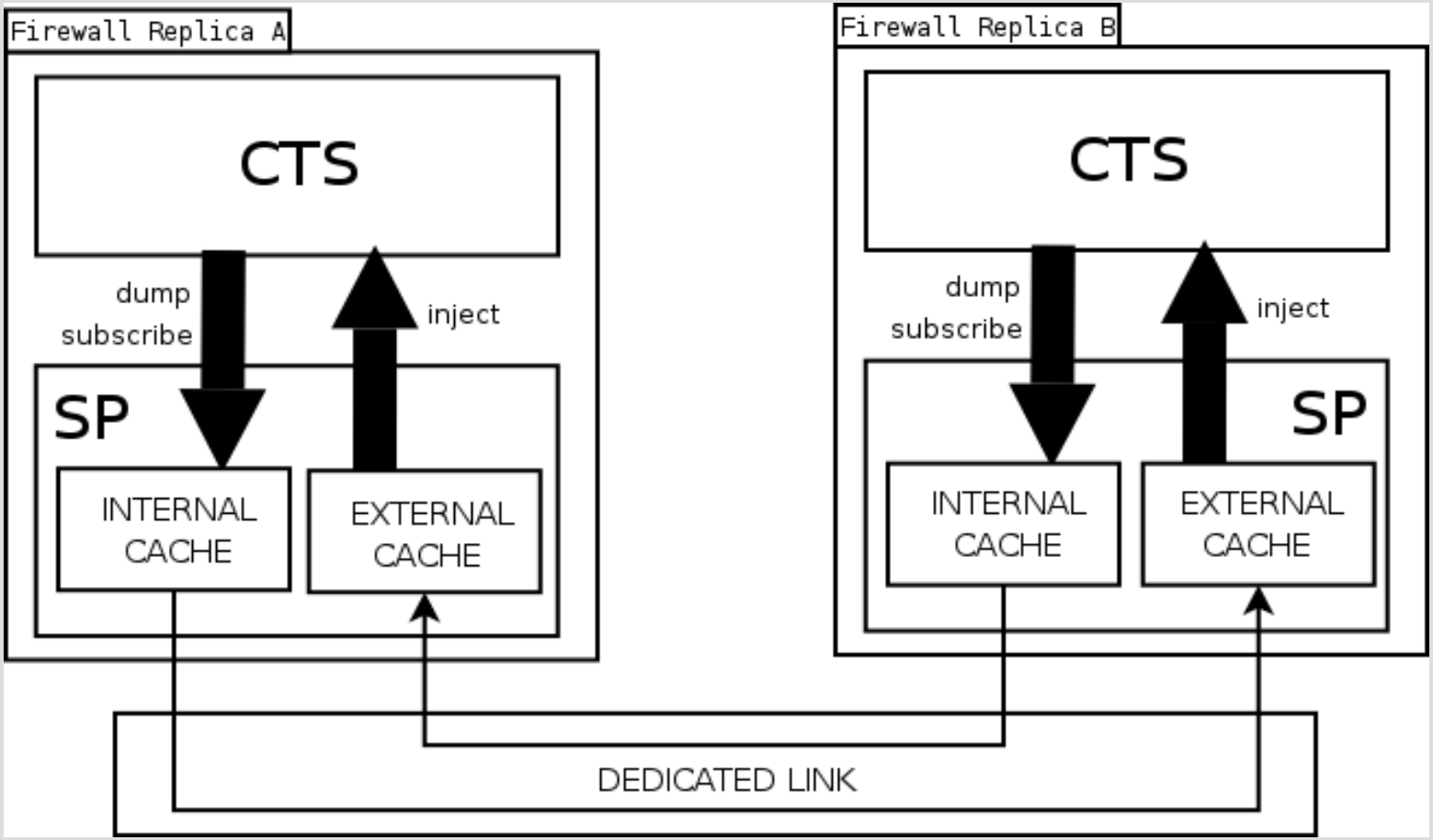
Conntrack-tools: High Availability for stateful Linux firewalls

<pablo@netfilter.org>

Overview

- **conntrackd** is a userspace daemon that covers the specific aspects of stateful Linux firewalls to enable high availability solutions
- First release: May 2006
- Current version: 0.9.5 - July 2007
- Requires an HA manager: keepalived
- http://people.netfilter.org/pablo/conntrack-tools/

Architecture



Features

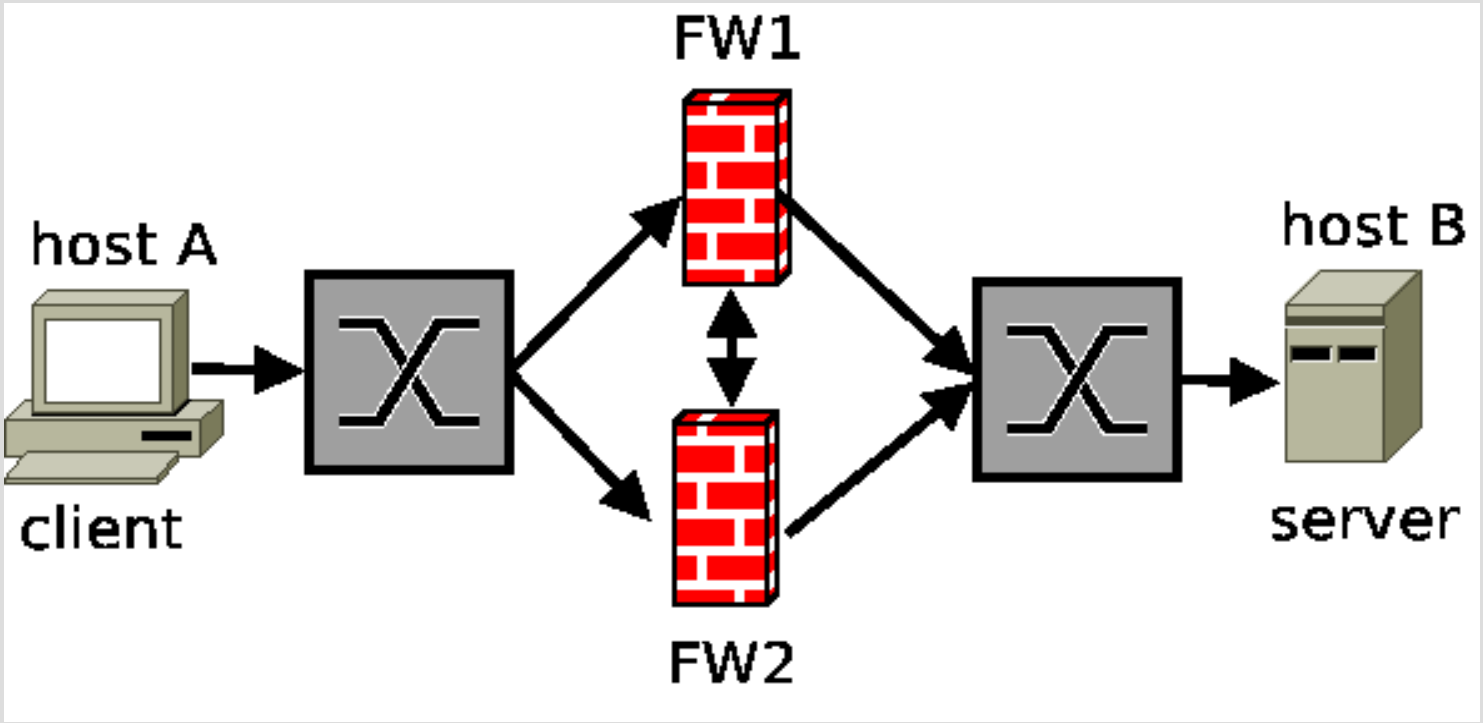
- Primary-Backup and Multiprimary support
- TLV-based message format: 60-76 bytes per message (not netlink but similar) and batch support
- Relatively easy to setup (see website)

Replication protocols

- Currently two protocols:
  - **Alarm-based**: Every N seconds a state message is sent (spamming)
  - **reliable UDP protocol** (sequence tracking): data, ACK, NACK (and RESYNC) messages
    - The receiver handles all messages even those that are out of sequence
    - The sender just resend the last state reached (reduces the number of messages retransmitted under message omission)
    - no congestion control

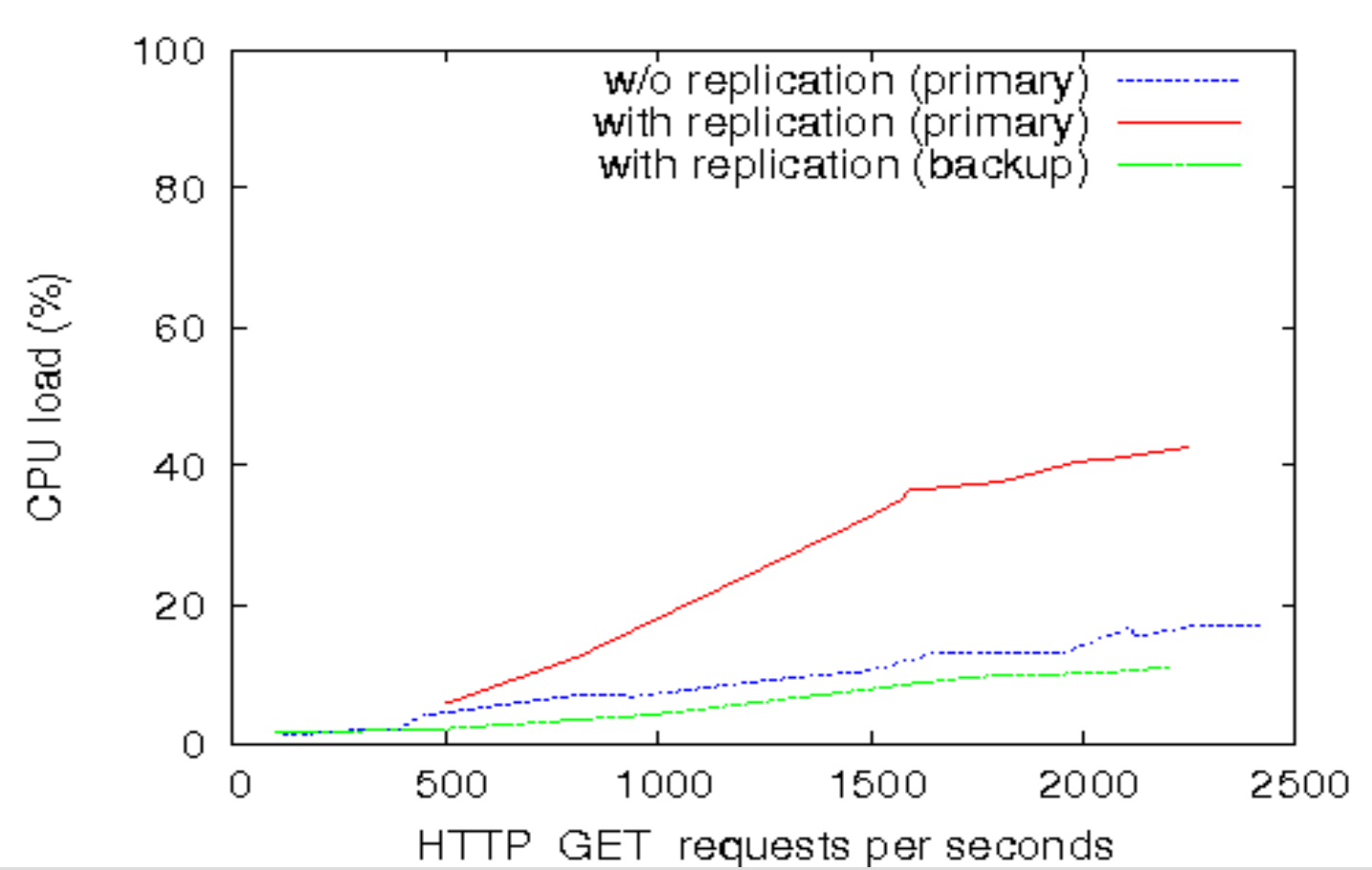
Evaluation

- Testbed: HP Proliant 145G2, AMD 2.2GHz, 1GBit

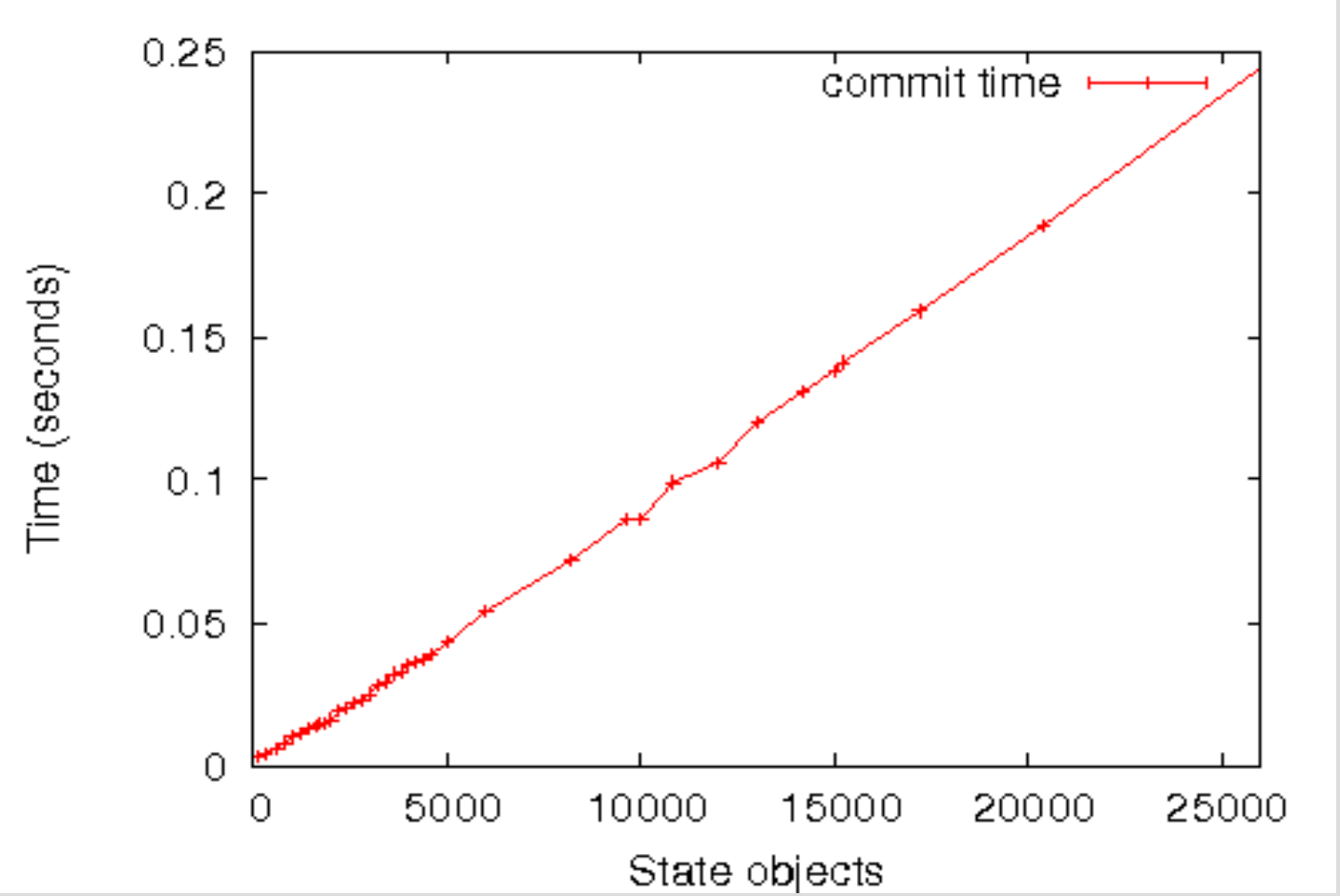


- HTTP GET requests from A to B (4 KB)

CPU consumption



Recovery Time



Open issues

- Netlink kernel-space filtering
- Only replicate certain states, e.g. TCP ESTABLISHED (already possible)
- TCP window tracking disabled
- IPv6 support
- Asynchronous solution: Replicas don't contain the same set of states at any time
- NAT helper sequence adjustments
- Netlink Overrun: synchronization problems