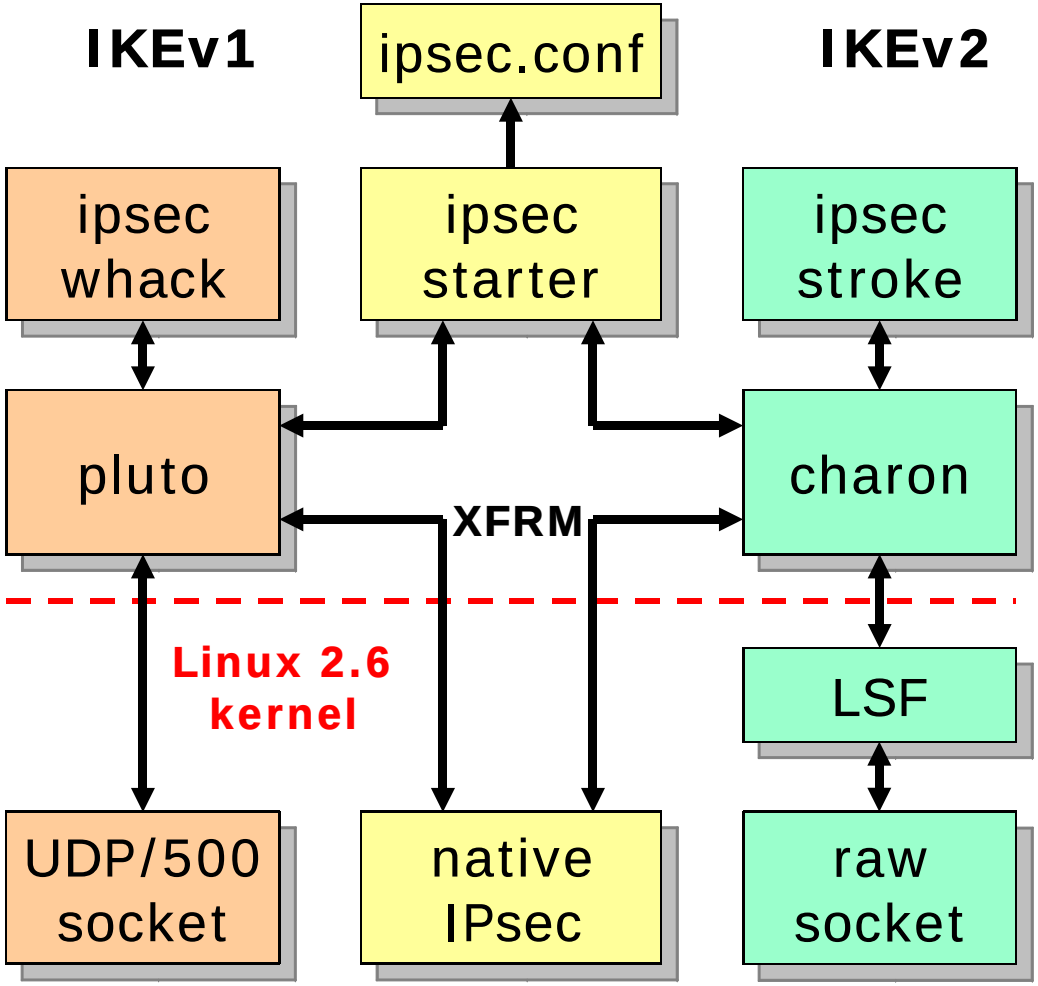
IKEv2 in

Martin Willi
martin@strongswan.org
www.strongswan.org

NEW! 4.0 release



IKEv2, und warum?

- RFC4306, Dezember 2005
- Vereinfachter Verbindungsaufbau
- 4 statt 9 IKE-Meldungen
- Weniger komplex, dadurch sicherer
- Flexiblere Authentisierung durch EAP
- Erweitertes Aushandeln von Policies
- Viele sinnvolle Ergänzungen zu IKEv1

Andere Projekte

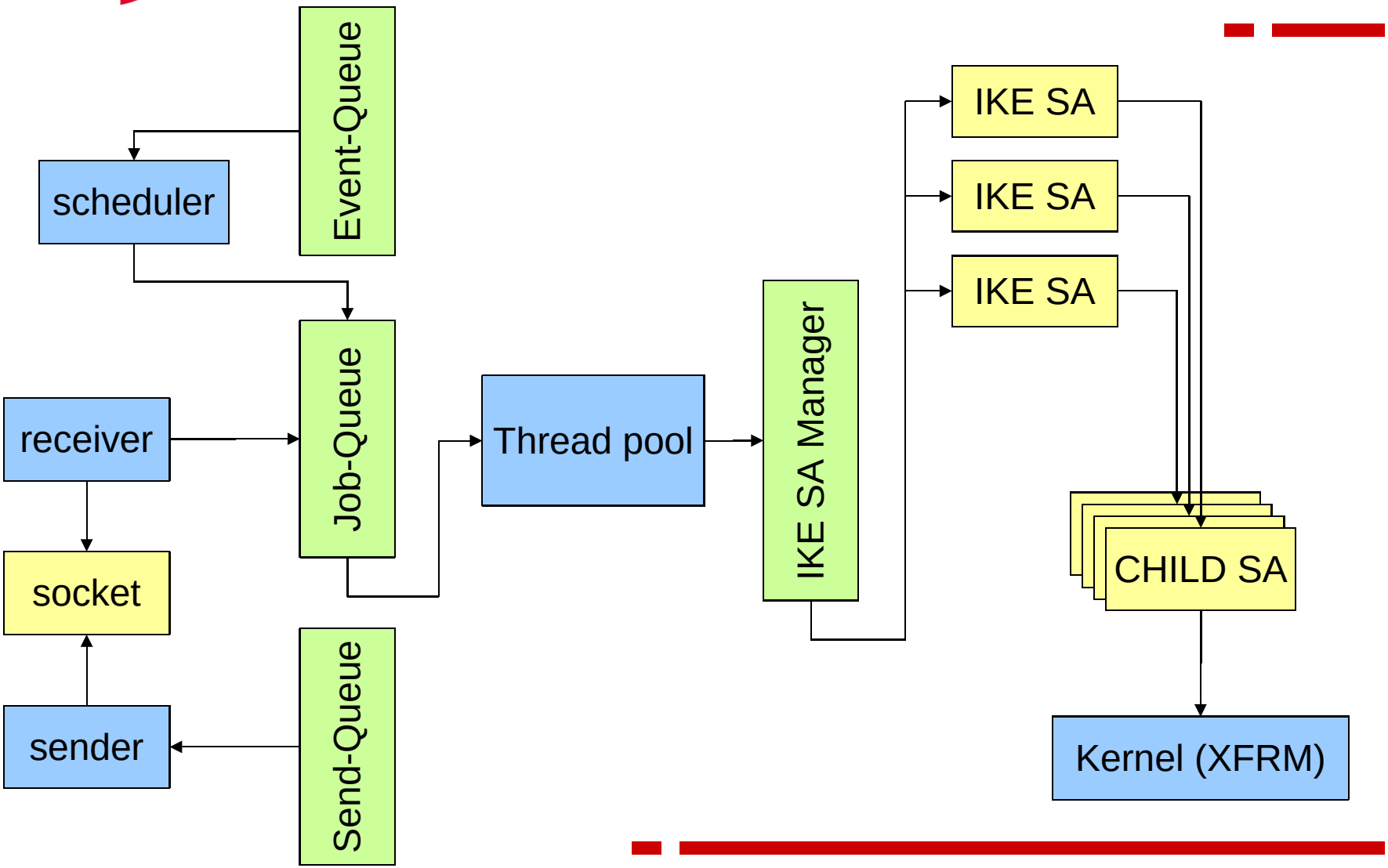
- **ikev2** (ikev2.sourceforge.net)
  - C/OpenSSL/PFKey
- **openIKEv2** (openikev2.sourceforge.net)
  - C++/OpenSSL/XFRM
- **racoon2** (www.kame.net)
  - C/OpenSSL/PFKey

- IKEv1 Support dieser Projekte?

IKEv2 in strongSwan

- Implementiert in eigenem Daemon
  - Integration in pluto kaum sauber möglich
  - Pluto trägt viele Altlasten
  - Single-threaded Architektur stösst an Grenzen (OCSP, DNS, ...)
- Nach wie vor möglichst wenig Abhängigkeiten (lediglich gmp Library)
- Linux 2.6, native IPSec

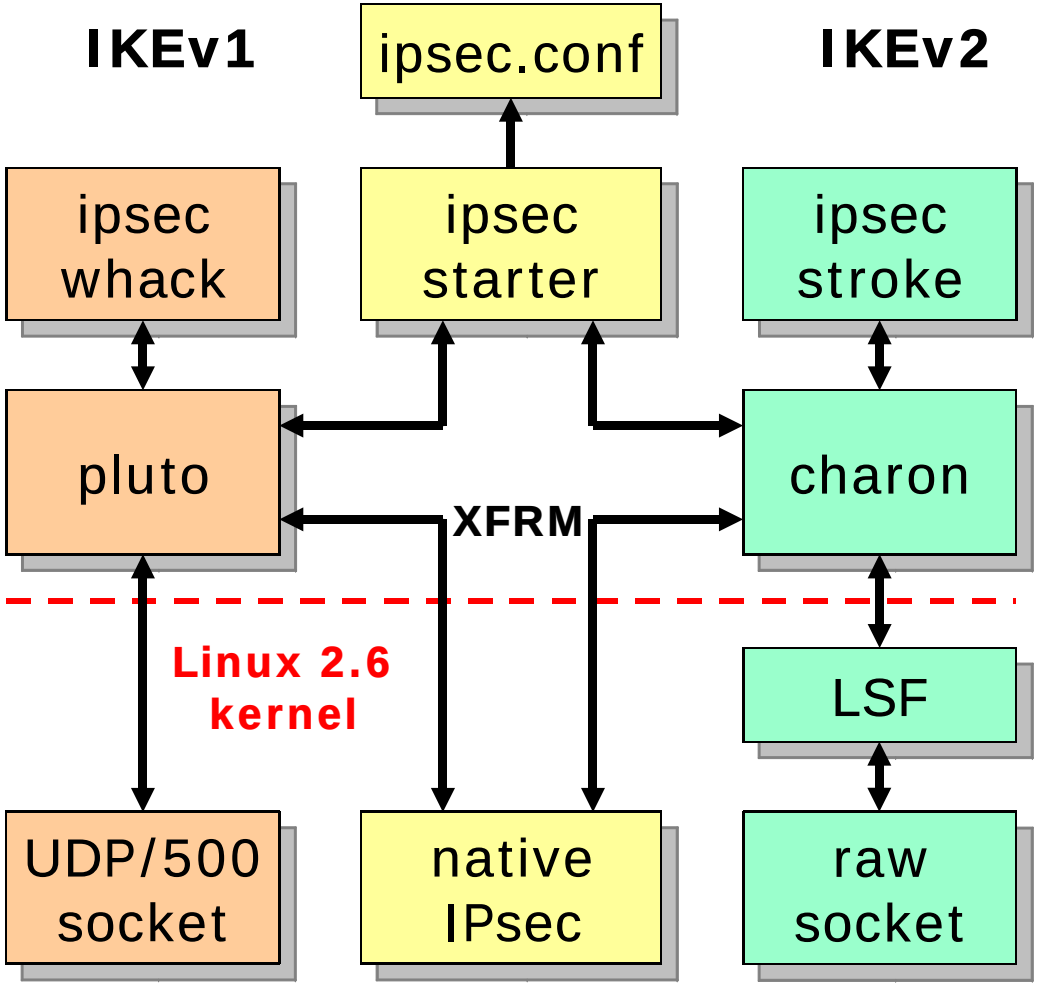
Architektur „charon“



Migrationsstrategie I

- Kurzfristig:
  - Paralleler Betrieb beider Daemons
  - Möglichst viel Code über **libstrongswan** gemeinsam nutzen.
  - Gemeinsame Konfiguration, wie bis anhin durch ipsec.conf
  - Steuerung beider Daemons über „ipsec starter“

Migrationsstrategie II



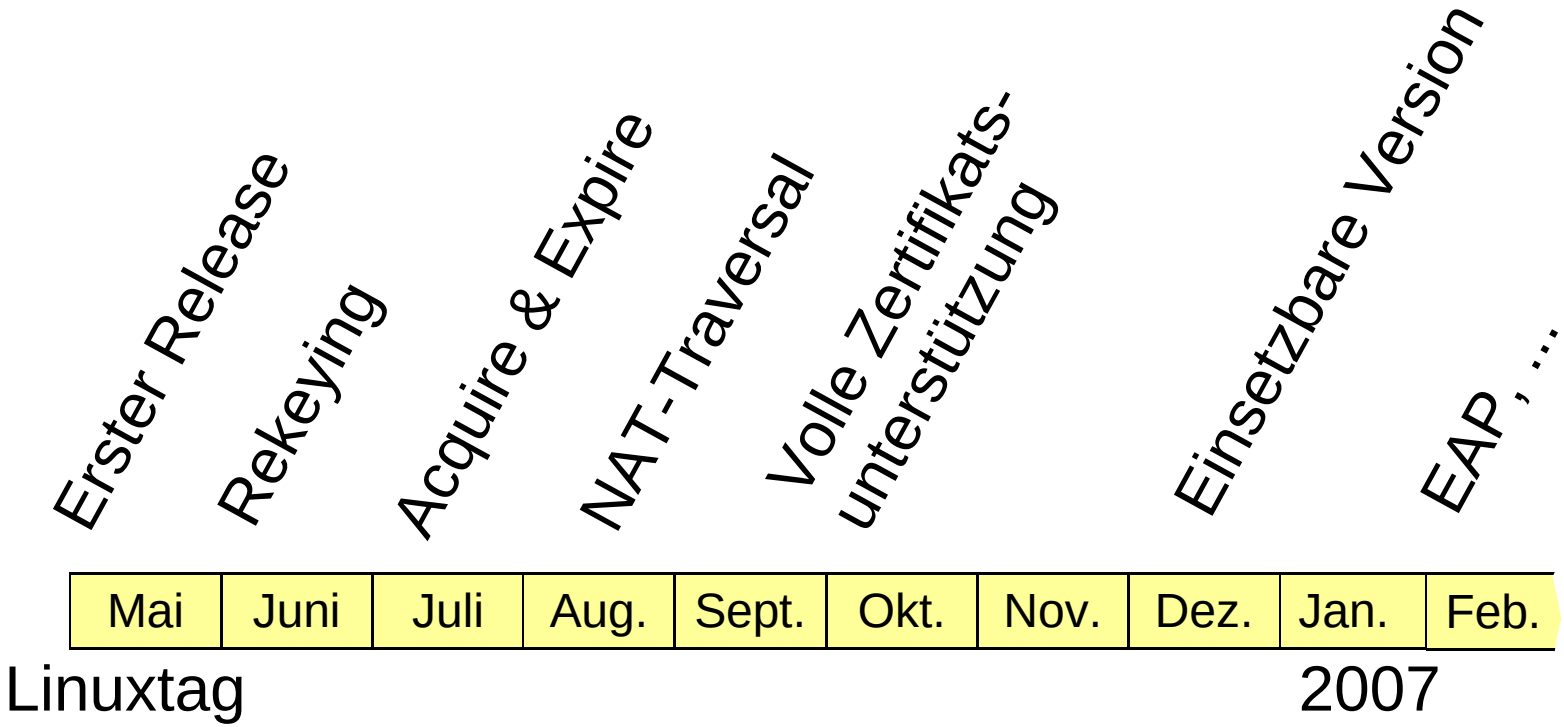
Migrationsstrategie III

- Vorteile:
  - Jetzt schon IKEv1 parallel zu IKEv2
  - Experimenteller IKEv2 Code gefährdet IKEv1 in keiner Weise
- Nachteile:
  - Zwei Daemons installieren Kernel-SAs
  - Fallback von IKEv2 auf IKEv1 noch nicht gelöst
- Mögliche Lösung:
  - Koordination durch „ipsec starter“

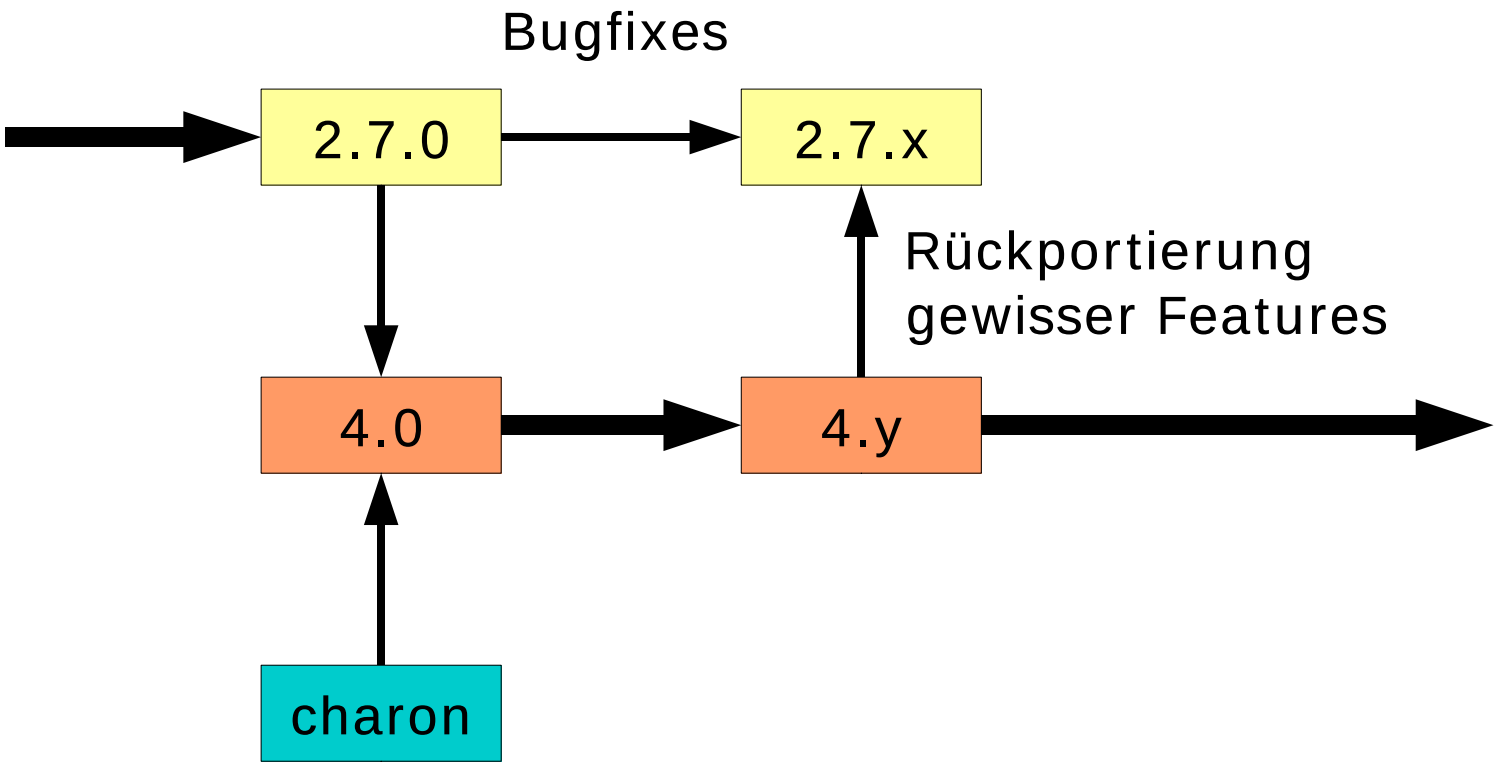
Migrationsstrategie IV

- Langfristig:
  - Ziel: IKEv1 in charon
  - Möglichst viel Code aus pluto portieren
  - Einzelner Thread verarbeitet IKEv1?
  - Komplette Portierung der State-Machine aus pluto?

Roadmap für charon



Roadmap strongSwan



Fragen & Diskussion