

A Fortinet 強化網閘保安

網絡防毒防火牆系統供應商Fortinet，上周正式為其網絡保安方案與服務組合，增添兩名新成員。

據 調查數據顯示，目前約六至七成的企業電郵均為垃圾電郵，並預期到了〇七年，每日送出的垃圾電郵，將達一百七十億封之多！垃圾電郵除對僱員工作效率有負面影響及耗費資源（如寬頻、記憶體等）外，更有可能為企業帶來不必要的保安風險。

■ 垃圾電郵潛藏危機 ■

雖然企業均已設置防火牆，且機構內的電腦，大部分亦已安裝防毒軟件，不過據Fortinet環球產品管理副主席Richard Hanke分析指出，一般用戶端防毒措施，實為成效最低的防毒產品，較難管理及維護，出現的漏洞亦較多（如用戶忘記定期更新等）。而基於電郵伺服器的防毒裝置，雖然簡化了管理及維護工序，然而就效率、功能及彈性方面，始終比不上基於網閘的過濾裝置。

■ 大包围過濾網閘 ■

Hanke續指，設於電郵伺服器的過濾裝置，畢竟仍會將垃圾電郵，或帶毒的郵件下載到伺服器內，佔去不少儲存空間，但設於網閘的安全訊息平台，則可在網閘直接阻截該類郵件，省下大量資源及儲存空間。

FortiMail-400系統為該安全訊息平台系列率先推出的產品，售價約為一萬二千美元，雖然專為中至大型企業而設，卻是中小企亦可接受的價格。FortiMail-400可為多達二千個電郵帳戶，處理每日約一百三十萬封電郵，並容許每位用戶建立個別的過濾設定，如指示系統只進行隔離，而不即時刪除被評為垃圾郵件的電郵，以方便日後覆核有否誤評等。

為應付大型企業、大學院校與MSSP供應商等，對高容量關鍵基礎的防護需求，Fortinet將推出FortiMail以作配合。

採用FortiOS技術的FortiMail安全訊息平台，可透過如FortiSpamshield這類偵察與過濾的方式，落實存取不同功能，包括策略過濾、內容過濾、全球與用戶黑白清單過濾、垃圾電郵即時黑名單（Real-time Blackhole List, RBL），並為用戶進行貝氏（Bayesian）過濾，以使用戶擬訂個人資料、啓發式過濾與阻斷服務攻擊。

據悉，FortiSpamshield可成功阻截或偵察多達四成垃圾電郵。其於FortiMail或FortiGate系統的「雙向流通」（dual pass）掃描技術，可藉Universal Resource Identifier（URI）進行掃描，查核濫發電郵者已知的IP郵址與



■ Fortinet環球產品管理副主席Richard Hanke指，用戶端防毒措施在防毒產品中成效最低，較難管理及維護。

電郵內容，包括郵件標題、內文及格式資訊等。

■ 三種操作模式 ■

FortiMail安全訊息平台分別為用戶提供三種防護操作模式：透明模式、網閘模式及伺服器模式。

在透明模式下，FortiMail平台將設於現有電郵伺服器前端，毋須改動現有電郵結構，即可與目前的網絡環境兼容；網閘模式同樣設於電郵伺服器前端，以提供收發電郵傳遞服務，並掃描所有郵件訊息；而在伺服器模式下，FortiMail平台除具有防病毒，與垃圾電郵過濾功能，也提供全面的電郵伺服器功能。

FortiMail-400系統與FortiSpamshield服務方案現已有售，而FortiMail 1.2版本則約在四月推出。如需更詳盡的產品資訊，請瀏覽以下網址：<http://www.fortinet.com>。



■ FortiMail-400售價約為一萬二千美元，可為多達二千個電郵帳戶，處理每日約一百三十萬封電郵。