新软周报
http://www.nusoft.com.tw
Internet Security Fighter
2010/3/29- 2010/4/11 第114期

多功能 UTM / MS 系列报导

技术浅谈与应用 - 管制条例的基础概念

随着时代的改变，信息技术日异月新，过去公司内所架设安装的信息安全设备也从多台式的机架型设备转变为单台整合式的设备，也就是多功能型的 UTM，并集其多项信息安全功能于一身，如此一来则可有效的简化公司内部安全部署以及人力资源的投资，让公司可以以最少的成本来换取更大的回馈。

新软系统多功能 UTM 使用单一操控画面，集中控管所有功能，有效减轻管理人员负担，而于多功能 UTM 系统中担当集中控管的重要角色就是『管制条例』该项功能。管制条例中的参数包含有来源网络地址、目的网络地址、服务名称、自动排程、认证名称、VPN Trunk、管制动作，外部网络端口、流量监控、流量统计、IDP、内容管制、网站管制、应用程序管制、病毒侦测、带宽管理、每个来源 IP 最大带宽、每个来源 IP 最多联机数、最多联机数、Quota Per Session、Quota PerSource IP 及 Quota Per Day 等。系统管理员可以经由这些参数来管理、设定不同出入埠间的数据传送以及服务项目，哪些网络对象、网络服务或应用程序的封包该予以拦截或放行。

新软多功能 UTM 为了让所有管理人员可更明白且轻松的为公司管理内部资源，依据不同来源地址的数据封包，管制条例设定功能详细的区分为『内部至外部』、『外部至内部』、『外部至非军事区』、『内部至非军事区』、『非军事区至内部』、『非军事区至外部』六个方向，以便利系统管理员针对不同数据封包的来源 IP、来源埠、目的 IP、目的端口制订管制规则，藉此达到更完善的多方面管理，让公司能够享有更安全、更有规划的网络环境。

（一）【内部至外部】：来源网络地址是在内部网络区，目的网络地址是在外部网络区。
（二）【外部至内部】：来源网络地址是在外部网络区，目的网络地址是在内部网络区（如 IP 对映、虚拟服务器）。
（三）【外部至非军事区】：来源网络区是外部网络区，目的网络区是在非军事区（如 IP 对映、虚拟服务器）。
（四）【内部至非军事区】：来源网络区是内部网络区，目的网络区是在非军事区。
（五）【非军事区至内部】：来源网络区是非军事区，目的网络区是在内部网络区。
（六）【非军事区至外部】：来源网络区是非军事区，目的网络区是在外部网络区。

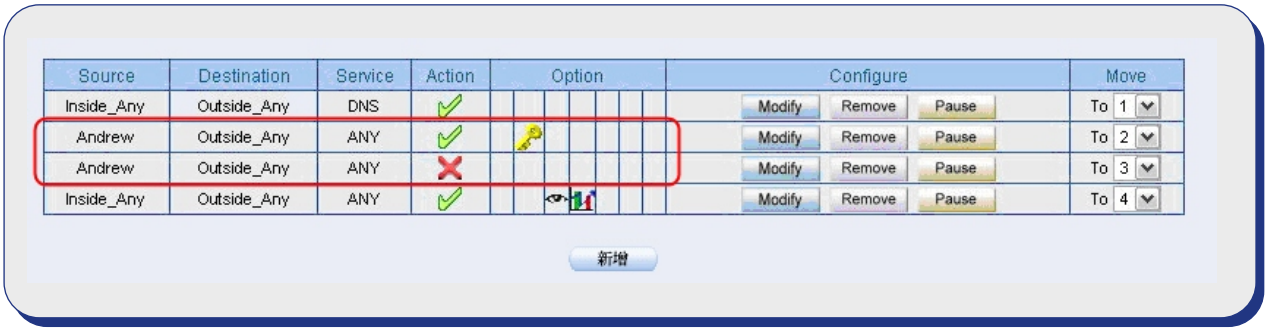
新软『多功能UTM-MS』所采用的是 SPI Firewall 架构，以『管制条列』为中心，将全部通路预设为阻挡，若无另行开放条例，封包便无法正常通过，有别于他其所采用 IP Sharing 先全部放行再自行设定阻挡的方式，SPI Firewall 的架构方式相对的让公司安全更加有保障。也正因为所采用的是 SPI Firewall 架构，所以管理人员于一开始架设新软多功能 UTM 时，最好暂时先于管理接口中“管制条例 > 内部至外部”下开放一条内部至外部为 Any 的条例，以供公司内部使用者能够暂时正常使用网络资源，防止网络因一时无法使用而影响公司运作，当管理人员将系统设定完成后，建议最后要将 Any 的条例拿掉以防止部份使用者走该条例出去，而失去了其管制的意义。

暂时开放 Any 管制条例让公司网络保持正常运作

此外，管理人员还要了解到 MS 中的管制条例运作的基本原理，于 MS 设备中管制条例是采用从上而下逐条比对的方式在运作（比对“来源地址”、“目的地址”、“服务”），每一个封包在通过 MS 时，需要从上而下逐条检查是否符合管制条例中所设定的条例内容。当封包的条件符合某条管制条例时，就会按该管制条例的设定来通过，而不会再向下检查其它的管制条例，所以当管理人员在设定管制条例时一定要特别注意到条例排列顺序，以免造成所设定的条例无实际作用。

封包通过管制条例，由上而下逐条比对，所以需注意排列顺序

另外当 MS 比对到有需要认证的管制条例时，系统会先向下比对看是否有可以允许放行的条例，若有，则会走下方条例出去。因此，若系统管理人员欲设置使用认证功能时，在设定其认证的管制条例下方，需再另设定一条阻挡的条例，其用意是为了让比对的动作到此为止，不再继续向下做比对。



在认证的管制条例下方，再设定一条阻挡的条例，让比对动作不再继续向下

文 陈殿鸿 kim@nusoft.com.tw

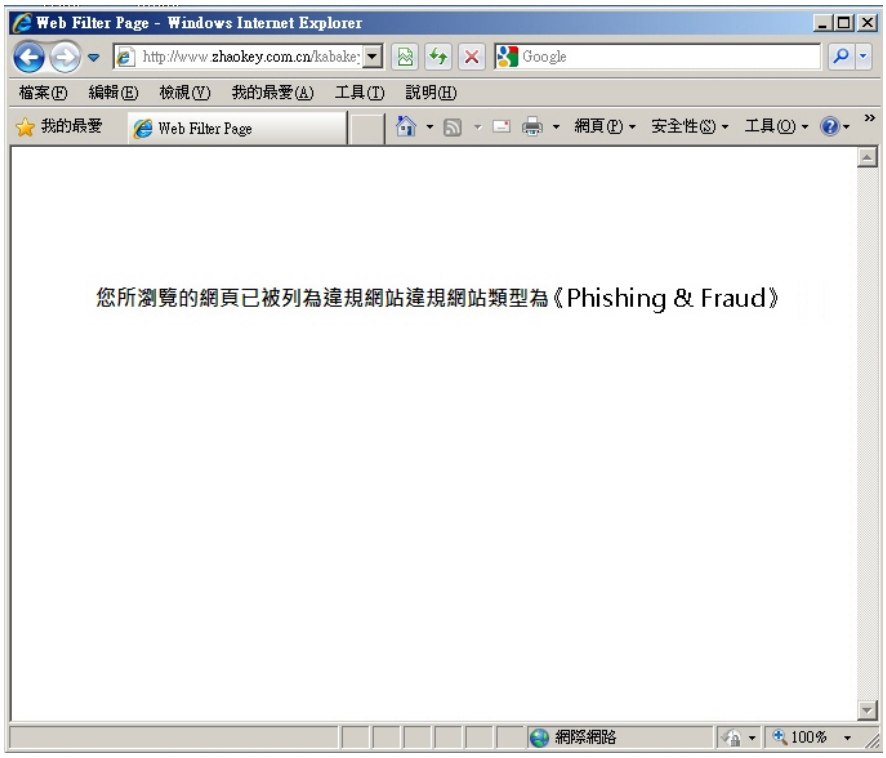
市场营销报导 - 新软多功能 UTM「网站管制」机制，让你不用担心再被“钓鱼”！

近年来网络技术发展越来越迅速，使得网络科技逐渐融入人类生活中进而开始全面生活 e 化，这类趋势使得许多人原本的生活模式渐渐开始「网络化」，最为显著莫过于生活周遭中的食、衣、住、行、育、乐，例如：网络购物、交友网站、甚至是“网络银行”等之类关于钱财方面的网络商业服务，这些网站都是黑客眼中非常适合“钓鱼”的绝佳平台，因为黑客可以利用这些埋藏网络钓鱼陷阱的网站，让轻忽网络资安陷阱的一般使用者上钩，藉此骗取使用者的账号密码来获得他们所想要的利益。

网络上钓鱼诈骗事件频传，一般企业防火墙、防毒墙亦无法提供完善保护

日前就传出多起网络购物拍卖网站及网络银行遭到黑客入侵并被植入钓鱼网页的案例；不肖人士企图诱骗该网站会员在不自觉的情况下登入，进而骗取该网站会员的账号密码欲用来获取不法利益。倘若发生此类问题将会带来难以估计的严重后果，轻则人或企业的机密数据外泄、重则财产身家遭到歹徒洗劫一空，因此对于此类钓鱼网站的防范将是时时刻刻不能掉以轻心的事，即便像是拥有防毒墙、防火墙的企业用户来说，也是无法在第一时间上得到最完善保护的。

网络科技、一日千里，网络上的资安陷阱危机也是每天不断地进化。而相同的，新软系统产品设计也是一向随着时代潮流趋势而不断研发、不断进步；因此对于此类问题，有别于一般企业防毒墙、防火墙简单的网络防御机制，新软多功能UTM（MS1500G 以上机型）能提供使用者有效且完善的管制功能。为了能有效避免企业底下的使用者因为被钓鱼网页“钓鱼”，所以提供给使用者有效的管制措施—「网站管制」机制；此机制能以新软多功能 UTM 内强大的「网站类别数据库」（内含 64 型网站分类包括：恶意网站、钓鱼 & 诈骗网站、殭尸网站、垃圾邮件网站...等等）来判别目前使用者所欲浏览的网站是否为“钓鱼网站”？若「是」，则会自动将使用者欲浏览连入的“钓鱼网站”自动屏蔽掉而让使用者无法顺利连结，并且可在该屏蔽网页上显示予使用者知晓，藉此让使用者知道“他被钓鱼网站骗了!”；如此一来，便可以让使用者免除于网络危机之外，也让企业能够妥善安稳的存在于安全保护之内。



新软多功能 UTM 提供用户有效的「防钓鱼诈骗机制」，藉此获得更完整的网络保护

新软多功能 UTM 除了替企业达到最完善的防毒墙、防火墙保护之外，也为了网络上日趋强大的网络资安危害而不断地研发更加完善的网络防护机制，最终的目标即是为了能辅助企业安全屹立于网络上，藉由网络的无限浩瀚，赚取更多的利益与商机，进而创造企业的营收高峰。

文 黄政铭 ming@nusoft.com.tw