

DMZ伺服器配置指南

企業需要將網頁伺服器放在Demilitarization Zone (DMZ) 非軍事區外
尚有其他伺服器需要放在此區域的嗎？

是的 

除了網頁伺服器（Web Server）之外，企業在 DMZ（Demilitarized Zone，非軍事區）中，通常還會放置「需要被外部存取、但不應直接接觸內部網路」的伺服器或服務。

下面用分類+理由的方式幫你整理，這也是資訊安全考試或實務中常見的答案。

一、什麼樣的系統「適合放在 DMZ」？

 同時符合這 2 個條件：

1. 需要被 Internet 存取
2. 不應直接連到內部 LAN（內網）

DMZ 的角色就是「緩衝區 / 隔離區」。

二、常見需要放在 DMZ 的伺服器種類

1 Web Server (最典型)

- 提供公司官網、客戶入口
- HTTP / HTTPS
- 外部可直接連線
-  一定放 DMZ

2 Mail Server (郵件伺服器，部分角色)

通常是：

- SMTP Gateway / Mail Relay
- 收外部郵件，再轉送內部信箱系統

 架構常見做法：

- DMZ：SMTP Relay
- 內網：Exchange / Mailbox Server

 收信端放 DMZ

3 FTP / SFTP Server

- 提供客戶或合作夥伴上傳 / 下載檔案
- 容易成為攻擊目標

✓ 對外 FTP / SFTP 放 DMZ

4 DNS Server (對外用)

通常分成：

- External DNS (公開解析) → DMZ
- Internal DNS (內部解析) → 內網

✓ 權威 DNS (Authoritative DNS) 放 DMZ

5 VPN Server (遠端連線入口)

- 讓員工在外部連線進公司
- VPN 是「進入內部的入口」

📌 為何放 DMZ ?

- 若 VPN 被攻破，不會直接進內網
- 仍需經過防火牆控管

✓ VPN Gateway 放 DMZ

6 Proxy Server (反向代理 / 應用代理)

- Reverse Proxy、WAF
- 幫內部系統擋攻擊、做負載平衡

✓ Reverse Proxy / WAF 放 DMZ

7 API Server (對外 API)

- 提供行動 App、合作夥伴 API
- 微服務常見

📌 做法：

- DMZ : API Gateway
- 內網 : 後端服務、資料庫

✓ API Gateway 放 DMZ

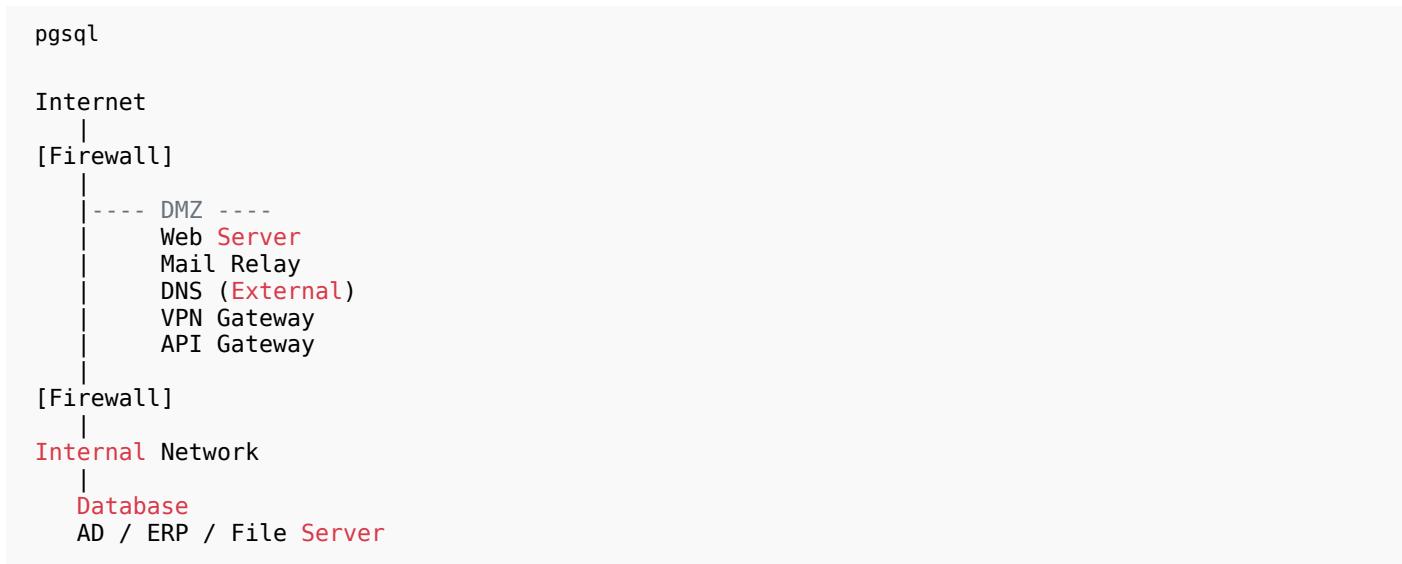
三、哪些「不應該」放在 DMZ？

- ✖ 資料庫 (DB Server)
- ✖ AD / 網域控制站 (Domain Controller)
- ✖ ERP / HR / 財務系統
- ✖ 檔案伺服器 (內部用)

👉 原因：

- 含有機密資料
- 一旦被攻破，後果嚴重

四、典型企業網路架構 (文字示意)



五、一句話總結 (考試超好用)

凡是「需要對外服務、但不能直接接觸內部網路」的伺服器，皆應放置於 DMZ。

如果你需要，我也可以幫你：

- 📊 整理成「表格版 (伺服器 / 放置位置 / 原因)」
- 📊 用「**考試申論題標準答案**」格式寫一題
- 📊 解釋「單層 DMZ vs 雙層 DMZ」

你比較想用在哪一種情境？

1. 在認知中從internet往內看，應該是 Router, DMZ, Firewall 對嗎？
2. 上圖中有2層的Firewall 請分別說明，那2層Firewall 有何不同？

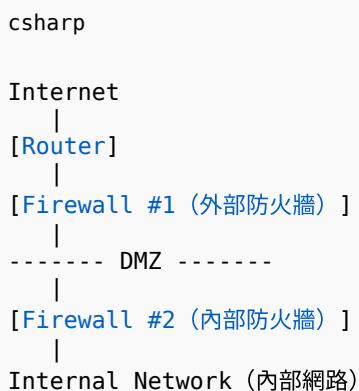
很好，這兩個問題都正中「企業網路架構 × 資安觀念」核心，而且你問的順序本身就很像考試題  我分別用「觀念釐清 → 正確架構 → 為什麼要這樣設計」來回答。

一、問題 1

 從 Internet 往內看，順序是 Router → DMZ → Firewall 嗎？

 結論先說：不完全正確（但你的想法很接近）

正確、最常見的企業架構是：



 為什麼不是「DMZ 在 Firewall 外面」？

- DMZ 本身不是設備
- DMZ 是「被防火牆規則隔離出來的一個網段（Zone）」
- 一定是被 防火牆「夾住」或「切出來」

 所以不能單獨存在於 Firewall 外側

二、問題 2

 為什麼有 2 層 Firewall？有何不同？

這題是標準考試必考題，我們來逐層說明。

 **Firewall #1 (外部防火牆 / Perimeter Firewall)**

 **位置**

- Internet 與 DMZ 之間

 **主要目的**

👉 防止 Internet 的直接攻擊

🛡️ 主要功能

- 封鎖非法 IP
- 僅開放必要服務
 - 80 / 443 (Web)
 - 25 (SMTP)
 - 53 (DNS)
- 防止掃描、DDoS、暴力攻擊 (部分)

📌 原則

Internet → DMZ：只開「必要」的服務

🔥 Firewall #2 (內部防火牆 / Internal Firewall)

📍 位置

- DMZ 與內部網路之間

🎯 主要目的

👉 防止 DMZ 被攻破後，橫向入侵內網

🛡️ 主要功能

- 嚴格限制 DMZ → Internal 的流量
- 僅允許「單向、指定服務」
 - Web Server → DB Server (指定 port)
- 記錄詳細存取 log

📌 原則

DMZ → Internal：預設全部拒絕 (Deny All)

三、兩層 Firewall 的差異整理 (表格版)

項目	Firewall #1 (外部)	Firewall #2 (內部)
位置	Internet ↔ DMZ	DMZ ↔ Internal
防禦對象	外部駭客	DMZ 被入侵後
規則嚴密度	中	非常嚴格
主要風險	外部攻擊	橫向移動

項目	Firewall #1 (外部)	Firewall #2 (內部)
設計重點	可用性 + 基本防護	機密性 + 最小權限

四、為什麼一定要「兩層」？（資安關鍵觀念）

🧠 核心思維：假設 DMZ 一定會被攻破

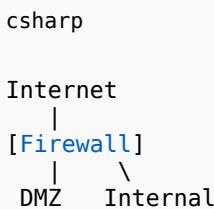
這是資安的「零信任 / 最壞假設」思想。

Web Server 是公開的
被打只是「時間問題」
所以 **不能讓它直接連內網**

👉 第二層 Firewall 就是「最後一道防線」

五、如果只有「一台 Firewall」怎麼辦？

單一防火牆（三介面 Firewall）



- 靠 VLAN / Zone 分隔
- 成本低
- 中小企業常見

📌 邏輯上仍是「兩層概念」

只是實體設備合併而已

六、考試用一句話總結（超重要）

外部防火牆負責阻擋 Internet 攻擊，
內部防火牆負責防止 DMZ 被攻破後入侵內部網路，
兩層防火牆形成縱深防禦（Defense in Depth）。

如果你願意，我可以幫你：

- 🤝 寫一題「申論題滿分答案」
- 📊 畫一張「考試等級 ASCII 架構圖」

- 🔒 延伸說明 DMZ × Zero Trust 的關係

你是準備考試、上課、還是實務架構設計？

如上: 五、如果只有「一台 Firewall」怎麼辦？

- 把DMZ放在Firewall 內, 會不會有些user上不了企業的網站呢?

這個問題問得非常好，而且是很多人第一次接觸 DMZ 都會卡住的關鍵點 🤝

答案先給你，再慢慢拆解：

不會。只要防火牆規則設計正確，把 DMZ 「放在同一台 Firewall 裡」完全不會影響外部使用者連上企業網站。

下面用「直覺疑問 → 真正原理 → 實際封包怎麼走」來說清楚。

一、為什麼你會直覺覺得「可能連不上」？

因為你腦中大概是這樣想的：

DMZ 在 Firewall 裡面

那 Internet 的封包不是被 Firewall 擋住了嗎？

這個直覺很正常，但關鍵誤解在於：

👉 Firewall 不是「全部擋」，而是「依規則放行」

二、單一 Firewall + DMZ 的正確觀念

📌 重要觀念 1：

DMZ 不是在 Firewall 「後面」，而是在 Firewall 「控制之下」

Firewall 會有 3 個介面（或 3 個 Zone）：

Zone	說明
Outside	Internet
DMZ	對外服務區
Inside	內部網路

📌 重要觀念 2：

外部使用者連的是「Firewall 的 IP」，不是 DMZ Server 的真實 IP

這裡會用到：

- NAT (DNAT / Port Forwarding)

三、實際封包流程（外部使用者連企業網站）

🌐 使用者在瀏覽器輸入：

```
arduino
https://www.company.com
```

封包實際走法：

```
pgsql
Internet User
  |
  | 目的 IP = 公網 IP (Firewall)
  v
[Firewall]
  | ① NAT: 80/443 → DMZ Web Server
  | ② ACL: 允許 Internet → DMZ:443
  v
DMZ Web Server
```

- ✓ 完全沒有經過內部網路
- ✓ 使用者感覺不到 DMZ 在哪

四、為什麼不會影響使用者？

🔑 關鍵原因只有一個：

防火牆規則決定「能不能進」，
NAT 決定「送到哪裡」

只要設定：

- ✅ Internet → DMZ : Allow 80/443
- ❌ Internet → Internal : Deny All

👉 外部使用者就能正常上網站

五、什麼情況下「真的會上不了網站」？

這題也很重要，代表你觀念已經到位了 🎉

✖ 常見錯誤設定

1. 沒設定 NAT

- 封包只到 Firewall 就停了

2. ACL 寫錯

- 放在錯誤方向
- Zone 寫錯 (Outside → Inside)

3. Web Server 放錯 Zone

- 被當成 Internal

4. DNS 指錯 IP

- 指到內部 IP (192.168.x.x)

六、單一 Firewall vs 兩台 Firewall (差異補充)

項目	單一 Firewall (三介面)	兩台 Firewall
外部可用性	✓ 正常	✓ 正常
安全邏輯	一樣	一樣
風險	單點失效	分散
成本	低	高
中小企業	常見	少

👉 差別在「風險與成本」，不是在「能不能連線」

七、一句話總結 (一定要記)

DMZ 放在 Firewall 裡，不是「擋住網站」，
而是「由 Firewall 精準控制誰可以連、連到哪」。

如果你願意，我可以下一步幫你：

- 🔒 寫一組「實際 Firewall 規則範例」
- 📘 用「考試選擇題陷阱」幫你記牢
- 🧱 比較 DMZ 與 Zero Trust 的差異

你現在是在準備考試，還是要實際設計網路？

 潘天佑課本P9-10頁-防火牆環境範例.pptx
簡報

如附件單頁的.pptx所示，它的外部網站伺服器
好像是放在第一層防火牆的外面，Router的裡面，是課本有錯，或是我誤解了呢？

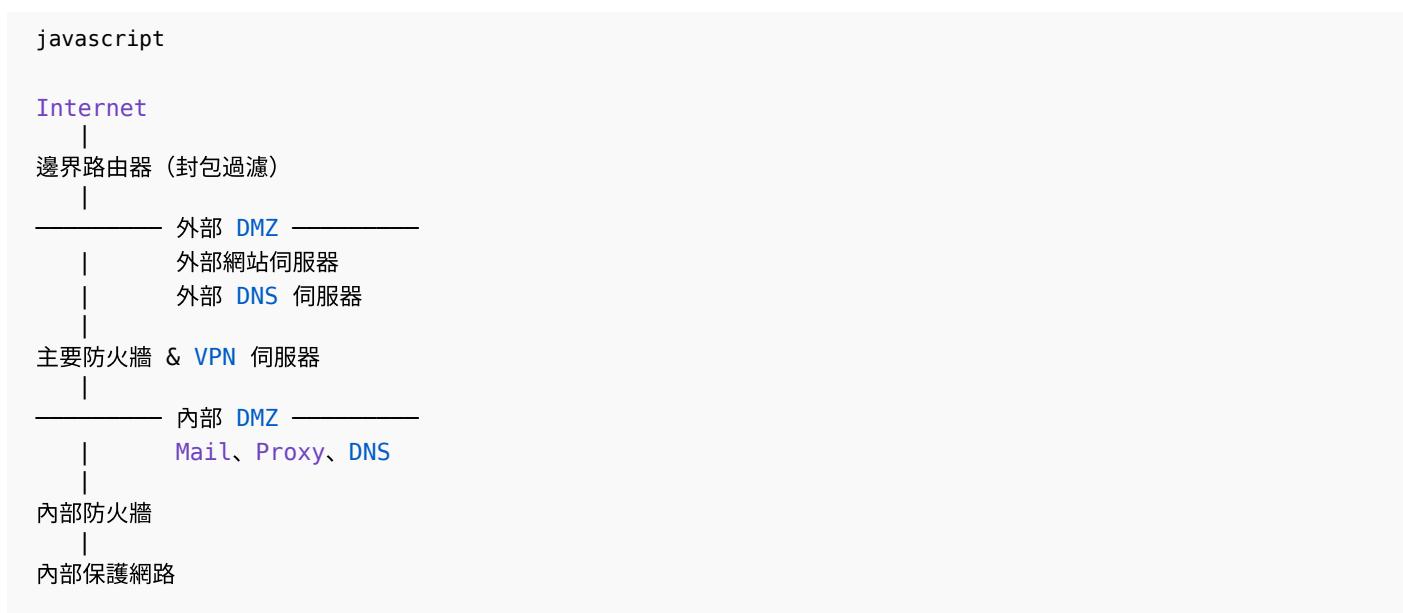
這一題你沒有誤解，而且也不能直接說課本錯——

真正的答案是：你看到的是「另一種合法、但比較少見」的 DMZ 架構畫法，而且課本畫的是「概念示意圖」，不是最佳實務圖。

我用你附的那張投影片（P9-10 防火牆環境範例）來「對照拆解」說清楚。

一、你看到的圖「實際在畫什麼？」

依照投影片內容（參考 NIST SP 800-41），結構大致是：



👉 你觀察得完全正確：

外部網站伺服器「確實畫在第一層防火牆（主要防火牆）之外」

二、這是不是「把 Web Server 放在 Firewall 外面」？

🔴 表面看起來是

🟢 但實際上不是「沒防火牆」

關鍵在於：

👉 課本把「邊界路由器（Packet Filtering Router）」視為第一道防火牆

三、課本架構的「真正防禦邏輯」

🧱 第一道防線：邊界路由器（L3/L4）

- 做封包過濾 (ACL)

- 只允許：

- TCP 80 / 443

- TCP 53

- ✗ 不允許直接進內部

📌 在 NIST SP 800-41 的年代

👉 「Router with ACL」被算是一種防火牆

🧱 第二道防線：主要防火牆 (Stateful / VPN)

- 保護「內部 DMZ」
 - 防止外部 DMZ 被入侵後再往內橫向移動
-

🧱 第三道防線：內部防火牆

- 保護核心內網
-

四、為什麼課本會這樣畫？（歷史 + 教學原因）

1 歷史背景

- 早期（2000 年前後）：
 - 路由器 ACL = 第一層防火牆
 - Stateful Firewall 昂貴
 - 所以常見：
 - Web / DNS 放在 Router 後、Firewall 前
-

2 教學示意用

- 課本重點是：
 - 「多層防禦（Defense in Depth）」
 - 不是在教：
 - 現代企業最佳實務
 - NGFW / Zero Trust 架構
-

五、那「現代實務」會怎麼做？

✓ 現代企業（考試 + 實務都推薦）

```
pgsql

Internet
|
[Firewall (Outside Zone) ]
|
DMZ (Web / DNS / Mail)
|
[Firewall (Inside Zone) ]
|
Internal Network
```

或

```
csharp

Internet
|
[NGFW (三介面) ]
|
DMZ      \ Internal
```

👉 Web Server 一定在 Firewall 控制之下

六、所以：課本錯了嗎？

✗ 不是錯

✓ 但「容易讓初學者誤解」

更精準的說法是：

課本畫的是「符合當年 NIST 架構的一種實作範例」，
不是現代企業的最佳安全實務示意圖。

七、考試時你該怎麼答？（超重要）

如果是「理解題 / 實務題」👉 用你現在學到的觀念

Web Server 應置於 DMZ，並受防火牆控管

如果是「照圖說明題」👉 這樣講才穩：

圖中外部網站伺服器雖位於主要防火牆之外，
但仍受邊界路由器之封包過濾保護，
並透過多層防禦設計避免直接連入內部網路。

八、一句話幫你「定錨觀念」

DMZ 的重點不在「畫在防火牆哪一側」，
而在於「是否被安全設備嚴格控管、且不與內網直通」。

如果你願意，我可以：

-  幫你寫一段「老師點頭的解釋答案」
-  幫你整理「課本圖 vs 現代架構對照表」
-  幫你列出「考試最愛用這張圖挖的陷阱」

你這題問得非常專業，已經不是新手等級了 