

CUDY 路由器 DMZ 設定與安全建議

什麼是 DMZ？

DMZ 是一種網路功能，允許您將內部網路中的一台裝置（例如 電腦、遊戲主機或伺服器）直接暴露在網際網路上，使所有來自外部的未指定封包都轉發到這台指定設備

此功能適用於某些不支援指定埠號的應用程式，例如某些線上遊戲、VoIP，或需要完整進入權限的遠端管理工具

安全風險提醒

啟用 DMZ 將使該裝置**直接面對網際網路**，可能會被惡意掃描或攻擊。請務必謹慎使用，並僅針對已知用途與已具備完整安全防護機制的裝置進行設定

CUDY 路由器 DMZ 設定步驟

步驟 1：登入路由器設定頁面

開啟網頁瀏覽器並前往 <http://cudy.net> 或 <http://192.168.10.1>

步驟 2：進入 DMZ 設定頁面

進入管理後台首頁後，請依序點選 「**進階設定**」 → 「**網路**」 → 「**DMZ**」



步驟 3：填入 DMZ 主機 IP 並保存

在功能頁面欄位中填入您要設置為 DMZ 主機的內部 IP 位址 (例如 `192.168.10.101`)，並點擊 「**保存 & 應用**」

設定完成後，該 IP 對應的裝置將接收所有來自外網但未被其他規則攔截的封包



安全強化建議

- DMZ 裝置本身需具備完善的防火牆或安全防護機制 (例如防毒軟體、作業系統內建防火牆)
- 若僅特定應用需要對外連接，建議優先使用**通訊埠轉發** 代替 DMZ，以縮小設備暴露在公網的範圍
- 不建議將無任何防護能力的安全設備 (如手機、智慧電視、物聯網 IoT 裝置) 設定為 DMZ 主機