應用商業智慧於網路安全之研究

A Study of Applying Business Intelligence to Network Security

涂國慶 李興漢
大同大學 資訊經營學系
E-Mail:wesleytu.tw@gmail.com
E-Mail:shli@ttu.edu.tw

摘要

在不同型態的公司中，為因應各個單位網路應用與管理的需求，有越來越多的網路相關產品因應而生，協助管理者管理用戶使用網路的行為。諸如防火牆、頻寬管理器、防毒牆與入侵偵測系統...等。然而每當有網路異常行為發生或者需要分析單位內網路使用者之行為時，管理者往往必須分別登入不同的網路設備，查詢相關的紀錄並個別分析，非常不方便也沒有效率。由於不同網路設備皆有其制式的操作介面及紀錄格式，使得這些異質平台的記錄管理起來相當不容易，花費了管理者相當多的時間。因此如何讓網路紀錄能夠透過單一平台整合並快速的管理及查詢，是本論文研究主要原因，而即時與適當分析需要資訊是我們最終的決策目的。

本論文先收集各網路設備之紀錄檔，將不同設備紀錄轉入資料倉儲後，再利用商業智慧系統，擷取單位時間內所需分析之資訊，將各項設備在此一時間條件中的使用紀錄比對分析及整合，協助節省各紀錄檔之查詢時間，且有效的分析用戶網路行為。

關鍵字:稽核、商業智慧、資訊安全

1. 前言

網際網路發展至今已將近 40 年，網路行為的應用模式已由原本單純通訊行為，到目前已有越來越多且複雜性的應用。也隨者這些複雜的網路應用行為，相對的亦產生了許多不同功能性的網路相關設備，這也使的網路管理者必須學習更多的不同功能性的網路設備，單就管理維護這些不同功能性的網路設備，已花費了網路管理者相當多的時間，而且這些網路設備的皆有各自 Log 的格式，網路設備間除了各自品牌相關的產品有相同的 Log 格式外，其餘各品牌網路產品的 Log 各自獨立存在。網路設備廠商通常亦僅提供各自生產設備的分析資料庫，資料庫內已內建廠商設計好的制式統計分析資料，這些分析資料對管理者而言是不夠全面性的。

每當公司網路環境發生網路異常事件或是日常網路行為管理時，要查詢及分析使用者的網路行為，往往需至個別的網路設備上查詢該台設備的紀錄檔且無法與其他的網路設備進行關聯性分析，而且必須由網路管理者自行對不同網路設備的資料進行比較分析，這樣的管理方式無法有效且快速的提供資料給網路管理者參考及分析。

本論文期望產生一個能夠分析多種資料來源及資料形式的關聯性分析系統，當發生網路異常行為或是日常網路行為管理時，網路管理者可使用單一系統平台，查詢時間區段內相關網路設備的 Log，分析網路使用的應用行為並產生相關報表給管理者參考。

2. 相關理論與技術

2-1 現有廠商之 Log 分析產品

目前已有資訊廠商推出可整合多種設備記錄檔的 Log 分析產品，這些 Log 分析產品大概分為兩類:

- 整合自有品牌相關產品紀錄檔的 Log 分析設備，如果公司網路產品都是使用單一品牌的設備，適合使用這種 Log 分析設備，其作法是將所有設備的記錄檔送一份到該 Log 分析產品已事先規劃好相關對應欄位的資料庫內，設備已內建常用的分析報表，網路管理者只需透過管理介面即可產生相關的報表。但此種 Log 分析設備的缺點在於無法整合其他廠牌的 Log，在實際使用環境中較少有僅使用單一品牌網路產品的公司，如無法整合其他廠牌 Log，則在異常事件分析或管理時，管理者將缺少一部分的分析資料，需要再就沒有整合到其他廠牌 Log 花費額外時間查詢分析，且兩邊的 Log 須再手動比對分析。

- 整合一部分大品牌相關產品記錄檔的 Log 分析設備，此種產品整合一些市面上常用品牌的設備，其作法是將有支援的品牌設備 Log 傳送到 Log Collect Server，此 Log Collect Server 再將收到的 Log 依照資料庫欄位重新

將 Log 切割後，再匯入 Log 分析設備的資料庫內，設備已內建常用的分析報表，網路管理者只需透過管理介面即可產生相關的報表。但此種 Log 分析設備的缺點在於，無法整合所有廠牌的 Log，當公司環境內有一網路設備為該 Log 分析產品不支援時，須等待廠商更新程式後支援此設備。

2-2 ETL (Extract-Transform-Load)

各項網路設備皆有其各自存儲資料的型態及方式，為了整合及分析不同設備的資料，利用 ETL 工具將各項設備的資料經過萃取、轉置、再載入至資料倉儲內，提供給商業智慧系統來分析相關的資料。

2-3 資料倉儲

隨者公司內部員工日常網路行為的使用，各項設備的 Log 跟著增加，設備資料庫的儲存空間及各項設備資料的應用是必須考量的，利用資料倉儲系統來存放各項設備的資料，有助於往後使用商業智慧系統查詢時資料的整合及分析。

2-4 商業智慧系統

利用商業智慧系統的工具，整合後台資料倉儲內各項網路設備的資料，透過資料的淬取、整合及分析，網路管理者可用來分析異常事件發生時相關設備的資料，並產生報表提供給決策者參考。

3. 使用資料分析

3-1 網路設備 Log 分析

目前一般企業環境較常使用到的設備，其設備記錄檔可呈現的資訊如下:

- 路由器是使用在公司內部要與網際網路連接時的設備，其功能在於決定封包進出 Internet 時，所經由的路徑，其所記錄的資料為進出該設備的詳細使用資料(例:Source IP、Destination IP、Source Port、Destination Port、封包大小，使用時間…等)。

- 防火牆是使用在公司管控內部到外部或外部到內部可存取的服務、IP，以及網路位址轉換(Network Address Translation)，其所記錄的資料為進出該設備的詳細使用資料(例:Source IP、Destination IP、Source Port、Destination Port、Source NAT Port、Destination NAT Port、封包大小，使用時間…等)。

- 網路頻寬管理器的功能在於限制網路進出的頻寬及網路應用行為的管控(例:P2P 上傳下載、Facebook、Online Game、Stremedia、FTP、HTTP…等，及其他已知的應用服務)，其所記錄的資料為進出該設備的詳細使用資料(例:Source IP、Destination IP、Source Port、Destination Port、應用服務類型、存取網址、封包大小、使用時間…等)。

- 網路防毒牆是檢查進出網路流量中是否含有病毒的傳遞，若有病毒經過防毒牆後該設備將進行阻檔，其所記錄的資料為發生病毒時的被該設備檢查到的記錄(例: Source IP、Destination IP、Source Port、Destination Port、應用服務類型、病毒檔案名稱、病毒碼名稱…等)。

- 入侵防禦系統內有攻擊行為特徵的資料庫，檢查進出的網路流量中是否含有攻擊行為，當有攻擊行為產生時，入侵防禦系統會進行阻擋，其所記錄的資料為發生攻擊時為時被該設備檢查到的記錄(例:Source IP、Destination IP、Source Port、Destination Port、應用服務類型、攻擊行為特徵碼、封包大小、使用時間…等)

- 核心網路交換器是在公司環境內有許多的 IP 網段時，處理內部跨網段間的路由， 其所記錄的資料為進出核心交換器的使用資料(例:Source IP、Destination IP、應用服務類型、封包大小、使用時間…等)。

- 無線網路閘道器是在管理網路環境內，無線網路使用者經由無線網路存取點(Access Point)存取內部及外部的網路服務，其所記錄的資料為進出無線網路閘道器的使用資料(例:Source IP、Destination IP、Source Port、Destination Port、Source NAT Port、Destination NAT Port、使用者帳號、無線網卡 MAC、Access Point IP、封包大小，使用時間…等)。

- 虛擬私有網路閘道器(Virtual Private Network)是在處理分公司或個人工作者與總公司間的網路連線，藉由網際網路建立虛擬通道連接兩地的網路並作兩地網路服務存取的控制，其所記錄的資料為進出該設備的詳細使用資料(例:Source IP、Destination IP、Source Port、Destination Port、Source NAT Port、Destination NAT Port、封包大小，使用時間…等)。

- 郵件閘道器是檢查進出網路流量中是否含有垃圾郵件的傳遞，若有垃圾郵件經過郵件閘道器將進行過濾，其所記錄的資料被設備檢查到的異常記錄(例: Source IP、Destination IP、寄件者、收件者、郵件名稱、垃圾信特徵、使用時間…等)。

- 門禁管理系統紀錄員工進出的門禁時間，可進行出缺勤的考核，其所記錄的資料(例: 門禁卡編號、使用者名稱、刷卡時間、刷卡機編號、門禁權限管理…等)。

3-2 網路異常事件分析

當結合了上述幾種設備的 Log 後，透過商業智慧系統來分析出一些相關網路應用的問題，提供管理者更多的參考資料以利後續決策使用。

- HTTP/HTTPS 病毒事件分析

當一個 HTTP 或 HTTPS 病毒在網路上傳遞被防毒牆找到時，這一個病毒事件所記錄的時間、來源 IP、目的 IP、應用服務類型、封包大小等。可再經由商業智慧系統查詢頻寬管理設備的相對應的 Log，分析有問題的 IP 在查詢時間內一些網路應用行為。例如可疑 IP 是用 HTTP 通訊協定被防毒牆攔截有問題的封包。此時可再查詢頻寬管理器的資料內，可疑 IP 在時間內到訪過那些網站，而這些網站是否為已知的有害網站。

- MAIL 病毒事件分析

當一個 SMTP/POP3 病毒在網路上傳遞被防毒牆找到時，此一病毒事件所記錄的時間、來源 IP、目的 IP、應用服務類型、封包大小等。可再經由商業智慧系統查詢頻寬管理設備的相對應的 Log。例如分析被攔截的信件內來源的 IP，再查詢頻寬管理器的資料內，可疑來源 IP 在時間內是否有寄信給單位內其他收件者。並可藉由資訊安全單位所發佈之有害網站及 IP，查詢此來源 IP 是否為有害的，使管理者進行過濾。

- FTP 病毒事件分析

當使用者存取 FTP 站台，其上傳或下載檔案行為，若被防毒牆攔截到病毒，這一病毒事件所記錄的時間、來源 IP、目的 IP、應用服務類型、封包大小等。再經由查詢頻寬管理器的資料，分析時間區段，單位內有那些 IP 存取該可疑的 FTP 站台，並可藉由資訊安全單位所發佈之有害網站及 IP，來查詢校內 IP 是否有存取可疑 FTP 站台。

- Mail Spam 事件分析

當外部信件傳送到郵件閘道器時，如發現信件內由大量 Mail Spam 時，可根據郵件閘道器的記錄檔來統計哪些 IP 發送大量垃圾信件，並可藉由資訊安全單位所發佈之有害 IP 清單，來比對該 IP 是否為可疑郵件伺服器。

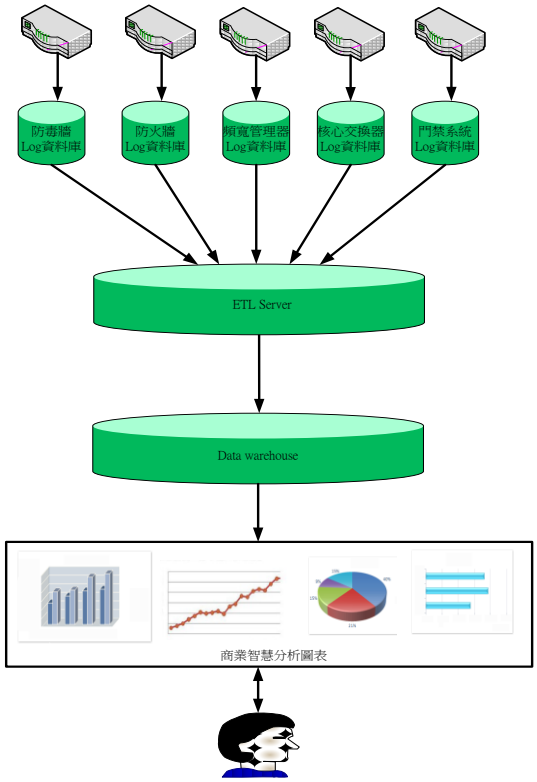
- 員工網路使用行為分析

透過頻寬管理器及防火牆的記錄檔可分析公司內部員工日常的網路使用行為，將這些使用行為分析後產生報表可提管給管理者作為決策的參考。並可利用網路設備及門禁管理系統 Log 的整合來分析異常使用行為，例如:A 員工週一請假沒有上班，但在網路行為的使用記錄上發現有該員工的使用者帳號或是 IP 的使用記錄，可藉此研判公司內部有其他員工使用 A 員工的電腦或帳號，可再對此一記錄進行網路行為使用分析，查看是否有不當的網路使用行為。

4. 系統架構

因目前市面上銷售的 Log 分析產品對不同品牌設備資料的整合不夠全面性，當網路環境中發生異常事件以及日常網路行為管理需求時，因分析資料的不足，無法有效提供資料給網路管理者參考。為了改善這些缺點，我們所規劃的系統功能主要是整合不同品牌網路設備的 Log，首先因各項網路設備的資料欄位格式及儲存欄位型態並不相同，須先將各項網路設備的資料經由 ETL 工具進行資料的萃取、轉置、再載入至資料倉儲內。

當異常事件發生或者日常的網路行為管理時，網路管理者使用商業智慧系統，查詢資料倉儲內各項設備的資料欄位，將時間區段定義完成後，選取欲查詢的相關資料欄位後進行整合分析，並可透過內建資料庫欄位比對方式快速找出需要的相關資料，進行後續報表產生及其他管理應用。



圖一 系統架構圖

5. 結論

本論文研究的網路設備記錄檔，只使用了網路防毒牆及頻寬管理器兩種設備，未來可再將其他諸如入侵防禦系統、無線網路系統、網路交換器、路由器等設備 Log 透過 ETL 工具載入資料倉儲內進行分析，這些網路設備資料整合後使用商業智慧系統進行後續的分析及提供更多有用的資料給主管，做為決策分析的參考。

參考文獻

[1] Design and Implementation of System Log Analysis and Abnormality Detection CCL TECHNICAL JOURNAL 3。25。2004。

[2] Jan Valdman(2001)， Log File Analysis，University of West Bohemia in Pilsen Department of Computer Science and Engineering Technical Report No。DCSE/TR-2001-04 July， 2001。

[3] Edward Balas and Camilo Viecco ，Towards a third generation data capture architecture for honeynets， Proceedings of the 2005 IEEE，United States Military Academy， West Point，NY， 15 - 17 June。

[4] 行政院國家科學委員會專題研究計畫成果報告 企業網路使用記錄之資料發掘 主持人：楊亨利 教授 國立政治大學 資訊管理學系 計畫參與人員：賴冠龍、郭展勝 執行期限：**90** 年**8** 月**1** 日至**91** 年**7** 月**31** 日

[5] 胡中強、沈芳逸、林佑群 大同大學 電算中心記錄檔分析為基礎的網路設備監控管理機制 2009

[6] 許浩屏 伍台國 傅振華 國防大學資訊管理系 應用誘捕系統進行網路攻擊蒐證之研究 2009 第十七屆國防管理學術暨實務研討會