



DNS Test 2025

Blocking Rates of Adult Websites

LAST REVISION: 25TH AUGUST 2025

IN COOPERATION WITH: PCGO, PC MAGAZIN

WWW.AV-COMPARATIVES.ORG

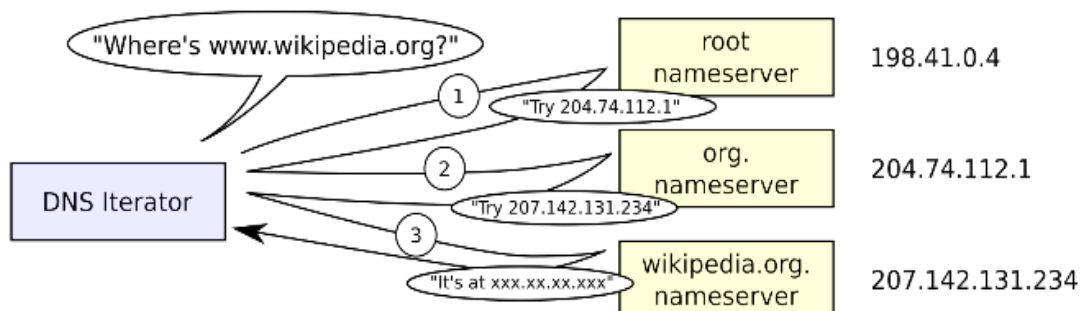
Introduction

In recent years, DNS filtering services have emerged as a practical alternative to traditional parental control tools. Instead of installing software on each device, DNS filtering works at the network level by blocking access to inappropriate or harmful websites before they ever load. With new DNS resolvers entering the market promising enhanced privacy and child protection, consumers face an increasing number of choices.

PCgo and PC Magazin initiated this evaluation partly because two EU-based DNS services, particularly **dns0.eu** and **DNS4EU**, have received widespread media coverage in recent months. They have been portrayed as privacy-friendly, sovereign European alternatives to global DNS providers. With many readers asking whether these new services are truly effective in protecting children online, the magazine sought independent test data to cut through marketing claims and media hype.

To address both the strong public interest in EU-based resolvers and the general uncertainty around the real-world effectiveness of DNS filters, the magazine commissioned AV-Comparatives to carry out this comparative test. The aim is to verify whether these widely discussed solutions live up to their promises of safety and privacy, and to give readers clear, evidence-based guidance on selecting a trustworthy DNS service for family use. To achieve this, **six freely available DNS services** that offer adult content filtering capabilities were selected for evaluation.

What is a DNS Service?



Source: https://commons.wikimedia.org/wiki/File:Example_of_an_iterative_DNS_resolver.svg

The Domain Name System (DNS) is often described as the “phonebook of the internet.” It is a globally distributed service that translates human-readable domain names, such as [av-comparatives.org](https://www.av-comparatives.org), into the numerical IP address computers use to locate servers and deliver content. When a user enters a web address in their browser, their device sends a DNS query to a DNS resolver, which first checks its cache for a stored result. If no match is found, the resolver contacts other DNS servers until it retrieves the correct IP address. Once the match is returned, the device uses it to establish a connection to the destination server and load the requested website. Beyond this fundamental role, DNS can also serve as a control point for managing and filtering internet traffic.

What is DNS Filtering?

DNS filtering works by intercepting requests to known domains and either allowing, blocking, or redirecting them based on predefined rules. In the context of blocking adult content, DNS filtering services maintain regularly updated lists of domains and IP addresses associated with pornography, explicit material, or other categories deemed inappropriate. When a user attempts to visit one of these sites, the DNS filter prevents access typically by displaying a block page or triggering a connection error. Since DNS filtering evaluates domains before any content is downloaded, it can also protect users from malicious or fraudulent sites without ever allowing a connection to be established.

Limitations of DNS Filtering

While DNS filtering is an effective and lightweight solution, it has several limitations. First, it operates at the **domain level**, meaning it cannot control specific pages within a domain. If an otherwise safe website hosts adult content under certain subpages, DNS filters may not block it. Another challenge is the growing use of **encrypted DNS protocols** such as DNS over HTTPS (DoH) and tools like VPNs. These can conceal DNS queries from the filtering service, allowing users to bypass restrictions. Similarly, if filtering is configured only at the **router or network level**, it may not apply once a device switches to mobile data or connects to a different network. DNS filters also rely on blocklists, meaning there can be **false positives**, where legitimate sites are wrongly blocked, and **false negatives**, where new or obscure adult domains remain accessible until added to the list.

Comparison with Conventional Parental/Web Control Products

When it comes to protecting users, especially children, from inappropriate or harmful online material, DNS filtering and conventional parental control products share the same goal. However, they achieve it through different methods and with varying levels of control.

- **Content Restriction:** Both approaches are designed to prevent access to unsuitable websites.
- **Customizable Settings:** Many services in both categories allow administrators or parents to choose filtering categories, create exceptions, and whitelist trusted domains.
- **Activity Insights:** Some DNS filtering services, like many parental control products, provide reports on blocked attempts and browsing patterns, helping caregivers monitor online behaviour.
- **Level of Control:** DNS filtering operates at the domain level, blocking entire websites based on their addresses, while parental control software can be more granular, sometimes filtering individual pages, images, or even search results.
- **Deployment:** DNS filtering can be applied at the router or network level, protecting all connected devices without requiring installation on each one. By contrast, parental control software typically requires installation on each device, which demands more setup but allows for user- or device-specific rules.
- **Bypass Resistance:** Parental control solutions often include tamper-resistant features, such as password protection, app blocking, and time management tools, making it more difficult for children or teens to circumvent restrictions. DNS filtering, however, is easier to bypass using encrypted DNS services, VPNs, or by simply switching to alternative networks.
- **Feature Scope:** While DNS filtering focuses primarily on content restriction and security, parental control products often include additional features such as screen-time limits, geolocation tracking, social media monitoring, and app usage management.

Tested Products

Each service either blocks adult content by default or provides the option to enable such filtering. Additionally, all products offer a free tier which was used in testing. Below, the full list of tested products along with a brief description and link to their respective website is provided. This selection includes established global DNS providers and newly introduced EU-based resolvers that have recently gained media attention, allowing readers to compare their effectiveness under the same conditions.

CleanBrowsing: The US-based company offers a free DNS service with multiple filtering levels, including malware protection. Strong track record among tech-savvy families seeking customizable protection.

Website: <https://cleanbrowsing.org/>

Control D: The Canada-based spin-off company of Windscribe offers adult content filtering and other filtering options, with flexible configuration for various use cases.

Website: <https://controld.com/free-dns>

dns0.eu: The French non-profit founded by NextDNS co-founders advertises having a fully EU-based infrastructure. It prioritizes child safety and privacy while maintaining full GDPR compliance.

Website: <https://www.dns0.eu/>

DNS4EU: The EU-based resolver is supported by the European Union and aims to reduce dependence on non-European DNS services. It provides content filtering and ensures compliance with GDPR standards.

Website: <https://www.joindns4.eu/>

NextDNS: The highly customizable DNS service offers many options as well as analytics. Popular among advanced users due to its detailed reporting options.

Website: <https://nextdns.io/>

Yandex Family DNS: The Russian tech company and search-engine provider Yandex offers different DNS options. The family option is designed to block adult content and dangerous websites and demonstrated a strong blocking rate in this test.

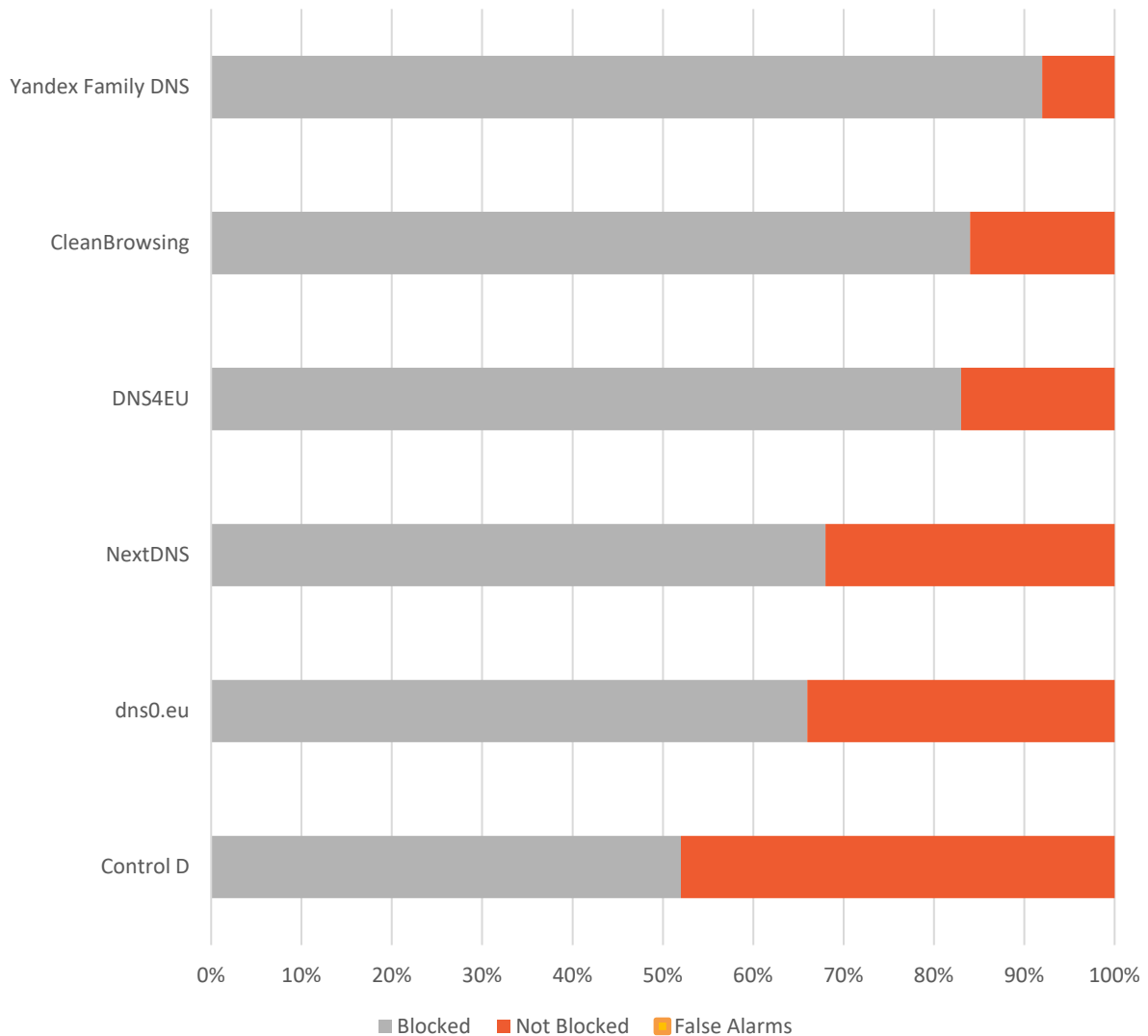
Website: <https://dns.yandex.com/>

Test Procedure

In this test, each evaluated product was configured according to the provider's official instructions, with adult content filtering enabled. DoH was enabled where available. To measure effectiveness, each service was tested against **1,000 unique adult websites**. In addition, a separate set of **200 child-friendly websites** was used to identify potential false positives. The test was performed in **July 2025**.

Test Results

The chart and table below present the detection rate for each tested product, along with the number of false positives.



	Blocked	False Alarms
Yandex Family DNS	92%	0
CleanBrowsing	84%	0
DNS4EU	83%	0
NextDNS	68%	0
dns0.eu	66%	0
Control D	52%	0

Only one service blocked over 90% of adult websites, while the lowest-performing solution blocked just over half. This shows that effectiveness varies widely between providers.

Discussion

This evaluation reflects two key factors driving public interest: first, the recent spotlight on European DNS initiatives promising digital sovereignty and strict GDPR compliance, and second, the lack of independent verification of how well free DNS solutions block adult content. By publishing this study, the commissioning magazine provides readers with reliable, impartial data beyond headlines and marketing messages.

From a consumer's perspective, choosing a free DNS service should balance two key factors: blocking unwanted content effectively and safeguarding privacy. **Yandex Family DNS** blocked the most adult content in this test (**92%**), while **Control D** blocked the least (**52%**), indicating clear room for improvement. EU-based services like **dns0.eu** and **DNS4EU** provide strong privacy assurances but currently allowed more adult websites through. This means that none of the single solution excels in both areas today. Notably, none of the tested products generated false alarms, meaning no child-friendly websites were incorrectly blocked. This suggests that, although filtering effectiveness varies, the precision of the tested solutions is consistently high.

These findings underline the importance of carefully selecting a DNS filtering service that offers robust protection against inappropriate content with little to no risk of over-blocking safe websites. However, consumers should also consider factors such as privacy, digital sovereignty, and legal compliance. Services operating entirely within the European Union, such as dns0.eu and DNS4EU, benefit from GDPR compliance and EU-based infrastructure. This ensures DNS traffic remains subject exclusively to EU law and strengthens protection against foreign surveillance and data misuse.

For vendors, the **results indicate clear areas for improvement**. Those with lower detection rates could benefit from integrating more comprehensive and regularly updated content classification databases or leveraging advanced machine-learning models. Collaboration with security organizations and independent testing bodies may also help refine their solutions and provide greater transparency to users. Vendors operating outside the EU could address privacy concerns by deploying infrastructure in Europe to better serve privacy-conscious users.

To put these results in context, AV-Comparatives provides certification for parental control software each year. In order to be certified, a product must block **at least 95%** of pornographic websites and have zero false alarms on child-friendly websites. While established parental/web control products tested by AV-Comparatives often meet this benchmark, the DNS filtering services tested here demonstrated lower detection rates.

Nonetheless, DNS-based solutions remain attractive due to their simplicity, low cost, and ability to provide network-wide coverage across multiple devices. While they may not yet match the performance of dedicated parental control software, they can serve as an effective first layer of defence. For parents seeking maximum protection, pairing a free DNS service with dedicated parental control software is recommended. DNS filtering alone may not be sufficient to block all adult content.

Vendors interested in having their products tested in 2026 are welcome to contact us for further details. The reports for parental control products certified in 2025 can be found on our website: <https://www.av-comparatives.org/news/parental-control-certification-test-2025/>



Copyright and Disclaimer

This publication is Copyright © 2025 by AV-Comparatives®. Any use of the results, etc. in whole or in part, is ONLY permitted after the explicit written agreement of the management board of AV-Comparatives prior to any publication. AV-Comparatives and its testers cannot be held liable for any damage or loss, which might occur as result of, or in connection with, the use of the information provided in this paper. We take every possible care to ensure the correctness of the basic data, but a liability for the correctness of the test results cannot be taken by any representative of AV-Comparatives. We do not give any guarantee of the correctness, completeness, or suitability for a specific purpose of any of the information/content provided at any given time. No one else involved in creating, producing or delivering test results shall be liable for any indirect, special or consequential damage, or loss of profits, arising out of, or related to, the use or inability to use, the services provided by the website, test documents or any related data.

For inquiries you can contact us via our contact form: <https://www.av-comparatives.org/contact/>

These results can be used by editors/media/bloggers etc. for free. Please give as source <https://www.av-comparatives.org>.

AV-Comparatives
(September 2025)