基于 OPENVPN的接入系统设计与实现

程克勤, 于 博, 周 健
(合肥工业大学网络中心, 安徽 合肥 230009)

摘要: 为方便教职工在校园网外能快速访问校园网络资源, 在开源项目 OPENVPN 的基础上设计开发了远程接入系统. 系统采用客户机/服务器模式, 用户通过客户端软件使用用户名和密码进行认证, 与 VPN 接入服务器建立连接后可快速访问校园网络资源.

关键词: OPENVPN; 路由; 认证
中图分类号: TP 393 08 文献标识码: A 文章编号: 0438-0479(2007)S2-0199-03

Internet的发展和教育信息化使得教育工作者越来越离不开校园网, 许多教育工作者经常要在校园网外使用校园网资源. 为使他们能在 Internet上快速方便地使用校园网络资源, 本文在 Linux平台上利用开源软件 OPENVPN 开发了 Virtual Private Network (VPN)接入用户管理系统.

OPENVPN[1]是一个强大、高度可配置的基于 SSL 的 VPN 开源软件, 它具有多种验证方式及强大的功能. OPENVPN 工作在 OSI模型的第 2或第 3层, 使用 SSL/TLS协议进行网络传输. 支持多种客户认证方法, 如证书、加上用户名密码的证书认证等. 此外, 支持动态 IP地址、地址转换和访问控制列表功能.

1 系统设计

1.1 功能要求

校园网 VPN用户接入系统基本功能如下:

(1)能访问校园网内资源;
(2)校园网外对校内 IP开放的资源;
(3)与原有校园网用户数据库关联;
(4)对用户身份进行认证;
(5)保证唯一性, 防止重复认证;
(6)记录日志.

1.2 系统模块

该系统分为两个模块, VPN 接入系统模块和用户管理模块. VPN 模块提供远程接入服务, 用户管理模块则对 VPN用户进行管理维护. VPN 模块涉及系统接入认证服务和路由策略等. 系统用户管理模块主要进行用户的日常管理维护, 以及日志查询等.

1.3 VPN接入结构

VPN接入系统的网络结构如图 1.

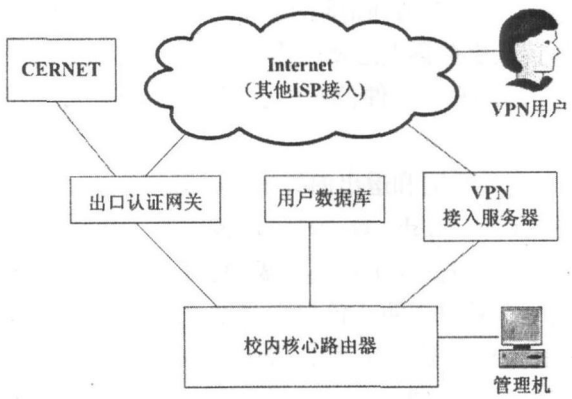

图 1 VPN接入服务网络结构

1.4 路由策略

VPN用户在认证成功后, 分配 IP地址给用户. 在 VPN接入服务器上面设置路由表, 将这些 IP地址的默认路由指向核心路由器, 核心路由器上做相应的返回路由. 核心路由器原有默认路由指向出口认证网关, 出口认证网关上对这些地址不再做认证, 并将这些地址的路由指向教育网出口. VPN分配的 IP地址访问校园内直接通过核心路由器进行路由.

1.5 数据库表

VPN用户系统数据库包括用户基本信息表, VPN 认证表和 VPN 日志表. 其中用户基本信息表是校园网用户信息表, 用于记录用户的基本信息. VPN 认证表用于用户登录时候, 进行身份密码认证. VPN 日志表用于保留 VPN用户登录的日志.

VPN认证表, 有 3个字段, 用户名、用户密码和用

收稿日期: 2007-08-19
作者简介: 程克勤, 男, 助理研究员.

户状态. 用户状态分为 3种, 正常、不允许登录和已登录. 当前正在使用的用户不能重复登录.

1.6 接入控制

用户使用 VPN客户端软件进行连接时输入用户名和密码, VPN服务器对比数据库中 VPN认证表进行身份确认, 如果确认成功则提示连接成功, 并将用户 VPN状态改为已登录, 同时在日志表里记录登录时间. 但用户主动使用客户端软件断开连接的时候, 再在日志表里记录离线时间, 非正常退出(如用户直接关机)则用户帐户在 5分钟后才能使用.

2 系统实现

2.1 系统软件安装和配置

在接入服务器上依据次序安装系统需要的软件[2-3], 有 lzo、lzo-devel、mysql-devebp和 OPENVPN.

在接入服务器 /etc/pam. d/目录下编辑 VPN与数据库连接的文件 openvpn, 其内容为主要是连接数据库服务器的用户名和密码, 以及 VPN用户认证表的数据库; 接入服务器上还要配置 VPN服务器的基本信息名称, 以及证书文件, VPN运行配置文件 openvpn. conf

在用户登陆和退出的时候执行脚本文件 connect sh和 disconnect sh connect sh脚本的主要用途是在客户端连接时修改用户认证表, 将客户端状态置为已登陆, 这样就可以防止该用户多次登陆. 另外, 还要将登陆信息插入到日志表中. disconnect sh脚本的主要用途是在客户端断开连接时修改用户认证表, 将客户端状态标志置为正常, 这样下次客户端就可以再次登陆了, 另外将用户退出登陆的时间添加到日志表中. 如果客户端非正常退出, 则服务器会在 5分钟左右的时间监测到, 然后执行 disconnect sh脚本将客户状态重置.

2.2 路由实现

出口网关和 VPN接入服务器采用 Linux平台, 在 Linux平台下使用 Ip route[4]实现策略路由功能. 下面是 VPN接入服务器部分路由配置, 210. 45. 243. 128/25是分配给 VPN用户的 IP地址, 192. 168. 1. 41是核心交换机与 VPN相连的 IP地址.

#源地址为分配地址的查找规则

ip rule add from 210. 45. 243. 128/25 table VPN_out pref 79

#到校园资源的路由表

ip route add via 192. 168. 1. 41 table VPN_out

#校内地址到分配地址的查找规则

ip rule add from 0/0 to 210. 45. 243. 128/25 table VPN_in pref 78

#到分配给用户的地址的路由表

ip route add dev tun0 table VPN_in

2.3 数据库表

数据库采用 MySQL[5], 在数据库服务器上创建数据库表, VPN接入系统主要使用 VPN认证表和日志表的数据库. 图 2是 VPN认证表和日志表的结构.

	字段	类型	属性	Null	默认
☐	user_id	bigint(16)	UNSIGNED	否	0
☐	user_name	varchar(20)		否	
☐	user_passwd	varchar(20)		否	
☐	user_state	smallint(2)		否	1

	字段	类型	属性	Null	默认
☐	user_name	varchar(20)		否	0
☐	login_date	date		否	0000-00-00
☐	login_time	time		否	00:00:00
☐	logout_date	date		否	1000-00-00
☐	logout_time	time		是	00:00:00
☐	from_ip	varchar(15)		否	000.000.000.000
☐	get_ip	varchar(15)		否	000.000.000.000

图 2 用户认证表和日志表

2.4 管理端

管理模块采用 Java语言开发, 通过 MySQL和 Java接口模块实现. 图 2是 VPN用户管理系统. 通过管理端软件可以对 VPN用户进行管理, 还可以查询用户的登陆时间以及在线用户等.

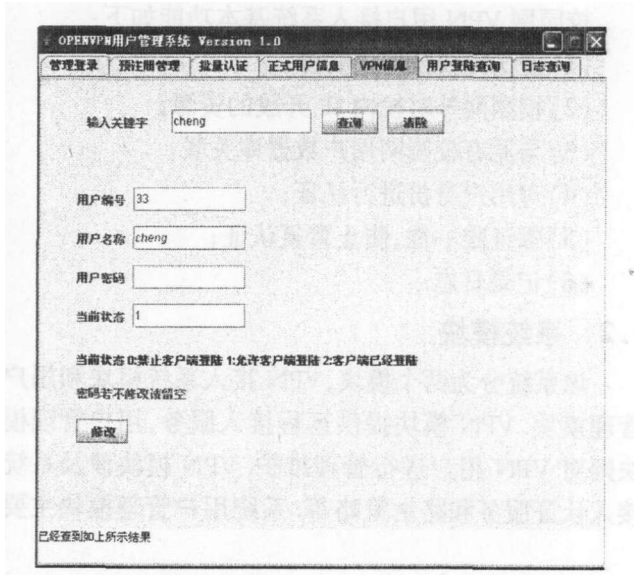

图 3 VPN用户管理

2.5 用户登陆端软件

从 OPENVPN官方网站[1]上下载用户接入客户端软件.然后将 VPN接入服务器上的相应的 ca.crt, ta.key以及客户端的配置文件 openvpn.ovpn放到客户端软件安装的配置目录下[3].

3 结束语

在校园网上使用 Linux平台架设 OPENVPN接入服务器,结合相应的策略路由,能有效地达到在 Internet上方便快速地访问校园网资源,开发的管理软件能有效地进行 VPN用户管理.

参考文献:

[1] OPENVPN [EB/OL]. 2005[2007-08-19]. http://www.openvpn.org

[2] OPENVPN. TM 2.0 HOWTO [EB/OL]. http://openvpn.net/howto.html

[3] OPENVPN.使用 User/Pass验证登录 [EB/OL]. 2007 [2007-08-19]. http://www.chinaunix.net/jh/50/513004.html

[4] Routing for multiple uplinks/providers [EB/OL]. 2006 [2007-08-18]. http://lartc.org/howto/.

[5] Mysql A B. Mysql[CP/OL]. 2005[2007-08-13]. http://dev.mysql.com/.

The Design and Implement of Access System Based on OPENVPN

CHENG Ke-qin, YU Bo, ZHOU Jian

(Network Center of Hefei University of Technology, Hefei 230009, China)

Abstract In order to make the staff access the resources of campus network at the outside of campus's network, we design and develop the remote access system based on OPENVPN which is an open source project. The system uses client/server mode. The user uses username and password as authentication way with client software. The user can quickly access the resources of campus network after make correct connection with VPN access server.

Key words OPENVPN; route; authentication