新軟週報
http://www.nusoft.com.tw
Internet Security Fighter
2011/12/1-2011/12/15 第133期

UTM / UTM系列報導

新軟UTM新增『FQDN』功能，讓網站管制更靈活應用

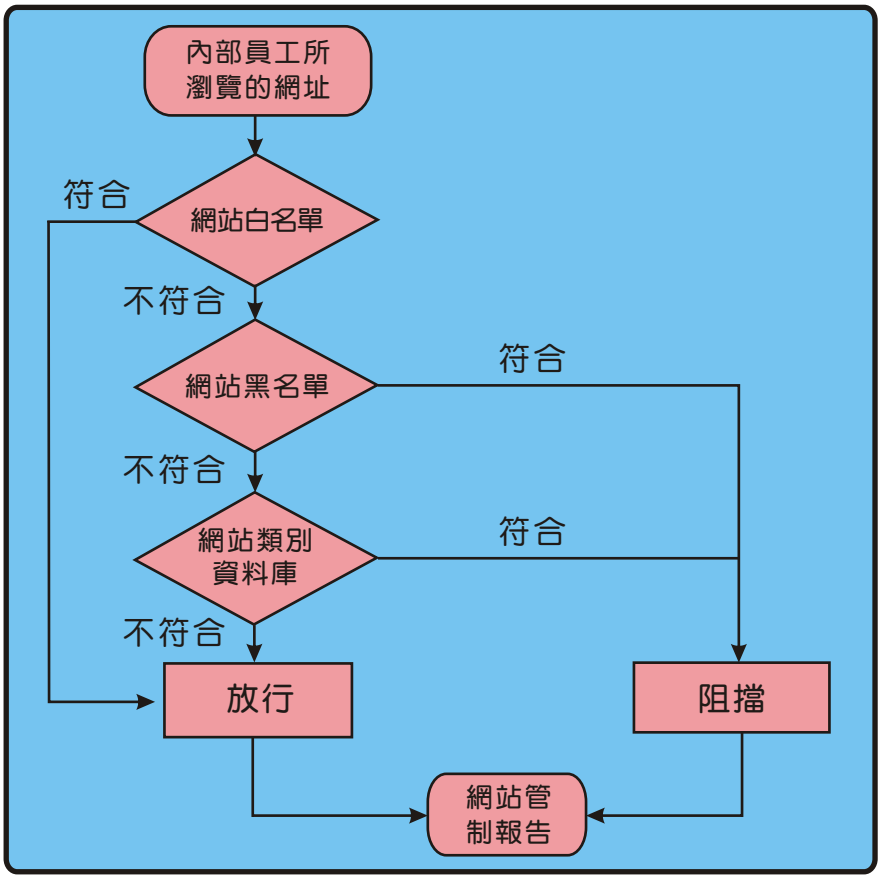
藉由網際網路的建立，使得電腦之間能相互傳遞訊息，彼此分享檔案資源、硬體設備等。所以網際網路的發展，無疑擴大了電腦的能力，也使得人們的知識領域更加寬廣、商業活動更加頻繁；但相對一些使用網路的弊病、陋習也逐漸浮現(如：上班時間在公司盯股票、逛部落格、facebook、線上影音…等等)，不但占據公司大量的網路頻寬，同時也造成電腦容易遭病毒入侵，而嚴重影響了員工工作效率、及公司正常營運。

為了能協助企業、公司有效控管網路資源存取，提高公司產能，新軟『UTM』系列產品提供『網站管制』機制。管理人員可設定欲開放或限制的網站，讓公司內部員工無法濫用網路資源進而達到有效管制。「網站管制」內容分為「網站白名單」、「網站黑名單」、「網站類別資料庫」、「檔案傳輸管制」、「MIME/Script管制」五種；利用此管制功能，不但能降低中毒的機率，同時控管內部員工上班時利用網路來打混摸魚的情況！同時亦提供詳細的「網站管制報告」，將其網站管制記錄做成統計報表與日誌，以協助管理人員後續的監控管理與資料存查。

新軟UTM『網站管制』機制	功能用途
網站白名單(Whitelist)	可透過“關鍵字”、“完整網域名稱”或“萬用字元(*)”設定開放存取的特定網址。
網站黑名單(Blacklist)	可透過“關鍵字”、“完整網域名稱”或“萬用字元(*)”設定限制存取的特定網址。
網站類別資料庫(Category)	勾選欲阻擋的網站類別，即可管制員工連線相關的網站。(此為付費功能，內含65種網站分類：惡意網站、社交網站、情色網站…等等)。
檔案傳輸管制(File Extensions)	可針對透過HTTP或FTP下載、上傳特定副檔名之檔案做管制。
MIME/Script管制	管制網頁Script程式(包含Pop-up Window、ActiveX Control、Java Applet、Browser Cookie)的存取權限，及網頁傳送的MIME資料型態。
網站管制群組	可群組所設定的「網站白名單」、「網站黑名單」、「網站類別資料庫」、「檔案傳輸管制」或「MIME/Script管制」項目，制定網站管制規則。
網站管制報告	將網站管制記錄做成統計報表與日誌，以便瞭解使用者存取外部網路資源的狀況。

表一 網站管制機制之各功能的用途

此外，『網站管制』機制特別需注意的是網址存取規則比對順序：「白名單」>「黑名單」>「網站類別資料庫」只要網站網址符合某一比對條件，本功能將不會再繼續向下比對！



圖一　網站管制網址比對流程

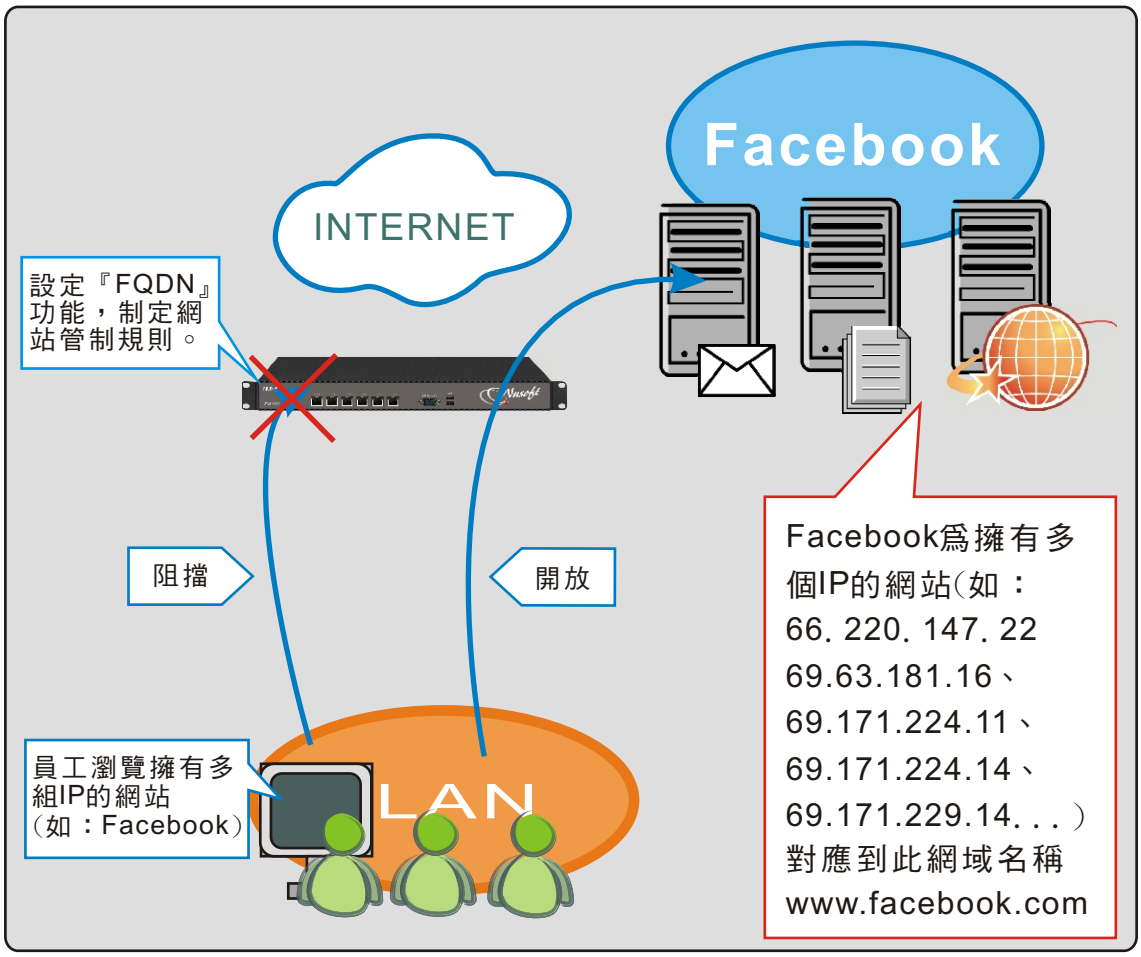
雖然說利用『網站管制』功能可以阻擋林林總總的網站，但對於員工以HTTPS連線網站(如：Yahoo、Google、Facebook...)，則無法管制。因此，新軟『UTM』系列產品新增『FQDN』功能，來解決這種窘境。何謂『FQDN』？其運作方式又為何？以下將一一說明。

何謂『FQDN』(Fully Qualified Domain Name，完整網域名稱)？

『FQDN』是由「主機名稱」+「網域名稱(包含最上層網域)」所組成的URL。從『FQDN』中包含的資訊可以看出主機在「網域名稱」樹狀結構中的位置。例如，www. symentev. com就是一個『FQDN』，其中www是主機、symentev是次級網域，而com則是最上層網域。此功能可運用在『網站管制』黑/白名單及網站類別資料庫功能鞭長莫及的地方(僅可管制HTTP)，如：HTTPS、FTP。

如何運用「FQDN」機制，方能達到企業最大利益？舉下列情況為說明：

透過HTTPS瀏覽擁有多個IP的網站(如：Facebook、Google...)時，「網站黑名單」、「網站類別資料庫」就無法阻擋。若以IP、網段方式管制連至上述網站，又很容易會有所遺漏。

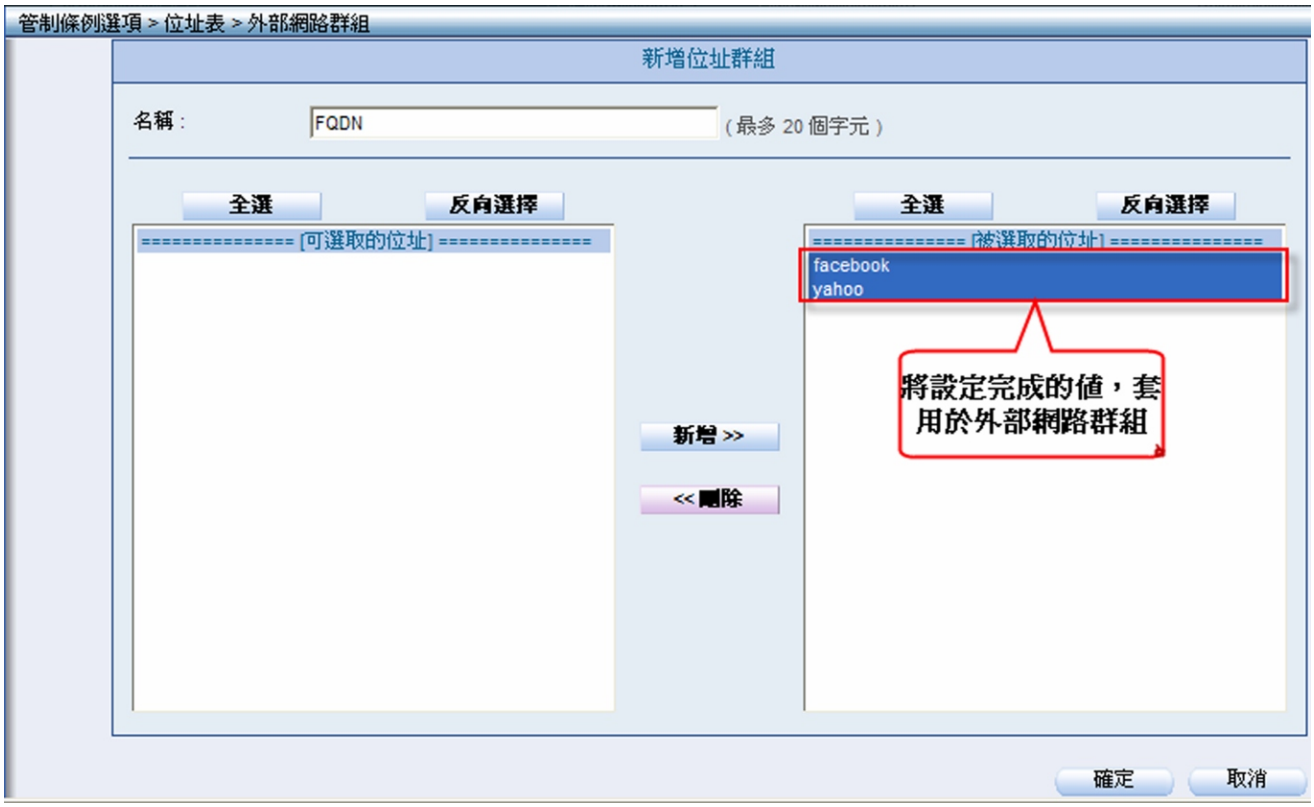


圖二 『FQDN』的運作方式

為了因應此種狀況，新軟UTM讓管理人員在外部網路位址表之『FQDN』設定方式－於欄位中填入目標網站的「主機名稱+網域名稱」，若網址為「http://www.facebook.com/#!/profile.php?id=105520583884516」的網站，則於『FQDN』欄位中填入「www.facebook.com」即可。

圖三 外部網路位址表填入目標網站的『FQDN』

若要阻擋二個以上擁有多個IP的網站，管理人員於『外部網路』位址表做相關設定後，再套用於「外部網路群組」位址表中。



圖四 外部網路『FQDN』群組位址表

上述所設定完成的值，最後於管制條例中套用，即可封鎖擁有多組IP的網站，且彌補了『網站管制』機制不足之地方。

圖五　將設定值套用於管制條例中

文 余光明 kongmeng@nusoft.com.tw