IPSec机制概述

IP安全(IPSec)

IPSec (IP Security)是一个多服务、多算法和多粒度的框架，提供的服务包括保密性、完整性和预防重放攻击的保护。

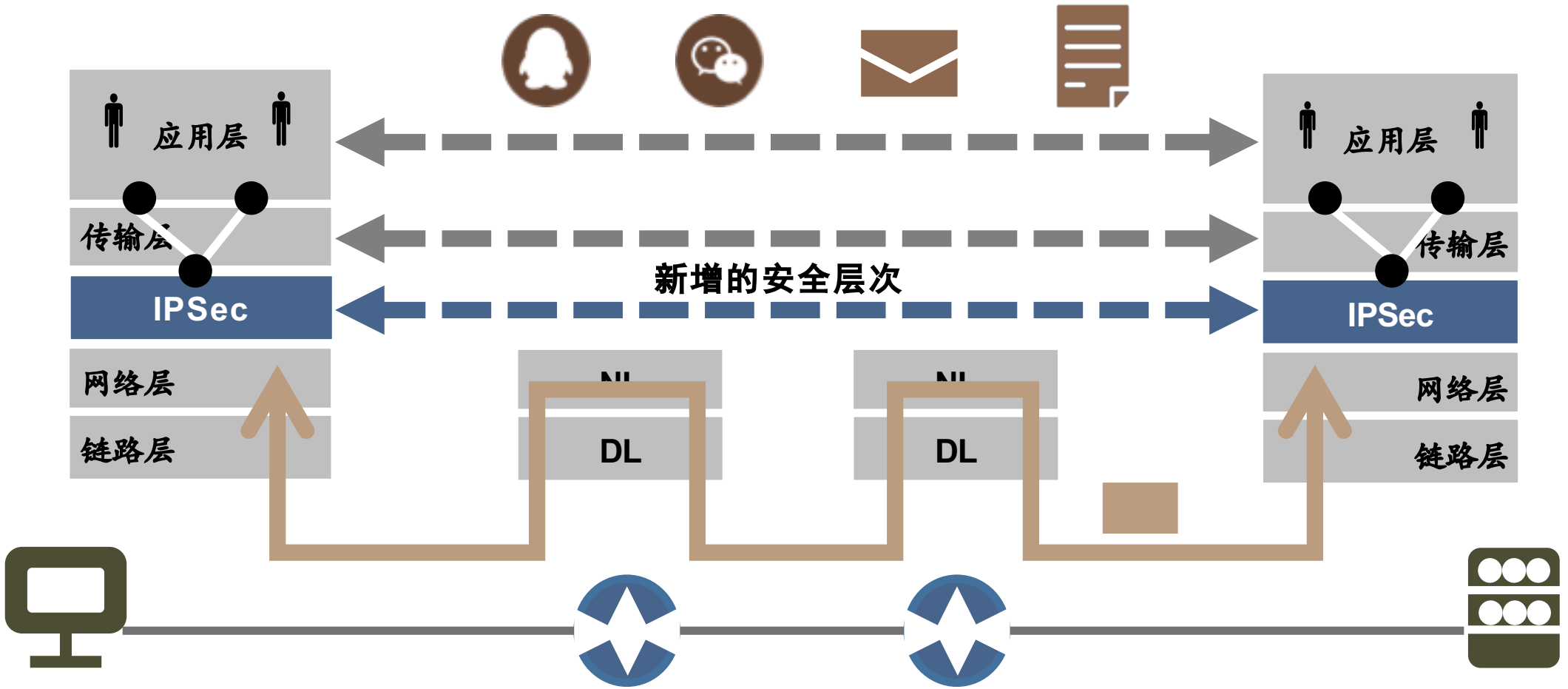
RFC 2401
RFC 2402
RFC 2406
……

- 访问控制
- 无连接的数据完整性
- 数据源端的认证
- 预防重放攻击
- 数据保密性（加密）
- 有限度的流量保密性

IPSec特点

- 多服务：给用户提供多种选择
- 多算法：与算法无关的设计，可替换成更加有效的算法
- 多粒度：包括单条TCP连接、一对主机之间的所有流量、一对路由器之的全部流量
- 工作基础是对称密钥密码学

IPSec的连接特性



网络层包

IPSec的连接特性

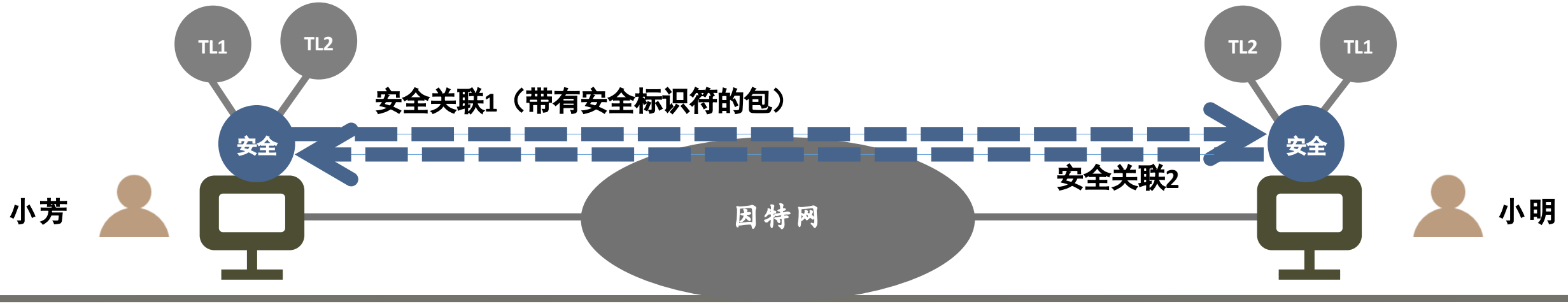
安全关联：两个端点之间的单向连接，由一个安全标识符表示。

- 安全标识符可用来查询密钥和其他有关安全信息
- 数据包必须携带安全标识符才能通过安全关联

安全标识符

一个安全标识符包括：

- 安全参数索引（SPI）
- IP目标地址
- 安全协议ID



IPSec的组成

新增两个头的描述

- 被加到IP包中，携带安全标识符、完整性控制和其他信息

因特网安全关联及密钥管理协议

- 建立密钥的有关事务
- 是一个框架

新头标准

这两个头被加到IP包，用来进行安全的传输控制。

规定了如何交换密钥

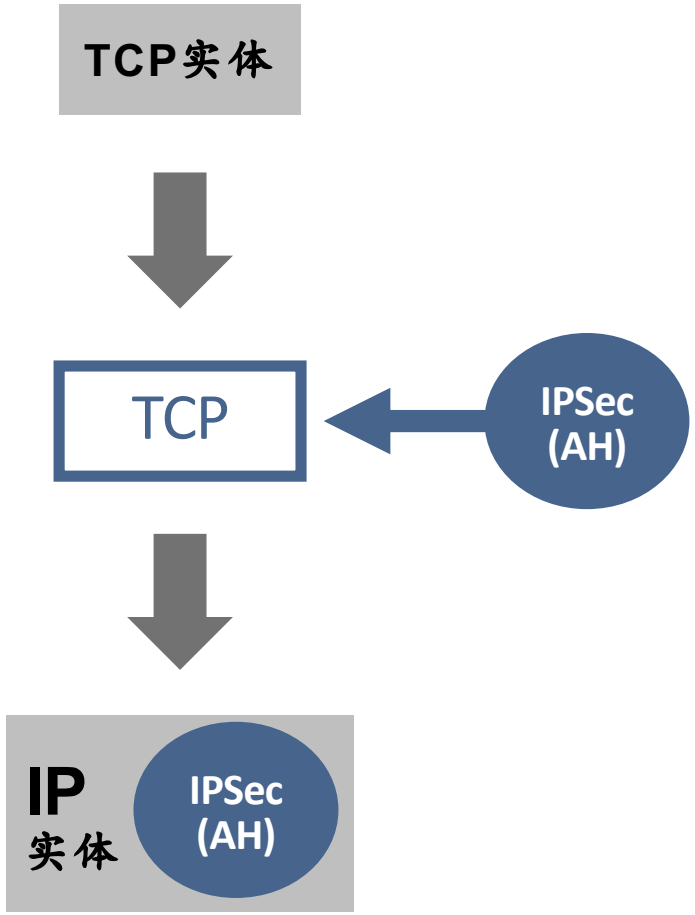
密钥管理

IPSec的传输模式一

传输模式：一种通常用于端-端通信的安全模式

(认证)传输模式

- 在IP包头和有效载荷之间增加IPSec新头
- IPSec新头称为认证头(AH)
- 包括安全关联ID、序号、有效载荷数据的完整性检查



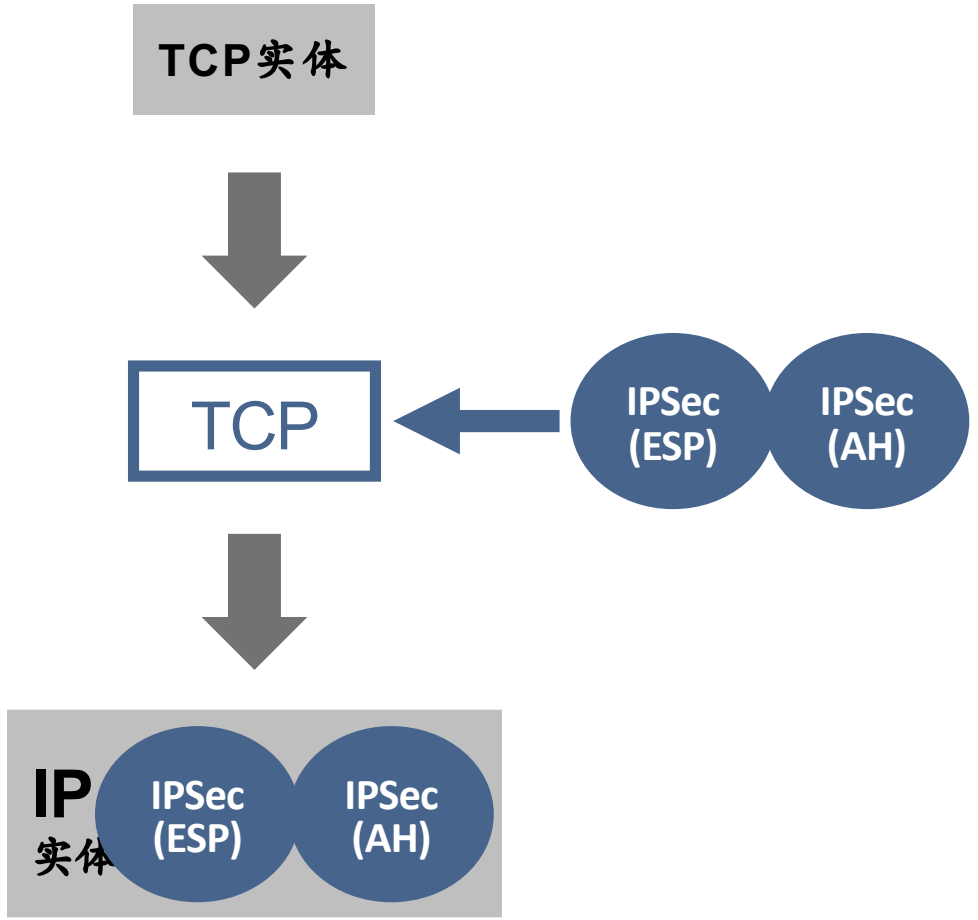
IP包有效载荷的认证和数据完整性检查可预防重放攻击。

IPSec的传输模式二

传输模式：一种通常用于端-端通信的安全模式

(加密)传输模式

- 在IP包头和有效载荷之间增加一个IPSec新头
- IPSec新头称为封装安全有效载荷头(ESP)



认证和加密传输模式不仅可预防重放攻击，还能预防窃听。

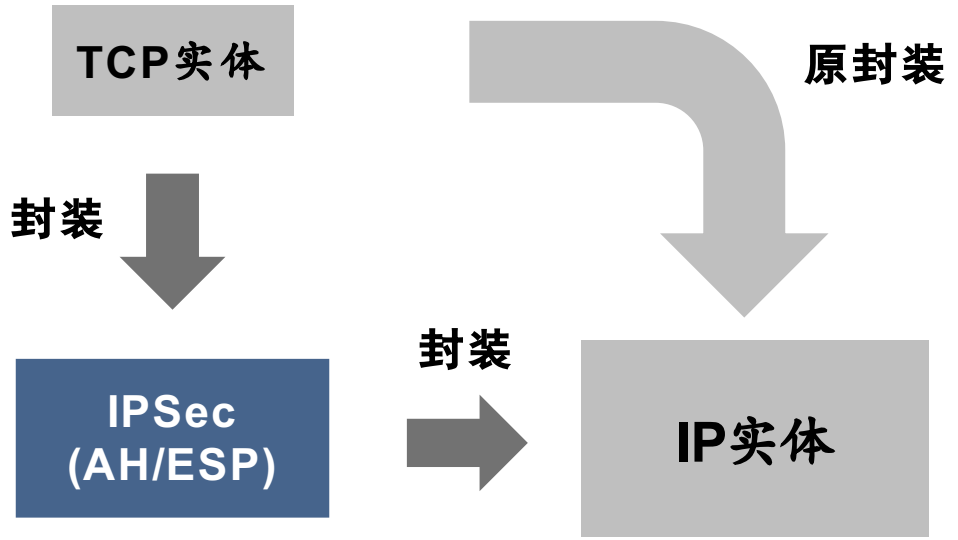
ESP: Encapsulating Security Payload

IPSec的隧道模式

隧道模式：一种通常用于网关-网关通信的安全模式.

隧道模式

- 整个IP包被封装到一个新的IP包的有效载荷部分
- 认证并加密内部IP包



内部IP包的认证和数据完整性检查可预防重放攻击，加密整个IP包又能防止窃听。