防火牆功能比較

1. 請說明防火牆的主要功能
2. 簡單說明它的封包過濾, 狀態檢查, 及運用代理閘道防火牆, 原理上的不同
3. 在現今微軟系統上, 學校可以如何簡單的設定操控它
-
4. 請說明VPN, 及如何在微軟PC 上設定
5.說明什麼是DMZ

以下以**繁體中文、教學取向**為你整理，適合學校或資訊課程說明使用：

1️⃣ 防火牆（Firewall）的主要功能

防火牆是**位於內部網路與外部網路（如 Internet）之間的安全設備或軟體**，主要功能包括：

1. **控管網路流量**
   - 決定哪些封包可以進出、哪些要阻擋
2. **防止未授權存取**
   - 阻擋駭客、惡意掃描、非法連線
3. **降低惡意攻擊風險**
   - 如：Port Scan、DoS、惡意程式回傳
4. **建立安全政策**
   - 依 IP、Port、通訊協定、應用程式設定規則
5. **記錄與稽核**
   - 產生連線紀錄（Log），利於資安追蹤

👉 **簡單比喻**：防火牆就像「大樓警衛」，決定誰可以進出、走哪個門。

2️⃣ 防火牆三種技術的原理差異

🔹（1）封包過濾（Packet Filtering）

原理

- 只檢查封包「表頭」資訊：
  - 來源 IP
  - 目的 IP
  - Port
  - 通訊協定（TCP / UDP / ICMP）

特點

- 不看連線是否完整
- 不理解封包內容

優點

- 快速、效能好
- 架構簡單

缺點

- 安全性較低
- 無法防止偽裝攻擊

📌 例：

> 「允許來自 140.0.0.0/16 的 TCP 80 封包」

🔹（2）狀態檢查（Stateful Inspection）

原理

- 會「記住連線狀態」
- 只允許**合法連線流程**中的封包

會檢查

- TCP 三向交握（SYN / ACK）
- 封包是否屬於已建立的連線

優點

- 安全性高於封包過濾
- 可防止偽造封包

缺點

- 比封包過濾耗資源

📌 現代主流防火牆（含 Windows Defender Firewall）皆屬此類

🔹（3）代理閘道防火牆（Proxy Firewall / Application Gateway）

原理

- 防火牆「代替用戶」與外部伺服器通訊
- 用戶不直接接觸外部網路

特點

- 可檢查「應用層內容」（HTTP、FTP、SMTP）
- 具備內容過濾、帳號驗證

優點

- 安全性最高
- 可隱藏內部 IP

缺點

- 效能較慢
- 架構與設定較複雜

📌 常見於企業 Proxy Server、Web 防火牆

🔍 三者比較總表

類型	檢查層級	安全性	效能
封包過濾	網路層	⭐	⭐⭐⭐
狀態檢查	傳輸層	⭐⭐	⭐⭐
代理閘道	應用層	⭐⭐⭐	⭐

3️⃣ 學校在現今微軟系統上的簡易防火牆管理方式

✅ 使用 Windows Defender 防火牆

路徑

```
控制台 → Windows Defender 防火牆 → 進階設定
```

學校常見設定方式

🔹 **（1）封鎖或允許程式**

- 封鎖遊戲、P2P、非教學軟體
- 只允許教學系統、瀏覽器

🔹 **（2）設定 Port 規則**

- 開放：80、443（Web）

- 封鎖：BT、遠端控制軟體 Port

🔹 **（3）使用「群組原則（GPO）」統一管理**

- Active Directory 網域環境
- 一次套用到全校電腦

📌 非常適合學校電腦教室管理

4️⃣ VPN 是什麼？以及在微軟 PC 的設定方式

🔐 什麼是 VPN（Virtual Private Network）

VPN 是一種：

> **在不安全的網路（如 Internet）上，建立加密的安全通道**

功能

- 保護資料不被竊聽
- 隱藏真實 IP
- 遠端安全連回校內 / 公司網路

📌 常見用途：

- 教師在家存取校內系統
- 學生連回校內伺服器
- 公共 Wi-Fi 保護隱私

🖥️ Windows 上設定 VPN（Windows 10 / 11）

設定步驟

1. 設定 → 網路與網際網路 → VPN
2. 新增 VPN 連線
3. 填寫：
    - VPN 伺服器位址
    - VPN 類型（PPTP / L2TP / IKEv2 / SSTP）
    - 帳號 / 密碼
4. 儲存並連線

📌 學校常使用：

- L2TP / IPsec
- SSL VPN

5️⃣ 什麼是 DMZ（Demilitarized Zone）

🧱 DMZ 的概念

DMZ 是：

> **位於內部網路與外部網路之間的「緩衝區」**

為什麼要有 DMZ？

- 對外服務（如網站、FTP）需要公開
- 但又不能讓外部直接進入內部網路

常放在 DMZ 的設備

- Web Server
- Mail Server
- FTP Server
- 校園網站伺服器

DMZ 架構示意（文字）

```
css

Internet
    |
[ 防火牆 ]
    |
    ├── DMZ（對外伺服器）
    |
    └── 內部網路（教師 / 學生）
```

📌 即使 DMZ 伺服器被攻破，內部網路仍受保護

✅ 總結一句話

- **防火牆**：控制誰能進出網路
- **VPN**：建立安全加密通道
- **DMZ**：隔離對外服務，保護內部網路

如果你需要 👉 **「適合資管系考試的重點整理」或「搭配實際校園案例說明」**，我也可以幫你再整理一版。