* Configure snort /etc/snort/snort.conf
  + $HOME\_NET is a variable that defines the network or networks you are trying to protect.
    - Default $HOME\_NET: any
    - HOME\_NET: 10.130.10.10
  + $EXTERNAL\_NET is the external, untrusted networks to which you are connected.
    - Default $EXTERNAL\_NET: any
    - EXTERNAL\_NET: !$HOME\_NET
  + It is good to use **any** for the $HOME\_NET if you are not sure which device to protect. But this is may cause false positive alerts, and also increase the overhead on Snort.
  + If you specify the $HOME\_NET this can decrease false positive alerts. However, may miss an internal-to-internal (i.e. $HOME\_NET to $HOME\_NET) attack.
* Rules
  + Defaults rules.
  + Designed rules
* Alerting
  + Alert on incoming to $HOME\_NET
  + Alert on outgoing from $HOME\_NET
* Example:
  + Alert for FTP traffic from EXTERNAL\_NET
    - Alert tcp $EXTERNAL\_NET any -> $HOME\_NET 21 (msg:”incoming FTP connection!”; flags:S; sid:10000;)
  + Alert for specific content (any word)
    - Alert tcp $HOME\_NET any -> $EXTERNAL 80 (msg:”XXXX”; content:”XXXX”; sid:10001;)
    - Case sensitive
      * Check Snort manual
    - Alert tcp $HOME\_NET any -> $EXTERNAL 80 (msg:”XXXX content found”; content:”XXXX”; nocase; sid:10001;)
  + Alert for smurf attack
    - Alert icmp $EXTERNAL\_NET any -> $HOME\_NET any (msg:”Smurf attack”; icode:0; itype:8; sid:10002;)
  + Alert on scanning
    - alert tcp $EXTERNAL\_NET any -> $HOME\_NET any (msg:"SCAN nmap XMAS"; reference:arachnids,30; classtype:attempted-recon; sid:10005; rev:7;)

sudo snort -A console -i eth0 -u snort -g snort -c /etc/snort/snort.conf

|  |  |
| --- | --- |
| **Option** | **Description** |
| -A fast | Fast alert mode. Writes the alert in a simple format with a timestamp, alert message, source and destination IPs/ports. |
| -A full | Full alert mode. This is the default alert mode and will be used automatically if you do not specify a mode. |
| -A unsock | Sends alerts to a UNIX socket that another program can listen on. |
| -A none | Turns off alerting. |
| -A console | Sends ``fast-style'' alerts to the console (screen). |
| -A cmg | Generates ``cmg style'' alerts. |

Resources:

<http://manual-snort-org.s3-website-us-east-1.amazonaws.com/node6.html>

<https://www.youtube.com/watch?v=RUmYojxy3Xw&t=620s>

<http://manual-snort-org.s3-website-us-east-1.amazonaws.com/node31.html>

<http://www.informit.com/articles/article.aspx?p=101171&seqNum=6>