志存高远 责任为先

第9章 IP安全

地址：赣州市红旗大道86号 信息工程学院
网址：www.jxust.edu.cn
邮编：341000

目录/Contents

01
Part

IPSec简介

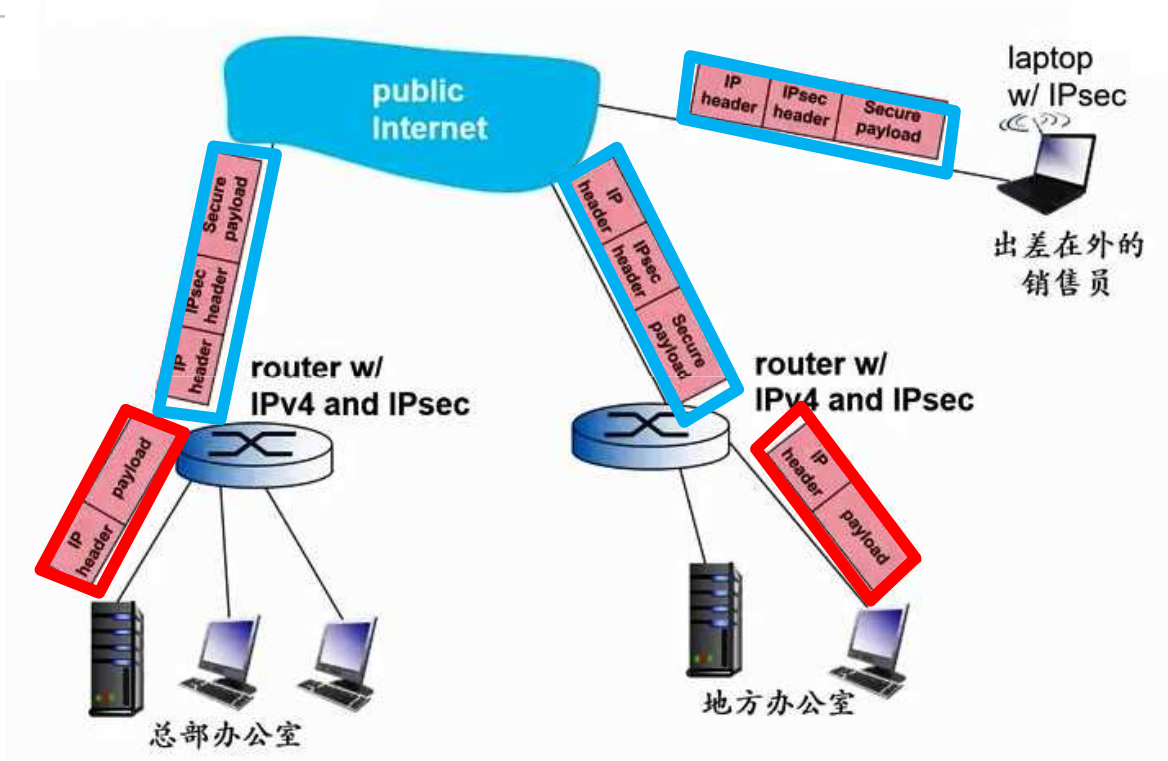
网络层机密性指什么？

- **对两个网络层设备（比如：路由器）**
- **发出方对网络层数据报（datagram)加密，这些被加密的内容可能是：**
  - **TCP or UDP协议包**
  - **ICMP协议信息**
  - **OSPF协议信息**
- **所有从一个网络设备发到另一个网络设备的数据必须被保护起来，不让攻击者随意获得**
  - **类比：将数据用一层“毯子”保护起来**

Virtual Private Network

- **为什么需要VPN**
  - **学校、公司、企业等单位需要自己的区域性私有网络来更好的保证信息及数据的安全性**
- **VPN的概念**
  - **一个单位办公室之间的网络信息流通过已有的因特网进行传输**
  - **但在数据发入到因特网之前进行加密**
  - **从逻辑上区分公有的因特网数据和单位内部的私密数据**

VPN(续)


public
Internet
laptop
w/ IPsec
IP header
IPsec header
Secure payload
出差在外的
销售员
router w/
IPv4 and IPsec
router w/
IPv4 and IPsec
payload
总部办公室
地方办公室

IPSec协议所提供的服务

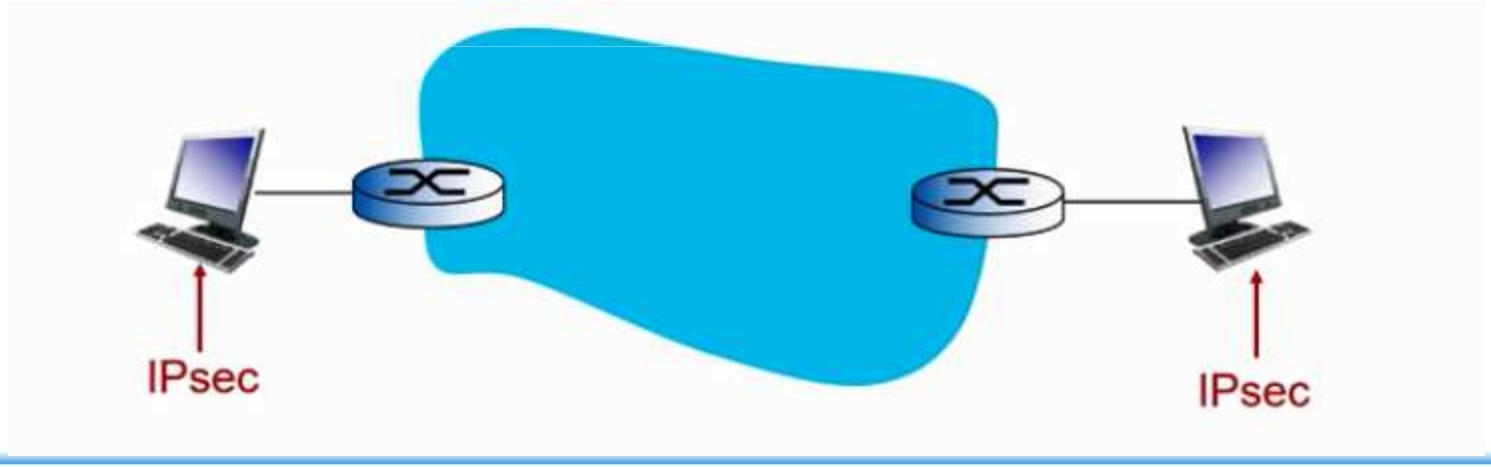
- **IPsec协议所提供的服务要求**
  - **数据完整性（data integrity)**
  - **发出方认证（origin authentication)**
  - **防范录播（重放）攻击（replay attack prevention)**
  - **信息隐秘性（message confidentiality)**
- **两种不同的协议可供选择**
  - **AH: Authentication Header**
  - **ESP: Encapsulation Security Protocol**

两种IPsec协议

- **Authentication Header (AH) protocol-鉴定文件头协议**
  - **对信息做发出方身份认证(authentication)，以及数据完整性(data integrity)检查，但不 提供保密性（ confidentiality)**
- **Encapsulation Security Protocol (ESP)-封装安全协议**
  - **对信息做发出方身份认证、数据完整性检查、并提供保密措施**
  - **应用更加广泛**

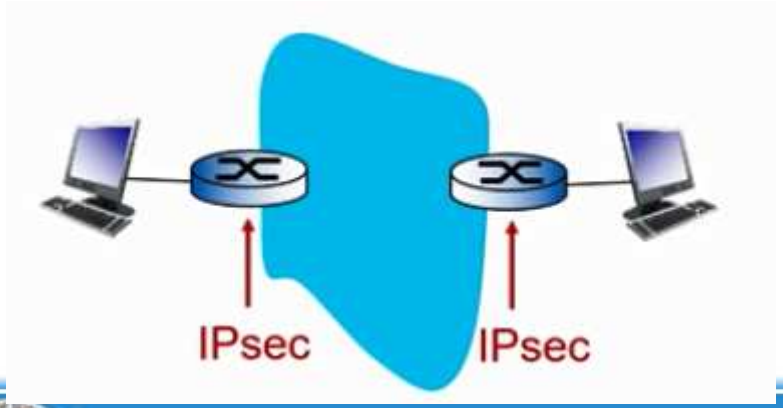
IPsec终端传输模式（transfer mode)

- **IPsec数据报（datagram)被连接的网络设备两个终端进行处理**
  - **为上层协议提供保护**
  - **在IP报文头和高层协议之间插入AH或ESP域**

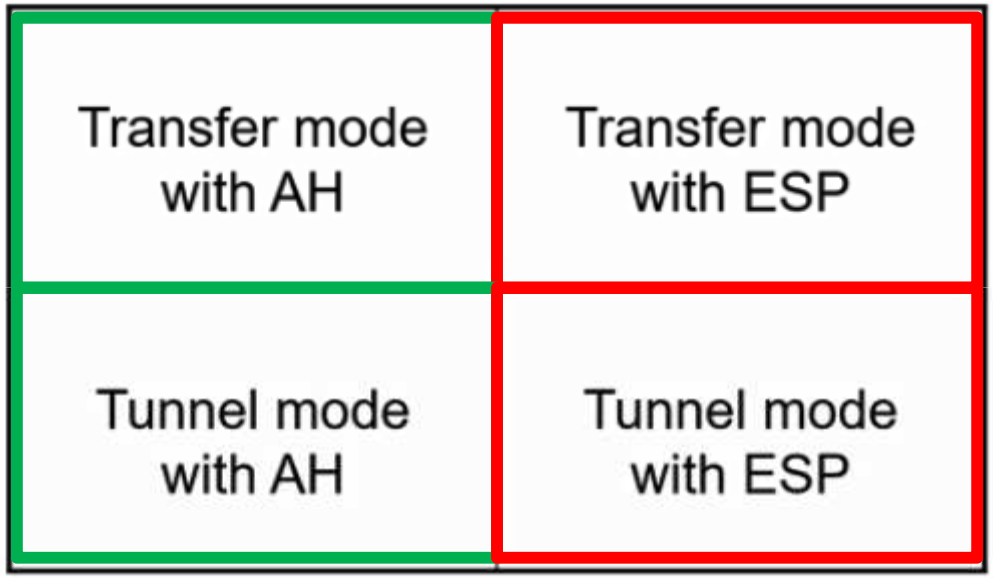


IPSec隧道模式（tunneling mode)

- **边界路由器安装IPsec**
- **终端同时也可以运行Ipsec**
  - **对整个IP包提供保护**
  - **把AH或ESP域添加到IP包中后，整个包在“隧道”上传输（增加新IP报文头）**



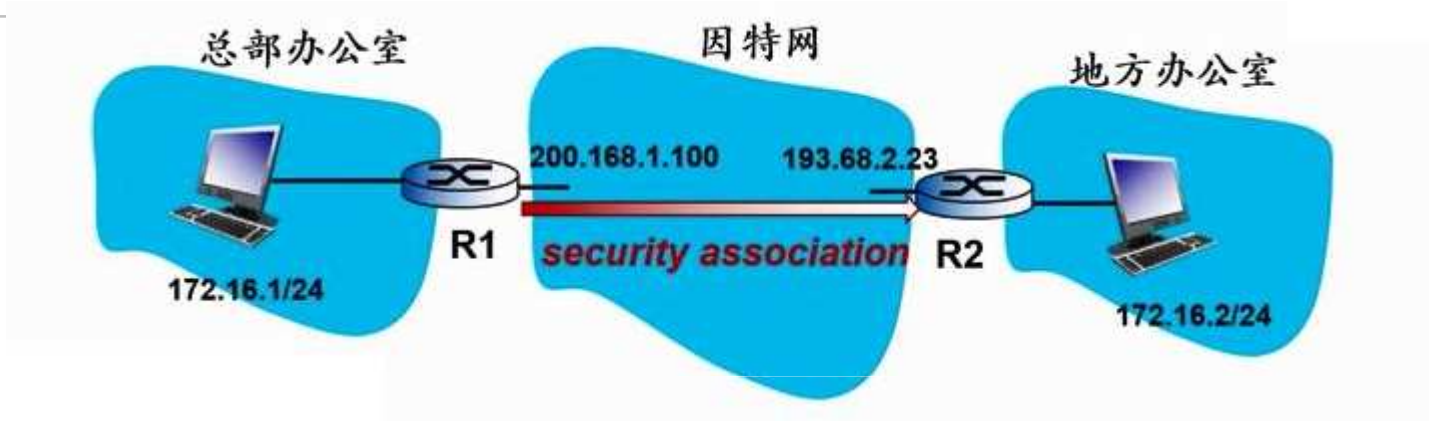
四种可能的协议及模式组合



安全联盟（security association — SA)

- **在发送数据之前，从发出端到接收端建立安全联盟（security association — SA)**
  - **安全联盟是单行的（simplex):由一方向另一方提出，非双向**
- **发出方和接受方分别保存和更新对SA的连接状态的信息（state information)**
  - **类似于:TCP连接两端的终端处理器保持TCP的连接状态信息（如：数据窗大小，序列号等等)**
  - **IP本身是无状态（connectionless)协议;但IPsec是保持状态信息（connection-orientcd)协议**
- **在总部办公室、地方办公室、n个出差人员之间的VPN里要建立多少个SA?**

例子：R1向R2建立SA



- ①32-bit identifier: Security Parameter Index (SPI)
- ②origin SA interface (200.168.1.100)
- ③destination SA interface (193.68.2.23)
- ④type of encryption used (e.g. : 3DES with CBC)
- ⑤encryption key
- ⑥type of integrity check used (e.g., : MD5 with HMAC)
- ⑦authentication key

security association实例

- **acl number 3001**
  - **rule 5 permit ip source 10.0.1.0 0.0.0.255 destination 10.0.3.0 0.0.0.255**
- **ipsec proposal trans1**
  - **esp authentication-algorithm sha1**
  - **esp encryption-algorithm 3des**

security association实例

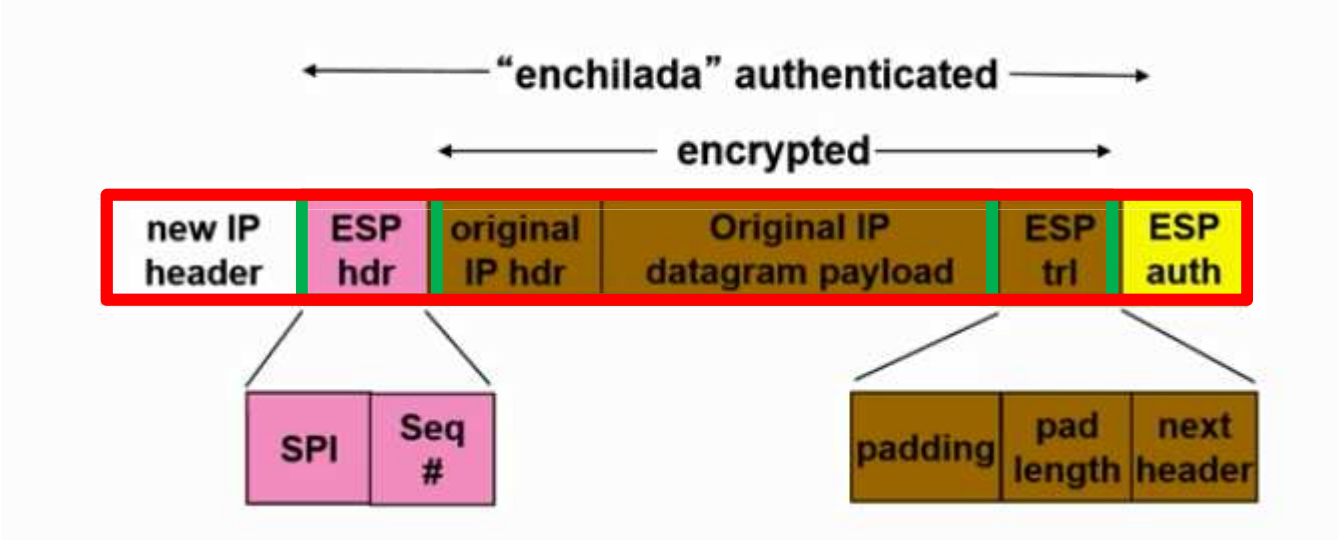
- **ipsec policy p1 10 manual**
  - **security acl 3001**
  - **proposal trans1**
  - **tunnel local 10.0.12.1**
  - **tunnel remote 10.0.23.3**
  - **sa spi inbound esp 12345**
  - **sa string-key inbound esp simple jxust**
  - **sa spi outbound esp 54321**
  - **sa string-key outbound esp simple jxust**

安全联盟数据库security association database (SAD)

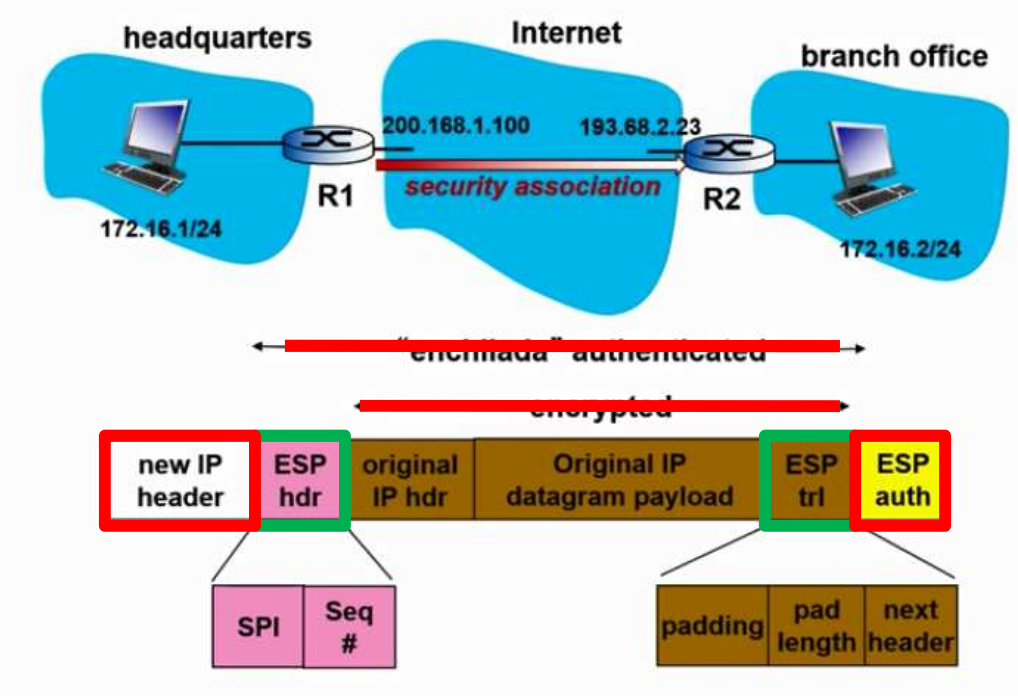
- **网络终端在安全联盟数据库security association database (SAD)中保存SA的状态息，并在需要用到此信息时到SAD中查找对n个出差的销售人员**
- **R1需要在SAD里存2 + 2n SAs**
- **当IPsec要传数据报的时候，R1查询SAD以决定如何处理数据报**
- **当IPsec的数据报抵达R2，R2对IPsec数据报中的SPI进行检查，将其在SAD中检索，并对相应的数据报进行处理**

IPSec数据报格式

- **以tunnel mode with ESP为例**



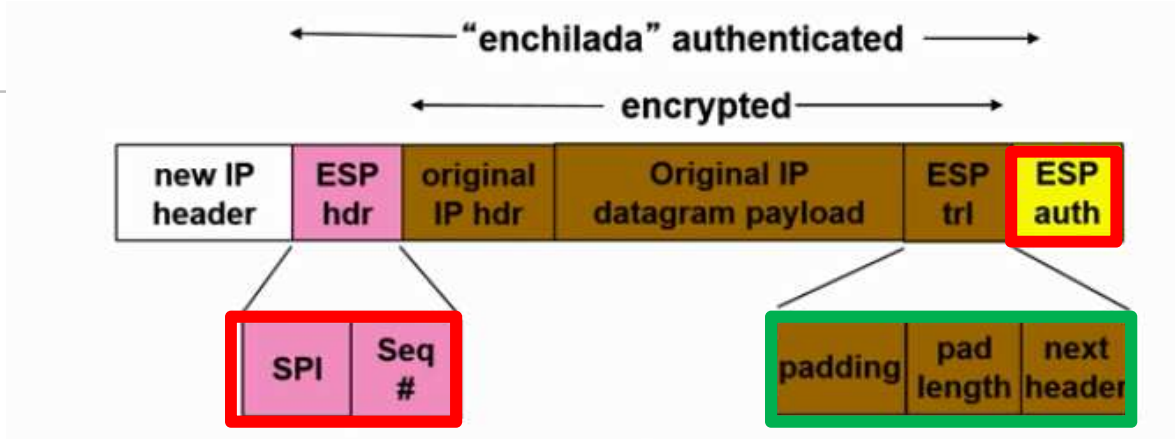
IPSec数据报生成过程



R1:将原来的普通网络数据报变成IPSec数据报

- 1把一个“ESP trailer"数据域接到原来普通数据报（包括原来数据报报头）的尾端
- 2用SA中设置好的编码算法和密钥将1.中的新数据报加密
- 3把“ESP header”加到2.中加密好的数据段之前形成一个“enchilada”
- 4用SA中设置好的算法和密钥对3.中生成的enchilada计算信息认证码（MAC)
- 5把4•中生成的MAC加到enchilada的后面，形成新的数据报的“上层数据段”(payload)
- 6创建一个全新的IP数据报报头，（含所有普通IPv4的规定数据域），将此报头加到5.中生成的payload之前

Enchilada的内容



- **ESP trailer: Padding为区块加密而设**
- **ESP header:**
  - **SPI,接收方可以进行相应SA管理**
  - **Sequence number,防止录播（重放）攻击**
- **MAC in ESP auth 由一个共享密信(shared secret)生成**

IPsec序列号

- 对一个新的SA，发出方初始设置序列号为0
- 每次有数据报通过SA传输时：
  - 发出方将相应序列号加1
  - 并把新的序列号放入报头中的序列号域
- 目的：
  - 防止攻击者通过监听进行录播（重放）攻击
  - 当重复接收到相同序列号的数据报时，可以判断将多余的数据报忽略以减小对服务器 资源的损耗
- 方法：
  - 接收方做“重复序列号”的检查
  - 并不记录“所有”收到的数据报，而是对一个“窗口”中的数据报进行检查

安全规则数据库（Security Policy Database-SPD)

- **规则规定**
  - **对于一个网络层数据报，发出方需要知道它是否要用IPSec**
  - **并同时需要知道用哪个SA**
    - **may use: source and destination IP address; protocol number**
- **SPD里的信息规定当收到一个网络层数据报时做些什么以及怎么做**
- **acl number 3001**
  - **rule 5 permit ip source 10.0.1.0 0.0.0.255 destination 10.0.3.0 0.0.0.255**

IPsec安全吗？

- **假设Trudy站在R1和R2中间，并且不知道任何这个连接的密钥，Trudy**
  - **可以看到原来数据报的内容吗？**

  比如收发方的IP地址，传输层的协议是什么，以及应用端口数（port number)
  - **可以把比特位的二维码黑白颠倒吗？**
  - **可以用R1的IP地址伪装成R1吗？**

IPsec IKE (Internet Key Exchange)协议

- **继续之前的例子：人工在IPsec的终端服务器上创建IPsecSA**

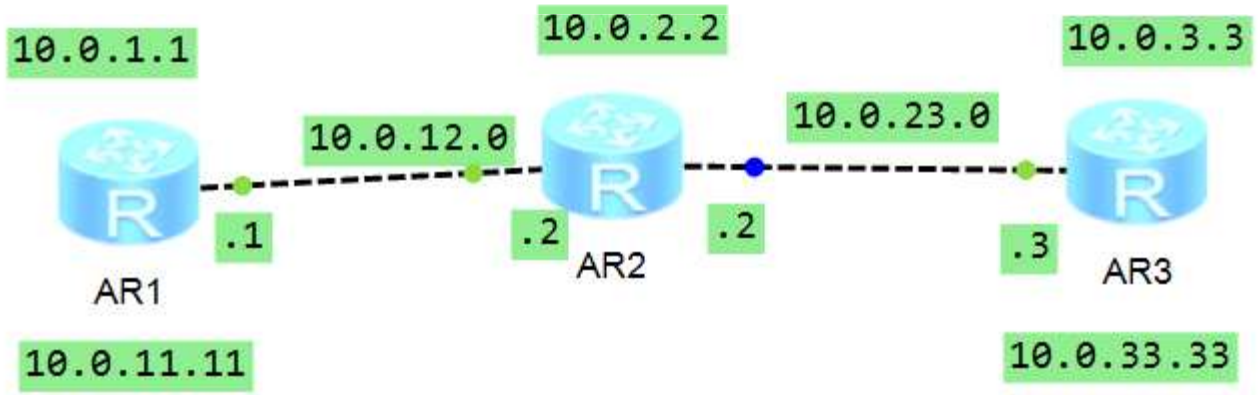
  Example SA
  - **SPI: 12345**
  - **Source IP: 200.168.1.100 Dest IP: 193.68.2.23 Protocol: ESP**
  - **Encryption algorithm: 3DES-cbc**
  - **HMAC algorithm: MD5 Encryption**
  - **key: 0x7aeaca-*-**
  - **HMAC key: 0xc0291f”**
- **但上述的人工设置过程对一个拥有100甚至几百以上的终端节点的VPN 是不适用的**
  - **由此，相应的采用IPsec IKE (Internet Key Exchange)协议**

IPsec总结

- IKE (ISAKMP)对加密算法、密钥、SPI值进行信息交换、协调
- 两种可选择的通讯协议AH或ESP(或两种都有）
  - AH提供信息完整性（integrity)、发出方身份认证（source authentication)
  - ESP (with AH)除了integrity和authentication，还提供信息的隐秘性保护（confidentiality)
- IPsec的通讯双方可以是两个网络终端（end systems)、一对路由器/防火墙、 或者是一个网络终端和一个路由器的组合

IPSec配置实验

- **企业总部的边缘路由器（R1）和分支机构路由器（R3）之间部署IPSec VPN解决方案**
  - **建立IPSec隧道，用于安全传输来自指定部门的数据流**



配置步骤

- **步骤1：基本接口配置**
- **步骤2：配置OSPF路由**
- **步骤3：配置ACL 定义感兴趣流**
  - **[R1]acl 3001**
  - **[R1-acl-adv-3001]rule 5 permit ip source 10.0.1.0 0.0.0.255 destination 10.0.3.0 0.0.0.255**

配置步骤

- **步骤4：配置IPSec VPN 提议**
  - **[R1]ipsec proposal tran1**
  - **[R1-ipsec-proposal-tran1]esp authentication-algorithm sha1**
  - **[R1-ipsec-proposal-tran1]esp encryption-algorithm 3des**

```
[R1]display ipsec proposal
Number of proposals: 1
IPSec proposal name :   tran1
 Encapsulation mode :   Tunnel
 Transform          :   esp-new
 ESP protocol       :   Authentication SHA1-HMAC-96
                        Encryption     3DES
```

配置步骤

- **步骤5：创建IPSec 策略**

```
[Huawei]dis ipsec policy

==========================================
IPSec policy group: "p1"
Using interface: Serial4/0/0
==========================================

    Sequence number: 10
    Security data flow: 3001
    Tunnel local  address: 10.0.12.1
    Tunnel remote address: 10.0.23.3
    Qos pre-classify: Disable
    Proposal name:trans1
    Inbound AH setting:
      AH SPI:
      AH string-key:
      AH authentication hex key:
    Inbound ESP setting:
      ESP SPI: 12345 (0x3039)
      ESP string-key: jxust
      ESP encryption hex key:
      ESP authentication hex key:
    Outbound AH setting:
      AH SPI:
      AH string-key:
      AH authentication hex key:
    Outbound ESP setting:
      ESP SPI: 54321 (0xd431)
      ESP string-key: jxust
      ESP encryption hex key:
      ESP authentication hex key:
```

配置步骤

- **步骤6：在接口下应用IPSec 策略**
  - **[R1]interface Serial 1/0/0**
  - **[R1-Serial1/0/0]ipsec policy P1**

检查结果

- **验证设备对不感兴趣流量不进行IPSec加密处理**
  - **<R1>ping -a 10.0.11.11 10.0.33.33**

```
<R1>display ipsec statistics esp
 Inpacket count                : 0
 Inpacket auth count           : 0
 Inpacket decap count          : 0
 Outpacket count               : 0
```

检查结果

- **验证设备将对感兴趣流量进行IPSec加密处理**
  - **<R1>ping -a 10.0.1.1 10.0.3.3**

```
<R1>display ipsec statistics esp

Inpacket count                : 5

Inpacket auth count           : 0
```

```
 5 9.219000   10.0.23.
 6 11.310000  10.0.12.
 7 11.341000  10.0.23.
 8 12.012000  10.0.12.
 9 12.059000  10.0.23.
10 12.729000  10.0.12.
11 12.745000  10.0.23.
12 13.556000  10.0.12.
13 13.587000  10.0.23.
14 14.399000  10.0.12.
15 14.414000  10.0.23.
```

```
⊞ Frame 8: 140 bytes on wire (1120 bits), 140 bytes captured (1120 bits)
⊞ Point-to-Point Protocol
⊞ Internet Protocol, Src: 10.0.12.1 (10.0.12.1), Dst: 10.0.23.3 (10.0.23.3)
⊟ Encapsulating Security Payload
    ESP SPI: 0x0000d431
    ESP Sequence: 369098752
```

```
0000  ff 03 00 21 45 00 00 88  00 16 00 00 fe 32 85 2a   ...!E... .....2.*
0010  0a 00 0c 01 0a 00 17 03  00 00 d4 31 16 00 00 00   ........ ...1....
0020  c5 54 dd 3c b0 59 f2 29  45 00 00 54 01 d1 00 00   .T.<.Y.) E..T....
0030  ff 01 a1 d4 0a 00 01 01  0a 00 03 03 08 00 f9 da   ........ ........
0040  d3 ab 02 00 cc 9d 40 00  00 00 00 00 50 49 4e 00   ......@. ....PIN.
0050  00 00 00 00 00 01 02 03  04 05 06 07 08 09 0a 0b   ........ ........
0060  0c 0d 0e 0f 10 11 12 13  14 15 16 17 18 19 1a 1b   ........ ........
0070  1c 1d 1e 1f 20 21 22 23  24 25 26 27 01 02 02 04   .... !"# $%&'....
0080  14 15 16 17 18 19 1a 1b  1c 1d 1e 1f               ........ ....
```

02
Part

IP安全概述

第9章 IP安全 (IP Security)

- **IP层的安全包含三个方面**
- **1. 认证**
  - **认证机制保证接收到的包是报头标识指出的源端实体发出的。保证包在传输过程中没有被篡改。**
- **2. 保密**
  - **对消息加密，防止第三方窃听。**
- **3. 密钥管理**
  - **与密钥交换有关**

9.1 IP安全概述

- 可以在Internet上的任何层次实现安全机制，各层机制有不同的特点
- 问题：用户的一些安全要求跨越多个协议层；此外，有的应用程序有安全机制，有的则没有。
- 在TCP/IP协议分层模型中，IP层是可能实现端到端安全通信的最底层。通过在IP层上实现安全性，不仅可以保护各种带安全机制的应用程序，而且可以保护许多无安全机制的应用。
- IP级安全性包括三个方面的内容：认证、保密和密钥管理

9.1 IPSec概述（续）

- 互联网工程任务组(IETF)于1998年11颁布了一套开放标准网络安全协议：IP层安全标准IPSec (IP Security)
- IPSec将密码技术应用在网络层，提供端对端通信数据的私有性、完整性、真实性和防重放攻击等安全服务
- IPSec对于IPv4是可选的，对于IPv6是强制性的

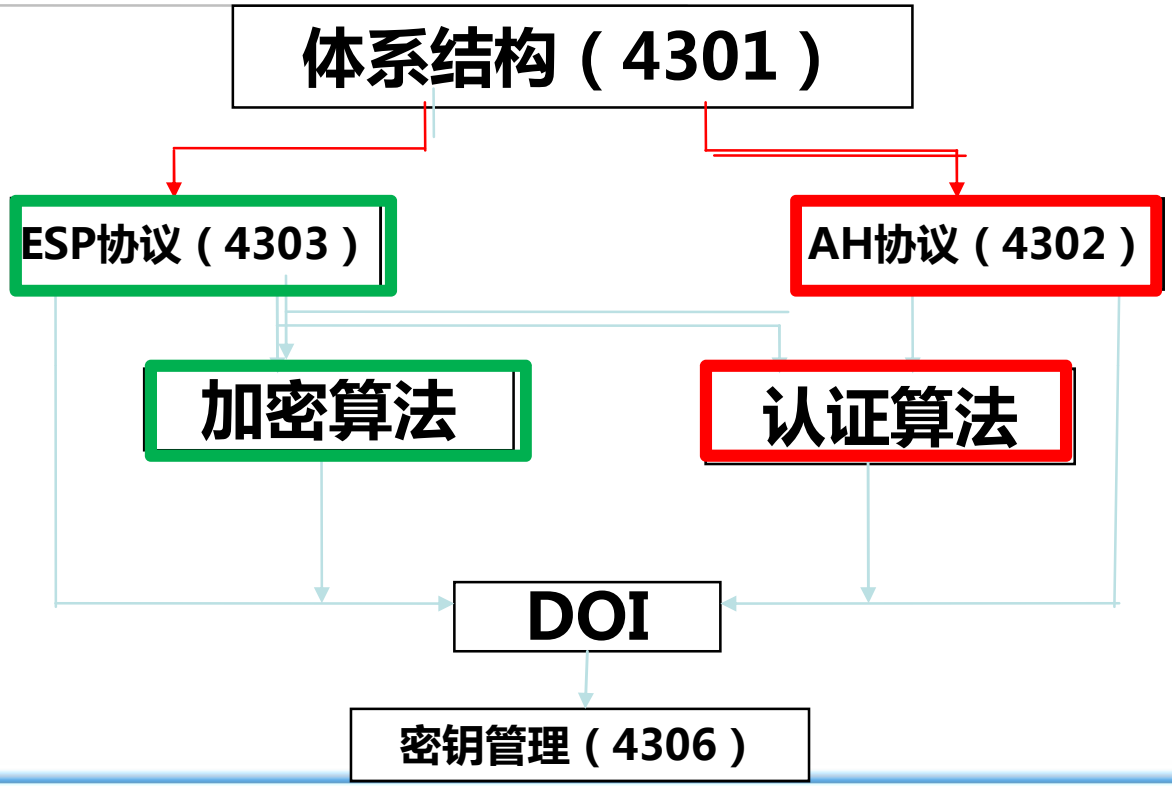
1. IPSec工作组

- IETF：IP Security Protocol Working Group
  - Architecture（体系结构）
  - Encapsulating Security Payload(ESP)（封装安全负载）
  - Authentication Header (AH)（身份验证标头）
  - Encryption Algorithm（加密算法）
  - Authentication Algorithm（认证算法）
  - Key Management（密钥管理）
  - Domain of Interpretation(DOI)（解释领域）

2. IPSec特点

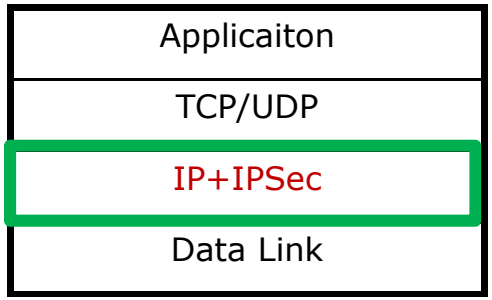
- **在操作系统内部实现安全功能，在不需要修改应用程序的前提下，为多个应用提供安全保护。**
- **IPSec独立于鉴别和加密算法，在一个基本框架上可使用不同的鉴别和加密模块以满足不同的安全需要**
- **IPSec实现在传输层以下，因此对于应用程序和用户都是透明的。**

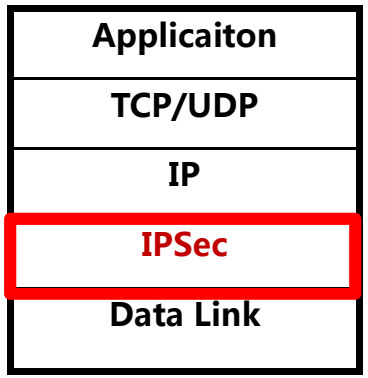
3. IPSec框架



4. IPSec协议的实现

- **OS集成**
  - IPSec集成在操作系统内，作为IP层的一部分
  - 具有较高的效率
  - IPSec安全服务与IP层的功能紧密集合在一块
- **嵌入到现有协议栈**
  - IPSec作为插件嵌入到链路层和IP层之间
  - 较高的灵活性
  - 效率受到影响





5. IPSec的部署 - 1

- 可配置和实施IPSec的端点包括主机、路由器、防火墙等
- 在终端主机上部署IPSec
  - 提供端到端的安全保障，保护终端之间的IP分组
  - 可以支持逐个数据流的安全保障
  - 能够支持IPSec定义的各种工作模式

5. IPSec的部署 - 2

- 在网络节点（路由器或防火墙）上实施IPSec
- 对通过公用网的子网间通信提供保护
- 对内部网的用户透明
  - 能同时实现对进入专用网络的用户进行身份认证和授权
  - 缺点：网络节点开销大

6. IPSec的工作模式

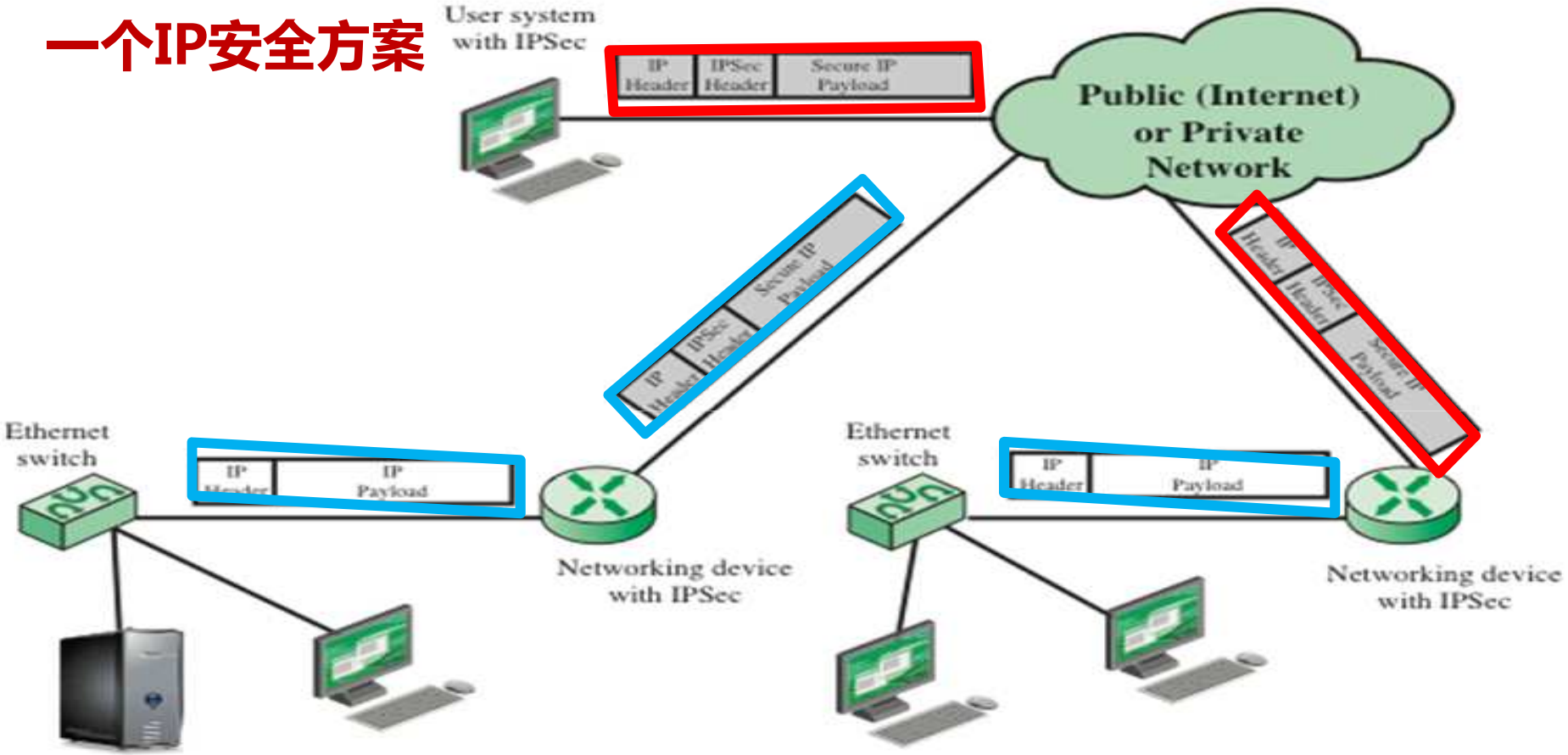
- 在IPSec中，AH/ESP协议用于保护IP分组
- 对IP分组的保护有两种方式
  - 保护IP分组的净荷（高层协议的数据）
  - 保护整个IP分组
- 保护的方式由工作模式决定
  - 传输模式：保护IP的上层协议
  - 隧道模式：保护整个IP分组

9.1.1 IPSec的应用

◆ **IPsec**提供了保护**LAN**，私有和公共**WAN**以及**Internet**之间通信的功能。

◆ **IPsec的主要特征是它可以加密和/或验证IP级别的所有流量. 因此，可以保护所有分布式应用程序（远程登录，客户端/服务器，电子邮件，文件传输，Web访问）**

一个IP安全方案


User system with IPSec
IP Header
IPSec Header
Secure IP Payload
Public (Internet) or Private Network
Ethernet switch
IP Header
IP Payload
Networking device with IPSec
Ethernet switch
IP Header
IP Payload
Networking device with IPSec

9.1.2 IPSec的好处

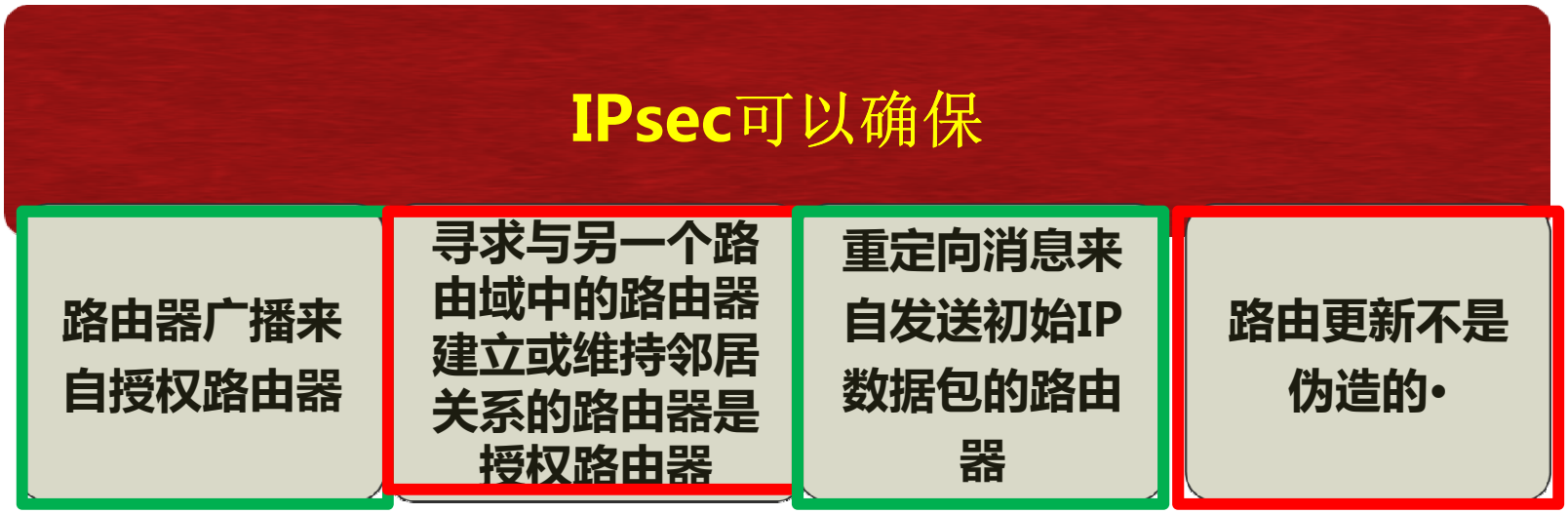
- 当IPsec在防火墙或路由器中实施时，它对通过边界的所有流量提供了强大的安全性。
  - 公司或工作组内的流量不会产生与安全相关的处理的开销。
- 如果来自外部的所有流量必须使用IP并且防火墙是从Internet进入组织的唯一手段，则防火墙中的IPsec可以抵抗旁路。
- IPsec低于传输层（TCP，UDP），因此对所有 的应用程序是透明的。
  - 在防火墙或路由器中实施IPsec时，无需更改用户或服务器系统上的软件。

9.1.2 IPSec的好处（续）

- **IPsec对最终用户可以是透明的**
  - **无需培训用户安全机制，基于每个用户发布密钥材料，或在用户离开组织时撤销密钥材料。**
- **如果需要，IPsec可以为个人用户提供安全性**
  - **这对于非现场工作人员以及在组织内为敏感应用程序设置安全虚拟子网非常有用**

9.1.3 路由应用

- IPsec可以在网络互联所需的路由架构中发挥至关重要的作用



9.1.4 IPSec文档

- IPSec有许多文档，整个文档分为7部分
- 体系结构：包括总体概念，安全需求，定义，以及定义IPSec技术的机制；
- 封装安全载荷（ESP）：使用ESP进行加密的消息格式和一般性问题，以及可选的认证；
- 认证报头（AH）：使用认证消息格式和一般性问题；
- 加密算法：描述将各种不同加密算法用于ESP的文档；
- 认证算法：描述将各种不同加密算法用于AH以及ESP认证选项的文档；
- 密钥管理：描述密钥管理模式；
- DOI：其它相关文档，批准的加密和认证算法标识，以及运行参数等；

9.1.5 IPSec提供的服务

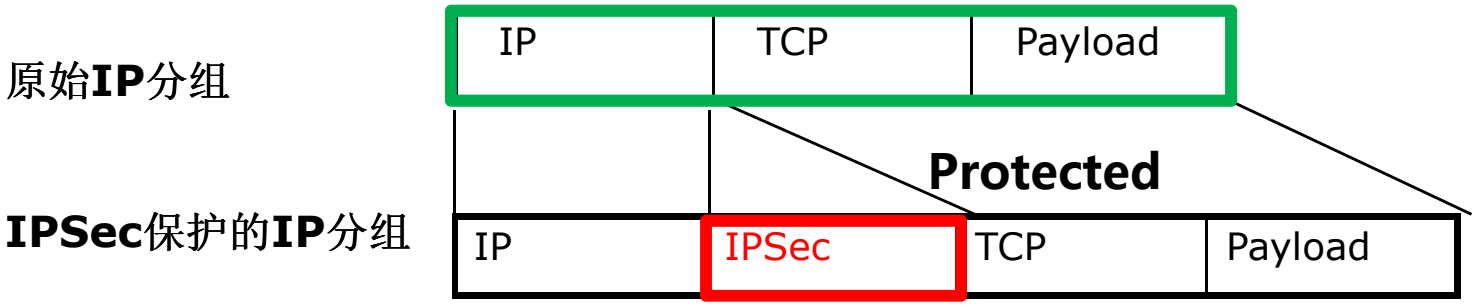
- 访问控制
- 数据完整性
- 数据源认证
- 重放攻击保护
- 数据保密性
- 密钥管理
- 有限通信流保密性

服务 \ 协议	AH	ESP 仅加密	ESP 加密、鉴别
访问控制	Y	Y	Y
数据完整性	Y		Y
数据源认证	Y		Y
重放攻击保护	Y	Y	Y
数据机密性		Y	Y
流量机密性		Y	Y

9.1.6 传输模式和隧道模式

◆ 传输模式

- **保护上层协议（TCP/UDP…）的数据（即增强对IP载荷的保护）**
- **安全操作（加密和认证）在通信终端上（主机）上进行**
- **提供端到端的保护**



隧道模式

- **在不安全信道上，保护整个IP分组**
- **安全操作在网络设备上完成**
  - **安全网关、路由器、防火墙……**

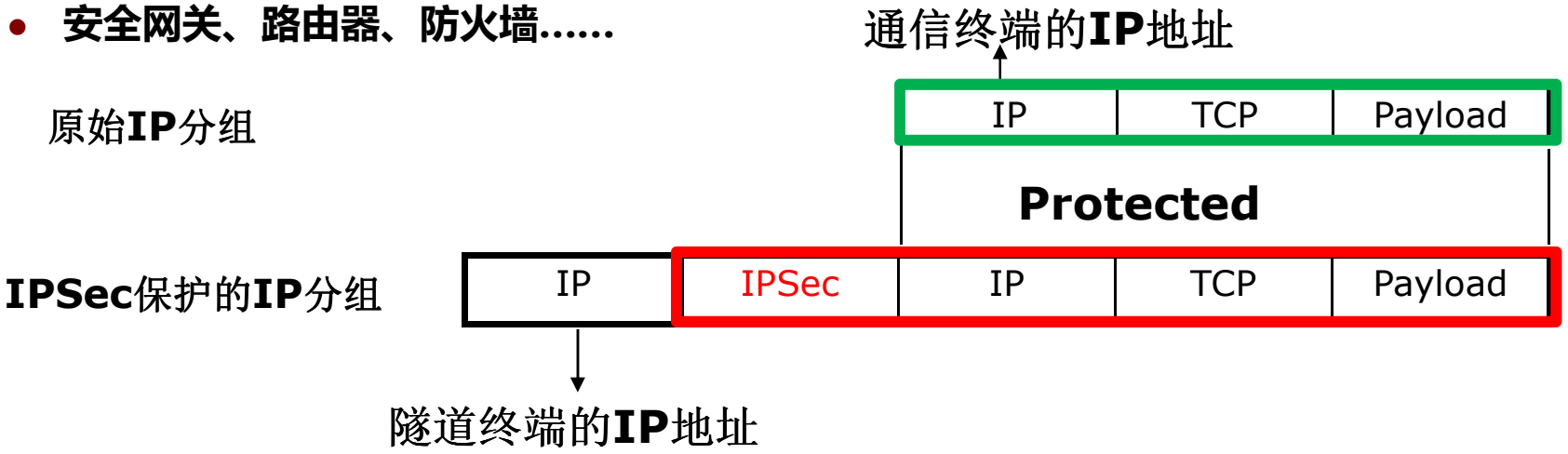


表9.1 传输模式和隧道模式的功能

	传输模式SA	隧道模式SA
AH	认证IP有效负载以及IP报头和IPv6扩展报头的选定部分。	认证整个内部IP数据包（内部标头加IP有效负载）以及外部IP报头和外部IPv6扩展报头的选定部分。
ESP	在ESP报头之后加密IP有效负载和任何IPv6扩展报头。	加密整个内部IP数据包。
带认证的ESP	在ESP报头之后加密IP有效负载和任何IPv6扩展报头。认证IP有效负载但不认证IP头。	加密整个内部IP数据包。 认证内部IP数据包。

03
Part

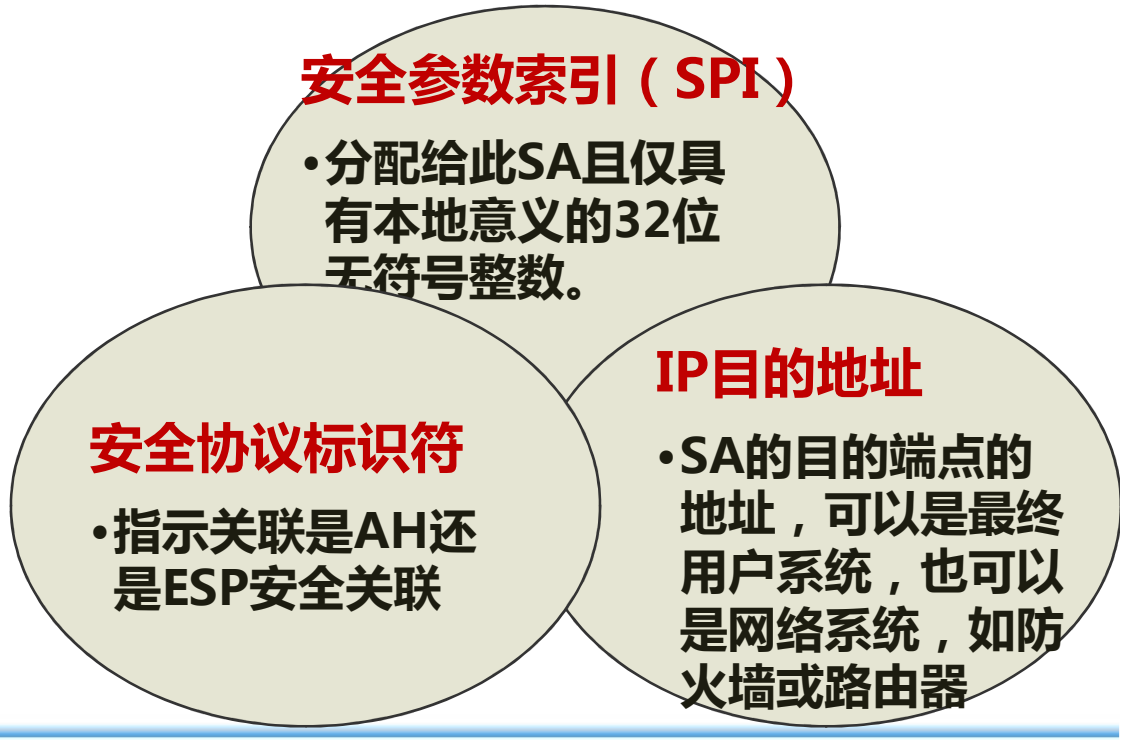
IP安全策略

9.2 IP安全策略

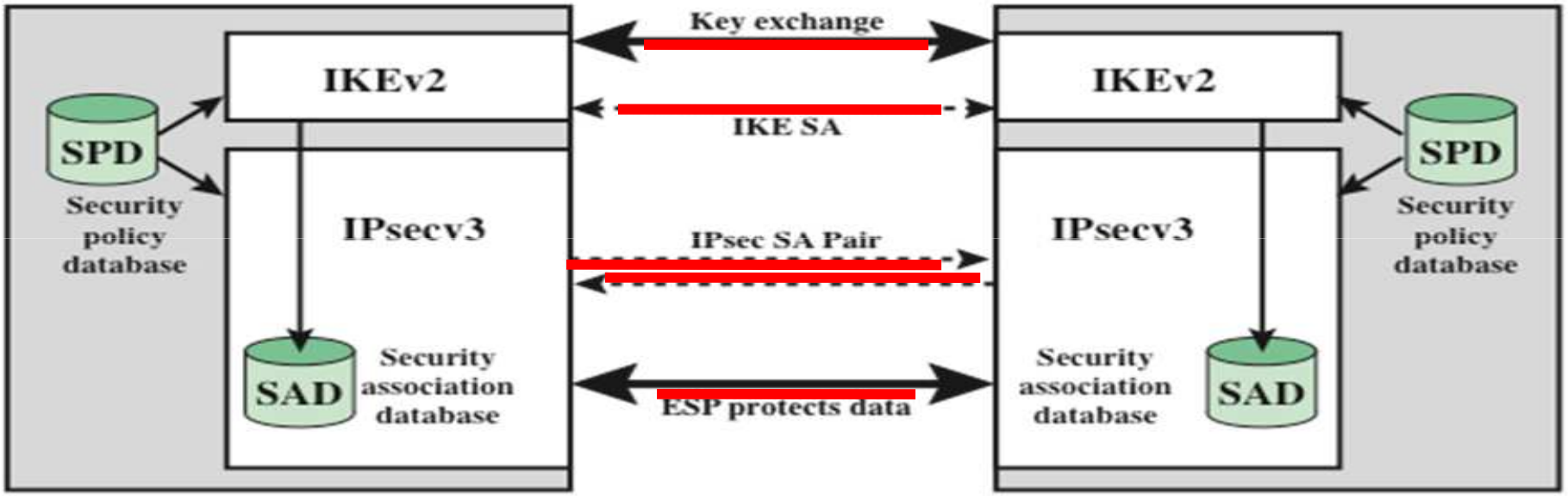
- **IPSec操作的基础**是应用于每个由源地址到目的地址传输中IP包安全策略的概念
- **IPSec安全策略本质上**由两个交互的数据库，**安全关联数据库（SAD）**和**安全策略数据库（SPD）**确定

9.2 IP安全策略（续）

- 安全关联是发送方和接收方之间用于对它们传递的数据流提供安全服务的单向逻辑连接。
- 如果需要一个对等关系，即双向安全交换，则需要两个安全关联SA。

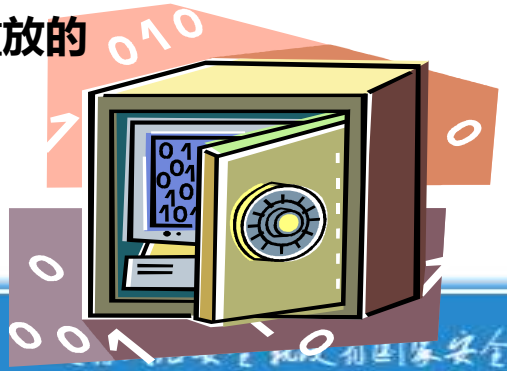


IP安全策略的体系结构



9.2.2 安全关联数据库（SAD）

- 定义与每个SA关联的参数
- 通常由SAD条目中的以下参数定义
  - 安全参数索引（SPI）：由SA接收端选定一个32比特数值。
  - 序号计数器：一个32比特的数值，它被用来生成AH和ESP报头的序列号域。
  - 序列计数器溢出：表明序列号计数器的溢出是否生成一个可审计并阻止在此SA上继续传输数据包。
  - 反重播窗口：用于判断内部的AH或者ESP数据包是否是重放的



9.2.2 安全关联数据库（SAD）

- **AH信息：**认证算法、密钥、密钥生成期和用于AH的相关参数。
- **ESP信息：**加密和认证算法、密钥、初始值、密钥生成期和用于ESP的相关参数。
- **此安全关联的生命周期：**一个时间间隔或字节计数。超过此值后，安全关联必须终止或被一个新的安全关联取代。
- **IPsec协议模式：**隧道模式、传输　模式或通配符模式。
- **最大传输单元路径MTU：**任何观察到的最大传输单元路径和迟滞变量

9.2.3 安全策略数据库（SPD）

- **IP流量与特定SA相关联的方法在名义上是安全策略数据库（SPD）。**
  - **一个SPD应该包括入口，每个入口都定义了一个IP流量子集并为该流量指向一个SA**
- **在更复杂的环境中，多个入口可以和一个SA相关或多个SA和一个SPD入口相关。**
  - **每个SPD入口由一个IP集和上层协议的域值定义，称为选择器。**
  - **这些选择器用于过滤传出流量以将其映射到特定SA**

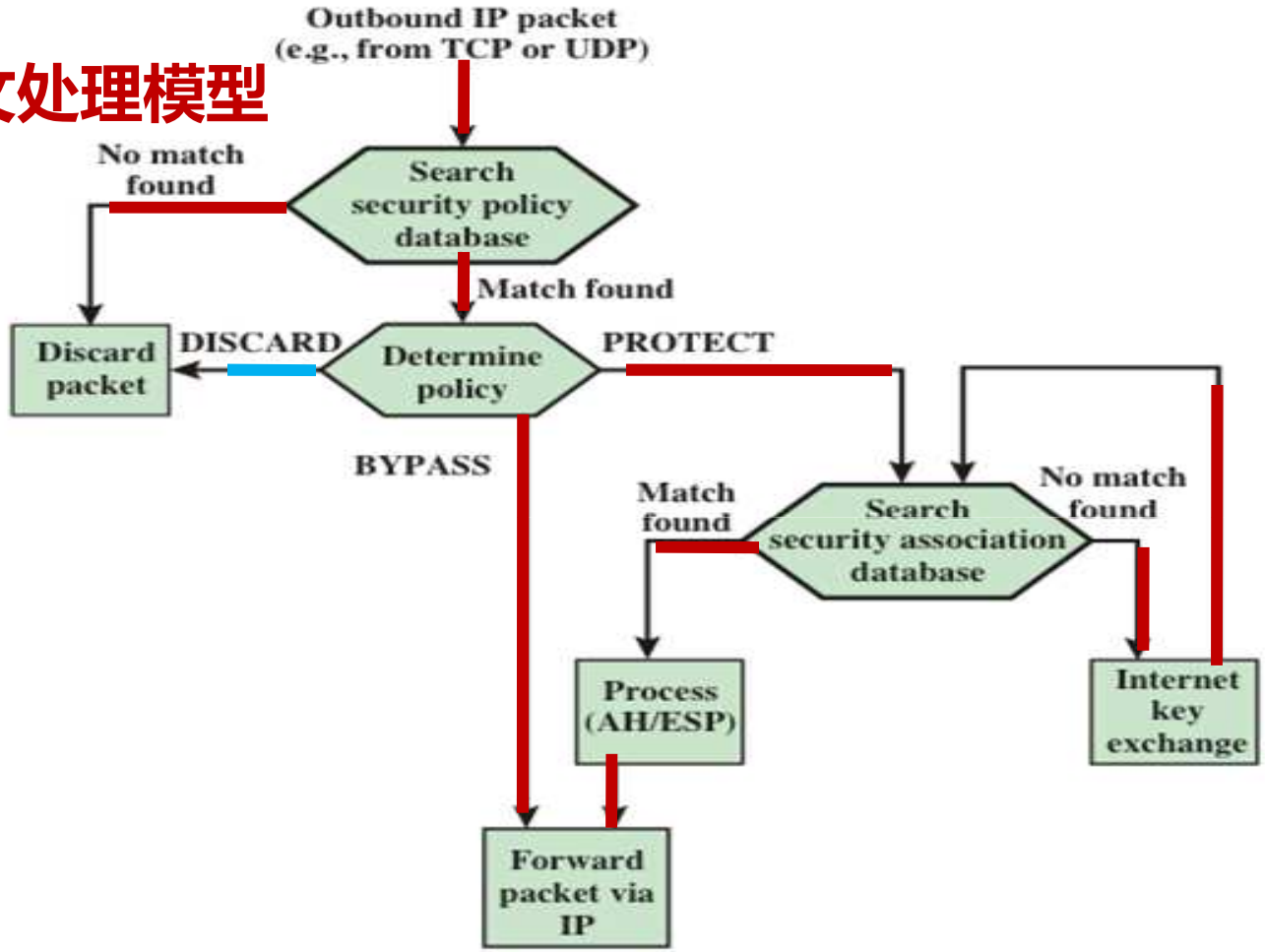
SPD入口


远程IP地址
这可以是单个IP地址，枚举列表或地址范围，或通配符（掩码）地址
后两者需要支持多个目标系统共享一个SA
本地IP地址
这可以是单个IP地址，枚举列表或地址范围，或通配符（掩码）地址
The latter two are required to support more than one source system sharing the
下层协议
IP协议头包括一个域，该域规定了IP层上的协议操作。
名称
来自操作系统的用户标识符
不是IP或上层报头中的字段，但如果IPsec与用户在同一操作系统上运行，则字段可获得。
本地和远程端口
这些可以是单独的TCP或UDP端口值，枚举的端口列表或通配符端口

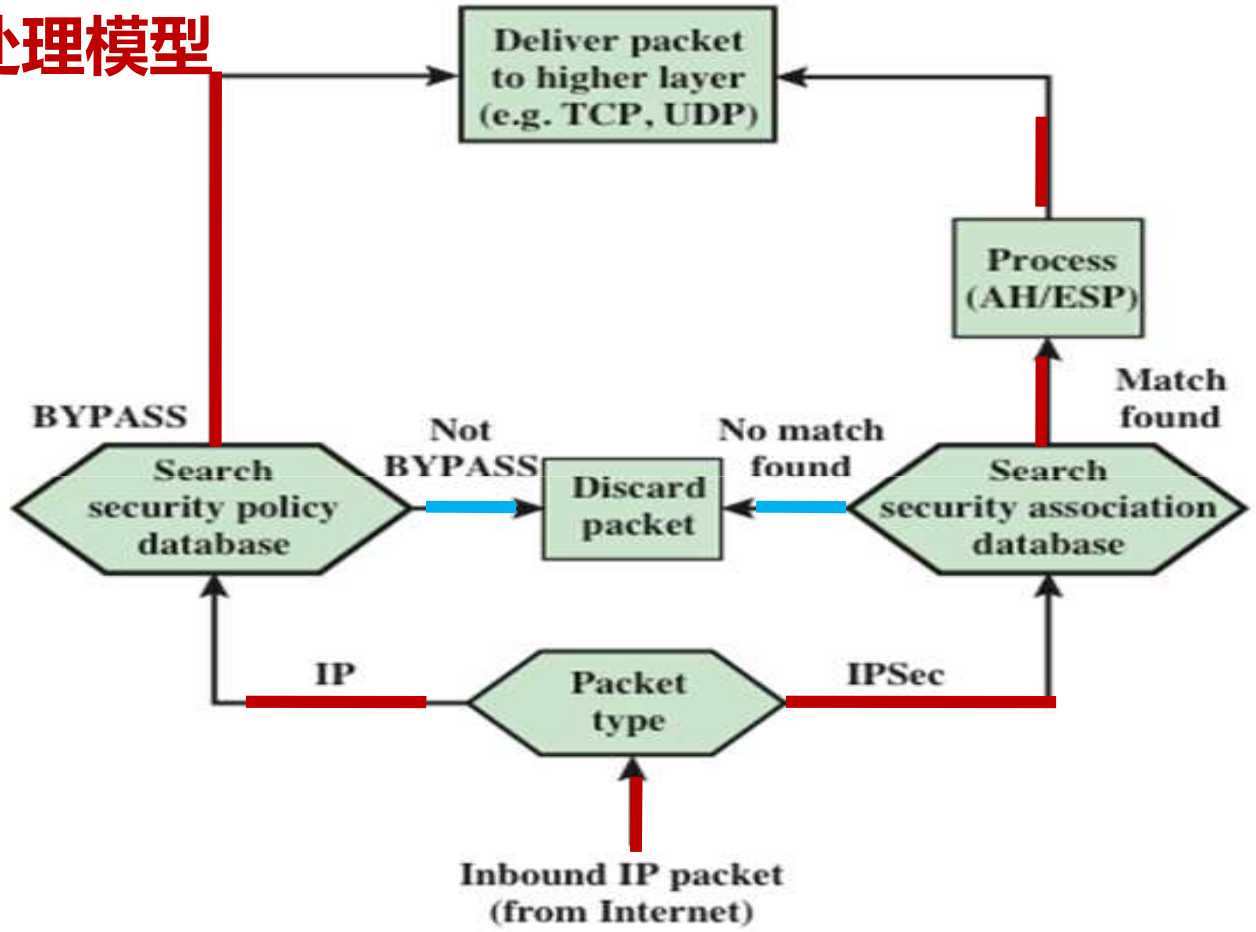
9.2.4 IP通信进程

- IPSec**是在报文到 报文的基础上执行的。当**IPSec**执行时，发往外部的**IP**包在传送之前经过**IPSec**逻辑的处理，而发往内部的**IP**包在接收之后并且发送报文内容到更高层之前（如**TCP**或**UDP）经过**IPSec**逻辑的处理。**
- **出站报文和入站报文的处理如图**9.3**和图**9.4**所示。**

出站报文处理模型


Outbound IP packet
(e.g., from TCP or UDP)
Search security policy database
No match found
Match found
Discard packet
DISCARD
Determine policy
PROTECT
BYPASS
Match found
Search security association database
No match found
Process (AH/ESP)
Internet key exchange
Forward packet via IP

入站报文处理模型


Deliver packet to higher layer (e.g. TCP, UDP)
Process (AH/ESP)
Match found
BYPASS
Not BYPASS
No match found
Search security policy database
Discard packet
Search security association database
IP
Packet type
IPSec
Inbound IP packet (from Internet)

04
Part

封装安全负载（ESP）

9. 3封装安全负载（ESP）

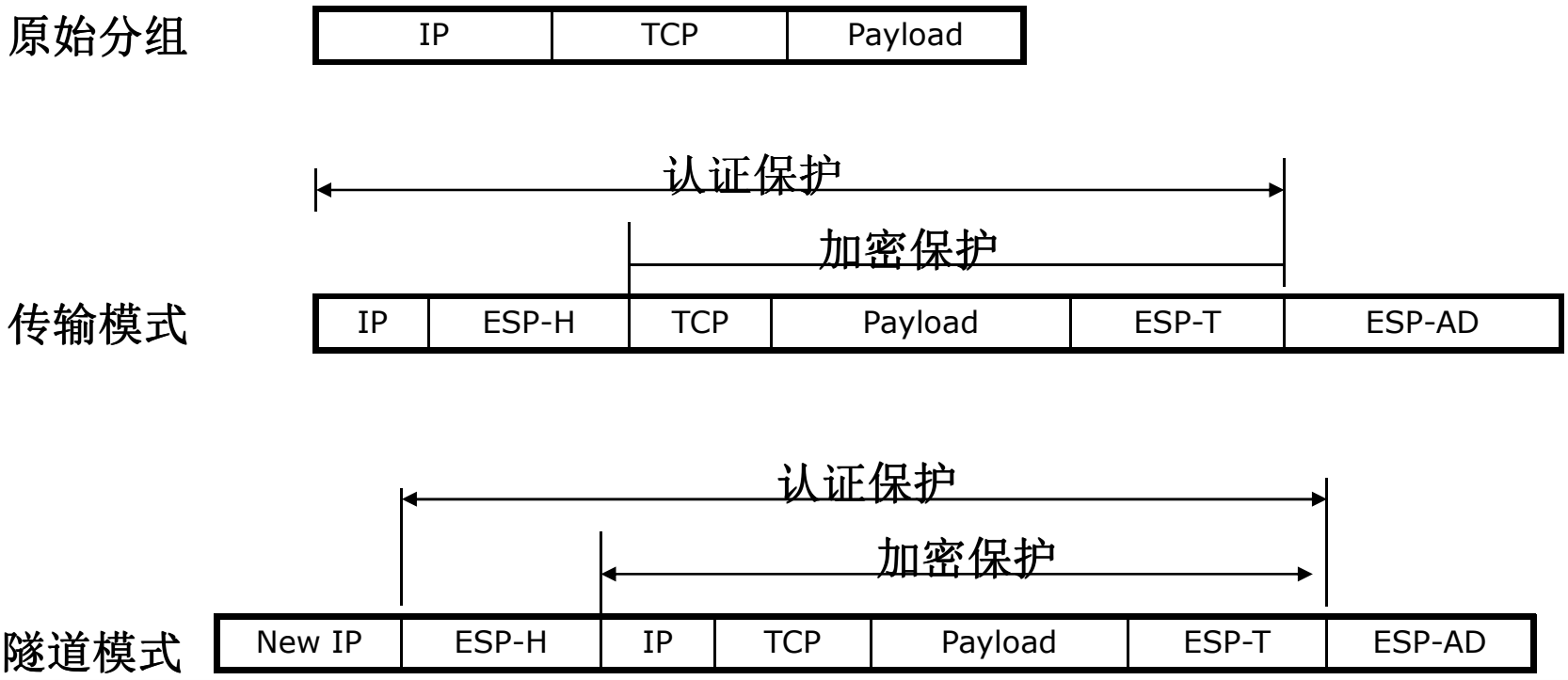
- ESP – Encapsulating Security Payload
  - 提供更高级别的安全保护
  - 数据源鉴别
  - 数据完整性
  - 数据内容保密性
  - 可选的重放保护
  - 有限的流量保密
- ESP支持的加密算法
  - 3DES、IDEA、RC5 ……
- 支持的鉴别算法
  - 与AH相同

9.3.1 ESP格式

SPI	SN	Payload (protected)	Pad	Pad Length	Next header	Authentication data

- **安全参数索引SPI**：标识与分组通信相关联的SA。
- **序列号SN**：单调递增的序列号，用来抵抗重放攻击。
- **净荷数据Payload**：被加密保护。
- **填充（PAD）与填充长度（ Pad Length ）**：被加密保护。
  - 通过填充使得ESP协议段的长度为32bits的整数倍。
  - 通过填充，隐藏了原始数据的长度，提供了有限的流量保密。
- **下一协议扩展头类型（ Next header ）**：被保护的数据的协议类型。
- **认证数据Authentication Data**：包含进行数据源认证的数据（MAC），即ICV。

9.3.2 ESP的安全保障 – IPv4



9.3.3 反重放服务

- 重放攻击是指攻击者得到一个经过认证的包后，后来将其传送到目的站点的行为。
- 序列号域就可以防止上述攻击。
- 当建立了一个新的SA时，发送方将序列号初值设为0，每次在SA上发送一个包，则计数器加l，将新值写入序列号域。
- 如果要求支持反重放(默认设置)，则发送方不允许循环计数。如果已经折返，则发送方要建立新的SA。

反重放服务

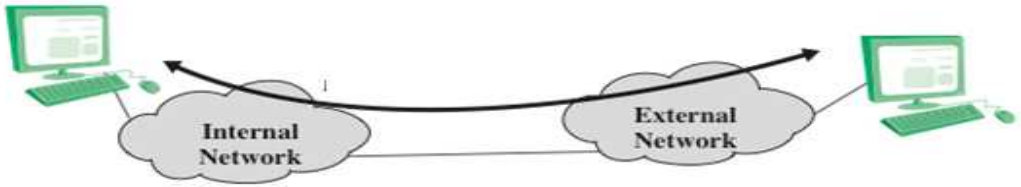
- 在每一个安全关联都维护一个防重放的滑动窗口，大小64，向右侧滑动
- 每个IPSec分组都被分配一个序列号
- 在接受方，满足以下条件的分组才是合法的：
  - 分组通过鉴别
  - 分组序号是新的，未在滑动窗口中出现过
  - 分组序号落在滑动窗口内或右侧
- 分组序号落在滑动窗口右侧，窗口向右滑动
- 通过这种机制，重放攻击的分组将被丢弃

9.3.4 传输模式和隧道模式

- 图9.7说明了可用于IPSec ESP服务的两种方式。
- 图9.7（a）在两个主机之间直接提供加密和认证（认证是可选）。
- 图9.7（b）说明了如何使用隧道模式建立虚拟专用网络。在这个例子中，一个组织有4个通过互联网相互连接的专用网络。

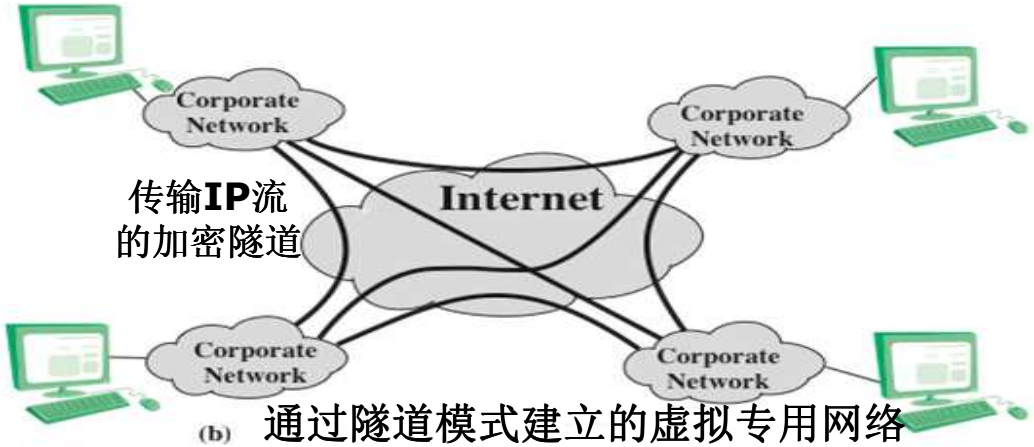
传输模式和隧道模式加密的比较

加密的
TCP会话



传输层安全

(a)



传输IP流
的加密隧道

(b) 通过隧道模式建立的虚拟专用网络

05
Part

安全关联组合

9.4 安全关联组合

- **单个SA可以实现AH或ESP协议，但不能同时实现两者。**
- **安全关联束**
  - **指的是提供特定的IPsec服务集所需的一个SA系列。**
  - **捆绑中的SA可以终止于不同的端点或同一端点。**
- **可以通过两种方式组合成安全关联束：**

运输邻接

- 指的是在不调用隧道的情况下将多个安全协议应用于同一IP数据包。
- 这种方法只允许一个级别的组合。

隧道迭代

- 指通过IP隧道实现多层安全协议的应用。
- 这种方法允许多级嵌套。

9.4.1 认证加保密

- 加密和认证可以组合起来以实现在主机之间传送同时需要保密和认证的IP包。
- 带认证选项的ESP
  - 在此方法中，第一个用户将ESP应用于要保护的数据，然后附加身份验证数据字段。

传输模式ESP

- 传送到主机的IP有效负载使用了身份认证和加密，但IP报头不受保护。

隧道模式ESP

- 身份认证适用于传递到外部IP目标地址的整个IP数据包，并在目的地执行身份认证。
- 整个内部IP分组受到隐私机制的保护，以便传送到内部IP目的地。

运输邻接

- 加密后应用身份认证的另一种方法是使用两个捆绑在一起的传输SA，内部是ESP SA，外部是AH SA
  - 在这种情况下，ESP使用时没有其身份认证选项；
  - 加密应用于IP有效负载；
  - 然后在运输模式中应用AH；
  - 这种方法的优点是认证涵盖更多领域；
  - 缺点是两个SA的开销，而不是一个SA的开销。

传输隧道束

- **在加密之前使用身份认证优点：**
  - **因为加密能保护身份认证数据**
  - **可能需要将认证信息与消息一起存储在目的地以供稍后参考。**

- 在两个主机之间先认证再加密的一种方法是使用由内部AH传输SA和外部ESP隧道SA组成的安全关联束。

（1）身份认证应用于IP有效负载和IP报头。

（2）然后由ESP以隧道模式处理所得到的IP分组。

（3）结果是整个经过身份认证的内部数据包被加密，并添加了新的外部IP报头。

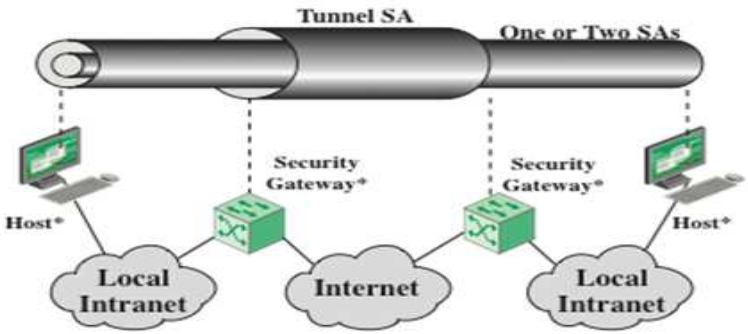
9.4.2 安全关联的基本组合

- IPSec 体系结构文档列举了IPSec 主机（如工作站、服务器）和安全网关（如防火墙、路由器）必须支持的4个SA组合的例子，如图9.10所示。
- 在该图中，每种情况的下部表示元素的物理连接；上部表示一个和多个嵌套SA逻辑连接。每个SA可以是AH或ESP。

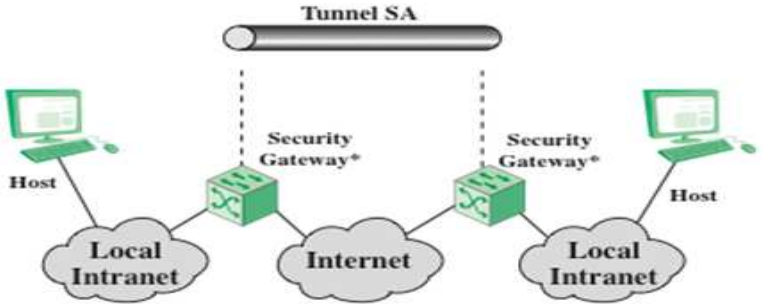
安全关联的基本组合

传输IP流
的加密隧道

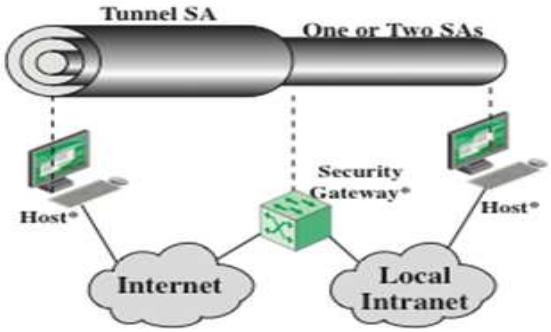
(a) Case 1



(c) Case 3



(b) Case 2



(d) Case 4

06
Part

IPSec密钥管理

9.5 IPSec密钥管理

- 手工管理
- 自动管理
  - Photuris
  - 简单Internet密钥管理协议SKIP
  - Internet密钥交换协议IKE
- IPSec默认的协议
  - IKE

1. IKE

- **AH & ESP**
  - **安全关联SA和会话密钥建立以后的工作过程**
- **IKE**
  - **IKE的目的是使用某种长期密钥（如共享的秘密密钥、签名公钥和加密公钥），在建立安全会话之前，自动地、以受保护的方式进行双向认证、建立共享的会话密钥和生成IPSec的SA ，以保护后续通信。**
  - **IKE代表IPSec对SA进行协商，并对安全关联数据库(SAD)进行填充。**

2. IKE组成

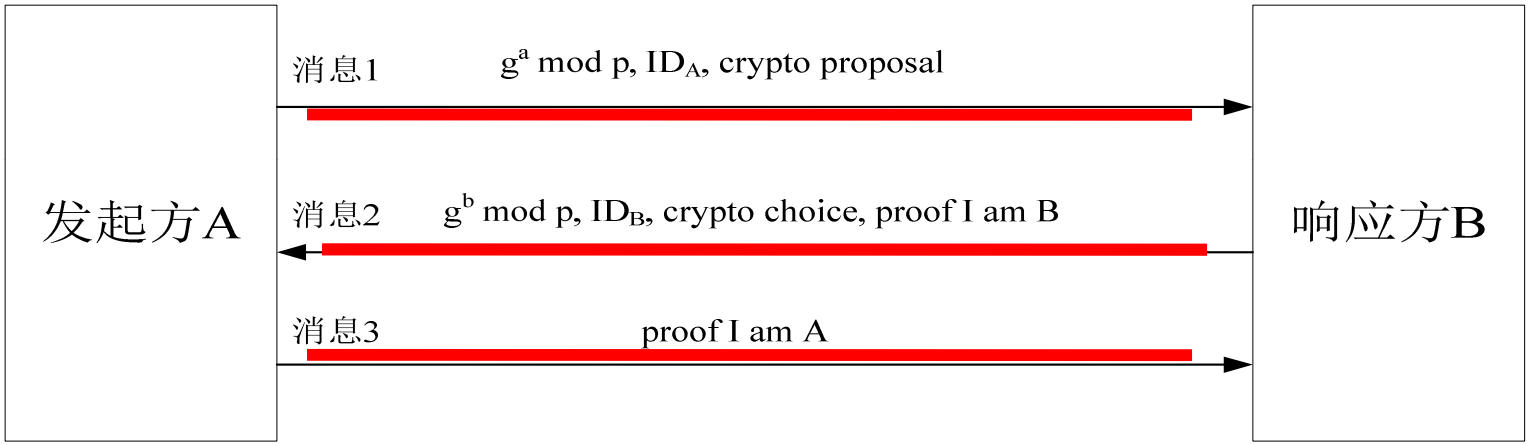
- Oakley
  - 一个基于Diffie-Hellman算法的密钥交换协议
- ISAKMP
  - 为认证和密钥交换提供了一个框架，用来实现多种密钥交换。
  - ISAKMP自身不包含特定的交换密钥算法，而是定义了一系列使用各种密钥交换算法的报文格式，规定了通信双方的身份认证，安全关联的建立和管理，密钥产生的方法，以及安全威胁(例如重放攻击)的预防。
- DOI
  - 定义了IKE具体如何协商IPSec SA

3. IKE的阶段

- IKE定义了两个阶段的ISAKMP交换
  - 阶段1建立IKE SA，对通信双方进行双向身份认证，并建立会话密钥；
  - 阶段2使用阶段1的会话密钥，建立一个或多个ESP或AH使用的SA。

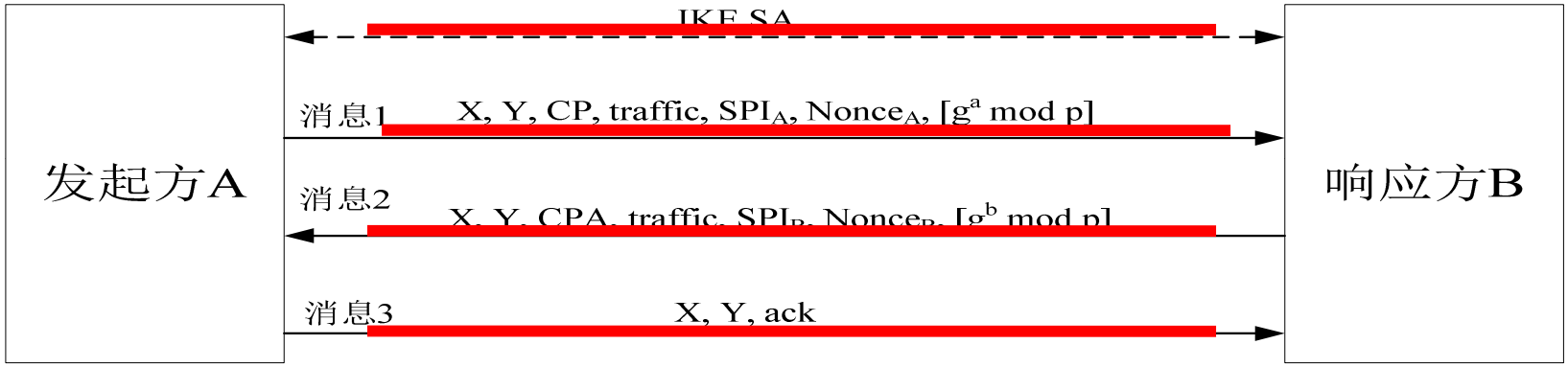
IKE阶段1 – 积极模式

- 前两条消息是Diffie-Hellman交换，用于建立会话密钥
- 消息2和消息3完成了双向认证



IKE阶段2

- **IKE阶段2定义了快速交换模式，用于建立ESP和AH的SA。**



小结

- 9.0 IPSec简介
- 9.1 IP安全概述
- 9.2 IP安全策略
- 9.3 封装安全负载（ESP）
- 9.4 安全关联组合
- 9.5 IPSec密钥管理

志存高远 责任为先

感谢聆听

网址：www.jxust. edu.cn
邮编：341000