新软周报
http://www.nusoft.com.tw
Internet Security Fighter
2011/5/1-2011/5/31 第127期

UTM / UTM系列报导

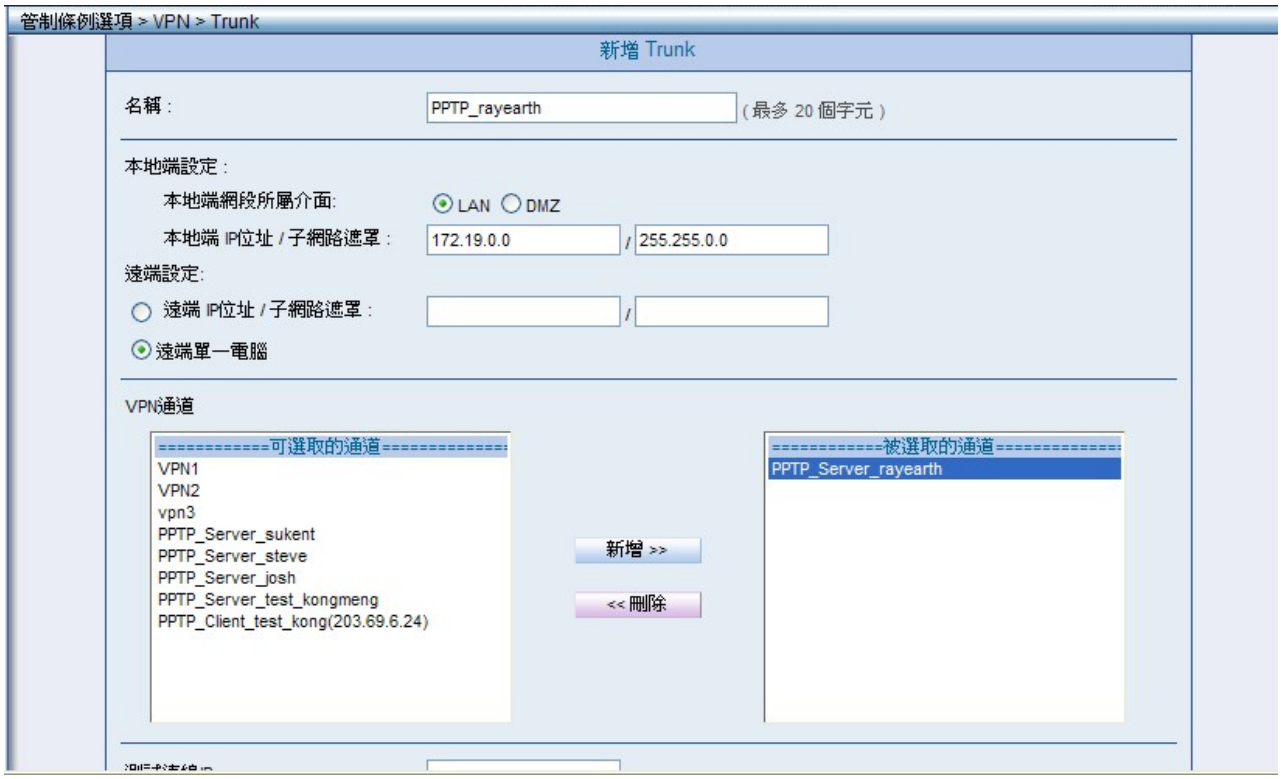
技术浅谈与应用 - 如何用智能型手机联机至公司内部网络

随着企业化与网络发展之演变，有越来越多在外奔波的商业人士、业务人员及行动通讯使用者，希望能随时在任何地方处理企业内部状况。以便能及时完成主管所交待的工作事项或立即响应客户之需求。但是，以往在外的管理人员，主要是透过笔记型计算机处理 工作项目；然而，就像你在外地的旅游景点休假，也会发生没有随身携带笔电，却接到公司内部突发状况，需要你处理。此时，必须放下手边的行程，赶回饭店的房间开启计算机上线解决。所幸，有了智能型手机这样的行动装置，在外的管理人员可以随时随地拿出口袋里的手机联机至公司，完成各项需要实时进行的工作。

由于智能型手机的风行，有许多企业IT厂商也把脑筋动到这个平台上(大致以iSO及Android平台为主)，推出不少该平台专用的应用程序，应用性质包括VPN远程联机、设备的远程登入等。其中，VPN远程联机为最热门的整合运用。因此，新软系统UTM/MHG系列之中“VPN”功能，提供建立安全与私密的网络通讯服务，并让管理人员透过智能型手机连至公司网络，简单易懂的操作画面，让管理人员在设定轻松许多。

首先，管理人员于系统「管制条例选项→VPN→PPTP服务器」新增PPTP服务器，输入使用名称与密码即可。并且在「管制条例选项→VPN→Trunk」新增Trunk，输入名称、本地端设定、远程设定，且可选取的通道新增至被选取的通道。设定好后，套入管制条例，便可设定智能型手机上VPN，连至公司网络。因此，不论是管理人员、业务人员、外勤人员只要拥有一组账号密码，便可联机至公司内部网络，完成各项需要实时进行的工作。

图一



图一

以 Android 平台为主的智能型之 3G 手机为例：

1. 进入 VPN 设定画面(路径：【无线与网络】>【VPN 设定】)，中“新增 VPN 设定”。(图二，由步骤 1~ 步骤 3)

图二

2. 新增 VPN 后，选择“新增 PPTP VPN”，在 PPTP 设定上，输入“VPN 名称”、“VPN 服务器”、“DNS 网域”（服务器可输入 Domain 或服务器 IP），连至网络。此时需输入“账号”与“密码”，输入正确，状态呈显已联机。（图三，由步骤 1~步骤 8）

图三

以 iOS 平台为主的苹果 iPhone 之 3G 手机为例：

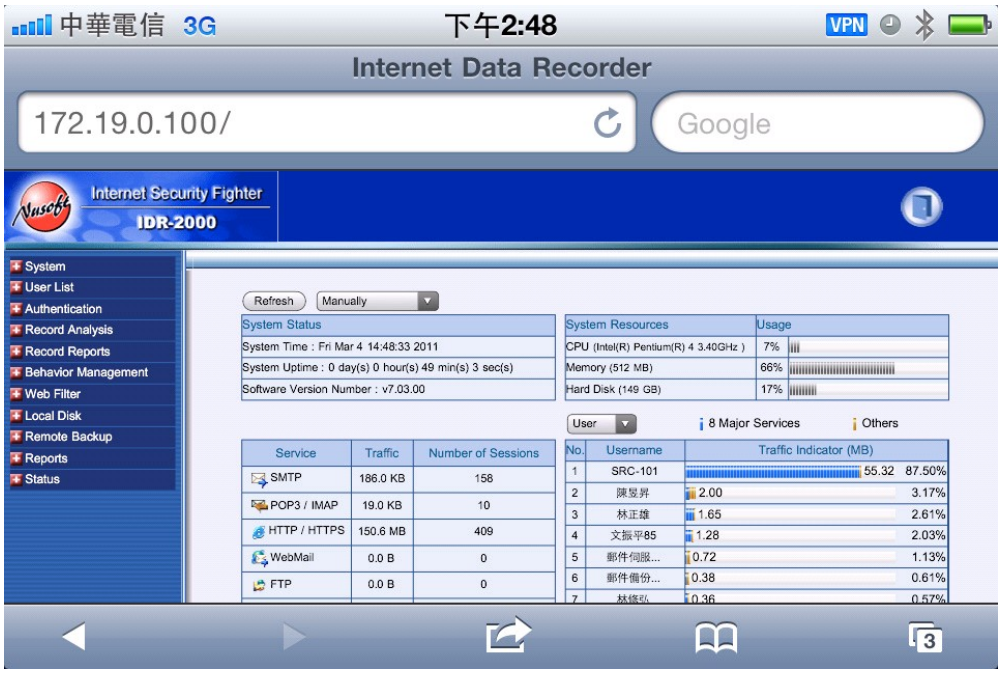
1. 进入 VPN 设定画面（路径：【设定】>【一般】>【网络】>【VPN】），新增 VPN 设定，选择 PPTP 选项。（图四，由步骤 1~ 步骤 2）

图四

2. 在 PPTP 设定上，输入“VPN 名称”、“服务器”、“账号”与“密码”（服务器可输入 Domain 或服务器 IP）。账号与密码输入正确，状态呈显已联机。（图五，由步骤 1~步骤 4）

图五

另外，VPN 联机成功后可直接联机设备的 Web 控制接口，可透过图形接口的 RDP、VNC 这类的远程控制软件直接操控 PC、或是透过网管 APP 管控公司内部服务器. . .（图六，联机设备的 Web 控制接口）



图六

文 余光明 kongmeng@nusoft.com.tw

市场营销报导 - UTM、MLS与MAF系列产品在于邮件安全防护功能的差异性

近几年电子邮件的普及带给人们许多便利，却也潜藏着许多陷阱与危机，因特网上到处充斥着垃圾邮件与病毒邮件的传播，不时有黑客利用电子邮件让企业成为转送垃圾邮件的跳板，进而对企业机密数据和业务管理造成相当的危害。因此，一个好的电子邮件安全防护就是需要面面俱到，不但要能够符合企业IT架构及稳定，并且同时兼具信息安全的议题。当然，在实务上能做到确实的电子邮件控管，才是最为重要的。

新软系统为了协助企业保护其电子邮件安全，一共推出了三款拥有邮件安全防护性质的产品—『MLS系列』、『MAF系列』、『UTM系列』供企业选择。『MLS』、『MAF』与『UTM』皆提供多重垃圾邮件过滤机制，与病毒邮件防护(内建ClamAV与Sophos双扫毒引擎)功能完美结合，可直接将垃圾、病毒邮件挡在企业网络之外。

同时导入『邮件稽核/归档』功能，来达到邮件管制的目的，以便提供主管稽核与邮件事后存盘调阅，作为全方位的邮件备份功能以及完整的左证需求。这些基本机制是MLS、MAF、UTM系列所共有的邮件安全防护。但是，三者功能不尽相同。因此，当客户有垃圾邮件过滤、病毒过滤、邮件稽核归档需求时，如何选择产品，须先了解MLS系列、MAF系列、UTM系列的差异性：

1. 产品类型之差异：

『MLS』－为Mail Server产品，内建完整Mail Server相关机制，需架设于企业内部网络中。

『MAF』－为Mail Gateway类型产品，架设于企业Mail Server前端，以协助企业之Mail Server稽核、归档信件与排除垃圾、病毒邮件侵扰。

『UTM』－为Gateway类型产品，架设于企业网络的最前端以保护企业网络。

2. 在“邮件安全(垃圾、病毒邮件过滤)”、“邮件稽核过滤”运作范围上的差异：

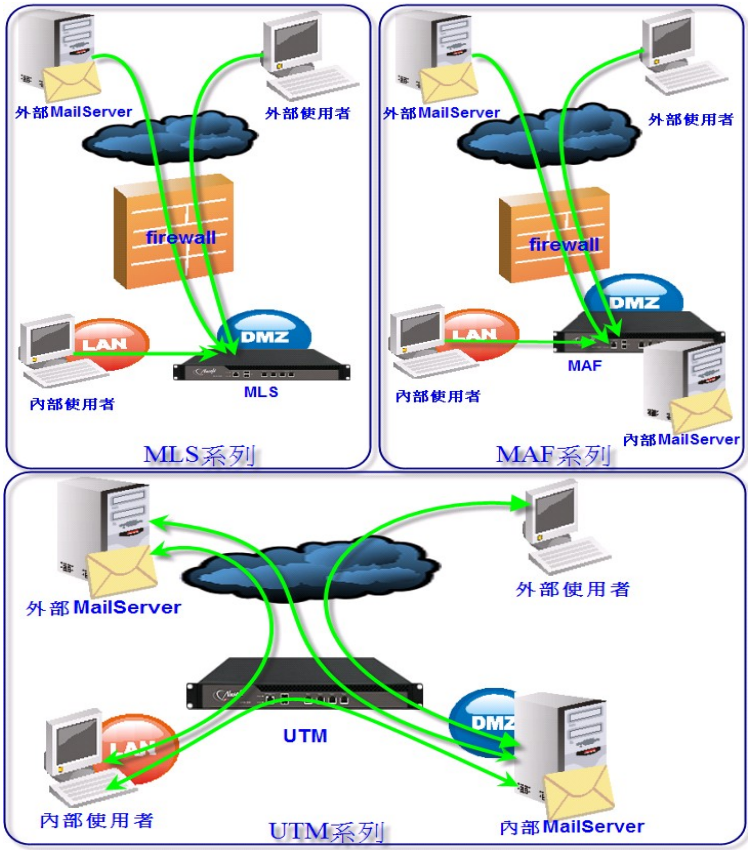
『MLS』、『MAF』－其邮件相关机制最主要是针对企业邮箱运作，企业往来信件皆可受到保护、管理与备份。

『UTM』－所有经过UTM之邮件(企业邮箱与外部邮箱)皆可受到保护、管理与备份。

3. 邮件备份的差异：

『MLS』、『MAF』－除了可主动备份企业往来之信件(企业邮箱)外，亦可以将信件额外备份至外部备份服务器(NAS、File Server. . .有提供网络芳邻机制的设备皆可）。

『UTM』－所有经过UTM之邮件(企业邮箱与外部邮箱)皆可备份。



注明：绿色代表邮件安全（垃圾、病毒邮件过滤）机制的方向

UTM、MAF、MLS 的垃圾及病毒邮件过滤图

新软系统产品	UTM	MAF	MLS
产品类型	Gateway	Mail Gateway	Mail Server
邮件安全、稽核、归档功能运作范围	所有往来信件（含企业邮箱、外部邮箱）	企业邮箱	企业邮箱
邮件归档	归档於设备内部	归档于设备内部 + 远程备份	归档于设备内部 + 远程备份
使用时机	欲保护整个企业网络	想要稽核、归档往来信件与排除垃圾、病毒邮件侵扰，却因故无法替换於邮件服务器。	欲替换邮件服务器。

表-UTM、MAF、MLS 在邮件安全（垃圾、病毒过滤）、邮件稽核归档的差异性

文 余光明 kongmeng@nusoft.com.tw