網安產品技術與市場分析

林盈達 林柏青

綜觀過去網路產業的發展，我們依照解決問題的類型可以大致歸納為三個階段：解決連結性(connectivity)的問題、解決安全性(security)的問題、提供內容(content)服務的問題。連結性的問題已大致獲得解決，而安全性問題的重要性則與日俱增。面對安全性問題，市場上主要有防火牆(firewall)及內容過濾器(content filter)來控制網路的存取，虛擬私有網路(VPN)來保護在公眾網路傳輸資料的內容，以及入侵偵測系統(IDS)和防毒系統(antivirus)來保護企業內部系統的安全。其中除了防火牆的技術需要處理封包的標頭(header)外，其餘四類的產品都需要深入的去處理或分析封包的內容。因此如何一方面在網路安全產品提供更豐富的功能，一方面又能維持其效能，就成為一個重要的課題。就市場上來看，我們已經可以看到市面上的防火牆大都已經整合了 VPN 及有限的內容過濾功能，而且更有整合各項功能的多合一的產品上市。國內新創的公司相對於原有專注在 firewall 和 VPN 的功能上的國內大廠，更是把矛頭直指第四層以上需要處理封包內容的安全產品，如入侵偵測系統、防毒系統及內容過濾器。

1 技術發展

回顧過去網際網路的歷史，從早期 ARPANET 的建立到後來整個 Internet 的普及以及各種區域網路標準的競爭，我們可以看到一個重要的議題就是解決連結性(connectivity)的問題。然而，這個議題如今已經大致獲得解決。根據資策會的統計，在去年台灣區的上網人口就已超過 800 萬人，今年更可望突破 900 萬人。幾乎每個政府機關、學校、企業都有自己的網站，網際網路已經融入每個人的生活。現階段乙太網路(Ethernet)幾乎成爲有線區域網路的唯一技術，現在更以 Gigabit 甚至 10 Gigabit 的速度要往都會區網路推進。另一方面，隨著無線區域網路產品價格的下降，無線上網的技術更廣爲被接受。現在有愈來愈多的公共場所提供無線上網的服務。IEEE 802.11g (最高速率 54 Mb/s)標準的通過以及 IEEE 802.11n(最高速率 108 Mb/s)標準小組的即將成立，意味著無線區域網路會繼續往更高速的方向發展，甚至在若干程度上將取代 Ethernet 的應用。在都會網路及廣域網路方面，Ethernet 和 DWDM(Dense Wavelength Division Multiplexing)的技術，將逐步取代現有的 ATM 和 SONET，提供更便宜而且更大的頻寬。在接取端方面，xDSL 的技術逐漸普及到每戶人家之中，小型 SOHO router 的普及率更可望逐步上升。

在連結性的問題逐步獲得解決之際，安全性的問題卻浮上檯面。根據 CERT® Coordination Center 的統計，過去三年內，網路安全事件每年增加約三萬件。單是今年上半年就有 76,404 件網路安全事件的回報，直逼去年全年的 82,094

件。近來的 blaster worm 事件更已躍上報紙頭條，安全議題遂成爲大家不得不去面對的問題。安全事件的不斷發生，不僅造成企業龐大的損失，更危及消費者使用網際網路服務的信心。例如在網路上使用信用卡消費時，就會懷疑是否私人資料有曝光的可能，使得未來提供內容服務的產業更難推展。因此安全性的問題已經成爲這個階段必須解決的問題。

目前在市場上主流的產品可以分爲連結性與安全性的產品。連結性的產品包含 Ethernet 卡和交換器、無線區域網路卡和 access point、各種 router 以及 xDSL 的相關產品。在安全性產品方面，主要可以分成三個方向：

(1) 存取的安全：存取安全的目的是在控制誰可以存取什麼。典型的例子爲防火牆(firewall)產品，可以控制外界任意進入企業內部的網路，以及企業內部員工可以使用哪些類網路資源。然而單是防火牆尚不足以提供足夠的存取控制。例如一般公司還是需要讓員工可以使用 email 或是瀏覽網站。防火牆只能決定要或不要使用哪些應用，卻沒辦法依據這些個別應用的*實際內容*來決定是否可存取。內容過濾器可以彌補這方面的不足。它可以限制員工瀏覽某些類的網站，或防止重要訊息從公司內流出。

(2) 資訊安全：一個較大型的企業可能有很多分公司散落在各地，或是企業的個人可能需要透過網際網路連線回公司存取資料。但是資料在公眾的網際網路中很容易被竊取、假冒、或是竄改。私有區域網路(Virtual Private Network, 簡稱 VPN)的技術，就是在解決這樣的問題。透過加密(encryption)、認證(authentication)等方式，來達成這個目標。

(3) 系統安全：即使做到了上述的工作，企業內部的網路還是有遭受入侵的可能。例如公司的網站還是應該讓外界存取，而不能用防火牆阻擋。電腦病毒還是可以透過電子郵件等方式傳入企業內部，蠕蟲(worm)更可以利用某些服務的弱點(vulnerability)侵入系統並恣意擴散。因此，入侵偵測系統(Intrusion Detection System，簡稱 IDS)以及防毒(antivirus)系統便成爲重要的網路安全產品。

2 功能介紹

在簡述前項安全產品的種類之後，我們現在分別就目的、功能、以及結果三方面來看這些產品：

(1) 防火牆(firewall)：防火牆的目的主要是控制企業內部網路與外部網路的存取。一個簡單的例子就是不讓外界可以存取到公司內部的電腦，或是可以限制員工在上班時間上 BBS 站等。防火牆的位置介於公司內部與外部的網路間，所有從外到內或從內到外的網路封包都必須經過防火牆。系統安全管理人員事先依據公司的政策及實際環境的需要設定防火牆的存取規則，防火牆便會忠實的執行這些規則來控制公司內外網路封包的進出。

例如公司有架設網站提供外界獲得公司的資訊，但是內部網路的電腦同

時有重要的資料不能給外界經由網路獲得。此時防火牆可以把網路分成三個區域：一爲外部(external)網路，指的是公司以外其他的網路；一爲內部(internal)網路，指的是公司內部一般不可讓外界存取的網路；另一個一般稱爲非軍事區(Demilitarized Zone，簡稱 DMZ)，介於外部網路和被保護的內部網路間，可以提供公司對外的網路服務而同時保護內部網路不被存取。有些防火牆甚至可以再定義額外的安全區域，提供網路管理人員更彈性的設定方式。

存取規則設定好後，一但網路的封包經過防火牆，不管是從內到外或是從外到內，防火牆都會檢視封包內的訊息來決定如何處理該封包。例如規則設定由外到內所有目的 port 爲 23 的封包都應該丟棄，那麼防火牆遇到這樣的封包就會丟棄。一般來說，處理的方式有通過、丟棄兩種，而且可以選擇要記錄或不要記錄這樣的封包。一般防火牆檢視的內容都是第四層以下的內容，位於封包的標頭且格式較固定，所以檢視的工作尚不會太複雜，較高檔的產品可以達到 wire speed 的效能。

由於硬體規格的進步，現在的防火牆已經整合愈來愈多的功能。除了網路位址轉換(Network Address Translation, 簡稱 NAT)及 DHCP 等功能外，幾乎所有的防火牆都已經有支援 VPN 以及若干內容過濾的功能。

(2) 虛擬私有網路(VPN)：

VPN 的目的主要是提供公司與公司間，以及個人與公司間，經由公眾網路傳輸時所需要的安全。因爲並非建立起真正的私有網路，而是經由公眾網路來提供如私有網路般的安全性，故稱爲虛擬私有網路。

資料在公眾網路傳輸可有會有下列的安全性問題：

- 資料會被不當的窺視，也就是第三者可能藉由監看封包的內容，來發現傳輸的內容。解決的辦法就是提供加密的機制，把傳輸的內容轉換成密碼，即使封包被監看了，第三者也無法解讀其內容。
- 資料會被竄改，也就是第三者可以偷改資料後再重新送出。解決的方法爲簽章(signature)機制。簡單的說，就是把原資料經由特殊的運算得到一段檢查碼，而接收到資料的人也將內容做同樣的運算就可以得到同樣的檢查碼。萬一資料遭到竄改，那麼就無法經由運算以得到相同的檢查碼。這時候接收人就知道資料遭到修改。
- 資料來源可以假冒。這時就要經由一些認證的機制，例如利用雙方的 secret key 計算前述的檢查碼。因此當接收人收到資料時，一方面可以驗證資料不被修改，一方面也可以得知來源端的真實性。因爲若非真實的來源端，就沒有那樣的 secret key 來得到現在的檢查碼。

虛擬私有網路會在傳輸的雙方建立起一個虛擬的傳輸通道，並應用上述的機制以確保資料的安全。

(3) 內容過濾器(content filter):

爲了防止員工或學生在上班上課的時間不當使用網路，例如員工在上班

時間連上股票網站以至於影響正常的工作，未成年的學生會瀏覽色情網站等。內容過濾器建有一個龐大的資料庫，可以針對網頁的要求進行比對。比方說，如果發現某個要求是屬於資料庫中某個色情類的網址，內容過濾器就會把這樣的要求擋下，而不讓它送出，自然內部的員工或學生就無法瀏覽這個網頁。有的內容過濾器可以讓管理人員輸入關鍵字，也就是說只要網頁的要求或內容有出現預設的關鍵字，就會予以擋下。有的內容過濾器還可以過濾掉網頁內容中的 JavaScript, ActiveX 等物件，避免那些網頁可以在內部網路的電腦執行不當的程式。除了阻擋瀏覽網頁的功能外，有的內容過濾器也可以記錄使用者瀏覽的記錄，或是動態監看使用者瀏覽網頁的情況。

(4) 入侵偵測系統(IDS)：

即便有了防火牆等措施，除非企業網路可以做到完全的與外界隔絕，否則仍然有被不當入侵的可能。特別是企業的網站、郵件伺服器等，入侵者可以利用這些架站程式的弱點(vulnerability)進行入侵，例如取得系統管理員的權限等。

然而這些典型的弱點以及入侵攻擊的方式通常有脈絡可循，在攻擊封包當中通常會含有某些特徵(signature)。因此入侵偵測系統可以藉由監看網路上流過的封包，一邊比對內容中是否含有攻擊的特徵，就可以發現是否有攻擊發生。一但發現有攻擊發生，入侵偵測系統可以記錄攻擊的事件，或是切斷連線避免攻擊繼續進行。

入侵偵測系統可以分爲 passive 和 in-line 兩種模式。Passive 模式採用被動的監看，較不會形成效能上的瓶頸，而且發生攻擊誤判時通常只是記錄入侵事件，而不會阻擋封包。In-line 模式介於封包流過的路徑上，可以即時阻擋攻擊。可是一但發生誤判時就跟著會誤擋封包，而且較容易形成效能上的瓶頸。

有些攻擊爲了不讓入侵偵測系統的檢查到，會採取迴避(evasion)的措施。例如將封包切割成許多個更小的封包(fragmentation)或是修改 URL 的內容躲避某些特徵。這時入侵偵測系統仍然需要針對這些迴避措施加以處理，而能照樣的偵測到入侵。

(5) 掃毒系統(antivirus)：

電腦病毒的散播一直是使用電腦的人長久以來面臨的問題。從早期透過磁片的散布，到現在透過電子郵件甚至以蠕蟲(worm)的形式直接在網路上尋找弱點主機散佈，都對電腦系統造成莫大的傷害。

如同入侵偵測系統，病毒也有其特徵。掃毒系統可以檢查檔案是否內是否有相關的特徵，來決定是否有夾帶病毒。然而實際的處理可能頗爲複雜。檔案可能經過事先壓縮過，在成爲郵件附檔時又經過編碼，如 BASE64 的編碼。因此在掃毒前就需要先行解碼、解壓縮才能開始掃毒。這些動作不是單單只看一兩個封包的訊息就可以做的到。

正如同入侵的迴避措施一樣，病毒本身也有許多種迴避檢查的方法。例如可以把病毒碼加密，待程式執行時再自動解密，而且解密的程式碼在每次複製時都有若干改變，使得偵測病毒的工作變得頗爲困難。甚至得使用 emulator 來模擬被偵測的執行檔執行的過程才能發現病毒。一但發現有病毒存在，防毒系統可以將檔案改名、刪除、或是直接清除檔案中之病毒碼。

3 技術分析

3.1 封包處理

一般防火牆的規則通常包括來源端和目的端的 IP 位址、來源端和目的端的 port 號碼、通訊協定(如 TCP、UDP、ICMP)等。這些值都位於封包標頭，位置以及長度都是固定的，所以在分析比對的時候較簡單，而且更容易以硬體來實現。

然而其他種類的安全性產品需要的技術就比防火牆複雜多了。以 VPN 爲例，資料在傳送之前都需要經過加密，接收後需要做解密的動作。所以它的效能就取決於加解密的運算速度是否夠快。所以較高階的產品都會使用專屬的加解密晶片來加速這些運算，以免形成網路的瓶頸。

IDS、內容過濾、防毒系統的問題就更複雜了。如果是一般內容過濾做 URL 配對其字串比對的動作還不至太複雜，因爲只要找到 URL 起始的位置，接著跟資料庫中的 URL 比對就行了，不用看到封包的深處。但是如果要過濾 JavaScript、ActiveX 的物件，除了找到這些物件外，還要去除其內容，所以牽涉到封包內容的修改及重組。IDS 和防毒系統爲了解決前述迴避的問題，需要對封包的內容做前置處理。以 IDS 來說，可能需要重組切割的封包，還原被修改的 URL 內容等，然後才進行特徵比對。特徵不見得位於封包的前頭，可能需要深入封包的底層才能發現特徵，總總問題都使得入侵偵測變得不易實行。防毒系統則需要把檔案解碼、解壓縮，遇到加密的病毒碼還要找出解密的方法，加以解密後才能比對病毒特徵。這些動作都不易實行，特別是做成硬體。雖然市場上已經有一些內容處理的晶片或處理器，但是在實際產品中仍不普及。

3.2 探討議題

這些安全性產品都有需要面對的問題。首先，防火牆並不能阻擋所有的封包，這不是技術上的問題，而是政策上的問題。公司的郵件伺服器、對外的網站等，仍然需要開放給外界能傳郵件或存取網頁。員工仍然需要上網查詢資料，收電子郵件等。防火牆能夠做的還是很有限。

我們可以使用內容過濾器來限制員工或學生上網瀏覽的內容。然而內容過濾器仍然會遭遇到漏擋或誤擋的問題。網際網路上的網站內容通常更新的

很快，如果沒有即時反應在 URL 資料庫上，那麼有些該擋的網頁就沒辦法擋到。一種方式就是經常去更新 URL 資料庫，但是這需要龐大的人力經常性的來維護。當然我們可以針對網頁內容去定義關鍵字甚至是分析網頁的內容來減少漏擋，但同時也可能因爲系統的誤判而擋到不該擋的網頁，是謂誤擋。

VPN 可以解決資料安全性的問題，但是由於相關協定和參數頗爲複雜，如果使用兩家不同廠牌的產品，或是設定上的疏忽，都可能造成兩端的 VPN 無法互通，因此在管理上的 overhead 頗大。另外就是前述效能的問題，通常需要用專屬的硬體加速晶片來加速加解密的動作。

IDS 面臨的困難有假警報(false alarm)的問題，例如內部網路沒有 FTP 站，但是如果沒有刪除相關 signature，一但外界有這樣的攻擊，即使不會對內部網路造成傷害，仍然會在 IDS 留下警報訊息。這類的訊息一多，不但增加管理人員無謂的負擔，更使得真正的攻擊容易魚目混珠而不引起注意。另一方面，一個攻擊可能會引發多個警報，要如何從多個警報中察覺是屬於同一個攻擊，而非多個不相干的警報，並不是一件容易的事。另外，IDS 也面臨特徵資料庫更新的問題，新攻擊的特徵若未來得及放入資料庫，就會面臨偵測不到的問題。此外，被動式的偵測也會漸漸往主動式的防禦發展，畢竟等到發現攻擊的記錄再去處理通常爲時已晚，能夠在發現攻擊時能及時阻斷才是真正的預防之道。

防毒系統也有同 IDS 一般遇到新病毒可能無法掃到的情形。另外，該在 desktop 端的電腦上掃毒或是在網路的閘道器上掃毒，則有互有利弊考量。前者需要每一台電腦都能即時的更新病毒，但實際上不容易做到。而後者可能會形成網路的瓶頸。而且在一些特殊的情形，例如進來的郵件本身就已加密，那麼就沒辦法做網路掃毒。

3.3 速度

綜合以上對技術的分析，防火牆對網路封包的處理是其中最簡單的，因此效能最高。其次爲 VPN，可以透過硬體加速的做法來提高效能。內容過濾器通常是在一個大型的 URL 資料庫中去配對網頁要求中的 URL，不需要在一大片文字中做搜尋，因此處理速度又次之。IDS 因爲需要做較多的前置處理以解決迴避的問題，所以花費的時間又較內容過濾爲長。防毒系統所做的前置處理可能會包含解碼、解壓縮、甚至解密，動作較 IDS 的前置處理複雜。病毒碼的 signature 個數也遠較 IDS 的爲多，也使得搜尋本身要花的時間更長。

3.4 signatures 數量

在前述的幾個種類當中，以內容過濾系統的 signature 個數最多，這裏的 signature 指的是 URL 的個數，通常有數百萬之多。防毒系統的 signature

個數居次，通常在 60,000 到 80,000 之間。IDS 第三，通常約一、兩千條之間。防火牆最少，通常在 100 條以內。

3.5 評比發現

我們在今年中舉辦網路安全產品的公開測試評比，內容包括前述的五大類產品。評比的結果有如下的發現：

- SOHO 等級的防火牆/VPN 產品變化較大，今年測試的幾款產品都是在去年測試時尚未出現的。相對於 SOHO 等級的變化，在 SME/Enterprise 等級的產品變動就顯得較爲緩慢。
- SME/Enterprise 等級的產品仍以 Intel x86 系統的平台爲主，而 SOHO 等級的平台硬體則多樣化且變化較快。另值得注意的是，在 SOHO 等級的 NetScreen 5GT 已經採用了 Intel IXP 425 的 Network Processor 做爲 CPU。是否意味著產品加速該往 Network Processor 而非 ASIC 的方向走，是值得未來注意的一件事。
- 各 VPN 產品皆能與 TeraVPN 做互通，顯示在互通性方面做的比去年好。
- 在壓力測試下，有的產品會自動視爲攻擊，而丟棄封包或拒絕 TCP 連線的建立，造成產品效能測試的困難。
- 在各類產品中，有不少產品都是在 Linux 系統上開發的。顯示 Linux 的平台，在產品開發上受到一定的青睞。
- 防火牆在需要處理封包內容的應用場合，如防毒或內容過濾系統，把封包 redirect 到專屬的系統仍然有其優勢。尤其是這些系統的特徵資料庫是否能經常或即時的更新，關係到偵測能力至爲重大。要防火牆廠商自行發展這些技術及維護資料庫並不是一件容易的事。
- 國內廠商的產品相較於國外廠商而言，差距主要還是在效能面，在功能面的差距還算不大。

4 市場趨勢

4.1 差異分析

針對上述的五大類安全性產品，我們觀察到其中仍有下列差異存在：

- 雖然未來的安全性產品有逐漸走向整合的趨勢，甚至已經有標榜多機一體的產品上市。然而就產品普及化的腳步來看，防火牆以及 VPN 的產品會最先做到，目前也以這兩項產品的廠商最多。下一步才是內容過濾器、IDS、防毒系統。
- 但從產值貢獻來看，卻有不同的結果。如果把桌上型電腦的防毒系統一塊列入考慮，反而是以防毒系統的產值最高，其次依序才是防火牆、VPN、IDS、以及內容過濾器。
- 對防毒系統、IDS、和內容過濾器來說，最重要的是它們的偵測或過

濾效果。而這個效果非常依賴於 signature 的維護和更新。因此在產品銷售出去之後，後續提供的服務才是重點。反觀防火牆及 VPN，在服務方面佔的比重就沒那麼重。

- 現有的國內大廠一開始時主要的產品是以 L2/L3 交換器與路由器的產品爲主，然後會往防火牆以及 VPN 的方向推進。主要的目標是全球市場。而國內新創的設備廠商一開始則會直接進入 IDS、防毒系統、內容過濾器的產品，其目標則較爲侷限在國內的市場。

4.2 綜合分析

就整體網路安全市場的狀況，我們的分析如下：

- 就網路安全功能在產品的穿透力(penetration)而言，這些功能會最先出現在閘道器、edge router、access point 等裝置上，但是可以看到的是，L2/L3 交換器也有若干程度的安全性功能。
- 就網路安全產品在市場的穿透力而言，大型企業會最先使用這些設備，然後是中小企業及電信服務單位，最後才進入 SOHO(Small Office, Home Office)以及家庭用戶。
- 就國內市場的分配而言，系統整合廠商(system integrator)所爭取的大型標案有 90%都還是由外商獲得，只有 10%由本土廠商獲得。而產品配銷商(distributor)的部分本土與外商的比例則呈現各 50%的態勢。在零售商(retailer)方面外商的比例最低，可能只有約 20%的比例，本土廠商則高達 80%。
- 在各項網路服務逐漸蓬勃發展之際，如何做到 AAA(Authentication, Authorization, Accounting)也是一個重要的安全性課題。例如提供無線上網的服務業者要如何確保他人不能不付費就能任意使用無線網路服務。這時一些存取的認證機制，如 IEEE 802.1X，就成爲一個重要的技術。
- 安全問題終究看來還是人的問題。目前的安全性產品大都還是集中在防範來自外面的入侵，但是如何處理內部員工可能造成的安全性問題，例如將公司資料任意攜出，卻是一個不可忽視的議題。

5 建議

爲了提升本土廠商在安全性產品的競爭力，有下列數點建議：

- 依前述分析，本土廠商雖然在產品配銷商及零售商方面的市場具有優勢，然而在系統整合市場卻趨於劣勢。爲了進入系統整合這塊市場，並往中高階產品發展，本土廠商應該與服務業者(含 SI、ISP 以及大學或大型企業)合作。政府的採購案也應該有一定比例(如 30%)限定採用本土廠商的產品，以扶植本土廠商的發展。
- 舉辦座談會以製造國內大廠與新創公司的合作與了解，以及合併的

可能，整合更多的資源和技術以發展更好的產品與經營模式。

- 由於系統的整合度及複雜性日益升高，因此良好的產品測試及認證的基礎設施以確保產品的功能及品質更形重要。
- 在教育市場上，應該多多舉辦相關的研討會，教育市場以及提供更多的技術交流。

6 網路安全產品發展的藍圖