新软周报
http://www.nusoft.com.tw
Internet Security Fighter
2009/1/12- 2009/2/8 第84期

多功能 UTM / MS 系列报导

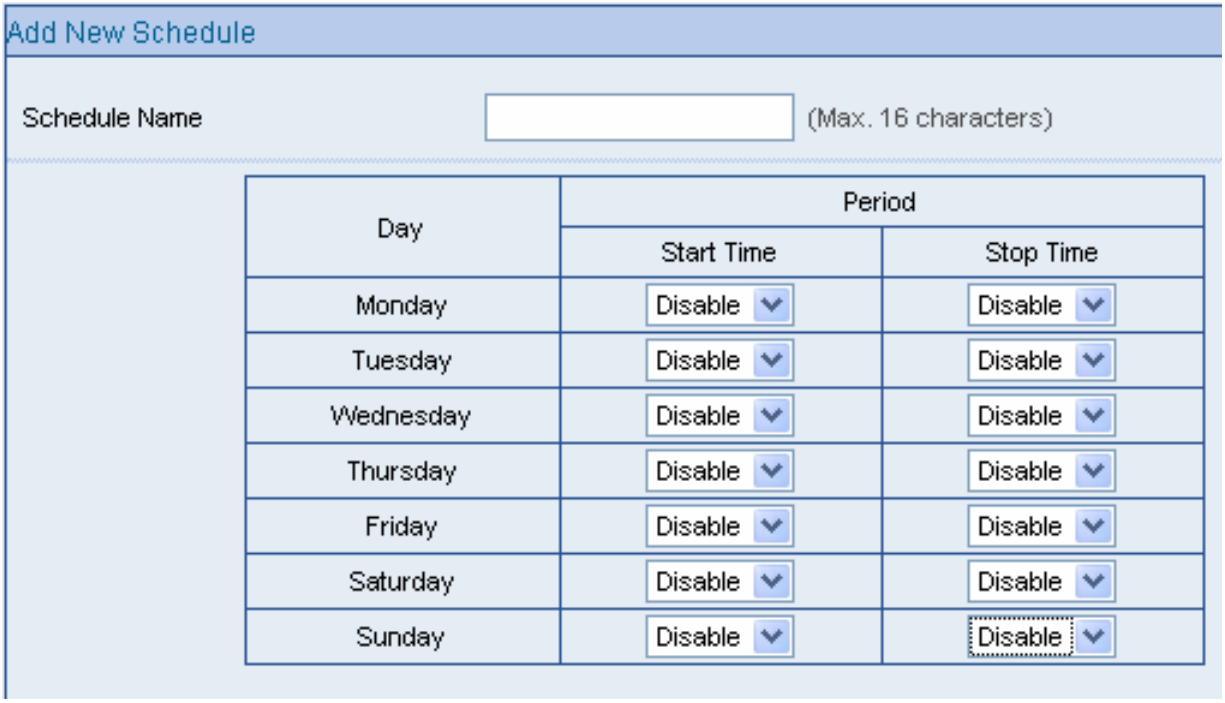
技术浅谈与应用 - 妥善使用排程表，帮公司打造优质的工作环境

因特网的方便，造就了企业不少的商机，因特网不但缩短了公司与客户间的距离，也同样的缩短了公司与公司间互相交流的距离，在现阶段的生活中一切的事物也大都与网络脱离不了关系，它的方便不但带来了不可否认的利益，也渐渐的促使现代人对它的依赖，但越是方便的东西就越容易遭人滥用。

根据调查分析，75% 的员工都曾使用过公司的网络来处理私人事情，举凡浏览网络拍卖、新闻及收发私人信件 or 使用网络通讯软件进行聊天…等，如此一来员工的工作效率相对降低而相继影响到的则是为公司所带来的收益减少，在这种恶性循环下，时间越久对公司的影响就越大。

身为公司的网管人员，为了要帮公司打造出一个优质的网络环境，除了要维持内部网络的稳定及安全之外，同样的也要兼顾到公司里网络资源所使用的情况，在做网络管理限制的同时还必须考虑到各部门或特定人事 (部门主管、老板…) 的网络资源，需求不同要给予不同的限制条件，在种种不同的需求情况下网管人员要如何去把多余的时间空出来处理这类烦杂的事情？而管理人员除了去限制内部使用应用程序、各式软件之外，还可利用什么方式加以辅助及管理内部人员的上网权限呢？

利用新软系统『多功能 UTM - MS』中所内建的 Schedule (排程表) 功能即可轻松的为管理人员来达成上述的要求，排程表可以针对特定的群组、人员来依网络的需求性不同而言，进一步的自由调整、设定每天的哪段时间是否开放使用网络的权限，规划内部使用者一周中每天透过管制条例，存取网络数据的有效时段，例如：面对平时正常工作时间不需要用到网络的部门人员来说 (仓库、基层做业员…)，就可以只设定每日的下班时间才开放此群组、部门或是特定人员的网络使用权限，也可设定成每日的中午休息用餐时间才开放网络使用或是设定成只有正常上班的时间才开放网络使用权限，来以防止部分员工利用下班回家时，使用公司网络来下载私人程序、软件…等，如此一来则可以有效的减少网络资源遭到滥用。而该如何做到适当的搭配则可视公司内部的状况而定。



产品功能 Schedule 画面

妥善利用排程表的自动执行功能，同时再配合上前端防火墙阻挡及限制，系统管理员可以节省更多的管理时间，同时让网络系统发挥最大的效能。适时的开放网络使用权限，可让公司内部更有制度化，而对于一个有制度的公司，相继影响到的就是有效的提升内部的工作效率，如此一来不但可帮公司创造更大的收益，也能为公司带来更多的商机。

最后要注意到的则是排程表必须配合『管制条例？』来使用，管理人员在设定完排程表后必须套用到『管制条例？』里，才能实际的运作。

排程表套入管制条例图示

文 陈殿鸿 kim@nusoft.com.tw

市场行销报导 - 新增管理帐号密码容错次数限制

在现今信息安全事件不断发生的环境下，不论是家用计算机、公司计算机、信息设备…等等，只要能跟网络有相关的设备、机器，都免不了网络上不断涌出的入侵攻击事件，而对于这类型的事件发生，也已经演变成多到让人觉得即使发生也见怪不怪了。

然而，为了防止同样的事情发生在自身家里或公司的机器设备上，除了于设备前端加装防火墙及安装防毒软件来防止机器设备遭入侵破坏，同时也要注意如何防范病毒入侵、黑客入侵，但往往会忽略了最基本的利用破解设备上账号密码来达到入侵目的，尤其是近期最常见的情况就是不少人为了探讨别人隐私而不择手段的去破解使用者放在网络上任何需要账号、密码的网络日志、相簿、信箱、设备…等，甚至在破解进入后将其数据内容加以破坏窜改来达到满足感及成就感。而谁又敢保证哪天公司里的机器设备IP能不被有心人士扫到而加以入侵及破坏呢？

面对如此最基础的入侵方式，为了能有效预防使用者利用账号密码破解的方式来进行入侵，近期也于功能内新增了账号密码容错次数的限制，不论对内或是对外皆可有效的防止有心人事暴力式的破解账号密码来达到入侵。管理人员可自行设定登入之账号及密码可容许的错误次数，及达到错误上限后所要将该登入之IP加以阻挡封锁的时间，相较于一般市售的前端防护设备只以单纯的登入系统方式来说，新软系统多功能UTM目前所拥有的账号密码容错限制绝对是优势许多。

同时于系统Event Log中也会记录所登入且账号、密码输入错误的IP讯息及遭阻挡之讯息，以供管理人员查看，让管理人员可以清楚的了解是内部使用者或是外来的IP在对系统做帐号、密码的破解，则可有效率的做防范。

Time	Event
Dec 30 15:21:47	admin user admin (192.168.10.78) Login Block (exceeded the bad logon attempt limit)
Dec 30 15:21:47	admin user admin (192.168.10.78) [Login failed]
Dec 30 15:21:43	admin user admin (192.168.10.78) [Login failed]

Event Log 登入遭阻挡画面

除此之外为了有效的防止黑客的入侵，新软系统所推出的多功能UTM中不仅是只单单内建管理账号密码容错次数限制的功能，同时还拥有强大的入侵防御侦测系统（IDP）可抵挡黑客的攻击，并且支持网页扫毒的功能，可补足防毒软件无法防护的项目，多方面的保护下让企业的网络安全防护更加有保障，相信多功能UTM一定是企业防护最好的帮手，也是最好的选择。

文 陈殿鸿 kim@nusoft.com.tw