



政府機構 – 台中縣政府案例

InstantScan-5000 + InstantQoS-5000 導入成效



L7 NETWORKS INC.

2008/6/22

政府機構 – 台中縣政府成功案例

IS-5000 + IQ-5000 導入成效

專案背景：

民國三十九年，本局借用當時豐原鎮中山堂作為臨時辦公廳，直至民國四十三年，始在現址興建二樓乙棟，兩側各平房乙棟使用，迄民國五十八年「戶警合一」及民國六十二年民防機構裁併本局，更無廳舍可容納，于民國六十三年增建，

由於時代進步，科技發展迅速，台中縣警局為加快並有效處理日益繁重之各項警政業務，資訊 e 化乃唯一提升效率之捷徑，不但可便已將業務資訊化，提升公文效率，更可便民讓資訊透明化以達到全民拼治安。

用戶面對的問題和挑戰：

問題一、機密外洩、上班聊天生產力低落、感染 IM 病毒

隨著網路開放，所面臨資訊安全問題也隨之而來，雖然警局制定資訊安全政策宣告，來規範內部同仁遵守，但壞人在外犯罪，會有人民保母警察同仁為我們維護社會秩序，但在自由的網路國度，也需一套完善網路資安設備來充當網路警察，抓出同仁不良上網行為。這些年縣警局常面臨部同仁工作效率低落，及內部網路常出現雍塞情況，但始終只以不斷加大對外網路頻寬來解決，當然問題依舊存在，甚至情況更嚴重。並且也發現局內同仁常使用外部信箱，如 Webmail：夾帶檔案，傳送個人信件出去，所以也就無法得知同仁傳送什麼樣的文件資料，就會有洩密資料的風險存在。並且這些年隨著即時通訊軟體使用

率普及，也造成局內資訊安全最大漏洞，許多同仁上班使用即時通訊軟體(MSN、Yahoo)，不斷聊天，造成工作效率低落，甚至藉由該通訊直接傳送檔案給對方，或者打開對方所傳送檔案，但目前即時通訊軟體有極大病毒風險威脅，所以常有同仁因打開即時通軟體來路不明檔案而感染病毒。上述情況不但嚴重違反局內所規定的資訊安全規範，更因即時通訊軟體中毒情況日與俱增，讓縣警局資訊室同仁為此困擾。所以台中縣警局公開找尋中信局相關設備：L7 Networks、國外知名大廠 Blue Coat 與 8e6 進行測試。

問題二、地道軟體放肆，穿過 BlueCoat 使用非法軟體

由於已經安裝了 BlueCoat 以過濾經過 http 的流量，但是發現 BlueCoat 除了無法過濾華文市場的應用外，連一些全世界都常用的地道軟體，例如 TOR、SoftEther 等等，都無法過濾。2005 年以 BS-7799 稽核為基礎的風潮，正盛大地在企業、政府推行中。

問題三、P2P 惡性侵佔網路資源，網路頻寬日趨緊張

在台中縣警局的網路中，雖然有 BlueCoat 過濾 BT、E-Donkey、KaZaA 等各類 P2P 應用，但仍無法真正過濾完所有的 P2P，例如迅雷就完全沒辦法控管。因此 P2P 佔用了大量網路頻寬，高峰時期，P2P 應用甚至佔據整個網路流量的 78% 以上，極大地影響了台中縣警局正常業務的開展及使用者正常網路應用的服務品質。同時這也導致公司網路經常處於超負荷運轉狀態。在缺乏控制和有效管理的過程中，寶貴的頻寬資源被惡意的、非關鍵應用所佔用，而大部分用戶的合法應用則使用小部分的頻寬資源，這是台中縣警局面臨的主要問題和挑戰。

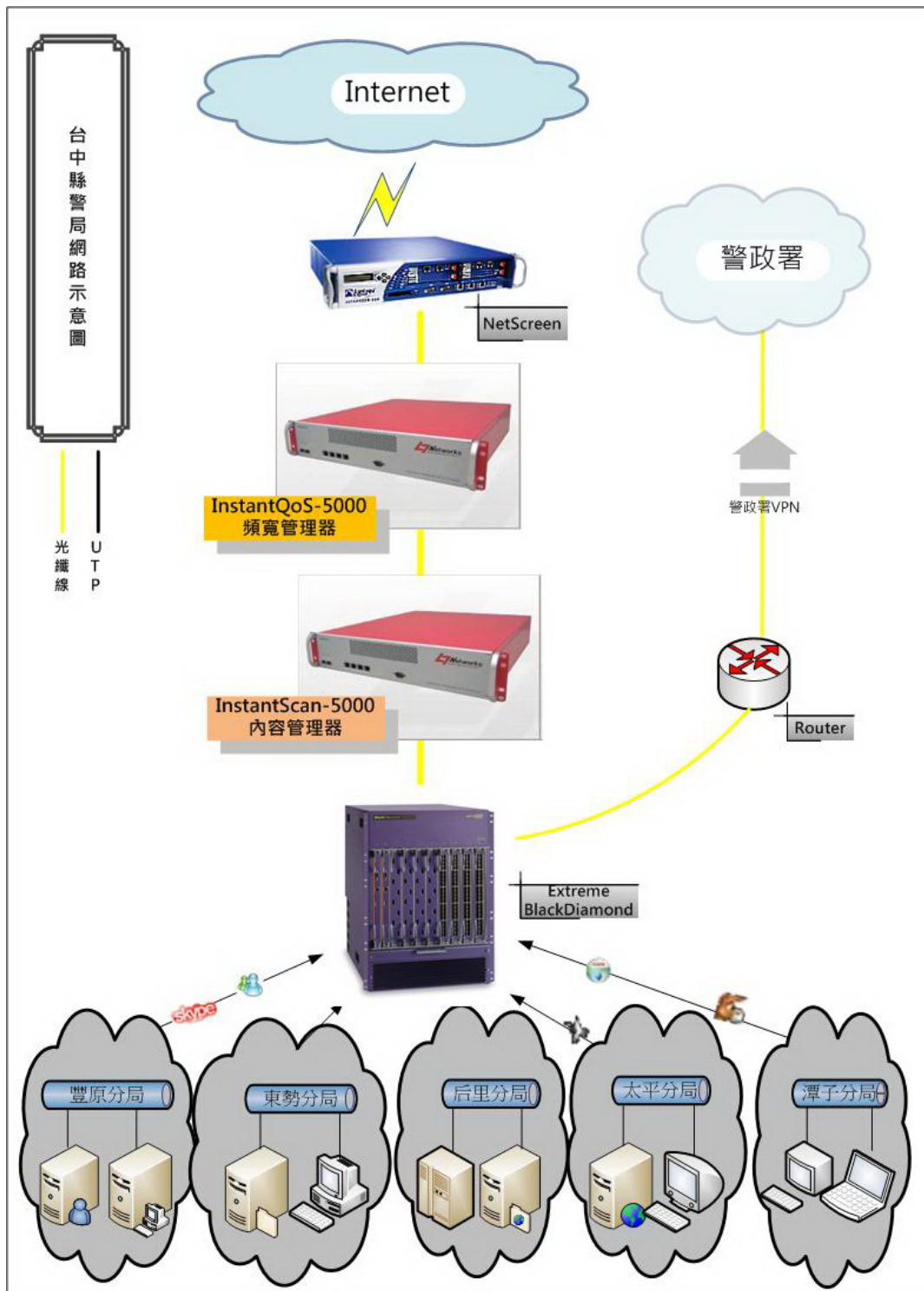
解決方案：

L7 Networks 推薦給客戶的解決方案是採用 InstantScan 與 InstantQoS 2 大產品系列，完整解決方案來應對客戶現今所面臨的網路問題。

台中縣警局資訊室沈先生說：「有時發現局內同仁使用不當 P2P 軟體大量下載，但因目前 P2P 軟體，並非一般網路行為模式，很難對其做限制，所以 L7 Networks 推薦 InstantQoS 來解決網路頻寬雍塞問題，因支援最多 P2P 種類通訊協定，可把 P2P 軟體全部限制阻擋下載，還可有效分配局內每位同仁頻寬使用量與連線數，不讓用量大戶的下載來影響其他同仁辦公效率；還可針對局內對外提供服務的主機，或某些特殊通訊協定，做頻寬使用的保證，如此一來就達到網路流量資源有效分配。」

沈先生形容 L7 的即時流量監控功能，有如「路口監視器，每分每秒監控網路狀態，可由應用(Protocol)找出是誰正在使用此流量，或者由人(IP)找出誰正在使用此應用(Protocol)，再搭配報表流量統計分析，很快就能抓出大量下載同仁，並立即做出警告。」這些事以前要好幾個工作天才能完成，現在只要幾分鐘，就可以整理出他要的報表讓他減輕了不少工作。

L7 Networks 所推薦的 InstantScan + InstantQoS Total Solution 不但可做到深層管理、細部分析，並且有效控制頻寬使用；搭配詳細豐富報表抓出內賊，打敗了國外知名大廠 Blue Coat 與 8e6 強勁對手。整體上來說不單讓資訊室同仁為之頭痛的頻寬不足問題，現今終得以解決。縣警局希望藉由 L7 Networks 監控與側錄，嚴密把關，不讓人員利用上班時間使用非法途徑，將機密文件或檔案傳送出去，做到內網防範，並藉由 L7 Networks 產品所提供豐富報表功能，抓出網路內賊。並且每周公布報表，對於違反資訊安全同仁，與頻寬使用大戶，人人自危，也因此提升工作效率，縣警局希望在每位同仁努力下在資訊安全工作，建立「資訊安全，人人有責」的觀念，制定嚴明規範，進行適當的資訊安全訓練，以提高資訊安全意識。



圖一、在台中縣警局的網路中，控管嚴密，每個機櫃都鎖緊不能打開，三台 L7 的 InstantScan-5000 在其中過濾應用與監控行為，

將 L7 Networks InstantScan 應用優化設備部署在台中縣警局的網路出口，可以為台中縣警局資訊化網路實現如下功能和效果：

方案二、限制非關鍵應用，並優化網路流量

限制沒有經過管理部門允許的通過公司網路的上網行為，如 P2P 下載、聊天、網路遊戲等嚴重影響警察正常的各類網路應用。L7 的設備自動偵測台中縣警局網路中異常的流量，使得網管人員可以詳細瞭解公司網路中運行著哪些應用和流量。它以資料化 和圖形化直觀的瞭解網路應用程式運行的性能，網路負載以及網路頻寬使用情況，提供多樣化的查詢方式。

內網 IP	數量	端口	外網 IP	端口	協議	字節		封包	
						下載	上傳		
Chat	502					11.76 G	4.62 G	6,398,890,8...	7,988
allwangwang	3					38.21 M	80.19 M	137,994,752	140
feison	13					276.63 K	75.11 K	368,384	
msn	9					97.04 K	34.91 K	104,192	
qq	390					248.39 K	379.03 K	354,816	
qqchatroom	2					22.68 M	55.14 M	108,436,736	106
qqmedia	18					1.29 M	75.96 K	1,239,808	1
qqsharc	19					12.67 M	30.82 M	22,555,136	27
webbirr	6					323.79 K	1.42 M	332,288	
xmpp	40					1.64 K	138 B	47,616	
yahoo	1					657.81 K	253.24 K	4,556,054	4
Email	4					0 B	35 B	256	
imap	1					15.72 K	2.04 K	14,336	
sntp	3					5.28 K	1.2 K	1,792	
File Transfer	75					10.44 K	863 B	12,544	
Game	10					168.21 M	4.14 K	33,281,792	19
P2P	23758					15.18 M	1.42 M	60,097,792	54
bittorrent	7594					8.12 G	2.64 G	4,814,124.8	6,455
edonkey	1604					2.5 G	291.74 M	1,165,453.8	1,352
fasttrack	1					2.63 G	39.85 M	1,258,206.8	1,448
fs2you	7					8.77 K	3.14 K	62,464	
gnutella	19					93.4 M	16.54 M	20,000,216	13
kugoo	38					224.06 K	222.98 K	2,016,256	2
maze	2					217.26 K	190.86 K	2,576,896	2
poco	898					5.04 K	5.07 K	48,384	
vagaa	19					22.92 M	6.57 M	18,074,112	118
xunlei	13578					26.85 M	14.49 M	10,541,824	8
Stocks	209					2.85 G	2.28 G	2,337,134.8	3,509
Streaming	2646					179.39 M	17.31 M	109,288,960	170
funshion	6					1.75 G	1.05 G	773,222,400	763
qob	275					280.38 M	400.71 K	56,605,952	23
rtsp	2361					130.16 M	210.75 M	85,257,728	85
shoutcast	2					1.35 G	863.42 M	830,645,760	853

方案三、導入個人計量配額，懲罰超量使用者，激起網路公德心

方案三、與既有 AD Server 結合，管理每位員工上網行為

而在內容控管方面 L7 Networks 推薦 InstantScan 與局內 AD Server 結合，採用個人化深層管理每位同仁上網行為，深度管理每位同仁瀏覽網頁權限，禁止同仁到 Webmail 網頁收發信件，並且紀錄每位同仁所瀏覽的網址。細部控管每位同仁即時通訊軟體權限，禁止透過即時通訊軟體傳送檔案，並做檔案掃毒，以防止即時通訊蠕蟲病毒危害。

用戶獲得的投資收益：

部署了 L7 Networks InstantScan 應用內容交換器設備對台中縣警局的網路進行規範化管理後，節省了大量寶貴的網路頻寬資源。L7 Networks InstantScan 應用內容交換器設備運行穩定可靠，性能表現相當出色。能夠為台中縣警局用戶帶來如下的收益：實現台中縣警局資訊出口的網路應用與網路流量的視覺化；保障 台中縣警局到 Internet 的暢通無阻；提高了台中縣警局的頻寬使用效率，降低 IT 投資成本；降低台中縣警局資訊中心的網路運維管理成本；提高整個台中縣警局網路運行的可見性、可測性、可控性和可優化性。