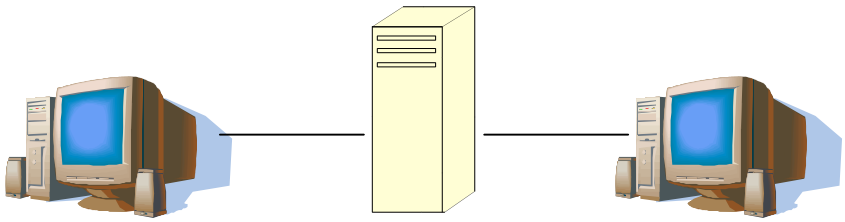
Linux Transparent Firewall架設完全攻略

文@Lawrence Chiu
Document Version: 0.2
Date: 2007/04/13

前言:
很多時候，在不想變動原本的網路架構下，如果有需要將網路隔離開時，就需用到透通式的防火牆，所謂的透通式的防火牆它是個in-line mode的裝置，你可以把它想成是一個Bridge裝置，但確有可以過濾封包的功能，提醒一下既然是Bridge裝置，當然它就是屬於Layer 2那一層囉!

Environment:
以下是筆者所測試的環境:



Server IP address: 192.168.1.100
Client IP address: 192.168.1.200
Firewall IP address: 192.168.1.1

Objective:
只允許Server可以透過網芳將檔案傳送到Client端（單向），Server與Client可互相透過icmp echo request確認彼此間的連線 (雙向)。

Setup Procedure:

1.Bind兩張網卡成一個bridge interface:
Firewall至少要有兩張網卡，然後只要將它們bind起來，Firewall就可以成了一個Bridge裝置。首先要安裝bridge-utils與bridge-utils-devel這兩個套件，這兩個套件可以把eth0與eth1 bind成一個bridge裝置，正好符合我們以上的需求，筆者是用RHEL4.4架設的，非常方便的是這兩個套件在安裝光碟裡面就有。

```
# rpm –ivh bridge-utils-*
```

緊接著將eth0與eth1 bind成bri0 interface.

```
# ifconfig eth0 0.0.0.0
# ifconfig eth1 0.0.0.0
# brctl addbr bri0
# brctl addif bri0 eth0
# brctl addif bri0 eth1
```

執行brctl show確認一下:

```
# brctl show
bridge name     bridge id               STP enabled     interfaces
bri0            8000.00034730c5b3       no              eth0
                                                        eth1
```

好了問題來了，既然bri0 interface已經建置好了，那麼是否可以在上面設定IP呢？答案當然是可以的囉～不然怎麼remote control它呢? 至於設定的方法有兩種，一種是設定Static IP，另一種是透過DHCP Server get到IP,以下是設定的方法:

Static IP:

```
# ifconfig bri0 192.168.1.1 netmask 255.255.255.0 up
```

DHCP Client:

```
# dhclient bri0
```

以上的所有動作您可以把它寫成一個shell script file，並讓它在開機時自動執行，以RHEL的話是放在/etc/rc.local，順便一提SLES是/etc/init.d/boot.local

2. Allow IP forwarding

```
# vi /etc/sysctl.conf
# Controls IP packet forwarding
net.ipv4.ip_forward = 1
#sysctl –p
```

請測試一下，目前Server與Client的網路是相通的。

3. 設定Policy

重頭戲來了，如何設定Policy? 一般來說Linux firewall的設定是透過iptables，iptables預設分為3個table，5個chain，我要把rule設定在那個table及那個chain是一開始該有的認知。先提醒一個觀念，iptables比對的順序為mangle->nat->filter，這是什麼意思？事實上mangle,nat與filter就是預設的三個table，若前面的規則是allow，到了後面的table卻是deny的話，那就是deny! 反之若前面是deny而後面是allow的話，那就是allow! 這是套用於不同

table時，規則相互抵觸時的法則，想一想有沒有可能在相同的chain中，設定相互抵觸的規則？當然是有可能的囉！這時是first match! 當hit到規則後，則不再進行比對，這點請特別注意！

可以確定的是，利用filter table就可以設定我們的policy，接下來考慮一下要設定在那個chain? INPUT OUTPUT FORWARD? 答案是 FORWARD，別忘了！它是個Bridge裝置，封包當然是透過eth0到eth1或是eth1到eth0囉！

為了最高安全指導原則，首先要把 FORWARD default policy設定為DROP，只放行SMB protocol與icmp echo request.

```
# iptables –P FORWARD DROP
```

測試一下 Server與Client目前應該是完全不通!

設定允許n個封包之後的連線:

```
# iptables –A FORWARD –m state –state RELATED,ESTABLISHED –j ACCEPT
```

設定允許icmp echo request:

```
# iptables –A FORWARD –s 192.168.1.0/24 –p icmp –icmp-type 8 –j ACCEPT
```

設定只有Server可以透過網芳將檔案傳送到Client:

```
# iptables –A FORWARD –s 192.168.1.100/32 –d 192.168.1.200/32 –p tcp –dport 139 –j ACCEPT

# iptables –A FORWARD –s 192.168.1.100/32 –d 192.168.1.200/32 –p tcp –dport 445 –j ACCEPT
```

這樣一來便可達到我們的需求！

筆者簡介:
Lawrence Chiu – 已取得RHCE與NCLP認證，曾任職於D-Link testing engineer，現任職於TrendMicro Anti-Spam Lab administrator。