# 安全认证网关移动端

# 概述

随着信息技术的发展，企业内部员工及合作伙伴间的信息交互逐渐频繁，如何通过互联网访问企业内部系统，实现远程办公成为企业发展的必然要求。

安全认证网关移动端是安装在有远程办公需求的用户员工移动设备上，是安全认证网关产品的一部分，主要完成手机端Android系统下，app负责与网关服务端建立安全vpn链路，使得手机端可通过符合国密标准的安全信道访问企业内网资源。

手机客户端的开发框架包括以下几部分：

* 修改支持国密算法

移动网关要支持Android手机的安全接入，需要在Android系统上的客户端软件采用国产商码算法进行通信数据加密。开源程序OpenVPN本身支持手机端接入，但是需要改成国密算法的客户端。

国密协议的支持：

* GM/T0024-2014《SSL VPN 技术规范》
* GM/T0025-2014《SSL VPN 网关产品规范》
* GM/T 0026-2014《安全认证网关产品规范》
* 进行原型设计和UI设计

将客户端改造成符合本公司自己风格的APP。去掉开源程序的logo,按照自己的风格改造app界面。

* 细节功能补充

对于一些需要后期补充的功能，由于Android系统上的应用程序是采用JAVA实现的，为了JAVA应用程序能调用C语言实现的应用接口，需要设计JNI接口。

# 应用场景

移动用户在移动终端上安装相应的VPN客户端，通过账号口令方式或者使用预先颁发的证书（此处先考虑软的）进行认证，进而与总部网关服务器建立安全的VPN隧道。

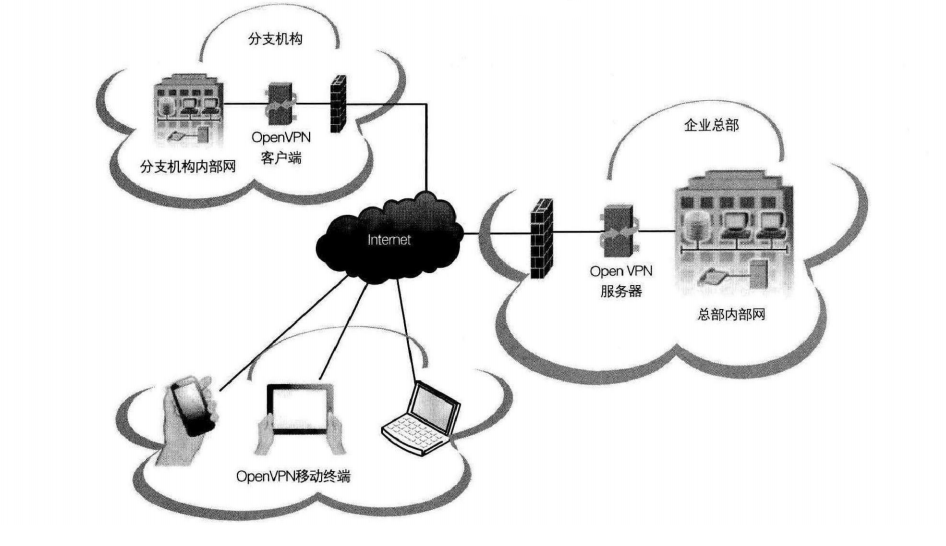


图 1 安全认证网关部署

安全认证网关移动端在安全认证网关产品中的位置如下图所示：

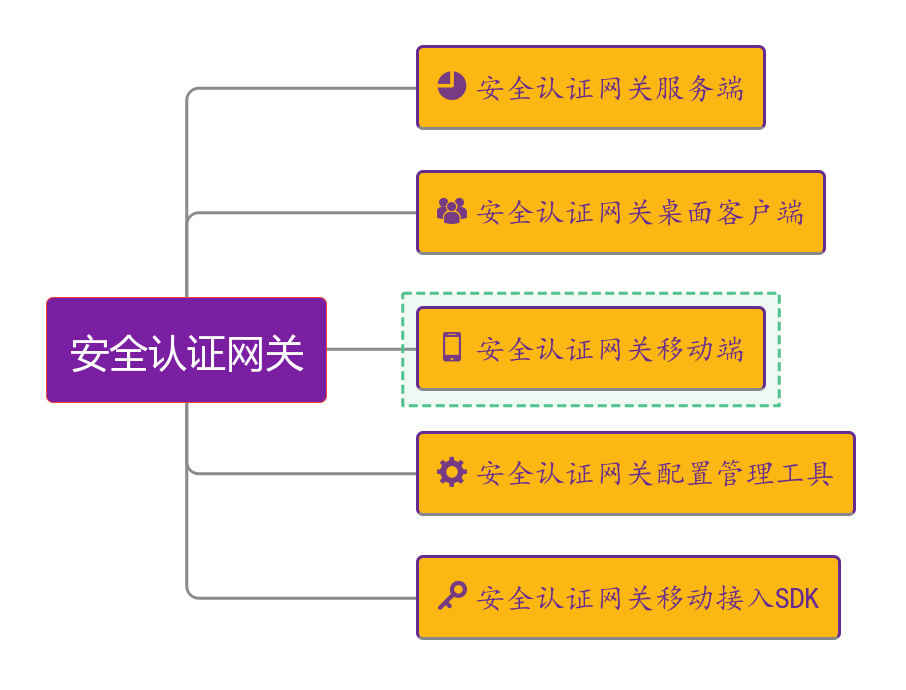


图 2 安全认证网关结构图

# 功能需求

安全认证网关移动端具备与安全认证网关桌面客户端近乎相同的功能，区别仅在于运行平台不同。安全认证网关桌面客户端运行在普通PC机上，支持windows和linux及国产化操作系统；安全认证网关移动端则运行在android 4.0+的手机端或PAD端。

整个移动VPN运行过程工作交互模式如下图所示。

图 3 工作交互模式

安全认证网关移动端模块设计如图 4 安全认证网关移动端结构图所示。

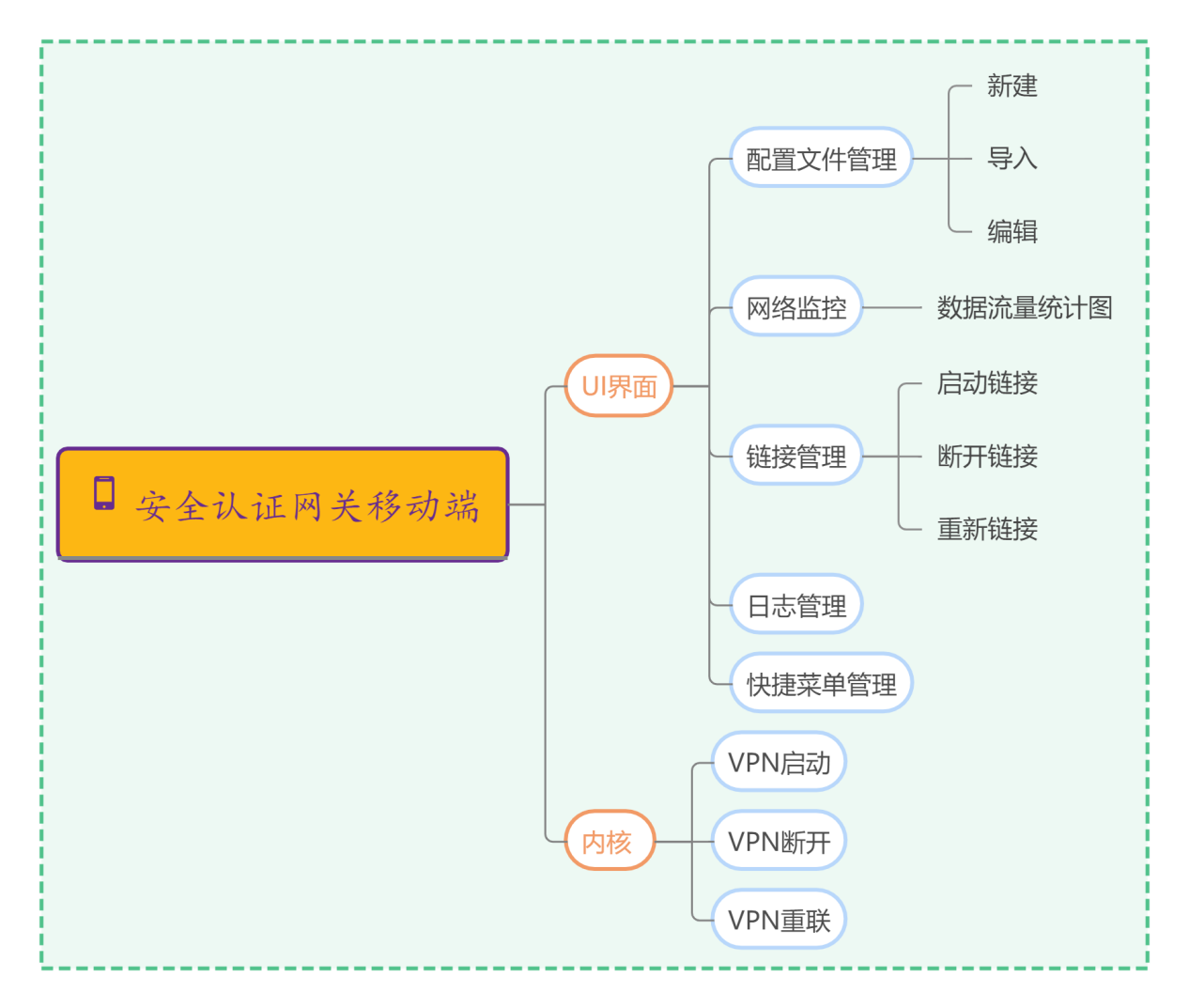


图 4 安全认证网关移动端结构图

# 界面设计

## 程序图标



## 配置文件管理

程序启动后，默认进入配置文件管理页面，如下图所示：

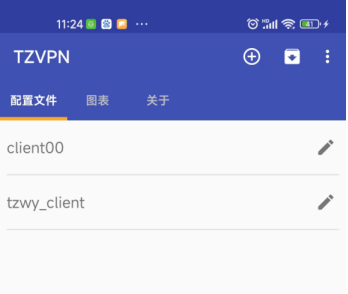


图 5 配置文件管理页

说明：

：新建配置文件

：导入配置文件

配置文件列表：

* client00：已导入的配置文件，文件名为client00，点击该列表项，程序启动vpn建立链接，链接建立后，再次点击该列表项，显示断开连接或断开重连菜单项
* tzwy\_client：新建的配置文件，文件名为tzwy\_client
* ：修改配置文件，编辑对应的配置文件。点击该按钮，切换至配置文件编辑页面

### 新建配置文件

点击按钮，程序跳转至新建配置文件页面，如下图所示：

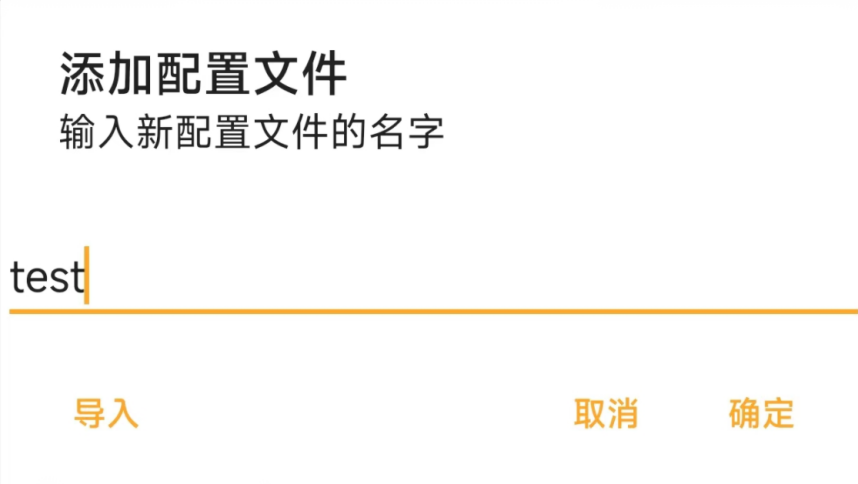


图 6 新建配置文件

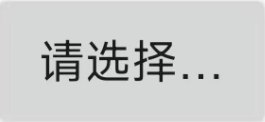
点击【确定】按钮，程序跳转至修改配置项页面，详情参见第3.2.3节，在此不做赘述。

### 导入配置文件

点击按钮，程序默认打开sd卡路径，选择要导入的ovpn文件，如tzwy\_client.ovpn，选择该文件后，程序跳转至配置文件转换页，如下图所示：



图 7 导入配置文件

程序自动判断导入的配置文件中，对证书和私钥的配置路径是否正确，在该页面可通过点击按钮重新选择证书和私钥路径，主要包括：CA证书、客户端签名证书、客户端签名私钥、客户端加密证书、客户端加密私钥。配置完成后，点击右上角按钮，保存配置，程序将跳转至配置文件管理页，同时将导入的配置文件名tzwy\_client插入配置文件列表中，如图 1 配置文件管理页所示。

### 编辑配置文件

编辑配置文件页可通过以下两种情景进入：

1. 新建配置文件后
2. 点击配置文件管理页如图 3 配置文件管理页中配置文件列表框中的图标。

编辑配置文件页界面包含三个小模块，分别是基本设置、服务器列表以及允许的应用程序。

1. 基本设置页



图 8 编辑配置文件-基本设置

基本配置页主要完成用户登陆方式的配置，常用的登陆方式有如下三种：

1. 用户名/密码
2. 证书
3. 用户名/密码 + 证书

登陆方式，可通过点击【类型】下的下拉列表框进行选择。



图 9 登录方式

登录方式的选择，取决于安全认证网关服务端内核的配置，默认使用用户名/密码+证书的登录方式。用户可在该页面配置相应的客户端证书和私钥。

1. 服务器列表



图 10 服务器列表页

服务器列表页用于配置手机端需要连接的网关服务器的IP、端口号，以及连接使用的协议，该协议的选择由服务端指定。

点击按钮，可以增加多个服务器配置。

点击按钮，可以删除当前服务器配置。

1. 允许的应用程序

允许的应用程序页面将列出手机中联网的程序，可在该页面设置是否允许应用程序使用安全认证网关上网。

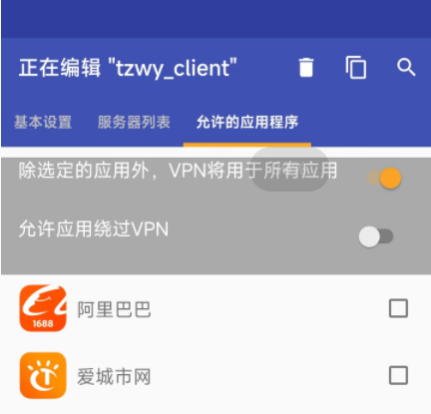


图 11 允许的应用程序

## 网络监控

网络监控页面可以统计并显示该手机终端不同时间段，通过安全认证网关发送和接收的速度。界面如下图所示：

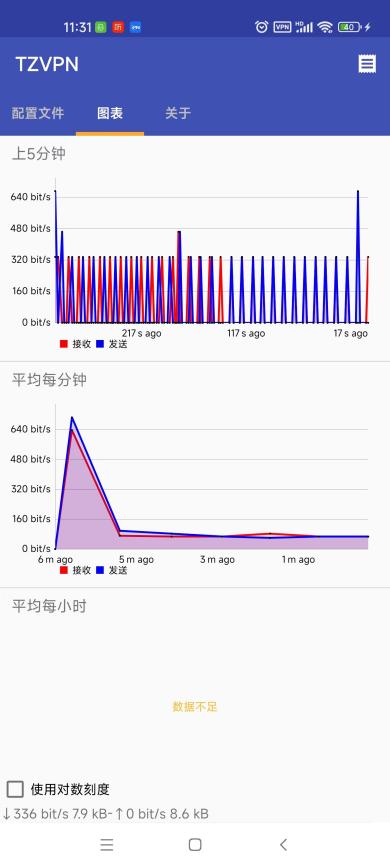


图 12 网络监控

## 链接管理

链接管理主要负责vpn信道的建立、断开，该部分功能通过点击配置文件管理页中配置文件列表中相应配置文件的列表项实现。

### 启动链接

导入或新建配置文件后，在配置文件管理页的列表中点击已导入或新建的配置文件名，如tzwy\_client。

1. 证书方式登录：

点击已导入的被配置为证书登录的配置文件如client00，系统自动跳入日志管理页面，显示Initialization Sequence Completed表示链接成功。返回配置文件管理页，在该配置文件列表项中显示【已连接：SUCCESS】表示链接成功，日志页显示如图 13 日志管理所示，返回配置文件管理页，如下图所示。

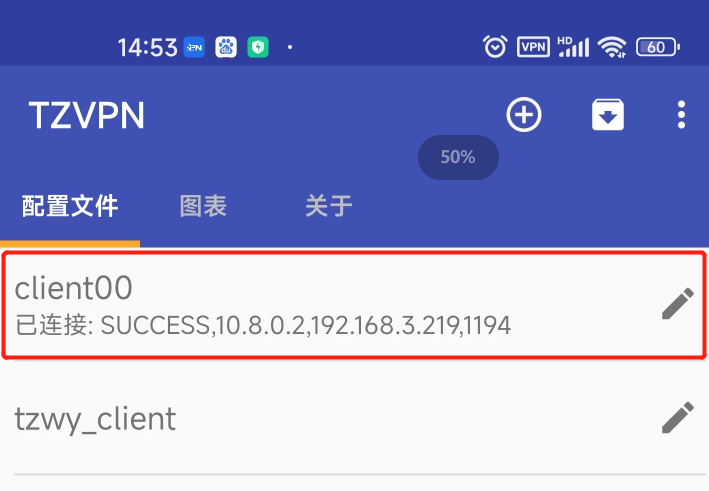


图 13 证书登录链接成功

其中，10.8.0.2为本机的虚拟ip地址，192.168.3.219和1194分别为安全认证网关的服务器ip和端口。

1. 用户名密码或用户名密码+证书方式登录

在弹出框中输入安全认证网关配置管理工具中为用户授权的用户名和密码，如下图所示。

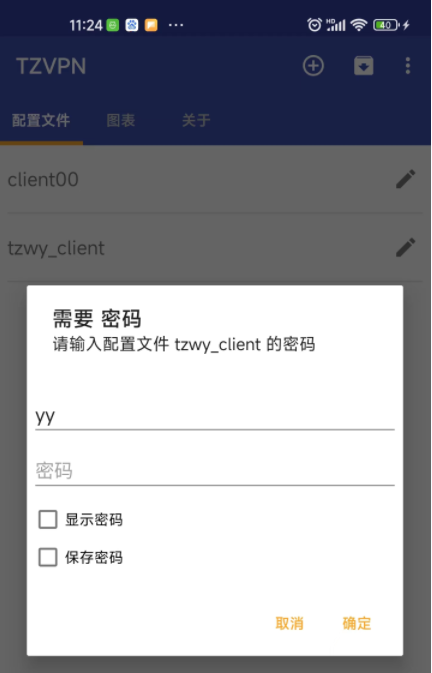


图 14 用户名密码方式登录

点击确定按钮，系统自动跳转至日志管理页面，显示Initialization Sequence Completed表示链接成功。返回配置文件管理页，在该配置文件列表项中显示【已连接：SUCCESS】表示链接成功，如下图所示

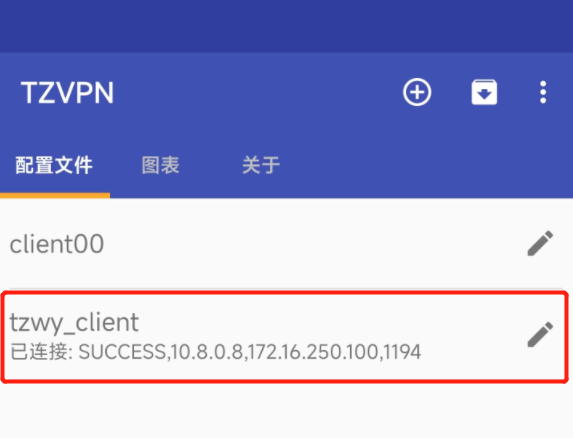


图 15 链接成功

其中，10.8.0.8为本机的虚拟ip地址，172.16.250.100和1194分别为安全认证网关的服务器ip和端口。

### 断开链接

在配置文件列表中，点击已链接的配置文件列表项，弹出窗口如下图所示：



图 16 断开连接

点击【断开】按钮，vpn链接将被断开，手机无法通过vpn信道访问安全认证网关配置的内网数据。

### 断开重连

在配置文件列表中，点击已链接的配置文件列表项，弹出如图 14 断开连接所示弹框，点击重新链接按钮，则依据配置文件配置项，重新建立与安全认证网关之间的vpn信道。

## 日志管理

日志管理页面显示vpn信道建立过程中的日志信息，可用于研发人员排错。界面如下图所示：



图 17 日志管理

## 快捷菜单管理

快捷菜单管理分为长按程序图标的快捷菜单和通知栏的快捷菜单管理。

### 长按程序图标快捷菜单



图 18 长按程序图标快捷菜单

说明:

Disconnect VPN:断开链接

连接到client00：连接到配置文件client00

连接到tzwy\_client：连接到配置文件tzwy\_client

卸载：卸载该app

### 通知栏快捷菜单



图 19 通知栏快捷菜单

说明:

TZVPN-tzwy\_client:当前链接使用的配置文件为tzwy\_client

336 bit/s 4.8kB 0 bit/s 5.5kB：该连接上传下载速度及流量

断开：断开该连接

暂停VPN:暂停该连接

# 设计原理

安全认证网关移动端的设计采用界面和逻辑分离的原则进行设计，app分为界面和内核两个部分，内核部分没有界面，仅提供vpn连接管理功能。界面部分如第3章界面设计所示。

安全认证网关移动端的核心 SSL VPN 功能是基于 GMSSL 加密库中的 GMSSL协议函数库实现的一种数据封装技术。通过虚拟网卡，SSL 加密隧道等一系列加密技术，确保通信过程中数据安全。

安全认证网关移动端连接到安全认证网关后的数据流向如下图所示：



图 20 数据流向图

如果用户访问一个远程的虚拟地址（属于虚拟网卡配用的地址系列，区别于真实地址），则操作系统会通过路由机制将数据包（TUN模式）发送到虚拟网卡上，安全认证网关移动端程序接收该数据并进行相应的处理后，通过 SOCKET 从外网上发送出去，安全认证网关服务端程序通过 SOCKET 从外网上接收数据，并进行相应的处理后，发送给虚拟网卡，则应用软件可以接收到，完成了一个单向传输的过程，反之亦然。

## OPENVPN协议

OpenVPN协议的封装格式如下图所示：

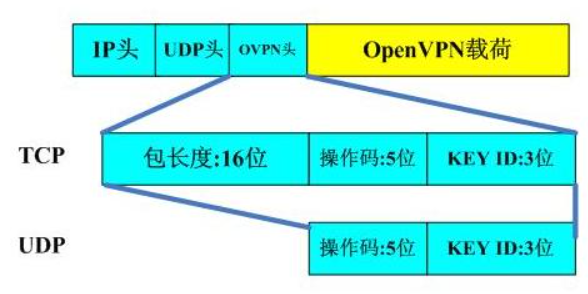


图 21 OPENVPN协议头结构

OVPN头封装了OpenVPN的握手协议和记录协议,按信道划分，OpenVPN的信道有两类，一类是控制信道，另一类是数据信道.操作码区分了控制信道和数据信道,也就是控制协议和记录协议，其中控制协议分为握手协议和密钥协议。

### OPENVPN控制协议

OPENVPN控制协议包含了两个部分，第一部分是握手协议，第二部分是密钥协议。SSL握手最终协商的那个密钥和SSL握手过程是分不开的，而OpenVPN最终的设计是希望将握手过程和数据传输过程完全分离，从而独立的实现单一的密钥重协商

控制协议包结构如下图所示：

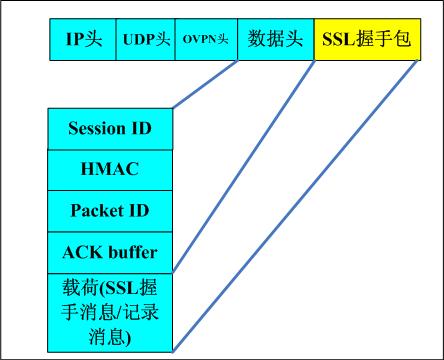


图 22 OPENVPN控制协议包结构

### OPENVPN记录协议

记录协议包结构如下图所示

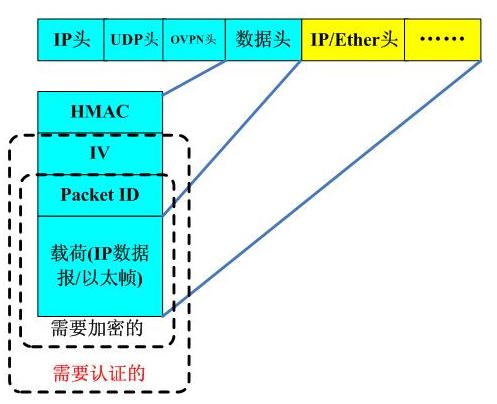


图 23 记录协议包结构

其中HMAC用于认证包的完整性，IV用于CBC解密，Packet ID用于防止重放。

### 握手协商过程

Openvpn协议的握手过程使用到了openvpn控制协议和密钥协议，OenVPN结合了SSL协议，但设计了独特的openvpn协议以及握手协议过程，所以OenVPN协议的握手协商过程包括SSL握手协商。它通过openvpn控制协议以及openssl第三方软件包的BIO几只有效的封装了SSL握手协议。

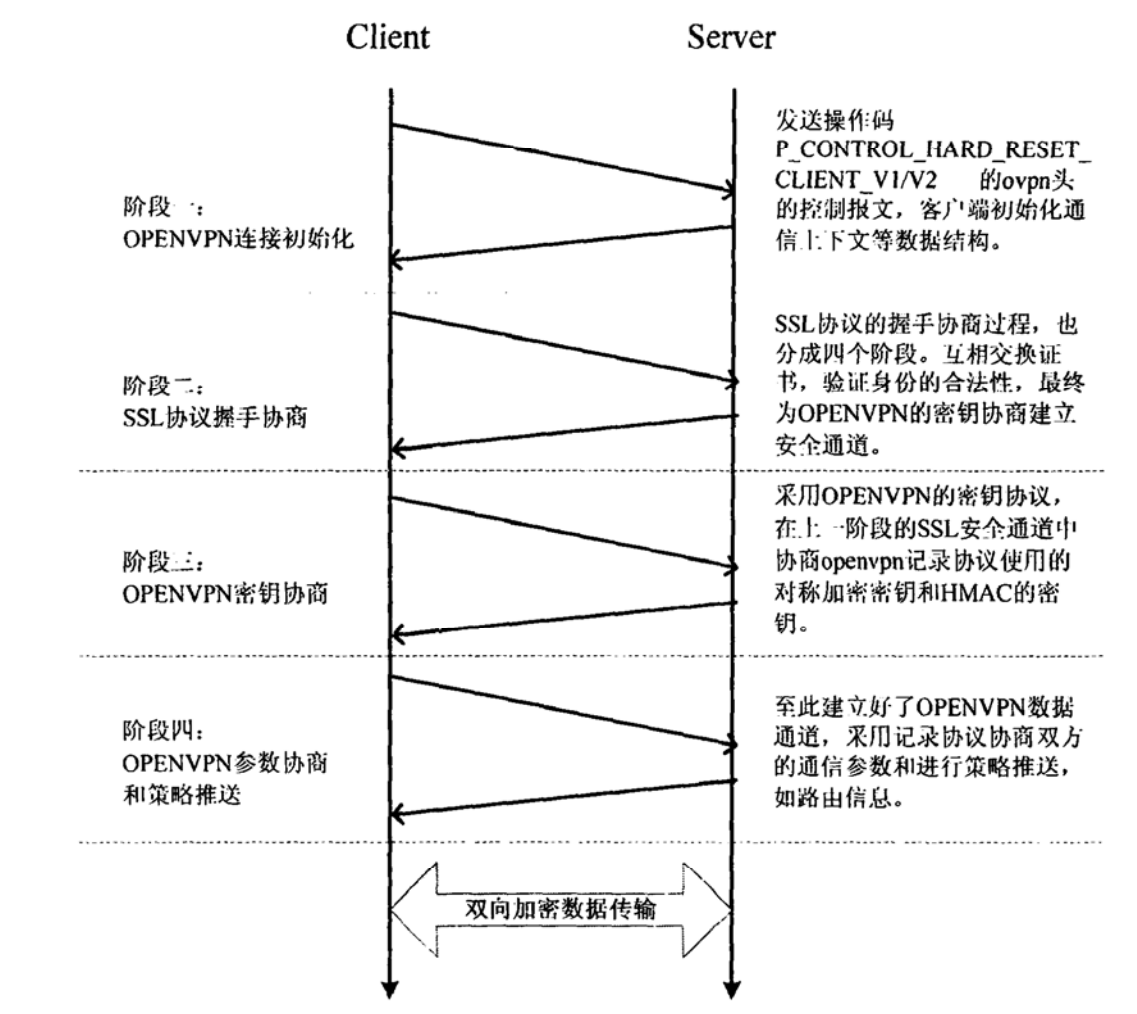


图 24 Openvpn的握手协商过程

### OPENVPN封装SSL



图 26 OPENVPN封装SSL

## 协议包结构

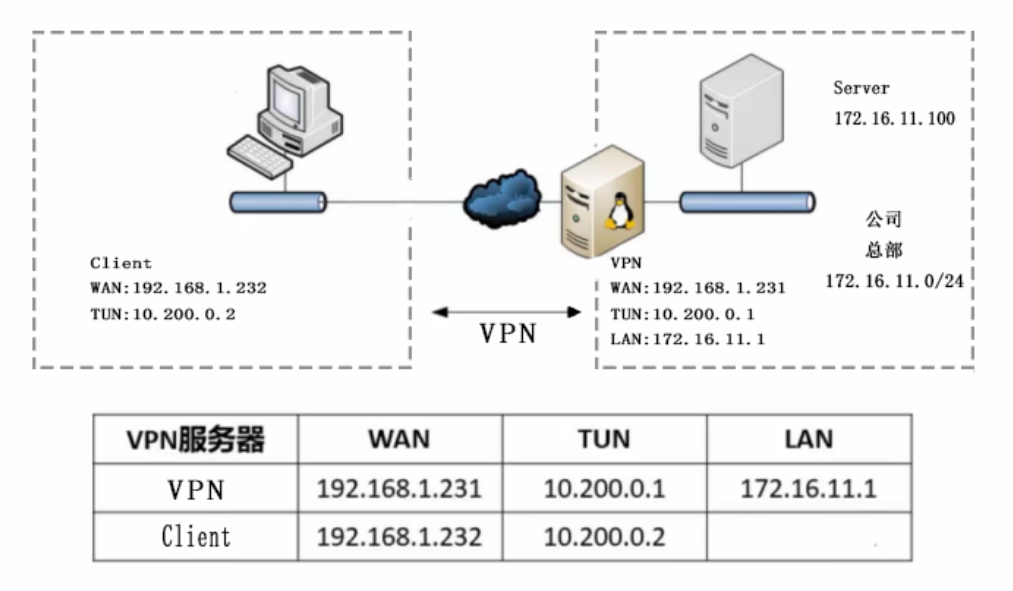


图 27 VPN简易应用场景

在图 19 VPN简易应用场景下，数据包的流向及协议结构如下图所示：

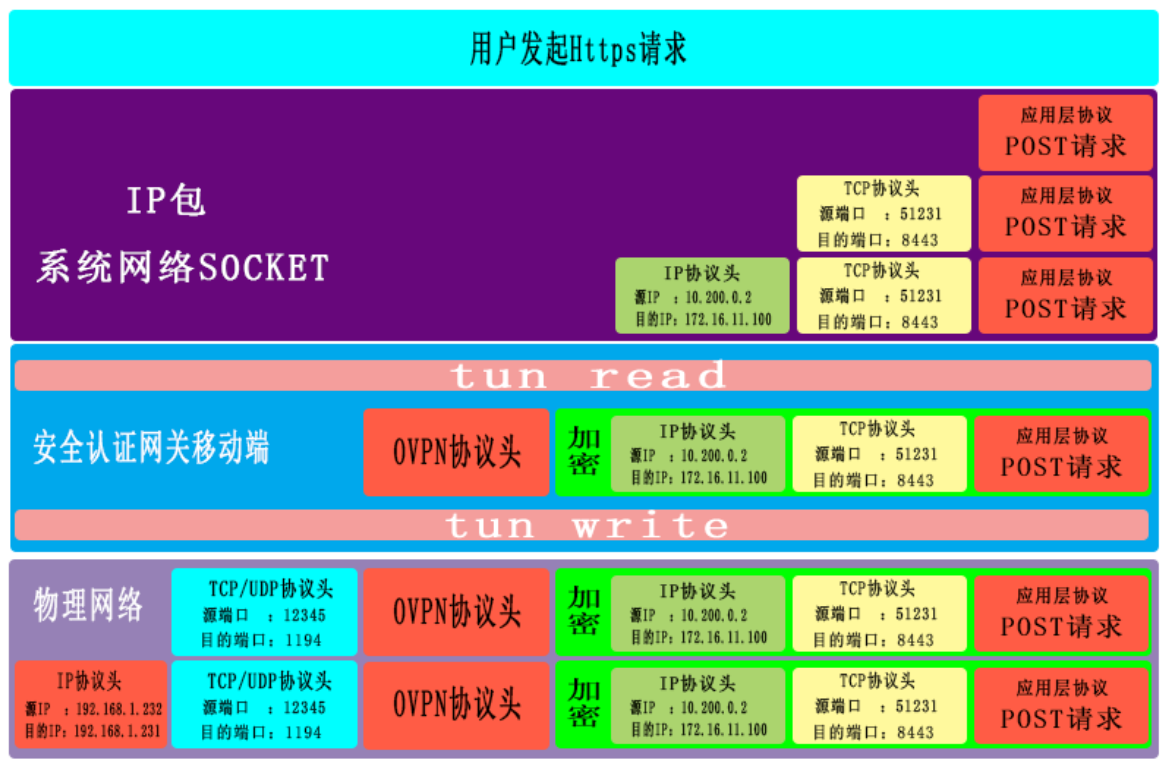


图 28 协议包数据结构

## Gmssl的Android版本编译

CPU：x86\_64

指令集：amd64

操作系统：

统信uos -Linux tzwy-PC 4.19.0-amd64-desktop

编译环境：

Android studio-2021.3：android-studio-2021.3.1.17-linux.tar.gz

JDK8u33：jdk-8u333-linux-x64.tar.gz

android-ndk-r25b：android-ndk-r25b-linux.zip

Android-sdk-24.4.1：androiddk\_r24.4.1-linux.tgz

Python-3.9.10

环境变量配置：

export JAVA\_HOME=/opt/jdk1.8.0\_333

export CLASSPATH=$:CLASSPATH:$JAVA\_HOME/lib/

export ANDROID\_NDK=/home/tzwy/zhouping/Android/android-ndk-r25b

export ANDROID\_SDK=/opt/android-sdk-linux

export PATH=/usr/local/bin:$PATH:$JAVA\_HOME/bin

编译脚本：

192.168.3.219:/home/tzwy/zhouping/Android/projects/gmssl-for-android-master/tools/build\_r.sh

编译命令：

登录192.168.3.219 用户名：tzwy 密码：zhouping

cd /home/tzwy/zhouping/Android/projects/gmssl-for-android-master/tools

./build\_r.sh

输出路径：

/home/tzwy/zhouping/Android/projects/gmssl-for-android-master/output/android/

使用：

将生成库拷贝至

E:\WorkSpace\projects\baseroot\openvpn\trunk\source\cpp\Android\ics-openvpn - 0.7.24\main\src\main\gmssl-libs

## Android代码中国密协议的编码支持

Android app代码中支持国密协议的修改步骤：

1. 将ics-openvpn - 0.7.24源码中使用的openssl库替换为新编译的gmssl库
2. 配置文件中增加双证书的支持
3. 代码中增加对配置文件中双证书字段的解析以及对双证书的加载使用
4. 增加对国密密码套件ECC-SM4-SM3的支持
5. 程序界面中配置文件设置中动态增加双证书选择