

第七章 中小企业安全路由器 VPN 配置

对于中小企业，VPN 相对于专线，在成本效益上的优点适合作为远程接入或是多个公司间联机的基础。企业信息化的风潮，包括 ERP、财务软件、CRM、CAD/CAM 的引入，更让不同的企业都感受到 VPN 的必要。对于略具规模的中小企业，利用现有的宽带接入，建置一个安全的远程或特定点之间的联机，显然很有必要。

VPN 极大地降低了用户的费用，而且提供了比传统方法更强的安全性和可靠性。但是对于初次接触的中小企业，或是有特殊需求的网管，仍时常发生有所不足的问题。下面就 Qno 侠诺接触中小企业的经验，针对不同问题，加以说明如下：

项目	问题	解决功能
1	有哪些 VPN 标准?该如何选择?各针对哪些问题解决?如何进行 VPN 规划?	IPSec、PPTP、SmartLink、SSL
2	行动用户如何进行配置?该使用哪一种客户端软件?	窗口操作系统、VPN 客户端软件
3	联机双方没有固定 IP 怎么办?如何设置动态 DDNS 功能?如何加强 DDNS 稳定性?是否有 DDNS 备援功能?	动态 DDNS 功能、DDNS 备援功能
4	多 WAN VPN 有哪些特性?如何简化外点的配置?是否能提供 VPN 备援功能?是否能于中央点一次完成所有点的监控?	SmartLink VPN 功能、中央控管功能
5	是否能解决跨网 VPN 不稳定问题?	策略路由
6	不同外点之间是否可以通联?在 VPN 上架设 VoIP 需要用到什么功能?	VPN Hub 功能
7	如何给予 VPN 封包较高的处理权限?如何确保 VPN 封包得到较多的带宽?	带宽管理

以下一一介绍相关功能

7. 1 IPSec、PPTP、SmartLink、SSL VPN 协定

选定适合的 VPN 协调是一个规划 VPN 网管会碰到的问题。以下先介绍一个可用于规划 VPN 所使用的流程

1. 依 VPN 应用及宽带接入决定总需要带宽，再决定总部线路及分支点线路，以及采用路由器 WAN 口数。
2. 如分支点散布在不同 ISP 区域，需作跨网 VPN 规划，总部需申请不同 ISP 线路。
3. 依应用需要决定 VPN 协议，常见的情况是混用不同的协议。网对网互联用 IPSec 或 SmartLink（侠诺科技特有的基于 IPSec 协议的简化的 VPN 连接方式）。简化管理可用 SmartLink。单一用户或行动用户可用 PPTP 或 IPSec，并决定适用 VPN 客户端软件。
4. 建立管理政策，列出优先保留带宽的应用，及需加以管理排除的应用。
5. 依需要 WAN 口及运算能力进行选型，决定总部及分支点产品。
6. 进行网络拓扑规划及各接入点功能规划
7. 加入网络安全及防护相关功能考虑

在以上的流程中，VPN 协议是一个需要决定的重大问题，必须根据远程访问的需求与目标而定。Qno 侠诺的 VPN 提供不同的协议，可应用于不同的情况，主要支持的协议包括 IPSec, PPTP, SmartLink, SSL。以下分别介绍：

1. IP_SECURITY 协议(IPSec):是互联网工程任务组(IETF)为 IP 安全推荐的一个协议。通过相应的通道技术，可实现 VPN、IPSec 有两种模式：通道模式和传输模式。IPSec 协议包括 ESP (Encapsulating Security Payload) 封装安全负载、AH (Authentication Header) 报头验证协议及 IKE 密钥管理协议等，可以用在公共 IP 网络上确保数据通信的可靠性和完整性，能够保障数据安全穿越公网而没有被侦听。它的特点是安全性极高，适用于点对点的 VPN 配置。Qno 侠诺科技 IPSec 通过国际 VPNC 认证，可以完成与其它 VPN 厂商的 VPN 设备相连接。

2. SSL 的英文全称是“Secure Sockets Layer”，中文名为“安全套接层协议层”，它是网景 (Netscape) 公司提出的基于 WEB 应用的安全协议。SSL 协议指定了一种在应用程序协议 (如 Http、Telenet、NMTP 和 FTP 等) 和 TCP/IP 协议之间提供数据安全性分层的机制，它为 TCP/IP 连接提供数据加密、服务器认证、消息完整性以及可选的客户认证。它的特点是

无需客户端软件，使用方便，适用于用户安装配置不易或是特定应用情况。

3. PPTP (Point to Point Tunneling Protocol) 点对点隧道协议:是一种支持多协议虚拟专用网络的协议。通过该协议，远程用户能够跨越 Microsoft Windows NT 工作站、Windows2000 和 Windows XP 操作系统以及其它点对点激活系统安全访问共同网络，并通过拨号本地互联网服务提供商安全链接它们互联网上的共同网络。优点也是简单易配置，对于初阶应用安全性足以因应。

4. SmartLink VPN 协议:这是 Qno 基于 IPSec 协议，所发展出特有 SmartLink VPN 功能，强调简易的配置及管理。Qno 侠诺 QVM 路由器的功能里通过设置确认联机后，路由器将大部份的设定参数交由 VPN 网关自动完成，只要进行简单的总部服务器 IP、用户名、及密码输入就能建立 IPSec 设定，也能轻易穿透不同的 IP 环境，建立方便、快捷的 VPN 连接。有着 PPTP 简易配置的优点，又有 IPSec 的高度安全性，适用于点对点的联机。

当前企业需要安全的点对点连接，或用单一装置进行远程访问，并且让企业拥有管理所有远程访问使用能力，应视使用的情况决定采用的技术为宜。IPSec 可以保护任何 IP 流量，而 SSL 专注于应用层流量。IPSec 适合长期的连接，即宽带、持续和网络层连接要求。SSL 仅适合于个别的，对应用层和资源的连接，而且支持的应用没有 IPSec 多。实现外出出差员工通过 PPTP 拨号或 VPN 软件连接等方式连接公司网络完成相关工作。

7. 2 行动用户 VPN 软件

对于在外的行动用户而言，除了 SSL 以外，往往都需要使用客户端软件才能建立 VPN。由于用户对配置了解程度不够，因此移动用户的客户端 VPN 软件，对网管造成相当的支持负担。Qno 侠诺 VPN 支持不同的客户端软件，包括常见的窗口操作系统的 IPSec/PPTP 客户端、TauVPN、Greenbow VPN、Symantec VPN、Fortinet、SoftRemote、SSH 都支持。

对于注重成本的用户，可以选择窗口操作系统内建的客户端软件或是免费的 CVP 客户端软件，例如 TauVPN 或是 SSH。其它的用户则可采用付费的商用软件，可得到对应的技术支持服务。

7. 3 动态 DDNS 功能

有了远程配置，中小企业的网管还面临另一个问题，就是一般企业用的 ADSL 线路使用的为动态 IP 地址。也就是 IP 地址是会变动的，今天和明天的 IP 不一定相同，这个小时和下个小时的 IP 也不一定相同。那网管要从家中，根本就找不到路由器了，要如何进行管理呢？还好，为了这个问题，市面上提供了动态域名的服务，用户的 IP 即使时时变动，也

能通过固定的域名，对应到特定的路由器，可解决以上的问题。用户可以登记例如 company.ddns.org.cn 的域名，就再也不用记 IP 地址了。

Qno 侠诺路由器支持动态域名服务，为了服务侠诺用户，也建置了动态域名系统，提供给最新产品的用户使用。用户可到 <http://www.qno.cn/ddns> 上进行登记，即可拥有 company.ddns.org.cn，可作远程登入，也可作为架设公共服务器使用。该服务未来也将在侠诺现有产品新的软件版本上使用。



图一：侠诺提供动态域名服务，部份产品型号用户只要键入电子邮件及产品序列号，即可申请免费的侠诺动态域名服务。

同时，现有 Qno 侠诺路由器也支持免费的 3322.org 动态域名服务，用户也可申请。一个 WAN 连络设定双重动态域名，可以起到动态域名备援的作用，进一步增加安全性。在路由器中，也必须在 " 进阶功能配置 " 菜单中的 " DDNS 动态域名解析服务中 "，进行相关的设定，依动态域名服务做对应的配置，才能开始运作。

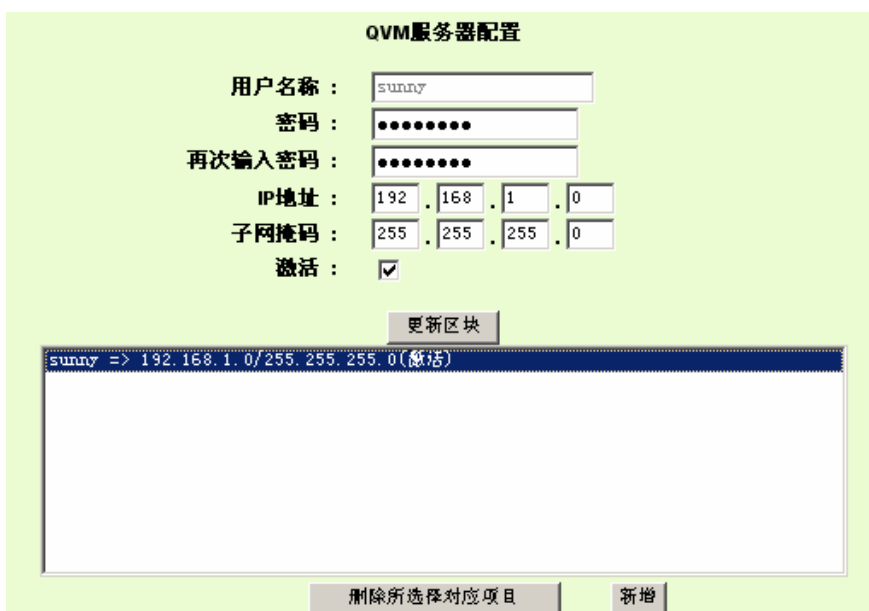
7. 4 SmartLink 快速配置

网管面临一个问题，就是外点不容易配置。例如一个公司在外部有十个分支点，因为一般的分支点往往没有具备网管能力的人员，因此 VPN 的配置就成问题。网管人要么需搭车到各地进行配置，要么就要利用电话，进行相关的配置。另外很多地方的 ISP 提供的 IP 地址都是虚拟 IP，对于一般的 VPN 配置会产生无法透通的困难。

QVM 系列路由器提供了方便配置的 SmartLink 功能，方便网管或集成商轻易的建置 VPN。另外它也支持不同网络的透通功能，减少以后 VPN 因 NAT 转换而无法建立，需要另

外配置的问题。SmartLink 配置的方法介绍如下：

- 1). 简单建立 VPN，解决了传统 VPN 建立复杂的缺点，只需用户名及密码就可以完成。
- 2). 用户在客户端上输入用户名以及密码，和服务端建立连接是通过 Qno 侠诺独有的 SmartLink IPsec VPN 的方式建立连接的。
- 3). 中央控管功能，让所有外点或分公司的 VPN 联机状态清楚且可直接在总部中心点中控画面，进入外点做设定。
- 4). VPN 断线备份机制，营运商掉线可从另一广域网端口重建，让 ISP 断线困扰造成外点或分公司资料无法对总公司传送问题顺利解决。



图二：QVM 服务端配置画面，简化的配置省去网管配置客户端的时间。

QVM 配置

激活 QVM 客户端功能

QVM用户名ID : sunny

密码 :

再次输入密码 :

QVM中心端IP地址或动态域名 : 172.17.17.102 中断

状态 : QVM隧道经由 广域网1 连线成功至 (172.17.17.102)

当QVM联机失败后,每 分钟自动重新拨接

QVM备援





图三：QVM 客户端配置画面，由原本二十多个参数减少到三个参数。

7. 5 QVM 中央控管功能

很多网管在进到办公室网络都需要一一登入到不同外点的 VPN 网关，以确定联机正常，这个工作占去了很多时间。以下这个功能可以简化这个工作：

中央控管功能让总部 VPN 服务器管理画面上可看到所有分点联机情形，无需一一作远程登入，一眼即可了解整体 VPN 网络运作情况。同时它可支持直接登入各分点进行配置，远程控管功能让网管免于奔波轻松管理，省时省费用。如图，我们可以点击远程用户“sunny”登录远程对路由器进行控制。

QVM服务器状态

No.	用户名称	状态	接口位置	启动时间	结束时间	持续时间	控制
1	suntao			---	---	---	请稍候
2	Sunny			---	---	---	请稍候

图四：中央控管的服务状态显示，一个画面即能显示多个点的 VPN 联机情况。

7. 6 VPN 备援

掉线是网管在管理 VPN 时另一个害怕的问题。当所有的业务都依赖 VPN 进行时，一旦掉线，所有的人都会找网管要求解决。传统的 VPN 支持单线，如果因为线路问题，完全无计可施。不过侠诺的多 WAN 路由器支持备援功能，可提供更进一步的稳定保证。

VPN 备援功能是采用 SmatLink VPN 连络时另一强大的功能。对于要求稳定的用户，它可增加 VPN 网络稳定性。输入 QVM 路由器中心端备援连接的 IP 或是网域名，一旦断线可从中心服务端路由器的另一个 WAN 端口自动建立 VPN 联机，确保 VPN 服务永不断线，保证数据传输的安全。

当QVM联机失败后,每 分钟自动重新拨接

QVM备援

中心端备援IP地址或动态域名2 :

中心端备援IP地址或动态域名3 :

中心端备援IP地址或动态域名4 :

图五：线路备援配置，可选择从不同条线路重新播入中心端。

7. 7 VPN Hub 功能

很多企业建置 VPN 是为了建置 VoIP，以达到较佳的通话质量，可是在建立之后才发现

只能建立各外点和中心点的 VoIP 连接，外点与外点之间无法通话。这是因为 IPSec VPN 是点对点互通的，并没有让各个外点互通，因此星状的 VPN 网络间，各外点间是不通的。VPN Hub 功能就是打通这个限制，让各外点间可以通过总部中心点互通的，这大大增加了数据分享及分散管理的方便性。

分点与总部连通后，可以让分点之间实现互联互通，不用再去各分点的设备之间建立通道，方便管理，更能节省资源。不同运营商电信网通线路可通过总部中央点进行转换，让联机速度不延迟，解决跨网 VPN 联机很卡的问题。同时还能结合侠诺专长的带宽管理功能，让总部的网管人员可以控制不同分支持点间的互相联机，达到更严密控管的功能。



图六：VPN 配置画面的 VPN Hub 功能只能配合 Qno 专有的 SmartLink VPN 使用。

7. 8 策略路由

有些企业由于经营的特性，在国内不同区域或国外都有分支办公室，都想经由 VPN 交流信息。但由于中国存在 "南电信北网通" 情况，位于南方的办公室往往采用电信线路，而位于北方的办公室则采用网通线路，因此总公司位于大都市，往往较有机会申请到二家运营商的线路。在采用单一线路时，若是总公司采用电信线路时，从网通线路建立 VPN 的办公室，会发生不稳定或 VPN 掉线情况；反之若总公司采用网通线路，则从电信建立 VPN 也会不稳定。若是采用多 WAN 路由器，总部可同时连接不同运营商线路，配合策略路由，指定不同运营商的分支办公室，各自自由对应的线路建立 VPN 通道，则可解决南电信北网通跨网瓶颈。

Qno 侠诺路由器中均配备有自动策略路由配置，内部建有不同 ISP 的网段进行判断，用

户只要启用即可。如果没有设定的范围，也可经由绑定协议或指定路由设定，或是手动键入方式达成。这样可解决企业面临的跨网 VPN 不稳定问题。

7. 9 VPN 及 QoS 带宽管理

对于上网人数较多又需要采用 VPN 的企业，网管往往希望能将 VPN 带宽及一般上网带宽分开，以免互相受到影响。多 WAN 路由器可支持多条线路，网管可将上网及 VPN 带宽分开，在这种情况下，VPN 应用不致受到上网用户，例如 BT 下载的影响，而 VPN 应用需要带宽时，也不会限制一般用户的上网。

对于 VPN 数据的传输是加密的，在传输过程以 GRE/ESP 的封包位于网络传输协议的网络层，如果我们需要对 VPN 的流量做 QoS 设定，比如保证 VPN 传输的质量，我们可以在 QoS 带宽管理将 GRE/ESP 的封包传输服务的优先级别调到最高级别来保证 VPN 联机的稳定畅通。



图七：ESP/GRE 封包传输优先级设定

小结

VPN 的配置，已成为成长型中小企业必备基础。如何在安全之外，还能作到方便，相信对于很多网管是很需要的。Qno 侠诺经由提供各种适用不同情况的功能，对于许多企业可以发挥到投入小效益大的效果。