金箍棒
Service Digital

IPsec VPN

V2.0 版本 操作指南

西安金箍棒信息技术服务有限公司

西安市碑林区雁塔北路 67 号红锋商务大厦 4 层

目 录

一、商品说明.....1

1、版本说明.....1

2、安全加固.....1

二、操作指南.....1

1、VPN 信息.....1

2、安全组开放相应的 UDP 端口 500 和 4500.....1

3、登录操作系统修改 ipsec 配置文件.....2

4、重启 VPN 服务进程.....4

5、Windows 客户端配置.....4

6、Linux 客户端链接.....6

7、IOS 手机客户端链接.....9

8、安卓手机客户端链接.....13

9、链接使用.....13

10、用户管理.....14

11、环境说明.....18

12、服务的启动以及关闭.....18

13、常规错误如何排查.....19

三、技术支持.....20

1、售后服务.....20

2、服务范围.....20

一、商品说明

1、版本说明

此镜像为 IPsec VPN 镜像 V2.0 版本，系统：Aliyun（兼容 CentOS），更新时间 2024 年 8 月。您可以一键快速搭建自己的 IPsec VPN 服务器。支持 IPsec/L2TP 协议。

2、安全加固

为进一步提升云服务的安全性，我公司对镜像产品实施了全面的安全加固，共计完成 88 项基线加固措施。这些精细化的安全改进，不仅确保我们的镜像产品严格符合等保 2.0 的安全标准，更在防御外部攻击、内部漏洞修复、数据加密保护等多个安全维度上实现了显著增强，为您的数据的安全存储与业务的平稳运行提供坚实保障。选择我们的镜像产品，意味着您将获得一个经过深度安全加固、符合高标准安全要求的云端解决方案，让您的业务在安全的护航下稳健运行。

如您的业务环境有其他安全需求，请与客服联系，我们可为您提供一对一定制服务。

二、操作指南

1、VPN 信息

包含四部分，公网 IP 地址、PSK、用户名、密码。

Server IP: VPN 服务端 IP 地址（阿里云公网 IP 地址）

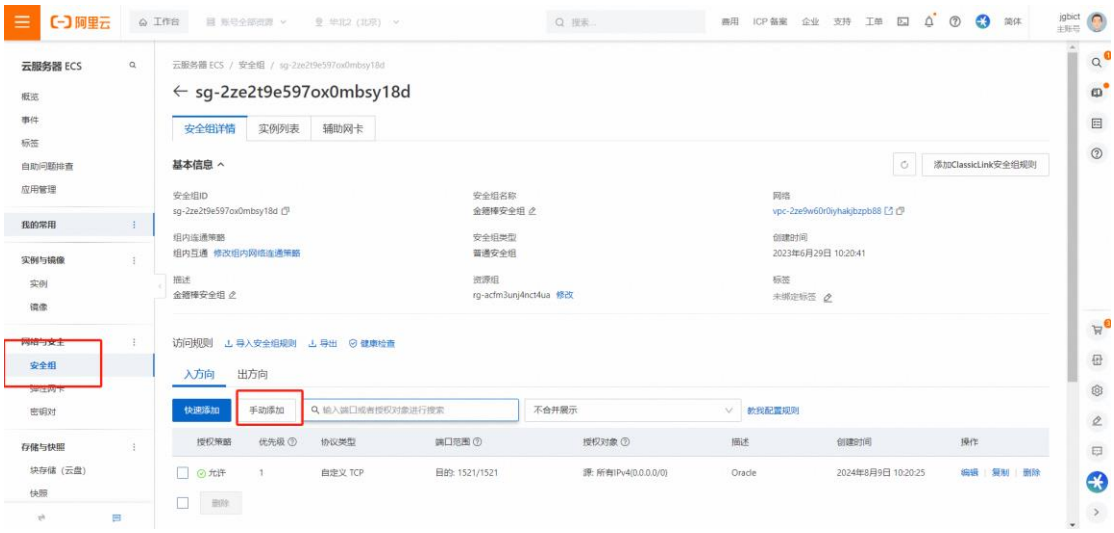
IPsec PSK: BZyAmPwijTHyfU4DyBYN

Username: vpnuser

Password: Y23KKbnNyBd56HJq

2、安全组开放相应的 UDP 端口 500 和 4500

点击阿里云 ecs，点击安全组，入方向，手动添加

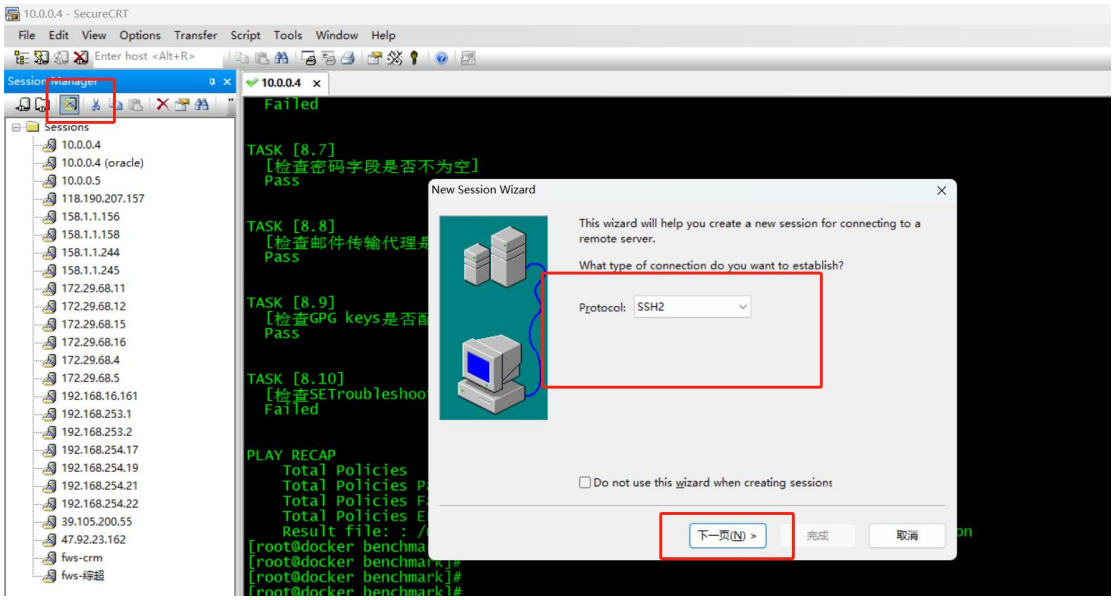


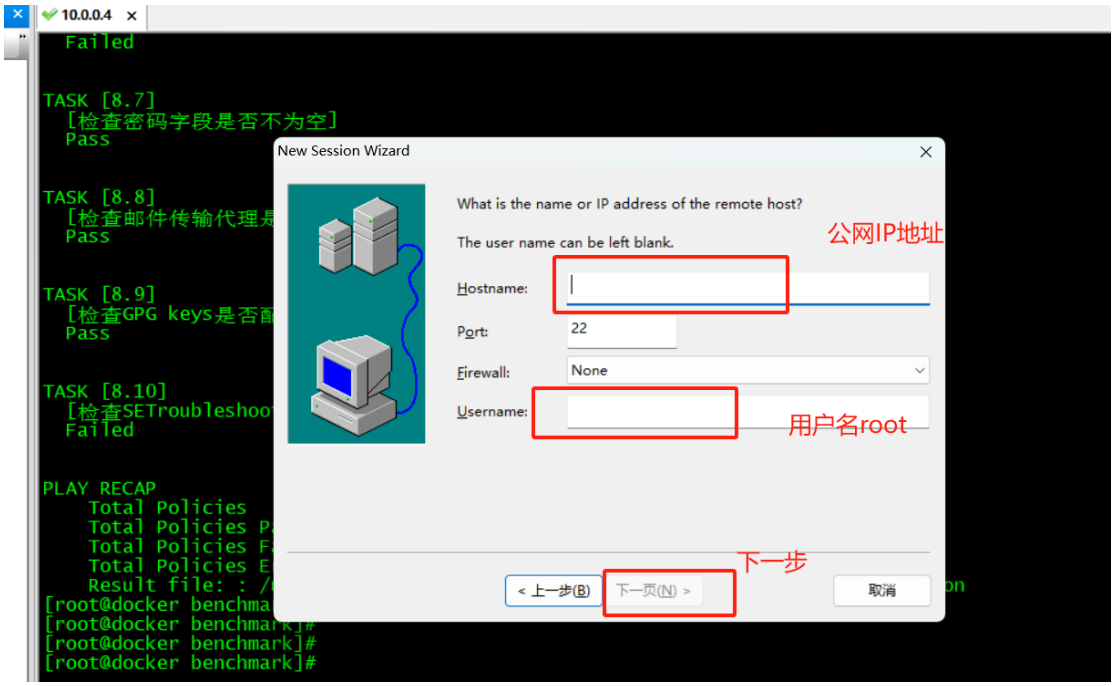
允许 UDP、端口 500 和 4500、允许所有 IPv4，保存即可。

3、登录操作系统修改 ipsec 配置文件

使用（Crt、putty、xshell 等远程工具进行链接）

选择 ssh 协议、输入公网地址以及账户名密码，进行远程链接。





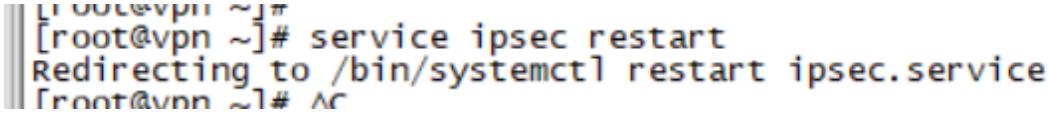
双击链接即可

修改 VPN 配置文件 IP 地址为 vpn 服务端 ECS 公网 IP 地址

vi /etc/ipsec.conf

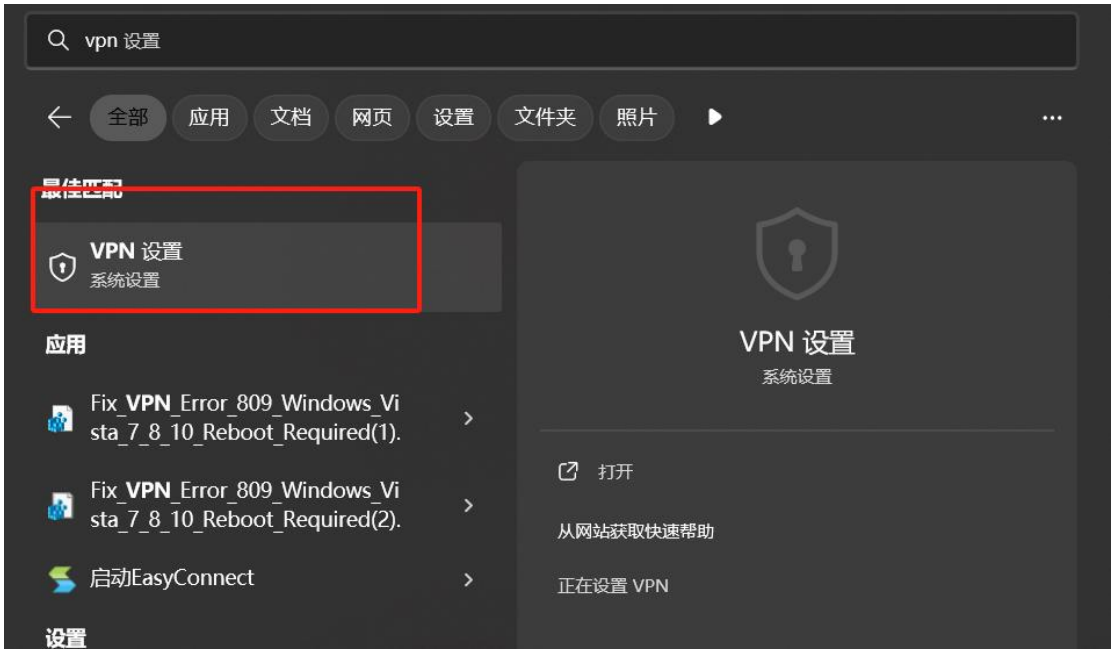
4、重启 VPN 服务进程

service ipsec restart



5、Windows 客户端配置

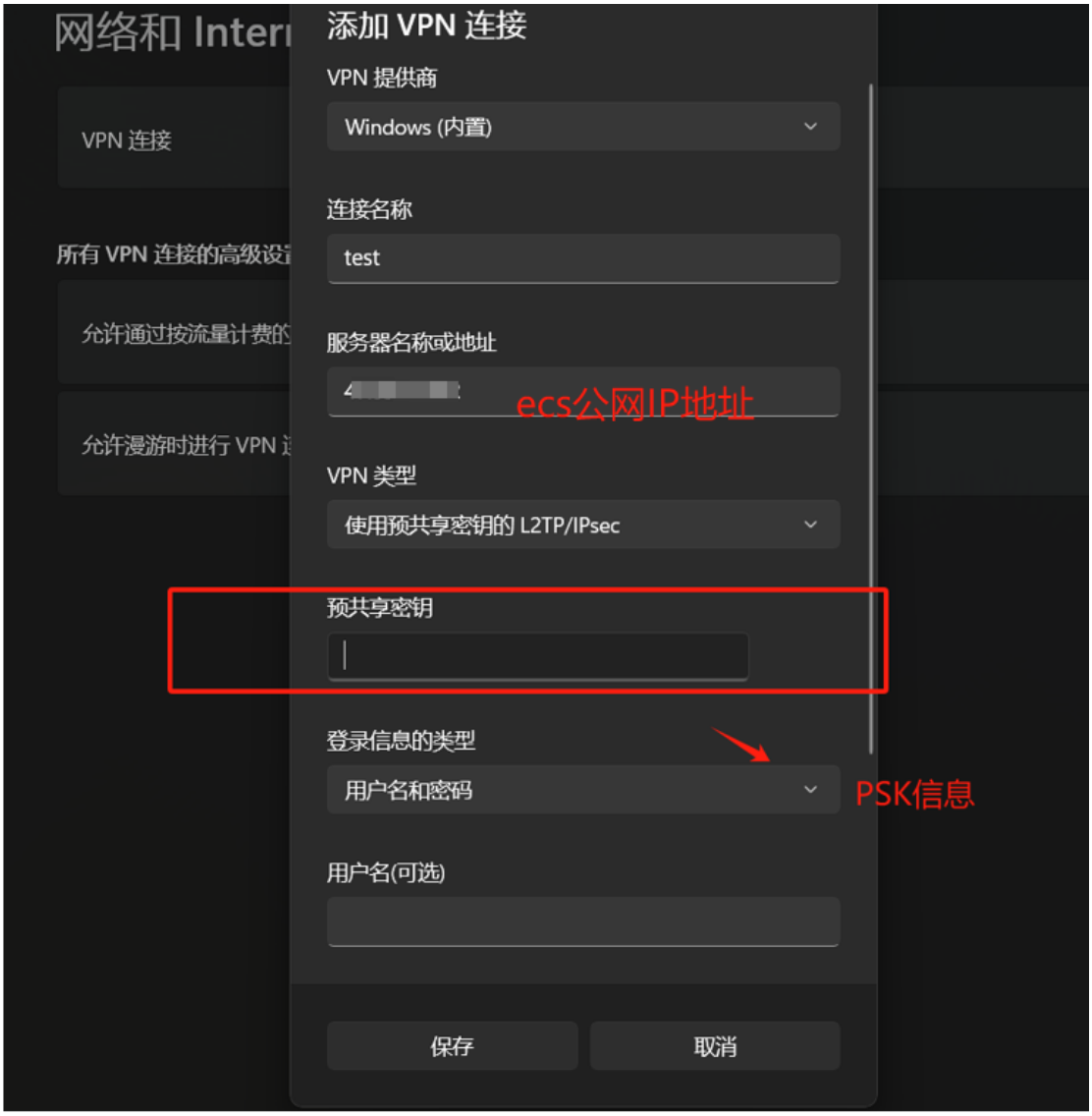
点击开始按钮进行搜索 VPN,到达 VPN 配置按钮（不同的系统或许有差异，以 win11 为类）。

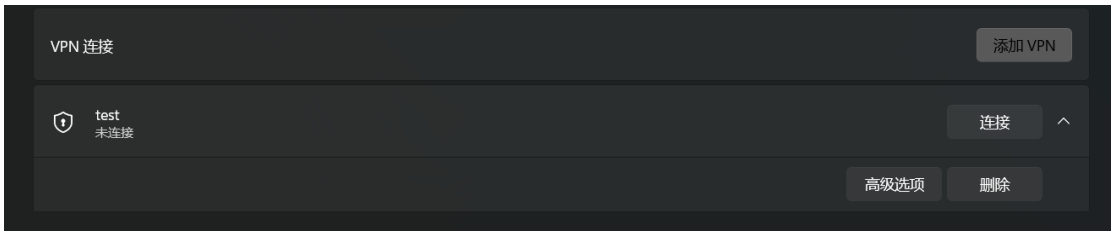


（VPN 登录信息在公告页面上面）

添加 vpn 链接

公网信息，PSK 信息输入，然后输入账户名密码

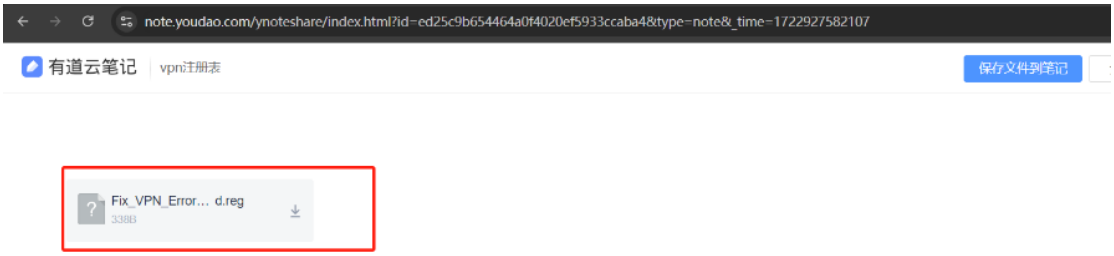




Windows 需要修改注册表信息，并且需要重启客户端操作系统。

vpn 注册表链接如下，

http://note.youdao.com/noteshare?id=ed25c9b654464a0f4020ef5933ccaba4&sub=37D5005876B141F8A94CF9914EB291AA



点击进行下载，然后双击运行，运行完成之后，进行重启 window 操作。

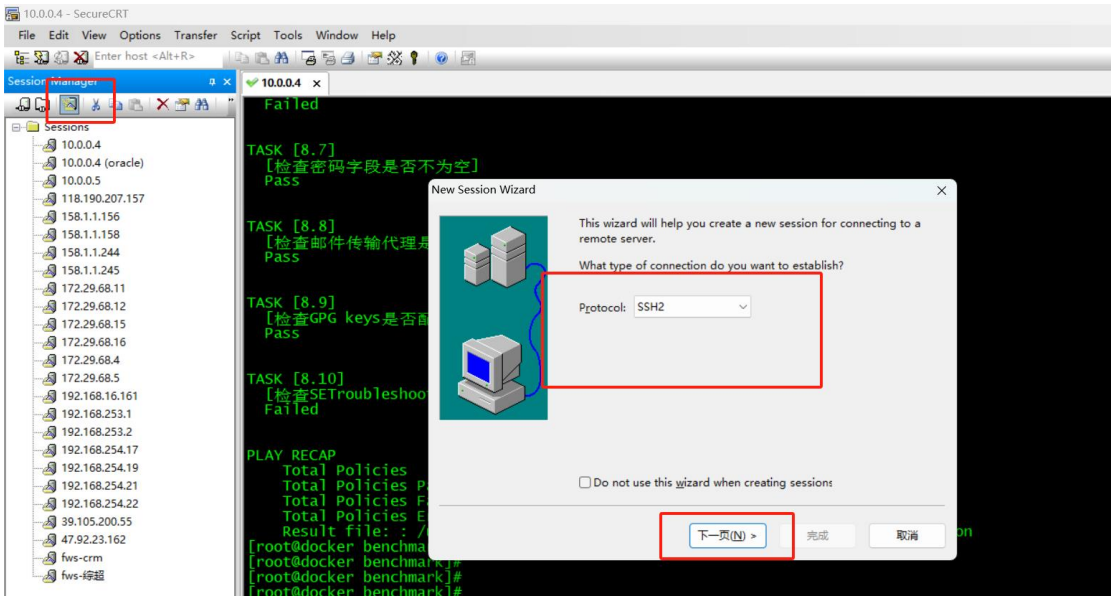
然后进行客户端链接

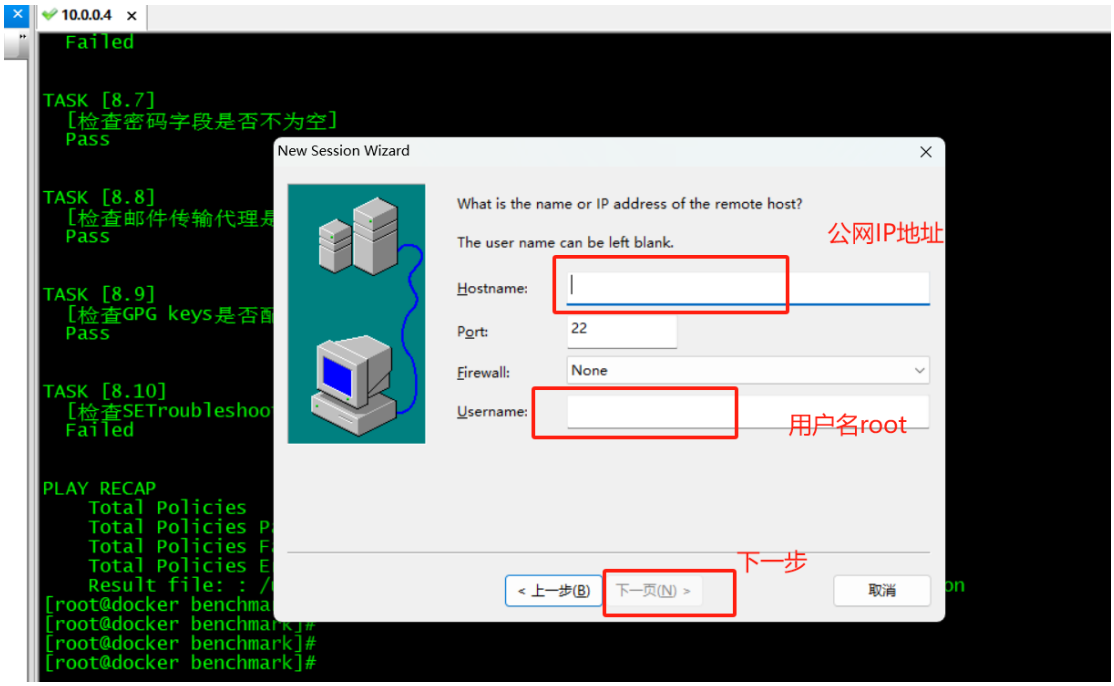
6、Linux 客户端链接

CentOS 需要安装图形界面，然后在进行如下操作。

使用（Crt、putty、xshell 等远程工具进行链接）

选择 ssh 协议、输入公网地址以及账户名密码，进行远程链接



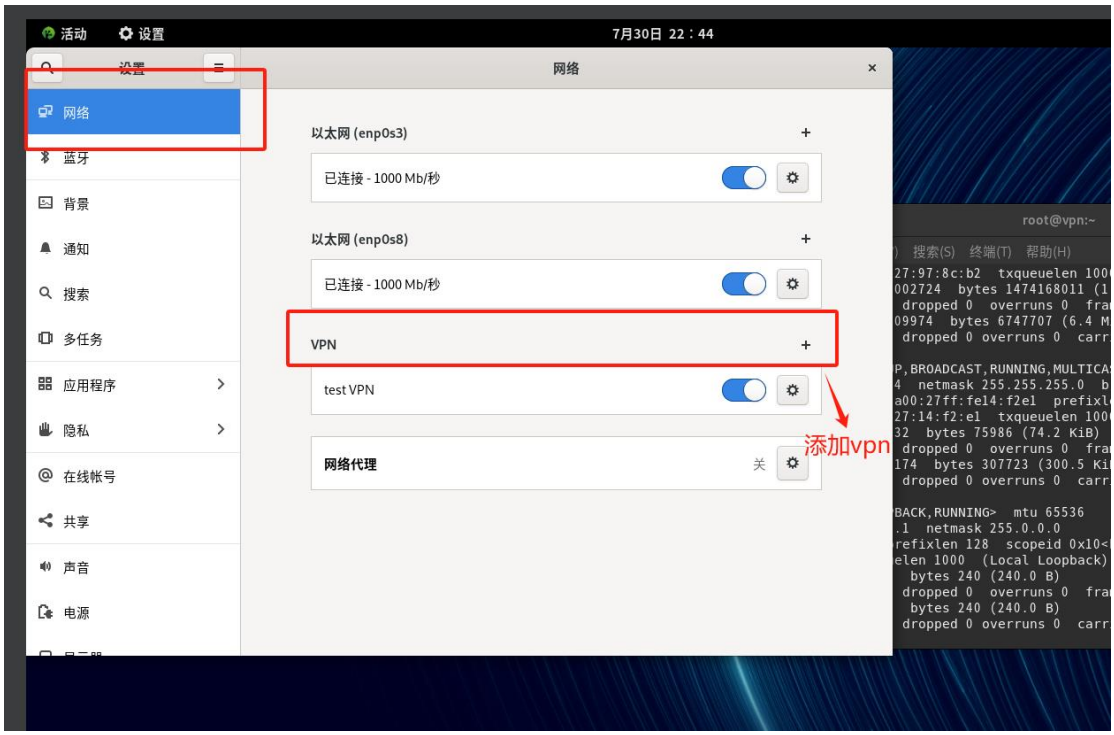


双击链接即可执行如下命令

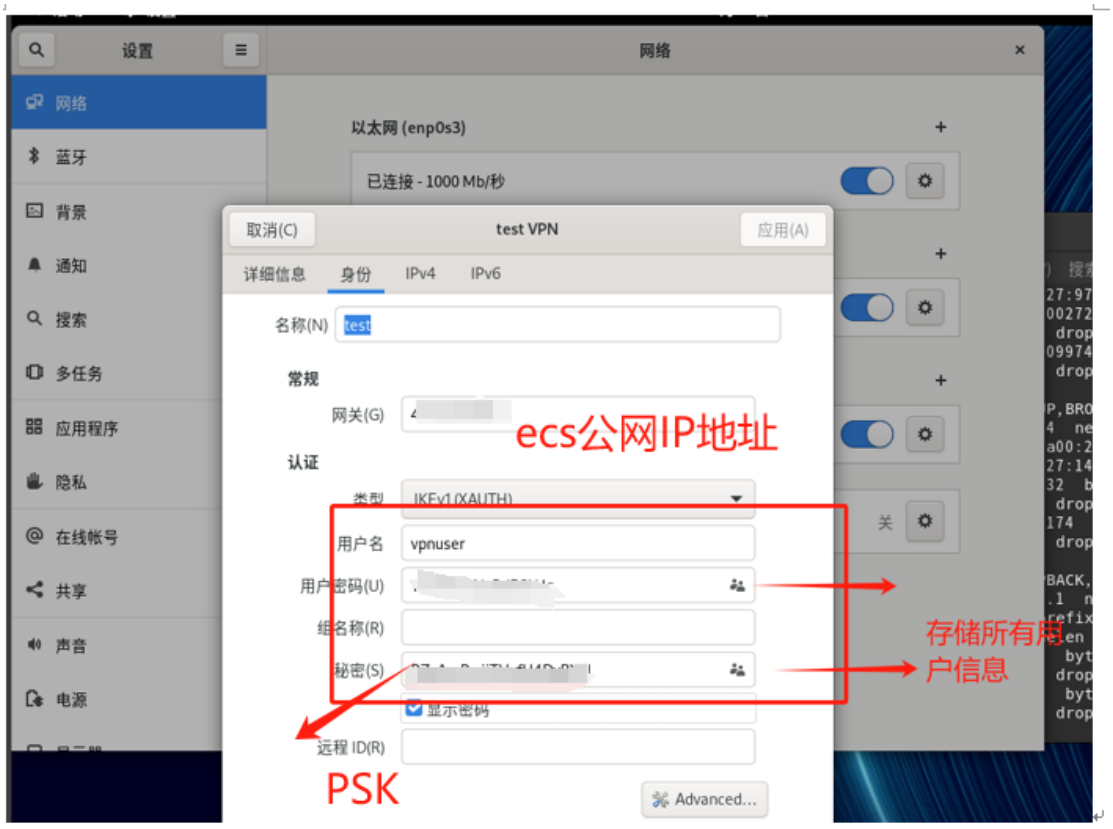
yum install epel-release

yum --enablerepo=epel install NetworkManager-libreswan-gnome

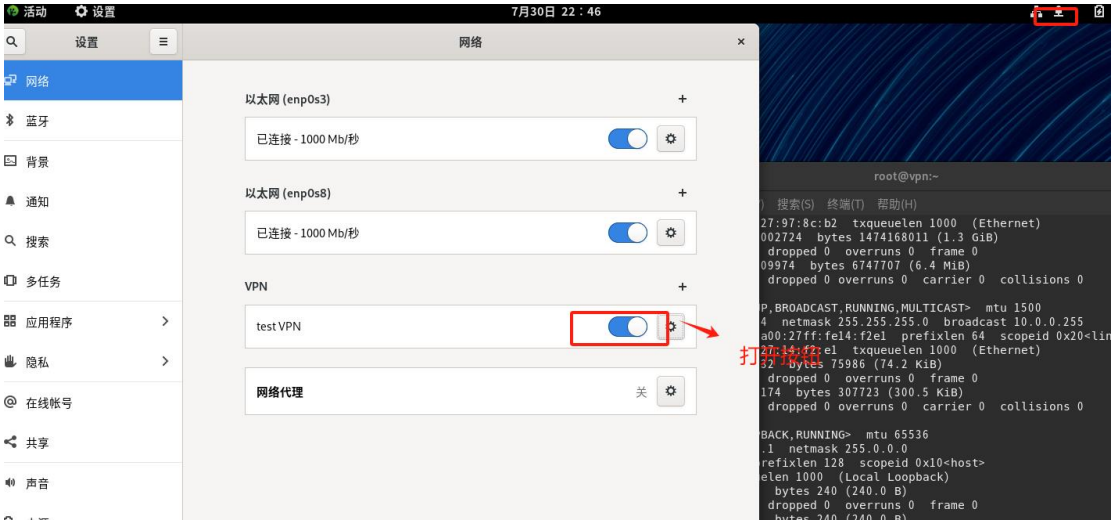
打开主机，然后点击设置



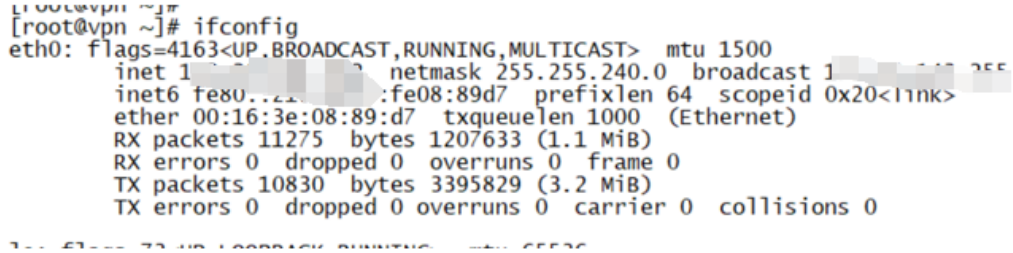
配置链接信息



打开链接信息



测试连通性



7、IOS 手机客户端链接

点击设置、下一步通用、通用里面的 VPN 与设备管理。


设置
通用
iPhone 储存空间
后台 App 刷新
日期与时间
键盘
字体
语言与地区
词典
VPN与设备管理
法律与监管
传输或还原 iPhone
关机

点击添加 VPN 链接

类型选择 L2TP，输入 IP 地址、账户、用户名、密码，密钥完成链接即可


取消
添加配置
完成
类型
L2TP
描述
必填
服务器
必填
账户
必填
RSA SecurID
密码
每次均询问
密钥
必填
发送所有流量
服务器：公网IP
账户：用户名
密码：密码
密码：共享密钥对
点击完成，链接即可。
代理
关闭
手动
自动

8、安卓手机客户端链接

由于 VPN 使用较老的 L2TP 协议，各个安卓厂家处于安全考虑已经对此协议不支持，或者已经屏蔽，无法使用。

9、链接使用

使用 ping 协议，以及 ssh 链接 VPN 局域网 IP 地址

查看服务端 VPN 局域网私有 IP 地址

ifconfig(Linux 客户端直接可以访问阿里的内网地址，windows 客户端需要查看 VPN 分配 192.168.42.0 网段的局域网地址，使用 ssh 192.168.42.2 进行访问)

```
[root@vpn ~]# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.28.141.212  netmask 255.255.240.0  broadcast 172.28.143.255
        inet6 fe80::216:3eff:fe08:89d7  prefixlen 64  scopeid 0x20<link>
        ether 00:16:3e:08:89:d7  txqueuelen 1000  (Ethernet)
        RX packets 11275  bytes 1207633 (1.1 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 10830  bytes 3395829 (3.2 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

ping 172.28.141.212

也可进行 ssh 远程链接 VPN 服务器，远程完成之后可进行业务使用。

ssh 172.28.141.212

```
[root@vpn ~]#
[root@vpn ~]# ping 172.28.141.212
PING 172.28.141.212 (172.28.141.212) 56(84) bytes of data.
64 bytes from 172.28.141.212: icmp_seq=1 ttl=64 time=2160 ms
64 bytes from 172.28.141.212: icmp_seq=2 ttl=64 time=1125 ms
64 bytes from 172.28.141.212: icmp_seq=3 ttl=64 time=1009 ms
64 bytes from 172.28.141.212: icmp_seq=4 ttl=64 time=51.0 ms
^Z
[3]+  已停止               ping 172.28.141.212
[root@vpn ~]# ssh 172.28.141.212
root@172.28.141.212's password:
```

10、用户管理

查看 VPN 用户

more /etc/ppp/chap-secrets

"vpnuser" l2tpd "Y23KKbnNyBd56HJq" *

```
done:

[root@vpn ~]# more /etc/ppp/chap-secrets
"vpnuser" l2tpd "Y23KKbnNyBd56HJq" *
[root@vpn ~]#
```

查看共享 PSK

more /etc/ipsec.secrets

[root@vpn ~]# more /etc/ipsec.secrets

%any %any : PSK "BZyAmPwijTHyfU4DyBYN"

一般不建议修改 PSK,建议保留。

更新 PSK

如果要更换一个新的 PSK，可以编辑此文件。不要在值中使用这些字符：\ " ，

vi /etc/ipsec.secrets

```
[root@vpn ~]#
[root@vpn ~]# vi /etc/ipsec.secrets
%any  %any  : PSK "BZyAmPwijTHyfU4DyBYN"
~
~
~
```

完成后必须重启服务：

service ipsec restart

service xl2tpd restart

添加新 VPN 链接用户并且设置密码 test 为用户名，密码为 test123

addvpnuser.sh 'test' 'test123'

```
[root@vpn ~]# addvpnuser.sh 'test' 'test123'

Welcome! Use this script to add or update a VPN user account for both
IPsec/L2TP and IPsec/XAuth ("Cisco IPsec") modes.

If the username you specify already exists, it will be updated
with the new password. Otherwise, a new VPN user will be added.

================================================

VPN user to add or update:

Username: test
Password: test123

Write these down. You'll need them to connect!

VPN client setup: https://vpnsetup.net/clients

================================================

Do you want to continue? [Y/n] y

Adding or updating VPN user...

Done!

Note: All VPN users will share the same IPsec PSK.
      If you forgot the PSK, check /etc/ipsec.secrets.
```

账 号 测 试 链 接 ， 链 接 成 功


09:05
5G
VPN
teat
编辑
类型
L2TP
服务器
39.105.200.55
账户
test
地址
192.168.42.10
连接时间
0:12
删除 VPN

更改 VPN 用户密码，test1234 为新密码

addvpnuser.sh 'test' 'test1234'

```
[root@vpn ~]#
[root@vpn ~]# addvpnuser.sh 'test'  'test1234'

Welcome! Use this script to add or update a VPN user account for both
IPsec/L2TP and IPsec/XAuth ("Cisco IPsec") modes.

If the username you specify already exists, it will be updated
with the new password. Otherwise, a new VPN user will be added.

================================================

VPN user to add or update:

Username: test
Password: test1234

Write these down. You'll need them to connect!

VPN client setup: https://vpnsetup.net/clients

================================================

Do you want to continue? [Y/n] Y

Adding or updating VPN user...

Done!

Note: All VPN users will share the same IPsec PSK.
      If you forgot the PSK, check /etc/ipsec.secrets.
```

删除指定 VPN 用户

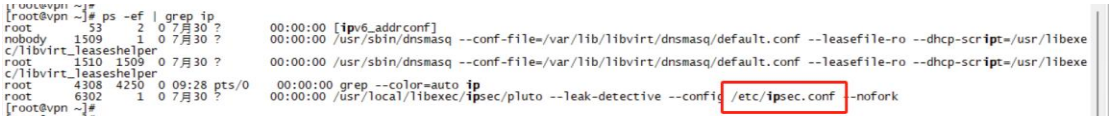
delvpnuser.sh 'test'

```
[root@vpn ~]# delvpnuser.sh 'test'

Welcome! Use this script to delete a VPN user account for both
IPsec/L2TP and IPsec/XAuth ("Cisco IPsec") modes.

================================================

VPN user to delete:

Username: test

================================================

Do you want to continue? [Y/n] Y

Deleting VPN user...

Done!
```

11、环境说明

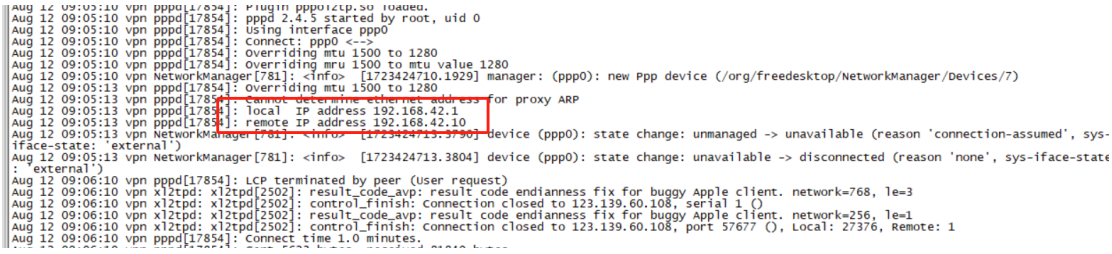
服务配置文件/etc/ipsec.conf

如何查看服务是否启动： ps -ef | grep ip



VPN 日志会记录到系统日志中/var/log/messages

tail -f /var/log/messages



12、服务的启动以及关闭

重启服务命令

service ipsec restart

启动服务命令

service ipsec start

关闭服务命令

service ipsec stop

查看服务状态

service ipsec status

13、常规错误如何排查

首先，重启 VPN 服务器上的相关服务：

service ipsec restart

service xl2tpd restart

然后重启你的 VPN 客户端设备，并重试连接。如果仍然无法连接，可以尝试删除并重新创建 VPN 连接。请确保输入了正确的 VPN 服务器地址和 VPN 登录凭证。

确认服务器 EC2/GCE 是否打开 安全组 UDP 端口 500 和 4500

检查 IPsec VPN 服务器状态：

ipsec status

```
[root@vpn log]# ipsec status
000 using kernel interface: xfrm
000
000 interface lo UDP [::1]:4500
000 interface lo UDP [::1]:500
000 interface lo UDP 127.0.0.1:4500
000 interface lo UDP 127.0.0.1:500
000 interface eth0 UDP 172.20.10.53:4500
000 interface eth0 UDP 172.20.10.53:500
000 interface virbr0 UDP 192.168.122.1:4500
000 interface virbr0 UDP 192.168.122.1:500
000
000 fips mode=disabled;
000 SElinux=disabled
000 seccomp=unsupported
000
000 config setup options:
000
000 configdir=/etc, configfile=/etc/ipsec.conf, secrets=/etc/ipsec.secrets, ipsecdir=/etc/ipsec.d
000 nssdir=/etc/ipsec.d, dumpdir=/run/pluto, statsbin=unset
000 sbindir=/usr/local/sbin, libexecdir=/usr/local/libexec/ipsec
000 pluto_version=4.14, pluto_vendorid=OE-Libreswan-4.14, audit-log=yes
000 nhelpers=-1, uniqueids=no, dnssec-enable=no, logappend=yes, logip=yes, shuntlifetime=900s, xfrmlifetime=30s
000 ddos-cookies-threshold=25000, ddos-max-halfopen=50000, ddos-mode=auto, ikev1-policy=accept
000 ikebuf=0, msg_errqueue=yes, crl-strict=no, crlcheckinterval=0, listen=<any>, nflog-all=0
000 ocsp-enable=no, ocsp-strict=no, ocsp-timeout=2, ocsp-uri=<unset>
000 ocsp-trust-name=<unset>
000 ocsp-cache-size=1000, ocsp-cache-min-age=3600, ocsp-cache-max-age=86400, ocsp-method=get
000 global-redirect=no, global-redirect-to=<unset>
000 secctx-attr-type=32001
000 debug:
000
000 nat-traversal=yes, keep-alive=20, nat-ikeport=4500
000 virtual-private (%priv):
000 - allowed subnets: 10.0.0.0/8, 192.168.0.0/16, 172.16.0.0/12
000 - excluded subnets: 192.168.42.0/24, 192.168.43.0/24
```

查看当前已建立的 VPN 连接：

ipsec trafficstatus

```
[root@vpn log]#
[root@vpn log]# ipsec trafficstatus
006 #40: "l2tp-psk"[32] 113.201.132.177, type=ESP, add_time=1723430916, inBytes=1900, outBytes=2356, maxBytes=2^63B, id='10.179.19.136'
[root@vpn log]#
```

查看链接日志

VPN 日志会记录到系统日志中/var/log/messages

tail -f /var/log/messages

```
Aug 12 09:05:10 vpn pppd[17854]: pppd 2.4.5 started by root, uid 0
Aug 12 09:05:10 vpn pppd[17854]: Using interface ppp0
Aug 12 09:05:10 vpn pppd[17854]: Connect: ppp0 <-->
Aug 12 09:05:10 vpn pppd[17854]: Overriding mtu 1500 to 1280
Aug 12 09:05:10 vpn pppd[17854]: Overriding mru 1500 to mtu value 1280
Aug 12 09:05:10 vpn NetworkManager[781]: <info>  [1723424710.1929] manager: (ppp0): new Ppp device (/org/freedesktop/NetworkManager/Devices/7)
Aug 12 09:05:13 vpn pppd[17854]: Overriding mtu 1500 to 1280
Aug 12 09:05:13 vpn pppd[17854]: Cannot determine ethernet address for proxy ARP
Aug 12 09:05:13 vpn pppd[17854]: local  IP address 192.168.42.1
Aug 12 09:05:13 vpn pppd[17854]: remote IP address 192.168.42.10
Aug 12 09:05:13 vpn NetworkManager[781]: <info>  [1723424713.3796] device (ppp0): state change: unmanaged -> unavailable (reason 'connection-assumed', sys-
iface-state: 'external')
Aug 12 09:05:13 vpn NetworkManager[781]: <info>  [1723424713.3804] device (ppp0): state change: unavailable -> disconnected (reason 'none', sys-iface-state
: 'external')
Aug 12 09:06:10 vpn pppd[17854]: LCP terminated by peer (User request)
Aug 12 09:06:10 vpn xl2tpd: xl2tpd[2502]: result_code_avp: result code endianness fix for buggy Apple client. network=768, le=3
Aug 12 09:06:10 vpn xl2tpd: xl2tpd[2502]: control_finish: Connection closed to 123.139.60.108, serial 1 ()
Aug 12 09:06:10 vpn xl2tpd: xl2tpd[2502]: result_code_avp: result code endianness fix for buggy Apple client. network=256, le=1
Aug 12 09:06:10 vpn xl2tpd: xl2tpd[2502]: control_finish: Connection closed to 123.139.60.108, port 57677 (), Local: 27376, Remote: 1
Aug 12 09:06:10 vpn pppd[17854]: Connect time 1.0 minutes.
```

三、技术支持

1、售后服务

（1）您可以第一时间在阿里云市场联系售后获取服务。

（2）服务时间：09:00-18:00（紧急情况请打电话）

（3）服务热线：18091296777、4009030002 转 15953

（4）服务邮箱：22958288@qq.com

2、服务范围

远程支持：如果您在使用过程中遇到技术操作问题，请及时联系客服，我们的工程师可远程协助您完成操作。

定制服务：本公司支持一对一定制服务，如您的业务环境有特殊需求，请与客服联系。

付费服务：本公司可提供镜像部署、故障处理、安全运维代维等一站式托管服务，全面涵盖服务器环境配置，网站程序调试，数据库配置更改，数据库权限、账户，系统安全加固，故障排查，系统调优，数据库优化等范围。如您有相关需求，请咨询客服。