电子科技大学信息与软件工程学院

**实 验 报 告**

学 号 2017221303023

姓 名 陈奎

（实验） 课程名称 网络安全协议

理论教师 罗绪成

实验教师 罗绪成

合作队友 郑烁

**电子科技大学教务处制表**

**电 子 科 技 大 学**

**实 验 报 告**

**学生姓名：陈奎/郑烁 学号：2017221303023/2017721304002 指导教师：罗绪成 实验地点：信软楼 实验时间：19.11.28**

**一、实验名称：**IPSec VPN 实验

**二、实验学时：**2学时

**三、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 协议套

**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)封装安全载荷等协议。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 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素材并协商 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。

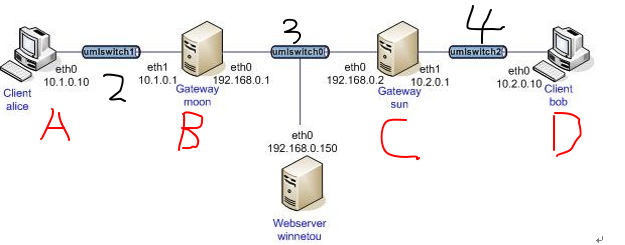
**五、实验内容**

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

**六、实验器材（设备、元器件）：**

台式机一台，能够安装一台 ubuntu 虚拟机，能够访问互联网。

**七、实验步骤：**



**步骤一、组网**

1. 创建4台虚拟机ABCD



1. 在设置里给 BC再添加一块网卡



1. 配置网段



1. 虚拟机接入子网

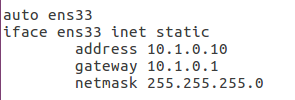
A配置

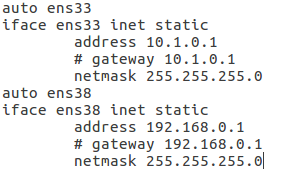
B配置

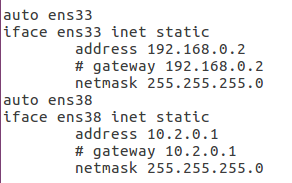
C配置

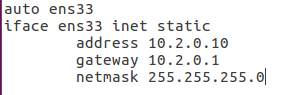
D配置

1. 配置虚拟机

A的IP配置

B的IP配置

C的IP配置

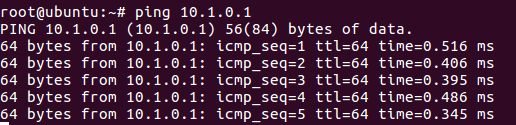
D的IP配置

1. 开启转发

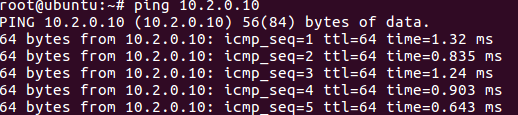


1. 通过ping命令测试

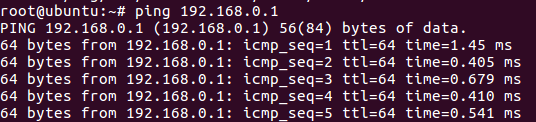
ApingB



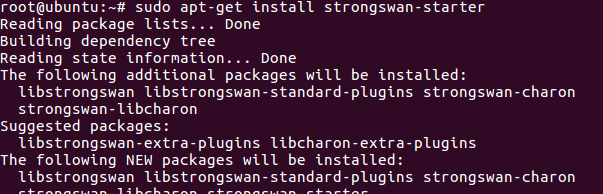
CpingD



CpingB

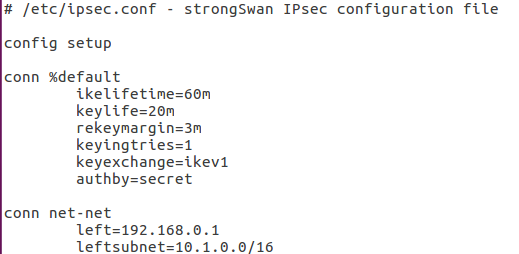


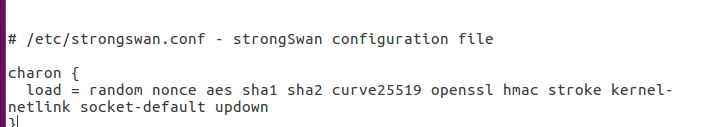
**步骤二、安装 Strongswan**



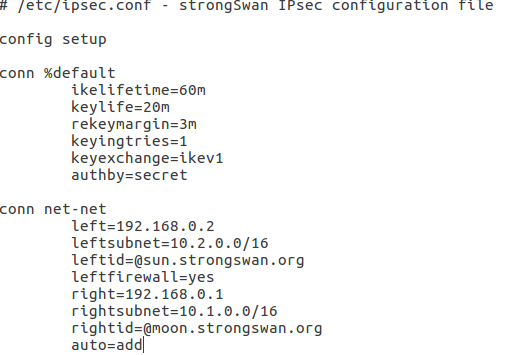
**步骤三、配置 net2net-psk**

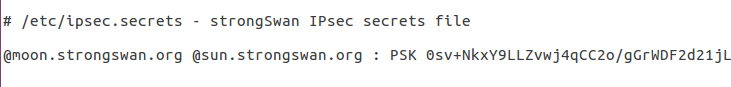
配置网关 B：

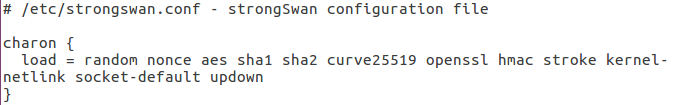




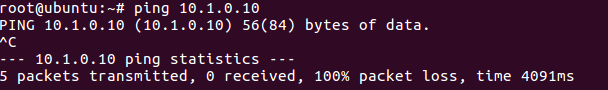
配置网关 C：



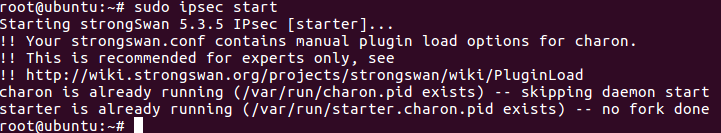




ApingB主机不通



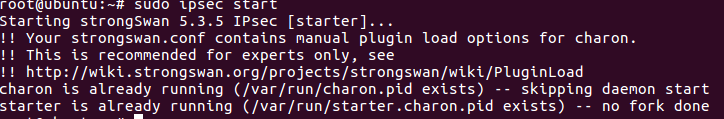
B 机启动 ipsec



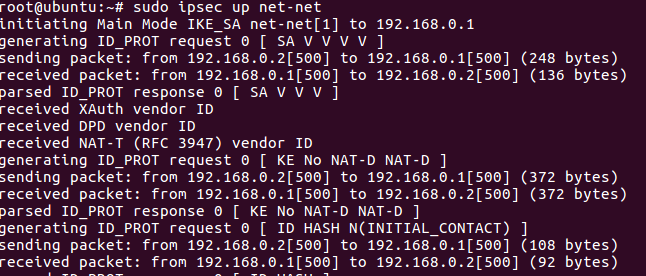
C 机启动 tcpdump

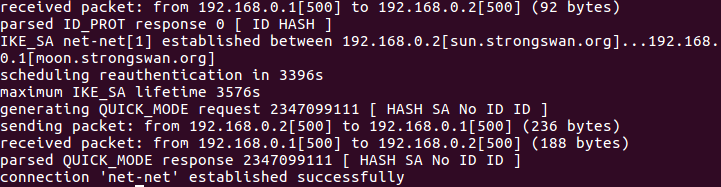


C 机启动 IPSec

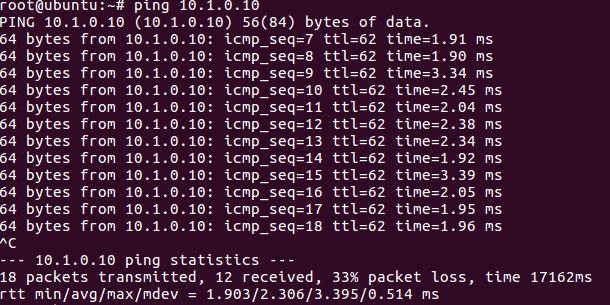


C机开启名字为 net-net 的连接



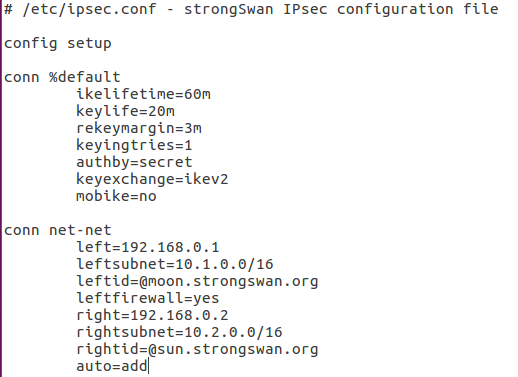


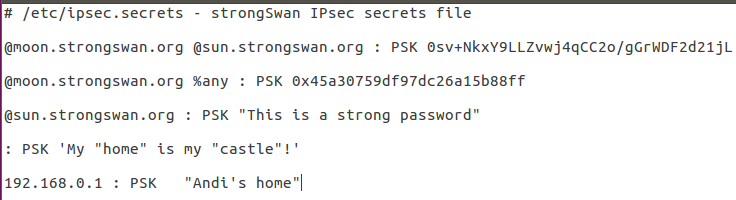
主机 D去 ping 主机 A，二者可以ping通

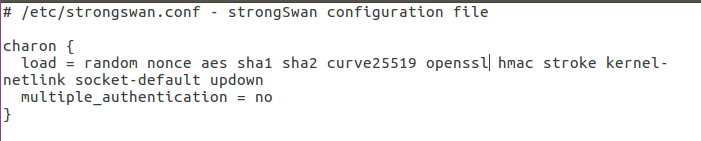


**步骤四、配置 IKEv2 的 net2net-psk**

配置网关 B：

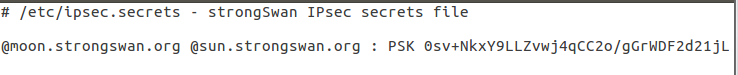


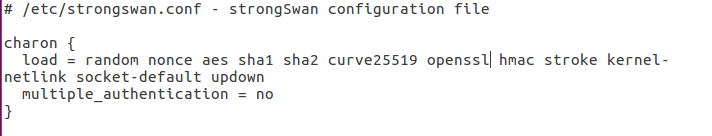




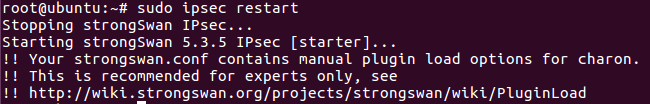
配置网关 C：



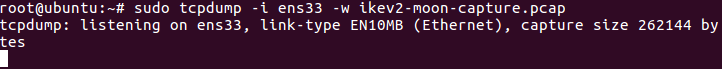




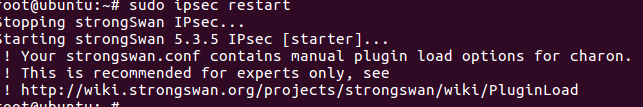
B 机启动 ipsec



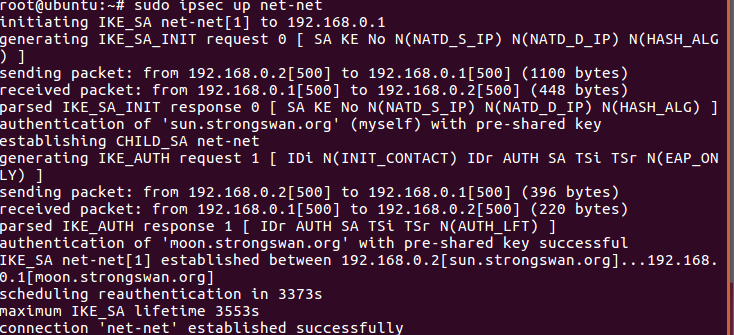
C 机启动 tcpdump



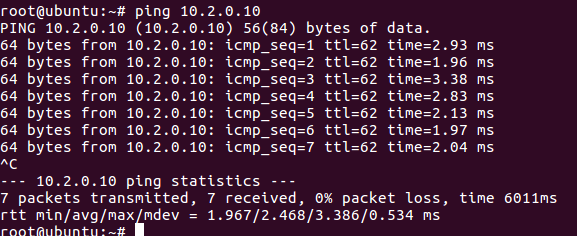
C 机启动 IPSec



C机开启名字为 net-net 的连接

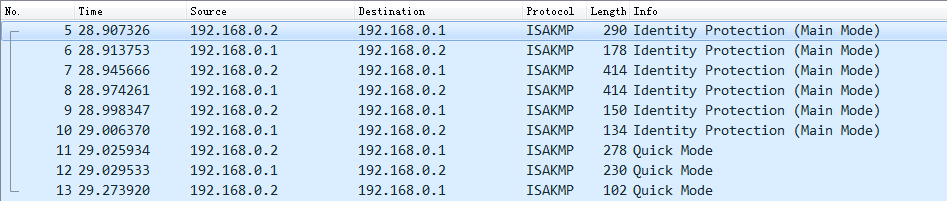


主机 A去 ping 主机 D，二者可以ping通



**八、实验结果与分析（含重要数据结果分析或核心代码流程分析）**

**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。现在抓包分析的是主模式，有6个来回交互的包，发起端是192.168.0.2，对端是192.168.0.1。

**主模式第一条消息（明文）：**

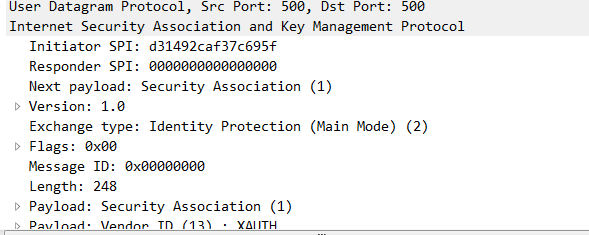
第一个包，发起端协商SA，使用的是UDP协议，端口号是500。对方的COOKIE为0。内容还包含一个SA负载，还有提议负载，转换负载。sa的负载是定位这个ISAKMP是为了IPSEC工作。因为IKE是一个标准的协议，所以在SA负载中通过DOI，解释域，来说明这条消息交换用于IPSEC。提议负载的内容包含一个提议号，协议ID，SPI，转换号，其中SPI为0，转换号指向了相应的转换负载。转换负载的内容是加密的参数，如des，dh算法，存活时间，hash算法等等。“Version：1.0 ”：IKE版本号，1.0表示使用ikev1建立连接。

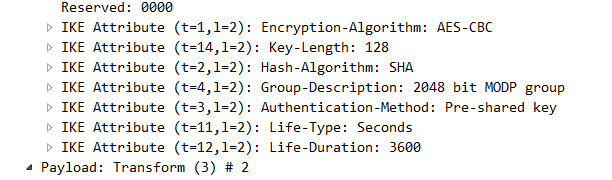
Initiator SPI：发送端的SPI值，告知响应端主机要使用IPSEC的哪一把密钥来加密这个封包。

Responder SPI：响应者的SPI值，告知发送端使用哪一把密钥加密数据包。

IKE Attribute (t=3,l=2): Authentication-Method: Pre-shared key使用预共享密钥认证.

以下是抓包结果：

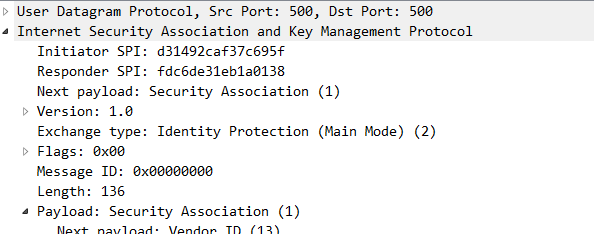


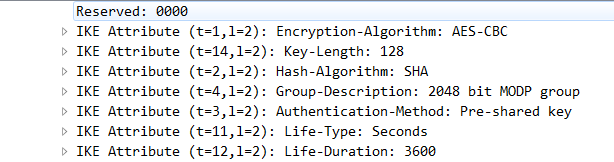


**主模式第二条消息（明文）：**

响应端收到发送端发送的加密套件后，对比自己是否有相对应的加密套件，如果有就使用和发送端相同的加密套件加密数据，把自己的cookie值和选择好的加密套件发送给发送端；如果没有相同加密套件则IKE建立失败响应。

以下是抓包结果：

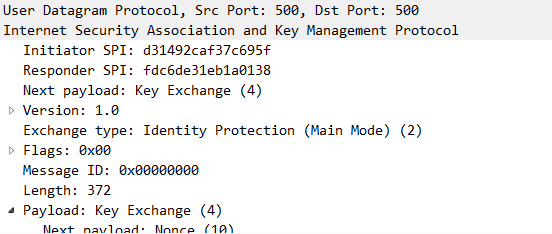


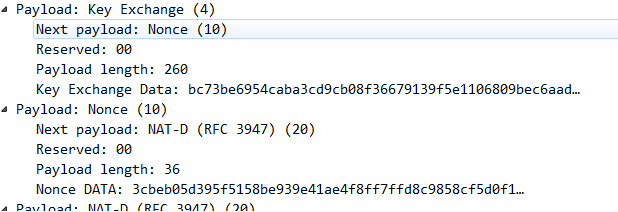


**主模式第三条消息（明文）：**

如果发起方接受了安全提议，就给对方发送密钥生成信息，对方用来生成IKE的秘钥。发送端生成随机数和DH公共值，包3的主要目的是向响应端发送自己的DH公共值和Nonce随机数。用于生成加密时所需要的KEY值。

以下是抓包结果：

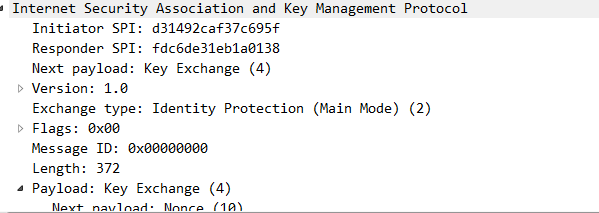


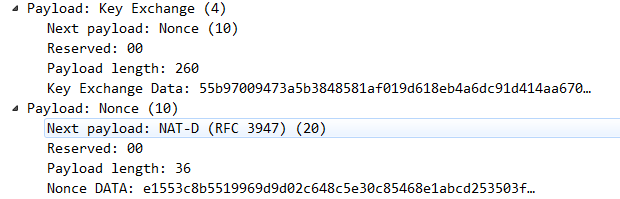


**主模式第四条消息（明文）：**

协商相应方给协商发起方发送密钥生成信息，使得协议发起方能生成密钥。接收方回应自己的公钥给初始方。包含一个随机数NR。然后双方各自计算出共享的密钥，一共有三个密钥，SKEYID\_a，d，e，其中d是根据z=pfs（pre-shared key，cookie\_i，cookie\_ni，nl|0），其中d用来给第二阶段提供密钥的素材。a用来对IKE的数据进行认证，e用来加密整个IKE协商的数据。

以下是抓包结果：

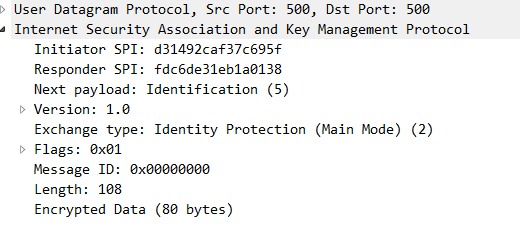




**主模式第五条消息（密文）：**

发起方发起身份验证，报文中带有认证的数据（预共享密钥或者数字签名）。由于包1和包2已经协商好了加密算法，包3和包4协商好了加密的KEY值，所以包5的消息被加密了。

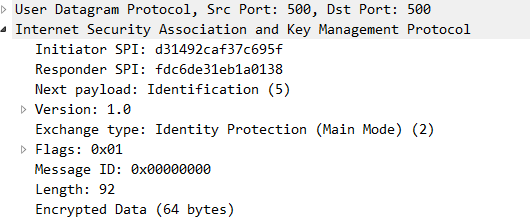
以下是抓包结果：



**主模式第六条消息（密文）：**

响应端回应报文，同样发送认证的数据（预共享密钥或者数字签名），验证对方身份信息。包6的数据同样使用包1、包2协商的算法和包3、包4协商的key值加密数据，所以包6的认证数据是加密的。双方身份验证通过后，IKE协商结束。

以下是抓包结果：



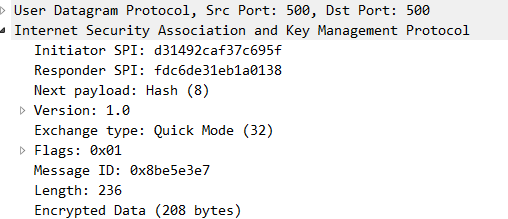
**快速模式第一条消息（密文）：**

发起方主要是进行IPSEC SA的协商，建立安全联盟，报文内容主要是协商用的封装方式以及后面的加密算法以及生存时间和感兴趣流等等。由于数据加密所以无法查看。

发起者以及响应者的SPI值是由上阶段IKE协商时已经确定的，所以IPSec协商依然使用上阶段的SPI。

Exchange type：Quick Mode（32），交换类型使用快速模式，IPSec协商时只有快速模式。

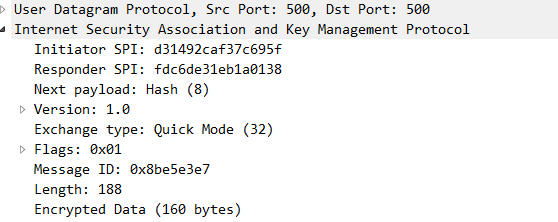
以下是抓包结果：



**快速模式第二条消息（密文）：**

响应方回包，同意包7发送的封装方式、加密算法、生存时间、感兴趣流等等，同时，也能起到确认收到对端消息的作用。由于数据加密所以无法查看。

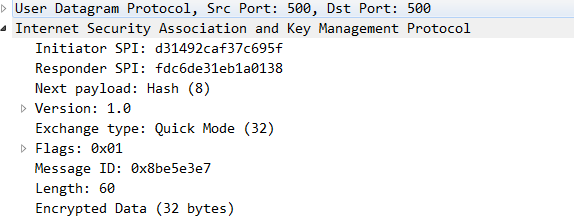
以下是抓包结果：



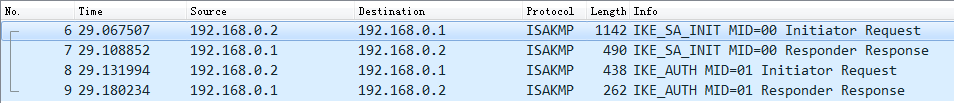
**快速模式第三条消息（密文）：**

发送确认报文。其中包含一个HASH，其作用是确认接收方的消息以及证明发送方处于主动状态（表示发送方的第一条消息不是伪造的）。由于数据加密所以无法查看。

以下是抓包结果：



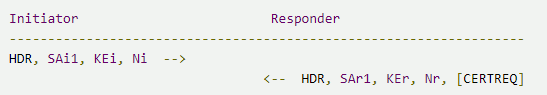
**IKEv2 的结果：**



从输出信息得出 IKE\_SA\_INIT 交换成功、IKE\_AUTH 交换成功。

IKEv2协议由两个阶段的交互过程（即两个来回，共四个报文）组成。第一阶段称为IKE\_SA\_INIT 交换。第二阶段称为IKE\_AUTH 交换。

RFC 7296中对IKEv2协议的规范说明：



来看第一阶段相互作用（IKE\_SA\_INIT），其第一个报文由发起方（192.168.0.2）发出，后面为响应方（192.168.0.1）的响应报文。

**第一、二条消息（明文）：**

KE\_SA\_INIT是ipsec vpn建立的初始交换，当完成IKE\_SA\_INIT交换之后后续其他的交互报文将被加密。通过查看可以看到，在基础的IKE头部里面有多个payload，在payload又有多个Proposal组成，在Proposal中由多个Transform 组成。

纵观整个IKE\_SA\_INIT数据包可以发现。在IKE\_SA\_INIT数据包中包括的内容有

· Security Association

　· Proposal

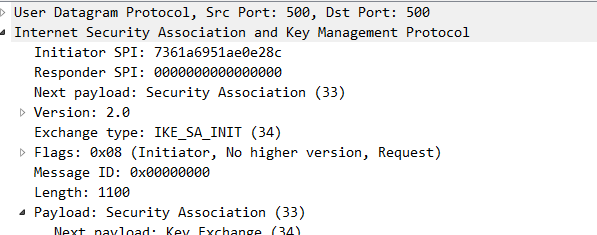
　· Transform（Encryption Algorithm、Pseudo-random Function、Integrity Algorithm、Diffie-Hellman Group）

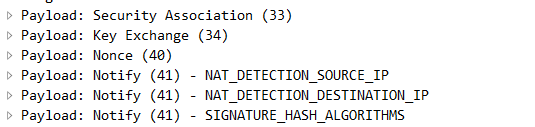
· Key Exchang

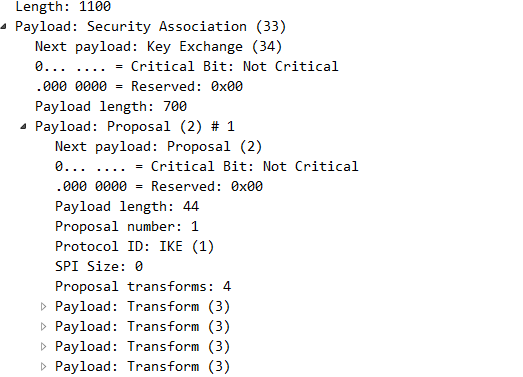
· Nonce

通过观察可以看到，其实IKE\_SA\_INIT数据包中的内容就是IKEv1中主模式的1~4个报文。也就是说，IKE\_SA\_INIT对IKEv1中1~4个报文进行了整合，使得交互更加高效。通过IKE\_SA\_INIT传递“材料”就可以完成后续报文的加密工作，当IKE\_SA\_INIT交互完成之后后续其他交互的报文将被加密。

以下是抓包结果：



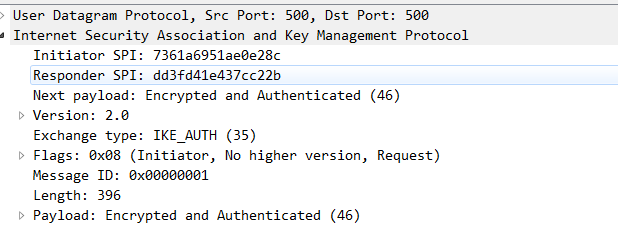


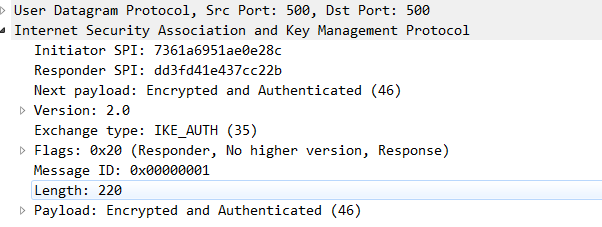


**第三、四条消息（密文）：**

一旦IKE\_SA\_INIT交换成功完成，IKE\_AUTH交换将会开始，用于认证对方，并产生IPsec Security Associations。下图是IKE\_AUTH的报文。因为关键的信息被加密，我们无法获知其中的内容。

以下是抓包结果：





**九、总结及心得体会：**

通过本次实验，了解了IPSec的基本配置，加深了对Linux操作系统的了解。在查看数据包以及进行分析的过程中，能够将理论与实际相结合，感受到了课本知识的实际应用。

**十、对本实验过程及方法、手段的改进建议：**

无。

**报告评分：**

**指导教师签字：**