IPSec VPN 技术规范

IPSec VPN Technology Specification

国 家 密 码 管 理 局

2010 年 8 月

目　次

目　次 I
前 言 II
引 言 III
1 范围 1
2 规范性引用文件 1
3 术语与缩略语 1
3.1 术语 1
3.2 缩略语 2
4 密码算法和密钥种类 3
4.1 密码算法 3
4.2 密钥种类 3
5 协议 3
5.1 密钥交换协议 3
5.2 安全报文协议 29
6 IPSec VPN 产品要求 37
6.1 产品功能要求 37
6.2 产品性能要求 38
6.3 安全管理要求 38
7 IPSec VPN 产品检测 39
7.1 产品功能检测 39
7.2 产品性能检测 40
7.3 安全管理检测 41
8 合格判定 41
附　录　A IPSec VPN 概述 42
A.1 安全联盟及安全联盟数据库 42
A.1.1 定义和范围 42
A.1.2 安全联盟的功能 42
A.1.3 安全联盟的组合 42
A.2 安全联盟数据库 43
A.2.1 安全策略数据库 43
A.2.2 选择符 43
A.2.3 安全联盟数据库 44

前 言

本规范由国家密码管理局提出。

本规范由国家密码管理局归口。

本规范中的附录A为资料性附录。

本规范主要起草单位：华为技术有限公司、深圳市奥联科技有限公司、深圳市深信服电子科技有限公司、网御神州科技（北京）有限公司、无锡江南信息安全工程技术中心。

本规范主要起草人：刘平、朱志强、董浩、雷建、刘建锋、李小京、邱钢、向明。

引 言

本规范对IPSec VPN的技术协议、产品的功能、性能和管理以及检测进行了规定，可用于指导IPSec VPN产品的研制、检测、使用和管理。

本规范的协议部分主要依据RFC4301、RFC4302、RFC4303、RFC4308、RFC4309等标准制定。按照我国相关密码政策和法规，结合我国实际应用需求及产品生产厂商的实践经验，对密钥协商、密码算法及使用、某些功能项的实施方法提出了一些特定的要求。

基于本规范研制的IPSec VPN产品所用的密码算法和密码部件须经国家密码管理局审批。

本规范内容同国家已发布的标准保持一致性。

本规范中未明确指明为可选要素的部分均为必备要素。

1 范围

本规范对IPSec VPN的技术协议、产品管理和检测进行了规定，可用于指导IPSec VPN产品的研制、检测、使用和管理。

2 规范性引用文件

下列文件中的条款通过本规范的引用而成为本规范的条款。凡是注明日期的引用文件，其随后所有的修改单（不包括勘误的内容）或修订版均不适用于本规范，然而，鼓励根据本规范达成协议的各方研究是否可使用这些文件的最新版本。凡是不注明日期的引用文件，其最新版本适用于本规范。

GB/T 20518-2006 《信息安全技术 公钥基础设施 数字证书格式》

《随机数检测规范》

RFC4301 《因特网安全协议体系》

RFC4302 《IP认证头协议》

RFC4303 《IP封装安全载荷协议》

RFC3947 《在IKE中协商NAT穿越》

RFC3948 《UDP封装IPsec ESP报文》

3 术语与缩略语

3.1 术语

本规范使用下列术语：

3.1.1 密码算法 crypto algorithm

描述密码处理过程的一组运算规则或规程。

3.1.2 密码杂凑算法 cryptographic hash algorithm

又称为密码散列算法或密码哈希算法。它是将一任意长的比特串映射到一个固定长的比特串的运算。满足下列两个特性：

（1）为一个给定的输出找出能映射到该输出的一个输入是计算上不可行的；

（2）为一个给定的输入找出能映射到同一个输出的另一个输入是计算上不可行的。

3.1.3 非对称密码算法/公钥密码算法 asymmetric cryptographic algorithm/public key cryptographic algorithm

加密和解密使用不同密钥的密码算法。其中一个密钥（公钥）可以公开，另一个密钥（私钥）必须保密。由公钥求解私钥在计算上是不可行的。

3.1.4 对称密码算法 symmetric cryptographic algorithm

加解密使用相同密钥的密码算法。密钥必须保密。

3.1.5 分组密码算法 block cipher algorithm

又称块密码算法，一种对称密码算法，将明文划分成固定长度的分组在密钥控制下进行加密。

3.1.6 密码分组链接工作模式 cipher block chaining(CBC)

分组密码算法的一种工作模式，当前的明文分组与前一密文分组进行异或运算后再进行加密。

3.1.7 初始化向量 initialization vector/initialization value（IV）

在密码变换中，为增加安全性或使密码设备同步而引入的用作数据变换的起始点的数。

3.1.8 数据源鉴别 data origin authentication

确认接收到的数据的来源是所声称的。

3.1.9 数字证书 digital certificate

由证书认证机构签名的包含公开密钥拥有者的信息和公开密钥、签发者信息、有效期以及一些扩展信息的数字文件。

3.1.10 安全联盟 security association（SA）

是两个通信实体经协商建立起来的一种协定，它描述了实体如何利用安全服务来进行安全的通信。安全联盟包括了执行各种网络安全服务所需要的所有信息，例如IP层服务（如头认证和载荷封装）、传输层和应用层服务或者协商通信的自我保护。

3.1.11 互联网安全联盟和密钥管理协议 Internet security association and key management protocol （ISAKMP）

互联网安全联盟和密钥管理协议定义了建立、协商、修改和删除安全联盟的过程和报文格式，并定义了交换密钥产生和认证数据的载荷格式。这些格式为传输密钥和认证信息提供了一致的框架。

3.1.12 载荷 payload

是ISAKMP通信双方交换信息的传输形式，是构造ISAKMP消息的基本单位。

3.1.13 IP 安全协议 IP security （IPSec）

一套用于保护IP通信的安全协议。它是IPv4的一个可选协议系列，也是IPv6的组成部分之一，是一个网络层协议，只负责其下层的网络安全，并不负责其上层应用的安全。它提供了两种安全机制：认证（authentication）与加密。

3.1.14 认证 authentication

认证机制使IP通信的数据接收方能够确认数据发送方的真实身份以及数据在传输过程中是否遭到篡改。

3.1.15 加密 encipherment/encryption

对数据进行密码变换以产生密文的过程。

3.1.16 认证头 authentication header（AH）

属于IPSec的一种协议，用于提供IP数据包的数据完整性、数据源鉴别以及抗重放攻击的功能，但不提供数据机密性的功能。

3.1.17 封装安全载荷 encapsulating security payload（ESP）

属于IPSec的一种协议，用于提供IP数据包的机密性、数据完整性以及对数据源鉴别以及抗重放攻击的功能。

3.1.18 虚拟专用网络 virtual private network（VPN）

一种在公共通信基础网络上通过逻辑方式隔离出来的网络。它是一组封闭的网络网段，即使通信与开放系统或其他VPN共享同一主干网络，其通信也是保持分离的。所谓“虚拟”指网络连接特性是逻辑的而不是物理的。在一个虚拟网内，所有用户共享相同的安全策略、优先级服务和管理策略。VPN技术可用于网关与网关之间的连接、网关与端点之间的连接、端点与端点之间的连接。

3.1.19 IPSec 实现 IPSec implementation

具体实现IPSec VPN协议的软硬件产品。

3.2 缩略语

本规范使用下列缩略语：

CBC	密码分组链接工作模式
IV	初始化向量
ISAKMP	互联网安全联盟和密钥管理协议
SA	安全联盟
VPN	虚拟专用网络
IPSec	IP安全协议

AH　　认证头
ESP　　封装安全载荷
NAT　　网络地址转换
HMAC　　带密钥的杂凑运算

4　密码算法和密钥种类

4.1　密码算法

IPSec VPN使用国家密码管理局批准的非对称密码算法、对称密码算法、密码杂凑算法和随机数生成算法。算法及使用方法如下：

——非对称密码算法使用1024比特RSA算法或256比特SM2椭圆曲线密码算法，用于实体验证、数字签名和数字信封等。

——对称密码算法使用128比特分组的SM1分组密码算法，用于密钥协商数据的加密保护和报文数据的加密保护。算法的工作模式使用CBC模式。

——密码杂凑算法使用SHA-1算法或SM3密码杂凑算法，用于对称密钥生成和完整性校验。其中，SM3算法的输出为256比特。

——随机数生成算法生成的随机数应能通过《随机数检测规范》规定的检测。

4.2　密钥种类

IPSec VPN使用下列密钥：

——设备密钥：非对称算法使用的公私钥对，用于实体验证、数字签名和数字信封等。

——工作密钥：在密钥协商第一阶段得到的密钥，用于会话密钥协商过程的保护。

——会话密钥：在密钥协商第二阶段得到的密钥，用于数据报文的加密和完整性保护。

5　协议

5.1　密钥交换协议

密钥交换协议定义了协商、建立、修改、删除安全联盟的过程和报文格式。协议报文使用UDP协议500端口进行传输。

本章节用到的符号如下：

HDR：　一个ISAKMP头。

HDR*：表示ISAKMP头后面的载荷是加密的。

SA：带有一个或多个建议载荷的安全联盟载荷。

IDi：发起方的标识载荷。

IDr：响应方的标识载荷。

HASHi：发起方的杂凑载荷。

HASHr：响应方的杂凑载荷。

SIGi：发起方的签名载荷。

SIGr：响应方的签名载荷。

CERT：证书载荷。

Ni：发起方的 nonce 载荷。

Nr：响应方的 nonce 载荷。

<p>_b：载荷<p>的主体，就是没有ISAKMP通用头的载荷。

pub_i：发起方公钥。

pub_r：响应方公钥。

prv_i：发起方私钥。

prv_r：响应方私钥。

CKY-I：ISAKMP头中的发起方 cookie。

CKY-R：ISAKMP头中的响应方 cookie。

x | y：x 与 y 串接。

[x]：x 为可选。

Asymmetric_Encrypt(msg, pub_key)：使用非对称算法Asymmetric，pub_key作为密钥对输入信息msg_b进行加密，其输出为msg的通用载荷头和密文串接。 如RSA_Encrypt(Ski, pub_key)表示使用RSA算法，使用公钥pub_key对Ski_b进行加密，其输出为Ski的通用载荷头和密文串接。

Asymmetric_Sign (msg, priv_key)：使用非对称算法Asymmetric，priv_key作为密钥对msg进行数字签名。

Symmetric_Encrypt(msg,key)：使用对称算法Symmetric,key作为密钥对输入信息msg_b进行加密，其输出为msg的通用载荷头和密文串接。如SM1_Encrypt (Ni, key)表示使用SM1算法，使用key作为密钥对Ni_b进行加密，其输出为Ni的通用载荷头和密文串接。

Hash(msg)：使用密码杂凑算法对msg进行数据摘要运算。

PRF(key，msg)：使用密钥 key 对消息 msg 进行数据摘要运算。

5.1.1 交换阶段及模式

5.1.1.1 交换阶段

密钥交换协议包括第一阶段和第二阶段。

在第一阶段交换中，通信双方建立了一个ISAKMP SA。该SA是协商双方为保护它们之间的通信而使用的共享策略和密钥。用这个SA来保护IPSec SA的协商过程。一个ISAKMP SA可以用于建立多个IPSec SA。

在第二阶段交换中，通信双方使用第一阶段ISAKMP SA协商建立IPSec SA，IPSec SA是为保护它们之间的数据通信而使用的共享策略和密钥。

5.1.1.2 交换模式

本规范规定了两种交换模式，分别为主模式和快速模式。

主模式用于第一阶段交换，实现通信双方的身份认证和密钥协商，得到工作密钥，该工作密钥用于保护第二阶段的协商过程。

快速模式用于第二阶段交换，实现通信双方IPSec SA的协商，确定通信双方的IPSec安全策略及会话密钥。

5.1.2 交换

交换使用标准ISAKMP载荷语法、属性编码、消息的超时和重传以及通知消息。

安全联盟SA采用的载荷封装形式为：变换载荷封装在建议载荷中，建议载荷封装在安全联盟载荷中。本规范不限制发起方可以发给响应方的提议数量，如果第一阶段交换中有多个变换载荷，应将多个变换载荷封装在一个建议载荷中，然后再将它们封装在一个安全联盟载荷中。有关变换载荷、建议载荷、安全联盟载荷等的具体定义见本规范5.1.4。

在安全联盟的协商期间，响应方不能修改发起方发送的任何提议的属性。否则，交换的发起方应终止协商。

5.1.2.1 第一阶段-主模式

主模式是一个身份保护的交换，其交换过程由6个消息组成。双方身份的认证可采用公私密钥对或数字证书的方式。如果采用公私密钥对的方式，通信双方应事先配置好对方的公钥；如果采用数字证书的方式，发起方应首先拥有响应方的数字证书，并在消息3中发送本方的数字证书。

本阶段涉及的消息头及载荷的具体内容见本规范5.1.4。

主模式的交换过程如下：

消息序列	发起方	方向	响应方
1	HDR, SA	---->	
2		<----	HDR, SA
3	HDR, XCHi, SIGi	---->	
4		<----	HDR, XCHr, SIGr
5	HDR*, HASHi	---->	
6		<----	HDR*, HASHr

消息1　发起方向响应方发送一个封装有建议载荷的安全联盟载荷，而建议载荷中又封装有变换载荷。

消息2　响应方发送一个安全联盟载荷，该载荷表明它所接受的发起方发送的SA提议。安全联盟载荷的具体内容见本规范5.1.4.3。

消息3和4　发起方和响应方交换数据，交换的数据内容包括nonce、身份标识（ID）、可选的证书等载荷。Nonce是生成加密密钥和认证密钥所必需的参数；ID是发起方或响应方的标识。这些数据使用临时密钥Sk进行加密保护，Sk用数字信封保护，最后，双方各自对数据进行数字签名后再加密。

发起方交换的数据如下：

XCHi = Asymmetric_Encrypt(Ski, pub_r) | Symmetric_Encrypt(Ni,Ski) | Symmetric_Encrypt(IDi,Ski) [| Symmetric_Encrypt(CERT,Ski)]

SIGi_b = Asymmetric_Sign(Hash(Ski_b | Ni_b | IDi_b [| CERT_b]), priv_i)

响应方交换的数据如下：

XCHr = Asymmetric_Encrypt(Skr, pub_i) | Symmetric_Encrypt(Nr,Skr) | Symmetric_Encrypt(IDr,Skr)

SIGr_b = Asymmetric_Sign(Hash(Skr_b | Nr_b | IDr_b), priv_r)

上述过程中使用的非对称密码算法、对称密码算法和密码杂凑算法均由消息1和消息2确定。临时密钥Sk由发起方和响应方各自随机生成，其长度应符合对称密码算法对密钥长度的要求。

对称密码运算使用CBC模式，第一个载荷的IV值为0；后续的IV使用前面载荷的最后一组密文。

加密前的交换数据应进行填充，使其长度等于对称密码算法分组长度的整数倍。所有的填充字节的值除最后一个字节外都是0，最后一个填充字节的值为不包括它自己的填充字节数。

当使用证书进行身份验证时，Idi和Idr的类型应使用ID_DER_ASN1_DN。

如果对方证书已经在撤销列表中，系统应发送INVALID_CERTIFICATE通知消息。

消息3和消息4交互完成后，参与通信的双方生成基本密钥参数SKEYID，以生成后续密钥SKEYID_d、SKEYID_a、SKEYID_e，计算方法分别如下：

SKEYID = PRF(Hash(Ni_b | Nr_b), CKY-I | CKY-R)

SKEYID_d = PRF(SKEYID, CKY-I | CKY-R | 0)

SKEYID_a = PRF(SKEYID, SKEYID_d | CKY-I | CKY-R | 1)

SKEYID_e = PRF(SKEYID, SKEYID_a | CKY-I | CKY-R | 2)

上述计算公式中的值0，1，2是单个字节的数值。

SKEYID_e 是ISAKMP SA用来保护其消息机密性所使用的工作密钥。SKEYID_a 是ISAKMP SA用来验证其消息完整性以及数据源身份所使用的工作密钥。SKEYID_d 用于会话密钥的产生。

所有SKEYID的长度都由PRF函数的输出长度决定。如果PRF函数的输出长度太短，不能作为一个密钥来使用，则SKEYID_e应进行扩展。例如，HMAC hash的一个PRF可产生128比特的输出，但密码算法要求用到320比特的密钥。那么，SKEYID_e就需要利用反馈及连接方法加以扩展，直到满足对密钥长度的要求为止。反馈及连接方法如下：

K = K1 | K2 | K3...

K1 = PRF(SKEYID_e, 0)

K2 = PRF(SKEYID_e, K1)

K3 = PRF(SKEYID_e, K2)

...

最后从K的起始位置开始取密码算法的密钥所需要的位数。

消息5和6发起方和响应方认证前面的交换过程。这两个消息中传递的信息使用对称密码算法加密。对称密码算法由消息1和消息2确定，密钥使用SKEYID_e。对称密码运算使用CBC模式，初始化向量IV是消息3中的Ski和消息4中的Skr串连起来经过hash运算得到的，即：

IV= Hash(Ski | Skr)

Hash算法由消息1和消息2确定。

加密前的消息应进行填充，使其长度等于对称密码算法分组长度的整数倍。所有的填充字节的值都是0。报头中的消息长度应包括填充字节的长度，因为这反映了密文的长度。

为了认证交换，发起方产生HASH_I，响应方产生HASH_R，计算公式如下：

HASH_I = PRF(SKEYID, CKY-I | CKY-R | SAi_b | IDi_b)

HASH_R = PRF(SKEYID, CKY-R | CKY-I | SAi_b | IDr_b)

5.1.2.2 第二阶段-快速模式

快速模式交换依赖于第一阶段主模式交换，作为IPSec SA协商过程的一部分协商IPSec SA的安全策略并衍生会话密钥。快速模式交换的信息由ISAKMP SA来保护，即除了ISAKMP头外所有的载荷都要加密。在快速模式中，一个HASH载荷应紧跟在ISAKMP头之后，这个HASH用于消息的完整性校验以及数据源身份验证。

在第二阶段，载荷的加密使用对称密码算法的CBC工作模式，第1个消息的IV是第一阶段的最后一组密文和第二阶段的MsgID进行hash运算所得到的，即：

IV= Hash(第一阶段的最后一组密文 | MsgID)

后续的IV是前一个消息的最后一组密文。消息的填充和第一阶段中的填充方式一样。

在ISAKMP头中的MsgID唯一标识了一个正在进行中的快速模式，而该ISAKMP SA本身又由ISAKMP头中的cookies来标识。因为快速模式的每个实例使用一个唯一的IV，这就有可能基于一个ISAKMP SA的多个快速模式在任一时间内同时进行。

在快速模式协商中，身份标识ID缺省定义为ISAKMP双方的IP地址，并且没有强制规定允许的协议或端口号。如果协商双方需要指定ID，则双方的身份应作为IDi和IDr被依次传递。响应方的本地安全策略将决定是否接受对方的身份标识ID。如果发起方的身份标识ID由于安全策略或其它原因没有被响应方所接受，则响应方应该发送一个通知消息类型为INVALID_ID_INFORMATION (18)的通知载荷。

在通信双方之间有多条隧道同时存在的情况下，身份标识ID为对应的IPSec SA标识并规定通信数据流进入对应的隧道。

本阶段涉及的消息头及载荷的具体内容见本规范5.1.4。

快速模式的交换过程如下：

消息序列	发起方	方向	响应方
1	HDR*, HASH(1), SA, Ni [, IDci, IDcr]	---->	
2		<----	HDR*, HASH(2), SA, Nr [, IDci, IDcr]
3	HDR*, HASH(3)	---->	

消息1　发起方向响应方发送一个杂凑载荷、一个安全联盟载荷（其中封装了一个或多个建议载荷，而每个建议载荷中又封装一个或多个变换载荷）、一个nonce载荷和标识载荷。

杂凑载荷中消息摘要的计算方法如下：

HASH（1）= PRF（SKEYID_a，MsgID | SA | Ni [| IDi | IDr]）

消息2　响应方向发起方发送一个杂凑载荷、一个安全联盟载荷、一个nonce载荷和标识载荷。

杂凑载荷中消息摘要的计算方法如下：

HASH（2）= PRF（SKEYID_a，MsgID | Ni |SA | Nr [| IDi | IDr]）

消息3　发起方向响应方发送一个杂凑载荷，用于对前面的交换进行认证。

杂凑载荷中消息摘要的计算方法如下：

HASH（3）= PRF（SKEYID_a，0 | MsgID | Ni | Nr ）

最后，会话密钥素材定义为：

KEYMAT = PRF(SKEYID_d, protocol | SPI | Ni_b | Nr_b)

其中，protocol和SPI从协商得到的ISAKMP建议载荷中选取。

用于加密的会话密钥和用于完整性校验的会话密钥按照算法要求的长度从KEYMAT中依次选取。先选取用于加密的会话密钥，后选取用于完整性校验的会话密钥。

当PRF函数的输出长度小于KEYMAT需要的密钥素材长度时，需要利用反馈及连接方法加以扩展，直到满足对密钥长度的要求为止。即：

KEYMAT = K1 | K2 | K3 | ...

其中：

K1 = PRF(SKEYID_d, protocol | SPI | Ni_b | Nr_b)

K2 = PRF(SKEYID_d, K1 | protocol | SPI | Ni_b | Nr_b)

K3 = PRF(SKEYID_d, K2 | protocol | SPI | Ni_b | Nr_b)

...

单个SA协商产生两个安全联盟—— 一个入，一个出。每个SA（一个由发起方选择，另一个由响应方选择）的不同的SPI保证了每个方向都有一个不同的KEYMAT。由SA的目的地选择的SPI，被用于衍生该SA的KEYMAT。

5.1.2.3　ISAKMP 信息交换

如果ISAKMP安全联盟已经建立，则ISAKMP信息交换过程如下所示：

发起方	方向	响应方
HDR*, HASH(1), N/D	---->	

其中N/D是一个ISAKMP通知载荷，或是一个ISAKMP删除载荷。HASH(1)的计算方法为：

HASH(1) = PRF(SKEYID_a, MsgID | N/D)

其中，MsgID不能与同一个ISAKMP SA保护的其他第二阶段交换的MsgID相同。

这个消息的加密使用对称密码算法的CBC工作模式，其密钥使用SKEYID_e，初始化向量IV是第一阶段的最后一组密文和MsgID进行hash运算所得到的，即：

IV= Hash(第一阶段的最后一组密文 | MsgID)

消息的填充和第一阶段中的填充方式一样。

如果ISAKMP安全关联在信息交换时还没有建立，则消息以明文发送，即：

发起方	方向	响应方
HDR, N	---->	

5.1.3 NAT 穿越

IPSec穿越NAT特性让IPSec数据流能够穿越网络中的NAT设备。NAT穿越由3个部分组成：首先判断通信的双方是否支持NAT穿越，其次检测双方之间的路径上是否存在NAT，最后决定如何使用UDP封装来处理NAT穿越。

实现NAT穿越的NAT_D载荷分别添加在第一阶段交换过程中消息3和消息4的载荷之后，这些载荷是独立的，不参与交换过程的所有密码运算。支持NAT穿越的第一阶段交换过程如下：

消息序列	发起方	方向	响应方
1	HDR,SA, VID	---->	
2		<----	HDR, SA, VID
3	HDR, XCHi, SIGi, NAT_D, NAT_D	---->	
4		<----	HDR, XCHr, SIGr, NAT_D, NAT_D
5	HDR*#, HASHi	---->	
6		<----	HDR*#, HASHr

#标志说明如果NAT存在，这些包将被发送到修改后的端口。

如果需要，NAT_OA载荷分别添加在第二阶段交换过程中消息1和消息2的载荷之后，同第二阶段的消息载荷一起参与密码运算。

实现 NAT穿越的处理过程和消息格式按RFC3947的规定执行。

5.1.4 密钥交换的载荷格式

5.1.4.1 消息头格式

密钥交换协议消息由一个定长的消息头和不定数量的载荷组成。消息头包含着协议用来保持状态并处理载荷所必须的信息。

ISAKMP的头格式如图5-1-1所示：

发起方cookie			
响应方cookie			
下一个载荷	版本号	交换类型	标志
消息ID			
长度			

图 5-1-1 ISAKMP 头格式

发起方cookie：这个字段是一个唯一的8字节比特串，由发起方随机生成。

响应方cookie：这个字段是一个唯一的8字节比特串，由响应方随机生成。

Cookie的生成方法应参照RFC2408 2.5.3要求生成。

下一个载荷：这个字段为1个字节，说明消息中的第一个载荷的类型。载荷类型的定义如表5-1-1所示：

表 5-1-1 载荷类型的定义

下一个载荷	值
无 (None)	0
安全联盟 (Security association)	1
建议 (Proposal)	2
变换 (Transform)	3
密钥交换 (Key exchange)	4
标识 (Identification)	5
证书 (Certificate)	6
证书请求 (Certificate Request)	7
杂凑 (Hash)	8
签名 (Signature)	9
Nonce	10
通知 (Norigication)	11
删除 (Delete)	12
厂商 (Vendor)	13
属性载荷	14
NAT_D	20
NAT_OA	21
对称密钥载荷（SK）	128
保留 (Reserved)	15-127
私有使用 (PrivateUse)	128-255

版本号：这个字段为1个字节，其中0-3位表示主版本号，4-7位表示次版本号。本规范规定主版本号为1，次版本号为0。

交换类型:这个字段为1个字节,说明组成消息的交换的类型。交换类型的定义如表5-1-2所示：

表 5-1-2 交换类型的定义

交换类型	分配的值
无 (None)	0
基本 (Base)	1
身份保护 (Identity protection)	2
仅认证 (Authentication only)	3
信息 (Informational)	5
将来使用 (Future use)	6-31
DOI具体使用	32-239
私有使用 (Private use)	240-255

本规范规定密钥交换第一阶段使用的交换类型为身份保护类型即主模式，其值为2。第二阶段交换使用的快速模式所分配的值为32。

标志：这个字段的长度为1个字节，说明为密钥交换协议设置的具体选项。目前使用了这个域的前3个比特，其他比特在传输前被置为0。具体定义如下：

——加密比特：这是标志字段中的最低有效比特。当这个比特被置为 1 时，该消息头后面所有的载荷都采用 ISAKMP SA 中指定的密码算法加密。当这个比特被置为 0 时，载荷不加密。

——提交比特：这是标志字段的第 2 个比特，本规范中其值为 0。

——仅认证比特：这是标志字段的第 3 个比特，本规范中其值为 0。

消息ID：这个字段的长度为4字节，第一阶段中该字段为0，在第二阶段为发起方生成的随机数。它作为惟一的消息标志，用于在第二阶段的协商中标识协议状态。

长度：这个字段的长度为4字节，以字节为单位标明包含消息头和载荷在内的整个消息长度。

5.1.4.2 通用载荷头

每个载荷由通用载荷头开始。通用载荷头定义了载荷的边界，所以就可以联接不同的载荷。通用载荷头的定义如图5-1-2所示：

下一个载荷	保留	载荷长度

图 5-1-2 通用载荷头格式

下一个载荷：这个字段的长度为1个字节，标识了本载荷后下一个载荷的类型。如果当前载荷是最后一个，则该字段将被置为0。载荷类型由表5-1-1定义。

保留：这个字段的长度为1个字节，其值为0。

载荷长度：这个字段的长度为2个字节，以字节为单位标明包含通用载荷头在内的整个载荷长度。

5.1.4.3 安全联盟载荷

安全联盟载荷用于协商SA，并且指定协商所基于的解释域DOI。安全联盟的格式依赖于他使用的DOI，本载荷的类型值为1。安全联盟载荷的格式如图5-1-3所示：

下一个载荷	保留	载荷长度
解释域（DOI）		
情形		

图 5-1-3 安全联盟载荷格式

下一个载荷：这个字段的长度为1个字节，标识了本载荷后下一个载荷的类型。如果当前载荷是最后一个，则该字段将被置为0。载荷类型由表5-1-1定义。

保留：这个字段的长度为1个字节，其值为0。

载荷长度：这个字段的长度为2个字节，以字节为单位标明整个安全联盟载荷的长度，计算范围包括SA载荷、所有建议载荷、和所有与被提议的安全联盟有关的变换载荷。

解释域DOI：这个字段长度为4个字节，其值为无符号整数，它指定协商所基于的DOI，这个字段的值为1。

情形：这个字段长度为4个字节，表明协商发生时的情形，用来决定需要的安全服务的信息。定义如下：

——SIT_IDENTITY_ONLY：其值为 1。表明 SA 将由一个相关的标识载荷中的源标识信息来标识。

——SIT_SECRECY：其值为 2。表明 SA 正在一个需经标记的秘密的环境中协商。

——SIT_INTEGRITY：其值是 4。表明 SA 正在一个须经标记的完整性环境中协商。

本规范默认采用SIT_IDENTITY_ONLY情形。

5.1.4.4 建议载荷

建议载荷用于密钥交换的发起方告知响应方它优先选择的安全协议以及希望协商中的SA采用的相关安全机制，本载荷的类型值为2。建议载荷的格式如图5-1-4所示：

下一个载荷	保留	载荷长度	
建议号	协议ID	SPI长度	变换数
变长的SPI			

图 5-1-4 建议载荷格式

下一个载荷：这个字段的长度为1个字节，如果后面还有建议载荷，其值为2，否则应为0。

保留：这个字段的长度为1个字节，其值为0。

载荷长度：这个字段的长度为2个字节，以字节为单位标明整个建议载荷的长度。计算范围包括包括通用载荷头、建议载荷、和所有与该建议有关的变换载荷，该长度仅用于标明本建议载荷的长度。

建议号：这个字段的长度为1个字节，标明本建议载荷的建议编号。多个建议的建议号相同标明这些建议是“逻辑与”的关系，不同标明这些建议是“逻辑或”的关系。单调递增的建议号表示对建议的优先选择顺序，建议号越小优先权越高。

协议ID：这个字段的长度为1个字节，标明协议标识符。协议标识符的定义如表5-1-3所示：

表 5-1-3 协议标识符的定义

协议标识符	描述	值
RESERVED	未分配	0
PROTO_ISAKMP	ISAKMP的协议标识符	1
PROTO_IPSec_AH	AH的协议标识符	2
PROTO_IPSec_ESP	ESP的协议标识符	3
PROTO_IPCOMP	IP压缩的协议标识符	4

SPI长度：这个字段的长度为1个字节，以字节为单位标明SPI的长度。在第一阶段该长度为0，在第二阶段该长度为4。

变换数：这个字段的长度为1个字节，标明建议的变换载荷个数。

变长的SPI：在第一阶段没有这个字段，在第二阶段这个字段的长度为4个字节，其内容是该建议的提出者产生的随机数。

5.1.4.5 变换载荷

变换载荷用于密钥交换的发起方告知响应方为一个指定的协议提供不同的安全机制，本载荷的类型值为3。变换载荷的格式如图5-1-5所示：

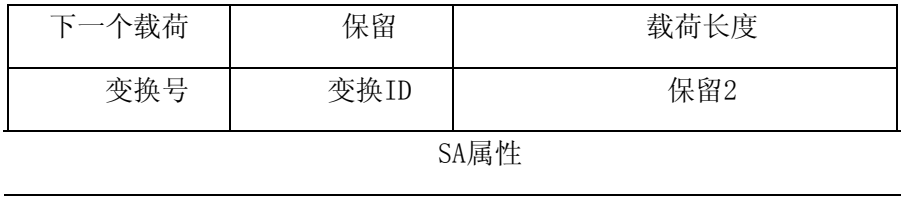

图 5-1-5 变换载荷格式

下一个载荷：这个字段的长度为1个字节，如果后面还有变换载荷，其值为3，否则应为0。

保留：这个字段的长度为1个字节，其值为0。

载荷长度：这个字段的长度为2个字节，以字节为单位标明本变换载荷的长度。计算范围包括通用载荷头、变换载荷和所有的SA属性载荷。

变换号：这个字段的长度为1个字节，标明本变换载荷的变换编号。单调递增的变换号表示对变换的优先选择顺序，变换号越小优先权越高。

变换ID：这个字段的长度为1个字节，标明建议协议的变换标识符。在第一阶段该字段的值为1，在第二阶段根据不同的协议选用不同的变换ID。AH协议的变换ID的定义如表5-1-4所示，ESP协议的变换ID的定义如表5-1-5所示：

表 5-1-4 AH 协议的变换 ID 的定义

变换ID	描述	值
RESERVED	未使用	0-1
AH_SHA	使用SHA-1杂凑算法的HMAC	3
AH_SM3	使用带256比特SM3密码杂凑算法的HMAC	20

表 5-1-5 ESP 协议的变换 ID 的定义

变换ID	描述	值
RESERVED	未使用	0
ESP_SM1	SM1分组密码算法	128

保留2：这个字段的长度为2个字节，其值为0。

SA属性：该字段的长度是可变的，标明本变换的SA属性。该字段的具体定义见本规范5.1.4.6。

5.1.4.6 SA 属性载荷

SA属性载荷只能用于变换载荷之后，并且没有通用载荷头，用于表示SA属性的数据结构，本载荷的类型值为14。SA属性载荷的格式如图5-1-6所示：

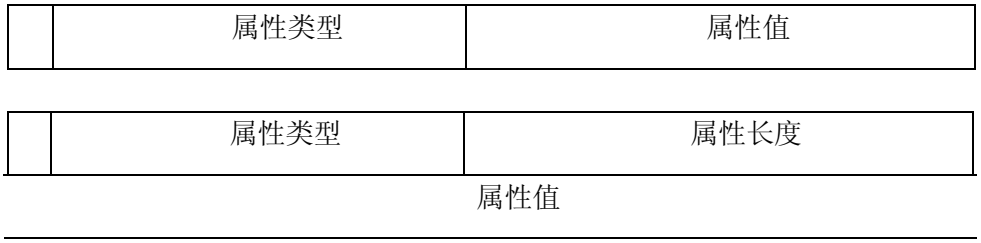

图 5-1-6 SA 属性载荷格式

属性类型：这个字段的长度为2个字节，标明属性类型。该字段的最高有效比特（比特0）如果为0，属性值是变长的，并且本载荷有3个字段，分别是属性类型、属性长度和属性值。如果属性类型最高有效比特为1，属性值是定长的并且本载荷仅有2个字段，分别是属性类型和属性值。

第一阶段密钥协商属性类型的定义如表5-1-6所示：

表 5-1-6 第一阶段密钥协商属性类型的定义

分类	值	长度
加密算法	1	定长
HASH算法	2	定长
认证方式	3	定长
交换组	4	定长
交换群类型	5	定长
群素数/不可约多项式	6	变长
群产生器1	7	变长
群产生器2	8	变长
群曲线A	9	变长
群曲线B	10	变长
SA生存期类型	11	定长
SA生存期 (SA Life Duration)	12	变长
伪随机函数（PRF）	13	定长
密钥长度	14	定长
字段大小	15	定长

群顺序	16	变长
块大小	17	定长
非对称算法类型	20	定长

第二阶段密钥协商属性类型的定义如表5-1-7所示：

表 5-1-7 第二阶段密钥协商属性类型的定义

分类	值	长度
SA生存类型 (SA Life Type)	1	定长
SA生存期 (SA Life Duration)	2	变长
组描述 (Group Description)	3	定长
封装模式 (Encapsulation Mode)	4	定长
认证算法 (Authentication Algorithm)	5	定长
密钥长度 (Key Length)	6	定长
密钥轮数 (Key Rounds)	7	定长
压缩字典长度 (Compress Dictionary Size)	8	定长
私有压缩算法 (Compress Private Algorithm)	9	变长

属性值：这个字段如果是定长的，其长度为2个字节。如果是变长的，其长度由属性长度字段指定。

属性长度：当属性值是变长时，该字段标明属性值的长度。

第一阶段加密算法属性值的定义如表5-1-8所示：

表 5-1-8 第一阶段加密算法属性值的定义

名称	描述	值
ENC_ALG_SM1	SM1分组密码算法	128

第一阶段密码杂凑算法属性值的定义如表5-1-9所示：

表 5-1-9 第一阶段密码杂凑算法属性值的定义

名称	描述	值
HASH_ALG_SHA	SHA-1密码杂凑算法	2
HASH_ALG_SM3	SM3密码杂凑算法	20

第一阶段认证方式属性值的定义如表5-1-10所示：

表 5-1-10 第一阶段认证方式属性值的定义

名称	描述	值
AUTH_METHOD_DE	公钥数字信封认证方式	10

SA生存期类型属性值的定义适用于第一阶段和第二阶段，如表5-1-11所示：

表 5-1-11 SA 生存期类型属性值的定义

名称	描述	值
SA_LD_TYPE_SEC	秒	1
SA_LD_TYPE_KB	千字节	2

第一阶段公钥算法类型属性值的定义如表5-1-12所示：

表 5-1-12 第一阶段公钥算法类型属性值的定义

名称	描述	值
ASYMMETRIC_RSA	RSA 公钥密码算法	1
ASYMMETRIC_SM2	SM2椭圆曲线密码算法	2

第二阶段封装模式属性值的定义如表5-1-13所示：

表 5-1-13 第二阶段封装模式属性值的定义

名称	描述	值
RESERVED	使用	0
ENC_MODE_TUNNEL	隧道模式	1
ENC_MODE_TRNS	传输模式	2
ENC_MODE_UDPTUNNEL_RFC	NAT穿越隧道模式	3
ENC_MODE_UDPTRNS_RFC	NAT穿越传输模式	4

第二阶段认证算法属性值的定义如表5-1-14所示：

表 5-1-14 第二阶段认证算法属性值的定义

名称	描述	值
RESERVED	使用	0
HMAC_SHA	SHA-1密码杂凑算法的HMAC	2
HMAC_SM3	SM3密码杂凑算法的HMAC	20

5.1.4.7 标识载荷

标识载荷用于通信双方交换身份信息，该信息用于确认通信双方的身份，本载荷的类型值为5。标识载荷的格式如图5-1-7所示：

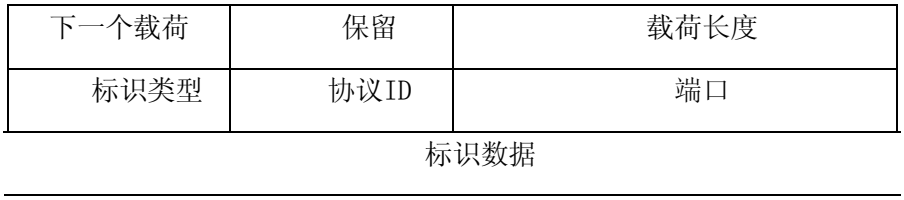

图 5-1-7 标识载荷格式

下一个载荷：这个字段的长度为1个字节，标识了本载荷后下一个载荷的类型。如果当前载荷是最后一个，则该字段将被置为0。载荷类型由表5-1-1定义。

保留：这个字段的长度为1个字节，其值为0。

载荷长度：这个字段的长度为2个字节，以字节为单位标明包含通用载荷头在内的整个载荷长度。

标识类型：这个字段的长度为1个字节，标明标识数据字段中的身份信息类型。标识类型的定义如表5-1-15所示：

表 5-1-15 标识类型的定义

ID类型	描　述	值
RESERVED	未使用	0
ID_IPv4_ADDR	一个单独的4字节IPv4地址	1
ID_FQDN	完全合格的域名字符串	2
ID_USER_FQDN	完全合格的用户名字符串	3
ID_IPv4_ADDR_SUBNET	带有4字节子网掩码的IPv4地址	4
ID_IPv6_ADDR	一个单独的16字节IPv6地址	5
ID_IPv6_ADDR_SUBNET	一个带有16字节子网掩码的IPv6地址	6
ID_IPv4_ADDR_RANGE	一个IPv4的地址范围	7
ID_IPV6_ADDR_RANGE	一个IPv6的地址范围	8
ID_DER_ASN1_DN	一个ASN.1X.500的文本编码	9
ID_DER_ASN1_GN	一个ASN.1X.500的二进制编码	10
ID_KEY_ID	用于传递特定厂商信息的字节流	11

在第一阶段可以使用的标识类型为：

ID_IPv4_ADDR

ID_IPv6_ADDR

ID_DER_ASN1_DN

ID_DER_ASN1_GN

ID_FQDN

ID_USER_FQDN

ID_KEY_ID

在第二阶段可以使用的标识类型为：

ID_IPv4_ADDR

ID_IPv6_ADDR

ID_IPv4_ADDR_SUBNET

ID_IPv6_ADDR_SUBNET

ID_IPv4_ADDR_RANGE

ID_IPV6_ADDR_RANGE

协议ID：这个字段的长度为1个字节，标明一个IP协议的上层协议号。值为0表明忽略这个字段，在第一阶段这个值应为0。在第二阶段是用户配置的安全策略五元组的协议，值为0表明忽略这个字段。

端口：这个字段的长度为2个字节，标明一个上层协议的端口。值为0表明忽略这个字段，在第一阶段这个值应为0。在第二阶段是用户配置的安全策略五元组的端口，值为0表明忽略这个字段。

标识数据：这个字段是变长的，标明与ID类型字段相对应的标识信息。

5.1.4.8 证书载荷

证书载荷用于通信双方交换证书以及证书相关信息，本载荷的类型值为6。

证书载荷的格式如图5-1-8所示：

图 5-1-8 证书载荷格式

下一个载荷：这个字段的长度为1个字节，标识了本载荷后下一个载荷的类型。如果当前载荷是最后一个，则该字段将被置为0。载荷类型由表5-1-1定义。

保留：这个字段的长度为1个字节，其值为0。

载荷长度：这个字段的长度为2个字节，以字节为单位标明包含通用载荷头在内的整个载荷长度。

证书编码：这个字段的长度为1个字节，标明证书数据字段的证书编码类型。证书编码类型定义如表5-1-16所示：

表 5-1-16 证书编码类型定义

证书类型	值
无 (NONE)	0
PKCS#7封装的X.509证书	1
PGP证书	2
DNS已签名密钥	3
X.509签名证书	4
X.509密钥交换证书	5
Kerberos令牌	6
CRL（证书吊销列表）	7
ARL（机构吊销列表）	8
SPKI证书	9
X.509属性证书	10
保留	11-255

在本规范中，只能使用X.509签名证书。

证书数据：这个字段是变长字段，标明证书。证书的结构及定义参见GB/T 20518-2006《信息安全技术 公钥基础设施 数字证书格式》。

5.1.4.9 杂凑载荷

杂凑载荷的内容是在SA协商过程中选定的密码杂凑算法生成的数据，本载荷的类型值为8。杂凑载荷的格式如图5-1-9所示：

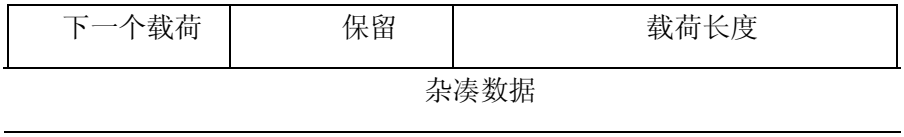

图 5-1-9 杂凑载荷格式

下一个载荷：这个字段的长度为1个字节，标识了本载荷后下一个载荷的类型。如果当前载荷是最后一个，则该字段将被置为0。载荷类型由表5-1-1定义。

保留：这个字段的长度为1个字节，其值为0。

载荷长度：这个字段的长度为2个字节，以字节为单位标明包含通用载荷头在内的整个载荷长度。

杂凑数据：这个字段的长度是变长的，其内容为密码杂凑算法生成的数据。

5.1.4.10 签名载荷

签名载荷的内容是在SA协商过程中的数字签名算法生成的数据，本载荷的类型值为9。签名载荷的格式如图5-1-10所示：

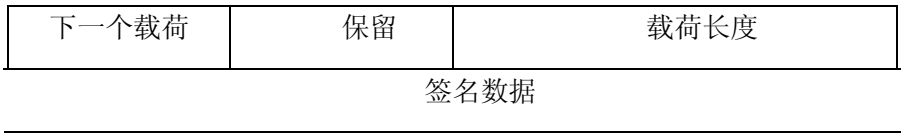

图 5-1-10 签名载荷格式

下一个载荷：这个字段的长度为1个字节，标识了本载荷后下一个载荷的类型。如果当前载荷是最后一个，则该字段将被置为0。载荷类型由表5-1-1定义。

保留：这个字段的长度为1个字节，其值为0。

载荷长度：这个字段的长度为2个字节，以字节为单位标明包含通用载荷头在内的整个载荷长度。

签名数据：这个字段的长度是变长的，其内容为签名算法生成的数据。

5.1.4.11 Nonce 载荷

Nonce载荷的内容是用于保护交换数据的随机数据，本载荷的类型值为10。Nonce载荷的格式如图5-1-11所示：

图 5-1-11 Nonce 载荷格式

下一个载荷：这个字段的长度为1个字节，标识了本载荷后下一个载荷的类型。如果当前载荷是最后一个，则该字段将被置为0。载荷类型由表5-1-1定义。

保留：这个字段的长度为1个字节，其值为0。

载荷长度：这个字段的长度为2个字节，以字节为单位标明包含通用载荷头在内的整个载荷长度。

Nonce数据：这个字段的长度是变长的，其内容为随机数。

5.1.4.12 通知载荷

通知载荷用于传送通知数据，本载荷的类型值为11，通知载荷的格式如图5-1-12所示：

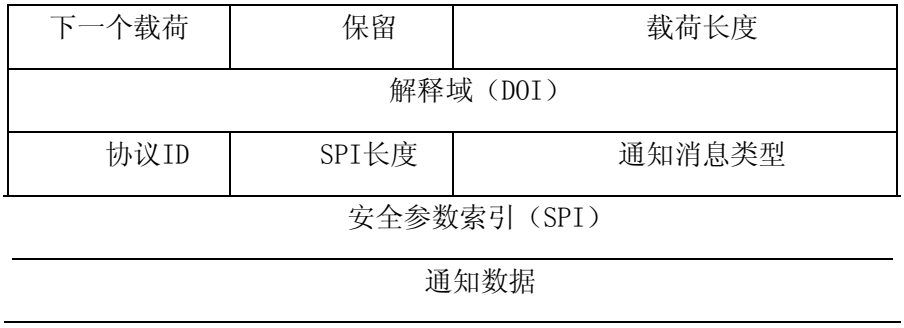

图 5-1-12 通知载荷格式

下一个载荷：这个字段的长度为1个字节，标识了本载荷后下一个载荷的类型。如果当前载荷是最后一个，则该字段将被置为0。载荷类型由表5-1-1定义。

保留：这个字段的长度为1个字节，其值为0。

载荷长度：这个字段的长度为2个字节，以字节为单位标明包含通用载荷头在内的整个载荷长度。

解释域（DOI）：这个字段的长度为4个字节，这个字段的值为1。

协议ID：这个字段的长度为1个字节，标明协议标识符。协议标识符的定义如表5-1-3所示。

SPI长度：这个字段的长度为1个字节，以字节为单位标明SPI的长度。在第一阶段该长度为0，在第二阶段该长度为4。

通知消息类型：这个字段的长度为2个字节，标明通知消息类型。通知消息的错误类型如表5-1-17所示，通知消息的状态类型如表5-1-18所示：

表 5-1-17 通知消息的状态类型

通知类型	描述	值
INVALID_PAYLOAD_TYPE	无效的载荷类型	1
DOI_NOT_SUPPORTED	不支持的DOI	2
SITUATION_NOT_SUPPORTED	不支持的SITUATION	3
INVALID_COOKIE	无效的COOKIE	4
INVALID_MAJOR_VERSION	无效的主版本	5
INVALID_MINOR_VERSION	无效的微版本	6
INVALID_EXCHANGE_TYPE	无效的交换类型	7
INVALID_FLAGS	无效的标志	8
INVALID_MESSAGE_ID	无效的消息ID	9
INVALID_PROTOCOL_ID	无效的协议号	10
INVALID_SPI	无效的SPI	11
INVALID_TRANSFORM_ID	无效的变换号	12
ATTRIBUTES_NOT_SUPPORTED	不支持的属性	13
NO_PROPOSAL_CHOSEN	建议不被接受	14
BAD_PROPOSAL_SYNTAX	错误的建议语法	15
PAYLOAD_MALFORMED	错误的载荷格式	16
INVALID_KEY_INFORMATION	无效的密钥信息	17
INVALID_ID_INFORMATION	无效的ID信息	18

INVALID_CERT_ENCODING	无效的证书编码	19
INVALID_CERTIFICATE	无效的证书	20
CERT_TYPE_UNSUPPORTED	不支持的证书类型	21
INVALID_CERT_AUTHORITY	无效的证书机构	22
INVALID_HASH_INFORMATION	无效的HASH信息	23
AUTHENTICATION_FALIED	失败的鉴别	24
INVALID_SIGNATURE	无效的签名	25
ADDRESS_NOTIFICATION	地址通知	26
NOTIFY_SA_LIFETIME	安全联盟生存周期通知	27
CERTFICATE_UNAVAILABLE	证书不可用	28
UNSUPPORTED_EXCHANGE_TYPE	不支持的交换类型	29
UNEQUAL_PAYLOAD_LENGTHS	错误的载荷长度	30
RESERVED	保留	31-8191
PRIVATE	私有	8192-16383

表 5-1-18 通知消息的状态类型

通知类型	值
已连接	16384
保留（将来使用）	16385-24575
特定于DOI的编码	24576-32767
私有（将来使用）	32768-40959
保留（将来使用）	40960-65535

SPI：在第一阶段没有这个字段。在第二阶段这个字段的长度为4个字节，其内容是接收方建议载荷中的SPI值。

通知数据：这个字段是变长的，用于传送通知消息类型对应的通知数据。

5.1.4.13 删除载荷

删除载荷用于通知对方某个SA已经取消，本载荷的类型值为12。删除载荷的格式如图5-1-13所示：

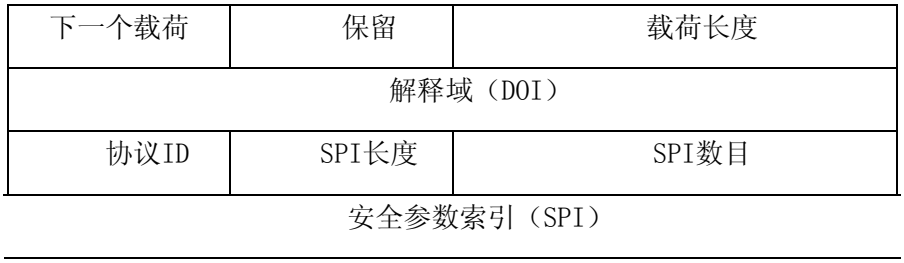

图 5-1-13 删除载荷格式

下一个载荷：这个字段的长度为1个字节，标识了本载荷后下一个载荷的类型。如果当前载荷是最后一个，则该字段将被置为0。载荷类型由表5-1-1定义。

保留：这个字段的长度为1个字节，其值为0。

载荷长度：这个字段的长度为2个字节，以字节为单位标明包含通用载荷头在内的整个载荷长度。

解释域（DOI）：这个字段的长度为4个字节，其值为1。

协议ID：这个字段的长度为1个字节，标明要删除的SA的协议标识符。协议标识符的定义如表5-1-3所示。

SPI长度：这个字段的长度为1个字节，以字节为单位标明SPI的长度。删除第一阶段的SA时该长度为16，删除第二阶段的SA时该长度为4。

SPI数目：这个字段的长度为2个字节，标明本载荷中包含的SPI数目。

安全参数索引（SPI）：这个字段是变长的，标明被删除SA的SPI。这个字段的长度由SPI长度字段和SPI数目字段的值决定。

5.1.4.14 厂商 ID 载荷

厂商ID载荷用于传递厂商自定义的常量，本载荷的类型值为13。厂商ID载荷的格式如图5-1-14所示：

图 5-1-14 厂商 ID 载荷格式

下一个载荷：这个字段的长度为1个字节，标识了本载荷后下一个载荷的类型。如果当前载荷是最后一个，则该字段将被置为0。载荷类型由表5-1-1定义。

保留：这个字段的长度为1个字节，其值为0。

载荷长度：这个字段的长度为2个字节，以字节为单位标明包含通用载荷头在内的整个载荷长度。

厂商ID（VID）：这个字段是变长的，其内容为厂商ID串的杂凑值。

5.1.4.15 NAT_D 载荷

NAT_D载荷用于检测两个密钥交换通信方之间是否存在NAT设备，以及检测NAT设备的确切位置，本载荷的类型值为20。NAT_D载荷的格式如图5-1-15所示：

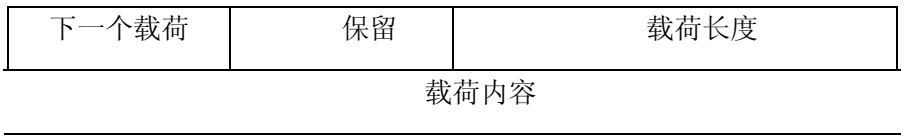

图 5-1-15 NAT_D 载荷格式

下一个载荷：这个字段的长度为1个字节，标识了本载荷后下一个载荷的类型。如果当前载荷是最后一个，则该字段将被置为0。载荷类型由表5-1-1定义。

保留：这个字段的长度为1个字节，其值为0。

载荷长度：这个字段的长度为2个字节，以字节为单位标明包含通用载荷头在内的整个载荷长度。

载荷内容：这个字段是变长的，其内容为：

HASH = Hash(CKY-I | CKY-R | IP | Port)

5.1.4.16 NAT_OA 载荷

NAT_OA载荷用于密钥协商第二阶段中，当使用传输模式穿越NAT时需要传送这个载荷，本载荷的类型值为21。NAT_OA载荷的载荷格式如图5-1-16所示：

下一个载荷	保留	载荷长度
ID类型	保留2	
NAT_OA数据		

图 5-1-16 NAT_OA 载荷格式

下一个载荷：这个字段的长度为1个字节，标识了本载荷后下一个载荷的类型。如果当前载荷是最后一个，则该字段将被置为0。载荷类型由表5-1-1定义。

保留：这个字段的长度为1个字节，其值为0。

载荷长度：这个字段的长度为2个字节，以字节为单位标明包含通用载荷头在内的整个载荷长度。

ID类型：这个字段的长度为1个字节，其值为表5-1-15中的ID_IPV4_ADDR的值或ID_IPV6_ADDR的值。

保留2：这个字段的长度为3个字节，其值为0。

NAT_OA数据：这个字段的值是4字节IPv4地址或16字节IPv6地址。

5.1.4.17 对称密钥载荷

对称密钥载荷用于在密钥交换第一阶段时，传递数字信封中的对称密钥，本载荷的类型值为128。对称密钥载荷的格式如图5-1-17所示：

下一个载荷	保留	载荷长度
对称密钥密文		

图 5-1-17 对称密钥载荷格式

下一个载荷：这个字段的长度为1个字节，标识了本载荷后下一个载荷的类型。如果当前载荷是最后一个，则该字段将被置为0。载荷类型由表5-1-1定义。

保留：这个字段的长度为1个字节，其值为0。

载荷长度：这个字段的长度为2个字节，以字节为单位标明包含通用载荷头在内的整个载荷长度。

对称密钥密文：这个字段的长度是可变的，其内容为由公钥加密的对称密钥。

5.1.5 密钥交换的数据包格式

密钥交换消息是基于UDP传输的，使用UDP 500端口或者4500端口。在UDP 500 端口上发送的密钥交换消息直接跟在UDP 报头后面。在UDP 4500 端口上发送的密钥交换消息，需要在UDP头与密钥交换消息之间插入4个全0的字节。

每一条密钥交换消息以消息头HDR 作为开始标志。每个HDR后可以有一个或者多个载荷。如果有多个载荷，则用每一个载荷内的“下一个载荷”字段进行标识，如果“下一个载荷”字段为0，说明消息结束。

在本节的所有图中，“下一载荷”用“NP”来表示。

5.1.5.1 主模式消息 1 的数据包格式

主模式消息1的数据包的格式如图5-1-18所示，其中SA载荷中有SM1-SHA1和SM1-SM3两种变换载荷。

发起方cookie			
响应方cookie			
NP SA：1	版本号:0x10	交换类型	标志：0
消息ID：0			
长度			
NP ：0	保留：0	载荷长度	
DOI：1			
情形：1			
NP NULL：0	保留：0	载荷长度	
建议号1	协议ID：1	SPI长度0	变换载荷数：2
NP变换：3	保留：0	载荷长度	
变换号1	变换ID：1	载荷长度	

首选变换中各属性载荷

NP NULL：0	保留：0	载荷长度
变换号2	变换ID：1	载荷长度

备选变换中各属性载荷

图 5-1-18 主模式消息 1 的数据包格式

5.1.5.2 主模式消息 2 的数据包格式

主模式消息2的数据包的格式如图5-1-19所示，其中SA载荷中选择了SM1-SHA1变换。下图中NP代表下一载荷。

发起方cookie			
响应方cookie			
NP SA：1	版本号:0x10	交换类型	标志：0
消息ID：0			
长度			
NP NULL：0	保留：0	载荷长度	
DOI：1			
情形：1			
NP NULL：0	保留：0	载荷长度	

建议号1	协议ID：1	SPI长度0	变换载荷数：2
NP NULL：0	保留：0	载荷长度	
变换号1	变换ID：1	载荷长度	
变换中各属性载荷			

图 5-1-19 主模式消息 2 的数据包格式

5.1.5.3 主模式消息 3 的数据包格式

使用证书认证的主模式消息3数据包的格式如图5-1-20所示：

发起方cookie			
响应方cookie			
NP 对称密钥:128	版本号:0x10	交换类型	标志：0
消息ID：0			
长度			
NP Nonce：10	保留：0	载荷长度	
受公钥加密的对称密钥			
NP 标识：5	保留：0	载荷长度	
受对称密钥加密的Nonce数据			
NP 证书：6	保留：0	载荷长度	
ID类型	协议ID：0	端口：0	
受对称密钥加密的标识数据			
NP 签名：9	保留：0	载荷长度	
证书编码	证书数据		
受对称密钥加密的证书数据			
NP NULL：0	保留：0	载荷长度	
签名数据			

图 5-1-20 使用证书的主模式消息 3 的数据包格式

使用公私密钥对认证的主模式消息3数据包的格式如图5-1-21所示：

发起方cookie			
响应方cookie			
NP 对称密钥:128	版本号:0x10	交换类型	标志：0
消息ID：0			
长度			
NP Nonce：10	保留：0	载荷长度	
受公钥加密的对称密钥			
NP 标识：5	保留：0	载荷长度	
受对称密钥加密的Nonce数据			
NP 签名：9	保留：0	载荷长度	
ID类型	协议ID：0	端口：0	
受对称密钥加密的标识数据			
NP NULL：0	保留：0	载荷长度	
签名数据			

图 5-1-21 使用公私钥对的主模式消息 3 的数据包格式

5.1.5.4 主模式消息 4 的数据包格式

主模式消息4数据包的格式如图5-1-22所示：

发起方cookie			
响应方cookie			
NP 对称密钥:128	版本号:0x10	交换类型	标志：0
消息ID：0			
长度			
NP Nonce：10	保留：0	载荷长度	
受公钥加密的对称密钥			
NP 标识：5	保留：0	载荷长度	
受对称密钥加密的Nonce数据			
NP 签名：9	保留：0	载荷长度	
ID类型	协议ID：0	端口：0	
受对称密钥加密的标识数据			

NP NULL：0	保留：0	载荷长度
签名数据		

图 5-1-22 主模式消息 4 的数据包格式

5.1.5.5 主模式第消息 5 的数据包格式

主模式消息5的数据包的格式如图5-1-23所示：

发起方cookie			
响应方cookie			
NP 杂凑：8	版本号:0x10	交换类型	标志：1
消息ID：0			
长度			
NP NULL：0	保留：0	载荷长度	
杂凑载荷			

图 5-1-23 主模式消息 5 的数据包格式

5.1.5.6 主模式第消息 6 的数据包格式

主模式消息6的数据包的格式如图5-1-24所示：

发起方cookie			
响应方cookie			
NP 杂凑：8	版本号:0x10	交换类型	标志：1
消息ID：0			
长度			
NP NULL：0	保留：0	载荷长度	
杂凑载荷			

图 5-1-24 主模式消息 6 的数据包格式

5.1.5.7 快速模式消息 1 的数据包格式

快速模式消息1的数据包的格式如图5-1-25所示，其中SA载荷中有一个ESP协议建议，建议中有两种变换。

发起方cookie			
响应方cookie			
NP 杂凑：8	版本号:0x10	交换类型	标志：1

消息ID：随机产生			
长度			
NP SA：1	保留：0	载荷长度	

杂凑载荷

NP Nonce：10	保留：0	载荷长度	
DOI：1			
情形：1			
NP NULL：0	保留：0	载荷长度	
建议号1	协议ID：3	SPI长度	变换载荷数

SPI

NP 变换：3	保留：0	载荷长度
变换号1	变换ID：128	载荷长度

首选变换中各属性载荷

NP NULL：0	保留：0	载荷长度
变换号2	变换ID：128	载荷长度

备选变换中各属性载荷

NP 标识：5	保留：0	载荷长度

Nonce数据

NP 标识：5	保留：0	载荷长度
ID类型	协议ID：0	端口：0

标识数据

0	保留：0	载荷长度
ID类型	协议ID：0	端口：0

标识数据

图 5-1-25 快速模式消息 1 的数据包格式

5.1.5.8 快速模式消息 2 的数据包格式

快速模式消息2的数据包的格式如图5-1-26所示，其中选择了其中一种变换。

发起方cookie
响应方cookie

NP 杂凑：8	版本号:0x10	交换类型	标志：1
消息ID：随机产生			
长度			
NP SA：1	保留：0	载荷长度	

杂凑载荷

NP Nonce：10	保留：0	载荷长度	
DOI：1			
情形：1			
NP NULL：0	保留：0	载荷长度	
建议号1	协议ID：3	SPI长度	变换载荷数

SPI

NP NULL：0	保留：0	载荷长度
变换号1	变换ID：128	载荷长度

变换中各属性载荷

NP 标识：5	保留：0	载荷长度

Nonce数据

NP 标识：5	保留：0	载荷长度
ID类型	协议ID：0	端口：0

标识数据

NP NULL：0	保留：0	载荷长度
ID类型	协议ID：0	端口：0

标识数据

图 5-1-26 快速模式消息 2 的数据包格式

5.1.5.9 快速模式消息 3 的数据包格式

快速模式消息3的数据包的格式如图5-1-27所示：

发起方cookie			
响应方cookie			
NP 杂凑：8	版本号:0x10	交换类型	标志：1
消息ID：随机产生			

长度		
NP NULL：0	保留：0	载荷长度

新建外部 IP 头*

图 5-1-27 快速模式消息 3 的数据包格式

5.2 安全报文协议

5.2.1 认证头协议 AH

5.2.1.1 概述

认证头协议AH用于为IP数据报文提供无连接的完整性、数据源鉴别和抗重放攻击服务。AH为IP头提供尽可能多的认证，同时为上层协议数据提供认证。对于抗重放攻击服务，AH依靠一个单调递增的抗重放攻击序列号来完成。AH不能提供机密性服务，因此本规范规定AH不能单独使用，而应和封装安全载荷协议ESP嵌套使用。

5.2.1.2 AH 头格式

AH头格式见图5-2-1，该格式里的所有字段都是强制的，并且被包括在完整性校验值（ICV）计算中。AH头紧跟在IP协议头（IPv4、IPv6、或者扩展）之后，在IP协议头中的协议字段（IPv4）或者下一个头（IPv6，扩展）字段的值是51。

0 1 2 3 4

下一个头	载荷长度	保留
安全参数索引（SPI）		
序列号		

认证数据（变长的）

图 5-2-1 AH 头格式

下一个头：下一个头是一个1字节的字段，该字段指定了认证头后面下一个载荷的类型。这个字段的值是由Internet分配数字机构（IANA）的最新“分配数字”[STD-2]中定义的IP协议数字集合分配的。

载荷长度：载荷长度是一个1字节的字段，该字段的值是AH头的长度减去“2”，长度值以4字节为单位。

保留：保留字段是一个2字节的字段，留给将来使用。该字段应被设置成“0”，并且参与完整性校验值ICV的计算。

安全参数索引：安全参数索引SPI是一个4字节值，它与目的IP地址和安全协议共同标识了这个数据报文的安全联盟。从1至255范围内的SPI值是保留给将来使用的， “0”值保留给本地的特定实现使用并且不能在网络上传送，通信协商得到的SPI值不能小于256。

序列号：序列号是一个无符号的4字节单调递增计数器，发送方对使用该SA的每个数据报文进行计数，接收方必须检测这个字段来实现SA的抗重放攻击服务。发送方的计数器和接收方的计数器在建立一个SA时被初始化为0，该序列号在一个SA生存期内不能循环使用，在这个计数器溢出之前，通信的双方应协商出一个新的SA来使这个字段复位为0。

认证数据：认证数据是一个变长字段，它是一个完整性校验值ICV，用于校验整个IP报文的完整性（可变字段除外）。该字段的长度必须是4字节的整数倍，具体长度取决于所使用的完整性校验算法。

5.2.1.3　认证头 AH 的处理

5.2.1.3.1　AH 头的位置

AH头在传输模式和隧道模式中分别有不同的放置位置。

在IPv4环境中使用传输模式，AH头应放在原IP头之后，上层协议ESP之前，如图5-2-3所示。

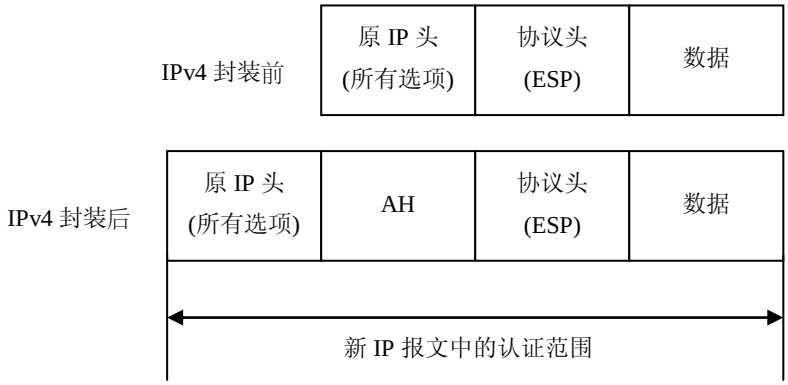

图 5-2-3 IPv4 的 AH 传输模式

在IPv6环境中使用传输模式，AH头被看作是一个端到端的载荷，因而应该出现在逐跳（hop-by-hop）、路由（routing）和分片扩展头（fragmentation extension headers）之后。目的选项扩展头（destination options extension header）既可以出现在AH头之前，也可以在AH头之后。如图5-2-4所示。

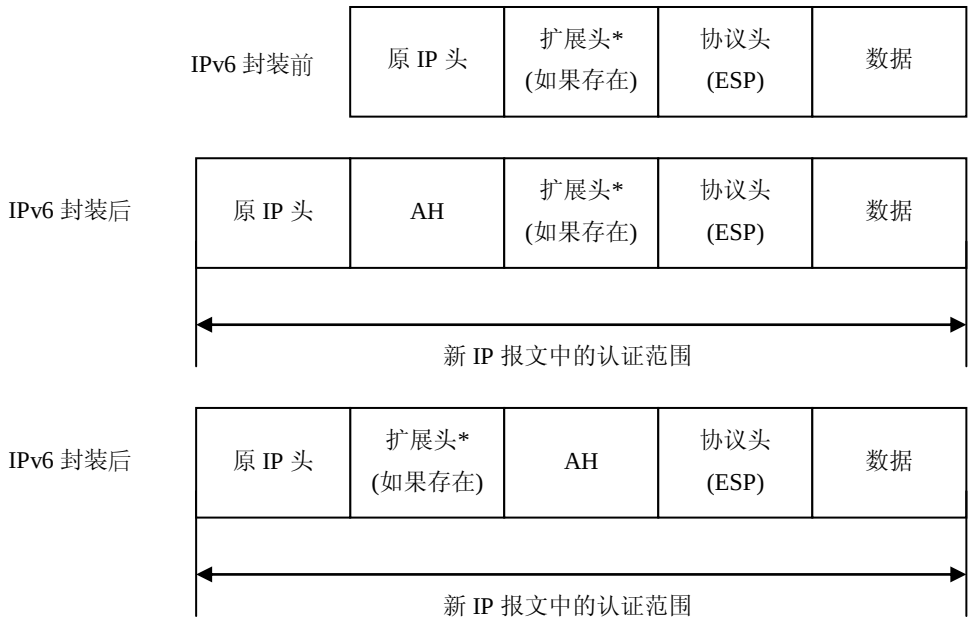

图 5-2-4　IPv6 的 AH 传输模式

在隧道模式中，AH头保护整个IP报文，包括整个原IP报文以及新建外部IP头的部分字段。图5-2-5和图5-2-6分别表示了隧道模式中典型的IPv4和IPv6报文的AH头的位置。

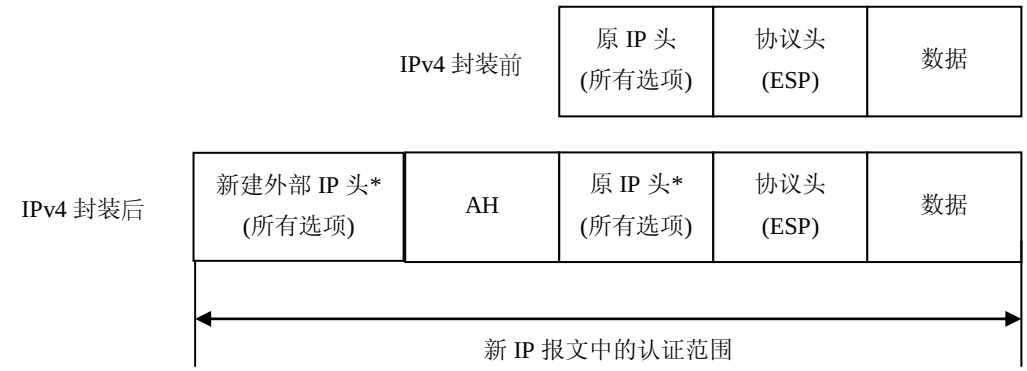

图 5-2-5　IPv4 的 AH 隧道模式

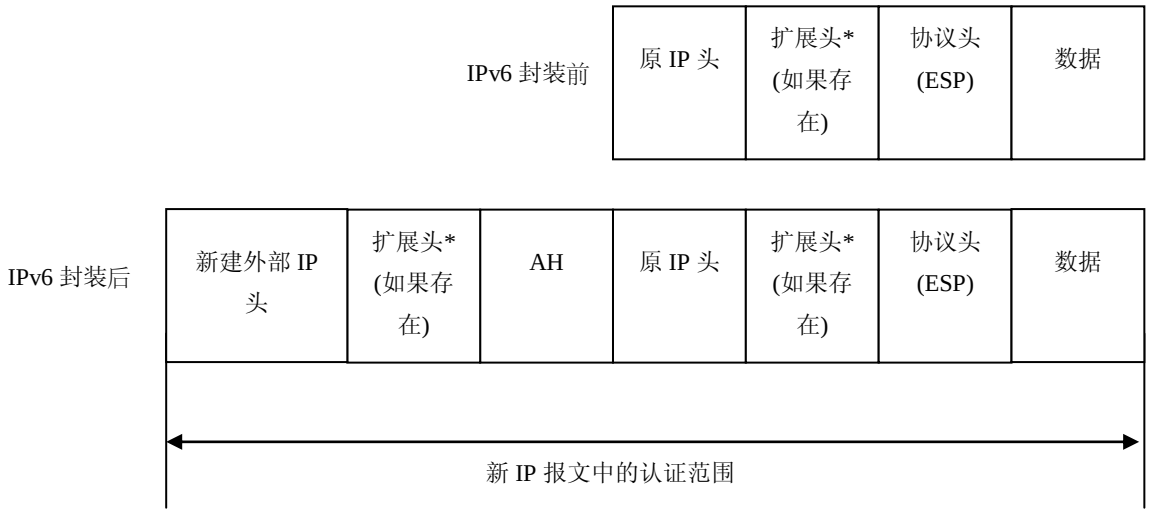

图 5-2-6　IPv6 的 AH 隧道模式

5.2.1.3.2　出站报文处理

出站报文的处理包括查找SA、产生序列号、计算完整性校验值、认证数据字段的填充和分片等过程。

1、查找SA

应根据本地策略查找SA，只有当一个IPSec实现确定了报文与该SA相关联后，AH才应用于一个出站报文。否则应开始新的密钥协商过程，建立SA。

2、产生序列号

当建立一个SA时，发送方的序列号计数器初始化为0，每发送一个报文之前，该计数器加1，并且把这个计数器值赋予序列号字段。当该计数器计数达到最大值前，应生成新的SA。

3、计算完整性校验值ICV

接收方采用指定的完整性校验算法对报文计算ICV。IPv 4 和IPv 6 的ICV计算方法分别如下所述：

（1）IPv4中的ICV计算

IPv4基本头字段、IPv4头的选项、AH头和上层协议数据都参与ICV计算。

IPv4基本头字段中，直接参与计算的字段为：版本（Version）、IPv4头长度(Header Length)、总长度(Total Length)、标识(Identification)、协议(Protocol)、源地址(Source Address)、目的地址(Destination Address)。

IPv4基本头字段中，在计算ICV之前设置为“0”的字段为：服务类型（TOS）、标志（Flags）、片偏移（Fragment Offset）、生存时间（TTL）、首部校验和（Header Checksum）。

IPv4头的整个选项被看作一个单元，选项中的类型和长度字段在传送中是不变的，但如果有一个字段是属于可变的，则整个选项用于计算ICV时都要清“0”。

整个AH头参与ICV计算，其中完整性校验值字段在计算ICV之前置“0”，在计算后，将计算得到的值赋于该字段。

整个上层协议数据直接参与ICV计算。

（2） IPv6中的ICV计算

IPv6基本头字段、IPv6扩展头、AH头和上层协议数据都参与ICV计算。

IPv6基本头字段中，直接参与计算的字段为：版本（Version）、 载荷长度（Payload Length）、下一个头（Next Header）、源地址（Source Address）、没有路由扩展头的目的地址（Destination Address）。

IPv6基本头字段中，在计算ICV之前设置为“0”的字段为：类别（Class）、流标签（Flow Label）、跳极限（Hop Limit）。

IPv6的扩展头中，在逐跳（Hop-by-Hop）和目的扩展头（Destination Extension Headers）中的IPv6选项包含有一个比特，该比特指出选项在传送过程期间是否会改变。对于在路由过程中内容可能变换的任何选项，整个“选项数据（Option Data）”字段在计算和校验ICV时必须被当作零值的字节串对待。选项类型（Option Type）和选项数据长度（Opt Data Len）被包括进ICV计算。由比特位确定为不变的所有选项都被包括进ICV计算。

整个AH头参与ICV计算，其中认证数据字段在计算ICV之前置“0”，在计算后，将计算得到的值赋于该字段。

整个上层协议数据直接参与ICV计算。

4、认证数据的填充

认证数据字段应确保是4字节（IPv4）或8字节（IPv6）的整数倍，否则需要填充。填充应放在认证数据字段的最末端，其内容由发送方任意选择，并且参与ICV计算。

5、分片

一个IPSec实现在AH处理之后，如果发现IP数据报文长度超过输出接口的MTU值，则对处理后的数据报文进行分片。

5.2.1.3.3 入站报文处理

入站报文的处理包括重组、查找SA、验证序列号和验证完整性校验值等过程。

1、重组

如果需要，在AH处理之前要进行IP数据报文重组。AH不处理分片报文，如果提供给AH处理的一个报文是一个分片的IP数据报文，接收方应丢弃该报文。

2、查找SA

当收到一个包含AH头的报文时，接收方应根据目的IP地址、AH和SPI来查找SA，查找失败则丢弃该报文。

3、验证序列号

所有AH实现必须支持抗重放攻击服务，在SA建立时，接收方序列号计数器应初始化为0。对于每个接收到的报文，接收方应确认报文包含一个序列号，并且该序列号在这个SA生命期中不重复，否则应丢弃该报文。

如果该序列号超出接收窗口有效检查范围的高端值，则对报文进行完整性校验。如果校验通过，接收窗口应相应调整；如果校验不通过则丢弃该报文。

接收窗口的大小默认为64。

4、验证完整性校验值

接收方采用指定的完整性校验算法对报文计算ICV，计算方法和参与计算的内容与出站报文计算ICV的一致。计算的结果与报文中的ICV进行比较。如果一致，则接收到的数据报文是有效的，否则接收方应将收到的数据报文丢弃。

5、匹配安全策略

检查数据包是否符合设置的安全策略要求。

5.2.2 封装安全载荷 ESP

5.2.2.1 概述

封装安全载荷ESP提供了机密性、数据源鉴别、无连接的完整性、抗重放攻击服务和有限信息流量的保护。当ESP单独使用时、必须同时选择机密性和数据源鉴别服务，当ESP和AH结合使用时不应选择数据源鉴别服务。

5.2.2.2 ESP 头格式

ESP头格式见图5-2-７，其位置紧接在IPv4、IPv6或者扩展协议之后，在头中的协议（IPv4）字段或者下一个头（IPv6，扩展）字段的值是50。

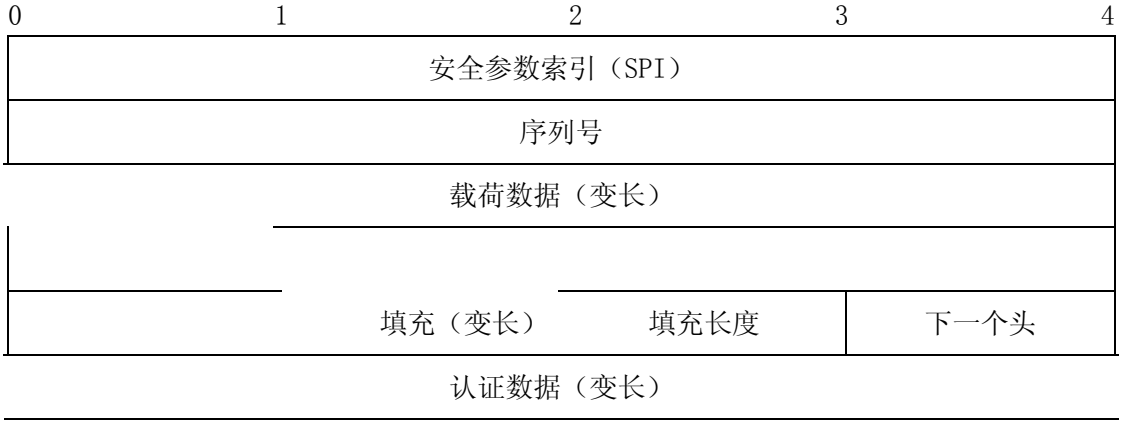

图 5-2-7 ESP 头格式

5.2.2.2.1 安全参数索引 SPI

安全参数索引SPI是一个4字节值,它与目的IP地址和安全协议共同标识了这个数据报文的安全联盟。从1至255范围内的SPI值是保留给将来使用的， “0”值保留给本地的特定实现使用并且不能在网络上传送，通信协商得到的SPI值不能小于256。

5.2.2.2.2 序列号

序列号是一个无符号的4字节单调递增计数器，发送方对使用该SA的每个数据报文进行计数，接收方必须检测这个字段来实现SA的抗重放攻击服务。发送方的计数器和接收方的计数器在建立一个SA时被初始化为0，该序列号在一个SA生存期内不能循环使用，在这个计数器溢出之前，通信的双方应协商出一个新的SA来使这个字段复位为0。

5.2.2.2.3 载荷数据

载荷数据是一个变长的字段，它包含初始化向量IV和下一个头字段所描述的数据，其长度单位为字节。

IV应置于载荷数据首部。

5.2.2.2.4 填充字段

如果载荷数据的长度不是加密算法的分组长度的整数倍，则需要对不足的部分进行填充，填充以字节为单位。如果需要，也可以提供更多的填充数据，但必须符合加密算法分组长度的要求。

填充的方法和内容应由指定的加密算法规定。如果加密算法没有规定，则附加在报文之后的第一个字节为 1 ，后续的填充字节按单调递增的顺序拼凑。

5.2.2.2.5 填充长度

填充长度字段指出了填充字节的个数。有效值范围是0至255，其中0表明没有填充字节。

5.2.2.2.6 下一个头

下一个头是一个1字节的字段，该字段指定了ESP头后面下一个载荷的类型。这个字段的值是由Internet分配数字机构（IANA）的最新“分配数字”[STD-2]中定义的IP协议数字集合分配的。

5.2.2.2.7 认证数据

认证数据是一个变长字段，它是一个完整性校验值ICV，是对ESP报文去掉ICV外的其余部分进行完整性校验计算所得的值。该字段的长度由选择的完整性校验算法决定。认证数据字段是可选的，只有当SA选择了完整性校验服务时才包含认证数据字段。

5.2.2.3 封装安全载荷 ESP 的处理

5.2.2.3.1 ESP 头的位置

ESP头在传输模式和隧道模式中分别有不同的放置位置。

在IPv4环境中使用传输模式,ESP应放在IP头和它包含的所有选项之后和上层协议之前，如图 5－2－8 所示,图中“数据”包含“载荷数据”和“填充”，“ESP尾”包含“填充长度”和“下一个头”字段。

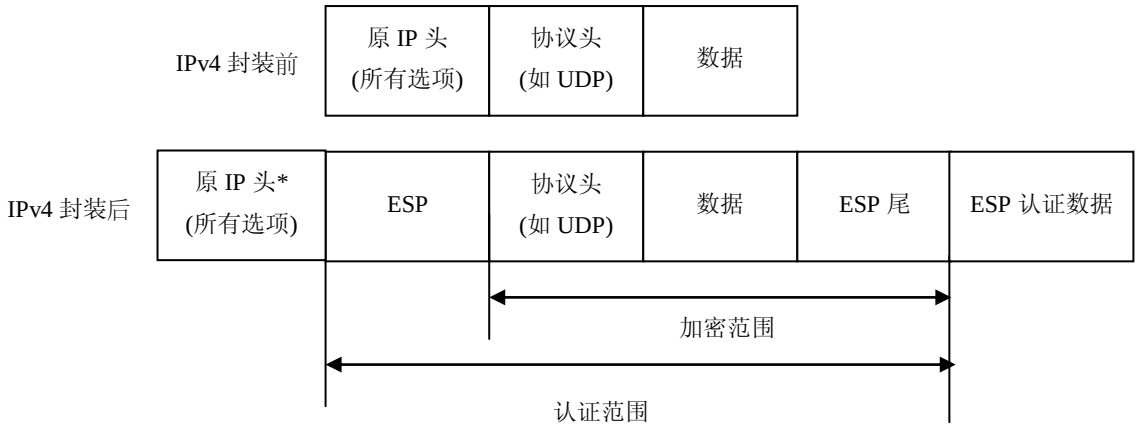

图5-2-8 IPv4的ESP传输模式

在IPv6环境中使用传输模式，ESP被看作是一个端到端的载荷，因而应该出现在逐跳（hop-by-hop）、路由（routing）和分片扩展头（fragmentation extension headers）之后，如图5-2-9所示，图中“数据”包含“载荷数据”和“填充”，“ESP尾”包含“填充长度”和“下一个头”字段。

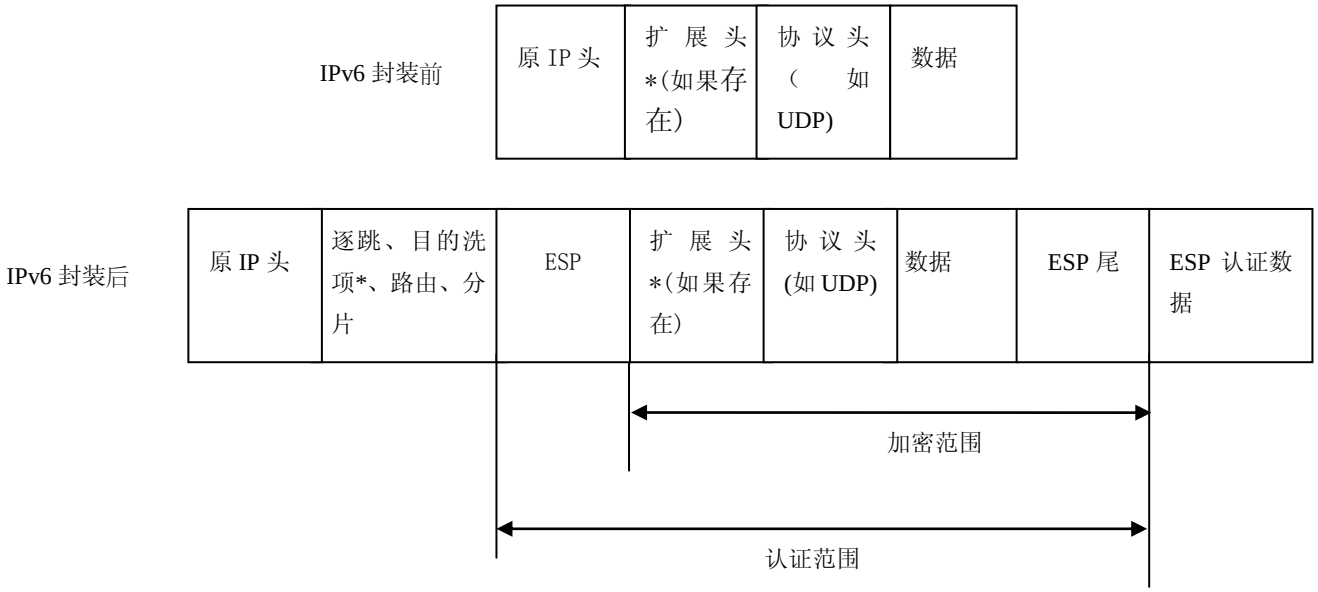

图5-2-9　IPv6的ESP传输模式

在IPv4 和IPv6中使用隧道模式，ESP保护包括原内部IP头在内的整个原IP报文，分别如图5-2-10和5-2-11所示，图中“数据”包含“载荷数据”和“填充”，“ESP尾”包含“填充长度”和“下一个头”字段。

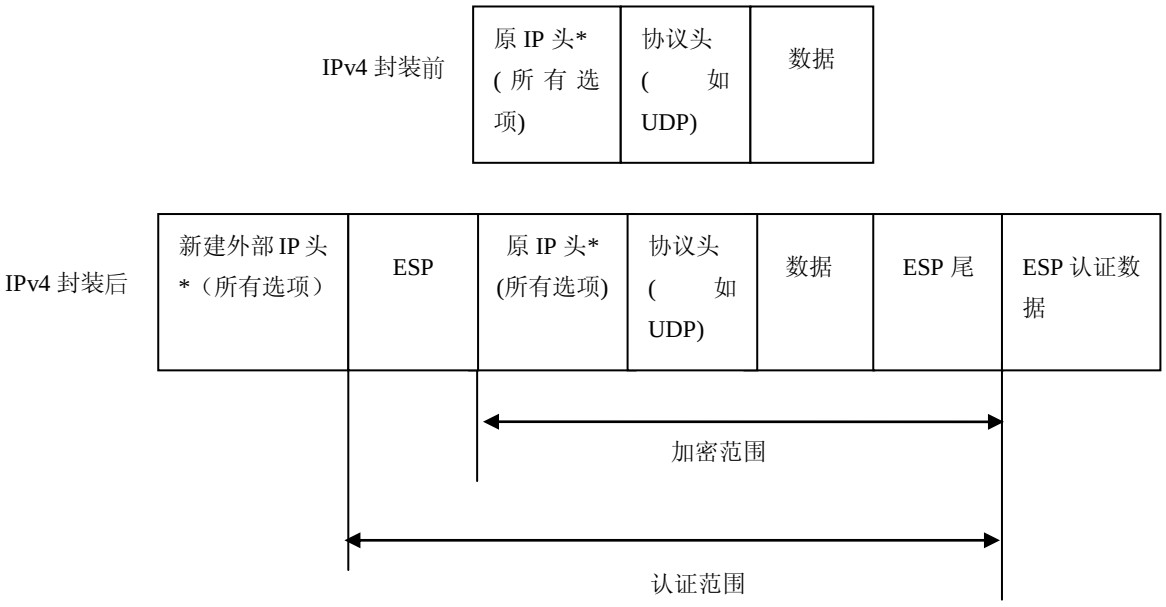

图5-2-10　IPv4的ESP隧道模式

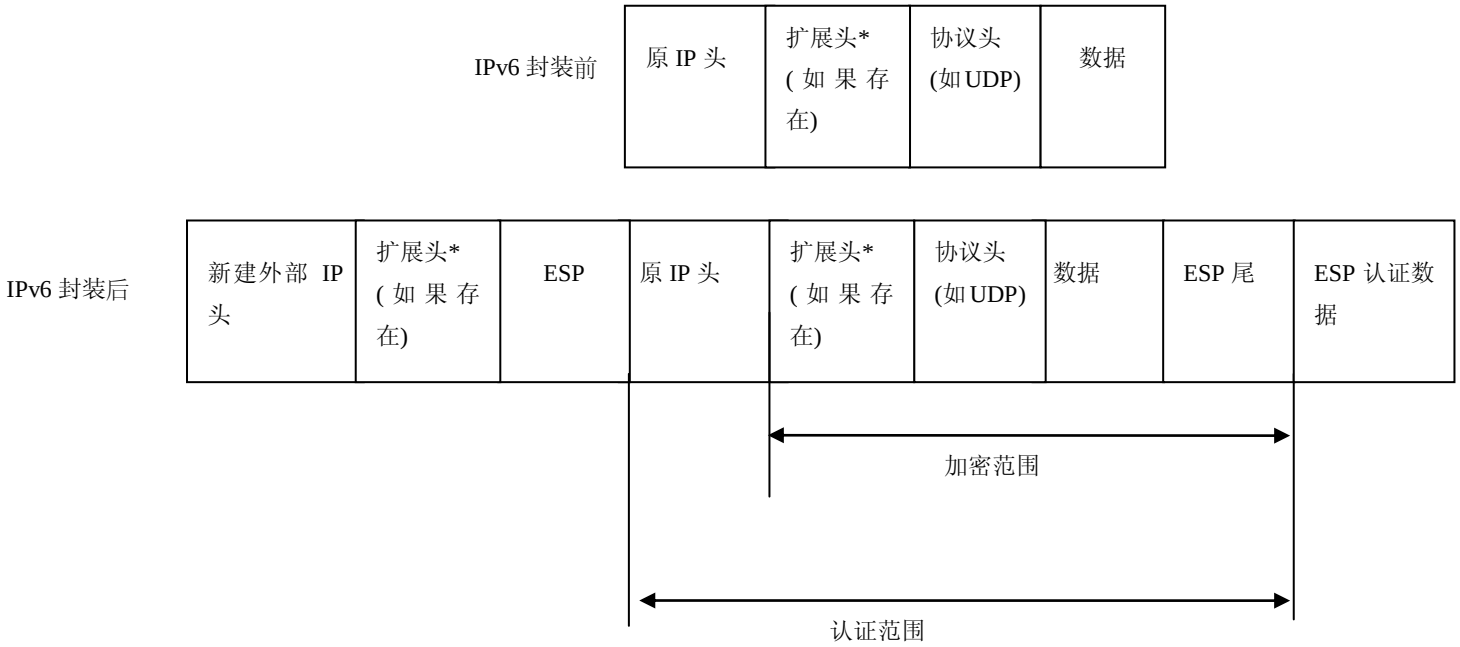

图5-2-11　IPv6的ESP隧道模式

5.2.2.3.2　出站报文处理

出站报文的处理包括查找SA、封装、加密报文、产生序列号、计算完整性校验值和分片等过程，并按照以下顺序进行处理。

1、查找SA

应根据本地策略查找SA，只有当一个IPSec实现确定了报文与该SA相关联后，ESP才应用于一个出站报文。否则应开始新的密钥协商过程，建立SA。

2、封装

在传输模式中，将原始上层协议封装到ESP载荷字段中。

在隧道模式中，将整个原始IP数据报文封装到ESP载荷字段中。

3、加密报文

首先对报文添加所有需要的填充，然后使用由SA指定的密钥、加密算法、算法模式和IV进行加密，加密范围包括载荷数据、填充、填充长度和下一个头。

4、产生序列号

当建立一个SA时，发送方的序列号计数器初始化为0，每发送一个报文之前，该计数器加1，并且把这个计数器值插入到序列号字段中。当该计数器计数达到最大值前，应生成新的SA。

5、计算完整性校验值

如果SA提供完整性校验服务，发送方在除去认证数据字段的ESP报文上计算ICV。将计算后得到的值赋于认证数据字段。

6、分片

一个IPSec实现在ESP处理之后，如果发现IP数据报文长度超过输出接口的MTU值，则对处理后的数据报文进行分片。

5.2.2.3.3　入站报文处理

入站报文的处理包括重组、查找SA、验证序列号、验证完整性校验值、解密报文和重构等过程，并按以下顺序进行处理。

1、重组

如果需要，在ESP处理之前要进行IP数据报文重组。ESP不处理分片报文，如果提供给ESP处理的一个报文是一个分片的IP数据报文，接收方应丢弃该报文。

2、查找SA

当收到一个包含ESP头的报文时，接收方应根据目的IP地址、ESP和SPI来查找SA，查找失败则丢弃该报文。

3、验证序列号

所有ESP实现必须支持抗重放攻击服务，在SA建立时，接收方序列号计数器应初始化为0。对于每个接收到的报文，接收方应确认报文包含一个序列号，并且该序列号在这个SA生命期中不重复任何已接收的其它报文的序列号，否则应丢弃该报文。

如果该序列号超出接收窗口有效检查范围的高端值，则对报文进行完整性校验。如果校验通过，接收窗口应相应调整；如果校验不通过则丢弃该报文。

接收窗口的大小默认为64。

4、验证完整性校验值

接收方采用指定的完整性校验算法对报文计算ICV，计算方法和参与计算的内容与出站报文计算ICV的一致。计算的结果与报文中的ICV进行比较。如果一致，则接收到的数据报文是有效的，否则接收方应将收到的数据报文丢弃

5、解密报文

使用SA指定的密钥、加密算法、算法模式和IV，对接收报文的加密部分进行解密。根据解密后报文中的填充长度和填充数据进行判断是否解密成功。如解密失败则丢弃该报文。

6、重构

对解密成功的报文，重构原始IP数据报文。

5.2.3 NAT 穿越

为了穿越NAT，在UDP报文中封装和解封装ESP报文的方法按RFC3948的要求实现。

5.2.4 匹配安全策略

检查数据包是否符合设置的安全策略要求。

6 IPSec VPN 产品要求

6.1 产品功能要求

6.1.1 随机数生成

IPSec VPN产品应具有随机数生成功能，在使用随机数前能对生成的随机数进行偏“0”、偏“1”、“0、1”平衡等常规检测，并提供检测接口，能通过检测接口对IPSec VPN产品所生成的随机数进行样本采集。

6.1.2 工作模式

IPSec VPN产品工作模式应支持隧道模式和传输模式，其中隧道模式是必备功能，用于主机和网关实现，传输模式是可选功能，仅用于主机实现。

6.1.3 密钥协商

IPSec VPN产品应具有密钥协商功能，通过协商产生工作密钥和会话密钥。

密钥协商协议应按照本规范5.1的要求进行。

6.1.4 安全报文封装

安全报文封装协议分为AH协议和ESP协议。

AH协议应与ESP协议嵌套使用，这种情况下不启用ESP协议中的验证操作。

ESP协议可单独使用，这种情况下应启用ESP协议中的验证操作。

安全报文封装协议应按照本规范5.2的要求进行。

6.1.5 NAT 穿越

IPSec VPN产品应支持ESP单独使用时NAT穿越。

NAT穿越协议应按照本规范5.1.3的要求进行。

6.1.6 认证方式

IPSec VPN产品应具有实体认证的功能，身份认证数据应支持数字证书或公私密钥对方式。

6.1.7 IP 协议版本支持

IPSec VPN产品应支持IPv4协议或IPv6协议。

6.1.8 抗重放攻击

IPSec VPN产品在安全报文传输阶段应具有对抗重放攻击的功能。

6.1.9 密钥更新

IPSec VPN产品应具有根据时间周期和报文流量两种条件进行工作密钥和会话密钥的更新功能，其中根据时间周期条件进行密钥更新为必备功能，根据报文流量条件进行密钥更新为可选功能。

工作密钥的最大更新周期不大于24小时。

会话密钥的最大更新周期不大于1小时。

6.2 产品性能要求

6.2.1 加解密吞吐率

加解密吞吐率是指分别在64字节以太帧长和1428字节以太帧长时，IPSec VPN产品在丢包率为0的条件下内网口上达到的双向数据最大流量。产品应满足用户网络环境对网络数据加解密吞吐性能的要求。

6.2.2 加解密时延

加解密时延是指分别在64字节以太帧长和1428字节以太帧长时，IPSec VPN产品在丢包率为0的条件下，一个明文数据流经加密变为密文，再由密文解密还原为明文所消耗的平均时间。产品应满足用户网络环境对网络数据加解密时延性能的要求。

6.2.3 加解密丢包率

加解密丢包率是指分别在64字节以太帧长和1428字节以太帧长时，在IPSec VPN产品内网口处于线速情况下，单位时间内错误或丢失的数据包占总发数据包数量的百分比。产品应满足用户网络环境对网络数据加解密丢包率性能的要求。

6.2.4 每秒新建连接数

每秒新建连接数是指IPSec VPN产品在一秒钟的时间单位内能够建立隧道数目的最大值。产品应满足用户网络环境对每秒新建连接数性能的要求

6.3 安全管理要求

6.3.1 密钥管理

6.3.1.1 设备密钥

设备密钥应由IPSec VPN产品自身产生或由外部产生并导入。设备密钥由产品自身产生时，其公钥应能被导出；设备密钥由外部产生时，应有安全措施保证私钥在产生、存储、分发和导入时的安全。设备密钥应保存在非易失性存储装置中，其私钥应有安全保护措施。设备密钥应按设定的安全策略进行更新。

设备密钥可以安全形式进行备份，并在需要时能够恢复。

6.3.1.2 工作密钥

工作密钥在密钥协商的第一阶段产生，产生后应保存在易失性存储器中，达到其更新条件后应立即更换，在连接断开、设备断电时应销毁。

6.3.1.3 会话密钥

会话密钥在密钥协商的第二阶段产生，产生后应保存在易失性存储器中，达到其更新条件后应立即更换，在连接断开、设备断电时应销毁。

6.3.2 数据管理

6.3.2.1 配置数据管理

所有的配置数据应保证其在设备中的完整性、可靠性。应有管理界面对配置数据进行配置和管理，管理员进入管理界面应通过身份认证。

6.3.2.2 日志管理

IPSec VPN产品应提供日志功能，日志可被查看、导出。

日志内容包括：

——操作行为，包括登录认证、参数配置、策略配置、密钥管理等操作。

——安全事件，安全联盟的协商成功、协商失败、过期等事件。

——异常事件，解密失败、完整性校验失败等异常事件的统计。

6.3.3 人员管理

IPSec VPN产品应设置管理员，进行设备参数配置、策略配置、设备密钥的生成、导入、备份和恢复等操作。管理员应持有表征用户身份信息的硬件装置，与登录口令相结合登录系统，进行管理操作前应通过身份认证。

登录口令长度应不小于8个字符。

使用错误口令或非法身份登录的次数限制应小于或等于8。

6.3.4 设备管理

6.3.4.1 硬件安全

IPSec VPN产品应提供安全措施，保证密码算法、密钥、关键数据的存储安全。

所有密码运算应在独立的密码部件中进行。

除必需的通信接口和管理接口以外，不提供任何可供调试、跟踪的外部接口。内部的调试、检测接口应在产品定型后封闭。

6.3.4.2 软件安全

所有的安全协议及管理软件应自主实现。

操作系统应进行安全加固，裁减一切不需要的模块，关闭所有不需要的端口和服务。

任何操作指令及其任意组合，不能泄露密钥和敏感信息。

6.3.4.3 设备初始化

IPSec VPN产品的初始化，除必须由厂商进行的操作外，参数的配置、安全策略的配置、密钥的生成和管理、管理员的产生等均应由用户完成。

6.3.4.4 注册和监控

IPSec VPN产品可具有向管理中心进行注册的功能，同时接受管理中心对其运行状态的实时监控管理。

6.3.4.5 设备自检

应对密码运算部件等关键部件进行正确性检查。

应对存储的密钥等敏感信息进行完整性检查。

在检查不通过时应报警并停止工作。

7 IPSec VPN 产品检测

7.1 产品功能检测

7.1.1 随机数功能

按照《随机数检测规范》的要求提取样本，并按照该规范的相关要求进行检测，检测结果应合格。

7.1.2 工作模式

将测试设备与被测设备均设置为隧道模式，应能成功完成密钥协商，建立IPSec隧道进行通信。

被测设备支持传输模式时，将测试设备与被测设备均设置为传输模式，应能成功完成密钥协商，进行通信。

将测试设备与被测设备一方设置为隧道模式，另一方设置为传输模式，密钥协商应失败，无法建立IPSec隧道进行通信。

7.1.3 密钥协商

密钥协商的检测按本规范7.1.2的方法进行。对密钥协商过程进行网络数据截获，查看其过程应符合本规范5.1的要求，应能正确进行加解密通信。该项测试通过，可以间接证明设备采用的对称密码算法、非对称密码算法和密码杂凑算法的实现正确性。

7.1.4 安全报文封装协议

将测试设备与被测设备的安全报文封装协议均配置为ESP协议，对通信的报文进行网络数据截获，查看其封装格式应符合本规范5.2的要求，应能正确进行加解密通信。

将测试设备与被测设备的安全报文封装协议均配置为AH协议嵌套ESP协议，对通信的报文进行网络数据截获，查看其封装格式应符合本规范5.2的要求，应能正确进行加解密通信。

7.1.5 NAT 穿越

将待检测设备放在NAT下，与检测中心设备进行隧道测试，建立ESP协议的隧道模式的IPSec VPN，测其功能是否完成，该项检测是必备检测。

按本规范5.1.3的方法进行密钥协商。对密钥协商过程进行网络数据截获，查看其过程应符合本规范6.1.3的要求，应能正确进行加解密通信；对加密通信的报文进行网络数据截获，查看其封装格式应符合本规范6.1.5的要求；

7.1.6 认证方式

按产品提供的认证方式，按本规范6.1.3的方法进行密钥协商，应能成功完成协商过程，建立IPSec隧道进行通信。

7.1.7 IP 协议版本支持

在IPv4或者IPv6的环境下，按本规范6.1.3的方法进行密钥协商，应能成功完成协商过程，建立IPSec隧道进行通信。

7.1.8 抗重放攻击

利用测试设备或网络报文截获工具重放报文传输阶段的安全报文，在被测设备的内网口应不能检测到重放的数据报文。

7.1.9 密钥更新

在被测设备上分别设定工作密钥和会话密钥的更新周期，当满足更新条件时，使用网络报文截获工具应能分别看到相应的第一阶段和第二阶段的密钥的协商过程。

如果设备具有根据流量更新密钥的功能，在被测设备上设定会话密钥的流量更新条件，当满足更新条件时，使用网络报文截获工具应能看到第二阶段的密钥的协商过程。

7.2 产品性能检测

7.2.1 加解密吞吐率

按本规范6.2.1的要求进行测试，记录测试结果。

7.2.2 加解密时延

按本规范6.2.2的要求进行测试，记录测试结果。

7.2.3 加解密丢包率

按本规范6.2.3的要求进行测试，记录测试结果。

7.2.4 每秒新建连接数

按本规范6.2.4的要求进行测试，统计一分钟时间内建立的IPSec隧道数，得到每秒新建连接数，并记录结果。

7.3 安全管理检测

7.3.1 密钥管理

在被测设备的管理界面上进行设备密钥的产生或导入、备份和恢复以及更新操作。应符合本规范6.3.1.1的要求。

7.3.2 数据管理

7.3.2.1 配置数据管理

通过管理界面对配置数据进行配置和管理，结果应符合本规范6.3.2.1的要求。

7.3.2.2 日志管理

查看并导出日志记录，结果应符合本规范6.3.2.2的要求。

7.3.3 人员管理

用非法的身份或错误的口令登录，系统应拒绝；当连续重试次数到达系统设定的限制值时系统应锁定。

用合法的身份和正确口令登录，应能进入管理界面，进行相应的管理操作。

7.3.4 设备管理

7.3.4.1 硬件安全

审查厂商提供的设计文档和厂商提交的产品安全性承诺，应符合本规范6.3.4.1的要求。

7.3.4.2 软件安全

使用扫描工具探测系统的端口和服务，并审查厂商提供的设计文档和厂商提交的产品安全性承诺，应符合本规范6.3.4.2的要求。

7.3.4.3 设备初始化

对设备进行初始化操作，结果应符合本规范 6.3.4.3 的要求。

7.3.4.4 注册和监控

当系统有管理中心时，进行设备的注册、状态监控等管理操作。结果应符合本规范6.3.4.4的要求。

7.3.4.5 设备自检

对设备进行自检操作，结果应符合本规范6.3.4.5的要求。

8 合格判定

本规范中，6.1以及6.3中除6.3.2.1和6.3.4.4以外的各项要求中，其任意一项要求不合格，判定为产品不合格。

附 录 A IPSec VPN 概述

（资料性附录）

本附录概要介绍了IPSec基础构架,基本概念和基本内容,详细内容参见RFC4301.

IPSec是为IPv4和IPv6数据报文提供高质量的、可互操作的、基于密码学安全性的协议。IPSec通过使用认证头（AH）和封装安全载荷（ESP）两种安全协议，以及密钥交换协议来实现这些目标。

AH协议提供数据源鉴别、数据完整性以及抗重放服务。ESP协议提供数据保密性、数据源鉴别、数据完整性以及抗重放服务。对于AH和ESP，都有传输和隧道两种封装模式。密钥交换协议用于协商AH和ESP协议所使用的密码算法和密钥。

IPSec允许系统或网络的用户和管理员控制安全服务提供的服务范围。例如，一个组织的安全策略可能规定来自特定子网的数据流应该使用AH和ESP保护，并使用SM1分组密码算法加密。另一方面，策略可能规定来自另一个站点的数据流应该只用ESP保护，并使用SM1分组密码算法加密。通过使用安全联盟（SA），IPSec能够区分不同的数据流，并提供相应的安全服务。

A.1 安全联盟及安全联盟数据库

安全联盟（SA）是IPSec VPN的基础。AH和ESP都使用了SA，而且密钥交换协议的一个主要功能就是建立和维护安全联盟。所有AH和ESP的实现都应支持安全联盟。下面分别描述了安全联盟管理的各个方面，定义了SA策略管理、通信处理、SA管理技术所需的特性。

A.1.1 定义和范围

一个SA为一个方向上传输的数据流提供AH或ESP协议的一种安全服务。如果AH和ESP同时被用于保护一个数据流，那么应该创建多个SA来提供对数据流的保护。为了保护两台主机之间或两个安全网关之的双向通信，需要两个安全联盟，每个方向一个。安全联盟由三元组唯一标识，该三元组包括安全参数索引（SPI）、目的IP地址（单播地址）和安全协议（AH或ESP）标识符。

SA有传输和隧道两种模式。传输模式SA是两台主机间的一个安全联盟。在IPv4环境中，一个传输模式安全协议头紧接在IP头和任意选项之后，且在任何更高层协议之前（例如TCP或UDP）。在IPv6环境中，安全协议头出现在基本IP头和扩展之后，但可能出现在目的地选项之前或之后，并在更高层协议之前。在ESP的情况下，一个传输模式SA仅为那些更高层协议提供安全服务，而并不为ESP头之前的IP头或任意扩展头提供服务。在AH情况下，这种保护也被扩展到IP头的可选部分、扩展头的可选部分和可选项（包含在IPv4头、IPv6逐跳扩展头、或IPv6目的扩展头中）。

隧道模式SA是运用于一个IP隧道的SA，只要一个安全联盟的任意一端是一个安全网关，SA就应是隧道模式。这里有一个指定了IPSec处理目的地的“外部”IP头，加上一个指定了报文最终目的地的内部IP头。安全协议头出现在外部IP头之后和内部IP头之前。如果在隧道模式中使用AH，部分外部IP头将受到保护，同样所有隧道里的IP报文也受到保护。如果使用ESP，则仅对隧道里的报文给予保护，而不保护外部头。

A.1.2 安全联盟的功能

一个SA所提供的安全服务集依赖于所选择的安全协议、SA模式、SA端点和对协议范围内可选服务的选择。

ESP为数据流提供加密服务，同时也提供认证服务。ESP所提供的认证范围比AH所提供的要窄，即ESP头“外面”的IP头不受保护。

如果使用ESP，则两个安全网关之间的ESP（隧道模式）SA能提供数据流保密。隧道模式的使用允许内部IP头被加密，也就隐藏了通信源和目的地的标识。而且，也可以使用ESP载荷填充来隐藏报文的大小，进一步隐藏通信的外部特性。保护范围较小的SA比保护范围更大的SA更容易受到流量分析的攻击。

A.1.3 安全联盟的组合

当单一的SA不能满足有更高安全要求的数据流时，需要采用多个SA的组合来实现必要的安全策略，这个组合称为“安全联盟束”或“SA束”。安全联盟可以通过两种方式组合成束：传输邻接和迭代隧道。传输邻接指的是对同一个IP数据包使用多于一个传输模式的安全协议。这种联合AH和ESP的方法只允许一级的联合，更多的嵌套并不能产生更多的好处。迭代隧道指的是通过IP隧道实现的安全协议的多层次应用。这种方法允许多重嵌套。

这两种方式也可以再组合，例如，一个SA束可以由一个隧道模式SA和一个或两个传输模式SAs依次应用而构成。迭代隧道也能发生在任何隧道源或目的端点都不相同的地方。

A.2 安全联盟数据库

在IPSec VPN实现中，处理IP通信的大量细节主要是一个本地事情，本规范并不做细节上的规定。但是本规范规定了一套SPD元素集标准，以保证实现的可操作性和最低限度的管理能力，这对于保证使用本规范的IPSec VPN设备之间的互通是必须的。下面描述了处理IP数据流的一个通用模式，该模式仅作参考，服从本规范的实现并不需要在细节上和这个模式相一致，但是应实现该模式所描述的所有功能。

这一模型中有两个名义上的数据库：安全策略数据库和安全联盟数据库。前者定义策略，这些策略决定所有IPSec实现入站和出站的IP通信的处理 。后者包括和每一个安全联盟有关的参数。本节定义了选择符、IP集和高层协议域值的概念，策略数据库通过使用这些值来把通信映射到一个策略，也就是一个SA或SA束。因为用作选择符的许多字段具有方向性，所以每一个激活了IPSec的接口要求名义上分开入站和出站数据库。

A.2.1 安全策略数据库

安全策略数据库（SPD）定义了哪些服务以何种方式提供给IP数据包。本规范并不强制规定安全策略数据库以及其接口的实现方式。但是，任何服从本规范的实现应提供本节描述的最小管理功能，以保证系统管理员能正确配置IPSec策略。

对于实现了IPSec的设备上，所有的数据包处理过程中都应查阅SPD。因此，SPD要求对于入站和出站数据包要有不同的入口。另外，对于每个激活了IPSec的接口，应提供一个名义上独立的SPD，它应区分受IPSec保护的数据包和允许绕过IPSec的数据包。对于任何出站或入站的数据包，这里有三种可能的处理选择：丢弃、绕过IPSec或使用IPSec处理。第一种选择是指根本不允许数据包离开主机、穿过VPN网关。第二种选择指的是允许数据包通过但不受IPSec保护。第三种选择指对数据包使用IPSec保护，在这种情况下，SPD应指出对数据流提供的安全服务、采用的协议、使用的算法等。

对于IPSec实现，应要有一个管理接口，该接口允许用户或系统管理员管理SPD。管理接口应允许用户定义进入或离开系统的数据流的处理方法。SPD的管理接口应允许创建与5.1.4.7节定义的选择符一致的入口，并且应支持这些入口的排序。

SPD包括一个有序的策略入口列表。策略入口由一个或多个选择符标识，这些选择符定义了哪些数据流应该应用该策略。每个入口包括一个标识，该标识指出匹配这一策略的通信是否允许绕过、丢弃、或进行IPSec处理。如果需要进行IPSec处理，则入口应包括一个SA或SA束的详细说明，其列举了IPSec的协议、模式、和使用的算法，以及是否需要嵌套使用SA。策略入口还应规定如何从SPD和报文中的值衍生得到一个新的安全联盟数据库入口值，可以有a. 使用报文自身拥有的值，b. 使用和策略入口相关的值两种选择。如果策略入口相关的值是个单值，则(a)和(b)没什么区别。但是，如果选择符的允许值是一个范围（对IP地址）或通配符时，那么在一个范围的情况下，(b)将激活对任何在该选择符范围值之内拥有一个选择符值的报文使用这个SA，而不仅仅是带有触发创建SA的选择符值的报文。在通配符的情况下，(b)允许对有该选择符任何值的报文使用这个SA。

SPD入口应被排序，并且总以相同顺序进行搜索，因此第一个相匹配的入口始终都会被选择。当一个安全策略要求按照一定的顺序，对数据流序应用多个SA时，SPD中的策略入口应规定如何使用这些SA的顺序。

A.2.2 选择符

SA或SA束可以是细致的或者是粗略的。例如，一对VPN网关之间的所有数据流可以基于单个SA来传输，也可以为每一对通讯主机指派一个SA，SA管理应支持下面的选择符参数:

- 目的 IP 地址（IPv4 或 IPv6）：这可以是单个 IP 地址（单播）、一个地址范围（包含高值和低值）、地址加掩码、或一个通配符地址。注意这一选择符同 SA 的<目的 IP 地址、IPSec 协议、SPI>三元组中的“目的 IP 地址”字段有概念上的不同。当一个封装在隧道中的报文到达了隧道的终点时，它的 SPI/目的地址/协议被用来在 SAD 中寻找这个报文的 SA。这一目的地址来自于封装的外部 IP 头。
- 源 IP 地址（IPv4 或 IPv6）：这可以是一个单一 IP 单播地址、一个地址范围（包含高值和低值）、地址加掩码、或一个通配符地址。
- 名字（Name）：域名字符串如：foo.bar.com 或者用户名字符串如：mozart@foo.bar.com
- 传输层协议：是从 IPv4 的“协议”或者 IPv6 的“下一个头”字段得到的。其可以是一个单独的协议号。
- 源和目的（如 TCP/IP）端口：这些可能是特殊的 UDP/TCP 端口值或是一个通配的端口。注意，在收到一个具有 ESP 头的报文的情况下可以不能得到源端口和目的端口，因此，应该支持一个“不透明的”的值。

A.2.3 安全联盟数据库

每个IPSec实现都有一个名义上的安全联盟数据库(SAD),它的每个入口都定义了与一个SA相关的参数。每个SA在SAD中都有一个入口，对于出站处理，SAD入口可以从SPD的入口得到。如果一个SPD入口现在没有指向一个适合该报文的SA,实现就应为该SPD入口创建一个适当的SA或SA束,并把SPD入口和该SAD入口关联到一起。对于入站处理，SAD中的每个入口根据一个目的IP地址、IPSec协议类型、和SPI进行索引。对于入站处理，下面的报文字段用于在SAD查找SA：

- 外部头中的目的 IP 地址：IPv4 或 IPv6 目的地址。
- IPSec 协议：AH 或 ESP，用作一个在这个数据库中查找 SA 的索引。
- SPI：4 字节的值，用于区别有相同的目的地和相同的 IPSec 协议不同的 SA。

对于每个选择符，SAD中的SA入口应包含一个或多个在创建SA时协商的值。对于发送者，这些值用于决定哪个SA应该被使用，对于响应方，这些值用于核对入站报文中的选择符值是否与SA的选择符值是否相匹配。下面的SA字段用在进行IPSec的处理中。

- 序列号计数器：用于产生 AH 或 ESP 头中的序列号。
- 序列号计数器溢出标志：用于指示序列号计数器的溢出是否应该产生一个日志记录，并且阻止用该 SA 继续传输报文。
- 抗重放窗口：包括一个计数器和一个检测窗口，用于判断一个入站 AH 或 ESP 报文是否是一个重放报文。
- AH 认证算法和密钥。
- ESP 加密算法、密钥、IV 模式和 IV。
- ESP 认证算法和密钥，如果不选择认证服务，该字段为空。
- 安全联盟生存期：可使用秒或千字节作为单位。
- IPSec 协议模式：隧道模式或者传输模式。