

# VPN 與 ISP 關係

企業欲使用VPN形成intranet, 應該是要跟它的ISP提出服務的需求協助吧?

如果它的ISP是A

它可以跟另一家的VPN伺服器廠商申請服務嗎?

不太可能, 對吧?

你的理解接近但需要一點修正。企業使用 VPN 形成 **intranet** (企業內部網路) , 不一定「只能」找自己的 ISP, 也完全有可能找第三方 VPN 服務或自行建置。下面我用「實務角度」幫你拆清楚 👇

## 一、企業要用 VPN 形成 Intranet，本質上在做什麼？

**本質需求：**

讓分散在不同地點的使用者或據點

透過「加密通道」

安全地連進同一個內部網路

這裡的關鍵是：

- VPN 是 **應用在 IP 層之上的加密技術**
- ISP 只負責「把封包送到目的地」
- VPN 通道本身不必由 ISP 提供

## 二、一定要跟 ISP 申請 VPN 服務嗎？

✗ 不一定 (常見誤解)

**ISP 的角色其實是：**

- 提供 **Internet 連線**
- 或提供 **專線 / MPLS / SD-WAN**

ISP 不是 VPN 的必要條件

ISP 只是「底層傳輸管道」

## 三、企業「可以」找另一家 VPN 伺服器廠商嗎？

✓ 完全可以，而且非常常見

**常見的 3 種做法：**

## ✓ 做法 1：自己建 VPN（最常見）

企業內部自行架設：

- 防火牆 (FortiGate / Palo Alto / Sophos)
- VPN Server (OpenVPN / WireGuard / IPsec)
- Windows / Linux Server

👉 只要有 Internet (不管 ISP 是誰) 就能用

## ✓ 做法 2：找第三方 VPN / 雲端廠商

例如：

- AWS VPN / Azure VPN
- Cloudflare Zero Trust
- Zscaler / Palo Alto Prisma Access

👉 ISP A → Internet → 第三方 VPN 服務 → 企業內網

這在跨國企業、遠距辦公非常普遍

## ⚠️ 做法 3：跟 ISP 申請「企業專網」

這其實 不是 VPN，而是：

- MPLS
- 專線
- SD-WAN

特點：

- 高穩定
- 高費用
- 繩定 ISP

## 四、為什麼你會覺得「不太可能」？

因為你可能把下面兩件事混在一起了 👇

| 項目      | VPN   | ISP 專線 |
|---------|-------|--------|
| 是否需 ISP | ✗ 不一定 | ✓ 必須   |
| 加密      | ✓ 有   | ✗ 不一定  |
| 彈性      | 高     | 低      |
| 成本      | 低～中   | 高      |

| 項目      | VPN | ISP 專線 |
|---------|-----|--------|
| 是否可用第三方 | ✓   | ✗      |

## 五、簡單一句話總結

VPN 是「跑在 Internet 上的加密通道」  
ISP 只負責連線，不必是 VPN 提供者

所以你的問題答案是：

- ✓ 可以不用找 ISP
- ✓ 可以找第三方 VPN 廠商
- ✗ 一點都不罕見
- ✗ 不「不太可能」，而是「非常常見」

如果你願意，我也可以幫你畫一張

👉 「ISP vs VPN vs 企業 Intranet」的架構圖

或用 中小企業 / 學校的實際案例來說明 👍

請說明：如果企業自建 VPN 伺服器，與 ISP 廠商工作的分工情形

這個問題問得**非常關鍵**，因為它正好切中

👉 「VPN 是誰在管？ISP 又在管什麼？」

我用 分工表 + 實際連線流程 + 常見誤解 來幫你完整說清楚。

## 一、一句話先給結論

企業自建 VPN 時：

- ISP 只負責「網路通不通」
- 企業負責「VPN 安不安全、怎麼連、誰能連」

## 二、企業 vs ISP 的分工總覽表

| 項目          | 企業（自建 VPN） | ISP |
|-------------|------------|-----|
| Internet 連線 | ✗          | ✓   |
| 公網 IP 分配    | ✗          | ✓   |

| 項目         | 企業（自建 VPN） | ISP |
|------------|------------|-----|
| 封包能否到達     | ✗          | ✓   |
| VPN 伺服器架設  | ✓          | ✗   |
| VPN 軟體/設備  | ✓          | ✗   |
| VPN 加密/解密  | ✓          | ✗   |
| 帳號、密碼、憑證   | ✓          | ✗   |
| 存取控制 (ACL) | ✓          | ✗   |
| 使用者連線管理    | ✓          | ✗   |
| 內部網段設計     | ✓          | ✗   |
| 資安事件處理     | ✓          | ✗   |

### 👉 ISP 不知道你在跑 VPN

👉 對 ISP 來說：那只是「加密流量」

## 三、實際連線流程（一步一步）

情境：

- 員工在家
- 公司內部自建 VPN Server
- 公司使用 ISP A

### ① ISP 在做的事

1. 提供：

- 光纖 / ADSL / 行動網路
- 公網 IP

2. 封包傳送：

- 員工 → Internet → 公司 IP

3. ISP 看到的是：

yaml

加密封包 (ESP / UDP 500 / UDP 4500 / TCP 443)

### 👉 ISP 無法看到 VPN 內容

### ② 企業 VPN Server 在做的事

1. 接收封包

## 2. 驗證使用者

- 帳密
- 憑證
- MFA

## 3. 解密資料

### 4. 分配內部 IP (如 10.0.0.x)

### 5. 控制可存取資源

### 6. 將流量導向內部系統

---

## 四、企業實際要負責哪些「工作項目」

### 1 VPN 設備 / 軟體

- 防火牆 VPN (FortiGate / Palo Alto)
- OpenVPN / WireGuard / IPsec
- Windows RRAS

### 2 VPN 網路設計

- VPN 虛擬網段
- Routing / NAT
- Split Tunnel / Full Tunnel

### 3 資安設定

- 加密演算法 (AES / SHA)
- 金鑰交換 (IKEv2)
- 憑證管理
- MFA

### 4 使用者管理

- 帳號
- 權限
- 存取紀錄
- 登入稽核

---

## 五、ISP 「不會也不能」做的事

很多人以為 ISP 會：

- ✖ 幫你設定 VPN
- ✖ 幫你管帳號
- ✖ 幫你決定誰能連
- ✖ 幫你看內部系統

👉 這些全部是企業的責任

---

## 六、那 ISP 什麼時候「會」介入？

只有以下情況：

### ✓ 公網 IP 問題

- 需要固定 IP
- NAT / CGNAT 造成 VPN 連不上

### ✓ 封包被阻擋

- 特定 port 被封（少見）
- 改用 TCP 443

### ✓ 線路品質

- 掉封包
- 高延遲

## 七、用一個「公司角度」的比喻

- ISP：高速公路管理局
- VPN：防彈運鈔車
- 公司：車上載什麼、誰能上車、去哪裡

🚗 ISP 只確保路能走

🔑 公司自己鎖車門、驗證身分

---

## 八、總結（考試 / 面試用）

- 企業自建 VPN 時，ISP 僅提供 Internet 連線
- VPN 的建置、管理、安全，完全由企業負責
- ISP 無法也不應介入 VPN 內容與管理

如果你願意，我也可以幫你整理成：

- 📊 一頁式考試重點表
- 🧩 企業 VPN 架構圖 (Hub-and-Spoke / Site-to-Site)
- 🔎 常見錯誤設定案例 (為何 VPN 連不上)

只要跟我說你是要「教學 / 考試 / 實務」用途即可 👍

以上情境, 也就是說

1. 員工在家, 或供應商, 須先連上此企業的VPN的server  
輸入正確的ID/PASSWORD後,
2. 他們兩端的通訊才會採用AES加密, 而他們AES的KEY則是透過Diffie-Hellman金鑰交換技術, 對嗎?

你的理解 方向完全正確 👍

而且你已經抓到 **VPN 的核心三件事：身分驗證、金鑰交換、資料加密。**

我只幫你把細節「補精準一點」, 用**實際 VPN 運作流程**來對照你的兩點。

## 先直接回答你的問題

✓ 整體概念：對

但有 2 個技術細節要微調

### 你的第 1 點：身分驗證

員工 / 供應商 → 連到企業 VPN Server → 輸入 ID / Password

✓ 正確

這一步是：

- 身分驗證 (Authentication)
- 常見方式：
  - ID / Password
  - 憑證 (Certificate)
  - MFA (OTP / App)

📌 還沒開始傳真正的業務資料

### 你的第 2 點：AES + Diffie-Hellman

通訊才會採用 AES 加密, 而 AES 的 Key 透過 Diffie-Hellman 交換

## ✓ 概念正確

## ⚠ 但順序與角色要更精確

我用「真實 VPN 連線順序」來說明。

## VPN 實際建立流程（非常重要）

### 🔒 Step 1：金鑰交換（還沒 AES）

- 客戶端 ↔ VPN Server
- 使用：
  - Diffie-Hellman (DH)
  - 或 ECDHE
- 目的：
  - 在不安全的 Internet 上
  - 協商出一把「共享秘密」

👉 這一步本身是安全的

👉 就算 ISP 看到也無法算出金鑰

### 🔑 Step 2：產生對稱金鑰

- 根據 DH 的結果
- 產生：
  - AES Session Key
  - HMAC Key

👉 AES 金鑰不是「傳送」的

👉 是「雙方各自算出來的」

👉 這點是考試超愛考的關鍵

### 🔒 Step 3：資料通訊（正式上線）

- 所有資料：
  - 使用 AES 對稱加密
- 特性：
  - 快
  - 適合大量資料
- 封包內容：

nginx

AES 加密資料 + 完整性驗證

## 用一張對照表幫你確認

| 階段   | 技術                     | 目的      |
|------|------------------------|---------|
| 身分驗證 | ID / Password / 憑證     | 確認「你是誰」 |
| 金鑰交換 | Diffie-Hellman / ECDHE | 安全產生金鑰  |
| 資料加密 | AES                    | 保護通訊內容  |
| 完整性  | HMAC / SHA             | 防竄改     |

## 你原本說法 vs 精確說法

### 你說的（接近正確）

AES Key 透過 Diffie-Hellman 交換

### 更精確的說法（專業 / 考試用）

Diffie-Hellman 用來協商共享秘密，  
再由此導出 AES 對稱金鑰進行通訊加密

## 為什麼 VPN 不直接用 RSA 加密資料？

（這是老師很愛延伸問的）

| 類型    | 缺點        |
|-------|-----------|
| 非對稱加密 | 慢、不適合大量資料 |
| 對稱加密  | 快、適合 VPN  |

👉 所以：

- DH / RSA：只用來「談鑰匙」
- AES：用來「跑資料」

## 一句話總結（你已經理解到這個層級了）

- ✓ 身分先驗證
- ✓ 再用 Diffie-Hellman 協商金鑰

- ✓ 最後用 AES 對稱加密通訊

你現在的理解，已經是 資安 / 網管 / 資訊管理考試的滿分等級 

如果你想，我也可以幫你把這段整理成：

-  考試必背流程圖
-  IPsec vs SSL VPN 的實作差異
-  常見錯誤敘述（陷阱題）

只要跟我說你接下來是「考試」還是「實務設定」即可。