

IPset for IPFire

Locked

33 posts [1](#) [2](#) [3](#)

Re: IPset for IPFire

by ktsaou » January 7th, 2016, 5:53 pm

Great work!

Notes:

-r is needed in update-ipsets only if you want to rebuild the site data. Rebuild = you already have a few lists downloaded, and then you enable the site generation. If you configure WEB_DIR, etc from the beginning, there is no need to specify -r.

Regarding the netsets:

In kernels 2.6 each ipset can either contain IPs (iphash) or CIDRs (nethash - which do not accept /32 mask). In kernels 3.x and 4.x, the key differences is that hash:ip and hash:net ipsets can have more than 65536 entries and that hash:net ipsets can also include /32 entries.

So, in recent kernels a hash:net can include IPs. There is no need to grep them out. Actually, if you let update-ipsets load the netsets in the kernel, it will optimize them so that the number of different mask is minimum (netsets kernel performance is affected by the number of different masks, not the number of entries).

If you really need to split the netsets in IPs and CIDRs, update-ipsets can do it too. Just touch /etc/firehol/ipsets/NAME.split and update-ipsets will produce NAME_ip.ipset and NAME_net.netset.

Regarding the HISTOGRAM error, I cannot reproduce it. Does it happen on all ipsets or a specific one? Does it happen repeatedly (still happening), or it was just once?

By the way, did you see the generated site on your web server?

Costa

ktsaou
 Posts: 5
 Joined: November 8th, 2015, 9:25 am

Re: IPset for IPFire

by ummeegge » January 9th, 2016, 7:19 am

Thanks for your feedback Costa,

ummeegge wrote:
 -r is needed in update-ipsets only if you want to rebuild the site data. Rebuild = you already have a few lists downloaded, and then you enable the site generation. If you configure WEB_DIR, etc from the beginning, there is no need to specify -r.

an idea can be a result of this clarification ? If update-ipset enables at a first 'all', the descriptions of all lists can locally be readed to make some good decisions which lists are interesting ones to process them further ? Nevertheless i left '-r' out of the script and everybody needs to make there his own configuration and decisions and added instead '-s' to reduce the output in messages.

ummeegge wrote:
 In kernels 2.6 each ipset can either contain IPs (iphash) or CIDRs (nethash - which do not accept /32 mask). In kernels 3.x and 4.x, the key differences is that hash:ip and hash:net ipsets can have more than 65536 entries and that hash:net ipsets can also include /32 entries.

So, in recent kernels a hash:net can include IPs. There is no need to grep them out. Actually, if you let update-ipsets load the netsets in the kernel, it will optimize them so that the number of different mask is minimum (netsets kernel performance is affected by the number of different masks, not the number of entries).

IPFire uses a 3.14.x Kernel so this distro are in a good stand in here. May you know if the hash:net entries do need the /32 suffix to accept them ? Have experienced that the processing of the before mentioned mixed lists (IPs in netsets) delivers in total a smaller amount of entries as i greped them as *.ipset to IPs and *.netset to CIDRs only, thats why the script checks now both suffixes for each list.

This is a great function but I think update-ipset searches for existing sets which have similar names then the downloaded lists to be able to load them into the kernel, so in my opinion it was impractical for a generic usage in the script cause the firewall rules for each set needs then to be configured too (which makes currently also the script), to grep (sort) them in only two sets delivers a way to have let's say 50 lists without the need to generate 50 appropriate IPTable rules with may different 'src' or 'dst' options. I think somewhere in there is the point where Firehol comes in ?!

ummeegge wrote:
 If you really need to split the netsets in IPs and CIDRs, update-ipsets can do it too. Just touch /etc/firehol/ipsets/NAME.split and update-ipsets will produce NAME_ip.ipset and NAME_net.netset.

Good to know and an important information i think, will try this with my individual configuration.

ummeegge wrote:
 Regarding the HISTOGRAM error, I cannot reproduce it. Does it happen on all ipsets or a specific one? Does it happen repeatedly (still happening), or it was just once?

☺, i think this only happens at the first time...

ummeegge wrote:
 By the way, did you see the generated site on your web server?

Yes, good that you mention it, if someone is interested in a vhost configuration a first idea:

```

CODE: SELECT ALL
Listen 12345
<VirtualHost *:12345>
    SSLEngine on
    SSLProtocol all -SSLv2
    SSLCipherSuite ALL:!ADH:!EXPORT56:1eNULL:!SSLv2:!RC4+RSA:+HIGH:+MEDIUM
    SSLCertificateFile /etc/httpd/server.crt
    SSLCertificateKeyFile /etc/httpd/server.key

    DocumentRoot "/srv/web/firehol-ipset"
    Include /etc/httpd/conf/conf.d/php*.conf
    ErrorLog "/var/log/httpd/firehol-error.log"
    CustomLog "/var/log/httpd/firehol-access.log" combined
</VirtualHost>
    
```

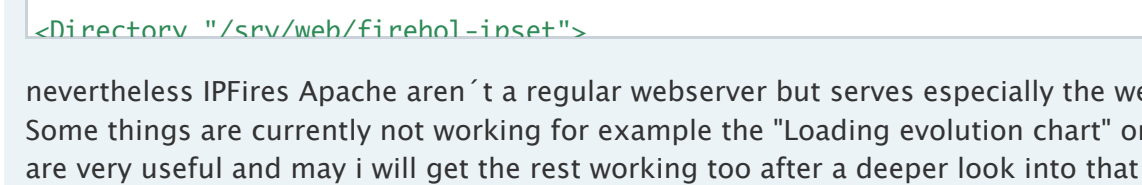
nevertheless IPFires Apache aren't a regular webserver but serves especially the webuserinterface to configure his tools and the FW. Some things are currently not working for example the "Loading evolution chart" or the "ipset data" are empty but the list descriptions are very useful and may i will get the rest working too after a deeper look into that matter.

As a first impression i like that tool it brings a lot of good and interesting functions with and i think if there is more time i will start to digging deeper into it. Thanks again Costa for this and for your support.

So far from here.

Greetings,

UE



Re: IPset for IPFire

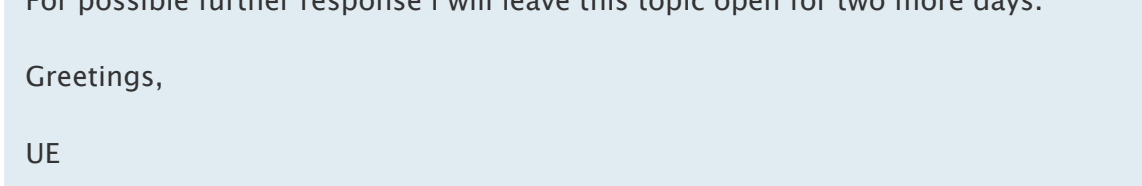
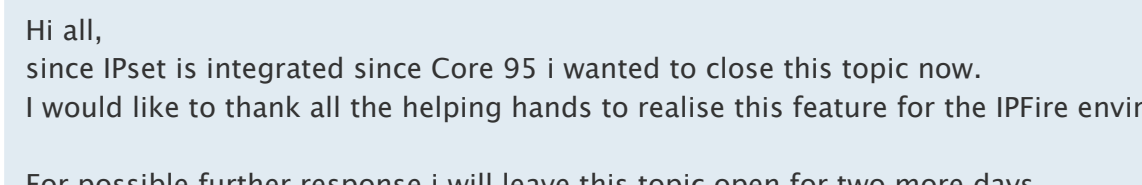
by ummeegge » June 2nd, 2016, 8:25 pm

Hi all, since IPset is integrated since Core 95 i wanted to close this topic now. I would like to thank all the helping hands to realise this feature for the IPFire environment... {Goood work ☺ }

For possible further response i will leave this topic open for two more days.

Greetings,

UE



Locked

33 posts [1](#) [2](#) [3](#)

< [Return to "Development"](#)