2nd Linuxwochenende meeting
Vienna 24./25. Oktober 2009
www.luga.at

Building redundant pair of firewals using OpenBSD and CARP

Elvir Kurić

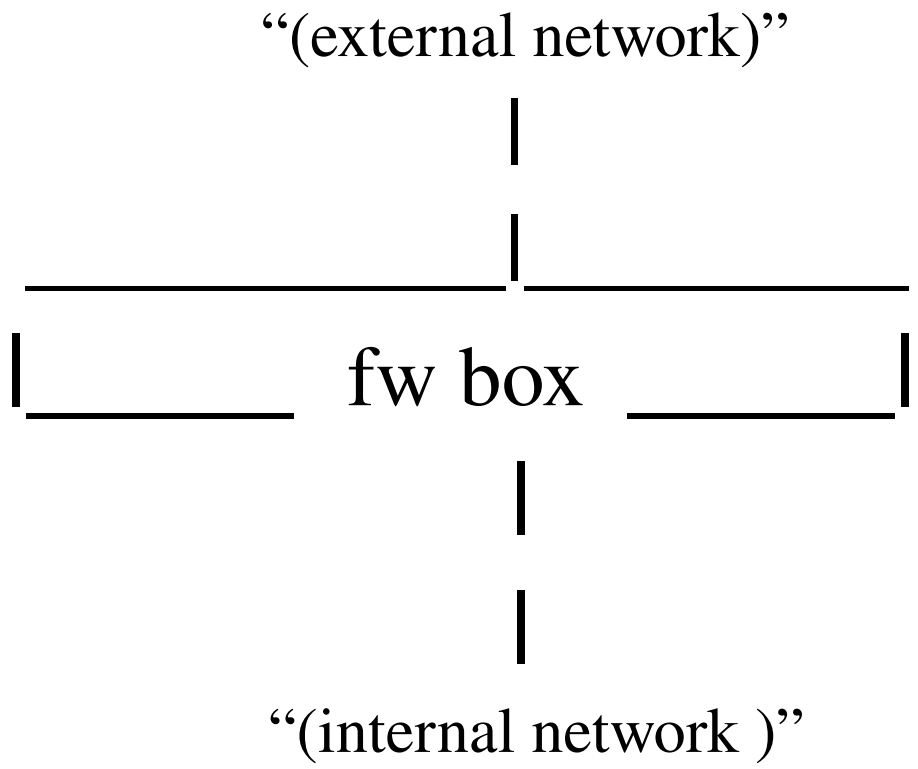
Short about me ...

- Degree in Telecommunications
- Worked for BH Telecom
- Working for HP
- Use linux/unix for job and fun
- In free time I read stuff related to linux/unix, travel, learn foreign languages (en/cz.../de/ru)...

Firewalls

- Are very (most) important network components
- If compromised/have some HW issue, all users will “hang” waiting on problem resolution
- Mostly firewalls are not built in redundancy pairs
- Very expensive commercial solution (redundancy increases additionally costs)
- Setting up “in house” firewall has its own pros. and cons.

In most cases we have situation like this



OpenBSD

- OS by default proactive oriented toward security
- Not very “popular” OS due to its “unfriendly” installation process
- Do not forget that security of an application is directly proportional to skills of administrator/programer who take care about it
- My favorite server OS system

PF

- PF is OpenBSD firewall tool
- Ported to FreeBSD/NetBSD
- Developed by Daniel Hartmeier
  http://www.benzedrine.cx/dhartmei.html

Pfsync

pfsync - packet filter state table logging interface

- protocol number 240 (not official)
- broadcast address used is 224.0.0.240 (by default)
- syncpeer (the syncpeer address is used as dest. for pfsync traffic)
- crossover cable/syncpeer address/ipsec

CARP
(Common Address Redundancy Protocol)

- Protocol number 112 (not official)
- Multiple host can share same ip address
- CARP is patent free replacement for VRRP (Virtual router redundancy protocol) and HSRP (Hot swap redundancy protocol), or some other protocol

CARP
(Common Address Redundancy Protocol)

- Virtual ip and MAC address (00-00-5e-00-01-xx)
- Supports Ipv4/IPv6
- Author is Rayan McBirde
- Linux port exist as well
  http://www.ucarp.org/project/ucarp

Setup

- Default OpenBSD installation include CARP and PF and Pfsync ... no need to install additional ports
- Recommended is to read about default features for PF
- Necessary to enable CARP in /etc files

/etc/rc.conf.local

- PF=yes
- pf_rules=/etc/pf.conf
- pflogd_flags=" "

/etc/sysctl.conf

- net.inet.carp.allow=1
- net.inet.carp.preempt=1
- net.inet.carp.log=1

/etc/sysctl.conf --to enable forwarding

- Machine will serve as router/gateway so necessary to enable forwarding
- net.inet.ip.forwarding=1
- #net.inet.ip.forwarding=1 (for IPv6)

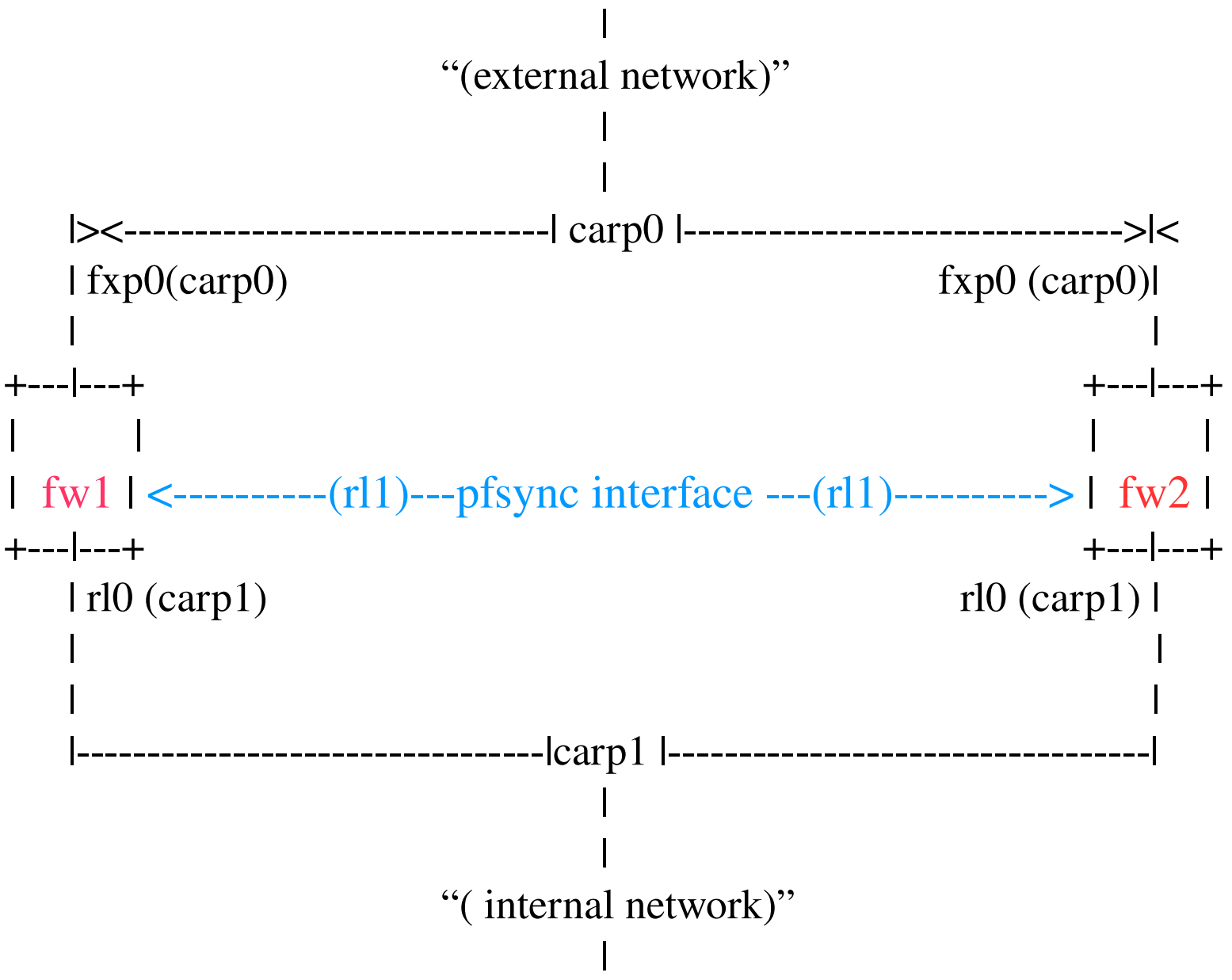
Carp virtual interface

- ifconfig carpX create (X carp id)
- Longer list of parameters as bellow
- Ifconfig carpX [advbase *n*] [advskew *n*] [carpdev *iface*] [carppeer *peer_address*] [pass *password*] [state *state*] [vhid *host-id*]

Carp virtual interface

- advbase (how often advertisements are sent out- *hello*)
- advskew (optional parameter, 0<=advskew<=255, default value is 0)
- carpdev *iface*
- pass *PaSSword*
- state *state* (master or backup)
- vhid *vhid-id*

Network layout



Network interfaces /etc/hostname.*

- fw1
  - fxp0
  - rl0
  - rl1
  - pfsync0
  - carp0
  - carp1
- fw1
  - fxp0
  - Rl0
  - rl1
  - pfsync0
  - carp0
  - carp1

OpenBSD has different network interfaces naming convention based on driver used by NIC (vendor)

fw1 configuration (cat /etc/hostnames.*)

- fxp0 (up)
- rl0 (inet 192.168.1.10 255.255.255.0 NONE)
- rl1 (inet 10.10.10.10 255.255.255.0 NONE)
- pfsync0 (up syncdev rl1 syncpeer 10.10.10.20)

fw1 configuration (cat /etc/hostnames.*) (cont.)

- carp0 (inet 11.22.33.44 255.255.255.224 11.22.33.63 vhid 1 pass PASS_IS carpdev fxp0 advbase 10 advskew 0 state master)
- carp1 (inet 192.168.1.21 255.255.255.0 192.168.1.255 vhid 2 pass PASS_IS carpdev rl0 advbase 10 advskew 0 state master)
  - *window* = advbase + (advskew/256)=10sec (advertisement about state will be sent out every 10sec)

fw2 configuration (cat /etc/hostnames.*)

- fxp0 (up)
- rl0 (inet 192.168.1.20 255.255.255.0 NONE
- rl1 (inet 10.10.10.20 255.255.255.0 NONE)
- pfsync0 (up syncdev rl1 syncpeer 10.10.10.10)

fw2 configuration (cat /etc/hostnames.*) (cont.)

- carp0 (inet 11.22.33.44 255.255.255.224 11.22.33.63 vhid 1 pass PASS_IS carpdev fxp0 advbase 10 advskew 0 state backup)
- carp1 (inet 192.168.1.21 255.255.255.0 192.168.1.255 vhid 2 pass PASS_IS carpdev rl0 advbase 10 advskew 0 state backup)

Pfsync network interface

- ifconfig pfsyncN syncdev iface [syncpeer peer_ip]
  - syncdev –name of physical interface over which sync updates will be send/received (rl1 in our case)
  - syncpeer (optional parameter to lock down sync updates to particular ip address)

ifconfig carp1

- carp1: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> mtu 1500 lladdr 00:00:5e:00:01:01 priority: carp: MASTER carpdev rl0 vhid 2 advbase 10 advskew 0 groups: carp inet6 fe80::200:5eff:fe00:102%carp2 prefixlen 64 scopeid 0x7 inet 192.168.1.21 netmask 0xffffff00 broadcast 192.168.1.255

- 00-00-5e-00-01-xx

pf.conf configuration

```
# Minimal working configuration for PF

ext_if="fxp0"
int_if="rl0"
carp_ext="carp1"
carp_int="carp2"
sync_if="rl1"

tcp_services="{22,25,80}"

table<box> persist
table <box> file "/etc/box"
```

pf.conf configuration (cont.)

```
set block-policy drop
set loginterface $ext_if
set skip on lo


scrub in

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

block in all
block quick from <box>
pass out keep state
```

pf.conf configuration (cont.)

pass quick on $sync_if proto pfsync keep state (no-sync)

pass on {$ext_if $int_if $carp_ext $carp_int } proto carp keep state (no-sync)

pass in on $ext_if inet proto tcp from any to $carp_ext port $tcp_services flags S/SA keep state (max-src-conn 2, max-src-conn-rate 1/30, overload <box> flush global)

pass in on $int_if inet proto icmp all icmp-type $icmp_types keep state
pass in quick on $int_if
pass in quick on $sync_if
pass in quick on $carp_int

Testing

- carpdemote feature
- ifconfig -g carpdemote
- ifconfig -g carp (-)carpdemote value
- ifconfig fxp0 down, or shutdown master/slave

- tcpdump -i fxp0
- man tcpdump

Interesting to read ...

- http://www.countersiege.com/doc/ifstated/
- http://www.openbsd.org/cgi-bin/man.cgi?query=ifstated

Resources

- www.openbsd.org
- Building firewalls with OpenBSD and PF, 2nd Edition -- (Jacek Artymiak)
- Absolute OpenBSD (Michael Lucas)
- http://www.linux-ha.org/

Q/A

Thank you

elvirkuric@gmail.com
elvir.kuric@hp.com