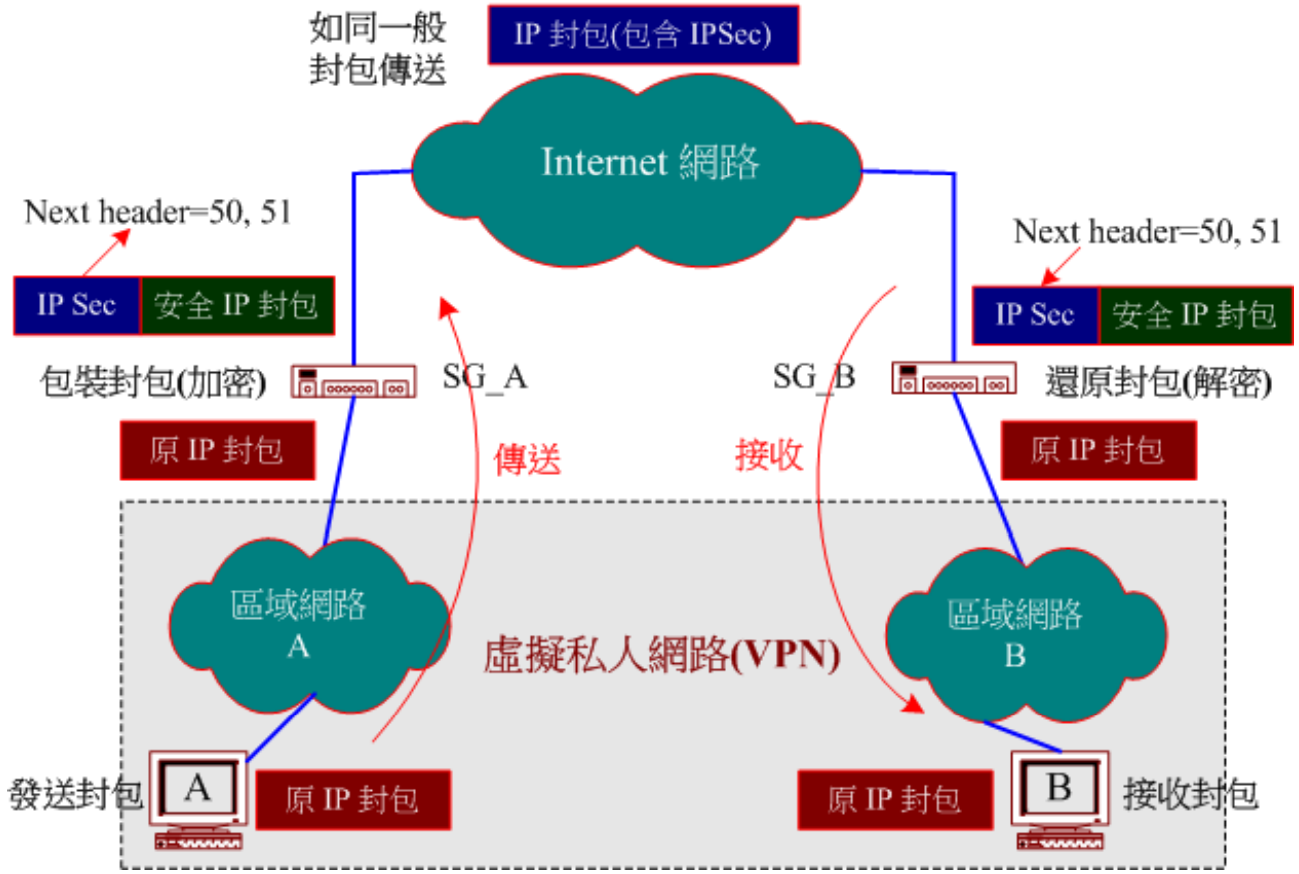
IPSec 運作概念

Security Gateway(SG) 運作程序



IPSec 運作概念

- IPSec 協定包含IPSec AH 與 IPsec ESP 兩種安全協定，這兩種安全協定都有傳輸模式和通道模式等兩種封包格式；
- 傳輸模式僅修改 IP 封包標頭；通道模式則新建立一個 IP 封包標頭；
- 至於通訊雙方是要採用哪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？係由通訊雙方利用 ISAKMP 協定所協議完成的；
- 在 ISAKMP 協議當中若需交換鑰匙來確定身份或制定會議鑰匙，可利用 IKE 協定來完成；
- 在雙方認證身分或交換鑰匙時，必須有表示身份的公開鑰匙，然而此公開鑰匙可由 PKI 系統中的憑證授權（CA）中心發給。