史上最详细保姆级教程部署OpenVPN

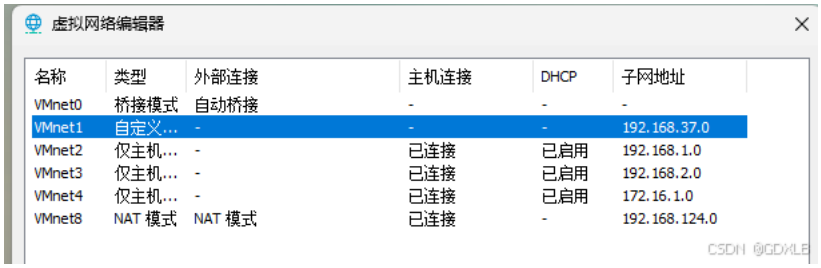
原创 置顶 GDXLB 已于 2024-10-13 11:06:05 修改 阅读量9.7k 收藏 36 点赞数 65 版权
文章标签： centos linux 运维

OpenVPN简单详细部署流程

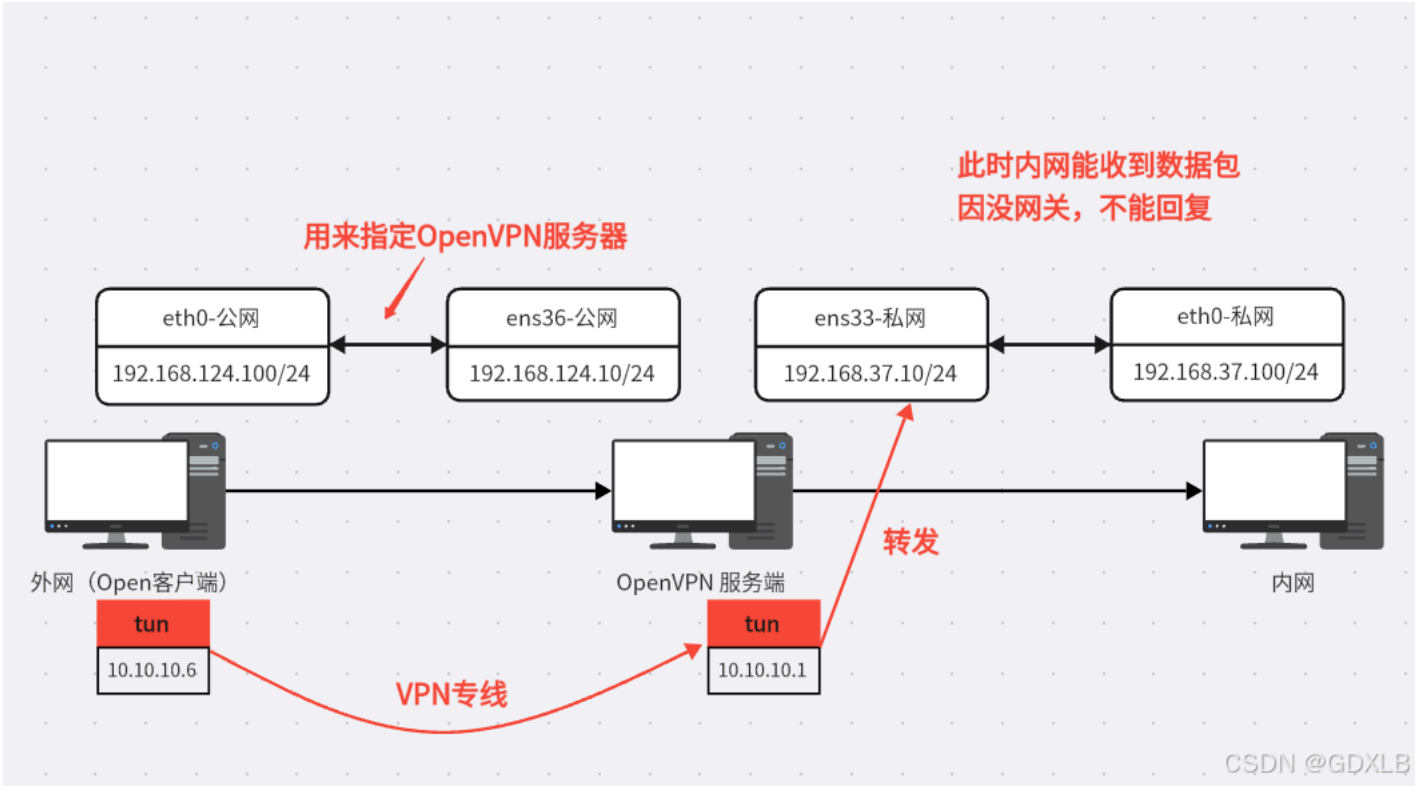
作用

提供给公司与子公司或者公司个人与公司之间建立安全的数据传输

整体环境搭建



主机	内网（均无网关）	外网
CentOS 7	192.168.37.10/24	192.168.124.10/24
Win10	N/A	192.168.124.100/24
Win Server 2008	192.168.37.100/24	N/A



VPN Server（CentOS 7）

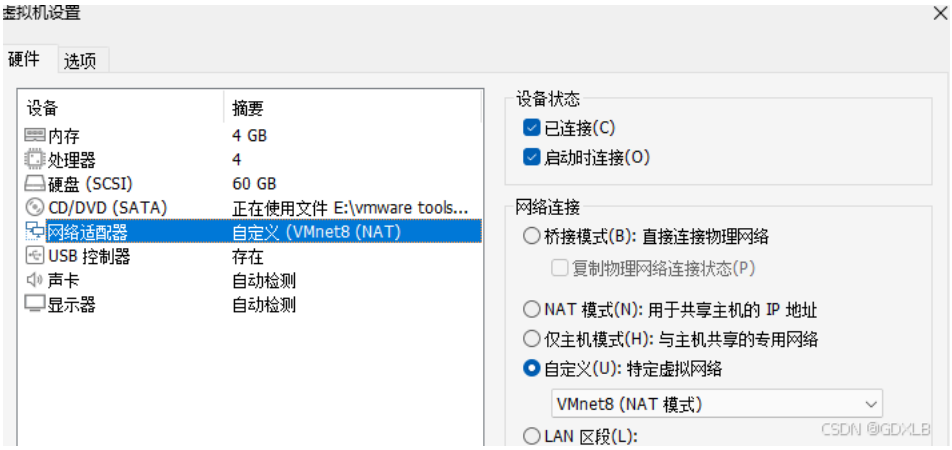
添加两张网卡

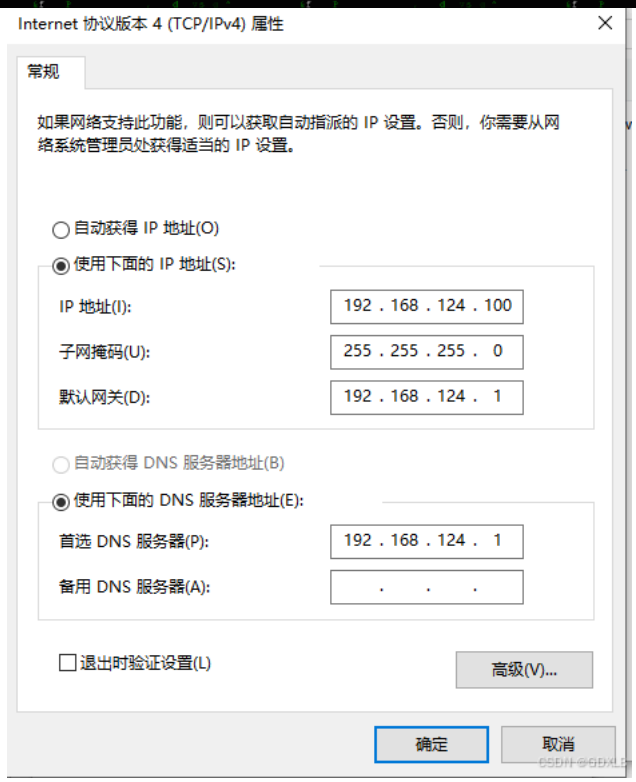
一张VMnet 1（192.168.37.10/24），连接内网

一张VMnet 8（192.168.124.10/24），连接外网

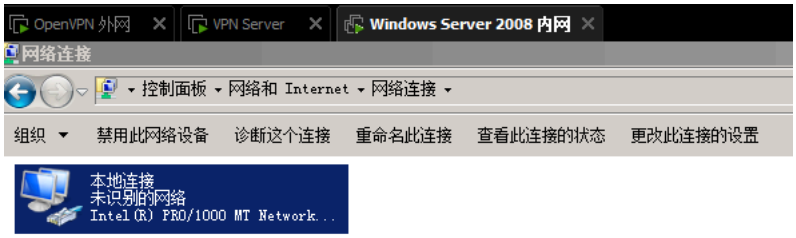

```
[root@xlb_agent ~]# ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.37.10  netmask 255.255.255.0  broadcast 192.168.37.255
        inet6 fe80::91f7:f31c:6944:d20e  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:dc:c1:8f  txqueuelen 1000  (Ethernet)
        RX packets 2993  bytes 354510 (346.2 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 292  bytes 39893 (38.9 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

ens36: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.124.10  netmask 255.255.255.0  broadcast 192.168.124.255
        inet6 fe80::b963:25ef:29b9:f0f2  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:dc:c1:99  txqueuelen 1000  (Ethernet)
        RX packets 102346  bytes 104721098 (99.8 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 57867  bytes 3518063 (3.3 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 545  bytes 47248 (46.1 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 545  bytes 47248 (46.1 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

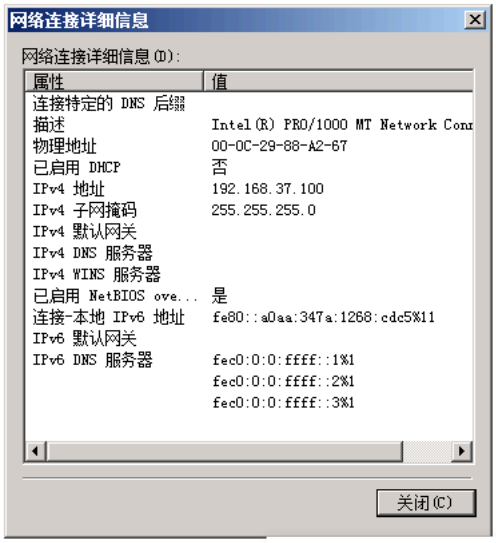

Client（Win10）





Client（Win 2008）





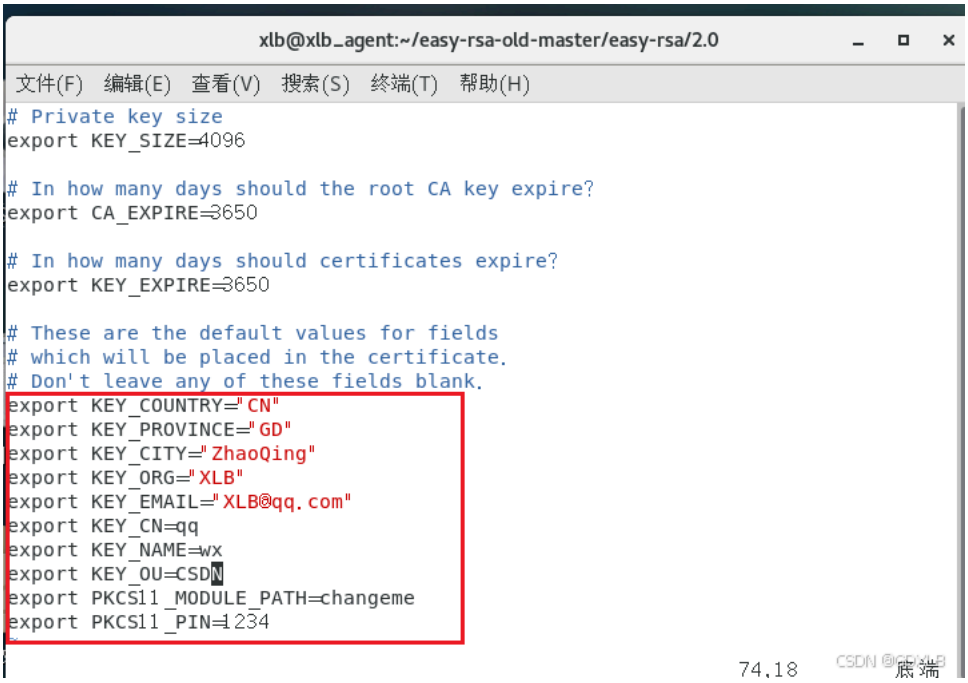
一、openVPN证书制作工具下载

下载easy-rsa


```
[root@xlb_agent ~]# cd easy-rsa-old-master/
[root@xlb_agent easy-rsa-old-master]# ls
configure.ac  COPYING  COPYRIGHT.GPL  distro  doc  easy-rsa  Makefile.am
[root@xlb_agent easy-rsa-old-master]# cd easy-rsa/2.0
[root@xlb_agent 2.0]# ls
build-ca         build-key-pkcs12  inherit-inter      pkitool
build-dh         build-key-server  list-crl           revoke-full
build-inter      build-req         openssl-0.9.6.cnf  sign-req
build-key        build-req-pass    openssl-0.9.8.cnf  vars
build-key-pass   clean-all         openssl-1.0.0.cnf  whichopensslcnf
[root@xlb_agent 2.0]# vim vars
```

CSDN @GDXLB

1、修改vars文件证书参数



使vars文件生效

> [root@xlb_agent 2.0]# source vars

```
[root@xlb_agent 2.0]# source vars
bash: /root/easy-rsa-old-master/easy-rsa/2.0/whichopensslcnf: 权限不够
NOTE: If you run ./clean-all, I will be doing a rm -rf on /root/easy-rsa-old-master/easy-rsa/2.0/keys
[root@xlb_agent 2.0]# ^C
[root@xlb_agent 2.0]# chmod +x whichopensslcnf
[root@xlb_agent 2.0]# source vars
NOTE: If you run ./clean-all, I will be doing a rm -rf on /root/easy-rsa-old-master/easy-rsa/2.0/keys
```

CSDN @GDXLB

生成keys目录，用来存放证书的信息，如私钥

> [root@xlb_agent 2.0]# ./clean-all

```
root@xlb_agent 2.0]# ls
build-ca      build-key-pass    build-req-pass  openssl-0.9.6.cnf  revoke-full
build-dh      build-key-pkcs12  clean-all       openssl-0.9.8.cnf  sign-req
build-inter   build-key-server  inherit-inter   openssl-1.0.0.cnf  vars
build-key     build-req         list-crl        pkitool            whichopensslcnf
root@xlb_agent 2.0]# ./clean-all
bash: ./clean-all: 权限不够
root@xlb_agent 2.0]# chmod +x clean-all
root@xlb_agent 2.0]# ./clean-all
root@xlb_agent 2.0]# ls
build-ca      build-key-pass    build-req-pass  list-crl           pkitool      whichopensslcnf
build-dh      build-key-pkcs12  clean-all
build-inter   build-key-server  inherit-int
build-key     build-req_        keys
```

2、生成根证书和根密钥

[root@xlb_agent 2.0]# ./build-ca

```
[root@xlb_agent 2.0]# ./build-ca
Generating a 4096 bit RSA private key
..............................................................................++
.....................................................................................................++
writing new private key to 'ca.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [CN]:
State or Province Name (full name) [GD]:
Locality Name (eg, city) [ZhaoQing]:
Organization Name (eg, company) [XLB]:
Organizational Unit Name (eg, section) [CSDN]:
Common Name (eg, your name or your server's hostname) [qq]:
Name [wx]:
Email Address [XLB@qq.com]:
```


keys目录生成ca.crt和ca.key文件

```
[root@xlb_agent 2.0]# ls keys
ca.crt  ca.key  index.txt  serial
[root@xlb_agent 2.0]#
```


3、生成服务端证书和密钥

[root@xlb_agent 2.0]# ./build-key-server server

```
[root@xlb_agent 2.0]# ./build-key-server server
Generating a 4096 bit RSA private key
..........................................................................................++
.....................................................................................................++
writing new private key to 'server.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [CN]:
State or Province Name (full name) [GD]:
Locality Name (eg, city) [ZhaoQing]:
Organization Name (eg, company) [XLB]:
Organizational Unit Name (eg, section) [CSDN]:
Common Name (eg, your name or your server's hostname) [server]:
Name [wx]:
Email Address [XLB@qq.com]:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
Using configuration from /root/easy-rsa-old-master/easy-rsa/2.0/openssl-1.0.0.cnf
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName           :PRINTABLE:'CN'
stateOrProvinceName   :PRINTABLE:'GD'
localityName          :PRINTABLE:'ZhaoQing'
organizationName      :PRINTABLE:'XLB'
organizationalUnitName:PRINTABLE:'CSDN'
commonName            :PRINTABLE:'server'
name                  :PRINTABLE:'wx'
emailAddress          :IA5STRING:'XLB@qq.com'
Certificate is to be certified until Aug 10 18:53:56 2034 GMT (3650 days)
Sign the certificate? [y/n]:y


1 out of 1 certificate requests certified, commit? [y/n]y
```


keys目录下生成server.crt、server.key、server.csr等文件

```
[root@xlb_agent 2.0]# ls keys
01.pem  ca.crt  ca.key  index.txt  index.txt.attr  index.txt.old  serial  serial.old  server.crt
server.csr  server.key
```


4、生成客户端证书和密钥

[root@xlb_agent 2.0]# ./build-key client

```
[root@xlb_agent 2.0]# ./build-key client
Generating a 4096 bit RSA private key
......
.....................................++
.....................................................................++
writing new private key to 'client.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [CN]:State or Province Name (full name) [GD]:
Locality Name (eg, city) [ZhaoQing]:
Organization Name (eg, company) [XLB]:
Organizational Unit Name (eg, section) [CSDN]:
Common Name (eg, your name or your server's hostname) [client]:
Name [wx]:
Email Address [XLB@qq.com]:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
Using configuration from /root/easy-rsa-old-master/easy-rsa/2.0/openssl-1.0.0.cnf
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName           :PRINTABLE:'CN'
stateOrProvinceName   :PRINTABLE:'GD'
localityName          :PRINTABLE:'ZhaoQing'
organizationName      :PRINTABLE:'XLB'
organizationalUnitName:PRINTABLE:'CSDN'
commonName            :PRINTABLE:'client'
name                  :PRINTABLE:'wx'
emailAddress          :IA5STRING:'XLB@qq.com'
Certificate is to be certified until Aug 10 19:01:03 2034 GMT (3650 days)
Sign the certificate? [y/n]:y


1 out of 1 certificate requests certified, commit? [y/n]y
```


keys目录下生成client.crt、client.key、client.csr等文件

```
[root@xlb_agent 2.0]# ls keys
01.pem  02.pem  ca.crt  ca.key  client.crt  client.csr  client.key  index.txt  index.txt.attr
index.txt.attr.old  index.txt.old  serial  serial.old  server.crt  server.csr  server.key
```


5、生成密钥交换文件

> [root@xlb_agent 2.0]# ./build-dh

```
[root@xlb_agent 2.0]# ./build-dh
Generating DH parameters, 2048 bit long safe prime, generator 2
This is going to take a long time
..................................................+.....................................
.....................................................................................
.....................+.........................+.....................................
.....................................................................................
.....+.....................................................+.....................
.....................+.....................................+.....+.....................
.....................................................................+.....................
.....................................+.....................................................
.....................................................................................
.+.................+.....................+.....................................
.....................................................................................
.............................+.....................................................
.....................................................................................
.....................................................+.....................................+..
.....................................................................+.................
.....................................................................+.....................
.....................................................................+.....................
.....................................................+.....................................
.....................................................................+.....................+.....
.....................................................................................+....
.....................................................................................
.....................................................................................
.....................................................................+.....+.....
...........+.........................................................................
.....................................................................................+..
.....................................................................................
.....................................................................................
.+.....................................................+.....................................
.....................................................................................
.....................................................................................
.....................................................................................
.....................................................+.....+.....................
.....................................................................................
[root@xlb_agent 2.0]#
```


keys目录下生成dh2048.pem文件

```
[root@xlb_agent 2.0]# ls keys
01.pem  ca.crt  client.crt  client.key  index.txt       index.txt.attr.old  serial      server.crt  server.key
02.pem  ca.key  client.csr  dh2048.pem  index.txt.attr  index.txt.old       serial.old  server.csr
```


二、配置OpenVPN服务器

1、配置阿里云源

```
[root@xlb_agent ~]# cd /etc/yum.repos.d/
[root@xlb_agent yum.repos.d]# curl -o epel.repo http://mirrors.aliyun.com/repo/epel-7.repo
[root@xlb_agent yum.repos.d]# yum clean all
[root@xlb_agent yum.repos.d]# yum makecache
```

```
[root@xlb_agent ~]# cd /etc/yum.repos.d/
[root@xlb_agent yum.repos.d]# ls
CentOS-Base.repo          CentOS-fasttrack.repo  CentOS-x86_64-kernel.repo
CentOS-Base.repo.backup   CentOS-Media.repo      docker-ce.repo
CentOS-CR.repo            CentOS-Sources.repo    mysql-community.repo
CentOS-Debuginfo.repo     CentOS-Vault.repo      mysql-community-source.repo
[root@xlb_agent yum.repos.d]# curl -o epel.repo http://mirrors.aliyun.com/repo/epel-7.repo
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100   664  100   664    0     0   2613      0 --:--:-- --:--:-- --:--:--  2624
[root@xlb_agent yum.repos.d]# yum clean all
已加载插件：fastestmirror, langpacks
正在清理软件源： base docker-ce-stable epel extras mysql-connectors-community
               : mysql-tools-community mysql57-community updates
Cleaning up list of fastest mirrors
[root@xlb_agent yum.repos.d]# yum makecache
已加载插件：fastestmirror, langpacks
Determining fastest mirrors
 * base: mirrors.aliyun.com
 * extras: mirrors.aliyun.com
 * updates: mirrors.aliyun.com
base                                                     | 3.6 kB  00:00:00
docker-ce-stable                                         | 3.5 kB  00:00:00
epel                                                     | 4.3 kB  00:00:00
extras                                                   | 2.9 kB  00:00:00
mysql-connectors-community                               | 2.6 kB  00:00:00
mysql-tools-community                                    | 2.6 kB  00:00:00
mysql57-community                                        | 2.6 kB  00:00:00
updates                                                  | 2.9 kB  00:00:00
(1/29): base/7/x86_64/group_gz                           | 153 kB  00:00:00
(2/29): base/7/x86_64/primary_db                         | 6.1 MB  00:00:27
(3/29): docker-ce-stable/7/x86_64/updateinfo             |  55 B   00:00:00
(4/29): docker-ce-stable/7/x86_64/filelists_db           |  66 kB  00:00:00
(5/29): docker-ce-stable/7/x86_64/primary_db             | 152 kB  00:00:00
(6/29): docker-ce-stable/7/x86_64/other_db               | 145 kB  00:00:00
```

配置阿里云源

清理yum包管理器的所有缓存和临时文件

从配置源中获取最新的软件包信息，并存储在本地缓存中

2、安装OpenVPN

```
[root@xlb_agent ~]# yum -y install openvpn
```

```
[root@xlb_agent ~]# yum -y install openvpn
已加载插件：fastestmirror, langpacks
Loading mirror speeds from cached hostfile
 * base: mirrors.aliyun.com
 * extras: mirrors.aliyun.com
 * updates: mirrors.aliyun.com
正在解决依赖关系
--> 正在检查事务
---> 软件包 openvpn.x86_64.0.2.4.12-1.el7 将被 安装
--> 正在处理依赖关系 libpkcs11-helper.so.1()(64bit)，它被软件包 openvpn-2.4.12-1.el7.x86_64 需要
--> 正在检查事务
---> 软件包 pkcs11-helper.x86_64.0.1.11-3.el7 将被 安装
--> 解决依赖关系完成

依赖关系解决

================================================================================
 Package              架构            版本                源              大小
================================================================================
正在安装:
 openvpn              x86_64          2.4.12-1.el7        epel           529 k
为依赖而安装:
 pkcs11-helper        x86_64          1.11-3.el7          epel            56 k

事务概要
```


3、配置OpenVPN

openvpn目录下建立keys文件夹

```
[root@xlb_agent ~]# cd /etc/openvpn/
[root@xlb_agent openvpn]# mkdir keys
```

```
[root@xlb_agent ~]# cd /etc/openvpn/
[root@xlb_agent openvpn]# ls
client  server
[root@xlb_agent openvpn]# mkdir keys
[root@xlb_agent openvpn]# ls
client  keys  server
[root@xlb_agent openvpn]# cd
[root@xlb_agent ~]# ls
anaconda-ks.cfg  easy-rsa-old-master  initial-setup-ks.cfg
[root@xlb_agent ~]# cd easy-rsa-old-master
[root@xlb_agent easy-rsa-old-master]# ls
configure.ac  COPYING  COPYRIGHT.GPL  distro  doc  easy-rsa  Makefile.am
[root@xlb_agent easy-rsa-old-master]# cd easy-rsa/2.0
[root@xlb_agent 2.0]# ls
build-ca         build-key-pkcs12  inherit-inter      openssl-1.0.0.cnf  whichopensslcnf
build-dh         build-key-server  keys               pkitool
build-inter      build-req         list-crl           revoke-full
build-key        build-req-pass    openssl-0.9.6.cnf  sign-req
build-key-pass   clean-all         openssl-0.9.8.cnf  vars
[root@xlb_agent 2.0]# cd keys
[root@xlb_agent keys]# ls
01.pem  ca.key      client.key  index.txt.attr      serial      server.csr
02.pem  client.crt  dh2048.pem  index.txt.attr.old  serial.old  server.key
ca.crt  client.csr  index.txt   index.txt.old       server.crt
```


将ca.crt、server.crt、server.key、dh2048.pem文件拷贝到/etc/openvpn/keys目录中

```
[root@xlb_agent openvpn]# cd ~
[root@xlb_agent ~]# cd /easy-rsa-old-master/easy-rsa/2.0/keys
[root@xlb_agent keys]# cp {ca.crt,server.crt,server.key,dh2048.pem} /etc/openvpn/keys
```

```
[root@xlb_agent keys]# cp {ca.crt,server.crt,server.key,dh2048.pem} /etc/openvpn/keys
[root@xlb_agent keys]# cd /etc/openvpn/keys
[root@xlb_agent keys]# ls
ca.crt  dh2048.pem  server.crt  server.key
```



```
//openvpn安装好后指定目录有模板文件
//(usr/share/doc/open...，不知道可以用Tab键补全提示)
//将模板配置文件server.conf复制到/etc/openvpn目录下
[root@xlb_agent keys]# cd ..
[root@xlb_agent openvpn]# cp /usr/share/doc/openvpn-2.4.12/sample/sample-config-files/server.conf ./
```

```
[root@xlb_agent keys]# cd ..
[root@xlb_agent openvpn]# ls
client  keys  server
[root@xlb_agent openvpn]# cp /usr/share/doc/op
opencc-0.4.3/         openldap-2.4.44/      openssl-1.0.2k/       opus-1.0.2/
openjpeg2-2.3.1/      open-sans-fonts-1.10/ open-vm-tools-11.0.5/
openjpeg-libs-1.5.1/  openssh-7.4p1/        openvpn-2.4.12/
[root@xlb_agent openvpn]# cp /usr/share/doc/openvpn-2.4.12/
AUTHORS               contrib/              management-notes.txt  README.down-root
ChangeLog             COPYING               README                README.systemd
Changes.rst           COPYRIGHT.GPL         README.auth-pam       sample/
[root@xlb_agent openvpn]# cp /usr/share/doc/openvpn-2.4.12/sample/sample-
sample-config-files/  sample-scripts/       sample-windows/
[root@xlb_agent openvpn]# cp /usr/share/doc/openvpn-2.4.12/sample/sample-config-files/
client.conf              openvpn-shutdown.sh      static-home.conf
firewall.sh              openvpn-startup.sh       static-office.conf
home.up                  README                   tls-home.conf
loopback-client          roadwarrior-client.conf  tls-office.conf
loopback-server          roadwarrior-server.conf  xinetd-client-config
office.up                server.conf              xinetd-server-config
[root@xlb_agent openvpn]# cp /usr/share/doc/openvpn-2.4.12/sample/sample-config-files/server.conf ./
[root@xlb_agent openvpn]# ls
client  keys  server  server.conf
```


修改配置文件vim server.conf

1、更改文件位置，以当前配置文件位置为准
2、修改vpn虚拟网段，用户通过vpn拨号进来就能自动获取到该网段IP地址
3、定义路由转发
4、修改拒绝服务攻击证书文件ta.key位置(还未建立)
5、修改加密模式，2.4版本后不能用CBC，得改成

```
# Any X509 key management system can be used.
# OpenVPN can also use a PKCS #12 formatted key file
# (see "pkcs12" directive in man page).
ca keys/ca.crt
cert keys/server.crt
key keys/server.key  # This file should be kept secret

# Diffie hellman parameters.
# Generate your own with:
#   openssl dhparam -out dh2048.pem 2048
dh keys/dh2048.pem

# Network topology
# Should be subnet (addressing via IP)
# unless Windows clients v2.0.9 and lower have to
# be supported (then net30, i.e. a /30 per client)
# Defaults to net30 (not recommended)
;topology subnet


# Configure server mode and supply a VPN subnet
# for OpenVPN to draw client addresses from.
# The server will take 10.8.0.1 for itself,
# the rest will be made available to clients.
# Each client will be able to reach the server
# on 10.8.0.1. Comment this line out if you are
# ethernet bridging. See the man page for more info.
server 10.10.10.0 255.255.255.0

# Maintain a record of client <-> virtual IP address
# associations in this file.  If OpenVPN goes down or
# is restarted, reconnecting clients can be assigned
# the same virtual IP address from the pool that was
# previously assigned.


# Push routes to the client to allow it
# to reach other private subnets behind
# the server.  Remember that these
# private subnets will also need
# to know to route the OpenVPN client
# address pool (10.8.0.0/255.255.255.0)
# back to the OpenVPN server.
;push "route 192.168.10.0 255.255.255.0"
;push "route 192.168.20.0 255.255.255.0"
push "route 10.10.10.0 255.255.255.0"
push "route 192.168.37.0 255.255.255.0"
# To assign specific IP addresses to specific
# clients or if a connecting client has a private
# subnet behind it that should also have VPN access,
# use the subdirectory "ccd" for client-specific


# The server and each client must have
# a copy of this key.
# The second parameter should be '0'
# on the server and '1' on the clients.
tls-auth keys/ta.key 0 # This file is secret

# Select a cryptographic cipher.
# This config item must be copied to
# the client config file as well.
# Note that v2.4 client/server will automatically
# negotiate AES-256-GCM in TLS mode.
# See also the ncp-cipher option in the manpage
cipher AES-256-GCM

# Enable compression on the VPN link and push the
# option to the client (v2.4+ only, for earlier
# versions see below)
;compress lz4-v2
;push "compress lz4-v2"
```

更改证书文件位置，以当前配置文件位置为准

修改虚拟网段

定义路由转发，一个本身

虚拟网段，一个内网网段

修改拒绝服务攻击证书文件位置

修改加密模式为GCM

4、启用路由转发功能

将net.ipv4.ip_forward = 1导入到内核里去，使系统永久生效开启路由转发功能

```
[root@xlb_agent openvpn]# echo "net.ipv4.ip_forward = 1" >> /etc/sysctl.conf
```

生效指令

```
[root@xlb_agent openvpn]# sysctl -p
```

```
[root@xlb_agent openvpn]# vim server.conf
[root@xlb_agent openvpn]# echo "net.ipv4.ip_forward = 1" >> /etc/sysctl.conf
[root@xlb_agent openvpn]# sysctl -p
net.ipv4.ip_forward = 1
[root@xlb_agent openvpn]#
```


5、建立ta.key文件（拒绝服务攻击证书文件）

```
[root@xlb_agent openvpn]# cd keys
[root@xlb_agent keys]# openvpn --genkey --secret ta.key
```

```
[root@xlb_agent openvpn]# ls
client  keys  server  server.conf
[root@xlb_agent openvpn]# cd keys
[root@xlb_agent keys]# ls
ca.crt  dh2048.pem  server.crt  server.key
[root@xlb_agent keys]# openvpn --genkey --secret ta.key
[root@xlb_agent keys]# ls
ca.crt  dh2048.pem  server.crt  server.key  ta.key
[root@xlb_agent keys]#
```


6、启动OpenVPN服务

```
[root@xlb_agent keys]# cd ..
[root@xlb_agent openvpn]# openvpn --daemon --config server.conf   //启动openvpn服务
[root@xlb_agent openvpn]# netstat -lntup | grep 1194   //查看openvpn是否启动成功
```

```
[root@xlb_agent keys]# cd ..
[root@xlb_agent openvpn]# ls
client  keys  server  server.conf
[root@xlb_agent openvpn]# openvpn --daemon --config server.conf
[root@xlb_agent openvpn]# netstat -lntup | grep 1194
udp        0      0 0.0.0.0:1194            0.0.0.0:*                           8452/openvpn

[root@xlb_agent openvpn]#
```


7、 查看并关闭VPN Server防火墙

```
[root@xlb_agent ~]# firewall-cmd --state
[root@xlb_agent ~]# systemctl stop firewalld
[root@xlb_agent ~]# systemctl disable firewalld
```

```
[root@xlb_agent ~]# firewall-cmd --state
running
[root@xlb_agent ~]# systemctl stop firewalld
[root@xlb_agent ~]# firewall-cmd --state
not running
[root@xlb_agent ~]# systemctl disable firewalld
[root@xlb_agent ~]#
```


8、临时关闭selinux策略

```
[root@xlb_agent ~] # setenforce 0
```

```
[root@xlb_agent ~]# getenforce
Enforcing
[root@xlb_agent ~]# setenforce 0
[root@xlb_agent ~]# getenforce
Permissive
```


三、配置OpenVPN客户端

1、复制并修改模板client.conf配置文件

```
[root@xlb_agent openvpn]# cd
[root@xlb_agent ~]# mkdir openvpn_client
[root@xlb_agent ~]# cd openvpn_client/
[root@xlb_agent openvpn_client]# cp /usr/share/doc/openvpn-2.4.12/sample/sample-config-files/client.conf ./
```

```
[root@xlb_agent openvpn]# cd
[root@xlb_agent ~]# mkdir openvpn_client
[root@xlb_agent ~]# cd openvpn_client/
[root@xlb_agent openvpn_client]# cp /usr/share/doc/openvpn-2.4.12/sample/sample-config-files/client.conf ./
[root@xlb_agent openvpn_client]# ls
client.conf
[root@xlb_agent openvpn_client]#
```


编辑配置文件vim client.conf

1、添加远程主机
2、修改加密模式为GCM

```
# The hostname/IP and port of the server.
# You can have multiple remote entries
# to load balance between the servers.
;remote my-server-1 1194
;remote my-server-2 1194
remote 192.168.124.10 1194

# Choose a random host from the remote
# list for load-balancing.  Otherwise
# try hosts in the order specified.
;remote-random

# Keep trying indefinitely to resolve the
# host name of the OpenVPN server.  Very useful
# on machines which are not permanently connected
# to the internet such as laptops.
resolv-retry infinite

# Select a cryptographic cipher.
# If the cipher option is used on the server
# then you must also specify it here.
# Note that v2.4 client/server will automatically
# negotiate AES-256-GCM in TLS mode.
# See also the ncp-cipher option in the manpage
cipher AES-256-GCM

# Enable compression on the VPN link.
# Don't enable this unless it is also
# enabled in the server config file.
#comp-lzo
```

分号注销默认远程主机
添加外网接口IP，端口1194
修改加密模式

2、打包上传客户端所需证书等文件

将ca.crt、client.key、client.crt、ta.key文件拷贝到/root/openvpn_client目录中

```
[root@xlb_agent openvpn_client]# cd ~
[root@xlb_agent ~]# cd easy-rsa-old-master/easy-rsa/2.0/keys
[root@xlb_agent keys]# cp {ca.crt,client.key,client.crt} /root/openvpn_client
[root@xlb_agent keys]# cd /etc/openvpn/keys
[root@xlb_agent keys]# cp ta.key /root/openvpn_client
```

```
[root@xlb_agent openvpn_client]# cd
[root@xlb_agent ~]# ls
anaconda-ks.cfg  easy-rsa-old-master  initial-setup-ks.cfg  openvpn_client
[root@xlb_agent ~]# cd easy-rsa-old-master/
easy-rsa-old-master/
[root@xlb_agent ~]# cd easy-rsa-old-master/
distro/   doc/      easy-rsa/
[root@xlb_agent ~]# cd easy-rsa-old-master/easy-rsa/
1.0/     2.0/     Windows/
[root@xlb_agent ~]# cd easy-rsa-old-master/easy-rsa/2.0
[root@xlb_agent 2.0]# ls
build-ca      build-key-pass    build-req-pass  list-crl           pkitool      whichopensslcnf
build-dh      build-key-pkcs12  clean-all       openssl-0.9.6.cnf  revoke-full
build-inter   build-key-server  inherit-inter   openssl-0.9.8.cnf  sign-req
build-key     build-req         keys            openssl-1.0.0.cnf  vars
[root@xlb_agent 2.0]# cd keys
[root@xlb_agent keys]# ls
01.pem  ca.crt  client.crt  client.key  index.txt       index.txt.attr.old  serial      server.crt  server.key
02.pem  ca.key  client.csr  dh2048.pem  index.txt.attr  index.txt.old       serial.old  server.csr
[root@xlb_agent keys]# cp {ca.crt,client.key,client.crt} /root/openvpn_client
[root@xlb_agent keys]# cd /root/openvpn_client
[root@xlb_agent openvpn_client]# ls
ca.crt  client.conf  client.crt  client.key
[root@xlb_agent openvpn_client]# cd /etc/openvpn/keys
[root@xlb_agent keys]# ls
ca.crt  dh2048.pem  server.crt  server.key  ta.key
[root@xlb_agent keys]# cp ta.key /root/openvpn_client
[root@xlb_agent keys]# cd /root/openvpn_client
[root@xlb_agent openvpn_client]# ls
ca.crt  client.conf  client.crt  client.key  ta.key
```


将client.conf改名为client.ovpn(因客户端识别ovpn后缀文件)

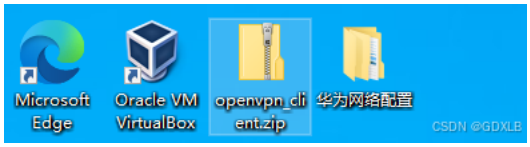
> [root@xlb_agent openvpn_client]# mv client.conf client.ovpn

```
[root@xlb_agent openvpn_client]# ls
ca.crt  client.conf  client.crt  client.key  ta.key
[root@xlb_agent openvpn_client]# mv client.conf client.ovpn
[root@xlb_agent openvpn_client]# ls
ca.crt  client.crt  client.key  client.ovpn  ta.key
[root@xlb_agent openvpn_client]#
```

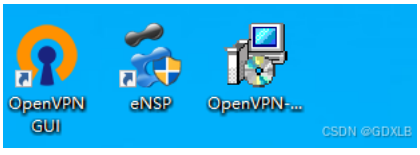

将ca.crt、client.key、client.crt、ta.key、client.ovpn打包上传至客户端

> [root@xlb_agent ~]# zip openvpn_client.zip openvpn_client/*

```
[root@xlb_agent ~]# zip openvpn_client.zip openvpn_client/*
  adding: openvpn_client/ca.crt (deflated 28%)
  adding: openvpn_client/client.crt (deflated 47%)
  adding: openvpn_client/client.key (deflated 24%)
  adding: openvpn_client/client.ovpn (deflated 54%)
  adding: openvpn_client/ta.key (deflated 40%)
[root@xlb_agent ~]# ls
anaconda-ks.cfg  easy-rsa-old-master  initial-setup-ks.cfg  openvpn_client  openvpn_client.zip
```

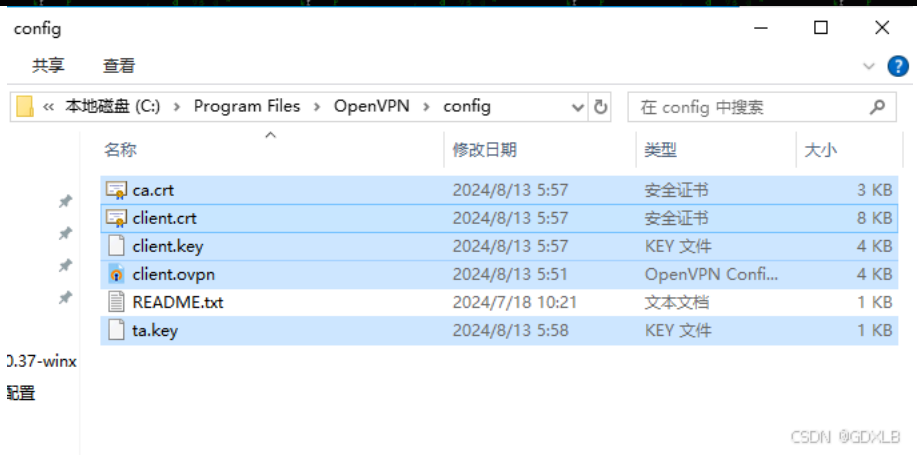



3、安装OpenVPN Windows客户端



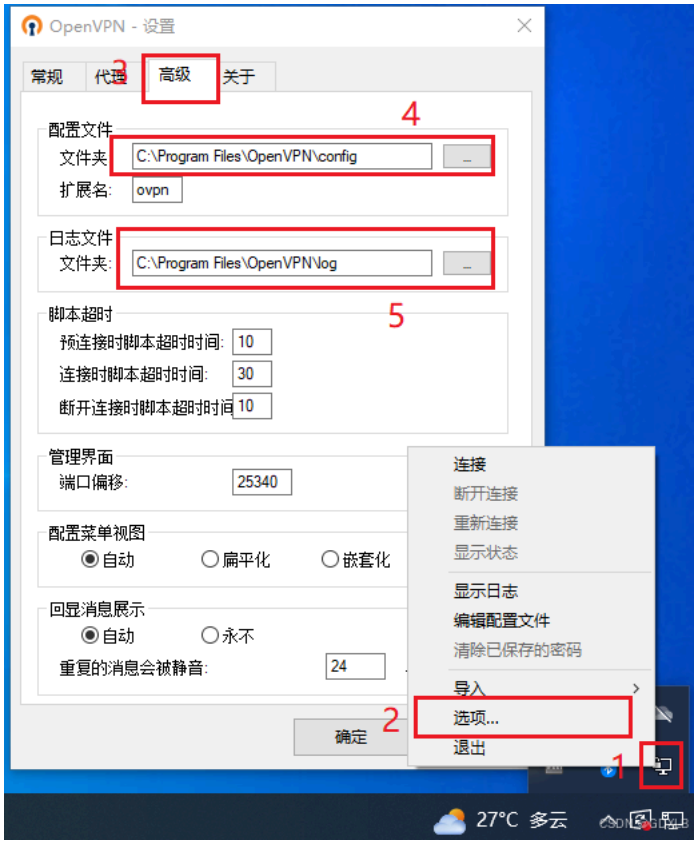
4、虚拟专用网连接设置

将openvpn_client.zip解压到OpenVPN安装目录的config文件夹中



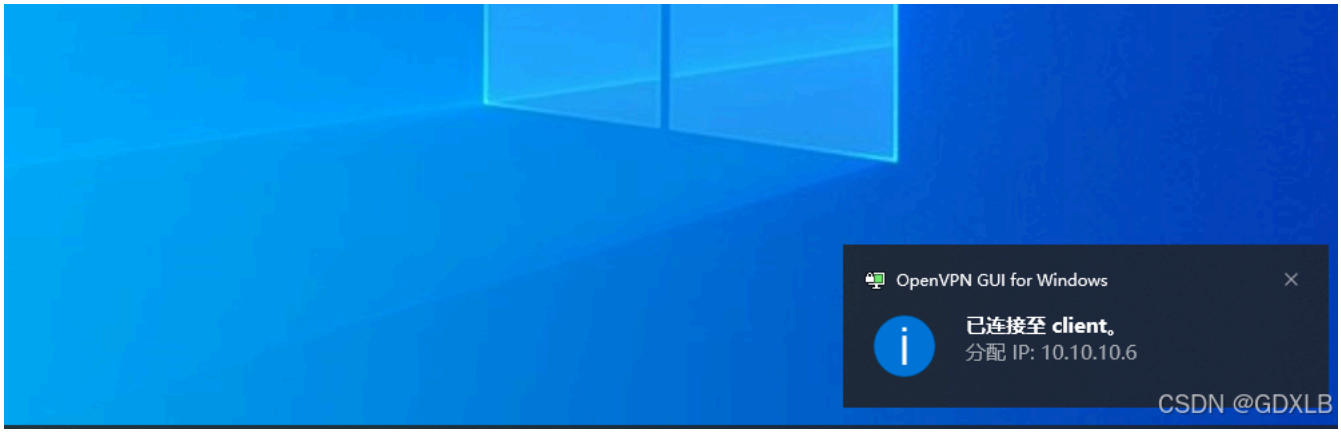
新建client.log文件放入OpenVPN安装目录的log文件夹中

更改配置路径



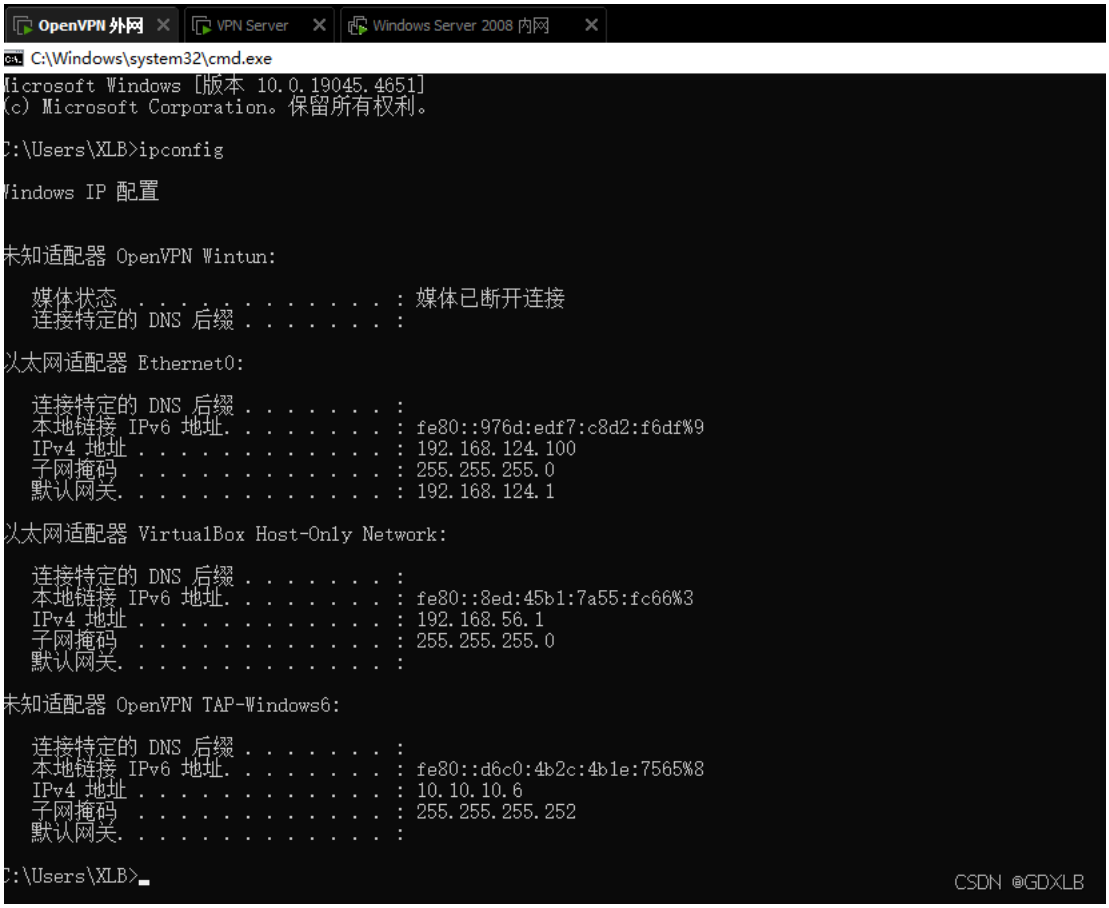
四、Windows 客户端连接测试

1、连接虚拟专用网



2、查看隧道接口地址分配

Client外网：



VPN Server：

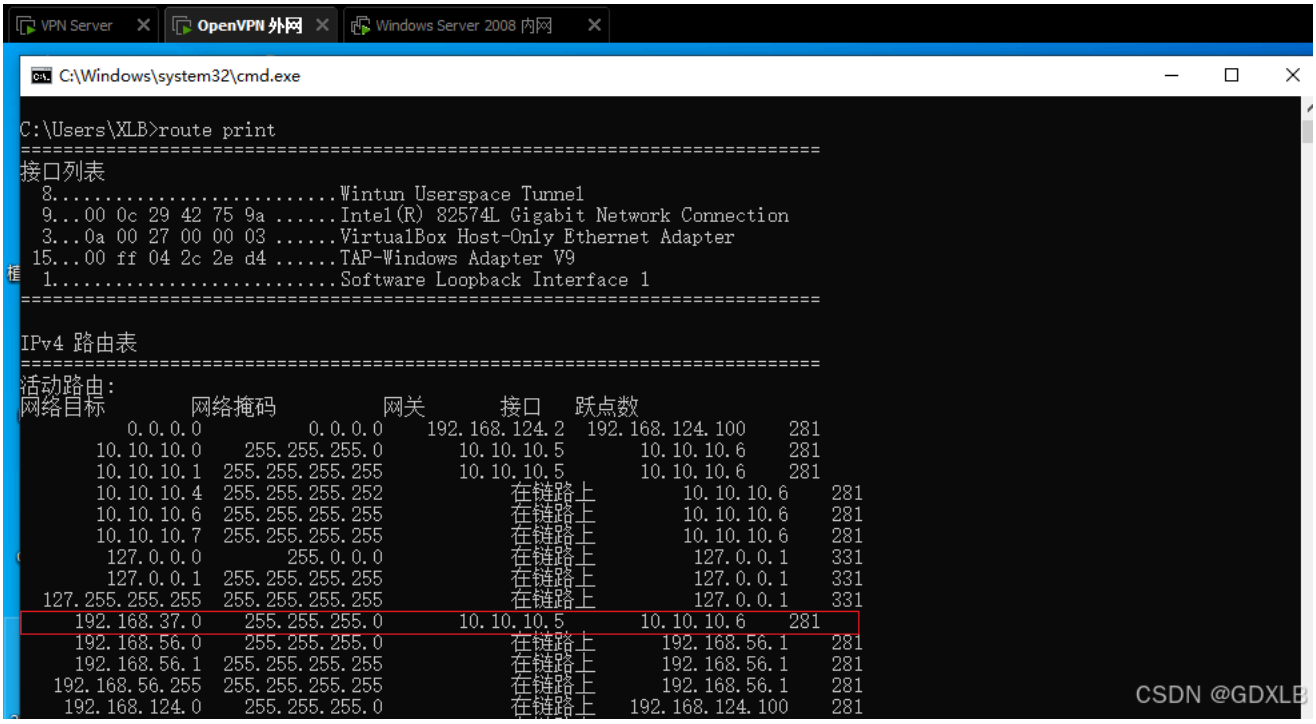
```
[root@xlb_agent openvpn]# ip address
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:0c:29:dc:c1:8f brd ff:ff:ff:ff:ff:ff
    inet 192.168.37.10/24 brd 192.168.37.255 scope global noprefixroute ens33
       valid_lft forever preferred_lft forever
    inet6 fe80::a4e3:5d0e:6c7b:2ee2/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
3: ens36: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:0c:29:dc:c1:99 brd ff:ff:ff:ff:ff:ff
    inet 192.168.124.10/24 brd 192.168.124.255 scope global noprefixroute ens36
       valid_lft forever preferred_lft forever
    inet6 fe80::b963:25ef:29b9:f0f2/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
4: virbr0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default qlen 1000
    link/ether 52:54:00:43:ea:63 brd ff:ff:ff:ff:ff:ff
    inet 192.168.122.1/24 brd 192.168.122.255 scope global virbr0
       valid_lft forever preferred_lft forever
5: virbr0-nic: <BROADCAST,MULTICAST> mtu 1500 qdisc pfifo_fast master virbr0 state DOWN group default qlen 1000
    link/ether 52:54:00:43:ea:63 brd ff:ff:ff:ff:ff:ff
6: tun0: <POINTOPOINT,MULTICAST,NOARP,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UNKNOWN group default qlen 100
    link/none
    inet 10.10.10.1 peer 10.10.10.2/32 scope global tun0
       valid_lft forever preferred_lft forever
    inet6 fe80::df40:15d:3ae8:4039/64 scope link flags 800
```


3、虚拟专用网Ping测试

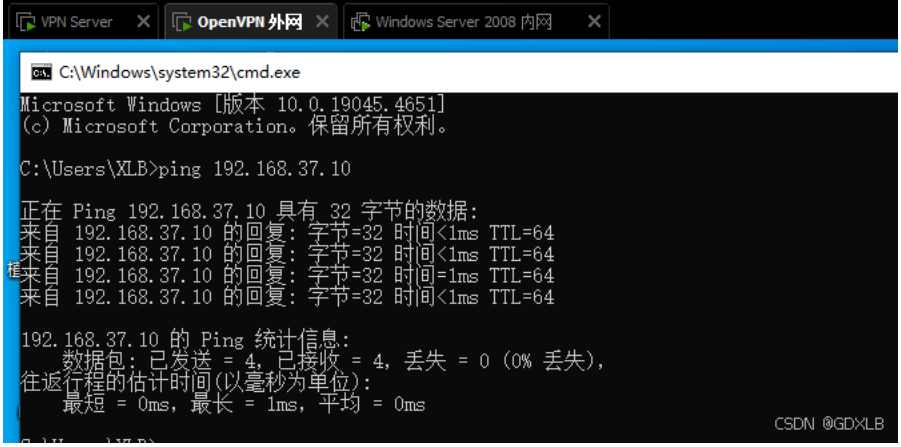
```
[root@xlb_agent openvpn]# ping 10.10.10.6
PING 10.10.10.6 (10.10.10.6) 56(84) bytes of data.
64 bytes from 10.10.10.6: icmp_seq=1 ttl=128 time=0.732 ms
64 bytes from 10.10.10.6: icmp_seq=2 ttl=128 time=1.67 ms
64 bytes from 10.10.10.6: icmp_seq=3 ttl=128 time=0.831 ms
64 bytes from 10.10.10.6: icmp_seq=4 ttl=128 time=0.705 ms
^C
--- 10.10.10.6 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 0.705/0.985/1.674/0.401 ms
```


五、测试内网连通性

1、查看路由表

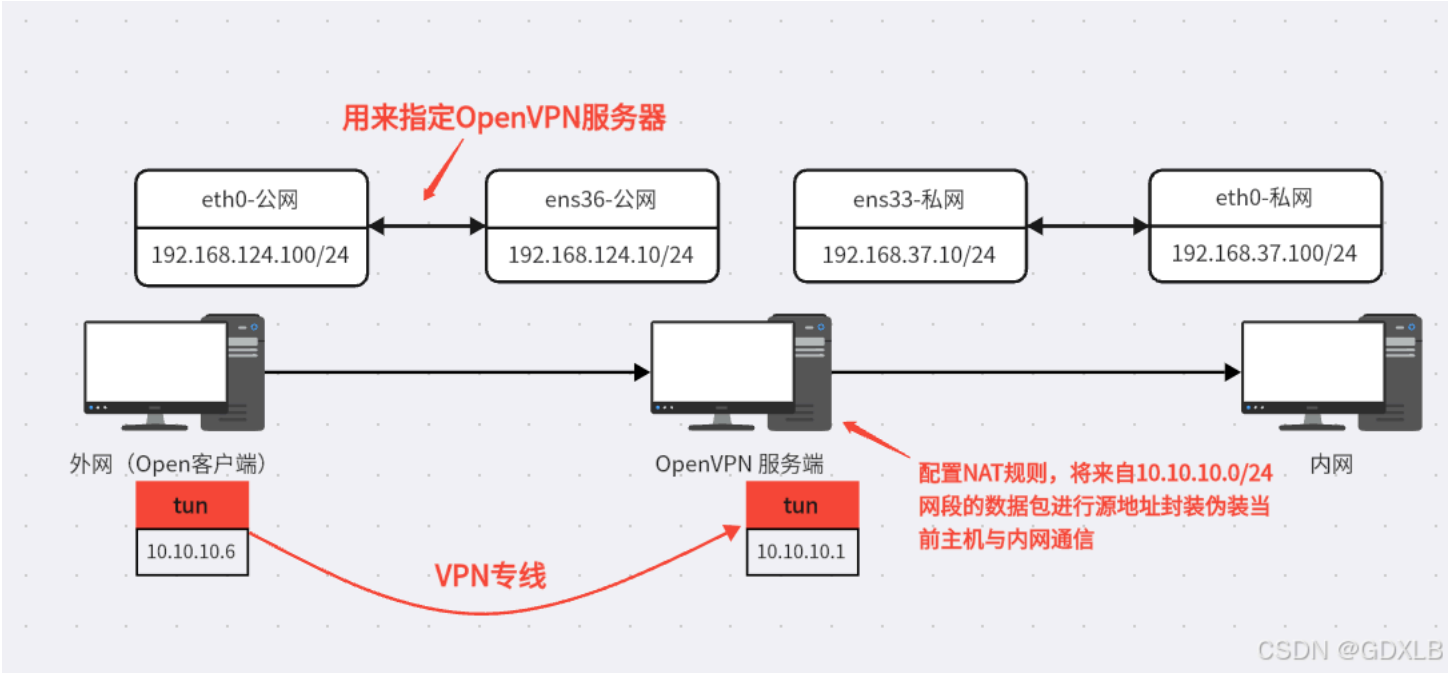


2、外网Ping内网接口



3、外网Ping内网服务器

六、配置NAT地址转换功能

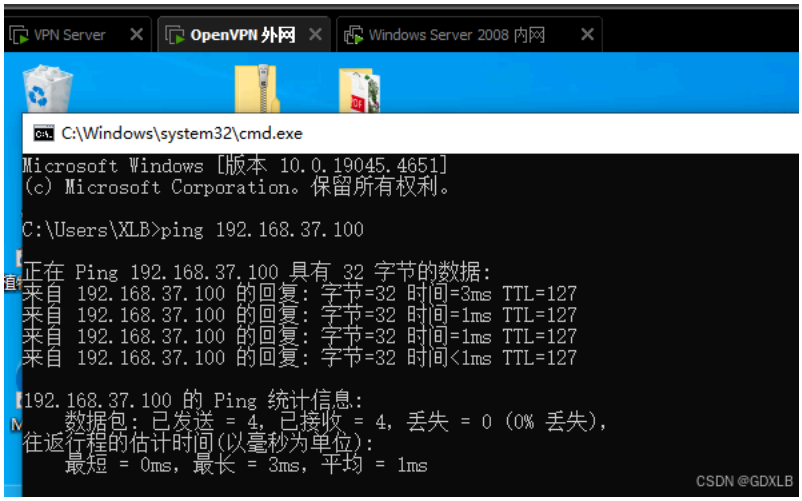


1、配置iptables的NAT功能

```
[root@xlb_agent network-scripts]# iptables -t nat -A POSTROUTING -s 10.10.10.0/24 -j MASQUERADE
```

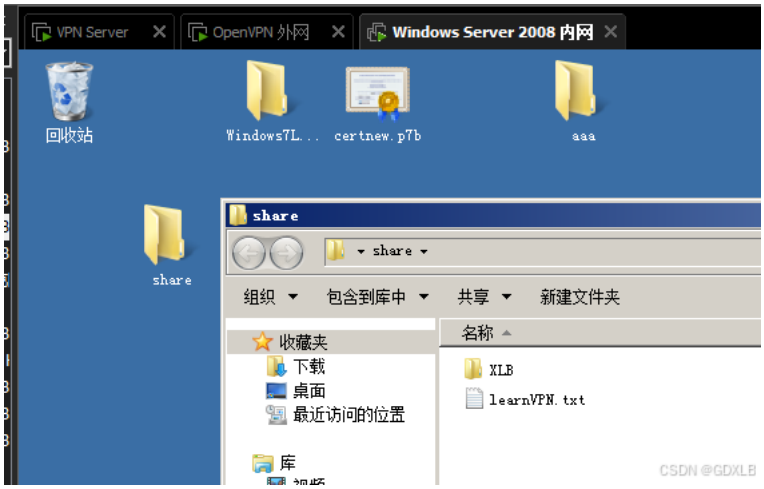
```
[root@xlb_agent network-scripts]# iptables -t  nat -L
Chain PREROUTING (policy ACCEPT)
target     prot opt source               destination

Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination

Chain POSTROUTING (policy ACCEPT)
target     prot opt source               destination
[root@xlb_agent network-scripts]# iptables -t nat -A POSTROUTING -s 10.10.10.0/24 -j MASQUERADE
[root@xlb_agent network-scripts]# iptables -t  nat -L
Chain PREROUTING (policy ACCEPT)
target     prot opt source               destination

Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination

Chain POSTROUTING (policy ACCEPT)
target     prot opt source               destination
MASQUERADE  all  --  10.10.10.0/24_       anywhere
```

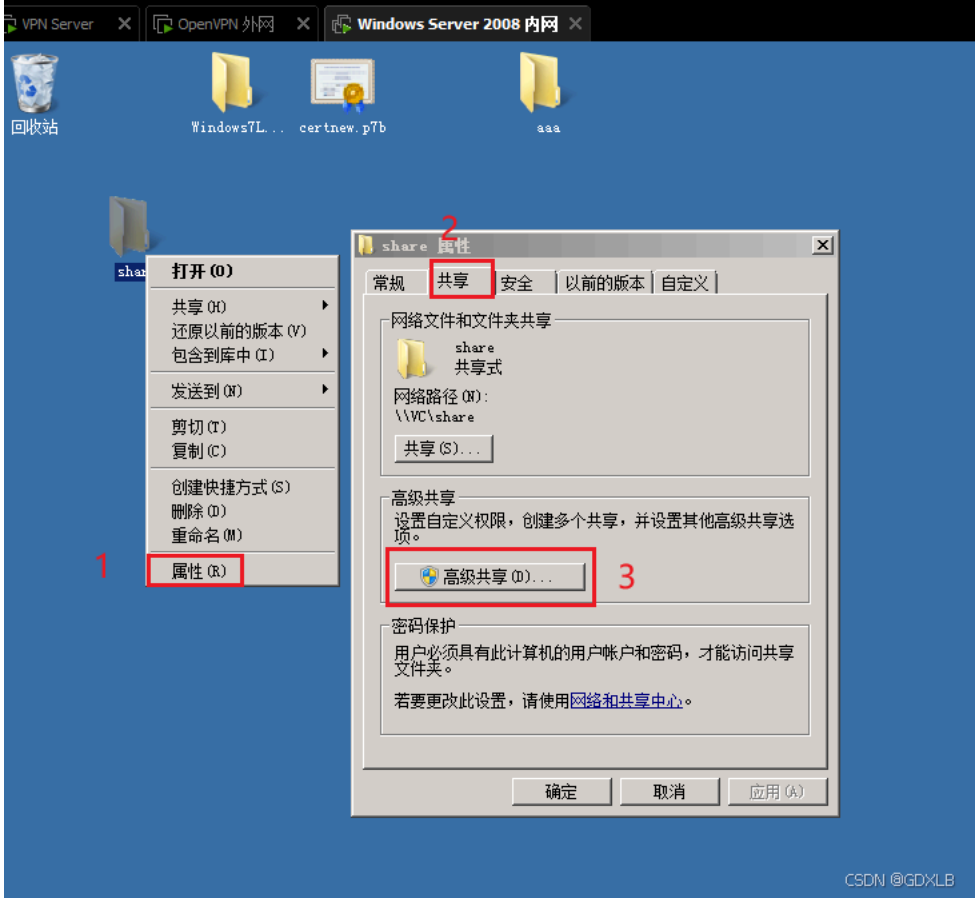

2、外网Ping内网服务器



七、功能测试

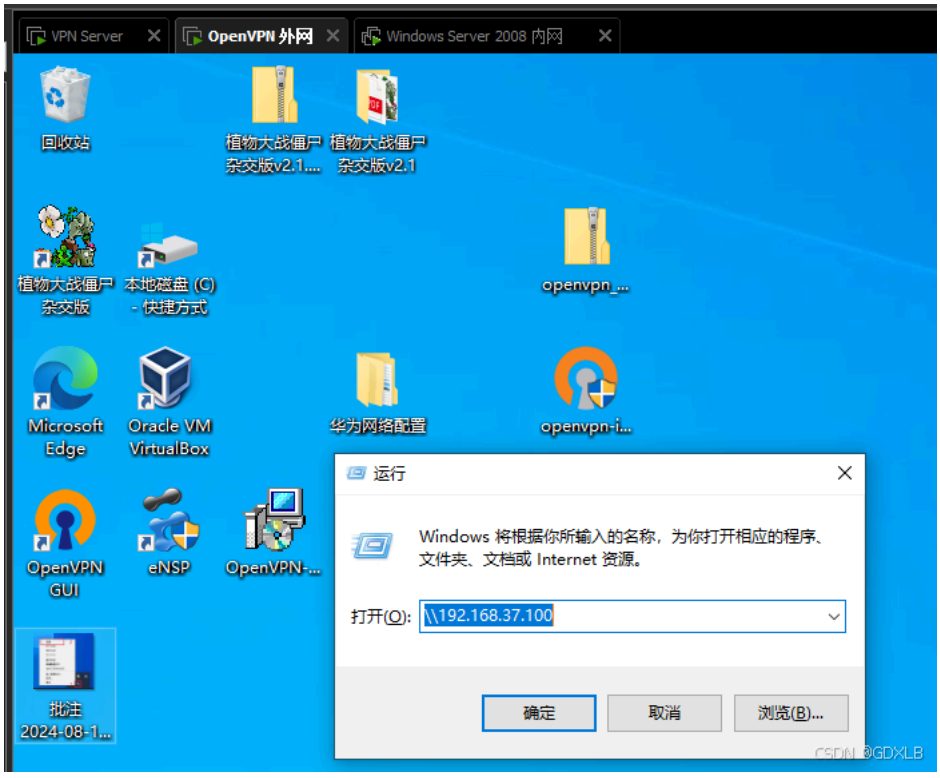
1、内网提供共享文件



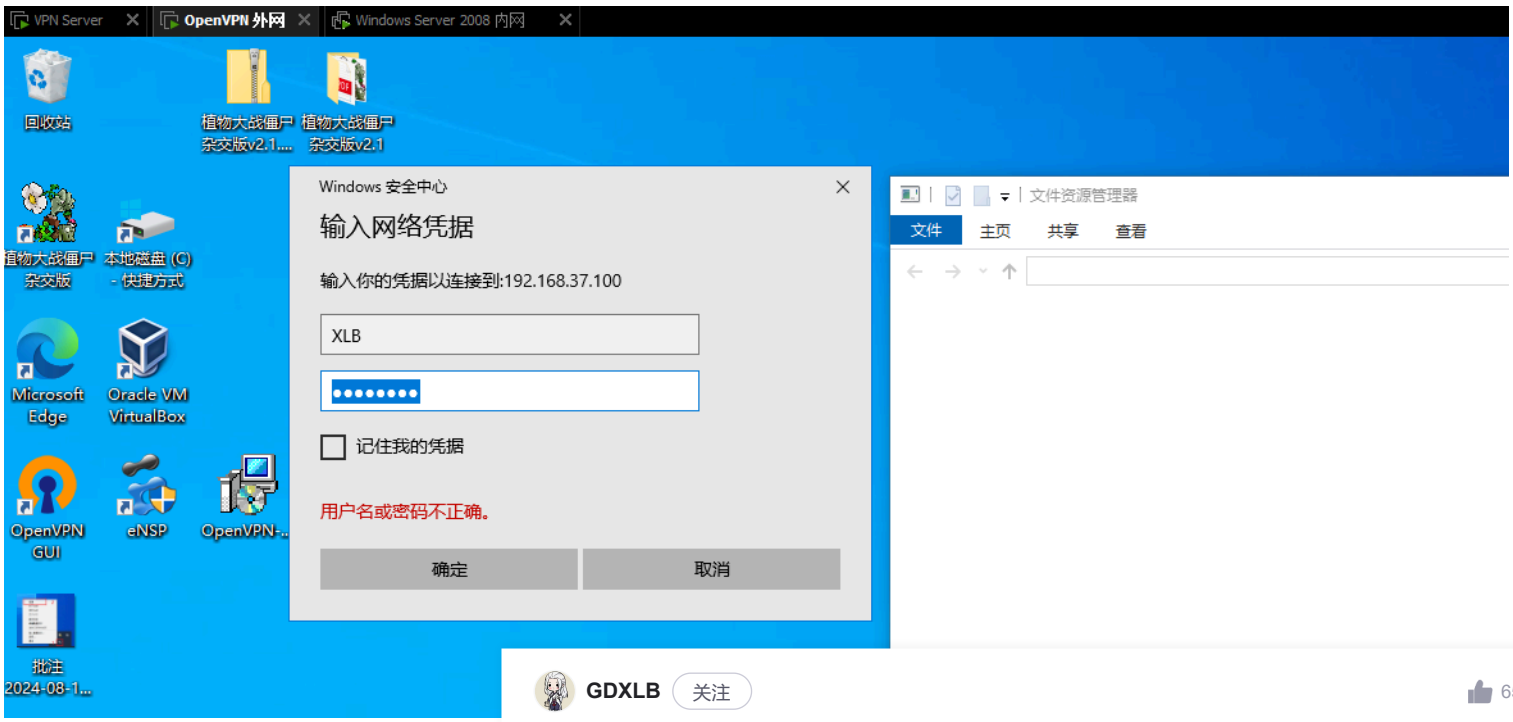


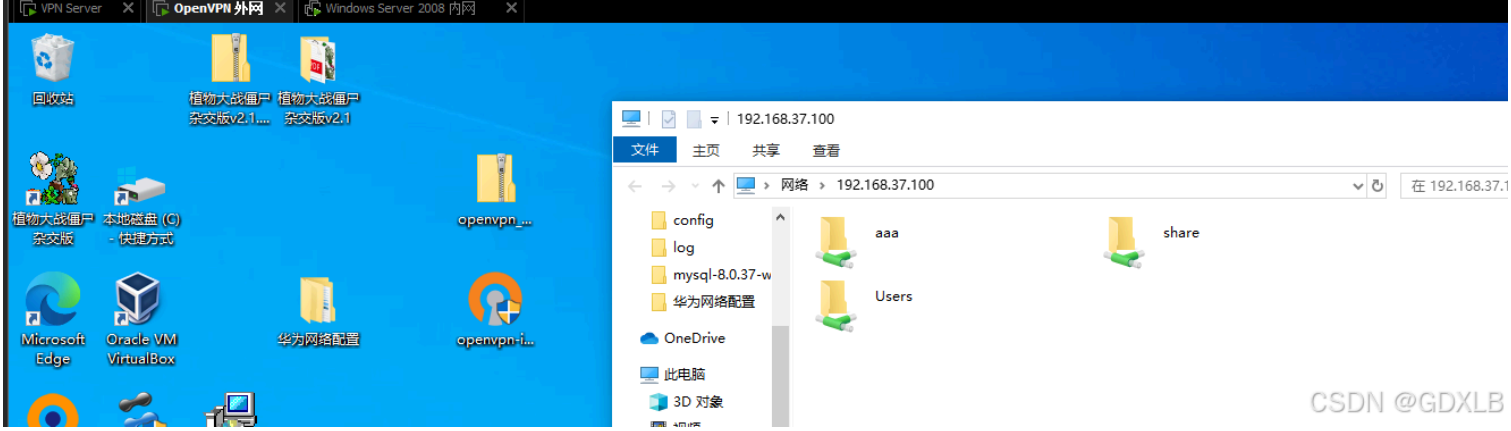
2、内网添加新用户供外网访问共享文件

3、外网访问内网共享文件



输入账号密码





文章知识点与官方知识档案匹配，可进一步学习相关知识

云原生入门技能树 > 首页 > 概览　20393 人正在系统学习中

OpenVPN部署　glisten0317的博客　5197
安装epel仓库安装easy-RSA安装openvpn服务端如果在线无法安装，可以通过离线文件进行安装。

基于openvpn的web管理系统，前后端分离设计。 最新发布　09-21
基于openvpn的web管理系统，前后端分离设计。

5 条评论 >　m0_37127604 热评 连个公网ip都没有，搭什么vpn啊　写评论

openVPN安装搭建步骤，实现内网穿透　QAZ600888的博客　1万+
这将告诉 OpenVPN 服务器将 client-moxa 客户端的请求路由到 10.8.1.6 这个 IP 地址（即 client-24 客户端的 IP 地址）。这将告诉客户端将流量路由到 10.8.1.0/24 子网，其中包括 c...

【亲测能用！OpenVPN实验教程】Win11主机连CentOS7服务器（用户名密码模式）　IT_GIRL_XYX的博客　2007
经过无数个日日夜夜，无数次调试、崩溃、再调试，甚至急得胃病复发。看到成功连接的那一瞬间，竟然无比平静。写这篇文章是希望其他使用OpenVPN的同志能够少走弯路，提供...

Centos7 搭建openVPN　三人行，必有我师焉。　1348
CentOS 搭建openVPN时需要一台有公网IP的服务器。openVPN 是一个基于SSL/TLS的虚拟专用网络（VPN），它允许你创建一个安全的连接，通过它你可以将你的网络流量封装...

OpenVPN 安装与使用　Shawn的个人博客　4074
可以添加、删除、查看等，网段默认是10.8.0.x，按照客户端启动顺序给予分配ip，同时客户端可以访问server端所在的内网(可以使用route命令查看，原因是转发到vpn网卡的流量全...

2、OpenVPN搭建　weixin_46371752的博客　6774
搭建OpenVPN，centos7搭建VPN，centos7部署OpenVPN，linux如何搭建VPN服务，cetnos7如何部署OpenVPN，centos7如何部署VPN服务

OpenVPN 简介及部署　wang11876的博客　1万+
OpenVPN 是一个健全且高效的 VPN 守护进程，它支持 SSL/TLS 安全、以太网桥，支持TCP 或者 UDP 代理或者是 NAT 通道传输，支持动态 IP 地址和 DHCP，可支持成百上千的...

OpenVPN安装部署详解　Aidon博客　5354
基于阿里云Centos 7.9操作系统的OpenVPN的客户端和服务端安装配置详细步骤及相关问题解决。

openvpn部署　这是一个将要崛起小达人　1万+
openvpn搭建大致步骤

OpenVpn部署　qq_46103493的博客　1346
OpenVpn部署，添加路由，实现路由流量走VPN，本地流量走本地。

搭建frp+OpenVPN实现公网服务器对内网服务器的访问　m0_59575008的博客　4571
本实验需求一台公网服务器，两台内网服务器。

Vyos OpenVPN (SSL TLS+User Auth) 本地PAM认证 SSLVPN服务器搭建　taylorgogo　1459
Vyos 基于OpenVPN的 多客户端拨入 PAM本地用户认证 SSLVPN

告别繁琐设置，用OpenVPN一键实现内网穿透与远程办公　weixin_40872310的博客　627
1、在公有云搭建openvpn的服务端登录后复制 # 安装openvp

GDXLB　关注　65