# VPN 配置

# 数引 VPN 配置和使用指南

数引 VPN 服务器支持 IPsec/L2TP(默认), Cisco IPsec 和 IKEv2 等多种协议，其中 IPsec 采用 Libreswan 作为服务器， L2TP则由 xl2tpd 提供。

VPN的架设可以使员工在外部互联网环境下轻松访问公司内网。

## VPN 服务

| 配置项 | 值 |
| --- | --- |
| 服务器地址 | vpn.suin.ltd |
| 预共享密钥 | suin.ltd |
| 用户名 | public |
| 密码 | szyl1332 |

## 默认配置方法

- Windows
- macOS
- Android
- iOS
- Linux

### Windows

> 以下为默认配置方法，你也可以使用 IPsec/XAuth 或者 IKEv2 模式连接。

#### Windows 11

1. 右键单击系统托盘中的无线/网络图标。
2. 选择 **网络和 Internet 设置**，然后在打开的页面中单击 **VPN**。
3. 单击 **添加 VPN** 按钮。

4. 从 **VPN 提供商** 下拉菜单选择 **Windows (内置)**。
5. 在 **连接名称** 字段中输入任意内容。
6. 在 **服务器名称或地址** 字段中输入 `VPN 服务器地址` 。
7. 从 **VPN 类型** 下拉菜单选择 **使用预共享密钥的 L2TP/IPsec**。
8. 在 **预共享密钥** 字段中输入 `VPN 预共享密钥` 。
9. 在 **用户名** 字段中输入 `VPN 用户名` 。
10. 在 **密码** 字段中输入 `VPN 密码` 。
11. 选中 **记住我的登录信息** 复选框。
12. 单击 **保存** 保存 VPN 连接的详细信息。

**注：** 在首次连接之前需要右键下载 **注册表补丁** (/uploads/blog/202204/attach_16e531f0f086af65.zip) 并运行，以解决 VPN 服务器 和/或 客户端与 NAT （比如家用路由器）的兼容问题。

要连接到 VPN：单击 **连接** 按钮，或者单击系统托盘中的无线/网络图标，单击 **VPN**，然后选择新的 VPN 连接并单击 **连接**。如果出现提示，在登录窗口中输入 `VPN 用户名` 和 `VPN 密码` ，并单击 **确定**。

## Windows 10 and 8

1. 右键单击系统托盘中的无线/网络图标。
2. 选择 **打开"网络和 Internet"设置**，然后在打开的页面中单击 **网络和共享中心**。
3. 单击 **设置新的连接或网络**。
4. 选择 **连接到工作区**，然后单击 **下一步**。
5. 单击 **使用我的Internet连接 (VPN)**。
6. 在 **Internet地址** 字段中输入 `VPN 服务器地址` 。
7. 在 **目标名称** 字段中输入任意内容。单击 **创建**。
8. 返回 **网络和共享中心**。单击左侧的 **更改适配器设置**。
9. 右键单击新创建的 VPN 连接，并选择 **属性**。
10. 单击 **安全** 选项卡，从 **VPN 类型** 下拉菜单中选择 "使用 IPsec 的第 2 层隧道协议 (L2TP/IPSec)"。
11. 单击 **允许使用这些协议**。选中 "质询握手身份验证协议 (CHAP)" 和 "Microsoft CHAP 版本 2 (MS-CHAP v2)" 复选框。
12. 单击 **高级设置** 按钮。
13. 单击 **使用预共享密钥作身份验证** 并在 **密钥** 字段中输入 `VPN 预共享密钥` 。
14. 单击 **确定** 关闭 **高级设置**。
15. 单击 **确定** 保存 VPN 连接的详细信息。

**注：** 在首次连接之前需要右键下载 **注册表补丁** (/uploads/blog/202204/attach_16e531f0f086af65.zip) 并运行，以解决 VPN 服务器 和/或 客户端与 NAT （比如家用路由器）的兼容问题。

要连接到 VPN：单击系统托盘中的无线/网络图标，选择新的 VPN 连接，然后单击 **连接**。如果出现提示，在登录窗口中输入 `VPN 用户名` 和 `VPN 密码` ，并单击 **确定**。

另外，除了按照以上步骤操作，你也可以运行下面的 Windows PowerShell 命令来创建 VPN 连接。将 `VPN 服务器地址` 和 `VPN 预共享密钥` 换成你自己的值，用单引号括起来：

```
# 不保存命令行历史记录
Set-PSReadlineOption –HistorySaveStyle SaveNothing
# 创建 VPN 连接
Add-VpnConnection -Name 'My IPsec VPN' -ServerAddress 'VPN 服务器地址' -L2tpPsk 'VPN
 预共享密钥' -TunnelType L2tp -EncryptionLevel Required -AuthenticationMethod Chap,MSC
hapv2 -Force -RememberCredential -PassThru
# 忽略 data encryption 警告（数据在 IPsec 隧道中已被加密）
```

### Windows 7, Vista and XP

1. 单击开始菜单，选择控制面板。
2. 进入 **网络和Internet** 部分。
3. 单击 **网络和共享中心**。
4. 单击 **设置新的连接或网络**。
5. 选择 **连接到工作区**，然后单击 **下一步**。
6. 单击 **使用我的Internet连接 (VPN)**。
7. 在 **Internet地址** 字段中输入 `VPN 服务器地址` 。
8. 在 **目标名称** 字段中输入任意内容。
9. 选中 **现在不连接；仅进行设置以便稍后连接** 复选框。
10. 单击 **下一步**。
11. 在 **用户名** 字段中输入 `VPN 用户名` 。
12. 在 **密码** 字段中输入 `VPN 密码` 。
13. 选中 **记住此密码** 复选框。
14. 单击 **创建**，然后单击 **关闭** 按钮。
15. 返回 **网络和共享中心**。单击左侧的 **更改适配器设置**。
16. 右键单击新创建的 VPN 连接，并选择 **属性**。
17. 单击 **选项** 选项卡，取消选中 **包括Windows登录域** 复选框。
18. 单击 **安全** 选项卡，从 **VPN 类型** 下拉菜单中选择 “使用 IPsec 的第 2 层隧道协议 (L2TP/IPSec)”。
19. 单击 **允许使用这些协议**。选中 “质询握手身份验证协议 (CHAP)” 和 “Microsoft CHAP 版本 2 (MS-CHAP v2)” 复选框。
20. 单击 **高级设置** 按钮。
21. 单击 **使用预共享密钥作身份验证** 并在 **密钥** 字段中输入 `VPN 预共享密钥` 。
22. 单击 **确定** 关闭 **高级设置**。
23. 单击 **确定** 保存 VPN 连接的详细信息。

**注：** 在首次连接之前需要右键下载 **注册表补丁** (/uploads/blog/202204/attach_16e531f0f086af65.zip) 并运行，以解决 VPN 服务器 和/或 客户端与 NAT （比如家用路由器）的兼容问题。

要连接到 VPN：单击系统托盘中的无线/网络图标，选择新的 VPN 连接，然后单击 **连接**。如果出现提示，在登录窗口中输入 `VPN 用户名` 和 `VPN 密码` ，并单击 **确定**。

## macOS

> 以下为默认配置方法，你也可以使用 IPsec/XAuth 或者 IKEv2 模式连接。

1. 打开系统偏好设置并转到网络部分。
2. 在窗口左下角单击 **+** 按钮。
3. 从 **接口** 下拉菜单选择 **VPN**。
4. 从 **VPN类型** 下拉菜单选择 **IPSec 上的 L2TP**。
5. 在 **服务名称** 字段中输入任意内容。
6. 单击 **创建**。
7. 在 **服务器地址** 字段中输入 `VPN 服务器地址` 。
8. 在 **帐户名称** 字段中输入 `VPN 用户名` 。
9. 单击 **认证设置** 按钮。
10. 在 **用户认证** 部分，选择 **密码** 单选按钮，然后输入 `VPN 密码` 。
11. 在 **机器认证** 部分，选择 **共享的密钥** 单选按钮，然后输入 `VPN 预共享密钥` 。
12. 保持 **群组名称** 字段空白。
13. 单击 **好**。
14. 选中 **在菜单栏中显示 VPN 状态** 复选框。
15. **（重要）** 单击 **高级** 按钮，并选中 **通过VPN连接发送所有通信** 复选框。
16. **（重要）** 单击 **TCP/IP** 选项卡，并在 **配置IPv6** 部分中选择 **仅本地链接**。
17. 单击 **好** 关闭高级设置，然后单击 **应用** 保存VPN连接信息。

要连接到 VPN：使用菜单栏中的图标，或者打开系统偏好设置的网络部分，选择 VPN 并单击 **连接**。

## Android

> 以下为默认配置方法，你也可以使用 IPsec/XAuth 或者 IKEv2 模式连接。Android 12 仅支持 IKEv2 模式。

1. 启动 **设置** 应用程序。
2. 单击 **网络和互联网**。或者，如果你使用 Android 7 或更早版本，在 **无线和网络** 部分单击 **更多...**。
3. 单击 **VPN**。
4. 单击 **添加VPN配置文件** 或窗口右上角的 **+**。
5. 在 **名称** 字段中输入任意内容。
6. 在 **类型** 下拉菜单选择 **L2TP/IPSec PSK**。
7. 在 **服务器地址** 字段中输入 `VPN 服务器地址` 。
8. 保持 **L2TP 密钥** 字段空白。
9. 保持 **IPSec 标识符** 字段空白。
10. 在 **IPSec 预共享密钥** 字段中输入 `VPN 预共享密钥` 。
11. 单击 **保存**。
12. 单击新的VPN连接。
13. 在 **用户名** 字段中输入 `VPN 用户名` 。
14. 在 **密码** 字段中输入 `VPN 密码` 。
15. 选中 **保存帐户信息** 复选框。
16. 单击 **连接**。

VPN 连接成功后，会在通知栏显示图标。

# iOS

> 以下为默认配置方法，你也可以使用 IPsec/XAuth 或者 IKEv2 模式连接。

1. 进入设置 -> 通用 -> VPN。
2. 单击 **添加VPN配置...**。
3. 单击 **类型** 。选择 **L2TP** 并返回。
4. 在 **描述** 字段中输入任意内容。
5. 在 **服务器** 字段中输入 `VPN 服务器地址` 。
6. 在 **帐户** 字段中输入 `VPN 用户名` 。
7. 在 **密码** 字段中输入 `VPN 密码` 。
8. 在 **密钥** 字段中输入 `VPN 预共享密钥` 。
9. 启用 **发送所有流量** 选项。
10. 单击右上角的 **完成**。
11. 启用 **VPN** 连接。

VPN 连接成功后，会在通知栏显示图标。

# Linux

> 以下为默认配置方法，你也可以使用 IKEv2 模式连接。

## Ubuntu Linux

Ubuntu 18.04 和更新版本用户可以使用 `apt` 安装 network-manager-l2tp-gnome (https://packages.ubuntu.com/search?keywords=network-manager-l2tp-gnome) 软件包，然后通过 GUI 配置 IPsec/L2TP VPN 客户端。

1. 进入 Settings -> Network -> VPN。单击 **+** 按钮。
2. 选择 **Layer 2 Tunneling Protocol (L2TP)**。
3. 在 **Name** 字段中输入任意内容。
4. 在 **Gateway** 字段中输入 `VPN 服务器地址` 。
5. 在 **User name** 字段中输入 `VPN 用户名` 。
6. 右键单击 **Password** 字段中的 **?**，选择 **Store the password only for this user**。
7. 在 **Password** 字段中输入 `VPN 密码` 。
8. 保持 **NT Domain** 字段空白。
9. 单击 **IPsec Settings...** 按钮。
10. 选中 **Enable IPsec tunnel to L2TP host** 复选框。
11. 保持 **Gateway ID** 字段空白。
12. 在 **Pre-shared key** 字段中输入 `VPN 预共享密钥` 。
13. 展开 **Advanced** 部分。
14. 在 **Phase1 Algorithms** 字段中输入 `aes128-sha1-modp2048` 。
15. 在 **Phase2 Algorithms** 字段中输入 `aes128-sha1` 。
16. 单击 **OK**，然后单击 **Add** 保存 VPN 连接信息。
17. 启用 **VPN** 连接。

### CentOS 和 Fedora

CentOS 8/7 和 Fedora 28（和更新版本）用户请使用 IPsec/XAuth 模式连接。

# IPsec / XAuth 客户端配置

- Windows
- macOS
- Android
- iOS
- Linux

## Windows

> 你也可以使用 IKEv2 或者 IPsec/L2TP 默认模式 连接。无需安装额外的软件。

1. 下载并安装免费的 Shrew Soft VPN 客户端 (https://www.shrew.net/download/vpn)。在安装时请选择 **Standard Edition**。
   **注：** 该 VPN 客户端 **不支持** Windows 10/11。
2. 单击开始菜单 -> 所有程序 -> ShrewSoft VPN Client -> VPN Access Manager
3. 单击工具栏中的 **Add (+)** 按钮。
4. 在 **Host Name or IP Address** 字段中输入 `VPN 服务器地址`。
5. 单击 **Authentication** 选项卡，从 **Authentication Method** 下拉菜单中选择 **Mutual PSK + XAuth**。
6. 在 **Local Identity** 子选项卡中，从 **Identification Type** 下拉菜单中选择 **IP Address**。
7. 单击 **Credentials** 子选项卡，并在 **Pre Shared Key** 字段中输入 `VPN 预共享密钥`。
8. 单击 **Phase 1** 选项卡，从 **Exchange Type** 下拉菜单中选择 **main**。
9. 单击 **Phase 2** 选项卡，从 **HMAC Algorithm** 下拉菜单中选择 **sha1**。
10. 单击 **Save** 保存 VPN 连接的详细信息。
11. 选择新添加的 VPN 连接。单击工具栏中的 **Connect** 按钮。
12. 在 **Username** 字段中输入 `VPN 用户名`。
13. 在 **Password** 字段中输入 `VPN 密码`。
14. 单击 **Connect**。

VPN 连接成功后，你会在 VPN Connect 状态窗口中看到 **tunnel enabled** 字样。单击 “Network” 选项卡，并确认 **Established - 1** 显示在 “Security Associations” 下面。

## macOS

> 你也可以使用 IKEv2 或者 IPsec/L2TP 默认模式 连接。

1. 打开系统偏好设置并转到网络部分。
2. 在窗口左下角单击 **+** 按钮。
3. 从 **接口** 下拉菜单选择 **VPN**。
4. 从 **VPN类型** 下拉菜单选择 **Cisco IPSec**。
5. 在 **服务名称** 字段中输入任意内容。
6. 单击 **创建**。
7. 在 **服务器地址** 字段中输入 `VPN 服务器地址` 。
8. 在 **帐户名称** 字段中输入 `VPN 用户名` 。
9. 在 **密码** 字段中输入 `VPN 密码` 。
10. 单击 **认证设置** 按钮。
11. 在 **机器认证** 部分，选择 **共享的密钥** 单选按钮，然后输入 `VPN 预共享密钥` 。
12. 保持 **群组名称** 字段空白。
13. 单击 **好**。
14. 选中 **在菜单栏中显示 VPN 状态** 复选框。
15. 单击 **应用** 保存VPN连接信息。

要连接到 VPN：使用菜单栏中的图标，或者打开系统偏好设置的网络部分，选择 VPN 并单击 **连接**。

## Android

> 你也可以使用 IKEv2 或者 IPsec/L2TP 默认模式 连接。Android 12 仅支持 IKEv2 模式。

1. 启动 **设置** 应用程序。
2. 单击 **网络和互联网**。或者，如果你使用 Android 7 或更早版本，在 **无线和网络** 部分单击 **更多...**。
3. 单击 **VPN**。
4. 单击 **添加VPN配置文件** 或窗口右上角的 **+**。
5. 在 **名称** 字段中输入任意内容。
6. 在 **类型** 下拉菜单选择 **IPSec Xauth PSK**。
7. 在 **服务器地址** 字段中输入 `VPN 服务器地址` 。
8. 保持 **IPSec 标识符** 字段空白。
9. 在 **IPSec 预共享密钥** 字段中输入 `VPN 预共享密钥` 。
10. 单击 **保存**。
11. 单击新的VPN连接。
12. 在 **用户名** 字段中输入 `VPN 用户名` 。
13. 在 **密码** 字段中输入 `VPN 密码` 。
14. 选中 **保存帐户信息** 复选框。
15. 单击 **连接**。

VPN 连接成功后，会在通知栏显示图标。

# iOS

> 你也可以使用 IKEv2 或者 IPsec/L2TP 默认模式 连接。

1. 进入设置 -> 通用 -> VPN。
2. 单击 **添加VPN配置...**。
3. 单击 **类型** 。选择 **IPSec** 并返回。
4. 在 **描述** 字段中输入任意内容。
5. 在 **服务器** 字段中输入 `VPN 服务器地址` 。
6. 在 **帐户** 字段中输入 `VPN 用户名` 。
7. 在 **密码** 字段中输入 `VPN 密码` 。
8. 保持 **群组名称** 字段空白。
9. 在 **密钥** 字段中输入 `VPN 预共享密钥` 。
10. 单击右上角的 **完成**。
11. 启用 **VPN** 连接。

VPN 连接成功后，会在通知栏显示图标。

# Linux

> 你也可以使用 IKEv2 模式连接，其它 Linux 版本用户请使用 IPsec/L2TP 默认模式连接。

## CentOS 和 Fedora

CentOS 8/7 和 Fedora 28 （和更新版本）用户可以使用 `yum` 安装 `NetworkManager-libreswan-gnome` 软件包，然后通过 GUI 配置 IPsec/XAuth VPN 客户端。

1. 进入 Settings -> Network -> VPN。单击 **+** 按钮。
2. 选择 **IPsec based VPN**。
3. 在 **Name** 字段中输入任意内容。
4. 在 **Gateway** 字段中输入 `VPN 服务器地址` 。
5. 在 **Type** 下拉菜单选择 **IKEv1 (XAUTH)**。
6. 在 **User name** 字段中输入 `VPN 用户名` 。
7. 右键单击 **User password** 字段中的 **?**，选择 **Store the password only for this user**。
8. 在 **User password** 字段中输入 `VPN 密码` 。
9. 保持 **Group name** 字段空白。
10. 右键单击 **Secret** 字段中的 **?**，选择 **Store the password only for this user**。
11. 在 **Secret** 字段中输入 `VPN 预共享密钥` 。
12. 保持 **Remote ID** 字段空白。
13. 单击 **Add** 保存 VPN 连接信息。
14. 启用 **VPN** 连接。

# IKEv2 客户端配置



## Windows

> Windows 8 以上用户可以自动导入 IKEv2 配置，Windows 7 及以前用户请使用 IPsec / XAuth 或者 IPsec/L2TP 默认模式 连接

1. 将数引vpn生成的 **suin.p12** (/uploads/blog/202203/suin.p12) 文件安全地传送到你的计算机。
2. 右键单击 **ikev2_config_import.cmd** (/uploads/blog/202203/ikev2_config_import.cmd) 并保存这个辅助脚本到与 `suin.p12` 文件 **相同的文件夹**。
3. 右键单击保存的脚本，选择 **属性**。单击对话框下方的 **解除锁定**，然后单击 **确定**。
4. 右键单击保存的脚本，选择 **以管理员身份运行** 并按提示操作。

## macOS

> 你也可以使用 IPsec / XAuth 或者 IPsec/L2TP 默认模式连接。

首先，将生成的 **suin.mobileconfig** (/uploads/blog/202203/suin.mobileconfig) 文件安全地传送到你的 Mac，然后双击并按提示操作，以导入为 macOS 配置描述文件。如果你的 Mac 运行 macOS Big Sur 或更新版本，打开系统偏好设置并转到描述文件部分以完成导入。在完成之后，检查并确保 “IKEv2 VPN” 显示在系统偏好设置 -> 描述文件中。

要连接到 VPN：

1. 打开系统偏好设置并转到网络部分。
2. 选择与 `VPN 服务器地址` 对应的 VPN 连接。
3. 选中 **在菜单栏中显示 VPN 状态** 复选框。
4. 单击 **连接**。

（可选功能）你可以选择启用 VPN On Demand（按需连接） (https://developer.apple.com/documentation/networkextension/personal_vpn/vpn_on_demand_rules) ，该功能在使用 Wi-Fi 网络时自动建立 VPN 连接。要启用它，选中 VPN 连接的 **按需连接** 复选框，然后单击 **应用**。

## iOS

> 你也可以使用 IPsec / XAuth 或者 IPsec/L2TP 默认模式连接。

首先，将生成的 **suin.mobileconfig** (/uploads/blog/202203/suin.mobileconfig) 文件安全地传送到你的 iOS 设备，并且导入为 iOS 配置描述文件。要传送文件，你可以使用：

1. AirDrop（隔空投送）；
2. 使用 文件共享 (https://support.apple.com/zh-cn/HT210598) 功能上传到设备（任何 App 目录），然后打开 iOS 设备上的 “文件” App，将上传的文件移动到 “On My iPhone” 目录下。然后单击它并到 “设置” App 中导入；
3. 将文件放在一个你的安全的托管网站上，然后在 Mobile Safari 中下载并导入它们。

在完成之后，检查并确保 “IKEv2 VPN” 显示在设置 -> 通用 -> VPN 与设备管理（或者描述文件）中。

要连接到 VPN：

1. 进入设置 -> VPN。选择与 `VPN 服务器地址` 对应的 VPN 连接。
2. 启用 **VPN** 连接。

（可选功能）你可以选择启用 VPN On Demand（按需连接） (https://developer.apple.com/documentation/networkextension/personal_vpn/vpn_on_demand_rules)，该功能在使用 Wi-Fi 网络时自动建立 VPN 连接。要启用它，单击 VPN 连接右边的 “i” 图标，然后启用 **按需连接**。

## Android

> Android12 之前的版本，也可以使用 IPsec / XAuth 或者 IPsec/L2TP 默认模式连接。

1. 将生成的 **suin.sswan** (/uploads/blog/202203/suin.sswan) 文件安全地传送到你的 Android 设备。
2. 下载并安装 **strongSwan** (/uploads/blog/202203/strongSwan.apk) VPN 客户端。
3. 启动 strongSwan VPN 客户端。
4. 单击右上角的 “更多选项” 菜单，然后单击 **导入VPN配置**。
5. 选择你从服务器传送过来的 `suin.sswan` 文件。
   **注：** 要查找 `suin.sswan` 文件，单击左上角的抽拉式菜单，然后浏览到你保存文件的目录。
6. 在 “导入VPN配置” 屏幕上，单击 **从VPN配置导入证书**，并按提示操作。
7. 在 “选择证书” 屏幕上，选择新的客户端证书并单击 **选择**。
8. 单击 **导入**。
9. 单击新的 VPN 配置文件以开始连接。

▶ 如果你的设备运行 Android 6.0 或更早版本，点这里查看额外的步骤。

（可选功能）你可以选择启用 Android 上的 “始终开启的 VPN” 功能。启动 **设置** App，进入 网络和互联网 -> 高级 -> VPN，单击 “strongSwan VPN 客户端” 右边的设置图标，然后启用 **始终开启的 VPN** 以及 **屏蔽未使用 VPN 的所有连接** 选项。

## Linux

> 你也可以使用 IPsec / XAuth 或者 IPsec/L2TP 默认模式连接。

要配置你的 Linux 计算机以作为客户端连接到 IKEv2，首先安装 NetworkManager 的 strongSwan 插件：

```
# Ubuntu and Debian
sudo apt-get update
sudo apt-get install network-manager-strongswan

# Arch Linux
sudo pacman -Syu  # 升级所有软件包
sudo pacman -S networkmanager-strongswan

# Fedora
sudo yum install NetworkManager-strongswan-gnome

# CentOS
sudo yum install epel-release
sudo yum --enablerepo=epel install NetworkManager-strongswan-gnome
```

下一步，将生成的 **suin.p12** (/uploads/blog/202203/suin.p12) 文件安全地从 VPN 服务器传送到你的 Linux 计算机。然后提取 CA 证书，客户端证书和私钥。

```
# 示例：提取 CA 证书，客户端证书和私钥。在完成后可以删除 .p12 文件。
# 注：你可能需要输入 import password，它可以在 IKEv2 辅助脚本的输出中找到。
#     如果在脚本的输出中没有 import password，请按回车键继续。
openssl pkcs12 -in .p12 -cacerts -nokeys -out ikev2vpnca.cer
openssl pkcs12 -in .p12 -clcerts -nokeys -out vpnclient.cer
openssl pkcs12 -in .p12 -nocerts -nodes  -out vpnclient.key
rm .p12

# （重要）保护证书和私钥文件
# 注：这一步是可选的，但强烈推荐。
sudo chown root.root ikev2vpnca.cer vpnclient.cer vpnclient.key
sudo chmod 600 ikev2vpnca.cer vpnclient.cer vpnclient.key
```

然后你可以创建并启用 VPN 连接：

1. 进入 Settings -> Network -> VPN。单击 **+** 按钮。
2. 选择 **IPsec/IKEv2 (strongswan)**。
3. 在 **Name** 字段中输入任意内容。
4. 在 **Gateway (Server)** 部分的 **Address** 字段中输入 `VPN 服务器地址` （或者域名）。
5. 为 **Certificate** 字段选择 `ikev2vpnca.cer` 文件。
6. 在 **Client** 部分的 **Authentication** 下拉菜单选择 **Certificate(/private key)**。
7. 在 **Certificate** 下拉菜单（如果存在）选择 **Certificate/private key**。
8. 为 **Certificate (file)** 字段选择 `vpnclient.cer` 文件。
9. 为 **Private key** 字段选择 `vpnclient.key` 文件。
10. 在 **Options** 部分，选中 **Request an inner IP address** 复选框。
11. 在 **Cipher proposals (Algorithms)** 部分，选中 **Enable custom proposals** 复选框。
12. 保持 **IKE** 字段空白。
13. 在 **ESP** 字段中输入 `aes128gcm16`.

14. 单击 **Add** 保存 VPN 连接信息。
15. 启用 **VPN** 连接。

---

作者：刘丹 创建时间：2022-04-13 10:32
最后编辑：刘丹 更新时间：2022-05-16 06:17