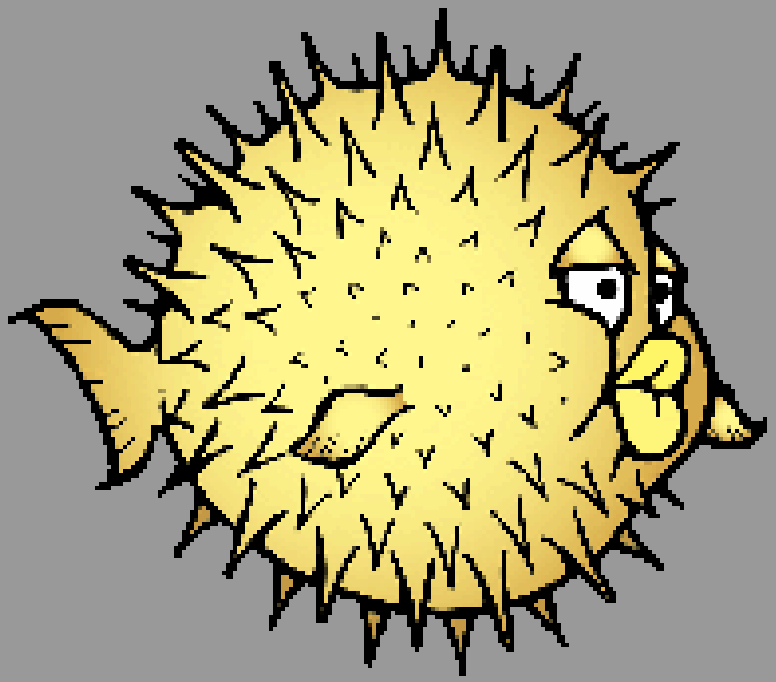
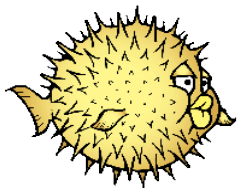
OpenBSD Firewall Cluster



by Lucy

What is this all about?

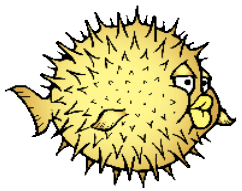
- OpenBSD Security
- History
- Cluster
- CARP Protocol
- Failover Configuration
- Loadbalancing Configuration
- Pfsync
- PF Rule Set
- Lessons learnt



OpenBSD

OpenBSD Security

- Memory Protection
- Cryptography
- Address Space Layout Randomization
- Security Levels
- Privileges separation and revocation
- Sandboxing (chroot)
- Security Code Audit
- ICMP redirect prevention (since 5.0)
- Patches for Security Problems
- X11 restrictions



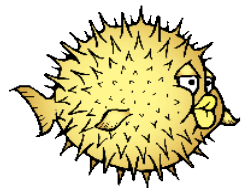
OpenBSD

History

- HSRP (Hot Standby Router Protocol)
- VRRP (Virtual Router Redundancy Protocol)

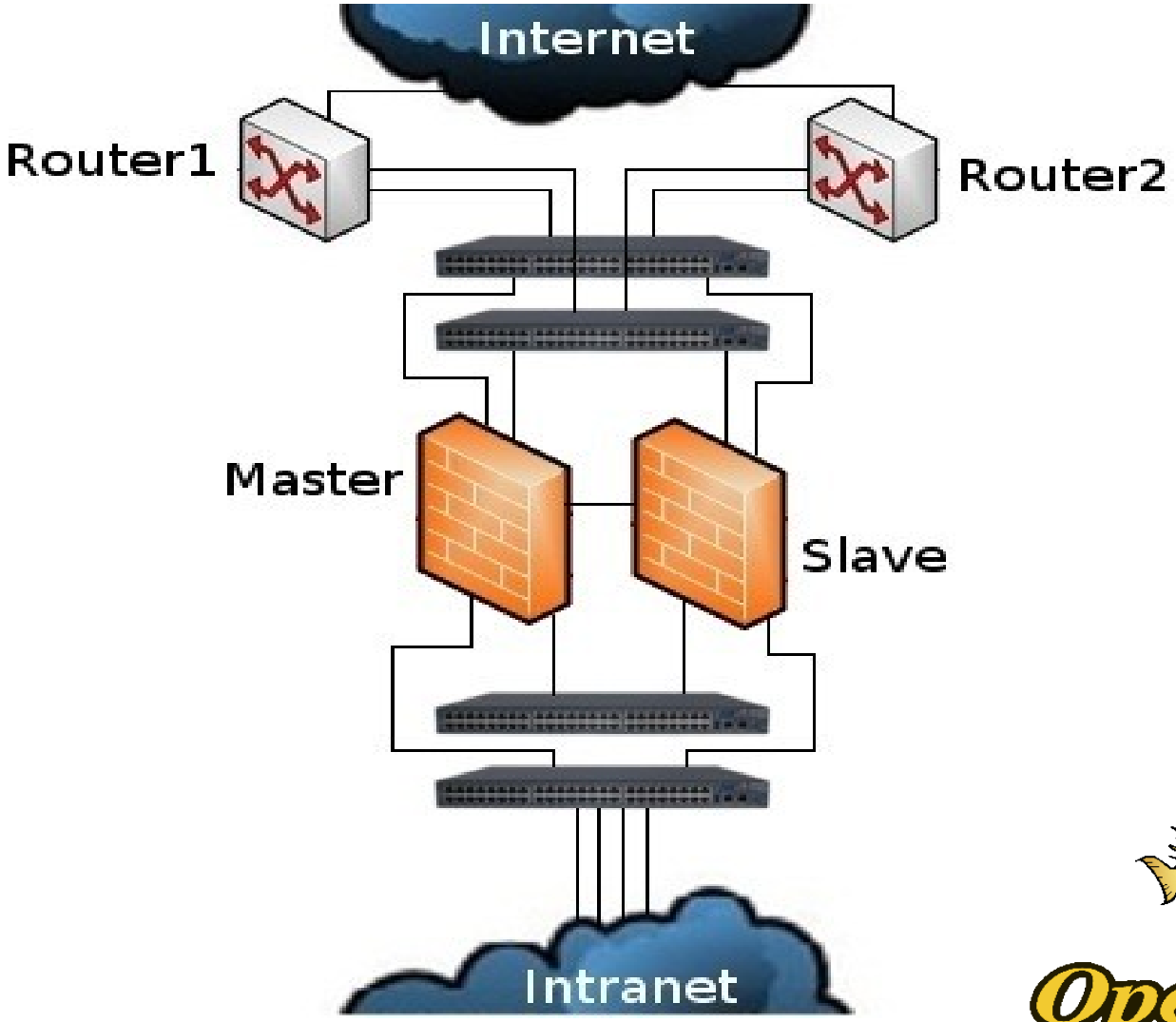
→ CARP (Common Address Resolution Protocol)

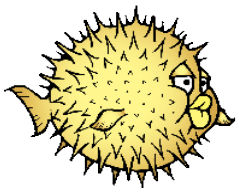
Michael Shalayeff, Ryan McBride & Gleb Smirnoff



OpenBSD

Firewall Cluster





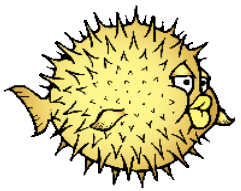
OpenBSD

Activate CARP

sysctl & /etc/sysctl.conf

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

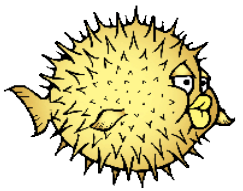
net.inet.carp.log= 1



OpenBSD

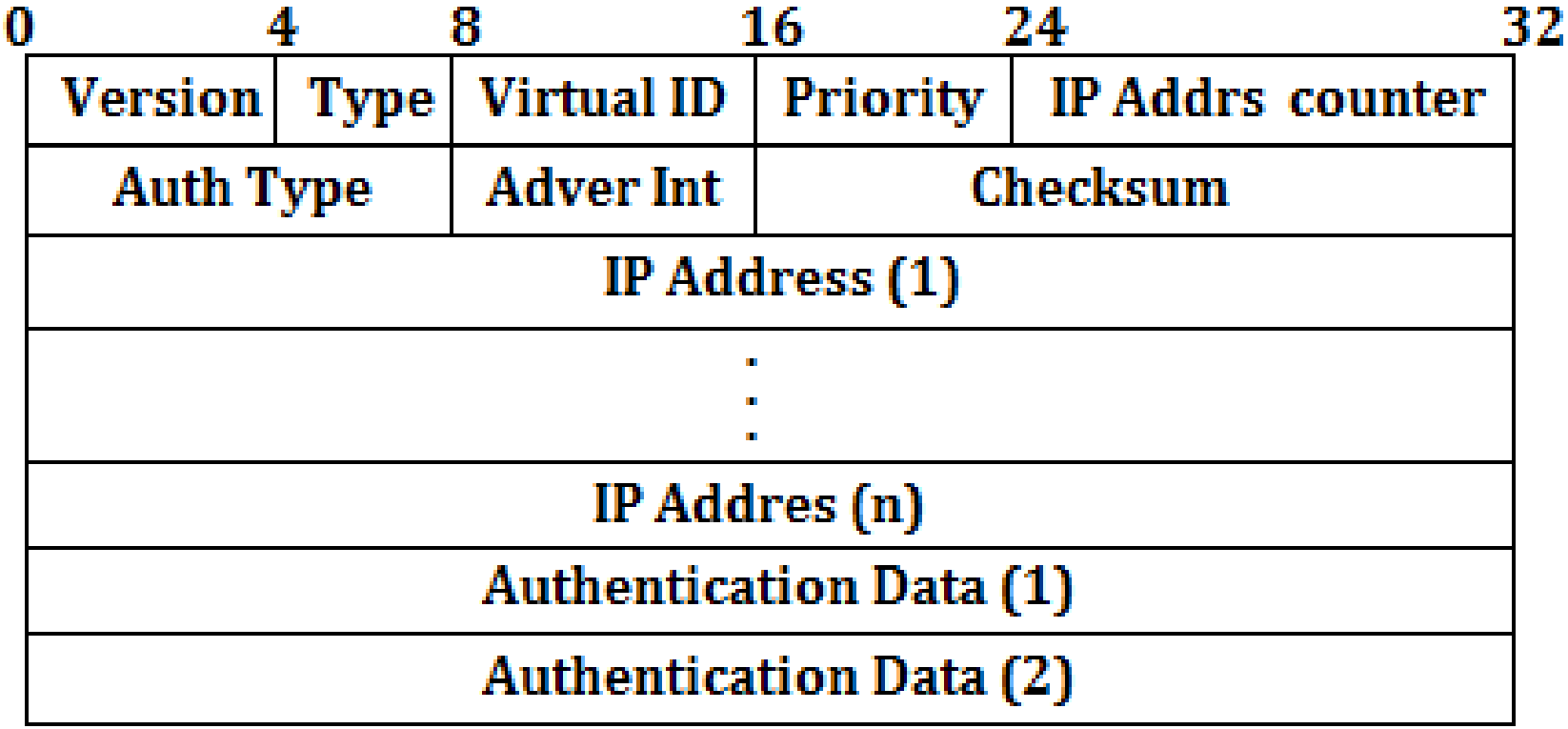
CARP Protocol

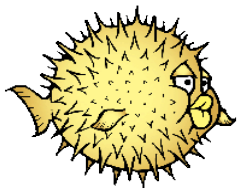
- ICANN Protocol Number 112
- Multicast Protocol
- IP 224.0.0.18
- TTL 255
- VHID (Virtual Host ID)
- not encrypted
- without password no authentification
- RFC 3768 (VRRP)



OpenBSD

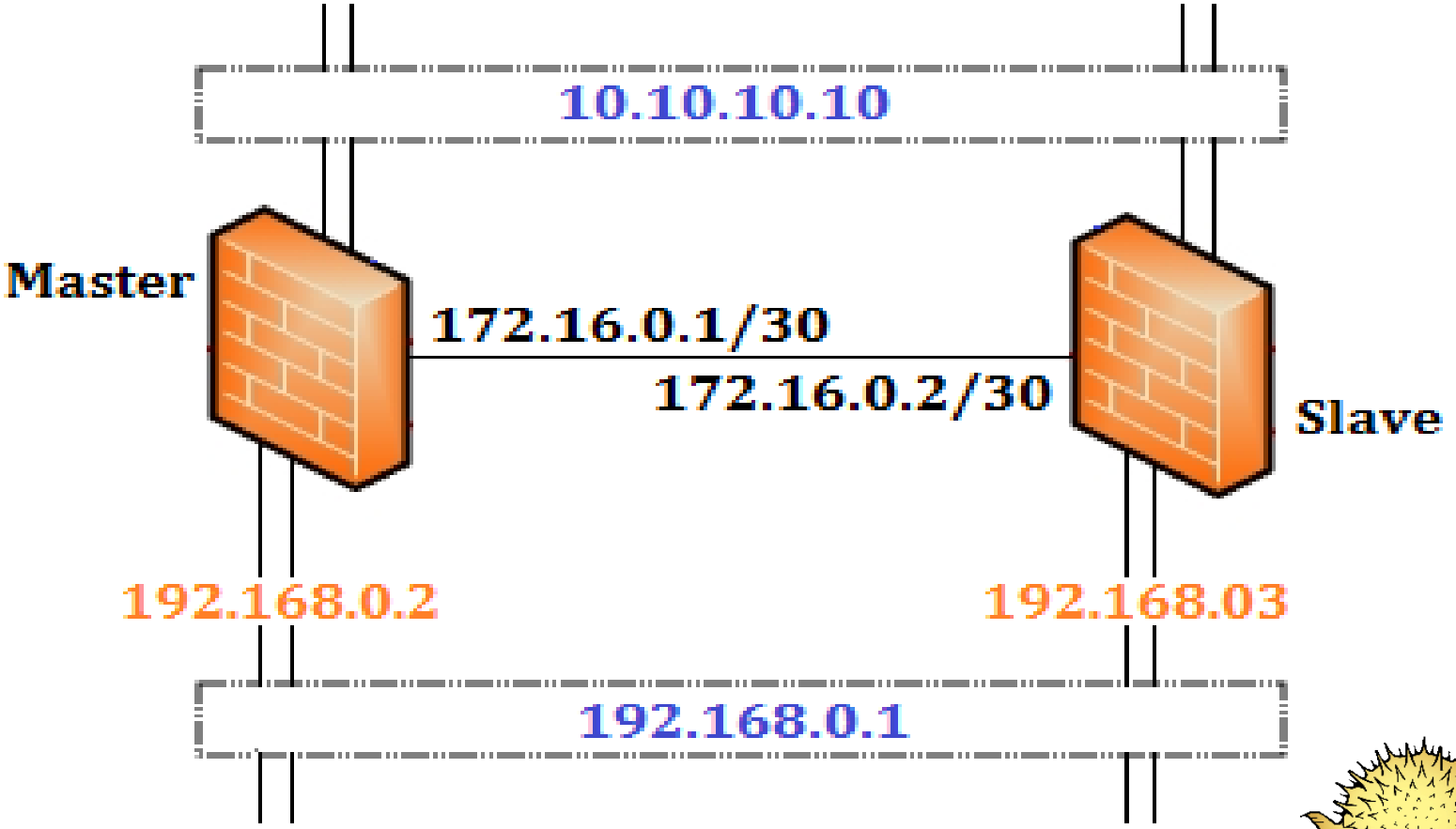
Carp Protocol Header

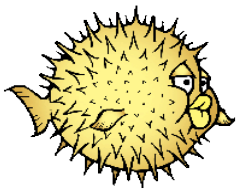




OpenBSD

Failover Cluster





OpenBSD

Interface Configuration

zile /etc/hostname.em[1-4]

up description **trunk interface**

zile /etc/hostname.trunk1

up trunkproto lacp

trunkport em1 trunkport em2

description **external trunk**

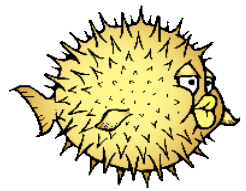
zile /etc/hostname.trunk2

192.168.0.2/24 trunkproto lacp

Trunkport em3 trunkport em4

description **internal trunk**

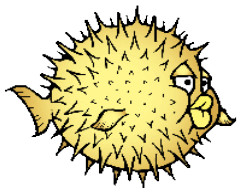
/etc/netstart



OpenBSD

CARP Options

- IP & netmask
- vhid <host id>
- advbase <n> (default 1)
- advkew <n> (default 0)
- pass <password>
- group <groupname> (default carp)
- carpdev <device>
- carppeer <peer_address>
- state <state>



OpenBSD

Failover Configuration

 # Master

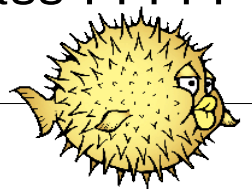
10.10.10.1/24 vhid 2 advskew **20** carpdev trunk1 pass ppppp
description external carp master

192.168.0.1/24 vhid 1 advskew **20** carpdev trunk2 pass PPPPP
description internal carp master

 # Slave

10.10.10.1/24 vhid 2 advskew **120** carpdev trunk1 pass ppppp
description external carp backup

192.168.0.1/24 vhid 1 advskew **120** carpdev trunk2 pass PPPPP
description internal carp backup

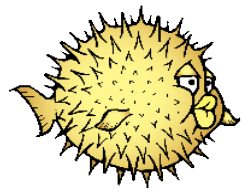


OpenBSD

CARP demote counter

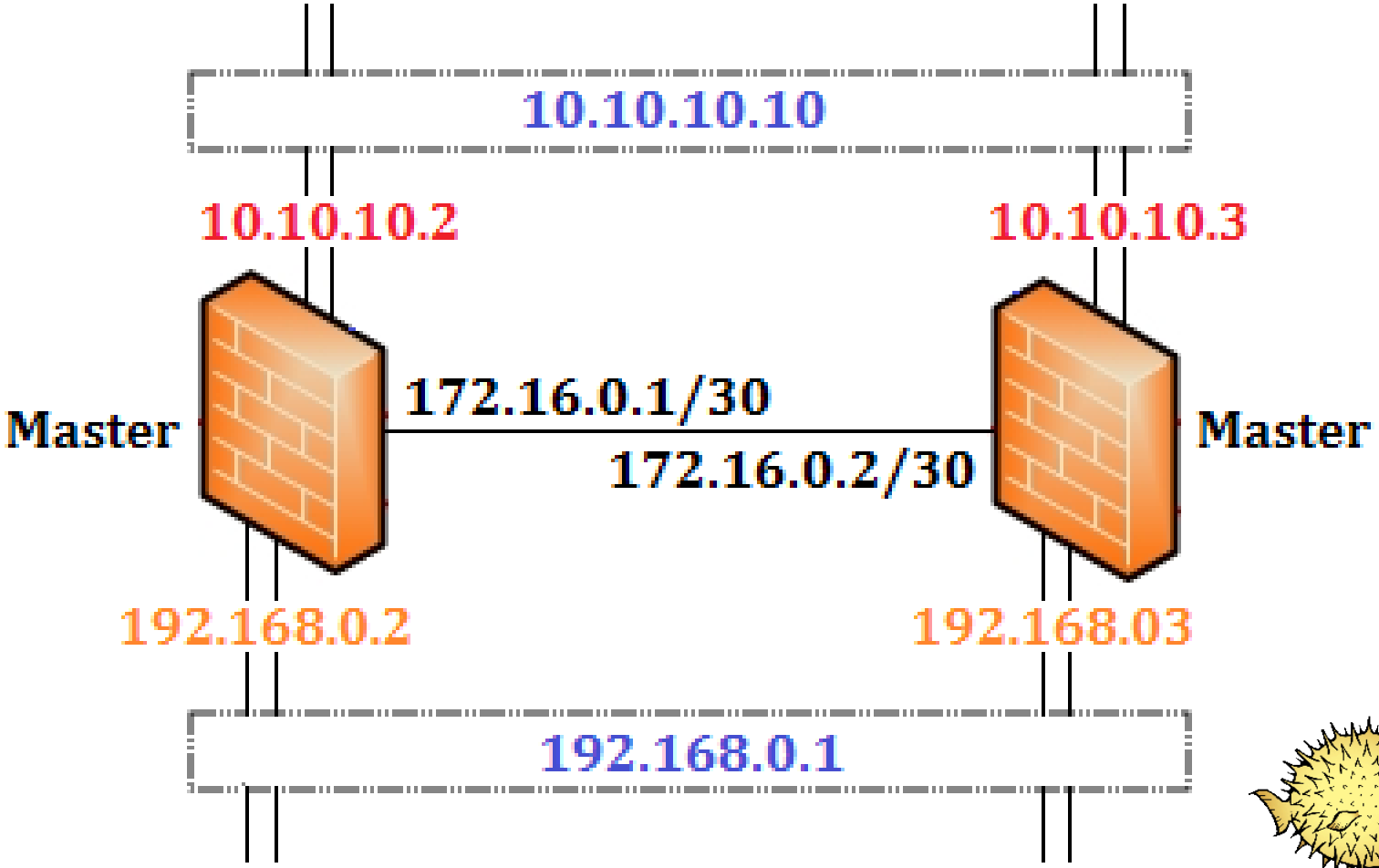
Show and set the carp group counter

ifconfig -g carp
ifconfig -g carp carpdemote 20
ifconfig -g carp -carpdemote 20



OpenBSD

Loadbalancing Cluster



OpenBSD

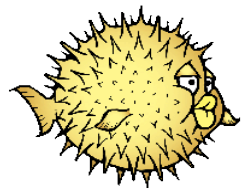
Interface Configuration

zile /etc/hostname.em[1-4]
up description **trunk interface**

zile /etc/hostname.trunk1
10.10.10.2 up trunkproto lacp
trunkport em1 trunkport em2
description **external trunk**

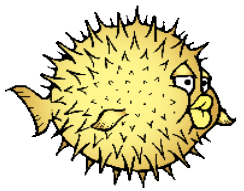
zile /etc/hostname.trunk2
192.168.0.2/24 trunkproto lacp
Trunkport em3 trunkport em4
description **internal trunk**

/etc/netstart



CARP Options

- IP & netmask
- vhid <host id>
- pass <password>
- group <groupname> (default carp)
- carpnodes <vhid:advkew, vhid:advkew>
- carpdev <device>
- carppeer <peer_address>
- state <state>



OpenBSD

Loadbalancing Configuration

 # Master 1

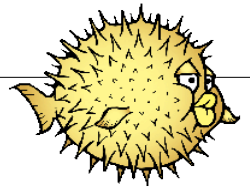
10.10.10.1/24 **balancing** carpdev trunk1 carpnodes **1:100,2:0**
description external carp master1

192.168.0.1/24 **balancing** carpdev trunk2 carpnodes **3:100,4:0**
description internal carp master2

 # Master2

10.10.10.1/24 **balancing** carpdev trunk1 carpnodes **1:0,2:100**
description external carp master2

192.168.0.1/24 **balancing** carpdev trunk2 carpnodes **3:0,4:100**
description internal carp master2



OpenBSD

PFsync

TCP State synchronisation

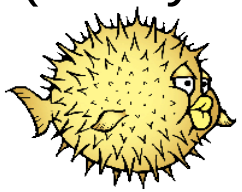
pfsync syncpeer 172.16.0.2 syncdev bnx0

sysat states

no authorisation no encryption

PF Ruleset

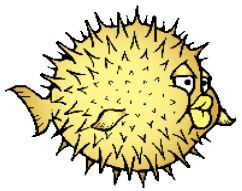
```
syncif= vr0
extif= vr1
intif= vr2


#  CARP rule
pass quick log on { $extif, $intif}  proto carp
#  PFSYNC rule
pass quick log on $syncif proto pfsync
#  SSH from internal rule
pass quick log on $intif to self proto ssh keep state (no-sync)
```



OpenBSD

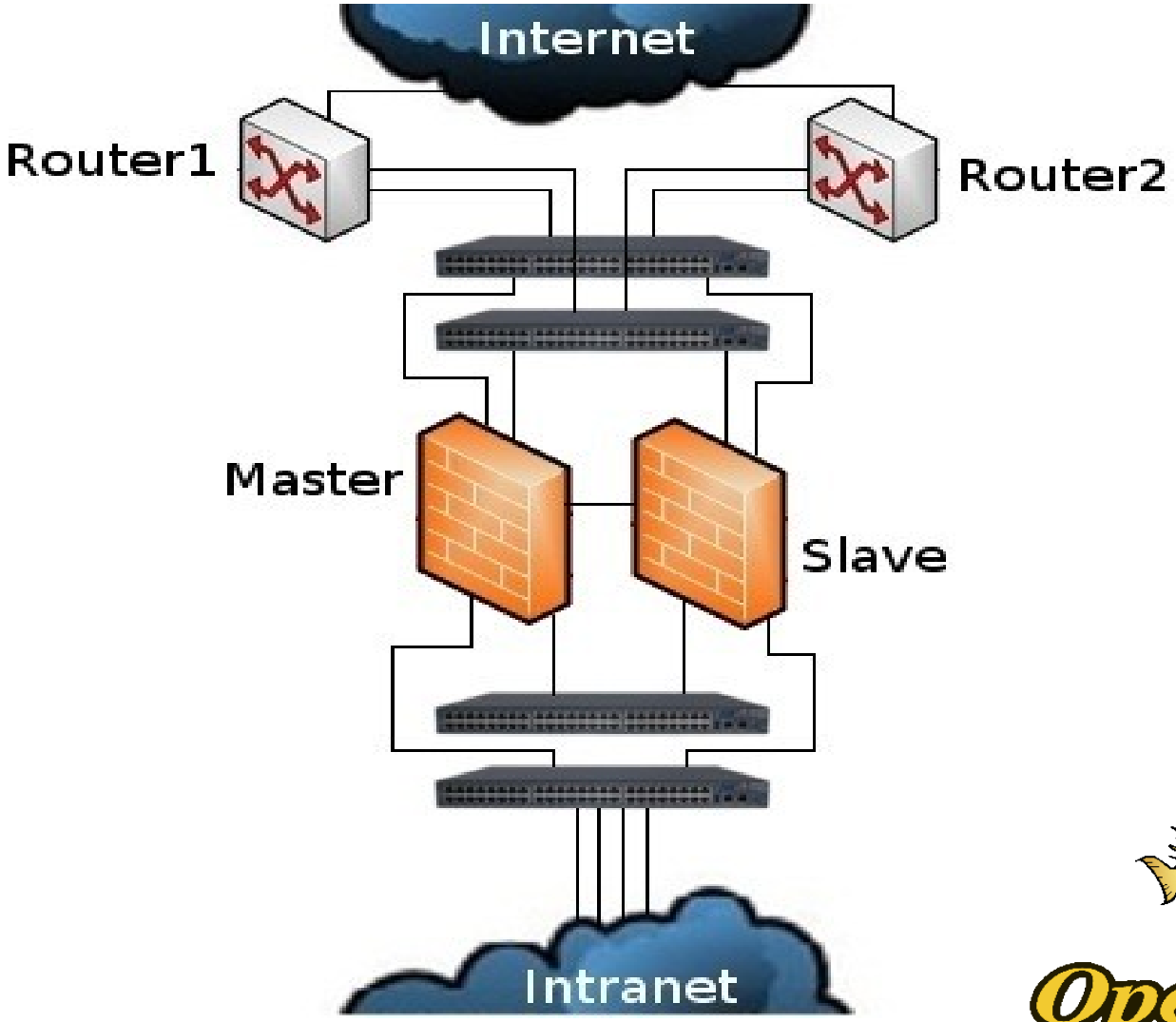
Lessons learnt

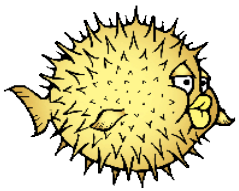
- Pros
  - Failover / Loadbalancing
  - OpenBSD Security Features
  - PF Features
  - Update tests
- Con
  - Synchronisation
  - Single Point of Failure
  - without password no authentification
  - No encryption



OpenBSD

Fragen?





OpenBSD

Referenzen

- The Book of PF
- Openbsd.org/faq
- networksorcery.com
- datenterrorist.de/cgi-bin/wiki.pl/PF_(OpenBSD)