IPsec 数据库

- 安全策略库 SPD Security Policy Database
  - 逻辑上分为三部分
    - SPD-S 所有需要 IPsec 保护的 IP 范围
    - SPD-O 离去流量中需要旁路（忽略 IPsec 保护）或丢弃的 IP 地址范围
    - SPD-I 进入流量中需要旁路或丢弃的 IP 地址范围
    - 到达报文查找顺序 SPD-I -> SPD-S -> SPD-O
- 安全联系库 SAD Security Association Database：已创建的安全联系存放在 SAD 中
- 对等授权库 PAD Peer Authorization Database：提供安全联系管理协议与 SPD 之间的关系
  - 没有出现在 PAD 中的实体不能使用 IPsec 功能

过程（重要）

1. 本地（被 IPsec 保护的实体）与远地（与本地通信的对等实体）通过 IKE 完成鉴别并建立会话密钥。信任关系和会话秘钥保存在<u>PAD 库（Entry-2）中
2. 节点 A 向节点 B（192.168.2.1）发送报文前：A 从 SPD 中找到适用的安全策略（Entry-2），保护措施记录在 SAD 的安全联系 2 中（SA-2：SPI 值；使用 AH 规程，具体算法为 HMAC-MD5；密钥内容；密钥有效期 1 天或应用的数据超过 100MB）
3. A 依据 SA-2 提供的参数对报文使用 IPsec 的 AH 规程进行保护，然后发送给 B
4. B 收到报文后同样使用 SA-2 提供的参数，验证报文的正确性

安全规程

负载安全封装 ESP

Encapsulating Security Payload

向 IPv4 和 IPv6 提供保密性和完整性的组合安全服务

- 加密
- 数据源鉴别
- 无连接的完整性保护
- 防回放服务
- 流保密

通过在 IP 报文中扩展 **ESP 报文**实现鉴别保护和加密保护

鉴别头 AH

Authentication Header

- 无连接的完整性保护
- IP 报文源点鉴别（对称密钥）
- 防回放攻击（顺序号）

密钥交换协议 IKE

Internet Key Exchange，IKE

目前标准：IKEv2

交换类型

- 初始化 IKE_SA_INIT：交换协商 IKE_SA 的安全参数
- 鉴别 IKE_AUTH：交换发送标识，互认共享秘密（会话密钥），建立第一个子安全联系
- 子安全类型创建 CREATED_CHILD_SA：建立更多子安全联系（子安全联系可用于具体的通信输出）
- 通知 INFORMATIONAL：传送控制信息。维护性操作，如：安全联系的活性检测（无负载）、差错报告、安全联系的删除