文章编号:1674－2869(2015)07－0075－04

采用 OpenVPN 的虚拟专用网设计方案

伊芸芸
安徽工程大学计算机与信息学院,安徽 芜湖 241000

摘　要:对于做科研的教师和学生,经常使用校园资源查询一些科研资料,由于 IP 地址的限制,只有位于校园网的电脑才能访问这些资源,回到家中或离开了学校,就无法使用这些资源,为了解决这个问题,需要建立一个虚拟专用网. 在不改变现有网络结构的情况下,采用 OpenVPN 技术,建立基于校园环境的虚拟专用网方案,采用用户名密码的认证方式,不使用证书认证方式,这样方便系统维护和客户使用. 同时该方案还实现了实时查看用户的状态,上线和下线时间,防止多用户同时用一个账号登陆虚拟网的功能,通过配置 Linux 自带的防火墙,保障了校园网的安全,最终实现了一个低成本高安全的虚拟专用网. 经过数月的运行,表明该虚拟专用网负载能力强,速度快,稳定性好.

关键词:OpenVPN;VPN;虚拟专线;校园网
中图分类号:TB35　　**文献标识码**:A　　**doi**:10. 3969/j. issn. 1674-2869. 2015. 07. 016

0　引　言

校园网资源对于做科研的教师和学生越来越重要,已经难以离开它们了,但是由于 IP 地址的限定,只能在校园内的主机才能访问校园网资源,对于住在校外的教师和假期回家的学生来说,就无法使用校园网资源了,一方面给他们带来了不便,另一方面也使得校园网资源不能充分利用. 为了解决这个问题,很多学校使用各种方式实现 VPN. **文献[1]**通过对 OpenVPN 技术改造,通过 StoneVPN 技术实现了较为安全的 VPN,**文献[2]**提出了在校园网环境下实现了一种虚拟专用网,并实现了 NAT,DNS 和访问控制,**文献[3]**提出了一种 WH-VPN 技术,该技术会对每一个数据包都要进行安全处理,降低了网络速度,它一旦接入 Internet 后,性能和质量往往很难控制,**文献[4]**使用 Windows 系统作为服务器建立 VPN,虽然操作简单,但是系统的稳定性无法保障.**文献[5]**设计了一种 Lan-to-Lan VPN,在 Centos6.04 操作系统下运行,性能比较稳定,但是缺乏必要安全配置,对网络的攻击抵御能力较弱,以上文献中均提到了建立一种 VPN 的技术方案,大部分对其安全性没有做有力保障,不能做到一个账号只能一个用户使用,本文使用Open-VPN 技术和防火技术提出了一个快速安全的基于校园网环境的 VPN 技术方案,实现了一个账号只能一个用户使用,提高了系统的安全性.

1　OpenVPN 技术

1.1　概　述

VPN 就是虚拟专用隧道,提供给企事业之间或个人与企业之间的一种安全的数据传输通道,OpenVPN 是 Linux 下开源软件,使用 Openssl 库加密数据与控制信息,能够使用任何 Openssl 支持的加密算法.

1.2　原　理

OpenVPN 支持 Tun 和 Tap 方式,其中Tun 方式使用 Udp 协议,传输速度较快,但是当网络丢包严重的情况下,效率极其低下,而 Tap 方式使用 Tcp 协议,具有良好的稳定性,当建立网络连接时,会自动创建一块虚拟的网卡,该网卡可以像真实的网卡一样工作,可以配置 IP 地址,网关,域名,路由出口等. 当有数据传送时,数据首先发往虚拟网卡,相关服务程序能够读到该数据并做相应的处理,通过 Socket 从外网上发送出去,当远程接收到该数据后,相关服务程序经过处理后发往虚拟网卡,应用软件可以读到该数据,从而完成了一次单向的传输.

1.3　验证方式

OpenVPN 支持基于证书的验证方式和用户名

收稿日期:2015-06-
基金项目:安徽工程大学青年基金(2007YQ031)
作者简介:伊芸芸(1981-),女,山东蒙阴人,讲师,硕士. 研究方向:网络与数据库.

密码的的认证方式,基于证书的认证方式必须为每个用户创建安全证书,当用户长久不用时也可以吊销该证书,基于用户名和密码的认证方式,灵活性大,需要第三方数据库支持.

2 设计方案

2.1 功能定义

在不影响现有校园网网络结构的前题下设计一台 VPN 认证服务器,该服务器能够使用原有校园网的用户名和密码,并且能够对该用户进行相关的权限控制. 设计方案如图 1 所示,主要功能如下:

使用校园网原有的认证系统进行认证.

(1)能够为合法用户分配正确的校园网 IP 地址.

(2) 能够使用认证用户访问校园网资源时走 OpenVPN 隧道,访问其他资源时走正常的 Internet 网络.

(3)能够记录用户上线,下线时间及在线时长.

(4)能够限制异常用户认证 VPN.

(5)能够防止同一账号多人同时使用.

(6)能够查看用户在线状态.

(7)管理员能够查看服务器负载情.

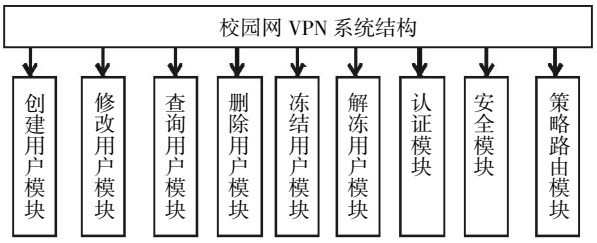

图 1 VPN 系统结构

Fig.1 A VPN system structure

2.2 各模拟说明

(1)创建用户模块

该模块主要为一些没有开设校园网账号的老师或学生创建一个本地账号,用于认证 VPN.

(2)修改用户模块

用于修改本地账号,如账号使用期限,账号密码等.

(3)查询用户模块

可以根据用户名查询该用户在线时间,下线时间,在线时长等信息,能够查询所有校园网用户和本地用户.

(4)删除用户模块

该模块主要用来删除本地用户,不能操作校园网用户,校园网用户的管理由校园网管理中心统一管理.

(5)冻结用户模块

当有些用户行为发生异常,比如大批量的下载文献,此时可以用该模块冻结该账户,冻结后用户不能认证到 VPN 服务器,必须解冻后才可以正常使用. 该模块可以冻结所有校园网用户和本地用户,冻结校园网用户只是冻结该用户认证 VPN 服务器,并不影响校园网的正常使用.

(6)解冻用户模块

用于解冻已经冻结的账户.

(7)认证模块

主要用于合法用户的正常认证,当认证成功后就可以使用 VPN 访问校园网资源了.

(8)安全模块

主要利用 Centos 6.4 自带的高性能防火墙来进行一些安全方面的设置,防止一些网络攻击而导致服务器瘫痪.

(9)策略路由模块

主要向用户推送路由信息,使用校外用户能够选择正常路由访问网络,当访问校内资源时走VPN,当访问其他网络时走正常的 Internet 网络.

2.3 主要算法设计

本节主要讨论认证算法的设计, 算法程序如图 2 所示. 由于校园网用户所占比例远远高于本地用户,所以认证算法先选择校园网认证服务器,如果认证失败再选择本地认证服务器, 这样更有利于缩短认证平均时间,提高认证速度.

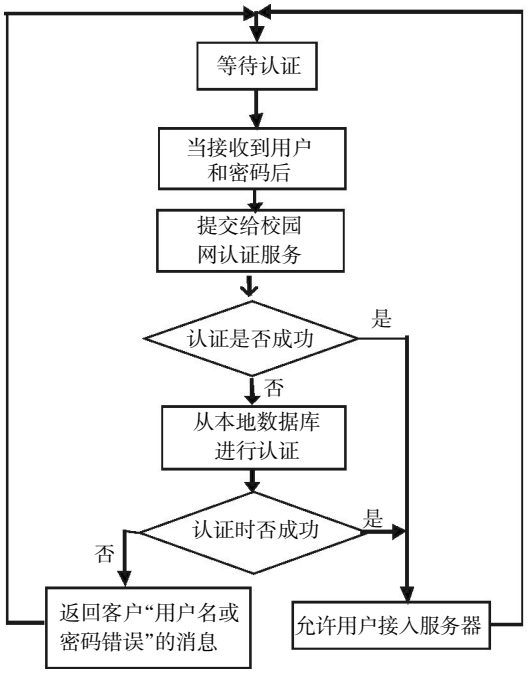

图 2 认证算法流程图

Fig.2 The authentication algorithm flow chart

3　实验结果

经过数月运行,服务器工作稳定,图 3 是在当前用户数 33 的情况下,网络的下行速度和上行速度,下行速度已经达到近 17 MBytes,上行速度达到近 1.7 MBytes,这是因为下载的人数多,上传的人数少. 图 4 显示了当前系统用户情况即当前用户数 33,图 5 显示了下行流量为 17 MBytes 的情况下系统负载情况,前 1 min 平均负载为 0.25,前 5 min 内平均负载为 0.15,前15 min 内平均负载为 0.15,由此可以看出,系统目前负载较轻,当更多用户接入 VPN 服务器时,服务器的服务能力应该不存在问题.

系统采用 Openvpn 技术进行搭建,和现有普遍使用 PPTP 技术而言,OpenVPN 使用 SSL/TLS 安全加密,这使得其安全性要比 PPTP 高很多,另外 OpenVPN 稳定性也要比 PPTP 稳定的多. 但是 PPTP 可以在很多操作系统上运行且不用安装客户端,而 OpenVPN 安装相对比较复杂,如果考虑稳定性和安全性,使用 OpenVPN 技术不失为一个好的选择. 和现有系统比较起来,系统不仅使用了 OpenVPN 技术自身的安全性,还使用了 Linux 自带的防火墙,进一步提高了系统的安全性.

Total rates:	20351.8 kbits/sec	Broadcast Packets:	0
	4546.2 packets/sec	Broadcast bytes:	0
Incoming rates:	17730.1 kbits/sec		
	2604.8 packets/sec		
Outgoing rates:	2621.7 kbits/sec	IP checksum errors:	0
	1941.4 packets/sec		

图 3　网络当前流量

Fig.3　The current traffic network

```
clients: 5 yinbei16427 2015/07/06--07:51:13--10.8.0.108----DOWN
clients: 6 yinbei16427 2015/07/06--07:51:13--10.8.0.108----UP
clients: 7 huenguang17301 2015/07/06--08:07:02--10.8.0.32----UP
clients: 8 jianshang17_327 2015/07/06--08:14:58--10.8.0.106----UP
clients: 9 yutianqiao31213 2015/07/06--08:26:25--10.8.0.107----UP
clients: 10 wanglifeng16424 2015/07/06--08:29:30--10.8.0.111----UP
clients: 11 yuanxufeng16503 2015/07/06--08:38:01--10.8.0.110----UP
clients: 12 wangzihao16424 2015/07/06--08:41:02--10.8.0.112----UP
clients: 13 taishuai17307 2015/07/06--08:42:25--10.8.0.63----UP
clients: 12 wangzihao16424 2015/07/06--08:47:43--10.8.0.112----DOWN
clients: 13 wangzihao16424 2015/07/06--08:47:43--10.8.0.112----UP
clients: 14 lukuo17302 2015/07/06--09:28:13--10.8.0.18----UP
clients: 15 zhaozaihua16501 2015/07/06--09:34:57--10.8.0.113----UP
clients: 14 wangzihao16424 2015/07/06--09:45:47--10.8.0.112----DOWN
clients: 15 wangzihao16424 2015/07/06--09:45:47--10.8.0.112----UP
clients: 16 lixiaosan17308 2015/07/06--10:01:32--10.8.0.27----UP
clients: 15 lukuo17302 2015/07/06--10:02:47--10.8.0.18----DOWN
clients: 16 chengleiyu02322 2015/07/06--10:05:06--10.8.0.13----UP
clients: 17 wangjun21504 2015/07/06--10:28:46--10.8.0.25----UP
clients: 16 wangzihao16424 2015/07/06--10:50:50--10.8.0.112----DOWN
clients: 17 wangzihao16424 2015/07/06--10:51:01--10.8.0.112----UP
```

图 4　用户上下线情况

Fig.4　The information of line up and down customers

```
top - 11:11:41 up  4:26,  2 users,  load average: 0.17, 0.17, 0.09
Tasks: 132 total,   1 running, 131 sleeping,   0 stopped,   0 zombie
Cpu(s):  0.9%us,  0.4%sy,  0.0%ni, 97.2%id,  0.0%wa,  0.4%hi,  1.1%si,  0.0%st
Mem:   3789328k total,   311708k used,  3477620k free,    30148k buffers
Swap:  2096440k total,        0k used,  2096440k free,   170800k cached
```

图 5　系统负载情况

Fig.5　The information of system load

4 结 语

笔者从校园网的实际情况出发,设计了一种可以胜任于校园网环境下的 VPN 服务器,由于使用了开源免费软件 OpenVPN 和防火墙,极大地降低了构建成本,提高了访问速度和安全程度,方便了校外师生无地域限制地访问校内资源. 该服务器不仅适用于校园网环境中,也适用于公司网络环境,并且仅更改服务器的少量配置即可达到目的,具有较好的扩展性.

致 谢

安徽工程大学为本研究提供了资金资助,特此感谢!

参考文献:

[1] 薛涛,赵维加,杨斌,等.Linux 环境下一种改进的技术在集团化公司网络传输中的应用[J].青岛大学学报:自然科学版,2012,25(1):68-72.
XUE Tao, ZHAO Wei-jia, YAN Bin,et al. An improved open VPN technology under linux for company group's network transmission[J]. Journal of Qin Dao University(Sience and Technology),2012,25(1):68-72.(in Chinese)

[2] 白雪峰, 刘洋, 李洋, 等. 基于校园网认证系统的 OpenVPN 的研究与实现 [J]. 沈阳工程学院学报,2011,7(4):354-356
BAI Xue-feng, LIU Yan, LI Yang ,et al. Research and implementation of OpenVPN system based on compus network authentication [J]. Journal of Shenyang Engineering College,2011,7(4):354-356.(in Chinese)

[3] 杨先麟,杨良榆.WH 证券虚拟专用网(VPN)的设计及应用[J].计算机工程,2004,30(2):135-137.
YANG Xian-lin,YANG Liang-yu. Disign and application for WH virtual private network[J]. Journal of Computer Engineering,2004,30(2):135-137.(in Chinese)

[4] 刘艺培.浅淡虚拟专用网(VPN)在校园网下的具体应用[J].无线互联科技,2013(10):28-29.
LIU Yi-pei. Introduction to a virtual private network (VPN) application in campus net[J]. Journal of Wireless Technology,2013(10):28-29.(in Chinese)

[5] 林圣东,陈小惠,赵瑞卿,等.基于 OpenVPN 的 Lan-to-Lan VPN 的设计与实现[J].电子测试,2012,4(4):86-92.
LIN Sheng-dong,CHEN Xiao-hui,ZHAO Rui-qing, et al. Lan-to Lan VPN design and implementation based on OpenVPN[J]. Electronic Test,2012,4(4):86-92.(in Chinese)

Design scheme of virtual private network based on OpenVPN

YI Yun-yun

School of Computer and Information ,Anhui Polytechnic University, Wuhu 241000, China

Abstract: Some teachers and students look up some scientific research data by using campus resources, but because of the limitation of the IP address, they only use the computers in the campus network to access these resources, or else they can't. To solve this problem, a virtual private networks should be set up. A scheme was proposed by using OpenVPN to establish VPN in campus network environment without changing the existing network architecture. The scheme checks the real-time state and on-line and off-line time of users, preventing multiple users landing virtual network at the same time with the same account using the username and password authentication mode, and it guarantees the safety of campus network by configuring the Linux built-in firewall. Finally a low cost and high security virtual private network was realized. After several months of running, it demonstrates that the virtual private network has advantages of good load capacity, fast speed and good stability.

Keywords: Openvpn; VPN; virtual private line; campus network

本文编辑:陈小平