7 CentOS7中預設的防火牆firewalld

如果曾經用過CentOS6或是更早之前的版本,應該會知道原本預設的防火牆是使用一個稱為iptables的程 式,而在CentOS7中則變成了firewalld□當然你還是可以裝回iptables繼續使用,不過如果你是還沒學過使 用iptables的人,先從firewalld下手應該會比較容易一點。

7.1 iptables與firewalld

iptables - 維基百科

firewalld - TWNIC 2015電子報

在以前,如果是使用iptables來管理防火牆的話,一般來說要編輯一份iptables的設定檔,所以的防火牆規 則都記錄在裡面,每次編輯之後都要重新套用。當然也是有圖形化或是其他管理介面可以來協助我們,不 過如果學會使用firewalld也只是幾行指令就可以解決的事。

7.2 firewalld設定指令

在firewalld中有幾個區域的規則組,分別是:

- drop 最低等級的信任,任何對內的請求都被丟棄不回覆,只開放對外傳輸。
- block 與上面類似,不過是使用icmp-host-prohibited或是icmp6-adm-prohibited□拒絕傳入的請求。
- public 公開的區域,大部分的連線設定都在這裡,只開放我們所允許連線接入。
- external 如果您使用防火牆作為網關,則為外部網路,適用於NAT環境。
- internal 提供信任的電腦,與一些額外的服務。
- dmz 用於DMZ中, 僅與許部分的連線接入
- work 用於工作的機器,信任大部分的電腦並提供更多的服務。
- home 用於家庭網路,信任大部分的電腦並提供更多的服務。
- trusted 信任所有電腦的網路連線,須謹慎使用。

首先先確認firewalld是否已經安裝並啟用,接下來可以用firewall-cmd來查詢或編輯防火牆設定。

[root@localhost cbb104026]# firewall-cmd --get-default-zone #顯示預設提供的區 域(zone)

block dmz drop external home internal public trusted work

[root@localhost cbb104026]# firewall-cmd --zone=block --list-all #列出block 區域內容

block

target: %%REJECT%%

icmp-block-inversion: no

interfaces: sources:

Jun Wu的教學網頁 國立屏東大學資訊工程學系

CSIE. NPTU Total: 233018

https://junwu.nptu.edu.tw/dokuwiki/

```
services:
 ports:
 protocols:
 masquerade: no
 forward-ports:
 source-ports:
 icmp-blocks:
 rich rules:
[root@localhost cbb104026]# firewall-cmd --list-all-zones #列出所有區域內容
[root@localhost cbb104026]# firewall-cmd --get-active-zones #列出運作中的區域
public
 interfaces: enp0s3
[root@localhost cbb104026]# firewall-cmd --get-services #列出所有支援的服務
[root@localhost cbb104026]# firewall-cmd --zone=public --permanent --add-
service=http #永久添加我們需要的服務規則
success
[root@localhost cbb104026]# firewall-cmd --zone=public --permanent --list-
services #列出public中永久允許的服務
[root@localhost cbb104026]# firewall-cmd --zone=public --permanent --add-
port=2001/tcp #允許指定連接埠
[root@localhost cbb104026]# firewall-cmd --zone=public --permanent --add-
port=2000-2100/udp #允許指定連接埠範圍
[root@localhost cbb104026]# firewall-cmd --zone=public --permanent --list-
ports #列出public中永久允許連接埠
```

那麼要怎麼樣移除防火牆規則呢?很簡單,我們怎麼新增(add)∏就怎麼移除(remove)∏

最後不要忘了重啟firewalld生效

[root@localhost cbb104026]# service firewalld restart

詳細參考資料

From:

https://junwu.nptu.edu.tw/dokuwiki/ - **Jun Wu**的教學網頁國立屏東大學資訊工程學系

CSIE. NPTU

Total: 233018

Permanent link:

https://junwu.nptu.edu.tw/dokuwiki/doku.php?id=linux:firewalld

Last update: 2019/07/02 15:01

