

全能防毒ASIC 監管網上行為 企業防毒新概念

筆者便就近日W32.Sasser的爆發，向多間電腦硬件及軟件保安產品開發公司問及他們對於這場世紀網絡病毒大戰有什麼對策和意見給我們廣大的讀者，是次我們便訪問其中兩間病毒保安公司，分別是WebSense及Fortinet。前者為全球處於領導地位之員工上網管理 (EIM)方案供應商，而後者更於早前勇奪2003年度網路事業之最佳防火牆大獎。

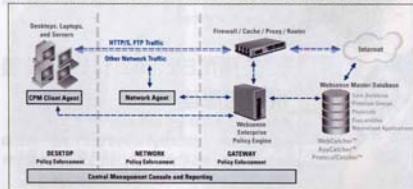
Part A. WebSense：預防勝於治療

對於一班已有一定使用電腦經驗的用戶來說，最有效的防毒方法是盡量避免受到感染，只要避免走進病毒設計者的圈套或在公司內禁止員工前往不知名的網站，便能有效地減少中毒的機會。而筆者早前便接觸了一間早前提供Site Filtering (網站過濾)，現在提供員工上網管理(EIM)方案的供應商WebSense。而他們旗下的產品WebSense Enterprise 5.1更於今年三月獲《PC Magazine》頒發Editor's Choice獎項。



a. 控制員工上網習慣是網上保安重點

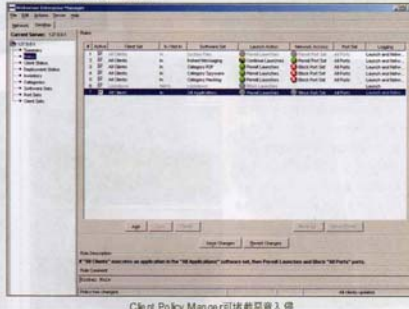
WebSense Enterprise是一套能夠從網路、網絡及桌面三個層面管理及保護員工運用電腦情況的管理軟件。在網路及網絡層面，WebSense可支援機構的互聯網應用政策；在桌面方面，WebSense可針對未知的保安威脅，為機構提供即時 (zero-day) 保護，以免被病毒、蠕蟲及木馬程式等隨時爆發的先進混合式攻擊有機可乘。這個方案不但可以有效地控制網絡用量，不讓員



工下載不必要的檔案，如MP3、影片等，而且又可以禁止他們使用IM (Instant Messenger) 軟件。有研究指出過去一年，25%電腦病毒是針對IM的漏洞而設計的，可見IM是高危軟件。另外WebSense亦能夠消除間諜軟件 (Spyware)、端對端P2P檔案共享系統的濫用、內部入侵及惡意程式等網絡威脅。WebSense Enterprise v5.2現可於www.web-sense.com/download 下載。

b. 預防惡意程式的即時入侵

很多惡意程式均能利用新發現的軟件漏洞，在用戶取得修正程式前趁機入侵電腦系統。這種名為「即時入侵」(zero-day assault) 的攻擊日益增多，對企業的桌面系統、筆記簿型電腦和伺服器構成嚴重威脅。WebSense有見及此便推出WebSense Enterprise Client Policy Manager (CPM)令企業能夠制定及執行政策，限制系統在特定時間才可以啟動指定的應用方案，藉此保護桌面系統等終端平台，填補網絡防禦的空隙。除了攔截間諜軟件之外，CPM亦可以阻止員工在任何桌面電腦、筆記簿型電腦或伺服器啟動黑客工具，以及阻截受病毒感染的附件經由即時訊息(IM)或端對端程式等不受管理的網絡進行入侵，甚至能夠消除其他隨時出現的混合式桌面安全威脅。此外，資訊科技主管亦可以利用CPM管理遊戲和串流媒體播放軟件等影響員工效率的桌面應用。

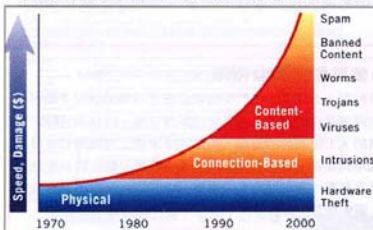


Client Policy Manager可堵截惡意入侵

Part B. 新世代病毒凸顯傳統保安方案的弊端

a. 傳統防毒方法已不合時宜

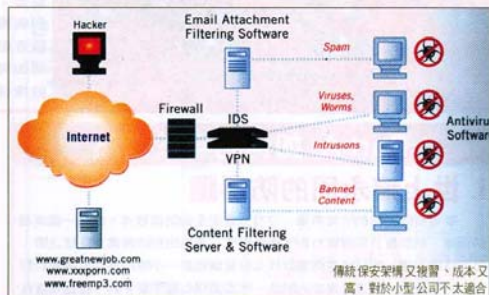
隨著全球經濟逐步復蘇，各大小企業開始轉虧為盈的時候，便開始計劃在網絡保安上投放更多資源。因為所有CIO皆意識到現時網絡上的電腦病毒已比以往更厲害、更複雜以及破壞力更驚人。如果仍然使用舊式的保安技術及概念，恐怕未能作出有效的防禦措施。指步入廿一世紀，網絡保安問題已不是單純以黑客入侵為主，而是以“Content-based”的入侵方式主要，當中包括垃圾郵件、蠕蟲及木馬等，但傳統的防火牆對於這些“Content-based”的攻擊卻是無力招架，因為它們的設計未能針對應用層(Application Layer)在網頁裡的内容，而防毒軟件雖能預防這類的入侵，但對於擁有過百



甚至過千員工的企業，那一筆巨大版權費就使很多CIO頭痛不已。
步入廿一世紀，如何預防“Content-based”的入侵已成為網絡保安的最大考慮問題。

b. 舊式保安方案未能防禦廣泛的入侵

傳統的網絡保安方案都是以「抄雜錦」的形式，把各種複雜的硬件放在網絡上，各自執行不同的保安工作，從人手和成本兩大角度上，都是低效率的做法。規模較細的公司，由於對預算的要求不高，傳統的方案所出現的問題未見明顯，但對於龐大的高階保安保安架構來說，便會出現很多根本的問題。



Part C. Fortinet：一體化實時保安方案

a. 整合性保安硬體效能更高

就以上多個問題，筆者早前採訪了美國大型保安硬體供應商Fortinet，並與該公司的亞太區副總裁及總經理Matt Young作了一次面對面的談話，提及未來的病毒發展以及對於現今病毒可作出的相應對策時，Matt指出作為一間成功的硬件網絡保安供應商，必須能為客戶提供即時網絡保安服務，以及能把各種保安功能的硬體集於一身，以便作出中央管理，加快網絡資料的監管。以這個概念為本，再加上不影響系統的運作速度為大前提下，利用獨有的ASIC技術製作出FortiGate-60，能有效地把六項保安功能集於一身，包括防火牆(Firewall)、虛擬專用網絡(VPN gateways)、防病毒內容過濾(Software-based antivirus and content filtering systems)、網上入侵偵察(Intrusion Detecting system, IDS)，都裝配在單一的裝置內。使硬件在網絡上的監管動作更快速和把成本降低。



b. 硬體防火牆速度上佔優，亦不如防毒軟件般不限量收費

傳統防毒軟件只能在網絡資料傳送的过程中，對電郵及其他檔案作非實時(non-real-time)的病毒掃描，但由於速度較慢，未能在觀看網頁的同時，對

病毒和蠕蟲作出及時預防。

在文章的前段也提及到Fortinet把不同的保安硬件統一化，而他們利用獨有的FortiASIC Content Processor (內容處理器) 品



片，做到實時(real-time)防病毒的完美效果。另外Matt又指出和其它防毒軟件不同，Fortinet的產品主張以單一收費，不存在以公司的人數或客戶端(Client PC)的數量收取無限量的版權費用，即表示不論公司的人數多少，只會收取該產品的固定費用。

後感： 提高網絡保安意識為最根本的勝算

Web sense 利用軟件監控網絡使用者的情況，目標旨在防止因電腦「不恰當」的使用而暴露保安漏洞；Fortinet利用整合式硬件保安方案，對網絡資料作實時的掃描，以避免出現保安危機。「危機」，是包含「危」和「機」，保安工具無疑能有助轉「危」為「機」，但即使擁有號稱完美的保安系統，如果使用者沒有正視網絡保安的問題，未有從過往曾經「化險為夷」的危難中得到教訓，終有天病毒一定會推土再來的。唯獨時刻保持高度警覺，再配合良好的保安工具，才是擊退入侵的最完整方案。