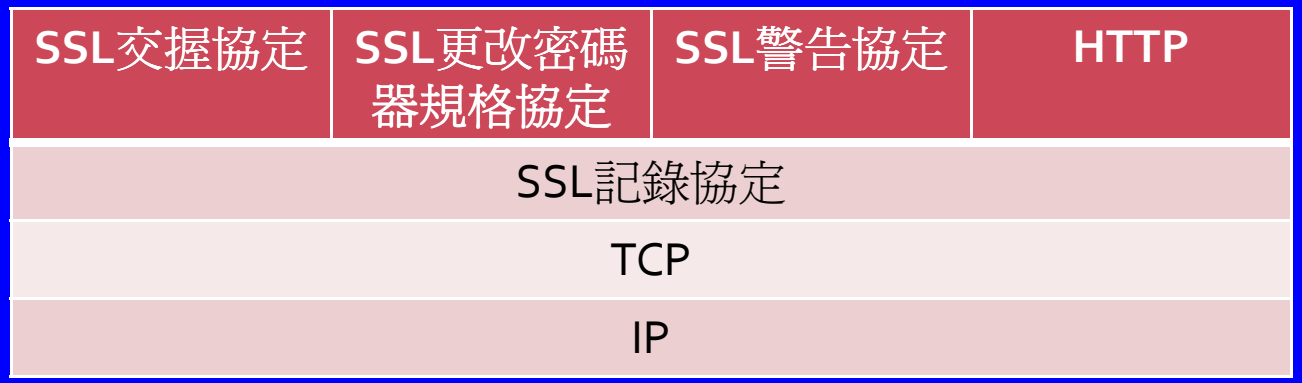
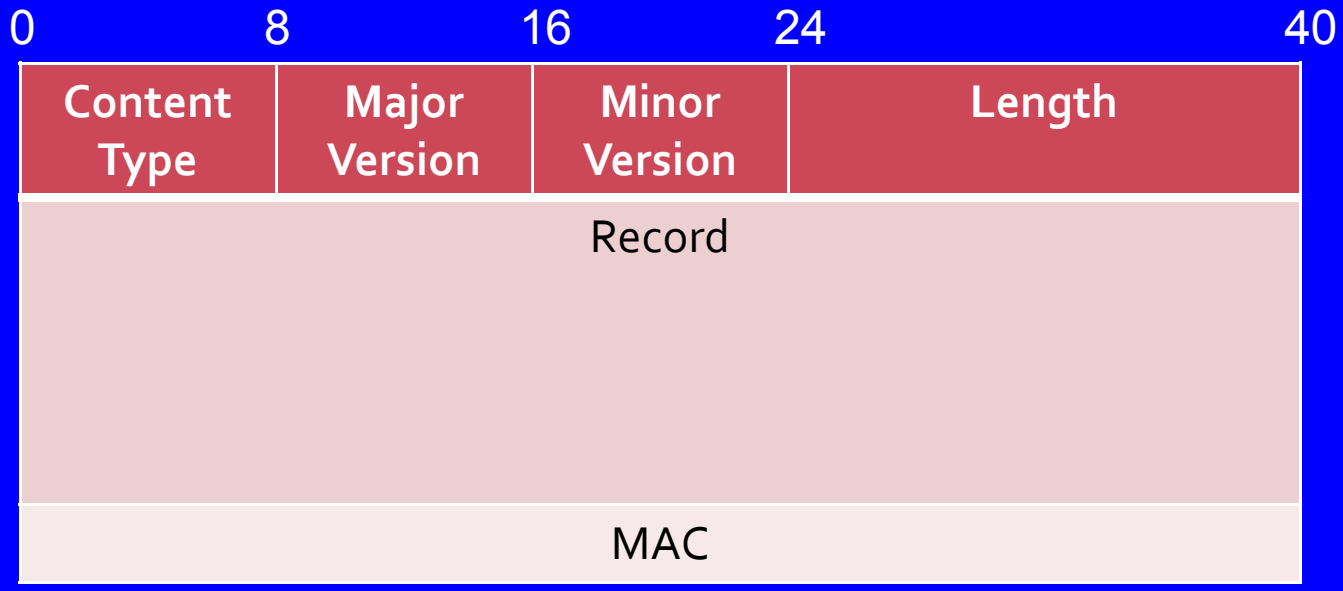
SSL/TLS

- SSL最初由Netscape提出，發表至SSL 3.0，最後沿用成為國際標準TLS 1.0，故SSL 3.0與TLS 1.0僅有些微差異。
- SSL/TLS運作階段：
  - 客戶端發送一個ClientHello消息，說明它支持的密碼演算法列表、壓縮方法及最高協議版本，也發送稍後將被使用的隨機數。
    - 非對稱金鑰系統：RSA、Diffie-Hellman、DSA及Fortezza等等。
    - 對稱金鑰演算法：RC2、RC4、IDEA、DES、Triple DES及AES等等。
    - 單向HASH函數：MD5、SHA。
  - 伺服器端回覆一個ServerHello消息，包含伺服器選擇的連接參數，源自客戶端初期所提供的ClientHello。
  - 當雙方確立了連接參數，客戶端與伺服器交換證書（依靠被選擇的公鑰系統）。
  - 伺服器請求得到客戶端的證書有可能成功，所以連接可以是相互的身份認證。但一般情況下客戶端不會有CA的驗證。
  - 使用交換的對稱金鑰加密傳輸內容。

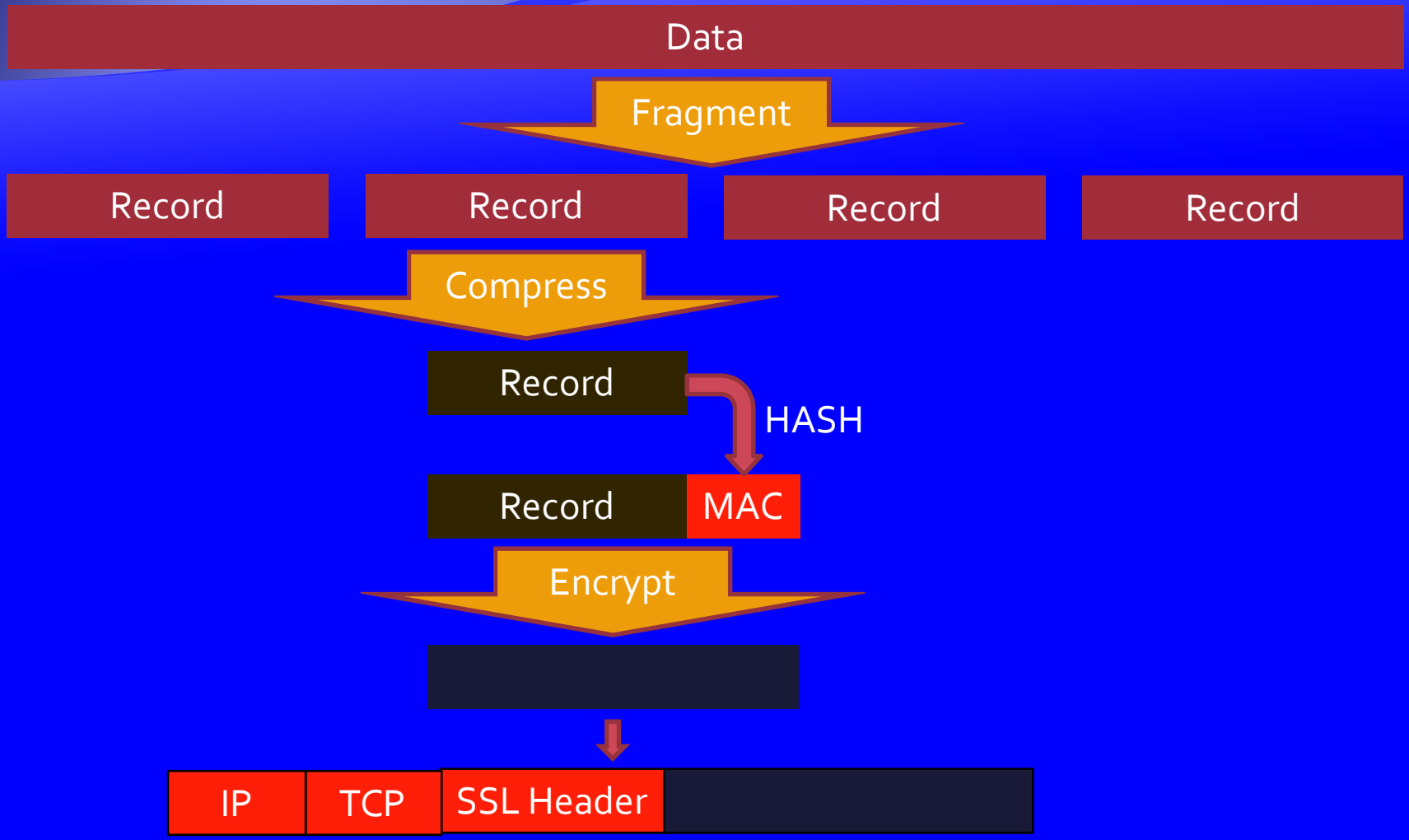
SSL/TLS 協定階層關係圖



SSL/TLS 紀錄協定封包格式



SSL/TLS 封裝過程


Data
Fragment
Record
Record
Record
Record
Compress
Record
HASH
Record
MAC
Encrypt
IP
TCP
SSL Header

SSL VPN 之應用 – OpenVPN

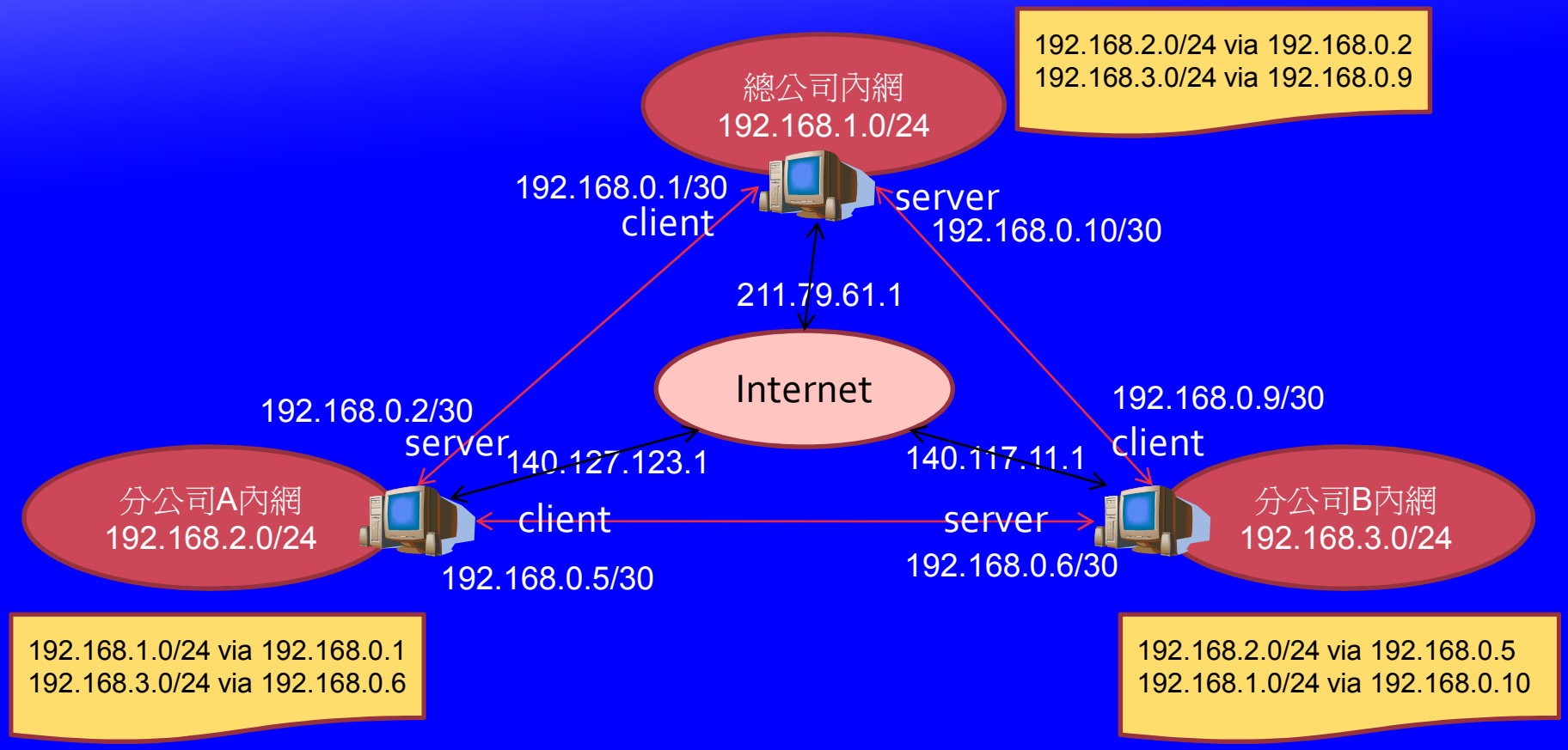
- http://openvpn.net/
- An Open Source VPN Server & Client
- Use SSL Lib
- 普通PC Server即足以應付數十人上線

OpenVPN 運作模式

- Routing Mode
  - VPN Server & Client 本身形同路由器，故IPX、Broadcast等封包不會被轉送。
  - 各內網之間的網芳若要相通，需透過NetBIOS over TCP/IP 功能，需要WINS或Samba的協助。
  - 效能較高，一般用來連結異地內網。
- Bridge Mode
  - VPN Server & Client 之間形同Layer2 Bridge，可轉送非IP型態的封包。
  - Broadcast與網芳可直接通過。
  - 使用方便但效率較低，一般用來讓使用者連回內網之用。

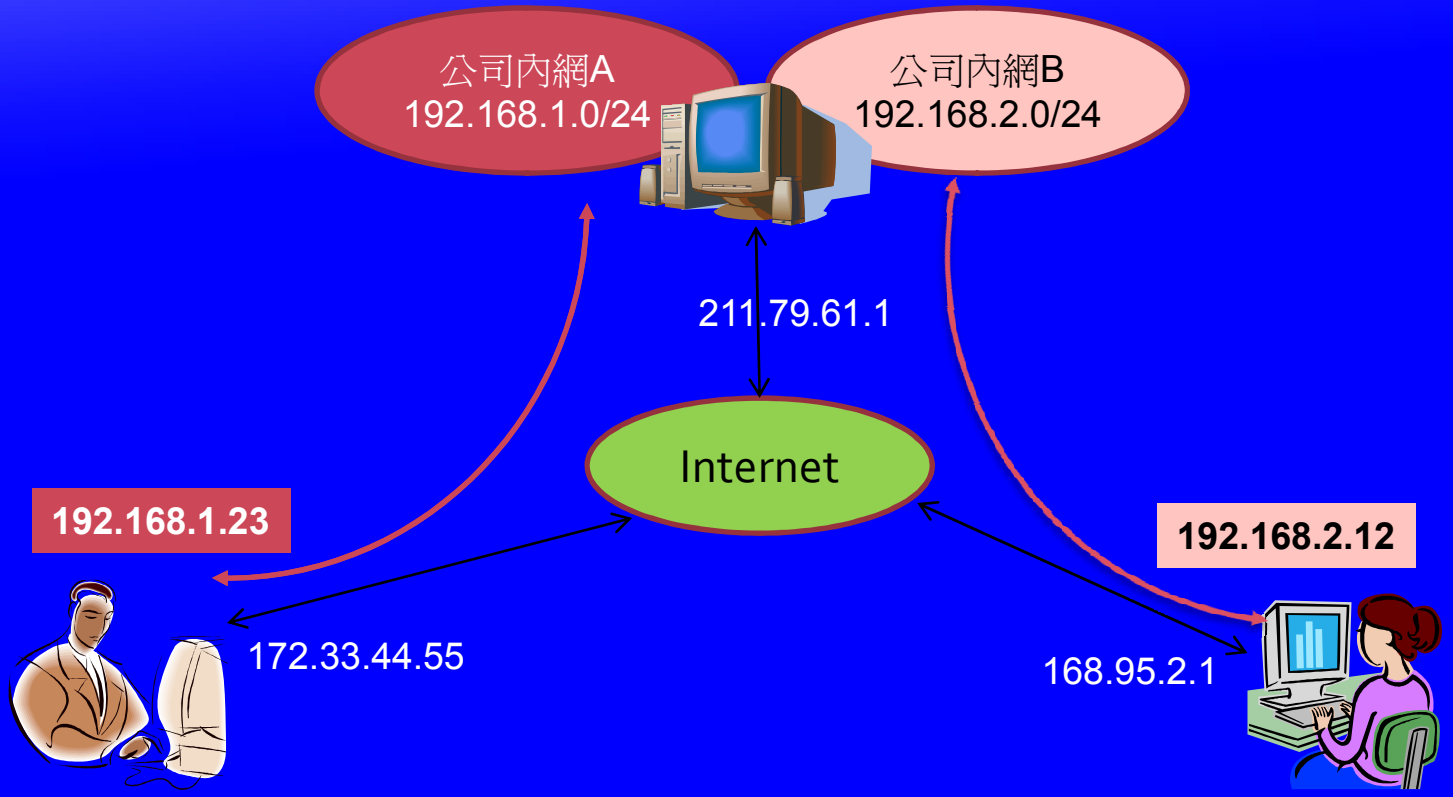
OpenVPN 運作模式

- Routing Mode



OpenVPN 運作模式

- Bridge Mode



SSH

- Secure Shell最初由芬蘭的一家公司開發，因受版權和加密算法等限制，現多轉用 OpenSSH
- SSH協定框架中最主要的部分是三個協定：
  - 傳輸層協定（The Transport Layer Protocol）：提供服務器認證，數據機密性，信息完整性等的支持。
  - 用戶認證協定（The User Authentication Protocol）：為服務器提供客戶端的身份鑒別。
  - 連接協定（The Connection Protocol）：將加密信息通道切成若干個邏輯通道，提供給更高層的應用協定重導使用，如FTP, VNC等等。
- SSH的安全驗證
  - 驗證客戶端
    - 基於密碼的身份驗證
    - 基於非對稱金鑰的身份驗證
  - 驗證伺服器端
    - 直接傳送公鑰給客戶端，由客戶端比對
    - 將公鑰存放於CA，客戶端直接跟CA索取伺服器公鑰

SSH

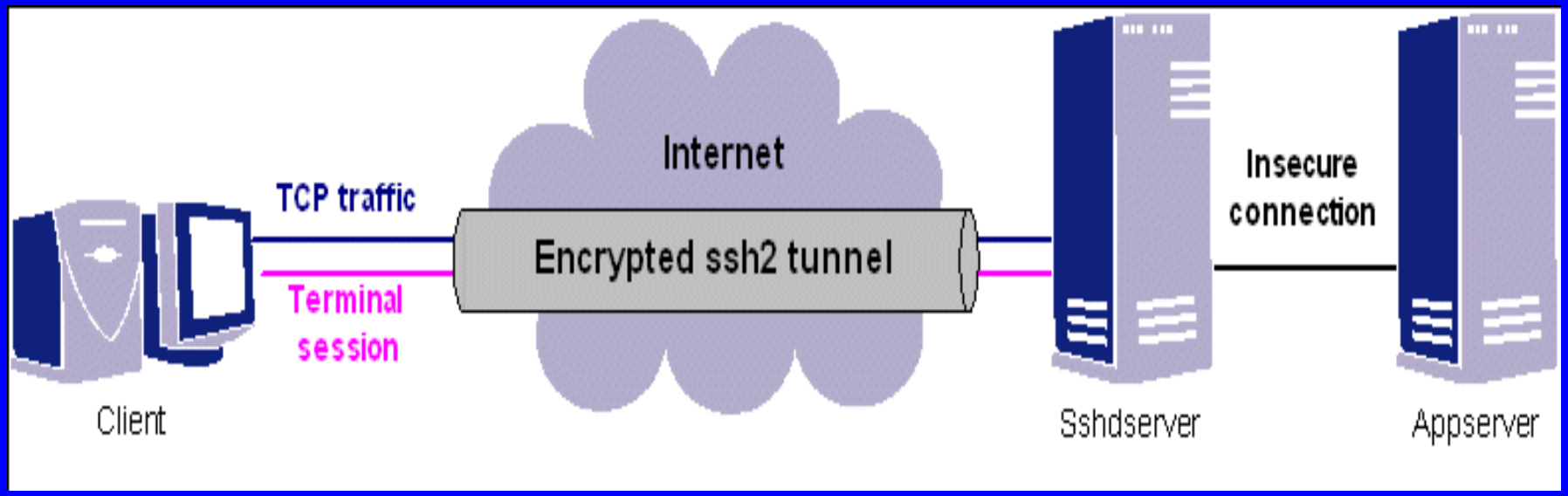
- SSH is a protocol, not a product. It is a secure way of transmitting data over TCP/IP networks from one computer to another.
- SSH protocol covers authentication, encryption, and the integrity of data transmitted over a network.
- SSH is today used by millions worldwide for secure system administration, secure file transfer, and secure application connectivity.

Threats Prevented by Secure Shell

- **Password Exposure**
  - Does not send passwords over the network in plaintext format, making it impossible for outsiders to "sniff" the passwords.
- **Data Eavesdropping**
  - Secure Shell implements encryption to prevent eavesdropping of confidential data while it travels over TCP/IP networks. Combining strong encryption and authentication, Secure Shell ensures that only the legitimate recipients can access the transmitted data.
- **Man-in-the-Middle Attack**
  - In the man-in-the-middle attack, an attacker residing between the client and server modifies the data communications. The Secure Shell protocol implements server authentication and cryptographic integrity checks to ensure that the transferred data cannot be modified undetected.

Port Forwarding

- Port forwarding, or tunneling, is a way to forward otherwise insecure TCP traffic through SSH Secure Shell. You can secure for example POP3, SMTP and HTTP connections that would otherwise be insecure.

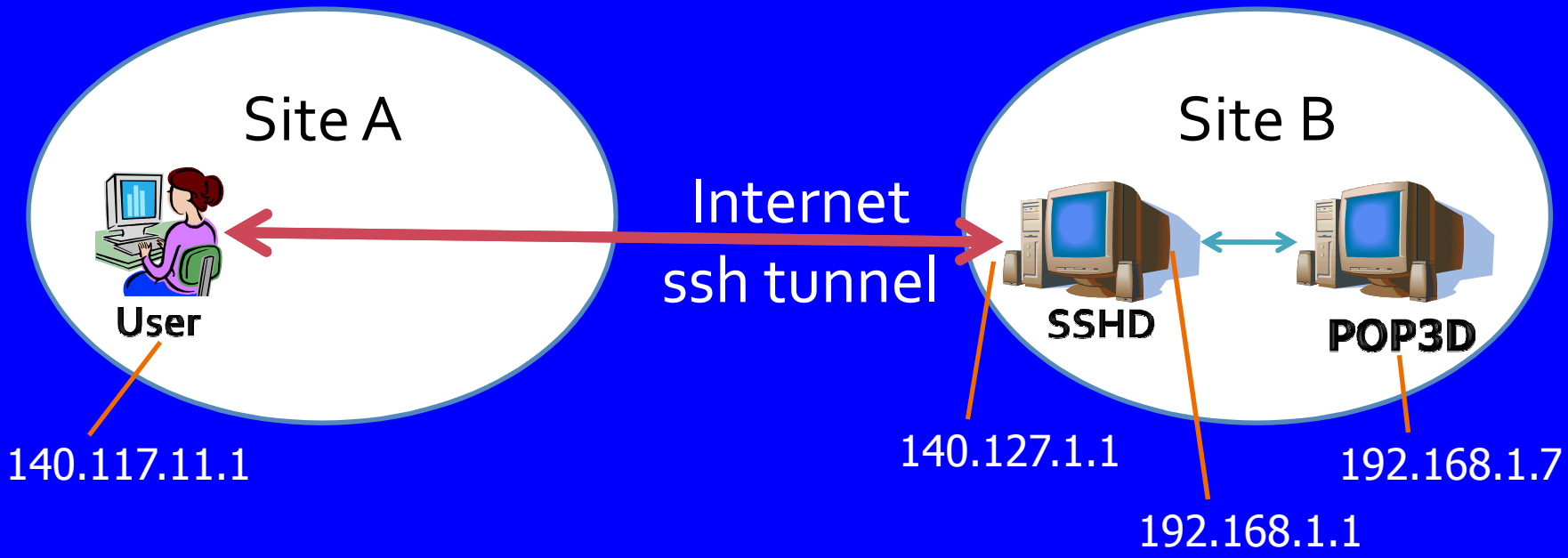


OpenSSH for Windows

- http://sshwindows.sourceforge.net/
- OpenSSH for Windows is a free package that installs a minimal OpenSSH server and client utilities in the Cygwin package without needing the full Cygwin installation.
- Daemon Quick Start
  - cd “C:\Program Files\OpenSSH\bin”
  - mkgroup -l >> ..\etc\group
  - mkpasswd -l [-u <username>] >> ..\etc\passwd
  - net start opensshd

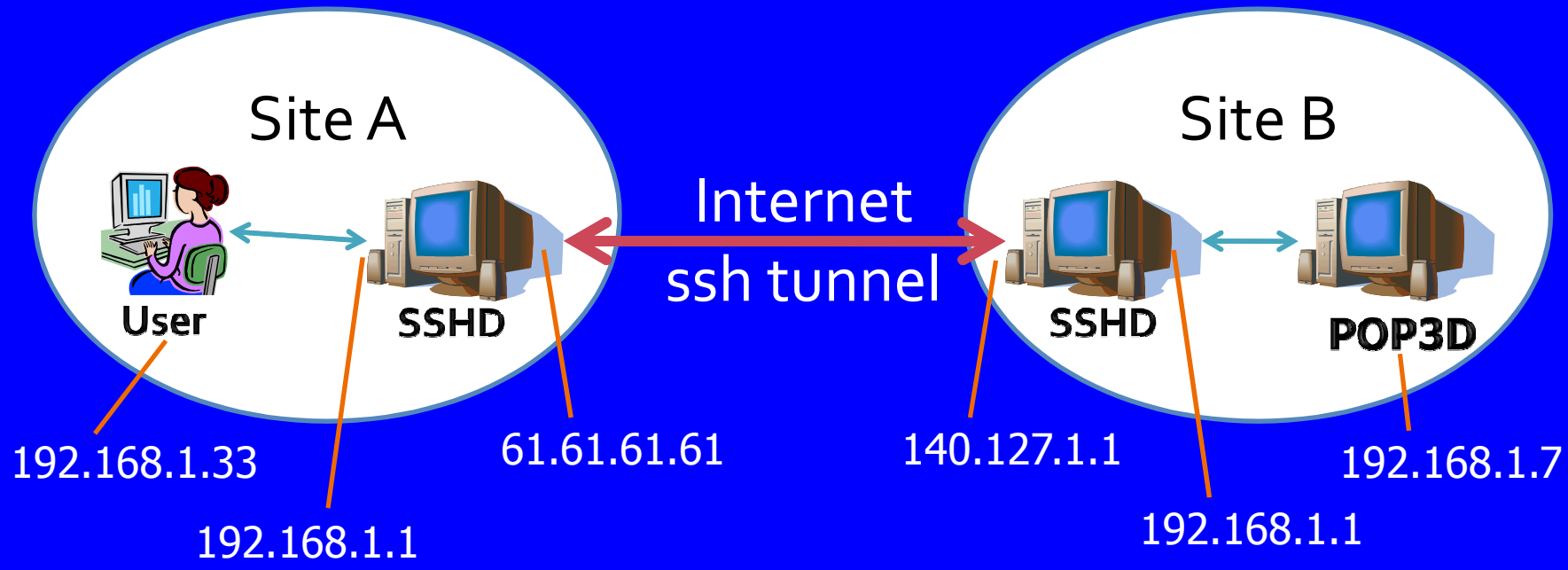
Port Forwarding Case 1

- Site B SSHD
  - 需有 aha 此帳號且需 allow 140.117.11.1 來連線
- User
  - 先利用 putty 做成 ssh tunnel
  - 收信軟體的 POP3 server 指向 127.0.0.1 即可



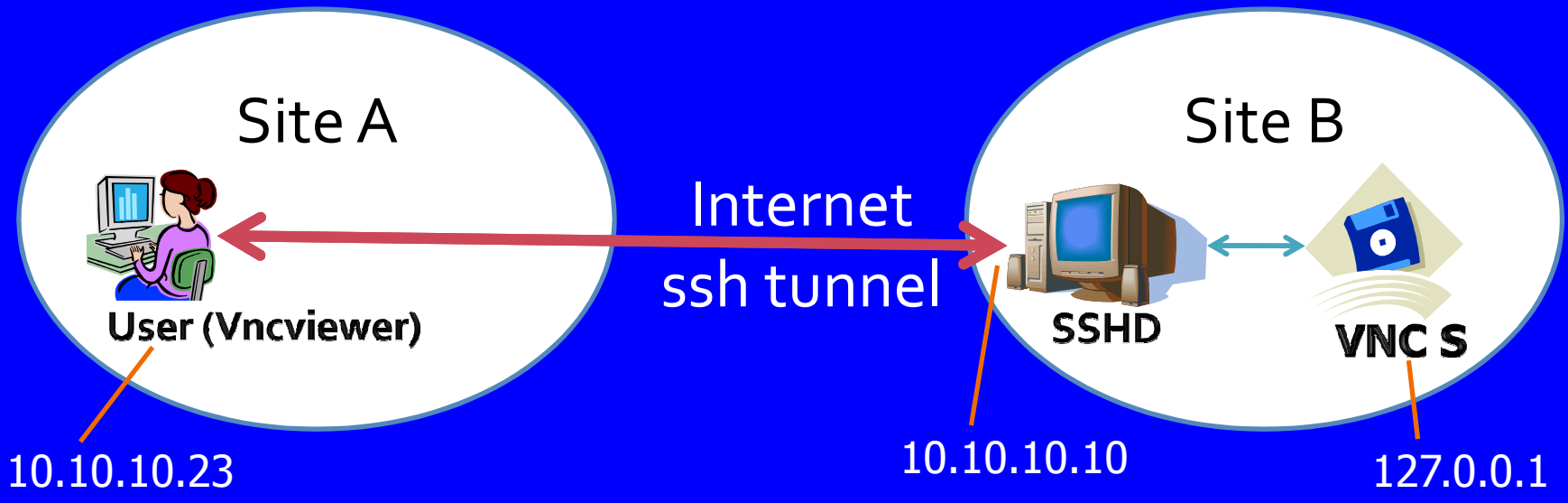
Port Forwarding Case 2

- Site A SSHD
  - ssh –f –L 192.168.1.1:110:192.168.1.7:110 aha@140.127.1.1 sleep 10000
- User
  - 收信軟體的 POP3 server 指向 192.168.1.1 即可
- Site B SSHD
  - 需有 aha 此帳號且需 allow 61.61.61.61 來連線



練習 1

- Site B SSHD
  - 需有 aha 此帳號且需 allow 10.10.10.23 來連線，VNC S 只允許 localhost
- User
  - 用 putty 連 10.10.10.10 port 22，forward localhost source port 5910 to destination localhost 5900
  - 注意！第一個 localhost 指 User 的 localhost，第二個 localhost 指 SiteB SSHD 的 localhost
  - Vncviewer 連 127.0.0.1:10 (亦即 5900+10=5910)



練習 2

- Site A SSHD
  - cd “C:\Program Files\OpenSSH\bin”
  - ssh –L 5900:127.0.0.1:5900 aha@10.10.10.33
- User
  - Vncviewer 連 127.0.0.1
- Site B SSHD
  - 需有 aha 此帳號且需 allow 10.10.10.12 來連線