中小企防火牆設定指南

防火牆可為電腦或網絡
阻截惡意或不必要的網絡通訊
有助防範網絡攻擊及數據外泄

www.cybersecurity.hk

www.cyberdefender.hk

GovCERT.HK 政府電腦保安事故協調中心

HKCERT 香港電腦保安事故協調中心

香港警務處

硬件與軟件防火牆有甚麼分別？

- 硬件防火牆是實體裝置；軟件防火牆則安裝於個別電腦或伺服器內，並通過應用程式進行操作。
- 硬件防火牆通常安裝在網絡的邊界，是抵禦網絡攻擊的第一道防線，在數據進入企業網絡前控制流入的通訊；軟件防火牆則控制進出電腦或伺服器的數據，阻截可疑通訊。

操作系統內的防火牆足夠嗎？

- 它是軟件防火牆的一種，在日常瀏覽互聯網期間或足以保護個別裝置。
- 可是，它未必足以為企業網絡提供全面覆蓋和保護，例如阻截特定通訊、病毒或惡意軟件感染。

路由器內的防火牆足夠嗎？

- 路由器使用網絡地址轉換（NAT）把進入網絡的請求導往指定裝置，功能接近硬件防火牆。
- 它可作不同的安全設定，例如利用白名單控制接達、把電腦納入網絡隔離區域（DMZ）。
- 儘管如此，它未必能如硬件防火牆般提供全面的覆蓋和保護。

哪種防火牆適合中小企？

須視乎業務需要和網絡規模而定。如要得到最佳保護，建議同時安裝硬件和軟件防火牆。但實際上，中小企在成本和維護方面有不同的考慮。以下是兩者的一些優點和缺點，以供參考：

- 硬件防火牆為整個網絡的裝置提供集中保護；軟件防火牆只保護個別電腦，並須分別配置和更新。
- 硬件防火牆佔用實體空間，安裝成本也較高。如在受保護的辦公室網絡外使用電腦，硬件防火牆便不能提供保護；軟件防火牆的配置則較有彈性，但可能會令電腦運作速度減慢。
- 硬件防火牆容易與其他保安功能整合，例如網絡入侵防禦系統（IPS）、沙盒隔離和威脅情報收集。

設置防火牆一般須知

基本防火牆保安

- 將防火牆韌體更新至最新版本
- 變更所有預設密碼
- 因應管理賬戶的權責設定有限的權限
- 不要共用帳戶

設置網絡區域

- 將功能、敏感度要求相近的裝置，組合成網絡區域
- 提供網絡服務（如電郵、虛擬私有網絡）的伺服器應放置在網絡隔離區域內以限制進入的通訊。其他伺服器（如檔案、資料庫）則應放置在內部伺服器區域內

設定接達控制名單

- 建立進出的接達控制名單，讓指定的通訊進出各區域
- 名單須列明能夠進出或被拒絕進出的IP地址／範圍和埠號碼

測試防火牆配置

- 進行漏洞掃描和滲透測試，以確保防火牆運作正常
- 為配置保存備份

防火牆管理

- 定期進行覆檢和審計，以及妥善保存和審查日誌記錄，確保防火牆運作正常