

基础章节-16-虚拟专用网络知识说明-VPN

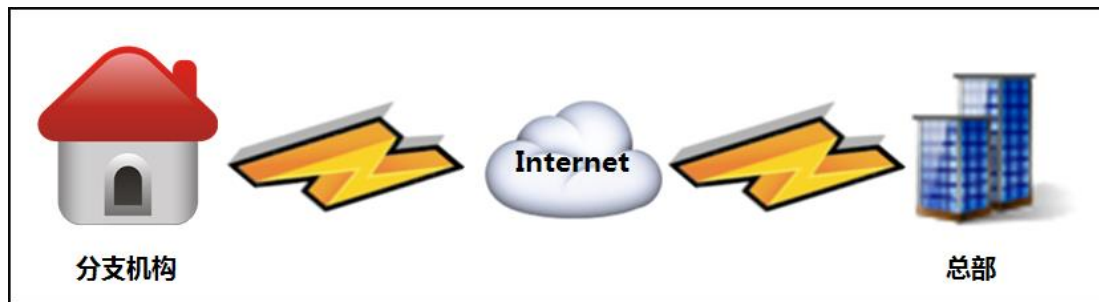
1.1 虚拟专用网络诞生

一个技术的出现都是由于某种需求触发的。那么为什么会出现 VPN 技术呢？

VPN 技术解决了什么问题呢？

早期在没有 VPN 之前，企业的总部和分支机构之间的互通都是采用运营商提供的 Internet 互联网尽心通信；

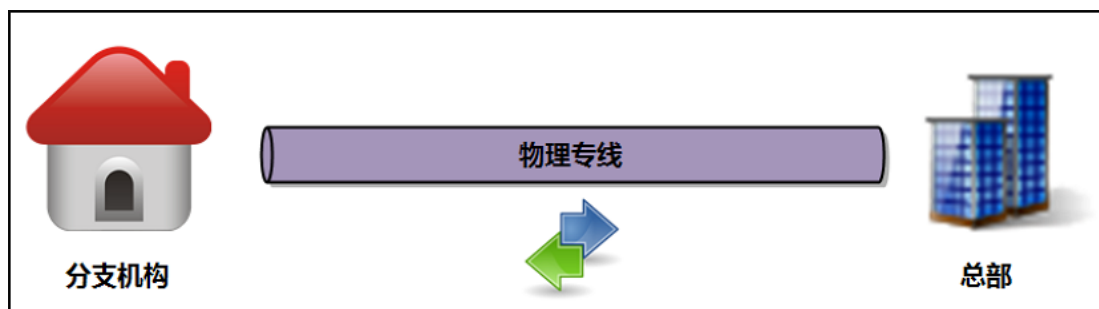
但是在 Internet 互联网中通讯往往是不安全的，通信的内容可能被窃取、修改等，从而造成安全隐患或者安全事件；



所以需要有一种技术既能实现总部和分支机构的互通，也能保证数据传输的安全性！

早期很多大型企业会联合运营商构建物理专线网络，在总部和分支机构之间拉条专线，只传输自己的业务；

但是这个专线的费用确实不是一般公司能够承受的，而且维护也很困难；



那么有没有成本比较低的解决方案呢？

因此，就引出了 VPN 技术，VPN 通过在现有的 Internet 网络中构建专用的虚拟网络，实现企业总部和分支机构的通信；

解决了互通、安全、成本的问题。

1.1.2 虚拟专用网络介绍

VPN（全称 Virtual Private Network）虚拟专用网络，是依靠 ISP 和其他的 NSP，在公共网络中建立专用的数据通信网络的技术；

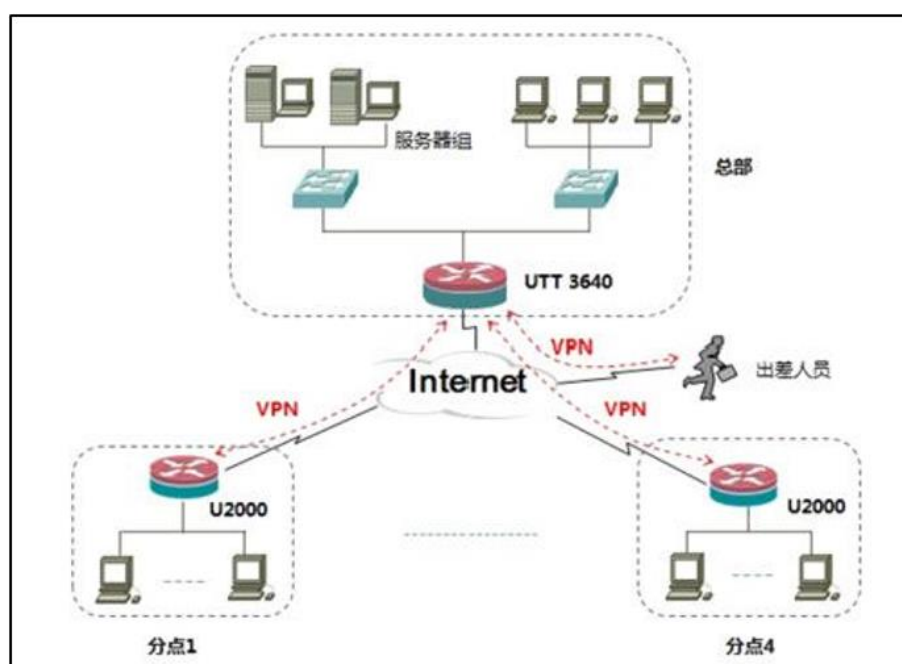
可以为企业之间或者个人与企业之间提供安全的数据传输隧道服务。

在 VPN 中任意两点之间的连接并没有传统专网所需的端到端的物理链路，而是利用公共网络资源动态组成的；

可以理解为通过私有的隧道技术在公共数据网络上模拟出来的和专网有同样功能的点到点的专线技术；

所谓虚拟是指不需要去拉实际的长途物理线路，而是借用了公共 Internet 网络实现。

为了便于理解 VPN 概念，利用一个网络示意图进行说明：

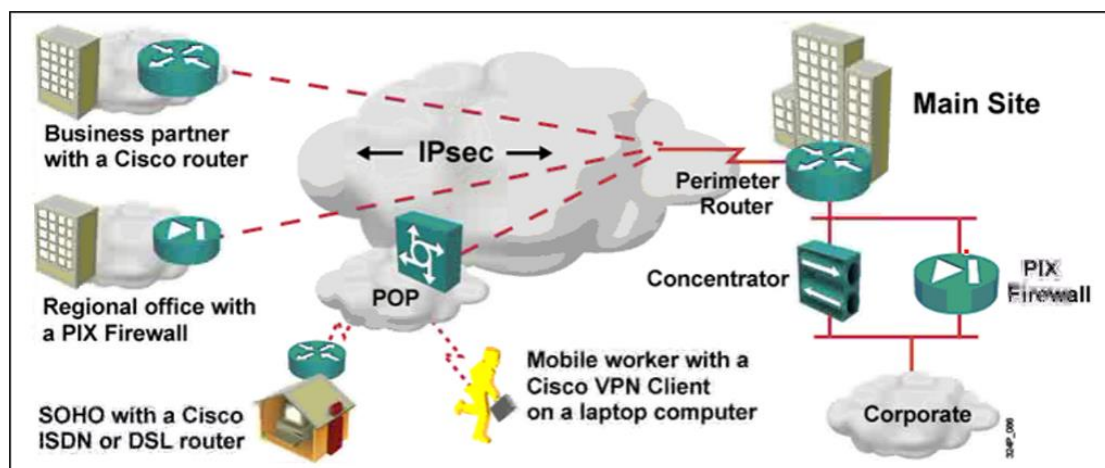


1.1.3 虚拟专用网络作用

VPN 功能可以帮助公司里的远程用户（出差、家里），公司的分支机构，商业合作伙伴及供应商等公司和自己的公司内部网络之间；

建立可信的安全连接或者是局域网连接，确保数据的加密安全传输和业务访问；

对于运维工程师来说，还可以连接不同的机房构成局域网，处理相关的业务流。



应用虚拟专用网络的优势特点：

- **安全性高**

在远端用户、驻外机构、合作伙伴、供应商与公司总部之间建立可靠的连接，保证数据传输的安全性。

这对于实现电子商务或金融网络与通讯网络的融合特别重要。

- **费用低廉**

利用公共网络进行信息通讯，企业可以用更低的成本连接远程办事机构、出差人员和业务伙伴。

- **支持移动**

支持出差 VPN 用户在任何时间、任何地点的移动接入，能够满足不断增长的移动业务需求。

- **可扩展性**

由于 VPN 为逻辑上的网络，物理网络中增加或修改节点，不影响 VPN 的部署。

1.1.4 虚拟专用网络分类

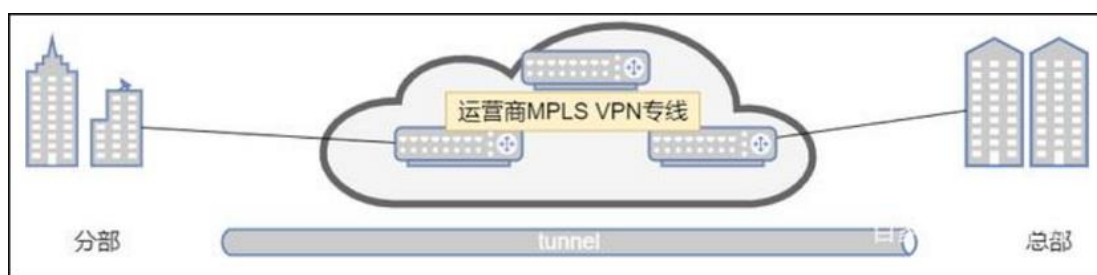
01 根据 VPN 建设单位不同进行划分

- **租用运营厂商专线搭建 VPN**

运营商的虚拟专线网络大多数都是使用 MPLS VPN；

企业通过购买运营商提供的 VPN 专线服务实现总部和分支机构间的通信需求；

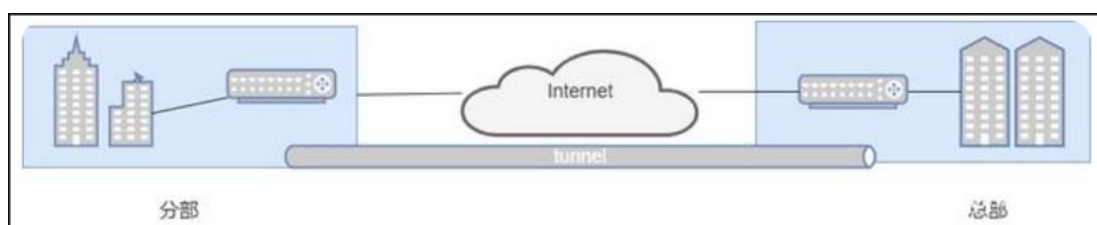
VPN 网关为运营商所有。



- **企业内部自建环境搭建 VPN**

企业内部自建基于 Internet 环境的 vpn 网络，常见的有 IPsev VPN、GRE VPN、L2TP VPN、SSL VPN

企业自己购买 VPN 网络设备，搭建自己的 VPN 网络，实现总部和分支机构的通信，或者是出差员工和总部的通信；



02 根据 VPN 组网方式不同进行划分

- **远程访问 VPN**

这种方式适用于出差员工拨号接入 VPN 的方式，员工可以在只要有 Internet 的地方都可以通过 VPN 接入访问企业内网资源。

最常见类型有：SSL VPN、L2TP VPN

- **站点之间 VPN**

这种方式适合用于企业两个局域网互通的情况；例如企业的分支机构访问总部；

最常见类型有：MPLS VPN、IPsec VPN

03 根据 VPN 工作网络层次进行划分

- 应用层 VPN：SSL VPN
- 网络层 VPN：IPsec VPN、GRE VPN
- 链路层 VPN：L2TP2 VPN、PPTP VPN

1.2 虚拟专用网络技术

1.2.1 网络通讯隧道技术

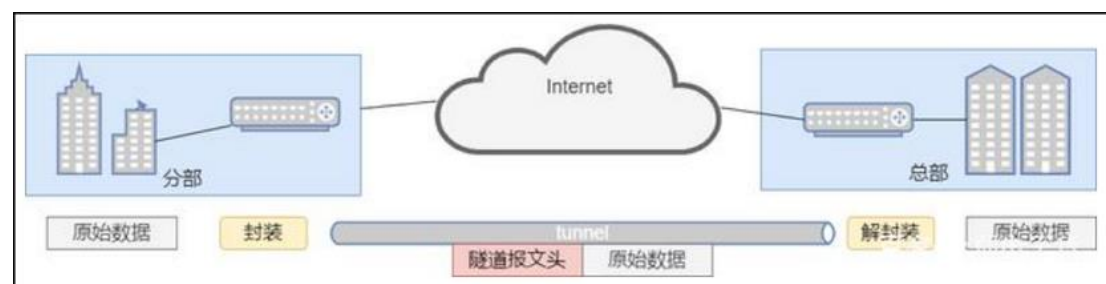
VPN 技术的基本原理其实就是用的隧道技术；

就类似于火车/地铁的轨道一样，从 A 站点到 B 站点都是直通的，不会堵车。

对于乘客而言，就是专车；

隧道技术其实就是对传输的报文进行封装，利用公网建立专用的数据传输通道，

从而完成数据的安全可靠传输；



从上图中可以看到原始报文在隧道的一端进行封装，封装后的数据在公网上传输，在隧道另一端进行解封装；

从而实现了数据的安全传输。

隧道协议通过在隧道的一端给数据加上隧道协议头，即进行封装，使这些被封装的数据能都在某网络中传输；

并且在隧道的另一端去掉该数据携带的隧道协议头，即进行解封装。

1.2.2 网络通讯安全技术

在利用 VPN 进行数据传输通讯时，身份认证、数据加密、数据验证可以有效保证数据传输的安全性；

01 身份认证作用

VPN 网关对接入 VPN 的用户进行身份认证，保证接入的用户都是合法用户。

02 数据加密作用

将明文通过加密技术成密文，哪怕信息被截获窃取了，也无法识别。

注意：保证数据的加密特性，会使用到对称加密技术，和非对称加密技术。

03. 数据验证作用

通过数据验证技术验证报文的完整性和真伪进行检查，防止数据被篡改。

不同 VPN 隧道身份认证、数据加密、数据验证区别如下表所示：

序号	VPN类型	身份认证	数据加密和验证	备注
01	GRE	不支持	支持 简单的关键字验证、检验	可以结合IPsec使用 利用IPsec的数据加密和验证特性
02	L2TP	支持 基于PPP的chap pap eap认证	不支持	可以结合IPsec使用 利用IPsec的数据加密和验证特性
03	IPsec	支持	支持	支持预共享密钥验证或证书认证 支持IKEv2的EAP认证
04	SSL	支持	支持	支持用户名/密码或证书认证
05	MPLS	不支持	不支持	一般运行在专用的VPN骨干网络

1.3 专用网络开源产品

1.3.1 开源产品分类介绍

01 PPTP VPN

点对点隧道协议（PPTP）是由包括微软和 3com 等公司组成的 PPTP 论坛开发的一种点对点隧道协议；

基于拨号使用的 PPP 协议，使用 PAP 或 CHAP 之类的加密算法，或者使用 Microsoft 的点对点加密算法 MPPE。

使用 PPTP VPN 的最大优势在于，无需在 windows 客户端单独安装客户端软件，默认就支持 PPTP VPN 拨号连接功能。

适用场景：适合远程的企业用户拨号到企业内部进行办公等的应用。

开源软件：pptp vpn

02 IPsec VPN

IPSec 隧道模式是封装、路由与解封装的整个过程。隧道将原始数据包隐藏（或封装）在新的数据包内部；

隧道与数据保密性结合使用时，在网络上窃听通讯的人将无法获取原始数据包数据（以及原始的源和目标）；

适用场景：企业异地两地总分公司或多个 IDC 机房之间的 VPN 不间断按需连接

开源软件：openswan

03 SSL VPN

SSL VPN 提供了数据私密性、端点验证、信息完整性等特性；

SSL 独立于应用，因此任何一个应用程序都可以享受它的安全性而不必理会执行细节。http+ssl == https

适用场景：企业异地或者移动用户拨号连接总部实现 VPN 不间断按需连接

开源软件：openvpn

注意：属于 C/S 架构的软件，需要单独安装 openvpn 客户端与服务端。

1.3.2 开源产品工作原理

openvpn 工作原理--部署过程 每一步在做什么

- 需要先关注保证数据安全传输的三要素：数据机密性 数据完整性 身份认证
- 需要掌握秘钥加密技术应用实现；
- 需要掌握证书概念的企业应用；

1.4 虚拟专用网络部署

1.4.1 虚拟专用网络部署架构

在部署构建 openvpn 虚拟专用网络前，需要准备好基本的架构环境：

序号	主机名称	地址规划(外网)	地址规划 (内网)	系统环境
01	vpnsrver	192.168.30.101/24	172.16.30.101/24	centos 7.9
02	vpnclient	192.168.30.1/24		window 10
03	webserver	N/A	172.16.30.102/24	centos 7.9

1.4.2 操作系统基础优化配置

01 系统默认 selinux 安全策略优化说明

```
1. # 临时关闭 selinux 策略
2. [root@oldboy ~]# setenforce 0
3. [root@oldboy ~]# getenforce
4. Permissive
5.
6. # 永久关闭 selinux 策略
7. [root@oldboy ~]# cat /etc/selinux/config
8. # This file controls the state of SELinux on the system.
9. # SELINUX= can take one of these three values:
10. #     enforcing - SELinux security policy is enforced.
11. #     -- 表示 selinux 安全策略功能是启用状态
12. #     permissive - SELinux prints warnings instead of enforcing.
13. #     -- 表示 selinux 安全策略只是显示警告信息，不会进行安全处理
14. #     disabled - No SELinux policy is loaded.
15. #     -- 表示 selinux 安全策略功能彻底禁用
```



```
16. SELINUX=enforcing
17. [root@oldboy ~]# sed -
    i '7s#enforcing#disabled#g' /etc/selinux/config
18. [root@oldboy ~]# reboot
```

02 系统默认防火墙服务优化说明

```
1. # 临时关闭防火墙
2. [root@oldboy ~]# systemctl stop firewalld.service
3.
4. # 永久关闭防火墙
5. [root@oldboy ~]# systemctl disable firewalld.service
6. Removed symlink /etc/systemd/system/multi-
    user.target.wants/firewalld.service.
7. Removed symlink /etc/systemd/system/dbus-
    org.fedoraproject.FirewallD1.service.
8.
9. # 操作配置查看确认
10. [root@oldboy ~]# systemctl status firewalld
11. firewalld.service - firewalld - dynamic firewall daemon
12. Loaded: loaded (/usr/lib/systemd/system/firewalld.service; disabled;
    vendor preset: enabled)
13. Active: inactive (dead)
14. [root@oldboy ~]# systemctl is-active firewalld.service
15. unknown
16. [root@oldboy ~]# systemctl is-enabled firewalld.service
17. disabled
```

03 系统软件程序下载优化方法

```
1. # 配置官方源更新地址:
2. [root@oldboy ~]# curl -s -o /etc/yum.repos.d/CentOS-
    Base.repo https://mirrors.aliyun.com/repo/Centos-7.repo
3.
4. # 配置第三方 epel 源更新地址:
5. [root@oldboy ~]# curl -s -
    o /etc/yum.repos.d/epel.repo http://mirrors.aliyun.com/repo/epel-
    7.repo
```

04 系统基础软件程序下载安装

```
1. # 企业应用基础工具程序:
2. [root@oldboy ~]# yum install -
    y tree nmap lrzsz dos2unix nc lsof wget -y
3.
4. # 企业应用扩展工具程序:
```

```
5. [root@oldboy ~]# yum install -y psmisc net-tools bash-completion vim-enhanced git -y
```

1.4.3 虚拟专用网络证书制作

根据之前的 openvpn 软件工作原理说明，在部署虚拟专用网络服务之前，需要进行相关证书文件制作；

证书文件制作过程，需要使用到 easy-rsa-old.zip 工具进行制作证书。

制作证书工具下载：<https://github.com/OpenVPN/easy-rsa-old>

将证书制作工具上传到主机中：

```
1. # 上传证书制作工具
2. [root@xiaoQ ~]# rz -y
3. [root@xiaoQ ~]# ll easy-rsa-old-master.zip
4. -rw-r--r--. 1 root root 59661 6月 21 03:56 easy-rsa-old-master.zip
5.
6. # 解压证书制作工具压缩包
7. [root@xiaoQ ~]# unzip easy-rsa-old-master.zip
8.
9. # 查看证书制作工具命令信息
10. [root@xiaoQ ~]# cd easy-rsa-old-master/easy-rsa/2.0/
11. [root@xiaoQ 2.0]# ls
12. build-ca      build-key      build-key-server  clean-
    all          openssl-0.9.6.cnf  pkitool          vars
13. build-dh      build-key-pass  build-req          inherit-
    inter  openssl-0.9.8.cnf  revoke-full  whichopensslcnf
14. build-inter  build-key-pkcs12  build-req-pass  list-
    crl          openssl-1.0.0.cnf  sign-req
```

编写 vars 文件，修改证书创建的配置文件参数信息：

```
1. # 编辑证书创建配置参数文件
2. [root@xiaoQ 2.0]# vim vars
3. 67 export KEY_COUNTRY="cn"
4. 68 export KEY_PROVINCE="beijing"
5. 69 export KEY_CITY="beijing"
6. 70 export KEY_ORG="oldboy"
7. 71 export KEY_EMAIL="test@qq.com"
8. 72 export KEY_CN=xiaoq
9. 73 export KEY_NAME=xiaoq
10. 74 export KEY_OU=xiaoq
11. 75 export PKCS11_MODULE_PATH=changeme
```

```

12. 76 export PKCS11_PIN=1234
13. -- 以上信息表示证书请求文件的参数信息
14.
15. # 加载配置文件修改参数信息
16. [root@xiaoQ 2.0]# source vars
17. NOTE: If you run ./clean-all, I will be doing a rm -rf on /root/easy-
    rsa-old-master/easy-rsa/2.0/keys
18. -- 执行./clean-all 会在目录中创建出 keys 目录，专门用于存放证书文件信息
19. [root@xiaoQ 2.0]# ./clean-all
20. [root@xiaoQ 2.0]# ls
21. .. 省略部署信息...
22. keys
23. -- 此目录中稍后会生成所创建的证书和私钥文件信息

```

生成根证书文件和私钥文件信息：

```

1. [root@xiaoQ 2.0]# ./build-ca
2. Generating a 4096 bit RSA private key
3. ....++
4. ....++
5. writing new private key to 'ca.key'
6. -----
7. You are about to be asked to enter information that will be incorpora
    ted
8. into your certificate request.
9. What you are about to enter is what is called a Distinguished Name or
    a DN.
10. There are quite a few fields but you can leave some blank
11. For some fields there will be a default value,
12. If you enter '.', the field will be left blank.
13. -----
14. Country Name (2 letter code) [cn]:
15. State or Province Name (full name) [beijing]:
16. Locality Name (eg, city) [beijing]:
17. Organization Name (eg, company) [oldboy]:
18. Organizational Unit Name (eg, section) [xiaoq]:
19. Common Name (eg, your name or your server's hostname) [xiaoq]:
20. Name [xiaoq]:
21. Email Address [test@qq.com]:
22. -- 一路回车操作，用于产生根证书和私钥文件信息
23.
24. [root@xiaoQ 2.0]# ll keys/
25. 总用量 12
26. -rw-r--r--. 1 root root 2346 6月 21 04:14 ca.crt -- 根证书
27. -rw-----. 1 root root 3272 6月 21 04:14 ca.key -- 私钥

```

生成服务端证书和密钥文件信息：

```
1. [root@xiaoQ 2.0]# ./build-key-server server
2. Generating a 4096 bit RSA private key
3. .....
   .....++
4. .....
   .....++
5. writing new private key to 'server.key'
6. -----
7. You are about to be asked to enter information that will be incorporated
   into your certificate request.
9. What you are about to enter is what is called a Distinguished Name or
   a DN.
10. There are quite a few fields but you can leave some blank
11. For some fields there will be a default value,
12. If you enter '.', the field will be left blank.
13. -----
14. Country Name (2 letter code) [cn]:
15. State or Province Name (full name) [beijing]:
16. Locality Name (eg, city) [beijing]:
17. Organization Name (eg, company) [oldboy]:
18. Organizational Unit Name (eg, section) [xiaoq]:
19. Common Name (eg, your name or your server's hostname) [server]:
20. Name [xiaoq]:
21. Email Address [test@qq.com]:
22.
23. Please enter the following 'extra' attributes
24. to be sent with your certificate request
25. A challenge password []:
26. An optional company name []:
27. Using configuration from /root/easy-rsa-old-master/easy-
    rsa/2.0/openssl-1.0.0.cnf
28. Check that the request matches the signature
29. Signature ok
30. The Subject's Distinguished Name is as follows
31. countryName          :PRINTABLE:'cn'
32. stateOrProvinceName  :PRINTABLE:'beijing'
33. localityName         :PRINTABLE:'beijing'
34. organizationName     :PRINTABLE:'oldboy'
35. organizationalUnitName:PRINTABLE:'xiaoq'
36. commonName           :PRINTABLE:'server'
37. name                 :PRINTABLE:'xiaoq'
```

```

38. emailAddress          :IA5STRING:'test@qq.com'
39. Certificate is to be certified until Jun 17 20:19:13 2032 GMT (3650 d
    ays)
40. Sign the certificate? [y/n]:y
41.
42.
43. 1 out of 1 certificate requests certified, commit? [y/n]y
44. Write out database with 1 new entries
45. Data Base Updated
46. -- 一路回车操作, 最后输入两个 y, 用于产生服务端证书和私钥文件信息
47.
48. [root@xiaoQ 2.0]# ll keys/
49. -rw-r--r--. 1 root root 8090 6月 21 04:19 server.crt -- 服务端证
    书
50. -rw-r--r--. 1 root root 1752 6月 21 04:19 server.csr -- 服务端请求
    证书文件
51. -rw-----. 1 root root 3272 6月 21 04:19 server.key -- 服务端私钥
    文件[root@xiaoQ 2.0]# ./build-key-server server
52. Generating a 4096 bit RSA private key
53. .....
    .....++
54. .....
    .....++
55. writing new private key to 'server.key'
56. -----
57. You are about to be asked to enter information that will be incorpora
    ted
58. into your certificate request.
59. What you are about to enter is what is called a Distinguished Name or
    a DN.
60. There are quite a few fields but you can leave some blank
61. For some fields there will be a default value,
62. If you enter '.', the field will be left blank.
63. -----
64. Country Name (2 letter code) [cn]:
65. State or Province Name (full name) [beijing]:
66. Locality Name (eg, city) [beijing]:
67. Organization Name (eg, company) [oldboy]:
68. Organizational Unit Name (eg, section) [xiaoq]:
69. Common Name (eg, your name or your server's hostname) [server]:
70. Name [xiaoq]:
71. Email Address [test@qq.com]:
72.
73. Please enter the following 'extra' attributes

```

```
74. to be sent with your certificate request
75. A challenge password []:
76. An optional company name []:
77. Using configuration from /root/easy-rsa-old-master/easy-
    rsa/2.0/openssl-1.0.0.cnf
78. Check that the request matches the signature
79. Signature ok
80. The Subject's Distinguished Name is as follows
81. countryName          :PRINTABLE:'cn'
82. stateOrProvinceName  :PRINTABLE:'beijing'
83. localityName         :PRINTABLE:'beijing'
84. organizationName     :PRINTABLE:'oldboy'
85. organizationalUnitName:PRINTABLE:'xiaoq'
86. commonName           :PRINTABLE:'server'
87. name                 :PRINTABLE:'xiaoq'
88. emailAddress         :IA5STRING:'test@qq.com'
89. Certificate is to be certified until Jun 17 20:19:13 2032 GMT (3650 d
    ays)
90. Sign the certificate? [y/n]:y
91.
92.
93. 1 out of 1 certificate requests certified, commit? [y/n]y
94. Write out database with 1 new entries
95. Data Base Updated
96. -- 一路回车操作，最后输入两个 y，用于产生服务端证书和私钥文件信息
97.
98. [root@xiaoQ 2.0]# ll keys/
99. -rw-r--r--. 1 root root 8090 6月 21 04:19 server.crt -- 服务端证
    书
100. -rw-r--r--. 1 root root 1752 6月 21 04:19 server.csr -- 服务端请
    求证书文件
101. -rw-----. 1 root root 3272 6月 21 04:19 server.key -- 服务端私
    钥文件[root@xiaoQ 2.0]# ./build-ca
102. Generating a 4096 bit RSA private key
103. ...++
104. ....++
105. writing new private key to 'ca.key'
106. -----
107. You are about to be asked to enter information that will be incorp
    orated
108. into your certificate request.
109. What you are about to enter is what is called a Distinguished Name
    or a DN.
110. There are quite a few fields but you can leave some blank
```

```

111. For some fields there will be a default value,
112. If you enter '.', the field will be left blank.
113. -----
114. Country Name (2 letter code) [cn]:
115. State or Province Name (full name) [beijing]:
116. Locality Name (eg, city) [beijing]:
117. Organization Name (eg, company) [oldboy]:
118. Organizational Unit Name (eg, section) [xiaoq]:
119. Common Name (eg, your name or your server's hostname) [xiaoq]:
120. Name [xiaoq]:
121. Email Address [test@qq.com]:
122. -- 一路回车操作，用于产生根证书和私钥文件信息
123.
124. [root@xiaoQ 2.0]# ll keys/
125. 总用量 12
126. -rw-r--r--. 1 root root 2346 6月 21 04:14 ca.crt -- 根证书
127. -rw----- 1 root root 3272 6月 21 04:14 ca.key -- 私钥

```

生成客户端证书和秘钥文件信息：

```

1. [root@xiaoQ 2.0]# ./build-key client
2. Generating a 4096 bit RSA private key
3. ....++
4. ....
   .....
   .....
   .....++
5. writing new private key to 'client.key'
6. -----
7. You are about to be asked to enter information that will be incorporated
   into your certificate request.
9. What you are about to enter is what is called a Distinguished Name or
   a DN.
10. There are quite a few fields but you can leave some blank
11. For some fields there will be a default value,
12. If you enter '.', the field will be left blank.
13. -----
14. Country Name (2 letter code) [cn]:
15. State or Province Name (full name) [beijing]:
16. Locality Name (eg, city) [beijing]:
17. Organization Name (eg, company) [oldboy]:
18. Organizational Unit Name (eg, section) [xiaoq]:
19. Common Name (eg, your name or your server's hostname) [client]:
20. Name [xiaoq]:

```

```

21. Email Address [test@qq.com]:
22.
23. Please enter the following 'extra' attributes
24. to be sent with your certificate request
25. A challenge password []:
26. An optional company name []:
27. Using configuration from /root/easy-rsa-old-master/easy-
    rsa/2.0/openssl-1.0.0.cnf
28. Check that the request matches the signature
29. Signature ok
30. The Subject's Distinguished Name is as follows
31. countryName          :PRINTABLE:'cn'
32. stateOrProvinceName  :PRINTABLE:'beijing'
33. localityName         :PRINTABLE:'beijing'
34. organizationName     :PRINTABLE:'oldboy'
35. organizationalUnitName:PRINTABLE:'xiaoq'
36. commonName           :PRINTABLE:'client'
37. name                 :PRINTABLE:'xiaoq'
38. emailAddress         :IA5STRING:'test@qq.com'
39. Certificate is to be certified until Jun 17 20:23:35 2032 GMT (3650 d
    ays)
40. Sign the certificate? [y/n]:y
41.
42.
43. 1 out of 1 certificate requests certified, commit? [y/n]y
44. Write out database with 1 new entries
45. Data Base Updated
46. -- 一路回车操作，最后输入两个y，用于产生客户端证书和私钥文件信息
47.
48. [root@xiaoQ 2.0]# ll keys/
49. -rw-r--r--. 1 root root 7972 6月 21 04:23 client.crt -- 客户端证书
50. -rw-r--r--. 1 root root 1752 6月 21 04:23 client.csr -- 客户端请求证
    书文件
51. -rw-----. 1 root root 3272 6月 21 04:23 client.key -- 客户端私钥

```

生成秘钥交换文件信息：

```

1. [root@xiaoQ 2.0]# ./build-dh
2. Generating DH parameters, 2048 bit long safe prime, generator 2
3. This is going to take a long time
4. ....
5. -- 用于产生秘钥交换文件信息
6.
7. [root@xiaoQ 2.0]# ll keys/
8. -rw-r--r--. 1 root root 424 6月 21 04:27 dh2048.pem

```


注意：利用证书制作工具 easy-ras.zip，最终会生成重要的 7 个文件，ca 两个，server 两个，client 两个，秘钥交换一个。

1.4.4 虚拟专用网络服务配置

在安装部署虚拟专用网络服务时，需要对 openvpn 服务配置文件进行修改调整；

下载安装 openvpn 服务程序包：`[root@xiaoQ ~]# yum install -y openvpn`

编写修改 openvpn 服务配置文件：

```
1. # 建立存放 openvpn 服务加载证书文件目录
2. [root@xiaoQ ~]# cd /etc/openvpn/
3. [root@xiaoQ openvpn]# mkdir keys
4.
5. # 将之前生成的证书文件信息进行拷贝迁移
6. [root@xiaoQ openvpn]# cp /root/easy-rsa-old-master/easy-rsa/2.0/keys/server.crt ./keys/
7. [root@xiaoQ openvpn]# cp /root/easy-rsa-old-master/easy-rsa/2.0/keys/server.key ./keys/
8. [root@xiaoQ openvpn]# cp /root/easy-rsa-old-master/easy-rsa/2.0/keys/ca.crt ./keys/
9. [root@xiaoQ openvpn]# cp /root/easy-rsa-old-master/easy-rsa/2.0/keys/dh2048.pem ./keys/
10.
11. # 检查确认是否拷贝迁移成功
12. [root@xiaoQ openvpn]# ll ./keys/
13. 总用量 20
14. -rw-r--r--. 1 root root 2346 6月 21 04:38 ca.crt
15. -rw-r--r--. 1 root root 424 6月 21 04:38 dh2048.pem
16. -rw-r--r--. 1 root root 8090 6月 21 04:38 server.crt
17. -rw-----. 1 root root 3272 6月 21 04:38 server.key
18.
19. # 拷贝 openvpn 服务模板配置文件
20. [root@xiaoQ openvpn]# cp /usr/share/doc/openvpn-2.4.12/sample/sample-config-files/server.conf ./
21. [root@xiaoQ openvpn]# ll server.conf
22. -rw-r--r--. 1 root root 10784 6月 21 04:41 server.conf
23.
24. # 编辑 openvpn 服务模板配置文件
25. [root@xiaoQ openvpn]# vim server.conf
```

```

26. 78 ca keys/ca.crt
27. 79 cert keys/server.crt
28. 80 key keys/server.key # This file should be kept secret
29. 85 dh keys/dh2048.pem
30. -- 更改配置加载的证书文件路径信息
31. 101 server 10.0.1.0 255.255.255.0
32. -- 当vpn拨号建立连接成功后，会生成的隧道连接网段信息
33. 143 push "route 10.0.1.0 255.255.255.0"
34. 144 push "route 172.16.30.0 255.255.255.0"
35. -- 表示路由信息推送，可以让拨号的客户端主机路由表中，添加以上两个路由条目信息；
36. -- 最终实现和企业私网以及vpn隧道私网建立通信
37. 246 tls-auth keys/ta.key 0
38. -- 表示拒绝服务攻击的证书
39. 254 cipher AES-256-GCM
40. -- 表示设置数据传输的加密模式，从2.4版本之后不能使用CBC模式了，需要改为GCM

```

设置开启 openvpn 服务路由转发：

```

1. [root@xiaoQ openvpn]# echo "net.ipv4.ip_forward = 1" >>/etc/sysctl.conf
2. [root@xiaoQ openvpn]# sysctl -p
3. net.ipv4.ip_forward = 1
4. -- 实现让vpn服务器具有路由器的功能，进行数据包的路由转发。

```

在 openvpn 服务端建立 ta.key 文件，主要用于拒绝服务攻击证书文件：

```

1. [root@xiaoQ openvpn]# cd keys/
2. [root@xiaoQ keys]# pwd
3. /etc/openvpn/keys
4. [root@xiaoQ keys]# openvpn --genkey --secret ta.key
5. [root@xiaoQ keys]# ls
6. ta.key
7. -- 生成此文件主要作用就是加固openvpn服务的安全性

```

启动运行 openvpn 服务程序：

```

1. [root@xiaoQ openvpn]# pwd
2. /etc/openvpn
3. [root@xiaoQ openvpn]# openvpn --daemon --config server.conf
4. [root@xiaoQ openvpn]# netstat -lntup | grep 1194
5. udp        0      0 0.0.0.0:1194      0.0.0.0:*
               2238/openvpn

```

1.4.5 虚拟专用网络客户配置

缩写配置 openvpn 客户端程序配置文件：

```

1. # 创建保存客户端文件信息的目录，并将客户端模板文件进行拷贝迁移
2. [root@xiaoQ ~]# mkdir client
3. [root@xiaoQ ~]# cp /usr/share/doc/openvpn-2.4.12/sample/sample-
   config-files/client.conf /root/client/
4.
5. # 编写客户端配置文件信息：
6. [root@xiaoQ ~]# vim client/client.conf
7. 44 remote 192.168.30.101 1194
8. -- 表示设置客户端要和哪个 vpn 服务器建立连接，设置为 vpn 服务器外网接口公网地
   址和服务端口 1194 信息
9. 116 cipher AES-256-GCM
10. -- 表示设置数据传输的加密模式，从 2.4 版本之后不能使用 CBC 模式了，需要改为
   GCM

```

导出保存 openvpn 客户端证书相关文件：

```

1. # 汇总拷贝整理客户端相关证书文件
2. [root@xiaoQ ~]# cp easy-rsa-old-master/easy-
   rsa/2.0/keys/client.key /root/client/
3. [root@xiaoQ ~]# cp easy-rsa-old-master/easy-
   rsa/2.0/keys/client.crt /root/client/
4. [root@xiaoQ ~]# cp easy-rsa-old-master/easy-
   rsa/2.0/keys/ca.crt /root/client/
5. [root@xiaoQ ~]# cp /etc/openvpn/keys/ta.key /root/client/
6.
7. # 检查确认客户端数据信息情况
8. [root@xiaoQ ~]# ll /root/client/
9. 总用量 24
10. -rw-r--r--. 1 root root 2346 6月 21 05:17 ca.crt
11. -rw-r--r--. 1 root root 3613 6月 21 05:15 client.conf
12. -rw-r--r--. 1 root root 7972 6月 21 05:17 client.crt
13. -rw-----. 1 root root 3272 6月 21 05:17 client.key
14. -rw-----. 1 root root 636 6月 21 05:17 ta.key
15.
16. # 修改客户端文件后缀名称信息
17. [root@xiaoQ ~]# cd /root/client/
18. [root@xiaoQ client]# mv client.conf client.ovpn
19. [root@xiaoQ client]# ll client.ovpn
20. -rw-r--r--. 1 root root 3613 6月 21 05:15 client.ovpn

```

将所有 openvpn 客户端所需的文件数据打包并下载保存

```

1. [root@xiaoQ ~]# pwd
2. /root
3. [root@xiaoQ ~]# zip client.zip client/*
4. adding: client/ (stored 0%)

```

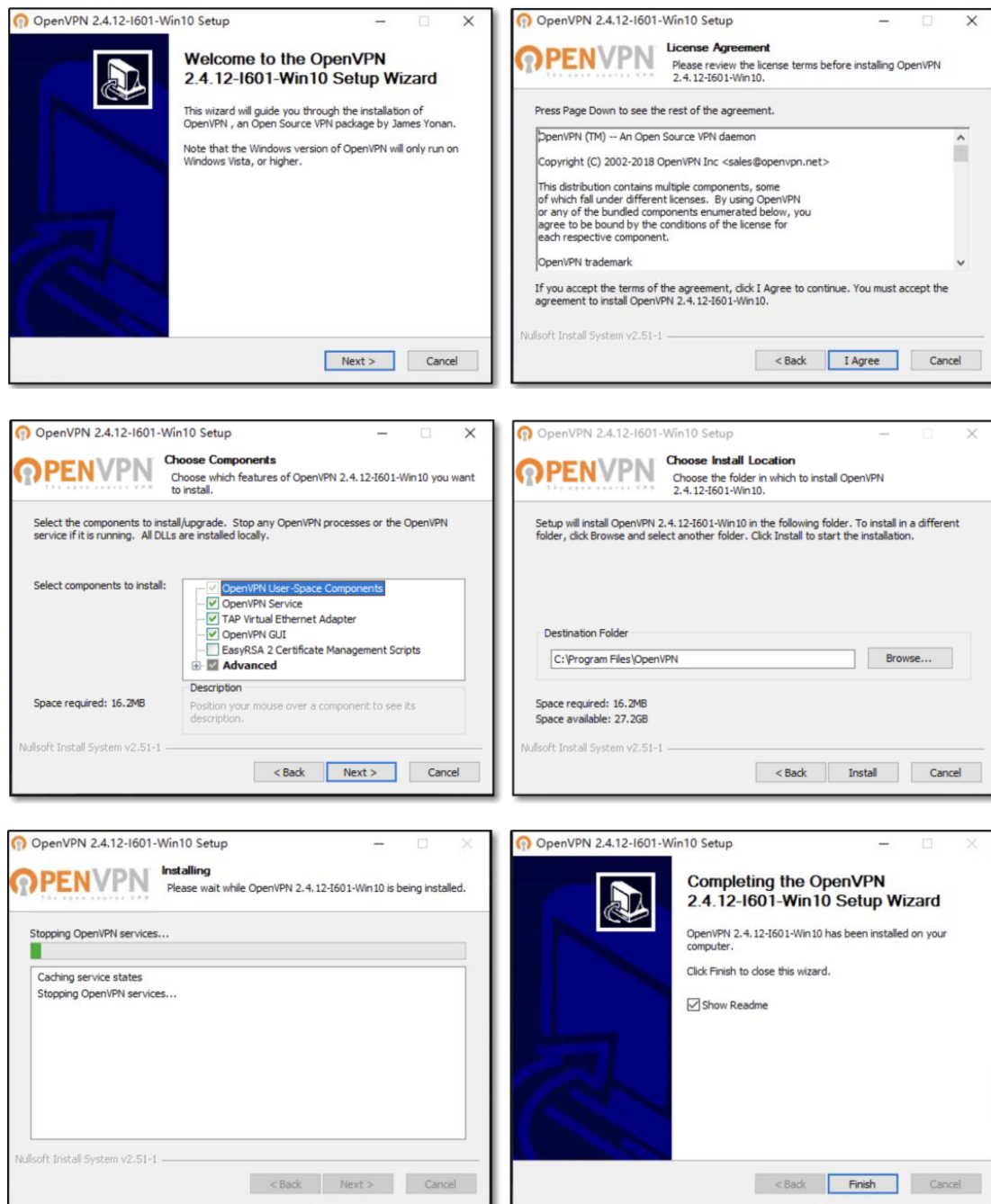
```
5. [root@xiaoQ ~]# ll client.zip
6. -rw-r--r--. 1 root root 164 6月 21 05:21 client.zip
7. [root@xiaoQ ~]# sz -y client.zip
```

1.4.6 虚拟专用网络连接设置

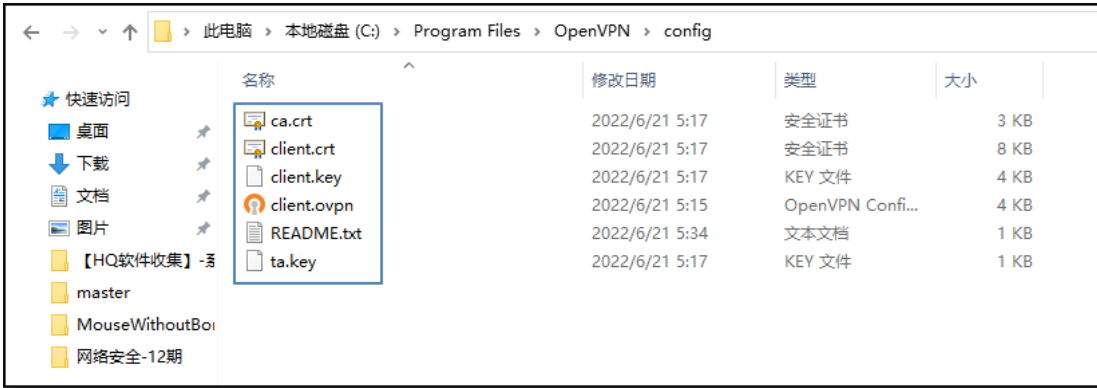
在 windows 10 系统上安装 openvpn 服务客户端软件程序：

客户端程序下载地址：<https://openvpn.net/community-downloads/>

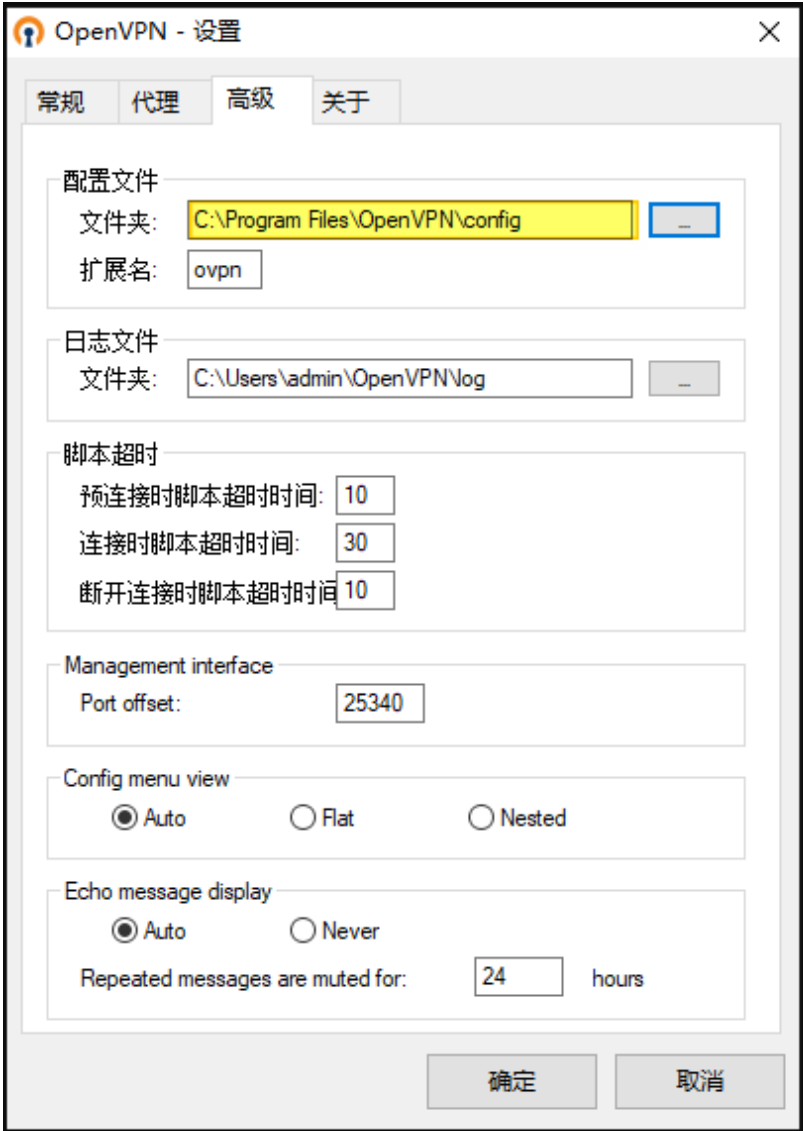
进行软件傻瓜式安装部署：



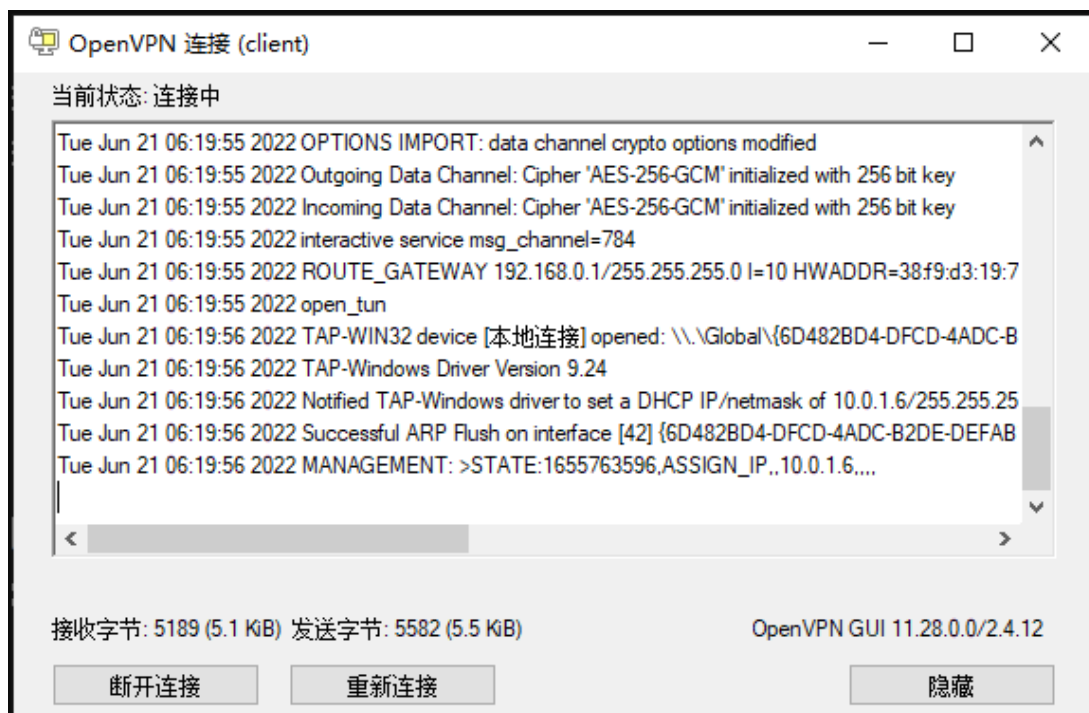
运行启动客户端软件程序，并将之前下载的客户端相关证书与配置文件导入到客户端软件程序中：



修改客户端程序设置中的高级选项配置信息：



配置完毕后，运行程序建立连接：



1.4.7 虚拟专用网络检查测试

检查虚拟专用网络客户端主机是否已经获取了建立 VPN 隧道的地址信息：

```
1. C:\windows\system32>ipconfig
2. 未知适配器 本地连接:
3.     连接特定的 DNS 后缀 . . . . . :
4.     本地链接 IPv6 地址. . . . . : fe80::5037:b117:fdb5:894%42
5.     IPv4 地址 . . . . . : 10.0.1.6
6.     子网掩码 . . . . . : 255.255.255.252
7.     默认网关. . . . . :
```

查看虚拟专用网络客户端主机系统路由表信息：

```
1. C:\windows\system32>route print
2. 172.16.30.0    255.255.255.0        10.0.1.5        10.0.1.6        281
```

进行内网地址信息连接测试：

```
1. # 测试 VPN 服务端局域接口已经连通
2. C:\windows\system32>ping 172.16.30.101
3. 正在 Ping 172.16.30.101 具有 32 字节的数据:
4. 来自 172.16.30.101 的回复: 字节=32 时间<1ms TTL=64
5. 来自 172.16.30.101 的回复: 字节=32 时间=1ms TTL=64
6.
```

```
7. # 测试企业内网主机连通失败
8. C:\windows\system32>ping 172.16.30.102
9.
10. 正在 Ping 172.16.30.102 具有 32 字节的数据:
11. 请求超时。
12. 请求超时。
13. 请求超时。
```

修改调整内网主机数据通讯配置信息：

```
1. # 方式一：添加网关路由信息
2. route add default gw 172.16.30.101
3.
4. # 方式二：配置防火墙 NAT 映射规则
5. iptables -t nat -A POSTROUTING -s 10.0.1.0/24 -j MASQUERADE
```