數位世界的防火牆

二十一世紀是數位化的世紀，數位化科技提供了
迅速又便捷的服務，但也面臨了駭客高技術的攻擊。
網路的安全性與隱密性，就成為當前推行數位化的首要任務之一，
在這一方面，網路防火牆扮演了重要的角色。
但有了防火牆就可高枕無憂了嗎？

孫宏民　謝濱璨

網際網路讓我們得以優游於資訊的大海中

近年來，我們的生活與網路有越來越不可分的關係。早期，電腦對於多數人而言，只是用來處理簡單的文書及帳務的工具；此外，電腦的另一個用途就是做爲提供電子遊戲的設備。其實早在十二年前左右，一般家中的電腦便有了「連線」的渴望。爲什麼要說是「連線」而不是網路呢？因爲在以前沒有所謂網際網路的時候，家中電腦只能靠跨接每秒傳送1,200位元（bit，電腦資料的最小單位）或每秒傳送2,400位元的數據機，以電話撥接的方式連接私人建立的電子布告欄站，這是屬於點對點的連線。私人的電子布告欄上有各式各樣的討論區及簡單的遊戲，並具備線上交友對談的功能。

以現在的眼光來看，雖然每秒傳送2,400位元的速度實在慢得可憐，但是大家依然樂在其中。雖然慢，卻代表個人電腦不再孤獨，已經可以走出戶外了。

往後的幾年間，台灣的業界與學術界有了網際網路。由於頻寬（網路上單位時間內的資料傳送量）的不足，當時主要以文字資料的共享爲主。從此人們開始體會到世界村的便捷，在短短的幾分鐘

內可以用網路走遍各國，要找的資料在短短幾分鐘的時間就能自國外以電子郵件寄回來。和傳統出國找資料或利用跨國傳眞的成本相比，實在經濟得多。

如今，每個人幾乎可以隨時隨地上網，而且是以寬頻上網，甚至利用行動電話直接無線上網。網路基礎建設的完備，讓我們能在網路上完成更多的工作，網路提供了更多的便利性、節省了更多的時間。利用網路我們可以進行電子式的消費、娛樂、金融服務，更重要的是資訊的快速傳遞，包括新聞、電子郵件等。試想，若將網路自人們的生活中移除，那會是怎樣的情況？這就好像將交通工具自人們的生活中移除，大家只能用雙腳走路，雖然不會癱瘓我們的生活，卻會造成相當大的不便。顯然在我們的生活中，網路已經扮演不可或缺的角色。

隨硬體設備的推陳出新，及網路頻寬的不斷加大，任何一個提供資訊或服務的單位，可以透過網路自由、彈性地設定及控管其資訊的散播，同時與其他相關服務的單位進行合作。網路串起了全球的資訊，使得任何資訊都可以四通八達，方便至極。然而，在方便中也會因爲過於便利，而產生一些負面的作用，就好比有了方便的汽、機車代步，但汽、機車數量與日俱增的結果，卻造成令人無法忍受的交通阻塞。

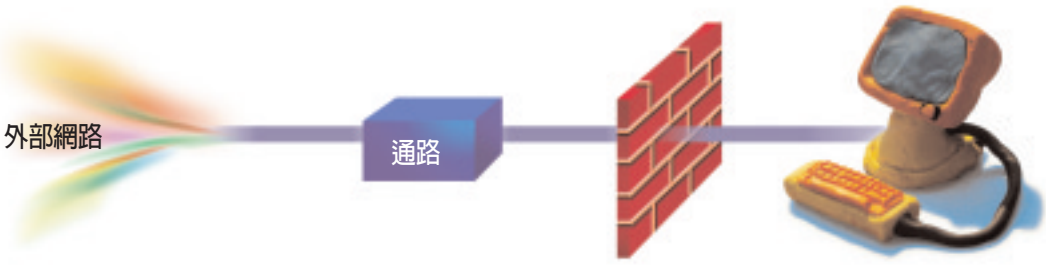
便捷的網際網路，也提供了不良分子作奸犯科的場所

同樣地，網路的方便性對於一些負面的事情亦有助長的作用，最常見的包括大量的廣告信、眞假難辨但卻造成人心惶惶的網路謠言、以及利用網路進行盜版軟體及色情光碟的銷售。這些負面的功能，我們都可以透過自我約束，不去相信或不去消費它。然而我們在網路上所受到的威脅、打擾，並非如此而已！更令人擔心的是，網路駭客入侵公司行號及金融體系等擾亂金融秩序、侵犯個人隱私的可怕行爲。

對於網路上非善意的使用者，須有一套防護措施

網路上的伺服器因爲提供了各式各樣的服務，包括電子郵件、網頁瀏覽、檔案傳輸等，可以說是門戶洞開。爲什麼這麼說呢？我們可以將一台提供多項服務的伺服器，想像成一個販賣多種商品的福利社，而每一種商品都有一個固定的結帳處，那麼若有四種商品，就會有四個結帳處。由於福利社是開放空間，所以有些人並不是眞的要進來買東西，可能只是進來逛逛，也可能是進來勘察地形而另有所圖。

爲了讓顧客在最快的時間內購得商品，我



防火牆的位置是設置在
所欲保護網路的最外層，依過濾方式
決定哪些資料是允許進入其內部網路的。

們希望只有眞正要買東西的顧客才進來，如此便可以降低福利社裡的人數，以便提供快速的服務。同樣地，爲了讓伺服器能夠完全地用在服務需求上，我們也會希望伺服器只開放其提供服務的窗口，關閉所有不必要的窗口，以避免伺服器資源的浪費。既然網路上提供服務的伺服器是開放式的，它又盡可能地提供服務給需要的使用者，因此也提供了多種管道及方法可讓駭客入侵。爲了阻斷駭客的入侵，關閉伺服器不必要的窗口，在網路上採行的機制叫防火牆。在談防火牆之前，先了解一下大廈的警衛制度。

與大樓警衛功能類似的網路防火牆

現在的住宅多半有著社區的觀念，爲了提供住家一個安全及安寧的生活環境，減少不必要的推銷及廣告上門，社區通常都會有保全警衛，辦公大樓也有大樓管理員駐守大樓門口。進出社區的住戶或進出辦公大樓的員工，通常要有識別證或門禁卡才能夠自由進出。對於外來的訪客則需要由警衛按鈴通報，由社區住戶或是大樓員工出來接待，才得以進入社區或辦公大樓。警衛除了守門、控管進出的人員外，還負責控管寄來的包裹郵件。這些郵件通常會由警衛代收，再於某一固定時間將當日的郵件分送投入各住戶的信箱，或請住戶至警衛室簽收包裹。

網路世界中的防火牆制度其實和社區的警衛制度是類似的，防火牆設置在所欲保護網路的咽喉點，也就是整個被保護網路與外界通訊時，資料傳送的必經之處。就如同社區的警衛是設置在整個社區的大門口，即所有人、物進出的必經之地，以達到控管的目的。

功能各異的三種網路防火牆

防火牆的主要目的在阻絕不必要的資料進出，並且監督、記錄必要的資料進出情況，以供日後稽核及查閱用。防火牆過濾往來資料的技術，可分爲下述三種方式：

封包過濾　封包是網路資料傳輸的一種單位，我們平常使用電子郵件、檔案傳輸、網頁瀏覽等過程，都是將資訊化成封包後在網路上傳送。每個封包進出伺服器有其窗口、格式、來源位址、目的位址等。防火牆便是依據這些資訊，透過訂定的過濾規則來決定哪些封包可以進入，哪些封包不允許進入。

應用程式代理　應用程式代理的方式，是在防火牆上採用一種代理的軟體，如檔案傳送代理（FTP）、遠端連線代理（TELNET）、電子郵件代理（MAIL）、全球資訊瀏覽代理

防火牆採封包過濾的方式，
決定哪些封包可以進入內部網路，
哪些無法進入內部網路。

（WWW）等。這些軟體的功能，使得防火牆對外（區域網路外的機器）扮演內部機器的角色，待處理完網路外機器傳入的資料後，防火牆再轉而對內扮演外部機器的角色，將資料傳給內部機器。應用程式代理的方式會較封包過濾的方式來得安全，因爲採用封包過濾時，只要符合過濾規則的封包都可以自由進出，駭客就會有機可乘，侵入所欲保護的網路內，攫取資訊，癱瘓網路運作。此外，應用程式代理的過濾方式所產生的記錄檔，較容易了解及稽核。

連線方式過濾　此種方式在運作時並非讓欲連線的雙方直接連線，而是由防火牆扮演居中的角色，同時向欲連線的雙方建立起連線，此時防火牆的工作便是將一端的連線資訊轉傳給另一端，只做轉傳的動作及記錄。一般而言，此種方式是管理者對網路內部的某一電腦有充分的信賴時，才使用的過濾方式。

如同先前所說的，防火牆的主要工作是在進行過濾的動作，允許管理者同意的資料進出所欲保護的網路，以降低不必要的資源浪費。另外便是記錄的工作，以便日後的稽核。當然，對於違反規則的資料欲進出其網路時，防火牆必須適時地提出警訊，以供網路管理者進行必要的措施。由於經過防火牆的資料量相當龐大，防火牆除了可以利用軟體的方式來實現外，現今亦有許多硬體防火牆，透過硬體的實現來提高處理的速度及效能。

防止駭客入侵的第二道防線——入侵偵測系統

談到防火牆，免不了要提到入侵偵測系統。防火牆看起來很完備，可以阻擋不必要的資料進出網路，爲什麼還需要有入侵偵測系統呢？因爲許多網路伺服器上提供服務的應用程式，有著一些當初沒有預期到的系統漏洞，透過網路應用程式的協定（通訊的規格），駭客們可以一試再試，千方百計地利用這些漏洞及既定的應用程式協定來達到入侵網路系統的目的，哪怕是該網路已經架設了防火牆。這就好比法律是死板的、固定的，鑽法律漏洞者的頭腦是靈活的，一試再試，總是有些破綻可以讓駭客成功地找出來。

入侵偵測系統主要在彌補防火牆的不足，它針對防火牆允許進入的資料進行檢查。傳統且常見的入侵偵測系統是建立在入侵樣本上，它將入侵方法的樣本建立成資料庫。所謂的樣本，即是入侵手法的一些特徵指令及字串，將現有已知的入侵方法建立資料庫後，再針對每一個已通過防火牆進來的連線及封包進行比對，以檢測是否有入侵的行爲。

當入侵偵測系統偵測到網路上有入侵行爲時，隨即與防火牆進行溝通合作，請防火牆關閉某些窗口或是修改其過濾規則，以阻斷入侵者的連線，或者由入侵偵測系統自行採取反制

防火牆採應用程式代理的過濾方式，是在防火牆上採用一允許被執行的代理程式，使防火牆對外扮演內部機器的角色，傳入的資料經防火牆處理後，防火牆再轉而扮演將資料傳入內部機器的角色。

措施。至於入侵偵測系統是否能夠和防火牆聯手打擊犯罪，端視防火牆是否預留與其他產品結合的空間，有些防火牆產品能夠支援並與其他入侵偵測系統結合，有些則否。

具有人工智慧的入侵偵測系統

傳統的入侵偵測系統，採用方式是將入侵方法的特徵建立資料庫，以逐筆比對方式來判斷是否有入侵行爲發生。然而這種方法有兩個主要缺點，一爲耗時，對於每個連線均須逐筆比對，耗費大量的尋找時間；另一個缺點是須定時更新入侵行爲的特徵資料庫，因入侵偵測系統的判斷準確率，全靠特徵資料庫的齊全與否，定時更新資料庫是必備的工作，否則其準確率將大打折扣。

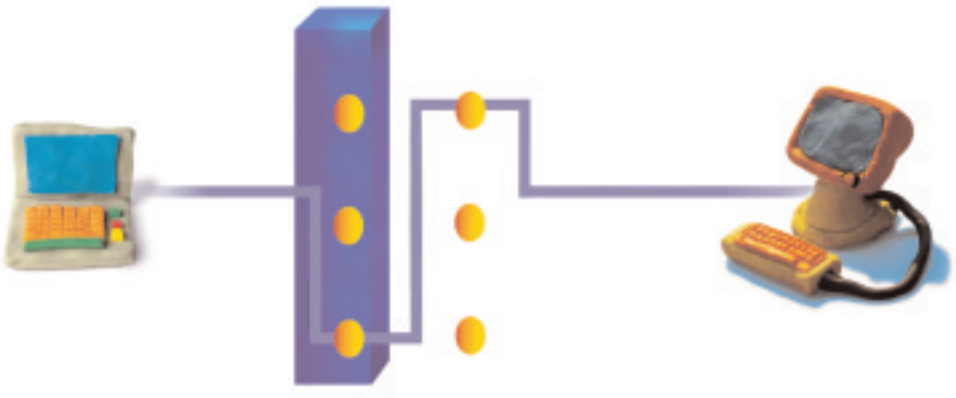
有鑑於此，新一代入侵偵測系統講求的是系統的判斷智慧，希望能夠解決上述耗時及入侵特徵資料庫須經常更新的問題。舉例來說，有些入侵偵測系統便嘗試以類神經網路的技術，提供系統學習的能力，以提高判斷的準確率，改善傳統資料庫搜尋耗時的缺點。類神經網路技術主要是以程式的方式，來模擬人類學習過程，若人類學會了一種方法來解決問題，當遇到新的、不曾出現過的問題時，他都能以該方法找出答案。就好比一個人學會了乘法，當他遇到任何乘法問題時，都能隨即計算出正確答案，不會因爲不曾算過，或不曾在九九乘法表（資料庫）內出現過，而算不出答案。

共同建構一個便捷、安全、隱密的網際網路

數位時代的來臨的確爲人們帶來了許多的便利及彈性，在我們日漸依賴網路完成許多重要工作的同時，駭客任意地入侵伺服器及惡意地耗費伺服器資源，成爲網路應用上最大的殺手。我們在網路上進行股票買賣、銀行轉帳、網路報稅、商品消費等，這些都關係著每個人的金錢、信用。破壞總是比建樹容易，只要駭客成功地破壞或入侵一、兩次，努力建構的便民措施、制度就無法獲得使用者的信任，造成使用的意願下降。

有效防止駭客的破壞與入侵，爲現今網路安全的重要課題，網路駭客的犯罪手法，可以說都屬於網路世界中的智慧型罪犯，我們期望防火牆技術及入侵偵測系統技術，能夠在學術界及業界的攜手合作下，有更高的阻絕效果及正確的偵測率。正如同在現實生活中有許多的經濟罪犯及智慧型罪犯，我們都希望人民的保母能夠提高破案率是一樣的。也唯有不斷地努力尋求技術上的突破，提高防火牆及入侵偵測系統的效能及準確率，才能有效壓制駭客囂張的行爲，爲數位時代提供舒適與安全的使用環境。 □

孫宏民 清華大學資訊工程學系
謝濱璨 成功大學資訊工程學系



防火牆採連線過濾方式，是指管理者只允許可資信賴的內部網路機器與網路外部機器建立連線。