

## DMZ功能說明



DMZ 理論上來說，是在防火牆上有三種區塊下的一種安全理論模式，依理論最少區分為三種區塊；**外部網路(LAN)、內部網路(LAN)、非軍事區(DMZ)**。

通常外部網路的安全係數是最低的，而內部網路安全係數是最高的。為了保護內部網路的安全係數能夠維持高安全狀況，外部網路要直接連結到內部網路通常是不被允許的，因此企業常把要公告的網路服務建置在 DMZ 環境中，那麼就算 DMZ 的伺服器被駭客入侵會被植入病毒碼還是能夠維持內網的安全。

一般企業通常要提供給外界存取的 Server，都會將它放到 DMZ 區，例如：DNS, Web Server, FTP Server 等等，而這些 Server 都有幾個共同點：

1. Server 區內沒有機密性的資料。
2. 提供外界存取的聯絡通道。
3. 這些 Server 區就算被入侵或病毒感染，也不至於影響整體運作。

但是，並不是說放在 DMZ 的 Server 就是直接對外，系統管理者還是要開對外的 port 對應的 IP，因此還是有基本的安全性，但是這些 Server (DNS, Web, FTP) 又提供服務給外部使用者存取（包含駭客、病毒），因此這些 Server 的風險是比較高的。如果將內部電腦或者及機制資料放在同一區域的話，那不是很危險？因此，才會有 DMZ 這個區域名詞衍生出來。

如果你的內網都是一些不重要的 Server，或是你認為即使被入侵也無所謂，那你就可以不需要區分 DMZ 通通放在內網就好了！



DMZ 架構圖