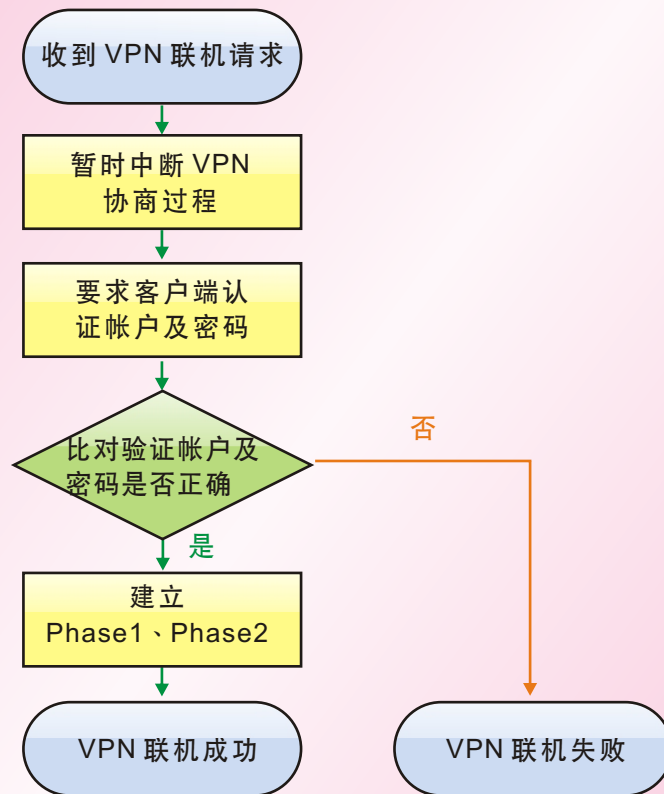


## UTM / UTM 系列报导

### 技术浅谈与应用 - 新功能 XAuth 应用，让 IPSec VPN 安全把关多一层

目前由于网络带宽的快速发展，企业部署 IPSec VPN 网络，构建分公司与总公司之间资源交流的安全管道已逐渐普遍。新软系统近期于 IPSec VPN 中新增了延伸认证功能 (XAuth)，让 IPSec VPN 在相互连接时不仅只是需要相同的数据安全传输协议，还需要经过账号及密码的认证才能有效的连结成功。

相信管理人员共同的问题是延伸认证 (XAuth) 功能的运作方式为何？当客户端开始一个 VPN 连接请求的时候，延伸认证 (XAuth) 功能会强行暂时中断 VPN 协商的过程，并要求客户端输入合法的账户名称与密码来进行验证，UTM 在接收到来自客户端提供的账户名称和密码之后，首先会搜寻 UTM 认证表并校对验证讯息是否正确，如果在认证表中找不到相对应的账户名称及密码则会立即中断该 VPN 连接。



延伸认证 (XAuth) 运作流程图

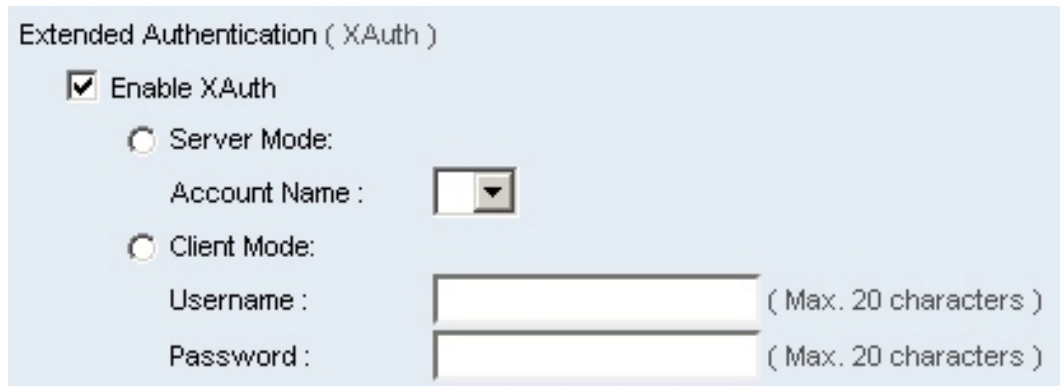
新春福兔送吉祥



吉 兔 蕴 福



管理人员如欲使用延伸认证功能 (XAuth) 时又该如何去设定呢？其实只需简单的两个步骤即可完成，首先需要于『Policy Object > Authentication > Account』下建立所需使用的认证账户名称与密码，并于『Policy Object > VPN > IPSec Autokey』建置 IPSec VPN 设定时勾选启用延伸认证 (XAuth) 功能即可。而设定内容又分为“Server Mode”、“Client Mode”两种，差别只在于“Server Mode”是要求认证的一方，而“Client Mode”则是接受认证要求的一方。



IPSec VPN 延伸認證功能 (XAuth)，只需簡單勾選啟用即可

这里要特别注意的则是，不可两端设备都勾选“Server Mode”或“Client Mode”，必须分别设定一端是为“Server Mode”而另一端为“Client Mode”才能成功的进行延伸认证 (XAuth) 并完成 VPN 连结的动作。

文  陈殿鸿 kim@nusoft.com.tw



## 市场营销报导 - 新软网站应用程序防火墙轻松保护公司网站

网络生活的普及化，公司内部设置相关网站的情况也愈益普遍，不论在产品销售或服务提供，透过网站架设来提供在线服务享受其便利性及随之而来的可观利益外，也伴随着网站应用程序得面临成为攻击目标的风险存在。这些攻击对公司营运所产生的冲击而造成财务上损失与重要数据因此外泄的严重后果，都是难以估计的。

一般人会认为网络与系统安全保护就等同于网站应用程序的安全，其实不然，传统的网络安全只防守网络层与传输层的攻击，而对于网站应用程序的攻击手法，如跨网站脚本攻击 (Cross-Site Scripting ; XSS) 或数据隐码攻击 (SQL Injection) 等针对网页应用程序弱点的攻击形式，传统的网络安全设备就明显的无能为力。

新软系统 UTM 为补足传统防火墙仅针对网络层与传输层过滤的缺憾，近期更新增加了『网站应用程序防火墙 (Web Application Firewall ; WAF)』功能，加强对公司内部的网站安全与防护。有别于其它『软件式』的网站安全布署模式，新软系统UTM所内建的网站应用程序防火墙完全不需要再另外安装于内部网站主机上，也没有烦杂的设定程序，同时还拥有大量的网站威胁防御特征码，让信息管理人员只需针对欲使用的特征码做简单的点击动作，即可让公司网站享有专业级的防护能力。



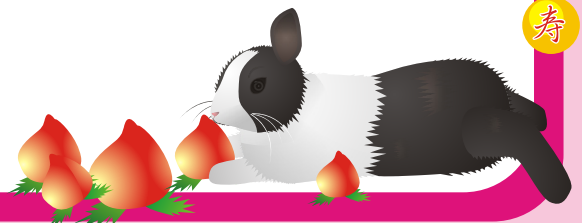
只需简单的点击动作，即可完成设定

为因应多变的网络攻击环境，新软系统除了会不断更新网站应用程序防火墙的网站威胁防御特征码之外，更增添了『自订特征』功能，让信息管理人员还可随时自行定义防御特征，以调整到最适合每间公司自己所使用的网站威胁防御特征环境，达到更完善的防护效果。

网站应用程序防火墙功能也提供了详细的记录日志与统计报告，可协助信息管理人员分析公司网站被攻击的方向并改善网站架设安全；定期寄送报告功能还能有效减轻管理人员查阅负担，同时也设有日志搜寻功能可供管理人员能针对攻击地址、联机网址、特征类型、攻击事件与特定日期时间做查询，让管理人员能够在网站应用程序防火墙管理方面更轻松省时。

灵  
兔  
献  
寿

福 禄 寿 喜 皆 满 载





拥有详细的记录日志与统计报告内容

文 陈殿鸿 kim@nusoft.com.tw

玉兔报喜



心想事成鸿运开

