Nusoft 新软周报
http://www.nusoft.com.tw
Internet Security Fighter
2011/12/1-2011/12/15 第133期

UTM / UTM系列报导

新软UTM新增『FQDN』功能，让网站管制更灵活应用

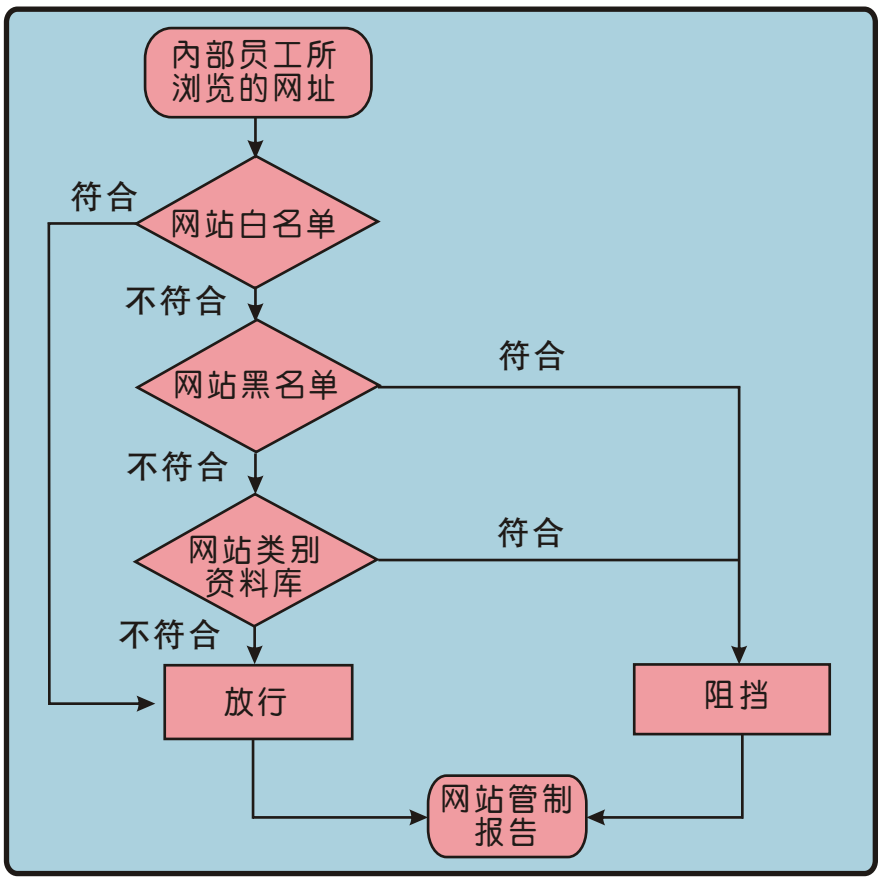
藉由互联网的建立，使得计算机之间能相互传递讯息，彼此分享档案资源、硬设备等。所以互联网的发展，无疑扩大了计算机的能力，也使得人们的知知识域更加宽广、商业活动更加频繁；但相对一些使用网络的弊病、陋习也逐渐浮现(如：上班时间在公司盯股票、逛微博、facebook、在线影音…等等)，不但占据公司大量的网络带宽，同时也造成计算机容易遭病毒入侵，而严重影响了员工工作效率、及公司正常营运。

为了能协助企业、公司有效控管网络资源存取，提高公司产能，新软『UTM』系列产品提供『网站管制』机制。管理人员可设定欲开放或限制的网站，让公司内部员工无法滥用网络资源进而达到有效管制。「网站管制」内容分为「网站白名单」、「网站黑名单」、「网站类别数据库」、「档案传输管制」、「MIME/Script管制」五种；利用此管制功能，不但能降低中毒的机率，同时控管内部员工上班时利用网络来打混摸鱼的情况！同时亦提供详细的「网站管制报告」，将其网站管制记錄做成统计报表与日志，以协助管理人员后续的监控管理与数据存查。

新软UTM『网站管制』机制	功 能 用 途
网站白名单(Whitelist)	可透过“关键词”、“完全网域名称”或“万用字符(*)”设定开放存取的特定网址。
网站黑名单(Blacklist)	可透过“关键词”、“完全网域名称”或“万用字符(*)”设定限制存取的特定网址。
网站类别数据库(Category)	勾选欲阻挡的网站类别，即可管制员工联机相关的网站。(此为付费功能，内含65种网站分类：恶意网站、社交网站、情色网站...等等)。
档案传输管制(File Extensions)	可针对透过HTTP或FTP下载、上传特定扩展名之档案做管制。
MIME/Script管制	管制网页Script程序(包含Pop-up Window、ActiveX Control、Java Applet、Browser Cookie)的存取权限，及网页传送的MIME数据型态。
网站管制群组	可群组所设定的「网站白名单」、「网站黑名单」、「网站类别数据库」、「档案传输管制」或「MIME/Script管制」项目，制定网站管制规则。
网站管制报告	将网站管制记录做成统计报表与日志，以便了解使用者存取外部网络资源的状况

表一　网站管制机制之各功能的用途

此外，『网站管制』机制特别需注意的是网址存取规则比对顺序：「白名单」>「黑名单」>「网站类别数据库」只要网站网址符合某一比对条件，本功能将不会再继续向下比对！



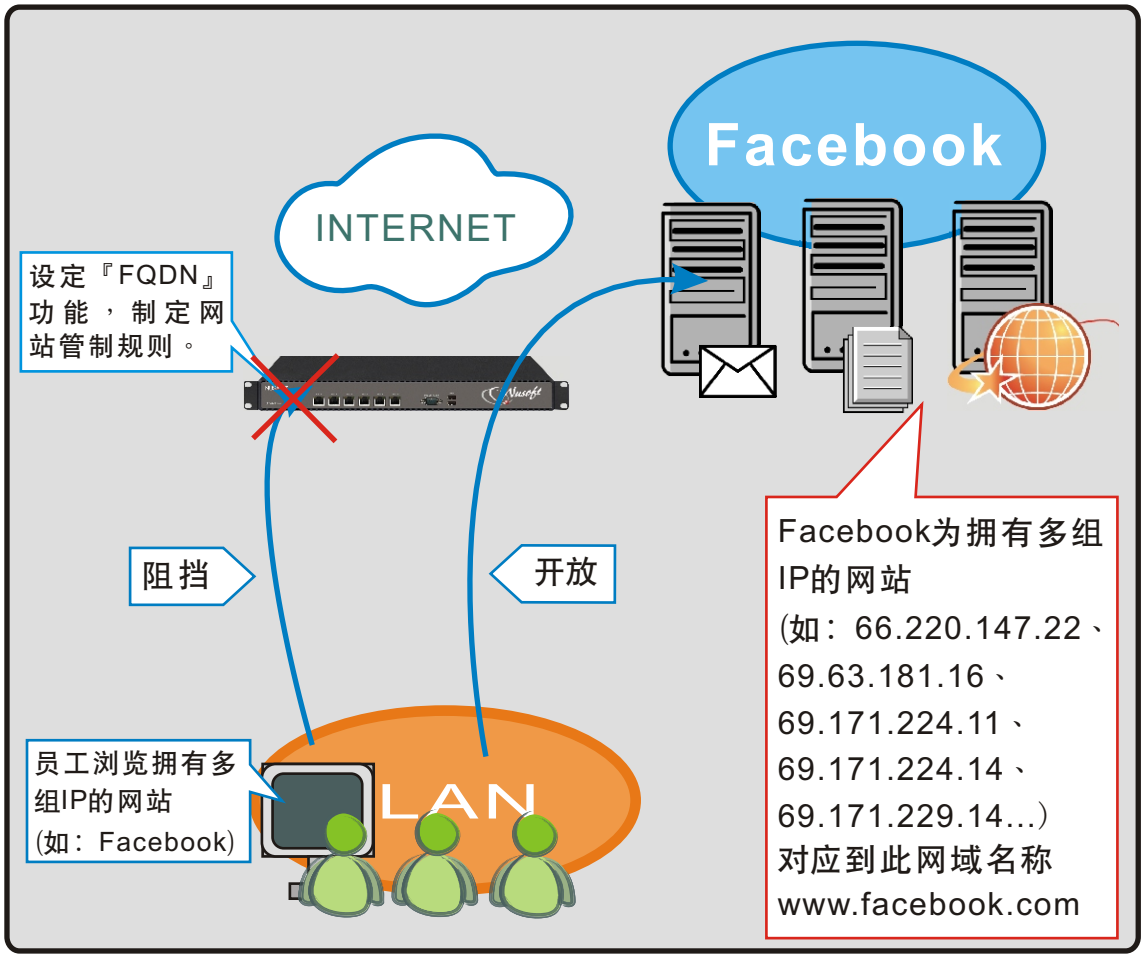
图一 网站管制网址比对流程

虽然说利用『网站管制』功能可以阻挡林林总总的网站，但对于员工以HTTPS联机网站(如：Yahoo、Google、Facebook...)，则无法管制。因此，新软『UTM』系列产品新增『FQDN』功能，来解决这种窘境。何谓『FQDN』？其运作方式又为何？以下将一一说明。

何谓『FQDN』(Fully Qualified Domain Name，完全合格域名/全称域名)?

『FQDN』是由「主机名称」+「网域名称(包含最上层网域)」所组成的URL。从『FQDN』中包含的信息可以看出主机在「网域名称」树状结构中的位置。例如，www. symentev. com就是一个『FQDN』，其中www是主机、symentev是次级网域，而com则是最上层网域。此功能可运用在『网站管制』黑/白名单及网站类别数据库功能鞭长莫及的地方(仅可管制HTTP)，如HTTPS、FTP。

如何运用「FQDN」机制，方能达到企业最大利益？举下列情况为说明：
透过HTTPS浏览拥有多个IP的网站(如：Yahoo、Google…)时，「网站黑名单」、「网站类别数据库」就无法阻挡。若以IP、网段方式管制连至上述网站，又很容易会有所遗漏。

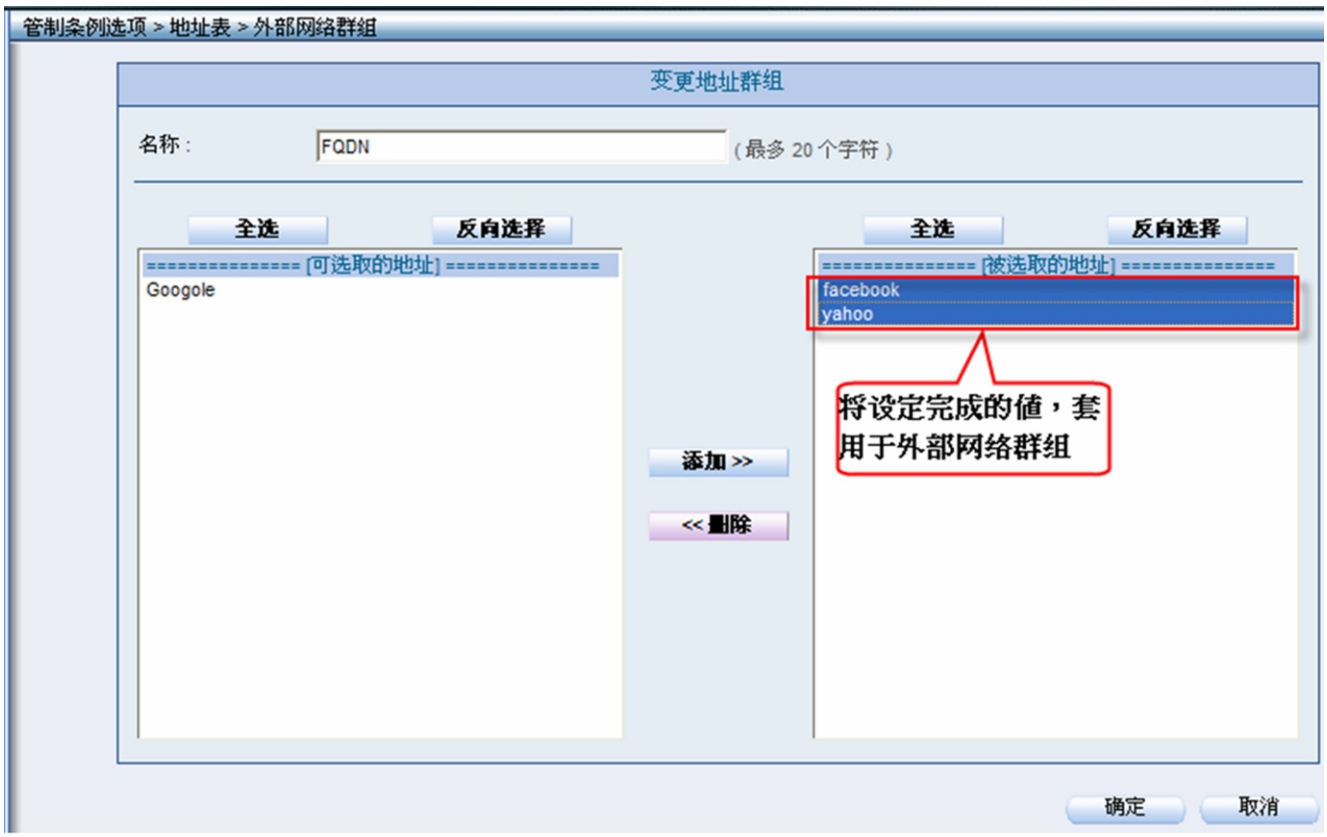


图二 『FQDN』的运作方式

为了因应此种状况，新软UTM让管理人员在外部网络地址表之『FQDN』设定方式一于字段中填入目标网站的「主机名称+网域名称」，若网址为「http://www.facebook.com/#!/profile.php?id=105520583884516」的网站，则于『FQDN』字段中填入「www.facebook.com」即可。

图三 外部网络地址表填入目标网站的『FQDN』

若要阻挡二个以上拥有多个IP的网站，管理人员于『外部网络』地址表做相关设定后，再套用于「外部网络群组」地址表中。



图四 外部网络『FQDN』群组地址表

上述所设定完成的值，最后于管制条例中套用，即可封锁拥有多组IP的网站，且弥补了『网站管制』机制不足之地方。

图五 将设定值套用于管制条例中

文 余光明 kongmeng@nusoft.com.tw