

# 麒麟 SSL VPN 使用指南

## 系统安装部分：

1. 生成一个初始化的 centos7.x 64bit, 系统需要有 yum 源
2. 下载 get.tosec.com.cn/vpn.tar.gz 到/tmp 目录
3. 运行如下命令

```
cd /tmp
tar xpvf vpn.tar.gz
bash yum.sh
bash install.sh
init 6
```

4. 找厂商生成许可（其它-licenses 菜单点击生成）
5. 管理员部分：

SSL VPN 主机配置主要分为三步，网络策略设置（用于打开 VPN 服务器服务端口）、创建 VPN 用户（用于 VPN 连接认证）、创建 VPN 路由（指定哪些 IP 或网段使用 VPN 隧道连接）

1. 安全策略配置

VPN 需要向公网开放 2 个端口，TCP 443 和 UDP 7286。

TCP 443 为管理端口，打开后管理员可以使用浏览器登录并设置用户和路由，普通用户  
可以登录并且修改密码。

UDP 7286 为 VPN 端口，用户通过连接 VPN 端口连接到内网

比如在云主机安全策略中，需要设置如下二条即可完成网络配置：

入站规则		出站规则		
来源	协议端口	策略	备注	操作
<input type="checkbox"/> 0.0.0.0/0	TCP:443	允许	-	编辑 插入 删除
<input type="checkbox"/> 0.0.0.0/0	UDP:7286	允许	-	编辑 插入 删除

2. 创建 VPN 连接帐号

系统安装完成后，使用 <https://ip> 可以访问到系统管理界面，默认口令为 admin/12345678。

用户需要使用 VPN 必须具有一个 VPN 帐号，使用 admin 登录后可以创建 VPN 帐号。

点击 资源管理-用户管理 菜单，点击添加按钮



**基本信息**

*用户名: testvpn	*真实姓名: testvpn
*密码: ***** 随机密码 中强	*确认密码: ***** 强制修改密码
*用户组: 用户组: 堡垒机默认管理员	证书CN:
电子邮件:	手机号码:
工作单位:	工作部门:
生效时间: 2019-04-10 08:05:54 选择时间	过期时间: 选择时间 永不过期
VPN: 允许	VPN IP:
用户权限: 认证用户	动态口令卡: 含有字符 未绑定 手机未扫描

### 3. 创建内网访问路由

内网访问路由是用户连接 VPN 后访问的内网资源 IP 或网段，只有在 VPN-路由中添加相应的网段或 IP 后，才通过 VPN 隧道访问这些 IP 或网段。

在 VPN 管理-VPN 路由中，点击增加按钮可以增加一条 VPN 路由，点击生效按钮即可生效

**VPN -路由**

IP	掩码	路由状态	操作
172.27.0.0	255.255.0.0	启用	删除
192.168.0.52	255.255.255.255	启用	删除
192.168.0.54	255.255.255.255	启用	删除
192.168.0.55	255.255.255.255	启用	删除
192.168.0.57	255.255.255.255	启用	删除
172.27.16.0	255.255.255.0	启用	删除
192.168.0.50	255.255.255.255	启用	删除

- 1.先点增加按钮增加内网云主机IP或网段
- 2.点生效按钮生效添加或删除的路由
- 3.断开重连VPN客户端即可生效

注意：VPN 路由添加后，所有的 VPN 服务会重新启动，所有的 VPN 客户端都需要断开重拨才能继续使用。

## 用户使用部分：

### Windows 客户端

#### 1. 安装

程序下载地址：<http://get.tosec.com.cn/soft/sslvpn-win-64.zip>

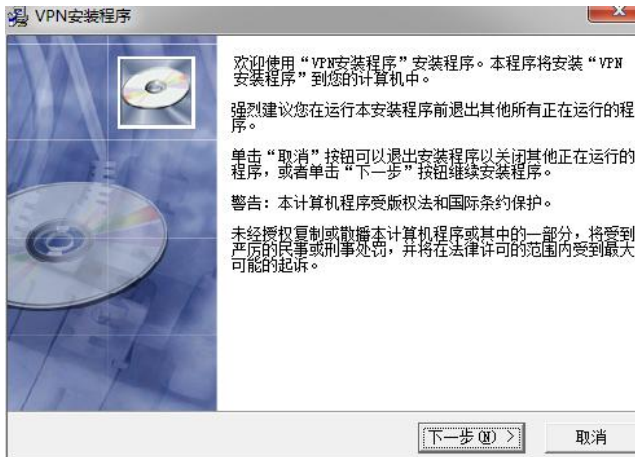
**注意事项：**

**XP、2000、2003、Vista 必须以管理员登录进行安装**

**Windows 7、10 必须采用以管理员身份进行安装**

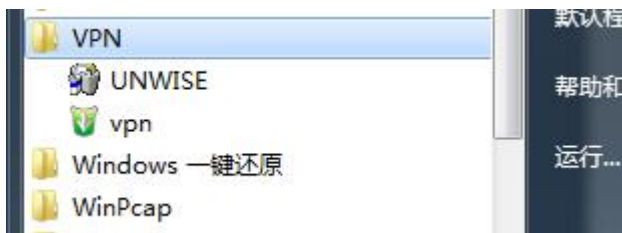
**Windows 8 必须管理员身份使用兼容 Windows 7 方式进行安装**

2.启动安装程序，直接点击“下一步”按钮



3.程序将自动启动安装，安装完毕后，点击完成按钮即可以退出安装

4.启动 VPN 系统，VPN 安装好以后，在菜单中会产生一个 VPN 的菜单，点击菜单里的 VPN 即可以启动 VPN 软件



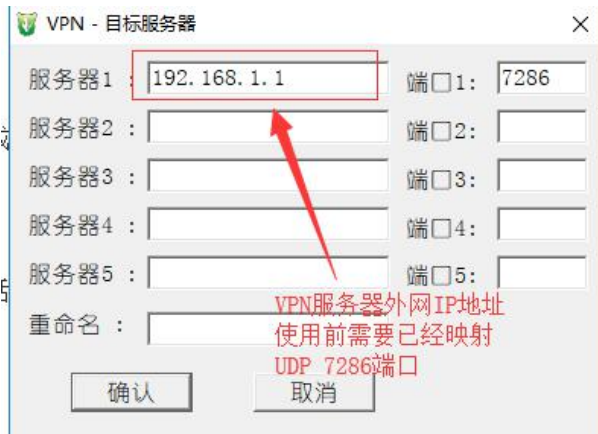
VPN 启动后在 Windows 右下角的工具栏会产生一个图标：



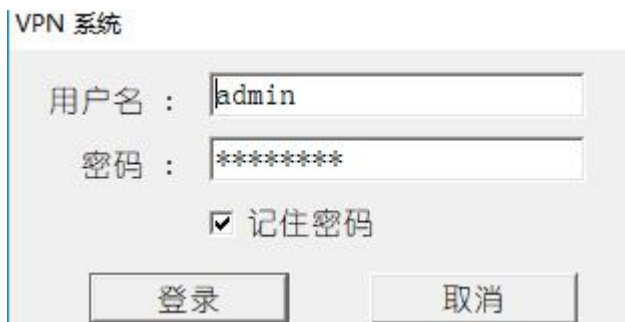
5. 设置 VPN 服务器，鼠标右击 VPN 图标，选择“系统配置”菜单



系统会打开 VPN 服务器对话框，在服务器 1 中输入堡垒机外网 IP，点击确认按钮即完成设置



6. 用户使用，鼠标右击 VPN 图标，选择“连接”菜单，即可以进行连接，在连接对话框中输入堡垒机的用户名、密码，即可以登录：



登录后，VPN 图标即可以显示为绿色，这时即可以通过堡垒机访问内网



7. VPN 连通后访问堡垒机：VPN 连通后，即可访问已经在 VPN 路由中发布的主机和网段

## 苹果 MACOS 使用

客户端下载地址:

<http://get.tosec.com.cn/soft/sslvpn-macos.zip>

1. 双击压缩包软件 Tunnelblick\_3.7.8\_build\_5180.dmg，出现如下图



2. 双击 "Tunnelblik"文字上的图标，会弹出窗口，输入 mac 系统帐号密码，完成以后就安装完毕。安装后系统会询问是否有配置，选择“我没有配置文件”退出

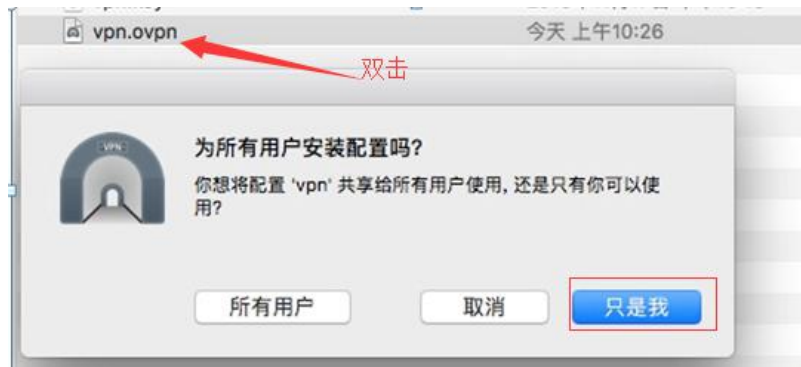


3. 将压缩包中的 config 目录解压，打开 config 文件夹，使用文本编辑器修改 vpn.ovpn 的配置，把其中的 ip 改为目标 vpn 服务器的外网映射 IP，编辑完退出。

```
client
dev tun
proto udp
remote 127.0.0.1 7286
remote-random
resolv-retry infinite
nobind
persist-key
persist-tun
ca vpn.crt
cert baoleiji.crt
auth-user-pass
```

修改为VPN服务器或堡垒机IP

4. 然后双击该配置文件，弹出窗口，选择“只是我”，系统会自动用 tunnelblick 打开，并配置好 vpn。



然后后就可以点击下图 tunnelblick 图标，下拉选择连接 VPN 菜单



弹出输入用户名和密码的窗口,输入 VPN 用户名和密码，如果有动态口令，则在密码处输入静态口令和动态口令的连接字符串



输入完点击确定，vpn 就开始连接，如果认证通过，很快就会连接上。连接成功。如图图标变亮了。



## 安卓平台使用

安卓版本 VPN 客户端下载地址:

<http://get.tosec.com.cn/ics-openvpn-0.7.8.apk>

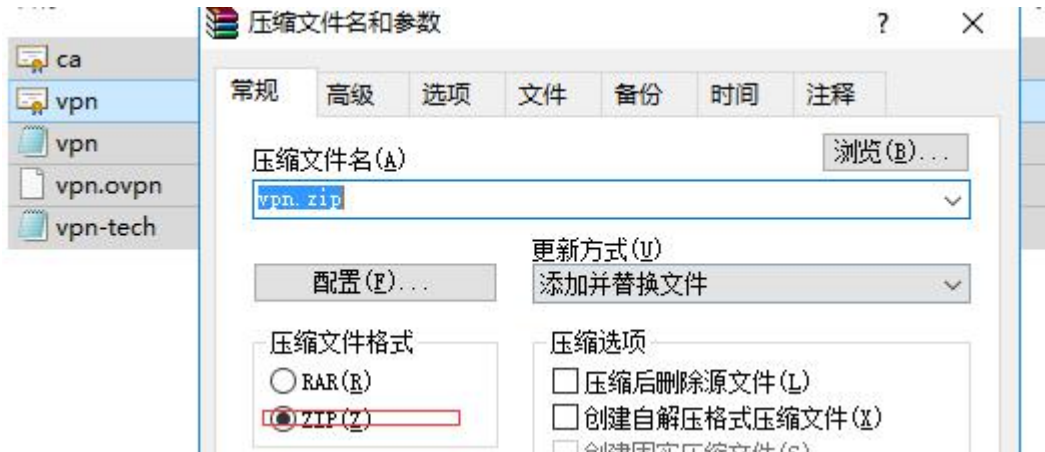
配置文件下载地址:

<http://get.tosec.com.cn/config.zip>

1. 在 windows 中解压的 config.zip, 里面有一个使用记事本打 vpn.ovpn 文件, 修改 remote 行, 将 IP 修改为 VPN 服务器公网 IP



2. 将所有的文件再次打包成 vpn.zip (注意最好用 zip, 不要用 rar, 不然有可能在安卓系统中打不开):



3. 在安卓平台上安装附件中的安卓 openvpn 安装包, 只需要默认安装即可
4. 将第 2 步打包的 vpn.zip 使用 qq 或微信解包, 解压后放在安卓设备 (一定要解压), 记住文件目录位置
5. 打开第 3 步安装的安卓 openvpn, 点击下图位置



6. 点击后会弹出文件管理器，找到第 4 步解压的位置，选择 `vpn.ovpn`

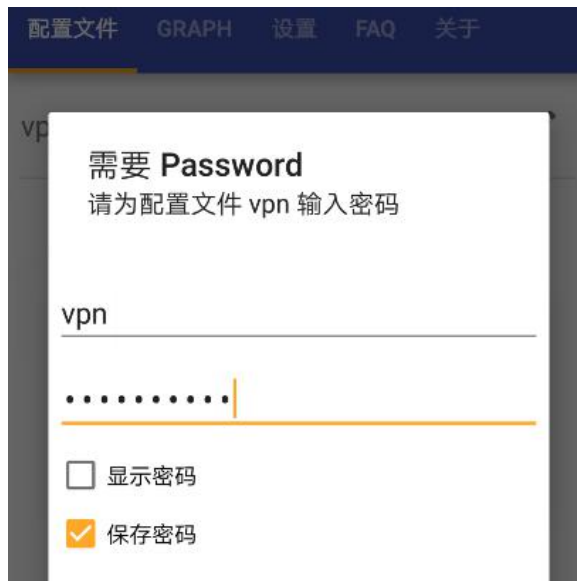


7. 在配置文件名称处输入一个名称（自定义，标识用），然后点击右上方的勾

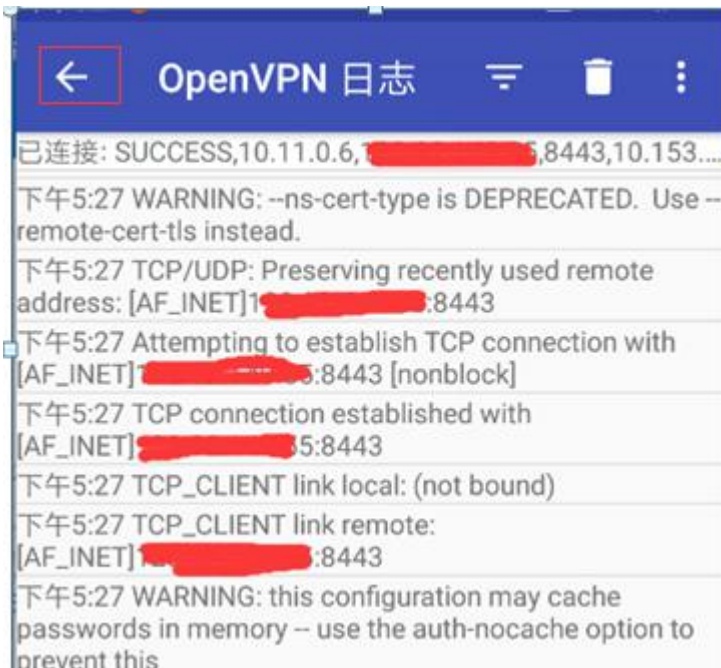




7. 在配置文件中点击刚才导入的名称，出现用户名和密码对话框，输入 VPN 用户名和密码（建议勾选保存密码）然后点击连接



8. 出现 VPN 连接日志，显示整个连接过程，直到最后一行出现 completed，即表示连接成功，点左上角的返回按钮



9. 屏上显示出 VPN 当前状态，这时如果 VPN 已经发布了内网应用即可以连接到内网进行操作

故障排查:

1.

