IPset for IPFire

IPset for IPFire

by **ummeegge** » October 23rd, 2015, 7:53 am

ummeegge
Community Developer
Posts: 5001
Joined: October 9th, 2010, 10:00 am

EDIT: IPset is meanwhile in IPFire Core 95 integrated so there is no need to install it manually like below described. This includes only the binary and installation directory the update script and the other integrations aren´t included in the Core update and currently only here available.

Hi all,
at the first i wanted to introduce a tool named IPset --> http://ipset.netfilter.org/ which is a companion application for IPTables. It allows you to setup rules to quickly and easily block a set of IP addresses, among other things.
And secondly what are you thinking about this feature for IPFire ?

An interessting Site in my opinion for this theme can be found in here --> http://iplists.firehol.org/ .

Greetings,

UE

Re: IPset for IPFire

by **jawz101** » October 26th, 2015, 7:04 pm

jawz101
Posts: 2
Joined: October 26th, 2015, 4:37 pm

Thanks. That FireHOL website is pretty damn awesome. It's nice to see someone has taken an analytical approach to the maintenance of all of these publicly available blocklists.

https://github.com/firehol

Re: IPset for IPFire

by **ummeegge** » October 27th, 2015, 9:58 am

ummeegge
Community Developer
Posts: 5001
Joined: October 9th, 2010, 10:00 am

Hi jawz101,

> **jawz101 wrote:**
> Thanks. That FireHOL website is pretty damn awesome.

i think so, very good sorted but also infos about list updates and some more goodies 🙂 .

But IPset is also a nifty tool. Have compiled it for IPFire now, wrote a little daily update script for it, included meanwhile 22 lists with currently 10062 IPs and 588 CIDRs and in puncto performance it makes a good impression for me. Also there would be no way to integrate this mass of IPs/CIDRs via IPTables directly without a subterraneously speed performance.
A nice site for performance test with and without IPset (and some more interessting infos) can also be found in here --> https://www.dbsysnet.com/2016/03/mass-b ... with-ipset .

UE

EDIT: Renewed link

Re: IPset for IPFire

by **Garp** » October 29th, 2015, 3:59 pm

Garp
Posts: 127
Joined: July 8th, 2014, 7:38 am
Location: The Netherlands
Contact:

Hi UE,

Can i help test it, in any way? I'm no application coder myself, so i cannot write this myself. May/Can i use your application?

Provide some additional protection for the clients on your network in a few easy steps: viewtopic.php?f=27&t=12122&p=78219#p78219

Re: IPset for IPFire

by **ummeegge** » October 29th, 2015, 5:38 pm

ummeegge
Community Developer
Posts: 5001
Joined: October 9th, 2010, 10:00 am

Hi Garp,

> **Garp wrote:**
> Can i help test it, in any way? I'm no application coder myself, so i cannot write this myself.

are you a little familar with the console/ssh ? If so, feel free to go for some testings. You can find IPset in here --> http://people.ipfire.org/~ummeegge/ipset/ <-- please check the sha256 sum.
Installation:
wget or what ever it to */opt/pakfire/tmp* unpack it with a

CODE: SELECT ALL
```
tar xvf ipset-6.26-1.ipfire
```

and install it with a

CODE: SELECT ALL
```
./install.sh
```

save the output so it is easier to uninstall it...
checkout if the appropriate kernel module is loaded

CODE: SELECT ALL
```
lsmod | grep ip_set
```

if there is something presant you are good to go, otherweise load it with a

CODE: SELECT ALL
```
modprobe ip_set
```

(above explanation do not include a reboot!!! <-- Please check the IPset man/homepage)
...

May it is a good idea that you go for a try on your own ways for the first 😳 ??, otherwise there are also some scripts out there which might accelerate further intends.
Have also one here.. still in testing mode 😉 .

Please use testing systems for this.

Greetings,

UE

Re: IPset for IPFire

by **Garp** » October 29th, 2015, 6:34 pm

Garp
Posts: 127
Joined: July 8th, 2014, 7:38 am
Location: The Netherlands
Contact:

Ok, thx.

I use IPFire as my home router. What would be the risk in using this addon in a home situation? Will it break anything?

Provide some additional protection for the clients on your network in a few easy steps: viewtopic.php?f=27&t=12122&p=78219#p78219

Re: IPset for IPFire

by **ummeegge** » October 29th, 2015, 6:43 pm

ummeegge
Community Developer
Posts: 5001
Joined: October 9th, 2010, 10:00 am

You are welcome,

> **Garp wrote:**
> What would be the risk in using this addon in a home situation? Will it break anything?

we are in development state , it could break anything anytimes.

greetings,

UE

Re: IPset for IPFire

by **ummeegge** » October 31st, 2015, 7:53 am

ummeegge
Community Developer
Posts: 5001
Joined: October 9th, 2010, 10:00 am

First idea for an daily update script:

Please use only testing systems for this.

- Don´t forget to make it executable with a

CODE: SELECT ALL
```
chmod +x ipset_updater.sh
```

- Debugger is still activated for testing
- After testing it can be placed under */etc/fcron.daily/* <-- 'set -x' can be deleted after testings.
- Blocks currently FORWARD, INPUT and OUTPUT (also IPFire itself) for all ports and protocols. Block works with REJECT not DROP. IPs/CIDRs will be rejected as source and destination.
- IPTable rules will be made automatically by the script. Rules are located under */etc/sysconfig/firewall.local* .
- Two sets will be created. One set is for IPs only and the other for CIDRs. A counter for bytes and packets are integrated too.
- Script contains currently 22 lists which have today 568 CIDRs and 11461 IPs.
- There is currently no IPset un- or installer but this should be no problem if needed.
- LAN, WAN, WLAN, DMZ, DNS1-2 and OpenVPN addresses will be automatically investigated and if presant in one of the list it will be deleted so yourself shouldn´t be locked out <-- got this problem with 192.168.0.0/16.
- restore command are placed under */etc/sysconfig/rc.local*, to reactivate IPset after a reboot.
- ip_set kernel module will be loaded if not already done.
- If byte and packets counter are not 0, the appropriate entries will be written to */etc/ipset/counterlist_ipset*, this works on two machines but on a third the counter do not work, don´t no why currently.
- All lists are located under /tmp/ipset which won´t be deleted in testing phase.
- Every update will be logged into syslog.
- **Attention**: If you use Tor cause a Tor blocklist is also integrated and it won´t work anymore if you use this list. Delete the " https://check.torproject.org/cgi-bin/To ... ip=1.1.1.1" line in the "## Blacklist addresses" section to prevent a Tor block.

CODE: SELECT ALL
```
#!/bin/bash -

set -x

#
# Update script example for blacklist update in IPset.
# Includes FW rule integration,  configuration entries, and restore command for system restart.
# ummeegge[at]ipfire.org $date 01.01.2016
##################################################################
#

## Locations
CONFDIR="/etc/ipset";
CONF="${CONFDIR}/ipset.conf";
```

Feedback and testings might be nice.

Greetings,

UE

EDIT(s):
- Fixed bug for list directory creation.
- Fixed echo command for timestamp in 'counterlist_ipset ' <-- byte and packet counter do not work on every machine, haven´t find the problem until now.
- Deleted honeypot lists cause they are currently off.
- Deleted 'firehol_level1.netset' cause content it is already in other lists but also of its mixture of IPs and CIDRs.
- Fixed rc.local command.
21.11.15
- Fixed initial set creation.
- Set appropriate src and dst for FW rule chains.
- Added 'No entries today' in counter_list if no blacklistet addresses where recognized by byte and packet counter.
07.12.15
- Changed wget command. Reduced connections retries to 3, added timeout to 10 sec. to prevent long time loops if an URL isn´t reachable. Added time stamping for dwnload.log. Prints now "HTTP request" to dwnload.log. Prints now also "Content-Security-Policy" to dwnload.log.
01.01.2015
- Deleted Github addresses from Firehol regarding Costas hint, provide instead update-ipsets from Firehol project --> https://forum.ipfire.org/viewtopic.php? ... =15#p93409 which serves all Firehol lists.
- Changed some smaller things in the script (syntax).
02.12.2016
- Added firewall.local reload in rc.local.

Re: IPset for IPFire

by **Garp** » October 31st, 2015, 9:05 am

Garp
Posts: 127
Joined: July 8th, 2014, 7:38 am
Location: The Netherlands
Contact:

I will test when i find the time to make a full backup of my SD card that i run IPFire on.

When going through your script, i notice that you use a lot of sources. I was under the impression that the FireHole source should be 'suffient' as a source because then do the combining.

What is the reason that you added the other sources?

Provide some additional protection for the clients on your network in a few easy steps: viewtopic.php?f=27&t=12122&p=78219#p78219

Re: IPset for IPFire

by **ummeegge** » October 31st, 2015, 9:49 am

ummeegge
Community Developer
Posts: 5001
Joined: October 9th, 2010, 10:00 am

Goedemiddag Garp,

> **Garp wrote:**
> When going through your script, i notice that you use a lot of sources. I was under the impression that the FireHole source should be 'suffient' as a source because then do the combining.
>
> What is the reason that you added the other sources?

different types of reaserches (u.a. honeypots) delivers different results, so in my opinion a better variation. A lot of IPs occurs double in this lists but the script sorts them out and makes them uniqe <-- IPset makes this job too but better to make this before.
The Firehol lists are very good but lists like e.g. this --> https://raw.githubusercontent.com/ktsao ... el1.netset brought some problems. In CIDR section was something i couldn´t work out until now which blocks browser traffic so i left the CIDRs out from this list.

Also everybody needs to check his own setup for his usage, for example i do not need the whole Spamhouse section in my environment so i left it out. Even the lists of the script are hold nearly general, please investigate the lists for your own purposes and add or delete what you need or you don´t need. The script is an example...

The grep commands to separate CIDRs and IPs from the rest should work in general, so you should be able to use it for your own lists too.

> **Garp wrote:**
> I will test when i find the time to make a full backup of my SD card that i run IPFire on.

All right.

UE

Re: IPset for IPFire

by **ummeegge** » November 7th, 2015, 5:42 am

ummeegge
Community Developer
Posts: 5001
Joined: October 9th, 2010, 10:00 am

Hi all,
have fixed somethings on the script --> https://forum.ipfire.org/viewtopic.php? ... 514#p91514 <-- which can be overviewed at the bottom in the 'EDIT(s)' section.

Also if someone is interessted in howto build IPset, take a look in here --> http://git.ipfire.org/?p=ipfire-2.x.git ... 9168399b10 .
Also IPFire will deliver IPset with Core 95, a wiki comes in the next view days, will announce it here if it is ready.

Greetings,

UE

Re: IPset for IPFire

by **Garp** » November 7th, 2015, 10:08 am

Garp
Posts: 127
Joined: July 8th, 2014, 7:38 am
Location: The Netherlands
Contact:

Great news, thx!

Provide some additional protection for the clients on your network in a few easy steps: viewtopic.php?f=27&t=12122&p=78219#p78219

Re: IPset for IPFire

by **ktsaou** » November 8th, 2015, 9:34 am

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

Hi all,

sorry for intervening, I just got a notification from mention.net you are referring to iplists.firehol.org.

I strongly suggest not to use files downloaded from the github repo, in production systems. They might not be updated regularly.

I have added a wiki where I explain the right way of updating all these IP lists. Check it here:
https://github.com/firehol/blocklist-ipsets/wiki

I don't know if you can use my method with ipfire, but anyway, I thought I should at least let you know.

Thanks!

Re: IPset for IPFire

by **ummeegge** » November 9th, 2015, 5:08 pm

ummeegge
Community Developer
Posts: 5001
Joined: October 9th, 2010, 10:00 am

Hi ktsaou and thanks for your intervention and your feedback which is very nice.
IPset will be delivered in IPFires next Core update but without Firehol which i think is a requirement for the usage of the 'update-ipsets' command, nevertheless i have build it for IPFire too and will go in media res with it.

> **ktsaou wrote:**
> I strongly suggest not to use files downloaded from the github repo, in production systems. They might not be updated regularly.

I´am not hundred procents clear of it but does for example an 'update-ipsets enable dshield' do not deliver the data from here --> https://github.com/firehol/blocklist-ip ... eld.netset ? In that case all the actual lists are probably located in here --> https://github.com/firehol/blocklist-ipsets/ ? May if i´am wrong please correct me.

The script above should do similar things but at this time not so comfortable like Firehol it does, may it will becomes better as time goes by or even may Firehol belongs sometimes also in to the distribution, will see.

So let me say a big thanks to your work in the firehol.org platform which is very usful but also your prompt support in this topic.

Greetings and keep up the good work 🙂 ,

UE

Re: IPset for IPFire

by **ummeegge** » November 11th, 2015, 8:42 am

ummeegge
Community Developer
Posts: 5001
Joined: October 9th, 2010, 10:00 am

Have made now the IPset wiki which can be found in here --> https://wiki.ipfire.org/en/configuration/firewall/ipset .
It might be great if you can go for correction readings. If you think there is something missing or not wright let it me know.

Greetings,

UE

IPset for IPFire

Re: IPset for IPFire

by **ktsaou** » November 11th, 2015, 7:37 pm

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

Hi again,

Sorry for the marketing material below :-)

update-ipsets is a tool to download and install IP lists directly from their sources. From their maintainers' sites. Actually update-ipsets is a large script capable of applying a policy to the download procedure with a lot of logic to convert the IP lists from their original format published, to a unified one.

update-ipsets, when run as root, can also apply the ipsets in kernel (for any iptables based firewall). It does this atomically (check this: https://github.com/firehol/blocklist-ip ... -in-kernel). There is no way for something to fail and stay with a non-operational ipset in kernel.

update-ipsets, will also maintain a site for you, exactly the same with iplists.firehol.org with your IP lists. So you can enable a few IP lists, run update-ipsets with cron, and have a site exactly the same to iplists.firehol.org with YOUR lists, your data, everything calculated based on your view of the world. Check this: https://github.com/firehol/blocklist-ip ... ate-ipsets

update-ipsets requires iprange is a C program, also supplied with FireHOL. iprange is a very fast ipset processor. It can also optimize hash:net ipsets for optimal kernel performance (minimum latency and minimum CPU usage - check this: https://github.com/firehol/firehol/wiki ... r-iptables).

update-ipsets and iprange are distributed with FireHOL, but will work with any iprables based firewall. They are GPL, so you are free to use them directly with ipfire.

Again, sorry for marketing my tools...

Costa

Re: IPset for IPFire

by **ummeegge** » November 13th, 2015, 4:48 pm

ummeegge Community Developer Posts: 5001 Joined: October 9th, 2010, 10:00 am

Hi Costa,
i think marketing isn´t per definition a bad thing, especially if the product which you are promote are a good/useful one (which it is in my opinion) but answer some before quested things is also not that bad 😉 , so if you may take also the time for this it might be a gain in experience for the usage of your work too?! Let´s see...

Also i do not think that Firehol and or iprange will belong to IPFire in the next time so there is the need for the first to handle with some good lists (may yours) where your qualified advice might be interessting and own/other scripts which could do the job as far/good as they can.

Greetings,

UE

IPFire - An open source firewall solution
IPFire - An open source firewall solution

Re: IPset for IPFire

by **SamSpade** » November 17th, 2015, 1:50 pm

SamSpade Posts: 26 Joined: April 22nd, 2011, 1:37 pm

How does ipset interfere with the geoip filter? Or is the geoip filter already based on ipset?

Re: IPset for IPFire

by **ktsaou** » November 17th, 2015, 6:51 pm

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

ok. Thanks!

iprange has now its own repo (https://github.com/firehol/iprange). This was required to maintain the noarch packaging of FireHOL. So, you can install just this, if you need the hash:net ipset optimizations it provides.

iprange has also an asynchronous, parallel queries, DNS resolver in it, so it can quickly translate a list of hostnames to an ipset.

Regards!

Costa

Re: IPset for IPFire

by **ummeegge** » November 18th, 2015, 1:50 pm

ummeegge Community Developer Posts: 5001 Joined: October 9th, 2010, 10:00 am

Hi Costa,
great will make then two IPFire packages for Firehol and iprange from your sources in the next time for further improvements. Thanks for that...

Greetings,

UE

IPFire - An open source firewall solution
IPFire - An open source firewall solution

Re: IPset for IPFire

by **ummeegge** » November 22nd, 2015, 10:26 am

ummeegge Community Developer Posts: 5001 Joined: October 9th, 2010, 10:00 am

Hi all,
have build now iprange --> https://github.com/firehol/iprange and Firehol --> https://github.com/firehol/firehol for IPFire --> http://people.ipfire.org/~ummeegge/ipset/ . If someone is interessted to go for some testings, wget or what ever it to */opt/pakfire/tmp*, check the sha256 sums, unpack it with an 'tar xvf {packagename}' and install it with an './install.sh' <-- it´s may a good idea to save the file list from STDOUT so it is easier to uninstall it but also to find the appropriate files since there is currently no un- installer available for that. You can set the console free again by typing [CTRL-c].

Have fixed/changed also some things in the ipset_updater.sh --> https://forum.ipfire.org/viewtopic.php? ... 124#p91514 which can be overviewed at the end of this post (checkout the EDIT(s)).

@Costa
have added also your firehol.org project in the wiki --> https://wiki.ipfire.org/en/configuration/firewall/ipset .

Since IPSet will be delivered with IPFires Core 95 --> http://git.ipfire.org/?p=ipfire-2.x.git ... ads/core95 , the testing phase will belong also to an ending state. If someone got more testing results or ideas of how to extend the mentioned things in here, it might be now a good time to announce new ideas and testing results/bugs and so on.

Greetings,

UE

IPFire - An open source firewall solution
IPFire - An open source firewall solution

Re: IPset for IPFire

by **mr.nice.** » December 12th, 2015, 10:42 am

mr.nice. Posts: 14 Joined: June 23rd, 2014, 9:49 am

Hello ummeegge, thank you for providing such a great ipset script!

I have updated my ipfire to 95 and put the ipset_updater.sh script to the fcron.daily folder, like you suggested. I did the chmod -x and ran the script, it went trough without any errors.

Now I have got a huge ipset.conf in /etc/ipset/ and it looks like it's working just fine.

One question, I have made a custom Win10 drop-list containing 106 destination IP-Addresses and I would like to integrate this list into your script. What be the best way to do this?

If you want I, I can post this list here.

Re: IPset for IPFire

by **ummeegge** » December 12th, 2015, 3:21 pm

ummeegge Community Developer Posts: 5001 Joined: October 9th, 2010, 10:00 am

Hi mr.nice. ,
and thanks for your feedback.

> **mr.nice. wrote:**
> One question, I have made a custom Win10 drop-list containing 106 destination IP-Addresses and I would like to integrate this list into your script. What be the best way to do this?

This should be no problem but it depense a little on what kind of list you have. If you found a good list in the web (CIDR or IP format is possible) which may are also regularily updated we could may integerate it in the ipset_updater in case you got a static local list it might be a better idea to define an appropriate new set and feed it one time with your content, it should be then also only a simple oneliner to integrate also a vast list of IP´s or CIDR´s.
But anyway, you can post me a link if the list(s) are WAN wide reachable or post them here if you have them wright on hand, will take then a look on it.

Greetings,

UE

P.S.

> **mr.nice. wrote:**
> I did the chmod -x and ran the script, it went trough without any errors.

A

CODE: SELECT ALL
```
chmod +x
```

should be better 😉

IPFire - An open source firewall solution
IPFire - An open source firewall solution

Re: IPset for IPFire

by **mr.nice.** » December 12th, 2015, 7:15 pm

mr.nice. Posts: 14 Joined: June 23rd, 2014, 9:49 am

Hello ummeegge you are right, my Linux-Fu is still weak but growing 😉
Currently the WIN10 IP blacklist is a static list and therefore I have put it into /etc/ipset.
I have created it on my own, based on the hosts file from this site https://blockwindows.wordpress.com/

I have modified your script a little and will provide the WIN10 list.
If it is okay for you, I would like to publish it in the ipfire thread on overclockers.at too.

CODE: SELECT ALL
```
#
# Update script for blacklist update in IPset
# ummeegge[at]ipfire.org $date 07.11.2015, modified by mr.nice. on 12.12.2015, WIN10 blacklist added
##############################################################
#

## Locations
CONFDIR="/etc/ipset";
CONF="${CONFDIR}/ipset.conf";
COUNTER="${CONFDIR}/counterlist_ipset";
IPSET="/usr/sbin/ipset";
DIR="/tmp/ipset";
DWNLOG="/tmp/ipset/dwnload.log";
CIDRLIST="${DIR}/CIDRLIST";
```

CODE: SELECT ALL
```
23.37.40.70
23.37.43.27
23.99.10.11
23.102.21.4
23.103.189.125
23.218.212.69
31.13.64.2
37.252.162.31
37.252.170.158
40.127.139.224
64.4.11.42
64.4.54.22
64.4.54.32
64.4.54.167
```

Re: IPset for IPFire

by **ummeegge** » December 14th, 2015, 6:48 am

ummeegge Community Developer Posts: 5001 Joined: October 9th, 2010, 10:00 am

Hi mr.nice.,

> **mr.nice. wrote:**
> Currently the WIN10 IP blacklist is a static list and therefore I have put it into /etc/ipset.

you can think about to handle it then seperated to the update script, as a fast howto:
Let´s say we call the new set 'telemetry' (won´t call it windoof 😉)
1) Create a new set for hash based storage of IPs with a bytes and packets counter:

CODE: SELECT ALL
```
ipset create telemetry hash:ip counters
```

checkout the sets:

CODE: SELECT ALL
```
ipset -n list
```

2) Now include your list to IPset, you can copy/paste it to a file in e.g. /tmp called telemetry.txt and read it out via a for loop:

CODE: SELECT ALL
```
for l in $(cat /tmp/telemetry.txt); do ipset --add telemetry ${l}; done
```

Check out the new content:

CODE: SELECT ALL
```
ipset -t list
ipset list telemetry
```

3) Save your new set:

CODE: SELECT ALL
```
ipset save > /etc/ipset/ipset.conf
```

4) If the updater script is already presant you do not need to set the restore command in */etc/sysconfig/rc.local* otherwise add there the following entry:

CODE: SELECT ALL
```
/usr/sbin/ipset restore < /etc/ipset/ipset.conf;
```

so after every FW restart your configuration should be persistent (no need for an initscript).
5) Add the new set to IPTables. Since the WUI currently do not offer a set configuration, */etc/sysconfig/firewall.local* is a good place to go for that.
start section:

CODE: SELECT ALL
```
        /sbin/iptables -I CUSTOMFORWARD -m set --match-set telemetry dst -j REJECT
        /sbin/iptables -I CUSTOMINPUT -m set --match-set telemetry src -j REJECT
        /sbin/iptables -I CUSTOMOUTPUT -m set --match-set telemetry dst -j REJECT
```

stop section:

CODE: SELECT ALL
```
    # IPSET flushing related chains
    /sbin/iptables -F CUSTOMFORWARD
    /sbin/iptables -F CUSTOMINPUT
    /sbin/iptables -F CUSTOMOUTPUT
```

FORWARD blocks all traffic to IPsets IPs, INPUT blocks all traffic from those IPs, OUTPUT blocks also IPFire to reach the IPs.
You can also set a IPTables variable but do not use ${IPSET} cause it is used by the updater script and it would delete the new entries while an update. Since you integrated the telemetry IPs into the script it´s doesn´t matter but if you seperate it remember this.
6) Reload the FW so that the changes takes affect:

CODE: SELECT ALL
```
/etc/sysconfig/firewall.local reload
```

> **mr.nice. wrote:**
> I have created it on my own, based on the hosts file from this site https://blockwindows.wordpress.com/

You converted the host addresses then to IPs which is important since IPTables have some DNS resolution problems with this and i think IPset won´t use hostnames anyway.
As short one, if you want to convert lists like this --> https://github.com/WindowsLies/BlockWin ... /hostslist , you can try to reslove them over a host command query like e.g. this one

CODE: SELECT ALL
```
for l in $(cat /tmp/telemetry_host_list); do host -t a ${l} | grep -E -o "([0-9]{1,3}[\.]){3}[0-9]{1,3}" >> /tmp/teleme
```

this command needs the hostname list under */tmp/telemetry_host_list* and after processing it stores a new list *telemtry_IPs* under /tmp which you can also use over IPset (example can be found in here --> viewtopic.php?t=14909#p90603 sadly in german but this should be no problem for you i think ;-).
As a beside info, there is another update script for Squids URL-Filter which onyl operates with hostnames but can also only be used for HTTP and HTTPS which you can find in here --> viewtopic.php?f=27&t=14895 .

> **mr.nice. wrote:**
> I have modified your script a little and will provide the WIN10 list.
> If it is okay for you, I would like to publish it in the ipfire thread on overclockers.at too.

No problem, if you are good to go with this, use it, extend it, share it, develop it, have fun 😉 .

There is another interessting thing for IPset --> http://git.zx2c4.com/ipset-dns/about/ which might be worth for a look over ?! Let´s see...

Greetings,

UE

IPFire - An open source firewall solution
IPFire - An open source firewall solution

Re: IPset for IPFire

by **dnl** » December 22nd, 2015, 9:14 am

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

Hello ktsaou,
Thanks for all your hard work and for taking the time to register and write to us here!
I look forward to using your lists from now on!

A question: I see that some of your sources are updated as quickly as every 5 minutes(!). Do you think it would cause you a problem with Github if we pulled updates hourly?

I guess the issue is probably more likely to come with the other lists Ummegge has included. (Hmm: I might drop them in the short-term)

Hey Ummegge,
Great work again! Thanks very much for the handy shell script and for all your work in testing and developing this! It's exactly what I've been wanting to do.

I've been able to remove the emerging-botcc, emerging-ciarmy and emerging-dshield rule sets from my IDS!

I've only quickly read this forum thread but is there a performance benefit we could get in future from using firehol rather than your shell script?

Also, I updated the "Installation" section of the IPSet wiki page you created. However now that I think about it, we should probably remove the "Installation" section, because IPSet is now included in the stable release of IPFire. What do you think?

Re: IPset for IPFire

by **ummeegge** » December 27th, 2015, 10:42 am

ummeegge Community Developer Posts: 5001 Joined: October 9th, 2010, 10:00 am

Hi dnl,

> **dnl wrote:**
> **Hey Ummegge,**
> Great work again! Thanks very much for the handy shell script and for all your work in testing and developing this! It's exactly what I've been wanting to do.
>
> I've been able to remove the emerging-botcc, emerging-ciarmy and emerging-dshield rule sets from my IDS!

thanks for you feedback.

> **dnl wrote:**
> I've only quickly read this forum thread but is there a performance benefit we could get in future from using firehol rather than your shell script?

EDIT: Need to check update-ipsets on my own so i´currently not sure about this.
I haven´t test Firehol until now nor have had a deeper look into all the functions or how it works with IPFire environment but a IPFire package for Firehol is available and testing people are invited to do so.

May Costa have also some additional informations for this but also to your before asked questions, will see.

> **dnl wrote:**
> Also, I updated the "Installation" section of the IPSet wiki page you created. However now that I think about it, we should probably remove the "Installation" section, because IPSet is now included in the stable release of IPFire. What do you think?

Thanks for that. I´am currently not sure which part you mean in installation section, 'how it works' is still important to know, the lsmod and modprobe stuff might also be good to mention cause i´m not sure that every machine response with an activated ip_set kernel modul (e.g. i needed to activate it on one machine manually).
Also may a short explanaition why IPSet is more effecient (bitmap <--> hash structure) should also takes place in the wiki i think ?! Not too much about that but a short explanation in the wiki is not that bad in my opinion.

As a beside info: A blacklist solution for IPSet and Ossec is also available --> https://github.com/kravietz/blacklist-scripts --> https://github.com/kravietz/blacklist-s ... et-drop.sh --> http://www.mbse.eu/linux/homeserver/mgm ... ver-ossec/ . But since Ossec is currently not official available this should only be seen as a beside info.

Greetings,

UE

EDIT: Changed some statements after Costa´s clarification.

IPFire - An open source firewall solution
IPFire - An open source firewall solution

Re: IPset for IPFire

by **ktsaou** » December 27th, 2015, 4:11 pm

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

Hi all,

FireHOL does NOT download IP lists from github.

I strongly suggest not to use IP lists from github. The IP lists are uploaded to github only for transparency and tracking. They are uploaded from my home router, which is not a reliable solution.

The program that downloads IP lists directly from their sources, unifies them and uploads them to github, is open source. It is called update-ipsets and is available in the FireHOL distribution.

update-ipsets will update the ipsets in kernel, for any firewalling solution. So, it will download a list, process it, and if an ipset with the same name exists in kernel, it will update the kernel too. I have done the most this process to be atomic (meaning that it will either succeed and a new list will be loaded into the kernel, or fail and the old list will be left untouched in the kernel and generic enough to be used with any iptables firewall manager).

update-ipsets will optimize IP lists for optimal kernel performance. Check this: https://github.com/firehol/firehol/wiki ... r-iptables

update-ipsets can also provide you with a site exactly the same with iplists.firehol.org. Your view of the world, available on your web server.

There is a wiki to help you setup and use update-ipsets: https://github.com/firehol/blocklist-ipsets/wiki

Merry Christmas!

Costa

Re: IPset for IPFire

by **ummeegge** » December 31st, 2015, 2:56 pm

ummeegge Community Developer Posts: 5001 Joined: October 9th, 2010, 10:00 am

Thanks for clarifying Costa,
have build now a reduced version of the Firehol package with a

CODE: SELECT ALL
```
        cd $(DIR_APP) && ./autogen.sh
        cd $(DIR_APP) && ./configure \
              --prefix=/usr \
              --disable-doc \
              --disable-man \
              --disable-firehol \
              --disable-fireqos \
              --disable-ipv6
```

which includes now also update-ipsets. If someone is interessted to test it, take a look in my public --> http://people.ipfire.org/~ummeegge/ipset/ .

Wish you all a happy and a good new year.

Greetings,

UE

IPFire - An open source firewall solution
IPFire - An open source firewall solution

Re: IPset for IPFire

by **ummeegge** » January 7th, 2016, 10:19 am

ummeegge Community Developer Posts: 5001 Joined: October 9th, 2010, 10:00 am

Hi all,
to step in the next round, i tried now to mix this two different approaches in this thread by integrating also Costas update-ipsets.sh .
Since i build it for IPFire --> http://people.ipfire.org/~ummeegge/ipset/ (update-ipsets only and iprange from master) but they aren´t available via Pakfire, a fast how to integrate it.
Navigate to */opt/pakfire/tmp* , download the packages, check the SHA256 sums, unpack them with a

CODE: SELECT ALL
```
tar xvf {packagename}
```

and install it with a

CODE: SELECT ALL
```
./install.sh
```

the console can be set free again with a [CTRL-c] btw. [STRG-c]. update-ipsets files can be found under

CODE: SELECT ALL
```
/usr/lib/firehol/functions.common.sh
/usr/etc/firehol
/usr/sbin/update-ipsets
```

iprange under

CODE: SELECT ALL
```
/usr/bin/iprange
```

Since Firehols tools are well documented, i used this side --> https://github.com/firehol/blocklist-ip ... ate-ipsets to enable update-ipsets. In IPFire terms it looks like this.
Add update-ipsets configuration:

CODE: SELECT ALL
```
# create /usr/etc/firehol/update-ipsets.conf
cat >>/usr/etc/firehol/update-ipsets.conf <<EOF
WEB_DIR="/srv/web/firehol/iplists"
WEB_OWNER="nobody:nobody"
EOF
```

Create web directory for downloaded lists:

CODE: SELECT ALL
```
# create the web directory
mkdir -pv /srv/web/firehol/iplists
```

download index and typeahead:

CODE: SELECT ALL
```
# get the index.html page
curl -o /srv/web/firehol/iplists/index.html 'http://iplists.firehol.org/index.html'
# get typeahead.css
curl -o /srv/web/firehol/iplists/typeahead.css 'http://iplists.firehol.org/typeahead.css'
```

Set permissions:

CODE: SELECT ALL
```
chown -R nobody:nobody /srv/web/firehol/
```

Now checkout which lists you want to get from Firehol. For a look through i find this side --> https://github.com/firehol/blocklist-ipsets very useful.

Lets say we use some Microsoft, Snort, EmergingThreads and some Zeus lists. To enable them use

CODE: SELECT ALL
```
update-ipsets enable iblocklist_org_microsoft snort_ipfilter et_dshield et_block zeus_badipsm zeus
```

there are a lot more but for this explanation this should be o.k. .
To activate the new configuration there is the need to use one time a

CODE: SELECT ALL
```
update-ipsets -r
```

which delivers the following content:

CODE: SELECT ALL
```
-> ls -la /srv/web/firehol/iplists/ /usr/etc/firehol/ipsets/
/srv/web/firehol/iplists/:
total 204
drwxr-xr-x 2 nobody nobody  4096 Jan  7 10:39 .
drwxr-xr-x 3 nobody nobody  4096 Jan  7 10:38 ..
-rw-r--r-- 1 nobody nobody  1139 Jan  7 10:39 all-ipsets.json
-rw-r--r-- 1 nobody nobody    71 Jan  7 10:39 et_block_changesets.csv
-rw-r--r-- 1 nobody nobody   371 Jan  7 10:39 et_block_comparison.json
-rw-r--r-- 1 nobody nobody   102 Jan  7 10:39 et_block_history.csv
-rw-r--r-- 1 nobody nobody  1497 Jan  7 10:39 et_block.json
-rw-r--r-- 1 nobody nobody   294 Jan  7 10:39 et_block_retention.json
-rw-r--r-- 1 nobody nobody    71 Jan  7 10:39 et_dshield_changesets.csv
-rw-r--r-- 1 nobody nobody   183 Jan  7 10:39 et_dshield_comparison.json
-rw-r--r-- 1 nobody nobody    84 Jan  7 10:39 et_dshield_history.csv
```

after this you can use update-ipsets without '-r' option.

I do not went throught the whole possibilities which update-ipsets delivers but it should be possible to add appropriate sets named like the lists to get specific updated sets (i know update-ipsets can makes there a delicater job ;-).

Let´s stay in the mix 😉 :
I used now the so called woodhammer method by adding only two sets for IP´s and CIDR´s which will be extracted from the Firehol lists with the old but modified script from this thread.

CODE: SELECT ALL
```
#!/bin/bash -

#set -x

#
# Update script for blacklist update in IPset
# Uses same mechanism as ipset_updater but uses now update-ipset´s from firehol project
# ummeegge[at]ipfire.org $date: 01.01.2015
####################################################################################
#

## Locations
CONFDIR="/etc/ipset";
CONF="${CONFDIR}/ipset.conf";
```

the script executes update-ipsets and will integrate all before configured lists but also
- add as before the firewall rules for this two sets,
- add an IPset configuration reload after a system reboot,
- invests internal used addresses which will be stripped out of all lists,
- will activates ip_set kernel modul if not already done,
- adds an bytes and packets counter list under */etc/ipset* if some blacklisted IPs/CIDRs has been matched it will be written to it,
- all extracted lists are findable as a summary under */tmp/update-ipsets* including a update.log,
- have used UIPSET instead of IPSET as variable name in firewall.local so existing scripts should not be affected.
@Costa
have recognized that some *.netset lists are mixed and contains also IPs, a short look over has figured the following lists out

> darklist_de, et_block, ipblocklist_abuse_speye, ipblocklist_abuse_zeus, ipblocklist_malc0de, ipblocklist_org_microsoft, ipblocklist_pedophiles, ipblocklist_spyware

That´s why the script greps currently *.ipset but also *.netset files for both sets.
Also the following message was delivered:

CODE: SELECT ALL
```
/usr/sbin/update-ipsets: line 1722: declare: RETENTION_HISTOGRAM: not found
```

as a short feedback from my side.

The script needed in another configuration (more lists) for 19492 IPs and 2920 CIDRs

CODE: SELECT ALL
```
real    2m5.902s
user    0m31.507s
sys     0m24.640s
```

got it under */etc/fcron.daily*, update starts at 01:25:00 AM. The extended version works also on weak systems like my e.g. ALIX board --> http://fireinfo.ipfire.org/profile/5362 ... b41388974b .

There can shurley be much more done so i´am curious for new ideas, corrections, clarifications, enhancements and/or constructive critics.

Greetings,

Erik

EDIT:
02.12.2016
- Added fw reload in rc.local

IPFire - An open source firewall solution
IPFire - An open source firewall solution

IPset for IPFire

Locked Search this topic... 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,

> **ktsaou 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 interessting 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.

> **ktsaou 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 ?!

> **ktsaou 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.

> **ktsaou 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...

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

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

CODE: SELECT ALL

```
Listen 12345
<VirtualHost *:12345>
    SSLEngine on
    SSLProtocol all -SSLv2
    SSLCipherSuite ALL:!ADH:!EXPORT56:!eNULL:!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

<Directory "/srv/web/firehol-ipset">
```

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 interesstng 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

ummeegge
Community Developer

Posts: 5001
Joined: October 9th, 2010, 10:00 am

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

ummeegge
Community Developer

Posts: 5001
Joined: October 9th, 2010, 10:00 am

Locked 33 posts 1 2 3

Return to "Development"
Home • Index