新软周报
HTTP WWW.NUSOFT.COM.TW
Internet Security Fighter
2009/8/10- 2009/8/23 第98期

多功能 UTM / MS 系列報導

技術淺談與應用 - 認證上網所需注意的事項

公司内部的网络资源，若被员工拿来做为私人用途，不但会占用到网络的带宽进而也会影响到公司的产能，因此有规画的网络运用对公司而言绝对是有必要的。

而新软系统所推出的『多功能 UTM-MS』系列产品，内建了"认证上网"之功能，让所有需使用网络资源的使用者都必须先通过认证才可使用，如此一来即可对公司内做初步的网络管理，同时也让不必使用网络资源之相关部门能有进一步的管制。但身为网络管理人员，在做该项认证的设定时，又该留意到哪些问题呢？

首先管理人员所需先了解到的是使用者计算机 DNS 设定情况为何？而 DNS 设定情况又可分为下列两种：

1. 使用者计算机中的DNS Server指向MS，由MS代为使用者PC去向外部的DNS Server做解析网域名称的动作。

2. 使用者计算机中的 DNS Server 指向外部，例如 HINET 的 DNS Server (168.95.1.1)。当使用此种设定时，则网络管理人员就必须要注意到 MS 中的管制条例设置。

因为 MS 上网的认证机制是利用 http 的 80 port 来做认证，但由于一般的使用者在上网时会习惯直接于网址列上输入 Domain Name (例如tw.yahoo.com)而非输入 IP 地址(例如：119.160.246.241)，因此，在输入 Domain Name 后还需要先藉由 DNS 的服务(53 port)来解析网域名称，才能够正常的经由 80 port (也就是 Http)来上网。因此当使用者为上述情况 1 时，则不必额外的考虑到上网做 DNS 解析时，是否会因为认证的限制，而无法正常的向外做解析的动作。但若为上述情况 2 时，则网络管理人员就得先确定管制条例中，是否有可供使用者能正确的连上 DNS 服务器做解析的条例存在。若是没有该项通过条例，就必须开一条让 DNS 通过的管制条例。

MS 的管制条例特性为「由上而下」、「逐条比对」，当比对到有符合的管制条例时，系统便会套用该条管制条例。而当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，在其认证的管制条例下方，需再设定一条阻挡的条例，用意为让比对的动作到此为止，不再继续向下做比对。

举例来说，如有一位使用者 Andrew 必须要经过认证才能上网，而其它人则不需认证的情况。那么于 MS 中 Policy 的设定如下：

Source	Destination	Service	Action	Option	Configure	Move
Inside_Any	Outside_Any	DNS	✓		Modify Remove Pause	To 1
Andrew	Outside_Any	ANY	✓		Modify Remove Pause	To 2
Andrew	Outside_Any	ANY	✗		Modify Remove Pause	To 3
Inside_Any	Outside_Any	ANY	✓		Modify Remove Pause	To 4

認證上網 Policy 設定範例圖

管制條例順序	來源	目的	服務	管制動作	用意
1	inside any	outside any	DNS	允許	置頂的用意為，先讓欲作 DNS 解析之封包能通過。
2	andrew	outside any	ANY	認證	來源為 Andrew 這位使用者，必須要通過認證才可使用網絡服務。
3	andrew	outside any	ANY	阻擋	因為使用認證的條例較特殊，故須在此多加一條條例做阻擋，讓來源為 Andrew 之使用者的封包不再繼續向下方其他管制條例做比對。
4	inside any	outside any	ANY	允許	讓其他非 Andrew 的使用者可以正常上網，同時不需經過認證。

Policy 設定說明表

另外还需要注意的是，当有使用外部 Proxy Server(代理服务器)的时候，其 Proxy Server 上网所用到的 port 号不一定会是 80 port，因此需通过认证才能上网的使用者，则须手动输入 IP 地址(82 port)来认证上网，使用者可在浏览器上输入「http://(MS 的 LAN Port IP):82/」进行认证。但IE在使用 Proxy Server 上网时，即使勾选了「近端网址不使用 Proxy」，IE 仍会无法正确分辨远程和近端，所以当打上「http://(MS 的 LAN Port IP):82/」时IE 会让 Proxy Server 向外部 Internet 查询该项 IP 地址，导致查无 IP 地址而无法认证。因此，解决方法，可使用 Firefox 浏览器，将「内部网段不使用代理服务器」的功能开启，便可顺利的经由认证来上网。

文 陳殷鴻 kim@nusoft.com.tw

市場營銷報導 - 新軟多功能 UTM 有效管制員工上網聊天

拜网络科技发达所赐，从早期 ICQ 乃至近几年的 Yahoo 实时通、MSN、Skype...等等，让人人于现今这个“全民E化”的时代里，至少有一个实时通账号，可用于朋友间交换讯息、工作时方便业务上之联系与传档交换等等...，不仅可建立快速便利的沟通桥梁，而且也比讲电话更能省下一笔费用开销。不过有些公司渐渐地发现员工经常利用上班时间使用 IM 从事私人行为，所以便开始加以管制，甚至直接禁止此类软件安装。但是道高一尺、魔高一丈，因此有些人动脑筋设计出「Web IM」这种不需要安装软件只要靠网页就能使用的实时通讯程序。

「提高员工产能、增益公司获利」为现代企业营运法则之一，因此企业为了使员工专心于自己的工作岗位上，无不积极采用相关管理设备。而目前市场上相关上网管制设备对于 IM 的管制方法大多采“防堵 Port 号”之简易方式来阻挡，可是如此之方式，仅能对不常易动 Port 号的 IM 或 Web IM 产生阻挡效果，倘若该程序后续所推出的新版本采用目前主流之“变动式 Port 号”机制的话，长时间下来自然是难以招架进而土崩瓦解，更别说管制变化性更大的「Web IM」。

拥有自家研发团队的新软系统，面对目前市场上不断推出新版本之 IM 或 Web IM 的挑战，皆以最严谨的态度、最缜密的心思来严阵以待。追求高效率的新软多功能 UTM 产品大大有别于一般市售设备仅以“防堵 Port 号”简易阻挡机制的方式，进而设计以新软独家阻挡机制将其阻挡：

＊关键词串特征比对

此机制为新软系统所独家研发，针对目前一些主流的 IM 或 Web IM 所特别设计。而且完全不受制于该程序所使用哪个特定的 Port 号，即使该 Port 号会不断地更换，新软多功能 UTM 的管制效果依然不减，只因为新软所采用的技术为在当传送的封包送至设备端时，会将封包比对新软独家建立的“关键词串特征数据库”，若有符合 IM 关键词串特征的封包，一律皆阻挡下来，其余的正常的封包将予以放行。如此一来，在新软多功能 UTM 网络架构底下，一般无予以授权使用 IM 实时通讯的员工，因为受到新软多功能 UTM 的管制便无法使用 IM 实时通讯软件，将能做到滴水不漏的管制机制。

有鉴于目前 Web IM 渐渐于网络上崭露头角，新软系统早在此之前便以独到的眼光发现问题之存在，并立即着力于开发此问题之解决方案。目前针对阻挡 Web IM 部分，新软系统所推出的多功能 UTM 采用上述新软独家技术已能成功管制大多数 Web IM 的使用。目前新软多功能 UTM 所能完整管制 Web IM 的网站如下：

MSN	people.live.com（官方網站）
	www.msn2go.com
	www6.messengerfx.com
Yahoo 實時通	webmessenger.yahoo.com (官方網站)
ICQ	icq2go (官方網站)
AIM	AIM Express (官方網站)
QQ	web.qq.com (官方網站)
All in 1 Web IM	iloveim.com (MSN、Yahoo 實時通、AIM)
	imo.im (MSN、Yahoo 實時通、ICQ、AIM)
	www.koolim.com (MSN、Yahoo 實時通、ICQ、AIM)
	www.meebo.com (MSN、Yahoo 實時通、ICQ、AIM)
	wablet.com (MSN、Yahoo 實時通、ICQ、AIM)
	www.ebuddy.com (MSN、Yahoo 實時通、ICQ、AIM)
	webuzz.im (MSN、Yahoo 實時通、AIM)
	www.imunitive.com (MSN、Yahoo 實時通、AIM)

然而人是会随着时间而变化的，网络科技更是如此，各家 IM 业者为了追求质量更好、更方便的聊天环境，势必会不断地推出新版本的 IM 实时通讯程序。而面对各家 IM 业者不停地推出之新版本 IM 的挑战，新软系统不畏网络世界潮流之变化，秉持着「兵来将挡、水来土淹」产品设研发理念，以坚强的技术研发团队为后盾，推出一系列相关对应程序供用户下载更新使用。

文 黃政銘 ming@nusoft.com.tw