陕西科技大学

《计算机网络安全》实验报告

实验四：网络安全通信

学　　生：

学　　院：电子信息与人工智能学院

专　　业：网络工程

指导教师：张楠

2022 年 6 月 2 日

实验四 网络安全通信

班级：_____ _____ _____

实验预习报告

一、实验目的

1、了解传统 IP 通信网络中存在的不安全因素

2、了解 VPN 技术的思想，知道常用 VPN 的工作方式

3、搭建一个局域网内的 VPN 网络，验证其安全性

二、实验要求

使用相关的命令和工具完成网络安全通信。了解常用的安全通信的协议，掌握安全通信的实现方法。

三、实验原理

1、传统 IP 网存在的不足

传统的 IP 网络通信是明文传输，缺乏终端到终端的加密保护，容易受到数据泄露、窃听、篡改和拒绝服务攻击等安全威胁。

2、VPN 技术的思想

技术的思想是通过在公共网络上创建一个加密的、安全的通信隧道，使得用户可以在不安全的公共网络上建立起一种类似于私有网络的安全连接。

3、VPN 的工作方式

VPN 的工作方式大致可以分为以下几个步骤：

认证和身份验证：在建立 VPN 连接之前，用户需要进行身份验证，以确保只有授权的用户可以访问 VPN 网络。这通常涉及输入用户名、密码或其他身份凭证进行身份验证。

加密通信隧道的建立：一旦用户通过身份验证，VPN 客户端和 VPN 服务器之间开始建立加密的通信隧道。在此过程中，使用加密协议来加密用户的数据包，以保证数据在公共网络上的传输安全。

数据封装和解封：当用户发送数据时，VPN 客户端将数据封装在加密的数据包中，包括添加加密头部和尾部信息。这样的封装使得数据在公共网络上是加密的，从而提供了数据的机密性。

数据传输和路由：封装后的数据包通过公共网络传输到 VPN 服务器。在传输过程中，数据包可能经过多个网络节点和路由器。为了保证数据包的安全和完整性，VPN 使用加密和身份验证来保护数据免受窃听、篡改和伪装攻击。

数据解封和解密：一旦数据包到达 VPN 服务器，服务器将对其进行解封和解密操作，还原出原始的数据内容。服务器根据目标地址和路由策略，将解密后的数据包发送到目标网络或目标设备。

访问内部网络资源：一旦解封后的数据包到达目标网络，用户可以通过 VPN 连接安全地访问内部网络资源，如文件共享、打印机、数据库等。用户的数据在内部网络和用户设备之间通过加密的通信隧道进行传输，保证数据的安全性和私密性。

连接终止：当用户完成对内部网络资源的访问或断开 VPN 连接时，通信隧道将关闭，断开用户和 VPN 服务器之间的连接。

四、实验预习内容

1、常见的 VPN 技术

IPsec 是一种广泛采用的 VPN 协议，它通过在网络层提供安全性和认证服务。IPsec 可以用于建立站点到站点（Site-to-Site）VPN 连接，也可以用于远程访问（Remote Access）VPN 连接。

SSL/TLS VPN 基于 SSL/TLS 协议，利用传输层加密技术建立安全的 VPN 连接。它通常以 Web 浏览器为客户端，通过 HTTPS 协议实现远程访问和加密通信。

OpenVPN 是一种基于 SSL/TLS 的开源 VPN 解决方案。它具有跨平台兼容性、灵活性和强大的安全特性。OpenVPN 支持多种身份验证方法和加密算法，可用于远程访问和站点到站点 VPN 连接。

L2TP/IPsec 是一种组合协议，结合了 L2TP 和 IPsec 技术。L2TP 提供了隧道化通信，而 IPsec 提供了数据加密和身份验证功能。它广泛应用于远程访问 VPN 和移动设备的 VPN 连接。

PPTP 是一种早期的 VPN 协议，它在数据链路层创建虚拟通信隧道。PPTP 具有较低的资源消耗和简单的配置，适用于远程访问 VPN 连接，但安全性较低，已逐渐被其他更安全的协议取代。

2、SoftEther VPN

SoftEther 是一种开源的多协议 VPN 解决方案，它支持多种 VPN 协议，包括 SoftEther VPN、OpenVPN、L2TP/IPsec 和 SSTP。SoftEther 提供了跨平台的支持，在实验中，可以使用 SoftEther 组建 VPN 网络，并验证网络的安全性。

3、Vmware 虚拟机平台

Vmware workstation 提供一个高度虚拟化的虚拟机平台，可以在其中运行多个 Windows 系统，同时，还支持在宿主机安装虚拟网卡，实现虚拟机到宿主机的通信。

实验中，可以使用虚拟机和宿主机之间进行通信，通过数据抓包测试其安全性，分析其数据包特征。

实验四 网络安全通信

班级：_____ _____ _____

实验报告

一、实验目的

1、了解传统 IP 通信网络中存在的不安全因素

2、了解 VPN 技术的思想，知道常用 VPN 的工作方式

3、搭建一个局域网内的 VPN 网络，验证其安全性

二、实验要求

使用相关的命令和工具完成网络安全通信。了解常用的安全通信的协议，掌握安全通信的实现方法。

三、实验原理

1、传统 IP 网存在的不足

传统的 IP 网络通信是明文传输，缺乏终端到终端的加密保护，容易受到数据泄露、窃听、篡改和拒绝服务攻击等安全威胁。

2、VPN 技术的思想

技术的思想是通过在公共网络上创建一个加密的、安全的通信隧道，使得用户可以在不安全的公共网络上建立起一种类似于私有网络的安全连接。

3、VPN 的工作方式

VPN 的工作方式大致可以分为以下几个步骤：

认证和身份验证：在建立 VPN 连接之前，用户需要进行身份验证，以确保只有授权的用户可以访问 VPN 网络。这通常涉及输入用户名、密码或其他身份凭证进行身份验证。

加密通信隧道的建立：一旦用户通过身份验证，VPN 客户端和 VPN 服务器之间开始建立加密的通信隧道。在此过程中，使用加密协议来加密用户的数据包，以保证数据在公共网络上的传输安全。

数据封装和解封：当用户发送数据时，VPN 客户端将数据封装在加密的数据包中，包括添加加密头部和尾部信息。这样的封装使得数据在公共网络上是加密的，从而提供了数据的机密性。

数据传输和路由：封装后的数据包通过公共网络传输到 VPN 服务器。在传输过程中，数据包可能经过多个网络节点和路由器。为了保证数据包的安全和完整性，VPN 使用加密和身份验证来保护数据免受窃听、篡改和伪装攻击。

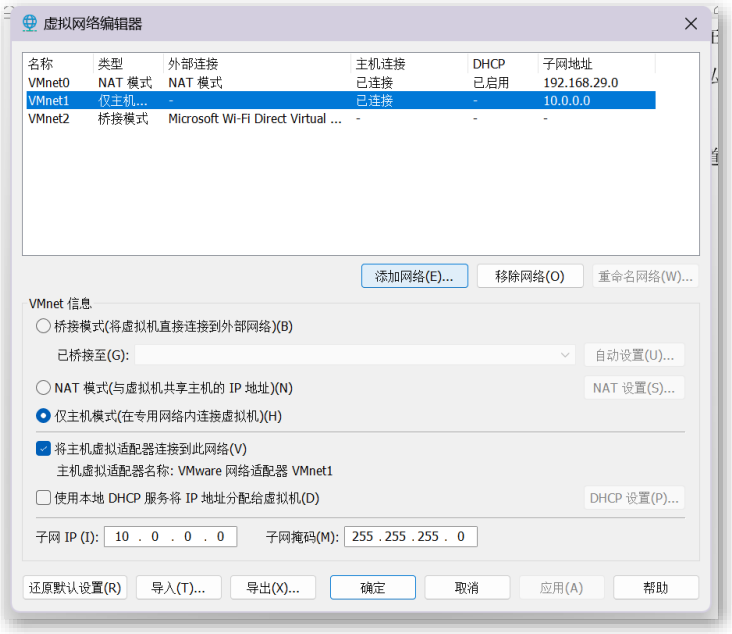
数据解封和解密：一旦数据包到达 VPN 服务器，服务器将对其进行解封和解密操作，还原出原始的数据内容。服务器根据目标地址和路由策略，将解密后的数据包发送到目标网络或目标设备。

访问内部网络资源：一旦解封后的数据包到达目标网络，用户可以通过 VPN 连接安全地访问内部网络资源，如文件共享、打印机、数据库等。用户的数据在内部网络和用户设备之间通过加密的通信隧道进行传输，保证数据的安全性和私密性。

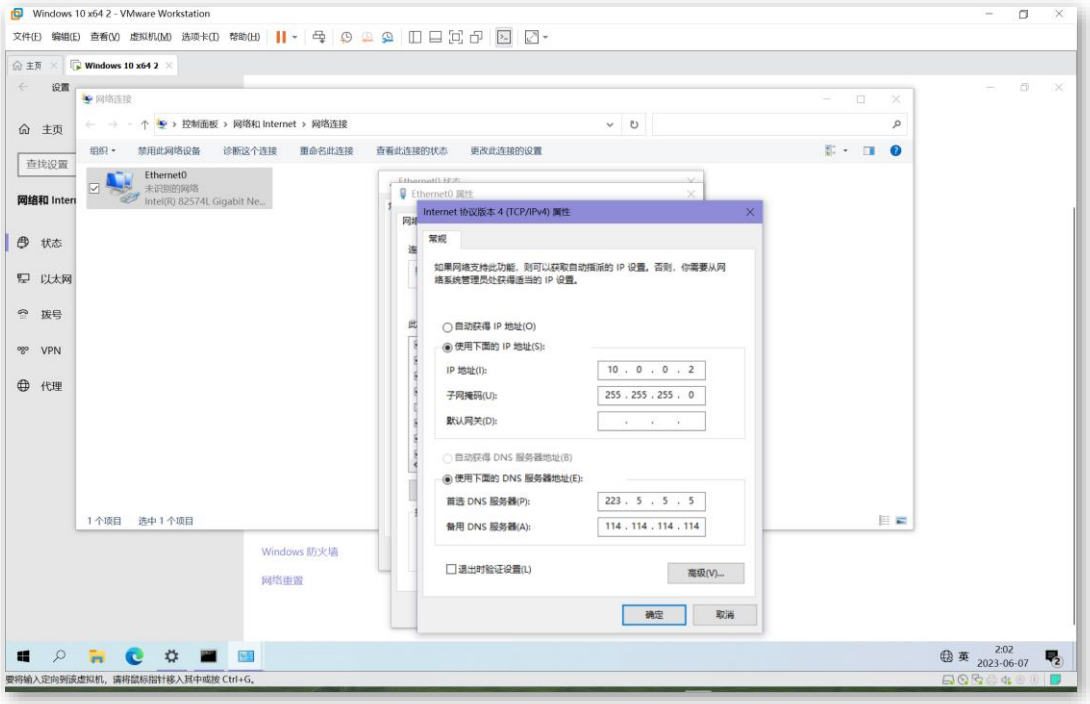
连接终止：当用户完成对内部网络资源的访问或断开 VPN 连接时，通信隧道将关闭，断开用户和 VPN 服务器之间的连接。

四、实验内容

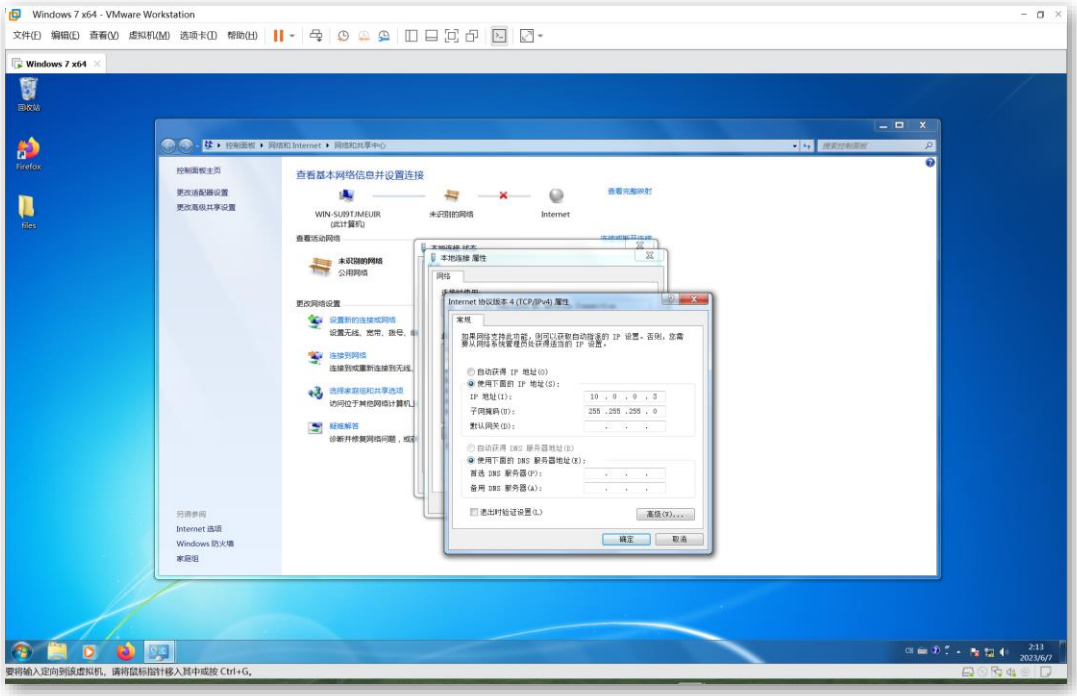
1、使用 VMware 虚拟网卡编辑器在本机新建虚拟网卡，添加网卡，设为“仅主机”模式，关闭 DHCP 服务器，设置网络地址为 10.0.0.0/24



2、打开虚拟机 Windows10，将虚拟网卡 Vmnet1 绑定到虚拟机上，在其网络共享中心中设置 IP 地址为 10.0.0.2/24，无 DNS 和默认网关。

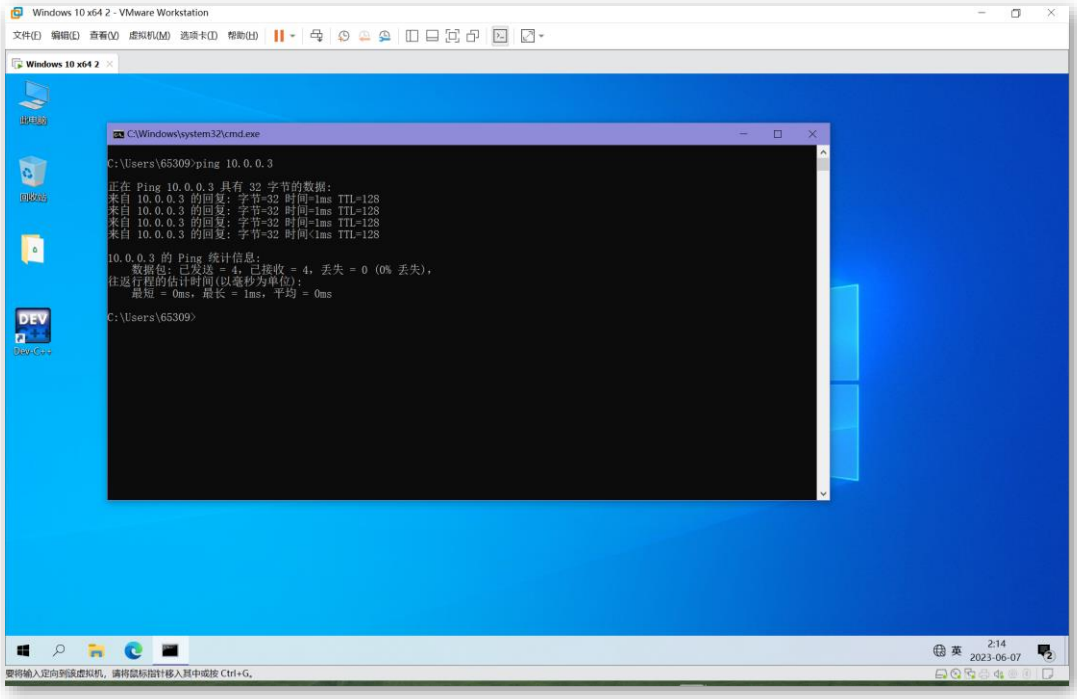


打开另一台虚拟机 Windows7，将虚拟网卡 Vmnet1 绑定到虚拟机上，网络共享中心设置 IP 地址为 10.0.0.3/24，无 DNS 和网关。

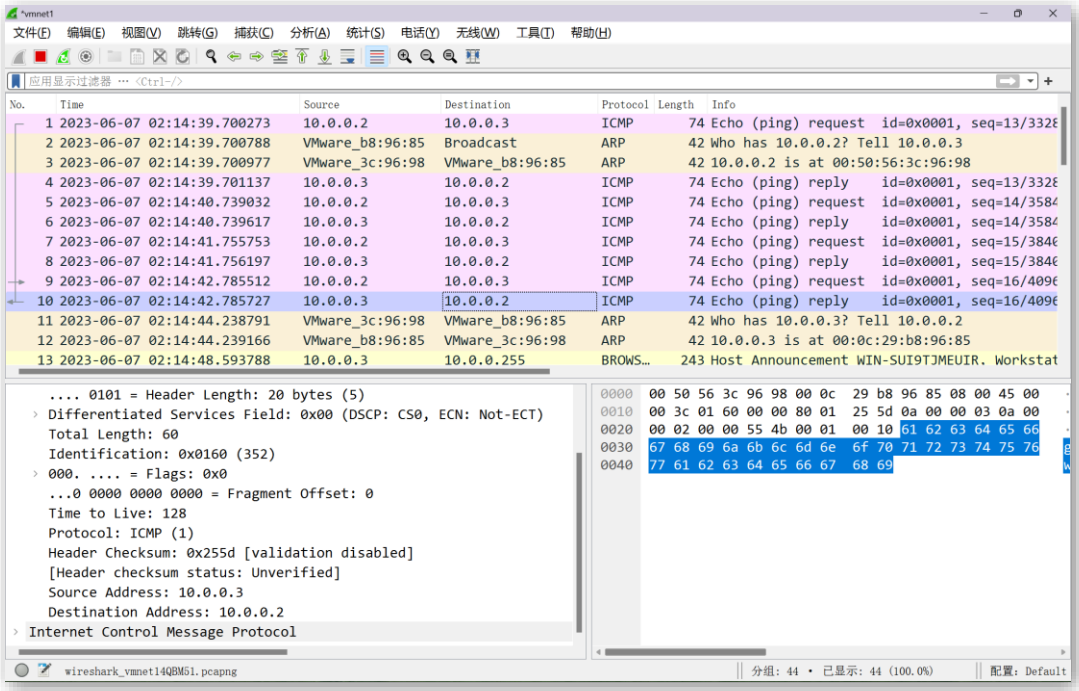


3、在本机上打开 wireshark 进行抓包，使用两台虚拟机互相 ping，在主机上进

行抓包



虚拟机 Windows10 成功 ping 通 Windows7，查看主机上的 wireshark 抓包：

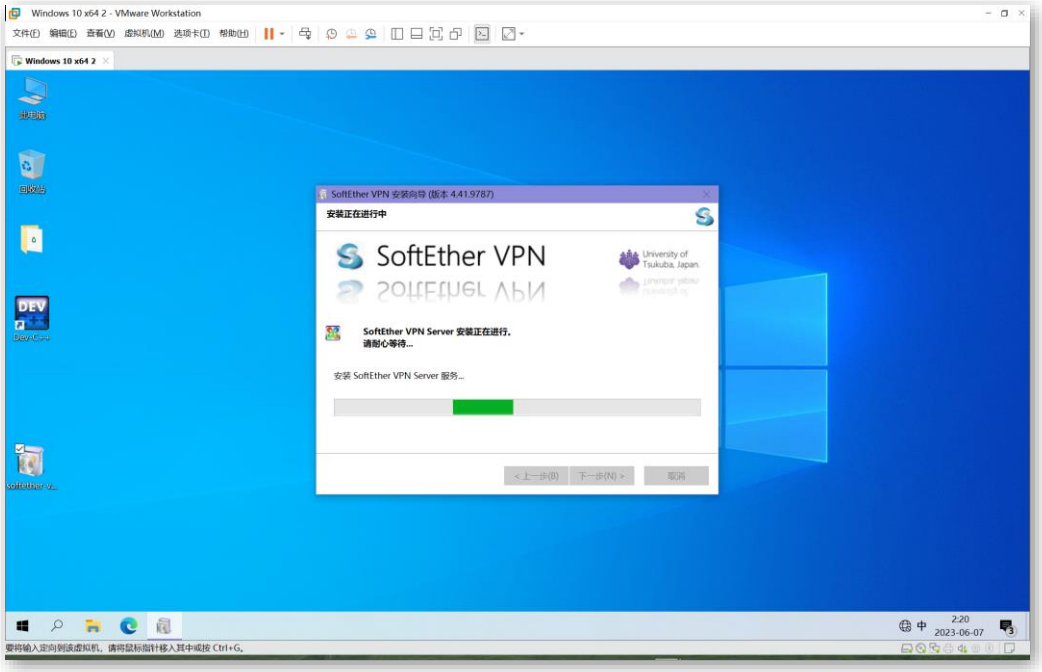


在 wireshark 当中抓取到了封装在 IP 数据分组当中的明文 ICMP 报文，这个时候，两台虚拟机进行通信，而主机就相当于起到了一个中间人进行监听的作用，此时，两台主机的通信内容一览无余。

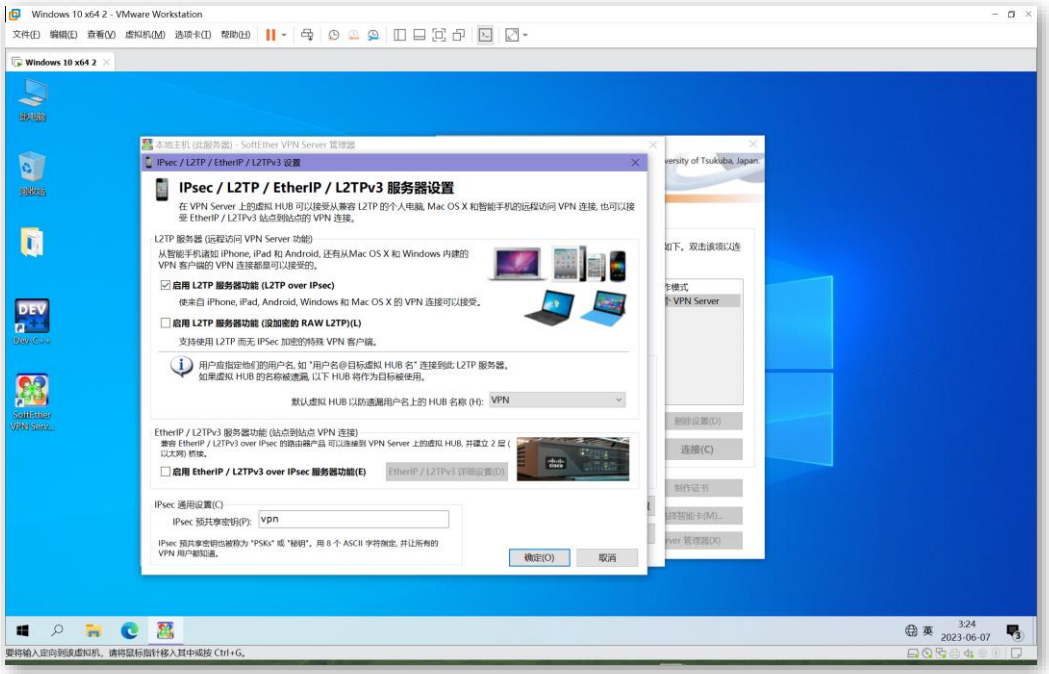
由此，可见 IP 网本身是不安全的，它的数据包在网络中采取明文发送，容易被监听、泄露数据。

4、在虚拟机 Windows10 上面设置 VPN 服务器，提供 VPN 服务

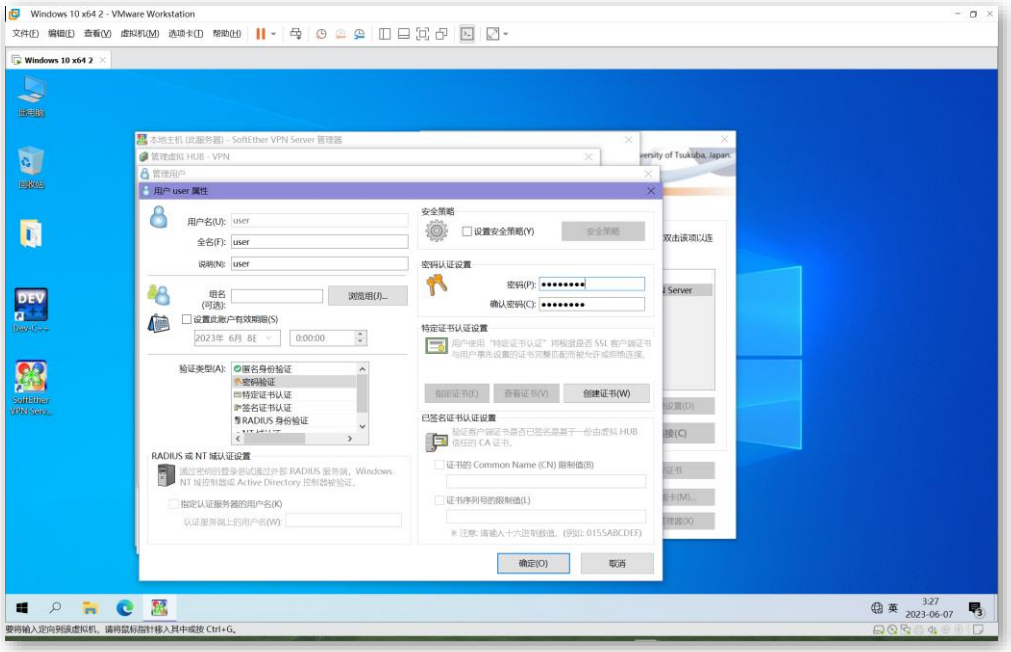
在 Windows10 虚拟机上面安装 SoftEther VPN 服务器程序



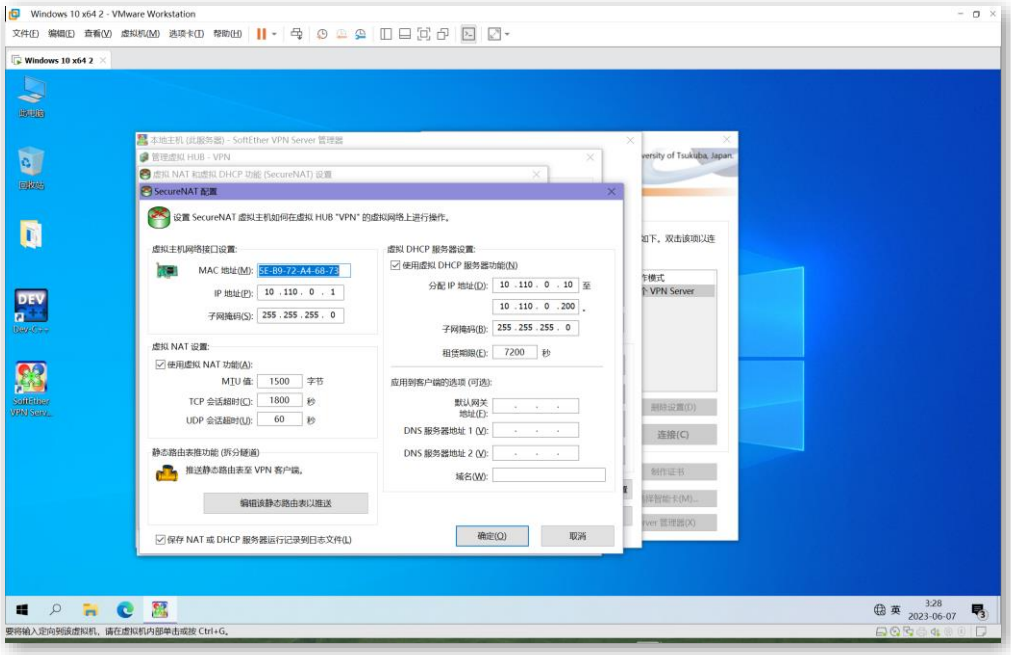
配置 VPN 服务



允许 L2TP over IPSec，预共享密钥设为 VPN。

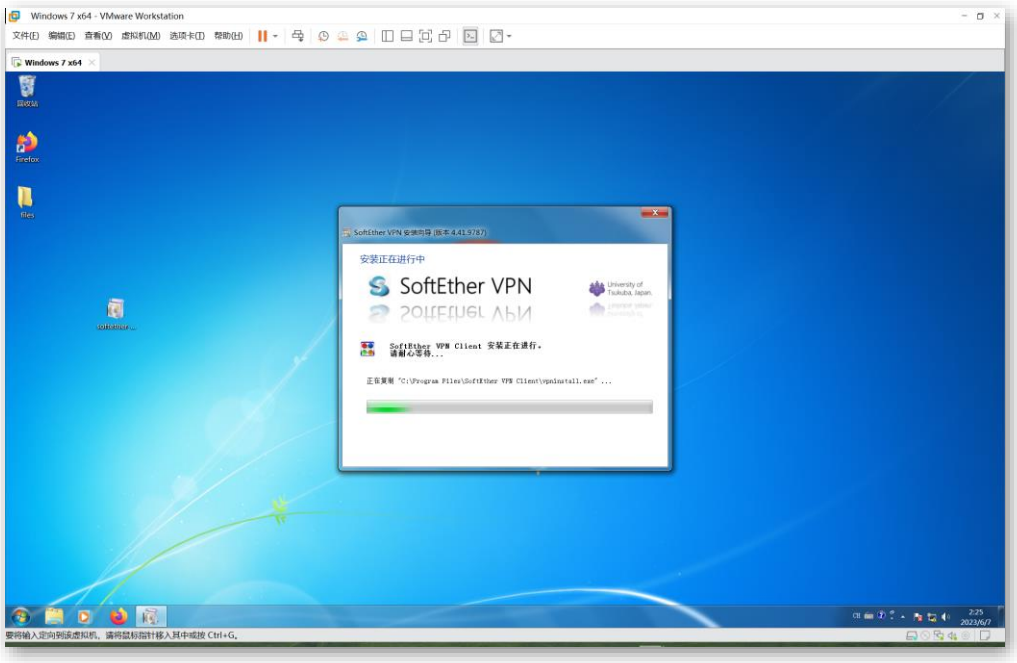


添加 VPN 认证用户。

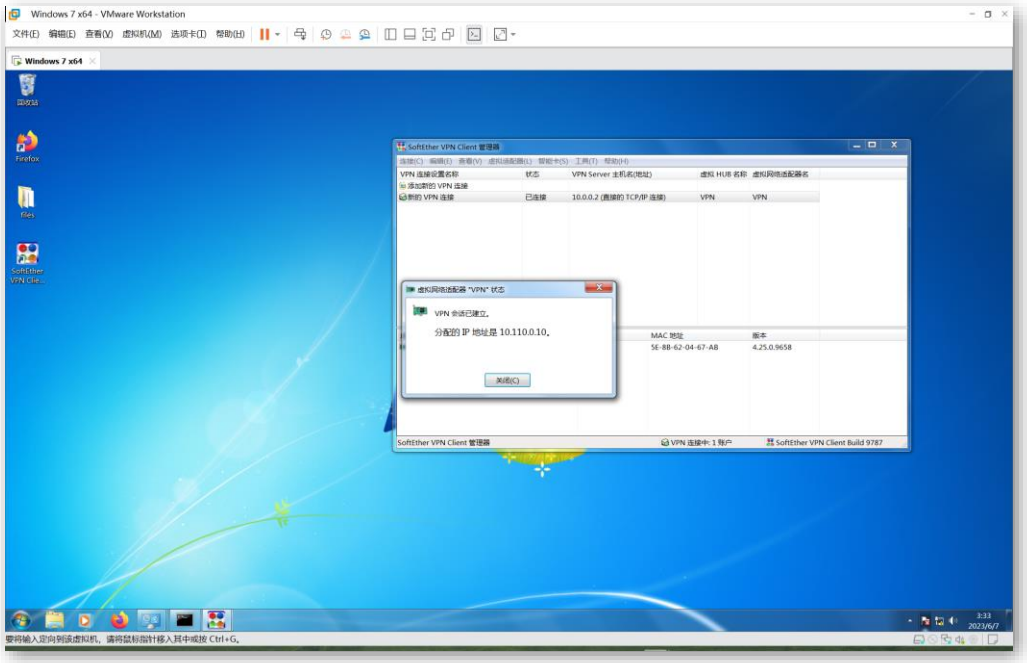


为用户设置虚拟 DHCP 地址组。

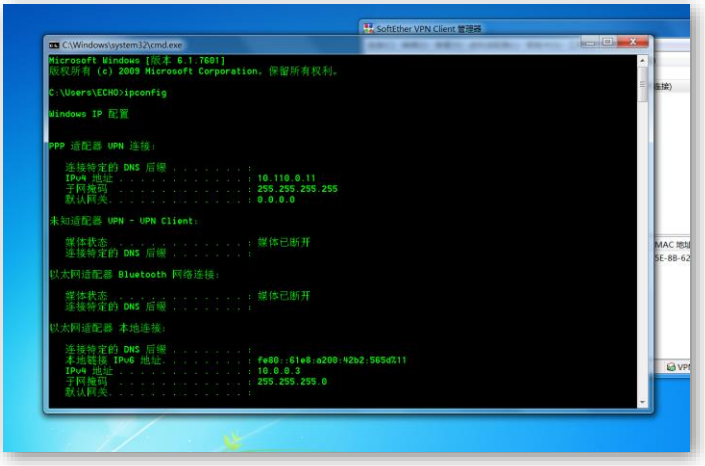
5、在虚拟机 Windows7 下安装 SoftEther VPN client



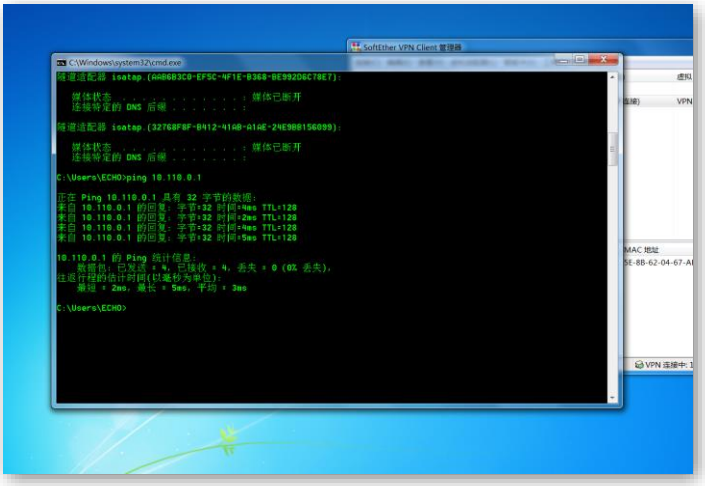
安装完成之后，在 client 中连接到 VPN 服务器：



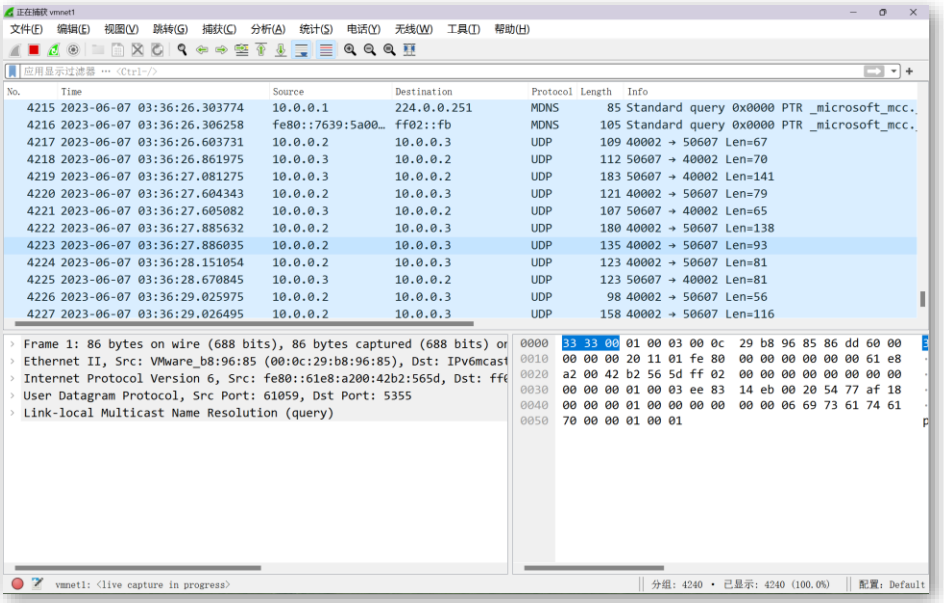
使用 443https 端口连接，成功分配 IP 地址，查看 VPN 地址：



VPN 已经获得地址，测试 ping 虚拟网关地址：

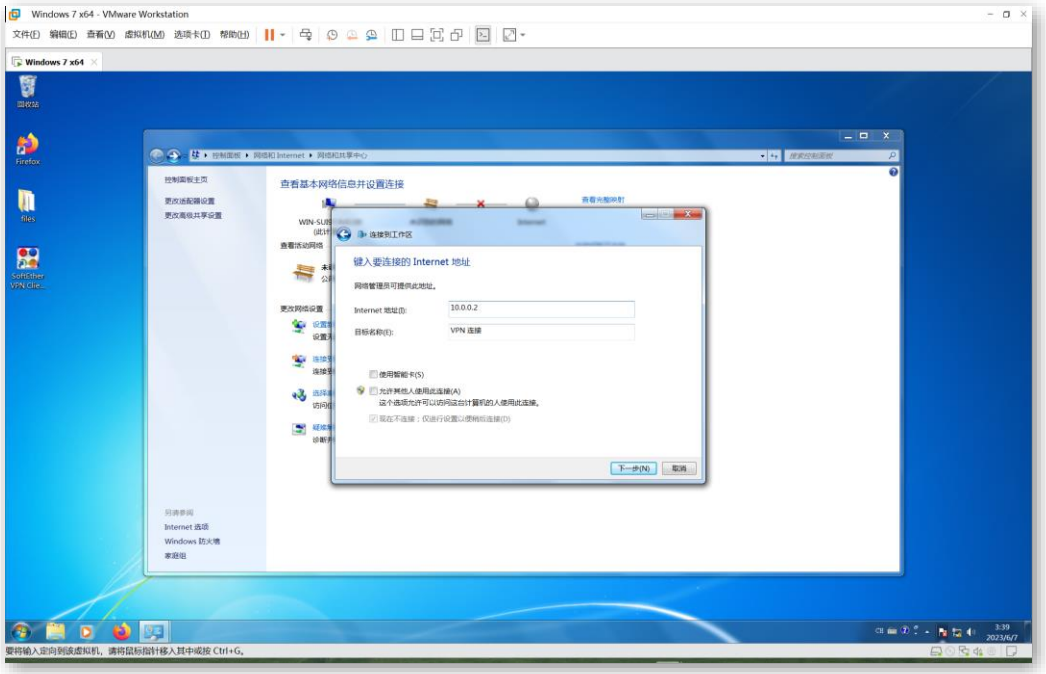


在 wireshark 中抓包：

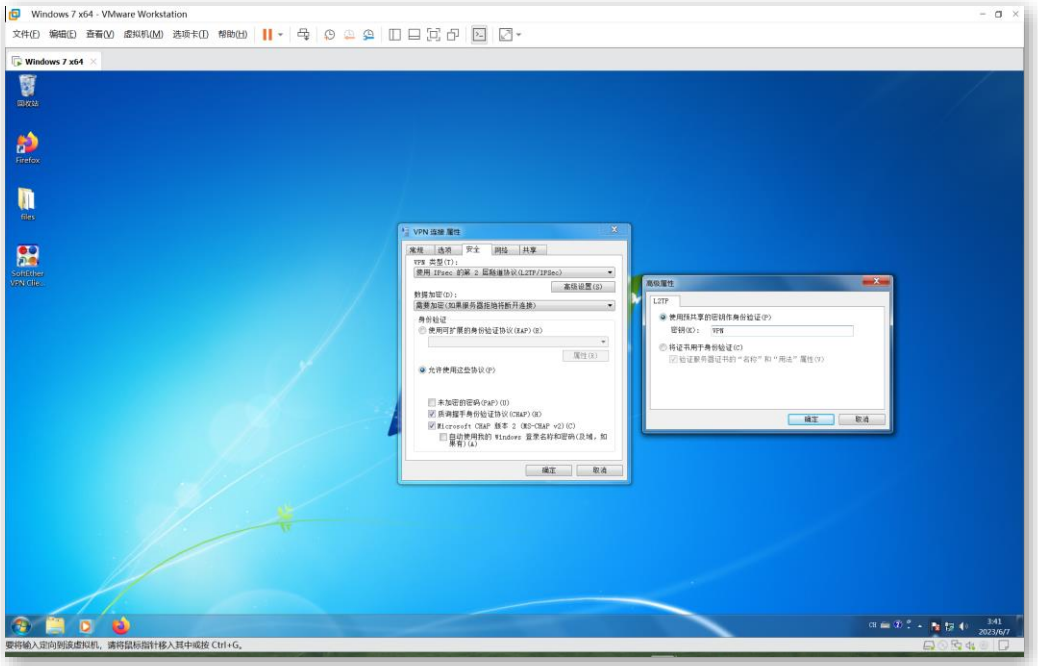


wireshark 中抓取不到明文的 icmp 包，证明两点之间的数据已经经过加密。

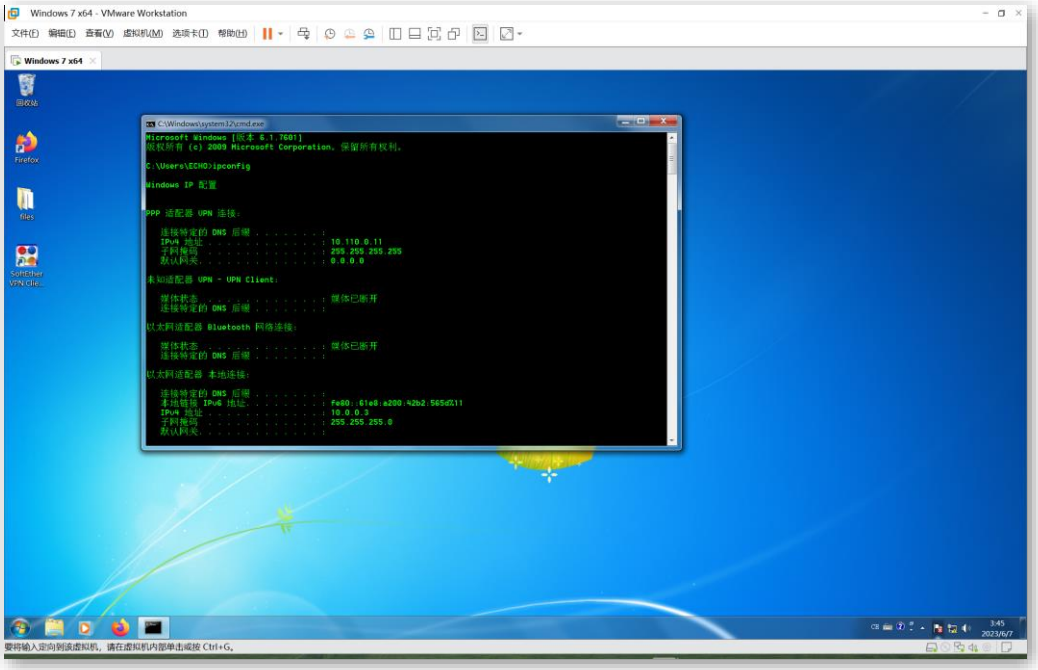
6、不使用 SoftEther client 进行 VPN 连接，直接使用系统 VPN 进行连接，配置 Windows7 直接连接到 VPN



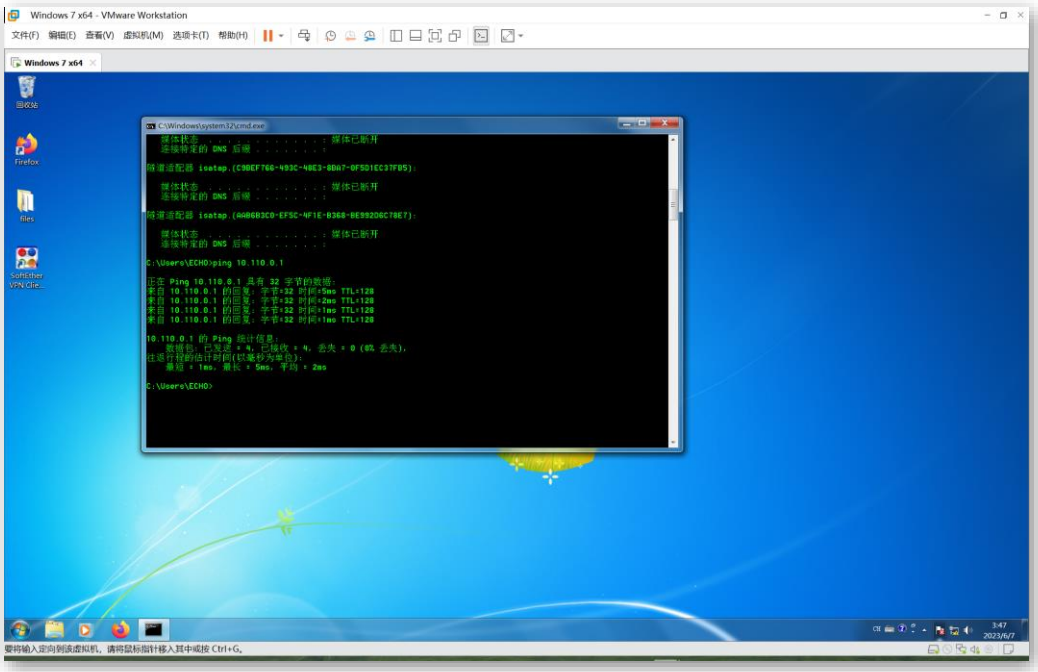
在控制面板设置 VPN 连接。



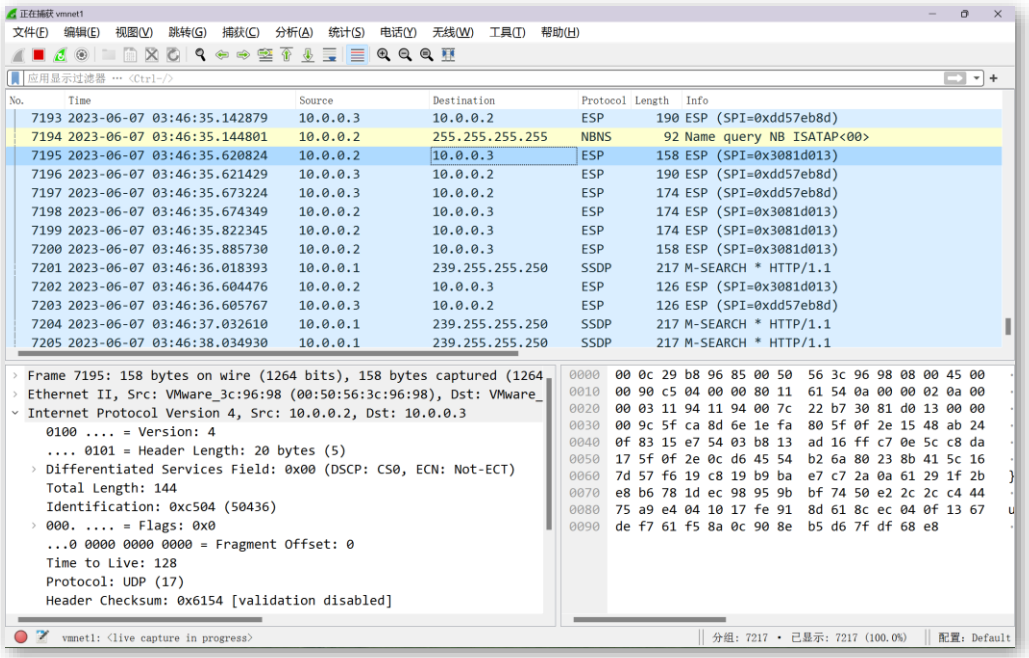
设置预共享密钥作为认证方式，将 VPN 类型指定为 L2TP over IPSec，保存配置，使用先前配置的用户名和密码进行登录、连接。



成功通过系统 VPN 连接到 VPN 服务器，获得了虚拟网关发给的 IP 地址，测试 ping 虚拟网关，并进行抓包分析：



成功 ping 通虚拟网关。



通过wireshark抓包发现,没有暴露的icmp报文,只有10.0.0.2到10.0.0.3之间的经过加密的ESP报文，即加密后的IPSec报文段。

五、实验结论

1、ip网使用明文传输网络报文，数据极其容易遭到监听和攻击，其本身是不安全的。

2、使用VPN技术可以对IP数据报进行加密，给不安全的IP明文加了一层安全措施。

3、VPN的实现技术多种多样，比如此处使用到SoftEther VPN，其实现加密流量的传输方式有TCP、UDP、ICMP等，不局限于某一种传输方式，所以，在使用SoftEther VPN客户端连接的时候，抓取到的数据包多是毫无规律的，其中包含着多种不同的报文。

4、安全的网络通信就是通过各种安全的方法，让本身不安全或者不够完全安全的通信方式变得更加安全，VPN就是这样的一种技术。

5、虽然VPN技术提供了一定的安全性，但仍然需要注意其他方面的安全措施。例如，使用强密码、定期更新密码等，以防止VPN用户的密钥被盗用，非法用户进入内网对网络造成破坏，如此方得以加强整个网络系统的安全性。