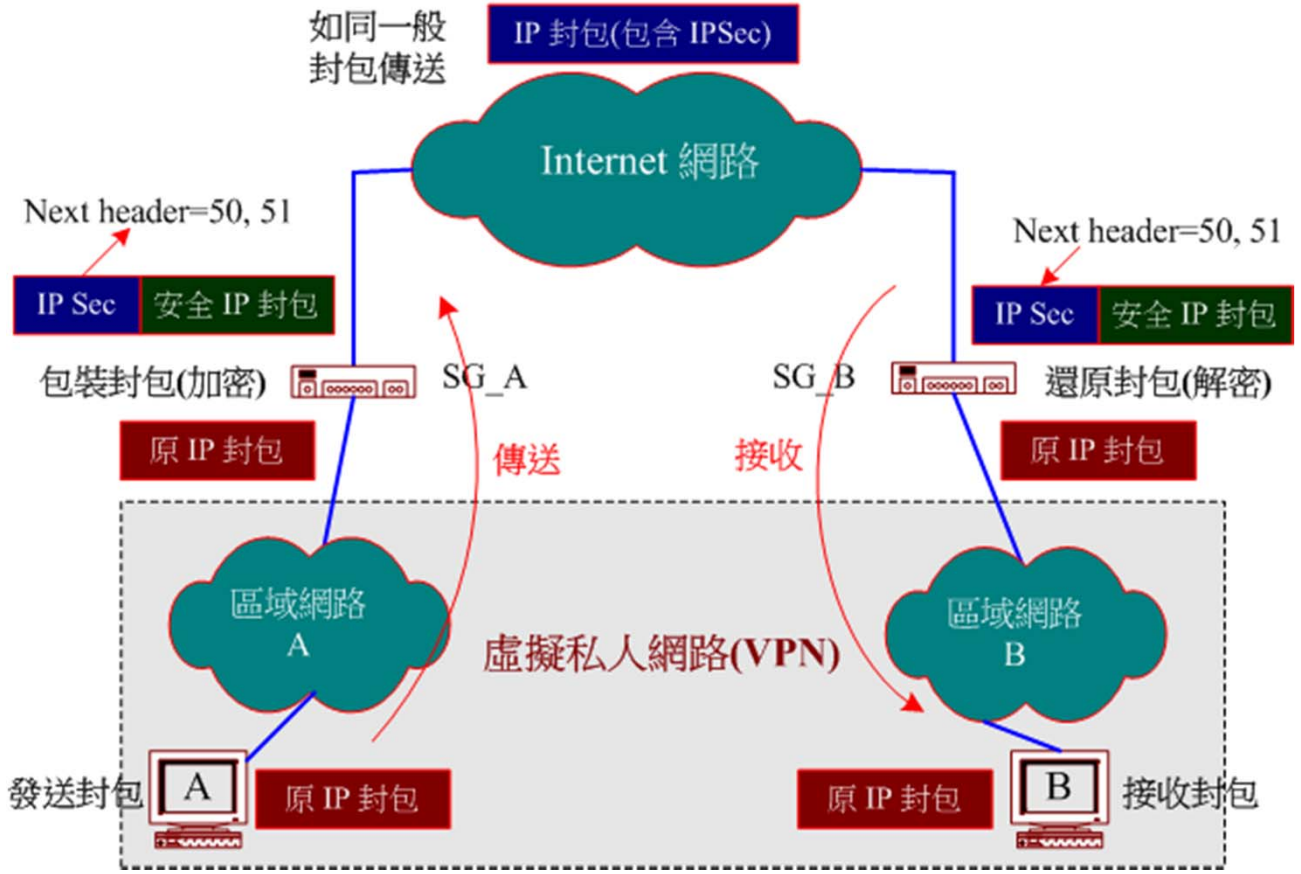
10-2-3 IPSec 運作程序 (一)

- **Security Gateway(SG) 運作程序**



10-2-3 IPSec 運作概念 (二)

- 運作概要：
  - IPSec 協定包含IPSec AH 與 IPsec ESP 兩種安全協定，皆有傳輸模式和通道模式；
  - 採用何種安全協定及封包格式？視安全關聯（SA）的規範而定
  - 如何制定 SA 的安全規範？由 ISAKMP 協議完成的；
  - 在 ISAKMP 協議當中若需交換鑰匙作為身份確定或制定會議金鑰，可利用 IKE 協定來完成；
  - 在雙方認證身分或交換鑰匙時，必須有代表身份的公鑰，然而此公鑰可由 PKI 系統中的憑證授權（CA）中心發給。