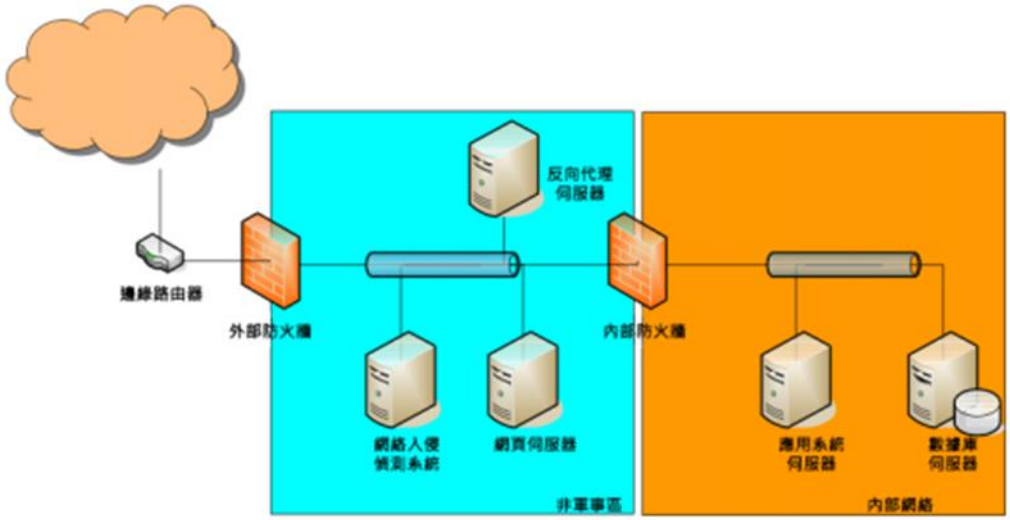
第八章
網頁及網上應用程式保安

8.1 網頁及網上應用系統保安架構

8.1.1 典型的網站及網上應用系統架構由三層組成，如下圖般分隔面向外界的網頁伺服器、應用系統伺服器及數據庫伺服器。透過這樣的層式架構，攻擊者即使成功由外界攻擊網頁伺服器，仍需要找尋方法攻擊內部網絡。



(a) 面向外界的網頁伺服器應置於非軍事區內（DMZ）。非軍事區是一個特別的網絡部分，裝有能接達互聯網服務的伺服器。載有敏感資料的伺服器都會置於內部網絡內，並設有額外保護。內部及外防火牆應由不同供應商提供，或兩者使用不同類型的防火牆，確保兩者不會有相同的保安漏洞。

(b) 應安裝網絡入侵偵測系統（NIDS）／入侵防禦系統（NIPS）以偵測／防範攻擊或非軍事區內的可疑通訊，以盡早識別攻擊，亦應經常以供應商提供的最新攻擊識別碼更新網絡入侵偵測系統／入侵防禦系統。此外，網上應用系統防火牆（WAF）及抗分布式拒絕服務（Anti-DDoS）攻擊保護是為特定應用系統而設的保安裝置，以保護網站及網上應用系統，防範如代碼插入攻擊及針對個別應用系統的分布式拒絕服務（DDoS）攻擊等常見威脅。應考慮部署這些裝置，以監察及阻截非軍事區內的通訊。

8.2 網頁伺服器保安

8.2.1 建議學校執行安全風險評估，以決定最合適的安全保護措施。

8.2.2 建議學校為網頁、應用系統、數據庫及檔案等相關的伺服器進行系統加強。

8.2.3 建議學校檢查其網頁伺服器，以確定伺服器已設定妥當並操作正常。為提升網頁伺服器的保安效能，學校可考慮以下建議：

(a) 依從資料保密級別的相關保安要求。

(b) 根據供應商的保安指引，安全地配置網頁伺服器。

(c) 以適當權限帳戶執行網頁伺服器程序。避免以特權帳戶（例如根帳戶、系統帳戶、管理員帳戶等）執行。

(d) 為網站組件安裝經審批的最新保安修補程式及避免使用已停止支援的組件。

(e) 根據系統加強指引和應用系統要求，嚴格配置接達權限，例如提供予公眾的資訊只容許唯讀接達。

(f) 停止所有沒有使用的帳戶，包括用戶及預設帳戶。若可以的話，在不影響網站及網上應用系統運作的情況下，移除沒被使用的帳戶。

(g) 避免於數據庫或檔案內儲存未受保護（如雜湊及／或加密）的用戶密碼。

(h) 於網頁伺服器安裝主機入侵偵測系統（HIDS）／入侵防禦系統（HIPS），特別是儲存或處理保密資料的網站，藉系統監察可疑活動或非法建立／刪除／修改／接達檔案。

(i) 覆檢由保安裝置如主機入侵偵測系統／入侵防禦系統所發出的警示及報告，盡早識別攻擊。此外，應經常以變更管理所批准的最新識別碼更新主機入侵偵測系統／入侵防禦系統。

(j) 不要透露配置資訊，如伺服器軟件版本、內部互聯網規約（IP）地址及檔案目錄結構等。

(k) 關閉不需要的模組。可以的話，刪除該等模組。

(l) 確保關閉不使用或較不常用的服務、規約、埠及功能，以減少受到攻擊的機會。

(m) 刪除網頁伺服器軟件內的預設或範例檔案。

(n) 對不應被搜尋或不應從公共搜尋器直接連結的內容，限制其網頁檢索。

(o) 識別執行網上應用系統的網頁伺服器內的重要檔案，並以合適控制如接達權限控制等，為它們提供保護。

(p) 當使用保密插口層（SSL）／傳輸層保安（TLS）時，備份私人密碼匙，作為伺服器核證之用，以防止未經授權的接達。

(q) 學校網站的備份包括資料檔案，數據庫和整個網站的設置。

8.3 網頁伺服器監控和保安事故處理

8.3.1 於保安監控方面，建議學校應主動覆檢網絡入侵偵測系統／入侵防禦系統發出的警報及報告，以盡早識別攻擊。

8.3.2 如遇上保安事故，例如網站塗改，阻斷服務攻擊／分布式拒絕服務攻擊，資訊科技人員應依照保安事故處理程序，處理有關事故，直至威脅得到紓緩。此外，學校應向警方及香港電腦保安事故協調中心（HKCERT）報告相關事故。

8.4 網上應用程式保安

8.4.1 以下是行政方面的建議措施，以強化網上應用系統及其所處理數據的保安：

(a) 為發展與維護網站及／或網上應用系統提供方向並列入關鍵的指引。

(b) 把網上應用系統編碼與發展的作業實務列入關鍵的指引。軟件發展小組應遵守一系列安全的網上應用系統編碼作業實務，用來應付一般的網上應用程式保安漏洞。

(c) 收集和管理敏感資訊及使用者數據時要符合政策與法規。

(d) 編製保安及品質保證計劃，並採用品質保證方法，如重新檢查原始碼、滲透測試、用戶驗收測試等。

(e) 在網上應用系統推出前或系統作出任何重大更改或升級後，進行完整的資訊科技保安審計。

8.5 保障學校網站的安全：

8.5.1 以下是保障學校網站安全的建議措施：

(a) 軟件更新：定期更新作業系統、應用程式和程式庫。

(b) 數據加密：加密網頁內的敏感資料。

(c) 遠程管理：使用安全的遙距接達方案進行網站管理。

(d) 驗證密碼：採用嚴謹的認證方式和密碼。

(e) 警報通知：啟用及檢視保安事件記錄和警告。

(f) 搜索索引：防止資料經搜尋引擎外泄。

(g) 安全掃描：進行保安漏洞掃描或滲透測試。

(h) 外判：選擇能夠滿足學校的保安要求的網站寄存服務供應商。

8.6 HTTPS 與網站安全

8.6.1 HTTPS 與網站安全的注意事項：

(a) 選用由認可核證機關發出的伺服器證書，並維持證書有效。

(b) 只使用較安全的規約（如 TLS 1.2）。

(c) 自動把網絡流量轉向到 HTTPS 網站（如啓用 HTTP Strict Transport Security（HSTS）支援）。

(d) 使用不易被破解的加密套件（如 SHA-256、AES 256-bit 等）及停用有安全風險的功能（如 TLS compression）。

(e) 定期更新作業系統、應用程式、程式庫及加密套件。

(f) 將敏感資料儲存於受適當保護的後端伺服器。

(g) 網址上不要包含敏感資料。

8.6.2 如要將網站設定為 HTTPS，學校需取得伺服器數碼證書。學校可參考以下政府資訊科技總監辦公室網頁所提供有關香港的認可核證機關的資訊：https://www.ogcio.gov.hk/tc/our_work/regulation/eto/ordinance/ca_in_hk/

8.7 抗分布式拒絕服務攻擊保護

8.7.1 分布式拒絕服務攻擊一般於互聯網發動。就此，解決容量及應用層分布式拒絕服務攻擊的其中一個有效方法是使用抗分布式拒絕服務攻擊的網絡管道清洗方案。這種方案提供實時保護，分析網絡通訊，阻截惡意通訊而容許合法的通訊。

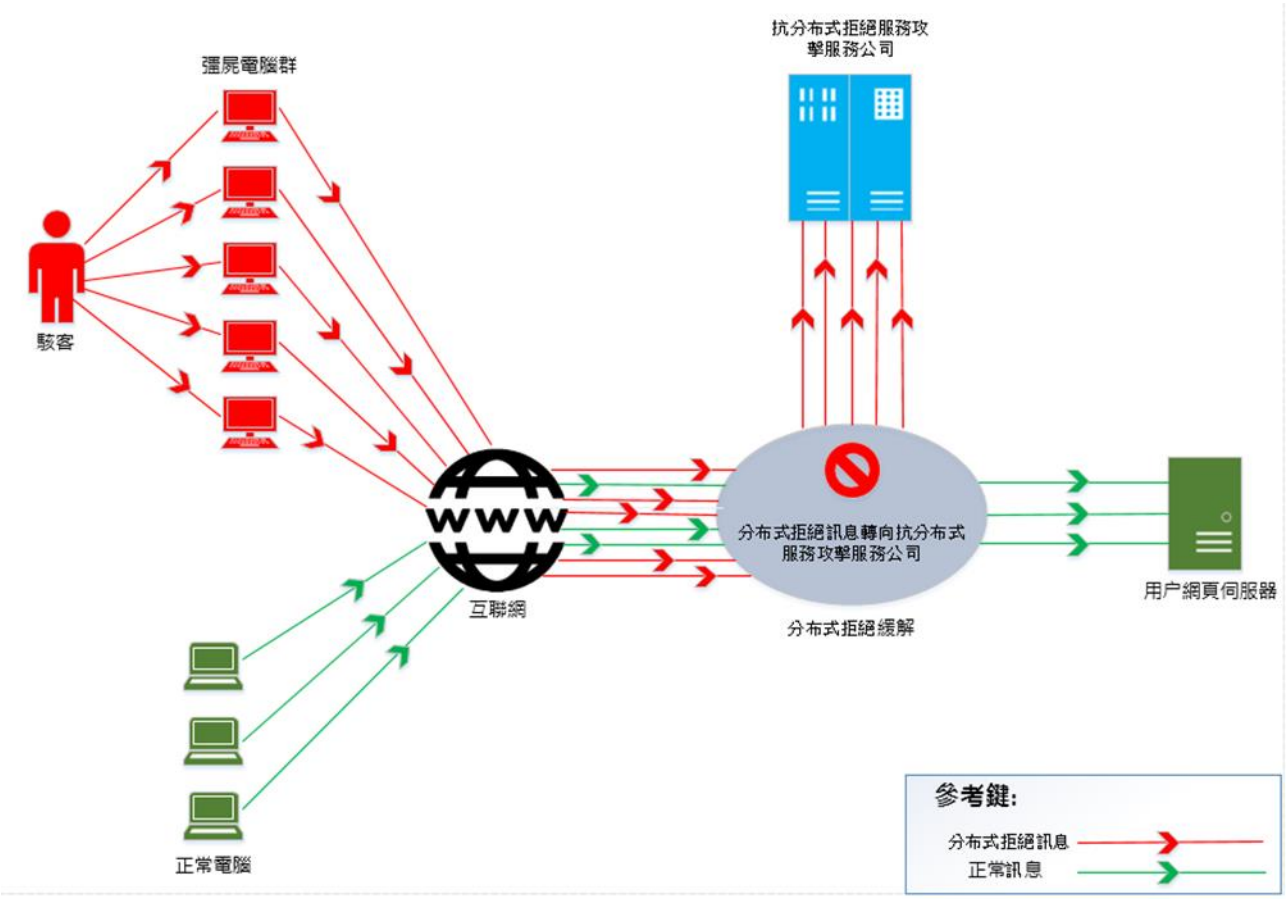
8.7.2 抗分布式拒絕服務攻擊清潔管道方案帶來的好處，包括實時及積極緩解分布式拒絕服務攻擊、更有效運用帶寬的同時提供基於網絡的防護，以及受到攻擊時立刻發出通知。

8.7.3 學校應界定服務要求，例如服務水平協議（SLA）、已申請的網絡管道清洗帶寬，以及對抗分布式拒絕服務攻擊保護的業務需要等，以此聘請外判或外聘抗分布式拒絕服務攻擊服務供應商。

8.7.4 用戶不應感受到抗分布式拒絕服務攻擊解決方案的運作，亦應盡量減少用戶參與其操作。用戶可能會接收有關分布式拒絕服務攻擊的警示和例行報告，以及服務水平摘要。用戶應在出現潛在接達問題，例如不能接達網站或遺失電郵的時候，向學校的資訊科技人員查詢或報告。

8.7.5 資訊科技人員負責由外判或外聘供應商提供的抗分布式拒絕服務攻擊解決方案的管理工作。資訊科技人員需要留意及及時跟進供應商發出的任何分布式拒絕服務攻擊警示，確保互聯網服務及有關電子服務維持運作。

8.7.6 資訊科技人員亦應覆檢服務報告，並與抗分布式拒絕服務攻擊解決方案供應商一起跟進問題，例如遺漏服務水平協議、未解決的技術問題，以及有需要時建議申請額外帶寬等。


抗分布式拒絕服務攻擊服務公司
殭屍電腦群
駭客
WWW
互聯網
分布式拒絕訊息轉向抗分布式服務攻擊服務公司
分布式拒絕緩解
用户網頁伺服器
正常電腦
參考鍵:
分布式拒絕訊息
正常訊息