VPN 技术分析与实现

摘要：随着 Internet 已成为全社会的信息基础设施，企业端应用也大都基于IP，在 Internet 上构筑应用系统已成为必然趋势，因此基于 IP 的 VPN 业务获得了极大的增长空间。本文介绍了虚拟专用网的技术原理和特点，以及利用 VPN 技术构建企业虚拟专用网的优势，提出利用公网的资源作为企业各级单位间传输信息的通道，在建设内部网实现信息安全共享的同时降低建设和维护成本，因此具有很好的应用前景。文章首先对 VPN 的技术的发展、优点等进行了分析；其次阐述了 VPN 的解决方案；最后，结合一个证券公司的实例说明企业 VPN 网络的具体实现。

关键词：虚拟专用网；虚拟局域网；网络安全；隧道技术

VPN technology analysis and implementation

Abstract: As the Internet has become a society-wide information infrastructure, enterprise-based applications are mostly IP, to build applications on the Internet have become an inevitable trend, so the service which based on the IP-VPN was great room for growth. This paper presents a virtual private network technology principles and characteristics, and presents the advantages that the companies use the VPN technology to build the virtual private network, by using public networks at all levels of resources as a business unit of the channel to transmit information, in building internal networks to share information security At the same time reduce the cost of construction and maintenance, so VPN has good prospects. The article first tell us something about the development of technologies VPN and other advantages of an analysis ; and secondly about the VPN solutions; Finally, it combinates a securities company examples of the specific enterprise VPN network to achieve.

Key words: VPN; VLAN; network security; tunnel

目　录

1 VPN 技术概述

1.1 VPN 产生的背景

随着 Internet 和电子商务的蓬勃发展，越来越多的用户认识到，经济全球化的最佳途径是发展基于 Internet 的商务应用。随着商务活动的日益频繁， 各企业开始允许其生意伙伴、供应商也能够访问本企业的局域网，从而大大简 化信息交流的途径，增加信息交换速度。这些合作和联系是动态的，并依靠网 络来维持和加强，于是各企业发现，这样的信息交流不但带来了网络的复杂性， 还带来了管理和安全性的问题，因为 Internet 是一个全球性和开放性的、基于 TCP/IP 技术的、不可管理的国际互联网络，因此，基于 Internet 的商务活动就面临非善意的信息威胁和安全隐患。 还有一类用户，随着自身的发展壮大与跨国化，企业的分支机构不仅越来越多，而且相互间的网络基础设施互不兼容 也更为普遍。因此，用户的信息技术部门在连接分支机构方面也感到日益棘手。用户的需求正是虚拟专用网技术诞生的直接原因。移动用户或远程用户通过拨 号方式远程访问公司或企业内部专用网络的时候，采用传统的远程访问方式不 但通讯费用比较高，而且在与内部专用网络中的计算机进行数据传输时，不能 保证通信的安全性。为了避免以上的问题，通过拨号与企业内部专用网络建立VPN 连接是一个理想的选择。

1.2 VPN 的定义

现在有很多连接都被称作 VPN，用户经常分不清楚，那么一般所说的 VPN 到底是什么呢？

VPN 的英文全称是“Virtual Private Network”，翻译过来就是“虚拟专用网络”。顾名思义，虚拟专用网不是真的专用网络，但却能够实现专用网络的功能。虚拟专用网指的是依靠 ISP（Internet 服务提供商）和其它 NSP（网络服务提供商），在公用网络中建立专用的数据通信网络的技术。在虚拟专用网中，任意两个节点之间的连接并没有传统专用网所需的端到端的物理链路，而是利用某种公众网的资源动态组成的。IETF 草案理解基于 IP 的 VPN 为："使用 IP

机制仿真出一个私有的广域网"是通过私有的隧道技术在公共数据网络上仿真一条点到点的专线技术。所谓虚拟，是指用户不再需要拥有实际的长途数据线路，而是使用 Internet 公众数据网络的长途数据线路。所谓专用网络，是指用户可以为自己制定一个最符合自己需求的网络。

我们所要构建的虚拟专用网络可以把它理解成是虚拟出来的企业内部专线。它可以通过特殊的加密的通讯协议在连接在 Internet 上的位于不同地方的两个或多个企业内部网之间建立一条专有的通讯线路，就好比是架设了一条专线一 样，但是它并不需要真正的去铺设光缆之类的物理线路。这就好比去电信局申 请专线，但是不用给铺设线路的费用，也不用购买路由器等硬件设备。VPN 是
基于公网,利用隧道加密等技术,为用户提供的虚拟专用网络,它给用户一种直接连接到私人局域网的感觉。

用户在电信部门租用的帧中继（Frame Relay）与 ATM 等数据网络提供固定虚拟线路（PVC-Permanent Virtual Circuit）来连接需要通讯的单位，所有的权限掌握在别人的手中。如果用户需要一些别的服务，需要填写许多的单据，再等上相当一段时间，才能享受到新的服务。更为重要的是两端的终端设备不但价格昂贵，而且管理也需要一定的专业技术人员，无疑增加了成本，而且帧中继、ATM 数据网络也不会像 Internet 那样，可立即与世界上任何一个使用 Internet 网络的单位连接。而在 Internet 上，VPN 使用者可以控制自己与其它使用者的联系，同时支持拨号的用户。

所以我们说的虚拟专用网一般指的是建筑在 Internet 上能够自我管理的专用网络，而不是 Frame Relay 或 ATM 等提供虚拟固定线路（PVC）服务的网络。

1.3 VPN 的特点

安全保障 ：虽然实现 VPN 的技术和方式很多，但所有的 VPN 均应保证通过公用网络平台传输数据的专用性和安全性。在非面向连接的公用 IP 网络上建立一个逻辑的、点对点的连接，称之为建立一个隧道，可以利用加密技术对经过 隧道传输的数据进行加密，以保证数据仅被指定的发送者和接收者了解，从而 保证了数据的私有性和安全性。在安全性方面，由于 VPN 直接构建在公用网上， 实现简单、方便、灵活，但同时其安全问题也更为突出。企业必须确保其 VPN

上传送的数据不被攻击者窥视和篡改，并且要防止非法用户对网络资源或私有信息的访问。Extranet VPN 将企业网扩展到合作伙伴和客户，对安全性提出了更高的要求。

服务质量保证（QoS） ：VPN 网应当为企业数据提供不同等级的服务质量保证。不同的用户和业务对服务质量保证的要求差别较大。如移动办公用户，提供广泛的连接和覆盖性是保证 VPN 服务的一个主要因素；而对于拥有众多分支机构的专线 VPN 网络，交互式的内部企业网应用则要求网络能提供良好的稳定性；对于其它应用（如视频等）则对网络提出了更明确的要求，如网络时延 及误码率等。所有以上网络应用均要求网络根据需要提供不同等级的服务质量。在网络优化方面，构建 VPN 的另一重要需求是充分有效地利用有限的广域网资源，为重要数据提供可靠的带宽。广域网流量的不确定性使其带宽的利用率很 低，在流量高峰时引起网络阻塞，产生网络瓶颈，使实时性要求高的数据得不 到及时发送；而在流量低谷时又造成大量的网络带宽空闲。QoS 通过流量预测与流量控制策略，可以按照优先级分配带宽资源，实现带宽管理，使得各类数 据能够被合理地先后发送，并预防阻塞的发生。

可扩充性和灵活性 ：VPN 必须能够支持通过 Intranet 和 Extranet 的任何类型的数据流，方便增加新的节点，支持多种类型的传输媒介，可以满足同时传输语音、图像和数据等新应用对高质量传输以及带宽增加的需求。

可管理性 ：从用户角度和运营商的角度应可方便地进行管理、维护。在 VPN 管理方面，VPN 要求企业将其网络管理功能从局域网无缝地延伸到公用网，甚至是客户和合作伙伴。虽然可以将一些次要的网络管理任务交给服务提供商去完成，企业自己仍需要完成许多网络管理任务。所以，一个完善的 VPN 管理系统是必不可少的。VPN 管理的目标为：减小网络风险、具有高扩展性、经济性、高可靠性等优点。事实上，VPN 管理主要包括安全管理、设备管理、配置管理、访问控制列表管理、QoS 管理等内容。

1.4 VPN 带来的好处

VPN 的最终目的是服务于企业，为企业带来可观的经济效益，为现代化企业的信息共享提供安全可靠的途径。由于 VPN 是在 Internet 上临时建立的安全专用虚拟网络，用户就节省了租用专线的费用，在运行的资金支出上，除了购

买 VPN 设备，企业所付出的仅仅是向企业所在地的 ISP 支付一定的上网费用，也节省了长途电话费。这就是 VPN 价格低廉的原因。

哪些用户适于使用 VPN 呢？在满足基本应用要求后，有三类用户比较适合采用 VPN：

①位置众多，特别是单个用户和远程办公室站点多，例如企业用户、远程教育用户；

②用户/站点分布范围广，彼此之间的距离远，遍布全球各地，需通过长途电信，甚至国际长途手段联系的用户；

③带宽和时延要求相对适中；

④对线路保密性和可用性有一定要求的用户。

相对而言，有四种情况可能并不适于采用 VPN：

①非常重视传输数据的安全性；

②不管价格多少，性能都被放在第一位的情况；

③采用不常见的协议，不能在 IP 隧道中传送应用的情况；

④大多数通信是实时通信的应用，如语音和视频。但这种情况可以使用公共交换电话网（PSTN）解决方案与 VPN 配合使用。

对于企业来说，VPN 提供了安全、可靠的 Internet 访问通道，为企业进一步发展提供了可靠的技术保障。而且 VPN 能提供专用线路类型服务，是方便快捷的企业私有网络。企业甚至可以不必建立自己的广域网维护系统，而将这一繁重的任务交由专业的 ISP 来完成。

对于用户来说可以从以下几方面获益：

实现网络安全：具有高度的安全性，对于现在的网络是极其重要的。新的服务如在线银行、在线交易都需要绝对的安全，而 VPN 以多种方式增强了网络的智能和安全性。首先，它在隧道的起点，在现有的企业认证服务器上，提供对分布用户的认证。另外，VPN 支持安全和加密协议，如 Secure IP（IP sec）和 Microsoft 点对点加密（MPPE）。

简化网络设计：网络管理者可以使用 VPN 替代租用线路来实现分支机构的连接。这样就可以将对远程链路进行安装、配置和管理的任务减少到最小， 仅此一点就可以极大地简化企业广域网的设计。另外，VPN 通过拨号访问来

自于 ISP 或NSP 的外部服务，减少了调制解调器池，简化了所需的接口，同时简化了与远程用户认证、授权和记账相关的设备和处理。

降低成本：VPN 可以立即而且显著地降低成本。当使用 Internet 时，实际上只需付短途电话费，却收到了长途通信的效果。因此，借助 ISP 来建立 VPN，就可以节省大量的通信费用。此外，VPN 还使企业不必投入大量的人力和物力去安装和维护 WAN 设备和远程访问设备，这些工作都可以交给 ISP。VPN 使用户可以降低如下的成本：

①移动用户通信成本。VPN 可以通过减少长途费用来节省移动用户的花费。

②租用线路成本。VPN 可以以每条连接的 40%到 60%的成本对租用线路进行控制和管理。对于国际用户来说，这种节约是极为显著的。对于话音数据，节约金额会进一步增加。

③主要设备成本。VPN 通过支持拨号访问外部资源,使企业可以减少不断增长的调制解调器费用。另外，它还允许一个单一的 WAN 接口服务多种目的，从分支网络互连、商业伙伴的外连网终端、本地提供高带宽的线路连接到拨号访 问服务提供者，因此，只需要极少的 WAN 接口和设备。由于 VPN 可以完全管理， 并且能够从中央网站进行基于策略的控制，因此可以大幅度地减少在安装配置 远端网络接口所需设备上的开销。另外，由于 VPN 独立于初始协议，这就使得远端的接入用户可以继续使用传统设备，保护了用户在现有硬件和软件系统上 的投资。

容易扩展：如果企业想扩大 VPN 的容量和覆盖范围。企业需做的事情很少，而且能及时实现：企业只需与新的 IPS 签约，建立账户；或者与原有的 ISP 重签合约，扩大服务范围。在远程办公室增加 VPN 能力也很简单：几条命令就可以使 Extranet 路由器拥有 Internet 和VPN 能力，路由器还能对工 作站自动进行配置。

可随意与合作伙伴联网：在过去，企业如果想与合作伙伴连网，双方的信息技术部门就必须协商如何在双方之间建立租用线路或帧中继线路。有了 VPN 之后，这种协商也毫无必要，真正达到了要连就连，要断就断。

完全控制主动权：借助 VPN，企业可以利用 ISP 的设施和服务，同时又完全

掌握着自己网络的控制权。比方说，企业可以把拨号访问交给 ISP 去做，由自己负责用户的查验、访问权、网络地址、安全性和网络变化管理等重要工作。

支持新兴应用：许多专用网对许多新兴应用准备不足，如那些要求高带宽的多媒体和协作交互式应用。VPN 则可以支持各种高级的应用，如 IP 语音，IP 传真，还有各种协议，如 RSIP、IPv6、MPLS、SNMPv3 等。

正由于 VPN 能给用户带来诸多的好处，VPN 在全球发展得异常红火，在北美和欧洲，VPN 已经是一项相当普遍的业务；在亚太地区，该项服务也迅速开展起来。

2 隧道技术

2.1 概述

众所周知，由于公共 IP 的短缺，我们在组建局域网时，通常使用保留地址作为内部 IP，这些保留地址在 Internet 上是无法被路由的，所以在正常情况下我们无法直接通过 Internet 访问到在局域网内的主机。为了实现这一目的， 我们需要使用 VPN 隧道技术[11]。

隧道技术是 VPN 的基本技术类似于点对点连接技术，它在公用网建立一条数据通道（隧道），让数据包通过这条隧道传输。

2.2 隧道协议

2.2.1 隧道协议

□ 隧道是由隧道协议形成的，分为第二、三层隧道协议，两者本质区别在于用户的数据包是被封装到哪一层的数据包在隧道里传输。第二层隧道协议是先 把各种网络协议封装到 PPP 中，再把整个数据包装入隧道协议中。这种双层封 装方法形成的数据包靠第二层协议进行传输。第二层隧道协议有 L2F 、PPTP、L2TP 等。第三层隧道协议是把各种网络协议直接装入隧道协议中，形成的数据包依靠第三层协议进行传输。第三层隧道协议有 VTP、IP Sec、GRE 等。

① PPTP(Point to Point Tunneling Protocol): PPTP 是 VPN 的基础。PPTP 的封装在数据链路层产生，PPTP 协议采用扩展的 GRE(Generic Routing Encapsulation) 头对 PPP/SLIP 报进行封装。点对点隧道协议 (PPTP) 是一种网络协议，其通过跨越基于 TCP/IP 的数据网络创建 VPN 实现了从远程客户端到专用企业服务器之间数据的安全传输。PPTP 支持通过公共网络（例如 Internet）建立按需的、多协议的、虚拟专用网络。PPTP 允许加密 IP 通讯，然后在要跨越公司 IP 网

络或公共 IP 网络（如 Internet）发送的 IP 头中对其进行封装。PPTP 连接只要求通过基于 PPP 的身份验证协议进行用户级身份验证。

② L2F(Layer 2 Forwording): L2F 可在多种介质（如 ATM、帧中继、IP 网）上建立多协议的安全虚拟专用网，他将链路层的协议（如 PPP 等）封装起来传送。因此网络的链路层完全独立于用户的链路层协议。

③ L2TP((Layer 2 Tunneling Protocol): L2TP 协议是目前 IETF 的标准，由 IETF 融合 PPTP 与 L2F 而形成,它结合了 PPTP 和 L2F 协议的优点，几乎能实现 PPTP 和 L2F 协议能实现的所有服务，并且更加强大、灵活。第 2 层隧道协议 (L2TP) 是一种工业标准 Internet 隧道协议，其可以为跨越面向数据包的媒体发送点到点协议 (PPP) 框架提供封装。L2TP 允许加密 IP 通讯，然后在任何支持点到点数据报交付的媒体上（如 IP）进行发送。Microsoft 的 L2TP 实现使用 Internet 协议安全 (IP Sec) 加密来保护从 VPN 客户端到 VPN 服务器之间的数据流。IP Sec 隧道模式允许加密 IP 数据包，然后在要跨越公司 IP 网络或公共 IP 网络（如 Internet）发送的 IP 头中对其进行封装。

④ IP Sec：在 IP 层提供通信安全的一套协议簇，包括封装的安全负载 ESP 和认证报头 AH、ISAKMP，它对所有链路层上的数据提供安全保护和透明服务。AH 用于通信双方验证数据在传输过程中是否被更改并能验证发送方的身份，实现访问控制、数据完整性、数据源的认证功能。ISAKMP 用于通信双方协商加密密钥和加密算法，并且用户的公钥和私钥是由可信任的第三方产生。IP Sec 上的 L2TP 连接不仅需要相同的用户级身份验证，而且还需要使用计算机凭据进行计算机级身份验证。

2.2.2 VPN 协议比较

PPTP、L2F、L2TP 和 VTP、IP Sec、GRE，它们各自有自己的优点，但对于隧道的加密和数据加密问题都密钥最佳的解决方案。同时，无论何种隧道技术，一旦进行加密或验证，都会影响系统的性能。

与 PPTP 相比，L2TP 能够提供差错和流量控制。两者共有的缺点：其一、认证的只是终端的实体，密钥对信息流（通道中的数据包）进行认证，对于地

址欺骗、非法复制包难以防范；其二、由于缺乏认证信息，如果向通道发送一些错误信息，则可能导致服务的关闭，这也成为常用的攻击手段。

GRE 只提供了数据包的封装，它并没有使用加密功能来防止网络侦听和攻击。在实际环境中它常和 IP Sec 一起使用，由 IP Sec 提供用户数据的加密，从而给用户提供更好的安全性。

只有 IP Sec 协议集合多种安全技术，建立了一个安全可靠的隧道。这些技术包括 Diffie-Hellman 密钥交换技术、DES、RC4、IDEA 数据加密技术、哈希散列算法 HMAC、MD5、SHA、数字签名技术等。IP Sec 不仅可以保证隧道的安全，同时还有一整套保证用户数据安全的措施，由此建立的隧道更具有安全性和可靠性。IP Sec 还可以和 L2TP、GRE 等其它隧道协议一同使用，提供更大的灵活性和可靠性。IP Sec 可以运行于网络的任意一部分，他可以在路由器和防火墙之间、路由器和路由器之间、PC 机和服务器之间、PC 机和拨号和访问设备之间。IP Sec 应作为目前较满意的解决方案。下面对 VPN 协议进行了比较,如表 2.1 所示。

表 2.1 VPN 协议的比较

协议	用途	安全	注释
IP Sec 隧道模式	连接到第三方 VPN 服务器	高	这是在您连接到非 Microsoft VPN 服务器时可以使用的唯一选项。
IP Sec 上的 L2TP	连接到 ISA Server 2004 计算机、ISA Server 2000 计算机或 Windows VPN 服务器	高	使用路由和远程访问在复杂性方面比 IP Sec 隧道解决方案低，但是需要远程 VPN 服务器是 ISA 服务器计算机或 Windows VPN 服务器。
PPTP	连接到 ISA Server 2004 计算机、ISA Server 2000 计算机或 Windows VPN 服务器	中	使用路由和远程访问在限制方面与 L2TP 相同，不同之处在于其更易于配置。由于使用 IP Sec 加密，因此 L2TP 被视为是一种更加安全的解决方案。

2.3 隧道技术实现过程

其实现过程如图 1 所示：

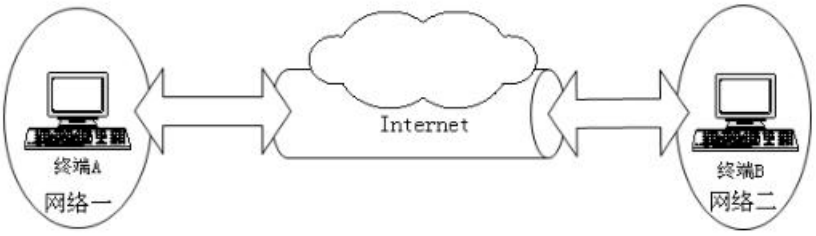

图 1　隧道示意图

通常情况下，VPN 网关采用双网卡结构，外网卡使用公共 IP 接入 Internet；

- 如果网络一的终端 A 需要访问网络二的终端 B，其发出的访问数据包的目标地址为终端 B 的 IP （内部 IP）；
- 网络一的 VPN 网关在接收到终端 A 发出的访问数据包时对其目标地址进行检查，如果目标地址属于网络二的地址，则将该数据包进行封装，封装的方式根据所采用的 VPN 技术不同而不同，同时 VPN 网关会构造一个新的数据包（VPN 数据包），并将封装后的原数据包作为 VPN 数据包的负载，VPN 数据包的目标地址为网络二的 VPN 网关的外部地址；
- 网络一的 VPN 网关将 VPN 数据包发送到 Internet，由于 VPN 数据包的目标地址是网络二的 VPN 网关的外部地址，所以该数据包将被 Internet 中的路由正确地发送到网关；
- 网络二的 VPN 网关对接收到的数据包进行检查，如果发现该数据包是从网络一的 VPN 网关发出的，即可判定该数据包为 VPN 数据包，并对该数据包进行解包处理。解包的过程主要是先将 VPN 数据包的包头剥离，在将负载通 VPN 技术反向处理还原成原始的数据包；
- 网络二的 VPN 网关将还原后的原始数据包发送至目标终端，由于原始数据包的目标地址是终端 B 的 IP，所以该数据包能够被正确地发送到终端 B。在终端 B 看来，它收到的数据包就从终端 A 直接发过来的一样；
- 从终端 B 返回终端 A 的数据包处理过程与上述过程一样，这样两个网络内的终端就可以相互通讯了。

2.4 隧道中的源和目标 IP 地址

隧道是封装、路由与解封装的整个过程。隧道将原始数据包隐藏（或封装）在新的数据包内部。该新的数据包可能会有新的寻址与路由信息，从而使其能够通过网络传输。隧道与数据保密性结合使用时，在网络上窃听通讯的人将无法获取原始数据包数据（以及原始的源和目标）。封装的数据包在网络中的隧道内部传输。封装的数据包到达目的地后，会删除封装，原始数据包头用于将数据包路由到最终目的地。

隧道本身是封装数据经过的逻辑数据路径。对原始的源和目的端，隧道是不可见的，而只能看到网络路径中的点对点连接。连接双方并不关心隧道起点和终点之间的任何路由器、交换机、代理服务器或其他安全网关。将隧道和数据保密性结合使用时，可用于提供 VPN。

通过上述说明我们可以发现，在 VPN 网关对数据包进行处理时，有两个参数对于 VPN 隧道通讯十分重要：原始数据包的目标地址（VPN 目标地址）和远程 VPN 网关地址。根据 VPN 目标地址，VPN 网关能够判断对哪些数据包需要进行 VPN 处理，对于不需要处理的数据包通常情况下可直接转发到上级路由；远程 VPN 网关地址则指定了处理后的 VPN 数据包发送的目标地址，即 VPN 隧道的另一端 VPN 网关地址。由于网络通讯是双向的，在进行 VPN 通讯时，隧道两端的 VPN 网关都必须知道 VPN 目标地址和与此对应的远端 VPN 网关地址。

3 VPN 中的安全技术

由于传输的是私有信息，VPN 用户对数据的安全性都比较关心。 目前 VPN 主要采用四项技术来保证安全，这四项技术分别是隧道技术（Tunneling）、加解密技术（Encryption & Decryption）、密钥管理技术（Key Management）、使用者与设备身份认证技术（Authentication）。 隧道技术在第二章已经加已说明,下面就其它三种安全技术[6]做相应说明。

3.1 加解密技术（Encryption & Decryption）

加解密技术[16]是数据通信中较成熟的技术，VPN 可以直接利用现有的技术。用于 VPN 上的加密技术由 IP Sec 的 ESP(Encapsulating Security Paylcad)实现。主要是发送者在发送数据以前对数据加密，当数据到达接收者时由接收者对数据进行解密处理，算法主要种类包括：对称加密算法、不对称加密算法等，如 DES、IDEA、RSA。

对称加密算法，通信双方共享一个密钥。发送方使用该密钥将明文加密成密文。接收方使用相同的密钥将密文还原成明文，对称加密算法运算速度快。不对称加密算法是通信双方各使两个不同的密钥，一个是只有发送方知道的密钥，另一个则是与之对应的公开密钥，公开密钥不需保密。在通信过程中，发送方用接收方的公开密钥加密信息，并且可以用发送方的秘密密钥对消息的某一部分或全部加密，进行数字签名。接收方收到消息后，用自己的秘密密钥解密消息，并使用发送方的公开密钥解密数字签名，验证发送方身份。

3.2 密钥管理技术（Key Management）

密钥管理技术的主要任务是如何在公网上传递密钥而不被窃取。现行密钥管理技术又分为 SKIP 与 ISAKMP 两种。SKIP 是利用 Diffie-Hellman 的演算法则，在网络上传输密钥；ISAKMP 双方都有两把密钥，分别用于公用、私用。

3.3 身份认证技术（Authentication）

CHAP：使用 MD5 来协商加密身份验证的安全形式，在响应时使用质询-响应机制和单向 MD5 散列。

MS-CHAP：同 CHAP 相似，对远程工作站进行身份验证，在响应时使用质询-响应机制和单向加密。而且 MS-CHAP 不要求使用原文或可逆加密密码。MS-CHAP V2 是第二版的质询握手身份验证协议，它提供了相互身份验证和更强大的初始数据密钥，而且发送和接收分别使用不同的密钥。

EAP：为适应使用其它安全设备的远程访问用户进行身份验证的需求，使用 EAP 可以增加对许多身份验证方案的支持，包括令牌卡、一次性密码、使用智能卡的公钥身份验证、证书及其它身份验证。使用 EAP 还可以防止暴力攻击和密码猜测。

4 VPN 解决方案

VPN 有三种解决方案，用户可以根据自己的情况进行选择。这三种解决方案分别是：远程访问虚拟网（Access VPN）、企业内部虚拟网（Intranet VPN）和企业扩展虚拟网（Extranet VPN），这三种类型的 VPN 分别与传统的远程访问网络、企业内部的 Intranet 以及企业网和相关合作伙伴的企业网所构成的 Extranet 相对应。

4.1 远程访问虚拟网（Access VPN）

如果企业的内部人员移动或有远程办公需要，或者商家要提供 B2C 的安全访问服务，就可以考虑使用 Access VPN。

Access VPN 通过一个拥有与专用网络相同策略的共享基础设施，提供对企业内部网或外部网的远程访问。Access VPN 能使用户随时、随地以其所需的方式访问企业资源。Access VPN 包括模拟、拨号、ISDN、数字用户线路(x DSL)、移动 IP 和电缆技术，能够安全地连接移动用户、远程工作者或分支机构。如图2所示。

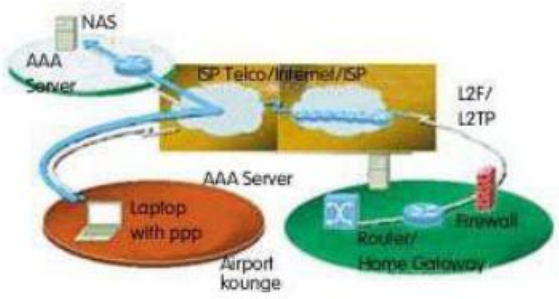

图 2 Access VPN 结 构 图

Access VPN 最适用于公司内部经常有流动人员远程办公的情况。出差员工利用当地 ISP 提供的 VPN 服务，就可以和公司的 VPN 网关建立私有的隧道连接。RADIUS 服务器可对员工进行验证和授权，保证连接的安全，同时负担的电话费用大大降低。

Access VPN 对用户的吸引力在于：

* 减少用于相关的调制解调器和终端服务设备的资金及费用，简化网络；

* 实现本地拨号接入的功能来取代远距离接入或 800 电话接入，这样能显著降低远距离通信的费用；

* 极大的可扩展性，简便地对加入网络的新用户进行调度；

* 远端验证拨入用户服务（RADIUS）基于标准，基于策略功能的安全服务；

* 将工作重心从管理和保留运作拨号网络的工作人员转到公司的核心业务上来。

4.2 企业内部虚拟网（Intranet VPN）

如果要进行企业内部各分支机构的互联，使用 Intranet VPN 是很好的方式。越来越多的企业需要在全国乃至世界范围内建立各种办事机构、分公司、研究所等，各个分公司之间传统的网络连接方式一般是租用专线。显然，在分公司增多、业务开展越来越广泛时，网络结构趋于复杂，费用昂贵。利用 VPN 特性可以在 Internet 上组建世界范围内的 Intranet VPN。利用 Internet 的线路保证网络的互联性，而利用隧道、加密等 VPN 特性可以保证信息在整个 Intranet VPN 上安全传输。Intranet VPN 通过一个使用专用连接的共享基础设施，连接企业总部、远程办事处和分支机构。企业拥有与专用网络的相同政策，包括安全、服务质量(QoS)、可管理性和可靠性。如图 3 所示。

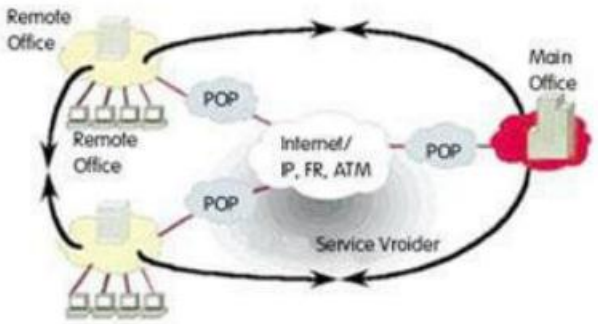

图 3 Intranet VPN 结 构 图

Intranet VPN 对用户的吸引力在于：

* 减少 WAN 带宽的费用；

* 能使用灵活的拓扑结构，包括全网络连接；

* 新的站点能更快、更容易地被连接；

* 通过设备供应商 WAN 的连接冗余，可以延长网络的可用时间。

4.3 企业扩展虚拟网（Extranet VPN）

如果是提供 B2B 之间的安全访问服务，则可以考虑 Extranet VPN。 随着信息时代的到来，各个企业越来越重视各种信息的处理。希望可以提供给客户最快捷方便的信息服务，通过各种方式了解客户的需要，同时各个企业之间的合作关系也越来越多，信息交换日益频繁。Internet 为这样的一种发展趋势提供了良好的基础，而如何利用 Internet 进行有效的信息管理，是企业发展中不可避免的一个关键问题。利用 VPN 技术可以组建安全的 Extranet，既可以向客户、合作伙伴提供有效的信息服务，又可以保证自身的内部网络的安全。Extranet VPN 通过一个使用专用连接的共享基础设施，将客户、供应商、合作伙伴或兴趣群体连接到企业内部网。企业拥有与专用网络的相同政策，包括安全、服务质量(QoS)、可管理性和可靠性。如图 4 所示。

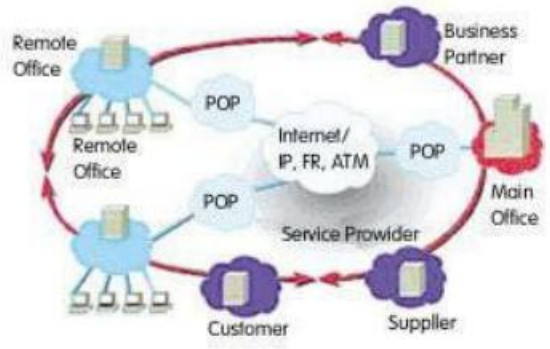

图 4 Extranet VPN 结 构 图

Extranet VPN 对用户的吸引力在于：能容易地对外部网进行部署和管理，外部网的连接可以使用与部署内部网和远端访问 VPN 相同的架构和协议进行部

署。主要的不同是接入许可，外部网的用户被许可只有一次机会连接到其合作人的网络。

5 VPN 网络方案设计

本文以证券公司网络为基础，设计证券公司内部 VPN、外部 VPN 网络方案。该证券有限责任公司作为一家全国性的综合类证券商,总部在北京，在上海有其分公司的营业部和服务网点,而且公司经常会有出差人员和外出团队。该证券公司的网络要能够使分部、外出人员和团队以及合作伙伴之间进行安全的数据传 输，而使用专线价格昂贵，所以该证券公司网络的主要目的是为此证券公司建 设覆盖全国各个地区的 VPN 网,使得分部、外出人员、外出团队和总部之间的数据安全传输[5]。

5.1 需求分析

北京总部分为信息中心、项目管理部和财务部三个部门，总部设置一个 VPN 服务器，在服务器和 Internet 之间设置防火墙保障服务器上的数据安全；上海分公司分为项目管理部和财务部，同样设置一个 VPN 服务器，该服务器和 Internet 之间也设置防火墙保障服务器上的数据安全；总部和分部以及外出移动用户、外出团队和总部之间使用 VPN 网络进行访问[12]。公司的网络结构如图 5 所示。

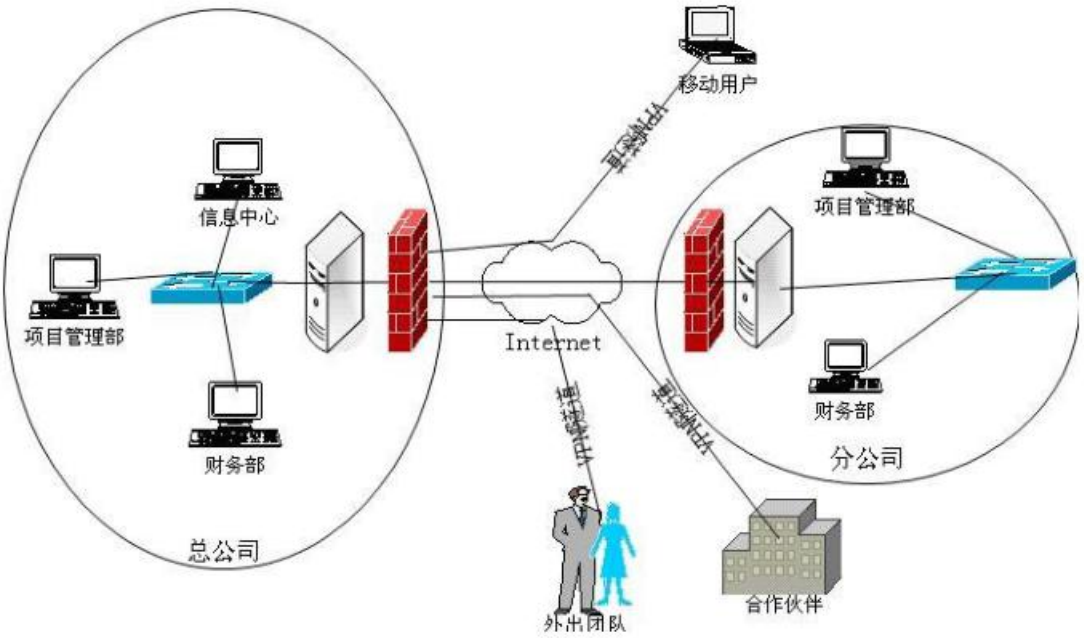

图 5　公司 VPN 网络结构示意图

5.2 拓扑设计

图 6　总公司拓扑结构

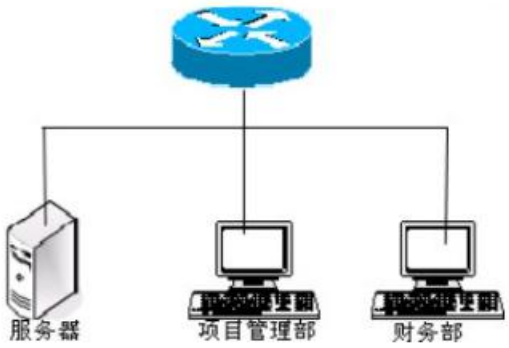

图 7　分公司拓扑结构

5.3 设备选型

公司的网络拓扑结果确定后，就开始选择合适的 VPN 服务器，下面有几种服务器的相关说明，具体如下表 5.1 所示。

表 5.1 VPN 服务器

名称	描述	参考价格	图片
FVS318	VPN 服务器，它利用 SPI、URL 访问和内容过滤、日志记录、汇报及实时告警提供最高的安全性---拒绝服务(DoS)攻击保护和入侵检测。它并且能同时启动多达 8 个 IP Sec VPN 隧道，从而降低您的运营成本，最大程度提高您网络的安全性。	25000 元	
DELL Power Edge 860	适合网络边缘以及针对各种规模用户组建基础结构或网络应用的平台，如 Web 服务器、独立的局域网(LAN)基础设施。	6500 元	
HP ProliantD L360	适用于企业数据中心、服务提供商、中小型企业等高密度计算环境。 DL360 将集中的 1U 计算能力、集成 Lights-Out 管理和基本容错性能集于一身，适用于在空间有限的安装	35000 元	
IBM X3650	这是一款采用 2U 机架式结构的服务器，占据的空间小，为企业节约了不少托管空 IBM X3650(7979RB4)应用了两颗英特尔四核至强 5335 处理器，主频为 2.0G、8M 二级缓存、1333MHz 的系统总线频率。同时标配 4G（2*2G）内存、一块 146GSAS 硬盘、内	29000 元	

置 COMBO 光驱。

联想 万全 T100	G7 S6320 1G/250S 千兆/GF8600 塔式服务器, Intel 酷睿 2 双核 E6320 处理器,标配 NVIDIA GeForce 8600GTS PCI-E 高性能显卡, WindowsServer2003 R2 Standard Edition 简体中文版、Windows 2000 Server(集成 SP4 版本)简体中文版、Lenovo Windows Storage Server 2003(存储增强版)、Windows XP 简体中文版系统支持。	7599 元

由于该证券公司主机数量不是很多，选用专业的 VPN 服务器在经济上不合算，所以使用安装了 windows 2003 的服务器做 VPN 服务器，该网络选用联想万 T100。

5.4 IP 地址分配

各个部门和用户的 IP 地址分配如表 5.2 所示。

表 5.2 IP 地址划分

		IP 地址
总公司		
服务器	私有地址	10.240.0.0
	公有地址	211.85.1.129
信息中心	10.240.64. 0/18	
项目管理部	10.240.128.0/18	
财务部	10.240.192.0/18	
上海分公司		
服务器	私有地址	10.240.0.0
	公有地址	211.85.1.139
项目管理部	10.240.64.0/17	
财务部	10.240.128.0/17	

5.5 权限设置

分为四个权限：管理员权限、部门管理员、公司职员，公司合作伙伴用户，具体的划分如下表 5.3 所示。

表 5.3 权限划分

权限	职能	用户名	密码
管理员权限	可以查看、更新、删除公司的所有数据	zhengquan	111111
部门管理员	可以查看、更新、删除公司该部门的所有数据	guanli	111111
公司职员	可以查看公司的所有数据	aaaaaa	111111
公司合作伙伴用户	可以查看一部分数据	bbbbbb	111111

5.6 具体配置

服务器端配置

服务器是 Windows　2003 系统，2003 中 VPN 服务叫做“路由和远程访问”，系统默认就安装了这个服务，但是没有启用。

在管理工具中打开“路由和远程访问”

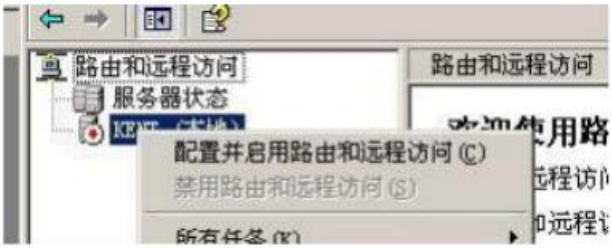

图 8 服务器端配置步骤一

在列出的本地服务器上点击右键，选择“配置并启用路由和远程访问”。下一步

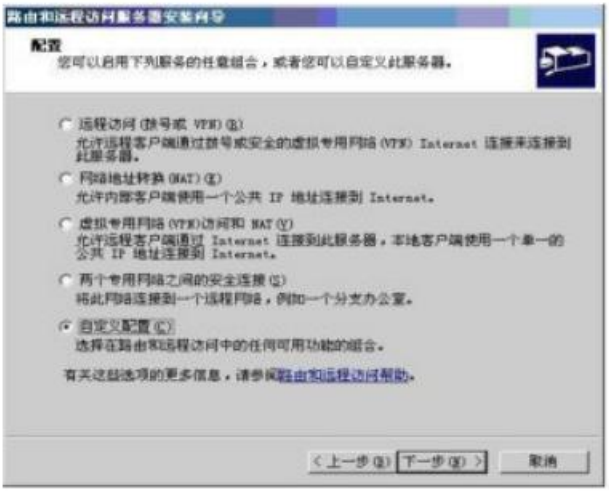

图 9　服务器端配置步骤二

在此，由于服务器是公网上的一台一般的服务器，不是具有路由功能的服务器，是单网卡的，所以这里选择“自定义配置”。下一步

图 10　服务器端配置步骤三

这里选“VPN 访问”，我只需要 VPN 的功能。下一步，配置向导完成。

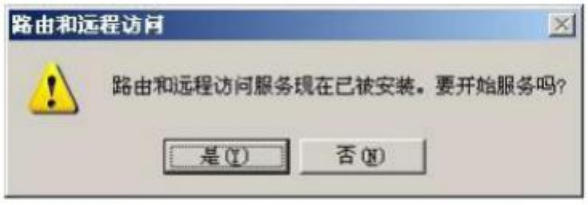

图 11 服务器端配置步骤四

点击“是”，开始服务。

看启动了 VPN 服务后，“路由和远程访问”的界面

图 12　服务器端配置步骤五

下面开始配置 VPN 服务器

在服务器上点击右键，选择“属性”，在弹出的窗口中选择“IP”标签，在“IP 地址指派”中选择“静态地址池”。

图 13　服务器端配置步骤六

然后点击“添加”按钮设置 IP 地址范围，这个 IP 范围就是 VPN 局域网内部的虚拟 IP 地址范围，每个拨入到 VPN 的服务器都会分配到一个范围内的IP，在虚拟局域网中用这个 IP 相互访问。

这里设置为 10.240.60.1-10.240.60.10，一共 10 个 IP，默认的 VPN 服务器占用第一个 IP，所以，10.240.60.1 实际上就是这个 VPN 服务器在虚拟局域网的 IP。

至此，VPN 服务部分配置完毕。

客户端配置

在控制面板中双击打开“网络和拨号连接”

图 14 客户端配置步骤一

在网络拨号中在打开“新建连接”

图 15　客户端配置步骤二

打开“新建连接”

图 16　客户端配置步骤三

左键单击“下一步”

图 17　客户端配置步骤四

选择第三项“通过 Internet 连接到专用网络”，单击“下一步”

图 18　客户端配置步骤五

在“主机名或 IP 地址这一栏”填上公司总部 VPN 服务器的 IP 地址

图 19　客户端配置步骤六

单击“下一步”

图 20　客户端配置步骤七

选择“只是我自己使用此连接”，单击“下一步”

图 21　客户端配置步骤八

在“在我的桌面上添加一快捷件方式”前打勾，单击“完成”

图 22 客户端配置步骤九

在“用户名”和“密码”两栏填上相应的用户名和密码单击连接就可以连接到相应的 VPN 网络了。

结束语

经过四个多月的学习,基本上完成了证券公司网络系统集成方案的设计。

本文件涉及到了有关 VPN 的大部分内容，比如 VPN 的好处，VPN 中的安全技术，VPN 的实现方法，VPN 的技术的应用等等。通过这次论文的写作，进一步的认识到网络技术在社会经济生活中的重要性，也再一次深入学习了网络方面的有关知识。

证券公司的发展是多方面的，这里我们只是从 VPN 网的建设的方向提供了一个参考性的网络方案，在计算机网络世界里我也只是一个小小的初学者，其中有些不足和不合理的地方，还请各位老师和同学多多的指教,同时也欢迎喜欢网络的同志们多提宝贵意见。

参考文献

[1] 【美】Craiy Zacker,Paul Doyle. 《计算机网络连网升级与维护维护大全》[M]. 西蒙与舒斯特国际出版公司，机械工业出版社.2002

[2] 【美】SaadatMalik 等 《网络安全原理与实践》[M].北京邮电出版社,2003.

[3] 刘有信.《网络互联技术》[M].人民邮电出版社.2001

[4] Cormac Long. 《IP 网络设计》[M].（第二版）人民邮电出版社.2002

[5] Steven browm.《构建虚拟专用网》[M].北京:人民邮电出版社,2001

[6] 陈天洲，陈纯，谷小妮. 《计算机安全策略》[M]. 浙江大学出版社.1999

[7] 石淑华.《用 Windows2000 实现企业 VPN 的分析与研究》[J]微机发展，2002，(5)：69--71

[8] 雷振甲.《网络工程师教程》[M]. 清华大学出版社.2004

[9] 陈学平. 《计算机网络工程与实训》[M]. 电子工业出版社

[10] 李思齐.《防火之道-Internet 安全构建深度应用》[M]. 电子工业出版社

[11] 孙为清.《VPN 隧道技术》[J]。计算机应用研究所,2000,17(8):55--58

[12] Stallings W.《虚拟专用网的创建与实现》[M].北京海洋出版社,2002.

[13] 中国教育和科研计算机网 《安全交换机的基本功能》[OL].www.cernet.edu.cn.2006.4

[14]Martin W Murhammer.《虚拟私用网技术》[M]. 清华大学出版社.2000.

[16]戴宗坤,唐三平.《VPN 与网络安全》[M].北京电子工业出版社.2002.