

启博 VPN 产品白皮书

(IPSEC VPN)

目录

一、产品概述.....	3
1.1 产品定义.....	3
1.2 产品简述.....	3
二、产品特点.....	4
2.1 支持国密局《IPSec VPN 技术规范》.....	4
2.2 全面支持 IPSec 协议标准.....	4
2.3 完善的 PKI 体系提高用户网络安全等级.....	4
2.4 支持全动态 IP 地址间建 VPN 隧道.....	5
2.5 实用的 IP 伪装功能.....	5
2.6 隧道间路由及 VPN 隧道接力技术 比专线更灵活.....	5
2.7 完善的 VPN 网络集中管理功能.....	5
2.8 功能强大的虚拟 IP 技术.....	6
2.9 多机多线路负载均衡与备份.....	6
2.10 支持灵活的移动用户接入策略.....	6
2.11 丰富多样的认证与授权.....	6
2.12 分级访问权限.....	7
2.13 简单易用的客户端.....	7
2.14 便捷的 APP 客户端.....	7
2.15 强大的防火墙功能.....	7
2.16 集成强大的网络附加功能.....	7
三、产品主要功能.....	8
四、产品规格.....	10
五、典型应用.....	12
5.1 企业用户 VPN 网络解决方案.....	13
1. 部署方案.....	13
2. 应用效果.....	14
5.2 移动办公 VPN 解决方案.....	14
1.部署方案.....	15
2.应用效果.....	15
5.3 小型企业 VPN 网络解决方案.....	15
1. 部署方案.....	16
2.应用效果.....	16

一、产品概述

1.1 产品定义

启博 VPN 网关符合国家密码管理局最新制定的《IPSEC VPN 技术规范》，是为用户基于互联网构建安全的虚拟专用网络而设计的系列产品。通过启博 VPN 网关可以实现企业总部与分支机构、合作伙伴、移动办公人员之间的远程安全接入的需求，同时对经由 VPN 隧道远程传输的数据提供私密性、完整性的安全防护。

1.2 产品简述

在信息化高度发展，电子商务、电子政务开始被企业和政府等行业普遍应用的今天，不同分支机构之间、不同的信息系统之间有着非常迫切的网络互联需求，如我们常见的业务系统（如财务软件、ERP、CRM、OA 等）、VOIP 和网络视频等应用。对于企业来说，很多都具有多个分支机构，并且随着企业规模的不断扩大和业务的不断扩充，企业跨地区、跨国发展成为一种必然的趋势。同时企业移动办公人员的数量也在逐渐增多，企业之间的联系也日趋频繁、密切。政府及事业单位一直是中国信息化的先行者，一些政府的网络基础建设已经比较完善。随着“电子政务”的进一步深入，政府与各分支机构、合作单位网络的互连互通和信息交互就变得非常必要。而且政府部门的相关局、处、办、所往往遍布于城市的各区县，也经常需要与所管辖的事业单位交互信息。同时，政府人员的外出移动办公需求也日益迫切。

所有这些应用，无论是企业信息化应用，还是电子政务应用，都离不开一个基本前提：要首先建立一个安全的、可靠的、互联互通的基础网络平台。建立这样的基础网络，传统的做法是采用电信运营商提供的专线，例如 DDN、帧中继、MPLS 等。一些特殊的行业，如金融、电力、铁路、政府等，他们对网络的可靠性、安全性有非常高的要求，通常都是采用专线的方式来连接分支机构和不同地域的局域网络。但是对于大部分企业和很多政府机构来讲，无论在建设成本上还是后期维护上，要建立一个物理专网都是比较困难的。而传统的拨号的方式速度太慢，也已经被淘汰。

随着 Internet 的迅速发展及 VPN 技术的出现，为企业、政府信息化应用提供了发展良机 and 更好的选择。VPN（Virtual Private Network，虚拟专用网）是利用公共网络资源来构建的虚拟专用网络，它是通过特殊设计的硬件或软件直接在共享网络中通过隧道、加密、认证等技术来实现远程网络的互连互通和确保信息远程传输的安全。通过 VPN 能提供与专线一样的安全性和功能保障，使得整个企业网络在逻辑上成为一个专用的透明内部网络，具有安全性、可靠性和可管理性。

随着国内运营商网络基础设施的不断完善和宽带互联网的高速发展，互联网普及到国内的各个角落，并且上网的宽带越来越快，使得 VPN 技术和应用也获得了空前的发展。今天，VPN 虚拟专用网已经具备了与专线相近的稳定性和安全性。事实上，利用 VPN 技术来组建自己的“专用网络”，已经成为当下大多数政府、企事业单位的首选组网解决方案。在各种 VPN 技术中，基于 IPSec 的 VPN 技术经过多年的实践、发展和完善，以其方便性、安全性、标准化等优势，在全球范围得到广泛应用，已成为实现企业网络跨地域安全互联的主要技术手段。

启博 VPN 网关就是在这样的应用背景下，经由深圳市启博网络有限公司长期潜心研发

而推出的 VPN 网关产品。启博网络专注于为用户提供综合的集成化的安全网关产品。

二、产品特点

2.1 支持国密局《IPSec VPN 技术规范》

启博 VPN 网关全面支持国家密码管理局制定的《IPSec VPN 技术规范》，支持多种国密办要求的硬件密码算法，采用硬件密码模块进行密码算法运算，支持国家密码管理局规定的 SM1、SM2、SM3、SM4 商用密码算法，产品的安全性和合规性有充分的保障。启博 VPN 安全网关可以与任何严格遵循《IPSec VPN 技术规范》实现的 IPSec 网关进行互通。《IPSec VPN 技术规范》对标准的 IPSec 协议进行了修正，以数字信封的认证方式替代了预共享密钥和签名的认证方式，抛弃了 DH 密钥交换方式，采用了公钥加密的方式，杜绝了中间人攻击的可能，同时，采用国家的商用密码算法替代公开的标准算法，为用户的数据提供了最大限度的安全保护。

2.2 全面支持 IPSec 协议标准

IPSec 作为一个全球性的安全标准，要求所有 IPSec 的实现必须严格遵循其各种协议规范，以便实现不同产品之间的互通。启博 VPN 产品经过严格的互通性测试，与 Cisco、Juniper、Fortinet 等著名厂家的 VPN 产品可以实现互通。产品遵循 RFC 1828、RFC1829、RFC 1851、RFC 1852、RFC 2085、RFC 2401-2412 等一系列协议标准。

- 支持标准 ESP、AH 加密认证协议；
- 支持隧道模式、传输模式的协议封装格式；
- 支持 IKEv1、IKEv2；
- 支持主模式、野蛮模式、快速模式多种协商模式；
- 支持证书认证和预共享密钥认证方式；
- 支持 DES、3DES、AES 等多种对称密钥算法；
- 支持 MD5、SHA1 等多种完整性验证算法；
- 支持 RSA、DH 等多种非对称密钥算法；
- 支持扩展认证和模式配置。

2.3 完善的 PKI 体系提高用户网络安全等级

随着 VPN 技术在政府、金融等高安全性要求领域的应用不断深入，用户对 VPN 网络的认证功能与其原有的 PKI 体系进行无缝结合的需求也越来越强烈。启博 VPN 产品全面支持标准 PKI 体系结构，既能够通过内置的 CA 模块独立为移动用户签发数字证书，又能够通过导入 CA 根证书+CRL 列表方式对第三方 CA 签发的证书进行认证，同时还能够通过 AD/LDAP 等标准协议向第三方 CA 提交在线证书认证请求。具体 PKI 功能包括：

- 支持标准 X509.V3 格式数字证书；
- 支持 DER、PEM、PKCS12 等多种证书编码格式；

- 支持通过内置 CA 模块为用户签发标准数字证书；
- 支持同时导入多个 CA 根证书和 CRL 列表，对不同 CA 签发证书进行认证；
- 支持通过 AD/LDAP 等标准协议向第三方 CA 进行在线证书认证；
- 支持生成 PKCS10 格式的证书请求，可生成证书请求，由第三方 CA 签名；
- 支持 CRL 列表文件的导入和通过 HTTP 自动下载。

启博网络与山东渔翁、三未信安、江南计算所等国内主要 CA 厂商有着长期的合作，启博 VPN 网关与这些厂商的 CA 系统均能够无缝集成。

2.4 支持全动态 IP 地址间建 VPN 隧道

目前国内 ADSL 宽带接入较为普遍，从 ISP 那里动态获取临时 IP 地址。这个 IP 地址不定时会改变变化的，如果 VPN 互联的两个分支机构都是动态 IP 地址，那么这两个分支机构之间的 VPN 隧道策略参数必须进行动态调整，这一过程对目前市场大部分的 VPN 产品（包括国内产品和国外产品）都无法自动完成，这为 VPN 网络的日常维护和广泛应用带来很大困难。启博 VPN 产品集成启博目录寻址服务，客户不需要申请固定 IP 也不用申请动态域名，只要部署启博 VPN 网关即可实现全动态 IP 之间自动建立 VPN 隧道。

2.5 实用的 IP 伪装功能

在大型的网络中，尤其是政府或事业单位的网络，如果分支机构通过 VPN 连接到本单位总部后，需要访问上级单位的业务系统，则需要上级单位的信息主管部门帮添加相应的路由表才行。现实情况是上级部门基本不会配合下级部门的这种要求，对此启博 VPN 的 IP 伪装技术显的非常实用，只要部署在单位总部的 VPN 设备能访问到的系统，通过 IP 伪装功能当分支机构访问上级单位系统时把自身的 IP 地址伪装成总部启博 VPN 设备的 IP 地址，这样就可以正常访问上级部门的网络了。

启博 VPN 网关 IP 伪装功能实用设置简单，只需要打勾选择启用 IP 伪装选项即可。该功能已在 BOSS 计费系统，政务网中等复杂网络中得到很好应用。

2.6 隧道间路由及 VPN 隧道接力技术 比专线更灵活

隧道间路由是指多个分支机构都与公司总部建立 VPN 隧道，通过配置静态路由表实现不同分支机构之间经由总部实现互通，分支机构之间不需要增加 VPN 隧道。避免了分支机构数量太多的情况下组建网状结构的 VPN 网络时要建很多的 VPN 隧道，后期维护量巨大。

VPN 隧道接力技术是指启博 VPN 网关所在的网络如果有 DDN 专线或 MPLS VPN 之类的连接到远程，其它与此节点启博 VPN 网关建立隧道的 VPN 网关端的网络，可以通过隧道接力的方式访问到 DDN 专线连接的远端，此应用方式广泛用于多级组网的行业应用中。

2.7 完善的 VPN 网络集中管理功能

利用基于互联网的 VPN 技术构建企业基础网络设施，低成本、高效率是其天然的优势，但与此相伴的则是安全性和可管理性的潜在风险。尤其是对于分支机构、营业网点遍布全国的大型企业来讲，其业务网络系统具有分布地域广泛、接入点多、网络结构复杂等特点。如何确保企业内部网络的安全，有效地管理、维护遍布企业各个结点的 VPN 设备，保证网络

的稳定运行，是 VPN 产品供应商必须解决的问题。启博网络推出 VPN 设备集中管理功能，可以远程管理和配置 VPN 设备，进行策略集中管控和策略下发，并成功运用于许多特大型企业的 VPN 建设中。

2.8 功能强大的虚拟 IP 技术

在大规模 VPN 组网时，IP 地址冲突的问题比较突出，比如好多公司都在用 192.168.1.0/24 的网段，这种问题是复杂而不好处理的，因为调整 IP 地址涉及面广，所有已经布署好的配置都需要重新调整，但是不调整 IP 地址 VPN 组网又有问题。

启博网络研发的虚拟 IP 地址功能能够很好的解决这个问题，启博 VPN 规划出一组虚拟 IP 地址与真实的 IP 地址做一对一绑定，实现访问虚拟 IP 地址就是访问真实 IP 地址的效果，轻松解决 IP 地址冲突问题。

2.9 多机多线路负载均衡与备份

启博网络 VPN 网关支持多机与多线路的组合应用，可以在多台设备与多条链路之间实现隧道内数据的负载均衡或备份。还能实现多线路自动选优，有效解决国内跨运营商线路的互通问题。当某条线路发生故障时，系统能自动的将数据流切换到其它线路；当一台设备发生故障时，系统能自动将数据流切换到其它网关设备，保证 VPN 网络的连通性。

2.10 支持灵活的移动用户接入策略

VPN 技术在远程移动办公领域的应用越来越广泛，因此支持安全灵活的移动用户接入策略已经成为 VPN 产品竞争的焦点。IPSec VPN 产品支持丰富的移动用户接入策略，为各种需求的用户提供了完善的解决方案。

- 支持基于用户+口令的认证机制；
- 支持基于数字证书的认证机制；
- 支持基于证书+口令的双因子认证机制；
- 支持 RADIUS/LDAP/AD 等用户认证协议；
- 支持 USB KEY、OPT 动态密码等强身份认证机制；
- 支持移动用户的硬件特征码绑定机制；

2.11 丰富多样的认证与授权

启博网络 VPN 产品内置有用户认证数据库，同时支持多种外部认证，如：RADIUS 认证、AD 认证、LDAP 认证等，并支持外部认证服务器对用户授权与计费。通过外部认证，可以方便的与用户原有的认证系统无缝的结合。

启博网络的 VPN 网关支持用户名、口令、证书、USBKEY、短信、硬件特征码、动态令牌、等多种认证方式以及它们的任意组合，为用户提供最强的安全接入机制。

2.12 分级访问权限

分级访问权限是指对远程接入的 VPN 客户端进行不同的等级划分,根据不同的等级获取不同的访问权限。比如 VPN 用户 A 可以访问公司 ERP 服务器、OA 服务器、CRM 服务器;用户 B 只允许访问 OA 服务器;用户 C 可以访问 OA 服务器和 CRM 服务器等等。启博网络 VPN 网关可以很好的管理公司不同部门员工,有不同的 VPN 接入权限,公司内部员工、经销商、供应商有不同的资源访问权限,即满足了业务的远程访问的需要,同时通过不同的权限划分又保障了访问的安全问题。

2.13 简单易用的客户端

启博 VPN 客户端软件支持主流的 Windows 操作系统,软件自动识别 64 位及 32 位操作系统,安装方式简单,只需要根据向导点击下一步即可完成安装,然后输入几个简单参数即可完成设置。启博 VPN 客户端软件支持开机自动连接和断线重连功能,只要能上网,VPN 客户端软件会自行连接,不需要人为干预。

对于其它语言的用户,启博 VPN 客户端软件有专门的英文版本,安装和配置方法与简体中文版本相同。

2.14 便捷的 APP 客户端

目前移动互联网已成为新的应用趋势,通过智能终端即可方便的实现远程办公。像 android 和苹果 IOS 系统都有带 VPN 连接功能,但是这些 VPN 菜单都藏的很深,不容易查找,也很难配置,尤其是对于年纪稍大的单位领导,让他们去 VPN 连接简直一件不可完成的任务,又不能随意看他们的手机或平板。为此启博网络专门开发了 Android 和 IOS 端的 APP 客户端软件。

启博 APP 客户端配置简单,使用方便,直接断线重连功能,再也不用担心领导不会使用了。同时安装了启博 APP 公司出差人员可随时处理公司事务,领导不在单位照样可以进行网上审批和签字。有了启博 APP 再也不用因为智能终端无法访问而把公司服务器发布到公网,带来很大的安全隐患和数据泄露风险,通过启博 APP 客户端就能实现和 PC 安装启博 VPN 软件一样的效果,所有的访问都是安全的,数据都是加密的,方便且有保障。

2.15 强大的防火墙功能

启博 VPN 网关集成了强大的防火墙功能,能为用户的 VPN 网络提供高等级的边界安全防护与访问控制。启博 VPN 集成防火墙功能分为流入防火墙、流出防火墙、区间防火墙、系统防火墙、VPN 防火墙五大模块。从网络的各个层面对单位内网及启博 VPN 网关本身进行周密防护。在启博 VPN 网关布署在单位网络出口时,能对公司的网络进行很好的防护。

2.16 集成强大的网络附加功能

启博 VPN 网关为用户组网提供了强大的网络附加功能,完全可以作为独立的相关网络设备进行配置使用,其主要功能如下:

- 功能丰富的 UTM 一体化网关,集 IPS、防病毒、内容过滤、反垃圾邮件等功能于一体的安全网关;

- 集成强大的网络附加功能，支持 NAT 转发、静态/动态路由、VLAN、带宽管理、DNS 代理、DHCP 服务器、IP/MAC 绑定、实时流量查看等。

三、产品主要功能

类别	功能	详细描述
网络特性	工作模式	支持网关、网桥、旁路模式
	路由功能	支持静态路由、动态路由
		支持基于源/目的地址、端口、协议及接口的策略路由
		支持单臂路由，可通过单臂模式接入网络，并提供路由转发功能
		支持 Vlan 路由，能够在不同的 VLAN 虚接口间实现路由功能
		支持 RIP、OSPF 等路由协议
	支持多线路捆绑和负载均衡	
DHCP	支持 DHCP Server、DHCP Client 工作模式，最多支持三路 DHCP Server	
DDNS	支持动态域名寻址功能，集成启博私有 DDNS 功能	
PKI	证书格式	支持 X.509 V3 数字证
		支持 DER/PEM/PKCS12 等多种证书编码
	本地 CA	支持内置 CA，为其他设备或移动用户签发证书
		支持证书废弃，支持生成标准 CRL 列表
		支持证书请求的生成，由第三方 CA 进行签名
第三方 CA	内置支持 SM2 算法的 CA	
支持同时导入多个第三方 CA 的根证书和 CRL 列表，对不同 CA 证书用户		
技术标准	IPSEC VPN	符合国密局制定的《IPSEC VPN 技术规范》
	协议	支持 ESP/AH/IKE/NATT 等标准 IPSEC 协议
		支持隧道模式、传输模式
		支持采用国密局标准 IPsec 协议互通
		支持与第三方标准 IPsecVPN 产品互通
	算法	支持隧道压缩协议
		支持 HMAC-MD5、HMAC-SHA1 校验算法
		支持 DES、3DES、AES-128、AES-256 加密算法
支持 DH Group 1/2/5, RSA 1024/2048 非对称算法		

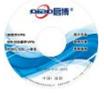
		支持国家商密专用的 SM1/SM2/SM3/SM4 算法
	IKE 协商	第一阶段协商支持主模式、野蛮模式
		第二阶段协商支持快速模式
		第一阶段身份认证支持预共享密钥、数字证书方式
		支持完全向前保密 PFS
		支持使用标准的 X.509 证书建立隧道
		支持 DPD 协议探测隧道状态
		支持隧道断线自动重建
		PSK 方式下支持用户自定义标识符
		支持 XAuth 认证和模式配置
	硬件加密卡	支持高速算法加速卡
	数据压缩	支持高效数据流压缩算法
	VPN 特性	支持网状、树型、星型等多种 VPN 网络拓扑
		支持隧道的 NAT 穿越、双向 NAT 隧道建立
		支持全动态 IP 地址间的 VPN 组网
		支持 HUB & SPOKE 功能
	VPN 客户端	支持多机多隧道的负载均衡和备份
		支持第三方标准 IPSec 客户端接入
		支持为移动用户定义访问权限
		支持多线路自动检测
		支持移动用户接入状态的监控和审计
		支持 UKEY 认证接入，绿色免安装驱动
		支持 Windows32 位和 64 位操作系统
		支持 Android 和 IOS 智能终端 APP 客户端
	VPN 种类	支持开机启动 VPN 自动连接
		IPSEC VPN
		L2TP VPN 服务器
		PPTP VPN 服务器
		启博 VPN 服务器和启博 VPN 客户端（私有协议）
		下一代 VPN 支持（启博 EPN）
安全特性	代理功能	支持 HTTP 代理
		支持 POP3 代理
		支持 FTP 代理
		支持 SMTP 代理
		支持 DNS 代理
	内容过滤	支持网页内容过滤
		支持 URL 过滤
		支持垃圾邮件过滤
	防火墙功能	流出防火墙
		区间防火墙
		系统防火墙
		VPN 防火墙

		IP/MAC 绑定	
	入侵防御	入侵防御系统	
	防病毒	支持 Clamav AntiVirus 功能	
	NAT		支持双向 NAT
			支持动态地址转换和静态地址转换
		支持多对一、一对多和一对一等多种方式的地址转换	
		支持虚拟服务器功能	
高级特性	WAN 扩展	支持增加 WAN 线路功能	
	虚拟 IP 功能	虚拟 IP 功能解决 VPN 组网中的 IP 地址冲突问题	
	双机热备	支持双机热备 (Active-Standby) 模式	
	配置同步	支持双机热备的两台设备之间可以同步配置	
	网络探测	可以自定义网络线路的优先级, 保证最短时间	
	组播转发	支持跨网段组播转发功能 (专利申请中)	
	智能 QOS	可根据业务需要设置不同业务数据的传输的优先级	
	域名服务器	设置内网域名服务器, 可以实现特殊的域名访问功能	
	Ntop 流控	集成 Ntop 流量控制功能	
日志	日志功能	系统日志、防火墙日志、VPN 日志、入侵检测日志等	
		日志等级设定功能	
		日志保留天数设置	
		日志输出功能	
配置管理	配置方式	支持 WEB 图形配置、命令行配置	
		支持基于 SSH、HTTPS 的安全配置	
	SNMP	支持 SNMP 的 v1、v2、v3 版本	
		支持 SNMP MIB 扩展	
		与当前通用的网络管理平台兼容, 如 HP Openview 等	
	配置管理	可以进行配置文件的备份、下载、删除、恢复和上载	
		可进行部分配置本地和异地的批量导出和导入	
支持定时备份配置功能			

四、产品规格

型号	图片	说明
MR-1000		高性价比 VPN 网关, 集成防火墙、MAC 绑定、IP 限速、访问控制等功能, 最大并发 5 条 VPN 隧道, 可带 20 台电脑, 加密吞吐率 4M/S, 防火墙吞吐率 20M/S, 最大并发会话数 8000。1WAN+4LAN, 集成

		第四代 VPN 技术启博 EPN 功能。
Mr-1300		高性价比 VPN 网关，集成防火墙、ARP 绑定、IP 限速、访问控制等功能，最大并发 10 VPN 隧道，可带 50 台电脑，加密吞吐率 6M/S, 防火墙吞吐率 30M/S, 最大并发会话数 15000。1WAN + 4LAN+1WLAN 10M/100M 网络接口，带 WIFI 功能，集成第四代 VPN 技术启博 EPN 功能。
MR-2600		高性价比 VPN 网关，集成防火墙、ARP 绑定、IP 限速、访问控制等功能，最大并发 30 VPN 隧道，可带 80 台电脑，加密吞吐率 8M/S, 防火墙吞吐率 60M/S, 最大并发会话数 20000。1WAN + 4LAN 10M/100M 网络接口，集成第四代 VPN 技术启博 EPN 功能。
MR-5100		高性价比 VPN 网关，集成防火墙、ARP 绑定、IP 限速、访问控制等功能，最大并发 60 VPN 隧道，可带 120 台电脑，加密吞吐率 10M/S, 防火墙吞吐率 80M/S, 最大并发会话数 40000。2WAN + 3LAN 10M/100M 网络接口，集成第四代 VPN 技术启博 EPN 功能。
MR-5200		高性价比 VPN 网关，集成防火墙、入侵检测、带宽限制、代理访问等功能，最大并发 80 VPN 隧道，可带 150-200 台电脑，加密吞吐率 20M/S, 防火墙吞吐率 100M/S, 最大并发会话数 100000。2WAN + 4LAN 10M/100M/1000M 网络接口，集成第四代 VPN 技术启博 EPN 功能。
MR-5400		高性价比 VPN 网关，集成防火墙、入侵检测、带宽限制、代理访问等功能，最大并发 100 VPN 隧道，可带 200-300 台电脑，加密吞吐率 30M/S, 防火墙吞吐率 200M/S, 最大并发会话数 200000。2WAN + 1DMZ+1LAN 10M/100/1000M 网络接口，集成第四代 VPN 技术启博 EPN 功能。
MR-5600		高性价比 VPN 网关，集成防火墙、入侵检测、带宽限制、代理访问等功能，最大并发 200 VPN 隧道，可带 300-400 台电脑，加密吞吐率 40M/S, 防火墙吞吐率 300M/S, 最大并发会话数 300000。3WAN + 1LAN 10M/100M/1000M 网络接口，集成第四代 VPN 技术启博 EPN 功能。
MR-5800		高性价比 VPN 网关，集成防火墙、入侵检测、带宽限制、代理访问等功能，最大并发 300 VPN 隧道，可带 500-600 台电脑，加密吞吐率 60M/S, 防火墙吞吐率 400M/S, 最大并发会话数 400000。3WAN + 1LAN 10M/100M/1000M 网络接口，集成第四代 VPN 技术

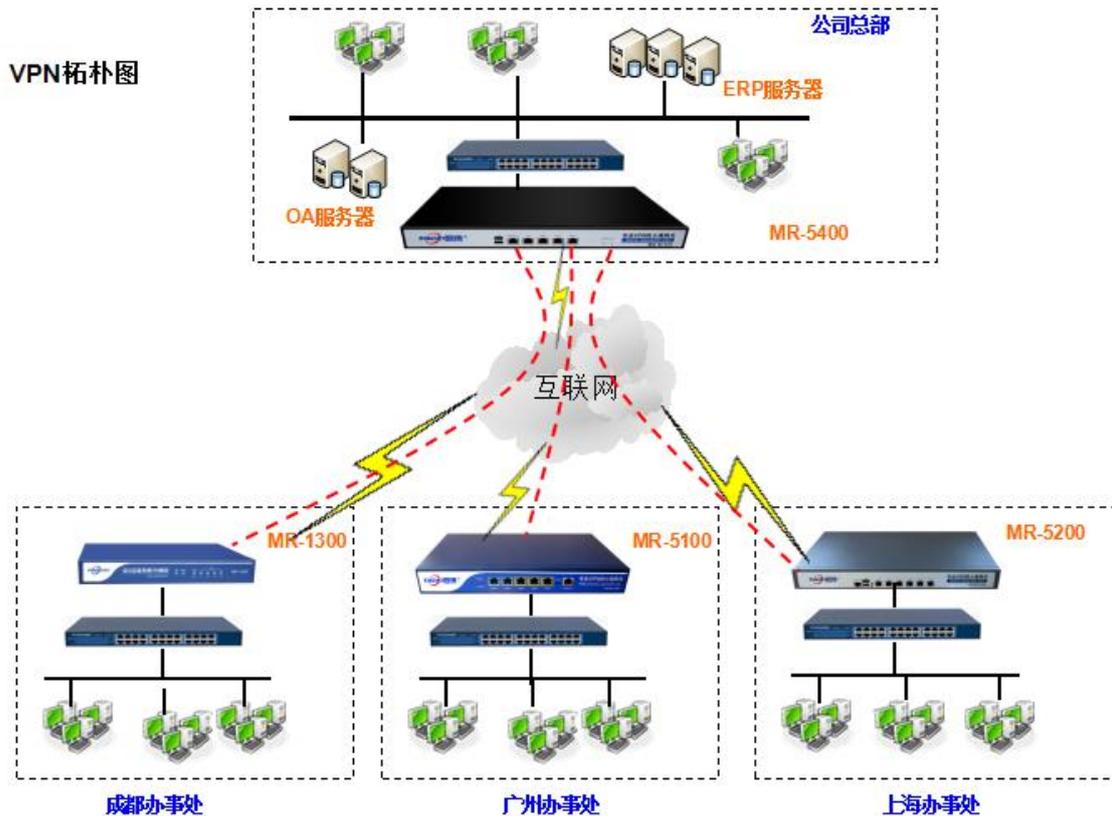
		启博 EPN 功能。
MR-6100		支持双线接入，解决电信和联通之间互通问题，与第三方设备可以对接，集成企业级防火墙，支持动态域名解析、虚拟服务和 DMZ，支持关键词过滤、URL 过滤、MAC 过滤、时间段过滤等功能，最大并发 500 VPN 隧道，可带 800 台电脑，加密吞吐率 100M/S, 防火墙吞吐率 500M/S，最大并发会话数 600000，2WAN+1LAN+1DMZ，10M/100M/1000M 网络接口，集成第四代 VPN 技术启博 EPN 功能。
MR-7100		高性价比 VPN 网关，集访问控制、VPN、防火墙、流理管理为一体，包括 SSL VPN、IPSEC VPN、L2TP VPN、PPTP VPN 多种接入 VPN 产品为一体，带流量控制和 PPPOE 服务器，最大并发 2048 VPN 隧道，4WAN（10/100/1000M）+1LAN（10/100/1000M）+1DMZ（10/100/1000M），可带 1200 台电脑，最大支持 2000000 并发会话数，防火墙吞吐率 800M/S，VPN 加密吞吐率 300M/S,集成第四代 VPN 技术启博 EPN 功能。
MR-8100		高性价比 VPN 网关，集访问控制、VPN、防火墙、流理管理为一体，包括 SSL VPN、IPSEC VPN、L2TP VPN、PPTP VPN 多种接入 VPN 产品为一体，带流量控制和 PPPOE 服务器，最大并发 8196 VPN 隧道，4WAN（10/100/1000M）+1LAN（10/100/1000M）+1DMZ（10/100/1000M），可带 2500 台电脑，最大支持 5000000 并发会话数,防火墙吞吐率 6GB/S,VPN 加密吞吐率 800M/S,集成第四代 VPN 技术启博 EPN 功能。
UKEY		即插即用，不需要安装软件，使用时直接插在电脑的 USB 接口，用完拔出 VPN 自动断开连接
VPN 客户端软件		PC 客户端软件
		APP 客户端软件

五、典型应用

5.1 企业用户 VPN 网络解决方案

许多企业在全国各地都建有分支机构或者办事处，随着企业信息化程度的不断提高，一般在企业总部会部署如财务软件、OA 系统、ERP 系统等应用软件，将企业分布在各地的分支机构和办事处与企业总部互联，实现安全地共享数据和软件资源的目的。

采用 VPN 网关互联 的解决方案如下图所示。



1. 部署方案

企业总部：公司重要的资料包括 ERP 软件、财务软件、OA 系统的服务器一般是放在总部，总部的人数和电脑数也比较多，因此对 VPN 设备的数据处理能力和防火墙功能都比较强，因此在企业总部一般布署一台处理能力较强的启博 VPN 网关，比如 MR-5400。考虑到企业总部对网络的实时性要求比较高，对于规模比较大且分支机构比较多的企业，建议布署两台启博硬件网关做双机热备方案，来提高企业整个网络包括 VPN 网络的容错性。

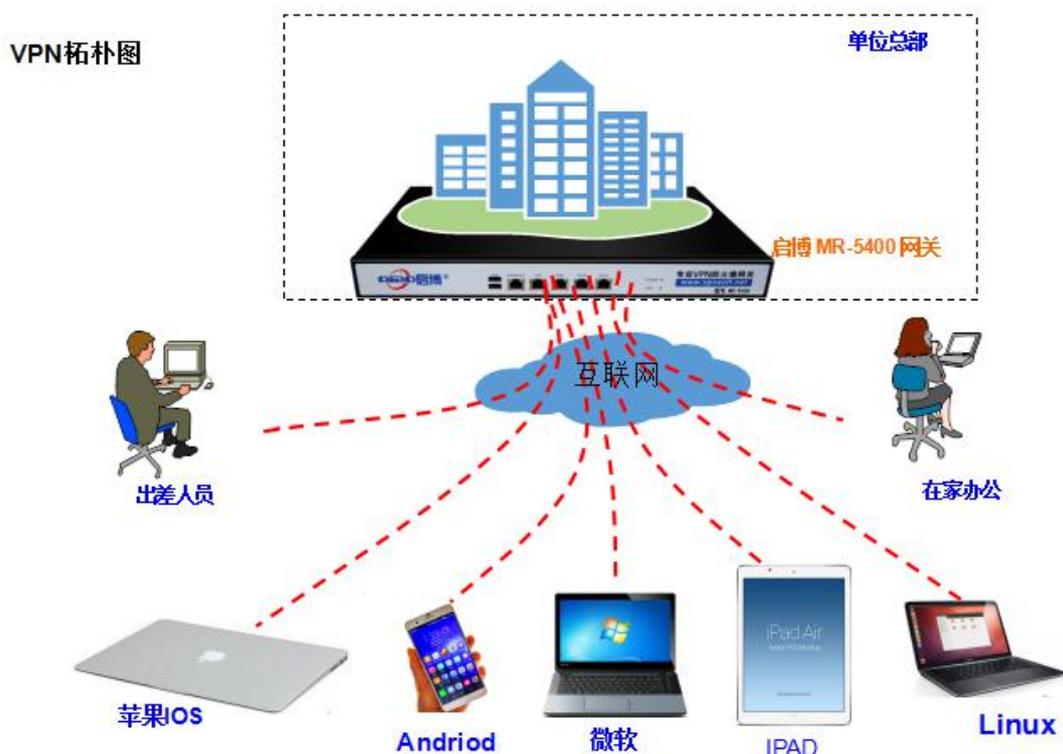
分支机构：分支机构是指分布在不同地域规模不等的分公司或办事处，分公司或办事处根据自身的规模情况，选择适合的 VPN 硬件网关。启博 VPN 网关可以直接当路由器使用、为内部主机提供功能完善的防火墙保护等功能。同时启博 VPN 网关自动与总部的 VPN 网关进行连接建立安全加密隧道，实现总部与分支机构之间的数据安全传输。

2、应用效果

- 公司的 ERP 管理软件（包括财务软件、OA、邮件系统等）远程扩展，以前只能在本地用的应用系统都可以通过 VPN 实现远程作业，总部与分支机构共用一套管理系统，方便公司统一管理，加快信息传递和处理的速度，提高办事效率，便于领导决策。
- 总部与分支机构之间可以进行远程文档的共享，相互访问（复制、合并、修改等），并可以实现远程打印，便于公司对重要文档统一使用，统一管理。
- 启博 VPN 实现的是 LAN TO LAN 互联，支持局域网中有文件操作方式，如远程打印、导入导出数据在本地等。不仅支持分支访问总部，同时总部也可以访问分支机构的内网电脑或监控设备。

5.2 移动办公 VPN 解决方案

随着公司的业务的发展，有些人员经常需要在外面出差，出差时如何使用内部业务系统或获取公司内网的资料，是一个亟待解决的问题。启博 VPN 针对这种应用推出了启博 VPN 软件客户端，包括 PC 软件、安卓和苹果 APP，出差人员只需在个人电脑上或手机上安装相应软件，即可轻松连接到公司总部内网，如同在总部一样处理事务，实现真正意义上的移动办公。



1.部署方案

在公司总部部署一台启博 VPN 网关，由它负责远程移动用户的接入和安全策略控制。如果用户已有自己的认证系统，希望 VPN 系统沿用业务系统的账号登录，启博 VPN 支持 LDAP 和 AD 方式与第三方认证服务器结合进行认证。启博 VPN 网关还包含强大的防火墙功能，能为总部内网提供全面的边界安全防护。

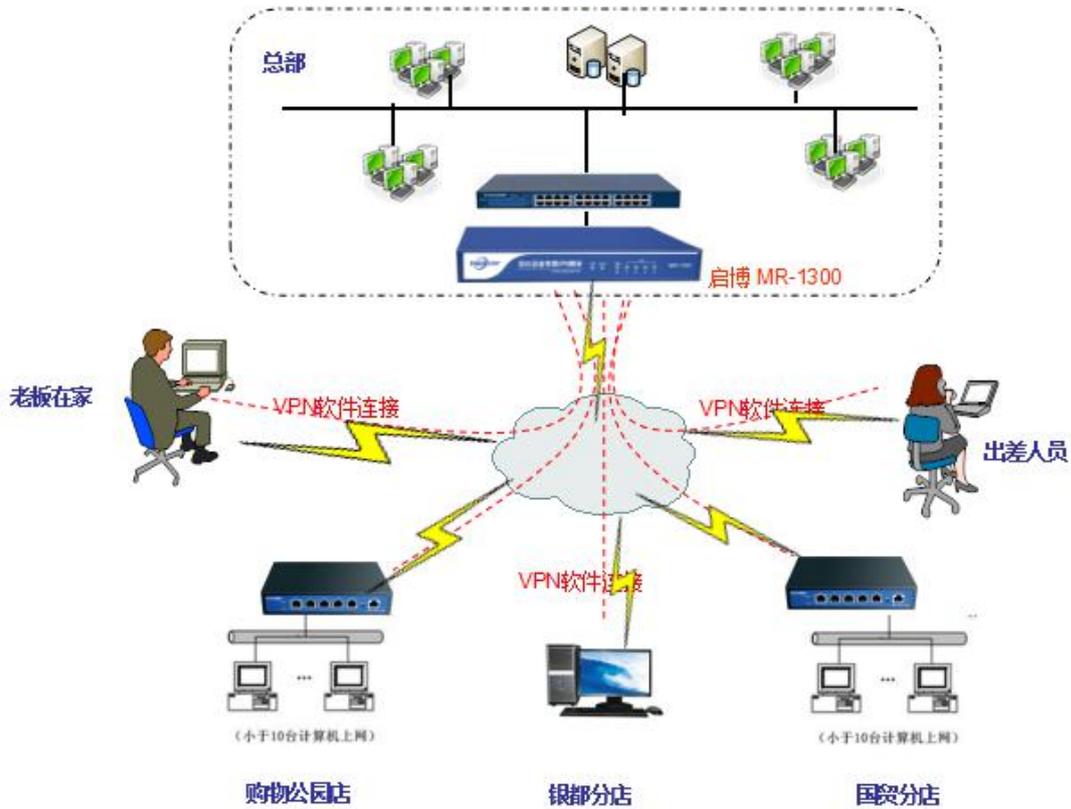
在移动用户的电脑上安装启博 VPN 客户端软件，启博 VPN 客户端软件支持主流 windows 系统包括 64 位，只需简单配置，即可和总部 VPN 网关建立隧道连接，进行安全通讯。对于 Android 和 IOS 智能终端，只需要安装启博 VPN 对应 app 即可接入中心 VPN 网关，安全的访问内网应用系统。

2.应用效果

- 总部管理员为移动办公用户提供的 VPN 接入帐号和密码，并在启博 VPN 网关上为其分配的权限访问相应的内部网络资源。使其访问内网资源更加安全、便捷。
- 移动办公用户只要能上网，不管是使用电脑还是智能手机都能方便接入公司内网，无论在酒店还是在高铁上都能照常处理办公文件。
- 启博 VPN 网关可以提供丰富的移动用户接入身份认证解决方案，可与第三方认证服务器结合应用，安全稳定。

5.3 小型企业 VPN 网络解决方案

许多小型企业可能仅有几家规模较小的分支机构，例如零售行业的珠宝店、便利店之类的。在公司总部有一台服务器，各分店或分支机机构只有 1-2 台电脑，在这种情况下，企业希望能够有一种配置灵活、投入较少的 VPN 解决方案，以完成所有的分支机构的相互访问需求。针对这类型的客户，启博有专门的低端 VPN 网关以及结合启博 VPN 软件客户来满足客户的需要。其解决方案网络拓扑如下图所示。



1. 部署方案

在企业各分公司（分店）安装启博低端桌面型 VPN 网关，设置好宽带的用户名和密码，分公司（分店）就能上互联网了，同时可以和总部的 VPN 网关进行联网，实现一个局域网的功能。

特别小的分公司或分店的电脑上安装启博 VPN 客户端软件，简单配置一下就可以连接到总部的 VPN 网关，共用总店的管理软件（销售系统、售后服务系统等）。

2. 应用效果

- 利用启博低端 VPN 网关能够快速组建全动态 VPN 网络，实现总部与分支机构的互联互通。
- 企业管理人员可以通过安装启博 VPN 客户端软件，实现远程接入和移动办公。

声明：

1. 本手册所提到的产品规格及资讯仅供参考，有关内容可能会随时更新，启博网络恕不另行通知。
2. 本手册中提到的产品功能或性能可能因产品具体型号、配备环境、配置方法不同而有所差异，此可能产生的差异为正常现象，相关问题请咨询启博网络客户服务中心 400-618-3858。
3. 本手册中没有任何关于其他同类产品的对比或比较，启博网络也不对其他同类产品表达意见，如引起相关纠纷应属于自行推测或误会，启博网络对此没有任何立场。
4. 本手册中提到的信息为正常公开的信息，若因本手册或其所提到的任何信息引起了他人直接或间接的资料流失、利益损失，启博网络及其员工不承担任何责任。