IDS Rule updater - with rule state persistance

IDS Rule updater - with rule state persistance

by **TimF** » June 26th, 2018, 4:56 pm

TimF
Posts: 83
Joined: June 10th, 2017, 7:27 pm

I've now got a script running that will not only download Snort rule updates automatically, but will also persist the state of existing rules. So if you want to enable all the rules and still have them enabled after an update, you can now do this (but don't – it's a really bad idea to enable all the rules). It also includes more checks than the previous script, adds a log page so you can see what's going on and can email you when it does an update.

The caveat is that doing a manual update will reset the state of the rules; it's only automatic updates that will persist the state.

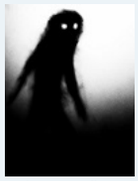
I've got it running on two machines and it seems to be working, but it should still be considered to be experimental. If you want to try it then go to:

https://github.com/timfprogs/ipfidsupdate

Make sure you read the instructions and especially the notes.

Re: IDS Rule updater - with rule state persistance

by **Roberto Peña** » June 26th, 2018, 6:59 pm



Roberto Peña
Posts: 761
Joined: July 16th, 2014, 3:56 pm
Location: Bilbao (España)
Contact:

Good afternoon TimF.

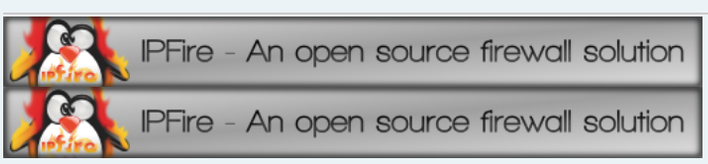
It looks good. But when I install it, it gives me the following error:

> VERSION 100%[===================>] 2 --.-KB/s in 0s
>
> 2018-06-26 20:56:00 (139 KB/s) - 'VERSION' saved [2/2]
>
> **./install-idsupdate.sh: line 96: /2: syntax error: operand expected (error token is "/2")**
>
> ---
>
> The system can check for an update to the rule files at a number
> of different rates: Hourly, Daily or Weekly. It will check for

Nor do I see any new page as it puts on the GitHub.

Does the new page appear to you?

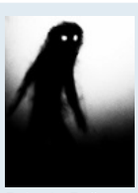
Greetings.



Donate to improve IPFire: https://www.ipfire.org/donate

Re: IDS Rule updater - with rule state persistance

by **Roberto Peña** » June 26th, 2018, 7:41 pm



Roberto Peña
Posts: 761
Joined: July 16th, 2014, 3:56 pm
Location: Bilbao (España)
Contact:

I'm sorry to say that by following the steps described, it has not been installed correctly.

I had to create or copy files by hand.

I have consulted this file and I have known what I had to copy:

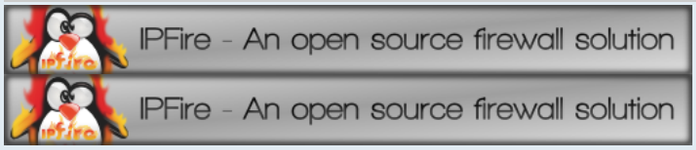
CODE: SELECT ALL

```
snort-update.pl /usr/local/bin root.root 0755  ---> Copy by hand.
ids-update.en.pl /var/ipfire/addon-lang root.root 0004 ---> Copy by hand.
idsflowbits.cgi /srv/web/ipfire/cgi-bin root.root 0755 ---> Copy by hand.
idsupdate.dat /srv/web/ipfire/cgi-bin/logs.cgi root.root 0755 ---> Copy by hand.
EX-idsupdate.menu /var/ipfire/menu.d nobody.nobody 644 ---> Copy by hand.
install-idsupdate.sh . root.root 0755
```

If you need more information, do not hesitate to ask me.

Greetings and good work.

Last edited by **Roberto Peña** on June 26th, 2018, 8:05 pm, edited 2 times in total.



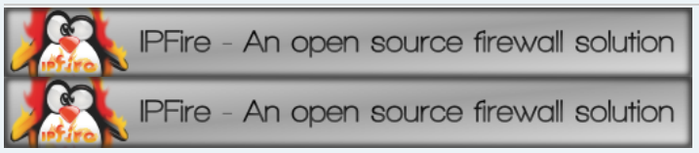
Donate to improve IPFire: https://www.ipfire.org/donate

Re: IDS Rule updater - with rule state persistance

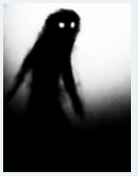
by **Roberto Peña** » June 26th, 2018, 8:04 pm

Another thing that I have seen is that it sends the emails without subject. It would be interesting if there was an subject in the mail.

Greetings.



Donate to improve IPFire: https://www.ipfire.org/donate



Roberto Peña

Posts: 761
Joined: July 16th, 2014, 3:56 pm
Location: Bilbao (España)
Contact:

Re: IDS Rule updater - with rule state persistance

by **TimF** » June 26th, 2018, 9:52 pm

I think I've fixed the problem – it was reading a null string for the downlink speed from the QOS settings and not handling it properly.

The lack of the log page and empty email subject is due to the language cache not being updated (the last thing the installer does). Running

CODE: SELECT ALL

```
update-lang-cache
```

from the command line should fix this.

(Both the boxes I've got running the script have just sent me emails saying they've installed updates)

TimF

Posts: 83
Joined: June 10th, 2017, 7:27 pm

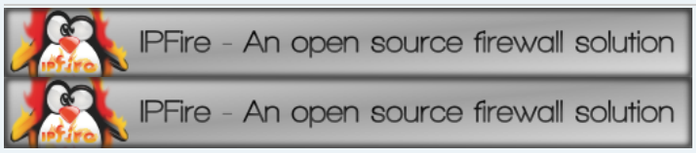
Re: IDS Rule updater - with rule state persistance

by **Roberto Peña** » June 27th, 2018, 4:53 am

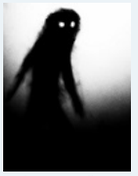
Thanks for answering.

Now it works correctly. When there is an improvement, post it.

Greetings.



Donate to improve IPFire: https://www.ipfire.org/donate



Roberto Peña

Posts: 761
Joined: July 16th, 2014, 3:56 pm
Location: Bilbao (España)
Contact:

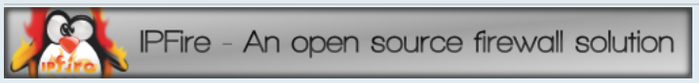
Re: IDS Rule updater - with rule state persistance

by **Drexbengel48** » July 6th, 2018, 4:26 am

Hi TimF,

looks really nice, thanx for your work!

Greetings!



Drexbengel48

Posts: 6
Joined: June 12th, 2017, 4:50 am
Location: Berlin

Re: IDS Rule updater - with rule state persistance

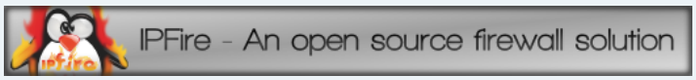
by **xPliZit_xs** » July 16th, 2018, 3:15 pm

Hello TimF,

this is working great so far!
Thanks for making it available to the community.

regards

xPliZit_xs



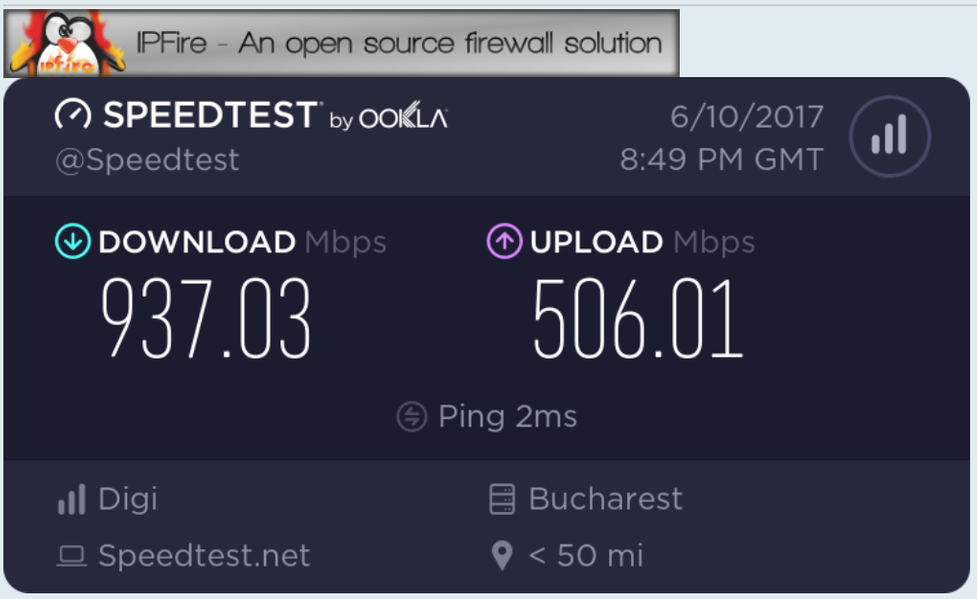
xPliZit_xs

Posts: 127
Joined: May 31st, 2014, 8:22 pm

Re: IDS Rule updater - with rule state persistance

by **Deepcuts** » July 21st, 2018, 1:48 am

At the moment snort-update.pl does not get copied to /usr/local/bin most likely because it is not downloaded as stated (The installer will download the files and install them in the correct places)
Did not have too much time to look into this, but it is not working by only downloading the installer.



Deepcuts

Posts: 461
Joined: March 1st, 2016, 3:18 pm
Location: Romania

Re: IDS Rule updater - with rule state persistance

by **TimF** » July 21st, 2018, 12:24 pm

Hopefully it's fixed now.

A minor problem with the code which is meant to stop downloading files if the latest version is already installed.

TimF

Posts: 83
Joined: June 10th, 2017, 7:27 pm

Re: IDS Rule updater - with rule state persistance

by **TimF** » August 17th, 2018, 3:21 pm

I've now uploaded a new version. I'm not entirely sure the installer will work correctly, so it's on a branch at the moment. You can find it at:

https://github.com/timfprogs/ipfidsupdate/tree/version3

The major change is in the handling of community rules. While it's true that the Talos VRT rules contain a version of the community rules, for the registered ruleset this is a month out of date, so the script will now update the community rules if the VRT ruleset is in use, and will ensure that only the rule in the community ruleset are used where the rule is found in both rulesets. This should ensure that the latest version of the rule is in use.

The full changelist:

- Updated processing of community ruleset.
- Internal storage rearranged to use less memory.
- New WUI page added under 'Services' to configure the updater - the installer no longer asks questions.
- Added language files for French, German and Spanish. Unfortunately they're machine translated so I expect some errors.
- Summary of updates added to daily log summary.
- Check that all expected Snort processes are running is now more robust.
- Some name changes to prepare for the switch from Snort to Suricata.
- Drops privileges for the most critical sections of processing updates.
- Changed mechanism for deciding when to check updates.

Because of the name changes and the change to the timing the installer has to move some files about. It should do this correctly now (some of my tests didn't work fully), but you can check the following to make sure:

- fcrontab -l has a reference to ids-update.pl near the end, and not one to snort-update.pl
- There's no directory /var/ipfire/snortupdate
- /var/ipfire/idsupdate and /var/ipfire/idsupdate/settings are owned by nobody
- The rule files in /var/tmp are owned by nobody (but the backup is owned by root).

TimF

Posts: 83
Joined: June 10th, 2017, 7:27 pm

Re: IDS Rule updater - with rule state persistance

by **xPliZit_xs** » August 25th, 2018, 6:47 pm

Hi TimF,

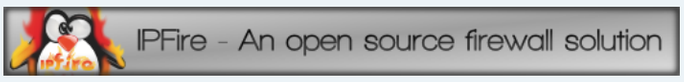
very nice.
I am having an issue with the "previous" version on core 123, its not working there anymore.
Must the "old" script/install uninstalled first?
However i am trying to install this new version now and see how it goes.

One more question,
Quote: Some name changes to prepare for the switch from Snort to Suricata.

Who or what is preparing to switch to Suricata?
I would be interested to use it as well since its using more than one core.

thx

xPliZit_xs



xPliZit_xs

Posts: 127
Joined: May 31st, 2014, 8:22 pm

Re: IDS Rule updater - with rule state persistance

by **TimF** » August 26th, 2018, 1:27 pm

TimF
Posts: 83
Joined: June 10th, 2017, 7:27 pm

Hi xPliZit_xs,

Have you any idea why it's stopped working in 123? If not a couple of things to check –

- Have a look at the crontab – log in as root and run `fcrontab -l` (lower case L). There should be a reference to `snort-update.pl` (`ids-update.pl` for the new version), probably near the bottom. A possibility is that core update 123 has replaced the crontab, removing this line.
- If the entry is in the crontab, try running the rule update script from the command line `/usr/local/bin/snort-update.pl` and see if that gives any errors.

Updating to the new version should not require the old version to be removed – the installer should rename, move files about and change permissions as necessary. However I'm not entirely sure of this, which is why it's on a separate branch. I believe that I've fixed all the problems that came up installing it on my machines, but there could be additional problems on a different set up. It's a good ideas to do the checks at the end of my previous post.

If the entry has gone from the crontab and you don't want to update to the new version, you should just be able to run the old installer.

The switch from Snort to Suricata is something the developers are working on. It was planned for IPFire V3, but they've decided to also implement it in V2 – it's ability to use multiple cores is, I think, one reason for the change. I can't tell you any more than that – all I've seen is a couple of entries in bugzilla and a couple of messages on the mailing list.

Re: IDS Rule updater - with rule state persistance

by **xPliZit_xs** » August 26th, 2018, 4:01 pm

xPliZit_xs
Posts: 127
Joined: May 31st, 2014, 8:22 pm

Hi,

i recently migrated from bare metal ipfire to a virtualized environment and use the ipfire backup to restore my data.
Then i installed the snort updater and since then i don't saw it working again. Reinstalled it multiple times but no luck.

With the new version of the IDS updater i have not seen an update yet:
Last rule update was Fri Aug 24 17:09:57 2018 according the GUI.
Perhaps they don't update rules during the weekend.

This is at the end of the fcrontab file:
Snort rule update
%nightly,nice(1),random(true),serialonce(true) 15-45 23-4 /usr/local/bin/snort-update.pl

Snort rule update
%hourly,nice(1),random,serialonce(true) 6-16 /usr/local/bin/ids-update.pl

running it manually gives this:
[root@ipfire bin]# ./ids-update.pl
(6) Starting Snort update check
(7) Connection and disk space checks OK
(7) Reading Oinkmaster configuration
(7) Reading classification file /etc/snort/rules/classification.config
(7) Reading classification file /etc/snort/rules/EMERGING_THREATS_classification.config
(7) Check for Emerging Threats Open update
(7) Versions: Old c2b9efcdc00f799204598d9efcc77f82, new c2b9efcdc00f799204598d9efcc77f82
(6) No updates available
(6) Checking that Snort is running correctly

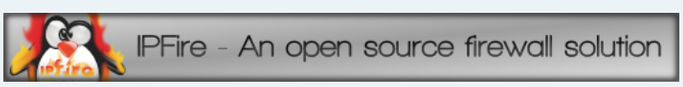
That looks OK i guess.

Assume that it should now work, i can probably remove the entry for the snortupdate since its outdated.
Thanks for your help.

regards

---

xPliZit_xs



Re: IDS Rule updater - with rule state persistance

by **TimF** » August 27th, 2018, 1:50 pm

TimF
Posts: 83
Joined: June 10th, 2017, 7:27 pm

The entry for snort-update.pl should have been removed by the installer – I've corrected it.

The output from running it looks OK. The Emerging Threats rules are updated around midnight (UK time) on weekdays so the true test that it's working OK should come tonight. Hopefully tomorrow you'll be able to see the evidence that the rules have been updated in Services > IDS Update, Logs > IDS Update Logs, and Logs > Log Summary.

Powered by phpBB® Forum Software © phpBB Limited
Privacy | Terms

IDS Rule updater - with rule state persistance

Re: IDS Rule updater - with rule state persistance

by **JonM** » August 27th, 2018, 5:18 pm

JonM
Posts: 144
Joined: August 4th, 2017, 5:49 pm
Location: US

> **TimF wrote:** ↑ August 27th, 2018, 1:50 pm
> The entry for snort-update.pl should have been removed by the installer - I've corrected it.

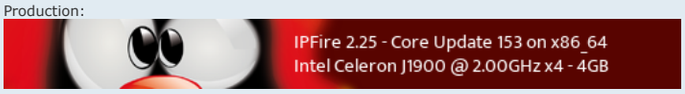
Is the **snort-update.pl** to be removed? or **ids-update.pl**?

EDIT: I found this line in crontab, should it be removed?

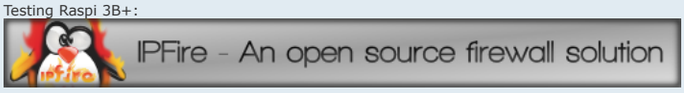
CODE: SELECT ALL

```
[root@ipfire ~]# fcrontab -l
...
# Update snort rules
#%hourly,random 3-29 /var/ipfire/snort/update.sh
...
```

Production:



Testing Raspi 3B+:



Re: IDS Rule updater - with rule state persistance

by **Drexbengel48** » August 28th, 2018, 2:37 am

Drexbengel48
Posts: 6
Joined: June 12th, 2017, 4:50 am
Location: Berlin

> **TimF wrote:** ↑ August 17th, 2018, 3:21 pm
> I've now uploaded a new version. I'm not entirely sure the installer will work correctly, so it's on a branch at the moment. You can find it at:
>
> https://github.com/timfprogs/ipfidsupdate/tree/version3
>
> The major change is in the handling of community rules. While it's true that the Talos VRT rules contain a version of the community rules, for the registered ruleset this is a month out of date, so the script will now update the community rules if the VRT ruleset is in use, and will ensure that only the rule in the community ruleset are used where the rule is found in both rulesets. This should ensure that the latest version of the rule is in use.
>
> The full changelist:
>
> - Added language files for French, German and Spanish. Unfortunately they're machine translated so I expect some errors.

Hi TimF,
can you please correct the lines in

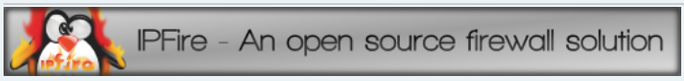
https://github.com/timfprogs/ipfidsupda ... date.de.pl

CODE: SELECT ALL

```
62 'idsupdate daily' => 'Daily',
63 'idsupdate weekly' => 'Täglich',
```

THX!!!

Greetings
Drexbengel48



Re: IDS Rule updater - with rule state persistance

by **TimF** » August 28th, 2018, 7:14 pm

TimF
Posts: 83
Joined: June 10th, 2017, 7:27 pm

@JonM snort-update.pl should be removed if you're using the latest version of the script.

I'm not sure where the other line came from, but it should be able to be removed.

@Drexbengel48 I've edited the file - hopefully correctly.

Re: IDS Rule updater - with rule state persistance

by **xPliZit_xs** » August 30th, 2018, 9:32 pm

xPliZit_xs
Posts: 127
Joined: May 31st, 2014, 8:22 pm

Hi TimF,

the new version is working for me using core123 again!

Thank you.

xPliZit_xs

IPFire - An open source firewall solution

Re: IDS Rule updater - with rule state persistance

by **xPliZit_xs** » September 30th, 2018, 1:54 am

xPliZit_xs
Posts: 127
Joined: May 31st, 2014, 8:22 pm

Hello TimF,

i am testing core 124 and the rule updater seems not to work anymore.
The services and Logs menu are missing.
This is just a head's up.

This is the install procedure output from the shell, maybe you can see whats wrong there already.

```
==========================================================================================
[root@ipfire ~]# wget https://github.com/timfprogs/ipfidsupda ... supdate.sh
--2018-09-29 21:48:04-- https://github.com/timfprogs/ipfidsupda ... supdate.sh
Resolving github.com... 192.30.253.113, 192.30.253.112
Connecting to github.com|192.30.253.113|:443... connected.
HTTP request sent, awaiting response... 302 Found
Location: https://raw.githubusercontent.com/timfp ... supdate.sh [following]
--2018-09-29 21:48:04-- https://raw.githubusercontent.com/timfp ... supdate.sh
Resolving raw.githubusercontent.com... 151.101.128.133, 151.101.192.133, 151.101.0.133, ...
Connecting to raw.githubusercontent.com|151.101.128.133|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 4439 (4.3K) [text/plain]
Saving to: 'install-idsupdate.sh'

install-idsupdate.sh 100%[=========================================>] 4.33K --.-KB/s in 0s

2018-09-29 21:48:04 (202 MB/s) - 'install-idsupdate.sh' saved [4439/4439]

[root@ipfire ~]# chmod +x install-idsupdate.sh
[root@ipfire ~]# ./install-idsupdate.sh
read old settings
Check for new version
--2018-09-29 21:48:20-- https://github.com/timfprogs/ipfidsupda ... n3/VERSION
Resolving github.com... 192.30.253.112, 192.30.253.113
Connecting to github.com|192.30.253.112|:443... connected.
HTTP request sent, awaiting response... 302 Found
Location: https://raw.githubusercontent.com/timfp ... n3/VERSION [following]
--2018-09-29 21:48:20-- https://raw.githubusercontent.com/timfp ... n3/VERSION
Resolving raw.githubusercontent.com... 151.101.0.133, 151.101.64.133, 151.101.128.133, ...
Connecting to raw.githubusercontent.com|151.101.0.133|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 2 [text/plain]
Saving to: 'VERSION'

VERSION 100%[=========================================>] 2 --.-KB/s in 0s

2018-09-29 21:48:20 (757 KB/s) - 'VERSION' saved [2/2]

2018-09-29 21:48:20 INFO listing root's fcrontab
2018-09-29 21:48:20 INFO installing file /root/fcrontab_old for user root
Modifications will be taken into account right now.
[root@ipfire ~]
==========================================================================================
=====================================
```

xPliZit_xs

IPFire - An open source firewall solution

Re: IDS Rule updater - with rule state persistance

by **TimF** » October 5th, 2018, 5:30 pm

TimF
Posts: 83
Joined: June 10th, 2017, 7:27 pm

Hello,

There's some code in the installer that is meant to stop it downloading files unless they belong to a newer version than the version that's installed. That's probably the reason the installer seems not to work.

I've removed it because I don't think it's really necessary.

Re: IDS Rule updater - with rule state persistance

by **xPliZit_xs** » October 5th, 2018, 8:40 pm

xPliZit_xs
Posts: 127
Joined: May 31st, 2014, 8:22 pm

Nice! Going to try it again.

xPliZit_xs

IPFire - An open source firewall solution

Re: IDS Rule updater - with rule state persistance

by **xPliZit_xs** » October 7th, 2018, 6:53 pm

xPliZit_xs
Posts: 127
Joined: May 31st, 2014, 8:22 pm

Hello,

it seems to install with core124 correctly if you download the correct github branch haha.

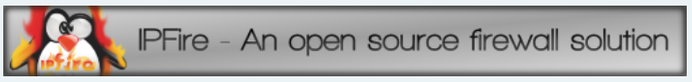
FYI:
USE: wget https://github.com/timfprogs/ipfidsupda ... supdate.sh

DONT USE: wget https://github.com/timfprogs/ipfidsupda ... supdate.sh

have to wait till it updates automatically...

regards

xPliZit_xs



Re: IDS Rule updater - with rule state persistance

by **TimF** » October 12th, 2018, 3:01 pm

TimF
Posts: 83
Joined: June 10th, 2017, 7:27 pm

The version 3 changes works, so I merged them onto the master branch and I modified the updater on that branch. So the version 3 branch is now obsolete.

Re: IDS Rule updater - with rule state persistance

by **dnl** » November 6th, 2018, 9:06 am

dnl
Posts: 375
Joined: June 28th, 2013, 11:03 am

Hi TimF,

Thanks for this, I've been busy and haven't read the forums in a very long time. Looks like I've missed out!

I've just updated the IPFire Security Hardening guide to reference the first post in this thread, rather than the old "snortupdate.pl" script written by Kick@ass, H&M and gitarman94 as that script doesn't seem to be maintained any longer and appears to have less features than yours.

I've been really annoyed by getting thousands of IDS hits daily, when the vast majority are just from blocklists. So I'll check out your blocklist addon also!

Have you spoken to one of the core developers about having your addons packaged as official IPFire addons? I'd rather not automate the download and execution of shell scripts from a remote website.

Thanks!

IPFire 2.x (Latest Update) on x86_64 Intel Bay Trail CPU, 4GiB RAM, RED + GREEN + BLUE + ORANGE

Re: IDS Rule updater - with rule state persistance

by **raffe** » November 6th, 2018, 10:10 am

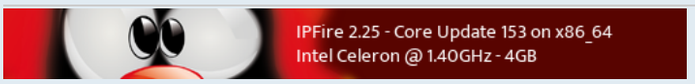
raffe
Posts: 17
Joined: August 20th, 2018, 8:40 am

Hi! Thanks for an excellent script! I think I soon have tweaked the choices of rules and flowbits so I can start thinking about blocklists 😃

But before that, I have one question about the "**Default policy**" setting in https://ipfire:444/cgi-bin/idsupdate.cgi. I can choose *Connectivity, Balanced, Security* and *Max-Detect*.

What do these settings really do? Do they set or change some rules? If so, how will the settings co-exist with the rules I have manually chosen? Or is this setting only activated and used during the automatic update?

With best regards
raffe



Re: IDS Rule updater - with rule state persistance

by **TimF** » November 7th, 2018, 8:57 pm

TimF
Posts: 83
Joined: June 10th, 2017, 7:27 pm

The settings affect new rules. The script will evaluate new rules against your selected policy and will enable the rule if it's in the selected policy or disable it if not. The default policy is 'Balanced' - this is what you would get if you just downloaded the rule files. It doesn't affect your existing rule selections.

In addition it will warn you of changes to rules that you've enabled (or disabled) and would normally be disabled (or enabled) in your policy. This is in case the reason that you enabled (or disabled) the rule is no longer valid.

Finally, if you select 'Apply policy changes' it will enable or disable rules if their policy changes. So, for example, if you've got a rule selected that is in the balanced policy, and that is your selected policy, it will disable the rule if the policy of the rule changes to 'Security'. This is very rare.

Re: IDS Rule updater - with rule state persistance

by **raffe** » November 8th, 2018, 9:22 am

raffe
Posts: 17
Joined: August 20th, 2018, 8:40 am

Thanks for the answer!

> **dnl wrote:** ↑ November 6th, 2018, 9:06 am
> Have you spoken to one of the core developers about having your addons packaged as official IPFire addons?

I agree with DNL, this is so good and important that it should really be included as an official addon! 😎

Or are you waiting for this? viewtopic.php?f=27&t=8323&start=75#p120129

IPFire 2.25 - Core Update 153 on x86_64
Intel Celeron @ 1.40GHz - 4GB

Re: IDS Rule updater - with rule state persistance

by **dnl** » November 8th, 2018, 9:54 am

dnl
Posts: 375
Joined: June 28th, 2013, 11:03 am

> **raffe wrote:** ↑ November 8th, 2018, 9:22 am
> I agree with DNL, this is so good and important that it should really be included as an official addon! 😎
>
> Or are you waiting for this? viewtopic.php?f=27&t=8323&start=75#p120129

Even if the Suricata feature comes with automatic updates, I still like the idea of moving the blocklist rules out.

So TimF can you please ask the core developers about including your other add-on? https://github.com/timfprogs/ipfblocklist

IPFire 2.x (Latest Update) on x86_64 Intel Bay Trail CPU, 4GiB RAM, RED + GREEN + BLUE + ORANGE

Re: IDS Rule updater - with rule state persistance

by **Hellfire** » November 16th, 2018, 6:49 pm

Hellfire
Posts: 697
Joined: November 8th, 2015, 8:54 am

Hi,

I've got a couple of questions, although some have already been asked above, there are still some (if not all) settings that are unclear to me at the moment:

I will start from the beginning:

1) If I configure IDS-Update for performing automatic updates, which rule sets will it download? All available sets from the drop down list configured at IDS: https://ipfire:444/cgi-bin/ids.cgi or just the one and only that is selected and saved.
I guess the later is true because both pages (IDS and IDS update) show exactly the same timestamp for the latest ruleset update, am I correct?

2) Although some explanations have been given für option "Default policy". Does the updater automatically choose which rules are best for me according to this option? What exactly happens when selecting:
Connectivity:
Balanced:
Security:
Max-Detect:
in respect to my already checked or unchecked rules from https://ipfire:444/cgi-bin/ids.cgi ?

3) Enabled live updates: What does this option mean? I thought checking "Enable automatic updates" already does the job of automatic ruleset updates?

4) Apply policy changes: You stated

> "it will enable or disable rules if their policy changes. So, for example, if you've got a rule selected that is in the balanced policy, and that is your selected policy, it will disable the rule if the policy of the rule changes to 'Security'. This is very rare"

I don't get the exact meaning of this quoted sentence. Does it mean, if I make any changes to option 2), the updater will automatically switch on/off rules that are not found within the new "Default policy"? This again raises the question where can I find the appropriate rules/rulesets behind Connectivity, Balanced, Security, Max-Detect?

5) Last but not least: Do I still have to check or unecheck those rules at https://ipfire:444/cgi-bin/ids.cgi for IDS updater to work correctly? Does this apply too for sub rules? Or is this job done by the updater according to the option chosen at 2)

Thanks for reading,
Michael

IPFire 2.25 - Core Update 153 on x86_64
AMD GX-412TC SOC @ 979MHz x2 - 4GB

Powered by phpBB® Forum Software © phpBB Limited
Privacy | Terms

IDS Rule updater - with rule state persistance

Re: IDS Rule updater - with rule state persistance

by **TimF** » November 17th, 2018, 6:15 pm

TimF
Posts: 83
Joined: June 10th, 2017, 7:27 pm

Hi Michael,

1) It will update any rulesets that you've previously downloaded, not just the currently selected one. (It looks at the rulefiles in /etc/snort/rules - community.rules is the community rules, emerging-*.rules is Emerging Threats, anything else is Talos VRT). This means that any rules listed in the Intrusion Detection WUI will be kept up to date.

2) For new rules the updater will choose to enable or disable the rule based on the selected default policy. Rules you've previously checked or unchecked in the Intrusion Detection WUI will be left in the checked or unchecked state you selected unless:

- You've checked 'Apply policy changes' *and*
- An updated version of the rule has a different policy.

In this case the rule will be enabled or disabled depending on the chosen policy.

The policies Connectivity -> Balanced -> Security -> Max-Detect have increasing numbers of rules enabled, with 'Connectivity' having the least and 'Max-Detect' the most. Each policy includes all the rules from the lower policies. The updater works out which policy a rule belongs to based on information in the rule. If you just use the WUI to manually download an update it implicitly uses the 'Balanced' policy.

3) Enable live update affects how the updated rules are applied. The default (and the method used by a manual update) is to stop all the instances on Snort and then to re-start them with the new rules. The problem with this is that your network will not be protected by the Intrusion Detection rules during this period, which will probably be a few minutes.

If you select 'Enable live update' the updater will tell Snort to re-read the rules without stopping, which means you will be protected throughout the update, however to do this the process is similar to starting up another instance of Snort to read the new rules, and then swapping it with the existing instance; this means that this method uses quite a bit more memory. If you run out of memory, the system will kill a process (this will change under core update 125).

If you're short on memory and you don't have reason to expect your network to be deliberately targeted, it should be OK not to check this option.

For an estimate of the extra memory, look at how much memory your Snort processes are using under 'Status > Services' in the WUI - you'll use about as much extra memory as one of the Snort processes is using. This is in addition to the memory used by the updater itself - which could be up to 140MB, depending on the selected rulesets.

4) If you have 'Apply policy changes' checked and you change the default policy it will not make any changes to the already existing rules unless, at some point in the future, the rule is changed. In this case the rule will be enabled or disabled according to the selected default policy and the policy of the rule. If you have 'Apply policy changes' unchecked the updater will not make changes to the state of existing rules, but only to new rules.

Unfortunately there's no list of which rules belong in which policy (or at least I can't find one). The Snort FAQ gives the information as to how Talos VRT assign policies, but I doubt you'll find it very helpful. The updater attempts to synthesise the policy from the data included in the rule.

The updater applies the following algorithm to work out the policy:

1. If there's metadata in the rule giving the policy, use it.
2. otherwise use the priority of the rule with a priority of one corresponding to 'Connectivity' and four to 'Max-Detect'.
3. make sure the resulting policy is either 'Connectivity' or 'Balanced' if the rule is distributed uncommented and 'Security' or 'Max-Detect' if it's commented (this corresponds to the process that the rule source uses to decide whether they're going to distribute the rule commented or uncommented).

The end result is a policy that should be a good approximation to the policy as decided by the supplier.

The most important outcomes of this process is that each policy has more rules included than the next lower policy and that selecting the 'Balanced' policy will select the same rules as just applying the update without any processing.

If you select 'Balanced' as your default policy you will get the same rules enabled or disabled as you would using a manual download of the rules, with only the changes you've made from the WUI.

5) You need to check or uncheck the rule categories that you want in the Intrusion Detection WUI; this controls whether Snort reads the rules from the corresponding rulefile. If a category is not checked, none of the rules in that category will be seen by Snort, no matter whether they're enabled or disabled or whether it's done manually or automatically from the updater. Note that the updater will still update the rules in the disabled categories - it's just that the rules won't be used.

For the individual rules under the top level categories, their state shown reflects the state of the rule. Any changes made by the updater will be shown here and any changes made manually will be taken into account the next time that an update is downloaded. this means that in most cases you can leave the state of individual rules to the updater, but you can still change the state of rules manually if you want.

I hope this answers all your questions adequately. Unfortunately some of the answers are a little completed.

Tim

Re: IDS Rule updater - with rule state persistance

by **Hellfire** » November 17th, 2018, 8:45 pm

Hellfire
Posts: 697
Joined: November 8th, 2015, 8:54 am

Thanks Tim for this comprehensive answer. I will go through your posting the next days.

Highly appreciated, thanks!

IPFire 2.25 - Core Update 153 on x86_64
AMD GX-412TC SOC @ 979MHz x2 - 4GB

Re: IDS Rule updater - with rule state persistance

by **skyfighter** » November 21st, 2018, 6:29 am

skyfighter
Posts: 12
Joined: November 15th, 2018, 7:12 pm

In the log files I get the error code "Oinkmaster failed returning 65280" and the number of activated rules doesn't change all the time. What does that mean and what can I do?

Re: IDS Rule updater - with rule state persistance

by **TimF** » November 21st, 2018, 8:08 pm

TimF
Posts: 83
Joined: June 10th, 2017, 7:27 pm

The most likely explanation is that some pf the old rulefiles in `/etc/snort/rules` have the wrong permissions. All the files should be owned by nobody and -rw-r--r-- . To fix:

CODE: SELECT ALL
```
chown nobody.nobody /etc/snort/rules/*
chmod 0644 /etv/snort/rules/*
```

If that doesn't work, try running `/usr/local/bin/ids-update.pl` from the command line, and look to see what errors you get.

Re: IDS Rule updater - with rule state persistance

by **skyfighter** » November 22nd, 2018, 5:29 pm

skyfighter
Posts: 12
Joined: November 15th, 2018, 7:12 pm

> TimF wrote: ↑ November 21st, 2018, 8:08 pm
> The most likely explanation is that some pf the old rulefiles in `/etc/snort/rules` have the wrong permissions. All the files should be owned by nobody and -rw-r--r-- . To fix:
>
> CODE: SELECT ALL
> ```
> chown nobody.nobody /etc/snort/rules/*
> chmod 0644 /etv/snort/rules/*
> ```
>
> If that doesn't work, try running `/usr/local/bin/ids-update.pl` from the command line, and look to see what errors you get.

This fixed it for me, thanks 🙂

Re: IDS Rule updater - with rule state persistance

by **H&M** » November 22nd, 2018, 8:27 pm

H&M
Posts: 471
Joined: May 29th, 2014, 9:38 pm
Location: Europe

Hi Tim,

Will it work for a fresh installed system that has never downloaded any rule?

in my case (fresh instal) I get these:

CODE: SELECT ALL
```
 /usr/local/bin/ids-update.pl
[root@black-x86-64 ~]#  /usr/local/bin/ids-update.pl
(6) Starting Snort update check
(7) Connection and disk space checks OK
(7) Reading Oinkmaster configuration
(3) Failed to open snort config file /etc/snort/rules/emerging.conf: No such file or directory
Failed to open snort config file /etc/snort/rules/emerging.conf: No such file or directory at /usr/local/bin/ids-update
```

I assume I have to make a manual download at least once, right?

PS: the snort.conf file with all active rules is already there, copied from an older system

Late edit:

IDSUpdate.cgi seems to have a problem to store the settings. No matter what I setup in there, next time when I open it is contains other values:

Download limit (kbit/s) = 0
Default policy = Connectivity (although I've setup Max-Detect)

Where are stored the values - just to check them...

Some errors are also reported by Squid in error_log:

CODE: SELECT ALL
```
cat error_log
[Sun Nov 18 00:01:01.683533 2018] [mpm_event:notice] [pid 14563:tid 139745323794944] AH00489: Apache/2.4.34 (Unix) Ope
[Sun Nov 18 00:01:01.683799 2018] [core:notice] [pid 14563:tid 139745323794944] AH00094: Command line: '/usr/sbin/http
[Thu Nov 22 23:10:27 2018] idsupdate.cgi: Use of uninitialized value in string eq at /srv/web/ipfire/cgi-bin/idsupdate
[Thu Nov 22 23:10:27 2018] idsupdate.cgi: Use of uninitialized value $settings{"EMAIL"} in string eq at /srv/web/ipfir
[Thu Nov 22 23:10:27 2018] idsupdate.cgi: Use of uninitialized value $mailsettings{"USEMAIL"} in string eq at /srv/web
[Thu Nov 22 23:10:42 2018] idsupdate.cgi: Use of uninitialized value $mailsettings{"USEMAIL"} in string eq at /srv/web
[Thu Nov 22 23:10:54 2018] idsupdate.cgi: Use of uninitialized value $mailsettings{"USEMAIL"} in string eq at /srv/web
[Fri Nov 23 08:14:01 2018] idsupdate.cgi: Use of uninitialized value in string eq at /srv/web/ipfire/cgi-bin/idsupdate
[Fri Nov 23 08:14:01 2018] idsupdate.cgi: Use of uninitialized value $mailsettings{"USEMAIL"} in string eq at /srv/web
[Fri Nov 23 08:14:15 2018] idsupdate.cgi: Use of uninitialized value $mailsettings{"USEMAIL"} in string eq at /srv/web
[Fri Nov 23 10:04:25 2018] idsupdate.cgi: Use of uninitialized value in string eq at /srv/web/ipfire/cgi-bin/idsupdate
[Fri Nov 23 10:04:25 2018] idsupdate.cgi: Use of uninitialized value $mailsettings{"USEMAIL"} in string eq at /srv/web
```

Thanks,
H&M

Re: IDS Rule updater - with rule state persistance

by **TimF** » November 23rd, 2018, 6:59 pm

TimF
Posts: 83
Joined: June 10th, 2017, 7:27 pm

You need to manually download your rules before the updater will work - it uses the existing rule files to work out which sets of rule to download.

I think the error:

CODE: SELECT ALL
```
(3) Failed to open snort config file /etc/snort/rules/emerging.conf: No such file or directory
```

is due to the old snort.conf file being used without any rule files existing. This should disappear when you download a set of rules.

For the second set of errors, the settings are in `/var/ipfire/idsupdate`: `settings` should be owned by nobody.nobody and `status` by root.root (status may not exist yet). Both should be `-rw-r--r--`. The directory should also be owned by nobody.nobody and `drwxr-xr-x`.

Re: IDS Rule updater - with rule state persistance

by **H&M** » November 23rd, 2018, 7:48 pm

H&M
Posts: 471
Joined: May 29th, 2014, 9:38 pm
Location: Europe

Thank you,

I did not know about idsupdate folder existence...

For the record, here is how it looks after install:

CODE: SELECT ALL
```
ls -l /var/ipfire/idsupdate/
total 264
-rw-r--r-- 1 root   root    74493 Nov 23 20:34 emerging_threats_oinkmaster.conf
-rw-r--r-- 1 nobody nobody    128 Nov 23 10:04 settings
-rw-r--r-- 1 root   root      141 Nov 23 20:42 status
-rw-r--r-- 1 root   root   180300 Nov 22 23:20 talos_vrt_oinkmaster.conf
```

I changed it like this:

CODE: SELECT ALL
```
ls -l /var/ipfire/idsupdate/
total 264
-rw-r--r-- 1 nobody nobody  74493 Nov 23 20:34 emerging_threats_oinkmaster.conf
-rw-r--r-- 1 nobody nobody    128 Nov 23 10:04 settings
-rw-r--r-- 1 root   root      141 Nov 23 20:42 status
-rw-r--r-- 1 nobody nobody 180300 Nov 22 23:20 talos_vrt_oinkmaster.conf
```

That seems to solve all errors:

CODE: SELECT ALL
```
 /usr/local/bin/ids-update.pl
(6) Starting Snort update check
(7) Connection and disk space checks OK
(7) Reading Oinkmaster configuration
(7) Reading classification file /etc/snort/rules/classification.config
(7) Reading classification file /etc/snort/rules/TALOS_VRT_classification.config
(7) Reading classification file /etc/snort/rules/EMERGING_THREATS_classification.config
(7) Check for Talos VRT registered or subscribed update
(7) Versions: Old 35bf06ce6b161e5f8d83d95bdb8abba6, new 35bf06ce6b161e5f8d83d95bdb8abba6
(7) Check for Emerging Threats Open No-GPL update
(7) Versions: Old e12c4ea090fb3bca80319a336971f7f3, new e12c4ea090fb3bca80319a336971f7f3
(6) No updates available
(6) Checking that Snort is running correctly
```

.

But there was an update available for emerging threats rules available ...

Snort.conf is manually updated to contain all rules - list is obtained with

CODE: SELECT ALL
```
ls -1 /etc/snort/rules/*.rules
```

Then list is manually added to short.conf.

Thank you!

H&M

Re: IDS Rule updater - with rule state persistance

by **Hellfire** » December 10th, 2018, 7:57 pm

Hellfire
Posts: 697
Joined: November 8th, 2015, 8:54 am

> TimF wrote: ↑ November 17th, 2018, 6:15 pm
> 1) It will update any rulesets that you've previously downloaded, not just the currently selected one. (It looks at the rulefiles in /etc/snort/rules - community.rules is the community rules, emerging-*.rules is Emerging Threats, anything else is Talos VRT). This means that any rules listed in the Intrusion Detection WUI will be kept up to date.

Hi Tim,

would it be possible to start over with IDS with the following steps?

1) Delete all current rulessets from /etc/snort/rules/*.rules
2) Re-Download rule sets e.g. "Emerginthreats.net Community Rules" and "Snort/VRT GPLv2 Community Rules"
3) Do not activate any of those listed categories and rules.
4) Change the default poliy of IDS Updater to e.g. "Security".
5) Activate option "Enable live update" and "Apply policy changes".
6) Manually update the rulsets with /usr/local/bin/ids-update.pl

Will those given steps automatically enable the appropriate categories and rules according to their policy and I do not have to worry about the rules anymore?

cu,
Michael

IPFire 2.25 - Core Update 153 on x86_64
AMD GX-412TC SOC @ 979MHz x2 - 4GB

Re: IDS Rule updater - with rule state persistance

by **TimF** » December 11th, 2018, 2:54 pm

TimF
Posts: 83
Joined: June 10th, 2017, 7:27 pm

Hi,

Unfortunately that won't work, since it'll read the state of the rulesets. I have though about adding a button to force the policy, but with the change to Suricata coming up that's not going to happen soon.

The only way I can think of to force a policy is:

1. Delete all the rulefiles fron /etc/snort/rules, leaving one in each category that you're interested in, that is community.rules (for the community rules), emerging-*.rules (for the Emerging Threats rules) and everything else (for the Talos VRT rules).
2. Empty these rule files, either with a text editor or by `echo > <filename>.rules`.
3. Change the default policy of the updater and activate option "Apply policy changes".
4. Delete the file `/var/ipfire/idsupdate/status`
5. Either run the updater from the command line with `/usr/local/bin/ids-update.pl` or wait for the next update to be due.

I think this will do what you want, but I've not tried it out.

Re: IDS Rule updater - with rule state persistance

by **Hellfire** » December 13th, 2018, 6:12 pm

Hellfire
Posts: 697
Joined: November 8th, 2015, 8:54 am

> TimF wrote: ↑ December 11th, 2018, 2:54 pm
> I think this will do what you want, but I've not tried it out.

Thank Tim, I will give it a try once my VM is up again...

IPFire 2.25 - Core Update 153 on x86_64
AMD GX-412TC SOC @ 979MHz x2 - 4GB

Re: IDS Rule updater - with rule state persistance

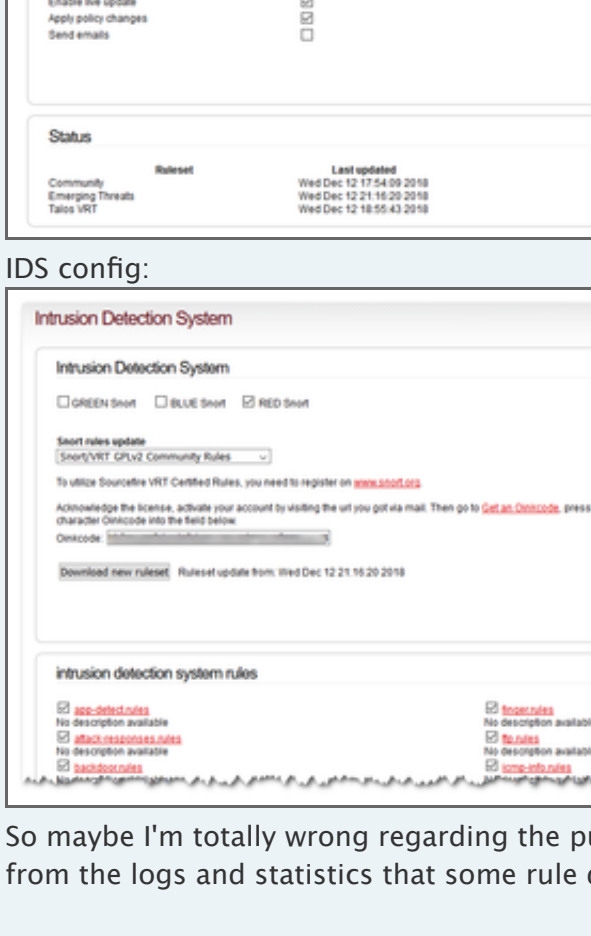
by **Hellfire** » December 13th, 2018, 6:20 pm

Hellfire
Posts: 697
Joined: November 8th, 2015, 8:54 am

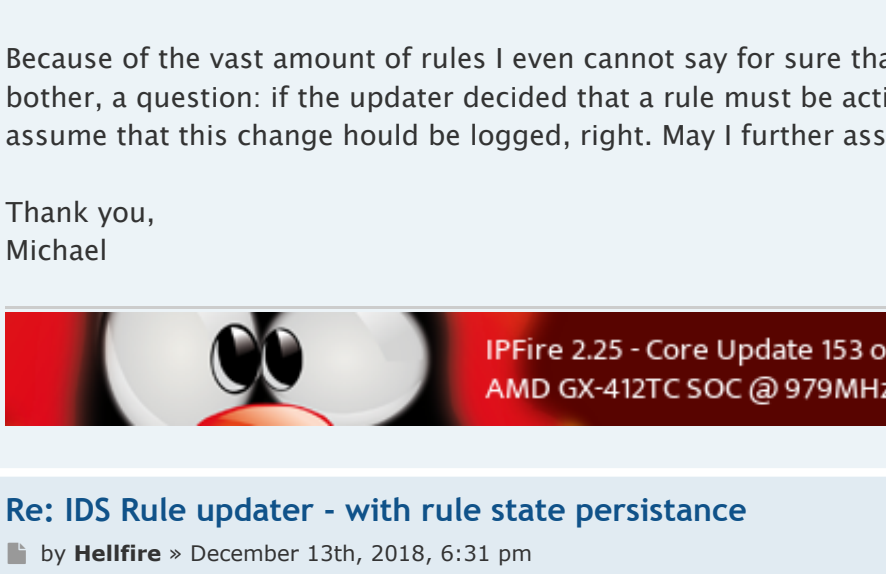
Hi Tim,

I really doubt that IDS Updater is doing anything on my IPFire - this does not mean the updater works wrong, that's no rant at all, however, the appropriate logs don't list any changes within the rules.

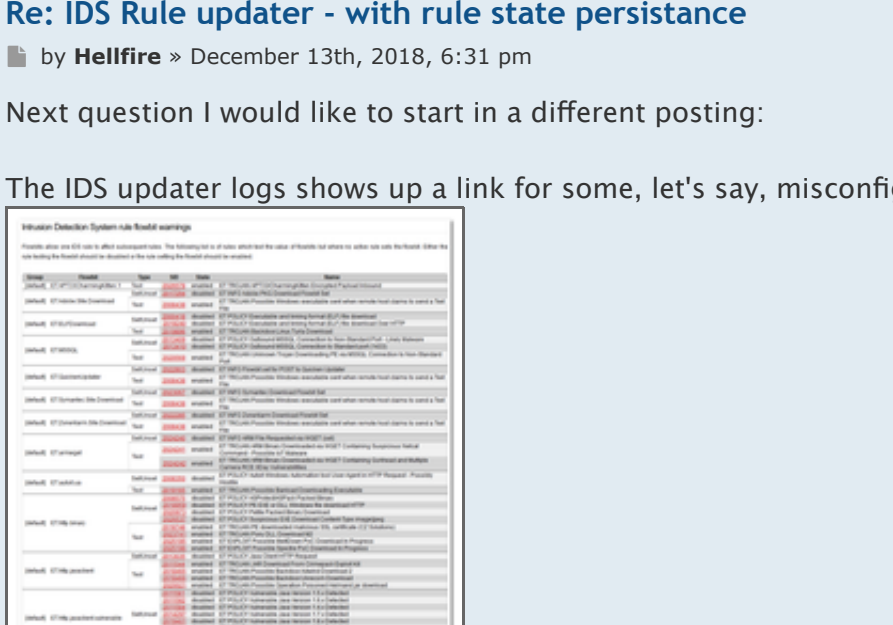
Here is the current log and my configuration:
Log:



Updater config:



IDS config:



So maybe I'm totally wrong regarding the purpose and functioning of IDS updater or sthg does not work properly on my side. I can see from the logs and statistics that some rule definitions have been downloaded, but I see no changes, at least not in the logs.

Because of the vast amount of rules I even cannot say for sure that any of those rules have been touched the last two days. Please don't bother, a question: if the updater decided that a rule must be activated according to the policy set and the appropriate options, I assume that this change hould be logged, right. May I further assume that any of those rules will get a (new) checkmark, too?

Thank you,
Michael

IPFire 2.25 - Core Update 153 on x86_64
AMD GX-412TC SOC @ 979MHz x2 - 4GB

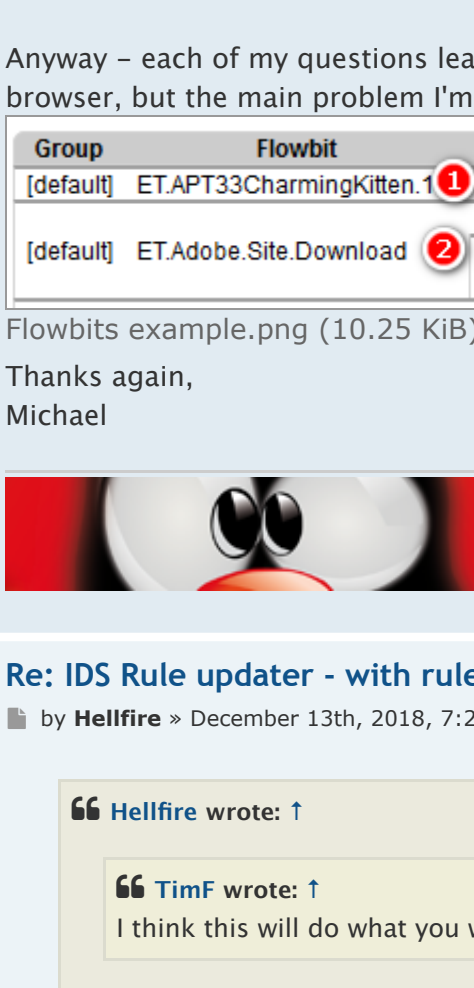
Re: IDS Rule updater - with rule state persistance

by **Hellfire** » December 13th, 2018, 6:31 pm

Hellfire
Posts: 697
Joined: November 8th, 2015, 8:54 am

Next question I would like to start in a different posting:

The IDS updater logs shows up a link for some, let's say, misconfigurated flowbits/rules sets, like:



So I tried to find which rule is the source of those issues. How would you start searching?

Let's take this example below. What does #1 exactly mean? Should I disable this rule because I've not set up any depending rules?

Let's head over to #2 There is a type **test** and **set/unset**: I assume that test was done by the updater and the action I've to take is to set or unset an appropriate sub-rule to get "[default]ET.Adobe.Site.Download" working, correct?

Anyway - each of my questions leads me to the main one: how do I find those rules in question? I've tried to perform a text search in browser, but the main problem I'm facing is, that I do not know which category the rule is in.

Group	Flowbit	Type	SID	State	Name
[default]	ET.APT33CharmingKitten.1 ①	Test	2026578	enabled	ET TROJAN APT33/CharmingKitten Encrypted Payload Inbound
[default]	ET.Adobe.Site.Download ②	Set/Unset	2017294	disabled	ET INFO Adobe PKG Download Flowbit Set
		Test	2008438	enabled	ET TROJAN Possible Windows executable sent when remote host claims to send a Text File

Flowbits example.png (10.25 KiB) Viewed 2997 times

Thanks again,
Michael

IPFire 2.25 - Core Update 153 on x86_64
AMD GX-412TC SOC @ 979MHz x2 - 4GB

Re: IDS Rule updater - with rule state persistance

by **Hellfire** » December 13th, 2018, 7:25 pm

Hellfire
Posts: 697
Joined: November 8th, 2015, 8:54 am

> Hellfire wrote: ↑ December 13th, 2018, 6:12 pm
>
> > TimF wrote: ↑ December 11th, 2018, 2:54 pm
> > I think this will do what you want, but I've not tried it out.
>
> Thank Tim, I will give it a try once my VM is up again...

Unfortunately this did not work.

I preserved two files from each rule set as suggested: emerging-exploit.rules and community.rules, deleted the other *.rules and wiped the content. Afterwards, I manually ran IDS updater and let it finish. At the end, both files are still empty and no further rule sets/categories have been loaded or created.
So I headed over to the IDS WebIf page and forced an update of community rules and emergingthreats.net - to no avail either. No futher files have been loaded. I then added Talos rule set for registered users and re-tried. Now some (new) files were fetched.

Once again I deleted the status file from the updater and manually ran ids-update.pl. After its finish I checked the rules files last moditication date and time and noticed that none of them have been touched in any way. No log was created either.

OK, last try: change the default policy from Security to Max-Detect and pressed save. The list box switched back to Connectivity, hence I could not finally test if changing to a new policy would force the IDS updater to modify any *.rules files.

Hence, I think the IDS Updater did not made any changes to the rules according to the default policy which is set to Security at the moment.

Michael

IPFire 2.25 - Core Update 153 on x86_64
AMD GX-412TC SOC @ 979MHz x2 - 4GB

Re: IDS Rule updater - with rule state persistance

by **TimF** » December 13th, 2018, 8:56 pm

TimF
Posts: 83
Joined: June 10th, 2017, 7:27 pm

it will only do an update when the rules have changed. It determines this by looking at the MD5SUM (this prevents it from downloading the large rulefiles unless necessary). You can force a change by modifying the appropriate lines in `/var/ipfire/idsupdate/status`. I usually just add a 'z' to the end of the appropriate lines since it's not a valid hex character.

IDS Rule updater - with rule state persistance

Re: IDS Rule updater - with rule state persistance

by **Hellfire** » December 14th, 2018, 3:10 pm

Hellfire
Posts: 697
Joined: November 8th, 2015, 8:54 am

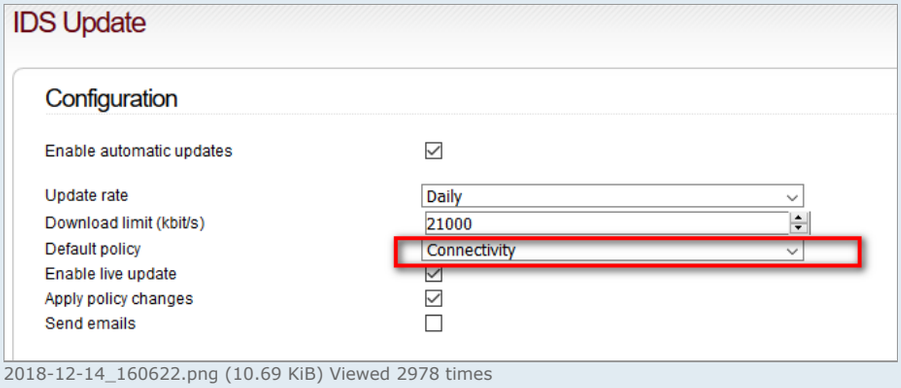
Tim,

I mentioned it briefly above: the settings file contains:

CODE: SELECT ALL

```
DEBUG=0
APPLY_POLICY_CHANGE=on
LIVE_UPDATE=on
EMAIL=off
DOWNLOAD_LIMIT=21000
ENABLE=on
RATE=DAILY
POLICY=MAX-DETECT
VERSION=3
```

And the WebIF shows:



2018-12-14_160622.png (10.69 KiB) Viewed 2978 times

Perhaps you could have a look and fix this?

This happens when switching to MAX-DETECT and press the save button. The WebIF always changes this back to CONNECTIVITY although the settings-files was update correctly. IMO there is a further issue with the download limit, too, since this value changes to zero after hitting the save button. A refresh of the web page brings back the value 21000 but not the correct policy.

Thanks,
Michael

Re: IDS Rule updater - with rule state persistance

by **Hellfire** » December 14th, 2018, 3:42 pm

Hellfire
Posts: 697
Joined: November 8th, 2015, 8:54 am

Maybe I'm too dumb to do some testing if the IDS updater works correctly, if all - at least on my side.

I've opened the rules file: **browser-ie.rules** and set all rules on comment by putting a #-char at the beginning of each line, e.g.

CODE: SELECT ALL

```
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"BROWSER-IE Microsoft Internet Explorer image download spoof
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"BROWSER-IE Microsoft Internet Explorer image download spoof
```

As a result the Intrusion Detection webpage lists all rules below the category **browser-ie.rules** as inactive.

I've then modified the status file of IDS updater like suggested and added a Z to each of those checksum lines and saved it again. Afterwards, I've fired this command

CODE: SELECT ALL

```
/usr/local/bin/ids-update.pl
```

and let the updater do its job. The policy is set to MAX-DETECT according to the settings file. The issues with the WebIF are posted above.

After the updater forced SNORT re-read its settings, I first had a look to the file modification date/time of the file browser-ie.rules - no changes made. Second, I checked the rules inside the file and in WebIF - no changes either.

I hope that the rule file I've used for those test does include at least one rule that the policy MAX-DETECT will detect and activate. If not how can I run some test to check if the updater does its job?

Michael

Re: IDS Rule updater - with rule state persistance

by **TimF** » December 16th, 2018, 8:48 pm

I'll set up a test to have a look at it.

TimF

Posts: 83
Joined: June 10th, 2017, 7:27 pm

Re: IDS Rule updater - with rule state persistance

by **Hellfire** » February 6th, 2019, 7:54 pm

Since weeks now, the updater does not log any changed rules now.

How can I uninstall the IDS updater. Unfortunately no instructions exists on github or within this forum posting.

Thx,
Michael

Hellfire

Posts: 697
Joined: November 8th, 2015, 8:54 am

Re: IDS Rule updater - with rule state persistance

by **TimF** » February 8th, 2019, 8:37 am

Unfortunately I've lost my normal internet access which makes responding difficult.

Have a look from the command line and see if there's a copy of ids-update.pl running - if there is kill it and hopefully the next update attempt will work. It appears that one of the downloads from the internet can lock up occasionally and not timeout. I've not been able to track down what is locking up.

To uninstall (from memory):

1. Use `fcrontab -e` and delete the lines for ids-update.pl (should be near the end).
2. Check ids-update.pl isn't running. Wait for it to finish if it is.
3. rm -R /var/ipfire/idsupdate
4. rm /var/ipfire/addon-lang/ids-update.*.pl
5. rm /usr/local/bin/ids-update.pl
6. rm /srv/web/ipfire/cgi-bin/idsflowbits.cgi
7. rm /srv/web/ipfire/cgi-bin/idsupdate.dat
8. rm /var/ipfire/menu.d/EX-idsupdate.menu
9. rm /usr/share/logwatch/scripts/services/ids-update
10. rm /usr/share/logwatch/dist.conf/services/ids-update.conf
11. rm /srv/web/ipfire/cgi-bin/idsupdate.cgi

I have written an uninstaller, but I can't upload it until I get my internet connection back.

TimF

Posts: 83
Joined: June 10th, 2017, 7:27 pm

Re: IDS Rule updater - with rule state persistance

by **Hellfire** » February 8th, 2019, 1:50 pm

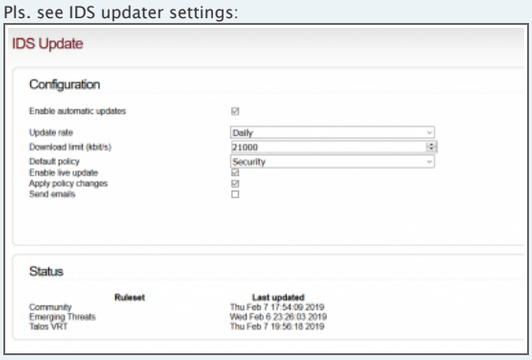
> **TimF wrote:** ↑ February 8th, 2019, 8:37 am
> Have a look from the command line and see if there's a copy of ids-update.pl running - if there is kill it and hopefully the next update attempt will work. It appears that one of the downloads from the internet can lock up occasionally and not timeout. I've not been able to track down what is locking up.

Unfortunately no process running like this. I don't think this is the source of the issue I'm seeing for weeks now when looking at the IDS updater logs, 'cause according to the update date time, there is an actual download taking place, however the updater did not update any of the IDS rules so far.

Hellfire

Posts: 697
Joined: November 8th, 2015, 8:54 am

Pls. see IDS updater settings:



Hence, I guess sthg. is wrong on my side, maybe missing some access right for important files?

Michael

IPFire 2.25 - Core Update 153 on x86_64
AMD GX-412TC SOC @ 979MHz x2 - 4GB

Re: IDS Rule updater - with rule state persistance

by **Hellfire** » February 8th, 2019, 2:46 pm

Hellfire
Posts: 697
Joined: November 8th, 2015, 8:54 am

FWIW, in case you did not see this posting: viewtopic.php?f=52&t=22266.

Michael

IPFire 2.25 - Core Update 153 on x86_64
AMD GX-412TC SOC @ 979MHz x2 - 4GB

Re: IDS Rule updater - with rule state persistance

by **TimF** » February 12th, 2019, 5:17 pm

TimF
Posts: 83
Joined: June 10th, 2017, 7:27 pm

You could try looking at the log file in /var/tmp.

Also check the permissions of the files in /etc/snort/rules – they should all be nobody.nobody (I think).

Finally the MANIFEST file on github gives the owner and permissions for all the updater files.

Re: IDS Rule updater - with rule state persistance

by **Hellfire** » February 15th, 2019, 8:14 pm

Hellfire
Posts: 697
Joined: November 8th, 2015, 8:54 am

All .rules files are set to owner nobody/nobody with exception of .config files those are set to root/root.
Guess this is OK.

OTH, /var/tmp/log shows:

> /usr/local/bin/oinkmaster.pl: Error: no write permission on "/etc/snort/rules/EMERGING_THREATS_classification.config"
> Write permission is required on all rules files inside the output directory.

But this seems to be caused by the above mentioned restricted permissions on .config files.

IPFire 2.25 - Core Update 153 on x86_64
AMD GX-412TC SOC @ 979MHz x2 - 4GB

Re: IDS Rule updater - with rule state persistance

by **Hellfire** » February 15th, 2019, 8:40 pm

Hellfire
Posts: 697
Joined: November 8th, 2015, 8:54 am

Some more feedback AND finally SUCCESS!

After setting permissions for those .config files to nobofy/nobody, to be precise for files

> TALOS_VRT_classification.config, EMERGING_THREATS_classification.config and COMMUNITY_classification.config

and firing a manual

CODE: SELECT ALL

```
./ids-update.pl
```

I now have some log enries telling me that some rules where deleted and others were updated. That's it!

This leaves one question open: why does the installer of IDS updater or whatever not set permissions as needed?

Michael

Edit: Tim, you should take notice of this posting, here viewtopic.php?f=52&t=22266, too as already mentioned above. Unless you do not fix ids-update-pl, the current Talos rules cannot be downloaded anymore.

IPFire 2.25 - Core Update 153 on x86_64
AMD GX-412TC SOC @ 979MHz x2 - 4GB

Re: IDS Rule updater - with rule state persistance

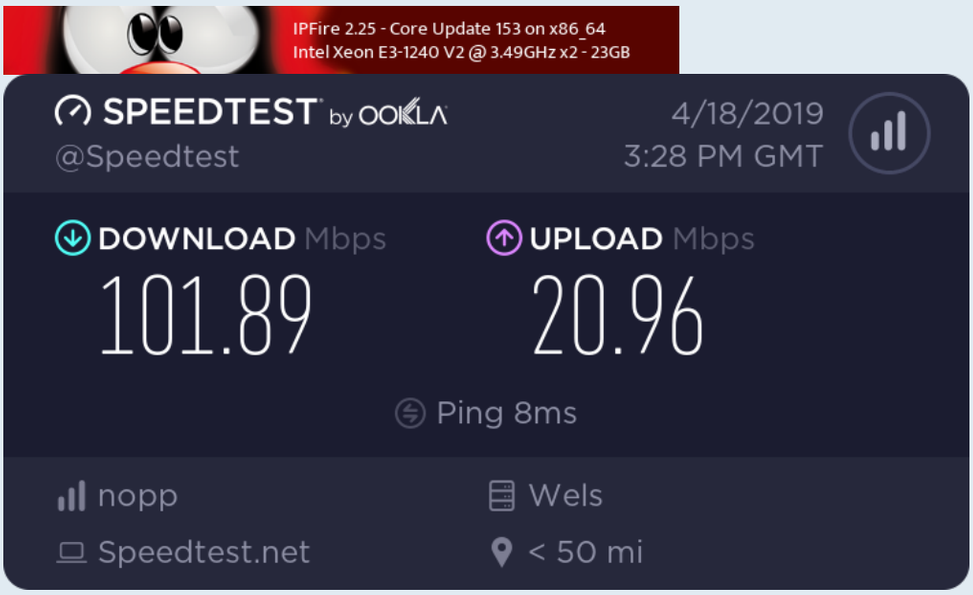
by **Stefan87** » April 25th, 2019, 1:15 am

Stefan87
Posts: 75
Joined: July 20th, 2017, 11:55 pm

> **TimF wrote:** ↑ February 8th, 2019, 8:37 am

I have written an uninstaller, but I can't upload it until I get my internet connection back.

the uninstaller would be great with the new suricata, the update tool is not needed



Re: IDS Rule updater - with rule state persistance

by **TimF** » April 27th, 2019, 2:49 pm

I've uploaded the uninstaller. You should be able to do:

CODE: SELECT ALL

```
wget https://github.com/timfprogs/ipfidsupdate/raw/master/uninstall-idsupdate.sh
chmod +x uninstall-idsupdate.sh
./uninstall-idsupdate.sh
```

TimF

Posts: 83
Joined: June 10th, 2017, 7:27 pm

Re: IDS Rule updater - with rule state persistance

by **Hellfire** » April 27th, 2019, 3:01 pm

Thanks Tim!

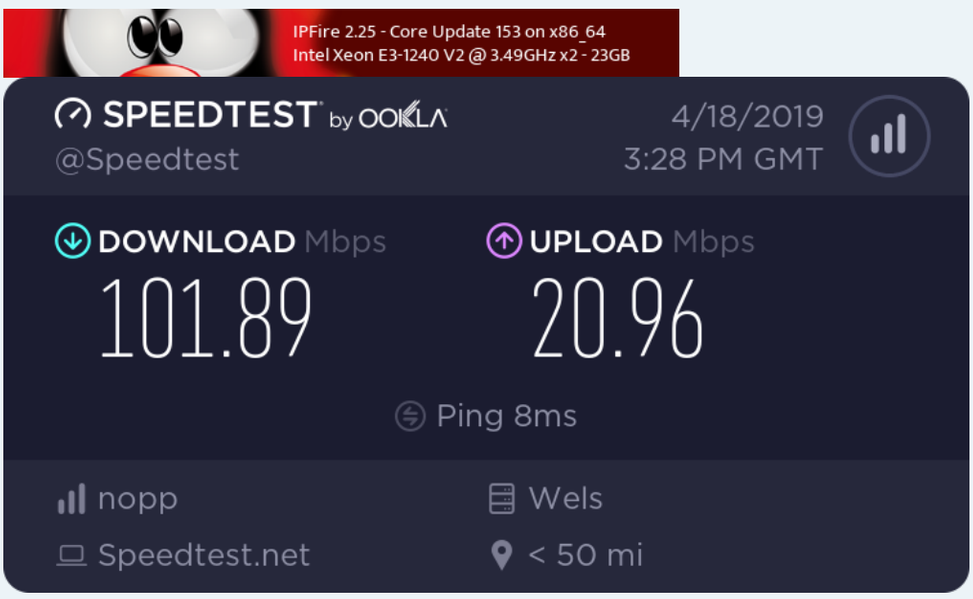
Hellfire

Posts: 697
Joined: November 8th, 2015, 8:54 am

Re: IDS Rule updater - with rule state persistance

by **Stefan87** » April 27th, 2019, 4:17 pm

Nice thanks



Stefan87

Posts: 75
Joined: July 20th, 2017, 11:55 pm

Powered by phpBB® Forum Software © phpBB Limited

Privacy | Terms