Turris

Our path to open-source routers

Michal Hrušecký • Michal.Hrusecky@turris.com

TURRIS

Who is CZ.NIC?

Czech top level domain registry

- association, but in reality non-profit
- spending all the money on making Internet better
- lot of open-source development
  - Bird routing daemon
  - Knot DNS server and resolver
- running Czech national CSIRT team

TURRIS

How it all started

Big question:

How safe are home users from network attacks?

Is anybody attacking them?

How often?

What kind of attacks are they facing?

Is it safe to have a public IPv4?

TURRIS

Turris is born

Let’s make a security probe 💪

- give it to people for free
- collect data about the attacks from the outside

How to do it?

- has to be the main gateway in every home
  - it has to be able to do at least NAT 🤔
- people have to be willing to install it and give us data
  - let’s make it more than just a simple pass through gateway
  - let’s make a full fledged router!

TURRIS

First Turris router

- given away for free in CZ
- even had a Wi-Fi in mPCIe slot
- contained an early version of our security research software
- monitored traffic and reported various information
  - various honeypots deployed
  - firewall logs collected
  - anonymized netflow characteristics
  - centrally controlled blacklist
- Hardware: 2 core PPC @ 1.2 GHz, 2G RAM, 250M NAND

TURRIS

Our way of doing things

- enough resources to run various services
  - we didn’t know, what would we need
- mandatory automatic updates
  - because security 🤷
  - also we needed to develop and change the security program 😉
- DNSSEC validation
- tinkerability and transparency
  - root account
  - open source
- some extra features over the time

TURRIS

Benefits of being open

Is there really any other way the open source one?

- easier to get started
- plenty of software to integrate
  - even multiple competing implementations of the same
- we have to do "just" the integration
- people can contribute and fix their issues
- people can do whatever they want

TURRIS

Downsides of being open

- plenty of software to integrate
  - people want everything 😱
  - but some of them will actually contribute 😌
- people can do whatever they want
  - they break stuff in unbelievable ways
  - they do crazy stuff that breaks after update
- you are not in control of your dependencies
  - unless you contribute
  - there is always a fork option
  - controlling closed source would be even harder

TURRIS

Follow-up - routers in retail

Probes were popular

⇒ let’s make something people can buy

We made a successful Indiegogo campaign

Turris Omnia was born

We are in retail since then and got even some B2B customers.

TURRIS

How we got B2B customers?

- we had a man inside 🤫
- we have good enough hardware
- we are open source and push our support to vanilla
  - you don’t need a SDK
  - you don’t NDA
  - you can take whatever you have and port it easily

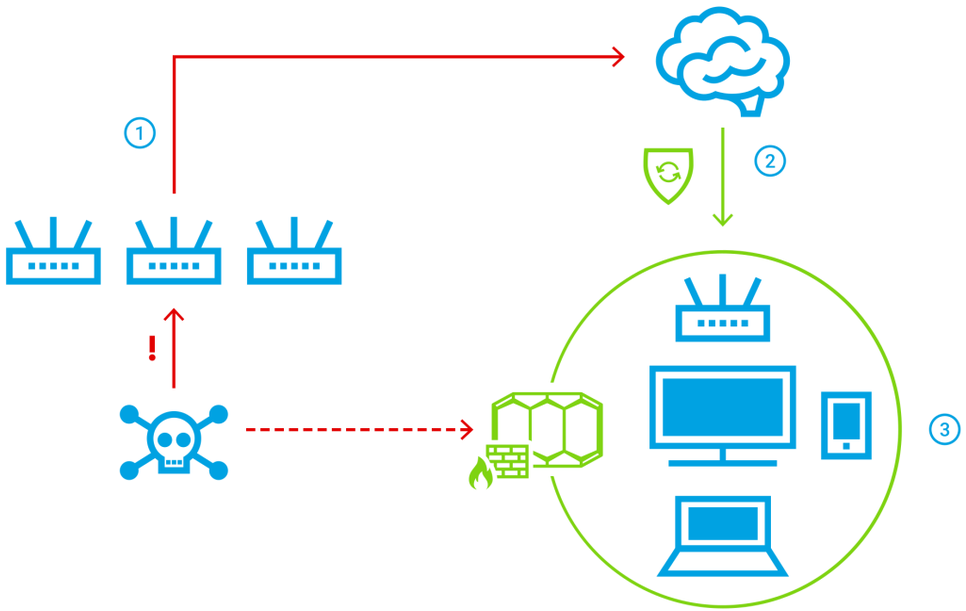
⇒ It is really easy to do PoC!

TURRIS

Back to the security research

Turris Sentinel

- nowadays opt-in
- minimal honeypots
  - http, telnet, smtp, ftp
- ssh honeypot (on CZ.NICs servers)
- firewall logs
- dynamic firewall
  - https://view.sentinel.turris.cz

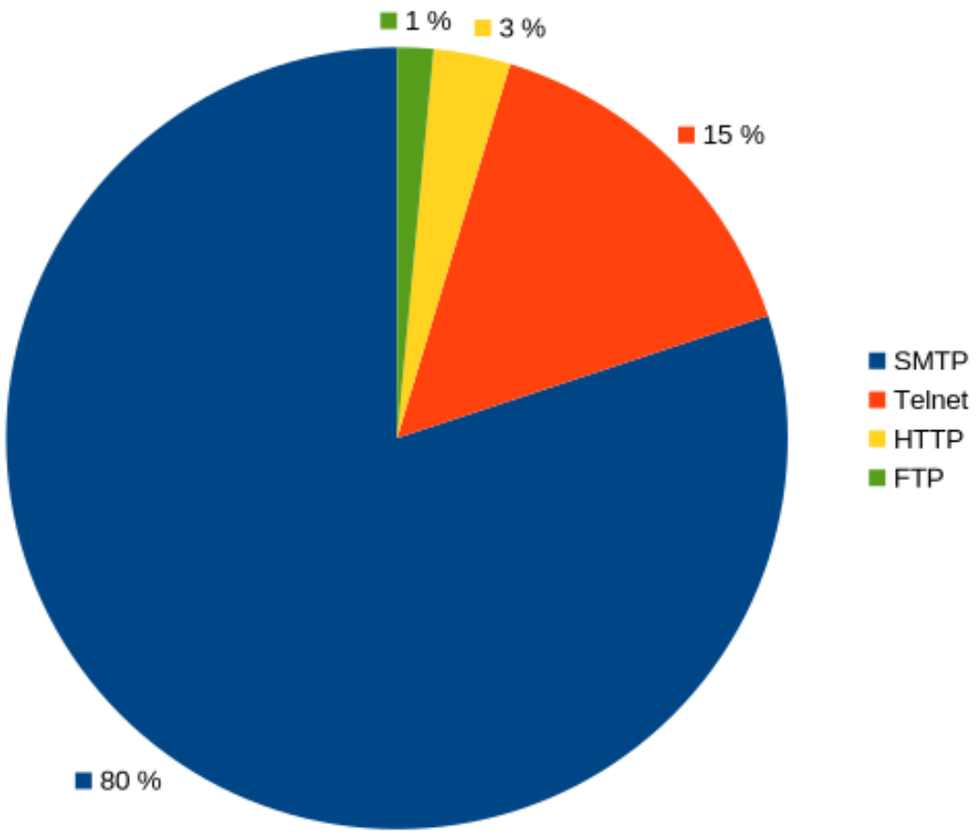


TURRIS

Statistics - protocols

- 22 millions of incidents on average every day
  - 15 thousands incidents every minute

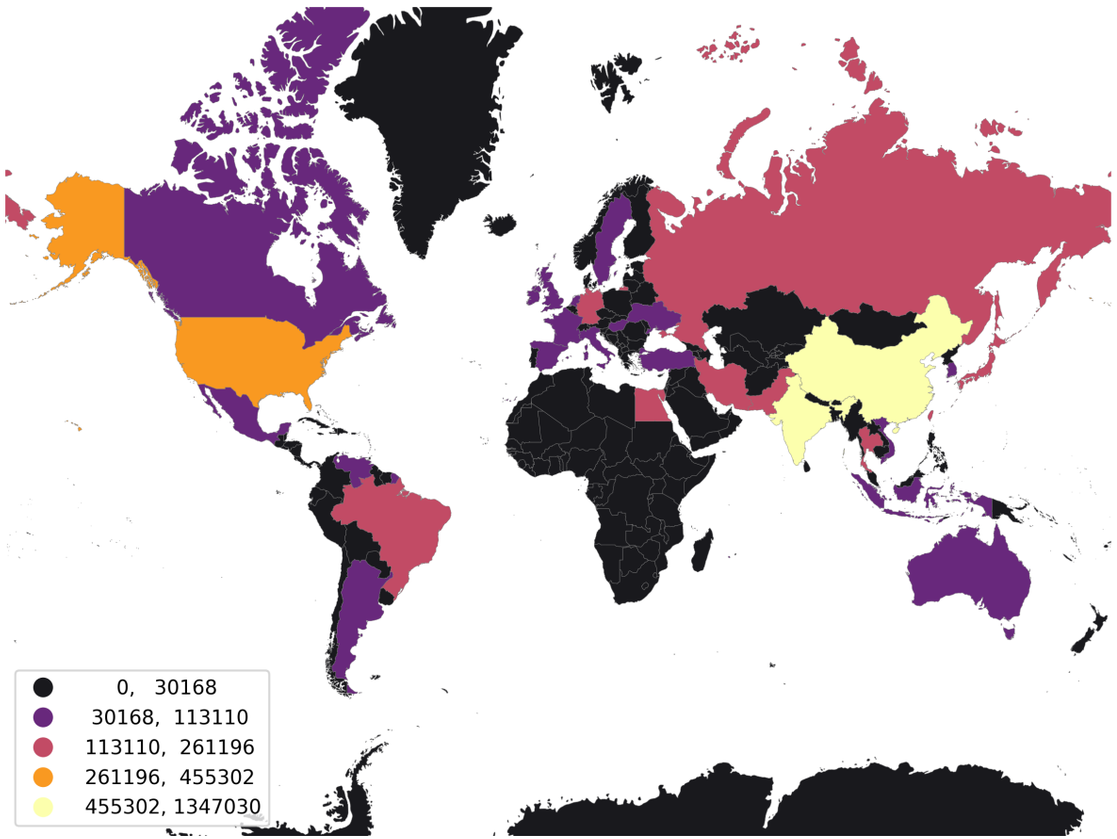
SMTP	18M	80%
Telnet	3M	15%
HTTP	723K	3%
FTP	339K	1%
Firewall	79K	0%



TURRIS

Statistics - countries

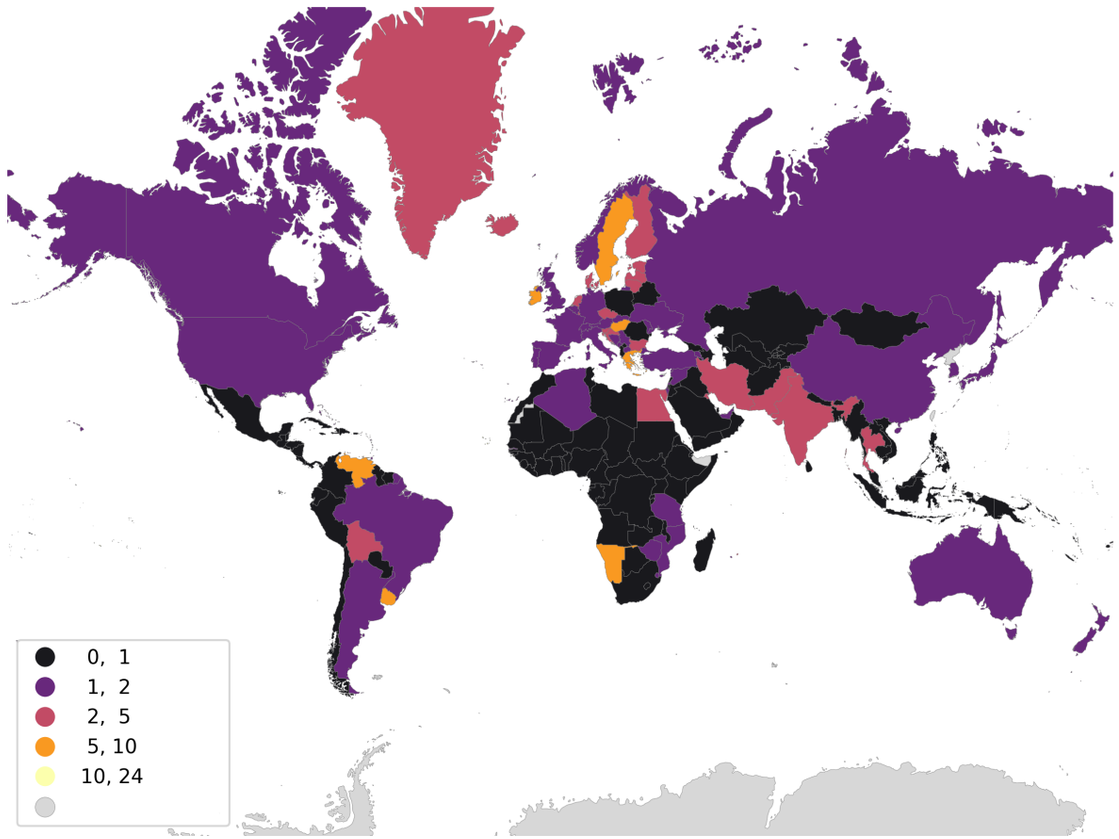
India	1347030
China	1102045
United States of America	455302
Brazil	261196
Taiwan	209389
Russian Federation	201878
Iran, Islamic Rep.	187923
Pakistan	180951
Egypt, Arab Rep.	176974
Thailand	136586
Germany	134941



- Czech republic is 35th, Sweden 20th

Statistics - countries relatively

Hong Kong SAR, China	8.597
Seychelles	8.463
Ireland	8.256
Namibia	7.608
Uruguay	6.655
Venezuela, RB	6.439
Sweden	6.182
Hungary	5.775
Finland	5.046
Netherlands	3.889



- Czech republic is 23rd, Sweden 7th

TURRIS

IPv6 attacks

- based on data from 1st of January till 13th of March
- about one third of the updates is done over IPv6
- 1 666 820 unique attackers (IPv4 + IPv6)
  - 1 070 unique /64 prefixes
  - 0,0642 % = 0,642 ‰ attacks come from IPv6

⇒ Want to be secure? Use IPv6!

End of IPv4 in Czechia is already set: 6. 6. 2032 💣

TURRIS

Check it out!

https://view.sentinel.turris.cz

TURRIS

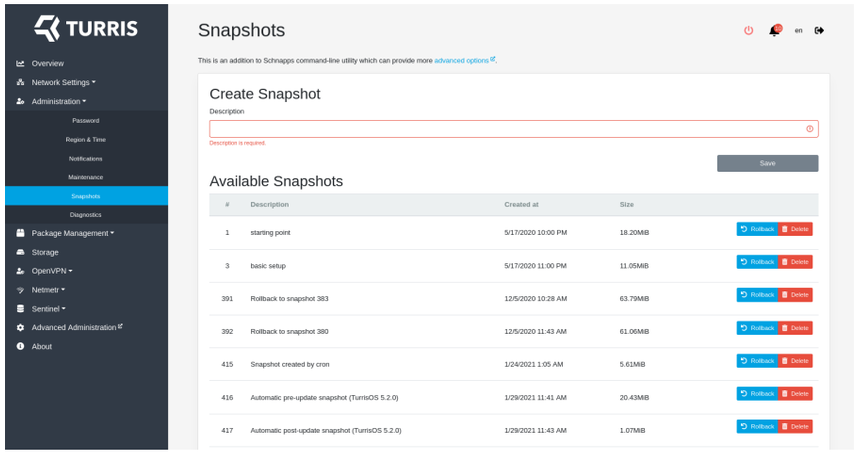
Turris OS

- OpenWRT based
  - optimized for small devices with limited resources
  - nice functionality for routers
- much simpler web interface reForis
  - advance functionality in an end-user-friendly way
  - simple OpenVPN server setup
  - guest network
  - …
- updater and automatic updates
- few extra integration bits

TURRIS

Btrfs

- used to be the "coolest" filesystem
- our filesystem of choice
- we are using snapshots heavily
  - automatic snapshots before update
  - automatic snapshots once a week
  - possibility to create a manual snapshot
  - rollback either using CLI or by pressing reset button
  - possibility to export locally or to remote location
- easy way to implement RAID
  - we made WebUI to format external drives



TURRIS

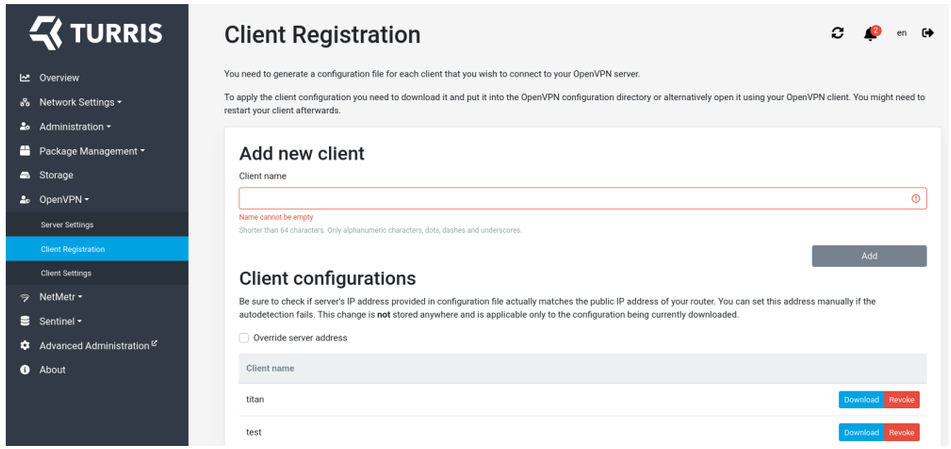
OpenVPN

Server

- great functionality to have
- CA is PITA to manage
  - we integrated CA management
  - one click to generate new keys
  - configs with embedded keys

Client

- could be useful
- simple to switch between multiple configs



TURRIS

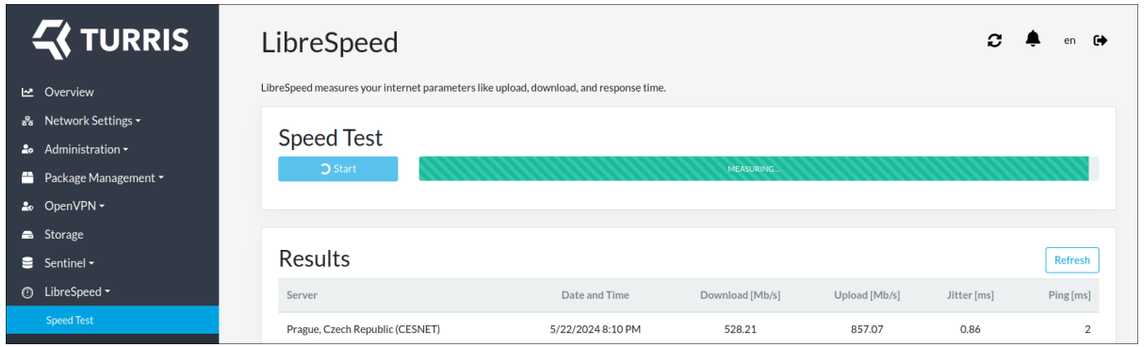
Nextcloud

- easy openvpn support
- RAID configuration in Web UI
- automatic updates
- Nextcloud packages ready
- WebUI to format and mount a drive
  - used for data storage and database

⇒ Sounds like a good platform 🤔

⇒ Nextcloud installation in Web UI

LibreSpeed



- open source bandwidth tester
- community servers around the world
  - Helsinki, Amsterdam, New York, Las Vegas, Tokyo, Prague, ..
  - automatically selects the best one to test against
- easy to deploy and maintain server
- easy to use and integrated into router

TURRIS

Pakon

- netflow monitoring
- overkill, but ATM uses Suricata to get information from TLS and DNS
- uses cotrack for the netflow monitoring and statistics
- collects, stores and aggregates traffic information
- displays it in CLI or in a web interface
- alerts you when new computer connects to your network
- exportable as CSV

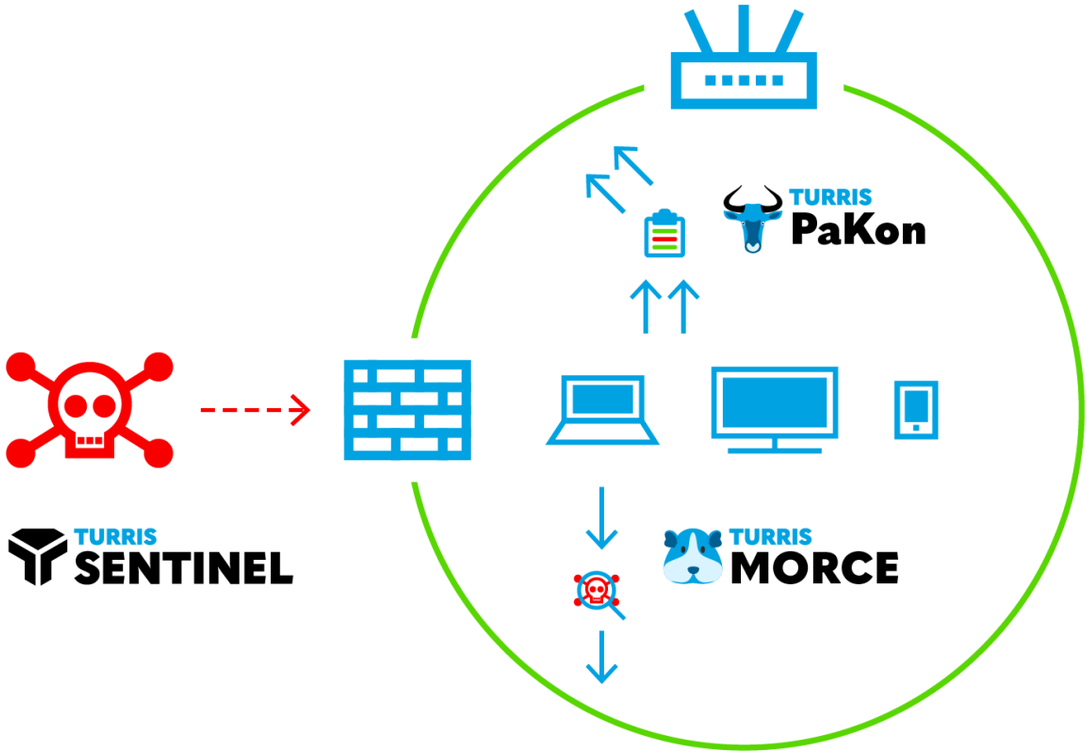
TURRIS

Morce

- integration of Snort
- early PoC phase
  - extended capabilities of plugins
  - integrated management of the rules
  - listens for suspicious traffic
  - sends notificiation/e-mail
  - stores data for further processing/evaluation

TURRIS

Security in general



TURRIS

Future of Turris

Turris Omnia NG

- 4 x 2,2 GHz
- 2 x 10 GBps SFP+
- 4 x 2.5 GBps RJ45
- 2G RAM
- 5G ready
- coming in fall 2025
- bellow 500 USD

Thank you

Few useful links

🐘 @turris@fosstodon.org

https://www.turris.cz

https://view.sentinel.turris.cz

https://docs.turris.cz

https://gitlab.labs.nic.cz/turris

https://mailing-turris.nic.cz

TURRIS