Qno 侠诺五招　轻松提高 VPN 稳定性

VPN 对于企业信息化的建设，已经是不可缺少的一环了。随着进销存、财务、ERP、CRM 等软件的的普及，很多中小企业为了达到进一步针对远程存取的目的，开始进行 VPN 环境的建置。有了 VPN，中小企业的分支机构及移动用户，可以通过互联网接入企业局域网的服务器，既可以达到实时办公的效果，又不必担心因此而在信息安全上有漏洞或折扣，方便实用！

根据 Qno 侠诺的多年服务经验，曾接触了很多中小企业的用户。中小企业用户的网管，由于人力有限，对于基本的 VPN 原理及配置的了解，通常较少，也没有时间一一检阅产品的使用手册。所以，经常在初始建置 VPN 时，只要求能达到接通、联网的目的即可，但随着使用经验的积累，却不知如何进行 VPN 配置的优化，进而达到较佳的远程接入效果。

下面，我们就针对中小企业用户进行 VPN 配置时，将可进行优化的配置加以说明，网管如能注意这些配置，相信 VPN 的稳定度可有效地提高。

一、要选择适当的 VPN 协议

大多数中小企业的网管，通常喜欢使用设定简单的 PPTP，而不喜欢设定较为繁复的 IPSec。因此，有时会看到同一个局域网多个用户同时使用 PPTP 协议，连回总部的 VPN 网关。由于 PPTP 协议需要的运算量较大，再加上一般 VPN 网关支持的 PPTP 用户有限，因此如果人数较多，就容易发生由于新的用户加入，原有用户掉线的情况；或者是因为用户人数较多而互相干扰的情况。没有经验的网管，直观认为是 VPN 有问题，但是却疏忽了是因为采用错误的 VPN 协议所致。

简单地说，PPTP 适用远程用户较少，移动用户的安全性要求较低，而 IPSec 适用远程的群组用户或安全度要求较高情况。因此若是分公司需要连接公司总部服务器人数较多时，就适用 IPSec。由于 IPSec 只要建立一条 VPN 隧道，就可提供多个用户使用，因此不管在运算能力使用或是稳定性方面，都比同时建立多条 PPTP 要好得多。相同的推断，也适用在 SSL 上，SSL 协议较 PPTP 安全，配置也方便，但是在同一群用户同时需要连接公司总部服务器时，多条 SSL 所占的系统资源及稳定性都会比 IPSec 还差。

对于害怕 IPSec 配置困难的用户，Qno 侠诺产品提供了专有的 SmartLink 协议，配有象 PPTP 一般简化的配置，既能建立起 IPSec 联机，又能节省系统资源，同时兼顾两种协议的优点。

二、持续 VPN 需要可善用 Keep-alive 功能

一般的 VPN 联机，具备有侦测的功能，当一段时间没有在 VPN 隧道传送网络包时，就会自动切断 VPN 联机。这个做法，既节省系统资源，也可防止没有必要的网络广播包通过

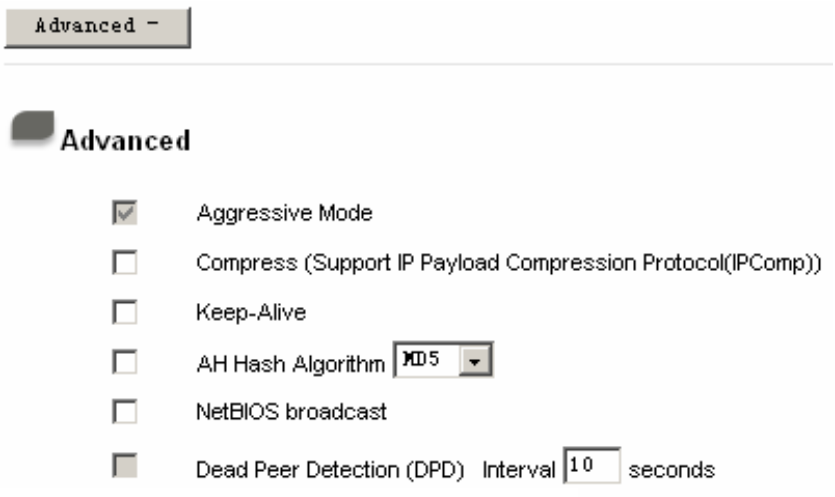
VPN 联机，影响到不同局域网的运作。例如微软的网络芳邻，在开启 NetBIOS Broadcast 的情况下，就会不同发出广播包，以便更新计算机的名称及位置。当内部碰到广播风暴攻击时，也会经过 VPN 隧道互相影响。

当 VPN 隧道切断时，随时可由存取远方服务器的封包而启动，例如用户向总部提出联机需要时，路由器可自动侦测而建立联机。建立联机的时间是很短的，用户只会感到稍有延滞，并不会有明显感觉。但是在有些应用情况下，例如辨认双方 IP 或是要有更高稳定性时，可启动“Keep-Alive”的选项，即可持续保持 VPN 的联机，不会因为没有用到而掉线。用户再需要相关功能时，立即就可进行存取，不会有任何不同。

三、有效利用 DPD VPN 通知侦测功能

VPN 的建立是由双方 VPN 网关进行，任一方网关有问题，都可能导致无法建立联机。由于两方的网络环境不同，加上中国的网络环境变化较大，因此在实际的用户使用中，常常发生分公司路由器，由于电源供应不稳定、ISP 网络不稳定，而突然掉线的情况，在这种情况下，分公司 VPN 网关所建立的 VPN 隧道自然也掉线了，但是此时总公司的 VPN 网关并不知道，经常发生分公司网关要重建 VPN 时，总公司 VPN 网关反而认为是不正常的联机要求，而加以拒絕。这样就会造成完全无法建立联机，或需要重启总部路由器，重建所有 VPN 隧道的不合理情况。

在 IPSec VPN 协议中，即规范了一个解决这个问题的机制，叫作 DPD（Dead peer detection），顾名思义，就是侦测 VPN 另一端 VPN 网关是否正常的机制。DPD 机制可以规范每过一段时间，例如 10 秒，就侦测联机另一端 VPN 网关是否运作正常。如若发生没有响应的情况，就认为远方 VPN 网关器掉线，而进行 VPN 隧道的参数清除，以利 VPN 隧道的重建。有了 DPD 机制，即使发生掉线，也能重建无碍。



图一：本文中所提到的一些功能，都能在 Qno 侠诺 VPN 路由器产品中 VPN 项目菜单内的

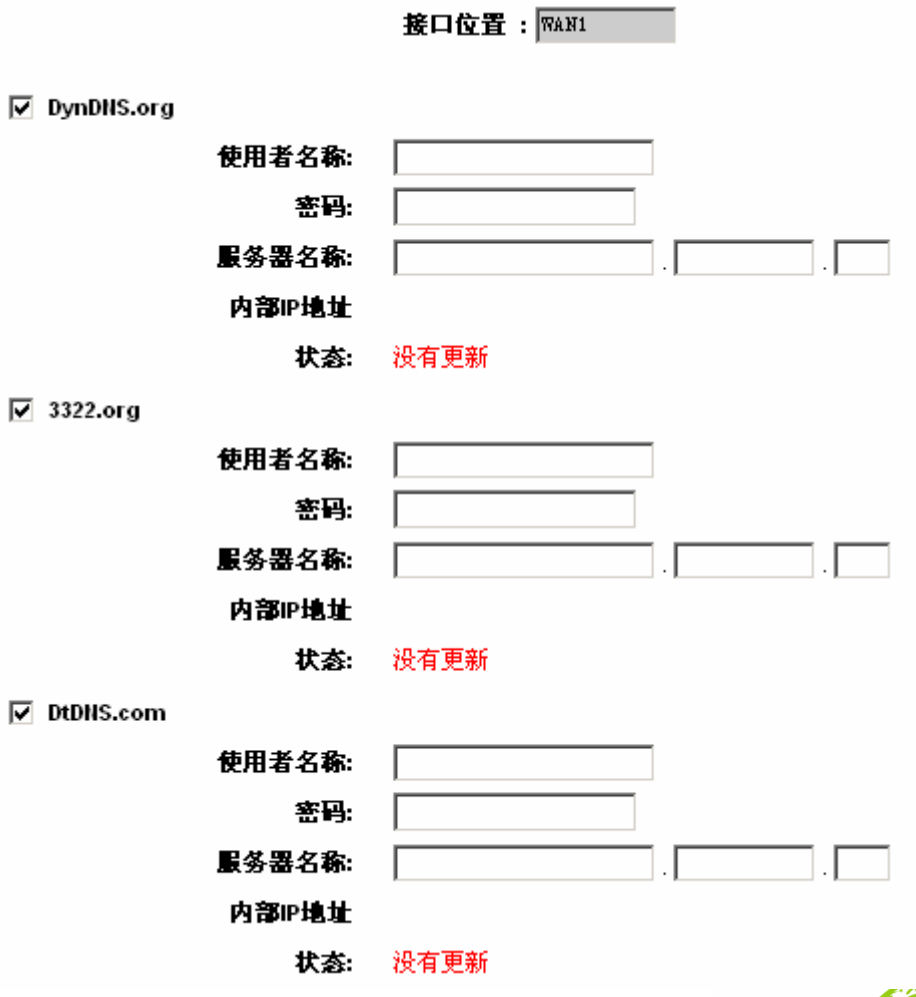
进阶作业模式中看到。其中 Keep-Alive 可以保持 IPSec VPN 永续联机；NetBIOS broadcast 是让微软的网络芳邻广播包可以发送到 VPN 远程，方便用户透过网络芳邻分享文档；DPD 功能是远方 VPN 网关的掉线侦测机制，对于 VPN 隧道的重建，有着重要的角色。

四、适当采用 DDNS 备份增加稳定度。

由于固定 IP 地址的费用较高，因此大部份的中小企业建立 VPN 是通过动态 IP 来进行。DDNS 动态域名扮演了重要的角色，它可以帮助两个动态 IP 的 VPN 网关找到对方，进行相关的程序。不过，由于常见的动态域名稳定性不高，因此常常会发生因为动态域名系统工作不正常，而完全无法建立 VPN 联机的情况。

Qno 侠诺的 QVM 系列 VPN 产品，提供了多套 DDNS 备份的设计。中小企业的网管可以为每个 WAN 口指定最多四家不同 DDNS 服务，互相进行备份。当某一个 DDNS 运作不正常时，就可以其它的 DDNS 替上，不致发生无法建立联机的情况。

同时，Qno 侠诺也建置自有的 DDNS 系统，将提供给购买 Qno 侠诺 VPN 产品的用户使用。



图二：每个 Qno 路由器的广域端口，均可提供多个 DDNS 服务，启用的 DDNS 服务还互为备份，可提高联机稳定度，减少因 DDNS 不稳定而产生无法建立 VPN 情况。同时 Qno 侠诺将推出自有的 DDNS 服务，提供给用户使用，再次提高稳定度。

五、发挥多 WAN VPN 特色增加稳定度

Qno 侠诺 VPN 产品均采用多 WAN 设计，也可针对常见的跨网不稳定及掉线备份加以应对。有些中小企业分公司遍布不同地区，采用电信或网通不同的线路，因此或是网部采用电信线路，采用网通线路的分公司建置的 VPN 就很卡或掉线。这种情况，总部可以同时使用电信及网通的线路，电信线路的分公司从电信线路接入，而网通线路的分公司从网通线路接入，这样可避开跨网带宽不足，既解决了稳定性问题，又可达到快速存取的目的。

同时，Qno 侠诺的 SmartLink VPN 支持 VPN 备份的功能，当 VPN 掉线时，可从另外的广域网端口重新建立 VPN。例如对于较重要的分公司，可以双方都同时接入电信及网通的线路，一般时间 VPN 是通过电信的线路建立，并进行传输，但是当电信线路因故中断时，即可由网通线路重建，避免因此对运营造成的影响。

六、小结

稳定是 VPN 联机必需要有的基础。但是，稳定并不是会从天上掉下来，网管必须在整体配置、细节功能、备份措施等方面都要有对应的准备，才能达到稳定的目的。中小企业也许在 VPN 的经验及了解都较为不足，但是如果选用产品得宜，建立稳定而快速的 VPN 联机，并不是太困难的！