

## 多功能 UTM / MS 系列报导

### 技术浅谈与应用 - 如何简单运用 SSL VPN

拜网络科技进步所赐，大部分企业皆将其各种业务放置于网络上，以增加企业竞争力。这些业务除了网站、电子邮件...企业常用之对外服务外，与子公司、海外/外地营运据点、驻外/外勤业务人员...之讯息沟通、文件传递也都常透过网络达到目的。而为了确保网络安全，这些讯息沟通、文件传递大多都是仰赖各种 VPN 联机作为桥梁，以确保企业机密不外泄。

由于各种 VPN 的特性不同，其适用之环境、场景亦有所差异；IPSec VPN 适用在“地点固定的公司间联机传输”、PPTP VPN 适用在“固定计算机的个人与公司之间的网络传输”...而相较于其它 VPN 联机，SSL VPN 的联机方式最为简单、易用、安全性高，而且可用在任何有提供网络联机的地点（家中、网吧、客户公司...），因此是最适合经常在外奔波的业务人员使用。

虽然说 SSL VPN 在使用上相当简单，很适合在外洽公之业务人员使用。但很可惜的是「相当简单」这形容词也只针对“有些了解计算机常识的人”而言，而一般「会用计算机」的业务人员顶多也只是会浏览网页、收发信件、使用实时通讯软件、编写文件...，超出这范围的计算机常识则一概不知。即使特地为此开班授课也是有听没有懂，想要他们了解 SSL VPN 如何使用变成一种奢求。因此，要如何让 SSL VPN 的操作变的更加简单上手，已成为让业务人员使用 SSL VPN 的首要条件。

其实这方法也不难，只要让 SSL VPN 的使用方式贴近使用者的计算机使用习惯，即可减轻其使用 SSL VPN 之困扰。需要注意的地方有三个：「如何让使用者记住 SSL VPN 的网址」、「如何让使用者记住 SSL VPN 的账号密码」、「如何让使用者记住所要联机之服务器的 IP 地址」。

#### 如何让使用者记住 SSL VPN 的网址？

新软 UTM 的 SSL VPN 联机网址是“<http://新软 UTM 之 IP/sslvpn>”，看起来很简单，但谁会去背这个 IP 啊！就算将「新软 UTM 之 IP」更改为企业的 Domain Name，时间一久使用者也很有可能把“/sslvpn”这一段字符串都忘的一乾二净。因此，让使用者记住 SSL VPN 的联机方式是件困难的事。那要如何让使用者轻松联机至 SSL VPN 的网址呢？

其实，要使用者记住 SSL VPN 之网址，还不如使用下列方式供其点选，省事又便利：



- 利用「快捷方式」记录 SSL VPN 之网址

SSL VPN 的网址以「快捷方式」方式提供给使用者，使用者只要点选该「快捷方式」，即可进入 SSL VPN 的登入网页。

- 利用我的最爱记录 SSL VPN 的网址

您在浏览网页时，是否会将常去的网站加入「我的最爱」呢？SSL VPN 的登入网页也可将它加入「我的最爱」中，使用者只要点选「我的最爱」，即可进入 SSL VPN 的登入网页中。

- 于企业网站，员工网页上刊载 SSL VPN 的连结网址

这方法可能有点麻烦，管理人员需要变更企业网站的设计，将 SSL VPN 的登入网址放到员工专用的网页中。使用者如有需要使用 SSL VPN，只要到此网页，点选该连结即可进入登入网页。

## 如何让使用者记住 SSL VPN 的帐号密码？

让使用者记住 SSL VPN 的账号密码可能是件最困难的事。根据统计，一个人通常需要记忆的账号密码有 6、7 组之多（MSN、网络银行、E-Mail...），而且为了安全考虑，这些密码又必须「长的奇形怪状」，如再加上一组 SSL VPN 的账号密码岂不是乱上加乱。因此，能把业务所会用到的账号密码加以整合，将会让使用者轻松许多。

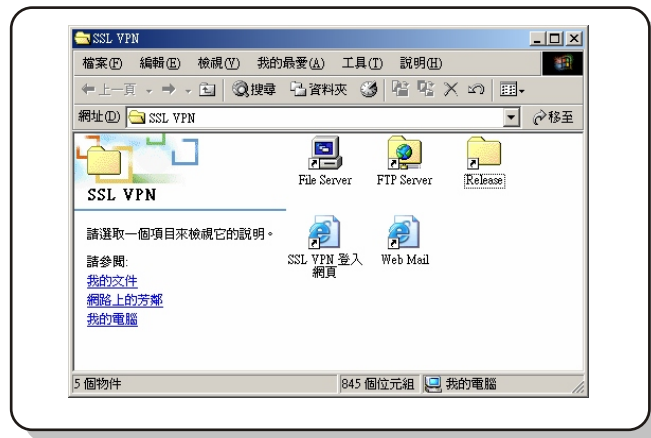
有鉴于此，新软系统产品中所内建的各种认证功能都有支持外部 RADIUS、LDAP、POP3 之机制，当然 SSL VPN 也不例外。管理人员可透过此机制，将业务所会用到的账号密码加以整合（E-Mail、SSL VPN、FTP...）。如此一来使用者只需要一组密码即可在企业网络中“趴趴走”。

## 如何让使用者记住所要联机之服务器的 IP 位址？

这是使用 SSL VPN 联机的最后一步，也是最重要的一步。倘若使用者 SSL VPN 成功联机，但不知如何进入各大服务器中（FTP Server、File Server...），岂不是前功尽弃？其实，可以套用先前提到的「快捷方式」、「我的最爱」、「员工网页」这三种方式让使用者直接用点选的方式联机至服务器：

### 1. 以「快捷方式」方式完成 SSL VPN 之联机

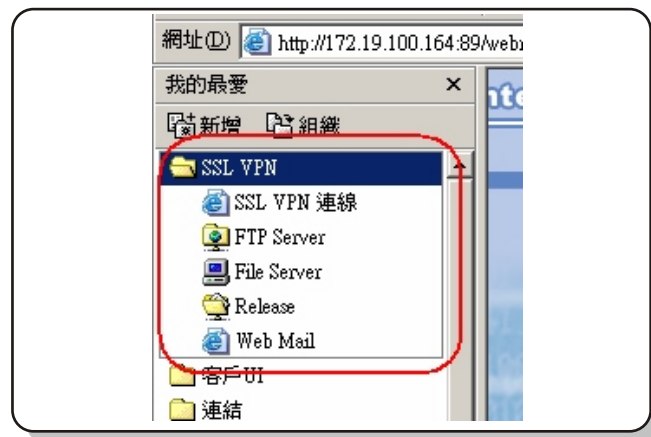
管理人员可将「SSL VPN 之登入网页快捷方式」、「各大服务器的联机快捷方式」存放在相同一个数据夹中，再发布给每一个使用者。使用者可将这数据夹放在桌面上或者是放在随身碟中随处携带，需要 SSL VPN 联机时点选其联机「快捷方式」即可。



图一 将 SSL VPN 相关之「快捷方式」存放在同一数据夹中

## 2. 采用「我的最爱」来联机 SSL VPN

管理人员可预先将「SSL VPN 之登入网址」、「各大服务器的联机 IP」加入至自己计算机的「我的最爱」中，再将它汇出。往后在教育使用者如何使用 SSL VPN 时，仅需帮使用者汇入先前所汇出的「我的最爱」文件于其计算机中，即可完成 SSL VPN 相关连接建置工作。往后使用者只要點選浏览器之「我的最爱」中的 SSL VPN 连结，即可完成 SSL VPN 联机之相关工作。



图二 利用「我的最爱」存放 SSL VPN 的相关连结


## 3. 使用者透过「员工网页」使用 SSL VPN

将「SSL VPN 登入网址」、「各大服务器的联机 IP」以超级链接的方式放在企业网站的员工网页中。使用者只要需要进入员工网页點選该超级链接，即可完成 SSL VPN 联机之相关工作。



图三 将 SSL VPN 的相关超链接至放於「员工网页」中

透过上面的文章可以知道其实使用 **SSL VPN** 的方法十分简单，要让使用者学会如何使用一点都不难。如要再更加省事，只要预先准备好相关设定文件，在教育员工时提供给使用者，其学习成果一定可以事半功倍。

文  程智伟 rayearth@nusoft.com.tw

## 市场行销报导 - 多功能UTM:有硬盘机种与无硬盘机种之差异

现今网络科技的发，虽带给企业无限商机，但也间接导致各种网络威胁的日益增多。在这企业网络安全备受威胁的时机，新软系统为企业研发了各种网络安全设备来替企业分忧，其中最为企业所瞩目的就是多功能 UTM (MS 系列产品)。其不仅整合了企业所需的各项网络安全防御机制，一次满足企业对于网络安全的所有需求。同时透过简单明了的管理接口，让管理者轻松完成设定，大大地减少管理者维护企业网络的工作量。

多功能 UTM 系列产品目前共有四个型号：NUS-MS3500、NUS-MS2800、NUS-MS1500G、NUS-MS700 可供企业选用。这四个型号最大差异在其效能方面（适用人数之差异），至于功能方面则虽大致相同，但也有部分差异。其中最显而易见的地方就是「有硬盘机种与无硬盘机种」之功能差别。

那到底有硬盘机种与无硬盘机种的差异何在呢？其主要的差别就在于：有硬盘机种多了「邮件通知 (Mail Notice)」与「隔离区」这两项功能。

	无硬盘机种 (NUS-MS700)	有硬盘机种 (NUS-MS1500G、NUS-MS2800 、NUS-MS3500)
提供邮件通知功能 (发送垃圾/病毒邮件通知信)	×	○
隔离区 (提供垃圾/病毒邮件保存、查询)	×	○

表一 有硬盘机种与无硬盘机种之主要功能差别

多功能 UTM 的内建硬盘最主要是作为「信件的隔离区」之用，凡是垃圾邮件、病毒邮件皆可隔离在「隔离区」中。倘若有信件被隔离至此，多功能 UTM 会主动发出「邮件通知」给收件者，告知使用者有哪些邮件因发现异常而被隔离。收件者亦可藉由此机制取回所需之邮件，完全不用麻烦管理人员。同时，储存于隔离区内的邮件，可依管理者的需求，来随时进行搜寻、查阅及取回的动作，方便管理者了解目前邮件安全系统运作情况。


至于在无硬盘机种方面，因没有内建硬盘作为「隔离区」之用，因此当电子邮件经多功能 UTM 判断为病毒或是垃圾邮件时，无法做到「隔离」这个动作；仅能对该邮件做「删除」、「传送给收件者」及「转寄邮件」之处置。在一般情况下，病毒邮件通常是直接「删除」没有任何问题，但是对垃圾邮件来说，却不是最好的选项。

要知道，现今再怎么厉害的邮件过滤机制，也无法百分之百完全正确判别所收到的邮件是否为垃圾邮件；如果是垃圾邮件判断错误还好，但正常邮件被误判为垃圾邮件而被删除，对于企业来说风险就相当高了，不可不慎。

那这些垃圾邮件该如何处置呢？难道就无法解决这难题了吗？其实，是有折衷方案的，对于无硬盘的 MS 系列产品，强烈建议垃圾邮件的处理方式是将这些信件，「转寄」至特定邮件信箱存放，往后只需要到这邮件信箱即可取回所需要的信件。

产品类别	邮件类别	直接删除邮件	转寄至特定邮件信箱	存放於隔离区
『有硬盘』之 MS 产品	垃圾邮件	✖	○	◎
	病毒邮件	○	○	◎
『无硬盘』之 MS 产品	垃圾邮件	✖	◎	—
	病毒邮件	○	◎	—
图形表示	○ 可以使用    ◎ 建议使用    ✖ 不建议使用    — 无此功能			

表二 有硬盘、无硬盘新软 MS 产品之垃圾／病毒邮件处置方式

文  黄赞中 isaac@nusoft.com.tw