



Co nového v Turrisu

Na čem jsme letos pracovali

Michal Hrušecký • michal.hrusecky@nic.cz

Miroslav Hanák • miroslav.hanak@nic.cz

Martin Prudek • martin.prudek@nic.cz

Turris OS 5.3

- vydán ve čtvrtek
- hlavní téma - lepší integrace Turris Sentinel
- poslední major release založený na OpenWrt 19.07
- poslední release s Forisem
 - dost možná ho už nemáte



Co zrušíme dál?

- Foris (úplně)
 - Server Side backups
 - Pakoň
- Turris OS 3.X
 - bude ale migrace
- portál project.turris.cz
 - máme Sentinel ;-)
 - máme sview



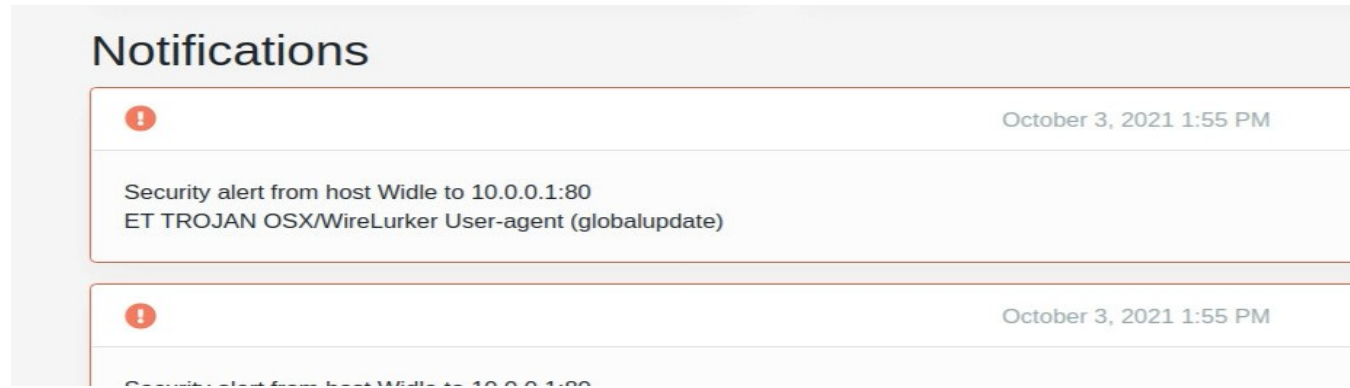
Na co se těšit? Pakoň!

- separátní web application
- nezávislá na Forisu/Turrisu
- CSV export
- nahradíme závislost na Surikatě
- časem bude i hezčí



Na co se těšit? Morče!

- další zvěřátko do sbírky
- integrace IDS do systému
- první krok - notifikace
- časem bude i log/přehled
- časem spojíme s Pakoňem a vymyslíme normální jméno
 - snad normální....



Na co se těšit? Migrace!

- začínáme po 5.3
- začneme postupně zapínat pro Omnie
- zapneme pro Turrisy 1.X s Btrfs

Co Turris 1.X bez karty?

- chystáme migraci na externí USB

Package lists



Migration to Turris OS 5.x (HIGHLY EXPERIMENTAL)

This is experimental migration to the latest version of Turris OS. Make sure that you thoroughly read https://docs.turris.cz/geek/tos3_migration/ before enabling this!



Omnia II

- nová vlajková loď
- víc jader a víc GHz
- víc RAM
- možná display?



Omnia II

- 10 Gbps metalika
- 10 Gbps SFP
- 2.5 Gbps metalika
- WiFi 6
- 5G ready
- Kdy? Velmi možná konec 2022

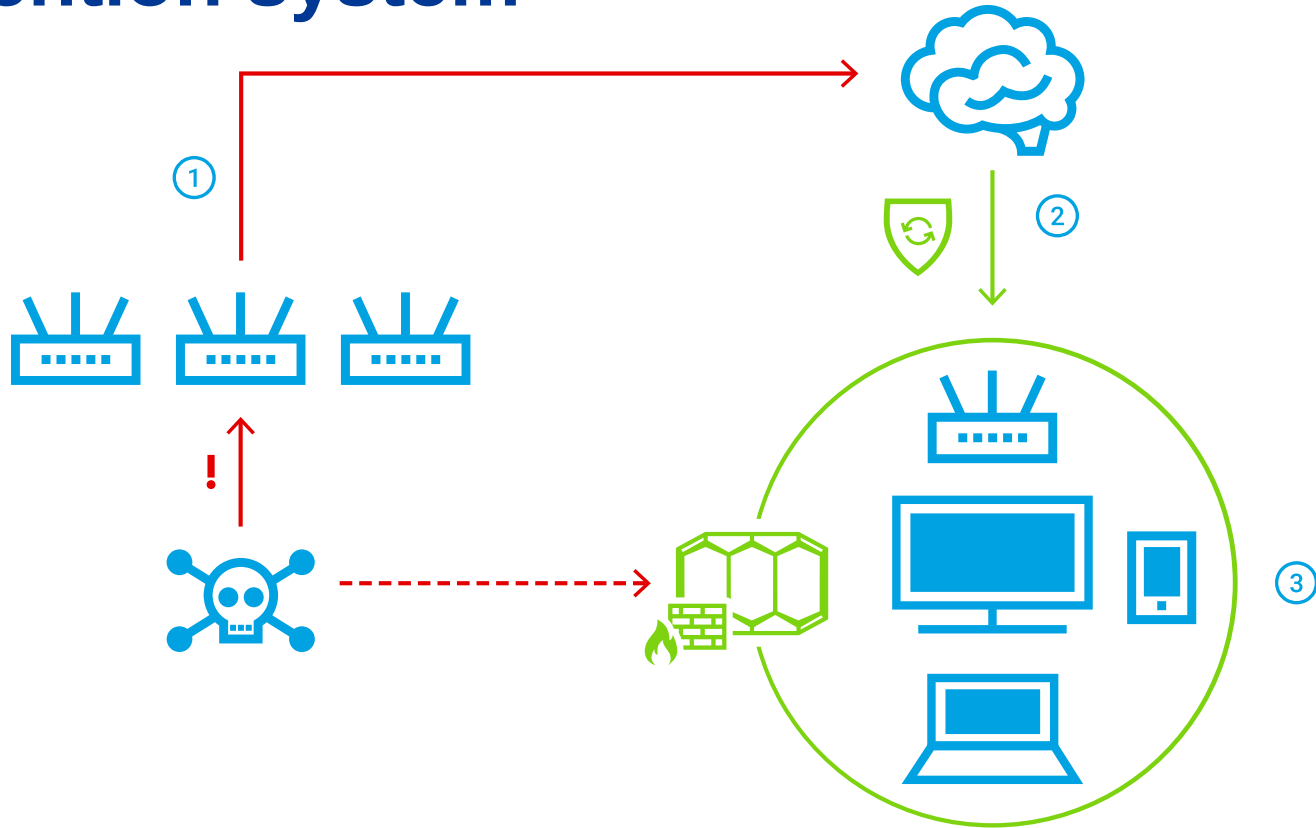


Co do tý doby?

- Turris OS 6.0
 - založen na OpenWrt 21.02
 - s trochou štěstí k Vánocům
- Omnia s WiFi 6
 - v průběhu 2022
- novinky v Sentinelu ;-)

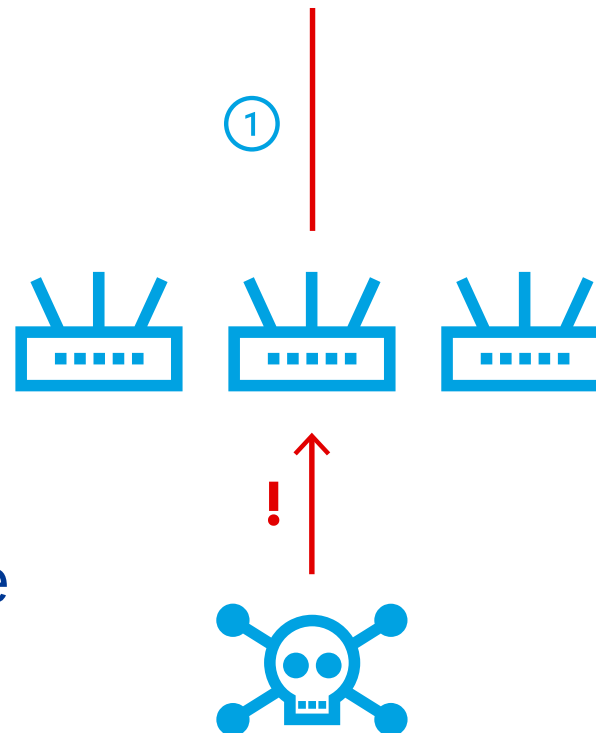


Sentinel – threat detection and cyberattack prevention system



Sběr dat

- Na routeru:
 - Minipoty
 - Firewall logy
 - Dobrovolnost
- Externí zdroje:
 - HaaS – SSH Honeypot as a Service
<https://haas.nic.cz>



Minipot – minimální honeypot

- Honeypot – past
 - Kontrolované prostředí
 - Sledování útočnickovy aktivity
- Minimální
 - Emulace známých služeb na aplikační vrstvě – Telnet, HTTP, FTP, SMTP
 - Pokusy o připojení a přihlášení



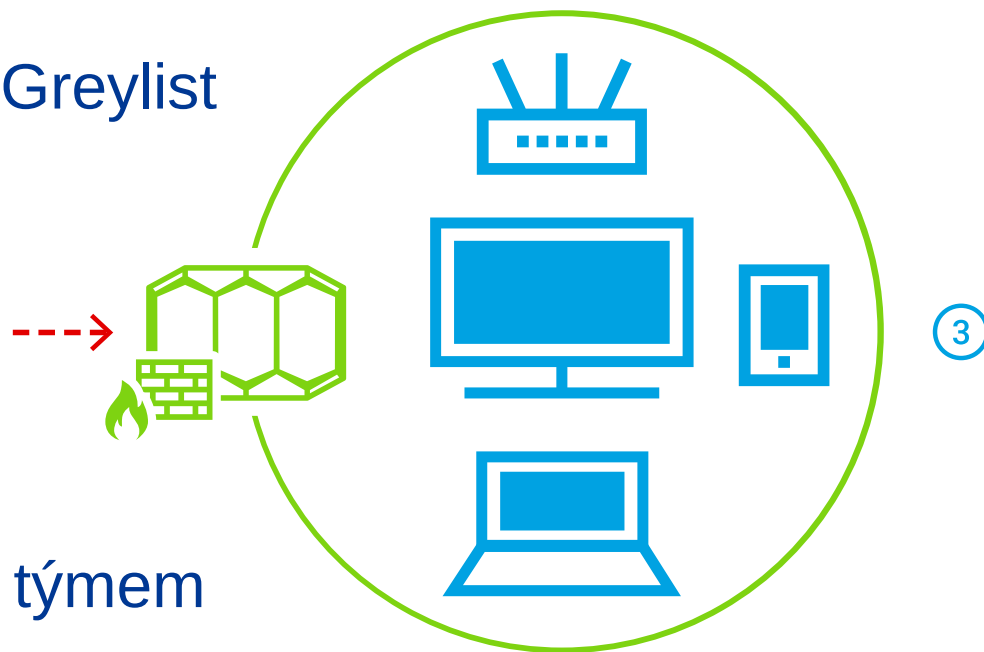
Zpracování dat

- Proudově – data pipelines
 - Message queues
- Série propojených komponent
 - Obohacení dat
 - Analýza
 - Databáze
- Každá IP adresa má skóre
 - Práh



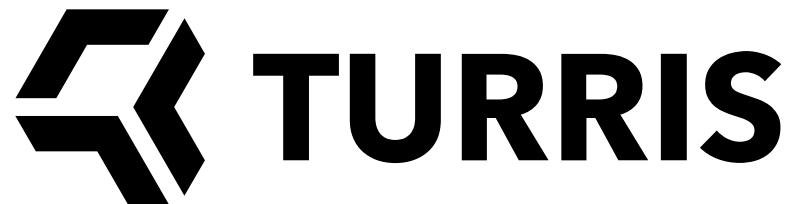
Výstupy

- Seznam škodlivých IP adres – Greylist
 - Veřejně dostupný
- Sentinel View
 - Statistiky dat
 - <https://view.sentinel.turris.cz>
- Spolupráce s národním CSIRT týmem



Sentinel novinky v TOS 5.3

- Turris Survey v0.2
- Minipoty v2.2 – sjednocení typů zpráv
- Nikola → FWLogs Collector
- Sentinel Proxy v1.4
- Sentinel Overview v reForisu
- Update serverové infrastruktury



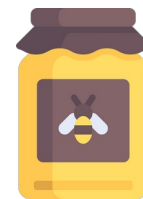
Sentinel novinky v TOS 5.3 – Turris Survey

- Volitená část Sentinelu
- Informace o používaných funkcích
 - Nainstalované balíčky
 - Jazykové mutace
- Nově ve verzi 0.2



Sentinel novinky v TOS 5.3 – Minipoty

- Volitená část Sentinelu
- „Minimální honeypoty“ - Telnet, SMTP, FTP, HTTP
- Produkuje eventy na základě chování útočníků
- Nově ve verzi 2.2 – sjednocení eventů
 - Connect
 - Login
 - Invalid
 - Message (pouze HTTP)



Sentinel novinky v TOS 5.3 – FWLogs collector

- Volitená část Sentinelu
- = Firewall monitoring
- Sběr FW logů o odmítnutých nebo zahozených spojeních
- Náhrada „one shot“ skriptu Nikola za FWLogs collector
 - C
 - Netlink, knihovna libnetfilter_log
 - Rychlejší odezva na události
 - Nižší režie



Sentinel novinky v TOS 5.3 – Sentinel Proxy

- Vychozí brána na routeru pro spojení na server
- Udržuje bezpečný komunikační kanál
- Nově ve verzi 1.4
 - Interní refactoring
 - Příprava pro zobrazení informací o aktivitě v reForisu



Sentinel novinky v TOS 5.3 – Sentinel Overview

- Network Settings ▾
- Administration ▾
- Package Management ▾
- Storage
- OpenVPN ▾
- NetMetr ▾
- Sentinel ▾
- Overview**
- License Agreement
- HaaS
- Advanced Administration [↗](#)
- About

Sentinel Components

You can select specific components that you want to enable or disable.

Enable Firewall Logs

Firewall Logs are logs gathered from iptables firewall. If enabled, Sentinel use them to monitor packets coming from outside network and trying to connect to potentially vulnerable local services. These techniques, also known as "port scans" usually try to detect whether specific ports are opened on local device. If enabled, Sentinel Firewall Logs gather information about origin of such malicious packets and about ports they try to scan on local device.

Enable Minipots

The main purpose of the Sentinel Minipot is to collect authentication information from the login attempts. It is possible to emulate some of the often attacked services - Telnet, HTTP, FTP, and SMTP. The goal is to catch the attacker red-handed when they think they attack a real service.

HTTP

Running on port 80.

FTP

Running on port 21.

SMTP

Running on port 25 and 587.

Telnet

Running on port 23.

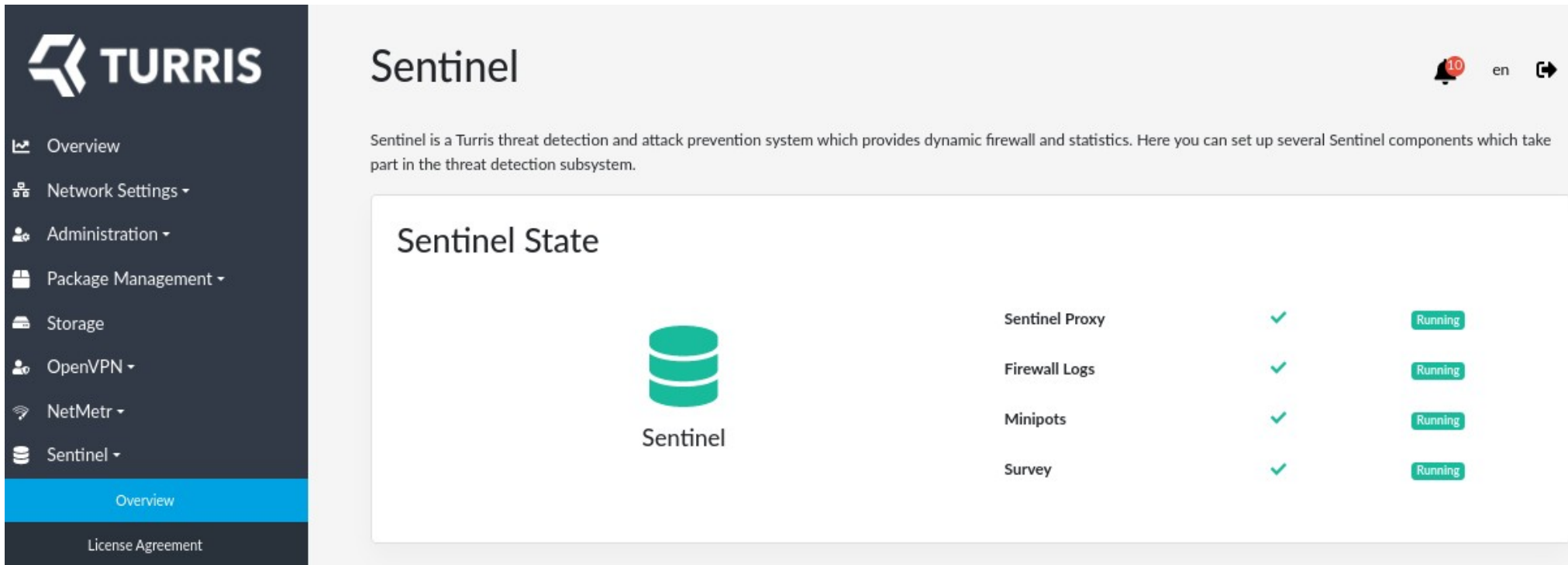
Enable Survey

Since our team has only limited manpower, we try to primarily focus on subjects that really matter. The Turris survey collects information about installed packages, used languages, and operating system versions. Based on this we are able to identify widely used packages, features and provide special support.

Save



Sentinel novinky v TOS 5.3 – Sentinel Overview



The screenshot shows the Turris Sentinel Overview page. On the left is a dark sidebar with the Turris logo and a menu with items: Overview (highlighted), Network Settings, Administration, Package Management, Storage, OpenVPN, NetMetr, and Sentinel. The main content area has a header 'Sentinel' with a notification bell (10) and language 'en'. Below the header is a descriptive paragraph: 'Sentinel is a Turris threat detection and attack prevention system which provides dynamic firewall and statistics. Here you can set up several Sentinel components which take part in the threat detection subsystem.' The main section is titled 'Sentinel State' and features a green database icon labeled 'Sentinel'. To the right is a table showing the status of four components: Sentinel Proxy, Firewall Logs, Minipots, and Survey, all of which are 'Running'.

Component	Status	Indicator
Sentinel Proxy	Running	Green checkmark
Firewall Logs	Running	Green checkmark
Minipots	Running	Green checkmark
Survey	Running	Green checkmark



Nápady do budoucna

- Zobrazení poslední aktivity v reForisu
- Inspirace službou „Have I been pwned“
- Příprava na plnohodnotný běh Sentinelu mimo Turris
- Nasazení nového Sentinel View





Děkujeme za pozornost

Michal Hrušecký • michal.hrusecky@nic.cz

Miroslav Hanák • miroslav.hanak@nic.cz

Martin Prudek • martin.prudek@nic.cz

6.11.2021