电子科技大学信息与软件工程学院

**实 验 报 告**

学 号 2017221302006

姓 名 周玉川

（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

**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：周玉川 学号：2017221302006 指导教师：罗绪成**

**实验地点：信软楼西305 实验时间：2019.11.18/2019.12.19**

**一、实验名称：IPSec VPN实验**

**二、实验学时：4**

**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。

**四、实验原理：**

（**1）IPSec介绍**

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。

**（2）IKE简介**

IKE（Internet Key Exchange）因特网密钥交换协议是 IPSec 的信令协议，IPSec 提供了自动协商交换密钥、建立安全联盟的服务，能够简化 IPSec 的使用和管理，大大简化 IPSec 的配置和维护工作。IKE 不是在网络上直接传送密钥，而是通过一系列数据的交换，最终计算出双方共享的密钥，并且即使第三者截获了双方用于计算密钥的所有交换数据，也不足以计算出真正的密钥。IKE 具有一套自保护机制，可以在不安全的网络上安全的分发密钥，验证身份，建立 IPSEC 安全联盟。

IKE 的交换过程（IKE 协商）分为两个阶段，分别称为阶段一和阶段二。

阶段一：在网络上建立 IKE SA，为其它协议的协商（阶段二）提供保护和快速协商。通过协商创建一个通信信道，并对该信道进行认证，为双方进一步的 IKE通信提供机密性、消息完整性以及消息源认证服务，是主模式；

阶段二：快速模式，在 IKE SA 的保护下完成 IPSec 的协商。IKE 协商过程中包含三对消息：第一对叫 SA 交换，是协商确认有关安全策略的过程；第二对消息叫密钥交换，交换 Diffie-Hellman 公共值和辅助数据（如：随机数），加密物在这个阶段产生；最后一对消息是 ID 信息和验证数据交换，进行身份验证和对整个 SA 交换进行验证。

**（3）ESP、AH简介**

ESP协议（报文安全封装协议）将用户数据加密封装到IP包，以保证数据的私有性。同时作为可选项，用户可以选择使用带密钥的哈希算法保证报文的完整性和真实性。ESP的隧道模式提供了对于报文路径信息的隐藏；

AH协议（认证头标协议）可对整个数据包（IP报头与数据包中的数据负载）提供身份验证、完整性与抗重播保护。但是它不提供保密性，即它不对数据进行加密。数据可以读取，但是禁止修改。

**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）：**

PC电脑一台，虚拟机4台。

**七、实验步骤：**

**步骤一、组网**

本实验对net2net-psk模式的VPN进行实验。

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；

（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，不让自主分配IP；

（5）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；

（6）配置虚拟机，四台机器都开机，使用图形界面，照着上图配置机器的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；

（7）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**

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。

**步骤四、配置IKEv2的net2net-psk**

网络配置和IKEv1的net2net-psk一致。

**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）**

（1）组网：

实验最开始，我使用的是实验室虚拟平台提供的组网拓扑，并按照实验指导书中的步骤完成了IKEv1的配置，将B机作为moon，C机作为sun，完成了配置，启动BC的ipsec和tcpdump后，A-D之间可以互相ping通，后续操作因为下课了就没有做了，后期也没有再去实验室进行实验。

所以，我使用了队友朱思宇搭建的拓扑网络，使用一台Ubuntu虚拟机，并使用克隆功能复制出另外三台机器，分别命名为ABCD，关闭其DHCP功能，将B、C设置为网关，配置双网卡，IP地址分别为10.1.0.1（10.2.0.1）和192.168.0.1（192.168.0.2），将A、D的IP地址设为10.1.0.10和10.2.0.20。

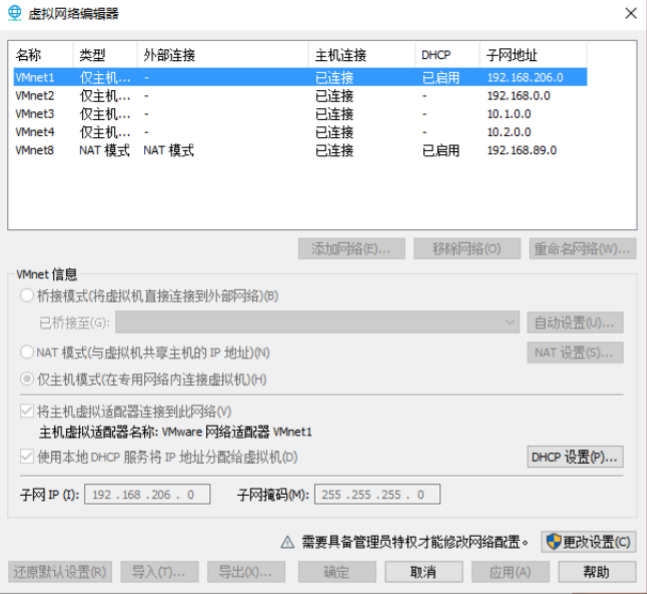


图8-1-1 拓扑网络配置

配置完成后，首先测试主机之间的连通性，发现A、B（C、D）以及B、C之间可以ping通，而A和D之间无法ping通。

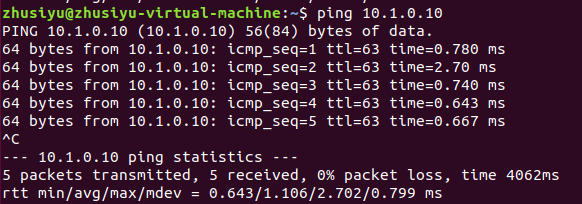


图8-1-2 AB连通性测试

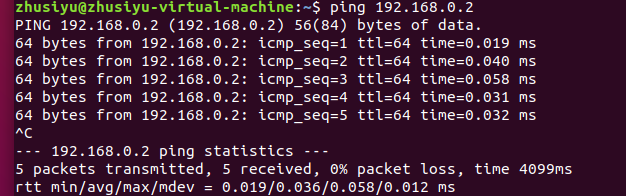


图8-1-3 BC连通性测试

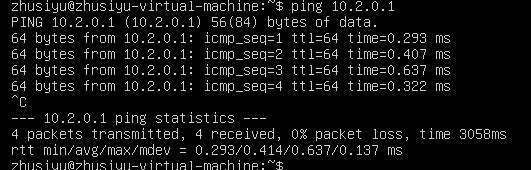


图8-1-4 CD连通性测试

（2）安装strongswan

在网关机上输入命令“sudo apt-get install strongswanstarter”安装，此处需要将连接A、D的网卡改为NAT模式，并打开DHCP功能。

（3）配置IKEv1

此处按照指导书操作，在配置文件网站上下载对应的monn和sun，并将ipsec.conf、ipsec.secret以及strongswan.conf文件分别拷贝到B和C机上，同时在strongswan.conf中添加openssl支持选项。

在B机启动ipsec，输入“sudo ipsec start”；在C机启动tcpdump，输入“tcpdump -i ens33 -w ikev1-sun-capture.pcap”,监听ens33网卡。输入“sudo ipsec up net-net”开启ipsec服务。

此时A机可以成功ping通D机了

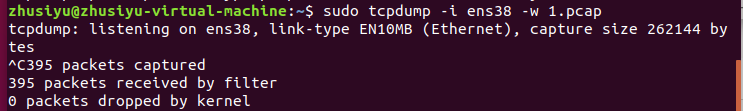


图8-3-1 监听网卡并抓包

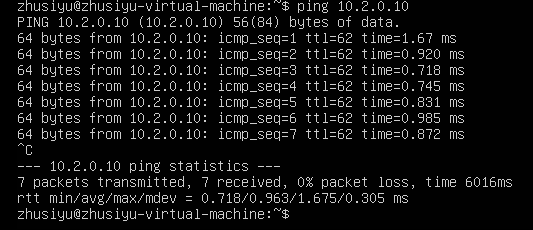


图8-3-2 AD连通性检测

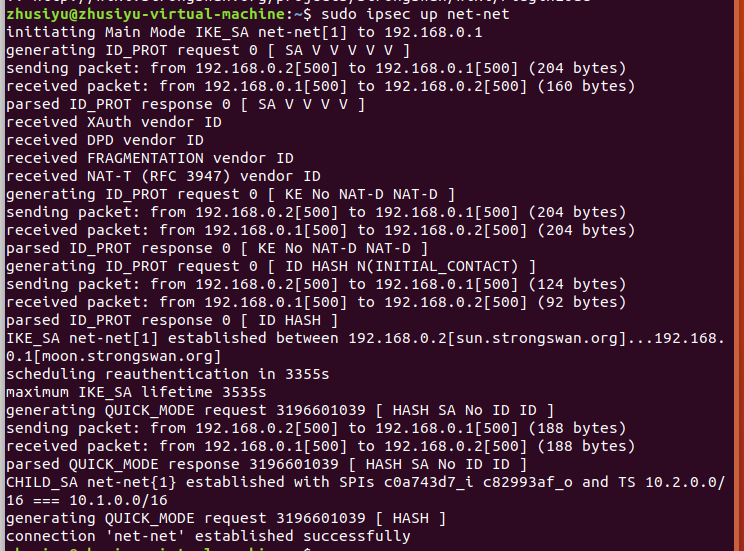


图8-3-3 ipsec net-net服务

（4）配置IKEv2

此处操作与第三步相同，故在此省略。

（5）IKEv1的抓包分析

使用wireshark打开包文件，设置筛选条件为esp||isakmp，筛选结果如下：

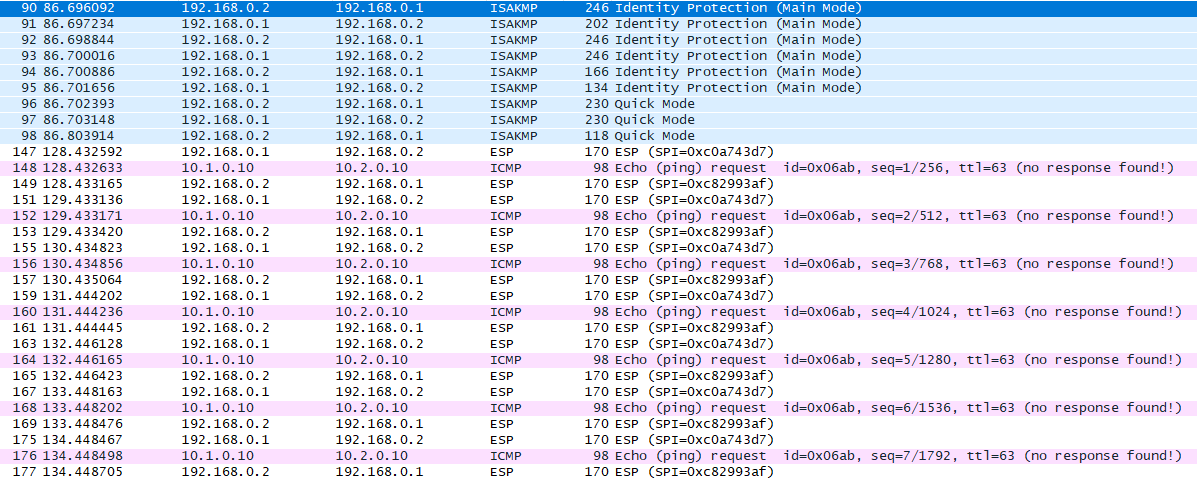


图8-5-1 筛选结果

IKEv1过程分为两个阶段，第一阶段为协商获得IKE SA，包含主模式和野蛮模式，第二阶段为协商获得IPSec的SA，使用快速模式。

**第一阶段：**

查看第一个包，对包中内容进行分析。

I-SPI告知接收方使用哪个密钥来加密这个包；

R-SPI此处还没有响应方，所以信息为空；

Next payload指定下一负载的类型，此处为SA商议；

Version说明版本号，此处为IKEv1，交换模式为主模式。野蛮模式相比之下更快速，但是也更不安全；

Flags前五位为0，后三位分别为A、C、E比特，分别表示认证位、同步位以及加密位；

Vendor id为厂商载荷，它向接收方提供了自己的信息；

Security association为SA载荷，接下来会展开分析。

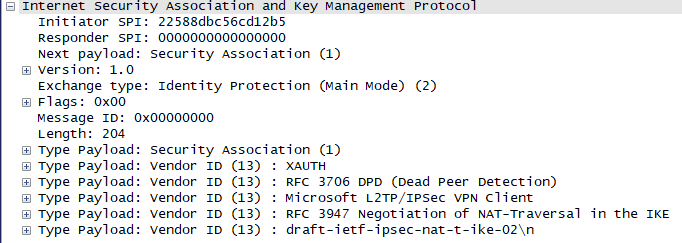


图8-5-2 第一阶段第一个包

展开SA载荷进行分析。

该SA载荷仅包含一个proposal即一个安全方案；

DOI：解释域，此处为1，表示使用ipsec协议进行解析；

Situation：取值与DOI相关；

P载荷：作为一种安全方案的标识，transform表示携带两个T载荷；

T载荷：详细介绍该套安全方案，比如此处解释加密算法为AES-CBC模式，密钥长度生存时间等，以及表明了主模式使用PSK模式进行认证。

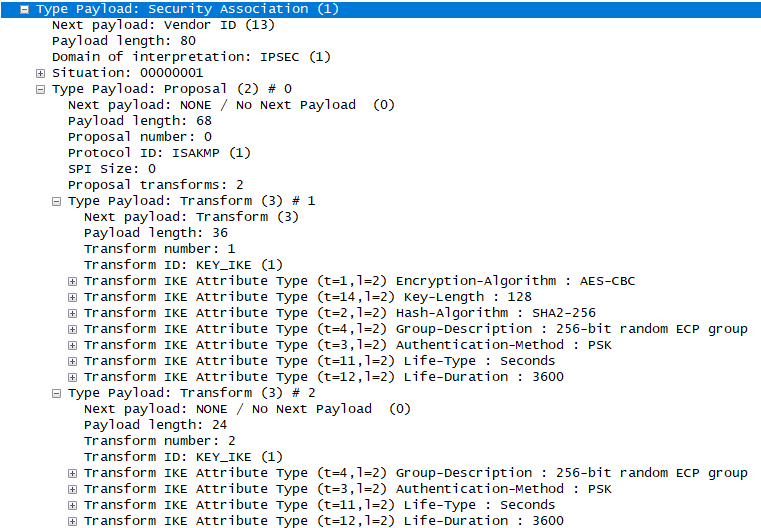


图8-5-3 SA载荷

查看第二个包并分析：

R-SPI已经发生了变化；

SA载荷和第一个包类似；

响应端选择对应的密码套件，然后将自己选择的R-SPI和加密套件发送给发送端。

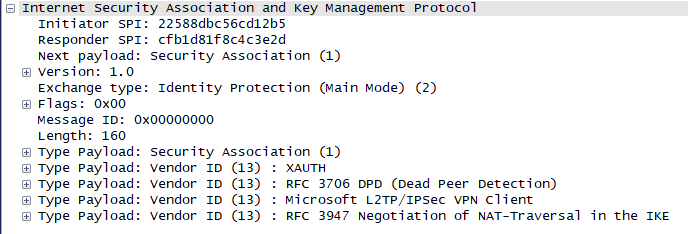


图8-5-4 第一阶段第二个包

一二包完成了SA策略交换，发送方提出了IKE安全建议供接收方选择，接收方选择安全提议后响应发送方。

查看并分析第三、四个包：

包中的payload变为了key exchange和nonce载荷，key exchange中的data即为DH公共值，因为传输链路此时还没有加密，所以只有通过双方交换DH公共值算出相同的key，和随机数一起发送给对方。

在第三、四个包中，对端完成了密钥信息及随机数等信息的交换。

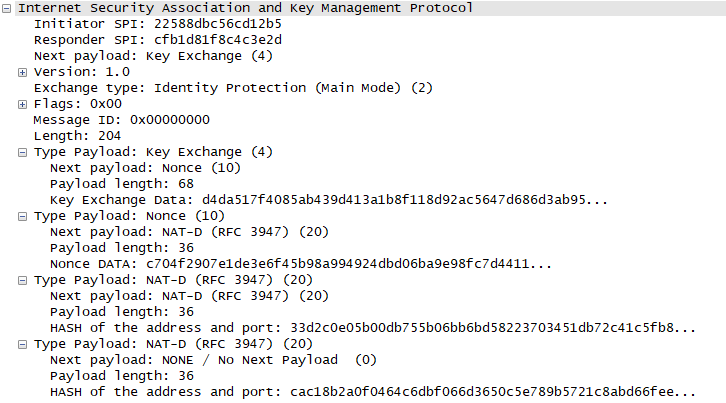


图8-5-5 第一阶段第三、四个包

查看并分析第五、六个包：

第五、六个包中，载荷变为了identification，同时flags中的E位被置1，表示数据已被加密，后续内容即为使用选择好的算法加密后的数据，这两个包通过加密内容正确与否来验证对端身份是否正确。

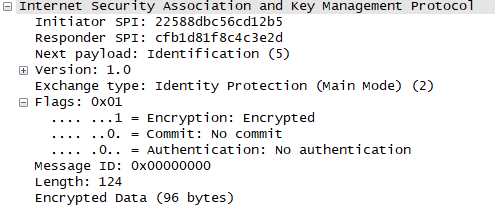


图8-5-6 第一阶段第五、六个包

至此，IKEv1第一阶段结束。

**第二阶段：**

这一阶段的目的是商议并建立IPSec的SA，通过三个包完成。

1.协商发起方发送本端的安全参数和身份认证信息。安全参数包括被保护的数据流和 IPSec 安全提议等需要协商的参数。身份认证信息包括第一阶段计算出的密钥和第二阶段产生的密钥材料等，可以再次认证对等体。

2.协商响应方发送确认的安全参数和身份认证信息并生成新的密钥。IPSec SA 数据传输需要的加密、验证密钥由第一阶段产生的密钥、SPI、协议等参数衍生得出，以保证每个 IPSec SA 都有自己独一无二的密钥。如果启用 PSF，则需要再次应用 DH 算法计算出一个共享密钥，然后参与上述计算，因此在参数协商时要为 PFS 协商 DH 密钥组。

3.发送方发送确认信息，确认与响应方可以通信，协商结束。

至此，IKEv1 协议完成。同时开始使用生成的秘钥生成 ESP 密文进行消息传递。

（6）IKEv2的抓包分析

使用wireshark对IKEv2的数据进行抓包，结果如下：

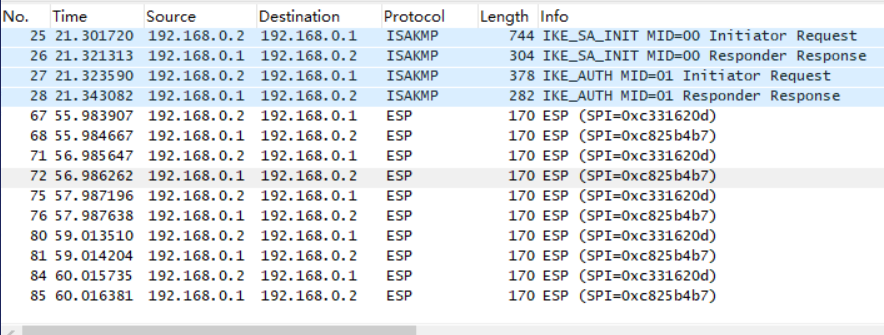


图8-6-1 IKEv2包

IKEv2的SA协商过程只用了四个包，比v1快了一倍多，第一二个包为IKE的SA初始化，第三四个包为IKE的认证。

分析第一个包：

初步观察可以发现，包中有SA载荷以及Key exchange和nonce载荷，对应了IKEv1中的第一个包和第三个包的功能，载荷中携带的信息和IKEv1的几乎相同，可以让接收方在选择了密码套件后直接生成密钥。

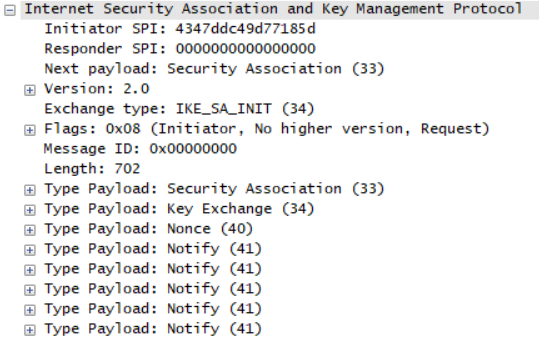


图8-6-2 第一个包

分析第二个包：

第二个包与第一个包内容相似，在功能上，它等同于IKEv1中的第二和第四个包，选择了发送方提供的密码套件，与发送方交换随机数、DH公共值等。

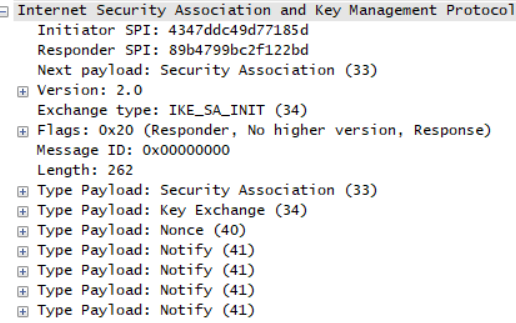


图8-6-3 第二个包

分析第三、四个包：

第三四个包是第二次交换信息（称为IKE\_AUTH交换），该部分以加密方式完成身份认证、对前两条信息的认证和IPSec SA的参数协商。它们对应了IKEv1模式下第五、六个包以及第二阶段quick模式。

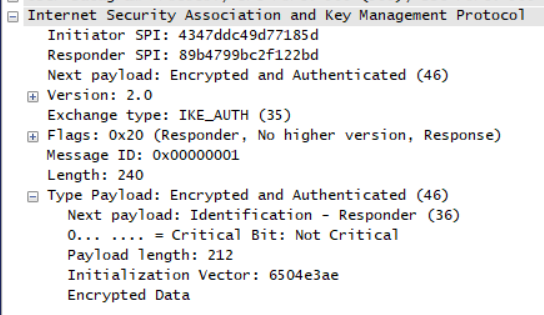


图8-6-4 第三、四个包

**九、总结及心得体会：**

通过本次实验，我基本掌握了IPSec的VPN中网关到网关的配置，而且通过流量分析，进一步理解IPSec协议套。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。

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。

**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：**