

# 網路安全閘道器產品評比 – 功能與效能面

測試計畫主持人：林盈達

測試報告撰寫人：吳明蔚

測試人員：吳明蔚、魏煥雲、黃俊穎、蔡昌憲、張智晴、梁元彪、蔡良恆

國立交通大學網路測試中心

新竹市大學路 1001 號

## 摘要

為了保護上網企業的網路安全，安全閘道器產品變成企業不可或缺的設備。本次測試計畫的對象定位在中小企業(SME: Small-Medium Enterprise)等級以上之企業級(Enterprise-Class)安全閘道器，有部分送測產品甚至定位為ISP (Internet Service Provider)之電信級(Carrier-Class)產品。本次計有七家廠商十一項產品參與測試計畫：Check Point(Firewall-1 NG)、Cisco(PIX-525 及 PIX-535)、Intrusion(PDS-5515)、NetScreen(NS-204 及 NS-500)、RapidStream(RS-6000)、SonicWall(PRO-300 及 GX-650)、WatchGuard(WG-2500 及 WG-4500)。比較的項目計有 12 項指標，包括管理簡易度(Ease-of-Use)、記錄檔之維護(Log Reporting)、安全性(Security)、互通性(Interoperability)、防火牆(Firewall)之功能及效能、虛擬私有網路(VPN)之功能及效能、內容過濾(Content-Filtering)之功能及效能、額外功能如頻寬管理(Bandwidth Management)、以及最後的價值比(Value-to-Price)。結果之圖表均經過所有受測廠商確認無誤，報告之結論依 1~5 顆星分別替 SME、Enterprise 及 Carrier 三個等級的產品打分數。在 SME 等級 SonicWall PRO300 及 WatchGuard 2500 屬於「四星級優良產品」。在 Enterprise 等級 NetScreen 204 及 RapidStream 6000 屬於「五星級傑出產品」，Intrusion PDS5515、WatchGuard 4500，以及 Cisco PIX 525 屬「四星級優良產品」。在 Carrier 等級 NetScreen 500 屬於「五星級傑出產品」，Check Point FW-1 NG (Dell)及 SonicWall GX650 屬於「四星級優良產品」。

關鍵字：安全閘道器，防火牆，虛擬私有網路，入侵偵測，內容過濾，頻寬管理，效能  
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。網路管理者必須建置防火牆(Firewall)才能有效控制封包的進出，進而管理及阻擋 Internet 上成員惡意存取企業內部的資源，或防止自己的員工由 Internet 下載或上傳不當內容；然而企業的子公司間在利用 Internet 傳送機密文件時，封包亦極可能被 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(Virtual Private Network：VPN)可以解決企業用戶的需求；而近幾年，隨手可得的攻擊工具造成網路攻擊層出不窮，阻斷服務(Denial of Service：DoS)與伺服器漏洞(exploits)的攻擊分別令網站及企業頭痛，企業級防火牆應記錄攻擊甚或加以阻擋，甚至能繼續提供服務。企業本身應意識到網路是個極不安全的國度，必須對自身的企業進行網路安全解決方案的規劃與評估。本測試報告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。圖一則是我們的測試環境。

### **功能指標：三類八項**

在本測試報告中，將安全閘道器(Security Gateway)的主要功能可分成三類共計八項指標：「基本系統功能」，包括(1)管理簡易度、(2)記錄檔稽核(安全稽核機制)、(3)互通性、以及(4)對於典型網路入侵之安全性(安全預防機制)；「基本防火牆功能」，包括(5)傳輸層防火牆(擷取安全機制)、(6)VPN(通訊安全機制)；「附加價值功能」，包括(7)應用層防火牆(內容安全機制)、與(8)頻寬管理(流量管理應變機制)。

### **效能指標：四項**

而其中，傳輸層防火牆、VPN、應用層防火牆，以及頻寬管理等四項功能，本測試有針對每台受測機器進行相關效能測試，進而產生四項效能數據。由於並非每間廠商皆

有頻寬管理，故其所佔評分比重僅佔一項。最後並附加一項價格指標，將各廠商的受測機器之價格，提供讀者作參考。因此，本測試報告最後的評比結果，即是對十二項指標作評分。

關於本測試計畫的動機，以及上述三大類十二指標，其目的在於幫助讀者瞭解一面追求高安全性(Security)的功能(Functionality)時，往往付出的代價是效能(Performace)，又或為了提升效能，進而得以價格(Price)換取更高階的硬體。為此，本測試試著透過上述三大分類，讓讀者瞭解其在選購防火牆時應該注意的環節。

### **基本系統功能**

首先，一台防火牆，「基本系統功能」一定要完整。不人性化的管理介面，難以檢視的紀錄檔，糟糕的互通性，以及無法有效防範典型的攻擊，這些對系統管理維護人員而言，絕對是一場夢魘。

### **基本防火牆功能**

接著根據你企業的個別需求，這包括企業的規模及對外流量(這關係到所需功能的效能要求)，以及企業必須量身訂做出清楚完整的安全機制(Security Policy)。簡單來說，傳輸層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。而基於這樣的規則，防火牆絕對會忠實地實行你設定的規則，但粗糙而不嚴謹的設定則會令你的防火牆無用武之地。所以瞭解你的安全需求以及效能需求，是善用防火牆的第一步。

另一方面，因為企業之間越發重視在透過網際網路傳遞資訊時之安全性，VPN 也成為安全閘道器所必須支援的功能之一。VPN 是利用 DES、3DES、或甚至 AES 加密，以及 MD5、SHA-1 等認證演算法，使得資料可以安全地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。而金鑰交換方式包括 Manual Keying 與 Automatic Keying，本次的效能測試是以後者為主。

### **附加價值功能**

最末，為了提供更完整的網路安全解決方案，許多市面上的安全閘道器皆有支援應

用層防火牆，部分受測產品更首次提供頻寬管理(Bandwidth Management)之品質保證(QoS)功能。應用層防火牆可檢查封包的 payload 部分是否有病毒(virus)或 Java/JavaScript/ActiveX 物件是否可以通過防火牆，也因此會比傳輸層防火牆更為安全。而另一逐漸獲得重視的額外功能是頻寬管理，其需求是企業在使用 Internet 各項服務時，因為這些流量的重要性不一，必須善用昂貴的頻寬。例如企業的 ERP(Enterprise Resource Planning)軟體、與顧客交易的電子商務連線的流量，不應該被不重要的 FTP 佔據頻寬。企業因而使用頻寬管理器來訂立許多策略(policy)，例如每部門或某項應用可分到多少頻寬，以謀求企業的最大利益；甚至同一大樓的多家分公司共租一條專線時也有切割頻寬的需求。policy 的訂立通常透過設定封包分類器(packet classifier)來分群(設定哪些 packet 符合此策略)，再設定各群的頻寬參數(符合此群者得到一定頻寬)。關於頻寬管理，本測試檢視各產品在設定各種頻寬上下限後能否真正落實。

綜觀此次企業級 Security Gateway 產品可以發現，多數廠商皆有考量防火牆的高可用性(High Availability:HA)，HA 確保當防火牆硬體故障時，另一台防火牆能接管其工作。基本來說有兩種 HA 模式，一種為 Stateless failover，當主要防火牆故障，而第二台防火牆接續其工作時，所有連線必須重新連結。另一種為 Stateful failover，則第二台防火牆進行接管時，所有連線仍能繼續進行。詳細的 HA 功能，各家防火牆廠商作法多有差異，由於高可用性往往意味著近乎雙倍的硬體建置成本，本測試報告並未將 HA 考慮進量測項目之一。

## 二、測試對象

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 Firewall 與 VPN 兩項功能(必要條件)且佔有率較高的產品，並挑選出兩種等級之產品，其一為企業等級(通常僅具有 10/100 Fast Ethernet 網卡介面)，其二為電信等級(通常具有 Gigabit 網卡介面)。並同時進行測試計畫的規劃與計畫書撰寫。接著由網路通訊雜誌社出面對各廠商發出邀請，並附上我們的測試計畫書。我們邀請了國外的 Check Point[1]、Cisco[2]、Intrusion[3]、

NetScreen[4]、Nokia[5]、RapidStream[6]、SonicWall[7]、Symantec[8]、以及 WatchGuard[9] 等廠商。最後有將產品送來的共計 8 家(除了 Nokia 之外)，但其中 Symantec 防火牆軟體並無法直接在安全閘道器上提供防毒軟體功能，而得透過使用者端自行安裝防毒軟體，再者其並無提供硬體的解決方案參與測試，故 Symantec 並沒有列入本測試計畫的評比。最後對 7 家廠商共計 11 項商業產品作比較。圖一是待測物及 SmartBits。其中 WatchGuard 4500 僅有一台，以及 Cisco PIX-535 之 Gigabit 網卡僅有兩張(需要四張)，而 TeraVPN 測試工具尚未正常工作，所以無法以單機測試這兩項產品的 VPN 效能；Cisco PIX 系列亦因 3DES 授權來不及申請，也未能進行 VPN 之 3DES/SHA-1 測試；而 Intrusion 則因與 WebBench 測試軟體不相容，並沒有進行內容過濾測試。表一是邀請的廠商與結果。邀請於今年 1 月中送出，產品於 2 月底收集完成，測試工作於 4 月初完成，所有列表與數據均經過所有廠商確認無誤。



圖一：待測物及 SmartBits

防火牆廠商	產品名稱	國內售價 (NT\$)	國內代理商	邀請結果
Check Point	VPN-1/Firewall-1 NG (電信等級) (硬體為 Dell 雙 CPU 機種)	31,000~ 1,176,000*	精誠公司	國外原廠直接空運送達
Cisco	PIX 525UR-BUN (高階企業等級) PIX 535 (電信等級)	1,020,000 2,475,000	聚碩科技	送達
Intrusion	PDS5515 (Secured by Check Point)	489,700	精誠公司	國外原廠直接空運送達

	(高階企業等級)			
NetScreen	NetScreen-204 (高階企業等級) NetScreen-500 (電信等級)	632,500 2,470,000	友冠資訊 敦新科技	送達
RapidStream	RapidStream 6000 (高階企業等級) RapidStream 8000 (電信等級)	599,000 1,499,000	新達電腦	部分送達 (RS8000 趕不及調度)
SonicWall	SonicWall PRO 300 (中階企業等級) SonicWall GX650 (電信等級)	265,000 1,979,000	富揚資訊	國外原廠直接空運送達
WatchGuard	Firebox III 2500 (中階企業等級) Firebox III 4500 (高階企業等級)	380,000 500,000	泓彥資訊	送達
Nokia	Nokia IP530 (高階企業等級) Nokia IP740 (電信等級)	N/A N/A	陸德資訊	未送達 (新版產品趕不上測試時程)
Symantec	Symantec Firewall/VPN Enterprise 7.0 (SOHO/低階企業等級)	N/A	賽門鐵克	送達 (經評估, 不列入測試對象)

\* license price ranges from 5 users to unlimited users

表一：邀請廠商與結果

本次受測機器皆由廠商提供硬體解決方案，即便是 Check Point 軟體產品，也是由國外原廠自行安裝至 Dell 雙 CPU 主機空運來台。其他如 Cisco、NetScreen、RapidStream、SonicWall 與 WatchGuard 則是以硬體形式銷售。較特別的是 Intrusion 的硬體產品，核心軟體是使用 Check Point 軟體。受測物之內部與外部硬體規格列於表二(a)及(b)。其中 Cisco、NetScreen、SonicWall 以及 WatchGuard 將作業系統放在 Flash ROM，硬體故障機率 MTBF(Mean Time Between Failure)會比 Check Point 及 Intrusion 來的小，因為後者這兩家廠商的產品是將作業系統放在硬碟。RapidStream 廠商向我們表示，其另一出貨版本之 RS6000(相同價格)亦將作業系統存放於 128MB Flash ROM。

	OS	CPU	Accelerator	RAM	Flash	Hard Disk
<b>SME-Class</b>						
<b>SonicWall PRO300</b>	VxWorks	StrongARM-233MHz	SonicWall ASIC	64MB	16MB	No
<b>WatchGuard 2500</b>	Linux	AMD-K6-500MHz	On-Board IC	128MB	8MB	No
<b>Enterprise-Class</b>						
<b>Cisco PIX525</b>	PIX	Intel-PIII-600MHz	SafeNet ADSP-2141L	256MB	16MB	No
<b>Intrusion PDS5515</b>	Linux	Intel-PIII-1GHz	BroadCom-5805	512MB	No	20.5GB
<b>NetScreen 204</b>	ScreenOS	350MHz PowerPC	GigaScreen ASIC	128MB	8MB	No
<b>RapidStream 6000</b>	Linux	Intel-Celeron-500MHz	RapidCore ASIC, HiFn-6500	128MB	No	10.2GB
<b>WatchGuard 4500</b>	Linux	AMD-K6-500MHz	PCI card	256MB	8MB	No
<b>Carrier-Class</b>						

Check Point Firewall-1 NG	Linux	Dual Intel-P4-1.7GHz	BroadCom-5805	1024MB	No	20.5GB
Cisco PIX535	PIX	Intel-PIII-1GHz	SafeNet ADSP-2141L	512MB	16MB	No
NetScreen 500	ScreenOS	300MHz MIPS	GigaScreen ASIC	256MB	16MB	No
SonicWall GX650	VxWorks	Intel-PIII-866MHz	HiFn-7811*3	256MB	16MB	No

表二(a)：內部硬體規格比較

	Connectivity Interface	Console	High Availability Ports	Display Panels	Rack Size
<b>SME-Class</b>					
SonicWall PRO300	10/100Base-T *3	1 (DB-9)	1 (LAN interface)	3 LEDs	1U
WatchGuard 2500	10/100Base-T *3	1 (DB-9)	No	10 LEDs	2U
<b>Enterprise-Class</b>					
Cisco PIX525	10/100Base-T *2	1 (RJ-45)	2 (DB-15 and LAN)	2 LEDs	2U
Intrusion PDS5515	10/100Base-T *3	1 (DB-9)	Optional	9 LEDs	1U
NetScreen 204	10/100Base-T *3	2 (RJ-45)	2 (RJ-45)	6 LEDs	1U
RapidStream 6000	10/100Base-T *3	1 (DB-9)	2 (RJ-45)	4 LEDs	2U
WatchGuard 4500	10/100Base-T *3	1 (DB-9)	No	10 LEDs	2U
<b>Carrier-Class</b>					
Check Point Firewall-1 NG	1000Base-SX *2	1 (DB-9)	Optional	N/A	N/A
Cisco PIX535	1000Base-SX *2	1 (RJ-45)	2 (DB-15 and LAN)	2 LEDs	3U
NetScreen 500	1000Base-SX *3	2 (DB-9)	2 (RJ-45)	12 LEDs + 1 LCD	2U
SonicWall GX650	1000Base-SX *3	1 (DB-9)	2 (RJ-45)	2 LEDs	3U

表二(b)：外部硬體規格比較表

### 三、功能比較

就產品功能面方面，我們將比較結果分成三類八項：(1)管理簡易度、(2)記錄檔稽核、(3)互通性、(4)安全性、(5)傳輸層防火牆、(6)VPN、(7)內容過濾、與(8)頻寬管理。

#### 管理簡易度

表三是受測機器本身的管理與設定規格比較表。此列表在於比較管理簡易度及協助偵錯與維護。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。

	MGT. Interfaces		System Maintenance		Trouble Shooting			
	GUI	CLI	Configuration Backup/Restore	Firmware Upgrade	Diagnostic Tools	Real-Time Monitoring	Network Statistics	CPU/MEM Utilization
Check Point and Intrusion	Check Point Policy Editor	YES	YES	Software	YES	YES	YES	Partial

Cisco	Web	YES	YES	YES	YES	YES	YES	YES
NetScreen	Web	YES	YES	YES	YES	YES	YES	YES
RapidStream	RapidStream Manager	YES	YES	YES	YES	YES	YES	YES
SonicWall	Web, ViewPoint	YES	YES	YES	YES	YES	YES	NO
WatchGuard	WatchGuard Manager	YES	YES	YES	YES	YES	YES	NO

表三：管理與設定規格比較表

管理簡易度方面，RapidStream、WatchGuard 與 Check Point 專有的設定管理程式，其介面較為精美，雖需要另外安裝於使用者端，然複雜管理功能之展現較 Web 強悍。其中 Check Point 之操作畫面雖有獨特的物件化與圖形化介面，且對同時操作管理多台防火牆時相當有幫助，但略不直覺。其次是 Web-based 操作介面最容易上手，包括 Cisco、SonicWall 及 NetScreen，然 Cisco 的 Web 操作介面之功能明顯不足(無 VPN 等設定)；最後則是指令式(CLI)的管理方式，所有廠家皆支援 CLI，其中 Cisco 的指令式操作環境作的最完整，但不太好用(指令太長、手冊在 VPN 設定交代不清楚、VPN 設定繁瑣)。

為了讓 ISP 或大型企業可以在一台機器上下單一指令同時管上百台甚至上千台的閘道器，許多廠商也提供了 CNM(Centralized Network Management)，我們發現所有受測產品皆有 CNM 功能，但大部分廠商把 CNM 列為選購功能，這次我們並沒有評比此項。

就系統維護方面，所有廠商都能提供設定檔的備份與回復。不過備份檔輸出格式不盡相同，以 NetScreen 為例，其輸出為純文字，RapidStream 為 XML 檔，而 SonicWall 會加以編碼。檔案格式的差異在於使用者是否有自行修改的彈性。對於網路或安全閘道器本身的狀態，所有廠商都提供即時監控，輔與基本的分析工具，網管人員能夠快速地掌握。

### **記錄檔稽核**

表四是記錄檔稽核規格比較表。記錄檔稽核完整性是要檢視 Security Gateway 是否有完善的記錄檔資訊，以通知網管人員進行安全處理及針對記錄檔進行解析。我們發現所有受測機器都提供主要的記錄檔，但大部分廠商並沒有加以分類，使得所有記錄檔會顯示在同一頁，而當安全閘道器本身不具有記錄檔篩選能力時(Cisco 及 WatchGuard)，如從幾百筆資料中過濾出某一項目，將會很難檢視過多的紀錄檔。另外，記錄檔除了儲存在

安全閘道器本身，是否能夠存放在外界的儲存媒體亦十分重要，包括 Email 發送、Syslog server 以及檔案直接下載。我們觀察到 RapidStream 在記錄檔稽核這部分作的相當完整，其次是 NetScreen 及 Check Point。

	Logging Items					Logging Functions				
	Firewall Log	VPN Log	Intrusion Log	Content Filtering Log	Event Log	Log Entry Filtering	Send Logs to Email (full/interval)	Syslog	Alarm Mail	Download-to-File
Check Point and Intrusion	YES	YES	YES	YES	Partial	YES	YES	Partial	YES	YES
Cisco	YES	YES	YES	YES	YES	NO	NO	YES	YES	NO
NetScreen	YES	YES	YES	YES	YES	YES(only CLI)	Full	YES	YES	YES
RapidStream	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES
SonicWall	YES	YES	YES	YES	YES	Partial	YES	YES	YES	NO
WatchGuard	YES	YES	YES	YES	YES	NO	YES	YES	NO	YES

表四：記錄檔稽核規格比較表

### 互通性

表五(a) (c)是不同廠商防火牆之間的互通性測試比較表，各廠商的防火牆產品之互通性，則藉由設定以下 6 種情況，看看各產品間是否可以順利建立起 VPN tunnel。

- [1] Manual Keying：ESP，NULL(無加密)，MD-5 認證法。
- [2] Manual Keying：ESP，DES 加密法，MD-5 認證法。
- [3] Manual Keying：ESP，3-DES 加密法，SHA-1 認證法。
- [4] Automatic Keying：ESP，NULL(無加密)，MD-5 認證法，PSK 金鑰認證機制。
- [5] Automatic Keying：ESP，DES 加密法，MD-5 認證法，PSK 金鑰認證機制。
- [6] Automatic Keying：ESP，3-DES 加密法，SHA-1 認證法，PSK 金鑰認證機制。

從表五可以發現所有廠商在互通性方面幾乎都沒有什麼問題。一年半前我們進行此項測試時，各家之間幾乎都不互通，所以改進很大。但 Check Point 並不支援 Manual keying，以及 Cisco 的 Manual keying 無法正常作用(Cisco 在截稿當日向我們表示利用 Manual Key 建立 VPN 通訊時，Cisco PIX 防火牆會顯示警告訊息，但 VPN tunnel 可以順利建立，VPN 傳輸也可正常運作。互通性應無虞)。另外，NetScreen 和 WatchGuard 之間，因為兩家廠商對 SPI(Security Parameter Index)給定的範圍不同，WatchGuard 只允許 257~1023 (十進位)，而 NetScreen 則是 1000~2ffffff (十六進位)。在 Manual-keying 完全無法互通。最後，因考量 Manual Keying 的設定已甚少使用於 VPN IPSEC，故我們以 IKE 的結果作為互通性評比依據。

	CheckPoint and Intrusion PDS5515		WatchGuard		RapidStream		Cisco		NetScreen		SonicWall	
	M	A	M	A	M	A	M	A	M	A	M	A
CheckPoint and Intrusion PDS5515	N/A	✓	N/A	✓	N/A	✗	(N/A)	✗	N/A	✓	N/A	✓
WatchGuard	N/A	✓	✓	✓	✓	✓	✗*	✓	✗	✗	✗	✗
RapidStream	N/A	✗	✓	✓	✓	✓	✗*	✓	✓	✓	✗	✗
Cisco	(N/A)	✗	✗*	✓	✗*	✓	✗*	✓	✗*	✓	✗*	✓
NetScreen	N/A	✓	✗	✗	✓	✓	✗*	✓	✓	✓	✓	✓
SonicWall	N/A	✓	✗	✗	✗	✗	✗*	✓	✓	✓	✓	✓

M: Manual key, A: Automatic-key (IKE); ✓: Pass, ✗: Fail; N/A: Not Available: Check Point; \*: Cisco

表五(a) : NULL/MD5 之 VPN 互通性測試比較表

	CheckPoint and Intrusion PDS5515		WatchGuard		RapidStream		Cisco		NetScreen		SonicWall	
	M	A	M	A	M	A	M	A	M	A	M	A
CheckPoint and Intrusion PDS5515	N/A	✓	N/A	✓	N/A	✗	(N/A)	✗	N/A	✓	N/A	✓
WatchGuard	N/A	✓	✓	✓	✓	✓	✗*	✓	✗	✓	✓	✓
RapidStream	N/A	✗	✓	✓	✓	✓	✗*	✓	✓	✓	✓	✓
Cisco	(N/A)	✗	✗*	✓	✗*	✓	✗*	✓	✗*	✓	✗*	✓
NetScreen	N/A	✓	✗	✓	✓	✓	✗*	✓	✓	✓	✓	✓
SonicWall	N/A	✓	✓	✓	✓	✓	✗*	✓	✓	✓	✓	✓

M: Manual key, A: Automatic-key (IKE); ✓: Pass, ✗: Fail; N/A: Not Available: Check Point; \*: Cisco

表五(b) : DES/MD5 之 VPN 互通性測試比較表

	CheckPoint and Intrusion PDS5515		WatchGuard		RapidStream		Cisco		NetScreen		SonicWall	
	M	A	M	A	M	A	M	A	M	A	M	A
CheckPoint and Intrusion PDS5515	N/A	✓	N/A	✓	N/A	✗	N/A	N/A	N/A	✓	N/A	✓
WatchGuard	N/A	✓	✓	✓	✓	✓	N/A	N/A	✗	✓	✓	✓
RapidStream	N/A	✗	✓	✓	✓	✓	N/A	N/A	✓	✓	✓	✓
Cisco	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
NetScreen	N/A	✓	✗	✓	✓	✓	N/A	N/A	✓	✓	✓	✓
Sonic Wall	N/A	✓	✓	✓	✓	✓	N/A	N/A	✓	✓	✓	✓

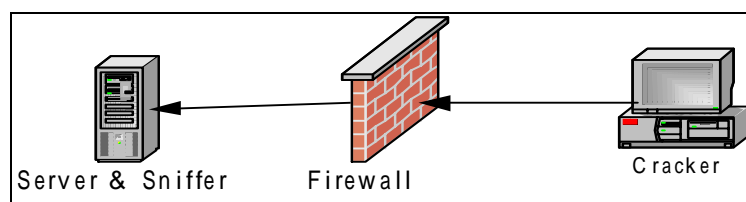
M: Manual key, A: Automatic-key (IKE); ✓: Pass, ✗: Fail; N/A: Not Available: (Check Point and Cisco)

表五(c)：3DES/SHA-1 之 VPN 互通性測試比較表

## 安全性

首先必須釐清的是，防火牆產品之安全性或並不能單純用 Nessus、Nmap，以及其他攻擊工具來評斷，然而我們在此是為了提供讀者關於一些典型攻擊的安全性之參考。企業網路的安全性也不是只依據建置較安全之 Security Gateway 或專門的 IDS(Intrusion Detection System)就可以無後顧之憂，因為整個企業網路的安全性，如前言所述，是跟企業本身制訂的安全策略與網路架構有密切的關係。

本測試報告歸納了三類最典型的網路安全問題，並於如圖二所示之環境進行測試。



圖二：安全性測試環境

### 1. Stealth Scanning(隱藏式掃描)

表六(a)列出三種常見的網路掃描之比較表，因為這些封包皆是不正常的 TCP 封包，一般情況下如果防火牆具備 Stateful Inspection 功能，應該都可以正確地擋下。

	NULL Scan	XMAS Scan	FIN Scan
Check Point	B	B	B

<b>Cisco</b>	B	B	B
<b>Intrusion</b>	B	B	B
<b>Netscreen</b>	B	B	B
<b>Rapidstream</b>	B	B	B
<b>SonicWall</b>	B	B	B
<b>WatchGuard</b>	B	B	B

表六(a)：Stealth Scanning 測試比較表

### 2. Application Exploits(應用程式漏洞攻擊)

表六(b)是針對五種常見的網路伺服器之漏洞進行攻擊的比較表。此項測試對一般的防火牆似乎較為嚴苛，因為目前的都未包涵完整的入侵偵測功能，可說全軍覆沒。但是 WatchGuard 由於內建許多 Application Proxy，例如可以關閉 FTP 的 SITE 指令，於是成功的阻擋此項攻擊。

	<b>IIS 5.0 .printer ISAPI exploit</b>	<b>MS Indexing Service ISAPI Extension exploit</b>	<b>Wu-ftp SITE EXEC</b>	<b>Sendmail Exploit</b>	<b>POP3 exploit</b>
<b>Check Point</b>	N	N	N	N	N
<b>Cisco</b>	N	N	N	N	N
<b>Intrusion</b>	N	N	N	N	N
<b>Netscreen</b>	N	N	N	N	N
<b>Rapidstream</b>	N	N	N	N	N
<b>SonicWall</b>	N	N	N	N	N
<b>WatchGuard</b>	N	N	B	N	N

表六(b)：Application Exploits 測試比較表

### 3. Denial of Service(阻斷服務)

表六(c)是三類常見的阻斷服務攻擊之比較表。NetScreen 可以自行設定門檻值 (threshold)，當遇到 SYN flooding 時，改以 proxy 方式建立連線，所以還能提供正常連線。Check Point 及 Intrusion 在 SYN-flooding 的防護上，可使用 SYNDefender Relay 和 SYNDefender Gateway 兩種技術，成功地擋下 SYN flooding 的攻擊封包。

	<b>SYN flood</b>	<b>ICMP flood</b>	<b>UDP flood</b>
<b>Check Point</b>	B	N	N
<b>Cisco</b>	D	N	N
<b>Intrusion</b>	B	N	N
<b>Netscreen</b>	B	B	D
<b>Rapidstream</b>	D	N	B
<b>SonicWall</b>	D	N	N
<b>WatchGuard</b>	D	B	N

表六(c)：Denial of Service 測試比較表

總結而言，NetScreen 較為完備，其次是 WatchGuard 與 RapidStream。除了本測試所列之安全性驗證之外，目前有在驗證防火牆安全性的機構包括：(1) ICSA(所有受測廠商都宣稱有通過這個標準)；(2) CheckMark；(3) ISO 15408；(4)ITSEC(歐規標準)。

**防火牆之功能**

在防火牆規格方面，所有廠商的受測物皆預設開啟 Stateful Inspection，理論上這對效能及安全的提升會有幫助。從表七(a)及(b)可以發現，大部分的產品都提供防火牆應有的基本功能。

	Firewall			NAT			
	Packet filter	Stateful Inspection	Classifier	1-1	M-1	M-M	Port Forwarding
Check Point FireWall-1 NG	Yes	Yes	4 tuples, Time	Yes	Yes	Yes	Yes
Cisco PIX 525	Yes	Yes	5 tuples	Yes	Yes	Yes	Yes
Intrusion PDS5515	Yes	Yes	4 tuples, Time	Yes	Yes	Yes	Yes
NetScreen 204	Yes	Yes	4 tuples (5 tuples in CLI mode)	Yes	Yes	Yes	Yes
SonicWALL PRO300	Yes	Yes	4 tuples plus incoming and outgoing NIC, Time, Fragments	Yes	Yes	No	Yes
WatchGuard 2500	Yes	Yes	4 tuples	Yes	Yes	Yes	Yes
RapidStream 6000	Yes	Yes	4 tuples plus incoming NIC, VLAN	Yes	Yes	Yes	Yes

表七(a)：防火牆規格比較表

	Firewall	NAT
	Application Support (*)	Application Support (*)
Check Point and Intrusion PDS5515	More than 150	More than 150
Cisco PIX 525	RPC, NetBIOS, RealAudio, Streamworks, CuseeMe, Internet Phone, VDOLive, MS SQL	RPC, NetBIOS, RealAudio, Streamworks, CuseeMe, Internet Phone, VDOLive, MS SQL
NetScreen 204	FTP, DNS, TFTP, XING, Real Media, NFS, TALK, rlogin, VDO Live, H.323	FTP, DNS, TFTP, XING, Real Media, NFS, TALK, rlogin, VDO Live, H.323
RapidStream 6000	AOL Instant Messenger, CU-SeeMe, DHCP/BootP Client/Server, DNS, FTP, HTTPS, VDOLive, Yahoo Messenger., and 20 more.	Telnet, FTP, TFTP

<b>SonicWALL PRO 300</b>	FTP, LDAP, Lotus Notes, DNS, Napster, Real Audio, TFTP, Timbuket, HTTPS, and 20 more.	FTP, LDAP, Lotus Notes, DNS, Napster, Real Audio, TFTP, Timbuket, HTTPS, and 20 more.
<b>WatchGuard 2500</b>	DCE-RPC, DNS-Proxy, FTP, H323, HTTP, Proxied-HTTP, RealNetworks, RTSP, SMTP, StreamWorks, VDOLive	N/A

\* means claimed by the vendors but not verified by us

表七(b)：防火牆規格比較表

### VPN 之功能

在 VPN 方面,所有受測機器皆支援 DES/3DES 加密方式以及 MD5/SHA-1 認證方式,其中較特別是 Check Point、Intrusion 與 NetScreen 已開始支援較新穎的 AES 加密,而 SonicWall 在 Manual-keying 方面有提供 ARC4 加密。而 Cisco 的 MD-5 驗證在 Manual Keying 的有問題,無法正常作用。

		Protocol Support		Encryption Algorithm			Authentication Algorithm	
		AH*	ESP	DES	3-DES	Others*	MD-5	SHA-1
<b>Check Point and Intrusion PDS 5515</b>		Yes	Yes	Yes	Yes	AES, CAST	Yes	Yes
<b>Cisco PIX</b>	<b>525</b>	Yes	Yes	Yes	Yes	No	Yes**	Yes
	<b>535</b>	Yes	Yes	Yes	Yes	No	Yes**	Yes
<b>NetScreen</b>	<b>204</b>	Yes	Yes	Yes	Yes	AES (128 bit)	Yes	Yes
	<b>500</b>	Yes	Yes	Yes	Yes	AES (128 bit)	Yes	Yes
<b>RapidStream 6000</b>		Yes	Yes	Yes	Yes	No	Yes	Yes
<b>SonicWall</b>	<b>Pro 300</b>	Yes	Yes	Yes	Yes	ARC4	Yes	Yes
	<b>GX 650</b>	Yes	Yes	Yes	Yes	ARC4	Yes	Yes
<b>WatchGuard</b>	<b>2500</b>	Yes	Yes	Yes	Yes	No	Yes	Yes
	<b>4500</b>	Yes	Yes	Yes	Yes	No	Yes	Yes

\* means claimed by the vendors but not verified by us

\*\* IKE okay, but manual-keying failed

表八(a)：VPN 加密驗證規格比較表

		Keying Method		IKE Authentication			IKE Misc.	
		Manual Key	IKE	PSK	RSA*	Others*	DH Group	PFS
<b>Check Point and Intrusion PDS 5515</b>		No	Yes	Yes	Yes	DSA	1, 2, 5	Yes
<b>Cisco PIX</b>	<b>525</b>	Yes	Yes	Yes	Yes	DSA	1, 2	Yes
	<b>535</b>	Yes	Yes	Yes	Yes	DSA	1, 2	Yes
<b>NetScreen</b>	<b>204</b>	Yes	Yes	Yes	Yes	DSA	1, 2, 5	Yes

	<b>500</b>	Yes	Yes	Yes	Yes	DSA	1, 2, 5	Yes
<b>RapidStream</b>	<b>6000</b>	Yes	Yes	Yes	Yes	DSA	1, 2	Yes
<b>SonicWall</b>	<b>Pro 300</b>	Yes	Yes	Yes	Yes (local certificate)	sonicwall cert. 3rd party cert.	1, 2, 5	Yes
	<b>GX 650</b>	Yes	Yes	Yes	Yes (local certificate)	sonicwall cert. 3rd party cert.	1, 2, 5	Yes
<b>WatchGuard</b>	<b>2500</b>	Yes	Yes	Yes	No	No	1, 2	Yes
	<b>4500</b>	Yes	Yes	Yes	No	No	1, 2	Yes

\* means claimed by the vendors but not verified by us

表八(b)：VPN Key Exchange 規格比較表

### 內容過濾之功能

在內容過濾規格方面，有一部份產品的 ACL/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，不同商業產品所能阻擋的物件種類也不盡相同。從表九可以發現 WatchGuard 所能提供的內容過濾功能十分完善，其次是 Check Point 與 Intrusion。

	Protocol	ACL/URL filter	Miscellaneous
<b>Check Point and Intrusion PDS5515</b>	HTTP	Built-in & External (WebSense)	Java/ActiveX/JavaScript Virus-Scanning (External)
	SMTP*	Built-in	Virus-Scanning (External)
	FTP*	Built-in	Virus-Scanning (External)
<b>Cisco PIX 525</b>	HTTP	External (Websense)*	Java/ActiveX
<b>NetScreen 204</b>	HTTP	External (Websense)*	Java/ActiveX/ZIP/EXE
<b>RapidStream 6000</b>	HTTP	N/A	Java
<b>SonicWall PRO300</b>	HTTP	Built-in (+Websense/H2N2)	Java/ActiveX/Cookie
	News, FTP, Gopher*	Built-in	Virus-Scanning (External)
<b>WatchGuard 2500</b>	SMTP (In)*	Built-in	Attachment, MIME, Spam, Header, SMTP Cmd.
	SMTP (Out)*	Built-in	Masquerade: Sender, M-ID
	FTP (In/Out)*	Built-in	Read-only connection
	HTTP	Built-in	Java/ActiveX/Cookie/MIME

\* means claimed by the vendors but not verified by us

表九：內容過濾規格比較表

### 頻寬管理之功能

在頻寬管理的功能比較上，僅有四家廠商(Check Point、NetScreen、RapidStream 及 SonicWall)能提供此額外功能，而此次 Check Point 的受測機器並沒有安裝選購的頻寬管理

產品 FloodGate-1，我們向原廠反應後，並沒能趕在截稿日期前有後續回覆，有關於 FloodGate-1 的評比，請參考我們刊載在去年 6 月網路通訊雜誌的頻寬管理器測試報告，其功能及效能表現不錯；另外 SonicWall 僅能針對由內往外之流量作頻寬管理。在頻寬管理功能比較表（表十），我們以去年六月網路通訊雜誌所登的頻寬管理器測試報告的功能表作比較，用較嚴苛的態度去檢視頻寬管理的功能。由表十得知，SonicWALL 僅能控制內對外的頻寬，是比較弱的一環；三項受測物皆可以控制「群組（class）」頻寬的上下限（Max/Min），使得 class 間可利用其他 class 剩餘沒用的頻寬。最末，所有受測物都可以控制經過資料經加密後的 tunnel 頻寬，然而處理的方式都是以一個 tunnel 的頻寬多少為單位，並不能控制到 tunnel 內不同應用的頻寬分配。

	Manageable Traffic Direction	Minimum Bandwidth	Bandwidth Sharing among classes*	Per-flow Bandwidth	Admission Control*	QoS per tunnel
NetScreen	Any	Y	Y	N	N	Y
RapidStream	Any	Y	Y	N	N	Y
SonicWall	LAN/DMZ to WAN	Y	Y	N	N	Y

\* means claimed by the vendors but not verified by us

表十：頻寬管理規格比較表

#### 四、效能比較

我們先整理效能測試的工具，各類工具及它們的用途整理於表十一，之後將個別去討論四項效能指標的各廠商之數據。

##### 測試工具列表

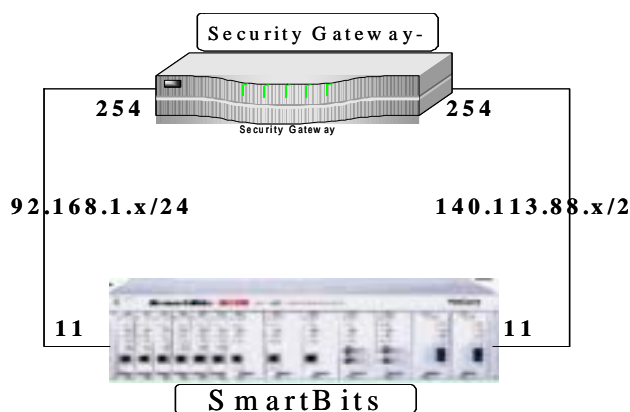
Tools (Firewall/VPN)	Description
Smartflow	Firewall/VPN measurement
WebSuite	Maximum connection/rate measurement
SmartBits 6000B	Network performance analysis test system
Tools (Intrusion Detection)	Description
Nmap	Scanning
Nessus	Exploits for the vulnerabilities
Apsend-1.61	Denial of Service
Tools (Content Filtering)	Description
WebBench	Emulates and measures Web traffic
Tools (Bandwidth Mgt.)	Description
Ncftpput	TCP traffic generator
Tcpdump	Packet sniffer
Nt	Real-time traffic bandwidth monitor

Awk script (self-written)	Data analyzer
---------------------------	---------------

表十一：是測試的項目及工具整理

### 防火牆之效能

Packet Filter 防火牆效能測試是透過 SmartBits 的一片 SmartCard 卡的兩個 port，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三種不同大小的封包(64 byte、256 byte 與 1518 byte)到模擬 Internet 上主機的卡，我們量測到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 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，本測試所定義的 Zero-loss 是封包遺失率小於 0.001%。這時 Security Gateway 的設定分別有：(1) 將 NAT 開啟及關閉；(2) 在 NAT 關閉的情況下，分別加 10 與 500 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 scalability。然而，此次所受測的機器皆預設為 Stateful Inspection，故所有受測機器在查詢多條防火牆規則時的負擔極小，或可忽略，故本測試並沒有附上此數據。



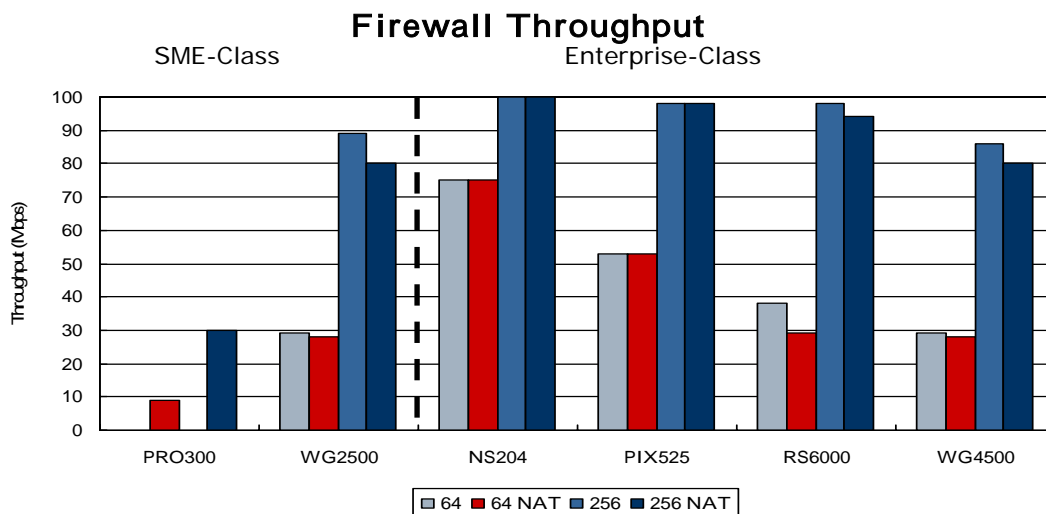
圖三：防火牆測試環境

在檢視效能比較之前，我們認為影響傳輸層防火牆效能的關鍵有下列幾項：(1) 比對防火牆規則的演算法；(3)佇列(Queue)長度；(2) 硬體規格(尤其是處理器及加速器效能)；(3) 作業系統以及協定實作的差異。

圖四 六是防火牆測試的結果。我們可以歸納下列幾點：(1)NAT 開啟後，會些微影

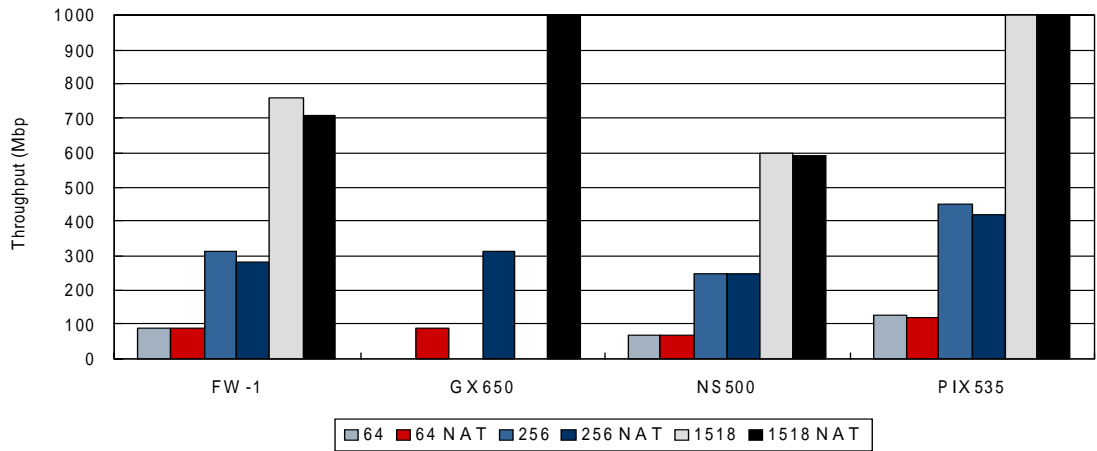
響效能；(2)較大的封包因為封包數目較少，有較佳的效能及較短的時間延遲；(3)越長的佇列長度會造成較大的時間延遲，但可能會有較高的 throughput，換言之當 throughput 與時間延遲都很高時，這表示佇列長度足以負荷大量的封包。在測試過程中，我們發現 WatchGuard 不能連續測試不同大小的封包，而必須分別獨立測試，雖然這只是測試方法的差異，但其他安全閘道器卻能夠一次測試完所有不同大小的封包。

首先要比較圖四(a)中各產品在 NAT 開啟與關閉時的效能差異(SonicWall 系統內部固定作 NAT，所以此產品沒有關閉 NAT 時的數據)。NAT 開啟時，throughput 應該會降低，而 NetScreen 204 及 Cisco PIX 525 並沒有下降，我們推測原因是這兩項產品應有較好的 NAT 演算法以及較強的硬體規格。在 SME 等級中，WatchGuard 2500 表現稱職，而 SonicWall PRO300 則差強人意；在 Enterprise 等級中，NetScreen 204 輸出可達 100%，Cisco PIX525 及 RapidStream 6000 亦相當接近 wire speed，而 WatchGuard 4500 次之。相對地，這些產品在圖五(b)及(c)的時間延遲，也較其他產品來的低。在圖四(b)中，Carrier 等級產品以 Cisco PIX 535 及 SonicWall GX650 的 throughput 表現最為出色，其次是 Check Point 及 NetScreen 500。綜觀而言，越是使用高階 CPU 及硬體加速器，效能就越出色。

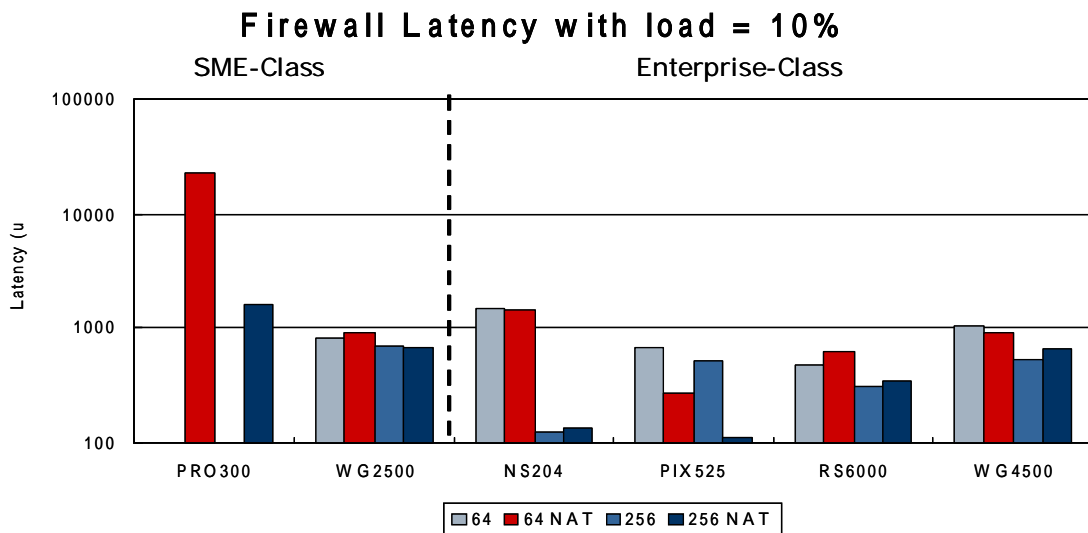


圖四(a)：NAT On/Off 時的 zero-loss maximum throughput (SME 及 Enterprise 等級)

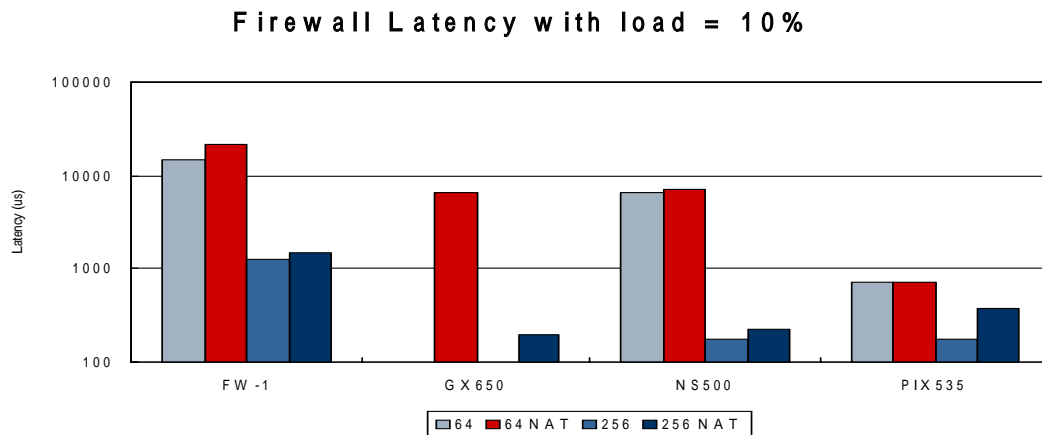
## Firewall Throughput



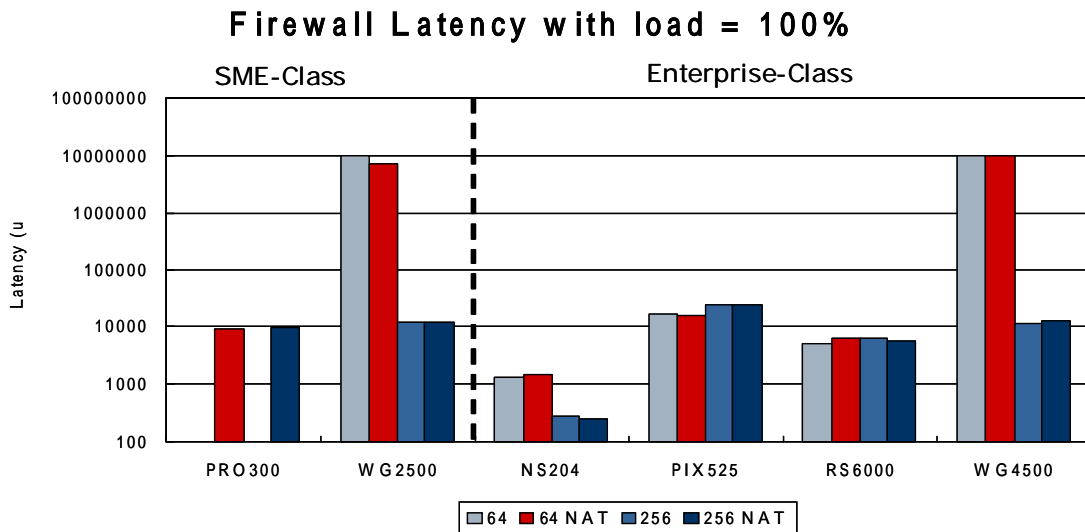
圖四(b) : NAT On/Off 時的 zero-loss maximum throughput (Carrier 等級)



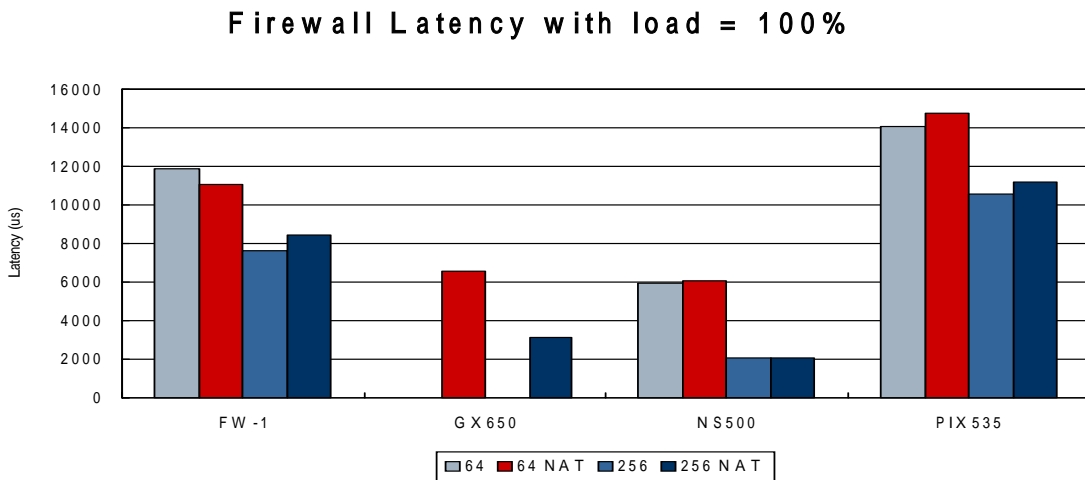
圖五(a) : Load=10%時, NAT 開啟與關閉時的 latency (SME 及 Enterprise 等級)



圖五(b) : Load=10%時, NAT 開啟與關閉時的 latency (Carrier 等級)

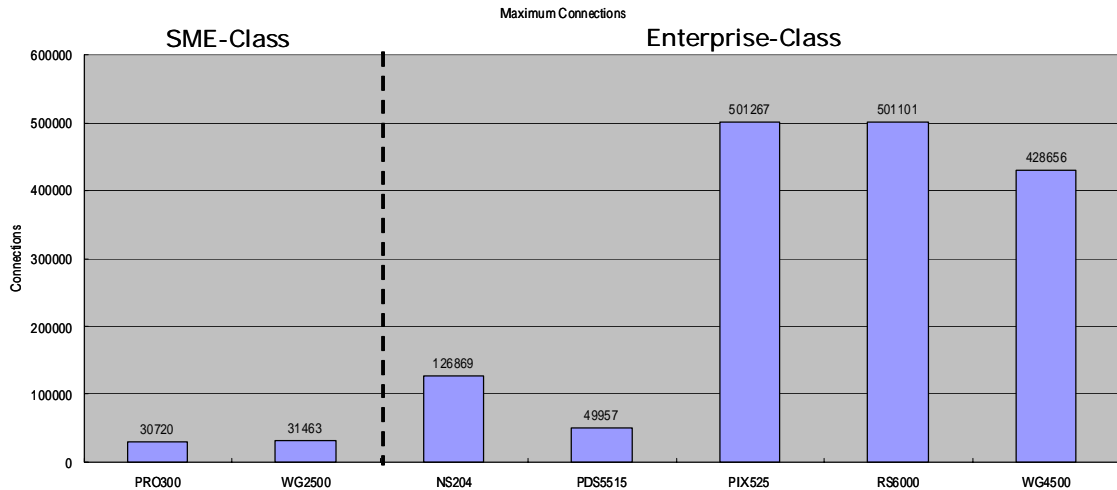


圖六(a)：Load=100%時，NAT 開啟與關閉時的 latency (SME 及 Enterprise 等級)

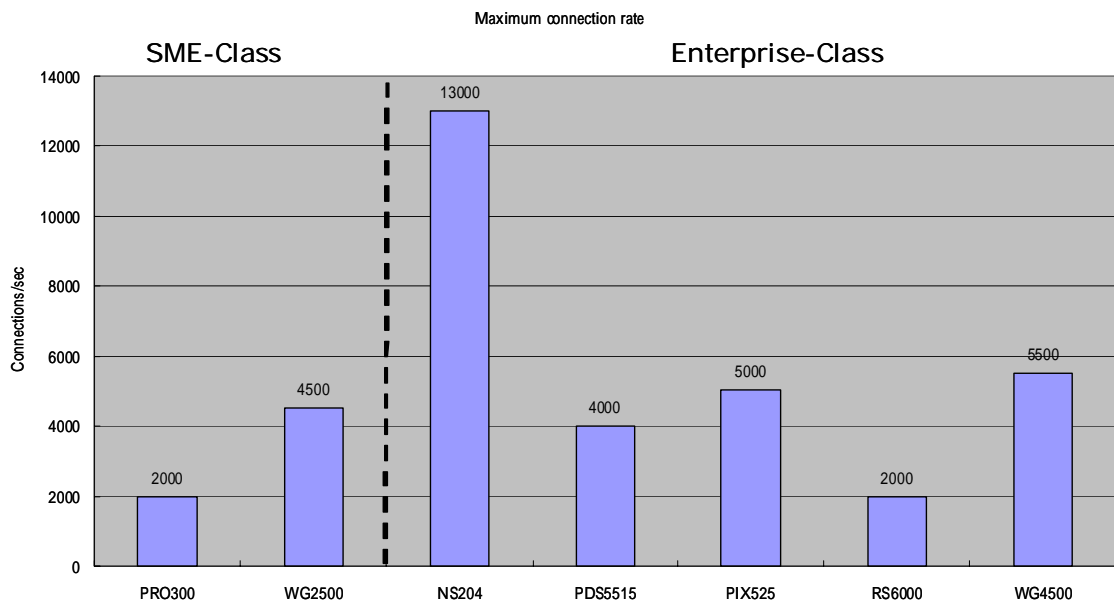


圖六(b)：Load=100%時，NAT 開啟與關閉時的 latency (Carrier 等級)

在圖七(a)測試各產品的最大連線數目，決定此數據的因素為(1)受測物內部的連線記憶空間之大小，以及(2)連線何時 timeout。我們發現 Cisco PIX 525 及 RapidStream 6000 可提供的最大連線數目最高，而 WatchGuard 4500 的次之。圖七(b)則是比較受測物建立新連線的速度(Ramp-up rate)，我們認為會影響此數據的因素為(1)CPU 處理能力、(2)連線狀態需要儲存的資訊多寡，以及(3)儲存這些連線狀態之演算法。NetScreen 204 能夠每秒建立 13,000 個新連線，極為出色。其次是 WatchGuard 4500 及 Cisco PIX 525。



圖七(a)：最大連線數目(SME 及 Enterprise 等級)



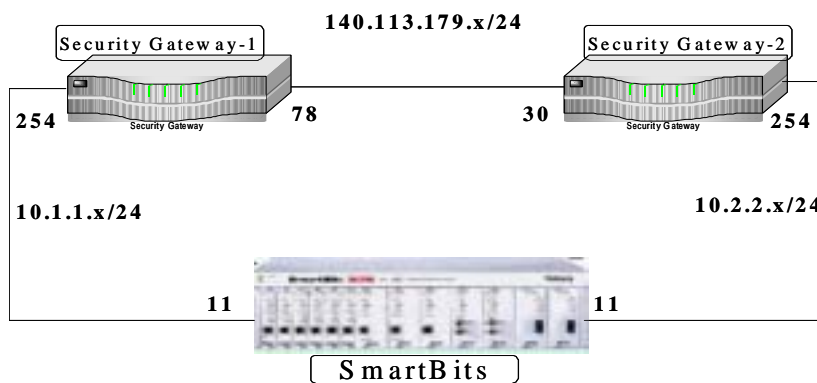
圖七(b)：建立新連線速度(SME 及 Enterprise 等級)

### VPN 之效能

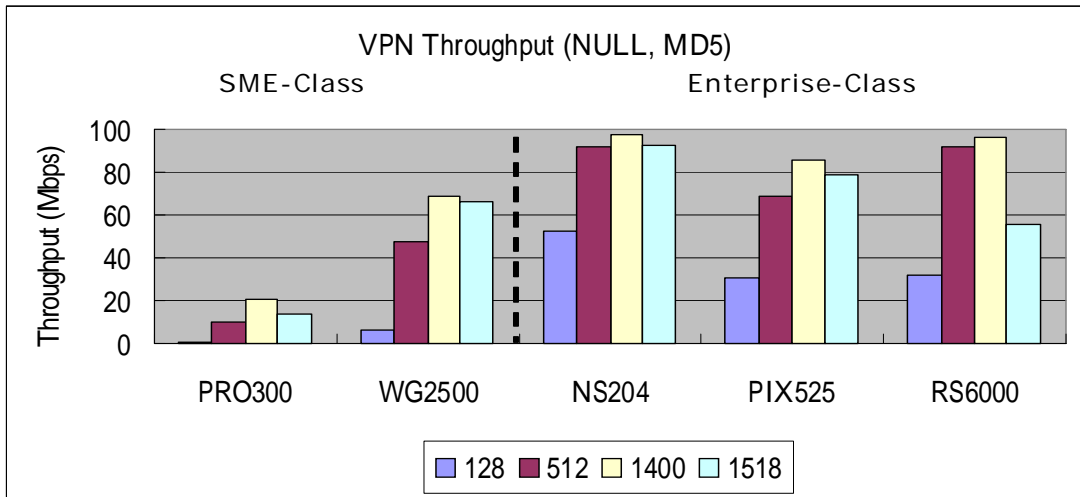
在 VPN 的測試方面，我們使用 SmartBits 的兩張 SmartCard 卡，分別模擬兩個虛擬網路的主機。如圖八所示，由其中一端分別傳送四種大小的封包(128 byte, 512 byte, 1400 byte 與 1518 byte)到另一端虛擬網路主機的 SmartMetrics Security Gateway 間的設定是用 IPSec 標準來建立通道(tunnel)，其中加密設定分別使用 NULL、DES 與 3-DES，認證設定用 MD-5 及 SHA-1，而金鑰交換方式用 Pre-share Key。其中，我們選擇觀察 128 byte 而非 64 byte 封包大小的原因是，當封包過小時，SonicWall PRO300 無法觀察到數據，而且 64 bytes

的 IPSec 封包代表。另一方面，傳送 1518 byte 的封包是因為經過 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。最末，我們的主要的測試結果是各產品的無封包遺失最大輸出效能與不同的傳輸負荷下之封包延遲。

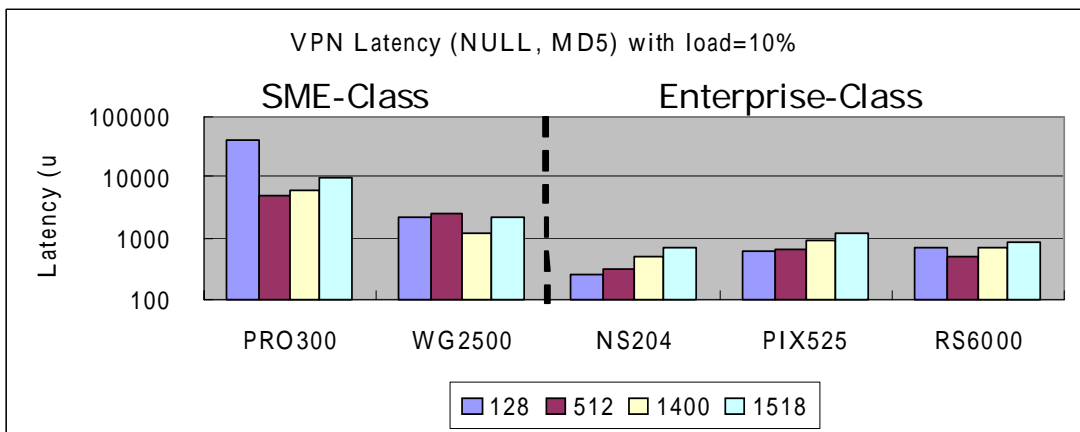
此項測試中，使用三種加密/認證測試搭配，包括 NULL/MD5、DES/MD5，以及 3DES/SHA-1。我們有作 ESP，NULL/MD5 之測試，原因是加密屬於 processor-intensive 的處理，VPN 還是有僅作封包認證的需求，所以 SME/Enterprise 等級產品有 NULL/MD5 之 VPN 效能比較，但 Carrier 等級產品不比較 NULL/MD5 是因為應該不會有 ISP 會拿 Carrier 等級產品用在建立單純的 NULL/MD5 VPN tunnel。圖九(a)是四種大小封包在不使用任何加密法，單純用 MD5 認證時的 zero-loss maximum throughput。NetScreen 204 與 RapidStream 6000 表現最好，近乎 100%的 VPN 效能，但 RapidStream 6000 在 1518 byte 經過切割的封包處理上，沒有處理很好。在圖九(b)我們發現硬體規格較差的產品，其時間延遲普遍較高。



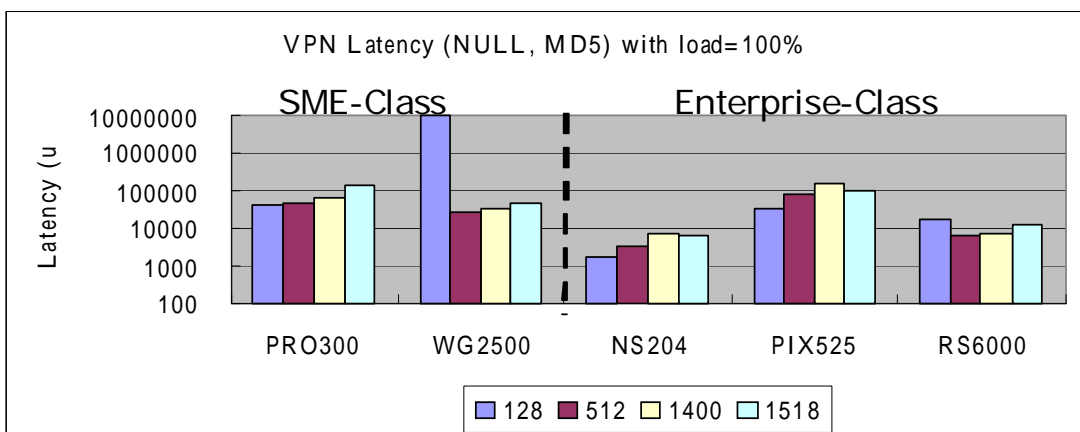
圖八：VPN 測試環境



圖九(a)：使用 NULL/MD5 之 VPN zero-loss 最大 throughput (SME 及 Enterprise 等級)



圖九(b)：Load=10%時，使用 NULL/MD5 之 VPN latency (SME 及 Enterprise 等級)

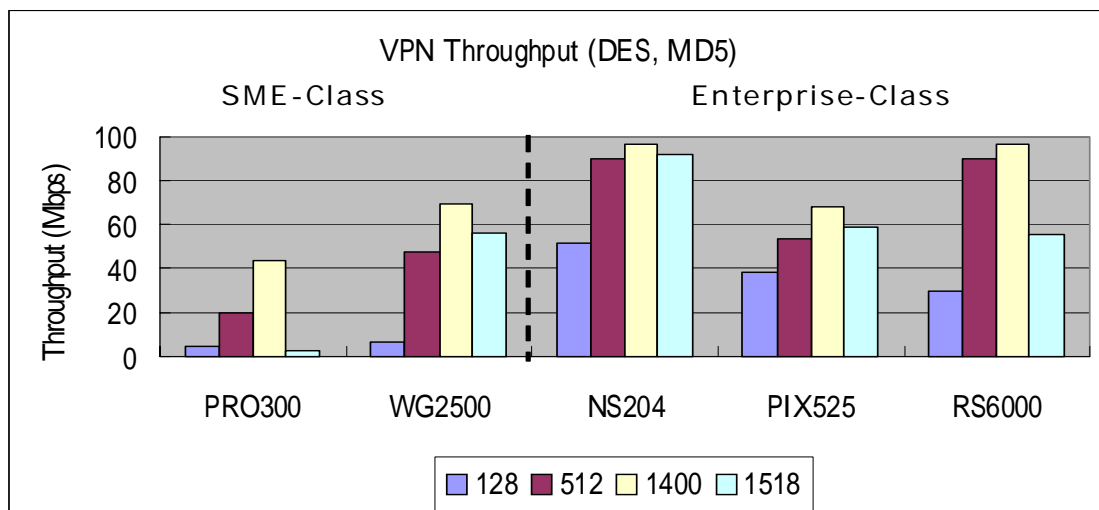


圖九(c)：Load=100%時，使用 NULL/MD5 之 VPN latency (SME 及 Enterprise 等級)

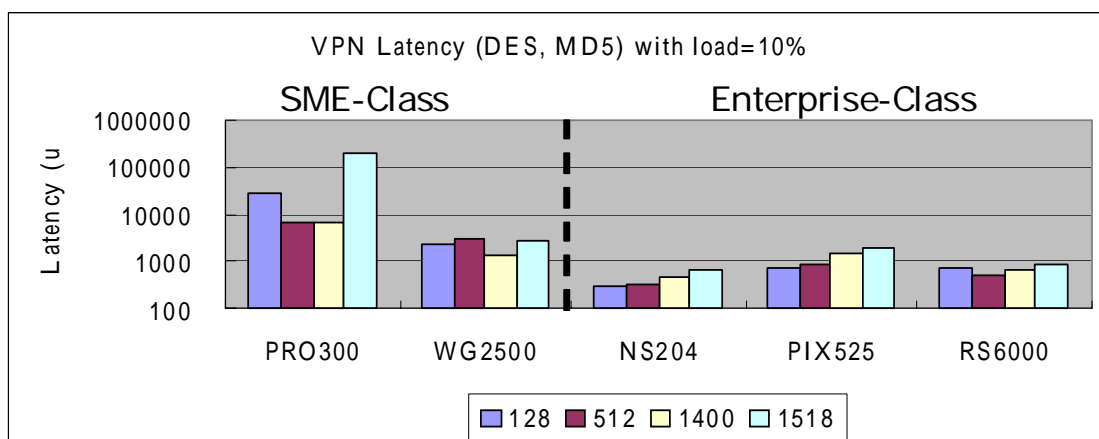
VPN 技術最耗費時間的工作在於用 DES 或 3-DES 加解密，因為加解密的演算法是固定標準，所以會影響效能的主要是 CPU 的等級以及有無硬體加速。在圖十(a)~(c)是 SME

及 Enterprise 等級產品的 DES 加密 VPN 效能，而圖十二(a)~(c)是 3DES 加密。我們發現 NetScreen 204 和 RapidStream 6000 的 throughput 較高，時間延遲較低。其次是 Cisco PIX 525。就 SME 等級產品而言，WatchGuard 2500 表現出色，而 SonicWall 雖有 VPN 加速卡，然而效能不夠好的原因應該是 CPU 等級較低。

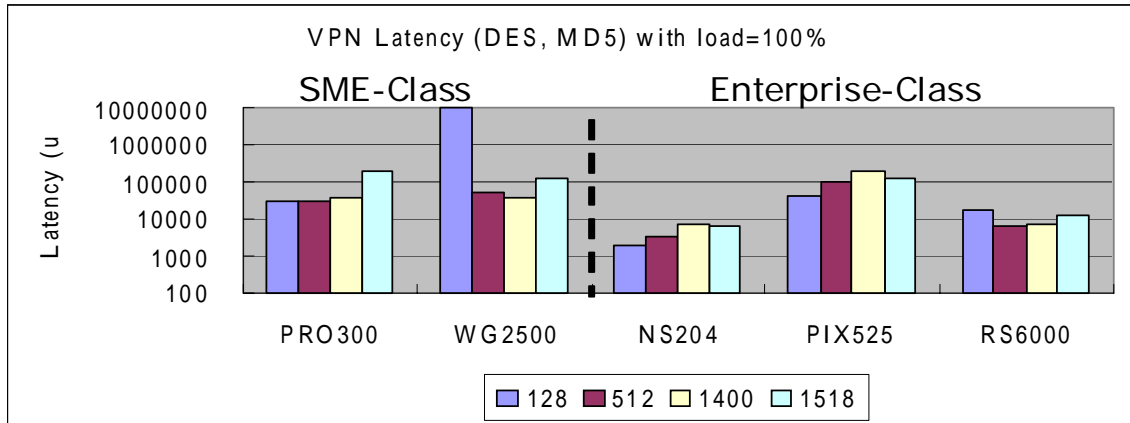
在圖十一(a)~(c)Carrier 等級產品的 DES 加密 VPN 效能，以及圖十三(a)~(c)的 3DES 加密 VPN 效能，我們發現 SonicWall GX650 的表現最佳，其次是 NetScreen 500。Check Point 廠商則向我們表示，其安裝於 Dell 硬體的 Check Point VPN-1/Firewall-1 NG 軟體，並沒有啟動 IPSec 加速卡。



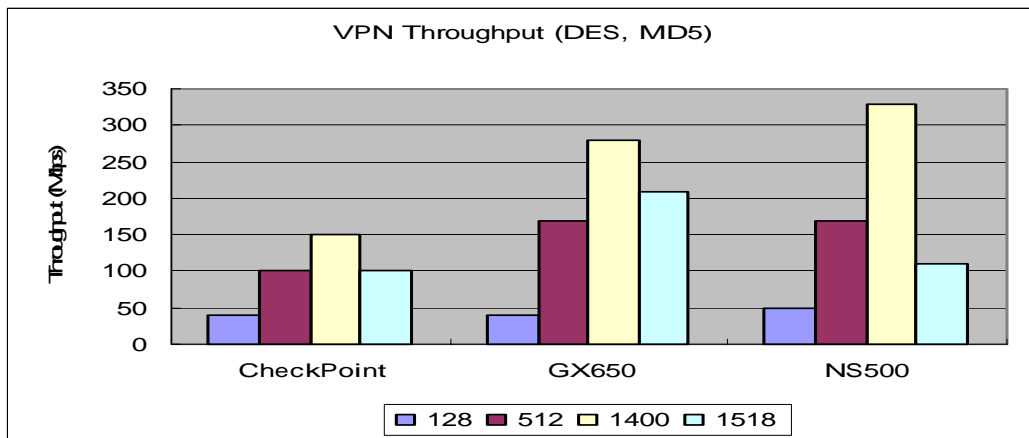
圖十(a)：使用 DES/MD5 之 VPN zero-loss 最大 throughput (SME 及 Enterprise 等級)



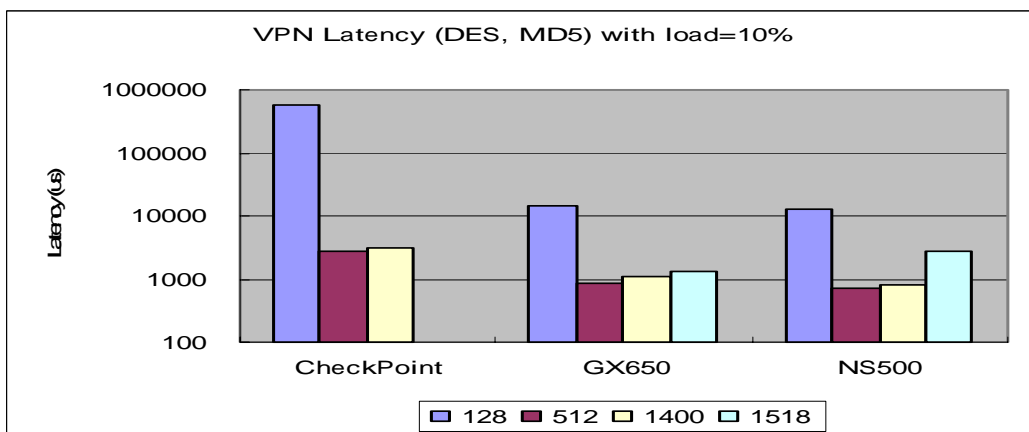
圖十(c)：Load=10%時，使用 DES/MD5 之 VPN latency (SME 及 Enterprise 等級)



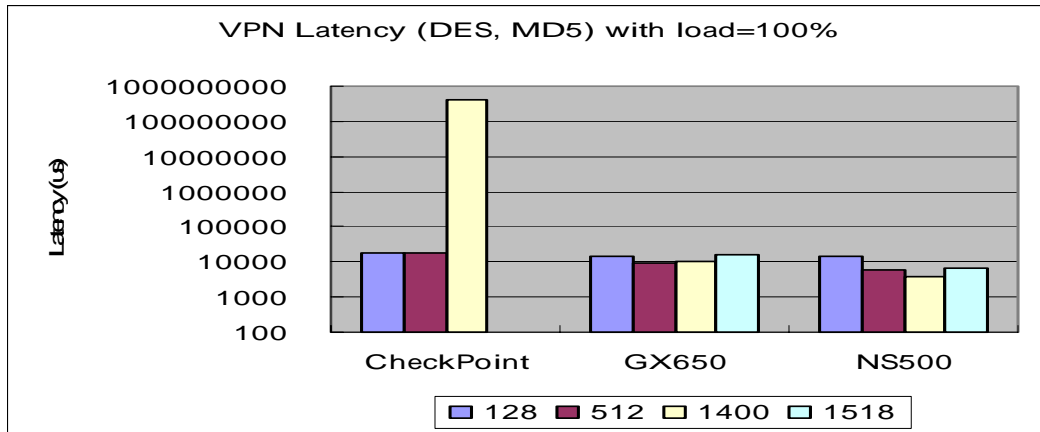
圖十(d)：Load=100%時，使用 DES/MD5 之 VPN latency (SME 及 Enterprise 等級)



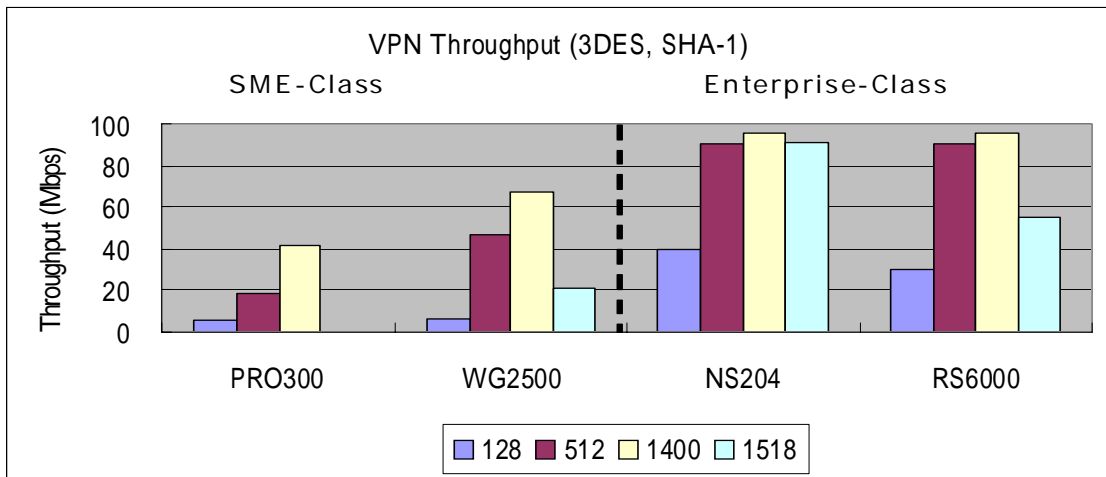
圖十一(a)：使用 DES/MD5 之 VPN zero-loss 最大 throughput (Carrier 等級)



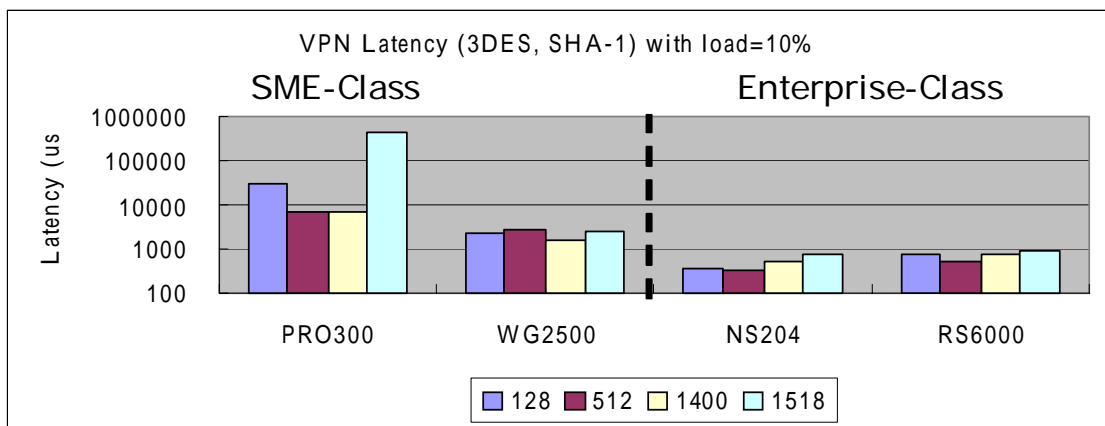
圖十一(b)：Load=10%時，使用 DES/MD5 之 VPN latency (Carrier 等級)



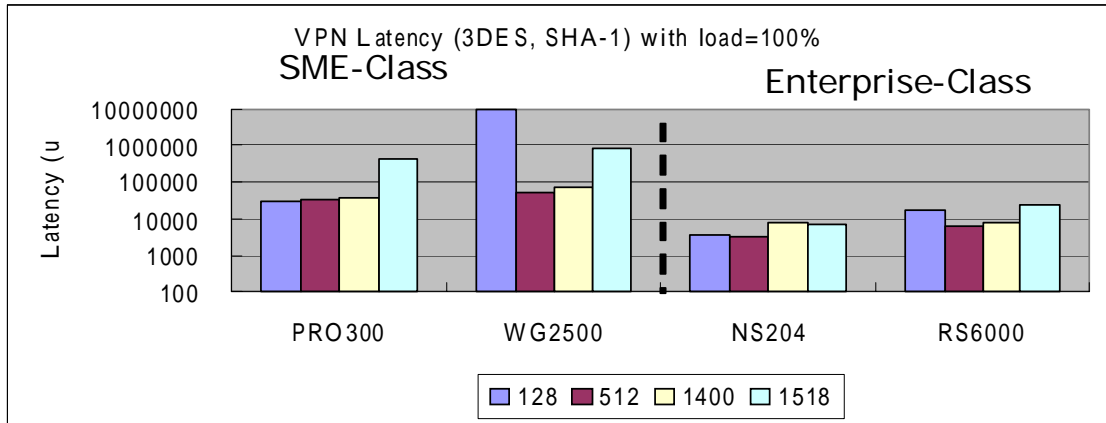
圖十一(c) : Load=100%時，使用 DES/MD5 之 VPN latency (Carrier 等級)



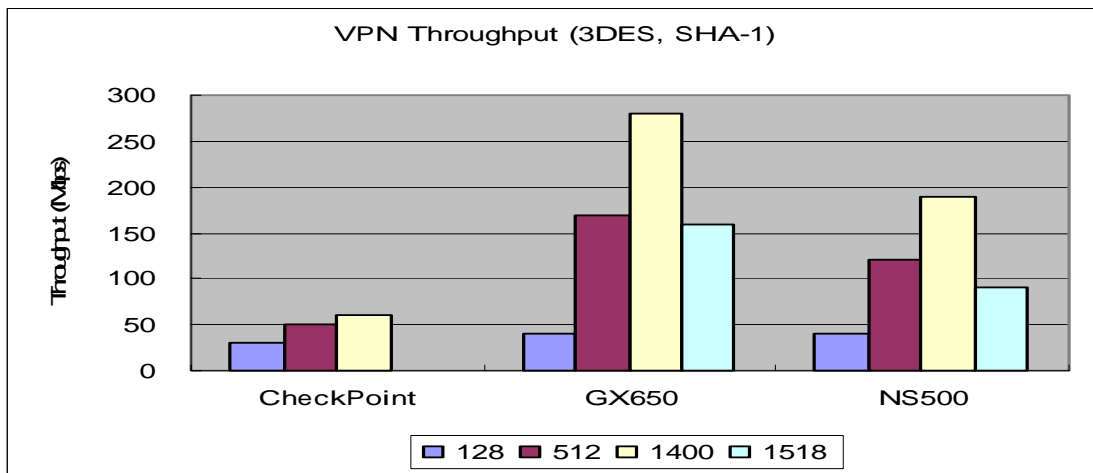
圖十二(a) : 使用 3DES/SHA-1 之 VPN zero-loss 最大 throughput (SME 及 Enterprise 等級)



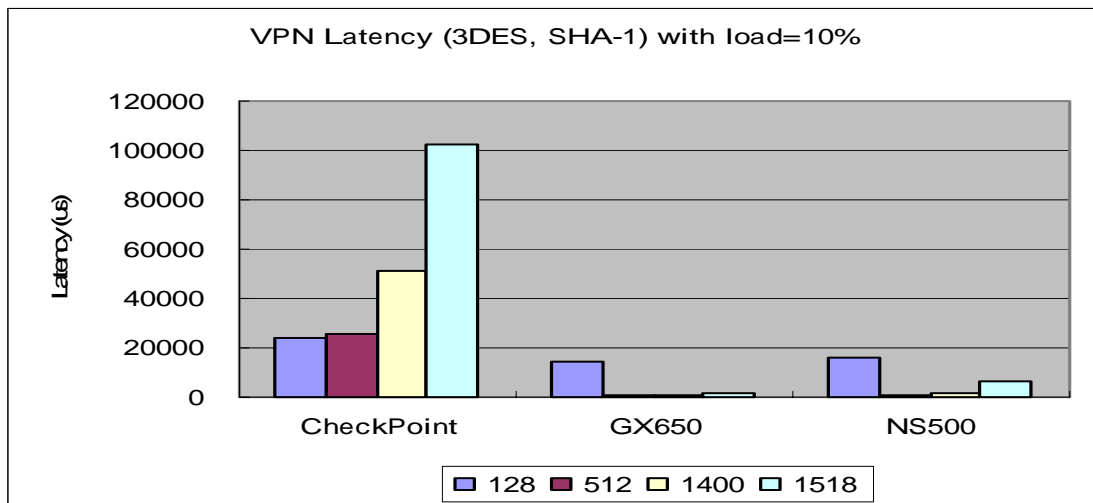
圖十二(b) : Load=10%時，使用 3DES/SHA-1 之 VPN latency (SME 及 Enterprise 等級)



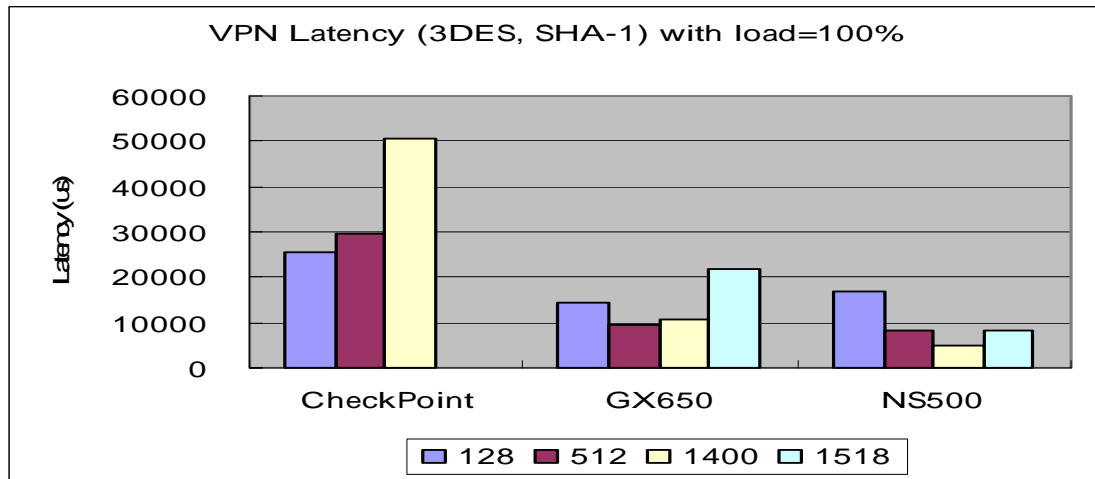
圖十二(c) : Load=100%時，使用 3DES/SHA-1 之 VPN latency (SME 及 Enterprise 等級)



圖十三(a) : 使用 3DES/SHA-1 之 VPN zero-loss 最大 throughput (Carrier 等級)



圖十三(b) : Load=10%時，使用 3DES/SHA-1 之 VPN latency (Carrier 等級)

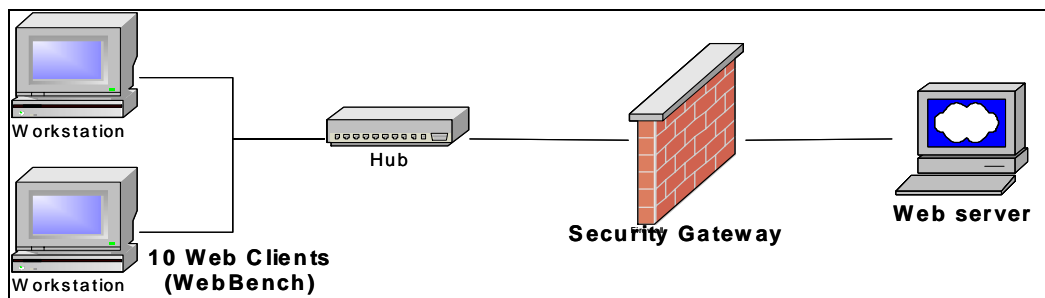


圖十三(c)：Load=100%時，使用 3DES/SHA-1 之 VPN latency (Carrier 等級)

### 內容過濾之效能

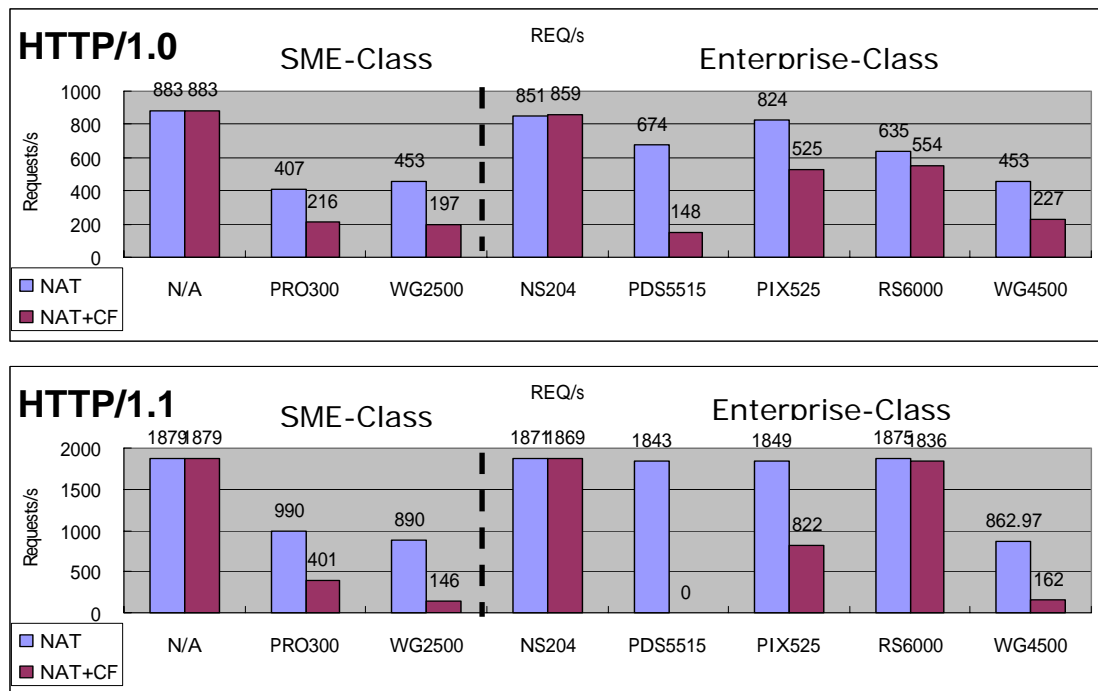
在應用層防火牆的測試方面，一般提供 URL-blocking 與 Content-Filtering 兩種功能，而典型的 Content-Filtering 能夠阻擋 Java/JavaScript/ActiveX 等物件。我們挑選所有受測機器都可阻擋的 Java 物件進行測試。本項目並沒有測試 Carrier 等級產品是因為一個 client 僅能產生約 10 Mbps 的網頁流量，要達到 1 Gbps 的流量會需要上百台的工業級電腦。

首先，圖十四是內容過濾的測試環境，我們用 WebBench clients 送出多個 HTTP request 的封包，並使得 HTTP 的封包在通過 Security Gateway 後送往 Web Server，再由 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)僅有 NAT 開啟(目的在於瞭解數據的基準值)；(2) NAT 及 Content Filter 同時開啟兩種情形，藉以觀察啟用或不啟用 Content Filtering 時對防火牆效能的影響。HTTP/1.0 主要測試的是 Content Filtering 啟用後對 request rate 所造成的影響；HTTP/1.1 則是測試啟用 Content Filter 後對 throughput 所造成的影響。

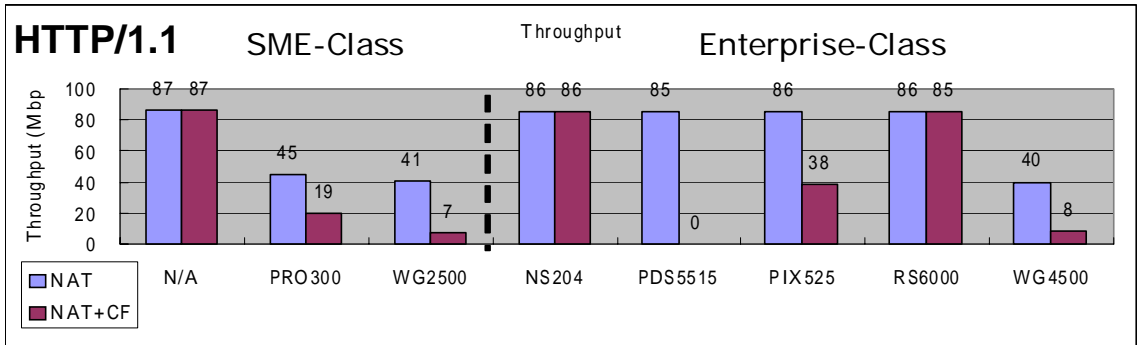
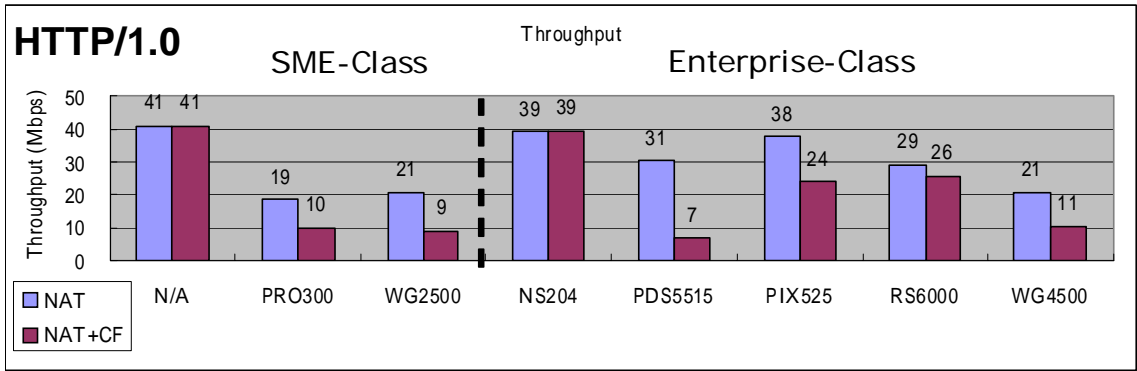


圖十四：內容過濾測試環境

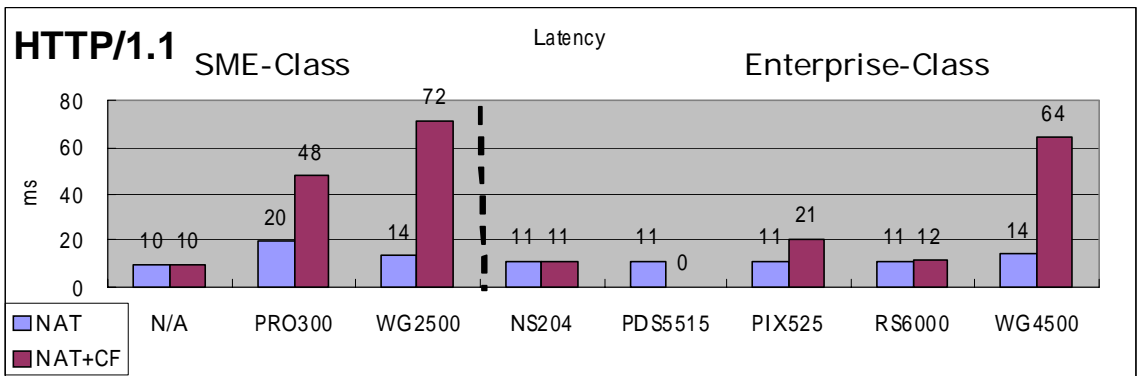
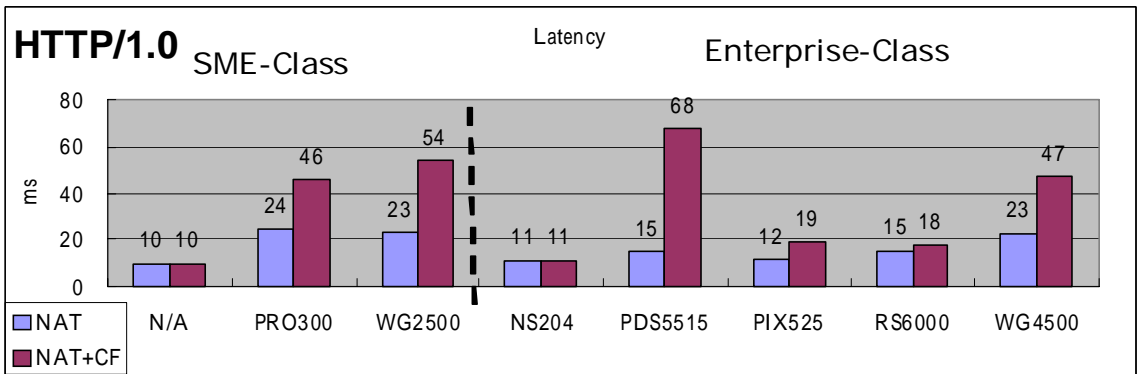
大部份的產品在測試只啟用 NAT 與同時啟用 NAT 和 content filter 可以明顯的看出 Content Filter 對其效能的影響。在圖十五 十七中，N/A 一欄的數據是 20 台 WebBench clients 所能產生的的效能上限，其中上方的圖是 HTTP/1.0，下方的圖是 HTTP/1.1。我們發現一個比較有趣的現象是功能做的愈完善的 Content Filter，其效能表現較差。測試結果是 NetScreen 的表現最為出色，開啟 Content-Filtering 後，仍十分接近 100%的效能，其次是 Cisco 及 RapidStream。但對照表九這三項產品的內容過濾功能較陽春。由於內容過濾屬於應用層處理，配備較好的 CPU 等級之產品，應有較高的內容過濾效能。最末，我們發現各廠商在內容過濾的實際作法略有差異，Cisco 產品會解析 html 檔案的 payload，而其他產品則是單純從 header 阻擋物件。



圖十五: Web clients 經過安全閘道器過濾至 Web server 的 Request Rate (SME 及 Enterprise 等級)



圖十六：Web clients 經過安全閘道器過濾至 Web server 的 Throughput (SME 及 Enterprise 等級)

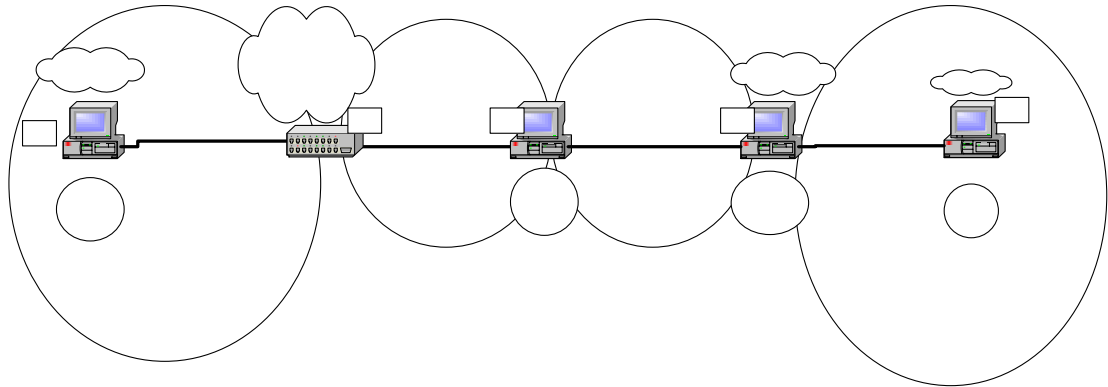


圖十七：Web clients 經過安全閘道器過濾至 Web server 的 Latency (SME 及 Enterprise 等級)

### 頻寬管理之效能

有關頻寬管理之測試平台與測試方法的細節是本節的重點，其重要性關係到測得的

數據，如圖十八所示，測試時資料流由 X → Y，為公平起見，所有測試皆在此平台上（同一時間僅一受測物啟動）。



圖十八：測試平台實體連接圖

測試項目	說明	比較標準	優劣評判
準確性	測試 5 次，各 class 「實際量測到」與「給定」的頻寬是否相符。	normalized goodput (註 1)，5 次取平均	越接近 1 越好
公平性	測試 5 次，各 class 中 4 連線之間（共 5 class，20 條連線）頻寬搶食之公平性。	CoV of goodputs among 4 connections in each class，5 次取平均	越接近 0 越好
重傳率	各 class 中封包重傳率。	重傳數/送出數，5 次取平均	越接近 0 越好

註 1：Goodput 為『有效輸出』(bytes\_sent/time)，意即因封包遺失導致 TCP 重傳者不計入有效輸出。

註 2：CoV 為 Coefficient of Variation，意即 standard deviation (標準差) 除以 mean (平均數)。

表十二：頻寬管理測試項目說明

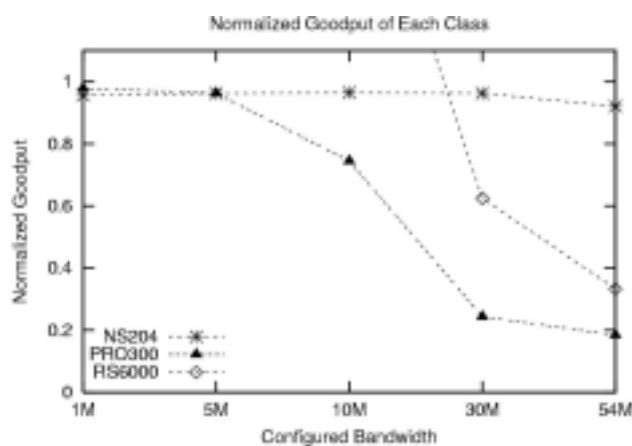
1. 受測物設定：設定對外專線的頻寬為 10Mbps 與 100Mbps，在此兩種 link 頻寬下各分為 5 種 class，比例同為 1:5:10:30:54（總共 100）。這些設定都是「固定式」的，沒有「互借頻寬」的設定，以彰顯其準確度。

2. 測試方法：由 A → I 灌入 20 個 FTP 資料流（每個 class 各 4 個）並由 tcpdump 收集資料，250 秒後 kill 掉所有的 ncftpput，取其中 20~30 秒資料作分析；分析完後等待 200 秒，重複以上過程共 5 次。表十二是列表測試項目及說明。

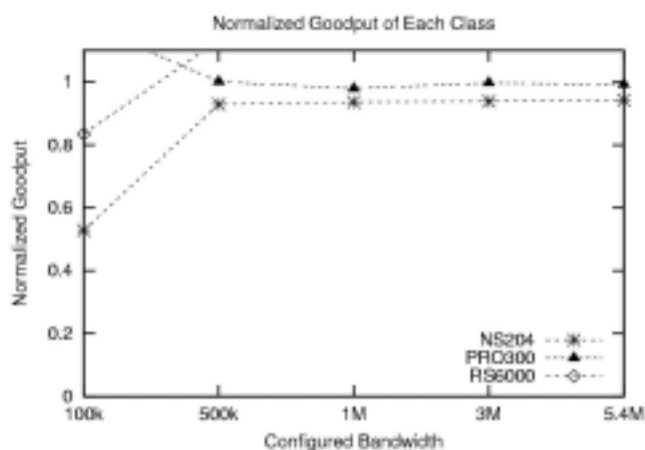
### 頻寬管理之「準確性」

由圖十九(a)及(b)的測試結果得知，NetScreen 204 在各種 link、各種群組設定下（除 10Mbps 下 100k 群組外）皆算準確；SonicWALL PRO 300 在 10Mbps link 下準確性甚高（除 100k 群組外），但在設定 WAN 頻寬為 100Mbps 時，由於最高的轉送速度降為只有 30Mbps，在將其分為 1M、5M、10M、30M、54M 後，越高頻寬的群組越不準。RapidStream 6000 在控制 WAN 頻寬為 100Mbps 時，各群組幾乎完全沒有管理，20 條連線幾乎得到相同的待遇（每個連線幾乎都為 100/20=5Mbps），因此各 class 都得到約 20Mbps，完全不準；

在 10Mbps 時，頻寬稍微準些，但都高出來 20%左右（除了 100kbps 外）



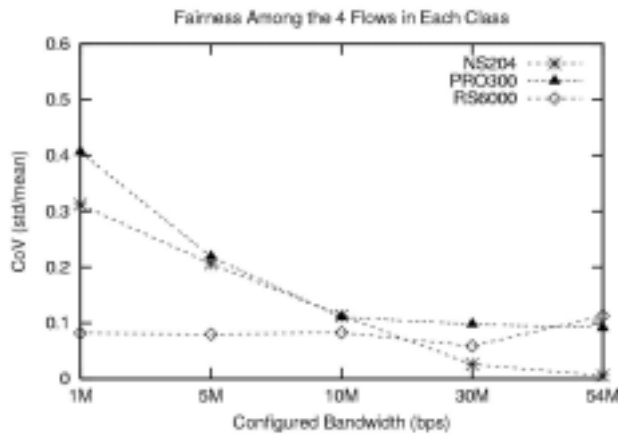
圖十九(a)：準確性測試結果(100 Mbps 對外專線)



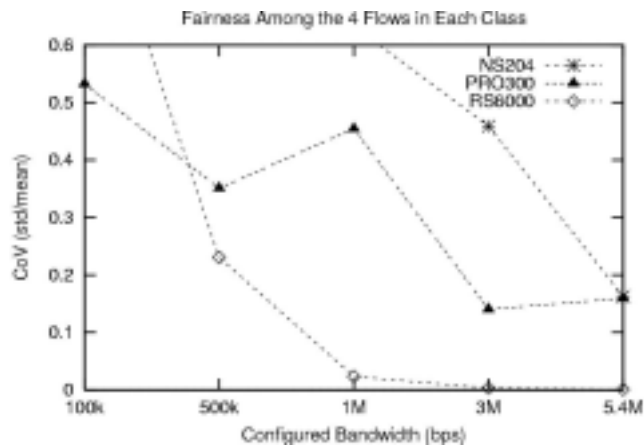
圖十九(b)：準確性測試結果(10 Mbps 對外專線)

### 頻寬管理之「公平性」與「公平性的穩定度」

由於 NetScreen、SonicWall、RapidStream 都尚無控制頻寬到連線的精確度，公平性自然較差。在圖二十(a)中特別要說的是 RapidStream 6000 在 100Mbps 下因如前述不準情況導致 20 條連線幾乎搶食同等頻寬，乍看之下公平性極佳，事實上其數據不具意義。而圖二十(b)為 10Mbps，低頻寬使搶奪頻寬的情況更為激烈，RapidStream 6000 在 1M、3M、5.4M 較佳，NetScreen 204 和 SonicWall RPO 300 則公平性較差。



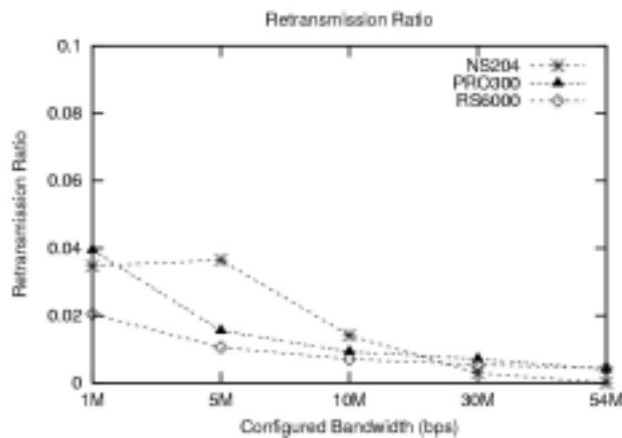
圖二十(a)：公平性測試結果(100 Mbps 對外專線)



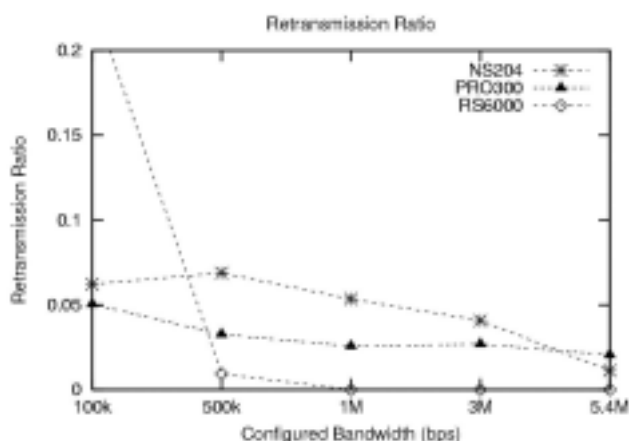
圖二十(b)：公平性測試結果(10 Mbps 對外專線)

**頻寬管理之重傳率：各 class 中封包重傳率。**

於圖二十一(a)及(b)中可見 RapidStream 6000 除了在低頻寬 100kbps 重傳率較高之外，其他頻寬的重傳率都維持很低，可能是因為有較大的 buffer，使 buffer overflow 情況較輕微；其次是 SonicWall PRO 300。



圖二十一(a)：重傳率測試結果(100 Mbps 對外專線)



圖二十一(b)：重傳率測試結果(10 Mbps 對外專線)

## 五、總結評比

對於測試報告的結論，我們對所有比較的功能與效能作十二項指標評分，滿分為 5 顆星。每項指標的評分，是依據前面的功能及效能比較結果作評比，其中管理簡易度較為主觀，是所有測試人員在操作過七家廠商十一項產品的管理介面後，所給予的評分之平均值；而價值比(Value-to-Price)的計算，是將前十一項指標加總後，對照各產品的國內售價，然後所有測試人員進行投票所決定的。對同一廠商但不同等級的產品功能評分，有時候會有一些差異，主要是考慮其在該等級的競爭力。

在 SME 等級中，SonicWall PRO300(共 40 顆星)及 WatchGuard 2500(共 43 顆星)屬於「四星級優良產品」。在 Enterprise 等級 NetScreen 204(共 56 顆星)及 RapidStream 6000(共 50 顆星)屬於「五星級傑出產品」，Intrusion PDS5515(共 41.5 顆星)、WatchGuard 4500(共 41.5 顆星)，以及 Cisco PIX 525(共 39.5 顆星)屬「四星級優良產品」。在 Carrier 等級 NetScreen 500(共 45 顆星)屬於「五星級傑出產品」，Check Point FW-1 NG (Dell) (共 41.5 顆星)及 SonicWall GX650(共 40.5 顆星)屬於「四星級優良產品」。

Model	基本系統功能			
	Ease-of-Use	Log Reporting	Interoperability	Security Rating
SonicWall PRO300	★★★★	★★★★	★★★★★	★★★★
WatchGuard 2500	★★★★★	★★★★	★★★★★	★★★★★
	基本防火牆功能及效能			
	Firewall Func.	Firewall Perform.	VPN Func.	VPN Perform.
SonicWall PRO300	★★★★	★★	★★★★★	★★★
WatchGuard 2500	★★★★★	★★★★★	★★★★★	★★★★★
	附加價值功能及效能			
	C.F. Func.	C.F. Perform.	Bandwidth Mgt.	Value-to-Price
SonicWall PRO300	★★★★	★★★★	★★	★★★★

WatchGuard 2500	★★★★★	★★★	N/A	★★★★
-----------------	-------	-----	-----	------

表十三：中小企業(SME)等級安全閘道器之總評

Model	基本系統功能			
	Ease-of-Use	Log Reporting	Interoperability	Security Rating
Cisco PIX525	★★★★↓	★★★★↓	★★★★★↓	★★★
Intrusion PDS5515	★★★★	★★★★	★★★★★↓	★★★★↓
NetScreen 204	★★★★	★★★★★↓	★★★★★	★★★★★
RapidStream 6000	★★★★★	★★★★★	★★★★★↓	★★★★↓
WatchGuard 4500	★★★★★	★★★★↓	★★★★★	★★★★★↓
	基本防火牆功能及效能			
	Firewall Func.	Firewall Perform.	VPN Func.	VPN Perform.
Cisco PIX525	★★★★★	★★★★★↓	★★★	★★★
Intrusion PDS5515	★★★★★	★★★★★↓	★★★★★	N/A
NetScreen 204	★★★★★	★★★★★	★★★★★	★★★★★
RapidStream 6000	★★★★	★★★★★	★★★★★↓	★★★★★
WatchGuard 4500	★★★★	★★★★	★★★★	N/A
	附加價值功能及效能			
	C.F. Func.	C.F. Perform.	Bandwidth Mgt.	Value-to-Price
Cisco PIX525	★★★★↓	★★★★↓	N/A	★★★↓
Intrusion PDS5515	★★★★★↓	★★★↓	Not Tested (Optional)	★★★★★
NetScreen 204	★★★★↓	★★★★★	★★★★★	★★★★★
RapidStream 6000	★★★	★★★★	★↓	★★★★★
WatchGuard 4500	★★★★★	★★★↓	N/A	★★★★★

表十四：企業(Enterprise)等級安全閘道器之總評

Model	基本系統功能			
	Ease-of-Use	Log Reporting	Interoperability	Security Rating
Check Point (Dell)	★★★★	★★★★	★★★★★↓	★★★
Cisco PIX535	★★★★↓	★★★★↓	★★★★★↓	★★★
NetScreen 500	★★★★	★★★★★↓	★★★★★	★★★★★
SonicWall GX650	★★★★↓	★★★★↓	★★★★★↓	★★★
	基本防火牆功能及效能			
	Firewall Func.	Firewall Perform.	VPN Func.	VPN Perform.
Check Point (Dell)	★★★★★	★★★★	★★★★★	★★★↓
Cisco PIX535	★★★★★	★★★★★	★★★	N/A
NetScreen 500	★★★★★	★★★★	★★★★★	★★★★★
SonicWall GX650	★★★★	★★★★★↓	★★★★	★★★★★
	附加價值功能及效能			
	C.F. Func.	C.F. Perform.	Bandwidth Mgt.	Value-to-Price
Check Point (Dell)	★★★★★↓	Not Tested	Not Tested (Optional)	★★★★★↓
Cisco PIX535	★★★★↓	Not Tested	N/A	★★★★↓
NetScreen 500	★★★★↓	Not Tested	Not Tested	★★★★★↓
SonicWall GX650	★★★★	Not Tested	Not Tested	★★★★★↓

表十五：電信(Carrier)等級安全閘道器之總評

## 六、參考文獻

## 廠商

[1] Check Point, <http://www.checkpoint.com>

[2] Cisco, <http://www.cisco.com>

[3] Intrusion, <http://www.intrusion.com>

[4] NetScreen, <http://www.netscreen.com>

[5] Nokia, <http://www.nokia.com>

[6] SonicWall, <http://www.sonicwall.com>

[7] Symantec, <http://www.symantec.com>

[8] WatchGuard, <http://www.watchguard.com>

## 工具

[9] SmartBits, <http://www.netcomsystems.com>

[10] Nmap, <http://www.nmap.org>

[11] Nessus, <http://www.nessus.org>

[12] apsend, <http://linuxberg.tele.net/files/apsend-1.61.tar.gz>

[13] hping, <http://www.hping.org/hping2.0.0-rc1.tar.gz>

[14] ncftpput, <http://www.ncftp.com>

[15] ttt, <http://www.csl.sony.co.jp/~kjc>

[16] SmartVoIPQoS, <http://www.netcomsystems.com>

[17] tcpdump, <http://www-nrg.ee.lbl.gov>

## 其他

[18] ICSA, <http://www.icsa.net>

[19] CheckMark, <http://www.westcoast.com>

[20] ISO 15408, <http://csrc.nist.gov/cc/ccv20/ccv2list.htm>

## **廠商回應**

### **Check Point and Intrusion (Check Point 原廠回應)**

精誠公司僅代表 Check Point 原廠向網路通訊雜誌、交通大學資訊科學所林盈達教授等全體測試成員，針對舉辦本次安全閘道器測試活動所展現專業性，以及在測試期間所提供的協助，表達由衷的感謝。

由於 Check Point VPN-1/Firewall-1 NG 有許多重要的功能並被未列入測試項目，因此我們針對本次測試內容與結果，有下列補充：

礙於時間的因素，測試單位無法對 Check Point VPN-1/Firewall-1 進行全面完整的測試，相當可惜。

Check Point VPN-1/Firewall-1 擁有許多其他產品所沒有的功能，因此在評比方面無法突顯 Check Point 產品特色與價值，如：(i). One-Click VPN、(ii). Extranet Manager、(iii) Internal Certificate Authority、(iv) SecureClient Desktop Security、(v). High Availability for Manager Server、(vi). Support for multiple hardware and OS Platform 等等，這些功能對於 Firewall/VPN 的管理便利性與擴充性來說是相當重要的

Check Point 協力廠商所研發 Intrusion PDS 7315 以及 Nokia IP740 等電信等級的 Multi-Gigabit 硬體防火牆雖未能參與本次測試，但 Check Point 僅以軟體之姿，在搭配一般企業內最常見的 Intel-base Server 的情況下，效能即已直逼其他廠牌的電信等級防火牆。此點證明 Check Point VPN-1/Firewall-1 本身，以及與協力廠商整合的硬體平台 (Appliance)在效能方面絕對足以與其他競爭者匹敵。

最後，再次感謝所有參與本次測試的全體工作人員。

### **Cisco (代理商聚碩科技回應)**

思科系統完整的全方位資訊完全解決方案 SAFE 一直秉持著對顧客的承諾，提供一個真正符合使用者需求且兼具效能與彈性的網路安全架構及安全政策管理方案，而非單一 BOX 的產品。防火牆是思科資安解決方案的重要成員，思科 PIX 防火牆承襲了思科解決方案的優點，具備效能高、功能強大豐富，以及與整體資安解決方案的高度整合性……等等特性，而且兼顧成本效益。

這次由交大林盈達教授指導的『網路安全閘道器產品評比』中，便證明了上述思科 PIX 防火牆的優勢。在評比中的「效能比較」一項中，思科 PIX525 與 PIX535 防火牆是所有參予評比的防火牆中效能最優異的。最大連線數的評比中，思科 PIX525 防火牆可支援 50 萬以上 (501,267) 的連線，居所有參予評比防火牆之冠。此外，思科 PIX 防火牆更能與思科整體資安解決方案的其他成員例如入侵偵測系統作完全的整合。

#### ***NetScreen (原廠亞太區銷售副總張韓生回應)***

連續兩年，NetScreen 的產品再次榮獲 ConnectTimes 網路安全閘道器產品評比的五顆星最高評級，進一步肯定 NetScreen 在確保速率效能的同時，能為用戶提供最卓越的彈性擴展能力、功能優化及操作簡易性。

在這次測試，NetScreen-204 和 NetScreen-500 兩款產品皆在其級別中問冠，確立 NetScreen 擁有最全面化產品系列的科技，同樣能為企業及電信級研創最高階專屬的安全方案。每款 NetScreen 基於 ASIC 的產品具備核心的安全功能，包括防火牆、VPN 和 DoS 的保護。自推出以來，NetScreen-204 和 NetScreen-500 已在美國榮獲多個獎項，今天我們更在亞洲區及台灣獲得同樣的評價。NetScreen 將繼續技術創新，為企業體及服務供應商提供最卓越的安全解決方案，滿足現今最嚴苛的網路需求。

#### ***RapidStream (代理商新達電腦回應)***

網際網路高度發展，對網路安全之需求與重視也日趨殷切。一般使用者對於建置本身網路(資訊)安全時，如何適切地評估產品則普遍被列為重要議題。幸運地，由國立交通大學網路測試中心針對國內網路安全產品供應商(代理商)所提供之設備做了相當客觀及公正的測試，並將所測結果清楚的刊登，對重視網路安全的企業或機關有極高的參考價值。

#### ***SonicWall (原廠大中華區域經理 Roger Luk 回應)***

很高興能受邀請參加網路安全閘道器產品評比。這次 SonicWALL 公司參加測試表現最突出的產品 GX 650 在這次受測產品中 3DES VPN 達到最高效能的機型，很可惜的是另一高效能企業級產品 GX2500 並未被列入這次受測邀請中，實屬美中不足。

SonicWALL firewall 以其最佳價格效能比的產品線，受到廣大寬頻上網用戶採用，全

球出貨已高達 25 萬部, 另外 SonicWALL 防火牆的穩定性亦是用戶感覺最滿意的地方, SonicWALL GX 系列是 SonicWALL 以高流量及高頻寬用戶需求為目標, 目前在台灣也有重要政府單位與企業採用並且非常滿意其效能表現。

### ***WatchGuard (代理商泓彥資訊回應)***

WatchGuard 雖然 focus 在中小型企業市場, 不過為了提供更完整的網路安全解決方案, 因此提供了完整的 VPN 解決方案。不只全系列產品皆內建 VPN 之功能, 還可配合 remote user, 符合各式之 VPN 需求。WatchGuard 的 VPN 效能或許不能和許多 high-end 的防火牆產品相比較, 但因其適用市場鎖定於中小型企業及政府部門, 故以其 70~100Mbps 的 3DES 加解密效能, 已可符合一般之使用。而其更以內建之整合工具 VPN Manager, 對於分散於各點的 VPN site, 提供了一個集中化、人性化之管理介面。VPN Manager 不但可在中心端監看各點之 VPN 連線狀況, 其管理介面更簡化了操作上的複雜度。例如若要建立兩點之間的 VPN 連線, 只需三個步驟即可完成—選擇兩點、選擇加密層級、按下 OK 鍵即可。WatchGuard 以其優異的管理功能, 為使用者提供最佳的管理環境。