[Feature Request] Peergaurdian CLI $$

[Feature Request] Peergaurdian CLI $$

by **apoptosis** » March 2nd, 2014, 12:58 pm

apoptosis
Posts: 5
Joined: March 2nd, 2014, 11:44 am

So I just made a big mistake. I thought ipfire supported blocklists like Peergaurdian, Peerblook, Moblock, pfBlock, IPList. However, I miss read Guardian's url blocklists to be this feature. I ended up buying hardware, and installing ipfire only to find out I was wrong.

Then I was like okay, I will just run Peergaurdian CLI like on arch linux:

https://wiki.archlinux.org/index.php/PeerGuardian_Linux

Only to discover that ipfire does use rpm or deb packaging and instead uses pakfire.

Ok, so I will download and build myself so I downloaded the source at sourceforge:

http://sourceforge.net/projects/peergua ... n%20Linux/

I want a command line only "slick" installation with

./configure --without-qt4 --disable-dbus

Only to discover ipfire doesn't come with gcc, and you must build ipfire from scratch if you want to add a package like this.

At this I don't have a linux system handy to do the ipfire build and make my own pakfire package, nor the knowhow to do a good pakfire package.

I am willing to pay a bounty over paypal for any one to make a pgl-cli-2.2.4.pakfire package and make it available to everyone...

$20 - For just command line integration. The ipfire web console doesn't need a interface.

$50 - For a full blown web interface where you can set up and schedule downloads of blocklists.

pfSense has pfBlock, however I am already invested in ipfire and like linux better than BSD. ipfire really needs this feature and I am willing to contribute this money to get it done.

Re: [Feature Request] Peergaurdian CLI $$

by **burningpenguin** » March 2nd, 2014, 2:55 pm

burningpenguin
Posts: 173
Joined: December 5th, 2012, 7:37 pm

Well an easy way if you are worried about HTTP-based blocking is to write a script downloading and translating the files to be used in URLFilter. Downloading would be based on wget and a fcron job. The translation of the files to plain IP/URL should also not be rocket science as long as you do not need the classification which is inside the files. If the files are stored in a dedicated folder on ipfire these would also be "selectable" via the urlfilter webui.

But anyway I guess you want to not only block URLs but IPs for all sort of traffic.

I am not sure whether the new Firewall of ipfire 2.15 would help you.
http://forum.ipfire.org/http://forum.ipfire.org//viewtopic.php?t=9

cheers

Re: [Feature Request] Peergaurdian CLI $$

by **apoptosis** » March 2nd, 2014, 4:05 pm

apoptosis
Posts: 5
Joined: March 2nd, 2014, 11:44 am

I am not worried about http-blocking at all. I am worried about blocking major portions of the internet from all protocols, based on dynamic blocklists that I do not have to maintain, because they are maintained by others already.

AKA I want to subscribe to ip block lists. ipfire can already subscribe to web proxy block lists via squid with guardian, but this is not what I need.

Last edited by **apoptosis** on March 2nd, 2014, 4:07 pm, edited 1 time in total.

Re: [Feature Request] Peergaurdian CLI $$

by **burningpenguin** » March 2nd, 2014, 9:56 pm

burningpenguin
Posts: 173
Joined: December 5th, 2012, 7:37 pm

Hi
I guess the solution is this here
http://wiki.ipfire.org/en/configuration/firewall/firewall.local

Try this
.... currently manually - no scripting yet

1) Create a local file with various IPs to be blocked for out/in traffic e.g. /etc/sysconfig/blacklistmalcode
with data from http://malc0de.com/bl/IP_Blacklist.txt

CODE: SELECT ALL

```
wget -O - http://malc0de.com/bl/IP_Blacklist.txt > /etc/sysconfig/blacklistmalc0de
```

2) Remove all non-IPs

CODE: SELECT ALL

```
egrep -v '(^[[:space:]]*/|^[[:space:]]*$)' /etc/sysconfig/blacklistmalc0de > /etc/sysconfig/blacklistmalc0de
```

3) change the config

CODE: SELECT ALL

```
nano /etc/sysconfig/firewall.local
```

4) in my case it looks like

CODE: SELECT ALL

```
#!/bin/sh
# Used for private firewall rules

BLACKLIST="/etc/sysconfig/blacklistmalc0de"

# See how we were called.
case "$1" in
  start)
        ## add your 'start' rules here
        #iptables -A CUSTOMINPUT -s 222.186.30.110 -j DROP
        for BLACKLIST in `cat $BLACKLIST`; do
         iptables -A CUSTOMINPUT -s $BLACKLIST -j DROP
         #echo "dropping $BLACKLIST ..."
        done
```

5) Reload the firewall

CODE: SELECT ALL

```
/etc/init.d/firewall reload
```

This should work - on my box it takes quite some time to reload the firewall - so there might be still something wrong here 🤔

Let me know

cheers

Last edited by **burningpenguin** on March 2nd, 2014, 10:12 pm, edited 1 time in total.

Re: [Feature Request] Peergaurdian CLI $$

by **apoptosis** » March 2nd, 2014, 10:54 pm

apoptosis

Posts: 5
Joined: March 2nd, 2014, 11:44 am

I appreciate the effort for a work around but this is not what I am looking for.

1) I need something that uses the format from this site;

https://www.iblocklist.com/lists.php

you can read about the format here:

http://en.wikipedia.org/wiki/PeerGuardian

The reason for this is the community around this.

2) Its more complicated thank you think. There are block lists, then there are allow lists. So you block huge ranges, but then allow say a steam or blizzard list.

3) I have a neworking friend who tried to make iptables do what you are. He rean into the same problem. iptables is not built for millions of rules, and is slow. I don't know the details but I think peerguardian is a different bread of firewall.

4) I am fine with running both firewalls, all I really need is to run peer guardian command line on my ipfire machine. It can run along sided iptables.

Re: [Feature Request] Peergaurdian CLI $$

by **BeBiMa** » March 3rd, 2014, 1:06 pm

BeBiMa

Posts: 2842
Joined: July 30th, 2011, 12:55 pm
Location: Mannheim

First: Peerguardian also uses iptables!
Second: I do not understand yet, why you want to use Peerguardian opposed to Snort/Guardian. What is the difference.
Third: What about the critic

> **wikipedia wrote:**
> Other criticism Besides the original criticism of Version 1 being slow and buggy, most other criticism of PeerGuardian is around the actual technique used to block peers. Critics have pointed out that the blocklists are open to the public, and thus parties who may wish to circumvent PeerGuardian can actively check the list to see if their IP addresses have been blocked.
> The blocklists are also managed by the public, but there is no fool-proof method on checking or reporting why an IP address or range are bad, nor on checking if the blocked IP addresses still remain bad. The list relies on the public to make submissions, and thus is vulnerable to attack itself (see above section on blocklist management issues).
> Vista 64 bit and Windows 7 64 bit are listed for application compatibility, but require a work around involving disabling driver signing that may require some degree of computer skill.

Unitymedia Cable Internet (32MBit)

Re: [Feature Request] Peergaurdian CLI $$

by **apoptosis** » March 3rd, 2014, 2:01 pm

apoptosis
Posts: 5
Joined: March 2nd, 2014, 11:44 am

It appears your right about it using iptables:

http://sourceforge.net/p/peerguardian/w ... Technical/

However, I have also see people talk about different iplists that are binary trees:

http://www.maeyanie.com/2008/12/efficie ... blocklist/

Maybe iptables will work...

Snort is IDS so it only logs potential threats, Gaurdian turns it into IPS where it will block ips for a while that where snort rules match. Snort is packet inspection.

What I want is to block by ipaddress based on these lists people make. These lists are hacks, they are like "Block all of china". "Block all universities". "Block this list of know P2P police". These lists change all the time and are quite large. Which make automation really the only route.

Your last thing, which just points out a potential flaw. Doesn't mean its not a worth while thing to do. Security is always a fuzzy process. There is not secure and not secure, but degrees of security.

Not to mention if it wasn't a valid thing to do why would so many people be doing it, and why would pfSense be able to do it. I am not saying this should be on by default, I just want the option to install it.

Re: [Feature Request] Peergaurdian CLI $$

by **burningpenguin** » March 3rd, 2014, 3:35 pm

burningpenguin
Posts: 173
Joined: December 5th, 2012, 7:37 pm

Anyway – I guess the suggested way of amending iptables works – at least for me. I can add to the blacklist all sorts of ips via some bash commands and even automated with fcron.
The more important questions is, **which direction to block these malicous IPs and what is the correct syntax**.

1) What I suggested is for ***CUSTOMINPUT*** only but should the rules not be duplicated for ***CUSTOMOUTPUT***. Is there anybody who could please give some advice here? The wiki does not have too much info about this.

2) Also is there a best practice of the amount of ips in iptables – at the moment my bash script adds about 7000 ips to be blocked. Reloading the firewall takes quite some time on my Core2Duo E6550

cheers

Re: [Feature Request] Peergaurdian CLI $$

by **BeBiMa** » March 3rd, 2014, 3:48 pm

BeBiMa
Posts: 2842
Joined: July 30th, 2011, 12:55 pm
Location: Mannheim

Sorry, but I didn't understand your intention.

Do you want to block access from outside for certain IP groups. This is done by the "normal" firewall in IPFire already. Being a stateful packet inspection firewall, only packets belonging to connections initiated from inside are allowed to pass. This includes most "IPs from china" etc.
To supplement this, there's the possibiltiy to block the establishment of connections by firewall rules and the Squid redirector URLFilter. I bet, most of the unwanted traffic can be suppressed by this means.

Remain the cases where malware establishes connections to unwanted targets. Partly you can minimize this by antivirus scanners (clamav in IPFire). But the problem with such sort of software are not mainly the accesses to the network, but the access to the clients. Therefore you need a security strategy for the inside either, which solves this mostly.

Unitymedia Cable Internet (32MBit)

Re: [Feature Request] Peergaurdian CLI $$

by **BeBiMa** » March 3rd, 2014, 4:02 pm

BeBiMa
Posts: 2842
Joined: July 30th, 2011, 12:55 pm
Location: Mannheim

A more basic topic.

You cannot **block** requests to your network really. The source of the request isn't controlled by you.
Therefore despite of all firewall/IPS systems the requests from unwanted sites reach your WAN side.
All attempts to suppress these accesses can't achieve more than the SPI method, but consume much more ressources on your system.

Unitymedia Cable Internet (32MBit)

Re: [Feature Request] Peergaurdian CLI $$

by **burningpenguin** » March 3rd, 2014, 4:07 pm

burningpenguin
Posts: 173
Joined: December 5th, 2012, 7:37 pm

Fair enough – so the remaining challenge is if one PC in the LAN is hijacked or infecting and connecting to a botnet or whatsoever server.
Of course there is CLAMAV in ipfire working (but not IDS/snort) and as well as an Antivirus software on each LAN client nevertheless to be on the safe side I would like to block LAN outgoing traffic to the internet.
Applying the config above I can at least not access these IPs and in the webui the packets are counted correctly as CUSTOMINPUT drop'ed

Re: [Feature Request] Peergaurdian CLI $$

by **BeBiMa** » March 3rd, 2014, 4:37 pm

BeBiMa
Posts: 2842
Joined: July 30th, 2011, 12:55 pm
Location: Mannheim

> **burningpenguin wrote:**
> Fair enough – so the remaining challenge is if one PC in the LAN is hijacked or infecting and connecting to a botnet or whatsoever server.
> Of course there is CLAMAV in ipfire working (but not IDS/snort) and as well as an Antivirus software on each LAN client nevertheless to be on the safe side I would like to block LAN outgoing traffic to the internet.
> Applying the config above I can at least not access these IPs and in the webui the packets are counted correctly as CUSTOMINPUT drop'ed

Your solution uses the possiblities of iptables for a "outgoing/forward blacklist firewall" very well.
If the syntax of these blacklists is known, you just can do that.

But with big files there is a timing problem (you observed that). Each rule definition calls iptables, that restarts with the new rule set.
For a greater number of changes the iptables-save/iptables-restore mechanism with changing by a Perl script using the IPTables module would be more convenient.

Unitymedia Cable Internet (32MBit)

Re: [Feature Request] Peergaurdian CLI $$

by **apoptosis** » March 3rd, 2014, 6:50 pm

apoptosis
Posts: 5
Joined: March 2nd, 2014, 11:44 am

So I get that this could be done with existing iptables and some scripts for scheduling downloads, parsing, and updating iptables.

I also appreciate you guys looking into this.

However, I don't understand going though all that trouble when there is already popular supported linux program that does it.
Wouldn't it be much easier to just build the pgl package?

This is why I was offering such a low bounty, I thought this was just a build a package problem that could be solved by someone who was setup with a ipfire build in a few hours.

Not sure what the objection is to offering additional packages...

Re: [Feature Request] Peergaurdian CLI $$

by **burningpenguin** » March 3rd, 2014, 9:11 pm

burningpenguin
Posts: 173
Joined: December 5th, 2012, 7:37 pm

Hi
attached is a script you might try - just run the via bash after unpacked.

CODE: SELECT ALL

```
scriptblacklistip.sh
```

The script gets the IP blacklists from
www.malc0de.com
www.openbl.org - the 90 days blocklist
zeustracker.abuse.ch

So this is just a PoC - proof of concept.
- download the files
- remove comments, #, /, etc
- sort | uniq
- add to tmp file
- reload filewall

Preconditions as the manual example above

CODE: SELECT ALL

```
nano /etc/sysconfig/firewall.local
```

Change to

CODE: SELECT ALL

```
#!/bin/sh
# Used for private firewall rules

BLACKLIST="/etc/sysconfig/blacklist"

# See how we were called.
case "$1" in
  start)
        ## add your 'start' rules here
        #iptables -A CUSTOMINPUT -s 222.186.30.110 -j DROP
        for BLACKLIST in `cat $BLACKLIST`; do
         iptables -A CUSTOMINPUT -s $BLACKLIST -j DROP
         #echo "dropping $BLACKLIST ..."
        done
```

Let me know whether this does to the trick for you.
Note, this will add about 10.000 IPs to be blocked from traffic from LAN/green+blue => WAN/Internet/red. Also this might take some time to reload - so you own risk. It does work on my ipfire nicely.

Check the webui FIREWALL/IPTABLES to see the IPs added to block sending data to.

If this is running for you I might improve the script and add it to the how-to or wiki.

cheers

Re: [Feature Request] Peergaurdian CLI $$

by **burningpenguin** » March 4th, 2014, 8:31 pm

burningpenguin
Posts: 173
Joined: December 5th, 2012, 7:37 pm

Nobody brave enough to give this script a try?
It works for me fine and it add security esp. in case a PC within the LAN is hijacked / infected / etc.

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

[Feature Request] Peergaurdian CLI $$

Re: [Feature Request] Peergaurdian CLI $$

by **BeBiMa** » March 4th, 2014, 9:55 pm

BeBiMa — Posts: 2842 — Joined: July 30th, 2011, 12:55 pm — Location: Mannheim

Isn't it much easier to block the infected client, identified by his MAC, by iptables rules?

I do this for the smartphone of our daughter.

Unitymedia Cable Internet (32MBit)

Re: [Feature Request] Peergaurdian CLI $$

by **burningpenguin** » March 5th, 2014, 8:18 pm

burningpenguin — Posts: 173 — Joined: December 5th, 2012, 7:37 pm

good idea - but for this you have to know the infected clients - assumption would be, if you know the infected clients, why don't you fix it
Anyway, I am convinced the solution works - I built it as I intended to do so for my installation anyway. If somebody re-uses it, you are welcome. I will improve the script to export the URL-list where to fetch the IP-lists from in a seperate file

BTW, any sense to update http://wiki.ipfire.org/en/configuration/firewall/firewall.local?

Re: [Feature Request] Peergaurdian CLI $$

by **burningpenguin** » April 2nd, 2014, 7:54 am

burningpenguin — Posts: 173 — Joined: December 5th, 2012, 7:37 pm

added to wiki
http://wiki.ipfire.org/en/configuration/firewall/firewall.local

enjoy

Re: [Feature Request] Peergaurdian CLI $$

by **Garp** » December 10th, 2014, 2:01 pm

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

I ove this script. Added it to my installation, now i'm already adding the yoyo adservers entries. It appears that also works.

The only thing i cannot find, is where to check in IPFire > IPTABLES is the rules are being loaded.

Can anybody tell me?

Maybe there are also people who made additions to the script, that they can share?

One thing i did was to place the blacklistupdatescript.sh in /etc/fcron.daily/ so it gets updated automatically.

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: [Feature Request] Peergaurdian CLI $$

by **5p9** » December 10th, 2014, 2:26 pm

5p9 — Mentor — Posts: 1865 — Joined: May 1st, 2011, 3:27 pm

Hi,

here are another way to block websites with dns-filtering:
index.php?topic=11144.15

Thx burningpenguin! Nice work!

5p9

EDIT: @Garp looking for the script-template here https://forum.ipfire.org/http://forum.i ... 2#msg65232 as attechment (loggin and y see it)

EDIT: here any more blacklists sort by function:
https://www.iblocklist.com/lists.php

I will try to added this lists (e.g. hijacked, webexploit, et cetera) in your script.

Last edited by Guest on December 10th, 2014, 3:06 pm, edited 1 time in total.

Mail Gateway: mail proxy

Re: [Feature Request] Peergaurdian CLI $$

by **5p9** » December 11th, 2014, 9:58 am

5p9 — Mentor — Posts: 1865 — Joined: May 1st, 2011, 3:27 pm

Hi,

http://wiki.ipfire.org/en/optimiziation/script/pg/start
and
http://wiki.ipfire.org/de/optimization/scripts/pg/start

feel free to edit this howto

5p9

EDIT:
Here is a better blacklist site: https://www.blocklist.de/de/export.html
update time from this list, all 30 min. and in the last 48 h detectet IP Sources...very laaaarg txt-file! i'm test this txt-file in peergaurad-setting and to advise if it works well...

without blacklist.de all.txt 9155 entrys with this txt 35246 entrys - WOW!

Last edited by Guest on December 11th, 2014, 11:37 am, edited 1 time in total.

Mail Gateway: mail proxy

Re: [Feature Request] Peergaurdian CLI $$

by **5p9** » December 11th, 2014, 6:05 pm

5p9 — Mentor — Posts: 1865 — Joined: May 1st, 2011, 3:27 pm

Hi,

i have changed the regex from:

CODE: SELECT ALL
```
egrep -v '(^[[:space:]]*/|^[[:space:]]*#|^[[:space:]]*$)' /etc/sysconfig/blacklisttmp > /etc/sysconfig/blacklist
```

to:

CODE: SELECT ALL
```
egrep -v '(^[[:space:]]*/|^[[:space:]]*#|^[[:space:]]*$)|/[0-9]|\:|/g' /etc/sysconfig/blacklisttmp > /etc/sysconfig/bla
```

for filtering ipv6 addresses in the lists from blocklist.de...now its running perfect!

5p9

Mail Gateway: mail proxy

Re: [Feature Request] Peergaurdian CLI $$

by **5p9** » December 12th, 2014, 7:01 am

5p9 — Mentor — Posts: 1865 — Joined: May 1st, 2011, 3:27 pm

Hi,

i have a small problem with the

CODE: SELECT ALL
```
firewall reload
```

function.
http://wiki.ipfire.org/en/configuration ... _from_file

When i try to use this value:

CODE: SELECT ALL
```
#!/bin/sh
# Used for private firewall rules

BLACKLIST="/etc/sysconfig/blacklist"

# See how we were called.
case "$1" in
  start)
        ## add your 'start' rules here
        #iptables -A CUSTOMINPUT -s 222.186.30.110 -j DROP
        for BLACKLIST in `cat $BLACKLIST`; do
         iptables -A CUSTOMINPUT -s $BLACKLIST -j DROP
         #echo "dropping $BLACKLIST ..."
        done
```

then tell me the script:

> iptables: Bad rule (does a matching rule exist in that chain

Now, when i try this stop-Rule:

CODE: SELECT ALL
```
#!/bin/sh
# Used for private firewall rules

IPT="/sbin/iptables"
BLACKLIST="/etc/sysconfig/blacklist"

# See how we were called.
case "$1" in
  start)
        ## add your 'start' rules here
        # Peerguardian
        for BLACKLIST in `cat $BLACKLIST`; do
         $IPT -A CUSTOMINPUT -s $BLACKLIST -j DROP
         #echo "dropping $BLACKLIST ..."
```

then I see no more clue. Is that a problem with use -F function?

5p9

Mail Gateway: mail proxy

Re: [Feature Request] Peergaurdian CLI $$

by **Garp** » December 12th, 2014, 1:31 pm

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

Thx for your update; i use the bloclist.de list too now.

The only thing is: i don't know if this is actually working. You state that running iptables -L can take a long time, but on my system it is done in a millisecond. Also, reloading the firewall is really quick.

To to it all off, i can ping an ip that i know is in the blocklist from my laptop. That is connected through VPN now, though. When i'm home i will try to connected from a machine on the green interface.

How can i verify that the blocklists are actually loaded?

Last edited by Garp on December 12th, 2014, 1:58 pm, edited 1 time in total.

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: [Feature Request] Peergaurdian CLI $$

by **5p9** » December 12th, 2014, 2:17 pm

5p9 — Mentor — Posts: 1865 — Joined: May 1st, 2011, 3:27 pm

Hi,

> The only thing is: i don't know if this is actually working. You state that running iptables -L can take a long time, but on my system it is done in a millisecond. Also, reloading the firewall is really quick.

do you see in the iptables -L output the CUSTOMINPUT Chain, is this view empty?
You must find for example following ips:

for all.txt

CODE: SELECT ALL
```
1.1.188.255
1.160.122.86
1.162.232.185
1.163.68.60
...
```

or for the ssh.txt:

CODE: SELECT ALL
```
1.192.129.232
1.209.22.55
1.234.21.115
1.234.27.46
1.234.79.121
1.234.83.221
...
```

do not forget to remove # in your script. for example:

active ruleset:

CODE: SELECT ALL
```
#get list from blacklist.de - ssh.txt
printf "\n Get files: blacklistede"
wget -O - http://lists.blocklist.de/lists/ssh.txt > /etc/sysconfig/blacklistblssh
cat /etc/sysconfig/blacklistblssh >> /etc/sysconfig/blacklist
```

deactivated ruleset:

CODE: SELECT ALL
```
#get list from blacklist.de - bruteforce webserver.txt
#printf "\n Get files: blacklistede"
#wget -O - http://lists.blocklist.de/lists/bruteforcelogin.txt > /etc/sysconfig/blacklistblbf
#cat /etc/sysconfig/blacklistblbf >> /etc/sysconfig/blacklist
```

I ping from ipfire to this ip:

CODE: SELECT ALL
```
ping 100.42.49.134
```

the answer is 100 % packet loss...from the vpn-session i also get an answer, too.

Mail Gateway: mail proxy

Re: [Feature Request] Peergaurdian CLI $$

by **Garp** » December 12th, 2014, 2:59 pm

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

It doesn't work for me somehow. I know about the # and stuff. I'm not a super advanced linux user, but i'm also not stupid, luckily :-)

I double checked everything, but somewhere i have something wrong. I even created an empty blacklist with only one IP in it, but after reloading (even rebooting), i can still ping that IP from my internal network.

Where can i check if firewall.local is actually started or used?

UPDATE: i figured it out.

I have to use CUSTOMFORWARD with -d instead of CUSTOMINPUT with -s in firewall.local. This because i do not want to block anything coming in, i want tot block connections from the LAN going out. Now, i can ping an ip i want to block and it stops replying when the list is loaded.

Additionally, i noticed that the firewall.local wasn't reloaded. Somehow, reloading the 'normal' firewall does not reload the firewall.local. So i adjusted the blacklist.sh to reload the firewall.local instead of the normal firewall. Now it works....

Let's see how i can tweak this some more.....

UPDATE 2: when adding this list (http://www.malwaredomainlist.com/hostslist/ip.txt) tot the script, i get errors. Looking at the textfile it downloads on the ipfire box, i can see carriage returns in it on some lines, like this:

CODE: SELECT ALL
```
129.121.219.126^M
129.121.221.48^M
129.121.239.156
129.121.34.250^M
129.121.49.164^M
129.121.53.4
129.121.93.148^M
```

Could someone (help me) add a way to remove carriage returns in the blacklist file? I don't speak regex unfortunately. I found the command

CODE: SELECT ALL
```
 sed 's/\r//g' filename > newfilename
```

but don't know how to adjust the already present string in the script.

This is the error i get:

CODE: SELECT ALL
```
Try `iptables -h' or 'iptables --help' for more information.
' not found.4.21: host/network `129.121.219.126
Try `iptables -h' or 'iptables --help' for more information.
' not found.4.21: host/network `129.121.221.48
Try `iptables -h' or 'iptables --help' for more information.
' not found.4.21: host/network `129.121.34.250
Try `iptables -h' or 'iptables --help' for more information.
' not found.4.21: host/network `129.121.49.164
Try `iptables -h' or 'iptables --help' for more information.
' not found.4.21: host/network `129.121.93.148
Try `iptables -h' or 'iptables --help' for more information.
' not found.4.21: host/network `130.185.84.10
Try `iptables -h' or 'iptables --help' for more information.
' not found.4.21: host/network `130.255.190.13
```

Last edited by Garp on December 14th, 2014, 9:07 am, edited 1 time in total.

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: [Feature Request] Peergaurdian CLI $$

by **Garp** » December 14th, 2014, 12:28 pm

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

Ok, i fixed it, i think. Also added some extra IP blacklists.

Let me sum up the changes made to reach my personal goals for using this script: defending clients on my network from getting infected with malware, contact C&C servers, and download malware payload by connecting directly to the ip of the 'bad' machine.

1. The file /etc/sysconfig/firewall.local has been changed to block access from blue and green connected machines to the internet. The original script didn't work for me. I could still ping ip's that were loaded into iptables. No i cannot.

I also changed the DROP to REJECT. I did this mainly for troubleshooting reasons; when sending a ping to an ip, you now get a different response than when you use DROP. When i ping an (unresponsive) ip from a client now, i can tell whether is has been rejected by my own firewall, or that it really isn't responding because of something else.

PS: this setup prevents connecting to blacklisted ip's from devices on the GREEN and BLUE networks, NOT from the firewall itself, so please test your setup from a connected device, not on the firewall itself.

CODE: SELECT ALL
```
#!/bin/sh
# Used for private firewall rules

IPT="/sbin/iptables"
BLACKLIST="/etc/sysconfig/blacklist"

# See how we were called.
case "$1" in
  start)
        ## add your 'start' rules here

        # Custom fix for slow connection of clients in GREEN and BLUE when loading a large blacklist
        $IPT -A CUSTOMFORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT
```

2. I adjusted the script to download the blacklists somewhat. I use malware-related blacklists that i know of and are freely available. I added a check/remove from some end of line issues (returns of some kind) that are there because of the differences in handling line ends between windows an linux. Also, i changed te order of things a little so when the script ends, i get a simple overview of the amount of lines in each blacklist. I also chose to remove the individual lists after the complete list has been created, to keep things nice and tidy.

I also wanted to be able to detemine how long it takes to reload the firewall.local, so i added a very simple check.

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

############################################################################
# 2014-03-03 by burningpenguin: scriptblacklistip
#
# add blocked IPs to the firewall to not be accessed from green/blue
############################################################################
# 2014-03-03 initial version
# 2014-12-13 adjustments by Garp
#
############################################################################
# forum: http://forum.ipfire.org/http://forum.ipfire.org//viewtopic.php?t=8
############################################################################
```

All of this is a work in progress; if someone has the ability and knowledge of adjusting the above script in a way that it uses variables, so it is easier to maintain: that would be great. If not, then not.

For now, this script is in /etc/frcon.daily/ so the rules are reloaded daily.

A side effect that i noticed: rebooting (well, booting) IPFire now takes a considerable amount of time. It takes it 10 minutes or so to be fully functional after a reboot. Reloading firewall.local only takes just under two minutes with approximately 5000 ip's in the blacklist. I have no idea why a reboot takes that long. I'm not planning to put much effort in finding out: it doesn't get rebooted that often.

Does anyone have more good blacklists?
As i am always interested in adding more IP's in the blacklist; please drop a note if you know of a publicly available list that is not present in the script yet. I will that add it to the script so everybody can use and enjoy it.

Last edited by Garp on January 2nd, 2015, 4:14 pm, edited 3 times in total.

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: [Feature Request] Peergaurdian CLI $$

by **H&M** » December 15th, 2014, 10:00 am

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

Hi,
Some collections of lists (many purposes!):

http://www.openbl.org/lists.html

http://www.joewein.de/sw/bl-text.htm#urls

Download URLs of plain text files
Here are plaintext versions of our blacklists. The domain blacklist consists of two files, the 419 blacklist of one file:

Domain blacklist base (spamvertised domains):
This file contains the bulk of the spam domains. It is updated infrequently and therefore need not be downloaded more than once a week. You must not download it more than once a day or your IP address may be blocked without notice:
http://www.joewein.net/dl/bl/dom-bl-base.txt

Domain blacklist new (recently added spamvertised domains):
This file contains additions made during the last week or two only. You can download once per day or more, but we currently don't recommend intervals more frequent than hourly.
http://www.joewein.net/dl/bl/dom-bl.txt

Email sender blacklist (419 scam and other spam senders):
http://www.joewein.net/dl/bl/from-bl.txt

List for AdBlock (the list contains links)
http://vxvault.siri-urz.net/URL_List.php
https://openphish.com/feed.txt

List in Windows HOST format:
http://hosts-file.net/.%5Cad_servers.txt

Have a nice day / Bonne journée / Haben Sie einen guten Tag
H&M

Re: [Feature Request] Peergaurdian CLI $$

by **N3ST** » December 15th, 2014, 12:30 pm

N3ST — Posts: 37 — Joined: September 12th, 2014, 7:22 am

Hello everyone,

I think you can also use the emerging threats IP blocking list https://rules.emergingthreats.net/fwrul ... ck-IPs.txt

Here you can find a perl script that update the IPtables rules : http://doc.emergingthreats.net/pub/Main ... ate.pl.txt

It could be interesting too integrate this kind of feature directly into the WEB GUI, and the possibilitie to suscribe to different IP blocking list, like a drop down menu.

This will be interresting to be able to block IP inbound and outbound especially the CnC ones.

What do you think of that ?

Best regards,

N3ST

Last edited by N3ST on December 15th, 2014, 12:32 pm, edited 1 time in total.

Re: [Feature Request] Peergaurdian CLI $$

by **5p9** » December 18th, 2014, 8:14 am

5p9 — Mentor — Posts: 1865 — Joined: May 1st, 2011, 3:27 pm

Hi,

> It could be interesting too integrate this kind of feature directly into the WEB GUI, and the possibilitie to suscribe to different IP blocking list, like a drop down menu.

i think this is a nice AddOn for one Peerguard-Section in the WUI. But, who can do it?

We have two options:

1. the manuell peerguard-script
2. the emerging threats IP blocking list

So, i think we must include the peerguard-script from this topic in the perl-script for more usability and functionality. That would be very nice!

5p9

Mail Gateway: mail proxy

[Feature Request] Peergaurdian CLI $$

Re: [Feature Request] Peergaurdian CLI $$

by **l0rdraiden** » December 27th, 2014, 4:55 pm

l0rdraiden
Posts: 13
Joined: September 30th, 2014, 8:35 am

> **5p9 wrote:**
> Hi,
>
> > It could be interesting too integrate this kind of feature directly into the WEB GUI, and the possibilitie to suscribe to different IP blocking list, like a drop down menu.
>
> i think this is a nice AddOn for one Peerguard-Section in the WUI. But, who can do it? 🤔
>
> We have two options:
>
> 1. the manuell peerguard-script
> 2. the emerging threats IP blocking list
>
> So, i think we must include the peerguard-script from this topic in the perl-script for more usability and functionality. That would be very nice!
>
> 5p9

If someone makes this via web interface for "noobs" I would donate some money.
I think this option should be more used http://wishlist.ipfire.org/ I think a lot of people in the community will be willing to pay to speed up the development of some features, in particular if you make them easy to use.

Re: [Feature Request] Peergaurdian CLI $$

by **Garp** » December 29th, 2014, 1:02 pm

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

I adjusted the script again. For those who are interested:

CODE: SELECT ALL

```
#!/bin/bash

##############################################################################
# 2014-03-03 by burningpenguin: scriptblacklistip
#
# add blocked IPs to the firewall to not be accessed from green/blue
##############################################################################
# 2014-03-03 initial version
# 2014-12-13 adjustments by Garp
# 2014-12-28 adjustments by Garp (blocklists added)
# 2014-12-29 Garp: Remove yoyo Ads, they are being blocked by using the
#                hostsfile and the url filter
#
```

Re: [Feature Request] Peergaurdian CLI $$

by **N3ST** » December 29th, 2014, 8:48 pm

N3ST
Posts: 37
Joined: September 12th, 2014, 7:22 am

Hello,

I tried your script, and I am getting this error message when I run it : iptables: Bad rule (does a matching rule exist in that chain?).

I can't find some of the emerging threat IP normally that kind of IP should appear in the file /etc/sysconfig/blacklist :

5.34.242.0/23
5.72.0.0/14
14.4.0.0/14
14.129.0.0/16
14.192.48.0/21
14.192.56.0/22)

If you check here and if you scroll down :

https://rules.emergingthreats.net/fwrul ... ck-IPs.txt

Otherwise with that there is almost 80000 lines this is nice.

We could even try to block then in and out, but it might take a long time to update the Iptables rules what do you think?

Is there also a way to only only certain host name from accessing the website I am hosting internally?

For exemple I can use my parents router to send an update for AAAA records in no-ip then only allow the host name from accessing the website, is that possible?

Thank you in advance.

Best regards,

N3ST

Re: [Feature Request] Peergaurdian CLI $$

by **5p9** » December 30th, 2014, 6:41 am

5p9
Mentor

Posts: 1865
Joined: May 1st, 2011, 3:27 pm

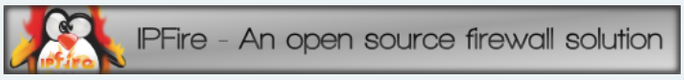
Hi Garp,

> Ok, i fixed it, i think. Also added some extra IP blacklists.
>
> Let me sum up the changes made to reach my personal goals for using this script: defending clients on my network from getting infected with malware, contact C&C servers, and download malware payload by connecting directly to the ip of the 'bad' machine.

thx for your work. I will update in the time the wiki-howto with your config-informations.

5p9

Mail Gateway: mail proxy



Re: [Feature Request] Peergaurdian CLI $$

by **N3ST** » December 30th, 2014, 11:58 am

N3ST

Posts: 37
Joined: September 12th, 2014, 7:22 am

Hello,

i also found this github project to create an utlimate blocklist :

https://walshie4.github.io/Ultimate-Blocklist/

https://gist.github.com/johntyree/3331662

Does anybody have an idea why we are getting werror message and why we can't add these kind of Ip addresses 192.168.25.0/24?

Bets regards,

N3ST

Re: [Feature Request] Peergaurdian CLI $$

by **5p9** » December 30th, 2014, 12:21 pm

5p9
Mentor

Posts: 1865
Joined: May 1st, 2011, 3:27 pm

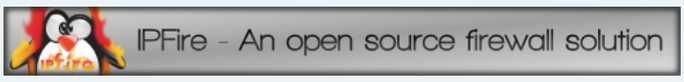
Hi,

> 192.168.25.0/24?

there is in your internal network (privacy Network range 192.168.xxx.xxx/24). You do not want to this Range in your Blocklist
You must exclude this local IPs.

5p9

Mail Gateway: mail proxy



Re: [Feature Request] Peergaurdian CLI $$

by **Garp** » December 30th, 2014, 12:29 pm

Garp

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

The Emerging blocklist that you mention doesn't work; they use entire blocks in the list. The script only works with single ip's.

> **N3ST wrote:**
> Hello,
>
> I tried your script, and I am getting this error message when I run it : iptables: Bad rule (does a matching rule exist in that chain?).
>
> I can't find some of the emerging threat IP normally that kind of IP should appear in the file /etc/sysconfig/blacklist :
>
> 5.34.242.0/23
> 5.72.0.0/14
> 14.4.0.0/14
> 14.129.0.0/16
> 14.192.48.0/21

14.192.56.0/22)

If you check here and if you scroll down :

https://rules.emergingthreats.net/fwrul ... ck-IPs.txt

Otherwise with that there is almost 80000 lines this is nice.

We could even try to block then in and out, but it might take a long time to update the Iptables rules what do you think?

Is there also a way to only only certain host name from accessing the website I am hosting internally?

For exemple I can use my parents router to send an update for AAAA records in no-ip then only allow the host name from accessing the website, is that possible?

Thank you in advance.

Best regards,

N3ST

Re: [Feature Request] Peergaurdian CLI $$

by **N3ST** » December 30th, 2014, 12:34 pm

N3ST

Posts: 37
Joined: September 12th, 2014, 7:22 am

No non this is not what il meant.

If you go take a look there :

You can find a lot of Ip addresse like these https://rules.emergingthreats.net/fwrul ... ck-IPs.txt :

141.253.0.0/16
143.49.0.0/16
143.64.0.0/16
143.135.0.0/16
143.189.0.0/16
144.207.0.0/16
146.3.0.0/16
147.50.0.0/16
148.105.0.0/16
148.154.0.0/16
148.178.0.0/16
148.248.0.0/16
149.109.0.0/16
149.118.0.0/16
149.143.64.0/18
150.10.0.0/16
150.22.128.0/17
150.107.220.0/22
150.126.0.0/16
150.141.0.0/16
150.230.0.0/16
151.123.0.0/16
151.192.0.0/16
151.212.0.0/16
151.237.184.0/22
152.136.0.0/16
152.147.0.0/16
153.14.0.0/16
153.121.128.0/17
153.127.0.0/17
155.204.0.0/16
157.162.0.0/16

But I cannot find them in the Iptables list or in the blacklist file, it seems that the script is ignoring them.

Best regards,

N3ST

Re: [Feature Request] Peergaurdian CLI $$

by **N3ST** » December 30th, 2014, 12:38 pm

N3ST

Posts: 37
Joined: September 12th, 2014, 7:22 am

> **Garp wrote:**
> The Emerging blocklist that you mention doesn't work; they use entire blocks in the list. The script only works with single ip's.

Ok thanks for the reponse.

Maybe we can take some part of this cript :

http://doc.emergingthreats.net/pub/Main ... ate.pl.txt

Best regards,

N3ST

Re: [Feature Request] Peergaurdian CLI $$

by **Garp** » January 1st, 2015, 5:47 pm

Garp

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

I noticed that when the more ip's are loaded in ip IPTables, the slower my - for example - usenet downloads on another machine in the green network get. If i flush the extra loaded firewall rules (with the command /etc/sysconfig/firewall.local stop), the speed goes back to normal.

I've played around with enabling and disabling of the various rulesets and thus varying the amount of ip's loaded, and did some measuring while downloading. Some indicators:

* With appr. 5000 ip's loaded, the speed of usenet downloads on a client machine is 1.6MB/s
* with appr. 3000 ip's loaded, the speed is 2.8MB/s
* With appr. 1200 ip's loaded, the speed is 8.4 MB/s
* Without ip's loaded (firewall.local stopped), the speed is 10.4MB/s

Anyone got any explanation for this? How cold this be prevented?

UPDATE: i appear to have found a fix.

In firewall.local, an extra line has to be added to accept established connections for the CUSTOMFORWARD chain:

CODE: SELECT ALL

```
$IPT -A CUSTOMFORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT
```

My script is now as follows:

CODE: SELECT ALL

```
#!/bin/sh
# Used for private firewall rules

IPT="/sbin/iptables"
BLACKLIST="/etc/sysconfig/blacklist"

# See how we were called.
case "$1" in
  start)
        ## add your 'start' rules here

        # Custom fix for slow connection of clients in GREEN and BLUE  when loading a large blacklist
        $IPT -A CUSTOMFORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT
```

Re: [Feature Request] Peergaurdian CLI $$

by **burningpenguin** » January 24th, 2015, 12:52 pm

burningpenguin

Posts: 173
Joined: December 5th, 2012, 7:37 pm

Hi all
quite amazing that eventually my first best try of scripting something handy for ipfire kicked off such a discussion and evolution of the script. I was offline for some time and will follow up what has been changed. Thanks for your interest and support.

About the last post:
I have to admit to, that adding a lot of IPs to be blocked and many URL-filters in parallel slows down ipfire. I currently have the case that accessing a richer web page causes my dual core intel 2 Ghz to be maxed out for a split of a second. There is some space for improvement for sure

regards

Re: [Feature Request] Peergaurdian CLI $$

by **burningpenguin** » January 24th, 2015, 2:01 pm

burningpenguin

Posts: 173
Joined: December 5th, 2012, 7:37 pm

Well while running thru the messages it looks like there ar enow different variations
1) script to block LAN outgoing traffic / requests
CUSTOMFORWARD with -d instead of CUSTOMINPUT with -s

2) script to block LAN incoming traffic / replies
iptables -A CUSTOMINPUT -s $BLACKLIST -j DROP

3) potentially 1+2 could be combined

And an option to speed up exisiting connections
$IPT -A CUSTOMFORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT

And as well a debate about whether DROP or REJECT is the best choice.

On another note, this way of doing IP blocking might be inefficient as DNS queries are send nethertheless 😬

Moreover the amount of blocked-IPs increased significantly. Hence the script needs some rework to make it more generic and read the URLs for blocked-IP-lists from a config file rather than having this in the script.

It would be good if a "iptables" expert could give some advice on custominput vs customforward and whether drop or reject is "better"

I assume I have some more time now to work on the script.

Re: [Feature Request] Peergaurdian CLI $$

by **Garp** » January 25th, 2015, 4:45 pm

Garp

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

Hi BurningP,

> And an option to speed up exisiting connections
> $IPT -A CUSTOMFORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT

This really helps lowering the load enormously on your machine. Try it in your config. Offcourse, in case you use CUSTOMINPUT instead of CUSTOMFORWARD in your /etc/sysconfig/firewall.local, you should use that.

> On another note, this way of doing IP blocking might be inefficient as DNS queries are send nethertheless 😬

You're right. Access to other DNS servers then your own should be blocked. That's wise to do. I already mentioned that in my post about protecting your clients on your LAN (http://forum.ipfire.org/viewtopic.php?f=27&t=12122&p=78219#p78219).

> It would be good if a "iptables" expert could give some advice on custominput vs customforward and whether drop or reject is "better"

It's just different.

CUSTOMINPUTrejects traffic coming in through the red interface (on ports that your have openened) which is initiated on the 'bad ip' side.

CUSTOMFORWARD denies traffic initiated on green or blue, going out through red. Because my ipfire is used at home, and no services are offered to the outside world, this scenario is right for me.

IPFire - An open source firewall solution

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: [Feature Request] Peergaurdian CLI $$

by **lordraiden** » January 26th, 2015, 1:42 pm

For me it looks like you are trying to reinvent the wheel, Peergaurdian is out there, and probably it could be integrated in IPFire somehow

lordraiden

Posts: 12
Joined: December 30th, 2014, 12:33 pm

Post Reply

44 posts 1 2 3

Return to "Development"

Home › Index

Delete cookies All times are UTC

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