

10-2-2 IPSec 相關技術



✦ IPSec 相關技術

- ◆ **IPSec 裝置**：安全主機與Security Gateway
- ◆ **安全關聯 (Security Association, SA)**：安全套件規範
- ◆ **網際網路安全關聯鑰匙管理協定 (Internet Security Association Key Management Protocol, ISAKMP)**
- ◆ **網際網路鑰匙交換協定 (Internet Key Exchange, IKE)**
- ◆ **公鑰基礎架構 (Public Key Infrastructure, PKI)**
- ◆ **認證標頭 (Authentication Header, AH)**
- ◆ **封裝安全承載 (Encapsulation Security Payload, ESP)**
- ◆ **操作模式 (Operating Mode)**
 - 傳輸模式 (Transport Mode)
 - 通道模式 (Tunnel Mode)
- ◆ **演算法 (Algorithm)**
 - 認證演算法
 - 加密演算法

