網路、資安與管理，一舉到位

網路運作、資安防護、管理維運不再拼拼湊湊各自為政，HP 為您提供一個品牌的網路資安結合新架構。

維持網路與所有系統正常運作是 IT 人員追尋的目標

在組織花費龐大的經費建置網路基礎架構、資料中心、各種軟體系統後，如何維持這些 IT 系統的正常運作，沒有效能緩慢甚至發生伺服器無法提供存取服務的問題，一直是 IT 人員每日的首要任務。觀察現今組織內發生的網路異常狀況，比例上甚少是因為基礎建設硬體損壞或是對外頻寬不足所造成，況且這類的問題處理起來並不困難。真正讓 IT 人員頭疼不已的狀況是時好時壞的效能；短暫性與間歇性的網路癱瘓；以及服務系統無法回應使用者請求的狀況。組織的管理階層常常質疑為什麼投入了龐大 IT 建置經費卻換不到系統時時刻刻維持順暢無虞的穩定度。究其根源，主要是導因於組織對 IT 系統出現異常問題前的預防措施與出現異常問題後的即時除錯能力尚未臻完善。其實，今日的網路冗餘與負載平衡技術已經相當成熟，網路頻寬價格便宜，各種應用於網路上的硬體設備功能齊備，伺服器的處理效能與日俱增，加上雲端架構的蓬勃發展，照理說不應該發生網路不通或是服務無法存取的窘況。然而，大家共同的經驗是處理異常狀況總是佔去了 IT 人員絕大多數的工作時間。組織不禁要問：這麼多的異常問題到底從何而來？有沒有方法可以即時找到造成異常問題的根源，快速且精準的處置？身為全球最大的 IT 供應商，HP 為客戶所提供的不僅是從網路到資料中心全系列的優質基礎建設，我們更重視協助客戶在 IT 建設完成之後做好維運工作，讓龐大的 IT 建置經費能夠真正發揮該有的效益。在本文中，我們將從資安的角度出發，深究探討組織的上網管理與端點防護需求、如何有效提升網路與服務系統的可靠度不受異常事件的干擾、因應個資法規要求等議題，以期為客戶找到真正有效且好操作的維運方式。

組織的上網行為控管

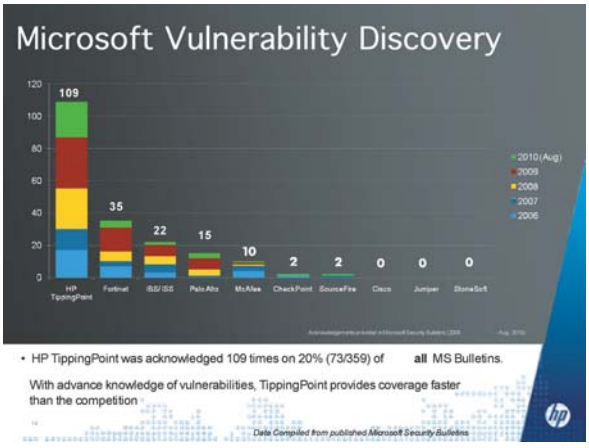
隨著網路上衆多應用服務如雨後春筍般出現，大部分的組織會制定管理內規用來規範人員瀏覽網際網路與使用網路服務的行為，諸如：P2P 與 MSN 傳檔的禁用；Facebook 與影音串流的管制；阻擋個人私建躲避防火牆管制的 VPN 通道等。這類的上網行為除了影響組織生產力之外，P2P 與 IM 軟體傳檔功能濫用的結果往往造成網路效能的沉重負荷、智慧財產侵權甚至組織重要資料的外洩。而 WEB 2.0 的互動功能早已成為駭客向組織內人員散播惡意程式的方便管道，就在人們觀賞微網誌、部落格或是社群網站的同時，惡意程式已經悄悄植入使用者的電腦，進行個資的竊取或是當成攻擊他人的跳板。

全球首屈一指的入侵防禦系統 HP TippingPoint 內建 AppDV＜應用程式數位疫苗＞能辨識數百種網路服務包括 P2P、IM、串流影音、社群網站、線上遊戲、VPN Tunnel/Proxy/ 遠端連線軟體、Web Mail 等等，並可依據組織的管理政策實行阻擋、監控或是限頻動作。然而上網政策的制定通常無法一視同仁，必須跟隨組織內各單位業務屬性的不同而設立適當的規範：例如某企業禁止上班時間員工使用 Facebook 服務，但是行銷部門因為有活動推廣的需求，在 Facebook 的管理政策上是允許通行的。採用新一代 XLR 網路晶片作為運算核心的 HP TippingPoint IPS 擁有優越的處理效能，能夠讓 IT 人員彈性的設定多個檢查與管理政策在同一部 HP TippingPoint 設備上卻沒有效能問題。

零時差與漏洞入侵的防護

駭客的終極目標就是要將他人的電腦設備佔為己有，戮力研究各種系統的漏洞並找到入侵手法一直都是全球駭客的首要課題。而當一個系統的漏洞被發現之後，該系統的研發原廠應立即修改程式，並發佈 Patch 讓使用者進行更新的工作以免遭駭。倘若研發原廠對漏洞修補動作回應時間太冗長導致遲遲無法提供 Patch 補丁給用戶，而在這段空窗期間駭客已經製作完成惡意程式並且開始進行入侵行為，這就形成了＜零時差攻擊＞，組織裡的電腦系統將面臨極高的入侵風險。不過，IT 部門常遇到的另一個狀況是：明明 Patch 已經可以下載了卻無法立即安裝更新系統！主要原因是軟體部門需要時間測試這個 Patch 是否會影響到既有運行中的程式；另外對許多組織裡的重要服務系統而言，維運部門也必須等待每月定期維護時間才能執行 Patch 安裝後的系統重開動作，導致系統曝露在風險中的時程拖得更長。

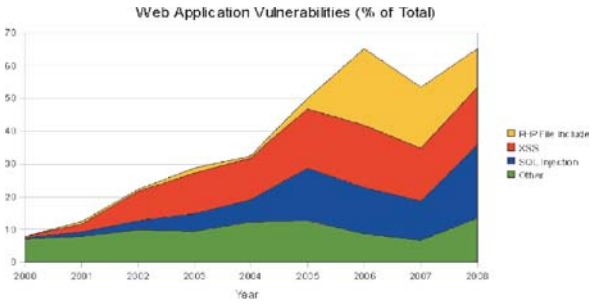
HP TippingPoint 多年以來致力於全球各種重要系統的漏洞研究上，其中 ZDI＜Zero Day Initiative http://www.zerodayinitiative.com/＞計畫結合了來自各國千名以上的資安專家共同為漏洞入侵提出防禦方案。以微軟系統為例，從 2006 年到 2010 年為止，HP TippingPoint 的 DVLabs 小組總共替微軟找到 73 個漏洞 (佔總數 359 的 20%)，提供給微軟作為修補漏洞的參考依據，微軟在官網的 Bulletin 中更提及 HP TippingPoint 達 109 次，這個研究成果遠優於其他競爭友商，所有建置 HP TippingPoint IPS 的客戶能夠最早最即時擁有防護能力，無須擔心＜零時差攻擊＞的為害。其延伸的效益還有：建置在資料中心入口處的 HP TippingPoint IPS 能夠阻擋漏洞入侵的攻擊行為，讓 IT 人員有充足的時間慢慢研究軟體相容性，也無需擔心定期維護時間未到無法重開系統的問題。



資料庫重要資訊的防竊

資料庫裡儲存的資料有著其重要性，這是數位資產的概念。許多組織的管理者都同意必須為實體資產投保保險、聘請保全、設立進出門禁等保護作為，然而對於組織的研發設計藍圖、客戶與員工資料、價格與庫存等已經數位化的資產所作的保護確不如實體資產完整。駭客入侵 IT 系統的目的不外乎是金錢誘因，就像歹徒之所以會搶銀行，因為哪裡有錢。

資料庫的竊取技術對很多懂資料庫語法與架構概念的駭客來說進入門檻並不高，而且一但入侵成功其獲利又會非常豐碩，因此讓許多駭客爭相投入這個領域，我們可以從下方統計圖中看出 SQL Injection 型態的攻擊佔所有攻擊事件的比例逐年遽增中，也就表示，IT 部門迫切需要建立相對應的防護能力來防止來自駭客的資料庫竊取行為。



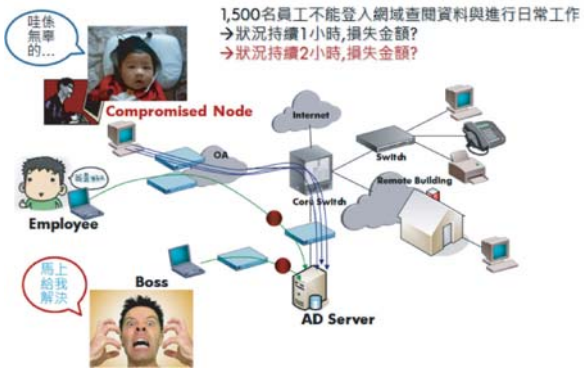
HP TippingPoint IPS 針對 SQL Injection 攻擊提供相當完整而有效的保護，我們建議組織將 HP TippingPoint IPS 建置在前端 Web Portal 與存取服務的 Client 之間。

暴力密碼猜測的阻止

除了透過漏洞入侵手法取得電腦的控制權之外，設法獲取管理者的帳號密碼資訊亦是駭客常用的方式之一。我們常遇見的帳號密碼取得技倆，包括運用社交工程詐騙類型的釣魚郵件 (Phishing) 以及發起巨量暴力猜測手段等。社交工程 (Social Engineering) 的防範之道多著重於人員的資安教育訓練方面，在技術做法上也可佈建 HP TippingPoint IPS，其內建的反釣魚 (Anti-phishing) 過濾器可保護組織裡的人員不會誤連釣魚網站。

本節的重點將放在談論如何偵測到暴力猜密碼的行為並予以立即阻絕。我們先來看一個實際案例：許多組織都會建置認證系統作為人員存取網路資源的檢查機制，其中微軟的 AD(Active Directory) 是運用非常廣泛的系統之一。為了安全性，IT 管理者會在 AD 上啓動認證錯誤管制作為：當某個帳號執行登入時卻連續敲錯密碼達一定次數時，系統會自動將該帳號鎖住，事後該帳號的使用者需要經過一個新密碼申請程序才能再次登入。在下述的實例中，這個看似正確的安全檢查機制卻造成該組織面臨多數員工無法登入網域從事工作的災害。

在某一個上班日，正當員工們開啓電腦欲登入網域開始一天的工作時，許多人發現自己的帳號遭到封鎖而無法登入。分析造成這個異常事件的原因是：組織內有幾部電腦設備遭植入惡意的暴力密碼猜測程式後假借員工身份對 AD 系統發送大量認證請求，肇致諸多員工帳號被 AD 鎖死而無法登入網域使用網路資源，嚴重影響到組織的生產力。



要根本解決這個問題就必須知道發動猜測的電腦在哪裡。過去這樣的大規模查找行動不僅相當耗費人力，效果也非常有限。現在駭客慣用的猜測作法都是分散到多台電腦並不定時輪流執行，以規避 IT 人員的追蹤。另一個更麻煩的問題是：IT 人員根本無法預期甚麼時候會遭到這樣的攻擊，缺乏一個準確的預警機制。

HP TippingPoint IPS 可以持續監控網路中 AD 登入失敗的行為，再透過自動學習機制了解組織過去的 AD 登入失敗行為曲線，用來比對每一分鐘的 AD 登入失敗次數是否合理，只要一發現異常突增情況，將立即通知 IT 管理者，並呈現出攻擊來源 IP、名稱、猜測次數以及在哪部網路交換機底下 (如果該 IP 位於內網中) 等資訊。下圖是實際的攻擊案例：

除了即時分析功能，HP TippingPoint IPS 亦提供方便好用的處置作為幫助 IT 管理者將這樣的攻擊瞬間排除掉，恢復組織正常營運。如果攻擊來自外部，IT 管理者可以下達阻擋指令到建置於 Internet 入口處的 HP TippingPoint IPS 上封阻後續的猜測行為；如果攻擊是來自內部，則阻擋指令能夠深入到 HPN L2 Switch 上，封鎖該 IP，避免惡意程式持續散播感染造成災害的擴大，等同於作到端點防護的效果。此外，IT 管理者也可以預設封阻時間的長短，系統將自動解除阻擋作為，大大減輕維運負擔。

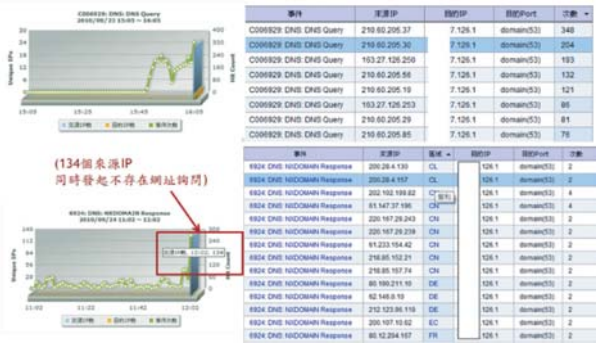
DDoS 與服務癱瘓攻擊的防禦

對組織而言，DDoS 防禦一直是個熱門議題。然而 DDoS 只是一個統稱，若要真正做到有效的防護，則必須逐一針對不同屬性的 DDoS 現象採個別研究模式，進而提出相對應的防禦手法。隨著頻寬建置的迅速擴充，加上價格低廉，傳統上發動巨量封包將頻寬損耗殆盡的 DDoS 攻擊型態正逐漸減少，取而代之的是針對特定服務的癱瘓，一樣可以造成網路近似停擺的效果，但是攻擊成本與難度卻降低許多。

我們可以將 DDoS 概分成兩類：一是每個攻擊端發送巨量封包，主要用意是侵蝕頻寬與造成網路設備如防火牆、線路負載平衡設備與路由器等的效能負擔；另一種則是集結眾多攻擊者一起發動服務請求，但是每一個攻擊者僅送小量的方式，訴求的目的通常是為了猜測帳號與資料竊取，也可用來讓伺服器的 CPU 飆高導致服務停擺。針對第一類的攻擊型態，HP TippingPoint IPS 透過 Threshold 的設定來制定每一個來源 IP 的可連線門檻，過濾超過合理值的巨量封包，達到保護的效果。

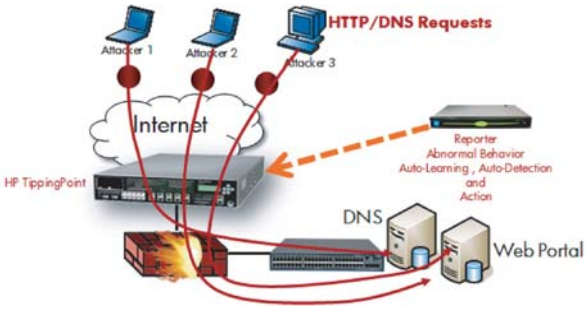
至於第二種 DDoS 攻擊類型則需要啓動異常行為自動學習機制作為監控的法則。這裡我們用另一個真實事件作為說明案例：一般來說，校園網路的基礎架構較其他型態的組織龐大，許多大學都擁有 1Gbps 以上的對外頻寬、大型的網路設備與效能優異的伺服器群等，如果要採用侵占頻寬的手法來癱瘓這樣規模的網路並不容易。然而，一個類似打蛇打七寸的巧打原理卻輕易地讓下述案例中的校園網路發生服務中斷的災害。

某個學校單位的資訊中心接獲許多師生的障礙報修電話宣稱校內無法上網，經過一連串的除錯發現原因出在 DNS 主機 CPU 值出現異常的飆高狀況導致無法回應師生的網域解析請求。該校建置有流量分析工具，並透過使用排序找到了重度查詢 DNS 的來源 IP，其結果呈現如下圖中的上半部表格。然而，列表中的來源 IP 群都是學術單位的 DNS，其查詢行為並無不妥。HP TippingPoint IPS 屬於第七層的資安設備，能夠深入分析各種 DNS 查詢行為對 DNS 伺服器所造成的影響。我們發現一種來自全球多個來源的＜不存在網址查詢 , NXDOMAIN 回應＞請求才是造成這次學校 DNS 服務癱瘓的主因。由於在 Cache 中沒有紀錄，查詢不存在網址動作往往會加重 DNS 伺服器的負載，而當我們的即時分析系統偵測到 NXDOMAIN 回應出現異常突增，IT 人員可以透過深入查詢功能即時找到集體發動 NXDOMAIN 查詢的來源 IP 群。運用下圖中的下半部表格資料，我們就能協助資訊中心清楚地了解這次 DDoS 攻擊的內容與手法：駭客運用網軍技術指揮多部電腦同時對這所學校的 DNS 發動不存在網址查詢，造成服務回應緩慢，影響師生的上網品質。過程中每部電腦僅發送少量請求，因此能夠輕易規避流量分析系統的監控不被找到。



HP 解決方案對於這個事件的處理流程是：HP TippingPoint IPS 持續在網路中監控 NXDOMAIN 查詢行為，分析系統根據過去的歷史紀錄比對後發現異常突增，即時發送訊息給學校的網路管理者，並顯示出攻擊來源 IP、國別以及查詢次數等資訊，管理人員確認無誤可以下達阻擋指令到 HP TippingPoint IPS 上將所有攻擊來源 IP 封阻在 Internet 入口處，DNS 效能回復正常，校內師生上網瀏覽也回復正常。整個過程從發生攻擊那刻起到確定攻擊手法與來源 IP 群，下達阻擋指令恢復網路運作僅耗時不到 10 分鐘。

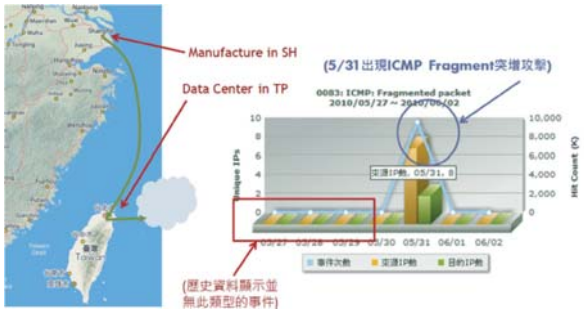
組織可能會面臨到不同嚴重程度、不同型態的 DDoS 攻擊，使用 HP 解決方案將可以有效抵擋 DDoS，確保網路運作與系統服務的平順。



內網端點防護的需求

組織內網電腦管理一向是 IT 人員的頭疼工作，有太多行動電腦可以進出組織、USB 行動碟管控不易、無線網路與 3G 服務的普及等因素讓組織內網電腦常常曝露在遭受入侵或是感染惡意程式的風險之中。許多 IT 人員會考慮使用 NAC 來加強管控，這個作法對於身分識別與連網設備的管控雖有其優勢，但是 IT 人員卻必須面對相當複雜的建置過程、人員教育、政策制定以及不斷的調整，工作負擔不減反增的情況比比皆是，而更嚴重的問題是：如果電腦遭植入惡意程式而操作這部電腦的使用者又通過了 NAC 認證取得網路存取權限，後續發送的惡意行為對 NAC 系統來說是非常難以察覺的。

那麼有沒有更好的方式來檢查與管理內網的惡意行為呢？在這裡同樣用一個實際案例來說明 HP Networking 端點防護整合方案的好處：這個事件發生在一個跨國企業的網路環境中，某日發生該企業位於海外的製造廠無法連回台灣總部的 ERP 與相關系統，檢視兩地之間 VPN 線路的 MRTG 流量監控圖發現頻寬已經塞滿用罄，這是過去少有的異常情況，卻在那段時間裡間歇性的出現，影響到產線的運作。從 HP TippingPoint IPS 的事件報表上我們發現巨量 ICMP Fragmented Packets＜大型的 ICMP 封包在網路傳遞時因為超過 MTU 限制所以需要切割＞來自於海外廠內的數十部電腦，同一時間對國外的少數幾個目標發動癱瘓攻擊，因流經 VPN 線路而導致頻寬消耗殆盡的窘況。而這樣的行為在過去並未曾出現於該廠區。透過行為分析系統，我們可以看見異常突增事件出現如下圖所示。



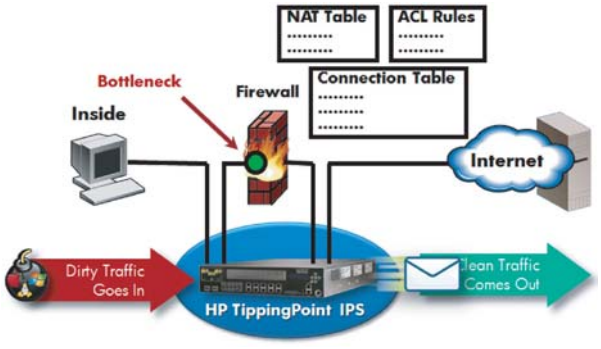
進階查詢出哪些內網的 IP 疑似遭駭客植入控制程式後，接收攻擊指令同時對外發動大量 ICMP Fragmented Packets，意圖癱瘓網路。

這次事件的處置作為分成兩個階段：首先，在 HP TippingPoint IPS 上將 ICMP Fragmented Packets 行為從監控模式改成攔阻，在這些封包進入到 VPN 線路前先行濾掉，避免頻寬資源遭佔據；如有必要，下個動作可針對這些發動攻擊的內部電腦進行端點阻擋，透過報表系統下達 IP Base 的阻擋條件到 HPN L2 Switch 上。

大量連線穿越造成防火牆導致效能不足的解決方式

過去十年防火牆設備普遍建置於組織的網路架構中擔任守門員的工作。但是當越來越多元的網路行為流經防火牆設備，尤其是現今許多網路應用服務，諸如 P2P、Skype 等會建立大量的連線數，IT 管理人員常會發現防火牆的效能似乎日漸不堪負荷。是否該置換更大型的防火牆來擴充效能？更換之後巨量連線數的問題就可迎刃而解？或是這樣的擴容永遠趕不上網路服務的發展速度？就技術理論言之，防火牆必須建立 Connection Table 資訊作為執行 NAT 轉換以及阻擋或是放行動作的依據。網路中過多的連線數很容易就可以注滿整張 Table 而讓防火牆出現效能障礙。由於防火牆的佈建位置通常都是在網路架構的重要節點上，當防火牆遇到效能問題時，往往導致網路中斷的災害。就算大多數的時候 Connection Table 尚稱足夠因應平時的網路傳輸需求，然而倘若發生如本文前面幾節所描述的網路異常攻擊事件，這些爆增的連線與封包就會是壓垮防火牆效能的最後稻草，雖然當時駭客發動攻擊的目標並不是組織本身，卻因為防火牆成為網路架構中的瓶頸 (Bottleneck) 問題，變成間接的受害者。

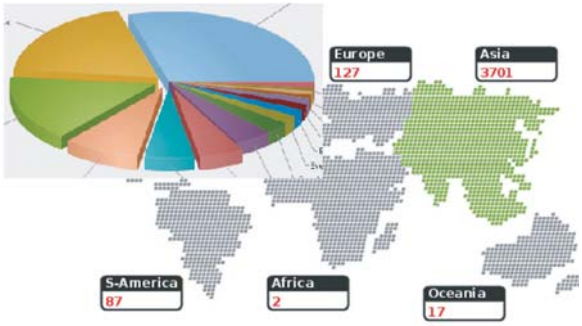
HP TippingPoint IPS 並不建立 Connection Table，所以不會成為網路的 Bottleneck。它的運作像是一部濾水器，將網路中的有害攻擊過濾後，僅放行乾淨無害的流量，不論這些攻擊是來自外網或是內網。我們建議組織將 HP TippingPoint IPS 用包夾防火牆的作法佈建於網路架構中，如下圖所示，如此就可為防火牆過濾掉許多不必要處理的惡意連線行為。此外，組織透過 HP TippingPoint IPS 執行人員上網行為控管，例如禁止 P2P 傳輸，亦可幫助防火牆省去不少 NAT 轉換的負擔。



因應新版個資法的 Syslog 儲存與中文報表需求

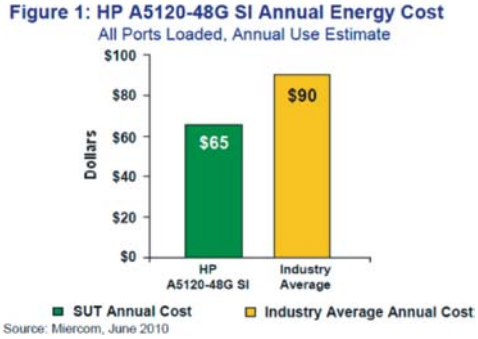
除了資安事件即時分析功能，我們在這次專案中所提供的中文報表系統亦具備多項優異功能：

- 自動偵測與接收多個來源的 Syslog Data，接收能力達 4,000/Sec
- 可輸入多筆查詢條件進行邏輯運算 (or 與 not)，條件內容包括事件關鍵字、IP、各項參數等，輸入條件數無限制
- 可儲存高達六億筆 Syslog Data
- 統計一千萬筆 Syslog Data 的 TOP 1000 報表僅需 48 秒
- 支援報表 Drill Down 查詢事件
- 動態呈現 3D/2D 多種圖型式樣
- 離線報表設定自動寄送功能
- 支援資料庫備份與回復功能
- 即時 Dashboard 呈現與全球 IP 的事件關聯性

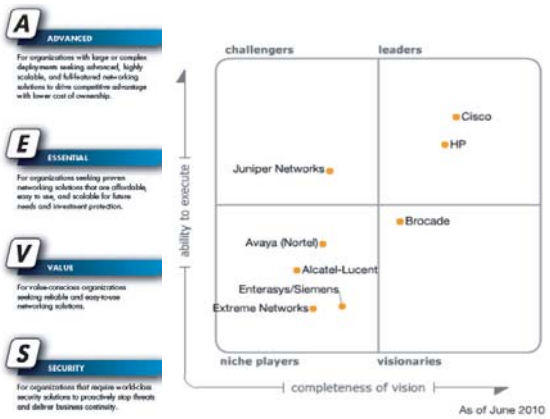


效能優越與節能環保兼具的網路設備

HP 在 "綠色" 的思維中，要讓網路更加 "GREEN"，因此一方面採用更環保的材料、更嚴格的檢測標準和設備、更精確和人性化的設計、更環保的製造工藝，以及更大力度的電子垃圾回收舉措，通過節能、減排和回收再利用提升產品的綠色屬性。另一方面，在綠色 IT 建設上，超越產品層面，將綠色理念提升到更高層次，簡化傳統網路基礎架構，初步實現網路資源的虛擬化，提高資源的利用率，從整體上降低 TCO 的同時，也讓設備、能源等資源的消耗更少。HP 網路設備都有通過 Miercom 綠能驗證，耗電量比業界平均還少，節省至少 20%。



Gartner 公司推出關於企業網路的魔術象限，它針對公司對於執行力與網路技術投資與遠景方面進行評估。魔術象限有四個象限組成，分別包括：領導者（Leaders），有遠見者（visionaries），挑戰者（challengers）和特定市場參與者（niche players）。而 Gartner 在 2010 年最新的魔術象限將 HP Networking 評比為領導者廠商與 Cisco Systems 一樣。在在證明 HP 網路的優異與創新性，為企業網路最佳品牌之一。此外融合伺服器與儲存設備達到融合式基礎架構 (Converge Infrastructure)，HP 網路則為業界 IT 考慮的唯一品牌。



HP 網路解決方案，包含 Advance、Essential、Valuable 以及 Security 四大產品系列，全方位提升網路的安全、管理、部署與延展，將永久性改變網路生態，為這個領域定義新法則。

HP 提供高安全性且易於部署的網路環境；提高效益與靈活度以及為客戶大幅降低網路成本。HP 網路服務是從網路邊緣至核心的完整服務方案組合，協助客戶建立一個整合、易於管理且安全的全新網路系統。而 HP「客戶導向」的網路改革進化方式，能為客戶建置輕鬆進階成長，高靈敏且適應性更高的網路環境。全新標準化網路架構，則為客戶節省成本同時增進創新的能力。

結論

現今許多網路運作異常；伺服器服務無法存取的問題都是起因於資安事件。我們可以這樣說：欲發揮 IT 系統的效益，就必須掌握並控制網路裡的每一個惡意行為，而優良且判斷準確的資安技術正是可以協助網路維運的關鍵角色。HP 網路部門這次所提的解決方案，由省能之星 HPN Switch 設備擔任基礎架構；全球最佳的入侵防禦系統 HP TippingPoint 負責資安工作；搭配方便易用的事件分析及中文報表系統，將可涵蓋組織的主要需求：效能優異的網路；異常事件的立即反映與處置；員工上網行為規範；資安防護與重要資料保護；準確而有效的端點管理；因應個資法的 Syslog 儲存備查要求；操作容易、報表清晰的中文介面操作系統；以及最重要的超高投資報酬率。

2011 年 2 月