虚拟专用网(VPN)的研究与实现*

徐秀芳
(盐城工学院 教务处,江苏 盐城　224003)

摘　要:虚拟专用网(VPN)技术是当前热门的网络技术,它利用 Internet 公共网络进行网络互连,在减轻企业费用的同时,保证了数据的安全性。分析了 VPN 的特点,对 VPN 中数据的加密、封装和隧道协议等进行了研究,最后给出了 VPN 在目前网络中的几种实现方法。

关键词:VPN;隧道;IPSec;Intranet;Extranet
中图分类号:TP393.03　　文献标识码:A　　文章编号:1671 - 5322(2002)03 - 0021 - 04

虚拟专用网 VPN(Virtual Private Networking)作为一门新的网络技术,是目前解决网络安全传输最有效的手段之一。它采用隧道技术在公网上开辟虚拟专用通道,在远程用户、分公司、商业合作伙伴与公司的内部网之间建立可信的安全连接,并利用成熟的加密和认证技术保证了传输中数据的私有性和安全性。另一方面,利用 VPN 可以将数据流转移到低成本的 IP 网络上,从而大幅度地减少用户在 WAN 和远程网络连接上的费用。此外,VPN 还能够利用公共网络分布广泛且传输能力较强的特性,降低用户内部网络的建设成本,提高用户的网络运行和管理的灵活性[1]。

1　VPN 的隧道协议

VPN 的实现主要采用隧道技术和加密、身份认证等方法,其中,VPN 技术中的隧道是由隧道协议形成的。现在大多数的 VPN 系统中的协议主要有以下 4 种[2~3]。

1.1　点对点隧道协议(PPTP 协议)

PPTP 协议是最早被用来设计 VPN 的协议之一,被广泛用于拨号连接的对专用数据封装和加密的主要 VPN 服务。PPTP 协议(Point-to-Point Tunneling Protocol)是 PPP 协议的扩展,增强了 PPP 的身份验证、压缩和加密机制。PPTP 利用 PPP 的功能通过因特网建立一条指向目的站点的隧道来实现远程访问。PPTP 提供 PPTP 客户机和 PPTP 服务器之间的加密通信,通过 PPTP,客户可采用拨号方式接入公共 IP 网络 Internet。拨号客户首先按常规方式拨号到 ISP 的接入服务器,建立 PPP 连接;在此基础上,客户进行二次拨号建立到 PPTP 服务器的连接,该连接称为 PPTP 隧道。

1.2　第 2 层隧道协议(L2TP)

L2TP 是由 Microsoft 支持的 PPTP 和由 Cisco 支持的 L2F 相结合的产物,Bay 等网络公司均是该工作组的成员。L2TP 对 PPP 连接作了延伸:它的起点和终点并不是远程主机和 ISP 的拨号服务设备,这种虚拟的 PPP 连接起始于远程主机,终止于公司企业网的网关。从表面上看,远程主机和公司企业网的网关好像处于同一子网中。L2TP 使用 PPP(RFV 1663)来实现数据包的可靠性发送,L2TP 隧道通过在两端 VPN 服务器之间采用口令握手协议 CHAP 来验证对方的身份,并可采用 IPSec 协议对数据包进行加密传送,以保证数据安全。

在安全性的考虑上,L2TP 仅仅定义了控制包的加密传输方式,对传输中的数据并不加密。因此,L2TP 并不能满足用户对安全性的需求,当用户需要安全的拨号 VPN 时,就需要结合 IPSec 一起使用,对数据封装和加密,以创建安全的虚拟专用网络连接。

1.2.1　封装

第 1 步:L2TP 封装

* 收稿日期:2002 - 06 - 13
作者简介:徐秀芳(1973-),女,江苏盐城人,盐城工学院助教,现主要从事计算机的教学管理与研究工作。

将 PPP 框架(IP 数据包、IPX 数据包或 NetBEUI 框架)包装成 L2TP 头和 UDP 头。

第 2 步:IPSec 封装

使用 IPSec 封装安全措施负载量(ESP)的头文件和尾文件、提供消息完整性和身份验证的 IPSec 身份验证尾文件及最后的 IP 头数据包装 L2TP 结果消息。在 IP 头文件中有与 VPN 客户机和 VPN 服务器相对应的源和目标 IP 地址。图 1 显示了 PPP 数据包的 L2TP 和 IPSec 封装过程。

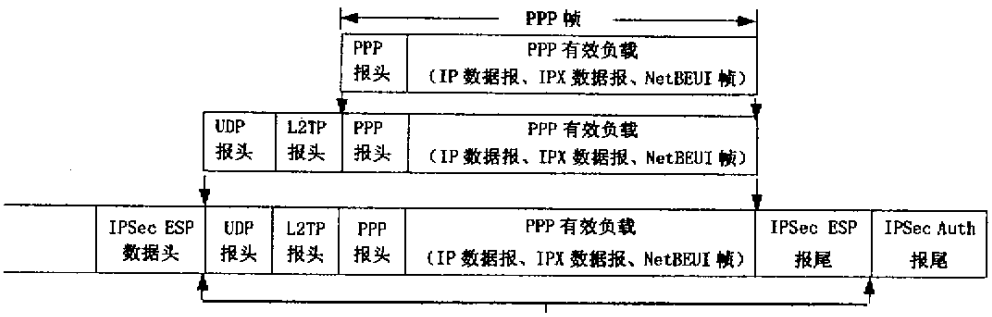

图 1 基于 IPSec 的 L2TP 数据包的封装

Fig.1 Encapsulation of L2TP data package based on IPSec

1.2.2 加密

通过使用在 IPSec 身份验证过程中生成的密钥,使用 IPSec 加密机制加密 L2TP 消息,数据包在传输之前先加密,确保其在传输过程中即使被攻击者监视或截取也不会暴露。只有具有共享密钥的计算机能够解释或修改数据。

1.3 IPSec 协议

虽然 PPTP 和 L2TP 都有它们各自的优点,但是都没有很好地解决隧道加密和数据加密的问题。而 IPSec 安全体系结构把多种安全技术集合到一起形成一个较为完整的体系,通过对数据加密、用户身份认证、数据完整性检查来保证数据传输的可靠性、私有性和完整性,从而可以建立一个安全、可靠的隧道。

IPSec 对使用 L2TP 协议的 VPN 连接提供机器级身份验证和数据加密。在保护密码和数据的 L2TP 连接建立之前,IPSec 在计算机及其远程隧道服务器之间进行协商。

IPSec 的主要目的是为 IP 数据包提供保护,它由 IP 认证头 AH(Authentication Header)、IP 封装安全载荷 ESP(Encapsulated Security Payload)和 IKE(Internet 密钥交换)3 个部分组成。

AH 协议保证了隧道中报文的数据源鉴别和数据的完整性保护,它对每组 IP 包进行认证,防止黑客利用 IP 进行攻击。

ESP 协议保证数据的保密性,ESP 可以在隧道模式和传送模式两种模式下运行。在隧道模式下,ESP 对整个 IP 数据包进行封装和加密,隐蔽了 IP 源和目的 IP 地址,从外部看不到数据包的路由过程;在传送模式下,ESP 只对 IP 有效数据载荷进行封装和加密,IP 源和目的 IP 地址不加密传送,安全程度相对隧道模式较低。

密钥管理协议是 IPSec 安全协议的一个重要组成部分,Internet 工程任务组(IETF)规定了 Internet 安全协议和密钥管理协议实现 IPSec 的密钥管理需求,这个协议在通信系统内建立了一个安全的联系,它是一个产生和交换 IPSec 密钥并对其进行管理的协议。

在上述 3 种隧道协议中,PPTP 和 L2TP 主要应用于远程访问,技术相对简单,容易实现,但缺乏可伸缩性和安全性;IPSec 不仅适用于远程访问,而且更适用于 Intranet 和 Extranet 的多点连接,具有良好的安全性、可靠性和灵活性,但技术复杂。

1.4 SOCKs v5 协议

SOCKs v5 协议是建立在 TCP 层上的安全协议,可以与特定的 TCP 端口建立特定的隧道,可以同低层的 IPSec、PPTP、L2TP 协议实现互操作。SOCKs v5 能够对连接请求进行认证和授权,建立代理连接并传送数据,可以增强系统的安全性并隐藏内部网络地址和网络拓扑结构。SOCKs v5 协议与 SSL 协议配合使用,可作为企业网络的防火墙,防止黑客通过 Internet 对企业内部网络进行攻击,SOCKS v5 通常用于 Extranet VPN。

2 VPN 的应用与实现

根据用户需求的不同,VPN 可以有多种不同的方法实现。通常情况下,有基于防火墙的 VPN、

基于路由器的 VPN、基于服务器的 VPN 和专用的 VPN 设备。用户的需求多种多样,差别可能较大,因此 VPN 产品应当能够为用户提供可伸缩的配置方案,做到量身定制,此外,VPN 的不同部件可能来自不同的厂商,所以要求它们有良好的互操作性。

VPN 的应用主要有 3 种类型:(1) Intranet VPN 用于企业网络与分支机构的连接,也称为内部 VPN 网;(2) Remote Access VPN 用于连接企业网络与远程用户和移动用户;(3) Extranet VPN 用于连接企业网络与合作伙伴和客户,也称为外连 VPN 网。VPN 可在 Internet 内建立一条隧道,经过防火墙后可保护信息的安全[3]。下面是 VPN 在这几种应用场合中的实现。

2.1　Intranet VPN

Intranet VPN 是指在一个组织内部如何安全地连接两个相互信任的内联网,要求在公司与分支机构之间建立安全的通信连接。这种应用模式需要做的不仅是要防范外部入侵者对企业内联网的攻击,还要保护在因特网上传送的敏感数据。

2.1.1　Intranet 上的远程访问

在企业 Intranet 中,某些部门的数据是非常敏感的,因此该部门的网络在物理连接上往往与企业 Intranet 上的其它部门断开。虽然这样保护了部门的数据,但是它对没有从物理上连接单独网络的用户产生了信息访问问题。在组织 Intranet 上有适当权限的用户可以与 VPN 服务器建立远程访问 VPN 连接,并可访问敏感部门网络的受保护资源。此外,为了数据机密性,所有通过 VPN 的通讯被加密。对没有授权建立 VPN 连接的用户,部门网络在视图中是隐藏的。图 2 显示了通过 Intranet 的 VPN 远程访问的过程。

2.1.2　通过 Intranet 连接网络

部门位置分散、数据高度敏感的单位,可能要使用路由器到路由器的 VPN 连接来相互通讯。例如,财务部门可能需要和人力资源部门通信,以交换工资信息。财务部门和人力资源部门连接到公用 Intranet,该处的计算机能充当 VPN 客户端或 VPN 服务器。一旦确定了 VPN 连接,各网络计算机上的用户就可以通过公司的 Intranet 来交换敏感数据。图 3 显示了通过 Intranet VPN 连接网络的原理。

2.2　基于 Internet 的 VPN

使用基于 Internet 的 VPN 连接,可以充分利用全球通用的 Internet,同时避免了长途电话的费用。

2.2.1　Internet 上的远程访问

Remote Access VPN 是指企业员工通过因特网远程拨号的方式访问企业内联网而构筑的 VPN,通常也叫做拨号访问。VPN 技术的这种应用代替了传统的直接拨入内联网的远程访问方式,这样可以大大降低远程访问的费用(不使用长途)。只需使用本地 ISP 建立的物理连接,远程访问客户即可通过 Internet 来初始化 VPN 连接到公司组织的 VPN 服务器。创建 VPN 连接后,远程访问客户即可访问 Intranet 上的资源。图 4 显示通过 Internet 的远程访问连接。

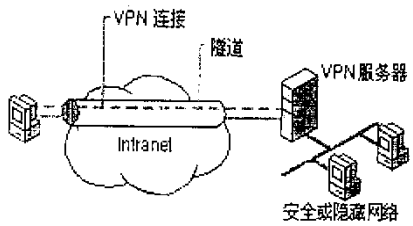

图 2　通过 Intranet 的 VPN 远程访问

Fig.2　VPN remote access through Intranet

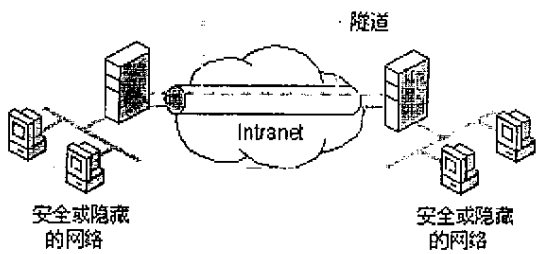

图 3　通过 Intranet 连接网络

Fig.3　Secure Network link through intranet

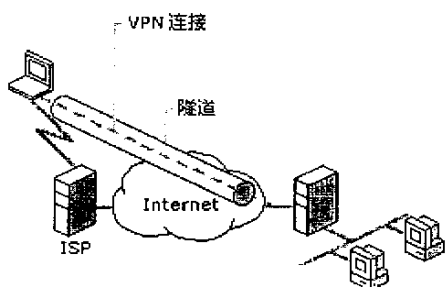

图 4　通过 Internet 的远程访问途径

Fig.4　Remote access to company network through internet

2.2.2　通过 Internet 连接网络

当网络通过 Internet 连接时,路由器通过 VPN 连接将包发送到其它路由器。对于路由器,VPN

将作为数据链路层之间的链接进行操作。图 5 是通过 Internet 的连接。

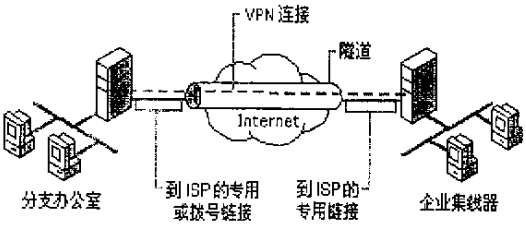

图 5 通过 Internet 连接公司网络

Fig.5 Network interlinkage between subsidiary Companies through Internet

2.3 Extranet VPN

Extranet VPN 是 Intranet 的一个扩展,是在供应商、商业合作伙伴的 LAN 和公司的 LAN 之间的 VPN,即通过因特网连接 2 台分别属于 2 个互不信任的内部网络的主机。它要求一个开放的基于标准的解决方案,以便解决企业与各种合作伙伴和客户网络的协同工作问题。考虑的重点从保护内部网免受外部攻击,扩展到同时还要保护内部网中的某些主机免受来自内部的可能攻击。对安全需求很高的公司,可在公司局域网设置两层防火墙,把局域网放在第 2 层防火墙后面,两层防火墙的中间区域即所谓的非军事区 DMZ(Demilitarized Zone)把 VPN 服务器和其它一些可以分开的服务器(如 WWW 服务器、E-mail 服务器等)放在 DMZ 区,黑客即使攻破第 1 层防火墙,还要通过 VPN 服务器的验证以及第 2 层防火墙的过滤,因此,很难达到公司内部资源网,从而保证了数据的安全性。

3 结束语

在当今信息世界,网际网络可以将远程用户连接至企业数据和应用系统,因此,采用高级的安全技术是必需的。将防火墙、NAT 和 IPSec VPN 功能集中在单一系统内,用户便可以获得高度的安全保障,而且管理起来也比较简单。VPN 代表了当今网络发展演化的最高形式,它通过 Internet 建立了安全的连接,既具有传统数据网络的优点,又具有共享数据网络的结构优点,且简单、成本低,因此,VPN 必将成为未来传输业务的主要载体。

参考文献:

[1] 彭湘凯. VPN 及其核心技术[J]. 成都大学学报,2001,(1):12.
[2] 微软公司. 实现 Microsoft Windows 2000 网络基础结构[M]. 北京:北京希望电子出版社,2001.
[3] 范志荣. 基于公共网络的虚拟专用网探析[J]. 计算机应用研究,2000,(3):28.
[4] 谢怀军. VPN 技术透视分析[J]. 中国金融电脑,2000,(10):16.

Research on and Realization of VPN

XU Xiu-fang

(Department of Studies of Yancheng Institute of Technology, Jiangsuu Yancheng 224003, China)

Abstract: VPN is pop network technology today. VPN interlinkage is realized through Internet. It decreases the cost of the corporation and at the same time, it ensures the safety of the data. In this paper, the writer introduced characteristic of VPN, and researched on the data encryption, encapsulation, tunnel protocol technology of VPN. Finally, Several realization ways of VPN are been given.

Keywords: VPN; tunnel protocol; IPSec; Intranet; Extranet