BSD Eesti MTÜ

Olev Hannula

PF ehk Packet Filter

Sissejuhatus OpenBSD'st alguse saanud tulemüüritarkvarasse mis on midagi enamat kui lihtsalt tulemüür

Ajalugu

2001. a.
- IPFilter'i litsents
- FreeBSD ja OpenBSD erinevad teed
- IPFW ja PF

2003. a.
- FreeBSD ja NetBSD integratsiooni algus

2005. a.
- Integratsioon lõpusirgel

PF arendamise alused

- Filtreerivad reeglid
- Olekutabel (State table)
- NAT
- Normaliseerimine
- TCP sequence numbri genereerimine
- Logimine
- Reeglite optimiseerimine rakenduse poolt

Lisaks ...

- ALTQ
- pfsync
- carp
- ... arendus käib edasi

pfctl

- pfctl -e
- pfctl -d
- pfctl -f failinimi
- pfctl -nf failinimi
- pfctl -sa
- pfctl -vsa

Kõik ühes kohas!

Üldine pf.conf failistruktuur:

- Makrod
- Tabelid
- Valikud (options)
- Normaliseerimine
- Järjekorrad (ALTQ)
- Transleerimine (NAT)
- Filtrid

Makrod

```
ext_if=”pppoe0”
int_if=”pcn0”
t2htis_masin=”192.168.0.20”
s6brad=”{ 192.168.0.2, 192.168.0.3 }”

esimene=”192.168.0.2”
teine=”192.168.0.3”
m6lemad=”{“ $esimene $teine “}”

teenused=”{ ssh, smtp, http }”
```

Tabelid

table <ssh_hosts> { 123.124.125.126, 210.211.212.23/28 }

table <lubatud> { 192.168.0.0/16, !192.168.0.22 }

table <t2htsad> const { 192.168.0.10, 192.168.0.11 }

table <sp2mm> persist file “/etc/sp2mmijad”

Hilljem käsurealt:
pftcl -t ssh_hosts -T add 121.231.187.111
pfctl -t ssh_hosts -T show
pfctl -t ssh_hosts -T delete 123.124.125.126
pfctl -t ssh_hosts -vTs

Valikud (options)

set block-policy return

set limit states 10000

set optimization high-latency

Normaliseerimine

scrub in all

scrub out on $ext_if

scrub out on $ext_if max-mms 1440

scrub out on $ext_if max-mms 1440 random-id

Järjekorrad (ALTQ)

- Class based Queueing
- Priority Queueing

```
altq on $ext_if cbq bandwidth 1Mb queue { std, ssh, ftp }
queue std bandwidth 80% cbq(default)
queue ssh bandwidth 10% priority 3 cbq(red)
queue ftp bandwidth 10% priority 2 cbq(borrow red)

altq on $ext_if priq bandwidth 1Mb queue { std, ssh, ftp }
queue std priq(default)
queue ftp priority 2 priq(red)
queue ssh priority 3 priq(red)
```

Transleerimine (NAT)

```
nat on $ext_if from 192.168.0.1/24 to any -> $ext_if

nat on $ext_if from $int_if:network to any -> $ext_if

no nat on $ext_if from 192.168.0.32 to any

nat on $ext_if from !($ext_if) to any -> ($ext_if:0)

rdr on $ext_if proto tcp from any to any port 80 -> 192.168.0.10 port 81

rdr on $ext_if proto tcp from 213.12.32.92 to any port 80 -> 192.168.0.20

rdr on $ext_if proto tcp from any to ($ext_if) port 6891:6899 -> $lauamasin

rdr on $ext_if proto tcp from any to any port 80 -> \
{ 192.168.0.1, 192.168.0.3, 192.168.0.4 } round-robin sticky-address
```

Filtrid

```
block all
pass all

block in on $ext_if all
block out on $ext_if proto udp all

pass out on $ext_if proto tcp from ($ext_if) to any

pass out on $ext_if proto tcp from ($ext_if) to any port 80

pass out on $ext_if proto tcp from any port > 1024 to any port 80

pass out on $ext_if proto tcp from ($ext_if) to any port > 49151

pass out on $ext_if proto tcp from ($ext_if) to any port http keep state

pass in proto tcp from any to any port www synproxy state
```

Filtrid edasi

pass out on $ext_if from any to any port 22 queue ssh
pass out on $ext_if from any to any port > 22 queue std

pass out on $ext if from any to any port 22 queue (ssh, ackid)

flags S/S ehk SYN'ist SYN peab olema
flags S/SA ehk SYN ja ACK'ist SYN peab olema, näiteks lähevad sellest läbi SYN, SYN+RST ja SYN+PSH, aga SYN+ACK ja niisama ACK ei lähe.

Näide:
block all
pass out proto tcp from any to any flags S/SA keep state
pass in on proto tcp from any to any port 113 flags S/SA keep state

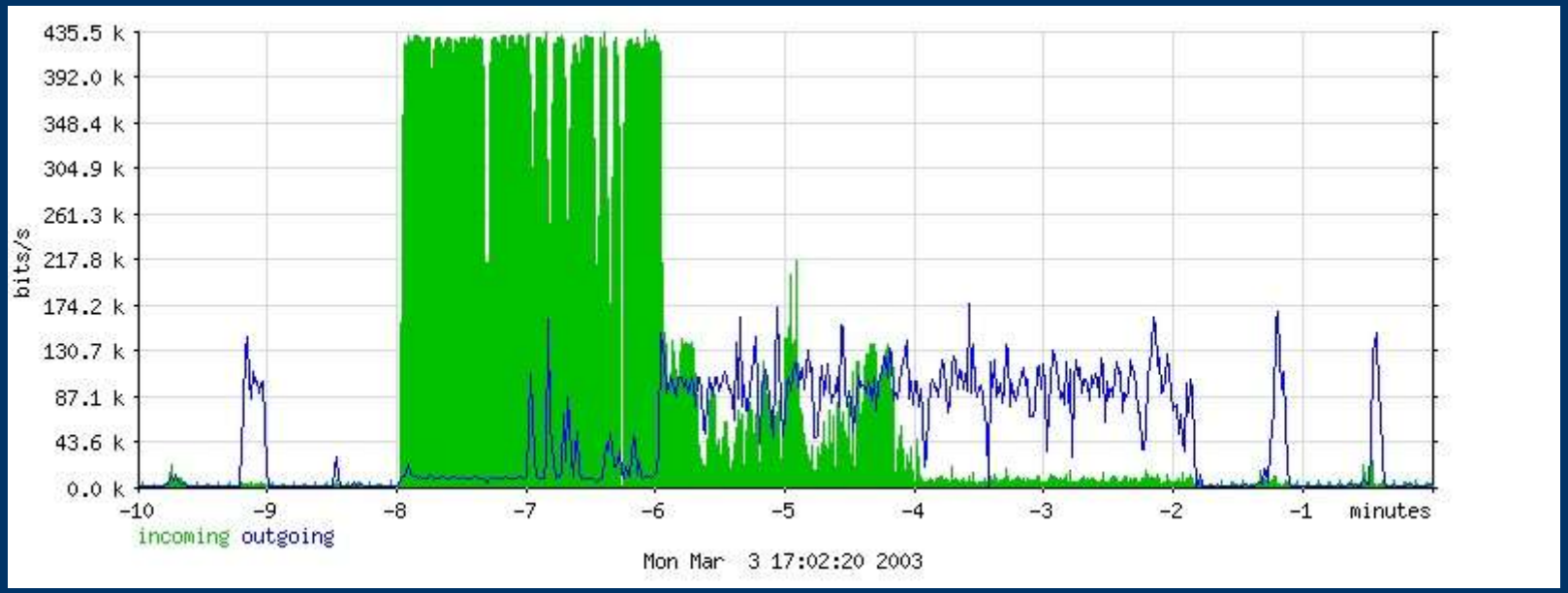
ALTQ näide

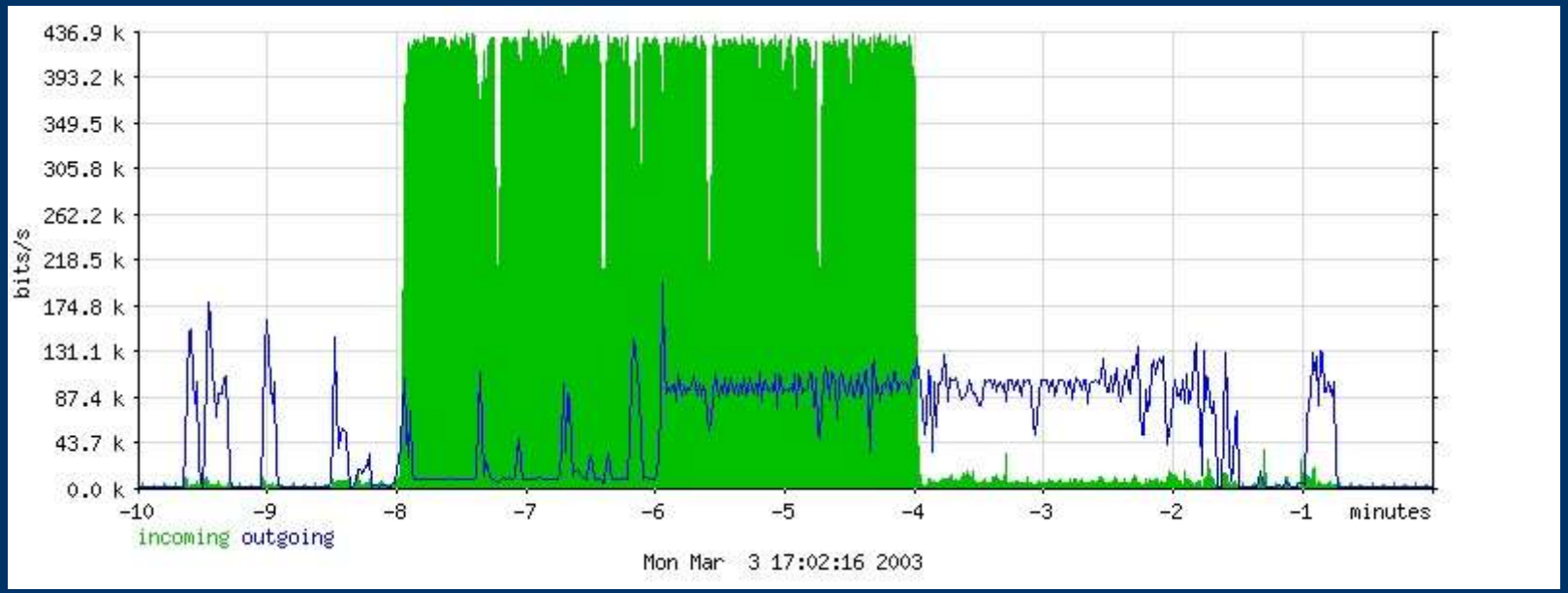
```
ext_if=”pppoe0”

altq on $ext_if priq bandwidth 200Kb queue { pri, def }
queue pri priority 7
queue def priority 1 priq(default)

pass out on $ext_if proto tcp from $ext_if to any \
flags S/SA keep state queue (def, pri)

pass in on $ext_if proto tcp from any to $ext_if \
flags S/SA keep state queue (def, pri)
```


435.5 k
392.0 k
348.4 k
304.9 k
261.3 k
217.8 k
174.2 k
130.7 k
87.1 k
43.6 k
0.0 k
bits/s
-10
-9
-8
-7
-6
-5
-4
-3
-2
-1
minutes
incoming
outgoing
Mon Mar 3 17:02:20 2003


436.9 k
393.2 k
349.5 k
305.8 k
262.2 k
218.5 k
174.8 k
131.1 k
87.4 k
43.7 k
0.0 k
bits/s
-10
-9
-8
-7
-6
-5
-4
-3
-2
-1
minutes
incoming
outgoing
Mon Mar 3 17:02:16 2003

ja veel ...

```
block in on $ext_if from any os “Linux 2.4”

block in on $ext_if proto tcp from any os “Windows 2000” \
    to any port = 25

pass in on $int_if route-to \
{ ($ext_if1 $ext_gw1), ($ext_if2 $ext_gw2) } round-robin \
from $lan_net to any keep state
```

Ning see oli alles jäämäe tipp

Edasiseks lugemiseks:

http://www.openbsd.org/faq/pf/index.html

man pf
man pfctl
man pf.conf