

# VPN 及其隧道技术研究

郝辉 钱华林

(中国科学院计算机网络信息中心 中国科学院研究生院 北京 100080)

**摘要:** 本文阐述了 VPN 及其实现的主要技术——隧道。先探讨了 VPN 的产生背景及其能够实现的功能,VPN 利用不可靠的公用互联网络作为信息传输媒介,通过附加的安全隧道,用户认证,访问控制等技术实现与专用网络类似的安全性能;接着分析了实现 VPN 的隧道技术和隧道协议,并着重分析了第二层隧道协议和 IPSec 第三层隧道协议的实现原理;然后对各种协议做了深入的比较,包括实现难度和性能等;最后对 VPN 的未来进行了预测并说明了技术实现的趋势。

**关键词:** VPN, 隧道, 隧道协议, GRE 封装

中图法分类号: TP393.03

文献标识码: A

## VPN and its Tunnelling Technology Study

HAO Hui QIAN Hua-Lin

(Computer Network Information Center, Chinese Academy of Sciences, Graduate School of the Chinese Academy of Sciences, Beijing 100080 China)

**Abstract:** This article presents VPN and its main implementing technology, that is the Tunnelling Technology. First, the paper analyses the emerging background and the functions it can realize of the VPN. VPN uses the fallible Internet as its information transport media, through the additional secure tunnel, authentication, access control and other technology, it can achieve the same safe functions as private network; and then the article proposes the Tunnelling Technology and Tunnelling protocol realizing VPN, and it analyses the realizing principles of layer two protocols and IPSec layer three protocols. and then it gives a compare between the protocols, including realizing difficulty, performance and so on. in the end, it forecasts VPN and shows the trends of realizing technology.

**Key words:** VPN, Tunnel, Tunnelling Protocol, GRE Encapsulation

### 1 VPN 概述

随着公司业务不断扩大,业务波及的范围也越来越大。员工要想实现建立在安全之上的信息交流和信息共享,公司内部局域网要覆盖几个城市甚至几个国家;有些要不断出差的公司员工可能会随时随地访问企业内部网络;而那些通过拨号由 ISP 动态分配的 IP 地址也无法穿越公司的防火墙及其他安全设备。

解决这些问题的一个办法是公司租用专用线路来连接不同的部门及分公司,这种方式虽然安全性高,也有一定的效率,但成本太高,并且浪费资源;同时也无法满足随时随地的接入要求;更重要的是扩展性不好,不方便新用户的接入。

VPN 利用不可靠的公用互联网络作为信息传输媒介,通过附加的安全隧道,用户认证,访问控制等技术实现与专用网络类似的安全性能,从而实现对重要信息的安全传输。这种方式成本低,并且克服了 Internet 不安全的特点。

## 2 隧道

### 2.1 隧道技术

所谓“隧道”就是这样一种封装技术,它利用一种网络传输协议,将其他协议产生的数据报文封装在它自己的报文中在网络中传输。在目的局域网和公网的接口处将数据解封装,取出负载。隧道技术是指包括数据封装,传输和解包在内的全过程。

有两种隧道类型:一是自愿式隧道,当一个客户终端利用隧道客户端软件主动与目标隧道服务器建立一个虚连接,则该连接称为自愿式隧道。这要求在该用户的终端上需要装载所需的协议并且与互联网要有连接;二是强制式隧道,在这种方式中,有一台网络设备(一般是 ISP 端的设备)代替拨号用户建立与目的地隧道服务器的隧道。

### 2.2 隧道协议

VPN 具体实现是采用隧道技术,而隧道是通过隧道协议实现的,隧道协议规定了隧道的建立,维护和删除规则以及怎样将企业网的数据封装在隧道中进行传输。隧道协议可分为第二层隧道协议 PPTP、L2F、L2TP 和第三层隧道协议 IPsec 等。它们的本质区别在于用户的数据包是被封装在何种数据包中在隧道中传输的。

无论哪种隧道协议都是由传输的载体、不同的封装格式以及被传输数据包组成的。以 L2TP 为例,看一下隧道协议的组成。

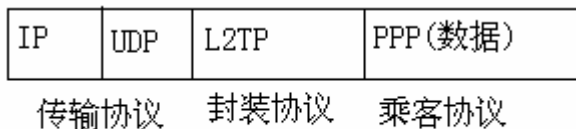


图1

传输协议被用来传送封装协议。IP 是一种常见的传输协议,这是因为 IP 具有强大的路由选择能力,可以运行于不同介质上,并且其应用最为广泛。此外,帧中继、ATM PVC 和 SVC 也是非常合适的传输协议。比如用户想通过 Internet 将其分公司网络连接起来,但他的网络环境是 IPX,这时用户就可以使用 IP 作为传输协议,通过封装协议封装 IPX 的数据包,然后就可以在 Internet 网上传递 IPX 数据。

封装协议被用来建立、保持和拆卸隧道。包括 L2F、L2TP、GRE 协议。而乘客协议是被封装的协议,它们可以是 PPP、SLIP。

隧道协议有很多好处,例如在拨号网络中,用户大都接受 ISP 分配的动态 IP 地址,而企业网一般均采用防火墙、NAT 等安全措施来保护自己的网络,企业员工通过 ISP 拨号上网时就不能穿过防火墙访问企业内部网资源。采用隧道协议后,企业拨号用户就可以得到企业内部网 IP 地址,通过对 PPP 帧进行封装,用户数据包可以穿过防火墙到达企业内部网。

## 3 第二层隧道协议

### 3.1 PPTP--点对点隧道协议

PPTP 将 PPP ( Point-to-Point Protocol ) 帧封装进 IP 数据报中，通过 IP 网络如 Internet 及其他企业专用 Intranet 等发送。PPTP 支持 Client - LAN 型隧道。

通过利用 PPP 所采用的身份验证、数据加密与协议配置机制，PPTP 连接提供了一种通过诸如 Internet 这样的公共网络针对远程访问与路由器到路由器虚拟专用网络 ( VPN ) 创建安全连接的有效方式。

PPTP 通信由以下两部分组成：

#### (一) PPTP 控制连接：

一种用以代表 PPTP 隧道并且必须通过一系列 PPTP 消息来创建、维护与终止的逻辑连接。PPTP 控制连接通信过程使用 PPTP 客户端上动态分配的 TCP 端口以及 PPTP 服务器上编号为 1723 的反向 IANA TCP 端口。

PPTP 控制连接数据包包括一个 IP 报头，一个 TCP 报头和 PPTP 控制信息，如图 2 所示：

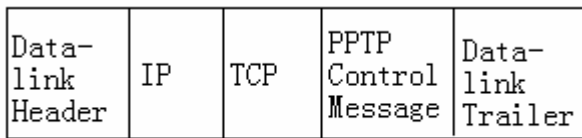


图2

PPTP 控制连接创建过程：

1. 在 PPTP 客户端上动态分配的 TCP 端口与 PPTP 服务器上编号 1723 的 TCP 端口之间建立一条 TCP 连接。
2. PPTP 客户端发送一条用以建立 PPTP 控制连接的 PPTP 消息。
3. PPTP 服务器通过一条 PPTP 消息进行响应。
4. PPTP 客户端发送另一条 PPTP 消息，并且选择一个用以对从 PPTP 客户端向 PPTP 服务器发送数据的 PPTP 隧道进行标识的调用 ID。
5. PPTP 服务器通过另一条 PPTP 消息进行应答，并且为自己选择一个用以对从 PPTP 服务器向 PPTP 客户端发送数据的 PPTP 隧道进行标识的调用 ID。
6. PPTP 客户端发送一条 PPTP Set-Link-Info 消息，以便指定 PPP 协商选项。

#### (二) 针对数据的 GRE 封装

当通过 PPTP 连接发送数据时，PPP 帧将利用通用路由封装 ( GRE ) 报头进行封装，这种报头包含了用以对数据包所使用的特定 PPTP 隧道进行标识的信息。

初始 PPP 有效载荷如 IP 数据报、IPX 数据报或 NetBEUI 帧等经过加密后，添加 PPP 报头，封装形成 PPP 帧。PPP 帧再进一步添加 GRE 报头，经过第二层封装形成 GRE 报文；第三层封装添加 IP 报头。IP 报头包含数据包源端及目的端 IP 地址。数据链路层封装是 IP 数据报多层封装的的最后一层，依据不同的外发物理网络再添加相应的数据链路层报头和报尾。

PPTP 数据包的接收处理：

1. 处理并去除数据链路层报头和报尾
2. 处理并去除 IP 报头
3. 处理并去除 GRE 和 PPP 报头
4. 如果需要的话，对 PPP 有效载荷即传输数据进行解密或解压缩。
5. 对传输数据进行接收或转发处理

PPTP 控制连接维护：

为维护 PPTP 控制连接，无论在 PPTP 客户端与服务器之间是否存在正在发送的 GRE

封装数据，PPTP 客户端每 60 秒钟发送一条 PPTP Echo Request 消息。当收到 PPTP Echo Request 消息后，PPTP 服务器发送一条 PPTP Echo Reply 消息。PPTP Echo Request 消息包含一个标识符字段，其取值随 PPTP Echo Reply 消息一同发回，从而确保 PPTP 客户端能够在其所发送的 PPTP Echo Request 消息与回复之间进行匹配。

### 3.2 L2F--第二层转发协议

L2F 是由 Cisco 公司提出的可以在多种介质如 ATM、帧中继、IP 网上建立多协议的安全虚拟专用网（VPN）的通信方式。远端用户能够透过任何拨号方式接入公共 IP 网络，首先按常规方式拨号到 ISP 的接入服务器（NAS），建立 PPP 连接；NAS 根据用户名等信息发起第二重连接，通向 HGW 服务器。在这种情况下隧道的配置和建立对用户是完全透明的。

### 3.3 L2TP--第二层隧道协议

L2TP 结合了 L2F 和 PPTP 的优点，可以让用户从客户端或访问服务器端发起 VPN 连接。L2TP 是把链路层 PPP 帧封装在公共网络设施如 IP、ATM、帧中继中进行隧道传输的封装协议。

L2TP 主要由 LAC(L2TP Access Concentrator)和 LNS(L2TP Network Server)构成，LAC(L2TP 访问集中器)支持客户端的 L2TP，他用于发起呼叫，接收呼叫和建立隧道；LNS(L2TP 网络服务器)是所有隧道的终点。在传统的 PPP 连接中，用户拨号连接的终点是 LAC，L2TP 使得 PPP 协议的终点延伸到 LNS。

L2TP 的建立过程是：

1. 用户通过公共电话网或 ISDN 拨号至本地的接入服务器 LAC；LAC 接收呼叫并进行基本的辨别，这一过程可以采用几种标准，如域名、呼叫线路识别(CLID)或拨号 ID 业务(DNIS) 等。
2. 当用户被确认为合法企业用户时，就建立一个通向 LNS 的拨号 VPN 隧道。
3. 企业内部的安全服务器如 RADIUS 鉴定拨号用户。
4. LNS 与远程用户交换 PPP 信息，分配 IP 地址。LNS 可采用企业专用地址(未注册的 IP 地址)或服务提供商提供的地址空间分配 IP 地址。因为内部源 IP 地址与目的地 IP 地址实际上都通过服务提供商的 IP 网络在 PPP 信息包内传送，企业专用地址对提供者的网络是透明的。
5. 端到端的数据从拨号用户传到 LNS。

在实际应用中，LAC 将拨号用户的 PPP 帧封装后，传送到 LNS，LNS 去掉封装包头，得到 PPP 帧，再去掉 PPP 帧头，得到网络层数据包。

## 4 IPSec 安全隧道

PPTP、L2F 和 L2TP 协议各自有自己的优点，但是都没有很好地解决隧道加密和数据加密的问题。而 IPSec 协议把多种安全技术集合到一起，可以建立一个安全、可靠的隧道。这些技术包括 DiffieHellman 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。

IPSec 安全结构包括 3 个基本协议：AH 协议为 IP 包提供信息源验证和完整性保证；ESP 协议提供加密保证；密钥管理协议(ISAKMP)提供双方交流时的共享安全信息。

IPSec 通过上述 3 个基本协议在 IP 包头后增加新的字段来实现安全保证。下面是一个 IPSec 数据包的格式。

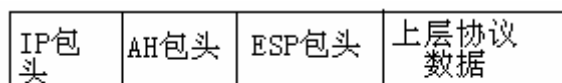


图3

AH 包头可以保证信息源的可靠性和数据的完整性。首先发送方将 IP 包头、高层的数据、公共密钥这三部分通过某种散列算法进行计算，得出 AH 包头中的验证数据，并将 AH 包头加入数据包中；当数据传输到接收方时，接收方将收到的 IP 包头、数据、公共密钥以相同的散列算法进行运算，并把得出的结果同收到数据包中的 AH 包头进行比较；如果结果相同则表明数据在传输过程中没有被修改，并且是从真正的信息源处发出的。

信息源可靠性可以通过公共密钥来保证。常用的散列算法有 HMAC，MD5 和 SHA。这些算法有一些共同的特点：

1. 不可能从计算结果推导出它的原始输入数据；
2. 不可能从给定的一组数据和它经过散列算法计算出的结果推导出另外一组数据产生的结果。

MD5 是单向数学函数，它可以对输入的数据进行运算，产生代表该数据的 128 比特指纹信息。在这种方式下，MD5 提供完整性服务。128 比特指纹信息可以在信息发送之前和数据接收之后计算出来。如果二次计算结果相同，那么数据在传输过程中就没有被改变。SHA1 与 MD5 类似，只是它产生 160 比特指纹信息，所以运算时间比 MD5 稍长，安全性更高一些。当 HMAC 和 MD5 共同使用时，可以对每 64 个字节的数据进行运算，得出 16 字节的指纹信息，并放入 AH 包头中。

AH 由于没有对用户数据进行加密。如果黑客使用协议分析照样可以窃取在网络中传输的敏感信息，所以我们使用有效负载安全封装(ESP)协议把需要保护的用户数据进行加密，并放到 IP 包中，ESP 提供数据的完整性、可靠性。

ESP 协议非常灵活，可以选择多种加密算法包括 DES、Triple DES、RC5、RC4、IDEA 和 Blowfish。

DES 是最常用的加密算法，其特点是采用 56 位的密钥，处理 64 位的输入，加密解密使用同一个密钥或可以相互推导出来。DES 把数据分成长度为 64 位的数据块，其中 8 位作为奇偶校验，有效码长为 56 位。DES 加密的第一步，将明文数据进行初始置换，得到 64 位混乱明文组，再将其分成两段，每段 32 位；第二步，进行乘积变换，在密钥的控制下，做 16 次迭代；最后，进行逆初始置换得到密文。由于计算机性能的提高，采用多台高性能服务器可以攻破 56 位 DES，所以 Triple DES 出现了，它采用 128 位密钥提高了安全性。

IDEA 算法采用 128 位密钥，每次加密一个 64 位的数据块。RC5 算法中数据块的大小、密钥的大小和循环次数都是可变的，密钥甚至可以扩充到 2048 位，具有极高的安全性。Blowfish 算法使用变长的密钥，长度可达 448 位，运行速度很快。

以上算法均要使用一个由通信各方共享的密钥，被称作对称密码算法。接收方只有使用发送方用来加密数据的密钥才能解密，所以其安全性依赖于密钥的安全。

工作模式：

IPSec 有两种工作方式：隧道模式和传输模式。在隧道方式中，整个用户的 IP 数据包被用来计算 ESP 包头，整个 IP 包被加密并和 ESP 包头一起被封装在一个新的 IP 包内。这样当数据在 Internet 上传送时，真正的源地址和目的地址被隐藏起来。在传输模式中，只有高层协议 (TCP、UDP、ICMP 等)及数据进行加密。在这种模式下，源地址、目的地址以及所有 IP 包头的的内容都不加密。

由于对称密钥存在着许多问题，密钥传递时容易泄密。网络通信时如果网内用户采用同样的密钥，就失去了保密的意义。但如果任意两个用户通信时都使用互不相同的密钥，N 个人就要使用  $N \times (N - 1) / 2$  个密钥，密钥量太大，在实际使用中无法实现，所以在 IPSec 中使用非对称密钥技术，将加密和解密的密钥分开，并且不可能从其中一个推导出另外一个。采用非对称密钥技术后，每一个用户都有一对选定的密钥，一个由用户自己保存，一个可以公开得到。它的好处在于密钥分配简单，由于加密和解密的密钥互不相同并且无法互相推

导,所以加密的密钥可以分发给各个用户,而解密密钥由用户自己保存。这样以来,密钥保存量少,N个用户通信最多只需保存N对密钥,便于管理,可以满足不同用户间通信的私密性,完成数字签名和数字鉴别。目前有许多种非对称密钥算法,其中有的适用于密钥分配,有的适用于数字签名。

IPSec 中的 AH 和 ESP 实际上只是加密的使用者, IETF 制定了 IKE 用于通信双方进行身份认证、协商加密算法和散列算法、生成公钥。

## 5 各种隧道协议比较

PPTP 和 L2TP 都使用 PPP 协议对数据进行封装,然后添加附加包头用于数据在互联网上的传输。尽管两个协议非常相似,但是仍存在以下几方面的不同:

1. PPTP 要求互联网络为 IP 网络。L2TP 只要求隧道媒介提供面向数据包的点对点的连接。L2TP 可以在 IP (使用 UDP), 帧中继永久虚拟电路 (PVCs), X.25 虚拟电路 (VCs) 或 ATM VCs 网络上使用。

2. PPTP 只能在两端点间建立单一隧道, L2TP 支持在两端点间使用多隧道。使用 L2TP, 用户可以针对不同的服务质量创建不同的隧道。

3. L2TP 可以提供包头压缩。当压缩包头时,系统开销 (overhead) 占用 4 个字节,而 PPTP 协议下要占用 6 个字节。

4. L2TP 可以提供隧道验证,而 PPTP 则不支持隧道验证。但是当 L2TP 或 PPTP 与 IPSEC 共同使用时,可以由 IPSEC 提供隧道验证,不需要在第 2 层协议上验证隧道。

与 PPTP 和 L2F 相比, L2TP 的优点在于提供了差错和流量控制; L2TP 使用 UDP 封装和传送 PPP 帧。面向非连接的 UDP 无法保证网络数据的可靠传输, L2TP 使用 Nr (下一个希望接受的消息序列号) 和 Ns (当前发送的数据包序列号) 字段控制流量和差错。双方通过序列号来确定数据包的次序和缓冲区,一旦数据丢失根据序列号可以进行重发。

作为 PPP 的扩展, L2TP 支持标准的安全特性 CHAP 和 PAP, 可以进行用户身份认证。L2TP 定义了控制包的加密传输, 每个被建立的隧道生成一个独一无二的随机钥匙, 以便抵抗欺骗性的攻击, 但是它对传输中的数据并不加密。

IPSec 与第二层隧道协议相比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, 利用它建立起来的隧道更具有安全性和可靠性。IPSec 还可以和 L2TP、GRE 等其他隧道协议一同使用, 给用户提供更灵活的灵活性和可靠性。此外, IPSec 可以运行于网络的任意一部分, 它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 机和拨号访问设备之间。当 IPSec 运行于路由器/网关时, 安装配置简单, 只需在网络设备上配置, 由网络提供安全性; 当 IPSec 运行于服务器/PC 机时, 可以提供端到端的安全, 在应用层进行控制, 但它的缺点是安装配置和管理比较复杂。

IPSEC隧道模式具有以下功能和局限:

- 1, 只能支持IP数据流

- 2, 工作在IP栈 (IPstack) 的底层, 因此, 应用程序和高层协议可以继承IPSEC的行为。

- 3, 由一个安全策略 (一整套过滤机制) 进行控制。安全策略按照优先级的先后顺序创建可供使用的加密和隧道机制以及验证方式。当需要建立通讯时, 双方机器执行相互验证, 然后协商使用何种加密方式。此后的所有数据流都将使用双方协商的加密机制进行加密, 然后封装在隧道包头内。

## 6 结束语

实现 VPN 的技术多种多样，它们各有千秋。一种趋势是将 L2TP 和 IPSec 结合起来用 L2TP 作为隧道协议，用 IPSec 协议保护数据。目前，市场上大部分 VPN 采用这类技术。

虚拟专用网（VPN）是平衡 Internet 的适用性和价格优势的最有前途的新兴通信手段之一。利用共享的 IP 网建立 VPN 连接，可以使企业减少对昂贵租用线路和复杂远程访问方案的依赖性。另外，它正快速成为新一代网络服务的基础，众多的服务供应商都纷纷推出了基于自身 VPN 传输网的各类增值服务。五花八门的新型服务，比如电子商务、应用主机托管和多媒体通信等等，这些服务类型不但可以让服务供应商找到新的利润增长点，而且还可同时维持其长期的竞争优势。

#### 参考文献

- [1] Ivan Pepelnjak, Jim Guichard, MPLS and VPN Architectures. Cisco Press, 2001 年
- [2] Adam Quiggle, Implementing Cisco VPNs: A Hands-On Guide, McGraw-Hill Companies, Inc., 2001 年
- [3] Carlton R. Davis. IPSec: Securing VPNs. McGraw-Hill Companies, 2001 年
- [4] Davis Carlton RIPSec, VPN 的安全实施, 清华大学出版社, 2002
- [5] 卢昱, 林琪, 网络安全技术, 中国物质出版社, 2001 年 2 月
- [6] 姚小兰, 李保奎, 董宁, 网络安全管理与技术防护, 北京理工大学出版社
- [7] 郭聃, L2TP 构建 VPN, 通讯世界, 2002.10
- [8] 谢杨, 虚拟专用网 VPN 系列讲座, 计算机世界, 2002, 1
- [9] 李津生, 红佩琳, 下一代 Internet 的网络技术, 人民邮电出版社, 2001 年
- [10] 戴宗坤, 唐三瓶, VPN 与网络安全, 金城出版社, 2000 年 9 月

#### 作者简介

郝辉 男, 1982 年生, 硕士。主要研究方向为计算机网络与通信, 互联网寻址技术。

钱华林 男, 1940 年生, 中国科学院计算机网络信息中心研究员, 博士生导师, 研究方向为计算机网络、网络工程和网络运行服务。