網路安全產品測試評比 – 功能與效能面

測試計畫主持人：林盈達

測試報告撰寫人：林柏青

測試人員：林柏青、林毓達、溫碩彥、歐陽銘康、詹智為、林權宏、黃福祥

測試單位：工研院交大網路測試中心

新竹市大學路 1001 號

摘要

隨著各種網路安全事件層出不窮，網路安全的技術與產品因此日益獲得重視。目前市面上的網路安全產品大致可分為五大類：防火牆(firewall)、虛擬私有網路(VPN)、入侵偵測系統(IDS)、防毒系統(antivirus)、以及內容過濾器 (content filter)。本次測試即以這五大類網路安全產品分別邀請共計十六家廠商二十五項產品進行測試，在防火牆及 VPN 部份，由於產品眾多，且等級不一，我們再依據產品的市場定位細分為 SOHO、中小企業(SME)、企業級(enterprise)、電信等級(carrier)。每樣產品均依據個別特性從使用簡易度、產品功能、效能評定、偵測的精確度、記錄檔的維護等項目檢視其優劣，結果之圖表均主動聯繫廠商尋求確認。報告之結論依 1~5 顆星分別替產品打分數，並將產品實際價格一塊列入考量予以價值總評。在 SOHO 防火牆等級，我們給予 NetScreen-5GT 最高的評價；在 SME 等級以及在 enterprise 等級則分別屬 WatchGuard 1000 及 CheckPoint NGAI 勝出，但在考慮產品價格後，由 Cisco PIX 515E 及 D-Link DFL-1500 分別在性價比上獲得最優。在 carrier 等級由於只有 NetScreen-5200 參加，故不予排名。但其實測效能較本中心去年安全閘道器測試中之任何一款 carrier 級的產品為佳。在 IDS 方面，我們給予 NetScreen-IDP 100 最高的評價。而 antivirus 及 content filter 方面則分別由趨勢的 InterScan VirusWall 以及 SurfControl Web filter 獲得優勝，另 WebSense 獲得 content filter 的最高性價比。

關鍵字：安全閘道器，防火牆，虛擬私有網路，入侵偵測，防毒系統，內容過濾，頻寬管理，效能評比

1、簡介

網際網路(Internet)發展快速，雖然帶給企業及個人相當大的便利，但是各種網路安全事件同時也不斷與日俱增。根據 CERT® Coordination Center(一個電腦安全事件反應的組織)所做的統計顯示，自 2000 年迄今，網路安全事件發生的案例每年約增加 30,000 筆。單是今年上半年的案例個數就以高達 76,404 筆，已逼近去年全年的案例個數(http://www.cert.org/stats/cert_stats.html)。而這類的安全事件更造成企業及個人的龐大損失，據 Computer Economics 雜誌的統計，單是著名的 CodeRed 病毒就在經濟上已造成約 26 億美元的損失。因此網路安全議題已經到了不容忽視的地步。

為了保護企業及個人的網路，各種網路安全產品就應運而生。綜觀市面上的防火牆產品，依功能可以歸類為五大類：防火牆(firewall)、虛擬私有網路(Virtual Private Network，簡稱 VPN)、入侵偵測系統(Intrusion Detection System，簡稱 IDS)、防毒系統(antivirus)、以及內容過濾器 (content filter)。防火牆可以控制封包的進出，以阻擋外界不當存取企業內部的網路或防止員工不當使用網路。虛擬私有網路可以在網際網路中，利用加密認證等技術建立起私有的傳輸通道，以確保資料不被窺視、修改、或假冒。入侵偵測系統可以監看封包內容，以查覺是否有入侵事件發生。防毒系統則可掃描進出網路的檔案或網頁，以避免病毒侵入。內容過濾器則可限制不當網頁的存取，或是不當資料的流出。本測試報告將檢視各家廠商的網路安全產品，比較各家產品的功能(functionality)、管理介面(management)、互通性(interoperability)、偵測率(detection rate)及效能(performance)，以提供網管人員選購網路安全產品時的參考準則。圖一及圖二則為本次測試的待測產品。

評量方式

由於目前防火牆產品幾乎都有 VPN 的功能，本次測試將防火牆及 VPN 合併為一大類進行評量。各大類主要觀察的項目如下：

防火牆/VPN：(1)產品硬體規格、(2)管理方式及簡易度、(3)記錄檔稽核、(4)防火牆功能、(5)防火牆效能、(6)VPN 功能、(7)VPN 互通性、(8)VPN 效能、(9)頻寬管理，並歸納為管理功能、產品功能、防火牆效能、VPN 效能做為評量標準。

入侵偵測系統：(1)產品硬體規格、(2)入侵偵測的功能、(3)管理方式、(4)入侵偵測的效能、(5)處理迴避偵測(evasion)的能力，並分管理功能、入侵偵測功能，以及偵測能力進行評量。

防毒系統：(1)支援的協定及檔案格式、(2)管理方式、(3)處理病毒方式、(4)遞送郵件及掃毒所需的時間。並以管理功能、支援的協定及格式、偵測能力、效能等指標進行評量。

內容過濾器：(1)過濾功能、(2)管理方式、(3)網頁過濾漏擋率、(4)通過內容過濾器的throughput。並以管理功能、成功過濾的比率、效能等指標進行評量。

圖一、防火牆/虛擬私有網路受測產品

圖二、入侵偵測系統、防毒系統、內容過濾器受測產品

2、測試評比對象

在篩選產品的過程中，我們先查詢各家廠商的網頁，找尋具有前述五大類產品且佔有率較高的產品。由於在防火牆/虛擬私有網路方面產品已臻成熟且為數眾多，我們再依據該類產品的市場定位再區分為(1) SOHO (Small Office, Home Office)，(2) 中小企業(SME, Small and Medium Enterprise)等級，(3) 企業(Enterprise)等級，(4) 電信(Carrier)等級。等級分類的原則是以各廠商對該產品在市場上設下的定位為準，而非以價格來做區分。接著我們對各廠商發出邀請，並附上測試計畫書。最後共計有 16 家廠商共計 25 項商業產品參與本測試，參與廠商、代理商、以及產品名稱則摘要於表一及表二當中，測試工具程式及設備則列於表三。其中防火牆/虛擬私有網路 7 家廠商 13 項產品，入侵偵測系統有 3 家廠商 5 項產品，防毒系統有 3 家廠商 3 項產品，內容過濾器有 4 家廠商 4 項產品參加。除此之外，在入侵偵測系統類我們也列入了 open source 軟體 Snort 2.0，並與商業產品一併做個比較。邀請於今年 5 月初送出，產品於 6 月底收集完成，測試工作於 8 月初完成，所有列表與數據均主動聯繫廠商尋求確認。

本次測試較過去兩次本中心舉辦之網路安全產品測試，具有以下特色：(1) 除了防火牆和虛擬私有網路外，本次測試首度加入了入侵偵測系統、防毒系統及內容過濾器進行測試。(2) 在防火牆、防毒系統、內容過濾器三類產品，均測試了國內廠商的產品。其功

能及效能大致不差，但在價格上更具競爭優勢。(3) 本次測試嘗試使用了一些新的測試工具，如 Spirent TeraVPN、Avalanche/Reflector 等設備，使得測試環境較為簡化，但同時也發現了新測試工具在測試上的限制。(4) 本次測試產品數量較前次多出一倍以上，對參與測試人員本身是一大考驗。

等級	原廠	代理商	產品名稱
SOHO	AboCom (友旺科技)	岱昇科技	AboCom FW 100
	Check Point	精誠資訊	Check Point S-box
	D-Link (友訊科技)	友冠資訊	D-Link DFL-100
	NetScreen	友冠資訊	NetScreen-5GT
	WatchGuard	泓彥資訊	WatchGuard SOHO6tc
	ZyXEL(合勤科技)	泓彥資訊	ZyWall 10W
SME	AboCom (友旺科技)	岱昇科技	AboCom FW 500
	Cisco		Cisco PIX 515E
	WatchGuard	泓彥資訊	WatchGuard 1000
Enterprise	AboCom (友旺科技)	岱昇科技	AboCom FW 1000
	Check Point	精誠資訊	Check Point NGAI
	D-Link (友訊科技)	友冠資訊	D-Link DFL 1500
Carrier	NetScreen	友冠資訊	NetScreen-5200

表一、防火牆/VPN 參與測試廠商及產品一覽表

種類	原廠	代理商	產品名稱
IDS	Intrusion	精誠資訊	Intrusion SecureNet 5545
	Intrusion	精誠資訊	Intrusion SecureNet 7145
	ISS	鈺松國際	RealSecure Gigabit Sensor
	ISS	鈺松國際	Proventia A201
	NetScreen	友冠資訊	NetScreen-IDP100
Antivirus	HGiga(桓基科技)	桓基科技	Virusherlock
	Panda	Panda Taiwan	PerimeterScan
	TrendMicro(趨勢科技)	精誠資訊	InterScan VirusWall
Content filter	AscenVision (亞盛科技)	亞盛科技	AscenGate 2000
	Axtronics(文佳科技)	文佳科技	防堵色情閘道系統
	SurfControl	一高商務科技	SurfControl Web Filter
	WebSense	精誠資訊	WebSense Enterprise v5

表二、IDS/Antivirus/Content filter 參與測試廠商及產品一覽表

種類	測試工具程式及設備
防火牆	Smartbits, SmartMetrics, SmartFlow, WebSuite
虛擬私有網路	Smartbits, TeraMetrics, TeraVPN
入侵偵測系統	Avalanche, Reflector, nessus, fragrouter, nikto, snot
防毒系統	自行撰寫的發信 script
內容過濾器	Avalanche

表三、測試工具程式及設備一覽表

3、SOHO 等級防火牆 / 虛擬私有網路產品測試

3.1 型號及規格

本次測試在 SOHO 等級共有六家廠商六項產品參與，國內及國外廠商各半。這些產品型號及功能列於表四。

	Firewall	VPN	IDS	Antivirus	Content filter	Bandwidth Mgmt
AboCom FW 100	Yes	Yes	No	No	Yes	No
Check Point S-box	Yes	optional	No	redirect	redirect	No
D-Link DFL 100	Yes	Yes	No	No	No	No
NetScreen-5GT	Yes	Yes	No	No	*Yes	Yes
WatchGuard SOHO6tc	Yes	Yes	No	No	Yes	No
ZyXEL ZyWALL 10W	Yes	Yes	No	No	Yes	No

*NetScreen can also redirect URL requests to WebSense or SurfControl.

表四、SOHO 等級防火牆/私有虛擬網路產品功能比較表

雖然上述的產品皆沒有完整 IDS 的能力，但是大都有複雜度不一處理攻擊的能力。在我們的效能測試中，有的機器會自動將大量封包的流入視為攻擊而予以阻絕，如 ZyWALL 10W。有的可以勾選特定攻擊的類型來阻絕，如 NetScreen-5GT。內容過濾則幾乎已經成為標準的功能，有的產品還可以另外搭配其他廠牌的內容過濾器增強過濾能力。Check Point 可 redirect 郵件做掃毒，而 NetScreen 則表示未來 5GT 將提供內建的掃毒功能。受測物的內部及外部規格則列於表五(a)及(b)。

	OS	**CPU**	**Accelerator**	**RAM**	**Flash**	**Hard disk**
AboCom FW 100	Linux	Wave WP 3200	No	32 MB	16 MB	No
Check Point S-box	N/A	Toshiba 32-bit RISC 133 MHz	No	32 MB	8 MB	No
D-Link DFL 100	N/A	Toshiba 64-bit RISC 200 MHz	Embedded in processor	32 MB	2 MB	No
NetScreen-5GT	ScreenOS ver 4.0.0	Intel IXP 425 400 MHz	Embedded in processor	128 MB	32 MB	No
WatchGuard SOHO6tc	Linux	Brecis MSP2000 150 MHz	Embedded in processor	16 MB	4 MB	No

ZyXEL ZyWALL 10W	ZyNOS ver 3.60	Toshiba 32-bit RISC 133 MHz	SafeNet CryptCore 1140	16 MB	8 MB	No

表五(a)、SOHO 等級防火牆/私有虛擬網路產品內部規格比較表

	Network interfaces	**Console**	**High-availability port**	**Reset button**	**Size**
AboCom FW 100	LAN: FEx4 DMZ: FEx1 WAN: FEx1	No	No	Yes	220mm(L) x 150mm(D) x 40mm(H)
Check Point S-box	LAN: FEx4 WAN: FEx1	No	No	Yes	200mm(L) x 121mm(D) x 30mm (H)
D-Link DFL 100	LAN: FEx3 DMZ: FEx1 WAN: FEx1	No	No	Yes	235mm(L) x 155mm(D) x 35mm(H)
NetScreen-5GT	Total: FEx5 (with WAN: FEx1)	DB-9	dual untrust (WAN) port & DB-9 (dial backup)	Yes	209mm(L) x 125mm (D) x 25mm(H)
WatchGuard SOHO6tc	LAN: FEx4 WAN: FEx1 optional:FEx1	DB-9	No	Yes	233mm(L) x 155mm(D) x 30mm(H)
ZyXEL ZyWALL 10W	LAN: FEx1 WAN: FEx1 WLANx1(optional)	DB-9	DB-9 (shared with console)	Yes	233mm(L) x 155mm(D) x 30mm(H)

表五(b)、SOHO 等級防火牆/私有虛擬網路產品外部規格比較表

從硬體規格來看，比較特別的是 ZyWALL 有提供 PCMCIA 規格的 wireless LAN 插槽，並支援 IEEE 802.1X 標準。在無線區域網路日漸普及的今天，這樣一個的設計對使用無線區域網路的單位是一項便利。此外，除了一般熟知的 LAN、WAN、DMZ，NetScreen-5GT 可以自行定義 security zone，並設定 security zone 與 port 間的對應關係，及定義 security zone 內部及彼此之間的規則。相對於多數產品固定 port 功用的做法，這樣的設計對網路管理而言較有彈性。

3.2 管理簡易度

表六是受測機器管理和設定的規格比較表。在操作介面上，這幾款防火牆操作均相當直覺。可以說只要具備基礎的網路概念，在不用翻閱手冊的情形下就可以完成基本的設定。除了 Web 介面的管理之外，我們認為 console 介面的管理也很重要。因為如果有設定錯誤的情形，使得無法正確從 Ethernet port 連進去管理的時候，就可以透過 console port 進行設定，而非束手無策。

就系統的維護來看，所有的產品均提供設定的備份及復原的功能。另外，也都有提供 Reset 按鈕，可以很快速的將系統還原回出廠時的設定值。

	Management Interfaces			System Maintenance		Troubleshooting	
	GUI	**CLI**	**SNMP**	**config restore**	**Firmware upgrade**	**Network statistics**	**CPU/MEM utilization**
AboCom FW 100	http	telnet	Yes	Yes	Yes	Yes	No
Check Point S-box	http https	No	No	Yes	Yes	Yes	No
D-Link DFL 100	http	telnet	Yes	Yes	Yes	Yes	Yes
NetScreen-5GT	http https	telnet SSH	Yes	Yes	Yes	Yes	Yes
WatchGuard SOHO6tc	http	No	No	Yes	Yes	Yes	No
ZyXEL ZyWALL 10W	http	telnet	Yes	Yes	Yes	Yes	Yes (in CLI)

表六、SOHO 等級防火牆/私有虛擬網路產品管理與設定規格比較表

3.3 記錄檔稽核

表七顯示的是記錄檔稽核的項目及功能。從上表可以看出，目前的產品大都能確實的記錄支援的功能中發生的事件。另外，記錄檔除了儲存在產品本身外，能夠輸出到外界的儲存媒體也很重要。大部分的產品都有支援用 email 發送的功能，以及 syslog 的功能。另 AboCom、NetScreen、以及 WatchGuard 的產品有支援直接將記錄檔下載成檔案的功能。值得一提的是，Check Point 可以針對事件的類別用不同的顏色標示，以及 NetScreen -5GT 提供了事件搜尋的功能。這些都可以讓管理者很快的在龐大的記錄檔中，找要重要記錄。

	Logging items					Logging functions			
	Firewall log	**VPN log**	**Intrusion log**	**CF log**	**Event log**	**Send logs to emails**	**syslog**	**Alarm mail**	**Down-load to file**
AboCom FW 100	Yes	No	Yes	No	Yes	Yes	Yes	Yes	Yes
CheckPoint S-box	No	No	No	re-direct	Yes	No	Yes	No	No
D-Link DFL 100	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	No
NetScreen-5GT	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
WatchGuard SOHO6tc	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
ZyXEL ZyWALL 10W	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No

表七、SOHO 等級防火牆/私有虛擬網路產品記錄稽核規格比較表

3.4 防火牆的功能

表八列出防火牆基本的功能。目前的防火牆皆有支援 stateful inspection 的功能，對 NAT 的支援功能也稱完善。其中值得一提的是，在防火牆規則的設定上，D-Link DFL 100 控制的是流量的方向(從外部到內部，或是從內部到外部)，而非特定範圍的 IP 位址，如果沒有特殊的需求的話，這樣的設計對一般 SOHO 使用者而言較為簡單。NetScreen-5GT 可以自行定義 address group，讓同一個 group 內的位址適用相同的規則。這點讓規則的設定上更有彈性。另外，NetScreen-5GT 還可以針對 time 和 VPN tunnel 設定規則。

	Firewall			**Network Address Translation (NAT)**			
	Packet filter	**Stateful inspection**	**Rule definition**	**NAT(1-1)**	**NAT(M-1)**	**NAT(M-M)**	**Port forwarding**
AboCom FW 100	Yes	Yes	SIP/DIP/SP/DP/ protocol	Yes	Yes	Yes	Yes
Check Point S-box	Yes	Yes	SIP/DIP/service/ protocol	optional	Yes	No	Yes
D-Link DFL 100	Yes	Yes	direction/DP/ service/protocol	Yes	Yes	Yes	Yes
NetScreen-5GT	Yes	Yes	SIP/DIP/service/ addr group/VPN tunnel/time/user	Yes	Yes	Yes	Yes
WatchGuard SOHO6tc	Yes	Yes	SIP/DIP/service/ protocol	No	Yes	No	No
ZyXEL ZyWALL 10W	Yes	Yes	SIP/DIP/service/ protocol	Yes	Yes	Yes	Yes

表八、SOHO 等級防火牆/私有虛擬網路產品防火牆/NAT 規格比較表

3.5 虛擬私有網路(VPN)的功能

在 VPN 的功能方面，結果如表九(a)和(b)所示。除了 Check Point S-box 的 VPN 功能為選購的之外，其他的受測產品皆附有 VPN 的功能，且支援 DES/3DES 加密方式以及 MD5/SHA-1 認證方式。其中 NetScreen-5GT 還支援較新的 AES 加密方式。我們使用 TeraVPN 工具做為互通性(interoperability)測試工具，驗證各家產品是否有能與 TeraVPN 互通。測試的結果發現所有的 VPN 產品皆能與 TeraVPN 互通。但由於時間關係，本次測試並沒有做各產品之間的互通性測試。

	Protocol support	**Encryption algorithm**	**Authentication algorithm**

	AH	ESP	DES	3DES	Others	MD5	SHA1
AboCom FW 100	Yes	Yes	Yes	Yes	No	Yes	Yes
Check Point S-box	optional	optional	optional	optional	AES (optional)	optional	optional
D-Link DFL 100	Yes	Yes	Yes	Yes	No	Yes	Yes
NetScreen-5GT	Yes	Yes	Yes	Yes	AES-128 bits	Yes	Yes
WatchGuard SOHO6tc	Yes	Yes	Yes	Yes	No	Yes	Yes
ZyXEL ZyWALL 10W	Yes	Yes	Yes	Yes	No	Yes	Yes

表九(a)、SOHO 等級防火牆/私有虛擬網路產品加密驗證規格比較表

	Keying method		IKE Authentication			IKE Misc.	
	Manual key	IKE	PSK	RSA	Others	DH group	PFS
AboCom FW 100	No	Yes	Yes	Yes	Refresh time	No	No
Check Point S-box	optional	optional	optional	No	No	No	No
D-Link DFL 100	Yes	Yes	Yes	No	No	1,2	Yes
NetScreen-5GT	Yes	Yes	Yes	Yes	DSA	1, 2, 5	Yes
WatchGuard SOHO6tc	Yes	Yes	No	No	No	No	No
ZyXEL ZyWALL 10W	Yes	Yes	Yes	No	No	1, 2	Yes

表九(b)、SOHO 等級防火牆/私有虛擬網路產品 key exchange 規格比較表

3.6 內容過濾的功能

目前的產品大都有支援內容過濾的功能，這些功能大致可分為三類：(1)過濾 HTTP requests，通常是內建一個 URL 資料庫，讓使用者勾選哪一類的網頁要求要過濾掉；或是讓使用者自行設定 URL 中的關鍵字，(2)防火牆本身不做過濾，而是把 HTTP request 或郵件導到外部的內容過濾器進行過濾，(3)過濾掉網頁中的 ActiveX, Java, cookie 等內容。各產品支援的功能如表十所指。

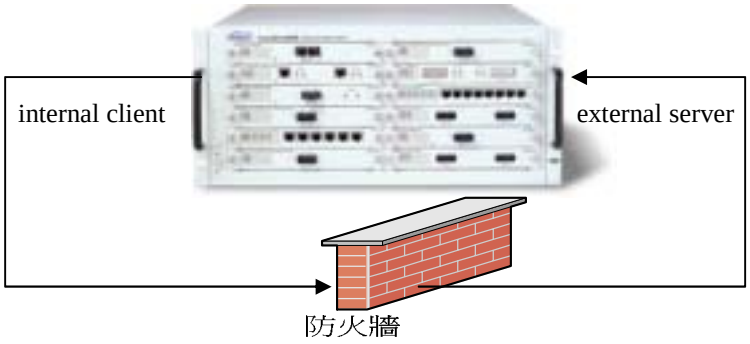
	Protocol	URL filter	Database update	Miscellaneous
AboCom FW 100	HTTP	Yes	No	ActiveX/Java/Popup/Cookie
Check Point S-box	HTTP	redirection	redirection	No

D-Link DFL 100	No	No	No	No
NetScreen-5GT	HTTP	redirection to WebSense or SurfControl, by pattern	from WebSense or SurfControl	ActiveX/Java/zip/exe
WatchGuard SOHO6tc	HTTP	Yes	Yes	Optional
ZyXEL ZyWALL 10W	HTTP	database/keyword	Yes	ActiveX/Java/cookie/web proxy

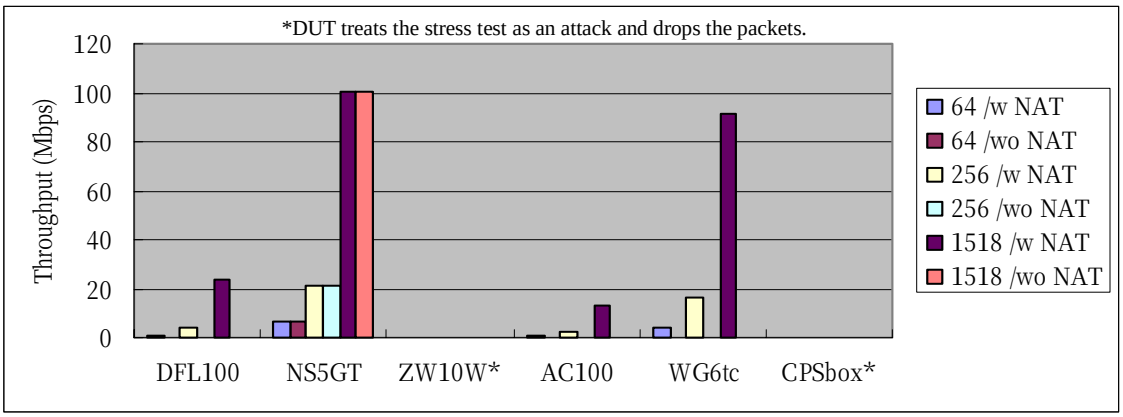
表十、SOHO 等級防火牆/私有虛擬網路產品內容過濾功能比較表

3.7 防火牆的效能

我們利用 SmartMetrics 3101A 測試設備的兩個 port 分別模擬企業內部 client 和外部的 server，如圖三的防火牆效能測試組態所示，然後使用 SmartFlow 2.2.0 由模擬 client 的 port 單向傳送 64 bytes、256 bytes、與 1518 bytes 三種大小的 raw IP 封包到達模擬 server 的 port。我們量測無封包遺失的最大輸出效能(zero-loss maximum throughput)與封包延遲(latency)兩個主要的結果。SmartFlow 會以 binary search 的方式找尋無封包遺失的最大輸出效能。我們發現防火牆的規則個數對效能的影響並不明顯，而且防火牆實際應用時的規則通常不會太多，因此我們只使用防火牆預設的規則，即封包可以從 LAN 到 WAN 通過。我們比較了(1) NAT 打開 (2) NAT 關閉兩種情形下受測設備的效能，測試結果以條狀圖表示於圖四。其中 AboCom FW 100、D-Link DFL-100、以及 WatchGuard SOHO6tc 無法關閉 NAT 功能，所以圖四只有 NAT 打開的數據。另外，ZyXEL 的 ZyWall 10W 以及 Check Point 的 S-box 在我們的測試環境下因為會把大量封包的灌入視為攻擊，經廠商試圖處理仍無法解決，故不列入數據。WatchGuard SOHO6tc 也有在一段時間後將大量封包視為攻擊的情形，因此我們藉由縮短測試時間來解決這個問題。在封包延遲時間方面，我們則使用了 10%和 100%兩種 load 進行測試。



圖三、防火牆效能測試環境

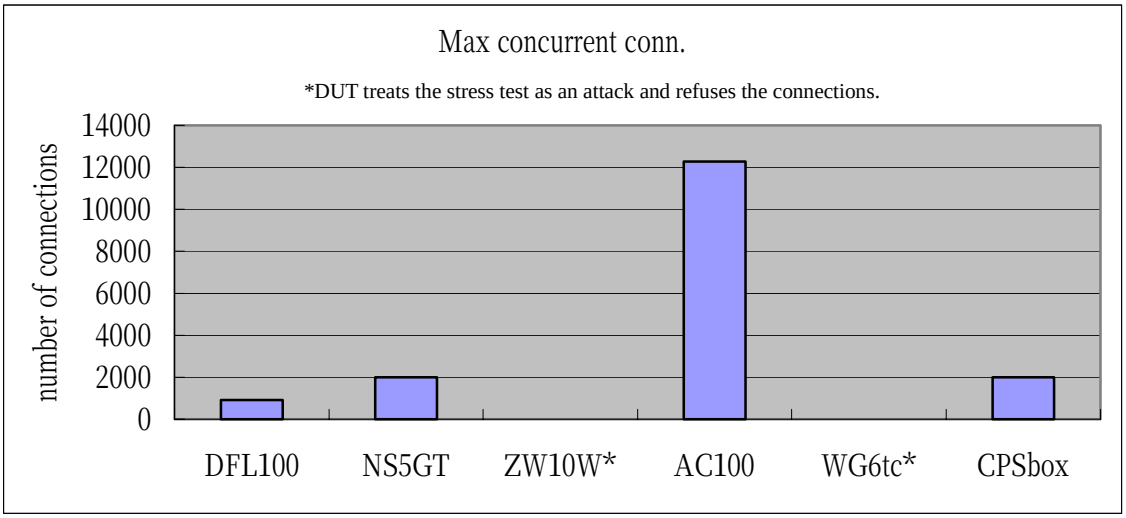


圖四、SOHO 等級防火牆/私有虛擬網路產品無封包遺失的最大輸出效能

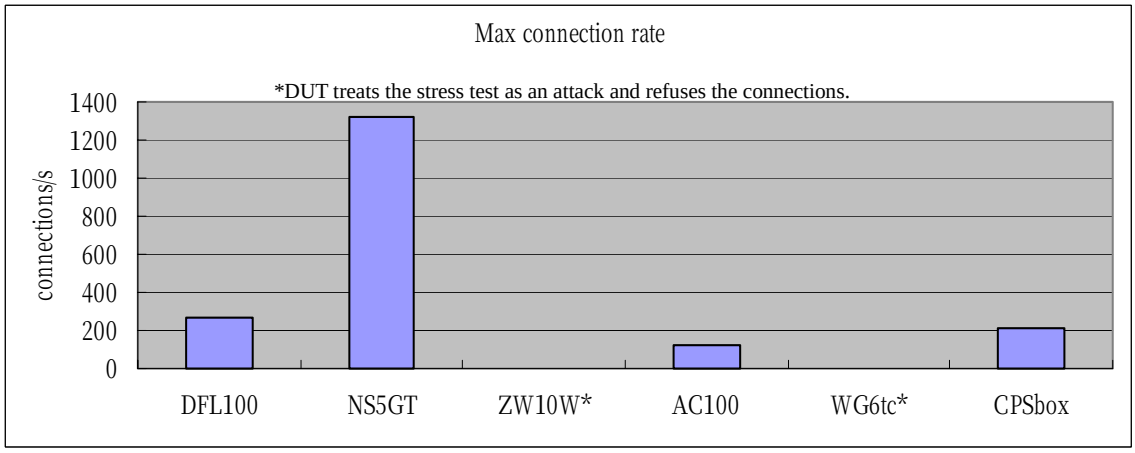
測試結果我們發現 NetScreen-5GT 的效能最佳，在最長封包 1518 bytes 時可以達到 wire speed。據推測應為其硬體較為高階之故。其次是 WatchGuard SOHO6tc。國內廠商部份則 D-Link DFL 100 表現較 AboCom FW 100 優。從延遲時間來看，也可以得到同樣的結論。在 10%的 load 及 64 bytes 的封包下，AboCom FW 100 延遲時間最長，較為奇怪；NetScreen-5GT 最短，為 12 ms。由於篇幅的關係，我們在此不將 latency 的數據列出。

接著我們測試受測物的最大同時連線個數及建立新連線的速度(connection rate)，測試環境的佈建與圖三相同。採用的測試工具為 WebSuite 2.10。首先我們先固定以一個較慢的建立新連線速度建立試圖連線，建立連線的方式為 TCP 的 3-way handshake。在遞增連線個數的情形下量測其成功建立連線的比率。我們訂定的允許錯誤率為 2%，也就是有 98%以上成功連線的前提下最大的同時連線個數，測試結果顯示於圖五。接著我們固定在最大的連線個數，開始調高建立新連線的速度，再量測在 98%以上成功連線的前提下的最大新建連線速度。最大新建連線速度的測試結果顯示於圖六。連線測試因所需時間較

長，因此在 WatchGuard SOHO6tc 上無法測得其數據，因為它會開始丟棄封包。而 Check Point 可以接受較大量的連線，因此在這邊反而可測出其數據。



圖五、SOHO 等級防火牆/私有虛擬網路產品最大同時連線個數

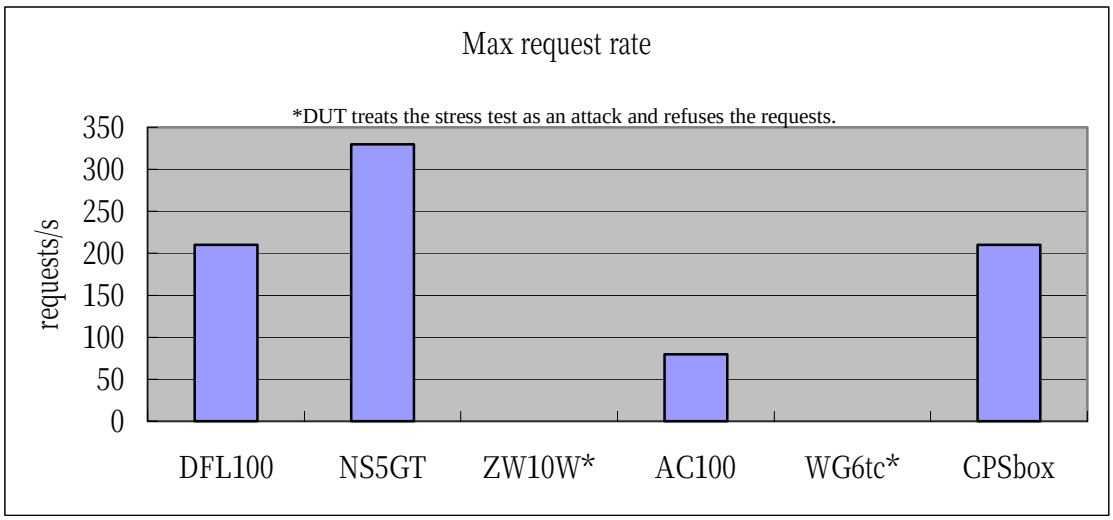


圖六、SOHO 等級防火牆/私有虛擬網路產品新建連線速率

最大的連線個數以 AboCom 的表現最佳，其次為 NetScreen-5GT 及 Check Point S-box。新增連線速度則以 NetScreen-5GT 最快。此項目各產品表現的排序與無封包遺失的最大輸出效能相仿，因此我們推測這些產品的效能應受硬體規格影響較大，而與特定功能的演算法關係較小。

我們並測量使用真正的 HTTP request 下的 request rate。由測試設備產生 HTTP request 及 response。Request 的內容為 WebSuite 預設 URI，即 http://www.spirent.com，帶有一個假的 cookie。Response 的部份則是一個 1460 bytes 的回應封包。測試結果顯示於圖七。其

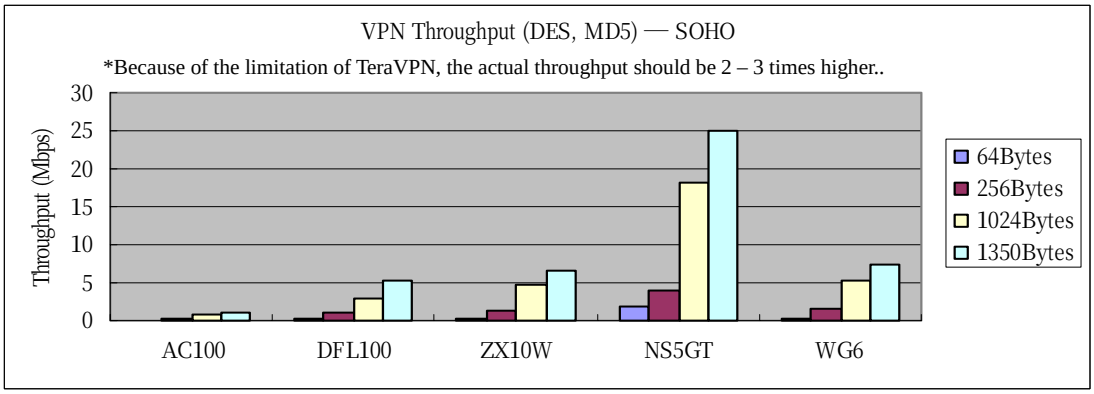
中仍為 NetScreen 表現最優，D-Link DFL-100 與 Check Point S-box 則並列第二。



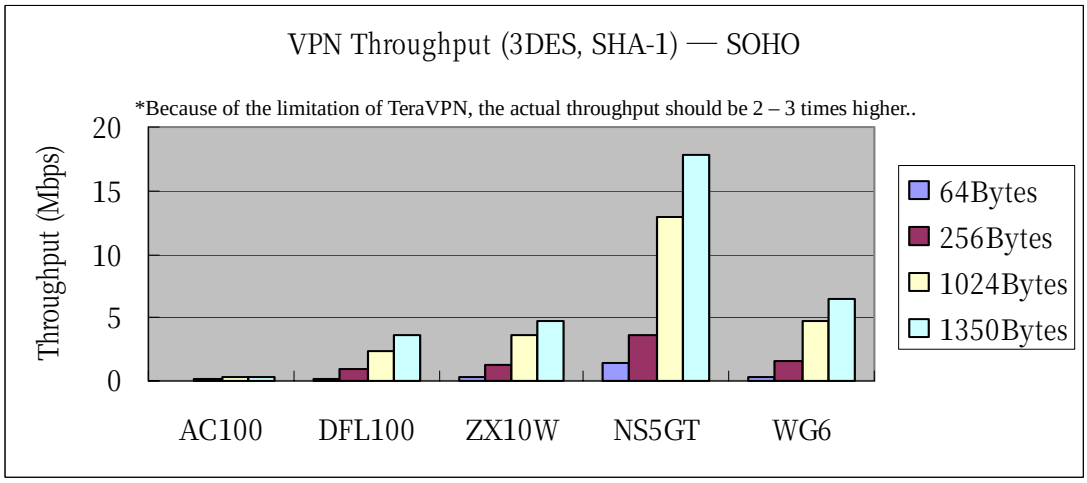
圖七、SOHO 等級防火牆/私有虛擬網路產品 HTTP request 速率

3.8 虛擬私有網路(VPN)的效能

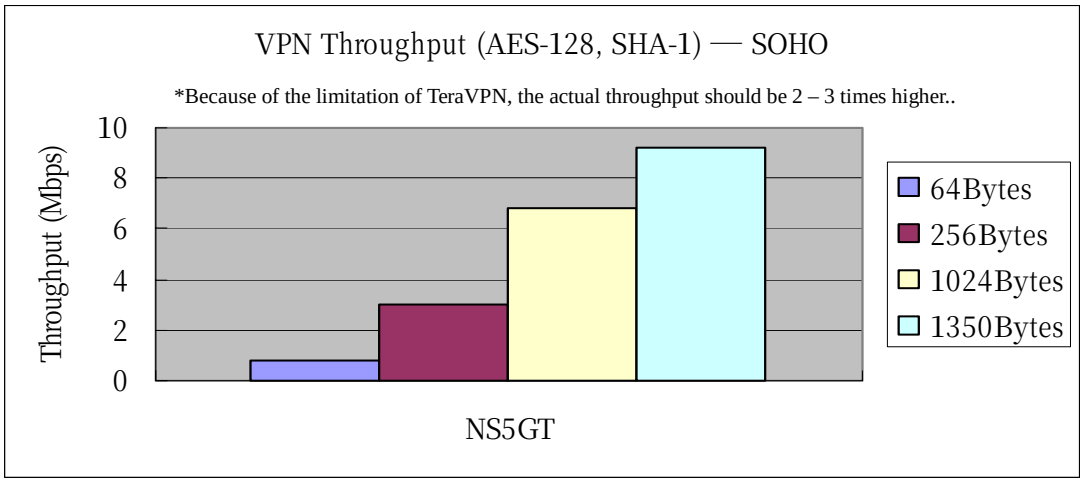
在 VPN 的效能測試方面，我們使用 Spirent TeraMetrics 3301A 附上 VPN 加速卡進行測試。原理為利用其中一塊 TeraMetrics 卡模擬一個 VPN gateway 與受測產品建立 VPN 通道相連，並測量其效能。在此項測試中，我們使用三種加密/認證測試搭配，包括 DES/MD5、3DES/SHA-1、以及 AES 128 bits/SHA-1(NetScreen 有支援)。測試結果顯示於圖八(a)、(b)、(c)三張。在這項測試當中，我們也利用兩台 DUT 互相建立 VPN tunnel 量測 performance，發現 TeraVPN 量測出來的普遍較真實情況偏低很多。因此圖八的數據僅做為各產品效能之相對參考，其數值不代表各產品的真正效能。我們並進一步建議目前在受測產品有二台以上的前提下，由這二台去建立 VPN 通道，再去測試此通道的效能會是較佳的測試方法。



圖八(a)、SOHO 等級防火牆/私有虛擬網路產品 DES/MD5 機制的效能



圖八(b)、SOHO 等級防火牆/私有虛擬網路產品 3DES/SHA1 機制的效能



圖八(c)、SOHO 等級防火牆/私有虛擬網路產品 AES-128/SHA1 機制的效能

在這個項目中，NetScreen-5GT 有最佳的表現。另外，ZyWall 10W 在這項可以測試，其效能是三項國內產品中表現最好的，據推測應與其使用硬體加速晶片有關。

3.9 其他測試 (頻寬管理精確度及其效能、內容過濾效能)

由於現在的安全性產品大都具有多項功能，因此一個有趣的問題就是當這些功能全部打開時，對整體的效能影響有多大。因時間關係，本次測試挑選 NetScreen-5GT 一台進行測試，而且也只有它支援頻寬管理功能。 當打開內容過濾功能之後，我們發現 request rate 有小幅度的下降，從原有的 330 requests/s 降至 320 requests/s。再將頻寬管理功能打開之後，其 throughput 又再略有下降，幅度較內容過濾為高。至於內容過濾功能的影響較小的原因，據推測應該是我們在這次測試中並沒有讓回應的網頁內容夾帶有要過濾的物件，使得內容過濾功能沒有對回應的網頁做進一步處理的關係。我們還針對頻寬管理功能的精確度做了個測試，將頻寬限在 30% (30 Mb/s)的範圍內，發現真實量測出來的頻寬亦相當精準，也是 30 Mb/s 上下。

4、SME/Enterprise 等級防火牆 / 虛擬私有網路產品測試

4.1 型號及規格

本次測試在 SME/Enterprise 等級共有六家廠商六項產品參與，國內及國外廠商各半。這些產品型號及功能列於表十一。

Level	Model	Firewall	VPN	IDS	Antivirus	Content filter	Bandwidth Mgmt
SME	AboCom FW 500	Yes	Yes	No	No	Yes	Yes
	Cisco PIX 515E	Yes	Yes	No	No	Yes *	No
	WatchGuard 1000	Yes	Yes	No	No	Yes	No
Enterprise	AboCom FW 1000	Yes	Yes	No	No	Yes	Yes
	Check Point NGAI	Yes	Yes	No	redirect	Yes *	No
	D-Link DFL 1500	Yes	Yes	Yes	No	Yes	Yes

*Cisco and Check Point NGAI can also redirect URL requests to WebSense.

表十一、SME/Enterprise 等級防火牆/私有虛擬網路產品功能比較表

值得一提的是，其中 D-Link DFL 1500 且有完整的 IDS 的功能，可以上網更新 signature

以及勾選 preprocessing 的動作。其他的產品，如 Check Point NGAI，也都有處理特定攻擊的能力。在我們的效能測試中，有的機器預設會自動將大量封包的流入視為攻擊而予以阻絕，如 Cisco PIX 515E 及 Check Point NGAI。內容過濾在這個等級則已經成為標準的功能，有的產品還可以另外搭配其他廠牌的內容過濾器增強過濾能力。受測物的內部及外部規格則列於表十二(a)及(b)。

Level	Model	OS	CPU	Accelerator	RAM	Flash	Hard disk
SME	AboCom FW 500	Linux	NS Geode 300 MHz	No	32 MB	8 MB	No
	Cisco PIX 515E	Cisco PIX 6.2	Intel Pentium II 433 MHz	VPN acceleration card (optional)	32 MB	16 MB	No
	WatchGuard 1000	Linux	AMD K6-2E+ 300 MHz	Yes	64 MB	8 MB	No
Enterprise	Abocom FW 1000	Linux	Intel	No	64 MB	16 MB	No
	CheckPoint NGAI	Linux	Intel Xeon 2.4 GHz (dual)	VPN acceleration card (optional)	2 GB	No	35 GB
	D-Link DFL 1500	NetOS ver 2.7	Intel Celeron 1.2 GHz	SafeNet SafeXcel 1141	256 MB	32 MB	No

表十二(a)、SME/Enterprise 等級防火牆/私有虛擬網路產品內部規格比較表

Level	Model	Interfaces	Console	high-availability port	Reset button	Size
SME	AboCom FW 500	LAN:FEx1 DMZ:FEx1 WAN:FEx1	No	No	Yes	210mm(L) x 155mm(D) x 30mm(H)
	Cisco PIX 515E	LAN:FEx1 WAN:FEx1	RJ-45	DB-15 and LAN	No	445mm(L) x 280mm(D) x 44mm(H)
	WatchGuard 1000	LAN:FEx1 WAN:FEx1 optional:FEx1	DB-9	optional	Yes	350mm(L) x 235mm(D) x 44mm(H)
Enterprise	AboCom FW 1000	LAN: FEx1 DMZ: FEx1 WAN: FEx1	DB-9	No	Yes	440mm(L)x305mm(D)x 45mm(H)
	Check Point NGAI	Total: FEx3 & GEx2	RJ-45	No	Yes	595mm(L) x 430mm(D) x 90mm(H)
	D-Link DFL 1500	LAN: FEx2 DMZ: FEx1 WAN: FEx2	DB-9	No	No	425mm(L) x 240 mm (D) x 44mm (H)

表十二(b)、SME/Enterprise 等級防火牆/私有虛擬網路產品外部規格比較表

從硬體規格來看，比較特別的是 Check Point NGAI，它事實上的純軟體的產品，但

如同其他家產品般，安裝在廠商建議規格的硬體中。

4.2 管理簡易度

表十三是受測機器管理和設定的規格比較表。在操作介面上，除了 Web 的管理介面外，Check Point 另有專屬的管理介面 Smart Client；而 WatchGuard 則是完全使用專屬的管理介面 Control Center 進行管理。Cisco PIX 515E 以及 Check Point NGAI 的操作頗為複雜，且設定較費時。

		Management Interfaces			**System Maintenance**		**Troubleshooting**	
Level	**Model**	**GUI**	**CLI**	**SNMP**	**config restore**	**firmware upgrade**	**Network statistics**	**CPU/MEM utilization**
SME	AboCom FW 500	http	telnet	Yes	Yes	Yes	Yes	No
	Cisco PIX 515E	https	telnet	Yes	Yes	Yes	Yes	Yes
	WatchGuard 1000	Control Center	No	No	Yes	Yes	Yes	Yes
Enterprise	AboCom FW 1000	http	telnet	Yes	Yes	Yes	Yes	No
	Check Point NGAI	https, Smart Client	SSH	Yes	Yes	Yes	Yes	Yes
	D-Link DFL 1500	http https	telnet SSH	Yes	Yes	Yes	Yes	Yes

表十三、SME/Enterprise 等級防火牆/私有虛擬網路產品管理與設定規格比較表

4.3 記錄檔稽核

表十四顯示在此等級的產品，其記錄檔稽核功能均相當完整，其項目說明如同 SOHO 產品，在此便不贅述。

		Logging items					**Logging functions**			
Level	**Model**	**Firewall log**	**VPN log**	**Intrusion log**	**CF log**	**Event log**	**Log to emails**	**syslog**	**Alarm mail**	**Download to file**
SME	AboCom FW 500	Yes	No	Yes	No	Yes	Yes	Yes	Yes	Yes
	Cisco PIX 515E	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	WatchGuard 1000	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Enterprise	AboCom FW 1000	Yes	No	Yes	No	Yes	Yes	Yes	Yes	Yes
	Check Point NGAI	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	D-Link DFL 1500	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

表十四、SME/Enterprise 等級防火牆/私有虛擬網路產品記錄稽核規格比較表

4.4 防火牆的功能

表十五列出防火牆基本的功能。其中 Check Point NGAI 除了基本的網路封包標頭內的欄位外，還提供了時間的選擇。也就是可以在不同的時間定義不同的防火牆規則，這點設計相同具有彈性。

		Firewall			NAT			
Level	**Model**	**Packet filter**	**Stateful inspection**	**Classifier**	**NAT(1-1)**	**NAT(M-1)**	**NAT(M-M)**	**Port forwarding**
SME	AboCom FW 500	Yes	Yes	SIP/DIP/SP/DP/protocol	Yes	Yes	Yes	Yes
	Cisco PIX 515E	Yes	Yes	SIP/DIP/SP/DP/protocol	Yes	Yes	Yes	Yes
	WatchGuard 1000	Yes	Yes	SIP/DIP/service/protocol	Yes	Yes	Yes	Yes
Enter-prise	AboCom FW 1000	Yes	Yes	SIP/DIP/service/protocol	Yes	Yes	Yes	Yes
	Check Point NG AI	Yes	Yes	SIP/DIP/service/protocol/time	Yes	Yes	Yes	Yes
	D-Link DFL 1500	Yes	Yes	SIP/DIP/service/protocol	Yes	Yes	Yes	Yes

表十五、SME/Enterprise 等級防火牆/私有虛擬網路產品防火牆/NAT 規格比較表

4.5 虛擬私有網路(VPN)的功能

在 VPN 的功能方面，結果如表十六(a)和(b)所示。在 VPN 的功能方面，所有的受測產品皆有 VPN 的功能，且支援 DES/3DES 加密方式以及 MD5/SHA-1 認證方式。其中 Check Point NGAI 還支援較新的 AES、CAST 加密方式。AboCom、Cisco、Check Point 三家產品還有實做 RSA 的 IKE 認證演算法。我們使用 TeraVPN 工具做為互通性(interoperability)測試工具。測試的結果發現所有的 VPN 產品皆能與 TeraVPN 互通。但由於時間關係，本次測試並沒有做各產品之間的互通性測試。

		Protocol support		Encryption algorithm			Authentication algorithm	
Level	**Model**	**AH**	**ESP**	**DES**	**3DES**	**Others**	**MD5**	**SHA1**
SME	AboCom FW 500	Yes	Yes	Yes	Yes	No	Yes	Yes

	Cisco PIX 515E	Yes	Yes	Yes	Yes	No	Yes	Yes
	WatchGuard 1000	Yes	Yes	Yes	Yes	No	Yes	Yes
Enterprise	AboCom FW 1000	Yes	Yes	Yes	Yes	No	Yes	Yes
	Check Point NGAI	Yes	Yes	Yes	Yes	AES, CAST	Yes	Yes
	D-Link DFL 1500	Yes	Yes	Yes	Yes	No	Yes	Yes

表十六(a)、SME/Enterprise 等級防火牆/私有虛擬網路產品加密驗證規格比較表

		Keying method		**IKE Authentication**			**IKE Misc.**	
Level	**Model**	**Manual key**	**IKE**	**PSK**	**RSA**	**Others**	**DH group**	**PFS**
SME	AboCom FW 500	No	Yes	Yes (128bits)	Yes (128bits)	Refresh time	No	No
	Cisco PIX 515E	Yes	Yes	Yes	Yes	No	1, 2, 5	Yes
	WatchGuard 1000	Yes	Yes	No	No	No	No	No
Enterprise	AboCom FW 1000	No	Yes	Yes (128bits)	Yes (128bits)	Refresh time	No	No
	Check Point NGAI	No	Yes	Yes	Yes	DSA	1, 2, 5	Yes
	D-Link DFL 1500	Yes	Yes	Yes	No	No	1, 2, 5	Yes

表十六(b)、SME/Enterprise 等級防火牆/私有虛擬網路產品 key exchange 規格比較表

4.6 內容過濾的功能

如表十七所示，目前的產品皆有支援內容過濾的功能，其中又國外以 Check Point NGAI，國內以 D-Link DFL 1500 功能支援的較多。

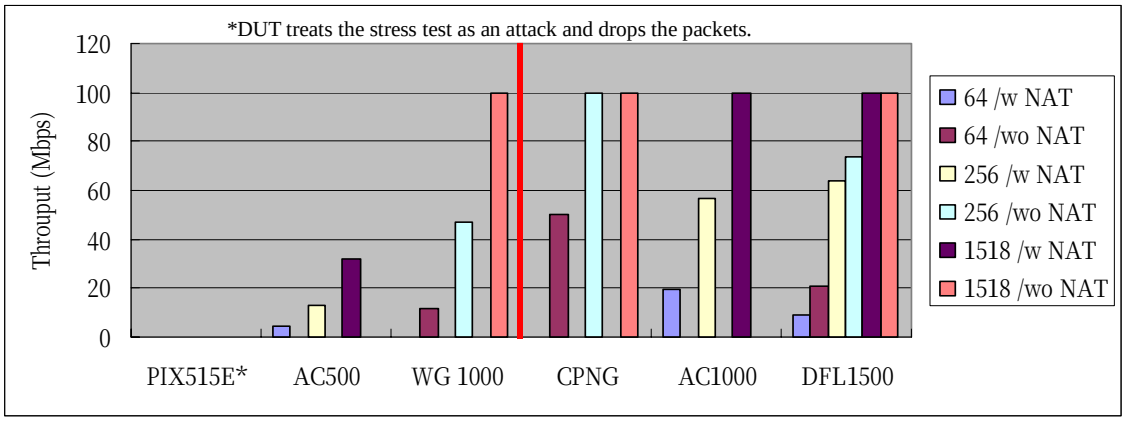
Level	**Model**	**Protocol**	**URL filter**	**Database update**	**Miscellaneous**
SME	AboCom FW 500	HTTP	Yes	No	ActiveX/Java/Popup/ Cookie
	Cisco PIX 515E	HTTP	redirection	redirection	ActiveX/Java/URL
	WatchGuard 1000	HTTP, FTP, DNS, SMTP	database, keyword	Yes	ActiveX/Java/Cookie/ Client connection/ Submission/Content type/ Unknown headers
Enterprise	AboCom FW 1000	HTTP	Yes	No	ActiveX/Java/Popup/Cookie
	Check Point NGAI	HTTP, SMTP, FTP, CIFS, peer-to-peer	user-defined database, redirection	Yes/re-direction	ActiveX/Java/JavaScript/ Script/FTP links/port strings/Virus-Scanning (redirection)

	D-Link DFL 1500	HTTP, SMTP, FTP	database/key word, file extension,	Yes	ActiveX/Java/JavaScript/ cookie/web proxy exempt zone time of day

表十七、SME/Enterprise 等級防火牆/私有虛擬網路產品內容過濾功能比較表

4.7 防火牆的效能

效能測試的方法如同 3.7 所述，這裏就不再重覆。測試結果以條狀圖表示於圖九。

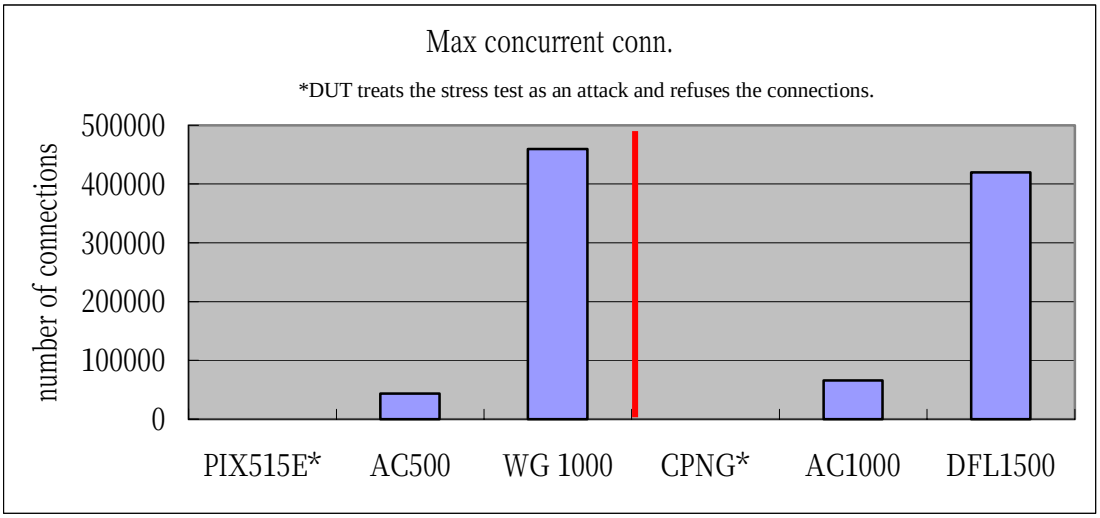


圖九、SME/Enterprise 等級防火牆/私有虛擬網路產品無封包遺失的最大輸出效能

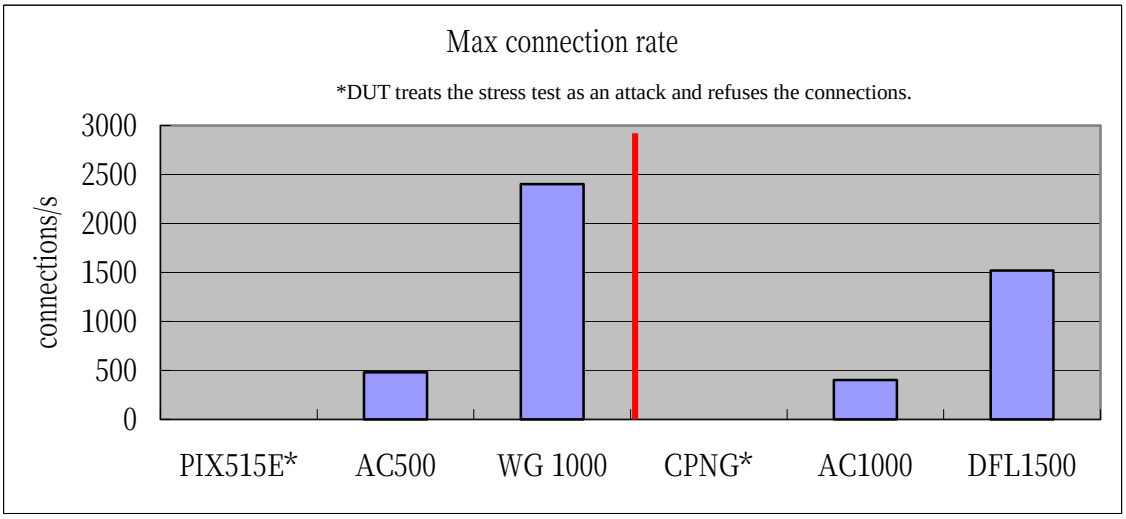
其中 AboCom FW 500 以及 AboCom FW 1000 因為無法關閉 NAT 功能，所以圖九只有 NAT 打開的數據。另外，Check Point NGAI、WatchGuard 1000 僅在沒有 NAT 的環境下可量測得數據。Cisco 則在我們的測試環境下因為會把大量封包的灌入視為攻擊，因此無法測得正確的數據，故不予列入。在封包延遲時間方面，我們則使用了 10%和 100%兩種 load 進行測試。

測試結果我們發現在 SME 等級 WatchGuard 1000 的效能最佳，在最長封包 1518 bytes 時可以達到 wire speed。在 Enterprise 等級則屬 Check Point NGAI 效能最佳。

接著我們測試受測物的最大連線個數及建立新連線的速度(connection rate)，測試環境的佈建與圖四相同，方法如同 3.7 所述。測試結果分別顯示於圖十及圖十一。其中

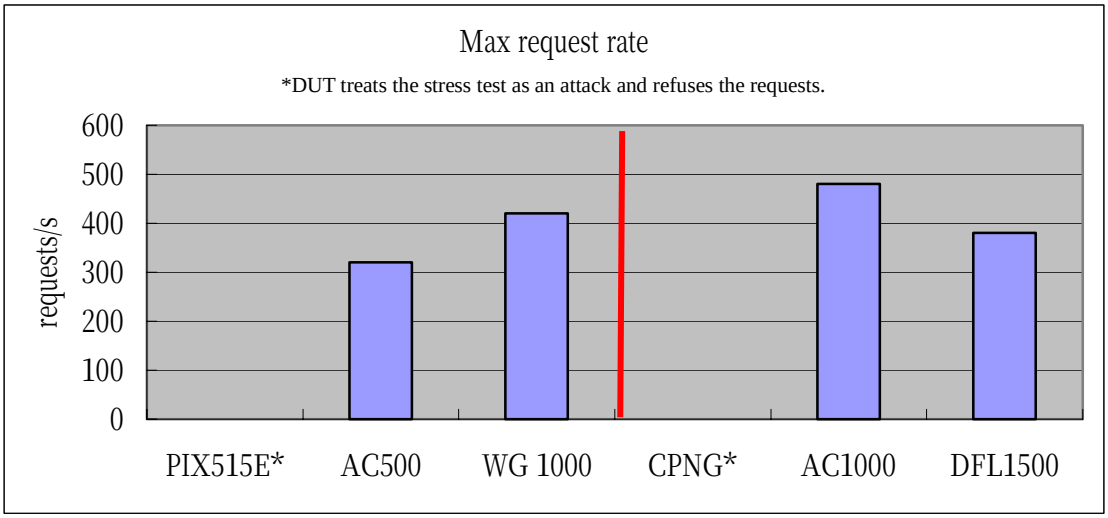


圖十、SME/Enterprise 等級防火牆/私有虛擬網路產品最大連線個數



圖十一、SME/Enterprise 等級防火牆/私有虛擬網路產品新建連線速率

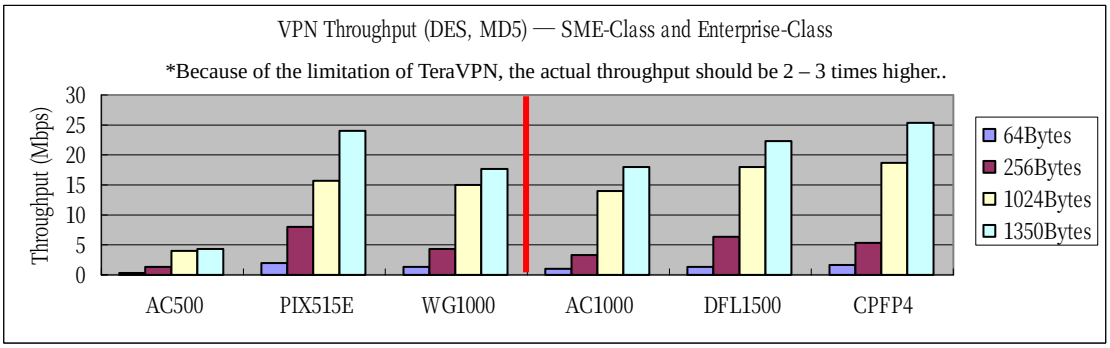
由於 Check Point NGAI 和 Cisco PIX 515E 在大量建立連線時會視為攻擊拒絕建立連線，因此圖十及十一並未列出該兩項產品的數據。在 SME 等級，最大的連線個數以及建立新連線速度以 WatchGuard 1000 的表現較佳。在 enterprise 等級，則由 D-Link DFL 1500 獲勝。圖十二 為各產品的 request rate，各產品的差距較小。在 SME 等級和 enterprise 等級則以 WatchGuard 1000 和 AboCom FW 1000 表現較佳。



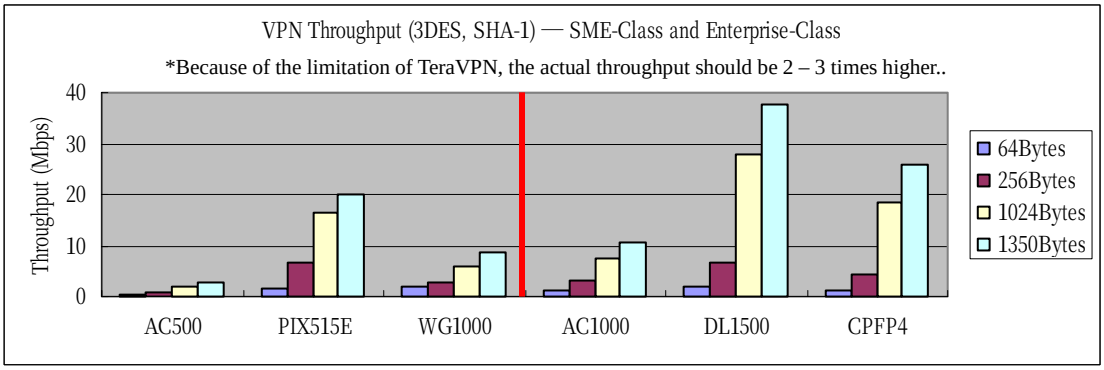
圖十二、SME/enterprise 等級防火牆/私有虛擬網路產品 HTTP request 速率

4.8 虛擬私有網路(VPN)的效能

在 VPN 的效能測試方面，測試方法如 4.8 所示。測試結果顯示於圖十三(a)、(b)二張。在這項測試當中，我們發現 TeraVPN 量測出來的普遍較真實情況偏低很多。因此圖十三的數據僅做為各產品效能之相對參考，其數值不代表各產品的真正效能。



圖十三(a)、SOHO 等級防火牆/私有虛擬網路產品 DES/MD5 機制的效能



圖十三(b)、SME/Enterprise 等級防火牆/私有虛擬網路產品 3DES/SHA1 機制的效能

在這個項目的 SME 等級中，Cisco PIX 515E 在 DES/MD5 以及 3DES/SHA1 中都有較佳的表現。而 enterprise 等級中，則分別以 Check Point NGAI 及 D-Link DFL 1500 表現較佳。

4.9 其他測試 (頻寬管理精確度及其效能、內容過濾效能)

這項我們挑選 D-Link DFL 1500 測試多合一功能對效能的影響。我們發現當 IDS 功能打開時，對系統效能影響很小，只有在 256 bytes 封包大小的測試時有從 64 Mb/s 的 throughput 下降了約 1~4 Mb/s 左右。而頻寬管理對效能的影響較大，在 256 bytes 封包大小的測試時下降了約 28 Mb/s 左右。所以可以看出頻寬管理對效能的影響較大，這點與在 SOHO 等級的 NetScreen-5GT 所做的觀察吻合。內容過濾功能打開後，則從每秒 380 requests 下降至 300 requests，影響並不大。我們也測試了 AboCom FW 500、AboCom FW 1000、Check Point NGAI、以及 D-Link DFL 1500 等四家產品對頻寬管理功能的精確度，將頻寬限在 30% (30 Mb/s)的範圍內，發現真實量測出來的頻寬亦相當精準，誤差都在 2 Mb/s 以內。

5、Carrier 等級防火牆 / 虛擬私有網路產品測試

5.1 功能面

在 carrier 等級這次只有 NetScreen-5200 參加。因此我們只列出該產品的規格及測試數據，但不做最後的評比。相關規格請見表十八(a)、(b)。其餘未列出的規格除 NetScreen-5200 頻寬管理的功能為可支援 DiffServ 及可設定最大頻寬外，與 NetScreen-5GT 皆相同。

	OS	CPU	Accelerator	RAM	Flash	Hard disk
NetScreen-5200	ScreenOS ver 4.0.0	PowerPC 600 MHz	GigaScreen ASIC	1 GB	32 MB	No

表十八(a)、NetScreen-5200 內部規格比較表

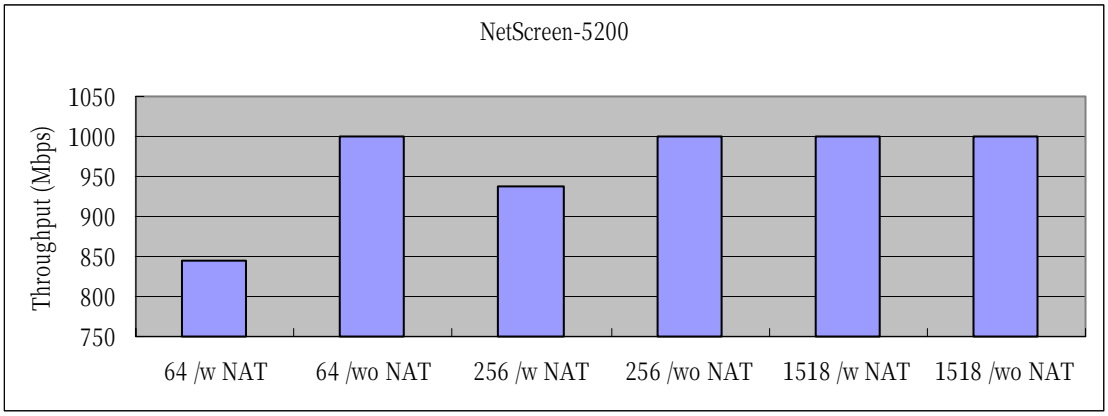
	Interfaces	Console	high-availability port	Reset button	Size
NetScreen-5200	Total: GEx8 or GEx2+FEx24	RJ-45	GE x2	None	445mm(L) x 495mm (D) x 85mm(H)

表十八(b)、NetScreen-5200 外部規格比較表

5.2 效能面

NetScreen-5200 擁有 8 個 Gigabit port。在效能測試方面如同前面的測試方法，我們利用 TeraMetrics Gigabit 模擬一個 client 經由 LAN port 單向送到 WAN port 上的 server 的情形。量得無封包遺失的最大輸出效能顯示於圖十四。在沒有打開 NAT 的前提下，NetScreen-5200 可以達到 1 Gb/s 的 wire speed，即使在打開 NAT 的情形其效能也逼近 wire speed，較去年測試報告中 carrier 等級的任何產品效能更佳。

在最大的 TCP 連線速度以及 HTTP request rate 方面，NetScreen-5200 的表現極優。最大的連線速度為每秒可建 67,000 個 TCP connections，而 request rate 則為每秒 15,000 個 request。最多同時連線個數方面，礙於測試工具的限制，我們只能測到 500,000 個連結。而據 NetScreen 台灣分公司表示，該款產品的最大連結個數可以高達一百萬個。在 VPN 互通性方面，NetScreen-5200 可以成功地與 TeraVPN 互通。



圖十四、NetScreen-5200 無封包遺失的最大輸出效能

6、防火牆 / 虛擬私有網路產品觀察與總結

在本次測試之後，我們對市面上的防火牆以及虛擬私有網路產品有下列幾點觀察：

1. 本次測試的防火牆幾乎都整合了虛擬私有網路以及複雜度不等的內容過濾功能。部分產品還整合了頻寬管理的能力。但是在入侵偵測的方面除 D-Link DFL 1500 之外，皆沒有完整的入侵偵測能力，只能對特定的攻擊做出反應。在防毒方面則只有 Check Point 的產品有 redirect 郵件到防毒系統的能力。
2. 大部分的產品都有若干防止入侵的能力。其中有些產品的預設值更是會直接擋掉大量

封包或連線的流入或流出，且不容易甚至無法關閉這樣的功能。我們在做 stress test 的時候便遇到這樣的困難。有些產品則可以設定 SYN flooding 的 threshold，或是讓使用者勾選要處理哪些類的攻擊。

3. 在這次測試中，我們首度看到防火牆產品有支援無線區域網路介面及 IEEE 802.1X 等功能。對日漸普及的無線網路環境來說，這樣的設計提供了不少便利。
4. 防火牆的效能會因為更多的功能同時打開而使得整體的效能下降。我們測試中發現會讓效能下降的功能依下降幅度大小排序依序是頻寬管理、內容過濾、以及入侵偵測。
5. VPN 的測試仍然有若干的困難存在。我們原先希望能夠測試一台 VPN 產品能夠建立的最大 tunnel 個數，然後 tunnel 的建立仍需仰賴人工對每個 tunnel 的參數逐一設定。這對有些宣稱可支援上千或上萬個 tunnel 的產品，驗證的工作將極為煩瑣，甚至難以做到。此外，TeraVPN 所量測得的數據仍然較真實情況偏低很多。使得實際效能的測試仍需仰賴在兩台受測機器建立 tunnel。這對如這次般公開測試而言，機器的調度會是一個困難。
6. 目前防火牆的 throughput 在 SOHO 等級國內產品大都未達到 wire speed。即使是最長封包也只有達到 23 Mb/s。在 enterprise 等級且用最長的封包測試下才有 wire speed 的表現。而同樣在 SOHO 等級國外的產品，如 NetScreen-5GT 或 WatchGuard SOHO6tc 在最長封包下就已經有達到或接近 wire speed 的表現了。一般來說，國外產品的效能面還是較優於國內產品。

7、入侵偵測系統產品測試

7.1 型號及規格

本次入侵偵測系統測試涵蓋三家廠商五項產品，同時我們也拿 open source 入侵偵測系統 Snort 2.0 對照，看看 open source 套件相對於這些商業產品其功能和效能又如何。這些產品都是以硬體形式銷售。表十九為各產品之內部規格比較表。其中比較值得注意的是，相對於一般的防火牆規格，入侵偵測系統使用的 CPU 都高檔許多，記憶體也都有 1 GB。畢竟，入侵特徵(signature)的偵測比對比起防火牆規則比對複雜許多。在相同的流量

而處理的時間增長的情形下，需要更大的記憶體來儲存更多等待處理的封包是必須的。

	OS	CPU	RAM	Interface	Console	Recovery
NetScreen-IDP 100	Linux	PIII 1133 MHz	1 GB	FEx2 GEx2	Yes	from CD
Intrusion SecureNet5545	Linux	PIII 1GHz	500 MB	FEx3	Yes	from CD
Intrusion SecureNet7145	Linux	2 * PIII 1.4 GHz	1 GB	FEx2 GEx1	Yes	from CD
ISS RealSecure Gigabit Sensor	Windows 2000	PIII 866 MHz	1 GB	FEx2 GEx1	Yes	from CD
ISS Proventia A201	Linux	Xeon 1.8 GHz	1 GB	FEx2	Yes	from CD
Snort	Linux	PIII 1GHz	128 MB	FEx1	No	N/A

表十九、入侵偵測系統產品規格比較表

7.2 入侵偵測功能

表二十為入侵偵測系統偵測及處理方式的比較表。我們看到特徵的個數的範圍大致落在 1000-3000 之間，相對於一般防毒系統中病毒碼或是內容過濾器的 URL list 的個數(見本文後面的數據)，這個值顯然小了很多。另外值得注意的是，這些產品當中只有 NetScreen-IDP 100 可以採用 in-line 的方式偵測入侵。所謂 in-line 的模式指的是入侵偵測系統位於封包行經的路徑上，因此當發現有入侵的訊息時，可以及時阻斷封包的路徑而阻止入侵。但缺點是因為比對入侵特徵的時間較久，如果效能不夠好的話可能會成為網路的瓶頸。此外，如果有誤判的情形出現，就會阻擋到不該阻擋的封包。NetScreen-IDP 100 的處理方式是增設 policy 來避免誤判。而被動式的模式指的是藉由監聽封包的技巧來找尋可能的入侵特徵，雖然仍然可以透過 RST 等封包切斷 TCP 連線，但是是否能及時阻擋攻擊封包以及 UDP 封包無法處理，是被動式監聽的缺點。雖然被動式的方式可能因網路流量過大而無法及時偵測到攻擊，但是並不會形成網路的瓶頸。另外即使有誤判發生，也只是多了不該出現的警告(alert)，而不會阻擋到不該擋的封包。

對 signature 劃分等級的好處是可以協助管理人員在大量的警告訊息當中很快的注意到重要的警告。但值得注意的是，雖然 Snort 的規則定義中有優先權的選項，但預設的規則定義中卻沒有任何一條有被定義優先權。

	Signatures	Detect mode	Signature priority	Action
NetScreen-IDP 100	2000+	In-line & Passive	Critical, high, medium, low, informational	Ignore, drop packet, drop connection, close client & server, log, alarm, send mail, run script
Intrusion SecureNet5545	1800	Passive	High, medium, low	Text log, tcp dump, binary log, tcp reset
Intrusion SecureNet7145	1800	Passive	High, medium, low	Text log, tcp dump, binary log, tcp reset
ISS RealSecure Gigabit Sensor	1400	Passive	High, medium, low	Rskill(RST), log db, log evidence, view session, email, snmp, opsec
ISS Proventia A201	1400	Passive	High, medium, low	Rskill(RST), log db, log evidence, view session, email, snmp, opsec
Snort	1821	Passive	priority number	Pass, log, alert, dynamic, activate

表二十、入侵偵測系統產品偵測功能比較表

7.3 管理功能

表二十一所列為管理功能的比較表。相對於防火牆大都採用 Web 介面的管理，表中的產品都是採用專屬的 Windows 程式管理。而 Snort 本身雖然沒有專屬的管理的套件，但是有相關的工具，例如 SnortSnarf 可以幫忙整理 log。

	Interface	Update	Traffic statistics	CPU/MEM utilization
NetScreen-IDP 100	Windows/Linux program	Yes	Partial (for anomaly detection)	Yes
Intrusion SecureNet5545	Windows program	Yes	No	Yes
Intrusion SecureNet7145	Windows program	Yes	No	Yes
ISS RealSecure Gigabit Sensor	Windows program	Yes	Yes	No
ISS Proventia A201	Windows program	Yes	Yes	No
Snort	Third-party tools	Yes	No	No

表二十一、入侵偵測系統產品管理功能比較表

7.4 攻擊測試

我們利用 nessus 弱點掃描程式產生八種新型攻擊，藉以測試 IDS 系統是否能正確偵測出該項攻擊，攻擊的項目及測試的結果如表二十二和表二十三所示。

弱點編號	攻擊名稱
CVE-2001-0507	IIS Remote Command Execution

CAN-2002-1123	Microsoft's SQL Hello Overflow
CAN-2002-1337	Sendmail remote header buffer overflow
CAN-2003-0161	Sendmail buffer overflow due to type conversion
CAN-2003-0086	Samba Fragment Reassembly Overflow
CVE-2000-0573	wu-ftpd SITE EXEC vulnerability
CVE-2001-0872	OpenSSH UseLogin Environment Variables
CVE-2002-0083	OpenSSH Channel Code Off by 1

表二十二、測試的攻擊項目

	IIS-attack	**MS-SQL-attack**	**Sendmail-attack 1**	**Sendma-attack 2**	**Samba-attack**	**Wu-ftpd-attack**	**OpenSSH-attack 1**	**OpenSSH-attack 2**
NetScreen-IDP 100	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Intrusion SecureNet 5545	Yes	Yes	Yes	Yes	Yes	Yes	*Yes	*Yes
Intrusion SecureNet 7145	Yes	Yes	Yes	Yes	Yes	Yes	*Yes	*Yes
ISS RealSecure Gigabit Sensor	Yes	*Yes	Yes	Yes	Yes	Yes	Yes	Yes
ISS Proventia A201	Yes	*Yes	Yes	Yes	Yes	Yes	Yes	Yes
Snort 2.0	No	No	No	No	Yes	Yes	No	No

*detected after updating signatures

表二十三、攻擊偵測結果

從表二十三來看，各家 IDS 對新型攻擊特徵的偵測能力均相當良好，我們所驗證的八項攻擊幾乎都被偵測到。其中 Intrusion 與 ISS 的系統分別是在更新 signature 之後才偵測到 OpenSSH 及 MS-SQL 的攻擊。Snort 的表現不盡理想，但是我們發現一些攻擊，如 IIS attack，確實有定義在 Snort 的規則中。至於為何無法偵測到需要做進一步詳查。

7.5 攻擊測試

入侵者為了避免 IDS 發現攻擊特徵，會採取各種的迴避(evasion)措施使得 IDS 無法正確配對到攻擊特徵。我們利用 fragrouter 封包切割工具分別產生 8/16/24 bytes 的 IP fragment，以及 1 或 2 bytes 的 TCP fragment。藉以驗證這些 IDS 產品是否仍然能正確的發現有攻擊產生。測試的結果發現在切割成 2 bytes 的 TCP fragment 的時候，Intrusion SecureNet

無法正確偵測出 MS-SQL 的攻擊，而在切割成 1 byte 的 TCP fragment 時，NetScreen-IDP 100 也無法偵測 MS-SQL 的攻擊，在這兩種情形下，Snort 都無法偵測 Samba attack。另外，我們也利用的 nikto 來模擬九項 URL 的 evasion 技巧(見表二十四)，發現所有產品包括 Snort 在內皆能處理 URL evasion 的問題。

URL encoding
Self-reference
Premature URL ending
Prepend long random string
Fake parameter
TAB as request space
Random case sensitivity
Windows directory separator
Session splicing

表二十四、nikto 的九項攻擊模式

7.6 攻擊測試

我們利用 Avalanche 模擬 250 至 1000 個使用者同時上網的流量，並發送攻擊封包，看看受測的 IDS 在大量的流量時，是否還能發現攻擊的封包。經過我們的測試之後，發現在 1000 個使用者的流量下(約 80 Mb/s)，各 IDS 系統仍然能夠正確的偵測到攻擊特徵。因此我們推論這些系統能正確偵測攻擊特徵的流量應該都在 100 Mb/s 以上。這點需要使用 Gigabit 等級的 Ethernet tap 以及 Avalanche 上也要有 Gigabit port 才能對這些 Passive 模式的 IDS 做進一步的效能驗證。

7.7 誤判測試

在需要建立 TCP 連線的攻擊型態中，如果一個封包只是帶有攻擊特徵，但是並沒有真正的去建立 TCP 連線，是不會對被攻擊的主機造成真正的入侵。如果 IDS 系統只是單單去檢查是否有攻擊特徵，而忽視是否真正有建立 TCP 連線，就會造成大量的警告(alert)被記錄下來。入侵者便可以利用這一點，大量發送帶有攻擊型態的封包，讓 IDS 留下大量的警告記錄，而讓真正的攻擊隱藏在這些假的攻擊記錄中而被忽視。

我們使用 snot 做為產生假攻擊的工具，發現除了 Snort 及 NetScreen-IDP 100 之外，其餘的 IDS 產品皆對假攻擊有反應，且視為 Denial of Service 類的攻擊。因此會遭遇前段描述的問題。我們推測或許是因為效能的考量，或是政策上仍然希望知道有這樣的假攻擊，

而使得這些產品在實做上仍然會對假攻擊產生警告。

7.8 觀察與總結

在本次測試之後，我們對市面上的入侵偵測系統產品有下列幾點觀察：

1. 單是偵測入侵已經無法及時阻止內部網路受害，及時的防禦變成是一個重要的課題。即使是被動式的偵測，也都有提供 RST 的方式阻斷 TCP 連線。而 NetScreen-IDP 100，以及 ISS 新的產品如 RealSecure Guard，或是 TopLayer 的產品(未於本次測試)，皆提供 in-line 的偵測模式，可即時阻絕攻擊。
2. 提供處理 evasion 的機制已經變成 IDS 產品標準的功能。在這次測試中，我們看到各項產品對我們測試的 evasion 幾乎都能正確的處理。我們這次測試的都屬於新的攻擊型態，各產品更新攻擊特徵的頻率也快到能處理這些新的攻擊。
3. 除了 Snort 及 NetScreen-IDP 100 之外，其餘產品都會對沒有真正建立 TCP 連線而只有帶有攻擊特徵的封包有反應，可能會造成大量的警告而混淆真正的攻擊。可能是基於政策或效能考量而做這樣的設計。
4. 在 80 Mb/s 左右的背景流量下，各產品仍然可以正確的偵測到攻擊，顯示偵測率並沒有在這個範圍的流量下受到影響。
5. 要能將 IDS 設定到正確的偵測攻擊而沒有誤判或漏判仍然不是一件簡單的事。需要對整個 IDS 系統的各項設定以及自身的網路有相當清楚的了解。而不像部分防火牆系統可以只具備基礎的網路知識就可完成設定。

8、防毒系統產品測試

8.1 型號及規格

在本項測試中，我們檢視了市面上三款網路防毒系統。這些系統都是以軟體產品，唯桓基科技送測機器時已事先將系統安裝在他們提供的 PC 上，其核心的掃毒引擎是採用 Sophos 的系統。本次參與測試的產品其功能規格列於表二十五。在表二十六中，我們檢查了十八種檔案壓縮格式，看看這些產品是否正確的偵測出壓縮檔內部的病毒碼。壓縮格式及支援狀況如表所示。其中 recursive compression 指的是壓縮後再壓縮的檔案。值得注

意的是，不同於 IDS 攻擊特徵的是，病毒碼特徵的個數遠超過一般攻擊特徵的個數，介於 60,000 至 80,000 之間。如果一個電子郵件夾帶有兩個以上的病毒檔案時，這三套系統也能夠正確的都找出來。

	Protocols Supported	Compression Format Supported	Support for Recursive Compressed File	E-mail : Multipart Attachment Scanning/Action	FTP : Active/Passive Mode Supported	FTP : Multibyte Charset Supported	Virus Action Supported	Number of virus signatures
Trend InterScanVirusWall Evaluation	SMTP, FTP, HTTP	11/18	YES	YES	YES	YES	Pass, Move,Delete, Clean	68,894
Panda PerimeterScan for Sendmail	SMTP	11/18	YES	YES	N/A	N/A	Clean, Move,Delete, Rename, Ignore	65, 849
HGiga Virusherlock	SMTP, POP3	7/18	YES	YES	N/A	N/A	Pass,Move, Delete,Clean	82, 908

表二十五、防毒系統功能比較表

Compression format	Trend InterScan VirusWall	Panda PerimeterScan	HGiga Virusherlock
PKZIP(.ZIP)	Yes	Yes	Yes
PKZIP(.exe)	No	No	No
LHA(.LZH)	Yes	Yes	No
LHA(.exe)	Yes	Yes	No
RAR(.RAR)	No	No	No
RAR(.exe)	No	No	No
ARJ(.ARJ)	Yes	Yes	Yes
ARJ(.exe)	No	No	No
TAR(.tar)	Yes	Yes	Yes
TAR/GZ(.tgz)	Yes	Yes	Yes
GZIP(.gz)	Yes	Yes	Yes
UNIX(.Z)	Yes	*Yes	Yes
BZIP(.bz)	No	No	No
BZIP2(.bz2)	Yes	*Yes	No
Uuencode(.UUE)	Yes	Yes	Yes
Base64(.B64)	No	No	No
ACE(.ACE)	No	No	No
MS(.XXX_)	Yes	*Yes	No

*表示有掃到病毒但沒有如設定的方式處理病毒

表二十六、防毒系統壓縮格式支援比較表

8.2 管理功能

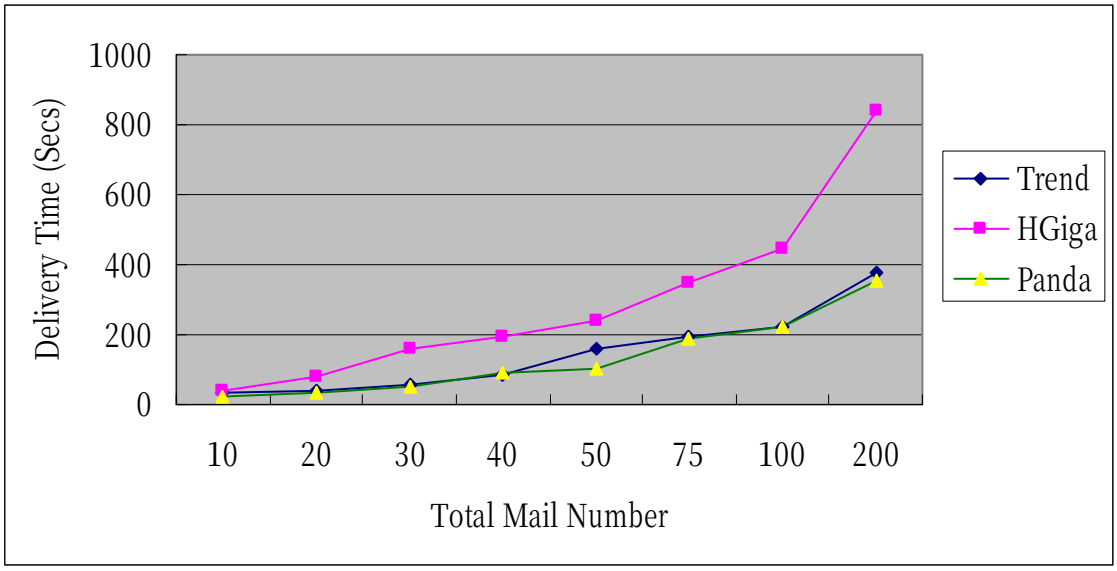
表二十七為這三樣產品的管理功能比較表。當這三樣產品發現有病毒時，都是以 Email 的方式通知使用者的，也都可以定期安排時間自動去更新病毒的 signature。其中管理介面以桓基科技的 Virusherlock 功能最多樣化，也方便使用。此外，趨勢科技的 InterScan VirusWall 支援較多的郵件檔案輸入方式。例如可以與 Check Point 的防火牆搭配，透過 CVP(Content Vectoring Protocol)或 CSP(Content Scanning Protocol)等方式將郵件 redirect 到趨勢的防毒系統掃毒。

	Notification Methods	Configuration Interfaces	Scheduled Signature Update	Integrated Methods	User Interface and Options	Centralized Management	Product Type	Machine Specification
Trend InterScan VirusWall	E-Mail	Window, Web	YES	Mail Relay Proxy, CVP,CSP	Normal	YES	Program	PIII 1G, 256MB RAM
Panda PerimeterScan	E-Mail	Web	YES	Mail Relay	Simple	YES	Program	PIII 1G, 256MB RAM
HGiga Virusherlock	E-Mail	Web	YES	Mail Relay	Beautiful and Versatile	NO	Appliance	P4 2.4G, 1280 MB RAM

表二十七、防毒系統管理功能比較表

8.2 效能

我們試著發送 10 到 200 封郵件，其中每封郵件皆帶有一個 1 MB 的附檔。我們檢查系統從第一封郵件進入到最後一封郵件處理完畢的時間。值得注意的是，這段時間包括除了掃毒的時間以外，還包括處理郵件的時間。測試的結果如圖十五。以 200 封郵件每封有 1 MB (8 Mb)，deliver 的時間為 400 秒計算，實際上每秒約有 4 Mb/s 的 throughput。



圖十五、處理信件所需的時間

8.3 觀察與總結

在本次測試之後，我們對市面上的防毒系統產品有下列幾點觀察：

1. 電子郵件仍然是病毒重要的傳播途徑，因此電子郵件本身，是掃毒的重要對象。這三樣當中，只有趨勢科技的 InterScan VirusWall 有另外支援 FTP 及 HTTP 的掃毒。
2. 儘管常見的病毒約莫只有數千個而已，但是病毒碼的個數卻都高達數萬個。
3. 支援壓縮的格式約有 7 到 11 個之間。
4. 目前防火牆產品中，有支援防毒功能的還不多。因此與防火牆廠商合作，將郵件流量導至防毒系統中掃毒。
5. 可以搭配阻擋垃圾郵件(anti-spam)的功能兩者一起使用。這次的產品中，桓基科技的產品同時就具備有 anti-spam 的功能，但此功能不列於本次測試當中。

9、內容過濾器測試

9.1 型號及規格

為了防止員工在工作時間存取與工作無關的網頁內容，或阻止學生或未成年人瀏覽色情網站，內容過濾器可以分析網頁存取的要求(request)或內容(response)，用以決定該要求或內容是否符合恰當。在本次測試中，我們比較了四家產品，其中亞盛科技的 AscenGate，以及 SurfControl 的 Web Filter 是安裝在 PC 中一起銷售，而文佳科技在這次則

是以軟體的方式提供光碟片給我們安裝測試。雖然安裝的平台記憶體較小，但對效能影響並不大。WebSense 的產品則是以純軟體的方式在銷售。我們將實際上這些系統安裝的平台列於表二十八。

	OS	CPU	RAM
AscenVision AscenGate 2000	Linux	INTEL P4 2.4 GHz	1 GB
文佳科技 防堵色情闡道系統	Linux	INTEL PIII 1 GHz	256 MB
SurfControl Web Filter	Windows 2000 Advance Server	INTEL PIII 800 MHz	1.2 GB
WebSense Enterprise v5	Windows 2000 Advance Server	AMD Athlon 1.6GHz (dual)	1 GB

表二十八、內容過濾器安裝平台比較表

9.2 管理功能

各產品管理的功能列於表二十九。

	GUI	CLI	Config/System Backup	Database Update	GUI Support Language
AscenVision AscenGate 2000	HTTP	telnet	No	Yes	3 種 (英文、繁/簡體中文)
文佳科技 防堵色情闡道系統	HTTPS	N/A	Yes	Yes	1 種（中文）
SurfControl Web Filter	Windows program	N/A	Yes	Yes	1 種（英文）
WebSense Enterprise v5	HTTP/Windows program	N/A	No	Yes	7 種

表二十九、內容過濾器安裝管理功能比較表

9.3 過濾功能

內容過濾器各產品過濾功能則列於表三十。目前各內容過濾器過濾的方式都是透過將 URL 與一個大型的 URL list 資料庫進行比對，以驗證是否該阻擋或監視該要求。或是可以讓使用者指定關鍵字，在要求中尋找該關鍵字進行阻擋或是監視。這些產品除了文佳科技的產品外只有賭博與色情兩類，其他的產品對網頁的分類種類在 30 到 80+之間，URL 資料庫裏面 URL 的個數約在三百萬到五百萬之間，其個數是在入侵偵測系統、防毒

系統、內容過濾器三者之間最多的。除了亞盛科技 AscenGate 2000 的 URL 是採用另一家公司 SmartFilter 的資料庫之外，其餘產品的資料庫都是由廠商自行維護。

	Block Method	Block Type	Monitoring Type	Categories	Number of URLs	URL maintainer
AscenVision AscenGate 2000	URL	Users/IP, Web page	Users/IP, URL, Keyword	30	3,700,000	From SmartFilter
文佳科技 防堵色情閘道系統	URL, Keyword (in content)	Users/IP, Web page	Users/IP	2	400,000	文佳科技
SurfControl Web Filter	URL, Keyword (in URL)	User Definition （File, Protocol, Port）	Users/IP, URL, Protocol	40	4,000,000	SurfControl
WebSense Enterprise v5	URL	User Definition （File, Protocol, Port）	Users/IP, URL, Protocol, Categories	80+	5,000,000	WebSense

表三十、內容過濾器過濾功能比較表

9.4 額外功能

表三十一為內容過濾器額外功能的比較表。這裏可以看出使用者階可以自行定義 URL 及關鍵字。另一方面也可以設定對某些 IP 位址或是在某個時段來實施內容過濾。除了文佳科技的系統外，其餘的產品也提供了頻寬管理的功能。

	User URL Definition	User Keyword Definition	IP Mgt.	Time Mgt.	Bandwidth Mgt.
AscenVision AscenGate 2000	Yes (configured from console only)	Yes (log only)	Yes	Yes	Yes
文佳科技 防堵色情閘道系統	Yes	Yes (within content)	Yes	Yes	No
SurfControl Web Filter	Yes	Yes (URL block)	Yes	Yes	Yes
WebSense Enterprise v5	Yes	Yes (URL block)	Yes	Yes	Yes

表三十一、內容過濾器額外功能比較表

9.5 監看與記錄

表三十二為各產品監看與記錄的功能比較表。目前除了文佳科技的產品外，其他的產品也都有即時監看使用者正在看哪個網頁的功能。提供報告的種類亦相當豐富，除了文佳科技的產品外都有數十種之多。

	Real-Time Monitoring	Notification Method	Report Categories	Reporting Format	System Logs
AscenVision AscenGate 2000	Yes	Mail	28	1 （HTML）	Yes
文佳科技 防堵色情閘道系統	No	N/A	2	1 （HTML）	Yes
SurfControl Web Filter	Yes	Mail	55	14 （PDF、HTML、MS Word..）	Yes
WebSense Enterprise v5	Yes	Mail	80	1 (proprietary format）	Yes

表三十二、內容過濾器監看及記錄功能比較表

9.6 色情網站阻擋準確度

我們任意挑選國內以及國外各 250 個色情網站，並測試各家阻擋的準確度，測試結果列於表三十三。其中在國內外色情網站的阻擋率以 SurfControl 的產品最高。原先文佳科技的產品阻擋率大約只有 50.6%左右，後來在他們提供最新的 URL 資料庫之後，阻擋的準確度大幅提升至 90%以上。雖然他們產品的 URL list 在各家比起來算少，但是仍然可以達到很高的阻擋率應該是他們的 URL 資料庫是最新的關係。由此可見，資料庫更新的頻率跟其內 URL list 的個數對準確率同樣重要。

	500 個色情網站阻擋率（國內 250／國外 250）		準確度
AscenVision AscenGate 2000	國內（158/250）	63.2%	63.0%
	國外（157/250）	62.8%	
文佳科技 防堵色情閘道系統	國內（233/250）(193/250)	93.2%(77.2%)	93.0% (50.6%)
	國外（232/250）(60/250)	92.8%(24%)	
SurfControl Web Filter	國內（204/250）	81.6%	89.6%
	國外（244/250）	97.6%	
WebSense Enterprise v5	國內（155/250）	62%	76.6%
	國外（228/250）	91.2%	

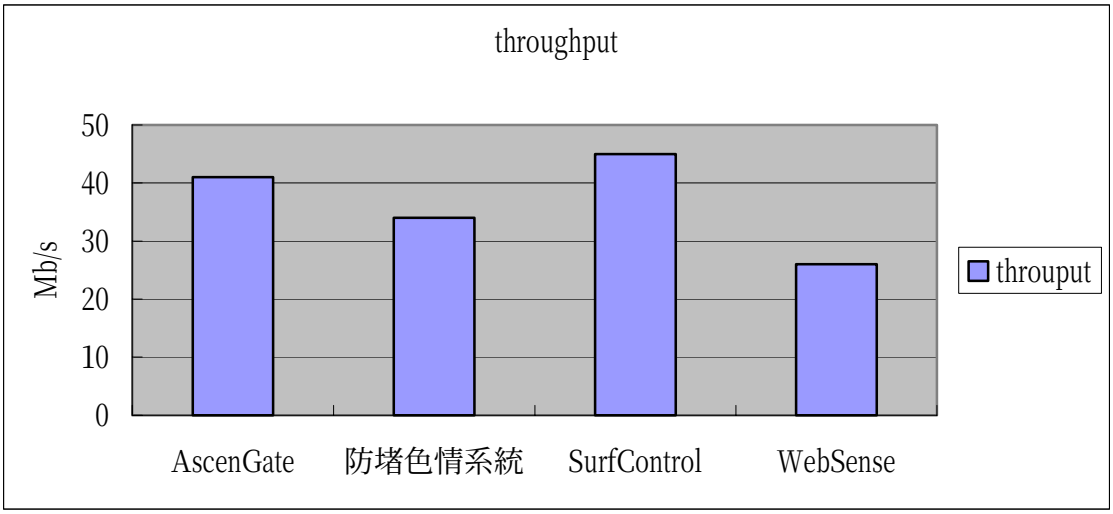
*文佳科技括號中的數據為更新 URL list 資料庫前的數據

表三十三、內容過濾器色情網站阻擋準確度比較表

9.7 效能

圖十六為內容過濾器效能比較表。我們利用 Avalanche 模擬大量使用者同時上網，藉以了解各產品最大的 throughput。其中效能最好的是 SurfControl 的產品。此外，必須說明

的是，防堵色情系統與 WebSense 係安裝在我們提供的 PC 上，安裝平台的規格如表二十八。



圖十六、內容過濾器效能比較表

9.8 觀察與總結

在本次測試之後，我們對市面上的內容過濾器產品有下列幾點觀察：

1. URL 比對仍是主流的技術，有些產品有加上內容中關鍵字的比對。這同時也意味著準確度十分仰賴資料庫更新的頻率與正確率，而不是從網頁的內容本身決定網頁是否該過濾。因為一但遇到一個新的網頁，如果 URL 資料庫內沒有該網頁的 URL 的話，便無法做出正確的判斷。
2. 語言本身的障礙並沒有如預期般的嚴重。即使是國外的產品，對於阻擋國內的色情網站也有一定的準確程度。
3. URL list 的個數都高達三百萬到五百萬之多。以一個 URL 有 10 bytes 計算，光是 URL list 的內容在記憶體中保守的估計就要佔掉 30 到 50 MB 的空間。
4. 除了文佳科技的產品外，網站種類的分類大約都在 30 到 80 之間。應該足夠應變學校或企業各種不同的需求。
5. 比對準確度約在 60%到 90%之間，仍然還是有一定比例的網頁沒辦法正確的擋下。
6. 通過內容過濾器的 throughput 有 25 Mb/s 到 50 Mb/s 之間，對於一般接取端的網路，這樣的 throughput 應該足以應付。至於在頻寬需求更大的場合，如電信單位，還是需要更高階的硬體。

10、產品總評

10.1 SOHO 防火牆 / 虛擬私有通道產品總評

對於測試報告的結論，我們對所有比較的功能與效能進行總評，共分使用(1) 簡易度、(2) 產品功能、(3) 防火牆效能、(4) VPN 效能等四項指標給分，滿分為五顆星。最後我們附上各產品的售價，並依售價列為評分項目之一，選出最物超所值的產品。評分的結果如表三十四。其中 NetScreen-5GT 以總分 19.5 拔得頭籌。

Model	Easy to use	Functionality	Firewall Performance	VPN Performance	Price/Value
Abocom FW 100	★★★★	★★★☆	★★★	★★★	$8,900
Check Point S-box	★★★★	★★★	★★★☆	No support	$28,000 ~ $48,000
D-Link DFL 100	★★★★	★★★☆	★★★★	★★★☆	$17,500
NetScreen-5GT	★★★★☆	★★★★★	★★★★★	★★★★★	$32,999
WatchGuard SOHO6tc	★★★★☆	★★★★	★★★★☆	★★★★☆	$32,000
ZyXEL ZyWALL 10W	★★★★★	★★★★	N/A	★★★★	$16,800

表三十四、SOHO 等級防火牆/私有虛擬網路產品總評

10.2 SME/Enterprise/Carrier 防火牆 / 虛擬私有通道產品總評

評分的結果請見表三十五。為節省篇幅，carrier 級的 NetScreen-5200 的評分一併列在這張表中。在 SME 等級，我們認為 Cisco 515E 在功能上見長，而 WatchGuard 1000 卻較易操作。在 enterprise 等級，我們認為 Check Point NGAI 的功能較多，而 D-Link DFL 1500 也整合了相當多符合市場需求的功能，以及操作更容易上手。但因為在屬於多人的企業環境當中，Check Point NGAI 需要較多的 license，價格上就偏高了許多。因此，我們給予 D-Link DFL-1500 最高的性價比排名。

	Easy to use	Functionality	Firewall Performance	VPN Performance	Price/ Value
AboCom FW 500	★★★★	★★★★	★★★	★★★	$29,000
Cisco PIX 515E	★★★	★★★★★	N/A	★★★★★	$175,000
WatchGuard 1000	★★★★★	★★★★	★★★★★	★★★★	$230,000
AboCom FW 1000	★★★★	★★★☆	★★★	★★★	$118,000
Check Point NGAI	★★★★☆	★★★★★	★★★★★	★★★★☆	$130,000 (25 users) ~ $1,100,000 (unlimited)
D-Link DFL 1500	★★★★★	★★★★☆	★★★★☆	★★★★★	$240,000
NetScreen-5200	★★★★☆	★★★★★	★★★★★	★★★★★	$4,740,000

表三十五、SME/enterprise/carrier 等級防火牆/私有虛擬網路產品總評

10.3 入侵偵測系統產品總評

表三十六為入侵偵測系統產品總評。在這次測試當中，我們主要從兩個角度去思考 IDS 的好壞。一是偵測能力，包括正常攻擊時的偵測能力，以及迴避時的偵測能力。二是 reporting 的好壞，因為牽涉到管理人員是否能很快的發現真正的、具有危害的攻擊。我們認為 NetScreen-IDP 100 在 reporting 方面格式的種類較為豐富，以及優先權的劃分上較為細緻，因此給予較高的評價。在偵測能力方面，各家產品在我們的測試條件下均有很好的表現，彼此間的差異並不大，僅僅在 MS-SQL 這項測試上有微小的差別。在我們的測試下，NetScreen-IDP 100 比 Intrusion 的產品多能處理 2 bytes 的 fragment 的 MS-SQL 攻擊，而 ISS 的產品可惜在更新 signature 後才偵測到這項攻擊，成為分數上差距的來源。但是我們仍然肯定這次參與的各家產品都有很好的表現。另外 Snort 在使用容易度、報告輸出、偵測能力等表現均不如商業產品。當然，免費是它的優勢，而且它的定位本來就不是要和商業產品競爭。

產品型號	Easy to use	Reporting	Detection capability	Price/Value
NetScreen-IDP 100	★★★★☆	★★★★★	★★★★★	$1,050,000
Intrusion SecureNet5545	★★★★	★★★★	★★★★☆	$797,000
Intrusion SecureNet7145	★★★★	★★★★	★★★★☆	$1,320,000
ISS RealSecure Gigabit Sensor	★★★★	★★★★	★★★★	$3,500,000
ISS Proventia A201	★★★★	★★★★	★★★★	$900,000
Snort 2.0	★★★	★★★	★★★	free

表三十六、入侵偵測系統產品總評

10.4 防毒系統產品總評

表三十七為防毒系統產品總評。趨勢科技的 InterScan VirusWall 不管在支援的協定、支援的壓縮格式、以及郵件輸入的方式上，都有三者中最好的表現，因此在功能上我們給予最高的評價。然而就好用的程度而言，桓基科技的操作最直覺，且可以設定的部分最多，因此我們在容易使用的程度上給予最好的分數。

Model	Easy to use	Functionality	Performance	Price/Value
Trend InterScanVirusWall	★★★★☆	★★★★★	★★★★★	$30,400 for 50 users ~ $304,000 for 500 users
Panda PerimeterScan for Sendmail	★★★	★★★★☆	★★★★★	$168,000 for 100 enterprise users $200,000 for 1000 student users
HGiga Virusherlock	★★★★★	★★★★	★★★★	$99,000 for 100 users $199,000 for 300 users

表三十七、防毒系統管理功能產品總評

10.5 內容過濾器產品總評

表三十八為內容過濾器產品總評，我們可以看到在各方面的比較 SurfControl 的產品都有最好的表現。文佳科技的系統在提供最新的資料庫後，在準確度上大幅提升。但是因為它提供的網頁分類種類只有賭博與色情兩類。

Model	Easy to use	Functionality	Reporting	Detection accuracy	Price/Value

AscenVision AscenGate 2000	★★★★	★★★★	★★★★	★★★	$599,990
文佳科技 防堵色情閘道系統	★★★	★★★	★★★	★★★★★	$4,950
SurfControl Web Filter	★★★★★	★★★★★	★★★★★	★★★★☆	$170,000 for 100 users
WebSense	★★★★☆	★★★★☆	★★★★★	★★★★	$120,000 for 100 users

表三十八、內容過濾器效能產品總評

10.6 所有產品總評

我們歸納前面結果選出各種類的最優良產品。列於表三十九。

種類	最優良產品	最物超所值產品
SOHO 防火牆/VPN	NetScreen-5GT	NetScreen-5GT
SME 防火牆/VPN	WatchGuard 1000	Cisco PIX 515E
Enterprise 防火牆/VPN	CheckPoint NGAI	D-Link DFL 1500
入侵偵測系統	NetScreen-IDP 100	NetScreen-IDP 100
防毒系統	TrendMicro InterScan VirusWall	TrendMicro InterScan VirusWall
內容過濾器	SurfControl Web Filter	WebSense

表三十九、最優良產品一覽表

11、觀察與總結

本次測試相較於去年的測試有幾點觀察值得注意：

1. SOHO 等級的防火牆/VPN 產品變化較大，今年測試的幾款產品都是在去年測試時尚未出現的。相對於 SOHO 等級的變化，在 SME/Enterprise 等級的產品變動就顯得較為緩慢。
2. SME/Enterprise 等級的產品仍以 Intel x86 系統的平台為主。另值得注意的是，在 SOHO 等級的 NetScreen-5GT 已經採用了 Intel IXP 425 的 Network Processor 做為 CPU。是否意味著在 SOHO 等級甚至 SME 等級以上的產品加速該往 Network Processor 而非 ASIC 的方向走，是值得未來注意的一件事。
3. 在 carrier 等級，由於需要極高的效能，ASIC 的做法仍是必需的。我們看到 NetScreen-5200 使用的 PowerPC CPU 雖然不算特別突出，但是在各項測試中均有極高的效能。探究其原因，在於使用新一代的 GigaScreen II ASIC 從事各項封包處理的工作，包括 NAT、

封包分類及解析(parsing)、session lookup、分割與重組、加解密等，而原 CPU 則專注在管理與控制的工作。另外，NetScreen-5200 可以做模組化的擴充，也是做為一個 carrier 等級產品的重要特性。

4. 各 VPN 產品皆能與 TeraVPN 做互通，顯示在互通性方面做的比去年好。
5. 在壓力測試下，有的產品會自動視為攻擊，而丟棄封包或拒絕 TCP 連線的建立，造成產品效能測試的困難。
6. 在各類產品中，有不少產品都是在 Linux 系統上開發的。顯示 Linux 的平台，在產品開發上受到一定的青睞。
7. 防火牆在需要處理封包內容的應用場合，如防毒或內容過濾系統，把封包 redirect 到專屬的系統仍然有其優勢。尤其是這些系統的特徵資料庫是否能經常或即時的更新，關係到偵測能力至為重大。要防火牆廠商自行發展這些技術及維護資料庫並不是一件容易的事。
8. 國內廠商的產品相較於國外廠商而言，差距主要還是在效能面，在功能面的差距還算不大。