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。

3. SSL 終止

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. 緩存功能

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。

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

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

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

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）。