QNO
your future life

SSL VPN

产 品 销 售 手 册

企业网络高速互连　移动办公无处不在

http://www.Qno.cn

目录

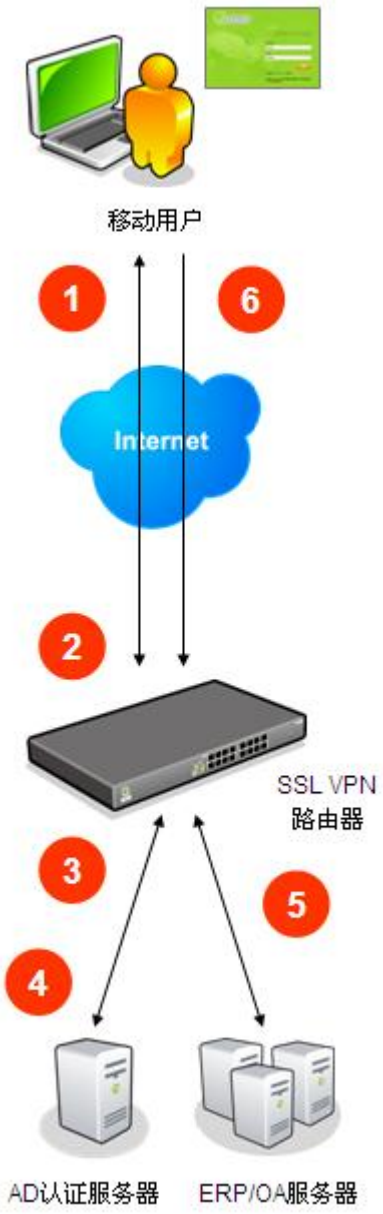
一、浅谈 SSL

当今世界全球化的进程越来越快，这使得分布在世界各地的企业各分支机构、合作伙伴和客户之间的联系越来越紧密，加上出差移动用户的需求日益频繁。因此，外部人员如何能安全、方便、快速的远程接入企业总部内网进行办公成为企业关注重要的议题。目前远程接入除了透过 IPSec、PPTP、Qno SmartLink VPN 等协议之外，同时结合简易、安全两项强大特性的 SSL VPN 协议，也因为多家网络安全设备厂商相继投入而逐渐被企业所关注应用。

SSL 是什么？简单来说 SSL（Security Socket Layer，安全套接层）是一种在互联网上，经由加密机制保证发送信息安全的通用协议，它包括：服务器认证、用户认证、SSL 链路上的数据完整性和数据保密性。在应用面而言，SSL VPN 是将局域网资源，以 VPN 网关功能，采 SSL 安全方式，提供给远程接入用户。由于 SSL VPN 采用目前所有通用标准浏览器内建的 SSL/HTTPS 作为安全传输机制，因此在客户端最关键的优势在于：无需安装、无需设置，只要通过浏览器如 IE 或 Netscape 便可进行远程数据存取，具有部署简单、无客户端、维护成本低、网络适应强等特点。相对在管理端上只需通过原有的身分认证机制，即可对使用者身份及权限加以分级管理，让企业信息不至于完全通透，安全保障可更上一层楼。

总的说来，SSL VPN 表现在简单应用、身分认证、使用权限区隔等方面，对企业网络安全运作具有强大的优势。如今，随着 SSL VPN 技术的发展，SSL VPN 产品所能提供的终端网络功能已经与传统的 IPSec VPN 产品几乎一样强大，SSL VPN 接入方式是点对网 VPN 接入的最佳选择的观点也越来越深入人心。SSL VPN 自出现之日起就作为一项主要的技术使企业大大降低其远程存取的费用，同时通过互联网提供专有服务。对于现在企业信息化建设步伐的加快，低成本的选择才能增加企业竞争力。我们通过以下工作流程与拓朴图可简易了解 SSL VPN 实际运作状况。

SSL VPN 工作流程与拓朴图：



远程用户通过 SSL/HTTPS，联机至 SSL VPN 路由器；

SSL VPN 路由器收到远程用户联机要求后，即开启登入页面，请该用户输入用户名/口令；

远程用户输入用户名/口令后，将数据送至后方身份认证服务器，验证该用户身份；

身分认证服务器验证远程用户身份后，通知 SSL VPN 路由器，允许该用户登入；

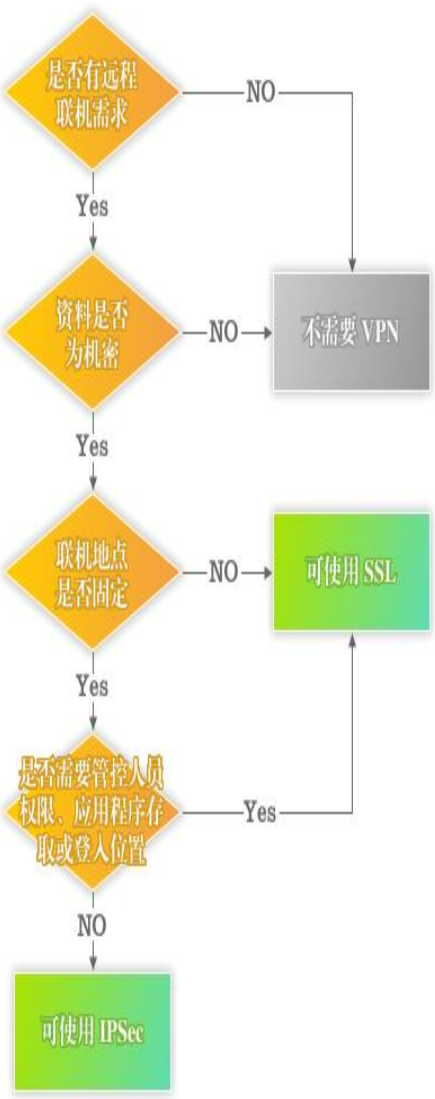
远程用户通过认证后，SSL VPN 路由器依据权限政策，开放相关应用服务让该用户存取；

远程用户现在可以浏览登入后的网页，并点选可存取的应用服务连结。

注：若外部配置有防火墙，需开启 PORT 443，允许 SSL/HTTPS 联机通过。

二、企业 SSL VPN 导入评估

通过 SSL VPN 远程接入办公，可拥有良好的机动性与使用弹性，不需受限于网络联机设备配置，企业外部人员可通过如网吧非自有电脑、或其它连线设备如：PDA、GPRS 手机等，只要能读取网页即可存取企业总部内部资源，随时随地取得所需数据进行办公作业。企业如何评估自身网络联机需求来导入 SSL VPN，可参考下列导入评估问题加以检视：



第 1 步：您的企业是否有远程接入需求？

员工是否需经常在公司以外的地点，存取业务文件、邮件、内部网站、资料库、或是特殊应用程序等内部资讯？

是，请继续接＃2；否，则不需要使用 VPN

第 2 步：资料是否为机密？

如果欲开放远程接入存取资料为内部机密或重要业务资料，则应考虑采用 VPN 方式存取，以确保资料传输安全。

是，请继续接＃3；否，则不需要使用 VPN

第 3 步：连线地点是否固定？

远程接入用户的连线地点如果都是固定位置，例如家中、分公司或上下游厂商，并且使用固定计算机，则不一定非用 SSL VPN 不可，也可使用 IPSec VPN。

是，请接＃5；否，则应考虑使用 SSL VPN

第 4 步：是否需要对用户作身份认证及权限控管？

如果需要管控远程接入用户身份认证、可存取的应用服务内容，则应采用 SSL VPN；如果应用服务可全部开放，不需特殊管控，且连线地点固定，则可采用 IPSec VPN。

是，则应考虑使用 SSL VPN；否，则可采用 IPSec VPN

- 企业适用 IPSec VPN 的需求：不需身份认证、权限控管、连线位置固定。
- 企业适用 SSL VPN 的需求：需要身份认证、权限控管、连线位置不固定。
- 否则，企业不需要 VPN。

三、中小企业专用 SSL VPN 解决方案

3.1、产品简介

由于取得 SSL 认证费用较为昂贵，SSL VPN 一般只应用在大型企业中。然而并不是只有大型企业才能用得起 SSL VPN。为了提供企业更丰富多元的 VPN 联机方案选择，Qno 侠诺科技提出专为中小企业应用设计的 SSL VPN 方案，除了注入侠诺研发团队长时间细心推敲成就出的友善优化的管理界面设计外，并打破大型企业独享高价 SSL 的传统，提供较适当的价位，使中小企业在满足对应用需求的基础上，能够和大型企业一样真正享受 SSL VPN 带来的良好服务。

配合新一代、多样化、高安全整合性的设备需求环境，侠诺 SSL VPN 系列产品也推陈出新，继之前适用于中大型企业总部级 SSL001+、SSL002+之后，又带来同样适用中大型企业的 SSL003 与中小型企业也适用的低端王者 SSL005, SSL006。高性能的网络运算核心，内建高规格 DDR2 超大容量服务器专用内存，封包处理快速稳定，处理速度及带机量直逼中、大型企业用户专用的昂贵 VPN 防火墙设备。多个广域端口与局域端口及方便扩展的 USB 端口，适用各种不同网络架构。除了强效的硬件效能外，侠诺还对 SSL 系列产品加入了诸多创新的软件功能，如增加稳定性能的双机热备援、有效管制上网行为的侠诺神捕网络监控、使网络畅通的进入流量负载均衡等等，软硬结合，将侠诺产品的功能极致发挥。

3.2、产品选型

针对不同规模的企业与不同的应用需求，Qno 侠诺科技提供 SSL001+、SSL002+、SSL003、SL005、SSL006 五款不同型号的多协议复合式 VPN 防火墙。

SSL001+多协议复合式 VPN 防火墙 SSL VPN 可支持最大 300 个并发用户；具备 PPTP 服务器功能，可提供 200 个 PPTP 移动用户进行 VPN 联机；VPN 隧道数最多可支持 250 条（包含 IPSec、QnoKey、SmartLink 不同和联机，用户可自行依需求弹性调整隧道数值）。

适用对象：中大型企业总部，如大规模的连锁销售业、制造业、物流仓储业、保险业、销售行业等。

SSL002+多协议复合式 VPN 防火墙 SSL VPN 可支持最大 700 个并发用户；具备 PPTP 服务器功能，可提供 200 个 PPTP 移动用户进行 VPN 联机；支持 QVM 服务器功能，VPN 隧道数最多可支持 400 条（包含 IPSec、QnoKey、SmartLink 不同和联机，用户可自行依需求弹性调整隧道数值）。

适用对象：中大型企业总部，如大规模的连锁销售业、制造业、物流仓储业、保险业、销售行业等。

SSL003 多协议复合式 VPN 防火墙 SSL VPN 可支持最大 100 个并发用户；具备 PPTP 服务器功能，可提供 80 个 PPTP 移动用户进行 VPN 联机；支持 QVM 服务器功能，VPN 隧道数最多可支持 200 条（包含 IPSec、QnoKey、SmartLink 不同和联机，用户可自行依需求弹性调整隧道数值）。配有 2 个 USB 端口，方便接入 3G 模式上网卡，便利无线上网。支持游戏端口加速。

适用对象：中大型企业，如中等规模的连锁网吧业、连锁销售业、制造业、物流仓储业、保险业等。

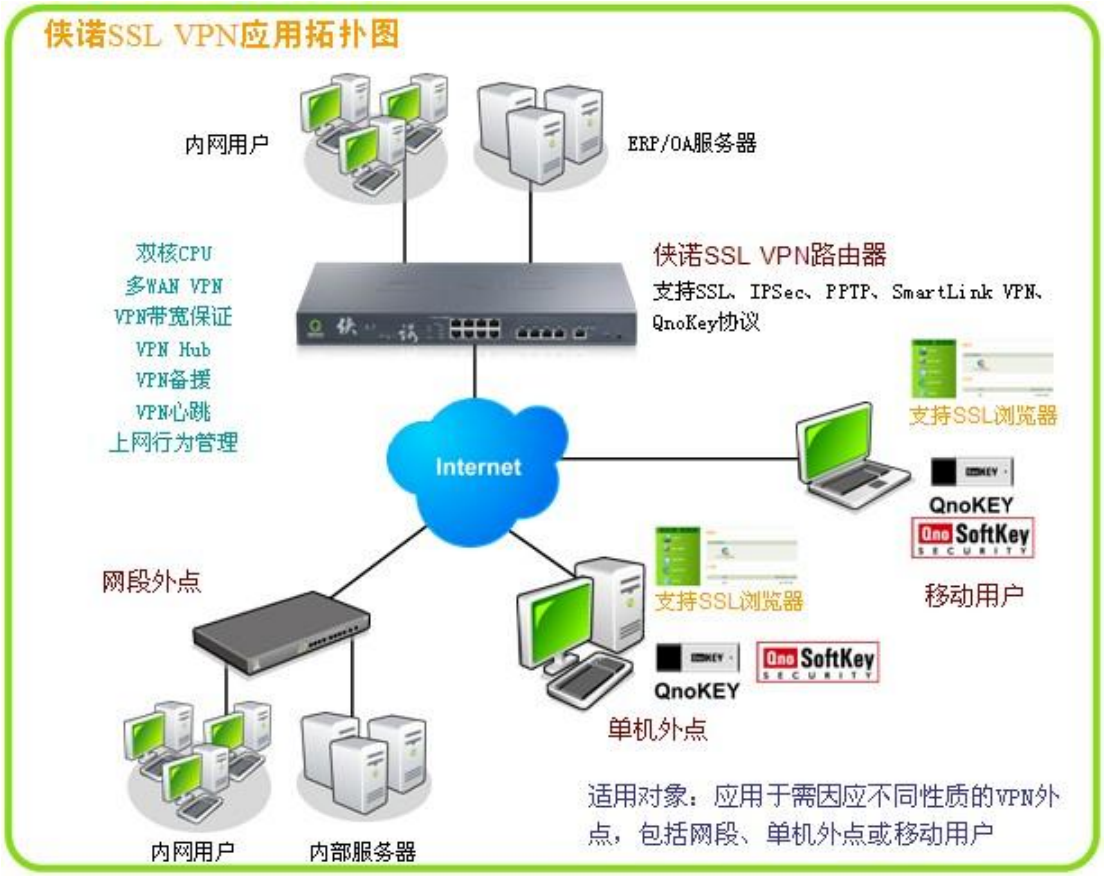
SSL005 多协议复合式 VPN 防火墙 ，SSL VPN 可支持最大 50 个并发用户；具备 PPTP 服务器功能，可提供 40 个 PPTP 移动用户进行 VPN 联机；支持 QVM 服务器功能，VPN 隧道数最多可支持 100 条（包含 IPSec、QnoKey、SmartLink 不同和联机，用户可自行依需求弹性调整隧道数值）。配有 2 个 USB 端口，方便接入 3G 模式上网卡，便利无线上网。

适用对象：中小型企业，如小规模的连锁销售业、制造业、物流仓储业、保险业、销售行业等。

SSL006 多协议复合式 VPN 防火墙，打破以往 SSL 只被大企业所拥有的传统，侠诺专为中小企业打造了系列 SSL 产品，而这款小而全的 SSL006 产品可以说是小型企业的福音。2WAN+4LAN+1USB 端口，具备传统路由器该有的功能(负载均衡、QoS、防火墙等)，支持传统的 VPN(PPTP、IPSec)，还可作为 SSL 服务器中心端接入，USB 界面，更可助力企业跨入无线网络时代。对于中小型企业来说，一人担当多重职务，经常各地奔走，功能全面的 SSL006 是兼顾安全方便又省钱的移动用户最佳 VPN 解决方案。

适用对象：中小型企业，如小规模的连锁销售业、制造业、物流仓储业、保险业、销售行业等。

3.3、应用拓扑图



图示：侠诺 SSL VPN 应用拓扑图

3.4、产品规格

产品型号	SSL001+	SSL002+	SSL003	SSL005	SSL006
硬件规格	MIPS64 双核高阶处理器	MIPS64 双核高阶处理器	MIPS64 双核 1G 处理器	MIPS64 双核处理器	MIPS64 双核处理器
广域端口	4 （千兆）	4 （千兆）	5 （千兆）	4	2
DMZ 端口	1 （千兆）	1 （千兆）	1（千兆）	1	1
局域端口	8 （千兆）	8 （千兆）	5 （千兆）	4	4
USB 端口	-	-	2xUSB Ports	1xUSB Ports	1xUSB Ports
绿色通道加速	硬件加速	硬件加速	硬件加速	硬件加速	硬件加速
联机数	300,000	300,000	160,000	50,000	30,000
防火墙效能	2Gbps	2Gbps	2Gbps	200Mbps	200Mbps
VPN 效能	3DES/175Mbps	3DES/175Mbps	3DES/116Mbps	3DES/97Mbps	3DES/97Mbps
负载均衡	进阶型联机数 / IP	进阶型联机数 / IP	进阶型联机数 / IP	进阶型联机数 / IP	进阶型联机数 / IP

进入流量负载均衡	支持*	支持*	支持*	支持*	支持*
DHCP 服务器	4 Class C	4 Class C	4 Class C	4 Class C	4 Class C
动态智能带宽管理	支持	支持	支持	支持	支持
高效防火墙	支持	支持	支持	支持	支持
QQ 号管理	支持	支持	支持	支持	支持
上网行为管理	支持	支持	支持	支持	支持
VPN 隧道数	最多 250	最多 400	最多 200	最多 200	最多 100
VPN Hub	支持	支持	支持	支持	支持
群组式 VPN	支持	支持	支持	支持	支持
NAT 穿透 (NATT)	支持	支持	支持	支持	支持
SmartLink VPN 服务器(中央控管)	支持	支持	支持	支持	支持
QnoKey IPSec VPN 客户端密钥	支持	支持	支持	支持	支持
QnoSoftKey IPSec 客户端密钥	支持	支持	支持	支持	支持
PPTP VPN 服务器	最多支持 200 个用户端	最多支持 200 个用户端	最多支持 80 个用户端	最多支持 60 个用户端	最多支持 40 个用户端
SSL VPN 并发用户数	100~300	100~700	最多支持 100 个用户端	最多支持 60 个用户端	最多支持 35 个用户端
SSL 硬件加速	支持	支持	支持	支持	支持
网络打印	支持	支持	支持	支持	支持
用户访问控制	支持	支持	支持	支持	支持
暂存资料清除	支持	支持	支持	支持	支持
超时自动退出	支持	支持	支持	支持	支持
动态域名 DDNS	QnoDDNS / 3322 / DynDNS	QnoDDNS / 3322 / DynDNS	QnoDDNS / 3322 / DynDNS	QnoDDNS / 3322 / DynDNS	QnoDDNS / 3322 / DynDNS
硬件端口镜像	支持	支持	支持	支持	支持
双机备援	支持*	支持*	支持*	支持*	支持*
侠诺神捕网络监控	支持*	支持*	支持*	支持*	支持*
典型带机量	1,000~1,200	1,000~1,200	250~400	200~250	100~200

注一：● 表示有支持此项功能 - 表示无支持此项功能 Future 表示未来可以支持

注二：＊此功能必须额外购买使用密钥

注三：侠诺公司保留产品数据内容的修改权利

3.5、SSL VPN 服务概述

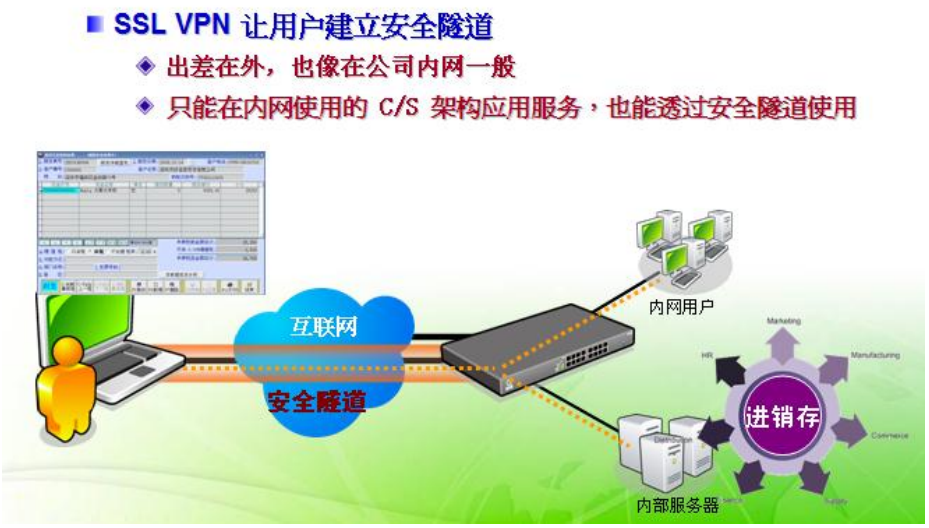
根据服务范围和种类的不同，侠诺 SSL VPN 的服务可分为两种：即基本 SSL 和高级 SSL。

侠诺 SSL VPN 提供的服务内容包括两个层极级：

SSL VPN 服务层级	服务项目	备注
基本 SSL VPN	SSL 安全隧道	几乎适用于所有企业用户
高级 SSL VPN	安全网页服务、微软终端服务、远程桌面、在线网络邻居	可对每一个用户管控所能使用的服务。

（1）基本 SSL

它主要指的是“安全隧道”功能，可提供远程接入使用局域网所有网络资源，具有和局域网计算机相同权限。它让远程用户计算机取得一个局域网的 IP 地址，应用上等于是一个局域网上的用户。这个功能让用户的所有运作，就好像是在局域网上的一台计算机，因此等于开放了最大的权限。这个功能和 PPTP/IPSec 的功能相近，只是通过 SSL 来运作，用户配置也较容易。


SSL VPN 让用户建立安全隧道
出差在外，也像在公司内网一般
只能在内网使用的 C/S 架构应用服务，也能透过安全隧道使用
互联网
安全隧道
内网用户
进销存
内部服务器

（2）高级 SSL


高级SSL VPN：完整的应用服务
网络服务
网页服务
安全网页服务
Telnet远程连接服务
SSH加密远程连接服务
FTP文件传输服务
微软服务终端
Word
Excel
PowerPoint
Access
Outlook
SSL
远程桌面服务
RDP5
VNC
RDP5远程桌面
VNC远程桌面
在线网络邻居
在线访问网络邻居
安全隧道
建立基于SSL的IP隧道
your future life
www.Qno.tw | www.Qno.cn

高级SSL VPN：入口网页显示用户可用的服务

安全网页服务：提供远程接入使用局域网 TCP/IP 相关服务。主要是将常见的 TCP/IP 服务，例如 Web、SSL Web、FTP、Telnet、SSH 等服务，经由 Qno SSL VPN 转换，变成 Web 界面让远程用户使用。应用的情况为从远程观看局域网内部网站或网站服务器的文件、从远程到局域网内 FTP 服务器存取文件、从远程进入局域网的服务器执行 Telnet 动作等等。这个功能适合一般的用户从外部回到局域网内观看文件，或是观看 HTTPS 加密过的网页文件、或者是技术人员回到局域网执行 TCP/IP 相关的指令。由于 TCP/IP 相关应用往往是公开性的，因此是远程接入资源关联范围最小的服务。

终端服务：提供远程接入使用局域网具有 Windows 终端服务器应用软件。主要将常见的微软终端服务，例如 Word、Excel、PowerPoint、Outlook 或任何可在 Windows 服务器运作的软件，经由微软终端服务功能，配合 Qno SSL VPN 提供给远程用户。最常见的应用就是用户从外部连回局域网执行 C/S 架构的财务软件或 ERP 软件，或是操作系统上常见的办公软件。使用这个功能的前提是提供应用服务器上，必须备有 Window 终端服务器，否则无法使用。这种应用只开放单一应用给远程用户，因此安全性高，运作速度也较快。

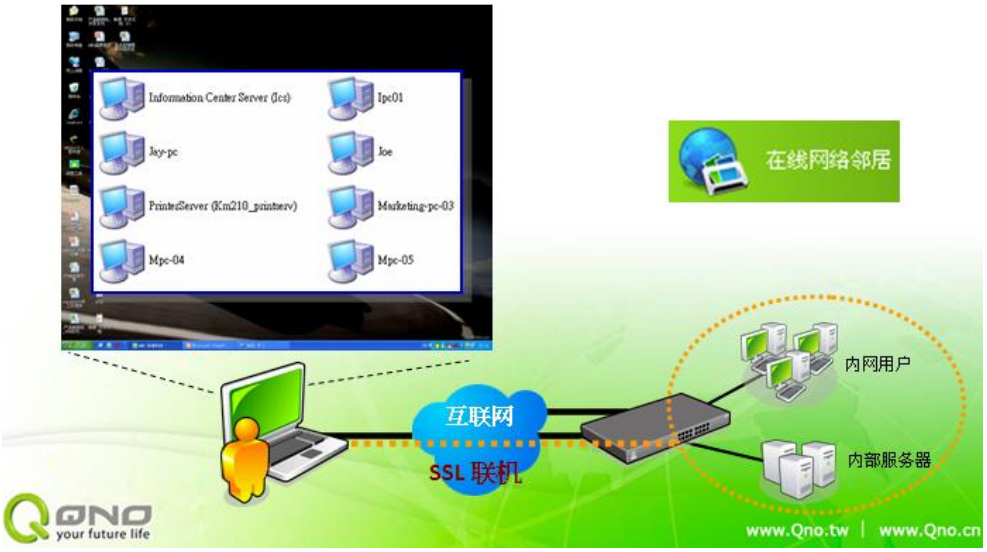
微软服务器作业系统提供的服务

远程桌面服务：提供远程接入使用局域网支持 RDP 或 VNC 计算机整个桌面资源。主要是经由远程遥控的功能，操控局域网上某一台计算机的画面，等于是在局域网上的一部计算机工作。这个工作主要经由 RDP（Remote Desktop Protocol）及 VNC（Virtual Network Computing）远程遥控协议运作，可支持 Windows、Linux、Mac 不同操作系统的计算机。主要的应用，例如提供远程技术支持、演示、联机回局域网计算机进行任意一种操作。这种应用等于开放局域网上一部计算机的所有资源，因此资源关联范围较大。也可以说前面提供的服务，如果有不足的地方，都可以以这个功能来实现。但是被遥控的计算机，必须安装 RDP 及 VNC 服务器软件，才可以实现这个功能，不是随时都可启用的。远程桌面的功能，等于将一部计算机的资源全部开放，安全性相对较低，另外由于每个动作都要将桌面传送到远程，因此运作速度较慢一些。

从远端控制内网计算机的桌面

在线网络邻居：提供远程接入使用局域网 Windows 网络邻居的文档服务。主要是将局域网上 Windows 网络邻居的服务，由 Qno SSL VPN 以网页文件的形式开放给远程的用户。这个服务的应用主要为支持远程的文件访问。由于网络邻居是常见的文档存取服务，而且只有用户自行规范愿意开放的文件，才能让其它用户存取。同时，用户也能对开放的文件，作不同存取权限的配置，因此，相对是较为安全的。不过这个功能，也等于是开放局域网上所有允许公开访问的文件，因此资源关联范围相对也是较大。对于寻找网络上的用户及文件是很方便，但是也具有外漏网络上所有文件的风险，因此使用上要较为小心。

从远端连接内网其他计算机的共享资料



3.6、应用特点

处理器高速升级

侠诺 SSL VPN 在 Intel-IXP 处理器的基础上全面升级为 64 位 MIPS 多核处理器，其性能大幅度提升，使路由器整体的效能提升了 3~20 倍。此外，CPU 除了能在同一时间分散处理联机外，也能维持封包最重要的顺序性，不至于让网络传输的数据秩序紊乱。用多核取代单核，有了更加强大的效能，企业内网数据转发更快、可增加更多的应用与服务、扩展更大的网络规模，同时，更强的效能意味着设备的抗攻击能力更强，使企业网络在更加安全的环境下高效的运转，全面提升企业的网络性能。

高安全性

Qno SSL VPN 通过 SSL 协议加密、用户身份认证、及严格的权限控管等重重安全管制，保证 VPN 联机安全。一般的用户只能使用特定应用，且不会有实际数据保存于客户端计算机，安全性极高。提供登录注销后清除 Web 缓存、Cookie 等各种记录功能，避免数据资料被有心人士窃取。允许设置用户使用时效，到期则无法接入 SSL，在安全上更增一层保障。

应用快速

Qno SSL VPN 终端服务让客户端不需安装应用软件，只需通过支持 SSL 浏览器登录，远程接入直接在中心端进行数据存取，以只传送画面的方式进行，带宽需求极小，不会有响应慢的问题，解决 C/S 架构远程接入响应慢、安全性低的问题。

方便易用

Qno SSL VPN 客户端无需安装软件，零配置、无需维护，只要会使用浏览器，就可通过身份认证访问企业内部资源，实现联机一键通。无论是在任何地点的分支机构、出差人员、合作伙伴等，都可以轻松通过互联网访问企业内部资源。简单直白图像化操作界面，不需要太多技术指导，用户可轻松上手，减轻网管负担，加速企业 SSL 全面应用。

简单易管

Qno SSL VPN 管理一键通，网管可以直接套用预置用户群组样版，省去繁复设置流程，快速完成配置。强调中文的配置画面，配合直白的单页配置设计，将复杂的配置放置在一个页面完成，简化管理。支持多种认证方式，包括：本地认证及外接的 RADIUS、Active Directory、LDAP、NT Domain 等，企业网管可采用最适当、方便或既有的认证方式，以缩短配置时间。

四、案例实际示范

案例背景

DEMO 公司为一中型连锁销售企业，目前在各区总共有 50 个销售门市，门市作业并不需要特别提供员工网络服务，因此只需要配置一台计算机可以上网与总部联机进行财务文件、ERP 销售数据存取。以下说明 DEMO 公司网络拓朴架构：

采用侠诺 SSL001+企业级四 WAN SSL 防火墙作为总部 SSL VPN 中心端网关；

线路采用电信、网通 ADSL 各一条汇聚带宽、互为备援；

总部内部网络建置一台 Microsoft Windows 2007 Server 作为企业的主要服务器。启用 Terminal Server 功能，提供微软办公室软件及 ERP 应用服务；

另一台服务器，安装 Exchange Server 作为 E-mail 服务器及 AD 认证服务器，企业员工登入网域、收发 E-mail、存取 ERP、及远程接入 SSL 服务器都采用同一个帐户，便于维护、使用；

为了提供企业对外宣传及外部人员文件存取服务，还建置一台 Web & FTP 服务器，对外提供相应服务。

以上网络配置可结合 Qno 侠诺 SSL001+产品提供远程用户 Web、FTP 等网络服务、Word、Outlook 等微软应用程序、远程桌面服务、在线网络邻居、安全隧道等五大类服务项目。

以下介绍 DEMO 公司网络实际的 SSL VPN 建置规划。

DEMO 公司将会需要使用 SSL VPN 远程接入服务的人员，规划高层、业务、外点销售、供应商等四大群组。高层群组用户需要拥有全 SSL 服务功能；业务群组用户常需要出差在外，需要能在各地连回进行业务文件存取、办公室软件应用、ERP 数据查询及存取、自有电脑接入等作业；外点门市销售群组用户需要能连回进行销售文件存取、办公室软件应用、ERP 数据查询及存取等作业；供应商群组用户则需要连到 DEMO 公司进行 ERP 库存资料查询。各群组人数有：高层 10 人、业务 20 人、外点销售 50 点、及供应商 20 家。规划目标是让不同用户群组、具有不同权限，并登入不同的用户界面。

依据群组工作需求各分配不同权限，举例如下：

服务项目	网络服务	微软终端服务	远程桌面服务	在线网络邻居	安全隧道
高层	●	●	●	●	●
业务	●	●	●	-	-
外点销售	●	●	-	-	-
供应商	-	●	-	-	-

侠诺科技考虑连锁企业外点众多，缺乏专业网管人力，产品设计上力求简单易用为原则。

Qno SSL VPN 支持群组管理，并以群组单位作设置基础，藉以加速设置时间。这里先提出 Qno SSL VPN 针对群组设置的几点规则，企业网管需要先理解清楚才好进行后续的设置动作。

(1). 使用者帐户必须建置在群组中，用以加速设置。

(2). 同一个使用者帐户，只能对应单一个群组，否则会发生群组权限分配冲突。

(3). 同一个群组名称，只能对应单一个认证服务，否则会发生认证服务冲突。

总部管理端

1. 超快速设置：

Qno SSL VPN 预置有四种用户群组样版，分别是：All Users（全功能群组）、Supervisor（高管群组）、Mobile User（移动用户群组）、Branch Staff（分公司人员群组），具有不同的权限分级，方便企业直接应用。高管、移动用户、分公司人员三类人员则是企业最需要使用 SSL VPN 服务的用户。

管理一键通：

在认证管理上，企业可采连接既有的 Exchange Server 的 AD（Active Directory）认证服务器，网管不需花时间一一重建员工帐户；在用户权限设置上，企业若需要达到快速 SSL 上手，可以选择直接套用预置的 All Users（全功能群组）群组样版，网管即不需再一一配置群组特性，AD 服务器建置的所有公司成员即可开始使用全功能的 SSL 服务，实现管理一键通，超快速的完成企业 SSL VPN 建置。

一次性登入（Single Sign-On）：

接入 Qno SSL VPN 后，为了安全考虑，点击各项应用服务仍会需要远程用户输入口令验证身份权限。Qno SSL VPN 具有一次性登入（Single Sign-On）功能，可免除登入每个应用服务需一再输入口令的困扰。用户登入内部服务器的用户名及口令如果和登入 SSL001 相同，只需进行一次登入 SSL 入口网站，后续再登入应用服务，SSL001 即可自动完成登入，节省登入动作，提高用户工作效率。

操作步骤：

进入 SSL001 管理端画面，由菜单选项中点击 SSL VPN > 群组管理。

认证管理项目上，点击 新增认证服务 按钮，跨出页面，在这里可依需要选择不同的认证服务，包括：本地认证 LOCAL DATABASE 或连接外部服务器：RADIUS、Active Directory / LDAP / NT Domain。这里选择 Active Directory，填入既有的 Exchange Server 的 AD 认证服务器识别名称及 IP，送出。

用户管理项目上，选择需要套用外接 AD 认证服务器的用户群组，这里选择具有全功能权限的 All Users 群组样版，并激活此群组；指派外接 AD 认证服务器作为认证服务，使用者数据库选择 使用内建的使用者数据库。

注意：在成功增加群组后，切记要激活每一个群组，否则这个群组的用户是无法在远程登入 SSL VPN 的。

点击 确定 按钮，即完成 SSL VPN 建置。只要在 AD 认证服务器上建置有帐户，即可以相同的用户名及密码登入 SSL VPN，并享有全功能服务权限。

2. 进阶设置：预置样版修改应用

上述超快速完成 SSL VPN 建置，可快速让公司内所有成员开始使用 SSL VPN 的服务，但只套用同一个用户群组，拥有相同的资源使用权限；若是如 DEMO 公司需要建置四种不同权限的用户群组，将每个群组分级管理，不同群组拥有不同权限、登入不同的操作界面，以上的快速建置结果就不能满足 DEMO 公司需求，这就需要更进一步的设置。

Qno SSL VPN 提供系统预置的四个群组模版，用户可以依需要套用模版，并针对实际需要作细部修改，如：认证服务、使用者、服务资源等配置内容。如此简化配置，加速企业 SSL VPN 上手。

我们先针对 DEMO 公司编制内员工需要用到 SSL 服务的高层、业务、外点销售三个群组设置进行说明。这三个群组可以对应套用系统预置的 Supervisor（高管群组）、Mobile User（移动用户群组）、Branch Staff（分公司人员群组）群组模版。

以下先来进行介绍外点销售群组的设置步骤。

操作步骤：

进入 SSL001+管理端画面，由菜单选项中点击 SSL VPN > 群组管理。

首先新增 DEMO 公司既有的 AD 认证服务器。于认证管理项目上，点击 新增认证服务 按钮，跨出页面，认证服务形式选择 Active Directory，填入既有的 Exchange Server 的 AD 认证服务器识别名称及 IP，点击 送出 按钮。

点选对应 DEMO 公司外点销售群组对应的系统内置 Branch Staff 群组，认证管理指派为外接 AD 认证服务，选择 使用内建的使用者数据库。

以下是系统预置 Branch Staff 群组默认的服务资源，具有 WEB、FTP 网络服务及 ERP 几项服务内容。

很明显的，Branch Staff 群组系统默认的服务资源并不完全符合 DEMO 公司规划的外点销售群组的的应用资源权限，在此我们可以点选 Branch Staff 群组，修改其服务资源，以符合 DEMO 公司规划外点销售群组的服务资源内容。依据 DEMO 公司规划，外点销售群组具有网络服务及终端全部服务。故另勾选网络服务及终端服务的所有选项，提供网络服务及办公软件应用等终端服务。至此完成外点销售群组设置。

注意：终端服务可以依据需求，仅勾选群组用户需要的项目。

接下来进行高层群组的设置。点选对应高层群组的内置模版 Supervisor 群组，同样指派 AD 认证服务器，但在使用者数据库选择 自定义使用者数据库。

在使用者管理项目上，网管需要对照 AD 服务器实际用户名依序新增高层群组用户，存在 Exchange Server 上原本的 AD 帐户其它的权限设置内容也还是同时存在。公司内同一个用户只有一个认证帐号，让网管达到集中管理、简单管理的目的。

于使用者管理项目上，点击 新增使用者 按钮。

跨出页面，网管可设置用户名称、密码、到期日、没有动作强制注销时间等。设置到期日及强制注销时间，时间一到，该帐户及无法登入或强制注销，避免内部网络被恶意入侵。到期日若不设置日期，则表示帐户永久有效。每增加一个用户即点击增加到对应列表按钮加入。持续完成所有的帐户设置后，点击 确定 按钮送出。

注意：务必要对照既有 AD 服务器实际用户名建置群组用户，否则 AD 认证服务无法辨识用户名称，远程用户将无法取得身份认证。

回到主页面，点选 Supervisor 群组，勾选所属的所有用户名。

服务资源上，勾选高层群组用户所需要的全功能服务资源。

同第 5~8 步骤，进行套用 Mobile User 预置群组的业务群组设置。至此完成高层及业务群组的设置内容。

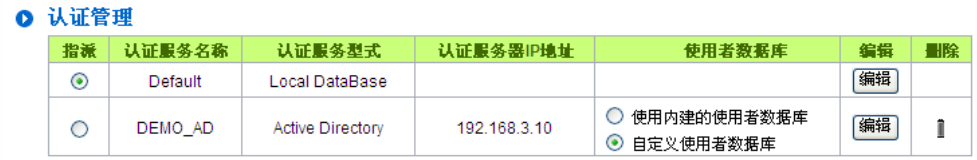
3. 高级设置：完全自订设置

接下来，我们将进行外部用户供应商群组的设置介绍。非公司编制内成员，需要额外增加的外部帐户，则采用系统默认的 LOCAL DATABASE 本地认证，一一建置使用者帐户，后续再依据需求配置服务资源。

操作步骤：

新增供应商群组，并激活此群组。

认证管理项目上，选择系统默认的 LOCAL DATABASE 本地认证。



用户管理项目，点击 新增使用者 按钮，新增供应商帐户。跨出页面，网管可设置用户名称、密码、到期日、没有动作强制注销时间等。设置到期日及强制注销时间，时间一到，该帐户及无法登入或强制注销，避免内部网络被恶意入侵。每增加一个用户即点击增加到对应列表按钮加入。持续完成所有的帐户设置后，点击 确定 按钮送出。

回到主页面，点选供应商群组，勾选所属的所有用户名。

使用者管理

指派到这个群组	使用者名称	编辑	删除
☑	A公司	编辑	
☑	B公司	编辑	
☑	C公司	编辑	

服务资源管理上，勾选供应商需要的 ERP 终端服务。如此供应商在客户端登入画面，只会看到 ERP 终端服务选项，避免对外开放太多资源，容易有被恶意入侵的风险。

终端服务			
☐	Word	☐	Excel
☐	PowerPoint	☐	Access
☐	Outlook	☐	Internet Explorer
☐	FrontPage	☑	ERP

其它设置操作：

新增/删除终端服务项目：若是需要另外新增/删除终端服务项目，可由菜单选项中点击 SSL VPN > 服务资源管理。

服务资源配置

资源名称	服务	服务器地址	编辑	删除	状态
Word			Edit		Disabled
Excel			Edit		Disabled
PowerPoint			Edit		Disabled
Access			Edit		Disabled
Outlook			Edit		Disabled
Internet Explorer			Edit		Disabled
FrontPage			Edit		Disabled
ERP			Edit		Disabled

新增微软终端服务

在服务资源配置项目中，网管可以增加或删除终端服务应用程序。点击 新增微软终端服务 按钮，在跳出的页面中，输入应用程序描述、所在路径、执行路径、服务器地址，再为应用程序选用一个程序图标，按下送出就完成了一个新应用程序的增加。当然，要增加的服务一定是企业服务器所开放提供

的，不然，加了程序，也无法应用，那就多作无用了。若使要删除某一个终端服务，只需要点击对应的代表删除标示垃圾桶即可。

服务资源书签设置：为方便用户使用资源，网管可以在这里设置好书签，让用户无需记忆相关登入服务器设置数据，即可于用户界面中直接开启服务。点击 为此群组建立服务资源路径书签，输入书签名称、IP 地址、并选择所要建置书签的服务。这里举例为 FTP 服务书签。

安全隧道服务客户端 IP 范围设置：若是远程用户会需要使用到安全隧道服务，网管需要设置提供给外部接入的 IP 配发范围。由菜单选项中点击 SSL VPN > 高级设定。

在安全隧道项目中，点击 IP 整合管理按钮，在跳出的页面中可依需要设置客户端接入的 IP 分配范围，这里需要与实际内网配置的 IP 范围区隔开，以避免发生 IP 冲突。

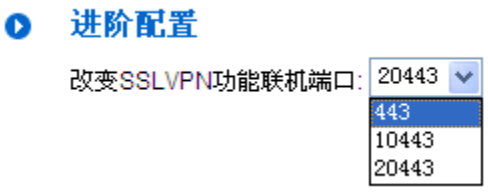
在 IP 整合管理页面中，还可便利管理其它 IP 项目。设置完毕点击确定按钮。

客户端欢迎词及资源名称设置：SSL001+提供企业可于 SSL 入口网站设置对登入用户的欢迎词及站台

名称。由菜单选项中点击 SSL VPN > 服务资源管理。

在标题项目中，可设置客户端登入界面的欢迎词及资源名称。网管在这设置企业名称为 DEMO，资源名称为 SSL VPN PORTAL。

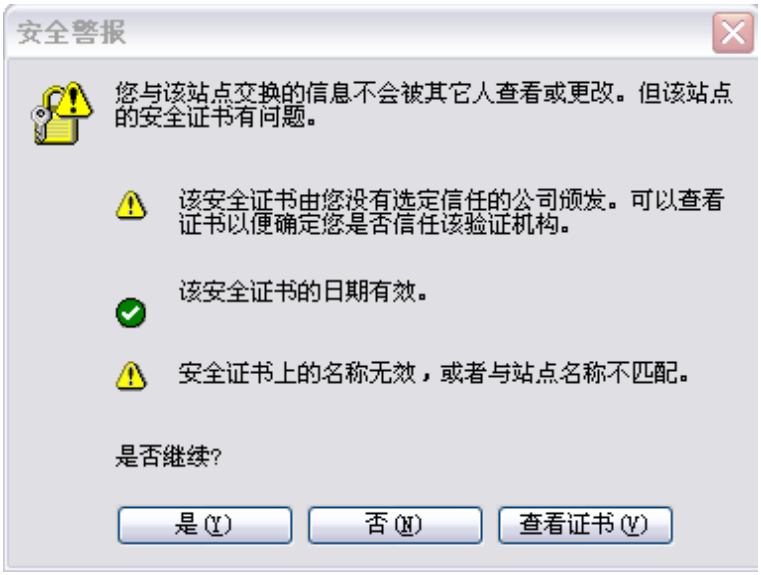
VPN 联机端口更改设置：Qno SSL VPN 支持更改 VPN 联机端口功能。如默认端口 443 被其它服务占用或被 Forwarding 到内网的某台机器，造成 Qno SSL VPN 无法联机，那么网管可以在高级设定菜单中更改联机端口为 10443 或 20443 进行联机。



现在，DEMO 公司网管员已经对不同的使用者群组配置好使用权限及相关的设置。接下来，看看远程客户端如何使用 SSL VPN 服务进行企业内部数据存取。

远程客户端

打开 IE 联机 Qno SSL VPN，跳出安全性警讯表示您正透过 SSL 的加密保护，点击“是”即可进入 Qno SSL VPN 入口网站登入画面。



登入画面，用户使用登入身份认证用户名/口令登入 Qno SSL VPN。支持软键盘输入。

权限不同，不同使用者看到的会是不同的登入界面。左侧功能列表与中心页面的功能清单，会因使用者不同面显示不同的内容。

高层群组用户可以使用全部五大类的服务项目。

业务群组用户可使用网络服务、微软应用程序、远程桌面服务等三项服务。

外点销售群组用户可使用网络服务、微软应用程序等两项服务。

供应商群组用户就只可使用微软终端服务单项。

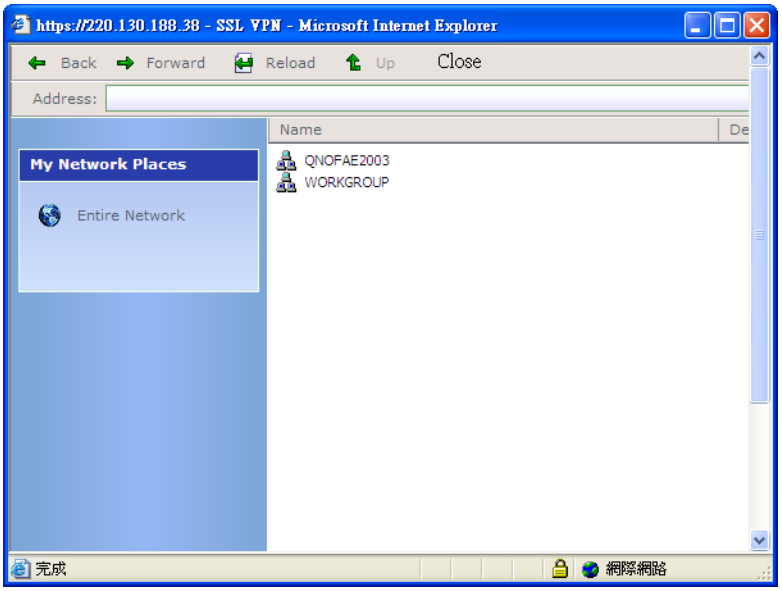
网络服务：登入 SSL 入口网站后，远程用户只要直接点选服务图示即可开启使用。例如点选 FTP 服务，浏览器会自动开启并联机到企业内部 FTP 服务器。

前面在管理端，网管可以为用户设置资源路径书签，在客户端界面，用户也可以自定义书签。点击 自定义书签 按钮，在跳出的页面中，输入书签名称、IP 地址和服务，点确定保存，这样下次再登入 SSL 入口网站，直接点选此书签即可，免去每次使用相关服务，都要一而再的输入服务器名称或 IP 数据。

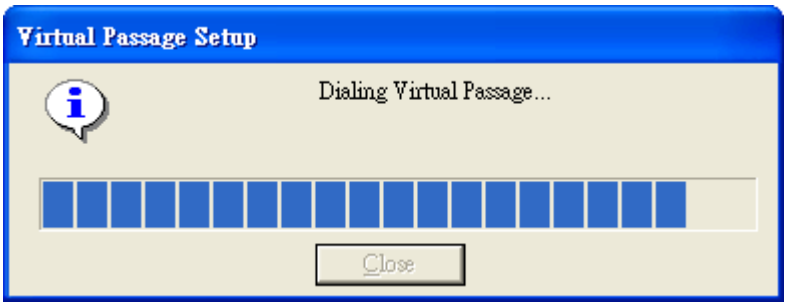
微软终端服务：点开 WORD 应用程序，出现的页面中可选择窗口大小，点确定后可以直接进行编辑文档。文档完成后还可以直接用 OUTLOOK 寄发，实现轻松办公。

远程桌面服务：可提供远程用户连入公司，使用自有计算机。计算机需要开机才可使用。

在线网络邻居：远程用户于公司自有计算机不需开机，也可使通过在线网络邻居服务连入，使用公司内部资源。

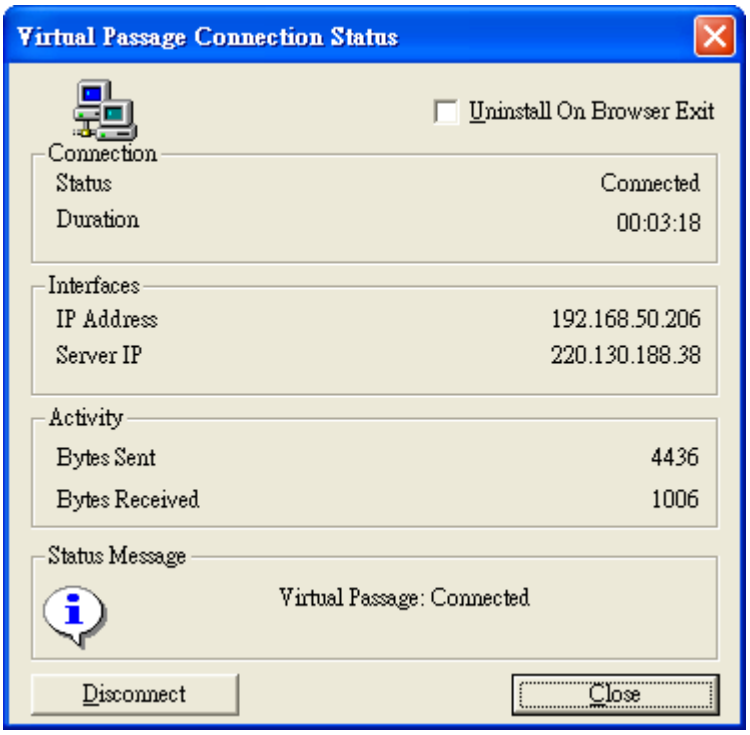


安全隧道：对于建立 VPN 安全隧道，Qno SSL VPN 产品提供了快速安全的一键连接方式，可建立基于 SSL 的 IP 隧道。点击安全隧道连按钮，不需要任何设置，快速建立隧道。



当 VPN 隧道连接成功，会在右下角任务栏中显示隧道联机图标。

点击隧道联机图标，可以看到 VPN 连接的状态信息。



当用户使用完毕 SSL VPN 服务，点击退出按钮即可断开服务。当点击退出按钮后，跳出删除记录警告提示，选择“是”删除使用记录，可确保资料信息安全。

综观上述，Qno SSL VPN 在其简易使用性及安全等级上，于互联网迅速扩展，针对远程、安全、动态登入的需求日益提升的时代，都是各种企业使用者最理想的选择。其建置、维护及大量散布的低成本更是吸引企业的优势！侠诺 SSL VPN 系列新产品分有低中高端不同的产品层次，让需要 SSL VPN 的企业有了更多的选择，有意的企业用户可拨打侠诺免费业务咨询专线：400-886-9850 或联系 Qno 侠诺当地代理商，详情请登录 Qno 侠诺官网 www.Qno.cn。

五、案例参考

侠诺 SSL VPN 部分用户案例展示

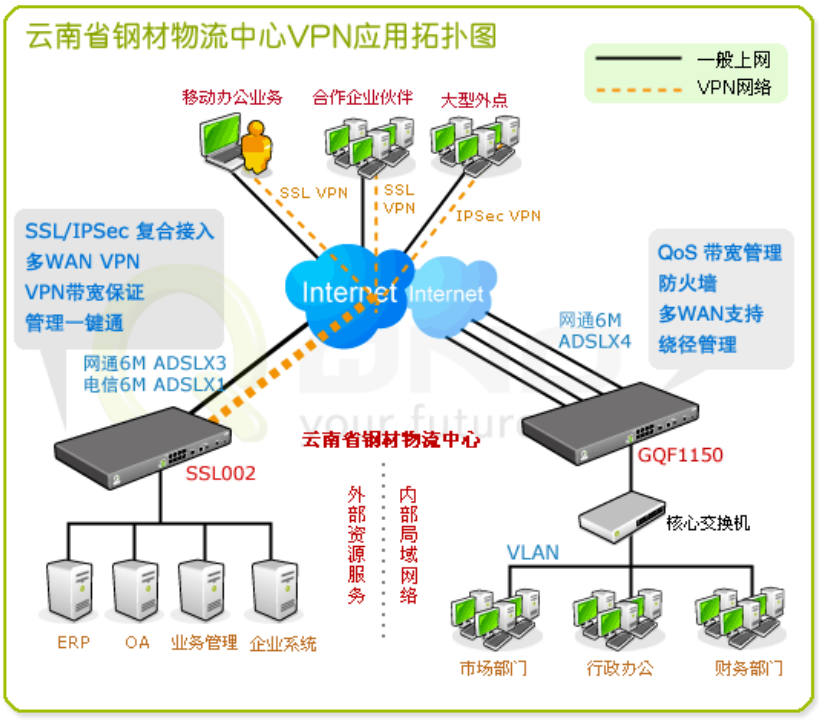
VPN 的迅猛发展之势有目共睹，国内市场已达到数十亿，尤其是目前比较流行的具有零用户端安装、适合移动用户等特点的 SSL VPN 设备，其应用扩张的步伐最为迅猛，拿知名网络设备厂商侠诺科技来说，所推出的适用于中小企业的 SSL VPN 系列产品，已经被广泛应用于连锁销售、连锁房地产、交通运输等行业，并在企业运营中发挥了不可替代的作用。通过以下诸多案例，可以看到 SSL VPN 已经成为新一代 VPN 的主流之选。

1、物流行业:云南钢材物流中心

云南钢材物流中心，由云南物流产业集团所属的云南省金属材料总公司投资建设，是于原“云南省钢材市场”的基础上实施改扩建而打造出的云南省大型的综合服务型钢材物流中心。云南钢材物流中心创建了云南省内首个技术较为先进、功能较为完善的集交易、融资、信息、仓储、加工为一体的大型专业化钢材物流平台，与同属云南省金属材料总公司的多家子公司及省内其它企业合作关系密切。为更有效的管理交易、运输等业务资源，加强合作伙伴间的联系，云南钢材在寻求一种安全、高速、智能且经济性较强的新企业 VPN 网络，希望凭借高速运转的信息化网络，能够轻松而高效的管理庞大的业务资源，增强市场竞争力，使云南钢材成为物流集团中最具竞争力的内核企业。

该中心目前大概有 20 多名移动办公的业务员工，关系来往密切的合作伙伴有 10 多家，且还有 3 个大的企业外点，也希望能与总部进行 VPN 连通实现资源共享。如何有效集成企业资源，加强信息共享渠道，实现安全稳定且可扩展的多点全网 VPN，这是规划构建云南钢材的企业 VPN 网络时必须要考虑的。

[方案]



图：云南省钢材物流中心 SSL VPN 互联网络应用拓扑图

云南省钢材物流中心本部作为中心端，统筹内外运营事宜，需要具备更优秀的网络环境，因此建议将其分为两部分。中心本部内部上网，采用了侠诺新一代千兆共享产品 GQF1150，四条 6M 网通 ADSL 汇聚接入，下接内核交换机连接到各部门 PC 提供局域网上网服务。并通过 VLAN 划分不同的子网，有效防止病毒传播的同时，也便于内网用户的管理。而对于外部资源访问服务等，则采用了侠诺 SSL/IPSEC 复合式防火墙 Qno SSL 002 作为中心端接入设备，ERP、OA、业务管理等系统服务器直连 SSL 002，提供微软终端、远端桌面、VPN 网络等信息远端共享服务。中心端网管根据远端用户不同的身份，划分不同的群组，以设置许可权区隔，达到保护机密信息资源的目的。

对于钢材市场的业务人员及企业合作伙伴来说，可采用 SSL VPN 方式接入，无需安装用户端即可轻松安全的远端存取企业服务资源。目前云南钢材正在全省范围内网络布点，规划中相对较大型的分支外点，可以同时采用 IPSec 或者 SSL VPN 方式，灵活调整。

[效果]

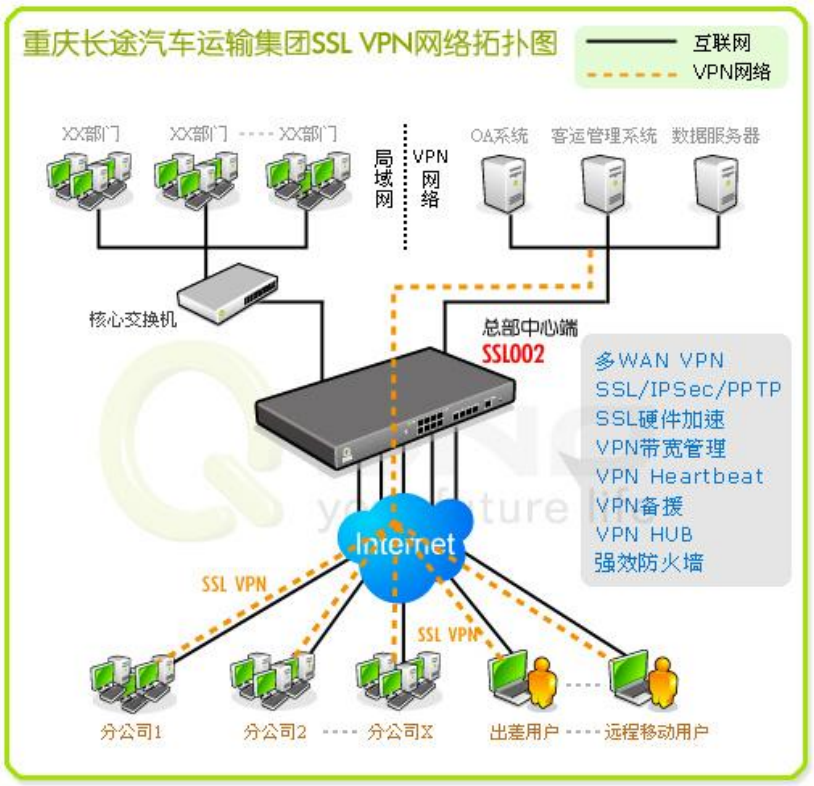
云南钢材市场正全面实施省内网络布点，侠诺 SSL 002 功能全面，体现出其安全、极简、快速等多项优异特色，在后续增加网点时一样会设置简易，便于访问与管理。由于多 WAN、备援及良好的硬件效能等使得该中心全网 VPN 稳定的运行，充分解决了以往应用 IIS 服务器不稳定的情况，大大提升了业务管理效能。另外，管理/联机一键通等诸多智能极简化的功能设置，及暂存资料清除、超时自动退出等保护措施，防火墙、带宽管理……这些优秀的功能设计让 SSL002 成功地为云南钢材市场构建了一个简便、快速、稳定、安全的企业信息全网 VPN！

2、长途汽运:重庆长途汽运集团

重庆长运集团始建于 1958 年 7 月，在重庆主城区、永川、江津、合川、黔江等区县设有 20 多个分公司（其中：汽车客运站 18 个。一级站 3 个，二级站 9 个，三级站 4 个，四级站 2 个），客运班线 400 多条，营运范围近至重庆辖区，远至上海、浙江、福建、广东、湖北、贵州、云南、四川、西藏等省市、自治区。是集“汽车修理、物流仓储、汽车销售、油料销售、驾驶培训、房产开发、宾馆酒店”为产业链一体化经营的市属国有道路运输骨干企业。

诸如重庆长运集团的交通行业，其网络系统建设本身是一个庞大、复杂、 动态的系统工程，边应用边扩展、集成内部资源进行统一的集中式管理、维护工作要容易修改、尽可能体现经济性原则等需求，使 SSL VPN 具有很大的发挥空间，它能使有限的资源发挥出更大的作用， 使交通行业的网络建设以最小的投入获取最大的效益。

[方案]



图：重庆长途汽车运输集团 SSL VPN 网络拓扑图

在总部，它采用了侠诺 SSL002（支持 SSL/IPSec/PPTP 三种 VPN 协定）作为内核 VPN 网关，分公司人员、移动人员等各种用户，只需具备普通 ADSL 上网环境，而不需要另外的 VPN 硬件，就可采用 SSL 流览器窗口登陆的方式与总部联网，总部中心端网管可对外点和移动用户进行统一的管理。侠诺 SSL002 以强大的硬件系统为前提，除了双核 CPU，内置有强效防火墙，免去了再购买安全防火墙的费用。同时也可作为总部内网的普通网络应用网关，用 VLAN 将内网与 VPN 网关分隔开来，既方便

管理也有利于 VPN 网络总部中心端的服务器数据的安全。

[效果]

重庆长运集团部署的侠诺 SSL VPN 产品 SSL002，专门应用于整个客运系统。通过将 SSL VPN 与客运管理系统进行集成，总公司内部、分公司、分支售票点等工作人员不需要任何软硬件安装，就可以随时查看客车票务、车次等信息，更好的服务客运旅客。同时，解决了出差人员、高管移动办公等问题，使得在外工作人员能方便安全的获取、交换数据信息，不仅节省成本，还打破了时间、空间的限制，大幅提高工作效率。

3、连锁教育：深圳动感蓝天连锁教育

动感蓝天教育是 2003 年经深圳市文化主管部门批准的中小学校外培优机构，是深圳教育大发展的产物。7 年来，办学规模不断扩大，现已开设包括一个园岭教学总部及百花、石厦、景田等了 11 个教学点，教学场地 10000 余平方米，在校学生 4000 多名，专职教师 200 余名。形成了从小学到高中全覆盖的教学格局和多学科并举的课程体系。面对信息化网络应用的趋势及学校当前良好的发展机遇，动感蓝天教育为了实现“信息化教育”的目标，目前架设了对外 WEB 网站和内部办公 OA 两个服务器系统，提供相应的对外 WEB 服务及内部各地教学分部使用。

由于教学分点的不断增加、移动人员的办公需求及学生家长的访问需求，普通的 IPSec VPN 已无法满足该教育机构的应用需求，在考虑安全、稳定、便利灵活的基础上，动感蓝天教育选择了侠诺复合式 SSL VPN，从而将多个校区的教育点、移动办公及学生家长全面快速的联接起来，形成高稳定高效能的教育服务系统网。

[方案]

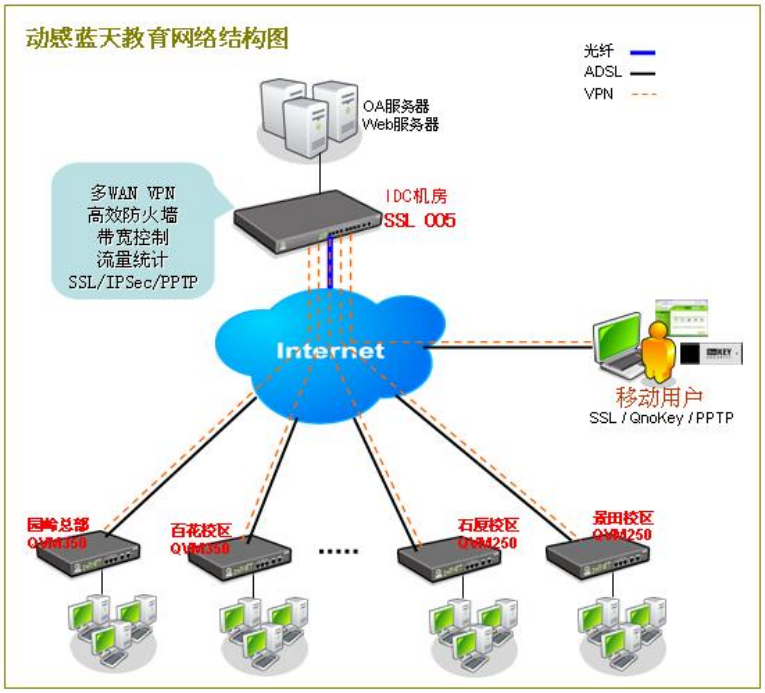


图:动感蓝天教育 VPN 组网图

在该方案中,托管在机房的 WEB 网站对外提供服务和内部办公 OA 软件仅供各地教学分部使用，考虑高性能转发和高强度的稳定需求，因此采用侠诺 SSL 005 VPN 防火墙作为 VPN 设备，实现各地网络互联 VPN 网络，联网使用。园岭总部规模结构大约 60 台电脑，两条 4M 的电信 ADSL 宽带，采用 QVM350 作为 VPN 网关接入设备，可满足较多的 VPN 连机需求。其它教学分部则采用侠诺 QVM250 作为 VPN 网关接入设备。每个教学点均通过侠诺设备设置流量管控,确保防止个别人员占用带宽过多,确保办公电脑能正常连接内部 OA 软件和总部做资料共享。而一些学生家长及移动办公用户可选择 SSL/PPTP/QnoKey 等方式灵活接入到网络。针对接入 VPN 网络的电脑均通过 ARP 智能双绑功能进行绑定，有效防止 ARP 病毒攻击的影响。

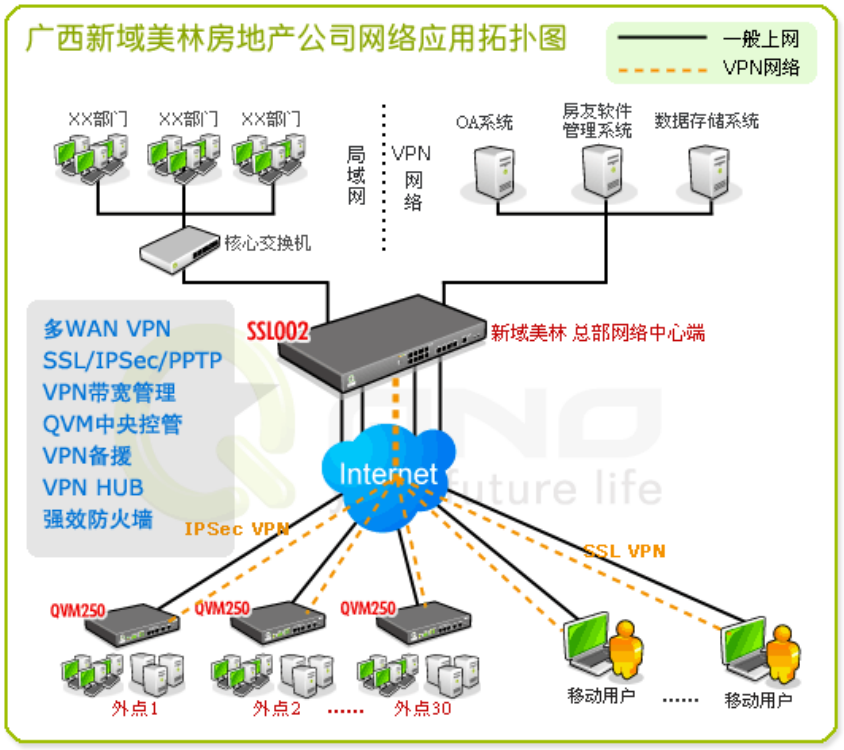
[效果]

Qno 侠诺 SSL005 产品特有的流量控管功能和稳定性需求为动感蓝天教育的主要网络需求，同时由于其采用 MIPS64 位双核 CPU 的网络处理器，可以提供高效能。作为连接全网 VPN 的网络设备，具备稳定性很好，使用起来很容易，更为人性化的特点，让网络管理工作省心又省力。通过 SSL VPN 组网，动感蓝天教育实现了各地教学分部实时通过 OA 办公软件办理学生的入读和缴费等工作，园岭总部与各教学分部办公电脑高速连网使用，达到数据资料同步的信息教学目的。并且，可针对不同级别的使用者设置不同的流量控制效果及使用资源，以保证网络的稳定及资料的安全，该组网方案完全能满足动感蓝天教育日常的教学服务等网络需求，有效促进该教育机构的运营及发展。

4、连锁房地产：广西新域美林连锁房产公司

广西新域美林房产置业有限公司，是南宁市一家专业代理楼盘租、售业务及一手楼盘行销策划的房产中介公司。经过多年的发展，新域美林建立了辐射南宁市区的店铺网络，数量已达 30 家之多。目前新域美林对信息化依赖程度比较高，包括业务系统、OA、CRM、计划管理等全部实现网上办公。员工可以在任何时间与地点利用 Internet 处理公司业务，实现从酒店、网吧、随身携带的电脑或其它无线设备上安全访问公司内部网、收发电子邮件、进行文档共享或调用内部应用系统和数据。新域美林的信息化系统不仅服务本公司管理人员和普通员工，还可为广大的业主为其提供便利(例如房屋信息查询、会员情况、网上交易等)。这时，SSL VPN 具有的节省成本、用户终端易部署、适合出差等移动用户的特性，可以更高效的结合信息化软件，可以使得企业运作效率达到最大化。广西的新域美林房地产公司，就是利用 SSL VPN 网络进行快速扩张的一个成功典型案例。

[方案]



图：广西房地产业拓扑图

“新域美林”采用了专业化的房友信息管理软件，以对企业信息进行集成化的管理。在总部，它采用了侠诺 SSL002（支持 SSL/IPSec/PPTP 三种 VPN 协定）作为内核 VPN 网关，30 个固定的分支外点部署了侠诺的 QVM250，而对于出差等移动工作人员，只需具备普通 ADSL 上网环境，而不需要另外的 VPN 硬件，就可采用 SSL VPN 的方式与总部联网，总部中心端网管可对 30 个外点和移动用户进行统一的管理。SSL002 内置有强效防火墙以保证网络的相对安全性，免去了再购买安全防火墙的费用。同时，SSL002 以强大的硬件系统为前提，也可作为总部内网的普通网络应用网关，用 VLAN 将内网与 VPN 网关分隔开来，既方便管理也有利于 VPN 网络总部中心端的服务器数据的安全。

[效果]

SSL VPN 的零用户端的特性，使得远端用户端不需要安装任何硬件设备，只需总部安装一台侠诺 SSL002，就可以通过网页浏览的方式访问总部 VPN 服务器数据。企业将需要的数据集中管理，业务人员可随时通过灵活的访问方式，掌握客户数据与目前即时房屋销售数量状况。由于侠诺 SSL002 支持 SSL /IPSec /PPTP，因此可采用任意一种接入方式接入互联网即可构建 VPN 系统，当未来的新门店扩张时可结合当地的实际情况灵活选择价廉物美的接入方式构建 VPN，不受地域、运营商等的限制，甚至可全球扩张。“新域美林”就根据不同的外点需求，选择不同的 VPN 接入方式，成功实现了将 IPSec VPN、SSL VPN 与自身需求完全集成在一起。更多信息请访问侠诺官网 www.Qno.cn，或是拨打免费业务电话 400-886-9850。

六、服务与支持

郑重提示：全国各地区销售渠道结合产品销售及技术支持功能，只有通过所属地区的销售伙伴才能得到完善的技术支持及配置指导。请广大用户务必向就近的侠诺所属经销商购买产品，以保障您的权益！

侠诺与各地区的销售代理商共同合作，提供的服务和支持包括：

用户购买产品之前对相关的技术方案、应用特点、产品选型等方面的免费咨询；

部分代理商提供的产品试用、测试，在损坏维修期间为用户提供备用机；

与购买产品的相关的三包企业责任与义务，如一定期限的退货换货、保修期等；

使用手册、产品软件等的免费下载服务；

可提供上门安装、设置等售后服务；

随时随地的在线 QQ、MSN、邮件、论坛、以及电话技术支持；

产品不定时的软件优化与升级，不收取任何费用。

以下为相关服务的联系方式：

业务咨询:

大陆总部：	苏州苏络电子科技有限公司
网　　址：	www.qno.cn
地　　址：	江苏省苏州市珠江南路 368 号 1119 室
电　　话：	0512-66556887
传　　真：	0512-66556578
台湾公司：	台湾新竹市埔顶路 25 号 10 楼之 2(德安科技园区五期)
网　　址：	www.qno.com.tw
电　　话：	+886-3-5678100 ext.8104
E - mail：	QnoSales@qno.com.tw

技术支持：

电　　话：	0512-66556887
电　　邮：	QnoFAE@qno.com.tw
MSN：	fae@qno.com.tw
QQl：	394743194