eBlocker

Open Source Project

Technical Background & Core Architecture

Overview

- eBlocker Features and Technology
- eBlocker User Interfaces
- eBlocker Setup
  - Automatic network mode (Plug&Play)
  - Individual network mode
- eBlocker Architecture
  - Core architecture
  - Supporting cloud services

eBlocker Features and Technology

eBlocker Core Feature Overview

eBlocker
Switch on Privacy.

	Browser private mode	Browser plugins	Local proxy	Internet proxy	DIY gateways	eBlocker		
	IE, Chrome, Firefox	AdBlock Plus + Ghostery	AdGuard + Tor-Client	hidemyass.com, disconnect.me	Pi-hole, AdTrap Danubebox	Base	Pro	Family
Supports all OS Platforms, Devices & Browsers	✗	✗	✗	✓	✓	No longer available		✓
No Software Installation	✓	✗	✗	✗	✓			✓
IP-Anonymization via Tor or VPN	✗	✗	✓	✓	✓			✓
DNS-Anonymization against profiling by provider	✗	✗	✗	✗	✗			✓
Device Cloaking	✗	✗	✗	✗	✗			✓
Blocks all Trackers	✓ Firefox > 42.0	✓ via config. only	✗	✗	✗			✓
Blocks all tracking ads	✗	✓ via config. only	✓	✓	✓			✓
Browser Protection against Malware & Phishing	✗	✗	✗	✗	✗			✓
Protects IoT-Devices against Trackers & IP-Leakage	✗	✗	✗	✗	✗			✓
Mobile Device Protection also on the road	✗	✗	✗	✓ Teilweise	✗			✓
Parental Controls incl. FragFinn Q3'18	✗	✗	✓	✗	✗			✓
Individual User Accounts	✗	✗	✗	✗	✗			✓
Browsing Speed with slow connections	→	↗	→	↘	↘			↗

Open Source Project

- Includes all features
- No limitations, but no commercial filters initially
- Availability of commercial filters depends on reaching donation goals

Benefits & Technologies (1/2)

eBlocker
Switch on Privacy.

Customer benefits	Enabling technologies
Supports all OSs, devices, browsers & apps	Runs on own HW, automatic mode by ARP messages; individual mode as DHCP server – or as gateway/proxy
No software installation	Runs on own HW, acts as gateway ➔ sees all IP packets
IP anonymization	Per device routing of IP traffic through Tor or VPN
DNS anonymization	Options: Choose own DNS servers; rotate DNS servers; use Tor for DNS; route DNS through VPN
Device cloaking	Adjust user agent per device
Blocks data collectors & trackers	Domain or pattern blocker with daily updated lists; supports own white and black lists
Blocks tracking ads	Domain or pattern blocker with daily updated lists; supports own white and black lists; pattern blocker can be disabled per site to avoid pay wall or other “conflicts”
Malware & phishing protection	Domain and pattern blocker with daily updated lists
Protects IoT / all connected devices	No SW installation on IoT device necessary: All connected devices are protected at once

Benefits & Technologies

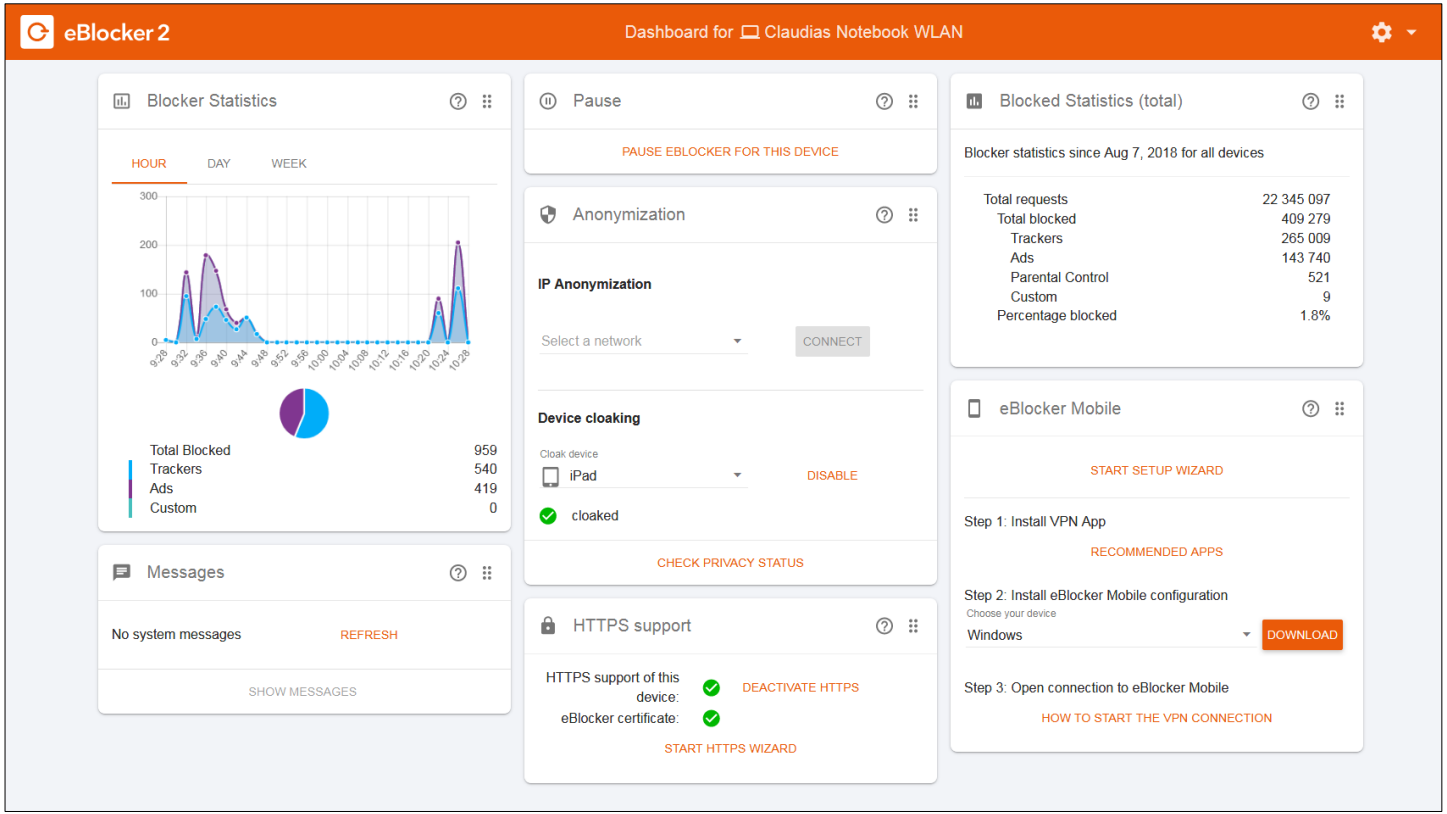
eBlocker
Switch on Privacy.

Customer benefits	Enabling technologies
Mobile device protection	Mobile devices connect via VPN from remote into home network; receiving same protection as in-house devices
Parental controls	Domain or pattern blocker with daily updated lists; curated black lists and white lists (for kids < 12 years) from partners; time based controls across all kids' devices in sum
User account management	All settings auto-roam to all user assigned devices; shared family devices can change owner by entering a PIN
Increased browsing speed experience	Tracking scripts, ad banners etc. not loaded; saves bandwidth and rendering time
Intrusion detection (Q2)	Analyzes the IP traffic from all devices; recognizes “unusual” traffic patterns; rule based handling of compromised devices
Intrusion prevention (Q4)	Rule based access rights for new network devices; i.e. blocks communication attempts of "new" devices if desired; automatically prevents intrusions based on traffic patterns

eBlocker Screen Shots

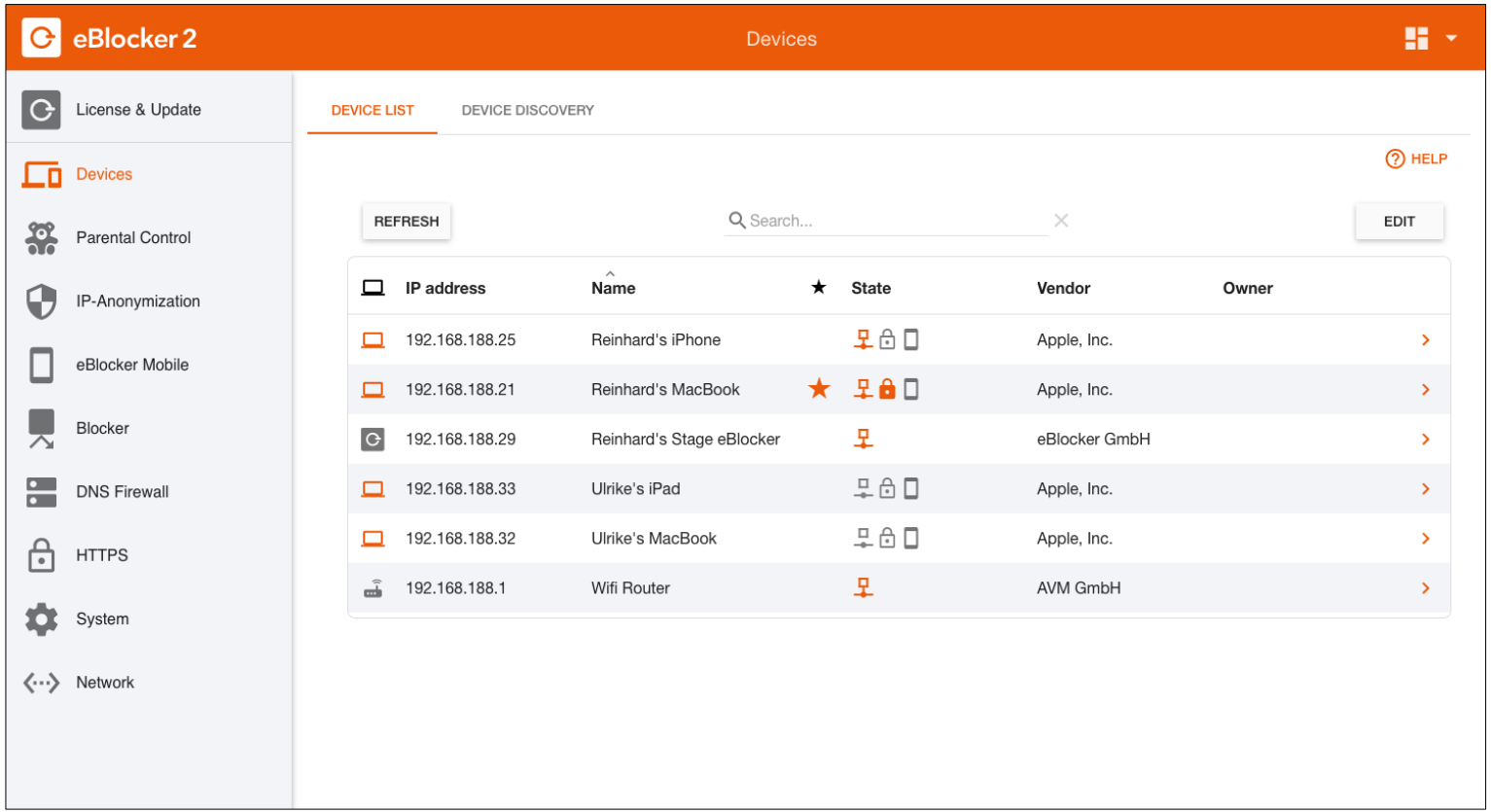
Interface: Dashboard

eBlocker
Switch on Privacy.

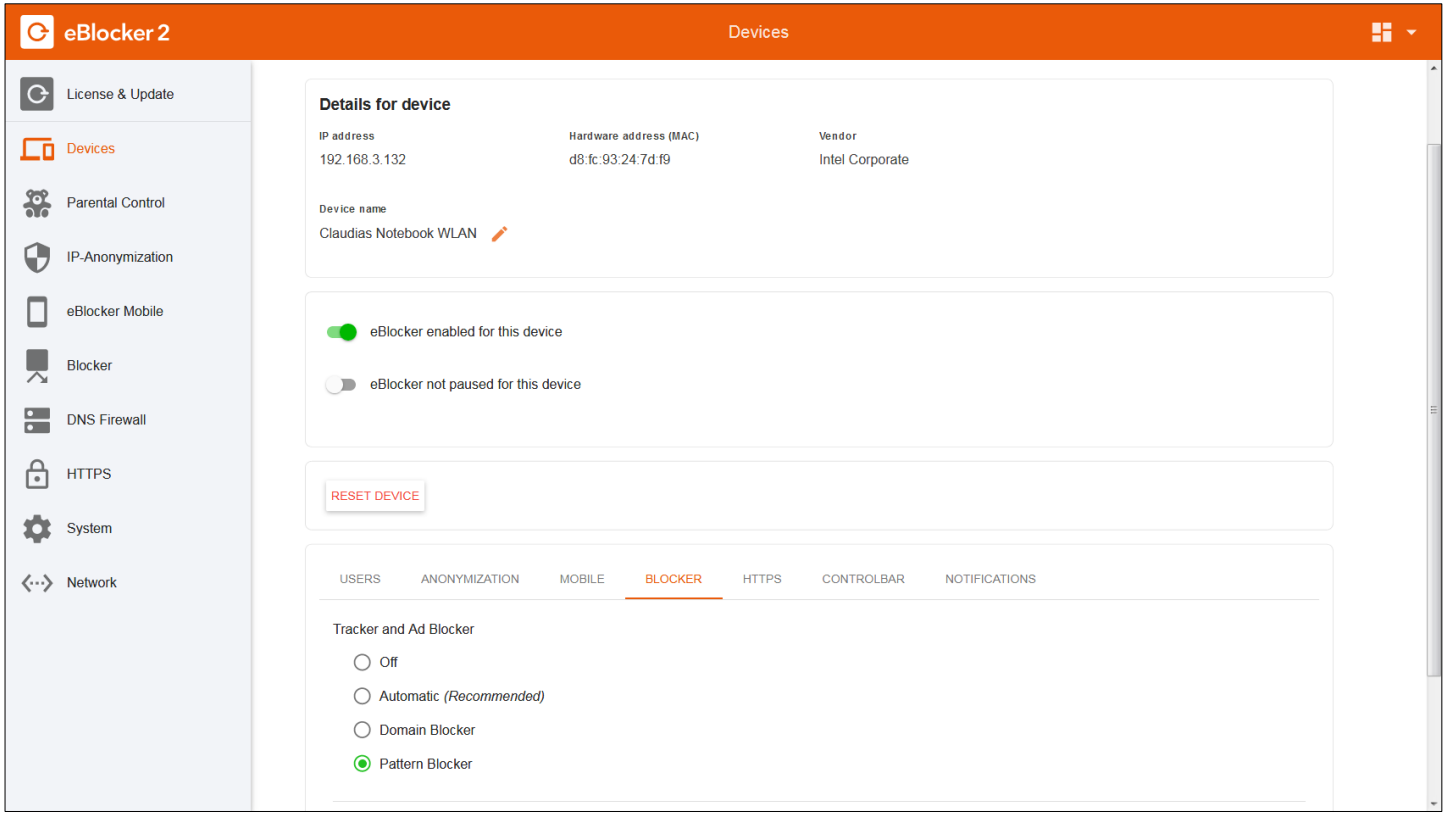


Interface: Settings / Devices Overview

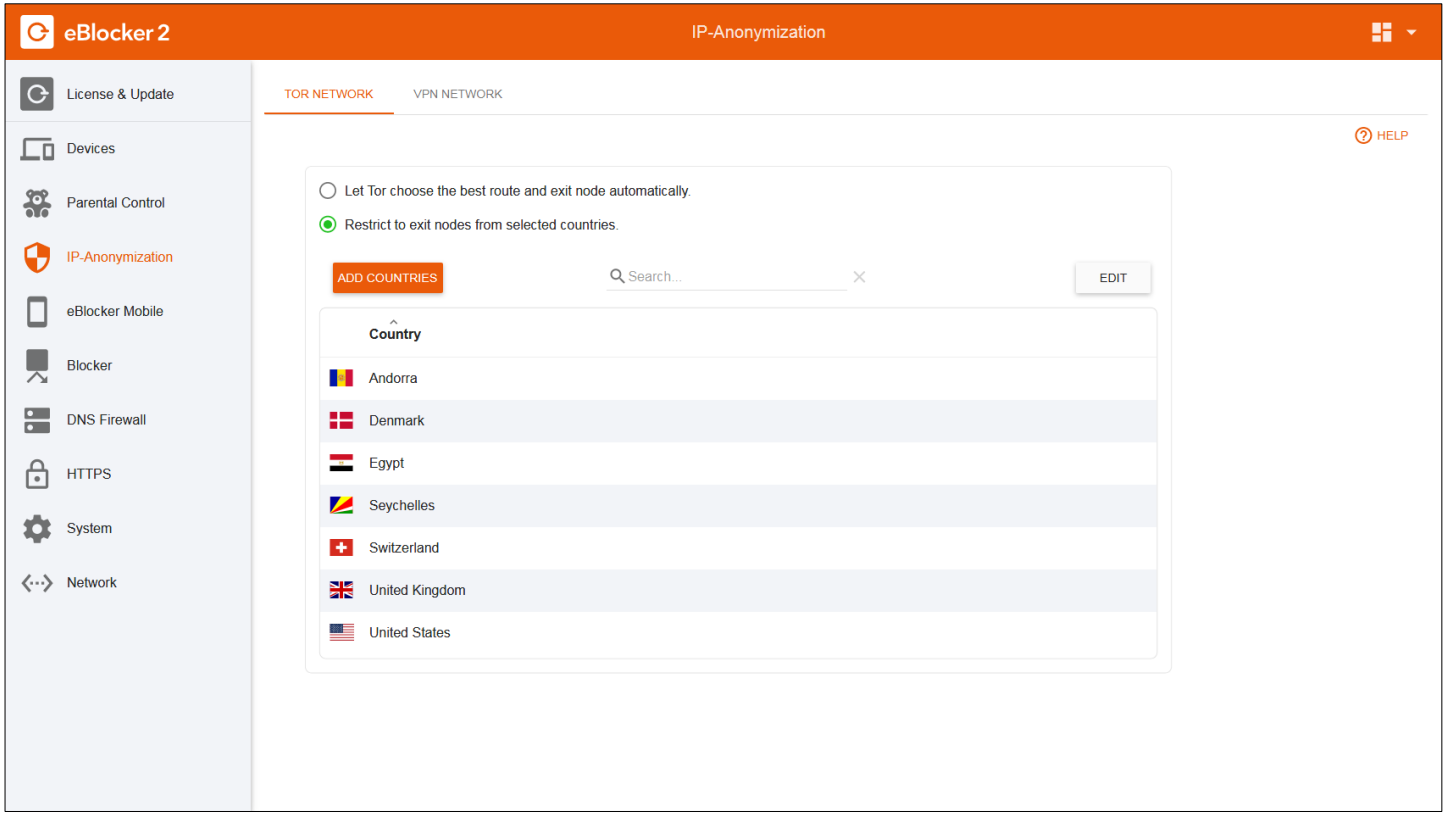
eBlocker
Switch on Privacy.



Interface: Settings / Devices Details

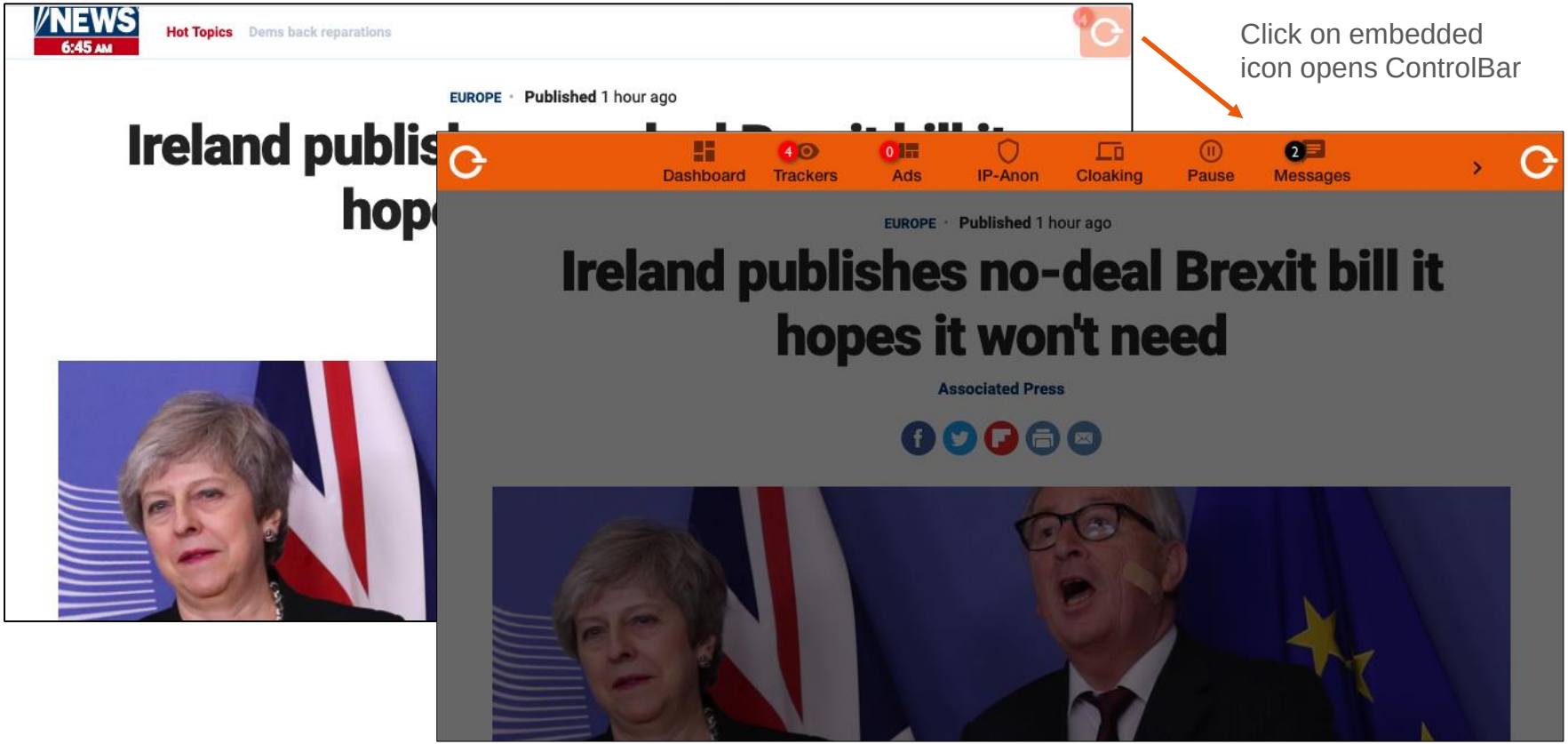


Interface: Settings / IP-Anonymization



Interface: Icon and ControlBar

eBlocker
Switch on Privacy.



Click on embedded icon opens ControlBar

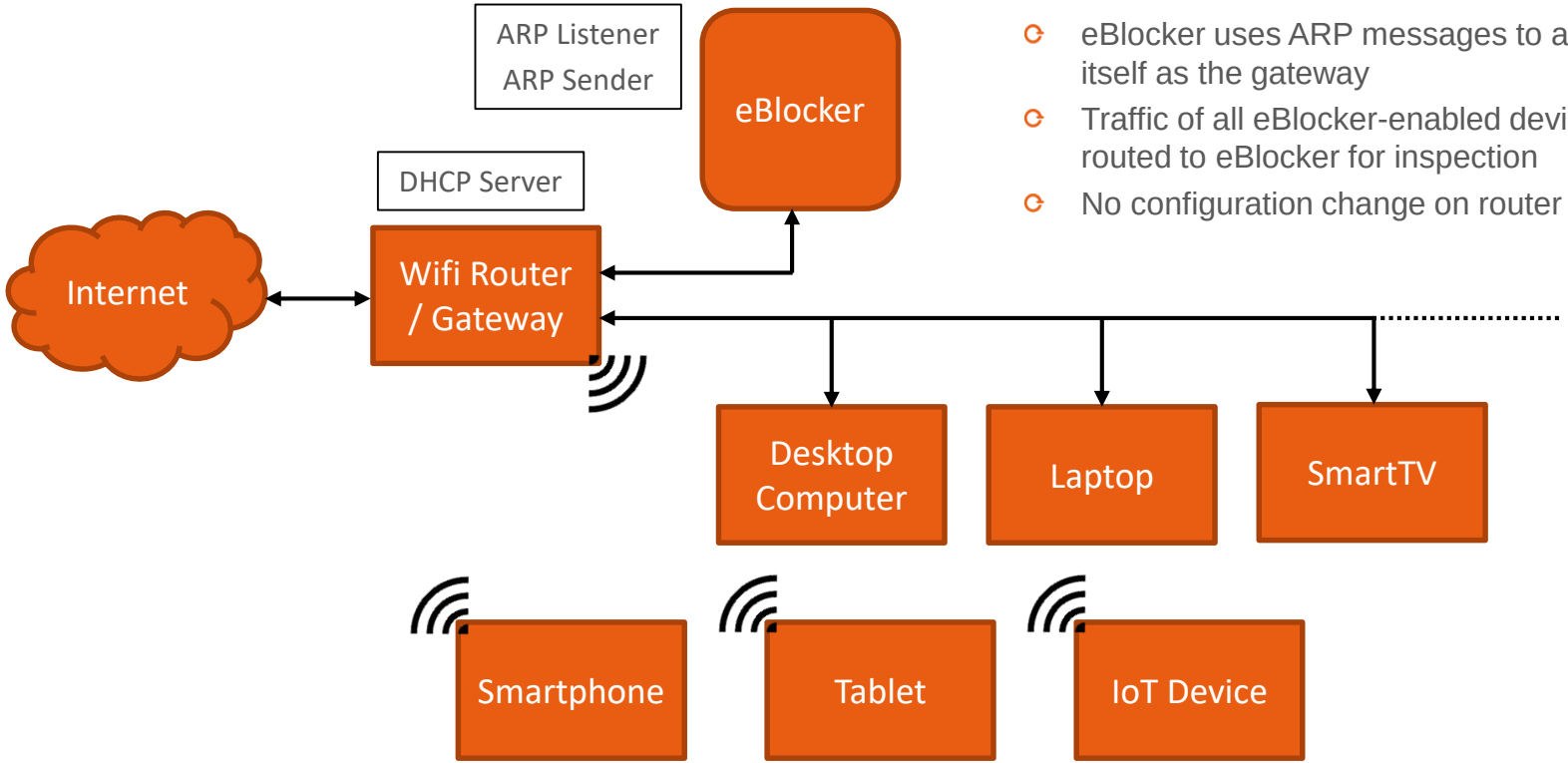
eBlocker Setup

Different ways to integrate eBlocker into home networks

eBlocker Setup Options & Compatibility

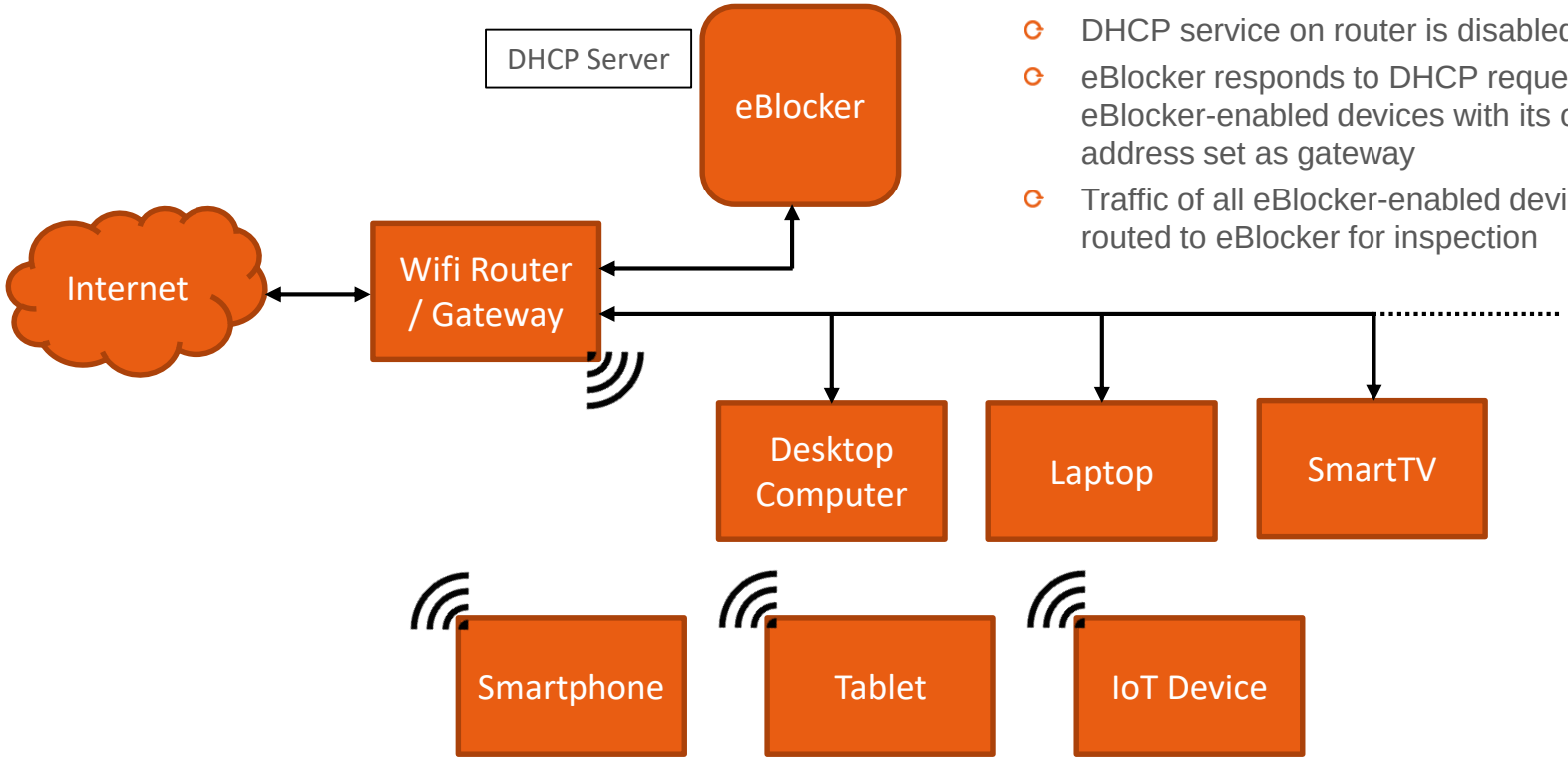
- Plug & Play / automatic network mode (default)
  - Today most network equipment is compatible with eBlocker's Plug & Play
  - Few devices that need "special treatment" to make them compatible are listed here: https://www.eblocker.com/en/compatibility/
  - Devices not listed explicitly are usually compatible
- Individual setup mode (if Plug & Play is not available for a network device)
  - Network devices can be configured for eBlocker compatibility with three alternative methods
    - Switching off DHCP on the router – so eBlocker takes over DHCP service to announce itself as gateway
    - Manually setting eBlocker as Gateway in the existing DHCP services or individually in each client
    - Using eBlocker as a proxy server (configuring each client for proxy usage; only some eBlocker services)

Default Setup – Automatic Network Mode



- eBlocker uses ARP messages to announce itself as the gateway
- Traffic of all eBlocker-enabled devices is routed to eBlocker for inspection
- No configuration change on router necessary

Alternative Setup – Individual Network Mode



- DHCP service on router is disabled
- eBlocker responds to DHCP requests from eBlocker-enabled devices with its own IP address set as gateway
- Traffic of all eBlocker-enabled devices is routed to eBlocker for inspection

eBlocker Architecture and Technical Details

eBlocker Solution

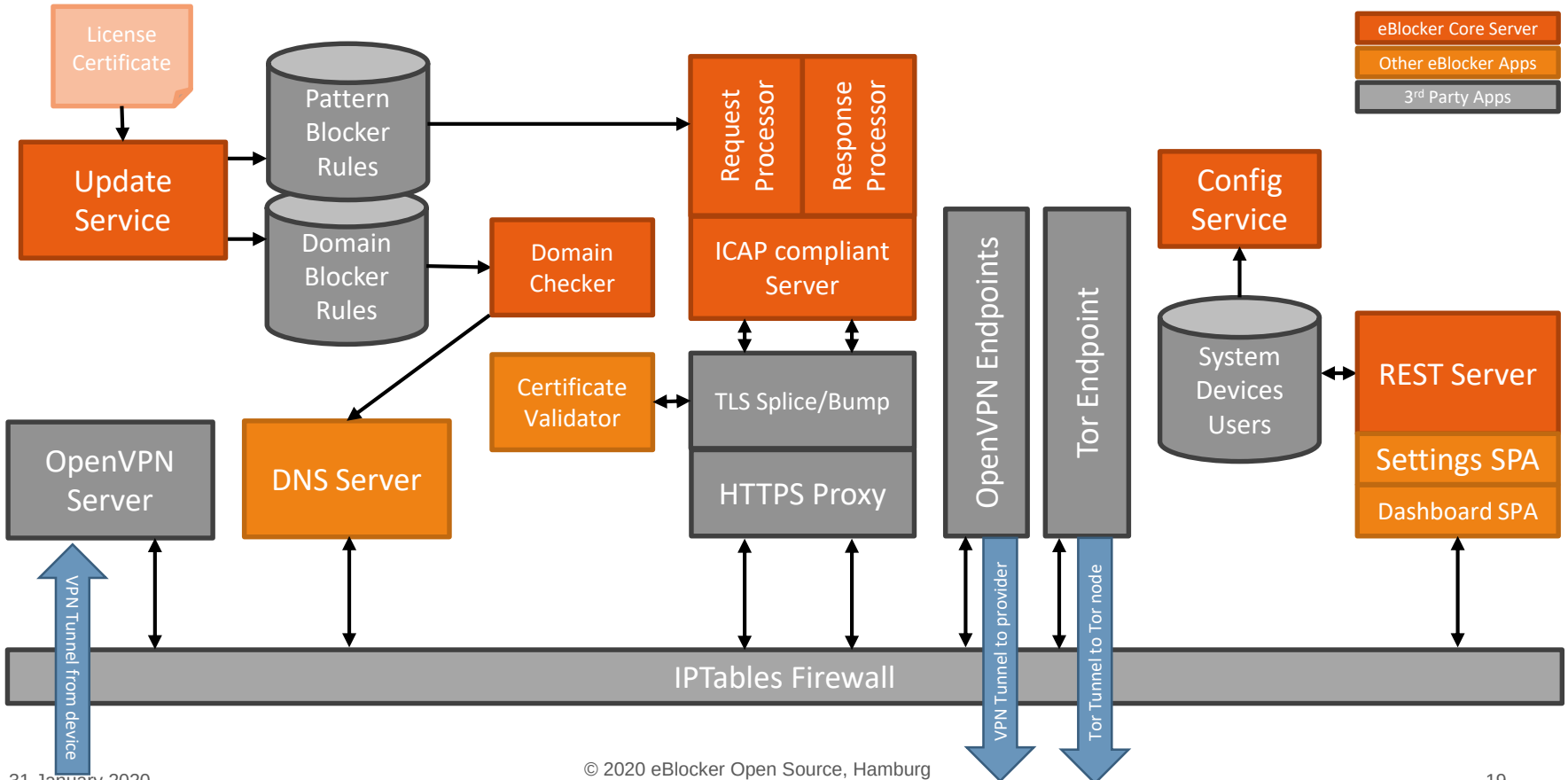
eBlocker
Switch on Privacy.

Technical approach

- Privacy by design
- No user data in the cloud
- Easy to setup and operate
- All network devices are protected
- Individual protection per device/user
- All devices and apps work as usual
- Existing WiFi router remains in place
- No changes to network topology
- Hardware independent development

- **eBlockerOS**
  - Open Source Code
    - Core in Java, JavaScript, C & Ruby
    - UI based on SPAs w/ REST-API
  - Based on standard protocols & OSS
    - HTTP, TLS, DNS, DHCP, ICAP
    - Debian Linux
- **Hardware Recommendations**
  - Standard ARM SBC (Raspberry Pi 4)
    - 4 core, 1 GHz, 2 GB RAM, 8 GB eMMC
  - Runs on any Linux system, incl. VM
    - Also prototyped on standard routers

eBlocker Core Architecture



Supporting eBlocker Cloud Services

- Update repository (Debian packages)
  - Daily filter lists and other configuration data (currently ~30MB)
  - Deploys hot fixes (eBlocker and system)
  - Deploys new releases (eBlocker and system)
- DNS service (for eBlocker Mobile)
- Internet connection test service
- Project website & user forum

Open Source Code & Collaboration

- Project will be released **during February 2020** on GitHub under EUPL

https://github.com/eblocker

- Please support our project and become part of our community
- Get in touch: voluntary@eBlocker.org
- More background information: www.eBlocker.org