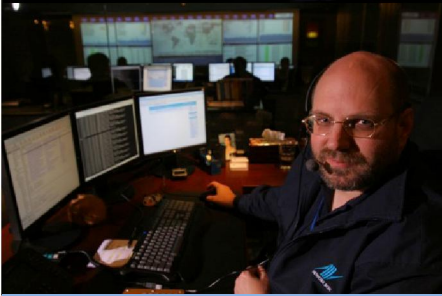


# In The Boxing Ring



來自 Network Box 首席技術官

Mark Webb-Johnson 的技術資訊

## Welcome

歡迎閱讀 2011 年 3 月刊的《In The Boxing Ring》。在這次的月刊中，我們將主要針對資料洩漏防護和出站策略掃描的課題進行了探討。

在第 2 頁，我們介紹了 Network Box NBR3-3.0 的一項新的功能——出站資料洩漏防護。雖然 Network Box 已經提供了比較全面的入站的反病毒、防垃圾郵件和策略執行，在出站方向上我們也採用 URL 內容過濾和入侵防禦。有些客戶會要求我們開啓反垃圾郵件出站功能並定義防垃圾郵件規則，以執行資料洩漏防護策略規則，但這並不是最理想的解決方案。而現在，我們很高興地宣佈，在 NBR3-3.0 平臺中，我們又有了一個新的出站策略引擎。這個新的引擎在 SMTP 郵件出站方向上，應用了同樣的曾獲獎項的 Network Box 反病毒技術，並且可以定義更加複雜的規則，執行策略攔截。

第 3 頁是關於每個月的新特性和一月份的提示。

本月刊將是這個版本格式的 In The Boxing Ring 的最後一次發佈了。鑒於 NBR5-5.0 平臺的開發正處於緊張有序地進行當中，下個月開始將會有一系列的關於 NBR5-5.0 各項功能特性的文章發佈出來。因此，本月刊將同時包含現有的 NBR3-3.0 平臺和即將到來的 NBR5-5.0 的相關內容。

和往常一樣，如果您有任何寶貴的回饋、意見或者建議，我們都非常歡迎並不勝感激。您可以通過郵箱（[nbhq@network-box.com](mailto:nbhq@network-box.com)）與我們總部取得聯繫，或者方便的話直接到我們辦公的地方來參觀指導。

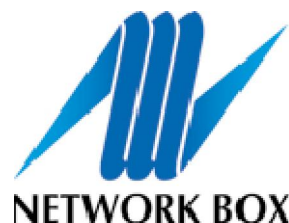
您也可以訂閱我們的 Network Box 安全響應 Twitter 對我們保持關注，網址為：

[twitter.com/networkboxhq](https://twitter.com/networkboxhq)

Mark Webb-Johnson

CTO, Network Box Corporation

2011 年 3 月



## 本期概要：

### 2. 資料洩漏保護

雖然 Network Box 已經提供了比較全面的入站的反病毒、防垃圾郵件和策略執行，在出站方向上我們也採用 URL 內容過濾和入侵防禦。而現在，我們很高興地宣佈，在 NBR3-3.0 中，我們又有了一個新的出站策略引擎。

### 3. 2011年3月 新特性

一如往常，我們將對所有的 NBR3-3.0 用戶進行我們持續不斷地增強、改善並部署，並進行相關的維護。

### 3. 2011年3月 提示

Box Office 的通知系統已經運行好幾個月了，但是相對於最大限度來看，還依然只是數量有限的用戶在使用。因此，我們建議您研究一下這個有用的功能，讓我們能更好地說明您做到最好的配置。

## DLP——數據洩漏防護



## 背景

在過去的幾年中，曾有很多的客戶要求我們通過執行策略攔截控制出站的內容。

例如，包括特別的文字、文檔檔、信用卡號碼、社會安全號碼等等。這部分客戶還經常要求我們把出站的反垃圾郵件功能開啓，而且他們自己還可以自行配置反垃圾郵件系統的規則。

但是問題是，反垃圾郵件系統是爲偵察入站垃圾郵件而設計的，而不是出站的。是爲保護內部用戶不受互聯網垃圾郵件侵害而設計的，而不是用於保護互聯網受內部用戶侵害而設計的，並且也沒有策略執行和通知的功能。

## Network Box 的 DLP 引擎

我們很高興地宣佈，馬上發佈的 NBRS-3.0 的升級包中(在 Network Box 2011 年 3 月份的 Patch Tuesday 中發佈)，就包含了一個全新的出站策略引擎，用於資料洩漏預防 (DLP)。

它分爲兩部分，這一嶄新的引擎對出站方向的 SMTP 郵件掃描也採用了 Network Box 所獲獎的反垃圾郵件技術，並且可以定義複雜的規則和執行策略攔截。

1、“dlp\_rules”引擎採用了和我們的反垃圾郵件引擎“as\_rules”(包括複雜的模式匹配，內容分析和啓發式)一樣的核心技術，用於對出站 SMTP 郵件進行掃描，並且設置了一個“tests”(類似於反垃圾郵件的 tests)，用於記錄某些規則(或者規則集)

的匹配情況。

2、“policy\_dlp”引擎用於檢查 DLP 的 tests，並且爲那些已經觸發的(以及那些已經配置爲攔截的) tests 應用策略攔截。

對其拆分爲掃描和執行兩個階段，我們可以非常靈活地對每個用戶有選擇性地啓用和禁用。

## “dlp\_rules”引擎

“dlp\_rules”引擎是在策略掃描階段運行的(在反病毒和反垃圾郵件掃描之後)。還可以配置爲單單出站(默認)，進站，或者雙向同時掃描。

這個引擎會對未封裝的郵件的每一部分都進行掃描，並使用其規則集對所有部分進行過濾。規則包括能夠執行複雜的模式匹配掃描，診斷信頭(例如生成的內容類型，和之前階段的掃描結果)，並對之前觸發的 tests 應用布林算術邏輯過濾。

這些規則的例子如：

- VISA 信用卡號。
- AMEX 信用卡號。
- VISA 或者 AMEX 信用卡號之一(使用布林算術邏輯)。
- 經審定的社會安全卡號碼。
- 一條匹配受限制檔集而被攔截的資訊的 MD5 校驗碼。

## “policy\_dlp”引擎

“policy\_dlp”引擎是使用方向簡單、命名的 DLP tests 和閾值來進行配置的。這樣就可以配置更加複雜的策略規則。例如包括：

· 對包含有超過 5 個信用卡號的郵件進行攔截。

· 對包含有特殊附件(通過 MD5 雜湊鑒定)的出站郵件進行攔截。

· 對包含有加密的 ZIP 檔的出站郵件進行攔截。

· 對包含有 Microsoft Excel 文檔的入站郵件進行攔截。

正如您所看到的，這些已經領先於常見的資料洩漏防禦系統所提供的功能。

## 用戶定制

“dlp\_rules”和“policy\_dlp”引擎和特徵碼集，現在都已經面向所有的 Network Box NBRS-3.0 客戶一併發佈了。這些引擎，在預設情況下是不啓用的，而且對不使用此功能的使用者也不會對其性能和輸送量產生任何影響。

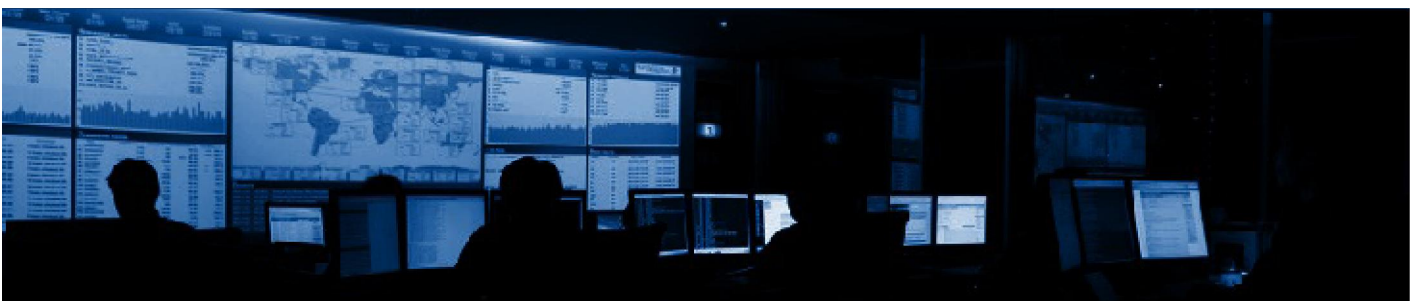
資料洩漏防護系統通常被要求有擴展的用戶定制功能，但這些卻已經超出了大部分客戶和 Network Box 所簽訂的標準管理服務協定的範圍。所有的客戶的要求各不相同，而這些規則集和策略通常必須爲基於獨立用戶而進行設計、開放和配置。

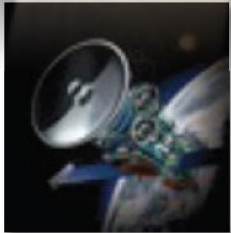
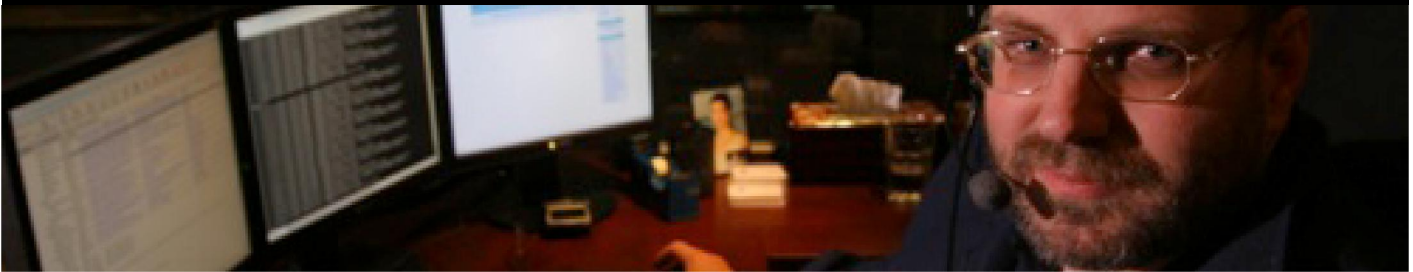
然而，引擎的有效性和複雜的規則語言應當很大程度上能夠加速這些定制的規則(並且適當地減少開銷)。

更重要的是，這些對現有的反病毒和反垃圾郵件階段的掃描不產生任何影響，也不會因此使用了不合適的工具而產生干擾。

## 結論

如果您對這項技術有什麼要求，請與您當地的 Network Box 的客戶經理或技術支援中心進行溝通。我們將竭盡我們的所能滿足您的要求，並且給予適當的建議。





### 2011 年 3 月 新特性

在 2011 年 3 月 1 日的星期二這一天，Network Box 將發佈這次的 Patch Tuesday 的補丁包，各區域 NOC 將會在未來的 7 天內安排這些新的功能的發佈和更新工作。這個月的更新補丁包包括：

- 全球監控系統 (GMS) 的增強，以及在 GMS 問題工單的性能和功能上做了優化提高。

- 全球監控系統 (GMS) 的可達性啓發式的增強，以便更好地檢測和鑒定可達性事件並且通過一個統一的方式進行報告。

- 對卡斯基 V8 反病毒引擎的修復，添加了對 winzip 新的檔案格式，並對一些非常大的檔案掃描進行了關切。

- 發佈了出站郵件資料洩漏預防功能以及郵件掃描的策略執行引擎。

在多數情況下，以上的修改並不會影響到正在運行的服務，也不需要硬體重啓。但在某些情況下（取決於具體配置），可能需要重啓設備。必要時您當地的區域 NOC 將會與您取得聯繫。

如果您還需要要關於這些的更多的資訊，請與您當地的區域 NOC 取得聯繫。他們將會進行相關的諮詢和安排。

### 2011 年 3 月 提示

雖然 Box Office 的通知系統在 2010 年 11 月份就已經發佈了，但至今只有有限的用戶在比較充分地使用這項功能。

通知系統提供了一個先進的機制，讓用戶能及時地瞭解 Box 的變化和發生的事件。這些可以通過 Network Box Office 的 My Account（以及使用者模組）進行配置。通知功能可以配置成單獨的類和事件類型（比如工單更新），並且可以以郵件、蘋果的 iOS APNS（推送通知）、Mail-to-SMS 或者 SMS 的形式發送。甚至，您還可以對不同的 box 配置發送不同的通知，並通過不同的方式（比如郵箱位址）進行發送，並且可以控制在一天中特定的時間進行通知（比如：SMS 的方式在 6:00PM 之後，郵件的形式則在這個時間之前）。

正確地對此功能進行配置，我們才能正確地向您通知關於您所管理的設備所發生的情況，並且重要的一點是，您可以有選擇地以何種方式在何時間段與您聯繫和發送通知。它也可以用於審查和對服務的管理控制。

您可以通過 Network Box Office 中右上方的“HELP”查看這項功能的線上的配置說明。

2011 年 3 月的提示就是，我們建議您研究一下 Network Box Office 的通知功能，讓我們能更好地說明您做到最好的配置。

Mark Webb-Johnson,  
CTO, Network Box Corporation

### 2011 年 3 月份 資料表

關鍵指標	#	與上月 差值百分比
PUSH升級數	611	-33.7
特徵碼發佈數	281,321	-38.6
防火牆攔截數(每BOX)	738,795	+0.2
IDP 攔截數(每BOX)	100,142	+0.1
垃圾郵件數(每BOX)	25,220	+8.2
惡意軟體數(每BOX)	705	+66.7
URL攔截數(每BOX)	119,637	+29.7
URL訪問數(每BOX)	3,939,024	+0.1

### 月刊 工作人員

總編輯：  
**Mark Webb-Johnson**

產品支援：  
**Michael Gazeley**  
**Jason Law**  
**Nick Jones**

撰稿：  
**Network Box Australia**  
**Network Box Hong Kong**  
**Network Box UK**

### 訂閱方式

寫電子郵件到以下郵箱位址：  
**Network Box Corporation**  
[nbhq@network-box.com](mailto:nbhq@network-box.com)

或寫信到以下地址：  
**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](http://www.network-box.com)

Copyright © 2011 Network Box Corporation Ltd.