第九章 防火牆規劃與管理

9-1 網路安全簡介

9-1-1 私有網路安全建置

『**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 9-1 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。

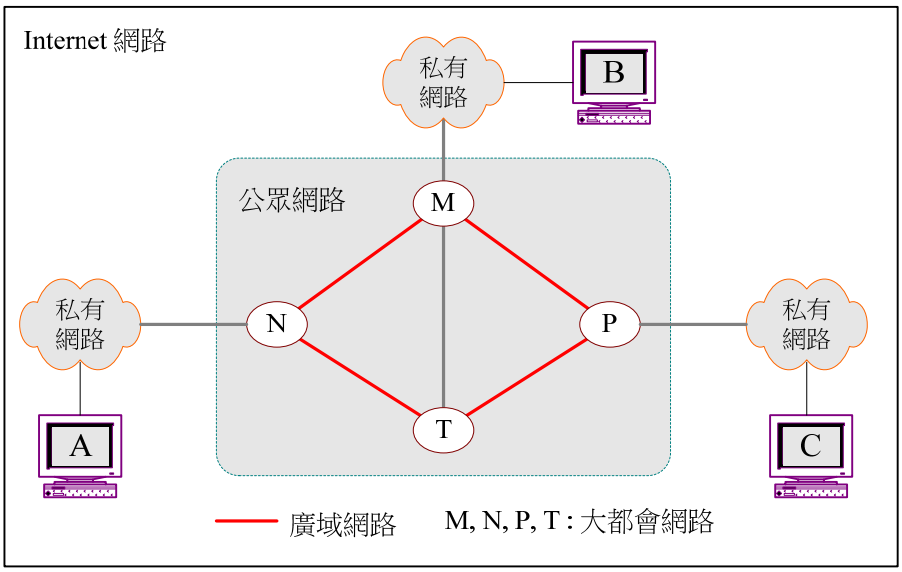

圖 9-1 私有網路與公眾網路

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；後者須建立一套**『虛擬私有網路』(Virtual Private Network, VPN)**，本章與下一章將分別介紹其網路規劃與建置。

9-1-2 防火牆簡介

(A) 何謂防火牆

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。

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。

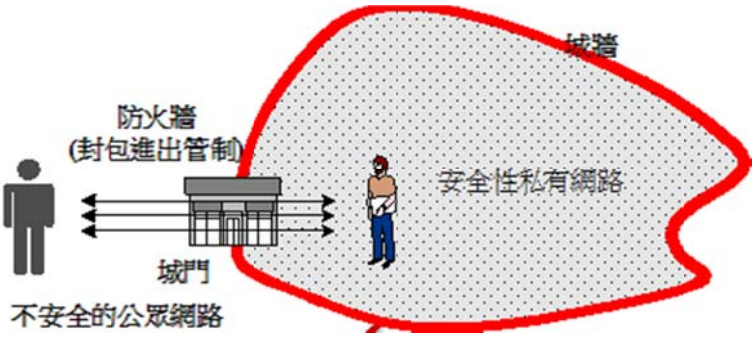

圖 9-2 防火牆的功能

(B) 防火牆措施

為了管制封包進出，一般建構防火牆有以下三大措施：

1. 『**封包過濾**』**(Packet Filter)**：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**』**(Proxy Firewall)**：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 位址轉譯著重於隱藏內部網路，對於管制封包進出功能還是需仰賴封包過濾器與代理機制，如圖 9-3 所示。

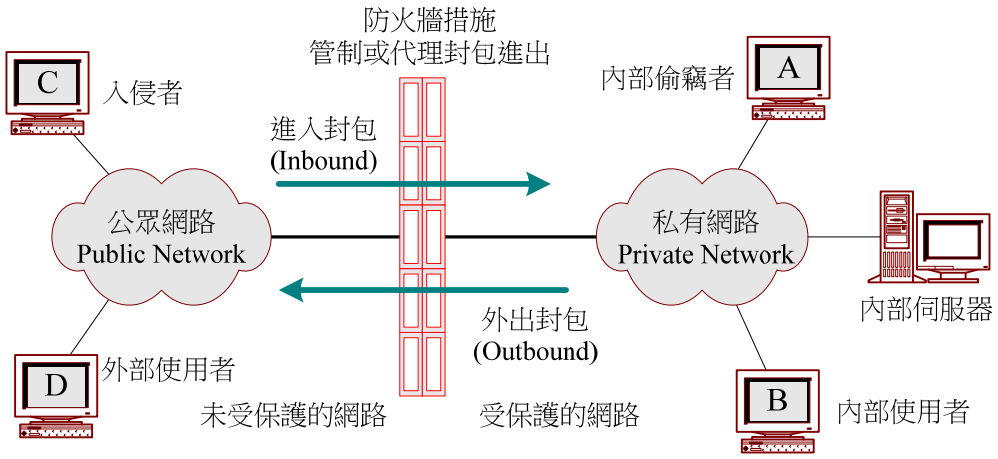

圖 9-3 封包過濾/代理功能

9-2 防火牆架構

9-2-1 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。

- 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。

9-2-2 防火牆架構

(A) 雙介面主機架構

雙介面主機（Dual-homed Host）是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。網路型態如圖 9-4 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**』。

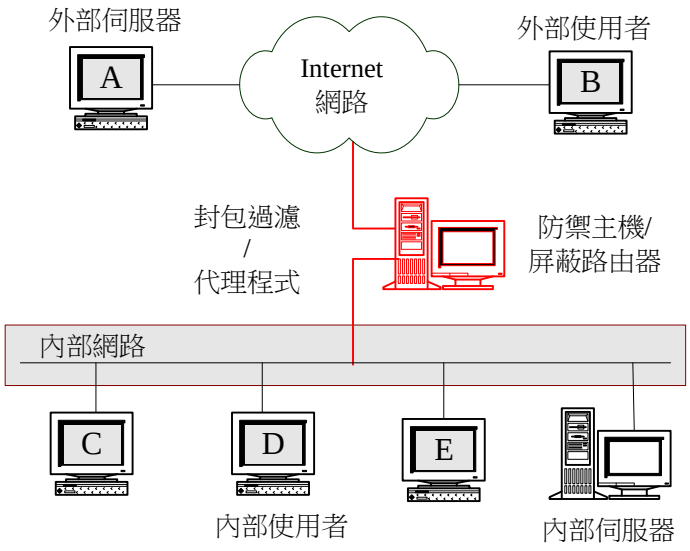

圖 9-4 雙介面主機式架構

(B) 屏蔽主機架構

屏蔽主機架構包含兩樣設施：

- 『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。
- 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。

此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 9-5 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。

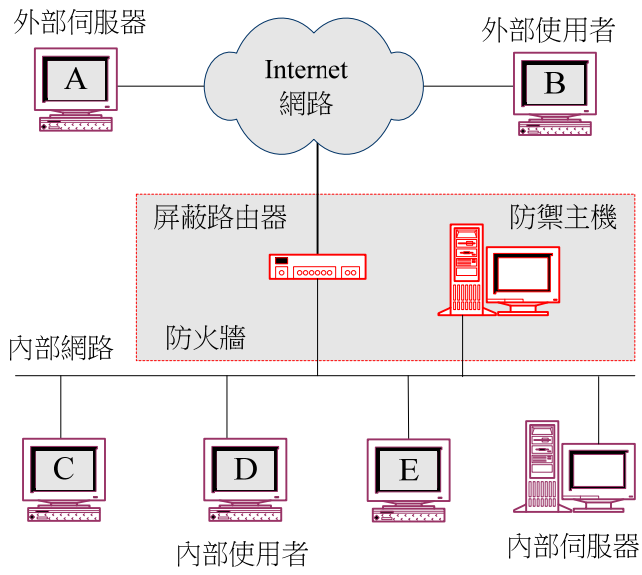

圖 9-5 屏蔽主機架構

(C) 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。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 9-6 所示。

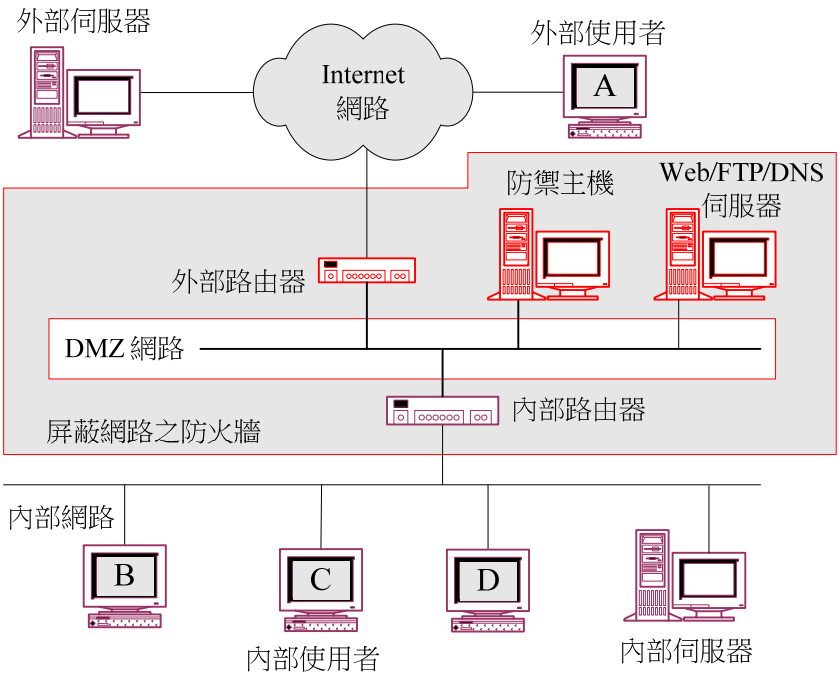

圖 9-6 屏蔽網路架構

9-3 網路位址轉譯

9-3-1 NAT 運作型態

『**網路位址轉譯**』(**Network Address Translator, NAT**)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。

一般吾人將 NAT 網路劃分為兩個區塊：內部(Inside) 與外部(Outside)，Inside 表示網路內使用私有 IP 位址；Outside 網路使用合法 IP 位址。NAT 目的是將 Inside 的

私有位址轉譯到 Outside 的公有位址。Cisco 路由器提供有三種 NAT 運作型態，可分別選擇使用，如下：

(A)『靜態 NAT』(Static NAT)

內部與外部位址是一對一的轉換，因此稱為靜態。這種架構型態完全沒有減少使用合法 IP，完全著重於隱藏內部 IP 的功能，大多應用隱藏內部 IP 位址，但又需要提供資源給外部主機使用的情況。

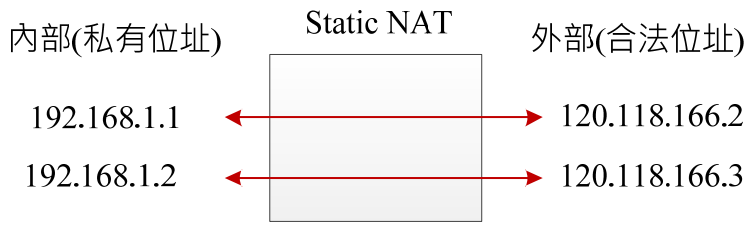

圖 9-7 Static NAT

(B)『動態 NAT』(Dynamic NAT)

內部與外部位址是多對多的關係。此架構在運作當中也是一對一的關係，內部位址對應到外部 IP 隨時改變當中，如此可以減低外部攻擊者探測內部位址的機率。它是將若干個外部 IP 做成一個『群組』(Pool)，並宣告某一網路區段內的主機可由此『群組』索取 IP，使用後立即釋放，又稱**『群組 NAT』(Pooled NAT)**。如圖 9-8 中 10 個合法 IP 被 250 個內部主機輪流使用。

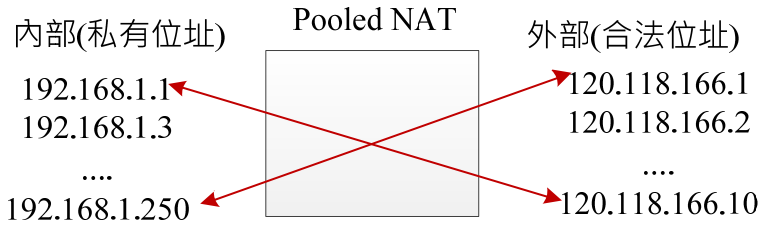

圖 9-8 Dynamic NAT

(C) 『埠口位址轉換 NAT』(Port Address Translation NAT, PAT NAT)

PAT 是利用埠口位址轉換型的 NAT，也是一般坊間常用的 NAT 設定，它內部與外部位址之間是多對一的關係。即是一個合法 IP 位址可以讓多個內部私有位址共用，之間就是利用埠口對應關係建立，即是**『IP 位址 + TCP 埠口』**，如圖 9-9 所示。

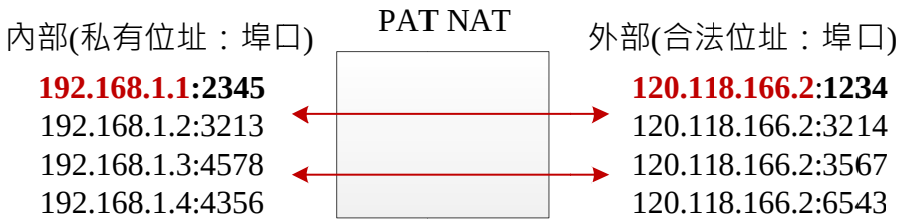

圖 9-9 PAT NAT

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。

一般 ISP 網路收到上述 IP 位址的封包 (無論來源位址或目的位址) 時，便將它拋棄不予轉送。

9-3-2 NAT 防火牆規劃

(請匯入 NAT 防火牆_空白.pkt)

(A) NAT 網路架構

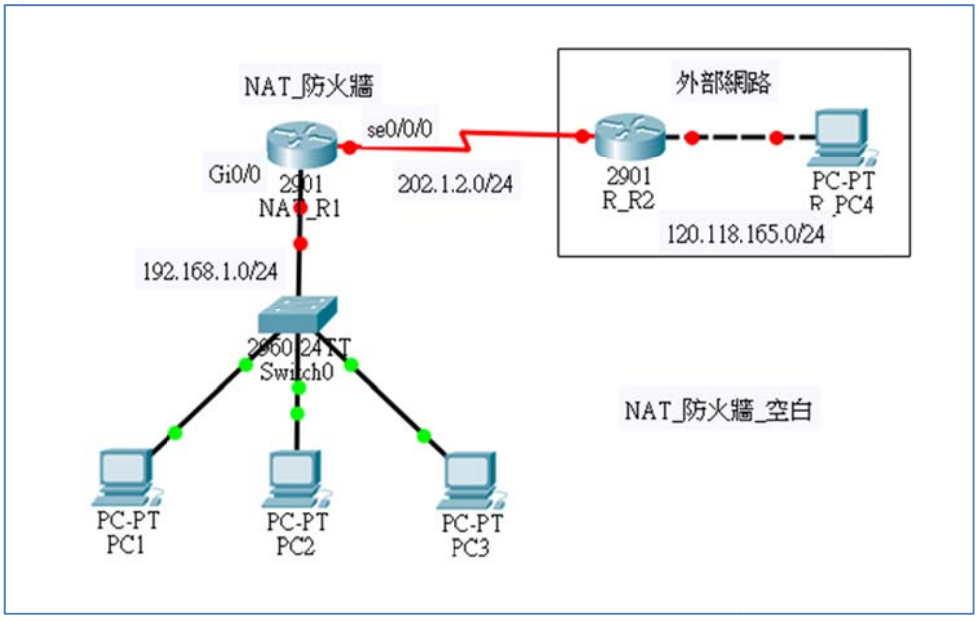

圖 9-10 NAT 防火牆架構

吾人規劃一套 NAT 防火牆架構如圖 9-10 所示，採用設備如下：

- Cisco 路由器 1901: 預設只有兩片 Gigabit Ethernet 介面卡，再增加 WAN Serial 介面卡一只(s0/0/0, s0/01)。取兩台當 NAT 防火牆 (R1) 與外部路由器 (R2)。
- Cisco 交換器 1960 一部、主機 PC 四部。

(B) 網路環境規劃

- 圖 9-10 網路環境的規劃如下：

網路區段	gateway	主機代表	IP 位址	連結介面
192.168.1.0/24	192.168.1.254	PC1	192.168.0.1	SW1(fa0/1)
		PC2	192.168.0.2	SW1(fa0/2)
		HTTP_Server	192.168.0.250	SW1(fa0/3)
120.118.166.0/24	120.118.166.254	R_PC4	192.168.1.1	SW2(fa0/1)

- **路由器規劃**

本網路使用了 2 只路由器，其網路介面卡規劃如下：

Router	Router port	IP 位址	Switch port
NAT_R1	Gi0/0	192.168.1.254	SW1(Gi0/1)
	Se0/0/0	202.1.2.1	R2(S0/0/0)
R_R2	Se0/0/0(DCE)	202.1.2.2	R1(Gi0/0)
	Gi0/0	120.118.166.254	R_PC4

- **RIPv2 規劃**

Router	Network_1	Network_2	Network_3
NAT_R1	192.168.1.0	202.1.2.0	
R_R2	202.1.2.0	120.118.166	

(C) 路由器介面與 RIPv2 設定

- **NAT_R1 設定**：

```
NAT_R1>en
NAT_R1#config ter
NAT_R1(config)#int Gi0/0
NAT_R1(config-if)#ip address 192.168.1.254 255.255.255.0
NAT_R1(config-if)#no shutdown
NAT_R1(config-if)#int s0/0/0
NAT_R1(config-if)#ip address 202.1.2.1 255.255.255.0
NAT_R1(config-if)#bandwidth 10
NAT_R1(config-if)#no shutdown
NAT_R1(config-if)#exit
NAT_R1(config)#ip routing
NAT_R1(config)#router rip
NAT_R1(config-router)#version 2
NAT_R1(config-router)#network 192.168.1.0
NAT_R1(config-router)#network 202.1.2.0
NAT_R1(config-router)#exit
```

- **R_R2 設定：**

```
R_R2>en
R_R2#config ter
R_R2(config)#int s0/0/0
R_R2(config-if)#ip address 202.1.2.2 255.255.255.0
R_R2(config-if)#bandwidth 10
R_R2(config-if)#clock rate 56000
R_R2(config-if)#no shutdown
R_R2(config-if)#int Gi0/0
R_R2(config-if)#ip address 120.118.166.254 255.255.255.0
R_R2(config-if)#no shutdown
R_R2(config-if)#exit
R_R2(config)#ip routing
R_R2(config)#router rip
R_R2(config-router)#version 2
R_R2(config-router)#network 202.1.2.0
R_R2(config-router)#network 120.118.166.0
R_R2(config-router)#exit
```

(C) 網路連線測試：(請匯入 NAT_防火牆_介面設定)

- PC1：ping 120.118.166.1 **[OK]**
- R_PC4：ping 192.168.1.2 **[OK]**

9-3-3 靜態 NAT 設定

(請匯入 NAT 防火牆_介面設定.pkt)

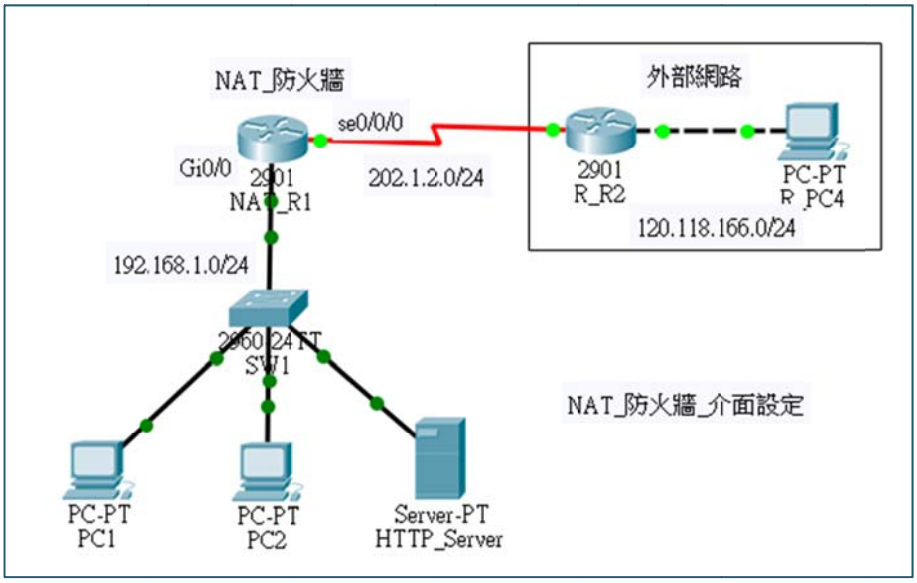

圖 9-11 NAT_防火牆網路_介面設定

『靜態 NAT』(Static NAT)：內部與外部位址是一對一的轉換關係，吾人規劃 NAT 轉換如下：

內部 IP (私有位址)	外部 IP (合法位址)
192.168.1.1	202.1.2.10
192.168.1.2	202.1.2.11
192.168.1.250	202.1.2.12

(A) NAT 設定

- **NAR_R1 設定**：
  - 設定靜態轉換表、
  - 指定 Inside/Outside 介面，如下：

```
NAT_R1>en
NAT_R1#config ter
NAT_R1(config)#ip nat inside source static 192.168.1.1 202.1.2.10
```

```
NAT_R1(config)#ip nat inside source static 192.168.1.2 202.1.2.11
NAT_R1(config)#ip nat inside source static 192.168.1.250 202.1.2.12
NAT_R1(config)#int Gi0/0
NAT_R1(config-if)#ip nat inside
NAT_R1(config-if)#int Se0/0/0
NAT_R1(config-if)#ip nat outside
NAT_R1(config-if)#exit
NAT_R1(config)#do show ip nat translation
  Pro     Inside global     Inside local       Outside local      Outside global
  ---     202.1.2.10        192.168.1.1        ---                ---
  ---     202.1.2.11        192.168.1.2        ---                ---
  ---     202.1.2.12        192.168.1.250      ---                 ---
```

(B) 網路連線測試：(請匯入 NAT_防火牆_static NAT.pkg)

- PC1：ping 120.118.166.1 **[OK]**
- R_PC4：**ping 202.1.2.10** **[OK]**
- R_PC4：**ping 192.168.1.250** **[OK]**
- R_PC4：**http://192.168.1.250** **[NO]**
- R_PC4：**http://202.1.2.12** **[OK]**

(C) 結論 (請自行思考)

- 由外部連線 ping 到內部主機，為何無論採用合法或私有 IP 位址皆可以成功？
- 為何外部電腦利用合法 IP 連線到內部 HTTP_Server 可以成功，但用私有 IP 則無法成功？

9-3-4 動態 NAT 設定

(請匯入 NAT 防火牆_介面設定.pkt)

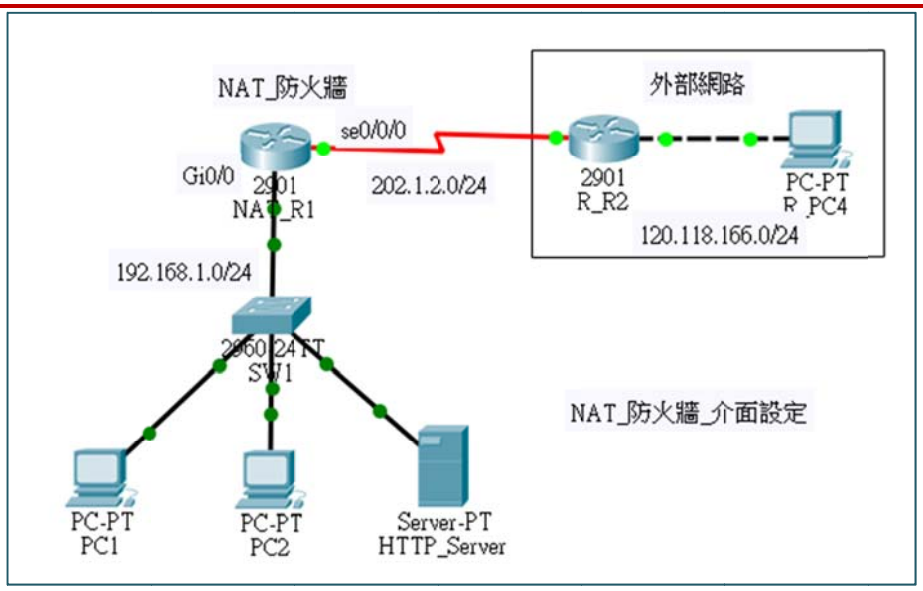

圖 9-11 NAT_防火牆網路_介面設定

『動態 NAT』(Dynamic NAT)內部與外部位址是多對多的關係，但對應之後也是一對一的關係。當內部主機要求向外連線，則路由器分配一只合法 IP，轉換後向外連線，則該 IP 就被占用，當連線終止則再釋放。吾人規劃 Static NAT 與 Dynamic NAT 同時存在，如下：

內部 IP (私有位址)	外部 IP (合法位址)
192.168.1.0/24	202.1.2.10 ~ 19 (動態 NAT)
192.168.1.250	202.1.2.20 (靜態 NAT)

(A) NAT 設定

- **NAR_R1 設定**：
  - 設定內部網路範圍：192.168.1.0/24 (access-list)
  - 設定外部位址槽與分配 IP：pool 名稱為 **nat192**，IP 位址是 202.1.2.10 ~ 202.1.2.19。
  - 指定哪一個 access-list 分配 IP Pool。
  - 指定 Inside/Outside 介面。

```
NAT_R1#config ter
NAT_R1(config)#ip nat inside source static 192.168.1.250 202.1.2.20
NAT_R1(config)#access-list 1 permit 192.168.1.0 0.0.0.255
NAT_R1(config)#ip nat pool nat192 202.1.2.10 202.1.2.19 netmask 255.255.255.0
NAT_R1(config)#ip nat inside source list 1 pool nat192
NAT_R1(config)#int Gi0/0
NAT_R1(config-if)#ip nat inside
NAT_R1(config-if)#int Se0/0/0
NAT_R1(config-if)#ip nat outside
NAT_R1(config-if)#exit
NAT_R1(config)#do show ip nat translation
    Pro  Inside global  Inside local  Outside local  Outside global
    ---  202.1.2.20     192.168.1.250 ---            ---
```

(B) 網路連線測試：(請匯入 NAT_防火牆_Pooled NAT.pkg)

- PC1：ping 120.118.166.1 **[OK]**
- R_PC4：**ping 192.168.1.1** **[OK]**

再觀察 NAT_R1 轉換表如下：

```
NAT_R1(config)#do show ip nat translation
    Pro      Inside global   Inside local    Outside local   Outside global
    Icmp     202.1.2.10:10   192.168.1.1:10  120.118.166.1:10 120.118.166.1:10
    icmp     202.1.2.10:11   192.168.1.1:11  120.118.166.1:11 120.118.166.1:11
    icmp     202.1.2.10:12   192.168.1.1:12  120.118.166.1:12 120.118.166.1:12
    icmp     202.1.2.10:1    192.168.1.1:1   120.118.166.1:1  120.118.166.1:1
    icmp     202.1.2.10:2    192.168.1.1:2   120.118.166.1:2  120.118.166.1:2
    icmp     202.1.2.10:3    192.168.1.1:3   120.118.166.1:3  120.118.166.1:3
    icmp     202.1.2.10:4    192.168.1.1:4   120.118.166.1:4  120.118.166.1:4
    ---      202.1.2.20      192.168.1.250     ---              ---
```

9-3-5 埠口 NAT 設定

(請匯入 NAT 防火牆_介面設定.pkt)

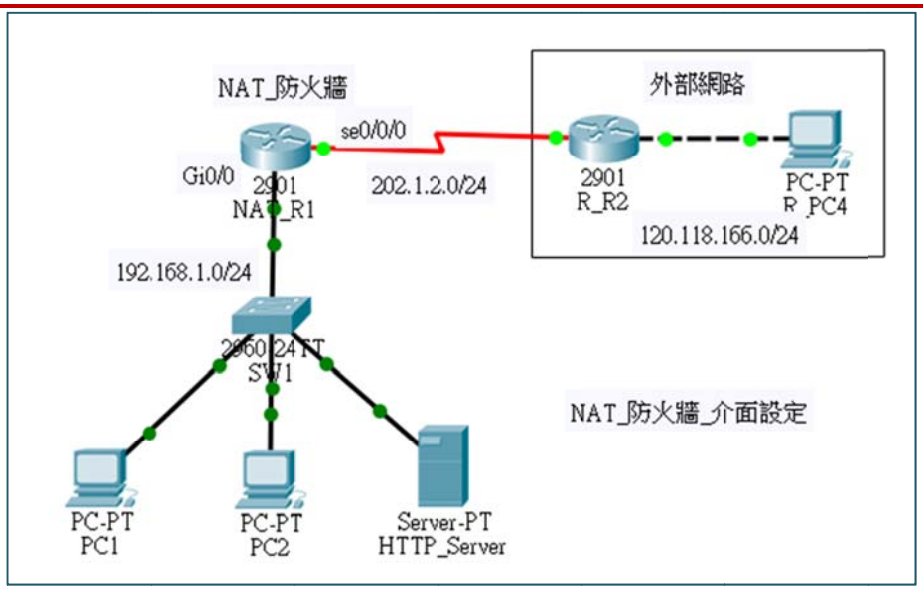

圖 9-11 NAT_防火牆網路_介面設定

『埠口位址轉換 NAT』 (PAT NAT)是利用埠口位址轉換型的 NAT，內部與外部位址之間是多對一的關係。即是一個合法 IP 位址可以讓多個內部私有位址共用。之間就是利用埠口對應關係建立，吾人規劃 NAT 轉換如下：

內部 IP (私有位址)	外部 IP (合法位址)
192.168.1.0/24	202.1.2.10 (PAT NAT)
192.168.1.250	202.1.2.20 (靜態 NAT)

(A) NAT 設定

- **NAR_R1 設定：**
  - 大多與 Dynamic NAT 相同。
  - 僅在指定哪一個 access-list 分配 IP Pool 時加入 Overload，表示一個外部 IP 可以被重複使用。

```
NAT_R1#config ter
NAT_R1(config)#ip nat inside source static 192.168.1.250 202.1.2.20    [Static NAT]
NAT_R1(config)#access-list 1 permit 192.168.1.0 0.0.0.255              [內部 IP 範圍]
NAT_R1(config)#ip nat inside source list 1 pool nat192 overload        [overload]
NAT_R1(config)#ip nat pool nat192 202.1.2.10 202.1.2.10 netmask 255.255.255.0
NAT_R1(config)#int Gi0/0
NAT_R1(config-if)#ip nat inside
```

```
NAT_R1(config-if)#int se0/0/0
NAT_R1(config-if)#ip nat outside
NAT_R1(config-if)#exit
NAT_R1(config)#do show ip nat translation
    Pro   Inside global   Inside local       Outside local      Outside global
    ---   202.1.2.20      192.168.1.250     ---                ---
```

(B) 網路連線測試：(請匯入 NAT_防火牆_Pooled NAT.pkg)

- PC1：ping 120.118.166.1 **[OK]**
- R_PC4：**ping 192.168.1.1** **[OK]**
- 再觀察 NAT_R1 轉換表如下：

```
NAT_R1(config)#do show ip nat translation
    Pro    Inside global    Inside local      Outside local      Outside global
    Icmp   202.1.2.10:10    192.168.1.1:10    120.118.166.1:10   120.118.166.1:10
    icmp   202.1.2.10:11    192.168.1.1:11    120.118.166.1:11   120.118.166.1:11
    icmp   202.1.2.10:12    192.168.1.1:12    120.118.166.1:12   120.118.166.1:12
    icmp   202.1.2.10:9     192.168.1.1:9     120.118.166.1:9    120.118.166.1:9
    ---    202.1.2.20 1     92.168.1.250      ---                ---
```

9-4 封包過濾器

9-4-1 封包過濾原則

『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。

(A) 封包過濾路由器

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. **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。
5. **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。

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。

(B) 服務方向與封包方向

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』**。封包經過有兩個方向：

- **『進入』(Inbound)**：當外部網路使用者欲傳送訊息進入內部網路的封包；
- **『外出』(Outbound)**：由內部使用者送往外部網路的訊息的封包。

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。但產生這兩種封包有兩種**『服務方向』**：

- **『進入』(In)**：外部主機向內部伺服器要求服務。可能會產生 Inbound 與 Outbound 封包。

- 『出去』(Out)：內部主機向外部伺服器要求服務。也會產生 Inbound 與 Outbound 封包。

由此可見，吾人僅管制 Inbound 與 Outbound 封包並無法完全達到目的，還須注意到外出服務或進入服務所產生的封包，如此一來，防火牆的管制就變成非常複雜。

9-4-2 IP 封包過濾

所謂 IP 封包過濾係路由器 (或防禦主機) 只拆解到 IP 協定標頭，其中可供過濾判斷的條件如下：(如圖 9-12 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。

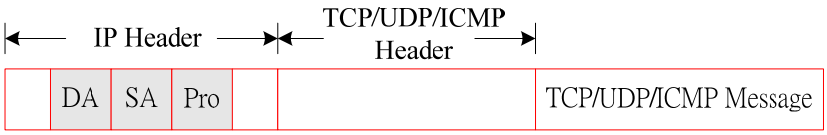

圖 9-12 IP 封包過濾訊息

9-4-3 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 9-13 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。

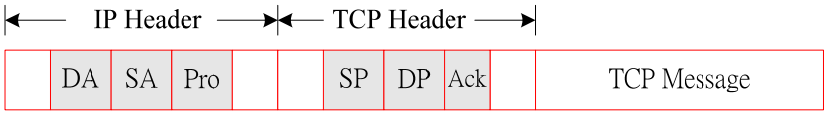

圖 9-13 IP/TCP 過濾封包訊息

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 9-8 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。

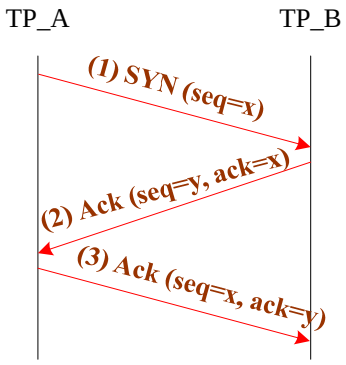

圖 9-14 TCP 三向握手式連絡法

9-4-4 IP/UDP 封包過濾

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 9-15 所示：

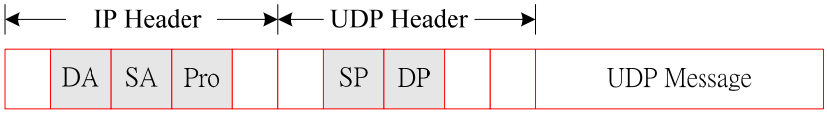

圖 9-15 IP/UDP 封包過濾訊息

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。

9-4-5 IP/ICMP 封包過濾

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 9-16 所示)

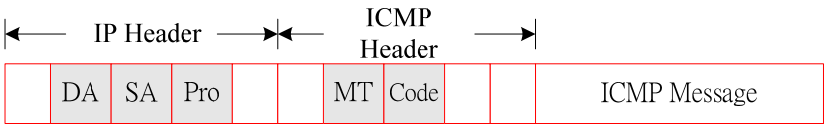

圖 9-16 IP/ICMP 封包過濾訊息

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，如表 9-1 所示。
5. **編碼（Code）**：各種訊息型態中的次型態。

表 9-1 ICMP 訊息型態

Message Type	ICMP 訊息功能
0	Echo Reply（回應答覆）
3	Destination Unreachable（目的地無法到達）
4	Source Quench（來源抑制）
5	Redirect（改變傳輸路徑）
8	Echo Request（回應要求）
9	Router Advertisement（路由器宣傳）
10	Router Solicitation（路由器懇請）
11	Time Exceeded for a Datagram（溢時傳輸）
12	Parameter Problem on a Datagram（參數問題）
13	Timestamp Request（時間標籤要求）
14	Timestamp Reply（時間標籤回覆）
17	Address Mask Request（位址遮罩要求）
18	Address Mask Reply（位址遮罩回覆）

9-5 封包過濾表 – 存取控制清單

9-5-1 ACL 運作模式

(A) 防禦主機與屏蔽路由器

防火牆最普遍的建構是架設封包過濾器，但它過濾的條件應該有許多條件。最簡單的建置是將所需的過濾條件歸納為『**存取控制清單』(Access Control List, ACL)**，Cisco 路由器大多具有此功能，如果管理得妥當，也是一個很理想的防火牆功能。但路由器 ACL 的過濾條件並沒有專屬防火牆那麼強，大多僅能過濾 IP 位址與 TCP/UDP 埠口為主，並無法辨識訊息型號，譬如 TCP 的 SYN 與 ACK 旗標，或 ICMP 訊息等等。雖然利用 ACL 製作的防火牆的功能較低，但是學習防火牆的入門功課，本章就先以 ACL 管理方式，來介紹防火牆的架設方法。

其實，ACL 控制封包進出並非只有路由器，一般伺服主機也大多具有，如果依照 ACL 所安裝的裝置，可區分為：

- **防禦主機：**伺服主機具有 ACL 功能，可過濾封包是否可以存取主機內所安裝的伺服器系統。**(本章有範例製作)**
- **屏蔽路由器：**路由器具有 ACL 功能，可過濾封包是否允許通過路由器，進入或出去內部網路。**(本章有範例製作)**

(B) ACL 運作模式

當封包進入路由器時，會依照 ACL 表內過濾條件逐條列出，比對順序如下：

(1) 由上而下依序比對每筆條件，一直到條件符合為止；

(2) 比對中，如符合條件是『允許』(permit) 表示允許該封包通過，並停止往下比對；

(3) 比對中，如符合條件是『禁止』(deny)，表示禁止該封包通過，並停止往下比對；

(4) 如果都沒有符合，但最後一筆是『 Permit Any』，則該封包允許通過；

(5) 如果都沒有符合，但最後一筆是『Deny Any』，則該封包不允許通過。

9-5-2 ACL 條件與種類

(A) ACL 從嚴或從寬條件敘述

每一個封包進入或出去都會逐條比對存取控制清單，但以上皆非時，最後一筆條件有兩種處理方式：

(1) 從嚴條件：最後一筆如是 Deny any，表示以上條件都不符合，則拒絕通過。

(2) 從寬條件：最後一筆如是 Permit any，表示以上條件都不符合，則允許通過。

(B) Cisco 路由器 ACL 種類

Cisco 路由器的存取控制清單有三種：

(1)『標準存取控制清單』(Standard ACL): 僅檢視 IP 封包中的來源位址(source address)，來決定封包是否允許通過，編號由 1~99, 1300~1999。

(2) 『延伸式存取清單』(Extended ACL)：可比對 IP 封包中的 IP 標頭與上一層(TCP、UDP、、)標頭內的多個欄位，屬於比較進階細膩的過濾條件。編號由 100 ~ 199、2000 ~ 2699。

(3) 『名稱式存取清單』(Named ACL)：是屬於前面兩種存取清單，但僅以名稱命名，也許這樣比較能了解該清單目的與功能。

(C) 存取條件的方向性

每筆存取條件都有其方向性：

(1) 『進入』(Inbound)：如存取清單被宣告成 Inbound，表示是針對進入裝置(路由器)封包的條件過濾。

(2) 『出去』(Outbound)：如存取清單被應用於 Outbound，表示是針對離開裝置(路由器)封包的過濾條件。

9-5-3 ACL 語法

(A) Standard ACL 語法

每筆 ACL 都有編號，由 1 ~ #，其中 1 ~ 99 保留給 Standard ACL 使用，每一個編號表示可以多筆 ACL 紀錄，宣告語法如下：

access-list 1~99 deny | permit host IP_address wildmask

譬如，在路由器的 fa0/1 介面哩，產生一個『進入』(in) 封包的過濾條件是：

- 禁止 192.168.1.1 主機通過、
- 允許 192.168.10.1 主機通過、
- 允許 192.168.2.0/24 網路內主機通過、
- 以上皆非時，進入所有封包通過

吾人將條件歸納於 ACL 10 表內，範例如下：

範例	功能
# access-list 10 deny host 192.168.11.1	禁止 192.168.11.1 主機通過
# access-list 10 permit host 192.168.10.1	允許 192.168.10.1 通過
# access-list 10 permit host 192.168.2.0 0.0.0.255	允許 192.168.2.0/24 主機通過
# access-list 10 deny host any	禁止任何主機通過(從嚴條件)
#int fa0/1 #ip access-group 10 in	在 fa0/1 中啟動 IN 方向的 ACL 10 過濾條件

(B) Extended ACL 語法

Extended ACL 過濾條件包含有 IP 封包標頭外，還可增加 TCP、UDP 或 ICMP 標頭訊息，語法如下：

access-list 100~199 deny|permit ip|TCP|UDP|ICMP host

語法順序如下：

- List-number (100 ~ 199)、
- 阻擋或通過 (Deny 或 Permit)、
- 封包標頭(IP、TCP、UDP、ICMP、、、)、
- 標頭內欄位內容，或服務名稱。

範例如下：

範例	功能
# access-list 101 permit ip any any	允許任何主機通過
# access-list 101 deny ip 192.168.3.4 192.168.4.5	阻擋 192.168.3.4 主機存取 192.168.4.5。
# access-list 101 deny 192.168.2.0 0.0.0.255	阻擋 192.168.2.0/24 主機
# access-list 101 permit tcp host 192.168.3.4 host 192.168.4.5 eq 80	允許 192.168.2.4 存取 192.168.4.5 主機的 tcp 埠口 80。
#int fa0/1 #ip access-group 101 out	在 fa0/1 中啟動 OUT 方向的 ACL 10 過濾條件

(C) Named ACL 語法

Names ACL 過濾條件允許包含 IP、TCP、UDP 或 ICMP 標頭訊息，取一只 ACL 條件名稱，再加入各種條件敘述，語法如下：

 # access-list extended ACL_Name

範例如下：

範例	功能
# ip access-list extended Server-ACL	
# permit tcp host 192.168.12.50 any eq WWW	允許 192.168.12.50 存取 www
# permit tcp host 192.168.12.51 any eq ftp	允許 192.168.12.51 存取 ftp
# deny ip any any	阻擋所有
#int fa0/1 #ip access-group Server-ACL out	嵌入埠口

9-6 具 DNZ 防火牆的私有網路

9-6-1 DNZ 防火牆規劃

(A) 系統分析

(請匯入：防火牆設定_空白.pkt)

吾人期望規劃一套具有 DNZ 防火牆防護的私有網路，並從中學習『防禦主機』、『內部屏蔽路由器』與『外部屏蔽路由器』的架設與管理技巧，網路架構如圖 9-17 所示。防火牆措施採用 ACL 控制方式。

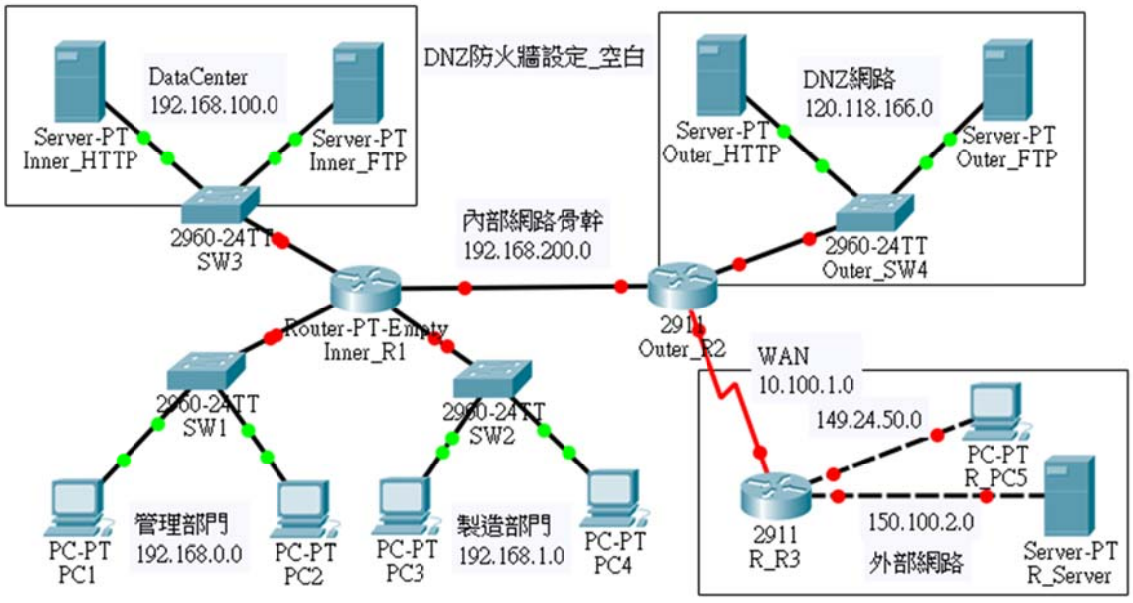

圖 9-17 具 DNZ 防火牆的私有網路

(B) 網路環境規劃

圖 9-17 網路環境的規劃如下：(交換器未使用 VLAN 功能，不需要設定)

網路區段	gateway	路由介面	主機代表	IP 位址	連結介面
192.168.0.0/24	192.168.0.254	R1(Gi0/0)	PC1	192.168.0.1	SW1(fa0/1)
		SW1(Gi0/1)	PC2	192.168.0.2	SW1(fa0/2)
192.168.1.0/24	192.168.1.254	R1(Gi1/0)	PC3	192.168.1.1	SW2(fa0/1)
		SW2(Gi0/1)	PC4	192.168.1.2	SW2(fa0/2)

192.168.100.0/24	192.168.100.254	R1(Gi2/0) SW3(Gi0/1)	Inner_HTTP	192.168.100.1	SW3(fa0/1)
			Inner_FTP	192.168.100.2	SW3(fa0/2)
120.118.166.0/24 DNZ 網路	120.118.166.254	R2(Gi0/1) SW4(Gi0/1)	Outer_HTTP	120.118.166.1	SW4(fa0/1)
			Outer_FTP	120.118.166.2	SW4(fa0/2)
192.168.200.0/24 內部網路骨幹				192.168.200.1	R1(Gi3/0)
				192.168.200.2	R2(Gi0/0)
10.100.1.0/24 WAN 網路			DCE	10.100.1.1	R2(s0/2/0)
			DTE	10.100.1.2	R_R3(s0/2/0)
149.24.50.0/24	149.24.50.254	R_R3(gi0/0)	R_PC5	149.24.50.1	R_R3(gi0/0)
150.100.2.0/24	150.100.2.254	R_R3(gi0/1)	R_Server	150.100.2.1	R_R3(gi0/1)

(C) 路由器規劃

本網路使用了 3 只路由器，其網路介面卡規劃如下：

Router	Router port	IP 位址	Switch port
Inner_R1	Gi0/0	192.168.0.254	SW1(Gi0/1)
	Gi1/0	192.168.1.254	SW2(Gi0/1)
	Gi2/0	192.168.100.254	SWW(Gi0/1)
	Gi3/0	192.168.200.1	R2(Gi0/0)
Outer_R2	Gi0/0	192.168.200.2	R1(Gi3/0)
	Gi0/1	120.118.166.254	SW4(Gi0/1)
	Se0/2/0	10.100.1.1	R3(se0/2/0)
Remote_R3	Se0/2/0	10.100.1.2	R2(se0/2/0)
	Gi0/0	149.24.50.254	R_PC5
	Gi0/1	150.100.2.254	R_Server

9-6-2 DNZ 網路環境設定

(A) 路由器介面設定

Inner_R1 介面設定

```
Inner_R1>en
Inner_R1#config ter
```

```
Inner_R1(config)#int gi0/0
Inner_R1(config-if)#ip address 192.168.0.254 255.255.255.0
Inner_R1(config-if)#no shutdown
Inner_R1(config-if)#int gi1/0
Inner_R1(config-if)#ip address 192.168.1.254 255.255.255.0
Inner_R1(config-if)#no shutdown
Inner_R1(config-if)#int gi2/0
Inner_R1(config-if)#ip address 192.168.100.254 255.255.255.0
Inner_R1(config-if)#no shutdown
Inner_R1(config-if)#int gi3/0
Inner_R1(config-if)#ip address 192.168.200.1 255.255.255.0
Inner_R1(config-if)#no shutdown
Inner_R1(config-if)#exit
Inner_R1(config)#do show ip int brief
      Interface IP-Address OK? Method Status Protocol
      GigabitEthernet0/0 192.168.0.254 YES manual up up
      GigabitEthernet1/0 192.168.1.254 YES manual up up
      GigabitEthernet2/0 192.168.100.254 YES manual up up
      GigabitEthernet3/0 192.168.200.1 YES manual up up
Inner_R1(config)#
```

Outer_R2 介面設定

```
R2>en
R2#config ter
R2(config)#int gi0/0
R2(config-if)#ip address 192.168.200.2 255.255.255.0
R2(config-if)#no shutdown
R2(config-if)#int gi0/1
R2(config-if)#ip address 120.118.166.254 255.255.255.0
R2(config-if)#no shutdown
R2(config-if)#int s0/2/0
R2(config-if)#ip address 10.100.1.1 255.255.255.0
R2(config-if)#bandwidth 10
R2(config-if)#clock rate 56000
R2(config-if)#no shutdown
R2(config-if)#exit
R2(config)#do show ip int brief
      Interface IP-Address OK? Method Status Protocol
      GigabitEthernet0/0 192.168.200.2 YES manual up up
      GigabitEthernet0/1 120.118.166.254 YES manual up up
      GigabitEthernet0/2 unassigned YES manual administratively down down
```

```
Serial0/2/0 10.100.1.1 YES manual up up
Serial0/2/1 unassigned YES unset administratively down down
Vlan1 unassigned YES unset administratively down down
```

R_R3 介面設定

```
R2>
R2>en
R2#config ter
R2(config)#int gi0/0
R2(config-if)#ip address 149.24.50.254 255.255.255.0
R2(config-if)#no shutdown
R2(config)#int gi0/1
R2(config-if)#ip address 150.100.2.254 255.255.255.0
R2(config-if)#no shutdown
R2(config-if)#int s0/2/0
R2(config-if)#ip address 10.100.1.2 255.255.255.0
R2(config-if)#bandwidth 10
R2(config-if)#no shutdown
R2(config-if)#exit
R2(config)#do show ip int brief
      Interface IP-Address OK? Method Status Protocol
      GigabitEthernet0/0 149.24.50.254 YES manual up up
      GigabitEthernet0/1 150.100.2.254 YES manual up up
      GigabitEthernet0/2 unassigned YES manual administratively down down
      Serial0/2/0 10.100.1.2 YES manual up up
      Serial0/2/1 unassigned YES unset administratively down down
      Vlan1 unassigned YES unset administratively down dow
```

(B) 路由器 RIP 動態路由設定

個路由器的相鄰網路(RIP 2 使用)，如下表：

Router	Network_1	Network_2	Network_3	Network_4
Inner_R1	192.168.0.0	192.168.1.0	192.168.100.0	192.168.200.0
Outer_R2	192.168.200.0	120.118.166.0	10.100.1.0	
R_R3	10.100.1.0	149.24.50.0	150.100.2.0	

Inner_R1 RIPv2 設定

```
Inner_R1(config)#route rip
Inner_R1(config-router)#version 2
Inner_R1(config-router)#network 192.168.0.0
Inner_R1(config-router)#network 192.168.1.0
Inner_R1(config-router)#network 192.168.100.0
Inner_R1(config-router)#network 192.168.200.0
Inner_R1(config-router)#exit
Inner_R1(config)#do show ip route
        …
```

Outer_R2 RIPv2 設定

```
R2(config)#route rip
R2(config-router)#version 2
R2(config-router)#network 192.168.200.0
R2(config-router)#network 120.118.166.0
R2(config-router)#network 10.100.1.0
R2(config-router)#exit
R2(config)#do show ip route
        …
```

R_R3 RIPv2 設定

```
R2(config)#route rip
R2(config-router)#version 2
R2(config-router)#network 10.100.1.0
R2(config-router)#network 150.100.2.0
R2(config-router)#network 149.24.50.0
R2(config-router)#exit
R2(config)#do show ip route
        …
```

(C) 網路環境測試

(請匯入：防火牆設定_網路設定.pkt)

由 PC1 (192.168.0.1) 連線測試

```
C:\>ping 192.168.1.1          [OK]
C:\>ping 192.168.100.1        [OK]
C:\>ping 120.118.166.1        [OK]
```

```
C:\>ping 150.100.2.1          [OK]
C:\>ping 149.24.50.1          [OK]
```

由 R_PC5 (149.24.50.1) 連線測試

```
C:\>ping 192.168.0.1          [OK]
C:\>ping 192.168.1.1          [OK]
C:\>ping 192.168.100.1        [OK]
C:\>ping 120.118.166.1        [OK]
```

9-6-3 內部伺服器 ACL 規劃

(請匯入：防火牆設定_網路設定.pkt)

在圖 9-18 私有網路中，有兩個內部伺服器：Inner_HTTP 與 Inner_FTP，是公司內重要資料彙整中心，期望內部資源規劃如下：

系統資源	IP 位址	服務	埠口	允許存取
Inner_HTTP	192.168.100.1	WWW	80/tcp	網路：192.168.0.0 主機：192.168.1.1 (管理者)
		ping	ICMP	主機：192.168.0.1 (管理者)
Inner_FTP	192,168.100.2	FTP	20, 21/tcp	網路：192.168.1.0 主機：192.168.0.1 (管理者)
		ping	ICMP	主機：192.168.1.1 (管理者)

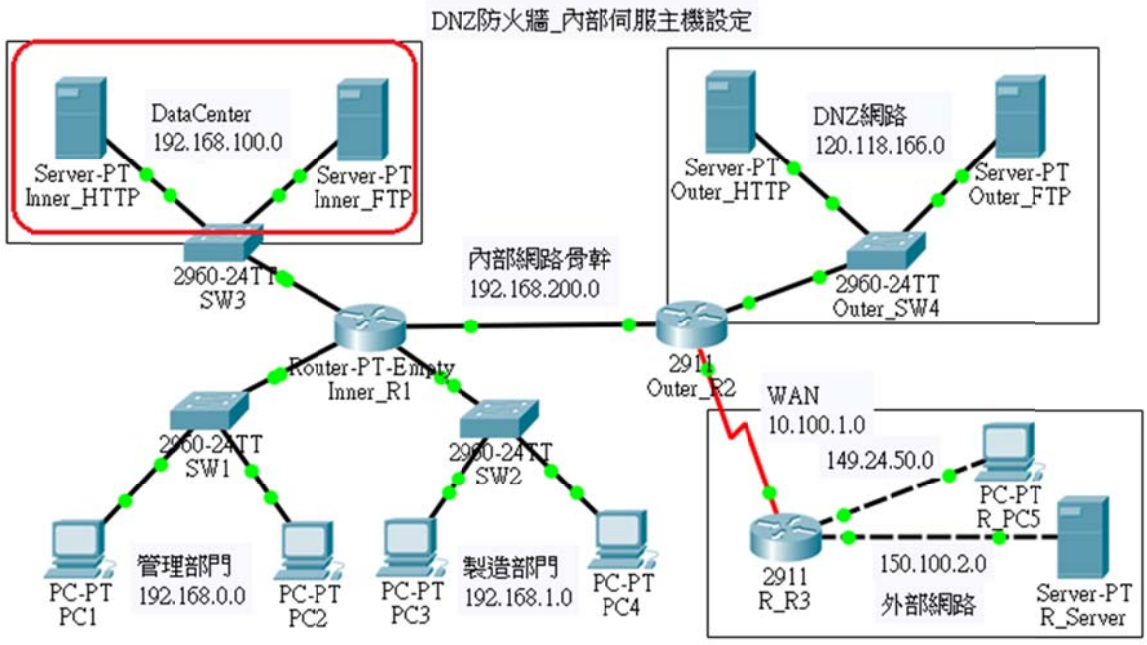

圖 9-18 內部伺服器 ACL 設定

(A) Inner_HTTP 防火牆設定

- 點選 HTTP Server 主機 => Desktiop => Firewall 進入防火牆設定視窗，再輸入 ACL 清單，如下：

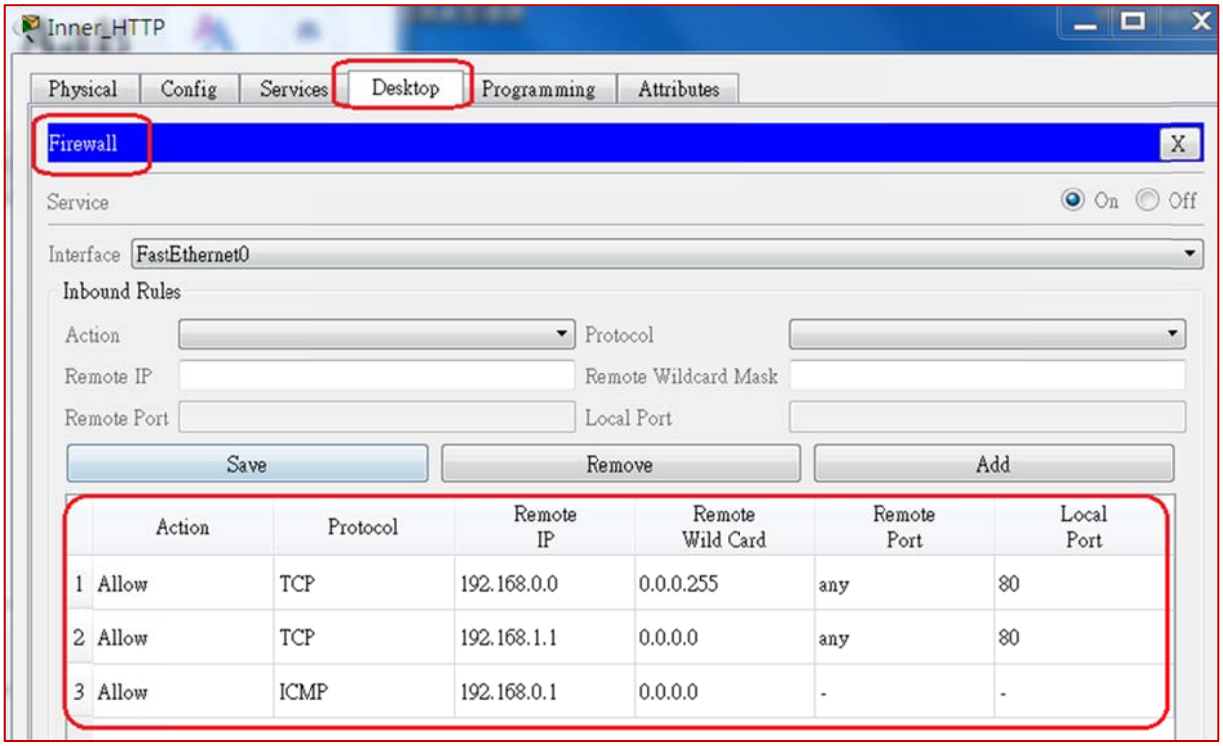

圖 9-18-1

- 測試：

1. 由 PC1(192.168.0.1) => Web Browser 進入：

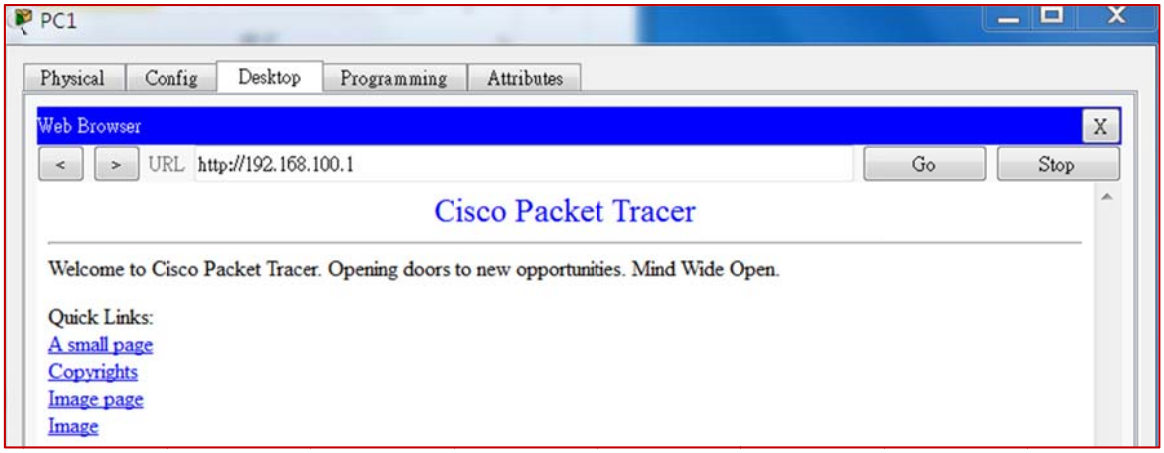

圖 9-18-2

2. 由 PC6(192.168.1.2) 進入 Web Browser：

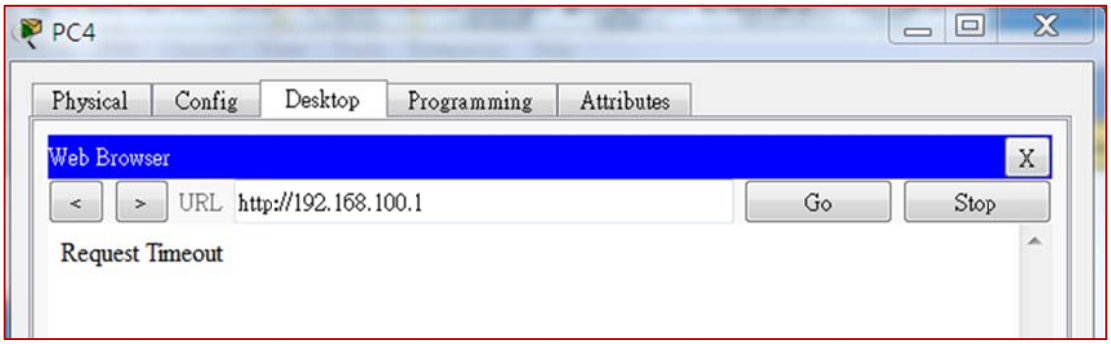

圖 9-18-3

3. 由 PC1(192.168.0.1) 進入 Command Prompt：

```
C:\>ping 192.168.100.1      [OK]
```

4. 由 PC2(192.168.0.2) 進入 Command Prompt：

```
C:\>ping 192.168.102.1      [NO、無法連線]
```

(B) Inner_FTP Server 防火牆設定

- 點選 FTP Server 主機 => Desktiop => Firewall 進入防火牆設定視窗，再輸入 ACL 清單，如下：

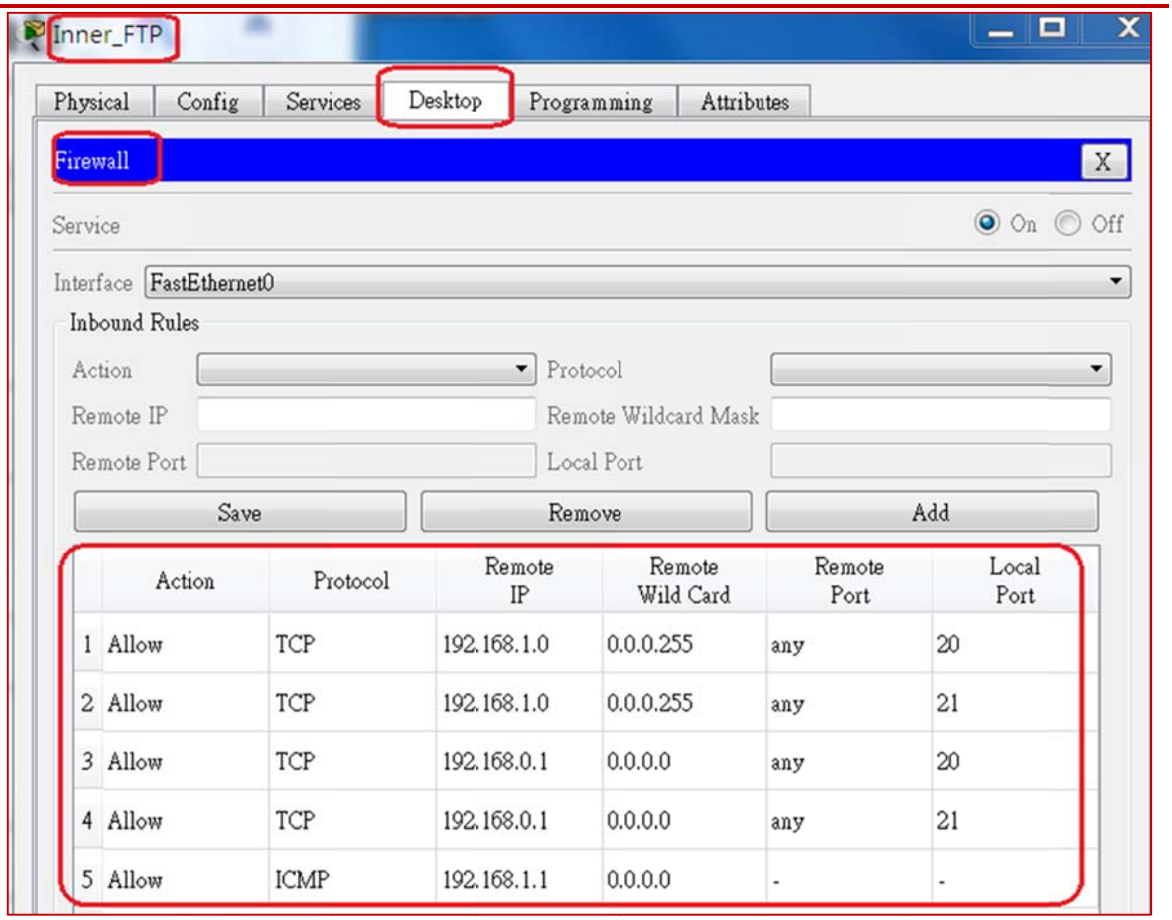

圖 9-18-4

■ 測試：(帳號：cisco、密碼：cisco)

(請匯入：防火牆設定_內部伺服主機設定.pkt)

1. PC3(192.168.1.1) 測試 fpt 連線：

```
C:\>ftp 192.168.100.2
Trying to connect...192.168.100.2
Connected to 192.168.100.2
220- Welcome to PT Ftp server
Username:cisco
331- Username ok, need password
Password:[ cisco]
230- Logged in
(passive mode On)
ftp>
```

2. 測試 fpt 連線：由 PC2(192.168.0.2) 進入 Web Browser：

```
C:\>ftp 192.168.100.2          [NO、無法連線]
```

3. 測試 ping 連線：由 PC3(192.168.1.1) 進入 Command Prompt：

```
C:\>ping 192.168.100.2        [OK]
```

4. 測試 ping 連線：由 PC1(192.168.0.1) 進入 Command Prompt：

```
C:\>ping 192.168.100.2      [NO、無法連線]
```

9-6-4 內部路由器 ACL 規劃

(請匯入：防火牆設定_網路設定.pkt)

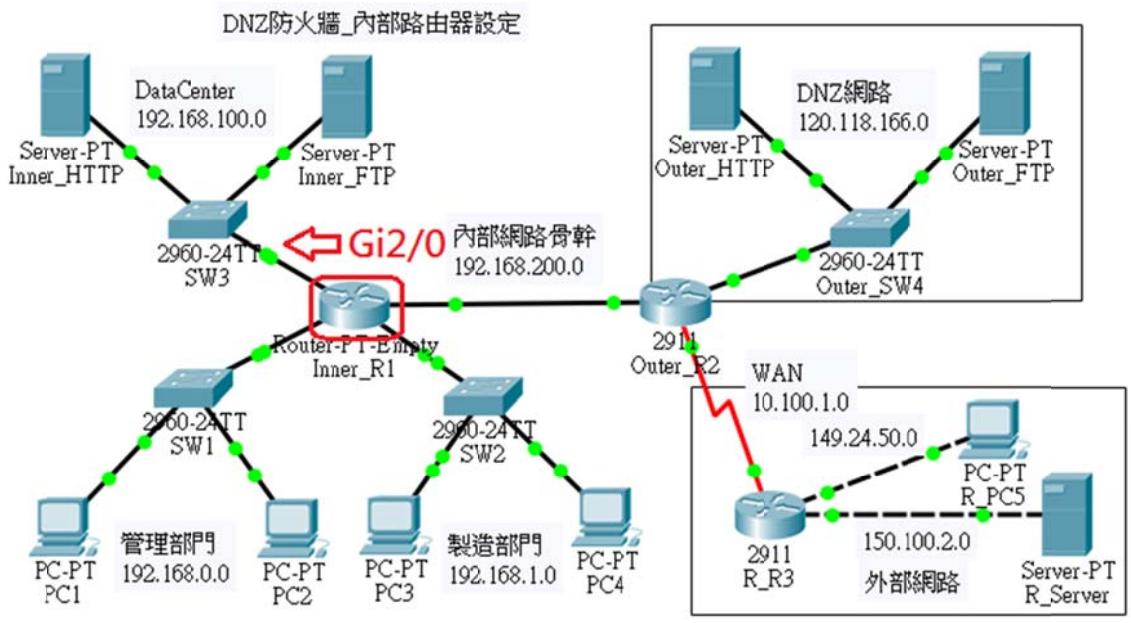

圖 9-19 內部路由器防火牆的 ACL 設定

對伺服器的防護，除了伺服器本身管制封包進出外**(9-6-3 節介紹)**，也可以透過內部路由路設定。吾人可以建立一個資料中心網路 (192.168.100.0/24)，將公司內重要資源皆架設在此網路內，再管制進出此網路的封包即可達到目的。圖 9-19 網路內資料中心網路是透過 Inner_R1 的埠口 Gi2/0 連結，因此，我們只要規劃此埠口的封包管制即可。除此之外，我們也希望建立一個 VTP 遠端連線埠口 (192.168.100.254)，並僅允許管理者 (192.168.0.1 與 192.168.1.1) 主機可以登入操作。

(A) 防火牆規劃：

- 對 Inner-R1 路由器 Gi2/0 (192.168.100.254) 管制內部伺服器的存取限制：

1. 允許來源是 192.168.0.0 網路與 192.168.1.1 主機等封包存取 192.168.100.1:80 (Inner_HTTP: Web Server)。
2. 允許來源是 192.168.1.0 網路與 192.168.0.1 主機等封包存取 192.168.100.2:22, 23 (Inner_FTP: FTP Server)。
3. 允許 192.168.0.1 主機測試(ping) 192.168.100.1。
4. 允許 192.168.1.1 主機測試(ping) 192.168.100.2。

Inner-ACL 條件：內部路由器 **(Gi2/0)** 管制存取資料中心的資源：

Inner_R1**(Gi2/0)** 外部路由器：**Inner-ACL**								
編號	Permit/ deny	封包類型	來源		目的		方向	備註
			IP	port	IP	port		
1	permit	tcp	192.168.0.0/24	any	192.168.100.1	80	out	www
2	permit	tcp	192.168.1.1	any	192.168.100.1	80	out	www
3	permit	icmp-echo	192.168.0.1	any	192.168.100.1		out	ping
4	permit	tcp	192.168.1.0/24	any	192.168.100.2	20, 21	out	ftp
5	permit	tcp	192.168.0.1	any	192.168.100.2	20, 21	out	ftp
6	permit	icmp-echo	192.168.1.1	any	192.168.100.2		out	ping

(B) 設定 Inner-ACL 防火牆規則

由 Inner_R1 路由器上設定：

```
Inner_R1>en
Inner_R1#config ter
Inner_R1(config)#ip access-list extended Inner-ACL
```

```
Inner_R1(config-ext-nacl)#permit tcp 192.168.0.0 0.0.0.255 host 192.168.100.1 eq www
Inner_R1(config-ext-nacl)#permit tcp host 192.168.1.1 host 192.168.100.1 eq www
Inner_R1(config-ext-nacl)#permit icmp host 192.168.0.1 host 192.168.100.1 echo
Inner_R1(config-ext-nacl)#permit tcp 192.168.1.0 0.0.0.255 host 192.168.100.2 eq ftp
Inner_R1(config-ext-nacl)#permit tcp host 192.168.0.1 host 192.168.100.2 eq ftp
Inner_R1(config-ext-nacl)#permit icmp host 192.168.1.1 host 192.168.100.2 echo
Inner_R1(config-ext-nacl)#deny ip any any
Inner_R1(config-ext-nacl)#
```

■ 顯示 Inner-ACL 與嵌入介面(Gi2/0)：

```
Inner_R1(config)#do show access-list Inner-ACL
        Extended IP access list Inner-ACL
        permit tcp 192.168.0.0 0.0.0.255 host 192.168.100.1 eq www
        permit tcp host 192.168.1.1 host 192.168.100.1 eq www
        permit icmp host 192.168.0.1 host 192.168.100.1 echo
        permit tcp 192.168.1.0 0.0.0.255 host 192.168.100.2 eq ftp
        permit tcp host 192.168.0.1 host 192.168.100.2 eq ftp
        permit icmp host 192.168.1.1 host 192.168.100.2 echo
        deny ip any any
Inner_R1(config)#int gi2/0
Inner_R1(config-if)#ip access-group Inner-ACL out
Inner_R1(config-if)#
```

(C) 測試 Inner_HTTP 連線：

(請匯入：防火牆設定_內部路由器設定.pkt)

1. 由 PC1(192.168.0.1) => Web Browser 進入：http://192.168.100.1。**[OK]**
2. 由 PC6(192.168.1.2) 進入 Web Browser：http://192.168.100.1 **[失敗]**
3. 由 PC1(192.168.0.1) 進入 Command Prompt：

```
C:\>ping 192.168.100.1          [OK]
```

4. 由 PC2(192.168.0.2) 進入 Command Prompt：

```
C:\>ping 192.168.100.1      [NO、無法連線]
```

(E) 測試 Inner_FTP 連線：

■ 測試：(帳號：cisco、密碼：cisco)

1. 由 PC3(192.168.1.1) 測試 fpt 連線：

```
C:\>ftp 192.168.100.2
Trying to connect...192.168.100.2
Connected to 192.168.100.2
220- Welcome to PT Ftp server
Username:cisco
331- Username ok, need password
Password:      [cisco]
230- Logged in
(passive mode On)
ftp>
```

2. 由 PC2(192.168.0.2) 測試 fpt 連線：

```
C:\>ftp 192.168.100.2          [NO、無法連線]
```

3. 由 PC3(192.168.1.1) 測試 ping 連線：

```
C:\>ping 192.168.100.2          [OK]
```

4. 由 PC1(192.168.0.1) 測試 ping 連線：

```
C:\>ping 192.168.100.2          [NO、無法連線]
```

9-6-5 內部路由器 DNZ 規劃

(請匯入：防火牆設定_網路設定.pkt)

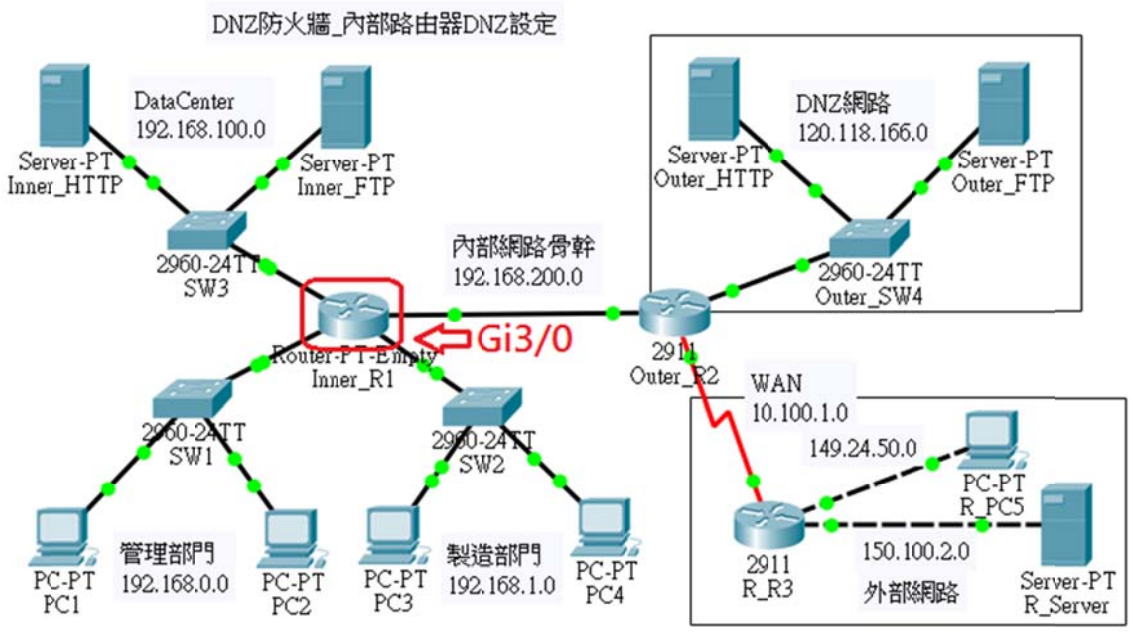

圖 9-20 內部路由器防火牆的 ACL 設定

內部路由器的 DNZ 防火牆功能是防止外部封包進入，又允許內部主機向外要求連線，或存取外部伺服器。但 DNZ 網路也安裝有伺服器提供內外網路使用者存取，對整個網路安全政策如下：(如圖 9-20 所示)

1. 禁止外部主機存取內部任何資源。
2. DNZ 網路(120.118.166.0/24) 上主機可以與內部網路 (192.168.0.0/16) 主機相互連線。
3. 允許 PC1 主機(192.168.0.1) 可登入 Inner_R1 內(利用 192.168.100.254 介面)。
4. DataCenter 網路(192.168.100.0/24) 上資源提供**內部任何主機存取**(沒有管制)。

(A) 靜態路由表規劃：

當防火牆被啟動之後，它管制了許多封包的進出，**當然也限制了動態繞路協定運作中的封包，此時動態繞路(RIP、OSPF、EGIRP、、)功能便失效**。因此需要再建立靜態路由表，才能維持網路之間繞路功能。吾人依照圖 9-20 規劃路由表如下：

Router	Destination AD	Network Mask	Net Hop

Inner_R1	120.118.166.0	255.255.255.0	192.168.200.2
	0.0.0.0	0.0.0.0	192.168.200.2
Outer_R2	192.168.0.0	255.255.0.0	192.168.200.1
	0.0.0.0	0.0.0.0	10.100.1.2
R_R3	0.0.0.0	0.0.0.0	10.100.1.1

■ 由 Inner_R1 路由器上設定路由表 (密碼：**User**)

```
Ineer_R1#config ter
Ineer_R1(config)#no router rip
Ineer_R1(config)#ip route 120.118.166.0 255.255.255.0 192.168.200.2
Ineer_R1(config)#ip route 0.0.0.0 0.0.0.0 192.168.200.2
Ineer_R1(config)#do show ip route
    Gateway of last resort is 192.168.200.2 to network 0.0.0.0

    120.0.0.0/24 is subnetted, 1 subnets
    S 120.118.166.0 [1/0] via 192.168.200.2
    C 192.168.0.0/24 is directly connected, GigabitEthernet0/0
    C 192.168.1.0/24 is directly connected, GigabitEthernet1/0
    C 192.168.100.0/24 is directly connected, GigabitEthernet2/0
    C 192.168.200.0/24 is directly connected, GigabitEthernet3/0
    S* 0.0.0.0/0 [1/0] via 192.168.200.2
```

■ Outer_R2 路由器上設定靜態路由表

```
Outer_R2#config ter
Outer_R2(config)#no router rip
Outer_R2(config)#ip route 192.168.0.0 255.255.0.0 192.168.200.1
Outer_R2(config)#ip route 0.0.0.0 0.0.0.0 10.100.1.2
Outer_R2(config)#do show ip route
      Gateway of last resort is 10.100.1.2 to network 0.0.0.0

    10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
    C 10.100.1.0/24 is directly connected, Serial0/2/0
    L 10.100.1.1/32 is directly connected, Serial0/2/0
    120.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
    C 120.118.166.0/24 is directly connected, GigabitEthernet0/1
```

```
L 120.118.166.254/32 is directly connected, GigabitEthernet0/1
S 192.168.0.0/16 [1/0] via 192.168.200.1
192.168.200.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.200.0/24 is directly connected, GigabitEthernet0/0
L 192.168.200.2/32 is directly connected, GigabitEthernet0/0
S* 0.0.0.0/0 [1/0] via 10.100.1.2
```

- R_R3 路由器上設定靜態路由表

```
R_R3#config ter
R_R3(config)#no router rip
R_R3(config)#ip route 0.0.0.0 0.0.0.0 10.100.1.1
R_R3(config)#do show ip route

Gateway of last resort is 10.100.1.1 to network 0.0.0.0

10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C 10.100.1.0/24 is directly connected, Serial0/2/0
L 10.100.1.2/32 is directly connected, Serial0/2/0
149.24.0.0/16 is variably subnetted, 2 subnets, 2 masks
C 149.24.50.0/24 is directly connected, GigabitEthernet0/0
L 149.24.50.254/32 is directly connected, GigabitEthernet0/0
150.100.0.0/16 is variably subnetted, 2 subnets, 2 masks
C 150.100.2.0/24 is directly connected, GigabitEthernet0/1
L 150.100.2.254/32 is directly connected, GigabitEthernet0/1
S* 0.0.0.0/0 [1/0] via 10.100.1.1
```

(B) 防火牆規劃：

- 對 Inner-R1 路由器 Gi3/0 (192.168.200.1) 管制封包進出內部網路：

1. 允許來源是 120.118.166.0/24 網路上主機進入內部網路。
2. 允許內部主機連結外部伺服器，但不允許外部主機連結內部伺服器。
3. 不允許外部網路主機進入內部網路。

- **Inner-DNZ-ACL 條件：**內部路由器 **(Gi3/0)** 管制存取資料中心的資源：

Inner_R1**(Gi3/0)** 外部路由器：**Inner-DNZ-ACL**

編號	Permit/ deny	封包類型	來源		目的		方向	備註
			IP	port	IP	port		
1	permit	TCP	192.168.0.0/16	any	any	<1024	out	
2	permit	TCP	any	<1024	192.168.0.0/16	any	in	
3	permit	UDP	192.168.0.0/16	any	any	<1024	out	
4	permit	UDP	any	<1024	192.168.0.0/16	any	in	
5	permit	ip	192.168.0.0/16		120.118.166.0/24		out	
6	permit	ip	120.118.166.0/24		192.168.0.0/16		in	
7	permit	Icmp-echo	192.168.0.0/16		any		out	ping
8	Permit	Icmp echo-reply	any		192.168.0.0/16		in	echo

備註：當內部主機存取外部資源時，外部伺服器大多設置於 < 1024 埠口的 TCP 或 UDP (目的埠口)。當外部伺服器回應時，其來源埠口也位於 < 1024 埠口上。

(C) 設定 Inner-DNZ-ACL-out 防火牆規則

由 Inner_R1 路由器上設定：**(管制 Gi3/0 介面出去封包)**

```
Ineer_R1>en
Ineer_R1#config ter
Ineer_R1(config)#ip access-list extended Inner-DNZ-ACL-out
Ineer_R1(config-ext-nacl)#permit tcp 192.168.0.0 0.0.255.255 any lt 1024
Ineer_R1(config-ext-nacl)#permit udp 192.168.0.0 0.0.255.255 any lt 1024
Ineer_R1(config-ext-nacl)#permit icmp 192.168.0.0 0.0.255.255 any echo
Ineer_R1(config-ext-nacl)#permit ip 192.168.0.0 0.0.255.255 120.118.166.0 0.0.0.255
Ineer_R1(config-ext-nacl)#deny ip any any
Ineer_R1(config-ext-nacl)#exit
Ineer_R1(config)#do show access-list Inner-DNZ-ACL-out
```

```
        Extended IP access list Inner-DNZ-ACL-out
        permit tcp 192.168.0.0 0.0.255.255 any lt 1024
        permit udp 192.168.0.0 0.0.255.255 any lt 1024
        permit icmp 192.168.0.0 0.0.255.255 any echo
        permit ip 192.168.0.0 0.0.255.255 120.118.166.0 0.0.0.255
        deny ip any any
Ineer_R1(config)#int gi3/0
Ineer_R1(config-if)#ip access-group Inner-DNZ-ACL-out out
```

(D) 設定 Inner-DNZ-ACL-in 防火牆規則

由 Inner_R1 路由器上設定：**(管制 Gi3/0 介面進入封包)**

```
Ineer_R1(config)#ip access-list extended Inner-DNZ-ACL-in
Ineer_R1(config-ext-nacl)#permit tcp any lt 1024 192.168.0.0 0.0.255.255
Ineer_R1(config-ext-nacl)#permit udp any lt 1024 192.168.0.0 0.0.255.255
Ineer_R1(config-ext-nacl)#permit icmp any 192.168.0.0 0.0.255.255 echo-reply
Ineer_R1(config-ext-nacl)#permit ip 120.118.166.0 0.0.0.255 192.168.0.0 0.0.255.255
Ineer_R1(config-ext-nacl)#deny ip any any
Ineer_R1(config-ext-nacl)#exit
Ineer_R1(config)#do show access-list Inner-DNZ-ACL-in
    Extended IP access list Inner-DNZ-ACL-in
    permit tcp any lt 1024 192.168.0.0 0.0.255.255
    permit udp any lt 1024 192.168.0.0 0.0.255.255
    permit icmp any 192.168.0.0 0.0.255.255 echo-reply
    permit ip 120.118.166.0 0.0.0.255 192.168.0.0 0.0.255.255
    deny ip any any

Ineer_R1(config)#int gi3/0
Ineer_R1(config-if)#ip access-group Inner-DNZ-ACL-in in
Ineer_R1(config-if)#
```

(E) 設定 telnet-ACL 防火牆規則 (允許主機登入路由器)

除此之外，我們也希望建立一個 VTP 遠端連線埠口 (192.168.100.254)，並僅允許管理者 (192.168.0.1 與 192.168.1.1) 主機可以登入操作，規劃內如如下表所示：

```
Inner_R1(config)#ip access-list standard telnet-ACL
Inner_R1(config-std-nacl)#permit host 192.168.0.1
Inner_R1(config-std-nacl)#permit host 192.168.1.1
Inner_R1(config-std-nacl)#deny any
```

```
Inner_R1(config-std-nacl)#exit
Inner_R1(config)#line vty 0 4
Inner_R1(config-line)#password cisco
Inner_R1(config-line)#login
Inner_R1(config-line)#access-class telnet-ACL in
Inner_R1(config-line)#exit
Ineer_R1(config)#enable password User
```

(F) 測試 DNZ 網路：

(請匯入：DNZ 防火牆_內部路由器 DNZ 設定.pkt)

■ 由內部網路測試連結外部伺服器：

1. 由 PC1(192.168.0.1) => Web Browser => http://120.118.166.1 **[OK]**
2. 由 PC1(192.168.0.1) => Web Browser => http://150.100.2.1 **[OK]**
3. 由 PC1(192.168.0.1) => ping 150.100.2.1 **[OK]**
4. 由 PC1(192.168.0.1) => ping 120.118.166.1 **[OK]**

■ 由外部網路連結內部網路及伺服器：

1. 由 R_PC5(149.24.50.1) => Web Browser => http://120.118.166.1 **[OK]**
2. 由 R_PC5(149.24.50.1) => Web Browser => http://192.168.100.1 **[NO]**
3. 由 R_PC5(149.24.50.1) => ping 120.118.166.1 **[OK]**
4. 由 R_PC5(149.24.50.1) => ping 192.168.0.1 **[NO]**

■ 由 DNZ 網路連結內部網路及伺服器：

1. 由 Outer_HTTP (120.118.166.1) => Web Browser => http://192.168.100.1 **[OK]**
2. 由 Outer_HTTP (120.118.166.1) => Web Browser => http://150.100.2.1 **[OK]**
3. 由 Outer_HTTP (120.118.166.1) => ping 149.24.50.1 **[OK]**
4. 由 Outer_HTTP (120.118.166.1) => ping 192.168.0.1 **[OK]**

9-6-6 外部路由器 DNZ 規劃

(請匯入：DNZ 防火牆_內部路由器 DNZ 設定.pkt)

(A) DNZ 防火牆規劃

DNZ 屏蔽網路主要是利用外部路由器 (Outer_R2) 與內部路由器 (Inner_R1) 管制封包進出私有網路，兩只路由器分擔不同的管制機制，也可以重複管制達到雙重安全效果，到底要達到何種防護機制，由各自治系統的安全政策而定。如圖 9-21 所示，本範例在內部路由器採用較嚴謹的官制機制，**如 9-6-4 節設定**，如下：

1. 禁止外部主機存取內部任何資源。
2. DNZ 網路(120.118.166.0/24) 上主機可以與內部網路主機相互連線。
3. DataCenter 網路(192.168.100.0/24) 上資源提供**內部任何主機存取**(沒有管制)。

在外部路由器(Outer_R2) 的 se0/2/0 埠口採用較鬆散的機制，期望它管制進入內部網路的封包，如下：(**管制 S0/2/0 埠口**)

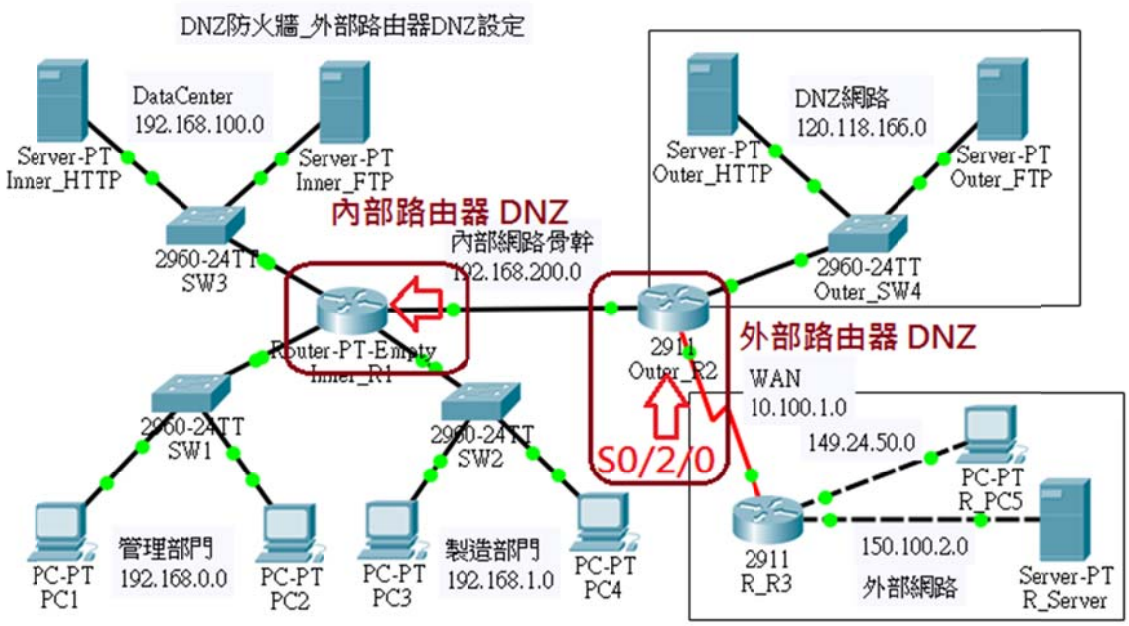

圖 9-21 外部路由器 DNZ 防火牆規劃

(1) 允許外部可以任意存取 DNZ 網路內伺服器。

(2) 允許外部網路可以測試 (Ping) DNZ 網路下主機。

(3) 允許內部網路主機可以任意進出。

(B) DNZ 防火牆規則

還未設定外部路由器 DNZ 之前，吾人先測試外部連結到內部網路狀態如何：

測試外部網路連結到內部網路：

1. 由 R_PC5(149.24.50.1) => Web Browser => http://120.118.166.1 **[OK]**
2. 由 R_PC5(149.24.50.1) => ping 120.118.166.1 **[OK]**
3. **由 R_PC5(149.24.50.1) => ping 192.168.200.2** **[OK]**

表示外部網路可以連結到 192.168.200.0 網路上，吾人需管制外部主機不可連結到內部網路。

DNZ-ACL 規則：管制進出 DNZ 網路封包 **(S0/2/0 埠口)**：

Outer_R2**(Gi0/1)** 外部路由器：**DNZ-ACL**								
編號	Permit/ deny	封包類型	來源		目的		方向	備註
			IP	port	IP	port		
1	permit	ip	any		120.118.166.0/24		in	
2	permit	ip	120.118.166.0/24		any		out	
3	permit	ip	192.168.0.0/16		any		out	
4	permit	ip	any		192.168.0.0/16		in	
5	deny	ip	any		any			

(C) 設定 DNZ-ACL 防火牆

DNZ-ACL-out 規則：(管制封包出去 S0/2/0 埠口)：

```
Outer_R2> en
Outer_R2#config ter
Outer_R2(config)#ip access-list extended DNZ-ACL-out
Outer_R2(config-ext-nacl)#permit ip 120.118.166.0 0.0.0.255 any
Outer_R2(config-ext-nacl)#permit ip 192.168.0.0 0.0.255.255 any
Outer_R2(config-ext-nacl)#deny ip any any
Outer_R2(config-ext-nacl)#exit
Outer_R2(config)#do show access-list DNZ-ACL-out
      Extended IP access list DNZ-ACL-out
      permit ip 120.118.166.0 0.0.0.255 any
      permit ip 192.168.0.0 0.0.255.255 any
      deny ip any any
Outer_R2(config)#int s0/2/0
Outer_R2(config-if)#ip access-group DNZ-ACL-out out
```

■ DNZ-ACL-in 規則：(管制封包進入 S0/2/0 埠口)：

```
Outer_R2(config)#ip access-list extended DNZ-ACL-in
Outer_R2(config-ext-nacl)#permit ip any 120.118.166.0 0.0.0.255
Outer_R2(config-ext-nacl)#permit ip any 192.168.0.0 0.0.255.255
Outer_R2(config-ext-nacl)#deny ip any any
Outer_R2(config-ext-nacl)#exit
Outer_R2(config)#do show access-list DNZ-ACL-in
    Extended IP access list DNZ-ACL-in
    permit ip any 120.118.166.0 0.0.0.255
    permit ip any 192.168.0.0 0.0.255.255
    deny ip any any
Outer_R2(config)#int s0/2/0
Outer_R2(config-if)#ip access-group DNZ-ACL-in in
```

(D) DNZ 防火牆測試

(請匯入：防火牆設定_外部路由器 DNZ 設定.pkt)

■ 由內部網路測試連結外部伺服器：

1. 由 PC1(192.168.0.1) => Web Browser => http://120.118.166.1 **[OK]**
2. 由 PC1(192.168.0.1) => Web Browser => http://150.100.2.1 **[OK]**
3. 由 PC1(192.168.0.1) => ping 150.100.2.1 **[OK]**

4. 由 PC1(192.168.0.1) => ping 120.118.166.1 **[OK]**

由外部網路連結內部網路及伺服器：

1. 由 R_PC5(149.24.50.1) => Web Browser => http://120.118.166.1 **[OK]**
2. 由 R_PC5(149.24.50.1) => Web Browser => http://192.168.100.1 **[NO]**
3. 由 R_PC5(149.24.50.1) => ping 120.118.166.1 **[OK]**
4. **由 R_PC5(149.24.50.1) => ping192.168.200.1** **[NO]**

- **由此可見，外部網路無法連結到 192.168.0.0/16 網路上任何主機，但內部網路連結外部主機都沒有問題。**

由 DNZ 網路連結內部網路及伺服器：

1. 由 Outer_HTTP (120.118.166.1) => Web Browser => http://192.168.100.1 **[OK]**
2. 由 Outer_HTTP (120.118.166.1) => Web Browser => http://150.100.2.1 **[OK]**
3. 由 Outer_HTTP (120.118.166.1) => ping 149.24.50.1 **[OK]**
4. 由 Outer_HTTP (120.118.166.1) => ping 192.168.0.1 **[OK]**

- **DNZ 網路主機可以任意連結內部網路。**

9-6-7 自我挑戰：外部管理主機設定

(請匯入：DNZ 防火牆_外部路由器 DNZ 設定.pkt)

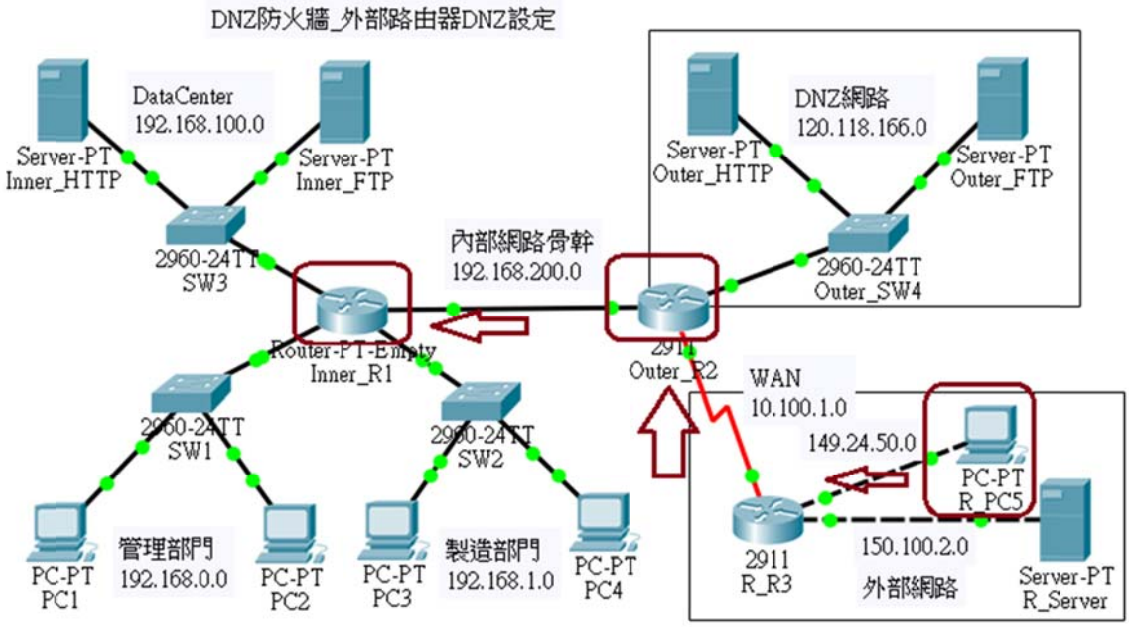

圖 9-22 外部管理主機設定

(A) 管理主機需求

本自治系統的網路管理工作可能委託外部廠商承包，外部管理者需要進入內部網路從事維護工作，而該主機的 IP 位址是 **149.24.50.1**，吾人期望它具有下列權限：

1. 可進入內部網路通行無阻。
2. 可登入 Inner_R1 與 Outer_R2 路由器從事網路管理工作。

(B) 防火牆規劃與設定

(需分別設定 Inner_R1 與 Outer_R2，請自行製作)

9-6-8 自我挑戰：DNZ+NAT 防火牆設定

(請匯入：DNZ 防火牆_外部路由器 DNZ 設定.pkt)

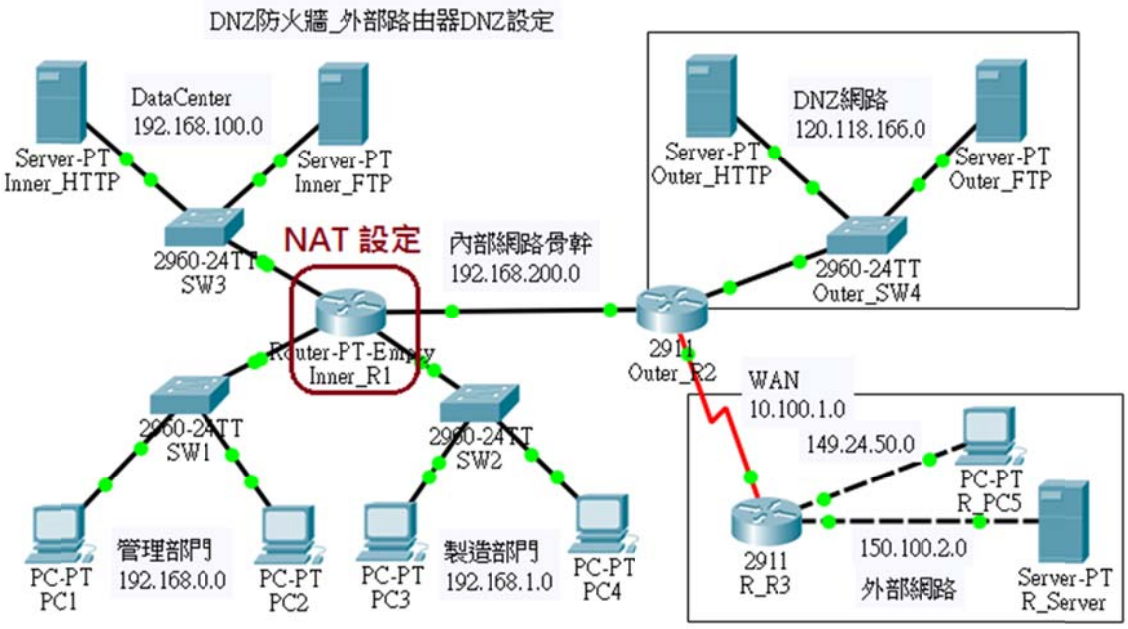

圖 9-23 DNZ+NAT 防火牆設定

(A) 系統需求

公司為了防範被駭客攻擊的可能，期望將內部網路位址完全隱藏，公司合法 IP 網路號碼為 120.118.165.0/24，期望分配給內部主機使用如下：

內部 IP (私有位址)	外部 IP (合法位址)
192.168.0.0/24	120.118.165.1 ~ 20 (動態 NAT)
192.168.1.0/24	120.118.165.21 ~ 40 (動態 NAT)
192.168.100.1	120.118.165.250 (靜態 NAT)
192.168.100.2	120.118.165.251 (靜態 NAT)

(B) NAT 防火牆設定

(請由 Inner_R1 路由器設定，請自行製作)

9-6-9 自我挑戰：協力廠商網路設定

(請匯入：DNZ 防火牆_外部路由器 DNZ 設定.pkt)

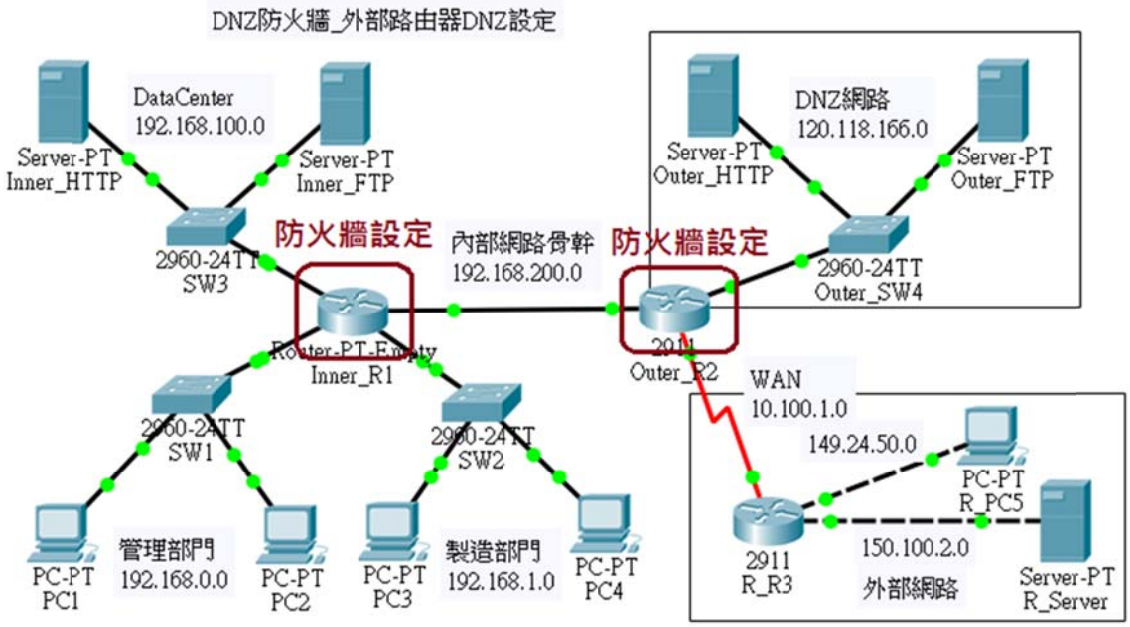

圖 9-24 協力廠商網路設定

(A) 系統需求

公司希望開放內部伺服器讓協力廠商的主機可以存取，協力廠商網路號碼是：150.100.3.0/24，期望開放下列功能：

1. 150.100.3.0/24 網路下主機可以存取 Inner_HTTP (192.168.100.1) 網頁資源。
2. 150.100.3.0/24 網路下主機可以存取 Inner_FTP (192.168.100.2) 檔案資源。
3. 不允許連結或測試內部各個主機。

(B) 防火牆設定

(請由分別 Inner_R1 與 Outer_R2 路由器設定，請自行製作)