

Linux Firewall & NAT



Kenduest Lee (小州)

內容大綱

- 大綱內容
 - Firewall 簡介與架構
 - Linux Firewall
 - Linux IPTables 設定
 - Linux NAT 設定
 - Transparent Proxy 設定

Firewall 簡介

- Firewall 簡介
 - 功能
 - 限制規範網路連線存取進出的政策
 - 可以用來提供防禦與保護主機功能
 - 作法
 - 透過硬體設備於封包進出時候進行限制規範
 - 由作業系統本身以軟體方式進行限制規範

Firewall 架構

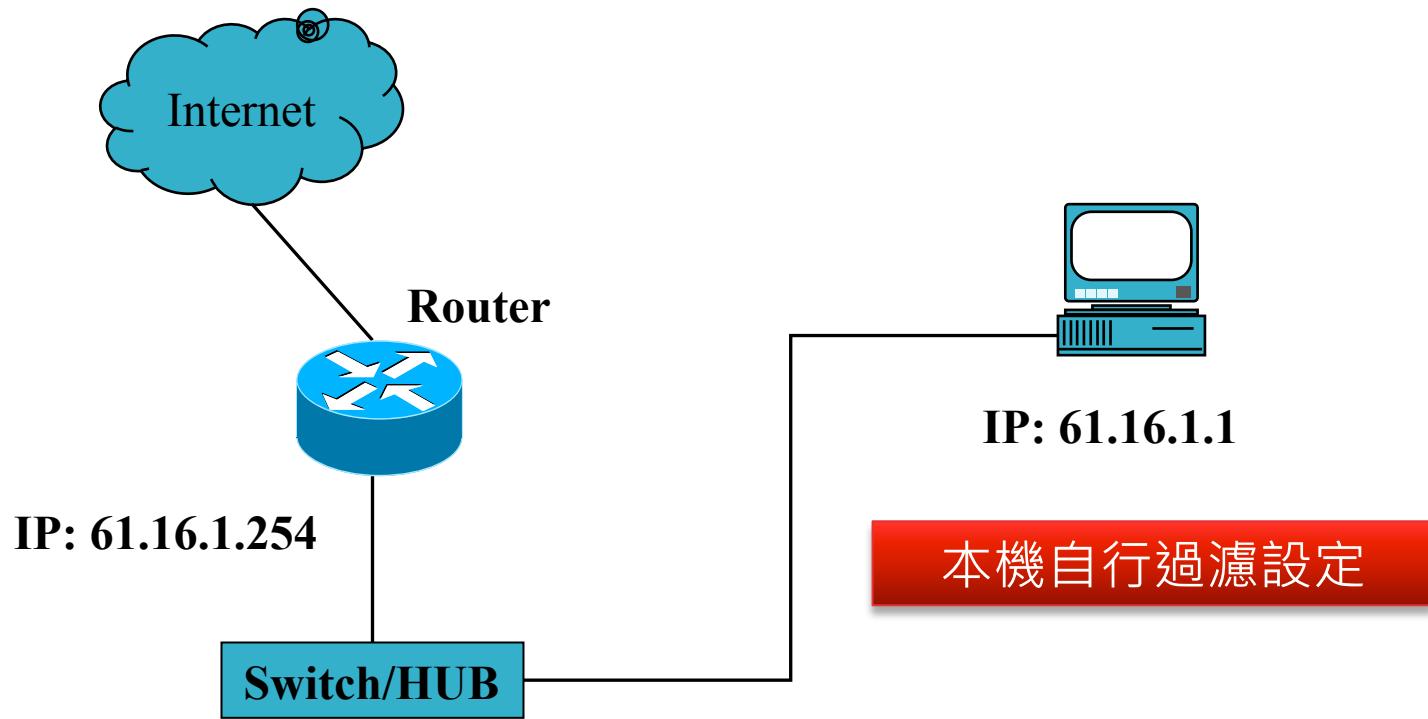
- Firewall 架構
 - 架構類型
 - Packet Filtering Firewall (封包過濾架構)
 - Proxy Firewall (代理架構)

Firewall 類型架構

- Firewall 類型架構
 - Packet Filtering Firewall (封包過濾防火牆)
 - 以網路封包 (Layer 2, Layer3 ..) 為基礎的低階過濾
 - 自己單機本身可以針對連入該主機的封包進行過濾
 - Router 設備可以針對通過主機的封包進行過濾

Firewall 類型架構

- Packet Filtering Firewall 架構圖

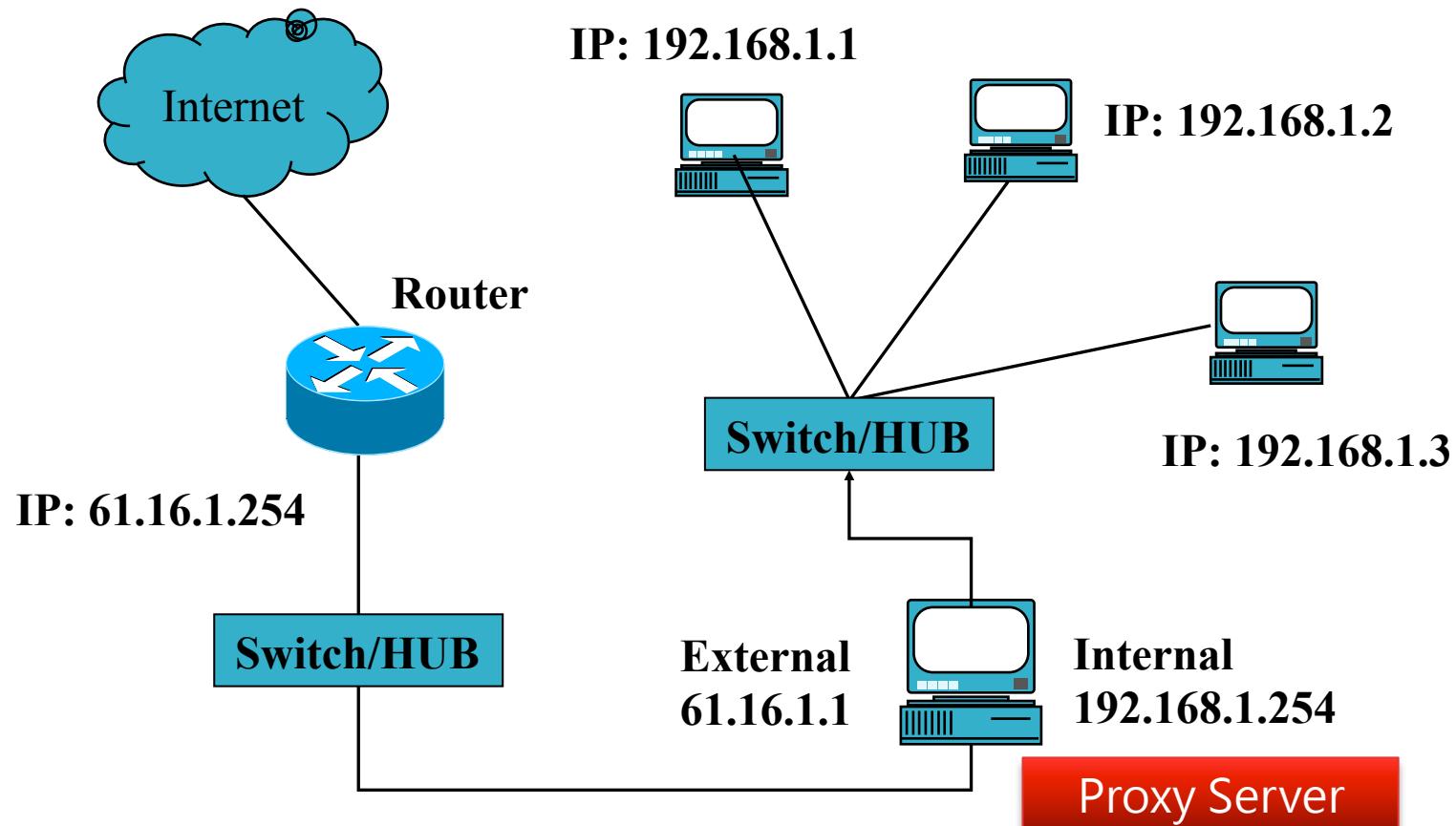


Firewall 類型架構

- Firewall 類型架構
 - Proxy Firewall (代理防火牆)
 - 透過代理 (HTTP, FTP, Socks) 為基礎的代理過濾
 - Client 端透過 Proxy Server 服務連結聯外

Firewall 類型架構

- Proxy Firewall 架構圖



Linux Firewall 發展

- Linux Firewall 世代發展
 - 世代版本
 - Linux kernel 2.0 世代使用 ipfwadm
 - Linux kernel 2.2 世代使用 ipchains + ipmasqadm
 - Linux kernel 2.4 世代開始使用 iptables
 - 另外還可以用 ebtables 提供更低階層級過濾功

Linux Firewall 發展

- Linux IPTables 簡介
 - 簡介
 - netfilter project 的專案計畫項目
 - 於 linux kernel 2.4 核心版本內納入支援使用
 - <http://www.netfilter.org/>
 -

Linux Firewall 發展

- Linux IPTables 功能
 - 功能
 - 支援 ipv4 與 ipv6 的網路協定
 - 主要針對 Layer3 (部分 Layer2) 層級的過濾
 - 支援 NAT 功能 (IP 偽裝，Port 轉送應對)
 - 支援額外擴充的延伸比對功能

Linux Firewall 過濾機制

- Linux **IPTables** 提供過濾功能項目
 - 針對一般 Layer3 範圍的過濾機制
 - Source IP, Destination IP
 - Source Port, Destination Port
 - Packet Type (TCP,UDP,ICMP..)
 - Header Flag (SYN,ACK...), Length

Linux Firewall 過濾機制

- Linux **IPTables** 提供過濾功能項目
 - 特殊的過濾機制 (搭配 Match Extension)
 - 封包類型 (Unicast, Broadcast, Multicast..)
 - 連線數量、時間區段、與封包傳輸總量限制
 - 網路卡的卡號過濾 (Mac Address)

Linux Firewall 過濾機制

- RHEL/CentOS Linux IPTables Firewall 設定
 - 內建配置設定方式
 - 圖形介面環境的 `system-config-firewall` 工具
 - 產生設定檔案位置
 - `/etc/sysconfig/iptables` (for ipv4)
 - `/etc/sysconfig/ip6tables` (for ipv6)
 - 設定服務管理方式
 - `/etc/init.d/iptables { start | stop | restart }`
 - `/etc/init.d/ip6tables { start | stop | restart }`

IPTables 封包過濾

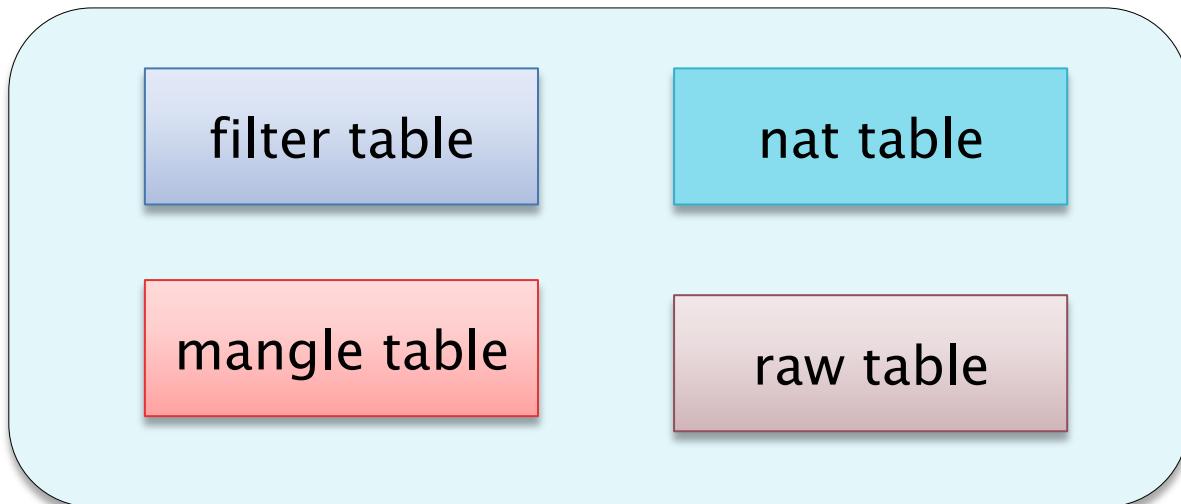
- **IPTables Table** 內容
 - iptables 依據不同需求用途提供不同 table 項目
 - 當封包進出系統時會依照 table 內的規則進行比對，包含封包改寫處理

封包傳入傳出時



IPTables 封包過濾

- IPTables Table 內容
 - Table 列表項目



IPTables 封包過濾

- IPTables Table 內容



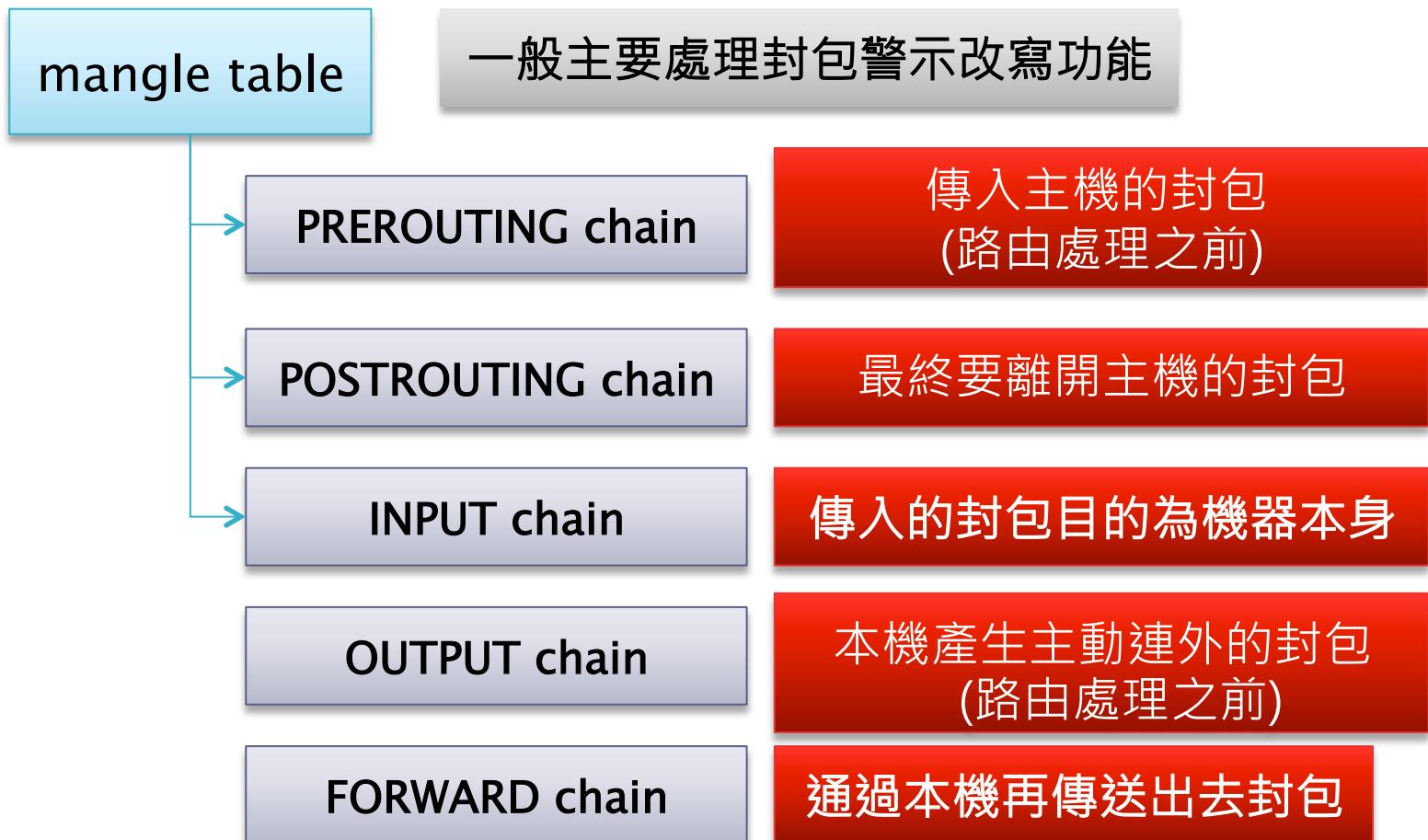
IPTables 封包過濾

- IPTables Table 內容



IPTables 封包過濾

- IPTables Table 內容



IPTables 封包過濾流程圖

- IPTables Table 內容
 - Table 配置使用
 - 一般設定以 filter 與 nat table 為主
 - 針對本機連入與連外過濾，使用 filter table
 - 需要改寫的封包 IP 與 Port 改寫，使用 nat table

IPTables 工具

- Linux **IPTables** 程式工具
 - 主要程式項目
 - `iptables` (for ipv4)
 - `ip6tables` (for ipv6)
 - 檢視與回復程式項目
 - `iptables-save` , `iptables-restore` (for ipv4)
 - `ip6tables-save`, `ip6tables-restore` (for ipv6)

IPTables 命令使用

- iptables 程式命令
 - iptables 命令語法
 - iptables [-t table] cmd rule [options] ...



filter table
(預設)

nat table

mangle table

raw table

IPTables 命令參數

- iptables 程式命令
 - iptables 命令參數

參數項目	參數說明
-A CHAIN	新增附加某個規則至 CHAIN 內
-D CHAIN	刪除 CHAIN 內某個規則
-I CHAIN	插入某個規則至 CHAIN 內
-L [CHAIN]	列出 CHAIN 內所有規則
-F [CHAIN]	清除 CHAIN 內所有規則
-Z [CHAIN]	CHAIN 封包/位元組計數器記錄歸零
-P [CHAIN]	設定 CHAIN 預設目標預設政策
-X [CHAIN]	刪除自定的 CHAIN 項目

IPTables 命令參數

- **iptables** 程式命令
 - 檢視目前系統核心內的 **firewall** 規則
 - 使用 **iptables-save** 命令
 - 使用 **iptables -L -n -t <tablename>** 命令
 - **-n** 表示不解析主機名稱 (使用 ip, port 編號顯示)
 - 整個敘述必要可以加上 **-v** 使用詳細模式檢視

IPTables 命令參數

- iptables 程式命令
 - 清空與重置規則
 - 使用 **-F** 參數可清除某個 table 內每個 chain 內的規則
 - 使用 **-X** 參數可刪除自訂 chain 項目
 - 清空與計數器歸零設定
 - `iptables -F` # filter table
 - `iptables -X` # filter table
 - `iptables -F -t nat` # nat table
 - `iptables -X -t nat` # nat table

IPTables 命令參數

- iptables 程式命令
 - 一般主要參數列表
 - -s [!] address[/mask]
 - 指定封包來源項目，預設沒指定表示所有來源
 - 使用！表示排除/不包含
 - -d [!] address[/mask]
 - 指定封包目的項目，預設沒指定表示所有來源
 - 使用！表示排除/不包含

IPTables 命令參數

- iptables 程式命令
 - 一般主要參數列表
 - -i interface 與 -o interface
 - 封包由指定的 interface 網路介面傳入/傳出
 - 沒指定時，預設等於配置使用 -i all 與 -o all 項目
 - 介面名稱，eth+ 表示 eth0 與 eth1...

IPTables 命令參數

- **iptables** 程式命令
 - 一般主要參數列表
 - **-p protocol**
 - 指定封包的 protocol 型態 (tcp、udp、icmp)
 - **-p icmp**
 - 搭配配 **--icmp-type** 指定 icmp 的類型
 - 執行 **iptables -p icmp -h** 可以查看完整類型列表

IPTables 命令參數

- iptables 程式命令
 - 一般主要參數列表
 - --sport (--source-port)
 - 指定 source port
 - 使用 port1:port2 表示 port1 ~ port2 範圍連接埠
 - --dport (--destination-port)
 - 指定 destination port
 - 使用 port1:port2 表示 port1 ~ port2 範圍連接埠

IPTables 命令參數

- iptables 程式命令
 - 一般主要參數列表
 - -j TARGET
 - 指定跳躍規則目標
 - 常見 TARGET 規則項目 (ACCEPT, DROP , REJECT ...)

IPTables 跳躍目標

- iptables 程式命令
 - 一般封包符合特定條件時處理的方式
 - ACCEPT
 - 允許封包通過
 - DROP
 - 丟棄封包
 - REJECT
 - 功能類似於 DROP 處理方式
 - 會回應錯誤封包資訊給傳送端

IPTables 跳躍目標

- **iptables 程式命令**
 - 一般封包符合特定條件時處理的方式
 - **QUEUE**
 - 把封包處理丟給 User Space 程式處理
 - **RETURN**
 - 停止繼續比對規則，返回到上一個 Rule
 - **SNAT**
 - 提供 SNAT 功能，針對來源 IP 改寫

IPTables 跳躍目標

- **iptables 程式命令**
 - 一般封包符合特定條件時處理的方式
 - **DNAT**
 - 提供 SNAT 功能，針對目的 IP 改寫
 - **REDIRECT**
 - 導向封包，將封包導向至本機某個 Port
 - **MASQUERADE**
 - IP 偽裝，一般為提供 SNAT 服務

IPTables 跳躍目標

- iptables 程式命令
 - 一般封包符合特定條件時處理的方式
 - LOG
 - 將封包傳輸資訊紀錄於 log 檔案
 - ULOG
 - 將封包傳輸資訊紀錄於透過 ulogd 程式處理

IPTables 規則設定

- iptables 規則設定範例
 - 清空重置核心內 iptables firewall 設定
 - iptables -F # filter table
 - iptables -X # filter table
 - iptables -F -t nat # nat table
 - iptables -X -t nat # nat table

IPTables 規則設定

- iptables 規則設定範例
 - 禁止 192.168.2.1 連入存取
 - `iptables -A INPUT -s 192.168.2.1 -j DROP`
 - 禁止 192.168.2.1 連入存取 ssh 服務
 - `iptables -A INPUT -s 192.168.2.1 -p tcp --dport 22 \ -j DROP`

IPTables 規則設定

- iptables 規則設定範例
 - 禁止 ping 的探測封包傳入
 - `iptables -A INPUT -p icmp --icmp-type echo-request -j DROP`
 - 設定禁止來自於 eth1 網路介面傳入存取 ssh 服務的來源
 - `iptables -A INPUT -i eth1 -p tcp --dport 22 \ -j DROP`

IPTables 規則設定

- iptables 規則設定範例
 - 設定本機存取自己服務不會有任何限制
 - `iptables -A INPUT -i lo -j ACCEPT`
 - 設定只有開放 192.168.2.0/24 來源可以連線存取 ssh 服務
 - `iptables -A INPUT -s 192.168.2.0/24 -p tcp \ --dport 22 -j ACCEPT`
 - `iptables -A INPUT -p tcp --dport 22 -j DROP`

IPTables 規則設定

- **iptables 規則設定範例**
 - 設定只有開放 192.168.2.0/24 來源連線存取 ssh 服務，但是其中特別禁止 192.168.2.100 不可以連線存取 ssh 服務
 - `iptables -A INPUT -s 192.168.2.100 -p tcp \--dport 22 -j DROP`
 - `iptables -A INPUT -s 192.168.2.0/24 -p tcp \--dport 22 -j ACCEPT`
 - `iptables -A INPUT -p tcp --dport 22 -j DROP`

IPTables 規則設定

- iptables 規則設定範例
 - 設定禁止 192.168.2.0/24 來源連線存取 ssh 服務，但是其中特別開放 192.168.2.100 允許存取 ssh 服務
 - `iptables -A INPUT -s 192.168.2.100 -p tcp \ --dport 22 -j ACCEPT`
 - `iptables -A INPUT -s 192.168.2.0/24 -p tcp \ --dport 22 -j DROP`

IPTables 比對延伸

- **iptables match extension**
 - 說明
 - iptables 內提供許多延伸封包比對的 module 功能提供進階項目的過濾機制
 - 可以透過使用 -m 參數方式指定載入某個 module 檔案使用該功能

IPTables 比對延伸

- iptables match extension
 - 常見 module 項目
 - mac - source mac address match
 - multiport - multi-port match
 - length - packet length match
 - owner - locally-generated packets by someone
 - state - connection state

IPTables 比對延伸

- iptables match extension
 - 說明：使用 mac module 提供網路卡過濾
 - 參數：`--mac-source HWADDR`
 - 問題
 - 禁止 lan 內網卡卡號為 00:10:22:EF:90:3E 連線存取
 - 範例
 - `iptables -A INPUT -i eth0 -m mac \ --mac-source 00:10:22:EF:90:3E -j DROP`

IPTables 比對延伸

- iptables match extension
 - 說明：使用 multiport module 提供多重 port 過濾
 - 參數：`--sports [port,..]` | `-dports [port,...]`
 - 問題
 - 禁止 192.168.1.1 存取本機的 25,80,110 tcp port
 - 範例
 - `iptables -A INPUT -p tcp -m multiport \ --dports 25,80,110 -j DROP`

IPTables 比對延伸

- iptables match extension
 - 說明：使用 length module 提供判斷封包本身的長度
 - 參數：`--length length:[length]`
 - 問題
 - 禁止類型 echo-request 的 icmp 協定超過 84 bytes 封包
 - 範例
 - `iptables -A INPUT -p icmp --icmp-type \ echo-request -m length --length !1:84 -j DROP`

IPTables 比對延伸

- iptables match extension
 - 說明：使用 owner module 提供判斷主動連外的身份
 - 參數：`--uid-owner username`
 - 問題
 - 禁止執行身份為 peter 的 process 對外連結存取 ssh 服務
 - 範例
 - `iptables -A OUTPUT -p tcp -m owner \ --uid-owner peter -j DROP`

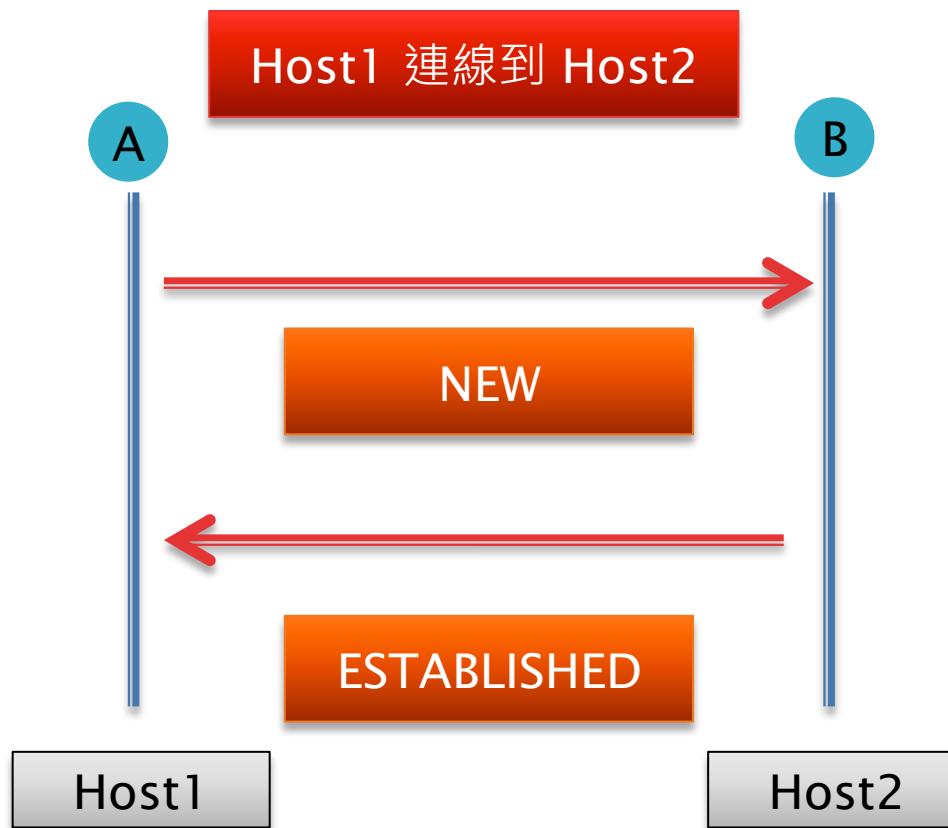
IPTables 比對延伸

- **iptables match extension**
 - 說明：使用 state module 判斷封包本身的連線性質狀態
 - 參數：`--state state[,...]`

狀態名稱	描述說明
NEW	表示新起始建立的封包
ESTABLISHED	表示雙向連線內回應建立的封包
RELATED	表示與之前連線有關進而新起始建立的封包，包含 FTP 資料傳輸或者是 ICMP 錯誤的封包
INVALID	表示未知

IPTables 比對延伸

- iptables match extension



IPTables 比對延伸

- iptables match extension
 - 設定禁止 192.168.2.1 主動連線存取本機
 - `iptables -A INPUT -i eth0 -s 192.168.2.1 \ -m state --state NEW -j DROP`
 - 設定因為本機連線進而回應傳入的封包
 - `iptables -A INPUT -m state --state \ ESTABLISHED -j ACCEPT`

IPTables 比對延伸

- iptables match extension
 - 設定只有開放 ssh 服務對外，剩餘連入存取都禁止
 - `iptables -A INPUT -p tcp --dport 22 -j ACCEPT`
 - `iptables -A INPUT -m state --state NEW -j DROP`

IPTables 預設政策

- IPTables Default Policy
 - 說明
 - 可以指定不同 chain 預設的規則為允許還是禁止
 - 參數使用 -P [chain-name] [ACCEPT | DROP]
 - 配置項目範例
 - `iptables -P INPUT ACCEPT`
 - `iptables -P INPUT DROP`

IPTables 預設政策

- IPTables Default Policy
 - 完整設定範例 (僅開放必要服務，其他都禁止)
 - iptables -F ; iptables -X
 - iptables -P INPUT ACCEPT
 - iptables -A INPUT -m state --state \
ESTABLISHED -j ACCEPT
 - iptables -A INPUT -i lo -j ACCEPT
 - iptables -A INPUT -p tcp --dport 21 -j ACCEPT
 - iptables -A INPUT -p tcp --dport 22 -j ACCEPT
 - iptables -A INPUT -m state --state NEW -j DROP

IPTables 預設政策

- IPTables Default Policy
 - 完整設定範例 (僅開放必要服務，其他都禁止)
 - iptables -F ; iptables -X
 - iptables -P INPUT DROP
 - iptables -A INPUT -m state --state \
ESTABLISHED -j ACCEPT
 - iptables -A INPUT -i lo -j ACCEPT
 - iptables -A INPUT -p tcp --dport 21 -j ACCEPT
 - iptables -A INPUT -p tcp --dport 22 -j ACCEPT

IPTables 與 FTP 環境

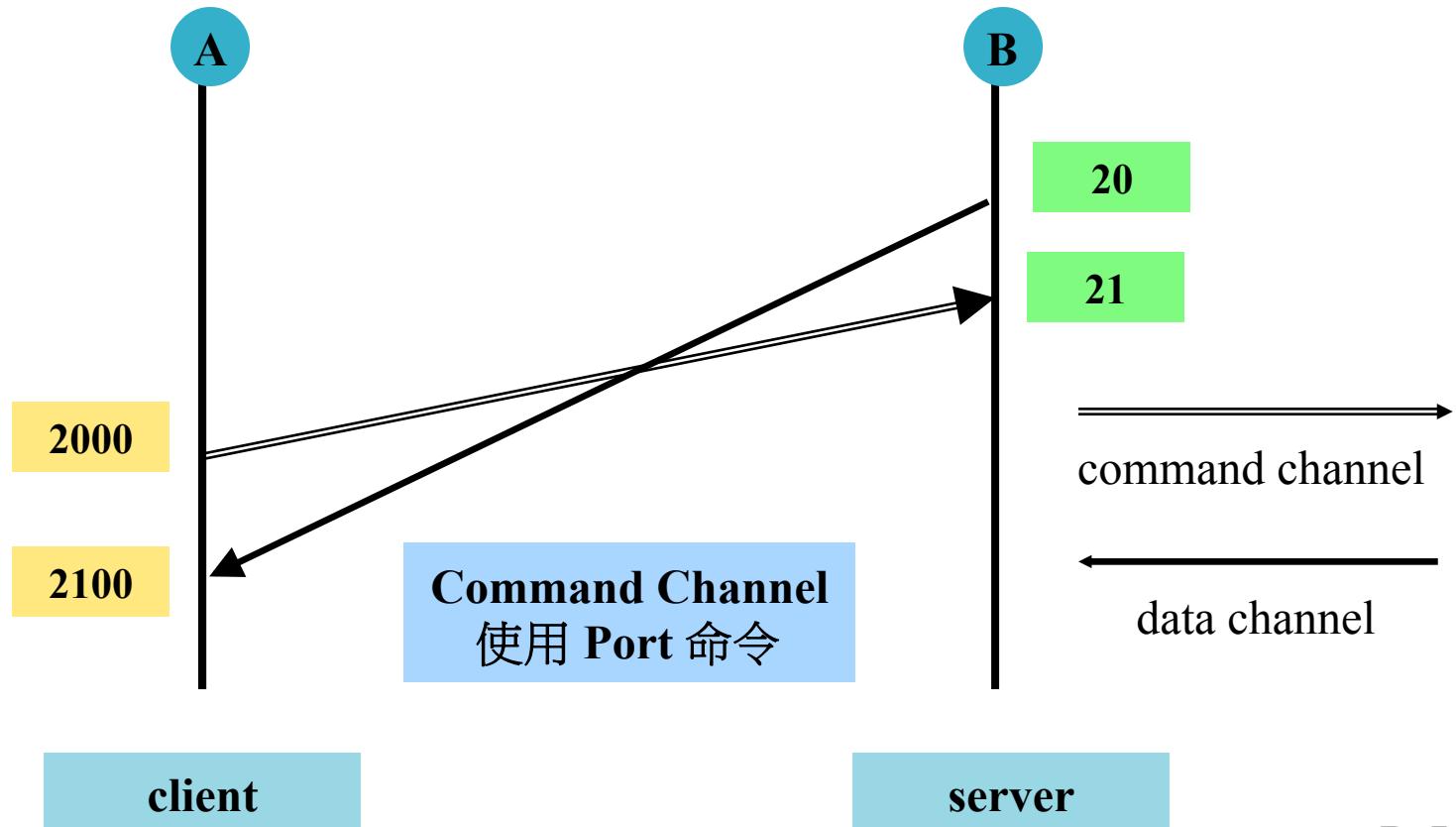
- IPTables 與 FTP 服務開放
 - 只有開放 ssh 與 ftp 服務對外，剩餘連入存取都禁止設定
 - `iptables -A INPUT -m state --state \ ESTABLISHED -j ACCEPT`
 - `iptables -A INPUT -i lo -j ACCEPT`
 - `iptables -A INPUT -p tcp --dport 21 -j ACCEPT`
 - `iptables -A INPUT -p tcp --dport 22 -j ACCEPT`
 - `iptables -A INPUT -m state --state NEW -j DROP`
 - FTP 協定實際溝通不是單一 port，若是只有開放 port 21 提供連線，實際 ftp 溝通傳輸會有問題

IPTables 與 FTP 環境

- IPTables 與 FTP 服務開放
 - FTP 協定本身有兩個 Channel 連線溝通
 - Command Channel
 - 命令交談使用的通道 (一般為 Port 21)
 - Data Channel
 - 傳輸所需要資料時所使用的通道
 - 可以細分 Active Mode , Passive Mode 協議傳輸模式
 - 依據不同協議方式 port 會動態調整而有所不同

IPTables 與 FTP 環境

- IPTables 與 FTP 服務開放
 - Active Mode 傳輸模式示意

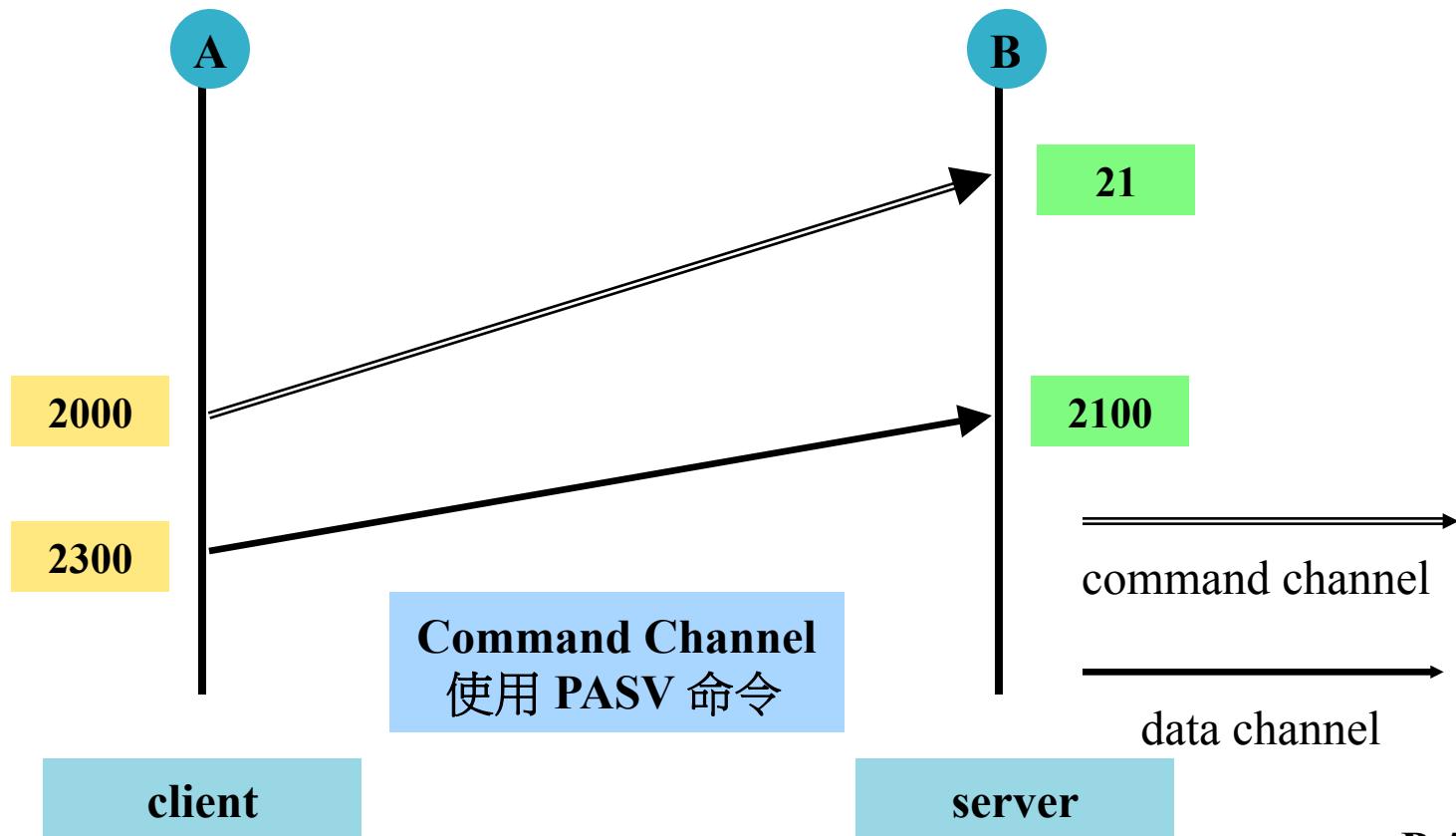


IPTables 與 FTP 環境

- IPTables 與 FTP 服務開放
 - Active Mode 傳輸模式說明
 - Client 端於高於 Port 1024 建立一個 Port 準備讓 Server 連線，並透過 Port 命令告訴 Server 其指定的 Port 編號
 - Server 端以 Port 20 連線至該 Client 指定的 Port 進行資料傳輸
 - Active Mode 通道使用情況
 - Command : (client > port 1024) → server port 21
 - Data : (client > port 1024) → server port 20

IPTables 與 FTP 環境

- IPTables 與 FTP 服務開放
 - Passive Mode 傳輸模式示意



IPTables 與 FTP 環境

- IPTables 與 FTP 服務開放
 - Passive Mode 傳輸模式說明
 - Client 端透過 PASV 命令告訴 Server 端使用 Passive Mode 進行後續資料傳輸溝通
 - Server 端於高於 Port 1024 建立一個 Port 準備讓 Client 連線，並告知 Client 端其指定的 Port 編號
 - Client 連線至該 Server 指定的 Port 進行資料傳輸
 - Passive Mode 通道使用情況
 - Command : (client > port 1024) → server port 21
 - Data : (client > port 1024) → (server > port 1024)

IPTables 與 FTP 環境

- IPTables 與 FTP 服務開放

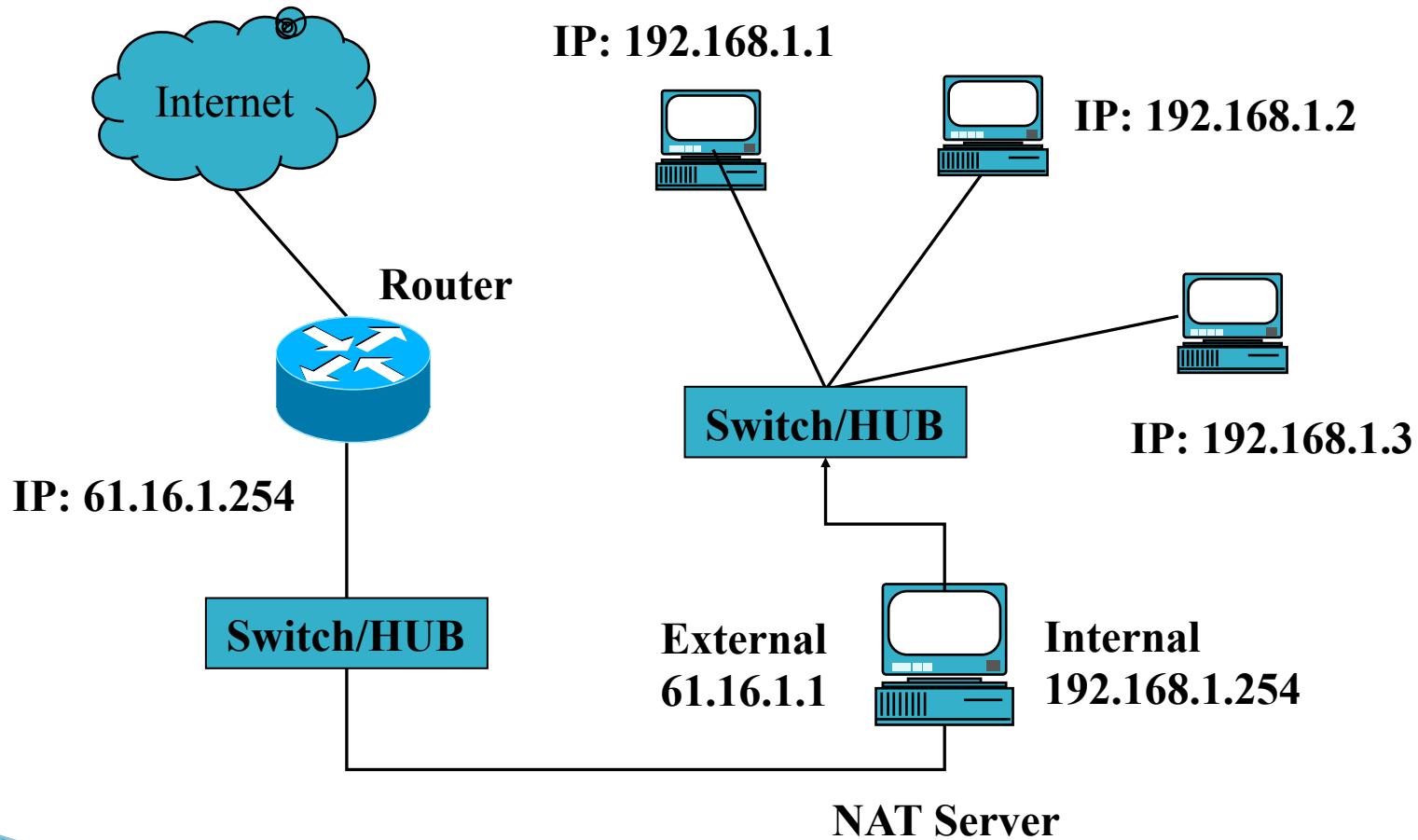
- 設定：主機僅開放 ssh 與 ftp 服務，其他連入存取皆禁止
 - modprobe nf_conntrack_ftp
 - iptables -A INPUT -m state --state \ ESTABLISHED,RELATED -j ACCEPT
 - iptables -A INPUT -i lo -j ACCEPT
 - iptables -A INPUT -p tcp --dport 21 -j ACCEPT
 - iptables -A INPUT -p tcp --dport 22 -j ACCEPT
 - iptables -A INPUT -m state --state NEW,INVALID -j DROP

NAT

- NAT (Network Address Translation)
 - 說明
 - NAT 全名為 Network Address Translation
 - NAT 提供針對封包內的 IP 位址進行改寫動作
 - NAT 主要可以區分成為 SNAT 與 DNAT 兩大類型

NAT 功能

- NAT (Network Address Translation) 環境示意圖



NAT 與 Private IP

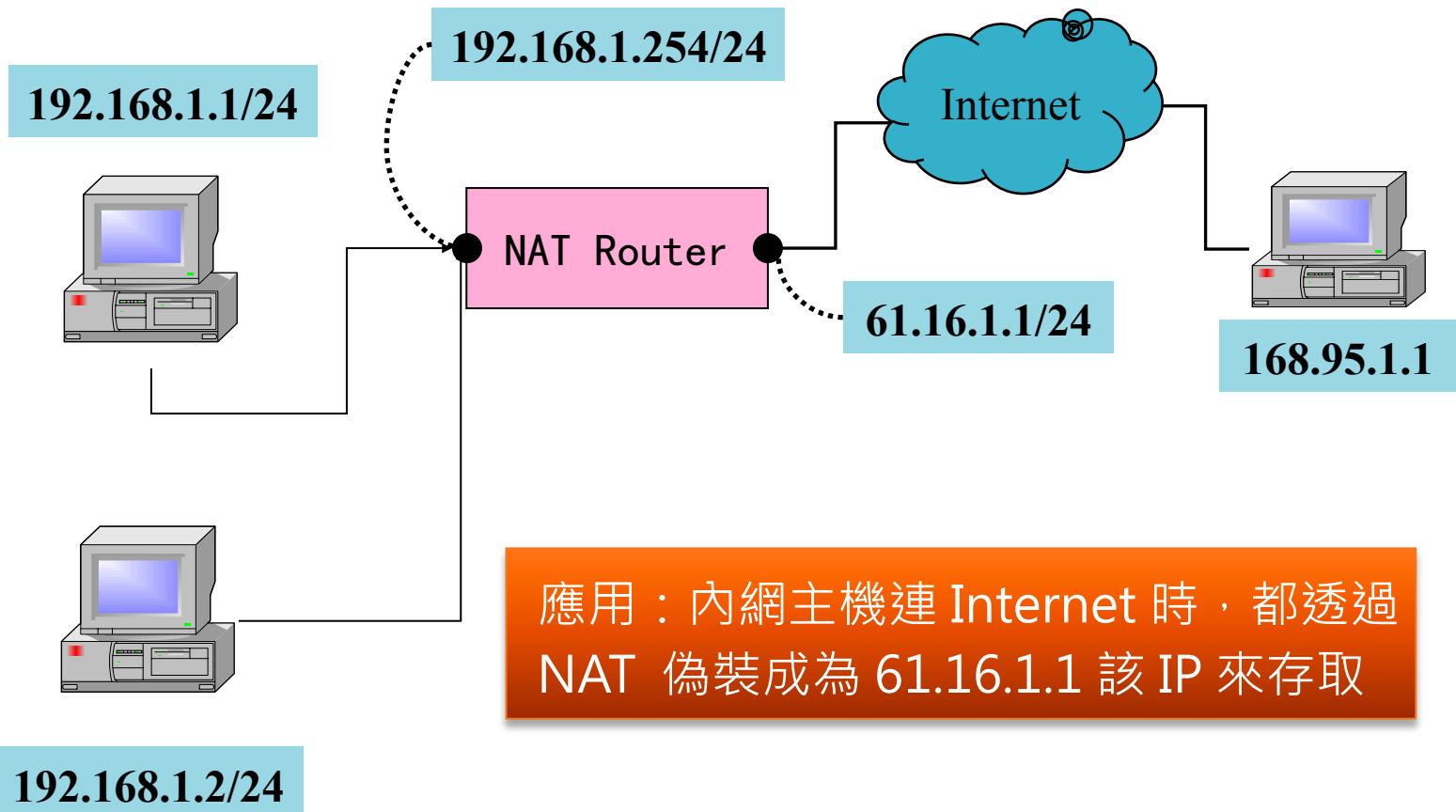
- NAT 與 Private IP
 - 說明
 - 該區段 IP 僅在內部網路使用，不會出現於 internet 環境
 - RFC 1918 內 Private IP 範圍
 - Class A : 10.0.0.0 ~ 10.255.255.255
 - Class B : 172.16.0.0 ~ 172.31.255.255
 - Class C : 192.168.0.0 ~ 192.168.255.255

NAT 功能

- NAT (Network Address Translation)
 - NAT 類型
 - SNAT
 - 提供來源 IP 的改寫轉換
 - 常應用於提供讓沒有 Private IP 以連上 Internet
 - DNAT
 - 提供目的 IP 的改寫轉換
 - 可提供目的轉換功能

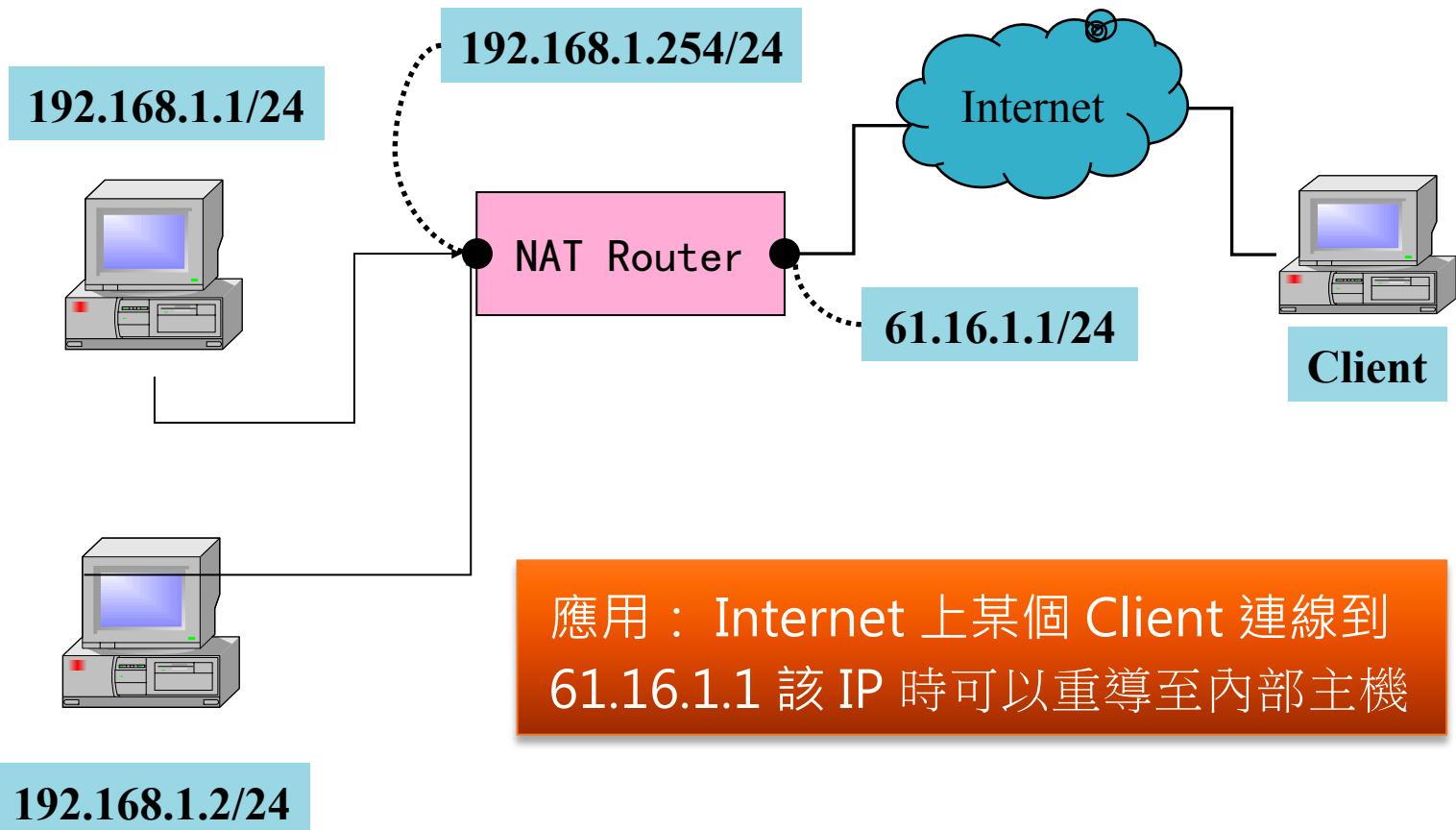
SNAT 功能

- SNAT 示意圖



DNAT 功能

- DNAT 示意圖



IP Forwarding

- Linux Kernel IPv4 Forwarding
 - 說明
 - 控制 Linux 核心底層是否允許封包轉送 (IP Forward) 功能
 - 檔案名稱為 `/etc/sys/net/ipv4/ip_forward`
 - 配置方式
 - 開啟
 - `echo 1 > /proc/sys/net/ipv4/ip_forward`
 - 關閉
 - `echo 0 > /proc/sys/net/ipv4/ip_forward`

IP Forwarding

- Linux Kernel IPv4 Forwarding 與 IPTables
 - 說明
 - 由 iptables 進一步控管是否允許 ip forwarding 功能
 - 設定項目
 - 預設允許封包流通 FORWARD chain
 - iptables -P FORWARD ACCEPT
 - 預設禁止封包流通 FORWARD chain
 - iptables -P FORWARD DROP

IP Forwarding

- Linux Kernel IPv4 Forwarding 與 IPTables
 - IP Forwarding 設定範例 #1
 - `iptables -P FORWARD ACCEPT`
 - `iptables -A FORWARD -s 192.168.1.1 -j DROP`

IP Forwarding

- Linux Kernel IPv4 Forwarding 與 IPTables
 - IP Forwarding 設定範例 #2
 - iptables -P FORWARD DROP
 - iptables -A FORWARD -m state --state ESTABLISHED \
-j ACCEPT
 - iptables -A FORWARD -s 192.168.1.0/24 -j ACCEPT

NAT 的 SNAT 配置

- IPTables 內 SNAT 功能配置
 - 使用語法
 - -j SNAT --to-source ipaddr[-ipaddr][:port-port]
 - -j MASQUERADE
 - 使用事項
 - 搭配於 nat table 內的 POSTROUTING chain 使用

NAT 的 SNAT 配置

- IPTables 內 SNAT 功能配置
 - 說明
 - 使用 MASQUERADE 該 target rule
 - 設定方式
 - echo "1" > /proc/sys/net/ipv4/ip_forward
 - iptables -t nat -A POSTROUTING -o eth0 \
-s 192.168.1.0/24 -j MASQUERADE

NAT 的 SNAT 配置

- IPTables 內 SNAT 功能配置
 - 說明
 - 使用 SNAT 該 target rule
 - 設定方式
 - echo "1" > /proc/sys/net/ipv4/ip_forward
 - iptables -t nat -A POSTROUTING -o eth0 \
-s 192.168.1.0/24 -j SNAT --to <external_ip>

NAT + FTP 架構配置

- IPTables 內 SNAT 環境與 FTP 服務配置
 - 說明
 - NAT 環境下包含先前提到 FTP 傳輸架構問題
 - 可以搭配 `nf_nat_ftp` 該 kernel module 協助處理
 - 主要設定方式
 - `modprobe nf_nat_ftp`
 - `echo "1" > /proc/sys/net/ipv4/ip_forward`
 - `iptables -t nat -A POSTROUTING -o eth0 \ -s 192.168.1.0/24 -j MASQUERADE`

NAT 的 DNAT 配置

- IPTables 內 DNAT 功能配置
 - 說明
 - 提供欲連線至某個目主機，可以改寫其連線目的位址
 - 使用語法
 - `-j DNAT --to-destination ipaddr[-ipaddr][:port-port]`
 - 注意事項
 - 搭配 nat table 內的 PREROUTING 與 OUTPUT chain 使用

NAT 的 DNAT 配置

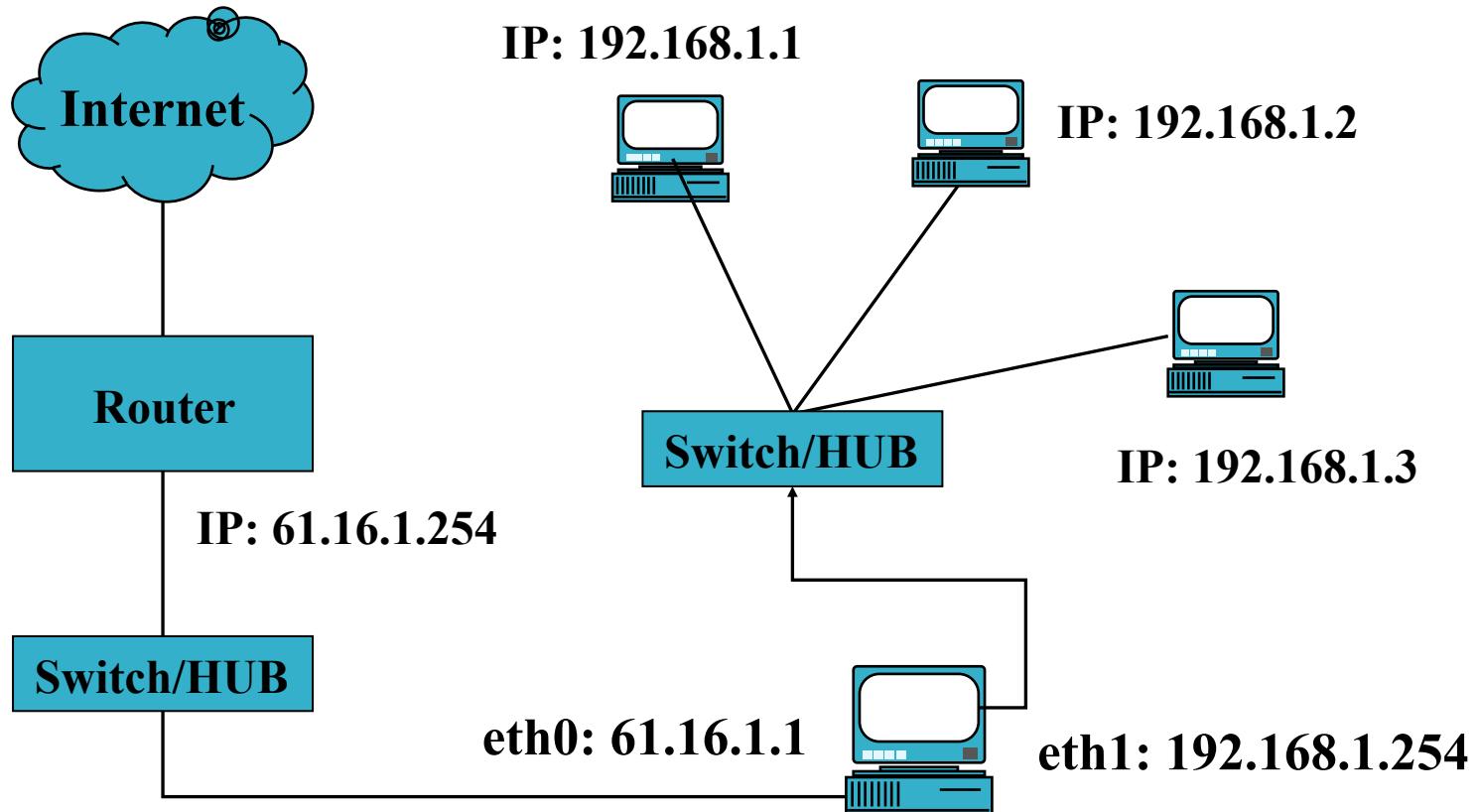
- IPTables 內 DNAT 功能配置
 - 配置設定
 - `iptables -A PREROUTING -t nat -p tcp -d 61.16.1.1 \ --dport 80 -j DNAT --to-destination 192.168.1.100:80`
(外部連線到 61.16.1.1:80 時透過 DNAT 到 192.168.1.100:80)
 - `iptables -A PREROUTING -t nat -d 61.16.1.2 -j \ DNAT --to-destination 192.168.1.101`
(外部連線到 61.16.1.2，改寫 DNAT 到 192.168.1.101)

Transparent Proxy

- **Transparent Proxy (透通代理)**
 - 說明
 - 提供 Client 端不需要特別設定 proxy 組態下都可以經 proxy server 代理方式連外
 - 一般常搭配 NAT 環境下使用

Transparent Proxy

- Transparent Proxy (透通代理) 架構圖



Proxy + NAT Server

Transparent Proxy

- Transparent Proxy (透通代理)
 - squid proxy server 配置
 - 設定檔案 : `squid.conf`
 - 配置設定 : `http_port 3128 transparent`
 - listen port 3128
 - 後面傳入指定 transparent 該 keyword

Transparent Proxy

- Transparent Proxy (透通代理)
 - iptables 調整配置項目
 - echo 1 > /proc/sys/net/ipv4/ip_forward
 - iptables -t nat -A POSTROUTING -o eth0 \
-s 192.168.1.0/24 -j MASQUERADE
 - iptables -t nat -A PREROUTING -p tcp --dport 80 \
-i eth0 -s 192.168.1.0/24 -j REDIRECT \
--to-ports 3128