**电 子 科 技 大 学**

**实 验 报 告**

**学生姓名：XXXXX 学 号：XXXX 指导教师：XXXXX**

**实验地点：YYYY 实验时间：YYY**

**一、实验室名称：** 网络安全专业课程实验室

**二、实验项目名称：** IPSec VPN实验

**三、实验学时： 2**

**四、实验原理：**

IPSec实际上是一套协议包而不是单个的协议，IPSec是在IP网络上保证安全通信的开放标准框架，它在IP层提供数据源验证、数据完整性和数据保密性。其中比较重要的有RFC2409 IKE(Internet Key Exchange)互连网密钥交换、RFC2401 IPSec协议、RFC2402 AH(Authentication Header)验证包头、RFC2406 ESP (Encapsulating Security Payload)加密数据等协议。IPSec独立于密码学算法，这使得不同的用户群可以选择不同一套安全算法。

IPSec主要由AH(认证头)协议，ESP(封装安全载荷)协议以及负责密钥管理的IKE(因特网密钥交换)协议组成。AH为IP数据包提供无连接的数据完整性和数据源身份认证。数据完整性通过消息认证码(如MD5、SHA1)产生的校验值来保证，数据源身份认证通过在待认证的数据中加入一个共享密钥来实现。ESP为IP数据包提供数据的保密性(通过加密机制)、无连接的数据完整性、数据源身份认证以及防重防攻击保护。AH和ESP可以单独使用，也可以配合使用，通过组合可以配置多种灵活的安全机制。密钥管理包括IKE协议和安全关联SA(Security Association)等部分。IKE在通信双方之间建立安全关联，提供密钥确定、密钥管理机制，是一个产生和交换密钥材料并协商IPSec参数的框架。IKE将密钥协商的结果保留在SA中，供AH和ESP通信时使用。

**五、实验目的：**

1．掌握基于IPSec的VPN中网关到网关的配置

2．通过流量分析，进一步理解IPSec协议

**六、实验内容：**

1. 搭建基于虚拟机的IPSec VPN实验环境；
2. 配置基于预共享密钥的IPSec的VPN；

**七、实验器材（设备、元器件）：**

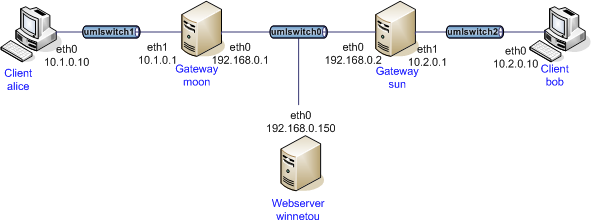
PC微机一台（需要同时支持4个虚拟机）或者在虚拟实验平台完成

**八、实验步骤**

1. 基于IKEv1的net2netPSK IPSec VPN

**步骤一、组网**

本实验对net2net-psk模式的VPN进行实验，实验网络环境如图所示：



根据图示，我们至少需要两个客户机Alice和Bob，两个网关Moon和Sun。net2net-rsa的组网与此相同。因此需要创建四台虚拟机A、B、C、D，其中B和C作为两个网关，A和D作为左右子网的主机。

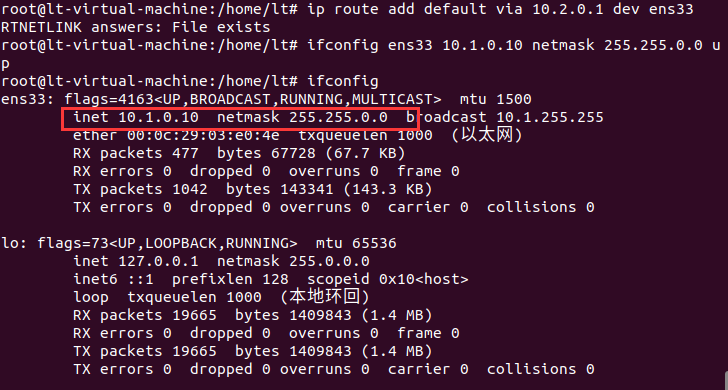
如果单机的硬件配置足够（包括CPU、内存和硬盘），我们可以在单机上通过vmware完成实验环境的部署。步骤如下：

1. 安装一台虚拟机A，虚拟机操作系统为Ubuntu16.10（任何版本都可以）；
2. 在创建完虚拟机A之后，使用VMware的Clone直接克隆出BCD；
3. 调整网卡，BC要作为网关存在，所以需要有两块网卡，因此要在设置里给BC再添加一块网卡；
4. 配置网段，在VMware的Edit选项中，选择Virtual Network Editor，添加三个虚拟网段vmnet2/vmnet3/vmnet4，类型为Host-Only，添加网段为上图的子网1、2、3的网段；DHCP选项关掉，不开启自动分配IP；

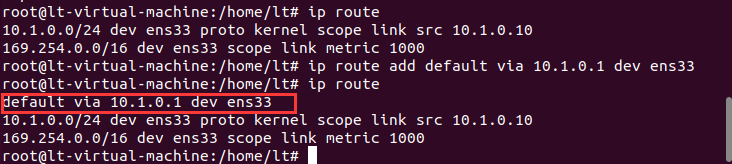


1. 虚拟机接入子网，将虚拟机A的网卡类型设置为Custom，选择vmnet2，则A接入子网1，将B的两块网卡一块设为vmnet2，一块设为vmnet3，则B同时接入了子网1和子网2；同理，设置C和D；
2. 配置虚拟机。四台机器都开机，使用命令行，按照上图配置机器的IP地址和子网掩码，其中A和D需要配置默认网关为B和C的IP，实验环境中B和C是充当网关的；

例：设置A的IP地址和子网掩码



例：设置A的默认网关



1. 开启转发。因为B和C充当网关，因此需要修改B和C中的/etc/sysctl.conf文件，将net.ipv4.ip\_forward=1那一行的注释取消，这样才能发挥其路由器的功能。

上述操作完成后，确保各个网段是通的，也就是网络设置正确无误。通过ping命令进行测试。测试过程中，如果遇到ping某个IP时没有反应（即不是报告有返回信息，也不是报告主机不可达），则从另外一端（被ping的主机）ping回来，一般情况下，可以解决问题。（注：这个可能是虚拟网络的问题。）

另一方面，我们可以在虚拟实验环境进行实验，直接通过操作面板创建虚拟主机和虚拟交换机，搭建类似的实验环境。

**步骤二、安装Strongswan**

输入命令：sudo apt-get install strongswan-starter即可。

**步骤三、配置net2net-psk**

psk的配置使用Pre-Shared-Key进行认证。这个预先设置好的key放在了ipsec.secrets中。

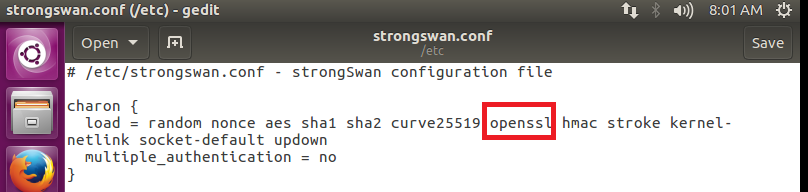
**（1） 配置文件**

配置网关B：只需要把https://www.strongswan.org/testing/testresults/ikev1/net2net-psk/index.html上所提供的moon的ipsec.conf、ipsec.secrets和strongswan.conf三个配置文件分别放到网关B的/etc/ipsec.conf、/etc/ipsec.secrets和/etc/strongswan.conf的位置即可。



配置网关C：同B。只不过这次使用sun的配置文件。

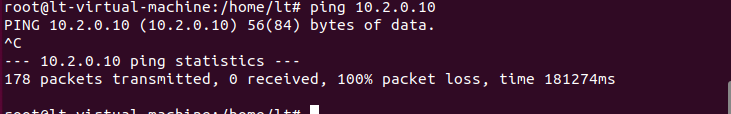
注意：对B和C的strongswan.conf配置文件，里面要增加openssl支持，如下：



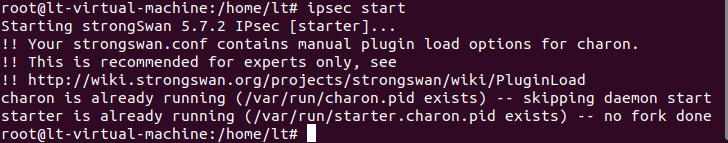
原文件里面没有openssl，这个是用来支持所需的密码算法。

**（2） 启动**

① 启动之前，A和D分别在不同的子网下，可以测试一下，A机不能ping通D机。



② B机启动ipsec，命令为：sudo ipsec start



③ C机启动tcpdump：tcpdump -i ens33 -w ikev1-sun-capture.pcap

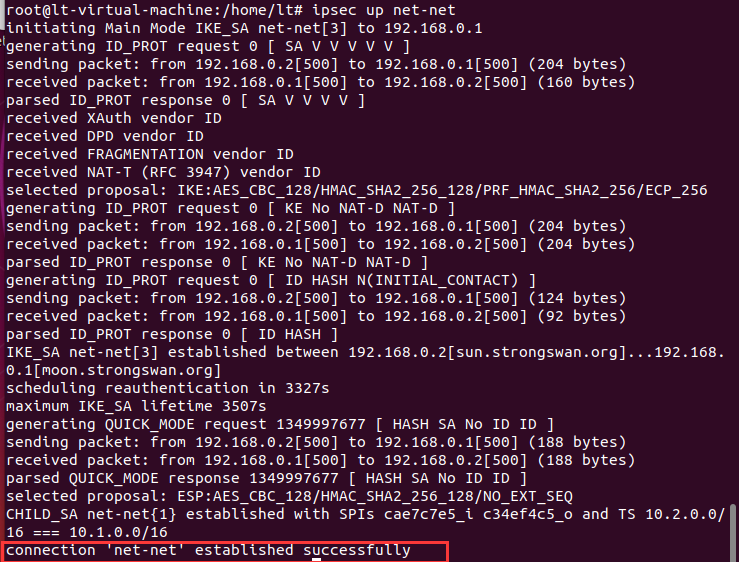
这里的ens33是要监听的网卡，也就是IP为192.168.0.2的网卡。保存的pcap数据可以放到windows平台的wireshark进行分析。（也可以直接在C机、B机里面用wireshark进行抓包分析）

如果是图形界面，开启一个新的终端来运行下述命令；如果是字符界面，采用ctrl+alt + F2/F3/F4等开启一个新的终端来输入下述命令。

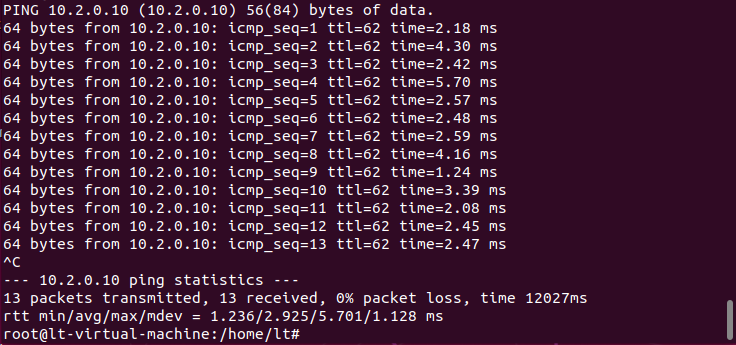
④ C机启动IPSec：sudo ipsec start或sudo ipsec restart，启动/重启StrongSwan；

⑤ C机运行sudo ipsec up net-net，即开启名字为net-net的连接，net-net的具体配置在ipsec.conf中。

如果正常，命令过后会显示输出信息，最后一句为：connection "net-net" established successfully。表明所有配置正常。



⑥ 这时候主机A去ping主机D，二者可以通了。



对wireshark的抓包文件进行分析，说明协议的语法、语义和时序。

1. 基于IKEv2的net2net PSK IPSec VPN

网络配置和IKEv1的net2net-psk一致。

配置文件的下载网址为：

https://www.strongswan.org/testing/testresults/ikev2/net2net-psk/index.html

分别下载针对moon和sun节点的配置文件：

ipsec.conf、ipsec.secrets、strongswan.conf

并把上述文件部署到/etc目录下。

与IKEv1类似，需要在strongswan.conf文件中添加openssl模块。

在moon或者sun节点启动抓包攻击tcpdump。比如：

sudo tcpdump -i ens33 -w ikev2-moon-capture.pcap

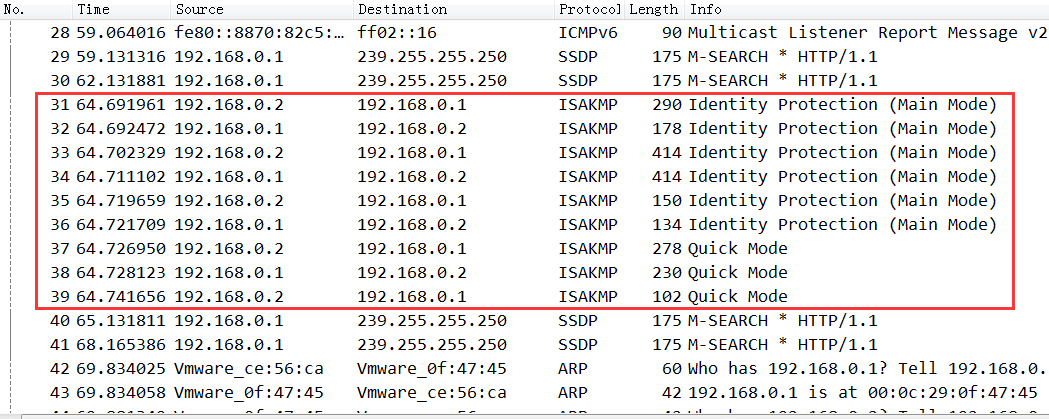
然后分别启动moon和sun的ipsec功能，如果显示connection建立成功，则从A机ping D机，或者从A机请求D机的服务，比如访问网页。

对抓包文件进行协议分析，列举出其中的关键信息。

### 【实验报告】

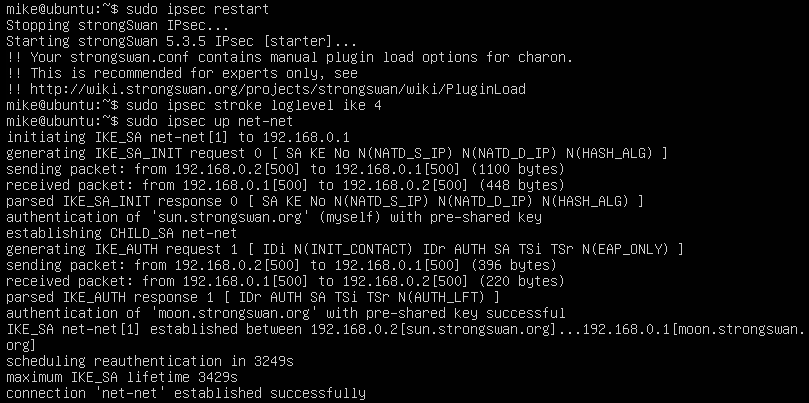
1. 说明实验过程。
2. 进行结果分析

IKEv1的结果：



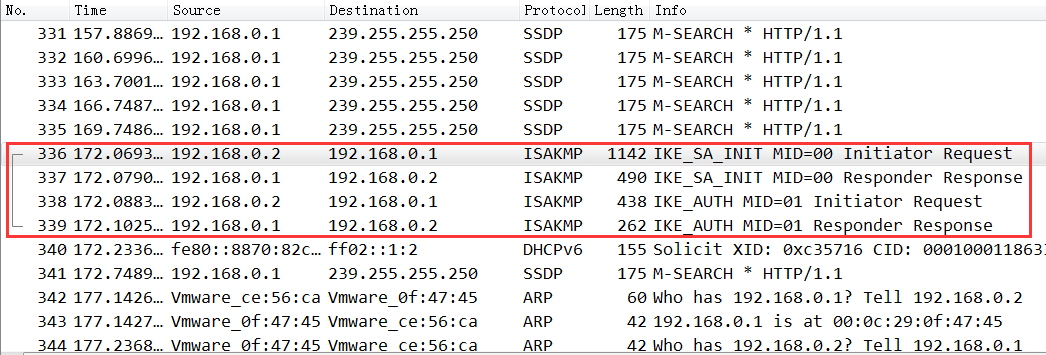
主模式的6条消息过后，是快速模式的3条消息，完成了SA协商、身份认证和密钥生成。

IKEv2的结果：



最后显示connection 'net-net' established successfully表示建立指定的net-net连接成功。也可以从输出信息得出IKE\_SA\_INIT交换成功、IKE\_AUTH交换成功。

wireshark抓包数据分析：

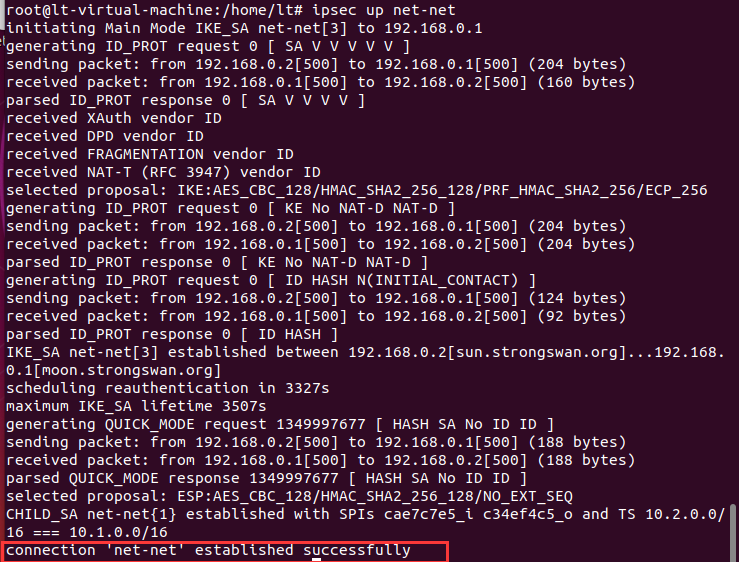


可以看出IKE\_SA\_INIT交换过后，是IKE\_AUTH交换，通过4条消息完成了IKEv2的交换过程。

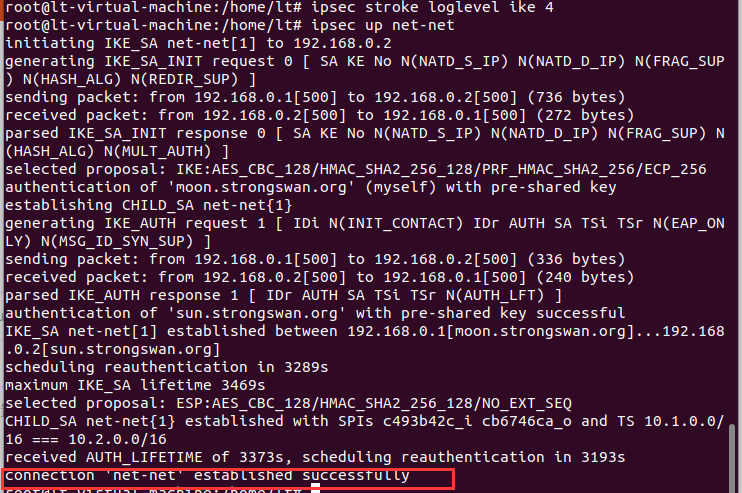
**九、实验数据及结果分析：**

（1）IPSec连接成功截图

C机启动成功截图：（这个是ikev1的）



B机启动成功截图：（IKEv2的）



（2）实验过程中所得抓包文件截图分析

**十、实验结论：**

**十一、总结及心得体会：**

**十二、对本实验过程及方法、手段的改进建议：**

**报告评分： XX**

**指导教师签字：XXX**