GM/T 0022-2014
IPSec VPN技术规范

宣讲人 罗俊

2014年7月24日

目录

- 标准的适用范围和作用
- 标准的编制思路和技术路线
- 标准的主要内容解读
- 标准应用时的注意事项
- 应用举例

目录

标准的适用范围和作用

- 适用范围
  - 对IPSec VPN的技术协议、产品管理和检测进行了规定
  - 用于指导IPSec VPN产品的研制、检测、使用和管理
- 作用
  - 统一IPSec VPN产品的协议规范和技术要求
  - 规范商用密码算法在IPSec VPN产品的使用
  - 为不同厂家IPSec VPN产品的互联互通提供标准

目录

标准的编制思路和技术路线

- 编制思路
  - 通用性：统一技术要求，实现基本技术规格一致
  - 灵活性：对管理方式、硬件配置等不做细节规定
  - 安全性：硬件、软件、管理安全性都有严格规定
- 技术路线
  - 支持我国自主研制的商用密码算法
  - 参照多个与IPSEC VPN相关的RFC文档，用一个文档实现IPSEC VPN技术协议的全面覆盖
  - 采用数字信封和双证书体制，取消预共享密钥模式和野蛮交换模式
  - 在标准ISAKMP载荷语法和属性编码基础上进行扩展

标准的编制思路和技术路线

- RFC2408 (ISAKMP)
  Internet Security Association and Key Management Protocol
- RFC2409
  The Internet Key Exchange (IKEv1)
- RFC3947
  Negotiation of NAT-Traversal in the IKE
- RFC3948
  UDP Encapsulation of IPsec ESP Packets
- RFC4301
  Security Architecture for the Internet Protocol
- RFC4302
  IP Authentication Header
- RFC4303
  IP Encapsulating Security Payload (ESP)
- RFC4308
  Cryptographic Suites for IPsec

标准的编制思路和技术路线

- 2007年启动本标准编制，2012年进行修订
- 由联合课题组承担编制工作
- 经多方、多轮征意、修改及评审
- 于2014年正式发布，标准号GM/T0022-2014

目录

标准的主要内容解读

- 本规范共分为8个章节
  - 1、范围
  - 2、规范性引用文件
  - 3、术语、定义与缩略语
  - 4、密码算法与密钥种类
  - 5、协议
  - 6、IPSec VPN产品要求
  - 7、IPSec VPN产品检测
  - 8、合格判定

标准的主要内容解读 密码算法

- 非对称算法：
  - SM2椭圆曲线密码算法
  - 2048位及以上的RSA算法
- 对称密码算法
  - SM1分组密码算法
  - SM4分组密码算法
  - CBC(分组链接)模式
- 密码杂凑算法使用SM3或SHA-1算法
- 随机数检测标准：GM/T 0005随机性检测规范

标准的主要内容解读密钥种类

- **密钥种类**
  - **设备密钥**

    签名密钥对和加密密钥对，用于实体验证、数字签名(签名密钥对)和数字信封(加密密钥对)等。
  - **工作密钥**

    在密钥交换第一阶段得到的密钥，用于第二阶段会话密钥交换过程的保护。
  - **会话密钥**

    在密钥交换第二阶段得到的密钥，用于安全协议中数据报文的加密和完整性校验。

设备密钥保存在非易失性存储介质，需安全可靠的保护手段。
工作密钥和会话密钥保存在易失性存储介质，掉电即丢失。

标准的主要内容解读 密钥交换协议

阶段	模式	目的	结果
一阶段	主模式	双方身份鉴别、协商保护二阶段密钥交换的安全策略和密钥	ISAKMP SA（密码套件、共享策略、工作密钥）
二阶段	快速模式	协商保护数据通信的安全策略和密钥	IPSec SA（密码套件、共享策略、会话密钥）

标准的主要内容解读 密钥交换协议

第一阶段-主模式

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

加密证书
签名证书
} 双证书

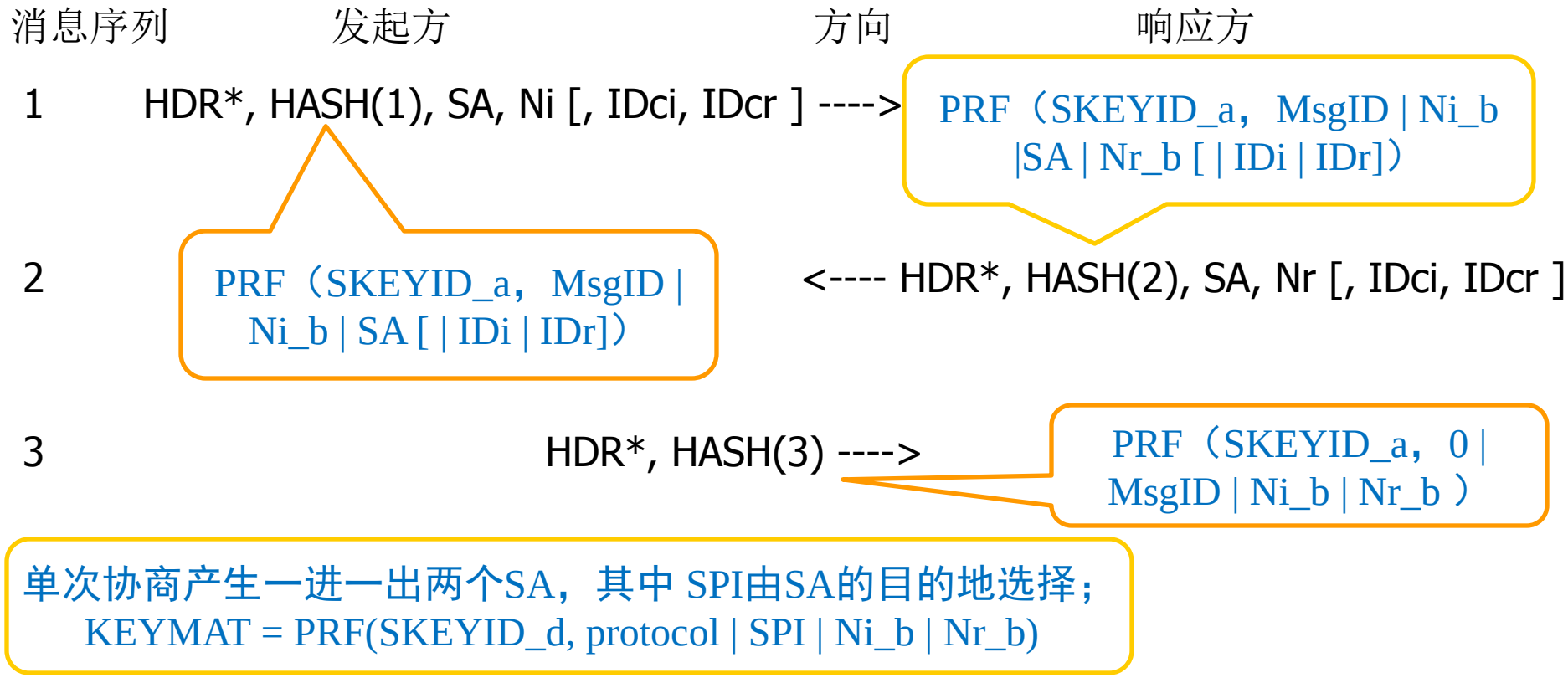
标准的主要内容解读 密钥交换协议

- 第一阶段-主模式

密钥参数	用途	生成方法
SKEYID	基本密钥参数	PRF(Hash(Ni_b | Nr_b), CKY-I | CKY-R)
SKEYID_d	用来产生会话密钥	PRF(SKEYID, CKY-I | CKY-R | 0)
SKEYID_a	验证ISAKMP消息完整性以及数据源身份	PRF(SKEYID, SKEYID_d | CKY-I | CKY-R | 1)
SKEYID_e	保护ISAKMP消息机密性	PRF(SKEYID, SKEYID_a | CKY-I | CKY-R | 2)

标准的主要内容解读 密钥交换协议

- 第二阶段-快速模式



标准的主要内容解读 密钥交换协议

- ISAKMP信息交换

如果ISAKMP安全联盟已经建立：

发起方 方向 响应方

HDR*, HASH(1), N/D ---->

PRF(SKEYID_a, MsgID | N/D)

如果ISAKMP安全关联在信息交换时还没有建立：

发起方 方向 响应方

HDR, N ---->

标准的主要内容解读 密钥交换协议

NAT穿越

消息序列	发起方	方向	响应方
1	HDR, SA, VID	---->	
2	$NAT\_D_{ir} \neq NAT\_D_{rl}$: 响应端存在NAT ; $NAT\_D_{il} \neq NAT\_D_{rr}$:发起端存在NAT	<----	HDR, SA, VID
3	HDR,XCHi,SIGi, NAT_D_{ir} , NAT_D_{il}	---->	
4	HASH(CKY-I | CKY-R | IP | Port)	<----	HDR, XCHr, SIGr, NAT_D_{rr} , NAT_D_{rl}
5	HDR*#，HASHi	---->	
6		<----	HDR*#，HASHr

如果NAT存在，包5、6及之后的协商包将被发送到修改后的端口

标准的主要内容解读 密钥交换协议

- 消息及载荷格式-ISAKMP头

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			

标准的主要内容解读 密钥交换协议

- 消息及载荷格式-通用载荷头

下一个载荷	保留	载荷长度

标准的主要内容解读 密钥交换协议

消息及载荷格式-载荷类型

载荷类型	用途	值
无（None）	表示无后续载荷	0
安全联盟载荷	协商SA	1
建议载荷	协商安全协议	2
变换载荷	协商安全机制	3
密钥交换载荷	协商密钥参数	4
标识载荷	交换身份信息	5

标准的主要内容解读 密钥交换协议

消息及载荷格式-载荷类型

载荷类型	用途	值
证书载荷	交换数字证书	6
证书请求载荷	发出证书请求	7
杂凑载荷	消息校验	8
签名载荷	签名鉴别	9
Nonce载荷	交换随机数	10
通知载荷	传送通知数据	11

标准的主要内容解读 密钥交换协议

消息及载荷格式-载荷类型

载荷类型	用途	值
删除载荷	取消SA	12
厂商载荷	传递自定义常量	13
属性载荷	交换SA属性	14
NAT-D载荷	NAT检测	20
NAT-OA载荷	传递原始地址	21
对称密钥载荷	传递对称密钥（数字信封）	128

标准的主要内容解读 密钥交换协议

消息及载荷格式-主模式消息一

标准的主要内容解读 密钥交换协议

消息及载荷格式-主模式消息二

		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	保留:0	载荷长度	
		DOI：1			
		情形：1			
SA载荷	建议载荷	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
	变换载荷	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			
	签名证书载荷	NP 证书：6	保留：0	载荷长度	
		证书编码：4	证书数据4		
		签名证书数据			
	加密证书载荷	NP NULL:0	保留：0	载荷长度	
		证书编码：5	证书数据5		
		加密证书数据			

标准的主要内容解读 密钥交换协议

消息及载荷格式-主模式消息三

	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			
对称密钥载荷	NP Nonce:10	保留:0	载荷长度	
	受公钥加密的对称密钥			
Nonce载荷	NP 标识:5	保留:0	载荷长度	
	受对称密钥加密的Nonce数据			
标识载荷	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			
证书载荷（签名）	NP 证书：6	保留：0	载荷长度	
	证书编码：4	证书数据4		
	签名证书数据			
证书载荷（加密）	NP 签名:9	保留：0	载荷长度	
	证书编码：5	证书数据5		
	加密证书数据			
签名载荷	NP NULL:0	保留：0	载荷长度	
	签名数据			

标准的主要内容解读 密钥交换协议

消息及载荷格式-主模式消息四

	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			
对称密钥载荷	NP Nonce:10	保留:0	载荷长度	
	受公钥加密的对称密钥			
Nonce载荷	NP 标识：5	保留:0	载荷长度	
	受对称密钥加密的Nonce数据			
标识载荷	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			
签名载荷	NP NULL:0	保留：0	载荷长度	
	签名数据			

标准的主要内容解读 密钥交换协议

消息及载荷格式-主模式消息五

	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：0			
	长度			
杂凑载荷	NP NULL:0	保留：0	载荷长度	
	杂凑载荷			

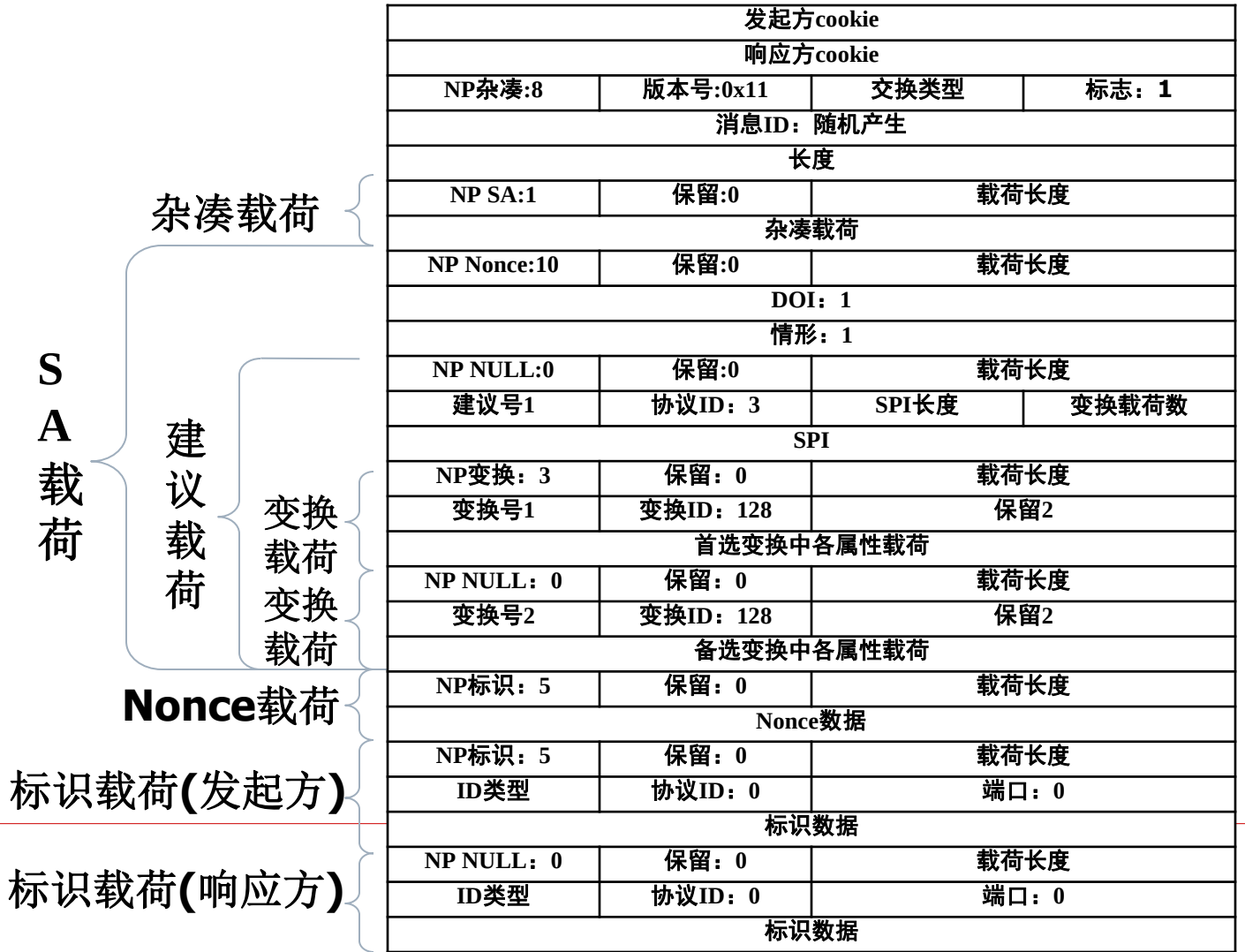
标准的主要内容解读 密钥交换协议

消息及载荷格式-主模式消息六

	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：0			
	长度			
杂凑载荷	NP NULL:0	保留：0	载荷长度	
	杂凑载荷			

标准的主要内容解读 密钥交换协议

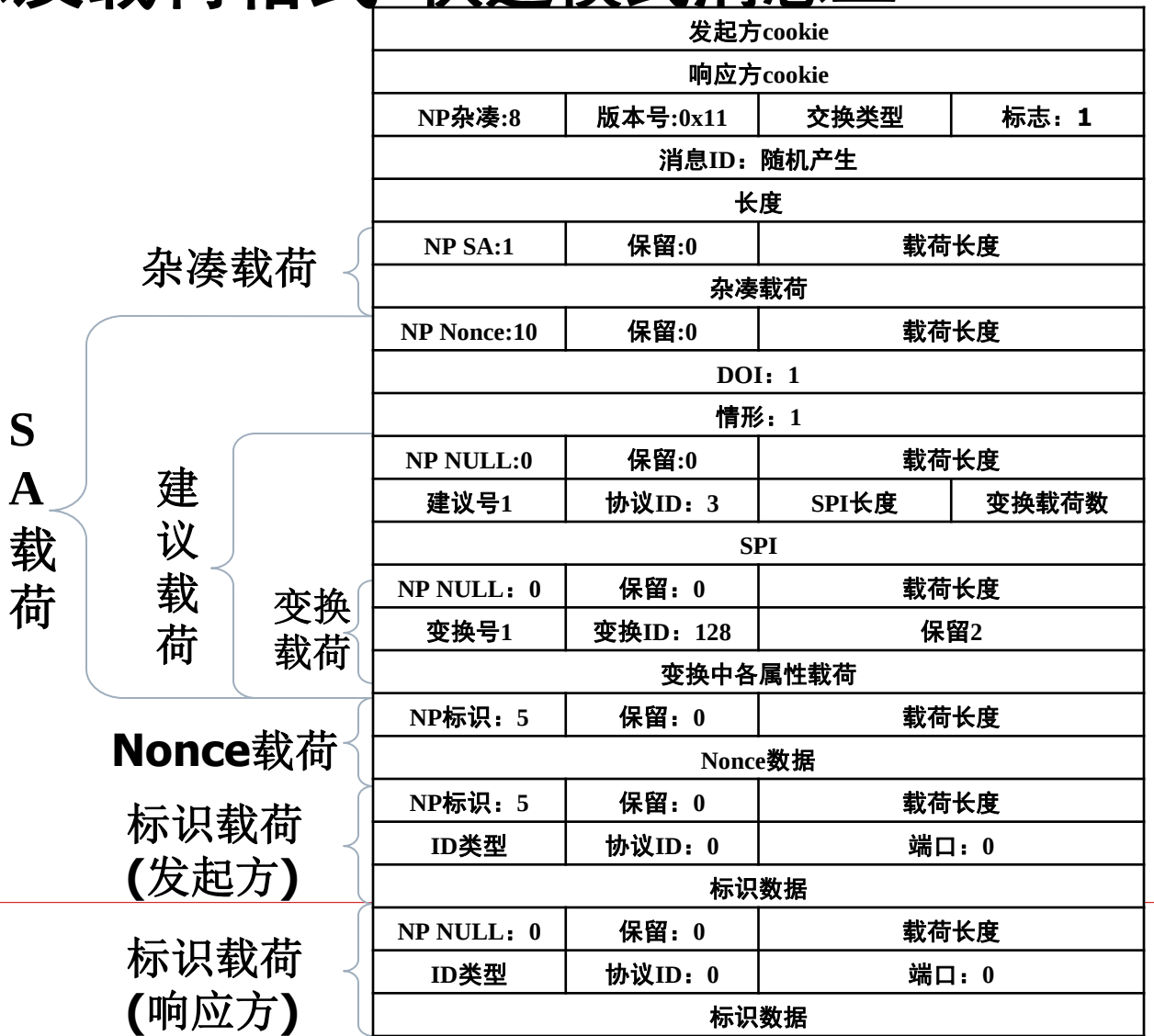
消息及载荷格式-快速模式消息一



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	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	保留2	
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	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			

标准的主要内容解读 密钥交换协议

消息及载荷格式-快速模式消息二



标准的主要内容解读 密钥交换协议

消息及载荷格式-快速模式消息三

	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			
杂凑载荷	NP NULL:0	保留：0	载荷长度	
	杂凑载荷			

标准的主要内容解读 密钥交换协议

ISAKMP扩展项变化

变化项	所处阶段	变化内容	类型值
ISAKMP载荷	1、2阶段	定义属性载荷	14
ISAKMP载荷	1阶段	对称密钥载荷	128
鉴别方式	1阶段	公钥数字信封	10
公钥算法	1阶段	RSA2048、SM2	1、2
密码杂凑算法	1、2阶段	SHA1、SM3	2、20
AH算法	2阶段	SHA1、SM3	3、20
ESP算法	2阶段	SM1、SM4	128、127
证书类型	1阶段	X.509签名证书 、X.509加密证书	4、5

标准的主要内容解读 安全报文协议

鉴别头协议AH(隧道模式)

AH不能单独使用，而应和封装安全载荷协议**ESP**嵌套使用。鉴别数据（完整性校验值**ICV**）具体长度取决于所使用的完整性校验算法。

IPv4封装前

原IP头 (所有选项)	协议头 （ESP）	数据

IPv4封装后

新建外部IP头(所有选项)	AH	协议头 （ESP）	原IP头 (所有选项)	数据

新IP报文中的认证范围

IPv6封装前

原IP头	扩展头	协议头 （ESP）	数据

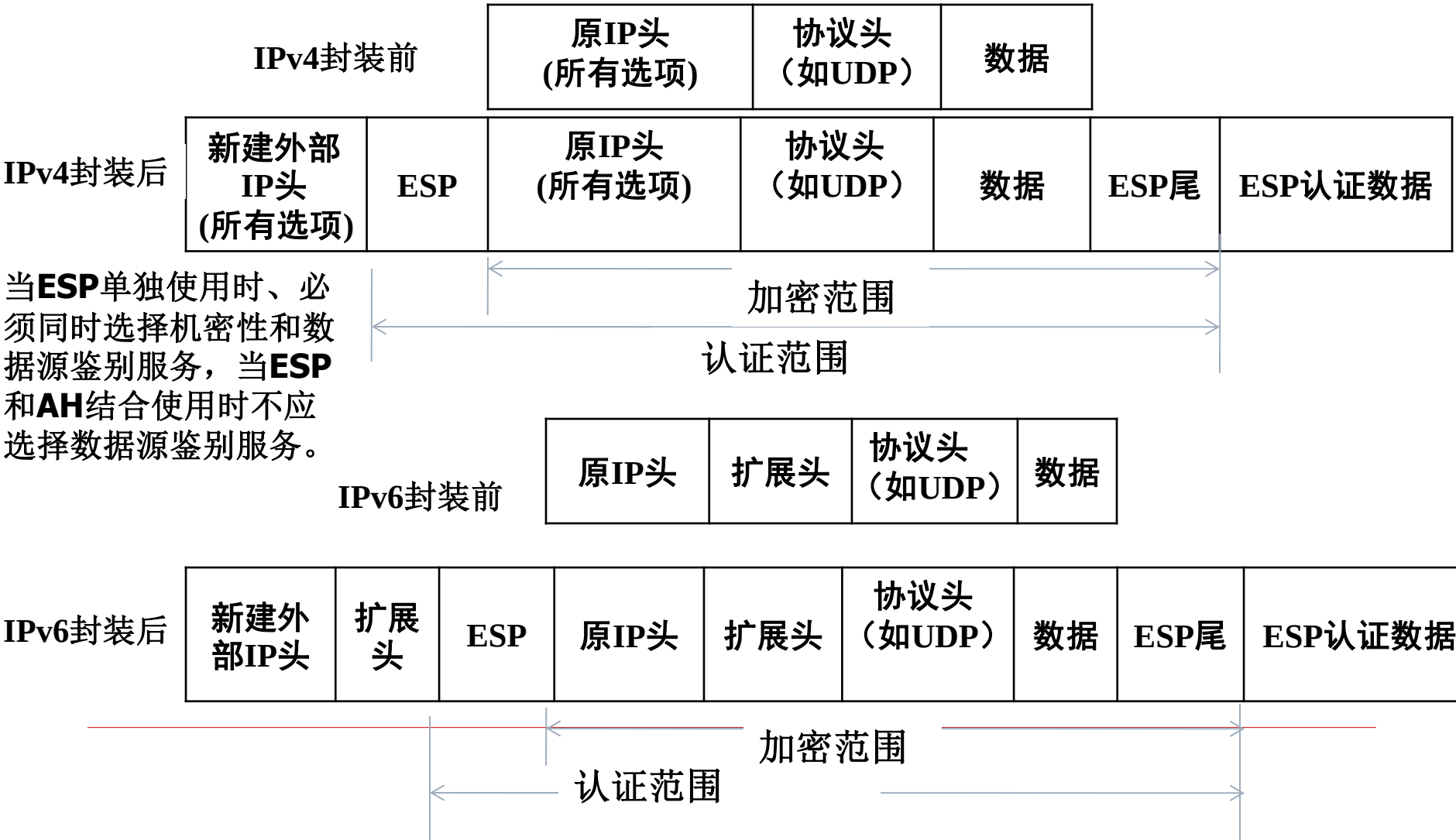
IPv6封装后

新建外部IP头	扩展头	AH	原IP头	扩展头	协议头 （ESP）	数据

新IP报文中的认证范围

标准的主要内容解读 安全报文协议

- 封装安全载荷ESP(隧道模式)



目录

- 标准的适用范围和作用
- 标准的编制思路和技术路线
- 标准的主要内容解读
- 标准应用时的注意事项
- 应用举例

标准应用时的注意事项（一）

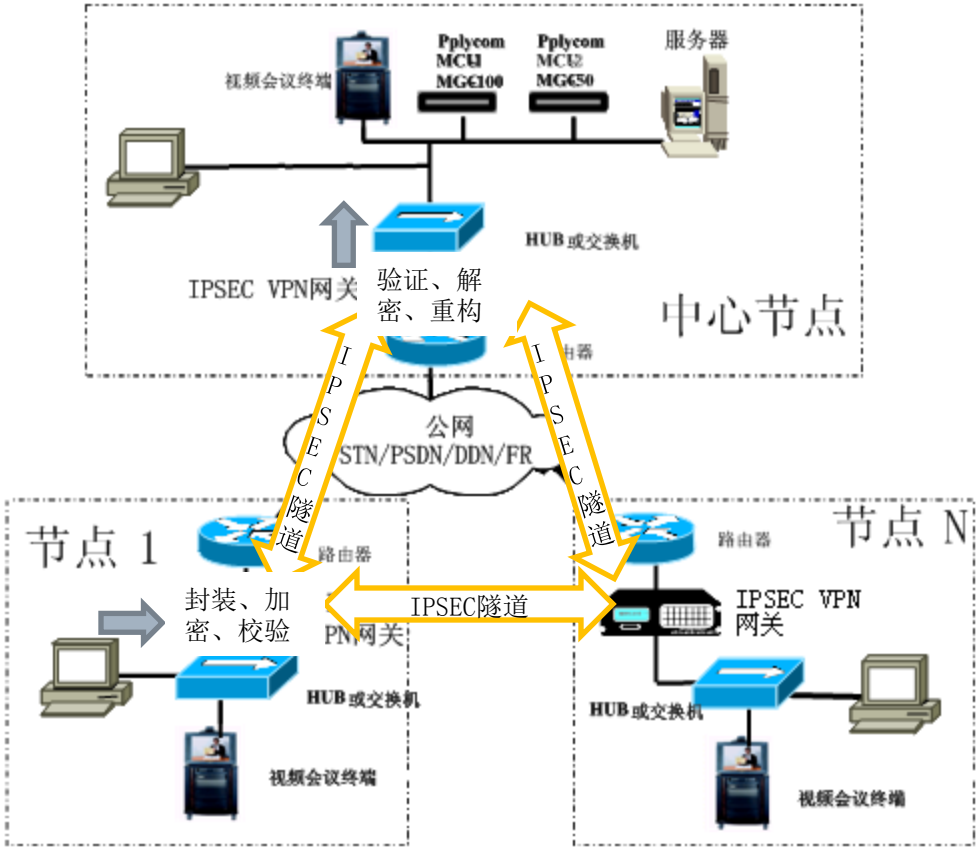
- 随机数生成算法生成的随机数应能通过《GM/T 0005随机性检测规范》规定的检测
- 当使用SM2算法进行加密和数字签名时，具体使用方法见《GM/T 0009 SM2密码算法使用规范》；当使用RSA算法进行加密和数字签名时，见PKCS#1
- 加密密钥对要通过CA从密钥管理中心申请，私钥保护方法见《GM/T 0014 数字证书认证系统密码协议规范》
- SM2证书的结构及定义见《GM/T 0015基于SM2密码算法的数字证书格式规范》
- 数字信封详细语法结构参见PKCS7（RSA证书）和《GM/T 0015基于SM2密码算法的数字证书格式规范》（SM2证书）

标准应用时的注意事项（二）

- 本规范不与IKEv1及v2兼容
- 对称加密算法可采用SM1或SM4分组密码算法
- 非对称加密算法可采用SM2或RSA2048
- 密码杂凑算法可采用SM3或SHA1
- 交换消息中的加密操作一般是对整个载荷进行；签名操作一般是对载荷的数据进行（不包含ISAKMP通用头）
- 实现 NAT穿越的处理过程和消息格式参照RFC3947的规定执行

目录

应用举例


视频会议终端
Pplycom MCU MGC100
Pplycom MCU MGC50
服务器
HUB或交换机
IPSEC VPN网关
验证、解密、重构
中心节点
公网
STN/PSDN/DDN/FR
IPSEC隧道
IPSEC隧道
节点 1
路由器
封装、加密、校验
PN网关
HUB或交换机
视频会议终端
IPSEC隧道
路由器
节点 N
IPSEC VPN网关
HUB或交换机
视频会议终端

感谢参与！