以封包過濾技術強化區域網路的安全管理

薛來銘 張阜民 高勝助

國立中興大學應用數學研究所

台中市南區國光路 250 號

TEL：(04)22840422–511，(04)22860133-506

FAX：(04) 22873028

Email：{lmshiue,fmchang,sjkao}@amath.nchu.edu.tw

摘要

網路技術的發達，網路服務也隨之增加，在使用這些服務的同時，暴露於網際網路的各區域網路使用者，將可能成為遭受網路攻擊的對象。除此之外，在區域網路內，也有可能因為其他區域內的其他不當使用者任意變更 IP 位址而產生衝突，亦或假借其他已註冊 IP 位址來超量使用網路，造成其他使用者的不便，這種種的問題一直存在區域網路之中。

為了有效解決這些問題，進而減少區域網路管理人員的工作量，在本文中將提出一個以 web 環境建構而成的區域網路管理系統，整合封包過濾防火牆、NAT 等技術，並且架設一個小型的區域網路和建構其區域網路安全系統，證明本文架構的可行性。

關鍵詞：Web-based、IPChains、NAT、Packet Filtering Firewalls、Network Management

一、前言

隨著網際網路的快速發展，網路資源與網路服務隨處可得，管理這樣開放及快速發展的網路環境，區域網路管理者常面臨著區域網路內外許多複雜的問題。由外部網路對內部區域網路而言，區域網路常面臨外界對內部網路惡意或不正常的存取行為，影響區域網路的安全，而對於內部網路，區域網路中未授權使用者盜用 IP 位址使用，造成區域網路 IP 位址衝突而無法使用，再者合法使用者超量使用網路嚴重影響對外網路連線的品質，甚至因為電腦設備增加而產生 IP 位址不足等問題。如何有效解決這些問題，以減少管理者的工作量，是區域網路管理課題的當務之急。

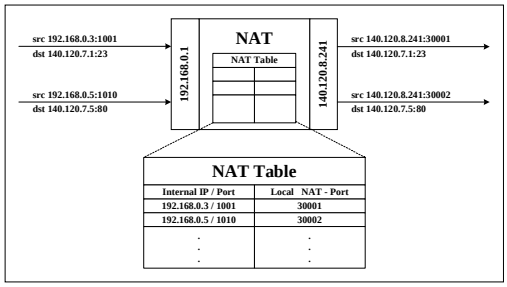
一般來說，為了保障區域網路的安全以及預防惡意或不正常的存取行為，防火牆的技術可以將區域網路與外界網路隔離，進而管制區域網路的進出，以保護區域內的網路免受於外界網路世界的干擾。防火牆基本上可分為二種：封包過濾防火牆 (Packet Filtering Firewalls) 和代理伺服器 (Proxy Servers) [1]。封包過濾防火牆主要是利用預先設定好的規則來決定資料封包是否能通過防火牆，亦即根據 IP 位址來識別封包是否合法，只有合法的 IP 位址才能自由來往於私有網路與網際網路之間。在此種機制之下，經由封包過濾器的過濾規則的事先定義，並根據所定義的規則來檢查由內而

外與由外而內各封包的資訊，並加以過濾，可以保障區域網路的安全。至於代理伺服器則是代理客戶端程式，連線至應用程式伺服器。對於應用程式伺服器而言，代理伺服相當於伺服器的客戶端程式；而對於客戶端程式而言，代理伺服器相當於應用程式伺服器。代理伺服器利用資料轉接(relay)的特性加上快取的機制來減少存取資料的時間，亦即當有重複存取資料時，可使用代理伺服器來減少了存取所需的時間。

上述所提兩種方式均能保障區域網路的安全，但對於外界多模式的攻擊，封包過濾防火牆可以利用自定過濾規則來防止這些攻擊。可是這些過濾規則的產生，如果完全由網路管理者來定義，對於網路管理者而言，是非常繁雜的工作，並且對於突發外來的攻擊與內部異常使用，無法即時的預防與阻止。因此將這類型的規則定義，採事先設定的方式，如單位時間內區網外單一機器對區網內連線的次數、區域內各使用者單位時間流量最大值的設定等等，再根據這些事先定義的設定值，利用防火牆收集由內而外與由外而內封包的資訊，經過統計與比對，自動的產生相對應的過濾規則。確定過濾規則後，對於由外而內的攻擊與異常連線，就可以加以阻擋於防火牆外。

除了惡意或不正常存取行為的問題之外，區域網路管理者也常遇到未授權使用者盜用主機位址(IP 位址)，導致主機位址衝突而無法使用，造成其他合法使用者的不便。這個問題可利用防火牆機制將其攔下，阻止其繼續使用，同時利用 ARP 表格[5]上 IP 位址和 MAC 號碼的對照，再加上硬體 Switch Hub 上的路由表，就可以查出其確切的位置。至於在管理區域下超量使用網路，導致區域對外連線品質不佳，嚴重影響其他使用者權利的問題，也可以利用定義封包過濾器規則的方式，記錄各使用者的連線狀態並加以累計，對於超量使用者，可以使用封包過濾防火牆將其阻擋，以保障其他使用者使用網路的權利。

此外，目前網際網路的興盛，新興網站如雨後春筍般大量建立，網路伺服器和個人電腦等網路設備數目的急遽增加，現有 IPv4[7]所能夠使用的 IP 位址明顯不足，新一版本 IPv6 雖提供足夠的 IP 位址，但目前未能廣泛地被採用。而面對 IP 位址的不足，可以使用 NAT (Network Address Translation) [2]的技術加以解決。在防火牆上建立 NAT Table，分別記錄區域網路對外要求連線的情形，利用這種區域網路的虛擬 IP 與對外單一 IP + port 對照，解決 IP 不足的問題，下圖為一個 NAT 運作的一個實例。



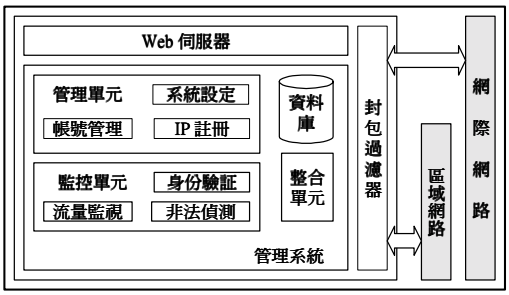
圖一、NAT 實例說明

在本篇論文中，我們研究整合封包過濾防火牆與 NAT 的技術，建立一個以 Web[8]為介面的區域網路管理系統，強化區域網路的安全性，有效地管理區域網路內主機位址，以簡化網路管理者的工作，智慧且自動地解決網路管理者所面臨的問題。

二、系統架構與運作流程

2.1 系統架構

本研究的架構由封包過濾器、Web 伺服器和管理系統三個部份組成，各部份的架構如圖二所示。



圖二、系統架構圖

在此架構下，封包過濾器扮演區域網路與網際網路的屏障，對外連接網際網路，對內連接區域網路，任何連繫區域網路與網際網的資料封包都必須通過此封包過濾器。網路管理者可以使用瀏覽器作為管理操作介面，透過 HTTP 協定[9]，連結至 Web 伺服器，進而監控及管理區域網路。

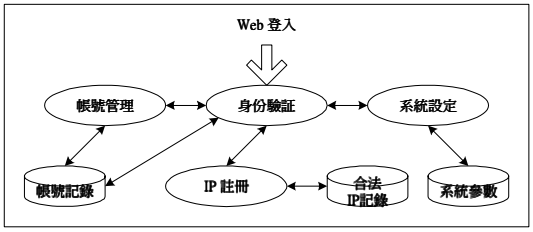
管理系統的部份則由管理單元、監控單元、整合單元和資料庫四個部份所組成：

1. 管理單元主要是在負責系統相關的設定，包括管理系統的帳號管理、授權並註冊區域網路下合法的 IP、以及設定系統相關的參數。系統的帳號以管理階級的方式來劃分，依不同的權限，可同時提供管理員與一般使用者相關的資訊。IP 註冊主要在授權區域網路下合法使用者並註冊其 IP 位址，提供系統使用，也只有註冊過的 IP，才能在區網下使用。系統設定主要是設定一些系統會使用的參數，提供給其他單元使用。
2. 監控單元負責在驗証使用者身份、區網下各 IP 的流量監視、以及區網下未授權者的非法偵測。驗証使用者主要是驗証連線至管理系統查詢相關資訊的使用者，並根據身份授與不同的權限。對於區網下各 IP 的流量加以統計匯整，提供管理系統相關資訊，進而得以控管區域網路下各 IP 的流量。在非法偵測方面，對於使用未授權 IP 或是被盜用已授權 IP 的非法使用，可以透過非法偵測的部份加以管理。
3. 整合單元為本系統的重要單元，利用系統收集的資訊，以及系統設定下的參數值，經由整合單元智慧且自動地加以匯整，建立相關資訊相對的規則，提供給封包過濾器做為封包過濾之規則之用。
4. 資料庫部份包括：系統帳號管理記錄、系統相關參數、合法授權 IP 記錄、非法盜用 IP 記錄、流量記錄和封包過濾規則記錄等等。

2.2 運作流程

在系統運作流程方面可以分成二大部分：一為網管人員的對系統的管理流程，另一為管理系統產生過濾規則的流程。

網管人員可以使用瀏覽器，透過 HTTP 協定，經由 Web 操作介面來登入本管理系統。登入時經由身份驗証單元來辨別管理人員是否合法，驗証成功後，便可合法登入本管理系統，登入後可以經由瀏覽器線上控管本管理系統，系統運作流程如圖三所示。



圖三、系統運作流程圖

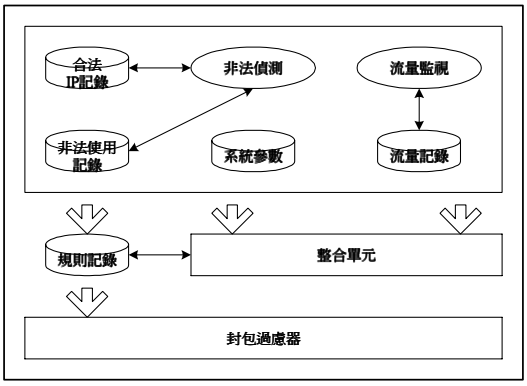
當使用者登入後根據登入帳號來劃分權限，通過身份驗証者，最多擁有三項管理設定的權限，包括帳號管理、IP 註冊、和系統設定等，並將其相關的數值分別存入帳號記錄、合法 IP 記錄、系統參數等資料庫內，提供給管理系統來使用。

管理系統產生過濾規則的流程的方面有三種產生方式：手動產生、系統相對應產生，

及經由整合單元自動產生。在手動產生過濾規則方面，主要是由因應系統的不足處，管理人員主動設定過濾規則；在系統相對應產生過濾規則方面，主要是對於臨時的改變，例如暫時停用某一個已註冊 IP 位址，將即時對此停用 IP 位址產生相關的過濾規則；第三部份由整合單元自動產生，則較為複雜，可以分列為下述幾點：

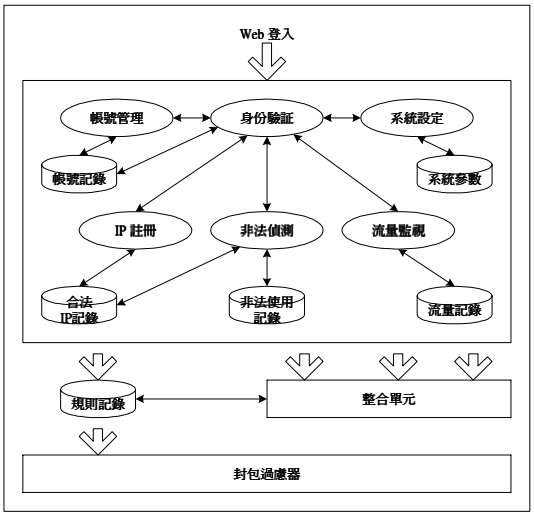
1. 非法偵測：經由已註冊(已授權)IP 的記錄，其中包括其 IP 位址和其 MAC 位址來預測，對於不合法的 IP 將無法通過封包過濾器。
2. 流量監視：藉由 IP 位址的註冊，監視區域網路的流量，若超過限定的使用量，自動地產生相對應的過濾規則來加以阻隔。
3. 區域網路安全：根據系統設定的系統參數值，可以加強區網的安全，如外界對區域網路使用 Ping 的窺視或是對區域網路下的使用者做服務的掃描。

透過以上的三種方式，可以經由整合單元自動產生過濾封包的規則，再交由封包過慮來執行。圖四為整合單元自動產生的流程圖：



圖四、各單元整合後之流程圖

整個系統經由上述兩大控制流程加以滙整，可以得的本系統的系統流程圖，如圖五所示：

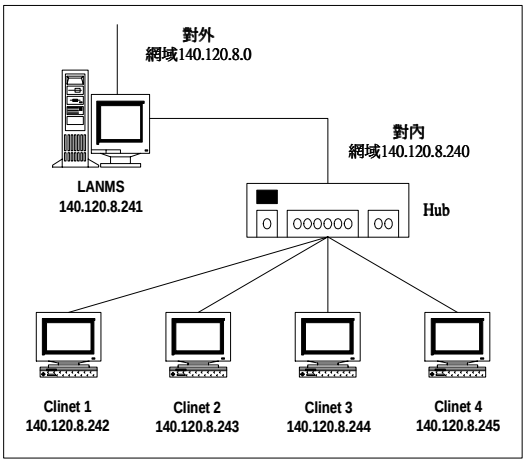


圖五、系統各單元整合流程圖

三、系統實作

3.1 實作環境介紹

本篇論文的實作環境是以一台 PC 作為區域網路管理的伺服器(LANMS)，利用此伺服器造出一個完全獨立的子網域：140.120.8.240 (140.120.8.240 ~140.120.8.248)，並以此子網域做為被保護的內部區域網路，其環境的設備如圖六所示：



圖六、實作環境設備圖

在此實作環境下，LANMS 為最主要的組成單元，也是管理系統的核心單元，對外連接網際網路，對內則保護內部區域網路，其軟體需求如下所示：

1. OS：Linux Slackware 7.1 (kernel 2.2.17)

2. 封包過濾器:IPCHAINS 1.3.9 [3] (Linux 內建)

3. Web 伺服器：Apache 1.3 for Linux

4. 程式語言：PHP 4.0、TCL 8.3

5. 資料庫系統：MYSQL 3.22.32

6. 網管發展工具：SCOTTY 2.1.10[4]

其他部份，如集線器及區域內使用者端的部份，只有本身具備支援網管功能的集線器，才可以透過集線器上 MIB[10]的相關資訊來找尋 MAC 位址、IP 位址和集線器上 port 號碼的對應。使用者端作業系統種類並無限制，只要設定閘道器 (140.120.8.241)，和子網路遮罩 (255.255.255.248) 即可。

3.2 實作系統的操作介面

1. 登入畫面

本網站位址為 http://140.120.8.241/nm/，使用者可以使用一般的瀏覽器連線至本管理系統，並輸入帳號和密碼來登入，其登入畫面如圖七所示。系統將各功能選項依權限劃分，帳號在登入後將賦予其擁有的權限，使用者也會因權限的不同，而擁有不同執行的權限。

圖七、系統登入畫面

2. 功能介紹

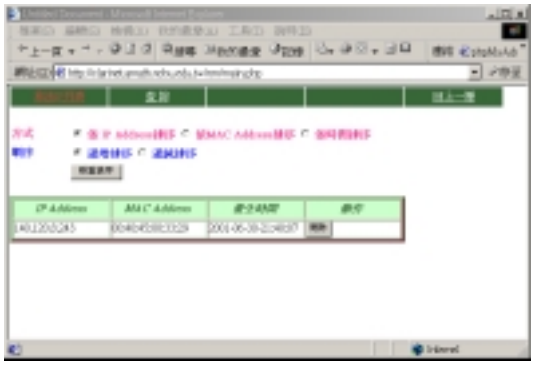
當登入系統後，可以看到其功能選項分別為：合法 IP 管理、非法記錄管理、流量管理、IPChains 設定和系統管理等五項，如圖八所示。

圖八、系統功能選項

合法 IP 管理主要負責管理區域網路下合法 IP 位址，包括管理 IP 位址和 MAC 的對照、記錄 IP 位址使用者的相關資訊、以及對各合法 IP 位址的啟用和停用，如圖九所示。

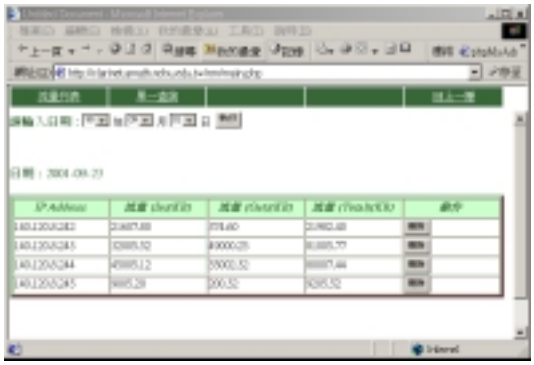
圖九、合法 IP 管理

非法記錄管理主要是記錄一些未經合非註冊，卻擅自使用合法使用者已註用的 IP 位址，有了這些記錄，再配合擁有網管功能的集線器，便可以輕易地找出盜用者的資訊，圖十記錄了盜用者盜用的時間和當時的使用機器的 MAC。本系統目前並未與擁有網管功能的集線器結合，只記錄盜用者資訊。



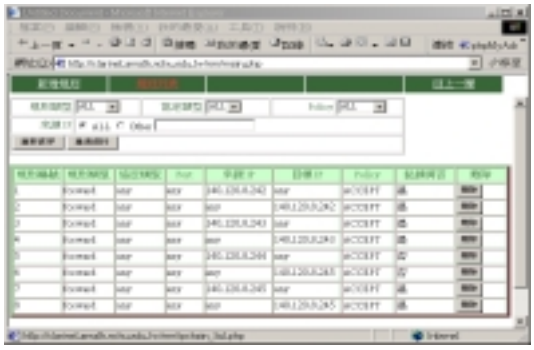
圖十、非法使用列表

流量管理在記錄區域網路內各 IP 位址的使用量，可以依日期或是 IP 位址來查詢，當使用量超過其可使用量，將自動停用些 IP 位址並將此資訊加入 IPChains 的限定，圖十一為各 IP 位址單日的使用量。



圖十一、單日流量使用圖列表

IPChains 設定在記錄和管理目前 IPChains 封包過濾器的過濾規則，可以使用自訂方式加以增刪，或是利用系統自動產生過濾規則，圖十二為過濾規則列表。



圖十二、過濾規則列表

系統管理在管理系統的帳號和常駐程式的時間設定，些功能選項影響系統的運作極深，當然也會因各登入帳號的權限來限制其使用權，圖十三為常駐程式的時間設定的運作畫面。

圖十三、常駐程式時間設定

四、結論

使用者在使用網路服務時，因暴露於網際網路上，可能成為遭受網路攻擊的對象，同時亦可能遭受區域網路內其他使用者因恣意變更 IP 位址而產生衝突，甚至超量使用網路，大大減低網路品質。區域網路管理人員在面臨這些複繁的問題，可能需要投入大量的時間來解決。本論文提出以封包過濾防火牆為核心來建構一區域網路管理系統，保護內部區域網路不受外界惡意的攻擊，以提高區域網路的安全，並選擇以 Web 作為操作介面，達到跨平台的優點，方便於管理者來管理區域網路。而區域網路下，因盜用已註冊 IP 位址而產生衝突、或是未經過註冊擅自使用 IP 位址，而會影響到合法者的權利，甚至於包括合法使用也可能因為網路的超量使用，嚴重的影響網路的品質。這種種的問題在本論文中，利用建立封包過濾規則和分析統計封包記錄的方式，也得到解決，大大地降低管理員的工作量。

在本論文的架構中提到加入 NAT 的技

術，藉由使用虛擬 IP 位址的方式來解決 IP 位址不足的問題，在實作的系統內並未引用，其主要原因在於本系統建立在中興大學應用數學系區域網路環境，目前當未有 IP 不足的問題，故未加入 NAT 的解決方案。但是一個多方位的區域網管理系統必須擁加入 NAT 的技術，以解決 IP 不足的問題，這也是未來可再繼續努力的方向。`

此外，本系統最主要的目的在於簡化網管人員的工作量。為了達到這個目的，我們以分析記錄的方式來自動增加封包過濾的規則，例如網路超量超用或是外界對內部網的攻擊等等。但事實上，記錄分析而產生封包過濾規則的機制，必須要有豐富的網路經驗和精確的判別能力，才能有效地設計出些機制，達到封包過濾的目的，這亦是日後有待努力的另一個方向。

參考資料

[1] Gary Palmer and Alex Nash, “Firewarll” in FreeBSD Handbook, http://www.freebsd.org/ , October 1995.

[2] Michael Hasenstein, “IP NETWORK ADDRESS TRANSLATION”, http://www.suse.de/~mha/HyperNews/get/linux-ip-nat.html, 1997.

[3] Paul Russell, “Linux IPCHAINS-HOWTO”, http://www.linuxdoc.org/HOWTO/IPCHAINS-HOWTO.html, Jul 2000.

[4] J. Schönwälder and H. Langendörfer, “Tcl Extensions for Network Management Applications”, http://wwwhome.cs.utwente.nl/~schoenw/, July 1995.

[5] David C. Plummer, “An Ethernet Address Resolution Protocol”, RFC 826, Nov. 1982.

[6] S. Bellovin, “Firewall-Friendly FTP”, RFC 1579, Feb. 1994.

[7] B. Carpenter, J. Crowcroft and Y. Rekhter, “IPv4 Address Behaviour Today”, RFC2101, Feb. 1997

[8] J. Patrick Thompson: “Web-Based Enterprise Management Architecture”, IEEE Communications Magazine, Mar. 1998.

[9] T. Berners-Lee, R. Fielding and H. Frystyk, “Hypertext Transfer Protocol -- HTTP/1.0”, RFC 1945, May 1996.

[10] K. McCloghrie, M. T. Rose, “Management Information Base for Network Management of TCP/IP-based internets: MIB-II”, RFC 1213, Mar. 1991.