联软科技
LEAGSOFT

LeagSoft UniVPN 客户端

终端用户接入指南

目 录

1 文档信息 1

2 从这里开始 4

3 安装软件 6

3.1 安装前须知 7

3.2 获取软件安装包 8

3.3 在 Windows 操作系统上安装软件 9

3.4 在 Linux 操作系统上安装软件 10

3.5 在 Mac OS 操作系统上安装软件 12

3.6 在国产化操作系统上安装软件 12

4 配置 VPN 连接 15

4.1 配置 SSL VPN 连接 16

4.2 配置 L2TP VPN 连接 18

4.3 配置 L2TP over IPSec VPN 连接 21

4.4 通过导入配置文件的方式配置 VPN 连接 27

5 建立 VPN 连接 30

5.1 发起 VPN 连接 30

5.2 用户身份认证 32

5.2.1 通过用户名/密码认证 32

5.2.2 通过导入 PKI 数字证书认证 33

5.2.3 通过 USB-Key 证书认证 34

5.2.4 通过双因子认证 36

6 可选配置 37

6.1 卸载软件 37

6.2 更新升级 39

6.3 修改登录密码 40

6.4 其他配置 41

7 故障处理 44

7.1 收集用于故障排除的信息 44

7.1.1 收集错误报告 44
7.1.2 导出配置文件 46
7.2 安装及更新类故障 47
7.3 连接类故障 48
7.4 业务类故障 48
8 附录 51
8.1 移动客户端 51
8.1.2 证书认证场景 54
8.1.3 IOS 问题反馈 61
8.1.4 取消自动登录（安卓） 67
8.2 在 Linux 操作系统下通过命令行方式配置客户端 68
8.2.1 启动客户端 68
8.2.2 配置 SSL VPN 连接 68
8.2.3 配置 L2TP VPN 连接 70
8.2.4 配置 L2TP over IPSec VPN 连接 71
8.3 在国产化操作系统下通过命令行方式配置客户端 75
8.3.1 启动客户端 75
8.3.2 配置 SSL VPN 连接 76
8.3.3 配置 L2TP VPN 连接 78
8.3.4 配置 L2TP over IPSec VPN 连接 79
8.4 VPN 配置及连接模板 83
8.4.1 SSL VPN 配置及连接模板 83
8.4.2 L2TP VPN 配置及连接模板 85
8.4.3 L2TP over IPSec VPN 配置及连接模板 87

1 文档信息

产品版本

本文档适用于 10781.02 及以后版本的 UniVPN 客户端产品。

读者对象

本文档面向需要通过 UniVPN 客户端建立 VPN 连接的移动终端接入用户。您可以参考 **2** 从这里开始，在您的移动终端设备上完成建立 VPN 连接所需的配置，远程接入企业内网并访问企业内部资源。

配套产品及版本

产品名称	产品版本	操作系统
USG6000	V500R005C20SPC500 及以后版本	• Windows • Linux • Mac OS • 国产化
USG9500	V500R005C20SPC500 及以后版本	• Windows • Linux • .Mac OS • 国产化
USG6000E	V600R007C20SPC300 及以后版本（SPC301/SPC 302 版本除外）	• Windows • Linux • Mac OS • 国产化
Eudemon200E-N	V500R005C20SPC500 及以后版本	• Windows • Linux • Mac OS • 国产化

产品名称	产品版本	操作系统
Eudemon200E-G	V600R007C20SPC300 及以后版本（SPC301/SPC 302 版本除外）	• Windows • Linux • Mac OS • 国产化
Eudemon1000E-N	V500R005C20SPC500 及以后版本	• Windows • Linux • Mac OS • 国产化
Eudemon1000E-G	V600R007C20SPC300 及以后版本（SPC301/SPC 302 版本除外）	• Windows • Linux • Mac OS • 国产化
Eudemon8000E-X	V500R005C20SPC500 及以后版本	• Windows • Linux • Mac OS • 国产化
SeMG9811	V500R005C20SPC500 及以后版本	• Windows • Linux • Mac OS • 国产化
NGFW Module	V500R005C20SPC500 及以后版本	• Windows • Linux • Mac OS • 国产化
USG12000	V600R021C10 及以后版本	• Windows • Linux • Mac OS • 国产化
USG6000F	V600R021C10 及以后版本	• Windows • Linux • Mac OS • 国产化
Eudemon9000E-X	V600R021C10 及以后版本	• Windows • Linux • Mac OS • 国产化

产品名称	产品版本	操作系统
Eudemon9000E-F	V600R021C10 及以后版本	• Windows • Linux • Mac OS • 国产化
Eudemon1000E-F	V600R021C10 及以后版本	• Windows • Linux • Mac OS • 国产化

修订记录

文档版本 03（2022-08-30）

第三次正式发布，配套 UniVPN10781.5.0

文档版本 02（2022-07-30）

第二次正式发布，配套 UniVPN10781.03

文档版本 01 (2021-12-30)

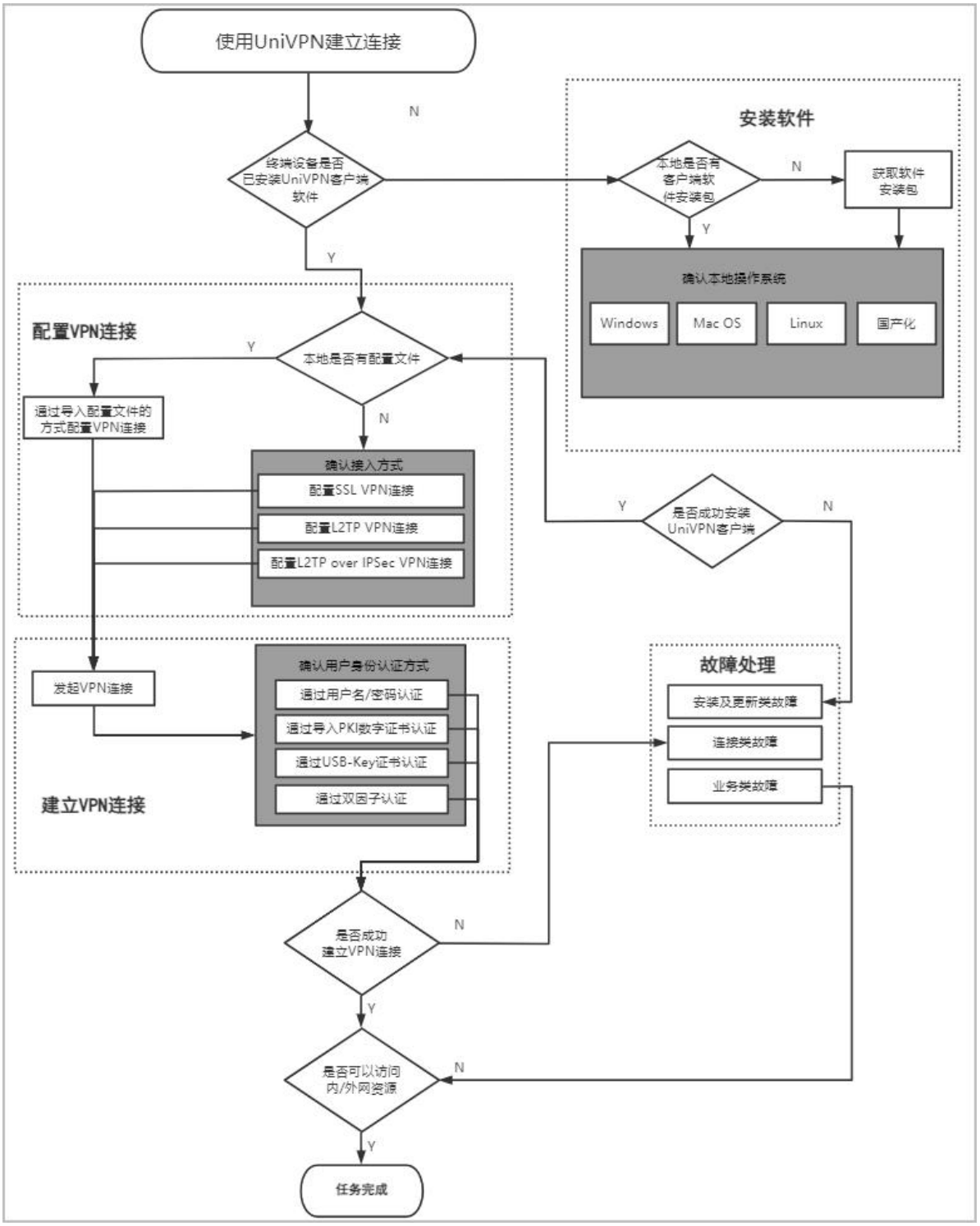
第一次正式发布，配套 UniVPN 10781.02 版本。

2 从这里开始

UniVPN 客户端是深圳市联软科技股份有限公司推出的一款用于 VPN 远程接入的终端软件，主要为移动办公用户远程访问企业内网资源提供安全、便捷的接入服务。

对于初次使用本软件的用户，可以参考图 2-1 中的任务地图，一步步完成建立 VPN 连接所需的配置操作。

图 2-1 终端设备接入用户任务地图



3 安装软件

使用 UniVPN 客户端建立 VPN 连接前，首先需要确保客户端软件已经完整、正确的安装到终端设备上。如果您的终端设备上未安装 UniVPN 客户端，请参考下文中的步骤进行安装。

1. 安装软件前，请您仔细阅读 **3.1** 安装前须知，了解软件安装的注意事项及系统配置要求。
2. 如果您的终端设备上没有提供配套对应操作系统的UniVPN客户端软件安装包或安装包的版本过于老旧，请先 **3.2** 获取软件安装包。
3. UniVPN 客户端目前支持 Windows、Mac OS、Linux 和国产化四种操作系统环境，并针对四种操作系统提供了不同格式的软件安装包。如果您已经获取到配套您终端设备操作系统环境的软件安装包，请参考以下节点的配置步骤安装软件：
   - **3.3** 在 Windows 操作系统上安装软件
   - **3.4** 在 Linux 操作系统上安装软件
   - **3.5** 在 Mac OS 操作系统上安装
   - **3.6** 在国产化操作系统上安装

3.1 安装前须知

安装和使用 UniVPN 客户端前，请仔细阅读下文中的内容。了解软件安装的注意事项，并确认您的终端设备系统配置满足要求。

3.2 获取软件安装包

下文中列出了 UniVPN 客户端软件安装包常见的几种获取途径。在实际的任务场景中，软件安装包的获取途径由企业网络管理员进行规划与部署，并最终告知终端接入用户。

3.3 在 Windows 操作系统上安装软件

UniVPN 客户端对 32 位和 64 位的 Windows 操作系统提供了统一软件安装包，请您根据当前使用的终端设备的操作系统环境选择正确的安装包。

3.4 在 Linux 操作系统上安装软件

UniVPN 客户端仅支持 64 位的 Ubuntu 20.04 操作系统。

3.5 在 Mac OS 操作系统上安装软件

UniVPN 客户端仅支持 64 位的 Mac OS 操作系统。

3.6 在国产化操作系统上安装软件

UniVPN 客户端仅支持银河麒麟操作系统。

3.1 安装前须知

安装和使用 UniVPN 客户端前，请仔细阅读下文中的内容。了解软件安装的注意事项，并确认您的终端设备的系统配置满足要求。

注意事项

- 安装或卸载软件时，请使用具有管理员权限的用户名和密码登录操作系统。
- 请勿在同一台终端设备上同时安装或使用多个 VPN 拨号软件，否则可能会导致 VPN 拨号软件或操作系统异常。
- 如果您的终端设备上之前已经安装了 UniVPN 客户端，则运行安装程序时会弹出提示要求您覆盖安装 UniVPN 客户端。您可以先根据提示操作或删除已经安装的旧版本客户端软件，并再次运行安装程序，将新版本的客户端软件安装到硬盘上。

系统配置要求

表 3-1 UniVPN 客户端的系统配置要求

系统配置项	配置要求			
操作系统环境	Windows	Linux	Mac OS	国产化

系统配置项	配置要求			
操作系统版本	• Windows 7（32 位/64 位） • Windows 8（32 位/64 位） • Windows 8.1（32 位/64 位） • Windows 10（32 位/64 位） • Windows Server 2008（32 位/64 位） • Windows Server 2012（64 位） • Windows 11	• Ubuntu-20.04（64 位）	• OS X 10.11.x（64 位） • OS X 10.12.x（64 位） • OS X 10.13.x（64 位） • OS X 10.14.x（64 位） • OS X 10.15.x（64 位） • OS X 11.x.x（64 位） • OS X 12.x.x（64 位）	• 银河麒麟+龙芯 linux4.4.131（3A3000） • 银河麒麟+龙芯 linux5.4.18（3A4000）
硬件资源要求	UniVPN 对操作系统的内存、硬盘、CPU 等软硬件资源没有特殊要求。			

3.2 获取软件安装包

下文中列出了 UniVPN 客户端软件安装包常见的几种获取途径。在实际的任务场景中，软件安装包的获取途径由企业网络管理员进行规划与部署，并最终告知终端接入用户。

开始之前

获取软件安装包之前，请先确认您的终端设备上搭载的操作系统环境及版本符合 **3.1** 安装前须知中的系统配置要求，并获取与您的操作系统环境相配套的软件安装包。

软件安装包的常见获取途径

1. 您可以**从您所在企业的网络管理人员处直接获取软件安装包**，上传并安装到您的终端设备上。
2. 您还可以登录网站 https://www.leagsoft.com，在首页进入“产品与方案 > 通用方案 > Uni VPN Client 远程接入终端方案”，在 UniVPN 介绍页面最下方单击链接下载对应版本的软件安装包。

说明

由于 SSL VPN 的用户认证方式不同，获取的用户登录信息和进行的操作存在如下差异，具体的用户认证方式请与企业网络管理员确认。

- 本地认证、服务器认证：获取用户名和密码。
- 证书匿名认证：获取并安装客户端证书。
- 证书挑战认证：获取客户端证书和密码，安装客户端证书。

后续操作

UniVPN 客户端目前支持 Windows、Linux 和 Mac OS 操作系统环境，并针对三种操作系统提供了不同格式的软件安装包。如果您已经获取到配套您终端设备操作系统环境的软件安装包，请参考以下节点的配置步骤安装软件：

- **3.3** 在 Windows 操作系统上安装软件
- **3.4** 在 Linux 操作系统上安装软件
- **3.5** 在 Mac OS 操作系统上安装软件
- **3.6** 在国产化操作系统上安装软件

您还可以回到 **2** 从这里开始，参照**任务地图**进行后续配置。

3.3 在 Windows 操作系统上安装软件

UniVPN 客户端对 32 位和 64 位的 Windows 操作系统提供了统一软件安装包，请您根据当前使用的终端设备的操作系统环境选择正确的安装包。

开始之前

安装软件之前，请先确认您的终端设备上搭载的操作系统环境及版本符合 **3.1** 安装前须知中的系统配置要求。

操作步骤

步骤 1 使用具有“Administrators”权限的操作系统用户登录 Windows 操作系统。

步骤 2 双击下载的安装包，进入安装向导。

步骤 3 安装向导会引导用户完成安装任务，请根据提示逐步完成安装。

说明

- UniVPN 客户端默认会被安装在系统盘下。例如，系统安装在 C 盘下，则 UniVPN 的默认安装路径为“C:\Program Files (x86)\UniVPN”。
- 首次安装 UniVPN 客户端时，会弹出安装网卡驱动程序的提示信息，请按照安装向导的提示完成安装。

----结束

后续操作

- 成功安装 UniVPN 客户端后，您可以开始 **4** 配置 VPN 连接。
- 若安装过程中发生错误导致安装失败，请参考 **7.2** 安装及更新类故障进行故障排查和处理。
- 您还可以回到 **2** 从这里开始，参照**任务地图**进行后续配置。

3.4 在 Linux 操作系统上安装软件

UniVPN 仅对 Ubuntu 20.04 的 64 位 Linux 操作系统提供了安装包，请您根据当前的操作系统环境选择正确的安装包。

开始之前

安装软件之前，请先确认您的终端设备上搭载的操作系统环境及版本符合 **3.1** 安装前须知中的系统配置要求。

操作步骤

下面以 Ubuntu 20.04 操作系统为例进行介绍 UniVPN 的安装方法。

步骤 1 使用具有“root”权限的操作系统用户登录 Linux 操作系统。

步骤 2 将下载的客户端安装包放到主文件夹（“计算机 > home > UniVPN”）中。

步骤 3 打开“终端”，在“home/UniVPN”目录下使用 root 身份执行**./ 安装包名称.run**，安装 UniVPN 客户端。

```
root@UniVPN-virtual-machine:~# cd /home/UniVPN/
root@uniVPN-virtual-machine:/home/UniVPN# ./UniVPN-xxxxx.xx.xxx.xxxx.run
/
install.sh
uninstall.sh
sysconfig.ini
qt.conf
bak/
component/
config/
driver/
image/
image/Customized/
image/Customized/customized.ini
image/UniVPN.desktop
image/UniVPNA.desktop
image/ICON.ico
language/
language/2052/
language/2052/l_UILabel.ini
```

步骤 4 安装成功，如下所示。

```
Starting UniVPNPromoteService daemon: UniVPNPromoteService.
```

```
*****The program has been installed in directory UniVPN of your home Directory!*****
*****Enjoy!*****
```

步骤 5 单击桌面上生成的 UniVPN 客户端图标，即可启动程序并进行配置。

----结束

后续操作

- 成功安装 UniVPN 客户端后，您可以开始 **4** 配置 VPN 连接。
- 若安装过程中发生错误导致安装失败，请参考 **7.2** 安装及更新类故障进行故障排查和处理。
- 您还可以回到 **2** 从这里开始，参照**任务地图**进行后续配置。

3.5 在 Mac OS 操作系统上安装软件

UniVPN 客户端仅支持 64 位的 Mac OS 操作系统。

开始之前

安装软件之前，请先确认您的终端设备上搭载的操作系统环境及版本符合 **3.1** 安装前须知中的系统配置要求。

操作步骤

步骤 1 登录 Mac OS 操作系统。

步骤 2 双击下载好的安装包，运行安装程序。

步骤 3 安装程序会引导用户完成安装任务，请根据提示逐步完成安装。

步骤 4 安装完成后，可在应用程序文件夹中找到应用程序。

步骤 5 双击“UniVPN”，即可启动程序并进行配置。

----结束

后续操作

- 成功安装 UniVPN 客户端后，您可以开始 **4** 配置 VPN 连接。
- 若安装过程中发生错误导致安装失败，请参考 **7.1** 安装及更新类故障进行故障排查和处理。
- 您还可以回到 **2** 从这里开始，参照**任务地图**进行后续配置。

3.6 在国产化操作系统上安装软件

UniVPN 客户端仅支持国产化银河麒麟的操作系统，请您根据当前的操作系统环境选择正确的安装包。

开始之前

安装软件之前，请先确认您的终端设备上搭载的操作系统环境及版本符合 **3.1** 安装前须知中的系统配置要求。

操作步骤

方法一：

步骤 1 使用具有“root”权限的操作系统用户登录国产化操作系统。

步骤 2 在网络连接成功的情况下，打开浏览器下载对应版本的软件安装包。

登录网站 https://www.leagsoft.com，在首页进入“产品与方案 > 通用方案 > Uni VPN Client 远程接入终端方案”，在 UniVPN 介绍页面最下方单击链接下载对应版本的软件安装包。

步骤 3 将下载的客户端安装包放到主文件夹（“计算机 > home > UniVPN”）中。

步骤 4 打开“终端”，在“home/UniVPN”目录下使用 root 身份执行./ 安装包名称.deb，安装 UniVPN 客户端。

```
root@UniVPN-virtual-machine:~# cd /home/UniVPN/
root@UniVPN-virtual-machine:/home/UniVPN# dpkg UniVPN-xxxxx.xx.xxx.xxxx.deb
/
UniVPNA.sh
install.sh
uninstall.sh
sysconfig.ini
qt.conf
bak/
component/
config/
driver/
image/
language/
help/
lib/
log/
plugins/
plugins/platforms/
serviceclient/
update/
UniVPN
UniVPNUpdate
```

步骤 5 安装成功，如下所示。

```
Starting UniVPNPromoteService daemon: UniVPNPromoteService.
*****The program has been installed in directory UniVPN of your home Directory!*****
*****Enjoy!*****
```

步骤 6 单击桌面上生成的 UniVPN 客户端图标，即可启动程序并进行配置。

----结束

方法二：

步骤 1 使用具有“root”权限的操作系统用户登录国产化操作系统。

步骤 2 在网络连接成功的情况下，打开浏览器下载对应版本的软件安装包。

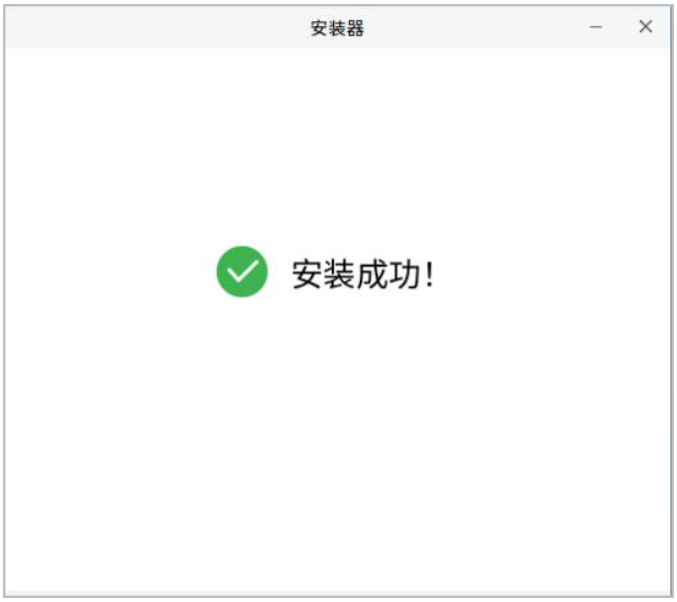
登录网站 https://www.leagsoft.com，在首页进入“产品与方案 > 通用方案 > Uni VPN Client 远程接入终端方案”，在 UniVPN 介绍页面最下方单击链接下载对应版本的软件安装包。

步骤 3 双击下载的安装包，进入安装界面，左键单击“一键安装”。

UniVPN 默认会被安装在系统盘下。例如，系统安装在/盘下，则 UniVPN 的默认安装路径为“/home/用户名/UniVPN”。

步骤 4 在授权界面输入正确的密码，单击“授权”，安装器自动完成安装。

步骤 5 安装成功，如下所示。



----结束

后续操作

- 成功安装 UniVPN 客户端后，您可以开始 **4** 配置 VPN 连接。
- 若安装过程中发生错误导致安装失败，请参考 **7.2** 安装及更新类故障进行故障排查和处理。

步骤 6 您还可以回到 **2** 从这里开始，参照**任务地图**进行后续配置

4 配置 VPN 连接

UniVPN 客户端支持通过两种方式配置 VPN 连接，一种是手工方式，另一种是配置文件方式。

使用哪种方式配置 VPN 连接取决于企业网络管理员是否向您提供了 VPN 连接配置文件。

- 若企业网络管理员已经向您提供了配置文件，您可以直接 **4.4** 通过导入配置文件的方式配置 VPN 连接。
- 若您没有获取到配置文件，则需要在客户端上通过**手工方式**配置 VPN 连接。

  在通过手工方式配置 VPN 连接时，待接入 VPN 的类型不同，需要配置的连接参数也存在差异。因此，首先需要与企业网络管理员确认待接入 VPN 的类型，并获取必要的连接参数。

  明确了待接入 VPN 的类型并获取到必要的连接参数后，请参考以下节点配置 VPN 连接：

  - **4.1** 配置 SSL VPN 连接
  - **4.2** 配置 L2TP VPN 连接
  - **4.3** 配置 L2TP over IPSec VPN 连接

Windows 操作系统和 Linux 操作系统下使用 UniVPN 配置 VPN 连接的方法基本相同，下面以 Windows 操作系统为例进行介绍。

4.1 配置 SSL VPN 连接

如果您已经与企业网络管理员确认待接入 VPN 的类型为 SSL VPN，请参考以下操作步骤配置 VPN 连接。

4.2 配置 L2TP VPN 连接

如果您已经与企业网络管理员确认待接入 VPN 的类型为 L2TP VPN，请参考以下操作步骤配置 VPN 连接。

4.3 配置 L2TP over IPSec VPN 连接

如果您已经与企业网络管理员确认待接入 VPN 的类型为 L2TP over IPSec VPN，请参考以下操作步骤配置 VPN 连接。

4.4 通过导入配置文件的方式配置 VPN 连接

配置文件是企业网络管理员利用客户端的配置文件导出功能生成的一份后缀为“.ini”的文件，其中携带了创建一条特定 VPN 连接需要配置的所有参数信息。在您获取到该配置文件后，可以将该配置文件导入到 UniVPN 中，直接生成一条配置好的 VPN 连接，从而简化您的配置工作。

4.1 配置 SSL VPN 连接

如果您已经与企业网络管理员确认待接入 VPN 的类型为 SSL VPN，请参考以下操作步骤配置 VPN 连接。

开始之前

在配置前请仔细检查如下表单，确认您已获取到建立 SSL VPN 连接所需的连接参数。

说明

您也可以通过 **8** 附录中的配置及连接模板，检查获取到的连接参数是否完整。

表 4-1 SSL VPN 连接参数检查项

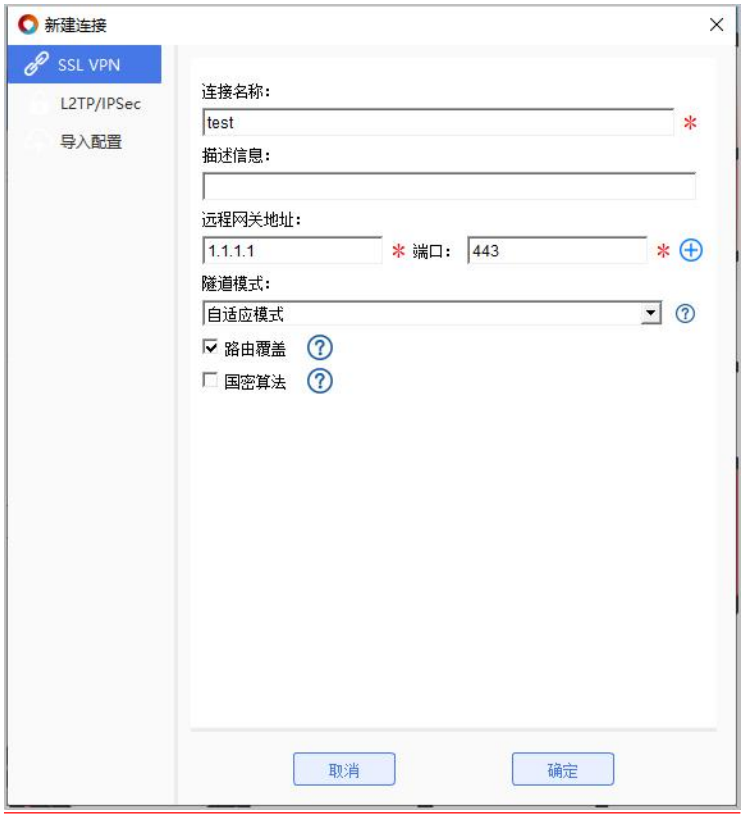
检查项		备注
是否使用代理设置	否	如果您当前访问 Internet 时没有使用代理服务器，则无需使用代理设置。
	是（使用系统代理）	使用代理服务器的场景细分为 3 种情况，选择代理类型后，需要输入地址、端口、账号及密码，该信息请从企业网络管理员处获取。
	是（使用 HTTP/HTTPS 代理）	
	是（使用 Socks5 代理）	
连接名称		用于标识一条 SSL VPN 连接，您可以自行设置。
描述信息		用于补充说明该条连接的相关信息（如创建者、创建时间、连接用途等），您可以自行设置。
远程网关地址		SSL VPN 虚拟网关地址，该信息请从企业网络管理员处获取。
端口		建立 SSL VPN 隧道的端口号，该信息请从企业网络管理员处获取。
隧道模式	可靠传输模式	• 此处配置请咨询企业网络管理员。 • 在网络环境不稳定的情况下推荐使用可靠传输模式；而网络环境比较稳定的情况下，推荐使用快速传输模式，数据传输的效率更高。在不了解当前网络环境的情况下可以选择自适应模式。
	快速传输模式	
	自适应模式	
路由覆盖		当对端网关下发的路由和本地已经存在的路由的目的地址和子网掩码完全相同时，如果启用了路由覆盖功能，则对端网关下发的路由会覆盖本地已经存在的路由，避免本地路由冲突造成网络访问异常。 缺省情况下，路由覆盖功能开启。

检查项	备注
国密算法	客户端支持使用国密算法与对端网关建立 SSL VPN 连接。 缺省情况下，国密算法功能关闭。勾选“国密算法”后，对端网关的加密套件会自动切换为 ECC-SM4-SM3。
证书认证 **说明** 仅在 Linux 操作系统下会显示此项。	如果使用证书认证的方式建立 SSL VPN 连接，则需要勾选“证书认证”。 勾选“证书认证”后，可以选择用于进行证书认证的证书。
密码 **说明** 仅在 Linux 操作系统下会显示此项。	用于设置证书认证时证书中提取的用户名对应的登录密码。 仅当使用证书认证的方式建立 SSL VPN 连接，且勾选了“证书认证”时可以设置此密码。

操作步骤

步骤 1 在 UniVPN 客户端主界面的右侧“选择 VPN 连接”列表框中，单击“+新建连接”。

步骤 2 在“新建连接”窗口中，选择左侧导航栏的“SSL VPN”，并配置相关的连接参数。



步骤 3 设置完成后，单击“确定”，返回 UniVPN 客户端主界面，在右侧选择 VPN 连接一栏可以看到一条 VPN 连接被成功创建。

----结束

后续操作

- 完成上述配置后，您可以尝试 **5** 建立 VPN 连接。
- 您还可以回到 **2** 从这里开始，参照**任务地图**进行后续配置。

4.2 配置 L2TP VPN 连接

如果您已经与企业网络管理员确认待接入 VPN 的类型为 L2TP VPN，请参考以下操作步骤配置 VPN 连接。

开始之前

在配置前请仔细检查如下表单，确认您已获取到建立 L2TP VPN 连接所需的连接参数。

说明

您也可以通过 **8** 附录中的配置及连接模板，检查获取到的连接参数是否完整。

表 4-2 L2TP VPN 连接参数检查项

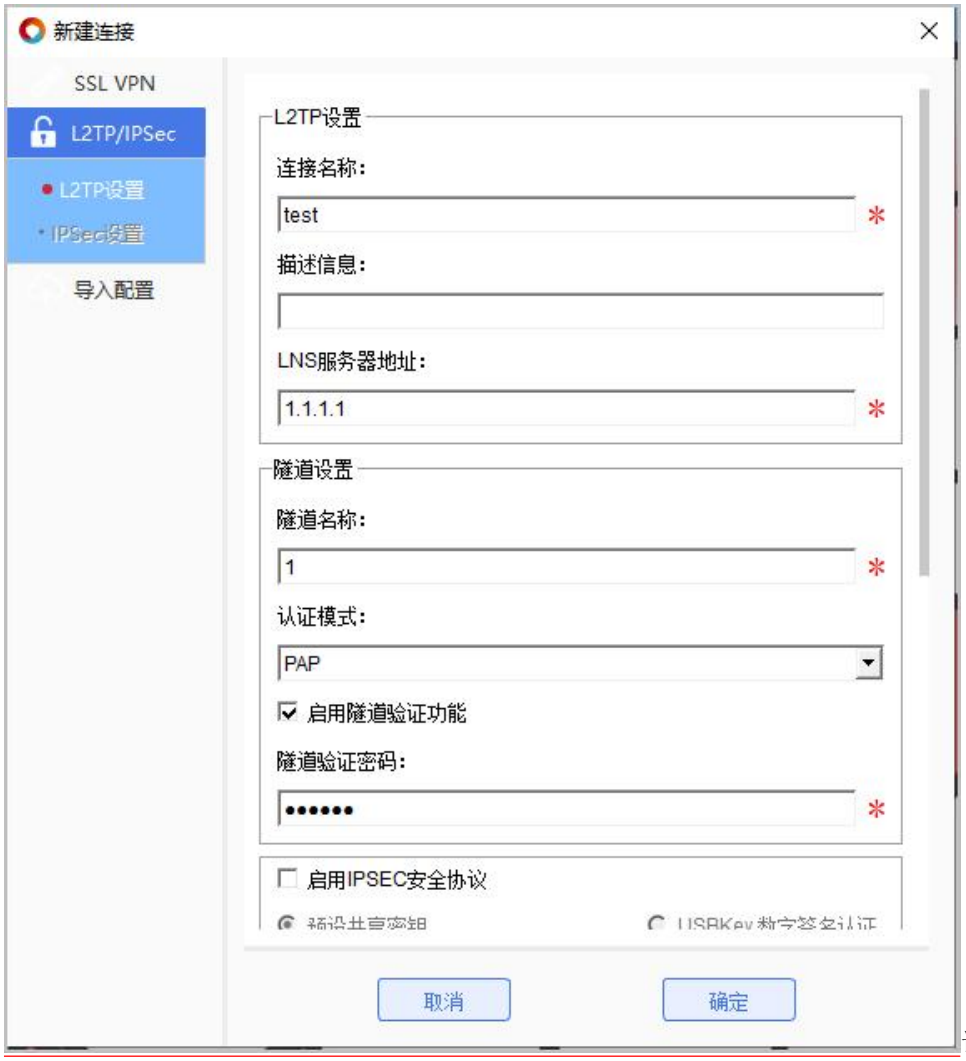
检查项		备注
代理设置		
是否使用代理设置？	说明 L2TP VPN 隧道不支持使用代理。	
L2TP 设置		
连接名称		用于标识一条 L2TP VPN 连接，您可以自行设置。
描述信息		用于补充说明该条连接的相关信息（如创建者、创建时间、连接用途等），您可以自行设置。
LNS 服务器地址		L2TP VPN 网关地址，该信息请从企业网络管理员处获取。
隧道设置		
隧道名称		用于在隧道中标识设备，该信息请从企业网络管理员处获取。
用何种认证模式？	CHAP 认证	此处配置请咨询企业网络管理员。
	PAP 认证	
是否勾选“启用隧道验证功能”？	否	• 此处配置请咨询企业网络管理员。 • 如果勾选了“启用隧道验证功能”，需要输入隧道验证密码，该信息请从企业网络管理员处获取。
	是	

检查项	备注
路由设置	• 此处配置请咨询企业网络管理员。 • 勾选“made config”，可以访问所有网络资源 • 此处包含如下三种配置方式： – 不勾选“连接成功后允许访问 Internet” 只能访问企业内网资源，不能访问 Internet。 – 勾选“连接成功后允许访问 Internet”，但未在 IP 地址列表框中添加 IP 地址 只能访问与对端网关分配的内网地址同网段的企业内网资源，同时还可以访问 Internet 和本地局域网。 – 勾选“连接成功后允许访问 Internet”，并在 IP 地址列表框中添加 IP 地址 可以访问 IP 地址列表框中设置的企业内网资源以及与对端网关分配的内网地址同网段的企业内网资源，同时还可以访问 Internet 和本地局域网。 IP 地址列表框中添加的 IP 地址信息请从企业网络管理员处获取。

操作步骤

步骤 1 在 UniVPN 客户端主界面的右边“选择 VPN 连接”列表框中，单击“+新建连接”。

步骤 2 在“新建连接”窗口中，选择左侧导航栏的“L2TP/IPSec”，并配置相关的连接参数。



设置完成后，单击“确定”，返回 UniVPN 客户端主界面，在右侧选择 VPN 连接一栏可以看到一条 VPN 连接被成功创建。

----结束

后续操作

- 完成上述配置后，您可以尝试 **5** 建立 VPN 连接。
- 您还可以回到 **2** 从这里开始，参照**任务地图**进行后续配置。

4.3 配置 L2TP over IPSec VPN 连接

如果您已经与企业网络管理员确认待接入 VPN 的类型为 L2TP over IPSec VPN，请参考以下操作步骤配置 VPN 连接。

开始之前

在配置前请仔细检查如下表单，确认您已获取到建立 L2TP over IPSec VPN 连接所需的连接参数。

说明

您也可以通过 **8** 附录中的配置及连接模板，检查获取到的连接参数是否完整。

表 4-3 L2TP over IPSec VPN 连接参数检查项

检查项		备注
代理设置		
是否使用代理设置？	否	如果您当前访问 Internet 时没有使用代理服务器，此处选择该类型。
	是（使用 Socks5 代理） **说明** L2TP over IPSec VPN 隧道仅支持使用 Socks5 代理。	选择“使用 Socks5 代理”后，需要输入地址、端口、账号及密码，该信息请从企业网络管理员处获取。
L2TP 设置		
连接名称		用于标识一条 L2TP over IPSec VPN 连接，您可以自行设置。
描述信息		用于补充说明该条连接的相关信息（如创建者、创建时间、连接用途等），您可以自行设置。
LNS 服务器地址		L2TP VPN 网关地址，该信息请从企业网络管理员处获取。
隧道设置		
隧道名称		用于在隧道中标识设备，该信息请从企业网络管理员处获取。
使用何种认证模式？	CHAP 认证	此处配置请咨询企业网络管理员。
	PAP 认证	
是否勾选“启用隧道验证功能”？	否	• 此处配置请咨询企业网络管理员。 • 如果勾选了“启用隧道验证功能”，需要输入隧道验证密码，该信息请从企业网络管理员处获取。
	是	
启用 IPSec 安全协议		在配置 L2TP over IPSec VPN 连接时必须勾选此选项。

检查项		备注
使用何种 IPSec 身份认证方式？	预设共享密钥	需要输入身份认证字，该信息请从企业网络管理员处获取。
	USB-Key 数字签名认证 **说明** 仅在 Windows 操作系统下支持。	需要输入 USB PIN 码，该信息请从企业网络管理员处获取。
IPSec 设置		
IPSec 服务器地址		• IPSec VPN 网关地址，该信息请从企业网络管理员处获取。 • 当 L2TP VPN 网关和 IPSec VPN 网关相同时，请勾选“使用 LNS 服务器地址”。
使用何种封装模式？	隧道模式	此处配置请咨询企业网络管理员。
	传输模式	
ESP 协议验证算法		包括 MD5、SHA1 和 SHA2-256，此处配置请咨询企业网络管理员。
ESP 协议加密算法		包括 DES、3DES 和 AES-128、AES-192 和 AES-256，此处配置请咨询企业网络管理员。
IKE 设置		
使用何种协商模式？	主模式	此处配置请咨询企业网络管理员。
	野蛮模式	
ID 类型		• 表示 IKE 协商过程中的身份认证类型，包括 IP 地址类型和名字类型。 • 此处配置请咨询企业网络管理员。
本端名字		• 当身份类型选择“名字”时，需要设置此参数。 • 此处配置请咨询企业网络管理员。
安全网关名字		
验证算法		包括 MD5、SHA-1 和 SHA2-256，此处配置请咨询企业网络管理员。
加密算法		包括 DES-CBC、3DES-CBC 和 AES-128/192/256，此处配置请咨询企业网络管理员。
DH 组标识		包括 Group1（768 bit）、Group2（1024 bit）和 Group5（1536 bit），此处配置请咨询企业网络管理员。

检查项		备注
IKE 高级设置		
启用 PFS 特性		• 表示在 IKE 协商时使用 PFS（Perfect Forward Secrecy）功能。 • 启用本功能后，需要配置相应的安全参数，包括 Group1（768 bit）、Group2（1024 bit）和 Group5（1536 bit）。 • 此处配置请咨询企业网络管理员。
安全联盟生存周期		• IKE 的安全联盟生存周期用于 IKE SA 的定时更新，降低 IKE SA 被破解的风险，有利于安全性。 • 此处配置请咨询企业网络管理员。
IPSec 高级设置		
安全联盟生存周期		• IPSec 的安全联盟生存周期用于 IPSec SA 的定时更新，降低 IPSec SA 被破解的风险，有利于安全性。 • 此处配置请咨询企业网络管理员。
路由设置	Mode Config	设置“Mode Config”参数后，实际效果取决于对端网关设备对 Mode Config 模式（或称为隧道分离模式）的支持情况： • 如果对端网关设备支持并配置了 Mode Config 模式 在访问企业内网资源的同时，可以访问 Internet 和本地局域网。 • 如果对端网关设备不支持或未配置 Mode Config 模式 只能访问企业内网资源，不能访问 Internet 和本地局域网。 此处配置请咨询企业网络管理员。

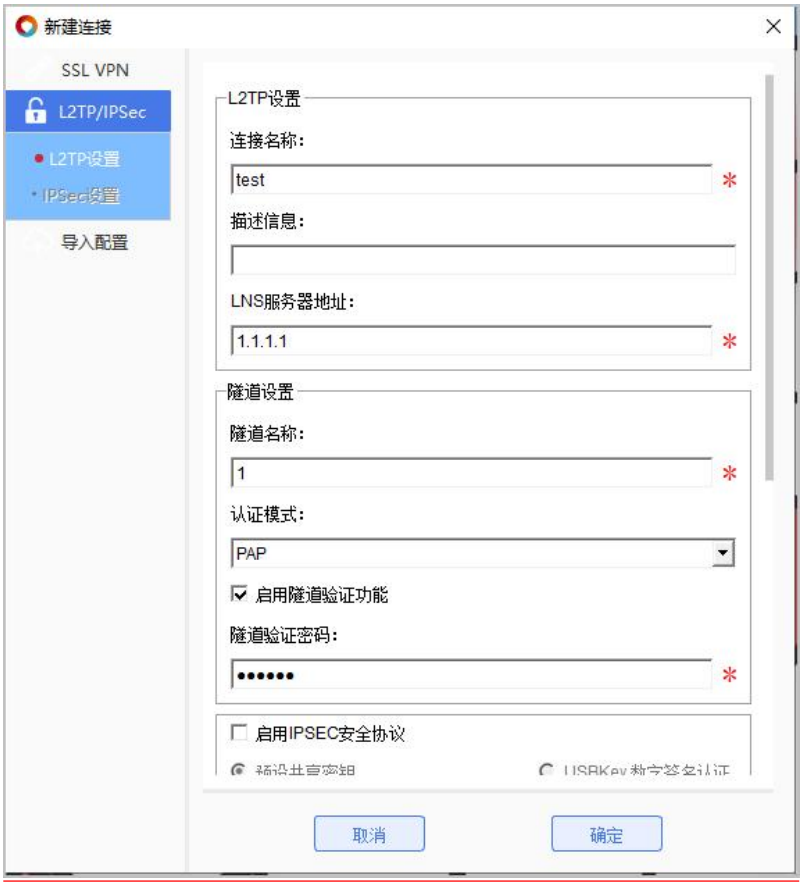
检查项		备注
	连接成功后允许访问 Internet	在设置“连接成功后允许访问 Internet”参数时有如下两种选择： • 勾选“连接成功后允许访问 Internet”，但不在 IP 地址列表框中添加 IP 地址 只能访问与对端网关分配的内网地址同网段的企业内网资源，同时还可以访问 Internet 和本地局域网。 • 勾选“连接成功后允许访问 Internet”，并在 IP 地址列表框中添加 IP 地址 可以访问 IP 地址列表框中设置的企业内网资源以及与对端网关分配的内网地址同网段的企业内网资源，同时还可以访问 Internet 和本地局域网。 IP 地址列表框中添加 IP 地址信息请从企业网络管理员处获取。 此处配置请咨询企业网络管理员。

操作步骤

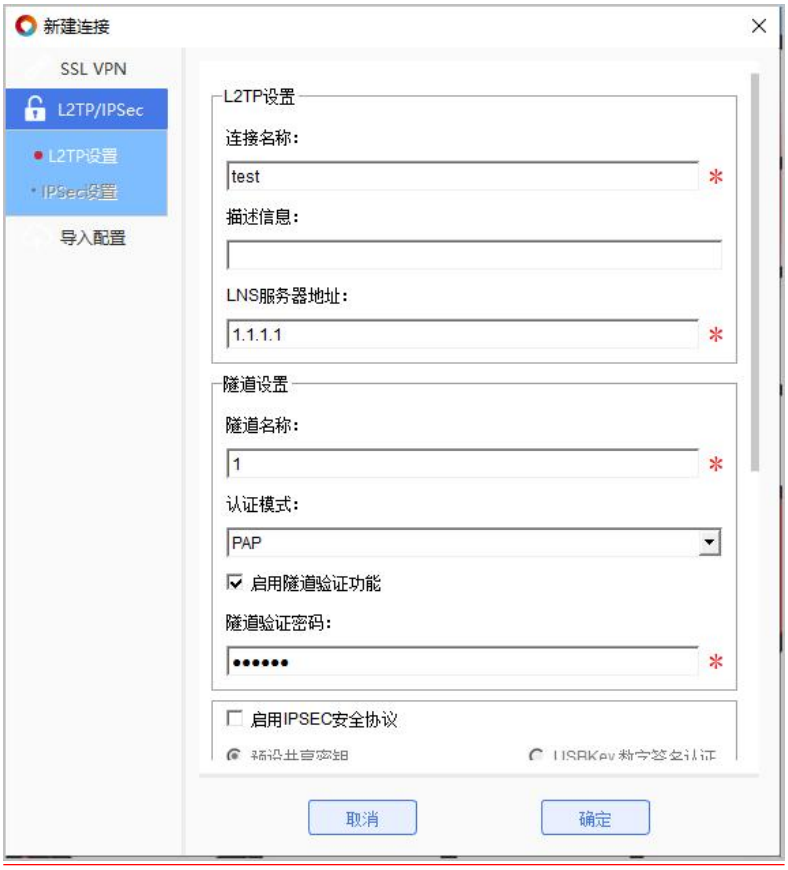
步骤 1 在 UniVPN 客户端主界面中单击“+新建连接”。

步骤 2 在“新建连接”窗口中，选择左侧导航栏的“L2TP/IPSec”，并配置相关的连接参数。

1. 配置 L2TP 参数


新建连接
SSL VPN
L2TP/IPSec
L2TP设置
IPSec设置
导入配置
L2TP设置
连接名称：
test
描述信息：
LNS服务器地址：
1.1.1.1
隧道设置
隧道名称：
1
认证模式：
PAP
启用隧道验证功能
隧道验证密码：
启用IPSEC安全协议
取消
确定

2. 配置 IPSec 参数



步骤 3 设置完成后，单击“确定”，返回 UniVPN 客户端主界面，可以看到一条 VPN 连接被成功创建。

----结束

后续操作

- 完成上述配置后，您可以尝试 **5** 建立 VPN 连接。
- 您还可以回到 **2** 从这里开始，参照**任务地图**进行后续配置。

4.4 通过导入配置文件的方式配置 VPN 连接

配置文件是企业网络管理员利用客户端的配置文件导出功能生成的一份后缀为“.ini”的文件，其中携带了创建一条特定 VPN 连接需要配置的所有参数信息。在您获取到该配置文件后，可以将该配置文件导入到 UniVPN 客户端中，直接生成一条配置好的 VPN 连接，从而简化您的配置工作。

开始之前

请您与企业网络管理员确认配置文件内容的完整性与准确性，如果配置文件中的内容存在缺失或参数配置有误，VPN 连接将无法成功建立。

操作步骤

步骤 1 在 UniVPN 客户端主界面的右侧“选择 VPN 连接”列表框中，单击“+新建连接”。

步骤 2 在“新建连接”窗口中，选择左侧导航栏的“导入配置”。

步骤 3 单击右侧窗口中的“导入配置”按钮，选择预先准备好的配置文件，单击“打开”。

步骤 4 单击“确定”返回 UniVPN 客户端主界面，可以看到一条 VPN 连接被成功创建。

----结束

后续操作

- 完成上述配置后，您可以尝试 **5** 建立 VPN 连接。
- 您还可以回到 **2** 从这里开始，参照**任务地图**进行后续配置。

5 建立 VPN 连接

VPN 连接配置完成后，UniVPN 客户端主界面的“选择 VPN 连接”栏下方会显示对应的连接条目。

1. 您可以选择该连接条目后尝试 **5.1** 发起 VPN 连接。
2. VPN 隧道建立后，对端网关设备需要对您进行 **5.2** 用户身份认证。认证成功后，您的终端设备会获得一个内网地址，此时您便可以通过终端设备安全访问企业内网资源。

   目前 UniVPN 客户端支持如下四种用户身份认证方式，您可使用的身份认证方式由对端网关上的配置决定。

   - **5.2.1** 通过用户名/密码认证
   - **5.2.2** 通过导入 PKI 数字证书认证
   - **5.2.3** 通过 USB-Key 证书认证
   - **5.2.4** 通过双因子认证

   在建立 VPN 连接前，请与企业网络管理员确认您可以使用的身份认证方式，并向其获取用户名、密码、证书等必要的认证信息。

Windows 操作系统和 Linux 操作系统下使用 UniVPN 建立 VPN 连接的方法基本相同，下面以 Windows 操作系统为例进行介绍。

5.1 发起 VPN 连接

VPN 连接配置完成后，即可发起 VPN 连接，建立 VPN 隧道。

5.2 用户身份认证

在您通过 UniVPN 客户端发起 VPN 连接请求以后，对端网关设备会返回用户身份认证请求。认证成功后，您的终端设备会获得一个内网地址，此时您便可以通过终端设备安全访问企业内网资源。

5.1 发起 VPN 连接

VPN 连接配置完成后，即可发起 VPN 连接，建立 VPN 隧道。

开始之前

- 发起 VPN 连接前，请确保 VPN 连接条目中的参数配置完整、准确。
- 如果您是通过导入配置文件的方式配置 VPN 连接，请进入配置修改界面，检查必填的配置项是否存在空缺。

操作步骤

步骤 1 在 UniVPN 客户端主界面的“选择 VPN 连接”栏下方，选择配置好的 VPN 连接条目。

步骤 2 双击连接条目进行连接，发起 VPN 连接请求。

或者选择 VPN 连接条目，单击界面左下角的“连接”

----结束

后续操作

- VPN 隧道建立后，对端网关设备需要对您进行 **5.2** 用户身份认证。认证成功后，您的终端设备会获得一个内网地址，此时您便可以通过终端设备安全访问企业内网资源。
- 若 VPN 连接过程中发生错误导致连接失败，请参考 **7.3** 连接类故障进行故障排查和处理。

- 您还可以回到 **2** 从这里开始，参照**任务地图**进行后续配置。

5.2 用户身份认证

在您通过 UniVPN 客户端发起 VPN 连接请求以后，对端网关设备会返回用户身份认证请求。认证成功后，您的终端设备会获得一个内网地址，此时您便可以通过终端设备安全访问企业内网资源。

目前 UniVPN 客户端支持四种用户身份认证方式，不同的认证方式需要的认证信息存在差异，您需要与企业网络管理员确认您可以使用的身份认证方式，并向其获取用户名、密码、证书等必要的认证信息。

如果您已经明确了将要使用的身份认证方式并已获取到相应的认证信息，请参考以下节点完成用户身份认证：

- **5.2.1** 通过用户名/密码认证
- **5.2.2** 通过导入 PKI 数字证书认证
- **5.2.3** 通过 USB-Key 证书认证
- **5.2.4** 通过双因子认证

5.2.1 通过用户名/密码认证

通过用户名/密码认证是最常见的一种身份认证方式。

开始之前

请从企业网络管理员处获取用户名/密码认证所需的认证信息，包括：

1. 可用的用户名
2. 用户名对应的密码

说明

您也可以通过 **8** 附录中的配置及连接模板，检查获取到的认证信息是否完整。

用户名/密码认证在不同操作系统和 VPN 类型下的支持情况如下：

表 5-1 用户名/密码认证的支持情况

VPN 类型/操作系统	Windows	Linux	Mac OS	国产化
SSL VPN	Y	Y	Y	Y
L2TP VPN	Y	Y	Y	Y
L2TP over IPSec VPN	Y	Y	Y	Y

操作步骤

步骤 1 发起 VPN 连接请求，客户端弹出用户名/密码认证界面。

步骤 2 输入用户名及密码，单击“登录”。

步骤 3 用户身份认证成功后，设备成功接入内网，客户端提示“连接成功”。

----结束

后续操作

- 若您还需要进行双因子认证，请参考 **5.2.4** 通过双因子认证。
- 若用户身份认证失败或 VPN 连接失败，请参考 **7.3** 连接类故障进行故障排查和处理。
- 设备成功接入内网后，您可以尝试访问内网资源，若此时内网资源无法访问，请参考 **7.4** 业务类故障进行故障排查和处理。
- 您还可以回到 **2** 从这里开始，查看**任务地图**中的其他内容。

5.2.2 通过导入 PKI 数字证书认证

您可以将企业网络管理员提供的 PKI 数字证书安装到终端设备中，通过证书认证的方式登录 VPN 网关。SSL VPN 场景下支持 PKI 数字证书匿名认证和 PKI 数字证书挑战认证。

开始之前

请从企业网络管理员处获取 PKI 数字证书认证所需的认证信息，包括：

1. 可用的 PKI 数字证书
2. 证书中提取的用户名对应的登录密码（仅在 PKI 数字证书挑战认证方式下需要此密码）
3. 登录用户名及登录密码（仅在 L2TP over IPSec VPN 场景下需要）

说明

您也可以通过 **8** 附录中的配置及连接模板，检查获取到的认证信息是否完整。

PKI 数字证书认证在不同操作系统和 VPN 类型下的支持情况如下：

表 5-2 PKI 数字证书认证的支持情况

VPN 类型/操作系统	Windows	Linux	Mac OS	国产化
SSL VPN（证书匿名认证）	Y	Y	Y	Y
SSL VPN（证书挑战认证）	Y	Y	Y	Y
L2TP VPN	N	N	N	N

VPN 类型/操作系统	Windows	Linux	Mac OS	国产化
L2TP over IPSec VPN	Y	N	N	N

操作步骤

步骤 1 将 PKI 数字证书导入到终端设备中，导入成功后即可在证书选择列表中选择对应证书。

- 在 Windows 证书认证场景下，证书都是导入到 IE 浏览器中的。
- 在 Linux 证书认证场景下，证书需要放入主目录下的 Certificate 文件夹。
- 在 MAC 证书认证场景下，证书需要导入到“凭证”中。
- 在国产化证书认证场景下，证书需要放入主目录下的 Certificate 文件夹。

步骤 2 双击证书，根据安装向导的提示完成证书的安装。

步骤 3 发起 VPN 连接请求，客户端弹出证书认证界面。

步骤 4 在“请选择证书”下拉列表中选择已导入的 PKI 数字证书（如果使用 SSL VPN 证书挑战认证方式则还需要输入证书中提取的用户名对应的登录密码；如果是 L2TP over IPSec VPN 连接则还需要输入登录用户名及登录密码），单击“登录”。

步骤 5 用户身份认证成功后，设备成功接入内网，客户端提示“连接成功”。

----结束

后续操作

- 若您还需要进行双因子认证，请参考 **5.2.4** 通过双因子认证。
- 若用户身份认证失败或 VPN 连接失败，请参考 **7.3** 连接类故障进行故障排查和处理。
- 设备成功接入内网后，您可以尝试访问内网资源，若此时内网资源无法访问，请参考 **7.4** 业务类故障进行故障排查和处理。
- 您还可以回到 **2** 从这里开始，查看**任务地图**中的其他内容。

5.2.3 通过 USB-Key 证书认证

您可以将企业网络管理员提供的 USB-Key 设备插入终端设备的 USB 接口中，通过 USB-Key 中内置的证书进行用户身份认证。SSL VPN 场景下支持 USB-Key 证书匿名认证和 USB-Key 证书挑战认证；L2TP over IPSec VPN 场景下若“IPSec 身份认证方式”选择“USB-Key 数字签名认证”，即表示通过 USB-Key 证书认证方式认证。

开始之前

请从企业网络管理员处获取 USB-Key 证书认证所需的认证信息，包括：

1. 可用的 USB-Key 设备及对应的驱动程序、PIN 码

2. 证书中提取的用户名对应的登录密码（此密码仅在 USB-Key 证书挑战认证方式下需要）
3. 登录用户名及登录密码（仅在 L2TP over IPSec VPN 场景下需要）

说明

您也可以通过 **8** 附录中的配置及连接模板，检查获取到的认证信息是否完整。

USB-Key 证书认证在不同操作系统和 VPN 类型下的支持情况如下：

表 5-3 USB-Key 证书认证的支持情况

VPN 类型/操作系统	Windows	Linux	Mac OS	国产化
SSL VPN（证书匿名认证）	Y	N	N	N
SSL VPN（证书挑战认证）	Y	N	N	N
L2TP VPN	N	N	N	N
L2TP over IPSec VPN	Y	N	N	N

操作步骤

步骤 1 将 USB-Key 设备插入终端设备的 USB 接口中，安装 USB-Key 的驱动程序。

步骤 2 发起 VPN 连接请求，客户端弹出证书认证界面。

步骤 3 在“证书”列表中选择系统识别出的 USB-Key 证书（如果使用 SSL VPN 证书挑战认证方式则还需要输入证书中提取的用户名对应的登录密码；如果是 L2TP over IPSec VPN 连接则还需要输入登录用户名及登录密码），单击“登录”。

步骤 4 系统弹出 PIN 码输入框，输入 USB-Key 设备的 PIN 码，单击“确定”。

步骤 5 用户身份认证成功后，设备成功接入内网，客户端提示“连接成功”。

----结束

后续操作

- 若您还需要进行双因子认证，请参考 **5.2.4** 通过双因子认证。
- 若用户身份认证失败或 VPN 连接失败，请参考 **7.3** 连接类故障进行故障排查和处理。
- 设备成功接入内网后，若您可以访问内网资源，但无法访问 Intrenet，请参考 **7.4** 业务类故障进行故障排查和处理。
- 您还可以回到 **2** 从这里开始，查看**任务地图**中的其他内容。

5.2.4 通过双因子认证

在 SSL VPN 场景下，客户端支持双因子认证，即在用户名/密码认证或证书认证的基础上通过动态令牌码或短信验证码进行二次认证。

开始之前

请咨询企业网络管理员，准备好动态令牌码或短信验证码的接收设备，用于获取双因子认证所需的验证信息。

在进行双因子认证前，需要您先进行初次认证，请与企业网络管理员明确认证方式，参考如下节点完成认证：

- **5.2.1** 通过用户名/密码认证
- **5.2.2** 通过导入 PKI 数字证书认证
- **5.2.3** 通过 USB-Key 证书认证

说明

- 您也可以通过 **8** 附录中的配置及连接模板，检查获取到的认证信息是否完整。

操作步骤

步骤 1 初次认证通过后，客户端会弹出输入框，要求您输入动态令牌码或短信验证码进行双因子认证。

步骤 2 在接收设备上获取动态令牌码或短信验证码，填入输入框内，单击“确定”。

步骤 3 双因子认证成功后，设备成功接入内网，客户端提示“连接成功”。

----结束

后续操作

- 若用户身份认证失败或 VPN 连接失败，请参考 **7.3** 连接类故障进行故障排查和处理。
- 设备成功接入内网后，您可以尝试访问内网资源，若此时内网资源无法访问，请参考 **7.4** 业务类故障进行故障排查和处理。
- 您还可以回到 **2** 从这里开始，查看**任务地图**中的其他内容。

6 可选配置

本节介绍 UniVPN 客户端的各种可选配置。

通过本节您可以了解如下内容：

- 如何 **6.1** 卸载软件
- 如何 **6.2** 更新升级
- 如何 **6.3** 修改登录密码
- 如何**配置验证服务器是否可信**
- 如何**配置开机自启动**
- 如何**配置取消自动登录**
- 如何**修改界面语言**

6.1 卸载软件

UniVPN 客户端目前支持 Windows、Linux、Mac OS 和国产化四种操作系统环境，四种操作系统环境下均需要通过运行卸载程序卸载软件。

6.2 更新升级

UniVPN 客户端支持版本检测与更新升级。

6.3 修改登录密码

UniVPN 客户端支持用户在本地修登录密码。

6.4 其他配置

本节介绍 UniVPN 客户端的其他可选配置，包括：验证服务器是否可信、开机自启动、取消自动登录、修改界面语言、检测新版本

6.1 卸载软件

UniVPN 客户端目前支持 Windows、Linux、Mac OS 和国产化四种操作系统环境，四种操作系统环境下均需要通过运行卸载程序卸载软件。

在 Windows 操作系统下卸载软件

步骤 1 选择“开始 > 所有程序 >UniVPN”。

步骤 2 单击“卸载”，系统弹出卸载提示，单击“是”，系统会自动删除所有用户配置及日志文件。

----结束

在 Linux 操作系统下卸载软件

步骤 1 使用具有“root”权限的操作系统用户登录 Linux 操作系统。

步骤 2 打开“终端”，进入“/usl/local/UniVPN”目录下。

```
root@rtw-virtual-machine:~# cd /usr/local/UniVPN
root@rtw-virtual-machine:/usr/local/UniVPN#
```

步骤 3 使用 root 身份执行**./ uninstall.sh**，卸载 UniVPN 客户端。

```
root@rtw-virtual-machine:/usr/local/UniVPN# ./uninstall.sh
Stopping UniVPNPromoteService daemon: ./uninstall.sh: 行 19: 28692 已杀死            sh
UniVPNPromoteService.sh stop
```

----结束

在 Mac OS 操作系统下卸载软件

步骤 1 在应用程序文件夹中双击“UniVPNUninstaller”启动卸载程序。

步骤 2 单击“卸载”，卸载 UniVPN 客户端。

----结束

在国产化操作系统下卸载软件

方法一：

步骤 1 使用具有“root”权限的操作系统用户登录 linux4.4.131（3A3000）操作系统。

步骤 2 打开“终端”，进入“/usr/local/UniVPN”目录下。

```
root@UniVPN-virtual-machine:~# cd  /usr/local/UniVPN
root@UniVPN-virtual-machine: /usr/local/UniVPN#
```

步骤 3 使用 root 身份执行 dpkg --purge --force-all univon，卸载 UniVPN 客户端。

```
root@zzh-virtual-machine:/usr/local/UniVPN# dpkg --purge --force-all univpn
Stopping UniVPNPromoteService daemon: /var/lib/dpkg/info/univpn.prerm: 行 38: 12855
 已杀死               sh UniVPNPromoteService.sh stop
```

----结束

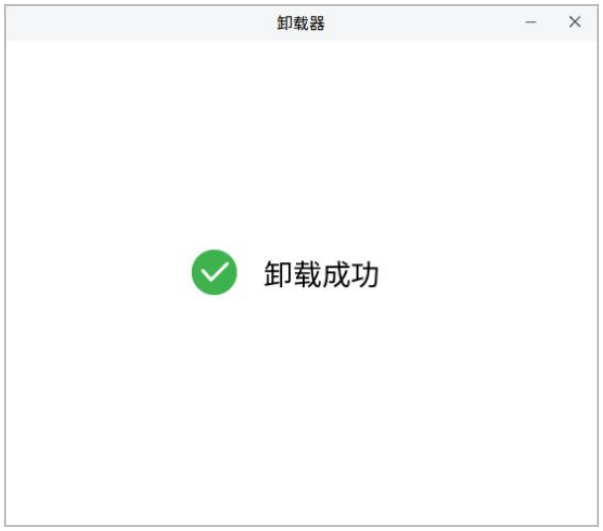
方法二：

步骤 1 打开“开始”菜单栏，选择“所有程序”，选择 UniVPN 单击右键。

步骤 2 选择“卸载”。

步骤 3 在授权页面，输入用户密码后左键单击“授权”。

步骤 4 卸载成功，如下所示。



----结束

6.2 更新升级

UniVPN 客户端支持版本检测与更新升级。

开始之前

- 只有当 UniVPN 客户端与对端网关已经建立 VPN 连接的时候才能检测软件版本并进行更新升级。

- UniVPN 客户端升级的基本过程如下：
  a. 企业网络管理员将新的 UniVPN 客户端软件安装包上传至企业网关。
  b. 用户通过 UniVPN 客户端与该网关建立 VPN 隧道时，UniVPN 客户端会自动检测并比较网关上客户端软件安装包的版本。
  c. 如果网关上的客户端软件安装包被判定为新版本，则提示用户进行升级。

操作步骤

步骤 1 单击客户端右上角的 按钮，在弹出的菜单中选择“设置”，其中提供了“检测新版本”的选项。勾选此项，客户端在与设备建立连接时会检查网关上是否存在新版本的软件安装包。

步骤 2 若在网关上发现了新版本的软件安装包，客户端会弹出提示窗口，提示用户更新升级软件。单击“是”，即可下载并安装。

说明

Linux 和 MAC OS 系统多用户同时登录时，不支持自动升级；国产化系统暂不支持自动升级。

----结束

6.3 修改登录密码

UniVPN 客户端支持用户在本地修改登录密码。

开始之前

只有当 UniVPN 客户端与对端网关已经建立 VPN 连接的时候才能修改密码。

说明

仅 SSL VPN 场景下支持修改密码。

操作步骤

步骤 1 单击客户端右上角的 按钮，在弹出的菜单中选择“修改密码”，或右键单击客户端的托盘图标，在弹出的菜单中选择“修改密码”。

步骤 2 在弹出的“修改密码”窗口中修改登录密码。

----结束

后续操作

修改密码成功后，客户端将中断当前的 VPN 连接，需要您使用新密码重新登录。

6.4 其他配置

本节介绍 UniVPN 客户端的其他可选配置，包括：

验证服务器是否可信

UniVPN 客户端与对端网关建立 SSL VPN 隧道时，会校验网关发送的设备证书。

单击客户端的右上角 按钮，在弹出的菜单中选择“设置”，其中提供了“验证服务器是否可信”的选项：

- 若勾选此选项

  当客户端校验网关设备证书失败时，系统会弹出“网关证书校验：不可信的 VPN 服务器证书！”的告警，在确认对端网关安全的情况下，可以选择“继续”，继续建立 SSL VPN 隧道。如果您无法确认对端网关的安全情况，可以选择“取消”，中止隧道建立过程。

- 若不勾选此选项

  当客户端校验网关设备证书失败时，系统不会给出告警提示，直接完成隧道建立。

配置开机自启动

UniVPN 客户端支持开机自动启动。

单击客户端右上角的 按钮，在弹出的菜单中选择“设置”，其中提供了“开机自启动”的选项。勾选此项，客户端在设备开机后会自动启动。

取消自动登录

右键单击客户端的托盘图标，在弹出的菜单中选择“取消自动登录”，可以取消建立 VPN 连接时勾选的自动登录设置。

修改界面语言

UniVPN 客户端支持中英文两种界面语言。

单击客户端右上角的 按钮，在弹出的菜单中选择“设置”，其中提供了“界面语言”的选项，您可以手动切换界面语言。

错误报告

右键单击右下角 UniVPN 的托盘图标，在菜单栏选择“错误报告”，填写故障信息后，单击“确定”，反馈错误报告。

代理屏蔽

- 在 Windows 操作系统下：

Windows 操作系统使用的是 IE 浏览器的代理信息，因此需要修改 IE 浏览器的代理信息设置。

a. 打开 IE 浏览器，单击“设置”按钮，打开“Internet 选项”。
b. 选择“连接”页签，单击“局域网设置”按钮。
c. 在“代理服务器”设置界面设置代理屏蔽信息。
d. 单击“确定”，保存设置。

- 在 Linux 操作系统下：

  Linux 操作系统缺省使用火狐浏览器自带的代理信息设置模块。

  a. 打开火狐浏览器，在地址栏中输入“about:preferences”。
  b. 选择“常规 > 网络设置”页签，单击“设置”按钮。
  c. 设置代理屏蔽信息。
  d. 单击“确定”，保存设置。

- 在 MAC 操作系统下：

  MAC 操作系统缺省使用火狐浏览器自带的代理信息设置模块。

  a. 打开火狐浏览器，在地址栏中输入“about:preferences”。
  b. 选择“常规 > 网络设置”页签，单击“设置”按钮。
  c. 设置代理屏蔽信息。
  d. 单击“确定”，保存设置。

- 在国产化操作系统下：

  国产化操作系统缺省使用火狐浏览器自带的代理信息设置模块。

  a. 打开火狐浏览器，在地址栏中输入“about:preferences”。
  b. 选择“常规 > 网络设置”页签，单击“设置”按钮。
  c. 设置代理屏蔽信息。
  d. 单击“确定”，保存设置。

当在“局域网设置”界面配置代理服务器并登录客户端成功后，会自动生成 PAC 文件。在“局域网设置”界面勾选“使用自动配置脚本”后，将会自动填充 PAC 文件地址，并在客户端登录期间使用该 PAC 文件进行代理屏蔽。在客户端退出后，浏览器会自动恢复登录前的代理设置。

PAC 文件中的设置可以引导流量正确访问网关和内网资源，从而防止浏览器中设置的代理服务器引起的内网资源无法正确访问的问题。PAC 文件中对原有代理信息不会做任何修改，不会影响原有的代理功能。

登录客户端期间，如果删除该 PAC 文件，在采用代理的情况下可能出现无法通过 IE 浏览器访问网关或内网资源的情况。

VPN 快速切换

UniVPN 客户端支持通过托盘菜单和悬浮窗快速切换不同的 vpn 连接。

单击客户端右上角的 按钮，在弹出的菜单中选择“设置”，其中提供了“VPN 快速切换”的选项。勾选此项，可通过悬浮窗和托盘菜单切换不同的 VPN 连接。

7 故障处理

本节收录了 UniVPN 在安装、使用过程中遇到的一些常见故障以及故障的处理方法。

根据终端用户的任务场景，可将故障划分为如下三类：

1. **7.2** 安装及更新类故障
2. **7.3** 连接类故障
3. **7.4** 业务类故障

若以上故障处理方法无法解决您遇到的问题，请联系企业网络管理员获取技术支持。为了便于快速的定位问题，需要您在获取帮助之前预先 **7.1** 收集用于故障排除的信息。

7.1 收集用于故障排除的信息

当您在安装或使用客户端的过程中遇到无法自行解决的故障时，需要联系企业网络管理员协助排除故障。在此之前，请您在终端设备上收集用于故障定位的信息。

1. 客户端支持 **7.1.1** 收集错误报告的功能，可以一键式收集信息并生成“.zip”格式的错误报告压缩文件。
2. 在此基础上，您还需要 **7.1.2** 导出配置文件，将配置文件与错误报告压缩文件一同发送给企业网络管理员。

7.1.1 收集错误报告

您可以使用收集错误报告的功能一键式收集用于进行故障定位的信息，生成“.zip”格式的错误报告压缩文件。

开始之前

UniVPN 生成错误报告时会收集客户端软件的使用信息及部分系统信息（参见下文），请确保以下信息受到严格保护。

- **error_detail.txt**：记录用户手动输入的对产生该错误的操作步骤的描述，以及所用客户端的版本号信息。
- **netcard_info.txt**：记录设备的网卡信息。

- **operate_system_info.txt**：记录设备的操作系统信息。
- **proxy_info.txt**：记录设备的代理服务器信息。
- **route_info.txt**：记录设备的路由信息。
- **UniVPN_UniVPN_0.log**：记录 UniVPN 客户端业务配置产生的日志信息，例如用户登录成功或失败、VPN 隧道建立正常或异常等信息。
- **UniVPN_UniVPN_0.log**：记录 UniVPN 客户端配置界面产生的日志信息，例如 VPN 连接配置和中英文界面切换所产生的日志信息。
- **UniVPN_UniVPNPromoteService_0.log**：记录 UniVPN 客户端的服务进程信息，服务进程用于确保客户端正常运行。
- **崩溃文件**：当 UniVPN 客户端出现异常关闭时会生成崩溃文件，造成异常关闭的原因不同，生成的崩溃文件名称也不同。在 Windows 操作系统下崩溃文件的后缀是“*.dmp”，在 Mac OS 和 Linux 操作系统下生成的崩溃文件后缀为“*.core”。

操作步骤

步骤 1 右键单击 UniVPN 的托盘图标。

步骤 2 选择“错误报告”，在输入框中描述产生故障的配置步骤或操作，单击“确定”。

步骤 3 单击“浏览”，选择错误报告的存放路径。

说明

在 Linux 和国产化操作系统下保存错误报告的压缩包时，选择的保存路径中不能含有~<>|;?' ，&#等特殊字符。

步骤 4 单击“确定”，将错误报告保存到选择的路径下。

----结束

后续操作

错误报告生成后，您还需要 **7.1.2** 导出配置文件，并将错误报告和配置文件通过邮件、U 盘或是其他方式发送给企业网络管理员，由企业网络管理员协助您处理故障。

7.1.2 导出配置文件

配置文件是企业网络管理员利用客户端的配置文件导出功能生成的一份后缀为“.ini”的文件，其中携带了创建一条特定 VPN 连接需要配置的所有参数信息，因此在故障排除和问题复现阶段具有重要的参考价值。

操作步骤

方法一：

步骤 1 选中一个已存在的 VPN 连接条目，单击连接条目右侧的编辑。

步骤 2 在“编辑连接”窗口中，单击导航栏侧的“导出配置”，并选择配置文件的保存位置。

配置文件默认会被保存为.ini 格式。

步骤 3 单击“保存”，完成导出。

方法二：

步骤 1 选中一个已存在的 VPN 连接条目，单击连接条目右侧的导出。

步骤 2 选择配置文件的保存位置，配置文件默认会保存为.ini 格式。

步骤 3 单击“保存”，完成导出。

----结束

后续操作

配置文件导出后，您可以将其与 7.1.1 收集错误报告时生成的错误报告通过邮件、U 盘或是其他方式发送给企业网络管理员，由企业网络管理员协助您处理故障。

7.2 安装及更新类故障

软件安装失败

请仔细阅读 **3.1** 安装前须知中的注意事项，检查您的登录帐户是否拥有管理员权限，只有具备管理员权限的用户才可以安装。

此外，请确认您的终端设备上搭载的操作系统环境及版本符合 **3.1** 安装前须知中的系统配置要求。

软件更新失败

发生此问题可能是由于企业网络管理员在网关中上传了错误的客户端软件安装包，请直接联系企业网络管理员进行确认。

7.3 连接类故障

首次建立 VPN 连接失败

造成此故障的原因可能是操作系统自带的防火墙阻断了客户端进行 VPN 连接的操作，请在“开始 > 控制面板 > 系统和安全 > Windows 防火墙”中将操作系统自带防火墙的访问规则设置为允许（此处路径以 Windows 7 操作系统为例）。

终端设备无法识别 USB-Key 中的证书

造成此故障的原因可能是 USB-Key 与终端设备的 USB 端口接触不良或是 USB-Key 的驱动程序存在问题。请将 USB-Key 从 USB 端口中拔出，并重新插入。如果系统依然无法识别，则需要重新安装 USB-Key 的驱动程序。

通过 L2TP 方式建立 VPN 连接时，客户端提示“隧道保活超时或协商超时”

造成此故障的原因可能是客户端和网关侧加解密协商参数配置不一致，或两端路由不可达。请直接联系企业网络管理员，确认配置的正确性及两端路由可达。

选择“使用系统代理”时提示“获取系统代理失败”

在“代理类型”中选择“使用系统代理”，表示客户端将使用系统浏览器中的代理配置。此处出现“获取系统代理失败”的提示，则表示系统浏览器中未设置代理。

此时，请参考如下操作配置代理服务器：

步骤 1 打开 IE 浏览器，在浏览器右上角选择“工具 > Internet 选项”，并在弹出的窗口中选择“连接”页签。

步骤 2 单击“局域网设置”，并配置代理服务器（代理服务器信息请从企业网络管理员处获取）。配置完成后，单击“确定”。

步骤 3 再次打开客户端，选择“代理类型”为“使用系统代理”，即可看到浏览器中配置的代理服务器信息已自动填充到客户端的“代理设置”中。

----结束

7.4 业务类故障

建立 VPN 隧道后用户无法访问 Internet

现象描述

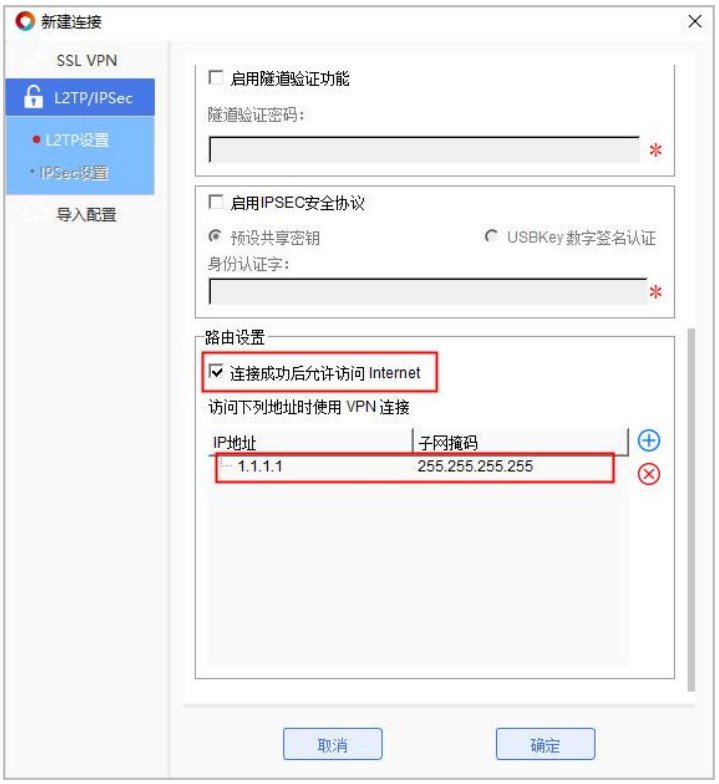
VPN 隧道建立完成后，客户端提示“连接成功”或“协商成功”。此时用户可以访问企业内网资源，但却无法访问 Internet。

故障分析及处理

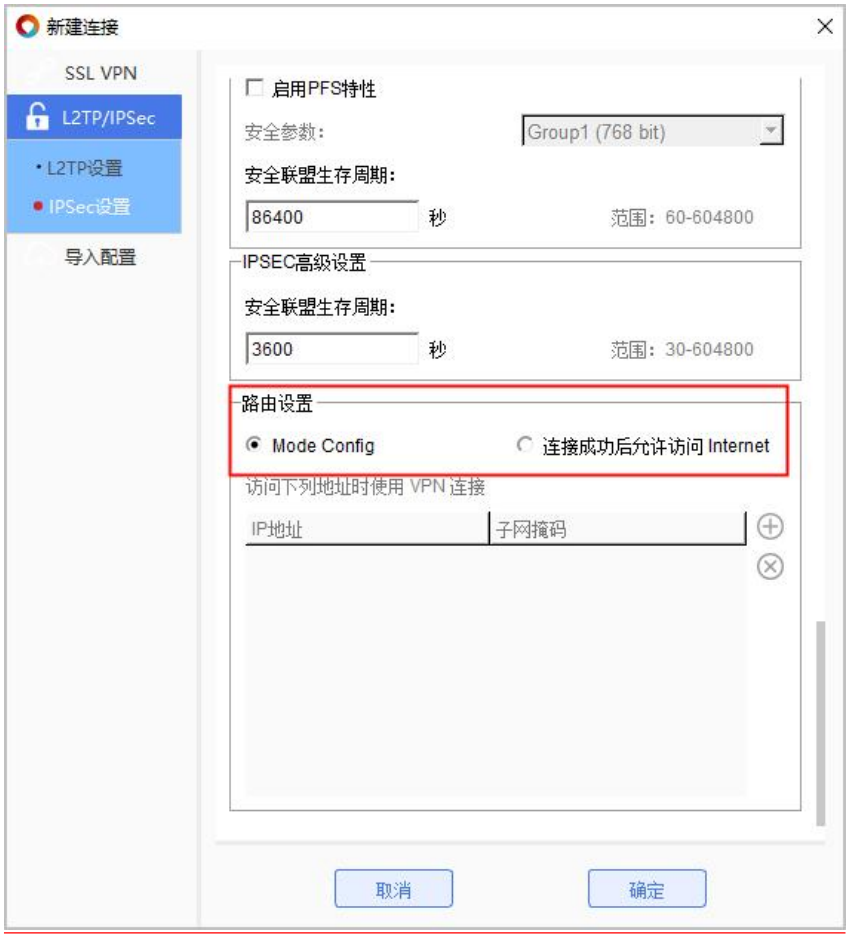
造成此故障的原因可能是由于未配置隧道分离，导致所有流量都进入 VPN 隧道。

SSL VPN、L2TP VPN 和 L2TP over IPSec VPN 都支持隧道分离技术，其中：

- SSL VPN 的隧道分离需要在网关侧配置，因此若您在 SSL VPN 连接中遇到无法访问 Internet 的问题，请直接联系企业网络管理员确认并修改网关上的配置。
- L2TP VPN 的隧道分离需要在客户端上进行配置，请检查客户端侧是否勾选“连接成功后允许访问 Internet”并设置了使用 VPN 访问的网段。若客户端侧配置无误，请联系企业网络管理员。



- L2TP over IPSec VPN 的隧道分离有两种配置方式，采用哪种方式取决于 VPN 连接中的路由设置：
  - 若客户端上的路由设置勾选了“Mode Config”，需要企业网络管理员在网关上配置隧道分离功能并下发路由，此时请直接联系企业网络管理员确认并修改网关上的配置。
  - 若客户端上的路由设置勾选了“连接成功后允许访问 Internet”，请检查列表中是否配置了使用 VPN 访问的网段。若客户端侧配置无误，请联系企业网络管理员。


新建连接
SSL VPN
L2TP/IPSec
L2TP设置
IPSec设置
导入配置
启用PFS特性
安全参数：
Group1 (768 bit)
安全联盟生存周期：
86400
秒
范围：60-604800
IPSEC高级设置
安全联盟生存周期：
3600
秒
范围：30-604800
路由设置
Mode Config
连接成功后允许访问 Internet
访问下列地址时使用 VPN 连接
IP地址
子网掩码
取消
确定

8 附录

提供了在 Linux 操作系统下通过命令行方式配置客户端的配置方法；提供了 SSL VPN、L2TP VPN、L2TP over IPSec VPN 的配置及连接模板，里面包含了配置和建立对应 VPN 所需的全部连接参数、认证信息检查项。终端用户可以参考此模板，逐一检查获取到的信息是否充足；企业网络管理员也可以使用此模板为终端用户提供必要的连接参数和认证信息。

8.1 移动客户端

除了 PC 版的 UniVPN 客户端外，联软公司还推出了基于 iOS 及 Android 操作系统的移动版客户端。

8.2 在 Linux 操作系统下通过命令行方式配置客户端

8.3 在国产化操作系统下通过命令行方式配置客户端

8.4 VPN 连接配置及连接模板

8.1 移动客户端

除了 PC 版的 **UniConnect** 客户端外，联软公司还推出了基于 iOS 及 Android 操作系统的移动版客户端。

获取

- **获取 iOS 操作系统版本的移动版客户端**

  方式一：打开“**APP Store**”APP，搜索“**UniConnect**”字段，即可下载最新版本的 UniConnect iOS 版本客户端。

- **Android 操作系统版本的移动版客户端**

  方式一：下载并打开“**华为应用市场、小米应用市场、oppo 应用市场、vivo 应用市场**”APP，搜索“**UniConnect**”字段，即可下载最新版本的 UniConnect Android 版本客户端。

规格

移动版 UniConnect 客户端目前仅支持建立 SSL VPN 连接，具体支持的机型及操作系统版本如下：

表 8-1 移动版 UniConnect 客户端支持的机型及操作系统版本

操作系统	iOS	Android
支持的操作系统版本	支持 iOS 10.0 及以上版本。	支持 Android 5.0 及以上版本。
支持的设备型号	• iPhone X • iPhone 8/8 Plus • iPhone 7/7 Plus • iPhone 6s/6s Plus • iPhone 6/6 Plus • iPhone 5s • iPad Pro • iPad Air 1/2 • iPad 4 • iPad mini 2/3/4	-
支持的设备屏幕分辨率	-	• 720*1280 • 1080*1920 • 1440*2560 • 2160*4096

移动版 UniConnect 客户端的功能规格如下：

表 8-2 移动版 UniConnect 客户端的功能规格

功能名称		iOS	Android
SSL VPN	网络扩展	支持	支持

功能名称		iOS	Android
	终端安全 **说明** 网关侧开启终端安全功能时，移动版 UniConnett 客户端可以拨号成功。	支持	支持
	网关优选	支持	支持
	断线重连	支持	支持
	链路备份 **说明** 网关侧开启链路备份功能时，移动版 UniConnect 客户端可以拨号成功。	支持	支持
	证书认证	支持	支持
	MAC 认证	不支持	不支持
	证书筛选	支持	支持
	双因子认证	支持	支持 可通过短信验证码进行双因子认证
L2TP VPN		不支持	不支持
L2TP over IPSec VPN		不支持	不支持
NAT 穿越		不支持	不支持
代理穿越		不支持	不支持
隧道分离		支持	支持
基本功能	开机自启动	不支持	不支持

功能名称		iOS	Android
	界面语言切换 说明 仅支持中英文切换。	支持	支持
	自动登录	支持	支持
配置文件	导入	不支持	不支持
	导出	不支持	不支持
故障定位		支持	支持
命令行配置		不支持	不支持
非管理员权限用户配置		支持	支持

移动版 UniConnect 客户端的性能规格如下：

表 8-3 移动版 UniConnect 客户端的性能规格

功能名称	规格
VPN 新建连接数	16 个

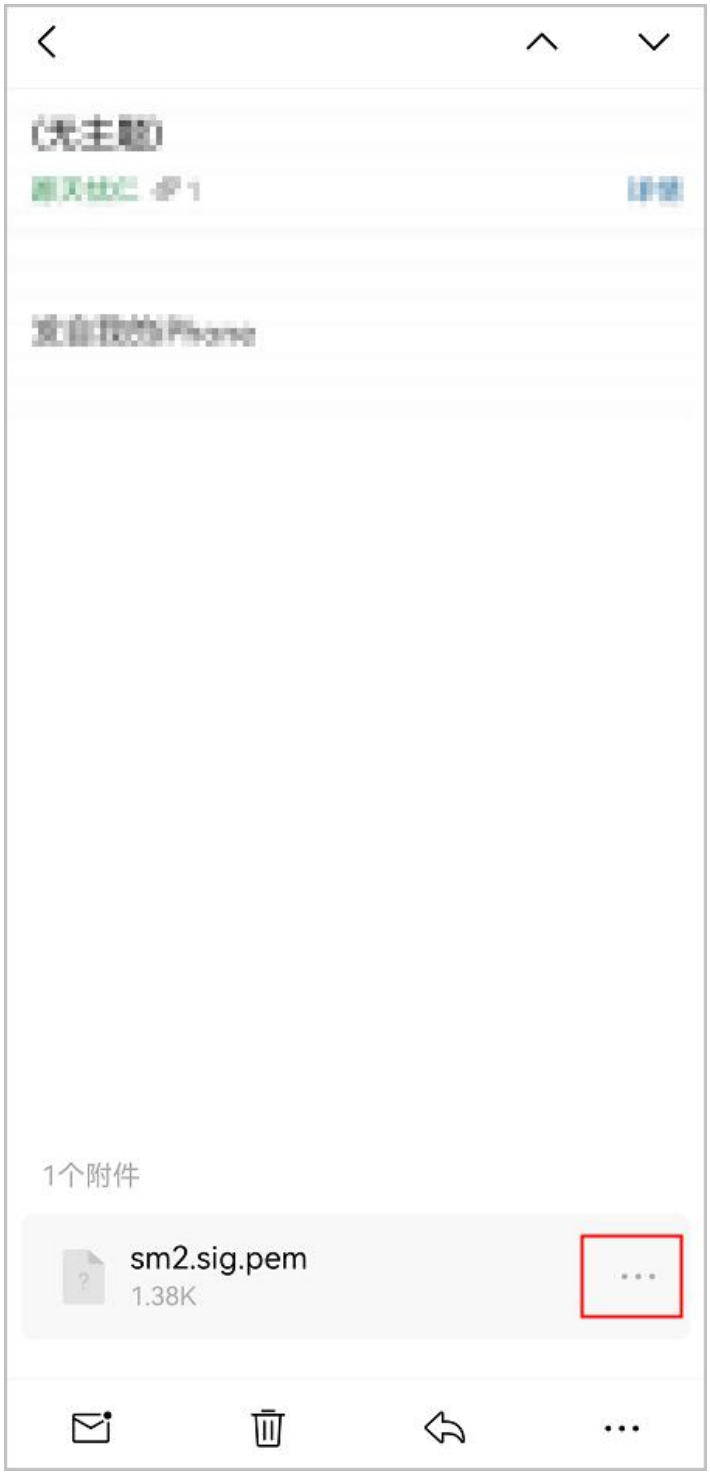
操作

移动版 UniConnect 客户端的具体操作，请参见 APP 内“ > 帮助”节点下的联机帮助。

8.1.2 证书认证场景

国密证书和非国密证书导入客户端方法一致，下面以国密证书导入 UniConnect 为例，介绍 UniConnect 导入并使用证书认证。

步骤 1 打开邮箱找到此文件，点击右下角的。



步骤 2 单击此文件（没有下载就会请求下载）选择**“分享文件”**。

步骤 3 选择 UniConnect。

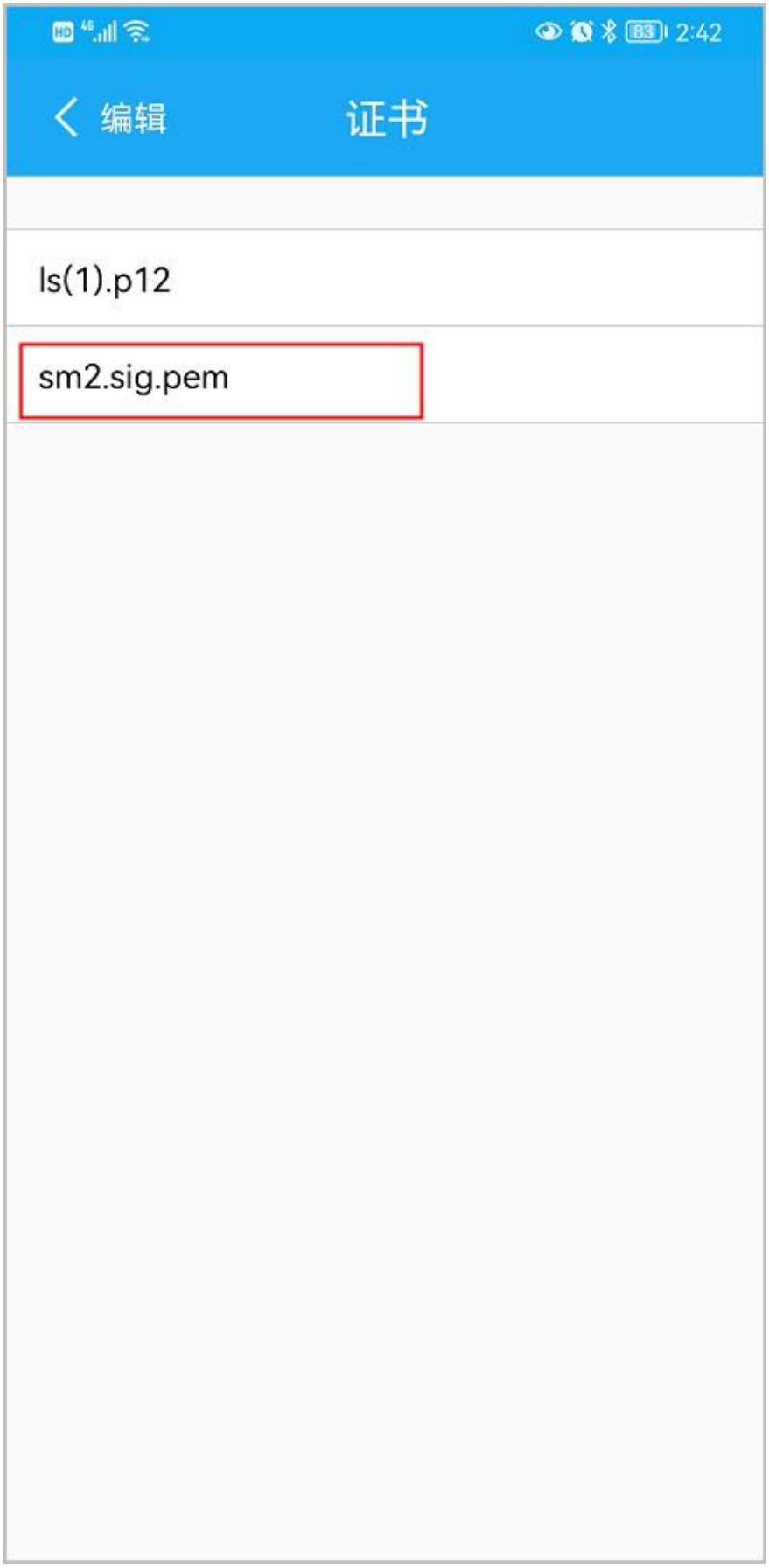
2:42
(无主题)
愿天忧仁 1
详情
请勿轻信邮件中的密保，汇款，中奖信息
分享文件
转为演示
转为PDF
AI 隐私保护
B612咔叽
EasyConnect
Fleet
Telegram
UniConnect
WLAN 直连
取消

步骤 4 单击“**确定**”。

2:42
返回
保存
提示
确认保存?
取消
确定

步骤 5 导入成功后开启“证书认证”开关。

步骤 6 单击“证书选择”选择国密证书。


2:42
编辑
证书
ls(1).p12
sm2.sig.pem

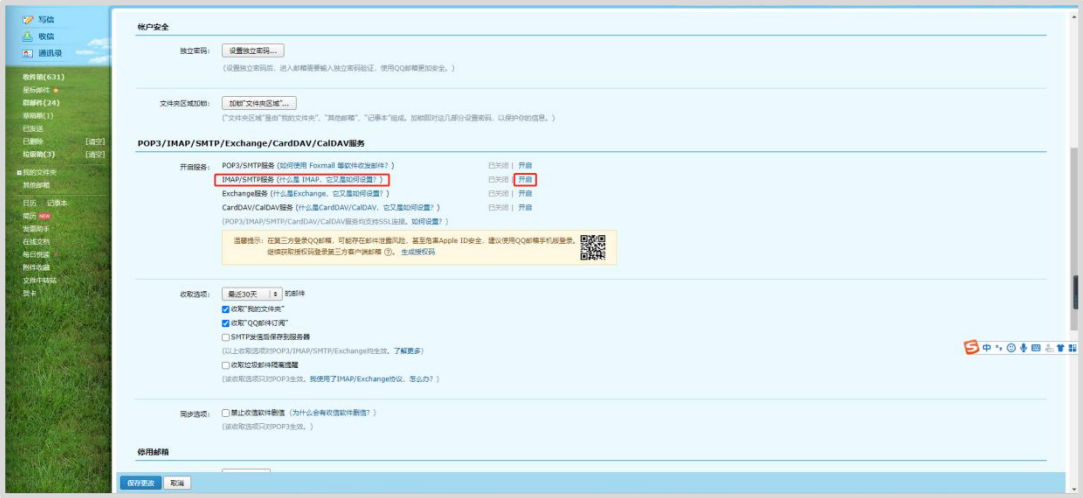
----结束

8.1.3 IOS 问题反馈

配置邮箱

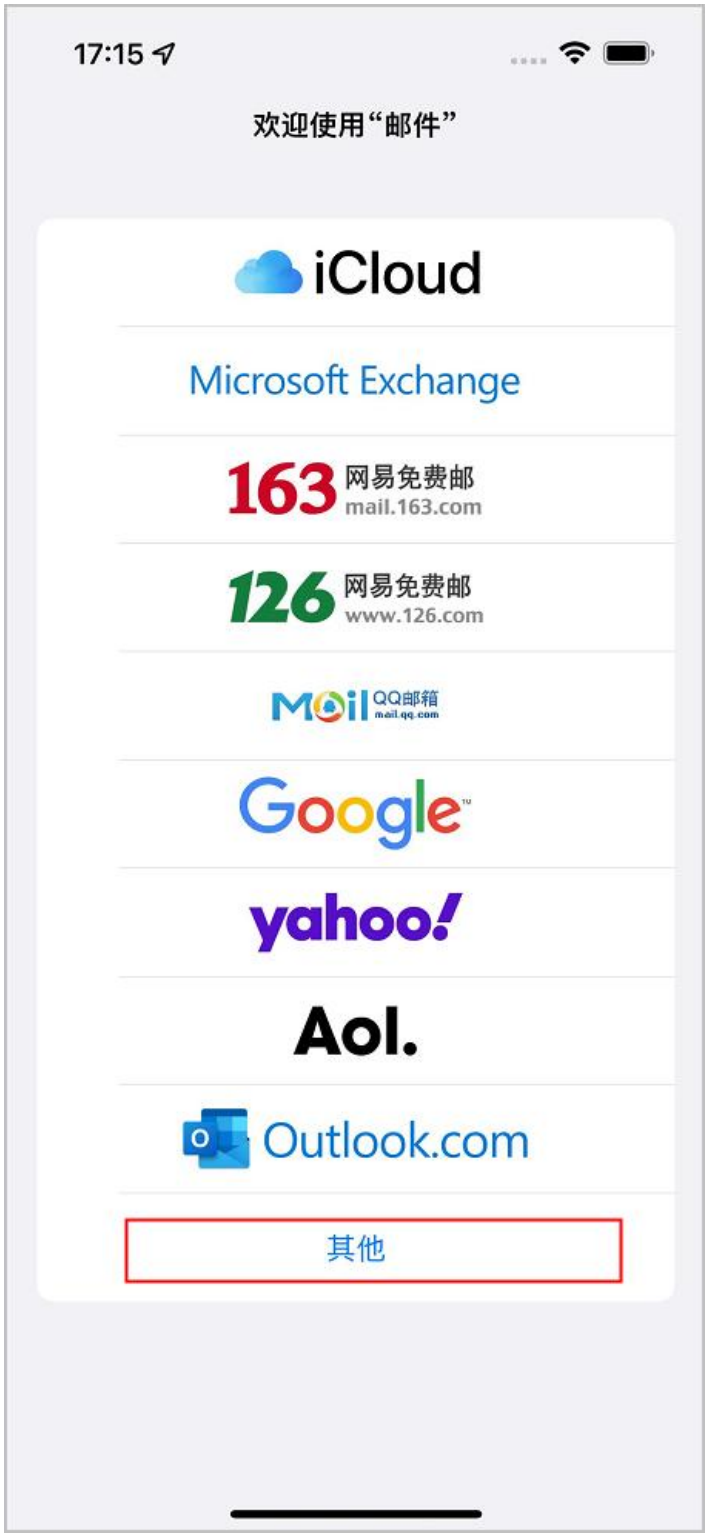
步骤 1 进入 QQ 邮箱，单击左上角“设置”，选择“账户”。

步骤 2 在 “账户”页中，单击 IMAP/SMTP 后的“开启”开启 IMAP 服务。



步骤 3 单击开启后发送短信，获得授权码。

步骤 4 打开手机桌面中的邮箱，选择“其他”QQ 邮箱。



步骤 5 将电脑页面显示的授权码填入此密码框。

步骤 6 单击右上角的 “下一步”。

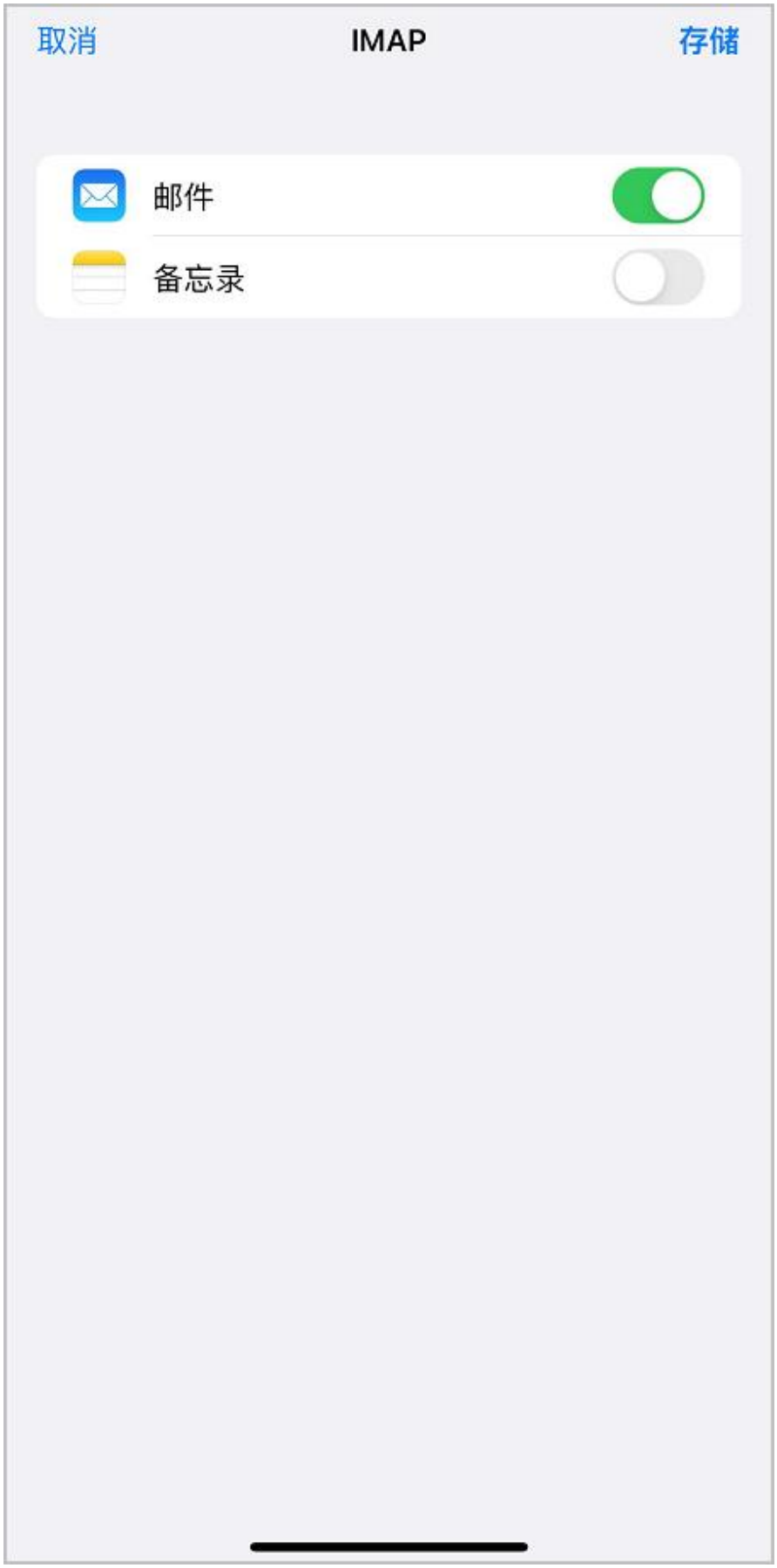
步骤 7 填写 QQ 账户信息：全名，电子邮箱，描述；

收件服务器： 主机名（imap.qq.com），用户名(为电子邮箱），密码（填写 step3 中获取的授权码）；

发件服务器所填写信息与收件服务器相同,（Host name 为 smtp.qq.com,密码填写授权码）

取消
帐户
完成
QQ 帐户信息
全名
电子邮件
描述
收件服务器
主机名
imap.qq.com
用户名
密码
发件服务器
SMTP
smtp.qq.com
高级

步骤 8 单击“存储”。


取消
IMAP
存储
邮件
备忘录

步骤 9 配置成功后，在登录页面选择“ >反馈”开启反馈日志后进行操作。

----结束

8.1.4 取消自动登录（安卓）

步骤 1 步骤 1 在登录时用户密码时开启自动登录，然后连接成功。

步骤 2 步骤 2 断开连接后，编辑任一连接将自动登录按钮关闭，单击“保存”即取消自动登录已。

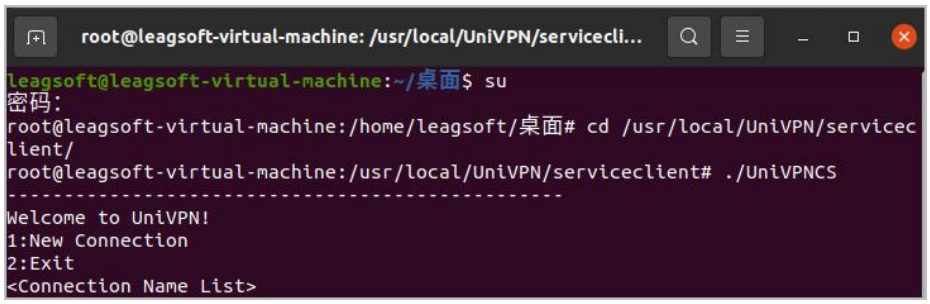
----结束

8.2 在 Linux 操作系统下通过命令行方式配置客户端

8.2.1 启动客户端

步骤 1 进入/usr/local/UniVPN/serviceclient 目录。

步骤 2 执行：./UniVPNCS，启动客户端。该命令普通用户和 root 用户均可执行。



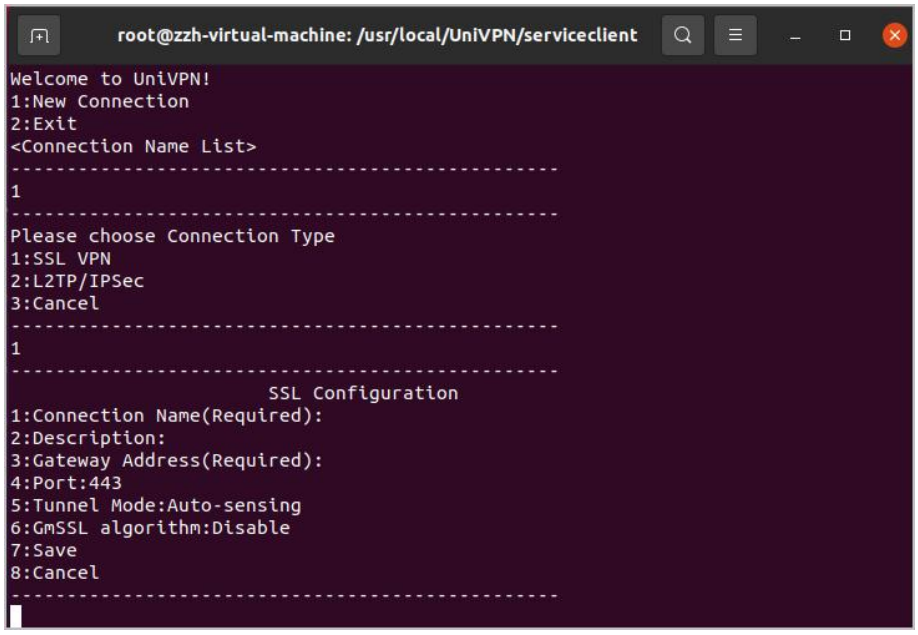
说明

通过命令行方式启动客户端前，请确保通过 UI 桌面启动的客户端已经关闭，二者无法同时运行。

----结束

8.2.2 配置 SSL VPN 连接

配置 SSL VPN



步骤 1 输入 **1**，创建新连接。

步骤 2 输入 **1**，选择创建的 VPN 类型为 SSL VPN。

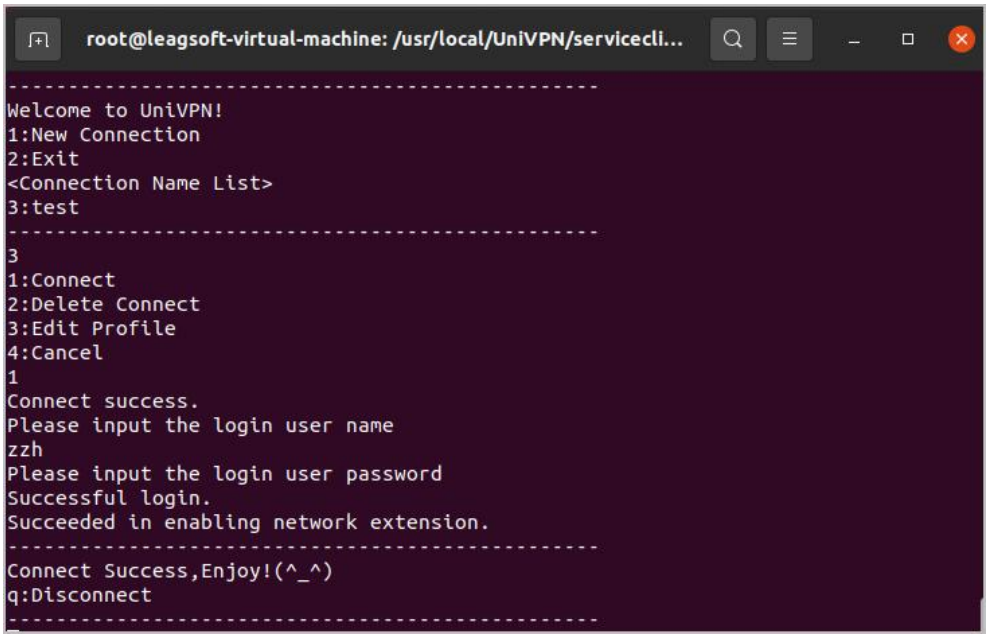
步骤 3 输入对应序号，完成参数 **1~5** 的配置。

- 1. Connection Name(Required)：连接名称；
- 2. Description：描述信息；
- 3. Gateway Address：远程网关地址；
- 4. Port(Required)：端口；
- 5. Tunnel Mode(Required)：隧道模式，可选模式有 Reliable Transmission（可靠传输模式）、Quick Transmission（快速传输模式）、Auto-sensing（自适应模式）。

步骤 4 输入 **7**，保存配置。

----结束

建立 SSL VPN 连接



步骤 1 输入对应序号，选择创建的 SSL VPN 连接。

步骤 2 输入 **1**，开始建立 SSL VPN 连接。

步骤 3 界面显示连接建立成功，输入用户名和密码进行登录。

----结束

说明

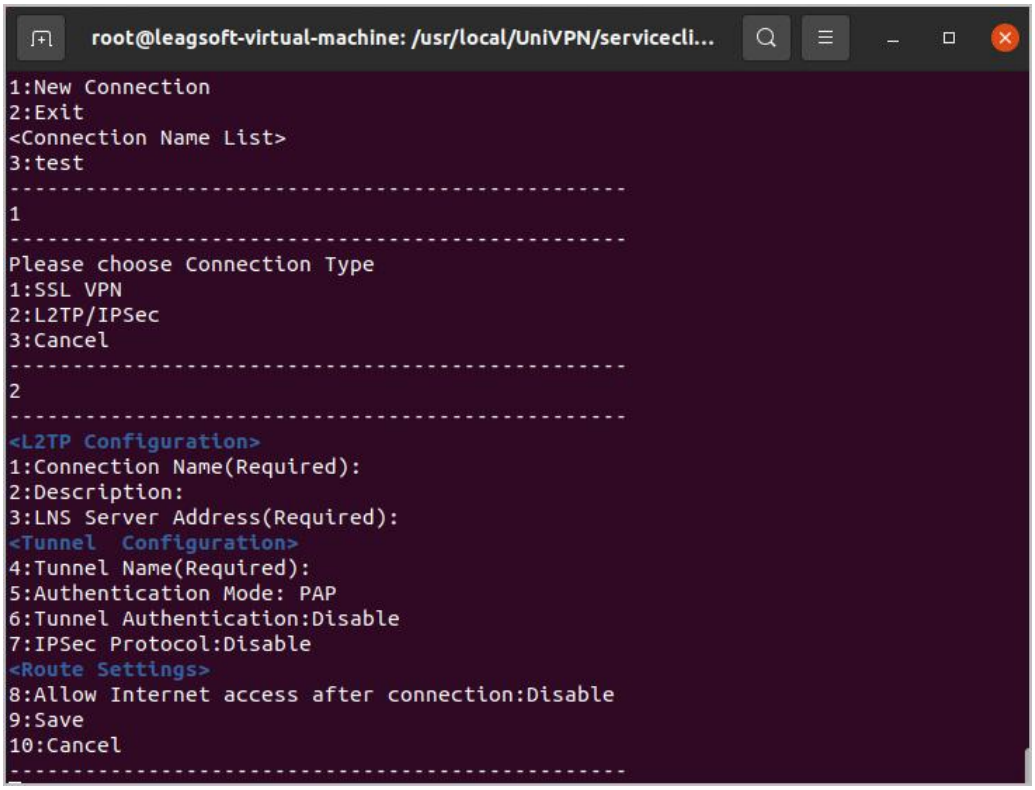
- 在 Linux 操作系统下通过命令行方式配置并建立的 SSL VPN 连接仅支持通过用户名/密码认证方式认证登录。
- 连接成功后，不能关闭该终端窗口，否则连接会断开。

断开 SSL VPN 连接

输入 **q**，即可断开连接。

8.2.3 配置 L2TP VPN 连接

配置 L2TP VPN



步骤 1 输入 **1**，创建新连接。

步骤 2 输入 **2**，选择创建的 VPN 类型为 L2TP/IPSec。

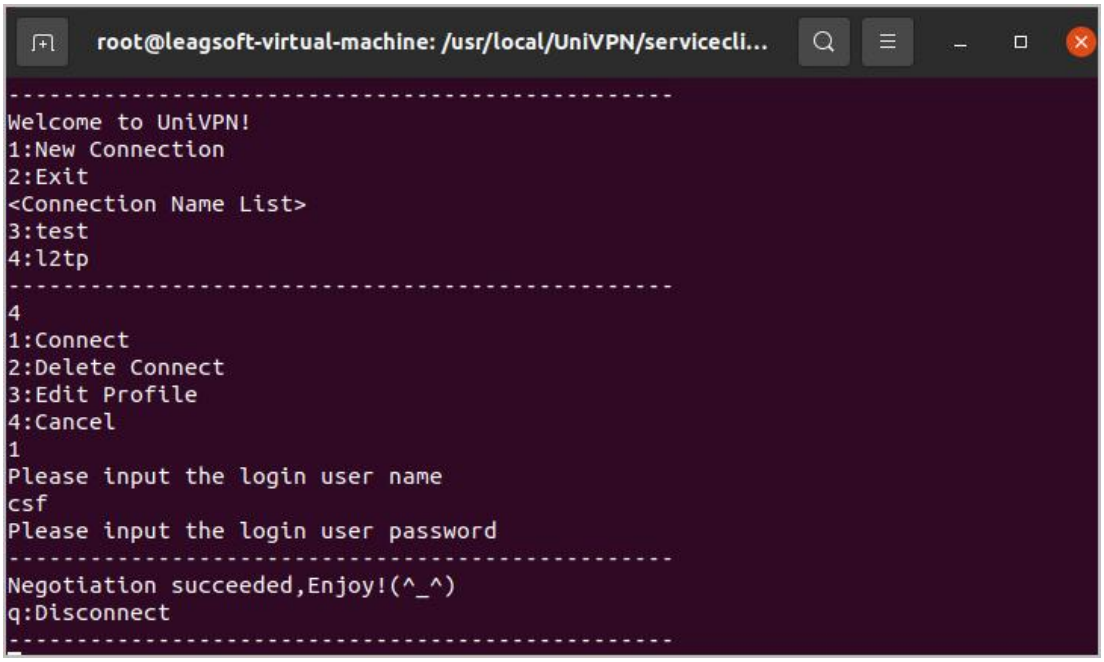
步骤 3 输入对应序号，完成参数 **1~8** 的配置。

- 1. Connection Name(Required)：连接名称；
- 2. Description：描述信息；
- 3. LNS Server Address(Required)：LNS 服务器地址；
- 4. Tunnel Name(Required)：隧道名称；
- 5. Authentication Mode：认证模式；
- 6. Tunnel Authentication：启用隧道验证功能，启用后，需要输入隧道验证密码（Tunnel Authentication Password）；
- 7. IPSec Protocol：启用 IPSec 安全协议，此功能请勿启用；
- 8. Allow Internet access after connection：路由设置，启用后，可以通过添加 IP 地址网段设置需要进入 VPN 隧道的待加密流量。

步骤 4 输入 **9**，保存配置。

----结束

建立 L2TP VPN 连接



步骤 1 输入对应序号，选择创建的 L2TP VPN 连接。

步骤 2 输入 **1**，开始建立 L2TP VPN 连接。

步骤 3 输入用户名和密码进行登录。

----结束

说明

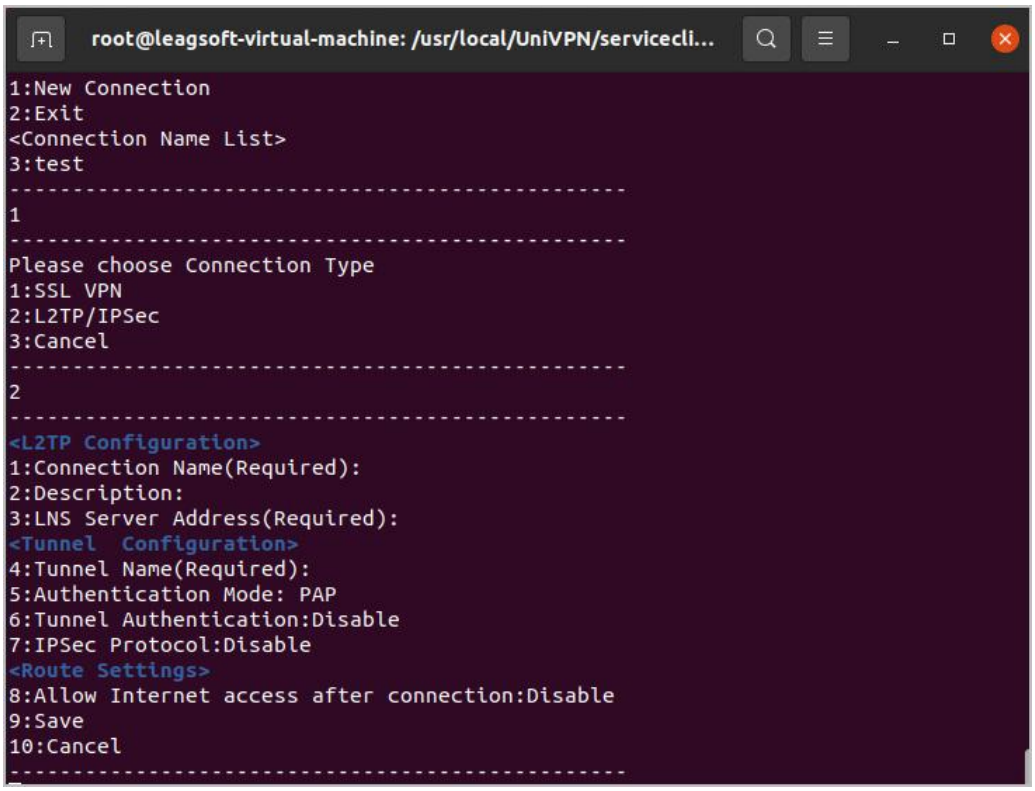
连接成功后，不能关闭该终端窗口，否则连接会断开。

断开 L2TP VPN 连接

输入 **q**，即可断开连接。

8.2.4 配置 L2TP over IPSec VPN 连接

配置 L2TP 参数



步骤 1 输入 **1**，创建新连接。

步骤 2 输入 **2**，选择创建的 VPN 类型为 L2TP/IPSec。

步骤 3 输入对应序号，完成参数 **1~6** 的配置。

- 1. Connection Name(Required)：连接名称；
- 2. Description：描述信息；
- 3. LNS Server Address(Required)：LNS 服务器地址；
- 4. Tunnel Name(Required)：隧道名称；
- 5. Authentication Mode：认证模式；
- 6. Tunnel Authentication：启用隧道验证功能，启用后，需要输入隧道验证密码（Tunnel Authentication Password）；

----结束

配置 IPSec 参数

```
root@leagsoft-virtual-machine: /usr/local/UniVPN/servicecli...
-----------------------------------------------
<L2TP Configuration>
1:Connection Name(Required):
2:Description:
3:LNS Server Address(Required):
<Tunnel  Configuration>
4:Tunnel Name(Required):
5:Authentication Mode: PAP
6:Tunnel Authentication:Disable
7:IPSec Protocol:Disable
<Route Settings>
8:Allow Internet access after connection:Disable
9:Save
10:Cancel
-----------------------------------------------
7
IPSec Protocol
1:enable
2:Disable
3:Cancel
1
-----------------------------------------------
<L2TP Configuration>
1:Connection Name(Required):
2:Description:
3:LNS Server Address(Required):
<Tunnel  Configuration>
4:Tunnel Name(Required):
5:Authentication Mode: PAP
6:Tunnel Authentication:Disable
7:IPSec Protocol:Enable
8:IPSec Authentication Mode:Pre-shared Key
  Pre-shared Key(Required):
<IPSEC Configuration>
9:IPSec Server address:Use LNS server address
10:Encapsulation Mode:Transmission mode
11:EPS Authentication Algorithm:SHA2-256
12:EPS Encryption Algorithm:AES-256
<IKE Basic Configuration>
```

```
<IKE Advanced Configuration>
17:PFS:Disable
18:SA Lifetime:86400
<IPSec Advanced Configuration>
19:SA Lifetime:3600
<Route Settings>
20:Route Settings:Mode Config
21:Save
22:Cancel
-----------------------------------------------
```

步骤 1 输入 **7**，启用 IPSec 安全协议。

步骤 2 输入对应序号，完成参数 **8~20** 的配置。

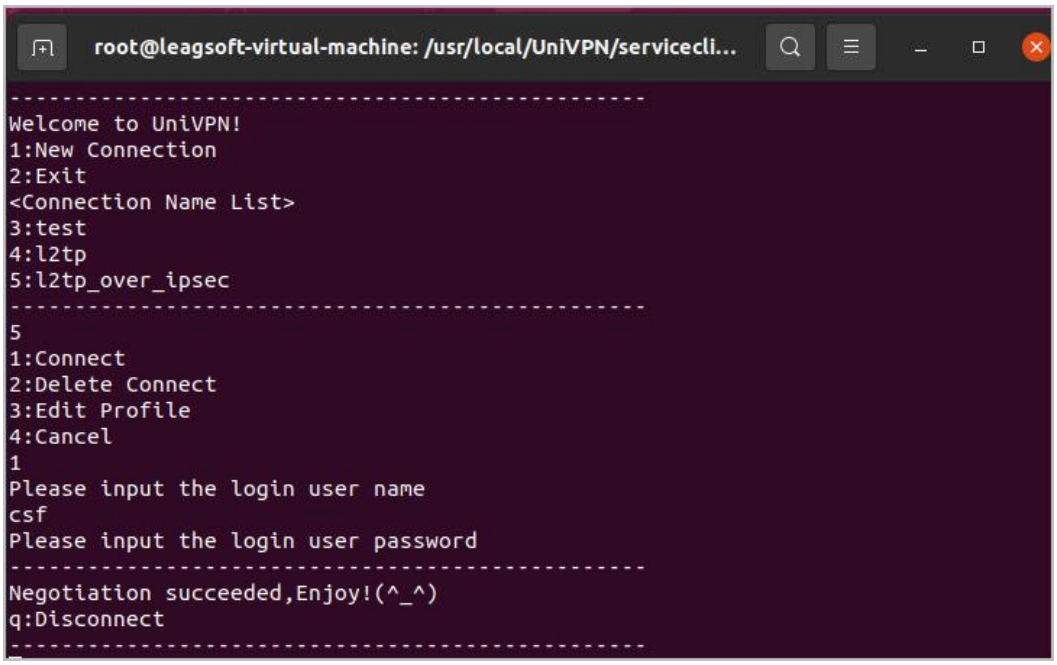
- 8. IPSec Authentication Mode：Linux 操作系统下 IPSec 的身份认证方式目前仅支持预共享密钥认证，预共享密钥方式下需要输入身份认证字（Pre-shared key）；
- 9. IPSec Server address：IPSec 服务器地址，缺省设置为使用 LNS 服务器地址（Use LNS server address）；
- 10. Encapsulation Mode：IPSec 封装模式，包括传输模式（Transmission mode）和隧道模式（Tunnel mode）两种；
- 11. ESP Authentication Algorithm：ESP 协议验证算法；
- 12. ESP Encryption Algorithm：ESP 协议加密算法；

- 13. Negotiation Mode：IKE 协商模式，包括主模式（Main Mode）和野蛮模式（Aggressive Mode）两种；
- 14. Authentication Algorithm：IKE 协商验证算法；
- 15. Encryption Algorithm：IKE 协商加密算法；
- 16. DH Group ID：IKE 协商 DH 组标识；
- 17. PFS：启用 PFS 特性，启用后，需要配置相应的安全参数（Security Parameter）；
- 18. SA Lifetime(IKE Advanced Configuration)：IKE 安全联盟生存周期；
- 19. SA Lifetime(IPSec Advanced Configuration)：IPSec 安全联盟生存周期；
- 20. Route Settings：路由设置，包括“Mode Config”模式和“Allow Internet access after connection”模式，设置为“Allow Internet access after connection”模式后，可以通过添加 IP 地址网段设置需要进入 VPN 隧道的待加密流量。

步骤 3 输入 **21**，保存配置。

----结束

建立 L2TP over IPSec VPN 连接



步骤 1 输入对应序号，选择创建的 L2TP over IPSec VPN 连接。

步骤 2 输入 **1**，开始建立 L2TP over IPSec VPN 连接。

步骤 3 输入用户名和密码进行登录。

----结束

说明

- 在 Linux 操作系统下通过命令行方式配置并建立的 L2TP over IPSec VPN 连接仅支持通过用户名/密码认证方式认证登录。
- 连接成功后，不能关闭该终端窗口，否则连接会断开。

断开 L2TP over IPSec VPN 连接

输入 **q**，即可断开连接。

8.3 在国产化操作系统下通过命令行方式配置客户端

8.3.1 启动客户端

步骤 1 进入/usr/local/UniVPN/serviceclient 目录。

步骤 2 执行：./UniVPNCS，启动客户端。该命令普通用户和 root 用户均可执行。

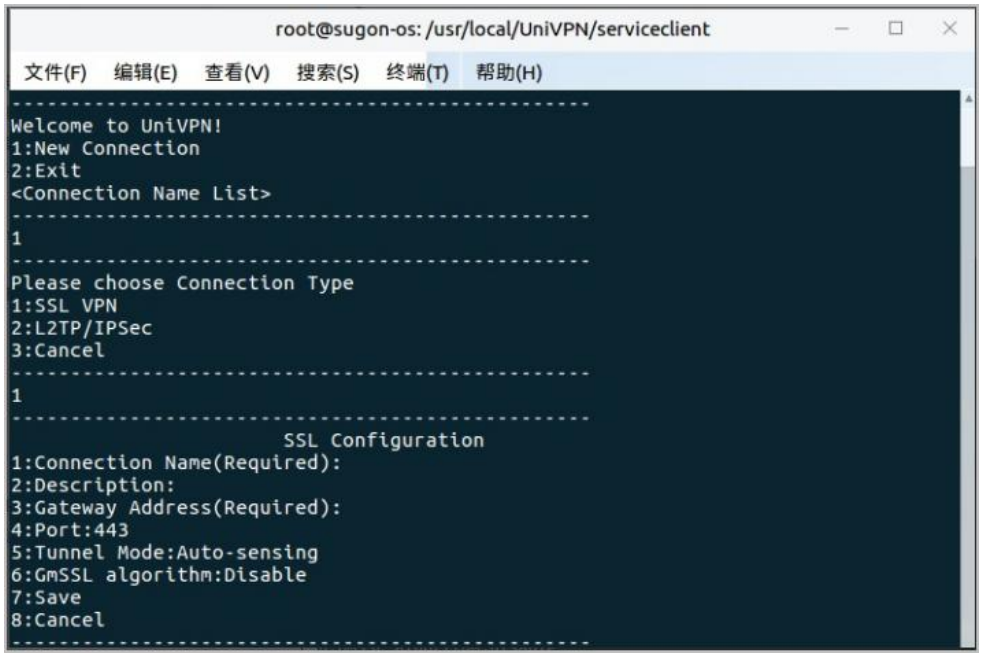
说明

通过命令行方式启动客户端前，请确保通过 UI 桌面启动的客户端已经关闭，二者无法同时运行。

----结束

8.3.2 配置 SSL VPN 连接

配置 SSL VPN



步骤 1 输入 **1**，创建新连接。

步骤 2 输入 **1**，选择创建的 VPN 类型为 SSL VPN。

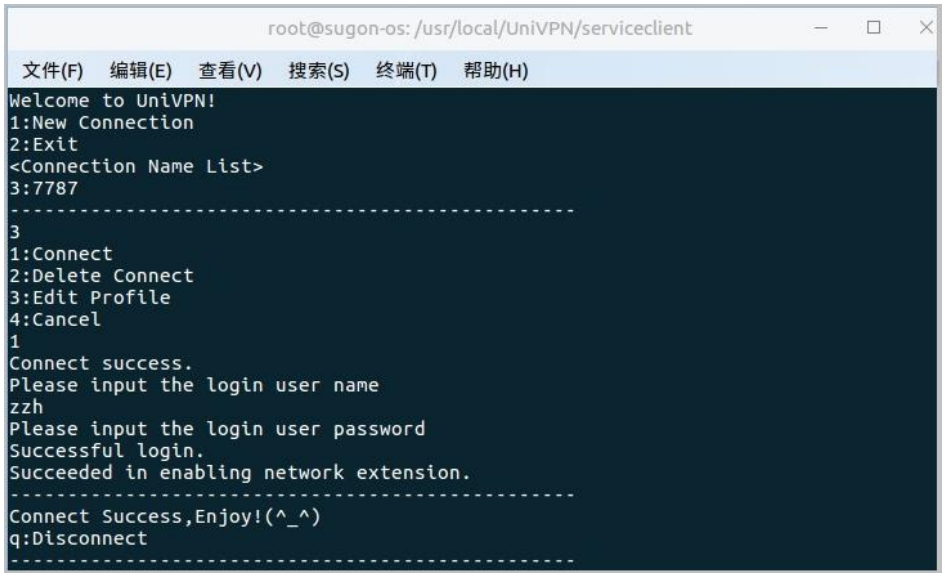
步骤 3 输入对应序号，完成参数 1~5 的配置。

- 1. Connection Name(Required)：连接名称；
- 2. Description：描述信息；
- 3. Gateway Address：远程网关地址；
- 4. Port(Required)：端口；
- 5. Tunnel Mode(Required)：隧道模式，可选模式有 Reliable Transmission（可靠传输模式）、Quick Transmission（快速传输模式）、Auto-sensing（自适应模式）。

步骤 4 输入 **7**，保存配置。

----结束

建立 SSL VPN 连接



步骤 1 输入对应序号，选择创建的 SSL VPN 连接。

步骤 2 输入 **1**，开始建立 SSL VPN 连接。

步骤 3 界面显示连接建立成功，输入用户名和密码进行登录。

----结束

说明

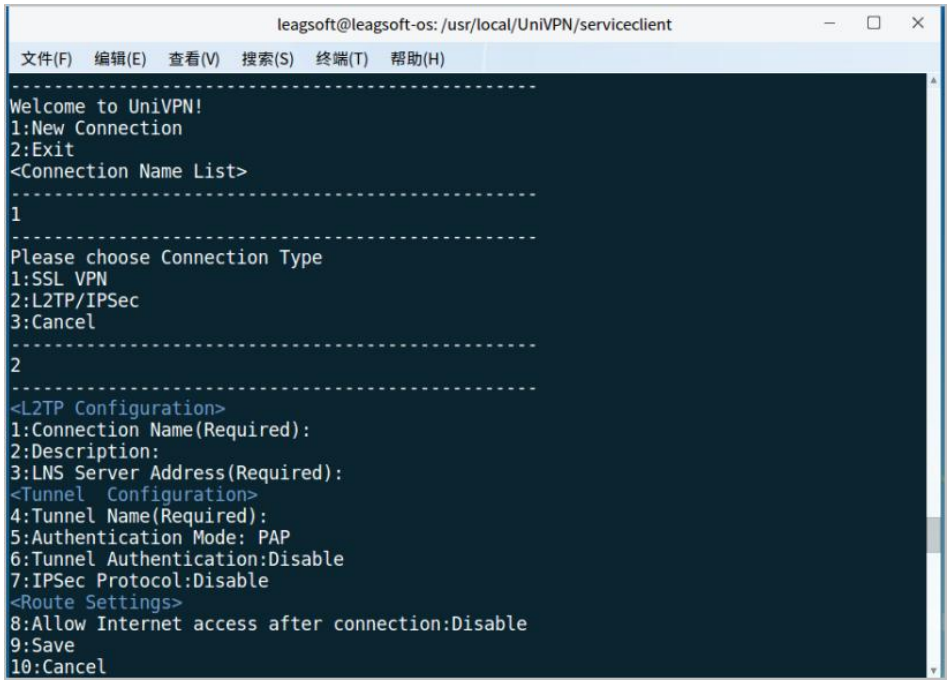
- 在国产化操作系统下通过命令行方式配置并建立的 SSL VPN 连接仅支持通过用户名/密码认证方式认证登录。
- 连接成功后，不能关闭该终端窗口，否则连接会断开。

断开 SSL VPN 连接

输入 **q**，即可断开连接。

8.3.3 配置 L2TP VPN 连接

配置 L2TP VPN



步骤 1 输入 **1**，创建新连接。

步骤 2 输入 **2**，选择创建的 VPN 类型为 L2TP/IPSec。

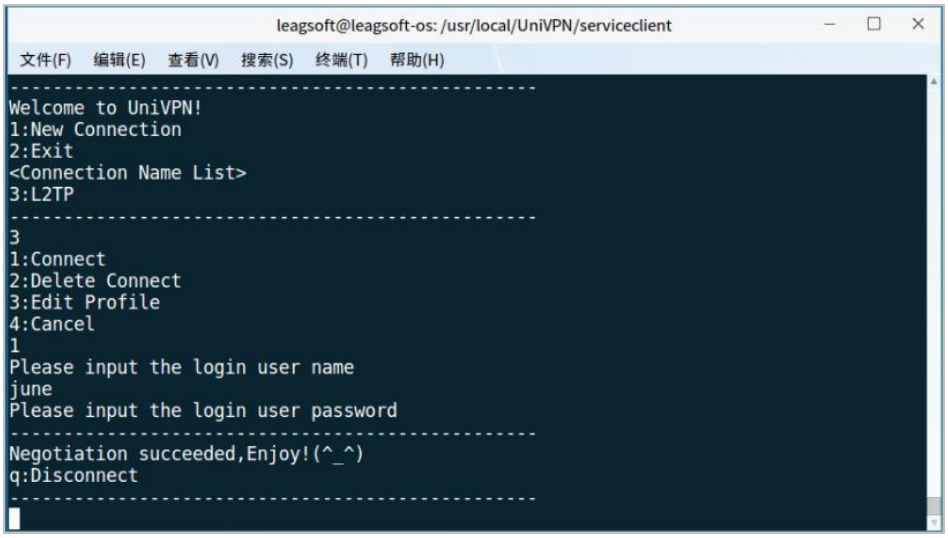
步骤 3 输入对应序号，完成参数 1~8 的配置。

- 1. Connection Name(Required)：连接名称；
- 2. Description：描述信息；
- 3. LNS Server Address(Required)：LNS 服务器地址；
- 4. Tunnel Name(Required)：隧道名称；
- 5. Authentication Mode：认证模式；
- 6. Tunnel Authentication：启用隧道验证功能，启用后，需要输入隧道验证密码（Tunnel Authentication Password）；
- 7. IPSec Protocol：启用 IPSec 安全协议，此功能请勿启用；
- 8. Allow Internet access after connection：路由设置，启用后，可以通过添加 IP 地址网段设置需要进入 VPN 隧道的待加密流量。

步骤 4 输入 **9**，保存配置。

----结束

建立 L2TP VPN 连接



步骤 1 输入对应序号，选择创建的 L2TP VPN 连接。

步骤 2 输入 **1**，开始建立 L2TP VPN 连接。

步骤 3 输入用户名和密码进行登录。

----结束

说明

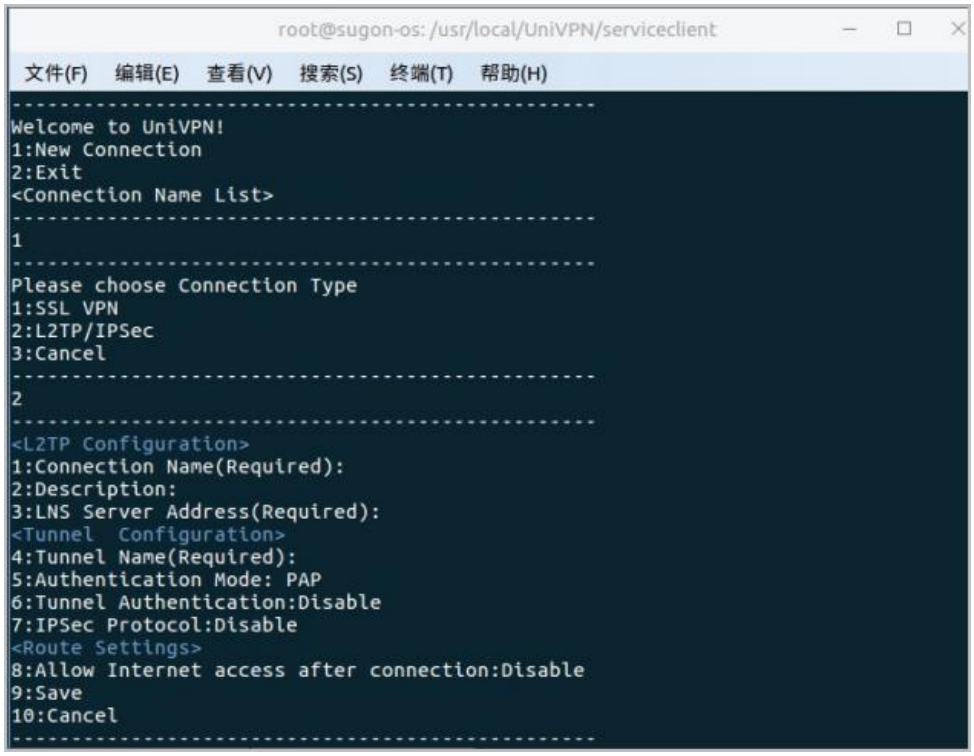
连接成功后，不能关闭该终端窗口，否则连接会断开。

断开 L2TP VPN 连接

输入 **q**，即可断开连接。

8.3.4 配置 L2TP over IPSec VPN 连接

配置 L2TP 参数



步骤 1 输入 **1**，创建新连接。

步骤 2 输入 **2**，选择创建的 VPN 类型为 L2TP/IPSec。

步骤 3 输入对应序号，完成参数 1~6 的配置。

- 1. Connection Name(Required)：连接名称；
- 2. Description：描述信息；
- 3. LNS Server Address(Required)：LNS 服务器地址；
- 4. Tunnel Name(Required)：隧道名称；
- 5. Authentication Mode：认证模式；
- 6. Tunnel Authentication：启用隧道验证功能，启用后，需要输入隧道验证密码（Tunnel Authentication Password）；

----结束

配置 IPSec 参数

步骤 1 输入 **7**，启用 IPSec 安全协议。

步骤 2 输入对应序号，完成参数 8~20 的配置。

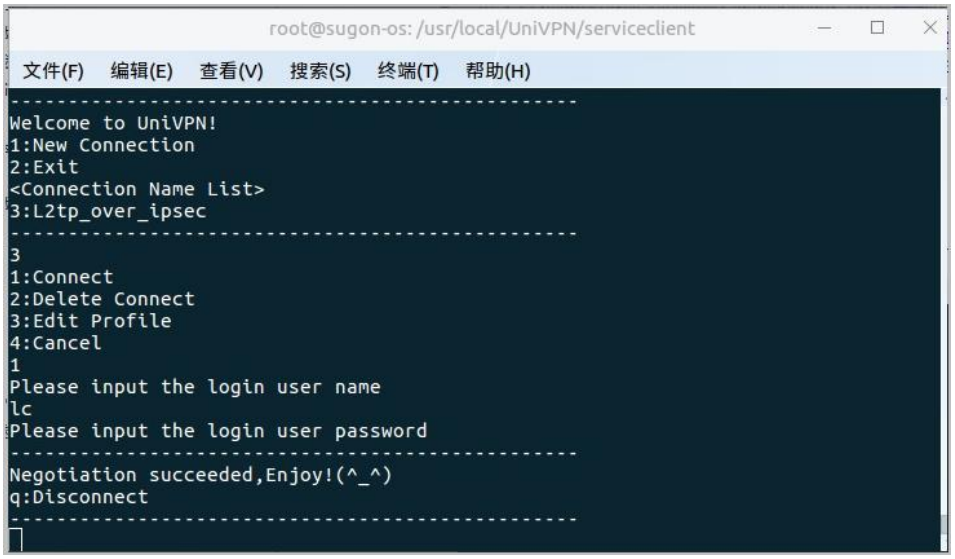
- 8. IPSec Authentication Mode：Linux 操作系统下 IPSec 的身份认证方式目前仅支持预共享密钥认证，预共享密钥方式下需要输入身份认证字（Pre-shared key）；
- 9. IPSec Server address：IPSec 服务器地址，缺省设置为使用 LNS 服务器地址（Use LNS server address）；
- 10. Encapsulation Mode：IPSec 封装模式，包括传输模式（Transmission mode）和隧道模式（Tunnel mode）两种；
- 11. ESP Authentication Algorithm：ESP 协议验证算法；
- 12. ESP Encryption Algorithm：ESP 协议加密算法；
- 13. Negotiation Mode：IKE 协商模式，包括主模式（Main Mode）和野蛮模式（Aggressive Mode）两种；

- 14. Authentication Algorithm：IKE 协商验证算法；
- 15. Encryption Algorithm：IKE 协商加密算法；
- 16. DH Group ID：IKE 协商 DH 组标识；
- 17. PFS：启用 PFS 特性，启用后，需要配置相应的安全参数（Security Parameter）；
- 18. SA Lifetime(IKE Advanced Configuration)：IKE 安全联盟生存周期；
- 19. SA Lifetime(IPSec Advanced Configuration)：IPSec 安全联盟生存周期；
- 20. Route Settings：路由设置，包括“Mode Config”模式和“Allow Internet access after connection”模式，设置为“Allow Internet access after connection”模式后，可以通过添加 IP 地址网段设置需要进入 VPN 隧道的待加密流量。

步骤 3 输入 21，保存配置。

----结束

建立 L2TP over IPSec VPN 连接



步骤 1 输入对应序号，选择创建的 L2TP over IPSec VPN 连接。

步骤 2 输入 **1**，开始建立 L2TP over IPSec VPN 连接。

步骤 3 输入用户名和密码进行登录。

----结束

说明

- **说明** 在 Linux 操作系统下通过命令行方式配置并建立的 L2TP over IPSec VPN 连接仅支持通过用户名/密码认证方式认证登录。
- 连接成功后，不能关闭该终端窗口，否则连接会断开。

断开 L2TP over IPSec VPN 连接

输入 **q**，即可断开连接。

8.4 VPN 配置及连接模板

8.4.1 SSL VPN 配置及连接模板

表 8-4 SSL VPN 配置及连接模板

<table>
<tr><td colspan="7">SSL VPN 配置模板</td></tr>
<tr><td>序号</td><td colspan="5">配置项</td><td>配置参数</td></tr>
<tr><td rowspan="4">1</td><td rowspan="4">是否使用代理设置？</td><td colspan="4">否</td><td>-</td></tr>
<tr><td rowspan="3">是</td><td rowspan="3">使用何种代理设置？</td><td>使用系统代理</td><td rowspan="3">地址、端口、账号及密码</td><td rowspan="3"></td></tr>
<tr><td>使用 HTTP/HTTPS 代理</td></tr>
<tr><td>使用 Socks5 代理</td></tr>
<tr><td>2</td><td colspan="5">连接名称</td><td></td></tr>
<tr><td>3</td><td colspan="5">描述信息</td><td></td></tr>
<tr><td>4</td><td colspan="5">远程网关地址</td><td></td></tr>
<tr><td>5</td><td colspan="5">端口</td><td></td></tr>
<tr><td rowspan="3">6</td><td rowspan="3">使用何种隧道模式？</td><td colspan="4">可靠传输模式</td><td>-</td></tr>
<tr><td colspan="4">快速传输模式</td><td>-</td></tr>
<tr><td colspan="4">自适应模式</td><td>-</td></tr>
<tr><td>7</td><td colspan="5">是否开启路由覆盖？</td><td>-</td></tr>
<tr><td>8</td><td colspan="5">是否开启国密算法？</td><td>-</td></tr>
<tr><td colspan="7">SSL VPN 连接模板</td></tr>
<tr><td>序号</td><td>用户</td><td colspan="5">所需的验证信息</td></tr>
</table>

	身份认证方式		
1	通过用户名/密码认证	用户名	
		密码	
2	通过导入PKI数字证书认证	使用证书匿名认证	可用的 PKI 数字证书
		使用证书挑战认证	可用的 PKI 数字证书
			证书中提取的用户名对应的登录密码
3	通过USB-Key证书认证	使用证书匿名认证	可用的 USB-Key 设备及对应的驱动程序、PIN 码
		使用证书挑战认	可用的 USB-Key 设备及对应的驱动程序、PIN 码
			证书中提取的用户名对应的登录密码

		证		
4	通过双因子认证	初次认证方式	通过用户名/密码方式认证（参考上文）	
			通过导入 PKI 数字证书方式认证（参考上文）	
			通过 USB-Key 证书方式认证（参考上文）	
		双因子认证方式	通过动态令牌码认证	从动态令牌码接收设备上获取
			通过短信验证码认证	从短信验证码接收设备上获取

8.4.2 L2TP VPN 配置及连接模板

表 8-5 L2TP VPN 配置及连接模板

L2TP VPN 配置模板				
序号	**配置项**			**配置参数**
代理设置				
1	是否使用代理设置？	否		-
		是（使用Socks5代理）	地址	
			端口	
			账号	
			密码	
L2TP 设置				
2	连接名称			
3	描述信息			
4	LNS 服务器地址			

<table>
<tr><td colspan="4">隧道设置</td></tr>
<tr><td>5</td><td colspan="2">隧道名称</td><td></td></tr>
<tr><td rowspan="2">6</td><td rowspan="2">使用何种认证模式？</td><td>CHAP 认证</td><td>-</td></tr>
<tr><td>PAP 认证</td><td>-</td></tr>
<tr><td rowspan="2">7</td><td rowspan="2">是否启用隧道验证？</td><td colspan="2">否</td><td>-</td></tr>
<tr><td>是</td><td>隧道验证密码</td><td></td></tr>
<tr><td colspan="4">路由设置</td></tr>
<tr><td rowspan="3">8</td><td colspan="2">不勾选“连接成功后允许访问 Internet”</td><td>-</td></tr>
<tr><td colspan="2">勾选“连接成功后允许访问 Internet”
未在 IP 地址列表框中添加 IP 地址</td><td>-</td></tr>
<tr><td>勾选“连接成功后允许访问 Internet”
并在 IP 地址列表框中添加 IP 地址</td><td>待添加的 IP 地址信息</td><td></td></tr>
<tr><td colspan="4">L2TP VPN 连接模板</td></tr>
</table>

序号	用户身份认证方式	所需的验证信息
1	通过用户名/密码认证	用户名
		密码

8.4.3 L2TP over IPSec VPN 配置及连接模板

表 8-6 L2TP over IPSec VPN 配置及连接模板

L2TP over IPSec VPN 配置模板				
序号	配置项			配置参数
代理设置				
1	是否使用代理设置？	否		-
		是（使用 Socks5 代理）	地址	
			端口	
			账号	
			密码	
L2TP 设置				
2	连接名称			
3	描述信息			
4	LNS 服务器地址			
隧道设置				
5	隧道名称			

6	使用何种认证模式？	CHAP 认证		-
		PAP 认证		-
7	是否启用隧道验证？	否		-
		是	隧道验证密码	
启用 IPSec 安全协议				
8	使用何种 IPSec 身份认证方式？	预设共享密钥认证	身份认证字	
		USB-Key 数字签名认证	USB PIN 码	
IPSec 设置				
9	IPSec 服务器地址	L2TP VPN 和 IPSec VPN 网关是否相同？	否	-
			是	勾选“使用 LNS 服务器地址”
10	使用何种封装模式？	隧道模式		-
		传输模式		-
11	使用何 ESP 协议验证算法？	MD5		-
		SHA1		-
		SHA2-256		-
12	使用何 ESP 协议加密算法？	DES		-
		3DES		-
		AES		-
IKE 设置				
13	使用何种协商模式？	主模式		-
		野蛮模式		-
14	使用何种 ID 类型？	IP 地址类型		-
		名字类型		-
15	本端名字（身份类型选择“名字”时，需要设置此参数）			
16	安全网关名字（身份类型选择“名字”时，需要设置此参数）			

17	验证算法	MD5			-
		SHA1			-
		SHA2-25			-
18	加密算法	DES-CBC			-
		3DES-CBC			-
		AES-128			
		AES-192			-
		AES-256			-
19	DH 组标识	Group1			-
		Group2			-
		Group5			-
IKE 高级设置					
20	是否启用 PFS 特性？	否			-
		是	安全参数	Group1	-
				Group2	-
				Group5	-
21	安全联盟生存周期				
IPSec 高级设置					
22	安全联盟生存周期				
路由设置					
23	选择“Mode Config”				-
	勾选“连接成功后允许访问 Internet” 未在 IP 地址列表框中添加 IP 地址				-
	勾选“连接成功后允许访问 Internet” 并在 IP 地址列表框中添加 IP 地址		待添加的 IP 地址信息		
L2TP over IPSec VPN 连接模板					
序号	**用户身份认证方式**				**所需的验证信息**
1	通过用户名/密码认证				用户名
					密码

2	通过导入 PKI 数字证书认证	可用的 PKI 数字证书
		用户名
		密码
3	通过 USB-Key 证书认证	可用的 USB-Key 设备及对应的驱动程序、PIN 码
		用户名
		密码