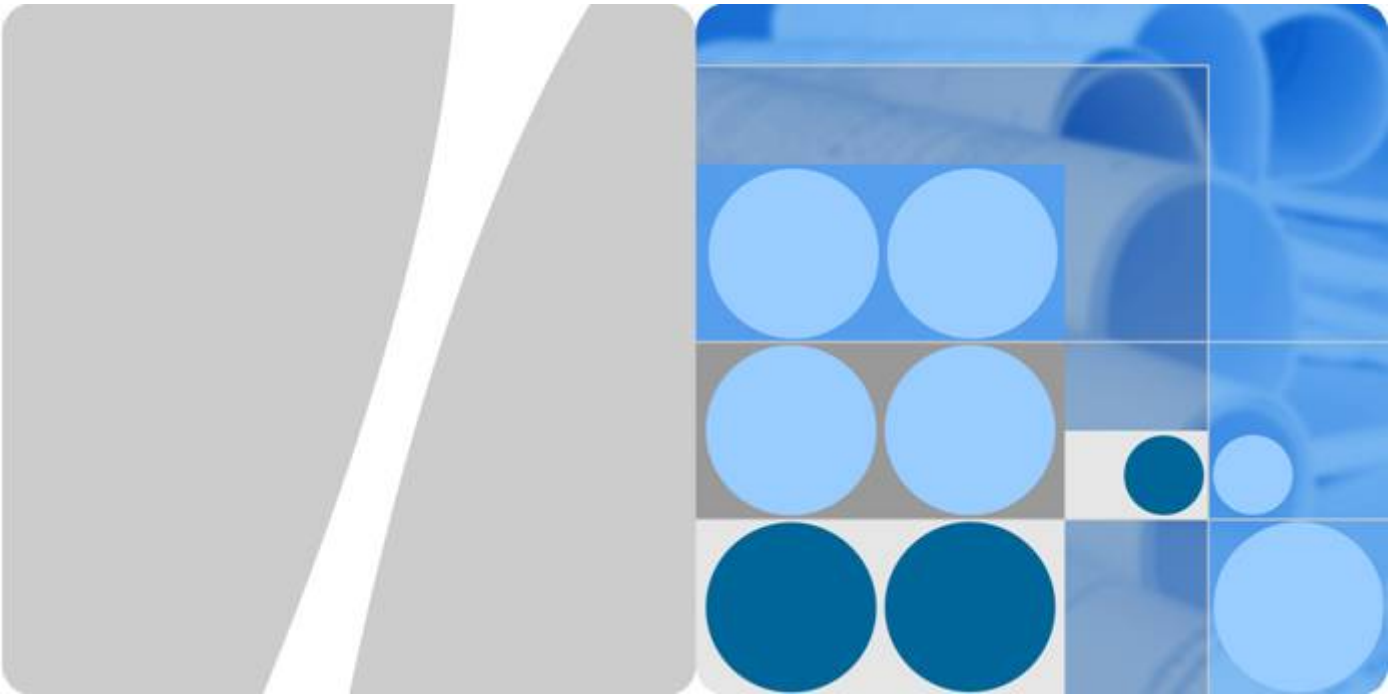


HUAWEI SecoClient 客户端

终端用户接入指南

文档版本　06

发布日期　2020-07-06

华为技术有限公司

HUAWEI

商标声明


和其他华为商标均为华为技术有限公司的商标。
本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为公司对本文档内容不做任何明示或默示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

华为技术有限公司

地址： 深圳市龙岗区坂田华为总部办公楼 邮编：518129

网址： https://www.huawei.com

客户服务邮箱： support@huawei.com

客户服务电话： 4008302118

目 录

1 文档信息 1
2 从这里开始 6
3 安装软件 8
3.1 安装前须知 8
3.2 获取软件安装包 10
3.3 在 Windows 操作系统上安装软件 12
3.4 在 Mac OS 操作系统上安装软件 12
3.5 在 Linux 操作系统上安装软件 13
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 22
4.4 通过导入配置文件的方式配置 VPN 连接 28
5 建立 VPN 连接 31
5.1 发起 VPN 连接 31
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 35
6 可选配置 37
6.1 卸载软件 37
6.2 更新升级 38
6.3 修改登录密码 39
6.4 其他配置 39
7 故障处理 41
7.1 收集用于故障排除的信息 41
7.1.1 收集错误报告 41
7.1.2 导出配置文件 43
7.2 安装及更新类故障 44
7.3 连接类故障 44

7.4 业务类故障 45
8 附录 48
8.1 移动客户端 48
8.2 在 Linux 操作系统下通过命令行方式配置客户端 51
8.2.1 启动客户端 51
8.2.2 配置 SSL VPN 连接 52
8.2.3 配置 L2TP VPN 连接 54
8.2.4 配置 L2TP over IPSec VPN 连接 56
8.3 VPN 配置及连接模板 59
8.3.1 SSL VPN 配置及连接模板 59
8.3.2 L2TP VPN 配置及连接模板 60
8.3.3 L2TP over IPSec VPN 配置及连接模板 61

1 文档信息

产品版本

本文档适用于5.0.1及以后版本的SecoClient客户端产品。

读者对象

本文档面向需要通过SecoClient客户端建立VPN连接的移动终端接入用户。您可以参考**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	V100R001C30SPCa00及以后版本 V500R001C30SPC100及以后版本	• Windows • Mac OS • Linux（V500R005C10SPC300及以后版本配套支持） • iOS（V500R001C60SPC500及以后版本配套支持） • Android（V500R005C00SPC100及以后版本配套支持）
USG6000E	V600R006C00及以后版本	• Windows • Mac OS • Linux（V600R006C00SPC300及以后版本配套支持） • iOS • Android

产品名称	产品版本	操作系统
USG9500	V500R001C30SPC100及以后版本	• Windows • Mac OS • Linux（V500R005C10SPC300及以后版本配套支持） • iOS（V500R001C60SPC500及以后版本配套支持） • Android（V500R005C00SPC100及以后版本配套支持）
Eudemon200E-N	V100R001C30SPCa00及以后版本 V500R002C00SPC100及以后版本	• Windows • Mac OS • Linux（V500R005C10SPC300及以后版本配套支持） • iOS（V500R002C20SPC500及以后版本配套支持） • Android（V500R005C00SPC100及以后版本配套支持）
Eudemon200E-G	V600R006C00及以后版本	• Windows • Mac OS • Linux（V600R006C00SPC300及以后版本配套支持） • iOS • Android
Eudemon1000E-N	V100R001C30SPCa00及以后版本 V500R002C00SPC100及以后版本	• Windows • Mac OS • Linux（V500R005C10SPC300及以后版本配套支持） • iOS（V500R002C20SPC500及以后版本配套支持） • Android（V500R005C00SPC100及以后版本配套支持）
Eudemon1000E-G	V600R006C00及以后版本	• Windows • Mac OS • Linux（V600R006C00SPC300及以后版本配套支持） • iOS • Android

产品名称	产品版本	操作系统
Eudemon8000E-X	V500R002C00SPC100及以后版本	• Windows • Mac OS • Linux（V500R005C10SPC300及以后版本配套支持） • iOS（V500R002C20SPC500及以后版本配套支持） • Android（V500R005C00SPC100及以后版本配套支持）
SVN5600	V200R003C10SPCa00及以后版本	• Windows • Mac OS
SVN5800	V200R003C10SPCa00及以后版本	• Windows • Mac OS
SVN5800-C	V200R003C10SPCa00及以后版本	• Windows • Mac OS
SeMG9811	V500R002C20SPC100及以后版本	• Windows • Mac OS • Linux（V500R005C10SPC300及以后版本配套支持） • iOS（V500R002C20SPC500及以后版本配套支持） • Android（V500R005C00SPC100及以后版本配套支持）
NGFW Module	V100R001C30SPCa00及以后版本 V500R002C00SPC100及以后版本	• Windows • Mac OS • Linux（V500R005C10SPC300及以后版本配套支持） • iOS（V500R002C20SPC500及以后版本配套支持） • Android（V500R005C00SPC100及以后版本配套支持）
USG6000V	V500R003C00SPC100及以后版本	• Windows • Mac OS • Linux（V500R005C10SPC300及以后版本配套支持） • iOS（V500R005C00SPC100及以后版本配套支持） • Android（V500R005C00SPC100及以后版本配套支持）

产品名称	产品版本	操作系统
Eudemon1000E-V	V500R003C00SPC100及以后版本	• Windows • Mac OS • Linux（V500R005C10SPC300及以后版本配套支持） • iOS（V500R005C00SPC100及以后版本配套支持） • Android（V500R005C00SPC100及以后版本配套支持）

说明

- 上表中列出的不同操作系统下的SecoClient客户端与网关之间的版本配套关系已经通过全量测试验证，明确宣称支持。
- 在实际使用时，由于SecoClient客户端是一个独立的VPN接入软件，与网关之间没有强绑定关系，因此上述配套关系以外的网关版本也可能支持与SecoClient客户端进行对接，具体支持情况以实际测试验证结果为准。

修订记录

文档版本 06 (2020-07-06)

第六次正式发布，配套SecoClient 7.0.3版本。

新增支持OS X 10.15.x版本的Mac操作系统，不再支持OS X 10.11.x 及以前版本的Mac操作系统。

对Linux版本的SecoClient，不再支持Ubuntu-14.4.04（32位/64位）和Ubuntu-16.4.04（32位），仅支持Ubuntu-16.4.04（64位）。

文档版本 05 (2019-05-21)

第五次正式发布，配套SecoClient 7.0.2版本。

SecoClient在SSL VPN场景下新增支持国密算法。

Windows版本的SecoClient在SSL VPN场景下新增支持路由覆盖。

Linux版本的SecoClient支持终端安全。

文档版本 04 (2018-12-28)

第四次正式发布，配套SecoClient 6.0.3版本。

SecoClient新增支持Linux操作系统。

文档版本 03 (2018-12-10)

第三次正式发布，配套SecoClient 6.0.2版本。

SecoClient开始支持与USG6000E、Eudemon200E-G、Eudemon1000E-G建立VPN隧道。

文档版本 02 (2018-06-30)

第二次正式发布，配套SecoClient 5.0.2版本。

文档版本 01 (2018-06-26)

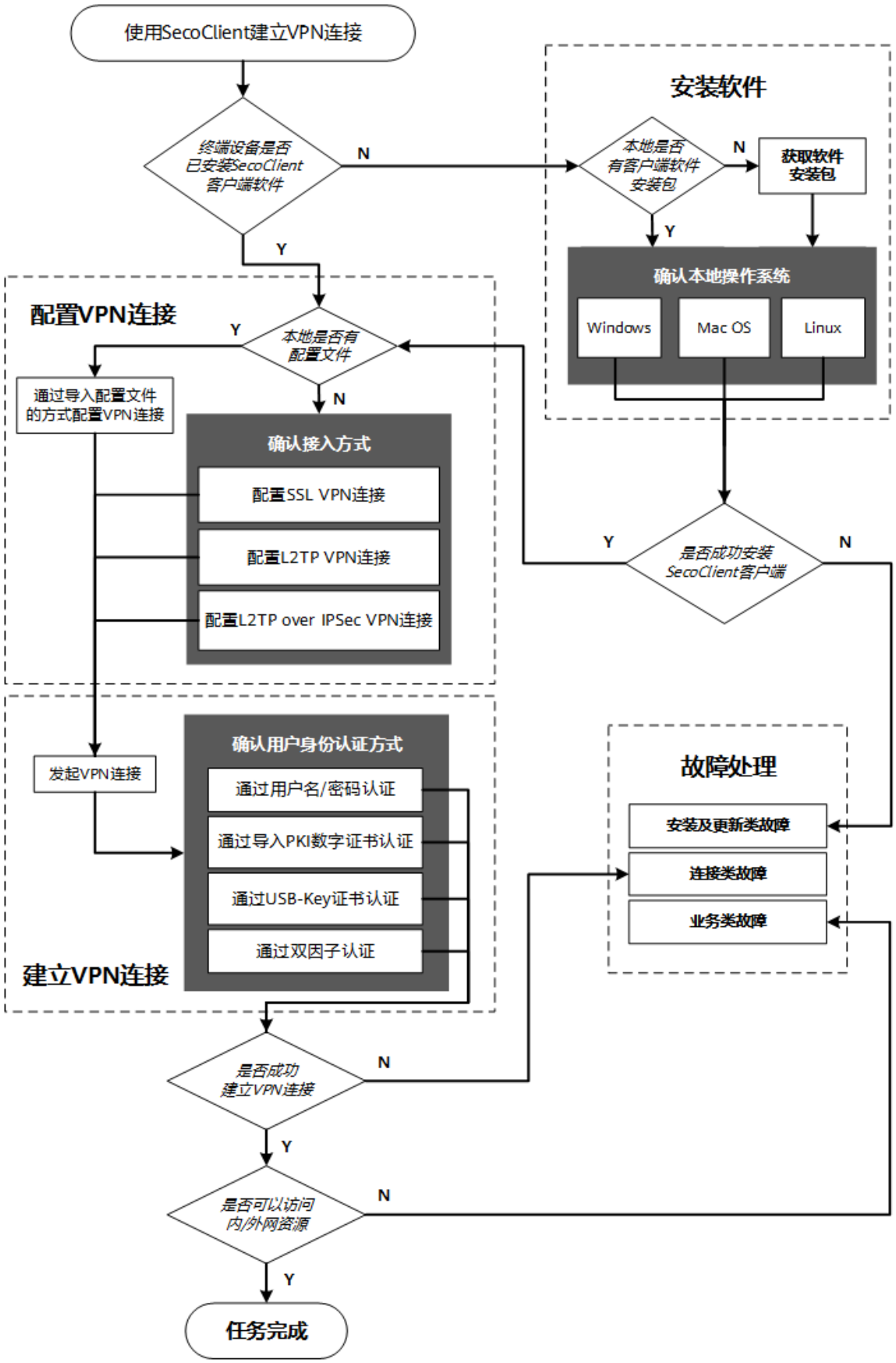
第一次正式发布，配套SecoClient 5.0.1版本。

2 从这里开始

SecoClient客户端是华为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SecoClient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SecoClient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**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SecoClent客户端软件安装包或安装包的版本过于老旧，请先**获取软件安装包**。
3. SecoClent客户端目前支持Windows、Mac OS与Linux三种操作系统环境，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：
   - **在Windows操作系统上安装软件**
   - **在Mac OS操作系统上安装软件**
   - **在Linux操作系统上安装软件**

3.1 安装前须知
安装和使用SecoClient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SecoClient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
SecoClient客户端针对32位和64位的Windows操作系统分别提供了软件安装包，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Mac OS操作系统上安装软件
SecoClient客户端仅支持64位的Mac OS操作系统。

3.5 在Linux操作系统上安装软件

3.1 安装前须知

安装和使用SecoClient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。

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SecoClient客户端，则运行安装程序时会弹出提示要求您卸载SecoClient客户端。您可以先根据提示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 SecoClient 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	Mac OS	Linux

系统配置项	配置要求		
操作系统版本	• Windows Vista（32位/64位） • 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（32位/64位）	SecoClient 7.0.2及以前版本： • OS X 10.7.x • OS X 10.8.x • OS X 10.9.x • OS X 10.10.x • OS X 10.11.x • OS X 10.12.x • OS X 10.13.x • OS X 10.14.x SecoClient 7.0.3及以后版本： • OS X 10.12.x • OS X 10.13.x • OS X 10.14.x • OS X 10.15.x	SecoClient 7.0.2及以前版本： • Ubuntu-16.4.04（32位/64位） • Ubuntu-14.4.04（32位/64位） SecoClient 7.0.3及以后版本： • Ubuntu-16.4.04（64位）
硬件资源要求	SecoClient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SecoClient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**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. 您还可以使用具有SecoClient客户端软件安装包下载权限的账号**登录华为技术支持网站下载软件安装包**。
   - 对于企业网用户：您可以使用注册帐号登录网站**http://support.huawei.com/enterprise**，进入“企业网络 > 安全 > 防火墙&VPN网关 >（选择款型）”，选择下载对应版本的软件安装包。
   - 对于运营商用户：您可以使用注册帐号登录网站**http://support.huawei.com/carrier**，进入“产品软件 > 网络 > 交换机与企业网关 > 交换机与企业网关 >（选择款型）”，选择下载对应版本的软件安装包。
3. 如果企业网络管理员在企业的出口网关上部署了SSL VPN虚拟网关，则您可以**通过浏览器登录SSL VPN虚拟网关页面下载软件安装包**。具体的操作步骤如下：
   a. 从企业网络管理员处获取用户登录信息。

      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。

   b. 在终端设备的浏览器中输入企业网络管理员提供的虚拟网关地址，进入SSL VPN虚拟网关登录界面。
   c. 根据SSL VPN的用户认证方式，输入用户名、密码或选择已安装的证书，单击“登录”。
   d. 登录成功后，进入虚拟网关页面，单击虚拟网关页面右上角的“用户选项”，在“下载网络扩展客户端软件”下可以看到SecoClient客户端软件安装包。
   e. 单击“下载网络扩展客户端软件”链接，下载对应操作系统的软件安装包。

后续操作

SecoClent客户端目前支持Windows、Mac OS与Linux三种操作系统环境，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：

- **在Windows操作系统上安装软件**
- **在Mac OS操作系统上安装软件**
- **在Linux操作系统上安装软件**

您还可以回到**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

SecoClient客户端针对32位和64位的Windows操作系统分别提供了软件安装包，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**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

- SecoClient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SecoClient的默认安装路径为“C:\Program Files\SecoClient”。
- 首次安装SecoClient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。

步骤4 安装完成后，系统桌面上会生成一个名称为“SecoClient.exe”的应用程序图标，双击图标即可启动SecoClient客户端。

----结束

后续操作

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

3.4 在 Mac OS 操作系统上安装软件

SecoClient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**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，系统会自动将安装包解压成文件夹，与安装包放置在同一级目录下。

步骤3 双击打开该文件夹，文件夹中包含“Info.plist”和“SecoClientInstaller.pkg”两个文件。双击“SecoClientInstaller.pkg”文件，运行安装程序。

步骤4 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。

说明

- SecoClient客户端默认会被安装在固定路径下，无法手动更改安装位置。
- 安装过程中可能需要对用户的系统权限进行鉴定，鉴定成功后方可继续安装。请输入具有“Root”权限的用户名和密码以允许执行安装操作。

步骤5 安装完成后，可在应用程序文件夹中找到名称为“SecoClient.app”的应用程序，双击即可启动SecoClient客户端。

说明

首次启动客户端时，需要使用系统的“Root”权限对客户端进行提升权限的操作，提权成功后方可运行程序。请输入具有“Root”权限的用户名和密码以允许执行提权操作。

----结束

后续操作

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

3.5 在 Linux 操作系统上安装软件

SecoClient针对32位Linux操作系统和64位Linux操作系统分别提供了安装包，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**安装前须知**中的系统配置要求。

操作步骤

32位操作系统和64位操作系统下SecoClient的安装方法相同，下面以64位操作系统为例进行介绍。

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 > sec”）中。

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

```
root@sec-virtual-machine:~# cd ..
root@sec-virtual-machine:/# cd home/sec
root@sec-virtual-machine:/home/sec# ./secoclient-linux-64.xx.x.xx.run
install.sh
uninstall.sh
sysconfig.ini
qt.conf
bak/
```

```
component/
config/
driver/
```

步骤4 安装成功，如下所示。

```
Starting SecoclientPromoteService daemon: SecoClientPromoteService.
*****The program has been install in directory SecoClient of your home Directory!*****
*****Enjoy!*****
```

步骤5 单击桌面上生成的SecoClient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SecoClient客户端后，您可以开始**配置VPN连接**。
- 若安装过程中发生错误导致安装失败，请参考**安装及更新类故障**进行故障排查和处理。
- 您还可以回到**从这里开始**，参照**任务地图**进行后续配置。

4 配置 VPN 连接

SecoClient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**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：

  - **配置SSL VPN连接**
  - **配置L2TP VPN连接**
  - **配置L2TP over IPSec VPN连接**

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SecoClient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。

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**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

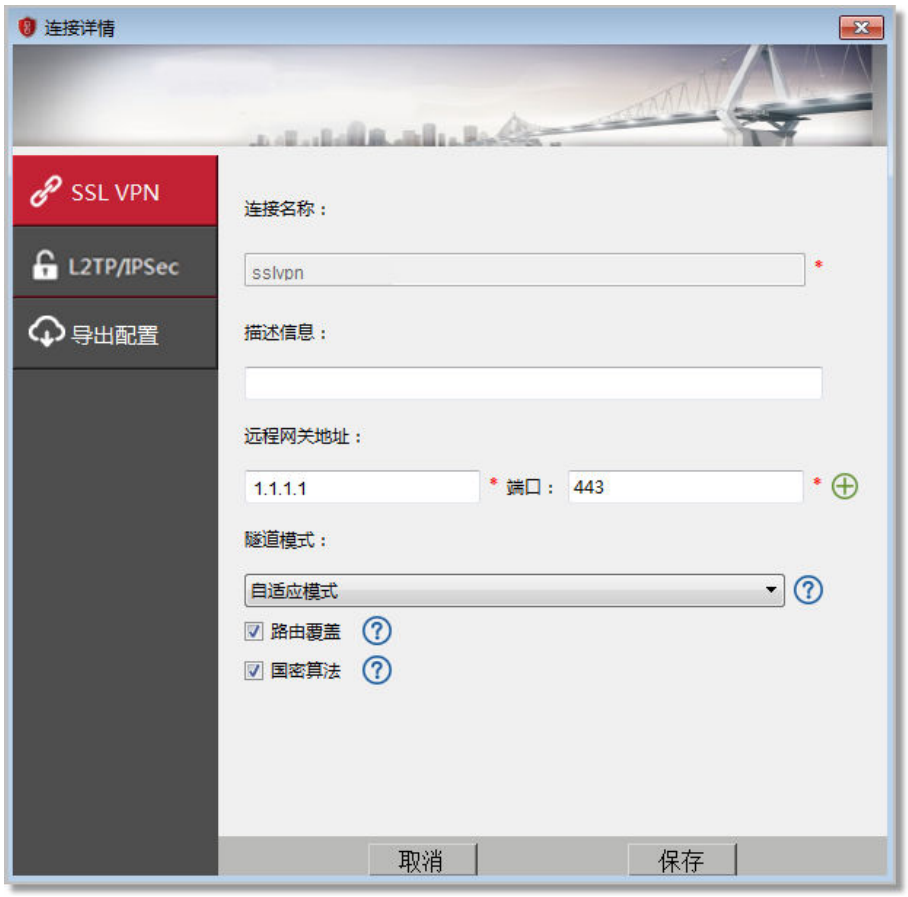
检查项		备注
是否使用代理设置	否	如果您当前访问Internet时没有使用代理服务器，则无需使用代理设置。
	是（使用系统代理）	使用代理服务器的场景细分为3种情况，选择代理类型后，需要输入地址、端口、账号及密码，该信息请从企业网络管理员处获取。
	是（使用HTTP/HTTPS代理）	
	是（使用Socks5代理）	
连接名称		用于标识一条SSL VPN连接，您可以自行设置。
描述信息		用于补充说明该条连接的相关信息（如创建者、创建时间、连接用途等），您可以自行设置。
远程网关地址		SSL VPN虚拟网关地址，该信息请从企业网络管理员处获取。
端口		建立SSL VPN隧道的端口号，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 **说明** 仅在Windows操作系统下会显示此项。		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。
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SecoClient客户端主界面的“连接”下拉列表框中，选择“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SecoClient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**建立VPN连接**。
- 您还可以回到**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**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

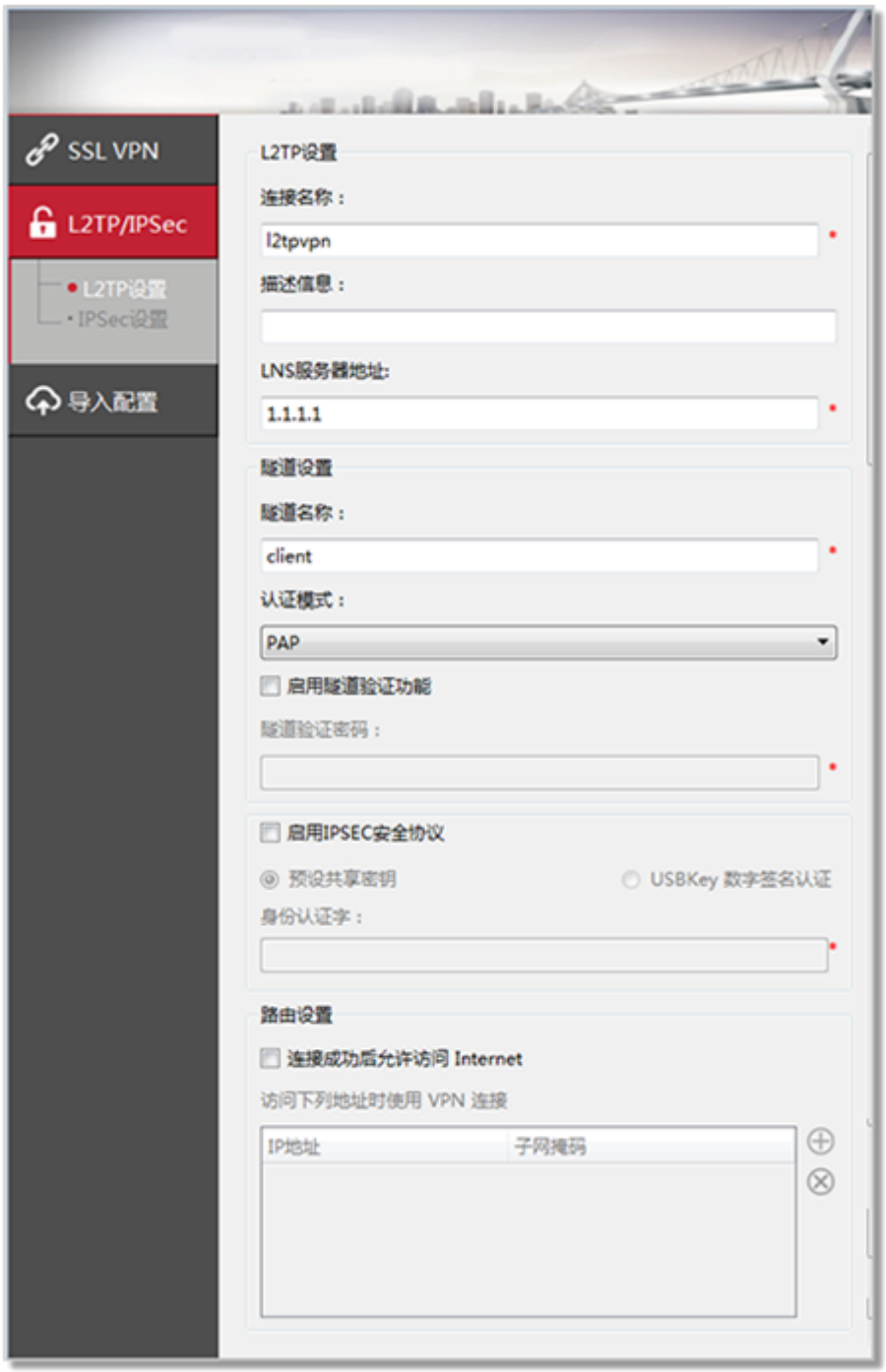
检查项		备注
代理设置		
是否使用代理设置?	否	如果您当前访问Internet时没有使用代理服务器，则无需使用代理设置。
	是（使用Socks5代理） **说明** L2TP VPN隧道仅支持使用Socks5代理。	选择“使用Socks5代理”后，需要输入地址、端口、账号及密码，该信息请从企业网络管理员处获取。
L2TP设置		
连接名称		用于标识一条L2TP VPN连接，您可以自行设置。
描述信息		用于补充说明该条连接的相关信息（如创建者、创建时间、连接用途等），您可以自行设置。
LNS服务器地址		L2TP VPN网关地址，该信息请从企业网络管理员处获取。
隧道设置		
隧道名称		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。 • 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SecoClient客户端主界面的“连接”下拉列表框中，选择“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。



步骤3 设置完成后，单击“确定”，返回SecoClient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**建立VPN连接**。
- 您还可以回到**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**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	

检查项		备注
启用IPSec安全协议		在配置L2TP over IPSec VPN连接时必须勾选此选项。
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，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、SHA1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、Group2和Group5，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、Group2和Group5。 ● 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。

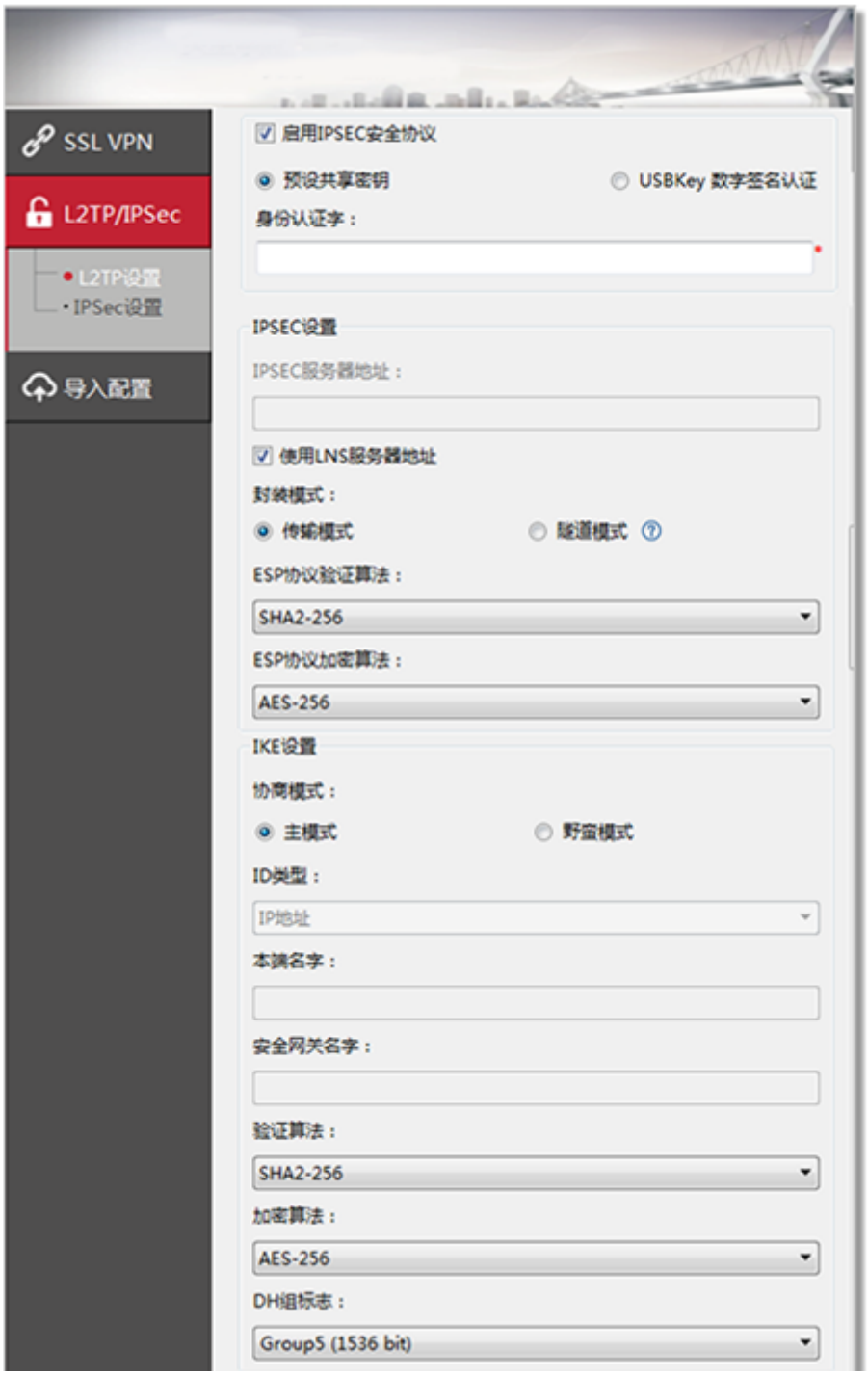
操作步骤

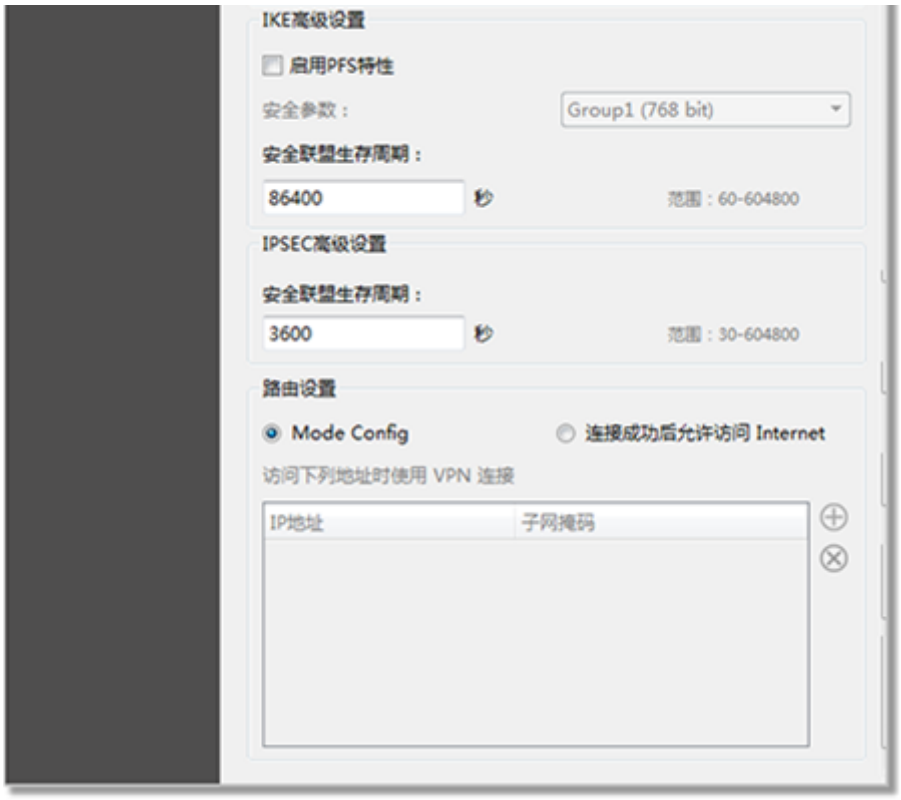
步骤1 在SecoClient客户端主界面的“连接”下拉列表框中，选择“新建连接”。

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

2. 配置IPSec参数





步骤3 设置完成后，单击“确定”，返回SecoClient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**建立VPN连接**。
- 您还可以回到**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SecoClient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。

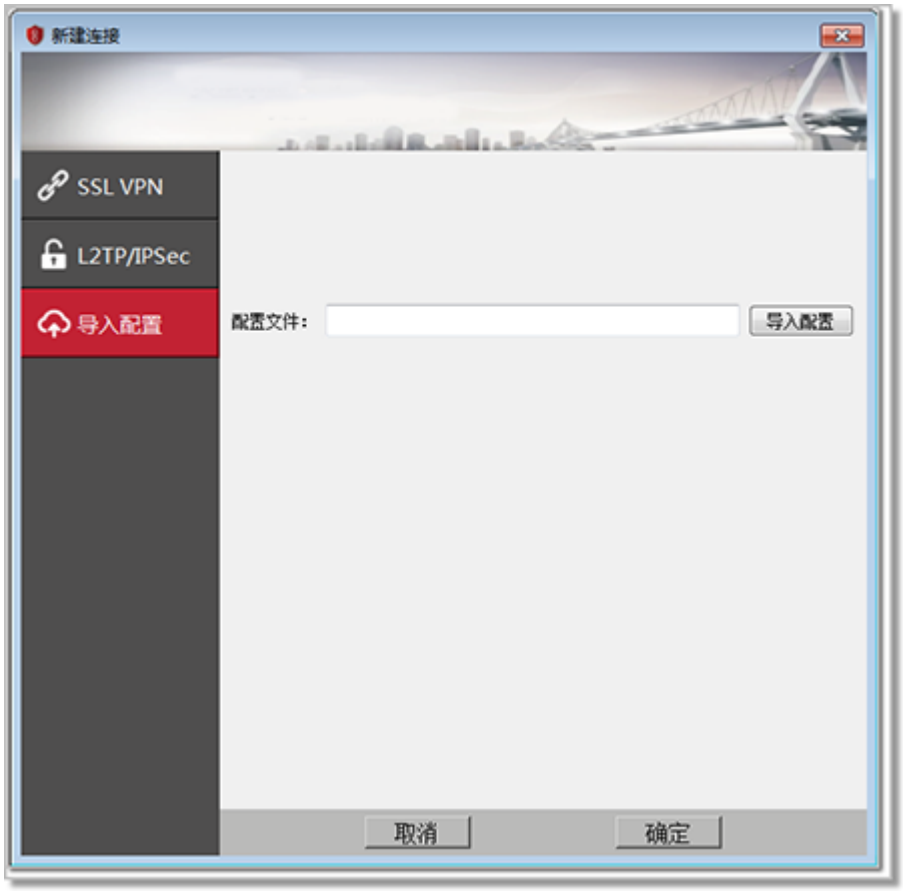
开始之前

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SecoClient客户端主界面的“连接”下拉列表框中，选择“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SecoClient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**建立VPN连接**。
- 您还可以回到**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，SecoClient客户端主界面的“连接”下拉列表框中会显示对应的连接条目。

1. 您可以选择该连接条目后尝试**发起VPN连接**。
2. VPN隧道建立后，对端网关设备需要对您进行**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SecoClient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。

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

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SecoClient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SecoClient客户端主界面的“连接”下拉列表框中，选择配置好的VPN连接条目。

步骤2 单击“连接”，发起VPN连接请求。

----结束

后续操作

- VPN隧道建立后，对端网关设备需要对您进行**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**连接类故障**进行故障排查和处理。
- 您还可以回到**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SecoClient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SecoClient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：

- **通过用户名/密码认证**
- **通过导入PKI数字证书认证**
- **通过USB-Key证书认证**
- **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**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	Mac OS	Linux
SSL VPN	Y	Y	Y
L2TP VPN	Y	Y	Y
L2TP over IPSec VPN	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”或“协商成功”。

----结束

后续操作

- 若您还需要进行双因子认证，请参考**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**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**业务类故障**进行故障排查和处理。
- 您还可以回到**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**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	Mac OS	Linux
SSL VPN（证书匿名认证）	Y	Y	Y
SSL VPN（证书挑战认证）	Y	Y	Y
L2TP VPN	N	N	N
L2TP over IPSec VPN	Y	Y	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MAC证书认证场景下，证书需要导入到“凭证”中；
- 在Linux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“证书”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”或“协商成功”。

----结束

后续操作

- 若您还需要进行双因子认证，请参考**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**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**业务类故障**进行故障排查和处理。
- 您还可以回到**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**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	Mac OS	Linux
SSL VPN（证书匿名认证）	Y	N	N
SSL VPN（证书挑战认证）	Y	N	N
L2TP VPN	N	N	N
L2TP over IPSec VPN	Y	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”或“协商成功”。

----结束

后续操作

- 若您还需要进行双因子认证，请参考**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**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**业务类故障**进行故障排查和处理。
- 您还可以回到**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：

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

说明

- Linux操作系统下目前不支持双因子认证。
- 您也可以通过**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”或“协商成功”。

----结束

后续操作

- 若用户身份认证失败或VPN连接失败，请参考**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**业务类故障**进行故障排查和处理。
- 您还可以回到**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SecoClient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**卸载软件**
- 如何**更新升级**
- 如何**修改登录密码**
- 如何**配置阻塞到不信任服务器的连接**
- 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
SecoClent客户端目前支持Windows和Mac OS两种操作系统环境，两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
SecoClient客户端支持版本检测与更新升级。

6.3 修改登录密码
SecoClient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SecoClient客户端的其他可选配置，包括：

6.1 卸载软件

SecoClent客户端目前支持Windows和Mac OS两种操作系统环境，两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 > SecoClient”。

步骤2 单击“Uninstall”，系统弹出卸载提示，单击“是”。

步骤3 在卸载过程中，系统会提示是否删除用户配置及日志文件，请根据需要进行选择。选择“是”，则删除用户配置及日志文件。

步骤4 单击“确定”，完成卸载。

----结束

在 Mac OS 操作系统下卸载软件

说明

请参考如下步骤，通过卸载程序卸载软件。不要通过将“SecoClient.app”程序直接拖入回收站（Trash）的方式进卸载软件，若系统中存在残留文件未被完全清除，可能导致下次安装时出现异常。

步骤1 在应用程序文件夹中找到卸载程序“SecoClientUninstaller.app”，双击启动。

步骤2 单击“卸载”，并进行用户权限的鉴定，仅具有“Root”权限的用户可卸载此软件。

步骤3 用户权限鉴定成功后，即可完成卸载。

----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“usr/local/SecoClient”目录下。

```
root@sec-virtual-machine:~# cd ..
root@sec-virtual-machine:/# cd usr/local/SecoClient/
root@sec-virtual-machine:/usr/local/SecoClient#
```

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

```
root@sec-virtual-machine:/usr/local/SecoClient# ./uninstall.sh
Stopping SecoClientPromoteService daemon: SecoClientPromoteService.
 Removing any system startup links for /etc/init.d/SecoClientPromoteService.sh ...
```

----结束

6.2 更新升级

SecoClient客户端支持版本检测与更新升级。

开始之前

- 只有当SecoClient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。
- SecoClient客户端升级的基本过程如下：
  a. 企业网络管理员将新的SecoClient客户端软件安装包上传至企业网关。
  b. 用户通过SecoClient客户端与该网关建立VPN隧道时，SecoClient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 右键单击SecoClient客户端的托盘图标，在弹出的菜单中选择“选项”，其中提供了“检测新版本”的选项。勾选此项，客户端会定时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。

----结束

6.3 修改登录密码

SecoClient客户端支持用户在本地修登录密码。

开始之前

只有当SecoClient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 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SecoClient客户端的其他可选配置，包括：

配置阻塞到不信任服务器的连接

SecoClient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。

右键单击SecoClient客户端的托盘图标，在弹出的菜单中选择“选项”，其中提供了“阻塞到不信任服务器的连接”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“安全告警：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

SecoClient客户端支持开机自动启动。

右键单击SecoClient客户端的托盘图标，在弹出的菜单中选择“选项”，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。

配置取消自动登录

右键单击SecoClient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

SecoClient客户端支持12种界面语言。

右键单击SecoClient客户端的托盘图标，在弹出的菜单中选择“选项”，其中提供了“界面语言”的选项，您可以手动切换界面语言。

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“高级 > 网络”页签，单击“连接”下的“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。

7 故障处理

本节收录了SecoClient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。如果您需要了解更多客户端常见故障的定位及处理方法，请登录**华为技术支持网站**获取防火墙产品的维护宝典。

根据终端用户的任务场景，可将故障划分为如下三类：

1. **安装及更新类故障**
2. **连接类故障**
3. **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**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。

7.2 安装及更新类故障

7.3 连接类故障

7.4 业务类故障

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**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**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

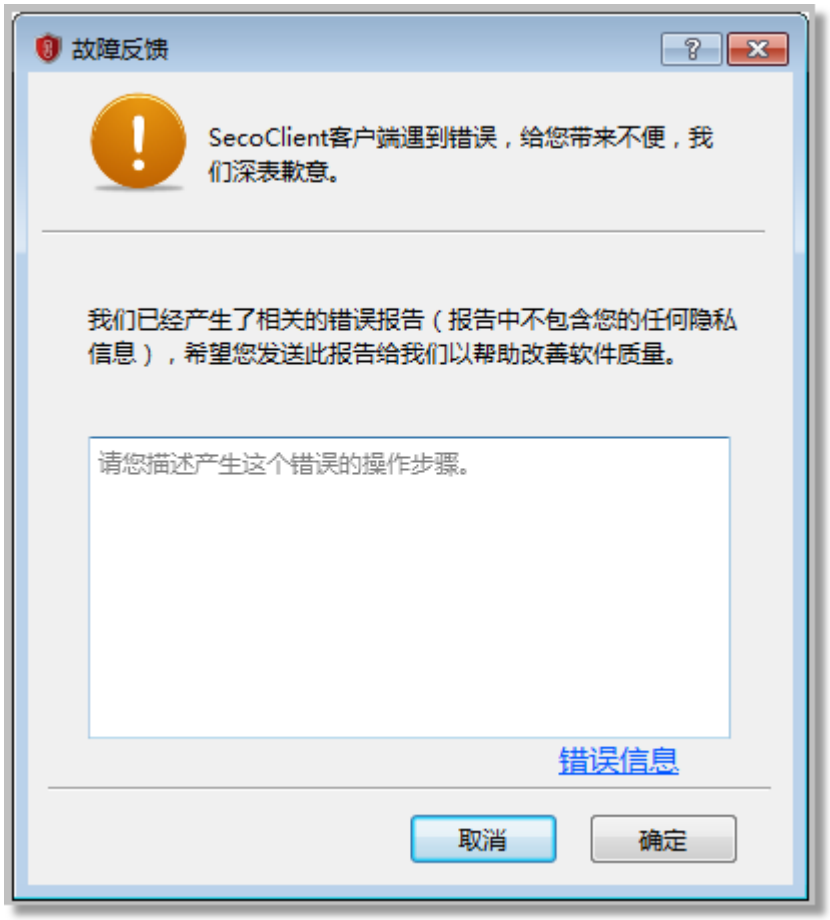
SecoClient生成错误报告时会收集客户端软件的使用信息及部分系统信息（参见下文），请确保以下信息受到严格保护。

- **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。
- **SecoClient_SecoClientCS_0.log**：记录SecoClient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。
- **SecoClient_SecoClientUI_0.log**：记录SecoClient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。
- **SecoClient_SecoClientPromoteService_0.log**：记录SecoClient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SecoClient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SecoClient的托盘图标。

步骤2 单击“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**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

步骤1 在SecoClient客户端主界面的“连接”下拉列表框中选中已配置的VPN连接，单击右侧的编辑  。

步骤2 在“连接详情”窗口中，单击导航栏左侧的“导出配置”，并选择配置文件的保存位置。配置文件默保存为“.ini”格式。

步骤3 单击“保存”，将配置文件保存到选择的路径下。

----结束

后续操作

配置文件导出后，您可以将其与**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**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**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。

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SecoClient客户端外，华为公司还推出了基于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 VPN配置及连接模板

8.1 移动客户端

除了PC版的SecoClient客户端外，华为公司还推出了基于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“**SecoClient**”字段，即可下载最新版本的SecoClient iOS版本客户端。

  方式二：在华为技术支持网站下载对应版本的软件安装包。

  - 对于企业网用户：使用注册帐号登录网站**http://support.huawei.com/enterprise**，进入“企业网络 > 安全 > 防火墙&VPN网关 > Secospace USG6600 > 软件”，选择下载对应版本的软件安装包。
  - 对于运营商用户：使用注册帐号登录网站**http://support.huawei.com/carrier**，进入“产品软件 > 网络 > 交换机与企业网关 > 交换机与企业网关 > Eudemon1000E-N 系列 > Eudemon1000E-N”，选择下载对应版本的软件安装包。

- **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**”APP，搜索“**SecoClient**”字段，即可下载最新版本的SecoClient Android版本客户端。

  方式二：在华为技术支持网站下载对应版本的软件安装包。

- 对于企业网用户：使用注册帐号登录网站**http://support.huawei.com/enterprise**，进入“企业网络 > 安全 > 防火墙&VPN网关 > Secospace USG6600 > 软件”，选择下载对应版本的软件安装包。
- 对于运营商用户：使用注册帐号登录网站**http://support.huawei.com/carrier**，进入“产品软件 > 网络 > 交换机与企业网关 > 交换机与企业网关 > Eudemon1000E-N 系列 > Eudemon1000E-N”，选择下载对应版本的软件安装包。

规格

移动版SecoClient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 SecoClient 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SecoClient客户端的功能规格如下：

表 8-2 移动版 SecoClient 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SecoClient客户端可以拨号成功。	不支持	不支持
	网关优选	不支持	不支持
	断线重连	不支持	不支持
	链路备份 **说明** 网关侧开启链路备份功能时，移动版SecoClient客户端可以拨号成功。	支持	支持
	证书认证	不支持	不支持
	MAC认证	不支持	不支持
	证书筛选	不支持	不支持
	双因子认证	不支持	不支持
L2TP VPN		不支持	不支持
L2TP over IPSec VPN		不支持	不支持
NAT穿越		支持	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
	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SecoClient客户端的性能规格如下：

表 8-3 移动版 SecoClient 客户端的性能规格

功能名称	规格
VPN新建连接数	16个

操作

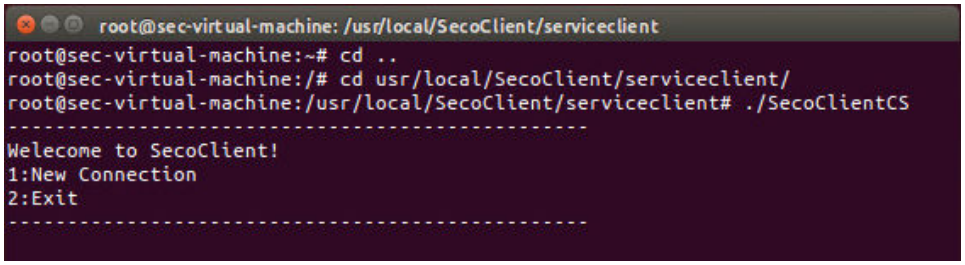
移动版SecoClient客户端的具体操作，请参见APP内“设置 > 帮助”节点下的联机帮助。

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/SecoClient/serviceclient目录。

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



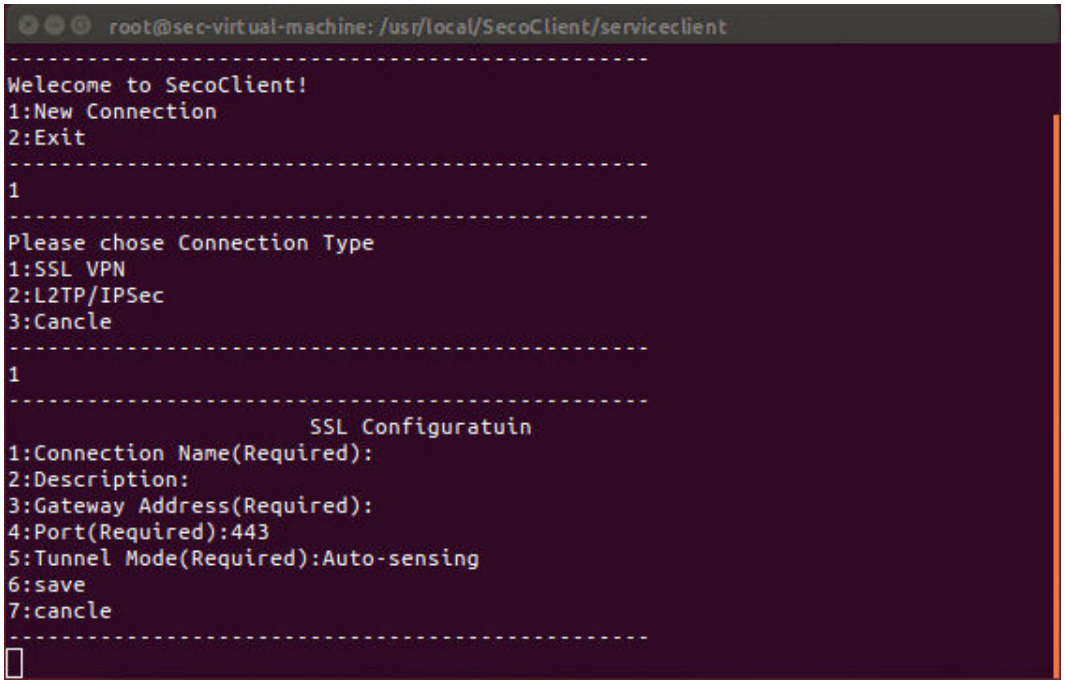
说明

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。

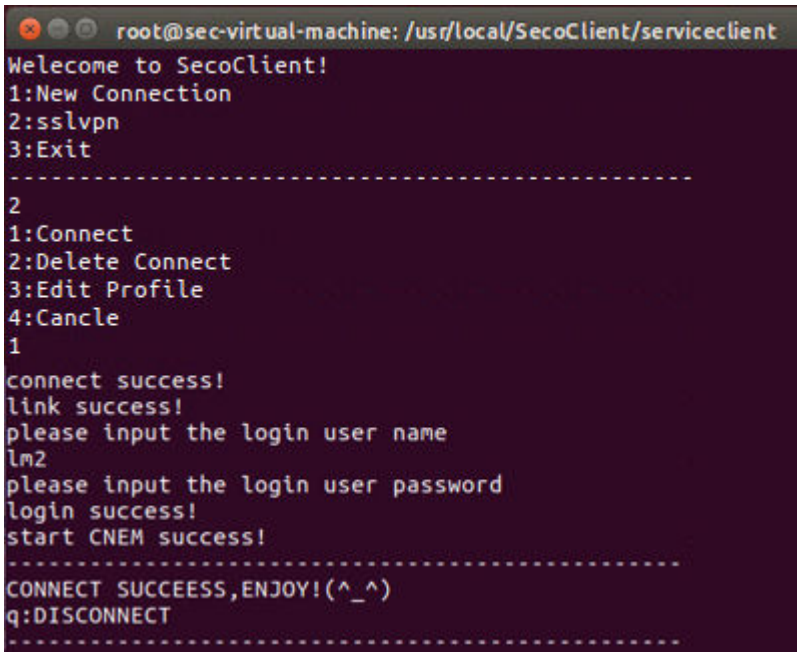
步骤3 输入对应序号，完成参数**1~5**的配置。

- 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**6**，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

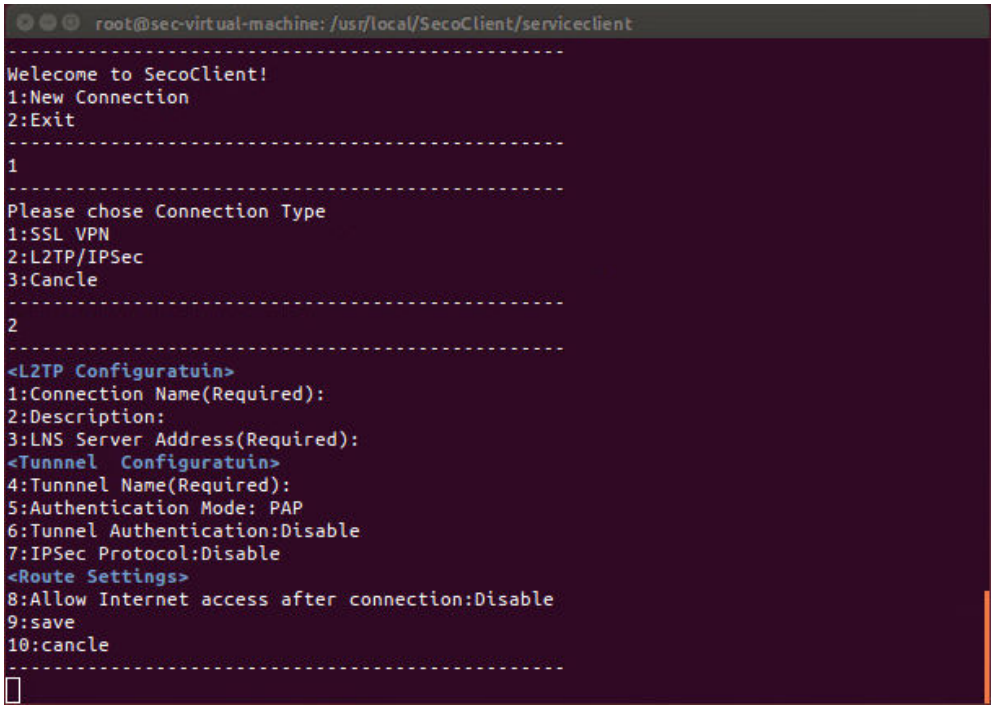
- 在Linux操作系统下通过命令行方式配置并建立的SSL VPN连接仅支持通过用户名/密码认证方式认证登录。
- 连接成功后，不能关闭该终端窗口，否则连接会断开。

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。

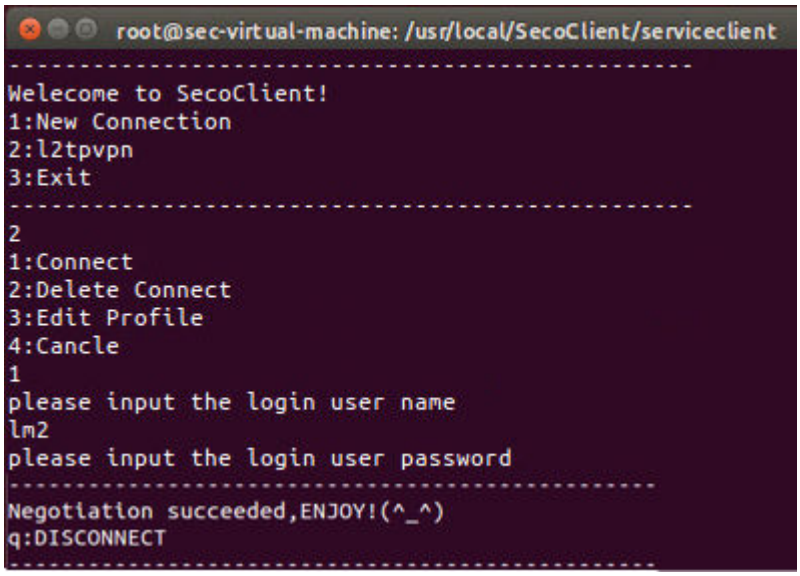
步骤3 输入对应序号，完成参数**1~8**的配置。

- 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

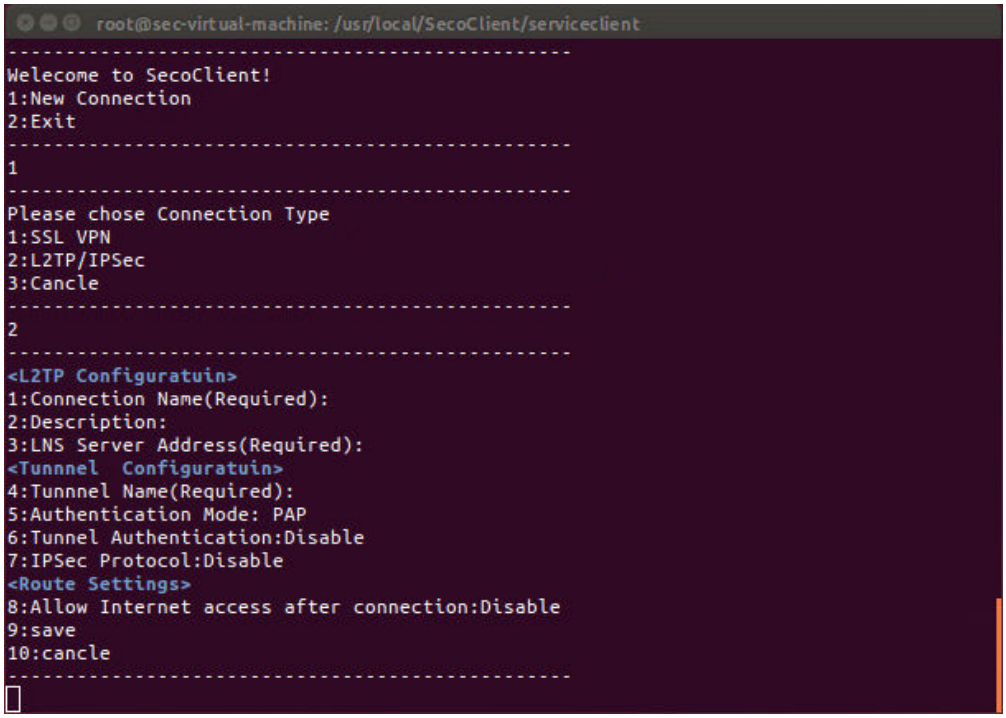
连接成功后，不能关闭该终端窗口，否则连接会断开。

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。

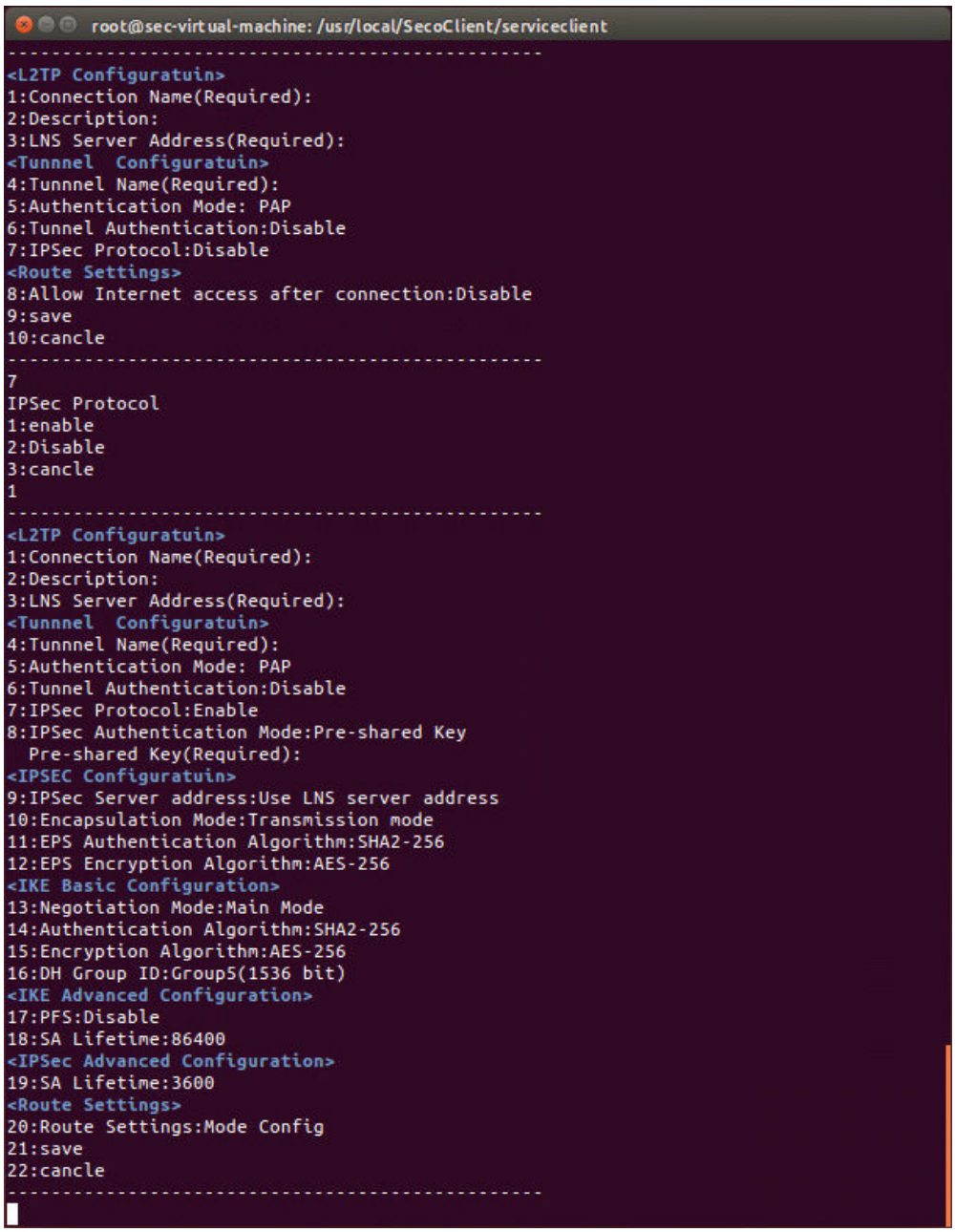
步骤2 输入**2**，选择创建的VPN类型为L2TP/IPSec。

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



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。

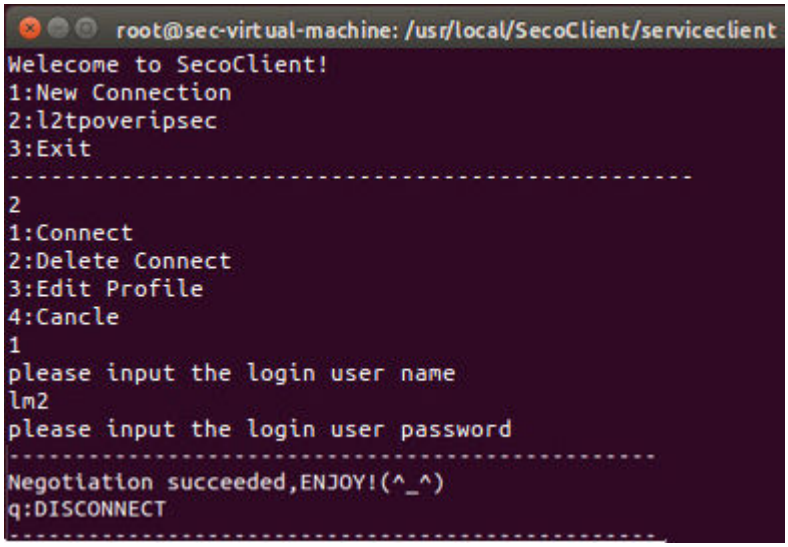
- 8. IPSec Authentication Mode：Linux操作系统下IPSec的身份认证方式目前仅支持预共享密钥认证，预共享密钥方式下需要输入身份认证字（Pre-shared key）；
- 9. IPSec Server address：IPSec服务器地址，缺省设置为使用LNS服务器地址（Use LNS server address）；
- 10. Encapsulation Mode：IPSec封装模式，包括传输模式（Transmission mode）和隧道模式（Tunnel mode）两种；
- 11. ESP Authentication Algorithm：ESP协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

- 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 VPN 配置及连接模板

8.3.1 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 colspan="2">用户身份认证方式</td><td colspan="4">所需的验证信息</td></tr>
<tr><td rowspan="2">1</td><td colspan="2" rowspan="2">通过用户名/密码认证</td><td colspan="4">用户名</td></tr>
<tr><td colspan="4">密码</td></tr>
</table>

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	
		使用证书挑战认证	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	
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

8.3.2 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			
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	
路由设置				
8	不勾选“连接成功后允许访问Internet”			-
	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 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		

8.3.3 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

