侠诺 VPN 助力江苏常松机械集团网络组建

一、用户背景介绍

江苏常松机械集团有限公司位于江苏省常州市市中心，创建于 1991 年，是工贸一体的集团型股份制企业。公司主导产品包括工程机械（装载机）、彩色钢板、镀锌板、塑料机械、内燃机配件等几大系列。 公司于常州有一号及二号两个分厂，在上海及江阴都设有分公司。

常松集团本着“以科技为先导，以质量为中心，不断创新，向用户提供满意的产品和服务”的质量方针，经过十几年的努力发展，先后荣获“国家二级企业”、“省级先进企业”、“AAA 级资信企业”、“工商免检企业”、“重合同守信用企业”、“江苏省优秀民营企业”、“常州市知名商标”等荣誉称号，并通过 ISO9001：2000 版质量管理体系认证，QS9000、ISO/TS16949 质量体系认证。

公司内部以及各分支机构网络以前一直在通过 D 牌 804 型号产品作为 VPN 网关，运行多种企业应用程序，如内部文档共享服务、ERP 系统以及 PDM 数据库服务器。随着企业规模的不断扩大，该产品已经无法满足企业应用需求。

二、用户需求

常松集团提出以下网络建置需求：

1、实现常州总公司内部局域网互联，分公司、各分支机构和办事处的内部局域网互联；

2、客户、合作伙伴或分公司可以安全访问公司授权访问的企业内部网络资源；

3、常州总部保证至少 100 台计算机连入国际网络，考虑到公司以后的发展接入信息点的增加，同时实现各分公司通过相关设备连接到总部网络，同时还内建 SQL Server 数据库服务器，提供相关数据服务，建立 ERP 服务器，提供公司财务，人事管理、添加和修改相关信息等要求；

4、上海、江阴分公司保证至少 50 台计算机联入国际网络，常州 1-2 号分厂保证至少 20 台计算机联入国际网络；还要考虑到公司以后的发展接入信息点的增加，同时与总部实现互联。访问公司总部 SQL Server 服务器，PDM 服务器；提交、查询和修改数据库相关信息。连接公司金蝶 K3 ERP 系统提交、查询与修改相关信息等要求；

5、在各分支机构和总公司之间创造一个集成化的办公环境，为工作人员提供多功能的桌面办公环境，解决办公人员处理不同事务需要使用不同工作环境的问题；

6、支持不同部门间信息传递，解决由人工传送纸介质或磁介质信息的问题，实现工作效率和可靠性的有效提高；

7、通过路由器对用户实行统一管理，对访问许可权实行分级管理等要求，实现流量控制、埠镜象等要求，通过路由器的相关防火墙功能实现网络的安全管理。

针对用户的需求 侠诺科技工程师建议通过 VPN 的配置可以解决互联问题 另外对 VPN 加以带宽管理及内部权限控管相应配置可以实现数据传输的安全性问题。

三、设备要求

根据江苏常松机械集团有限公司用户的需求，对于 VPN 设备的选择，必须严格遵循着方便实用、高效低成本、安全可靠、网络架构弹性大等相关原则来选择 VPN 设备网络设备。下面就用户需求情况总结选择设备的几个要点：

1、所选用硬件 VPN 网关，保证能安全、方便、快捷地进入，并能够访问指定的内部网络资源和服务；

2、总公司和分公司网络建立 VPN 加密隧道，确保数据传输安全， VPN 设备须具有高稳定性和高可靠性，以保障信息网络的正常运行；

3、支持以 ADSL 线路基础的经济型的全动态 IP 地址 VPN 组网方案，并具有 DHCP 功能，以实现局域网自动分配 IP 需求；

4、对本地内网实施上网的访问控制，通过 VPN 设备的访问控制策略，对内网 PC 进行严格的访问控制。如：为确保安全性，可对允许上网的 PC 进行 IP 和 MAC 绑定，并通过 VPN 网关中的安全策略设置对这些 PC 的数据流程进行状态检测，以确保不能被仿冒；也可以使用产品中的“用户上网认证”功能，使用户在使用流览器上网流览时，首先要通过闸道的访问密码认证等；

5、对外网可以抵御黑客的入侵，起到 Firewall 作用。其自身强大的全状态检测 Firewall 功能和 IDS 抗攻击微引擎，将对内网实施有效保护。另外，如果已经部署了 Firewall 也可和 Firewall 一起，构成两道网络防护屏障，为以后进一步加强总部内网的安全留下发展的空间。须具有控制和限制的安全机制和措施，应具备防火墙和抗攻击等功能；

6、具备完善的带宽管理功能，将网络出口带宽合理地分配给隧道流量（业务数据）和其它网际网络流量（浏览、邮件等）；

7、整个公司 VPN 网络的建立，必须统一规划全网的 IP 地址。对总部以及各分支机构的网络节点的 IP 地址要进行统一规划，对各个功能子网段做明确划分，通常以“满足目前需求，保留一定的扩展性”为原则，整个 VPN 网络内部的 IP 地址不能有冲突；

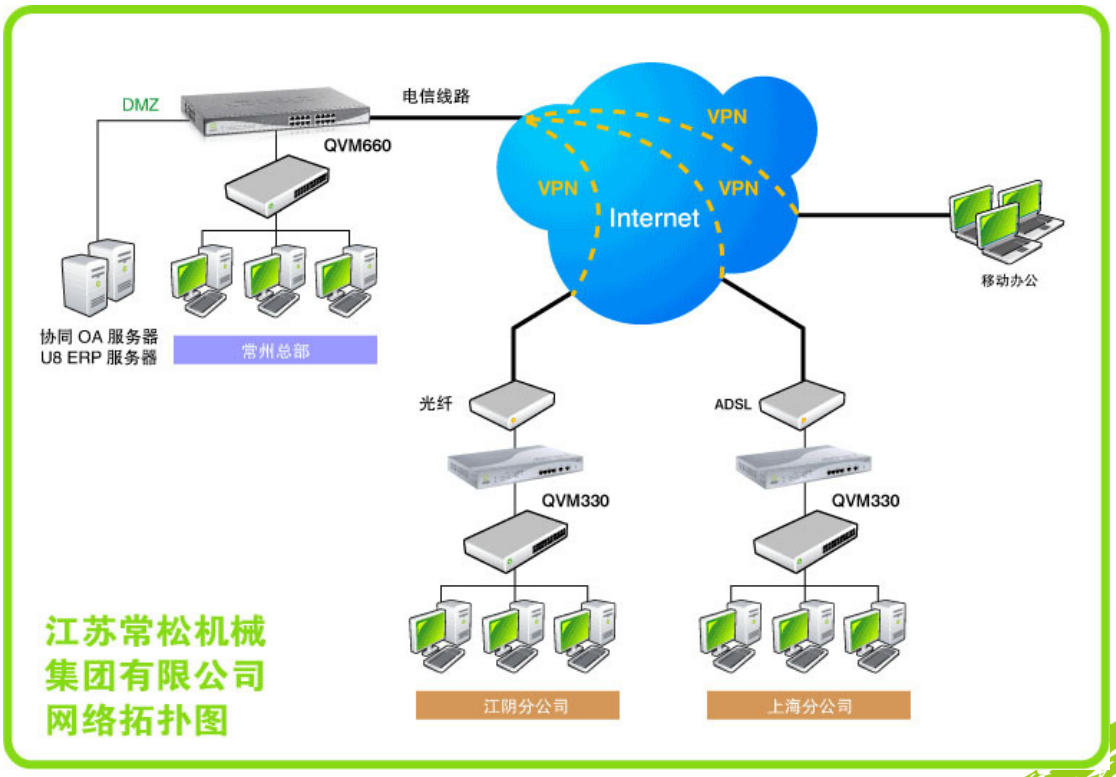
8、部署灵活，维护方便，提供强大的管理功能，以减少系统的维护量以适应大规模组网需要。

现在时下的 VPN 产品繁多，而且功能各不相同，由 Qno 侠诺常州地区代理商——常州程锦网络公司，通过上述用户要求，建议在选选择 VPN 连接设备上推荐侠诺科技的 QVM 系列 VPN 防火墙路由器。

QVM 系列 VPN 防火墙路由器产品内建进阶型防火墙功能，能够阻绝大多数的网络攻击行为， 使用了 SPI 封包主动检测检验技术(Stateful Packet Inspection)，封包检验型防火墙主要运作在网络层，执行对每个连接的动态检验，也拥有应用程序的警示功能，让封包检验型防火墙可以拒绝非标准的通信协议所使用的链接，默认自动检测并阻挡。QVM 系列亦同时支持使用网络地址转换 Network Address Translation (NAT)功能以及 Routing 路由模式，使网络环境架构更为弹性，易于规划管理。

此外，Qno 侠诺另有领先于业界的独家 QVM 功能，独有 SmartLink IPSec VPN 设定，只需输入 VPN 服务器 IP、用户名、密码即可自动完成 IPSec VPN 建置，直接进入路由器 QVM 功能设定用户端与 QVM 服务器进行虚拟私有网联机，或是设定为 QVM 服务器功能接受用户端的虚拟私有网联机，支持备援功能，断线可从另一个 WAN 自动建立联机。

四、VPN 网络设计以及网络拓扑结构



江苏常松机械集团有公司网络应用拓朴图

在了解集团整个网络状况和集团领导要求后，考虑到下一代网络业务（VOIP，网络视频会议）对带宽的要求，决定采用台湾侠诺 QNO QVM660 VPN 防火墙作为集团总部的 VPN 网关，同时接入电信 10M 光纤一条；江阴分公司/常州 1-2 号分厂各接入电信 10M 光纤一条，上海分公司接入电信 ADSL 宽带一条；鉴于各分公司的规模，均采用 QNO QVM330 作为接入端的 VPN 网关，QVM660 和 QVM330 都具有多 WAN 口，为以后分公司的 VPN 链路备援和带宽增加提供了升级条件，保障了客户的投资； QNO QVM 系列的 VPN 路由器具有的 VPN Smartlink 功能让原先 VPN 相关的 23 个参数设置简化成 3 个参数，在公司总部即可观察和修改分部的 VPN 设置，极大的减少了网管的工作量。

常州总部：100 信息点接入，选用 QVM660；

上海 江阴分公司：50 信息点接入，逐步更换成 QVM330；

常州 1-2 号分厂： 20 信息点接入，逐步更换成 QVM330；

五、方案达到目的

常州总部与上海 江阴分公司，常州 1-2 号分厂透过 VPN 联机采用 IPSec 协定，确保传输数据的安全；

1、多 WAN 口的设计，可根据不同带宽的需求，也可同时满足 VPN 备援的功能，提供多一层的安全保障。公司领导对于 VPN 联机要求高度稳定，即使断线也要立即接回，不影响正常运作；

2、管制内网用户上网行为，内网用户使用 BT、点点通影响其它人上网或限定时间管制上 MSN、QQ、或上网；

3、解决了疾风病毒及蠕虫毒病所苦，通过 QVM 系列的路由器的设置解决了网速因被黑客攻击而受影响或内网用户常被疾风病毒及蠕虫毒病的侵扰。

六、效果评测与扩展建议

应用侠诺科技的 QVM 系列产品及其解决方案 1 个月以来，江苏常松机械集团有限公司的网络管理人员表示比较满意，网络运行良好。特别是 QNO VPN 路由器的一些人性化设置非常方便（比如一键封 QQ、弹性 QoS 流量控制），很好的对企业员工进行了权限控制，另外现在分公司连接公司 ERP 系统提交、查询与修改相关信息非常方便，与各分公司业务往来再也不用花费更多的时间了。

在网络扩展方面，针对江苏常松机械集团有限公司的实际情况和发展，工程技术人员给出了以下建议：

1、QVM660 可支持高速双向 Cable Modem (有线电视) 上网，或是使用 ADSL 以及光纤接入。在应用上，对外的 WAN 口联机可支持高速双向 Cable Modem (有线电视) 上网，或是使用 ADSL 以及光纤接入。而对内的联机则可透过 DMZ 端，连接到对外开放的服务器。内部用户则通过 LAN 端连接。DMZ 服务器，如论坛、下载服务器，可对外界用户开放；LAN 口用户则受到防火墙的保护，网管人员也可对其存取加以控管；

2、为了改善总公司与分点单位的沟通，还可架设视频会议系统，进行生产协调或信息交流，需要稳定的传输能力；

3、对于以后公司的 B/S 访问模式的应用程序，公司可以随时嵌入 SSL VPN 网关设备来实现移动用户或临时用户的远程安全快捷的访问。

4、连接多条线路，以取代带宽升级，例如以多条 ADSL 取代光纤，费用节省又可弹性运用；

5、VoIP 网络电话：公司内部建置网络电话 VoIP 服务，公司之间所有通话全部免费；

6、同时考虑到公司信息点的增加，其 QVM660 最大满足 300 个信息点的连入，以支持同时 100,000 个联机数。QVM330 最多支持 100 个信息点的连入，以支持同时 10,000 个联机数。