在云端
云计算最佳实践

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

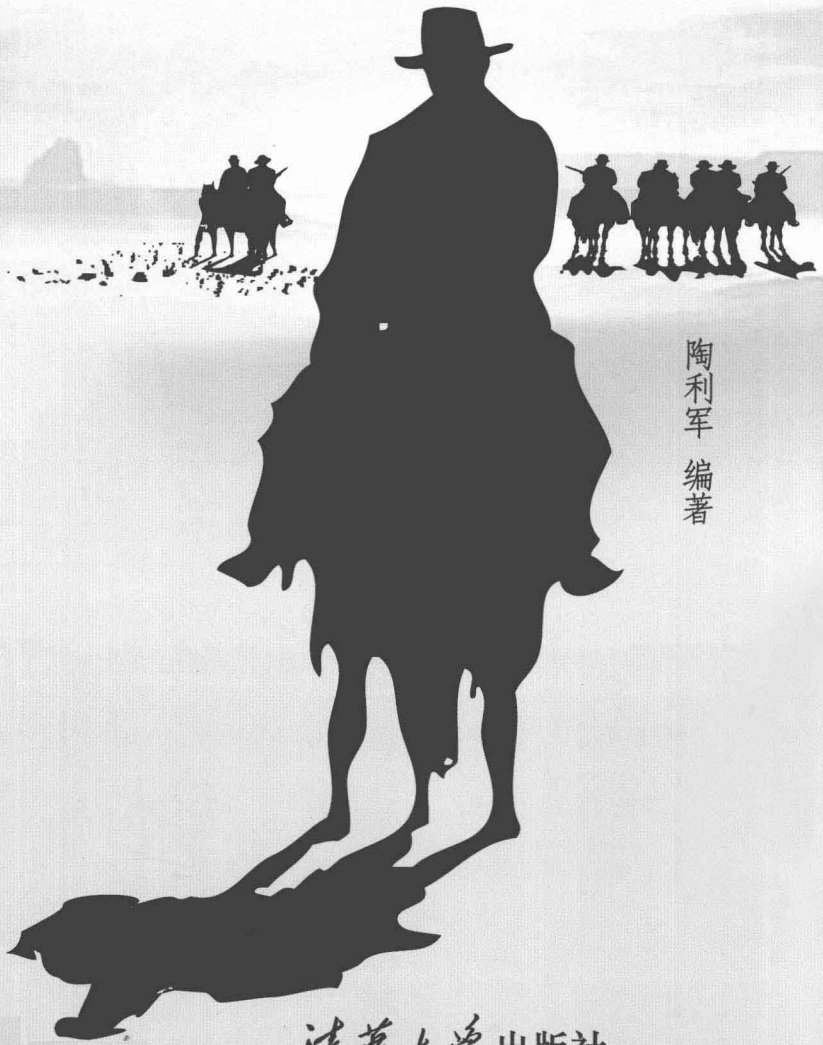
陶利军 编著

清華大學出版社

在云端

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

清華大學出版社
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。

此为试读，需要完整PDF请访问：www.ertongbook.com

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（比如你在家里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，二是不想说什么是权威。

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 2 部分 OpenVPN 的应用

此为试读，需要完整PDF请访问：www.ertongbook.com

第3部分 应用案例—使用FreeRADIUS验证OpenVPN用户登录

第 4 部分 商业 OpenVPN 服务器

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端的证书公钥安全（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>
```


此为试读，需要完整PDF请访问：www.ertongbook.com