




IDPS 基本介紹與運作

1. 簡單說明入侵偵測與防禦系統
2. IDPS 英文全名
3. 請說明它的主要工作原理?
4. 中型企業 IDPS 會有自己專用的伺服器? 或一般會把 IDPS 功能的軟件安裝在防火牆的主機中?

以下依你的 4 個問題，用資安課程／企業實務常見的角度，簡單但完整說明：

1 什麼是入侵偵測與防禦系統（IDPS）？

入侵偵測與防禦系統（IDPS）是一種用來：

-  監控網路流量與系統行為
-  偵測是否有入侵或攻擊行為
-  即時阻擋或回應攻擊

的資安防護系統。

👉 可視為「比防火牆更聰明的保全系統」

- 防火牆：看「能不能進來」
- IDPS：看「進來後在幹嘛」

2 IDPS 的英文全名

IDPS = Intrusion Detection and Prevention System

（入侵偵測與防禦系統）

早期常分成 IDS 與 IPS

現在多半整合成 **IDPS**

3 IDPS 的主要工作原理

IDPS 的運作流程可分為 4 個核心步驟：

◆ (1) 監控（Monitoring）

- 監看：
 - 網路封包（Network traffic）
 - 系統行為（登入、程式執行）

- 應用程式請求 (Web 攻擊)

◆ (2) 分析與比對 (Analysis)

常見 三種偵測方式：

✓ ① 特徵比對 (Signature-based)

- 比對已知攻擊特徵
- 類似防毒病毒碼

✓ 快速、準確

✗ 無法抓新型攻擊

✓ ② 行為／異常偵測 (Anomaly-based)

- 建立「正常行為模型」
- 發現異常流量或行為

✓ 可偵測未知攻擊

✗ 誤判率較高

✓ ③ 規則／政策偵測 (Policy-based)

- 管理者自訂規則
- 如：禁止某 IP 存取特定服務

◆ (3) 偵測結果處理

類型	行為
IDS (Detection)	只記錄、警告
IPS (Prevention)	即時阻擋攻擊

◆ (4) 回應 (Response)

可能的動作包括：

- ✗ 丟棄封包
- 🔒 封鎖 IP
- 📧 發送警報 (Email / SIEM)
- 📝 記錄事件 (Log)

4 中型企業的 IDPS 部署方式（實務面）

這題非常「考試+實務常考」，答案如下 📌

◆ 情況一：整合在防火牆中（最常見）✅

🔪 中型企業主流做法

- IDPS 功能內建在：
 - Next-Generation Firewall (NGFW)
 - UTM (Unified Threat Management)

優點：

- 💰 成本較低
- 🛠️ 管理方便
- 🧩 整合度高

適合：

- 中小～中型企業
- 校園、一般公司

◆ 情況二：獨立 IDPS 專用伺服器／設備 ⚠️

🔪 較大型或高資安需求企業

- 獨立硬體或伺服器
- 串接核心交換器或鏡像埠

優點：

- 🚀 效能高
- 🎯 偵測更細緻
- 🔍 可深度分析流量

缺點：

- 💰 成本高
- 🏠 維運複雜




◆ 實務總結比較表

企業規模	常見做法
小型企業	防火牆內建 IDPS
中型企業	防火牆整合 IDPS（最常見）
大型企業	獨立 IDPS + 防火牆 + SIEM

一句話總結（考試好用）

IDPS 是用來即時監控、偵測並阻擋入侵行為的資安系統，中型企業多半將 IDPS 功能整合在新世代防火牆中，而非獨立部署專用伺服器。

如果你願意，我也可以幫你整理成：

-  「考試重點版」
-  「防火牆 vs IDPS 比較表」
-  「校園／企業實際架構圖說明」

你比較想要哪一種？