瞭解每種協定的優點和缺點。特別要講出來的是，爲什麼Network Box（以及其他閘道設備）可以隔離使用某些協定的電子郵件，而不是其他的。另外，也將討論郵件頭兒中"from"(發送人）和"envelope sender"（信封發件者）之間的區別。

在第3頁，我們將向您介紹Network Box的防垃圾郵件系統的概況，以及如何有效地使用白名單（和黑名單）來調節和優化系統。

打開第4頁，按照慣例將提供關於月度總結和使用技巧的小提示。

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
November 2009

Internet eMail
SMTP, POP3 and IMAP4 Protocols

眾所周知互聯網電子郵件的歷史可以追溯到本世紀80年代初，同時正式發行了RFC821標準和SMTP協議。這個議定直到今天幾乎一點兒未變地仍在使用 中，是一種互聯網的核心協定，負責將電子郵件從一個郵件伺服器傳遞到另一個伺服器。雖然其他專有的解決方案仍然存在（如Microsoft Exchange長途交換和Lotus Notes協議），直至今日SMTP仍是目前最流行的郵件交換協議。

SMTP協議

SMTP（簡單郵件傳輸協定）提供了電子郵件信封（和郵寄實體信件相比是在前面列出的收件人地址及供退信的寄信人位址）和電子郵件（包括郵件頭兒 和主體內容——類似實體信封內紙張上的內容）之間的差異。該議定書規定了三個傳輸階段——首先是伺服器識別對方，表明自己的能力，然後發送郵件信封，最後 就是傳播資訊本身。

雖然大部分和實體信件是一樣的，但是信封中列出的發件人和收件人與電子郵件標題中列出的不必相同。重要的是，作爲標準，卻並沒有信件頭兒或信 封地址驗證——這使發送虛假的SMTP電子郵件變得非常容易（儘管許多如SPF和數字簽名方案等可選的擴展機制來試圖解決這個問題）。其他的關於實物郵件 和SMTP電子郵件的主要區別在於，SMTP電子郵件可以（在信封上）有多個收件人位址——這有點像在信封上列出所有收件人的位址，希望郵局複印郵件並逐 個交付給所有收件人。

一旦郵件已交付給最終SMTP郵件伺服器上的郵箱，以等待最終用戶來收取時，信封通常會被丟棄。

SMTP伺服器可以選擇成接受電子郵件，暫時擱置接受或永久拒絕——這一步驟可以在信封或郵件的傳輸階段完成。如果郵件無法送達（DNS錯誤或下一 跳的SMTP伺服器表明永久拒絕），該郵件會被退回——也就是說，一個未送達回執（NDR）將被生成並返回給信封發件人。在有的情況下，如沒有信封發件 人，該郵件將被丟棄。

SMTP是一種郵件傳輸協議。雖然有可選的可擴展反向傳輸可用（即目標伺服器將成爲郵件發送方和發送回所有佇列中的郵件）， 但是這種方式目前未能普遍使用。在正常使用，SMTP是一種推送協定。排隊等待郵件傳遞的伺服器將連接到目標（使用SMTP協定）進行郵件傳遞，然後從隊 列中刪除它們。在佇列中等太久（通常數天）的郵件通常會被退回（採用上述NDR的機制標識其爲無法投遞）。

SMTP是一個非常靈活的協議。接收SMTP伺服器可以接受消息（然後選擇放行，隔離，或者丟棄），推遲傳送或者拒絕。它也可以改變郵件信封，以便將消息重定向（轉發）至別處。Network Box已經非常好地利用了所有這些靈活性。

因此，如果SMTP是傳輸協議，郵件是如何到達郵件用戶端（如Outlook，Thunderbird，Eudora或Apple Mail）的呢？除了專有的解決方案存在（如Microsoft Exchange和Lotus Notes）之外，有兩種常見的互聯網標準存在——POP3和IMAP4。

POP3協議

POP3是郵局協定版本3，最初記錄在90年代中期的RFC1939中。這是一種相對簡單的協議旨在讓郵件用戶端連接郵件伺服器，驗證用戶的郵箱訪問權限，得到一個郵箱中的郵件列表，並將這些郵件轉移到用戶端，然後選擇性地刪除在伺服器上該郵箱裏的郵件（大概是在將它們添加到一個用戶端郵箱的本地副本之後）。

POP3協議很簡單，但是也很有限。一旦用戶端發出資訊請求，伺服器沒有相關的機制不提供給它（除了發送一個錯誤來終止連接之外）。爲此，高級的功能如對郵件進行復位向（轉發）或隔離是不可能基於POP3協定使用的。

IMAP4協議

IMAP4是互聯網郵件訪問協議版本4，它的最初發佈文檔是RFC2060，和POP3大約是同一時間公佈的。和POP3相比，它提供了一些更爲強大的機 制（如支持郵箱內的檔夾，只收取郵件的某個部分，和先進的檢索機制）。而POP3只是爲了讓郵件用戶端保持一個郵箱的本地副本（在副本上可以執行先進的 功能），IMAP4被設計成用戶端伺服器模式（以確保郵件用戶端不需要本地副本並且所有的消息都可以保留在郵件伺服器上）。

IMAP4協議，無論如何，仍然受到許多如POP3同樣的限制。在基本的IMAP4協議上，伺服器端沒有相關的機制，拒絕郵件請求（沒有討厭的錯誤消息），也沒有諸如資訊重定向和隔離等先進的功能。

結論

在SMTP協定用於將電子郵件從郵件伺服器發送到郵件伺服器。它有高可靠性，並緊密集成進了DNS系統，它是互聯網上的電子郵件的核心骨幹。

POP3和IMAP4協議是用於從郵件伺服器上獲取郵件，用於顯示在一個郵件用戶端上。

大多數的互聯網郵件用戶端都有配置螢幕，可以來定義SMTP伺服器用於郵件發送和POP3/IMAP4伺服器用於郵件的接收。

Anti-Spam and Whitelisting / Blacklisting

對付垃圾郵件包含分析給定的電子郵件資訊，並作出該郵件是否是垃圾郵件的裁定。

Network Box採用並部署了先進的防垃圾郵件系統技術，以最大限度地全面提升了垃圾郵件的成功檢測率，同時儘量減少假陽性。這些技術包括：合作的垃圾郵件校驗，簽字和垃圾郵件評分，白名單和黑名單，啓發式，即時IP和URL黑名單（又名信譽），網址到IP映射和黑名單，網址分類，功能變數名稱年齡，貝葉斯過濾，挑戰/響應系統，數位簽名，光學字元識別，模糊簽名和關係爲基礎的資料庫。

反郵件系統的輸出結果是確定一封郵件是否肯定是垃圾郵件/正常郵件（黑名單或白名單）或它是垃圾郵件的可能性（表示爲得分，得分越高的郵件越接近是垃圾郵件）。

在黑名單中或分數足夠高（是垃圾郵件的可能性很高）的郵件將被回饋到自學習系統，進而訓練系統可能性非常高的垃圾郵件是什麼樣子（以改進今後的垃圾郵件檢測性能）。在白名單的郵件，也會被回饋到自我學習系統，用於訓練系統正常的郵件是什麼樣子（以降借未來垃圾郵件判斷的假陽性率）。

自學習系統包括諸如貝葉斯統計分析和關聯資料庫等技術。

因此，對白名單和黑名單制度的理解和有效利用是極爲重要的——以避免錯誤的自學習系統培訓。

白名單和黑名單通常是使用電子郵件的發件人位址。問題是，正如前面討論過的，發件人是很容易被僞造的。

Network Box的郵件關係系統具有一個很大的優勢，便是基於在絕大多數情況下垃圾郵件發送者知道你是誰，但是不知道你會接受誰的事實。當使用白名單和黑名單時，儘管有造假的問題仍然存在，您仍然可以充分利用這一優勢。

關鍵是要避免白名單或黑名單郵件網域，那樣的話垃圾郵件發送者就會知道你會接受誰。這樣的功能變數名稱包括您自己的（約1% - 3%的垃圾郵件目前是僞造成似乎來自自己的功能變數名稱）和大眾常見的功能變數名稱（如雅虎，Hotmail，Gmail和流行的互聯網服務供應商的功能變數名稱）。

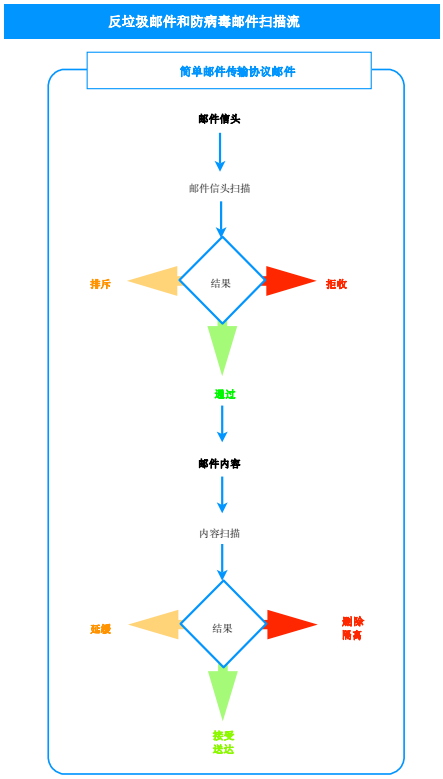
對於不想要大量垃圾，列入黑名單通常無效（因爲垃圾郵件發送者在發送每條電子郵件消息時都會更改他的發件人位址）。對於這種情況，最好是轉發（作爲附件）漏掉的垃圾郵件至spam@network-box.com，讓Network Box的專家來處理。

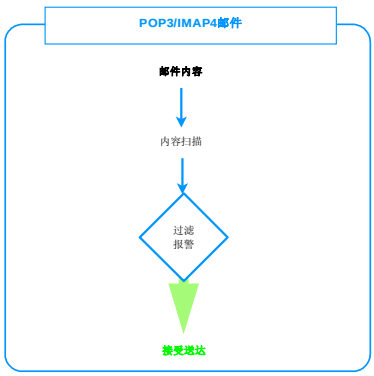
對於不想要的郵件列表樣式的電子郵件，黑名單是非常有效的。

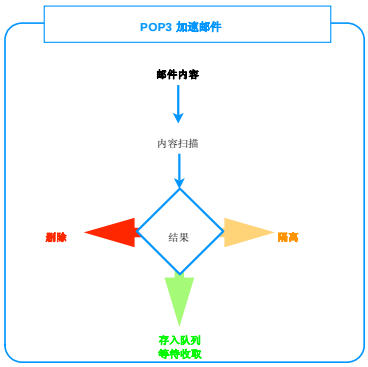
被那些想要（但是被錯誤地標記爲垃圾郵件）的郵件，白名單發件人的電子郵件位址是非常有效的——只要它不是使用您自己的功能變數名稱。

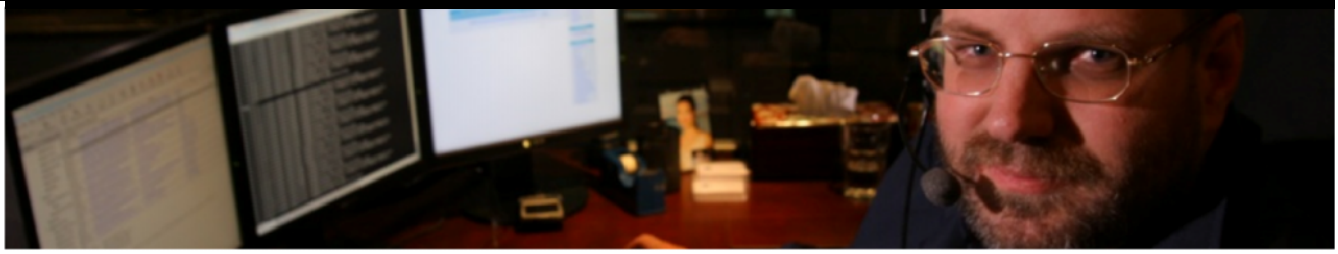
對於您自己的功能變數名稱內的用戶，最好的辦法是讓所有此類郵件向外發送即出站（無論是從局域網，通過VPN，或通過身份驗證的SMTP連接）。 對這些出站的電子郵件不進行垃圾郵件的掃描，也就絕不會因此受阻。

如果您能確保您所有網域的郵件都會通過您定義的IP地址範圍向外發送，那麼你也應該部署發送方策略框架SPF。這樣做可以立即停止1%至3%的以你作爲發件人的垃圾郵件，同時也可以幫助其他檢查SPF記錄的人免受垃圾郵件發送者假冒您所造成的危害。如果每個人都實行SPF，就不會有更多的僞造電子郵件位址的垃圾郵件發送。









November 2009 Features

On Tuesday, 3rd November 2009, Network Box will release our patch Tuesday set of enhancements and fixes. The regional NOCs will be conducting the rollouts of the new functionality in a phased manner over the next 7 days. This month, these include:

- Some minor enhancements and fixes to my.network-box.com and mail portal interfaces (mostly involving quarantine release, searching, and the administrative display of challenged eMails for customers using the challenge/response system).
- A new option to allow the suppression of the malware table in the Mail Portal eMail report.
- Relaxing of the default restriction to allow whitelisting of individual eMail addresses on common domains (but to maintain the default restriction against whitelisting entire common domains).
- Support for NBIDPS in the weekly reporting system. If you have deployed this system, you will now see IPS alerts reported in the weekly report.
- Enhanced support for syslog and eMail alerts for SSL VPN connections.

In most cases, the above changes should not impact running services or require a device restart. However, in some cases (depending on configuration), a device restart may be required. Your local NOC will contact you to arrange this if necessary.

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

November 2009 Hint

乾淨地關閉/重新啓動Network Box非常重要，我們提供如下各種機制來幫助你。這些措施包括：

- 對於有前面板顯示器和鍵盤的型號，您可以從顯示幕選擇關機或者重啓。
- 對於通過串列聯接的型號，VPANEL設施會給你一個和麵板顯示器相同的功能，它支持關機和重新啓動。
- 對於有電源開關的型號，按一下開關後會啓動一個乾淨關閉（在前面板螢幕會顯示關閉進度）。
- 對於所有的型號，my.network-box.com的管理介面在Box/CONTROL中提供了“重新啓動”，“關機”的選項供遠端使用。

乾淨地關閉或重新啓動Network Box將確保（一）所有在更新過程中的任務可以被取消，（b）所有磁片被徹底地卸載，（c）所有的服務都被乾淨地停止，和（d）資料庫和未完成的傳輸被寫入到磁片。

不乾淨關機或重新啓動您的Network Box，可能會損壞硬體和/或系統檔。我們建議，只應在不可避免的情況下才可拔掉電源插頭。

Mark Webb-Johnson
CTO, Network Box Corporation
November 2009

OCTOBER 2009 NUMBERS

Key Metric)	#	% difference (since last month)
PUSH Updates	1,361	-12.2
Signatures Released	220,552	-2.8
Firewall Blocks (/box)	613,146	-3.9
IDP Blocks (/box)	190,456	+6.0
Spams (/box)	65,247	+9.8
Malware (/box)	4,060	+19.3
URL Blocks (/box)	106,173	-14.2
URL Visits (/box)	2,947,567	-11.2

NEWSLETTER STAFF

Mark Webb-Johnson
Editor

Michael Gazeley
Jason Law
Nick Jones
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