pfSense - Bug #3334

Status/Traffic Graph isn't IPv6 ready

11/21/2013 05:18 AM - Armin Fasold

Status:	Confirmed		**Start date:**	11/21/2013
Priority:	Normal		**Due date:**	
Assignee:			**% Done:**	0%
Category:	Web Interface		**Estimated time:**	0.00 hour
Target version:				
Affected Version:	All		**Affected Architecture:**	

Description

In /usr/local/www/bandwith_by_ip.php, which is called per AJAX/XHR to provide the data for the right table in "Traffic Graph" page (status_graph.php), the program "rate" is called to acquire that data.

Looking into the source code of "rate", to see what all the given parameters do, I noticed that it uses u_int32_t [0] for storing the IP addresses. This results in a silent fail if called with an IPv6 netmask and no listing of IPv6 traffic sources.

[0]: https://fossies.org/dox/rate-0.9/rate__abusers_8c_source.html#l00062

History

#1 - 11/15/2015 12:23 AM - Chris Buechler

- Status changed from New to Confirmed

#2 - 07/28/2016 04:35 PM - Luca Moncelli

IPv6 issue still present in 2.3.2

#3 - 02/23/2017 07:24 AM - Jim Pingle

- Affected Version changed from 2.1-IPv6 to All

#4 - 04/05/2017 09:31 AM - Pim Pish

When will this be resolved? This is a really old bug.

#5 - 04/05/2017 09:51 AM - Jim Pingle

The underlying program, rate, still doesn't work with IPv6 as far as I'm aware.

I'd love to see rate swapped out for iftop (which does support IPv6) but the output of iftop isn't easy to parse and it has some issues running on interfaces that are disconnected or have no traffic, which makes it difficult to work with in an automated manner. iftop is also connection-oriented so it doesn't give per-host stats like rate. I have some testing code for it but I'm not terribly happy with how it operates yet. I don't see it replacing rate, but perhaps it might work as an add-on package.

#6 - 01/15/2019 11:55 PM - Daryl Morse

Jim Pingle wrote:

> The underlying program, rate, still doesn't work with IPv6 as far as I'm aware.
>
> I'd love to see rate swapped out for iftop (which does support IPv6) but the output of iftop isn't easy to parse and it has some issues running on interfaces that are disconnected or have no traffic, which makes it difficult to work with in an automated manner. iftop is also connection-oriented so it doesn't give per-host stats like rate. I have some testing code for it but I'm not terribly happy with how it operates yet. I don't see it replacing rate, but perhaps it might work as an add-on package.

I looked at the man page for rate. It appears to have been written in 2003 by Mateusz Golicz <mteg@jaszczur.org>, aka github.com/mteg. There doesn't appear to be a repository for rate, so you have to think he abandoned it and moved on. I tried emailing him, but he didn't reply. In the absence of the author, the code isn't going to fix itself.

#7 - 01/17/2019 11:22 AM - Joshua Sign

Jim Pingle wrote:

> I'd love to see rate swapped out for iftop (which does support IPv6) but the output of iftop isn't easy to parse and it has some issues running on interfaces that are disconnected or have no traffic, which makes it difficult to work with in an automated manner. iftop is also connection-oriented so it doesn't give per-host stats like rate. I have some testing code for it but I'm not terribly happy with how it operates yet. I don't see it replacing rate, but perhaps it might work as an add-on package.

Me too, I am looking for a way to replace rate by iftop.
Since iftop-1.0pre3 (2014-01-01), a text output mode was added, so it is possible to get an output like rate.
An awk script is good enough for that, i just test something like that :

```
# iftop -nNb -i eth0 -s 1 -o 2s -F 10.0.0.0/8 -t | awk -f iftop_parse.awk
10.0.50.233 3,27Kb 3,27Kb 1,87Kb 1,87Kb
216.58.198.206 1,87Kb 1,87Kb 3,27Kb 3,27Kb
10.0.50.233 1,59Kb 1,59Kb 2,18Kb 2,18Kb
216.58.204.101 2,18Kb 2,18Kb 1,59Kb 1,59Kb
10.0.48.251 896b 896b 0b 0b
224.0.0.18 0b 0b 896b 896b
10.0.51.217 660b 660b 0b 0b
239.255.255.250 0b 0b 660b 660b
10.0.51.9 644b 644b 0b 0b
239.255.255.250 0b 0b 644b 644b
```

The awk script is very simple :

```
BEGIN {
        FS              = " "
        numlist = 0
}
{
        if ( numlist == 1 && $1 == "----------------------------------------------------------------------------------------------" ) {
                numlist = 2
                next
        }

        if ( numlist == 0 && $1 == "----------------------------------------------------------------------------------------------" ) {
                numlist = 1
                next
        }

        if ( numlist == 1 ) {
                if ( $0 ~ "=>") {
                        SENDER = $2
                        STX = $4
                        STXAVG = $5
                        getline
                        RECEIVER = $1
                        RTX = $3
                        RTXAVG = $4
                        print SENDER" "STX" "STXAVG" "RTX" "RTXAVG
                        print RECEIVER" "RTX" "RTXAVG" "STX" "STXAVG

                }
                next
```

```
            }

        if ( $1 == "=========================================================================
==" ) {
                numlist = 0
                next
        }

}
END {
}
```

I also notice no errors on disconnected interfaces or when there is no trafic.
(version 1.0pre4 of iftop, on 2.4.4 pfsense release)

Please tell me if I can help, or if I just waste our time.

#8 - 01/17/2019 12:02 PM - Jim Pingle

That does help a bit. It would be even better if iftop had an output mode like libxo where it would be trivial to parse the output, but I'm not sure how the project author(s) would feel about that.

Can you create a PR that changes rate to iftop? No need to worry about the dependency issues at first (adding iftop to base, that is), since we'd need to run it through manual tests before it gets merged anyhow.

#9 - 01/17/2019 12:14 PM - Joshua Sign

ok i will work on it and create a PR to change rate by iftop as soon as it works
(normaly it should be ok on sunday or before)

#10 - 01/18/2019 10:19 AM - Joshua Sign

Hi Jim,

FYI, I just finish some tests : it seems to works as expected.

All we need to test is :

This awk script 'iftop_parser.awk' :

```
BEGIN {
        FS              = " "
        numlist  = 0
        nblines  = 15
        printf "\n\n"
}
{
```

```
        if ( numlist == 1 && $1 == "-------------------------------------------------------------------------
------------------" ) {
                exit
        }

        if ( numlist == 0 && $1 == "-------------------------------------------------------------------------
------------------" ) {
                numlist = 1
                next
        }

        if ( numlist == 1 ) {
                if ( $0 ~ "=>" && nblines > 0 ) {
                        SENDER = $2
                        STX = pfFormat($4)
                        getline
                        RECEIVER = $1
                        RTX = pfFormat($3)
                        printf "%s;%s;%s\n", SENDER,RTX,STX
                        printf "%s;%s;%s\n", RECEIVER,STX,RTX
                        nblines--
                        if ( nblines < 1 ) {
                                exit
                        }
                }
                next
        }

}
END {
}

function pfFormat(str) {
        sub("b","",str)
        return str
}
```

And these changes in /usr/local/www/bandwidth_by_ip.php :

- replace line 112 by the code bellow :

```
$_grb = exec("/usr/bin/timeout 5 /usr/local/sbin/iftop -nNb -i {$real_interface} -s 1 -o 2s -t | /usr/bin/awk
-f /root/iftop_parse.awk", $listedIPs);

// Functions format
// TODO : replace by existing function or put this in pfsense-utils.inc
function GMK2bits($val) {
        $val = strtolower($val);
        if ( strpos($val,"g") !== false ) {
                $val = str_replace("g","",$val) * 1000 * 1000 * 1000;
        } else if ( strpos($val,"m") !== false ) {
                $val = str_replace("m","",$val) * 1000 * 1000;
        } else if ( strpos($val,"k") !== false ) {
                $val = str_replace("k","",$val) * 1000;
        }

        return $val*1;
}

function bits2GMK($val) {
        $units = array ( 0 => "", 1 => "K", 2 => "M", 3 => "G" );
        $u=0;
        while ($val > 1000) {
                $val = $val/1000;
                $u++;
        }
        return round($val,2).$units[$u];
}
// END of Functions format

// order and group by
```

```php
foreach ($listedIPs as $k => $line){
        if ($line != "") {
                $arrLine = explode (";", $line);
                $ip  = $arrLine[0];
                $in  = GMK2bits($arrLine[1]);
                $out = GMK2bits($arrLine[2]);
                if ( isset($arr_in[$ip]) ) {
                        $arr_in[$ip]  += $in;
                        $arr_out[$ip] += $out;
                } else {
                        $arr_in[$ip]  = $in;
                        $arr_out[$ip] = $out;
                }
        }
}

if ($sort == "out") {
        arsort($arr_out,SORT_NUMERIC);
        $arrIP = array_keys($arr_out);
} else {
        arsort($arr_in,SORT_NUMERIC);
        $arrIP = array_keys($arr_in);
}

unset($listedIPs);
$listedIPs[] = "";
$listedIPs[] = "";
foreach ($arrIP as $k => $ip) {
        $listedIPs[] = $ip.";".bits2GMK($arr_in[$ip]).";".bits2GMK($arr_out[$ip]);
}
```

- change separator ":" by ";" on the line 180
(it was line 122 before adding the code above) :

```php
$infoarray = explode (";", $bandwidthinfo);
```

Unfortunally i don't use IPV6, so i can't test this part.
But it was necessary to change this separator to avoid IPV6 confict.

The exec of iftop may take between 1 or 2 seconds most of time.
But i experienced some cases where iftop wait more than 7 seconds before giving a result (or no result because not enough traffic).
Maybe thats what you experienced when you was talking about issues, so i add 'timeout 5' to the command line to ensure that iftop will not stay stucked and overload the system.
Yes it is a crappy solution, but it is not the best we can do.
This is even more usefull if there are many users on the status_graph.php : multiples concurrent processes are created.
We can look for another way to avoid multiples concurrent processes and increase performances. (i got some ideas)

Please tell me :
- if i miss something (i don't use '-F' or '-G' flag, maybe needed for ipv6?)
- if the order of IN/OUT bis are corrects... they seems to me
- where is the best place for the awk script ? (/etc ? /usr/local/bin ?)
- is there an equivalent of GMK2bits / bits2GMK in pfSense ? If there is not, should i add them to pfsense-utils.inc ?
- do we try to improve performances about concurrent processes if many users are on the same graph ?

It also should be possible to create a PR by adding iftop as an additional feature instead of replacing rate. (iftop must be added by pkg install)
This could be better to avoid any revert if somes have problems with iftop.
Otherwise, the old unused code can be removed.

I wait for your instructions and feedbacks if some of us can test it.

#11 - 01/18/2019 05:36 PM - Daryl Morse

Joshua Sign wrote:

> Unfortunaly i don't use IPV6, so i can't test this part.

I have IPv6 so I would be happy to test when you have something ready. Can you provide it as a patch based on the latest development snapshot?

#12 - 01/18/2019 06:10 PM - Joshua Sign

yes it will be possible soon.

I just wrote this script to avoid process concurrent creation when many users are on the same graph.
My tests looks good.

I'll put it in the PR.

```sh
#!/bin/sh

# Usage
if [ $# -ne 1 ]; then
        echo "Usage : $0 iface"
        exit
fi

# files paths
pid_file=/var/run/iftop_$1.pid
cache_file=/var/db/iftop_$1.log
awk_script=/root/iftop_parse.awk

# Binaries paths
DATE=/bin/date
STAT=/usr/bin/stat
CUT=/usr/bin/cut
PS=/bin/ps
GREP=/usr/bin/grep
CAT=/bin/cat
RM=/bin/rm
IFTOP=/usr/local/sbin/iftop
AWK=/usr/bin/awk

# test if pid file exist
if [ -f $pid_file ]; then
        # check how old is the file
        curTS=`$DATE +%s`
        pidTS=`$STAT -r $pid_file | $CUT -d " " -f 10`
        # if more than 10 seconds,
        # it must be a dead pid file (process killed?)
        # or a stucked process that we should kill
        if [ $(( curTS - pidTS )) -gt 10 ]; then
                oldPID=`$CAT $pid_file`
                # test if pid still exist
                run=`$PS -p $oldPID | $GREP -F '$0'`
                if [ "$run" != "" ]; then
                        kill -9 $oldPID
                fi
                $RM $pid_file
                $RM $cache_file
                exit
        fi
        if [ -f $cache_file ]; then
                $CAT $cache_file
        fi
        exit
fi
```

```
echo -n $$ > $pid_file

$IFTOP -nNb -i $1 -s 1 -o 2s -t 2>> /dev/null | $AWK -f $awk_script > $cache_file.1
$CAT $cache_file.1 > $cache_file
$CAT $cache_file
$RM $pid_file
```

Then just change the exec in /usr/local/www/bandwidth_by_ip.php by

```
$_grb = exec("/root/iftop_parser.sh {$real_interface}", $listedIPs);
```

I'll create a PR soon.

#13 - 01/18/2019 06:17 PM - Joshua Sign

- File bandwidth_by_ip.php added

- File iftop_parse.awk added

- File iftop_parser.sh added

here are the files you need to easely test, it is faster thant the PR
just put the two scripts into the root directory, and replace the /usr/local/www/bandwidth_by_ip.php

#14 - 01/19/2019 12:27 AM - Joshua Sign

- File pfSense_status_graph.patch added

Here is the patch

/usr/local/bin/iftop_parser.sh must have +x

#15 - 01/19/2019 02:12 AM - Joshua Sign

PR : https://github.com/pfsense/pfsense/pull/4039

#16 - 01/19/2019 12:33 PM - Daryl Morse

Joshua Sign wrote:

> PR : https://github.com/pfsense/pfsense/pull/4039

I installed this patch on the most recent snapshot, built on Sat Jan 19 05:32:33 EST 2019. I used http://ipv6-test.com/speedtest/ to test it, because there are separate speedtests for ipv4 and ipv6, making it easy to see traffic for both protocols. I tried both WAN and LAN, but the patch doesn't show anything for ipv6. For ipv4, I did not see any difference with the patch applied or not applied. I did not reboot after applying the patch. Should I have?

#17 - 01/20/2019 05:36 AM - Joshua Sign

can you chexk over console if iftop shows you some IPV6 adresses just by : `iftop -n` ?

as far as i didn't have any ipv6, it will be difficult to test this part.

#18 - 01/20/2019 10:47 AM - Daryl Morse

Joshua Sign wrote:

> can you chexk over console if iftop shows you some IPV6 adresses just by : `iftop -n` ?
>
> as far as i didn't have any ipv6, it will be difficult to test this part.

Sorry mate. iftop -n shows ipv4 and ipv6 traffic, but there is no indication of it in the list of hosts or ip addresses. iftop -n display formats ipv4 and ipv6 traffic exactly the same, except for the addresses (obviously). If you use iftop without -n, it's not possible to tell the difference between ipv4 and ipv6.

#19 - 01/20/2019 12:09 PM - Joshua Sign

ok,

to debbug it you can check if there is any ip6 in this output :

```
/usr/local/bin/iftop_parser.sh eth0
```

if there is no ipv6 in the output, please check the output of this command line :

```
iftop -nNb -i eth0  -s 1 -o 2s -t
```

You must find ipv6 here, so give me the output for example, the awk script may be wrong.
If there is no ipv6 here, i dont understand why.

#20 - 01/20/2019 03:58 PM - Daryl Morse

Joshua Sign wrote:

> ok,
>
> to debbug it you can check if there is any ip6 in this output :
> [...]
>
> if there is no ipv6 in the output, please check the output of this command line :
> [...]
>
> You must find ipv6 here, so give me the output for example, the awk script may be wrong.
> If there is no ipv6 here, i dont understand why.

My system does not have a device called eth0. It's using hn1 for the wan and hn0 for the lan. I'd say that's part of the problem.

I got permission denied when I tried to run the script from the console shell.

When I executed the iftop command, there was ipv4 and ipv6 output for both hn0 and hn1. Except for the address format, the output is indistinguishable for ipv4 and ipv6. It's a shame there isn't a way to select ipv4 or ipv6 because if it resolves the hostnames, there is no way to tell them apart.

#21 - 01/20/2019 04:01 PM - Daryl Morse

just a thought, if you don't have ipv6, you could set up a tunnel with hurricane electric. It's free, it works very well, and it's easy to set up.

#22 - 01/20/2019 04:53 PM - Joshua Sign

Daryl Morse wrote:

> I got permission denied when I tried to run the script from the console shell.

please check if the script got +x permission,
or give it anyway, type this in console :

```
chmod 755 /usr/local/bin/iftop_parser.sh
```

obiously, eth0 was un axemple,
you have to change it according your system.

in the iftop mode, the informations are grabbed by this command for your WAN card :

```
iftop -nNb -i hn1 -s 1 -o 2s -t
```

and this one for you LAN card :

```
iftop -nNb -i hn0 -s 1 -o 2s -t
```

Does it gives you ipv6 results ?

#23 - 01/20/2019 05:57 PM - Daryl Morse

- File Capture iftop.PNG added

- File Capture iftop hn0.PNG added

- File Capture iftop hn1.PNG added

Joshua Sign wrote:

> Daryl Morse wrote:
>
>> I got permission denied when I tried to run the script from the console shell.
>
> please check if the script got +x permission,
> or give it anyway, type this in console :
> [...]
>
> obiously, eth0 was un axemple,
> you have to change it according your system.
>
> in the iftop mode, the informations are grabbed by this command for your WAN card :
> [...]
>
> and this one for you LAN card :
> [...]
>
> Does it gives you ipv6 results ?

I attached a screen capture of the output of the script. There are some errors.

I already told you the output of iftop shows ipv4 and ipv6 and they are identical except for the addresses. A couple of screen captures attached.

#24 - 01/20/2019 06:02 PM - Daryl Morse

- File iftop status graph.PNG added

Another screen capture from the status graph.

#25 - 01/20/2019 06:48 PM - Joshua Sign

ok,

the first file "File Capture iftop.PNG" show that there is a problem with the awk script.
This script is less than 40 lines and errors are about lines 43,76.

Can you check if this is the same file than this :
https://github.com/pfsense/pfsense/blob/8e73bf65ab51822b438872f13bdf7475ac370365/src/usr/local/bin/iftop_parse.awk

#26 - 01/20/2019 10:34 PM - Daryl Morse

Joshua Sign wrote:

> ok,
>
> the first file "File Capture iftop.PNG" show that there is a problem with the awk script.
> This script is less than 40 lines and errors are about lines 43,76.
>
> Can you check if this is the same file than this :
> https://github.com/pfsense/pfsense/blob/8e73bf65ab51822b438872f13bdf7475ac370365/src/usr/local/bin/iftop_parse.awk

I installed the script using the patch, so it must be the same.

#27 - 01/21/2019 04:12 AM - Joshua Sign

- File iftop_parse.awk.gz added

you are certainly in an issue with bads crlf in the awk script.
please update by this one, i gzip it to avoid any copy/paste problem.

fetch it in your pfsense and use this command line to replace the old one :

```
fetch https://redmine.pfsense.org/attachments/download/2695/iftop_parse.awk.gz
gzcat iftop_parse.awk.gz > /usr/local/bin/iftop_parse.awk
```

#28 - 01/21/2019 09:42 AM - Jim Pingle

With some small modifications, it does work. See my comments on the PR (and future discussion should happen on the PR rather than here)

#29 - 01/21/2019 05:52 PM - Daryl Morse

Jim Pingle wrote:

> The underlying program, rate, still doesn't work with IPv6 as far as I'm aware.
>
> I'd love to see rate swapped out for iftop (which does support IPv6) but the output of iftop isn't easy to parse and it has some issues running on interfaces that are disconnected or have no traffic, which makes it difficult to work with in an automated manner. iftop is also connection-oriented so it doesn't give per-host stats like rate. I have some testing code for it but I'm not terribly happy with how it operates yet. I don't see it replacing rate, but perhaps it might work as an add-on package.

As I mentioned, I emailed the author of rate. He replied this morning and confirmed that he is no longer developing rate. He offered up the source code, if you don't have it already. Let me know if you are interested in the details.

#30 - 01/22/2019 09:24 AM - Jim Pingle

Daryl Morse wrote:

> As I mentioned, I emailed the author of rate. He replied this morning and confirmed that he is no longer developing rate. He offered up the source code, if you don't have it already. Let me know if you are interested in the details.

We already have access to the source code for rate, or it couldn't be compiled into our images. Adapting the GUI to use iftop is almost certainly easier than adapting rate to handle IPv6.

iftop is still being actively developed. If we attempt to adapt rate, then we'd be taking on all the technical debt of maintaining it going forward, on top of the work to make it function now.

Files

bandwidth_by_ip.php	6.31 KB	01/19/2019	Joshua Sign
iftop_parse.awk	986 Bytes	01/19/2019	Joshua Sign
iftop_parser.sh	1.07 KB	01/19/2019	Joshua Sign
pfSense_status_graph.patch	7.95 KB	01/19/2019	Joshua Sign
Capture iftop.PNG	24.1 KB	01/20/2019	Daryl Morse
Capture iftop hn0.PNG	22.9 KB	01/20/2019	Daryl Morse
Capture iftop hn1.PNG	22.9 KB	01/20/2019	Daryl Morse

| iftop status graph.PNG | 77.6 KB | 01/21/2019 | Daryl Morse |
| iftop_parse.awk.gz | 308 Bytes | 01/21/2019 | Joshua Sign |