

OpenBSD and Linux: Insights into a migration project at ETH

Stephan A. Rickauer

StarTek – secure by design
and

Institute of Neuroinformatics
ETH / University Zurich

OpenExpo '07, Zurich

Introduction

The IT Infrastructure at INI

Problems with INI's Linux Setups

The Migration to OpenBSD

The Outcome / Summary

Conclusion

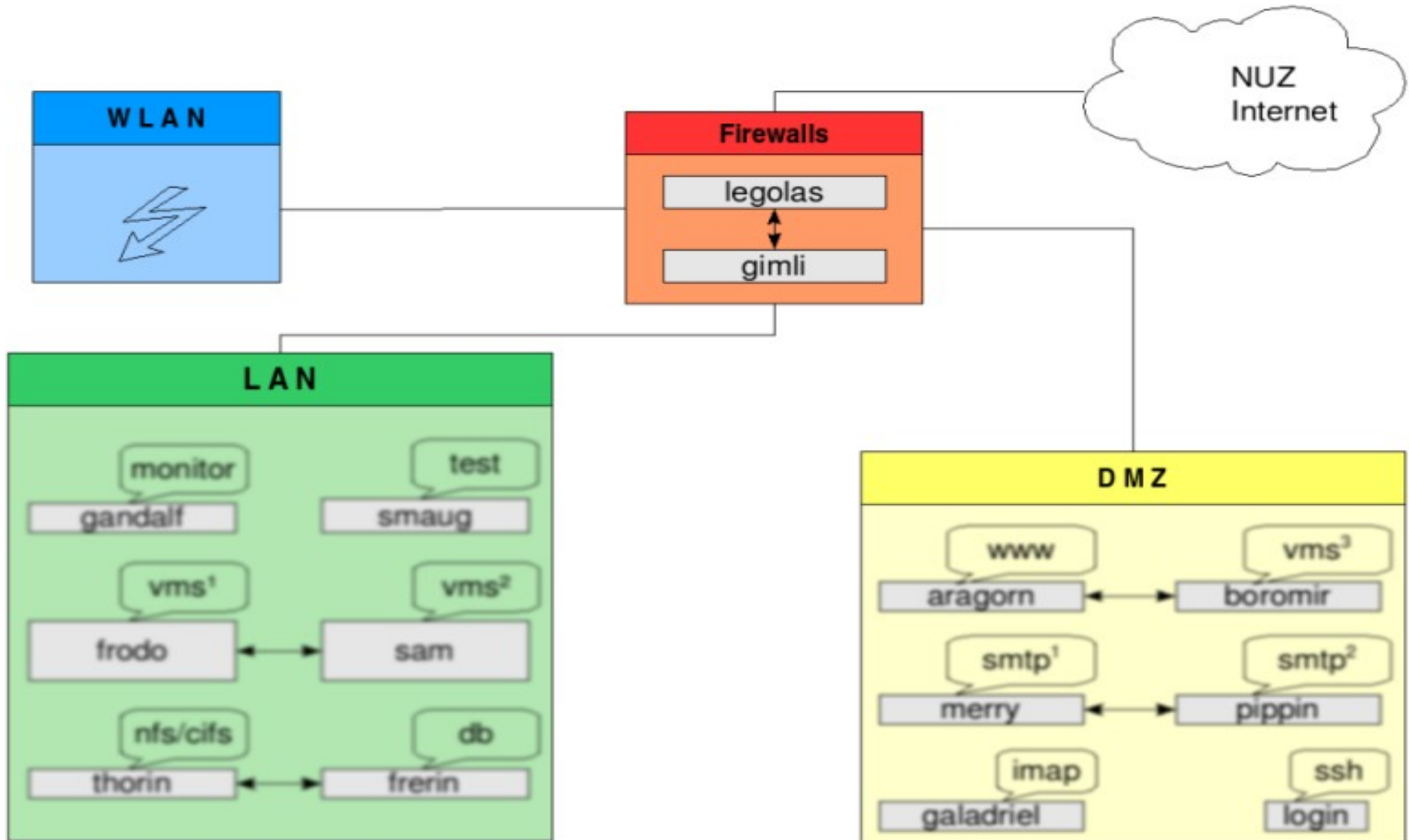
- The Institute of Neuroinformatics
 - Established in 1995
 - At University and ETH Zurich
 - ~ 100 researchers / 3 professors

“The mission of the Institute is to discover the key principles by which brains work and to implement these in artificial systems that interact intelligently with the real world.”



- Heterogeneous IT environment
 - 120 Linux workstations
 - 20 Windows PC's
 - 20 Servers
 - 30 Special purpose machines
 - 1.45 full time equivalent positions
- Four network segments
 - LAN, WLAN, DMZ, NUZ (Uplink)

Network overview



Why high-availability at all?

- Redundancy is no longer 'the Big Guys only'
- Think of it:
 - Outbound and Inbound VPN sessions
 - Voice over IP
 - IT maintenance during business hours = cheaper



● heartbeat

- Slow:
takeover up to 20s due to ARP broadcasts ('Gratuitous ARP')
- Buggy (well, it does work - sometimes)

● Netfilter

- No state synchronisation
- 'conntrackd' tries to fix this, but still:
 - No ipv6 support
 - Only certain states sync'ed (TCP established)
 - Quite new, not 'production ready'

- Why a life cycle?
- Linux release cycle choices:
 - 'Community release'
 - short / frequent / undefined
 - Often less quality focused
 - 'Business release'
 - long
 - You will run old (= less secure) software
 - Ever tried upgrading a five year old system?

Why the hell OpenBSD?



Why OpenBSD: Concepts

Secure by default



Knobs suck

Enforce open standards

Free, as in air

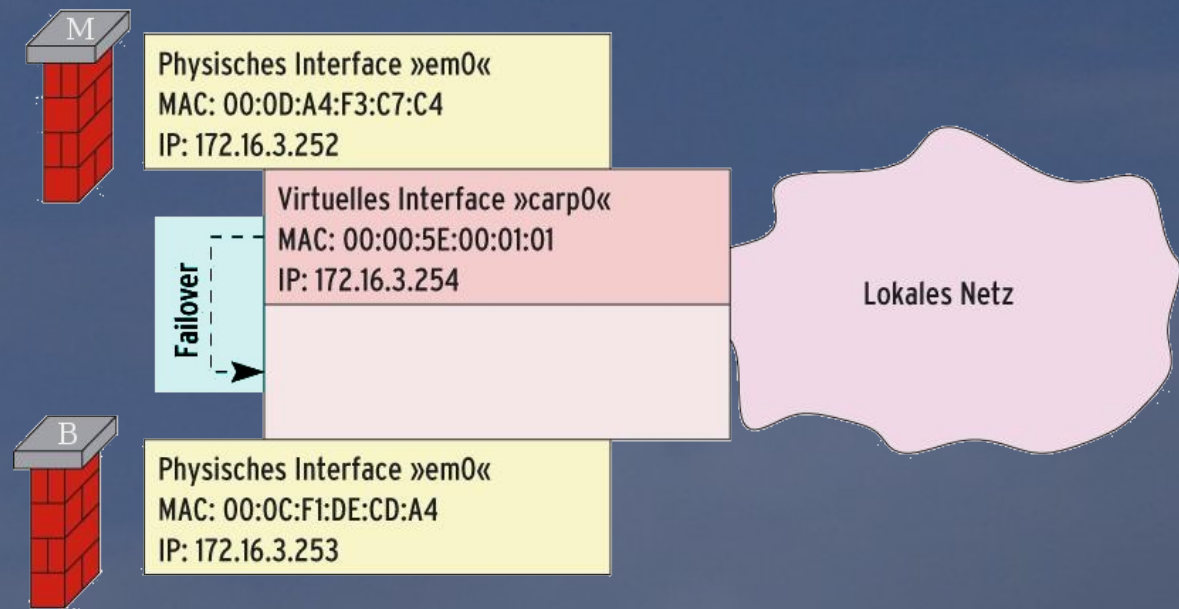
The migration to OpenBSD: Lifecycle

- Short (one year):
 - Fast and steady evolution
 - Quality driven improvements
- Fixed (1st of May / Nov.)
 - Very easy to plan (budget, time, support)
- Smart Upgrades
 - very well documented
 - even with no physical access
 - 30min down to 10min per machine
 - easy to deploy on many machines ('man release')

The migration to OpenBSD: CARP

● CARP

- Common Address Redundancy Protocol
- Free implementation of Cisco's HSRP/VRRP
- Covers layer 2 *and* 3
- Quick!
- unlimited nodes
- active/passive
- active/active (ARP and IP loadbalancing)



The migration to OpenBSD: pf/pfsync

- pf (OpenBSD's Packet Filter)

- Human readable syntax

- “pass in inet proto tcp from any to \$if port ssh”

- Complete feature set

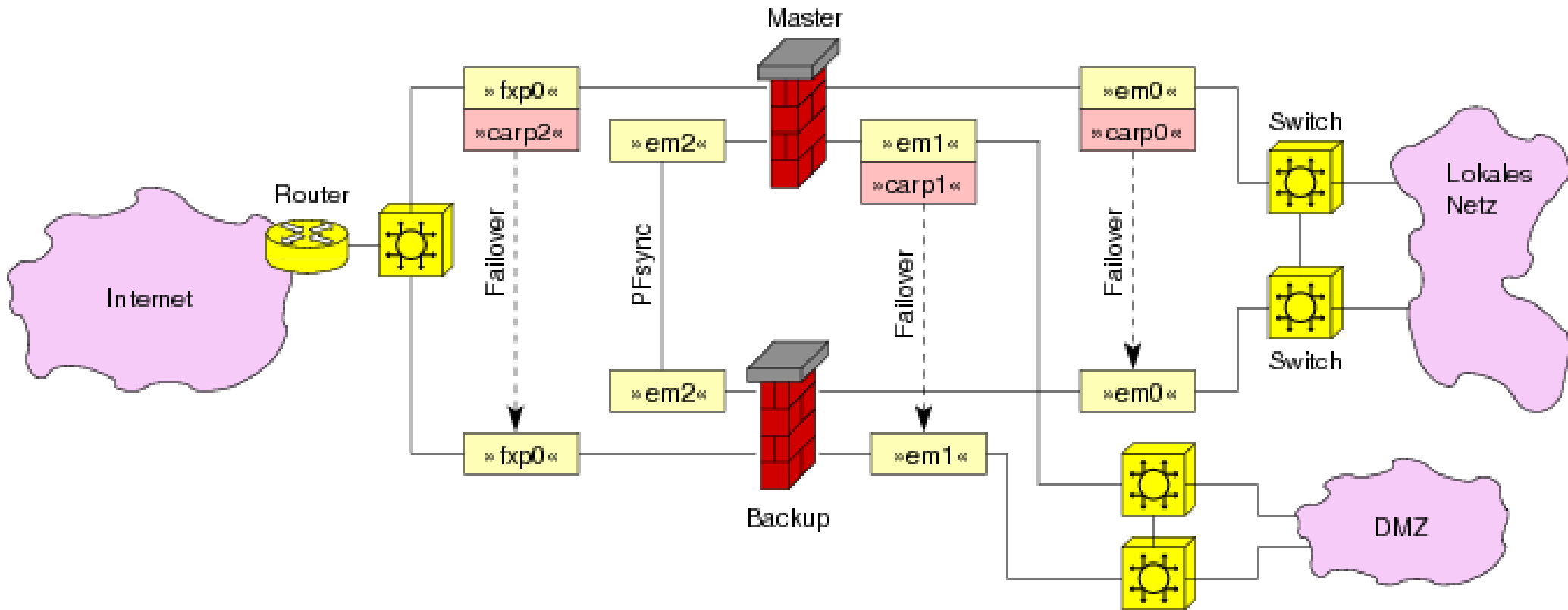
- Logging via pflog interface

- pfsync

- PF state table synchronisation

- 'standard' network interface config

The full picture: CARP/pf/pfsync @INI



- Original plan to migrate only two firewalls has led to eight machines being migrated to OpenBSD.
- New OpenBSD machines have been introduced and there are likely to be more to come.
- Maintenance overhead was drastically reduced.
- Overall security and availability was increased.



OpenBSD has become
the strategic platform no. 1 @INI

BSD and Linux Consulting is available
via my IT consulting company
StarTek (<http://startek.ch>)
- secure by design.

:wq