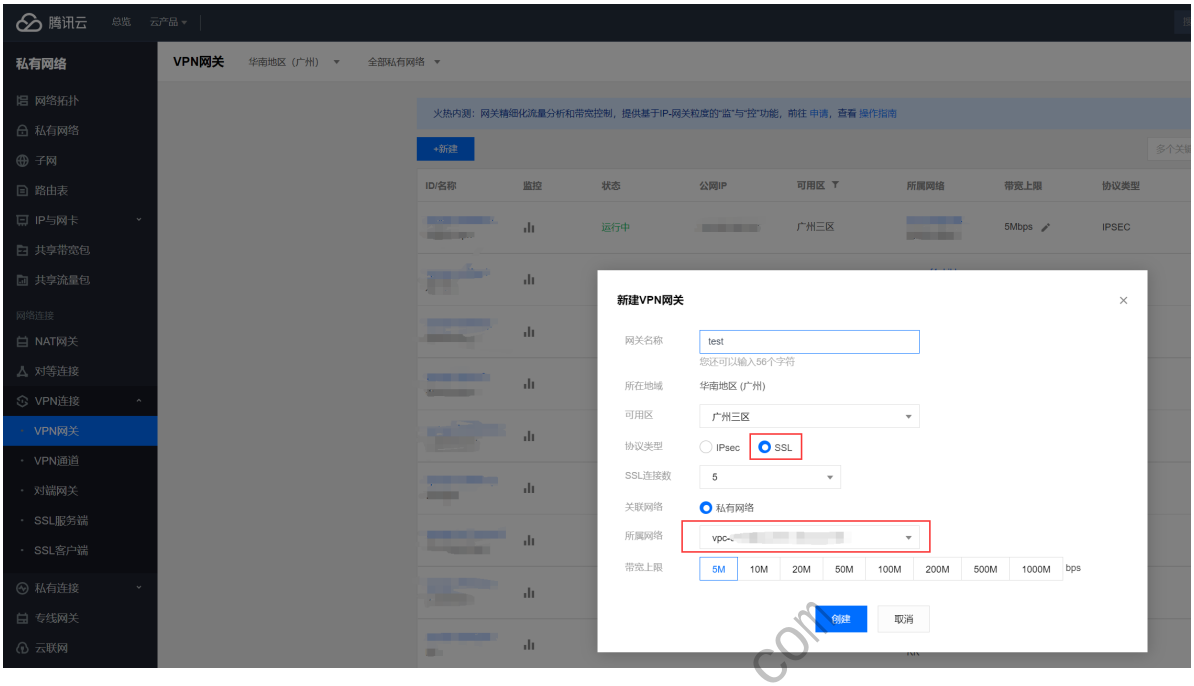
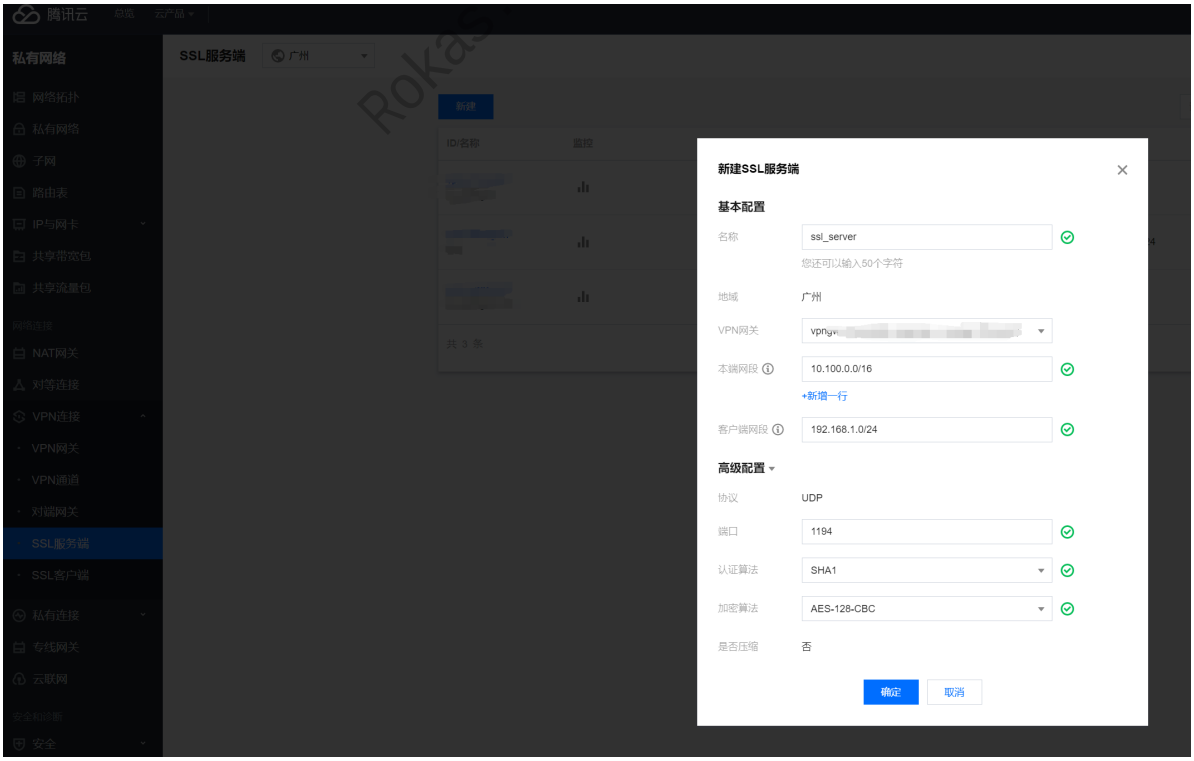
一、创建腾讯云SSL VPN网关

协议类型选择SSL，选择要打通云上所属VPC网络，如下图：



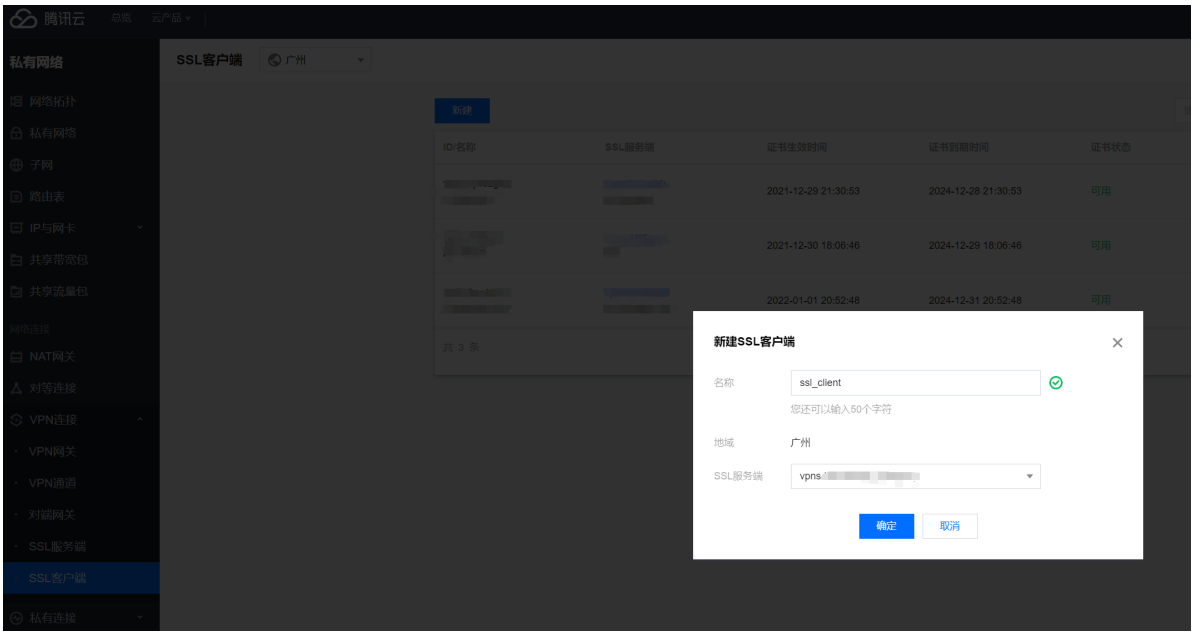
二、创建SSL服务端

目前腾讯云支持的SSL VPN协议只有UDP，暂不支持TCP；按照如下步骤填写本端网段(要打通的VPC网段)和对端网段(客户端内网网段)，填写端口、认证算法、加密算法等信息：



三、创建SSL客户端

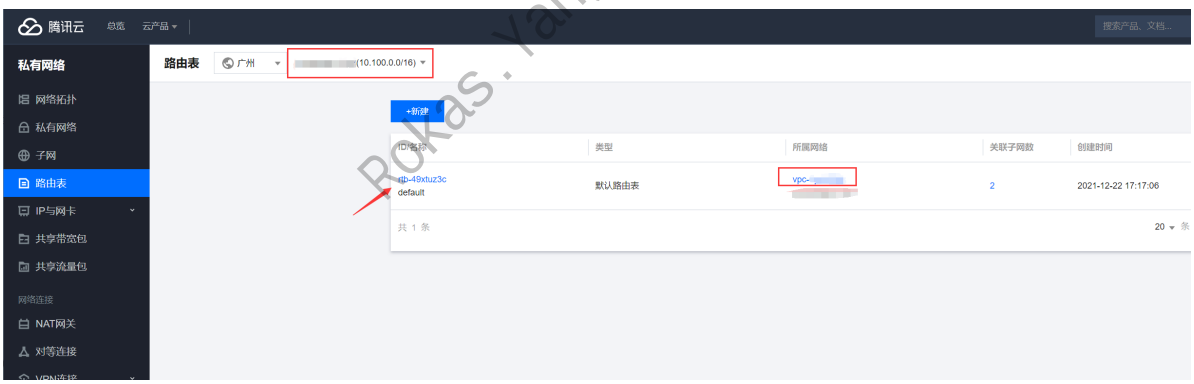
选择上一步创建的服务端，填写好备注名后点确定即可：



四、添加VPC路由

云上访问云下时，会查找VPC路由表指向，因此需要在对应的VPC路由表里面加一条到云下客户端网段的规则，下一跳指向SSL VPN网关。

在私有网络控制台，路由表里面选择对应VPC，对应路由表：

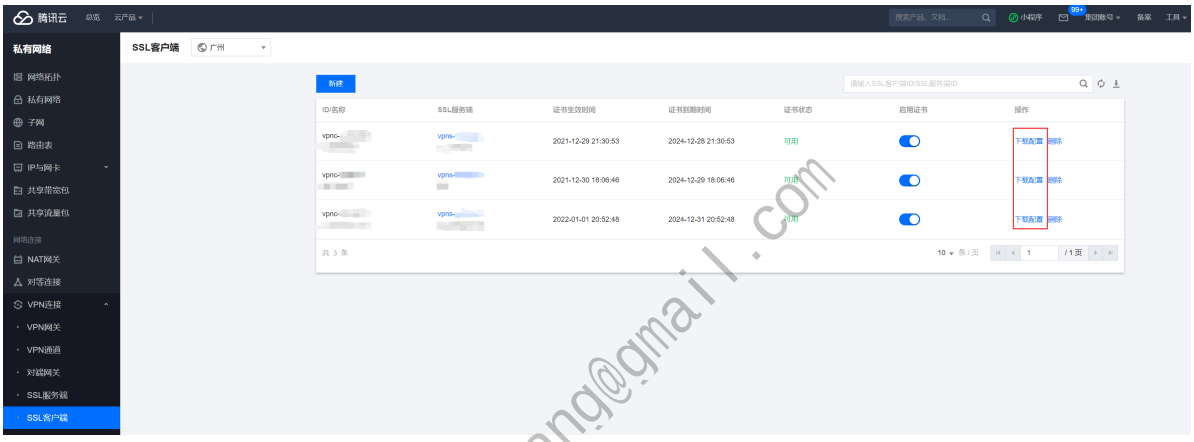


进入到路由表后，选择新增路由策略：

到此云上SSL VPN所有操作已经完成。

五、SSL配置文件下载

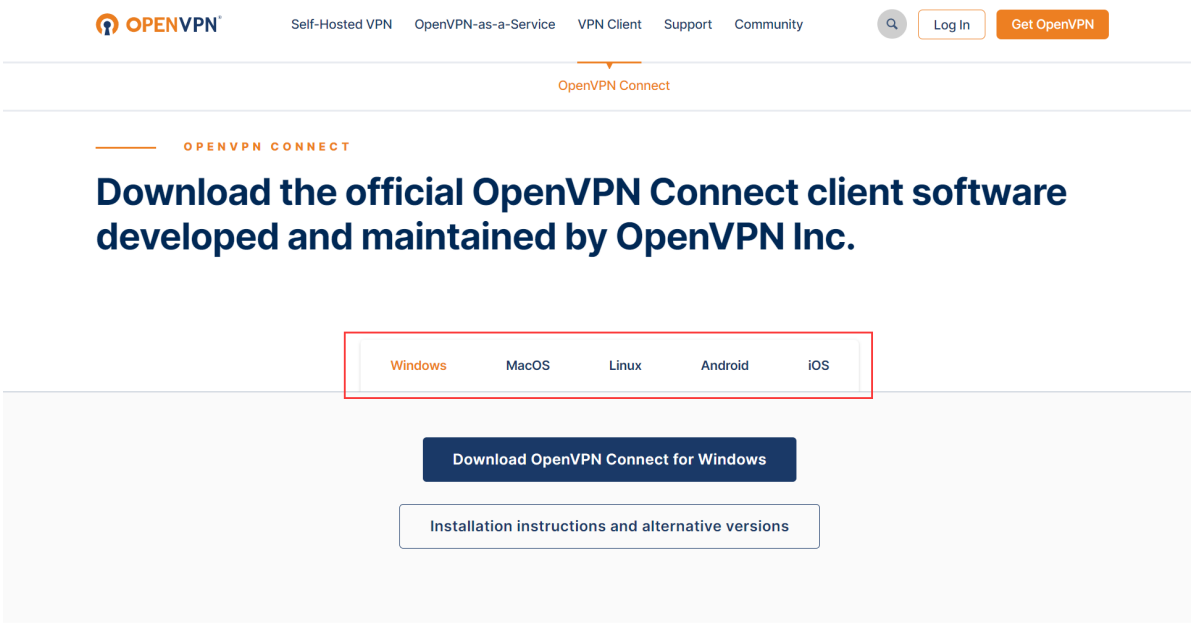
openvpn是Linux下的开源先锋，提供了良好的性能及友好的用户GUI，官方也推荐使用openvpn作为ssl vpn客户端使用，接下来将展示在Windows、Debian、Centos等系统中如何配置openvpn客户端，客户端配置文件在创建SSL客户端后会生成出来，在SSL客户端页面下载即可：



六、Windows配置OpenVpn Client

1.下载及安装

首先到**openvpn官方下载页面**下载openvpn connect（注意connect才是openvpn客户端，别下成服务端了）：

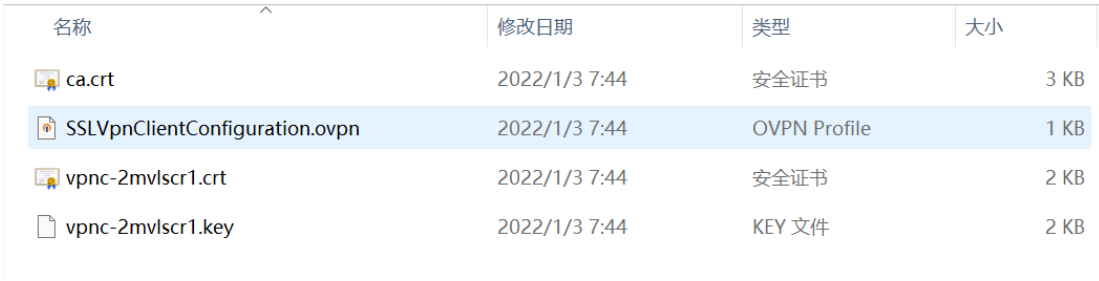


选择Windows这一栏，并点击Download即可，如果被墙打不开此下载页面，可在**此链接**下载。

2.配置及导入

安装好选择Import Profile，导入配置文件：

将配置文件解压后，把.ovpn结尾的配置文件拖拽进去：

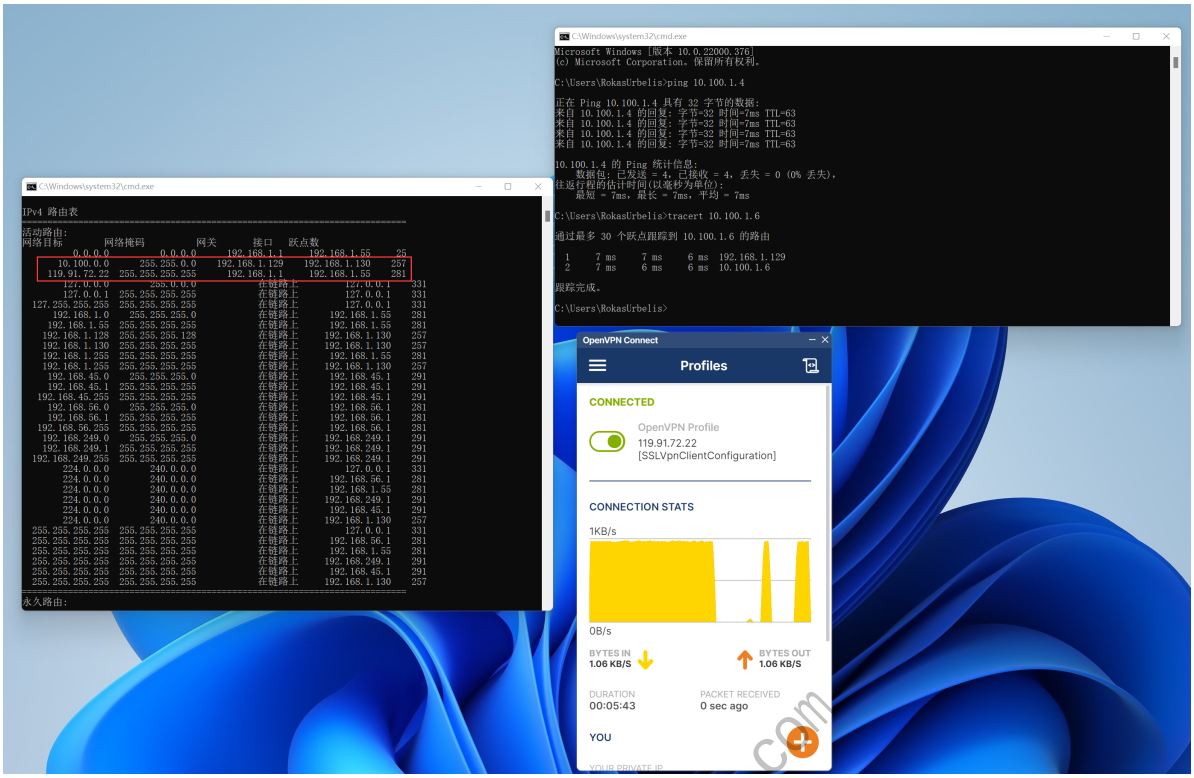


名称	修改日期	类型	大小
ca.crt	2022/1/3 7:44	安全证书	3 KB
SSLVpnClientConfiguration.ovpn	2022/1/3 7:44	OVPN Profile	1 KB
vpnc-2mvlscr1.crt	2022/1/3 7:44	安全证书	2 KB
vpnc-2mvlscr1.key	2022/1/3 7:44	KEY 文件	2 KB


OpenVPN Connect
Imported Profile
Profile Name
119.91.72.22 [SSLVpnClientConfiguration]
Server Hostname (locked)
119.91.72.22
Rokas.Yang@gmail.com
PROFILES
CONNECT

3.验证连通性

导入后点击connect，并验证连通性：



通过 `route print` 命令可以看到openvpn正常运行后，会自动下发路由到对端网关，同时ping对端VPC网段连通性正常，有出入流量，说明已正常打通。如果ping不通云上vpc机器，确保机器没有禁ping、安全组、acl有正常放通客户端内网网段。

此时使用wireshark抓包看，可以发现和对端内网交互时，实际是和对端vpn网关交互，因此也会依赖两端的公网质量：

udp.stream eq 1

No.	Time	Source	Destination	Protocol	Length	Identification	tcp.analysis.ack_rtt	Info
66	2022-01-03 15:58:48.768486	192.168.1.55	119.91.72.22	OpenVPN	66	0x4c11 (19473)		MessageType: P_DATA_V2
67	2022-01-03 15:58:48.775449	119.91.72.22	192.168.1.55	OpenVPN	66	0xbde3 (48611)		MessageType: P_DATA_V2
80	2022-01-03 15:58:49.730682	192.168.1.55	119.91.72.22	OpenVPN	128	0x4c12 (19474)		MessageType: P_DATA_V2
83	2022-01-03 15:58:49.738177	119.91.72.22	192.168.1.55	OpenVPN	156	0xbecd (48845)		MessageType: P_DATA_V2
108	2022-01-03 15:58:52.733986	192.168.1.55	119.91.72.22	OpenVPN	128	0x4c13 (19475)		MessageType: P_DATA_V2
109	2022-01-03 15:58:52.740701	119.91.72.22	192.168.1.55	OpenVPN	156	0xbfaa (49066)		MessageType: P_DATA_V2
116	2022-01-03 15:58:53.463554	192.168.1.55	119.91.72.22	OpenVPN	110	0x4c14 (19476)		MessageType: P_DATA_V2
117	2022-01-03 15:58:53.471113	119.91.72.22	192.168.1.55	OpenVPN	110	0xbfb3 (49075)		MessageType: P_DATA_V2
129	2022-01-03 15:58:54.471467	192.168.1.55	119.91.72.22	OpenVPN	110	0x4c15 (19477)		MessageType: P_DATA_V2
130	2022-01-03 15:58:54.477792	119.91.72.22	192.168.1.55	OpenVPN	110	0xc025 (49189)		MessageType: P_DATA_V2
138	2022-01-03 15:58:55.474033	192.168.1.55	119.91.72.22	OpenVPN	110	0x4c16 (19478)		MessageType: P_DATA_V2
139	2022-01-03 15:58:55.480667	119.91.72.22	192.168.1.55	OpenVPN	110	0xc027 (49191)		MessageType: P_DATA_V2
142	2022-01-03 15:58:55.738366	192.168.1.55	119.91.72.22	OpenVPN	128	0x4c17 (19479)		MessageType: P_DATA_V2
143	2022-01-03 15:58:55.744750	119.91.72.22	192.168.1.55	OpenVPN	156	0xc03b (49211)		MessageType: P_DATA_V2
152	2022-01-03 15:58:56.482420	192.168.1.55	119.91.72.22	OpenVPN	110	0x4c18 (19480)		MessageType: P_DATA_V2
153	2022-01-03 15:58:56.488801	119.91.72.22	192.168.1.55	OpenVPN	110	0xc09f (49311)		MessageType: P_DATA_V2

```
> Frame 66: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{C690E3AD-EE35-40BD-99BA-8BBD42EDBE27}, id 0
> Ethernet II, Src: ASUSTekC_3c:36:14 (50:eb:f6:3c:36:14), Dst: VMware_be:5a:26 (00:0c:29:be:5a:26)
> Internet Protocol Version 4, Src: 192.168.1.55, Dst: 119.91.72.22
v User Datagram Protocol, Src Port: 62447, Dst Port: 1194
    Source Port: 62447
    Destination Port: 1194
    Length: 32
    Checksum: 0x8182 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 1]
  > [Timestamps]
    UDP payload (24 bytes)
v OpenVPN Protocol
  v Type: 0x48 [opcode/key_id]
      0100 1... = Opcode: P_DATA_V2 (0x09)
      .... .000 = Key ID: 0
    Peer ID: 0
  v Data (20 bytes)
      Data: 0000011f2a187bf3641eb4cb07ed2d0a981fc748
```

七、Debian/Centos配置OpenVpn Client

1.Debian安装软件源、存储库秘钥及openvpn client

确保Debian支持https传输：

```
apt install apt-transport-https
```

安装openvpn官方存储库秘钥：

```
curl -fsSL https://swupdate.openvpn.net/repos/openvpn-repo-pkg-key.pub | gpg --dearmor
> /etc/apt/trusted.gpg.d/openvpn-repo-pkg-keyring.gpg
```

安装对应系统版本代号的软件源：

```
curl -fsSL https://swupdate.openvpn.net/community/openvpn3/repos/openvpn3-$DISTRO.list
>/etc/apt/sources.list.d/openvpn3.list
apt-get update
```

官方支持的发行版代号：

发行版	版本	代号($DISTRO)	架构
Debian	9	stretch	amd64
Debian	10	buster	amd64,arm64*
Debian	11	bullseye	amd64,arm64*
Ubuntu	18.04	bionic	amd64, arm64*
Ubuntu	20.04	focal	amd64,arm64*
Ubuntu	21.04	hirsute	amd64, arm64*

这里以Debian9 stretch作为演示，其他发行版同理，因此软件源安装应该是：

```
curl -fsSL https://swupdate.openvpn.net/community/openvpn3/repos/openvpn3-stretch.list
>/etc/apt/sources.list.d/openvpn3.list
apt-get update
```

境内机器由于GFW原因，可能无法使用以上软件源，或者受到速度限制，可以参考 **这篇文章** 搭建代理服务器使用。

```
apt install openvpn3
```

2.Centos安装openvpn客户端

Centos、Redhat系列支持的发行版代号：

发行版	版本	架构
Fedora	33, 34, Rawhide (*2)	aarch64, s390x, x86_64
Red Hat Enterprise Linux / CentOS	7	x86_64
Red Hat Enterprise Linux / CentOS	8	aarch64, x86_64

安装yum copr模块：

```
yum install yum-plugin-copr
```

启用Copr存储库：

```
yum copr enable dsommers/openvpn3
```

安装Openvpn client：

```
yum install openvpn3-client
```

3.导入配置文件并运行

将从腾讯云SSL客户端控制台导出的配置上传到Debian，解压后通过如下命令运行：

```
openvpn3 config-import --config ${MY_CONFIGURATION_FILE}   #导入配置文件，以便后续会话重用
openvpn3 session-start --config ${MY_CONFIGURATION_FILE}   #开启会话
```

```
 root@Server  ~/sslvpnconfig  openvpn3 session-start --config sslvpnclient.ovpn
Using configuration profile from file: sslvpnclient.ovpn
Session path: /net/openvpn/v3/sessions/c8dc3562s9986s465asa21es5f9329437101
Connected
 root@Server  ~/sslvpnconfig
```

sslvpnclient.ovpn替换成正确的ovpn配置文件，腾讯云官网的配置文件名应该是SSLVpnClientConfiguration.ovpn，可以看到connected说明已连接。

到此openvpn已正常运行，另开一个tty测试连通性：

```
 root@Server  ~/sslvpnconfig  ping 10.100.1.6
PING 10.100.1.6 (10.100.1.6) 56(84) bytes of data.
64 bytes from 10.100.1.6: icmp_seq=1 ttl=63 time=6.28 ms
64 bytes from 10.100.1.6: icmp_seq=2 ttl=63 time=6.84 ms
64 bytes from 10.100.1.6: icmp_seq=3 ttl=63 time=6.97 ms
^C
--- 10.100.1.6 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2002ms
rtt min/avg/max/mdev = 6.286/6.702/6.974/0.306 ms
 root@Server  ~/sslvpnconfig  traceroute 10.100.1.6
traceroute to 10.100.1.6 (10.100.1.6), 30 hops max, 60 byte packets
 1  192.168.1.129 (192.168.1.129)  7.059 ms  6.866 ms  7.537 ms
 2  10.100.1.6 (10.100.1.6)  8.216 ms * *
 root@Server  ~/sslvpnconfig
```

4.openvpn会话管理

openvpn允许同时运行多个配置文件及会话，通过以下命令可以管理会话：

```
openvpn3 sesstions-list  #查看当前运行的会话列表
```

```
root@Server ~/sslvpnconfig openvpn3 sessions-list
--------------------------------------------------------------------------------
        Path: /net/openvpn/v3/sessions/c8dc3562s9986s465asa21es5f9329437101
     Created: Mon Jan  3 17:05:41 2022                PID: 14259
       Owner: root                                  Device: tun0
 Config name: sslvpnclient.ovpn  (Config not available)
Session name: 119.91.72.22
      Status: Connection, Client connected
--------------------------------------------------------------------------------
root@Server ~/sslvpnconfig
```

重启会话：

```
openvpn3 session-manage --config ${CONFIGURATION_PROFILE_NAME} --restart
```

```
root@Server ~/sslvpnconfig openvpn3 session-manage --config sslvpnclient.ovpn --restart
Restarting session: /net/openvpn/v3/sessions/c8dc3562s9986s465asa21es5f9329437101
Connected
root@Server ~/sslvpnconfig
```

断开会话：

```
openvpn3 session-manage --session-path /net/openvpn/v3/sessions/..... --disconnect
```

```
root@Server ~/sslvpnconfig openvpn3 session-manage --session-path /net/openvpn/v3/sessions/c8dc3562s9986s465asa21es5f9329437101 --disconnect
Initiated session shutdown.

Connection statistics:
     BYTES_IN.................22568
     BYTES_OUT................36418
     PACKETS_IN...............136
     PACKETS_OUT..............247
     TUN_BYTES_IN.............12904
     TUN_BYTES_OUT............604
     TUN_PACKETS_IN...........128
     TUN_PACKETS_OUT..........7
     N_RECONNECT..............4

root@Server ~/sslvpnconfig                                                    ✔ 10650 17:18:43
```

断开会话后会统计流量使用明细。

查看会话状态：

```
openvpn3 session-stats --config ${CONFIGURATION_PROFILE_NAME}
openvpn3 session-stats --session-path /net/openvpn/v3/sessions/...
```

```
root@Server ~/sslvpnconfig openvpn3 session-stats --config sslvpnclient.ovpn                8 ↵ 10668 17:23:39

Connection statistics:
     BYTES_IN.................8484
     BYTES_OUT................12213
     PACKETS_IN...............40
     PACKETS_OUT..............69
     TUN_BYTES_IN.............3216
     TUN_PACKETS_IN...........32
     N_RECONNECT..............1

root@Server ~/sslvpnconfig openvpn3 session-stats --session-path /net/openvpn/v3/sessions/17e12a7as5760s4fe4sa449saa46b2cc2122  ✔ 10669 17:23:42

Connection statistics:
     BYTES_IN.................8508
     BYTES_OUT................12213
     PACKETS_IN...............41
     PACKETS_OUT..............69
     TUN_BYTES_IN.............3216
     TUN_PACKETS_IN...........32
     N_RECONNECT..............1

root@Server ~/sslvpnconfig                                                    ✔ 10670 17:23:46
```

查看会话日志：

```
openvpn3 log --config ${CONFIGURATION_PROFILE_NAME}
```

```
root@Server ~/sslvpnconfig openvpn3 log --config sslvpnclient.ovpn
Attaching to session /net/openvpn/v3/sessions/17e12a7as5760s4fe4sa449saa46b2cc2122
```