SSL VPN 隧道技术研究与应用

董 辉[1,2],于润桥[1],沈 翀[2]
(1.南昌航空大学 测试与光电工程学院,江西 南昌 330063;
2.福建星网锐捷网络有限公司,福建 福州 350000)

摘 要:阐述了SSL VPN隧道技术以及它在实际项目中的应用。介绍VPN技术的产生背景和采用的关键技术,对新兴的VPN解决方案——SSL VPN隧道协议原理进行分析研究;结合实际项目情况,介绍了SSL VPN在教育城域网中的应用实现;对SSL VPN技术现有优势和适用范围做出总结。

关键词:虚拟专用网;隧道技术;隧道协议;SSL
中国分类号:TP393 **文献标识码**:A **文章编号**:1674-7720(2012)24-0054-04

Tunnel technology research and application of the SSL VPN

Dong Hui[1,2], Yu Runqiao[1], Shen Chong[2]
(1.College of Test and Optoelectronic Engineering, Nanchang Hangkong University, Nanchang 330063, China;
2.The Ruijie Co., Ltd. of Fujian Star-net Network, Fuzhou 350000, China)

Abstract: This paper presents the SSL VPN tunneling technology and its application in practical projects. Firstly, VPN technology's background and the use of key technologies are introduced; then the paper analyzes the principle of the emerging VPN solution-SSL VPN tunneling protocol; and then combining with the actual project, it gives an introduction of the SSL VPN's application in the Education MAN. Finally, a summary of the existing advantages of SSL VPN technology and scope will be made.

Key words: VPN; tunneling technique; tunneling protocol; SSL

随着现代企事业单位业务的多样化发展和单位本身需求的不断增长,单位总部与分部之间、出差员工之间的联系日趋紧密。怎样利用公共互联网建立一个安全的、专用的网络以实现单位、员工之间的信息交流和信息共享已成为时代之需。专用线路(如帧中继、DDN、ATM等)因其成本高、不灵活且资源不能合理利用而令很多企业望而却步,虚拟专用网VPN(Virtual Private Network)的出现可以从根本上满足企事业用户的低通信费和高灵活性的双重需求,更重要的是它可以提供与专线相媲美的通信安全保障,是一种低成本、安全、灵活的远程网络接入解决方案[1]。SSL VPN作为VPN新技术的一种,因其简洁的Web登录模式、较低的维护管理费用和良好的安全性逐渐被广泛关注。

1 隧道技术

隧道技术是实现VPN的关键技术之一,也是VPN技术的核心。VPN就是依靠隧道技术跨越基于IP协议的公用网络建立起来的一条透明的虚拟通道,可达到公网虚拟专用的目的,这个虚拟通道即称为一个隧道。

隧道技术的核心是隧道协议[1]。为建立一个隧道,隧道两端的客户机和服务器必须使用相同的隧道协议。隧道协议用附加的带有路由信息的报头封装数据帧,它规定了隧道建立、维护、删除规则以及数据在隧道中的封装及传输原理。隧道可以在TCP/IP网络模型的任何一层上建立。按照封装后的数据包在OSI参考模型传输层次的不同,隧道协议可分为第二层协议、第三层协议以及上层(Upper Layer)隧道协议。VPN技术各层隧道协议与OSI参考模型对应关系如图1所示[2]。

第二层隧道协议也称数据链路层隧道协议,在网络中的数据链路层运行。先把各种网络协议封装到PPP包中,再把整个数据包装入隧道协议中,这种经过两层封装的数据包由第二层协议进行传输。第二层隧道协议有L2F、PPTP、L2TP等。

第三层隧道协议也称网络层隧道协议,在网络层运行。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。第三层隧道协议主要有GRE和IPSec等。

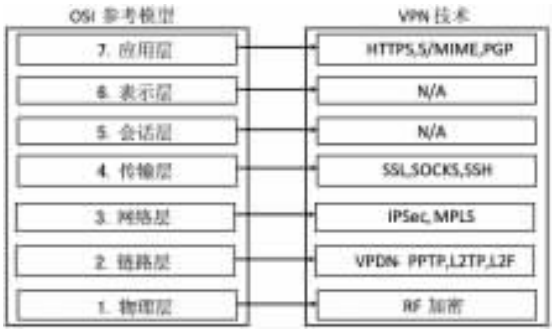

图 1 OSI 参考模型与 VPN 隧道协议

上层(Upper Layer)隧道协议在传输层或其上层运行。把上层传来的数据进行加密等处理后,由传输层把数据传输出去。在这一层工作的协议主要是安全套接协议 SSL(Secure Socket Layer)。SSL 是一种新兴的 VPN 解决方案,与其他 VPN 相比其主要优点是用户使用网页浏览器登录而不需要安装任何专门的客户端软件[3]。

2 SSL 隧道协议[1,4]

SSL 是 Netscape 公司设计的主要用于 Web 的安全传输协议。SSL 技术位于 OSI 参考模型的传输层和应用层之间,最初主要是为 TCP 提供一个可靠的端到端的安全服务。同 IPSec 协议类似,它不是一个单独的协议,而是由多个协议组成的一个两层的协议体系,包括 SSL 握手协议(SSL Handshake Protocol)、SSL 修改密文规约协议(SSL Change Cipher SpecProtocol)、SSL 警告协议(SSL Alert Protocol)和 SSL 记录协议(SSL Record Protocol)。如图 2 所示。图示体系结构分为两层:握手层协议层和记录层协议层。其中握手层协议层包含 3 个协议,即 SSL 握手协议、SSL 密钥更改协议和 SSL 告警协议。

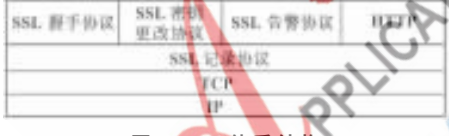

图 2 SSL 体系结构

2.1 握手层协议

握手层协议用来在客户端和服务器端传输应用数据之前建立安全通信机制,并保持通信双方进行安全通信所需的安全参数及状态信息。它使得服务器和客户机能够进行双向的身份认证,并协商加密算法、MAC(消息认证代码)算法以及 SSL 记录中所用的加密密钥。

首次通信时,双方通过握手层协议协商密钥加密算法、数据加密算法和报文摘要算法;然后互相验证对方身份,最后使用协商好的密钥交换算法产生一个只有双方知道的秘密信息,客户端和服务器端各自根据这个秘密信息确定数据加密算法的参数(一般是密钥)。

握手层协议过程分为如下 4 个阶段:

(1)建立安全能力。主要包括协商压缩算法、报文摘要算法、加密算法以及 SSL 版本、会话标识符等安全参数与状态信息。

(2)服务器认证和密钥交换。此时服务器向客户发送其数字证书,利用该证书对服务器进行认证。

(3)客户认证和密钥交换。此时客户向服务器发送其数字证书,利用该证书对客户进行鉴别。

(4)握手结束阶段。握手建立过程如图 3 所示。

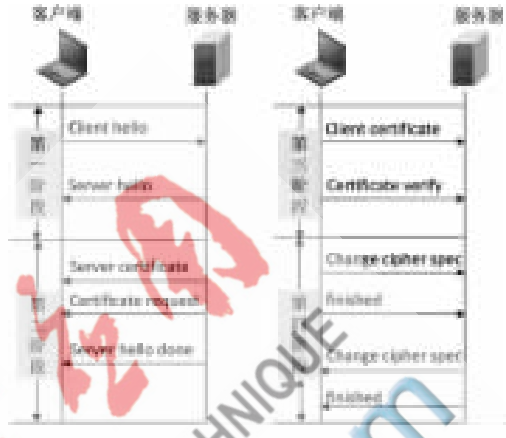

图 3 SSL 协议握手建立过程

首先客户端启动握手请求,发送 Client Hello 消息给服务器端,消息中包括客户端支持的各种算法。若对端服务器不能支持,则本次会话失败,握手协议不能建立。

服务器收到客户端发来的 Hello 消息后发送 Server Hello 消息进行回复,并向客户端发送 Server Certificate 证书消息,证书类型一般为 x.509v3(若此阶段服务器不使用证书,或证书中提供签名而不提供密钥时,服务器发送密钥交换信息 Server Key Exchange)。Certificate Request 消息用于服务器向客户端要求一个客户证书。Server Hello Done 消息表示服务器端的握手请求报文已经发送结束,正等待客户端的回应信息。

客户端收到 Server Hello Done 消息时检查服务器提供的证书以及其他参数是否有效。Client Certificate 是客户端对服务器 Certificate Request 消息的响应,只有在服务器端要求客户证书时使用。一般该消息是客户端收到 Server Hello Done 消息后所发送的第一条消息。若客户端没有合适的证书,则向服务器端发送 No Certificate 的告警消息(无证书可能导致握手失败。当客户不使用证书,或其证书中仅提供签名而不提供密钥时,使用 Client Key Exchange 消息来交换密钥)。Certificate Verify 消息用于向服务器提供对客户证书的验证。

当客户端发出修改密钥协议(Change Cipher Spec)消息之后,发出 Finished 消息,至此完整的握手消息交换已经全部完成。

握手协议完成之后,客户端与服务器端传输应用加密数据。应用加密数据一般为密钥协商时确定的对称加解密密钥,如 DES、3DE 等。SSL 中的握手协议将公钥加密技术与对称密钥加密技术的应用有效、巧妙地结合在一起,有机地组成了互联网(或其他网络)上信息安全传输的通道。

2.2 记录层协议

记录层协议定义了要传输数据的格式，它位于可靠的传输协议 TCP 之上，用于各种更高层协议的封装。主要提供数据分块、压缩、添加 MAC、加密以及完整性服务，把应用数据封装成多条记录进行传输。协议数据采用SSL 握手协议中协商好的加密算法及 MAC 算法进行保护。记录层协议传送的数据包括一个序列号，这样就可以检测消息的丢失、改动或重放。协商好压缩算法后，SSL 记录协议还可以执行压缩功能。如图 4 所示。

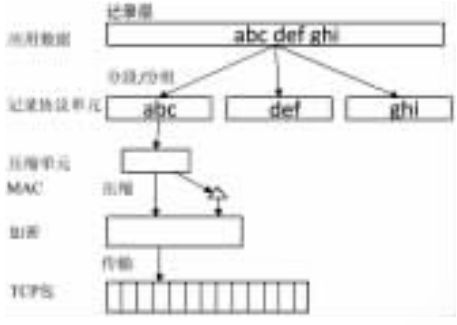

图 4 SSL 协议记录层工作模式

发送数据时，将数据分成可操作的块，对各分块单元进行压缩，接着再添加上由 HASH 算法得出的 MAC 值并加密，最后加上记录协议头部进行传输；接收方接收数据后，首先对其进行解密，接着校验 MAC，然后对各单元解压并重新组合，把结果提供给相应的应用程序协议。

3 SSL VPN 技术特点[5-6]

SSL 运行于网络体系结构中的传输层和应用层之间，它独立于应用，因此任何一个应用程序都可以利用它的安全性而不必考虑执行细节。另外，SSL 本身可以被几乎所有的 Web 浏览器支持，这意味着客户端不需要为了支持 SSL 连接而安装额外的软件。这两个特征就是 SSL 能应用于 VPN 的关键原因。SSL VPN 技术的发展是对现有 SSL 应用的一个补充，它增加了企业执行访问控制和安全性的级别和能力。到目前为止，SSL VPN 是解决远程用户访问单位内部数据最简单且安全的解决方案。与复杂的 IPsec VPN 相比，SSL VPN 通过简单易用的方法实现了信息的远程连通。SSL VPN 主要有以下技术特点：

(1)部署与应用：SSL VPN 设备部署灵活方便，以桥接或侧挂方式接入对原网络拓扑结构不会造成影响。在终端，用户可以在任何安装了 Web 浏览器的 PC 上进行 SSL VPN 拨号登录访问内部网络资源。这也是无需安装客户端软件的 SSL VPN 的主要优势。

(2)访问控制：SSL VPN 能对加密隧道进行细化，使终端用户能够同时接入 Internet 和访问内部企业网资源。另外，SSL VPN 还可以对接入控制功能进行分级，提供不同等级的用户权限，依据安全策略授权不同权限的用户访问不同的内部网络资源。

(3)安全性：SSL 安全通道建立于客户与所访问的资源之间，客户对资源的每一次操作都需要经过身份验证和数据加密，保障了远程连接过程中传输数据的安全。

(4)远程连接：SSL VPN 工作在传输层之上，能够遍历所有的 NAT/PAT 设备以及防火墙设备，这使得用户可以从任何远程网络访问到内网资源，极大地方便了出差用户的远程办公。

4 SSL VPN 应用实例

为满足 L 市教育城域网各校区教职工远程办公的需要，该网络建设之初便设计 SSL VPN 远程访问解决方案。出差教职工利用当地 ISP 提供的 VPN 服务，就可以与学校的 VPN 网关建立私有的隧道连接，使远程用户随时随地地以其所需的方式访问学校内部网络资源，实现远程办公或者家庭办公。

4.1 L 市教育城域网特点

L 市教育城域网共有 3 个大校区，分别为东区高校区、西区中学和北区中学，每个区下属 15~40 个中学。为实现各校区之间的高速互联，在核心配置了两台 S12000 系列核心路由交换机，每个大校区各放置了一台 S8610 交换机。全网采用网状组网类型，物理接口采用万兆或千兆光口高速互联。L 市教育城域网设计有两个出口，分别为中国联通出口和 CERNET 教育网出口。SSL VPN 网关设备采用侧挂的方式与核心交换机相连接，如图 5 所示。

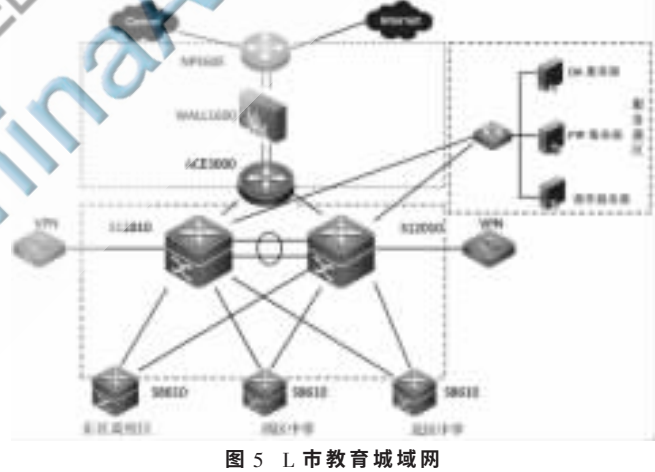

图 5 L 市教育城域网

4.2 SSL VPN 接入平台

L 市教育城域网建设的 SSL VPN 主要应用是内部网页浏览、电子邮件以及文件传输等业务。通过一个拥有与专用网络相同策略的共享基础设施，可以对校园内网资源随时随地进行远程访问。能随时使用包括如模拟拨号 Modem、ISDN、数字用户线路(xDSL)无线上网等拨号技术，安全方便地连接远程工作者。其接入平台拓扑如图 6 所示。

L 市教育城域网的 SSL VPN 平台由一台高性能防火墙、VPN 网关 RG-FW1600V、线路负载均衡设备 RG-NPE 组成。通过网络出口的负载均衡设备与电信运营商

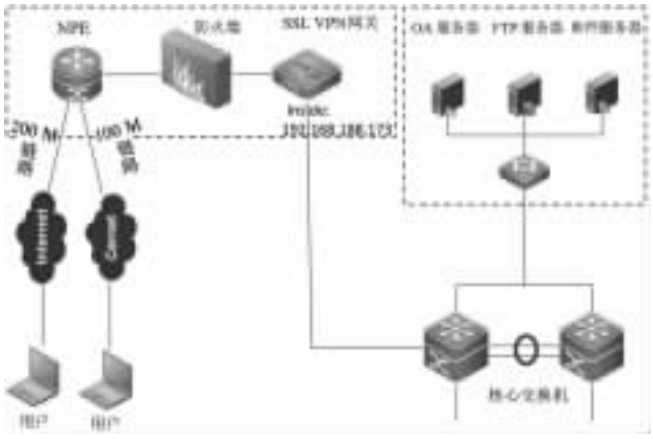

图 6 L 市教育城域网 SSL VPN 接入平台

提供的互联网线路相连，出口租用联通 200 M、教育网 100 M 的线路以保障带宽需求及链路热备。通过运营商与 VPN 接入平台的接口线路构建 VPN 隧道接入办公网。

4.3 SSL VPN 登录

SSL VPN 技术帮助用户使用标准的 Web 浏览器就可以通过公共网络平台接入所要访问的远程资源。在用户终端上，不需要安装客户端软件及进行复杂的配置，大大方便了用户，仅仅通过一台接入了 Internet 的计算机就能访问远程资源。

用户使用 Web 界面进行 SSL VPN 拨号登录，与 SSL VPN 网关协商完毕，建立 VPN 隧道后，用户并没有获得校内资源外网的地址，用户所获得的是 VPN 网关通过 DHCP 方式所分配的虚拟 IP 地址。每个用户所获得的虚拟 IP 是不同的，VPN 网关用虚拟 IP 来区分不同用户的 VPN 隧道。

当多个用户同时登录时，VPN 网关的支持情况如图7所示。

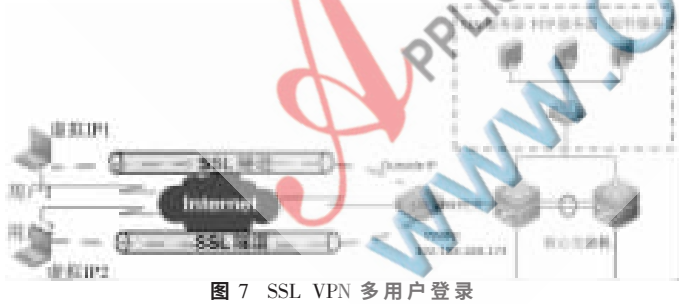

图 7 SSL VPN 多用户登录

用户在获得虚拟地址后访问校园内部资源时，经过 VPN 网关时要进行地址转换，转换为 VPN 网关的内口地址，由于 VPN 网关的内口地址只有一个，多用户登录转换完毕后，不同的虚拟 IP 转换成内网地址并对应不同的端口号。也就是说，在访问校园网内部资源时用 VPN 网关的内口地址和端口号来对接入用户进行区分。

至此，SSL VPN 连接成功。用户可以像在单位一样使用本地的 IP 地址访问内网资源，方便快捷地处理日常办公事务。

SSL VPN 技术以其简洁、低成本和良好的网络安全管理措施将逐渐成为首选的远程访问解决方案，同时 SSL 协议所采用的加密算法和认证算法也使它具有较高的安全性。但是，由于 SSL VPN 只对通信双方单个应用通道进行加密，不是对通信双方主机之间的整个通道加密，所以对安全性要求较高的行业远程系统建设建议采用 IPSec VPN 技术或 IPSec VPN 和 SSL VPN 混合接入的方式进行安全防护。

参考文献

[1] 王达.虚拟专用网(VPN)精解[M].北京：清华大学出版社，2004.
[2] CARMOUCHE J H.IPsec virtual private network fundamentals[M].Cisco Press，2006.
[3] DEAL R.The complete cisco VPN configuration guide[M].Cisco Press，2005.
[4] 张学杰，李大兴.SSL 技术在构建 VPN 中的应用[J].计算机应用，2006，26(8)：1827-1830.
[5] 马淑文.SSL VPN 技术在校园网中的应用与研究[J].计算机工程与设计，2008(11):5137-5143.
[6] 何亚辉.基于 SSL 协议的 VPN 技术研究及在校园网中的应用[J].重庆理工大学学报(自然科学版)，2011，25(2)：86-90.

(收稿日期：2012-08-23)

作者简介：

董辉，男，1985 年生，硕士在读，主要研究方向：网络技术与应用。

于润桥，男，1963 年生，硕士，教授，主要研究方向：电磁检测技术与仪器。

沈翀，男，1974 年生，硕士，高级工程师，主要研究方向：软件开发。