新软周报
http://www.nusoft.com.tw
Internet Security Fighter
2011/6/1-2011/6/30 第128期

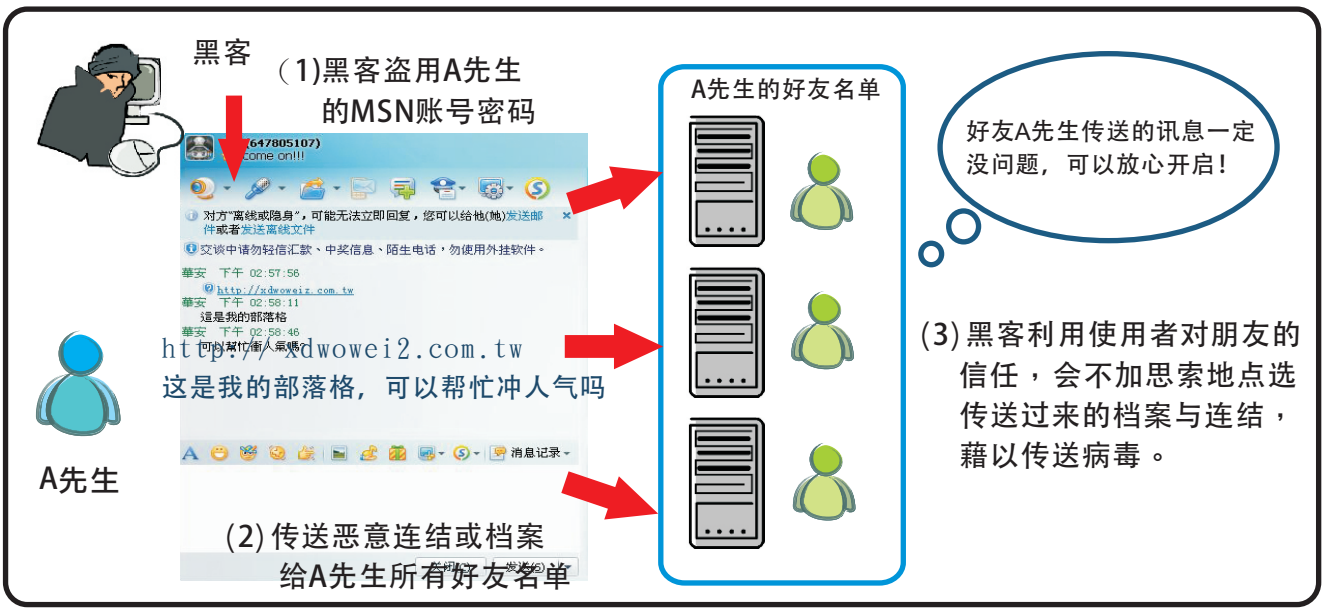
## UTM / UTM系列报导

# 技术浅谈与应用 ─新软UTM有效预防社交工程攻击

近年来因特网发展迅速，使得计算机网络已成为社会发展与人们日常生活中不可或缺的重要工具，举凡购物网站、网络银行、社群网站等，须透过因特网联机至这些相关商业服务的网站。因此，人们在日常生活中已与因特网密不可分。但是，因特网除了带来生活的便利外，也伴随着各种网络犯罪手法的快速成长，已对个人数据、财产、公司系统等产生极大的威胁。其中「社交工程」成为最常用且难以防范的攻击手法。

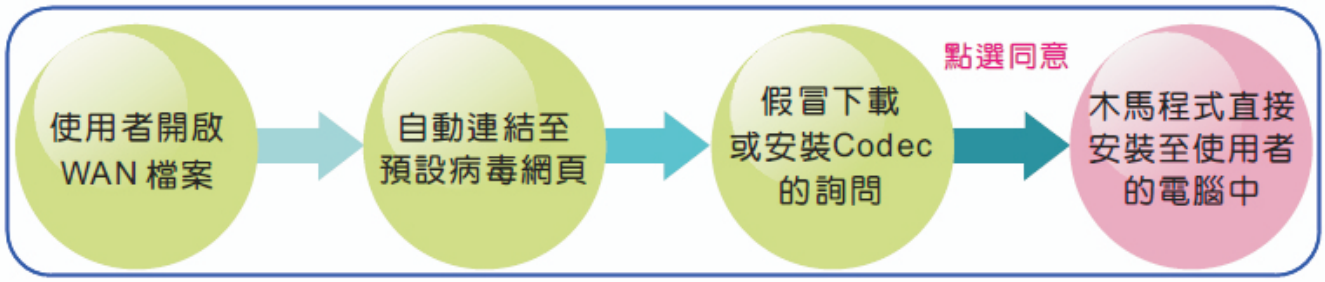
何谓「社交工程」(Social Engineering)？是一种「非全面」技术性的信息安全攻击方式，藉由人性的弱点进行诈骗。如恶意人士利用电话、电子邮件或假扮身分，取得他人信任进行欺骗。这些手法的特性是攻击者并不需具备顶尖的计算机专业技术或攻击工具，仅利用人缺乏警觉性或好奇心的弱点，就可轻松骗取个人数据、系统账号密码等重要数据。

1. 各种实时通讯软件(IM)：
实时通讯软件病毒必须仰赖使用者之间互相传递，因此，黑客藉由入侵计算机，窃取计算机使用者的IM软件账号(如MSN、Yahoo…等)，并传送恶意档案或URL连结等方法，利用假冒使用者的身分诱骗使用者好友点击传送的连结。



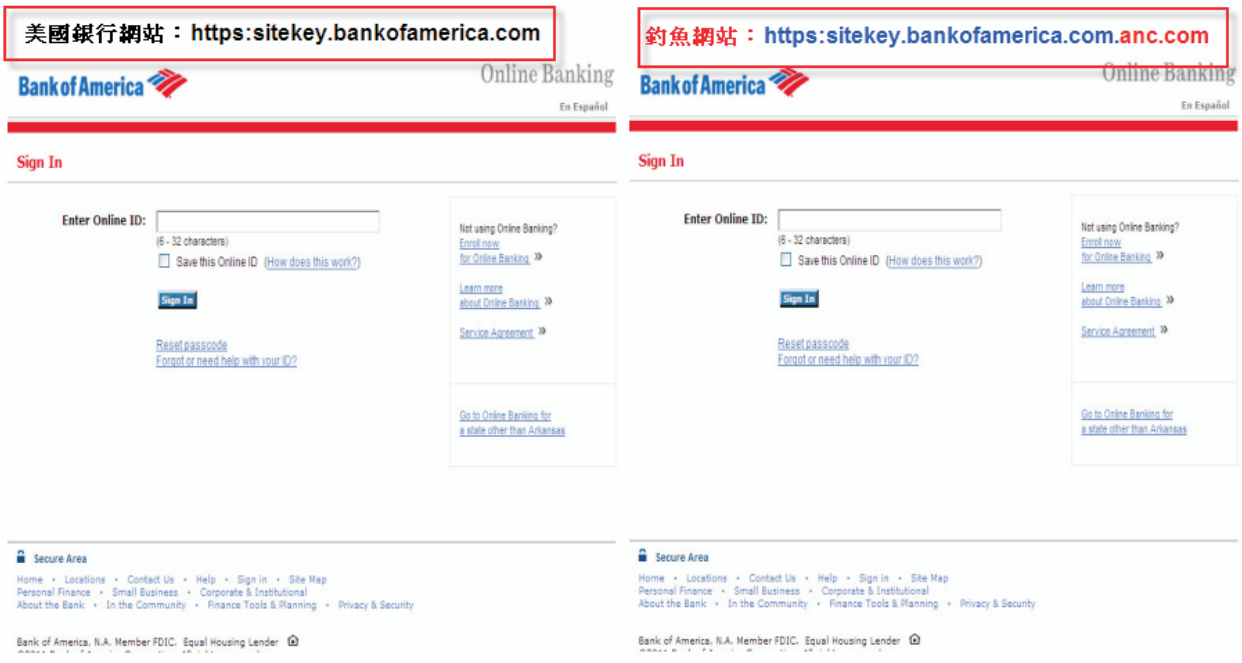

图一

2. 多媒体影音中的恶意程序：
是针对影音播放程序攻击的木马，将多媒体档案嵌入恶意程序，使用者一旦用影音播放程序打开受感染的多媒体档案，计算机就会被连上恶意程序。




图二

3. 网络钓鱼：
网络钓鱼所用的诱饵千奇摆怪，包括伪装知名银行或机关单位通知收件人资料过期、无效需要更新，或登入某网址输入个人数据等诈骗方式。取得个人账户、信用卡或公司机密…等数据，造成公司数据外泄或个人账号密码被盗用等严重后果。




图三

4. 伪装修补程序：
伪装系统厂商或防毒软件业者，寄送假的修补程序或更新程序的电子邮件，引诱使用者下载安装。此种手法不但不会修补操作系统的任何漏洞，还可能被安装了远程窃取数据的木马程序。

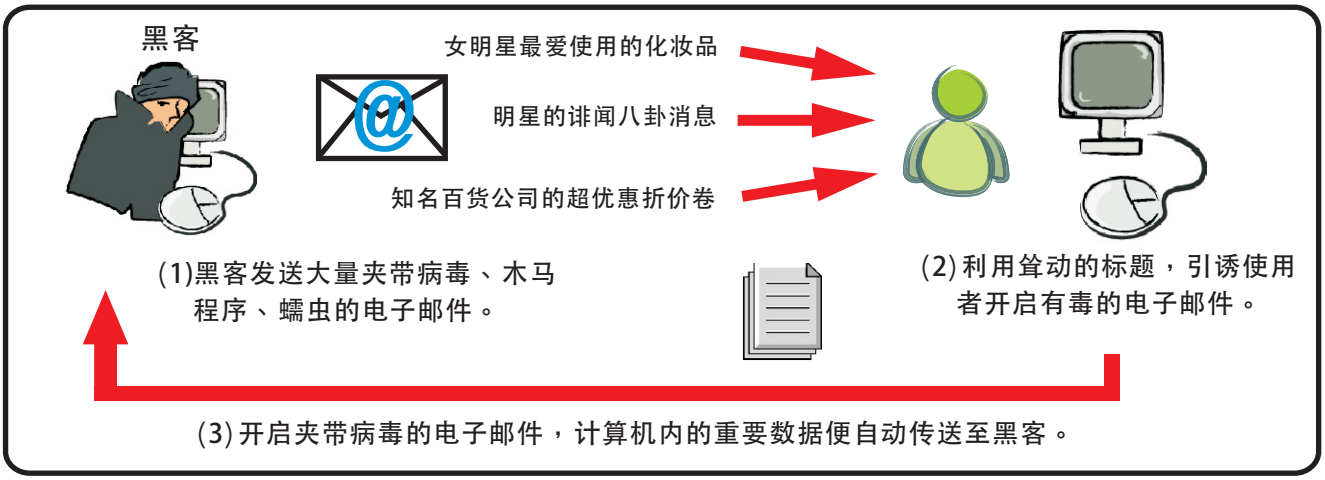
5. 交互式社群网站攻击：

是一种通过社群网站传播的蠕虫，可以在推特、facebook、噗浪等知名网站散布；一旦受害，计算机会被启动后门程序，私密个资可能不保，同时还会发送有害连结给在线朋友。


图四

6. 电子邮件：

黑客利用电子邮件夹带病毒、木马等恶意程序，邮件标题再藉由热门时事、养生保健或情色相关等耸动标题，引诱收件者开启邮件所附带的恶意程序。甚至假冒收件人好友，骗取收件人的信任，进而开启邮件，造成数据外泄。




图五

在了解社交工程的攻击手法后，有效防范社交工程企业应着手于三大方向：一是内部资安政策，另一网络防护的软硬件，最后员工须有正确的资安观念。此三大方向是相辅相成，缺一不可，小则造成个人用户使用的不便，大则造成网络的瘫痪、重要机密数据被窃、存盘数据遗失…。因此，新软系统UTM系列产品，提供「邮件安全机制」、「入侵侦测防御」、「应用程序管制」、「网站管制」等几种方式，且搭配公司的资安政策，有效防止公司成为社交工程攻击的对象。

1. 邮件安全机制：

由于电子邮件的便利，却带来垃圾邮件与病毒邮件的危害。因此，新软系统「MLS」、「MAF」与「UTM」系列是拥有邮件安全防护性质的产品，皆提供「多重垃圾邮件过滤机制」与「病毒防护」(内建ClamAV与Sophos双扫毒引擎)功能结合，除了直接将垃圾、病毒邮件阻挡在公司网络之外；亦可将阻挡钓鱼邮件。而且公司资安政策中应规定内部员工须确认信件来源，不要开启来路不的电子邮件（如过于耸动的主旨、陌生人或少往来对象来信、要求输入机密数据等）及可疑的附件档案(如exe、dll、scr、bat等)；也避免开启与公务无关的电子邮件。

2. 应用程序管制：

继电子邮件之后，各种应用程序软件成为现代人或公司员工所广泛使用的通讯及娱乐的桥梁，如实时通讯软件(MSN、QQ、Yahoo、Web IM…)已成为与客户商业往来的重要沟通工具。由于实时通讯软件的便利，进而使黑客利用IM传送恶意连结或木马程序等攻击，来窃取个人或公司内部相关重要资料。而且公司网管人员可依据各部门业务的需求给予开放或限制使用实时通讯软件的权限，且透过新软系统「UTM」、「IDR」系列产品之内建「应用程序管制」功能作IM管制。此功能采用独有的「应用程序特征码」阻挡机制，针对目前一些主流的IM或Web IM所特别设计，不论这些应用程序的 Port 号再怎么改变、版本再如何异动，只要符合IM「应用程序特征码」的封包一律皆阻挡下来。并且新软UTM「应用程序特征码」提供永久免费在线更新，让应用程序特征码保持最新状态。另外，给予开放使用实时通讯软件的员工，新软UTM提供了详细的实时通讯讯息记录，藉此防止员工泄漏公司数据。

3. 网站管制：

若针对FaceBook、网络银行…等网站，容易成为伪装平台，须作为有效管制。新软「UTM」、「IDR」系列皆提供「网站管制」机制。公司网管人员利用「网站白、黑名单」功能，针对特定网站做开放或限制进入的制订，同时亦可对FTP或HTTP上传档案之扩展名做阻挡，以免造成员工泄漏公司重要数据；且「UTM」内建的「网站类别数据库」(此为付费功能，内含65型网站分类包括：钓鱼&诈骗网站、社交网站…等等)来判别目前使用者所欲浏览的网站是否为「钓鱼网站」且将钓鱼网站自动屏蔽掉，让使用者无法顺利连结，藉此告知使用者所浏览的网页为钓鱼网站；而且云端的「网站类别数据库」保持在最新状态。所以网管人员依公司网络政策管制员工所不能浏览之网站类别(社群网站、非官Web IM网站…等)，及员工不慎开启恶意连结或附件档案并加以阻挡。

4. 入侵侦测防御(Intrusion Detection Prevention)：

如上述之「应用程序管制」和「网站管制」二项功能，搭配新软UTM「入侵侦测防御」机制，增强防御社交工程攻击。由于黑客藉由实时通讯登入/传文件，电子邮件及网页等攻击方式，窃取公司重要数据网管人员利用可针对公司网络实际需求，自订所要的特征加以阻挡或通行；并且内建的「IDP特征数据库」会每两小时自动上线检查是否有新的特征挡下载，以维持数据库在最新的状态。另外，网管人员藉由「异常侦测」设定，可针对各种网络攻击模式防御；当网络联机符合攻击模式时，新软UTM会将它视为网络攻击，并依管理人员所订定的处理方式处理该联机。

随着信息科技日新月异，社交工程手法也不断翻新。因此企业除了投资各种网络防护的软硬件外，须建立正确防范社交工程的观念(包括员工教育训练与平常的倡导)，且企业应拟定内部资安政策，即使有违法员工也会受到该有的处置。尽管不断研发出新技术加强信息防护，但整个信息系统环节中，最脆弱的部分仍然是「计算机使用者」，因为只要有「人」，就会有弱点。所以计算机使用者须有正确资安观念与良好的计算机使用习惯，也随时具备危机意识及警觉心，才能减少社交工程攻击伤害。

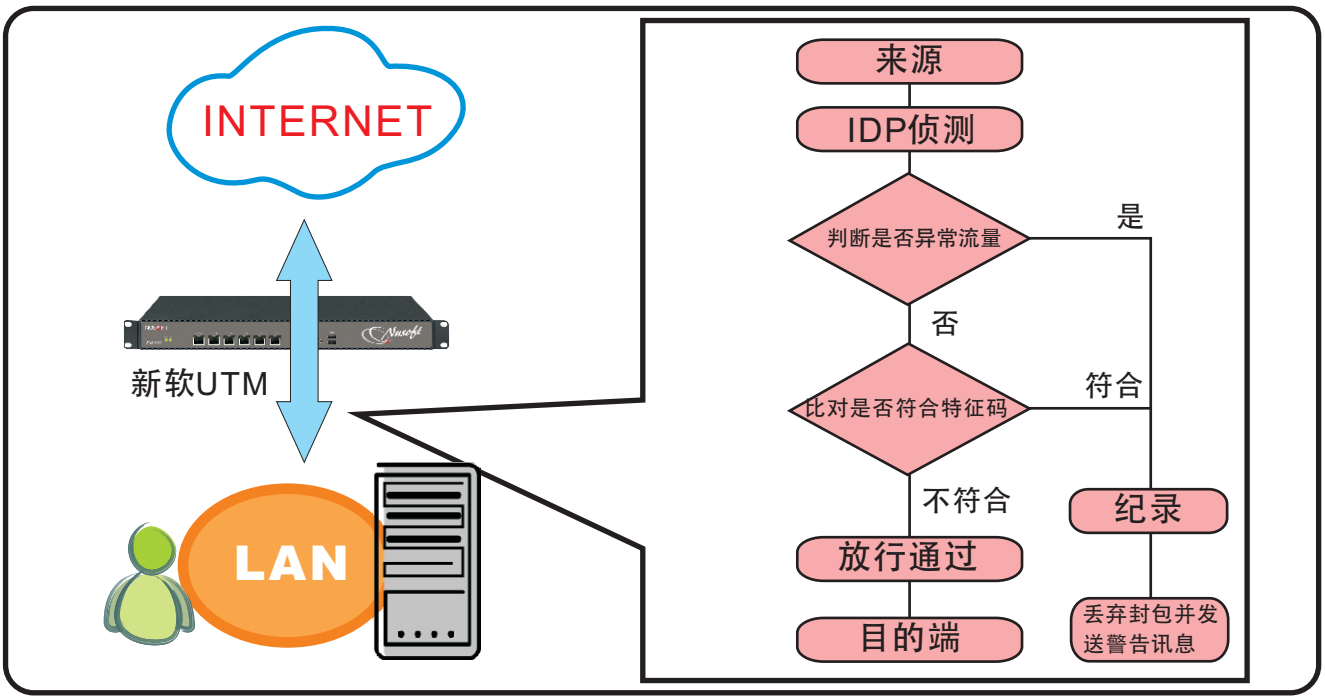
文 余光明 kongmeng@nusoft.com.tw

## 市场营销报导 - 新软UTM帮企业做好防护措施，不怕黑客入侵

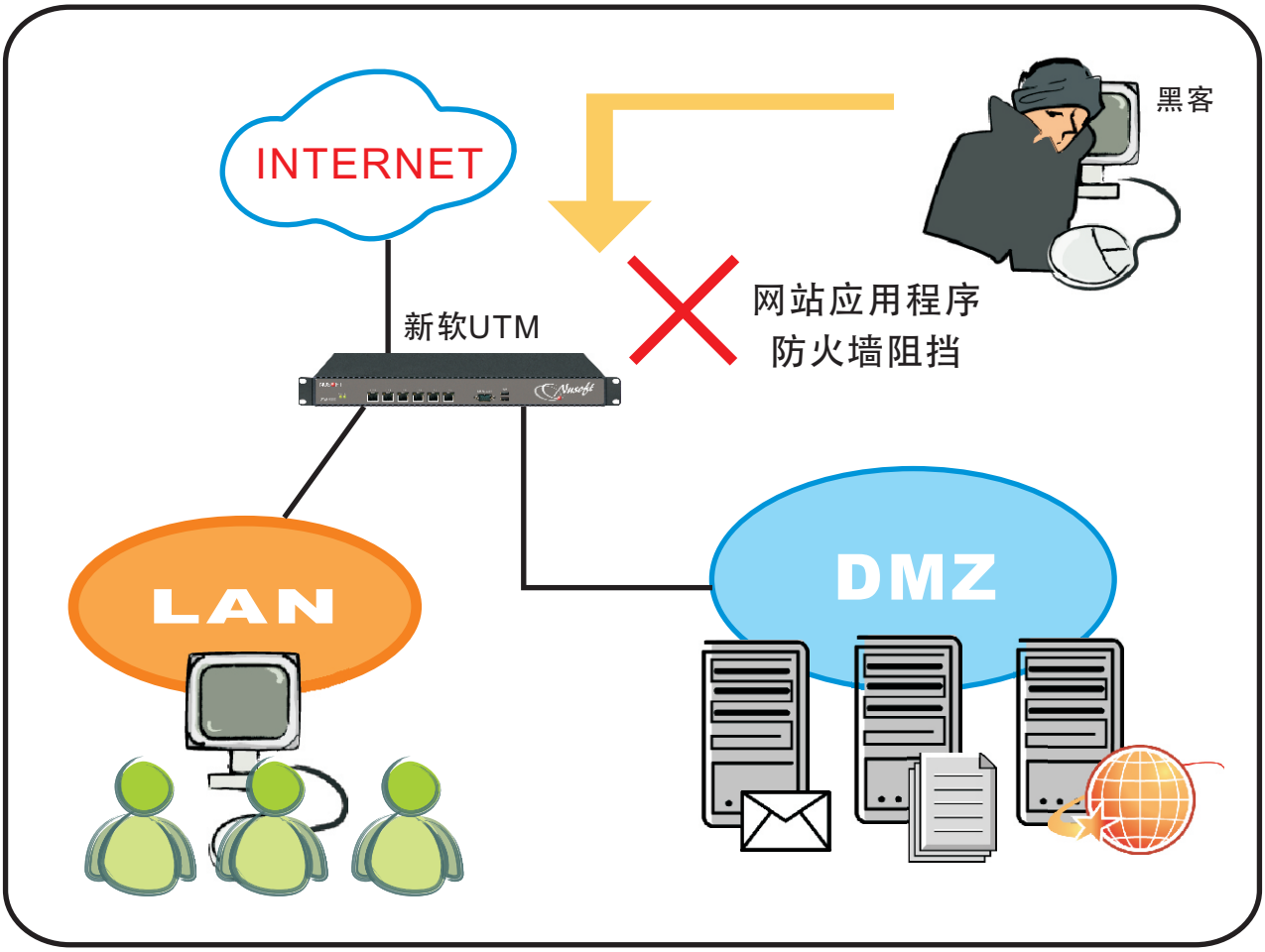
网络生活的普及化，却也潜藏着许多陷阱与危机，网络上到处充斥着黑客的攻击，不时有黑客入侵企业网络中盗取机密数据造成企业损失的负面新闻报导，如Sony旗下游戏平台PlayStation Network在近期数日遭黑客入侵、被窃取1亿笔用户的个人数据，甚至连资安大神HBGary Federal也踢到铁板，该网站遭黑客入侵，被窃取主管电子邮件约6万封，而且1TB以上的备份数据被销毁，这些受害案例层出不穷，如何防止黑客入侵已成为资安重要的课题。

黑客入侵企业网络，通常利用系统的应用程序漏洞，再以数据隐码攻击(SQL Injection)或跨网站脚本攻击(Cross-Site Scripting)等攻击方式入侵系统植入木马程序，以便黑客自由进出该系统窃取档案数据，甚至黑客利用殭尸网络(Botnet)中的受害计算机对特定目标发动大规模的分布式阻断服务(DDoS)或阻断服务(DoS)等其它攻击手法，藉以把目标的系统资源耗尽并瘫痪其网络资源，若该目标是企业对外提供服务的服务器，必然会造成企业若大的损失。

因此，新软系统推荐UTM作为企业网络与因特网间的大门守卫，新软UTM内建「入侵侦测防御系统」(Intrusion Detection and Prevention；IDP)，能依照各种网络服务的漏洞做防护，无论黑客想透过系统的应用程序漏洞入侵企业网络，还是利用殭尸网络中的受害计算机发动大规模的攻击，新软UTM均会依黑客攻击的途径及模式做判断而加以阻挡，加上新软UTM具有SPI防火墙的功能可在预设情况下拒绝所有对外的服务，只要符合已建立的规则，封包就能通过防火墙进入内部网域；并且透过NAT地址转址的功能让内部计算机不易成为黑客攻击的目标，在新软UTM层层的保护之下，黑客想入侵企业网络是难上加难。



此外新软UTM还拥有「网页应用程序防火墙」(Web Applicaltion Firewall；WAF)功能，加强对企业内部的网站安全与防护，而且有别于其它「软件式」的网站安全布署模式，新软UTM所内建的「网页应用程序防火墙」完全不需要再另外安装内部网站主机上，也没有烦杂的设定程序，让管理人员只需针对欲使用的特征码做简单的勾选动作，即可让企业网站享有专业级的防护能力。




为因应多变的网络攻击环境，新软UTM除了会不断自动在线更新「入侵侦测防御特征码」和「网页应用程序特征码」之外，管理人员亦可针对企业网络实际需求，自订所要的特征码，让新软UTM的IDP和WAF防护更具弹性。另外，新软UTM之「异常流量IP」功能，当内部计算机中毒时，导致区域内网中产生大量且不明的对外联机，新软UTM侦测出异常流量并将相关信息记录于设备中，且实时阻断发生问题的使用者，以确保网络安全，在发生异常流量的同时，新软UTM根据管理人员所设定的警讯通知形式发出警讯(如：E-Mail、SNMP Trap、NetBIOS)，通知该使用者及管理人员协助处理，使资安事件的发生达到实时且有效的控管，以避免异常流量对于企业网络造成危害。

文 余光明 kongmeng@nusoft.com.tw