ICS 35.030
CCS L 80

GM

中华人民共和国密码行业标准

GM/T 0022—2023
代替 GM/T 0022—2014

IPSec VPN 技术规范

IPSec VPN technical specification

2023-12-04 发布　　2024-06-01 实施

国家密码管理局　发布

目　　次

前　言

本文件按照 GB/T 1.1—2020《标准化工作导则　第 1 部分：标准化文件的结构和起草规则》的规定起草。

本文件代替 GM/T 0022—2014《IPSec VPN 技术规范》，与 GM/T 0022—2014 相比，除结构调整和编辑性改动外，主要技术变化如下：

a) 删除了术语和定义：“密码算法”（见 2014 年版的 3.1.1）、“密码杂凑算法”（见 2014 年版的 3.1.2）、“非对称密码算法/公钥密码算法”（见 2014 年版的 3.1.3）、“对称密码算法”（见 2014 年版的 3.1.4）、“分组密码算法”（见 2014 年版的 3.1.5）、“密码分组链接工作模式”（见 2014 年版的 3.1.6）、“初始化向量/值”（见 2014 年版的 3.1.7）、“数字证书”（见 2014 年版的 3.1.9）、“鉴别”（见 2014 年版的 3.1.14）、“加密”（见 2014 年版的 3.1.15）、“SM1 算法”（见 2014 年版的 3.1.20）、“SM2 算法”（见 2014 年版的 3.1.21）、“SM3 算法”（见 2014 年版的 3.1.22）、“SM4 算法”（见 2014 年版的 3.1.23）；

b) 增加了术语和定义“可鉴别的加密机制”（见 3.6）；

c) 增加了“缩略语”GCM 和 PRF（见 4.2）；

d) 增加了与 GCM 加密模式相关的加密密钥选取说明（见 6.1.3.3）；

e) 更改了与 GCM 加密模式相关的快速模式中消息 1 的数据包格式（见 6.1.6.8，2014 年版的 5.1.5.7）、快速模式中消息 2 的数据包格式（见 6.1.6.9，2014 年版的 5.1.5.8）、快速模式中消息 3 的数据包格式（见 6.1.6.10，2014 年版的 5.1.5.9）；

f) 更改了“封装安全载荷 ESP 头格式”中与 GCM 相关的数据包封装和解封操作的详细说明（见 6.2.2.2，2014 年版的 5.2.2.2）、“封装安全载荷 ESP 的处理”中与 GCM 相关的数据包封装和解封操作的详细说明（见 6.2.2.3，2014 年版的 5.2.2.3）；

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由密码行业标准化技术委员会提出并归口。

本文件起草单位：深信服科技股份有限公司、无锡江南计算技术研究所、格尔软件股份有限公司、迈普通信技术股份有限公司、北京数字认证股份有限公司、华为技术有限公司、中电科网络安全科技股份有限公司、西安交大捷普网络科技有限公司、山东得安信息技术有限公司、国家密码管理局商用密码检测中心、深圳奥联信息安全技术有限公司、中国科学院信息工程研究所、鼎铉商用密码测评技术（深圳）有限公司、北京天融信网络安全技术有限公司、奇安信网神信息技术（北京）股份有限公司、武汉三江航天网络通信有限公司、中国电子技术标准化研究院、深圳市网安计算机安全检测技术有限公司、杭州奕锐电子有限公司、智巡密码（上海）检测技术有限公司。

本文件主要起草人：刘平、叶润国、罗俊、郑强、付夏冰、范恒英、朱志强、董浩、雷建、刘建锋、李小京、邱钢、向明、孔凡玉、李述胜、谭武征、王振、张勇、潘利民、罗鹏、李渝川、徐明翼、马洪富、凌杭、周欣、王雨晨、何建锋、李琳、龙军、刘松、但波、雷晓锋、刘玉岭、燕爽、王银平、吴安然、安高峰、刘晨、赵松、曹金、李露、樊俊诚、黄敏、吴俊雄、顾伟平、杨柳、匡云。

本文件及其所代替文件的历次版本发布情况为：

——2014 年首次发布为 GM/T 0022—2014；

——本次为第一次修订。

IPSec VPN 技术规范

1 范围

本文件规定了 IPSec VPN 的技术协议和产品功能，包括密钥交换协议和安全报文协议，以及产品功能要求和安全管理要求。

本文件适用于 IPSec VPN 产品的研制、检测、使用和管理。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本(包括所有的修改单)适用于本文件。

GB/T 20518—2018 信息安全技术 公钥基础设施 数字证书格式

GB/T 32905—2016 信息安全技术 SM3 密码杂凑算法

GB/T 32907—2016 信息安全技术 SM4 分组密码算法

GB/T 35276—2017 信息安全技术 SM2 密码算法使用规范

GB/T 36624—2018 信息技术 安全技术 可鉴别的加密机制

GM/T 0005—2021 随机性检测规范

GM/T 0016 智能密码钥匙密码应用接口规范

GM/T 0062—2018 密码产品随机数检测要求

GM/T 0092—2020 基于 SM2 算法的证书申请语法规范

GM/Z 4001 密码术语

RFC 2408 互联网安全联盟与密钥管理协议(Internet security association and key management protocol)

RFC 3947 密钥交换过程中 NAT 穿越协商(Negotiation of NAT-traversal in the IKE)

RFC 3948 IPSec ESP 包的 UDP 封装(UDP encapsulation of IPsec ESP packets)

RFC 4304 互联网安全关联和密钥管理协议(ISAKMP)IPsec 解释域(DOI)的扩展序列号(ESN)附录[Extended sequence number (ESN) addendum to IPsec domain of interpretation (DOI) for ISAKMP]

3 术语和定义

GM/Z 4001 界定的以及下列术语和定义适用于本文件。

3.1

安全联盟 security association

两个通信实体经协商建立起来的一种协定。

注 1：它描述了实体如何利用安全服务来进行安全的通信。

注 2：安全联盟包括了执行各种网络安全服务所要求的所有信息，例如：IP 层服务(如头鉴别和载荷封装)、传输层

和应用层服务或者协商通信的自我保护。

3.2

载荷　payload

ISAKMP 通信双方交换消息的数据格式。

注：载荷是构造 ISAKMP 消息的基本单位。

3.3

鉴别头　authentication header

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的 IPSec 协议。

3.4

封装安全载荷　encapsulating security payload

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的 IPSec 协议。

3.5

数据源鉴别　data origin authentication

一种确认接收到的数据的来源是所声称的机制。

3.6

可鉴别的加密机制　authenticated encryption mechanism

用于实现数据机密性保护并提供数据完整性和数据源鉴别的密码技术。

注：包括加密和解密两个处理过程。

[来源：GB/T 36624—2018，3.2，有修改]

3.7

虚拟专用网络　virtual private network

使用密码技术在通信网络中构建安全通道。

3.8

IPSec 实现　IPSec implementation

具体实现 IPSec VPN 协议的软硬件产品。

注：IPSec 实现包括软硬一体形态的硬件产品，以及纯软件实现的 IPsec VPN 产品（比如虚拟机或容器形态 IPSecVPN 产品）。

4　符号和缩略语

4.1　符号

下列符号适用于本文件。

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。

HASH_<n>：双方进行协商交互时的中间 Hash 数据。

SIGi：发起方的签名载荷。

SIGr：响应方的签名载荷。

CERT_sig_r：签名证书载荷。

CERT_enc_r：加密证书载荷。

Ni：发起方的 nonce 载荷。

Nr：响应方的 nonce 载荷。

<p>_b：载荷[1)]<p>的主体。

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。

4.2 缩略语

下列缩略语适用于本文件。

AH：鉴别头(Authentication Header)

CBC：密码分组链接(Cipher Block Chaining)

ESP：封装安全载荷(Encapsulating Security Payload)

GCM：Galois 计数器模式(Galois Counter Mode)

HMAC：采用带密钥杂凑的消息鉴别码(Keyed-Hash Message Authentication Code)

IPSec：IP 安全协议(Internet Protocol Security)

IPv4：互联网通信协议第四版(Internet Protocol version 4)

IPv6：互联网通信协议第六版(Internet Protocol version 6)

ISAKMP：互联网安全联盟与密钥管理协议(Internet Security Association and Key Management Protocol)

IV：初始化向量(Initialization Vector)

MAC：消息鉴别码(Message Authentication Code)

NAT：网络地址转换(Network Address Translation)

PRF：伪随机函数(Pseudo Random Function)

SA：安全联盟(Security Association)

UDP：用户数据报协议(User Datagram Protocol)

VPN：虚拟专用网络(Virtual Private Network)

5 密码算法和密钥类别

5.1 密码算法

IPSec VPN 使用的非对称密码算法、对称密码算法、密码杂凑算法和随机数生成算法应当符合密

1) 包括没有 ISAKMP 通用头的载荷。

码国家标准、行业标准的相关要求。各算法及使用要求如下。

a) 非对称密码算法应支持 SM2 椭圆曲线密码算法，用于实体鉴别、数字签名和数字信封。

b) 对称密码算法应支持 SM4 分组密码算法，用于密钥交换数据的加密保护和报文数据的加密保护；算法的工作模式应支持 CBC 或 GCM 模式。SM4 算法的使用应遵循 GB/T 32907—2016。GCM 模式的使用应遵循 GB/T 36624—2018 的机制 5。

c) 密码杂凑算法应支持 SM3 密码杂凑算法，用于完整性校验。SM3 算法的使用应遵循 GB/T 32905—2016。

d) 随机数生成算法生成的随机数应符合 GM/T 0005—2021 的要求，以及 GM/T 0062—2018 对 E 类产品的规定。

5.2 密钥类别

IPSec VPN 使用下列类别的密钥。

a) 设备密钥：非对称算法使用的公私钥对，包括签名密钥对和加密密钥对，用于实体验证、数字签名和数字信封。

注：设备包括硬件实现的产品（如软硬一体硬件产品），也包括纯软件实现的产品（如虚拟机形态产品）。

b) 工作密钥：在密钥交换第一阶段得到的密钥，用于会话密钥交换过程的保护。

c) 会话密钥：在密钥交换第二阶段得到的密钥，用于数据报文的加密和完整性校验。

6 协议

6.1 密钥交换协议

6.1.1 相关函数定义

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 SM2_Encrypt(Ski, pub_key)表示使用 SM2 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)：使用对称加密算法 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 SM4_Encrypt (Ni, key)表示使用 SM4 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，HASH 函数计算出的结果为定长值。如使用 SM3 密码杂凑算法对 msg 进行数据摘要计算，则计算出 256 位的杂凑值。

PRF(key,msg)：使用密钥 key，对消息 msg 进行数据摘要运算，计算结果为定长值。PRF 的计算方法如下：

PRF(key,msg)=HMAC(key,msg)。其中，HMAC 基于 SM3 实现。

6.1.2 交换阶段及模式

6.1.2.1 交换阶段

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。协议报文应使用 UDP 协议 500 或 4500 端口进行传输。

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 安全联盟。该安全联盟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。用这个安全联盟来保护 IPSec 安全联盟的协商过程。一个 ISAKMP 安全联盟可以用于建立多个 IPSec 安全联盟。

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

6.1.2.2 交换模式

本文件定义的密钥交换协议包括两种交换模式：主模式和快速模式，其中：主模式用于第一阶段交换，实现通信双方的身份鉴别和密钥交换，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 安全联盟的协商，确定通信双方的 IPSec 安全策略及会话密钥。

6.1.3 交换

6.1.3.1 概述

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。

SA 载荷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 SA 载荷中。本文件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，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 SA 载荷中。安全联盟的定义参见附录 A 的 A.21，有关变换载荷、建议载荷、SA 载荷的具体定义见 6.1.5。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，交换的发起方需终止协商。

6.1.3.2 第一阶段——主模式

主模式的交换过程由 6 个消息组成。双方身份的鉴别采用数字证书的方式。

本阶段涉及的消息头及载荷的具体内容见 6.1.5。

主模式的交换过程见图 1。

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

图 1 主模式的交换过程

消息 1：发起方向响应方发送一个封装有建议载荷的 SA 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 SA 载荷以及响应方的签名证书和加密证书，该载荷表明它所接受的发起方发送的 SA 提议。SA 载荷的具体内容见 6.1.5.3。

消息 3 和消息 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)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 用对方加密证书中的公钥加密保护，并且双方各自对数据进行数字签名。

当使用 SM2 算法进行加密和数字签名时，应遵循 GB/T 35276—2017 的要求。

发起方交换的数据如下：

XCHi = Asymmetric_Encrypt(Ski, pub_r) | Symmetric_Encrypt(Ni,Ski) | Symmetric_Encrypt(IDi,Ski)|CERT_sig_i|CERT_enc_i

SIGi_b = Asymmetric_Sign(Ski_b | Ni_b | IDi_b | CERT_enc_i_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(Skr_b | Nr_b | IDr_b|CERT_enc_r_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。

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（下述计算公式中的值 0，1，2 是单个字节的数值）：

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)

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 的一个 PRF 可产生 128 位的输出，但密码算法要求用到大于 128 位的密钥的时候，SKEYID_e 应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要求的位数。

消息 5 和消息 6：发起方和响应方鉴别前面的交换过程。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：

IV= HASH(Ski_b | Skr_b)

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。

为了鉴别交换，发起方产生 HASHi，响应方产生 HASHr，计算公式如下：

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

HASHr = PRF(SKEYID, CKY-R | CKY-I | SAr_b | IDr_b)

6.1.3.3 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：

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 cookie 来标识。因为快速模式的每个实例使用一个唯一的 MsgID，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。如果协商双方应指定 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 由于安全策略或其他原因没有被响应方所接受，则响应方应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 6.1.5。

快速模式的交换过程见图 2。

消息 1：发起方向响应方发送一个杂凑载荷、一个 SA 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 | Ni_b | SA [| IDi | IDr])

消息 2：响应方向发起方发送一个杂凑载荷、一个 SA 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_b |SA | Nr_b [| 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鉴别。

杂凑载荷中消息摘要的计算方法如下：

HASH_3= PRF(SKEYID_a,0 | MsgID | Ni_b | Nr_b)

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 是从协商得到的 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。

如果 IPSec SA 协商过程中选择的是 GCM 模式的可鉴别的加密机制，则加密算法所要求的加密密钥和 Salt 值都按照各自长度要求从 KEYMAT 中依次选取。本文件规定，在为 ESP 协议协商 IPSec SA 时，如果双方协商使用 GCM 模式的 SM4 加密算法（简称 SM4_GCM），此时则先选取 16 字节长度的 SM4 加密密钥，然后再选取 4 字节长度的 Salt 值，该 Salt 值用于构建 SM4_GCM 加密算法所要求的启动变量 S。GCM 模式的可鉴别的加密机制应遵守 GB/T 36624—2018 的规定。

当 PRF 函数的输出长度小于 KEYMAT 要求的密钥素材长度时，应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。

6.1.3.4 ISAKMP 信息交换

在第二阶段密钥交换过程中，安全联盟已经建立，则 ISAKMP 信息交换过程见图 3。

发起方	方向	响应方
HDR*, HASH_1, N/D	---->	

图 3 第二阶段的 ISAKMP 信息交换

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：

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 是最后一组密文和 MsgID 进行 Hash 运算所得到的，即 IV= HASH(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。在第一阶段密钥交换过程中，如果一方要启动 ISAKMP 消息交换，则按照图 4 的消息交换格式进行。如果双方密钥材料交换还未成功完成，则 ISAKMP 信息交换以明文发送；但如果双方密钥材料交换成功，则 ISAKMP 信息交换以密文发送，加密所使用的对称密码算法、加密工作模式和加密密钥跟第一阶段中消息 5 和消息 6 中的加密工作机制完全一致。

发起方	方向	响应方
HDR, N	---->	

图 4 第一阶段的 ISAKMP 信息交换

6.1.4 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见图 5。

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

图 5　支持 NAT 穿越的第一阶段交换过程

如果有必要，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应按照 RFC3947 的规定执行。

6.1.5　密钥交换的载荷格式

6.1.5.1　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备的信息。

ISAKMP 的头格式应与图 6 相符合。

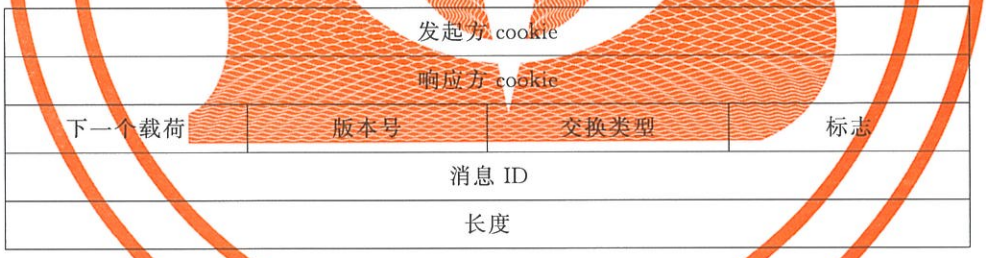

图 6　ISAKMP 头格式

发起方 cookie：这个字段是一个唯一的 8 字节二进制字符串，由发起方随机生成。

响应方 cookie：这个字段是一个唯一的 8 字节二进制字符串，由响应方随机生成。

Cookie 的生成方法应按照 RFC2408 的 2.5.3 要求生成。

下一个载荷：这个字段为 1 字节，说明消息中的第一个载荷的类型。

载荷类型的定义见表 1。

表 1　载荷类型的定义

下一个载荷	值
无（None）	0
安全联盟（Security association）	1

表 1　载荷类型的定义（续）

下一个载荷	值
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（Notification）	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）	15～19，22～127
私有使用（PrivateUse）	129～255

版本号：这个字段为 1 字节，其中 0～3 位表示主版本号，4～7 位表示次版本号。本文件规定主版本号为 1，次版本号为 1。

交换类型：这个字段为 1 字节，说明组成消息的交换的类型。交换类型的定义见表 2。

表 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
仅鉴别（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

本文件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 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 位，其他位在传输前被置为 0。具体定义如下：

——加密位：这是标志字段中的最低有效位。当这个位被置为 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。当这个位被置为 0 时，载荷不加密。

——提交位：这是标志字段的第 2 个位，本文件中其值为 0。

——仅鉴别位：这是标志字段的第 3 个位，本文件中其值为 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。它作为唯一的消息标志，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。

6.1.5.2 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。通用载荷头的格式应与图 7 相符合。

下一个载荷	保留	载荷长度

图 7 通用载荷头格式

下一个载荷：这个字段的长度为 1 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 1 定义。

保留：这个字段的长度为 1 字节，其值为 0。

载荷长度：这个字段的长度为 2 字节，长度数值以字节为单位，计算范围包含通用载荷头在内的整个载荷长度。

6.1.5.3 SA 载荷

SA 载荷用于协商安全联盟(包括 ISAKMP 安全联盟和 IPSec 安全联盟)，并且指定协商所基于的解释域 DOI。载荷的格式依赖于它所使用的 DOI，SA 载荷的类型值为 1。SA 载荷的格式应与图 8 相符合。

下一个载荷	保留	载荷长度
解释域(DOI)		
情形		

图 8 SA 载荷格式

下一个载荷：这个字段的长度为 1 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 1 定义。

保留：这个字段的长度为 1 字节，其值为 0。

载荷长度：这个字段的长度为 2 字节，长度数值以字节为单位，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 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 字节，表明协商发生时的情形，用来决定要求的安全服务的信息。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 正在一个需经标记的完整性环境中协商。

本文件默认采用 SIT_IDENTITY_ONLY 情形。

6.1.5.4 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。建议载荷的格式应与图 9 相符合。

图 9 建议载荷格式

下一个载荷：这个字段的长度为 1 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 字节，其值为 0。

载荷长度：这个字段的长度为 2 字节，长度数值以字节为单位，用于表示整个建议载荷的长度，计算范围包括通用载荷头、建议载荷所有与该建议有关的变换载荷，该长度仅用于标示本建议载荷的长度。

建议号：这个字段的长度为 1 字节，用于表示本建议载荷的建议编号。多个建议的建议号相同表示这些建议是“逻辑与”的关系，多个建议的建议号不同表示这些建议是“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 字节，用于表示协议标识符。协议标识符的定义见表 3。

表 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 字节，长度数值以字节为单位，用于表示 SPI 的长度。在第一阶段该长度值为 0，在第二阶段该长度值为 4。

变换数：这个字段的长度为 1 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 字节，其内容是该建议的提出者产生的随机数。

6.1.5.5 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。变换载荷的格式应与图10相符合。

下一个载荷	保留	载荷长度
变换号	变换ID	保留2
SA属性		

图10 变换载荷格式

下一个载荷：这个字段的长度为1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字节，其值为0。

载荷长度：这个字段的长度为2字节，长度数值以字节为单位，用于表示本变换载荷的长度。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字节，用于表示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字节，用于表示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的定义见表4。ESP协议的变换ID的定义见表5。

表4 AH协议的变换ID的定义

变换ID	描述	值
RESERVED	未使用	0、1
AH_SM3	使用带256位SM3密码杂凑算法的HMAC	20

表5 ESP协议的变换ID的定义

变换ID	描述	值
RESERVED	未使用	0
ESP_SM4_CBC	采用SM4分组密码算法的CBC模式	127
ESP_SM4_GCM	采用SM4分组密码算法的GCM模式	130

保留2：这个字段的长度为2字节，其值为0。

SA属性：该字段的长度是可变的，用于表示本变换的SA属性。该字段的具体定义见6.1.5.6。

当为ESP协议选择ESP_SM4_GCM变换时，由于SM4_GCM模式能同时为数据报文提供私密性和完整性校验服务，因此无需为ESP协议单独协商完整性校验服务。本文件规定，当为ESP选择ESP_SM4_GCM变换时，SM4_GCM加密算法的输入为启动变量S由IPSec SA协商时生成的4字节Salt值和8字节初始化向量IV串接得到(启动变量S总长度为12字节)；额外可鉴别数据AAD为ESP头中的4字节安全参数索引(SPI值)和序列号(如果双方协商采用扩展序列号属性，则序列号为8字节，否则为4字节)的串接，额外可鉴别数据AAD总长度为8字节或12字节。SM4_GCM加密算法的

输出中，除了输出与明文同等长度的密文外，还输出长度为16字节的标签数据。应按照RFC4304的要求使用扩展序列号属性。

6.1.5.6 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属性载荷的格式应与图11相符合。

图11 SA属性载荷格式

属性类型：这个字段的长度为2字节，用于表示属性类型。该字段的最高有效位(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位为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。如果属性类型是变长的，并且属性值能在2字节中表示，那么变长的属性可以用定长表示。

第一阶段密钥交换的SA属性载荷的属性类型的定义见表6。

表6 第一阶段密钥交换属性类型的定义

分类	值	长度
加密算法	1	定长
HASH算法	2	定长
鉴别方式	3	定长
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
分组大小	17	定长
非对称算法类型	20	定长

第二阶段密钥交换属性类型的定义见表7。

表7 第二阶段密钥交换属性类型的定义

分类	值	长度
SA生存期类型（SA Life Type）	1	定长
SA生存期（SA Life Duration）	2	变长
封装模式（Encapsulation Mode）	4	定长
鉴别算法（Authentication Algorithm）	5	定长

表 7　第二阶段密钥交换属性类型的定义（续）

分类	值	长度
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
扩展序列号(Extended Sequence Number)	11	定长

属性值：这个字段如果是定长的，其长度为 2 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。

如果一个 IPSec 实现接收到了一个它不支持的属性值，它应发送一个属性不支持通知消息，并终止本次 SA 协商。

第一阶段加密算法属性值的定义见表 8。

表 8　第一阶段加密算法属性值的定义

可选择算法的名称	描述	值
ENC_ALG_SM4	SM4 分组密码算法	129

第一阶段密码杂凑算法属性值的定义见表 9。

表 9　第一阶段密码杂凑算法属性值的定义

名称	描述	值
HASH_ALG_SM3	SM3 密码杂凑算法	20

第一阶段鉴别方式属性值的定义见表 10。

表 10　第一阶段鉴别方式属性值的定义

名称	描述	值
AUTH_METHOD_DE	公钥数字信封鉴别方式	10

适用于第一阶段和第二阶段的 SA 生存期类型属性值的定义见表 11。

表 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见表 12。

表 12　第一阶段公钥算法类型属性值的定义

名称	描述	值
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见表 13。

表 13　第二阶段封装模式属性值的定义

名称	描述	值
RESERVED	未使用	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

第二阶段鉴别算法属性值的定义见表 14。

表 14　第二阶段鉴别算法属性值的定义

名称	描述	值
RESERVED	未使用	0
HMAC_SM3	采用 SM3 密码杂凑算法的 HMAC	20

当为 ESP 协议协商的加密服务为 SM4_GCM 时，由于 SM4_GCM 可以同时提供加密和完整性校验服务，因此无需为 ESP 协商单独的鉴别算法。

第二阶段扩展序列号属性值的定义见表 15。

表 15　第二阶段扩展序列号属性值的定义

名称	描述	值
RESERVED	未使用	0
64BITSEQNUM	采用 64bit 的扩展序列号	1

6.1.5.7　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。标识载荷的格式应与图 12 相符合。

下一个载荷：这个字段的长度为 1 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 1 定义。

保留：这个字段的长度为 1 字节，其值为 0。

载荷长度：这个字段的长度为 2 字节，长度数值以字节为单位，用于包含通用载荷头在内的整个载

荷长度。

下一个载荷	保留	载荷长度
标识类型	协议 ID	端口
标识数据		

图 12　标识载荷格式

标识类型：这个字段的长度为 1 字节，用于表示标识数据字段中的身份信息类型。标识类型的定义见表 16。

表 16　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_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_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：

ID_DER_ASN1_DN。

在第二阶段可以使用的标识类型：

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 字节，用于表示一个 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 字节，用于表示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，用于表示与 ID 类型字段相对应的标识信息。

6.1.5.8　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。

证书载荷的格式应与图 13 相符合。

下一个载荷	保留	载荷长度
证书编码	证书数据	
证书数据		

图 13　证书载荷格式

下一个载荷：这个字段的长度为 1 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 1 定义。

保留：这个字段的长度为 1 字节，其值为 0。

载荷长度：这个字段的长度为 2 字节，长度数值以字节为单位，用于表示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 字节，用于表示证书数据字段的证书编码类型。证书编码类型定义见表 17。

表 17　证书编码类型定义

证书类型	值
X.509 签名证书	4
X.509 加密证书	5

在本文件中，只能使用 X.509 格式的签名证书和加密证书。

证书数据：这个字段是变长字段，证书的结构及定义应遵循 GB/T 20518—2018。

6.1.5.9　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。杂凑载荷的格式应与图 14 相符合。

下一个载荷	保留	载荷长度
杂凑数据		

图 14　杂凑载荷格式

下一个载荷：这个字段的长度为 1 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 1 定义。

保留：这个字段的长度为 1 字节，其值为 0。

载荷长度：这个字段的长度为 2 字节，长度数值以字节为单位，用于表示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。

6.1.5.10　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。签名载荷的格式应与图 15 相符合。

下一个载荷	保留	载荷长度
签名数据		

图 15　签名载荷格式

下一个载荷：这个字段的长度为 1 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 1 定义。

保留：这个字段的长度为 1 字节，其值为 0。

载荷长度：这个字段的长度为 2 字节，数值长度以字节为单位，用于表示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。

6.1.5.11　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 载荷的格式应与图 16 相符合。

下一个载荷	保留	载荷长度
Nonce 数据		

图 16　Nonce 载荷格式

下一个载荷：这个字段的长度为 1 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 1 定义。

保留：这个字段的长度为 1 字节，其值为 0。

载荷长度：这个字段的长度为 2 字节，长度数值以字节为单位，用于表示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。

6.1.5.12　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，通知载荷的格式应与图 17 相符合。

下一个载荷	保留	载荷长度
解释域(DOI)		
协议 ID	SPI 长度	通知消息类型
安全参数索引(SPI)		
通知数据		

图 17　通知载荷格式

下一个载荷：这个字段的长度为 1 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 1 定义。

保留：这个字段的长度为 1 字节，其值为 0。

载荷长度：这个字段的长度为 2 字节，长度数值以字节为单位，用于表示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字节,这个字段的值为1。

协议ID:这个字段的长度为1字节,用于表示协议标识符。协议标识符的定义如表3所示。

SPI长度:这个字段的长度为1字节,长度数值以字节为单位,用于表示SPI的长度。在第一阶段该长度值为0,在第二阶段该长度值为4。

通知消息类型:这个字段的长度为2字节,用于表示通知消息类型。

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。

通知消息的错误类型见表18。

表18 通知消息的错误类型

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

表 18　通知消息的错误类型（续）

通知类型	描述	值
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	31～8 191
PRIVATE	私有	8 192～16 383

通知消息的状态类型见表 19。

表 19　通知消息的状态类型

通知类型	值
已连接	16 384
保留(将来使用)	16 385～24 575
特定于解释域(DOI)的编码	24 576～32 767
私有(将来使用)	32 768～40 959
保留(将来使用)	40 960～65 535

6.1.5.13　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。删除载荷的格式应与图 18 相符合。

图 18　删除载荷格式

下一个载荷：这个字段的长度为 1 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 1 定义。

保留：这个字段的长度为 1 字节，其值为 0。

载荷长度：这个字段的长度为 2 字节，长度数值以字节为单位，用于表示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字节,其值为1。

协议ID:这个字段的长度为1字节,用于表示要删除的SA的协议标识符。协议标识符的定义如表3所示。

SPI长度:这个字段的长度为1字节,长度数值以字节为单位,用于表示SPI的长度。删除第一阶段的SA时该长度值为16,删除第二阶段的SA时该长度值为4。

SPI数目:这个字段的长度为2字节,用于表示本载荷中包含的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。

6.1.5.14 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载荷的格式应与图19相符合。

图19 厂商ID载荷格式

下一个载荷:这个字段的长度为1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1定义。

保留:这个字段的长度为1字节,其值为0。

载荷长度:这个字段的长度为2字节,长度数值以字节为单位,用于表示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。

6.1.5.15 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载荷的格式应与图20相符合。

图20 NAT_D载荷格式

下一个载荷:这个字段的长度为1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1定义。

保留:这个字段的长度为1字节,其值为0。

载荷长度:这个字段的长度为2字节,长度数值以字节为单位,用于表示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(CKY-I | CKY-R | IP | Port)

6.1.5.16 NAT_OA载荷

NAT_OA载荷用于密钥交换第二阶段中,当使用传输模式穿越NAT时应传送这个载荷,本载荷

的类型值为 21。NAT_OA 载荷的载荷格式应与图 21 相符合。

下一个载荷	保留	载荷长度
ID 类型	保留 2	
NAT_OA 数据		

图 21　NAT_OA 载荷格式

下一个载荷：这个字段的长度为 1 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 1 定义。

保留：这个字段的长度为 1 字节，其值为 0。

载荷长度：这个字段的长度为 2 字节，长度数值以字节为单位，用于表示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 字节，其值为表 16 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 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。

6.1.5.17　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应与图 22 相符合。

下一个载荷	保留	载荷长度
对称密钥密文		

图 22　对称密钥载荷格式

下一个载荷：这个字段的长度为 1 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 1 定义。

保留：这个字段的长度为 1 字节，其值为 0。

载荷长度：这个字段的长度为 2 字节，长度数值以字节为单位，用于表示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。

6.1.6　密钥交换的数据包格式

6.1.6.1　概述

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，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 6.1.6 的所有图中，“下一载荷”用“NP”来表示。

6.1.6.2　主模式消息 1 的数据包格式

主模式消息 1 的数据包的格式应与图 23 相符合，其中 SA 载荷中应支持 SM4-SM3 变换载荷。

发起方 cookie			
响应方 cookie			
NP SA:1	版本号:0x11	交换类型	标志:0
消息 ID:0			
长度			
NP :0	保留	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(ISAKMP)	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	保留	
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	保留	
备选变换中各属性载荷			

图 23　主模式消息 1 的数据包格式

6.1.6.3　主模式消息 2 的数据包格式

主模式消息 2 的数据包的格式应与图 24 相符合。

发起方 cookie			
响应方 cookie			
NP SA:1	版本号:0x11	交换类型	标志:0
消息 ID:0			
长度			
NP:6(证书)	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:1
NP NULL:0	保留:0	载荷长度	
变换号 1	变换 ID:1	保留 2	
变换中各属性载荷			
NP 证书:6	保留:0	载荷长度	
证书编码:4	签名证书数据 4		
签名证书数据			
NP NULL:0	保留:0	载荷长度	
证书编码:5	加密证书数据 5		
加密证书数据			

图 24　主模式消息 2 的数据包格式

6.1.6.4 主模式消息 3 的数据包格式

使用证书鉴别的主模式消息 3 数据包的格式应与图 25 相符合。

发起方 cookie			
响应方 cookie			
NP 对称密钥:128	版本号:0x11	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	
受对称密钥加密的标识数据			
NP 证书:6	保留:0	载荷长度	
证书编码: 4	签名证书数据 4		
签名证书数据			
NP 签名:9	保留:0	载荷长度	
证书编码: 5	加密证书数据 5		
加密证书数据			
NP NULL:0	保留:0	载荷长度	
签名数据			

图 25 主模式消息 3 的数据包格式

6.1.6.5 主模式消息 4 的数据包格式

主模式消息 4 数据包的格式应与图 26 相符合。

发起方 cookie			
响应方 cookie			
NP 对称密钥:128	版本号:0x11	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	
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 26 主模式消息 4 的数据包格式

6.1.6.6 主模式消息 5 的数据包的格式

主模式消息 5 的数据包格式应与图 27 相符合。

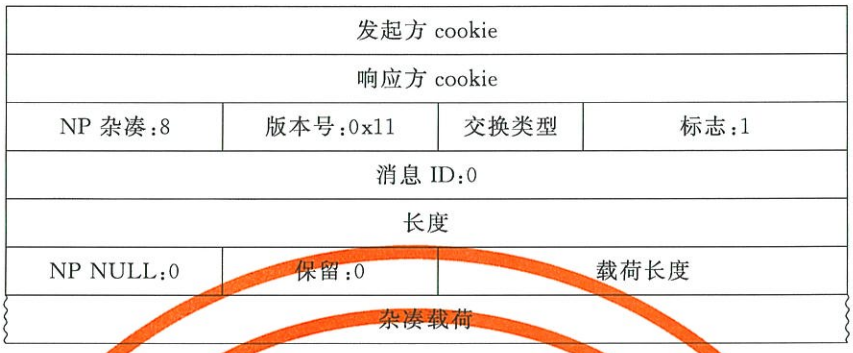

图 27 主模式消息 5 的数据包格式

6.1.6.7 主模式消息 6 的数据的包格式

主模式消息 6 的数据包的格式应与图 28 相符合。

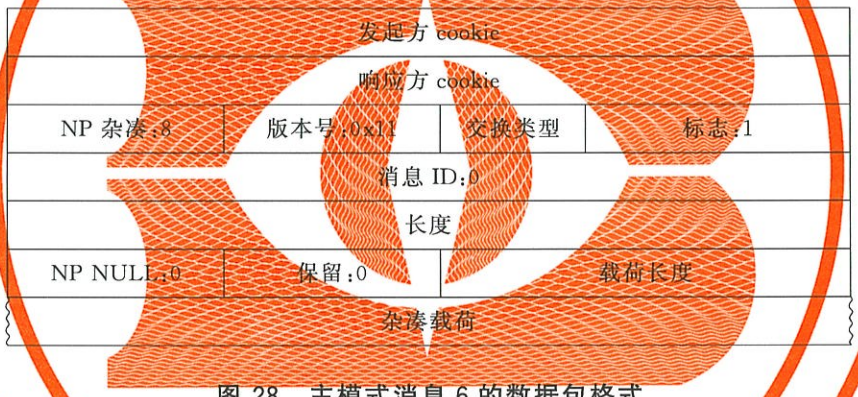

图 28 主模式消息 6 的数据包格式

6.1.6.8 快速模式消息 1 的数据包格式

快速模式消息 1 的数据包的格式应与图 29 相符合，其中 SA 载荷中有一个 ESP 协议建议，建议中有两种变换，其中一个为 ESP_SM4_CBC，另一个为 ESP_SM4_GCM(并采用扩展序列号机制)。

发起方 cookie			
响应方 cookie			
NP 杂凑:8	版本号:0x11	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(ESP)	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:130 (ESP_SM4_GCM)	保留 2	
首选变换中各属性载荷(包括扩展序列号属性载荷)			
NP NULL:0	保留:0	载荷长度	
变换号 2	变换 ID:129 (ESP_SM4_CBC)	保留 2	
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			
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 29　快速模式消息 1 的数据包格式

图 29 中,属性载荷字段包括了扩展序列号属性载荷,其位置没有特别要求。

6.1.6.9　快速模式消息 2 的数据包格式

快速模式消息 2 的数据包的格式应与图 30 相符合。

发起方 cookie			
响应方 cookie			
NP 杂凑:8	版本号:0x11	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(ESP)	SPI 长度	变换载荷数:1
SPI			
NP NULL:0	保留:0	载荷长度	
变换号 1	变换 ID:130 (ESP_SM4_GCM)	保留 2	
变换中各属性载荷(包括扩展序列号属性载荷)			
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 30　快速模式消息 2 的数据包格式

图 30 中:选择了 ESP_SM4_GCM 变换,并接受扩展序列号模式;属性载荷字段包括了扩展序列号属性载荷,其位置没有特别要求。

6.1.6.10　快速模式消息 3 的数据包格式

快速模式消息 3 的数据包的格式应与图 31 相符合。

发起方 cookie			
响应方 cookie			
NP 杂凑:8	版本号:0x11	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	
杂凑载荷			

图 31　快速模式消息 3 的数据包格式

6.2　安全报文协议

6.2.1　鉴别头协议 AH

6.2.1.1　概述

鉴别头协议 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 头提供尽可能多的鉴别,同时为上层协议数据提供鉴别。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,因此本文件规定 AH 不能单独使用,而需和封装安全载荷协议 ESP 嵌套使用。

6.2.1.2　AH 头格式

AH 头格式应与图 32 相符合。AH 头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				
鉴别数据(变长的)				

图 32　AH 头格式

下一个头:这个字段的长度为 1 个字节,该字段指定了鉴别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:这个字段的长度为一个 1 字节,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:这个字段的长度为一个 2 字节,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(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 1～255 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 字节或 8 字节(当双方协商采用扩展序列号时)的单调递增计数

器，发送方对使用该 SA 的每个数据报文进行计数，接收方应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。扩展序列号的使用方法可参考 RFC 4302 的附录 B 和 RFC 4303 的附录 A。

鉴别数据：鉴别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）。该字段的长度应为 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。

6.2.1.3 鉴别头 AH 的处理

6.2.1.3.1 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（见图 33）。

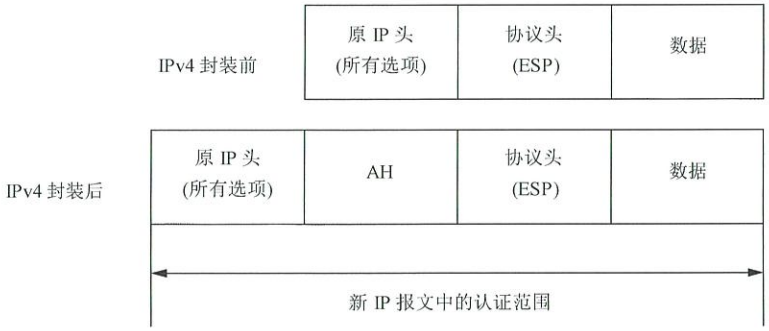

图 33 IPv4 的 AH 传输模式

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（见图 34）。

图 34 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 35和图 36 分别表示了隧道模式中典型的 IPv4 和 IPv6 报文的 AH 头的位置。

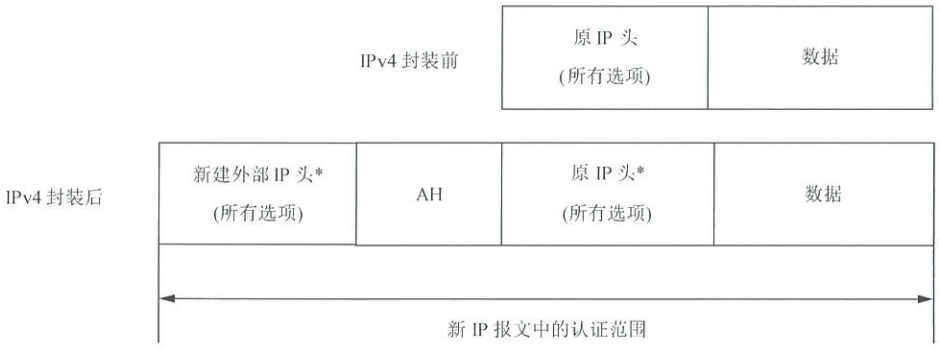

图 35　IPv4 的 AH 隧道模式

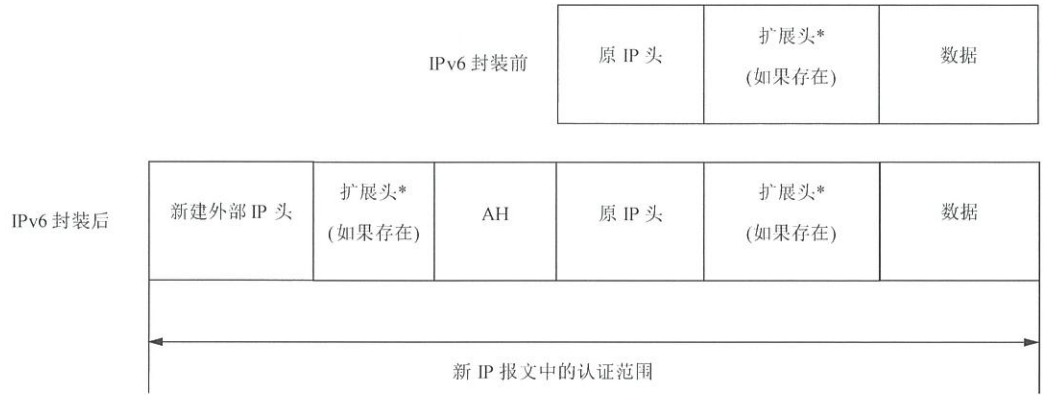

图 36　IPv6 的 AH 隧道模式

6.2.1.3.2　出站报文处理

6.2.1.3.2.1　概述

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、鉴别数据字段的填充和分片过程。

6.2.1.3.2.2　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交换过程，建立 SA。

6.2.1.3.2.3　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（当双方协商使用扩展序列号时，序列号计数器为 8 字节计数器，否则为 4 字节计数器）。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（如果采用扩展序列号模式，则该序列号字段值为扩展序列号值的低端 4 字节值）。当该计数器计数达到最大值前，应生成新的 SA。

6.2.1.3.2.4　计算完整性校验值 ICV

6.2.1.3.2.4.1　概述

发送方采用指定的完整性校验算法对报文计算 ICV。本文件规定的完整性校验算法为 SM3，摘要

值长度为256位。IPv4和IPv6的ICV计算方法分别见6.2.1.3.2.4.2～6.2.1.3.2.4.3。

6.2.1.3.2.4.2 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。

6.2.1.3.2.4.3 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选项包含有一位，该位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改变的任何选项，整个“选项数据(Option Data)”字段在计算和校验ICV时应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。由该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，其中鉴别数据字段在计算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。

6.2.1.3.2.5 鉴别数据的填充

AH头中的鉴别数据字段应确保是4字节(IPv4)或8字节(IPv6)的整数倍，否则应填充。填充应放在鉴别数据字段的最末端，其内容由发送方任意选择，并且参与ICV计算。

6.2.1.3.2.6 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。

6.2.1.3.3 入站报文处理

6.2.1.3.3.1 概述

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过程。

6.2.1.3.3.2 重组

如果有必要，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。

6.2.1.3.3.3 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。

6.2.1.3.3.4 验证序列号

所有 AH 实现应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。

6.2.1.3.3.5 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。

6.2.1.3.3.6 匹配安全策略

检查数据包是否符合设置的安全策略要求。

6.2.2 封装安全载荷 ESP

6.2.2.1 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，同时选择机密性和数据源鉴别服务，或选择可鉴别的加密机制同时实现机密性和数据源鉴别功能。当 ESP 和 AH 结合使用时，不能为 ESP 选择单独的数据源鉴别服务，也不能为 ESP 选择可鉴别的加密机制。

6.2.2.2 ESP 头定义

6.2.2.2.1 ESP 头格式

ESP 头格式见图 37，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。

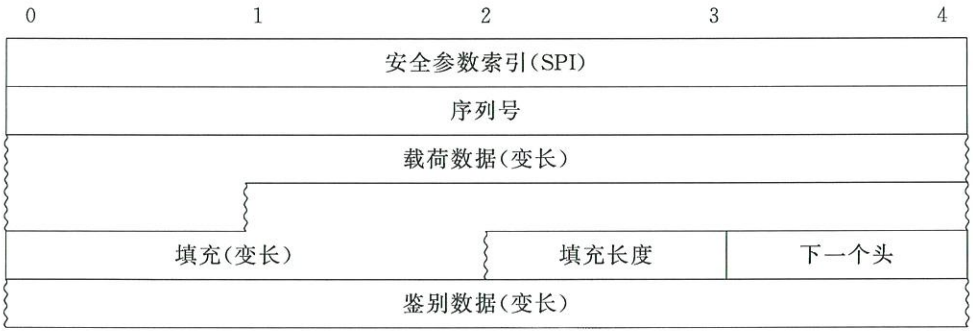

图 37　ESP 头格式

6.2.2.2.2　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 1～255 范围的 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。

6.2.2.2.3　序列号

序列号是一个无符号的 4 字节或 8 字节(当双方协商使用扩展序列号时)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，接收方应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。

6.2.2.2.4　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。

当为 ESP 协议选择 ESP_SM4_GCM 变换时，IV 长度为 8 字节。

6.2.2.2.5　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，则应对不足的部分进行填充，填充以字节为单位。如果有必要，也可以提供更多的填充数据，但应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。

6.2.2.2.6　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 0～255，其中 0 表明没有填充字节。

6.2.2.2.7　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。

6.2.2.2.8　鉴别数据

鉴别数据是一个变长字段，它是一个完整性校验值 ICV，该字段是可选的，只有当 SA 选择了完整

性校验服务或选择了可鉴别的加密机制时，才包含鉴别数据字段。

在 ESP 协议选择了完整性校验服务时，鉴别数据是对 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。

当 ESP 协议选择了 ESP_SM4_GCM 变换时，鉴别数据字段的值为 SM4_GCM 加密算法输出的标签 T，长度为 16 字节。

6.2.2.3 封装安全载荷 ESP 的处理

6.2.2.3.1 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（见图 38），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。

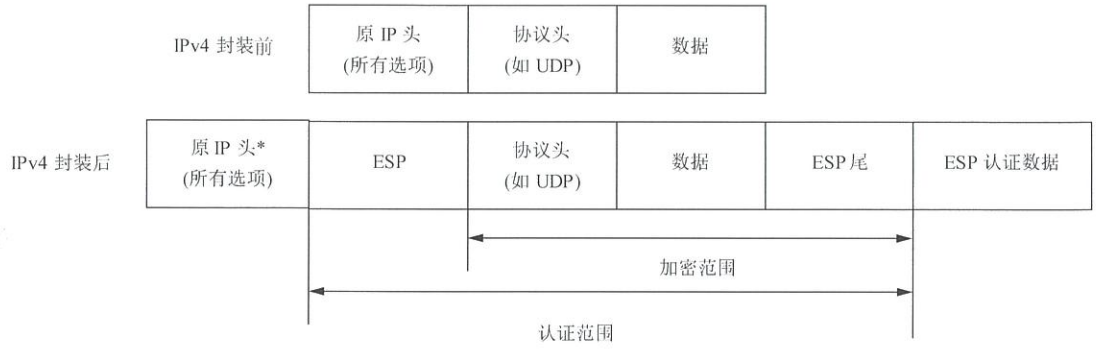

图 38 IPv4 的 ESP 传输模式

在 IPv6 环境中使用传输模式，ESP 被看作是一个端到端的载荷，因而应出现在逐跳（hop-by-hop）、路由（routing）和分片扩展头（fragmentation extensionheaders）之后（见图 39），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。

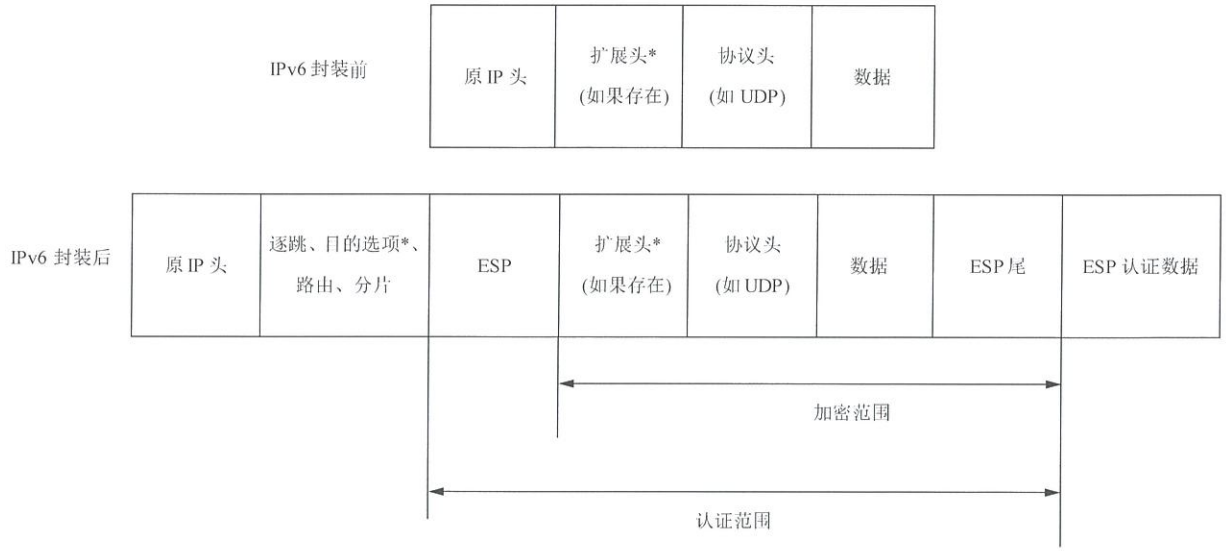

图 39 IPv6 的 ESP 传输模式

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（分别见图 40

和图 41)，图 40 和图 41 中的“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。

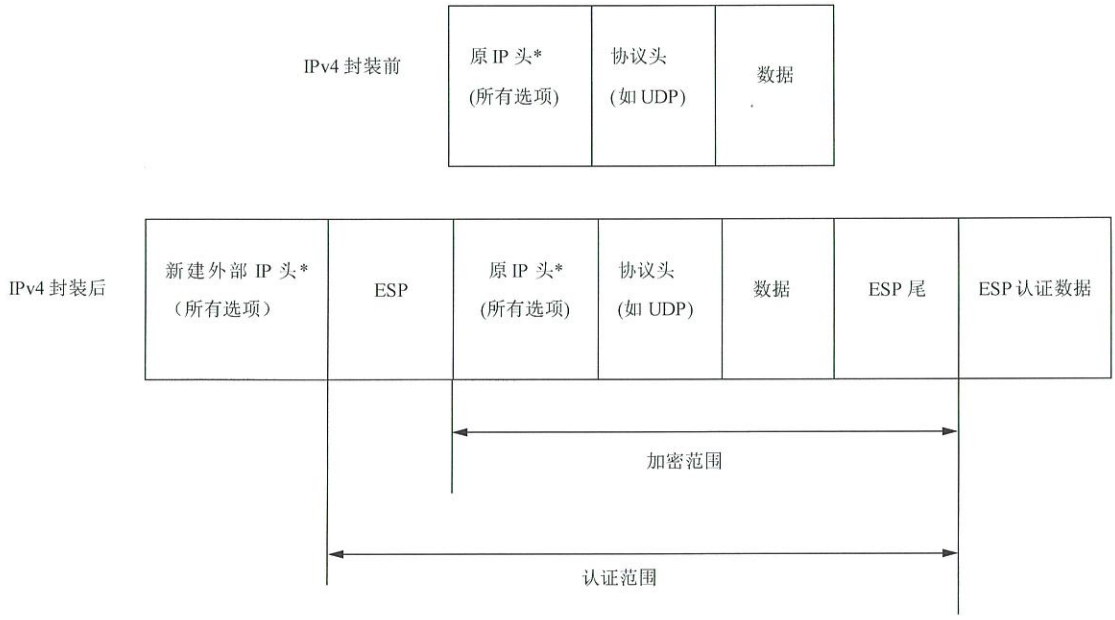

图 40　IPv4 的 ESP 隧道模式

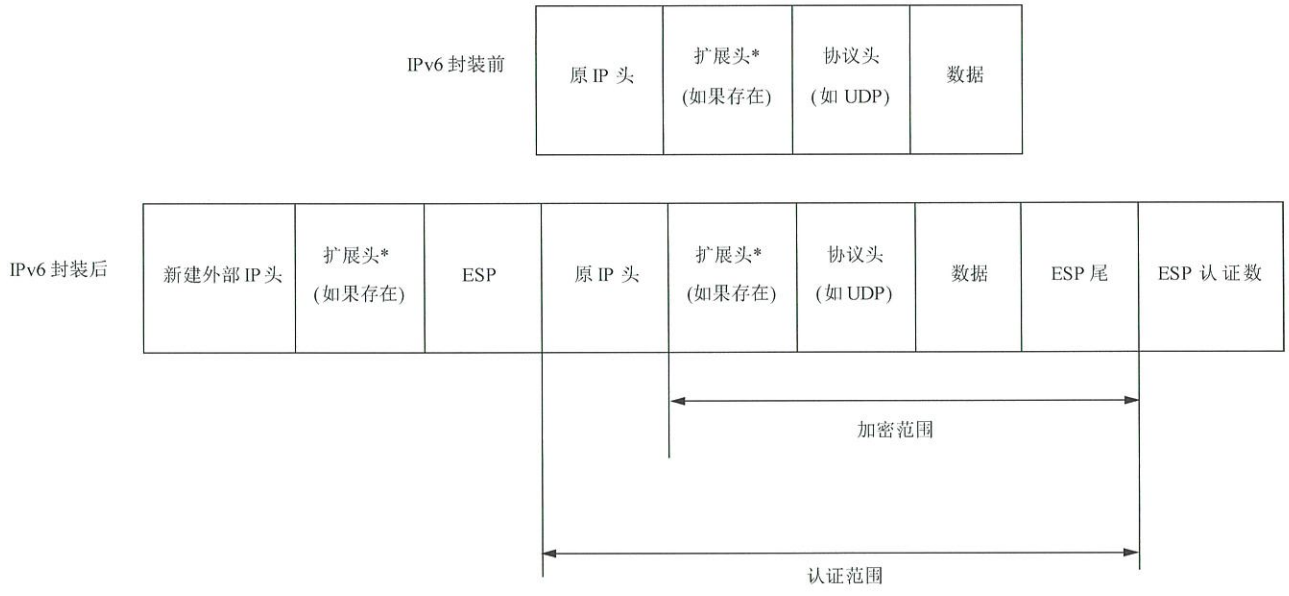

图 41　IPv6 的 ESP 隧道模式

6.2.2.3.2　出站报文处理

6.2.2.3.2.1　概述

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过程，并按照以下顺序进行处理。

6.2.2.3.2.2 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交换过程，建立 SA。

6.2.2.3.2.3 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。

6.2.2.3.2.4 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(当双方协商使用扩展序列号时，序列号计数器为 8 字节计数器，否则为 4 字节计数器)。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(如果采用扩展序列号模式，则只是计数器的低端 4 字节值)。当该计数器计数达到最大值前，应生成新的 SA。

6.2.2.3.2.5 加密报文

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

如果 ESP 协议协商使用 GCM 模式的可鉴别的加密机制，则在加密报文时，应提供额外的可鉴别数据 AAD 作为可鉴别的加密机制的输入(AAD 数据构造方式见 6.1.5.5)。采用可鉴别的加密机制对报文进行加密操作后，除了得到同等长度的密文数据，还会生成一个 16 字节的用于数据完整性校验的标签 T。这个标签 T 将赋值于 ESP 报文中的鉴别数据字段，用于实现对数据的完整性校验。

6.2.2.3.2.6 计算完整性校验值

如果 SA 提供完整性校验服务，发送方在除去鉴别数据字段的 ESP 报文上计算 ICV。将计算后得到的 ICV 值赋于鉴别数据字段。

如果 SA 协商的是 GCM 模式，则无需选择额外的完整性校验服务，而是直接使用 GCM 加密模式中输出的标签 T 作为 ICV，然后赋于鉴别数据字段。

6.2.2.3.2.7 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。

6.2.2.3.3 入站报文处理

6.2.2.3.3.1 概述

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、解密报文和重构过程，并按 6.2.2.3.3.2～6.2.2.3.3.7 的顺序进行处理。

6.2.2.3.3.2 重组

如果有必要，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。

6.2.2.3.3.3 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。

6.2.2.3.3.4 验证序列号

所有 ESP 实现应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。

6.2.2.3.3.5 验证完整性校验值

如果 ESP 加密时选择的不是 GCM 模式，则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。

如果为 ESP 协议协商的是 ESP_SM4_GCM 变换，则验证完整性校验值的操作在执行解密报文的操作中同步完成(见 6.2.2.3.3.6)。

6.2.2.3.3.6 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。根据解密后报文中填充数据的长度及内容判断是否解密成功，解密失败则丢弃该报文。

如果为 ESP 协议协商的是 ESP_SM4_GCM 变换，则 SM4_GCM 解密算法输入为：额外鉴别数据 AAD 为 ESP 头中的安全参数索引(SPI 值)和序列号(4 字节或 8 字节)的串接；启动变量 S 为 SA 协商时得到的 4 字节 Salt 值和 8 字节 IV 值的串接；T 为 ESP 报文尾部的数据鉴别字段中获取的 ICV 值。在执行 SM4_GCM 解密算法时，如果计算得到的标签 T′值与 T 值不一致，则将丢弃收到的数据报文。

6.2.2.3.3.7 重构

对解密成功的报文，重构原始 IP 数据报文。

6.2.3 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 RFC 3948 的要求实现。

6.2.4 匹配安全策略

检查数据包是否符合设置的安全策略要求。

7 IPSec VPN 产品要求

7.1 产品功能要求

7.1.1 随机数生成

IPSec VPN 产品使用的随机数应采用安全方式生成，随机数质量应符合 GM/T 0005—2021 要求。

7.1.2 密码算法

IPSec VPN 产品应支持 SM2、SM3、SM4 等密码算法，并将 SM2、SM3、SM4 等密码算法作为默认密码套件使用。

7.1.3 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。

7.1.4 密钥交换

IPSec VPN 产品应具有密钥交换功能，通过协商产生工作密钥和会话密钥。

密钥交换协议应按照 6.1 的要求进行。

7.1.5 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，或者应协商采用可鉴别的加密机制。

安全报文封装协议应按照 6.2 的要求进行。

7.1.6 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 6.2.3 的要求进行。

7.1.7 鉴别方式

IPSec VPN 产品应具有实体鉴别的功能，身份鉴别数据应支持数字证书方式。

7.1.8 IP 协议版本支持

IPSec VPN 产品应支持 IPv4 协议或 IPv6 协议。

7.1.9 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。

7.1.10 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 h。

会话密钥的最大更新周期不大于 1 h。

7.2 产品性能参数

7.2.1 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(IPv6 是 1408 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。

7.2.2 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(IPv6 是 1408 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。这里要注意,在计算加解密时延时,要去掉网络本身时延。

7.2.3 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(IPv6 是 1408 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。

7.2.4 每秒新建连接数

每秒新建连接数是指 IPSec VPN 产品在 1 s 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。

7.3 安全管理要求

7.3.1 密钥管理

7.3.1.1 设备密钥

设备密钥是非对称密钥,包括签名密钥对和加密密钥对。

签名密钥对由 IPSec VPN 产品自身产生,其公钥应能按照 GM/T 0092—2020 规定的格式导出,用于向 CA 认证机构申请证书。

加密密钥对由 CA 的密钥管理系统产生,并在申请签名证书时由 CA 一并签发加密证书,签名证书、加密证书和用保护机制保护的加密私钥应能被导 IPSecVPN 产品中,其中私钥保护应遵循 GM/T 0016要求。

签名证书、加密证书和加密密钥对的私钥应能被导入 IPSec VPN 产品中。

在 IPSec VPN 产品中,设备密钥的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,并在有必要时能够恢复。

7.3.1.2 工作密钥

工作密钥在密钥交换的第一阶段产生,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、设备关机或断电时应销毁。

7.3.1.3 会话密钥

会话密钥在密钥交换的第二阶段产生,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、设备关机或断电时应销毁。

7.3.2 数据管理

7.3.2.1 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鉴别。

7.3.2.2 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：

a) 操作行为，包括但不限于登录认证、参数配置、策略配置、密钥管理操作。

b) 安全事件，包括安全联盟的协商成功、协商失败、过期事件。

c) 异常事件，包括但不限于解密失败、完整性校验失败异常事件的统计。

7.3.3 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、备份和恢复操作。管理员进行管理操作前应通过身份鉴别。

登录口令长度应不小于 8 个字符。登录失败重试次数不应超过 8 次，并具有重复登录失败的安全保护机制。

7.3.4 产品管理

7.3.4.1 硬件安全

应提供安全措施确保 IPSec VPN 产品中密码算法、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。产品内部的调试、检测接口应在产品定型后删除。

7.3.4.2 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，裁减一切不要求的模块，关闭所有不要求的端口和服务。

任何操作指令及其任意组合，不能泄露密钥和敏感信息。

7.3.4.3 设备初始化

IPSec VPN 产品的初始化，除应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、管理员的产生操作均应由用户完成。

7.3.4.4 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。

与管理中心的通信应采用加密通道和身份鉴别安全措施。

7.3.4.5 设备自检

产品启动时，应对密码运算部件或模块关键部件或模块进行正确性检查。

应对包括存储密钥在内的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。

7.3.4.6 设备物理安全防护

在工艺设计、硬件配置等方面要采取相应的保护措施，保证设备基本的物理安全防护功能。

8 IPSec VPN 产品检测

8.1 产品功能检测

8.1.1 随机数功能

按照 GM/T 0005—2021 的要求提取样本，并按照该标准的相关要求进行检测，检测结果应合格。

8.1.2 密码算法

测试产品在出厂状态下，建立一条 IPSec 配置，查看其密码套件配置选项，默认使用的算法应为 SM2、SM3、SM4 等国家密码算法。

8.1.3 工作模式

将测试产品与被测产品均设置为隧道模式，应能成功完成密钥交换，建立 IPSec 隧道进行通信。

被测产品支持传输模式时，将测试产品与被测产品均设置为传输模式，应能成功完成密钥交换，进行通信。

将测试产品与被测产品一方设置为隧道模式，另一方设置为传输模式，密钥交换应失败，无法建立 IPSec 隧道进行通信。

8.1.4 密钥交换

密钥交换的检测按 7.1.4 的方法进行。对密钥交换过程进行网络数据截获，查看其过程应符合 6.1 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。

8.1.5 安全报文封装

将测试产品与被测产品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 6.2 的要求，应能正确进行加解密通信。

将测试产品与被测产品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 6.2 的要求，应能正确进行加解密通信。

8.1.6 NAT 穿越

将被测产品放在 NAT 下，与测试产品进行隧道测试，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 6.1.3 的方法进行密钥交换。对密钥交换过程进行网络数据截获，查看其过程应符合 7.1.4 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 7.1.5 的要求。

8.1.7 鉴别方式

按被测产品提供的鉴别方式，按 7.1.4 的方法进行密钥交换，应能成功完成协商过程，建立 IPSec 隧道进行通信。

8.1.8 IP 协议版本支持

在 IPv4 或者 IPv6 的环境下，按 7.1.4 的方法进行密钥交换，应能成功完成协商过程，建立 IPSec 隧道进行通信。

8.1.9 抗重放攻击

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

8.1.10 密钥更新

在被测产品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。

如果被测产品具有根据流量更新密钥的功能，在被测产品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。

8.2 产品性能检测

8.2.1 加解密吞吐率

按 7.2.1 的要求进行测试，记录测试结果。

8.2.2 加解密时延

按 7.2.2 的要求进行测试，记录测试结果。

8.2.3 加解密丢包率

按 7.2.3 的要求进行测试，记录测试结果。

8.2.4 每秒新建连接数

按 7.2.4 的要求进行测试，统计一分钟时间内建立的 IPSec 隧道数，然后计算得到每秒新建连接数，并记录结果。

8.3 安全管理检测

8.3.1 密钥管理

在被测产品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 7.3.1.1 的要求。

8.3.2 数据管理

8.3.2.1 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 7.3.2.1 的要求。

8.3.2.2 日志管理

查看并导出日志记录，结果应符合 7.3.2.2 的要求。

8.3.3 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。

8.3.4 产品管理

8.3.4.1 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 7.3.4.1 的要求。

8.3.4.2 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 7.3.4.2 的要求。

8.3.4.3 产品初始化

对被测产品进行初始化操作，结果应符合 7.3.4.3 的要求。

8.3.4.4 注册和监控

当系统有管理中心时，进行产品的注册、状态监控管理操作。结果应符合 7.3.4.4 的要求。

8.3.4.5 产品自检

对设备进行自检操作，结果应符合 7.3.4.5 的要求。

9 判定规则

8.1 以及 8.3 中除 8.3.2.1 和 8.3.4.4 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
（资料性）
IPSec VPN 简要介绍

A.1 综述

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 RFC 4301。

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 通过使用鉴别头（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 协议提供数据机密性、数据源鉴别、数据完整性以及抗重放服务。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使用 AH 和 ESP 保护，并使用 SM4 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只用 ESP 保护，并使用 SM4 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.2 安全联盟及安全联盟数据库

A.2.1 安全联盟概述

安全联盟（SA）是 IPSec VPN 的基础。AH 和 ESP 都使用了安全联盟，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，定义了安全联盟策略管理、通信处理、安全联盟管理技术所需的特性。

A.2.2 定义和范围

一个安全联盟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间的双向通信，创建两个安全联盟，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 的情况下，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，则 SA 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 IP 头。

A.2.3 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，同时也提供鉴别服务。ESP 所提供的鉴别范围比 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.2.4 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，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.3 安全联盟数据库

A.3.1 安全联盟数据库概述

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，本文件并不做细节上的规定。但是本文件规定了一套安全策略数据库元素集标准，以保证实现的可操作性和最低限度的管理能力，确保使用本文件的 IPSec VPN 设备之间可以互通。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，遵从本文件的 IPSec VPN 实现并不要求在细节上和这个模式相一致，但是需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。A.3 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.3.2 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。本文件不规定安全策略数据库以及其接口的实现方式。但是，任何服从本文件的实现需提供本条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，其所有的数据包处理过程中都查阅 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，提供一个名义上独立的 SPD，它区分受 IPSec 保护的数据包和允能绕过 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能数据包离开主机、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 指出对数据流提供的安全服务、采用的协议、使用的算法。

对于 IPSec 实现，需要有一个管理接口，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基于选择符（选择符定义见 A.3.3）的处理入口，并且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。如果要进行 IPSec 处理，则入口包括一个 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，以及是否要嵌套使用 SA。策略入口还规定如何从 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，可以有两种选择：

a) 使用报文自身拥有的值；

b) 使用和策略入口相关的值。

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 中的策略入口规定如何使用这些 SA 的顺序。

A.3.3 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 管理支持下面的选择符参数。

a) 目的 IP 地址（IPv4 或 IPv6）：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。

b) 源 IP 地址（IPv4 或 IPv6）：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。

c) 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。

d) 传输层协议：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。

e) 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能得不到源端口和目的端口，因此，支持一个“不透明的”的值。

A.3.4 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。

a) 外部头中的目的 IP 地址：IPv4 或 IPv6 目的地址。

b) IPSec 协议：AH 或 ESP，用作一个在这个数据库中查找 SA 的索引。

c) 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 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。

a) 序列号计数器：长度为 4 字节（如果采用了扩展序列号机制，则为 8 字节无符号整数），用于产生 AH 或 ESP 头中的序列号。

b) 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产生一个日志记录，并且阻止用该 SA 继续传输报文。

c) 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。

d) AH 鉴别算法和密钥。

e) ESP 加密算法、密钥、IV 模式和 IV。

f) ESP 鉴别算法和密钥，如果不选择鉴别服务，该字段为空。

g) 安全联盟生存期：可使用秒或千字节作为单位。

h) IPSec 协议模式：隧道模式或者传输模式。

参 考 文 献

[1] RFC 4301 Security architecture for the internet protocol

[2] RFC 4302 IP authentication header

[3] RFC 4303 IP encapsulating security payload(ESP)

[4] RFC 4308 Cryptographic suites for IPSec

[5] RFC 4106 The use of galois/counter mode (GCM) in IPsec encapsulating security payload (ESP)