实验目的与要求：

1、 理解 SSL 证书。
2、 理解 HTTPS 的运行机制。
3、 配置 SSL VPN 服务端。
4、 配置客户端进行 SSL VPN 连接。

实验环境：

Windows 操作系统, SimpleISES

实验原理：

简单描述 HTTPS 访问机制，SSL VPN 连接。

HTTPS (HTTP over SSL | TLS) 是安全超文本传输协议，是在 TCP 之上进行了加密之后，再基于 HTTP 传输。HTTPS 在传输数据之前需要客户端（浏览器）与服务端（网站）之间进行一次握手，在握手过程中将确立双方加密传输数据的加密密钥。

HTTPS 工作原理：客户端和服务器端通过协商机制得到一个对称加密算法，就此双方使用该算法进行加密解密，从而解决了客户端与服务器端之间的通信安全问题。

- 协商机制采用非对称加密保证安全
- 使用数字证书签发机构颁发的证书来保证非对称加密过程本身的安全
- 使用对称加密、解密传输数据

SSLVPN 一般的实现方式是在企业的防火墙后面放置一个 SSL 代理服务器，SSL 代理服务器将提供一个远程用户与各种不同的应用服务器之间的连接，实现起来主要有握手协议、记录协议、警告协议的通信，SSLVPN 的通信过程主要集中在握手协议上，主要有：

第 1 步：SSL 客户机连接到 SSL 服务器，并要求服务器验证身份；

第 2 步：服务器通过发送它的数字证书证明自身的身份。这个交换包括整个证书链，直到某个证书颁发机构（CA），通过检查有效日期并确认证书包含可信任 CA 的数字签名来验证证书的有效性；

第 3 步：服务器发出一个请求，对客户端的证书进行验证；

第 4 步：双方协商用于加密的消息加密算法和用于完整性检查的 HAS 日函数，通常由客户端提供它所支持的所有算法列表，然后由服务器选择其中最强大的加密算法；

第 5 步：客户机和服务器通过下列步骤生成会话密钥。（1）客户机生成一个随机数，并使用服务器的公钥（从服务器证书中获得）对它加密，再送到服务器，（2）服务器用更加随机的数据、用客户机的公钥加密，发送至客户机以表示响应：（3）使用 HAS 日函数从随机数据中生成密钥。

实验内容：

1、 举例 HTTPS 网址，查找 SSL 证书及其从属结构。
2、 配置 SSL VPN 服务端并实现客户端连接。

实验步骤与结果：

项目一：举例 HTTPS 网址，查找 SSL 证书及其从属结构。

一般而言，需要保证用户信息和服务端信息的网站都需要使用 HTTPS，笔者这里以笔者自己的个人网页（https://ferryxie.cn/）为例进行。

图 1

接下来，笔者开始查找 SSL 证书及其从属结构。

第一步，打开网站点击网上边上的小锁，如图 2 所示，可以看到连接是安全的。

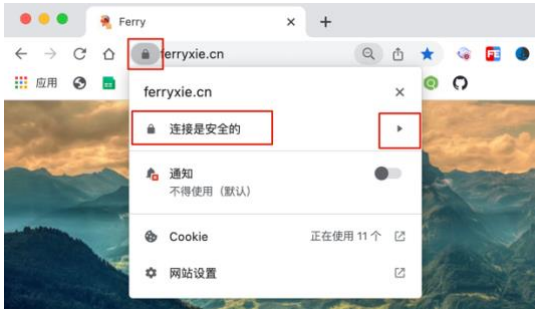

图 2

第二步，接着点击图二中的小箭头，在弹出的窗口中点击进入证书页面，如图 3 所示，可以看到证书有效。

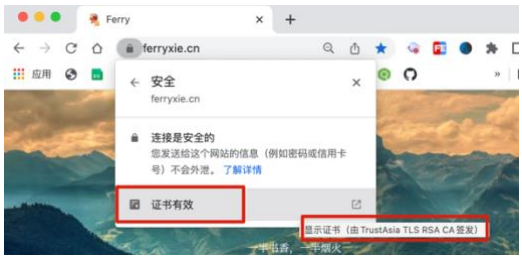

图 3

第三步，打开证书窗口，如图 4 所示，最顶端是证书路径，可以看到证书的颁发者和颁发路径、信任选项以及其他细节。

图 4

项目二：配置 SSL VPN 服务端并实现客户端连接

本部分是 Windows 下 SSL_VPN 实验，笔者在学院平台上完成（实验位置：主机安全课程-vpn 技术）。主要的实验原理是（1） 配置 SSL VPN 服务端。 （2） 配置客户端进行连接。客户端和服务端两个虚拟机的关系如下图 5 所示：

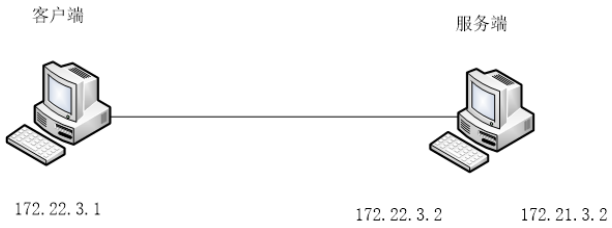

图 5

接下来笔者阐述具体的实验步骤。

一、 客户端安装

1.1 在客户端（其 IP 地址为 172.22.3.1）（如图 6 所示）上，双击桌面上 *“openvpn-install-2.3.10-I601-x86_64”* 进行安装，默认安装即可。 如图 7 所示

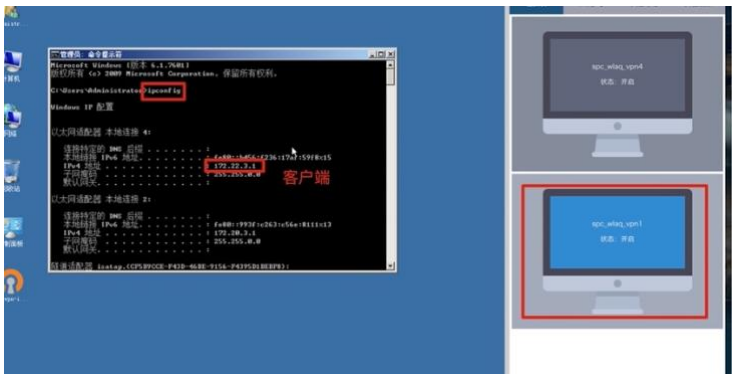

图 6

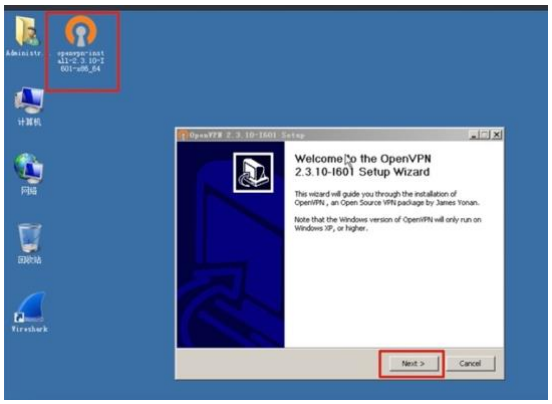

图 7

1.2 在安装过程中会弹出如下提示，选中”始终信任来自 OpenVPN Technologies,INC 的软件”，单击“安装”按钮，后面继续默认安装即可。如图 8 所示

图 8

二、PN 服务器软件安装

2.1 在服务端（其 IP 地址为 172.22.3.2）上（如图 9 所示），双击桌面上的 *openvpn-install-2.3.10-I601-x86_64*”进行安装，选中软件所有功能，然后单击“Next”安装。如图 10 所示

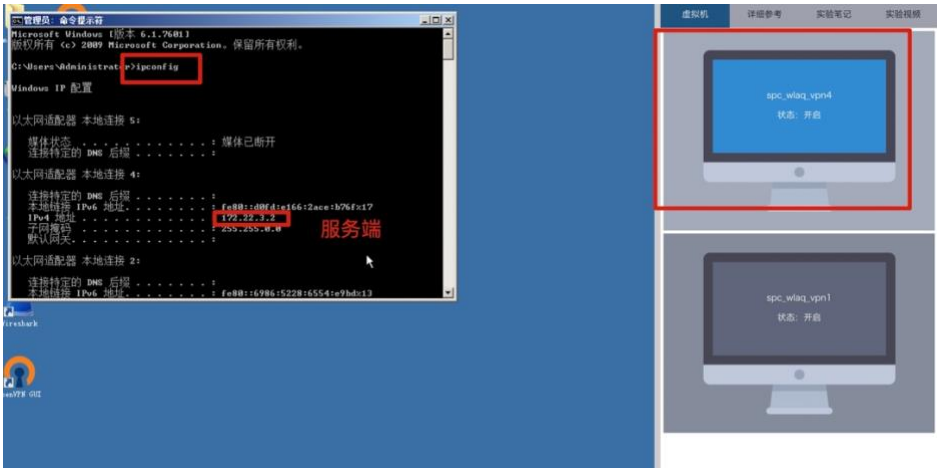

图 9

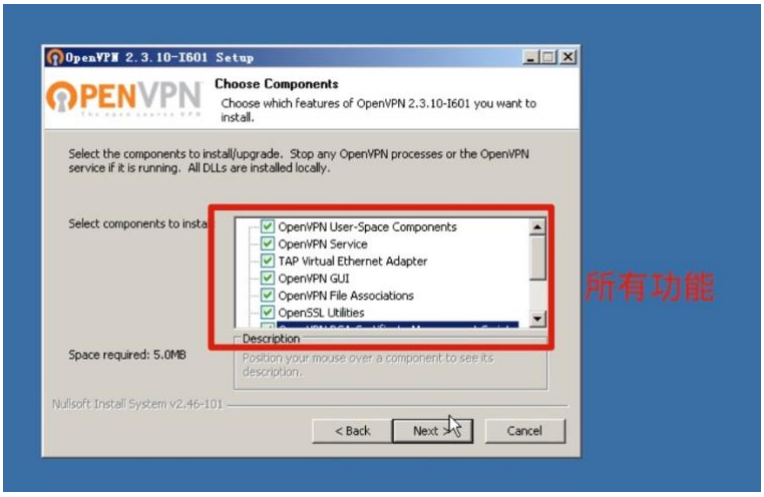

图 10

2.2 在安装过程中会弹出如下提示，选中”始终信任来自 OpenVPN Technologies,INC 的软件”，单击“安装”按钮，后面继续默认安装即可。如图 11 所示

图 11

2.3 复制一份目录“C:\Program Files\OpenVPN\easy-rsa”下的 vars.bat.sample 文件，重命名为 vars.bat，右键该文件，选择编辑。如图 12 所示

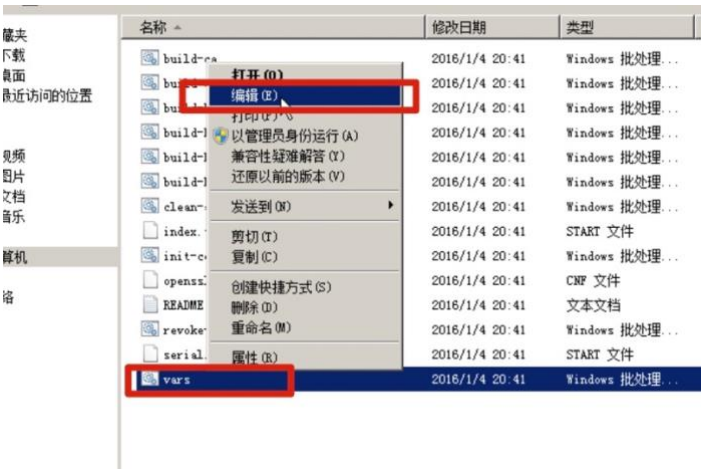

图 12

2.4 修改配置文件的参数“set KEY_COUNTRY=CN、set KEY_PROVINCE=BJ、set KEY_CITY=BeiJing、set KEY_ORG=xipu、set KEY_EMAIL=xipu@host.domain”，保存并关闭文件。如图 13 所示

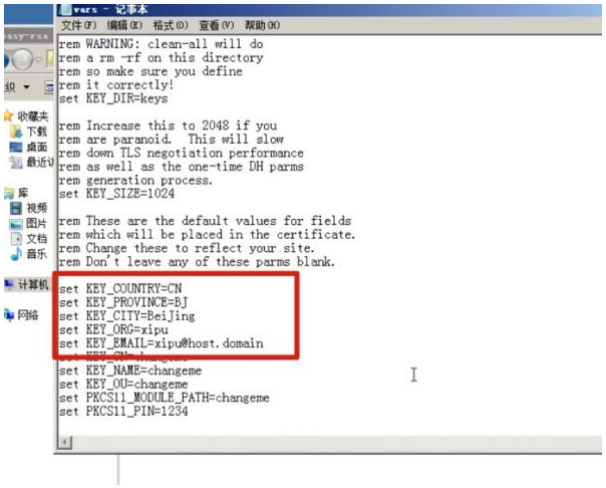

图 13

2.5 单击“开始”->”运行”->输入 cmd 命令。如图 14 所示

图 14

2.6 在命令行下输入“cd C:\Program Files\openvpn\easy-rsa”。如图 15 所示

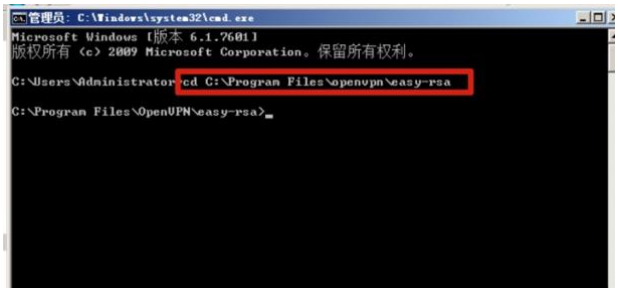

图 15

2.7 输入命令“vars”，设置相应的局部环境变量。如图 16 所示

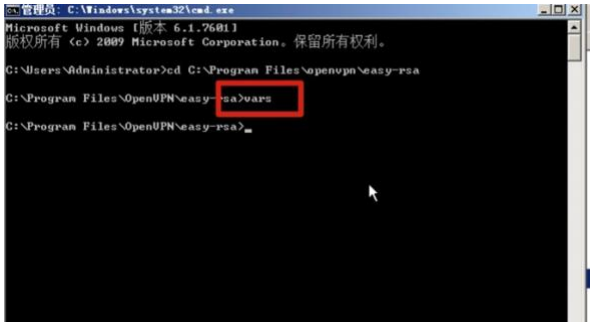

图 16

2.8 输入命令“clean-all”，清理操作。如图 17 所示

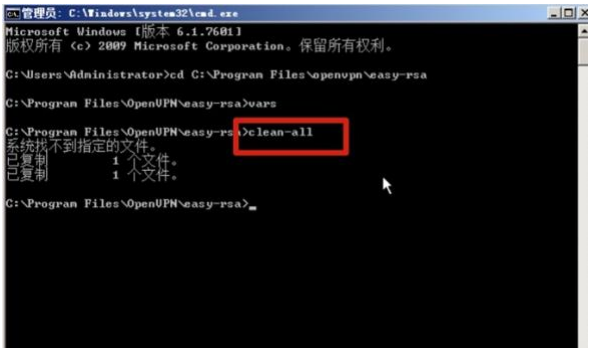

图 17

三、生成 CA

3.1 继续在服务端的 cmd 上输入命令“vars”。如图 18 所示

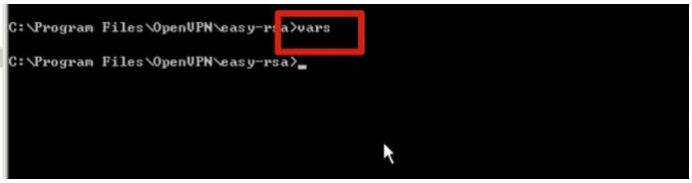

图 18

3.2 输入命令“build-ca”,填写参数，创建 CA 根证书（保持默认参数也可以）。如图 19 所示

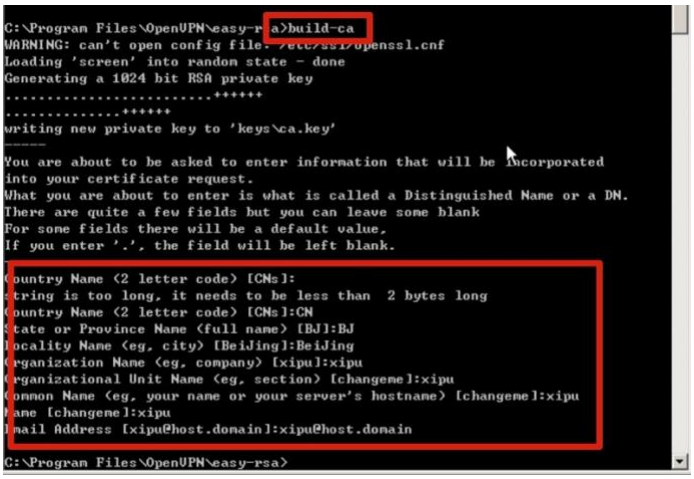

图 19

四、生成 dh1024.pem 文件

4.1 继续在服务端的 cmd 上输入命令“vars”。

4.2 输入命令“build-dh”。如图 20 所示

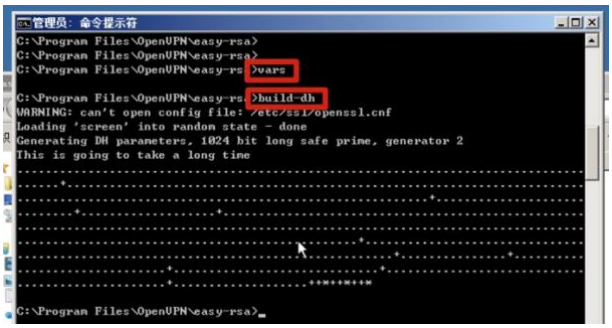

图 20

五、生成服务端正书

5.1 继续在服务端的 cmd 上输入命令“vars”。

5.2 输入命令“build-key-server xipuserver”填写参数，创建服务端证书。如图 21 所示

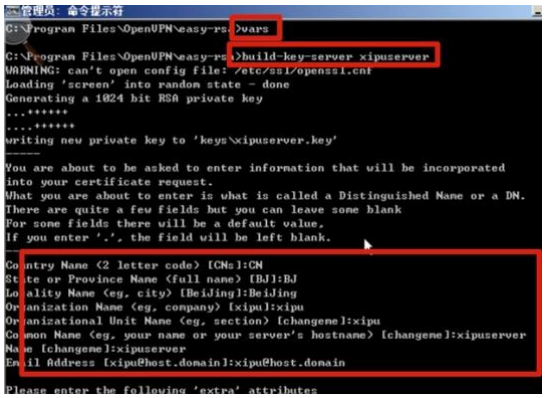

图 21

六、生成客户端证书

6.1 继续在服务端的 cmd 上输入命令“vars”。

6.2 输入命令“build-key xipuclient”，生成客户端证书。如图 22 所示

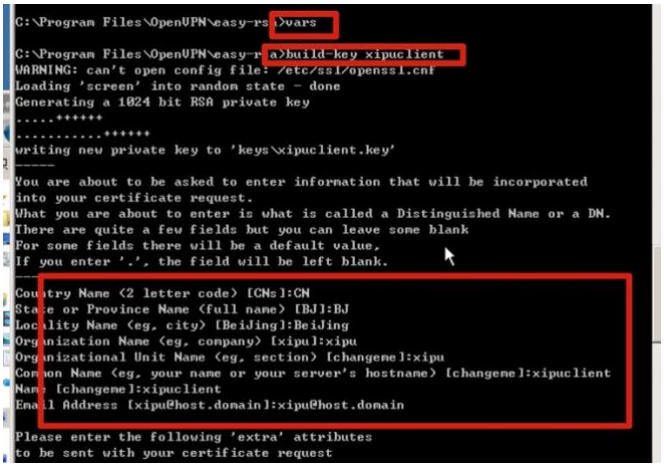

图 22

七、修改服务端配置文件参数

7.1 在服务端上，进入“C:\Program Files\OpenVPN\sample-config”目录，右键 server.ovpn 文件，选择打开，修改服务端配置参数。如图 23 所示

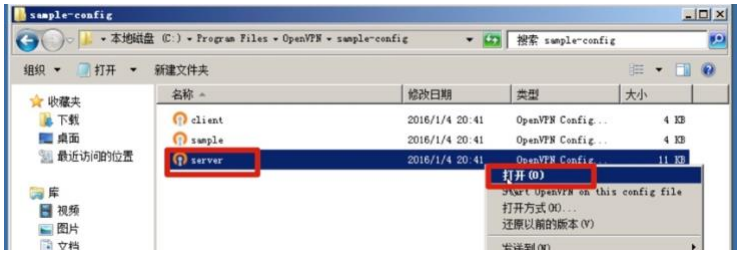

图 19

7.2 下面代码为配置文件中需要修改的地方，其他保持默认，修改完后保存即可。如图 24 所示：

cert xipuserver.crt #服务端证书

key xipuserver.key #服务端 key

dh dh1024.pem #迪菲亚证书

server 10.10.10.0 255.255.255.0 #给虚拟局域网分配的网段

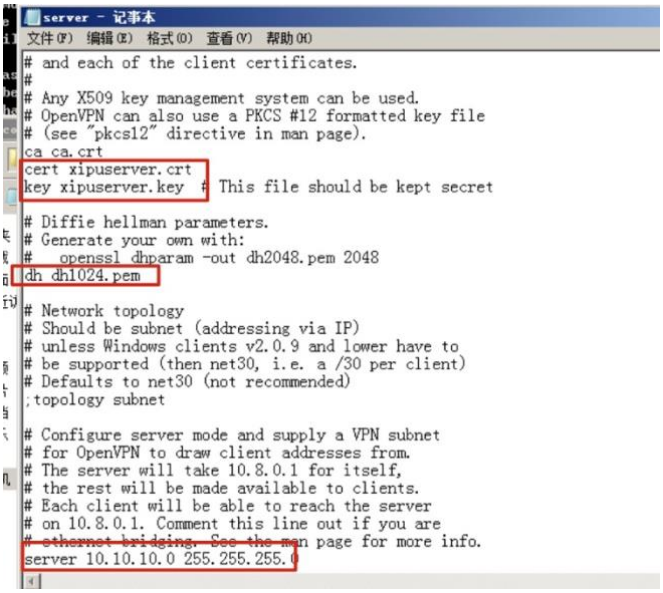

图 24

7.3 将修改后的 server.ovpn 文件复制到目录“C:\Program Files\OpenVPN\config”下，把“C:\Program Files\OpenVPN\easy-rsa\keys”目录中的“ca.crt、ca.key、dh1024.pem、xipuserver.crt、xipuserver.csr、xipuserver.key”复制到“C:\Program Files\OpenVPN\config”目录下。如图 25 所示

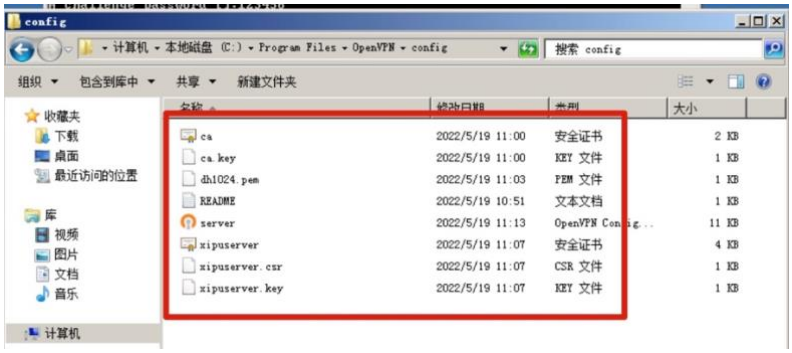

图 25

7.4 双击桌面上的 OpenVPN GUI 图标，启动软件。如图 26 所示

图 26

7.5 在任务栏，右键 openvpn 图标，选择“Connect”即可。如图 27 所示

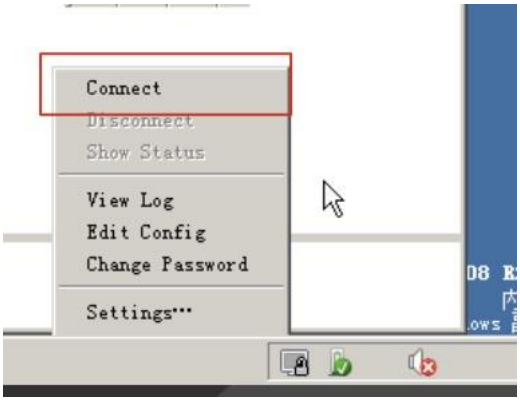

图 27

7.6 图标变绿色，表示连接成功。如图 28 所示

图 28

7.7 重新打开一个 cmd，输入命令 ipconfig，可以看到服务端 VPN 网卡 IP 地址分配为 10.10.10.1。如图 29 所示

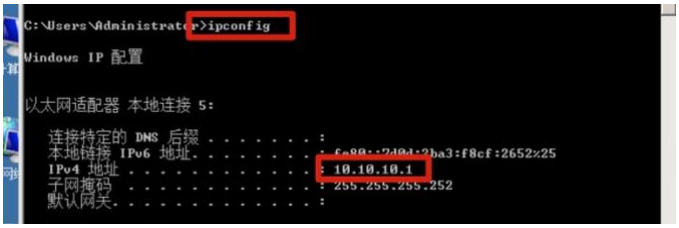

图 29

八、客户端配置文件操作

8.1 在客户端上，进入“C:\Program Files\OpenVPN\sample-config”目录，右键 client.ovpn 文件，选择打开，修改客户端配置参数。如图 30 所示

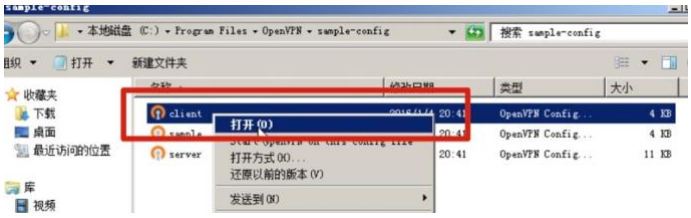

图 30

8.2 修改客户端文件，参数按照下面进行更改。保存后关闭文件。将修改后的 client.ovpn 文件复制到目录“C:\Program Files\OpenVPN\config”下。如图 31 所示：

remote 172.22.3.2 1194 #VPN 服务端的 IP 地址和端口

cert xipuclient.crt #服务端证书

key xipuclient.key #服务端 key

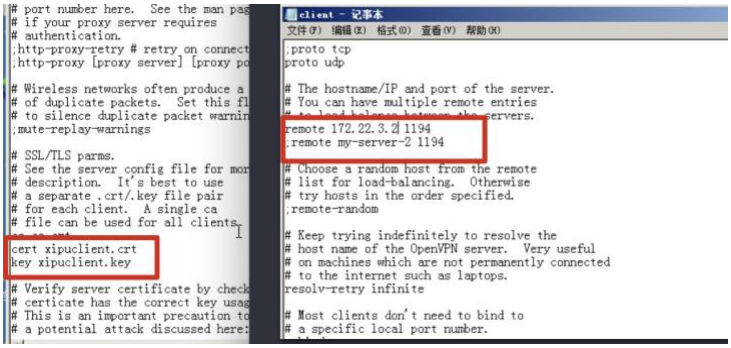

图 31

九、复制服务端配置文件到客户端机器上

9.1 在客户端上，单击“开始”->”运行”->”mstsc”。如图 32 所示

图 32

9.2 在弹出的对话框输入服务器 IP 地址 172.22.3.2、账号 administrator 和密码 Simplexue123，远程连接服务器，拷贝客户端文件。如图 33 所示

图 33

9.3 把服务端“C:\Program Files\OpenVPN\easy-rsa\keys”目录中的“ca.crt、ca.key、xipuclient.crt、xipuclient.csr、xipuclient.key”复制到客户端“C:\Program Files\OpenVPN\config”目录下。如图 34 所示

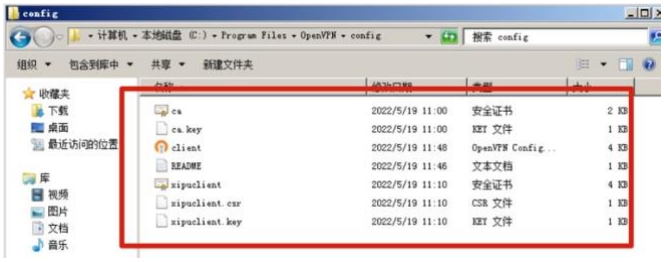

图 34

9.4 双击客户端桌面上的 OopenVPN GUI 图标，启动软件。如图 35 所示

图 35

9.5 在任务栏，右键 openvpn 图标，选择“Connect”即可。如图 36 所示

图 36

9.6 图标变绿色，表示连接成功。如图 37 所示

图 37

9.7 打开 cmd，输入命令 ipconfig，可以看到客户端 VPN 网卡 IP 地址 1 为 10.10.10.6。如图 38 所示

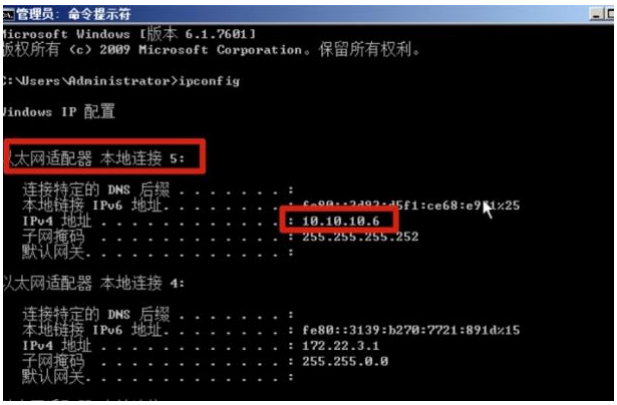

图 38

十、验证加密性

10.1 在服务端上为了使 wireshark 能够显示 VPN 网卡，需要进行下面几步的操作。

1） 单击开始-->控制面板-->硬件-->设备和打印机处的设备管理器，打开设备管理器。单击查看-->显示隐藏的设备。如图 39 所示

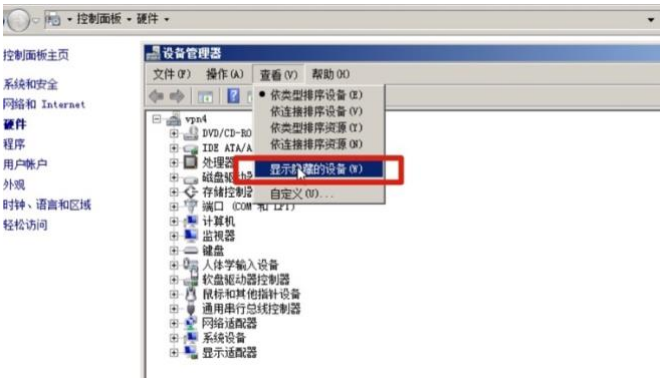

图 39

2） 右键非即插即用驱动程序下的 NetGroup Packet Filter Driver，选择属性。如图 40 所示

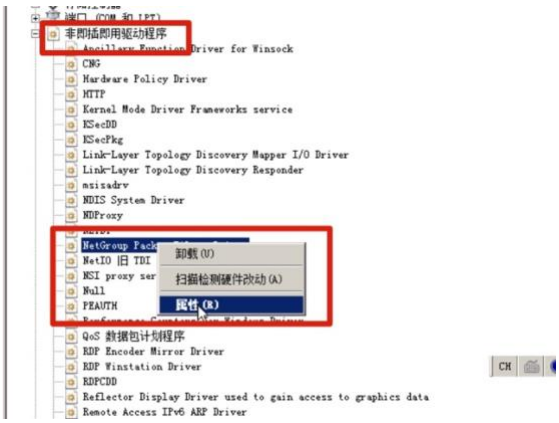

图 40

3） 切换到驱动程序选项卡，将启动类型改为系统，单击确定。如图 41 所示

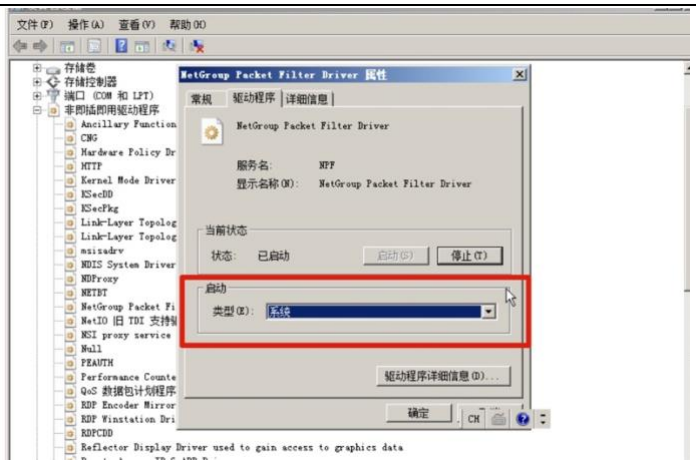

图 41

4） 打开 cmd，输入命令 net stop npf 和 net start npf，重启 npf 服务。如图 42 所示

图 42

5） 输入命令 ipconfig，可以看到 10.10.10.1 所在的网卡为本地连接 5，172.22.3.2 所在的网卡为本地连接 4。如图 43 所示

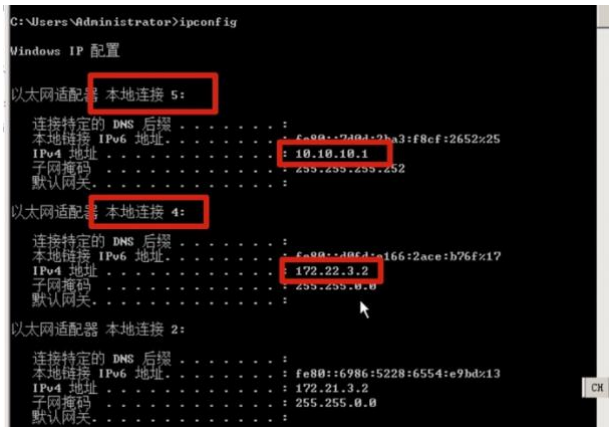

图 43

10.2 在客户端打开两个命令行窗口,分别输入命令 ping 172.22.3.2 -t 和 ping 10.10.10.1 -t。如图 44、45 所示

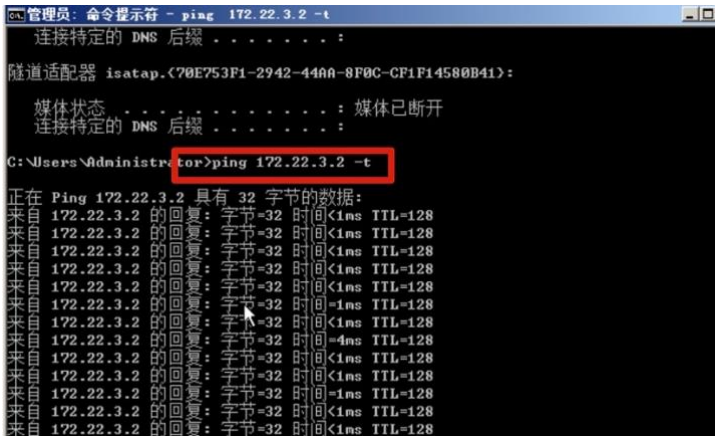

图 44

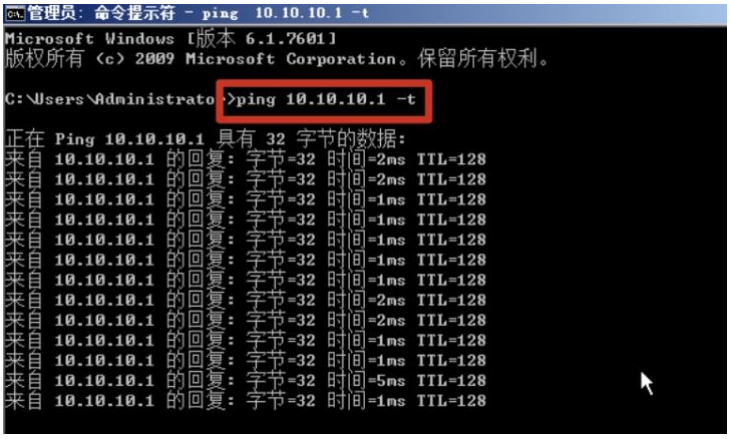

图 45

10.3 双击桌面上的 wireshark 图标，选择本地连接 4，单击开始捕获分组按钮。如图 46 所示

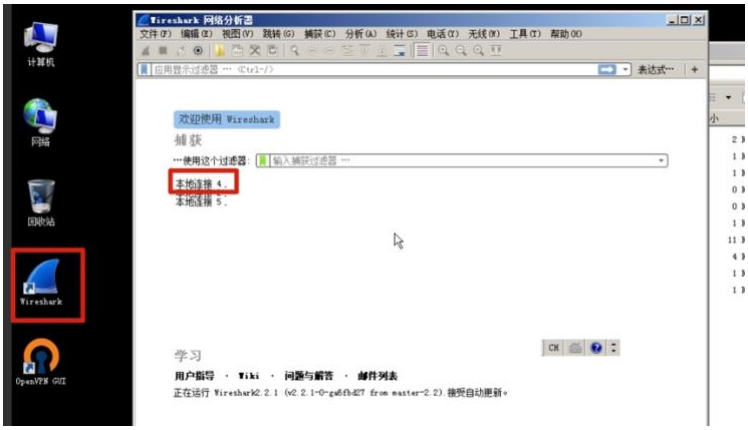

图 46

10.4 抓取 172.22.3.2 所在网卡本地连接 4 的数据包。如图 47 所示

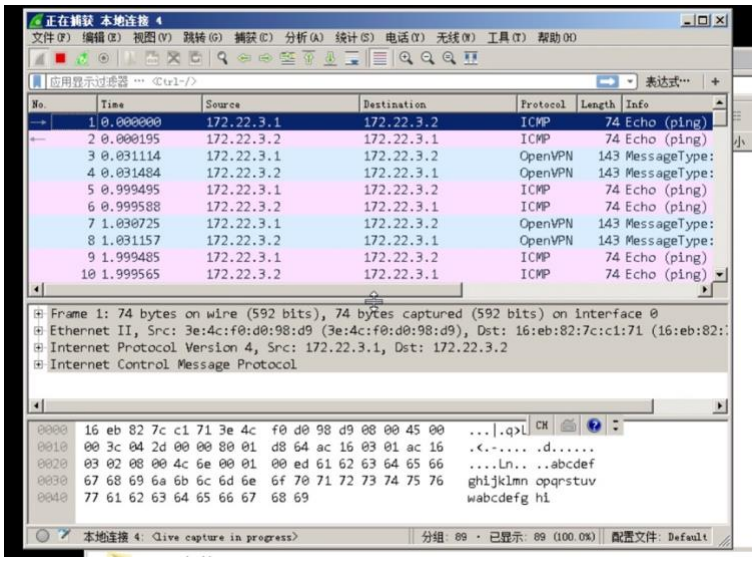

图 47

10.5 关闭并重新打开 wireshark，选择本地连接 5，单击开始捕获分组按钮。如图 48 所示

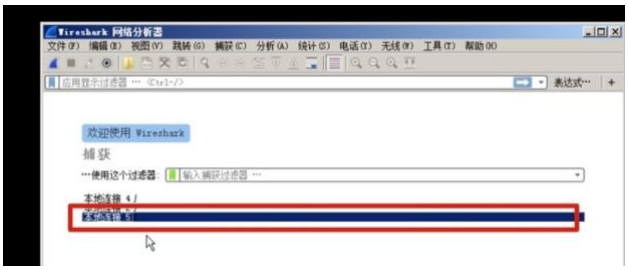

图 48

10.6 抓取 10.10.10.1 所在网卡本地连接 5 的数据包。如图 49 所示

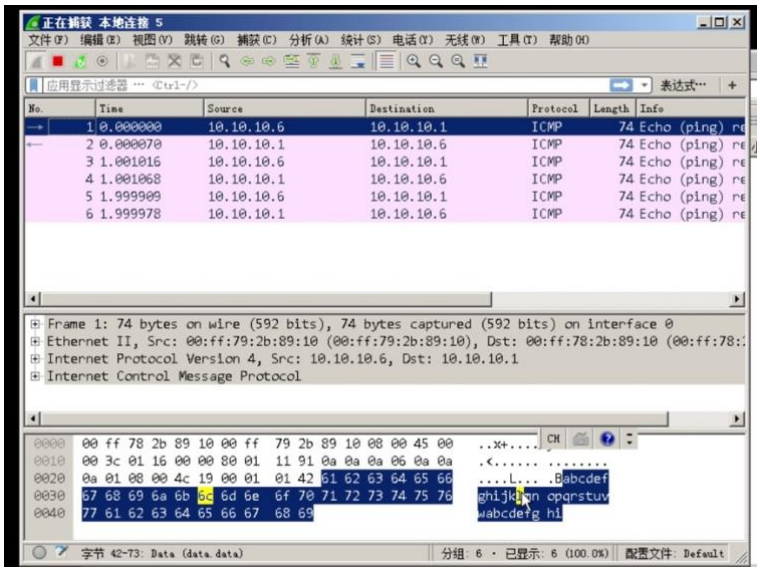

图 49