

淺談防火牆

華銀資訊室 王世達

什麼是防火牆

網路安全涉及到通信和網路、密碼學、芯片、操作系統、數據庫等多方面技術。目前的網路安全產品，主要分為以下幾類：3A類產品、安全操作系統、安全隔離與信息交換系統、安全WEB、防毒產品、IDS和弱點評估產品、防火牆、VPN、保密機制、PKI等。其中，防火牆是網路安全的第一道屏障，安全技術也比較成熟。

防火牆是目前最為流行也是使用最為廣泛的一種網路安全技術，在構建安全網路環境的過程中，防火牆作為第一道安全防線，正受到越來越多用戶的關注，防火牆是一個系統，主要用來執行兩個網路間的訪問控制策略，它可為各類企業網路提供必要的訪問控制，但又不造成網路的瓶頸，並通過安全策略控制進出系統的數據，保護企業的關鍵資源。

企業在構建安全網路環境的過程中，總是把防火牆列為首先要購買的網路安全設備，所以目前防火牆已經成為世界上用得最多的網路安全產品之一，那麼防火牆是如何保證網路系統的安全，又如何實現自身的安全？

其實防火牆並不是真正的牆，它是一種防範措施的總稱，是一種有效的網路安全模型，是組織總體安全策略的一部份，它阻擋的是對內，對外的非法訪問與不安全數據的傳輸，在網際網路的時代，透過它隔離風險區域(即網際網路的各種風險)與安全區域(組織內部網路)的連接，能夠增強內部網路的安全性，防火牆可以作為不同網路間之訊息出入口，能根據企業的安全策略控制出入網路的資訊流，且本身具有較強的抗攻擊能力，它是提供資訊安全服務，實現網路和資訊安全的基礎建設，在邏輯上，防火牆是一個分離器，限制器及分析器，有效地監控內部網路與網際網路間之任何活動，保護企業內部網路的安全。

防火牆發展概述

傳統的防火牆通常是存取控制列表(ACL)的數據流“篩濾器”，安裝在內網域的入口處。隨著網路技術的發展，出現了幾種特殊的防火牆技術，數據流通過網路控制節點時就會被檢查，以保護內網域免受攻擊。在實際

運用上，這些技術差別非常大，有的是在OSI模型的網路和傳輸層執行對數據封包的檢查，有的則是在應用層實施檢查。

迄今為止，有四種主要的數據封包過濾技術，分別是靜態封包過濾、應用層(代理伺服器)、電路層(透明代理)和狀態封包檢查(動態封包過濾)。靜態封包過濾是最差的安全解決方案，其應用存在著一些不可克服的限制。現在已經沒有防火牆廠商單獨使用這種技術。應用層和電路層是比較好的安全解決方案，它們在應用層檢查數據封包。但是，我們不可能對每一個應用都執行這樣的代理伺服器，而且部分應用技術還要求客戶端安裝有特殊的軟體。這兩種解決方案在性能上也有很大的不足之處。狀態封包過濾是依連接狀態對數據封包進行檢查。由於狀態封包過濾解除了靜態封包過濾的安全限制，並且比代理技術在性能上有了很大的改善，因而大多數防火牆廠商都採用這種技術。但是隨著主動攻擊的增多，狀態過濾技術也面臨著巨大的挑戰，更需要其它新技術的輔助。

除了訪問控制功能外，現在大多數的防火牆製造商在自己的設備上還集成了其它的安全技術，如NAT和

VPN。

從技術層面看：

防火牆技術本身經歷3次巨變，早期的防火牆只是採用簡單的“封包過濾技術”-即是對進出網路的數據封包進行檢查，雖然效率高但漏洞大，缺乏安全性，很快被淘汰出局，隨後的應用代理技術，讓通信經應用代理層轉發，可徹底隔絕兩端的直接通信，可想而知安全性增加很多但卻是犧牲了效率。

隨後一家以色列的技術公司Check Point 創建的狀態監測技術，擯棄了前兩種技術的不足，它對每一個數據封包的檢查不僅根據策略表，還考慮會話狀態，提供了對傳輸層的完全控制能力，狀態監測技術一經推出就廣受大眾青睞，目前他已經成為防火牆的技術標準，全球幾乎所有的主流防火牆公司都採用此技術。

從防火牆的型態看：

追根究底，防火牆畢竟是一種軟體技術，但防火牆的型態，同樣經歷了三代演變。

從軟體到PC硬體

早期的防火牆多以軟體型態出現，以軟體著稱的Check Point 公司，典型的第一代軟體式防火牆架構是運行在標準的PC或小型伺服器以及

通用操作系統(OS)的平台上,在沒有其他安全技術或設備時,軟體式防火牆非常流行,但很快軟體式防火牆的弱點開始暴露出來,通用操作系統並非專門為安全設計,本身帶有很多漏洞,尤其是當微軟操作系統在全世界流行的同時,卻也將大量的漏洞或Bug帶到了每一個客戶終端設備上,這些漏洞很快成為攻擊目標,就像建立在浮沙上的摩天大廈,有何安全可言?從性能上說,CPU, RAM, PCI等資源是各種應用程式共享公共的,而防火牆的拆包解包需要大量的數學運算,CPU不勝負荷,性能大受影響。

防火牆廠商很快發現了問題,開始在世界各地尋求硬體合作廠商,於是目前最流行的第二代防火牆架構---軟體+硬體因應而生。

國外的第二代防火牆以Cisco和Nokia為代表,這類防火牆的特點是仍保留PC結構,但不再使用通用操作系統,而使用各類廠商自主研發的專用操作系統,同時不再以PC的面貌出現,而是一些專用的硬盒子。

為安全而訂製的操作系統,從根本上解決了軟體式防火牆存在的嚴重安全隱憂,由於是專用設備,在防火牆上並不運跑其他的應用系統,因此整體處理性能上也大幅提高,另外它

最大的優點是靈活性高,通過軟體就可以完成各類工作,且升級非常容易,只需透過網路下載,將內置的軟體升級同樣在其中整合多種安全功能也輕而易舉,現在某些廠商整合了VPN、病毒掃描、IDS或內容過濾等,就是靈活性帶來的好處。

無論是廠商主推的百兆防火牆或是千兆防火牆無不是這種架構,但是隨著寬頻網路的發展,隨著商業運算複雜程度的增加,PC結構的防火牆在巨大數據流量的狀況下,逐漸顯得力不從心,典型的寬頻應用會帶來數萬甚至數十萬的並行連結(connection),更多的連結(connection)意味著更多的中斷,這會帶來處理能力的急遽下降,甚至設備當機,因此連結(connection)數是最能展現防火牆處理能力的參數之一,另一個參數是加解密能力,二代防火牆需借助附加的加密卡,才能達到較高的處理速度,因此,在電信級應用以及每天大量數據傳輸的大型企業網路,這類防火牆逐漸陷入困境。

從PC硬體到 ASIC硬體

人們開始考慮使用ASIC技術,這種演變與其他網路設備非常類似,

如路由器的發展，經歷了由PC路由軟體，到專用路由器，到ASIC的路由交換器的過程。

ASIC的全名為 Application Specific Integrated Circuit，意思為專用的系統集成電路，是一種具有邏輯處理的加速處理器，簡單的說，ASIC就是用硬體的邏輯電路實現軟體的功能，使用ASIC可把一些原先由CPU完成的通用工作，用專門的硬體實現，從而在性能上獲得突破性的提高，因此，在單一領域，人們希望ASIC能帶來較高的運算效率。

第三代防火牆是以NetScreen公司為代表，1999年NetScreen 在關鍵業務處理中拋棄了CPU而以ASIC替代，這使原先需要上萬條指令才能完成的處理，可在瞬間由數個循環完成，多總線結構保證在端口上進行數據傳輸時，內部仍可高速處理數據，不再受傳統的“中斷”限制。

第三代防火牆也採用專用操作系統和CPU，有人對此仍有所詬病，因為本質上仍然沒有走出軟體式防火牆的窠臼，但事實上它並不依賴操作系統的性能，因為他們的作用只有兩個----驅動ASIC硬體和管理接口，所以他們只負責總體協調，卻不參與任何數據處理工作，在ASIC高效處理數

據時，CPU甚至很空閒，所以第三代防火牆的 CPU，甚至沒有前兩代那麼高檔，升級速度也不需太快。

第三代防火牆仍不完善，ASIC的特點使得它的靈活性相對較差，如果要進行升級，只能換一台設備，如果要加入新功能，也只能另買設備，第三代防火牆廠商，目前正在考慮解決這些問題，如何在硬體的結構上兼顧靈活性？他們做法有的提供系統升級方案，讓設備預留容量及能力，以支持未來新的需求，有的與其他策略性廠商合作的銷售方案，有些廠商援引了刀鋒 (blade) 裝卸容易的特性，解決軟體升級。我們相信改進後的第三代防火牆必將成為未來的主流。

附註：刀鋒是一種薄型的系統，可像書本插到書架裡一樣插入機櫃。機櫃則有刀鋒共用的元件，例如電源供應和連外網路。除了伺服器之外，刀鋒還可容納其他的設備，例如加密加速或網路刀鋒，也因此許多人把刀鋒伺服器視為「模組化運算」(modular computing) 的典範。

防火牆未來的技術趨勢

隨著新的網路攻擊的出現，防火

牆技術也有了新的發展趨勢。

第一個趨勢就是一些防火牆廠商，把在AAA系統上運用的用戶認證及其服務擴展到防火牆中，使其擁有可能支援用戶角色的安全策略功能。該功能在無線應用中非常必要，同時它也使得防火牆的功能從其傳統的角色得以擴展，從而能在內網中發揮更大的作用。

第二種趨勢是在防火牆中加入內容過濾功能，這樣防火牆就可以防止越來越多的針對應用層的攻擊。這種技術在性能上比採用網路層技術的防火牆有很大的優勢，卻不會以犧牲安全作為提升性能的代價。

第三種趨勢就是將IDS模組加入到防火牆中，這樣，防火牆就會具有更高的智能來分析網路數據，從而能迅速地對攻擊產生反應，而不是僅進行數據封包的檢查。

第四種趨勢是使防火牆具有病毒防護功能。防止病毒在網路中的傳播比坐在PC面前等待攻擊的發生更加積極。擁有病毒防護功能的防火牆可以大大減少公司的損失。

除了以上提到的幾種安全特性，QoS和負載均衡也是現代防火牆系統的另外兩種必要的特性。

防火牆的系統管理也有一些發展

趨勢：首先是集中式管理，分布式和分層的安全架構是將來的趨勢。集中式管理可以降低管理成本，並保證在大型網路中安全策略的一致性。快速響應和快速防禦也要求採用集中式管理系統。其次是強大的稽核功能和自動日誌分析。這兩點的應用可以更早地發現潛在的威脅及預防攻擊的發生。

總括的說，未來防火牆的發展趨勢是朝高速、多功能化、更安全的方向發展。

1、高速。目前防火牆一個很大的局限性是速度不夠，真正達到線速的防火牆少之又少。防患DoS（拒絕服務）是防火牆一個很重要的任務，防火牆往往用在網域出口，如造成網路堵塞，再安全的防火牆也無法使用。運用ASIC、FPGA和網路處理器是實現高速防火牆的主要方法，但尤以採用網路處理器最優，因為網路處理器採用微碼編程，可以根據需要隨時升級，甚至可以支持IPv6，而採用其他方法就不那麼靈活。實現高速防火牆，算法也是一個因素，因為網路處理器中集成了很多硬體式平行處理單元，因此比較容易實現高速。對於採純CPU的防火牆，就必需有算法支撐，例如ACL算法。

2、多功能化。多功能也是防火牆的發展方向之一，鑒於目前路由器和防火牆價格都比較高，網路環境也越來越複雜，一般用戶總希望防火牆可以支持更多的功能，滿足架設網路和節省投資的需要。例如，防火牆支持廣域網路，並不影響安全性，但在某些情況下卻可以為用戶節省一台路由器，支持部分路由器協定，如路由、撥號等，可以更好地滿足架網需要；支持IPSec VPN，可以利用網際網路架構安全的專用通道，既安全又節省了專線投資。據IDC統計，國外90%的加密VPN都是通過防火牆實現的。

3、安全。未來防火牆的操作系統會更安全。隨著算法和芯片技術的發展，防火牆會更多地參考應用層分析，為應用提供更安全的保障。在資訊安全的發展與對抗過程中，防火牆的技術一定會不斷更新、日新月異，在資訊安全的防禦體系中，發揮堡壘的作用。

防火牆系統結構的發展

近年來隨著千兆(Giga)網路開始在國內大規模推廣應用，隨著網路應用的增加，對網路頻寬提出了更高的要求。這意味著防火牆要能夠以非常高的速率處理數據。另外，在以後幾

年裡，多媒體應用將會越來越普遍，數據穿過防火牆要求最少的延遲，用戶對千兆防火牆的需求已逐漸升溫。為了滿足這種需要，一些防火牆製造商開發了ASIC的防火牆和網路處理器(NP)的防火牆。從執行速度的角度看來，網路處理器的防火牆也是軟體的解決方案，它需要在很大程度上依賴軟體的性能，但是由於這類防火牆中有一些專門用於處理數據層面任務的引擎，從而減輕了CPU的負擔，這類防火牆的性能要比傳統防火牆的性能好很多。與ASIC的純硬體式防火牆相比，網路處理器的防火牆具有軟體色彩，因而更加具有靈活性。ASIC的防火牆使用專門的硬體處理網路數據流，比起前兩種類型的防火牆具有更好的性能。但是純硬體的ASIC防火牆缺乏可編程性，這就使得它缺乏靈活性，從而跟不上防火牆功能的快速發展。理想的解決方案是增加ASIC芯片的可編程性，使其與軟體更好地配合。這樣的防火牆就可以同時滿足靈活性和運跑性能的要求。

千兆(Giga)防火牆：NP還是ASIC？

在很多網路環境下，傳統的 X86 體系架構的防火牆已不能滿足千兆防火牆高吞吐量、低遲延的要求，因

此，兩種新的技術，即網絡處理器（Network Processor）和專用集成電路（ASIC）技術成為眾多國內外廠家實現千兆防火牆的主要選擇。可以說，防火牆的硬體系統架構正面臨著一次變革。

百兆(Mega)防火牆的不足

在百兆防火牆時代，國內外防火牆廠商普遍採用的是用CPU配合軟體的技術方案。雖然很多廠家也把它稱之為硬體式防火牆，但實際上都是 X86 架構的伺服器。這類防火牆一般運跑在經過強化(裁減)的操作系統上（通常是Linux或BSD），所有的數據包括解析和審查工作都由軟體完成。雖然這種技術方案在百兆防火牆市場取得了很大的成功，但由於CPU處理能力和PCI速度的制約，在實際運用中，尤其在小封包情況下，這種結構的千兆防火牆遠遠達不到千兆的轉發速度（64字長封包，雙向轉發速率一般為百分之二十以下），難以滿足千兆骨幹網路的應用要求。

千兆防火牆的兩種技術實現

要實現真正的千兆防火牆，目前的技術基本上有兩種選擇：一種是採

用網路處理器，另一種是採用ASIC。下面來分析一下這兩種技術架構各自的特點。

網路處理器是專門為處理數據封包而設計的可編程處理器，它的特點是內含了多個數據處理引擎，這些引擎可以平行進行數據處理工作，在處理2到4層的分組數據上比通用處理器具有明顯的優勢。網路處理器對數據封包處理的一般性任務進行了強化，如TCP/IP數據的校驗和計算、封包分類、路由查尋等。同時硬體式系統架構的設計也大多採用高速的接取技術和總線規範，具有較高的I/O能力。這種網路處理器的網路設備的封包處理能力得到了很大的提升。它具有以下幾個方面的特性：完全的可編程性、簡單的編程模式、最大化系統靈活性、高處理能力、高度功能集成、開放的編程接口、第三方支持能力。網路處理器架構的防火牆與通用CPU架構的防火牆相比，在性能上可以得到很大的提高。網路處理器能彌補通用CPU架構性能的不足，同時又不需要具備開發ASIC技術的防火牆所需要的大量資金和技術累積。

第二種方案是採用ASIC技術的架構。ASIC (Application Specific Integrated Circuit) 稱為專用的系統集成電路，是一種帶有邏輯處理的

加速處理器，簡單的說，ASIC 就是用硬體的邏輯電路實現軟體的功能，Netscreen是採用該技術的代表廠商。採用ASIC技術可以為防火牆應用設計專門的數據封包處理匯流排，強化儲存設備等資源的利用，是公認的使防火牆達到線速千兆，滿足千兆環境骨幹使用的技術方案。Netscreen公司也因此取得了令人矚目的成功。但ASIC技術開發成本高、開發周期長且難难度大，一般的防火牆廠商難以具備相應的技術和資金。

附註：乙太網路吞吐量最大理論值稱線速，即指網路設備有足夠的能力以全速處理最小的數據封包轉發。

那種方案更適合用戶應用

網路處理器與ASIC方案哪種更適合千兆防火牆的應用是目前爭議的一個焦點。用戶可以從性能、靈活性、功能完整性、成本、開發難度、技術成熟性等方面來評比。從性能上看，由于網路處理器的防火牆本質是軟體式的解決方案，它在很大的程度上依賴軟體設計的性能，而ASIC由於是將算法固化在硬體中，因而在性能上有比較明顯的優勢。

反過來看，網路處理器的軟體色

彩使它具有更好的靈活性，在升級維護方面有較大的優勢。純硬體的ASIC防火牆缺乏可編程性，這使得它缺乏靈活性從而跟不上防火牆功能的快速發展。

現代的ASIC技術通過增加ASIC芯片的可編程性，使其與軟體更好地配合，從而同時滿足來自靈活性和運行性能的要求。從實現功能方面看，ASIC技術可以比較容易地集合IDS、VPN等功能，也有產品已經實現了內容過濾和防毒功能，而網路處理器受限於它的計算能力，這些功能一般只能靠平行(n-way)處理器來實現。從今後產品的成本上看，一片網路處理器的價格在三、四百美金左右，如果需要平行處理器，還要加上平行處理器的成本。ASIC技術前期如果使用FPGA (Field Programmable Gate Arrays, 現場可編程陣列) 來實現，兩者價格大致相當。不過如果量產投片以後，ASIC的價格可以降低一個量級，因而長遠來看ASIC技術更有潛力。

在開發難度、開發成本和開發周期方面，網路處理器技術有比較明顯的優勢，畢竟網路處理器產生的一大原因，就是降低這方面的門檻，這也是很多防火牆企業選中網路處理器的原因。不過從技術成熟度方面來看，

相比ASIC這樣已經為實現證明了的成熟技術，網路處理器用於防火牆，其實是近一年多才出現的。在此之前網路處理器在市面上的表現並不理想，一般只被用於低端路由器、交換機等數據通信產品。究其原因，主要是網路處理器開發需要的編程技術，比預期的複雜困難，而且在實際應用中的性能往往並不理想，遠低於其廠商所宣稱性能。這種技術應用在防火牆這樣複雜的網路設備上，究竟能否在不影響功能的前提下達到預期的性能？還有待觀察。

目前防火牆的體系結構已經處於一個更新時代門檻上，未來的發展趨勢基本上是網路處理器與ASIC兩條道路。從性能、功能、技術成熟度方面考量，ASIC方案較好，從進入門檻、研發成本和靈活性考量則網路處理器占優勢。

從目前的情況來看，高檔防火牆大部分採用的是ASIC技術，少部分選用網路處理器。今後高檔防火牆的技術將是ASIC和網路處理器這兩種主流技術並存，它們各自都會繼續向前發展，在速度、功能方面都還有很大的進展空間。究竟誰將成為最後的贏家，只能有待時間的檢驗了。而用戶在選擇千兆防火牆產品時也要考慮廠

商實力、實際應用需求、採購成本、防火牆技術與產品的成熟度等多種因素全盤考量為宜。

如何選擇防火牆

防火牆作為網路安全體系的基礎和核心控制設備，它貫穿於受控網路通信主幹線，對通過受控幹線的任何通信行為進行安全處理，如控制、稽查、警告、反制等，同時也承擔著繁重的通信任務。由於其自身處於網路系統中的敏感位置，還要面對各種安全威脅，因此，選用一個安全、穩定和可靠的防火牆產品，其重要性不言而喻。以下是一些參考項目

一、防火牆自身是否安全

防火牆自身的安全性主要體現在自身設計和管理兩個方面。設計的安全性關鍵在於操作系統，只有自身具有完整信任關係的操作系統才可以談論系統的安全性。而應用系統的安全是以操作系統的安全為基礎的，同時防火牆自身的安全也直接影響整體系統的安全性。防火牆安全指標最終可歸結出以下兩項：

- 1、防火牆是否採用安全(甚至是專用)的操作系統；

2、防火牆是否採用專用的硬體平台。

只有採用安全（甚至是專用）的操作系統及專用硬體平台的防火牆才可能保證防火牆自身的安全。

國際上描述資訊安全產品或系統安全的參考文件ISO15408標準，可提供我們參考，ISO15408標準內容分為獨立但彼此相關連的三部分：

Part 1 為導論，內容主要定義IT安全評估的一般性概念與原則，並提供評估的一般性模式。Part 1 也包括了如何描述IT安全目標、選擇和定義IT安全條件、撰寫高階產品或系統規格等項目的概念。

Part 2 為安全功能性條件，其建立了一套安全功能性元件，用以一致化描述評估目標（Targets of Evaluation）安全功能性條件的方法。

Part 3 為安全等級條件，其建立了一組保證元件（assurance component）用以一致化描述評估目標的保證條件方法。

防火牆至少應該通過國際主要的認證機構Information Technology Security Evaluation Criteria (ITSEC) 之 E3 Level, Common Criteria 之EAL4+ Level, Trusted Computer System Evaluation

Criteria(TCSEC) 之 C2 or B1 Level

二、系統是否穩定

就一個成熟的產品來說，系統的穩定性是最基本的要求。防火牆的穩定性從廠家宣稱的材料中是看不出來的，但可從以下幾個管道得：

- 1、國際的認證機構的認證 如 ICSA, ITSEC, CC, TCSEC, OPSEC等。
- 2、與其它產品相比，是否獲得更多國際認證。
- 3、實際調查。這是最有效的辦法，考察這種防火牆是否有單位使用，其用戶量也很重要，特別是用戶對於防火牆的評價。如有可能，最好咨詢一下那些對穩定性要求較高的用戶，如政府機構，金融同業等。
- 4、自己試用，先在自己的網路上進行一段時間的試用（一個月左右），如果在試用期間經常有當機現象，這種產品就可以完全不用考慮了。
- 5、廠商研發的歷史，這也是一個重要指標，一般來說，如果沒有兩年以上的研發經歷恐怕難保產品的穩定性。
- 6、廠商的實力，這點也應該考慮，如資金、技術研發人員、市廠銷售人員和技術服務人員等等。

三、是否高效

高性能是防火牆的一個重要指標，它直接展現了防火牆的可用性，也代表用戶使用防火牆所需付出的代價。吞吐量測試數據丟包率測試數據級延遲測試數據是衡量防火牆性能的指標，吞吐量指標根據 RFC (Internet Requests for Comments) 的定義：網路設備在不丟失任何一個封包(Cell)情況下的最大轉發速率，即吞吐量 = 端口速率 × 2 (全雙工)，乙太網路吞吐量最大理論值稱線速，即指網路設備有足夠的能力以全速處理最小的數據封包轉發。一般來說，防火牆有上百條規則，其性能下降不應超過5% (指封包過濾防火牆)。支援多少個連接也可以計算出一個指標。

四、是否可靠

可靠性對防火牆類訪問控制設備來說尤為重要，其直接影響受控網路的可用性。從系統設計上，提高可靠性的措施一般是提高本身零件的強健性和可用度，這要求有較高的生產標準和可用度，如使用工業標準、雙電源供應、系統熱備援不管是HA (High Availability) or LB(load balance) 等。

五、功能是否靈活

對通信行為的有效控制，要求防火牆設備有一系列不同等級別，滿足不同用戶的各類安全控制需求的控制策略。控制策略的有效性、多樣性、等級別目標的清晰性、制定的難易性和經濟性等，影響著控制策略的高效和質量。例如對普通用戶，只要對IP地址進行過濾即可。如果是內部有不同安全等級的子網，有時則必需允許高等級別子網對低等級別子網進行單向訪問。如果還有移動用戶，如出差人員，還要求能根據用戶身份進行過濾。

六、配置是否方便

在網路入口和出口處安裝新的網路設備是每個網管人員的噩夢，因為這意味著幾乎全部現有設備的配置均必需修改，還得面對由於運行不穩定而招至的責難。其實有時並不是設備有問題，而是網路經過長時運行後，內部情況極端複雜，做任何變動都需要一段整合期。防火牆有沒有比較簡潔的安裝方法呢？有！那就是支持透明通信的防火牆，它依舊接在網路的入口和出口處，但是在安裝時不需要對原網路配置做任何變動，所做的工

作只相當於接一個Hub。需要時，兩端一連線就可以工作；不需要時，將網路恢復原狀即可。

七、管理是否方便

網路技術發展很快，各種安全事件不斷出現，這就要求安全管理人員經常調整網路安全。對於防火牆設備本身的安全控制外，應用系統的安全控制也很頻繁，這些都要求防火牆的管理在充分考率安全需要的前提下，必需提供方便靈活的管理方式和方法，這主要應考慮的因素為管理途徑、管理工具和管理權限。

首先管理方式要適合管理人員操作習慣，如遠程Telnet登錄管理及管理命令的線上支援等。管理工具應具備GUI介面。權限管理是管理本身的基礎，但是嚴格的權限認證可能會帶來管理方便性的降低。但應具備基本的權限控管，如限制管理者的IP，另外是否有提供SSH或WEB VPN的連結方式。

各種的管理稽查報表的提供也是很重要，報表的判讀容易性，對管理者在追查問題時更是重要。

八、是否可以抵抗拒絕服務攻擊(DoS)

在當前的網路攻擊中，拒絕服務攻擊(DoS)是使用率最高的方法，

Yahoo等網站遭受的就是拒絕服務攻擊(DoS)。拒絕服務攻擊(DoS)可以分為兩類：一類是由於操作系統或應用軟體本身設計或編程上的缺陷而造成的，只有上修補程式的方法來解決；另一類是由於TCP/IP協定本身的缺陷造成的，只有少數的幾種，但危害性非常大，如SynFlooding等。

要求防火牆解決第一類攻擊是強人所難。系統缺陷和病毒不同，沒有病毒碼可以作為依據，因此在判斷到底是不是攻擊時，常常出現誤報的現象。防火牆能做的是對第二類攻擊，當然要澈底解決這類攻擊也是很難的。抵抗拒絕服務攻擊(DoS)是防火牆的基本功能之一，目前有很多防火牆號稱可以抵禦拒絕服務攻擊(DoS)，實際上嚴格地說，它應該是可以降低拒絕服務攻擊(DoS)的危害而不是抵禦這種攻擊。

九、是否可以針對用戶身份進行過濾

防火牆過濾時，最基本的是針對IP地址進行過濾。但IP地址是非常容易修改的，只要打聽到內部網路誰可以穿過防火牆，那麼將自己的IP地址改成和他的一樣就可以了。因此防火牆需要一個針對用戶身份而不是IP地址進行過濾的辦法。目前防火牆上常用的是拋棄式密碼機制，通過特殊的

算法，保證用戶在登錄防火牆時，密碼不會在網路上洩露。

十、是否具有可擴展、可升級性

網路不是一成不變的，現在可能主要是在公司內部網路和外部網路之間做過濾，隨著業務的發展，公司內部可能具有不同安全等級的子網，這就需要在這些子網之間做過濾。目前市面上的防火牆一般僅配三個網路接口，分別接外部網路、內部網路和SSN。因此，在購買防火牆時必需確定，是否可以增加網路接口。

和防毒軟體及IDS一樣，隨著網路技術發展和黑客攻擊手段的變化，防火牆也必需不斷地進行升級，此時軟體升級就很重要了。如果不支援升級的話，為了抵禦新的攻擊手段，用戶就必需進行硬體更新，而在更新期間網路是不設防的。

結論

防火牆是資訊安全管理系統(ISMS: Information Security Management System)的一環，但不是全部，有了它不代表資訊安全就百分之百的沒有問題，請記住，防火牆其本身只是一個“篩選器”而已，雖然我

們都有一個期望，就是防火牆能一肩扛起所有的資訊安全工作，目前有許多廠商宣稱其防火牆雖不是俱備十八般武藝，但基本的資訊安全機制，如入侵偵測(IDS)，防毒，內容過濾等均一應俱全，但就現有技術及其發展趨勢分析，目前這類產品在靈活性，安全性，管理方便性及總擁有成本上均未臻至完善。

其實如果就資訊安全涉及的層面看，即使防火牆具備上述的功能，也僅是在企業網路邊際上或各子網路間的資訊安全而已，如就國際組織的規範，如ISO17799，BSI7799(part1)或國內的CMS17799及CMS 17800，防火牆所能涵蓋的層面，僅是其中的一小部份。

根據ISO17799 & BSI7799(part1)的文件，資訊安全是企業全體員工的責任，其推行落實的方式，在企業組織中是由上而下的，與大家一般的認知“資訊安全是某些人或某些設備的工作及由下而上的方式”差異很大。

不管如何，防火牆是企業資訊安全基礎建設中不可或缺的要角之一，如何選擇一個合適的防火牆，及如何充分運用它的特點，以達到高效率與安全?實有賴企業所有員工一起完成的。