IDS & IPS

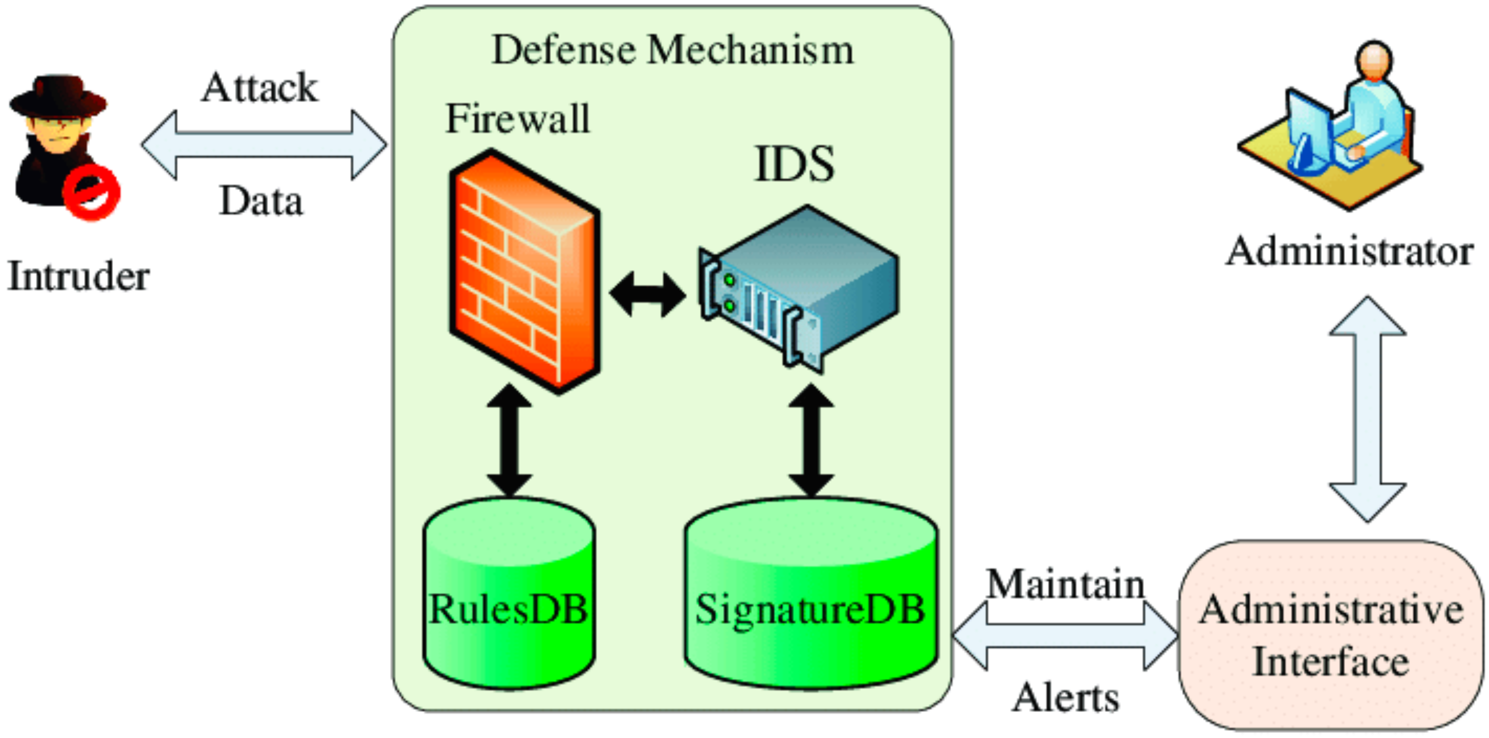
jnlin

IDS & IPS

- ❑ Intrusion detection system (IDS) is a device or software application that monitors a network or systems for malicious activity or policy violations.

- ❑ The main functions of intrusion prevention systems (IPS) are to identify malicious activity, log information about this activity, report it and attempt to block or stop it.

IDS / IPS with Firewall



Detection Method

❑ Signature-based

- Patterns of known malicious events
- Difficult to detect new attacks

❑ Anomaly-based

- Use machine learning to create a model of trustworthy activity, and then compare new behavior against this model.

Pros & Cons

❑ Pros

- Simple
- Cost Efficiency

❑ Cons

- False positives are frequent
- Need to update signature library

Snort

- An open source IDS
  - GPLv2
- Very simple to use it

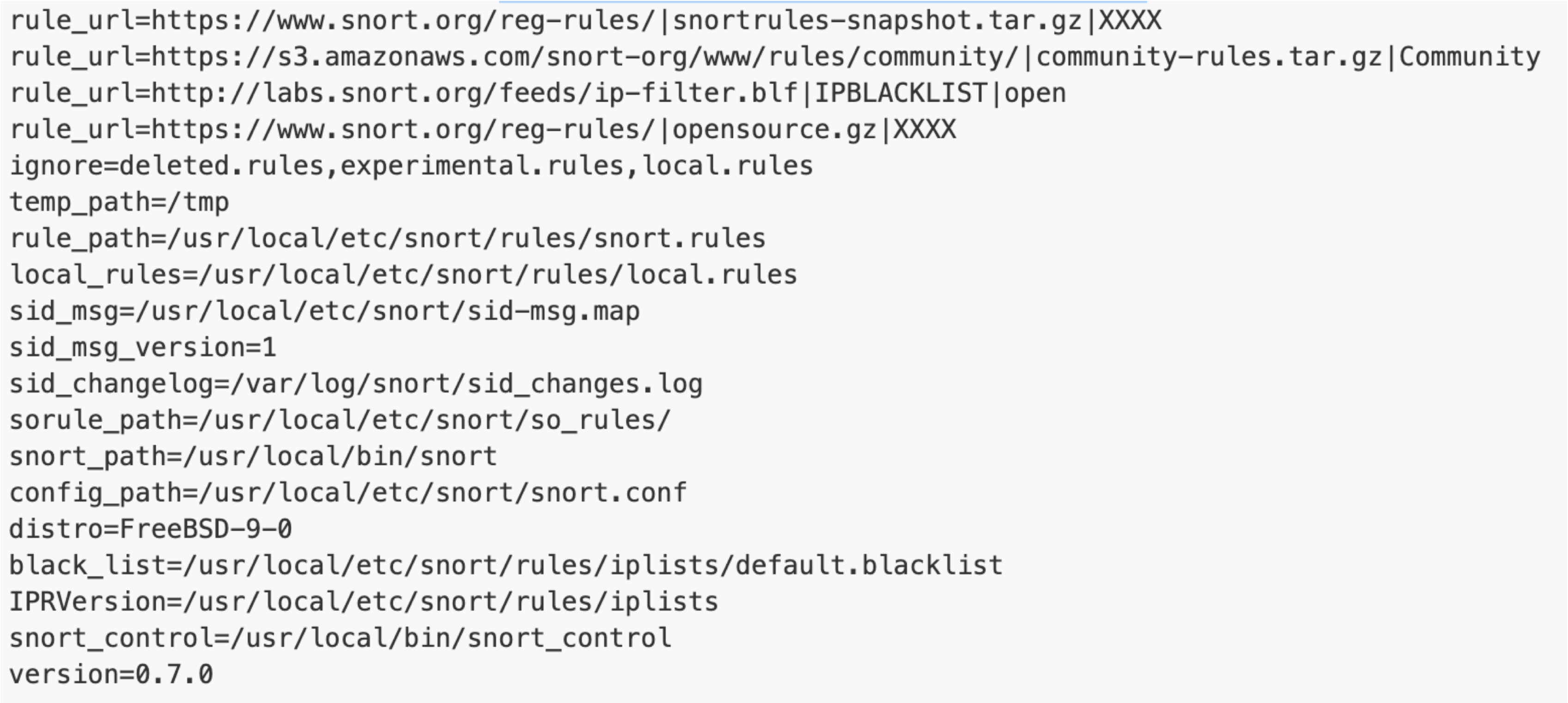
Snort - installation

- ❑ FreeBSD: pkg install snort

- ❑ Don’t forget to update latest updated rules
  - Configure PulledPort
    - cp /usr/local/etc/pulledpork/pulledpork.conf.sample /usr/local/etc/pulledpork/pulledpork.conf
    - mkdir /usr/local/etc/snort/so_rules
    - mkdir /usr/local/etc/snort/rules/iplists
    - touch /usr/local/etc/snort/rules/local.rules
    - cp /usr/local/etc/snort/preproc_rules/sensitive-data.rules-sample /usr/local/etc/snort/preproc_rules/sensitive-data.rules
    - /usr/local/etc/snort/rules/white_list.rules
    - /usr/local/etc/snort/rules/black_list.rules

Snort - PulledPort

- ❑ /usr/local/etc/pulledpork/pulledpork.conf



```
rule_url=https://www.snort.org/reg-rules/|snortrules-snapshot.tar.gz|XXXX
rule_url=https://s3.amazonaws.com/snort-org/www/rules/community/|community-rules.tar.gz|Community
rule_url=http://labs.snort.org/feeds/ip-filter.blf|IPBLACKLIST|open
rule_url=https://www.snort.org/reg-rules/|opensource.gz|XXXX
ignore=deleted.rules,experimental.rules,local.rules
temp_path=/tmp
rule_path=/usr/local/etc/snort/rules/snort.rules
local_rules=/usr/local/etc/snort/rules/local.rules
sid_msg=/usr/local/etc/snort/sid-msg.map
sid_msg_version=1
sid_changelog=/var/log/snort/sid_changes.log
sorule_path=/usr/local/etc/snort/so_rules/
snort_path=/usr/local/bin/snort
config_path=/usr/local/etc/snort/snort.conf
distro=FreeBSD-9-0
black_list=/usr/local/etc/snort/rules/iplists/default.blacklist
IPRVersion=/usr/local/etc/snort/rules/iplists
snort_control=/usr/local/bin/snort_control
version=0.7.0
```

Run PulledPork

- pulledpork.pl -c /usr/local/etc/pulledpork/pulledpork.conf -l

Start Snort

❑ In /etc/rc.conf.local

- snort_enable="YES”
- snort_interface="em0”

❑ /usr/local/etc/rc.d/snort start

Update rules periodically

- crontab
  - 0 6 * * * /usr/local/bin/pulledpork.pl -c /usr/local/etc/pulledpork/pulledpork.conf -l > /dev/null