多种平台的 VPN 应用比较①

吴 刚

(达州职业技术学院 机械电子与信息工程系，达州 635001)

摘 要： VPN 技术提供更好的企业网络安全性，有多个技术体系，而且在多种平台上可以配置实现。分析主要的 VPN 隧道技术的区别，并对 Cisco IOS、Linux、Windows 三种系统平台的 VPN 配置步骤进行详细的解析，以展示平台之间的配置特色及异同。

关键词： VPN；网络安全；Cisco IOS；Linux；Windows

Comparison of VPN Application to Multiple Platforms

WU Gang

(Department of Machinery & Information Engineering, Dazhou Vocational and Technical College, Dazhou 635001, China)

Abstract: VPN technology provides better network security. There are more technology architectures. It can be realized by configuration on multiple platforms. This paper analyzes the differences of tunneling technologies of VPN, and explain the VPN configuration steps in detail on the Cisco IOS, Linux, Windows etc. It displays configuration features and differences on the platforms.

Key words: VPN; network security; Cisco IOS; Linux; Windows

远程接入企业内部网的方式有拨号接入、专线租用、网关端口映射、VPN（虚拟专用网）等。拨号接入方式成本高、速率低；专线租用成本更高、速率高，在远程接入访问量不大的情况下很浪费；网关端口映射是在防火墙上开个端口映射到内部服务器，让内部服务器直接暴露在 Internet 中，远程用户直接在 Internet 中访问该服务器可以完成某些工作，这种方式成本低，速率高，但是信息传输完全暴露在外部网中，安全堪忧；VPN（虚拟专用网）是通过 Internet 建立一条加密的传输隧道，隧道中的数据包在互联网中不可识别，远程接入的两端仿佛是在同一个内部网中，既保证了隧道中数据的安全，又共享了 Internet 的高速带宽，而且免去了专线租用的高成本，是目前广泛应用、大力发展的远程接入技术。市场上多种平台提供 VPN 的接入技术，不仅包括传统的路由器、防火墙、服务器操作系统平台，而且有多种专门的 VPN 网关设备产品。

1 VPN技术体系

主要 VPN 技术体系如图 1 所示。

		SSL(验证 IKE/令牌、加密 AES/DES/3DES、代理)	Socks5(验证、加密、代理)
TCP/UDP	TCP/UDP	TCP	TCP/UDP
IP	IPSec (封装：ESP) (验证：IKE) (加密：AES/DES/3DES) IP	IP	IP
PPTP (封装：GRE) (验证：PAP/CHAP/EAP) (加密：MPPE)	L2TP (封装：)		

图 1 主要 VPN 技术体系

① 基金项目:安徽省教育厅自然科学基金(2005KJ004ZD)
收稿时间:2010-12-05;收到修改稿时间:2011-01-07

PPTP 创建的隧道采用 PAP/CHAP/EAP 进行验证，在链路层对内网的第三层数据包进行封装，并采用 MPPE 加密，然后加上外网的 IP 头形成新的 IP 数据包；

L2TP/IPSec 创建的隧道采用 IPSec 的 IKE 证书体系进行验证（也可使用共享密钥对点对点隧道连接进行验证），在链路层对内网的第三层数据包用 UDP 方式封装，然后在第三层使用 IPSec 再次封装并签名，并采用 DES/3DES 加密，形成 ESP 载荷，之后加上外网的 IP 头形成新的 IP 数据包；

SSL 在传输层之上（会话层）采用 IKE 证书体系进行连接验证，数据传输也采用 AES/DES/3DES 加密，客户端使用浏览器通过代理连接 SSL VPN 服务器；

Socks5 在会话层也采用 IKE 证书体系进行连接验证，用 Socks5 的瘦客户端通过代理建立连接[1,2]。

几种 VPN 技术比较起来，PPTP 最简单，效率高，安全性不足；L2TP/IPSec 安全性强，支持所有应用；SSL 和 Socks5 安全性强，易于部署，但支持的应用有限，正在进一步完善之中。

2　Cisco IOS平台上实现IPSec VPN

在 CiscoIOS 平台上的 VPN 配置通常只用 IPSec 隧道，而不用 PPTP、L2TP、SSL 等创建隧道，通常相关的资料也只有 IPSec 隧道的建立方法，企业网之间的网关到网关的 VPN 是路由器之间创建 IPSec 隧道，电脑客户端要和路由器设备创建远程访问 VPN 连接需要安装 Cisco 的 VPN Client 软件。

（1）第一步：创建 ISAKMP/IKE 策略

在路由器全局配置模式下用 crypto isakmp enable 启用 IKE，并用 crypto isakmp policy 定义策略优先级。在这个步骤中，用 authentication [rsa-sig|rsa-encr|pre-share]定义身份验证方式，用 encryption 定义隧道加密方式，用 group 定义密钥分发算法，用 hash 定义摘要算法。

（2）第二步：配置身份类型

只需要指定路由器使用主机名还是 IP 地址做为身份标志，这些信息会被包含在证书当中，所以也非常重要。用 crypto isakmp identity 指定使用主机名还是 IP，为了避免多个 IP 地址造成的主机识别问题，应该采用主机名。如果用主机名，需要在本地和其他对端的路由器上用 ip host 建立一个主机名到 IP 地址的映射。

（3）第三步：配置验证密钥

有三种方式的验证密钥，预共享密钥、RSA 加密随机数和 RSA 数字证书。

①配置最简单的是 pre-share 预共享密钥，只要在本地和对端保持一致就行了，但是对于电脑客户端，密钥是很容易泄露的。对于两个企业网络之间的网关到网关的 VPN，路由器之间采用预共享密钥可以简化配置，用 crypto isakmp key 命令指定密码串。

②RSA 加密随机数。首先要定义好设备的主机名和域名，然后用 crypto key generate rsa [general-keys|usage-keys]命令生成公钥/私钥对，以后把设备的公钥摘录下来，在对端的设备使用 crypto key pubkey-chain rsa 命令及子命令添加公钥。

③RSA 数字证书。也要先用第二种方式产生 RSA 密钥对，然后用 crypto [ca|pki] trustpoint 命令指定 CA 机构的 FQDN 名，并用 enrollment url 子命令指定申请证书的链接，这个链接也是 Cisco 自己的 IOS CA 服务最方便，直接用 http://IP 地址 就行，如果用 mic－rosoft 的证书服务，额外要安装 SCEP，引用的 URL 如 http://IP 地址 /CertSrv/mscep/MSCEP.dll。再用 crpto [ca|pki] authenticate 用前面指定的 CA 机构名下载 CA 本身的证书，最后用 crypto [ca|pki] enroll 从指定的 CA 机构名下载路由器自己的证书。这种方式并没有显示地配置对端路由器的公钥数字证书，在进行隧道验证时路由器应该自动访问 CA 服务器获取对端公钥证书以验证签名。从 CA 机构获取证书的方式还有自动申请、手动申请、剪切粘贴的手动申请等方式，命令繁杂。

（4）第四步：定义用于映射条目中的访问控制列表

用 ip access-list extended 创建一个扩展访问控制列表，用于允许隧道两端的两个企业网之间互相访问。

（5）第五步：配置 vpn client 地址池

用 crypto isakmp client configuration address-pool local pool-name 命令指定地址池名，并用 ip local pool pool-name 指定客户端可以获得的地址范围。

（6）第六步：配置 vpn client 有关参数

用 crypto isakmp client configuration group group-name 指定客户端组名，用 key 子命令指定客户组的验证 password，用 pool 子命令指定客户端的 ip 地址选取的地址池名，这两个参数必须配置，其他参数还包括 domain、dns、wins 等。

第五步和第六步用在多客户端远程访问 VPN，路由器之间的网关到网关 VPN 不需要这两步。

（7）第七步：指定传输集

用 crypto ipsec transform-set trans-name 定义一个设定加密方法的传输集，加密方法如 esp-des、esp-md5-hmac 等。

（8）第八步：定义加密动态映射模板

用 crypto dynamic-map template-map seq_#定义一个序号做为模板，并用 set transform-set trans-name 将第六步的传输集作为映射的参数。

动态映射也用在多客户端远程访问 VPN，路由器之间的网关到网关 VPN 不需要这一步。

（9）第九步：配置映射

对于远程访问 VPN，在第八步后用 crypto map map-name seq_# ipsec-isakmp dynamic template-map 命令定义映射名并应用模板，用 crypto map map-name isakmp authorization list group-name 指定第六步中的客户端组名，用 crypto map map-name client configuration address respond 允许客户端从地址池获取地址。

而对于路由器之间的网关到网关 VPN，不是用上面几条命令，而是应该创建静态映射，用 crypto map map-name seq_# ipsec-isakmp 命令定义映射名，用 set peer IP 子命令限定对端路由器 IP 地址，set transform-set trans-name 子命令指定传输集，用 match address ACL-name 指定第四步定义的 ACL。

（10）第十步：在接口上激活映射

在设备接口配置模式用 crypto map map-name 激活映射[3,4]。

以上十个步骤中，第五步、六步、八步适用于多客户端远程访问 VPN，而路由器之间的网关到网关 VPN 不需要配置，另外，在对端路由器也是做相应的配置。以上可以看出，路由设备上配置 VPN 步骤多，难度大，需要熟悉的专业人员才能完成。另一方面，路由器可以支持多种不同的广域网类型，又处于企业网边界，用路由器配置 VPN 适用范围广。

3 Linux平台上实现VPN

计算机直接作为 VPN 接入服务器可以降低成本，如果企业有以前不支持 VPN 功能的防火墙产品，因为防火墙支持广域网接入，所以计算机的 VPN 服务器可以部署在防火墙内侧支持 VPN 连接。规模较大的企业网内部各局域网之间也可以用计算机的 VPN 服务器创建隧道，另外，Linux 平台是开源系统，性能和安全特征都很优秀，应用广泛，网络教学中用于实验也是低成本的方案。

Linux 平台有支持 PPTP、L2TP/IPSec、L2TP、IPSec 几种 VPN 连接方式，IPSec 方式可以和 Cisco 路由器互联，windows 平台一般是 L2TP/IPSec 捆绑的，不能单独建立 IPSec VPN，L2TP/IPSec 方式从安全性和适用范围看都很好，下面分析 L2TP/IPSec 方式创建 VPN 连接。

（1）第一步：在 VPN 服务器端下载及安装组件。

这些组件包括 ppp（PPP 主程序）、openssl（生产证书的主程序，如果使用预共享密钥可以不要）、xl2tpd（L2TP 拨入服务器）、openswan（IPSec 主程序，2.6.22 版以上可以支持 NAT），另外对 Linux 系统的内核要 2.6.6 以上才能支持 NAT。

WindowsXP 客户端自带 L2TP/IPSec 拨号组件可以很方便地拨号建立 VPN 连接。

（2）第二步：操作 openssl 以生成 CA 自身的证书、VPN 服务器证书、VPN 客户端证书。

用带选项的 openssl 命令来生成各种证书，并将 VPN 服务器的公钥证书、私钥证书、CA 公钥证书复制到到 VPN 服务器对应目录中。

如果使用预共享密钥进行隧道验证的话就不用这一步了。

（3）第三步：配置/etc/ipsec.conf 文件。

主要用于配置本地和对端的 IP 地址、验证方式、证书、协议端口等。其中，Left=配置左端 IP，right=配置右端 IP（用%any 自动获取），leftsubnet=和 rightsubnet=指定左端企业网和右端企业网子网范围，pfs=no/yes 配置预共享密钥验证或者 RSA 密钥验证，leftrsasigkey=配置左端 RSA 验证密钥（加密随机数），rightrsasigkey=配置右端 RSA 验证密钥（加密随机数），如果使用 authby=rsasig 指定用 RSA 证书验证，则 leftrsasigkey=%cert，rightrsasigkey=%cert，leftcert=和 rightcert=指向证书文件，如果 VPN 服务器在 NAT 转换设备后面需要使用 nat_traversal=yes 选项。

（4）第四步：配置/etc/ipsec.secrets 文件指定预共享密钥。

这个配置格式是：源 IP 目标 IP：PSK “密钥串”，多行 IP 地址对可以为多个连接配置单独的预共享密

钥。如果采用 RSA 密钥（加密随机数）或者证书文件就不用指定预共享密钥了。

（5）第五步：配置/etc/xl2tpd/xl2tpd.conf 文件。

主要用于配置 L2TP 拨号的接入参数。其中，listen-addr 指定 l2tpd 监听的 IP 地址,默认情况下，l2tpd 将监听本机所有 IP 地址；ip range 指定供远程用户使用的一段内网 IP 地址范围；local ip 指定供 Linux 服务器上隧道接口 ppp0 使用的 IP 地址。这个 IP 地址必须是内网的有效地址，这个 IP 地址必须属于 ip range 相同的网络，但是它又不在 ip range 中；require chap=yes 和 refuse pap=yes 设置口令加密方式，一般情况下启用 CHAP 并且禁止 PAP；require authentication=yes 来启用 PPP 认证；pppoptfile = /etc/ppp/options.l2tpd 指定包含其它拨号选项的配置文件；auth file = /etc/ppp/chap-secrets 指定 PPP 登录验证用户名和密码的配置文件。

（6）第六步：配置/etc/ppp/options.xl2tpd 文件。

用于指定 PPP 连接的参数。其中，ms-dns 指定客户端自动获取隧道接口的 DNS 服务器地址；mtu 指定帧最大长度；auth 是启用 PPP 登录验证；defaultroute 指定缺省路由，也可用 nodefaultroute 自动使用服务器隧道接口地址；客户端强制使用 ms-chapv2 验证方式的话，需要用+mschap-v2 选项，这也需要 pppd 服务版本支持，不过 windows 客户端一般支持含 chap 的自动协商。

（7）第七步：配置/etc/ppp/chap-secrets 文件。

用于配置客户端拨号验证用户名和密码。包括四个字段：用户名、密码串、客户端 IP，例如：user1 * password1 192.168.1.130 ，IP 地址和服务器都可以用*通配符，则拨号到本服务器 IP 的用户获取的地址从第五步 /etc/l2tpd/l2tpd.conf 文件中指定的 IP 范围中选择[5,6]。

整个过程中用到的密码串有两个，一个是 IPSec 预共享密钥，用于隧道验证，要保持隧道两端一致，在第四步设置；另一个是 PPP 拨号验证的用户名和密码串，用于拨号验证，在第七步设置。

以上是 Linux 平台 VPN 服务端配置步骤，如果是网关到网关的 VPN，使用 IPSec VPN 方式更方便，不需要配置 L2TP，对端的 Linux 服务器也做相应的配置；如果对端是 Linux 客户端也只需要配置 IPSec，但要配置为 RoadWarrior 模式。Linux 平台的网关到网关模式同 RoadWarrior 模式配置的区别是，前者/etc/ipsec.conf 文件中 Left 和 Right 是相同的，通讯的主机处于固定的位置上，而后者 RoadWarrior 配置，Left 就是自己（Local），Right 就是远程主机（Remote）。如果是 windowsXP 客户端则集成了 L2TP/IPSec 拨号工具且无法单独使用 IPSec VPN 方式。

4 Windows平台上实现VPN

基于 windows 的 VPN 功能很完善，windows server 2003 发行包中集成了路由和远程访问组件，将路由功能、远程访问接入服务、NAT 转换服务、VPN 服务都集成在这个组件中，使用很方便。Windows 平台的 VPN 功能也支持网关到网关方式和客户端远程访问方式，应用的隧道协议有 PPTP 和 L2TP/IPSec 两种，在此以 L2TP/IPSec 协议和网关到网关的方式为例说明。

（1）第一步：从 CA 证书服务器获取 CA 自身的证书、VPN 服务器网关证书。

当然，可以到互联网的证书网站申请，不过 windows server 2003 发行包中集成了证书服务器组件，可以用来创建企业独立的 CA。安装证书服务组件之前必须先安装 IIS 这个 WEB 服务器而且要求支持 ASP。在证书服务的 web 页面选择“高级证书申请”，然后证书类型应为“服务器身份验证证书”，建议“标记密钥为可导出”以方便密钥备份。如果是客户端就应该选“客户端身份验证证书”了。

在 VPN 服务器上是用 MMC 管理控制台，添加“证书单元”，并把下载的 CA 证书安装到“信任的根 CA”，CA 证书链安装到“中级证书颁发机构”，VPN 服务器自身的证书安装到“个人”分类中。如果网关之间的隧道验证使用预共享密钥，就不需要这一步了。

（2）第二步：启用管理工具中的“路由和远程访问”服务。

网关 1 和网关 2 都要设为 LAN 和请求拨号路由器，这样双方都可以提起 VPN 的初始化请求。

（3）第三步：添加连接对端 VPN 网关的网络接口。

这会启动一个向导界面，首先设置接口名称，要用对端登录到本机的用户名作为接口名，如 cquser；然后选择连接类型为 VPN，VPN 类型建议为 L2TP；设置对端网关的公网 IP；允许路由并用接口名添加帐号；添加本地内网 IP 范围到静态路由；为拨入帐户设置验证密码；最后设置拨出到对端的帐号和密码。

（4）第四步：设置预共享密钥。

在 VPN 拨号连接的属性中设置预共享密钥，预共享密钥要保持两端相同。如果使用证书进行身份验证，就不需要这一步了[7,8]。

网关 2 服务器也做上述步骤的相应配置。如果对端是 windowsXP 远程访问客户端，在 XP 的网络连接管理中新建 VPN 拨号连接，不过也需要安装证书或者设置预共享密钥，另外拨号验证的用户名和密码在 VPN 服务器中必须存在，且该用户允许拨入。

5 三种平台的VPN技术比较

用表 1 来表示几种平台的 VPN 实现的特点及性能比较。

表 1 三种平台的 VPN 技术比较

	Cisco IOS	Linux	Windows
成本/价格	高	低	中
适用环境	企业网边界	防火墙内侧	防火墙内侧
配置方式	命令行	配置文件	图形向导
配置复杂度	难	难	简单
通信性能	强	中	中
安全性	强	强	中

6 结语

本文分析了主要的 VPN 隧道技术的区别，并对 Cisco IOS、Linux、Windows 三种系统平台的 VPN 配置步骤进行详细的解析，以展示平台之间对 VPN 技术的配置特色及异同。其实市面上早已有成熟的专用 VPN 产品，这些硬件产品性能好、配置简便、价格各异。不过很多场合我们并不需要专用的 VPN 产品，而是希望在以前的路由器或服务器上集成 VPN 功能以减少设备，而且希望通用平台的配置更趋于简便和高性能，所以研究通用操作系统平台的 VPN 技术仍然有意义。

参考文献

1 徐家臻,陈莘萌.基于 IPSec 与基于 SSL 的 VPN 的比较与分析.计算机工程与设计,2004,26(4):586−588.
2 操惊雷.VPN 安全性分析与应用.黄冈职业技术学院学报,2002,(4):77−79.
3 Deal R. Cisco VPN 完全配置指南.北京:人民邮电出版社,2007.451−510.
4 丛日权.VPN 构建实战—在 Cisco 路由器之间配置基于 IPSec 的 VPN.网管员世界,2005,(5):110−111.
5 郝占军,党小超.Linux 中基于 IPSec VPN 的教育城域网研究与实现.现代计算机(下半月版), 2009,(8):156−159.
6 唐浪,孟相如,陈莉.基于 Linux 的 IPSec VPN 网关的设计与实现.计算机应用与软件,2008,25(12):138−140.
7 刘黎明,张松娟.Windows 2003 Server 下构建 VPN 网络.网管员世界,2009,(1):37−41.
8 赵婧如,王宣政.基于 Windows2000 路由器到路由器 VPN 的设计与实现.西安邮电学院学报,2005,10(4):131−135.

(上接第 224 页)

参考文献

1 赵欣然.基于 μC/OS-Ⅱ系统的 USB 驱动程序的设计[硕士学位论文].呼和浩特:内蒙古师范大学,2009.
2 Mark S. USB Embedded host controller:for removable mass storage devices. Elektor Electronics, 2004, 23(30): 58−63.
3 张德旭.基于 ARM 的嵌入式 USB 主机系统的研究[硕士学位论文].哈尔滨:哈尔滨理工大学,2009.
4 韩志耕,王健.实时内核 μC/OS-II 在 S3C44BOX 上的移植的研究与实现.计算机工程与设计,2006,27(5):828−831.
5 傅得立.基于 USB2.0 的数据记录回放单元设计[硕士学位论文].成都:中国科学院光电研所,2007.
6 陈莉君.Linux 内核设计与实现.第 2 版.北京:机械工业出版社,2009.60−61.