

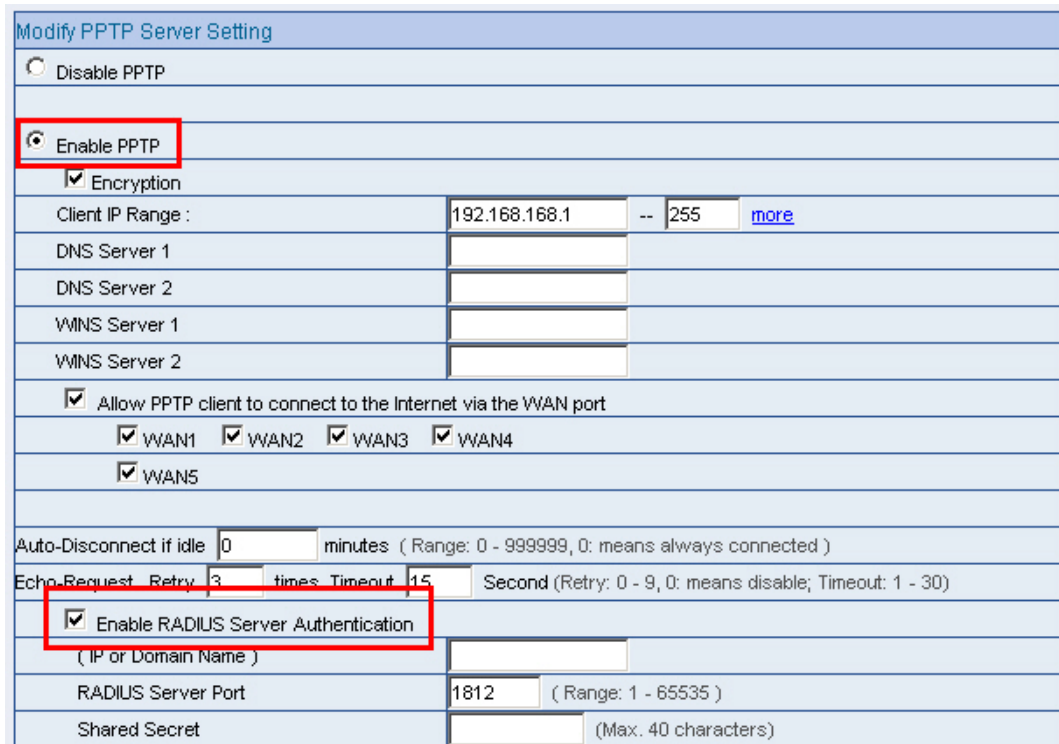
多功能 UTM / MS 系列报导

技术浅谈与应用 - PPTP 如需使用 Windows2003 的 RADIUS , WINDOWS 需要有些设置

RADIUS (Remote Access Dial In User Service) 主要用来提供 Authentication 机制, 用来辨认使用者的身份与密码, 确认通过之后, 经由 Authorization 授权使用者登入网域使用相关资源。

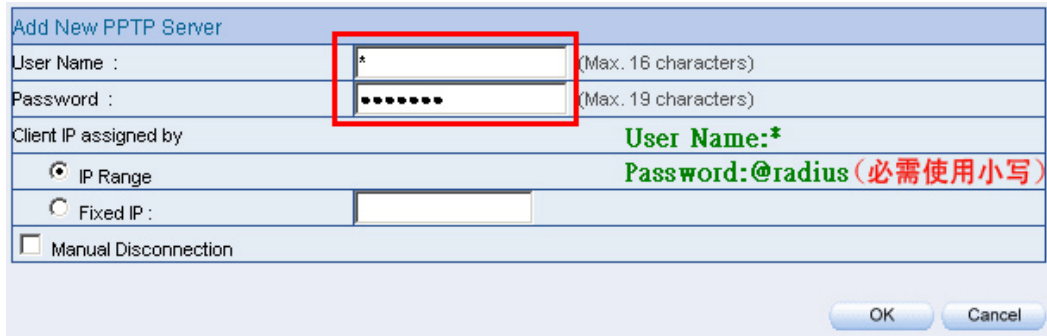
而新软系统所推出的 MS 系统产品中也同样的支持 RADIUS Server Authentication 功能, 但对于使用 PPTP 时, 在 Windows2003 操作系统的 RADIUS 该如何设置才能正常的与新软系统产品中的 MS 来正常搭配使用呢?

首先必须于 MH、MS 设备系统中 Policy Object > VPN > PPTP Server 下开启『PPTP Server』、『RADIUS Server』两项设定。



Modify PPTP Server Setting	
<input type="radio"/>	Disable PPTP
<input checked="" type="radio"/>	Enable PPTP
<input checked="" type="checkbox"/>	Encryption
Client IP Range :	192.168.168.1 -- 255 more
DNS Server 1	
DNS Server 2	
WINS Server 1	
WINS Server 2	
<input checked="" type="checkbox"/>	Allow PPTP client to connect to the Internet via the WAN port
<input checked="" type="checkbox"/>	WAN1
<input checked="" type="checkbox"/>	WAN2
<input checked="" type="checkbox"/>	WAN3
<input checked="" type="checkbox"/>	WAN4
<input checked="" type="checkbox"/>	WAN5
Auto-Disconnect if idle	0 minutes (Range: 0 - 999999, 0: means always connected)
Echo Request Retry	3 times Timeout 15 Second (Retry: 0 - 9, 0: means disable; Timeout: 1 - 30)
<input checked="" type="checkbox"/>	Enable RADIUS Server Authentication
(IP or Domain Name)	
RADIUS Server Port	1812 (Range: 1 - 65535)
Shared Secret	(Max. 40 characters)

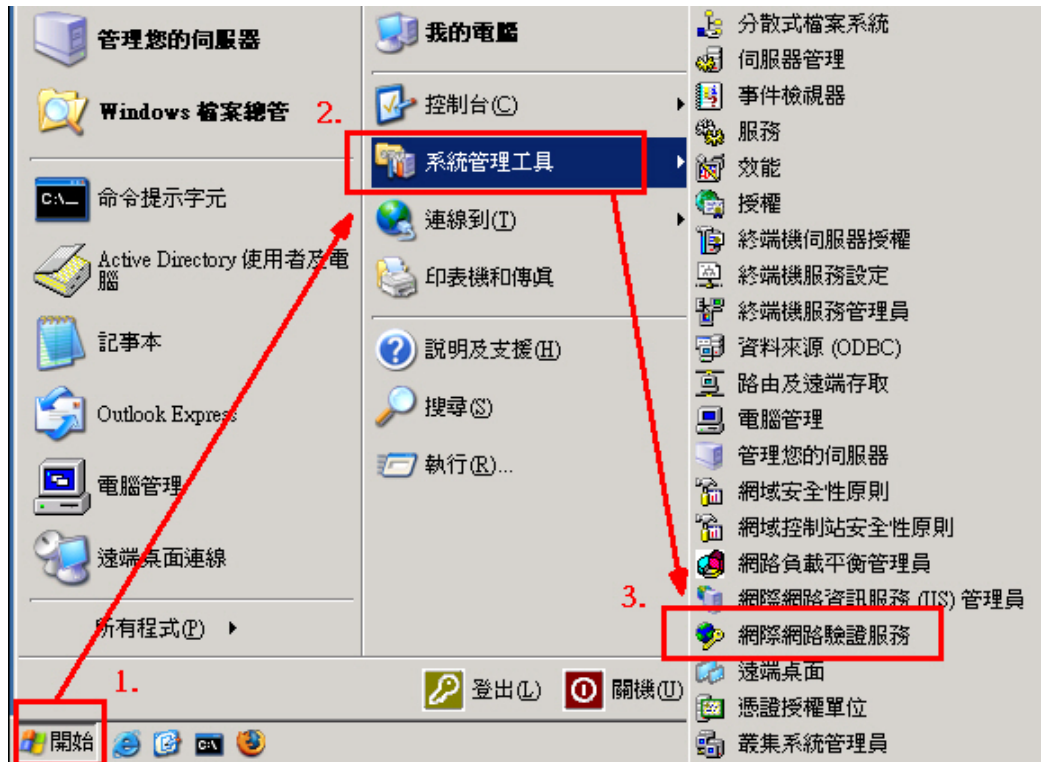
并且于 Add New PPTP Server 新增一组账号及密码，而账号为“*”，密码为“@radius”（特别注意密码部份必须使用小写），如此的设定其用意是让 PPTP Server 主动去问 RADIUS 上的账号与密码。



而于 Windows 2003 操作系统中，RADIUS Server 的相关设定方式与内容如下。

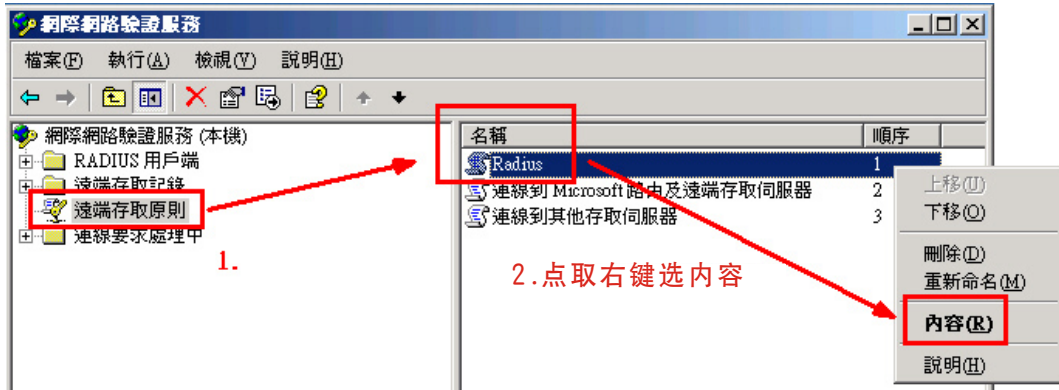
步骤一：

点取 Windows 2003 操作系统下的『开始菜单』，选择『系统管理工具』下的『因特网验证服务』



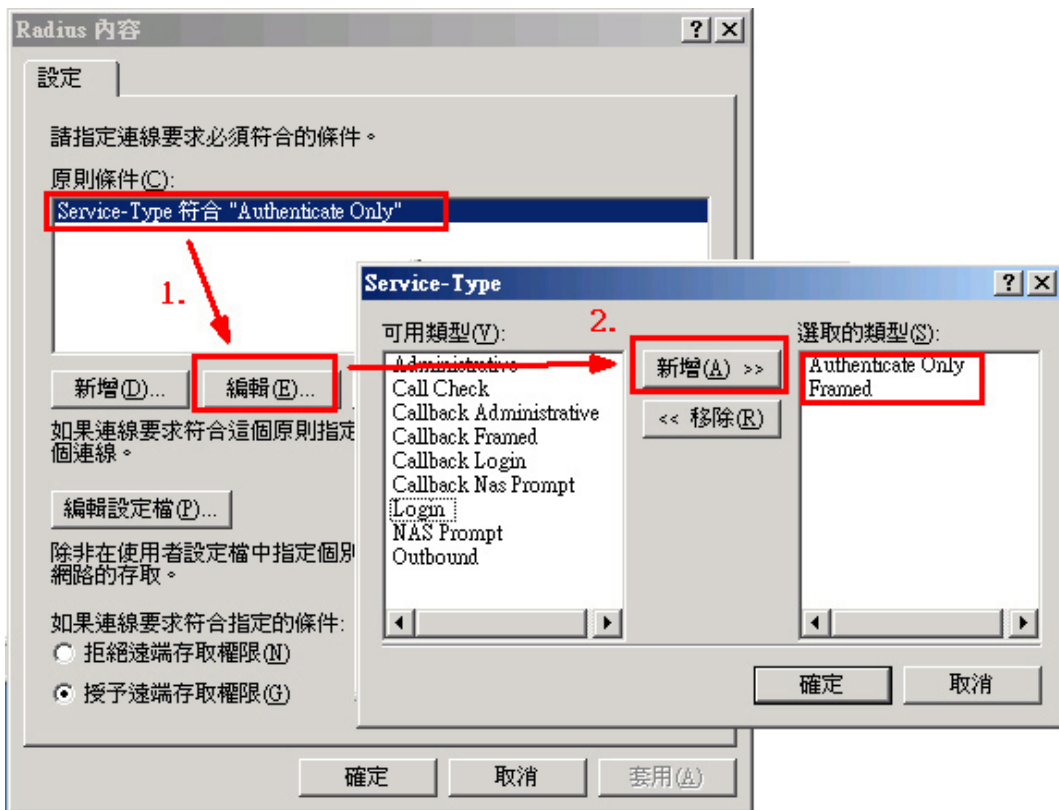
步骤二：

点取进入『因特网验证服务』后，选择底下的『远程访问原则』，并选择该公司所设定的 Radius 的名称，同时利用鼠标右键选取『内容』。



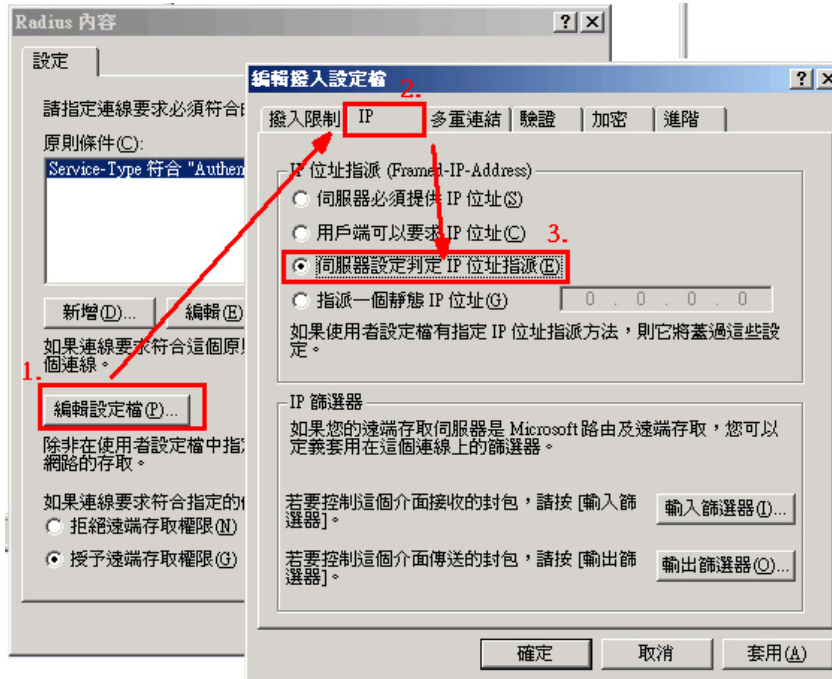
步骤三：

进入内容后，点取原则条件下的『Service-Type 符合 "Authenticate Only"』，并选择下方『编辑』。于编辑接口中将左方可用类型栏中点选『Authenticate Only』（此为 82 埠用）、『Framed』（此为 PPTP 用）并新增该选项。



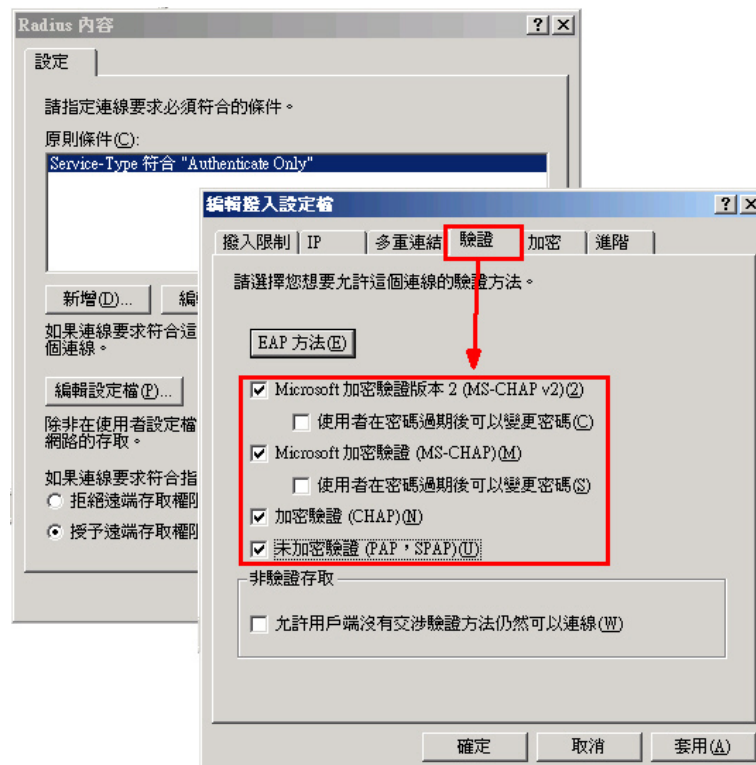
步骤四：

完成上述设定后，回到 Radius 内容接口，并点击下方的『编辑设定文件』选项进入。于编辑拨入设定文件接口中选择『IP』设定，将其设定内容中的『服务器设定判定 IP 地址指派』选择启用。



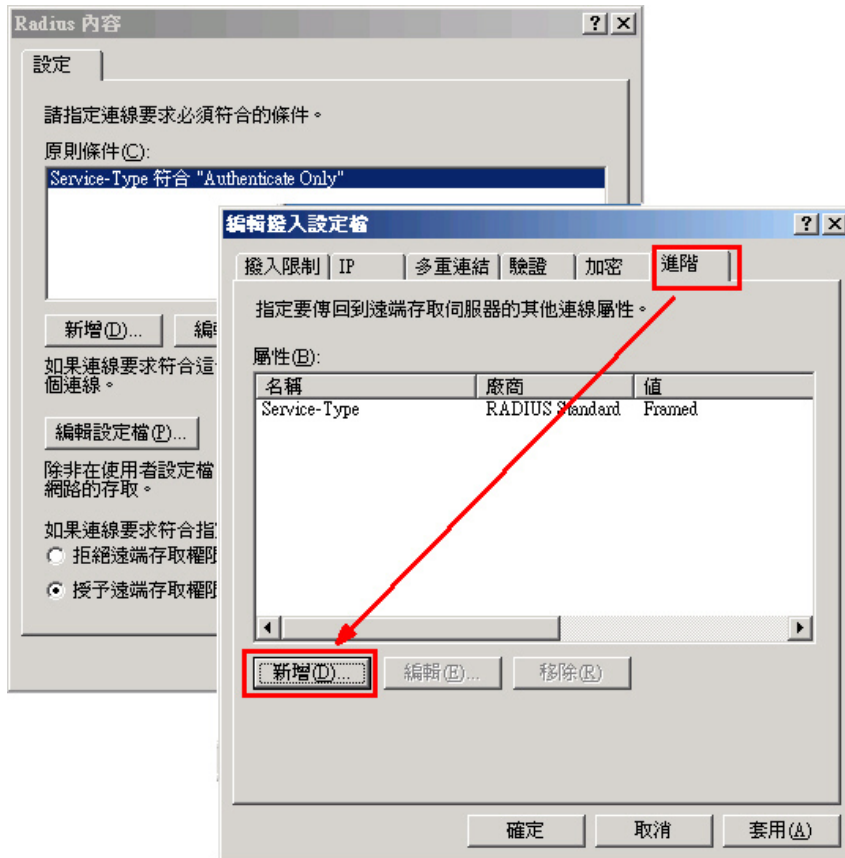
步骤五：

同样的于编辑拨入设定文件接口中选择『验证』设定，将其设定内容中的『Microsoft 加密验证版本 2 (MH-CHAP v2)』、『Microsoft 加密验证 (MH-CHAP)』、『加密验证 (CHAP)』、『未加密验证 (PAP、SPAP)』四项点取启用。



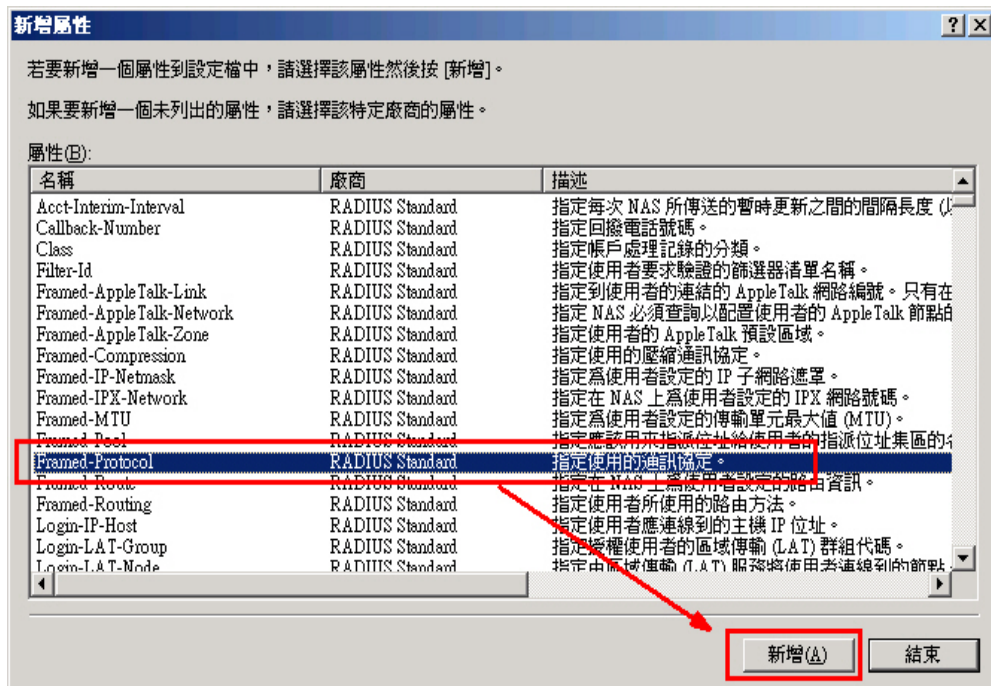
步骤六：

同样的于编辑拨入设定文件接口中选择『进阶』设定，并且于下方选择『新增』。



步骤七：

于新增属性内容中，新增『Framed-Protocol』。



步骤八：

并设定属性名称『Framed-Protocol』属性值为『PPP』。

可列舉的屬性資訊

屬性名稱:
Framed-Protocol

屬性編號:
7

屬性格式:
Enumerator

屬性值(A):
PPP

確定 取消

步骤九：

将另外的属性名称『Service-Type』，属性值设定为『Framed』。

可列舉的屬性資訊

屬性名稱:
Service-Type

屬性編號:
6

屬性格式:
Enumerator

屬性值(A):
Framed

確定 取消

步骤十：

重新启动 RADIUS Server，即可。

市场营销报导 - VPN 搭配管制条例，建立真正安全的传输管道

现代许多企业为了提高公司营运获利，因而积极拓展事业版图，于世界各地设立分公司，但是为了能让分公司保持对总公司重要讯息连络的实时性，所以得有一套适当的讯息联络方式，因此早期的企业采用电子邮件、实时通讯、FTP 之方式交换讯息，然而这样之传输方式，安全性实在令人不敢领教。所以后来又发展出以架设安全性较高的「专线」来应付如此之需求，但是向电信业者申请一条独立专线所需花费之费用，对企业来说是相当沉重的一项负担。


因此在经济又得实用之商业需求下，以「低成本」、「高安全性」著称的 VPN 技术逐渐导入于各公司企业内，其原理是将所欲传送之封包予以加密包装再送至目的地解密打开，如此之 VPN 技术比起以往赤裸裸的封包传送方式，以安全性来说是有过之而无不及，而且在成本上也不必依靠高成本所架设的独立专线来完成，就算是一般 ADSL 线路也可以轻松架构完成，因此这样的 VPN 技术在导入市场初期是相当盛行。

然而，所有科技都会不断地进步，如此方便之 VPN 技术，虽然可以将来源地封包安全无虞地送到目的地，但是相对的，过于密不通风且无适当过滤机制的传送架构也渐渐地产生一些问题。例如：来源地计算机已经中毒或是被安装木马程序，但是不自知，此时若使用 VPN 技术传送数据到目的地计算机，等于也将带有病毒和木马程序之数据加密保护传送至目的地计算机内，间接造成目的地计算机跟着中毒。这样一来，原本以高安全性著称的 VPN 技术，反而变成计算机与计算机之间互相传染计算机病毒、木马程序的最佳途径。

新软系统为了做到 VPN 技术“真正的高安全性”，将新软系统 MH/MS 产品与资安管理机制整合，在此以 MS 系列产品为例：当 VPN 在建构时，可以搭配管制条例来过滤 VPN，限定只有某些特定「使用者」能登入，并限定这些使用者能使用哪些特定「服务」（如：FTP、HTTP...等等），另外为了过滤病毒及木马，可再搭配「IDP」入侵防御侦测机制及「Anti-Virus」病毒过滤机制一起来使用。藉此，就可有效防范有心人士透过企业内部之间互相信赖的 VPN 通道来做相关违法的事情（如：窃取商业机密、非法存取相关资源...等等）。

	新软系统多功能 UTM (使用 VPN 时)	一般市售网关设备 (使用 VPN 时)
过滤病毒能力	优 可搭配「Anti-Virus」病毒过滤机制一起使用，在 VPN 中过滤病毒。	无 若来源端计算机所传送过来的数据中有夹带病毒，那麽目的端的计算机也将岌岌可危。
过滤木马能力	优 可搭配「IDP」入侵防御侦测机制一起使用，在 VPN 中阻挡木马程式。	无 若来源端计算机所传送过来的数据中有夹带木马程式，那麽目的端的计算机也将会处於後门大开，让有心人士为所欲为的状况。

图 新软多功能 UTM 与一般市售网关设备在 VPN 联机上的安全性比较表。

文  黄政铭 ming@nusoft.com.tw

