In the Boxing Ring

Network Box 技術資訊

Network Box 技術總監 Mark Webb-Johnson編輯

歡迎閱讀2012年11月刊的《In The Boxing Ring》

這個月，就以我們的應用防火牆、識別、控制和監測引擎、APP掃描爲背景，來一起深入探討關於應用識別的內容。

就目前而言，大多數公司中的防火牆對所有進站協議和埠預設都是被封鎖的，只有部分特別需要的才會開放。而對於出站資料，所有的協定和埠都是被放開的，而只在特定協議和埠的流量被限制。

這個時候，問題就來了，當我們想要通過策略來加強監管控制的時候，我們需要先瞭解在LAN裡面的用戶都在運行一些什麼樣的應用，他們又是如何使用（或者濫用）互聯網連接的共用資源。

那麼，我們就來看看應用識別功能是如何解決這個問題的，並討論其更深入的細節：它是什麼，不是什麼，它又能用來做什麼。

在第4頁，是這個月對NBRS-3.0的發佈的新特性和新修復的補丁的詳情。在可預見的未來幾年，我們將繼續NBRS-3.0的開發和提高技術支援。這一頁將讓您瞭解到我們核心產品的動態資訊。

Mark Webb-Johnson
CTO, Network Box Corporation
November 2012

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

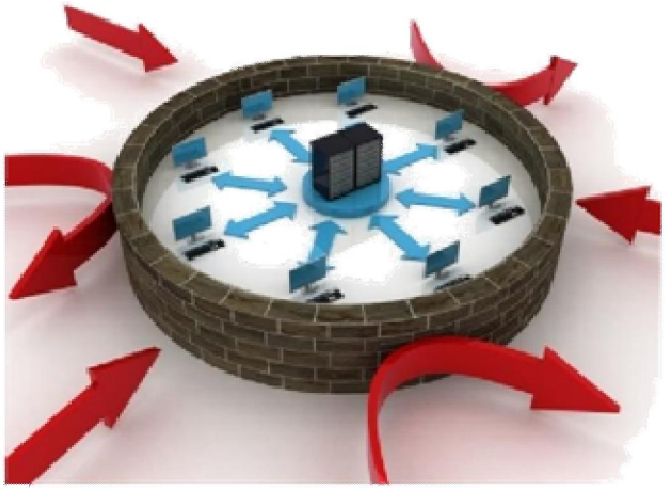
本 刊 概 要

應用識別

什麼是應用識別？

從歷史上來看，防火牆一直是通過對定義的協議和埠進行封鎖或放開的。

對於進來的資料（互聯網 --> LAN或者DMZ），在早期的電腦安全方面，防火牆開放了所有的埠，而只是對特別的埠進行了封鎖（例如：telnet以及其它管理埠）。這很容易就暴露出了問題，然後就行業性地轉移到當前市面上非常普遍的一種模式——那就是對所有進站協議和埠預設都是被封鎖的，只有部分特別需要的才會開放。如果您在DMZ區有一台WEB伺服器，偵聽著TCP/80埠，那麼將這個埠（通過防火牆）開放給互聯網，讓WEB應用的流量進入到您的WEB伺服器。



對於出去的資料（LAN或者DMZ --> 互聯網），在我看來，當前的情形依然處在電腦安全的黑色時代——允許大比例的用戶通過防火牆策略可以出站訪問所有的協議和埠，而只是對少數特別的協議和埠進行限制。

請看看上面的這個關於安全的示意圖（保持您內部組織資料系統的安全——將非法的傢伙隔離在外，而保證合法用戶正常工作不受影響），在這個圖中，對出站流量的控制可能只占了5%，而入站安全威脅問題仍然占到了95%。那麼，是不是可以說，一個寬鬆的出站安全性原則，也沒什麼可值得憂慮了呢？

當我們關注於這5%的時候，並且想要通過策略來對其加強監管控制，那麼問題就來了，我們需要先瞭解在LAN裡面的用戶都在運行一些什麼樣的應用，他們又是如何使用（或者濫用）互聯網連接的共用資源的。

應用識別便是用於解決這個問題的，它通過對經過的資料進行監視，並對其相關的應用進行識別，不通過協議或埠（例如HTTP網頁流量對應的TCP/80埠），而是通過流量的簽名特徵以及行爲分析（例如HTTP網頁流量在任何的埠上）。應用識別的方法是在最初允許流量通過，然後才能對其進行監視並發現它是什麼。這樣一來，應用就可以被識別出來，然後再對其作出相應的處理對策。

應用識別不是什麼？

我想很明確的一點是應用識別並不是一個真正意義上的安全工具。

對於入站流量（涵蓋了95%的安全問題）來說，它是沒有任何用處的，因爲您已經知道在您的網路裡面所運行的所有服務。而對於出站流量（涵蓋了5%的安全問題），一套有效的出站策略，再加上內容過濾控制，就已能足夠解決這些問題了——而且幾乎能達到零失誤率。

它能爲我們做些什麼？

我認爲應用識別最清晰、最合理的使用方法是針對允許出站的埠進行進一步的流量分析，從而提高政策執行的細微性精確性。

一旦應用被識別出來之後，便可以做出相應的策略決定。比如允許/禁止流量通過，或者應用QoS和其它頻寬控制。

應用識別的層級分類

應用識別系統可以被劃分爲7個不同精細化程度的層級，它們分別是：

1. **會話分析**
   從原始的網路資料中確定會話（以及相關的會話）。
2. **應用封裝**
   鑒定識別應用程式或用於封裝應用程式資料的協定。
3. **應用識別中的應用程式**
   通過其它應用程式或協定來識別應用程式的通道。
4. **終端解密的支援**
   在加密資料流中對應用進行識別，在應用識別的裝置上對終端到該裝置的被保護的資料進行解密的能力。
5. **以中介軟體身份進行解密的支持**
   在被保護資料經過應用識別裝置時對其進行解密的能力，並且在對資料的接收者不產生任何影響的情況下對加密資料流進行應用識別（到達接收者的資料依然是被加密的資料）。
6. **中繼資料的提取**
   對相關應用中繼資料的提取的能力。例如SMTP郵件中的郵寄地址，HTTP請求中的URL位址，以及Skype中的事務類型（聊天，檔案傳輸等等）。
7. **內容的提取**
   對相關應用傳輸的內容的提取的能力。例如SMTP會話中的郵件資訊，HTTP會話中的頁面內容，以及MSN聊天會話中所傳輸的檔等。

NBRS-3的支持

NBRS-3可以支援應用識別到左邊這個表中的第4個精細化層級。它可以在網路流量層識別比較流行的一些應用，這樣防火牆、路由、QoS以及其它一些基於控制的策略就可以被應用於這些流量了。這些還可以應用於被終端到NBRS-3.0的Network Box上的加密通道中的資料流程。

NBRS-5的支持

NBRS-5可以支持應用識別到左邊這個表中的所有的7個精細化層級。它包括識別的簽名特徵以及針對當前被廣泛使用的成百上千種不同的應用的啓發式技術。

更重要的是，應用識別存在於NBRS-5.0中核心的所有的日誌記錄、分析以及其它的基礎系統之中。NBRS-5.0還可以對網路中的應用進行統計報告，這和我們給到客戶的是一樣的。

支援對加密資料流的應用的識別，包括終端身份（VPN方式）以及中介軟體身份（代理方式）的方式均可以支援。

支援成千上萬種中繼資料，支援內容提取，並可以制定複雜規則以便策略的執行。例如，策略規則不僅可以允許/禁止MSN，還可以控制MSN與特定聊天好友進行聊天。再加上NBRS-5.0代理提供了深入和全面的協議解碼的支援，在通用的代理中應用識別內容提取就可以提供更細緻的掃描並對成百上千中應用協議進行控制。

總結

應用識別技術在安全系統中的使用時有限的，但對出站策略控制的問題提供了一個高度精確的解決方案。再加上Network Box設備上其它的策略控制系統，應用識別也將是Network Box的一項非常必要的功能。而且就現在而言，NBRS-3.0在一定程度上可以獲得支持，而在即將上市的NBRS-5.0將是可以全面地獲得支持。

Network Box Certified ISO 9001 / ISO 20000 / ISO 27001 Security Operations Centre

2012年11月 新特性

在2012年11月6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將會在此之後的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：

- 各種內部NOC系統的改進；
- 對PDF每週報告系統的微小修正；
- 即將推出的S-Scan內容過濾引擎的支援方面的改進；
- NBRS-5.0在Box Office系統中的進一步支援；
- 一系列針對Box Office和支援系統的（主要是內部）功能增強。

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。

NETWORK BOX 中東分部 | 一個新的安全響應中心（SOC）

Network Box 非常高興地向大家宣佈，我們即將又建成另外一個Network Box安全響應中心（SOC），它地處迪拜矽谷的中心地帶。將由我們Network Box中東分部的新的團隊進行管理，並由在安全領域具有一定威望的資深人士穆罕默德·阿卜杜勒·卡比爾（**Mohammad Abdul Kabeer**）進行領導。

籌建工作正在進行當中，並將在年底之前投入運作。這個全新的Network Box安全回應中心，將致力於爲中東以及北非地區（MENA）新客戶以及現有客戶提供世界一流的安全託管服務。在中東和北非地區的組織若希望能與Network Box的中東分部取得聯繫，您可以隨時與我們取得聯繫，我們將非常樂意爲您效勞。

SEPTEMBER 2012 NUMBERS

關鍵指標	數據	與上月差比
PUSH Updates	472	-10.8
Signatures Released	380,652	+16.6
Firewall Blocks (/box)	905,377	-2.4
IDP Blocks (/box)	140,423	-5.1
Spams (/box)	12,848	-8.3
Malware (/box)	1,003	+32.8
URL Blocks (/box)	160,989	-10.2
URL Visits (/box)	4,393,675	-1.9

NEWSLETTER STAFF

Mark Webb-Johnson
Editor

Michael Gazeley
Jasmine Arif
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