### Firewall(ip6tables) Chapter o6

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





### 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 protopt source	destination
Chain OHTPHT (nolicy ACCEPT)	
target mot out source	destination
[mootflocalhost ~1#	

### 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 [root0localhost ~]# _	destination

#### • 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 [root0localhost ~]# _	destination



- 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

🥖 Apache	HTTP Server Test Page powered by CentOS - Windows	Internet Explorer		
▲案(F) 約	を 2015年1月11日の11日の11日の11日の11日の11日の11日の11日の11日の11	🖌 🖄 🍑 🗙 🎦 Google 搜尋		
🔶 我的最新	E 🏉 Apache HTTP Server Test Page power	🟠 🔹 🗟 🐘 🖃 🖶 🝷 網頁(P	C Apache HTTP Server Test Page powered by Cent05 - Windows Internet Explorer	i 🗉 🖬 🐹
	Apache 2 powered by	Test Page CentOS	<ul> <li>(○) ● (●) https://[2001:e10:1440:1:e00:27ff#e84-e767]) ● (● **) × (▲ ==========</li> <li>(○) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ● (●) ●</li></ul>	• م ۱۹(0) • 🕡 • "
	This page is used to test the proper operation installed. If you can read this page it means the sworking properly.	n of the Apache HTTP server a nat the Apache HTTP server in	Apache 2 Test Page powered by CentOS	<u>^</u>
	If you are a member of the general public:	<b>If you are the website</b> You may now add content	This page is used to test the proper operation of the Apache HTTP server after it has bee installed. If you can read this page it means that the Apache HTTP server installed at this is working properly.	n site
	The fact that you are seeing this page indicates that the website you just visited is either experiencing problems or is undergoing routine maintenance.	directory /var/www/html you do so, people visiting see this page and not you prevent this page from eve follow the instructions in th	If you are a member of the general If you are the website administrat public:	or:
完成	If you would like to let the administrators of	file /etc/httpd/conf.d/	The fact that you are seeing this page indicates that the website you just visited is either experiencing problems or is undergoing routine maintenance. If you would like to let the administrators of	ntii ntii
			元成 🥥 素料(初始) 🖓	• 💐 100% •

2009/12/10



- 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

• 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





• 而IPv6則無法連線了,確認防火牆已生效

🥖 Internet Explorer 無法顕示網頁 - Wi	ndows Internet Explore		_ 🗆 🔀
🔆 🔆 🗢 🙋 http://[2001:e10:1440:	1:a00:27ff:fe84:a767]/	🖌 🐓 🗙 🚼 Google 搜尋	
檔案(F) 編輯(E) 檢視(V) 我的最愛	A) 工具(T) 說明(H)		
🙀 我的最愛 🔘 連線中		🚹 🔹 🔝 👘 🖃 🍓 💌 網頁(P) 🕶	安全性(5) ▼ 工具(0) ▼ 🕢 ▼ 🎽
Internet Explore	- 無法顯示網頁		
您可以嘗試的方式:			
診斷連線問題			
反 其他資訊			
) 正在等候 http://[2001:e10:1440:1:a00:27ff]		😜 網際網路	🖓 🕶 🎕 100% 👻 🚊



#### http://linux.vbird.org/linux\_server/0250simple\_fire wall.php





## END



