Turris Sentinel

Running on non-Turris hardware

Michal Hrušecký

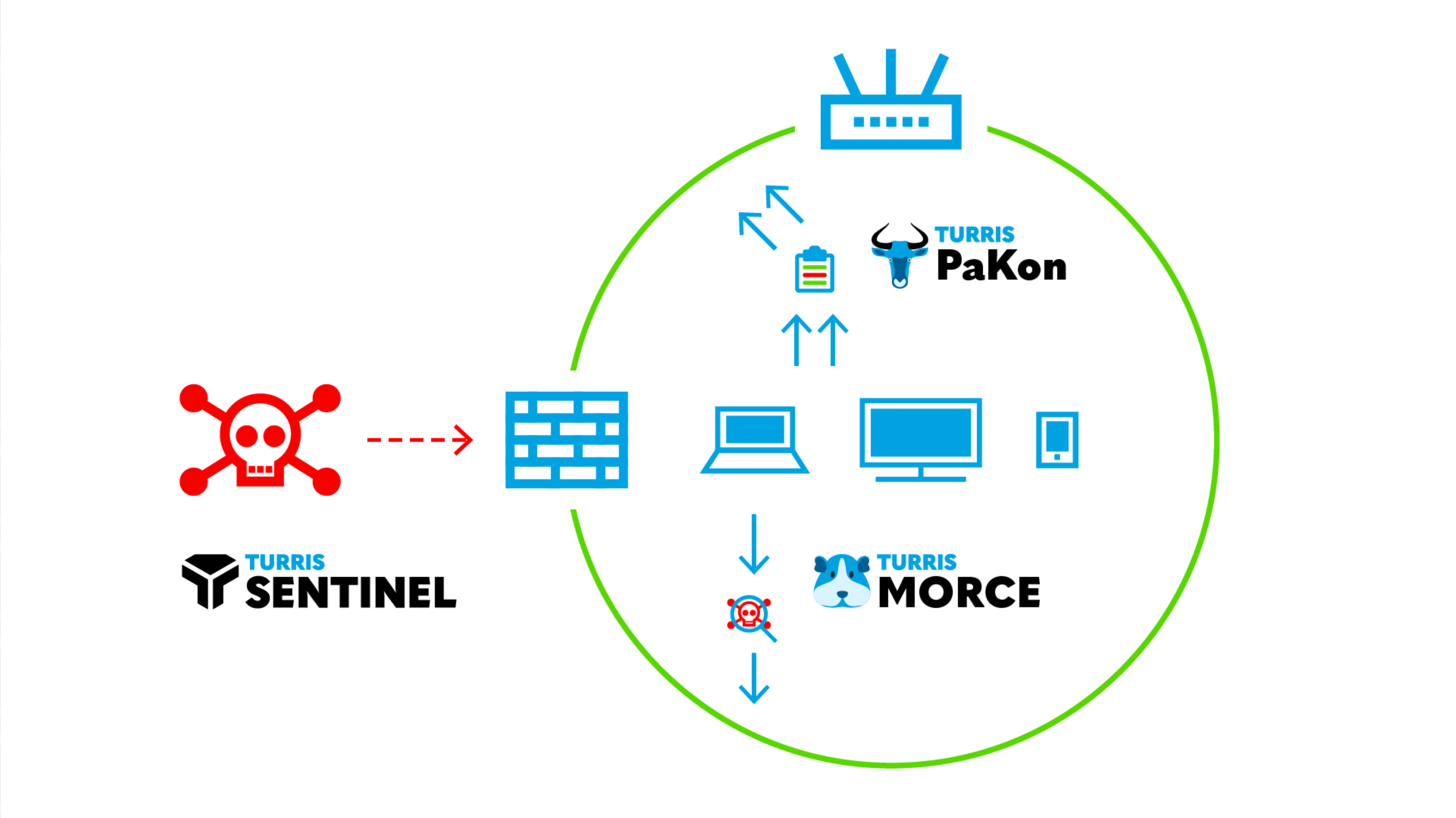
Michal.Hrusecky@turris.com

Who are we?

- part of CZ.NIC
- developing Turris routers
    - enough resources to run various services
        - repositories full of additional software
    - automatic updates
    - DNSSEC validation
    - root account for everybody
    - extra security features

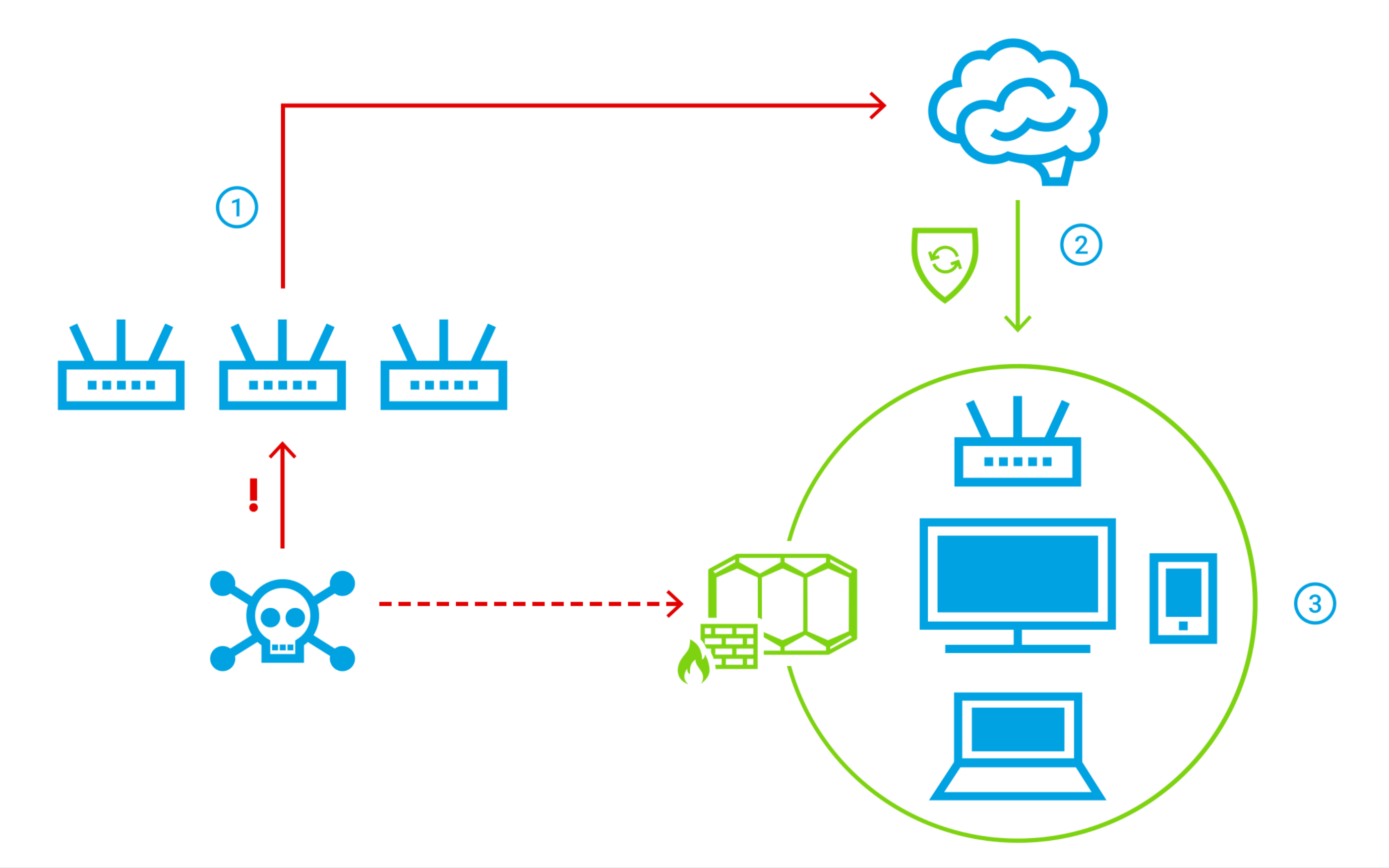
Extra security features?

- Pakon
  - netflow collector
  - using DPI to get server names
- Morce
  - simple IDS integration
- Sentinel
  - looking for attackers from outside
  - dynamic firewall

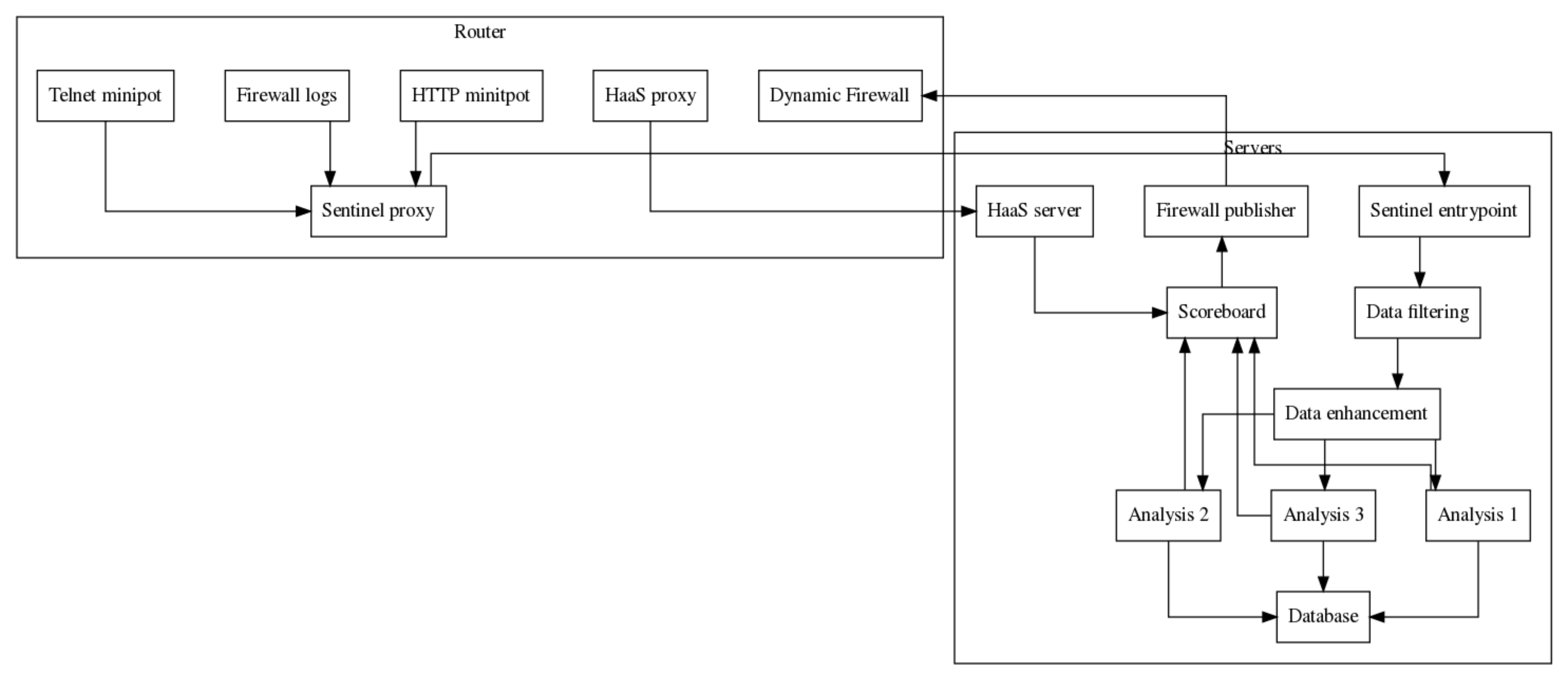


Turris Sentinel

- set of minipots
  - minimal honeypot
  - FTP
  - SMTP
  - HTTP
  - Telnet
- firewall logs



Data processing



Requirements

- get attackers on the list quickly
- remove them from the list quickly
- protect ourselves from false reports
    - one router can’t bring you to the greylist

Technicalities

- data processing and scoring is done on our server
- dynamic firewall publishes both full list and differences
- all data are sent via channel established using

Running outside of the router

- Dynamic firewall is easy
  - client that can maintain ipset
  - firewalld and systemd integration
- sending data is much harder
  - needs unique identification of the other party
- needs packaging for various distributions
  - OBS to the rescue

Open Build Service

- project security:sentinel
- one source - multiple distributions
    - Fedora, openSUSE, SLE, Debian, Ubuntu
    - source services to fetch directly from git
- automatic dependencies tracking
- automatic rebuild
- easy repositories creation

Identification

- every router has it’s serial number
- two possible handshakes
    - Turris Omnia - symetric, challenge/response
    - Turris MOX - eliptic curves, asymetric
- we know what key belongs to which serial

⇒ Let’s fake the routers

- everybody gets fake serial
- everybody will pretend that they are MOX
    - will generate private key locally
    - will send us their public key

First step - B2B

- simple communication
- individual approach
- every company has unique ID already
- big impact fro every partner
    - more IPs to listen on
    - more exposed then average home user
    - more endpoints to protect
- PoC in progress

Next step - end users

- identification will be hard
  - everybody can have plenty of logins and e-mails
- communication has to be automatic
  - much wider audience

Possible help - digital identities

- mojeID or CACert

The end - so far

Questions?

Suggestions?

Links:

- https://www.turris.cz
- https://view.sentinel.turris.cz
- https://download.opensuse.org/repositories/security:/sentinel/
- michal.hrusecky@nic.cz