Firewall(ip6tables)

Chapter 06

主講人: 宜蘭區網中心 陳建宏
電子郵件: joechen@niu.edu.tw

大綱

- iptables與ip6tables 簡介
- 系統環境
- iptables/ip6tables 查詢與清除規則
- 阻擋ipv6 web連線
- 參考資料

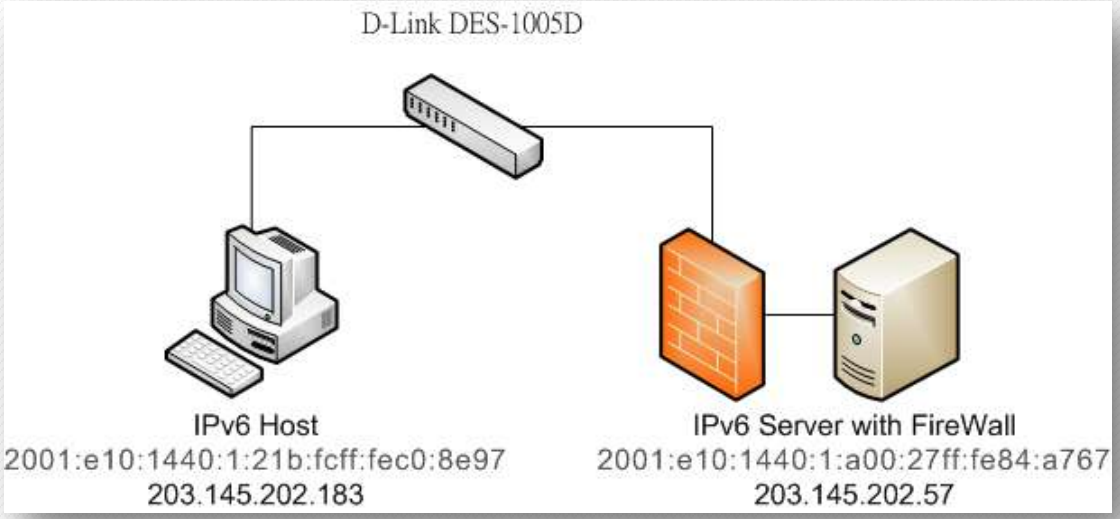
iptables與ip6tables 簡介

- 從 Kernel 2.4 開始，iptables 一直是 Linux 系統中內建的防火牆，不但可以寫入各式各樣的規則，也可以讓我們建立 NAT(Network Address Translation) 網路，實現多台電腦共用一個實體IP上網的模式。
- 在 IPv6 網路中，同樣有一套 ip6tables 可以作為我們電腦的防火牆。
- ip6tables 與 iptables 最大的不同是在於 ip6tables 可以支援 IPv6 的 Address/Prefix 設定，而其他大多數的用法都與iptables 相同，所以對於熟悉 iptables 的用戶，ip6tables 一定可以輕鬆上手。

系統環境

- 系統環境：
  - IPv6 Server with Firewall : CentOS 5.3
  - IPv6 Host: Windows XP
  - Switch：D-Link DES-1005D

- 系統架構圖：



iptables/ip6tables 查詢與清除規則

- 查詢防火牆規則
  - #ip6tables -L
  - 目前防火牆沒有任何規則，預設也都是ACCEPT

```
[root@localhost ~]# ip6tables -L
ip6_tables: (C) 2000-2006 Netfilter Core Team
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
[root@localhost ~]# _
```

iptables/ip6tables 查詢與清除規則

- 清除v6與v4的防火牆規則
  - #ip6tables -F
  - #ip6tables –X
  - #ip6tables –Z
  - #iptables –F
  - #iptables –X
  - #iptables -Z

```
[root@localhost ~]# ip6tables -F
[root@localhost ~]# ip6tables -X
[root@localhost ~]# ip6tables -Z
[root@localhost ~]# iptables -F
[root@localhost ~]# iptables -X
[root@localhost ~]# iptables -Z
[root@localhost ~]# _
```

iptables/ip6tables 查詢與清除規則

- 查詢v6規則
  - #ip6tables -L

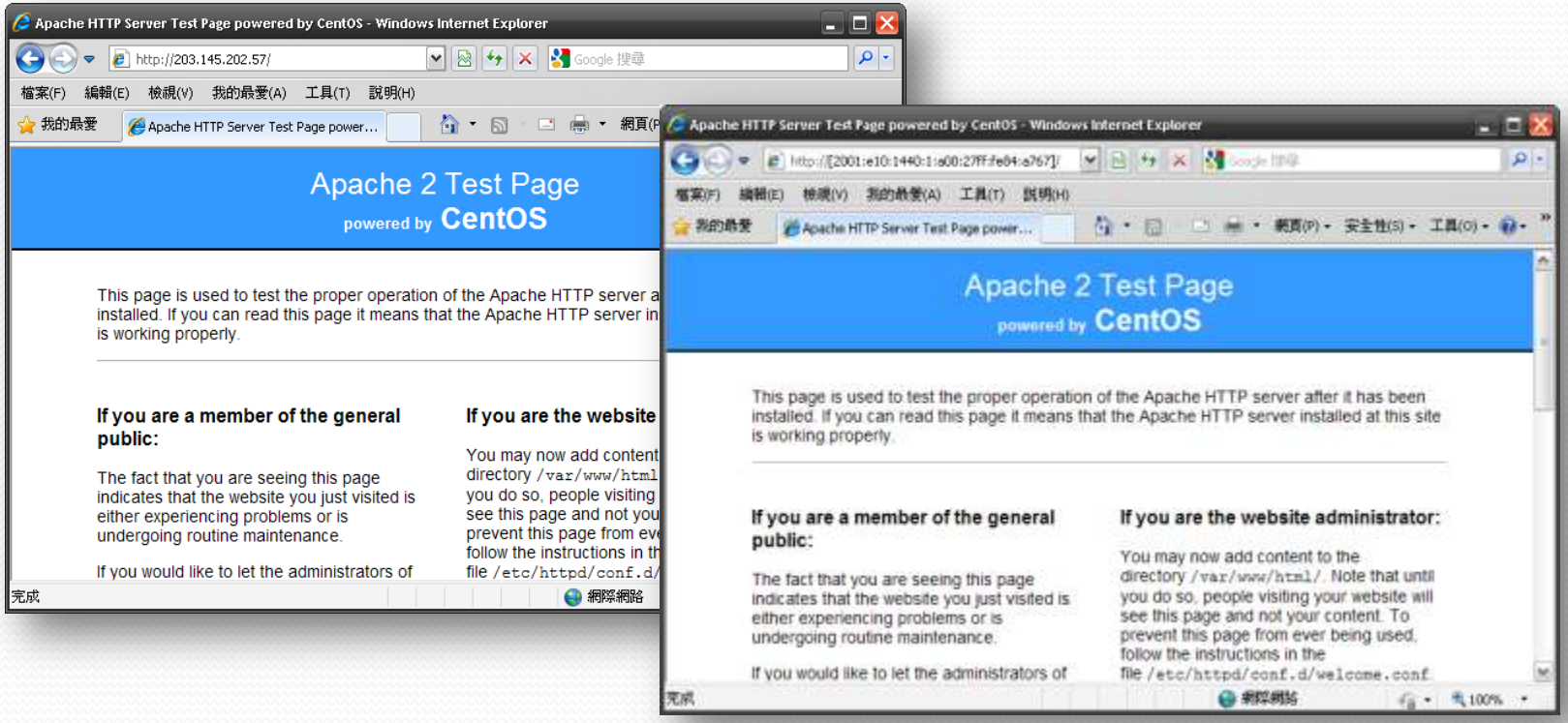
```
[root@localhost ~]# ip6tables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination

Chain RH-Firewall-1-INPUT (0 references)
target     prot opt source               destination
[root@localhost ~]# _
```

- 查詢v4原則
  - #iptables -L

```
[root@localhost ~]# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination

Chain RH-Firewall-1-INPUT (0 references)
target     prot opt source               destination
[root@localhost ~]# _
```

阻擋ipv6 web連線

- 在清除完IPv4與IPv6的防火牆規則後，以下示範如何鎖定IPv6的網頁瀏覽
  - 先確認 IPv4 與 IPv6 皆可瀏覽網頁

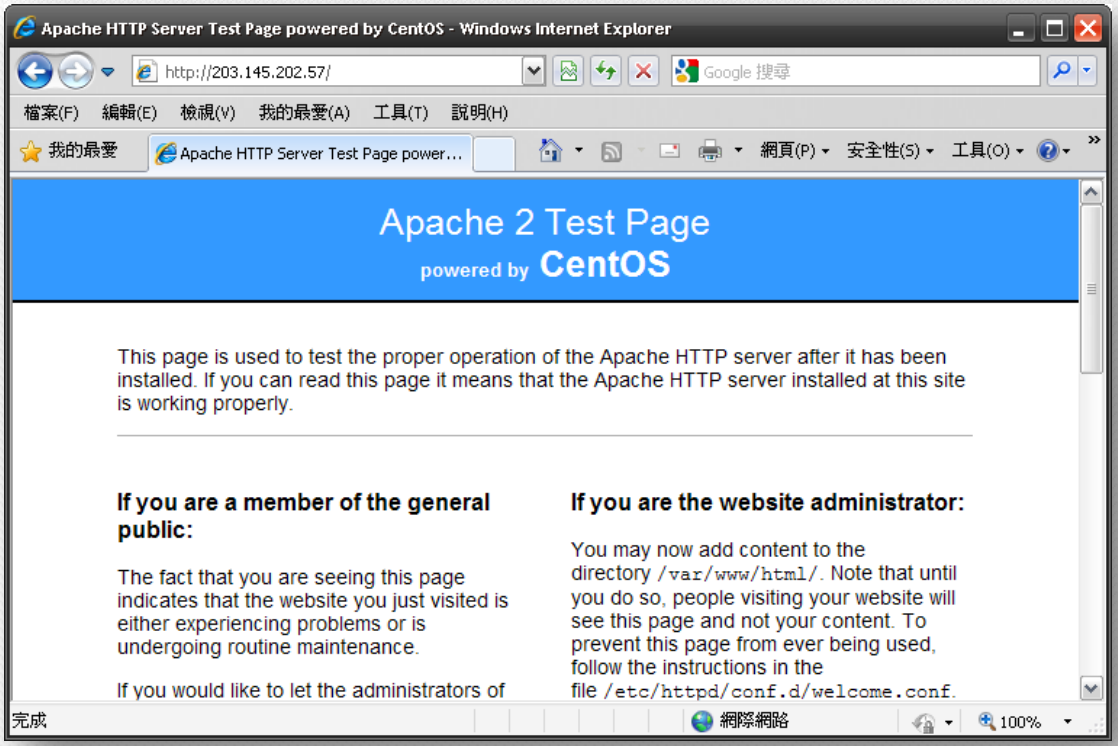


阻擋ipv6 web連線

- 在確認都可以正常連線後，在ip6tables加入一條規則
  - #ip6tables –A INPUT –i eth0 -p tcp --dport 80 -j DROP
    - -A 代表新增一條規則
    - INPUT 代表要設定的chain
    - -i 代表輸入的介面
    - -p 代表通訊協定
    - --dport 為目的端 port
    - -j 則是符合規則所採取的行動

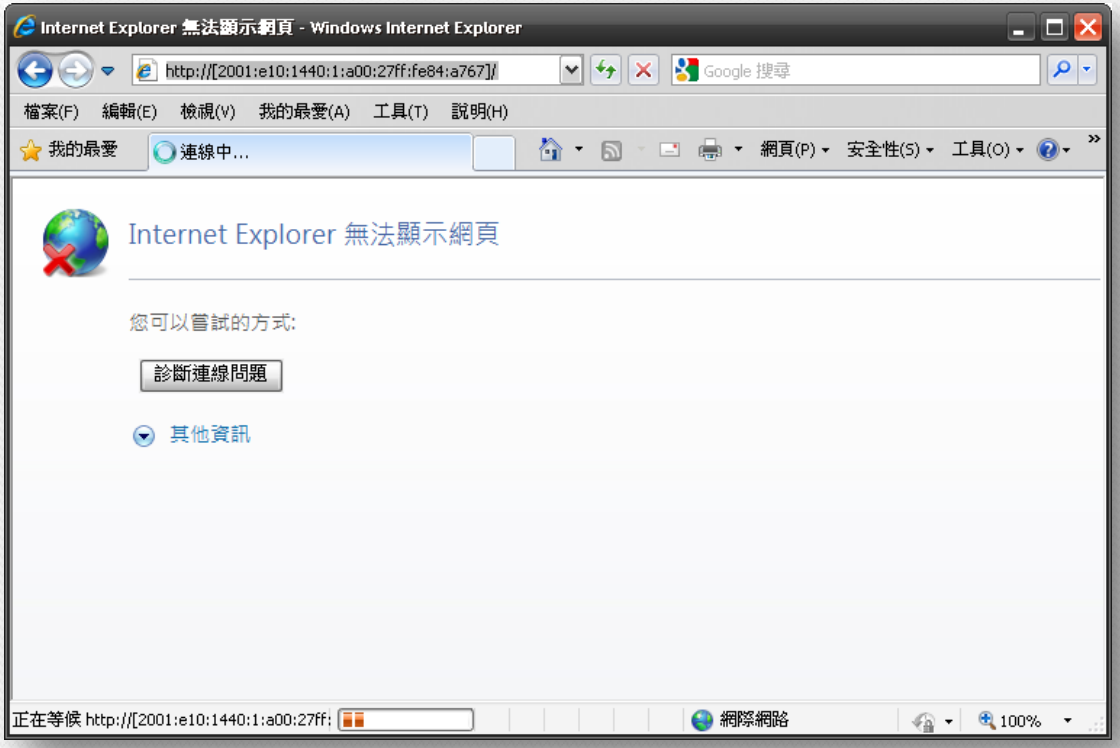
阻擋ipv6 web連線

- 設定完成後，再次以IE瀏覽器連接IPv4與IPv6的頁面
- IPv4還是可以正常連線



阻擋ipv6 web連線

- 而IPv6則無法連線了，確認防火牆已生效



參考資料

- http://linux.vbird.org/linux_server/0250simple_firewall.php

END