第十章 防火牆

『防火牆？』倒像古代護城牆，不僅防禦外來的侵犯，更要保持居民的進出方便；當一道城牆不足於保護時，可再挖掘護城河，或多建幾道長城環環保護著。

10-1 私有網路安全簡介

10-1-1 各種網路型態簡介

『私有網路』(Private Network) 係指一般區域性網路，其範圍可能是組織單位、公司行號、學校、乃至個人的網路系統；應用範圍則涵蓋電子化辦公室、電子化生產系統、行銷系統、或某種特殊目的所構成的網路。基本上，私有網路是組織內獨立網路系統，所傳輸訊息亦較屬機密性，大多不希望讓外人窺視。隨著組織營運規模的擴充，大多需要與外部其他公司資訊系統互相通訊，因此獨立性的私有網路已漸不符所需。更進一步，也許需要提供內部訊息讓其他相關行業存取，或透過網路從事商業性行為，如此一來，內部機密性訊息可能暴露到組織外。

『公眾網路』(Public Network) 提供許多私有網路之間的溝通橋樑，其構成可區分為兩大部份，一者是建設基礎線路的電信公司，稱之為『網路服務提供者』(Network Service Provider, NSP)，譬如，中華電信公司、速博公司等等；另一者是提供網路服務的公司，稱之為『網際網路服務提供者』(Internet Service Provider, ISP)，譬如，HiNet、TANet、SeedNet 等等。NSP 公司主要提供數據傳輸專線、ADSL 連線、或國際衛星線路，經由這些連線可以擴展到任何地區，亦稱為『廣域網路』(Wide Area Network, WAN)。ISP 公司向 NSP 公司承租各種傳輸線路，將各地區網路結合一個穩定性較高的網路系統，並提供各種網路服務，如網頁空間、郵件系統、主機代理等服務。因此，習慣上將 ISP 所建構的網路稱為『大都會網路』(MAN)。一般私有網路公司可向 NSP 公司承租線路，加入 ISP 網路下的成員，再透過 ISP 網路連接之後，即可將訊息傳送到全世界任何角落上。由此可見，Internet 網路是由獨立性的私有網路與公眾網路所構成，然而公眾網路是結合全球各地的 ISP 與 NSP 網路而成。圖 10-1 為 Internet 網路系統的

概念圖，其中 M、N、T 與 P 是 ISP 所建構的大都會網路，至於 ISP 網路之間則透過 NSP 公司的數據傳輸線路來相互連接；私有網路可以向 NSP 公司承租專線或 ADSL 連線，連接到 ISP 公司的網路上，成為 ISP 網路下的成員。因此，私有網路透過公眾網路連接之後，便可通行於全世界。

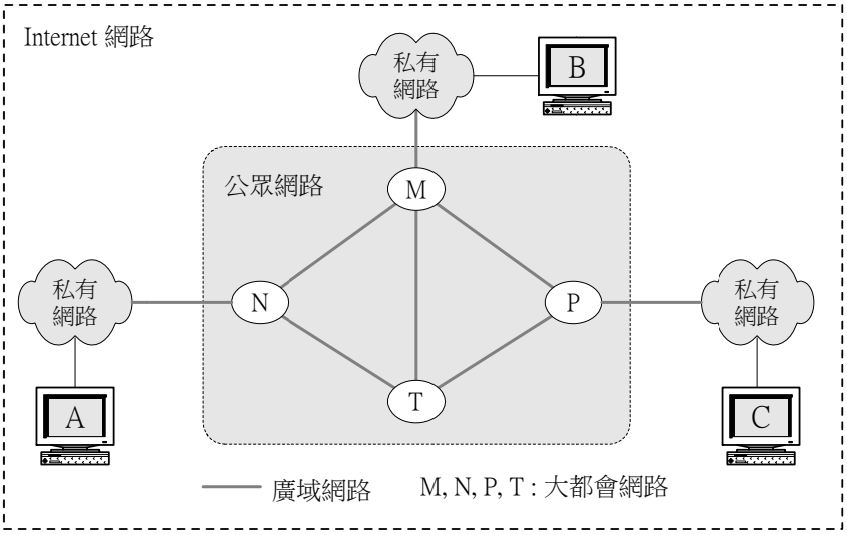


圖 10-1 私有網路與公眾網路

10-1-2 建構安全性私有網路

基本上，為了提高訊息流通量，公眾網路大多不會限制傳輸訊息的內容，並允許任何人由公眾網路上存取訊息，且僅依訊息封包之目的地給予轉送到適當位址上。也就是說，任何人都可藉由公眾網路傳送或接收訊息，並且不受限於時間或地點。由此可見，在公眾網路上傳輸的訊息是不安全的，易受有心人士窺視、竄改、或仿造，但話說回來。私有網路非藉由公眾網路傳輸訊息不可，因此如何達成私有網路安全性的問題，更顯得重要。

如何確保私有網路的安全？可由『點』與『線』兩個方向來思考。『點』表示確保某一區域性私有網路的安全；『線』表示如何透過公眾網路結合多個私有網路，並確保之間通訊的安全。前者大多仰賴一個『防火牆』(Firewall) 作為私有網路與公眾網路之間的隔離措施，它可以是一部主機電腦或一套網路設施，本章將介紹其相關技術。

圖 10-1-1

10-2 防火牆簡介

何謂『防火牆』(Firewall) ？ 這是初學者最迫切想知道的答案，如果從字面來解釋，好像是防止火災氾濫，建構一道堅固如銅牆鐵壁般的隔離措施。其實這樣解釋並不能完全表現出防火牆的功能，倒比較像中國古代的護城牆。護城牆保護著城內的居民免受外敵侵犯 (如秦始皇所建的萬里長城)，它除了阻擋外敵侵犯外，還必須維持城內和城外居民進出暢通，因此必須設有進出城門。有了城牆與城門之後，如何管制人民的進出？如何限制城內外人民的通訊方式？如何防範敵人偽裝混入城內從事破壞的工作？如何偵測出偽裝入城的敵人？以及如何恢復入侵敵人的破壞？以上等等便是『防火牆』所涵蓋的安全措施。

10-2-1 防火牆的功能

簡單的說，防火牆好比是城門的防護措施，如果防護太過嚴密 (甚至關閉城門)，便會失去建構網路的目的；但過於鬆散，易使內部資料暴露於外人之手，其間實難取捨。一般就安全措施的鬆緊度而言，主要依照私有網路的『安全政策』(Security Policy) 而定，並沒有一定的標準。

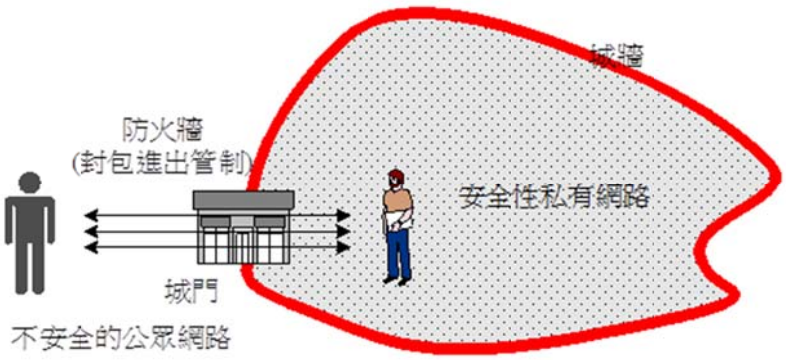


圖 10-2 防火牆的功能

我們可用圖 10-2 來說明防火牆的功能。防火牆是介於公眾網路和私有網路 (或稱內部網路、受保護的網路) 之間，是所有對內/對外通訊的『咽喉點』。當外部網路使用者欲傳送訊息進入內部網路，稱為『進入』(Inbound) 封包；而內部使用者送往外部網路的訊息，則稱為『外出』(Outbound) 封包。防火牆功能就是管制『進入』與『外出』封包的進出，以達到安全防護的目的。

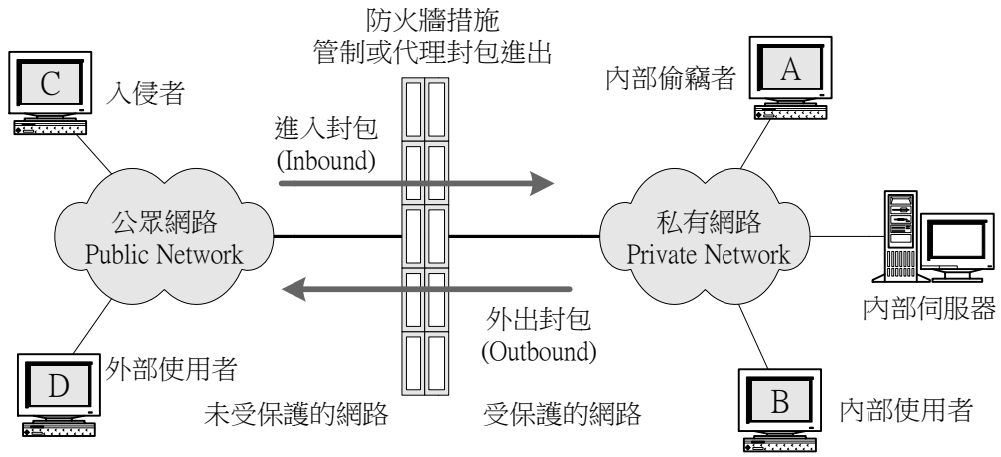


圖 10-2-1 防火牆架構

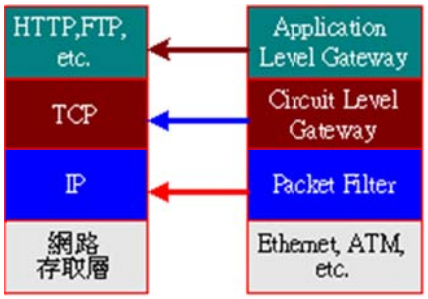


圖 10-3 防火牆協定堆疊

10-2-2 防火牆的措施

為了管制封包進出，一般建構防火牆有以下三大措施：

1. 過濾封包：依照封包的型態或內容來過濾它是否可以進出私有網路。過濾封包並不能保證完全防止入侵，許多入侵者都會偽造封包來矇騙封包過濾器。再者，過濾封包的原則也很容易產生漏洞，讓入侵者有機可乘。

2. 代理機制：進入或外出的封包並不直接通過防火牆，而是由某一個代理伺服器（Proxy Server）來完成客戶端的要求，再轉傳給客戶端。代理程式可以檢視封包內的『內容』(Content)，並決定是否給予轉送（過濾功能）。

3. 網路位址轉譯 (Network Address Translation, NAT)：其功能是隱藏內部網路位址。將內部私有網路位址轉譯到外部的合法位址，便可隱藏內部伺服器的真正位址，免除成為外部攻擊者的攻擊目標。

雖然 NAT 位址轉譯功能也是屬於防火牆的一種，但透過位址轉譯的伺服器將無法獨立運作於外部網路，它可說是接近於『鐵幕』般的安全措施。一般討論防火牆功能還是以封包過濾、電路閘門與應用層閘門等三種為主。

10-3 防火牆架構

10-3-1 防火牆設備

防火牆架構的型態是安全防護能力的主要關鍵，這是一般網路管理者必須詳細研究的課題。不安全的防火牆架構除了浪費許多精神維護之外，說不定連最基本的安全性也無法達成。但話又說回來，也不可能存在百分之百的安全架構，如欲達到一定的安全性，仍需仰賴維護人員隨時摸索，尋找網路的破綻以防止被攻擊。再說，各私有網路的情況不同，所面臨的挑戰也不會相同，因此，毫無標準規範可循。在介紹防火牆架構之前，首先介紹一些相關名詞及其所需的設備：

- 雙介面主機（Dual-homed Host）：表示某一主機上安裝有兩片網路卡，其中一片網路卡連結自己的網路系統，以達到隔離兩邊網路之目的；主機依照安全策略決定是否允許封包由某一網路轉送到另一個網路卡，因此，雙介面主機就好像是護城牆中的城門一樣，負責過濾或轉送人民進出的功能。至於雙介面主機可以是路由器、網路閘門、以及防禦主機等等。

- 防禦主機(Bastion Host): 防禦主機是進出封包的轉驛站，直接暴露於外部網路上，並且公告週知由此主機可以和內部網路通訊。防禦主機上可能安裝有封包過濾或代理程式，可依照防火牆架構決定是雙介面或單介面主機。防禦主機就好像辦公大樓的大廳一樣，任何人想與大樓內的人員從事交易行為，都必須先到大廳和管理人員交涉，再決定是過濾或代理。

- 封包（Packet）：防火牆檢測的最基本資料單位，一般指 IP 封包。

- 屏蔽路由器（Screening Router）：某一路由器具有封包過濾功能，並直接暴露於外部網路上，又稱為外部路由器。

- 周圍網路（Perimeter Network）：隔離外部網路與內部網路（受保護網路）之間的

網路，以提高內部網路的安全性。一般將周圍網路稱之為『DMZ 網路』（De-Militarized Zone，如南北韓之間的停戰區）。

接下來，我們將介紹三種防火牆的基本架構，一般私有網路的防火牆措施多半是由這三種基本架構演變而來。

10-3-2 雙介面主機架構

『雙介面主機』(Dual-homed Host)是最簡單的防火牆架構，網路型態如圖 10-4 所示。它利用一部雙介面主機作為隔離外部網路與內部網路（受保護網路），並依照防火牆的安全保護層次，決定雙介面主機是『屏蔽路由器』或『防禦主機』。如果採用防禦主機，則此主機上必須安裝有代理程式（如 SOCKS 或 ISA 2000）；如果採用屏蔽路由器，則此路由器必須安裝封包過濾程式，當然防禦主機上也可以安裝封包過濾程式，同時達到封包過濾與代理器的功能。一般較小企業公司喜歡採用此種架構，因為它的價格最便宜，但防護能力有限，容易被攻破。

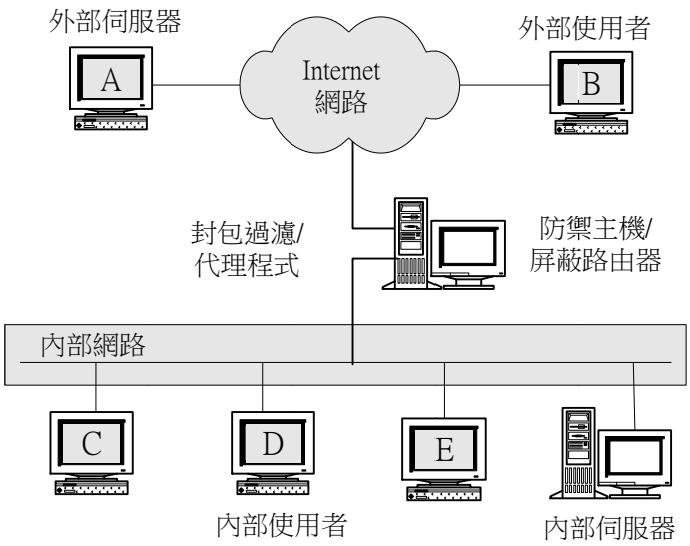


圖 10-4 雙介面主機式架構

無論主機是採用防禦主機或屏蔽路由器，它都將直接暴露於外界網路上，攻擊者只要尋找出該主機的漏洞，便可趁虛而入侵系統。最簡單的方法是搜尋主機是否有其它埠口打開（通常選擇較少使用或較不起眼的埠口），再利用此埠口從事破壞的工作。另外，既然外部使用者可以直接進入內部網路，便可循正規管道將病毒帶入系統內，利用該病毒打開一些較不起眼的埠口（一般都是 1024 以後的埠口，又稱為開後門），讓外

界入侵者長驅直入。

10-3-3 屏蔽主機架構

『屏蔽主機』(Screening Host) 架構會比雙介面主機的安全性高一點，也是目前私有網路中普遍採用的型態。屏蔽主機架構是由一部屏蔽路由器及一部防禦主機所構成，如圖 10-5 所示，其中屏蔽路由器的功能是過濾封包，限制封包進出私有網路，至於防禦主機則是扮演代理伺服器的功能，代理外部使用者存取內部伺服器，或代理內部使用者存取外部伺服器。兩者的工作項目必須互相配合，最基本的設定是：

- ◈ 對外部使用者而言：只允許外部使用者連結到防禦主機，亦即屏蔽路由器只允許目的地是防禦主機的封包可以通過，並完全隔離掉其他封包，既然由防禦主機代理外部使用者存取內部伺服器，所以可以減少暴露內部主機的機會。

- ◈ 對內部使用者而言：由私有網路的『安全政策』決定，是否允許內部使用者通過屏蔽路由器，存取外部伺服器或與外部網路通訊。較嚴密的單位為了安全考量是不允許的，所以屏蔽路由器阻擋往外的連線，至於所有通訊行為都必須透過防禦主機代理，並且可以在防禦主機上登錄所有向外的通聯記錄。一般公司學校大多允許內部使用者自行決定，是要直接通過屏蔽路由器向外連線，還是透過防禦主機上的代理程式 (如 Proxy Server)。

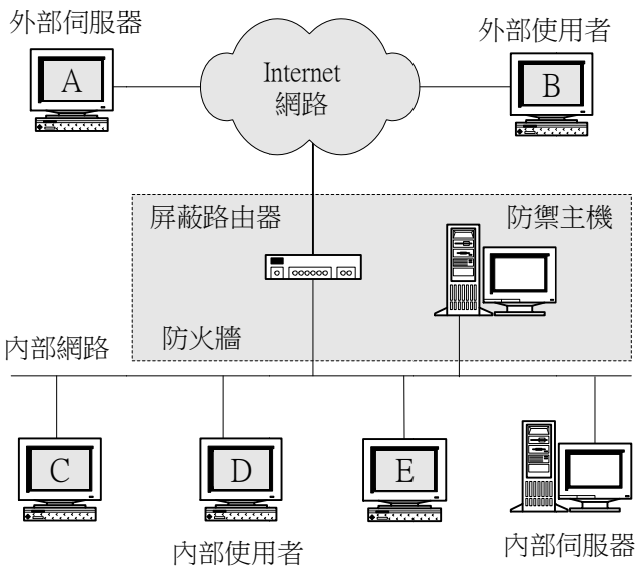


圖 10-5 屏蔽主機架構

乍看之下，防禦主機架構好像對外或對內都可達到很好的安全措施，但無論如何，攻擊者還是可以通過屏蔽路由器（無論合法或非法擊破）進入內部網路。另一方面，我們雖然可禁止內部連線通過屏蔽路由器，達到隱藏內部主機的目的。若不幸讓入侵者通過屏蔽路由器，便可以在內部網路上收集所有通訊訊息，再由訊息中分析出系統主機；只要得到主機的相關資料，欲從事破壞或偷竊的行為就不會很難了。由此可見，防禦主機架構的安全性並非如想像中的完美，有心人士還是可以輕而易舉攻破它。

10-3-4 屏蔽網路架構

在防火牆概念中，並無所謂百分之百的安全架構，而是設法架設一種讓攻擊者較不容易擊破的防護措施，也就是說，『建立一種讓攻擊者必須耗費多時難以擊破的防火牆』。上述兩種架構只築一面城牆（或城門）從事安全措施，攻擊者祇要突破這個城門便可長驅直入內部網路。為了延長被攻擊進入內部網路的時間，簡單的方法就是多建立幾道城牆，亦即當入侵者擊破第一道門之後，必須再經過第二道、第三道、等等，始可進入到內部網路。因此，網路管理者必須隨時監視是否有被入侵的情況，只要在入侵者尚未完全進入到內部網路之前，將之揪出，正所謂亡羊補牢，尤時未晚。

多建立幾道城門（或城牆）之後，城牆和城牆之間稱為『周圍網路』（Perimeter Network），一般將周圍網路稱為『非軍事區網路』（DMZ 網路，De-Militarized Zone），如南北韓之間的停戰區。但在防火牆措施上稱之為『屏蔽式子網路』（Screened Subnet，簡稱屏蔽網路）架構，網路基礎型態如圖 10-6 所示。

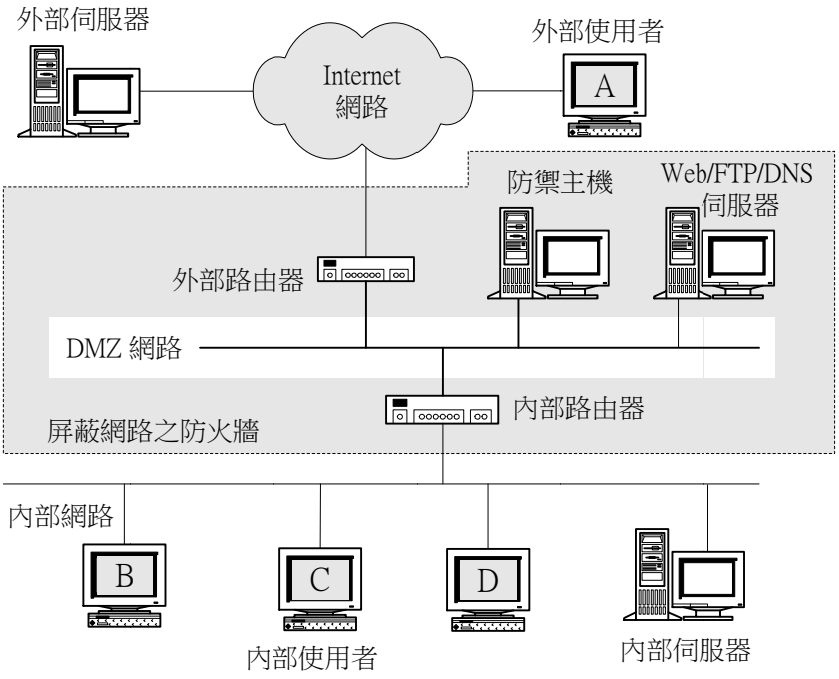


圖 10-6 屏蔽網路架構

圖 10-6 中包含外部路由器、內部路由器與防禦主機等三個主要設備，並沒有一定的規則來定義它們應該處理什麼樣的安全措施，完全視私有網路的『安全政策』而定。簡單的設定是將外部與內部路由器設定成封包過濾器，而將防禦主機安裝成代理伺服器（如 Proxy Server、FTP Server、SOCKS Server），其管理措施如下：

◈ 對外部使用者而言：外部路由器僅允許連結到防禦主機的封包進入，再透過防禦主機的代理系統存取內部的伺服器，至於內部路由器也只允許來源目的為防禦主機的封包進入內部網路。

◈ 對內部使用者而言：一般系統大多不會採取嚴格的限制，但某些較特殊的單位不在此限。簡單的做法是，內部路由器祇允許目的位址為防禦主機的封包出去，並由防禦主機的代理系統存取外部伺服器，另一方面，外部路由器也只允許來源位址為防禦主機的封包進入；另一種做法是，將內部路由器設定成『網路位址轉譯器』(NAT)，如此便可達到隱藏內部網路位址的功能，而內部使用者連結到外面也比較不容易被追蹤出來。

◈ 對公開伺服器而言：私有網路也許需要將某些伺服器公開給外部使用者存取，譬如，電子商務系統必須公開網頁伺服器、FTP 伺服器等等。私有網路可以選擇將公開伺服器架設於周圍網路或內部網路，如果選擇放在內部網路，則外部使用者

都必須透過防禦主機存取；如放在周圍網路，則可在外部路由器上設定，是否允許外部使用者直接存取公開伺服器，或需透過防禦主機代理。

在 DMZ 網路之下，入侵者擊破外部路由器之後，還隔著一道牆，因此無法直接觀察到內部網路的通訊行為，仍需花費一段時間才能攻擊內部路由器。一旦入侵者擊破內部路由器之後，始可搜尋到內部網路訊息，所以在這個期間，管理者必須設法將入侵者找出來，並將它堵死。這個情況好比，入侵者先派間諜進入城內（無論合法或非法進入），並開啟另一道門（也就是通訊埠口），再讓入侵程式直接由那一道城門進入；另一種情況是，間諜並不開啟後門（通訊埠口），直接將收集的資料透過合法管道傳送給外部入侵者。當然有許多入侵方法不勝枚舉，但無論如何，管理者必須在入侵者得逞之前發現，並將它刪除。

10-4 封包過濾器

10-4-1 封包過濾器的種類

『封包過濾』（Packet Filtering）是防火牆最基本的功能，是最不可或缺的工具。在 Internet 網路上，訊息跨越網路之間傳輸的最基本資料單元為 IP 封包，當 IP 封包經過某一路由器時，路由器將會拆解它，再由封包標頭上的目的位址決定如何轉送（或是否給予轉送）。如果路由器除了判斷目的位址之外，還增加判斷其他訊息（如來源位址或協定型態），再決定是否給予轉送，便成為『封包過濾器』。基本上，由一般路由器改變成為封包過濾器並不困難，所以一般路由器都兼具有封包過濾功能。

再說，Internet 網路上各種通訊協定（如 TCP、UDP、ICMP），都是利用 IP 封包傳輸，因此，只要針對 IP 封包來過濾，便能達到防火牆的功能。但封包過濾並不只拆解到 IP 封包標頭，隨著防火牆的安全考量，或許會拆解到上一層的協定封包，所以有所謂 IP/TCP、IP/UDP、以及 IP/ICMP 等封包過濾功能。但無論封包拆解到何種程度，都是由該協定標頭上的訊息決定是否給予過濾。

但話說回來，限制何種封包可以進出防火牆，看似非常容易，其實這些規則設定時可說是漏洞百出，而且有些漏洞不易被發現，於是便成為被攻擊的目標，這對網路管理者而言不失為一大挑戰。

10-4-2 封包過濾器的設定規則

如將封包過濾功能安裝於路由器上，便稱之為『封包過濾路由器』(Packet Filtering Router)，它與一般路由器有很大的不同，以下是封包過濾路由器應該注意的事項：

1. 關閉路由功能：封包過濾路由器必須完全關閉路徑選擇的功能，封包是否給予通過完全由過濾訊息判斷。
2. 關閉閒置的埠口：必須完全關閉閒置的傳輸埠口，因為入侵者會隨時去搜尋過濾路由器上有那些傳輸埠口接受服務，並由這些埠口進入系統。
3. 關閉不需要的服務：許多過濾路由器是利用 Unix/Linux 或 Windows 2003 主機來裝置，這些主機系統會預設執行許多應用服務，管理者應該刪除掉與過濾功能無關的應用程式，甚至對於不了解其功能的程式，最好也關閉。
4. 協定是雙向的：一般通訊協定都是必須經過雙方溝通，即一方送出詢問，另一方收到後便會自動給予回應。因此，在制定過濾原則時，必須弄清楚雙方通訊的內容，有時候不同協定之間的通訊內容可能會互相牴觸。
5. 進入 (Inbound) 和出去 (Outbound) 的方向性：既然通訊協定是雙向的，對於訊號的外出或進入，設定過濾規則時不可搞混，否則將失去過濾的功能。
6. 內定值為拒絕：將所有過濾條件的內定值都預設為拒絕，除了經過設定允許的條件才給予通過，這對防火牆而言較為安全。如將內定值預設為允許，要找出不允許通過的條件必定非常繁雜，徒增系統的不安全性。

至於 IP 封包內有那些訊息可以作為過濾判斷的條件，這並沒有一定的規範可循。基本上，若依照封包上的訊息來判斷過濾的條件，就封包被拆解程度，以及封包種類，可區分為：IP 封包過濾、IP/TCP 封包過濾、IP/UDP 封包過濾、以及 IP/ICMP 封包過濾等四種型態，下一節將會說明這些封包過濾的設定原則。

封包過濾器必須依照安全措施，設定某些過濾規則。然而在建立規則時必須考慮到該通訊協定 (如 IP、TCP) 的運作方式，如此說來，設定過濾規則恐非易事，一般可依照下列步驟設定：

◈ 步驟 1：關閉所有封包過濾，一般封包過濾器的內定值都是『拒絕』轉送的，所以未經開放的封包是無法通過的。

◈ 步驟 2：選擇欲開放的應用協定，如 Telnet、FTP、Ping 等等。

◈ 步驟 3：選擇拆解封包標頭的訊息，如 IP、IP/TCP、IP/ICMP、IP/UDP 等等

◈ 步驟 4：列出該應用協定運作時可能產生的訊息，並製作一個『封包訊息表』。

◈ 步驟 5：由上述表格中尋找可供開放的規則，並建立『過濾規則表』。

◈ 步驟 6：將上述規則設定於封包過濾器上，一般封包過濾器都有提供輸入命令（如 iptable）或圖形介面（如 ISA Server），讓管理者輸入過濾規則。

並非所有應用都需要依照這些規則來設定，可視管理者自己如何變通。

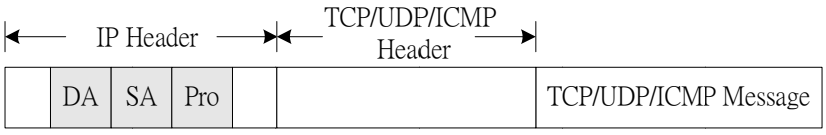
10-5 IP 封包過濾

所謂 IP 封包過濾係路由器（或防禦主機）祇拆解到 IP 協定標頭，其中可供過濾判斷的條件如下：（如圖 10-8 所示）

1. 來源位址（Source Address, SA）：表示此封包的來源位址，由此位址可以判斷出該封包是來自外部網路或內部網路（受保護的網路）。

2. 目的位址（Destination Address, DA）：表示此封包所欲連結的位址。由此位址可以知曉該封包欲前往外部網路或內部網路。

3. 協定（Protocol, Pro）：表示此封包所承載的訊息是何種通訊協定，可能是承載 TCP、UDP、ICMP 等協定。



10-8 IP 封包過濾訊息

10-5-1 IP 過濾訊息與範例

IP 封包過濾大多祇針對網路位址作為過濾的依據，我們舉一個範例來說明它的運

作情形，以其過濾規則的設定。圖 10-9 為一簡單的防火牆設備，內部網路的網路位址為 163.15.0.0/16（網路遮罩為 255.255.0.0），希望設定的條件為：

1. 僅允許目的位址為 163.15.0.0/16 的封包，通過防火牆進入內部網路。
2. 內部網路可以通往外部網路的任何地方（0.0.0.0）。

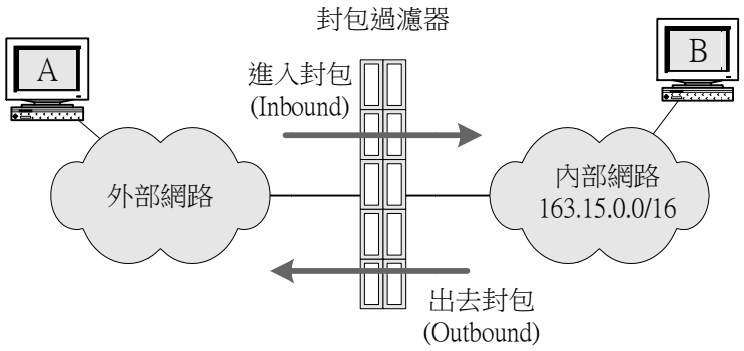


圖 10-9 IP 封包過濾範例

依照上述條件，所制定的防火牆規則如表 13-1 所示。

表 10-1 IP 封包過濾規則表

規則	方向	來源位址	目的位址	措施
A	進入	任意	163.15.0.0/16	允許
B	出去	任意	任意	允許
C	皆可	任意	任意	拒絕

其中規格 C 為內定值，並預設為『拒絕』。我們用幾個範例來探討看看，這些規則是否符合所期望的防火牆條件：

1. 如果內部工作站（163.15.4.32）欲通過防火牆，連結到外部伺服器（124.12.6.7），其目的位址為 124.12.6.7，因為符合規則 B，防火牆給予通過。
2. 如果外部伺服器 (124.12.6.7) 欲傳送訊息給內部工作站（163.15.4.32），其目的位址為 163.15.4.32；來源位址是 124.12.6.7，因為符合規則 A，防火牆給予通過。
3. 如果外部伺服器 (124.12.6.7) 欲傳送訊息給某一工作站（164.15.4.123），其目的位址為 164.15.4.123，來源位址是 124.12.6.7，因為符合規則 C，防火牆拒絕通過。

由此可見，僅利用 IP 標頭訊息來過濾封包，其安全性功能非常的低，幾乎與原來路徑選擇的功能沒有兩樣；接下來介紹其他較有效果的過濾方法。

10-6 IP/TCP 封包過濾

對一般應用而言，僅利用 IP 封包標頭從事過濾條件是不夠的，若能拆解到上一層協定（如 TCP、UDP）標頭，了解該封包功能之後，再判斷是否允許通過防火牆，這樣可能比較實際一點。圖 13-10 為 IP 封包中包裝 TCP 訊息，一般防火牆所採用的判斷訊息如下：

1. 來源位址（SA）：由 IP 標頭取得，表示該封包的來源 IP 位址。
2. 目的位址（DA）：由 IP 標頭取得，表示該封包的目的 IP 位址。
3. 協定型態（Pro）：由 IP 標頭取得，表示該封包所承載的協定，如 TCP 協定。
4. 來源埠口（Source Port, SP）：此封包的來源傳輸埠口（TCP Port）。
5. 目的埠口（Destination Port, DP）：此封包之目的傳輸埠口（TCP Port）。
6. 位元碼（Code bits）：此為 TCP 標頭欄位，包含有 URG、ACK、PSH、RST、SYS 與 FIN 等位元控制訊息。至於應該取用那些控制訊息，作為封包過濾的判斷條件，管理者可依照防火牆的安全條件決定，但較常取用的訊息有：
   - ◈ ACK（Acknowledge）：表示回應確認給原發送端。此旗號是判斷條件的關鍵性因素，但它必須配合三向握手式連絡法的運作程序，容後說明。
   - ◈ SYN（Synchronous）：表示通知對方要求連線的控制訊息。

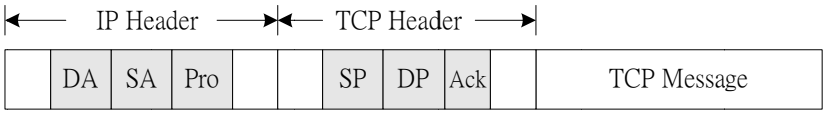


圖 10-10 IP/TCP 過濾封包訊息

一般 TCP/UDP 1024 以前的埠口皆歸劃為系統管理者使用，並且將較常用的『著名埠口』(Well-known) 設定在 1024 之前的埠口，至於使用者的隨機埠口都介於 1024 ~ 65535 之間。在正常的情況下，由埠口號碼就可以知道該封包所欲連結之伺服器，譬

如，HTTP 伺服器固定在埠口 80、Telnet 伺服器則在埠口 23。

封包過濾條件是由 IP 和 TCP 標頭上的訊息所構成，更能表示出封包的特性。再說，一般系統為了達到多重連線的功能（譬如，一個 Web 伺服器可同時接受多個客戶端連線），每一個通訊連線都是由雙方的 IP 位址與 TCP 埠口號碼來表示，譬如，192.38.24.50:80 ←→ 163.15.2.30:3456，則表示兩部電腦（192.38.24.50 與 163.15.2.30）的傳輸埠口（80 與 3456）之間的連線。由此可見，的確須拆解到 TCP 封包標頭，對於封包過濾的條件判斷才具意義。

10-6-1 TCP 過濾訊息與 ack 參數

我們不可能為了架設防火牆設施，去修改目前運作中的 TCP 協定，只能就現有運作的程序中找尋可能過濾的條件因素。TCP 協定是屬於連接導向的傳輸方式，通訊雙方必須先建立連線，才可以傳輸資料。因此，如欲限制 TCP 連線是否可通過防火牆的話，只要限制其連線與否即可。也就是說，只要過濾 TCP 建立連線的封包，即可決定是否允許該訊息通過防火牆。

TCP 連線是採用三向握手式連絡法，如圖 10-11 所示。它是利用封包標頭上的兩個旗號：SYN（Synchronous，要求連線）與 ACK（Acknowledge，確認），達到雙方溝通的目的，其運作程序如下：發起者發送要求連線封包（SYN = 1、ACK = 0，訊號 (1)），回應者發送同意連線封包（SYN = 0、ACK = 1，訊號 (2)），發起者再確認同意連線（SYN = 0、ACK = 1，訊號 (3)）。由此可以發現一個重要現象，除了要求連線封包的 ACK 旗號為零外（ACK=0），其它封包的 ACK 旗號都為 1（ACK=1），因此只要從 ACK 的內容即可判斷是否為連線要求封包，其中：

- ACK = 0：表示連線要求訊號。
- ACK = 1：表示回應同意連線訊號。

如此一來，再由 ACK 旗號、目的位址、以及來源位址，便可判斷出是外出或進入的連線要求，或是回應連線要求的訊號；如果再增加傳輸埠口號碼，更可以瞭解該連線所欲連接的應用系統（如 Telnet 或 FTP），一般只要利用這些參數來過濾封包，皆可達到防火牆的功能。

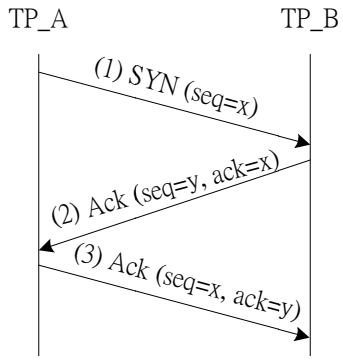


圖 10-11 TCP 三向握手式連絡法

10-6-2 TCP 過濾範例：Telnet 連線

接下來，我們利用 Telnet 連線為範例來說明 IP/TCP 封包過濾規則的設定方法，以及是否加入 ACK 旗號可能出現的問題。圖 10-12 為 Telnet 連線範例，首先我們來觀察 Telnet 連線會產生哪些訊號，如下：(IP 與 TCP 埠口位址皆為假設值，Telnet 埠口位於 23/tcp)

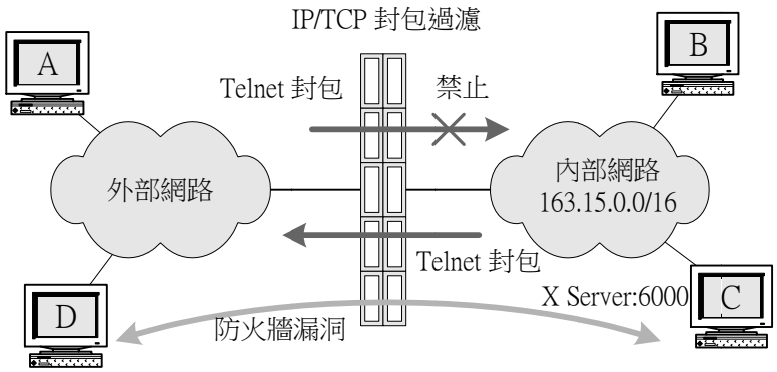


圖 10-12 IP/TCP 封包過濾範例

1. 外部使用者要求建立 Telnet 連線之封包：IP 標頭之目的位址為 163.15.2.3、來源位址為 138.4.5.23、協定是 TCP，TCP 標頭之目的埠口為 23、來源埠口為 5860 (>1024)、ACK 未設定。

2. 內部主機回應 Telnet 連線之封包：目的位址=138.4.5.23、來源位址= 163.15.2.3、協定= TCP、目的埠口= 5860、來源埠口= 23、ACK =1 (有設定)。

3. 內部使用者要求 Telnet 連線到外部主機之封包：目的位址= 138.4.5.23、來源位址= 163.15.2.3、協定= TCP、目的埠口= 23、來源埠口= 4567、ACK =0 (未設定)。

4. 外部主機回應內部使用者 Telnet 連線之封包：目的位址= 163.15.2.3、來源位址= 138.4.5.23、協定= TCP、目的埠口= 4567、來源埠口= 23、ACK = 1。

吾人依照網路內外發送 Telnet 連線，可能產生的訊息建立一個『封包訊息表』，如表 10-2 所示。

表 10-2 Telnet 封包訊息表

序號	服務方向	封包方向	來源位址	目的位址	封包型態	來源埠口	目的埠口	設定 ACK
1	出去	出去	任意	內部	TCP	>1024	23	No
2	出去	進入	內部	任意	TCP	23	>1024	Yes
3	進入	進入	任意	內部	TCP	> 1024	23	No
4	進入	出去	內部	任意	TCP	23	>1024	Yes

序號(1) 為內部工作站利用 telnet 連結外部工作站，所產生的封包訊息。序號(2) 是外部工作站同意 telnet 連結所產生的訊息。序號(3) 與 (4) 則是外部工作站向內部發送 telnet 連線與回應所產生的訊息。接下來，我們依照幾個防火牆的安全措施，再參照『訊息封包表』，來建立『封包過濾規則表』，以及討論可出現哪些問題。

10-6-3 允許 Telnet 無 ack

假設防火牆僅允許內部與外部之間利用 telnet 通訊，且不允許利用其他協定連線。假設吾人所採用的封包過濾表不考慮 ACK 訊號，依照表 13-2 的封包訊息表，所建立『封包過濾表』，如表 10-3 所示（未採用 ACK 旗號）。

表 10-3 Telnet 封包過濾規則表之一（無 ACK 旗號）

規則	封包方向	來源位址	目的位址	協定	來源埠口	目的埠口	措施
A	出去	內部	任意	TCP	>1023	23	允許
B	進入	任意	內部	TCP	23	>1024	允許
C	進入	任意	內部	TCP	>1023	23	允許
D	出去	內部	任意	TCP	23	>1024	允許

E	皆可	任意	任意	TCP	任意	任意	拒絕

在正常情況下，測試這些規則是否可行，如下：

1. 外部主機要求對內部主機做 Telnet 連線時，符合規則 C 和 D，連線是許可的。
2. 內部主機要求對外部主機做 Telnet 連線時，符合規則 A 和 B，連線是許可的。
3. 外部主機要求對內部主機做 FTP 連線（埠口為 TCP/21）時，不符合 A、B、C 和 D 規則，且符合規則 E，封包被拒絕通過。

10-6-4 允許 Telnet 有 ack

假設封包過濾如表 10-3 方式設定，其中沒有考慮到 ACK 旗號，吾人來探討它可能產生的漏洞與補救方法。一般製作過濾規則時，大多假設客戶端的傳輸埠口都大於 1024；而伺服端的傳輸埠口都小於 1024。但有許多情況並非如此，目前在 Internet 有些伺服器可能架設於 1024 以後的埠口上，譬如，較常見的 Proxy Server 便架設在 8080 埠口上，還有許多資料庫伺服器也是一樣；另一方面，客戶端的埠口也可以由使用者自行選定（並非一定是動態），甚至可以使用小於 1024 的埠口（假設使用者有系統管理的權限），然而上述的假設是非常危險的。

舉一個簡單的例子，原來圖 10-11 架構是僅允許 telnet 連線通過，但內部網路有一個 X-Server 設定在 TCP/6000 埠口上，並不允許外部使用者透過防火牆進入連線。外部入侵者發現了這個伺服器之後，並利用自己主機的 23 埠口來要求連線，所傳送的封包如表 10-4。

表 10-4 X-Server 訊息表

服務方式	封包方向	來源位址	目的位址	封包型態	來源埠口	目的埠口	措施
要求連線	進入	外部	內部	TCP	23	6000	符合規則 B
同意連線	出去	內部	外部	TCP	6000	23	符合規則 D

結果發現這個連線是被允許的，其中原來規則 B 是內部網路連結（Telnet）到外部網路時，防火牆讓外部網路的回應訊息進入所使用的，竟被用來同意外部網路要求連結內部網路的 X-Server。最主要原因是，防火牆並未判別『要求連線』和『回應連線』封包之間的不同點，如何去判別它們之間的不同，這需視 ACK 旗號而定；如果 ACK 旗號未設定，則表示是『要求連線』封包；否則為其它封包。

如果您堅持不使用 ACK 旗號，是否可達到防護的能力，答案當然是肯定的。但您必須非常清楚系統上到底有多少伺服器被啟動，並且針對每一個伺服器去做限制的過濾規則。我們用上述的例子，假設系統中有一個 X-Server 位於 TCP/6000 埠口上，並不願意讓外界使用，則防火牆設定規則如表 10-5。

表 10-5 Telnet 封包過濾規則表之二（無 ACK 旗號）

規則	封包方向	來源位址	目的位址	協定	來源埠口	目的埠口	措施
A	出去	內部	任意	TCP	>1023	23	允許
B	進入	任意	內部	TCP	23	>1024	允許
C	進入	任意	內部	TCP	>1023	23	允許
D	出去	內部	任意	TCP	23	>1024	允許
E	進入	任意	內部	TCP	>1023	6000	拒絕
F	出去	內部	任意	TCP	6000	>1023	拒絕
G	皆可	任意	任意	TCP	任意	任意	拒絕

上表中增加了規格 E 和 F 便可限制外部使用者存取 X-Server（TCP/6000），接下來，我們來探討加入 ACK 旗號的現象。

假設允許內部與外部網路之間的 Telnet 連線，但拒絕其它連線；還是利用前面的『封包訊息表』來設定規則，但如考慮到 ACK 旗號，則設定規則如表 13-6：

表 10-6 Telnet 封包過濾規則表之三（有 ACK 旗號）

規則	封包方向	來源位址	目的位址	協定	來源埠口	目的埠口	ACK 設定	措施
A	出去	內部	任意	TCP	>1023	23	皆可	允許

B	進入	任意	內部	TCP	23	>1024	是	允許
C	進入	任意	內部	TCP	>1023	23	皆可	允許
D	出去	內部	任意	TCP	23	>1024	是	允許
E	皆可	任意	任意	TCP	任意	任意	皆可	拒絕

當過濾規則設定好之後，如前述圖 10-12 範例，入侵者欲以來源埠口 23，連接內部 X-Server（TCP/6000）的運作情形變為：

1. 入侵者要求連線的封包:來源位址 = 外部主機、目的位址 = 內部主機、協定 = TCP、來源埠口 = 23、目的埠口 = 6000、ACK = 否。可以比較一下規則 B，規則 B 上的 ACK 必須是被設定的，因此不符合規則 B 的條件，此封包是被拒絕的。

2. X-Server 回應入侵者的封包：來源位址 = 內部主機、目的位址 = 外部主機、協定 = TCP、來源埠口 = 6000、目的埠口 = 23、ACK = 是。可以比較一下規則 A，它是被允許通過的，但這個封包是在要求連線封包可以進來的情況下，才有可能發生，所以永遠不會發生。

10-6-5 僅允許內部往外 Telnet 連線

假設只允許內部使用者以 Telnet 連線到外部主機，但不允許外部使用者連線到內部主機；還是利用上述的『封包訊息表』，所設定的過濾規則如 10-7。

表 10-7 Telnet 封包過濾規則表之四（有 ACK 旗號）

規則	封包方向	來源位址	目的位址	協定	來源埠口	目的埠口	ACK 設定	措施
A	進入	任意	內部	TCP	>1023	23	皆可	允許
B	出去	內部	任意	TCP	23	>1024	是	允許
C	皆可	任意	任意	TCP	任意	任意	皆可	拒絕

由以上的過濾規則範例，我們大略可以知道設定規則最基本的原則如下：首先所有可能進出的封包都設定為『拒絕』(如上述的規則 C)；欲開放哪一種服務再依照該服務的埠口、協定設定開放規則；接下來，必須追蹤所開放的規則中是否有漏洞，如有

的話，必須針對漏洞找出原因，並且將它設定成『拒絕』。

10-7 IP/UDP 封包過濾

10-7-1 UDP 過濾訊息

UDP 協定是屬於非連接方式，每一個封包都是獨立的，因此，決定 IP/UDP 封包是否給予通過的判斷訊息如圖 10-13 所示：

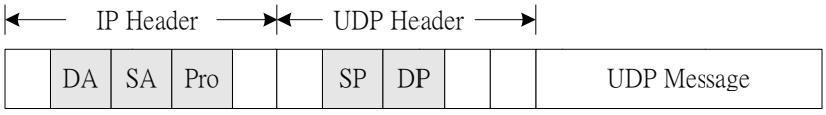


圖 10-13 IP/UDP 封包過濾訊息

1. 來源位址（SA）：封包的來源位址。
2. 目的位址（DA）：封包的目的位址。
3. 協定型態（Protocol, Pro）：UDP 型態。
4. 來源埠口（Source Port, SP）：封包的來源 UDP 埠口。
5. 目的埠口（Destination Port, DP）：封包的目的 UDP 埠口。

雖然 UDP 封包只有來源和目的埠口可作為過濾條件的判斷，但 UDP 協定並沒有交談式的建立連線（三向握手式連絡法），每一個封包的進出都是獨立的，因此，只要針對封包的目的埠口做過濾判斷即可。

一般來講，我們設定防火牆都是以所提供的服務為基礎，並且以伺服器的傳輸埠口與所使用的協定（TCP 或 UDP）為過濾條件。但有許多伺服器為了方便連結使用都會同時使用 UDP 或 TCP 協定，也就是說，伺服器是固定在某一傳輸埠口（如 161），客戶端可使用 TCP 協定去連接它（TCP/161）或 UDP 協定來連接（UDP/161），因此，我們在設定過濾規則時，必須同時考慮到可能連接的兩種協定。

10-7-2 SNMP 封包過濾範例

我們舉一個較複雜的範例來說明，如何同時考慮到 UDP 和 TCP 協定。圖 13-14

為『簡易網路管理協定』(Simple Network Management Protocol, SNMP) 的運作程序。一般網路只允許所有 SNMP 封包在內部網路運作，而不能跨越防火牆到外部網路；另一方面，也禁止外部使用者以 SNMP 命令來入侵內部網路，從事破壞或偷竊內部網路的狀態 (SNMP 資料)。但某些情況，為了管理方便而允許外部使用者管理內部網路，我們就以這個範例說明 UDP/TCP 同時過濾的情況，但需先瞭解 SNMP 協定的運作程序：

1. 命令運作程序：由 SNMP Manager 下達命令 (Set/Get/GetNext/GetBulk) 給 SNMP Agent，其中目的埠口為 161；SNMP Agent 收到命令後，並回應訊息給 SNMP Manager，其中來源埠口為 161。

2. Trap 運作程序：當 SNMP Agent 有異常事件時，會以 Trap 命令傳送訊息給 SNMP Manager，而 SNMP Manager 聆聽埠口 162，隨時等待 SNMP Agent 的 Trap 訊息，如收到訊息便回應給 SNMP Agent，其中來源埠口為 162。

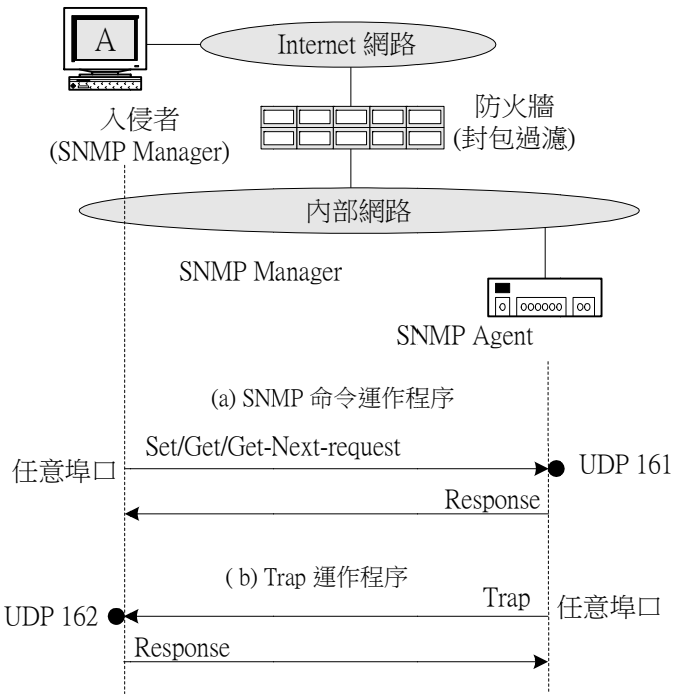


圖 13-14 SNMP 封包過濾設定範例

(A) SNMP 封包訊息表

假設外部網路有一個 SNMP Manager，想通過防火牆來操控內部網路的 SNMP Agent (使用 Set/Get 等命令)，此外，內部 SNMP Agent 也可能以 Trap 命令，將網

路狀態傳送給外部 SNMP Manager。若採用 TCP 或 UDP 協定傳輸，則可能出現的封包如表 13-8。

表 13-8 SNMP 封包訊息表

編號	封包方向	來源位址	目的位址	封包型態	來源埠口	目的埠口	ACK	封包功能
1	進入	外部	內部	UDP	>1024	161	Null	外部 Manager 傳送命令給內部 Agent（UDP）。
2	出去	內部	外部	UDP	161	>1024	Null	內部 Agent 回應訊息給外部 Manager（UDP）。
3	進入	外部	內部	TCP	> 1024	161	No	外部 Manager 向內部 Agent 要求 TCP 連線。
4	出去	內部	外部	TCP	161	>1024	Yes	內部 Agent 同意外部 Manager 的 TCP 連線要求。
5	出去	內部	外部	TCP	>1024	161	No	內部 Agent 向外部 Manager 要求 TCP 連線，以備傳送 Response。
6	進入	外部	內部	TCP	161	>1024	Yes	外部 Manager 同意內部 Agent 要求 TCP 連線，以備傳送 Response。
7	出去	外部	內部	UDP	>1024	162	Null	內部 Agent 傳送 Trap 訊息給外部 Manager（UDP）。
8	進入	內部	外部	UDP	162	>1024	Null	外部 Manager 回應 Trap 訊息給內部 Agent（UDP）。
9	出去	外部	內部	TCP	>1024	162	No	內部 Agent 向外部 Manager 要求建立 TCP 連線，以備傳送 Trap 訊息。
10	進入	內部	外部	TCP	162	>1024	Yes	外部 Manager 同意內部 Agent 所要求的 TCP 連線（Trap 訊息）。
11	進入	外部	內部	TCP	162	>1024	No	外部 Manager 向內部 Agent 要求建立 TCP 連線，以備回應 Trap 訊息。

12	出去	內部	外部	TCP	>1024	162	Yes	內部 Agent 同意外部 Manager 所要求的 TCP 連線（回應 Trap）。

(B)僅允許外部某主機連線

我們假設允許某一外部主機（138.45.6.32），可以經過防火牆來管理內部網路，但不允許內部網路設備以 Trap 命令通知外部 SNMP Manager，所設定的規則如表 13-9 所示。

表 13-9 SNMP 封包過濾表

規則	封包方向	來源位址	目的位址	協定	來源埠口	目的埠口	ACK 設定	措施
A	進入	138.45.6.32	內部	UDP	>1024	161	Null	允許
B	出去	內部	138.45.6.32	UDP	161	>1024	Null	允許
C	進入	138.45.6.32	內部	TCP	>1024	161	皆可	允許
D	出去	內部	138.45.6.32	TCP	161	>1024	是	允許
E	皆可	任意	任意	TCP	任意	任意	皆可	拒絕
F	皆可	任意	任意	UDP	任意	任意	皆可	拒絕

如果欲增加內部電腦可以利用 Trap 命令與外部電腦(138.45.6.32)通訊，可再加入 Trap 的相關規則，這留給讀者自行練習，作者不再贅言。

10-8 IP/ICMP 封包過濾

10-8-1 ICMP 過濾訊息

攻擊者最喜歡利用 ICMP 封包來探測網路的狀態；相對的，防火牆必須針對 ICMP 封包做特殊處理，才可達到隱藏內部網路狀態的目的。一般來講，ICMP 訊息並不一定

Google 翻轉工作室：粘添壽

要通過防火牆，只要由防火牆回應 ICMP 的訊息中，也可以瞭解內部網路的狀態。因此，封包過濾器收到 ICMP 封包後，除了必須判斷是否給予通過之外，還必須考慮是否可以給予回覆 ICMP 訊息。IP/ICMP 封包過濾可供判斷的訊息如下:(如圖 10-15 所示)

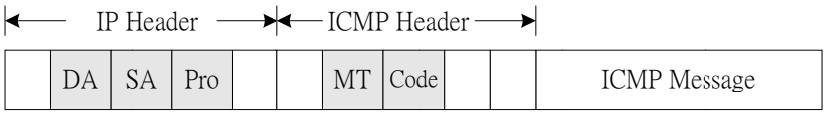


圖 10-15 IP/ICMP 封包過濾訊息

1. 來源位址 (SA): 封包的來源位址。
2. 目的位址 (DA): 封包的目的位址。
3. 協定型態 (Protocol, Pro): ICMP 型態。
4. 訊息型態 (Message Type, MT): 表示此 ICMP 訊息的控制型態，計有 13 種。
5. 編碼 (Code): 各種訊息型態中的次型態。

10-8-2 ping 封包過濾範例

ping 命令是測試網路連結狀態的最佳利器，也是入侵者所喜歡用來探測內部網路情況；因此，一般防火牆都會限制 ping 封包的進出。我們用圖 13-16 來說明 ping 命令的運作程序；ping 命令是利用 ICMP Echo Request 封包 (Echo 請求) 來探測網路，當目的主機 (或路由器) 收到該封包後，立即以 ICMP Echo Response (Echo 回應) 給原發送端，ICMP Echo Request 的訊息型態為 0 (MT = 0)，又 ICMP Echo Response 為 8 (MT = 8)。接下來，我們將 ping 命令可能產生的封包歸類如表 13-10 所示 (進出防火牆)。

表 10-10 ping 命令封包訊息表

編號	封包方向	來源位址	目的位址	協定型態	訊息型態	封包功能
1	進入	外部	內部	ICMP	8	外部進入的 ping 命令封包。
2	出去	內部	外部	ICMP	0	內部主機回應外部 ping 命

						令的封包。
3	出去	內部	外部	ICMP	8	內部主機向外部網路 ping 的命令封包。
4	進入	外部	內部	ICMP	0	外部主機回應內部 ping 的命令封包。

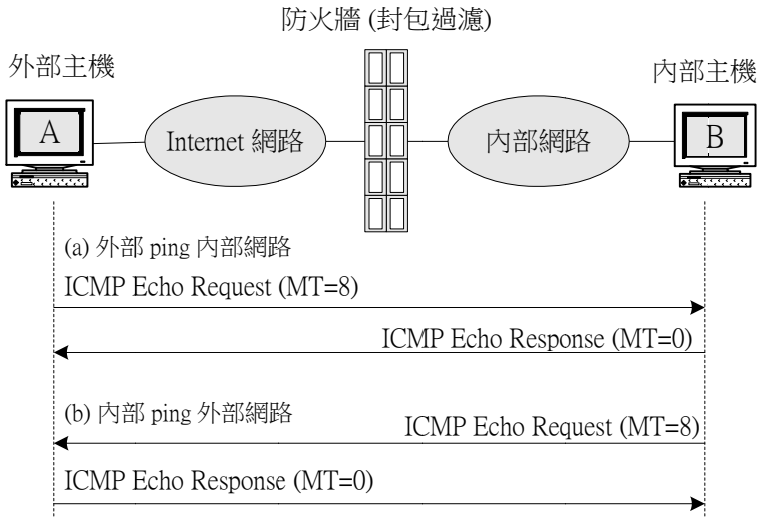


圖 10-16 ping 封包過濾範例

如果將防火牆設定成內部主機可以用 ping 來測試外部網路，但外部主機不可以用 ping 測試內部網路，設定過濾規則如表 10-11 所示。

表 10-11 ping 命令封包過濾規則

規則	封包方向	來源位址	目的位址	協定	訊息型態	措施
A	出去	內部	任意	ICMP	0	允許
B	進入	任意	外部	ICMP	8	允許
C	皆可	任意	任意	ICMP	任意	拒絕

10-8-3 traceroute 封包過濾範例

另一個重要的管理命令是 traceroute，當我們希望瞭解封包到達目的地的路徑時，就必須利用 traceroute 來追蹤封包所經過的路徑。入侵者常利用 traceroute 探測內部網路的架構，防火牆也大多會阻止 traceroute 封包進入內部網路，以達到隱密性的要

求。

traceroute 是使用 ICMP 及 IP 標頭裡的 TTL (Time-to-Live) 欄位，作為判斷已經追蹤過多少個網路端點 (路由器)。一般情況下，封包每經過一個網路閘門 TTL 值就被減 1，如果路由器收到一個 TTL 值減 1 以後為 0 時，便會回送一個 ICMP Time Exceeded (Type 11) (逾時) 給原發送端，並將該封包丟棄，traceroute 就是利用這種特性來追蹤路徑。它的運作情況如下：首先 traceroute 送出一個 TTL 為 1 的 IP 封包到目的主機，第一個收到的路由器將 TTL 減 1，丟棄該封包，並回送 ICMP 給原發送主機，這個過程確認了這條路徑的第一個路由器；接下來，traceroute 再送 TTL 為 2 的 IP 封包，又可以得到第二個路由器位址，如此重覆一直到封包到達目的主機為止。但當封包到達目的位址時，它的 TTL 同樣被減成 0，也回應 ICMP Time Exceeded 封包，發送端如何判斷封包已到達目的與否？

因為 traceroute 是以 UDP 封包格式發送，我們只要將 UDP 埠口設定在不可能使用的埠口，一般都會將它設定較大的值，通常是在 33434 到 33523 之間任一個即可。當目的主機收到後，判斷是自己的 IP 位址，但無此埠口服務，便會回應一個 ICMP Port Unreachable(埠口無法到達)給發送端。發送端就可利用『ICMP 埠口無法到達』和『ICMP 逾時』來判斷是否到達目的主機。一般封包的 TTL 欄位預設值為 255 (如 ping)，這可能造成 traceroute 的封包在網路上無窮的回繞，因此，traceroute 的 TTL 預設值為 30，表示最高可以追蹤 30 個經過的網路閘門，但可以設定改變其大小。

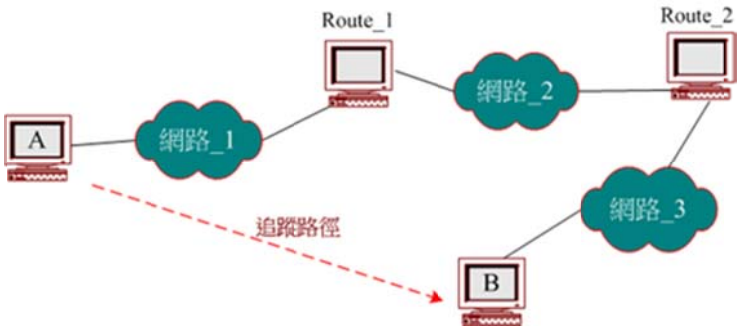


圖 10-17 traceroute 運作原理

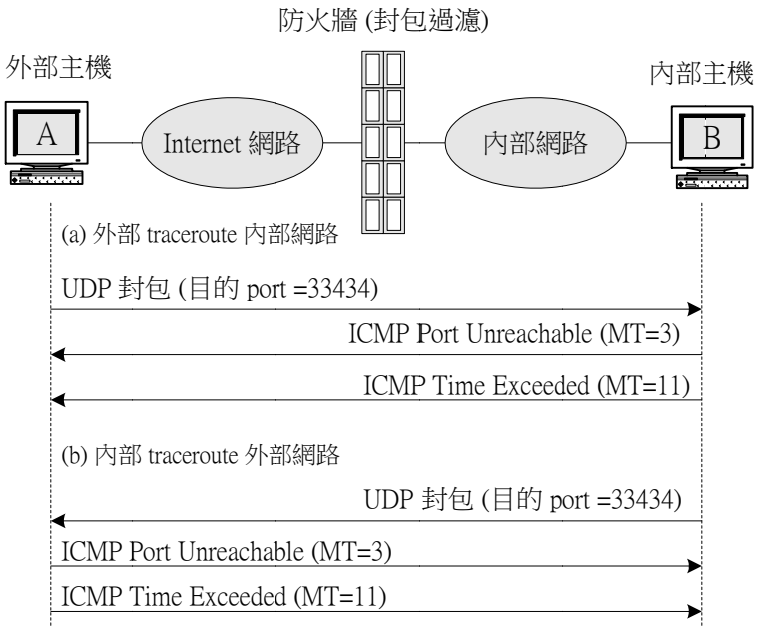


圖 10-17-1 traceroute 封包過濾範例

圖 10-17 為 traceroute 封包過濾範例，它可能通過防火牆的封包如表 10-12 所示。

表 10-12 traceroute 命令封包訊息表

編號	封包方向	來源位址	目的位址	協定型態	來源埠口	目的埠口	訊息型態	封包功能
1	進入	外部	內部	UDP	>1024	33434 ~ 33523		外部進入 traceroute 的 UDP 封包。
2	出去	內部	外部	ICMP			3	內部主機回應外部 UDP 封包的 ICMP Port Unreachable 封包。
3	出去	內部	外部	ICMP			11	內部主機回應外部 UDP 封包的 ICMP Time Exceeded 封包。
4	出去	外部	內部	UDP	>1024	33434 ~33523		內部主機向外部網路 traceroute 所送出的 UDP 封包。
5	進入	內部	外部	ICMP			3	外部主機回應內部 UDP 封包的 ICMP Port Unreachable 封包。

6	進入	外部	內部	ICMP			11	外部主機回應內部 UDP 封包的 ICMP Time Exceeded 封包。

如將圖 10-16 防火牆設定成允許內部主機以 traceroute 去追蹤外部網路，也就是說，允許內部主機的 traceroute 命令通過防火牆；但另一方面，不允許外部網路以 traceroute 命令來測試內部網路，則封包過濾規則如表 10-13 所示。

表 10-13 traceroute 命令封包過濾規則

規則	封包方向	來源位址	目的位址	協定	來源埠口	目的埠口	訊息型態	措施
A	出去	內部	外部	UDP	>1024	33434 ~33523	Null	允許
B	進入	外部	內部	ICMP	Null	Null	3	允許
C	進入	外部	內部	ICMP	Null	Null	11	允許
D	任意	任意	任意	ICMP	Null	Null	任意	拒絕

由上述表格可以發現，為了開放 tranceroute 命令，我們幾乎允許所有 UDP 封包通過防火牆到達外部網路；開放了這一條規則，可能會影響到其他連線的限制，這便是設定封包過濾規則的風險所在。

10-9 代理系統

10-9-1 代理系統簡介

早期『代理系統』(Proxy) 的使用主要為了提高網路傳輸效應，將較常被連結之網頁儲存於『代理伺服器』(Proxy Server) 上，以備其他使用者瀏覽相同網頁時，直接回應給它，以減少網路傳輸的機會。在 Internet 網路未進入電子商務領域之前，代理系統的確在這方面扮演極重要的角色。但近年來，代理伺服器僅為了提高傳輸速率已漸不符環境所需，其主要原因有三：(1) 網路傳輸速率已經提高了許多，客戶端漸漸不需要仰賴代理伺服器來抓取網頁；(2) 電子商務上網路更新非常快速，代理伺服器上的快取網頁可能已經過時；(3) 目前網頁上大多有動態伺服的功能 (譬如，Active X、ASP)，無論是否經過代理伺服器轉接，都需要再連結原伺服器端，來做動態伺服的處理。

然而電子商務的風行，各公司行號都期望建立一個固若金湯的防火牆，代理伺服器的轉接功能，剛好能符合防火牆的需求，於是代理系統又熱絡起來。利用代理系統來建設防火牆，又稱為『代理防火牆』(Proxy Firewall)，其安全性功能如下：

- 隱藏內部網路：無論內部使用者存取外部網路上的伺服器(如 HTTP、FTP、SMTP)，或外部使用者存取內部伺服器都透過代理伺服器轉接，如此外部網路就不易窺視內部網路架構，便可達到隱藏內部網路的功能。
- 網址阻隔：在代理伺服器上可登錄某些網址，當內部使用者欲透過代理伺服器存取這些網址的資料時，代理伺服器可過濾並拒絕服務，如此便可限制內部使用者通往外部網路的範圍。
- 內容過濾：代理伺服器可依照網頁的內容來過濾拒絕轉送不良網頁，譬如色情圖片、或損傷本公司的文件、甚至病毒網頁。
- 路由阻絕：透過代理伺服器轉送，完全不需要路由選擇，甚至可以將主機 (安裝代理伺服軟體) 上的路由選擇功能關閉，因此，外部使用者完全無法透過此主機到達內部網路。
- 登錄與稽核：所有網頁 (或傳輸資料) 都必須經過代理伺服器轉送，很自然的，可以在代理伺服器上登錄哪些使用者存取何種網頁(或資料)，並可經過統計與分析，趁早揪出內部破壞者或外部入侵者的動向。

以上所介紹是代理伺服器扮演防火牆可以提供哪些安全性的功能，接下來介紹代理伺服器的種類，以及其運作原理。如果以使用者 (外部或內部) 進出防火牆的方向來觀察，代理伺服器可區分為『聯外代理伺服』與『轉向代理伺服』兩種，以下分述之。

10-9-2 聯外代理伺服

所謂『聯外代理伺服』，係指內部網路透過代理系統轉接到外部伺服器，如圖 10-18 所示。我們以網頁伺服器為範例，當內部使用者欲抓取外部伺服器之網頁時，首先將連結到代理伺服器上 (訊號 (1))，代理伺服器檢視網頁位址 (一般都檢視 IP 位址) 是否允許存取，再稽核使用者存取權限及存取時間，如果允許存取該網頁，則代理伺服器搜尋快取伺服器是否有該網頁，如果有便直接將網頁傳送給使用者 (訊號 (1-1))；如果快

Google 翻轉工作室：粘添壽

取伺服器上沒有備存網頁，則代理伺服器便發送存取命令向外部伺服器抓取(訊號 (2))。接著，外部伺服器將網頁傳送給代理伺服器，首先代理伺服器檢視網頁內容是否有違反安全政策 (譬如色情網頁或不雅圖片)，如果違反安全政策便丟棄該網頁而不轉送給使用者；如果沒有，便將其儲存於快取伺服器上，並轉送給客戶端。

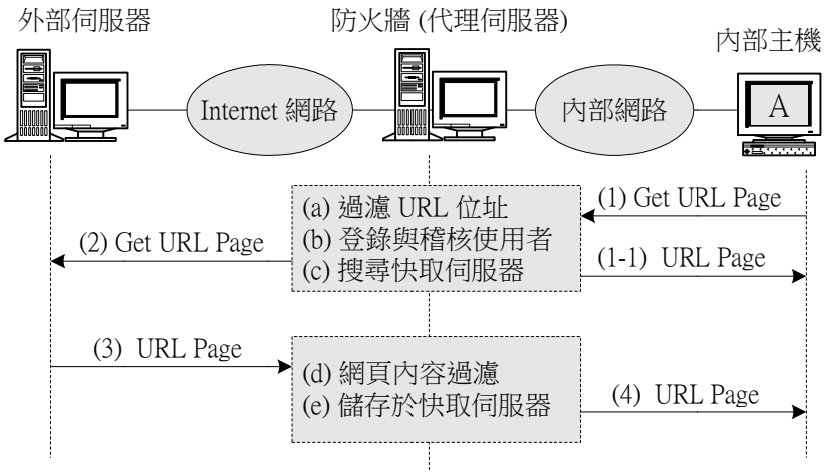


圖 10-18 聯外代理伺服器

10-9-3 轉向代理伺服

當外部使用者欲存取內部伺服器時，可經由『轉向代理伺服』轉送到適當的伺服器上。內部網路只公佈轉向代理伺服器的位址，由外部網路來看，根本不曉得真正伺服器的所在位址，所有存取內部網路資源都需要經由代理伺服器轉送，這個行為又稱為『打洞』，而代理伺服器都安裝在『防禦主機』上。圖 10-19 為轉向代理伺服器的運作程序，它的運作程序和聯外代理伺服器大同小異，祇不過方向相反而已。

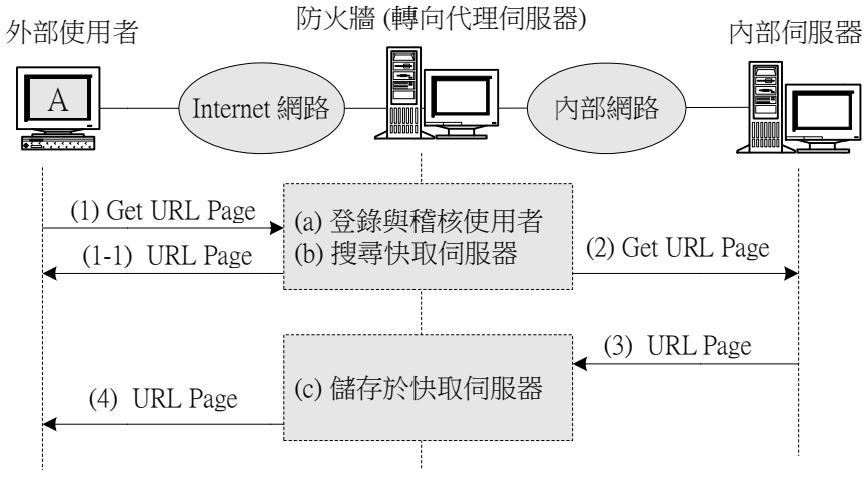


圖 10-19 轉向代理伺服器

轉向代理伺服器在使用者稽核方面要比聯外代理伺服器不容易達成，聯外代理伺服器對認證使用者身份大多可以仰賴內部的網路作業系統(如 Windows 2000)來達成，但轉向代理的使用者可能來自 Internet 網路的任何角落，因此，對使用者的認證問題就需要一個共通的協定來達成。目前 Internet 網路上最普遍的認證協定是 Kerberos 認證協定，也有許多防火牆採用此協定來實現，譬如 ISA Server 或 SOCKS 5。由另一角度來看，轉向代理也是『私有虛擬網路』(VPN) 的最佳利器，遠端使用者可以經由認證程序來存取內部網路，如果再附加資料加密的功能，不失為一個很好的防範措施。

圖 10-20 為轉向代理的防火牆架構，一般在防禦主機上安裝有轉向代理程式，並公佈它的傳輸埠口 (一般都使用著名埠口)，對外界網路而言，防禦主機上的埠口便是伺服器的所在位址，而防禦主機將所收到的資源請求命令 (如 HTTP、FTP、SMTP)，再將其轉送到內部網路的伺服器位址上，如此便可以完全隱藏內部網路。

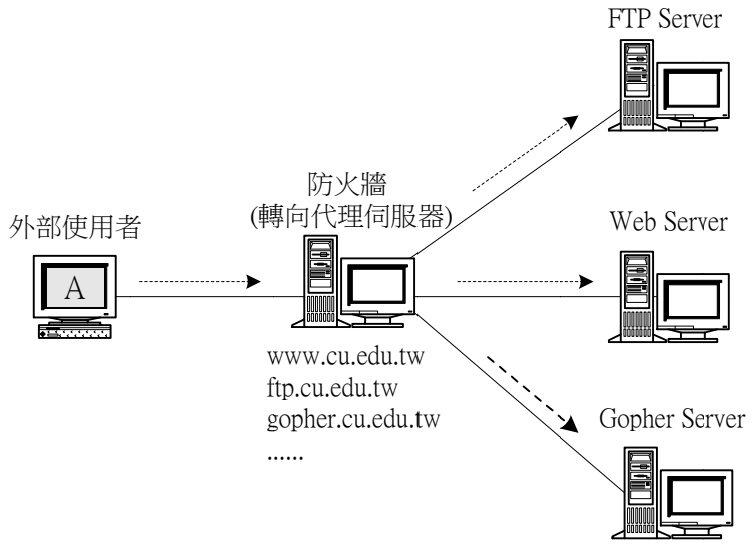


圖 10-20 轉向代理的防火牆功能

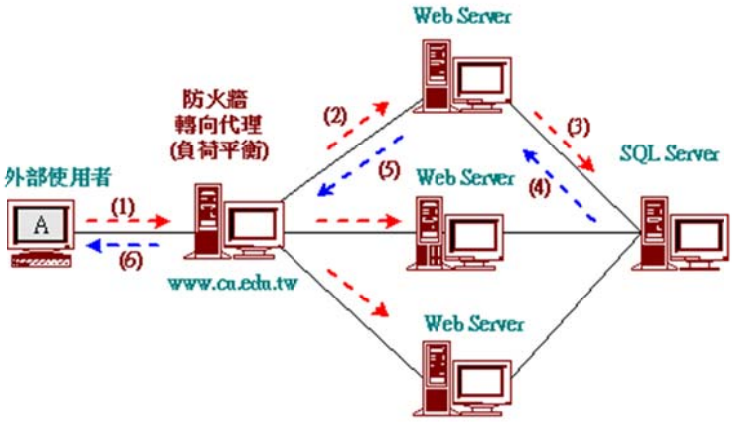


圖 10-20-1 負載平衡

10-10 網路位址轉譯

『網路位址轉譯』(Network Address Translator, NAT) 是屬於防火牆的一種設施，它主要的功能是做內部網路位址和外部網路位址之間的轉譯，一般企業將它作為合法 IP 位址和私有位址之間的轉譯功能。目前 IP 位址漸漸不足，因此對外網路位址不可能分配太多，便利用 NAT 來建構私有網路空間。一般 ISP 公司為了克服 IP 位址不足的問題，都給予客戶動態 IP 位址，我們也可以透過 NAT 將動態 IP 轉譯成私有網路空間。

NAT 的基本原理是多個連線共用一個 IP 位址來往外傳送封包，既然我們瞭解 IP 連線是由『IP 位址 + TCP 傳輸埠口』所構成，因此對內的每一個 IP 位址對應到一個 IP 連線 (IP + TCP Port)，並且在主機內維護一只對照表，便可達到 NAT 的功能。我們用圖 10-24 來說明 NAT 的運作程序，其中主機 A 作為 NAT 主機，外部網路位址是 168.15.0.50，而轉譯內部網路 165.15.2.0/24，NAT 主機的內部位址是 165.15.2.62。假設內部主機 B(165.15.3.30)連結到外部主機 M(147.15.3.12)的 Telnet Server(Port 23)；另外主機 C (165.15.2.34) 連結到 Web Server (180.3.2.67:80)。我們來觀察主機 B 連線的轉譯運作，首先主機 B 連結 (165.15.2.30:4520) 到 NAT 主機上的某一傳輸埠口 (165.15.2.62:1458)，並將其填入內部對照表，由 NAT 主機的內部位址 (165.15.2.62:1458)轉換到外部位址(168.15.0.50:3045)，也將其填入 NAT 轉譯表內。再由 NAT 主機要求連線到主機 M 的 Web Server，連線成功後將其填入外部對照表。

因此由主機 B 到主機 M 之間的連線，就利用 NAT 主機內三個對照表建立而成，如果由主機 M 下載資料到主機 B 之間連線運作就經由： 147.15.3.12:23 到 168.15.0.50:3045，再轉送到 165.15.2.62:1458，最後再轉送到 165.15.2.30:4520。同樣的道理，上傳資料也是經由這條連線傳送。對外部網路而言，連線是經由 168.15.0.50 的位址通訊，外部網路無法知道內部網路的 IP 位址，如此便可達到內部網路主機的隱密性，因此，也稱之為『IP 偽裝』(IP Masquerade)。主機 C 連結到主機 K 的運作程序亦相同，不再另述。

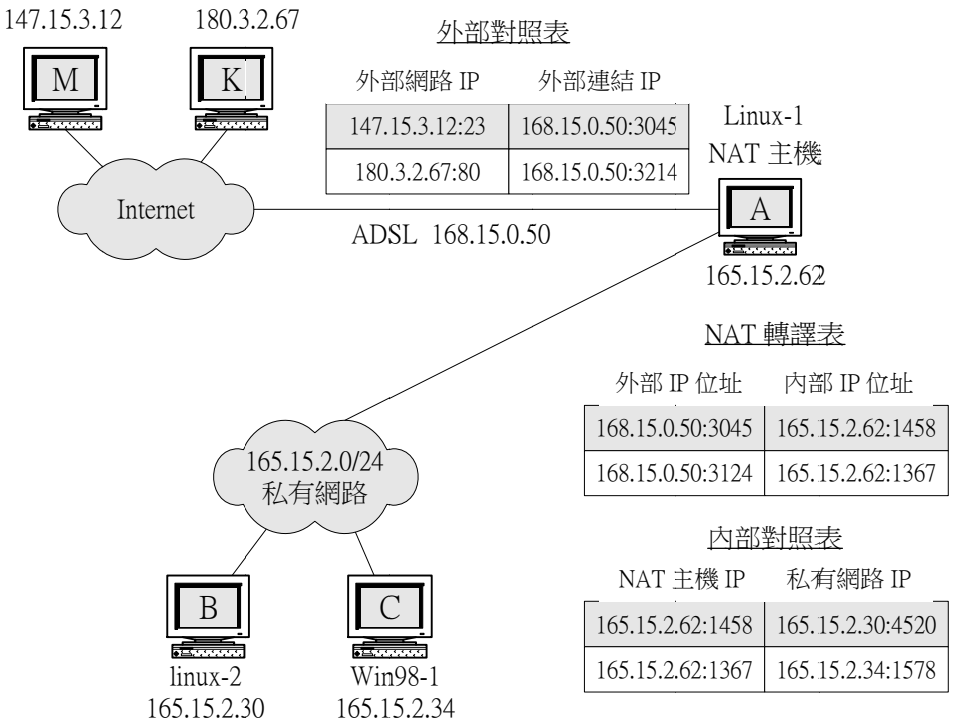


圖 10-24 NAT 運作原理

當內部網路位址透過 NAT 轉換之後，內部網路位址有可能流露於外，一般為了分辨是合法位址或內部虛擬位址，都將私有位址的範圍設定在：(RFC 1918)

- Class A：10.0.0.0 ~ 10.255.255.255，IP Mask：255.0.0.0。
- Class B：172.16.0.0 ~ 172.31.255.255，IP Mask：255.240.0.0。
- Class C：192.168.0.0 ~ 192.168.255.255，IP Mask：255.255.255.0。

當外部路由器接收到一個目的位址為上述範圍內的封包，便將它拋棄不予轉送。