新软周报
http://www.nusoft.com.tw
Internet Security Fighter
2010/2/8- 2010/2/28 第111期

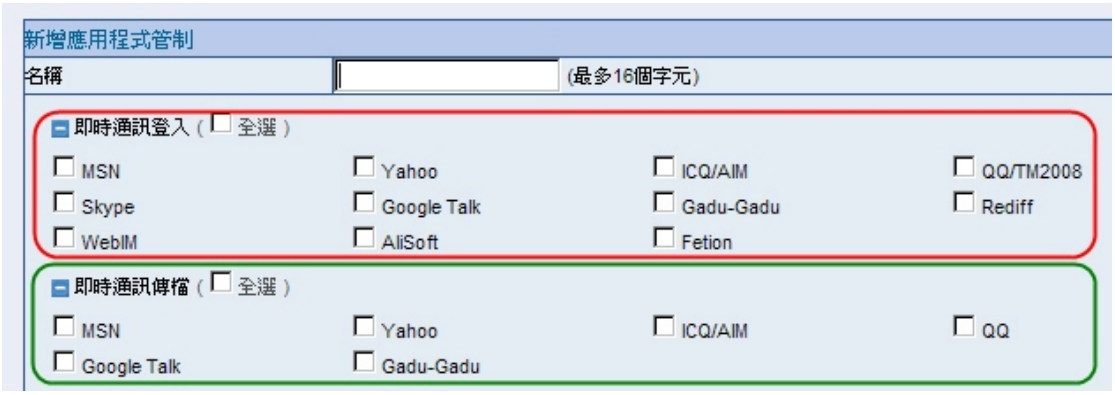
多功能 UTM / MS 系列报导

技术浅谈与应用 - 实时通讯软件的弹性管制及防护

实时通讯软件目前已成为最为受欢迎的沟通工具，是继电子邮件之后另一项最受公司所广范使用的讯息沟通管道。透过实时通讯软件使用者可立即相互的传达文字、语音、视频、绘图与文件，却也因为如此的方便性，渐渐让各公司机关不得不重视相对而来的安全问题，而最近所爆发利用实时通讯软件来泄露公司机密的事件，让关于实时通讯软件的安全议题不断在持续发烧，也明白显现出实时通讯软件近年来对于各公司的重要性。

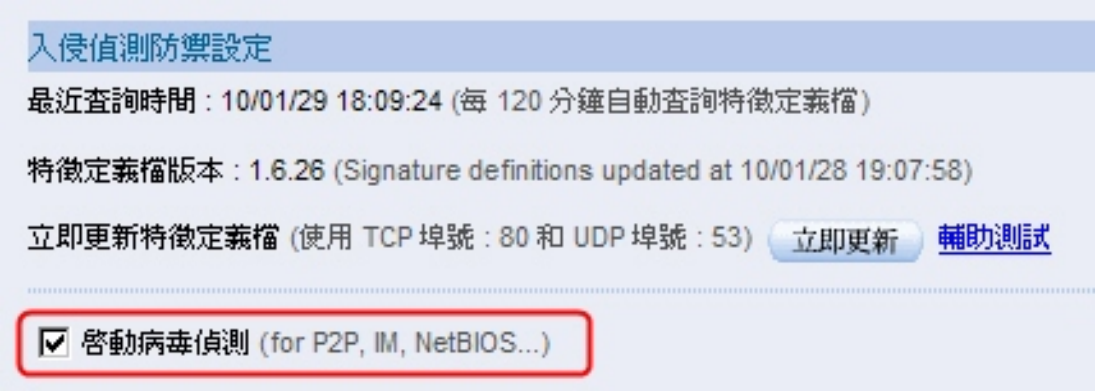
目前公司对于使用实时通讯软件所存在的顾虑不外乎是『病毒的流入』、『文件的交换』两大方向，其次才是员工利用实时通讯软件来进行私人用途，影响工作效率，传送大容量影音文件浪费公司带宽资源...等。面对上述安全问题，公司网络安全管理人员又该如何去适当管制及防范实时通讯软件来捍卫公司信息安全呢？其实管理人员只需要利用新软系统多功能 UTM 所内建的『应用程序管制』与『入侵侦测防御』两大功能，即可满足公司针对实时通讯软件 1.有效管制 (阻挡、开放) 2.允许使用但限制传送文件 3.允许使用且同时搭配 Anti-Virus 防护，的三项信息安全防护需求。

管理人员可于多功能 UTM “管制条例选项 > 应用程序管制 > 设定” 下进行实时通讯软件限制的相关设定，而且没有麻烦的设定手续，只须针对所欲管制的选项进行勾选即可完成设定，但管理人员还要注意到的地方则是，对于设定完成的限制条件，一定要套入 “管制条例” 中才会有实际的作用。同时还可针对不同的来源 (部门) 来搭配不同的限制条件，如此一来能更灵活运用的做适当管制。



应用程序管理设定画面

此外，在开放使用实时通讯软件的情况下，为防止病毒藉此管道流入，管理人员还可于系统“入侵侦测防御 > 组态 > 设定”下，进一步的启动病毒侦测功能，来做到更完善的保护。同时管理人员须于管制条例中勾选启用 IDP 选项才能有实际作用。



可针对实时通讯软件启动入侵侦测防御

除了使用新软系统多功能 UTM 来进行有效的控管及防护之外，公司还可搭配利用教育训练的方式来传达及教导员工该如正确运用实时通讯软件等相关知识，让员工养成良好的使用习惯，以达到更加优化的使用环境。以下将分别提出简略的使用注意事项，以供公司教育参考使用。

1.使用即时通讯软件要以处理公事为使用之目的

于上班时间不以实时通讯软件与他人过度闲聊，或许与客户间的情感交流对公司有莫大的帮助，但过度的滥用实时通讯软件来进行与公司无关的私人聊天，不但有可能会于无意间泄露重要信息，也会影响到公司使用实时通讯软件的正面义意。

(管理人员除了可使用多功能 UTM 来做分别管理，同时也可搭配网络记录器 -IR 来做到更进一步的监视与管制)

2.不使用『自动储存密码』来当作实时通讯软件平时登入的方式

因为无法确定公司计算机一定不会遭他人所使用，若是员工使用实时通讯软件中的『自动储存密码』来当作平时登入方式，就容易让有心人事藉此发送病毒、木马或其它有害程序至其它联络人计算机中，甚至假冒其身份来传送公司或个人的重要文件及内容。

3.不随意传递公司信息、文件或其他软件

若使用者任意传递与分享公司文件，很容易发生泄密疑虑，而使用者若是透过实时通讯软件于公司传递非法软件，还可能会因此而触犯法律同时也影响到公司商誉。

4.不明的文件别任意接收

即使是认识的人所传送的文件，也要在询问确认之后才进行收取的动作，因为当下并无法得知对方是否是在被植入有害程序的情况所发送出的文件，若任意接收来路不明的文件，使用者计算机可能会因此也感染病毒或被植入有害程序，除了危害到自身计算机，还可能会经由通讯软件管道来散布至公司内其它使用者计算机造成更严重的损害，甚至是因有害程序而让使用者计算机里的公司重要信息外泄。

(利用多功能 UTM 虽可做到文件传递与接收的限制以及病毒的防护，但若能搭配员工的良好使用习惯，才可以更有效的提升公司网络质量)

5.定期更改使用者登入密码

定期更改使用者登入密码，可有效降低被有心人士破解的情况发生。

只要作好适当的防护设定并搭配完善的管理政策，便可让公司有个安全、稳定的通讯环境，特别是现今以速度决胜的商场上，善用实时通讯软件还能够协助公司追求更多更大的商机。

文 陈殿鸿 kim@nusoft.com.tw

市场营销报导 - 新软多功能 UTM『联合防御系统』协助网管人员快速找出企业内部资安危机源

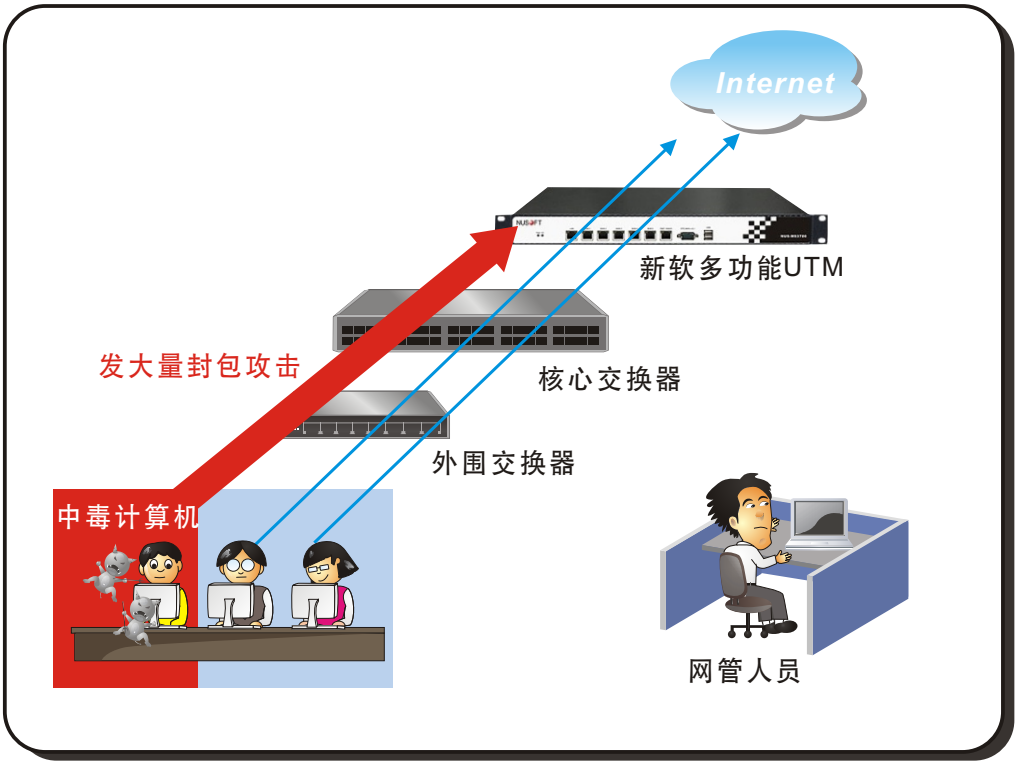
网络科技随着时间增长而快速进步，并为人类带来大幅度的文明进化，就连现代的公司企业也得依靠网络 e 化藉此提升企业本身的竞争力进而创造更高的企业营收。然而企业 e 化虽然能使企业获取更高的利润，但是这在黑客眼中将是他们『赚钱』好机会，因此许多网络黑客相继研究出令企业闻风丧胆的计算机病毒进而在网络上散播，想藉此赚取他们所想要的金钱利益。因此危害企业信息财产安全的计算机病毒问题一直存在于各大企业中且令许多企业十分头痛；所以企业本身的信息安全必然得做到最好、最完善，才能安安全全的保护企业信息财产。

因为如此许多企业便斥资采购相关防火墙设备，想藉此安全保护自家企业信息安全。不过现在市场上许多防火墙设备仅单纯做到网络防护的功能，简单来说：只是单纯用来阻挡外部网络攻击的网络前端防护设备；但是现在计算机病毒攻击方式千变万化，只靠单纯的前端防护设备是不足以安全保护企业的。假使企业内部计算机的使用者误下载含有计算机病毒之文件的话，那么计算机病毒便是从内部扩散出来，此时该使用者的计算机便在不自觉的情况下『中毒』了。目前最常见的攻击方式便是采用发出大量封包 (阻断式攻击) 来瘫痪企业网络的手法，此时即便是装设有一般防火墙的企业遇到此状况的话，也是完全束手无策而任人宰割。

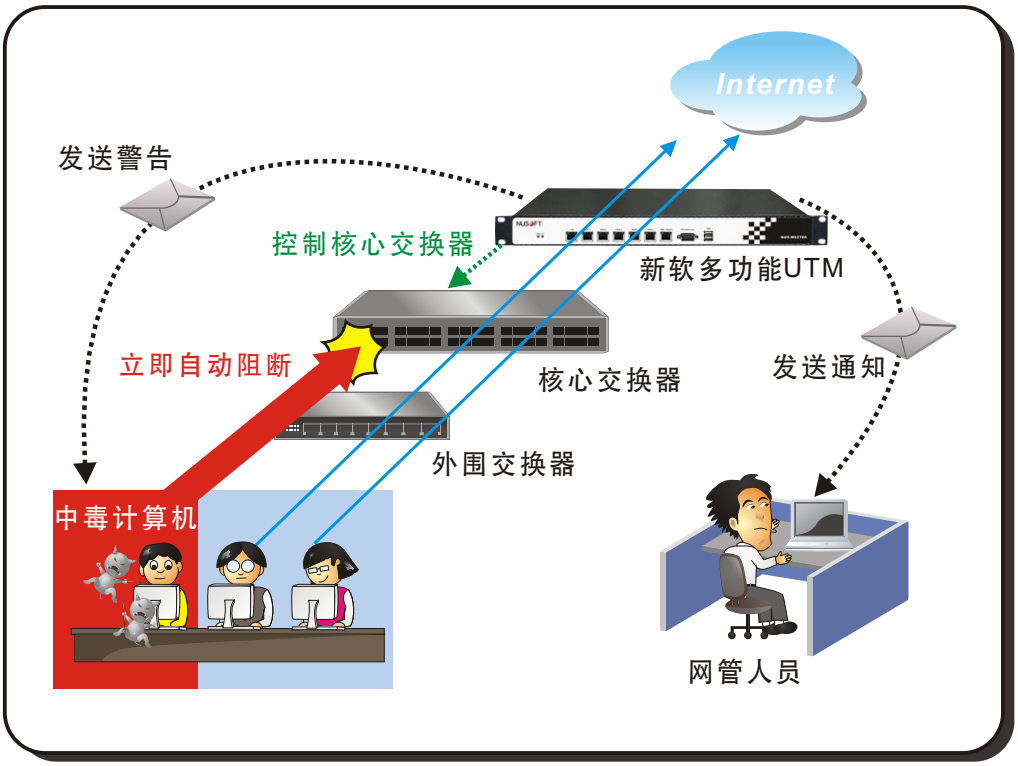
有鉴于此，新软系统在多功能 UTM 中建置『联合防御系统』此智能型防御机制，有别于其它市售产品，此功能着重于“内部安全防护”重点上，机制启动后将会主动检查网络架构内所有计算机之网络流量，假设发现内部有台计算机会不断发送大量封包企图攻击其它计算机藉此瘫痪企业网络，此时新软多功能 UTM 经过规则分析比对后，判断此部计算机为『中毒计算机』，便会依照规则控『核心交换器 (Core Switch)』立即阻断该计算机所传送的连接端口，接着发送通知给网管人员并发送警告予该计算机用户。如此一来，便可以在第一时间内防止该部计算机继续发送攻击，也可避免其它计算机遭到中毒计算机的病毒感染。

假设企业内部核心交换器 (Core Switch) 后端另接有周边交换器 (Edge Switch) 的话，为了避免该核心交换器 (Core Switch) 后端其它无辜没中毒的计算机用户遭到网络封锁，那么收到通知的网管人员可以依照『交换器 MAC 表』所显示的信息，快速找出核心交换器后端“哪个周边交换器在发送封包攻击？”，接着单独阻断此周边交换器并快速查出此周边交换器“哪个通讯端口后端的哪部计算机在发送攻击？”，藉此避免其它无辜计算机用户遭到无妄之灾而影响原本的工作进度。

新软系统多功能 UTM 产品设计理念不单单只是『网络前端防护设备』而是以『全面性企业网络安全防护设备』为主；即使遇到资安危机发生源位于企业网络内部的话，新软多功能 UTM 也能有效率地快速处理状况，以避免资安危机的扩散，让企业信息财产能获得更妥善的保护。



当企业内部有中毒计算机发动大量封包企图瘫痪企业网络时



新软多功能 UTM 会控制核心交换器阻挡发送攻击的通讯端口，
并发送通知给管理员和该计算机用户

文 黄政铭 ming@nusoft.com.tw