nft-sync

Distributing nftables rulesets across the network

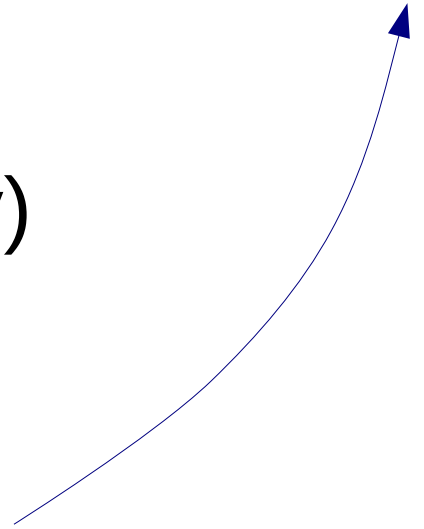
Arturo Borrero Gonzalez
arturo.borrero.glez@gmail.com

Netfilter Workshop 2014
Montpelier, France

nft-sync

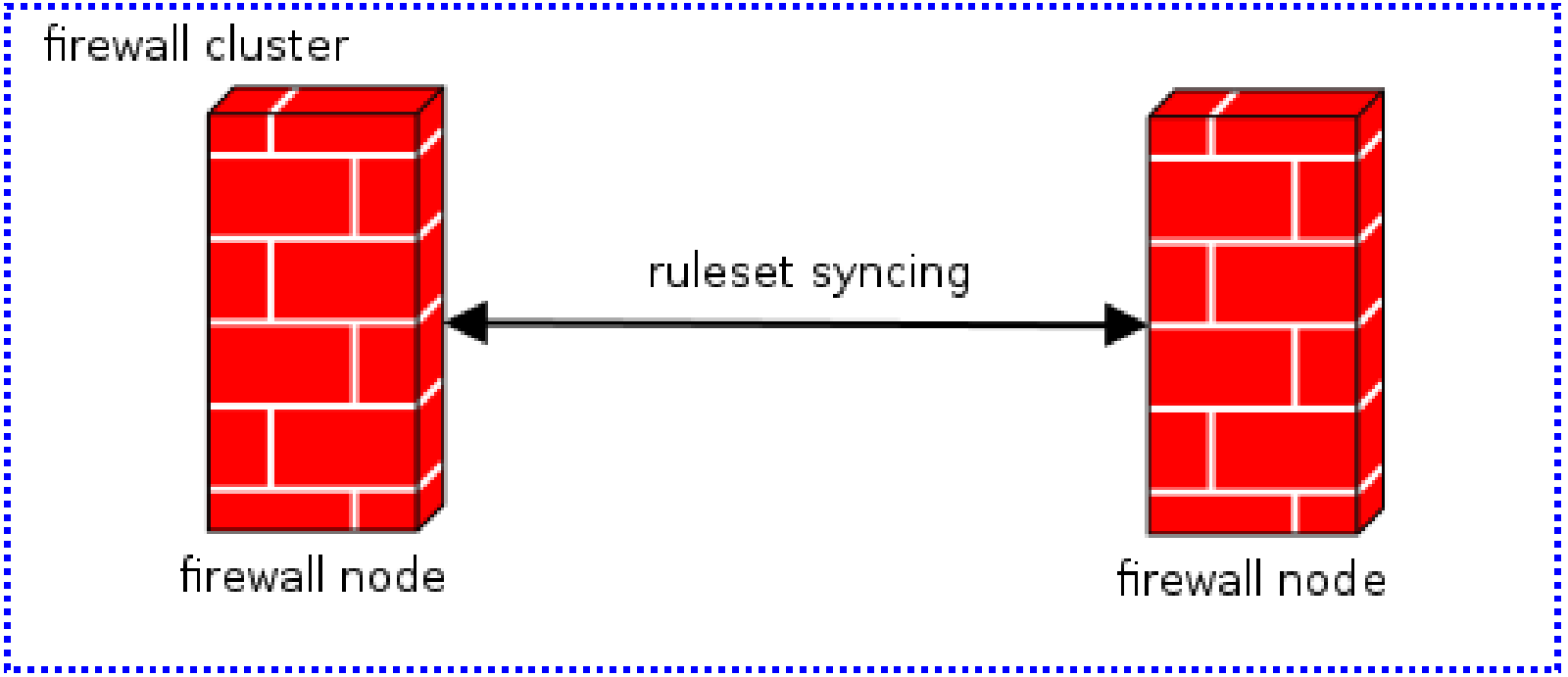
Main scenarios to face:

- Cluster syncing
- Ruleset distribution (repository)

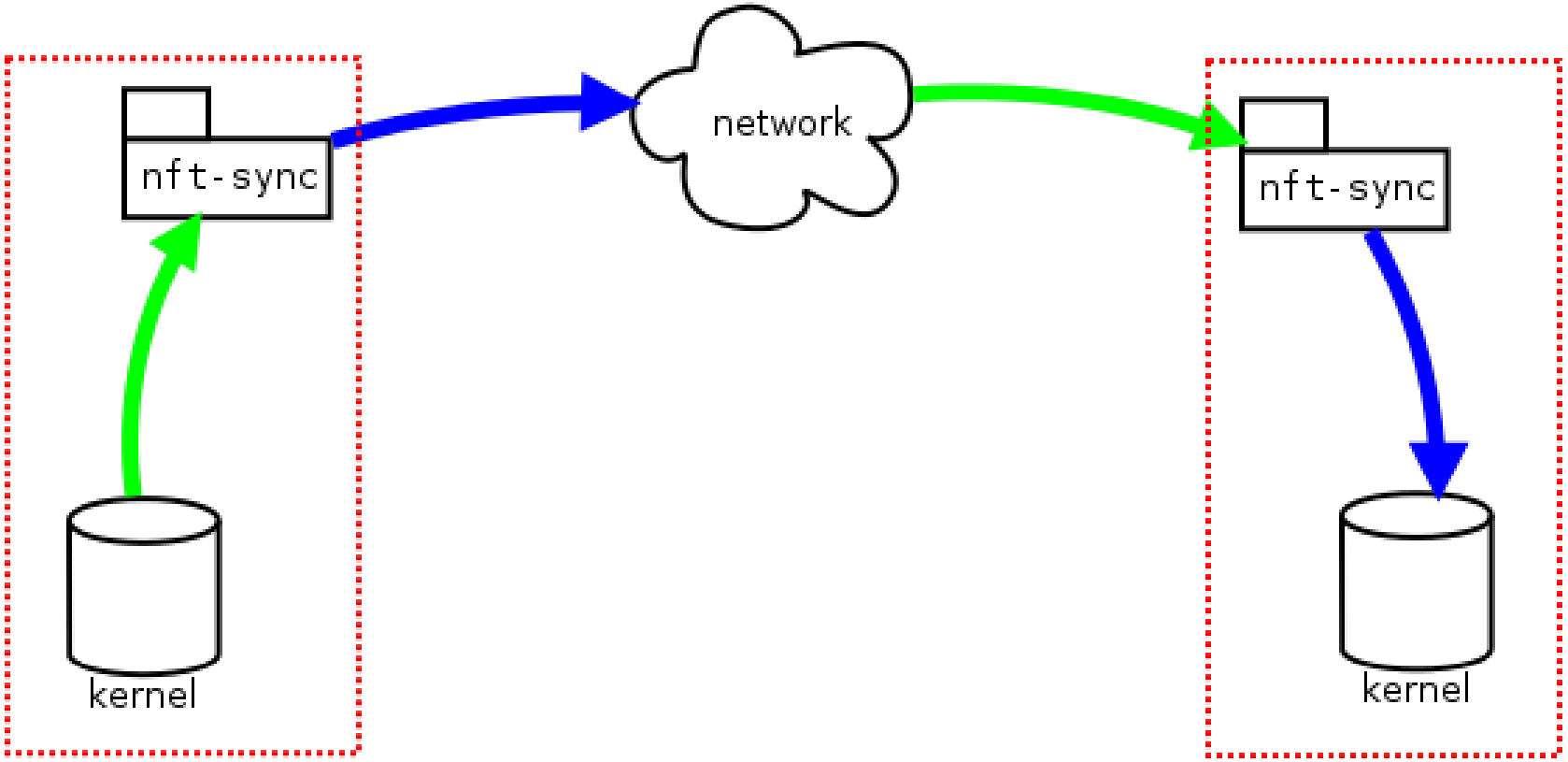


nft-sync

Cluster syncing



nft-sync

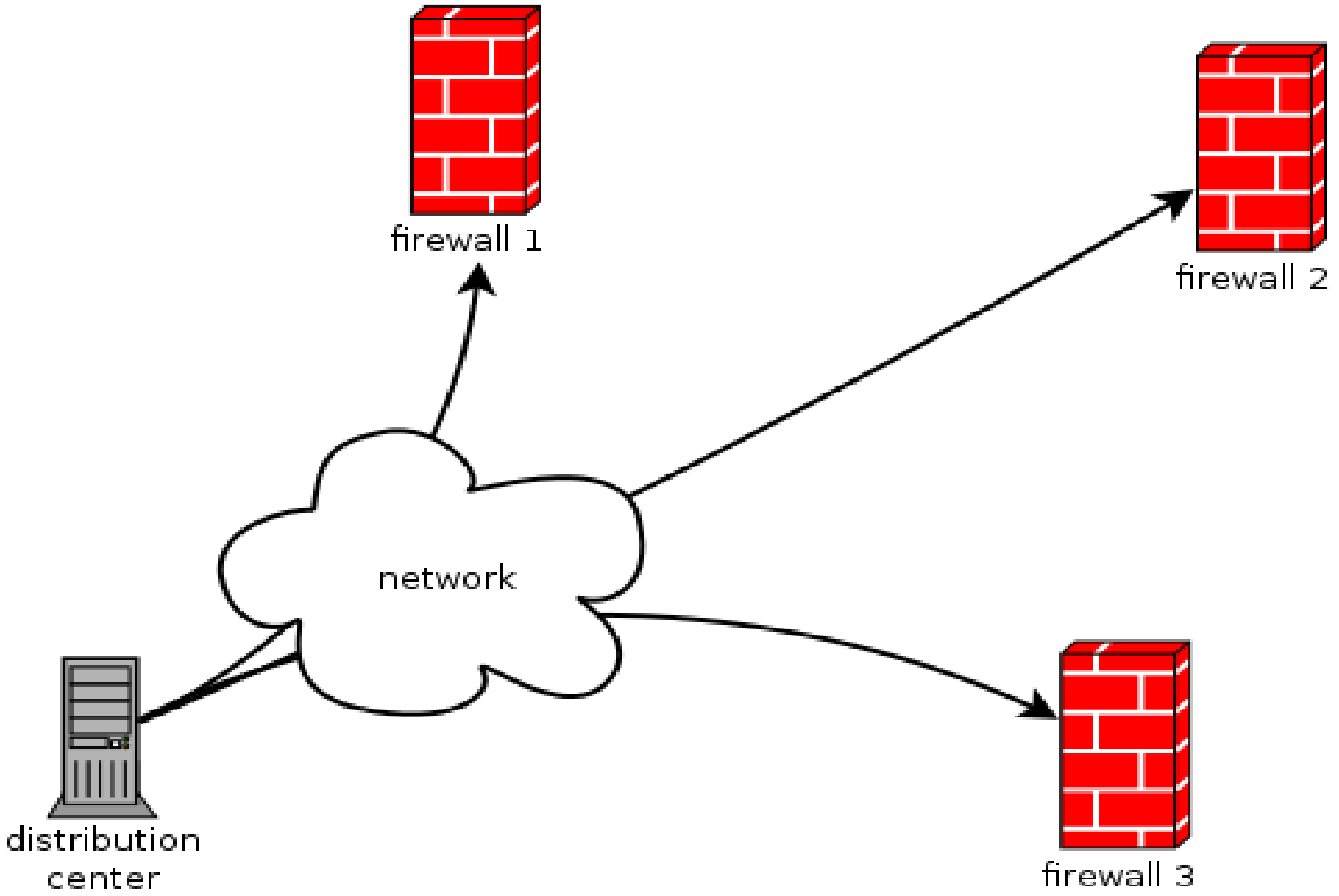


→ Event handler

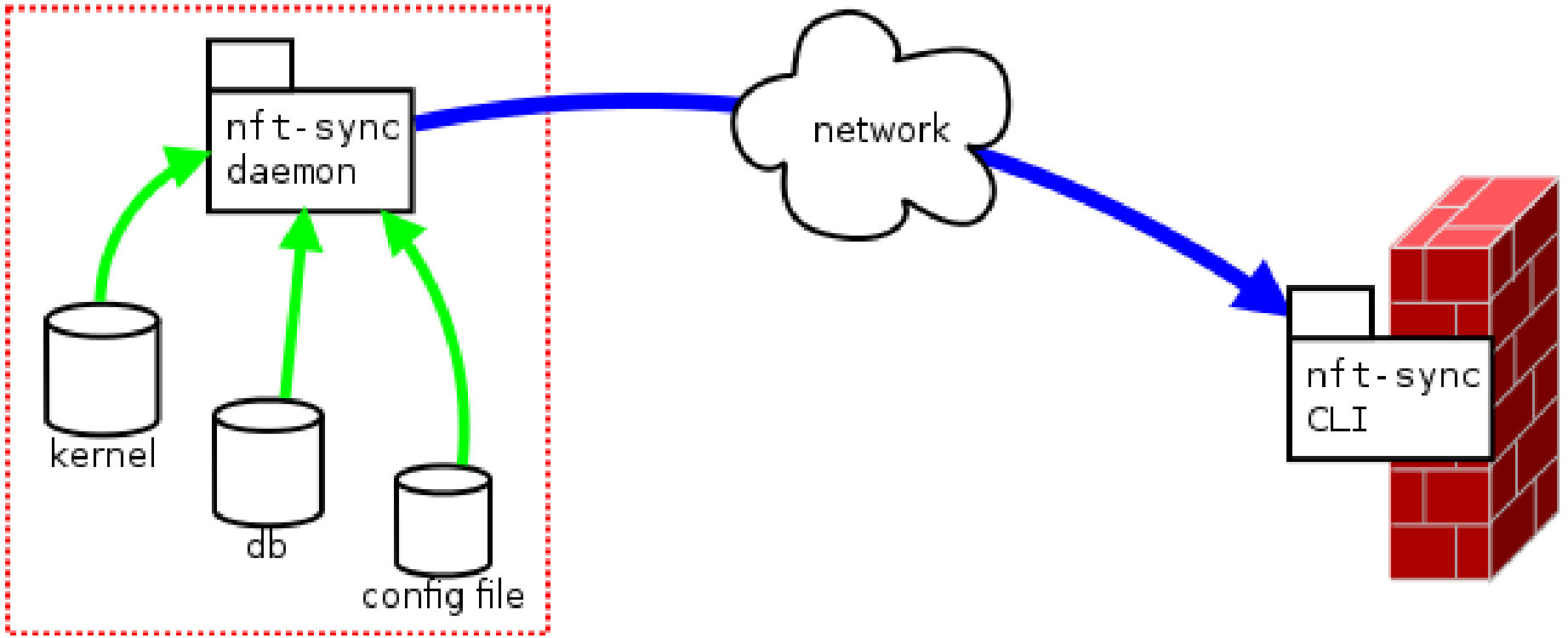
→ Action

nft-sync

Ruleset distribution (repository)



nft-sync



→ Ruleset reading
→ Distribution

nft-sync

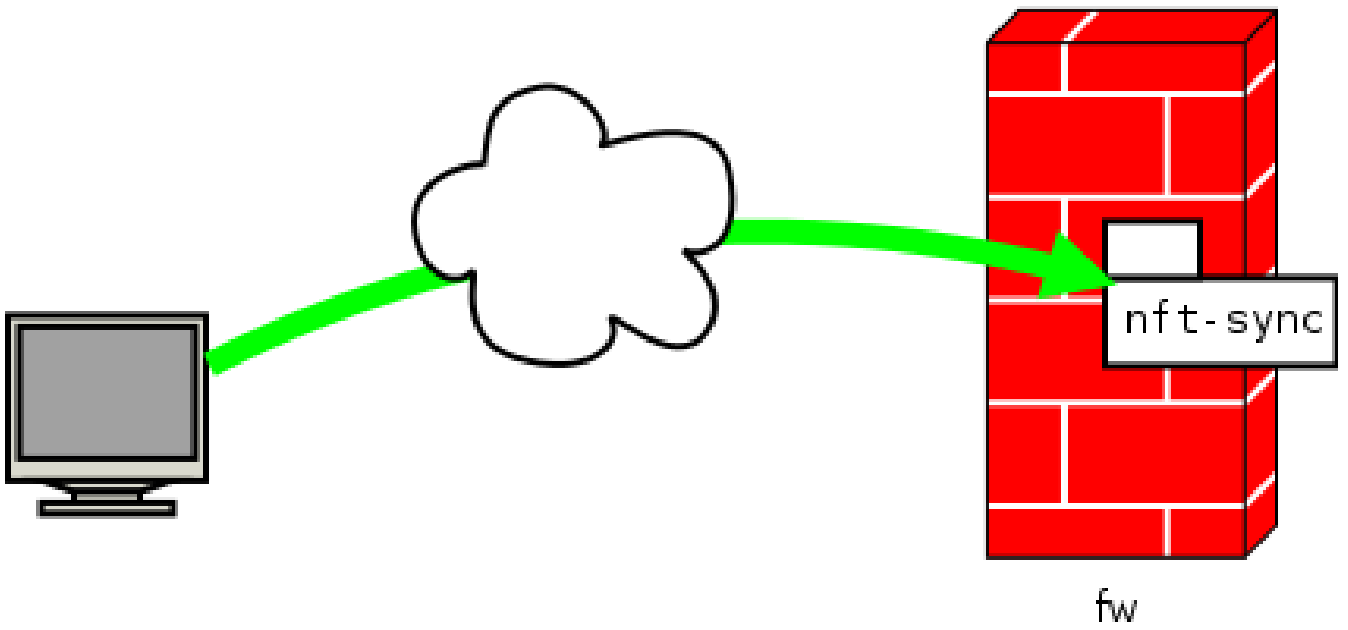
Derivated scenarios:

- Remote management
- Distributed policing

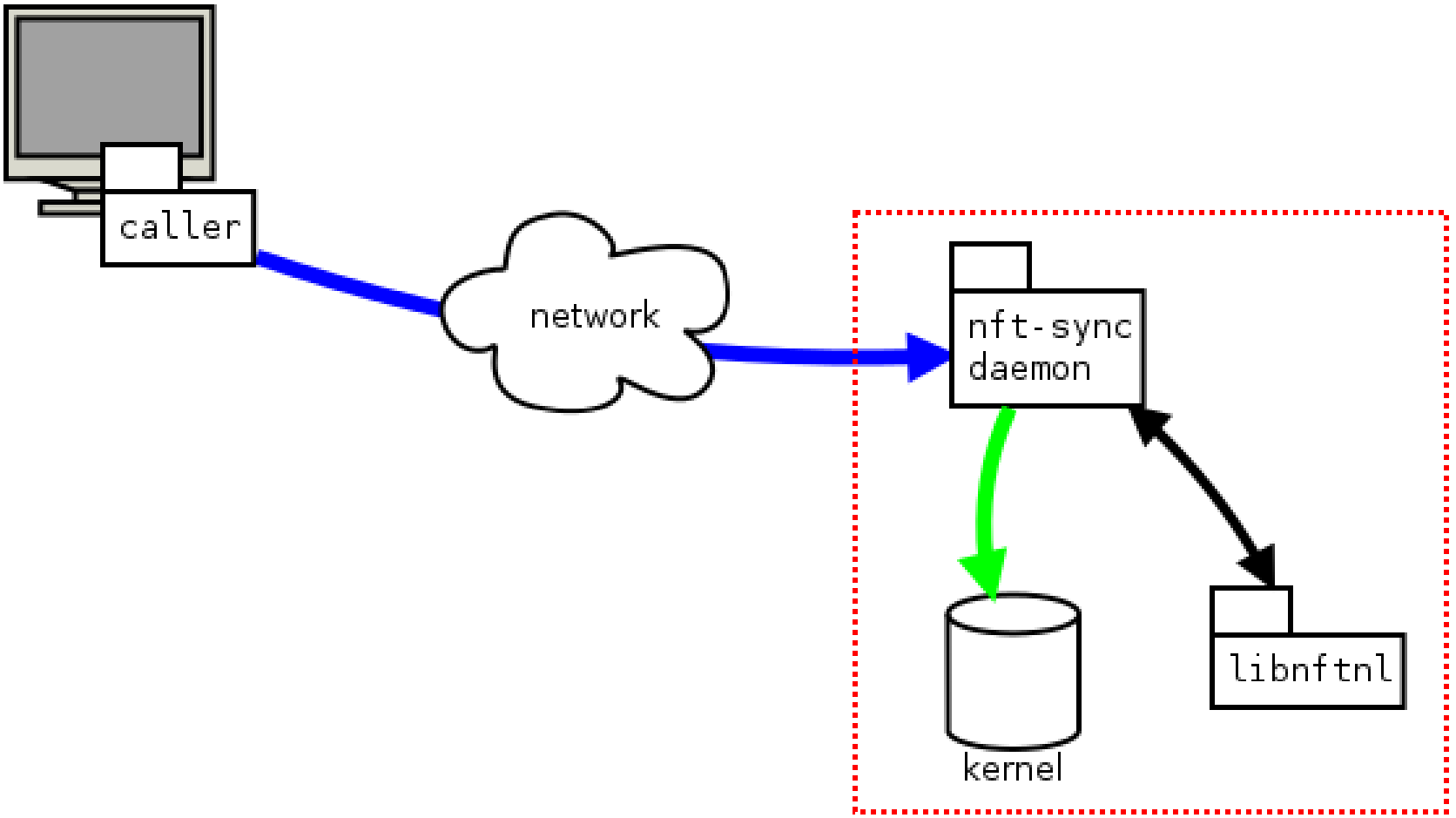
nft-sync

Remote management

- Offers a public API

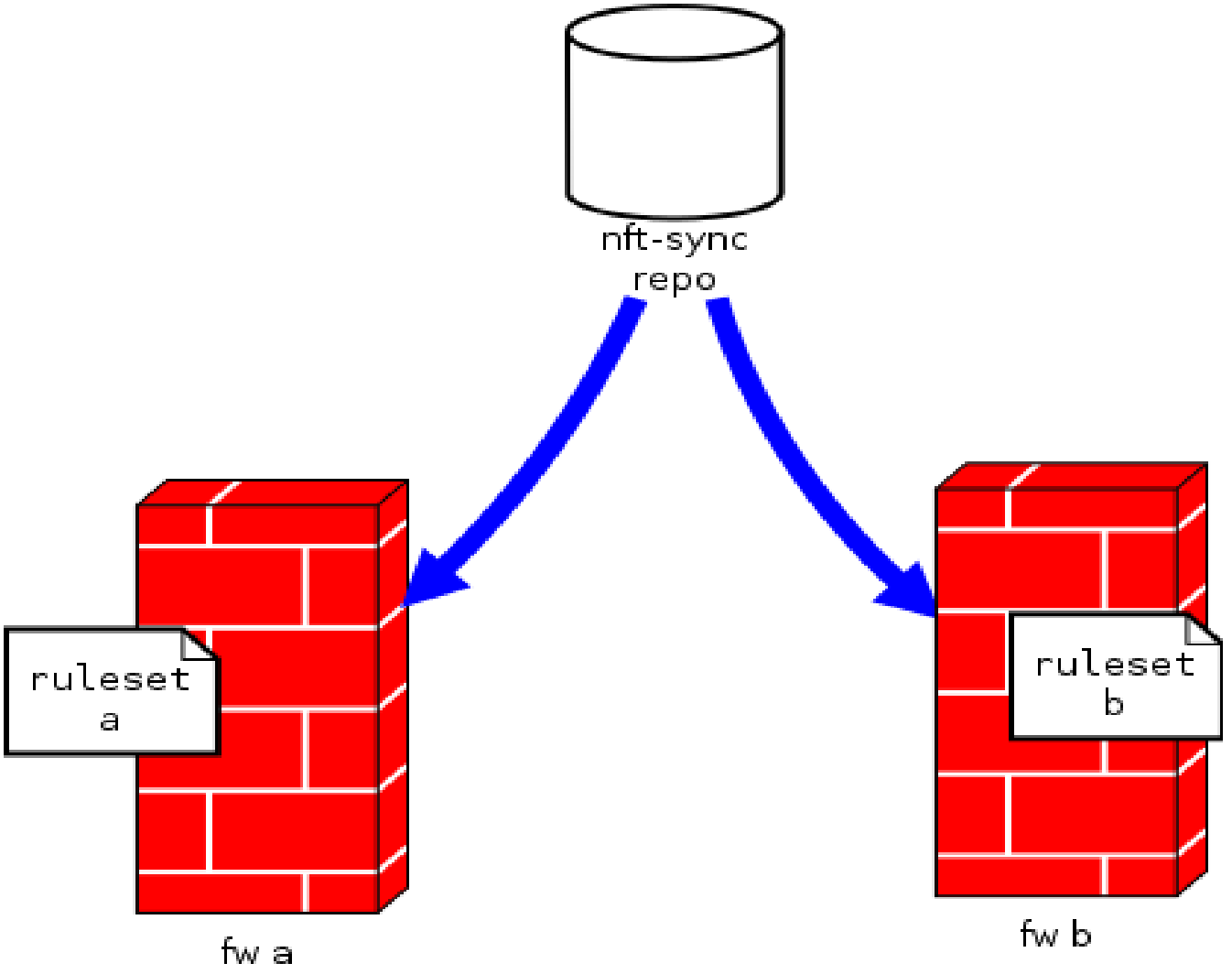


nft-sync



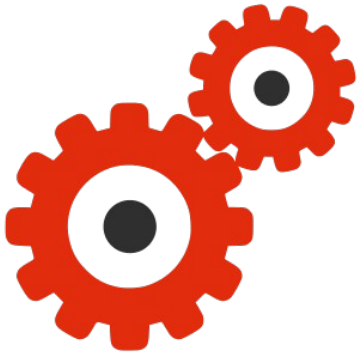
nft-sync

Distributed policing



nft-sync

How it works



→ Basic config file

→ Running modes: daemon, CLI

→ Operations: fetch, pull, sync, …

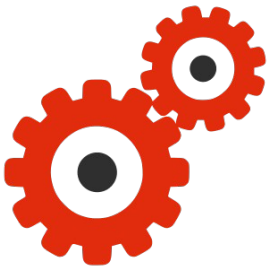
nft-sync

How it works

→ Simple sync protocol (inspired by git)

→ XML / JSON (provided by libnftnl)

→ libev based



nft-sync

The protocol:

```
struct nft_sync_hdr {
        uint32_t        len;
        char            data[0];
};
```

nft-sync

iptables vs nftables

	iptables	nftables
Events reporting	no	Yes
XML / Json	weak	Yes
Public library / API	no	Yes
Built-in data sets	no	Yes

nft-sync

Conclusions:

- Just bootstraped (May 2014)
- Proof of concept
- Initial work funded by nlnet and Google

nft-sync

Future works:

- Complete all operations
- SSL-Based comunications
- Give flexibility, config options

nft-sync

More info:

- Announcement by Netfilter Project

  http://marc.info/?l=netfilter&m=139991701024628&w=2

- Source code

  http://git.netfilter.org/nft-sync/

nft-sync

Distributing nftables rulesets across the network

Arturo Borrero Gonzalez
arturo.borrero.glez@gmail.com

Netfilter Workshop 2014
Montpelier, France