



# centos7部署OpenVpn

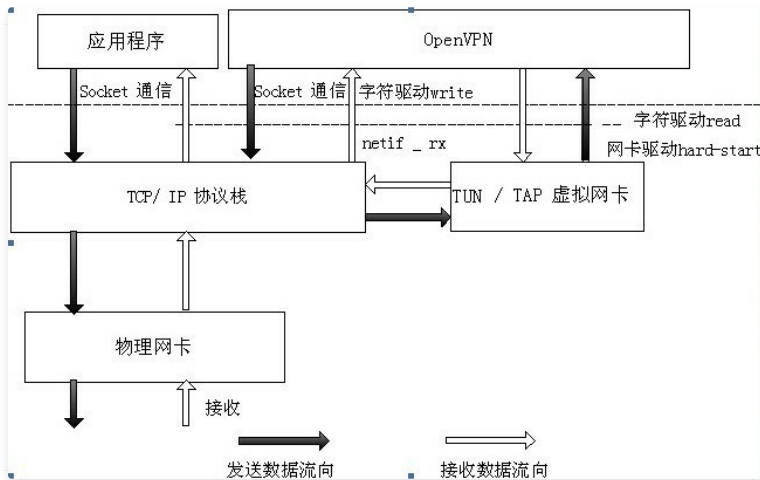
2021-08-17 阅读 292

## 一、简介

VPN直译就是虚拟专用通道，是提供给企业之间或者个人与公司之间安全数据传输的隧道，OpenVPN无疑是Linux下开源VPN的先锋，提供了良好的性能和友好的用户GUI。

OpenVPN大量使用了OpenSSL加密库中的SSLv3/TLSv1协议函数库。

OpenVPN 是一个基于 OpenSSL 库的应用层 VPN 实现。和传统 VPN 相比，它的优点是简单易用。



## 二、环境规划

openvpn 服务端 centos7

IP 192.168.31.168

双网卡

## 三、安装部署

### 1.配置yum源（安装epel）

参考地址：<https://fedoraproject.org/wiki/EPEL>

```
yum install https://dl.fedoraproject.org/pub/epel/epel-release-latest-7.noarch.rpm
yum update
yum repolist
```

### 2.生成证书

#### 2.1.下载证书生成工具 easy-rsa

## 目录

### 一、简介

### 二、环境规划

### 三、安装部署

- 1.配置yum源（安装epel）
- 2.生成证书

### 四、OpenVPN服务端配置

- 1.安装openvpn软件
- 2.修改配置文件
- 3.拷贝证书到openvpn主配置文件目录下
- 4.启动openvpn

### 五、OpenVPN客户端部署

- 1.安装OpenVPN客户端软件
- 2.配置客户端
- 3.编写客户端配置文件
- 4.启动OpenVPN客户端软件

## 精选专题



腾讯云原生专题  
云原生技术干货，业务实践落地。

## 活动推荐

云加社区写手招募令

立即查看

最壕十一月，敢写就有奖

腾讯云自媒体分享计划

入驻云加社区，共享百万资源包。

立即入驻

运营活动



```
yum -y install easy-rsa
```

## 2.2.创建证书环境目录

```
mkdir -p /opt/easy-rsa
cp -a /usr/share/easy-rsa/3.0.8/* /opt/easy-rsa/
cp -a /usr/share/doc/easy-rsa-3.0.8/vars.example /opt/easy-rsa/vars
```

## 2.3.生成秘钥前，准备 vars 文件

修改文件 `/opt/easy-rsa/vars` 中的如下配置（要取消注释）

```
set_var EASYRSA_DN "cn_only"
set_var EASYRSA_REQ_COUNTRY "CN"
set_var EASYRSA_REQ_PROVINCE "Shanghai"
set_var EASYRSA_REQ_CITY "Shanghai"
set_var EASYRSA_REQ_ORG "lucifer"
set_var EASYRSA_REQ_EMAIL "pc1107750981@163.com"
set_var EASYRSA_NS_SUPPORT "yes"
```

## 2.4.初始化

在当前目录下创建 `pki` 目录，用于存储证书

```
[root@openvpn easy-rsa]# cd /opt/easy-rsa/
[root@openvpn easy-rsa]# /opt/easy-rsa/easyrsa init-pki

Note: using Easy-RSA configuration from: /opt/easy-rsa/vars

init-pki complete; you may now create a CA or requests.
Your newly created PKI dir is: /opt/easy-rsa/pki
```

## 2.5.创建根证书

根证书用于ca对之后生成的server和client证书签名时使用。（输入两次密码，直接回车）

```
[root@openvpn easy-rsa]# /opt/easy-rsa/easyrsa build-ca

Note: using Easy-RSA configuration from: /opt/easy-rsa/vars
Using SSL: openssl OpenSSL 1.0.2k-fips 26 Jan 2017

Enter New CA Key Passphrase:
Re-Enter New CA Key Passphrase:
Generating RSA private key, 2048 bit long modulus
.....+++
.....+++++
e is 65537 (0x10001)
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Common Name (eg: your user, host, or server name) [Easy-RSA CA]:

CA creation complete and you may now import and sign cert requests.
Your new CA certificate file for publishing is at:
/opt/easy-rsa/pki/ca.crt
```

## 2.6.创建server端证书和私钥文件

nopass表示不加密私钥文件，生成过程中直接回车默认

```
[root@openvpn easy-rsa]# /opt/easy-rsa/easyrsa gen-req server nopass

Note: using Easy-RSA configuration from: /opt/easy-rsa/vars
Using SSL: openssl OpenSSL 1.0.2k-fips 26 Jan 2017
Generating a 2048 bit RSA private key
.....+++
.....+++
writing new private key to '/opt/easy-rsa/pki/easy-rsa-1326.TifM4D/tmp.rXSnIM'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Common Name (eg: your user, host, or server name) [server]:

Keypair and certificate request completed. Your files are:
req: /opt/easy-rsa/pki/reqs/server.req
key: /opt/easy-rsa/pki/private/server.key
```

## 2.7. 给server证书签名（输入yes，输入密码）

```
[root@openvpn easy-rsa]# /opt/easy-rsa/easyrsa sign server server

Note: using Easy-RSA configuration from: /opt/easy-rsa/vars
Using SSL: openssl OpenSSL 1.0.2k-fips 26 Jan 2017

You are about to sign the following certificate.
Please check over the details shown below for accuracy. Note that this request
has not been cryptographically verified. Please be sure it came from a trusted
source or that you have verified the request checksum with the sender.

Request subject, to be signed as a server certificate for 825 days:

subject=
  commonName = server

Type the word 'yes' to continue, or any other input to abort.
Confirm request details: yes
Using configuration from /opt/easy-rsa/pki/easy-rsa-1397.ds5qpo/tmp.lX0IFN
Enter pass phrase for /opt/easy-rsa/pki/private/ca.key:
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
commonName :ASN.1 12:'server'
Certificate is to be certified until Jun 3 14:02:46 2023 GMT (825 days)

Write out database with 1 new entries
Data Base Updated

Certificate created at: /opt/easy-rsa/pki/issued/server.crt
```

## 2.8. 创建Diffie-Hellman文件，秘钥交换时的Diffie-Hellman算法

```
/opt/easy-rsa/easyrsa gen-dh
```

## 2.9. 创建client端证书和私钥文件

nopass表示不加密私钥文件，生成过程中直接回车默认

```
[root@openvpn easy-rsa]# /opt/easy-rsa/easyrsa gen-req client nopass

Note: using Easy-RSA configuration from: /opt/easy-rsa/vars
Using SSL: openssl OpenSSL 1.0.2k-fips 26 Jan 2017
Generating a 2048 bit RSA private key
.....+++
.....
writing new private key to '/opt/easy-rsa/pki/easy-rsa-1761.HYs4Xv/tmp.z0ZJuI'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Common Name (eg: your user, host, or server name) [client]:

Keypair and certificate request completed. Your files are:
req: /opt/easy-rsa/pki/reqs/client.req
key: /opt/easy-rsa/pki/private/client.key
```

#### 2.10. 给client端证书签名（输入yes，输入密码）

```
[root@openvpn easy-rsa]# /opt/easy-rsa/easyrsa sign client client

Note: using Easy-RSA configuration from: /opt/easy-rsa/vars
Using SSL: openssl OpenSSL 1.0.2k-fips 26 Jan 2017

You are about to sign the following certificate.
Please check over the details shown below for accuracy. Note that this request
has not been cryptographically verified. Please be sure it came from a trusted
source or that you have verified the request checksum with the sender.

Request subject, to be signed as a client certificate for 825 days:

subject=
  commonName              = client

Type the word 'yes' to continue, or any other input to abort.
  Confirm request details: yes
Using configuration from /opt/easy-rsa/pki/easy-rsa-1828.VwQHeF/tmp.eYqBSS
Enter pass phrase for /opt/easy-rsa/pki/private/ca.key:
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
commonName      :ASN.1 12:'client'
Certificate is to be certified until Jun  3 14:09:37 2023 GMT (825 days)

Write out database with 1 new entries
Data Base Updated

Certificate created at: /opt/easy-rsa/pki/issued/client.crt
```

## 四、OpenVPN服务端部署

### 1.安装 openvpn 软件

```
yum -y install openvpn
```

## 2.修改配置文件

自行创建配置文件 `/etc/openvpn/server.conf`，并加入如下配置

```
port 1194 #端口
proto udp #协议
dev tun #采用路由隧道模式tun
ca ca.crt #ca证书文件位置
cert server.crt #服务端公钥名称
key server.key #服务端私钥名称
dh dh.pem #交换证书
server 10.8.0.0 255.255.255.0 #给客户端分配地址池, 注意:不能和VPN服务器内网网段有相同
push "route 192.168.31.1 255.255.255.0" #允许客户端访问内网192.168.31.1网段
ifconfig-pool-persist ipp.txt #地址池记录文件位置
keepalive 10 120 #存活时间, 10秒ping一次, 120 如未收到响应则视为断线
max-clients 100 #最多允许100个客户端连接
status openvpn-status.log #日志记录位置
verb 3 #openvpn版本
client-to-client #客户端与客户端之间支持通信
log /var/log/openvpn.log #openvpn日志记录位置
persist-key #通过keepalive检测超时后, 重新启动VPN, 不重新读取keys, 保留第一次使用的keys。
persist-tun #检测超时后, 重新启动VPN, 一直保持tun是linkup的。否则网络会先linkdown然后再linkup
duplicate-cn
```

## 3. 拷贝证书到openvpn主配置文件目录下

```
cp -a /opt/easy-rsa/pki/ca.crt /etc/openvpn/
cp -a /opt/easy-rsa/pki/issued/server.crt /etc/openvpn/
cp -a /opt/easy-rsa/pki/private/server.key /etc/openvpn/
cp -a /opt/easy-rsa/pki/dh.pem /etc/openvpn/
```

## 4 启动openvpn

```
systemctl -f enable openvpn@server.service
systemctl start openvpn@server.service
```

# 五、OpenVPN客户端部署

## 1.安装OpenVPN客户端软件

这里是在windows环境下部署OpenVPN的客户端的，首先需要下载安装OpenVPN客户端软件

## 2.配置客户端

拷贝服务端生成的证书到OpenVPN安装目录的 `config` 目录下

分别拷贝以下几个文件

```
/opt/easy-rsa/pki/ca.crt
/opt/easy-rsa/pki/issued/client.crt
/opt/easy-rsa/pki/private/client.key
```

## 3.编写客户端配置文件

在OpenVPN安装目录的 `config` 目录下, 新建一个 `client.ovpn` 文件, 在文件中添加如下配置:

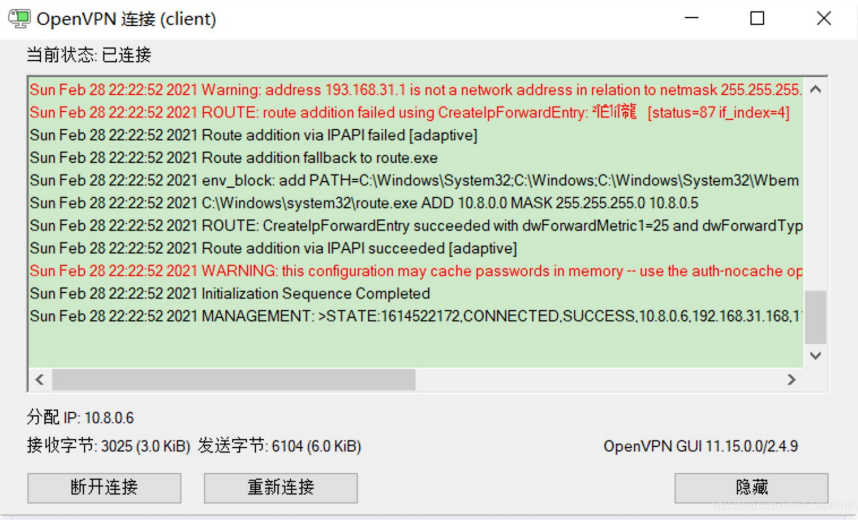
```
client #指定当前VPN是客户端
dev tun #使用tun隧道传输协议
proto udp #使用udp协议传输数据
remote 192.168.31.168 1194 #openvpn服务器IP地址端口号
resolv-retry infinite #断线自动重新连接, 在网络不稳定的情况下非常有用
```

```
nobind #不绑定本地特定的端口号
ca ca.crt #指定CA证书的文件路径
cert client.crt #指定当前客户端的证书文件路径
key client.key #指定当前客户端的私钥文件路径
verb 3 #指定日志文件的记录详细级别, 可选0-9, 等级越高日志内容越详细
persist-key #通过keepalive检测超时后, 重新启动VPN, 不重新读取keys, 保留第一次使用的keys
persist-tun #检测超时后, 重新启动VPN, 一直保持tun是linkup的。否则网络会先linkdown然后再linkup
```

4.启动OpenVPN客户端软件

双击安装好后的OpenVPN软件，然后右键点击连接。

连接成功后，在托任务栏位置的OpenVPN图标会变绿色，则说明OpenVPN已经连接成功。



OpenVPN会分配一个IP地址给客户端，客户端会使用该虚拟网络IP地址与服务端进行通信。

本文参与[腾讯云自媒体分享计划](#)，欢迎正在阅读的你也加入，一起分享。

举报

点赞 3

分享

0 条评论

我来说两句


登录后参与评论

相关文章

centos7部署OpenVpn




VPN直译就是虚拟专用通道，是提供给企业之间或者个人与公司之间安全数据传输的隧道，OpenVPN无疑是Linux下开源VPN的先锋，提供了良好的性能和友好的用户...

 玫柒的小窝

## Centos7安装与配置OpenVPN服务器

安装 OpenVPN、Firewalld 软件包以及用于生成各种证书的 EasyRSA

 用户7639835

## ubuntu部署VPN中openvpn（上）

如果在一个非信任网络下比如旅社或者咖啡店的WiFi网络下，想要通过你的智能手机或者笔记本电脑安全地访问互联网，那么VPN可以满足你的要求。VPN（Virtual...


 陈不成

## ubuntu部署VPN中openvpn（下）

1.创建客户端目录，存储客户端文件 mkdir -p ~/client-configs/files

 陈不成

## OpenVPN原理及部署使用

 常见\_youmen

## 基于 WireGuard 和 OpenVPN 的混合云基础架构建设

可以找一台能联网的 centos7 测试一下这个端口，如果没有 nc 工具可以yum install nc安装下。：

 米开朗基杨

## 当我有一台服务器时我做了什么

由于 dev 的机器与去年列举出来的事情相似，这里只介绍下在这台 1C2G 的服务器上做了什么

 山月

## nftables 与 OpenVPN 的结合实践

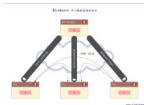
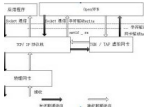
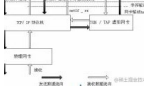
鉴于之前写的 VPN 权限管理项目的缺点，以及对比 iptables(ipset)、nftables、ebpf-iptables 后，确定过滤网络数据包的底层工...

 米开朗基杨

## centos7部署Jenkin

去jenkins官网<https://jenkins.io/index.html>下载jenkins安装包

 拓荒者



## CentOS7部署Grafana

前往<https://github.com/grafana/grafana/tree/v6.7.x> 下载源码

 院长技术

## CentOS7 部署WordPress

依次执行以下命令，进入/usr/share/nginx/html/目录，并下载与解压 WordPress。

 若尘\_

## CentOS7部署WordPress

依次执行以下命令，进入/usr/share/nginx/html/目录，并下载与解压 WordPress。

 若尘\_

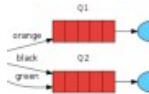
## nftables 日志解决方案实践

根据官方 wiki 中Logging traffic[1]这篇文章的说明：从 Linux 内核 3.17 开始提供完整的日志支持。如果您运行较旧的内核，则必须 ...

 米开朗基杨

## Centos7部署RabbitMQ 3.7.6


rabbitmq是采用Erlang（一种通用的面向并发的编程语言）编写的符合AMQP（Advanced Message Queuing Protocol）规范的...



 阿dai学长


## CentOS7部署harbor2.0(https)

Harbor(港口,港湾)是一个用于存储和分发Docker镜像的企业级Registry服务器

 常见\_youmen


## centos7部署mysql-5.7

使用二进制包部署会下载比较大，大约500M左右，而源码包就几十M。但使用二进制包不用编译，部署较快，相比于yum可以自定义目录，方便维护。

 用户1348170

## CentOS7下部署Zabbix4.0

总结：本文只是zabbix初始安装部署入门篇，zabbix强大的监控功能后续有空再继续探索

 yuanfan2012



## CentOS7下部署GitBook

GitBook是一个基于 Node.js 的命令行工具，可使用 Github/Git 和 Markdown 来制作精美的电子书

 yuanfan2012





## centos7部署mysql-5.7

使用二进制包部署会下载比较大，大约500M左右，而源码包就几十M。但使用二进制包不用编译，部署较快，相比于yum可以自定义目录，方便维护。

 陈不成

[更多文章 >](#)

### 社区

[专栏文章](#)  
[阅读清单](#)  
[互动问答](#)  
[技术沙龙](#)  
[技术快讯](#)  
[团队主页](#)  
[开发者手册](#)  
[腾讯云T1平台](#)

### 活动

[原创分享计划](#)  
[自媒体分享计划](#)  
[邀请作者入驻](#)  
[自荐上首页](#)  
[在线直播](#)  
[生态合作计划](#)

### 资源

[技术周刊](#)  
[社区标签](#)  
[开发者实验室](#)

### 关于

[视频介绍](#)  
[社区规范](#)  
[免责声明](#)  
[联系我们](#)  
[友情链接](#)

### 云+社区



扫码关注云+社区  
领取腾讯云代金券

### 热门产品

[域名注册](#)

[云服务器](#)

[区块链服务](#)

[消息队列](#)

[网络加速](#)

[云数据库](#)

[域名解析](#)

[云存储](#)

[视频直播](#)

### 热门推荐

[人脸识别](#)

[腾讯会议](#)

[企业云](#)

[CDN 加速](#)

[视频通话](#)

[图像分析](#)

[MySQL 数据库](#)

[SSL 证书](#)

[语音识别](#)

### 更多推荐

[数据安全](#)

[负载均衡](#)

[短信](#)

[文字识别](#)

[云点播](#)

[商标注册](#)

[小程序开发](#)

[网站监控](#)

[数据迁移](#)

