行政院及所屬機關出國報告（出國類別：實習）

「實習網路安全新技術」報告

服務機關：中華電信數據通信分公司
姓名職稱：邱俊穎　專　員
出國地點：美國、加拿大
出國期間：93 年 11 月 28 日 93 年 12 月 11 日
報告日期：94 年 3 月 10 日

摘要

本次奉派赴美國及加拿大 ScanAlert 與 Fortinet 實習，ScanAlert 公司介紹其用於風險管理的稽核技術，以每日掃描頻率讓通過認證的站台得到 Hacker Safe 網站安全標章，使得該網站之客戶在該網站上的線上購物(online purchase)行爲更信任。ScanAlert 不只是提供安全標章，透過其功能強大的弱點管理入口網站 (Vulnerability Management Portal) 的使用者介面，展示之技術核心及支援方式及能力；Fortinet 則介紹其下一代及時統一威脅管理(UTM)系統，以 ASIC 加速晶片的技術，將網路層的防火牆 (Firewall)、入侵偵測及預防 (Intrusion detection and prevention)、流量管理 (Traffic shaping) 以及應用層的防毒牆 (AntiVirus gateway)、內容過濾 (Content filtering) 整合於一台專屬、單一的平台上。對於網路資料中心 IDC 來說，客戶多爲已經能從網路上賺取利潤的企業用戶，能否增進網路安全進而讓其產生更大的營收是其所需要的，能達到此需求的加值服務是目前 HiNet IDC 尚欠缺的。故本實習將 ScanAlert 及 Fortinet 的公司及技術能力作全面的了解，引進其技術及產品來提供完善的網路安全加值服務。最後針對本次實習所學提出一些看法及建議，希望對 HiNet IDC 未來發展的參考有所助益。

目錄

1 前言

隨著網路的發達以及電子化的進步，企業大量採用資訊系統來促進各個產業的發展，因此，企業重要的研發展機密以及相關交易資訊常常隱含於各系統當中，若缺乏良好的企業安全政策或者是資訊安全管理機制，可能會因爲安全事件的發生而對整體企業造成程度不一的影響及衝擊。HiNet IDC 乃是企業開始專注於其本業，重視專業分工，捨棄自建機房網路設施、資訊管理人員等龐大成本尋求之資訊委外服務的最佳選擇。企業將其資訊設備、網路存取交給 IDC 機房後，原來的資訊安全課題仍然需要重視。然而資訊安全並不是僅止於資訊部門架設好防火牆、入侵偵測系統、防毒軟體等硬體防護設備就可以高枕無憂，就如我們所知道的，企業架設了層層的防護系統，但是實際的安全狀況並沒有完全的改善，各種大小不一的安全事件還是時有所聞。

IDC 強調專業分工，企業將原本機房基礎建設及網路管理業務托由 IDC 管理，則大部分的網路安全重責大任就移轉給 IDC 掌管，當然，企業本身仍需要了解企業內部何者爲有價值的資訊及哪些是需要保護的資料，制定其良好的安全政策才能夠做到全面的資訊安全。本報告就企業可能面臨的弱點威脅，試圖替客戶找出如何稽核弱點進而修補的方法，及整合威脅管控系統(UTM)的解決方案，期能在網路安全方面真正幫助 IDC 用戶，也使得 HiNet IDC 提供完善的加值服務，達到整合全方位服務。

2 行程概要

本次實習行程自九十三年十一月二十八日至九十三年十二月十一日止，共計八天，實習地點爲美國舊金山及加拿大溫哥華，對象爲 ScanAlert 與 Fortinet 這兩家公司，行程安排如下：

日期	地點	行程概述
11 月 28 日	台北至舊金山	行程。
11 月 29 日 -12 月 03 日	舊金山	ScanAlert 實習: 安全稽核及認證技術研討、 HACKER SAFE 方案研討、實際服務案例研討。
12 月 06 日 -12 月 07 日	舊金山	美國 Fortinet 實習: 防火牆技術研討、實際線上展示等研討。
12 月 08 日 -12 月 09 日	溫哥華	加拿大 Fortinet 實習: 病毒處理程序、內容過濾及全球更新散佈網路研討。
12 月 10 日 -12 月 11 日	溫哥華至台北	回程。

值得一提的是，ScanAlert 這家公司位於舊金山北部有最有名的酒鎮 Napa Country，鄰近許多葡萄酒廠及葡萄園，不同於 Fortinet 所在高科技公司密集的矽谷 (Silicon Valley) 一帶，具有清新的空氣及田園景色。

圖 2-1. Napa Valley 一望無際的葡萄園

3 網路安全稽核及應用

3.1 網路安全稽核系統

在現今網路的發展，企業越來越多的資產儲存於公司的網站、主機及伺服器上，如果稍有不慎，可能形成企業莫大的損失。既然網站是企業的重要資產，要考慮的就是企業所面對的弱點以及威脅，對於企業內部可能發生的危機做好妥善的規劃，避免這些威脅的發生或面臨威脅時能夠有良好的應變措施。所謂弱點（Vulnerabilities）是指組織資訊安全的弱點或漏洞，本身不會造成傷害，但若未妥善管理，則可能促成威脅的得逞。在資訊安全相關方面，所謂的弱點可能是由於系統設計不良，例如：作業系統的本身的漏洞、網頁表單輸入驗證機制的不完全、或者是採用的系統有未察覺的弱點，都可能被加以利用來竊取企業相關的重要資訊，造成資訊洩漏。例如之前喧騰一時的「資料隱碼」(SQL Injection)攻擊技術，便可能因爲驗證機制的不完善造成重要資訊外洩，這些事件的發生不僅造成了內部資訊的洩漏，也會對商譽造成莫大的傷害。

但是如何知道我的伺服器主機或應用程式有弱點呢？一個網路安全檢測系統是必須的。這項重要技術的原理是採用模擬駭客入侵的手法去測試系統上有沒有安全上的漏洞，對目標可能存在的已知安全漏洞進行逐項檢查。目標可以是工作站、伺服器、交換機、資料庫應用等各種對象。然後根據掃描結果向系統管理員提供周密可靠的安全性分析報告，從掃描出來的安全漏洞報告中去了解系統上的安全漏洞有多少？如何去修補及到那裡下載修補程式。

圖 3-1. 開放原始碼的掃描工具 nmap

故這個弱點安全稽核程式必須先進行掃描工作，找出網路的配置，及主機的連接埠號，例如 nmap [1]就是蒐集網路資料最常被使用的工具。nmap 足以勝任安全弱點偵測的第一步驟。掃描完畢後，接下來就要根據掃描找到的開放服務，與弱點資料庫 (Vulnerability Database) 的已知簽章 (Signature) 做比對，找到弱點時回報給系統管理者。例如 Nessus [2] 就是一種全服務的安全性掃描程式，Nessus 的插增架構使得使用者可以爲他們的系統與網路自訂此程式。它含有完整回報、 主機掃描以及即時的弱點搜尋等特色。 即使像 Nessus 程式功能如此的強大， 而且經常地更新，還是可能發生主動錯誤訊息和被動錯誤訊息。另外

還有時常更新的 osvd [3] (Open Source Vulnerability Database) 來幫助安全掃描的精準度。舉例來說：SAS [4] (Security Auditing System) 即是 TWCERT/CC 爲台灣最早開始幫政府單位以及國內各公司單位進行電腦網路安全檢測的單位所開發的網路安全檢測系統。又如本公司 hiCERT 所開發的資通安全檢測系統 [5] 也是一個基於網路的安全檢測系統。

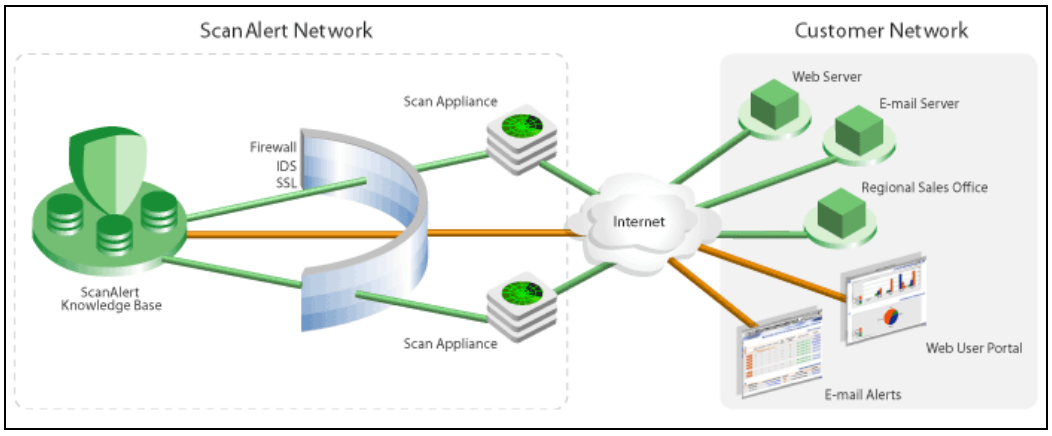

圖 3-2. 網路型安全弱點掃描之整體架構

3.2 網站安全標章

在現今，企業的網站往往是一個企業重要的資產。隨著電子商務的發展，數以萬計的企業更以網站購物爲主，幾乎可說是其生存命脈。確保網站是安全的沒有被攻擊或者淪陷 (compromised) 作爲駭客擷取資料或作爲跳板主機是最基本的第一步。一個安全的網站能夠得到網站來訪者的信任，才有可能促成一個網路上的交易行爲，一個能夠保障交易雙方的安全的網站才能帶來購物者及店家的雙贏局面。

那我們怎麼確保網站交易是安全的呢？網路上最常用的是 SSL (Secure Socket Layer) 的資料保密機制，該機制能夠確保資料在網路中傳送是經過加密編碼的，不易被擷取。但僅僅是傳輸中不被擷取，但後端的的伺服器主機是安全的嗎？如果是的話，我們怎麼知道呢？故**網站安全標章**因此產生。如果一個經由認證的安全稽核系統每天對網站進行弱點稽核掃描，經過掃描沒有新的弱點者給予安全標章，換言之若有新的弱點會影響系統時時，該安全標章就不能夠顯示；如此反覆進行對弱點的發現、評估 (assessment)、分析 (analysis) 、修正 (remediation) 最後給予標章的過程，便能夠確保這個網站是安全無虞的。

圖 3-3. HACKERSAFE 網站安全標章

國內尚無對這個弱點掃描程序的官方規範，而在美國有所謂的業界規範，例如 Visa 公司的CISP (Cardholder Information Security Program) [6] 中規定的弱點掃描部分及 MasterCard 公司 SDP (Site Data Protection) [7]。

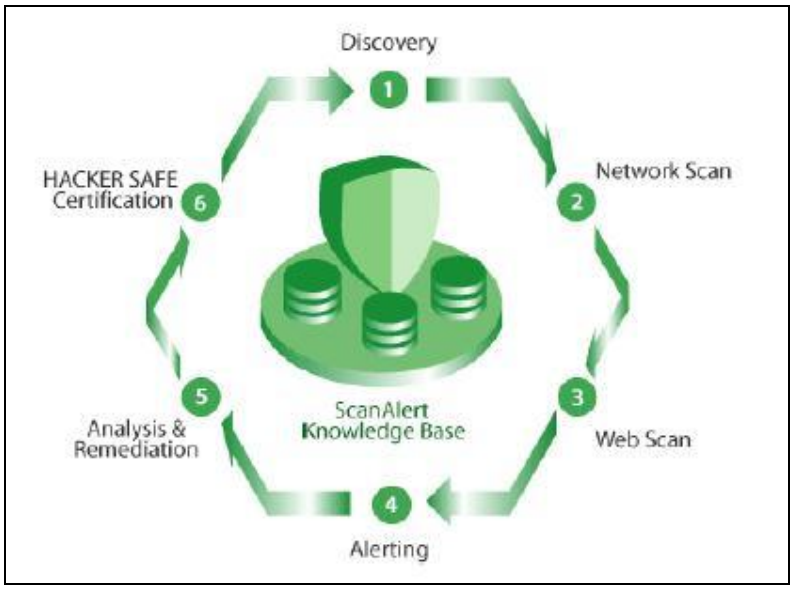

圖 3-4. 每日的弱點掃描及標章產生過程

3.3 HACKERSAFE 產品及解決方案

要自行開發一套網路安全稽核系統是一向高門檻且維持不易的。對於規模不大的時候，我們可以基於一些 open source 專案加以開發，如 Nessus，沿用其弱點資料庫，取之 open source 社群的眾專家之力，並貢獻回饋給社群，但並不是各企業都是專精於網路安全，且有能力去判讀這個發現的弱點爲何，是否爲誤判 (false positive)？如何修補？此時就需要一個完成的解決方案，不僅可供 HiNet

IDC 內部使用，並且可提供給客戶使用。本次奉派到美國實習，即到一家專精網路安全的公司 ScanAlert 實習。透過他們的技術展示及研討，得知 HACKERSAFE 產品即是一個不錯的網路安全稽核產品，並且已有超過 60,000 個網站使用其安全標章[8]，及超過 100 個案例證明其簡單易用的稽核系統確實值得。

在此就我實習的結果，提出以下三個該系統的優點，並於文後總結該系統作爲 HiNet IDC 加值服務的可行性探討。

3.3.1 不間斷的多層次掃描

就像其他的弱點稽核系統一樣，HACKERSAFE 配有一個弱點資料庫，一個弱點管理入口網站，分散式的掃描網路，每日的掃描以及時以電子郵件作弱點回報。比較不一樣的是，HACKERSAFE 每 15 分鐘會從幾百個不同弱點發現來源檢查是否有最新的弱點，並且驗證其正確性，及其正確修正方式。本身的主機都有 7x24 的監控，確保其可用。分散式的掃描架構可以依照需求，將分散於全球 20 個國家的客戶之掃描工作可靠地分派給位於不同的掃描主機 (Scan Appliance) 去掃描。

下一代的安全工具所做的是事前的 (Proactive) 弱點掃描及深度的 (penetration) 測試，正是 ScanAlert 所帶領的方式[9]。亦即此一安全工具可以模擬駭客一樣的去嘗試入侵，找出可能的弱點，更包含了網頁程式的弱點掃描 (Web Application Scan)。這是一般防火牆、SSL 無法做到的事情。一但弱點被發現之後，使用者會馬上收到一封 Alert 的電子郵件，但該次掃描所得到的結果如開放連接埠、弱點資料等並不會出現在這個 Alert 電子郵件上，使用者必須以帳號密碼登入到管理的入口網站才能獲得資訊。

每日的稽核分爲下列三個不同的步驟：

- Phase 1: 發現連接埠掃描 (Port Discovery Scan)
  不論是入侵或者預防入侵，掃描連接埠都是最重要的第一步；ScanAlert 的動態埠掃描可以針對桌上型 PC、主機、到防火牆、IDS、IPS 等等。
- Phase 2: 網路服務掃描 (Network Services Scan)
  決定什麼服務監聽 (listen) 在什麼連接埠上；決定是什麼軟體、如何被組態的。
- Phase 3: 網頁應用程式掃描 (Web Application Scan)
  我個人認爲掃描到網頁層是最困難的挑戰之一，根據 Gartner Group 的產業分析得知，預估有 70% 的安全漏洞都是發生在 Web Application Layer。ScanAlert 的第三層掃描便能偵測出全部的應用層弱點，如 code revelation、cross-site scripting 及 SQL injection。

3.3.2 弱點管理入口網站

空有一個功能強大的稽核系統如果沒有一套簡單易用的操作介面也是枉然。使用者需要知道我有什麼弱點，我要如何更新系統程式來除去這個弱點。在我實際看到其使用者 Portal 之後，發覺 ScanAlert 的 Vulnerability management Portal 使用很簡單，其具有下列功能：

- 互動式的弱點管理
  其弱點網頁並不是列出洋洋灑灑的 10 大頁告訴你弱點在哪，而是具有分類、排序的顯示方式。進而產生 PDF 報表。
- 設備分群
  使用者可以依照設備種類、所在位置、功能等等方式自訂分類，然後依照不同的群組進行排程、修正或者產生報表。
- 排程或手動掃描
  有些會影響到主機效能的掃描選項，如 DoS (Denial of Service) 及嘗試攻擊 (Full exploit) 的掃描方式只能手動排程。
- 多使用者角色
  擁有階層式的多使用者角色環境，安全管理者可以集中式地指派不同的角色定義不同的工作給不同的使用者。
- 報表產生
  我認爲這也是 ScanAlert 的優點之一，你可以產生有趨勢分析的摘要報表或者詳細的技術報表，甚至客製化你的報表範本。

圖 3-5. 簡單易用的 ScanAlert 弱點管理入口網站

3.3.3 網路架構及支援服務

營運 HACKERSAFE 的伺服器主機位於一個安全的 IDC 裡面，我相信跟中華電信一樣，非常重視服務的可靠性及安全性。其網路架構也是多層次的，除了快速的網路連結外，主機也都有 redundant 的設計，以負載平衡器及群組伺服器來確保高可用度(High Availability)。在負責掃描的 Scan Appliance 方面，他可以分散置於世界各地，其中的資料傳輸都以加密 VPN 方式與主中心的伺服器連結。參訪時，筆者也曾經請求其技術長 Scott 實際展示其管理後台，對其技術與支援方式印象很深刻。對於如何引進，如何去行銷，如何去技術支援，ScanAlert 公司都有不錯的方式來進行。回國之後旋即進行試用，並且在機房內建置 Scan Appliance，截至目前結果都還不錯。

圖 3-6. 於 ScanAlert 公司進行實習過程

4 新一代的網路安全系統

4.1 網路安全的面面觀

2003 年初剛開始，各地紛紛傳出不明原因的網路攻擊事件，導致各區網路骨幹一度因此而癱瘓或無法提供正常運作，結果是因爲 SQL Slammer 蠕蟲病毒所造成的，SQL Slammer 感染了 20 萬台沒有安裝修補程式的微軟 SQL Server。該蠕蟲估計在病發十分鐘內便感染了 90% 有漏洞的伺服器。並且發送大量的 UDP 封包，阻斷網路的正常運作；縱觀賽門鐵克、趨勢科技和矽塔科技的 Sophos

統計顯示，求職者病毒（W32.Klez.H）也不遑多讓，而且災情每日不斷，變種速度也愈來愈快。

回顧 2004 年，第一季就有 12 次重大病毒爆發，是因爲 BAGLE、MYDOOM 及 NETSKY 三種病毒不斷出現新變種。。5 月 Sasser 感染全球無數電腦，許多個人及企業未能及時安裝漏洞修補程式，繼而蒙受嚴重損失。7 月網路仿冒詐欺 (Phishing) 陷阱大量出現，案例在短短兩個月內增加 28 倍，令許多警覺性不足的用戶被騙取銀行帳戶密碼等機密資料。 8 月是病毒感染案例最多的月份，比案例最少的月份高出 10.5 倍。 11 月感恩節前後，有黑客以電郵向用戶發出虛假的獲獎通知，誘騙用戶到假冒的網站輸入信用卡號碼等個人資料。12 月 WORM_ZAFI.D 病毒僞裝爲聖誕賀卡郵件，藉此四處散播。

於 2004 年 5 月至 11 月間，在趨勢科技所監察到的網路仿冒詐欺(phishing)事件中，以花旗銀行(Citibank)作爲首要目標的數量最多，佔總數 52%；排行第二的目標是美國銀行，是全美最大的金融服務機構之一，佔總數 21%；排行第三的 Suntrust 佔 10%，而知名拍賣網站 eBay 則以 8%排行第四。而 8 月是惡意程式最活躍的月份。趨勢科技於該月共發現了 3,809 個惡意程式，佔全年總數 23%。[10]

一連串的全球病毒爆發事故，令 2004 年的網路動盪不安。黑客透過控制其他電腦、盜取機密數據或詐騙手段取得金錢利益，成爲了網路攻擊事件頻傳的原因之一。快速增加的 Bot 遙控程式、垃圾郵件、網路仿冒詐欺、以及越來越猖獗的間諜軟件 (spyware) 與廣告軟件 (adware)，顯示現在的網絡攻擊十分全面化 (sophistication)：網路環節的每個弱點、每台未修補漏洞的電腦、每位欠缺警覺性的用戶，都是黑客的攻擊目標，成爲他們賺取利益的機會。黑客的攻擊技術日新月異，惡意程式傳播的速度與範圍也大幅增加。這些惡意程式多數不會在特定日期內發動攻擊，而是隨時出現、隨時令用戶蒙受損失。

4.1.1 產生威脅的技術提升

承上所述，各種威脅及攻擊越來越快速，需要 IT 人員更快速的反應。惡意程式碼 (Malicious Code) 的攻擊增加，混雜的攻擊針對不止單一的應用程式，而且越來越聰明，如 IIS、IE、SQL、Exchange，甚至 P2P 的即時通訊軟體 (Instant Messaging) 都是目標。而且，爲了出名的動機減少，取而代之的是對於偷取財務或擷取個人資料。我們還觀察到造成這些威脅的技術越來越高超：

- 混合式的 (blended) 方法造成大規模的阻斷攻擊
  如 Blaster、MyDoom、DeadHead、DoomJuice
- 透過網路快速散佈
- 大量的寄件者借自大眾的地址簿 (address book)
- SPAM 用來夾帶病毒、惡意程式碼、網路仿冒詐欺 (Phishing)
- 透過感染植入的後門進行遠端執行或發動 DoS 攻擊

- 利用 P2P 軟體及 MS 協定攻擊
  如 TCP/4662、TCP/6346、UDP/41170、TCP/445、UDP/137
- 社交攻擊法
  - 騙使用者安裝或執行惡意程式碼
  - 假冒網站偷取有用資料
- 灰色軟體 (Grayware) 快速成爲企業的擔心的對象

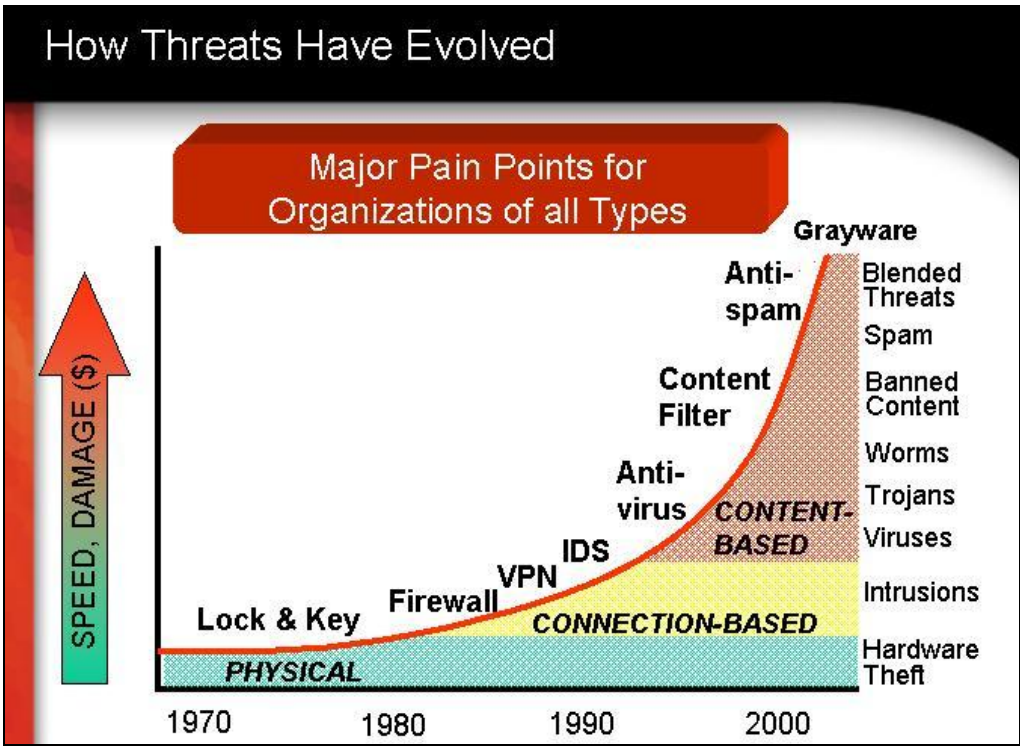

圖 4-1. 各種網路安全的威脅

4.1.2 灰色軟體

何謂灰色軟體 (Grayware)？灰色軟體即是一種不請自來的軟體，通常使用者在不知不覺或是不懂的情況下安裝，該軟體會蒐集資訊或者追蹤使用者行爲。可分爲下列幾種：

- 廣告軟體 Adware - Toolbar Editors - Browser Helper Objects
- 自動撥號軟體 Dialers - Web Page Hijacker - Download Programs
- 小遊戲 Game - Browser Plugins - Keystroke Loggers
- 笑話 Jokes - Network Management Tools - Peer2Peer
- 間諜程式 Spyware - Remote Administration Tools

使用者並不知道他們是多麼容易被植入灰色軟體，可能是按了一個按鈕，可能是下載了一個小遊戲，然後他的按鍵就被側錄了。黑客們也可使注意到灰色軟體的技術，來讓使用者執行他們的惡意程式碼。灰色軟體可以產生新的威脅，因

爲作業系統的修補程式、傳統的防火牆跟防毒軟體並沒有辦法提供保護。威脅包括了：

- 使用者資料被竊取，傳送給黑客
- 按鍵被錄下來，其中包含了使用者名稱跟密碼
- 搜尋硬碟中的資料，讀使用者的 Cookies
- 加入工具列的惡意後門軟體
- 讓使用者的瀏覽器不聽使喚，重導到其他站台或者限制在某個站台
- 利用使用者數據機撥打高額付費電話
- 讓電腦當機 crash，以增加 IT 人員的負荷。

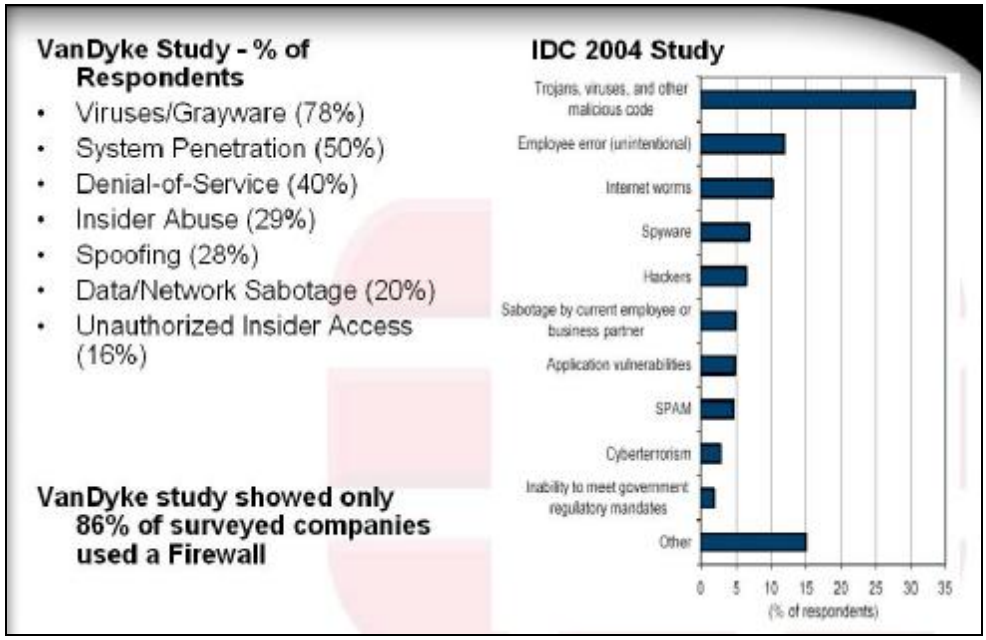

圖 4-2. 企業的安全考量

4.1.3 企業的安全考量

根據各家的調查結果，灰色軟體很快的就成了企業十大擔憂 (concern) 的前幾名，政府也開始正視這個現象，制定規範來使電子通訊更安全。企業也很注意員工的生產力 (productivity)、合法的義務及使用網路資源，表示他們需要規範員工們的網頁內容 (Web contents)。

要如何將這些威脅逐出企業呢？傳統的防禦模式是將防火牆跟 IDS 放在周圍，然後將企業內部跟外部分爲信任的與非信任的兩個區域，從外部進來的攻擊由防火牆跟 IDS 把關，但內部的病毒威脅、是定期更新都倚賴內部基於主機的管理軟體；並且員工從家裡的的遠端存取、外地員工的行動存取、以及連上無線網路的 AP 都會造成此一防禦模式的瓦解。

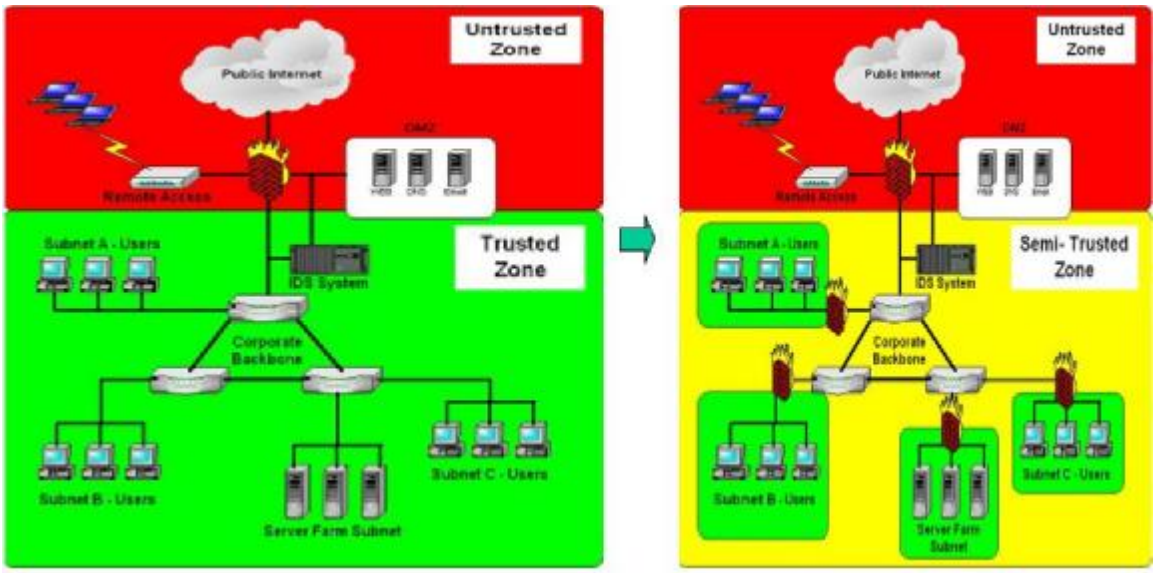

圖 4-3. 傳統的防禦模式到新一代的防禦模式

許多的安全威脅及攻擊實際上是存在於企業內部，所以信任區域(Trusted zones) 縮小了，變成各個區域都必須有防火牆管控，設定使用者的存取權限及防禦威脅的行爲，才可以有效降低內部主機受到感染的速度及未經授權的存取。

4.2 新一代的網路安全防禦系統

新一代的安全防禦系統不僅僅是防火牆加上入侵偵測系統，必須還要有能夠主動防禦的入侵預防系統 IPS (intrusion prevention system)系統、基於網路的掃毒系統 (Network based AntiVirus system)及網頁內容過濾系統(Web content filtering system)才足以對付快速爆發的網路安全威脅。以下列章節逐項敘述之。

4.2.1 入侵預防系統 IPS

首先以下列表格說明入侵偵測系統 (IDS)與入侵預防系統(IPS)的比較。

入侵偵測系統	入侵預防系統
被動模式、mirrored traffic	網路流量通過
只有告警機制	事先攔阻惡意的流量及告警
失效的話並不影響網路流量，但無法進行偵測	失效的話會影響到整個網路或丟棄封包
誤判是惱人的，不影響正常流量	誤判會攔阻正常流量
不會是效能的瓶頸	若偵測引擎不夠強的話，會是效能瓶頸
可靠度比起 IPS 來說並不要緊	可靠度非常重要

新一代的 IPS 系統是位於網路上流量會通過的點上，作 inline 模式的檢測與攔阻，而其並不是一種基於 IDS ”反應式” 的系統，止於產生告警、送出 TCP reset、或重新組態防火牆的規則而已。他要能夠偵測流經過的任何的連接埠的惡意流量，而且在該惡意行爲造成災害前分辨出來並加以攔阻。故一個新一代的 IPS 必須含有下列幾部分：

- 標準的 IDS
- 及時的 IPS 防護
- Stateful Firewall
- 封包重組功能 – 修正失序(out-of-order)、切割 (fragmented) 及重疊的 IP 封包，在送出到目的主機前。

在世界最主流的網路、通訊、資安相關產品測試的 NSS Group 對現代 IPS 的需求定義如下[11]：

- In-line Operation
- Reliability & Availability (fail-open, real-time updates, etc)
- Resilience (HA clustering, fail-over, etc)
- Low Latency (performance)
- High Performance (packet processing speeds with signatures on)
- Detection Accuracy (low false positives)
- Fine-grained Granularity & Control (what to block)
- Advanced Alert Handling & Forensic Analysis

更重要的是，IPS 不能阻擋正常流量，或者過度影響網路效能。

4.2.2 基於網路的防毒 AntiVirus

相較於我們每天在使用的基於主機(Host-based)的防毒系統，這是一個比較新的觀念。直覺上認爲幾乎不可行。此種掃描方式很好，因爲對於網路或使用者來說，幾乎是透通的(transparent)，而且如果將病毒與 grayware 在網路上就解決掉，則可以大大減低公司內部的病毒感染及內部 PC 發生問題的機會。然而在一般 PC 安裝了防毒軟體後，主機的效能常常因此受到影響，更何況是在當封包還在網路上這麼短的時間內，如何快速比對掃描？

此行拜訪了 Fortinet 負責 Antivirus 的 AV 實驗室，詢問了該負責的 team leader，得到的答案是：快速針對還在野外散佈發作的病毒 (Wild list) 進行掃描即可。相較於 PC 上的防毒軟體，花很多時間在掃描所有已知 “動物園” 中的病毒，是可以節省不少時間。至於要如何知道哪些病毒正在世界的某處發作，就靠世界各地不同來源的回報機制及 Antivius 業界的互通有無來維持這個風險資料庫，提供最及時的掃描服務。

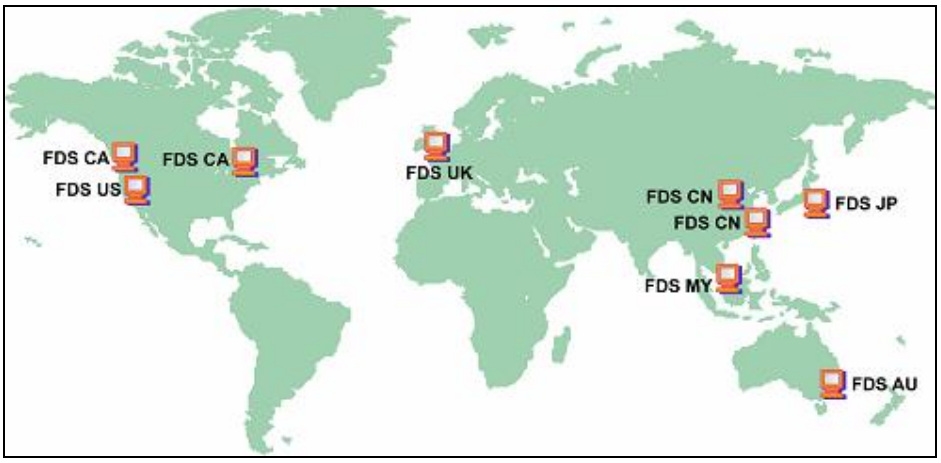

圖 4-4. 最新病毒資訊的蒐集需要來自全球各地

4.2.3 網頁資料過濾(Web Content Filtering)

全球資訊網是一種重要的革命，但有其缺點：

- 員工降低生產力，因爲非工作所需
- 非法的下載及不正確使用
- 智慧財產的議題，如音樂、電影的下載
- 使用越多的頻寬代表需付出更多的支出
- 經由不安全的傳輸將敏感資訊存放於公眾網站，如免費的 webmail 或 web 儲存空間
- 非公務的 Internet 存取造成病毒、spyware 等的感染

許多新的攻擊是基於網頁的，例如黑客攻陷合法的網站，利用其讓使用者感染、在使用者不知情的情況下，惡意的程式碼下載植入使用者電腦中以竊取資訊等等。

我們可以透過以下的方式過濾網頁內容：

- 攔阻字表 Banned Word List
- 阻擋網址 URL Block / URL Exemption
- 特徵比對 Pattern Matching
- 分類內容排名 Category Content Rating and Blocking

4.2.4 整合威脅管控(UTM)

'The UTM market is being created because it is quickly catching on with customers and vendors. UTM incorporates firewall, intrusion detection and prevention, and AV in one high-performance appliance." -- IDC, 2004

綜合前述新一代的網路安全防護系統的特點來說，資訊安全設備的需求已經漸漸地從單點式的產品發展到多個功能整合在單一平台上，IDC 稱之爲整合威脅管控(UTM, Unified Thread Management)的產品，其包含數種資訊安全功能，整合有防火牆、入侵偵測與預防、與閘道防毒等功能，甚至內容過濾、防垃圾郵件等功能。IDC 預測會有越來越多的供應商朝向提供這種服務。[12]

Worldwide Threat Management Security Appliances Forecast, 2004-2008 ($M)

	2003	2004	2005	2006	2007	2008	2003 Share (%)	CAGR (%)	2008 Share (%)
Firewall/VPN	$1,479.1	$1,667.7	$1,791.6	$1,804.4	$1,823.5	$1,462.3	93.4%	-0.2%	42.4%
UTM Security Appliance	$104.9	$225.0	$517.5	$828.0	$1,324.8	$1,987.2	6.6%	80.1%	57.6%
Total TM Security Appliance	$1,584.0	$1,892.7	$ 2,309.1	$2,632.4	$2,948.3	$3,449.5		16.8%	

表 4-1.全球的 UTM 安全產品預測

4.3 Frotinet 產品及解決方案

4.3.1 Fortinet 產品特點

此行參訪實習的 Fortinet 公司，目前爲業界在 UTM 方面第一的位置，其防毒防火牆產品 FortiGate 結合硬體與韌體，以提供完整的網路層及應用層安全服務平台，特點包含最著名地動態威脅預防、木馬程式保護、與防毒軟體結合的入侵偵測預防(IDP) 防火牆等。透過 FortiGate 平台，用戶得以突破傳統，將網路防毒 (Antivirus)、防火牆 (Firewall)、入侵偵測(IDP)、VPN、內容過濾、anti-spam、spyware 偵測和預防，及流量控管等七大功能平台合而爲一。Fortinet 可將具威脅性的資訊分享及散佈至其每一個安全元件中，以保護客戶的資料得在現今的網路環境中安全地傳輸。

值得一提的是，Fortinet 從一開始就設計將許多原本軟體做的事情在 ASIC 完成。故其產品能夠快速的對於經過的流量加以重組、威脅偵測及過濾等等。傳統的防火牆由於是純粹做到網路第四層的偵查，故封包並不會重組而無法過濾新的威脅。傳統的 IDS 的深層封包檢測也因爲是不是 inline 模式，且不會將封包組合起來再檢測，故都可能無法攔阻一些新的威脅。唯有將封包組合起來 (Reassemble) 成原本內容再處理，才有辦法做到完整的內容保護。

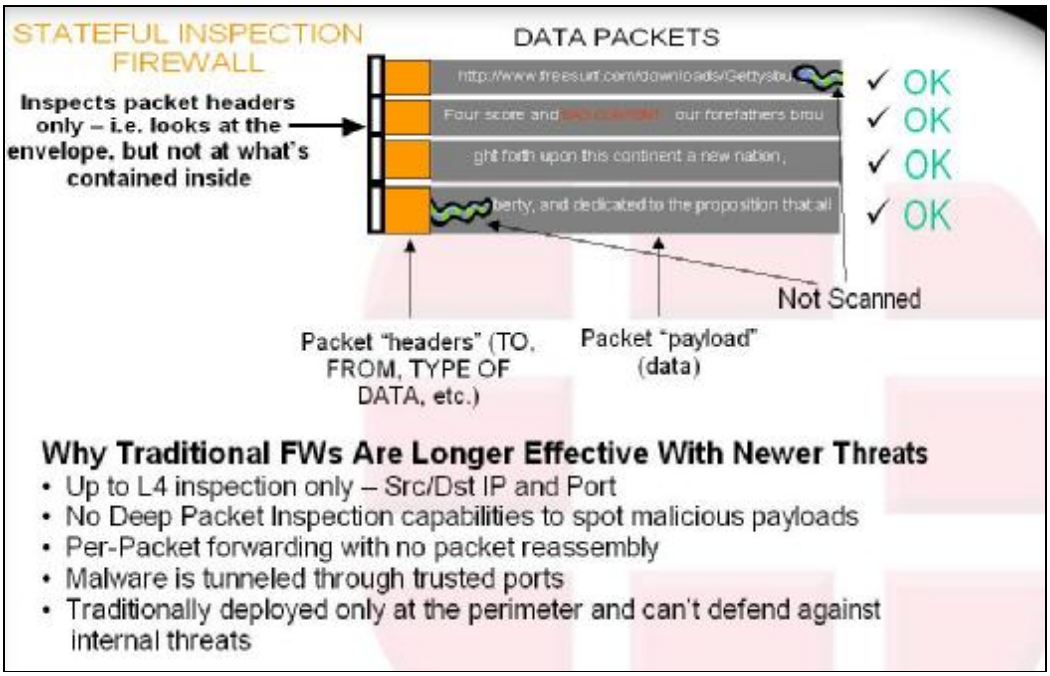

圖 4-5. 傳統 stateful 防火牆不容易進行深層封包檢測

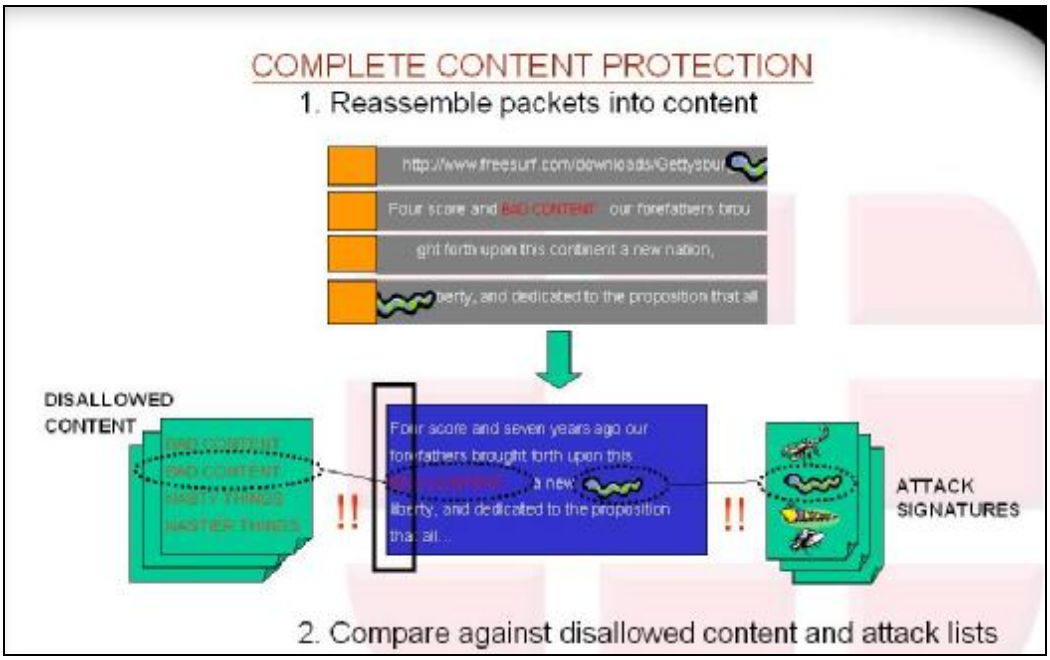

圖 4-6. 唯有將封包組成內容，才有辦法停止 Content-based 的威脅

4.3.2 Fortinet 的解決方案

Fortinet 公司對於企業用戶、中小型企業及服務供應商 (如 HiNet IDC) 都有提供完整的產品及解決方案，全系列的產品分成下列幾部分：

- 核心技術

Fortinet 的核心技術爲 FortiASIC 與 FortiOS，全系列的產品都配置。其 FortiASIC 是專屬內容處理晶片(Content Processor)，FortiOS 爲其產品的作業系統。這兩者提供了 FortiGate 系列產品各項功能。

- FortiManager 管理平台

提供單一集中式的管理平台，便於管理所有的 FortiGate 防火牆產品。

- FortiProtect 網路

此一網路提供了 Fortinet 系列產品的病毒定義更新，攻擊特徵更新等重要的服務網路。對於中華電信 IDC 來說，我們可以利用其產品提供專屬的 UTM 給 IDC 用戶使用。

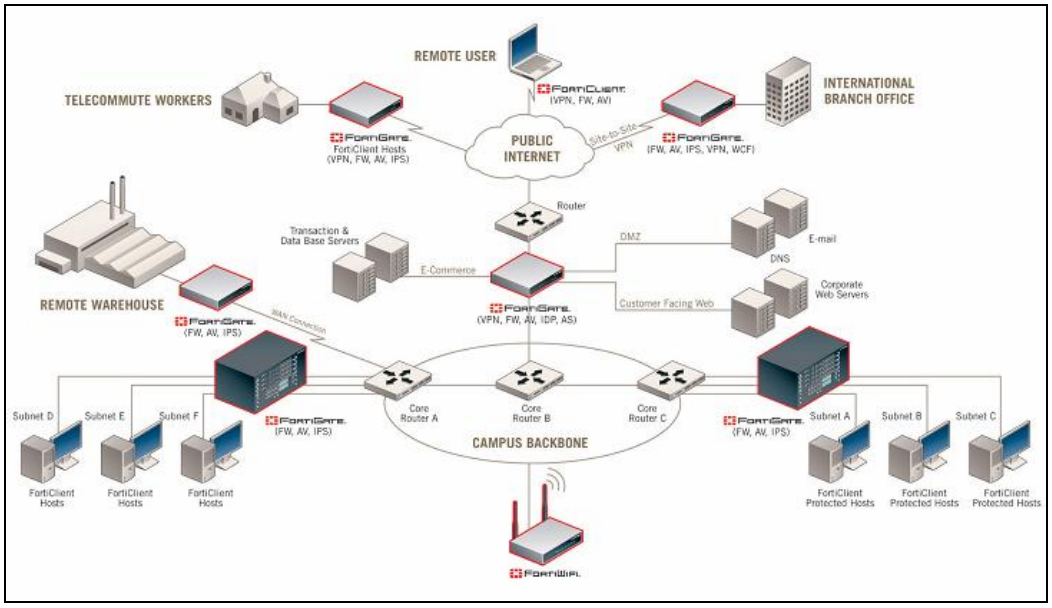

圖 4-7. Fortinet 提供企業的 UTM 產品

圖 4-8. Fortinet 在 IPSec、Antivirus、Firewall、IDS 的認證

5 心得及建議

2005 年將是各種全面化的攻擊快速增加的一年：遠端遙控程式、垃圾郵件、網絡仿冒詐騙、越來越猖獗的各式灰色軟體(spayware、adware)融合了系統弱點進而攻擊的病毒等等。企業需要一個能夠保護的機制及工具，讓其網路不被這些接踵而來的攻擊影響，藉由安全的網路建立其客戶的信任及商譽。這些正是重視專業分工的 IDC 提供加值服務的契機。

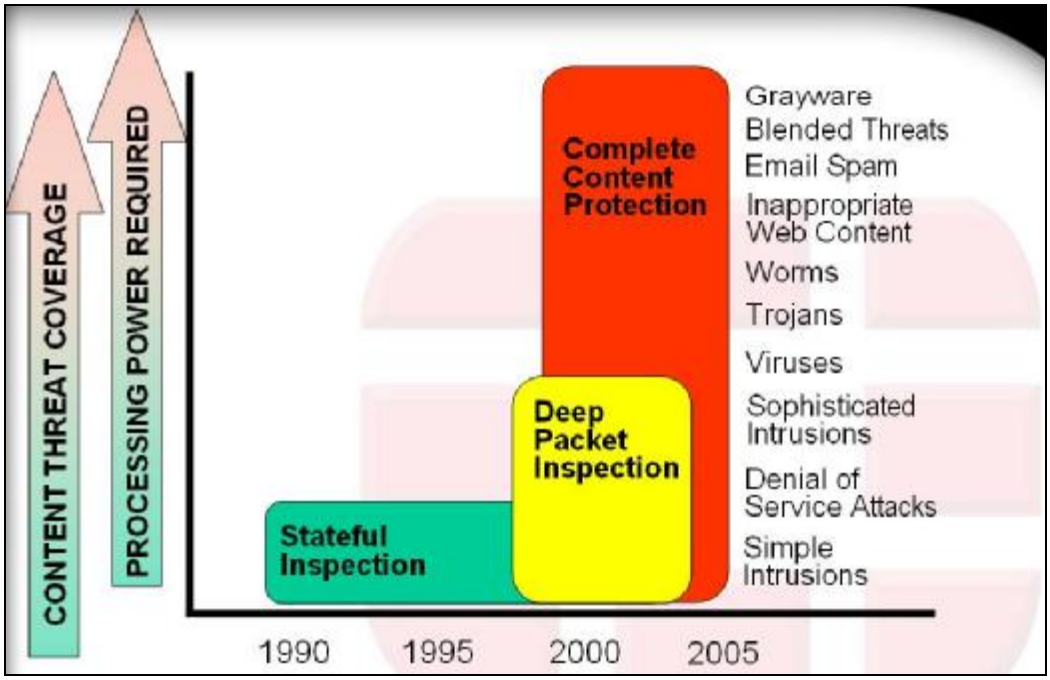

圖 5-1. 網路安全產品必須革新以應付日新月異的網路安全威脅

本次赴美國、加拿大實習，針對路安全方面可能面臨的弱點威脅，找出 ScanAlert 與 Fortinet 的解決方案。 ScanAlert 提供的 HACKERSAFE 網站安全標章，其實是一個具有弱點管理功能的風險管理系統，對於系統的弱點進行每日的稽核，讓使用者很快的找到修補的方法；Fortinet 的防毒防火牆系列產品，是最新的整合威脅管控 (UTM) 系統解決方案。我想都是符合 IDC 客戶的需求，能真正幫助用戶的網路安全工具。故提出以下幾點建議：

1. 引進 ScanAlert 與 Fortinet 技術及產品，透過教育訓練讓 IDC 內部人員了解網路安全的新威脅及處理方案，改進 HiNet IDC 的體質。
2. 利用其既有產品，提供網站安全標章及 UTM 產品租賃加值服務。
3. 從產品的維護過程中，與廠商互相合作，例如協助其蒐集攻擊手法、spam 的糖罐 (honeypot)等，以學習更多的安全中心 (SOC) 核心技術。

最後期望這次的出國研習，能使得 HiNet IDC 提供更完善的加值服務，達到整合全方位服務。

6 參考資料

1. Fyodor, “nmap: Network Mapper”, http://www.insecure.org/nmap/, Sep. 1998
2. Renaud Deraison, “Nessus is the world's most popular open-source vulnerability scanner used in over 75,000 organizations world-wide.” http://www.nessus.org/, Apr. 1998.
3. Sullo and Forrest, “OSVDB is an independent and open source database created by and for the security community.” http://www.osvd.org/ , Aug. 1, 2003
4. TWCERT/CC 網路安全檢測系統(SAS , Security Auditing System), http://www.cert.org.tw/service/VulDB/ , Jan. 2004
5. CHTD 資通安全技術中心, “HiNet SOC: 全球資安預警情報網”, 數據分公司內部網站 http://hicert.chtd.com.tw/ , 2004
6. Visa company, “CISP Vulnerability Scanning session”, http://www.visacisp.info/, Apr. 2000
7. Mastercard , Industry Standard, “Payment Card Industry Data Security Standard “, https://sdp.mastercardintl.com/ , Jan. 2005
8. ScanAlert, “FIND HACKER SAFE SITES”, http://www.scanalert.com/directory/2/52/index.html, Feb. 2005
9. ScanAlert, “ScanAlert Technology White Paper’, http://images.scanalert.com/pdf/ScanAlert_Technology.pdf , Dec. 2004
10. TrendMicro, “2004 年網路威脅報告”, http://www.trendmicro.com.hk/html-pccillin/news/news_20041231.htm , Dec. 31, 2004
11. NSS Group, “Intrusion Prevention Systems white paper”, http://www.nss.co.uk/WhitePapers/intrusion_prevention_systems.htm , Jan. 2004
12. IDC Taiwan, “台灣資訊安全市場，由單點防護走向整合性之資安解決方案”, http://www.idc.com.tw/report/news_050105.htm, Jan. 5, 2005