

多層次防禦說明

1. 請說明什麼是多層次防禦
2. 都有那些層次？
3. 每個層次主要的工作重點是什麼？

以下以資訊安全（Cybersecurity）角度，用繁體中文、教學導向來說明「多層次防禦（Defense in Depth）」：

一、什麼是多層次防禦？

多層次防禦（Defense in Depth）

是一種資安策略，不依賴單一安全機制，而是在系統、網路與資料的不同層面上，同時部署多道防線。

👉 核心概念是：

就算某一層被攻破，後面還有其他層可以攔阻、偵測或降低傷害

就像城堡的設計：

城牆 → 護城河 → 守衛 → 內門 → 保險箱

每一層都讓攻擊者「更難成功、花更久時間、留下更多痕跡」。

二、多層次防禦通常包含哪些層次？

實務上常見的多層次防禦可分為 **7 大層**（由外而內）：

1. 實體層（Physical）
2. 網路邊界層（Perimeter / Network）
3. 網路內部層（Internal Network）
4. 主機 / 作業系統層（Host / OS）
5. 應用程式層（Application）
6. 資料層（Data）
7. 人員與管理層（People / Policy）

三、各層次的主要工作重點

1 實體層（Physical Security）

🔒 防止未授權的人接觸設備

重點工作

- 管理機房、伺服器、網路設備的實體存取
- 防止設備被偷、被破壞、被插惡意裝置

常見措施

- 門禁卡、指紋、人臉辨識
- 機房監控攝影機
- 伺服器上鎖、USB 存取限制

2 網路邊界層 (Perimeter / Network)

阻擋外部攻擊進入內部網路

重點工作

- 控制「誰可以從外部連進來」
- 過濾惡意流量

常見措施

- 防火牆 (Firewall)
- IDPS (入侵偵測與防禦系統)
- VPN (安全遠端連線)
- DDoS 防護

3 網路內部層 (Internal Network)

防止攻擊在內部橫向擴散

重點工作

- 即使攻擊者進來，也限制活動範圍
- 防止「一台中毒，全公司淪陷」

常見措施

- VLAN 網路分段
- 零信任 (Zero Trust)
- 內部流量監控
- NAC (網路存取控制)

4 主機 / 作業系統層 (Host / OS)

保護單一電腦或伺服器

重點工作

- 防止惡意程式執行
- 修補系統漏洞

常見措施

- 防毒軟體（如 Windows Defender）
- 主機型防火牆
- 系統更新與修補（Patch）
- 帳號權限控管（最小權限原則）

5 應用程式層（Application）

防止應用程式被攻擊或濫用

重點工作

- 防止 SQL Injection、XSS 等攻擊
- 確保使用者只能做「被允許的事」

常見措施

- WAF（Web Application Firewall）
- 安全程式設計（Input Validation）
- 身分驗證 / 授權（Login、MFA）
- 程式漏洞掃描

6 資料層（Data）

保護最有價值的資產：資料

重點工作

- 防止資料外洩、竄改或遺失
- 即使系統被入侵，資料仍不可讀

常見措施

- 資料加密（Encryption）
- 存取權限控管
- DLP（資料外洩防護）
- 備份與還原機制

7 人員與管理層（People / Policy）

降低「人為疏失」造成的風險

重點工作

- 防止社交工程、釣魚郵件
- 建立安全意識與制度

常見措施

- 資安教育訓練
- 資安政策與流程
- 密碼政策
- 事件通報與應變演練

四、整體快速對照表

層次	防禦重點	代表技術
實體層	防止設備被接觸	門禁、監控
邊界層	擋外部攻擊	防火牆、IDPS
內部網路	防橫向移動	VLAN、Zero Trust
主機層	保護單機	防毒、Patch
應用層	防程式漏洞	WAF、驗證
資料層	保護資料	加密、備份
人員層	防人為風險	教育、政策

如果你願意，我也可以幫你：

- **◆ 用「中型企業 / 校園網路」實際畫一個多層次防禦範例**
- **◆ 把它整理成 考試用重點版本**
- **◆ 或搭配你前面問過的 防火牆、IDPS、Windows Defender 串起來說明**