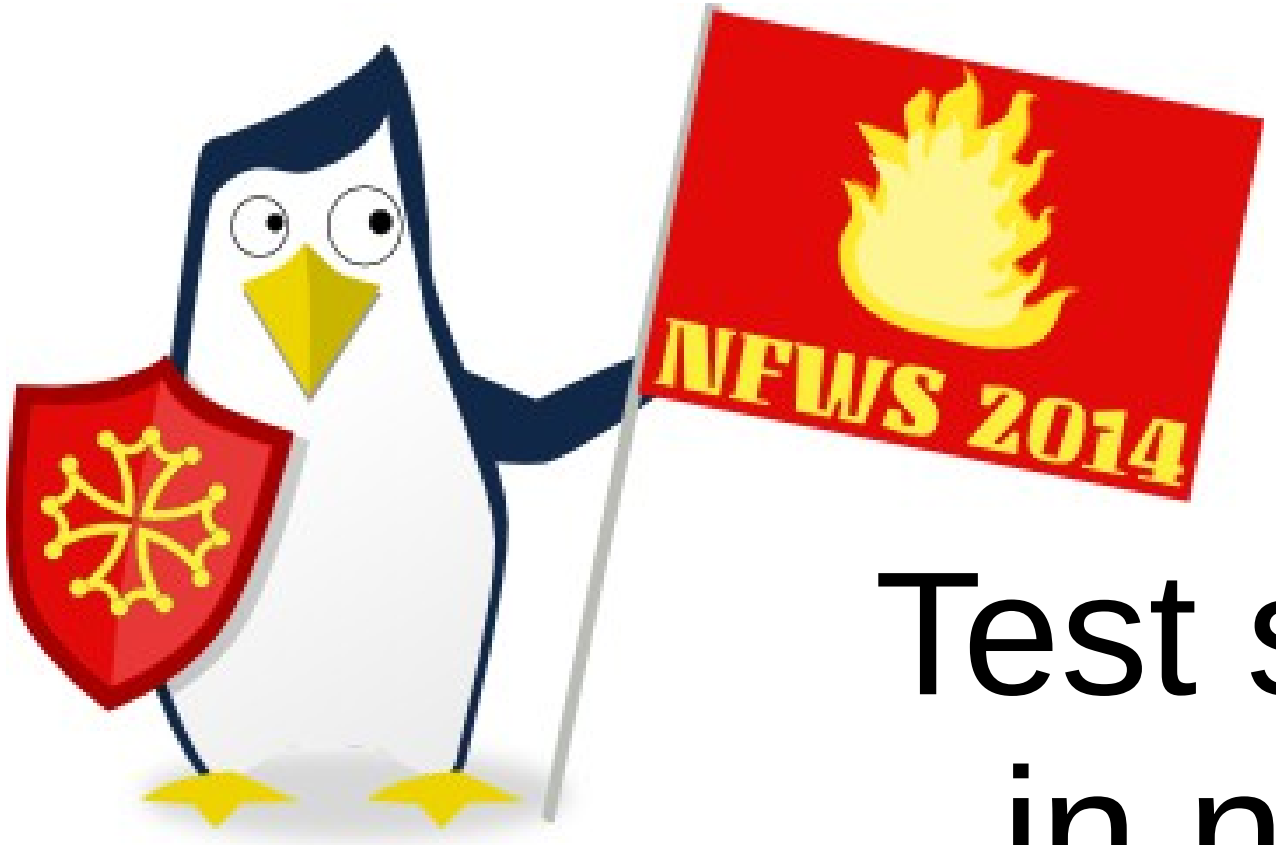


Test system in nftables

Ana Rey (@anaRB)

http://blog.anarey.info

10th Netfilter Workshop
7th-11th July 2014. Montpellier, France

netfilter
firewalling, NAT, and packet mangling for linux

Summary

- Motivation.
- What are we checking?
- Examples:
  - Run all test.
  - Detect errors in the output
  - Run all marked-lines
  - Debug mode
- Nft-test: The tool.
- Test-file structure.
- Workflow.
- In the future.
- In conclusion

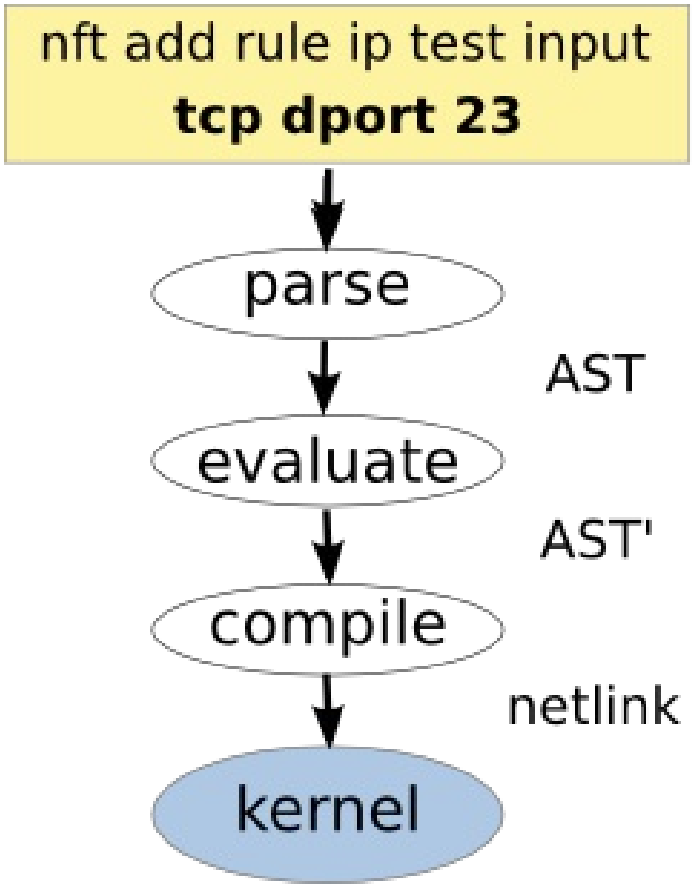
Motivation

- Check nft tool quickly
- Secure the previous development.

What are we checking?

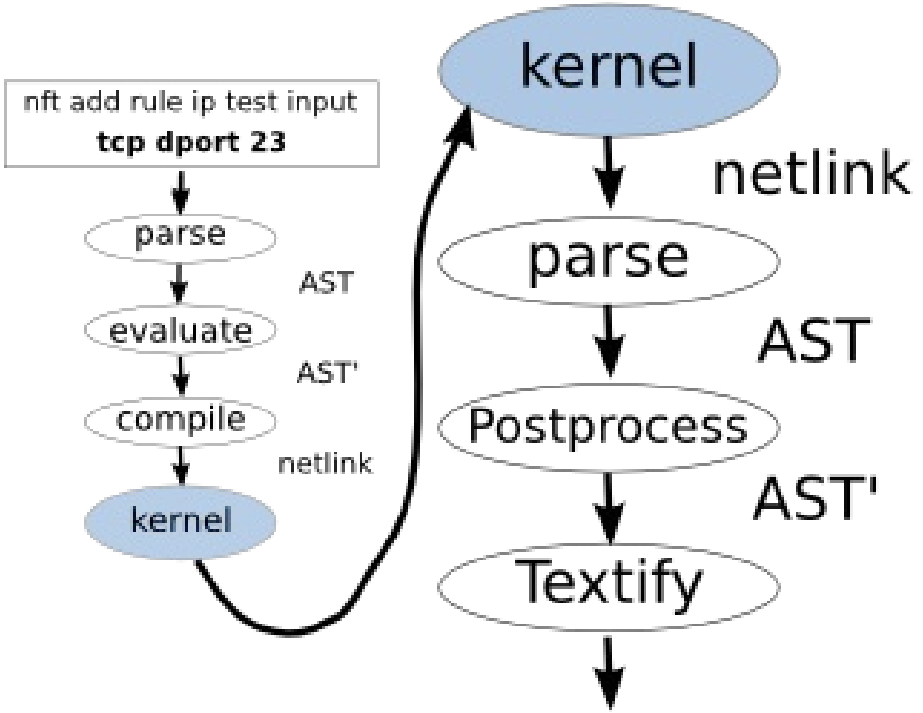
Check inputs

./nft-test.py ipv4/tcp.t



Check inputs and outputs

./nft-test.py -c ipv4/tcp.t




```
table ip test {
        chain input {
                type filter hook input priority 0;
                 tcp dport ssh
        }
}
```

Example: Run all tests:

sudo ./nft-test.py

tests/invert-range-any-alvaro.t: OK

tests/any/frag.t: OK

tests/any/limit.t: OK

any/queue.t: OK

any/ct.t: OK

any/log.t: OK

any/meta.t: OK

tests/invert-range-any.t: ERROR: line 69:
nft add rule ip t-test-ip c-input meta skuid != {101-105} accept:
This rule should not have failed

[…]
42 test files, 1096 unit tests, 1081 passed

Example: Detect errors in the output (1/2)

./nft-test.py **-c**

Rule init: arp operation {nak, inreply, inrequest, rreply}

Rule exit: WARNING: arp operation { 1024, 2048, 2304, 2560 }

Rule init: arp operation != reply
Rule exit: WARNING: arp operation != 512

Rule init: ah spi {111, 122}
Rule exit: WARNING: ah spi { 2046820352, 1862270976 }

Example: Detect errors in the output (2/2)

./nft-test.py **-c**

Rule init: icmpv6 **mtu** {33, 55, 67, 88}
Rule exit: WARNING: icmpv6 **parameter-problem** { 1476395008, 1124073472,
922746880, 5

Rule init: meta iifname {"eth0", "wlan0"}
Rule exit: WARNING: iifname { "", "" }

Rule init: meta priority 33-45
Rule exit: WARNING: meta priority >= 7fea:0033 meta priority <= 4500:ff7f

Rule init: frag frag-off 22 counter
Rule exit: WARNING: counter packets 0 bytes 0 } }
netlink: Error: Relational expression size mismatc

Example: Run all marked-lines

./nft-test.py ipv4/dccp.t **-r**

Rule OK: line 16:dccp dport 21-35

ipv4/dccp.t: ERROR: line 19: nft add rule ip t-ip4 c-input dccp dport != {27, 34}: This rule should not have failed.

Rule fail: line 19: dccp dport != {27, 34}

Ipv4/dccp.t test-file

```
#dccp dport 21-35;ok
dccp dport {23, 24, 25};ok
# dccp dport != {27, 34};ok
```

Example: Debug mode

./nft-test.py **-d** any/queue.t

```
nft add table ip test-t
nft add chain ip test-t output\{ type filter hook output priority 0\; \}
nft add rule ip test-t output queue
nft add rule ip test-t output queue num 2
nft add rule ip test-t output queue num 2-3
nft add rule ip test-t output queue num 4-5 fanout bypass
nft add rule ip test-t output queue num 4-5 fanout
nft add rule ip test-t output queue num 4-5 bypass
nft flush chain ip test-t output
nft delete chain ip test-t output
nft delete table ip test-t
nft list -nn table ip test-t
```

any/queue.t

```
*ip;test-t
:output;type filter
        hook output
        priority 0

queue;ok
queue num 2;ok
queue num 2-3;ok
# queue num {3, 4, 6};ok
queue num 4-5 fanout bypass;ok
queue num 4-5 fanout;ok
queue num 4-5 bypass;ok
```

Example of a test file

tests/ipv4/tcp.t

```
 *ip;test-t
 :c-input;type filter hook input priority 0

tcp dport 22;ok;tcp dport ssh
tcp dport != 233;ok
tcp dport 33-45;ok
tcp dport != 33-45;ok
tcp dport {33, 55, 67, 88};ok
#tcp dport != {33, 55, 67, 88};ok
tcp dport {33-55};ok
#tcp dport != {33-55};ok
tcp dport {telnet, http, https} accept;ok
```

```
*type;table-name

 :chain-name; type

 Rule;state;exit-in-nft

  #marked-line
```

List of current test files

any/

ct.t

frag.t

limit.t

log.t

meta.t

queue.t

Ipv4/
ah.t
chains.t
dccp.t
esp.t
icmp.t
intervals.t
ipcomp.t
ip.t
ip_test.t
nat.t
reject.t
sctp.t
sets.t
tcp.t
udplite.t
udp.t

Ipv6/
ah.t
chains.t
dst.t
hbh.t
icmpv6.t
ip6.t
mh.t
nat.t
reject.t
rt.t
sets.t
vmap.t

Arp/
arp.t
chains.t

Bridge/
Chain.t

Inet/
[...]

Workflow

- Case 1: Before of sending a patch:
  - Check all is correct. => We do not break anything.
  - Example: v1 of “src: add events reporting” patch broke ct state new.
- Case 2: Before of sending a patch for a specific bug/new feature.
  - Check all is correct.
  - Add specific test (or file) for this bug.
  - Examples: “netlink: Allow to invert the ranges” and “queue: More compact syntax”

nft-tests

```
 $ sudo ./nft-test.py --help
usage: nft-test.py [-h] [-v] [-c] [-d] [-r] [path/to/file.t]

Run nft tests

positional arguments:
  path/to/file.t        Run only this test

optional arguments:
  -h, --help            show this help message and exit
  -v, --version         show program's version number and exit
  -c, --check-output    Check the output of nft
  -d, --debug           Debug mode: list all commands that are run
  -r, --run-marked-lines
                        Run all marked-lines in a file or all files
```

nft-tests

- ./nft-test.py Run all test files.
- ./nft-test.py ipv4/ip.t Run this test file.
- ./nft-test.py -d [file.t] Debug mode: List all command-lines that are running.
- ./nft-test.py -c [file.t] Check the output of nft with theses command-lines
- ./nft-test.py -r [file.t] Run marked-lines in the file/s

In the future

- **The matching of packets:** Generate an artifical and specific packet. After, Check that nftable filter correctly them.
- **Generation of code in netlink messages.**
- Add these tests in an automatic tools.

Conclusion

With this nft test system:

- We can check all nft-tool quickly.
- We can check all is correct.
- We discover new bugs that there are in nft or someone adds.
- We want to improve the testing system.

Thank you!

The Outreach Program for Women (OPW) helps women get involved in free and open source software. It provides a supportive community for beginning to contribute any time throughout the year and offer focused internship opportunities twice a year with a number of free software organizations.

https://gnome.org/opw/

Pablo Neira for being my mentor during this intership