

# DNSSEC Validation at CPE

## What we learnt from Project Turrís



Ondřej Filip • 14 Mar 2018 • ICANN61 • San Juan



# Project Turris

- Started in 2013 – project of shared cyber defence
- Security research, improve the situation of SOHO routers
- First two generations – Turris 1.0 and Turris 1.1 – (2x1000) mainly in Czech Republic
- Later crowdfunding campaign – Turris Omnia



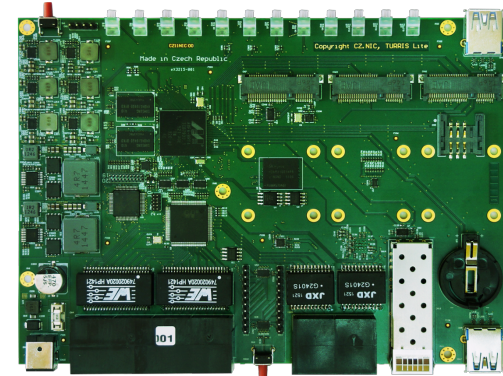
# Turris 1.0



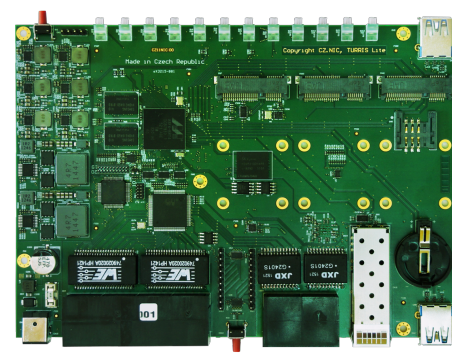
# Turris 1.1



# Turris Omnia



# Turris Omnia



- Open source SW & HW, powerful HW
- Turris OS - (based on OpenWRT) – **automated updates** and security fixes
- Secure configuration – crypto chip
- Many security features – honeypots, flow analysis, adaptive firewall, VPNs, ...
- Many other features – IPv6, LXC, ...
- **DNSSEC validating resolver by default**




# Experience with DNSSEC validation

- At the beginning, things broke
  - Turris users & ISPs lacking DNSSEC support
  - Ability to get debug information is essential
- Main problem categories are
  - broken ISP infrastructure
    - broken DNS recursors at ISP
    - broken middleboxes modifying DNS traffic
    - hidden redirects port 53 to recursor
  - bugs in resolver software
  - broken authoritative servers (EDNS)



# Dealing with problems



HOME PAGE

PASSWORD

WAN

**DNS**

LAN

WI-FI

ADVANCED ADMINISTRATION

MAINTENANCE

UPDATER

DATA COLLECTION

ABOUT

ENGLISH | LOG OUT

## DNS

Router Turris uses its own DNS resolver with DNSSEC support. It is capable of working alone or it can forward your DNS queries through your internet service provider's DNS resolver.

The following setting determines the behavior of the DNS resolver. It is usually better to use the ISP's resolver in networks where it works properly. In case this does not work for some reason, it is necessary to use direct resolving without forwarding.

In rare cases ISP's have improperly configured network which interferes with DNSSEC validation. If you experience problems with DNS, you can **temporarily** disable DNSSEC validation to determine the source of the problem. However, keep in mind that without DNSSEC validation, you are vulnerable to DNS spoofing attacks! Therefore we **recommend keeping DNSSEC turned on** and resolving the situation with your ISP as this is a serious flaw on their side.

**Use forwarding**

**Disable DNSSEC**

[Save](#)

## Connection test

Here you can test your internet connection. This test is also useful when you need to check that your DNS resolving works as expected. Remember to click on the **Save** button if you changed your forwarder setting.

Test type	Status
IPv4 connectivity	✓ OK
IPv4 gateway connectivity	✓ OK
IPv6 connectivity	✓ OK
IPv6 gateway connectivity	✓ OK
DNS	✓ OK
DNSSEC	✓ OK

[Test connection](#)



# Summary

- Mostly upgrade/configuration problems at ISP
  - Usually "fix & forget" problems
- Configuration interface with built-in tests helps
  - Power users often can solve problem immediately
  - ISP could detect & report problems automatically
- Broken authoritative servers will get in trouble
  - Sunset of workarounds in resolvers during 2019
  - Test yourself! <http://ednscomp.isc.org/>



... and BTW





**THANK  
YOU!**



**Ondřej Filip**

**<http://www.turris.cz/en/>**

