

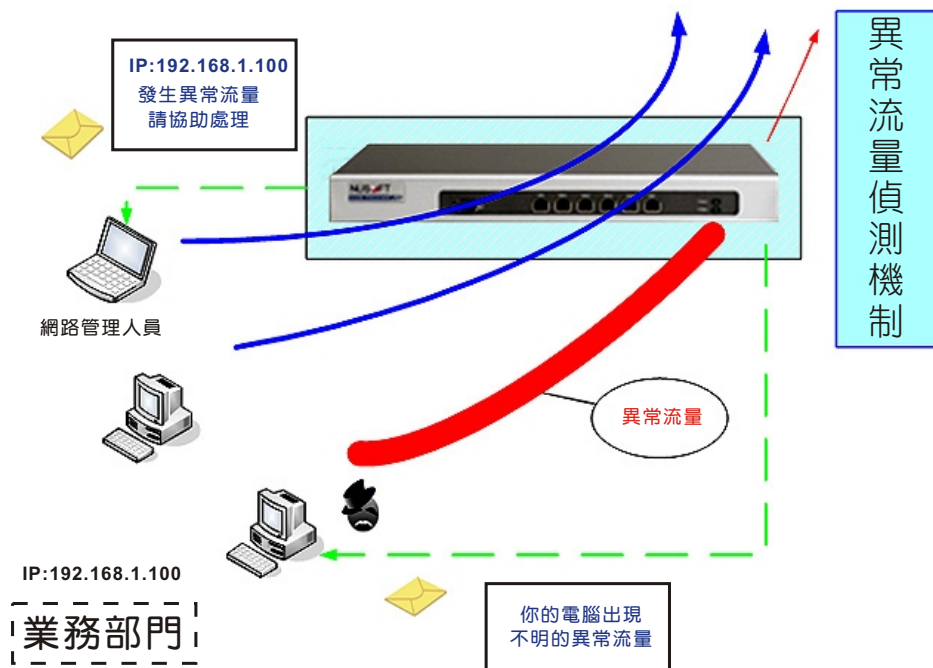
## 多功能 UTM、負載平衡器 / MS、MH 系列報導

### 技術淺談與應用 - 異常流量IP

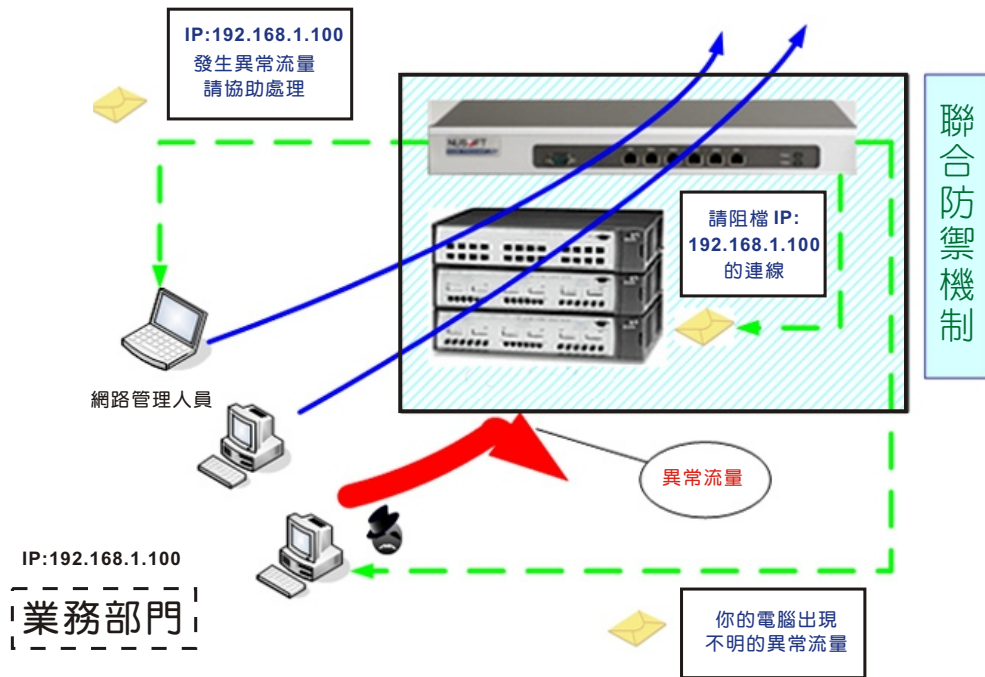
◎內部異常流量偵測與建置聯合防禦網路機制

新軟公司另一獨創鉅作 — 『內部異常流量偵測與聯合防禦機制』，拒絕網路癱瘓與杜絕病毒擴散的唯一選擇。

長期以來，企業的安全防護措施，大致都有著「防外有餘、防內不足」的弊病，解決方案不外乎是防火牆、UTM、閘道防毒、IDS 等閘道防護，雖然在防範來自外部的各類威脅攻擊時，皆有相當程度的防禦能力，但面對企業內部網路的惡意攻擊，因而產生的大流量或高連線數時卻往往無法有效杜絕，造成企業網路頻寬阻塞。而在惡意程式擴散蔓延方面，以往的管理人員總是在眾多電腦中，花上好幾天的時間一台一台找一台一台掃，增加了尋找中毒電腦的時間，因而導致整個網路癱瘓影響企業資訊安全。



於是，新軟公司為強化即時異常流量偵測，以提升區域內網的安全性。推出的各項產品中皆擁有獨創的【異常流量 IP】偵測機制，如上圖所示，透過管理人員的設定，主動察覺企業內部每位使用者的使用流量，不僅可針對較高流量之主機或主機群設定【不偵測 IP】來符合網路需求，更可以針對各企業網路環境需求制訂異常流量臨界值，來達到中毒電腦對外連線有效管制及零誤判的企業需求。



此外，一般的偵測機制著重於偵測並未能達成即時阻斷的效果。新軟公司研發團隊憑藉多年對市場需求的研究與瞭解，不僅在各產品均擁有優異的零誤判異常流量偵測機制，更開發出一般市售產品所欠缺的聯合防禦機制。如上圖範例所示，當業務部門 IP: 192.168.1.100 的電腦中毒時，導致區域內網中產生大量且不明的對外連線，系列產品將於第一時間內主動偵測出異常流量（中毒電腦）並將相關資訊記錄於設備中，且立即通知事先指定的交換器（Core Switch），共同組成聯合防禦連線，即時阻斷發生問題的使用者，以最快速的時間達到即時阻絕的效果確保網路安全。在發生異常流量的同時，系列產品均能在第一時間內根據管理人員所設定的警訊通知形式發出警訊（如：E-Mail、SNMP Trap、NetBIOS），通知該使用者及管理人員協助處理，使資安事件的發生達到即時且有效的控管，以避免異常流量對於企業網路造成危害。

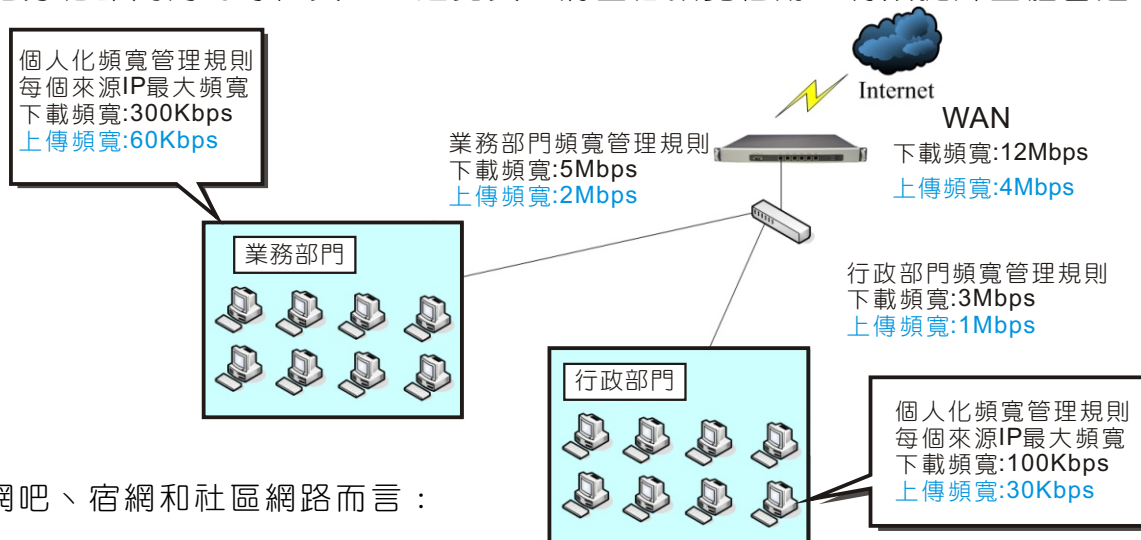
文  賴鴻文 tony@nusoft.com.tw

## 市場行銷報導 - 如何有效管理有限的頻寬？

A.以公司單位來說：

一般企業都設有許多部門，掌管著整體的運作，在企業 e 化後，業務的往來幾乎由網路來傳遞。但往往會發生頻寬不敷使用的問題，導致訊息傳遞窒礙和使用者怨聲載道。最後，都只能以提升對外頻寬這種治標不治本的做法，來暫時性解決問題。原因就出在頻寬的分配上過於籠統，又無法有效阻絕頻寬的濫用。

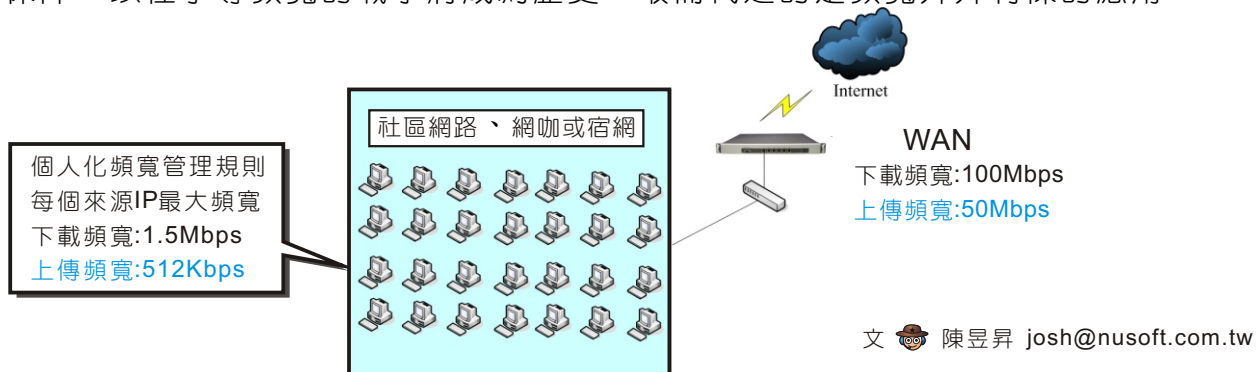
有鑒於此，新軟系統將頻寬管理擴及到各個層面，利用原有的 QoS 功能，讓企業可以依照各部門的特性，規畫頻寬使用的原則，使彼此間在對外傳遞資料時，不會相互影響和衝突。同時，獨創的個人化頻寬管理(Personal QoS)，可將 QoS 所保留的頻寬，再細分給部門內的每位員工，避免員工將整個頻寬佔用。有效提升整體營運的效率。



B.針對網吧、宿網和社區網路而言：

在一個共用網路的環境中，常常上演網路資源的攻防戰，只要有人打破正常使用原則，往往搞的人仰馬翻。不僅是網管人員焦頭爛額，使用者也會瀰漫在一股攻訐的氣氛當中。在顧客至上的原則下，既無法完全阻絕用戶的異常需求，又要承擔來自於各方的壓力。

基於公平原則，新軟系統針對個人使用網路的特性，獨具匠心的個人化頻寬管理(Personal QoS)設計，不再只是異常行為的偵測與防堵。而是，制定可供各種正常需求運作的通則，不再需要針對每個用戶設定 QoS，讓每位使用者在網路頻寬的使用上都有保障。以往爭奪頻寬的戰事將成為歷史，取而代之的是頻寬井井有條的應用。



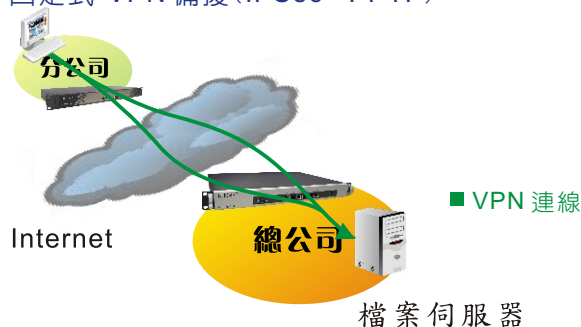
文 陳昱昇 josh@nusoft.com.tw

## 市場行銷報導 - 如何從遠端存取企業內檔案？

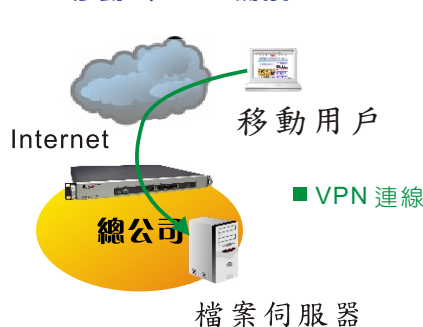
一般企業需要從遠端來存取檔案時，都會以安全性為第一考量。而在以往，通常是企業專線來達到安全傳輸檔案的目的。這種傳輸方式安全性高，但價格昂貴。目前，較為大眾所能接受的方式是採用 VPN 連線。而 VPN 連線分為兩大類：固定式 VPN，還有移動式 VPN。

固定式的 VPN 就是已經使用多年的 IPSec 與 PPTP。這兩種 VPN 大多是用在兩個子網路之間的傳輸，像是總公司與分公司。在過去，這兩種 VPN 都是連線後就無法有效控管兩個子網路之間的傳輸。這樣的傳輸方式對企業網路安全性，也是一大隱憂。現在，新軟系統特地将“管制條例”的概念，導入了 IPSec 與 PPTP 中。管理員可以利用“管制條例”輕鬆達到控管（甚麼人、甚麼時候、去哪裡、使用何種服務…）兩個子網路之間的傳輸。甚至可以做到利用病毒過濾、入侵防禦偵測等方式達到超高安全性的檔案傳輸。至於在固定式 VPN 的線路連接方面，新軟系統獨創的 VPN 負載平衡功能，可做到多條 VPN 線路頻寬的合併、VPN 斷線備援…，讓 VPN 的連線永無後顧之憂。

固定式 VPN 備援 (IPSec、PPTP)



移動式 VPN 備援 (SSL VPN)



移動式 VPN 就是近幾年來才崛起的 SSL VPN。大多是移動用戶、在外奔波的業務、出國洽公之人員所使用。不管使用者在哪裡，網咖、客戶公司、甚至在家裡。只要有網路，透過電腦的瀏覽器，短短 20 秒就能完成 SSL VPN 的連線。

也許有人會說：在外面使用 VPN，用 PPTP 就好了。簡單方便，何必再學一種新的 VPN。實際上，PPTP 的安全性在所有 VPN 中是最差的。況且使用者所在網路的閘道器若不支援 PPTP Pass Through (PPTP 透通)，使用者將無法成功建立 PPTP VPN。相較起來，SSL VPN 的資料加密能力比 PPTP 高出許多，且不會受限於網路環境，使用上安全且方便。

多功能 UTM 內建 VPN 比較

	固定式 VPN		移動式 VPN
	IPSec VPN	PPTP VPN	SSL VPN
安全性	高	中	高
架設難度	難	難	容易
VPN 負載平衡	○	○	×
Policy 管控	○	○	×
適用環境	總公司與分公司	總公司與分公司	移動使用者

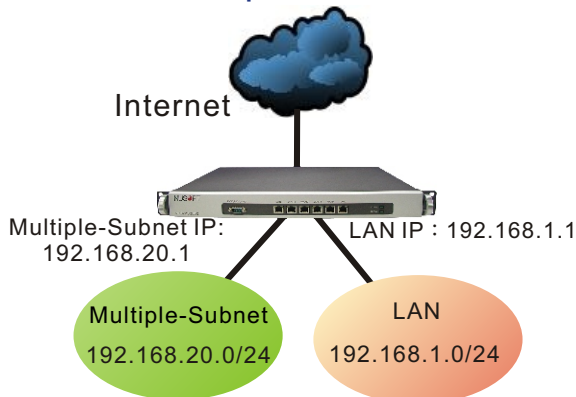
文 程智偉 rayearth@nusoft.com.tw

## 市場行銷報導 - 如何管理企業內不同子網路？

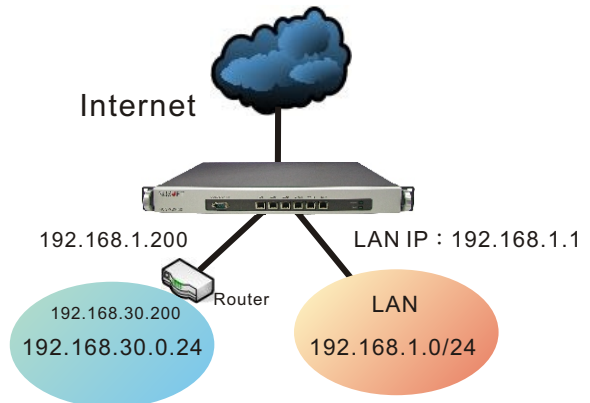
企業網路在規劃時，往往為了管理方便，會把整個企業網路劃分為多個不同子網路，並將這些子網路分配給各大部門所使用。在過去，建構這種企業網路架構的方法，就是在每個子網路前架設路由器。藉由路由器能夠溝通不同子網路的特性來建構多子網路的企業網路環境。這種企業網路的建構方式，不只架設經費提高了，在網路維護方面也會變為複雜，增加管理上的困難度。事實上這個問題，可以利用新軟多功能 UTM 內建的 Multiple-Subnet 功能輕鬆解決。

Multiple-Subnet 這功能適用在”企業有多個部門，而這些部門需要區分為不同的子網路”之網路環境。管理員只需要幾個簡單的設定，指定這些子網路在連線至外部網路時，需透過 Multiple-Subnet 機制所設定的網路介面，就可輕鬆完成設定。此後，位於這些子網路的用戶就可直接透過多功能 UTM 上網，並完全能受到多功能 UTM 的管控。

Multiple-Subnet




指定路由表



假如企業網路環境必須使用路由器來連接不同的子網路時，多功能 UTM 也能利用內建的指定路由表功能達到建構多子網路環境之目的。指定路由表的功能就是在告訴多功能 UTM，如果收到需要傳送至特定子網路的封包時，要往哪個路由器傳送。

Multiple-Subnet 與指定路由表，這兩的功能的使用環境其實是很相近的。都是企業網路中有多個不同的子網路。兩者之間的差異就只有”指定路由表使用於有路由器環境”，而”Multiple-Subnet 則不需使用”。只需要弄清楚這一點，在建構多子網路的企業網路，就不會有選擇錯誤的問題發生。

文  程智偉 rayearth@nusoft.com.tw