**老男孩linux运维实战培训**

**老男孩教育教学核心思想6重：重目标、重思路、重方法、重实践、重习惯、重总结**

**学无止境，老男孩教育成就你人生的起点！**

**版权声明：**

本文作者为《老男孩linux运维实战培训》学生—**你的名字**

本文的所有内容均来自老男孩培训**命令总结**，未经本人及老男孩培训许可，禁止私自转发及使用。

QQ: **你的**XXXX

E-mail: **你的**XXXX

**联系方式:**

|  |  |  |  |
| --- | --- | --- | --- |
| 网站运维交流群： | | | |
| **Linux QQ交流群 385168604** | | **架构师 QQ交流群 390642196** | |
| **Python QQ交流群 29215534** | | **大数据 QQ交流群 421358633** | |
| =================================================================================== | | | |
| **老男孩linux实训联系方式** |  | |  |
| **咨询QQ** | **41117397（丹丹）** | | **70271111（歪歪）** |
|  | **80042789（飞雪）** | | **390320151（小雨）** |
|  | **41117483（冰冰）** | |  |
| **电话：** | **158-1059-0206（丹丹）** | | **189-1171-8229（歪歪）** |
|  | **135-5261-2571（飞雪）** | | **186-0046-2391（小雨）** |
| **网站:** | <http://www.etiantian.org> | | <http://www.oldboyedu.com> |
| **博客:** | http://oldboy.blog.51cto.com | | <http://blog.oldboyedu.com> |

**快捷方式说明:**

**ctrl + 1 一级标题**

**ctrl + 2 二级标题**

**ctrl + 3 三级标题**

**ctrl + 5 程序代码**

**ctrl + 6 正文**

**格式约定：**

蓝色字体：内容注释

目 录

[VPN课程总结 1](#_Toc512866000)

[第1章 VPN 概述 1](#_Toc512866001)

[1.1 Vpn类型 1](#_Toc512866002)

[1.2 查看系统是否支持PPP 2](#_Toc512866003)

[1.3 设置内核转发 2](#_Toc512866004)

[1.4 安装PPTP 3](#_Toc512866005)

[1.5 配置PPTP 3](#_Toc512866006)

[1.6 设置用户与密码 3](#_Toc512866007)

[1.7 6. 启动pptp 3](#_Toc512866008)

[1.8 7. 通过windows客户端连接VPN 4](#_Toc512866009)

[第2章 企业案例-记录登录登出的日志信息 4](#_Toc512866010)

VPN课程总结

# VPN 概述

VPN（全称Virtual Private Network）虚拟专用网络

依靠ISP和其他ISP，在公共网络中建立专用的数据通信网络的技术，可以为企业之间或者个人与企业之间提供给安全的数据传输隧道服务

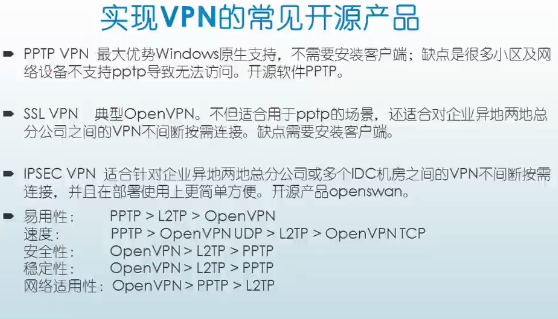
在VPN中任意两点之间的连接并没有传统专网所需的端到端的物理链路，而是利用公共网络资源动态组成的，可以理解为通过私有的隧道技术在公共网络上模拟出来的和专网有同样功能的点到点的专线技术

所谓虚拟是指不需要去拉实际的长途物理线路，而是借用了公共internet网络实现

## Vpn类型

Ssh;VLC;TUN;PPTP;IPsec;OpenVPN

Pptp:第二层数据链路层点对点隧道协议，端口1723

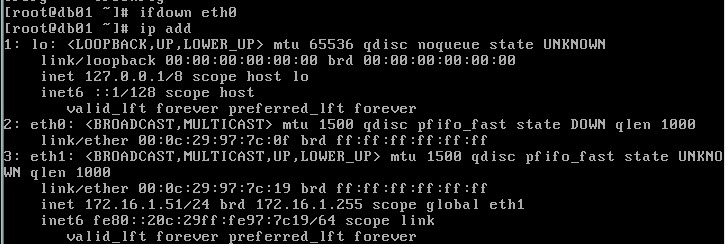


PPTP实战环境

m01 172.16.1.61

db01 172.16.1.51

down了db01的外网IP



## 查看系统是否支持PPP

一般自己的系统支持，VPS需要验证。

[root@oldboyedu ~]# cat /dev/ppp

cat: /dev/ppp: No such device or address

如果出现以上提示则说明ppp是开启的，可以正常架设pptp服务，若出现Permission denied等其他提示，你需要先去VPS面板里看看有没有enable ppp的功能开关，如果没有则需要发个消息给你的提供商，让他们帮你开通，否则就不必要看下去了，100%无法成功配置PPTP。

## 设置内核转发

[root@m01 ~]# grep forw /etc/sysctl.conf

# Controls IP packet forwarding

net.ipv4.ip\_forward = 0

[root@m01 ~]# sed -i 's#net.ipv4.ip\_forward = 0#net.ipv4.ip\_forward = 1#g' /etc/sysctl.conf

[root@m01 ~]# grep forw /etc/sysctl.conf

# Controls IP packet forwarding

net.ipv4.ip\_forward = 1

[root@m01 ~]# sysctl -p

net.ipv4.ip\_forward = 1

net.ipv4.conf.default.rp\_filter = 1

net.ipv4.conf.default.accept\_source\_route = 0

kernel.sysrq = 0

kernel.core\_uses\_pid = 1

net.ipv4.tcp\_syncookies = 1

kernel.msgmnb = 65536

kernel.msgmax = 65536

kernel.shmmax = 68719476736

kernel.shmall = 4294967296

## 安装PPTP

1. # 需要安装epel源

wget -O /etc/yum.repos.d/epel.repo http://mirrors.aliyun.com/repo/epel-6.repo

yum -y install pptpd

## 配置PPTP

[root@m01 ~]# vim /etc/pptpd.conf

localip 10.0.0.61

remoteip 172.16.1.234-238,172.16.1.245

# 添加本机公网IP（localip），分配VPN用户的内网网段（remoteip）。

## 设置用户与密码

[root@m01 ~]# vim /etc/ppp/chap-secrets

####### system-config-network will overwrite this part!!! (begin) ##########

oldboy（用户名） \* 123456（密码） 172.16.1.100（指定连接IP）

####### system-config-network will overwrite this part!!! (end) ############

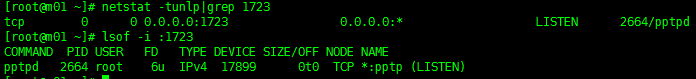
## 6. 启动pptp

[root@oldboyedu ~]# /etc/init.d/pptpd start

Starting pptpd: [ OK ]

[root@oldboyedu ~]# netstat -tunlp|grep 1723

tcp 0 0 0.0.0.0:1723 0.0.0.0:\* LISTEN 26574/pptpd



## 7. 通过windows客户端连接VPN

控制面板\网络和Internet\网络和共享中心

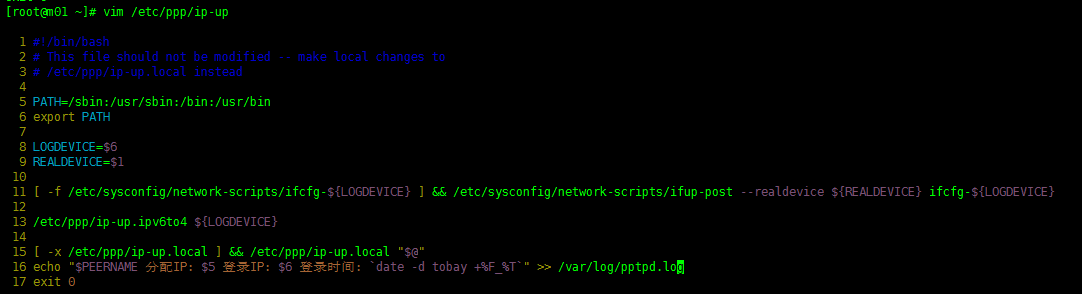


# 企业案例-记录登录登出的日志信息



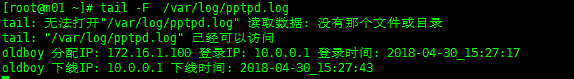
[root@m01 ~]# vim /etc/ppp/ip-up

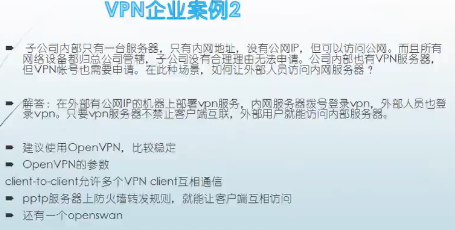
echo "$PEERNAME 分配IP: $5 登录IP: $6 登录时间: `date -d today +%F\_%T`" >> /var/log/pptpd.log



[root@m01 ~]# vim /etc/ppp/ip-down

echo "$PEERNAME 下线IP: $6 下线时间: `date -d today +%F\_%T`" >>/var/log/pptpd.log





企业案例二

子公司内部只有一台服务器，只有内网地址，没有公网IP，但可以访问公网。而且所有网络设备都归总公司管辖，子公司没有合理理由无法申请。公司内部也有vpn服务器，但VPN账号也需要申请，在此场景，如何让外部人员访问内网服务器？

解答：在外部有公网IP的机器上部署VPN服务，内网服务器拨号登录VPN，外部人员也登录vpn，只要VPN服务器不禁止客户端互联，外部用户就能访问内部服务器。

建议使用OpenVPN，较为稳定 其中有一项就是 Client-to-Client 允许多个VPN Client相互通信

PPTP服务器上防火墙转发规则，可以让客户端互相访问