網路安全閘道器產品評比 – 功能與效能面

余少棠、黃俊穎、蔡昌憲、張智晴、林盈達

國立交通大學資訊科學所

新竹市大學路 1001 號

摘要

網路安全問題逐漸受到重視，安全閘道器也變成企業不可或缺的設備。開放原始碼的資源豐富，我們也將相關的開放原始碼整合在一起，主要包括防火牆、虛擬私有網路、路由器、侵入偵測系統。本文將把開放原始碼解決方案與六個商業產品做功能與效能上的比較。這六家廠商分別是 BorderWare、CheckPoint、Cisco、NetScreen、SonicWall、WatchGuard，其中 BorderWare 與 CheckPoint 是提供純軟體的套件，其他則是硬體。比較的方式是利用 Nessus、Nmap、WebStone 軟體工具及 SmartBits 測試儀對產品做一系列的測試與比較，並用一些長條圖與表格顯示產品在功能與效能上的差異，報告的結論以 1~5 顆星替各產品打分數。

就 6 項商業產品而言，我們主觀地覺得功能完整性及管理簡易度上 NetScreen 與 SonicWall 最優；在 Packet Level 防火牆及 VPN 效能上 NetScreen 最優；在 VPN 互通性上 Cisco 與 NetScreen 最優；在 Content Level 防火牆上 NetScreen 與 WatchGuard 最優。就開放原始碼解決方案而言，除了效能與管理簡易度外，均可列入最優等級，效能可再由硬體(加速卡或 ASIC)加速，管理簡易度則可以撰寫 web-based 管理介面達到。

關鍵字：安全閘道，防火牆，虛擬私有網路，侵入偵測，評比

一、簡介

網際網路(Internet)發展快速，網路上的組成份子也愈來愈多且複雜。管理者爲了阻擋 Internet 上成員存取企業內部的資源以及控制封包的進出而有防火牆(Firewall)的需求；然而企業的子公司間在利用 Internet 傳送機密文件時，封包將可以被 ISP 或網路上的有心人士所監聽，因此具有封包加密與認證機制的虛擬私有網路(VPN)可以解決使用者的需求;2000 年年初,Yahoo、Amazon、CNN、eBay 被分散式阻斷服務(Distributed Denial of Service：DDoS)的手法攻擊[1]，然而這可以用侵入偵測系統(Intrusion Detection System：IDS)作某種程度上的避免。近來人們開始意識到網路是個不安全的國度，所以對網路的安全性極度重視。在此，我們將檢視各家廠商的網路安全閘道器(Security Gateway)，比較各家產品的功能(Functionality)、管理介面(Management)、互通性(Interoperability)、安全性(Security)及效能(Performance)，以提供網管人員選購 Security Gateway 時的參考準則。另外，開放原始碼(Open Source)的資源豐富，所以我們也將相關的開放原始碼整合在 Linux 路由器上(也解決了 NAT 與 VPN 在 kernel 衝突的問題)，用以比較商業產品與開放原始碼解決方案的優劣。圖一則是我們的測試環境。

圖一：我們的測試環境

一般來說，Security Gateway 的功能主要可分成幾類：防火牆(擷取安全機制、內容安全機制)、VPN(通訊安全機制)、侵入偵測(安全管理機制)與使用者認證機制(User Authentication Mechanism) (安全管理機制)。

其中防火牆根據 TCP/IP 通訊協定堆疊(Protocol Stack)，我們將其分爲 Packet Level[2]、URL Level[3]與 Content Level[4]三類。Packet Level 防火牆主要是根據封包標頭(header)的來源端 IP 位址(Source IP Address)、目的端 IP 位址(Destination IP Address)、來源埠(Source Port)、目的埠(Destination Port)與協定種類(Protocol Type)來決定封包是否可以通過防火牆。URL Level 防火牆主要是判斷企業內部主機可否連往特定的網址觀看網頁，例如不准員工在上班時間上股票網站。Content Level 防火牆則會檢查封包的 payload 部分是否有病毒(virus)或 Java/JavaScript/ActiveX 物件是否可以通過防火牆。

VPN 則是利用一些加密與認證演算法，使得資料可以安全的由傳送端送往目的端且目的端也可以確認資料的來源是否正確。加密演算法包括 DES、3-DES 等，認證演算法包括 MD-5、SHA-1 等，而金鑰交換方式包括 Manual Keying 與 Automatic Keying，在 Automatic Keying 中的金鑰認證方式又包括 Pre-share Key 與 RSA Signature。

使用者認證機制主要是用在兩方面：(1) 使用者透過撥接(dial-up)連上 Security Gateway 時，必須先得到 Security Gateway 的身份認證，而認證技術包括用 PAP、CHAP、RADIUS 等通訊協定。(2) Internet 上成員想要透過 Security Gateway 連往企業內部主機前，必須先得到 Security Gateway 的身份認證，而認證的方式是讓 Security Gateway 將使用者的連線需求攔截下來，待使用者輸入完帳號密碼後，才可連進企業內部。

綜觀 Security Gateway 產品可以發現，很少有廠商把 Firewall、VPN 與 Router 整合在一起(例如 Cisco PIX 及我們整合的系統)，大部分都是 Firewall 與 VPN 整合(本次測試的所有產品)或 Firewall 與 Router 整合。把這三項都整合在一起的話，好處是可以節省企業成本以及網路管理較方便容易。相對地，整合型方案將會減少 Router 與 Security Gateway 之間的網段，可能降低了遭受攻擊時的安全性。

二、測試對象

在篩選產品的過程中，我們首先查詢各家廠商的網頁，找尋哪些產品具有 Firewall 與 VPN 兩項功能(必要條件)。接著就由網路通訊雜誌社出面對各廠商發出邀請，說明希望能借產品給我們測試並附上我們的測試計畫書，如果是國外廠商則轉向國內的代理商借產品。有些公司網頁的產品規格描述不夠清楚，以致於我們無法清楚判斷其完整規格，例如 VPN 是採用何種技術。我們邀請了國內的台華科技(GenNet)[5]、新網趨勢(ipTrend)[6]、合勤科技(ZyXEL)[7]與國外的 Cisco[8]、NetScreen[9]、CheckPoint[10]、SonicWall[11]、WatchGuard[12]、Intel[13]、Nortel[14]、CyberGuard[15]等廠商。後來，組合國際[16]、舜遠科技[17]、BorderWare[18]與 TopLayer[19]也有意參與產品測試計畫。最後有將產品送來的共計 10 家，但因爲我們是要測具備 IPSec 標準的產品(因爲 IPSec 是通訊安全所需加密與認證的 total solution)，所以將對剩下的 6 家商業產品作比較。其中 SonicWall 因廠商要求產品歸還日期較早，所以有些項目沒有測試到。表一是邀請的廠商與結果。邀請於 10 月中送出，產品於 12 月初收集完成，測試工作於 1 月初完成。

產品製造商	產品名稱	國內代理商	邀請結果
Cisco	PIX 525R	聚碩科技	送達
NetScreen	NetScreen-100	友冠資訊	送達
CheckPoint	VPN-1 Appliance 650	通路美	改送 VPN/Firewall -1Software
SonicWall	SonicWall PRO VX	富揚資訊	送達
BorderWare	Firewall Server	飛雅高科技	送達
WatchGuard	Firebox Ⅱ FastVPN	空運來台	改送 FireBox Ⅱ Plus
組合國際	ETrust		送達(非 IPSec)
台華科技	WebGuard		送達(使用 proprietary 方式，非 IPSec)
合勤科技	Prestige 312		送達(使用 PPTP 方式，非 IPSec)
TopLayer	TopLayer	凌群電腦	送達(單純防火牆產品，非 VPN 產品)
Intel	NetStructure 3130 VPN Gateway	網通科技	未送達(無可借用的機器)
CyberGuard	KnightSTAR 2U	岱凱通訊	未送達(無可借用的機器)
Nortel	Contivity Extranet Switch 4500	凌群電腦	未送達(機型太大，沒有庫存)
舜遠科技	N/A		未送達
新網趨勢	eStation		未送達(經過評估，沒有參與測試的意願)

表一：邀請廠商與結果

除了這些商業產品外，我們也將現有的開放原始碼整合在一台 Linux 2.2.16 核心、Penitum !!! 700 CPU、128MB DRAM 的工業級電腦(IPC)上並完成 web-based 的管理介面，以便讓我們比較商業產品與開放原始碼解決方案的差異。整合的原始碼包括：Firewall(ipchains)[2] 、 VPN(FreeS/WAN)[20] 、 Router(Zebra)[21] 、 Proxy(Squid)[3] 、

Application Proxy(TIS)[4] 、 IDS(snortd)[22] 、 RADIUS Client(portslave)[23] 、 PPP Server(pppd)[24]及 Alarm Mechanism(Logsurfer)[25]。至於 BorderWare 與 CheckPoint 的軟體產品也是安裝在與開放原始碼解決方案相同的硬體配備上。而 Cisco、NetScreen、SonicWall 與 WatchGuard 則是以硬體形式銷售，其部分硬體規格可參考表四，因這些產品都是借的且有些有封條，硬體規格多由網站得知。

我們將對產品規格的比較結果分成三類：防火牆規格、VPN 規格與其他規格。表二是各商業產品與開放原始碼解決方案在防火牆規格的比較。表三是 VPN 規格上的比較。表四則是其他規格的比較。可以發現在防火牆規格方面，有一部份產品的 URL Filter 功能，必須在額外的主機上安裝軟體，然後由 Security Gateway 負責把 HTTP request 導入該主機檢查。此外，開放原始碼解決方案比商業產品多了阻擋 JavaScript 的功能。BorderWare 的防火牆則屬於 Application Level Gateway 類型，即所有防火牆處理均由 Application 層的程式處理。在 VPN 方面，只有開放原始碼方案 Cisco 與 NetScreen 有較新穎的 RSA Signature 金鑰認證方式。在其他方面，只有我們整合的開放原始碼方案與 Cisco 有將防火牆、VPN 與路由器整合在一台 Security Gateway 上。

Company/ Product	Packet Filter	DMZ	URL Filter		HTTP Content Filter			Stateful Inspection
			Exactly String Match	Regular Expression	Java	ActiveX	JavaScript	
Linux (Open Source)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	*
BorderWare Firewall Server	Yes	Yes	(need license)	N/A	No	No	No	No
CheckPoint VPN/Firewall-1	Yes	Yes	No	No	No	No	No	Yes
Cisco PIX 525R	Yes	Need card	External	N/A	Yes	Yes	No	Yes
NetScreen-100	Yes	Yes	External	N/A	Yes	Yes	No	Yes
SonicWall PRO VX	Yes	Yes	Yes	Keyword only	Yes	Yes	No	Yes
WatchGuard FireBox Ⅱ Plus	Yes	Yes	No	No	Yes	Yes	No	Yes

* means available but not implemented by us

表二：防火牆規格比較表

Company/ Product	Protocol Support		Encryption Algorithm			Authentication Algorithm		
	AH	ESP	DES	3-DES	Others	MD-5	SHA-1	Others
Linux (Open Source)	Yes	Yes	Yes	Yes	No	Yes	Yes	No
BorderWare Firewall Server	No	Yes	Yes	(need license)	(Blowfish, CAST need license)	Yes	Yes	No
CheckPoint VPN/Firewall-1	Yes	Yes	Yes	(need license)	RC2, CAST, FWZ1	Yes	(need license)	CBC-DES MAC
Cisco PIX 525R	Yes	Yes	Yes	(need license)	No	Yes	Yes	No
NetScreen-100	Yes	Yes	Yes	Yes	No	Yes	Yes	No
SonicWall PRO VX	Yes	Yes	Yes	Yes	ARCFour	Yes	No	No
WatchGuard FireBox Ⅱ Plus	Yes	Yes	Yes	Yes	No	Yes	Yes	No

Company/ Product	Keying Method		Automatic Key Authentication	
	Manual Key	Automatic Key	PSK	RSA Signature
Linux (Open Source)	Yes	Yes	Yes	Yes
BorderWare Firewall Server	Yes	Yes	Yes	No
CheckPoint VPN/Firewall-1	Yes	Yes	Yes	No
Cisco PIX 525R	Yes	Yes	Yes	Yes
NetScreen-100	Yes	Yes	Yes	Available in ScreenOS2.5
SonicWall PRO VX	Yes	Yes	Yes	No
WatchGuard FireBox Ⅱ Plus	Yes	Yes	Yes	No

表三：VPN 規格比較表

Company/ Product	Routing		NAT/PAT	IDS	RADIUS	DHCP	Bandwidth Control	Fail Over
	RIP	OSPF						
Linux (Open Source)	Yes	Yes	Yes	Yes	Yes	*	*	*
BorderWare Firewall Server	No	No	Yes	No	No	No	No	No
CheckPoint VPN/Firewall-1	No	No	Yes	Yes	Yes	Yes	Yes	Yes
Cisco PIX 525R	V2 (passive mode)	No	Yes	Yes	Yes	Yes	No	Yes
NetScreen-100	No	No	Yes	Yes	Yes	No	Yes, per rule	Yes
SonicWall PRO VX	No	No	Yes	Yes	Yes	Yes	No	Yes
WatchGuard FireBox II Plus	No	No	Yes	N/A	Yes	Yes	No	Optio-nal

Company/ Product	Load Balance	Static Log	Attractive Features	ICSA Certificated	Solution	Price
Linux (Open Source)	*	No	*	No	S/W (P!!! 700, 128MB DRAM)	NT$0
BorderWare Firewall Server	No	Yes	Secure Mail, DNS, FTP and WWW	Firewall IPSec	S/W (BDS version, P!!! 700, 128MB DRAM)	NT$550,000 (用戶報價)
CheckPoint VPN/Firewall-1	Yes	Yes	N/A	Firewall	S/W (NT version, P!!! 700, 128MB DRAM)	NT$559,860 (廠商提供)
Cisco PIX 525R	No	Yes	Mail Guard	未來不參加此驗證，改參加 EAL2, EAL4 驗證	H/W, (P!!! 598, 128MB DRAM, 16 MB Flash, 未安裝加速卡)	NT$880,000 (廠商提供)
NetScreen-100	Yes	Yes	DNS cache https web management	Firewall IPSec	H/W, (processor unknown, ASIC)	NT$665,000 (廠商提供)
SonicWall PRO VX	No	Yes	Anti-virus, Web proxy forwarding	Firewall	H/W, (Intel StrongARM 233MHz, Accelerator Card)	NT$325,000 (廠商提供)
WatchGuard FireBox II Plus	N/A	Yes	N/A	N/A	H/W, (K6-III-P 366 256 MB DRAM 8 MB Flash)	NT$363,720 (廠商提供)

* means available but not implemented by us

表四：其他規格比較表

三、測試方法

我們測試的方向分成兩類：功能面(Functionality)與效能面(Performance)。功能面包

括管理的簡易度、功能的完整性、互通性與安全性。效能面包括 Packet Level 防火牆、URL/Content Level 防火牆以及 VPN 的效能。

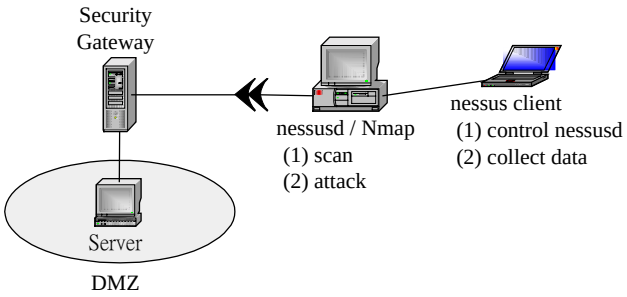
功能面

管理簡易度方面，主要是檢視產品的控制介面是否簡單易用。功能完整性則專注在 Security Gateway 應有的功能上作比較。此兩項的比較方式是以較主觀的方式，由 4 個人分別替各產品打分數後取平均。

產品的互通性，則藉由設定以下 4 種情況，看看各產品間是否可以建立起 VPN tunnel。

[1] Manual Keying：DES 加密法，MD-5 認證法。
[2] Manual Keying：3-DES 加密法，MD-5 認證法。
[3] Automatic Keying：DES 加密法，MD-5 認證法，Pre-share Key 金鑰認證機制。
[4] Automatic Keying：3-DES 加密法，MD-5 認證法，Pre-share Key 金鑰認證機制。

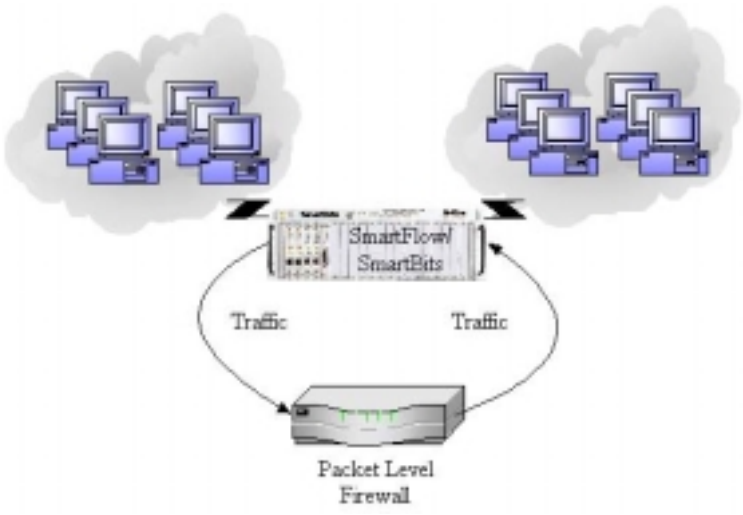
安全性測試是要用 Nmap[26]套件掃瞄產品所提供的服務，然後用 Nessus[27]套件攻擊各服務可能的漏洞。測試環境如圖二所示，首先我們會攻擊產品本身，檢視產品是否有安全漏洞，並觀察產品能否將攻擊封包記錄(log)下來。接著攻擊 DMZ 內的一台主機，檢視產品能否將攻擊 DMZ 主機的封包記錄下來，甚至將攻擊 DMZ 主機的封包丟棄。



圖二：安全性測試環境

效能面

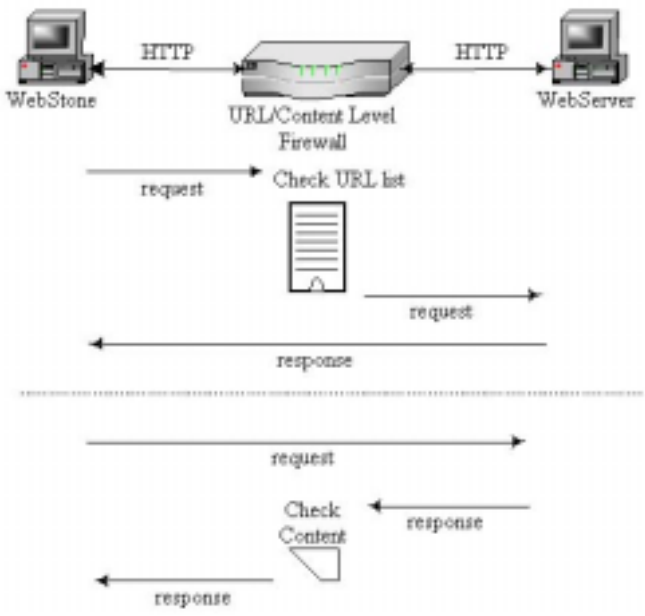
Packet Filter 防火牆效能測試是透過 SmartBits[28]的兩片 SmartCard 卡，分別模擬企業內部 200 台主機與 Internet 上的 200 台主機，測試環境如圖三所示，由模擬企業內部主機的卡分別傳送兩種不同大小的封包(128 byte 與 1518 byte)到模擬 Internet 上主機的卡，SmartFlow 測試軟體會以 binary search 方式尋找測出待測物之無封包遺失最大輸出(no-loss max throughput)。這時 Security Gateway 的設定分別有：(1) 將 NAT 開啓及關閉；(2) 在 NAT 開啓的情況下，分別加 10 與 100 條"不會"阻擋封包由內部網路轉送到外部網路的防火牆規則。我們的目的是要檢視 NAT 對系統效能的影響以及拿封包對多條防火牆規則作查詢時的負擔(overhead)。在此，我們將可以量測到無封包遺失的最大輸出效能(no-loss max throughput)與封包延遲(latency)兩個主要的結果。



圖三：防火牆測試環境

在 URL 與 Content Filter 防火牆的測試方面，我們將用 WebStone[29]送出一個或同時多個 HTTP request 的封包，並使得 HTTP 的封包在通過 Security Gateway 後送往 Web Server，然後由 Web Server 回傳網頁，測試環境如圖四所示。此時 Security Gateway 的

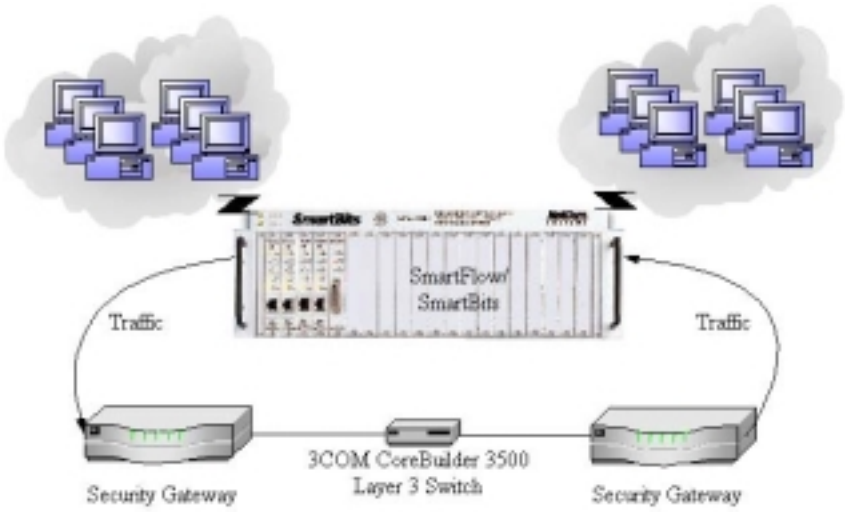
設定分別有：(1) Content Filter 開啓與關閉兩種情形；(2) URL entries 10 與 100 條兩種情形。我們的目的是要檢視 Content Filter 對系統效能的影響以及拿 HTTP 封包查詢多條 URL entries 對效能的影響。



圖四：URL/Content Level 防火牆測試環境

在 VPN 的測試方面，我們也是用 SmartBits 的兩片卡，分別模擬兩個虛擬網路的主機。如圖五所示，由其中一片 SmartCard 模擬 40 台虛擬網路的主機，分別傳送三種大小的封包(128 byte, 1024 byte 與 1518 byte)到另一片模擬 40 台虛擬網路主機的 SmartCard。這時 Security Gateway 間的設定是用 IPSec 標準來建立通道(tunnel)，其中加密法分別用 DES 與 3-DES，認證法用 MD-5，而金鑰交換方式用 Pre-share Key。爲了模擬公司與多個子公司分別建立多條 VPN tunnel 的情形，我們也有測試在兩個 Security Gateway 之間建立 20 個 tunnel 情況。設定方式是將兩邊的虛擬網路切成 20 個子網路，分別記作 s1 ~ s20 與 d1 ~ d20，且兩邊的 40 台主機都平均分配在 20 個子網路上，然後讓 si 的主機傳送封包給 di，其中 i = 1~20。然而，我們傳兩種大封包的原因是：1518 byte 的封包會因爲經過 IPSec 標準的處理後，超過 ethernet 所能容忍的最大封包，所以必須多做封包切割(Fragmentation)的動作，有些產品會在封包切割的表現上特別差。在此，

我們也可以量測到無封包遺失最大輸出效能與封包延遲兩個主要的結果。



圖五：VPN 測試環境

表五是測試的類別、項目以及使用工具的整理。

比較類別	使用工具	比較項目
Management		1. 管理介面是否簡單易用。 2. VPN tunnel 的建立過程是否簡單。 3. 各家產品可否互通(互通性測試)。
Security	Nessus, Nmap	1. 系統是否有安全漏洞。 2. 系統被攻擊時是否會 log 起來。 3. 攻擊 DMZ 內主機時，系統是否會將攻擊型態 log 起來，甚至替 DMZ 內主機阻擋攻擊。
Packet Level Firewall	SmartBits	1. NAT 開啟及關閉時的無封包遺失最大輸出效能(no-loss max throughput)及封包延遲(latency)。 2. 10 及 100 條防火牆規則時的無封包遺失最大輸出效能及封包延遲。
URL Level Firewall	WebStone	1. 10 及 100 條 URL entries 時，一個 web client 每秒鐘所能建立的連結數(connection)與輸出效能(throughput)。 2. 10 及 100 條 URL entries 時的最大連結(connection)數、輸出效能以及交易延遲(transaction latency)。
Content Level Firewall	WebStone	1. 開啟及關閉 Java / ActiveX / JavaScript 時，一個 web client 每秒鐘內所能建立的連結數與輸出效能。 2. 開啟及關閉 Java / ActiveX / JavaScript 時的最大連結數、輸出效能以及交易延遲。
VPN	SmartBits	1. 建立 1 個 LAN-to-LAN tunnel 時的無封包遺失最大輸出效能及封包延遲。 2. 建立 20 個 LAN-to-LAN tunnel 時的無封包遺失最大輸出效能及封包延遲。

表五：測試項目與工具

四、測試結果 – 功能面

管理簡易度與功能完整性

管理的簡易度方面，我們覺得 NetScreen 與 SonicWall 的 web-based 操作介面最容易使用，其次是 WatchGuard 與 BorderWare 的設定管理程式，CheckPoint 雖然有圖形式管理介面，但操作介面不太直覺，最後則是 Cisco 的指令式管理方式。功能完整性方面，NetScreen 與 SonicWall 功能相對較多，其次是 CheckPoint 與 Cisco，再其次是 WatchGuard。此外，BorderWare 屬於各種 Server(含 Web、Mail、DNS 等)與 Security Gateway 整合的 All-in-one 產品，所以功能也是很多，但專就 Security Gateway 而言，功能並不完整。

互通性

在互通性測試上，因爲各產品不是都支援 DES 與 3-DES 兩項加密演算法，所以我們分成兩個表格來表達。表六是採用 3-DES 加密法的互通性，而表七是採用 DES 加密法的互通性，我們發現很少產品可以順利的互通，且在此表現較好的是 NetScreen 與 Cisco。

	Linux(Open Source)	NetScreen	WatchGurard
Linux(Open Source)	a, m	m	
NetScreen	m	a, m	
WatchGuard			a, m

表六：使用 3-DES 加密演算法、MD-5 認證演算法的互通性

(a: automatic；m: manual)

	BorderWare	CheckPoint	Cisco	NetScreen	WatchGuard
BorderWare	a, m		m		
CheckPoint					
Cisco	m		a, m	m	
NetScreen			m	a, m	
WatchGuard					a, m

表七：使用 DES 加密演算法、MD-5 認證演算法的互通性

(a: automatic；m: manual)

安全性

首先必須釐清的是，產品的安全性並不能單純用 Nessus 與 Nmap 套件來評斷，所以在此我們只提供讀者參考。企業網路的安全性也不是只依據 Security Gateway 那個較安全就可以評斷，因爲整個企業網路的安全性還跟網路的架構有密切的關係[30]。由表八得知，大部分產品的漏洞都很少，應該都已經考慮這個問題，開放程式原始碼方案的漏洞主要來源是 TIS 套件。這些產品中，較爲特殊的應屬結合 server 與 gateway 的 BorderWare，該防火牆是屬與 Application Level Gateways，以通訊協定堆疊的角度來看，算是安全等級較高的防火牆，然而整個系統的效能也會大受影響。此外，BorderWare 有一項特殊設計，也就是分別在 trust 與 untrust 兩個網段建立 gateway 上的內\外伺服器，讓網管人員可以避免網路規劃疏失所造成的不安全。

目前有在驗證防火牆安全性的機構包括：(1) ICSA[31](大部分的防火牆都有通過這個標準)；(2) CheckMark[32]；(3) ISO 15408[33](最近成爲 IT 產品安全的認證標準，其中 BorderWare 是唯一通過此項標準的產品，Cisco PIX 目前還在驗證階段)。

Items / Products	Security Gateway			DMZ	
	Security Hole	Security Warning	Log	Log	Drop
Linux (Open Source)	4	6	Yes	Yes	No
BorderWare	0, 無法掃瞄	0, 無法掃瞄	No	No	No
CheckPoint	0, 無法掃瞄	0, 無法掃瞄	Yes	Yes	Yes
Cisco	0	0	Yes	Yes	Yes
NetScreen	0, 無法掃瞄	0, 無法掃瞄	Yes	Yes	Yes
SonicWall	0	1	Yes	Yes	Yes
WatchGuard	0, 無法掃瞄	0, 無法掃瞄	Yes	Yes	No

表八：安全性測試

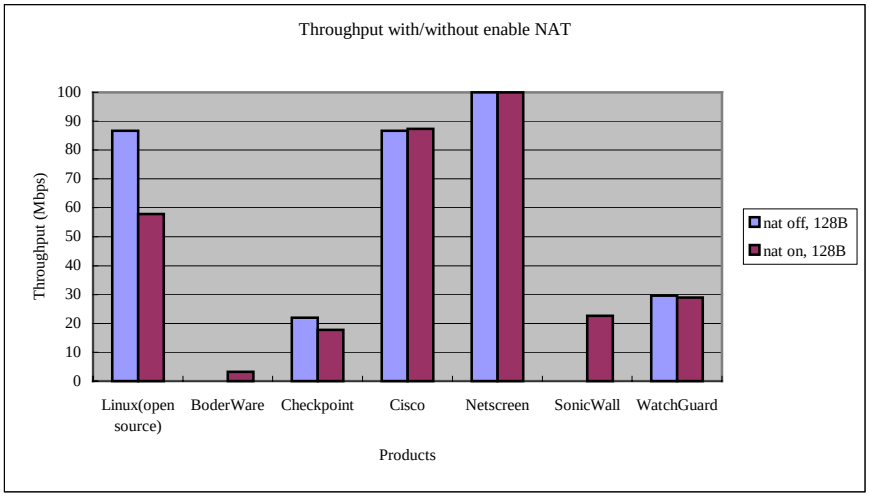
五、測試結果 – 效能面

Packet Level 防火牆

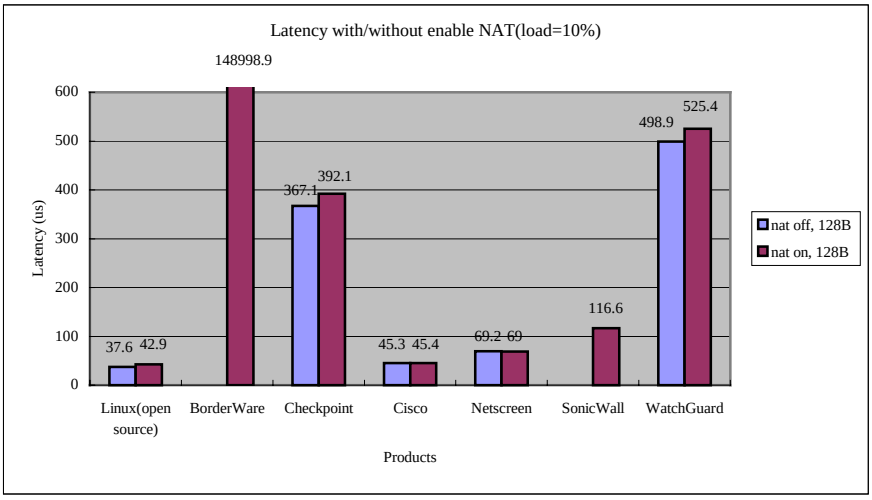
影響 Packet Level 防火牆效能的關鍵有三項：(1) 比對防火牆規則的演算法；(2) CPU 等級；(3) 有無用硬體加速。關於比對防火牆規則的演算法，是要將封包 TCP/IP 標頭的 5 個欄位(field)，拿來與防火牆規則作比對，檢查封包是否符合(match)某條防火牆規則，這也就是 multi-field classification 的問題。因爲需要比對的欄位有 5 個，所以演算法設計的好壞將會影響系統效能。我們覺得 Cisco 與 NetScreen 應該是用硬體加速防火牆的處理，所以效能突出。Linux 則是因爲 CPU 等級較高，所以效能也不錯。SonicWall 與 WatchGuard 則是因爲 CPU 等級較低，所以效能比 Linux 差。CheckPoint 與 Linux 使用相同的硬體配備，但效能較 Linux 差很多，原因應該是 CheckPoint 防火牆軟體套件與 NT 作業系統之間的溝通介面會造成系統很大的負擔(overhead)。

首先要比較圖六中各產品在 NAT 開啓與關閉時的效能差異(其中 BorderWare 系統內部固定作 NAT，SonicWall 廠商要求歸還日期較早，所以此兩項產品沒有關閉 NAT 時的數據)。可以發現只有開放原始碼方案在 NAT 開啓時，效能降幅較大。NetScreen 輸出可達 100%；而 BorderWare 因屬於 Application Level Gateway 類型的防火牆，所以效能明顯差很多。圖七是 Load 在 10%時的 latency，可以發現 CheckPoint 與 WatchGuard 的 latency 較長(因 per-packet 處理時間較長，封包都 queue 在 buffer 中)，BorderWare 則因本身 no-loss max throughput 未達 10%，所以 latency 特大。比較圖六與圖七，SonicWall 的 no-loss max throughput 與 CheckPoint 及 WatchGuard 一樣小，但 latency 卻比較小，依據 Little's Result(N= λ *T，當 λ =no-loss throughput，T=latency 時，N 爲 buffer size)，可以發現這是因爲 SonicWall 的 buffer 很小的緣故，會將來不及處理的封包直接丟棄，而不像其他兩者將封包 queue 起來。圖八則是 Load 達 100%時的封包延遲，可以明顯的看出 Load 很高時各產品的優劣(此圖的 latency y 軸是以指數成長)。圖九則是在 10 或 100 條防火

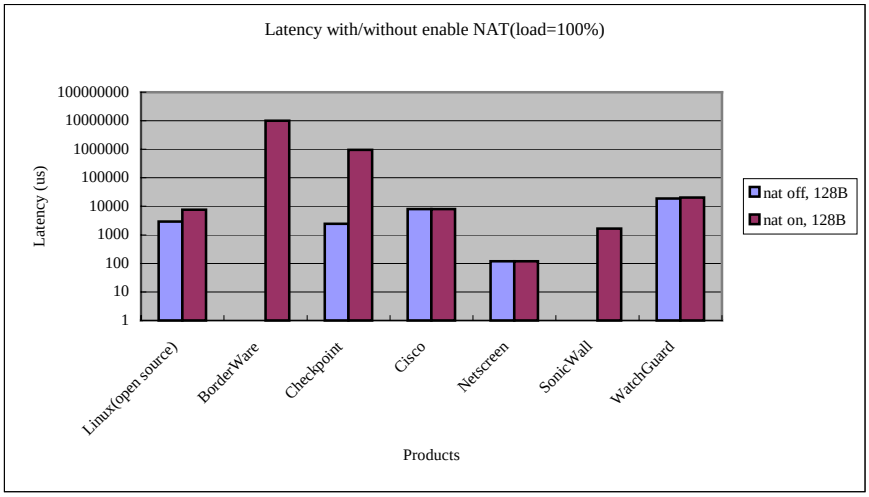
牆規則時，各產品的 no-loss max throughput。可以發現商業產品在 10 或 100 條 rules 時並沒有什麼差異，而開放原始碼方案因爲 ipchains 採用 linear search 演算法檢查所有規則，所以在 10 與 100 條防火牆規則時，no-loss max throughput 差異較大。圖十與圖十一分別是 Load 爲 10%與 100%時的 latency。至於 1518 byte 封包的結果，除了 BorderWate 外，其他產品的表現都很好。



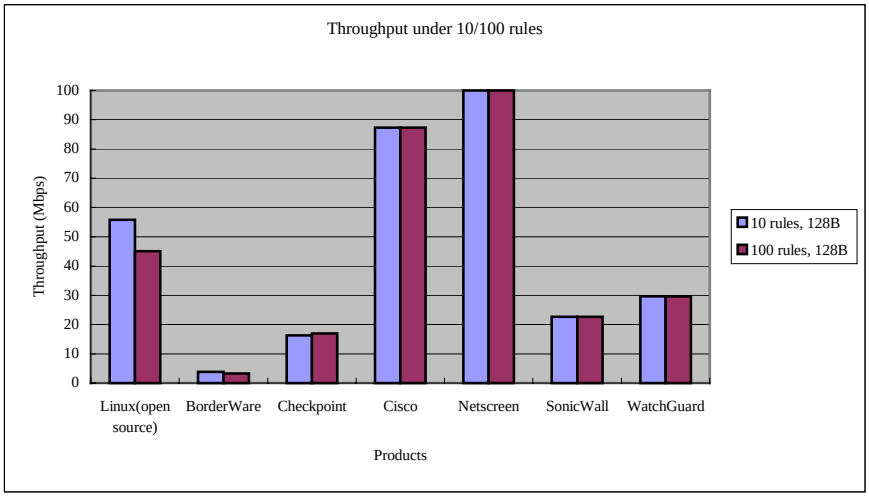
圖六：NAT 開啓與關閉時的 no-loss max throughput



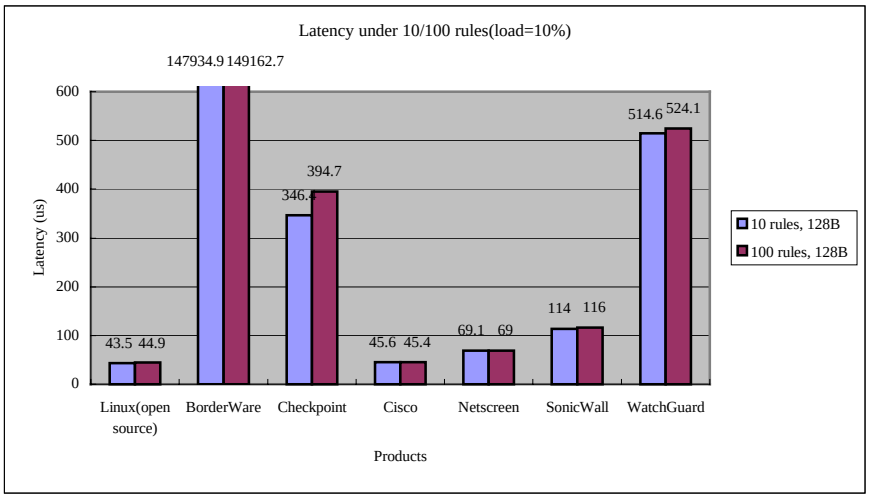
圖七：Load=10%時，NAT 開啓與關閉時的 latency



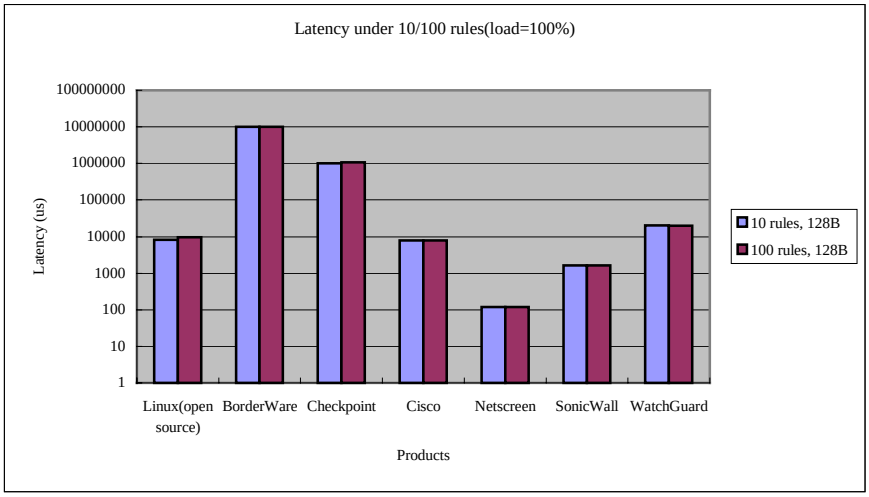
圖八：Load=100%時，NAT 開啓與關閉時的 latency



圖九：10/100 條 firewall rules 時的 no-loss max throughput (NAT 已開啓)



圖十：Load=10%時，10/100 條 firewall rules 時的 latency (NAT 已開啓)



圖十一：Load=100%時，10/100 條 firewall rules 時的 latency (NAT 已開啓)

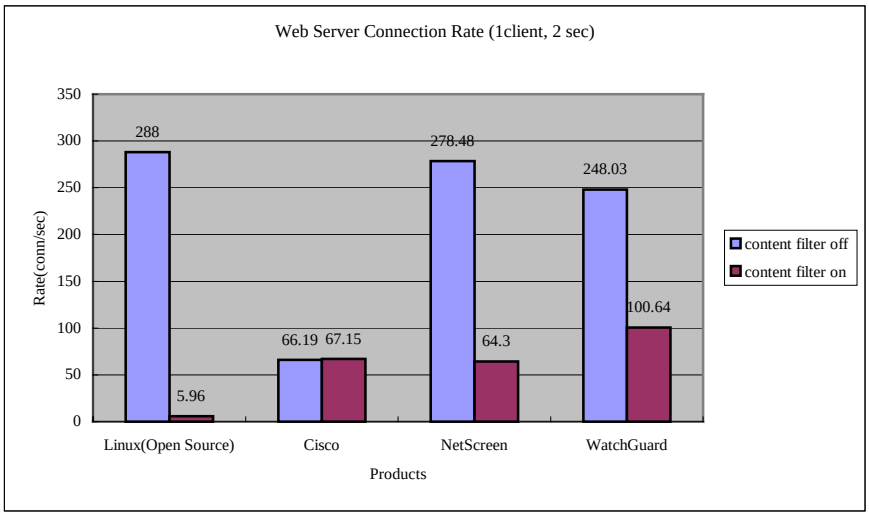
URL Level 防火牆

在 URL Level 防火牆的部分，Cisco 與 NetScreen 只能將 HTTP 封包轉交給作 URL 檢查的主機，而不是在 Security Gateway 上作 URL 的檢查，BorderWare 需要 license 才能使用，SonicWall 因廠商要求歸還日期較早，CheckPoint 與 WatchGuard 沒有此項功能，所以 URL 防火牆的部分就沒有比較數據。

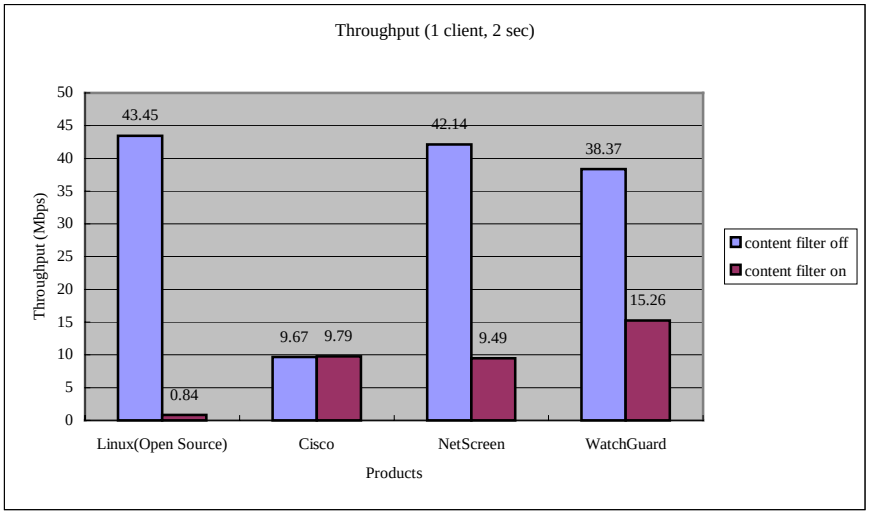
Content Level 防火牆

Content Level 防火牆部分，主要是攔截 java 與 ActiveX 的程式。比較好的作法是，檢查 HTTP 標頭，若發現沒有被允許的 java 或 ActiveX 物件，就將封包攔截並且將其後續封包一併攔截。另外一個比較不好的作法是，將 HTTP response 的所有封包組合之後，再去 parse 檢查有無不被允許的 java 或 ActiveX 物件，並將與 java 或 ActiveX 相關的 HTTP 程式碼移除。我們發現 NetScreen 與 WatchGuard 採用前者作法，Linux 上的 TIS 套件則屬後者。Cisco 的作法則屬於後者的變形，避免將相關的 HTTP 程式碼移除，而是將 java 與 ActiveX 物件註解(remark)掉，這可以避免多做資料在 memory 中搬動的動作。

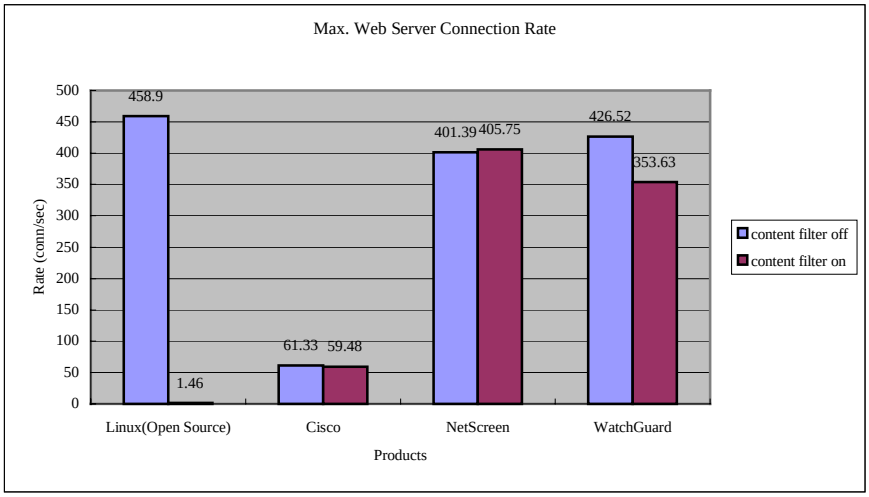
Content Level 防火牆的效能測試方面，因爲 BorderWare 與 CheckPoint 沒有此項功能，且 SonicWall 因廠商要求產品歸還日期較早，所以只有四個評比對象。圖十二是 1 個 web client 連往 web server，中間經過 Security Gateway 時的接通率(Connection Rate)。圖十三則是 1 個 web client 連往 web server，中間經過 Security Gateway 時的 throughput。因爲每個 HTTP connection 所抓取的資料量相同，所以圖十二與圖十三比例類似。圖十四則是在各個產品所能容忍的最大 client 數下，每個 client 各自連續發送 HTTP request，檢視每秒鐘最大的接通數。圖十五則是各產品在每秒最大接通數的情況下，所造成的 throughput。我們發現 Cisco 在 1 個 client 時所造成的 connection rate 與多個 client 造成的 connection rate 差不多，而多個 client 造成 connection rate 稍微下降的原因應該是 Security Gateway 必須同時檢查更多 HTTP response 的網頁資料，而這個情況在 Linux 上則更爲明顯，顯示 TIS 的效能欠佳，我們將換掉此模組。圖十六則是各產品在每秒最大接通數的情況下，HTTP request 發出至接到 HTTP response 之間的 latency。



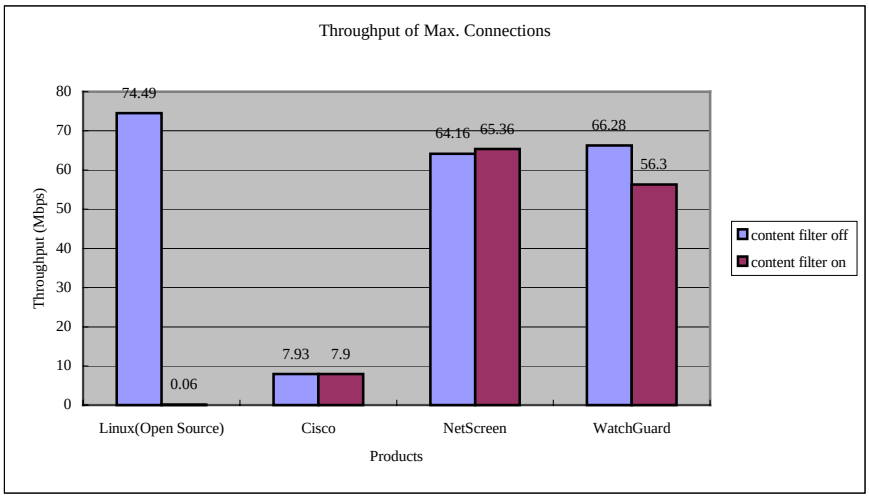
圖十二：1 個 web client 連結 web server 的 Web Server Connection Rate



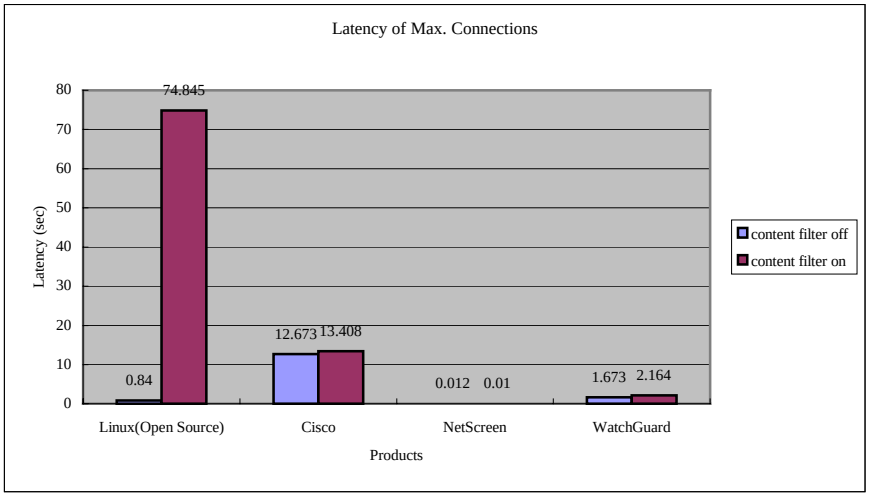
圖十三：1 個 web client 時的 throughput



圖十四：每秒鐘所能建立的最大 connection 數



圖十五：最大 connection 數時的 throughput



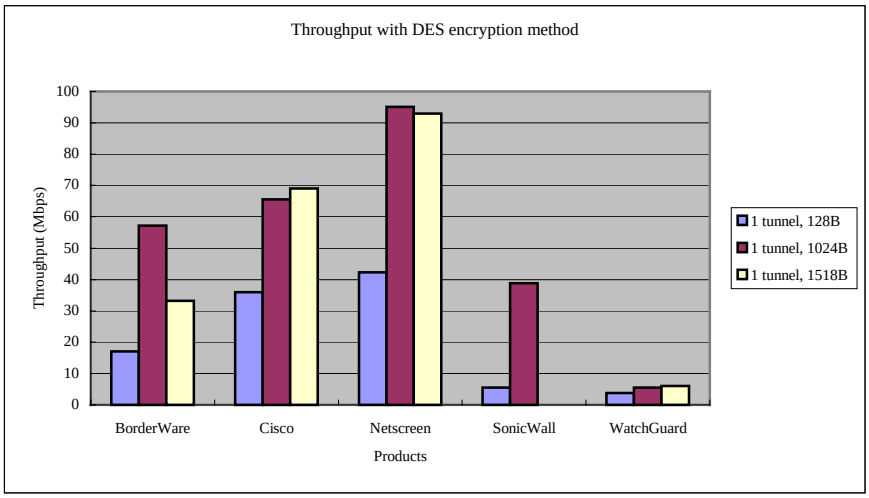
圖十六：最大 connection 數時，HTTP request 發出至接到 HTTP response 間的 latency

VPN 效能

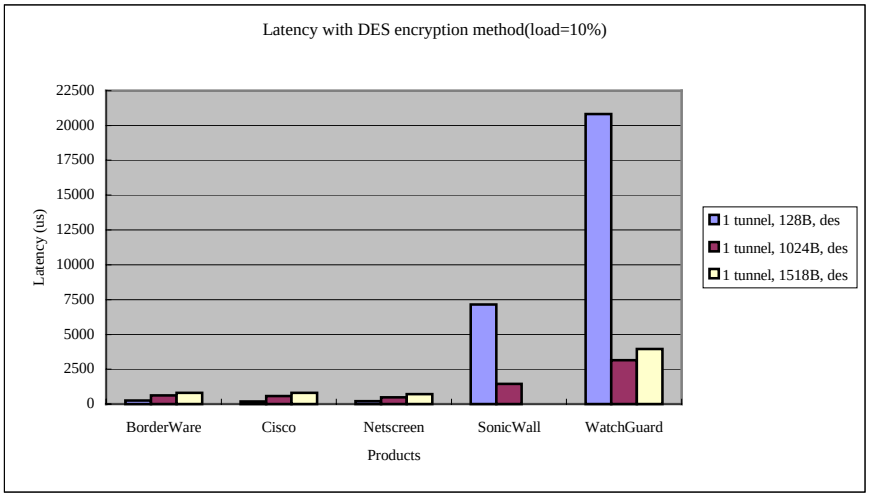
VPN 技術最耗費時間的工作在於用 DES 或 3-DES 加解密，但加解密的演算法固定，所以會影響效能的主要是 CPU 的等級以及有無硬體加速。NetScreen 用 ASIC 加速，所以效能突出。SonicWall 雖使用 VPN 加速卡加速，然而效能不夠好的原因是應該是 CPU 等級較低。Linux 則因 CPU 等級較高，所以 VPN 效能不會太差。

此項測試中，只有 BorderWare、CheckPoint、Cisco、NetScreen、SonicWall 與 WatchGuard 有 DES 加密演算法，且只有 Linux、NetScreen、SonicWall 與 WatchGuard 有 3-DES 加密演算法。另外，可惜的是我們所拿到的 CheckPoint 防火牆是 NT 的版本，不是原本要求的 Appliance 型號。我們發現在 CheckPoint 的控管程式設定好後，還必須在 NT 作業系統上重新啓動 CheckPoint 服務，設定上較不親切。一個多月來，我們照著手冊作，但是並沒有將 CheckPoint 的 VPN tunnel 建立起來。代理商則因人手不足，無法給我們這方面的幫助。圖十七是三種大小封包在使用 DES 加密法時的 no-loss max throughput。因爲 1518 byte 封包經過 IPSec 標準的處理後，封包會大於 ethernet 所能容忍的大小，所以需要多作切割的動作。由此可見，BorderWare 在此項的表現不太好。圖十八與圖十九則是 Load 爲 10%與 100%時的 latency。從 SonicWall

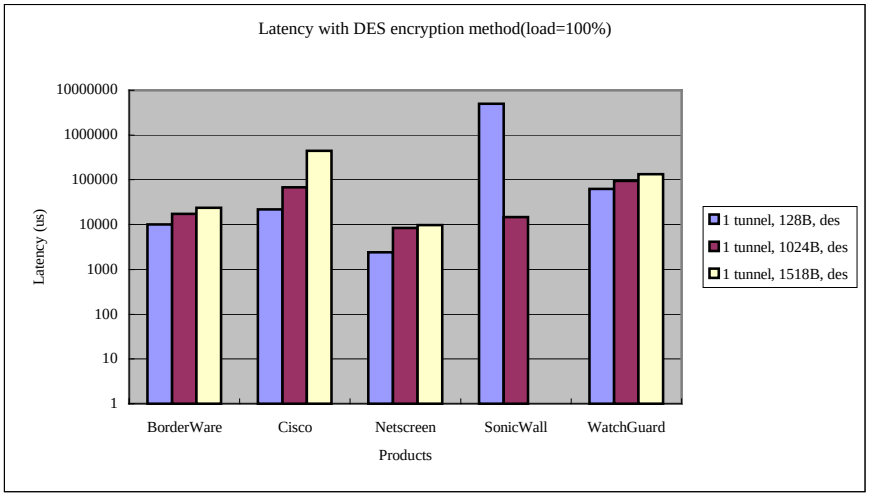
與 WatchGuard 的結果可以看出，當 load 大於 no-loss max throughput 時，可能會因爲系統接受太多的 interrupt (也就是系統在替內部的封包加解密時，仍然有過量封包一直送到系統來)，導致 latency 過大。圖二十、二十一、二十二則是採用 3-DES 加密時的狀況，結果與 DES 類似。關於 20 個 tunnel 與 1 個 tunnel 時的 no-loss max throughput 與 latency，我們發現各產品不會因爲 tunnel 數多了 19 個就會比較慢。唯一例外的是 Load 爲 100%時，SonicWall 大封包的 latency 在 tunnel 數爲 20 個時較高，如圖二十三所示。



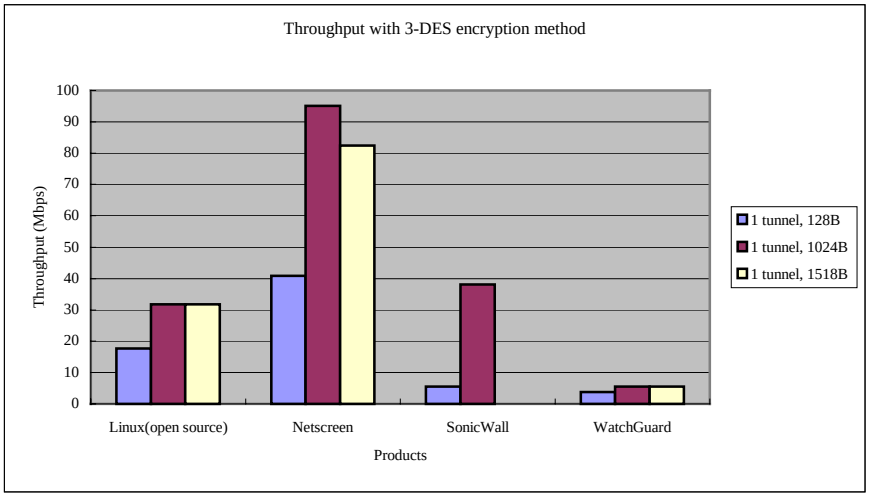
圖十七：使用 DES 加密的 no-loss max throughput



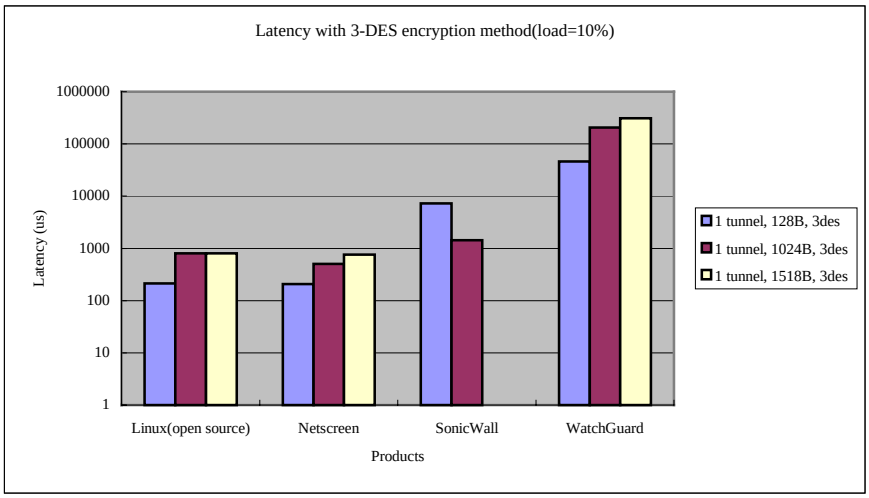
圖十八：Load=10%時，使用 DES 加密的 latency



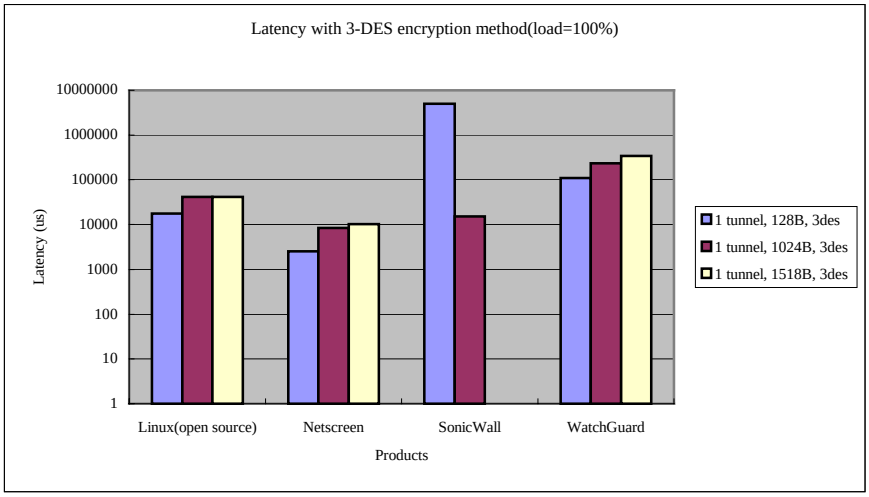
圖十九：Load=100%時，使用 DES 加密的 latency



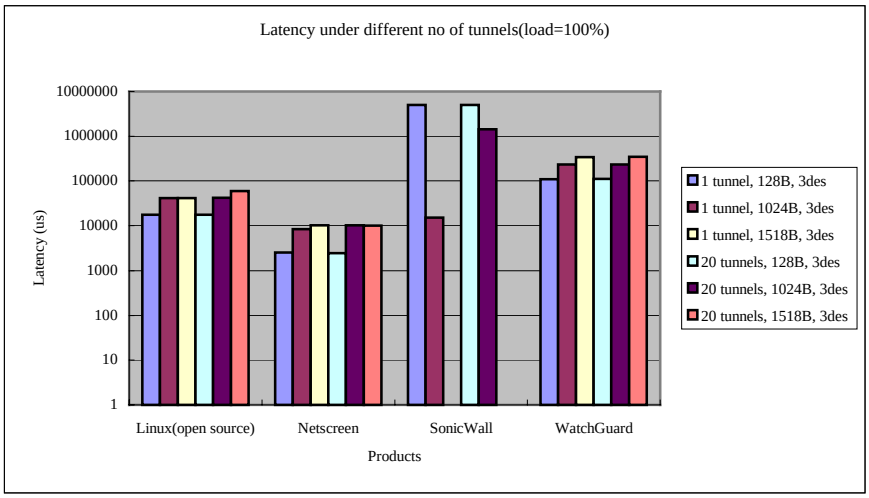
圖二十：使用 3-DES 加密的 no-loss max throughput



圖二十一：Load=10%時，使用 3-DES 加密的 latency



圖二十二：Load=100%時，使用 3-DES 加密的 latency



圖二十三：Load=100%時，1 與 20 個 VPN tunnel 的 latency

六、結論

做 Security Gateway 產品測試的動機是，起先我們利用 Linux 開放原始碼的套件在工業級電腦上整合完成一個 Security Gateway，並撰寫了 web-based 控管介面。然而，我們對開放原始碼解決方案與商業產品的功能與效能差異感到好奇。效能方面，結果讓我們驚訝地發現它沒有特殊硬體加速時的表現傑出。功能上也很完整，當然也發現商業產品有一些獨特的功能可以學習，使我們的開放原始碼解決方案可以更進一步提升。我們發現國外的 Security Gateway 測試計畫，常常只測防火牆效能、安全性與管理，或者只測 VPN 效能、安全性與管理。而我們的測試項目比較廣泛，包括管理簡易度、功能完

整性、互通性、安全性、Packet Level 防火牆效能、URL/Content Level 防火牆效能與 VPN 效能。我們發現國外並沒有非 Packet Level 防火牆的效能測試，這也是本次測試的獨特性。此外還可以發現國外的測試方式多用 TCP 連線來測試產品防火牆與 VPN 的效能，而我們選擇使用 SmartBits 來產生封包並量測結果，使用 SmartBits 的好處是，可以量測出產品的實際效能，而不會受到 TCP 協定本身被 blocking 等待的影響。URL/Content Level 防火牆效能測試上，則因 SmartBits 功能上的限制而改用實際建立 TCP 連線的方式。值得一提的是，除了 SmartBits 外，其他的測試工具都是開放原始碼套件，大家都可以自行驗證產品的效能，也就是這些結果是 reproducible。

此次測試最花時間的就是測試方式的調整，原本我們用 SPECWeb 來產生 HTTP 封包，但是發現 SPECWeb 主要是測 Web Server 的效能，所以改用 Web Bench 套件。Web Bench 則因收集到的結果太少，所以最後改用著名的 Web Stone 套件。測試中還發現，效能測試上會有一些例外情況，也就是產品會不小心遺失幾個封包(如 1 個)，使得用 binary search 來量測單項產品的無封包遺失最大輸出，數據差異很大，這通常只要多測幾次就不會有這種情形。此外，像 Cisco 與 CheckPoint 產品設定比較不容易，所以也花費了一些時間學習。當每家產品的數據圖表都完成後，看到各種解決方案的效能差異以及效能上奇特的變化是我們覺得產品測試最有趣的地方。對學術界而言，有時會是以研究別人的論文爲切入點，或者自行定義問題，其實我們也可以從實作中找到可以改進的地方與研究主題。對於產業界，我們所要表達的是，本土業界常常只重視功能的多寡，而往往忽略系統效能，我們必須從能動(70 分)進展到跑得快(90 分)。從這次測試也學習到測試工具的使用方式以及工具的設計理念，所以未來需要開發此類工具時，將會知道如何設計。我們也發現了開放原始碼套件的問題，期待開放原始碼可以繼續成長。

對於測試報告的結論，我們對所有比較的功能與效能作評分，滿分爲 5 顆星。最後並以主觀的角度對產品做整體的評價。我們將原本整合開放原始碼套件的系統標示爲 original，而附加 web-based 控管介面的系統標示爲 SecureStar。

	管理簡易度
Linux (original)	★
Linux (SecureStar)	★★★½
BorderWare	★★★★
CheckPoint	★★★
Cisco	★★
NetScreen	★★★★★
SonicWall	★★★★★
WatchGuard	★★★★

表十：管理簡易度

	功能完整性
Linux (original)	★★★★
Linux (SecureStar)	★★★★
BorderWare	★★
CheckPoint	★★★★
Cisco	★★★★
NetScreen	★★★★★
SonicWall	★★★★★
WatchGuard	★★★

表十一：功能完整性

	安全性
Linux (original)	★
Linux (SecureStar)	★
BorderWare	★★★★★
CheckPoint	★★★★★
Cisco	★★★★★
NetScreen	★★★★★
SonicWall	★★★★
WatchGuard	★★★★★

表十二：安全性

	互通性
Linux (original)	★★★
Linux (SecureStar)	★★★
BorderWare	★★
CheckPoint	未建起 tunnel
Cisco	★★★★
NetScreen	★★★★
SonicWall	歸還日期較早
WatchGuard	★

表十三：互通性

	Packet Level 防火牆效能
Linux (original)	★★★
Linux (SecureStar)	★★★
BorderWare	★½
CheckPoint	★★
Cisco	★★★★
NetScreen	★★★★★
SonicWall	★★
WatchGuard	★★

表十四：Packet Level 防火牆效能

	Content Level 防火牆效能
Linux (original)	★
Linux (SecureStar)	★
BorderWare	無此功能
CheckPoint	無此功能
Cisco	★★★
NetScreen	★★★★
SonicWall	歸還日期較早
WatchGuard	★★★★

表十五：Content Level 防火牆效能

	VPN 效能
Linux (original)	★★★
Linux (SecureStar)	★★★
BorderWare	★★★
CheckPoint	未建起 tunnel
Cisco	★★★★
NetScreen	★★★★★
SonicWall	★★
WatchGuard	★½

表十六：VPN 效能

	performance/price
Linux (original)	★★★★★
Linux (SecureStar)	★★★★★
BorderWare	★★
CheckPoint	★★
Cisco	★★★
NetScreen	★★★★★
SonicWall	★★★
WatchGuard	★★

表十七：performance/price

	整體評價
Linux (original)	★★½
Linux (SecureStar)	★★★★
BorderWare	★★½
CheckPoint	★★★½
Cisco	★★★★½
NetScreen	★★★★★
SonicWall	★★★½
WatchGuard	★★½

表十八：整體評價

六、參考文獻

[1] CERT Coordination Center, “Denial of Service Attacks”, Feb 12 1999, http://www.cert.org/tech_tips/denial_of_service.html.

[2] Linux ipchains Document, http://netfilter.filewatcher.org/ipchains/HOWTO.html.

[3] Squid Proxy Server, http://www.squid-cache.org.

[4] Trust Information System (TIS), http://www.tis.com.

[5] GenNet, http://www.gennet.com.tw.

[6] ipTrend, http://www.iptrend.com.tw.

[7] ZyXEL, http://www.zyxel.com.tw.

[8] Cisco, http://www.cisco.com.

[9] NetScreen, http://www.netscreen.com.

[10] CheckPoint, http://www.checkpoint.com.
[11] SonicWall, http://www.sonicwall.com.
[12] WatchGuard, http://www.watchguard.com.
[13] Intel, http://www.intel.com.
[14] Nortel, http://www.nortelnetworks.com.
[15] CyberGuard, http://www.cyberguard.com.
[16] Computer Associates, http://www.cai.com.tw.
[17] TeleSynergy, http://www.telesynergy.com.tw.
[18] BorderWare, http://www.borderware.com.
[19] TopLayer, http://www.toplayer.com.
[20] FreeS/WAN, http://www.freeswan.org.
[21] Zebra, http://www.zebra.com.
[22] Snort, http://www.snort.org.
[23] portslave, http://www.psychosis.com/linux-router/portslave/.
[24] pppd, http://www.redhat.com.
[25] Logsurfer, http://www.cert.dfn.de/eng/logsurf/.
[26] Nmap, http://www.nmap.org.
[27] Nessus, http://www.nessus.org.
[28] SmartBits, http://www.netcomsystems.com.
[29] WebStone, http://www.mindcraft.com/webstone/.
[30] D. Brent Chapman and Elizabeth D. Zwicky, “Building Internet Firewalls”, O’ REILLY, Oct. 1998.
[31] NCSA, http://www.ncsa.net.
[32] CheckMark, http://www.westcoast.com.
[33] ISO 15408, http://csrc.nist.gov/cc/ccv20/ccv2list.htm.