iptables-透過ipset by國別阻擋

版本修訂記錄

|  |  |  |  |
| --- | --- | --- | --- |
| 版本編號 | 修訂人 | 修訂內容 | 修訂日期 |
| 0.1 |  |  | 2019/10/15 |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

內容

[主題 一-1](#_Toc257879348)

[一、 序言 一-1](#_Toc257879349)

[二、 內容 二-1](#_Toc257879350)

# 序言

# 內容

參考網址: <https://4xc.cc/linux/centos7-uses-ipset-to-quickly-block-ip-access-to-specified-countries.html>

ipset是iptables的擴展，它允許你創建匹配整個IP位址集合的規則。可以快速的讓我們遮罩某個IP段。這裡分享個遮罩指定國家訪問的方法，有時候還可以有效的幫網站阻擋下攻擊。

1. 從[http://www.ipdeny.com/ipblocks/](https://4xc.cc/go/aHR0cDovL3d3dy5pcGRlbnkuY29tL2lwYmxvY2tzLw==" \t "_blank)  取得國家網段
2. 安裝ipset

**yum** -y install ipset

1. 可透過firewalld 或 iptables 實現

因為目前部分cdn中轉機可能無法使用firewalld+ipset實現

改使用iptables+ipset步驟如下:

1.停用firewalld 安裝iptables

systemctl disable firewalld

systemctl mask firewalld

systemctl stop firewalld

yum install iptables-services

複製iptables 及 ipset\_twlist至/etc/sysconfig

或執行create\_ipsetlist.sh 產生新的 ipsetlist於 /etc/sysconfig/ipset\_twlist

iptables <-為iptables 規則配置檔

**#allow office & jumpsvr**

-A INPUT -p tcp -m state --state NEW -m tcp -s 61.220.186.5 -j ACCEPT

-A INPUT -p tcp -m state --state NEW -m tcp -s 34.92.211.206 -j ACCEPT

**# allow zabbix serve**r

-A INPUT -p tcp -m state --state NEW -m tcp -s 182.16.84.198 --dport 10050 -j ACCEPT

-A INPUT -p tcp -m state --state NEW -m tcp -s 182.16.84.212 --dport 10050 -j ACCEPT

**#block twip to tcp:80,443,8068**

-A INPUT -m set --match-set twblocks src -p tcp -m multiport --dport 80,443,8068 -j DROP

**#allow service port**

-A INPUT -p tcp -m multiport --dport 80,443,6780,8058,8068,8078,8085,8086,8087,9080,9087 -m state --state NEW -j ACCEPT

ipset\_twlist IP清單

use\_ipset.sh <- 載入 ipset配置與執行iptables規則

設置 /etc/rc.local 開機執行

chmod 775

/usr/local/sbin/use\_ipset.sh