



链滴

openVPN 搭建内网环境

作者: [bao1991213](#)

原文链接: <https://ld246.com/article/1509173940216>

来源网站: [链滴](#)

许可协议: [署名-相同方式共享 4.0 国际 \(CC BY-SA 4.0\)](#)

OpenVPN配置

server 安装:

```
1 setenforce 0
2 sed -i '/^SELINUX=/c\SELINUX=disabled' /etc/selinux/config
3 yum -y install openssl openssl-devel
4 yum -y install lzo
5 rpm -ivh [http://mirrors.sohu.com/fedora-epel/6/x86_64/epel-release-6-8.noarch.rpm](http
//mirrors.sohu.com/fedora-epel/6/x86_64/epel-release-6-8.noarch.rpm)
6 sed -i 's/^mirrorlist=https/mirrorlist=http/' /etc/yum.repos.d/epel.repo
7 yum -y install openvpn easy-rsa
8 cd /usr/share/easy-rsa/2.0/
9 yum install -y vim
10 vim vars
```

```
export KEY_COUNTRY="CN"
export KEY_PROVINCE="ZHEJIANG"
export KEY_CITY="HANGZHOU"
export KEY_ORG="ABC123"
export KEY_EMAIL="ABC123@mABC123.COM"
export KEY_OU="ABC123"
```

```
11 source vars
12 ./clean-all
13 ./build-ca
14 ./build-key-server server
15 ./build-key client1
16 ./build-dh
17 openvpn --genkey --secret keys/ta.key
18 mkdir /etc/openvpn/keys
19 cp /usr/share/easy-rsa/2.0/keys/{ca.crt,server.{crt,key},dh2048.pem,ta.key} /etc/openvpn/k
ys
20 cp /usr/share/doc/openvpn-2.3.14/sample/sample-config-files/server.conf /etc/openvpn/
21 echo "" > /etc/openvpn/server.conf
22 vim /etc/openvpn/server.conf
23 sed -i '/net.ipv4.ip_forward/s/0/1/' /etc/sysctl.conf
24 sysctl -p
25 iptables -I INPUT -p tcp --dport 10194 -m comment --comment "openvpn" -j ACCEPT
26 iptables -t nat -A POSTROUTING -s 11.8.0.0/24 -j MASQUERADE
27 service iptables save
28 cd /etc/openvpn
29 vim checkpsw.sh
```

```

#!/bin/sh
#####
# checkpsw.sh (C) 2004 Mathias Sundman <[mathias@openvpn.se](mailto:mathias@openvpn
se)>
#
# This script will authenticate OpenVPN users against
# a plain text file. The passfile should simply contain
# one row per user with the username first followed by
# one or more space(s) or tab(s) and then the password.

PASSFILE="/etc/openvpn/psw-file"

LOG_FILE="/var/log/openvpn/openvpn-password.log"

TIME_STAMP=`date "+%Y-%m-%d %T"`

#####

if [ ! -r "${PASSFILE}" ]; then

    echo "${TIME_STAMP}: Could not open password file \"${PASSFILE}\" for reading." >> ${LOG
FILE}

    exit 1

fi

CORRECT_PASSWORD=`awk '!/^;/&&!/^#/&&$1=="${username}"{print $2;exit}' ${PASSFILE}`

if [ "${CORRECT_PASSWORD}" = "" ]; then

    echo "${TIME_STAMP}: User does not exist: username=\"${username}\", password=\"${passw
rd}\"." >> ${LOG_FILE}

    exit 1

fi

if [ "${password}" = "${CORRECT_PASSWORD}" ]; then

    echo "${TIME_STAMP}: Successful authentication: username=\"${username}\"." >> ${LOG_FIL
}

    exit 0

fi

echo "${TIME_STAMP}: Incorrect password: username=\"${username}\", password=\"${passw
rd}\"." >> ${LOG_FILE}

exit 1

#####

```

#####

```
30 chmod +x checkpsw.sh
31 cd /etc/openvpn
32 echo "openvpn openvpn" > psw-file
33 chmod 400 psw-file
34 chkconfig openvpn on
35 service openvpn start
```

server 服务端配置 centos :

```
port 10194
proto tcp
dev tun
ca keys/ca.crt
cert keys/server.crt
key keys/server.key # This file should be kept secret
dh keys/dh2048.pem
server 11.8.0.0 255.255.255.0
ifconfig-pool-persist ipp.txt
push "route 11.0.0.0 255.0.0.0"
push "route 192.168.0.0 255.255.0.0"
push "dhcp-option DNS 8.8.8.8"
push "dhcp-option DNS 8.8.4.4"
client-to-client
duplicate-cn
keepalive 10 120
cipher AES-256-CBC
comp-lzo
max-clients 100
persist-key
persist-tun

;调试使用 使用完删除 会记录ip
;log openvpn.log
;log-append openvpn.log
;verb 5

script-security 3 system
auth-user-pass-verify /etc/openvpn/checkpsw.sh via-env
```

client-cert-not-required

username-as-common-name

client 客户端配置:

cd C:\Program Files\OpenVPN\config

1. 新建 test 文件件 和 test.ovpn

2. 复制从服务端 /etc/openvpn/keys/ca.crt 复制到 test 文件下

3. 编辑 test.ovpn

client

dev tun

proto tcp

;服务端地址

remote 120.77.220.15 10194

resolv-retry infinite

nobind

persist-key

persist-tun

;socks-proxy-retry

;代理

;socks-proxy 192.168.157.150 7070

;证书地址

ca test/ca.crt

ns-cert-type server

cipher AES-256-CBC

comp-lzo

verb 5

;是否所有流量走服务端

;redirect-gateway def1

auth-user-pass

reneg-sec 360000