Buat konfigurasi file sbb :

- Make sure our HOME and EXTERNAL_NET are correctly set
  - HOME_NET: 10.130.3.30 (only trusted computer)
  - EXTERNAL_NET: !HOME_NET
- Comment out all rules except myrules.rules
- Create a file called /etc/snort/rules/myrules.rules that contain the following rules
  - Alert for FTP traffic from any EXTERNAL_N ET
  - Alert for 'terrorism' in content OUTGOING from HOME_NET
  - Alert for pings from EXTERNAL_NET

Pada komputer IDS install snort dan ftp server
Editing

editing snort.conf

```
pc@ubuntu:~$ sudo vim /etc/snort/snort.conf
```

Pastikan dua baris ini ada

```
var HOME_NET 192.168.14.129
var EXTERNAL_NET !$HOME_NET
```

Note : HOME_NET adalah komputer snort

Tambahan rule

```
include $RULE_PATH/myrules.rules
```

Buat file di /etc/snort/rules/Myrules.rules

```
# These are my experimental rules
alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"Incoming FTP connection!"; flags:S; sid:10
000;)
alert tcp $HOME_NET any -> $EXTERNAL_NET 80 (msg:"terrorism content found"; content:"terrori
sm"; nocase; sid:10001;)
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"We are being pinged!"; icode:0; itype:8;
 sid:10002;)
```

Running

```
pc@ubuntu:~$ sudo /usr/sbin/snort -d -l /var/log/snort -c /etc/snort/snort.conf
-i eth0
```

Lihat alert dgn perintah sbb :

```
pc@ubuntu:/var/log/snort$ tail -f ./alert
```

Percobaan lihat hasil :

1. Dari komputer lain Jalankan ftp ke snort dan Lihat hasil alert di komputer snort

2. Dari komputer yang diinstall snort jalankan browser dan buka google searching menggunakan keywod “terrorism” Lihat hasil alert di komputer snort

3. Dari komputer lain jalankan ping ke snort Lihat hasil alert di komputer snort

Running daemon

```
pc@ubuntu:~$ sudo /usr/sbin/snort -D -d -l /var/log/snort -u snort -g snort -c /etc/snort/sn
ort.conf -i eth0
```