第10章：IP 安全性 (IPSec) 学习笔记

一、IPSec 概述

1.1 基本定义

IPSec (Internet Protocol Security) 是 IETF 制定的网络层安全协议族，为 IPv4/IPv6 通信提供端到端安全保障。

核心特性：

- 工作层次：网络层 (OSI Layer 3)
- 透明性：
  - 对上层协议透明：可保护所有基于 IP 的协议（TCP、UDP、ICMP 等），无需应用层修改
  - 对用户透明：安全处理过程对终端用户不可见

1.2 协议组成

IPSec 由两个核心安全协议组成:

1. AH (Authentication Header, 协议号 **51)**

- 提供：数据源认证、完整性校验、抗重放
- 限制：不提供机密性（数据明文传输）

2. ESP (Encapsulating Security Payload, 协议号 **50)**

- 提供：机密性（加密）、数据源认证（可选）、完整性校验（可选）、抗重放
- 特点：机密性为核心功能，认证为可选但通常启用

1.3 安全服务

IPSec 提供四项核心安全服务（设发送方 A、接收方 B、消息 M、密钥 K）：

1.3.1 机密性 (Confidentiality)

- 机制：对称加密（AES、3DES 等）
  - 阶段一：*握手与协商 (IKE 协议) ← 用混合加密和数字签名（非对称加密）。*
  - 阶段二：*数据传输 (ESP 协议) ← 只用对称算法。*
- 公式：$C = E_{K_{enc}}(M)$
  - C：密文，E：加密算法，K_{enc}：协商的密钥

1.3.2 数据完整性 (Data Integrity)&认证(Data Origin Authentication)

这就是下文的“鉴别”

- 机制：HMAC (基于密钥的哈希函数)
- 公式：$ICV = HMAC(K_{auth}, M)$
- 验证过程：接收方重算 ICV'，若 $ICV' = ICV$ 则:
  - *数据未被篡改；*
  - *只有合法方基于共享密钥 K_{auth} 能生成正确的 ICV。*

1.3.3 抗重放 **(Anti-Replay)**

- 机制：序列号 + 滑动窗口
  - *发送方：每个数据包附加单调递增的序列号 SN*
  - *接收方：维护滑动窗口 W，丢弃窗口外或重复的 SN*

二、IPSec 核心组件与考点

2.1 安全关联 (Security Association, SA)

2.1.1 SA 的定义与特性

- 定义：通信对等方之间建立的一种单向逻辑连接，存储了所有必要的安全参数（如密钥、算法、生命周期等）。
- 单向性 **(Simplex)**：SA 是单向的。
- 如果 A 和 B 需要进行双向安全通信，必须建立两个 SA：
  i. $SA_{A \to B}$：保护 A 发往 B 的流量。
  ii. $SA_{B \to A}$：保护 B 发往 A 的流量。
- 这两个 SA 组成一个 **SA Bundle (**安全关联组**)** 。

2.2 SA 的唯一标识 (三元组)

在接收端（Inbound 处理），系统通过以下三元组在 **SAD (Security Association Database)** 中唯一定位一个 SA：

1. **SPI (Security Parameter Index)**：
   - 存在于 AH 或 ESP 的包头中。
   - 一个 32 位的任意标识符，类似于数据库的 **Primary Key** 。
2. 目的 **IP** 地址 **(Destination IP)**：
   - 数据包的终点地址（单播、广播或多播）。
3. 安全协议标识符 **(Security Protocol ID)**：

- 区分该 SA 是用于 AH 还是 ESP。

2.3 SA 与 AH/ESP 协议的关系

核心逻辑：**SA** 为 **AH/ESP** 提供运行时参数。

当内核的网络栈处理一个 IPSec 数据包时，流程如下：

1. 协议头识别：网络层看到协议号（Protocol ID），识别出这是 AH (51) 或 ESP (50) 包。
2. 上下文查找：
   - AH/ESP 协议本身不包含密钥。
   - 系统必须根据包头中的 **SPI (Security Parameter Index)** 去数据库中查找对应的 **SA**。
3. 参数注入：找到 SA 后，取出其中的密钥（Key）和算法（Algorithm），注入到 AH/ESP 的处理逻辑中，完成解密或完整性校验。

2.4 两个关键数据库：SPD 与 SAD

IPSec 的实现依赖于内核中的两个数据库：

数据库	全称	作用	逻辑阶段
SPD	**Security Policy Database**(安全策略库)	决策者。决定这股流量是“丢弃”、“绕过(不加密)”还是“应用IPSec”。类似于防火墙规则表(ACL)。	流量分类阶段(数据包刚进入或即将发出时)
SAD	**Security Association Database**(安全关联库)	参数库。存储了所有活跃 SA 的具体参数（密钥、SPI、序列号窗口等）。	处理阶段(确定要加密/解密时)

2.5 密钥管理 (Key Management)

IPSec 的密钥管理负责安全地分发和维护 SA 所需的密钥，主要分为手动和自动两种方式。

2.5.1 手动管理 (Manual Key Management)

- 机制：系统管理员直接在通信两端手动配置密钥和 SA 参数（如 SPI、加密算法）。
- 适用：仅适用于规模极小、静态的局域网环境。
- 缺点：扩展性差（N 个节点需配置 $N(N-1)/2$ 对密钥），难以定期更新密钥，安全性较低。

2.5.2 自动管理 (Automated Key Management)

- 核心协议： **IKE (Internet Key Exchange)** 是 IPSec 的事实标准。
- **IKE** 的复合结构：IKE 并非单一协议，而是基于以下两个协议的组合：
  - **ISAKMP** (Internet Security Association and Key Management Protocol)：
    - 定义了协商 SA 的框架、流程和消息格式，但不指定具体的密钥交换算法。
  - **Oakley**：
    - 基于 **Diffie-Hellman** 算法，提供了具体的密钥生成和交换机制。
- 加密方式：
  - 阶段一 **(IKE** 协商**)**：使用非对称加密（公钥加密）和数字签名进行身份认证和密钥协商
  - 阶段二 **(**数据传输**)**：使用对称加密（AES、3DES 等）进行高效的数据加密
- 工作流程 **(Two-Phase Handshake)**：
  - 第一阶段 **(Phase 1)**：建立 **IKE SA**。双方协商安全策略并建立一个加密的控制通道，用于保护后续协商。
  - 第二阶段 **(Phase 2)**：建立 **IPSec SA**。在 IKE SA 的保护下，快速协商出用于实际传输用户数据（AH/ESP）的 SA。

三、核心协议：AH 与 ESP

3.1 AH (Authentication Header, 协议号 51)

功能定位：提供认证和完整性，不加密。

- 提供服务：
  - 数据完整性（HMAC）
  - 数据源认证
  - 抗重放
- 认证范围：原 IP 数据包（包括 IP 头不变字段 + 载荷）

- 注：IP 头中变动字段（TTL、Checksum）不在认证范围

3.2 ESP (Encapsulating Security Payload, 协议号 50)

功能定位：IPSec 最全面的协议，同时提供机密性和认证。

- 提供服务：
  - 机密性（核心功能，对载荷加密）
  - 数据完整性与源认证（可选，通常启用）
  - 抗重放
- 结构：
  - **ESP** 头：SPI + 序列号（明文）
  - **ESP** 尾：填充 + 下一首部（加密）
  - **ESP** 认证数据：ICV（明文）

3.3 AH 与 ESP 对比总结

特性	**AH (Authentication Header)**	**ESP (Encapsulating Security Payload)**
IP 协议号	51	50
机密性**(**加密**)**	无(数据明文传输)	有(核心功能)
完整性/认证	必选	可选 (通常使用)
认证范围	整个 **IP** 包(含 IP 头非变动字段 + 载荷)	仅 **ESP** 头部 **+** 载荷(不含外部 IP 头)
抗重放	支持	支持
适用场景	仅需防篡改，无需保密	需要保密 (如 VPN)、防篡改

四、工作模式

IPSec 支持两种封装模式，取决于通信端点类型（主机 vs. 网关）。需区分 **AH** 和 **ESP** 在这两种模式下的不同表现。

4.1 传输模式 (Transport Mode)

特征 ：端到端保护，保留原 IP 头。

- 适用场景 ：主机 ↔ 主机 (End-to-End)。

- 局限：无法隐藏通信行为（源/目 IP 暴露），易受流量分析攻击。

(1) AH 封装（传输模式）

- 结构：AH 头插在原 IP 头和上层协议（TCP/UDP）之间。
- 认证范围：`原 IP 头(不变部分) + AH + TCP + Data`。
- 注：AH 会保护 IP 头中的源/目 IP 地址，导致其无法穿越 NAT（NAT 会修改 IP 头，从而破坏 AH 签名）。

```
原始数据包：  [原 IP 头] [TCP 头] [数据]
              ↓
AH 封装：     [原 IP 头] [AH 头] [TCP 头] [数据]
              └──────── 鉴别范围 ──────┘
                        (含 IP 头中的不可变字段)
```

(2) ESP 封装（传输模式）

- 结构：ESP 头插在 TCP 之前，ESP 尾插在最后。
- 保护范围：只保护上层载荷（TCP/UDP 段）。不保护 **IP** 头。

```
原始数据包：  [原 IP 头] [TCP 头] [数据]
              ↓
ESP 封装：    [原 IP 头] [ESP 头] [TCP 头] [数据] [ESP 尾] [ESP 鉴别]
                         │      └──── 加密范围 ────┘      │
                         └──────────── 鉴别范围 ──────────────┘
```

4.2 隧道模式 (Tunnel Mode)

特征：网关到网关保护，封装整个原始 IP 包。

- 适用场景：VPN（网关 ↔ 网关）、主机 ↔ 网关。
- **IP** 头处理：生成新 **IP** 头（网关地址），将原 **IP** 头作为载荷隐藏。

(1) AH 封装（隧道模式）

- 结构：`[新 IP 头] [AH] [原 IP 头] [TCP] [Data]`
- 鉴别范围：`新 IP 头(不变部分) + AH + 原 IP 头 + TCP + Data`。
- 注：AH 甚至鉴别了新的外部 IP 头。

```
原始数据包：  [原 IP 头] [TCP 头] [数据]
              ↓
AH 封装：     [新 IP 头] [AH 头] [原 IP 头] [TCP 头] [数据]
```

```
└──────────────── 鉴别范围 ────────────────┘
(含新 IP 头中的不可变字段)
```

(2) ESP 封装（隧道模式）

- 结构：`[新 IP 头] [ESP 头] [原 IP 头] [TCP] [Data] [ESP 尾]`
- 保护范围：加密并保护原内部 **IP** 包。

```
原始数据包：  [原 IP 头] [TCP 头] [数据]
              ↓
ESP 封装：    [新 IP 头] [ESP 头] [原 IP 头] [TCP 头] [数据] [ESP 尾] [ESP 鉴别]
                         |      └──────────── 加密范围 ────────────┘       |
                         └──────────────── 鉴别范围 ──────────────────────┘
```

4.3 协议与模式功能矩阵（考点核心）

此表总结了 AH 与 ESP 在不同模式下的保护范围差异（参考自课件图表）：

协议 / 模式	传输模式 **SA (Transport Mode)**	隧道模式 **SA (Tunnel Mode)**
AH(鉴别头)	鉴别范围： 1. Payload (TCP/UDP报文) 2. 原 **IP** 首部 （不可变字段）	鉴别范围： 1. 原内部 IP 包（含原 IP 头） 2. 新外部 **IP** 首部 （不可变字段）
ESP(不带鉴别)	加密 **IP** 载荷 *(IP 首部是明文，不加密)*	加密内部 **IP** 分组 *(新外部 IP 首部是明文)*
ESP(带鉴别)	加密 **IP** 载荷 鉴别**ESP** 头 + 密文 (***不鉴别****IP 首部*)	加密内部 **IP** 分组 鉴别**ESP** 头 + 密文 (***不鉴别****新外部 IP 首部*)

> **补充说明（关于 IP 头鉴别）：**
>
> - **AH** 的核心特点是 **总是鉴别 IP 头** 。
> - 这使得 AH 能够防止 IP 地址欺骗；
> - 但也导致它无法通过 NAT（网络地址转换），因为 NAT 会修改 IP 头，导致 AH 校验失败。
> - **ESP** 即使开启鉴别功能，也**从不鉴别外部 IP 头**。

五、应用场景

5.1 站点到站点 VPN (Site-to-Site VPN)

场景：通过 Internet 连接地理分离的局域网。

模式：隧道模式

工作流程：

1. 发送：内网主机 A → 本地网关
2. 封装：网关加密整个包，添加新 IP 头（指向对端网关）
3. 传输：加密包通过 Internet 传输
4. 解封：对端网关解密，还原原始包
5. 转发：对端网关将包转发至目标主机 B

特点：内网主机无感知，如同在同一局域网通信。

5.2 远程访问 VPN (Remote Access VPN)

场景：移动用户通过 Internet 安全接入企业内网。

模式：隧道模式

工作流程：

- 客户端：安装 VPN 客户端软件
- 建立隧道：客户端与企业 VPN 网关协商建立 IPSec 隧道
- 虚拟 **IP**：网关分配内网虚拟 IP
- 通信：所有内网流量在客户端加密封装后通过隧道传输

六、核心要点总结

6.1 IPSec 四大安全服务

1. 机密性：对称加密（AES/3DES）保护数据内容
2. 完整性/认证：依赖HMAC
3. 抗重放：序列号 + 滑动窗口防止重放攻击

6.2 SA 三元组（唯一标识）

- **SPI**（32位安全参数索引）
- 目的 **IP** 地址
- 安全协议标识（AH/ESP）

6.3 核心数据库

数据库	作用	时机
SPD	决策：丢弃/绕过/加密	流量分类阶段
SAD	存储 SA 参数（密钥等）	加密/解密阶段

6.4 协议选择

- 仅需鉴别：使用 AH（注意：无法穿越 NAT）
- 需要保密：使用 ESP
- 最佳实践：ESP + 鉴别（同时提供：加密+认证+完整性）

6.5 模式选择

- 主机 ↔ 主机：传输模式（端到端保护）
- 网关 ↔ 网关（**VPN**）：隧道模式（隐藏内部通信）

6.6 密钥管理

- 手动配置：仅适用于小规模静态环境
- **IKE** 自动管理（推荐）：
  - 阶段一：建立 IKE SA（使用非对称加密）
  - 阶段二：建立 IPSec SA（保护实际数据传输）

6.7 关键考点

1. **AH** 特点：
   - 总是鉴别 IP 头（包括源/目 IP）
   - 无法穿越 NAT
   - 不提供机密性
2. **ESP** 特点：
   - 核心功能是加密
   - 即使开启鉴别也不鉴别外部 IP 头
   - 可穿越 NAT
3. 传输模式 **vs** 隧道模式：
   - 传输模式：保留原 IP 头，仅加密载荷
   - 隧道模式：封装整个原 IP 包，添加新 IP 头

4. **IKE** 两阶段握手：

- Phase 1：建立安全通道（IKE SA）
- Phase 2：协商数据保护参数（IPSec SA）