具有 AAA 之動態防火牆研究與建置

[1]廖鴻圖　[2]吳瑞堯　[3]陳進偉
世新大學資訊管理學系
[1]htliaw@cc.shu.edu.tw
[2]rywu@cc.shu.edu.tw
[3]alan.chen@wpghome.com

摘要

近年來網際網路的盛行，已改變人們日常生活的作息，人們已逐漸依賴網路的連線使用，不論是上網查詢資訊、網路購物、使用網路銀行轉帳、收發電子郵件...等，無時無刻均需要網路的使用，無論在公司、家中、機場、咖啡廳、甚至於速食店均有網路連線的需求，以供公務、私人、休閒...等需求。有了網路連線需求，自然衍生出帳號認證管理(Authentication)、連線授權管控(Authorization)、進而再繁衍出計費管理需求(Accounting)，以增加商務提供服務之收入。

現今大多數企業均以架設防火牆作為管控網路安全為核心，設定適合多數人員之通用防火牆規則，以及限定少數特殊 IP 擁有較多的網路連線存取功能。並未能依使用的人員來設定使用網路連線權限，只能設定使用者的設備來作為依據，其未能符合實際使用情境。故綜觀網路使用認證、網路連線授權與計費管理需求，需要一套機制及系統來達到依使用者認證角色觀念來授與網路使用權且具有計時計量之計費管理機制，以符合現況之需求。

本研究以動態防火牆為核心基礎，以使用者認證及依角色授權觀念延伸至網路連線使用層面，來建構一個系統。使用者在使用網路時，需要藉由網路認證授權機制，並依其認證之角色來授予網路使用權，動態地即時建立防火牆規則，並以使用者的網路連線之時間與流量來完成計時計量之計費管理機制，以達到認證、授權及計費(簡稱 AAA) 目的之需求。

關鍵詞：認證(Authentication)、授權(Authorization)、計費(Accounting)、動態防火牆(Dynamic Firewall)。

1. 前言

近年來網際網路的盛行，已改變人們日常生活的作習，人們已漸漸依賴網路的連線使用，不論是上網查詢資訊、網路購物、使用網路銀行轉帳、收發電子郵件...等，無時無刻需要網路的使用，無論在公司、家中、機場、咖啡廳、甚至於速食店均有網路連線的需求，以供公務、私人、休閒...等需求。有了網路連線需求，自然衍伸出帳號管理(Authentication)、連線授權管控(Authorization)、進而再繁衍出計費管理需求(Accounting)[5][6]，以增加商務提供服務之收入。

現今大多數企業均以架設防火牆作為管控網路安全為核心，設定適合多數人員之通用防火牆規則，以及限定少數特殊 IP 擁有較多的網路連線存取功能。當有來賓來訪需要用網路連線時或擁有特殊網路權限使用者想暫時使用他人電腦要連線時，就會發生網路管理者需要常常修改防火牆規則，或事後忘了要取消暫時開通的防火牆規則，以致造成網路安全的漏洞。

現行企業之授權使用觀念，大都局限在應用系統之認證，使用者認證後再以使用者角色觀念來依不同角色授予有不同的使用權。在使用者電腦與應用系統要建立連線時，第一步要通過的是網路使用權，企業大都以防火牆來作為網路使用權的管控，而防火牆的規則通常為符合大眾通用原則來設定，除了少數特定使用者設定固 IP 及依特定 IP 來設定特殊的防火牆規則外，另手提電腦、PDA..等行動設備普及，更增加管理固定 IP 的困難度，缺乏了依使用者角色觀念來建立防火牆規則及網路使用權。故需要一套機制來依使用者認證角色授權觀念來建立網路使用權，並達動態防火牆規則建置。

除了網路安全問題外，部份的企業、餐廳或社區管理委員會...等服務業者，需要提供給使用者網路連線服務，進而從網路連線服務的提供，來獲取網路加值服務費用，以創造新的營業收入，以及對網路流量的管控與限制。進一步地需要帳戶管理及網路連線計費管理之需求。

綜觀網路使用認證、網路連線授權與計費管理需求，需要一套機制及系統來達到依使用者認證角色觀念來授與網路使用權且具有計時計量之計費管理機制，以符合現況之需求。

2. 研究目的

本研究以動態防火牆[7]為核心基礎，以使用者認證及依角色授權觀念延伸至網路連線使用層面，來建構一個系統。使用者在使用網路時，需要透由網路認證授權機制，並依其認證之角色來授予網路使用權，動態地即時建立防火牆規則，並以使用者的網路連線之時間與流量來完成計時計量之計費管理機制，以達到 AAA [17]目的之需求。

此研究使用 Linux 平台之 iptables、php、mysql、apache、perl、ntop… open source [1][2]套件，建構一個完整且安全的 SSL 加密網路認證機制，並使用網路流量資訊[3]與使用時間來達到計時計量之網路計費管理之需求。

2.1 將使參與者獲下列幾點心得:

a).瞭解 Linux 平台架構與基本認識。
b).Linux 各奪件間之連結與整合應用。
c).動態防火牆基本原理與整合應用。
d).運用 SSL 加密與網路認證之整合應用。
e).網路流量管理原理與分析。
f).計費應用架構與分析管理。
g).系統自動化及網路安全監控。

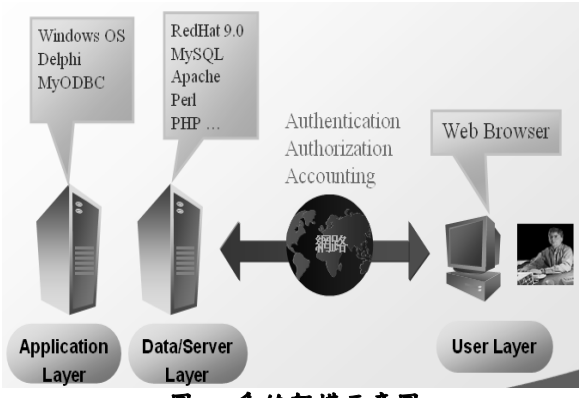
2.2 預計達成功能:

a).在 Linux 平台上建構 SSL 加密網路認證機制[9]，加強網路認證安全[10]。
b).建置網路計費管理機制，提供網路使用權與計費觀念整合。
c).無需在使用者電腦安裝特殊軟體，即可達到認證需求。
d).改善現有防火牆單向(正面 or 負面表列)統一規則限制，達到以使用者角度來訂定動態防火牆規則。
e).提供有線網路與無線網路認證服務。
f).提供個人化及團體計費拆帳服務。
g).提供使用者認證鎖定 IP 與 MAC address 功能。
h).自動判別使用者已離開網路連線機制。
i).網路連線異常時，自動進行流量限制或切斷使用者連線。
j).整合 DHCP server，防範自定 IP 之違法電腦進入網路連線。
k).結合網路認證及網路連線授權之整合。
l).系統整合管理介面。

3. 系統架構

系統架構將以系統架構示意、系統功能架構、計費架構等三個層面來分別作說明及討論。

3.1 系統架構示意



圖一 系統架構示意圖

網路認證、授權、計費管理系統架構依管理設定主控端(Application Layer)、系統主機運作端(Data/Server Layer)及使用者端(User Layer)，區分為 3 個 Layer，以下為圖一 系統架構示意圖之 3 個 Layer 說明。

a).Application Layer：

為管理設定主控端，平台是在 windows OS，管理設定主控端程式是由 Delphi 來開發設計管理介面程式，並透由 ODBC 來與 server 連接資料庫，並作為帳戶管理、網路權限設定、計費機制設定…等相關維護管理用途。

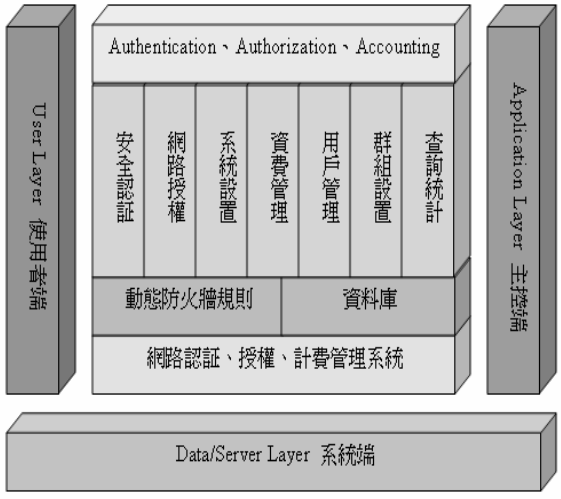
b).Data/Server Layer：

是主要核心運作的伺服器，平台是在 Linux RedHat 9.0 [16]上建置，安裝的套件有 MySQL、Appache、Perl、PHP、ntop、iptables…等 Linux OpenSource 套件。整合相關套件之連結整合來達到使用者認證機制、帳號權限判斷、使用者是否已離開網路、計時計量累計及使用費用計算…等相關功能運作。

c).User Layer：

使用者方面，只要使用 IE 瀏覽器開啟任意的網站，其 Server 會將其連線 session 轉導到 Server 的網路認證網頁，故使用者不需要額外安裝任何的 agent 軟體，即可作認證登入及網路授權使用，方便使用者操作。

3.2 系統功能架構



圖二 系統功能架構圖

網路認證、授權、計費管理系統以動態防火牆規則作為網路使用授權及網路管控用途，以資料庫作為用戶資料、系統設置參數、資費管理及查詢統計之基礎核心，以下為各模組說明。

a).用戶管理：

i.開戶、銷戶、收費、查詢、修改用戶資料功能
ii.可鎖定未繳費之用戶。
iii.可設定群組。
iv.匯出使用者資訊。

b).群組設置：

i.群組建立、刪除、修改資料功能。

ii.封鎖用戶群組。

c).系統設置：

i.使用者權限設定，細項設定各模組功能。

ii.系統參數設定，決定系統細項功能行為。

iii.多個操作員同時操作。

iv.用戶可以即時查詢自己的使用紀錄，修改資料。

d).安全認證：

i.支持用戶端登錄，Web 登錄。

ii.使用 SSL 加密網路認證。

iii.可鎖定 MAC 及限定用戶 IP 上網行為。

iv.支援內網 NAT，多段 DHCP，位址對應。

e).網路授權：

i.多功能選擇使用者網路服務功能。

ii.可設定群組決定提供網路服務功能。

iii.目標位址控制過濾策略。

iv.完整的登錄紀錄，訪問紀錄。

v.即時顯示線上用戶資料、使用時間和流量。

vi.監看使用者可依條件是選擇要監試使用者。

vii.封鎖上線使用者。

f).資費方案：

i.可設定時間優惠、流量優惠、時間包套、流量包套。

ii.用戶結帳可支援單一用戶結帳及群組多人同時結帳。

iii.用戶繳費單一及群組繳費方案。

iv.可列印使用帳單。

v.支援計費方式多樣，如時段計時、時段計量、級距計時、級距計量、大額級距優惠、月結型、限量型、企業拆帳等。

g).查詢統計：

i.可條件式查詢已繳費或未繳費。

ii.可根據年月及使用者資訊查詢繳費資訊。

iii.每日線上使用人次統計表。

iv.每日應收費用及總流量統計表。

v.每月未結帳單統計表。

3.3 計費架構

網路認證、授權、計費管理系統的計費架構主要是依"計時間"及"計流量"來作基本元素，再加上"依時段"及"級距"來搭配作多種變化。其"時段"是指"0-24"小時，每一個小時作為一個計費時段，每個小時可依不同費率來設定，且不同資費方案可以有不同的時段費率表。如表一 依時段之計時計量示範表，其 1 時為 0-1 點，依"計時"費率為每分鐘/0.5 元，依"計量"費率為每 100KB/1 元，其餘依不同時段有不同的費率。

"級距"就是指"累積使用量"，不同階段的累積量有不同的計費費率，其 0-20 小時、21-50 小時…或 0-5GB、5GB-10GB…流量值，各擁有不同的費率，且不同資費方案可以擁有不同的時段費率表。如"表二 依級距之計時計量示範表"，其"計時/級距"之 0-20 是指 0-20 分鐘期間內費率為每一分鐘/1 元，21-50 是指第 21 至 50 分鐘期間其費率為每一分鐘/0.9 元。其"計量/級距"之 0-5BG 是指使用流量 0-5GB 內費率為 100KB/1 元，5-10GB 是指第 5GB-10GB 內費率為 100KB/0.9 元。其餘級距以此類推。

表一 依時段之計時計量示範表

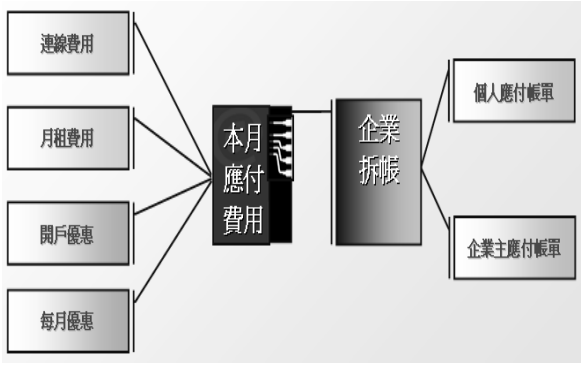
時段	計時	計量	時段	計時	計量
1 時	0.5 元/分	1 元/100KB	13 時	1 元/分	1 元/50KB
2 時	0.5 元/分	1 元/100KB	14 時	1 元/分	1 元/50KB
3 時	0.5 元/分	1 元/100KB	15 時	1 元/分	1 元/50KB
4 時	0.5 元/分	1 元/100KB	16 時	1 元/分	1 元/50KB
5 時	0.5 元/分	1 元/100KB	17 時	1 元/分	1 元/50KB
6 時	0.5 元/分	1 元/100KB	18 時	1 元/分	1 元/50KB
7 時	0.5 元/分	1 元/100KB	19 時	0.7 元/分	1 元/75KB
8 時	1 元/分	1 元/50KB	20 時	0.7 元/分	1 元/75KB
9 時	1 元/分	1 元/50KB	21 時	0.7 元/分	1 元/75KB
10 時	1 元/分	1 元/50KB	22 時	0.7 元/分	1 元/75KB
11 時	1 元/分	1 元/50KB	23 時	0.7 元/分	1 元/75KB
12 時	1 元/分	1 元/50KB	24 時	0.7 元/分	1 元/75KB

表二 依級距之計時計量示範表

級距	計時	級距	計量
0-20	1 元/分	0-5GB	1 元/100KB
21-50	0.9 元/分	5-10GB	0.9 元/100KB
51-100	0.8 元/分	10-20GB	0.8 元/100KB
101-200	0.7 元/分	20-50GB	0.7 元/100KB
200-1000	0.6 元/分	50-100GB	0.6 元/100KB
1000↑	0.5 元/分	100GB↑	0.5 元/100KB

表三 資費方案與附加方案表

		附加方案			
		每月租費	開戶優惠	每月優惠	企業拆帳
資費方案	分時計時	Yes/No	Yes/No	Yes/No	Yes/No
	分時計量	Yes/No	Yes/No	Yes/No	Yes/No
	級距計時	Yes/No	Yes/No	Yes/No	Yes/No
	級距計量	Yes/No	Yes/No	Yes/No	Yes/No
	大額限時	Yes/No	Yes/No	Yes/No	Yes/No
	大額限量	Yes/No	Yes/No	Yes/No	Yes/No



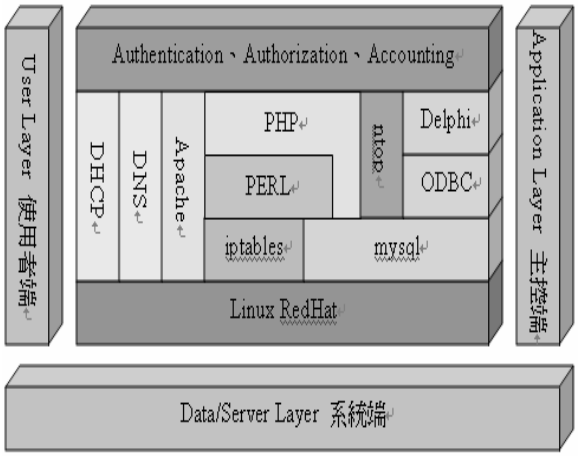
圖三 計費架構圖

資費方案有四個基本方案為“分時計時”、“分時計量”、“級距計時”、“級距計量”、以及”大額級距”與計時計量搭配,另再增加二種資費方案為”大額限時”及”大額限量” ，其變化為 6 個基本型資費方案，如”表三 資費方案與附加方案表”。每個基本型資費方案配合“每月租費”、“開戶優惠”、“每月優惠”方式來計算出用戶”本月應付費用”，如”圖三 計費架構圖”。最後再以個人或企業拆帳方式來作最終的應付款項，以因應不同使用需求。而這些的應用,可以發展出 96 種的計費方式。

4. 系統建置

系統建置單元將分別以系統端建置說明、運作流程說明、網路架構圖來探討

4.1 系統端建置說明



圖四 系統架構圖

網路認證、授權、計費管理系統是建構在 Linux RedHat 9.0 平台上，運用各套件功能並加以整合，以達到所需之目的，以下為各系統架構之說明。

a). Linux

系統建置在 Linux RedHat 9.0 OS，並安裝 iptables、DHCP、DNS、apache、php、mysql、perl、ntop…等 opensource 套件，並設定套件相關設定，及套件之間的連結整合，以達到所需功能運作及目的。

b). DHCP

網路 IP 發放部份以 DHCP 來配發網路 IP address，除 IP 發放功能外，因其 DHCP server 在發放 IP 外均會在 log file 上記載那一台電腦名稱及 MAC address 分配到那一個 IP address，有了這些資訊，使用者在認證時，系統主機可以在認證時判斷其 IP address 是否為系統所發出來的 IP address，藉此判斷出 IP address 是否合法或為使用者自定 IP address，合法 IP 則進行後續程序，若為非法 IP 或自定 IP，則可拒絕作認證程序，如此可以強化網路安全及解決 IP 被偷用的狀況。

c). DNS

DNS 用途為作 DNS cashe 用途,系統會設定使用者在詢問 DNS 時，會先詢問系統主機，系統主機會詢問後再回覆給使用者電腦，以節省 DNS 詢問流量。

d). Apache+PHP

系統以 apache[4]來作 Web server,並起動 SSL 加密機制來保護使用者連線登入認證時的資訊，搭配 php[14]程序來建構出 web 認證程式，透由 php+apache 整合來達到 web 認證介面。

e). mysql

系統之資料庫採用 mysql[11]，並定義相關 tables，及搭配 php[15]與 perl 程式來存取資料，以讓系統可以達到計算及判斷所需。

f). ntop

ntop[12]套件為收集網路流量資料，配合 perl 程式來將 ntop 所獲取網路流量資料取出及整理,再轉存回 mysql 資料庫內，以供即時偵測程式或系統程式判斷相關資訊用途。也以此獲取流量資訊來計算出使用者所使用之流量值。

g). iptables

使用 iptables[8]來作動態防火牆規則定義，利用 iptables 彈性的指令及配合 perl 程式來達到動態設定防火牆規則，故可以使用者角色來授權使用可以用的網路權。一般防火牆均以通用的規則及正面規則表列或負面規則表面，此種通用的原則是以管理者角度來思考及方便設定，而實際狀況為不同的用戶會有不同的方式，故以用戶角色觀念來實現不同用戶會有不同的防火牆規則，也強化網路安全。

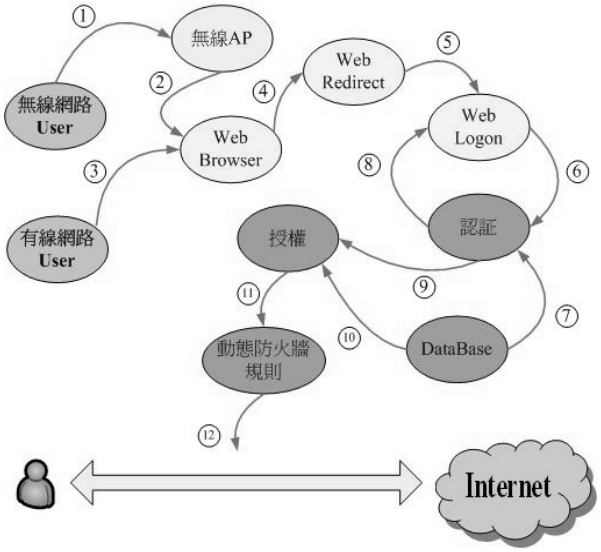
h). perl

藉以 perl[13]程式來執行 Linux 系統程式及連結 mysql 資料庫，以系統程式所需來獲取相關資料及計算數值，並可執行 iptables 指令來達到動態防火牆功能。

i). Delphi

系統設定相關介面將於 Delphi 程式開發主控台程式，以供管理者設定相關資料及建立帳號用途，也以此介面來作報表查看及線上網路監看。

4.2 運作流程說明



圖五 運作流程說明

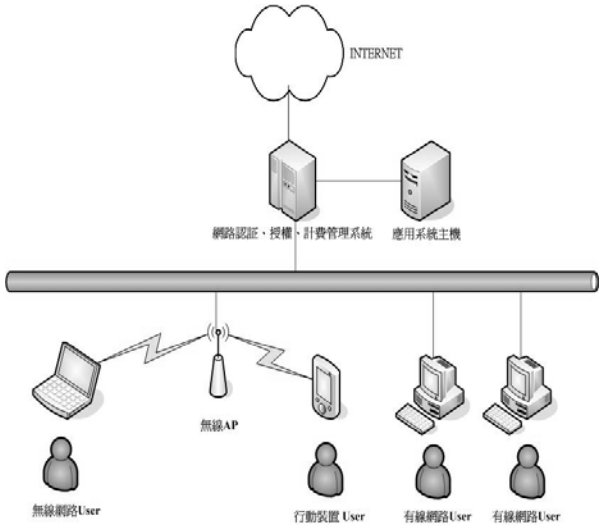
本研究為了方便使用者操作使用，希望在使用者端不要額外安裝任何的 Agent 軟體，且要符合網路認證需求，故利用 iptables Redirect 功能來將使用者之 Web 轉導至系統認證網頁，並啟動 Apache SSL 加密機制來保護認證資訊及加強網路認證安全。認證後並以角色來授予網路使用權，使用者即可以被授權程度來使用網路連線，系統主機會依使用時間及使用流量來記錄及計算，系統也會自動判斷使用者是否已離開網路，以達到自動判斷是否已離開網路功能，以下為運作流程步驟說明。

1) 無線網路使用者需先透過無線 AP 之加密機制來取得網路連線。
2) 無線網路使用者需先開啟 IE Web Browser 輸入任一的網址來作網路認證。
3) 有線網路使用者在接上網路後，需先開啟 IE Web Browser 輸入任一的網址來作網路認證。
4) 使用者開啟 Web 後，電腦會連線到網路並透過系統主機作網頁下載動作。
5) 系統主機 iptables 會判斷是否已有防火牆規則，若無則自動將此 session 轉導至系統 Web Logon 網頁，以提供使用者認證，並啟動 SSL 加密機制。
6) 使用者依個人帳號及密碼輸入並作認證。
7) 系統確認帳號密碼是否符合、有無鎖定 IP/MAC address、IP 是否為 DHCP server 所發出、是否被帳號封鎖…等機制判斷。
8) 若認證不過則網頁會重導回網路認證網頁，以作重新認證。
9) 認證通過後，系統會依使用者角色來授權。
10) 系統依資料庫定義使用者的網路使用權限、是否有被限制的網站及主機 IP address，來判斷並授予權限。
11) 系統依使用權限來設定 iptables rule 來達到動態防火牆規則。
12) 使用者即可開啟所需要的應用軟體，如 email、ERP、Web Browser、MSN…等所需要使用的網路連線。

4.3 網路架構圖

網路認證、授權、計費管理系統的網路架構如圖六 網路架構圖，其系統是放置在 Internet 與 Intranet 中間，使用者電腦屬於 Intranet，使用者任何的網路連線均會經過系統作判斷是否擁有網路使用權，若擁有網路使用權，系統會讓此連線通過。無線網路使用者需先通過無線 AP 加密機制後，才可以經由無線 AP 來連接網路，包含行動裝置使用者也需通過無線 AP 來使用網路。

應用系統主機可放置在網路認證、授權、計費管理系統的非軍事區網段、可達到對應用系統主機之網路連線判斷、以加強對應用系統主機之網路安全。使用者連線至 Internet 時，系統會作 NAT 轉址以透過系統來連上 Internet，且無需增加 NAT 裝置，讓使用者可以方便 Internet 連線。



圖六 網路架構圖

5. 結論

本系統以 Linux 為平台，搭配 Open Source 套件-Apache、php、mySQL，建構網路認證機制，在系統上加入帳戶管理、MAC/IP Address 鎖定功能，並結合 SSL 加密網路認證機制，以強化網路認證安全性，也結合 DHCP server 並在使用者登入時判斷是否為非法自定 IP 用戶，來抑制非法使用網路連線。在無線網路可配合無線 AP 之 WEP 加密功能，來保障無線網路連線安全。系統也會隨時判斷網路使用戶是否已離開網路，並把已離開網路用戶取消網路使用權，以保障用戶權益及網路連線安全。

利用動態防火牆為核心基礎，藉由使用者依角色授權觀念來動態地即時產生防火牆規則，來授予網路使用權，並可依使用者角色來訂定正面表列防火牆規則或負面表列防火牆規則，以改善目前大多

數防火牆只能單一地使用面表列或負面表列防火牆規則的困擾，大大地加強防火牆規則彈性，且具有即時性動態防火牆功能。並可以設定那些是以連線的 IP address，甚至於可鎖定 port service，以強化網路連線的嚴謹度。

使用者在網路連線認證時，系統利用 redirect 功能轉導至認證網頁，使用者無需額外加裝 agent 軟體即可完成網路認證，增加使用者的方便性，也減少網路管理人員去使用者端安裝軟體的負擔。系統也提供了管理介面及線上網路監控機制，以方便管理者設定及監控網路異常行為。計費機制部份，利用"時間"、"流量"分成六個計費基本型，搭配不同的優惠需求，組合成多種的資費方式，來因應市場多樣化的需求，且提供了個人與企業拆帳方式，更提供了不同付款方式，更能符合市場需求。

本研究以動態防火牆為核心，建構具有網路認證、角色授權、計費管理系統，把依角色授權概念從應用系統延伸至網路使用權，即時動態地產生防火牆規則，加入 SSL 加密網路認證及結合計時計量功能來計算使用時間及使用流量並搭配多樣化的資費方案來達到具有 AAA (Authentication、Authorization、Accounting) 之動態防火牆系統。

參考文獻

[1] 鳥哥（VBird）, "鳥哥的 Linux 私房菜－基礎學習篇增訂版", 2003 年，台灣，上奇科技。

[2] 鳥哥（VBird）, "鳥哥的 Linux 私房菜－伺服器架設篇 , 2003 年，台灣，上奇科技。

[3] 蔡一郎, "Linux 網管技術" ，2003 年，台灣，上奇科技。

[4] Apache, http://www.apache.org/

[5] Authentication , Authorization and Accounting in Ad Hoc networks 26th of May 2000 Sami Levijoki Department of Computer Science Helsinki University of Technology, http://www.tml.hut.fi/Opinnot/Tik-110.551/2000/papers/authentication/aaa.htm#chap3.1

[6] Authentication Authorization and Accounting requirements document, http://www-unix.gridforum.org/mail_archive/ur-wg/msg00164.html

[7] Building Internet Firewalls, 2nd Edition By Elizabeth D. Zwicky, Simon Cooper, D. Brent Chapman 2nd Edition June 2000, http://www.oreilly.com/catalog/fire2/

[8] iptables, http://ccw0729.wakanet.com.tw/linux/linux_iptables.html

[9] Kerberos:The Network Authentication Protocol, http://web.mit.edu/kerberos/www/

[10] Linux Security Cookbook By Daniel J. Barrett, Richard Silverman, Robert G. Byrnes, http://www.oreilly.com/catalog/linuxsckbk/index.html

[11] MySQL Database, http://www.mysql.com/

[12] Ntop, http://www.ntop.org/ntop.html

[13] Perl, http://www.perl.com/, http://www.perl.org/

[14] PHP , http://www.php.net/

[15] PHPMyAdmin, http://www.phpmyadmin.net/home_page/

[16] RedHat, http://www.redhat.com/

[17] RFC 3539 on Authentication, Authorization and Accounting (AAA) Transport Profile, http://www.mail-archive.com/aaa-wg@merit.edu/msg00010.html