需求四

**根据需求三最后的识别结果采取封锁恶意IP的防控措施。再针对不同类型攻击的特征对服务器进行相应的防护，及时存储相关防御日志，日志详细可溯源，并通过邮件等方式通知相关安全人员。构建起防御措施后要对网站服务器性能进行监控。**

需求4.1：针对各种攻击采取防御措施

根据需求三神经网络模型的识别结果采取封锁恶意攻击IP的防控措施。针对不同类型攻击的特征对服务器进行相应的防护，及时存储相关防御日志，日志详细可溯源，并通过邮件等方式通知相关安全人员。

1. 封锁恶意攻击IP

1. CentOS 7下使用 iptables 代替 FireWall 防火墙：

关闭 FireWall：

systemctl stop firewalld.service

systemctl disable firewalld.service

安装 iptables：

yum install iptables-services

systemctl restart iptables.service

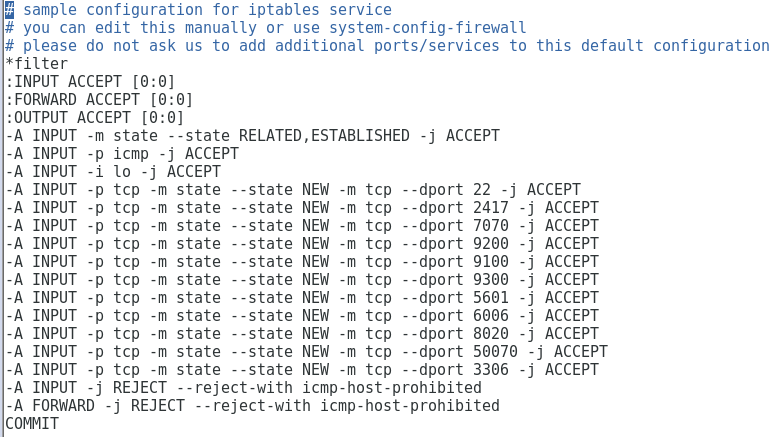
systemctl enable iptables.service

2. 开启访问端口：

vim /etc/sysconfig/iptables

添加需要开放的服务端口：

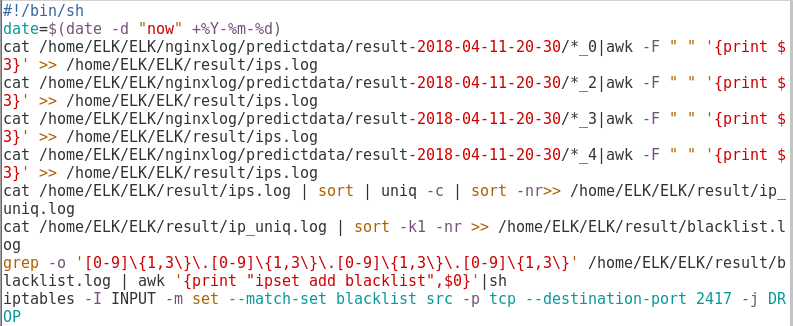
-A INPUT –p tcp –m state –state NEW –m tcp –dport 2417 –j ACCEPT



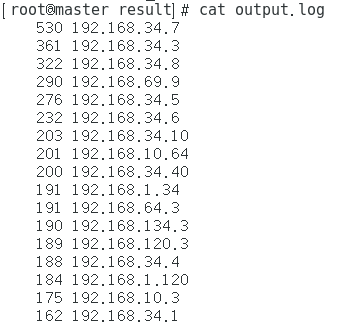
3. 重启防火墙使配置生效:

systemctl restart iptables.service

4. 编写intercept.sh脚本收集神经网络识别出的恶意IP



收集到的恶意攻击IP如下，左边一列为该IP出现次数。



5. intercept.sh脚本将恶意IP加入iptables

安装ipset：yum install ipset

创建一个名称为 blacklist 的IP集合，最大容量为10000

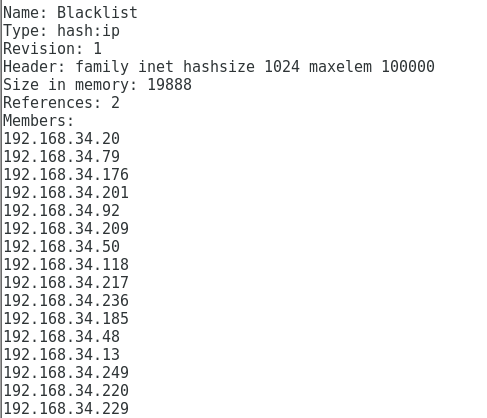
ipset create blacklist hash:ip maxelem 100000

将恶意IP导入到ipset中

grep -o '[0-9]\{1,3\}\.[0-9]\{1,3\}\.[0-9]\{1,3\}\.[0-9]\{1,3\}' output.log | awk '{print "ipset add blacklist",$0}'|sh

导入ip后查看ipset的恶意ip列表

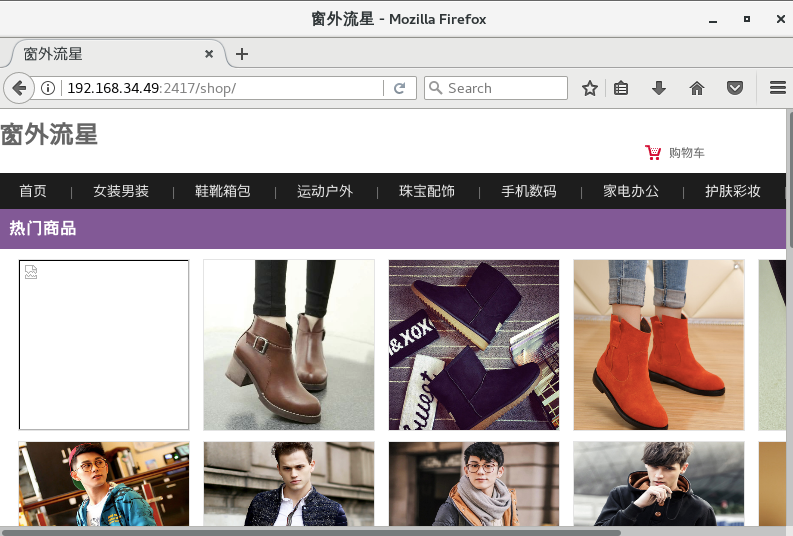
ipset list



intercept.sh脚本还将ipset与iptables关联，禁止黑名单IP访问2417端口。

iptables -I INPUT -m set --match-set blacklist src -p tcp --destination-port 2417 -j DROP

效果如下：原先可以正常访问页面：



当IP加入到防火墙黑名单之后，该IP无法访问网站：



1. 配置邮件告警

1） 安装过程：

1. 关闭 SELINUX；

2. CentOS 7 下使用 iptables 代替 FireWall 防火墙：

3. 更新系统：

yum -y update

4. 安装邮件系统mailx：

yum install -y mailx

1. 创建符号链接

为了创建符号链接，运行以下命令（用/bin/email所需的链接名称替换）：

ln -s /bin/mailx /bin/email

1. 外部邮件服务器转接

可以选择通过外部SMTP服务器（即您的电子邮件提供商或商业电子邮件服务）转发邮件，vim /etc/mail.rc，加入如下配置

# set smtp=smtp://smtp.server.tld:port\_number

set smtp=smtp.126.com

# tell mailx that it needs to authorise

set smtp-auth=login

# set the user for SMTP

# set smtp-auth-user=user@domain.tld

set smtp-auth-user=chenjiale1997627@126.com

# set the password for authorisation

set smtp-auth-password=root2417（此处的密码为126邮箱的客户端授权密码，需要提前开启并设置）

从现在开始，所有发送的邮件都将使用您刚刚设置的配置进行中继。

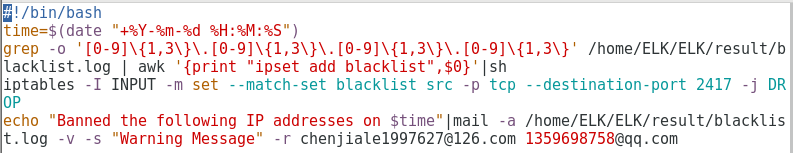
1. 测试

测试办法：echo "Test" | mail -s "Message subject" -r chenjiale1997627@126.com 1359698758@qq.com -r表示电子邮件的发件人地址

（若报错smtp-server: 535 Error: authentication failed则因为smtp-auth-password没有写对应客户端授权密码）

1. 实现邮件告警：
2. 编写warning.sh脚本

功能是将IP黑名单关联防火墙封杀并将黑名单发送给管理员



1. 安装触发工具incrontab

yum install incron

1. 开启触发工具

incrond start

1. 编写触发任务

/home/ELK/ELK/result/blacklist IN\_MODIFY /root/Desktop/warning.sh

说明在/home/ELK/ELK/result/blacklist写关闭后即执行warning.sh脚本。

1. 邮件告警效果



1. 防御DDOS攻击

使用工具：

Ddos-deflate，ddos-deflate是一个Shell脚本，它通过netstat监测跟踪创建大量网络连接的IP地址，在检测到某个结点超过预设的限制时，程序会通过APF或IPTABLES禁止或阻挡这些IP。

1） 安装过程：

1. 关闭 SELINUX；
2. CentOS 7 下使用 iptables 代替 FireWall 防火墙：

关闭 FireWall：

systemctl stop firewalld.service

systemctl disable firewalld.service

安装 iptables：

yum install iptables-services

systemctl restart iptables.service

systemctl enable iptables.service

1. 更新系统：

yum -y update

1. 安装邮件系统mailx：

yum install -y mailx

1. 创建符号链接

为了创建符号链接，运行以下命令（用/bin/email所需的链接名称替换）：

ln -s /bin/mailx /bin/email

1. 外部邮件服务器转接

可以选择通过外部SMTP服务器（即您的电子邮件提供商或商业电子邮件服务）转发邮件，vim /etc/mail.rc，加入如下配置

# set smtp=smtp://smtp.server.tld:port\_number

set smtp=smtp.126.com

# tell mailx that it needs to authorise

set smtp-auth=login

# set the user for SMTP

# set smtp-auth-user=user@domain.tld

set smtp-auth-user=chenjiale1997627@126.com

# set the password for authorisation

set smtp-auth-password=root2417（此处的密码为126邮箱的客户端授权密码，需要提前开启并设置）

从现在开始，所有发送的邮件都将使用您刚刚设置的配置进行中继。

1. 测试

测试办法：echo "Test" | mail -s "Message subject" -r chenjiale1997627@126.com [1359698758@qq.com](mailto:1359698758@qq.com) -r表示电子邮件的发件人地址

（若报错smtp-server: 535 Error: authentication failed则因为smtp-auth-password没有写对应客户端授权密码）

#!/bin/bash

time=$(date "+%Y-%m-%d %H:%M:%S")

echo "Banned the following IP addresses on $time"|mail -a /root/Desktop/ip.txt -v -s "Warning Message" -r chenjiale1997627@126.com 1359698758@qq.com

/root/Desktop/test.log IN\_MODIFY /root/Desktop/warning.sh

即说明在/var/www/proftp-user.sh写关闭后即执行incron-proftp.sh脚本。

1. 下载防DDOS攻击工具

wget -q -O - https://raw.githubusercontent.com/Amet13/ddos-deflate/master/install.sh | bash

1. 编辑配置文件：

vim /usr/local/ddos-deflate/ddos-deflate.conf

NO\_OF\_CONNECTIONS=500

EMAIL\_TO="1359698758@qq.com "

BAN\_PERIOD=60

CUSTOM\_PORTS=":80|:443:|:53|:21"

ENABLE\_LOG=YES

1. 编辑脚本文件：

将cat $BANNED\_IP\_MAIL | mail -s "IP addresses banned on $dt" $EMAIL\_TO

修改为：

cat $BANNED\_IP\_MAIL | mail -s "IP addresses banned on $dt" –r [chenjiale1997627@126.com](mailto:chenjiale1997627@126.com) $EMAIL\_TO

保存并退出。

1. Ddos-deflate测试过程：
2. 首先实现同网段两台机器之前可以相互ping通：

第一台运行

ifconfig eth0 本地IP netmask 255.255.255.0 up

第二台运行

ifconfig eth0 本地IP netmask 255.255.255.0 up

之后就可以ping通。

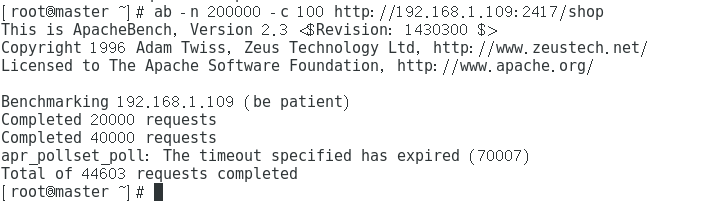
1. 将Ddos-deflate所在主机的iptables.service关闭。

systemctl stop iptables.service

1. 在一台机子上运行指令：

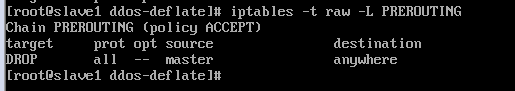
ab -n 200000 -c 100 <http://192.168.1.109>:2417/shop

如下：



1. 在被攻击机子上查看防火墙：

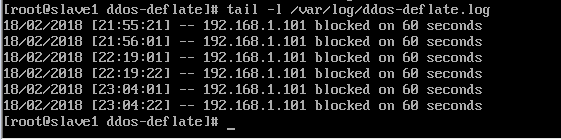
iptables -t raw -L PREROUTING



可以看到iptables将IP源给DROP封锁了

1. 检查日志：

tail -1 /var/log/ddos-deflate.log



日志中记录了IP源攻击时间，并且该IP已经被DROP封锁了。

1. 邮件告警：



邮件中显示攻击源IP攻击时间，并且显示该IP已经被DROP封锁了。

三． 防御慢链接攻击

1. 限制周期内统计报文数量

一个TCP连接，HTTP请求的报文中，报文过多或者报文过少都是有问题的，如果一个周期内报文数量非常少，那么它就可能是慢链接攻击。

2. 检查日志，查找类似的错误报警

[error] server reached MaxClients setting, consider raising the MaxClients setting

看看有没有被这种攻击锁定。

3. 限制HTTP头部传输的最大许可时间：

超过指定时间HTTP Header还没有传输完成，直接判定源IP地址为慢链接攻击，中断连接并加入黑名单。

四． 防御撞库攻击

1. 限制同一个IP的请求次数和请求频率；
2. 使用cookie，flash cookie以及帆布指纹等方法；
3. 可以通过增强登录入口识别能力的方法来提高登录入口的安全性，如图片验证码、文字验证码等，提高验证码生成的强度。

五．防御爆破攻击

1. 定期修改管理员密码；

2. 设置IP信誉库，拒绝频繁访问账户请求以及匿名账户登录请求等。

需求4.2：网站服务器性能监控

当网站防御体系构建起来之后，使用Zabbix对网站服务器性能进行监控。具体可以分为在无攻击无拦截、有攻击无拦截和有攻击有拦截等三场景下，对服务器CPU、内存占用率、出入网流量、用户交互时间、正常用户请求时间、响应时间等指标的监控。监控需要进行实测。

1. 网站服务器监控指标

监控网站服务器性能的方式分为两大类：内部监控和外部监控。通过性能指标的表现形式，分析网站性能是否稳定。外部监控会监控所有web资源参数。可监控指标如下：

网站响应时间（分析性能是否稳定）

平均网页加载时间

网页功能

Web页面和场景压力测试

真实用户监控

API监控

内部监控本地设备的性能。可监控指标如下：

网络带宽吞吐量、吞吐率

服务器CPU、内存和驱动器利用率

磁盘空间

网络接口所消耗的带宽

不同的系统进程

系统事件

应用服务器的日志

1. 网站服务器监控工具

Zabbix是一个基于WEB界面的提供分布式的系统监视以及网络监视功能的企业级的解决方案。能监视各种网络参数，保证服务器系统的安全运营；并提供灵活的通知机制以让系统管理员快速定位、解决存在的各种问题。

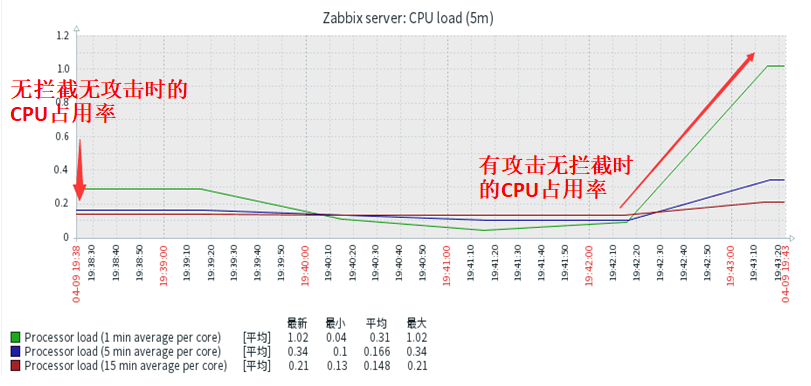
Zabbix主要监控指标：CPU负荷、内存使用、磁盘使用、网络状况、端口监视、流量监视等。

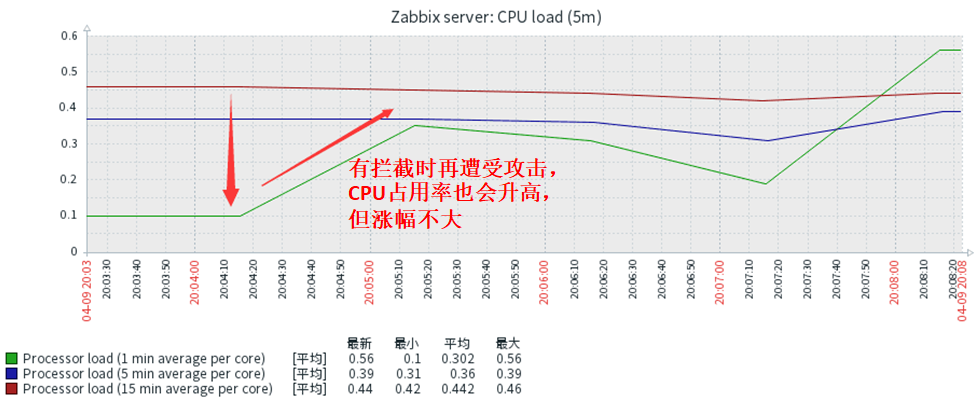
三、 网站服务器性能监控的局限性

由于本项目搭建的网站本身只是一个模拟的网站，响应报文和并发性能可能不符合实际要求。此外，由于不是真实服务器环境，很难模拟大数量请求来测试网站性能，如5000个正常用户的并发访问请求。

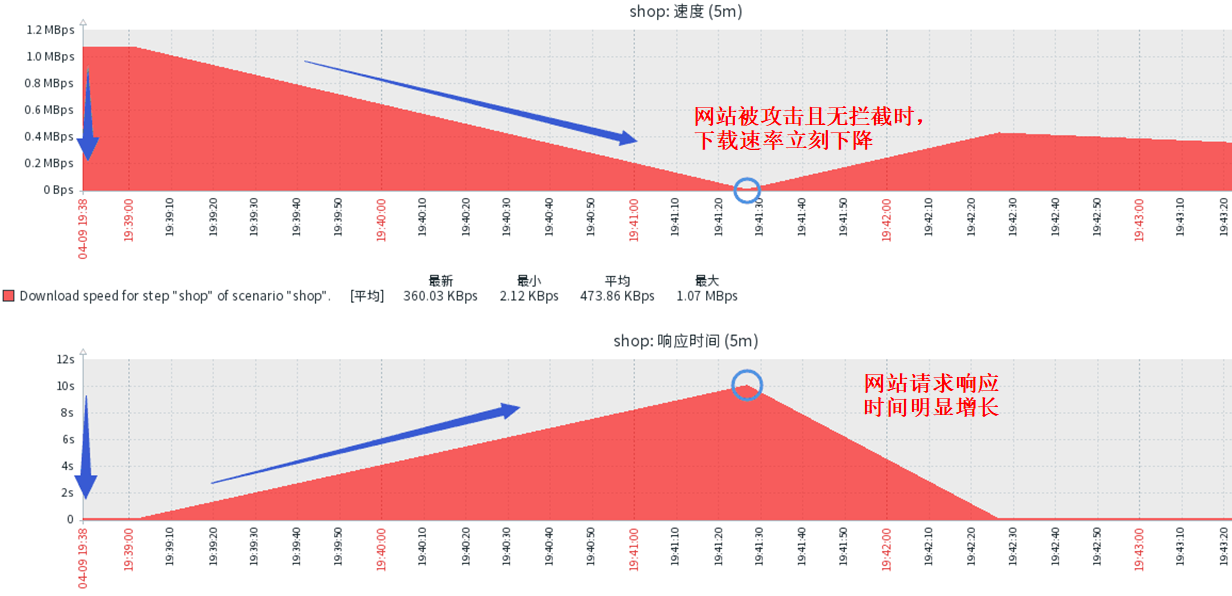
1. 网站服务器监控效果

如下图，Zabbix重点监控的CPU占用率在服务器无拦截受到攻击时陡增。

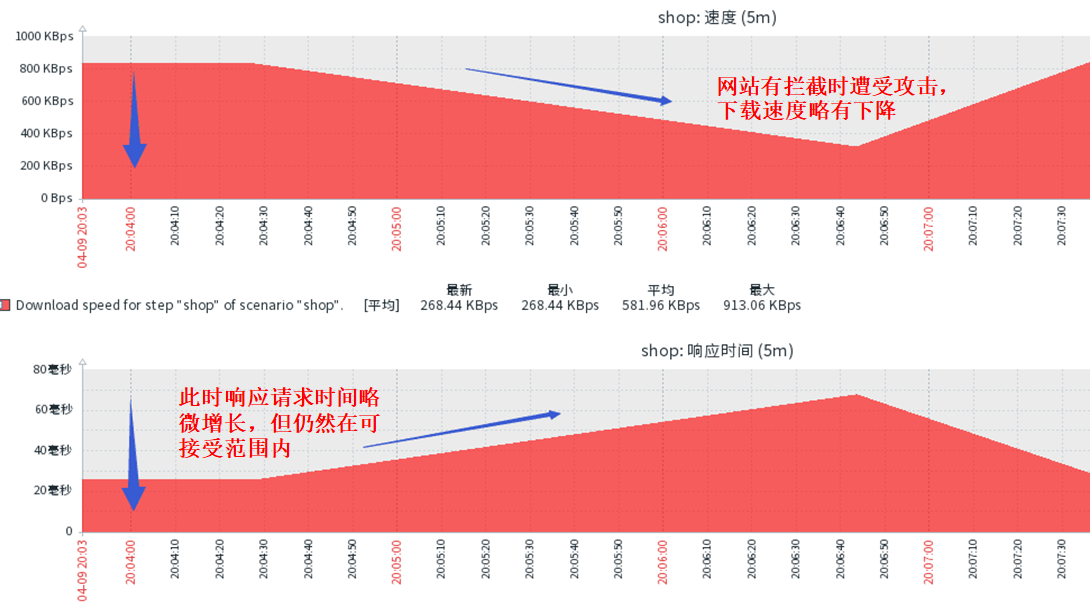


之后在有拦截的情况下遭受攻击CPU占用率增幅较小。

如下图，Zabbix重点监控的网站下载速度在服务器无拦截受到攻击时骤降，请求时间明显增长，时间超出可承受范围。



之后在有拦截的情况下遭受攻击网站下载速度降幅较小，请求响应时间略有增长可忽略不计，依旧在可承受时间范围内。



Zabbix监控各个指标的仪表盘如下：

