奕锐云安全接入系统

快速配置指南

杭州奕锐电子有限公司

2019-3-10

目　录

一、云端控制台安全组规则

序号	协议	端口	说明
1	TCP	443	WEB 管理端口
2	UDP	25500	PC 端的 VPN 接入端口
3	UDP	500 4500	移动端的 VPN 接入端口
2	TCP	22	SSH 端口：部署、升级、后台维护管理

二、系统 WEB 登陆

WEB 管理地址：https://x.x.x.x （一般情况下，访问地址是系统的 EIP）

WEB 登陆：系统管理员（username：admin password：etapublic）

注意：

1. VPN 镜像的缺省 web 管理端口为 TCP 443 端口，管理员需要在云端控制台的安全组规则的入方向规则中增加 TCP 443（web 管理端口），否则通过外网无法进行 web 管理；

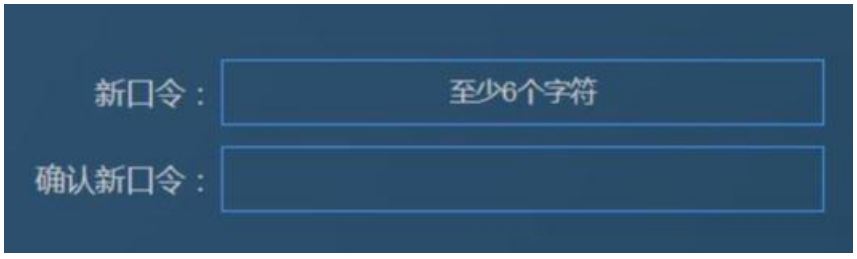
2. 推荐使用谷歌浏览器；

三、系统快速配置实例

3.1 首次登陆 WEB 管理界面

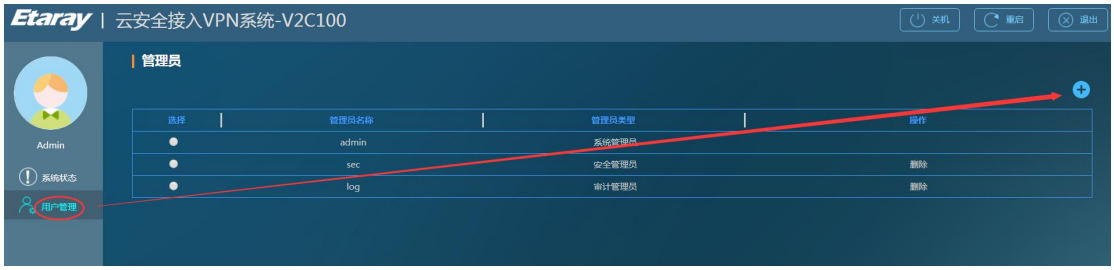
- 登陆 web 管理界面 https://x.x.x.x（EIP 地址）
- 用户名：admin 缺省密码：etapublic

首次登陆界面后，需要修改缺省口令：



3.2 配置安全管理员、审计员

用新口令再次登陆**系统管理员**管理界面，在“用户管理”菜单中，为安全系统增加“安全管理员”与“审计管理员”



创建完成后，退出登录。

3.3 进入安全管理员的管理界面

使用**安全管理员**登陆管理界面（可以看到当前的系统状态、系统基本信息、VPN 服务的启停状态、硬件资源状态）

3.4 配置“系统设置”

菜单“系统设置”中的必填项目：

（1）**服务端外网 IP 地址：**填入映射后对外的 IP 地址（或者可以理解为客户端的连接地址）

（2）**接入端口：**缺省为 25500（管理员可按需更改），协议为 UDP；

（3）**客户端虚拟 IP 池：**该网段地址是分配到客户端的虚拟 IP 池，原则上不与客户端本地网段与云端真实网段冲突（缺省为：192.168.88.1/255.255.255.240)，其中 192.168.88.1 将为 VPN Server 所占用的虚拟地址，则客户端隧道建立成功后获取到的虚拟地址将从 192.168.88.2 开始动态或静态分配。

（4）**WEB 服务端口：**缺省为 TCP 443 端口，管理员可按需更改；

（5）**预共享密钥：**如果系统有移动端接入的场景，需要配置预共享密钥；

（6）**系统激活文件：**用户向厂商提供设备序列号（*在系统状态菜单中可以查看序列号*），而后厂商将根据该序列号生成测试或者正式的 license 文件（文件名：licence.lic)给用户。选择该文件后，提交配置，即可激活 VPN 系统。

注意：不能对该文件重命名再导入。

点击“提交”后，可通过查看“系统状态”菜单中的“系统激活状态”是否激活系统。

3.5 启停 VPN 服务

修改过 2.4 节系统设置后，需要启停 VPN 服务才能生效，先关闭 VPN 服务，然后再开启 VPN 服务，在“系统状态”菜单中，点击 VPN 服务。

VPN 服务启动成功后，显示如下：

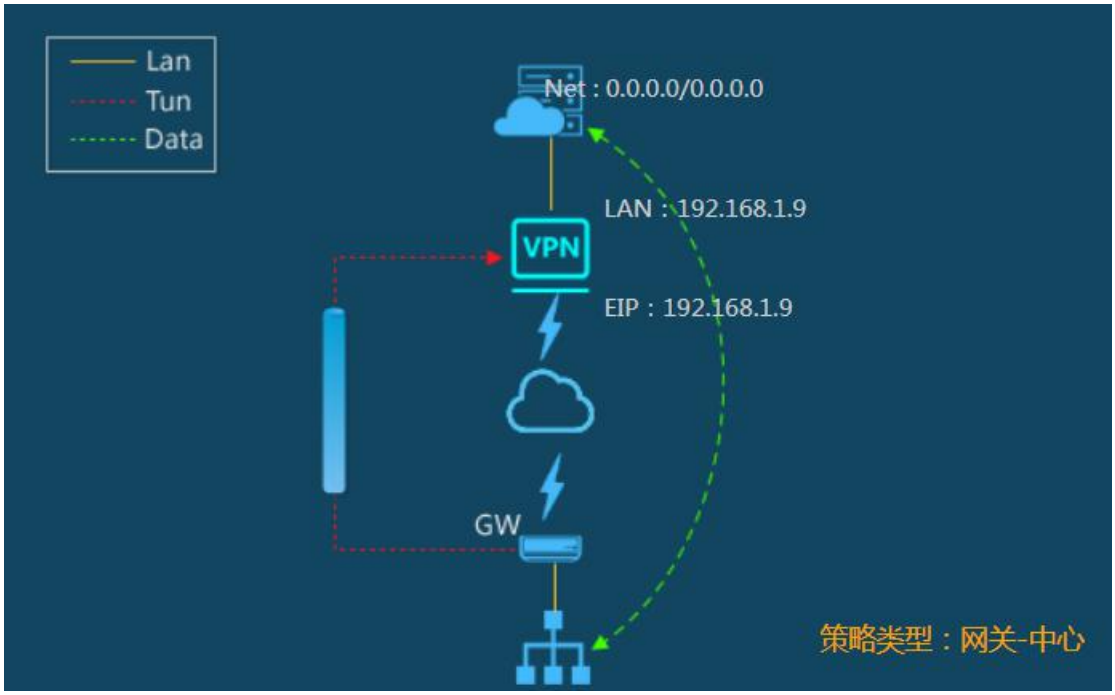
3.6 四类场景分析

第一种：客户端访问中心

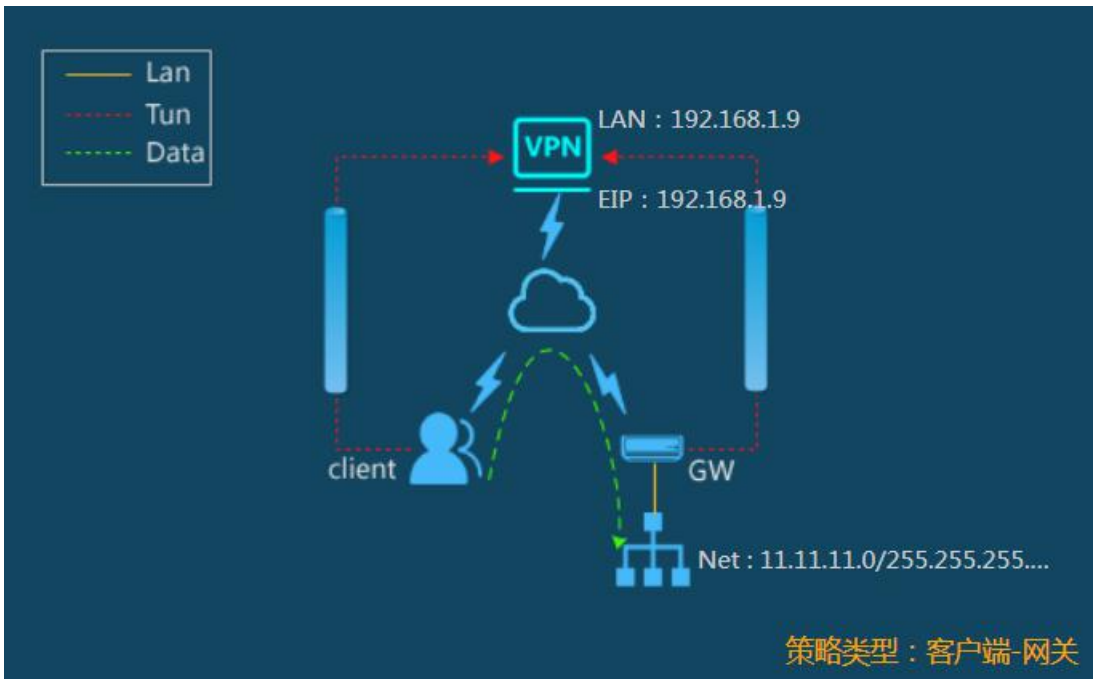
此类场景最为常见，客户端软件通过隧道访问云端内网 IP 资源。

第二种：网关访问中心

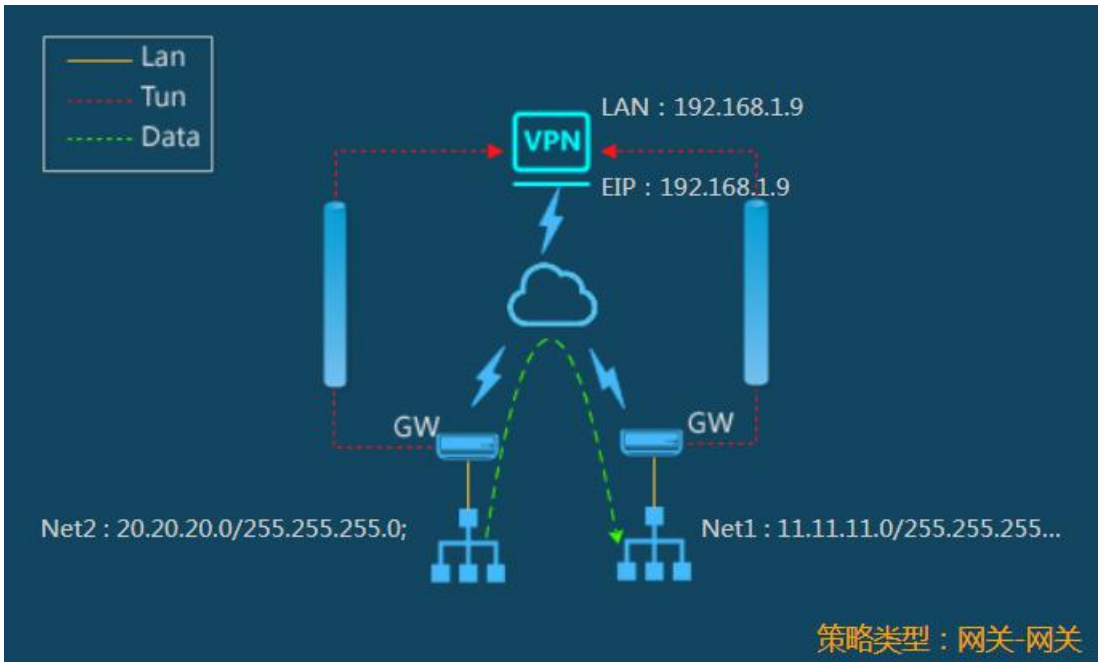
线下允许以网关方式接入云端系统，形成网对网的安全隧道。



第三种：客户端访问网关



第四种：网关访问网关



3.7 配置“隧道设置->客户端”

客户端开户过程：用户名、密码，可指定虚拟 IP 地址。同时也允许批量添加用户，如下图所示：

在“动作”设置中点击“允许”

3.8 配置“隧道设置->网关”

某些场景中，在线下可以通过网关方式接入系统，

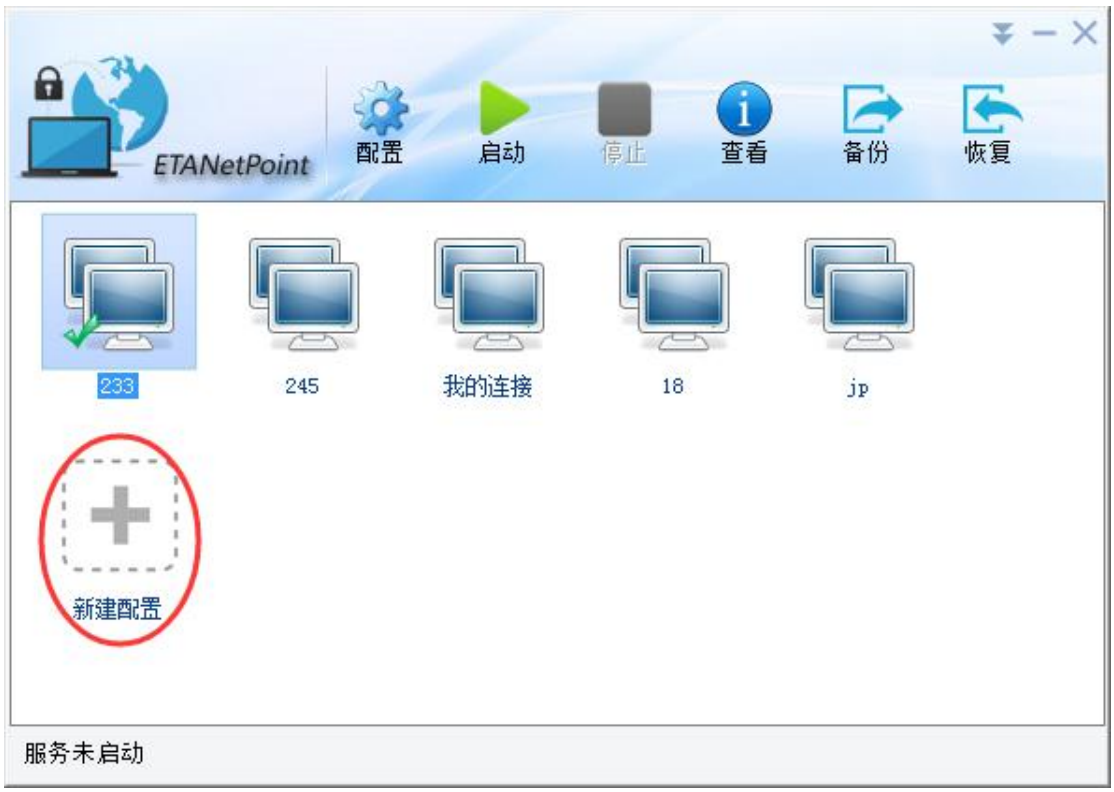
3.9 配置“隧道设置->访问策略”

在“访问策略”中，根据用户的使用场景（参考 3.6 节）设置访问策略类型，选定客户端用户或者网关，输入访问的网段等，如下图所示：

访问策略设置要素	详细
模式选择	（1）软件客户端->云端 VPN 保护网段； （2）硬件网关->云端 VPN 保护网段； （3）软件客户端->硬件网关保护网段； （4）硬件网关<->硬件网关；
选择谁要通过 VPN 访问	（1）软件客户端 （2）硬件网关
选择需要访问什么网段	自定义网段规则，以下都是正常写法： 192.168.11.0/255.255.255.0 192.168.11.6/255.255.255.255

四、windows 客户端配置

下文以 windows 客户端为例，安装好客户端后，新建连接，如下图所示：



配置界面如下，需要输入连接标签、接入地址、接入端口、选择认证方式、输入与选定的认证方式相关的认证信息：

系统缺省是用户名、口令方式，如果需要其他认证方式，则需要在后台 web 管理上调整相关配置，如下图所示：

客户端中的“接入端口”一般有两种情况：

（1）“接入端口”与“2.4 节”中配置的“接入端口”保持一致；

（2）如果在云环境中使用了负载均衡产品，“接入端口”与负载均衡的外部映射端口保持一致；

五、手机客户端配置

5.1 Android 系统

打开设置，选择“网络和连接”中的“其他连接方式”->“VPN”->“添加 VPN”->“IPSec Xauth PSK”，填写名称、服务器 IP、预共享密钥（参考 3.4 节中的配置），保存设置，然后输入用户名、密码即可连接到 VPN 服务器。

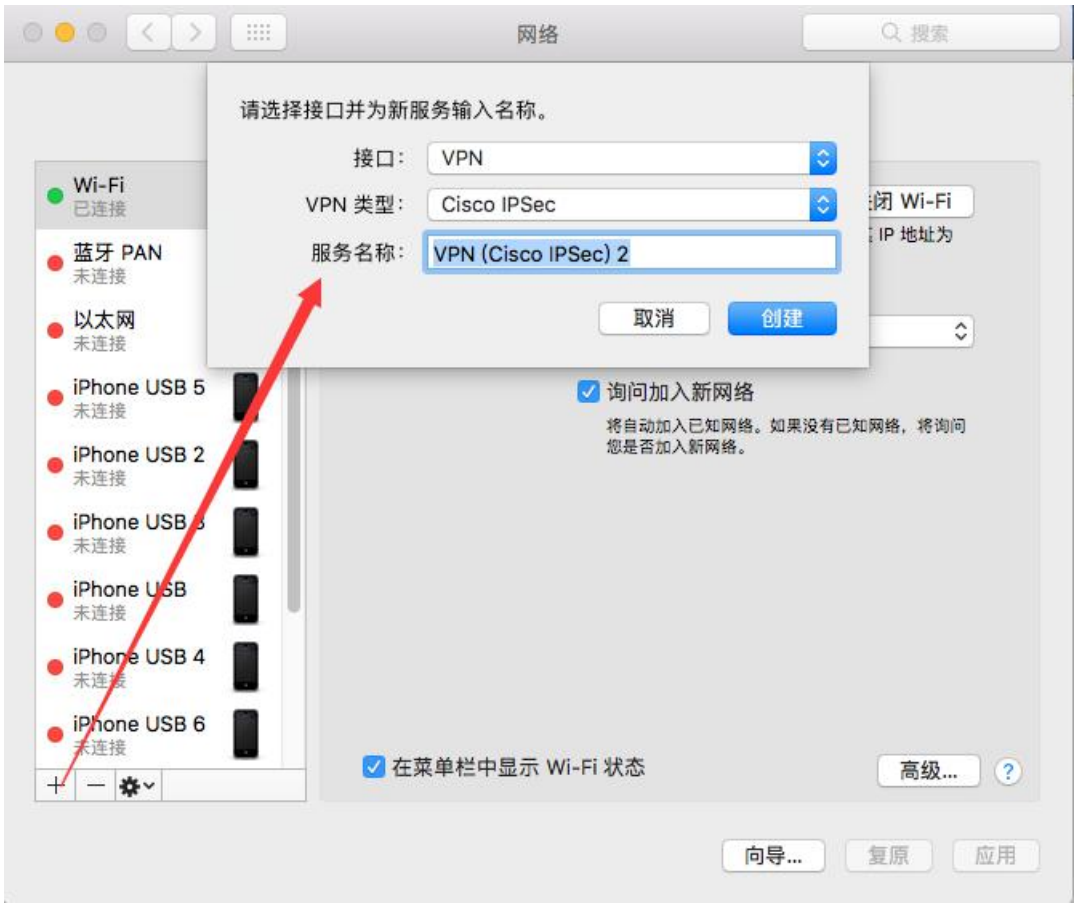
5.2 IOS 系统

打开设置->通用->VPN->添加 VPN 配置->选择 IPSec 类型并填写描述、服务器、账户、密码、密钥（预共享密钥），完成后打开 VPN 状态，设备连接。

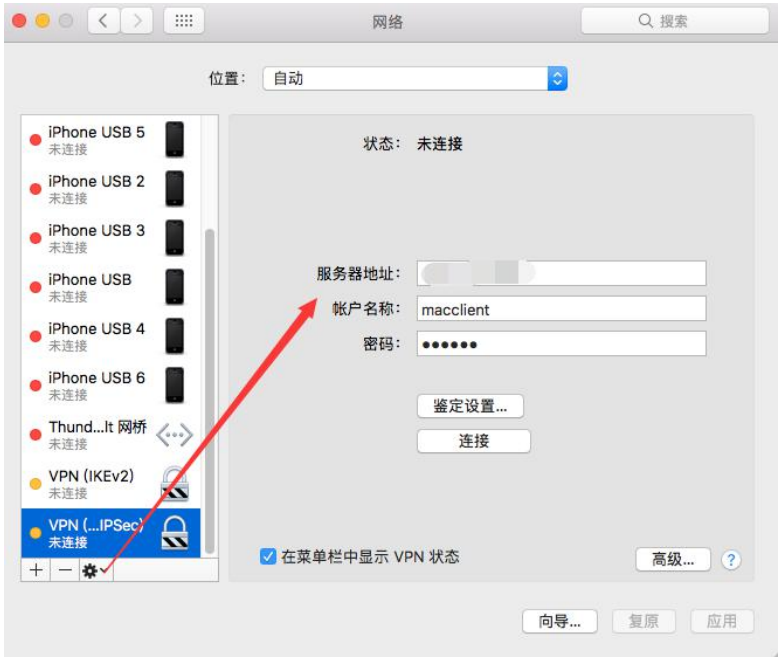
六、MAC OSx

6.1 MAC OSx 系统自带 APP

“打开网络偏好设置 -> 点击”+”号，添加新的网络连接 -> 接口选择 VPN -> VPN 类型选择 Cisco IPSec。

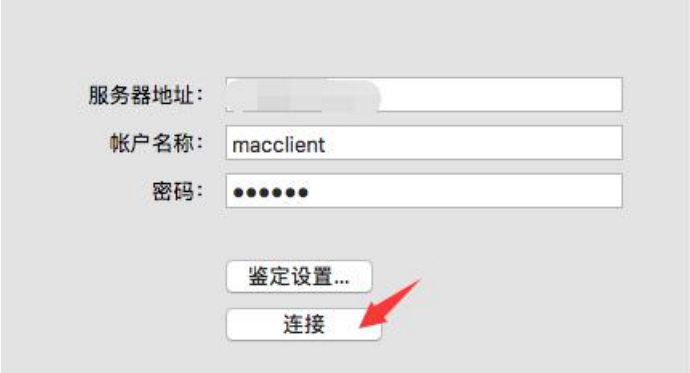


建立好连接之后，点击该连接的“设置”：



输入“服务器地址”、“账户名称”、“密码”，同时在“鉴定设置”中设置“预共享密钥”：

最后点击“连接”即可建立隧道。



6.2 MAC OSx 系统专用 APP

仅支持“用户名、口令”方式认证，配置要素与 windows 客户端

一致，参考第四节。

七、Linux 系统

Linux 系统支持 Centos、Ubuntu、Redhat 等不同版本的系统，甚至是一些专用 linux 系统，包括 ARM Linux。非标准的 Linux 系统需要提供编译环境才能编译出对应的 Linux 客户端。

按照以下步骤执行 Linux 客户端程序：

7.1 检查虚拟网络设备

查看是否内核支持虚拟网络设备：

ll /dev/net/tun ，查看结果如下图所示：

```
[root@localhost ~]# ll /dev/net/tun
crw-rw-rw-. 1 root root 10, 200 12?28 08:57 /dev/net/tun
```

✓ 如果有 tun 设备，说明该系统内核支持虚拟网络设备（跳至 2.1 节）

✓ 如果没有 tun 设备，请查收是否有 tun 驱动（跳至 1.2 节）

7.2 检查 tun 驱动

执行 modprobe tun，执行完成后，再执行 lsmod |grep tun

```
[root@localhost ~]# lsmod |grep tun
tun                    16934  2 vhost_net
```

如果看到 tun 驱动已经加载成功，可跳至 2.1 节。

7.3 无 tun 驱动

如果以上两步均执行失败，则需要客户联系奕锐电子技术人员并提供 linux 系统对应的内核源码来编译出 tun.ko，或者进入定制内核环节。

7.4 执行

确认执行该命令的时候，必须有 root 权限（1. root 账户可直接执行；2.或者加 sudo 可以执行）

命令：sudo ./ETANet_Client -l VPN 外网 IP 地址:VPN 端口 -U VPN 账户名 -P 账户密码

如：sudo ./ETANet_Client -l x.x.x.x:25500 -U test -P 123456

7.5 查看执行结果

ifconfig 查看是否有 ETANetTAP 网卡，并获得了 VPN 网的虚拟 IP 地址。