# Windows环境下Snort配置指南

## Snort规则配置

下载并安装好Snort，使用记事本或编辑器打开安装目录下/etc/snort.conf文件，更改位置的配置代码（其中的路径改为自己的安装目录）。以安装目录为D:\Snort为例，打开D:\Snort\etc\snort.conf文件，更改规则配置路径如下图所示：

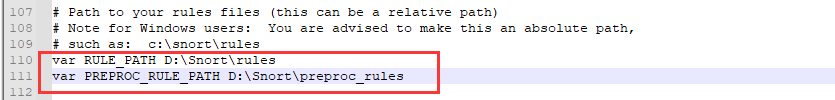


图1 规则配置1

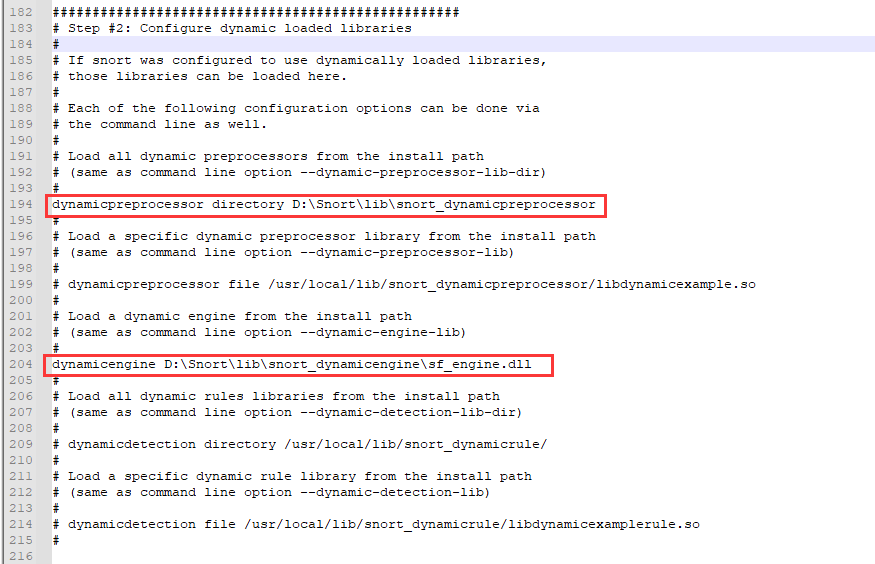


图2 规则配置2

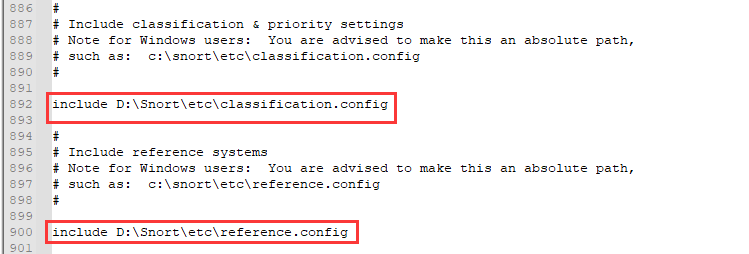


图3 规则配置3

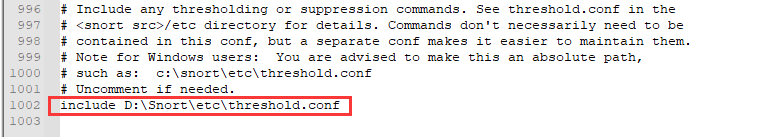


图4 规则配置4

更改好配置路径后，将下载好的规则（如snortrules-pr-2.4.tar.gz）解压，并将.rules文件放至安装目录下的 rules文件夹中。

## 错误解决

（1）ERROR: ../etc/snort.conf(250) Missing/incorrect dynamic engine lib specifier.

仔细检查snort的配置是否正确，我这里是在规则配置图2那里末尾多了个\，去掉即可

（2）Unable to open address file D\ Snort\etc\../rules/white\_list.rules, Error: No such file or directory

在rules文件夹内新建文件white\_list.rules即可

（3）ERROR: D: \Snort\etc\snort.conf(512) => Unable to open address file D: \Snort\etc\../rules/black\_list.rules, Error: No such file or directory

同上，新建该文件即可

（4）ERROR: (rules/web-misc.rules)97 => Cannot use 'rawbytes' and 'http\_uri' as modifiers for the same "content" nor use 'rawbytes' with "uricontent".

类似这种错误代表规则配置有问题，使用“#”注释掉报错规则即可。如下图，注释掉..\rules\web-misc.rules中第97行规则。

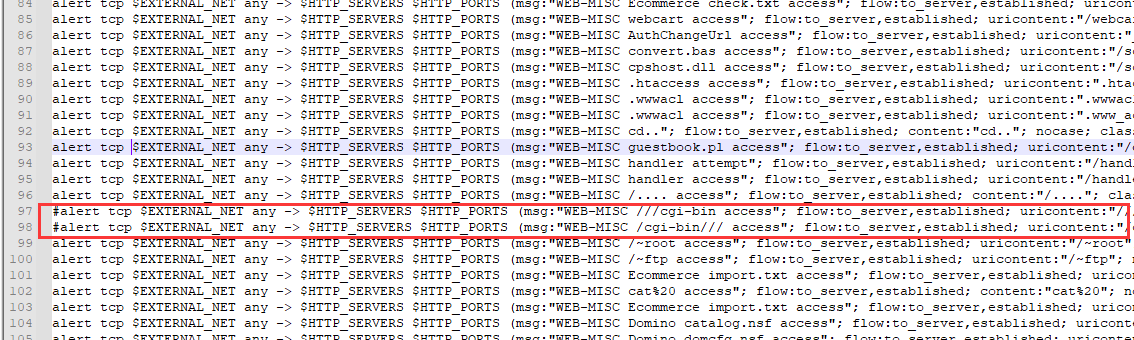


图5 规则注释