第一章 網路負載平衡器

教育部建構「新一代校園寬頻有線及無線網路環境」2009 年迄今已經有六年的時間，整個校園網路環境有很大的改變。

1.1 背景分析

為了達成 IPv6 的環境，各縣市通常採購不外乎 L3 交換器或防火牆，這些設備經過了六年的時間，有些已經老舊或效能不敷使用，有部分縣市及學校在經費許可下已經採購新的設備，但有些縣市因為預算的關係，無法採購新的 IPv6 防火牆設備。

教育部中小學行動學習推動計畫於 2014 開始，其中有補助一條 200M 的線路供行動學習使用，但大部分於「新一代校園寬頻有線及無線網路環境」所購置的防火牆的 WAN 埠實際傳輸無法到達 200M 以上。

1.2 pfSense 簡介

pfSense 為免費、開放原始碼的一套作業系統，主要專注在防火牆以及路由器上。pfSense 基於 FreeBSD 作業系統，源自於輕量化 m0n0wall 防火牆系統發展而來，迄今已經有十年的時間。由於 pfSense 功能強大並提供 Web 方式的操作介面，在全世界已有超過 20 萬台的 pfSense 主機正在運作。

pfSense 可用來取代學校舊有的路由設備，並簡化校園的網路架構，除了 Multi-WAN 與 IPv6 支援以外，搭配 pfSense 所提供的套件，可以獲得網址過濾、流量分析、Botnet 黑名單偵測阻擋、VPN 等功能，因此透過機架式主機安裝 pfSense，可以讓學校使用最少的預算到達最高的網路效能。

1.3 pfSense 功能特色

pfSense 可免費取得，提供高效能、穩定性的選擇，主要特色以下說明：

（1） Web GUI 介面提供使用者方便操作與設定
（2） 設定檔為 XML 格式，可備份與還原，透過南投版設定檔便於各校導入
（3） 透過 Squid 快取伺服器，節省頻寬並降低網路負載
（4） 提供 URL 黑名單過濾機制，可以自行定義或由網路上自動下載黑名單
（5） 七萬筆 IP 黑名單，包含 Botnet、Spyware、Malicious、OpenBL 等
（6） 使用 OpenVPN，可自動產生設定程式，方便安裝與使用
（7） 內建 unbound DNS，未來可搭配 DNS 黑名單協助阻擋 Botnet
（8） 提供 Google 與 Bing 安全搜尋，避免學生搜尋到不必要的網站
（9） 可提供 IP 與介面為主的流量與連線數控管機制
（10） 套件提供詳細的流量，並可自訂項目傳送系統資訊報表
（11） 支援 IPv6、802.1Q VLAN 與 Captive Portal 網頁認證等功能

1.4 套件列表

PfSense 可安裝套件很多，為搭配行動學習學校的需求以及安裝套件的穩定性，建議可選擇以下套件，如表 1-1

表 1-1 行動學習學校安裝的套件

名稱	版本	說明
Cron	0.1.8	排程，例如可設定 ntopng 清理舊的記錄
Lightsquid	1.8.2	快取伺服器達成流量統計圖表化
ntopng	1.2.1	網路流量監控顯示
OpenVPN Client Export Utility	1.2.16	將 OpenVPN 自動產生安裝執行檔
pfBlockerNG	1.06	結合防火牆與黑名單阻擋
Squid	2.7.9	快取伺服器，提昇瀏覽速度
SquidGuard	1.4_7	URL 網址過濾
mailreport	2.3	可搭配 Gmail 寄送報表

這些套件也都持續在發展中，因此也有套件也有較新的測試版本，但穩定性考量，建議使用較為穩定的版本以避免在使用上遇到無法解決的問題。例如 Squid 建議用版本 2 而不是版本 3。

1.5 pfSense 官方網站

pfSense 官方網站（http://www.pfSense.org）於 2015 年改版，如圖 1-1，網站包含系統簡介、下載點、英文文件、產品、論壇以及會員支援服務等介紹。

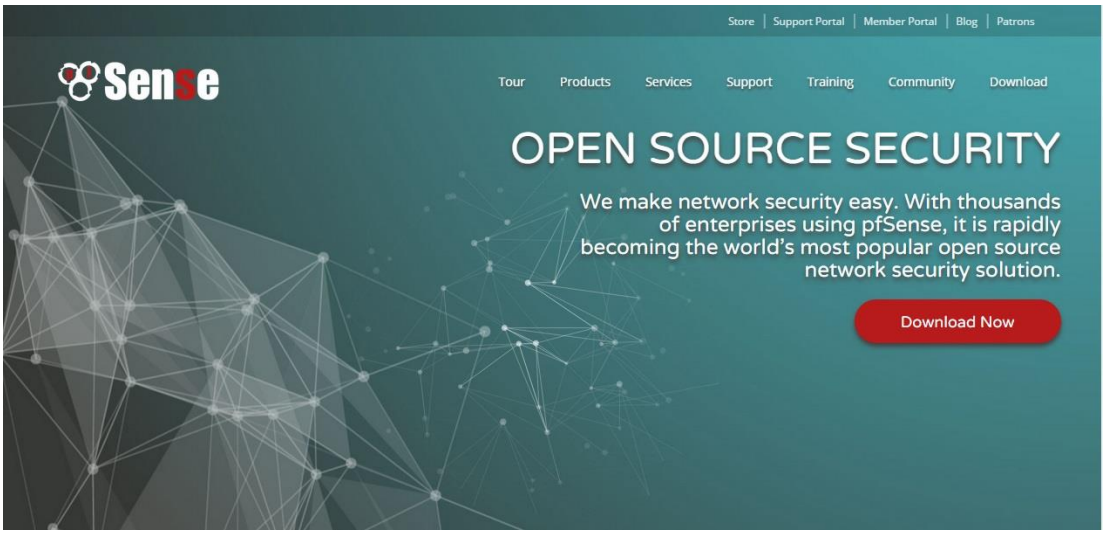

圖 1-1 pfSense 官方網站

第二章 工業級機架型主機

pfSense 主要安裝在 x86 的系統上，所以也就可以安裝在一般個人電腦上，但由於學校的環境需要高度的穩定性，加上南投版設定值需搭配主機，因此設備的選擇上並不建議使用一般電腦來安裝。

2.1 硬體的選擇

使用工業級機架型主機可以在硬體的支援度、穩定性、省電獲得不錯的方案，因此南投縣行動學習學校大部分都採工業級機架型主機來安裝 pfSense。流程大致為：安裝 pfSense、WAN 接上學術網路、匯入設定檔、更新黑名單、依據學校環境稍做設定後即可開始使用。

2014 年 pfSense 2.2 尚未釋出，為確保 pfSense 與硬體的相容性，因此此次行動學習學校採用的工業級機架型主機非主流的規格。而此次採用的機器為 A 公司的 NA-710，規格如表 2-1。

表 2-1 A 公司 NA-710

品項	說明
CPU	Intel Core 2 Quad CPU Q9400 2.66GHz
Chipset	Intel G41 + ICH7R
Memory	2 x DDR3-800/1066 DIMM max. up to 4 GB
HDD	2 x 2.5" SATA SSD
Network	Intel 82583V, 6 x 1000Mbps
Expansion Slot	PCIe x 8 slot
Dimensions	44 mm (1.73") (H) x 430 mm (16.92") (W) x 394.4 mm (15.52") (D)

由於硬體規格會影響 pfSense 使用效能，因此除了硬體的相容性外，以下針對有影響的部份做說明。

網路卡：使用廉價的網路卡會使得系統的 CPU 忙碌，無法處理更多的封包數。因此我們推薦使用 Intel 的 Gigabit 網路晶片來獲得最好的表現。

中央處理器：使用 2.0GHz 以上的處理器可以提昇吞吐量，尤其系統需要到達 500Mbps 以上，這邊講的吞吐量為跨網段並開啟防火牆與 NAT 的情況下。另外若有支援 AES-NI 指令集的 CPU 可以提昇 VPN 傳輸的速度。

晶片組：中央處理器、記憶體、網路卡之間的溝通速度會影響 pfSense 整體的成效。因此，較新晶片組整體效能也會比較好。

記憶體：除了 pfSense 本身運作的系統與套件需要消耗記憶體外，pfSense 預設會使用安裝記憶體中的 1/10 來做為連線數使用，也可手動調整。使用 pfSense 時，一個連線數需要 1KB，因此 2GB 的記憶體可以提供 2,000,000 的連線數。另外較多的記憶體也可當做 Squid 快取使用，效果比硬碟好。

硬碟：除了系統外，還須考慮硬碟本身的 I/O，因為還須提供快取伺服器與 URL 過濾使用。而流量統計檔案可能會占較多容量，inode 數也會增加，建議至少 64GB 以上。如果使用兩顆 SSD，也可將快取伺服器用的檔案放至於另一顆 SSD 硬碟。SSD 除了本身讀取與寫入速度外，開啟 TRIM 可以提昇 SSD 的壽命與效能，其中 Intel SSD 本身的效能與穩定相容性較佳。

pfSense 於 2015 年 1 月釋出 2.2 版，基於 FreeBSD 10 對於效能與硬體支援度較高，加上系統 PF 支援多執行緒，因此現在工業級機架型主機建議使用多核心 SoC 架構，如圖 2-1。

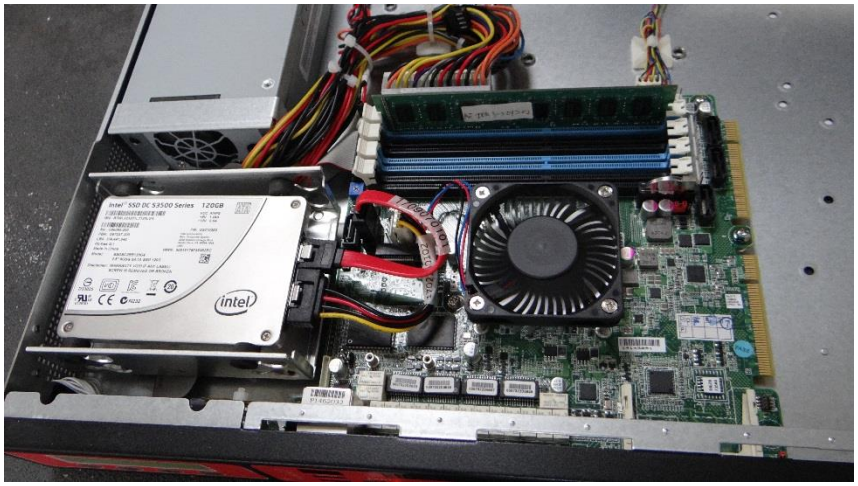

圖 2-1 SoC 架構機架型主機

SoC 的全名為 System On a Chip，中文稱為「系統單晶片」，透過 CPU 能處理大部分的運算與 I/O，達到精簡、省電、微型化，但由於 A 公司四核心 SoC 架構的機器有最小訂單需求，因此這邊 SoC 架構範例採用 B 公司的主機。其中 Soc 最具代表性為 Intel C2000 系列代號為 Rangeley 的晶片，分別為 C2358、C2558、C2758 最推薦給 pfSense 使用，小型學校可以選擇 C2358，而中大型學校可以選擇 C2558 或 C2758。工業級機架型主機除了有 Soc 架構以外，也提供彈性的擴充槽，方便主機擴充網路或光纖，如圖 2-2。

圖 2-2 前置網路擴充卡

第三章 校園環境分析

大部分的學校會面臨到一個問題，學校架構是否適合行動學習，然而影響學校網路運作的情況有很多，但一個好的架構可以讓管理者在發生問題時，方便快速的判斷問題發生點。

3.1 學校網路架構

學校既有的網路架構往往是經過多年的時間慢慢建置完成，也因此這過程有可能會經過不同的管理者，管理者對於架構上的觀念是否正確也影響校內網路環境的品質。

南投縣行動學習學校網路架構上的建議：

（1）校內交換器階層數需適量，接法勿取巧

（2）網路線接近或超過 100 公尺時需使用光纖

（3）網路線使用 Cat.5e 以上，建議可直接使用 Cat.6

（4）網路佈線來源目標需編號清楚

（5）教室需預留多個資訊插座，並使用市售的網路線連接，如圖 3-1

（6）使用資訊插座與跳線面板搭配，減少線路異常，如圖 3-2

（7）網路線於戶外需使用適當管路包覆

（8）網段需適當切割，避免同一網段節點數過多

（9）無線網路規劃要點與有線不同，需費心思量

（10）學校由防火牆或交換器來切割不同網段，而非 IP 分享器

對於學校來說，網路架構往往是容易被忽略的一個部分，因為他不像設備一樣那麼顯而易見，並且一旦佈線完成，就會可能使用好幾年甚至更久的時間。因此，對於未來有網路佈線計畫的學校需費心規劃。

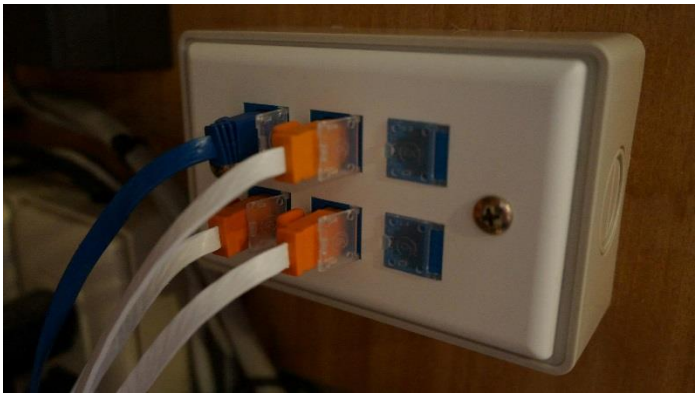

圖 3-1 資訊插座

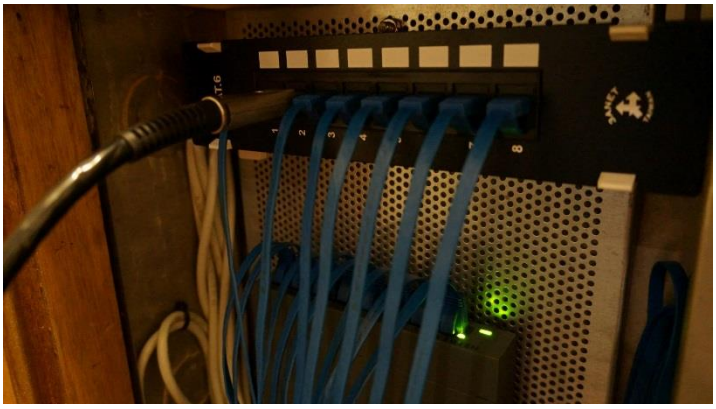

圖 3-2 跳線面板與交換器

3.2 防火牆使用限制

儘管 pfSense 功能與效能足夠大部分學校使用，但由於某些的限制，在行動學習學校導入時會遇到以下的問題：

（1）操作介面為英文，尚未提供中文語系

（2）缺少有系統的中文教學文件或影片，較難上手

（3）第七層的管理阻擋機制較為不足，需用其他方式協助處理

（4）系統與套件由時會有小 Bug，更新速度較慢

（5）若發生問題時，較難以尋找「協助人員」

（6）各縣市網路環境不同，設定值匯入前需修改

一般來說，學校管理人員需要 1-2 天的時間才能對 pfSense 系統有一定程度的了解，當學校人員不熟悉或無其他協助者的幫忙時，導入 pfSense 可能會無法到達預期的成效。除此之外，當網路架構已建置完成，學校如果有攻擊事件或是其他問題時，也會影響到正常的網路運作，例如：學校內部伺服器 DOS 攻擊、非法 DHCP 設備或是網路剪刀手等，這些防火牆只能協助發現問題，必要時還需要網管型交換器，因此找出並解決問題的來源才是正確方法。

3.3 結論與建議

對於行動學習學校來說，網路的穩定度會影響教學的進行，但有一半的網路問題並不是出在設備上，而是學校網路架構以及無線網路設定的適用性，因此防火牆也只是網路穩定順暢其中一個部分，加上學校的行政政策與良好的使用者習慣，才能把問題降至最低。

pfSense 為開放原始碼的防火牆方案，相對於一般商業防火牆，不需付出高昂的使用與維護費用，也不需每年購買 License，可用最少的預算到達接近 1Gbps 的吞吐量。因此對各縣市來說，問題在維護人員與操作文件，若能針對 pfSense 這部份做加強，對大部分的學校為最佳 CP 值的選擇。