

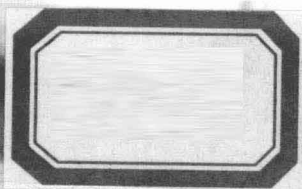
构建虚拟专用通道

OpenVPN服务器详解与架设指南 (基于Linux)



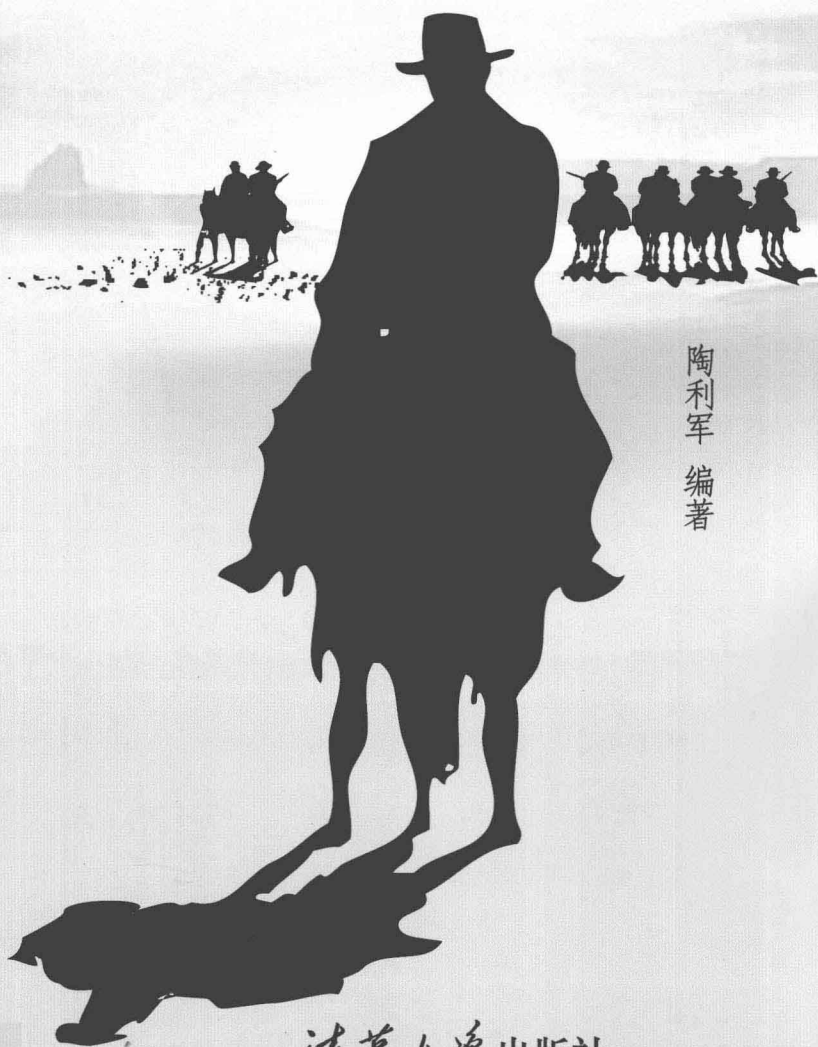
- 使用强大的OpenVPN构建免费VPN通道
- OpenVPN服务器配置选项
- 基于多平台客户端的安装
- 讲述OpenVPN多种认证方式(基于证书、MySQL、OpenLDAP、FreeRADIUS等)
- 阐述企业的实际应用(多用户远程接入、远程局域网互联)
- 基于生产环境实际案例
- 实施OpenVPN细粒度访问控制(包括OpenVPN内建包过滤机制和iptables实现)
- OpenVPN-AS商业OpenVPN的使用

陶利军 编著



构建虚拟专用通道

OpenVPN服务器详解与架设指南
(基于Linux)



陶利军
编著

清华大学出版社
北京

内 容 简 介

OpenVPN 是 VPN 的一个具体实现,它穿透能力强,是所有 VPN 产品中的佼佼者,不但性能优越,而且是开源软件,可以免费使用,也可以二次开发,提供了多种平台的安装版本。此外,它还提供了多种客户端(包括 Window、Linux、Mac 以及各种移动设备的客户端安装包)。

本书将讲述 OpenVPN 的安装使用以及案例实践,全书分为 12 章内容,包含:OpenVPN 基础,OpenVPN 应用,两种用户验证方式,典型应用,运行模式,管理 OpenVPN 服务器,控制 VPN 用户的访问,使用 MySQL 后台,使用 OpenLDAP 后台,商业 OpenVPN 服务器(OpenVPN_AS)等内容。

本书作者长期奋战于网站运维一线,书中内容凝聚了作者多年的经验和技巧。

本书读者群包括:广大的 Linux 爱好者,具有一定 Linux 基础的系统管理员,Linux 下的安全工程师,培训中心师生,运维人员,构建和使用 VPN 的广大用户。

本书封面贴有清华大学出版社防伪标签,无标签者不得销售。
版权所有,侵权必究。侵权举报电话:010-62782989 13701121933

图书在版编目(CIP)数据

构建虚拟专用通道:OpenVPN 服务器详解与架设指南(基于 Linux)/陶利军编著.

—北京:清华大学出版社,2012.8

ISBN 978-7-302-29219-7

I. ①构… II. ①陶… III. ①虚拟网络—研究 IV. ①TP393.01

中国版本图书馆 CIP 数据核字(2012)第 143368 号

责任编辑:栾大成

装帧设计:杨玉兰

责任校对:胡伟民

责任印制:宋 林

出版发行:清华大学出版社

网 址: <http://www.tup.com.cn>, <http://www.wqbook.com>

地 址:北京清华大学学研大厦 A 座 邮 编:100084

社总机:010-62770175 邮 购:010-62786544

投稿与读者服务:010-62776969, c-service@tup.tsinghua.edu.cn

质 量 反 馈:010-62772015, zhiliang@tup.tsinghua.edu.cn

印 刷 者:清华大学印刷厂

装 订 者:北京市密云县京文制本装订厂

经 销:全国新华书店

开 本:188mm×260mm 印 张:33.5 插 页:1 字 数:930 千字

版 次:2012 年 8 月第 1 版 印 次:2012 年 8 月第 1 次印刷

印 数:1~4000

定 价:69.00 元

产品编号:047452-01

前 言

随着互联网的发展和计算机技术的普及，在网络中传输的数据的安全也尤为重要，因此在很多地方都使用了虚拟专用网，也就是我们所说的 VPN。通过使用 VPN，在两个连接在公网的点上构建一条虚拟通道，这样，传输在此通道中的数据将被看做是安全的数据。

在实现 VPN 的技术中，有 Cisco 提供的专用设备，由硬件实现，还有其他通过软件实现的 VPN。在众多的 VPN 产品中，OpenVPN 以其优秀的性能被开源市场认可，尤其是它对网络的强大穿透力。

OpenVPN 就是 VPN 的一个具体实现，它穿透能力强，是所有 VPN 产品中的佼佼者，不但性能优秀，而且是开源软件，可以免费使用，并进行二次开发。OpenVPN 提供了多种平台的安装版本，此外，它还提供了许多种类的客户端，包括 Windows、Linux 和 MAC 下的客户端，以及各种移动设备的客户端安装包。

OpenVPN 适用于以下情况：

- 两个局域网的互联；
- 异地传输（保存）数据（涉及安全的数据）；
- 异地办公（出差在外的员工或者是公司的合作伙伴）。

为网络数据的安全传输保驾护航是我们作为安全工程师的重要责任，但愿本书能够为读者提供帮助。

本书内容

在本书中我们将讲述 OpenVPN 的安装和使用，以及 OpenVPN 的基础知识，全书分为 4 个部分，共 12 章的内容。

第 1 部分 OpenVPN 的基础

本部分包括以下 4 章内容：

- 认识 OpenVPN
- 安装 OpenVPN 服务器
- 分析 OpenVPN 安装包中的部分目录和文件
- 安装 OpenVPN 客户端

第 2 部分 OpenVPN 的应用

本部分包括以下 5 章内容：

- OpenVPN 的两种用户验证方式
- OpenVPN 的两种典型应用
- OpenVPN 有两种运行模式
- 管理 OpenVPN 服务器
- 控制 OpenVPN 用户的访问

第 3 部分 应用案例——使用 FreeRADIUS 验证 OpenVPN 用户登录

本部分包括以下 2 章内容：

- 使用 MySQL 后台
- 使用 OpenLDAP 后台

第 4 部分 商业 OpenVPN 服务器

本部分包括一章内容，讲述 OpenVPN 的另一个分支——商业 OpenVPN 服务器 OpenVPN_AS，被称为 OpenVPN 访问服务器。

内 容 声 明

如果你在任何地方看到了与本书内容雷同的内容，则需要确定一下它的内容是否来自于相应软件的官方网站、man 文档、howto、README、Changelog、INSTALL、LICENSE、*.conf 等这些原创。在我看来，什么是原创？只有这些才是原创（我个人的观点，别拿砖头拍我！），我们只是对它们进行衍生和应用。本书中的内容就是这样，这是我个人的一种学习方法，对于每一种新使用的软件，我都会看它提供的相关文档和其官方网站，配置文件绝对是软件的精华所在，因此在本书中讲述了大量的配置文件，没办法，Linux 下的服务不就是命令加上配置吗？

由于这些官方网站、man 文档、howto、README、Changelog、INSTALL、LICENSE、*.conf 等都是英文的，因此对于我们的认识和阅读是非常不方便的，事实上我们也正是缺乏这些文档的知识，才导致我们一直徘徊在技术的门口。本人就是基于这个基础来编写本书，将这些最基础也是最权威的文档通过理解来实现汉语化，以方便更多的国人阅读，以我个人的感觉，这些东西实际上是我们最需要的，它是认知的第一步，毕竟我们的官方语言是汉语。

书中的内容是我在工作中的一个总结，没有刻意地去改变任何说法，相反，只要是官方文档中有的，我就尽可能地使用它们的说法及方法。

使用对象

- 广大的 Linux 爱好者；
- 具有一定 Linux 基础的系统管理员；
- Linux 下的安全工程师；
- 培训中心；
- 运维人员；
- 构建和使用 OpenVPN 的广大用户。

关于读者

全书分为 12 章，如果你是初学者，那么不要从第 1 章开始，而要从第 2 章开始，因为第 1 章是基础部分，对于初学者来说，看起来很累；如果你急于使用 OpenVPN，那么可以从第 6 章开始，然后是第 3 部分；如果你是一个有经验的 OpenVPN 管理者，那么有必要看看第 1 章，在这些内容中找到新的使用，以便组合出新的功能。

本书的最后一章是针对 OpenVPN 的商业版所写，对于开源用户不妨也参考一下，毕竟这两个版本是一母同根，而且它还提供了两个客户端的免费使用，这对于不提供 OpenVPN 用户访问，而是作为管理员自己使用方法（比如你在家就可以访问公司的内网，或者管理公司的服务器）已经足够了。

作者声明

本书的内容是我在工作中的一个总结，在生产环境中都使用过，并非纸上谈兵，但是书中的例子，我尽可能地不使用生产环境中的例子，一是怕对你造成误导，二是不想说什么权威。

我在前面说了本书内容的来源，而对于其内容的构成，其一是培训员工的资料；其二是培训中心的一些文案；其三是我在学习中的笔记。本书由这三部分融合而成，而不是简单地拼凑。

另外，毕竟我们都是做互联网的，每天面对着无数个页面，我所要说的是，如果读者在阅读本书的过程中发现有和网络上相似的内容，那么确定一下是否是两者（即笔者和您看到的文章的作者）参考了同一个官方的资料，本人绝对没有有意抄袭其他作者的内容；第二，如果我写的内容确实和您的内容有相同之处，那么及时和我联系（绝对是缘分！）；第三，互联网给了我们发展，也给了我们交流，如果您在阅读本书的过程中发现有个别说法、方法和您的相同，那么请您海涵，往往是一个提法、方法用久了就觉得是自己的方法了（我相信谁都会犯这种错误！）；第四，由于本人是做运维（系统管理和网络管理）的，因此在写作风格上是按照自己的认知过程所写，既没有受过专业的训练也没有模仿某个作者或者某个作

品的写作风格，如果和您的写作风格相同，那么绝对是巧合（这个就不要计较了！）；第五，本书引用了互联网的一些内容，由于同一个内容被转载来转载去，确实很难找到原出处，因此在应用的内容处只指明了来源于互联网。

由于本人才疏学浅，因此本书难免会有疏漏和不足，希望广大读者有什么建议和意见可以给本人发邮件：linux_safe_openvpn@126.com。

关于 OpenVPN

OpenVPN 是实现 VPN 的一个开源软件，在了解 OpenVPN 之前首先要理解 VPN。VPN 的全名是“Virtual Private Network”，翻译为中文就是“虚拟专用网”，因此又引出一个“专用网”的概念，也就是说 OpenVPN “概念”的形成是这样的：

专用网→虚拟专用网（VPN）→OpenVPN

专用网就是在两个点（例如，北京和广州）之间架设一条专用线路，但是它并不需要真正地去铺设光缆之类的物理线路。虽然没有亲自去铺设，但是需要申请专线，在这条专用的线路上只能传输自己的东西。这种专用网的费用可想而知。

虚拟专用网就是在这两个点之间通过公网实现的一种“专用网”，因此称为“虚拟专用网”，不需再铺设专用线路，也不需再申请专线，而是只要这两个点之间属于公网的一个节点就可以了，对于服务器端需要有一个公网地址，而客户端则能够接入互联网就可以了。

OpenVPN 就是 VPN 的一个具体实现，它穿透能力强、无须修改协议栈（例如，基于 IPSec 实现的 VPN 需要修改）、无须编写专门的策略来解决 VPN 数据穿越 NAT 的问题，便可以在现有的网络上进行构建，所以它是 VPN 产品中的佼佼者，不但性能优秀，而且是开源软件，不但可以免费使用，还可以二次开发。

举一个简单的例子，对于一个在外跑业务的员工，需要时刻访问公司的资源。如果一个员工在甲方的网络中访问自己公司的资源，那么甲方只要在业务员连接的交换机上采取点小措施，那么所有的信息将会被甲方获取，如果该员工在正常连接网络后使用了 VPN，那么被获取的数据也是被加密的数据，也就是说甲方获取的数据等于是无效的垃圾数据。

因此，无论是在何种情况下，使用 VPN 非常重要。

OpenVPN 在本质上是将虚拟网卡设备、TCP/IP 网络技术、路由技术以及 SSL 加密技术结合而成的一个具体实现，虚拟网卡实现连接设备，TCP/IP 实现连接协议，路由技术实现网络间的穿透，而 SSL 加密技术实现虚拟通道的安全，即认证和加密。所以在学习、使用和处理 OpenVPN 的问题时要从这四个方面去分析。

目 录

第 1 部分 OpenVPN 的基础

第 1 章 认识 OpenVPN	2	第 2 章 安装 OpenVPN 服务器	101
1.1 OpenVPN 的选项	2	2.1 相关软件的安装	101
1.1.1 通道选项	3	2.1.1 安装 TUN/TAP 驱动	101
1.1.2 服务器模式选项	29	2.1.2 安装 OpenSSL 库	102
1.1.3 客户端模式选项	42	2.1.3 安装 lzo	103
1.1.4 数据通道加密选项	44	2.2 安装 OpenVPN 服务器	105
1.1.5 TLS 模式选项	47	2.2.1 下载 OpenVPN 服务器	106
1.1.6 TUN/TAP 持久通道配置 模式	69	2.2.2 解压缩并安装 OpenVPN 服务器	106
1.1.7 PKCS#11 独立选项	70	2.2.3 安装 OpenVPN 后的 目录结构	110
1.2 脚本和环境变量	70	2.2.4 创建证书	110
1.2.1 脚本的执行顺序	70	2.3 启动 OpenVPN 服务器	115
1.2.2 字符串类型和重新映射	71	2.3.1 命令行方式启动	115
1.2.3 环境变量	71	2.3.2 后台服务方式启动	115
1.3 可用信号	76	第 3 章 分析 OpenVPN 安装包中的 部分目录和文件	123
1.4 TUN/TAP 驱动设置	80	3.1 sample-keys 目录	123
1.5 举例	80	3.2 sample-config-files 目录	127
1.5.1 TUN/TAP 设置	80	3.2.1 OpenVPN 运行在 C/S 多客户端 下的示例配置文件	127
1.5.2 Firewall 设置	81	3.2.2 OpenVPN 运行在 SSL/TLS 模式下的示例配置文件	136
1.5.3 VPN 地址设置	81	3.2.3 OpenVPN 运行在预共享的 静态密钥方式下的示例 配置文件	145
1.5.4 例 1: 没有安全保护的简单 VPN 通道	81	3.2.4 OpenVPN 用于测试的 TLS 示例配置文件	151
1.5.5 例 2: 使用静态安全密钥的 VPN 通道	85		
1.5.6 例 3: 基于 TLS 的 安全通道	90		
1.5.7 路由设置	98		
1.6 防火墙设置	99		

3.2.5 相关的脚本文件	156	4.1.2 运行 OpenVPN 客户端	173
3.3 sample-scripts 目录	161	4.2 Linux 系统下安装 OpenVPN	
3.3.1 auth-pam.pl 文件	162	客户端	176
3.3.2 ucn.pl 文件	165	4.2.1 安装 OpenVPN 客户端	176
3.3.3 verify-cn 文件	165	4.2.2 运行 OpenVPN 客户端	176
3.3.4 bridge-start、bridge-stop 和		4.3 Mac 系统下安装 OpenVPN	
openvpn.init 文件	167	客户端	182
3.4 easy-rsa 目录	167	4.3.1 安装 OpenVPN 客户端	182
3.5 plugin 目录	168	4.3.2 运行 OpenVPN 客户端	183
3.5.1 auth-pam 插件	169	4.4 对其他客户端的支持	183
3.5.2 down-root 插件	169	4.4.1 IOS 系统下安装 OpenVPN	
3.5.3 defer 插件	169	客户端	184
第 4 章 OpenVPN 客户端的安装	171	4.4.2 Android 系统下安装 OpenVPN	
4.1 Windows 系统下安装 OpenVPN		客户端	184
客户端	171	4.4.3 Windows Mobile 系统下安装	
4.1.1 安装 OpenVPN 客户端	172	OpenVPN 客户端	185
 第 2 部分 OpenVPN 的应用			
第 5 章 OpenVPN 的两种用户登录		5.4.4 安装 pam_mysql 模块	197
验证方式	189	5.4.5 创建 mysql 表	199
5.1 证书验证方式	189	5.4.6 配置 pam_mysql 模块	201
5.1.1 证书的使用	189	5.4.7 访问测试	207
5.1.2 吊销证书	189	5.5 使用 OpenLDAP 验证 OpenVPN	
5.2 用户名/密码验证方式	192	用户登录访问	214
5.3 脚本验证方式	192	5.5.1 下载 openvpn-auth-ldap	
5.3.1 下载并编辑脚本	192	插件	215
5.3.2 编辑一个密码文件	194	5.5.2 安装必要的依赖软件	215
5.3.3 访问测试	194	5.5.3 安装 OpenLDAP	220
5.4 使用 MySQL 验证 OpenVPN 用户		5.5.4 安装 auth-ldap	221
登录访问	195	5.5.5 认识 auth-ldap	221
5.4.1 下载 pam_mysql 模块	195	5.5.6 实例运行	223
5.4.2 解压缩 pam_mysql 模块	196	第 6 章 OpenVPN 的两种典型应用	231
5.4.3 认识 configure 选项	196	6.1 多个远程单用户访问内网	231

6.2 连接两个局域网	232	7.5.6 查看客户端的网络情况	284
6.2.1 安装 OpenVPN 服务器端和 客户端	236	第 8 章 管理 OpenVPN 服务器	285
6.2.2 内网机器的设置	238	8.1 管理命令	285
第 7 章 OpenVPN 的两种运行模式	241	8.2 管理消息输出格式	315
7.1 网桥	241	8.3 实时消息格式	315
7.1.1 什么是网桥	241	8.4 CLIENT 通知格式	316
7.1.2 网桥的实现方式	242	8.5 命令解析	317
7.2 Linux 下实现网桥	242	8.6 管理工具的使用	317
7.2.1 安装 bridge-utils	244	8.6.1 命令行工具——telnet	317
7.2.2 安装后的目录结构	245	8.6.2 OpenVPN MI GUI 工具	318
7.3 brctl 命令	245	8.6.3 OpenVPN-Admin 工具	322
7.3.1 设置网桥的实例	246	8.7 实现 OpenVPN 服务器的高可用	323
7.3.2 设置网桥的端口	249	8.7.1 客户端实现	324
7.3.3 MAC 地址管理	251	8.7.2 服务器端实现	326
7.3.4 设置生成树协议	253	8.7.3 实例	327
7.4 桥接模式 OpenVPN	254	8.8 客户端 IP 地址的使用	329
7.4.1 网桥管理	255	8.8.1 net30 模式	330
7.4.2 修改配置文件	258	8.8.2 subnet 模式	333
7.4.3 启动网桥式 OpenVPN 服务器	259	8.8.3 p2p 模式	336
7.4.4 查看服务器端的网络情况	266	第 9 章 控制 OpenVPN 用户的访问	341
7.4.5 客户端连接 OpenVPN 服务器	267	9.1 包过滤文件格式	341
7.4.6 查看客户端的网络情况	270	9.1.1 限制对象	341
7.5 路由模式 OpenVPN	270	9.1.2 过滤文件语法	341
7.5.1 修改配置文件	271	9.2 配置 OpenVPN 服务器	342
7.5.2 启动路由模式 OpenVPN 服务器	272	9.2.1 编译 minimal_pf.so 模块	343
7.5.3 查看服务器端的网络情况	279	9.2.2 编写脚本	345
7.5.4 开启路由转发	280	9.2.3 策略文件	346
7.5.5 客户端连接 OpenVPN 服务器	280	9.3 启动 OpenVPN 服务器	346
		9.4 实例测试	348
		9.4.1 针对用户的限制	348
		9.4.2 针对 IP 的限制	358
		9.5 通过 iptables 防火墙规则限制 OpenVPN 用户访问资源	370

9.5.1 OpenVPN 的配置文件370

9.5.2 针对 OpenVPN 用户的
防火墙策略371

9.5.3 针对 OpenVPN 用户组的
防火墙策略 374

第3部分 应用案例—使用FreeRADIUS验证OpenVPN 用户登录

第10章 方案一：MySQL 后台379

10.1 安装 FreeRADIUS379

10.1.1 下载 FreeRADIUS380

10.1.2 出错处理381

10.1.3 安装 FreeRADIUS 后的
目录结构383

10.2 安装 RadiusPlugin384

10.2.1 下载 RadiusPlugin385

10.2.2 解决依赖问题385

10.2.3 安装 RadiusPlugin385

10.3 相关配置386

10.3.1 配置 FreeRADIUS386

10.3.2 添加数据库390

10.3.3 配置 RadiusPlugin396

10.3.4 配置 OpenVPN398

10.4 启动服务398

10.4.1 启动 FreeRADIUS 服务器398

10.4.2 启动 OpenVPN 服务器408

10.5 OpenVPN 用户登录验证409

10.5.1 添加 OpenVPN
客户端用户409

10.5.2 测试 OpenVPN 用户410

10.5.3 OpenVPN 客户端登录411

10.6 了解 OpenVPN 的使用情况414

10.7 使用 daloRADIUS Web 程序415

10.7.1 下载安装416

10.7.2 解决依赖前提 417

10.7.3 导入数据库 420

10.7.4 设置数据库连接 422

10.7.5 使用 daloRADIUS 423

10.8 禁止用户登录 428

10.8.1 通过操作 MySQL 数据库
禁止用户登录 428

10.8.2 通过 daloRADIUS Web
应用程序禁止用户登录 429

第11章 方案二：OpenLDAP 后台431

11.1 下载安装 FreeRADIUS
-Server-2.1.12 431

11.1.1 编译安装 432

11.1.2 安装后的目录结构 432

11.2 相关配置 433

11.2.1 配置 FreeRADIUS-Server 433

11.2.2 配置 OpenLDAP 438

11.2.3 配置 RadiusPlugin 439

11.3 启动服务 439

11.3.1 启动 FreeRADIUS 服务器 439

11.3.2 启动 OpenVPN 服务器 440

11.3.3 启动 OpenLDAP 服务器 440

11.4 OpenVPN 用户登录验证 440

11.4.1 添加 OpenVPN 客户端
用户 440

11.4.2 登录测试 450

11.4.3	OpenVPN 客户端登录	452	11.5.1	通过 LAM Web 应用程序 ..	457
11.5	禁止用户登录	457	11.5.2	使用 ldapdelete	458

第 4 部分 商业 OpenVPN 服务器

第 12 章	OpenVPN_AS 服务器	461	12.3	配置 OpenVPN_AS 服务器	479
12.1	认识 OpenVPN Access Server	462	12.3.1	服务器状态 (Status)	480
12.1.1	OpenVPN Access Server 系统 的构成	462	12.3.2	AS 服务器配置 (Configuration)	482
12.1.2	OpenVPN Access Server 开启 的端口和服务	463	12.3.3	用户管理 (User Management)	495
12.1.3	OpenVPN Access Server 在 网络中的部署图	463	12.3.4	设置用户的认证方式 (Authentication)	498
12.1.4	OpenVPN Access Server 的 用户认证和管理	464	12.3.5	工具 (Tools)	502
12.1.5	Virtual VPN 子网配置	465	12.4	防火墙设置	503
12.1.6	Admin Web UI 的主菜单	466	12.4.1	运行中的规则	503
12.2	安装 OpenVPN_AS 服务器	466	12.4.2	将运行的规则保存为文件 ..	506
12.2.1	下载并安装 OpenVPN_AS 服务器	467	12.5	使用 OpenVPN_AS 服务器	508
12.2.2	安装 OpenVPN_AS 后的目录 结构	472	12.5.1	启动 OpenVPN_AS 服务器 ..	509
			12.5.2	客户端的安装及访问	519
			12.5.3	使用 LDAP 方式验证 OpenVPN 用户	523

第 1 部分

OpenVPN 的基础

本部分内容包括以下 4 章内容:

- 认识 OpenVPN
- 安装 OpenVPN 服务器
- 分析 OpenVPN 安装包中的部分目录和文件
- OpenVPN 客户端的安装

第 1 章 认识 OpenVPN

OpenVPN 是一个健全且高效的 VPN 守护进程，它支持 SSL/TLS 安全、以太网桥，支持 TCP 或者 UDP 代理或者是 NAT 通道传输，支持动态 IP 地址和 DHCP，可支持成百上千的用户，并且可以移植到大多数主要平台的操作系统上。

OpenVPN 需要使用 OpenSSL 库，这是因为它使用了 OpenSSL 的加密功能。

OpenVPN 支持常规的加密，即使用预共享密钥（即静态 Key 模式）或者客户端和服务器的证书公钥安全（即 SSL/TLS 模式）。它还支持非加密的 TCP/UDP 通道。

OpenVPN 被设计为使用 TUN/TAP 虚拟网络接口连接网络，这种接口可以在大多数平台上使用。

总体而言，OpenVPN 的目的是提供 IPsec 的主要功能，是一个相对轻量级的服务器。

1.1 OpenVPN 的选项

OpenVPN 允许任何选项放置在命令行或者是配置文件中（在配置文件中我们称选项为指令），但是放置在命令行中的选项要在选项前面添加“--”（英文格式的两个破折号）。

选项名称：--help

功能：显示帮助信息。

选项名称：--config file

功能：该选项用于载入指定的配置文件。需要注意的是配置文件中的选项没有“--”，另外，如果--config file 是 OpenVPN 命令的唯一一个命令行选项，那么可以移除 --config 选项，也就是说在 OpenVPN 命令之后直接跟随配置文件的名称。注意配置文件可以嵌套到一个合理的深度。

对于参数，如果包含空格的参数，可以包含在双引号或者是单引号中（"","'），出现在首行的“#”或者“;”字符表示注释行。

注意，OpenVPN 2.0 及以上的版本，对于不在单引号中的反斜线将会执行基于 shell 的反斜线转义符。例如：

\\ 被映射为单个反斜线 (\)；

\\" 被解释为一个双引号字符；

\[SPACE] 被解释为一个空格字符或者是 tab 字符；

对于 Windows 系统，使用双斜线来表示路径名：

```
secret "c:\\OpenVPN\\secret.key"
```

下面是一个简单的配置文件：

```
# Sample OpenVPN configuration file for
# using a pre-shared static key.
```

```
#  
# '#' or ';' may be used to delimit comments.  
  
# Use a dynamic tun device.  
dev tun  
  
# Our remote peer  
remote mypeer.mydomain  
# 10.1.0.1 is our local VPN endpoint  
# 10.1.0.2 is our remote VPN endpoint  
ifconfig 10.1.0.1 10.1.0.2  
  
# Our pre-shared static key  
secret static.key
```

1.1.1 通道选项

下面是相关的通道选项（Tunnel Options）。

选项名称：--mode m

功能：设置 OpenVPN 的模式。默认情况下，OpenVPN 运行在点对点模式（p2p）。在 OpenVPN 2.0 中引入了一种新的模式—server，这种模式能够使得 OpenVPN 运行在多客户端服务器模式。可选值有 P2P 和 Server 两个值。

在点对点的模式中，只有两台主机：一台是 OpenVPN 服务器，而另一台则是 OpenVPN 客户端；在 Server 模式下，有一台 OpenVPN 服务器和多个客户端。

选项名称：--local host

功能：设置用于绑定 OpenVPN 服务器的本地机器的名字或者是 IP 地址。如果指定了具体的 IP 地址或者是机器名字，那么 OpenVPN 服务器仅绑定到这个地址上，否则 OpenVPN 服务器将会在所有网卡上监听。

选项名称：--remote host [port] [proto]

功能：该选项用于指定远程主机名称或者是 IP 地址（这里所说的远程，就是指远程的 OpenVPN 服务器）。在客户端可以指定多个 --remote 选项，以便指定多个 OpenVPN 服务器，每一个选项都要指定一个不同的 OpenVPN 服务器，从而实现冗余。OpenVPN 客户端将会以 host:port 的格式按照 “--remote options” 列表的顺序来尝试连接服务器。在这个选项中，proto 表示在连接时使用的协议，可以指定的值有 TCP 或者是 UDP。当客户端在连接一个远程 OpenVPN 服务器失败时，那么客户端将会移动到列表中的下一台指定的 OpenVPN 服务器。但是需要注意的是，在任何一个时刻，OpenVPN 客户端最多能够连接到一台 OpenVPN 服务器。

需要注意的是,由于 UDP 是无连接的,因此连接失败是通过--ping 和 --ping-restart 选项来定义。

注意下面的特殊案例:

如果使用了多个 --remote 选项,并且通过--user 和 (或) --group 设置了客户端降级运行的用户和 (或) 组,而且客户端运行在非 Windows 系统上。当客户端切换到不同的 OpenVPN 服务器,服务器需要推送不同的 TUN/TAP 或者路由设置,但是由于客户端使用了降级运行,因此会导致客户端无法重新设定设备及路由信息,这将会导致致命错误的发生,并且最终导致客户端退出。

如果没有指定 --remote 选项,那么 OpenVPN 将会监听在所有的 IP 地址,但是不响应这些数据包,除非这些数据包通过所有的认证测试。

如果使用了 TCP 模式,那么 --remote 选项首先将会担当一个过滤器,对于任何不匹配主机的都会被拒绝。

如果在该选项之后指定的是一个 DNS 名字,并且这个域名被解析到多个 IP 地址,那么被解析到的 IP 地址将会是随机的,这样便有了一个基本的负载均衡,并且提供了失败保护,或者说是简单的高可用。

选项名称: --remote-random-hostname

功能: 为 DNS 主机名添加一个随机字符串 (6 个字符), 以便阻止 DNS 缓存。例如, “foo.bar.gov” 被修改为 “<random-chars>.foo.bar.gov”, 添加这个随机的字符串 (6 个字符) 是为了阻止 DNS 缓存。

选项名称: <connection>

功能: 定义客户端连接的配置文件。客户端连接的配置文件是一组 OpenVPN 选项, 通过这些选项描述了客户端如何连接一个给定的 OpenVPN 服务器, 这些配置被定义在 OpenVPN 的配置文件中, 每一部分的配置都被放置在 <connection> 和 </connection> 之间。

OpenVPN 客户端将会尝试每一个定义连接的部分, 直到实现了一个成功的连接。

--remote-random 选项可以“爬行”这个连接列表。

例如:

```
client
dev tun

<connection>
remote 198.19.34.56 1194 udp
</connection>

<connection>
remote 198.19.34.56 443 tcp
</connection>
```