写一个脚本解决DOS攻击生产案例

提示：根据web日志或者或者网络连接数，监控当某个IP并发连接数或者短时内PV达到100，即调用防火墙命令封掉对应的IP，监控频率每隔3分钟。防火墙命令为：iptables -I INPUT -s 10.0.1.10 -j DROP。

#!/bin/bash

source /etc/profile

iplist=`netstat -ntu | awk '{print $5}'| cut -d':' -f1| sort |uniq -c | sed 'N;$d;P;D' | awk '{if($1>100)print $2}'`

for ip in $iplist

do

iptables -I INPUT -s $ip -j DROP

echo "$ip is drop!"

done

crontab -e

\*/3 \* \* \* \* /bin/bash 上面脚本的路径