Project Turris

http://www.turris.cz/en/

PROJECT:
TURRIS

Ondřej Filip • 12 May 2014 • RIPE 68 • Warsaw

CZ.NIC, CZ.NIC Labs

- Domain name registry - .cz
  - 1.1M, 35% DNSSEC
- Project for local and global community

Knot DNS

Project Turris - motivation

- Started in 2013 – project of shared cyberdefence
- Main goals
  - Security research
  - End user security
  - Improve the situation of SOHO routers

Project Turris - motivation

- Security research
  - Currently – Honeynet, DNS anomaly detection
  - Probes close to end users
  - Distributed in many networks
  - IP(v4/6) Anomaly detection
- End user security
  - Adaptive firewall based on collected data
  - Feed for CERT team (CSIRT.CZ)

Problems of current CPE devices

- SOHO routers
  - No or very bad support of IPv6
  - Problems with DNS, DNSSEC, no validation
  - No support for third party applications – app store
  - Limited security features
  - No automated software upgrades
  - Current security issues

Data collection - probes

- Distribute 1000 probes - SOHO routers to end users for free (lease for 1 CZK/3Y = 0,03 EUR/3Y)
- Probe – powerful enough to forward 1Gbps of traffic with analysis – no HW found on the current market => HW development
- Additional features to increase value for end users

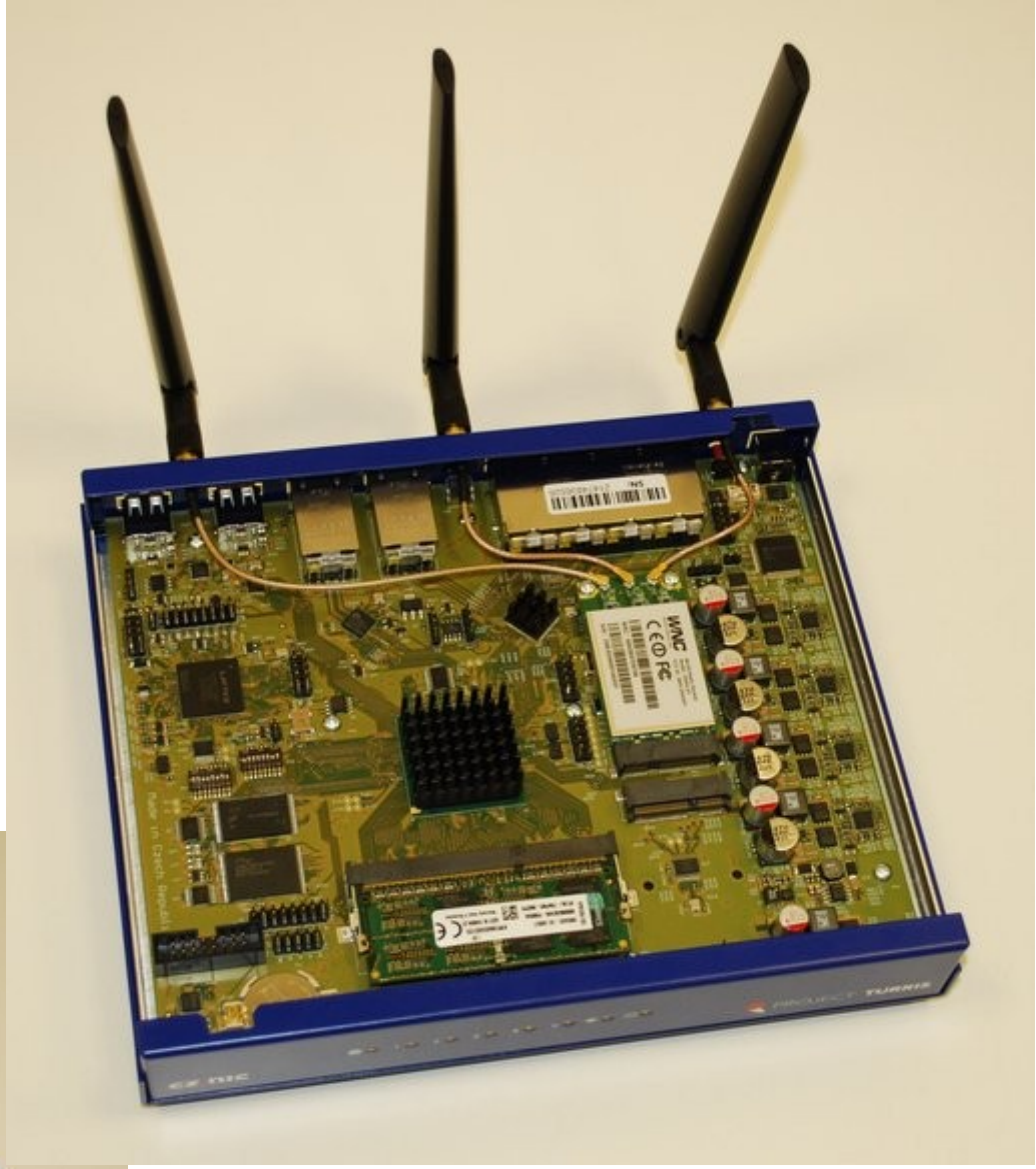
Router Turris

- Developed from scratch
- 1000 pcs – produced in Czech Republic
  - Freescale 1.2 GHz dual core (PPC)
  - 2 GB DDR memory – slot
  - 256 MB NAND + 16 MB NOR flash
  - 5x LAN – 1 Gbps ports (Ethernet switch with 7 ports - 2 Gbps lines to CPU)
  - 1x WAN – 1 Gbps port (directly to CPU)

Router Turris

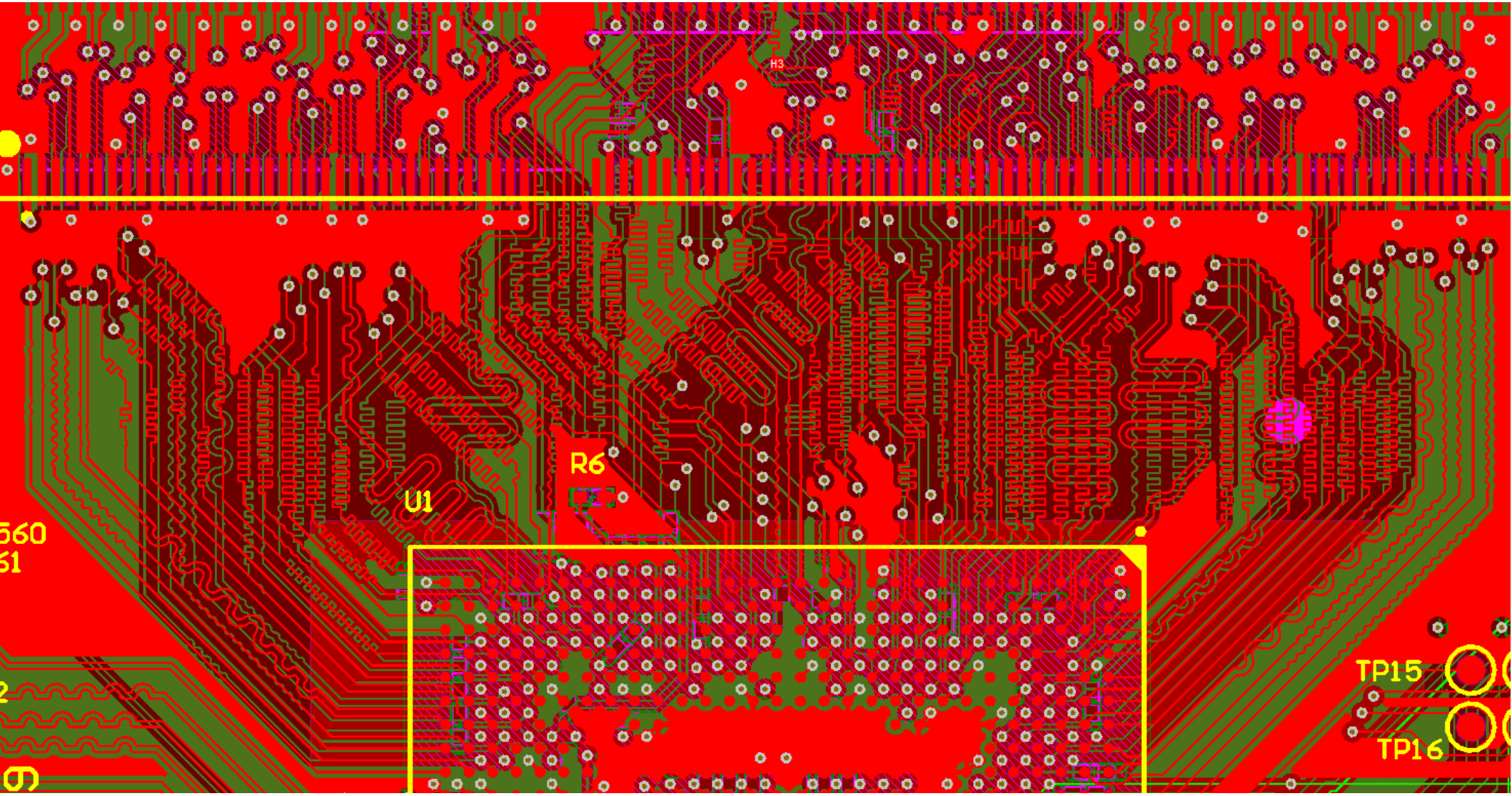
- 2x miniPCIe (1 occupied by WiFi)
- WiFi 802.11 a/b/g/n – 3x3 MIMO
- 2x USB 2.0
- UART, SPI, I2C, GPIO
- Free microSHDC slot
- Low power consumption – 9-14 W
- Open source license

Router Turris

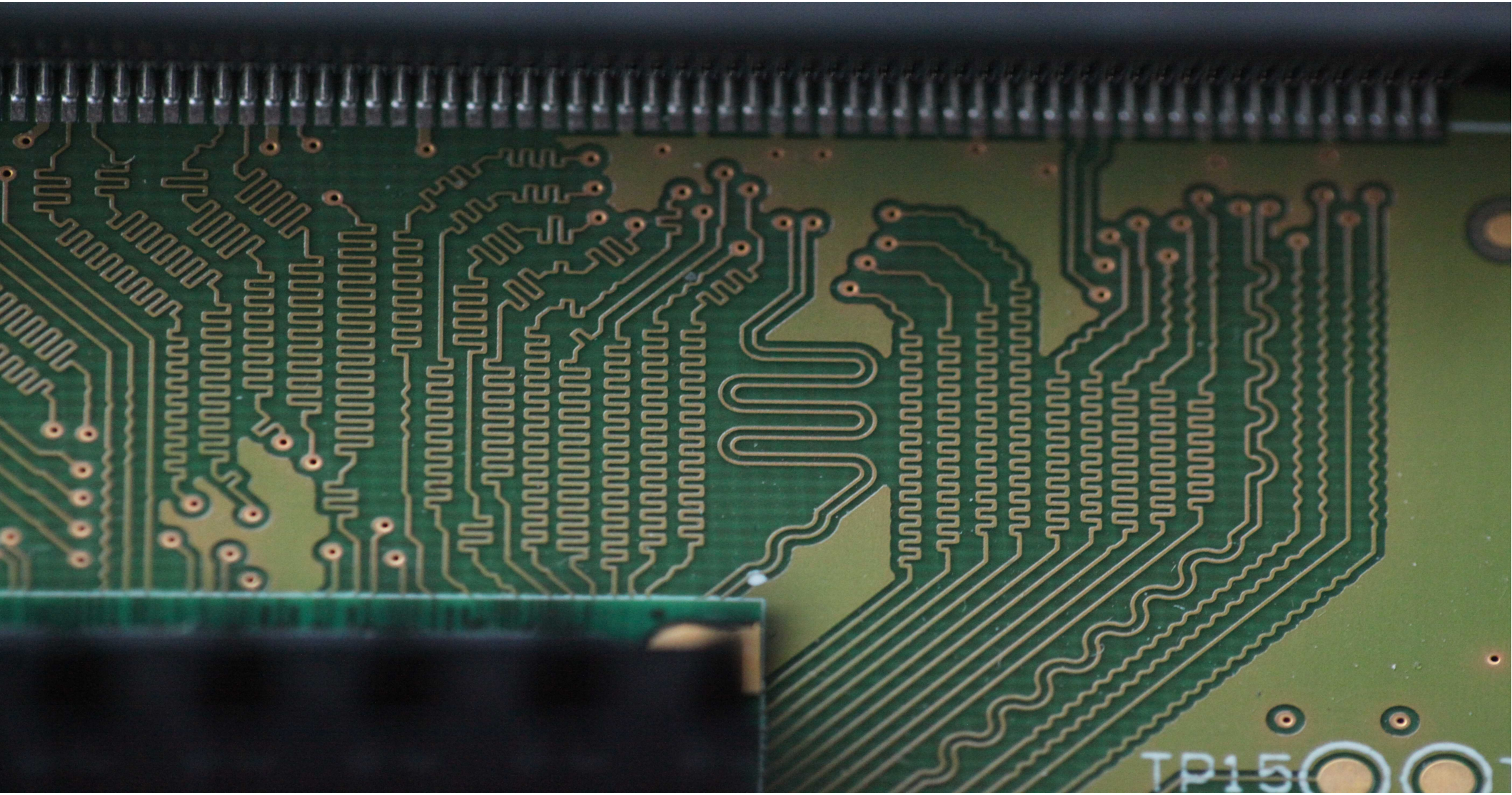


cz.nic | CZ DOMAIN REGISTRY

Router Turris



Router Turris



Router Turris – killer feature

- LED brightness intensity tunable (!)
  - Software managed (RGB)
  - Button at the back
  - :-D

Router Turris - software

- Based on OpenWRT – open source
- Own configuration wizard – based on NETCONF
- Automatic updates – user can avoid certain time periods
- Encrypted communication with central server
- Data collector – only mandatory process
- IPv6, DNSSEC, passwords, ...
- Android application

Router Turris - usage

- Network testing
  - Reachability tests (ping, RTT)
  - Protocol specific
  - Speed measurement
- Other research - planned
  - Discussion with universities, security researchers (agreement limits)

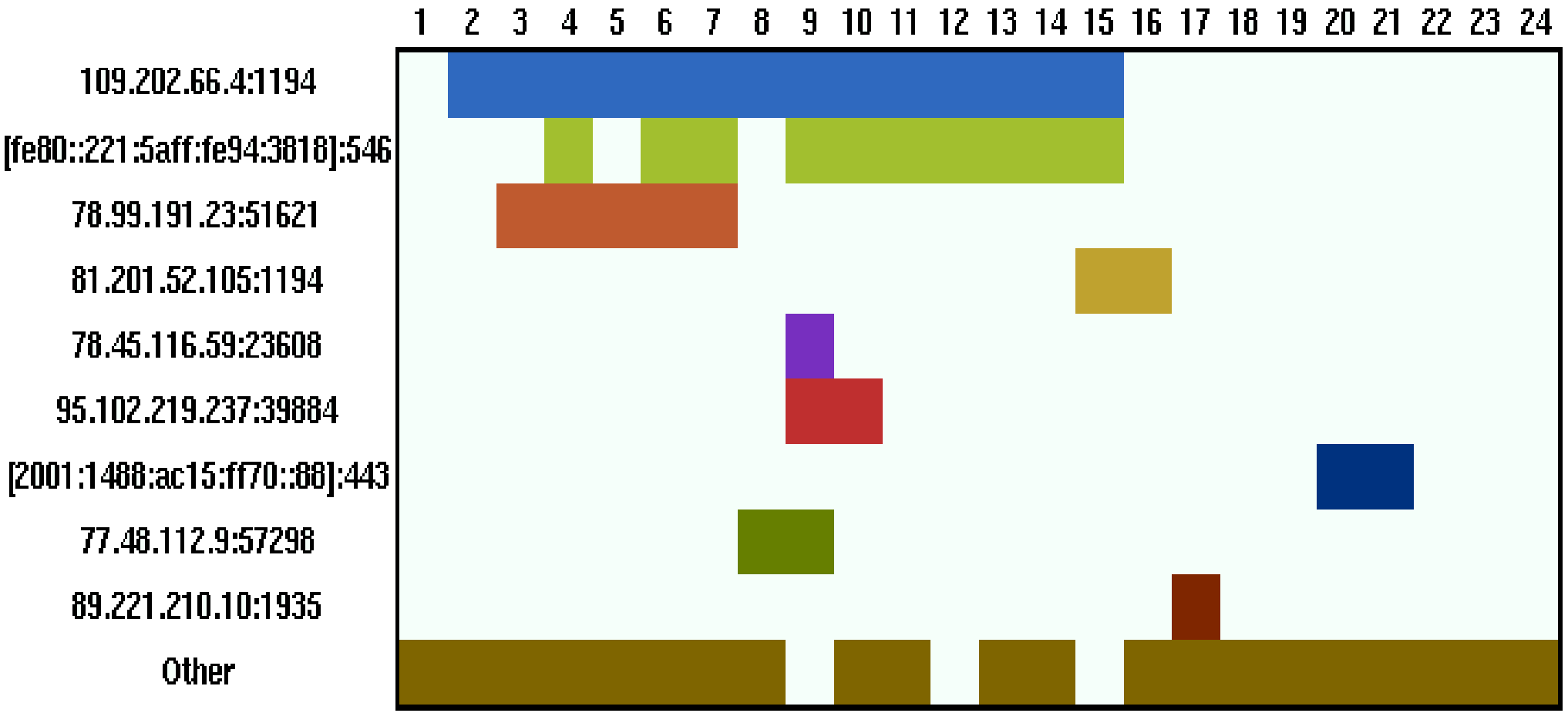
Data collection

- µCollect
  - Basic stats, PCAP stats, anomaly detection
- Firewall logs
- Router logs - upgrade status, SW problems
- Other measures – temperature, load, memory and flash utilization etc.

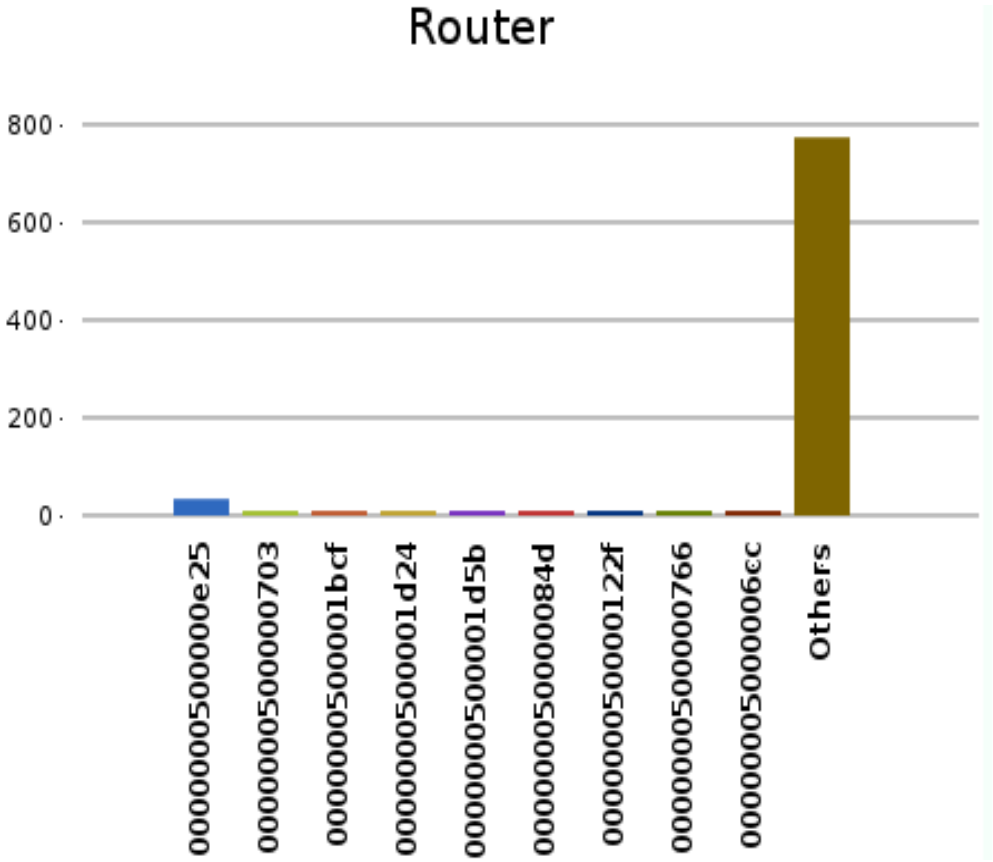
Data collection - µCollect

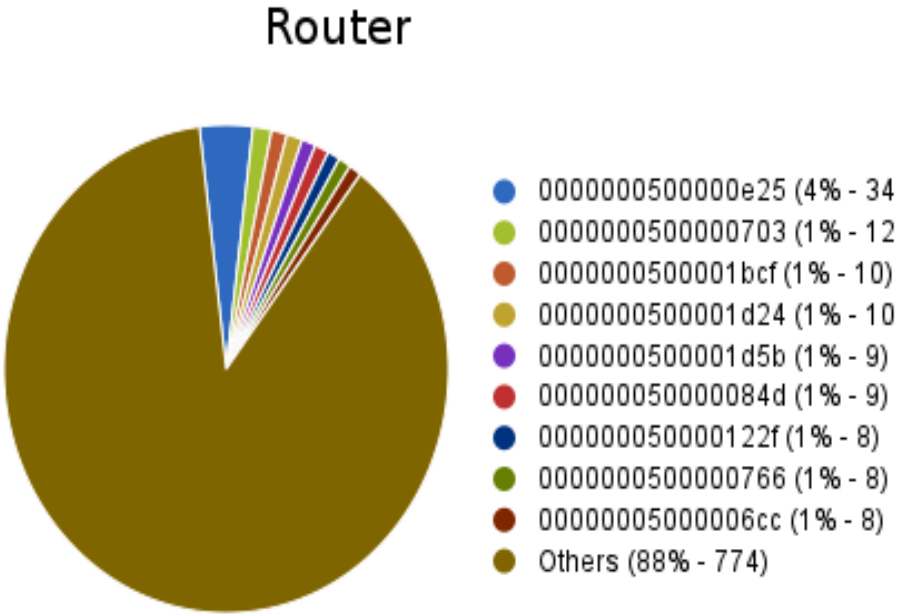
- Modular system for data collection and reporting
  - Module "count" – TCP/UDP/.. stats - displayed on portal
  - Modules “buckets“ - IP anomaly detection
    - Hashed by multiple functions
    - Central server tries to find anomaly
- Send – secure way – crypto HW – into central repository

Data collection - µCollect

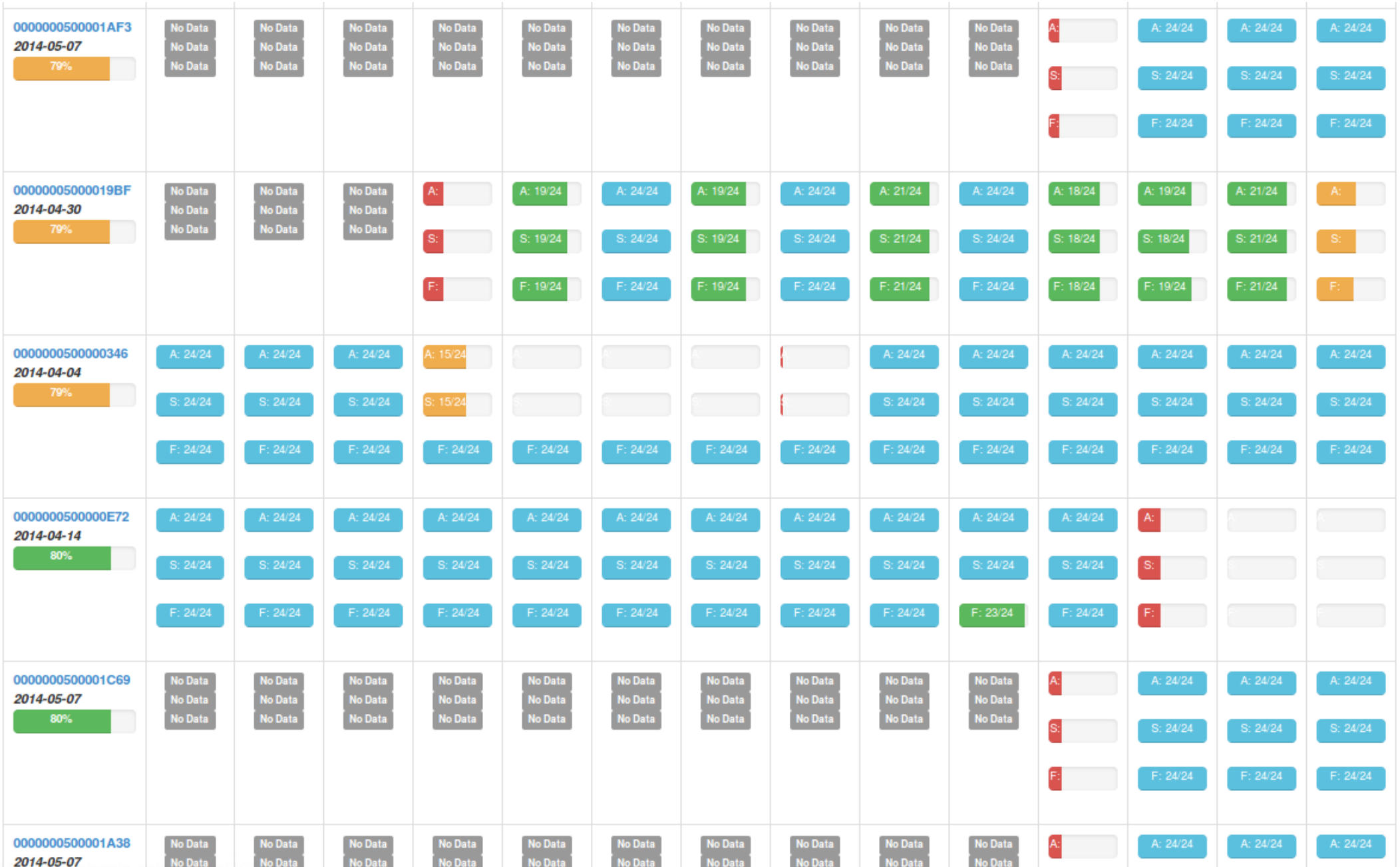


Data collection - µCollect





Data collection - µCollect



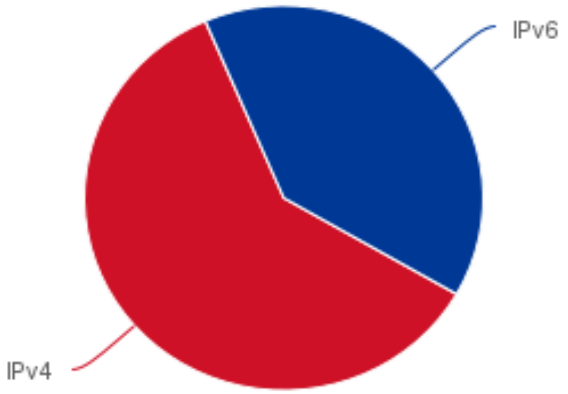
End user portal

- Communication with users
- Graphs
- Tutorials
- End user forum – very active

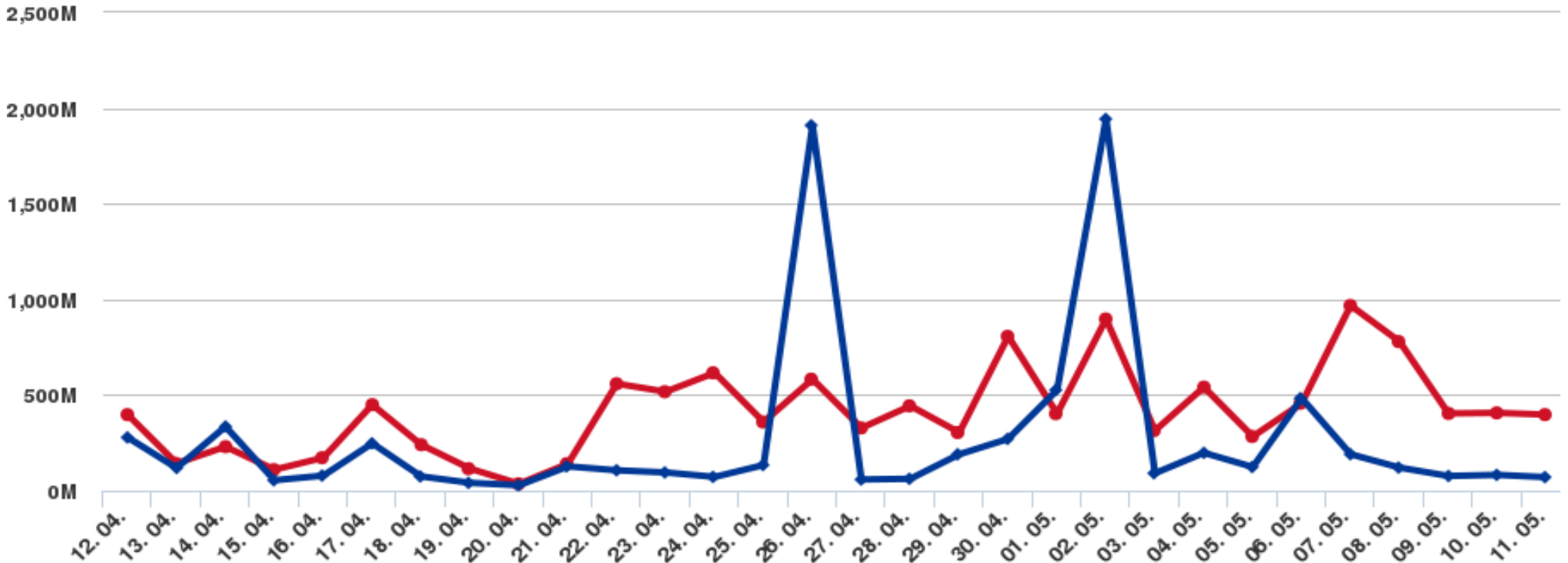
End user portal

Statistics - IPv4 vs. IPv6 (size)

CSV



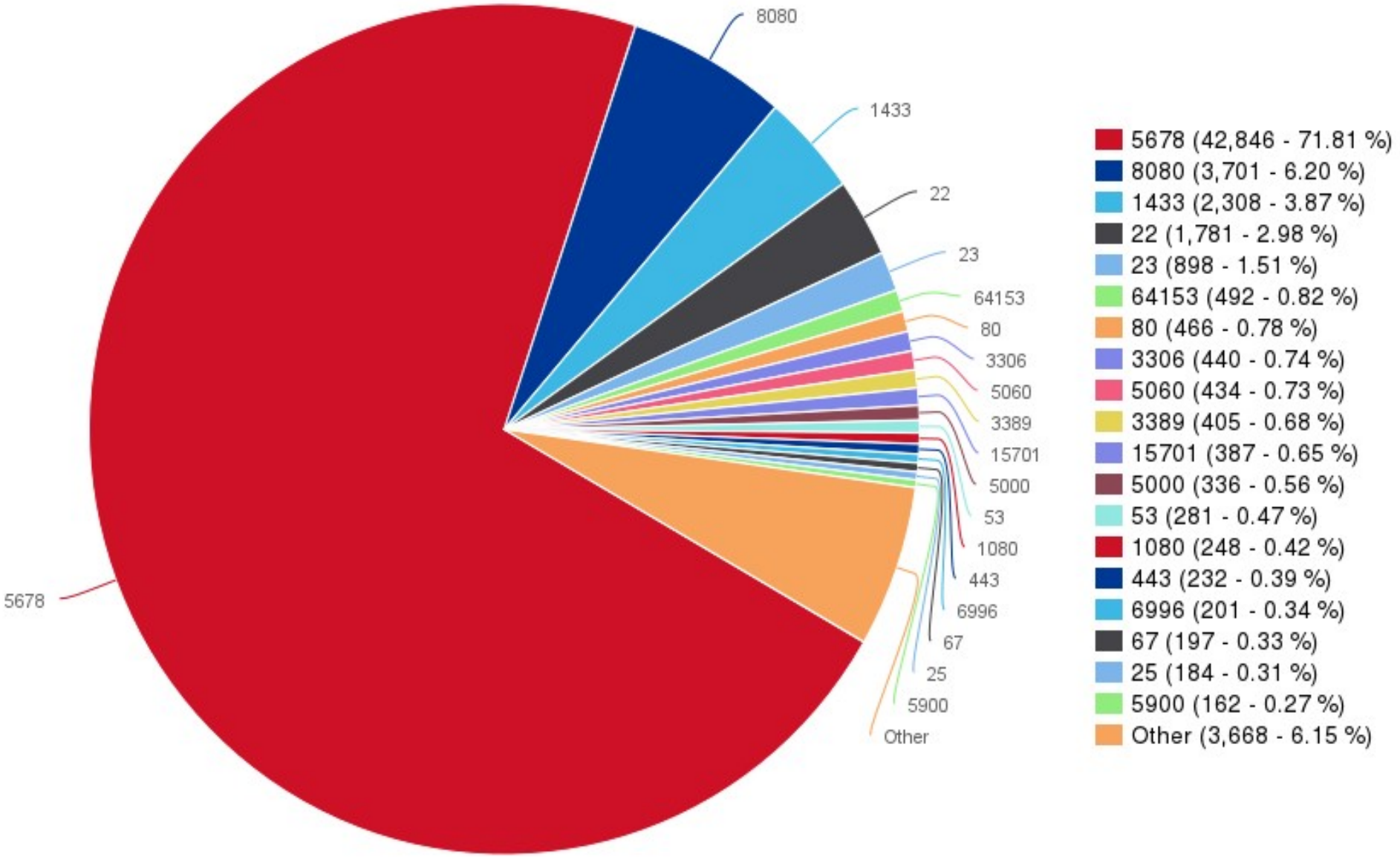
IPv4 (12.41 GB - 60.23 %)
IPv6 (8.19 GB - 39.77 %)



End user portal

Logged firewall packets - Target port

CSV



End user agreement

- Leasing, 3Ys + selling off
- Main router connecting to the Internet
- No switch off – non stop operation
- Open access – SSH + root
- Free modification except data collection and communication with central servers

Privacy issues

- Agreement
- Separate DB for account an data
- ISO27001
- Consulted with personal data protection authority
- POSITIVE Big Brother Awards CZ 2013
- Open Source
- Packet headers, data retention

Status

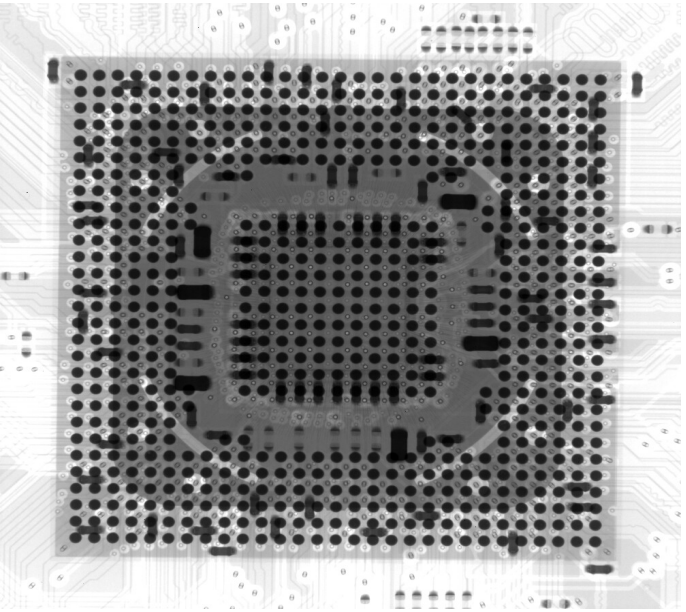
- 55% distributed to end users (>4000 requests)
- Distributing about 100 per week
- OS improvements – small incremental updates and one larger (OS version 1.1)
- Central portal improvements
- Tutorials – Turris as NAS, DLNA, VPN concentrator, multi WAN setup, 3G backup, VLAN setup, ...

Status

- Improving detection methods – calibration of the sensors
- Some IP scanners detected – portscanners, NTP, DNS scanners
- Checking flows to well known botnet C&Cs
- Publishing grey and black list
- Filtering some IPs based on CSIRT.CZ information

Future

- Another batch of 800 routers this year
- VDSL interface – small dongle
- SW improvements – OS + collection
- Universal OS for SOHO routers
  - Market
- Sweet to the end users – HW upgrades, tutorials – e.g. camera, smart home



Thank You!

PROJECT: TURRIS

Ondřej Filip • ondrej.filip@nic.cz • http://www.turris.cz

CZ DOMAIN REGISTRY