Use OpenVPN construct a VPN

jskyzero

2017 年 12 月 7 日

摘要

本文将概述如何使用 OpenVPN 搭建一个 VPN。本次实验，服务端选用 Linux 系统 (Linux 4.10.0-33-generic)，客户端选用 Windows 系统 (Windows 10 Fall Creator Update)。本次实验将直接使用 Static Key，这里不再赘述 Static Key 的优点缺点，可以查阅文末的参考。

1 安装

这里仅针对上述系统说明。

1.1 Linux

打开 Shell 输入 sudo apt-get install openvpn

1.2 Windows

打开 OpenVPN 官网下载安装包，按照安装向导安装。

2 服务端

首先我们生成密匙

openvpn –genkey –secret static.key

这个密匙是客户端和服务端都要使用的，关于怎样将这个密匙交给客户端又是另一个故事了。

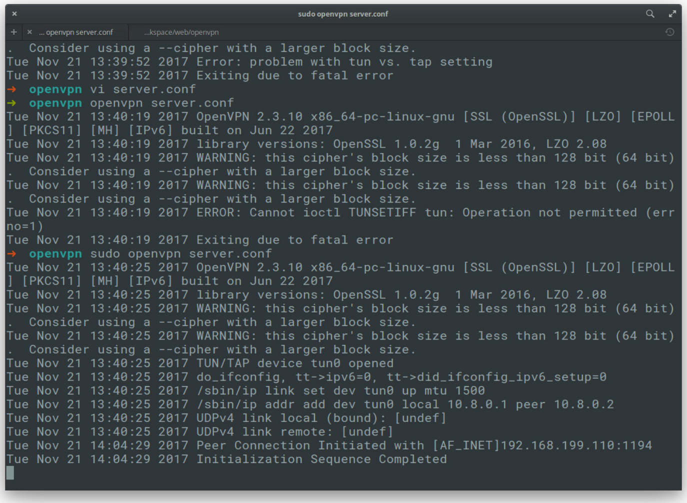
接着我们来编写服务端脚本，我们的目的是尽可能的简单，所以就尽可能的简单的来写。

dev tun

ifconfig 10.8.0.1 10.8.0.2

secret static.key

把这个文件命名为 server.conf，输入 openvpn server.conf 运行服务端，如果遇到权限问题，就加上 sudo。



```
.  Consider using a --cipher with a larger block size.
Tue Nov 21 13:39:52 2017 Error: problem with tun vs. tap setting
Tue Nov 21 13:39:52 2017 Exiting due to fatal error
➜  openvpn vi server.conf
➜  openvpn openvpn server.conf
Tue Nov 21 13:40:19 2017 OpenVPN 2.3.10 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [EPOLL
] [PKCS11] [MH] [IPv6] built on Jun 22 2017
Tue Nov 21 13:40:19 2017 library versions: OpenSSL 1.0.2g  1 Mar 2016, LZO 2.08
Tue Nov 21 13:40:19 2017 WARNING: this cipher's block size is less than 128 bit (64 bit)
.  Consider using a --cipher with a larger block size.
Tue Nov 21 13:40:19 2017 WARNING: this cipher's block size is less than 128 bit (64 bit)
.  Consider using a --cipher with a larger block size.
Tue Nov 21 13:40:19 2017 ERROR: Cannot ioctl TUNSETIFF tun: Operation not permitted (err
no=1)
Tue Nov 21 13:40:19 2017 Exiting due to fatal error
➜  openvpn sudo openvpn server.conf
Tue Nov 21 13:40:25 2017 OpenVPN 2.3.10 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [EPOLL
] [PKCS11] [MH] [IPv6] built on Jun 22 2017
Tue Nov 21 13:40:25 2017 library versions: OpenSSL 1.0.2g  1 Mar 2016, LZO 2.08
Tue Nov 21 13:40:25 2017 WARNING: this cipher's block size is less than 128 bit (64 bit)
.  Consider using a --cipher with a larger block size.
Tue Nov 21 13:40:25 2017 WARNING: this cipher's block size is less than 128 bit (64 bit)
.  Consider using a --cipher with a larger block size.
Tue Nov 21 13:40:25 2017 TUN/TAP device tun0 opened
Tue Nov 21 13:40:25 2017 do_ifconfig, tt->ipv6=0, tt->did_ifconfig_ipv6_setup=0
Tue Nov 21 13:40:25 2017 /sbin/ip link set dev tun0 up mtu 1500
Tue Nov 21 13:40:25 2017 /sbin/ip addr add dev tun0 local 10.8.0.1 peer 10.8.0.2
Tue Nov 21 13:40:25 2017 UDPv4 link local (bound): [undef]
Tue Nov 21 13:40:25 2017 UDPv4 link remote: [undef]
Tue Nov 21 14:04:29 2017 Peer Connection Initiated with [AF_INET]192.168.199.110:1194
Tue Nov 21 14:04:29 2017 Initialization Sequence Completed
```

3 客户端

客户端和服务端写起来是差不多的，

remote 192.168.199.100

dev tun

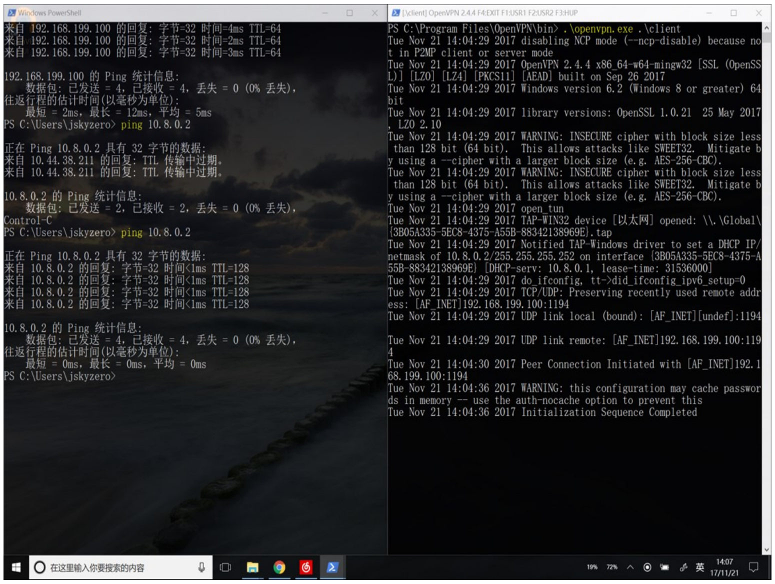
ifconfig 10.8.0.2 10.8.0.1

secret static.key

记得把上面那个 IP 改成服务器的地址。

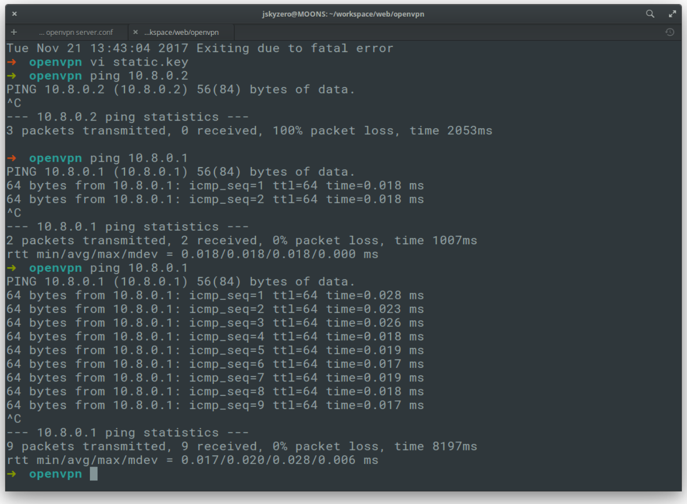
把这个文件命名为 client.conf，输入 openvpn clent.conf 运行客户端

接着我们就可以测试一下看看连接情况。



```
来自 192.168.199.100 的回复: 字节=32 时间=4ms TTL=64
来自 192.168.199.100 的回复: 字节=32 时间=2ms TTL=64
来自 192.168.199.100 的回复: 字节=32 时间=3ms TTL=64

192.168.199.100 的 Ping 统计信息:
    数据包: 已发送 = 4，已接收 = 4，丢失 = 0 (0% 丢失)，
往返行程的估计时间(以毫秒为单位):
    最短 = 2ms，最长 = 12ms，平均 = 5ms
PS C:\Users\jskyzero> ping 10.8.0.2

正在 Ping 10.8.0.2 具有 32 字节的数据:
来自 10.44.38.211 的回复: TTL 传输中过期。
来自 10.44.38.211 的回复: TTL 传输中过期。

10.8.0.2 的 Ping 统计信息:
    数据包: 已发送 = 2，已接收 = 2，丢失 = 0 (0% 丢失)，
Control-C
PS C:\Users\jskyzero> ping 10.8.0.2

正在 Ping 10.8.0.2 具有 32 字节的数据:
来自 10.8.0.2 的回复: 字节=32 时间<1ms TTL=128
来自 10.8.0.2 的回复: 字节=32 时间<1ms TTL=128
来自 10.8.0.2 的回复: 字节=32 时间<1ms TTL=128
来自 10.8.0.2 的回复: 字节=32 时间<1ms TTL=128

10.8.0.2 的 Ping 统计信息:
    数据包: 已发送 = 4，已接收 = 4，丢失 = 0 (0% 丢失)，
往返行程的估计时间(以毫秒为单位):
    最短 = 0ms，最长 = 0ms，平均 = 0ms
PS C:\Users\jskyzero>
```

```
PS C:\Program Files\OpenVPN\bin> .\openvpn.exe .\client
Tue Nov 21 14:04:29 2017 disabling NCP mode (--ncp-disable) because no
t in P2MP client or server mode
Tue Nov 21 14:04:29 2017 OpenVPN 2.4.4 x86_64-w64-mingw32 [SSL (OpenSS
L)] [LZO] [LZ4] [PKCS11] [AEAD] built on Sep 26 2017
Tue Nov 21 14:04:29 2017 Windows version 6.2 (Windows 8 or greater) 64
bit
Tue Nov 21 14:04:29 2017 library versions: OpenSSL 1.0.21  25 May 2017
, LZO 2.10
Tue Nov 21 14:04:29 2017 WARNING: INSECURE cipher with block size less
 than 128 bit (64 bit).  This allows attacks like SWEET32.  Mitigate b
y using a --cipher with a larger block size (e.g. AES-256-CBC).
Tue Nov 21 14:04:29 2017 WARNING: INSECURE cipher with block size less
 than 128 bit (64 bit).  This allows attacks like SWEET32.  Mitigate b
y using a --cipher with a larger block size (e.g. AES-256-CBC).
Tue Nov 21 14:04:29 2017 open_tun
Tue Nov 21 14:04:29 2017 TAP-WIN32 device [以太网] opened: \\.\Global\
{3B05A335-5EC8-4375-A55B-88342138969E}.tap
Tue Nov 21 14:04:29 2017 Notified TAP-Windows driver to set a DHCP IP/
netmask of 10.8.0.2/255.255.255.252 on interface {3B05A335-5EC8-4375-A
55B-88342138969E} [DHCP-serv: 10.8.0.1, lease-time: 31536000]
Tue Nov 21 14:04:29 2017 do_ifconfig, tt->did_ifconfig_ipv6_setup=0
Tue Nov 21 14:04:29 2017 TCP/UDP: Preserving recently used remote addr
ess: [AF_INET]192.168.199.100:1194
Tue Nov 21 14:04:29 2017 UDP link local (bound): [AF_INET][undef]:1194

Tue Nov 21 14:04:29 2017 UDP link remote: [AF_INET]192.168.199.100:119
4
Tue Nov 21 14:04:30 2017 Peer Connection Initiated with [AF_INET]192.1
68.199.100:1194
Tue Nov 21 14:04:36 2017 WARNING: this configuration may cache passwor
ds in memory -- use the auth-nocache option to prevent this
Tue Nov 21 14:04:36 2017 Initialization Sequence Completed
```



```
Tue Nov 21 13:43:04 2017 Exiting due to fatal error
➜  openvpn vi static.key
➜  openvpn ping 10.8.0.2
PING 10.8.0.2 (10.8.0.2) 56(84) bytes of data.
^C
--- 10.8.0.2 ping statistics ---
3 packets transmitted, 0 received, 100% packet loss, time 2053ms

➜  openvpn ping 10.8.0.1
PING 10.8.0.1 (10.8.0.1) 56(84) bytes of data.
64 bytes from 10.8.0.1: icmp_seq=1 ttl=64 time=0.018 ms
64 bytes from 10.8.0.1: icmp_seq=2 ttl=64 time=0.018 ms
^C
--- 10.8.0.1 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1007ms
rtt min/avg/max/mdev = 0.018/0.018/0.018/0.000 ms
➜  openvpn ping 10.8.0.1
PING 10.8.0.1 (10.8.0.1) 56(84) bytes of data.
64 bytes from 10.8.0.1: icmp_seq=1 ttl=64 time=0.028 ms
64 bytes from 10.8.0.1: icmp_seq=2 ttl=64 time=0.023 ms
64 bytes from 10.8.0.1: icmp_seq=3 ttl=64 time=0.026 ms
64 bytes from 10.8.0.1: icmp_seq=4 ttl=64 time=0.018 ms
64 bytes from 10.8.0.1: icmp_seq=5 ttl=64 time=0.019 ms
64 bytes from 10.8.0.1: icmp_seq=6 ttl=64 time=0.017 ms
64 bytes from 10.8.0.1: icmp_seq=7 ttl=64 time=0.019 ms
64 bytes from 10.8.0.1: icmp_seq=8 ttl=64 time=0.018 ms
64 bytes from 10.8.0.1: icmp_seq=9 ttl=64 time=0.017 ms
^C
--- 10.8.0.1 ping statistics ---
9 packets transmitted, 9 received, 0% packet loss, time 8197ms
rtt min/avg/max/mdev = 0.017/0.020/0.028/0.006 ms
➜  openvpn
```

参考文献

[1] openvpn howto