

网络安全协议及分析

IP层安全IPSec

密码与网络安全系 刘虹

2025年春季学期

课程体系

第一章 概述

第二章 链路层扩展L2TP

第三章 IP层安全IPSec

第四章 传输层安全SSL和TLS

第五章 会话安全SSH

第六章 代理安全Socks

第七章 网管安全SNMPv3

第八章 认证协议Kerberos

第九章 应用安全

本章学习目标

- ▲ IKE协议流程
- ▲ 认证首部AH
- ▲ 封装安全载荷ESP

提纲

一、 IKE协议流程

二、 认证首部AH

三、 封装安全载荷ESP

四、 IPSec应用

IPSec协议

▲ 交换协议：

- 互联网安全关联与密钥管理协议 (Internet Security Association and Key Management Protocol, ISAKMP)
- 互联网密钥交换 (Internet Key Exchange, IKE)

▲ 数据封装协议：

- 数据封装处理协议的认证首部 (Authentication Header, AH)
- 封装安全载荷 (Encapsulating Security Payload, ESP)

IKE协议

- ▲ 互联网密钥交换 (Internet Key Exchange, IKE)：
 - SA协商、密钥生成、身份认证
- ▲ 主要功能：
 - 协商通信双方安全特性、参数
 - 进行通信双方身份认证
 - 用安全的方法产生、交换密钥
 - 管理、更新、删除安全关联SA

IKE协议：SA协商

IKE协商的核心内容是SA协商，涉及的SA属性包括：

- 加密算法
- 散列算法
- 认证方法
- D-H群信息
- 伪随机函数
- 群描述
- 群类型
- 生命期类型、生命期
- 密钥长度



IKE协议：SA协商

- Diffie-Hellman (D-H) 群相关属性
 - D-H群决定在进行一次D-H交换时通信双方需要使用的参数是什么。
- 定义四种具体的群
 - 768比特模数的MODP (模指数群)
 - 1024比特模数的MODP群
 - 域尺寸为155比特的EC2N群 (在有限域 $GF[2^N]$ 上的椭圆曲线群)
 - 域尺寸为185位的EC2N群 (在有限域 $GF[P]$ 上的椭圆曲线群)

IKE协议：SA协商

▶ Diffie–Hellman (D-H) 密钥协商：

- 通信双方共享模数p (大质数) , 发生器g

对于任意 $z < p$, 存在 w , 使得 $g^w \bmod p = z$

假设 $x < p$, 计算: $y = g^x \bmod p$, 最终 x 被作为私钥, y 被作为公钥

设 x_a 和 y_a 是Alice的私钥和公钥, x_b 和 y_b 是Bob的私钥和公钥

$y_a = g^{x_a} \bmod p$, $y_b = g^{x_b} \bmod p$

Alice计算: $K_{ab} = (y_b)^{x_a} \bmod p = (g^{x_b})^{x_a} \bmod p = g^{x_b \cdot x_a} \bmod p$

Bob计算: $K_{ba} = (y_a)^{x_b} \bmod p = (g^{x_a})^{x_b} \bmod p = g^{x_a \cdot x_b} \bmod p$

IKE协议：SA协商

- 伪随机函数PRF
 - PRF以秘密信息和其他信息作为输入，并产生随机的比特流。
- IKE使用这种函数生成以下四种秘密信息来对数据进行验证和保护
 - **SKEYID**: 用于推导其他秘密信息；
 - **SKEYID_d**: 为IPSec衍生出加密的素材；
 - **SKEYID_a**: 用于数据完整性检验及进行数据源发认证；
 - **SKEYID_e**: 用于数据加密。

IKE协议：SA协商

1 认证方法

- 基于数字签名的方法 *Bob* 
- 基于公钥的方法   **PRF**
- 改进的基于公钥加密的方法    **PRF**
- 基于预共享密钥的方法 

IKE协议：交互模式

◀ 协商获取IKE SA

- 主模式
- 野蛮模式

◀ 协商安全协议SA

- 快速模式
- 新群模式
- 通知模式

IKE协议：交互模式

1 主模式

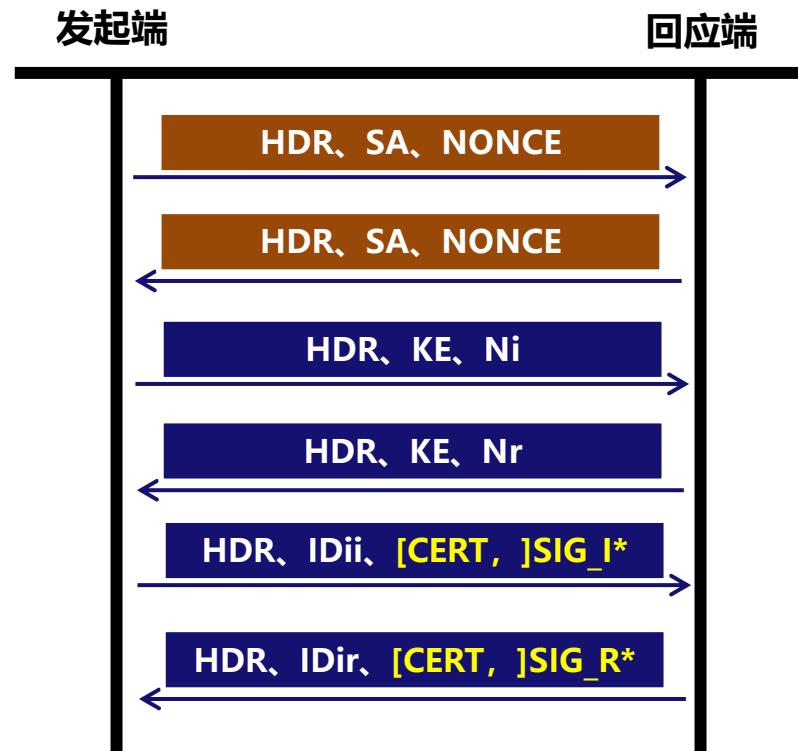
- 使用数字签名认证方法
- 使用公钥加密认证方法
- 使用改进的公钥加密认证方法
- 使用预共享密钥认证方法

IKE协议：交互模式-主模式

（1）使用数字签名认证方法

- Ni 和 Nr 表示NONCE；
- $SIG-I$ 和 $SIG-R$ 表示签名；
- []中的内容为可选字段；
- *标识的消息是经过安全处理的消息。

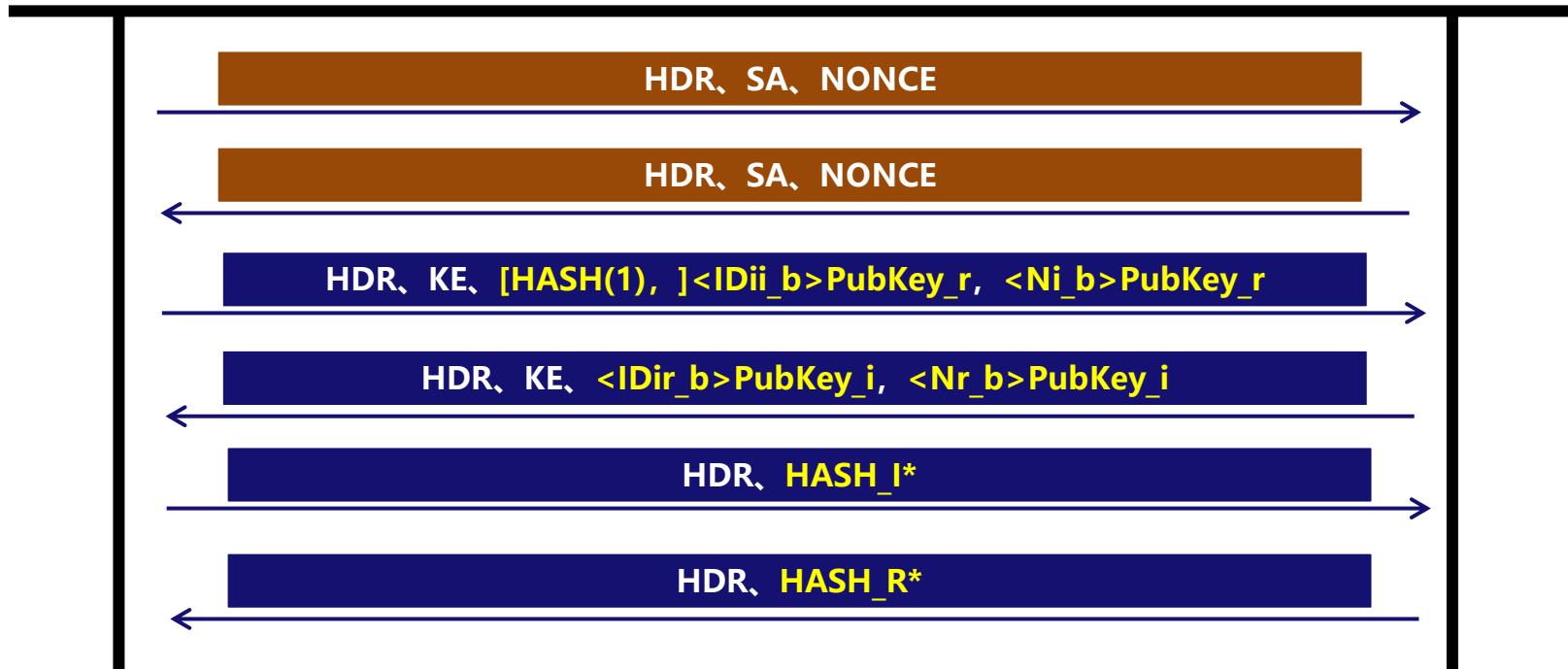
$SKEYID = \text{prf}(Ni_b | Nr_b, g^x y)$



IKE协议：交互模式-主模式

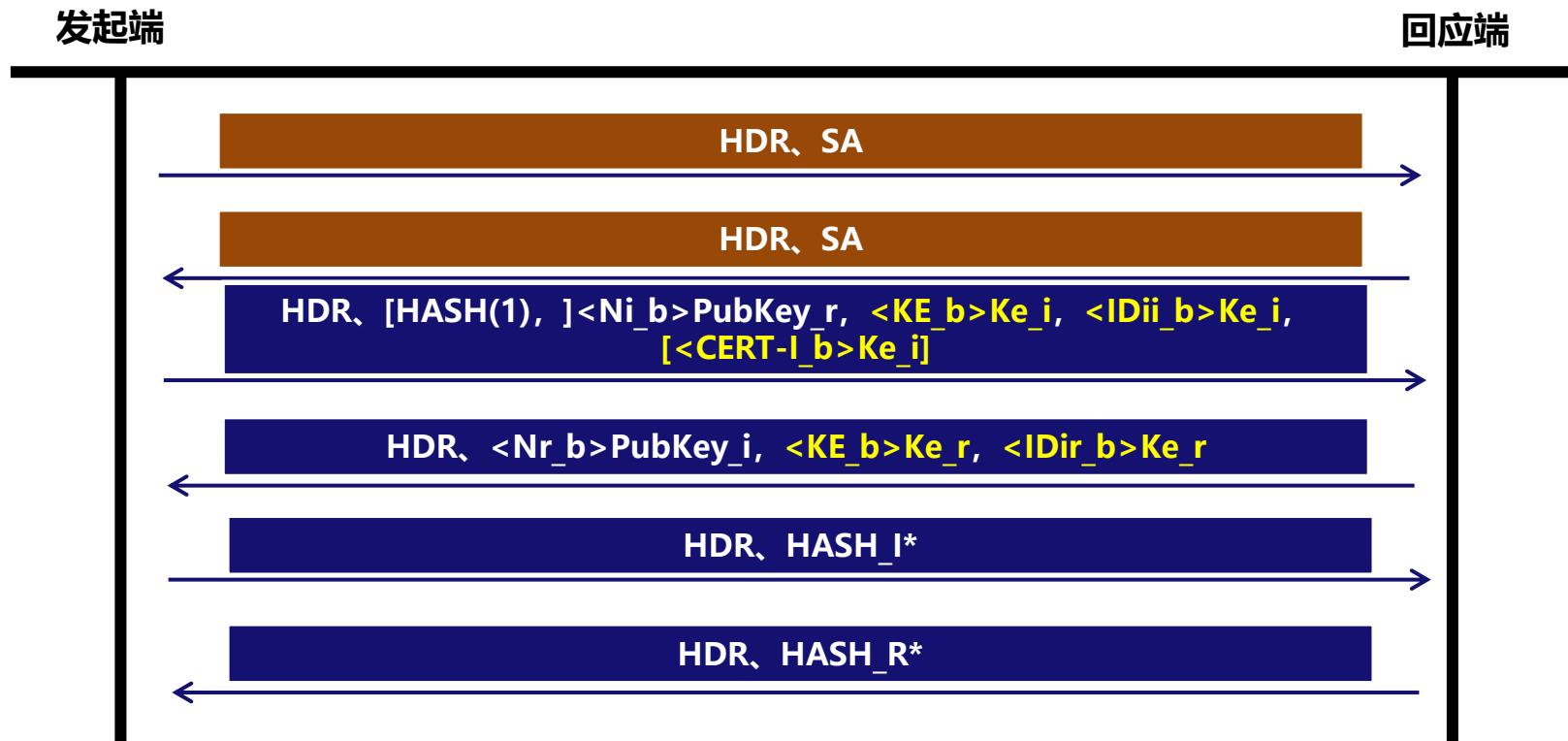
（2）使用公钥加密认证方法

发起端 $SKEYID = \text{prf}(\text{HASH}(N_i_b | N_r_b), \text{CKY-I} | \text{CKY-R})$ 回应端



IKE协议：交互模式-主模式

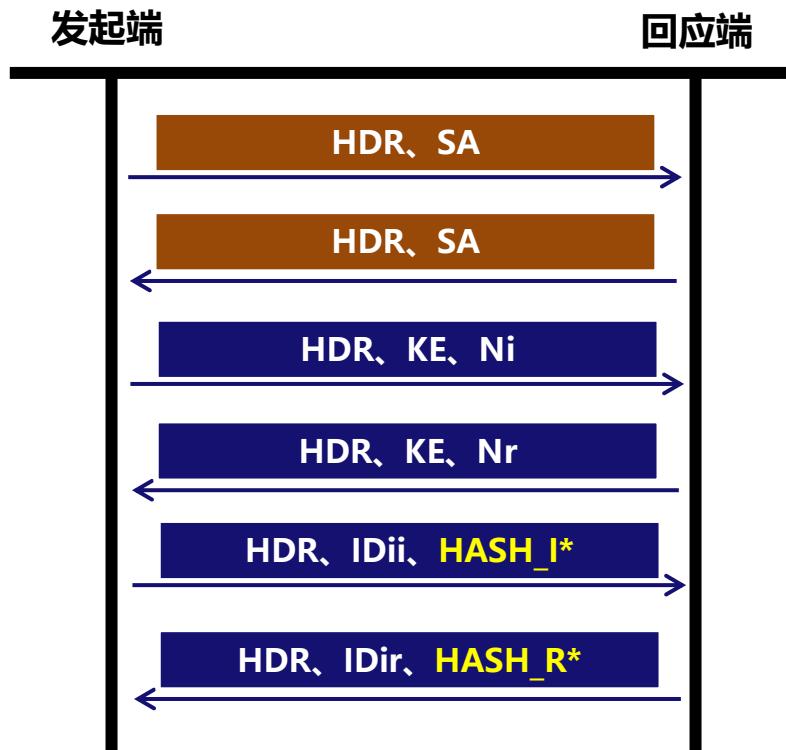
（3）使用改进的公钥加密认证方法



IKE协议：交互模式-主模式

（4）使用预共享密钥认证方法

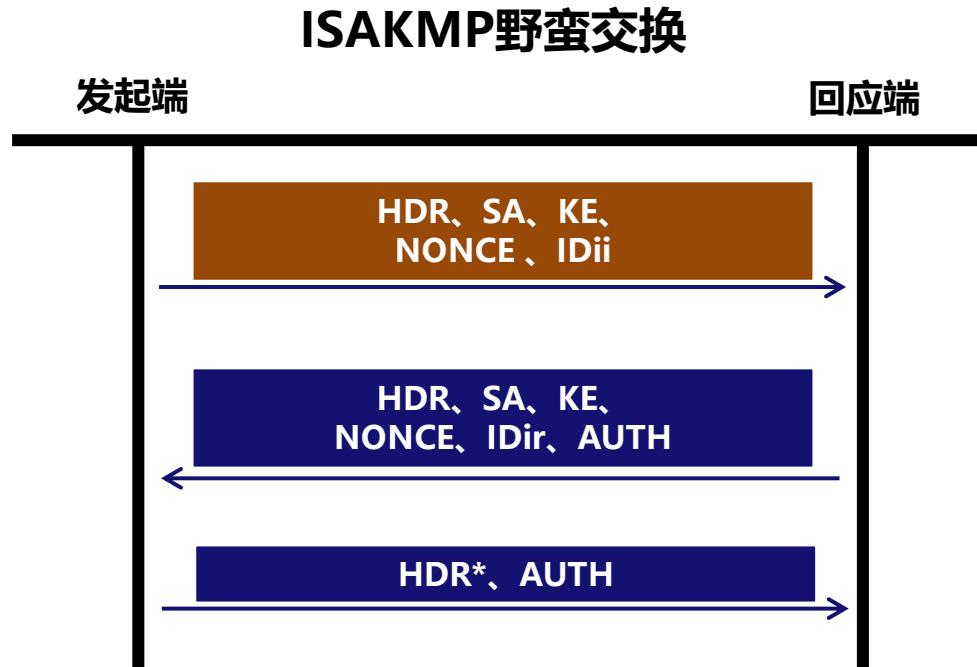
$SKEYID = \text{prf}(\text{预共享密钥}, Ni_b | Nr_b)$



IKE协议：交互模式

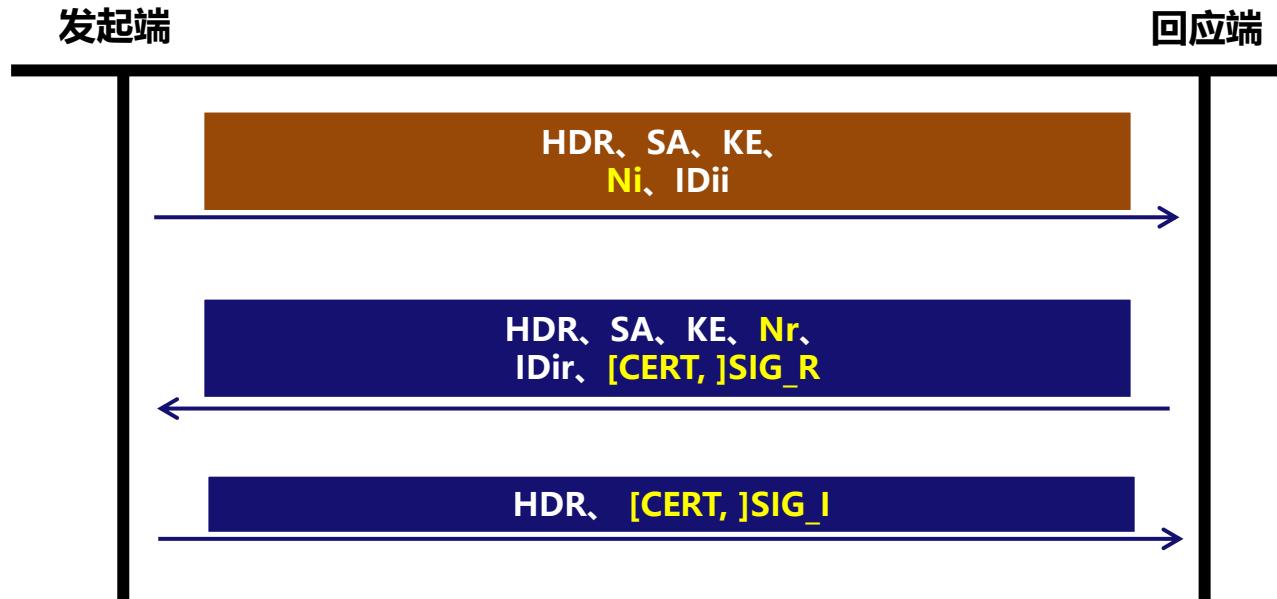
野蛮模式

- 使用数字签名
- 使用公钥加密
- 使用改进的公钥加密
- 使用预共享密钥



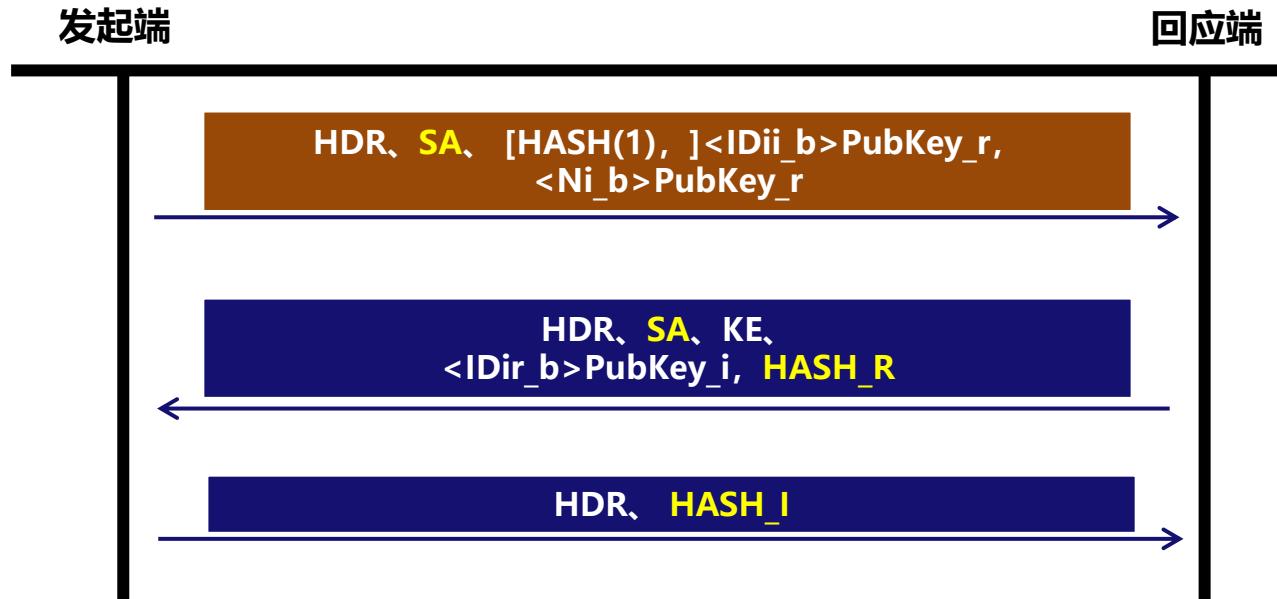
IKE协议：交互模式-野蛮模式

（1）使用数字签名



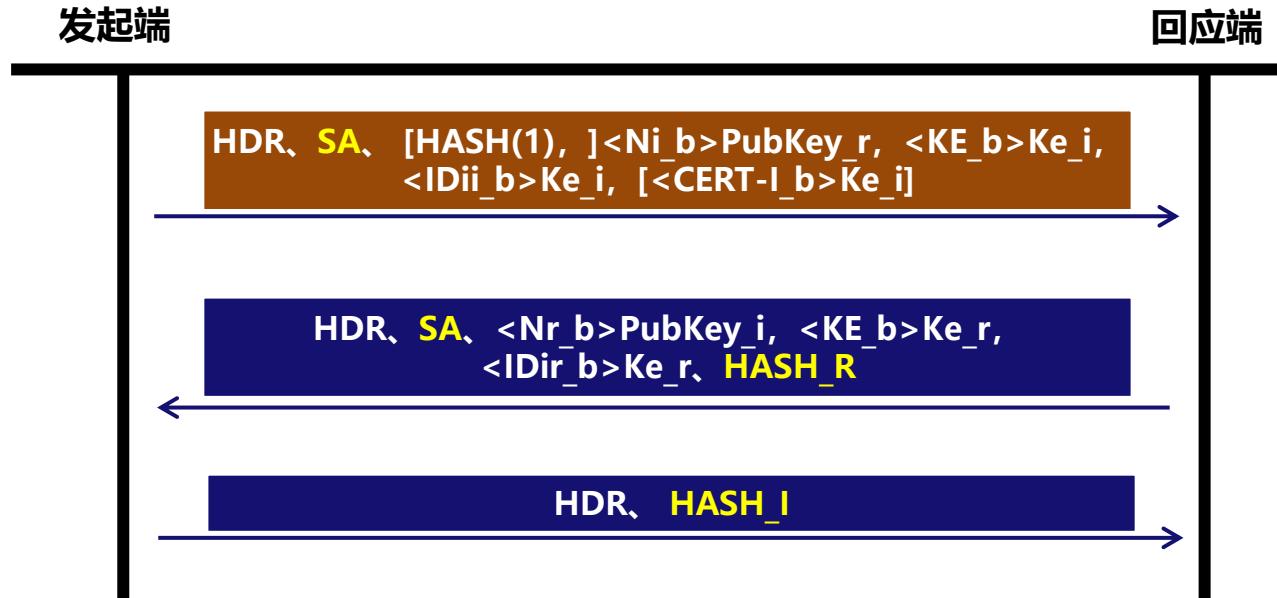
IKE协议：交互模式-野蛮模式

（2）使用公钥加密



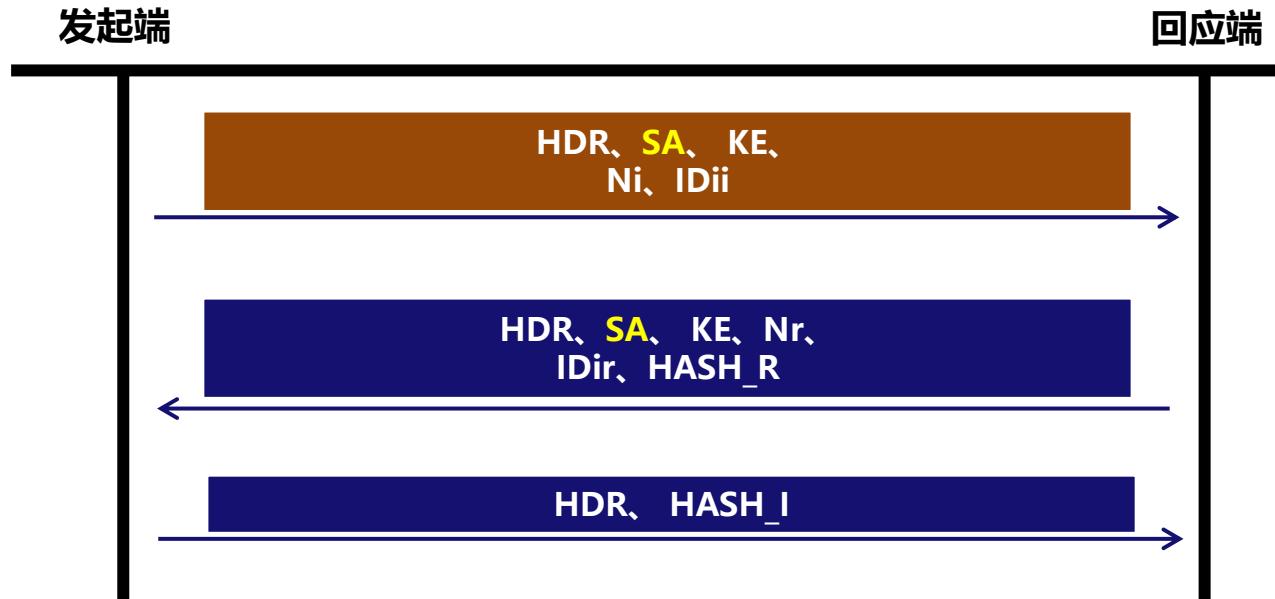
IKE协议：交互模式-野蛮模式

（3）使用改进的公钥加密



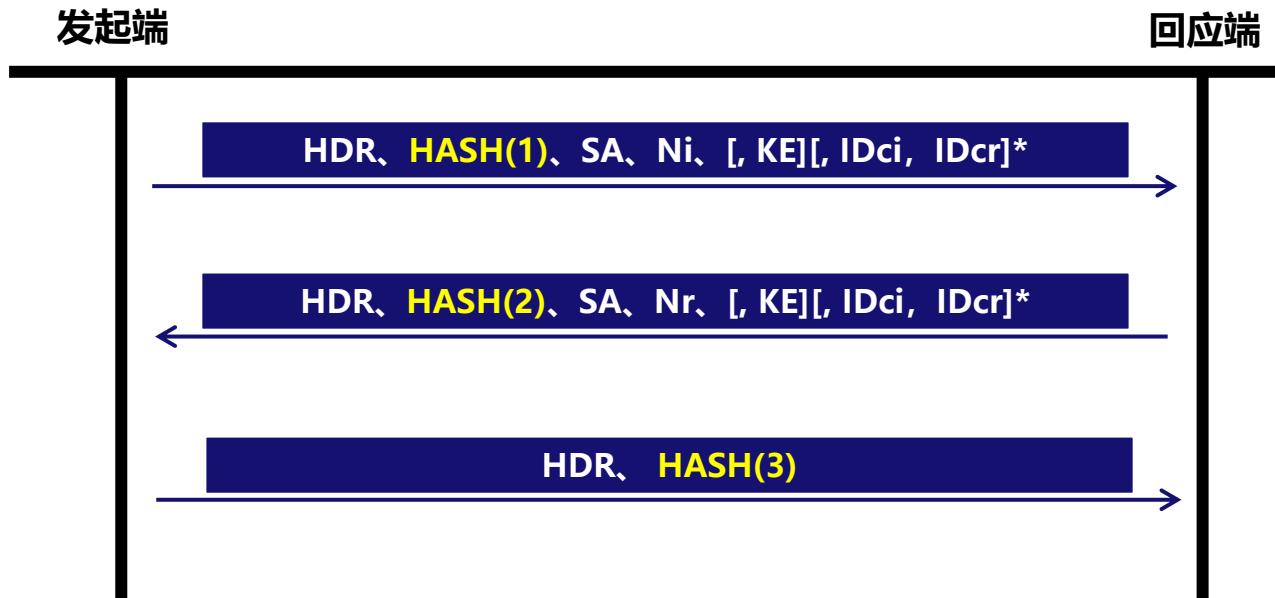
IKE协议：交互模式-野蛮模式

（4）使用预共享密钥



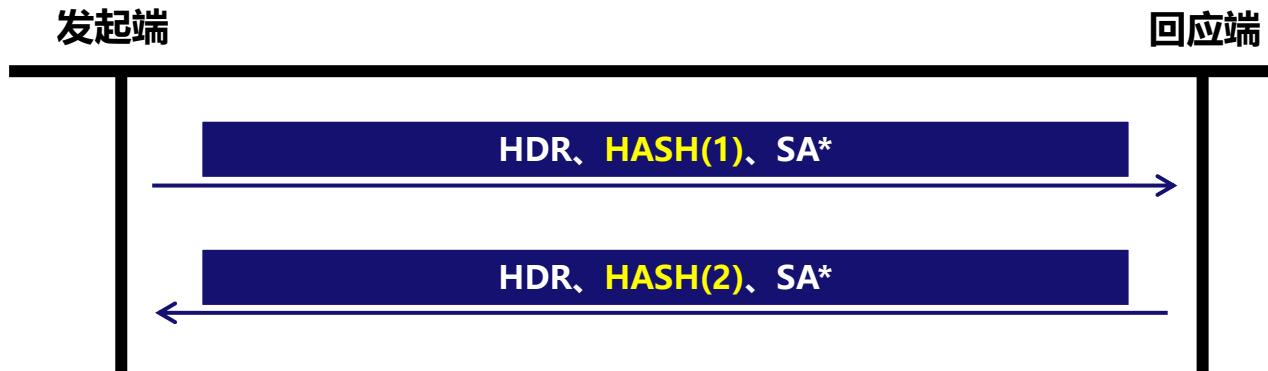
IKE协议：交互模式-快速模式

- IKE快速模式用于第二阶段协商，所有报文都使用第一阶段协商好的安全参数进行了处理。



IKE协议：交互模式-新群/通知模式

- 新群模式用于协商新的D-H群



- 通知交换用于错误通告、状态通告和SA删除

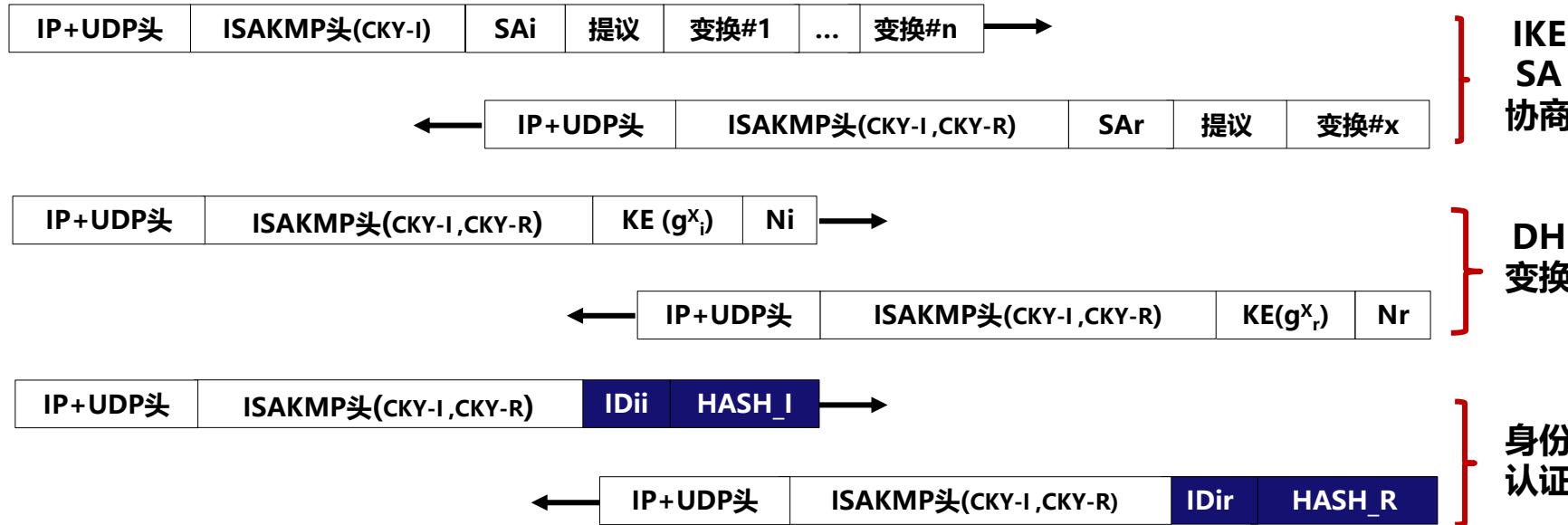


举例：预共享密钥主模式+快速模式

阶段1

发起端

回应端



举例：预共享密钥主模式+快速模式

```
Frame 43: 126 bytes on wire (1008 bits), 126 bytes captured (1008 bits)
Ethernet II, Src: Hangzhou_13:fa:45 (3c:e5:a6:13:fa:45), Dst: Hangzhou_13:f9:88 (3c:e5:a6:13:f9:88)
Internet Protocol, Src: 200.1.1.1 (200.1.1.1), Dst: 200.1.1.2 (200.1.1.2)
User Datagram Protocol, Src Port: isakmp (500), Dst Port: isakmp (500)
Internet Security Association and Key Management Protocol
  Initiator cookie: fdb34af23105bb78
  Responder cookie: 0000000000000000
  Next payload: Security Association (1)
  Version: 1.0
  Exchange type: Identity Protection (Main Mode) (2)
  Flags: 0x00
  Message ID: 0x00000000
  Length: 84
  Type Payload: Security Association (1)
    Next payload: NONE / No Next Payload (0)
    Payload length: 56
    Domain of interpretation: IPSEC (1)
  Situation: 00000001
  Type Payload: Proposal (2) # 1
    Next payload: NONE / No Next Payload (0)
    Payload length: 44
    Proposal number: 1
    Protocol ID: ISAKMP (1)
    SPI Size: 0
    Proposal transforms: 1
  Type Payload: Transform (3) # 0
    Next payload: NONE / No Next Payload (0)
    Payload length: 36
    Transform number: 0
    Transform ID: KEY_IKE (1)
    Transform IKE Attribute Type (t=1,l=2) Encryption-Algorithm : DES-CBC
    Transform IKE Attribute Type (t=2,l=2) Hash-Algorithm : SHA
    Transform IKE Attribute Type (t=3,l=2) Authentication-Method : PSK
    Transform IKE Attribute Type (t=4,l=2) Group-Description : Default 768-bit MODP group
    Transform IKE Attribute Type (t=11,l=2) Life-Type : Seconds
    Transform IKE Attribute Type (t=12,l=4) Life-Duration : 1
```

发起Cookie协商

下一个载荷

IKE第一阶段模式

最后一个载荷

DOI=1表示第二阶段用于IPSec

加密算法

验证算法

身份认证算法

选择DH组

SA更新方法和周期

举例：预共享密钥主模式+快速模式

```
Frame 44: 126 bytes on wire (1008 bits), 126 bytes captured (1008 bits)
Ethernet II, Src: Hangzhou_13:f9:88 (3c:e5:a6:13:f9:88), Dst: Hangzhou_13:fa:45 (3c:e5:a6:13:fa:45)
Internet Protocol, Src: 200.1.1.2 (200.1.1.2), Dst: 200.1.1.1 (200.1.1.1)
User Datagram Protocol, Src Port: isakmp (500), Dst Port: isakmp (500)
Internet Security Association and Key Management Protocol
    Initiator cookie: fdb34af23105bb78
    Responder cookie: 6e09f77d6992197c
    Next payload: Security Association (1)
    Version: 1.0
    Exchange type: Identity Protection (Main Mode) (2)
    Flags: 0x00
    Message ID: 0x00000000
    Length: 84
    Type Payload: Security Association (1)
        Next payload: NONE / No Next Payload (0)
        Payload length: 56
        Domain of interpretation: IPSEC (1)
        Situation: 00000001
    Type Payload: Proposal (2) # 1
        Next payload: NONE / No Next Payload (0)
        Payload length: 44
        Proposal number: 1
        Protocol ID: ISAKMP (1)
        SPI Size: 0
        Proposal transforms: 1
    Type Payload: Transform (3) # 0
        Next payload: NONE / No Next Payload (0)
        Payload length: 36
        Transform number: 0
        Transform ID: KEY_IKE (1)
        Transform IKE Attribute Type (t=1,l=2) Encryption-Algorithm : DES-CBC
        Transform IKE Attribute Type (t=2,l=2) Hash-Algorithm : SHA
        Transform IKE Attribute Type (t=3,l=2) Authentication-Method : PSK
        Transform IKE Attribute Type (t=4,l=2) Group-Description : Default 768-bit MODP group
        Transform IKE Attribute Type (t=11,l=2) Life-Type : Seconds
        Transform IKE Attribute Type (t=12,l=4) Life-Duration : 1
```

响应Cookie协商

协商一个自己支持的提议

举例：预共享密钥主模式+快速模式

```
+ Frame 45: 210 bytes on wire (1680 bits), 210 bytes captured (1680 bits)
+ Ethernet II, Src: Hangzhou_13:fa:45 (3c:e5:a6:13:fa:45), Dst: Hangzhou_13:f9:88 (3c:e5:a6:13:f9:88)
+ Internet Protocol, Src: 200.1.1.1 (200.1.1.1), Dst: 200.1.1.2 (200.1.1.2)
+ User Datagram Protocol, Src Port: isakmp (500), Dst Port: isakmp (500)
+ Internet Security Association and Key Management Protocol
    Initiator cookie: fdb34af23105bb78
    Responder cookie: 6e09f77d6992197c
    Next payload: Key Exchange (4)
    Version: 1.0
    Exchange type: Identity Protection (Main Mode) (2)
+ Flags: 0x00
    Message ID: 0x00000000
    Length: 168
+ Type Payload: Key Exchange (4) 密钥交换载荷
    Next payload: Nonce (10)
    Payload length: 100
    Key Exchange Data: 7fe68564021def232dcf963c2839a1b10933280406bd289e...
+ Type Payload: Nonce (10)
    Next payload: Vendor ID (13)
    Payload length: 20
    Nonce DATA: 9a1c087ff1ba99e023c37d9c14ad31b8 随机值Ni, 用于密钥生成
+ Type Payload: Vendor ID (13) : RFC 3706 DPD (Dead Peer Detection)
    Next payload: NONE / No Next Payload (0)
    Payload length: 20
    Vendor ID: afcad71368a1f1c96b8696fc77570100
    Vendor ID: RFC 3706 DPD (Dead Peer Detection)
```

交换是未经加密的

举例：预共享密钥主模式+快速模式

```
Frame 46: 210 bytes on wire (1680 bits), 210 bytes captured (1680 bits)
Ethernet II, Src: Hangzhou_13:f9:88 (3c:e5:a6:13:f9:88), Dst: Hangzhou_13:fa:45 (3c:e5:a6:13:fa:45)
Internet Protocol, Src: 200.1.1.2 (200.1.1.2), Dst: 200.1.1.1 (200.1.1.1)
User Datagram Protocol, Src Port: isakmp (500), Dst Port: isakmp (500)
Internet Security Association and Key Management Protocol
  Initiator cookie: fdb34af23105bb78
  Responder cookie: 6e09f77d6992197c
  Next payload: Key Exchange (4)
  Version: 1.0
  Exchange type: Identity Protection (Main Mode) (2)
  Flags: 0x00
  Message ID: 0x00000000
  Length: 168
  Type Payload: Key Exchange (4) -> 密钥交换载荷
    Next payload: Nonce (10)
    Payload length: 100
    Key Exchange Data: 683c0835605984e4123b0e6c791a3d74ad463116d97dd018...
  Type Payload: Nonce (10)
    Next payload: Vendor ID (13)
    Payload length: 20
    Nonce DATA: 4f8a4b39d01fdf1bb465d5156d40f0ba -> 随机值Nr, 用于密钥生成
  Type Payload: Vendor ID (13) : RFC 3706 DPD (Dead Peer Detection)
    Next payload: NONE / No Next Payload (0)
    Payload length: 20
    Vendor ID: afcad71368a1f1c96b8696fc77570100
    Vendor ID: RFC 3706 DPD (Dead Peer Detection)
```

举例：预共享密钥主模式+快速模式

阶段2

发起端

回应端



IKE与ISAKMP的区别

▲ IKE和ISAKMP

- IKE抛弃了ISAKMP的“交换”概念，引入“模式”描述不同的协商过程。
- IKE抛弃了ISAKMP的“基本交换”和“只有认证的交换”，继承了“身份保护交换”（即主模式）和“野蛮交换”（即野蛮模式）。
- IKE定义了“加密算法”和“散列算法”这两个属性，这为指明认证首部（AH）和封装安全载荷（ESP）所使用的MAC算法提供了便利。

提纲

一、IKE协议流程

二、认证首部AH

三、封装安全载荷ESP

四、IPSec应用

认证首部AH

安全服务

- 数据完整性
- 数据源发认证
- 抗重放攻击



提纲

一、IKE协议流程

二、认证首部AH

三、封装安全载荷ESP

四、IPSec应用

封装安全载荷ESP

安全服务

- 数据完整性
- 数据源发认证
- 抗重放攻击
- 机密性
- 有限的传输流机密性



隧道模式和传输模式

- 隧道模式可以适用于任何场景
- 传输模式只能适合PC到PC的场景

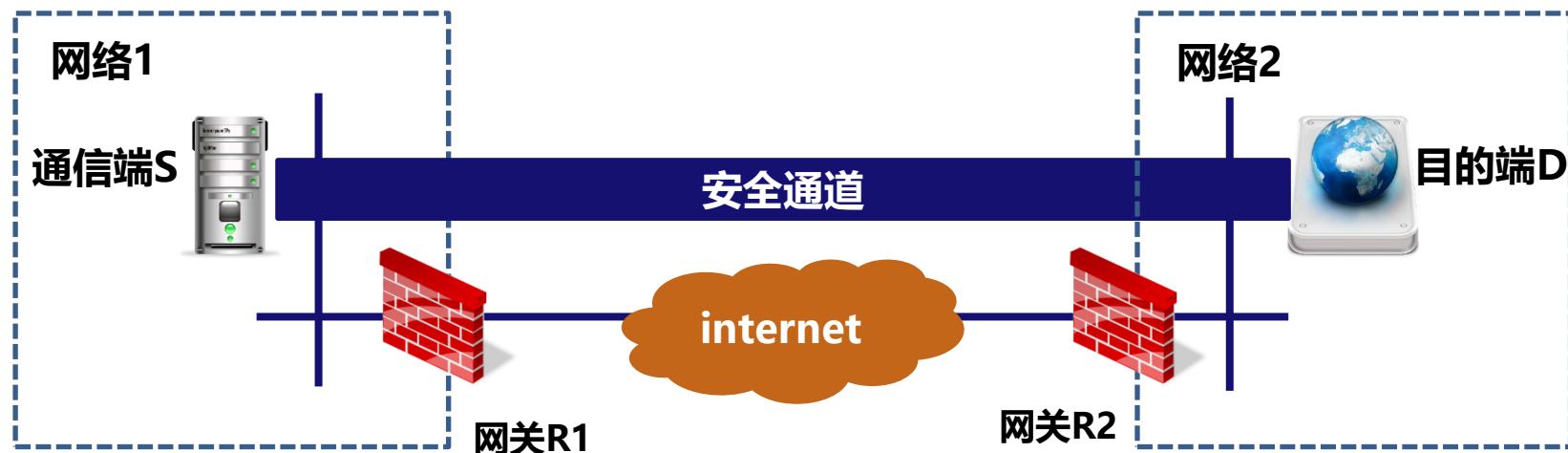


- End-to-End (端到端或者PC到PC) : 两个PC之间的通信由两个PC之间的IPSec会话保护，而不是网关。
- End-to-Site (端到站点或者PC到网关) : 两个PC之间的通信由网关和异地PC之间的IPSec进行保护。
- Site-to-Site (站点到站点或者网关到网关) : 3个机构分布在互联网的3个不同的地方，各使用一个网关相互建立VPN隧道，企业内网（若干PC）之间的数据通过这些网关建立的IPSec隧道实现安全互联。

提纲

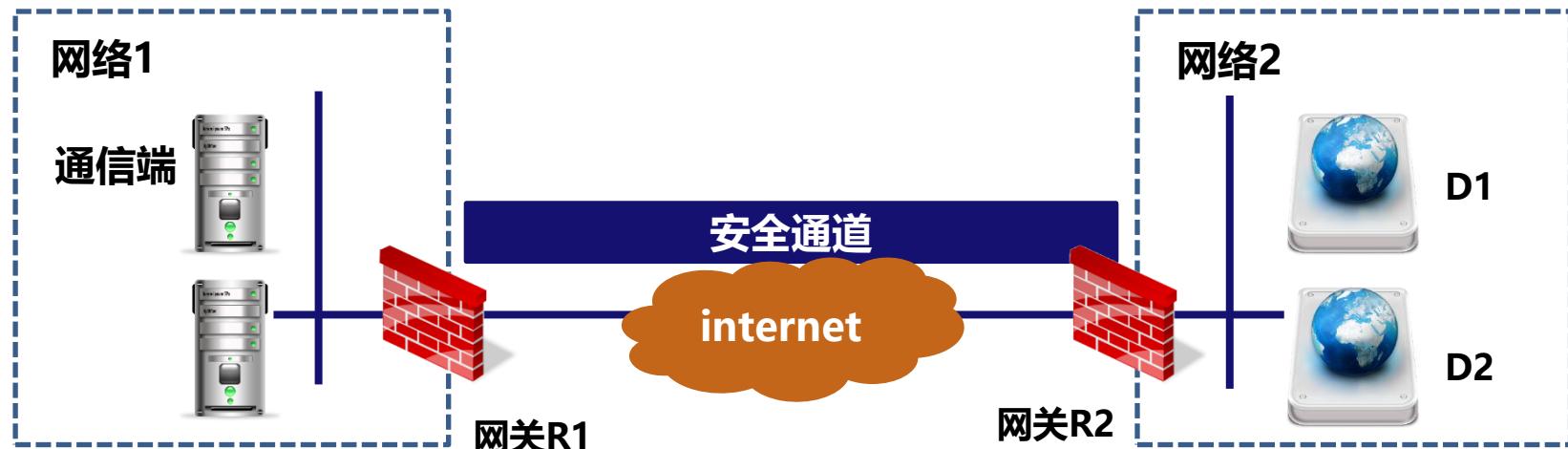
- 一、IKE协议流程
- 二、认证首部AH
- 三、封装安全载荷ESP
- 四、IPSec应用

端到端安全



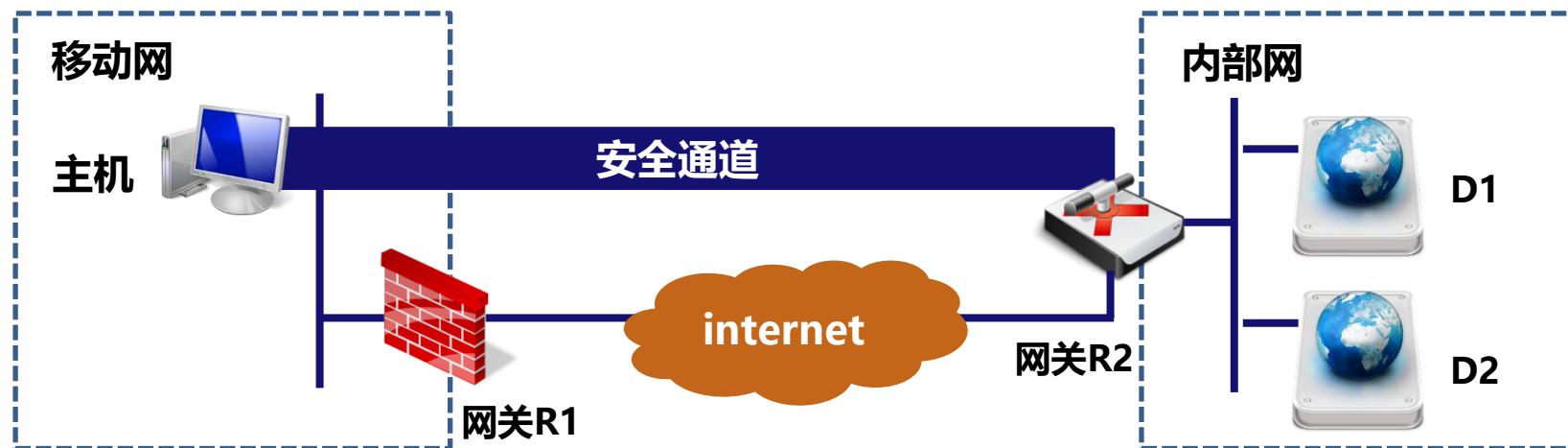
- 通信源S和目的端D都要部署IPSec，通信的源点和目的点就是安全的起点和终点。这种应用通常使用传输模式。S发送数据前对数据进行安全处理，到达D后由D验证并还原安全通道。

◀ 基本VPN支持



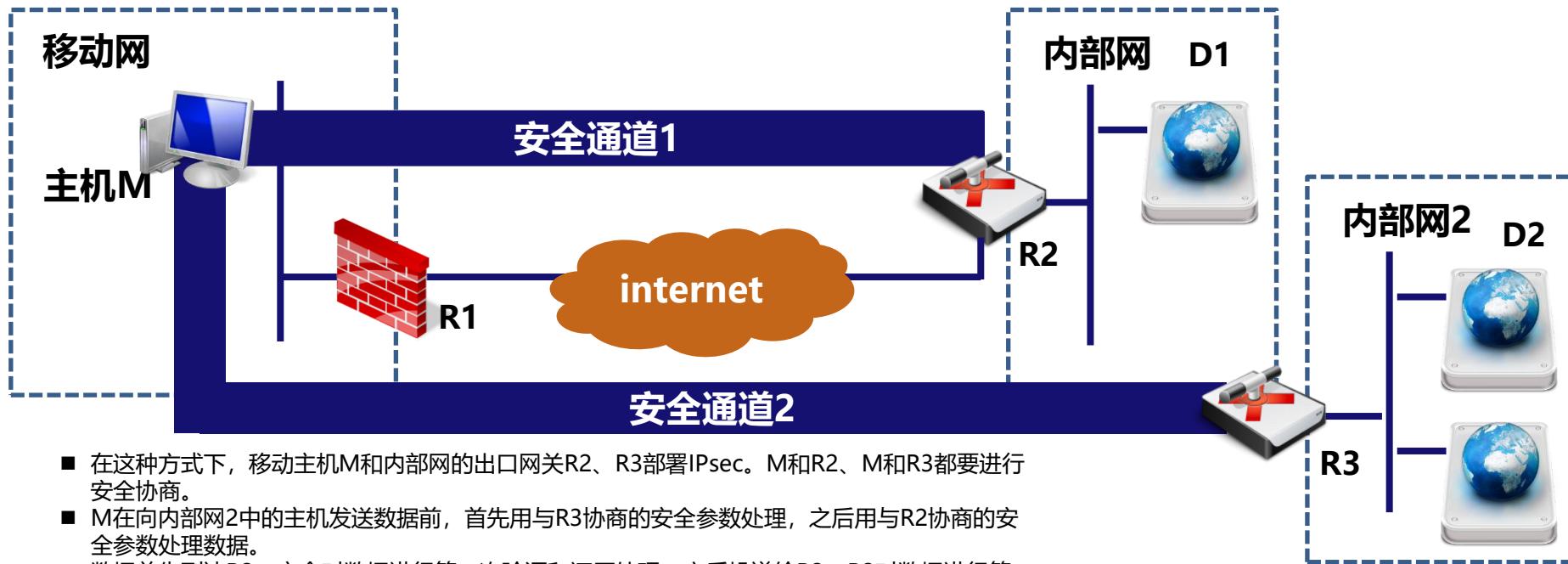
- 网络1和网络2的出口网关部署IPsec。通信的源点和目的点为网络中的主机，安全的起点和终点是两个出口网关。这种应用使用隧道模式。
- 网络1中的数据首先发送给R1进行安全处理，到达R2后对数据进行验证和还原，之后递交给网络2内部的目的端。封装IPsec报文时，内部IP头中包含的IP地址分别是通信的源点和目的点；外部IP头中包含的IP地址是2个出口网关的地址。

4 保护移动用户访问内部网



- 移动主机M和内部网的出口网关部署IPsec。通信源点和目的点为移动主机和内部网中的主机，安全的起点和终点则是移动主机和内部网的出口网关。这种应用使用隧道模式。
- 移动主机M在向内部网中的主机发送数据前，首先进行安全处理，之后发送给网关。网关收到后对数据进行验证和还原，之后递交给内部网中的目的端。封装IPSec报文时，内部IP头中包含的IP地址分别是移动主机通信的源点和目的点。

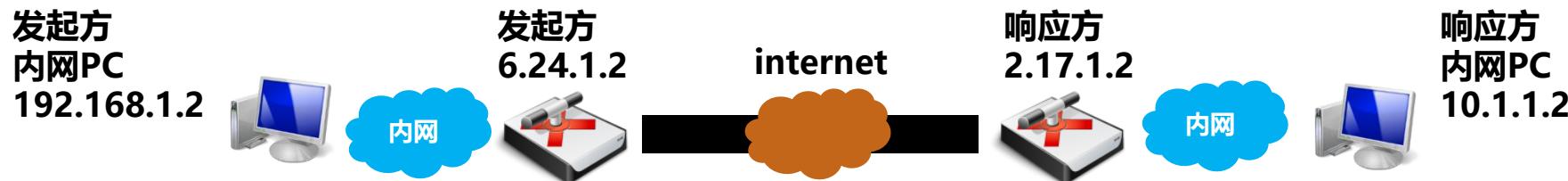
4 嵌套式隧道



案例分析

在站点-站点交换中，传输模式是否可行？【反证法】

- 源、目的地址都是私有地址，因为私网路由问题，该数据包在互联网中被丢弃；
- 假设数据包成果穿越了互联网，因为目的地址不是响应方网关，因此响应方并不进行解密，而是直接转发给内网PC；
- 响应方内网PC因为没有进行IPSec协商，因此密文数据无法进行解密而被PC丢弃。



小结

- ▲ 5种安全服务
 - 数据完整性、数据源发认证、抗重放攻击、机密性、有限的传输流机密性
- ▲ 2个核心概念
 - 安全策略SP：针对某个IP数据报，应用IPsec、绕过IPsec、丢弃处理
 - 安全关联SA：安全策略的实例化，安全协议、加密算法和认证算法等
- ▲ 应用方式
 - 主机-主机、主机-网关、网关-网关、嵌套隧道



办公地点：理科大楼B1209

联系方式：17621203829

邮箱：liuhongler@foxmail.com