De Turris MOX is een uniek modulair netwerkapparaat.

automatische updates heeft. Standaard staat dit ingeschakeld, zodat je Turris-router zichzelf periodiek updatet en je dus altijd zo veilig mogelijk blijft. Je kunt ook instellen dat je alleen notificaties van updates ontvangt (in de webinterface en/of via e-mail) en dat je elke update nog manueel dient te bevestigen.

VOLLEDIG OPEN

Alle Turris-software is opensource, te vinden op de GitLab-website van CZ.NIC (**https://gitlab.labs.nic.cz/turris**). De makers proberen zoveel mogelijk met upstreamprojecten samen te werken en hun code upstream te krijgen. Met OpenWrt is dat in het verleden niet altijd even goed geslaagd, maar tegenwoordig blijft de codebase van Turris OS veel dichter bij die van OpenWrt.

Ook de hardware van de Turris-routers is open: de volledige elektronische schema's zijn te vinden op de documentatiewebsite (**https://docs.turris.cz/basics/models/**). Voor de Turris MOX vind je zelfs van elke module de schema's. Zo kun je in principe je eigen modules of uitbreidingen maken, of de bestaande componenten aanpassen. Leuk voor de hardwarehackers die hun netwerkapparatuur willen aanpassen.

HOU JE NETWERKVERKEER IN HET OOG

Maar interessanter nog dan de openheid van de software en hardware van de Turris-routers is het hele ecosysteem van software en diensten errond. Dat begint bij kleine dingen. Zo kun je in Turris OS een pakket "Device detection" installeren dat je via een melding waarschuwt als er een onbekend apparaat met je netwerk verbindt. Je krijgt dan het mac-adres, de producent (afgeleid uit het oui-gedeelte van het mac-adres) en de hostname te zien.

Wil je meer informatie over je netwerk verzamelen, installeer dan Pakon. Dit project maakt gebruik van het ids (intrusion detection system) Suricata (https://suricata-ids.org/) en toont het resultaat van de continue netwerkanalyse in een overzichtelijke word cloud met de meest gebruikte domeinen. Je kunt deze nog filteren op tijdstip en ook alleen het verkeer van specifieke hostnames en/of clients tonen.

Het is ook mogelijk om in een shell het verkeer te bekijken:

```
> pakon-show
```

GEDISTRIBUEERDE FIREWALL

CZ.NIC heeft ook een onderzoeksproject Project Turris (**https://project.turris.cz/en/**) dat onder de naam Sentinel verdacht netwerkverkeer op alle aangesloten routers detecteert en een centrale server waarschuwt. Als er dan iemand in jouw Turris-router probeert in te breken, wordt die aanval niet alleen in jouw router tegengehouden, maar vanaf dan ook onmiddellijk in alle andere bij het project aangesloten Turris-routers. In zekere zin is dit dus een gedistribueerde firewall.

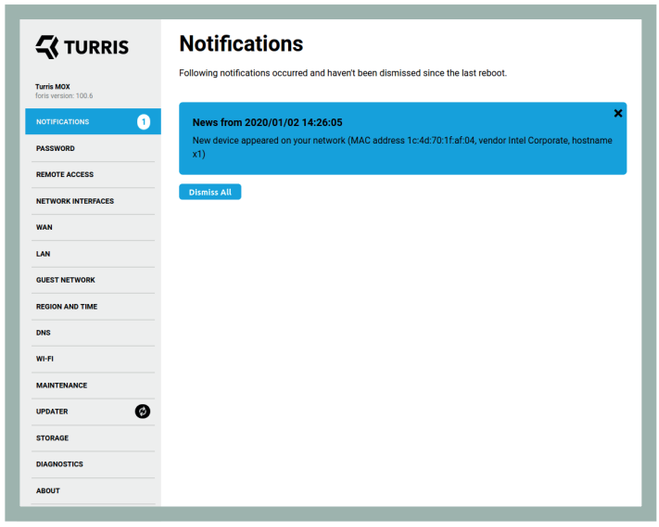
In Turris OS schakel je de gedistribueerde firewall Sentinel in door het pakket **Data Collection** te installeren. Helaas is het voorlopig nog niet mogelijk om in de webinterface in te stellen welke data Sentinel van je mag verzamelen.

Sowieso worden alleen de headers van de pakketten die via de wanpoort binnenkomen verzameld en doorgestuurd. Inbraakpogingen via SSH of port scanning worden door de service Nikola uit de logs van iptables gehaald en doorgestuurd. Data van meerdere routers worden geaggregeerd zodat later niet meer na te trekken is van welke specifieke router een pakket kwam, en elke tien dagen worden de data ook verwijderd.

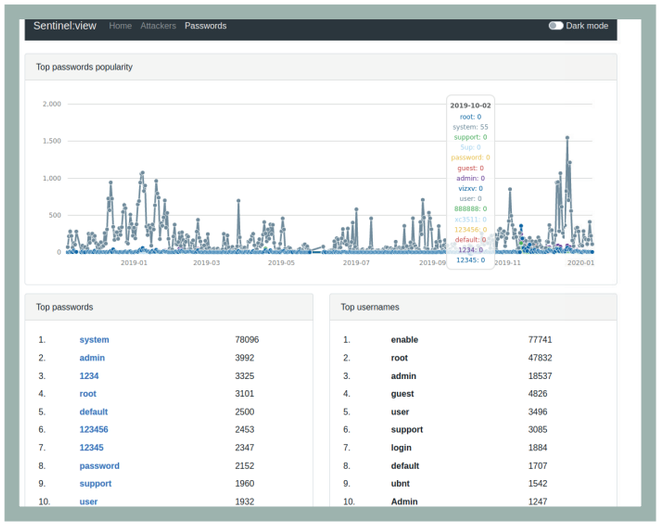
Je kunt ook een "honeypot" op je Turris-router draaien: Turris Minipot is een gesimuleerde Telnet-server die elke aanmeldpoging afwijst, maar ondertussen wel elke ingevoerde combinatie van gebruikersnaam, wachtwoord en IP-adres verzamelt, wat interessant is voor onderzoek naar nieuwe bedreigingen op internet. Je installeert Nikola en Minipot eenvoudig met:

```
> opkg update
> opkg install sentinel-nikola
sentinel-minipot
```

In de webinterface Foris kun je bij de pakketten ook **SSH Honeypot** inschakelen om een SSH-honeypot te installeren. Daarmee neem je deel aan Honeypot as a Service (HaaS) van Turris Project (**https://haas.nic.cz/**). Als een aanvaller dan via SSH op je router probeert in te loggen via je publieke IP-adres, wordt die door een proxy op je router doorgestuurd naar een honeypotserver van Turris. Zowel van HaaS als Sentinel zijn statistieken online te bekijken (**https://haas.nic.cz/stats/** en **https://view.sentinel.turris.cz/**), wat een interessante inkijk in de onderwereld op internet geeft.



Je Turris-router waarschuwt je wanneer er een onbekend apparaat op je netwerk komt.



De statistieken van inbraakpogingen op de gedistribueerde firewall Sentinel van Turris Project zijn online te bekijken.