題組五　參考答案

有人說：「沒有防火牆就沒有 Intranet。」這句話絕對不會言過其實，當一個企業要開放 Internet 給企業的員工，並且在企業內部建置 Intranet 以後，如果沒有一個防火牆系統放在 Internet 和 Intranet 之間的話，企業的內部網路和電腦系統，就等於是直接開放給全世界。

在世界各地的電腦駭客，不論何時都可以進入到企業內部的電腦之中，為所欲為，那還得了？倒底防火牆是用什麼神秘的方法來將在企業外面 Internet 上的駭客阻擋在牆外？它又如何能應付各種不同的入侵技倆呢？

雖然不同的防火牆採用不同的技術去實現保全的工作，但綜歸起來它無非是一些電腦軟體和硬體的組合，只可以讓一些特定的資料從防火牆的一端到另一端。它通常是企業內部網路和外界 Internet 之間的唯一通道，例如將它放置在企業網路和 Internet 服務提供者（ISP）的路由器之間，讓企業所有到外界的資料，或是從外面 Internet 進入企業網路的資料，都經過防火牆的確認手續，才能放行。防火牆所作的確認手續，是由一些事先設定的安全規則和政策來完成的，最普遍採用的兩種確認交通的方式是資料封包過濾和應用程式層的過濾方式，其他還有一些新式的過濾方法，諸如電路層過濾式防火牆和代理式防火牆等。

一、資料封包過濾防火牆：資料封包過濾式（Packet Filter）的防火牆將過往的資料封包（packet）仔細地檢查確認，以阻擋不該進出防火牆的交通。最簡單的一種資料封包過濾型式就是路由器（router）。在路由器之中的路徑轉換表就可以設定誰可以通過，而誰不准通過。當這種管道建立起來之後，其他程式應用如果是採用相同的埠口，防火牆會以為它是 FTP 檔案傳輸的資料，照樣放行，因而造成了一個安全上的漏洞。在電腦網路上的一些駭客，甚至開發了一些繞過資料封包過濾的技倆，最有名的是利用「扮豬吃老虎」的方式，用一個假的 IP 位址就可以將防火牆騙得團團轉。目前大部分資料封包過濾式防火牆都在這方式下了一番功夫，不讓歹徒可以輕易地闖入，但是電腦網路專家們也都認為，只用封包過濾式防火牆這單一的方法是無法保衛企業網路的安全的。

二、應用程式層過濾式的防火牆：應用程式層過濾式（*Application Filter*）的防火牆是屬於代理閘通道的方式，它利用專門性的程式來做一些 *Internet* 上的程式應用的佣介者，使其成為閘通道（*Gateway*）而將企業的網路和外界的 *Internet* 隔開。它檢查 *OSI* 模式的最高層的資料，驗可後才將內外網路連接起來。由於這種型式的防火牆作用在 *OSI* 模式的最高一層，因此它可以瞭解所有過往資料的通訊協定，並且可以加上各種特定的安

全功能，應該是一種比較安全的防火牆型式，不過它也有一些缺憾：對於使用者而言，它不是完全透通的，有些程式應用很可能會莫名其妙地被阻擋在門外；當有新的程式應用或是 TCP/IP 的服務要增加時，必須要重新開發新的過濾器；使用者在網路上所能使用的程式應用數目，以及服務項目，受到代理器的數量限制，不能任意加添。以一個檔案傳輸（FTP）的相同實例來看，在應用程式層的過濾方式可以用應用程式閘通道（Application Gateway）來實現。比較先進的防火牆在這一方面都做了一些補強措施，只讓真正在檔案傳輸狀態的資料封包能通過防火牆。

三、電路層過濾式防火牆：電路層過濾式（Circuit-level Filter）的防火牆是介乎上述資料封包過濾式和應用程式層過濾式之間的防火牆型式，它把應用程式閘通道變成一個更廣泛的型態，它也是依據一些規則來設定出入的管制，但是它作用於比較低的層次，因此不必專門為每一個應用程式來特別設定組態。

此外，最近有一種新型的過濾技術檢查動態的資料封包狀態（state），這種名為狀態檢驗（statefull inspection）的技術在查驗高層通訊協定的同時，順便將過往交通的狀態記錄下來。由於有了狀態的記錄，防火牆系統可以分辨出哪些是從企業外發出的通訊服務要求，而哪些是回應企業內發出通訊服務的返回資料。

（1）影像與圖形技術應用研究發展計畫預期研發成果

成果名稱	智慧型網格圖形向量化工具(v2.0)	GIS 網路分析模式工具
聯絡人	石長江	謝祯冏
電話	02-3776100 轉 743	02-3776100 轉 742

（2）功能提昇技術研發前置作業及航電系統維修計畫預期研發成果

成果名稱	自動測試平台系統晚體雛形	ACARS 操作輔助訓練系統
聯絡人	朱海燕	朱海燕
電話	02-7389799 轉 713	02-7389799 轉 713