modify regexes not being applied reliably

Example converting all drop rules with noalert back to alert:

re:. "^drop(.*)noalert(.*)" "alert\1noalert\2"

This fails to work on the following rule (leaves it unmodified):


I've tested this regex (https://regex101.com/r/rqBaSC/3) and it should be applied to this rule, but is not. It is not only this rule that is effected. I have not been able to identify why this rule or any other is being exempted from modification.

Related Issues:
Related to Documentation #3535: Document the order in which configuration is ... Assigned

History
#1 - 03/03/2020 12:30 PM - J Cliff Armstrong
Appologies, I am very very tired. suricata-update version is `suricata-update version 1.1.0 (rev: 63493db)`

#2 - 03/09/2020 09:47 PM - Kenneth Kolano
This is likely due to the flowbits.

Flowbit rules are re-enabled late in the update process. To disable these rules one apparently must purge the flowbits clause from the rules in addition to disabling them. Refer... https://redmine.openinfosecfoundation.org/issues/3102

#3 - 03/09/2020 10:55 PM - J Cliff Armstrong
- File modify.conf added

There seems to be a misunderstanding. I am not attempting to disable any rules. I'm using `/etc/suricata/modify.conf` to change the rules of certain classtypes from alert to reject/drop (suricata is operating in IPS mode). Then the rule above is last in the file and is used to change rules with the `noalert` keyword back from reject/drop to alert. It's unclear from the documentation what regex capabilities are available (I assume whatever python provides) but I felt using read-aheads would be unnecessarily computationally expensive/prone to error and simply reverting such rules at the end a better choice.

I've attached my current modify.conf as an example. I've removed the `^` anchor from the modify rules so that commented suricata rules will be affected as well without "enabling" them. Then, if they are enabled elsewhere, they should be set to the correct action. Regardless, I have tried with the modify rule exactly as stated in the documentation and it does not correctly apply the change from reject/drop back to alert in all cases.

Additionally, I've recompiled suricata to the latest stable version and so now have suricata-update 1.1.1... the issue remains.

#4 - 03/10/2020 03:54 AM - Kenneth Kolano
You may need to revise the rev # as well?

#5 - 03/10/2020 05:04 AM - J Cliff Armstrong
Kenneth Kolano wrote in #note-4:

You may need to revise the rev # as well?

```bash
wolferz@tiphares ~ $ sudo suricata-update -V
suricata-update version 1.1.1
```

:-/ no revision listed.

#6 - 03/10/2020 06:53 PM - Jason Ish

The problem here is that the original rule is commented out: "#alert tcp any any ...". Your modifications that turn this into a drop don't consider the enabled state of the rule, so its converted to "#drop ...". Your reversion does consider the commented out, so it never gets converted back.

The flowbit resolution comes up and sees this rule is required by another enabled rule, and turns it on, but in its drop state.

My suggestion is to keep your conversion to drop rules only to those that are enabled. For example:

```regex
re:classtype:s\*attempted-dos
   "^alert\.(.*)" "drop\\1" # medium Attempted Denial of Server
```

Which should resolve this issue.

#7 - 03/10/2020 06:55 PM - Jason Ish

- Tracker changed from Bug to Support

Changing tracker to support for now.

#8 - 03/10/2020 07:05 PM - J Cliff Armstrong

Jason Ish wrote in #note-6:

Your reversion does consider the commented out, so it never gets converted back.

No, it doesn't. Check the modify.conf file I attached. As I explicitly stated in my previous note, I removed the `^` anchor from all modify rules. All of them. The problem remains. Putting it back on all modify rules also doesn't solve the problem (even if this rule is fixed, others aren't).

Oops. Typo on my part. Should have set does not consider the commented out.

I see the problem now, 2014384 does not have noalert set, and is disabled by default. So what is happening is:
- Rule is modified from "# alert ..." to "# drop ..."
- At this point is does not have noalert set, so the regex to turn it back into an alert will not match.
- This rule is now enabled as part of flowbit resolution, which is what enables it and adds noalert.

Open for discussion is if a drop rule is enabled as part of flowbit resolution, should it also be converted to alert?

For now, I'd suggest your modify.conf match and convert rules that are "*alert", so you don't change disabled rules.

If you are having issues with another rule, please point it out specifically.

#9 - 03/10/2020 09:20 PM - Jason Ish

J Cliff Armstrong wrote in #note-8:

Jason Ish wrote in #note-6:

Your reversion does consider the commented out, so it never gets converted back.

No, it doesn't. Check the modify.conf file I attached. As I explicitly stated in my previous note, I removed the `^` anchor from all modify rules. All of them. The problem remains. Putting it back on all modify rules also doesn't solve the problem (even if this rule is fixed, others aren't).

Oops. Typo on my part. Should have set does not consider the commented out.

The problem now, 2014384 does not have noalert set, and is disabled by default. So what is happening is:
- Rule is modified from "# alert ..." to "# drop ..."
- At this point is does not have noalert set, so the regex to turn it back into an alert will not match.
- This rule is now enabled as part of flowbit resolution, which is what enables it and adds noalert.

Open for discussion is if a drop rule is enabled as part of flowbit resolution, should it also be converted to alert?

For now, I'd suggest your modify.conf match and convert rules that are "*alert", so you don't change disabled rules.

If you are having issues with another rule, please point it out specifically.

#10 - 03/11/2020 02:51 PM - J Cliff Armstrong

Ah, I see.

What order are the suricata-update configuration files processed in? I can't find it in the documentation. As long as enable.conf is processed before modify.conf then I can do as you suggest without issue. Otherwise I'm going to have to start using modify.conf to enable rules as well to ensure they get enabled first.

06/12/2020
J Cliff Armstrong wrote in #note-10:

Ah, I see.

What order are the suricata-update configuration files processed in? I can't find it in the documentation. As long as enable.conf is processed before modify.conf then I can do as you suggest without issue. Otherwise I'm going to have to start using modify.conf to enable rules as well to ensure they get enabled first.

Yeah, this doesn't appear to be documented. We'll have to do so. The order is:
- disable.conf
- enable.conf
- drop.conf
- modify.conf

#12 - 03/17/2020 07:44 AM - Shivani Bhardwaj

- Related to Documentation #3535: Document the order in which configuration is applied to rules added

#13 - 03/17/2020 07:45 AM - Shivani Bhardwaj

Hi J Cliff Armstrong!

Does Jason's suggestion help you with your issue? I have added a ticket to update the documentation regarding the same. Please let me know if this works for you and if this issue can be closed. Thanks for reporting!

#14 - 03/17/2020 11:33 AM - J Cliff Armstrong

Apologies, I've had the last few days overturned by Covid-19 related issues.

Yes, it seems the issue is resolved, now that I'm aware of the addition of `noalert;` to rules which are auto-enabled for flowbits it is also clear why I must anchor the regexes to the beginning of the line. I'd suggest this is added to the documentation as well, assuming I didn't simply miss it.

#15 - 03/17/2020 11:52 AM - Shivani Bhardwaj

Please expect this in the documentation in the next major release. Closing the issue for now. In case you come across anything similar again, please feel free to open a new issue.

Stay safe!

#16 - 03/17/2020 11:52 AM - Shivani Bhardwaj

- Status changed from New to Closed

Files

<table>
<thead>
<tr>
<th>File</th>
<th>Size</th>
<th>Date</th>
<th>User</th>
</tr>
</thead>
<tbody>
<tr>
<td>modify.conf</td>
<td>5.92 KB</td>
<td>03/09/2020</td>
<td>J Cliff Armstrong</td>
</tr>
</tbody>
</table>