第2部分 因特网安全体系

第 6 章 网络层安全协议--IPSec

- 6.1 IPSec协议概况
- 6.2 认证头协议AH
- 6.3 ESP协议
- 6.4 IPSec安全策略、算法与应用模式
- 6.5 Internet密钥交换IKE

引言

- IP协议维系着整个TCP/IP协议的体系结构，除了数据链路层外，TCP/IP的所有协议的数据都是以IP数据报的形式传输的
- 针对互联网上的不同应用，定义了多种应用相关的安全协议
- IP层安全不仅能为具有安全机制的应用提供安全保证，而且可以为那些没有安全机制的应用提供安全服务

6.1 IP Sec协议概述

- IP几乎不具备任何安全性
  - 没有为通信提供数据源鉴别机制
  - 没有为数据提供机密性保护
  - 没有为数据提供完整性保护机制
- 1995年开始，IETF着手制定了一套用于保护IP通信的IP安全协议（IP Security，IPSec--Required for IPv6, optional for IPv4)
- IPsec 提供了标准、健壮且包含广泛的机制保证IP 层安全。

IP Sec协议概述

- **IP层面临的安全攻击及安全服务需求分析**

攻击	安全服务
数据窃取	无连接机密性
数据伪造	数据源认证
数据篡改	无连接完整性
流量分析	(受限制的)流量机密性
路由攻击	访问控制

数据加密

数据认证

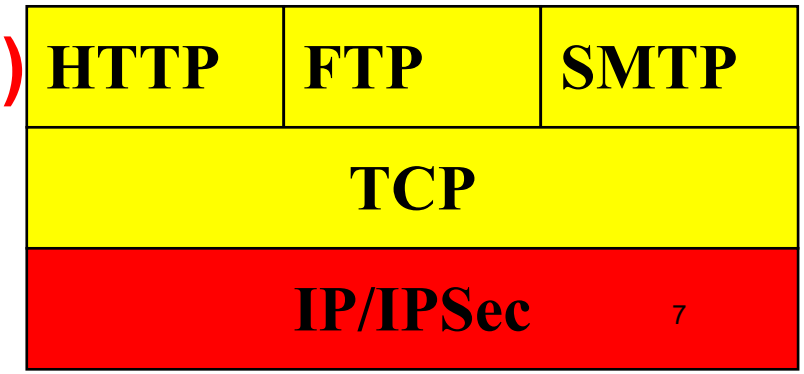
算法/密钥
协商与分发

IP Sec的功能、特点与应用

- 与防火墙或路由器相结合，为跨越边界的所有流量提供安全性
- IPSec位于传输层(TCP、UDP)之下，对应用程序透明，对端用户透明
- IPsec在网络设备(routers, Firewalls)上运行
- 应用
  - LAN与WAN安全连接(如大学的VPN)
  - 安全远程访问
  - 与其他组织内设备之间的安全通信
  - 电子商务安全

IP Sec协议概述

- IPsec 是能够在 IP 层提供互联网通信安全的协议族。
- 相关IETF的RFC建议标准
  - 体系结构（RFC4301）
  - Internet协议安全结构（RFC2401）
  - IP认证头AH （RFC4302）
  - IP封装安全净荷ESP(RFC4303)
  - Internet密钥交换IKE(RFC4306)
- IPSec在TCP/IP中的位置



IP Sec协议概述

- IPsec 是个框架，它允许通信双方选择合适的算法和参数（例如，密钥长度）。
- 为保证互操作性，IPsec 还包含了所有 IPsec 的实现都必须有的一套加密算法。

IP Sec协议概述

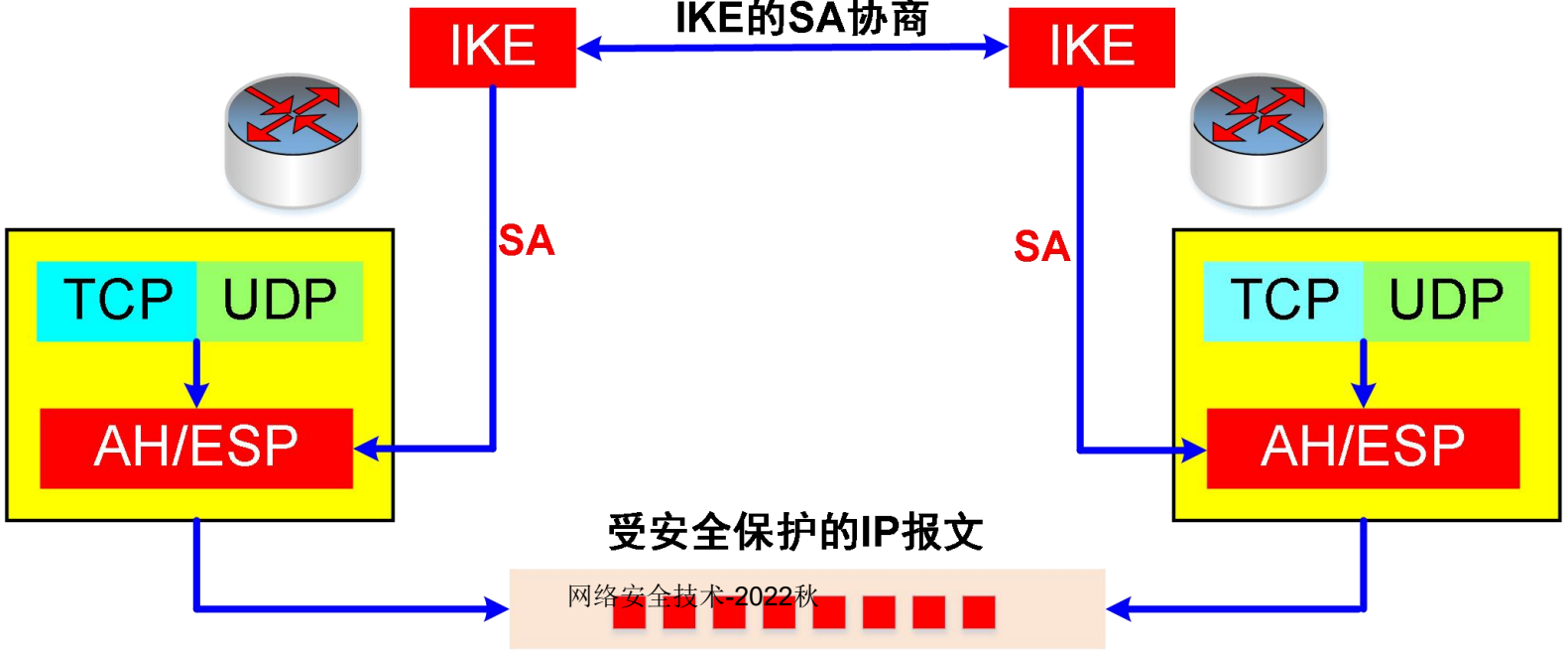
- IPSec的安全结构包括以下四个基本部分
  - 安全协议：AH和ESP
  - 安全关联(SA)
  - 密钥交换：手工和自动（IKE）
  - 认证和加密算法
- IPSec包括三类协议
  - 安全协议AH
  - 安全协议ESP
  - 密钥管理协议IKE

IPsec协议组成

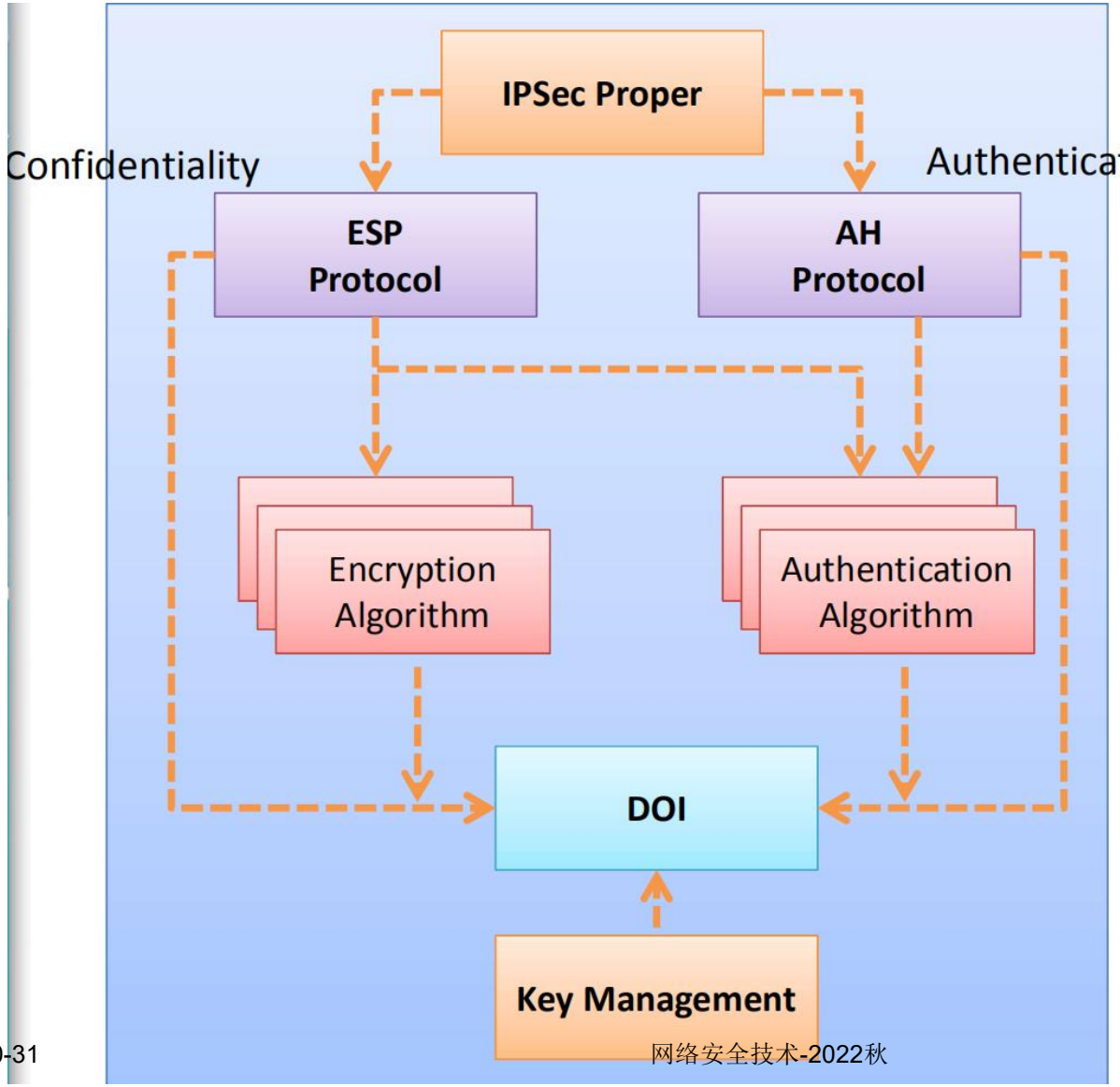
- IPSec的安全协议
  - 鉴别首部 AH (Authentication Header)协议
    - 提供源点鉴别和数据完整性，但不能保密。
  - 封装安全有效载荷 ESP (Encapsulation Security Payload)协议
    - 提供源点鉴别、数据完整性和保密。
- 密钥交换 IKE (Internet Key Exchange)协议
  - 定义了通信实体间进行身份认证、创建安全关联、协商加密算法以及生成共享会话密钥的方法

IPSec协议组成

- IKE是UDP之上的一个应用层协议，是IPSec的信令协议；
- IKE为IPsec协商建立SA，并把建立的参数及产生的密钥交给IPSec；IPSec使用IKE建立的SA对IP报文加密或者验证处理



IPSec协议体系架构



- Encapsulate Security Payload (ESP)
- Authentication Header (AH)
- Domain of Interpretation (DOI)

IPSec的安全服务

- IPSec的安全功能或服务

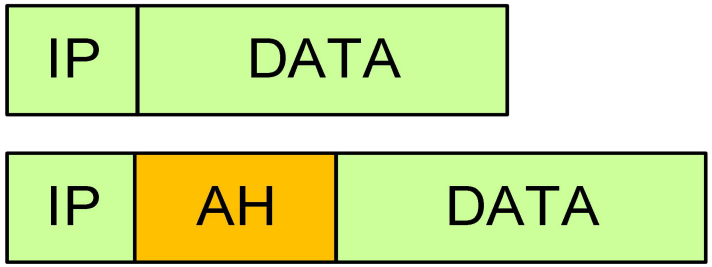
安全功能（服务）	相关协议
访问控制	AH
无连接完整性	
数据起源认证	
抗重放攻击	
机密性	ESP
有限的数据流机密性	
抗重放攻击	
访问控制	

6.2 认证头协议(AH)

- AH为IP报文提供无连接的数据完整性、数据起源认证，还具备可选择的重放攻击保护
- AH不提供数据加密保护。AH不对受保护的IP数据报的任何部分进行加密，除此之外，AH具有ESP的所有其他功能。
- AH的作用是为IP数据流提供高强度的密码认证

认证头协议(AH)

- AH采用消息认证码MAC对，最常用的MAC是96-bit HMAC



- AH的消息摘要的生成需要通信双方共享密钥
- AH和ESP同时保护数据，在顺序上，AH在ESP之后

认证头格式

- **AH头标格式**

下一头标	净符长度	保留域
安全参数索引(SPI)		
序列号		
认证数据（长度可变）		

- **位置**

IPv6头标	AH	TCP头标+数据	
IPv6头标	逐跳、路由、分段	AH	TCP头标+数据
IPv6头标	AH	信宿头标	TCP头标+数据
IPv6头标	信宿头标	AH	TCP头标+数据

信宿头标仅被目的主机处理

信宿头标被目的主机列表中的多个目的主机处理

完整性校验值ICV的计算

- ICV(Integrity Check Value)是AH或ESP用来验证IP数据报完整性所用的验证数据(96-bit HMAC)
- 使用前需要双方协商SA
- 计算原则
  - 认证范围包括整个IP头
  - 与传输过程相关的域（可变域）清零(Why? How?)

IPv4的可变域与不变域

- 可变域

服务类型(Type of Service)	生命周期TTL
标志(Flag)	头校验值(Header Checksum)
分段偏移量(Fragment Offest)	可选项(Options)

- 不变域

版本(Version)	协议(Protocol)
头标长度(Header Length)	源IP地址
总长度(Totle Length)	目的IP地址
标识(Identification)	数据(Data)

IPv6的可变域与不变域

- 可变域

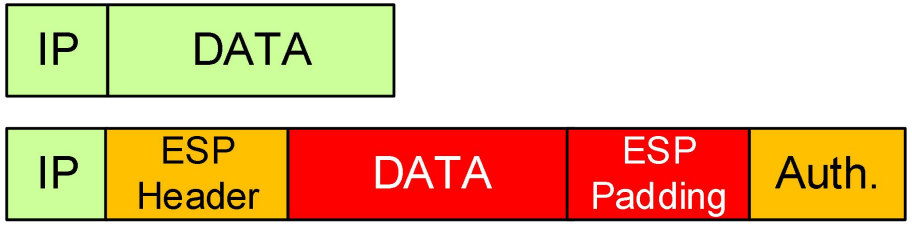
优先级(Priority)	相当于V4的服务类型
流标记(Flow Lable)	新增加的域
跳数限制(Hop Limit)	相当于V4的TTL

- 不变域

版本(Version)	含义与v4相同
载荷长度(Payload Length)	相当于V4的总长度
下一头标(Next Header)	相当于V4的协议类型
源IP地址、目的IP地址	含义与v4相同

6.3 封装安全载荷协议(ESP)

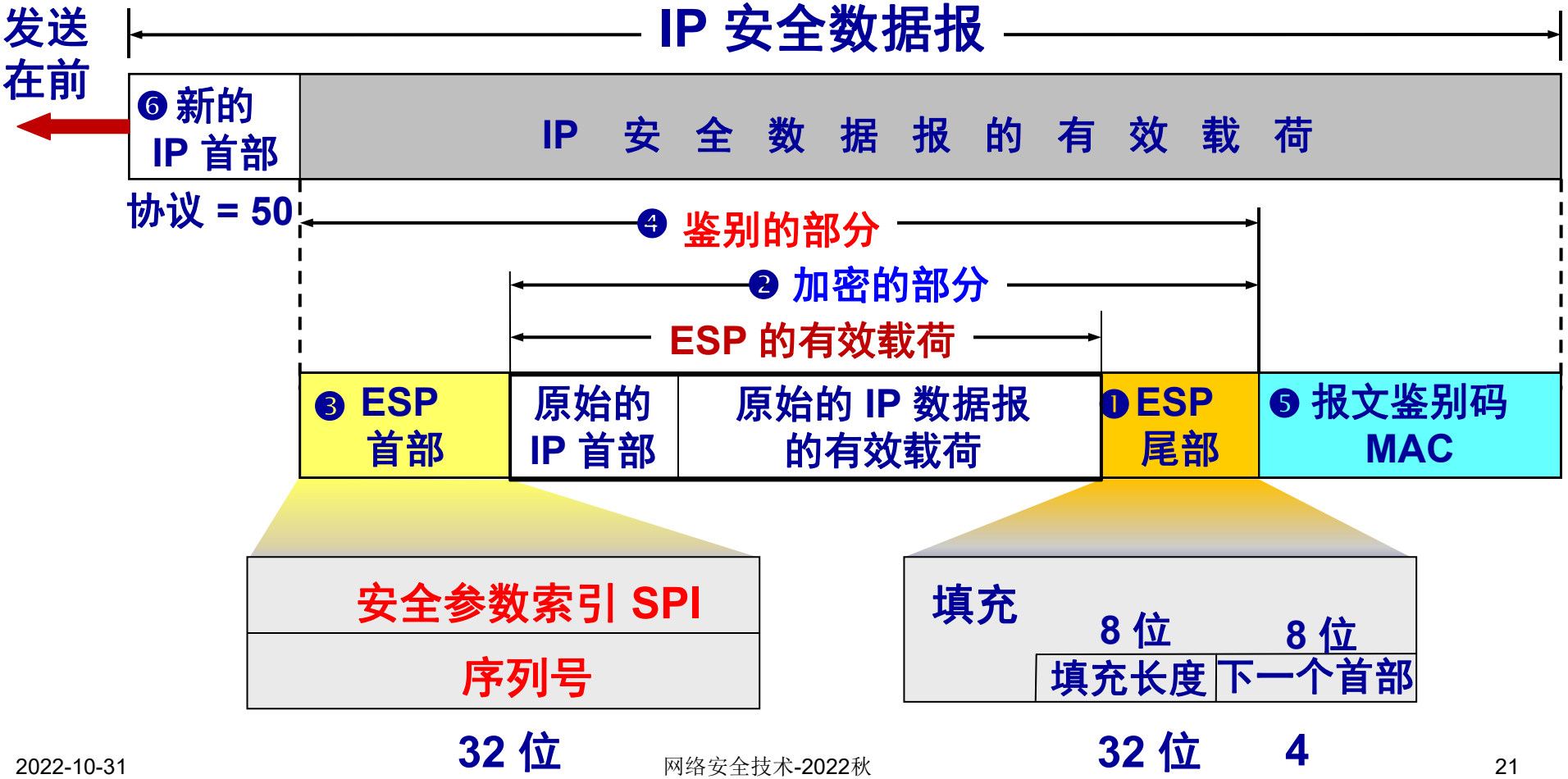
- ESP为IP报文提供数据数据机密性、数据源认证、无连接完整性、重放攻击保护以及有限的数据流机密性。
- 比AH增加了数据机密性服务（使用加密算法实现）和有限的数据流机密性服务（由隧道模式下的机密性服务提供）。
- ESP头可以位于IP头与上层协议之间，或者用它封装整个IP数据报。



- ESP协议分配数为50
- ESP可以单独使用、嵌套使用或者与AH结合使用

ESP数据包格式

隧道方式下的 IP 安全数据报的格式



6.4 IPSec安全策略与算法

- 安全策略：指应用于从源端到目的端传输的IP数据报的安全策略,由两个数据库（SPD和SAD）的交互决定
  - 安全策略数据库SPD（Security Policy Database）
  - 安全关联数据库SAD（Security Association Database ）

6.4 IPSec安全策略与算法

- 安全算法
  - 加密：CBC-DES
  - 认证：HMAC/MD5， HMAC/SHA(96 bits)
- 增加的可选的DOI(Domain of Interpretation)依赖算法（抗重放攻击）
  - TDES
  - Blowfish
  - CAST-128
  - IDEA
  - RC5

6.4 IPSec安全策略与算法

- 安全关联SA（Security Association）的概念是IPSec的基础
  - AH和ESP均使用SA
  - IKE协议的一个主要功能是SA的管理与维护
- 在使用 AH 或 ESP 之前，先要从源主机到目的主机建立一条网络层的逻辑连接。此逻辑连接叫做安全关联 SA (Security Association) 。
- SA是通信对等方之间对某些要素的一种协定

例如：IPSec协议、协议的操作模式（传输模式和隧道模式）、密码算法、密钥以及密钥生存期等

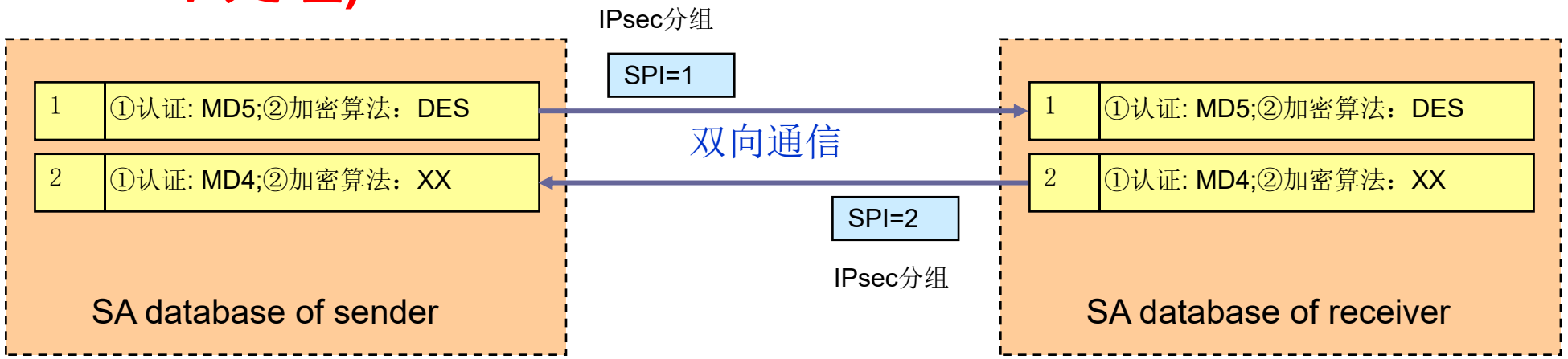
6.4.1 安全关联

- 安全关联SA（Security Association）：一种描述安全服务的发送方和接收方之间的单向关系
  - AH和ESP均使用SA
  - IKE协议的一个主要功能是SA的管理与维护
- 在使用 AH 或 ESP 之前，先要从源主机到目的主机建立一条网络层的逻辑连接。此逻辑连接叫做安全关联 SA (Security Association) 。
- SA是通信对等方之间对某些安全要素的一种协定

例如：IPSec协议、协议的操作模式（传输模式和隧道模式）、密码算法、密钥以及密钥生存期等

安全关联SA

- SA通过密钥管理协议IKE在通信对等方之间协商，当一个SA协商完成后，双方安全关联数据库(SAD)中均存储有该SA参数
- 在安全关联 SA 上传送的就是 IP 安全数据报。
- 接收系统根据SPI选择合适的SA(接收到的数据包在此SA下处理)



安全关联SA

- SA是单向的，因此，对于输入和输出的数据流需要独立的SA

举例：若 *n* 个员工进行双向安全通信，一共需要创建 *n(n-1)* 条安全关联 SA。

- 通常SA是成对的形式存在的，每个朝一个方向
- SA具有生存期，SA驻留在安全关联数据库（SAD）内，当SA终止时从SAD中删除
- SA既可人工创建它，亦可采用动态创建方式。

SA的标识

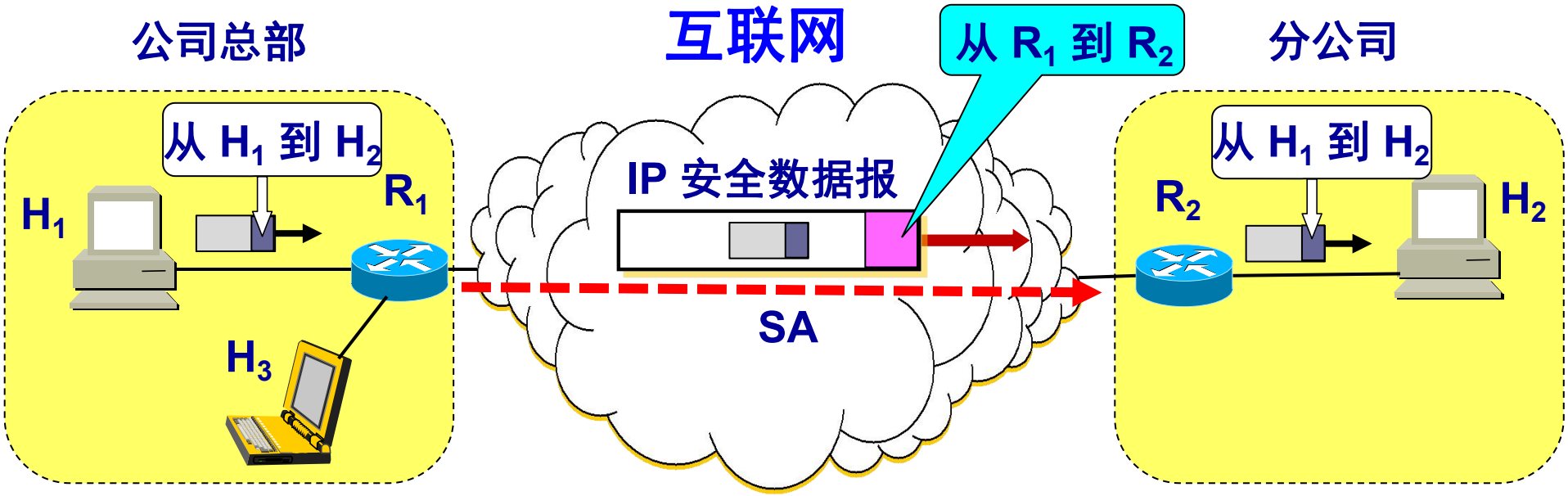
- SA由一个三元组唯一地标识

  ＜安全参数索引SPI，目标IP地址，安全协议＞

  - 安全参数索引SPI（Security Parameter Index）：32位，在AH和ESP协议头中传输，用于对SA进行标识及区分同一个目的地址所链接的多个SA
  - IPSec协议值（AH或ESP）
  - 目的IP地址（单播地址）
- 接收方根据收到的消息中的三元组标识搜索SDA, 确定与该数据报相关的SA或者SA束

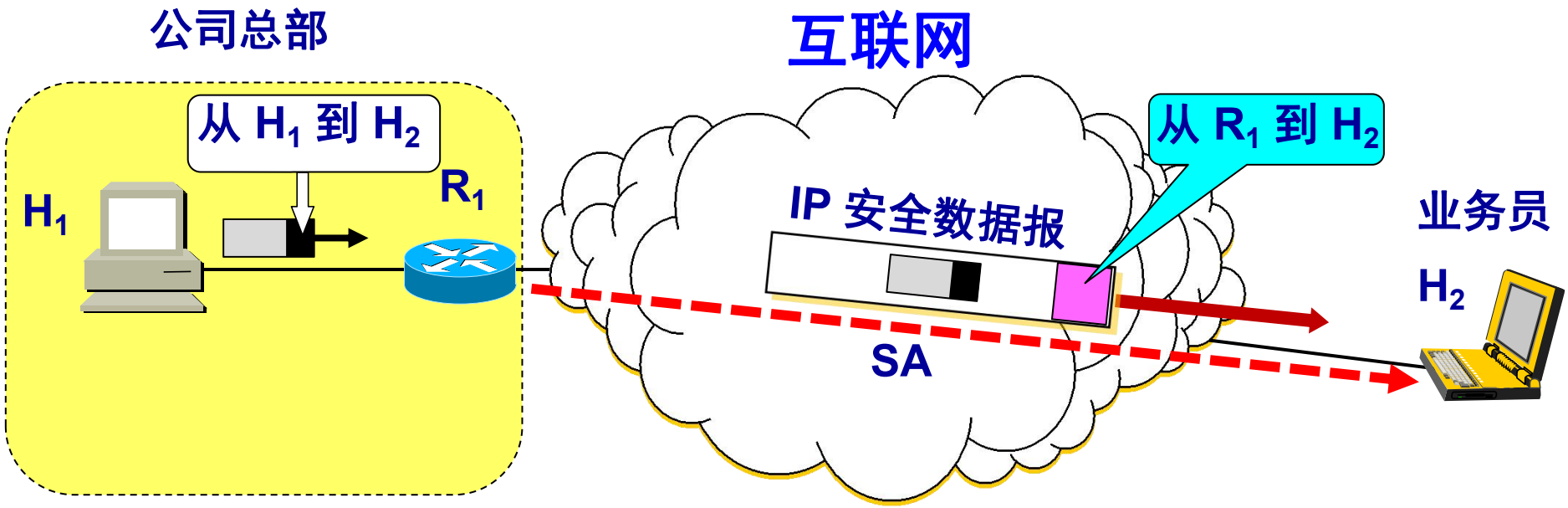
路由器 R_1 到 R_2 的安全关联 SA

假定公司总部的主机 H_1 要和分公司的主机 H_2 通过互联网进行安全通信。公司总部与分公司之间的安全关联 SA 就是在路由器 R_1 和 R_2 之间建立的。



路由器 R_1 到主机 H_2 的安全关联 SA

若公司总部的主机 H_1 要和某外地业务员的主机 H_2 进行安全通信，需要在公司总部的路由器 R_1 和外地业务员的主机 H_2 建立安全关联 SA。



6.4.2 IPSec的工作模式

- 操作过程
  - 使用SPI查找SA
  - 使用SA进行数据完整性验证
  - 使用SA对认证后的数据进行加解密

- 两种操作模式
  - 传送模式--只保护IP分组中的数据(Payload)
  - 隧道模式--保护整个IP分组

隧道

- **隧道**是把一个包封装在另一个新包中，即在一个数据包前面**增加一个新的IP头**
- 新增加的外部头的目的地址通常是IPSec防火墙、安全网关或路由器
- 利用隧道技术可以隐藏内部数据和网络细节

IP安全数据报两种工作方式

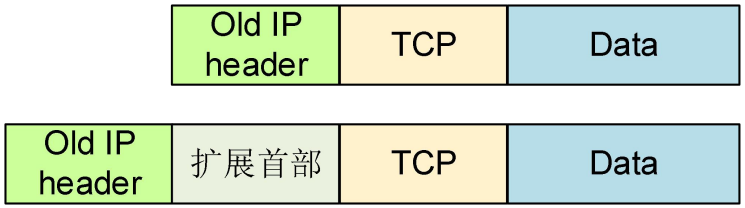
- 无论使用哪种方式，最后得出的 IP 安全数据报的 IP 首部都是不加密的。
- 所谓“安全数据报”是指数据报的数据部分是经过加密的，并能够被鉴别的。
- 通常把数据报的数据部分称为数据报的有效载荷(payload)。
  - 传送模式--只保护IP分组中的有效载荷
  - 隧道模式--保护整个IP分组

ESP的操作模式

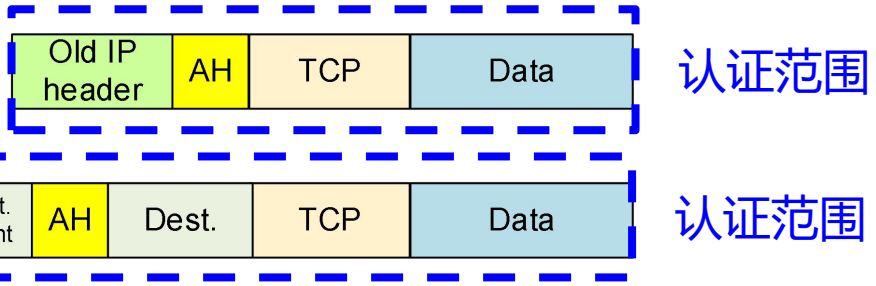
- ESP有两种操作模式
  - 传送模式
  - 隧道模式
- 传送模式：用于终端之间通信，提供数据机密性
- 隧道模式：用于在安全网关之间建立虚拟专用网，抗流量分析

AH的传输模式与隧道模式

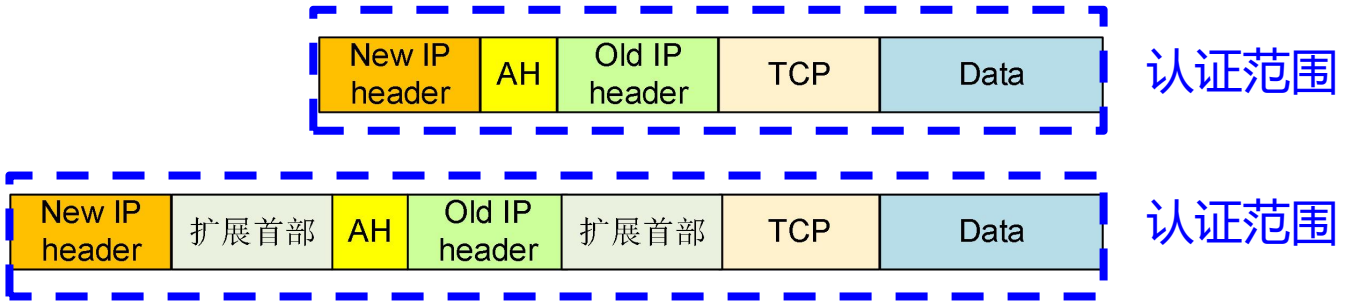
原始IP数据分组



传输模式

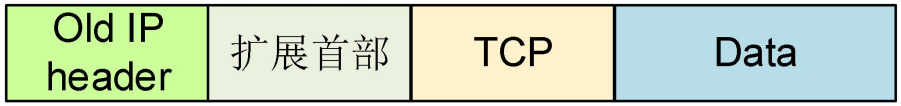


隧道模式

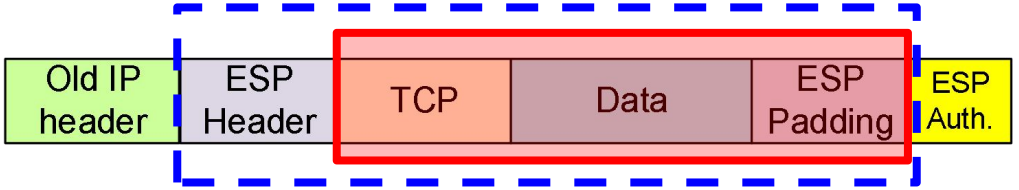


ESP的传输模式与隧道模式

原始IP数据分组

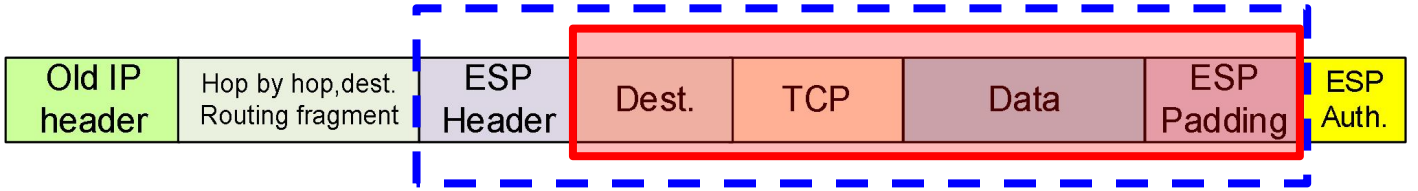


传输模式

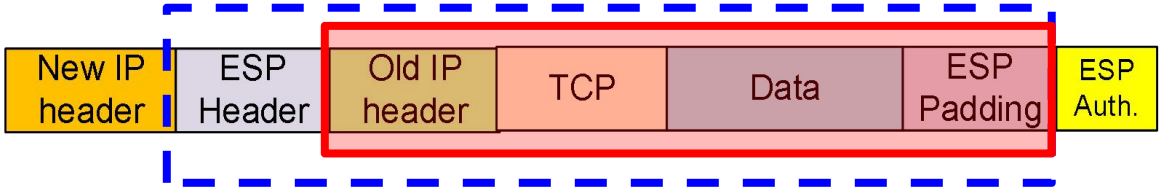


认证

加密



隧道模式



6.4.3 IPSec的处理过程

- 与IPSec相关的两个数据库
  - 安全策略数据库SPD（Security Policy Database）
  - 安全关联数据库SAD（Security Association Database ）
- SPD：指定了流入或者流出主机或者路由器的数据流的安全策略
- SAD：包含有与当前活动的SA相关的参数。

安全策略数据库SPD

- 对于一个IPSec节点，进入和流出包都需要参考安全策略数据库（SPD）
- 对于进入或流出的数据包，有三种可能的选择：丢弃、绕过IPSec或应用IPSec。
  - 丢弃是指根本不允许离开主机、穿过安全网关，或最终传递到某一应用程序
  - 绕过(通过)是指允许通过而不用额外IPSec保护的传输
  - 应用(保护)是指需要IPSec保护的传输并且对于这样的传输SPD必须规定提供的安全服务，所使用的协议、算法等等。

安全策略数据库SPD

- SPD中包含有一个策略条目的有序列表
- 每个条目包含一个或多个选择符和一个标志
- 选择符包括：目的IP地址、源IP地址、传输层协议等
- 标志：表明与条目中的选择符匹配的数据报是否丢弃、绕过或应用。如果应用，则条目中需包含一个指向SA内容的指针
- 匹配原则
  - 选择符与数据通信流相匹配的第一条目被应用到该通信中
  - 如果没有匹配的条目，数据包被丢弃
- SPD中的条目应按照应用程序所希望的优先关系排序

SPD举例

- 某主机SPD

协议	本地IP	端口	远程IP	端口	动作	注释
UDP	1.2.3.101	500	*	500	通过	IKE
ICMP	1.2.3.101	*	*	*	通过	错误信息
*	1.2.3.101	*	1.2.3.0/24	*	保护：ESP传输方式	加密传输，SA指针
TCP	1.2.3.101	*	1.2.4.10	80	保护：ESP传输方式	加密到服务器
TCP	1.2.3.101	*	1.2.4.10	443	通过	TLS
*	1.2.3.101	*	1.2.4.0/24	*	丢弃	DMZ其他内容
*	1.2.3.101	*	*	*	通过	Internet

返回

安全关联数据库SAD

- SAD中包含SA条目(无序)，SA由三元组索引{SPI，IP地址，安全协议}
- 输入和输出IPSec处理要保存单独的SAD
  - 根据三元组找到的第一个匹配条目，将该SA的参数与IPSec数据包中的域比较
  - 如果一致，则处理该数据包；否则，丢弃
  - 如果没有检索到SA条目且数据包是输入包，则丢弃
  - 如果没有检索到SA条目且数据包是输出包，则创建一个新的SA
- SAD中找到的第一个匹配条目将被应用
- 生存期两种限制：软限制和硬限制
  - 达到软限制时通信双方必须重新协商一个新SA来代替旧SA，但旧SA不在数据库中删除直到硬限制过期

安全关联数据库SAD

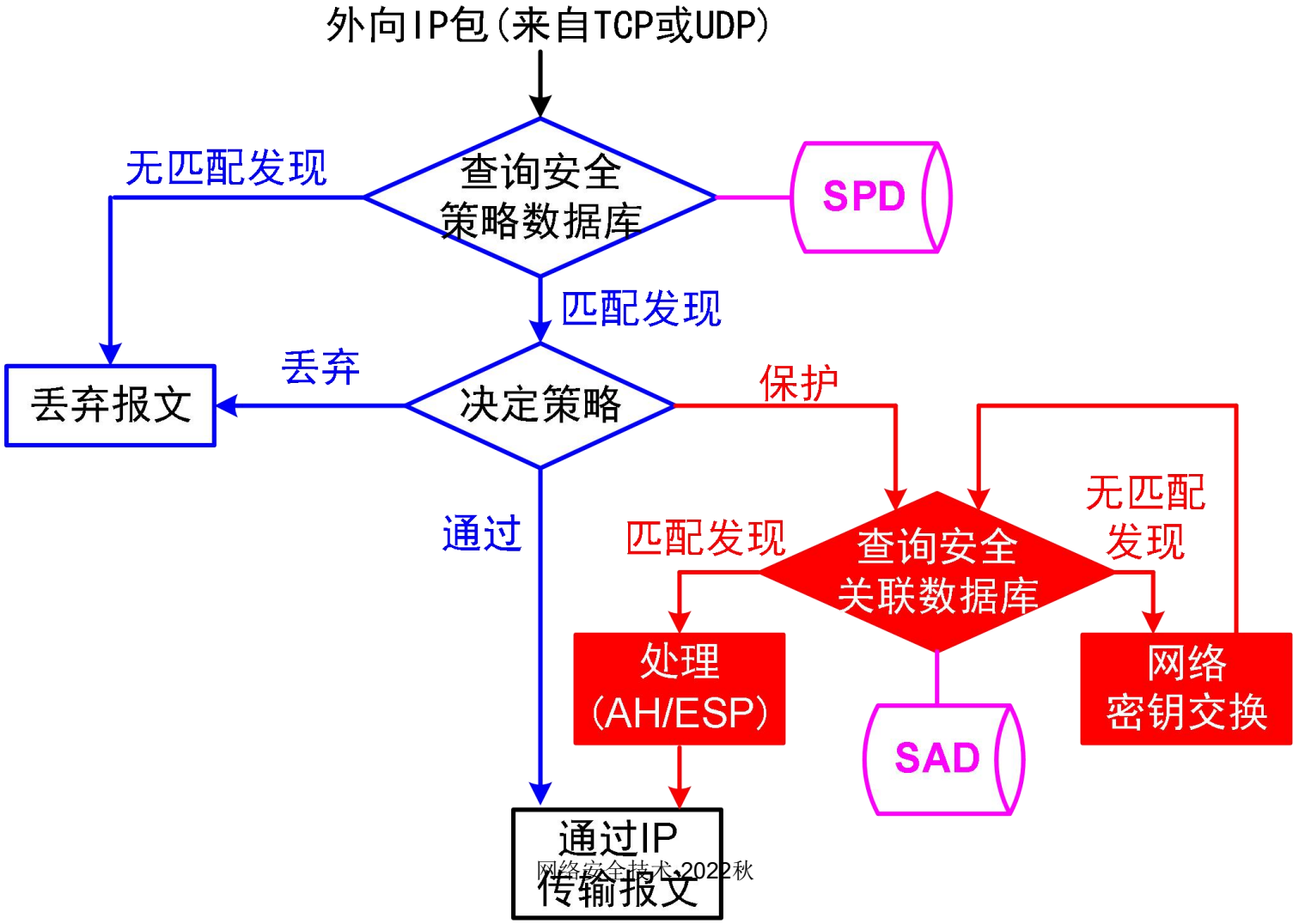
- SAD条目包含如下域
  - 安全参数索引：由SA接收端选定的一个32比特数值
  - 序列号计数器（32位）
  - 序列号溢出标志: 标识序列号计数器是否溢出，溢出时，阻止在此SA上继续传输包
  - 抗重放窗口：用于判断AH或ESP数据包是否为重放
  - AH信息：认证算法、密钥、密钥生存期及相关参数
  - ESP信息：加密和认证算法、密钥、初始值、密钥生存期及相关参数
  - SA的生存期
  - IPSec操作模式（传输模式、隧道模式、通配模式）
  - 路径最大传输单元PMTU

防止重放服务

- **重放攻击**：指攻击者在得到一个经过认证的包后，在以后的某个时刻将其传送到目的站点的行为。
- SA的序号
  - 新SA建立，发送方将序号设置为0；
  - 在SA上发送一个数据包，计数器加1；
  - 序号到达$2^{32}-1$，SA终止，使用IKE协商新的SA.

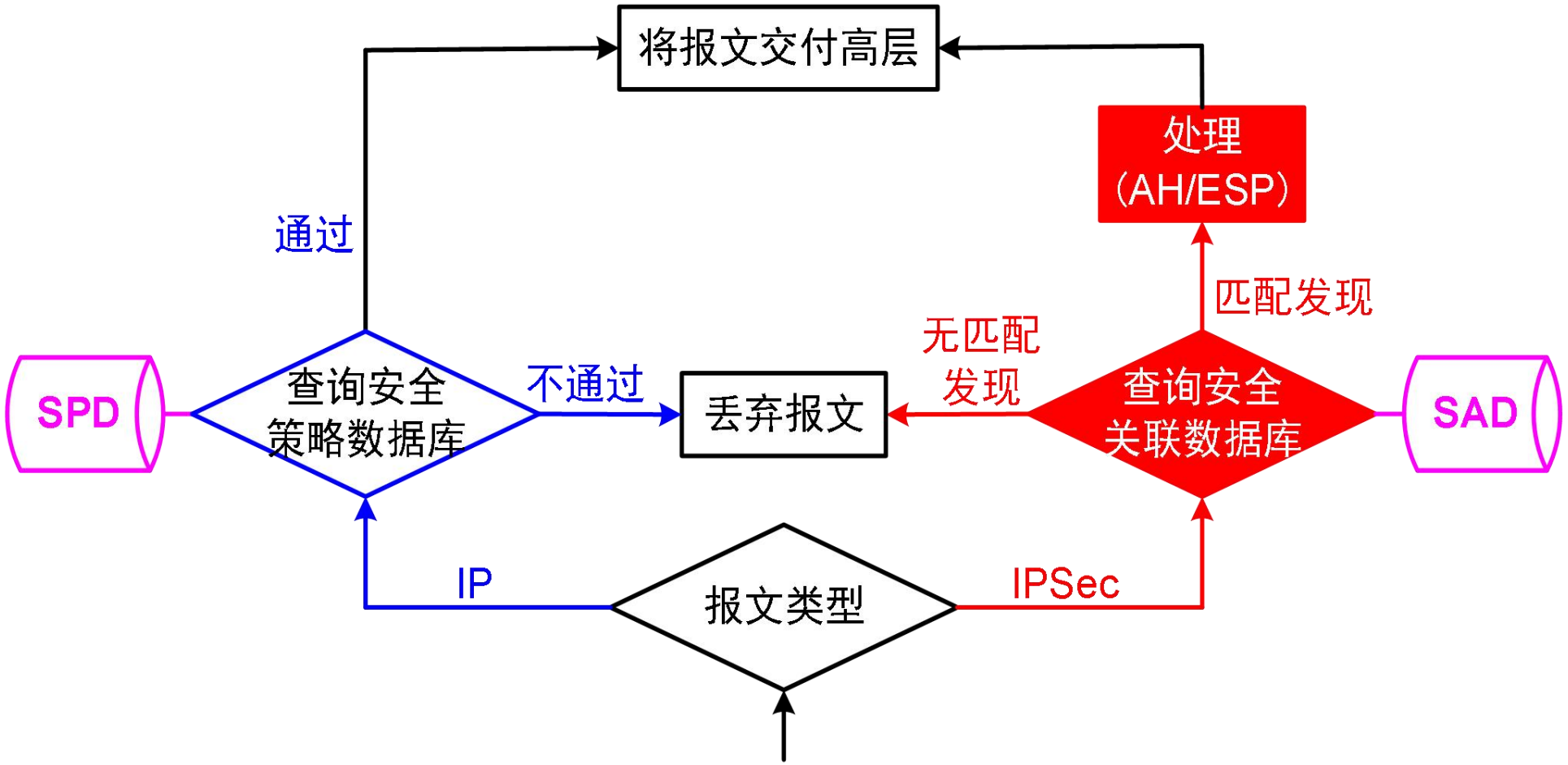
IP通信进程

- 出站报文处理模型

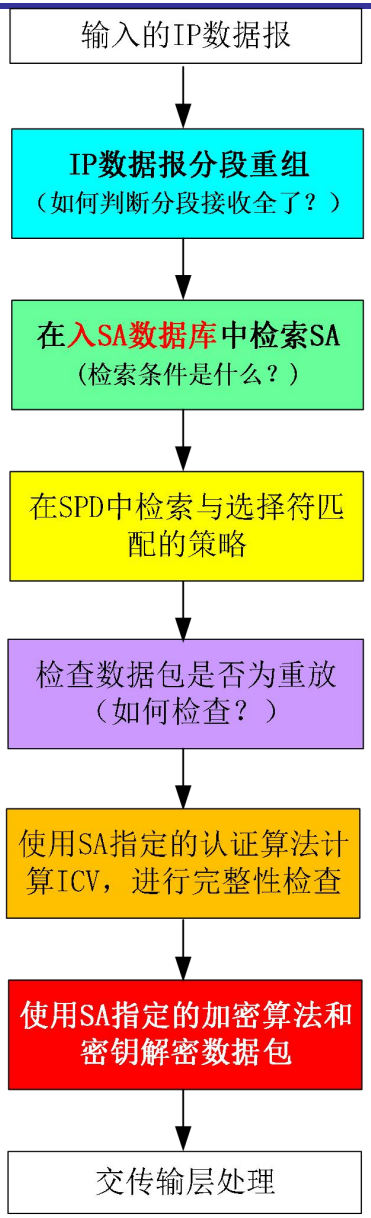


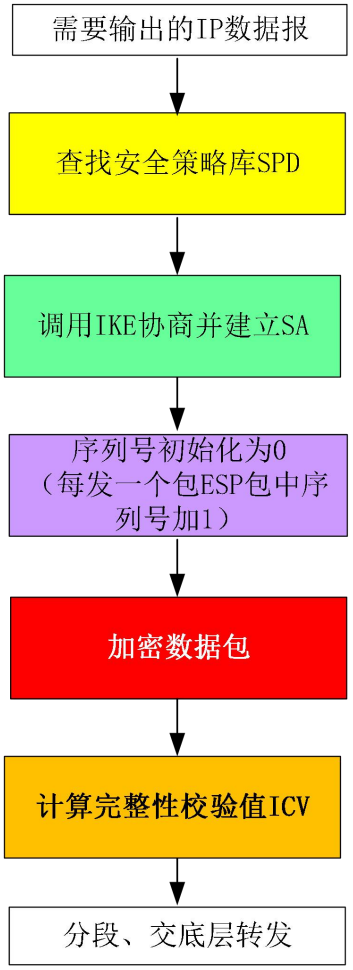
IP通信进程

- 入站报文处理模型



ESP输入和输出处理过程





组合安全关联SA

- 单个SA可以实现AH协议或ESP协议，但是不能同时实现这两个协议
- 为相同流量采用多个SA
  - 形成安全关联束(security association bundle)
  - 多个SA可在不同或相同的端点终止
  - 多个安全关联组合成束的方法
    - 传输邻接：指在不调用隧道的情况下，对一个IP包使用多个安全协议（仅允许一级组合）
    - 隧道迭代：利用隧道来应用多层安全协议。允许多层嵌套。
  - 两种方法可以组合使用

6.5 Internet密钥交换（IKE）

- Internet密钥交换（IKE）解决了在不安全的网络环境（如Internet）中安全地建立或更新共享密钥的问题。
- IKE是一个通用的协议，不仅可为IPSec协商安全关联，而且可以为SNMPv3、OSPFv2等任何要求保密的协议协商安全参数
- IKE主要用于完成密钥协商(密钥的确定和分发)，在2014年10月已成为互联网的正式标准 [RFC 7296]。

IKE

- 两个应用之间安全(完整性、保密性)双向通信需要4个密钥
- IETF的IPSec指定所有兼容的系统必须同时支持手工和自动的SA和密钥管理
- 手工
  - 最简单的密钥管理方式，手工配置每一个系统安全通信使用的密钥信息及密钥管理数据
  - 适用于小范围、静态环境，对大型网络不适合
- 自动
  - 通过使用自动的密钥管理协议，创建SA所需要的密钥，IKE是目前的工业标准
  - 适合大型、分布式系统，可扩展性好

IKE的功能

- 降低手工配置的复杂度
- 定时更新SA
- 定时更新密钥
- 允许端与端之间的动态认证

Internet密钥交换（IKE）

- IKE属于一种混合型协议，主要包括Internet安全关联和密钥管理协议（ISAKMP）和密钥交换协议OAKLEY。

  (1) Oakley——是密钥确定协议，基于Diffie-Hellman密钥交换。

  (2) 互联网安全关联和密钥管理协议ISAKMP ——提供了因特网密钥管理框架和所支持的专用协议，包括格式和安全属性协商。

  ISAKMP提供安全协议框架，Oakley提供安全机制

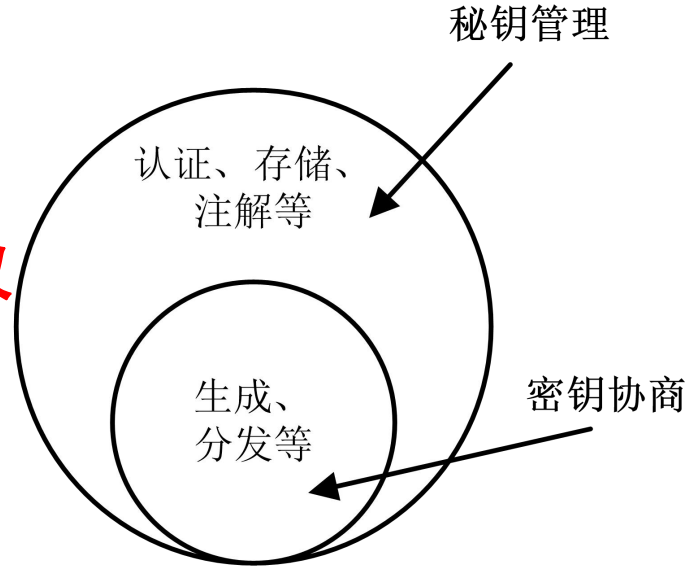


图 7-12 密钥管理与密钥协商

- IKEv2不再区分两个协议

IKE密钥确定协议

- 是Diffie-Hellman密钥交换协议的细化
- Diffie-Hellman特点
  - 仅在需要时才创建密钥
  - 仅需协商全局参数q和a
  - 不提供身份信息，易受*重放攻击(replay attack)*
  - 不验证用户身份，易受*中间人攻击(man in the middle)*
  - 具有计算密集性，易受*阻塞攻击(clogging attack)*

IKE密钥确定协议的特征

- 协商指定Diffie - Hellman算法的全局参数
- 交换Diffie-Hellman的公钥值
- 运用Cookie机制来防止拥塞攻击
- 使用随机数nonce阻止重放攻击
- 对Diffie-Hellman交换进行认证，阻止中间人攻击

IKE的身份认证方式

- **数字签名**: 利用数字证书来表示身份，利用数字签名算法计算出一个签名来验证身份。用双方均可以得到的散列码进行签名的方法来认证交换，每一方都用自己的私钥加密散列值。散列值是使用重要的参数（用户ID、随机数）生成的。

- **公开加密**:用发送方的私钥对参数（如ID、随机数）加密来认证交换。

- **对称密钥加密**:使用其他方法传送密钥，并用该密钥对交换参数进行对称加密，从而实现对密钥交换过程的认证。

IKEv2交换

- 用于交换安全参数(但不建立密钥)的安全协议
  - 建立、协商、修改和删除IPSec安全关联的协议(过程和数据包格式)
  - 交换cookie、安全参数、密钥管理和识别的通用框架
  - 细节由其他协议定义
- 两个阶段
  - SA--建立安全、认证信道
  - KMP--协商安全参数

一个完整的IPSecVPN工作原理

192.168.1.25

公司A

192.168.2.34

公司B

Source Address	Destination Address	Secure Service	Others
192.168.1.25	192.158.2.34	安全	……
192.158.1.34	192.168.1.25	绕过、丢弃	……
SPD中的数据项类似于防火墙的配置规则			

SPI	Destination Address	Security Protocol
256	192.168.1.25	AH
257	192.168.1.25	ESP
258	192.168.2.34	AH
259	192.168.2.34	ESP

SPI	Security Protocol	Algorithm	Key	Others
256	AH	加密MD5	010	……
257	ESP	DES CBC 4	101	……
258	AH	加密SHA-1	001	……
259	ESP	3DES CBC	110	……
SAD中包含每一个SA的参数信息，如算法、密钥等				

负 载

IP 头

哪些安全服务

为流入的IP数据提供

查找SPD数据库决定

查找对应SA的参数

建立相应的SA

写入SAD

要求建立安全相应的关联

对原有数据包进行相应的安全处理

通过IKE建立安全关联，产生或者刷新密钥

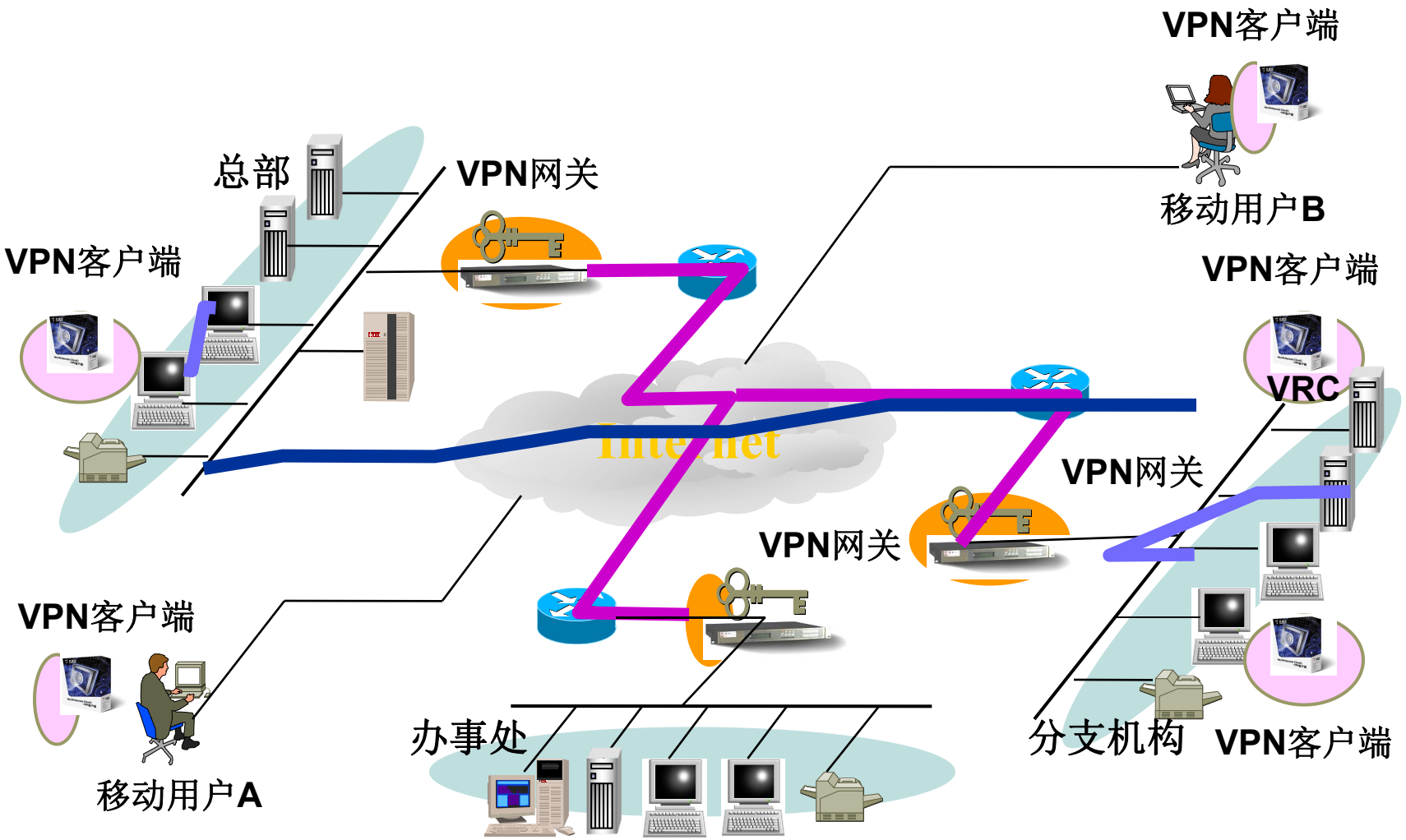
VPN网关A

VPN网关B

AH头 | ESP头 | 内IP头 | 负 载 | ESP尾

Internet

VPN的部署


VPN客户端
移动用户B
总部
VPN网关
VPN客户端
VPN客户端
VRC
Internet
VPN网关
VPN网关
VPN客户端
办事处
分支机构
VPN客户端
移动用户A