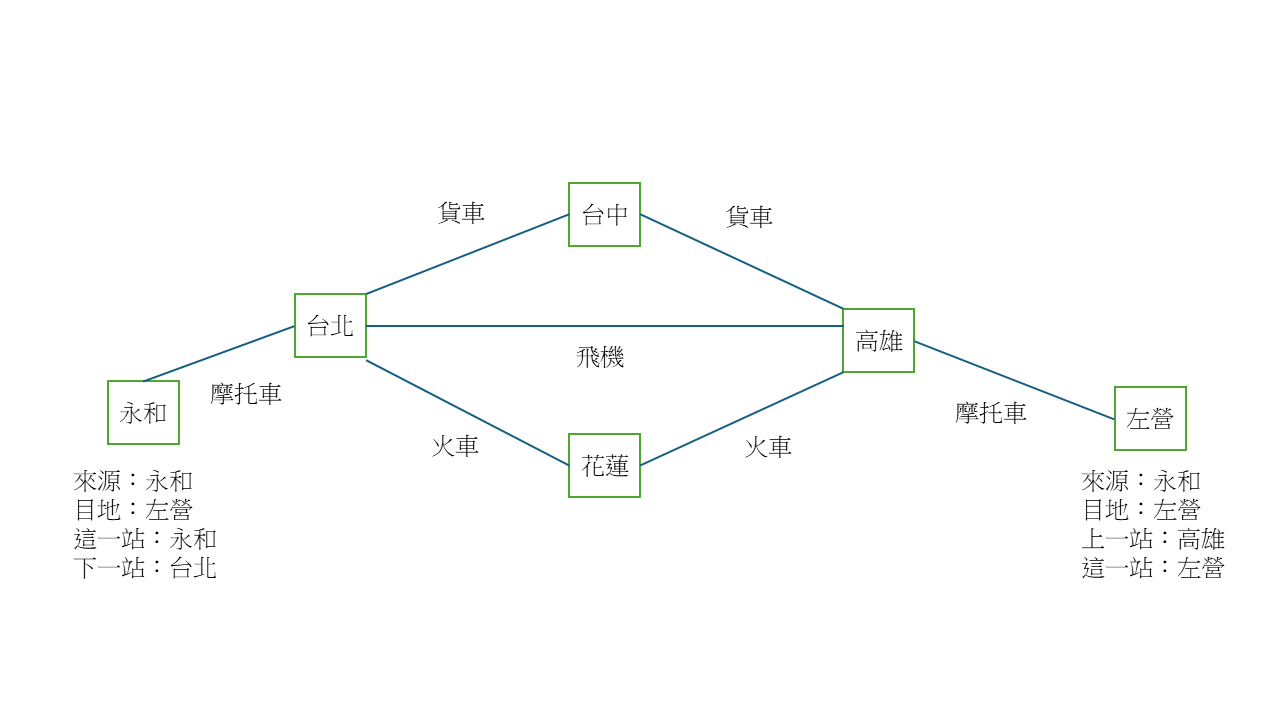
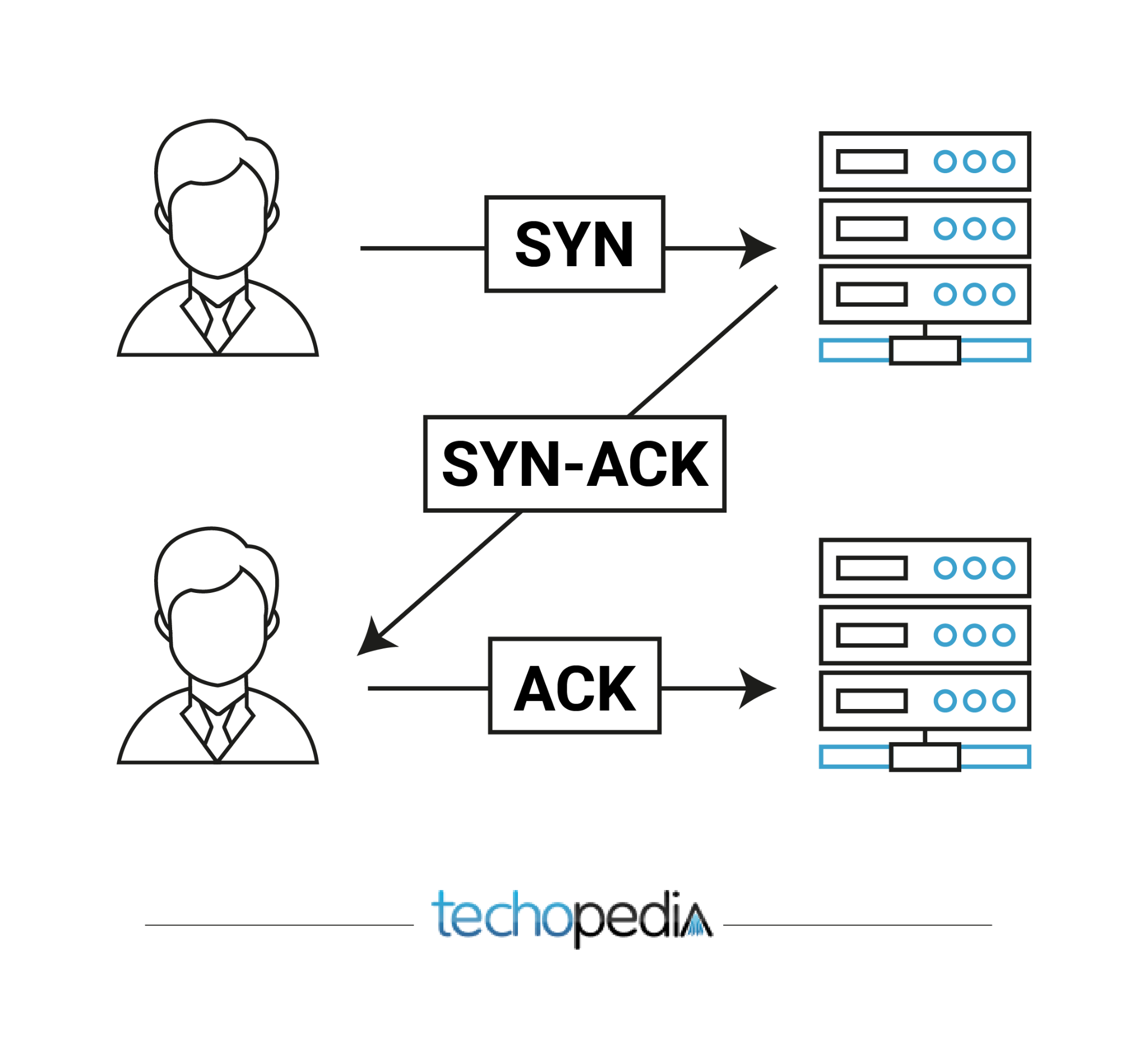
網路安全

**網路通訊協定基礎**

* OSI七層參考模型
  + 應用層 (Application Layer)：跟TCP/IP相同。
  + 表現層 (Presentation Layer)：TCP/IP沒有，將資料進行壓縮與解壓縮以提高傳輸效率。
  + 會議層 (Session Layer)：TCP/IP沒有，主要的功能是負責管理和控制不同應用程式之間的對話。
  + 傳輸層 (Transport Layer)：跟TCP/IP相同 。
  + 網路層 (Network Layer)：跟TCP/IP網際網路層 (Internet layer) 相同。
  + 資料連結層 (Data Link Layer)：跟TCP/IP網路存取層 (Netwrok Access Layer) 相同。
  + 實體層 (Physical Layer)：TCP/IP沒有，但與實體(電波、銅線、光纖)相關，設備有中繼器 (Repeater) 和集線器 (Hub) ，主要只是放大訊號。

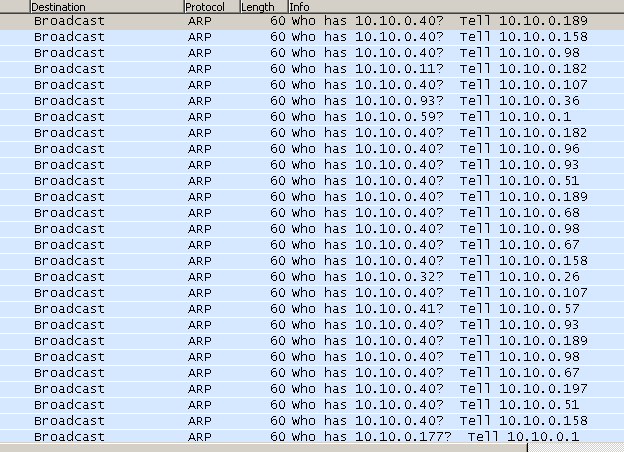
| **分層功能** | **TCP/IP 模型** | **OSI 模型** |
| --- | --- | --- |
| 應用程式協議 (應用程式) | 應用層(Application) | 應用層、表示層、會話層 |
| 端到端傳輸(Port) | 傳輸層(Transport) | 傳輸層 |
| 邏輯定址與路由(IP) | 網路層(Internet) | 網路層 |
| 實體定址與訊號傳輸(MAC) | 網路接入層 (Network Access) | 資料鏈路層 + 實體層 |



* IP就像是來源和目的，永遠都不會變，MAC Address就像是下一站，過程一直會變，實體層像是交通工具，不管是摩托車、火車、飛機、貨車(光纖、網路線、Cable)，只是傳輸性質發生變化，實際上傳輸的還是封包。
* TCP/IP協定架構
  + 應用層 (Application Layer)
    - 常見協定：HTTPS、DNS。
    - 應用防護：Web 應用程式防火牆 (Web Application Firewall，WAF)、代理伺服器 (Proxy)。
  + 傳輸層 (Transport Layer)
    - TCP (傳輸控制協定) ：可靠，三項交握協定 (SYN、SYN-ACK、ACK) 。

(資料來源：網際網路)

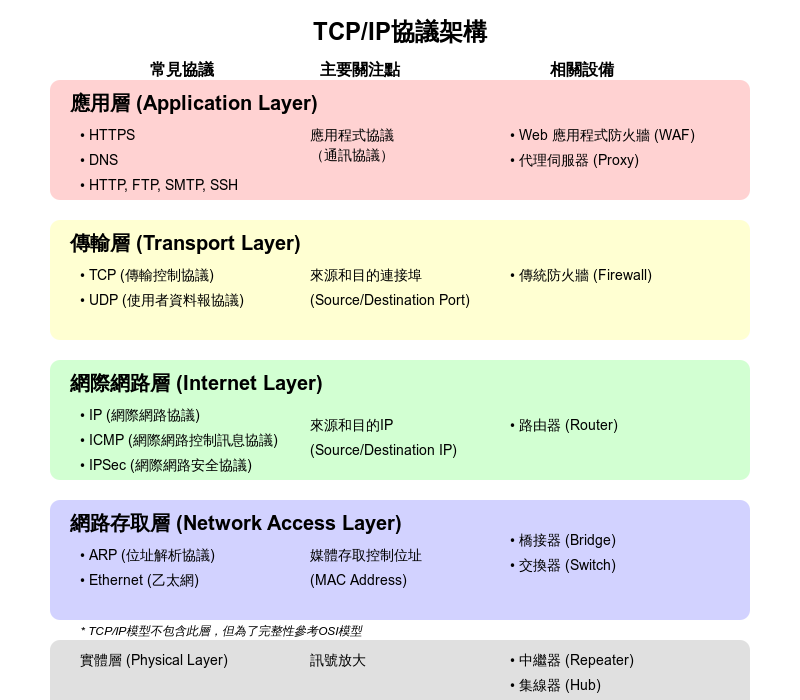
* + - UDP (使用者資料報協定) ：不可靠，適用於即時性高的通訊。
    - 應用防護：傳統防火牆 (Firewall)。
  + 網際網路層 (Internet layer)
    - 常見協定：IP (網際網路協定)、ICMP (網際網路控制訊息協定) 、IPSec (網際網路安全協定) 。
    - 設備：路由器 (Router)。
  + 網路存取層 (Netwrok Access Layer)
    - 常見協定：ARP (位址解析協定)：以 IP位址查詢其相對應之媒體存取控制 (MAC Address) 位址。
    - 設備：橋接器 (Bridge) 、交換器 (Switch) 。



(資料來源：網際網路，ARP範例)

| **階層** | **常見協議** | **主要關注點** | **相關設備** |
| --- | --- | --- | --- |
| 應用層 (L7) | HTTPS、DNS、FTP、SMTP、SSH | 應用程式協定、 實際字串或資料內容 | WAF、Proxy |
| 傳輸層 (L4) | TCP、UDP | 來源埠、目的埠 | Firewall |
| 網路層 (L3) | IP、ICMP、IPSec | 來源 IP、目的 IP | Router |
| 資料鏈結層(L2) | ARP | MAC Address | Bridge、Switch |
| 實體層 (L1) | – | 電波、銅線、光纖  電波／電訊號放大 | Repeater、Hub |

(資料來源：筆者整理，考試使用簡表)

(筆者自行整理)

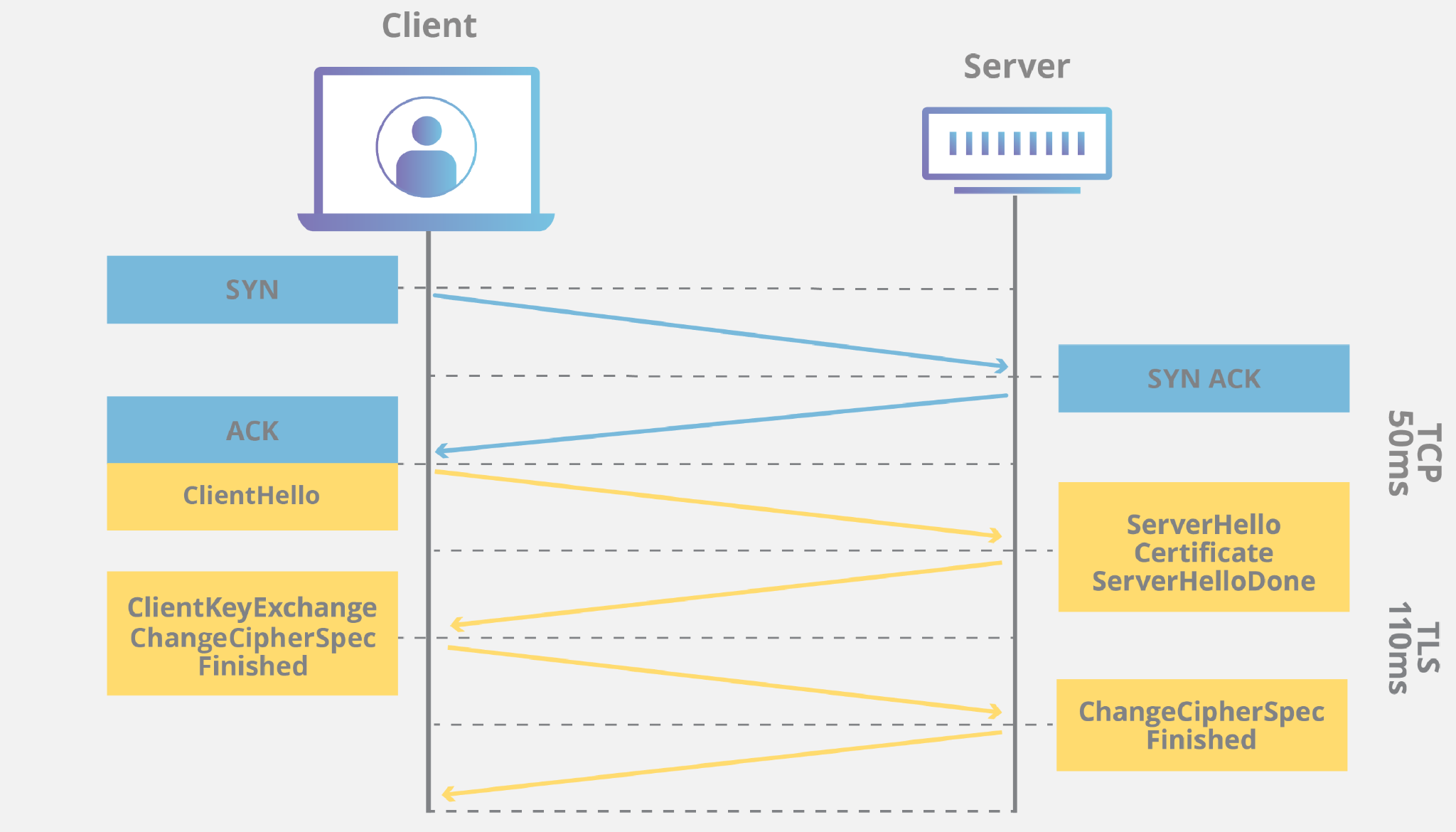
* 常見通訊埠 (Port) 服務
  + FTP：TCP 21
  + SSH、SFTP：TCP 22
  + TELNET：TCP 23
  + SMTP：TCP 25；加密SMTPS TCP 587
  + HTTP：TCP 80
  + NTP：UDP 123
  + HTTPS：TCP 443
  + SMB：UDP 137、138；TCP 139、445
  + DNS：UDP 53 (查詢) ；TCP 53 (Zone Transfer)
  + LDAP：TCP 389
  + POP3：TCP 110；加密POP3S TCP 995
  + Syslog：UDP 514
  + Microsoft SQL：TCP 1433
  + PPTP：TCP 1723
  + RADIUS：UDP 1812
  + RDP：TCP 3389
* 常見有無加密傳輸協定
  + 有加密：HTTPS、SSH、FTPS、SMTPS。
  + 沒加密：HTTP、Telnet、FTP、SMTP。
* 安全和不安全的技術
  + Wi-Fi 加密協議
    - 不安全：WEP、WPA、WPA2
    - 安全： WPA3
  + 檔案分享協議
    - 不安全：SMBv1、SMBv2
    - 安全：SMBv3
  + 網路管理協議
    - 不安全：SNMPv1、SNMPv2
    - 安全：SNMPv3
  + HTTPS加密協議：
    - 不安全：SSL1.0、SSL2.0、SSL3.0、TLS1.0、TLS1.1
    - 安全：TLS1.2、TLS1.3
  + 雜湊演算法
    - 不安全： MD5、SHA1
    - 安全：SHA2、SHA3
  + 資料加密演算法
    - 不安全：DES、3DES、RC4
    - 安全：AES
* 私有網路位置 (Private IP)
  + 10.0.0.0/8
  + 172.16.0.0/12
  + 192.168.0.0/16
* 網路位址轉換(Network Address Translation, NAT)
  + 定義：將內部私有 IP 位址轉換為外部公有 IP 位址，允許內部設備與網際網路通信。
  + 功能：
    - 減少公有 IP 使用數量。
    - 隱藏內部 IP 位址，提升內部網路安全性。
    - 支援內部網路使用私有 IP 位址。
  + 限制：NAT 不是防禦技術，無法防止暴力攻擊 (Brute Force Attack) 。
* 連接埠映射 (Port Mapping)
  + 定義：將外部網路的連接埠對應到內部網路的特定 IP 和連接埠，允許外部存取內部服務。
  + 功能：
    - 使外部使用者能存取內部網路服務。
    - 將外部請求導向指定的內部伺服器。
    - 支援遠端管理和服務提供(如遠端桌面、網站伺服器)。
  + 限制：開放連接埠可能增加安全風險，需謹慎設定存取控制。

**IPSec 傳輸模式**

* Transport Mode (傳輸模式) ：
  + 定義：僅保護封包的資料部分 (Payload) ，不加密 IP 標頭。
  + 特性：適用於端到端的通訊 (如兩台主機之間的加密通訊) 。
  + 加密範圍：
    - AH：驗證封包完整性，但不加密資料。
    - ESP：加密資料本身 (Payload) 。
  + 適用場景：內部網路的安全通訊。
* Tunnel Mode (隧道模式) ：
  + 定義：對整個 IP 封包 (標頭和資料) 進行加密，並封裝進新的封包。
  + 特性：適用於網路設備間的通訊 (如 VPN 伺服器間的加密通訊) 。
  + 加密範圍：
    - AH：驗證整個封包的完整性。
    - ESP：加密整個封包 (標頭和資料) 。
  + 適用場景：跨網路的安全通訊 (如遠端分公司 VPN)。

**TLS 傳輸模式 (Transport Layer Security)**

* 用途：保護網路傳輸，提供加密和完整性保護。
* 技術結合：
  + 非對稱加密：交換對稱密鑰 (Session Key) 。
  + 對稱加密：使用 Session Key 加密資料傳輸。
* Session Key：支援動態更新，定期重新產生密鑰以提高安全性。
* 版本建議：建議使用 TLS 1.2 以上，舊版本存在資安風險。
* 流程簡述：
  + TCP 三次握手 → 建立連線。
  + TLS 握手 → 交換憑證與密鑰，建立安全通道。



(資料來源：網際網路)

**考古題：**

9. 有關OSI模型中會議層（Session Layer）之敘述，下列何者正確？

(A) 主要的功能是負責管理和控制不同應用程式之間的對話 (會議層)

(B) 確保資料傳輸的可靠，並處理錯誤復原 (傳輸層)

(C) 處理封包的路由與轉發 (網路層)

(D) 將資料進行壓縮與解壓縮以提高傳輸效率 (表現層)

技術 113-2 答案A

10. 下列哪一種攻擊行為屬於OSI第七層（應用層）的DDoS攻擊手法？

(A) SYN Flood Attack (傳輸層)

(B) Fragmentation Attack (網路層)

(C) HTTP Flood Attack (應用層)

(D) UDP Flood Attack (傳輸層)

技術 113-2 答案C

14. 當電腦A位於防火牆B後面，只想要開放電腦A上的遠端桌面服務，供外部使用者可以從網際網路連線進入時，防火牆B應該設定下列何種功能最合適？

(A) Port Mapping

(B) Virtual Server

(C) DHCP

(D) DNS

技術 113-2 答案A

(NAT是由內而外，而Port Mapping是由外向內)

17. 在網路中，路由器（Router）是一種常見的網路硬體設備。下列何項是路由器的主要功能？

(A) 分配IP位址給網路中的裝置 (DHCP)

(B) 在區域網路（LAN）中將資料封包轉送到正確的裝置 (交換器)

(C) 為網路中的所有資料封包加密 (VPN)

(D) 負責將資料封包從一個網路轉送到另一個網路

技術 113-2 答案D

5. 在 OSI（Open System Interconnection Model）的參考模型中諸如 Chrome、 Firefox等瀏覽器軟體應該屬於下列何項層次？

(A) 應用層（Application Layer）

(B) 網路層（Network Layer）

(C) 資料連結層（Data Link Layer）

(D) 傳輸層（Transport Layer）

技術 113-1 答案A

(應用程式都在應用層)

6. 下列何項網路設備可以找出傳送封包的最佳路徑？

(A) 中繼器 (實體層)

(B) 橋接器 (資料連結層)

(C) 路由器 (網路層)

(D) 集線器 (實體層)

技術 113-1 答案C

9. 關於通訊埠（Port）預設端口的敘述，下列何項錯誤？

(A) SFTP，通訊埠 21 (通訊埠 22)

(B) RDP為遠端桌面，通訊埠 3389

(C) HTTP，通訊埠 80

(D) DNS，通訊埠 53

技術 113-1 答案A

11. 有關 TCP/IP（DoD）模型之敘述，下列何者有誤？

(A) 包含應用層（Application Layer）

(B) 包含會談層（Session Layer） (TCP/IP沒有)

(C) 包含網際網路層（Internet Layer）

(D) 包含網路存取層（Network Access Layer）

技術 113-1 答案B

12. 當企業有大量的內部網址時，會自行架設 DNS Server，如果

DNS Server的需求量較高，可能需要建置多台 DNS Server互相備援，並且使用一個特定功能來傳輸各台 DNS Server彼此的 DNS Record，讓每一台 DNS Server的紀錄都保持一致。但是如果該功能沒有限制存取來源，可能會導致任意使用者都可以透過該功能直接跟企業的 DNS Server索取該企業全部的 DNS Record，造成內部的網址外流。請問下列何項就是上述的特定功能？

(A) DNS Tunneling

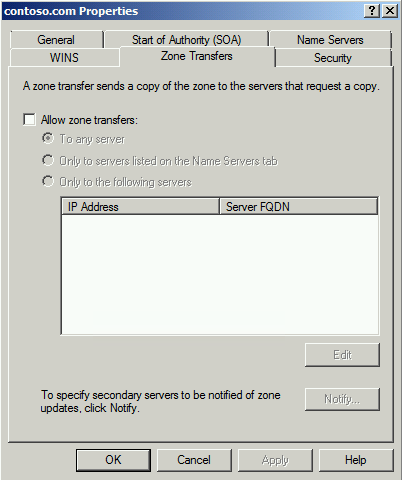
(B) DNS Amplification

(C) DNS Zone Transfer

(D) DNS Spoofing

技術 113-1 答案C

(企業架設多台 DNS Server 並需要保持紀錄一致時，會使用 DNS 區域傳輸（Zone Transfer） 來同步各伺服器之間的 DNS 紀錄。若此功能未限制存取來源，攻擊者可能透過區域傳輸取得企業全部 DNS 紀錄，導致內部資訊外流)



13. 下列哪一個通訊協定沒有經過加密傳輸，直接採用明文的方式傳輸，有機會被攻擊者竊聽？

(A) TELNET

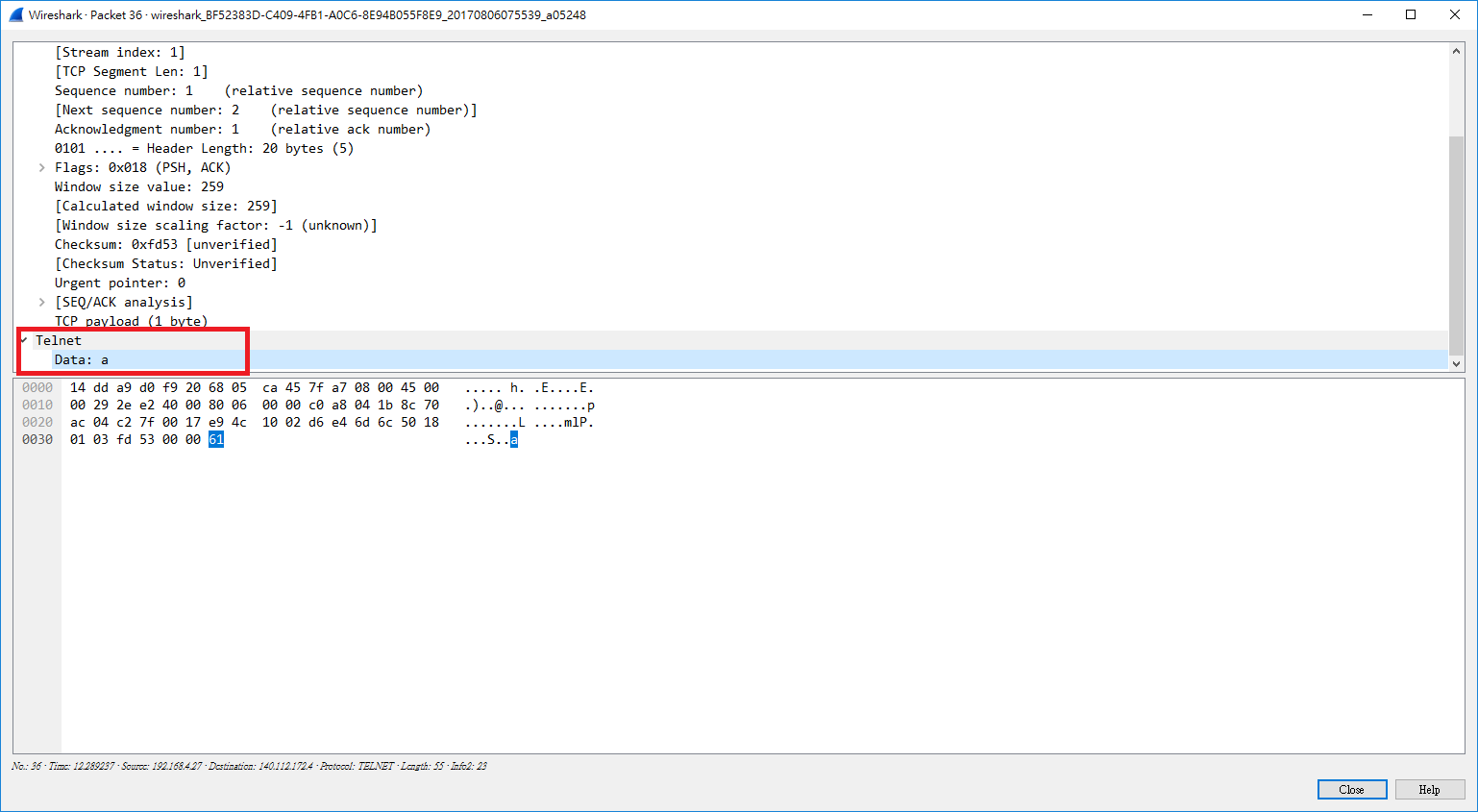
(B) FTPS

(C) HTTPS

(D) SSH

技術 113-1 答案A

(TELNET是明文傳遞)



18. 下列何者是微軟網路芳鄰會使用到的port？

(A) TCP 248

(B) TCP 445

(C) TCP 80

(D) TCP 20

技術 113-1 答案B

(網路芳鄰是使用 SMB協定來發現和連接到網路上的共享資源的。當你在網路芳鄰中看到其他電腦和共享資料夾時，實際上是 Windows 在背後使用了 SMB協定來進行通訊。)

10. 下列何項技術可以讓組織在公開網路上共用一個外部 IP位址，與外部只有一個接點有效隱藏內部網路，並能監控進入組織的資料兼具防火牆過濾功能？

(A) NAT

(B) DMZ

(C) VPN

(D) VLAN

技術 112-2 答案A

11. 有關位址解析協定（Address Resolution Protocol, ARP）功能之敘述，下列何者正確？

(A) 以IP位址查詢其相對應之媒體存取控制（MAC）位址

(B) 管理網路流量並決定封包路徑

(C) 對網路流量進行加密與解密，確保安全的通訊

(D) 控制網路流量以防止分段與碎片產生

技術 112-2 答案A

13. 中間人攻擊（Man-in-the-Middle Attack，又稱為 MITM Attack）是一種用來竊聽、竄改流量的攻擊行為。以下列舉了幾種用來防範中間人攻擊的防禦機制，請問哪一種防範機制已經被驗證有明顯的弱點並且 已被建議棄用？

(A) 將位址解析協定設定為靜態（Static ARP），避免ARP位址被污染

(B) 在 HTTPS或 SMTPS使用 SSLv2協定來保護傳輸資料，避免被看到明文內容

(C) 使用 DNSSEC來驗證 DNS的安全性，避免存取假冒的網域名稱

(D) 只使用家中自行設定的 Wi-Fi或 4G網路，並且連上網路之後全程使用公司 VPN，確保網路環境在掌控範圍之內

技術 112-2 答案B

(SSL或TLS建議使用TLSv1.2以上)

3. 請問在關於開放式系統互聯模型（Open System Interconnection Model, OSI）中，下列哪一層負責 IP之間的傳輸？

(A) 應用層（Application Layer）

(B) 表達層（Presentation Layer）

(C) 傳輸層（Transport Layer）

(D) 網路層（Network Layer）

技術 112-1 答案D

10. 以下關於TCP與UDP協定的特性，下列敘述何者較「不」正確？

(A) 兩者均屬於OSI模型中的傳輸層

(B) 兩者皆需進行三向式的握手程序

(C) TCP速度較慢、UDP速度較快

(D) TCP穩定性高、UDP穩定性低

技術 112-1 答案B

(只有TCP需要三向式的握手程序)

11. 關於通訊安全的敘述，下列何者錯誤？

(A) 當兩個系統進行通訊時，務必確保系統透過安全通道進行通訊，獲授權存取雙方使用共用資源

(B) 安全通訊端層（SSL）是對網際網路通訊提供隱私、驗證和整合性的安全性通訊協定

(C) SSL是通道加密，資料也加密保護

(D) 傳輸層安全標準（TLS）是標準網際網路通訊協定可以加密處理電子郵件，確保郵件在傳輸過程中安全不外洩

技術 112-1 答案C

(SSL僅加密傳輸資料，但資料本身需要透過額外的方式，例如7-zip或WINRAR軟體加密)

18. 當某 Windows電腦，想要開放遠端桌面服務供其他電腦連入時，而該服務採用預設設定，請問防火牆應該開放下列哪一個通訊埠（Port）？

(A) 53 (DNS)

(B) 23 (Telnet)

(C) 443 (HTTPS)

(D) 3389

技術 112-1 答案D

(遠端桌面連線Port為3389)

31. 請問 DNS快取污染 (DNS Cache Poisoning)是針對開放式系統互聯模型（OSI Model Open System Interconnection Model）的哪一層的攻擊？

(A) Layer 2資料連接層（Data-Link Layerl）

(B) Layer 3網路層（Network Layerl）

(C) Layer 4傳送層（Transport Layerl）

(D) Layer 7應用層（Application Layerl）

技術 112-1 答案D

(DNS就是屬於第七層應用層，因此是屬於應用層攻擊)

4. 下列何者為遠端使用者撥入驗證服務（Remote Authentication Dial In User Service,RADIUS）常使用之通訊埠（Port）？

(A) 1812

(B) 123

(C) 389

(D) 390

技術 111-2 答案A

5. 在網際網路的世界中，每台主機都需要使用 IP位址協定，才能相互溝通並傳送資料。請問下列哪一個 IP位址為公用 IP位址（非私人 IP）？

(A) 10.10.10.10

(B) 100.100.100.100

(C) 172.16.172.16

(D) 192.168.192.168

技術 111-2 答案B

(虛擬IP為10.0.0.0/8、172.16.0.0/12、192.168.0.0/16)

6. 通訊埠（Port）是應用層每種服務皆有的唯一埠號碼，其範圍介於 0~65536。其中 1024之前為公認通訊埠（Well-Known Port）關於通訊埠用途的敘述，下列何項錯誤？

(A) Port:53/TCP用途：DNS域名解析服務

(B) Port:123/UDP用途：LDAP輕型目錄存取協定 (TCP 389)

(C) Port:445/UDP用途：Microsoft-DS SMB檔案分享 (TCP 445)

(D) Port:995/TCP用途：基於SSL的 POP3收發電子郵件加密傳輸

技術 111-2 答案B、C皆送分

9. 請問可以將網際網路封包加密的是下列何項通訊協定？

(A) SMTP

(B) HTTP

(C) HTTPS

(D) FTP

技術 111-2 答案C

10. TCP三向交握（Three-way Handshake）的順序為下列何項？

(A) SYN，SYN/ACK，ACK

(B) SYN，ACK，SYN

(C) SYN，SYN，SYN

(D) ACK，SYN，SYN

技術 111-2 答案A

1. 下列 OSI模型層次，何者定義 IPSec協定？

(A) 資料鏈結層（Data Link Layer）

(B) 傳輸層（Transport Layer）

(C) 會議層（Session Layer）

(D) 網路層（Network Layer）

技術 111-1 答案D

6. 下列何者為輕型目錄存取協定（Lightweight Directory Access Protocol, LDAP）較常使用之通訊埠（Port）？

(A) 311

(B) 123

(C) 389

(D) 390

技術 111-1 答案C

7. 有心人士將電腦網卡設定為混雜模式，再加上由網路上下載網路監看

Sniffing）工具（如 Wireshark），就可以側錄到下列何種應用協定的密碼封包？

(A) IPSec

(B) PGP

(C) HTTPS

(D) Telnet

技術 111-1 答案D

(有加密：HTTPS、SSH、FTPS、SMTPS

沒加密：HTTP、Telnet、FTP、SMTP)

16. 開放式系統互聯模型（Open System Interconnection Model, OSI）中，下列哪些「不」是在傳輸層（Transport Layer）的攻擊手法？（複選）

(A) Smurf Attack (網路層， 使用icmp封包淹沒目標伺服器 所以是傳輸層)

(B) DNS Poisoning (應用層)

(C) SYN Flood (傳輸層)

(D) Ping of Death (網路層)

防護 111-1 答案ABD

44. 下列何者攻擊「不」屬於第七層攻擊？

(A) SQL Injection

(B) Command Injection

(C) Cross Site Scripting

(D) SSL Hijacking (傳輸層)

技術 111-1 答案D

49. 下列何者為超文本傳輸安全協定（HTTPS）較常使用之通訊埠

（Port）？

(A) 22

(B) 25

(C) 80

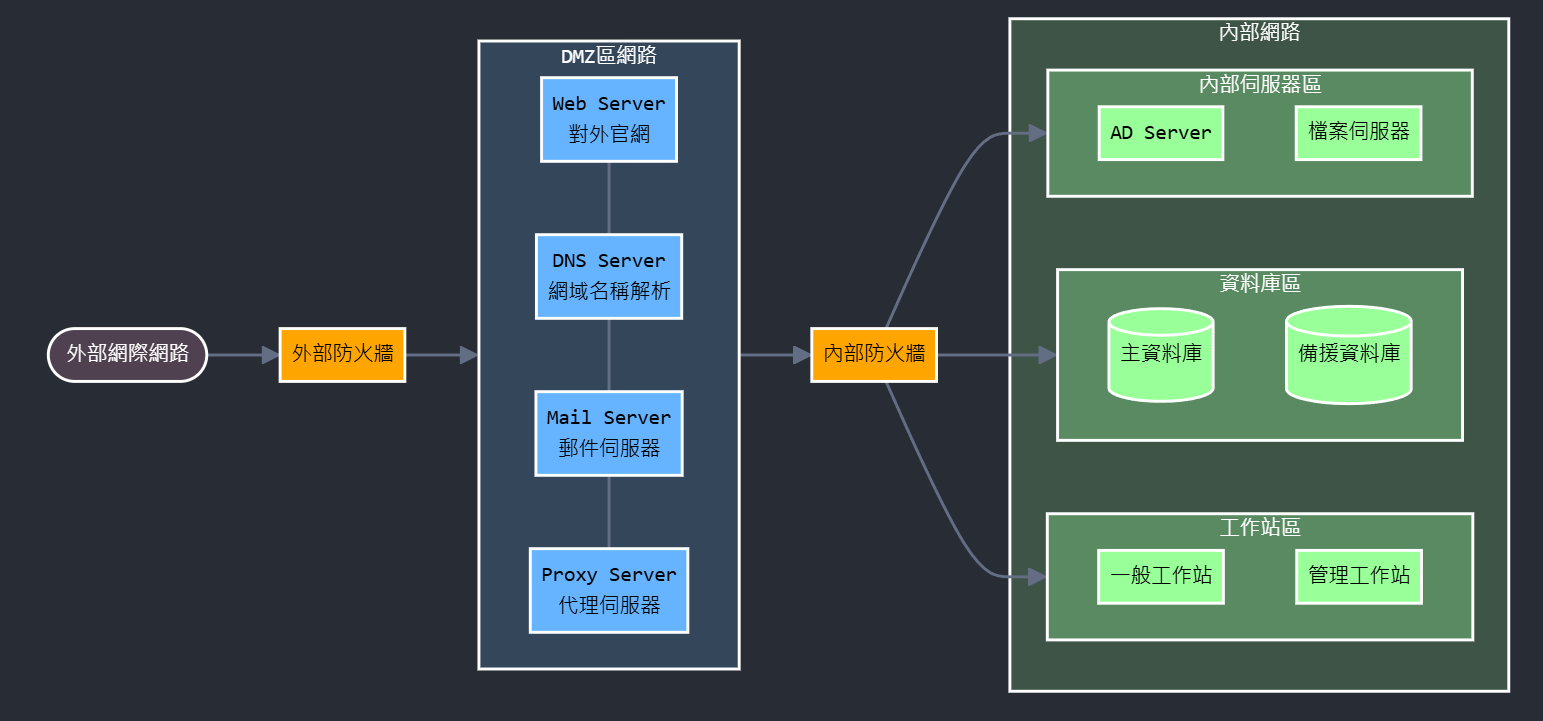
(D) 443

技術 111-1 答案D

資安設備

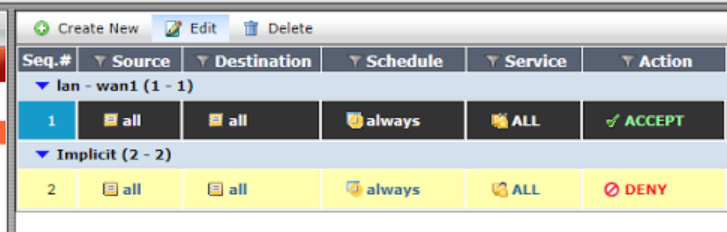
**防火牆(Firewall)**

* 防火牆類型
  + 封包過濾防火牆(Packet-filtering Firewall)：
    - 根據 IP 位址、通訊埠進行基本過濾控制。
  + 狀態檢查防火牆(Stateful Inspection Firewall)：
    - 動態追蹤和記憶連線狀態，自動允許已建立連線的往來通訊，不需額外設定規則。
  + 應用代理閘道防火牆(Application-Proxy Gateway Firewall)
    - 代理用戶請求並建立中間連線，提供精細的安全控制，例如可以下載但不能上傳。
    - 員工上網都要進過它，屬於應用層 ，能深入檢查協定細節，並透過抽換網站憑證查看實際通訊內容。
  + 網頁應用程式防火牆(Web Application Firewall, WAF)
    - 專門保護網站應用程式，匯入伺服器私鑰解密 HTTPS 流量，防止 SQL 注入、XSS 等攻擊。
* 防火牆架構：DMZ (Demilitarized Zone, 非軍事區)
  + 定義：
    - 位於內部網路與外部網際網路之間的一個隔離區域，用於放置公開服務(如網站伺服器、FTP 伺服器)，限制外部使用者直接存取內部網路。
  + 用途：
    - 將對外服務的伺服器與內部網路隔離，降低內部網路暴露風險。
    - 外部使用者只能訪問 DMZ 內的伺服器，無法直接接觸內部資源。
  + 架構示例：
    - 外部網際網路 → 外部防火牆 → DMZ區網路 → 內部防火牆 → 內部網路。
  + 常見服務：
    - Web 伺服器、DNS 伺服器、郵件伺服器、FTP 伺服器。



(DMZ區架構圖，資料來源：筆者自行整理)

* 防火牆規則：
  + 比對條件為：來源位置、目的位置、協定、來源埠、目的埠、網路界面和動作(允許或拒絕)
  + 規則執行順序：按照規則順序依次比對，**第一條成功比對的規則會被執行，後續規則不再比對**。
  + 若所有規則都不匹配，系統會套用隱藏的**拒絕所有規則**，因此可被視為一種白名單。



(資料來源：Fortinet防火牆介面)

**入侵偵測與防護(IDS/IPS)**

* 類型：
  + IDS (入侵偵測系統)
    - 被動型：僅監控異常活動，不主動防禦，通常僅發出警報 (如通知管理員) 。
  + IPS (入侵防護系統)
    - 主動型：可自動阻斷攻擊 (如丟棄惡意封包、重置連線) 。
* 安裝位置：
  + HIPS (Host-based Intrusion Prevention System)
    - 針對單一設備進行保護，通常監控主機的系統呼叫、檔案存取、登錄檔修改等，適合防護端點設備 (如伺服器、個人電腦) 。
  + NIPS (Network-based Intrusion Prevention System)
    - 部署於網路閘道 (如防火牆旁)，分析流量模式，適合防護大範圍網路攻擊 (如 DDoS、掃描行為)。
* 掃瞄規則：
  + 基於特徵的偵測 (Signature-Based)
    - 描述：根據已知攻擊模式的特徵碼 (Signature) 進行比對。
    - 優點：偵測已知攻擊模式的準確性高，誤判率低。
    - 缺點：無法發現未知攻擊，需要病毒特徵庫的更新才能檢測到新病毒。
  + 基於啟發的偵測 (Heuristic-Based)
    - 描述：透過模擬惡意程式的結構或行為特徵，根據經驗法則判定是否為潛在威脅，常見於沙箱 (Sandbox) 模擬執行環境，分析程式行為 (如嘗試修改系統檔案、大量寫入暫存檔) 。
    - 優點：能偵測未知病毒或全新惡意程式，即使沒有完整的病毒特徵碼，能檢測多態性 (Polymorphic) 惡意程式。
    - 誤判率較高，可能將正常程式或行為誤認為威脅，需平衡靈敏度與誤報率 (需調整閾值) 。
  + 基於異常的偵測(Anomaly-Based Detection)
    - 描述：建立正常行為的基準(Baseline)，透過偏離基準的行為來偵測異常活動，常用機器學習建立基準線(Baseline)，適用於檢測 APT (進階持續性威脅) 等長期潛伏攻擊。
    - 優點：適合偵測未知攻擊或複雜威脅，特別有效於動態環境或多態性惡意程式的行為分析，無需依賴特徵庫，適應新型攻擊。
    - 缺點：誤判率較高，正常偏差可能也被視為威脅，建立行為基準需耗費時間，動態環境 (如頻繁變更的網路架構) 可能需重新建立基準線。

**進階防護機制**

* 行動裝置管理 (MDM)
  + 定義：管理員工連線進公司內部網路存取資源的行動裝置。
  + 用途：設定在存取公司的信箱時，不能截圖和不能下載附件。
* 虛擬區域網路 (VLAN)
  + 定義：邏輯劃分實體網路為多個隔離的虛擬網路。
  + 用途：分隔流量、限制廣播領域 (Broadcast Domain) 範

圍、提升網路效率與安全性。

* 蜜罐 (Honeypot)
  + 定義：誘餌系統，模擬真實環境以吸引攻擊者。
  + 用途：偵測威脅、收集攻擊情報、誤導攻擊者。
* 虛擬私有網路 (VPN)
  + 定義：利用隧道技術建立安全加密的通訊連線。
  + 用途：保護資料隱私，實現遠端安全連線。
* 防毒軟體 (Antivirus)
  + 定義：透過特徵比對來偵測已知惡意程式。
  + 用途：防止病毒與惡意程式感染系統。
  + 掃描方式：
    - 基於特徵：根據特徵方式判斷，速度快也使用較少資源，但無法偵測全新病毒，誤判率低。
    - 基於啟發：根據檔案行為判斷，能偵測全新病毒，但是誤判率較高。
* 資料外洩防護 (DLP)
  + 定義：防止敏感資料未經授權被洩露或外傳。
  + 用途：保護個資、信用卡等敏感資訊。
  + 使用方式：因為網路上大多數資料都是加密，因此必須安裝在主機上，才能事先得知有無機敏資料。
* 端點偵測與回應 (EDR)
  + 定義：記錄所有端點上發生的活動和事件， 分析事件以偵測可疑行為，可協助使用者快速回應安全事件。
  + 用途：即時偵測威脅、隔離攻擊並調查來源，例如：封鎖惡意程式、記錄異常連線、回報給 SOC 分析。
* 網路偵測與回應 (NDR)
  + 定義： NDR 是一種資安技術，專注於分析網路流量中的異常行為，以識別潛在的威脅或攻擊活動。它通常使用機器學習與行為分析，來偵測傳統防禦工具難以發現的攻擊模式。
  + 用途： NDR 能持續監控東西向（East-West）與南北向（North-South）流量，即時發現未授權存取、資料外洩或橫向移動等異常行為。常與 EDR、SIEM 搭配，提升整體威脅可視性與回應能力。
  + EDR 負責「主機層」的安全監控與防禦，可即時對端點進行調查與隔離；NDR 則補足無法裝代理的裝置或監控整體「網路流量」，適合放在網路邊界或流量鏡像點。
* 擴展偵測與回應 (XDR)
  + 定義：XDR（eXtended Detection and Response）是一種整合式安全解決方案，將來自多種資安來源的資料（如：EDR、NDR、Email、Cloud、Identity 等）集中分析、關聯與回應，提供跨平台的威脅偵測與自動化應變能力。
  + 用途：XDR 解決了單一工具視角有限的問題，透過整合 EDR、NDR、SIEM、Email 安全、雲端防護等資料來源，可更準確識別進階威脅，降低誤判率，並自動協調各系統的回應動作。它通常由單一廠商提供統一介面與分析平台，提升可視性與效率。
  + 補充說明：XDR 雖具備高度整合與自動化能力，但仍需專業團隊持續監控與調校規則，因此在實務上常與委外的安全維運中心（SOC）服務結合。透過委外 SOC，由專業的資安團隊 24/7 運營 XDR 平台，提供事件通報、調查與應變處理，企業無需自建資安團隊即可享有即時防禦與回應能力。這類組合常稱為 MDR（Managed Detection and Response）服務，是企業導入 XDR 的常見策略之一。
* 安全資訊與事件管理 (SIEM)
  + 定義：收集並分析安全事件與日誌。
  + 用途：提供即時警報與威脅情報，協助快速反應。
* 安全協同自動化與回應 (SOAR)
  + 定義：整合人員、流程與技術，將安全事件的調查與回應流程自動化的進階平台。SOAR 可理解為具有自動化功能的資安平台，協助企業更有效率且智慧地處理資安事件。
  + 用途：
    - 安全編排 (Orchestration)：整合多種資安工具與系統。
    - 自動化 (Automation)：根據預設規則，自動執行調查與回應作業。
    - 即時回應 (Response)：快速處理與回應資安事件，縮短事件存活時間。
    - 支援決策與分析：整合 SIEM、EDR 等平台資料以協助判斷事件優先順序。
    - 事件稽核與報告：提供流程追蹤與稽核功能，便於事後檢討與合規。
* 安全維運中心 (SOC)
  + 定義：SOC 是組織中的集中式安全指揮中心，它利用人員、流程、技術，24/7 持續監控並提升安全狀態，同時預防、偵測、分析、回應網路安全事件。
  + 用途：
    - 主要：保護資產
    - 使用 SIEM 工具集中分析日誌，協助判斷是否遭受攻擊，並觸發後續調查或回應流程（SIEM 是 SOC 的核心分析工具）。
    - 可搭配 SOAR 平台進行自動化回應，例如：自動封鎖惡意 IP、通報資安團隊、觸發調查流程等。
    - 提供完整事件追蹤、通報與稽核流程，提升應變效率並減少人工負擔。
* 簡單網路管理協定 (SNMP)
  + 是一種應用層協定，用於網路管理員監視和管理網路上裝置的狀態和配置。
  + SNMP v1和v2有預設使用public的社群字串作為驗證機制，且以明文形式傳輸資料等問題，建議使用v3，它提供了使用者名稱和密碼的驗證機制，並支援資料加密和資料完整性驗證。
* 虛擬修補 (Virtual Patching)
  + 定義：安裝在主機上，監控已無維護的元件，使用類似HIPS的方式在封包進入主機前阻擋，降低受駭風險。
* 內容傳遞網路 (CDN)
  + 定義： CDN 是由分散在多個地理位置的伺服器所構成的網路，透過快取技術將網站內容儲存在接近使用者的位置，加速內容傳輸。
  + 用途： 提升網站載入速度、減輕原始伺服器負擔、降低延遲，並能緩解分散式阻斷服務（DDoS）攻擊的影響，提升網站的可用性與安全性。

**考古題：**

12. 在規劃企業資安的縱深防禦過程中，需要使用各種不同的技術與產品來應對不同情境的資安議題，下列哪一種技術最適合用來避免「內部資料被未經授權地傳輸到外部」的情況？

(A) 網路流量分析與回應（Network Detection and Response，NDR）

(B) 內容傳遞網路（Content Delivery Network，CDN）

(C) 入侵偵測系統（Intrusion Detection System，IDS）

(D) 資料外洩防護（Data Loss Prevention，DLP）

防護 114-1 答案D

(資料外洩防護（DLP）系統設計目的是防止內部敏感資料未經授權地傳輸到外部。它能識別、監控及控制資料流出企業網路，確保只有符合規定的資料流動，而非其他選項僅著重於偵測或分發流量。)

13. 有關「網頁應用程式防火牆（Web Application Firewall，WAF）」的描述，下列何者較為適切？

(A) WAF主要用於過濾電子郵件內容，防止垃圾郵件 (說明與 WAF 無關，屬於電子郵件過濾功能)

(B) WAF的規則有機會被攻擊者繞過，無法完全阻擋網頁攻擊 (網頁應用程式防火牆（WAF）雖然能夠有效防範許多已知攻擊，但其規則和簽名可能存在漏洞或被攻擊者透過變化繞過，因此無法保證百分之百攔截所有網頁攻擊)

(C) WAF只能用來防止OWASP Top 10 2021裡面的A03:2021 Injection (過於侷限 WAF 的功能範圍，實際上 WAF 可應用於多種攻擊類型)

(D) WAF只能阻擋已知特徵的SQL注入攻擊，但是特徵必須一模一樣，如果特徵稍微有變化WAF就無法阻擋 (過於侷限 WAF 的功能範圍，實際上 WAF 可應用於多種攻擊類型)

防護 114-1 答案B

16. 安全性資訊與事件管理（Security Information and Event Management，SIEM）是蒐集、分析、關聯日誌，並且提供即時的警報與威脅檢測，可針對事件回溯與調查，當我們設定要將一台Windows Server 2019的安全性事件，拋送回到SIEM進行分析，可以透過下列哪些通訊協定無需額外的透過cmd指令串接、設定、組態即可傳送？（複選）

(A) Syslog（System Logging Protocol） (多數 SIEM 系統支援 Syslog 協定，可以直接接收來自 Windows Server（通常透過代理或內建支援）傳送的安全性事件，而無需額外的 cmd 指令組態)

(B) SNMP（Simple Network Management Protocol） (通常用於網路裝置的管理與監控，不適合直接用來傳送 Windows 安全事件)

(C) Agent-Based (使用代理程式來收集並傳送事件到 SIEM 是一個常見做法，代理程式可自動運作，不需要額外透過命令列設定)

(D) Windows Event Forwarding（WEF） (這是 Windows 內建的功能，可將安全性事件轉發給指定的收集器，配置相對簡單且不需要額外命令)

防護 114-1 答案ACD

18. 關於設計供應鏈遠端存取架構的敘述，下列何項最「不」適切？

(A) 身份識別應該要有多重身份驗證機制（MFA）

(B) 可以透過虛擬私人網路（Virtual Private Network，VPN）做存取控制

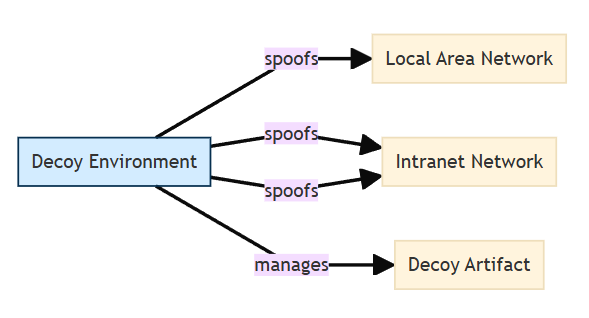
(C) 使用資料外洩防護（Data Loss Prevention，DLP）即可做到個人資料保護

(D) 可以透過傳輸加密保護營業秘密

規劃 114-1 答案C

(雖然資料外洩防護（DLP）可以協助監控與防止敏感資訊的外洩，但僅依賴 DLP 並不足以達成個人資料的全面保護。個人資料保護除了需要防止資料外洩之外，還涉及隱私權、存取管控、加密傳輸等多層面措施。)

23. 如附圖所示。誘餌環境（Decoys Environment）常被稱為密罐（Honeypot），被拿來偵測、吸引與分析網路攻擊，用於欺騙並轉移攻擊者對關鍵系統的注意力，而達成提前預警回應的控制措施之一。關於誘餌環境相關敘述，下列何者「最不正確」？



(A) 誘餌（Decoys）是一種仿真的數位人造物、物件或現象，旨在欺騙攻擊者的監控設備或誤導其評估。例如：假的 - 文件、帳戶、主機和網段…等

(B) 整合式蜜網（Integrated Honeynet）於生產環境中設置誘餌以吸引攻擊者互動，但攻擊者有機會利用其位置進行網路流量竊聽

(C) 連接式蜜網（Connected Honeynet）連接到生產環境的誘餌服務、系統或環境，模擬特定功能而不暴露系統完全存取權，可完整偵測新攻擊模式與識別零日漏洞攻擊

(D) 獨立式蜜網（Standalone Honeynet）為吸引攻擊者並引出其行為而創建的環境，該環境不連接到任何生產系統，相較於整合式蜜網與連接式蜜網的風險更低

防護 114-1 答案C

(「連接式蜜網（Connected Honeynet）」確實可能連接到生產環境，但選項 (C) **誇大**了它可以「完整偵測新攻擊模式與識別零日漏洞攻擊」的能力。雖然蜜網能協助捕捉攻擊手法與樣本，但並不能保證**完全**偵測所有新攻擊或「自動」識別所有零日漏洞。)



2. 下列何項「不」是過濾型網路防火牆所過濾的網路封包參數？

(A) 來源端IP Address

(B) 目的端IP Address

(C) 來源端TCP/UDP Port

(D) 目的端MAC Address

技術 113-2 答案D

(MAC Address非防火牆所過濾之參數)

5. 附圖為防火牆的過濾規則表及封包資訊。在判斷封包是否通過防火牆時，請根據規則表來決定並選擇正確的選項。請問該封包依據防火牆規則是否通過，以及符合哪條規則？



(A) 通過，符合規則1

(B) 通過，符合規則3

(C) 通過，符合規則4

(D) 被拒絕，符合規則5

技術 113-2 答案D

(不符合任何一條防火牆規則，因此最後一條隱藏拒絕)

17. 某公司新增了一業務型態，員工（20員，每員配置筆電乙部以及隨身硬碟乙顆）必須至客戶端長期駐點處理有關受託業務，並於客戶端透過網際網路連線回公司內部網路處裡公司相關業務，為了降低此一新增業務型態所衍伸出來的資安風險，該公司正評估採取有效的控制措施來降低此風險，請問下列控制措施何項較無法降低此風險？

(A) 網站應用防火牆（Web Application Firewall WAF） (WAF 主要用於保護網路上的 Web 應用程式，針對 HTTP/HTTPS 流量進行過濾及防護。此情境中，重點在於遠端員工透過網際網路連線回公司內部網路，並非針對 Web 應用程式的防護，因此 WAF 較無法降低此一新增業務型態所衍生的資安風險)

(B) 端點偵測及應變機制（Endpoint Detection and Response EDR）

(C) 虛擬私有網路（Virtual Private Network VPN）

(D) 防毒軟體（Antivirus Software）

規劃 113-2 答案A

18. 關於網路安全架構中的基本要素，下列何項敘述「有誤」？

(A) 包含雲端儲存設備 (雲端儲存主要是提供資料儲存、備份或協作服務，並非直接用於防護網路安全的設備，它反而需要被安全架構所保護，是被保護的對象而非保護措施。基本的網路安全架構通常著重在防護設備與技術，如防火牆、入侵偵測/防禦系統、VPN 等，而雲端儲存設備並非其中之一)

(B) 包含防火牆設備

(C) 包含惡意軟體偵測設備

(D) 包含虛擬私人網路（VPN）設備

規劃 113-2 答案A

19. 規劃端點安全架構時，納入端點偵測及應變機制（Endpoint Detection and Response，EDR）的最主要目的之敘述，下列

何者正確？

(A) 防禦網路入侵行為

(B) 監控端點入侵行為 (主要的功能是持續監控端點（如筆記型電腦、桌面電腦等）上的活動，收集並分析異常事件資料，以偵測可能的惡意行為或入侵行為，並在發現異常時迅速回應處理。這與傳統防火牆等網路設備防禦網路流量的作法有所不同，因此其主要目的是針對端點內部發生的安全事件進行監控與偵測)

(C) 管理端點網路流量

(D) 管理端點資料傳輸

規劃 113-2 答案B

30. 請問下列哪一項防護措施是主要針對惡意程式的防護方法？

(A) 將所有電腦系統與網路斷開連接，避免受到外部攻擊

(B) 定期備份重要資料，防止資料遺失

(C) 安裝防毒軟體，並定期更新病毒碼

(D) 僅下載來自知名網站的檔案，避免受到釣魚攻擊

技術 113-2 答案C

46. 組織內員工可以使用個人擁有的智慧型手機或平板等行動裝置執行組織內的業務的狀況，可適應移動辦公趨勢，滿足現代行動化商務需求，其優點非常多，但不包括下列何項？

(A) 使用個人的行動裝置可以提高工作效率

(B) 個人裝置由個人保管，減少資料外洩的風險 (反而是增加風險)

(C) 減少組織購買設備的費用

(D) 組織透過行動裝置管理系統（Mobile Device Management, MDM）管理組織內的行動裝置，主要目的在於限制行動裝置可以從事的行為

技術 113-2 答案B

3. 下列何項是正確的防火牆策略設定機制？

(A) 經適當的申請流程後即可無限期使用 (定期盤點)

(B) 保護服務主機的防火牆，可預設允許由主機連出internet的連接

(C) 防火牆策略應由受過專業訓練的人員審核及設定

(D) 「黑名單」的設定方式優於「白名單」 (應該是白名單為其他拒絕連線較安全)

技術 113-1 答案C

4. 某公司建置的測試區域遭受駭客入侵，導致重要客戶資料外流。以

下哪些選項可作為前述資安問題的改善措施？（複選）

(A) 避免使用真實資料做為測試資料

(B) 強化防火測試區防火牆管理

(C) 在公司測試系統輸入重要客戶資料 (這與 (A) 相反，會增加資料外洩的風險，是絕對應該避免的行為，測試環境的安全等級通常低於正式環境，不適合存放重要資料)

(D) 將測試區與公司正式區實施安全、明確之區隔

規劃 113-1 答案 ABD 或 AD

8. 建置虛擬私有網路（Virtual Private Network VPN）的主要目的是下列何項？

(A) 加速網路連接，增加下載檔案的速度

(B) 增加網站流量，創造瀏覽次數

(C) 保護網路傳輸的資料安全

(D) 阻擋廣告，避免廣告消耗網路頻寬

技術 113-1 答案C

10. 有關防火牆進行封包過濾時所考慮之因素，下列描述何者最

「不」適切？

(A) 僅考慮封包的目的位址

(B) 封包的協定

(C) 封包的連接埠編號

(D) 封包的網路界面

技術 113-1 答案A

(需要考慮來源位置、目的位置、協定、來源埠、目的埠、網路界面和動作(允許或拒絕))

17. 關於端點偵測及回應（ Endpoint Detection and Response EDR）的作用敘述，下列何者較「不」正確？

(A) 記錄所有端點上發生的活動和事件

(B) 分析事件以偵測可疑行為

(C) 可協助使用者快速回應安全事件

(D) 能夠完全防止所有端點安全事件發生 (沒有任何安全解決方案可以保證 100% 的安全性。EDR 雖然可以大幅提升端點安全防護能力，但它主要側重於 **偵測和回應**，而不是 **完全防止**。新的攻擊手法不斷出現，零時差攻擊也難以預防。EDR 的目標是盡可能地縮短偵測和回應時間，降低安全事件造成的影響。這是**不正確**的敘述。)

規劃 113-1 答案D

24. 網站應用程式中的元件存在弱點，若要有效避免遭受攻擊者利用的改善措施，下列何者錯誤？

(A) 移除不必要的元件、功能或檔案

(B) 持續盤點用戶端與伺服器端元件的版本，並確認是否含有漏洞

(C) 僅從官方網站與知名論壇取得相關元件

(D) 監控已無維護的元件，可透過虛擬修補（Virtual Patch）降低受駭風險

技術 113-1 答案C

(優先從官方網站取得元件。

驗證元件的完整性，例如使用官方提供的雜湊值 (hash) 進行比對。

即使是從官方取得的元件，也需要保持警惕並持續監控其安全性。)

39. 關於安全性資訊與事件管理（SIEM）的敘述，下列何者較「不」適切？

(A) SIEM結合了安全相關的資訊管理及事件管理

(B) SIEM用途包含偵測攻擊

(C) SIEM不會有誤報與誤判的問題

(D) SIEM側重於日誌的集中式管理和審計

技術 113-1 答案C

(只要是判斷就會有假陽性和假陰性的問題)

41. 入侵偵測與防禦系統（Intrusion Detection and Prevention Systems IDPS）可以主動反應偵測到的威脅，下列敘述何項最「不」適切？

(A) 發出入侵警告訊息

(B) 記錄入侵事件

(C) 可即時阻擋所偵測到的威脅

(D) 將入侵者引導到 DMZ（Demilitarized Zone）區

技術 113-1 答案D

(這個選項描述的行為更接近於蜜罐(Honeypot) 技術，而蜜罐通常是獨立系統，不是 IDPS 的標準功能。將入侵者引導至蜜罐屬於一種誘捕的手段，而DMZ並非誘捕入侵者的環境)

48. 關於行動裝置的安全保護措施，下列敘述何者錯誤？

(A) 軟體下載與使用應該檢視權限的要求，確保沒有資料外洩的風險

(B) 軟體應自動或定期手動安裝更新修補程式

(C) 資安威脅不會影響行動裝置的電池壽命

(D) 行動裝置管理系統（Mobile Device Management, MDM）會限制行動裝置的行為，甚至可以遠端變更與清除行動裝置的內容

技術 113-1 答案C

(資安威脅（如惡意軟體）可能會在背景執行大量任務，導致電池消耗加快，進而影響電池壽命)

8. 在系統或網路之間建立一條虛擬的專屬通道，屬於下列何種網路安全技術？

(A) DMZ

(B) Tunneling

(C) VLAN

(D) NAT

技術 112-2 答案B

9. 有關防火牆之敘述，下列何者錯誤？

(A) 防火牆是安裝在多個網路之間的網路安全防護裝置，主要目的係用來過濾資料封包

(B) 防火牆是提供控制存取網路資源等服務

(C) 封包是輸入向的（Inbound）都應先經過防火牆的檢查，輸出向的（Outbound）封包則無需檢查

(D) 封包必須符合管理者制定之規則才能予以放行，以防止內部網路受到攻擊

技術 112-2 答案C

(不管輸入和輸出都要檢查)

11. 關於進行網路架構設計的敘述，下列何者較「不」適當？

(A) 應區分內外網

(B) 網站跟資料庫最好在不同網段

(C) 目錄伺服器AD應該放在辦公網段 (目錄伺服器 AD (Active Directory) 儲存著組織內重要的使用者帳戶、權限等資訊，屬於核心系統，需要高度安全保護。將 AD 放在辦公網段會增加風險，因為辦公網段通常有較多使用者和設備，更容易受到攻擊或內部威脅。最佳實務是將 AD 伺服器放在**獨立且高度安全的網段**，並嚴格限制訪問權限。甚至可以再細分為僅放網域控制站(DC) 的網段，以及放應用程式的網段。)

(D) 可以透過VLAN 切割網段

防護 112-2 答案C

18. 關於網路規劃的敘述，下列何項較「不」安全？

(A) 對外服務的伺服器，設置於防火牆的DMZ區

(B) 外部分支機構須以VPN連入公司內網

(C) 將所有使用者與伺服器置於同一網段 (不同保護的等級伺服器須放置不同網段)

(D) 使用入侵防護系統（IPS）協助維護內部網路安全

規劃 112-2 答案C

19. 某廠商其日誌服務採用syslog，該伺服器A另有透過防火牆強化保護，公司的伺服器B要傳輸日誌給伺服器A時，發現無法正常傳輸，但伺服器B 透過ping確認其與伺服器A可以正常連線並取得回應，請問下列那項方案最合適解決此項狀況？

(A) 重新安裝伺服器A的syslog

(B) 於該防火牆放行目的埠號514的UDP 流量

(C) 移除保護伺服器A的防火牆設備

(D) 將伺服器B移至與伺服器A相同的網段 (這是一種繞過防火牆的權宜之計，且可能涉及網路重構，不僅增加管理複雜性，還可能不符合公司的網路設計策略。)

防護 112-2 答案B

(由於 **syslog** 使用 **UDP 514 埠**，防火牆可能阻擋了這個埠的流量，導致 **伺服器B** 無法傳輸日誌。放行 **UDP 514 埠** 的流量可以允許 **syslog** 資料順利傳輸。)

20. 端點偵測與回應（Endpoint Detection and Response EDR）係指可偵測並調查主機以及端點上的一些可疑活動，並透過自動化方式通知資安團隊進行快速回應的資安措施，關於EDR所提供的主要功能的敘述，下列哪些正確？（複選）

(A) 主動監控端點，並針對具有威脅跡象的活動收集資料

(B) 對蒐集的主機弱點執行分析，以識別是否有任何未知的威脅模式 (弱點掃描工具)

(C) 針對所有已識別威脅產生自動回應，以移除或遏止威脅

(D) 利用分析和鑑識工具，針對可能導致其他可疑活動的已識別威脅執行研究

規劃 112-2 答案ACD

23. 請問關於「安全性資訊與事件管理」（簡稱SIEM）的描述，下

列哪些較正確？（複選）

(A) 可協助組織在威脅傷害企業營運之前，先進行偵測、分析和回應安全性威脅

(B) 缺乏記錄管理的功能 ( SIEM 系統具有強大的日誌管理功能。它能夠收集、儲存、正規化和分析來自各種來源的大量日誌資料。日誌管理是 SIEM 的基礎功能之一，它為威脅偵測、事件調查和合規性報告提供了必要的資料。)

(C) 讓組織就可以迅速回應潛在的網路攻擊，並滿足合規性要求

(D) 結合了安全性資訊管理（SIM）和安全性事件管理（SEM） (SIEM 系統結合了SIM 和 SEM 的功能。SIM 專注於長期儲存和分析日誌資料，主要用於合規性報告和歷史事件調查。SEM 則專注於即時監控和分析安全事件，並提供警報和回應功能。SIEM 將兩者結合，提供了一個全面的安全監控和管理平台。)

防護 112-2 答答案ACD

1. 對於各式網路攻擊之防禦措施，以下敘述何者最正確？

(A) 入侵防禦系統（IPS）無法偵測網路攻擊，僅能進行阻擋 (IPS有不阻擋模式)

(B) 使用防火牆能有效阻擋分散式阻斷服務（DDoS）攻擊 (防火牆不能有效阻擋DDoS，DDoS可以ISP清洗流量或CDN阻擋)

(C) 透過佈署密罐（Honeypot）服務可偵測異常網路活動

(D) 入侵偵測系統（IDS）可偵測網路攻擊，並進行阻擋 (IDS僅能提供偵測，不能阻擋)

技術 112-1 答案C

9. 可以使用下列何者，降低廣播領域（Broadcast Domain）範圍？

(A) Virtual Local Area Network（VLAN）

(B) Network Address Translate（NAT）

(C) Dynamic Trunking Protocol（DTP）

(D) Inter-Switch Link（ISL）

技術 112-1 答案A

(VLAN技術可以降低降低廣播領域)

12. 有關防火牆功能之敘述，下列何者錯誤？

(A) 過濾一般用戶所禁止的網路服務，許可之網路服務則無須過濾

(B) 具有內部使用者與外部網站伺服器不會建立雙方之TCP/IP連線，而是透過內部防火牆以網頁用戶端的身分向外部網站要求存取網頁資料的應用代理閘道防火牆（Application-Proxy Gateway Firewalls）功能

(C) 可以隱藏內部 IP位址，讓外部無法得知內部網路實際 IP的網路位址轉譯（NAT）模式

(D) 可以在不修改網路設備的設定下，提供動態封包過濾功能的透通橋接模式（Transparent Mode）

技術 112-1 答案A

(就算是許可之網路服務也要進行IPS或防毒的過濾)

12. 當網路防火牆受到偵測攻擊時，下列何者最「不」適宜？

(A) 對外管理Port應該關閉

(B) 最高權限應該提供給維護廠商 (應該自行保管)

(C) 定期檢視規則是否過期

(D) 告警應該有專人確認與處置

防護 112-1 答案B

13. 企業外部網路可以包含組織的內部網路與外部夥伴組織之間的連結，夥伴可能是供應商或委外廠商等，為了讓互相信任的組織進行連線可以透過專線或架設虛擬私有網路來完成，其技術名稱為下列何項？

(A) VPN

(B) LAN

(C) DMZ

(D) NAT

技術 112-1 答案A

(VPN可以建立一條安全的虛擬通道讓從網際網路連到公司內部)

47. 疫情期間，居家上班成為重要防疫處置，某 IC設計公司，擔心員工在家使用Smartphone或Laptop收發公司郵件，恐有附件機密資料外洩疑慮，下列哪一個選項，「最不具備」資料保密措施？

(A) 手機透過 VPN登入公司網路，在虛擬化桌面環境（VDI）中收取電子郵件，無法讓附件儲存在個人手機中

(B) 讓公司員工直接遠端（RDP）登入到公司配發個人電腦，收發電子郵件

(C) 公司配發專用手機，手機充電孔已不具備資料傳輸能力， NFC也被禁用，必須透過 VPN才能連線公司郵件伺服器

(D) 公司配發專用 Laptop，且安裝資料外洩防護 DLP進行管控外接儲存裝置、網路傳輸活動，必須透過VPN連上公司郵件伺服器

技術 112-1 答案B

(公司直接開放遠端給員工從網際網路存取是最危險的，應該要使用VPN搭配VDI等方式)

48. 關於行動裝置安全的方案，下列何者較「不」適當？

(A) 利用端點安全方案，監控公司每部存取網路行動裝置檔案與程式，透過持續掃描惡意行為，來及早識別威脅

(B) 透過VPN讓裝置到公司網路加密連線，確保安全傳輸資料，防止未經授權人員竊聽，讓員工安全地進行遠距工作

(C) 員工在公司電腦安裝隱匿通道（Tunnel）保護家裡到公司的連線，確保只有自己可以使用，來安全傳輸資料

(D) 提升電子郵件安全，透過檔案內容淨化與重組（CDR）進行郵件檔案清洗，阻絕勒索病毒或是惡意檔案，利用行動裝置擴散到公司網路

技術 112-1 答案C

(公司電腦不可安裝隱匿通道（Tunnel）這樣可能會造成資安破口，應該是統一透過管控的VPN裝置)

2. 請問下列何者為常見的 SNMP（Simple Network Management Protocol）安全問題？

(A) 使用 public community string

(B) 使用 SNMP v3

(C) 使用 UDP

(D) 使用 161 作為服務 Port

技術 111-2 答案A  
(因為SNMP v1和v2有使用 public community string的資安問題，因此建議使用SNMP v3)

8. 面對組織化、多變化的駭客攻擊，建立資訊安全監控維運中心（ Security Operation Center, SOC）以加強資訊安全系統安全，下列何者是 SOC的較主要運作功能？

(A) 決定風險處理方法

(B) 進行資安弱點管理

(C) 即時監看資安事件

(D) 處理資安事故原因

技術 111-2 答案C

33. 防毒軟體使用「啟發 /探索方法（ Heuristic Method）」最主要優點 為下列何項？

(A) 偵測全新病毒

(B) 偵測已知病毒

(C) 避免誤隔離

(D) 可更快速偵測已知惡意程式

技術 111-2 答案A

(傳統防毒軟體使用特徵方法，但無法發現全新的病毒)

3. 下列何者為 L7 layer Firewall ？

(A) Antivirus

(B) WAF

(C) IPS

(D) IDS

技術 111-1 答案B

8. 欲將外部網路（Internet）建立連線至內部網路（Intranet），採用下列何種連線方式，單一使用者可以較安全連接至某個私人網路？

(A) WAF

(B) SSD

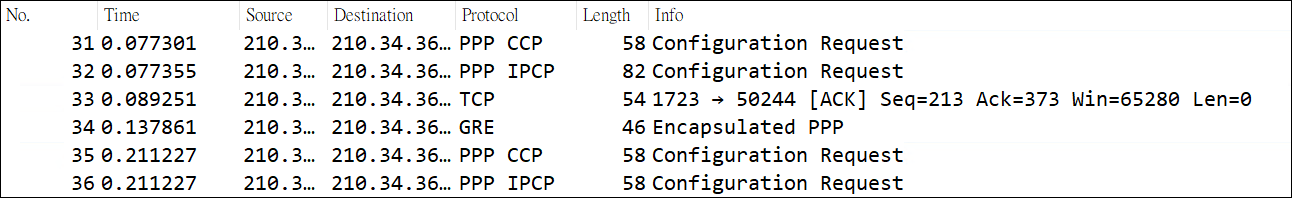
(C) VPN

(D) PBX

技術 111-1 答案C

9. 某公司管理人員正在診斷 VPN的安全性問題， 附圖為其截取到的部

份 VPN封包，請問這家公司使用下列何種 VPN通道協定？



(A) OpenVPN

(B) IPSec VPN

(C) SSL VPN

(D) PPTP VPN

技術 111-1 答案D

(按照圖上所示，PPTP使用的Port為1723)

18. 關於虛擬修補（Virtual patch），下列敘述哪些正確 ？（複選）

(A) 透過分析與攔截惡意網路封包內容，而達成防護效果

(B) 虛擬修補對網路攻擊防護極為有效，可取代弱點修正與更新

(C) 針對已知攻擊特徵， 亦可於入侵防禦系統（IPS）或網站應用程

式防火牆（WAF）上設定規則阻擋

(D) 常於零時弱點（Zero day）、老舊系統無法修復、人力不足無法更

新程式等情境應用

防護 111-1 答案A、C、D  
(B選項，虛擬修補是一種**臨時性的安全措施**，用於在正式修補程式發布之前提供保護。它**不能取代**對系統和應用程式進行實際的弱點修復和更新。根本的解決方案仍然是修復底層的漏洞)

46. 關於入侵檢測系統（Intrusion-Detection System, IDS），下列敘述何者「不」正確？

(A) 需定期更新特徵碼

(B) 可阻擋偽造 IP之攻擊 (IDS不會阻擋流量，僅監控)

(C) 不會因設備異常導致網路環境異常

(D) 可完整紀錄流量特徵

技術 111-1 答案B