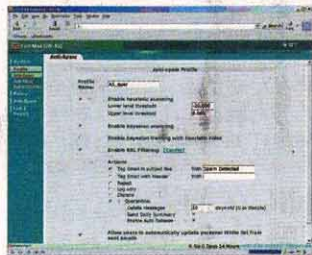


# 硬件夾服務截擊Spam

## Fortinet 新方案攻中小企



FortiMail 400提供網絡介面管理。



Fortinet環球產品管理副總裁Richard Hanke。

現時垃圾電郵氾濫，宜且情況愈來愈嚴重為保障企業網絡安全，除了引用反間諜軟件及軟硬兼施的保安方案外，堵截垃圾電郵亦是保安當務之急。最近，網絡保安方案供應商Fortinet就特為堵截垃圾電郵推出硬件方案及專業服務，搶佔中小企市場。



FortiMail 400為企業解決垃圾電郵的問題。

據 Fortinet 環球產品管理副總裁 Richard Hanke 表示，垃圾電郵不單令員工生產力流失，耗費網絡資源，還浪費電腦內的儲存空間、記憶體及處理器等資源。

他指出，現時反垃圾電郵主要有 4 個方法：一是採用客戶端軟件，二是在電郵伺服器上安裝軟件，三是透過網關攔截，最後是外判子服務供應商。

### 軟件方案未具效率

Hanke 強調，上述首兩種都不是具效率的方案，客戶端軟件更難以管理；反之，第三及第四個方法更有效，可以在垃圾電郵到達公司系統內前進行阻截，其中網關方案可以更準確地截擊，而外判式服務則可以節省企業反垃圾電郵的投資。故此，Fortinet 這次同時推出 FortiMail 400 網關方案以及 FortiSpamshield Service 兩個方案。

### 每日掃描1.3m 電郵

Hanke 表示，FortiMail 400 採用堅固的操作系統，以網絡介面管理，配備兩個 Gigabit 網絡埠，以及內置 120GB 硬碟，可支撐 2000 個郵箱。至於速度，他指，以全功能開啓模式，每小時可以掃描 5 萬 4,000 個電郵，每日可以掃描達 130 萬個電郵（以每個電郵 1 至 3KB 大小計算）。他指，由於現時一些垃圾電郵都會內藏病毒，故此他們的方案產品原有的防毒掃描功能及技術，對阻止垃圾郵件亦有相當幫助。其他功能方面，該方案可以為不同用戶作個人化設

定，以及對不同郵件作評級，進行不同程度的篩選；此外，亦包含防毒、阻擋拒絕服務(DoS)攻擊。

FortiMail 400 亦可以 3 種不同的方式配置。據 Hanke 解釋，分別是安裝於網絡之內作電郵掃描的透明模式；或是以其作為網關，直接阻擋垃圾電郵；又或者是以其作為電郵伺服器，掃描所有接獲的電郵。而在 FortiMail 400 內的硬碟就是用作暫存郵件及隔離垃圾郵件之用，而這功能不只針對中小型企業需求，其實服務供應商市場也合用。

另外，新推的 FortiSpamshield Service 不單可以配合 FortiMail 400，亦可以配合旗下另一網絡保安硬件 FortiGate，以提供整個反垃圾電郵方案。Hanke 表示，該項服務以兩方面斷定一個郵件是否屬於垃圾電郵，並將會讓 FortiMail 或 FortiGate 連接由 Fortinet 維護的數據庫，首先以寄出電郵的 IP 地址作第一重的篩選，而第二重則以郵件的內容為依據。

### 成立報料網站

為更廣泛收集濫發郵件者資料，該項服務還包括建立一個舉報網站，讓各企業用戶可以提供有關資料。Hanke 並強調，透過他們的服務，配合 FortiGate 則可以減少 40% 的垃圾電郵量，而配合 FortiMail 的話，數量更可以銳減 95%。他補充，現時他們在美國試用 FortiSpamshield Service 的客戶，亦錄得相近數字。

面對激烈競爭，Hanke 表示，有別於他們競爭對手以用戶量作收費根據，取而代之，他們的方案是以固定的硬件售價，而服務則是每年收取 FortiGate 售價的 20%。他又指，其他對手的方案大多是以軟件為基礎，不及他們以硬件為基礎具效率。

未來發展方面，他表示，現時推出的 FortiMail 400 只屬入門級型號，所以未來會推出更高速度、負載量更高的高階型號，這系列產品預期於今年上半年內推出。

目前網絡保安的發展重點，明顯趨向到將軟件整合到硬件之內，充當更高效能的保安組件，為用戶提供更全面的保障。這趨勢對於傳統的保安軟件公司帶來的衝擊尤其顯著，相信惟有改變產品策略，才是這些公司未來生存之道。