参考链接：

https://redmine.openinfosecfoundation.org/projects/suricata/wiki/Suricata\_Snorby\_and\_Barnyard2\_set\_up\_guide

http://hi.baidu.com/huting/item/7a60eb725e66cb206e29f6b8

http://drops.wooyun.org/tips/413

http://www.freebuf.com/articles/network/51473.html

http://www.freebuf.com/articles/network/51473.html

http://www.oschina.net/p/suricata/

## **Snorby服务器安装**

系统版本：ubuntu-12.04.5-server-amd64

1）系统最小化安装，过程略，并切换到root账户（图方便）。

2）修改apt-get源为国内源，并apt-get update。

3）安装依赖包，mysql，ruby环境等。

4）下载wkhtmltopdf（可选）

5）安装apache，（可选）

6）更改gem源为淘宝源，安装相关gem包，并下载snorby

7）编辑snorby配置文件

8）修改相关配置，并安装相关gem包，创建和初始化snorby数据库。

修改文件Gemfile

第一行改为source 'http://ruby.taobao.org'

然后把gem 'rake', '0.9.2'   改成  gem 'rake', '> 0.9.2'

修改文件Gemfile.lock

把 rake (0.9.2)  改成  rake(0.9.2.2)

9）配置mysql相关账户远程访问权限

注释bind-address 项

10）启动mysql和snorby

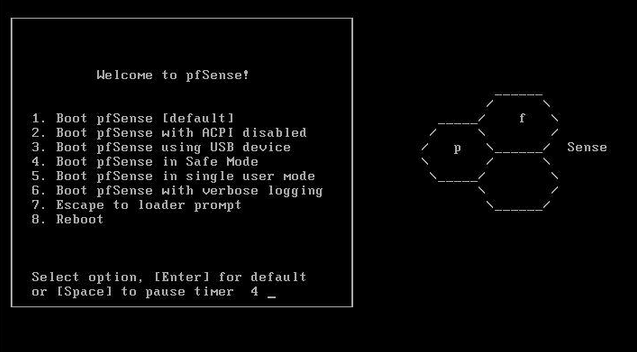
11）访问http://ip:3000，默认账号snorby@snorby.org 密码snorby 。

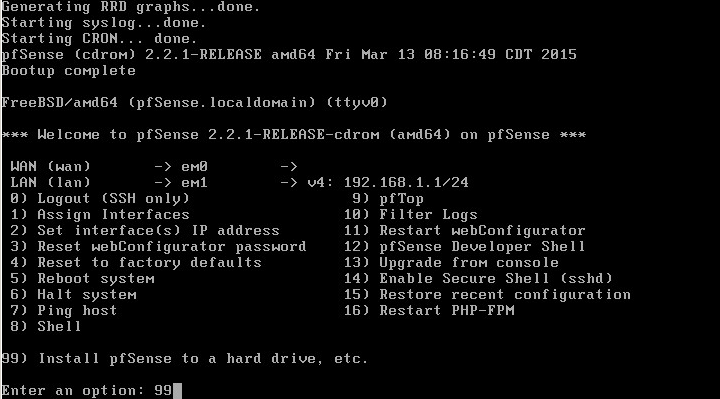
## **安装pfsense**

pfsense集成了Suricata和Barnyard2，图形界面配置比较方便，所以直接采用pfsense。

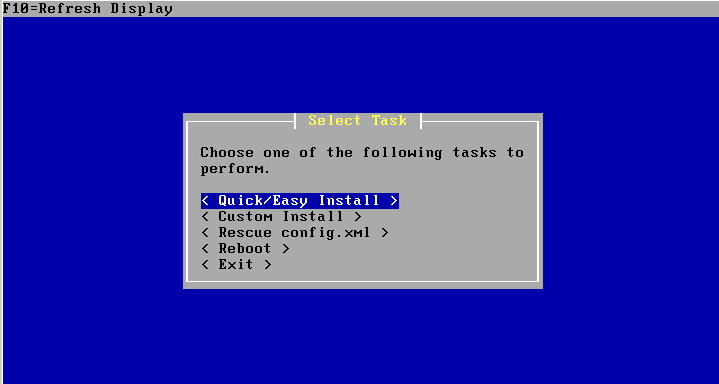
1. 安装pfsense

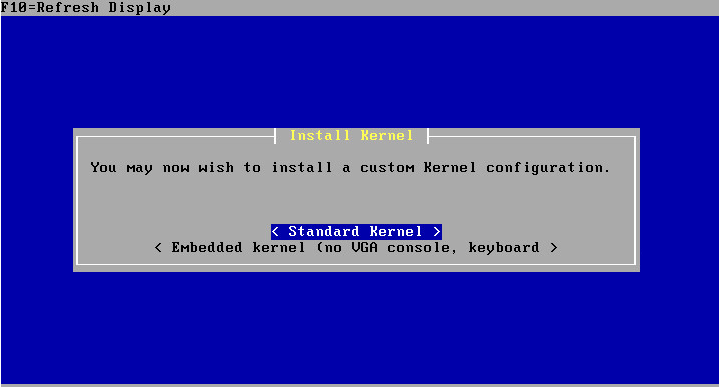
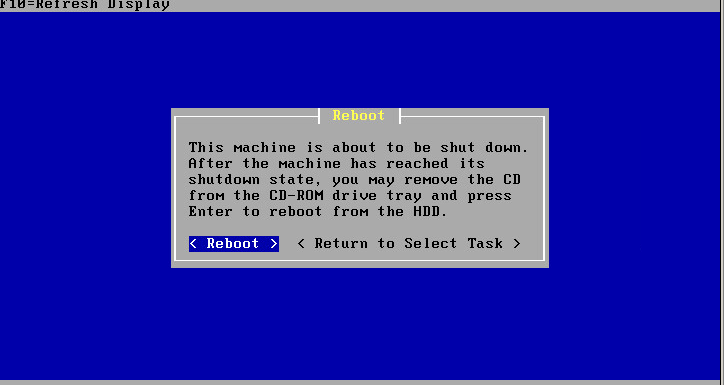
挂好系统镜像pfSense-LiveCD-2.2.1-RELEASE-amd64-20150313-0816.iso打开电源回车

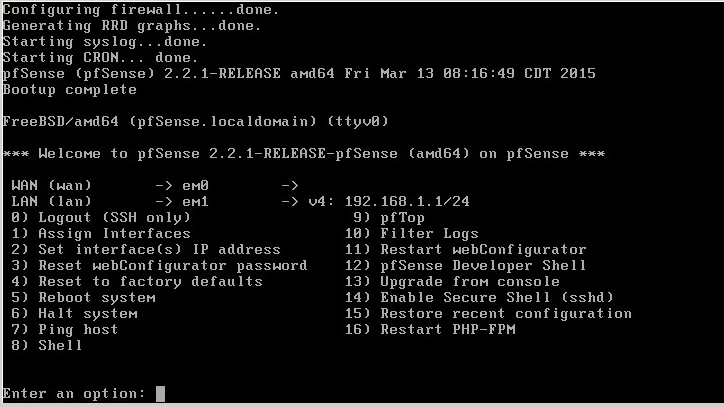










基本安装到此结束，后面讲具体配置。

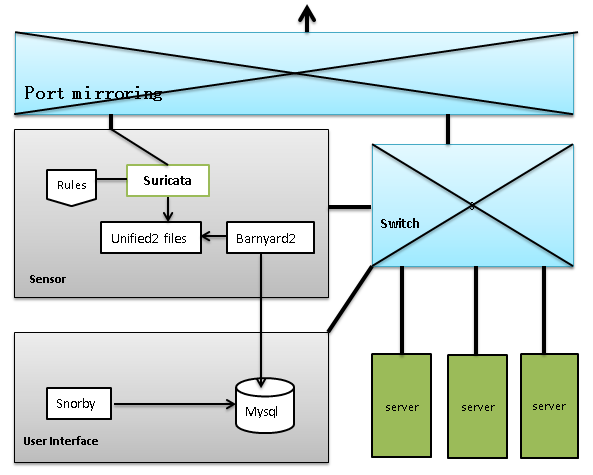
## **配置pfsense**

**拓扑说明**：本环境为实际生产环境部署，由于是软件IDS，性能稳定性有限，所以采用离线模式部署。

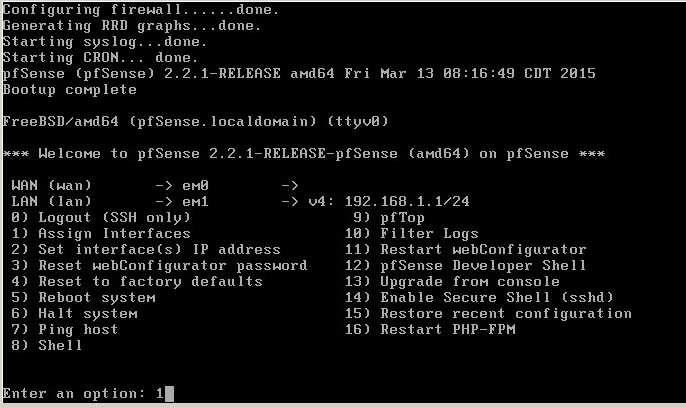
出网交换机把出网端口流量全部做了镜像，镜像端口连在pfsense的LAN口上，即LAN口抓所有数据。

Pfsense的WAN连到可上外网的任意一台交换机上，用于联网下载suricata包

Snorby+mysql为单独机器也连在交换机上，保证能与pfsense的WAN口通讯。



1. 选1配置接口，注意这里只指定WAN口，删除LAN口，因为pfsense配置了LAN口后默认只能用LAN口登陆后台，而我这里的LAN是镜像流量口，无法联网的。

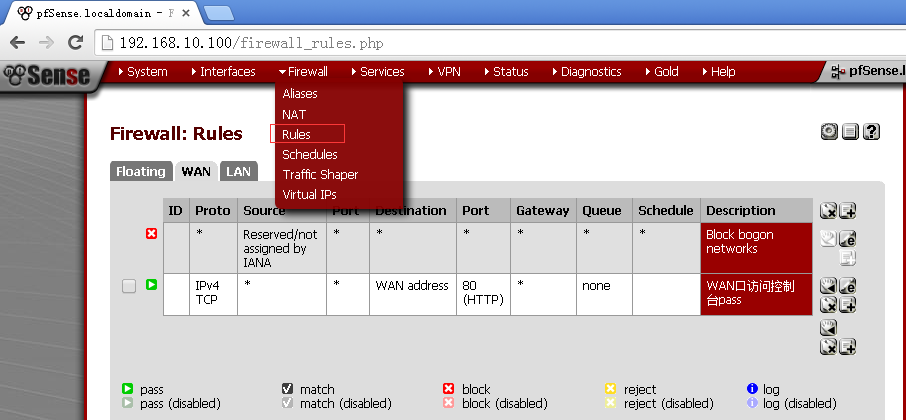


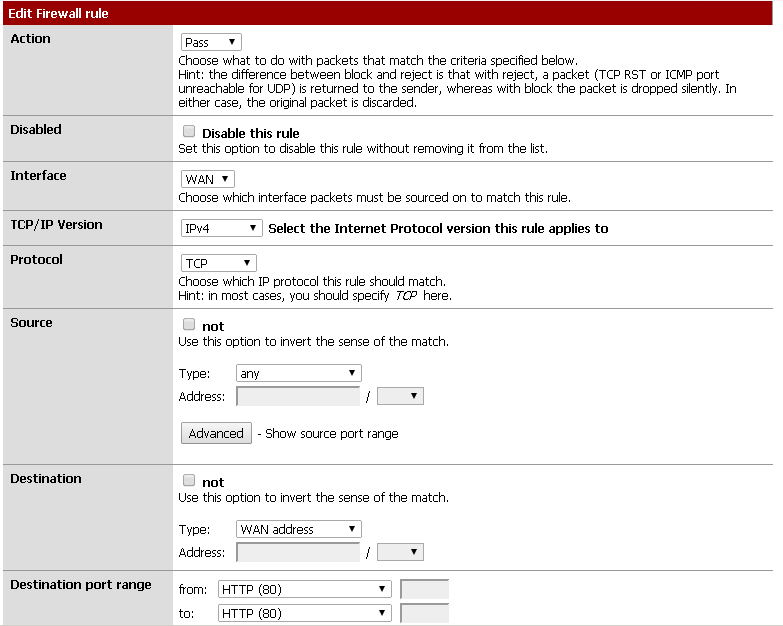
1. 选2，配置WAN口IP，我这里设置的192.168.10.100,



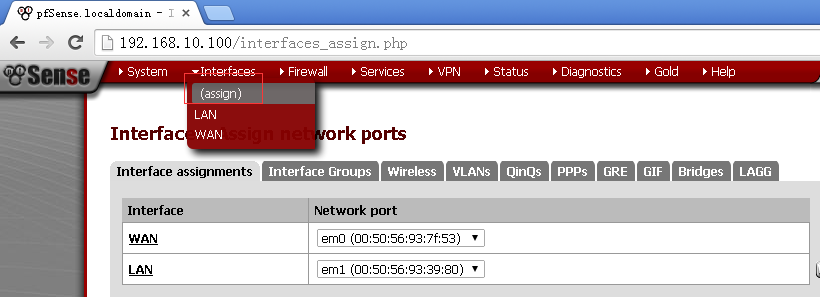
1. 访问http://192.168.10.100，默认账号密码admin pfsense

如图，选择防火墙规则，设置好WAN口80端口的pass规则，接着就可以设置LAN口了。

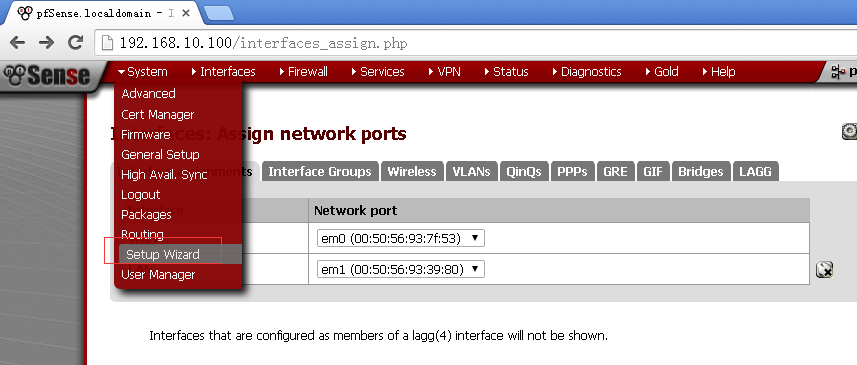




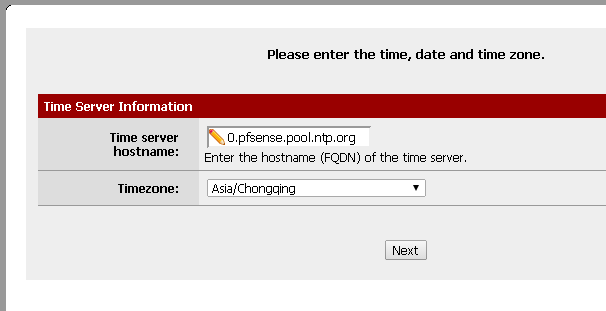
配置LAN口



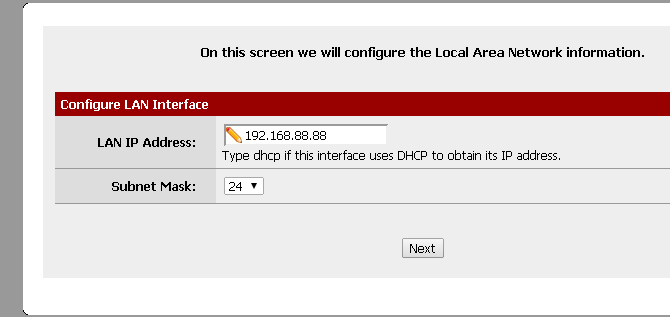
1. 配置向导



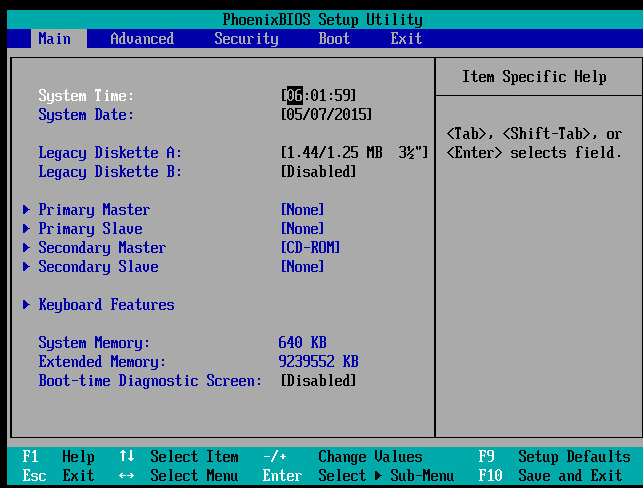
时区选择重庆



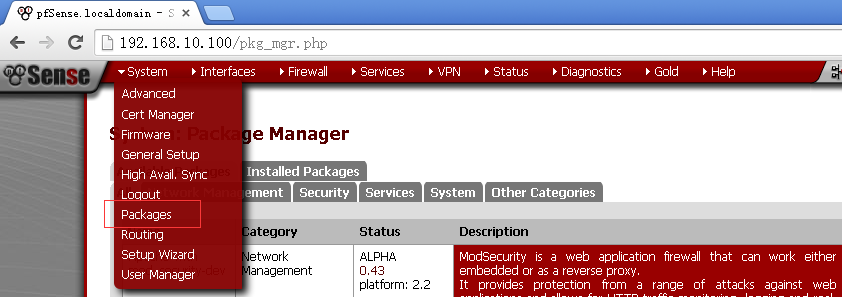
LAN口Ip任意配置（不配置应该也可以）

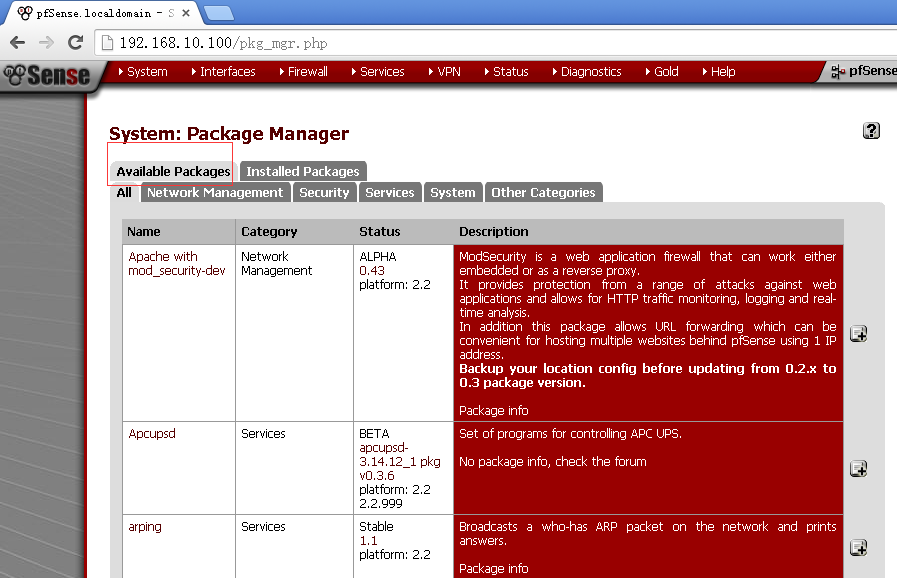


补充比较重要的一步，一定要重启进入bios修改时间，不然后面IDS日志时间始终不对。

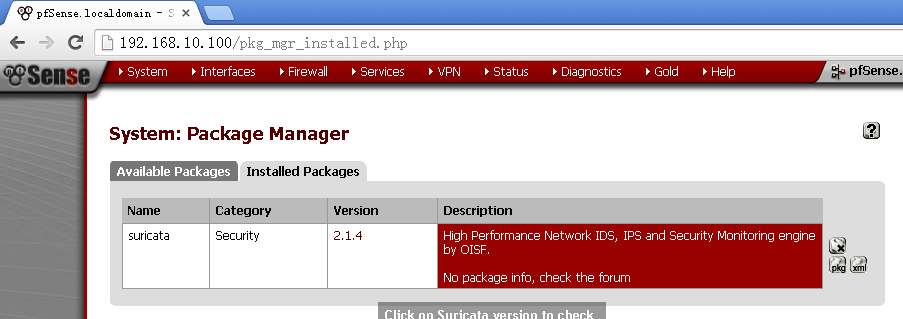


1. 安装suricata



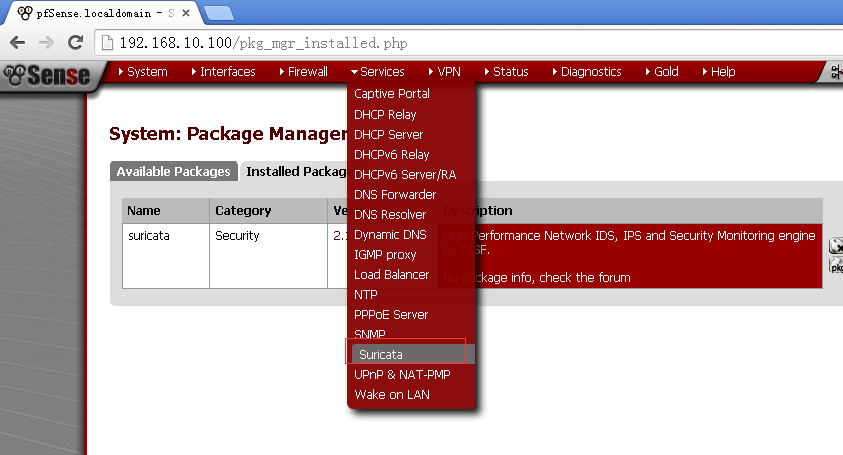


然后按照提示安装完成

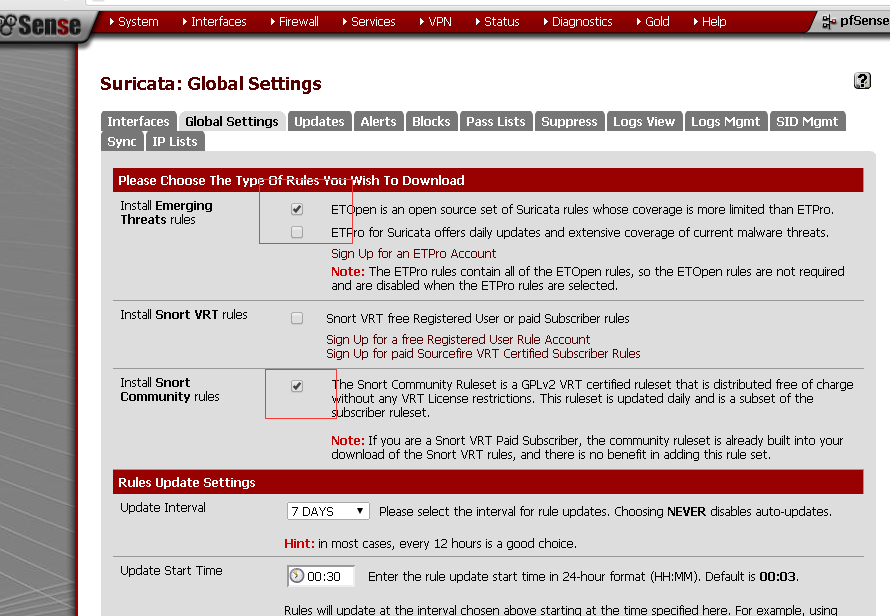


1. 配置suricata

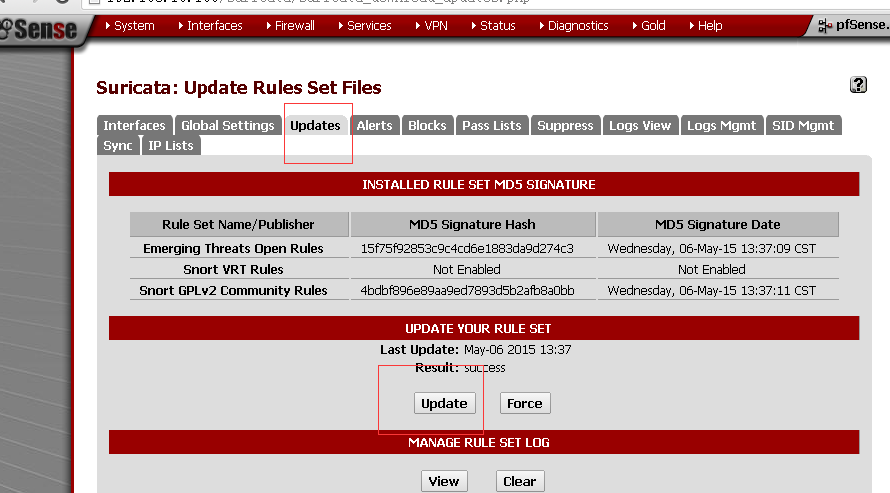
如图进入suricata模块



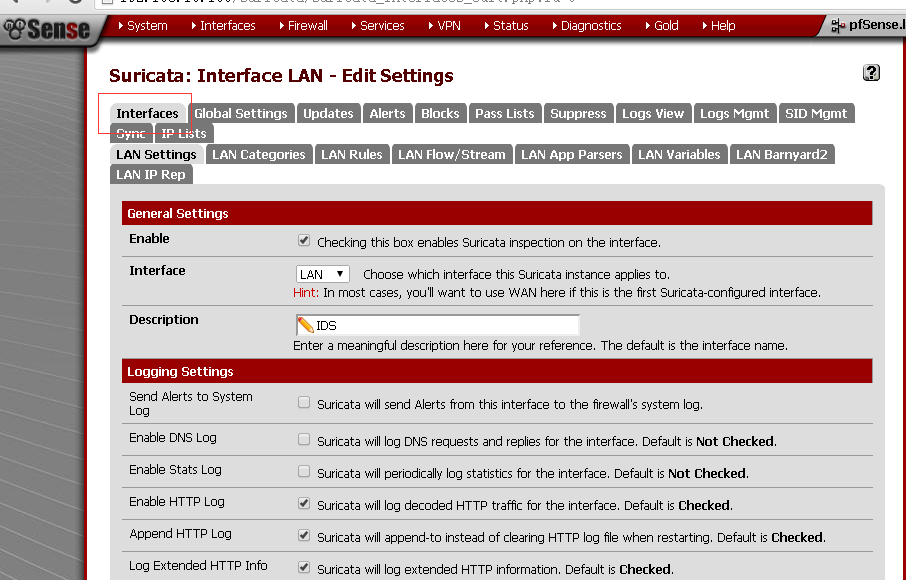
如图两个勾选并保存，其它规则应该要收费



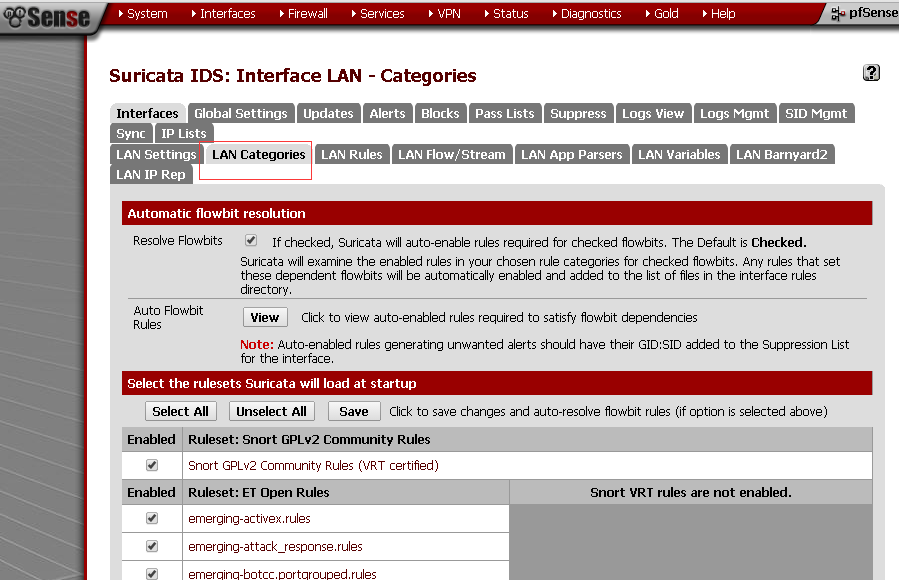
升级规则



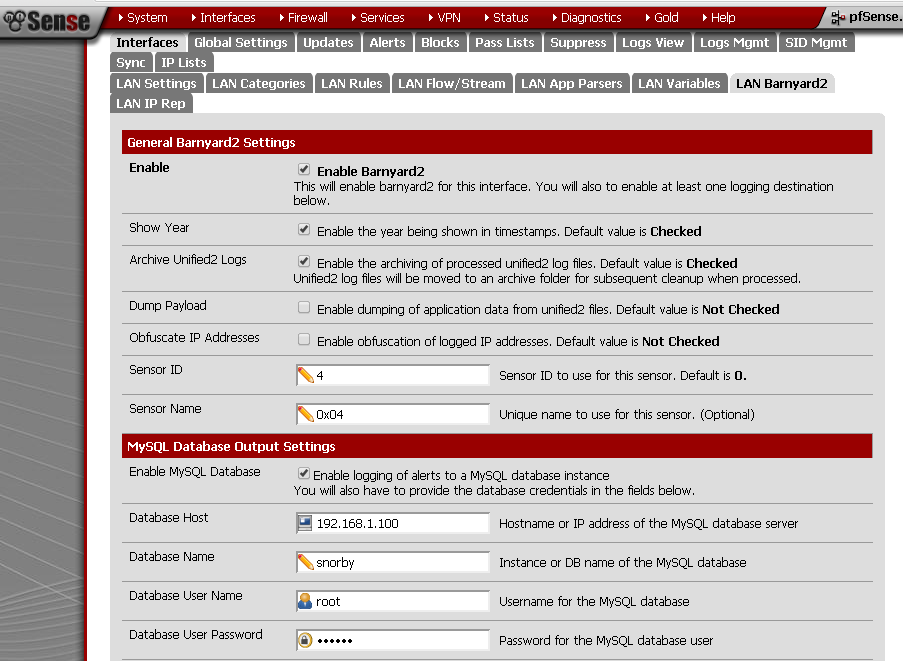
点击interfaces选项，并添加配置，这里暂时先选择监控LAN口，直接保存，其它先默认，后面再详细配置。



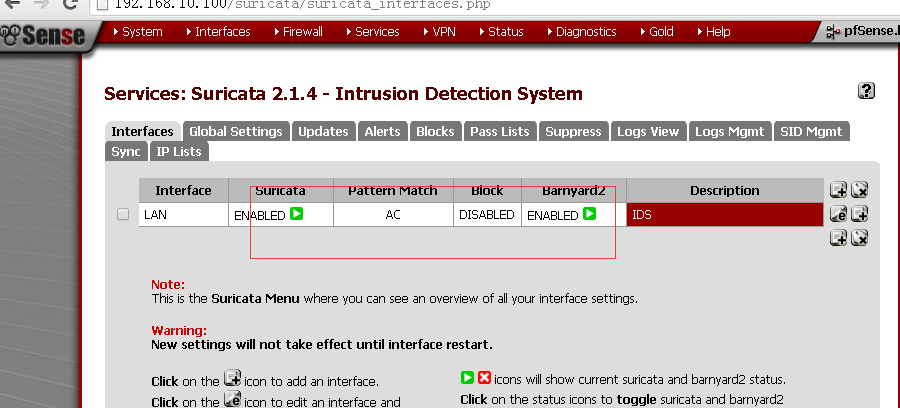
接口规则，先全选并保存，后面再进行删减添加。



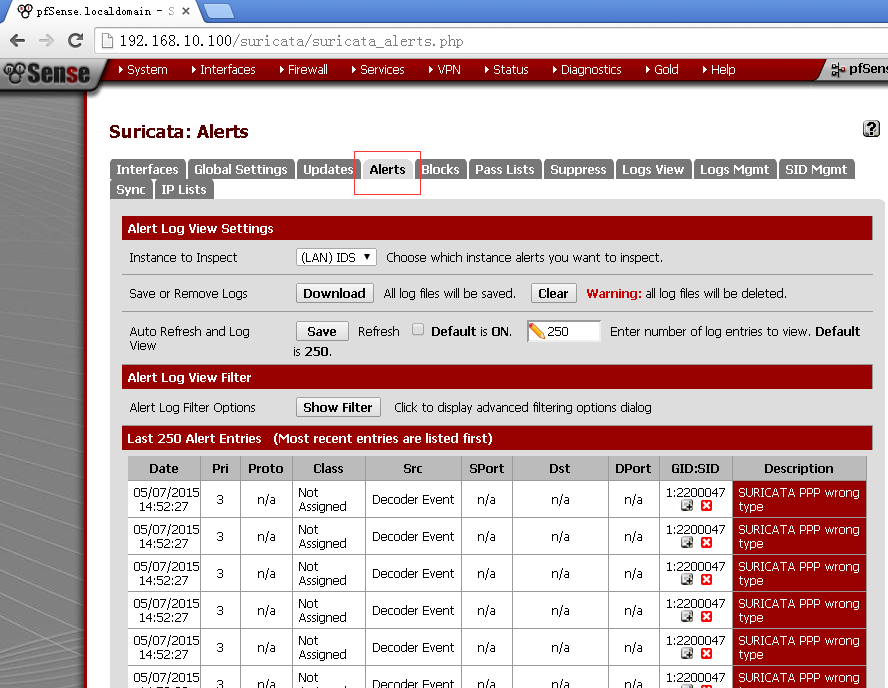
配置Barnyard2，sensor ID ，sensor name 随意命名，下面填写mysql数据库相关信息，即把日志存储到snorby所在mysql数据库中，最好先测试下数据库连接是否可达。



如图点击按钮suricata+barnyard2就开始工作了

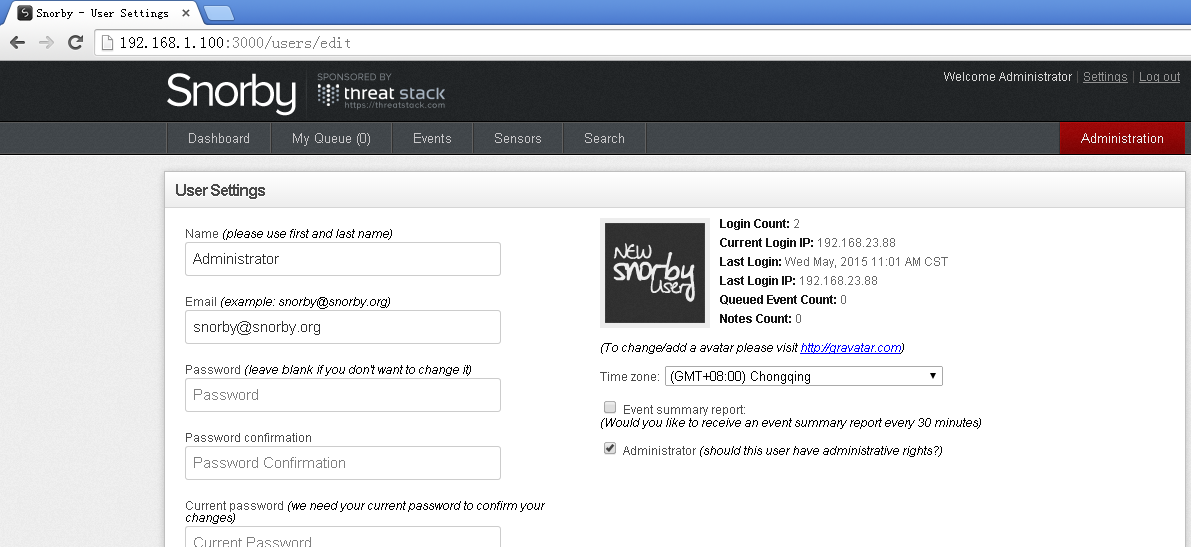


点击alerts，发现运行正常，风险数据已出现

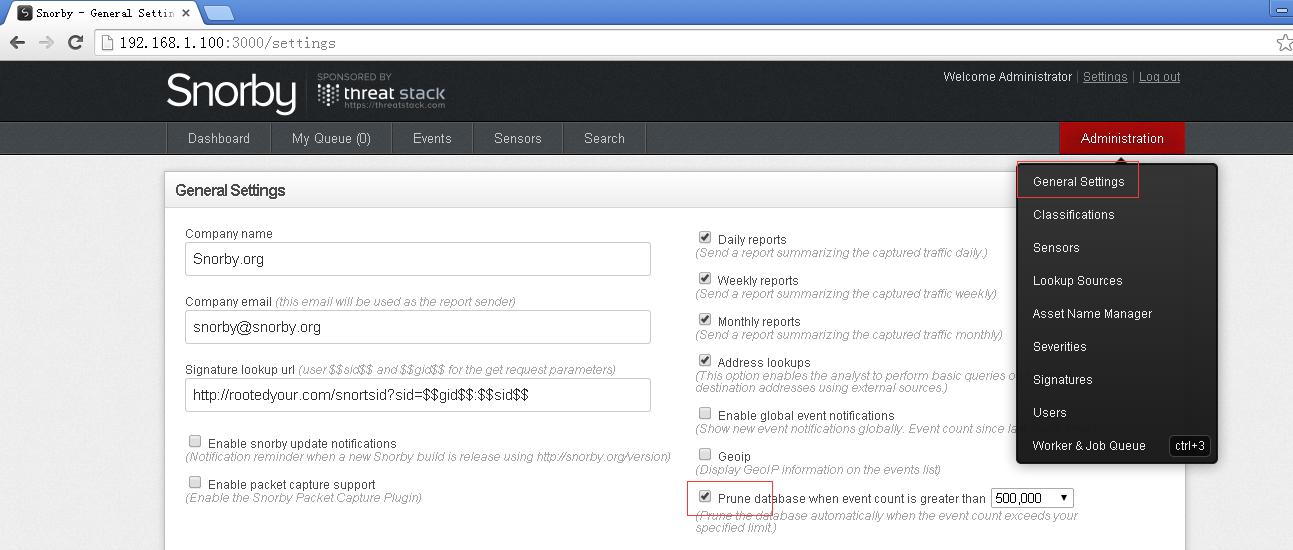


## **Snorby控制台配置**

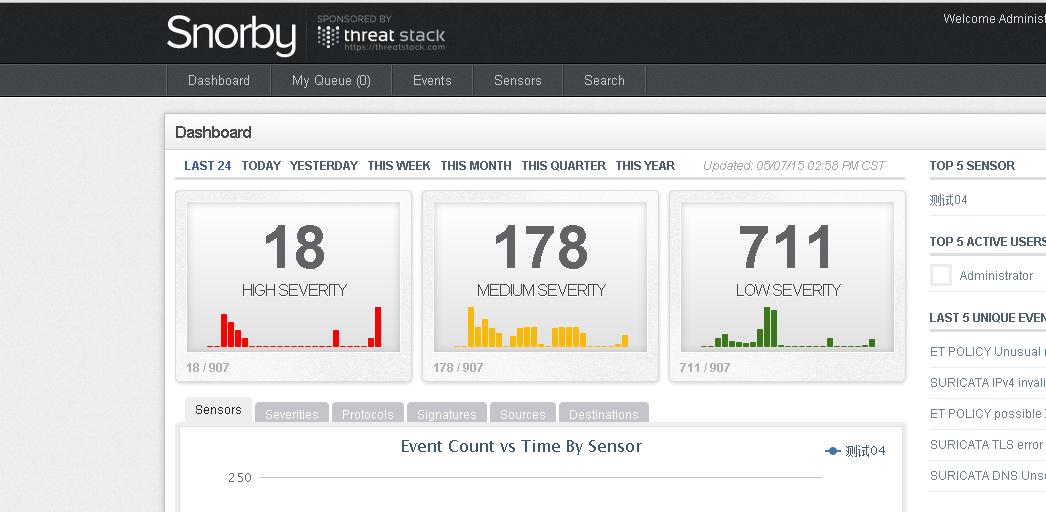
1）点击右上角settings ，然后设置时区为重庆，其它修改密码之类可选。

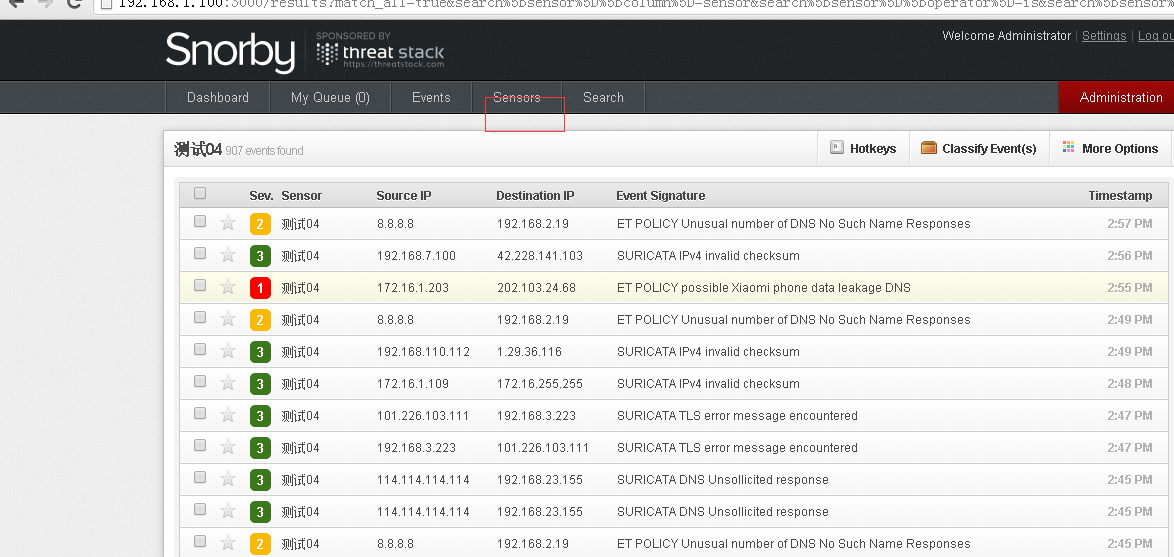


1. 如图管理员选项勾选右下那个选项，事件数据达到500000就对数据进行自动修剪，在实际环境运用应该比较重要。



1. 数据成功接收，其它操作比较简单了。

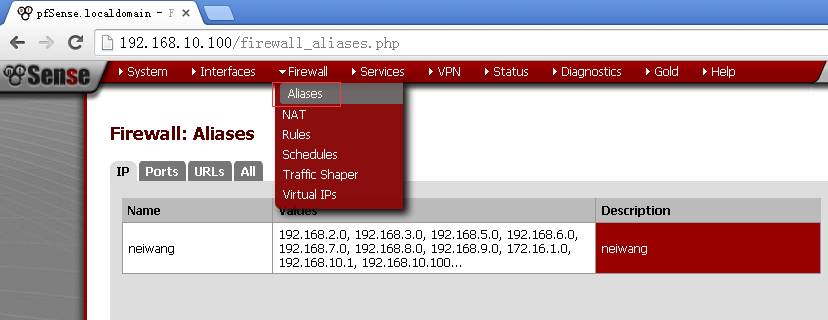




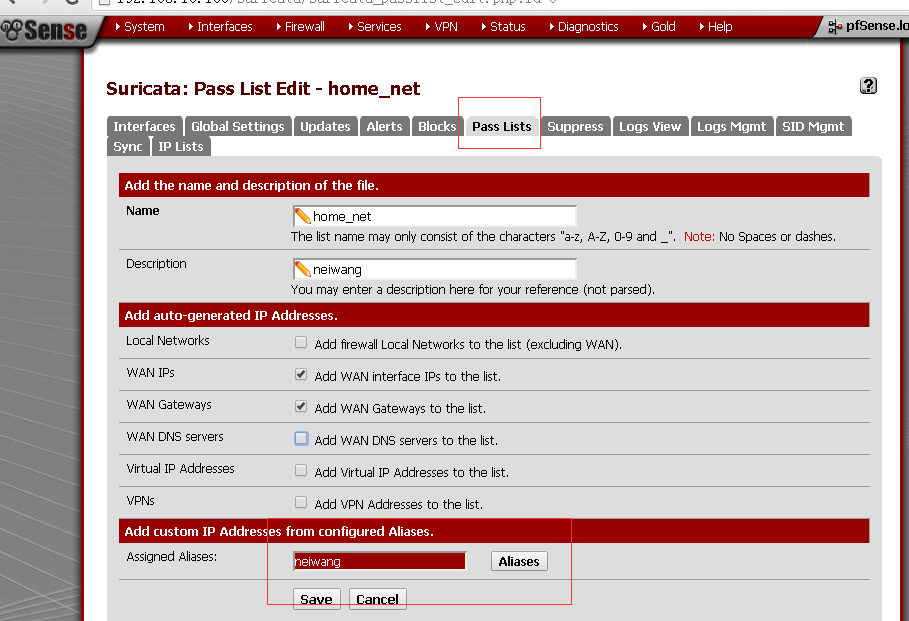
## **生产环境下suricata规则设置**

1. 由于是端口镜像的数据，所以要手动指定内外网IP

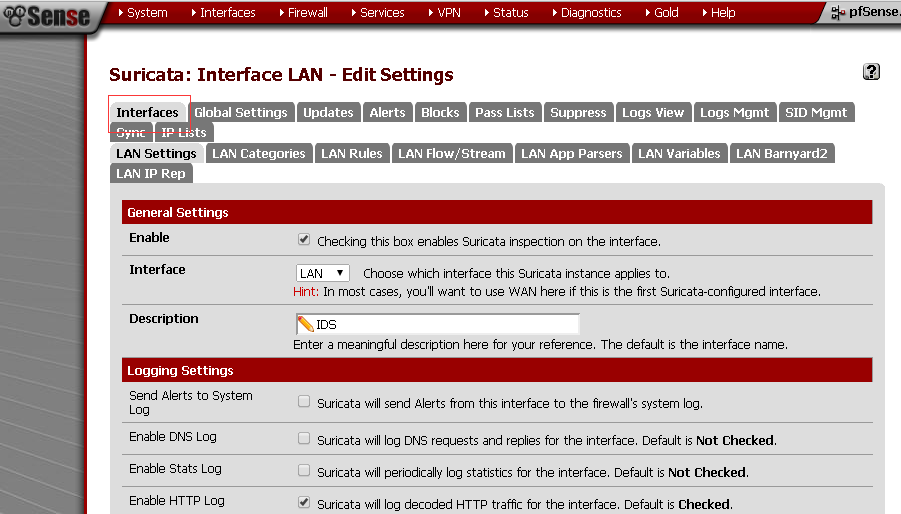
如图



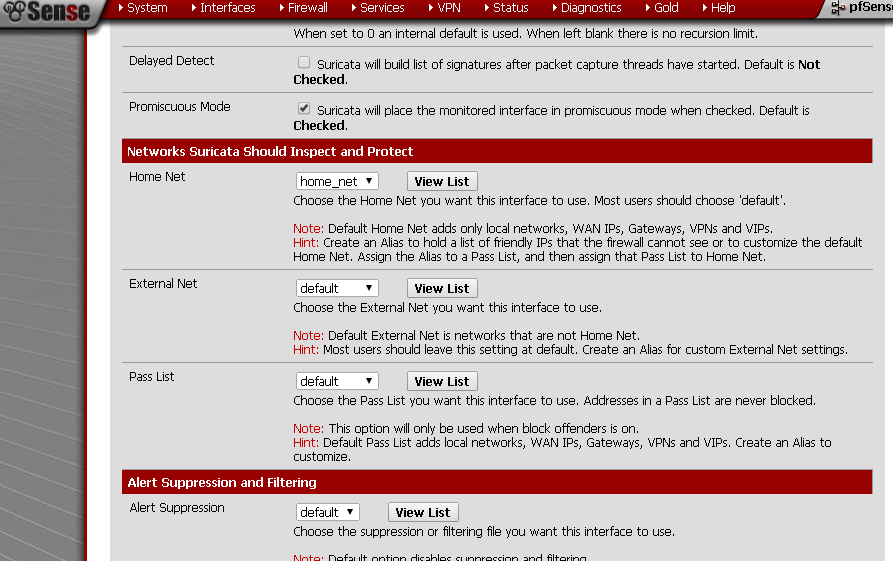
打开suricata的pass lists，如图设置



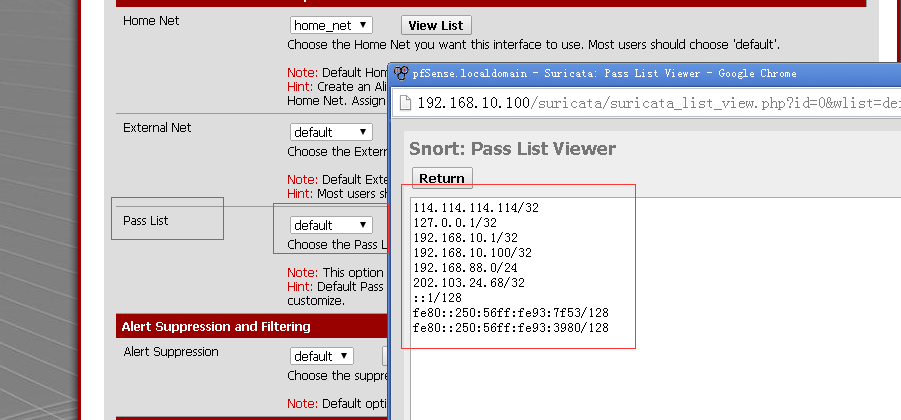
然后进入interface，页面拉到最下面



Home\_net（内网） 选择前面pass lists的相应配置，external Net（外网）默认是除home\_Net外的所有网络



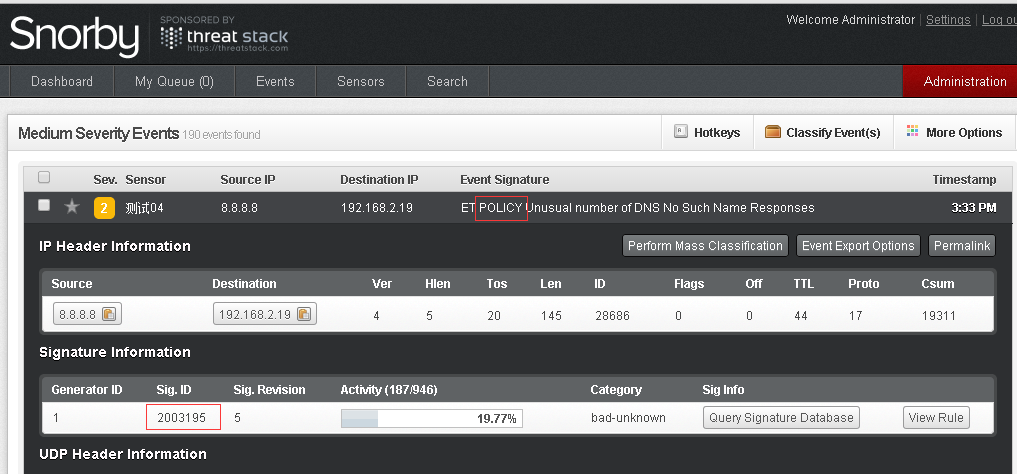
下面的pass list 选项可以使用同样的办法进行配置，我这里没有配置，使用的默认。



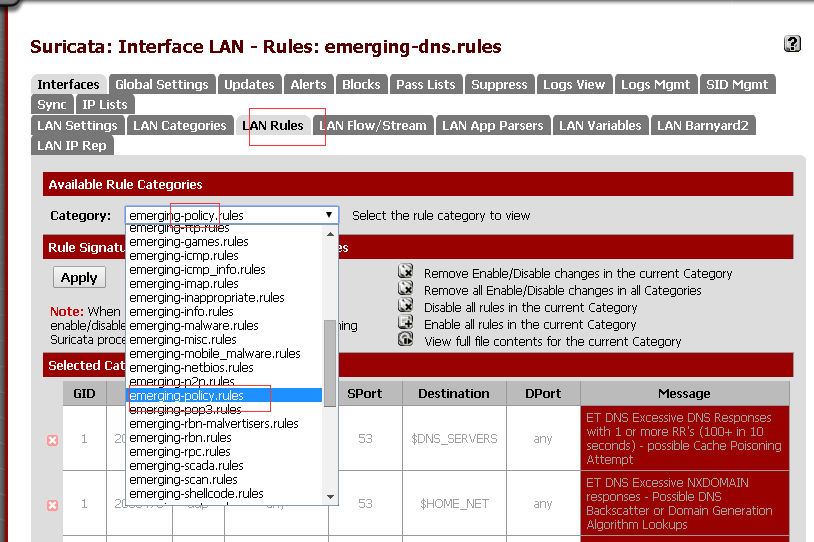
1. 由于之前的引擎检测规则全选，所以会导致海量风险日志，所以在实际生产环境中规则的设置就显得十分重要。

如下图snorby接收的风险日志，风险描述命名的第二个单词为规则的大类，

GID为规则的优先级，越小越优先，SID为规则编号。



如下图，打开LAN rules，找到上图规则大类policy



搜索Gid ，2003195，点击前面的红叉，关闭。



点击apply ，规则关闭生效，此规则已被关闭。



3）root , pfsense

/usr/pbi/suricata-amd64/local/etc/suricata