

# OpenWRT 通过连接在公网下的 OpenVPN 访问16 ACS服务器

由 earth 朱梦园 or 曾澳创建, 最后修改于四月 30, 2024

起因：测试TR069通信，需要 CPE 从 4/5G 公共网络访问到公司内部 16 ACS服务器

先确保拉下来的代码烧录后在VPN页面存在OpenVPN配置界面，若没有，可自行编译对应.ipk包安装，或直接在编译固件时选中 OpenVPN 和 OpenVPN 有关的包有（只考虑OpenWRT做client，不考虑在OpenWRT上部署OpenVPN server）：

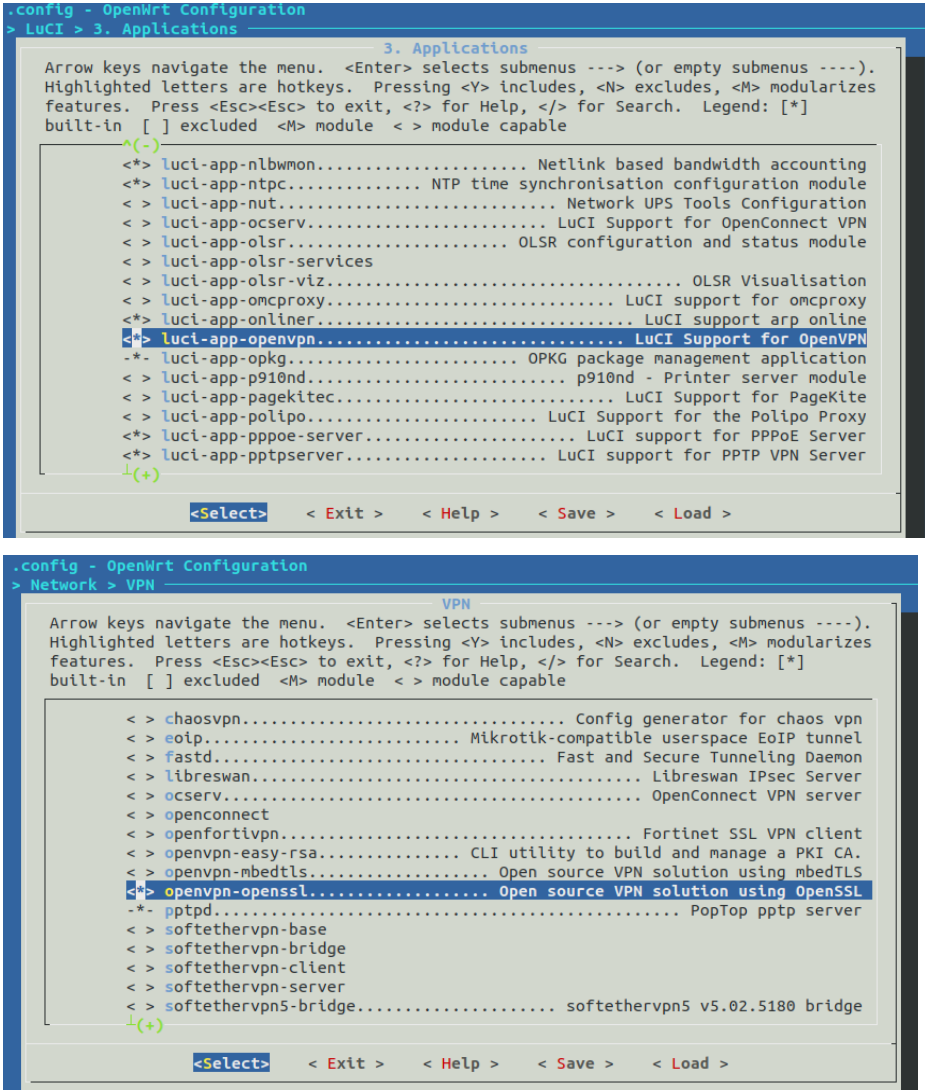
软件包名称	版本	大小 (ipk)	描述	
openvpn-openssl	2.5.3-4	-	-	移除...
luci-app-openvpn	git-23.363.21126-25c5fc0	-	-	移除...
luci-i18n-openvpn-en	git-23.363.21126-25c5fc0	-	-	移除...
luci-i18n-openvpn-es	git-23.363.21126-25c5fc0	-	-	移除...
luci-i18n-openvpn-zh-cn	git-23.363.21126-25c5fc0	-	-	移除...

luci-app-openvpn 是web GUI配置界面

i18n是对应的国家语言的web GUI翻译

openvpn-openssl 才是应用程序

编译时 make menuconfig 务必选中：



参考<http://192.168.10.16/share/%E5%88%86%E4%BA%AB/Pan/OpenVPN>将文件全部下载在本地

对client.ovpn进行修改：

client

dev tun

这是一个客户端配置文件  
 TUN 用于路由模式、TAP 用于桥接模式

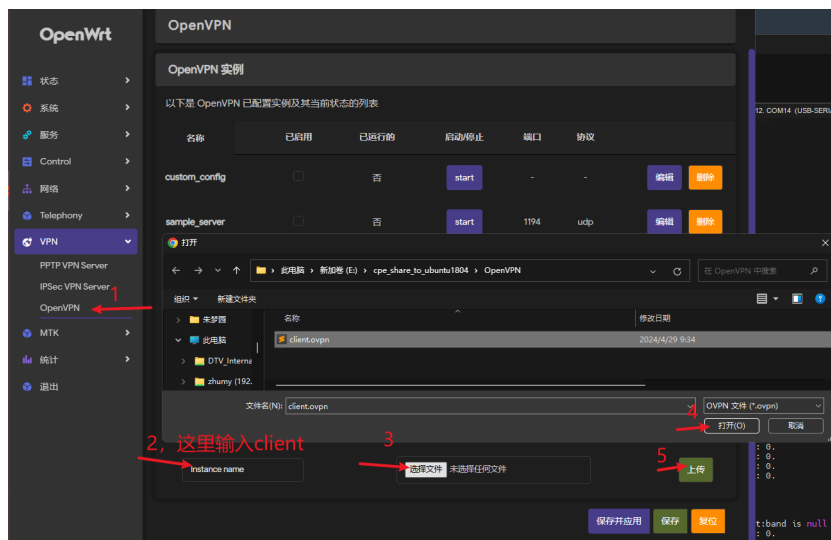
```
proto tcp
remote 14.21.46.164 1194
resolv-retry infinite
nobind
persist-key
persist-tun
ca /etc/openvpn/ca.crt
cert /etc/openvpn/opensslClient.crt
key /etc/openvpn/opensslClient.key
comp-lzo
verb 3
```

协议使用 TCP, 也支持 UDP  
OpenVPN 服务器的 ip 通信端口为 1194  
连接失败重试次数, infinite 表示无限次  
不绑定特定本地 IP 或端口, 由服务器指定  
重启 OpenVPN 时, 保持密钥的持久  
重启 OpenVPN 时, 保持虚拟网络设备的持久  
服务器 CA 证书路径  
客户端证书路径  
客户端私钥路径  
启用数据压缩, 以提高数据传输效率  
OpenVPN 日志等级

上述/etc/openvpn/路径为稍后文件上传到openwrt路径

但是推荐只上传 ca.crt opensslClient.crt opensslClient.key 这三个文件

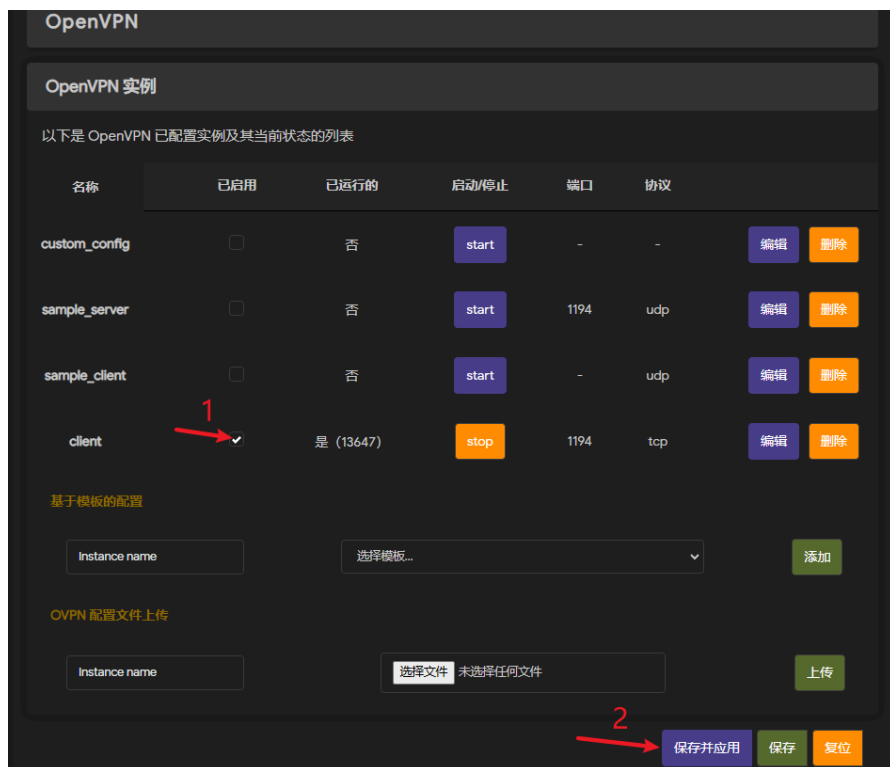
然后在web GUI 的 OpenVPN配置界面, 通过配置上传 client.ovpn



随后进入对应路径查看:

```
root@OpenWrt:/etc/openvpn# ls
ca.crt          client.ovpn     opensslClient.crt  opensslClient.key
```

在GUI界面, 选择刚创建的client, 然后保存并应用:



此时ifconfig应该会出现tun0设备 (图片中是已经建立连接后有了ip, 这一步只要创建了tun0就算成功):

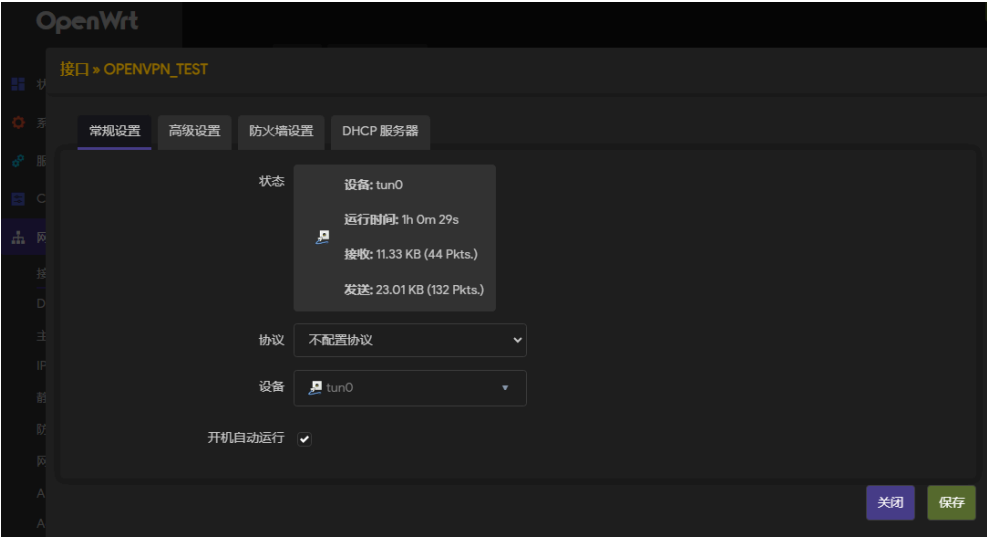
```
tun0      Link encap:UNSPEC  HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
        inet addr:192.168.222.14  P-t-P:192.168.222.13  Mask:255.255.255.255
        inet6 addr: fe80::d931:f4c4:436e:358/64  Scope:Link
        UP POINTOPOINT RUNNING NOARP MULTICAST  MTU:1500  Metric:1
        RX packets:44  errors:0  dropped:0  overruns:0  frame:0
        TX packets:127  errors:0  dropped:0  overruns:0  carrier:0
        collisions:0 txqueuelen:500
        RX bytes:11327 (11.0 KiB)  TX bytes:22713 (22.1 KiB)
```

若没创建，可以使用下述方式手动开启 OpenvVPN 连接查看 log

```
openvpn --config ./client.ovpn
```

```
root@OpenWrt:/etc/openvpn# ls
ca.crt      client.ovpn  opwrtclient.crt  opwrtclient.key
root@OpenWrt:/etc/openvpn# openvpn --config ./client.ovpn
2024-04-29 16:59:55 WARNING: Compression for receiving enabled. Compression has been used in the past to break encryption. Sent packets are not compressed unless
"allow-compression yes" is also set.
2024-04-29 16:59:55 --cipher is not set. Previous OpenVPN version defaulted to BF-CBC as fallback when cipher negotiation failed in this case. If you need this f
allback please add --data-ciphers-fallback BF-CBC to your configuration and/or add BF-CBC to --data-ciphers.
2024-04-29 16:59:55 OpenVPN 2.5.3 aarch64-openwrt-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL] [PM/PKTINFO] [AEAD]
2024-04-29 16:59:55 library versions: OpenSSL 1.1.1t  7 Feb 2023, LZO 2.10
2024-04-29 16:59:55 WARNING: No server certificate verification method has been enabled. See http://openvpn.net/howto.html#mitm for more info.
2024-04-29 16:59:55 TCP/UDP: Preserving recently used remote address: [AF_INET]14.21.46.164:1194
2024-04-29 16:59:55 Socket Buffers: R=[6291456->6291456] S=[2097152->2097152]
2024-04-29 16:59:55 Attempting to establish TCP connection with [AF_INET]14.21.46.164:1194 [nonblock]
2024-04-29 16:59:55 TCP connection established with [AF_INET]14.21.46.164:1194
2024-04-29 16:59:55 TCP_CLIENT link local: (not bound)
2024-04-29 16:59:55 TCP_CLIENT link remote: [AF_INET]14.21.46.164:1194
2024-04-29 16:59:55 TLS: Initial packet from [AF_INET]14.21.46.164:1194, sid=e66748b8 4f7e3eff
2024-04-29 16:59:55 VERIFY OK: depth=1, CN=Easy-RSA CA
2024-04-29 16:59:55 VERIFY OK: depth=0, CN=STBRocks
```

未配置防火墙的话，可能会导致断开，然后又重连，又断开，又重连的log循环输出，这是正常现象，只要 tun0 存在就可，后续配置防火墙后，连接会稳定接着去接口新建接口选择该设备（不配置任何协议）：



配置好是这样：


接口

设备

全局网络选项

接口

OPENVPN\_TEST

tun0

协议: 不配置协议

运行时间: 2h 0m 42s

接收: 11.33 KB (44 Pkts.)

发送: 26.61 KB (192 Pkts.)


重启

停止

编辑

删除

LAN

br-lan

协议: 静态地址

运行时间: 2h 1m 33s

MAC: 86:F1:ED:BE:31:58

接收: 3.20 MB (11416 Pkts.)

发送: 7.62 MB (11076 Pkts.)

IPv4: 192.168.1.1/24

IPv6: 240e:47c:34d0:b549::1/64

IPv6: fd88:daa5:5daa::1/60


重启

停止

编辑

删除

WAN

ccmni2

协议: Quectel Cellular

运行时间: 0h 29m 42s

接收: 180.41 KB (971 Pkts.)

发送: 158.66 KB (1041 Pkts.)

IPv4: 10.20.148.155/29

IPv6: 240e:47c:34d0:b549:17ca:b43a:d8f8:7c68/128

IPv6-PD: 240e:47c:34d0:b549::/64


重启

停止

编辑

删除

WAN6

ccmni

协议: DHCPv6 客户端

接收: 0 B (0 Pkts.)

发送: 0 B (0 Pkts.)

错误: 网络设备不存在

重启

停止

编辑

删除

添加新接口...

保存并应用

保存

复位

Powered by LuCI rezhu\_5\_2 branch (git-23.363.21126-25c5fc0) / ArgonTheme v2.3.1 / OpenWrt 21.02.7 r16847-f8282da11e

防火墙这里先新建一个防火墙（未配置）：

OpenWrt

接口 » OPENVPN\_TEST

常规设置

高级设置


防火墙设置

DHCP 服务器

创建/分配防火墙区域

ovpn

OpenVPN\_test



为此接口分配所属的防火墙区域，选择未指定可将该接口移出已关联的区域，或者填写创建栏来创建一个新的区域，并将当前接口与之建立关联。

关闭

保存

接着去防火墙配置界面对新增的防火墙进行配置：

防火墙 - 区域设置

常规设置

高级设置

连接跟踪设置

额外的 iptables 参数

本节定义 "ovpn" 的通用属性。入站数据和出站数据项用于设置此区域入站和出站流量的默认策略，转发选项描述该区域内不同网络之间的流量转发策略。涵盖的网络指定从属于这个区域的网络。

名称

ovpn

入站数据

接受

出站数据

接受

转发

拒绝

IP 动态伪装


☐

MSS 钳制

☐

涵盖的网络

OpenVPN\_test




以下选项控制此区域（ovpn）和其它区域间的转发策略。目标区域接收源自 ovpn 的转发流量。源区域匹配的转发流量来自目标为 ovpn 的其它区域。转发规则的作用是单向的，例如：转发从 lan 到 wan 的流量并不意味着允许反向转发从 wan 到 lan 的流量。

允许转发到目标区域:

未指定

允许来自源区域的转发:

lan

lan: 

关闭

保存

防火墙 - 区域设置

常规设置

高级设置

连接跟踪设置

额外的 iptables 参数

以下选项控制此区域（ovpn）和其它区域间的转发策略。*目标区域接收源自 ovpn 的转发流量。源区域匹配的转发流量来自目标为 ovpn 的其它区域。*转发规则的作用是单向的，例如：转发从 lan 到 wan 的流量并不意味着允许反向转发从 wan 到 lan 的流量。

涵盖的设备

涵盖的子网

地址族限制

要限制 IP 动态伪装的源子网

要限制 IP 动态伪装的目标子网

启用此区域的日志记录

tun0

☐ 以太网适配器: "rai0"

☐ 以太网适配器: "rmdis0"

☐ 以太网适配器: "teq10"

☒ 以太网适配器: "tun0" (OpenVPN\_test)

☐ -- 自定义 --

0.0.0.0/0

0.0.0.0/0

☐

关闭

保存

最后保存并应用

防火墙 - 区域设置

防火墙通过在网络接口上创建区域来控制网络流量。

常规设置

区域

启用 SYN-flood 防御

丢弃无效数据包

入站数据

出站数据

转发

lan

⇒

wan

ovpn

接受

接受

接受

☐

编辑

删除

wan

⇒

REJECT

拒绝

接受

拒绝

☒

编辑

删除

ovpn

⇒

REJECT

接受

接受

拒绝

☐

编辑

删除

添加

保存并应用

保存

复位

然后重启 reboot

此时 ifconfig tun0 设备已经自动获取ip，说明 CPE 与公网 VPN 建立连接成功：

```
tun0      Link encap:UNSPEC HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
          inet addr:192.168.222.14 P-t-P:192.168.222.13 Mask:255.255.255.255
          inet6 addr: fe80::d931:f4c4:436e:358/64 Scope:Link
          UP POINTOPOINT RUNNING NOARP MULTICAST MTU:1500 Metric:1
          RX packets:44 errors:0 dropped:0 overruns:0 frame:0
          TX packets:132 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:500
          RX bytes:11327 (11.0 KiB) TX bytes:23013 (22.4 KiB)
```

打开 16 服务器上的 OpenVPN 连接：

```
sudo openvpn --config /etc/openvpn/client/ubuntu16Client.ovpn
```

此时 ifconfig：

```
tun0: flags=4305<UP,POINTOPOINT,RUNNING,NOARP,MULTICAST> mtu 1500
    inet 192.168.222.10 netmask 255.255.255.255 destination 192.168.222.9
    inet6 fe80::4dd8:b635:f9f8:459c prefixlen 64 scopeid 0x20<link>
    unspec 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00 txqueuelen 100 (UNSPEC)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 6 bytes 288 (288.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

16服务器与公网VPN建立连接成功

不使用时请关闭16服务器的 VPN 连接!!!

当关闭了 16 服务器的 VPN 时, ifconfig 是不存在 tun0 设备的

测试二者连接:

```
64 bytes from 192.168.222.10: seq=93 ttl=64 time=308.267 ms
64 bytes from 192.168.222.10: seq=94 ttl=64 time=51.822 ms
^C
-- 192.168.222.10 ping statistics --
95 packets transmitted, 95 packets received, 0% packet loss
round-trip min/avg/max = 23.265/54.534/492.422 ms
root@OpenWrt:~#

64 bytes from 192.168.222.14: icmp_seq=91 ttl=64 time=30.3 ms
64 bytes from 192.168.222.14: icmp_seq=92 ttl=64 time=255 ms
^C
-- 192.168.222.14 ping statistics --
93 packets transmitted, 92 received, 1% packet loss, time 92141ms
rtt min/avg/max/mdev = 20.997/141.270/804.942/123.701 ms
zhumy@GiecDtv:~$
```

由于CPE插卡走4/5G网络会有信号波动, 延迟时高时低是正常现象, 但是不会出现断联

进入Openwrt界面, 修改easycwmp文件:

```
root@OpenWrt:/etc/openvpn# cd /etc/config/
root@OpenWrt:/etc/config# cat easycwmp

config local
    option enable '1'
    option port '7547'
    option ubus_socket '/var/run/ubus.sock'
    option date_format '%FT%T%z'
    option authentication 'Digest'
    option logging_level '3'
    option interface 'tun0'

config acs
    option periodic_enable '1'
    option url 'http://192.168.222.10:7547'
    option periodic_interval '300'
    option periodic_time '1970-01-01T19:17:10.703Z'

config device
    option hardware_version 'v0'
    option software_version 'r16847-f8282da11e'
    option oui 'GIEC_CPE_001'
    option serial_number 'GIEC_CPE123456'
    option product_class 'Generic'
    option manufacturer 'OpenWrt'
https__openwrt.org_
```

192.168.222.10:7547 是16服务器连接 VPN 后 tun0 的 ip, 7547 是 ACS 服务器使用的端口

保存后重启 easycwmpd 服务

在<http://192.168.10.16:3000/>可以看到CPE设备, 也可以正常下发参数

 GIEC\_CPE\_001-Generic-GIEC\_CPE123456: Summoned

Overview

Devices

Faults

Admin

GIEC\_CPE\_001-Generic-GIEC\_CPE123456

< +

Pinging 192.168.222.14: 39 ms

Last inform

2024/4/29 15:17:20

● Online now

Summon

Serial number

GIEC\_CPE123456

Product class

Generic

OUI

GIEC\_CPE\_001

Manufacturer

OpenWrt https\_\_openwrt.org\_

Hardware version

v0

Software version

r16847-f8282da11e

重启后也可以自动先连接 VPN 然后连接到 16 的 ACS 服务器, 至此 ACS 即可实时监控 CPE 并下发参数

整体网络拓扑为:

