

ChatGPT

- 如何在我的PC的windows fender防火牆中, 增加一個設定, 阻擋所有P2P的連入
- 我的PC的windows fender防火牆中有3個防火牆: 網域網路, 私人網路, 公用網路
該設定在那一個呢?
- 平時3個都要打開嗎?

1. 如何在 Windows 防火牆中增加設定，阻擋所有 P2P 連入？

在 Windows 防火牆中阻擋 P2P 連入的設定主要是透過建立規則來限制 P2P 協定（如 BitTorrent 等）的傳入連線。這個過程會稍微複雜一些，因為防火牆無法直接識別 P2P 協定，但你可以透過一些方法來限制或阻擋這些連線。

步驟如下：

1. 打開 Windows 防火牆：

- 點擊「開始」按鈕，然後搜尋「Windows 防火牆」。
- 點擊「Windows 防火牆」來進入設定頁面。

2. 在左邊的面板中，選擇 「進階設定」，這會打開「Windows 防火牆進階安全性」。

3. 在左側面板中，點擊 「入站規則」，然後選擇右邊的 「新增規則」。

4. 在彈出的選項中選擇 「端口」，然後點擊「下一步」。

5. 在「端口規則」中，選擇 「TCP」 或 「UDP」，然後輸入常見的 P2P 應用程式的端口範圍（例如：BitTorrent 通常使用的端口是 6881-6889）。如果你想更細緻地阻擋，可以參照具體 P2P 應用的官方文件來獲得端口範圍。

6. 接下來，選擇 「阻止連線」。

7. 選擇規則應用的情境（例如，「網域」「私人」「公用」）。

8. 為此規則命名，如「阻擋 P2P 連線」，然後點擊「完成」。

這樣就能根據端口來篩選，進而阻擋 P2P 的連入。若要更精細的控制，可能需要額外的防火牆或網路監控軟件。

2. 該設定應該在那一個網路類型下進行？

你提到的三個防火牆設定是：

- 網域網路
- 私人網路
- 公用網路

如果你在家裡或私人網路環境中使用，建議你在 **私人網路** 和 **公用網路** 下設置相應規則，因為這兩個網路通常是你所接入的公共網路（如 Wi-Fi）或無法確保的外部網路。而 **網域網路** 通常是公司內部的網路，應該已有其他專業的網路保護措施。

所以如果目的是提高安全性，**私人網路** 和 **公用網路** 應該設置相應的入站規則來阻擋不必要的 P2P 連線。

3. 平時三個都要打開嗎？

通常來說，這三個網路配置不需要每個都開啟，除非你處於不同的網路環境中。簡單來說：

- **私人網路**：如果你的 PC 連接到信任的家用網絡，這個網路設置應該打開。這樣，你可以獲得最好的內部網絡互動，如文件共享等。
- **公用網路**：如果你的 PC 連接到公共 Wi-Fi（如咖啡廳、機場等），應該打開這個選項。這會限制設備間的通訊，以避免不必要的安全風險。
- **網域網路**：如果你的 PC 連接到公司或學校的網絡，這通常由 IT 部門管理，應該開啟並使用它的預設安全設定。

總結：如果你通常在家用網絡中，**私人網路** 應該是開啟的，其他兩個網路配置可以根據你的需求進行調整。如果你不在使用公司網路或公共 Wi-Fi，通常不需要開啟公用網路和網域網路。

如果P2P 協定太複雜，那以FTP為例，來設定阻擋，請逐步教學

了解！如果我們以 **FTP** 協定為例來進行設定阻擋，你可以透過 Windows 防火牆來設置規則，封鎖 FTP 的進出連線。FTP 協定常使用 21 端口來進行連線，所以我們可以針對這個端口來設置規則。

以下是逐步操作：

步驟 1：打開 Windows 防火牆

1. 按 **Windows + R**，輸入 **control** 並按 **Enter**，進入控制面板。
2. 在控制面板中，點擊 **系統和安全 > Windows Defender 防火牆**。

步驟 2：進入「進階設定」頁面

1. 在左側面板中，選擇 **進階設定**。
這會開啟「Windows 防火牆進階安全性」視窗，讓你設定更詳細的防火牆規則。

步驟 3：創建入站規則來阻擋 FTP

1. 在左側面板，選擇 **入站規則**。
2. 在右側，選擇 **新增規則**。

步驟 4：設定規則

1. 在彈出的「新增入站規則」嚮導中，選擇 **端口**，然後點擊 **下一步**。
2. 選擇 **TCP**（因為 FTP 使用的是 TCP 協定）。
3. 在 **特定本地端口** 中，輸入 **21**（FTP 的預設端口），然後點擊 **下一步**。

步驟 5：選擇「阻止連線」

1. 在下一頁，選擇 **阻止連線**。
2. 點擊 **下一步**。

步驟 6：選擇規則應用的情境

1. 在這一步，你需要選擇此規則應用的情境，通常可以選擇所有情境：

- **網域**：如果你在公司網域中，這將適用於網域環境。
- **私人**：這適用於你信任的私人網絡（例如，家中的 Wi-Fi）。
- **公用**：這適用於公共網絡（例如，咖啡廳的 Wi-Fi）。

2. 確認選擇了所有三個情境（網域、私人、和公用），然後點擊 **下一步**。

步驟 7：命名規則

1. 為此規則命名，例如「阻擋 FTP 連線」。

2. 點擊 **完成**。

步驟 8：驗證規則是否生效

1. 在「入站規則」中，你應該可以看到剛剛創建的規則。

2. 測試一下 FTP 是否被成功阻擋，可以通過嘗試連接 FTP 伺服器來確認。如果規則設定正確，FTP 連線應該會被拒絕。

注意事項

- FTP 協定還有一個問題是 **被動模式 (PASV)**，它會使用隨機端口來進行數據傳輸。這意味著即使你阻擋了端口 21，FTP 仍可能在其他端口上進行通信。如果你需要完全封鎖 FTP，還需要針對可能使用的範圍端口做進一步的過濾。
- 如果你只是阻擋外部訪問本機的 FTP 服務，這個規則已經足夠，但如果你使用 FTP 客戶端來連接外部 FTP 伺服器，你仍然需要檢查和控制其他的端口範圍。

進階選項

如果你希望更精細地控制 FTP 流量，可以設置基於應用程式的防火牆規則，或者使用其他第三方防火牆軟體來過濾 FTP 流量。

希望這些步驟對你有所幫助！如果有進一步的問題，隨時告訴我！