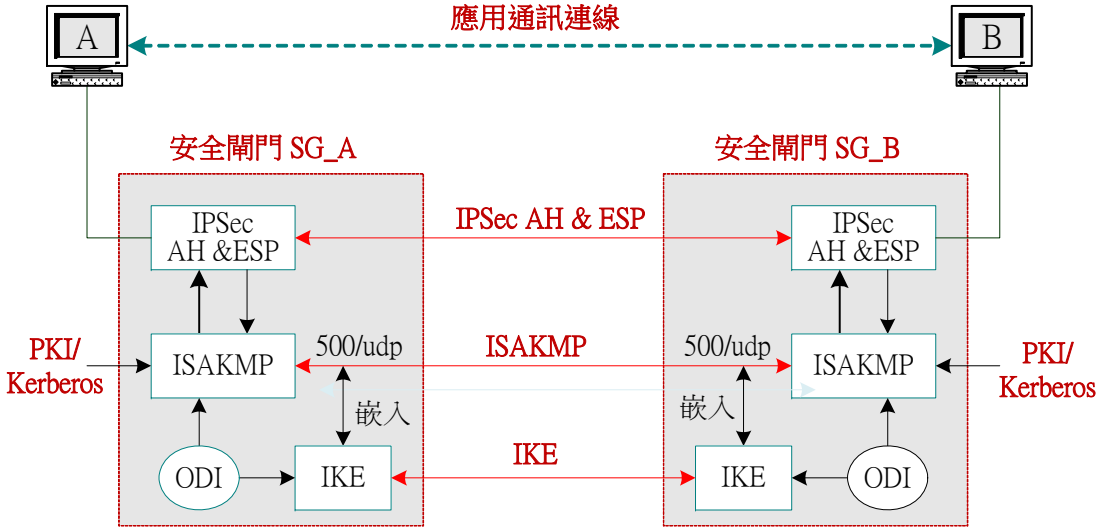
10-5-1 ISAKMP 協定簡介 (一)

- 『網際網路安全關聯金鑰管理協定』（Internet Security Association Key Management Protocol, ISAKMP）
  - 建立、修改與刪除『安全關聯』（Security Association, SA）
  - 『安全關聯資料庫』（SA Database, SAD）
  - 協議 VPN 相關協定
    - IP Sec AH、IPSec ESP、ISAKMP、IKE 與 IPSec DOI 等 5 個協定



10-5-1 ISAKMP 協定簡介 (二)

ISAKMP 運作簡介 (一)

- 工作站 A 將封包安全閘門（SA_A），SG_A 查詢是否有 SA，如果發出 IPSec 封包（ESP 或 AH 協定）；如果沒有，則啟動 ISAKMP 協定。
- SG_A 啟動 ISAKMP 協定與 SG_B 建立連線（500/udp），雙方協議建立 SA其實，ISAKMP 協定只提供基本架構，至於如何協議則 IKE 協定來完成。
- IKE 協定並無法獨立運作，也沒有專屬通訊的傳輸埠口，而是被嵌入於 ISAKMP 協定上。
- 建立 SA 時，必須先確認對方的身份，則利用數位憑證或帳戶/密碼方式。
- 各種協議事項都是利用 IPSec ODI 規範來編碼。