家庭网关斐讯 k3 组网拓展篇

作者：evling
原文链接：https://ld246.com/article/1607184602445
来源网站：链滴

导读

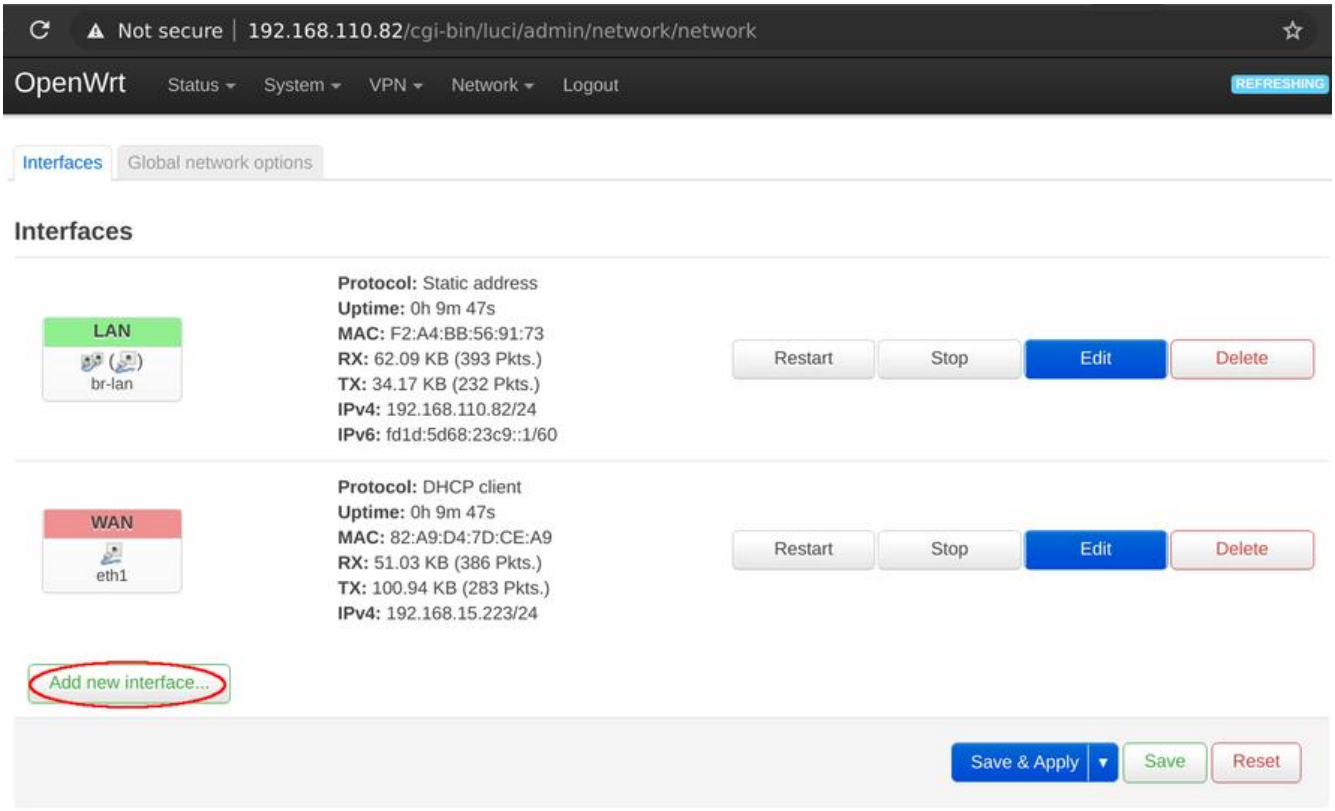
基于 openwrt 组建家庭网络是非常有优势的，能搭载 openwrt 的也基本上是一些嵌入式设备，全天机，现在就来教大家如何异地组网的高级技巧。继上篇带给大家的《家庭网关斐讯 k3 面向公网篇》留下了三个问题：

- 接入后可访问公网
- 各个客户端指定固定 IP ，推送不同的路由
- 服务端所在网络如何与客户端机器所在网络进行通信

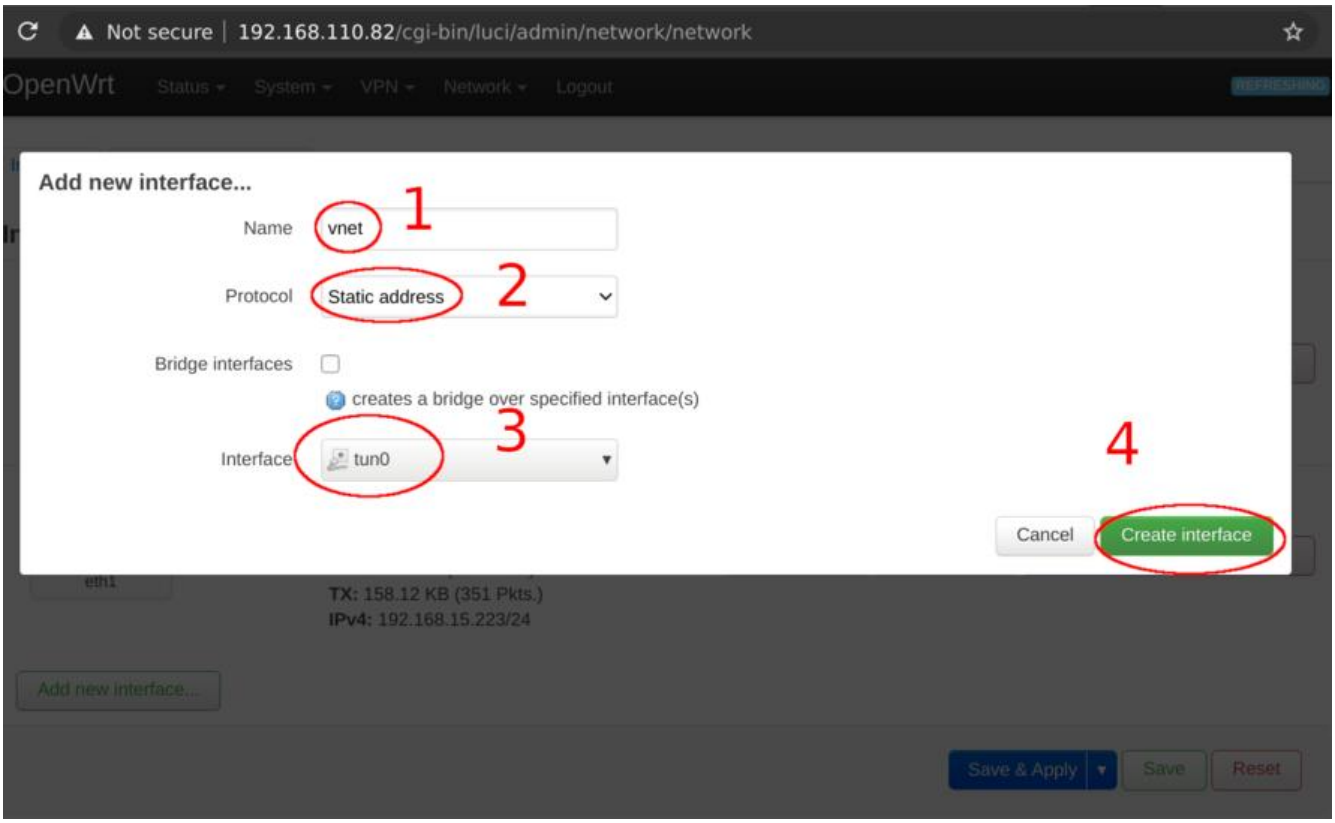
接入后可访问公网

上篇仅仅完成了虚拟专用网网络连接，但并未做规则转发，利用搭建好的家庭网关服务直接访问公网不可行的，现在简单来步操作就能解决这个问题了，看好了，兄弟，易霁君来刷屏来了。

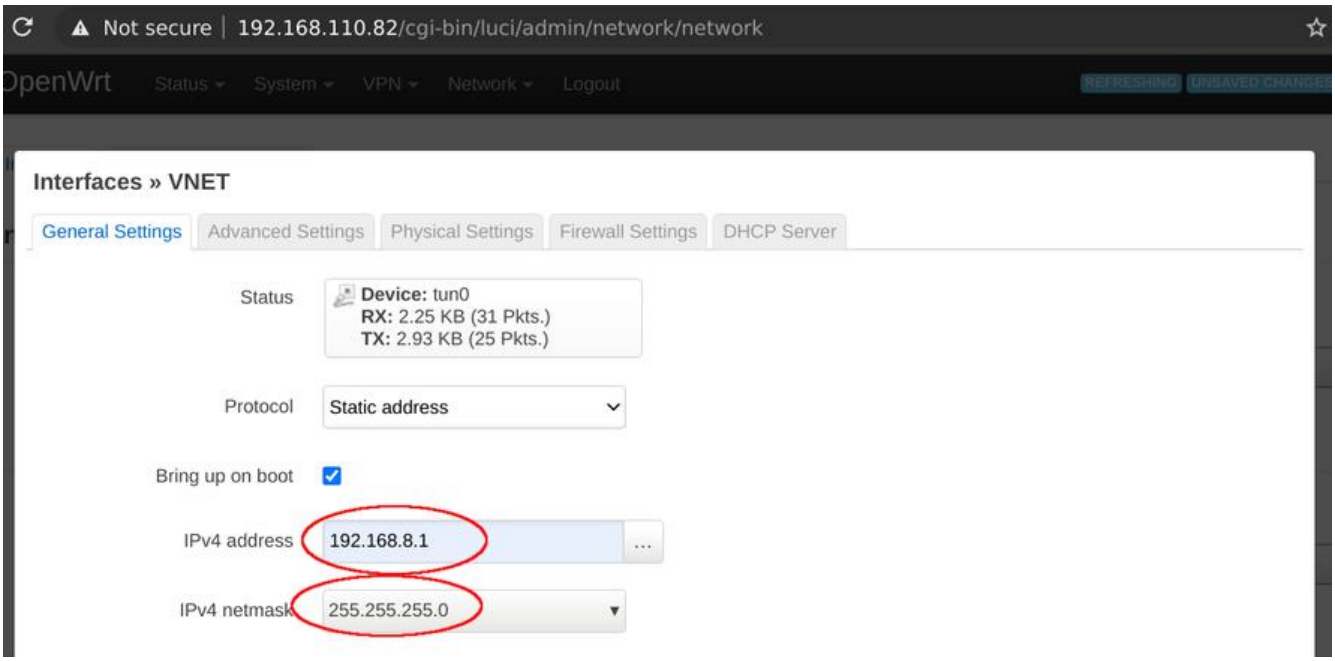
在网页控制面板打开网路接口页 Network/Interfaces，添加一个新接口。



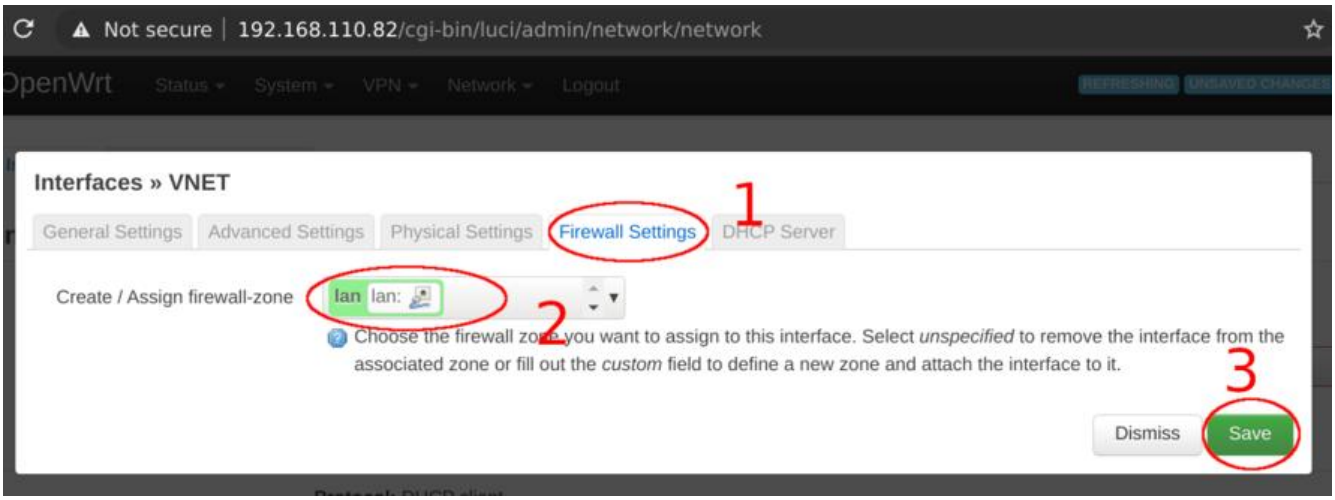
给虚拟接口取个名字曰 vnet，选定静态 IP 分配方式、tun0接口，如下



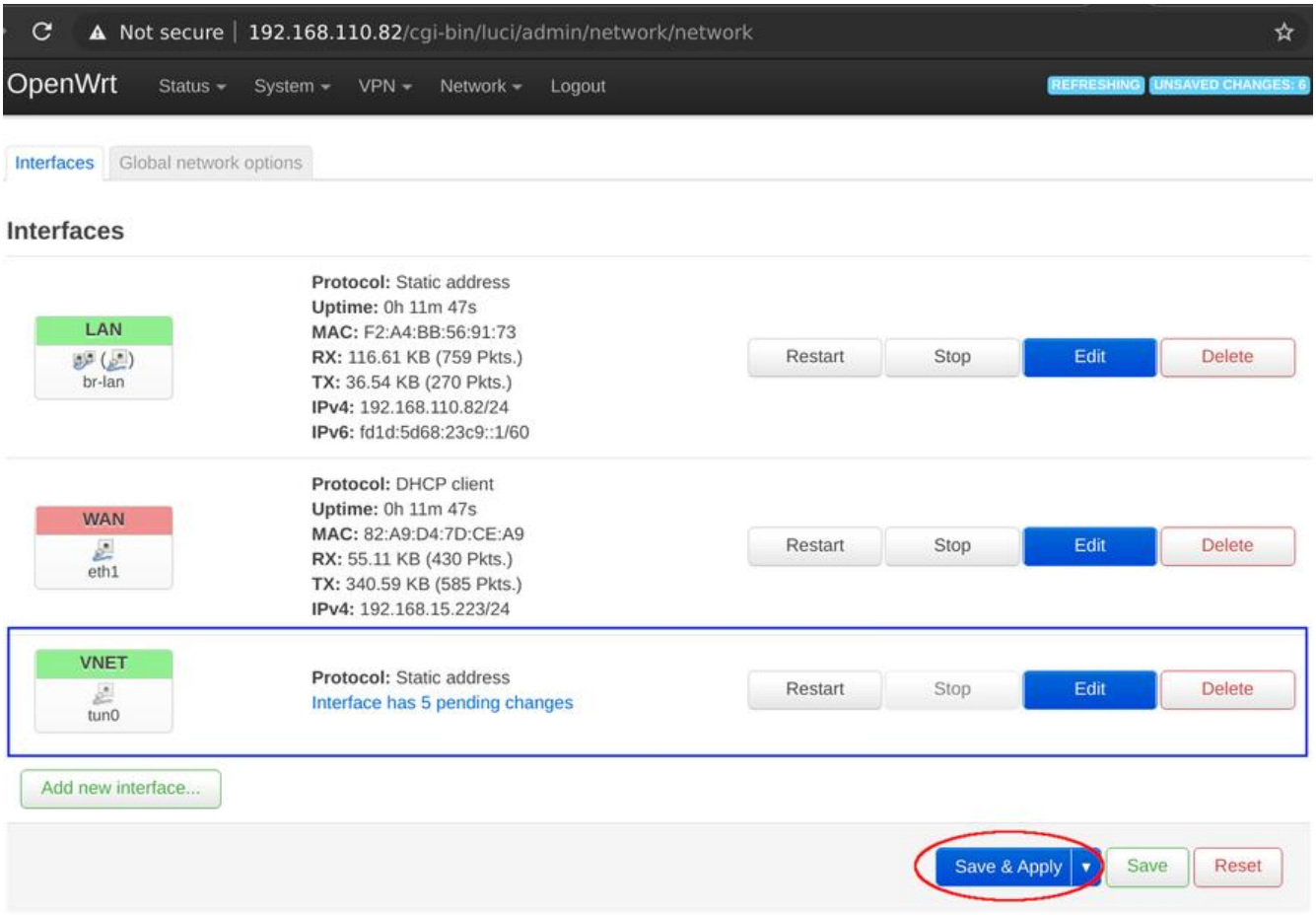
随后指定咱们先前设定的网关地址 192.168.8.1/24



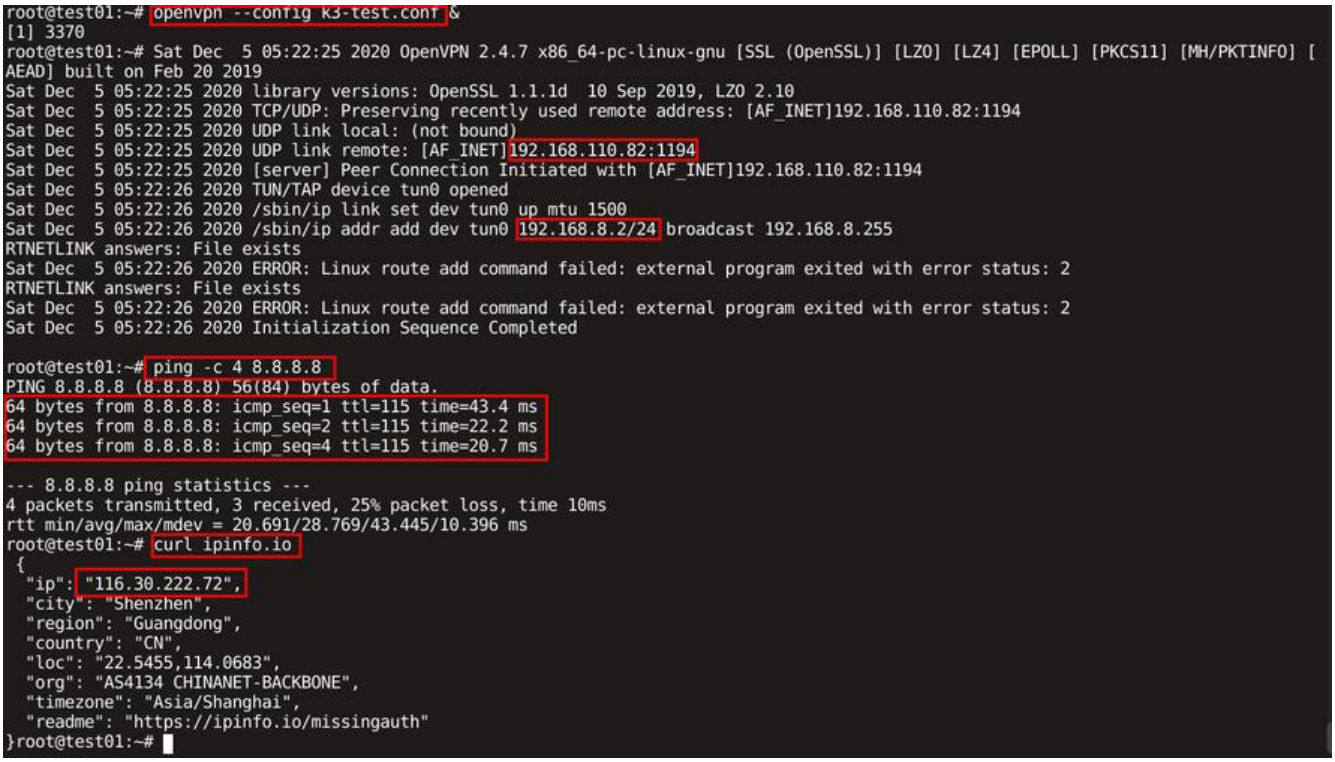
在当前页面切换到防火墙设置选项下，应用为 lan策略，就可让tun0接口下的网络享受本地lan的访问限，犹如是在家里一样。



回到网络设置主页，发现新增了一个接口 VNET，点击 保存并应用就灵验了。



最后义雾君来做个验证，访问外网试试呗



显然，咱们就这么几步的操作就能让的虚拟内网实现了在家里访问内外网的效果。

客户端指定静态IP

如果需要对客户端进行指定静态 IP ，就要使用到 OpenVPN 里的 ccd ，同时我们需要在生成客户端书时指定 COMMON_NAME如下是 client1，记住这个，用的上，当然可以通过修改它生成更多的客端配置文件，这里易雾君引用下上篇《家庭网关斐讯 k3 面向公网篇》中脚本的部分内容，注意修改户端名称：

```
# Base vars
COMMON_NAME="client1"
CCD_DIR="/etc/openvpn/ccd"
OVPN_DIR="/etc/openvpn"
OVPN_PKI="/etc/easy-rsa/pki"
OVPN_PORT="1194"
OVPN_PROTO="udp"
OVPN_POOL="192.168.8.0 255.255.255.0"
OVPN_DNS="${OVPN_POOL%.* *}.1"
OVPN_DOMAIN="$(uci get dhcp.@dnsmasq[0].domain)"
OVPN_SERV="vnet.evling.me" # Please change to yours


# Configuration parameters
export EASYRSA_KEY_SIZE="2048"
export EASYRSA_PKI="${OVPN_PKI}"
export EASYRSA_REQ_CN="ovpnca"
export EASYRSA_BATCH="1"

# Generate a key pair and sign locally for a client
easyrsa build-client-full ${COMMON_NAME} nopass
```

```
# Configuration parameters
OVPN_DH="$(cat ${OVPN_PKI}/dh.pem)"
OVPN_TC="$(sed -e "/^#/d;/^\w/N;s/\n//" ${OVPN_PKI}/tc.pem)"
OVPN_CA="$(openssl x509 -in ${OVPN_PKI}/ca.crt)"
NL=$'\n'

# Configure VPN service and generate client profiles

umask go=
ls ${OVPN_PKI}/issued \
| sed -e "s/\.\w*$//" \
| while read -r OVPN_ID
do
OVPN_KEY="$(cat ${OVPN_PKI}/private/${OVPN_ID}.key)"
OVPN_CERT="$(openssl x509 -in ${OVPN_PKI}/issued/${OVPN_ID}.crt)"
OVPN_CERT_EXT="$(openssl x509 -in ${OVPN_PKI}/issued/${OVPN_ID}.crt -purpose)"
OVPN_CONF_SERVER="\
user nobody
group nogroup
dev tun
port ${OVPN_PORT}
proto ${OVPN_PROTO}
server ${OVPN_POOL}
topology subnet
client-to-client
client-config-dir ${CCD_DIR}
keepalive 10 60
persist-tun
persist-key
push \"dhcp-option DNS ${OVPN_DNS}\"
push \"dhcp-option DOMAIN ${OVPN_DOMAIN}\"
push \"persist-tun\"
push \"persist-key\"
<dh>${NL}${OVPN_DH}${NL}</dh>"
OVPN_CONF_CLIENT="\
dev tun
nobind
client
remote ${OVPN_SERV} ${OVPN_PORT} ${OVPN_PROTO}
auth-nocache
remote-cert-tls server"
OVPN_CONF_COMMON="\
<tls-crypt>${NL}${OVPN_TC}${NL}</tls-crypt>
<key>${NL}${OVPN_KEY}${NL}</key>
<cert>${NL}${OVPN_CERT}${NL}</cert>
<ca>${NL}${OVPN_CA}${NL}</ca>"
case ${OVPN_CERT_EXT} in
(*"SSL server : Yes"*) cat << EOF > ${OVPN_DIR}/${OVPN_ID}.conf ;;
${OVPN_CONF_SERVER}
${OVPN_CONF_COMMON}
EOF
(*"SSL client : Yes"*) cat << EOF > ${OVPN_DIR}/${OVPN_ID}.ovpn ;;
${OVPN_CONF_CLIENT}
```

```
${OVPN_CONF_COMMON}
EOF
esac
done
```

诸位可以将如上准备好的命令直接复制到终端执行即可，就会的到文件 /etc/openvpn/client.ovpn 成功得到该文件的前提是诸位已经执行过了上篇的操作，这点值得注意哈。

创建 ccd 目录

```
mkdir /etc/openvpn/ccd
```

比如易雾君想给客户端指定 192.168.8.118这个 IP ，那么新增 ccd 配置文件/etc/openvpn/ccd/clien 1，内容如下

```
ifconfig-push 192.168.8.118 255.255.255.0
```

PS: 文件名 client1 一定是你生成客户端证书文件的 COMMON_NAME，不然不会生效。

重启服务

```
/etc/init.d/openvpn restart
```

验证如下：

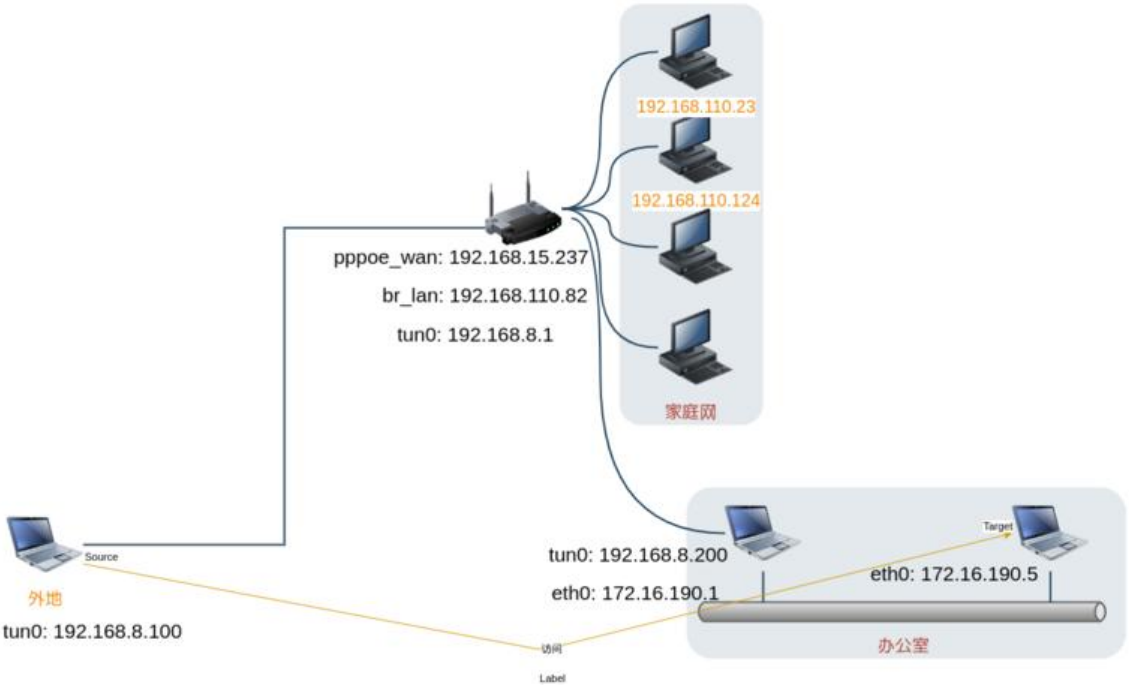
```
root@test01:~# openvpn --config k3-client1.conf &
[1] 11951
root@test01:~# Sat Dec  5 08:48:56 2020 OpenVPN 2.4.7 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [E
POLL] [PKCS11] [MH/PKTINFO] [AEAD] built on Feb 20 2019
Sat Dec  5 08:48:56 2020 library versions: OpenSSL 1.1.1d  10 Sep 2019, LZO 2.10
Sat Dec  5 08:48:56 2020 TCP/UDP: Preserving recently used remote address: [AF_INET]192.168.110.82:1194
Sat Dec  5 08:48:56 2020 UDP link local: (not bound)
Sat Dec  5 08:48:56 2020 UDP link remote: [AF_INET]192.168.110.82:1194
Sat Dec  5 08:48:56 2020 [server] Peer Connection Initiated with [AF_INET]192.168.110.82:1194
Sat Dec  5 08:48:57 2020 TUN/TAP device tun0 opened
Sat Dec  5 08:48:57 2020 /sbin/ip link set dev tun0 up mtu 1500
Sat Dec  5 08:48:57 2020 /sbin/ip addr add dev tun0 192.168.8.118/24 broadcast 192.168.8.255
Sat Dec  5 08:48:57 2020 Initialization Sequence Completed
```

至此该目标就实现了

逆向访问客户端所在网络

易雾君先假设一个场景，一个在国内任意地方接入家庭网关的机器，想要访问办公室里边某台机器所的内部网络，前提是办公室机器也接入了家庭网关，如下：

逆向访问网络模拟图



假设咱们给外地的机器客户端配置命名为 client2，而办公室接入网关机器的配置命名为 client3，命是为了静态分配IP，明确资产。

咱们再设定更细致的需求：

- client2 全局流量走家庭网关
- client3 仅仅允许目标网段为 192.168.110.0/24 的数据走家庭网关
- 最终要 client2 访问到图中的 172.16.190.5

配置 /etc/openvpn/ccd/client2 内容如下，实现全局流量走家庭网关，如果不希望某个网段 172.16.7.0/24 走 VPN 可以设置 net_gateway，自定义 dns 服务器 8.8.8.8：

```
ifconfig-push 192.168.8.100 255.255.255.0
push "redirect-gateway def1 bypass-dhcp"
push "route 172.16.77.0 255.255.255.0 net_gateway"
push "dhcp-option DNS 8.8.8.8"
```

配置 /etc/openvpn/ccd/client3 内容如下，自定义 dns 服务器 114.114.114.114 ：

```
ifconfig-push 192.168.8.100 255.255.255.0
push "route 192.168.110.0 255.255.255.0"
push "dhcp-option DNS 114.114.114.114"
iroute "172.16.190.0 255.255.255.0"
```

PS: client3 中的 iroute 指定的网段，须是 client3 机器能直达访问的网段，这里是 172.16.190.0/24 。

最后在家庭网关服务端配置 /etc/openvpn/server.conf里增加一行

```
route 172.16.190.0 255.255.255.0
```

重启家庭网关服务即可

```
/etc/init.d/openvpn restart
```

至此该目标就实现了，有疑问请在评论区提出，或者前往 易雾山庄论坛 进行提问。

结语

今天易雾君有点高兴，给诸位瞅瞅你们一直在好奇的我家里的设备，那就直接看看它们的真面目吧：

原文链接：家庭网关斐讯 k3 组网拓展篇

原文链接：家庭网关斐讯 k3 组网拓展篇

惊不惊喜，意不意外，就是这么 low ，你们也可以的，哈哈，不过感谢诸位能够耐心看到这里，敬请待下篇《打造更持久的树梅派》。

对了对了，更多精彩不要错过，扫码关注我哟！诸位有心的话请前往“易雾山庄”公众号进行多多点，点得越凶，那我也更得越猛。要不要告哈嘛，都是准备好的干货。