中小型企業防火牆備援機制系統-以 mono 嵌入式系統為例

張逸為　林豐智　王昌斌

南榮技術學院資訊中心　逢甲大學　南華大學

技佐暨南華大學資管所　電子商務研究中心主任　電子商務管理學系主任

security@mail.njtc.edu.tw　fjlin@fcu.edu.tw　cbwang@mail.nhu.edu.tw

摘要

近年來資訊化與網路運用日益普及，大部份企業營運採用透過網路運作之方式，將資訊放置在網路上，便利相關系統、人員存取，以增加作業流程效率。面對資訊安全事件不斷產生的網路環境，如何保護這些資訊，就顯得格外重要，所以企業網路架構建置防火牆，管控網路進出，保護企業網路資訊安全成為一重要課題，但防火牆可能面對故障的問題。本研究報告中提出了一個快速建立備援防火牆的機制，讓企業面臨防火牆故障時，可有一個快速、便利、且便宜的替代方案，而避免企業網路中斷造成經濟損失、或無防火牆的防護下冒險上網。

關鍵字：嵌入式系統、防火牆

1. 前言

近年來網路的運用已經十分普及，受到各界的青睞；相對經由網路所發生資訊安全事件卻也大幅度的成長，在 CERT/CC(2006)的報告中指出全球資訊安全事件，在 2001 年為 52,658 件，2002 年 82,094 件，2003 年更提高到 137,529 件[6]，這種情況下造成企業界極大的損失，圖 1-1 是由 CERT/CC 網站的統計數據所彙製之資訊安全事件成長趨勢圖。在美國 CSI/FBI (2006)電腦犯罪與安全調查中，電腦資料被非法存取的損失單一事件平均為 85,621 美元，資訊安全所造成的總損失為 52,494,290 美元[7]；由此可見建立網路安全的管理機制，已是當下的網路安全防護最基本的執行工作。

在資訊安全的提倡下，企業紛紛加強網路管理、資料安全防護的工作，讓企業可在享受網路帶來便利之餘，同時可以達到資訊安全防護的目的。然而，企業、學術、機關單位網路裡最常見的防護機制是採用防火牆來防護網路安全，而在防火牆的選擇中，以硬體式防火牆的高效能[1]、穩定性受到較多資訊人員的喜愛；在資訊安全機制備援機制中，常必須同時購買兩套硬體式防火牆，但硬體式防火牆屬於高單價資訊安全產品，對中小企業而言相對地提高了成本，故要以硬體式防火牆建立資訊安全備援機制，在實際建置上有相當的困難度；此外，如果採用軟體式防火牆來當備援機制，又必須仰賴對防火牆軟體，具有深入了解的技術人員輔助。因此，尋找一個經濟且能達到企業所需求的資訊安全備援機制，對中小型企業是一個非常重要課題。

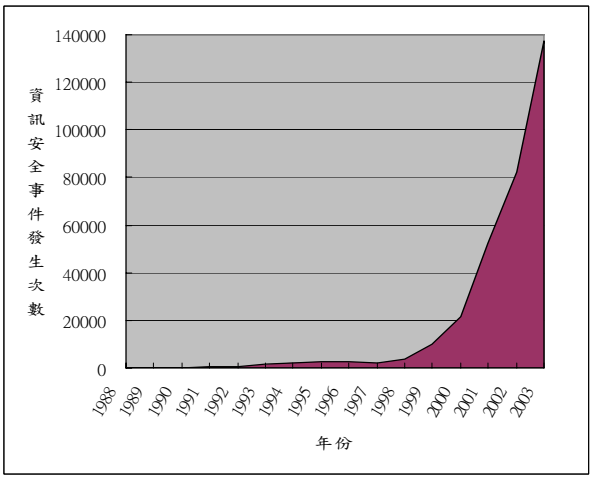

圖 1.1 資訊安全事件成長趨勢圖
(CERT/CC 網站的統計數據所彙製)

本論文中採用嵌入式防火牆系統當資訊安全備援機制，在實際環境測試中具有良好之表現，無須有繁雜的作業，克服了採用軟體式防火牆的困擾，同時也兼具硬體式防火牆高效能的表現，大幅降低了成本，提供讓無法承受高價格硬體式防火牆的企業，一個極佳的選擇。

2. 文獻探討

李英瑞(2004)認為「嵌入式系統」是一種是以應用為中心，軟、硬體乃可視需求而被改變的，適合應用系統在功能、可靠性、成本、體積及功耗等綜合性嚴格要求的專用電腦系統[3]。王金龍(2006)也提到，嵌入式系統與傳統型電腦設備之差異，為配合特定應用的特殊設計、高效率、產品壽命長、穩定的系統、不易被竊取和高安全性、容易操作等優點[2]。故嵌入式系統可以說是一個客製化的高效率系統，且具高彈性可針對需求變化而有所調整。

周樹林(2004)調查報告[4]中顯示，綜觀 2002 至 2004 年間，自嵌入式系統應用產值遠超過伺服器應用產值，在嵌入式系統的年複合平均成長率高達 123%，成長幅度明顯超越伺服器，顯示出嵌入式系統在未來的發展性是個非常具有潛力的系統。

李俊德(2005)探討嵌入式系統開發產品關鍵因素研究[5]中說明，嵌入式系統一般是燒錄在非揮發性記憶體中，避免系統被更改或遭破壞，但隨著時代改變，小型記憶卡的發達，目前有些嵌入式系統是安裝於 Flash Card 中，具有可隨時更新軟體的優點，又可以克服傳統硬碟裝置容易故障的問題。

Manuel Kasper (2006) 提到 mono 為一種自由軟體的嵌入式防火牆系統[8]，軟體總容量大小不超過 6MB，並提供了 net45、net48、wrap、一般電腦等多種平台；該系統可安裝於 Flash Card 中搭配桌上型電腦使用，讓電腦立即可提供防火牆的功能，且具效能及穩定性。

3. 系統架構與實測

3.1 嵌入式防火牆軟體的選擇

目前嵌入式防火牆的種類有許多類型，一般是以 Linux 為核心的版本居多；在 Nathan Boeger(2001)提出的報告[9]與 FreeBSD 網站(2005)的評比資料[10]顯示，皆以 FreeBSD 作業系統的總表現優於 Linux，故在本文中是採用以 FreeBSD 為核心的 mono 嵌入式防火牆，希望可以在使用等級有限的硬體時，仍有良好的表現效能。

Mono 為 Manuel Kasper 所研發的嵌入式防火牆軟體，該軟體核心為 FreeBSD，屬於自由軟體。作者在網路中發現許多 Linux 開發的 Web 界面防火牆，但功能均不符合需求，因此開發了 mono，建立一個完整的、新的嵌入式防火牆軟體。

3.2 mono 防火牆功能

在 mono 系統 1.22 的版本中，提供了一般商用防火牆常用的功能，其中包括了 WEB 管理界面、無線網路功能、封包過濾、網頁認證、802.1Q VLAN、NAT、IPsec VPN、PPTP VPN、靜態路由、DHCP 伺服器與中繼、DNS 轉發、動態 DNS 客戶端、SNMP 代理、流量限制、網路介面卡的流量圖、WEB 界面進行韌體升級、設定檔備份/還原、中央處理器負載狀況以及記憶體負載狀況等功能，上述功能足以滿足大部分企業之需求。

3.3 狀況假設

假設環境為中小型企業網路架構中，管理資訊安全的硬體式閘道型防火牆故障，當下企業網路中段，B2B 資訊系統停擺，企業網站對外服務中斷，造成電子訂單無法下單，與上游廠商的物料管理系統停擺，企業損失即將亮起紅燈；硬體式防火牆經評估後無法立即修復，且已超過產品保固期限的情況下，此時採用 mono 嵌入式防火牆系統為備援機制，不僅能讓企業網路恢復連線，並且受到防火牆的保護，使企業損失降低，同時獲得緩衝時間得以評估，購置新的硬體式防火牆。

3.4 測試環境

在網路架構裡，將原本硬體式防火牆的設備

(如圖 3.1 所示)以 mono 嵌入式防火牆系統(如圖 3.2 所示)取代，並採用 Network Address Translation(NAT)模式，並在防火牆規則中，限制對外連線開放 FTP、TELNET、SMTP、DNS、HTTP、POP3、HTTPS 等服務外，其餘則限制對外連線，以模擬現實環境中，企業限制內部網路對外連線狀況，開放的通訊埠為 TCP 20、21、23、25、80、110、443、UDP 53。測試之硬體規格分別以 A、B、C、D (如表 3.1、3.2、3.3、及 3.4 所示)四個等級，測試 mono 嵌入式防火牆的負載。

表 3.1 嵌入式防火牆電腦(等級 A)

	等　級	備註
中央處理器	200 MHz	Pentium
記憶體	32 MB	EDO RAM
硬碟	8MB	Flash Card
網路卡	1000 Mbps	兩張網路卡

表 3.2 嵌入式防火牆電腦(等級 B)

	等　級	備註
中央處理器	733 MHz	Pentium III
記憶體	64 MB	SD RAM
硬碟	8MB	Flash Card
網路卡	1000 Mbps	兩張網路卡

表 3.3 嵌入式防火牆電腦(等級 C)

	等　級	備註
中央處理器	1.6 GHz	Pentium 4
記憶體	256 MB	SD RAM
硬碟	8MB	Flash Card
網路卡	1000 Mbps	兩張網路卡

表 3.4 嵌入式防火牆電腦(等級 D)

	等　級	備註
中央處理器	3.0 GHz	Pentium 4
記憶體	512 MB	DDR2 RAM
硬碟	8MB	Flash Card
網路卡	1000 Mbps	兩張網路卡

表 3.5 使用者電腦等級

	等　級	備註
中央處理器	2.8 GHz	Pentium 4
記憶體	256 MB	DDR RAM
硬碟	80 GB	3.5 吋硬碟
網路卡	100 Mbps	內建式

外部網路以一台檔案伺服器提供檔案下載，企業內部使用者端以 50 台電腦模擬，規格如表 3.5 所示，並同時針對外部網路伺服器所提供的檔案進行下載，測試在各個嵌入式防火牆硬體所能可承受的網路最大下載頻寬。

網路架構中，外部網路連接到嵌入式防火牆線路(圖 3.2 中線路 A)頻寬為 1000 Mbps，嵌入式防火牆與內部網路設備，交換器連接線路(圖 3.2 中線路 B、C) 頻寬為 1000 Mbps，交換器與使用者端的網路連線頻寬均為 100 Mbps。

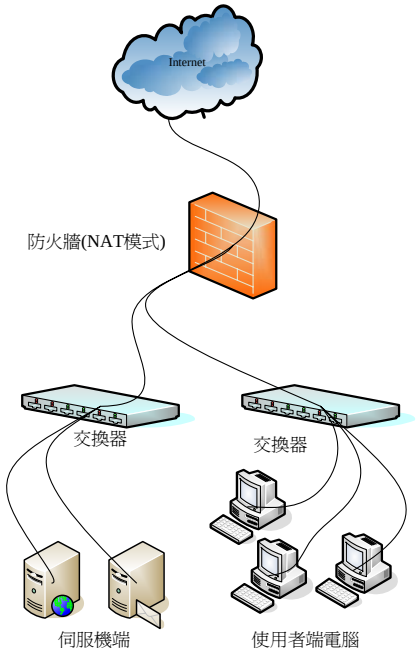

圖 3.1 使用硬體式防火牆企業網路架構

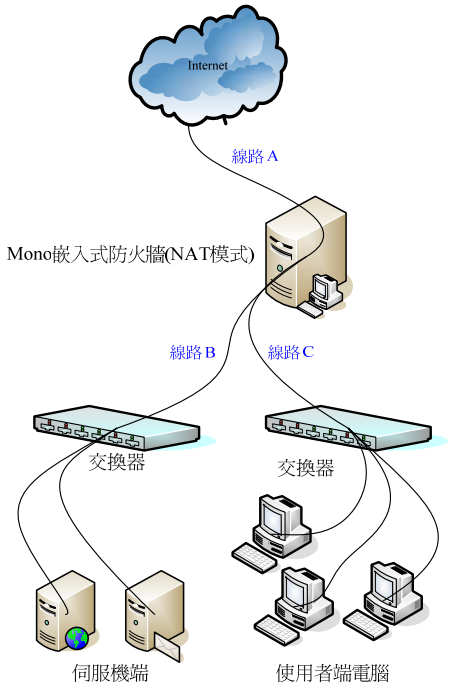

圖 3.2 使用 mono 嵌入式防火牆備援網路架構

3.5 測試結果

mono 嵌入式系統在各 CPU 等級的，可承受最大下載頻寬、CPU 負荷數值如表 3.6 所示；CPU 數值當負荷增加時，均會以上下 5%跳動，故以平均數值顯示。

表 3.6 mono 嵌入式系統在各等級環境之效能參數

CPU 類型	等級	最高下載頻寬	CPU 負荷
Pentium	200 MHz	26 Mbps	90%
Pentium III	733 MHz	220 Mbps	85%
Pentium III	1.6 GHz	380 Mbps	88%
Pentium 4	3.0 GHz	420 Mbps	55%

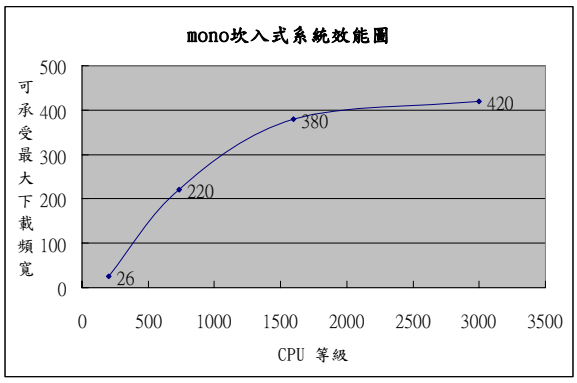

圖 3.3 mono 嵌入式效能圖 (可承受最大頻寬)

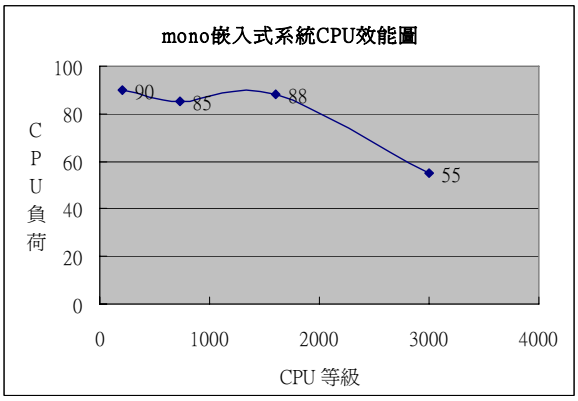

圖 3.4 mono 嵌入式效能圖 (CPU 負荷)

表 3.6 中的數據顯示，mono 嵌入式防火牆系統在硬體需求，除了網路卡速度需配合實際網路頻寬外，著重於 CPU 的效能表現，當 CPU 時脈越高時，所承受的頻寬越高，而對記憶體並沒有特別的需求，在 CPU 負載由低升高，承受頻寬由小變大時，記憶體的負荷並沒有增加；在 CPU 方面與所承受的頻寬大小則有正比的關係，當下載流量增加時，CPU 的負荷則會馬上爬升，但當下載量下降時，CPU 的負荷也會隨即減少，該狀況證實 mono 系統著重於 CPU 的效能，且該系統並不會有佔住 CPU 的現象。

CPU 負荷方面，當負荷超過 80%以上時，進行變更系統設定值，在套用設定值時，會讓負荷瞬間上升至 100%，造成 Web 控制介面網頁停頓，但該段時間仍可保持網路暢通，並不會有斷線狀況，套用設定值所停頓的時間，會隨著 CPU 原本的負荷增加而延長停頓時間，在測試過程中當 CPU 負載高達

90%時，進行變更設定值，所停頓時間為 7 秒鐘。

在本文數據中使用 Pentium 4 3.0GHz 的硬體環境時，CPU 最高負載為不超過 60%，而最高下載頻寬為 420Mbps，變更設定值並不會有任何停頓狀況，顯示該狀況下 CPU 負載並不高，但頻寬能無法上升，推判是該測試架構中，檔案伺服器無法提供更大的下載量，所以造成下載頻寬無法上升，CPU 負荷偏低的狀況。

在系統轉移的便利性方面，該次測試中效果良好，當硬體平台變換時，如保持網路卡型號一致，並無需設別更改設定值，開機後即可運作，且防火牆規則執行正常；但如有變更網路卡型號時，仍只需執行定義外部網路卡與內部網路卡的部份，變更後能可運作，同樣無需變更防火牆設定值，故在硬體平台的轉移性十分的良好。

3.6 實際案例

除了上述測試數據外，關於 mono 嵌入式防火牆系統之實際表現有兩個實際案例。第一是南台灣的開喜烏龍茶廠區。該廠區於 2005 年 12 月發生硬體式防火牆故障狀況，內部電腦數為 33 台，對外連線的網路頻寬為 8M 兩線，一線為通往 Internet 的對外網路，另一線為通往台北伺服端的 VPN 連線網路，硬體式防火牆經資訊人員劉建辰判斷後無法立即修復，故採用 mono 嵌入式防火牆軟體代替原本的硬體式防火牆，將 mono1.2 generic-pc 版本，安裝於 8MB 的 Flash Card 中，裝設於 CPU 等級 Pentium III 500、網路卡為 100 Mbps 的 Realtek RTL8139 晶片，從安裝到防火牆規則設定，約花費 20 分鐘；企業網路在 25 分後恢復連線，避免了企業的損失，該防火牆系統運作超過 8 個月，並無發生系統當機或異常的狀況，並經過一次線上更新版本，更新過程並無異狀；對於 mono 嵌入式防火牆系統穩定與效率的表現，得到該廠區的資訊人員劉建辰的認同。

第二個案例是台南縣南榮技術學院電腦教室。由於校內真實 IP 不足，且為避免學生私自在電腦教室架設地下站台，因此電腦教室全面使用虛擬 IP，連接外部網路時，使用 IP 分享器進行 Network Address Translation 來轉換真實 IP；此外因學校對外頻寬由原本 1.5Mbps 的 T1 專線升級為 200Mbps 的光纖網路，電腦教室的下載頻寬也相對的提高，每台電腦下載的平均速度由原本的 50Kbps 不到的速度上升到 5Mbps，因此發現原本使用的 IP 分享器無法負荷這樣的下載頻寬，造成時常當機的狀況；因此採用 mono 嵌入式防火牆系統來擔任 Network Address Translation 的角色，硬體則使用 CPU 為 PentiumII 266 MHz、記憶體為 64MB，兩張 100Mbps 的網路卡，上線後對於承受下載頻寬的效能表現良好，該系統運作至今已超過 6 個月並無當機或其他異狀。

4. 結論

如何使網路更加安全是企業一直努力的目標，而使網路達到安全同時，如何兼顧經濟和效能，則是企業界更希望獲得的答案，至今網路發展的迅速，讓網路的運用更多元化，相對也造成更多的危機，在這樣危險的網路環境中，替我們把關的重要角色往往是防火牆，因此如果沒有一個完善的備援機制，所造成的潛在危機是值得企業擔心的問題。

本論文中旨在藉由嵌入式防火牆系統，作為企業網路的安全機制備援，希望透過這樣的架構，可以提供給企業在面臨網路安全威脅時，有一個經濟、安全、穩定且便利的選擇。

本實驗結果顯示 mono 嵌入式防火牆系統，在效能、平台轉移性和設定簡易性、均有良好的表現，證實具有替代傳統硬體式防火牆的能力；但隨著網路攻擊手法變化，以單純的防火牆條件管制來維護資訊安全，已不足應對多樣化的網路攻擊，所

以希望日後在 FreeBSD 核心類型的嵌入式防火牆系統，除具備有傳統的防火牆管制方式外，還兼具入侵偵測系統（Intrusion Detection System；IDS）等功能，讓企業用戶在未來選擇資訊安全防護時，甚至可以直接選用嵌入式系統，作為企業專用防火牆的首選。

參考文獻

[1] 余少棠、黃俊穎、蔡昌憲、張智晴、林盈達，2002，網路安全閘道器產品評比：功能與效能面，網路通訊雜誌，130期。

[2] 王金龍，2006，嵌入式系統硬體架構與設計，碁峰資訊股份有限公司。

[3] 李英瑞，2004，嵌入式系統與網際網路之整合與應用，國立中山大學機械與機電工程研究所碩士論文。

[4] 周樹林，2004，2003-2004我國自由軟體之硬體應用趨勢分析，軟體產業通訊-第56期軟體產業通訊。

[5] 李俊德，2005，應用Embedded Linux系統開發產品關鍵因素之研究—以台灣工業電腦產業例，世新大學管理學院資訊管理學系究所碩士論文。

[6] CERT/CC, http://www.cert.org/stats/cert_stats.html, 2006.

[7] Computer Security Institute, http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2006.pdf, 2006.

[8] Manuel Kasper, http://www.m0n0.com.tw/wall/index.php , 2006.

[9] Nathan Boeger,Is FreeBSD a Superior Server Platform to Linux, http://www.webtechniques.com/archives/2001/01/infrrevu/, 2001.

[10] FreeBSD,FreeBSD vs. Linux vs. Windows 2000, http://www.freebsd.org/marketing/os-comparison.html, 2005.