

Fortinet FortiMail 2000

整合式安全防護架構因應各類安全威脅



由 Fortinet 所推出的 FortiMail 2000 產品，是 1 款針對大型企業用戶，並同時支援中繼閘道式、穿透式及郵件伺服器軟體模式的郵件安全閘道設備。該產品採取整合式安全防護架構，不僅內建多層次垃圾郵件過濾機制，並提供自動升級的病毒特徵庫和檢測引擎。

提 供整合式的安全防護機制的 Forti-Mail 2000，在垃圾郵件防護上，採用多層次的過濾機制，首先以黑白名單比對 (RBL 及 DCC)、表頭檢查、URL 過濾等一般技術，進行第一關的篩選，再來，則透過 Fortinet Dual Pass 掃描技術進行第二道過濾程序，該技術乃藉由 FortiGuard-Antispam Service 及 URI (Universal Resource Identifier) 掃描，同時進行郵件發送 IP 位址及郵件內容的檢查工作，如此可提昇垃圾郵件的偵測率。其中，FortiGuard-Antispam

Service 是該公司針對全球用戶所設立的黑白名單資料庫伺服器。

根據 Fortinet 表示，透過上 2 道過濾機制，即可預先擋掉高達 90% 的垃圾郵件，最後，則是位於 Local 閘道端的第三道過濾機制，總而言之，目前 Fortinet 多功能閘道器是採用結合貝氏演算法與 900 多條的啟發式偵測 (Heuristic) 規則等多層次技術的綜合性垃圾郵件過濾技術。

至於防毒方面，該產品採用 FortiGate 病毒檢測引擎，並透過 FortiProtect 全球網路

資料庫，取得自動升級的病毒碼和攻擊特徵碼，不但支援 SMTP 流量、壓縮附件的安全掃描，並且提供感染檔案隔離、病毒偵測通知，以及指定阻擋檔案類型等防護功能。此外，該產品並提供使用者群組定義 (User/Group Defined) 功能，以因應不同的反垃圾郵件標準及政策。

目前反垃圾郵件產品大致可分成中繼閘道式、穿透式及郵件伺服器軟體 3 大類型，其中，閘道式採用專用積體電路晶片 (Application Specific Integrated Circuit; ASIC)，再加上簡單的 DNS MX 記錄，不但設定方便，而且能提供最佳的掃描效能；穿透式與郵件伺服器軟體，則具備安裝時完全不用更改任何網路架構及 DNS 設定的優點，而 FortiMail 2000 則同時兼顧上述 3 種模式。

一般市面上的企業級反垃圾郵件產品，多半以公司內部人數為授權依據，由於人數會隨著企業的成長與否而有所變動，因

FortiMail 2000 是 1 款針對大型企業用戶，並同時支援中繼閘道式、穿透式及郵件伺服器軟體模式的郵件安全閘道設備。



內建完整的報告和日誌，對郵件使用的每一方面，提供可視性和審記功能。

此上述授權方式不但極其麻煩，同時還會增加建置成本，因此，Fortinet 提供無限人數版本的授權方案，能大幅降低企業支出。