1. 負載均衡

反向代理可以將請求分發到多台後端服務器，幫助分擔負載，提高整體性能和可用性。

2. 安全性

反向代理隱藏了內部服務器的真實 IP 地址，增加了安全性。它可以作為防火牆，過濾惡意請求。

對用戶來說，回應其請求的伺服器是EDGE（反向代理伺服器Reverse Proxy），因此用戶不會得知源站的存在，也就避免源站的IP地址直接曝光，成為攻擊目標。

3. SSL 終止(X)

可以處理 HTTPS 加密，減少後端服務器的負擔，提高性能。客戶端與反向代理之間的通信是加密的，而反向代理與後端服務器之間的通信可以是非加密的。

4. 快取功能

反向代理可以緩存靜態內容（如圖片、CSS 文件等），減少後端服務器的請求數量，提高響應速度。

在我們的開發過程中呢，有的請求是需要動態的計算的，比如需要連接mysql數據庫去增刪查改，這些屬於動，而對於前端的一些文件html、css、js等這些文件呢，實際並不需要後台處理，那麼我們就可以通過動靜分離的模式將其區分開，就可以將這些靜態文件進行緩存操作，這樣就可以提高效率了。

5. 集中化訪問控制

可以集中管理訪問控制、身份驗證和其他安全策略，簡化了後端服務的配置。

6. 內容壓縮(X)

反向代理可以對響應進行壓縮，減少傳輸的數據量，提高加載速度。

7. 請求路由(X)

可以根據 URL、請求頭或其他參數，將請求路由到不同的後端服務，適用於微服務架構。

8. 監控和日志記錄(X)

反向代理可以集中監控和記錄所有進入的請求，便於分析和故障排除。

9. 故障轉移

可以在後端服務器出現故障時自動將請求轉發到其他可用的服務器，增強系統的可靠性。

10. API 網關功能

反向代理可以作為 API 網關，管理和路由不同的 API 請求，簡化服務之間的交互。

反向代理在現代網絡架構中廣泛應用，特別是在微服務和雲計算環境中，可以極大地提升系統的性能、安全性和可維護性。

防插旗置換（又稱為防止「旗子」替換）是一種網站安全措施，主要用來防止某些攻擊，比如跨站請求偽造（CSRF）和會話劫持。在這些攻擊中，惡意用戶可能會試圖利用合法用戶的會話來執行未經授權的操作。

防插旗置換的主要原則是：

防範 CSRF：通過要求每個請求都包含一個隨機生成的令牌（CSRF Token），這樣攻擊者就無法偽造合法請求。

驗證用戶會話：確保用戶的會話信息不被篡改或劫持，通常通過加密和安全的會話管理來實現。

使用 HTTPS：加密通信，防止中間人攻擊，保護數據的完整性和保密性。

總之，防插旗置換的目的是保護用戶的操作不被未經授權的第三方所篡改或模仿。

防插旗置換的英文是 "flag substitution prevention"。不過，這個術語在資訊安全中不如其他術語常見，例如 "CSRF protection"（跨站請求偽造防護）或 "anti-CSRF tokens"（反CSRF令牌）。

Tomcat server: Tomcat是web容器。你在做web項目時，多數需要http協議，也就是基於請求和響應，比如你在百度輸入一行內容搜索，那麼百度服務器如何處理這個請求呢，他需要創建servlet來處理，servlet其實就是java程序，只是在服務器端的java程序servlet通過配置文件攔截你的請求，並進行相應處理，然後展示給你相應界面。

前後端分離的網站開發有許多優點，包括：

獨立開發：

前端和後端可以獨立開發，團隊可以並行工作，提高開發效率。

技術棧靈活：

前端和後端可以使用不同的技術棧，開發者可以選擇最適合的工具和框架。

可維護性：

代碼結構清晰，前後端職責分明，便於維護和更新。

更好的用戶體驗：

前端可以通過 AJAX 或其他技術實現更流暢的用戶體驗，而無需重新加載整個頁面。

API重用：

後端提供的 API 可以被不同的前端應用（如 Web、移動端等）重用，提升了系統的靈活性和可擴展性。

分布式開發：

團隊可以根據需求將前後端部署在不同的服務器或服務上，支持微服務架構。

更易於測試：

前後端分離使得單元測試和集成測試更加方便，可以分別對前端和後端進行測試。

適應多種設備：

前端可以針對不同設備（如手機、平板、桌面）進行優化，提升響應式設計的效果。

通過這些優點，前後端分離的開發模式能夠提高開發效率、降低維護成本，並提升用戶體驗。