



(右) Fortinet 香港及東南亞業務總監歐敬表示，使用高速的 ASIC 處理器，可以 Real-Time 同步掃描幾 MB 甚至幾十 MB 的封包數據，當檢查到有問題的封包便將它們即時刪除。

## Real Time 實時掃描有害封包 企業保安最前防線 FortiGate 100

面對病毒、蠕蟲、惡意程式碼，有公司會選擇安裝病毒軟件和防火牆，有些甚至會為電郵伺服器加裝垃圾電郵和殺毒等過濾引擎，但這些保安設備，對一些用 ADSL 或者是專線的小企業來說並不足夠，其實最理想的做法是在 ADSL 數據機後面，在未連接 Hubs 或 Switch 之前，加裝一些裝置，將所有進出的 IP Packets 進行 Real Time 過濾，直接研究封包流 (IP Stream) 是否藏有病毒、蠕蟲、惡意程式碼，這類型保安方案，因為價錢關係，以往在大公司或政府部門使用較多，但隨著技術意見進步，這些裝置便宜至 HK\$15,000 已經有交易。

### 常遇問題

面對病毒、蠕蟲、惡意程式碼，要在專機電腦安裝防火牆和病毒軟件，甚至安裝 Antivirus for SMTP Gateway 之類產品並不足夠，如果 ADSL 線得令中小企業資料庫出的境一掃而空的話，如果有產品每 24 小時檢查網際網路的進出的封包是否有病毒、蠕蟲、惡意程式碼，有的話即時過濾，那麼基本上可以做到 90% 以上的 Virus 和 Spam Free 的效果。

### 解決方法

FortiGate 是 Fortinet 公司新一代的 Gateway Appliance，它並不是加防那些號碼 Appliance，但只不過是一部純 U 網際器，用以防火牆或保安軟件的裝置。FortiGate 基本上是一個硬體裝置，使用高速的 ASIC 處理器，可以 Real-Time 同步掃描幾 MB 甚至幾十 MB 的封包數據，當檢查到有問題的封包便將它們即時刪除，這功能要求的硬體規格十分之高，這也解釋為何 FortiGate 使用 ASIC 高速處理器。

## 近

年，香港政府大力加強資訊科技，大部份中小企已設有伺服器，並接上互聯網，在科技設備數目不斷增加，已接上互聯網的區域網絡系統越來越不安全，易受外面的黑客非法入侵。此外，在互聯網的世界裡，不少網站的內容含有大量色情、暴力、不良意識的文字、圖片，和惡意程式，令人防不勝防；加上電腦病毒的廣泛在互聯網上流傳，一封含有病毒的小小電郵或 Blaster 等蠕蟲已足以令整台電腦或伺服器癱瘓甚至崩潰。

問：本刊記者 答：Fortinet 香港及東南亞業務總監歐敬

問：你們的硬體盒是使用 Linux 的嗎？這些硬體盒跟防火牆有何分別，防火牆過濾的 IP 和 Ports 不也都是 Real Time 的嗎？你們的產品跟這些有何不同？

答：我們的硬體盒為 Hardware Based 的，使用專用的 OS 配合 ASIC 處理器，來將 Gateway 進出的 IP 封包進行實時掃描。這些封包可以是來自 SMTP、POP3、IMAP、HTTP 進入公司的網絡，當 FortiGate 100 檢查到這些 IP Protocol 裡的程式碼跟其資料庫中的 Signature Pattern 相同時，便表示這些 IP Packet 裡有問題，可以是病毒、蠕蟲、惡意程式碼，這時 FortiGate 100 會將這些封包刪除，所以即使用公司內存放了電郵伺服器，有時後 SMTP 封包在未進入電郵伺服器時，已經被 FortiGate 100 在公司裡的 Gateway 攔截了，由於整個過程是 Real Time 的，所以用戶不會發現。

編者按：所謂 Real Time 就算用戶瀏覽網頁，經 http 的封包由 Request 到 Reply 整個過程都是實時的，FortiGate 100 做了過濾，當中感受不到延誤。

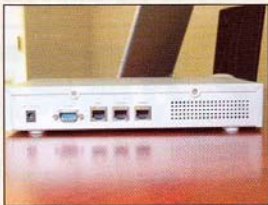
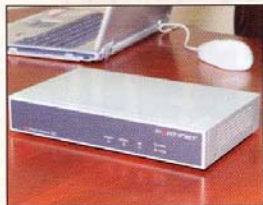
問：FortiGate 100 有哪些特別功能？如果公司裡設有網站伺服器，FortiGate 100 可以帶來跟傳統寬頻分享器有何優勢？

答：(一) FortiGate 100 有大量的 Intrusion Detection 的 Signature Pattern，其實網上有很多 DDoS 的攻擊方法，針對伺服器的便已經有 1300 種，這還未包括一些病毒程式碼在內，FortiGate 100 又發現了這些 DDoS 的 Signature Pattern，便會即時將它們攔截，這些類攻擊攻擊保護包括 IP Source Routing、IP Spoofing、SYN flood、ICMP flood、UDP flood、Address sweep、Tear Drop、WinNuke、Port Scan、Ping of Death、Land attack、Denial of Service 以及其他多種攻擊方式，當類攻擊被偵測到時會傳送警告到 3 個設定的電子郵件信箱。而市面的寬頻分享器能提供的防 DDoS 功能，多數是一些 IP Spoofing 技術，部分已經過時。(二) FortiGate 100 提供一個 DMZ 接口來將公司區域網的電腦 Traffic 跟 DMZ Zone 裡的隔開，這個很重要的，萬一公司員工電腦中毒，也不會波及公司的伺服器，因為很多寬頻分享器將公司的電腦和伺服器放在同一個 Subnet 上，也就是說區域網可以是 192.168.10 這個 Subnet，而放伺服器的 DMZ Zone 可以是 192.168.20 這個 Subnet，兩邊 Traffic 也是可以互水不犯井水。(三) FortiGate 100 本身也有 Static IP、PPPoE、DDNS 或 DHCP 等連接方式，而 DDNS 這些是免費提供給我們客戶的，是免費服務。而它亦可以配搭 RADIUS 伺服器或 LDAP (配 Active Directory) 來做認證，那樣我們便可以指定哪些員工可以上網，規範員工的上網習慣。而員工的上網權限是可以分類的，例如同事的上網時段，可以進入的網站，會那些「字眼」的網站不能進入，又或者按我們的內容過濾引擎 (Web Category Filtering) 將有問題的網站過濾。(四) FortiGate 100 本身也有它的 Spam Engine，可以實時將 POP3、SMTP 或 IMAP 的垃圾電郵封包刪除。(五) 針對一些企業級運算環境，例如學校或政府部門，高階型號的 FortiGate 可以做到平行分工 (Load Balancing) 和兼業運算 (Clustering)，FortiGate 最多可以做到 24 隻一萬平行分工，所以 Availability 很高。(六) 目前的寬頻服務愈來愈便宜，有些公司可能用幾家的寬頻服務公司，我們部份型號的 FortiGate 有兩個 WAN 埠，可以減少上綱的 Down Time。(七) 值得一提的是 FortiGate 提供了一種 Traffic Shaping 技術，可以在 FortiGate 裡根據員工的 IP 地址、用戶或網絡卡的 MAC Address 進行 Bandwidth 分配，即 QoS，那便不怕些員工用得太多 Bandwidth 而減慢其他同事了。

將有問題的網站過濾。(四) FortiGate 100 本身也有它的 Spam Engine，可以實時將 POP3、SMTP 或 IMAP 的垃圾電郵封包刪除。(五) 針對一些企業級運算環境，例如學校或政府部門，高階型號的 FortiGate 可以做到平行分工 (Load Balancing) 和兼業運算 (Clustering)，FortiGate 最多可以做到 24 隻一萬平行分工，所以 Availability 很高。(六) 目前的寬頻服務愈來愈便宜，有些公司可能用幾家的寬頻服務公司，我們部份型號的 FortiGate 有兩個 WAN 埠，可以減少上綱的 Down Time。(七) 值得一提的是 FortiGate 提供了一種 Traffic Shaping 技術，可以在 FortiGate 裡根據員工的 IP 地址、用戶或網絡卡的 MAC Address 進行 Bandwidth 分配，即 QoS，那便不怕些員工用得太多 Bandwidth 而減慢其他同事了。



## FortiGateTM-100 技術規格及功能

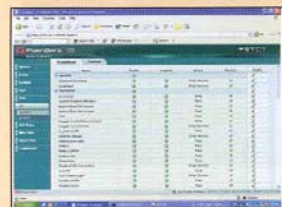


- \* 3組 10/100BaseTX Ethernet 介面 (Internal、External 及 DMZ)
- \* 1 個 RS-232 Console 埠

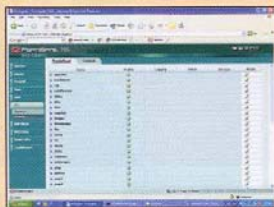
公司名稱 Fortinet  
 產品價錢 約 HK\$1,500  
 資料更新 為硬件的 30% (每年計)  
 電話查詢 (852) 3171-3000

- 1 最新電腦病毒及病毒資料庫用以阻擋千計最新和最危險的電腦病毒及病毒。所有電子郵件附加檔案 (SMTP、POP3、IMAP) 和網站內容及 HTTP 進行病毒碼比對及巨集病毒掃描。
- 2 網站內容過濾提供 URL 阻斷及關鍵字比對模式以禁止使用者存取網站內容。
- 3 工業級標準的封包檢驗型防火牆。提供易於設定的防火牆管理原則且包含流量紀錄及流量管理。操作模式包括 NAT (Network Address Translator) / Transparent、PAT (Port Address Translator)、Route 模式。
- 4 使用者認證：支援 RADIUS 以及內部資料庫以供使用者認證。多種紀錄內容：包含流量、事件以及攻擊紀錄。VPN 具有工業標準的 IPSec、PPTP 及 L2TP VPN，以提供網絡端及使用者端安全通訊。FortiGate 有硬件加速方式加密：DES & 3DES (Triple-DES) 加密方式，它們可線上更新為 AES。

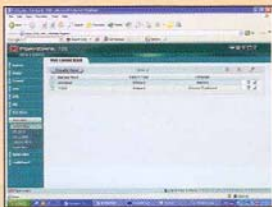
## FortiGate 100 功能解構



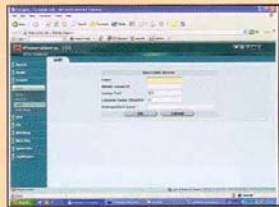
**Check 1** FortiGate 100 有大量的 Intrusion Detection of the Signature Pattern，其實網上有許多 DDoS 的攻擊方法，針對伺服器的便已經有 1300 種，圖中是不同 DDoS 攻擊的處理手法。



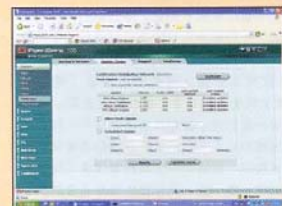
**Check 2** 基於不同的應用程式、Protocols 的 IDS Signature 在 FortiGate 100 有仔細的分類，例如針對 Apache、NetBIOS、IIS、FTP 等等。



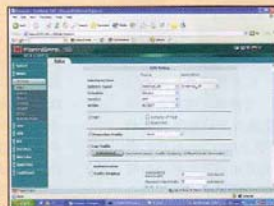
**Check 3** 已有超過萬個不良意識的英文、日文、繁體中文、簡體中文的網站的網址 (URL) 和詞匯 (Keyword) 的數據庫。



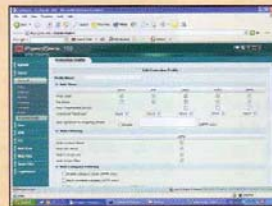
**Check 4** FortiGate 100 可以配搭 RADIUS 伺服器或 LDAP (配 Active Directory) 來做認證，那讓我們便可以指定哪些員工可以上網，規範員工的上網習慣，因為每個上網的同事上網時都須要先進行身份認證。



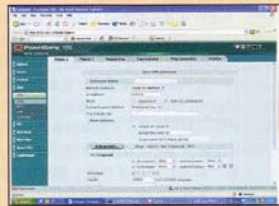
**Check 5** Fortinet 會第一時間自動下載最新的病毒數據庫到 FortiGate 100 上，以確保公司連上互聯網的電腦安全。同樣，網絡非法入侵偵測的 (Network Intrusion Detection System) 數據庫也自動下載到 FortiGate 100，使黑客 (Hacker) 無從入手。



**Check 6** 用戶可以在 Firewall 自行設定 Policy 來指定同事的上網習慣，例如那些同事用到 Instant Messenger，那些同事可以使用瀏覽器，FortiGate 100 裡你可以限定哪些檔案員工可以下載，又或者限制網頁那些字眼會進行過濾。



**Check 7** 圖中為針對 HTTP、FTP、IMAP、POP3、SMTP 進行 Virus Scan、File Block、Over Sized Email、網頁內容管理等設定介面。



**Check 8** 管理員以通過 FortiGate 100 的虛擬私人網絡網關 (VPN)，安在家中從互聯網安全地遠距離登陸公司的電腦，利用虛擬私人網絡網關 (VPN) 的保密性可防止公司機密的文件在互聯網傳送中洩漏。

## 專業短評：值得投資

FortiGate 100 是一種高效能和硬件式的裝置，透過它可以避免被電腦病毒或病毒等威脅電腦網路，它本身結合防火牆、VPN、入侵偵測 (Intrusion Detection)、網站內容過濾 (Content Filtering) 及頻寬管理功能的產品。FortiGate 100 是利用 FortiNet 專有的 FortiASIC 內容處理器及 FortiOS 作業系統來提供快速資料掃描能力。FortiGate-100 安裝容易且能夠用 Web 介面進行管理，適合 SOHO 族到大型企業使用。