哈尔滨工业大学

《网络安全》

实验报告

计算机科学与技术学院

计算机系网络教研室制

|  |  |
| --- | --- |
| 课程名称： | 网络安全 |
| 实验名称： | Linux下搭建OpenVPN服务器 |
| 指导教师： | 王彦 |
| 学生姓名： | 符兴 |
| 组 号： |  |
| 实验日期： | 2023.04.07 |
| 实验地点： | 格物213 |
| 实验成绩： |  |

实验报告撰写要求

实验操作是教学过程中理论联系实际的重要环节，而实验报告的撰写又是知识系统化的吸收和升华过程，因此，实验报告应该体现完整性、规范性、正确性、有效性。现将实验报告撰写的有关内容说明如下：

1、 实验报告模板为电子版。

2、 下载统一的实验报告模板，学生自行完成撰写和打印。报告的首页包含本次实验的一般信息：

*  组 号：例如：2-5 表示第二班第5组。
*  实验日期：例如：05-10-06 表示本次实验日期。(年-月-日)……
*  实验编号：例如：No.1 表示第一个实验。
*  实验时间：例如：2学时 表示本次实验所用的时间。

实验报告正文部分，从六个方面（目的、内容、步骤等）反映本次实验的要点、要求以及完成过程等情况。模板已为实验报告正文设定统一格式，学生只需在相应项内填充即可。续页不再需要包含首页中的实验一般信息。

3、 实验报告正文部分具体要求如下：

一、实验目的

本次实验所涉及并要求掌握的知识点。

二、实验环境

实验所使用的设备名称及规格，网络管理工具简介、版本等。

三、实验内容与实验要求

实验内容、原理分析及具体实验要求。

四、实验过程与分析

根据具体实验，记录、整理相应命令、运行结果等，包括截图和文字说明。

详细记录在实验过程中发生的故障和问题，并进行故障分析，说明故障排除的过程及方法。

五、实验结果总结

对实验结果进行分析，完成思考题目，总结实验的心得体会，并提出实验的改进意见。

六、附录

一、实验目的

1）安装OpenVPN

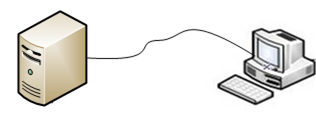
2）配置OpenVPN

  3）客户端配置

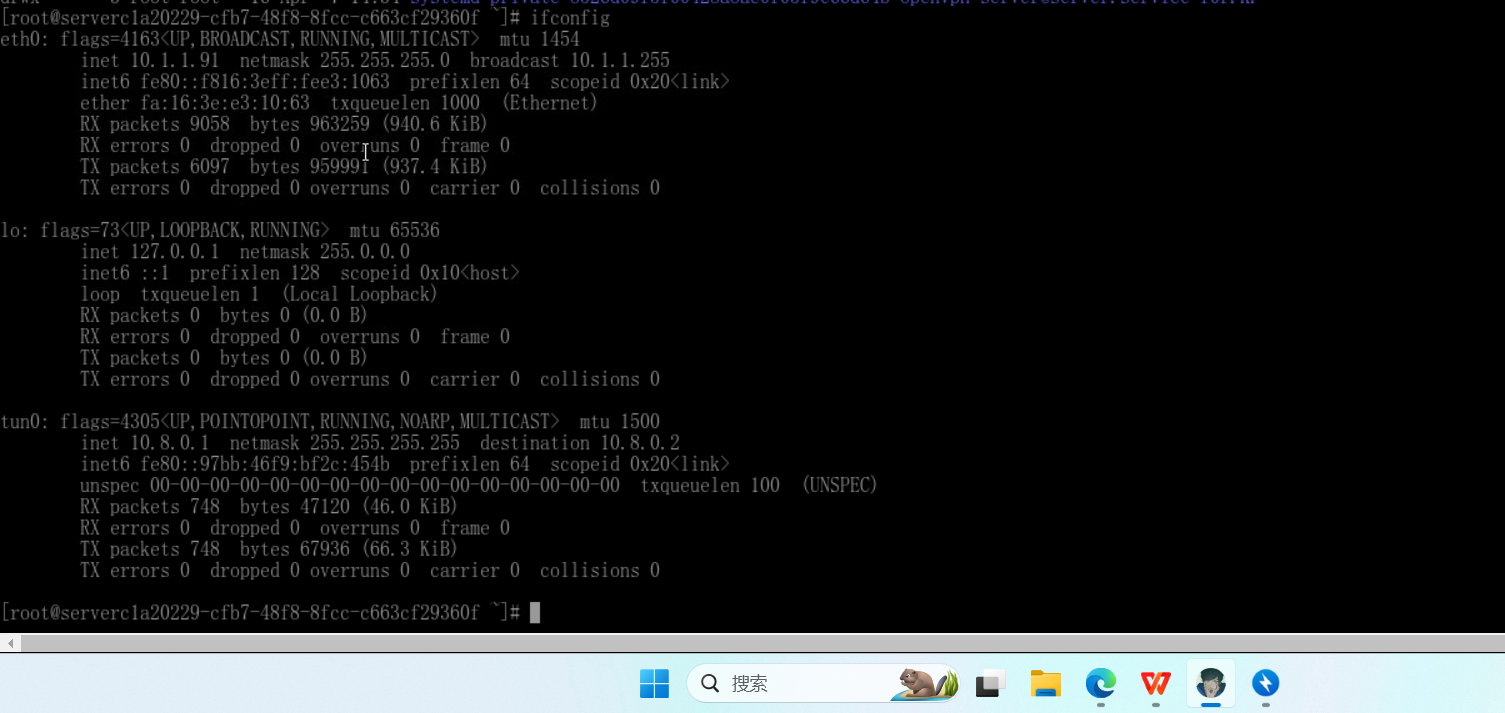
二、实验环境

操作系统：服务端：Centos7 客户端：windows 7

网络拓扑见下图：



IP地址为：10.1.1.91



所用软件：openvpn, easy-rsa,openvpn-gui,tap-windows

三、实验内容与实验要求

OpenVPN是一个功能齐全的SSL VPN，它使用行业标准的SSL/TLS协议实现了OSI模型第2层(数据链路层)或第3层(网络层)的安全网络扩展。OpenVPN支持基于证书、智能卡以及用户名/密码等多种形式的灵活的客户端认证方法。本实验介绍在linux下搭建OpenVPN 服务器。

实验所属系列：虚拟专用网VPN

实验对象： 信息安全从业人员

相关课程及专业：计算机网络基础，Linux基础

实验时数（学分）：2学时

实验类别：实践类

本实验要求实验者具备如下的相关知识

OpenVPN是一个功能齐全的SSL VPN，它使用行业标准的SSL/TLS协议实现了OSI模型第2层(数据链路层)或第3层(网络层)的安全网络扩展。OpenVPN支持基于证书、智能卡以及用户名/密码等多种形式的灵活的客户端认证方法，并可以通过应用于VPN虚拟接口的防火墙规则为指定用户或用户组设置访问控制策略。OpenVPN不是一个Web应用程序代理，也不需要通过Web浏览器来进行操作。

OpenVPN2.0 采用可扩展升级的客户端/服务器模式，从而在OpenVPN 1.x的基础上大幅提高了扩展能力。OpenVPN 2.0允许多个客户端连接到一个单一的OpenVPN服务器进程，并且只占用一个TCP或UDP端口。

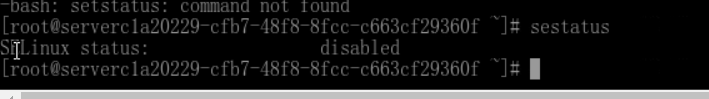
本实验将引导你一步一步地完成OpenVPN 2.x 客户端和服务器的相关配置。

四、实验过程与分析

1. 基本配置

1、关闭系统的SELinux

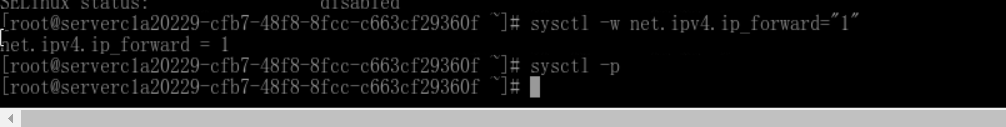
由于SELinux的审计规则十分严格，但是这里并不会涉及到SELinux配置，所以建议关闭SELinux。使用 sestatus 查看selinux状态，如果非 “disabled”状态，使用 setenforce 0设置selinux为permissive模式。



2、开启IP转发。在sysctl中开启IP转发。

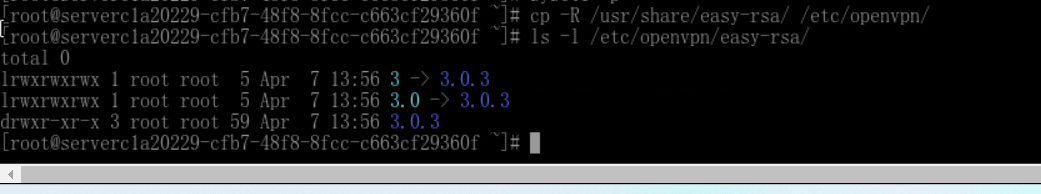
sysctl -w net.ipv4.ip\_forward="1"

sysctl -p //生效



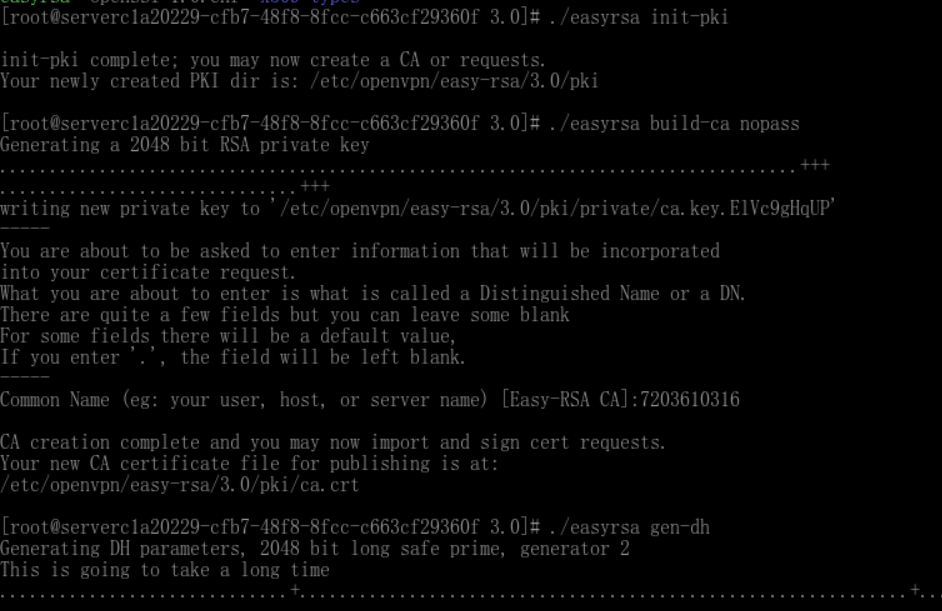
1. 生成证书

1、使用easy-rsa生成证书。将相关文件复制到OpenVPN的配置目录：

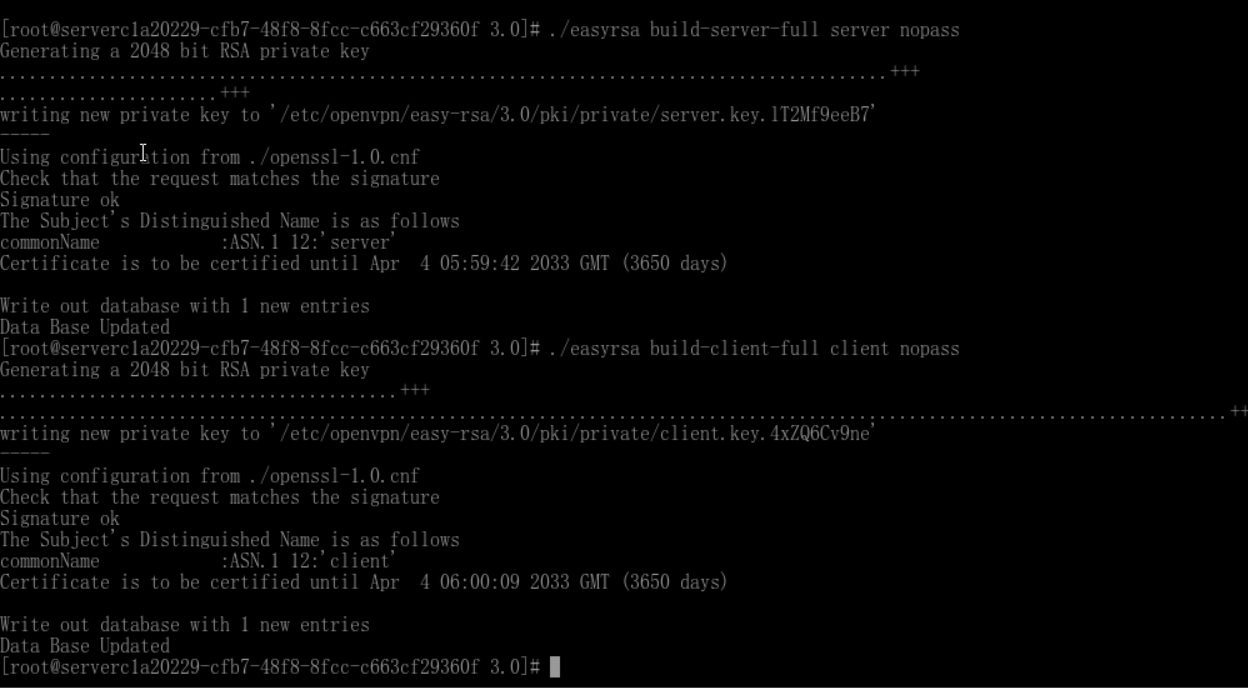


现在有关的文件都在/etc/openvpn/easy-rsa/3.0/这个目录中

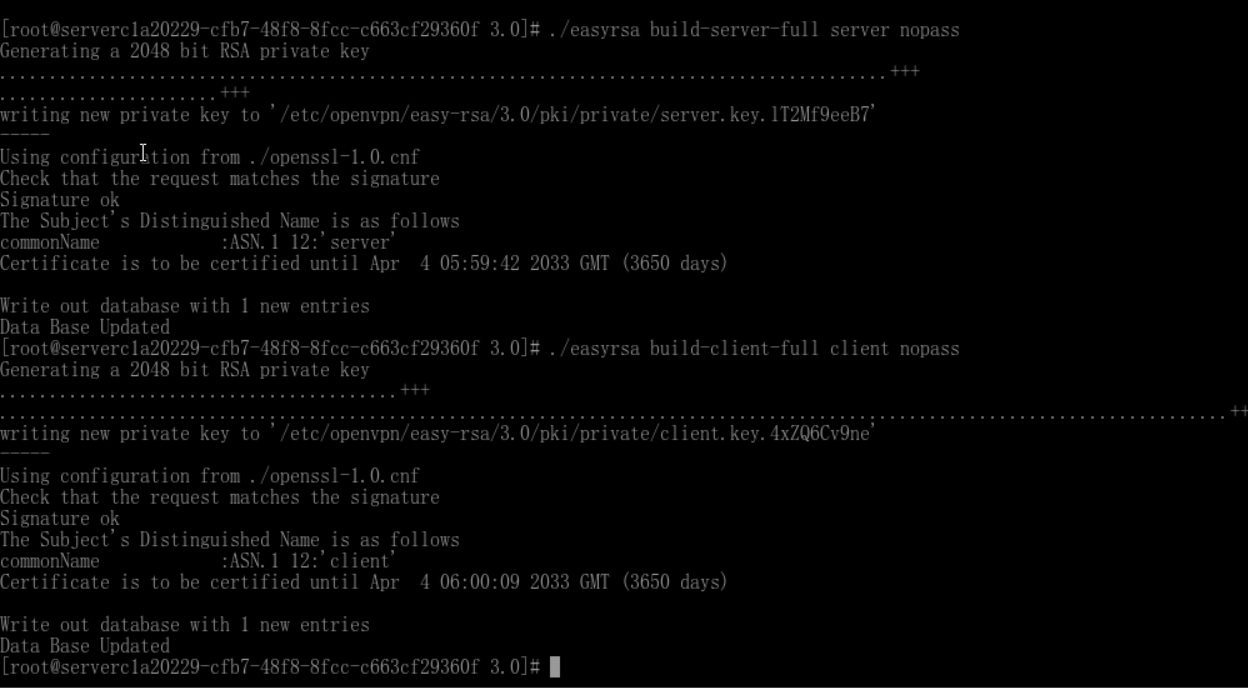
2、生成根证书



3、生成服务端证书

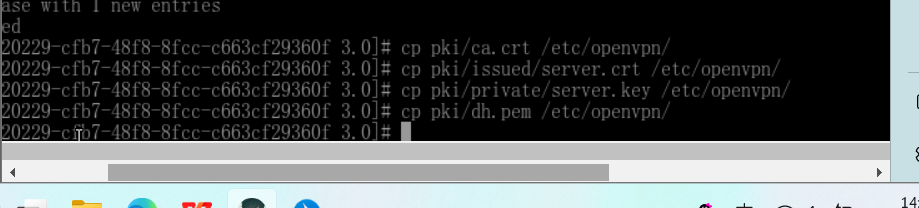


1. 生成客户端证书

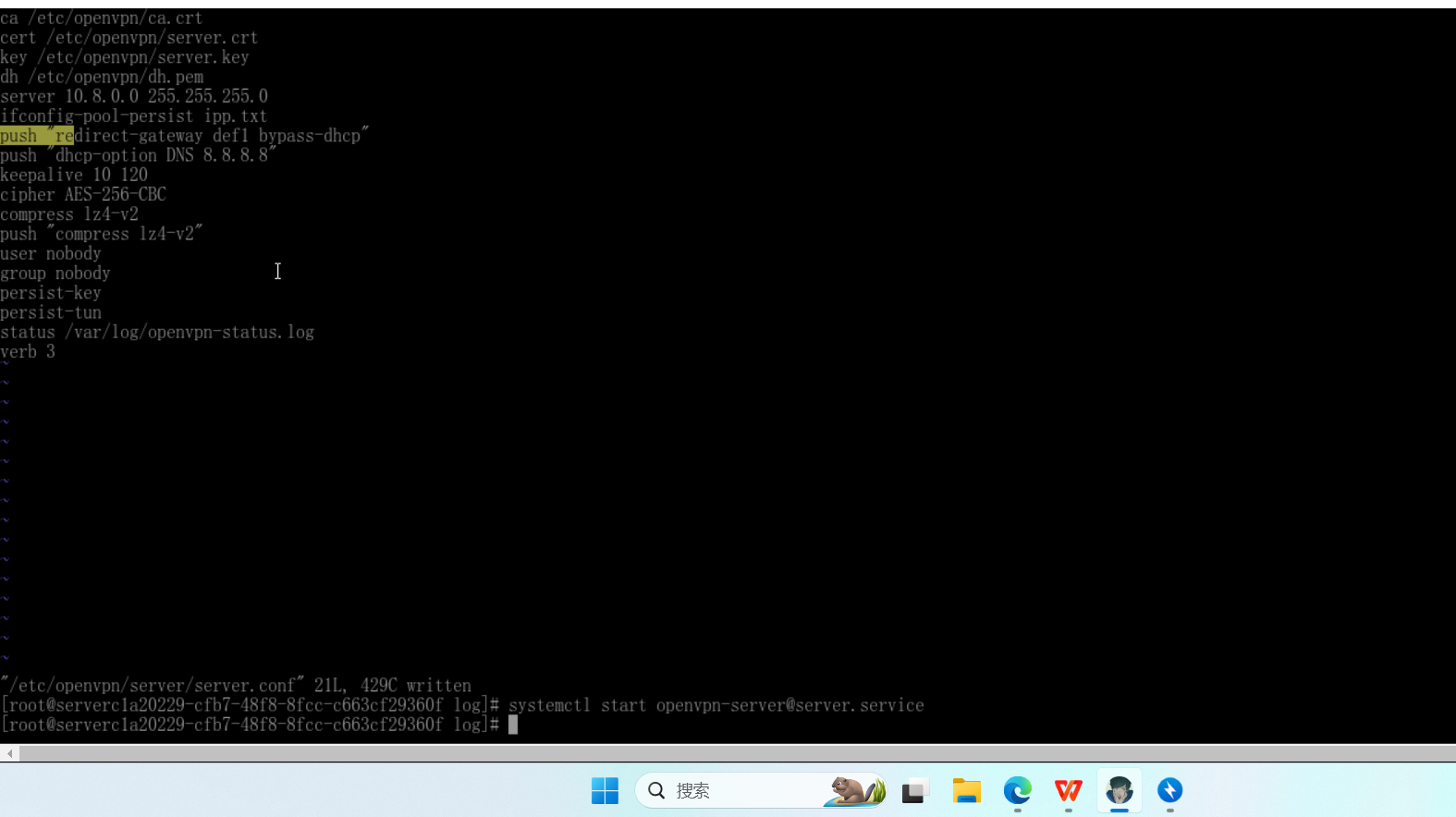


1. 配置OpenVPN服务端

1、复制服务端所需证书文件到OpenVPN配置目录（可自定义此目录）



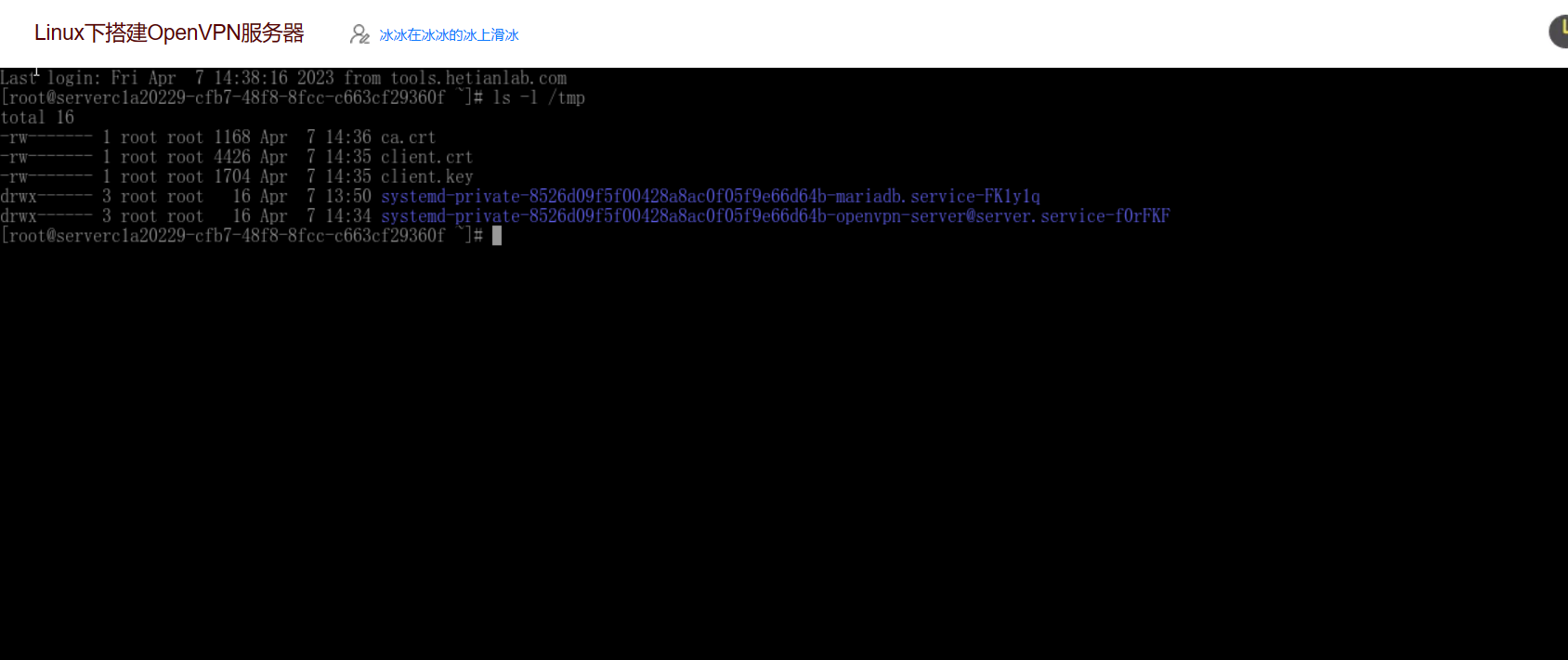
2、server.conf配置。从示例配置文件复制一份配置文件到/etc/openvpn/server/，使用vim对 /etc/openvpn/server/server.conf 进行修改修改后内容如下：



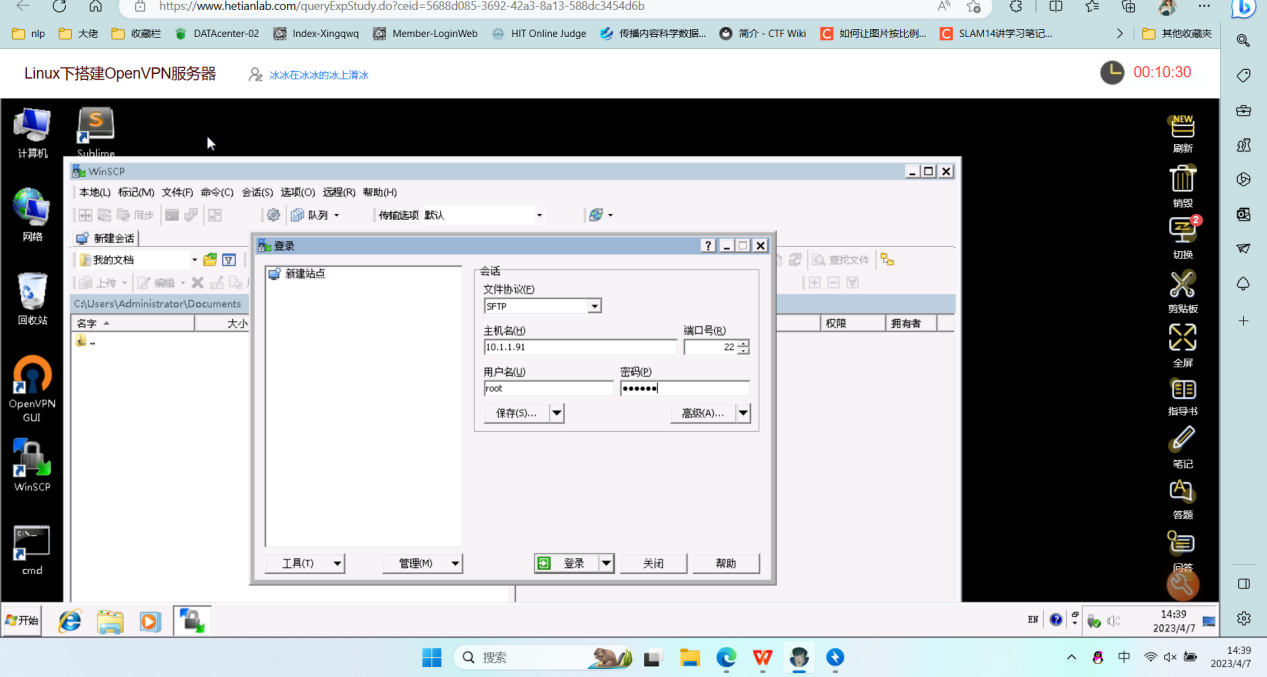
3、启动OpenVPN服务

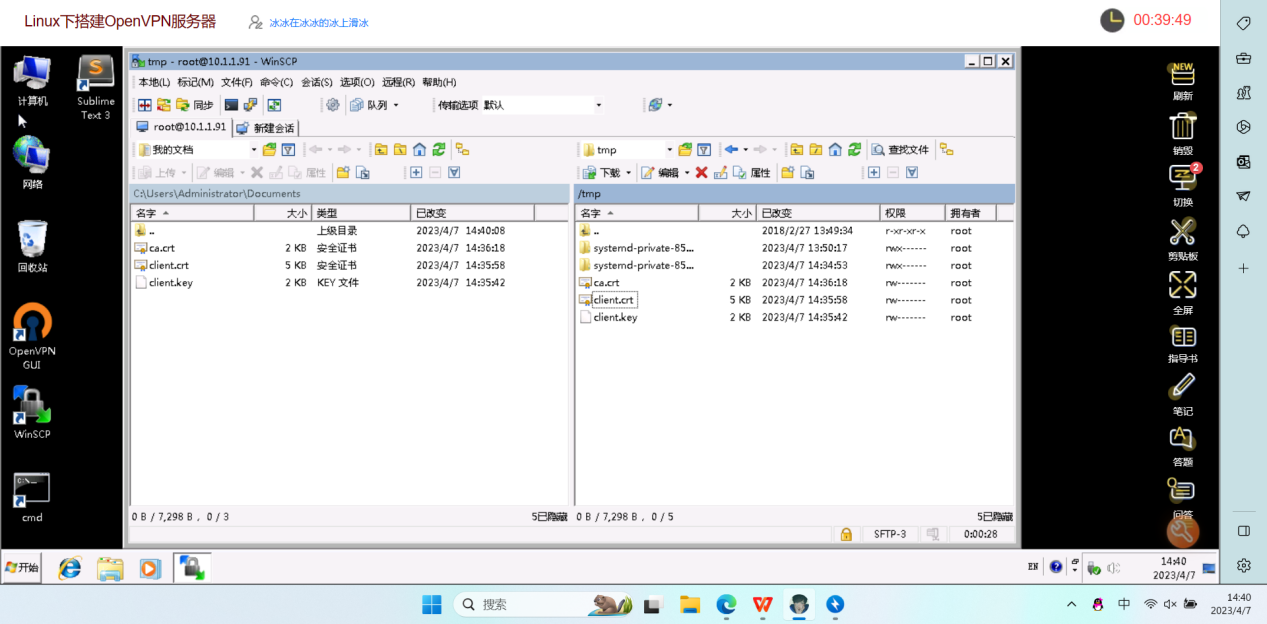
4. 客户端配置

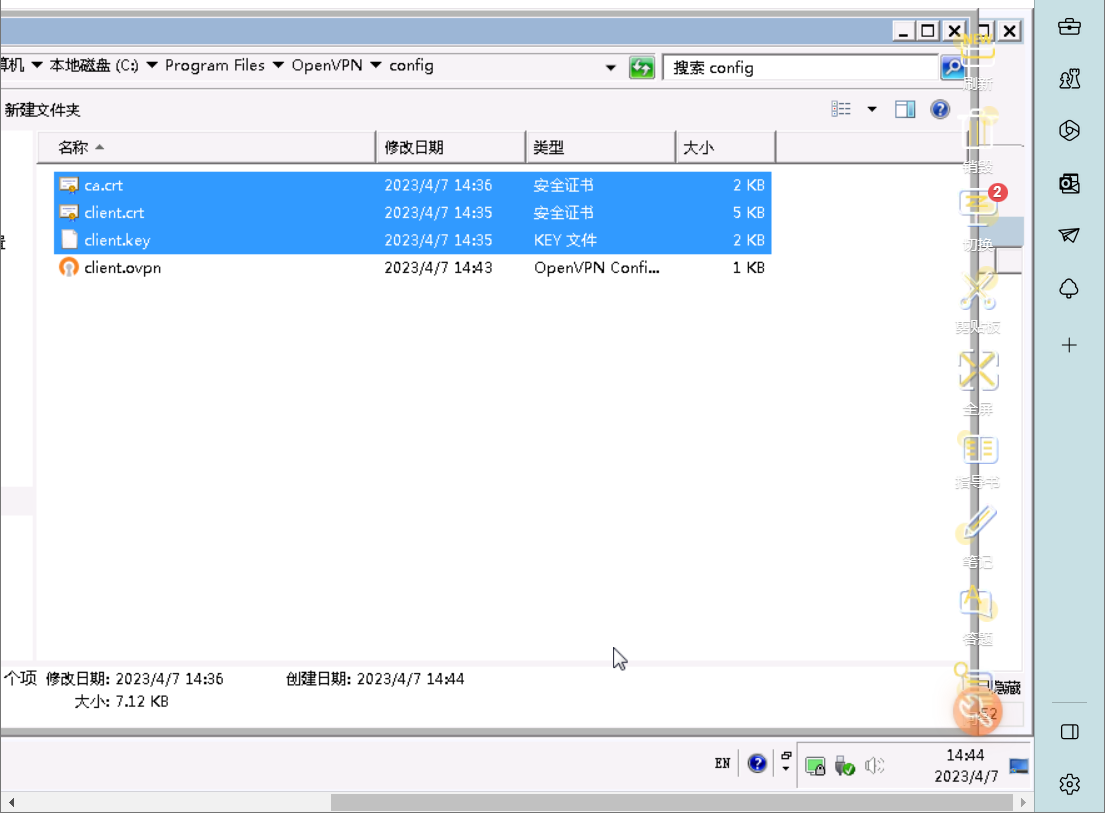
1、复制客户端所需证书文件到 “/tmp” 目录。



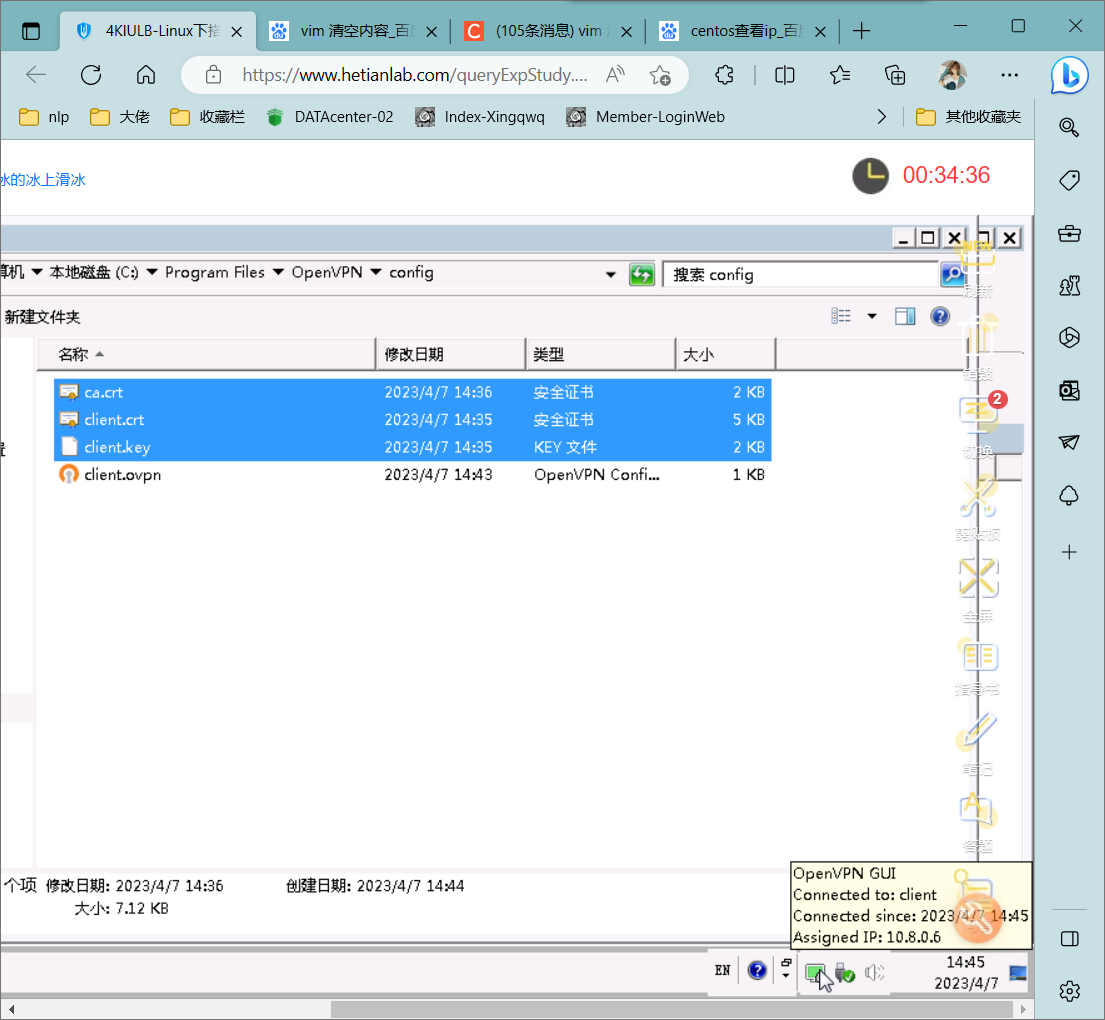
2、客户端配置。切换实验机到客户端，首先使用winscp下载客户端证书文件







3、连接测试。双击桌面上的 openvpn-gui ，打开后会在右下角的任务栏有显示。在右下角的图标上右键选择 connect会看到连接过程。稍等片刻，即可连接成功，连接成功后，图标会呈绿色，鼠标放上去会显示通过openvpn获取到的ip



五、实验结果总结

1. 了解了使用OpenVpn构建VPN服务器的过程，包括生成根证书、服务器证书、客户端证书以及服务端参数的设置。

2. 了解了使用OpenVPN连接VPN服务器的过程。

六、思考题

1、如何修改openvpn服务器配置文件，推送指定的路由到客户端？

通过设定config文件中的 push “route 指定路由”。

2、多用户可以使用同一个证书连接openvpn server吗？如果能，该怎么配置？

多用户可以使用同一个证书连接openvpn server。使用duplicate-cn 参数, 即可允许两个具有相同公用名的连接，即一个证书可以由多个连接/用户使用.