

# 為中小企建立最強防護網

## 專 Fortinet 國際產品管理副總裁 訪 Richard Hanke



公司國際產品管理副總裁 Richard Hanke 解釋有關 Fortinet 網絡保安系統的運作。

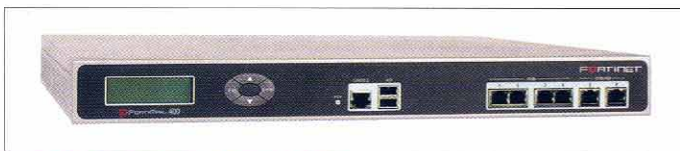
今時今日，企業對網絡保安問題絕不能再掉以輕心，尤其是對於日益嚴重的 Spam 電郵及 Spyware 間諜軟件入侵，以及長久以來的電腦病毒問題，而為了保障公司的利益，很多公司都會願意花錢在網絡保安架設上。有見及此，不少網絡保安公司因此應運而生，其中一間在海外多個國家設有辦事處的網絡保安公司 Fortinet，最近亦推出了 FortiMail-400 系統，早前本刊更有幸與該公司國際產品管理（Global Product Management）副總裁 Mr. Richard Hanke 會面，在專訪中分享該產品的各項功能。

### 保安問題愈趨惡化

Richard Hanke 指出：「垃圾郵件不但減低生產力，亦加重了網絡頻寬及電腦運算上的負荷，已經不再是單單滋擾用家這般簡單。據去年 19/12 - 25/12 一周內的數據顯示，我們其中二千個客戶當中，就曾受到約 3,700 萬次不同類型的網絡襲擊。而同一時期，我們每部 FortiGate 800 網絡保安系統亦受到超過一萬種病毒入侵。」雖然憑著 FortiGate 的完善保安系統，終可一一成功防禦襲擊，但可以肯定的是，這個問題將會愈來愈嚴重。

### FortiMail 400 本月登場

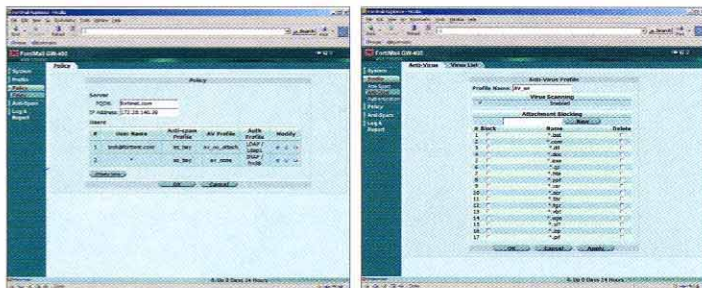
據知，FortiMail-400 系統亦已準備好在本月面世，機身內置了兩個 120GB 硬碟及以 RAID 0 或 RAID 1 陣列式運作，另外亦配有 1GB ECC DDR 記憶體，絕對足夠處理大量資料傳送，而 Richard 更表示：「FortiMail-400 目前每小時可處理約 57000 封 1K 容量的電郵或 50000 封 3K 電郵，絕對足夠一般公司或企業使用。」



Fortinet 最新推出的網絡保安系統 FortiMail-400。

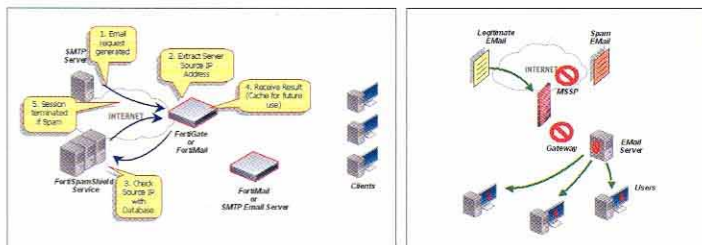
### 三種防護模式

而 FortiMail 為用戶提供了三種防護操作模式，分別為「透明模式」、「網關模式」和「伺服器模式」。「透明模式」設於現有電郵伺服器前面，毋須改動原本的電郵結構，能與目前的網絡妥善兼容。而「網關模式」和「透明模式」一樣設於電郵伺服器前方，並提供了接收及發送電郵服務，以助掃描所有收發電郵。至於「伺服器模式」，除了具備防毒及過濾電郵功能外，亦提供了全面的伺服器功能。



FortiMail 的操作介面。

另外，據知他們亦會在稍後時間推出電郵管理服務 — FortiSpamshield，來配合該公司早前推出的 FortiGate 以及 FortiMail 系統，該服務擁有先進的電郵偵察及過濾技術，有效防止病毒及間諜軟件 (Spyware) 入侵，而 FortiSpamshield 更使用了該公司獨有的「雙向流通」(Dual Pass) 掃描技術，能查核濫發電郵者的 IP 及電郵內容。Richard Hanke 解釋：「這個技巧的背後原理很簡單，當用戶收到電郵後，FortiGate 或是 FortiMail 便會自動尋找有關發件人的 IP 地址及有關電郵內容，並將有關資料傳送到 FortiSpamshield 系統中，倘若發覺是垃圾或是間諜軟件等不良電郵的話，就會立即截斷該電郵，阻止該電郵入侵。」



FortiSpamshield (左) 與一般 Anti-Spam 軟件及硬件 (右) 的運作比較。