Qno 俠诺远程联网 VPN 解决方案

● 背景介绍

互联网的高速发展加速了企业的信息化发展，企业利用 ERP 管理软件、CRM、财务软件、数据监控、影像监控、远程控制、远程打印、文文件共享、以及方便行动用户的连接、视频会议、VoIP VPN 应用，增加了企业在市场中竞争的砝码。利用网络来实现在供应商、客户、合作伙伴、员工等之间建立一个信息沟通的平台，就企业发展信息化道路是必不可少的一个配置。

但对于有不同的分支机构以及办事处，比如一家制造业公司总部可能在都市的繁华区，而工厂在城市的郊区，甚至根本和总部就不在同一个城市；还有一些买卖业，有自己的卖点以及连锁店分布在城市的不同角落或者分布在不同的城市；有的公司可能需要和自己的供应商、合作伙伴以及客户等需要建立网络联系的；一些政府机关机构等也存在地区间隔等问题。企业在构建自己的网络的时候，就必须得建立一个安全的远程连接，才能完善网络来满足我们相关的网络服务要求。

要建立远程联机，传统的方法会采用各大通信运营商建立专线，比如 DDN 线路。但是专线昂贵的费用会给企业带来一笔不菲的支出。最新的作法是透过互联网建立 VPN（Virtual Private Network），中文称为虚拟专用网络，进行连接，可以以比较经济的方式来建立远程连接。VPN 即是指在公众网络上所建立的企业网络，并且此企业网络拥有与专用网络相同的安全、管理及功能等特点，它替代了传统的拨号访问，利用互联网 公网资源作为企业专网的延续，可节省昂贵的长途费用。

VPN 乃是原有专线式企业专用广域网络的替代方案，VPN 在更为符合成本效益的基础上来达到原有广域网络特性。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。VPN 可分为三大应用：分别为直接远程访问（Remote Access）、Intranets 及 Extranets 。远程访问 VPN 乃是连接移动用户（Mobile User）及小型的分公司，通过电话拨号上网来存取企业网络资源。 Intranet VPN 是利用互联网来将固定地点的总公司及分公司加以连接，成为一个企业总体网络。而 Extranet VPN 则是将 Intranet VPN 的连接再扩展到企业的经营伙伴，如供货商及客户，以达到彼此信息共享的目的。

VPN 的建网应该遵循以下原则：开放性、扩展性、可靠性、标准化、安全性、实用性、易升级、易管理。我们可以通过这样的技术在预算控制条件下，达成单一的目的或功能来建立经济的远程连接，来提供完善优质的网络服务。

● 需求特性

本方案定义的远程联线，为用户需要透过 VPN 建立单一或特定功能的联机需求，例如 ERP 接入、视频会议、或财务软件接入。以下为一般用户利用 VPN 建立远程联机的需求：

- 很合理的控制预算，达到节省开支的目的；
- 保证远程连接通讯的稳定性；
- 带宽按照不同的需要进行选择（软件得视为 CS 或 BS 架构、监控则视传输数据）；
- 在建立 VPN 连接的同时保证内网连接互联网的稳定；
- 多点连接必须克服跨 ISP 通讯时，VPN 不易联机问题；
- 提供对内部网络的管理以及对远程的相关控制等；
- 需要考虑到架构简易性、灵活性以及数据传输的安全性；
- 考虑到今后的发展应该选择合适的可扩展的 VPN 连接；
- VPN 及宽带接入共享带宽，必须以 VPN 应用优先。

● VPN 联网规则要点

VPN 规划必须根据远程访问的需求与目标而定。目前主流 VPN 方案有：IPSec/IKE、SSL VPN、及移动用户运用比较多的 PPTP 协议。

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。通过相应的隧道技术，可实现 VPN，IPSec 有两种模式：隧道模式和传输模式。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。它的特是安全性极高。

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。

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、Windows© 95 和 Windows 98 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。

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。

Qno 俠诺科技发展的 QVM 系列路由产品支持国际标准协议 IPSec 和 PPTP 两种协议，通过了国际 VPNC 认证，可以完成与其它 VPN 厂商的 VPN 设备相连接。在此基础上，Qno 还提供了基于 IPSec 协议的 SmartLink VPN 功能，强调简易的配置及管理。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。

对于具体的需求我们列举以下程序供用户参考：

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（俠诺科技特有的基于 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. 进行网络拓朴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

● 组网方案及特性

对于企业或公司，有着不同的需要，根据这些不同的需要来选择不同的连接来到预期的目的，下面我们就 Qno 俠诺科技有限公司提供的几种不同的连接方案加以介绍供用户参考，用户可以结合自己网络的特点以及各种不同的需要来选择下例不同的方案来组建 VPN 远程网络。

Qno 俠诺 QVM (QoS VPN Management) 系列产品适用于注重分点与总部安全联机及有弹性多 WAN 宽带配置需求机构。内建强效 Intel IXP425 系列高效能网络处理器，是专为解决虚拟私有网络 VPN 配置及网络有效管理方便性所设计。结合提供带宽扩充/线路备援用多 WAN 端口、电信网通加速跨网用策略路由、带宽管理用 QoS 功能、防止内外部蠕虫/各种攻击/ARP 软件用强效防火墙功能、设置简易安全联机用 VPN 功能、动态域名解析服务 DDNS 功能以及提供系统日

志/威胁告警用的 Log 功能；一机多功、全方位的特色独步业界，更能符合企业对于高性价比、高整合度的产品需求，是您最优的企业网关选择。

图：全系列 QVM 系列路由器产品图

以下为 QVM 系列路由器一些相关重要参数表：

产品型号	QVM100 曜日	QVM330 皓月	QVM660 闳天	QVM1000 极光
CPU 处理器	网络专用处理器	Intel IXP425 266MHz RISC	Intel IXP425 533MHz RISC	Intel IXP425 533MHz RISC
Flash 快闪	8MB(64Mbit)	8MB(64Mbit)	16MB(128Mbit)	16MB(128Mbit)
DRAM 内存	32MB(256Mbit)	32MB(256Mbit)	64MB(512Mbit)	128MB(1024Mbit)
广域网 WAN 端口	2	2	2~4	2~8
可设定的 DMZ/WAN 端口	1 (WAN2/DMZ)	1 (W/DMZ)	-	-
局域网 LAN 端口	3	4	11~13	7~13
非军事区 DMZ 端口	1	1	1	1
联机数 Sessions	5,000	10,000	100,000	120,000
防火墙效能	双向转发 20-30Mbps	双向转发 100Mbps	双向转发 200Mbps	双向转发 200Mbps
VPN 效能	3DES/5Mbps	3DES/60Mbps	3DES/90Mbps	3DES/90Mbps
支持 IPSec 通道数	5	50	200	300
认证功能	MD5/SHA1	MD5/SHA1	MD5/SHA1	MD5/SHA1
加解密功能	DES/3DES/AES	DES/3DES/AES	DES/3DES/AES	DES/3DES/AES
IKE Key Management	●	●	●	●
VPN 透通	●	●	●	●
VPN 备援	●	●	●	●
VPN Hub	●	●	●	●
群组式 Group VPN	-	●	●	●
QVM 服务器(远程中央控管功能)	-	支持 5 个客户端	支持 30 个客户端	支持 50 个客户端
QVM 客户端	●	●	●	-
PPTP VPN 服务器	-	最多支持 10 个客户端	最多支持 50 个客户端	最多支持 100 个客户端

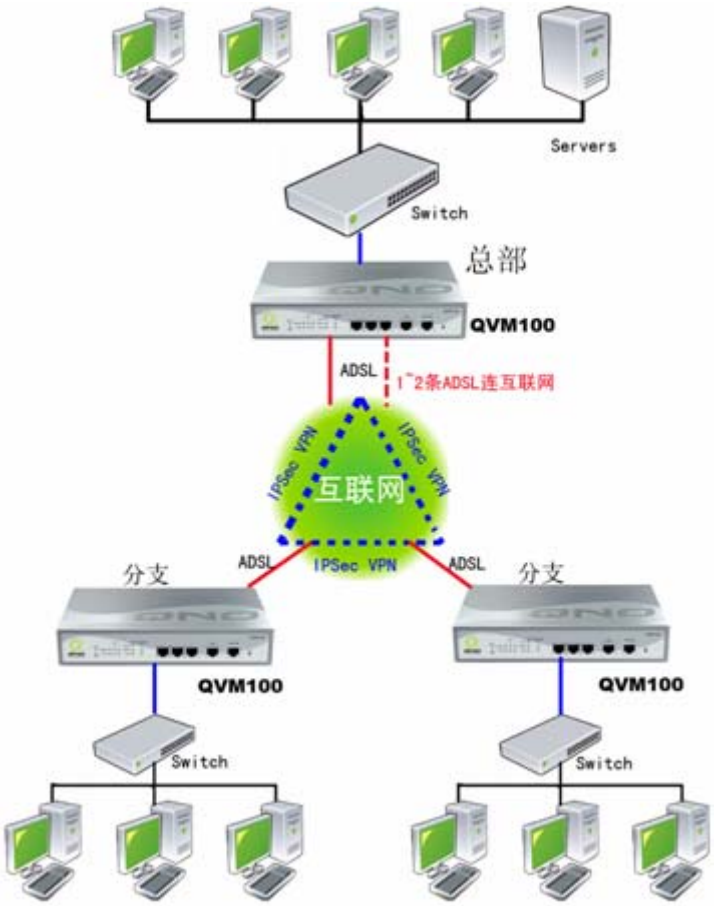
我们可以根据以上参数选择合适的路由器产品来建立 VPN 网络。

1、 经济型方案

对于一些小的企业、机构等，5 个点以下的要实现远程联网的客户，而且无需提供移动用户连接总部网络服务。我们可以采用 QVM100 建立经济型的 VPN 网络来满足要求：总部路由器与分支路由器来建立 IPSec 隧道；如果需要，其分支之间路由器也可以建立建立 IPSec 隧道，保证网络流量传输的畅通与安全。内部应用软件可为 CS 或 BS 架构、监控则视传输数据等，CS 架构

需要的带宽相对较大。就企业的需要，比如公司财务软件服务器、ERP 管理服务器、数据监控制服务器、打印服务器、文件共享服务器等连接总部路由器交换机下提供公司相关服务。带宽需要较大的点可以连接二条线路，以增加传输效率。

具体拓扑图如下。



图：QVM100 通过 ADSL 连接互联网，建立 IPSec 通道 VPN 连接，通过相关设置达到远程连接的目的。

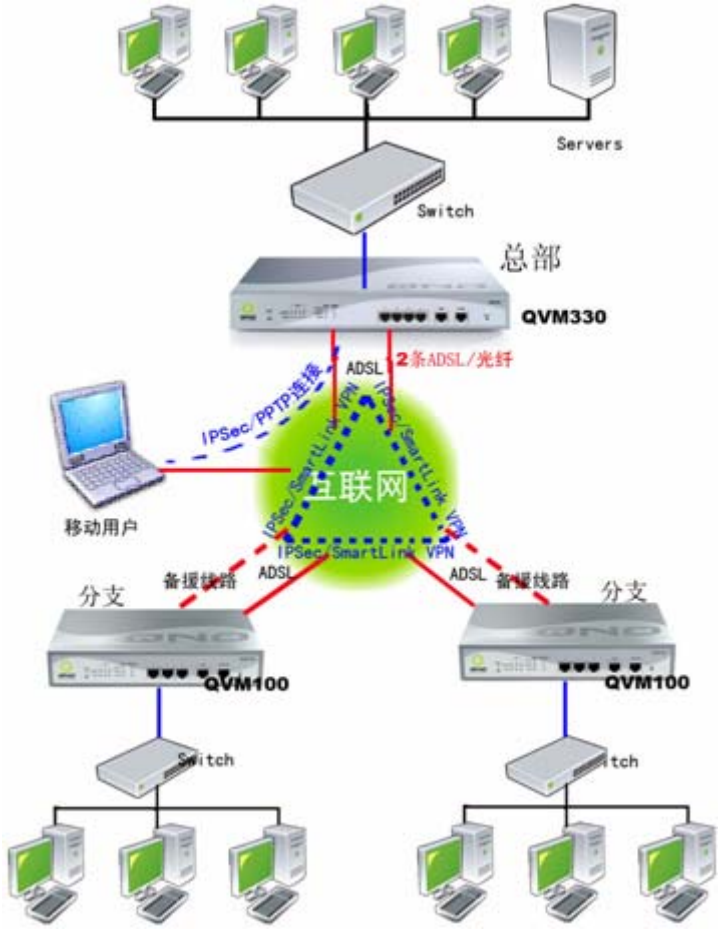
2、 入门级方案

有多个点需要实现远程联网的客户，而且有移动用户连接公司网络，在公司的发展上预留成长空间的用户，总部可以采用 QVM330、外点采用 QVM100 来建立经济型的 VPN 网络来满足要求。总部路由器与分支路由器来建立 IPSec 隧道，如果需要，其分支之间路由器也可以建立建立 IPSec 隧道，保证网络流量传输的畅通与安全。也可以采取 Qno 俠诺科技特有的 SmartLink VPN 技术来实现方便、快捷的 VPN 连接，对于公司移动用户可以采用 PPTP 拨号以及通过 IPSec 方

式连接公司网络。内部应用，软件得视为 CS 或 BS 架构、监控则视传输数据等。就企业的需要，比如公司财务软件服务器、ERP 管理服务器、数据监控制服务器、打印服务器、文件共享服务器等连接总部路由器交换机下提供公司相关服务。

本方案的用户也可由经济型方案升级，将总部路由器升级到 QVM300，原本的总部路由器 QVM100 移到任一分支点即可。

具体拓扑图如下。



图：QVM330 双线接运营商 ADSL/光纤，QVM100 通过 ADSL 接互联网，建立 IPSec/SmartLink 通道 VPN 连接，移动用户通过 IPSec/PPTP 连接公司网络，通过相关设置达到远程连接的目的。

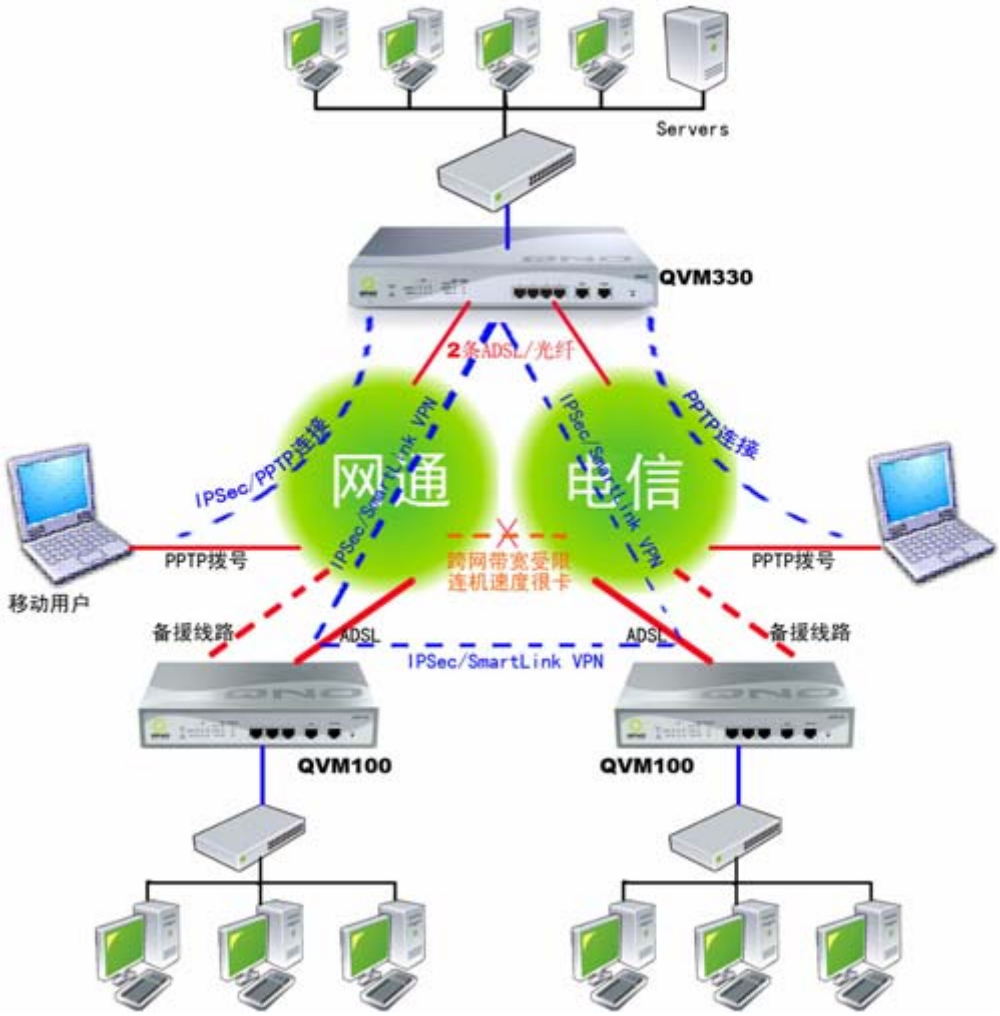
内部应用，软件得视为 CS 或 BS 架构、监控则视传输数据等决定对外的带宽需要，QVM330 性能足以因应一般小型企业的 VPN 联网需求。就企业的需要，比如公司财务软件服务器、ERP 管理服务器、数据监控制服务器、打印服务器、文件共享服务器等连接总部路由器交换机下提供公司相关服务。

基于以上要求的网络，但由有跨网要求的，分支机构有连接电信线路的也有连接网通线路的结构，这个时候就需要架设跨网 VPN 连接，对于 Qno 的 QVM 系列路由器而言，多 WAN 口的

设计相关技术正好可以解决这样的问题，QVM330 路由器有 2 个 WAN 口，总部配置 WAN1 端口对外数据封包使用电信线路；配置 WAN2 端口对外数据封包使用网通线路，依据分点线路运营商分别配置与总部的 VPN 联机，让电信走电信、网通走网通，确保联机反应快速，解决跨网通讯因带宽受限 VPN 联机很卡的问题。在此种架构中建议采取 Qno 俠诺科技特有的技术来实现方便、快捷的 VPN 连接，总部路由器与分支路由器来建立采用 SmartLink VPN 隧道或是 IPSec 隧道。

另外，对于公司移动用户可以采用 PPTP 拨号以及通过 IPSec 方式连接公司网络。

具体拓扑图如下。



图：QVM330 分别通过电信和网通 ADSL/光纤线路连接互联网，QVM100 通过 ADSL 连接互联网，建立 IPSec/SmartLink 通道 VPN 连接，移动用户通过 IPSec/PPTP 连接公司网络，解决跨网通讯因带宽受限 VPN 联机很卡等问题，通过相关设置达到远程连接的目的。

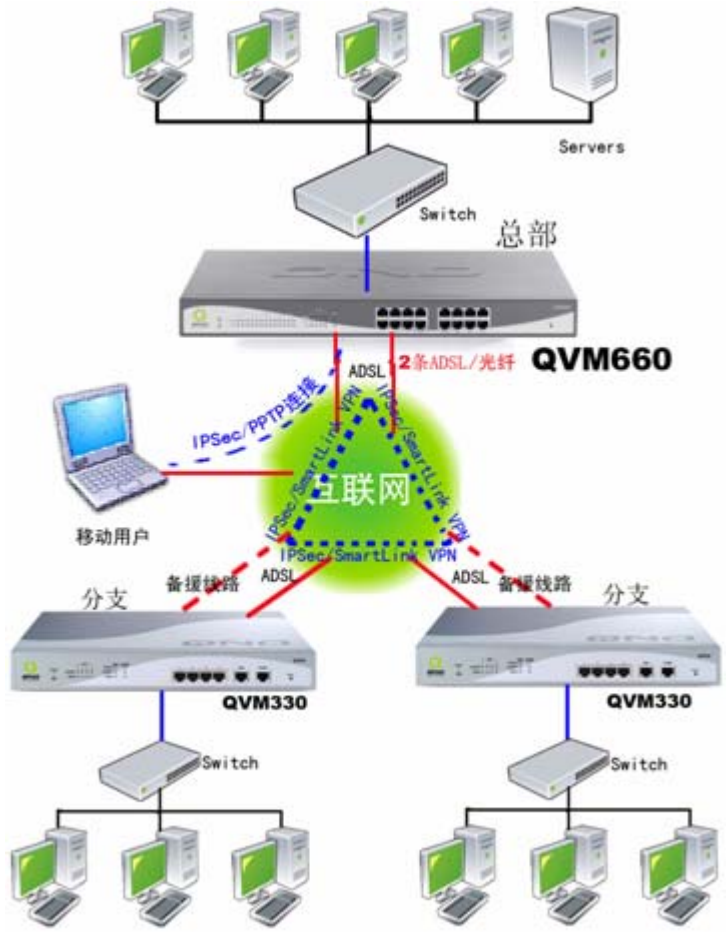
3、 大带宽连线 VPN 方案

对于多个点需要进行影像监控、视频会议等以及内网用户较多时，而且有移动用户连接公司网络，对带宽的要求比较大，公司的远程联网发展需预留成长空间的用户。这种客户，在总部可以采用 QVM660（最多 4 个 WAN 口，4 线接入个）、外点采用 QVM330 来建立经济型的 VPN 网络来满足要求，在分支机构规模很小的情况下外点也可以采用 QVM100 节约成本。

公司内部应用，得视软件为 CS 或 BS 架构、监控则视传输数据等，决定适当的带宽。QVM660 具有较高的性能及 VPN 处理能力，对于有大带宽联网要求的企业客户，可以较好的满足。就企业的需要，比如公司财务软件服务器、ERP 管理服务器、数据监控制服务器、打印服务器、文件共享服务器等连接总部路由器交换机下提供公司相关服务。

总部路由器与分支路由器来建立 IPSec 隧道，如果需要，其分支之间路由器也可以建立建立 IPSec 隧道，保证网络流量传输的畅通与安全。也可以采取 Qno 俠诺科技特有的 SmartLink VPN 技术来实现方便、快捷的 VPN 连接。移动用户可以采用 PPTP 拨号以及通过 IPSec 方式连接公司网络。

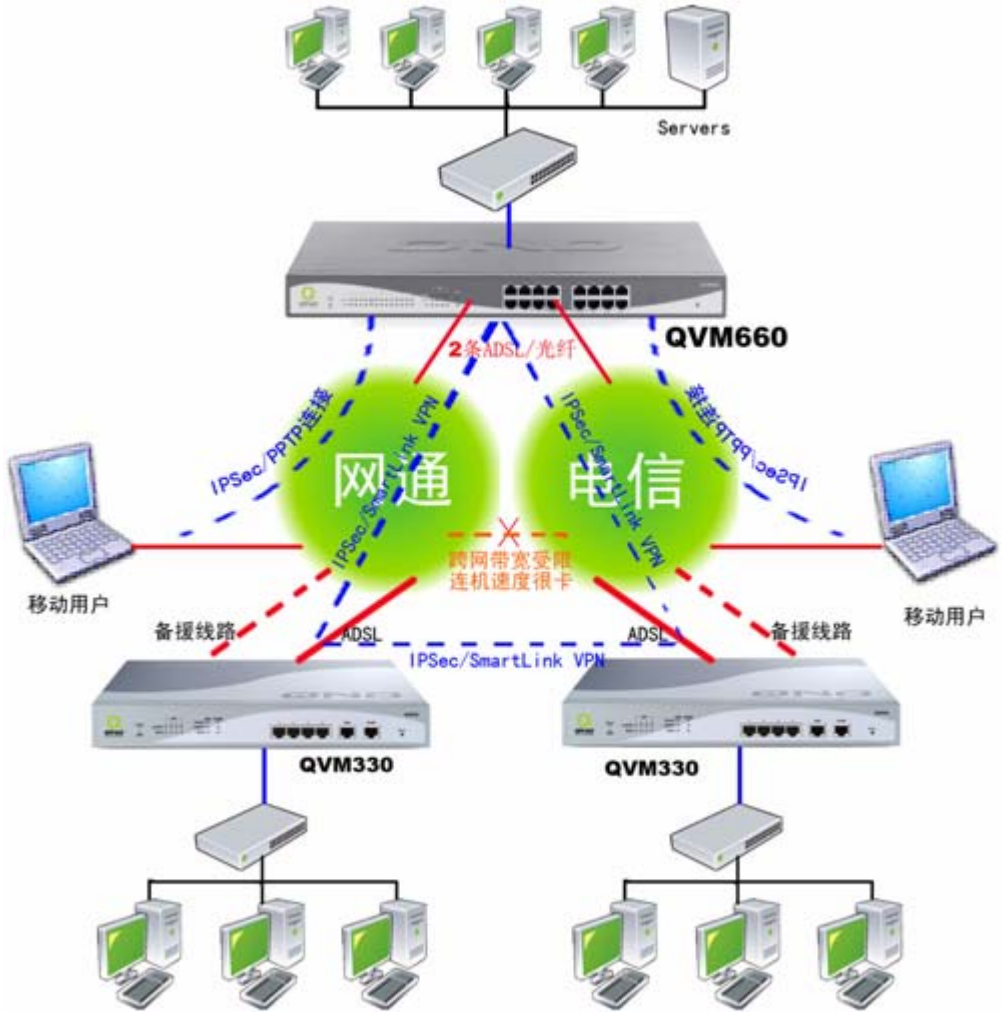
具体拓扑图如下。



图：QVM660 以及分支 QVM330 通过 ADSL/光纤连接互联网，建立 IPSec/SmartLink 通道 VPN 连接，移动用户通过 IPSec/PPTP 连接公司网络，通过相关设置达到远程连接的目的。

跨网 VPN 连接架设，对于 Qno 的 QVM 系列路由器而言，多 WAN 口的设计相关技术正好可以解决这样的问题，QVM660 路由器有 4 个 WAN 口，总部配置 WAN1 端口对外数据封包使用电信线路；配置 WAN2 端口对外数据封包使用网通线路（在运用 4 线接入的时候可采用 WAN1 和 WAN2 端口对外数据封包使用电信线路；配置 WAN3 和 WAN4 端口对外数据封包使用网通线路，具体情况可根据需要来选择），依据分点线路运营商分别配置与总部的 VPN 联机，让电信走电信、网通走网通，确保联机反应快速，解决跨网通讯因带宽受限 VPN 联机很卡的问题。在此种架构中建议采取 Qno 俠诺科技特有的技术来实现方便、快捷的 VPN 连接，总部路由器与分支路由器来建立采用 SmartLink VPN 隧道，如果需要，通过路由器的 VPN Hub 功能可以满足分支之间实现互通，同时也可以建立 IPSec 隧道，保证网络流量传输的畅通与安全。对于公司移动用户可以采用 PPTP 拨号以及通过 IPSec 方式连接公司网络。

具体拓扑图如下。



图：QVM660 分别通过电信和网通 ADSL/光纤线路连接互联网，QVM330 通过 ADSL 连接互联网，建立 IPSec/SmartLink 通道 VPN 连接，移动用户通过 IPSec/PPTP 连接公司网络，解决跨网通讯因带宽受限 VPN 联机很卡等问题，通过相关设置达到远程连接的目的。

4、 超大容量 VPN 联网方案

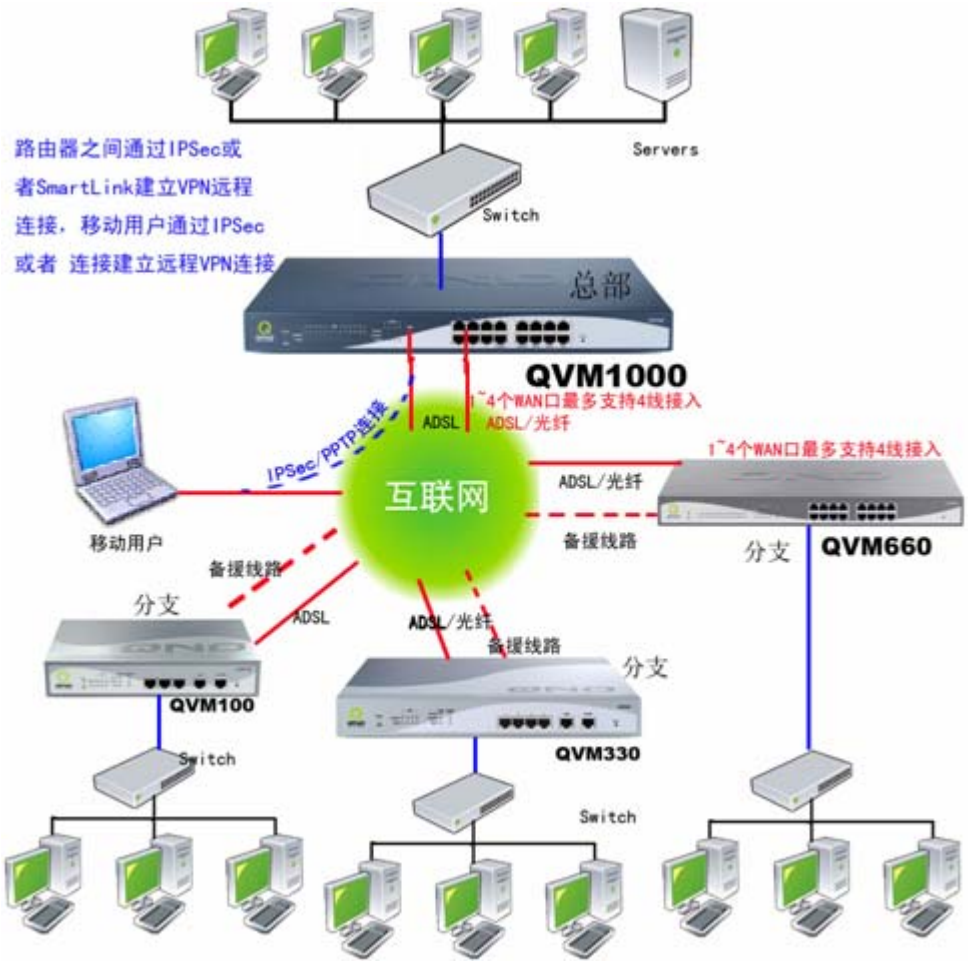
有大量连接点需要实现远程联网的客户，例如进行影像监控、视频会议等以及内网用户很多，而且有移动用户连接公司网络时，对带宽的要求很大。这时远程接入网络的发展上需预留成长空间，同时强调高稳定以及线路备援功能。对于这种用户，总部可以采用 QVM1000（VPN 模式下最多 4 个 WAN 口，4 线接入个）、外点依带宽需要采用 QVM660、QVM3300 或者 QVM100 来建立 VPN 网络来满足要求。

总部路由器与分支路由器来建立 IPSec 隧道，如果需要，其分支之间路由器也可以建立建立 IPSec 隧道，保证网络流量传输的畅通与安全。也可以采取 Qno 侠诺科技特有的 SmartLink VPN

技术来实现方便、快捷的 VPN 连接。

公司移动用户可以采用 PPTP 拨号以及通过 IPSec 方式连接公司网络。内部应用，则可支持软件为 CS 或 BS 架构、监控、传输数据等。

具体拓扑图如下。



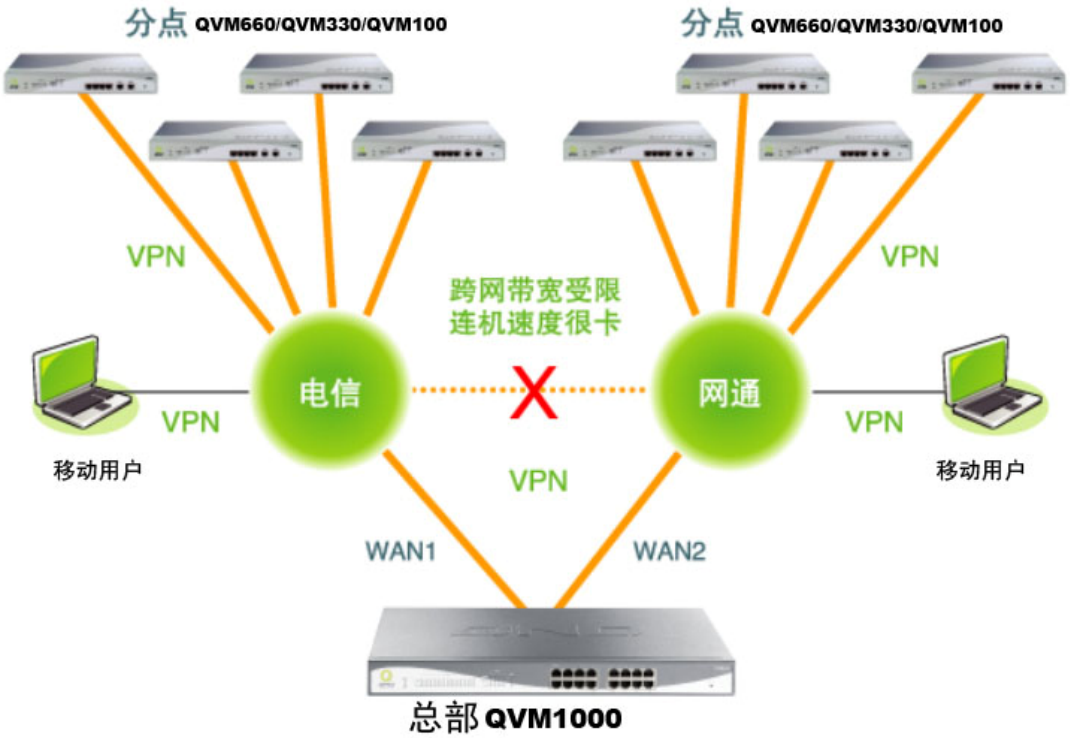
图：QVM1000 以及分支 QVM660/QVM330/QVM100 通过 ADSL/光纤连接互联网，建立 IPSec/SmartLink 通道 VPN 连接，移动用户通过 IPSec/PPTP 连接公司网络，通过相关设置达到远程连接的目的。

当分支机构有连接电信线路的也有连接网通线路的结构时，这个时候就需要架设跨网 VPN 连接。Qno 的 QVM 系列路由器而言，多 WAN 口的设计相关技术正好可以解决这样的问题，QVM1000 路由器有 4 个 WAN 口，总部配置 WAN1 端口对外数据封包使用电信线路；配置 WAN2 端口对外数据封包使用网通线路（在运用 4 线接入的时候可采用 WAN1 和 WAN2 端口对外数据封包使用电信线路；配置 WAN3 和 WAN4 端口对外数据封包使用网通线路，具体情况可根据需要来选择），依据分点线路运营商分别配置与总部的 VPN 联机，让电信走电信、网通走网通，确

保联机反应快速，解决跨网通讯因带宽受限 VPN 联机很卡的问题。

总部路由器与分支路由器也可采用 IPSec 隧道或 SmartLink VPN 隧道，如果需要，分支之间实现互通可通过路由器的 VPN Hub 功能可以满足。公司移动用户可以采用 PPTP 拨号以及通过 IPSec 方式连接公司网络。内部应用，可支持 CS 或 BS 架构、监控视频传输数据等软件。企业常见的的需要，比如公司财务软件服务器、ERP 管理服务器、数据监控制服务器、打印服务器、文件共享服务器等连接总部路由器交换机下提供公司相关服务。

具体拓扑图如下。



图：QVM1000 通过不同运营商多线连接互联网，分支 QVM660/QVM330/QVM100 以及移动用户通过不同运营商 ADSL/光纤连接互联网，与总部建立 VPN 连接，通过相关设置达到远程连接的目的。

● 其它 VPN 设置

1、 SmartLink 快速配置

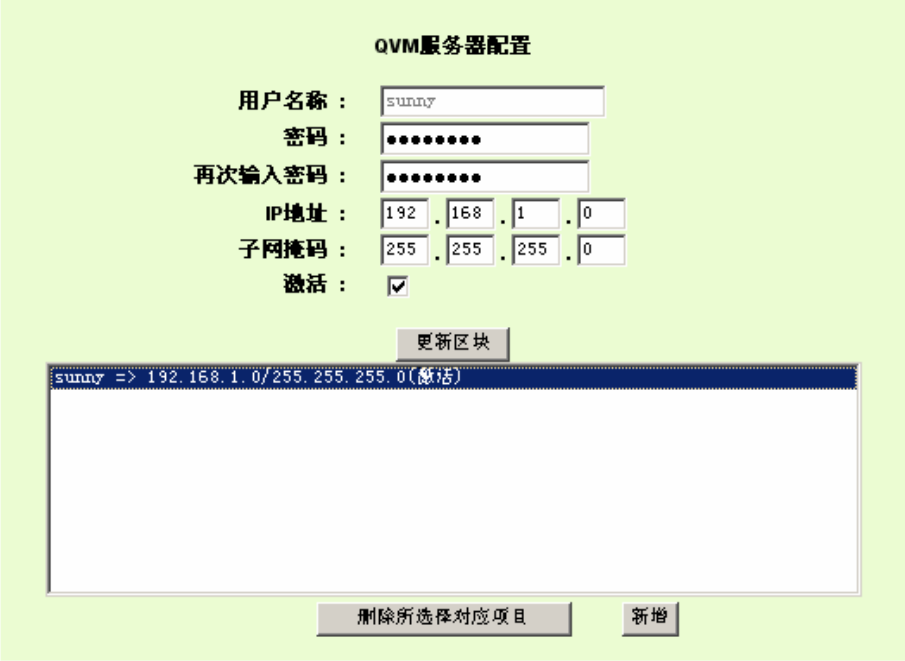
QVM 系列路由器提供了方便配置的 SmartLink 功能，方便网管或集成商轻易的建置 VPN。另外它也支持不同网络的透通功能，减少以后 VPN 因 NAT 转换而无法建立，需要另外配置的问题。SmartLink 配置的方法介绍如下：

1）.简单建立 VPN，取代传统 VPN 建立的复杂缺点，只需要用户名及密码就可以完成。

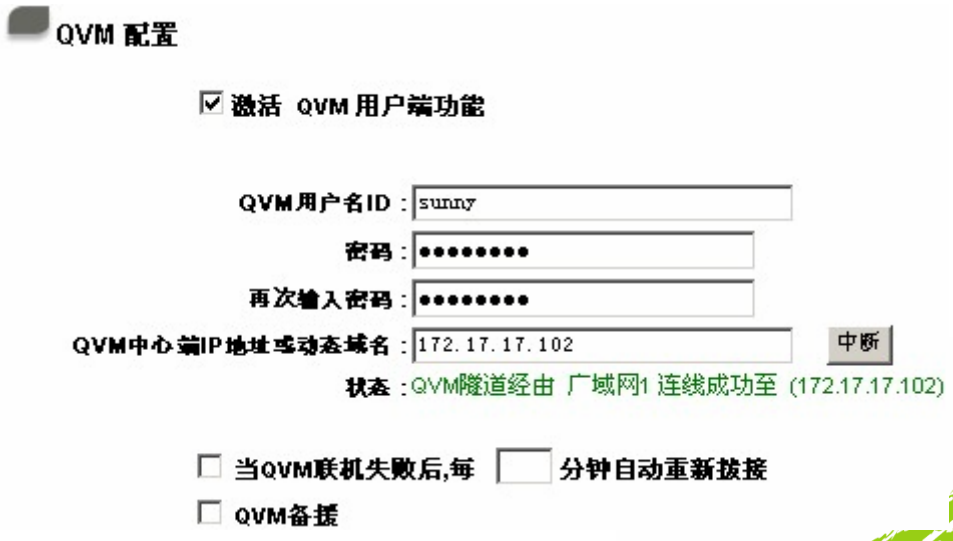
2）.在用户在客户端上输入用户名以及密码的和服务端建立连接是通过独 SmartLink IPSec VPN 的方式建立连接的。

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 QVM660 中控画面，进入外点如 QVM660/QVM330/ QVM100 做设定

4）.VPN 断线备份机制，营运商掉线可从另一广域网站口重建，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：QVM 服务端配置画面



图：QVM 客户端配置画面

2、 QVM 中央控管功能

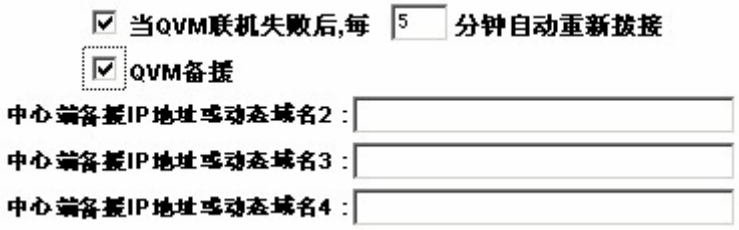
中央控管功能：总部 VPN 服务器管理画面上可看到所有分点联机情形，无需一一作远程登入，一眼即可了解整体 VPN 网络运作情况。同时它可支持直接登入各分点进行配置，远程控管功能让网管免于奔波轻松管理，省时省费用。如图，我们可以点击远程用户“sunny”登陆远程对路由器进行控制。

图：服务状态显示

3、 VPN 备援

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。

对输入 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。



图：线路备援配置

4、 VPN Hub 功能

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透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：VPN 配置画面

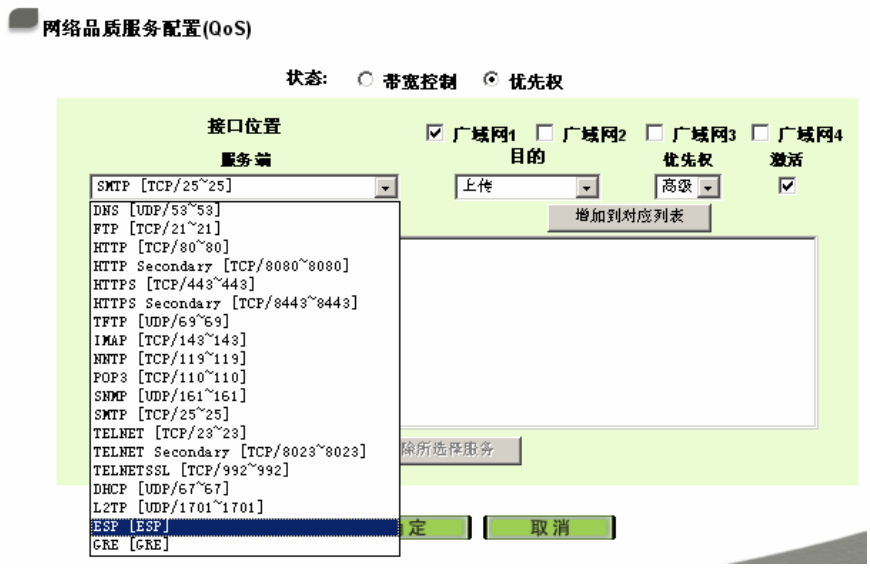
5、 VPN 线路扩充

QVM660 可以支持最多 4 个 WAN 口，最多 4 条线连接广域网络，而对于 QVM1000 而言，在接入模式下最大支持 8 个 WAN 口，（VPN 模式下最大支持 4 个 WAN 口）提供足够的线路扩充弹性。

图：QVM1000 做 VPN 连接最多支持 8WAN 口

6、 VPN 及 QoS 带宽管理

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 的封包传输服务的饿优先级别调到最高级别来保证 VPN 联机的稳定畅通。



图：ESP/GRE 封包传输优先级设定

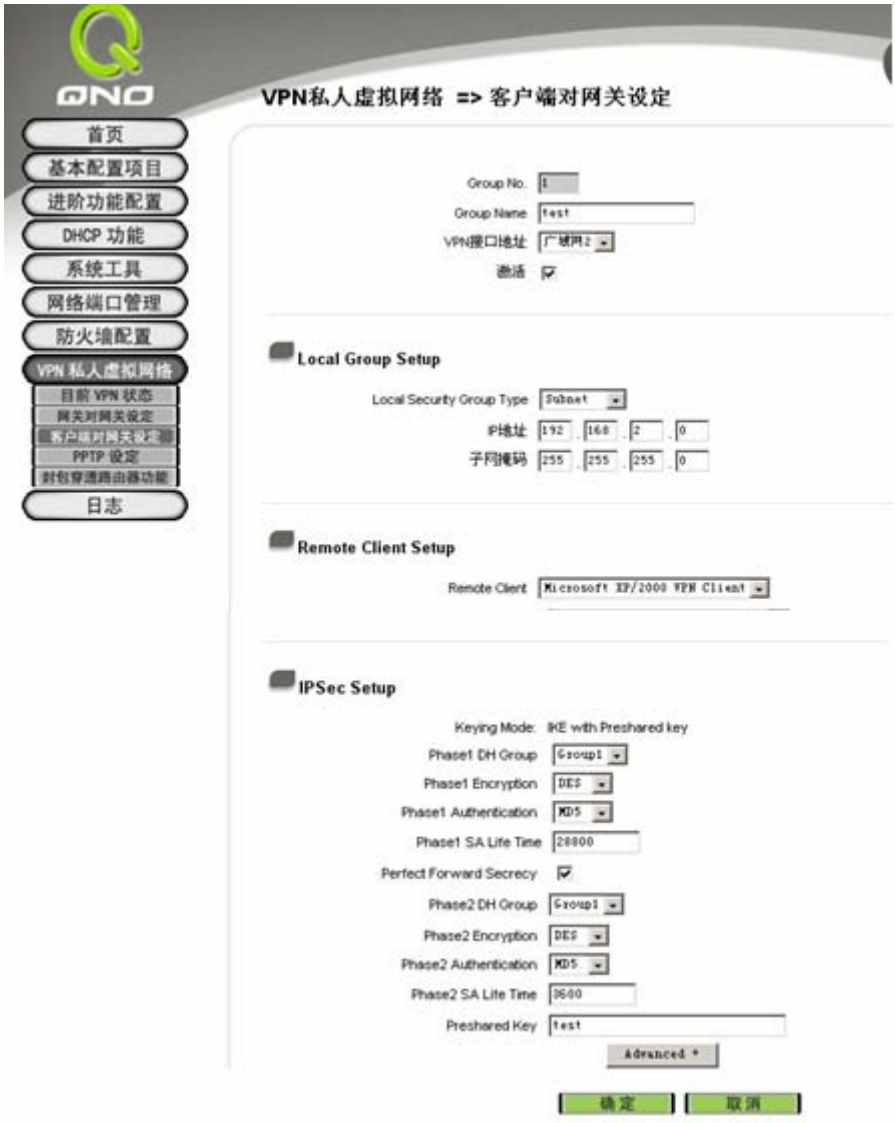
7、 VPN 兼容性

Qno 的 VPN 通过国际 VPNP 人证，支持国际标准协议 IPSec 用户端联及功能，与各开发商的 IPSec 或 PPTP 连接软件互通。以及支持各种 VPN 用户软件联机，行动单机客户端用户可自行任意选用 IPSec 或 PPTP 连接软件，接入总部 VPN 服务器。在 VPN 方面与其它厂商的 VPN 设备兼容好，可以构建稳定、安全、可靠的 VPN 连接。

8、 VPN 用户软件

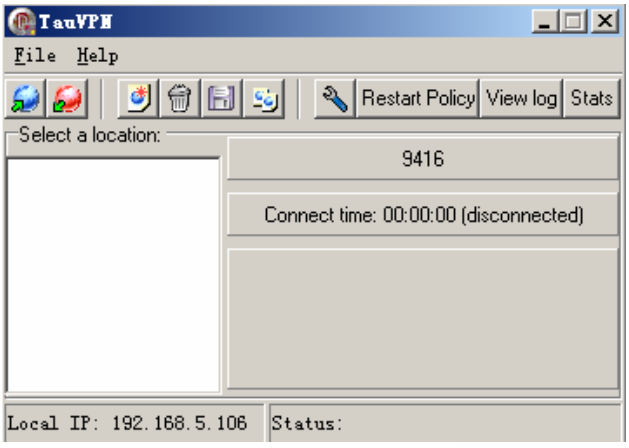
远程接入用白可以通过一些 VPN 用户软件软件与路由器建立客户端与服务端的连接，比如 TauVPN、Forticlient VPN 软件以及 SSH VPN 软件软件等,我们可以通过相关设置与路由器建立 IPSec 连接，Qno 工程师通过大量的测试以及客户的应用都能达到预期效果，下面我们就介绍一下 TauVPN 与路由器之间建立 VPN 连接的相关设置。

在路由器 Web 管理页面的 VPN 虚拟私有网络选择客户端对 VPN 网关的设定，VPN 服务端的设置如下图。



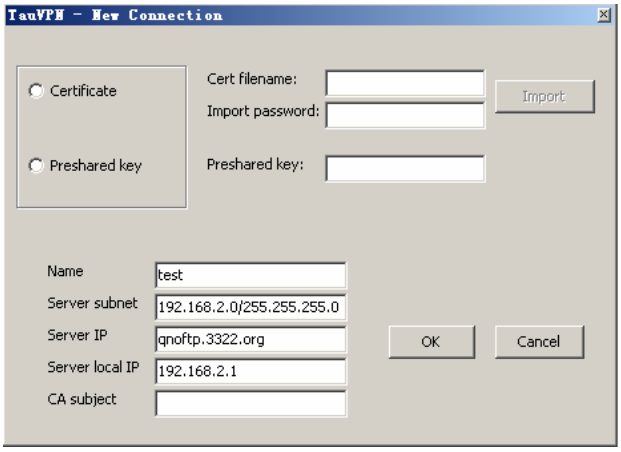
图：路由器 IPSec VPN 设置

然后就是对 TauVPN 软件进行设置，下图点击  新增加一条 VPN。



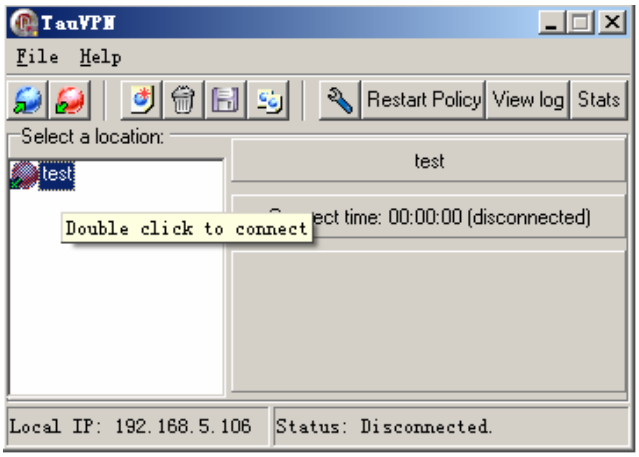
图：TauVPN 软件配置画面 1

在弹出对话框里，添入设置内容，如图设置，然后点 ok。



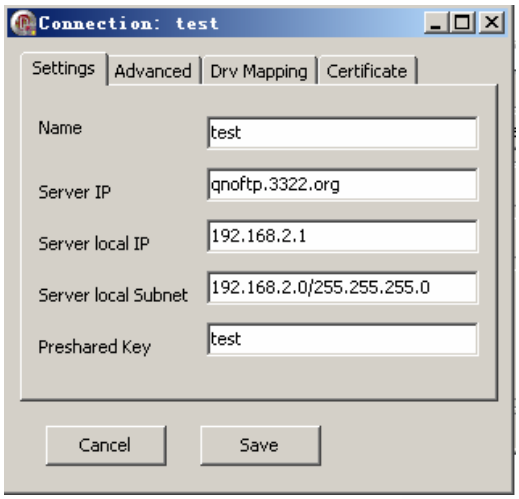
图：TauVPN 软件配置画面 2

建立了一条 VPN 后，TauVPN 界面会如下图。



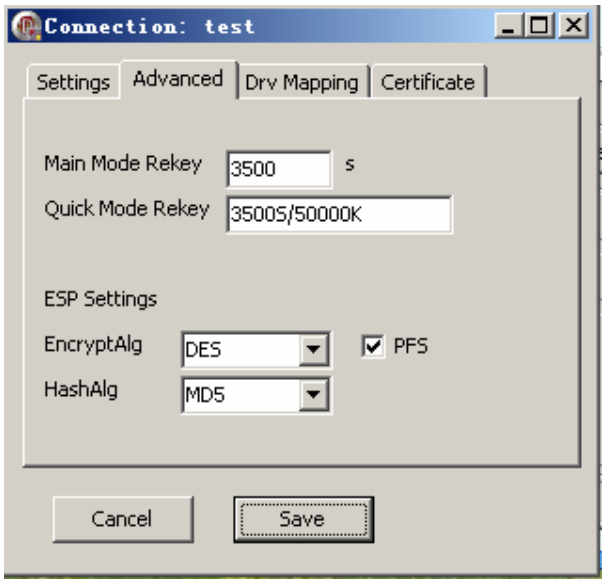
图：TauVPN 软件配置画面 3

然后在刚才建立的 VPN 名字上面点右键，会出现左图的设置界面，具体设置如下图。



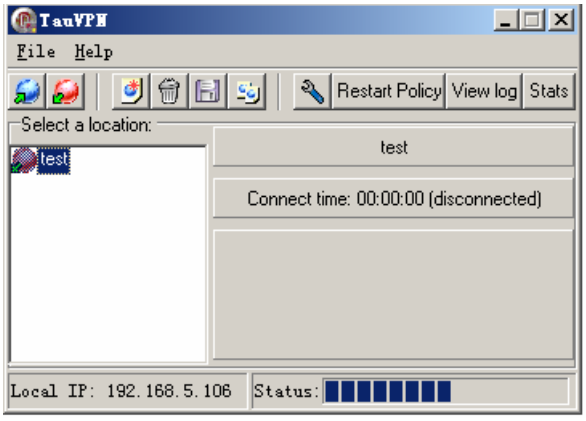
图：TauVPN 软件配置画面 4

点击 Advanced，设置如左图，然后点 save，这样一条 VPN 就建立成功。



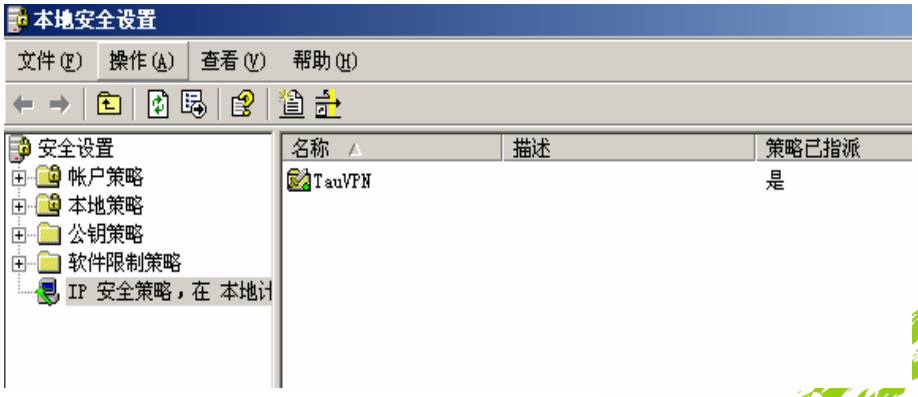
图：TauVPN 软件配置画面 5

点击  图标，会出现如左图所示连接 VPN 的画面。



图：TauVPN 软件配置画面 6

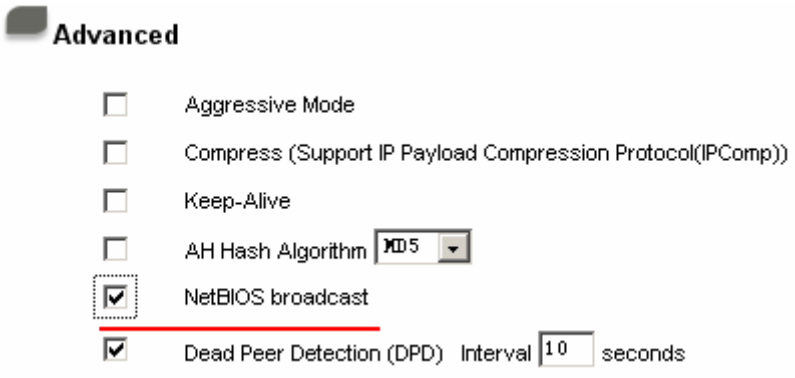
连接 VPN 后，在 windows 的控制面板->管理工具->本地安全策略的页面中会出现如左图的情况，代表 TauVPN 已经和服务端联通了 VPN。



图：Windows 系统确认 VPN 连接画面

9、 网络邻居配置（NetBIOS broadcast 功能）

若选择此项目勾选，则连接的 VPN 信道中会让 NetBIOS 广播封包通过。有助于微软的网络邻居等连接容易，但是相对的占用此 VPN 信道的流量就会加大。



图：NetBIOS broadcast 配置画面

● 共享功能配置

1、 群组管理

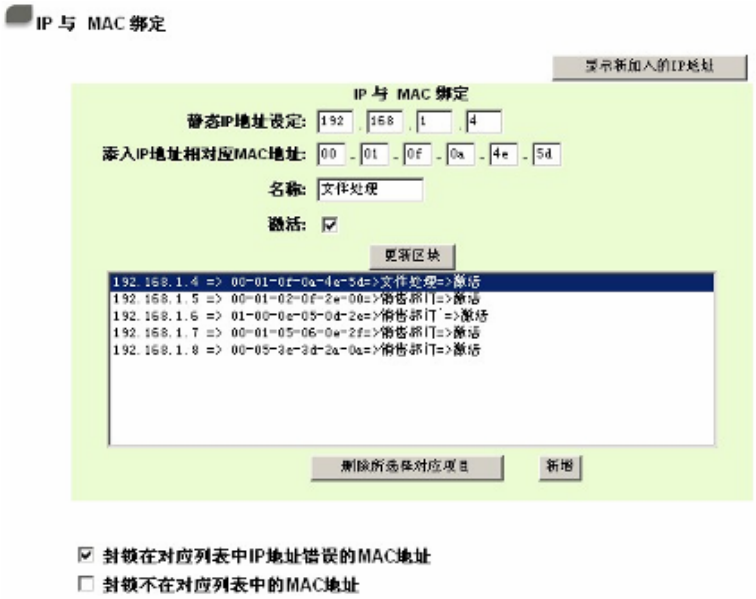
此方式设定方便用户对网络内连续的 IP 做同样的操作。比如一个公司的同一部门分得了一段连续的 IP（192.168.1.100~192.168.1.110），路由器将对这个部门做访问存取规则的设定，我们就把这个连续的 IP 地址绑在一起做相同的设定，相对于对每个 IP 分别进行设定节约了时间和操作过程中容易输入错误，来达到提高工作效率的目的，如下图，进入路由器的 DHCP 功能页面下方的 IPGROUP 管理页面做如下设定。

图：IP 群组管理页面

2、 IP 与 MAC 绑定

有些企业，对不同部门或个人设定了不同的上网权限，可能有的部门以及个人工作比较特殊，没有联入互联网的上网权限，为了避免这些用户去修改 IP 地址逃脱规则的设定而达到上网的目的的，我们可以通过 IP/MAC 的绑定功能使得这些用户即使修改了 IP 地址也无法达到上网目的。比如公司有一台专门做文件处理的电脑和销售部门的 4 台电脑是不可以上网的，他们的 IP 地址分别是 192.168.1.4~8（分别对这 5 个 IP 地址做存取规则的设定，阻止联入互联网），我们通过对 IP/MAC 的绑定后，无任用户改变什么 IP 地址，都是不可以上网的。

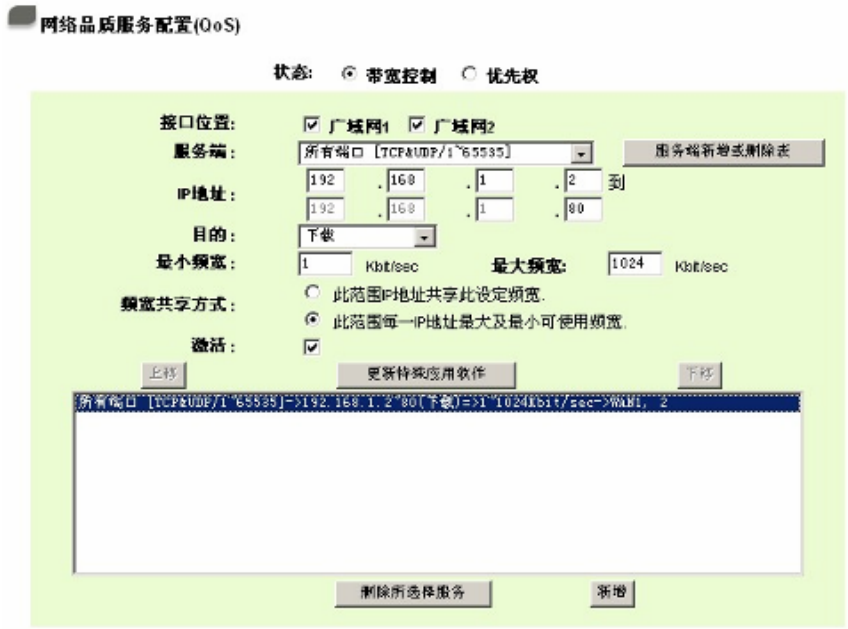
具体设定如下。



图：IP/MAC 绑定画面

3、 防止 BT 以及电影等大量下载

限制大量占用带宽：现在企业的环境中，BT，kugoo，电驴，迅雷等软件的使用，更是线路带宽的杀手，因此，如何保证企业的带宽得到有效的利用，成了各往管人员的当务之急。而使用 Qno 的路由器，可以针对每个区用 QoS（带宽管理）功能，来限制内网每个 IP 或者服务端口的流量，可以把 P2P，迅雷等软件的使用带宽限制到非常小，再也不会因为内网的某台电脑大量下载而占用比较多的线路带宽。例如我要限制内网 192.168.1.x 段（192.168.1.2~192.168.1.80）的每台电脑最大只能使用 2M 的带宽，只需如下设置即可：



图：限制内网 192.168.1.x 段的每台电脑最大只能使用 2M 的带宽的配置。

4、 防止 ARP、DOS 等攻击

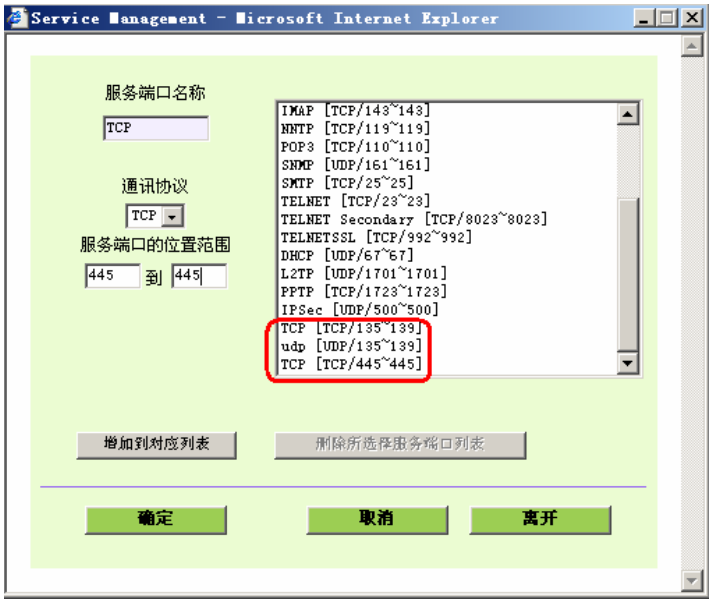
Arp 攻击，DOS 攻击是同样可以影响到企业网络的正常运行，前者可以让内网电脑不定时的掉线，后者可以使网络瘫痪。而 Qno 路由器的防火墙功能则可以很好的解决此问题，提供侦测、阻文件及配置的功能。

图：FVR420 的防火墙配置画面。

5、 防止蠕虫攻击

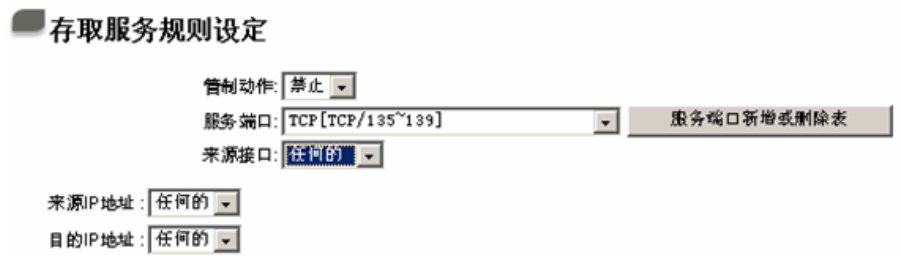
有许多用户内网中冲击波及蠕虫病毒造成内网访问互联网 很慢及联机数(Session)大量增加造成路由器大量处理。 所以以下为指导您封锁此些病毒相应端口以达到防制目的。

a.增加此 TCP135-139，UDP135-139 还有 TCP445 端口：



图：添加服务端口的设置

b.用防火墙里面的"访问存取规则"功能将设定好的此三组端口封锁：



图：存取规则设定画面

c.将这三组的优先级提至于最高:

图：存取规则优先级设定画面

6、 远程管理

路由器提供了远程管理功能，我们只要开激活路由器的远程管理功能，管理人员不论在任何地点只要有电脑连入互联网，都可以通过路由器的广域网 IP 地址远程登陆路由器对路由器做相关设置，方便了管理人员同时提高了工作效率和减少了工作时间，如图。

图：远程管理激活

● Qno 俠诺方案特点

1、 多 WAN 接入技术

当企业需要扩展带宽又想节省成本、想要稳定不中断的联机、同时需要连接不同运营商时，配置多 WAN 端口弹性应用，带宽汇聚、线路备援、负载均衡、以及多 WAN 协议绑定等功能就派上用场了。

QVM 系列可以多条 ADSL 取代光纤，汇聚多条线路增加带宽，取代带宽升级，即可解决企业带宽不足的问题，费用节省又可弹性运用。线路备援功能：当一条线路断线不能使用时，则会自动改用另一个 WAN 端口的线路，进行互联网连接，确保企业联机永不断线。负载均衡功能支持多 WAN 口设计可以方便解决跨网连接 VPN 带来的不稳定因数等问题，配置 WAN1 端口对外数据封包使用电信线路；配置 WAN2 端口对外数据封包使用网通线路，依据分点线路运营商分别配置与总部的 VPN 联机，让电信走电信、网通走网通，确保联机反应快速，解决跨网因带宽受限 VPN 联机很卡的问题。

2、 简化管理

提供了 Web 管理页面，可以通过 Web 页面的简单的设置达到网络的相关需求，即使非网络管理人员也可以通过相关设置达到一定的要求。

同时在 VPN 的连接设置上不仅支持传统的 IPSec 以及 PPTP 连接以外，还特别增加了 Qno 俠诺独有的 SmartLink VPN 连接，在路由器的 QVM 功能页面，我们在服务端填入用户名、密码以及本地内网的 IP 段添加远程用户，以及在远程客户端填入与服务端对应的用户名、密码以及服务端广域网 IP 地址然后就可以方便、快捷的连接服务端路由器。

IP 群组管理功能：可依据 IP 群组作带宽管理，弹性应用，简化管理规则的配置，减少网管的负担。

3、 带宽管理

俠诺 QVM 系列产品均内建强化的带宽管理功能，可让网管依不同的要求进行带宽管理的配置。QVM 系列产品可依时间、内外部 IP 地址、应用 TCP/UDP 端口、VPN 内传输及优先级，对带的应用进行弹性的配置。同时，QVM 系列采用的网络处理器已考虑到带宽管理需要的效能，可提供较好的处理速度。

对于 VPN 客户而言，QVM 系列产品所提供的多 WAN/VPN/带宽管理，可以提供完整的宽带接入及远程接入方案，可因应现在及未来的需求。

4、 兼容性

兼容性好，可以完成连接不同厂商的 VPN 产品（包括硬件产品与软件产品），而且配置起来比较容易，解决不由于客户特殊需求购买其它厂商 VPN 产品建立 VPN 的难题。

● Qno 侠诺方案的效果

提供高性价比要求的弹性方案，提供多选择性的方案以方便用户根据自己的需要来选择，构建自己合适的网络达到自己要求。

强大的 VPN 功能支持各种认证安全协议以满足用户构造不同需求的 VPN 安全网络。以及路由器内部高性能硬件设备保证上网稳定，反应迅速。

SmartLink VPN 功能提供了方便、快捷的 VPN 连接，以及远程管理等功能方便管理人员对网络采取有效的管理，既简化管理操作，还避免了有时候设置多参数出现错误，而且还节约了时间，提高工作效率。

以上方案解决中小型企业来说是一个可以值得信赖的比较好的方法，此方案经过 Qno 的多个技术人员和工程师的讨论以及实际应用，无论从架构成本以及企业所需要的功能、目的以及管理上所要达到的要求都能够满足客户的需要。