

Turris

Our path to open-source routers

Michal Hrušecký • Michal.Hrusecky@turris.com



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

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 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!

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



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

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

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

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.



How we got B2B customers?

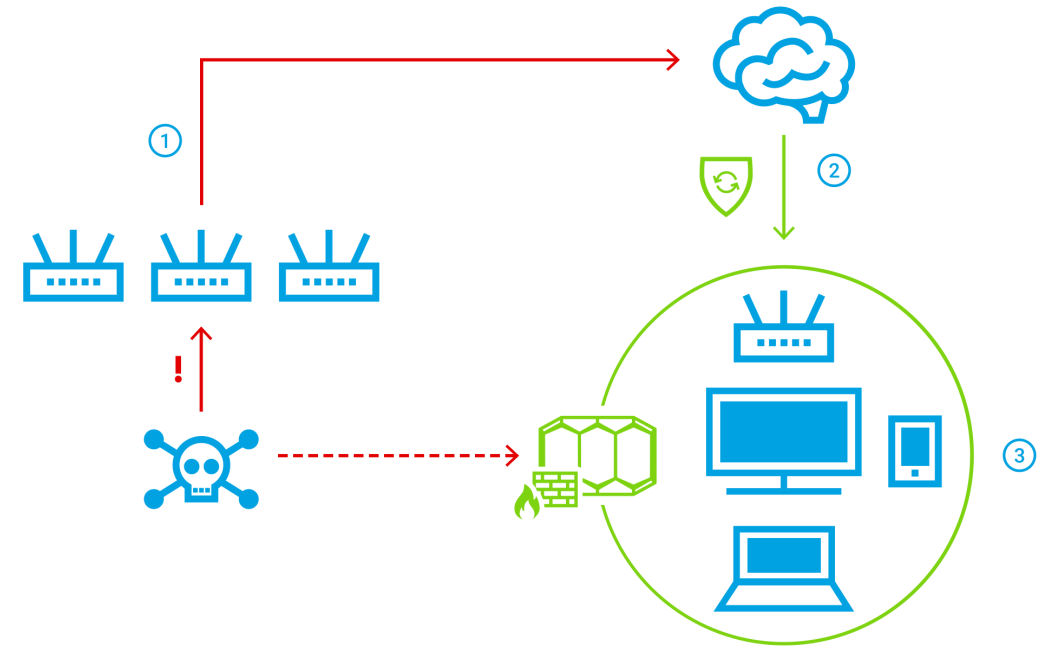
- we had a man inside 🤫
- we have good enough hardware
- we are open source and push our support to vanilla
 - you don't need a SDK
 - you don't NDA
 - you can take whatever you have and port it easily

⇒ It is really easy to do PoC!

Back to the security research

Turris Sentinel

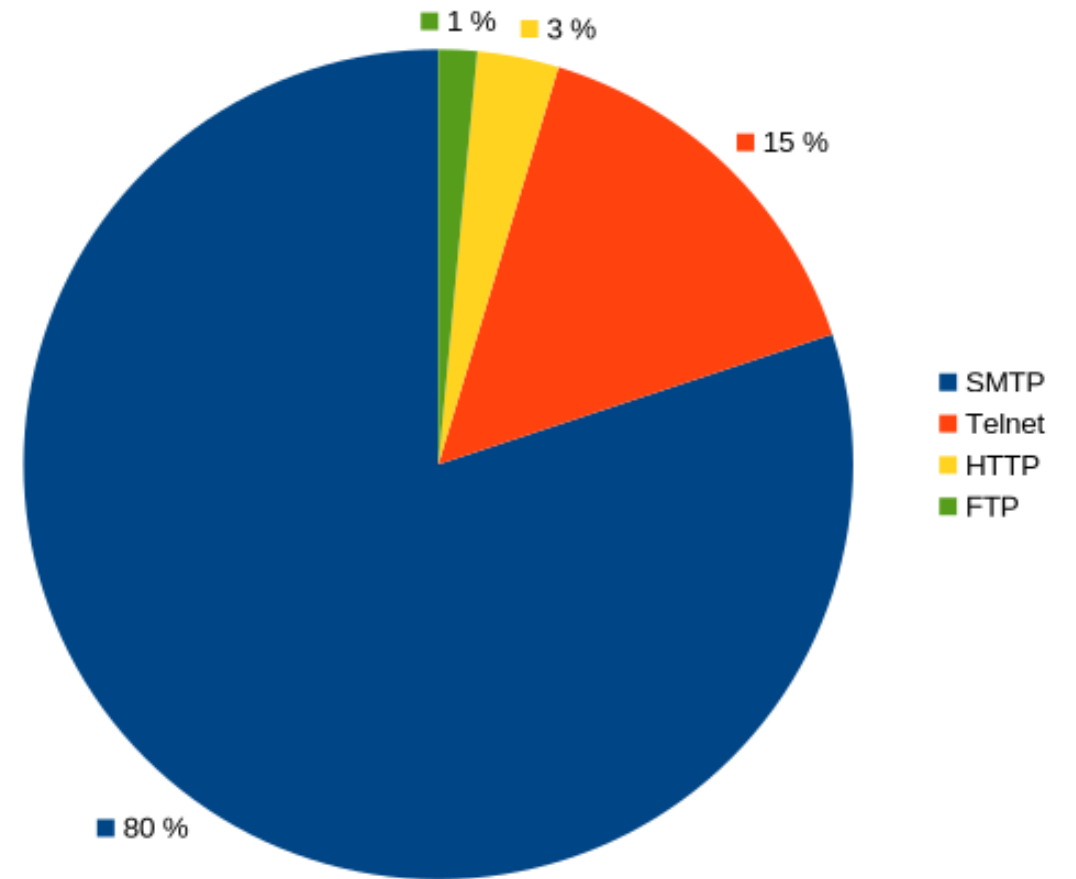
- nowadays opt-in
- minimal honeypots
 - http, telnet, smtp, ftp
- ssh honeypot (on CZ.NICs servers)
- firewall logs
- dynamic firewall
 - <https://view.sentinel.turris.cz>



Statistics - protocols

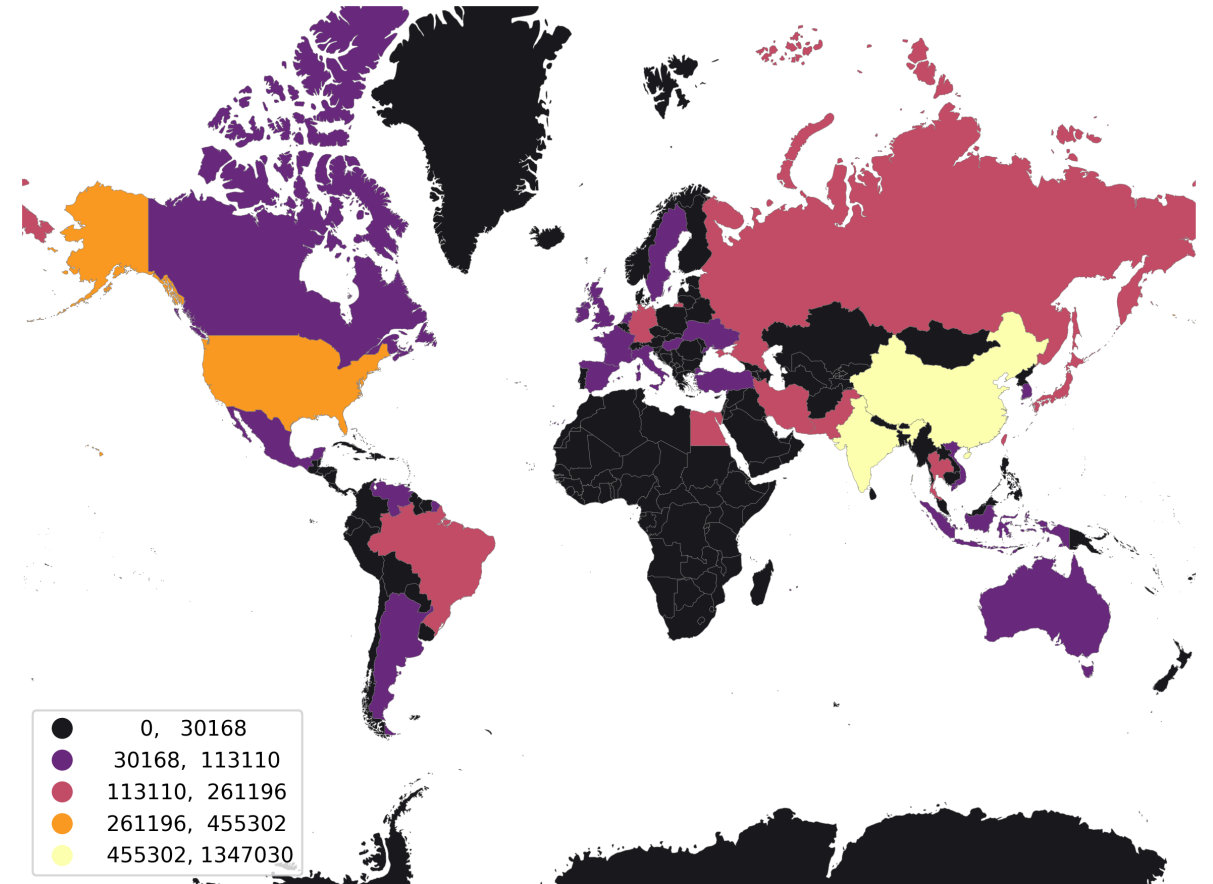
- 22 millions of incidents on average every day
 - 15 thousands incidents every minute

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



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

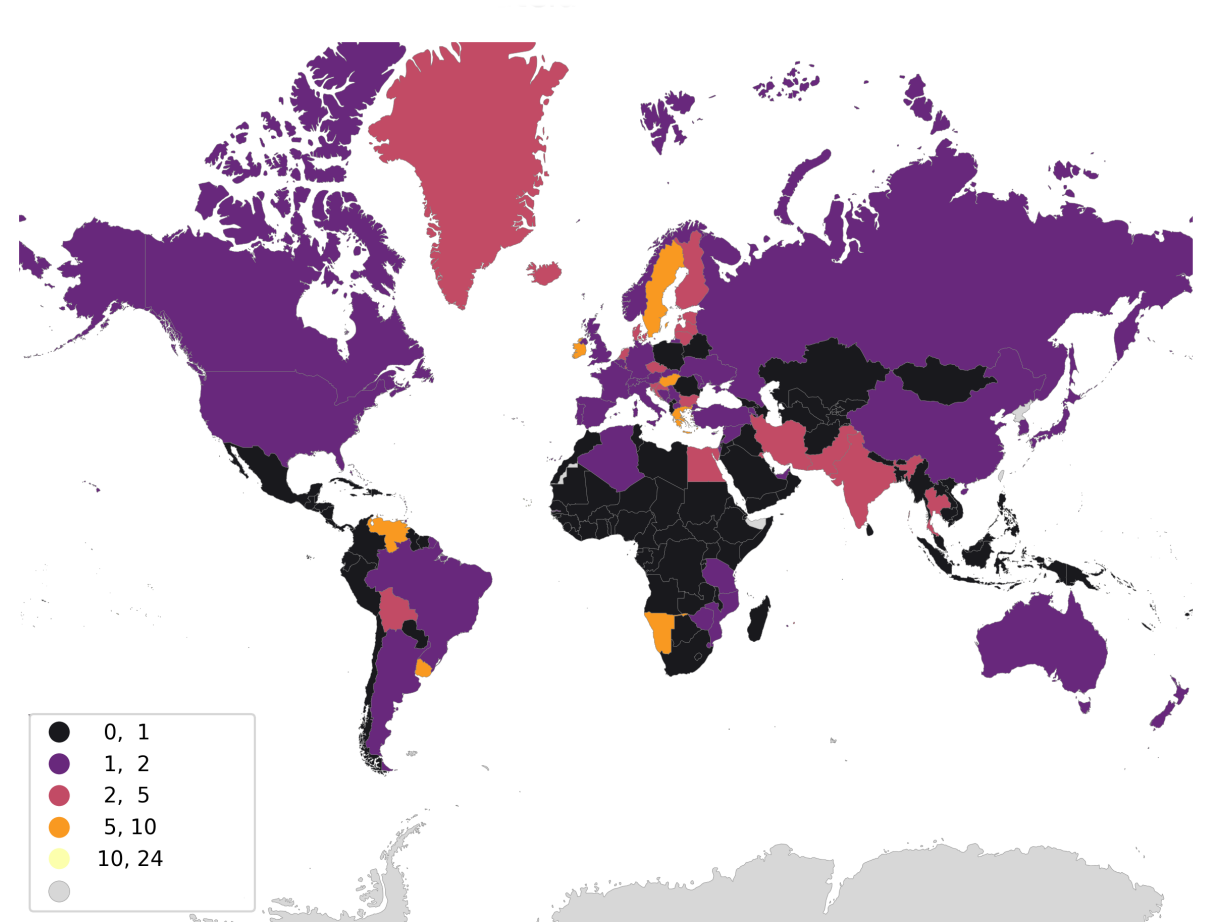


- Czech republic is 35th, Sweden 20th

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



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 💣

Check it out!

<https://view.sentinel.turris.cz>

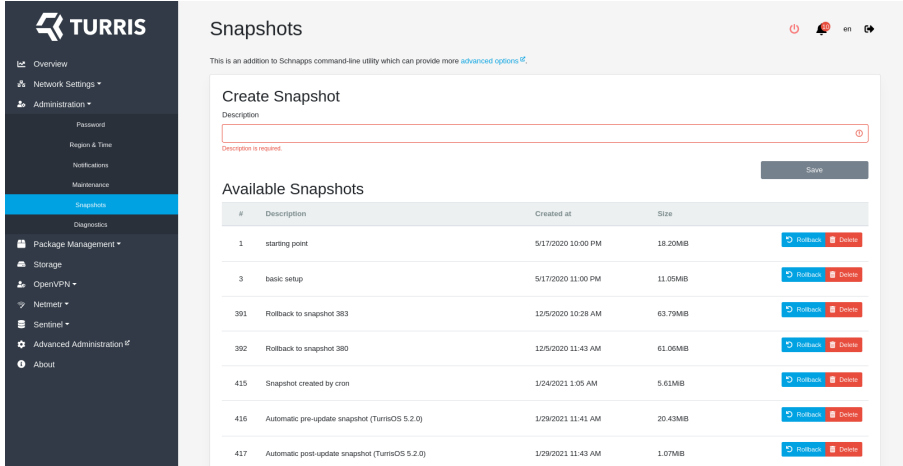


Turris OS

- 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

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



The screenshot shows the TURRIS web interface for managing snapshots. On the left is a dark sidebar with navigation options: Overview, Network Settings, Administration, Password, Region & Time, Notifications, Maintenance, Snapshots (highlighted), Diagnostics, Package Management, Storage, OpenVPN, Netmeter, Sentinel, Advanced Administration, and About. The main content area is titled 'Snapshots' and contains a 'Create Snapshot' form with a 'Description' field and a 'Save' button. Below the form is a table of 'Available Snapshots' with columns for ID, Description, Created at, and Size. Each row has 'Rollback' and 'Delete' buttons.

#	Description	Created at	Size	Rollback	Delete
1	starting point	5/17/2020 10:00 PM	18.20MB	Rollback	Delete
3	basic setup	5/17/2020 11:00 PM	11.05MB	Rollback	Delete
391	Rollback to snapshot 383	12/5/2020 10:28 AM	63.79MB	Rollback	Delete
392	Rollback to snapshot 380	12/5/2020 11:43 AM	61.00MB	Rollback	Delete
415	Snapshot created by cron	1/24/2021 1:05 AM	5.61MB	Rollback	Delete
416	Automatic pre-update snapshot (TurrisOS 5.2.0)	1/29/2021 11:41 AM	20.43MB	Rollback	Delete
417	Automatic post-update snapshot (TurrisOS 5.2.0)	1/29/2021 11:43 AM	1.07MB	Rollback	Delete

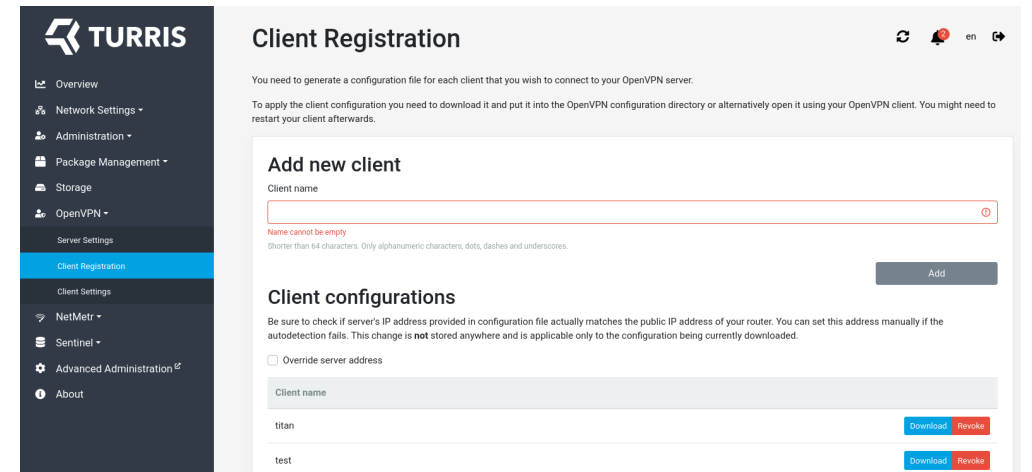
OpenVPN

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



The screenshot shows the TurrIS web interface for Client Registration. On the left is a dark sidebar with the TurrIS logo and a navigation menu including Overview, Network Settings, Administration, Package Management, Storage, OpenVPN, Server Settings, Client Registration (highlighted), Client Settings, NetMet, Sentinel, Advanced Administration, and About. The main content area is titled 'Client Registration' and contains instructions: 'You need to generate a configuration file for each client that you wish to connect to your OpenVPN server. To apply the client configuration you need to download it and put it into the OpenVPN configuration directory or alternatively open it using your OpenVPN client. You might need to restart your client afterwards.' Below this is a form to 'Add new client' with a 'Client name' input field. A red error message states 'Name cannot be empty' and 'Shorter than 64 characters. Only alphanumeric characters, dots, dashes and underscores.' An 'Add' button is to the right. Underneath is a 'Client configurations' section with a warning: 'Be sure to check if server's IP address provided in configuration file actually matches the public IP address of your router. You can set this address manually if the autodetection fails. This change is not stored anywhere and is applicable only to the configuration being currently downloaded.' There is an unchecked checkbox for 'Override server address'. Below are two rows of client configurations: 'titan' and 'test', each with 'Download' and 'Revoke' buttons.

Nextcloud

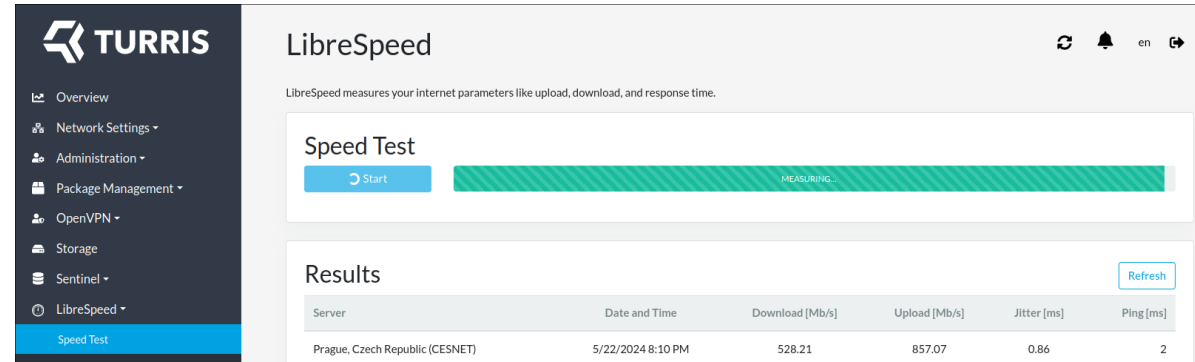
- easy openvpn support
- RAID configuration in Web UI
- automatic updates
- Nextcloud packages ready
- WebUI to format and mount a drive
 - used for data storage and database

⇒ 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

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

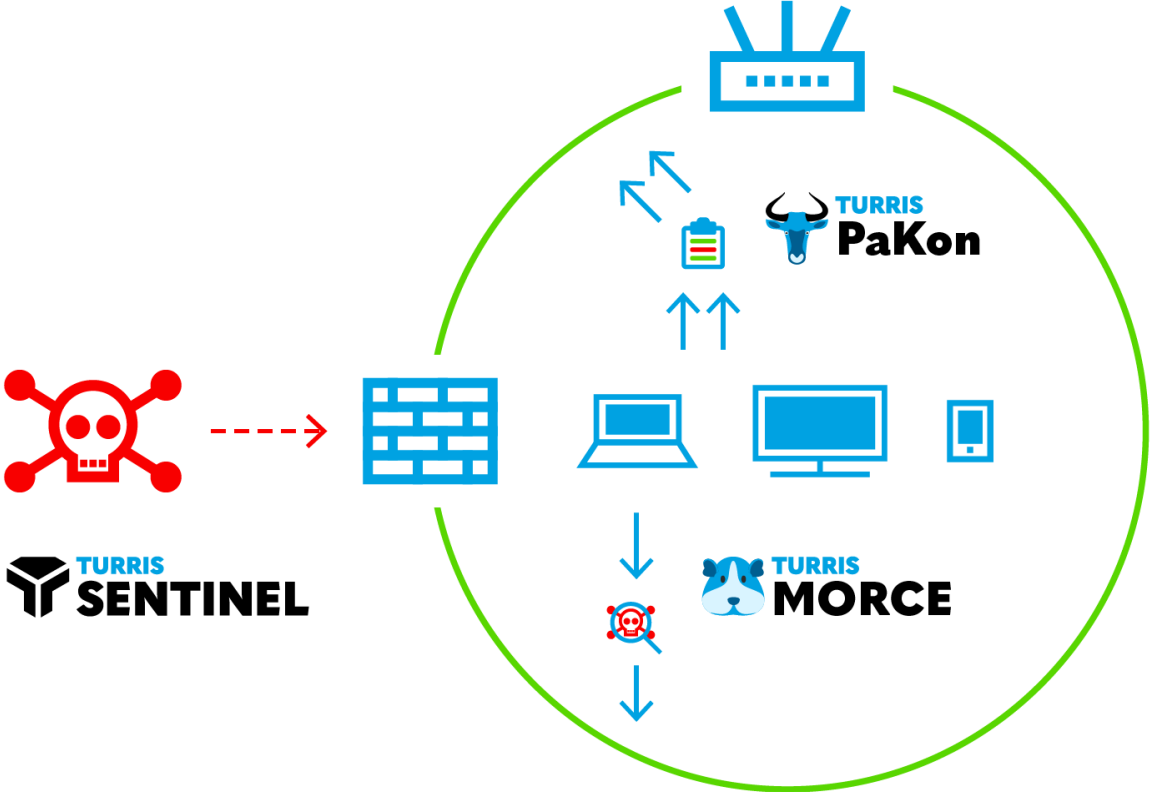


Morce

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



Security in general



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
- below 500 USD



Thank you

Few useful links

 [@turris@fosstodon.org](mailto: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>