防 火 牆

產品類型

從防火牆產品和技術發展來看，分爲三種類型：基於路由器的包過濾防火牆、基於通用作業系統的防火牆、基於專用安全作業系統的防火牆。

LAN 介面　　列出支援的 LAN 介面類型：防火牆所能保護的網路類型，如乙太網、快速乙太網、千兆以太網、ATM、權杖環及 FDDI 等。支援的最大 LAN 介面數：指防火牆所支援的區域網路介面數目，也是其能夠保護的不同內網數目。

伺服器平臺：防火牆所運行的作業系統平臺（如 Linux、UNIX、Win NT、專用安全操作系統等）。

協定支援

支援的非 IP 協定：除支援 IP 協定之外，又支援 AppleTalk、DECnet、IPX 及 NETBEUI 等協定。

建立 VPN 通道的協定： 構建 VPN 通道所使用的協定，如密鑰分配等，主要分爲 IPSec，PPTP、專用協定等。

可以在 VPN 中使用的協定：在 VPN 中使用的協定，一般是指 TCP/IP 協定。

加密支援

支援的 VPN 加密標準：VPN 中支援的加密演算法, 例如資料加密標準 DES、3DES、RC4 以及國
內專用的加密演算法。

除了 VPN 之外，加密的其他用途： 加密除用於保護傳輸資料以外，還應用於其他領域，
如身份認證、報文完整性認證，密鑰分配等。

提供基於硬體的加密： 是否提供硬體加密方法，硬體加密可以提供更快的加密速度和更
高的加密強度。

認證支援

支援的認證類型： 是指防火牆支援的身份認證協定，一般情況下具有一個或多個認證方
案，如 RADIUS、Kerberos、TACACS/TACACS＋、 口令方式、數位證書等。防火牆能夠爲本地或遠端用戶提供經過認證與授權的對網路資源的訪問，防火牆管理員必須決定客戶以何種方式通過認證。

列出支援的認證標準和 CA 互操作性：廠商可以選擇自己的認證方案，但應符合相應的國際標準，該項指所支援的標準認證協定，以及實現的認證協定是否與其他 CA 產品相容互通。

支援數位證書：是否支援數位證書。

訪問控制

通過防火牆的包內容設置：包過濾防火牆的過濾規則集由若干條規則組成，它應涵蓋對所有出入防火牆的資料包的處理方法，對於沒有明確定義的資料包，應該有一個缺省處理方法；過濾規則應易於理解，易於編輯修改；同時應具備一致性檢測機制，防止衝突。IP 包過濾的依據主要是根據 IP 包頭部資訊如源地址和目的地址進行過濾，如果 IP 頭中的協定欄位表明封裝協定爲 ICMP、TCP 或 UDP，那麼再根據 ICMP 頭資訊（類型和代碼值）、TCP 頭資訊（源端口和目的埠）或 UDP 頭資訊（源埠和目的埠）執行過濾，其他的還有 MAC 地址過濾。應用層協定過濾要求主要包括 FTP 過濾、基於 RPC 的應用服務過濾、基於 UDP 的應用服務過濾要求以及動態包過濾技術等。

在應用層提供代理支援：指防火牆是否支援應用層代理，如 HTTP、FTP、TELNET、SNMP 等。代理服務在確認用戶端連接請求有效後接管連接，代爲向伺服器發出連接請求，代理服務器應根據伺服器的應答，決定如何回應用戶端請求，代理服務進程應當連接兩個連接（客戶端與代理服務進程間的連接、代理服務進程與伺服器端的連接）。爲確認連接的唯一性與時效性，代理進程應當維護代理連接表或相關資料庫（最小欄位集合），爲提供認證和授權，代理進程應當維護一個擴展欄位集合。

在傳輸層提供代理支援：指防火牆是否支援傳輸層代理服務。允許 FTP 命令防止某些類型文件通過防火牆：指是否支援 FTP 文件類型過濾。

用戶操作的代理類型：應用層高級代理功能，如 HTTP、POP3 。

支援網路位址轉換(NAT)：NAT 指將一個 IP 位址域映射到另一個 IP 位址域，從而爲終端主機提供透明路由的方法。NAT 常用於私有地址域與公有地址域的轉換以解決 IP 地址匱乏問題。在防火牆上實現 NAT 後，可以隱藏受保護網路的內部結構，在一定程度上提高了網路的安全性。

支援硬體口令、智慧卡： 是否支援硬體口令、智慧卡等，這是一種比較安全的身份認證技術。

防禦功能

支援病毒掃描： 是否支援防病毒功能，如掃描電子郵件附件中的 DOC 和 ZIP 文件，FTP 中的下載或上載文件內容，以發現其中包含的危險資訊。

提供內容過濾： 是否支援內容過濾，資訊內容過濾指防火牆在 HTTP、FTP、SMTP 等協定層，根據過濾條件，對資訊流進行控制，防火牆控制的結果是：允許通過、修改後允許通過、禁止通過、記錄日誌、報警等。 過濾內容主要指 URL、HTTP 攜帶的資訊：Java Applet、 JavaScript、ActiveX 和電子郵件中的 Subject、To、From 域等。

能防禦的 DoS 攻擊類型：拒絕服務攻擊(DoS)就是攻擊者過多地佔用共用資源，導致服務器超載或系統資源耗盡，而使其他用戶無法享有服務或沒有資源可用。防火牆通過控制、檢測與報警等機制，可在一定程度上防止或減輕 DoS 黑客攻擊。

阻止 ActiveX、Java、Cookies、Javascript 侵入：屬於 HTTP 內容過濾，防火牆應該能夠從 HTTP 頁面剝離 Java Applet、ActiveX 等小程式及從 Script、PHP 和 ASP 等代碼檢測出危險代碼或病毒，並向瀏覽器用戶報警。同時，能夠過濾用戶上載的 CGI、ASP 等程式，當發現危險代碼時，向伺服器報警。

安全特性

支援轉發和跟蹤 ICMP 協定（ICMP 代理）：是否支援 ICMP 代理，ICMP 爲網間控制報文協定。

提供入侵即時警告：提供即時入侵告警功能，當發生危險事件時，是否能夠及時報警，報警的方式可能通過郵件、呼機、手機等。

提供即時入侵防範：提供即時入侵回應功能，當發生入侵事件時，防火牆能夠動態回應，調整安全策略，阻擋惡意報文。

識別/記錄/防止企圖進行 IP 位址欺騙：IP 地址欺騙指使用僞裝的 IP 地址作爲 IP 包的源地址對受保護網路進行攻擊，防火牆應該能夠禁止來自外部網路而源地址是內部 IP 地址的資料包通過。

管理功能

通過集成策略集中管理多個防火牆：是否支援集中管理，防火牆管理是指對防火牆具有管理許可權的管理員行爲和防火牆運行狀態的管理，管理員的行爲主要包括：通過防火牆的身份鑒別，編寫防火牆的安全規則，配置防火牆的安全參數，查看防火牆的日誌等。防火牆的管理一般分爲本地管理、遠端管理和集中管理等。

提供基於時間的訪問控制：是否提供基於時間的訪問控制。

支援 SNMP 監視和配置：SNMP 是簡單網路管理協定的縮寫。

本地管理：是指管理員通過防火牆的 Console 口或防火牆提供的鍵盤和顯示器對防火牆進行配置管理。

遠端管理：是指管理員通過乙太網或防火牆提供的廣域網介面對防火牆進行管理，管理的通信協定可以基於 FTP、TELNET、HTTP 等。

支援帶寬管理：防火牆能夠根據當前的流量動態調整某些用戶端佔用的帶寬。

負載均衡特性：負載均衡可以看成動態的埠映射，它將一個外部地址的某一 TCP 或 UDP 埠映射到一組內部地址的某一埠，負載均衡主要用於將某項服務（如 HTTP）分攤到一組內部伺服器上以平衡負載。

失敗恢復特性（failover）：指支援容錯技術，如雙機熱備份、故障恢復，雙電源備份等。

記錄和報表功能

防火牆處理完整日誌的方法：防火牆規定了對於符合條件的報文做日誌，應該提供日誌資訊管理和存儲方法。

提供自動日誌掃描：指防火牆是否具有日誌的自動分析和掃描功能，這可以獲得更詳細的統計結果，達到事後分析、亡羊補牢的目的。

提供自動報表、日誌報告書寫器：防火牆實現的一種輸出方式，提供自動報表和日誌報告功能。

警告通知機制：防火牆應提供告警機制，在檢測到入侵網路以及設備運轉異常情況時，通過告警來通知管理員採取必要的措施，包括 E－mail、呼機、手機等。

提供簡要報表（按照用戶 ID 或 IP 地址）：防火牆實現的一種輸出方式，按要求提供報表分類列印。

提供即時統計：防火牆實現的一種輸出方式，日誌分析後所獲得的智慧統計結果，一般是圖表顯示。

列出獲得的國內有關部門許可證類別及號碼：這是防火牆合格與銷售的關鍵要素之一，其中包括：公安部的銷售許可證、國家資訊安全測評中心的認證證書、總參的國防通信入網證和國家保密局的推薦證明等。