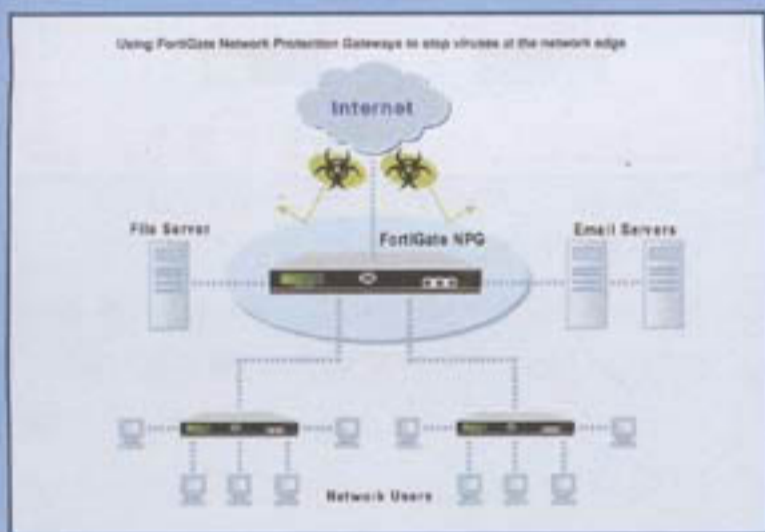


FortiGate網路安全匣道器

在網路閘道端阻擋病毒

雖然升級firmware、Service Pack都是在增加電腦的免疫力，可以保護自身本機的安全減低可能感染的風險，但是主要的解決方案應該還是要做到網路出口隔離/阻止擴散才能防止外部的電腦病毒入侵。



伺服器防毒因為龐大的病毒碼會影響電腦效能。而且防毒軟體因為屬於file-based，所以必須將檔案載入主機的記憶體後才能偵測到。網路防毒(NAV；Network-based AV)的佈建，目的是將病毒的感染進行隔離、阻擋病毒的擴散，避免更多的電腦與主機遭受到病毒的威脅與損失。典型的解決方案是將防毒牆安裝在公司對外的閘道上，或是公司內部不同的建物或單位間。

網路防毒(NAV)特性與優點：

- 網路防毒(NAV)系統提供單一邊際區域的保護，也就是該區域不會再有任何可能的對外出口，以有效防護。
- 網路防毒(NAV)要能阻擋病毒在閘道外端，以避免主機受到感染後，殘留在伺

伺服器主機記憶體的風險。

- 網路防毒(NAV)能夠降低伺服器主機的負載，因為病毒阻擋在網路閘道，所以對外伺服器主機就不必花資源來處理。
- 網路防毒(NAV)最大的挑戰是在處理的效能上如何能提供防毒功能又不會遞延即時的網路應用程式。
- 傳統上Host-based Anti-Virus(HAV)掃描，已經存在電腦作業系統中的檔案，HAV攔截這些檔案比對在電腦中的病毒碼，這些病毒碼包含成千上萬的病毒碼，至於需要多久來掃描，全賴硬體效能來決定。網路防毒(NAV)必須要能在硬體採用ASIC才能解決「效能」問題。網路防毒ASIC主要以包處理的引擎及Signature掃描引擎來加速處理與提升防毒效能。
- 封包處理的引擎能夠處理封包的表頭，同時加速辨證應用層的資料流為哪一個封包。
- Signature掃描引擎會重組封包的payloads內容流(content streams)在系統記憶體上，同時載入適當的病毒碼直接比對。

網路防毒(NAV)更重要的工作是一全球病毒回報中心全年無休的防護機制。全球病毒回報中心有病毒防禦的研究人員，負責研究新型病毒與攻擊模式，一但取得隔離病毒的樣本、決定病毒威脅的等級後，便同時研發新的病毒碼。當確認新種病毒，各個區域的病毒碼更新資料庫主機，會同步更新所有NAV的主機，讓顧客能及時防禦。