I have downloaded the emerging threat rules using suricata-update, Can we apply the filters enable.conf, disable.conf, modify.conf and drop.conf in the current existing rules folder without fetching the rules from url or from cache location everytime?

Likely related to the desire here to enable quick testing of config modifications...

I've found that modifications made via modify.conf may not be applied. I'm not clear, but I'm guessing that it's likely due to such modifications not revising the rule's revision #. We may need to detect when updates occur to those files and ignore rev # checks on effected rules, or at least document that modify rules may need to also update revision to be applied.

So you are telling, if we modify any rule from alert to drop manually and if we do suricata-update, it will consider the rule as modified one and revert it back.(in order to do nothing with changes, we have to update that rule sid in modify conf).

But here the tool must act like management tool right irrespective of downloading and managing....

No, it always rebuilds from from online or the cache. It will only go online if the cache is older than 15 minutes. You can force it to not go online with the --offline option.

The process is:
- Load files from cache
- Make modifications
- Write output

So you are telling, if we modify any rule from alert to drop manually and if we do suricata-update, it will consider the rule as modified one and revert it back.(in order to do nothing with changes, we have to update that rule sid in modify conf).

That is correct. It doesn't look at any modifications you may have made to the output file. If you use suricata-update, you must use it to make your modifications. This is the same as the tools before this like Oinkmaster and PullPork.

ok thanks for the information.

- Priority changed from Urgent to Normal

Hi Rahul!

Does Jason's comment help you with your situation? Please let us know if we're good to close this issue now. Thank you.
Status changed from New to Closed

Closing this issue assuming it has been resolved because of inactivity. Please feel free to open a new issue in case you face this again. Thank you.