植基於開放式軟件之網路防火牆設計與建置

許書瑋、蔡巧雯、許君綾、黃順利
南華大學資訊管理系
謝昆霖助理教授
klhsieh@cc.nttu.edu.tw
台東大學資訊管理系

摘　要

隨著資訊網路的風行與普及，「資訊安全」(Information Security)已嚴然成為了時下重要的課題，每個企業或學校皆使用資訊網路來支援校務的運作或企業業務的運作，但往往因為成本因素的考量下，使得企業與學校在建置資訊安全環境(防火牆)時，遇到的很大的瓶頸。開放式軟件 Netflow 是 Cisco 發展的流量統計協定，雖然擁有著強大的網路監控能力，但並無自動阻斷與異常判斷的功能，若遇到突發狀況像是流量暴增或是病毒不正常入侵，而網路管理員卻不在座位上或非上班時間，甚至是短短的幾分鐘離座時間，都有可能會使得整個環境的網路癱瘓，此時就需要能有一套整合性的操作系統把 Netflow 補強，再加上配合 NetFlow Exporter 的輸出功能，讓網管人員即使不在座位或是非上班時間情形下,也能利用這個系統來使用遠端控制網路功能或是自動切斷此有問題之網段以維護資訊網路的安全性。

關鍵字:資訊安全、防火牆、開放式軟件、NetFlow、NetFlowExporter

壹、緒論

在資訊網路的普及化之下，資訊安全的課題越顯重要，特別是電腦病毒的傳播及發作的方式也變得複雜及多樣化，早期的電腦病毒只是純粹破壞電腦的作業系統，使電腦無法作用，並藉由磁片或網路感染其它電腦，而近幾年的病毒不只如此，例如一種稱作Dos/DDos(Denial of Service、Distributed Denial of Service)攻擊模式的病毒類型，它們藉由網路四處傳播病毒，使每一台中毒的電腦對外發出大量封包，讓該區域的頻寬嚴重阻塞，嚴重影響到企業的運作。因此如何有效預防病毒的攻擊，便成爲資訊人員首要的課題及關注的焦點[1, 9, 10, 11]。

NetFlow[2, 4]是屬於一種開放式的軟件，其特色爲成本的低廉並擁有強大的網路狀態的監控能力，也因NetFlow的出現，使許多學校及企業對於資訊安全防護建設的成本大爲降低，監控能力也大幅的提高，但是由於NetFlow僅只擁有監控之能力，而無法自動的判別及阻斷異常的網路

現象，這對於網管人員在管理上來說還是稍嫌不便，因此本論文嘗試以開放式軟件中的NetFlow 爲基本架構，發展並實作一套整合性的操作系統來使整個監控系統能自動的進行連線異常訊息的判讀以及異常訊息阻斷，使得整個資訊安全防護環境更爲安全可靠。

貳、相關文獻探討

2.1 開放式軟件-NetFlow (Open Source-NetFlow)

NetFlow是Cisco發展的流量統計協定，這些統計被有效的使用在網路管理、計數及網路規劃等，目前受到很多廠商支援。Flow指的是特定來源和目地的單向流量資料，也就是分爲來源IP、目地IP、來源Port以及目地Port這四個屬性相同的封包之資料傳送量總合爲一個Flow。

2.2 NetFlow的輸出工具－NetFlowExporter

由於NetFlow廣泛被使用，相對的量測工具也非常普遍，但可惜的是NetFlow只能有少數高價的設備輸出。NetFlowExporter是一個在平凡網路設備的環境中來製造出NetFlow的輸出，可謂之爲窮人的NetFlow，因此，對於無法購置昂貴機器的公司企業來說，這是一個很好用的工具。

2.3警報過濾機制

一般網路上的警報過濾機制可以分呈動態處理和被動處理[3]，其中動態處理爲分析引擎產生警報之前就先行判斷，以避免警報資料流向管理者端造成不必要的負載或是警報氾濫。所以Tedesco[8]提出在空管網路流量機制的Token Bucket Filter運用在空管警報流量上，一旦警報流量超過其限制，就會丟棄皆下來所產生的警報，這限制了入侵偵測系統所能夠承受警報最大流量。而Klaus Julisch[5]也提出兩種方式：一種是以人工的方式來訂定無效的警報，建立這些警報的樣版，接著警報過濾器便可利用這些樣版爲條件，限制警報的產生；第二種方法則是採用被動式的找出警報在正常狀況下所產生的資料模式。至於所謂的被動處理爲分析引擎在產生大量警報資料所做的分析，利用分析所得的條件進行必要的篩選，如Manganaris[6]就是利用資料探勘的方法來找出警報在正常情況下會有的特徵方程式，同樣地把這些行爲模式建立樣本後，以作爲後續的警報過濾機制。

2.4 異質資訊偵測

Han和Cho[7]利用了所謂的系統呼叫(system call)方式計量程式在正常執行的行爲下所具有的特徵，系統資源的使用和檔案存取事件則是利用統計和條件式的方法加以模組化，最後整合這些特性和條件式的方法來描述，也就是利用不同的資料型態來描述系統正常的行爲特徵，以有效地降低誤判率。

參考文獻

[1] Stalling, William, **Network Security Essentials: Applications and Standards**, 2/e Prentice Hall, Inc. (2003).

[2] Cisco systems, **Netflow**, http://www.cisco.com/warp/public/732/Tech/nmp/netflow/index.shtml (2004)

[3] Erwan Lemonnier, **Guidelines for a long term competitive intrusion detection system**, http://downloads.ecurityfocus.com/libarary/IDS_Guidlines-Lemonnier-200110.pdf (2002)

[4] InMon Corp, **Netflow applications**, http://www.inmon.com/technology/netflowapps.php (2004)

[5] Klaus Julisch, **Dealing with false positives in intrusion detection**, extended abstract at RAID 2000, Toulouse (2000)

[6] Manganaris. S., Christensen. M., Zerkle. D. and Hermiz. K., "A data mining analysis of RTID alarms", *Computer Network*, **34**(4) (2000)

[7] Sang-Jun Han and Sung-Bae Cho, "Rules-based integration of multiple measure-models for effective intrusion detection", *IEEE International Conference on Systems, Man and Cybernetics*, **1**, 120-125 (2003)

[8] Tedesco G. and Aickelin U., **Adapative alert throttling for intrusion detection systems**, http://www.scaramanga.co.uk/words/03IJIM_aatids.pdf (2004)

[9] 林祝興、張真誠著，**電子商務安全技術與應用**，旗標出版，台北 (2003)

[10] 湯耀中，**從戰爭的觀點論資訊安全**，全華圖書出版，台北 (2003)

[11]羅榮典、潘得龍譯，**系統危機終結：透視Linux系統安全(Anonymous)**，培生教育出版，台北 (2002)