

eBlocker

Open Source Project

Technical Background & Core Architecture

- 🔄 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

	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	✓ <small>Firefox > 42.0</small>	✓ <small>via config. only</small>	✗	✗	✗			✓
Blocks all tracking ads	✗	✓ <small>via config. only</small>	✓	✓	✓			✓
Browser Protection against Malware & Phishing	✗	✗	✗	✗	✗			✓
Protects IoT-Devices against Trackers & IP-Leakage	✗	✗	✗	✗	✗			✓
Mobile Device Protection also on the road	✗	✗	✗	✓ <small>Telnetwise</small>	✗			✓
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](#)

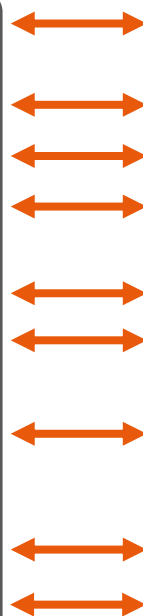
Benefits & Technologies (1/2)

Customer benefits

- Supports all OSs, devices, browsers & apps
- No software installation
- IP anonymization
- DNS anonymization
- Device cloaking
- Blocks data collectors & trackers
- Blocks tracking ads
- Malware & phishing protection
- Protects IoT / all connected devices

Enabling technologies

- Runs on own HW, automatic mode by ARP messages; individual mode as DHCP server – or as gateway/proxy
- Runs on own HW, acts as gateway → sees all IP packets
- Per device routing of IP traffic through Tor or VPN
- Options: Choose own DNS servers; rotate DNS servers; use Tor for DNS; route DNS through VPN
- Adjust user agent per device
- Domain or pattern blocker with daily updated lists; supports own white and black lists
- 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”
- Domain and pattern blocker with daily updated lists
- No SW installation on IoT device necessary: All connected devices are protected at once



Customer benefits

- 🔗 Mobile device protection
- 🔗 Parental controls
- 🔗 User account management
- 🔗 Increased browsing speed experience
- 🔗 Intrusion detection (Q2)
- 🔗 Intrusion prevention (Q4)

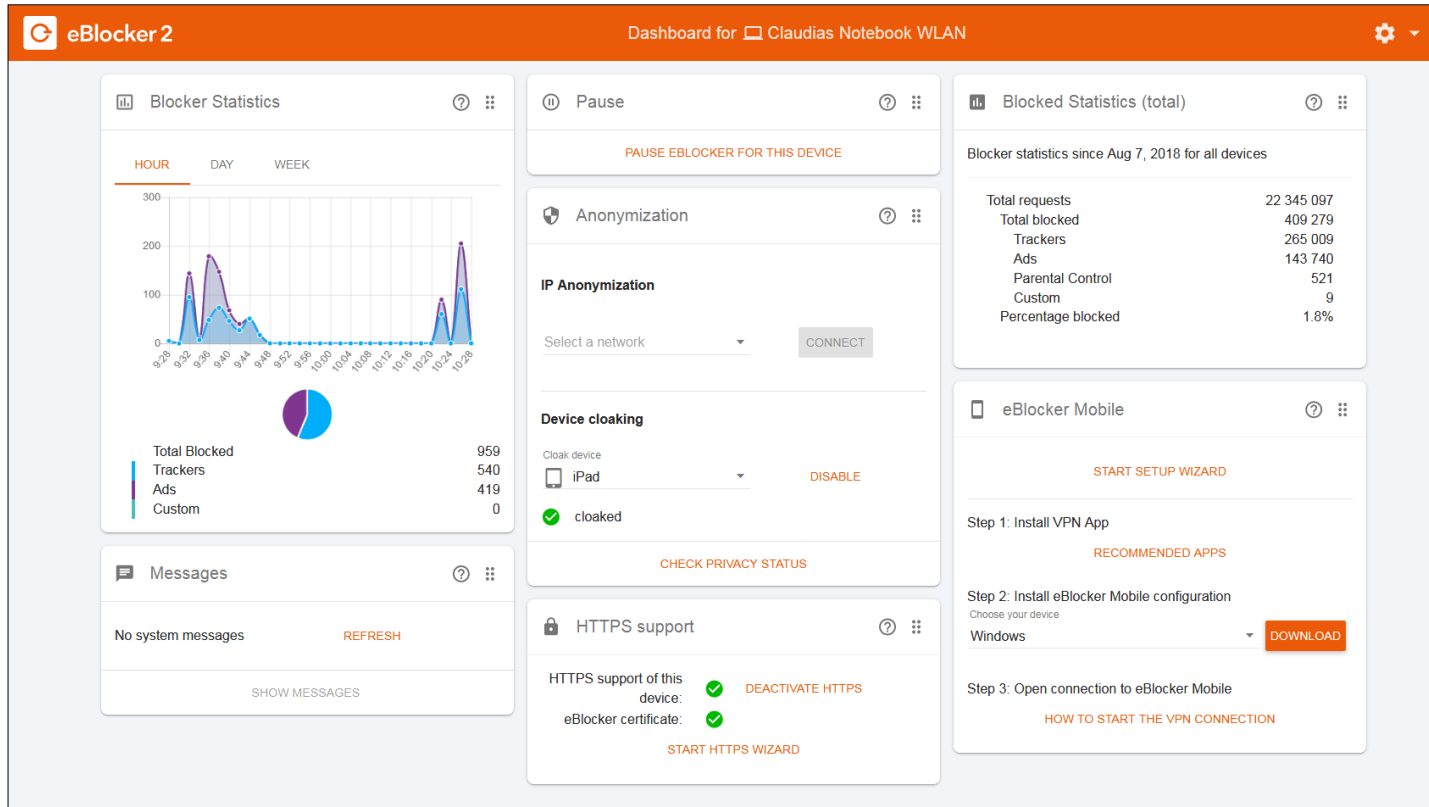


Enabling technologies


- 🔗 Mobile devices connect via VPN from remote into home network; receiving same protection as in-house devices
- 🔗 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
- 🔗 All settings auto-roam to all user assigned devices; shared family devices can change owner by entering a PIN
- 🔗 Tracking scripts, ad banners etc. not loaded; saves bandwidth and rendering time
- 🔗 Analyzes the IP traffic from all devices; recognizes "unusual" traffic patterns; rule based handling of compromised devices
- 🔗 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





Interface: Settings / Devices Overview


 eBlocker2


Devices





 License & Update


 Devices


 Parental Control


 IP-Anonymization


 eBlocker Mobile

 Blocker

 DNS Firewall


 HTTPS

 System

 Network

DEVICE LIST






















DEVICE DISCOVERY

 HELP

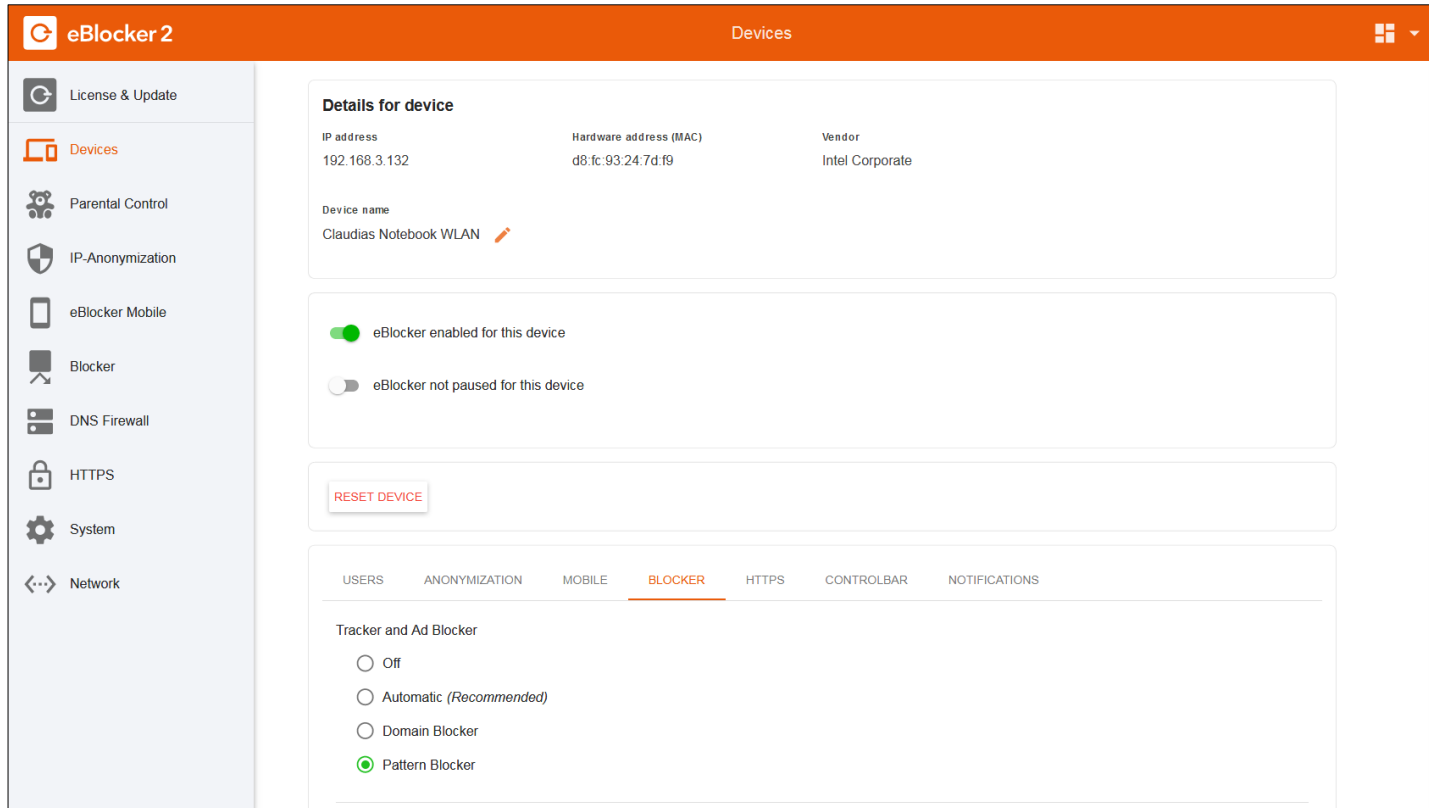
REFRESH

Search...

EDIT

 IP address	Name	★ State	Vendor	Owner
 192.168.188.25	Reinhard's iPhone	  	Apple, Inc.	>
 192.168.188.21	Reinhard's MacBook	★   	Apple, Inc.	>
 192.168.188.29	Reinhard's Stage eBlocker		eBlocker GmbH	>
 192.168.188.33	Ulrike's iPad	  	Apple, Inc.	>
 192.168.188.32	Ulrike's MacBook	  	Apple, Inc.	>
 192.168.188.1	Wifi Router		AVM GmbH	>

Interface: Settings / Devices Details



eBlocker 2 Devices

License & Update

Devices

Parental Control

IP-Anonymization

eBlocker Mobile

Blocker

DNS Firewall


HTTPS

System

Network

Details for device

IP address	Hardware address (MAC)	Vendor
192.168.3.132	d8:fc:93:24:7d:f9	Intel Corporate

Device name
Claudias Notebook WLAN 

☒ eBlocker enabled for this device

☐ eBlocker not paused for this device

RESET DEVICE

USERS **ANONYMIZATION** **MOBILE** **BLOCKER** **HTTPS** **CONTROLBAR** **NOTIFICATIONS**

Tracker and Ad Blocker

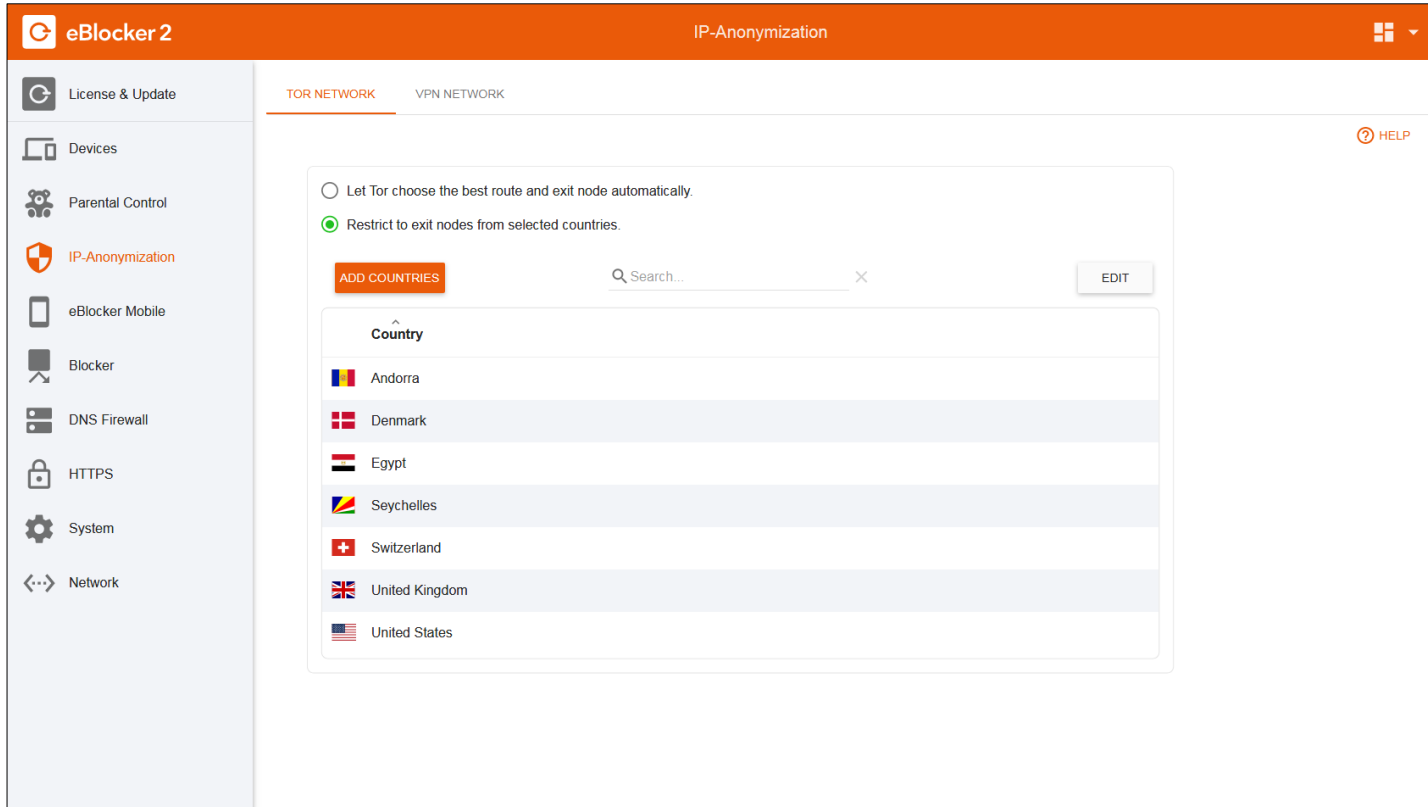
☐ Off

☐ Automatic (Recommended)

☐ Domain Blocker

☒ Pattern Blocker

Interface: Settings / IP-Anonymization



The screenshot shows the eBlocker 2 application interface. The top bar is orange with the eBlocker 2 logo on the left, the title "IP-Anonymization" in the center, and a window control icon on the right. A left sidebar contains navigation links: License & Update, Devices, Parental Control, IP-Anonymization (highlighted in orange), eBlocker Mobile, Blocker, DNS Firewall, HTTPS, System, and Network. The main content area has two tabs: "TOR NETWORK" (active) and "VPN NETWORK". Below the tabs, there are two radio button options: "Let Tor choose the best route and exit node automatically." (unselected) and "Restrict to exit nodes from selected countries." (selected). Below these options is a list of countries with flags, each on a light blue background. The countries listed are Andorra, Denmark, Egypt, Seychelles, Switzerland, United Kingdom, and United States. Above the list is an "ADD COUNTRIES" button, a search bar with the placeholder "Search..." and a close button "X", and an "EDIT" button. A "HELP" link with a question mark icon is located in the top right corner of the main content area.

License & Update

Devices

Parental Control

IP-Anonymization

eBlocker Mobile

Blocker

DNS Firewall

HTTPS

System

Network

IP-Anonymization

TOR NETWORK VPN NETWORK

Let Tor choose the best route and exit node automatically.

Restrict to exit nodes from selected countries.

ADD COUNTRIES

Search...

EDIT

Country

Andorra

Denmark

Egypt

Seychelles

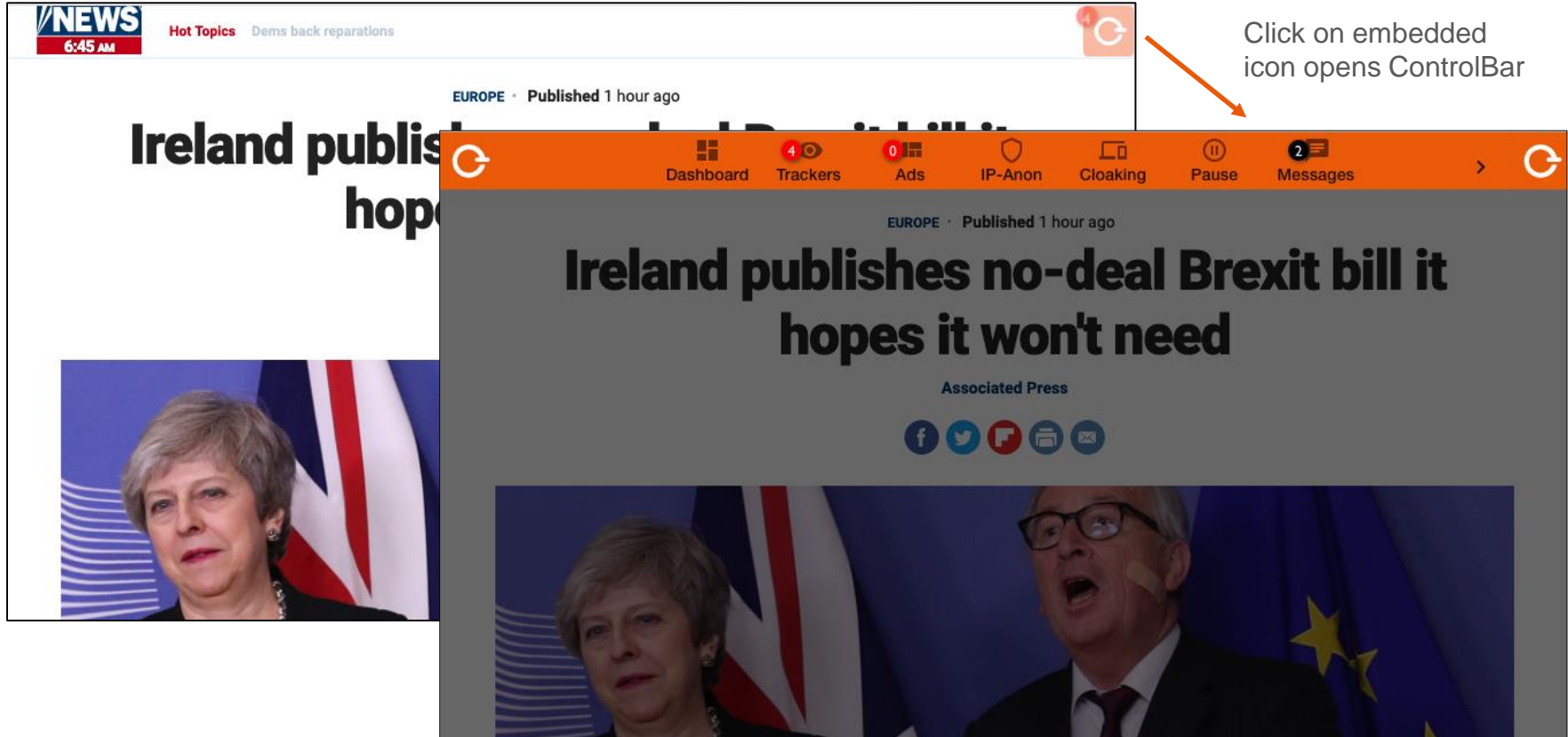
Switzerland

United Kingdom

United States

HELP

Interface: Icon and ControlBar

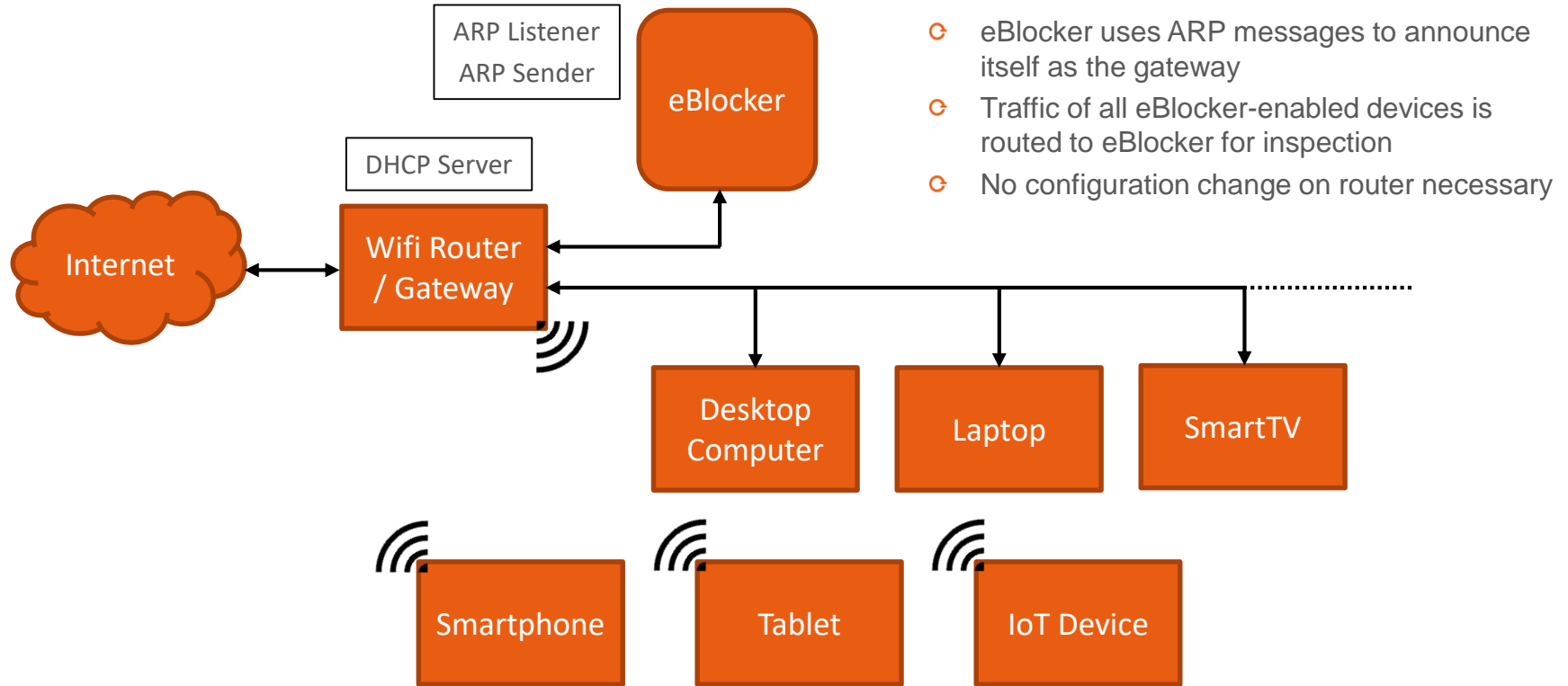


eBlocker Setup

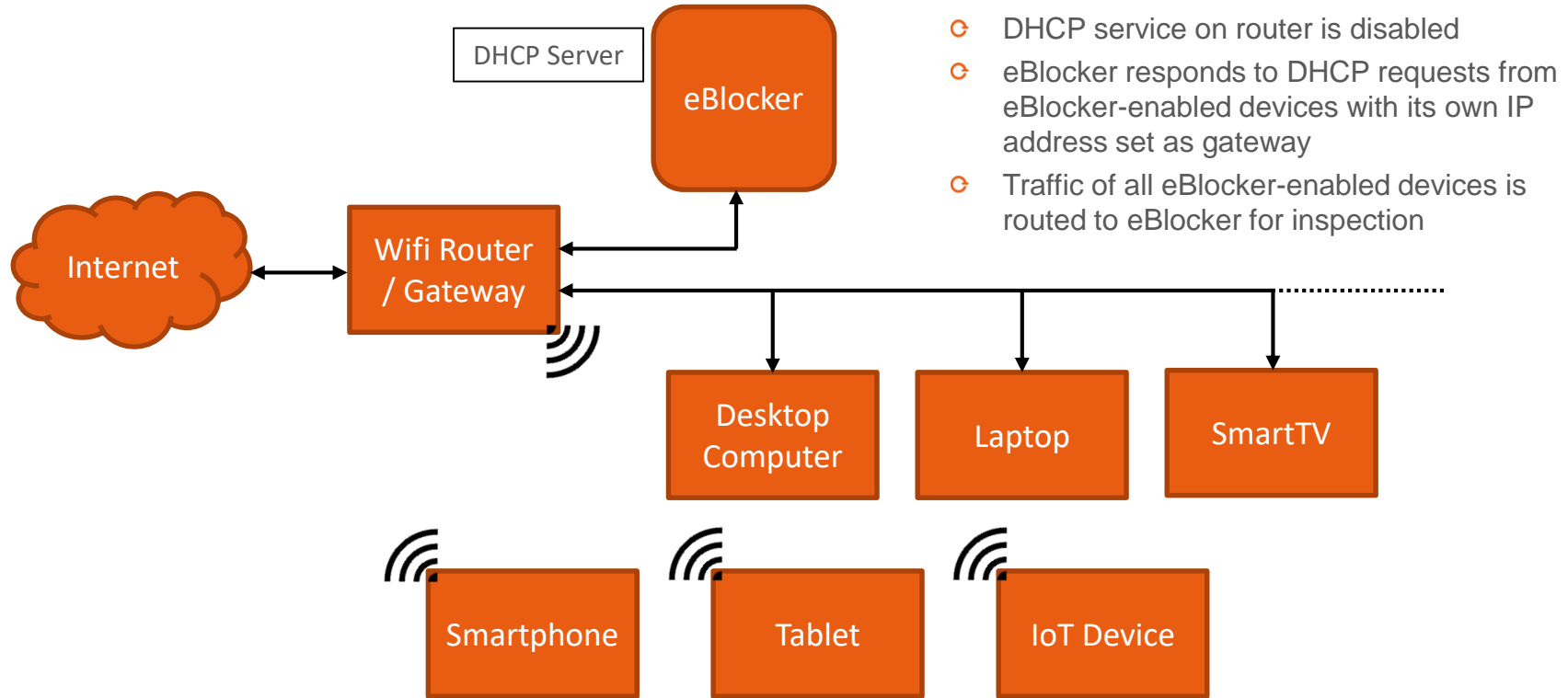
Different ways to integrate eBlocker into home networks

- ⌚ 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



Alternative Setup – Individual Network Mode



eBlocker Architecture and Technical Details

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

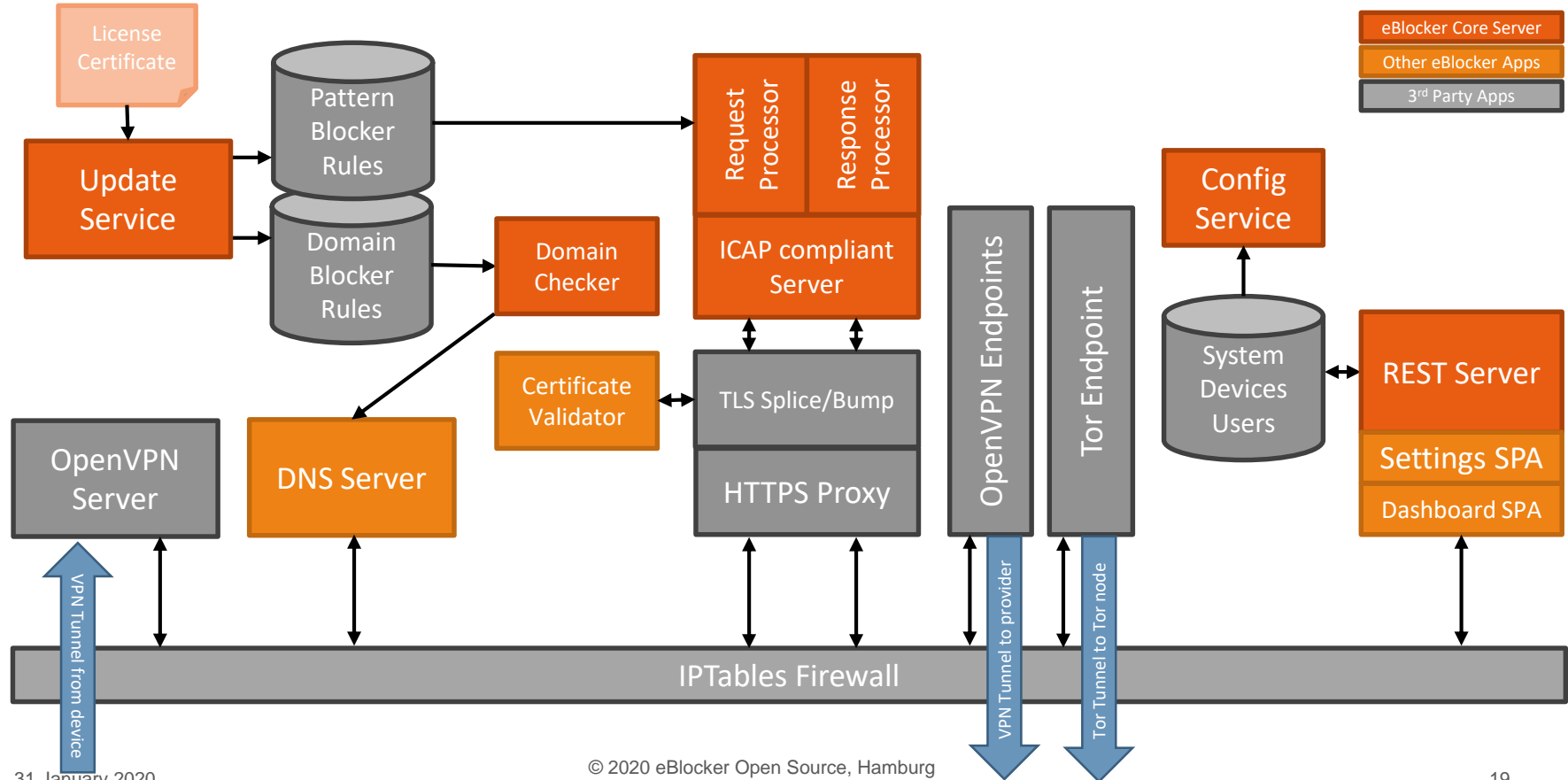
🔄 eBlockerOS

- 🔄 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