D

DNS Filtering: How It Works, Response Types, Limits, and Setup

Learn how DNS filtering blocks harmful or prohibited domains, what response policies do, how encrypted DNS affects coverage, and how to deploy it safely.

PUBLISHER
Gridinsoft Support

UPDATED
Oct 8, 2026

READ TIME
4 min

CONTENTS

In this guide

01 DNS filtering vs. web and URL filtering
02 How DNS filtering works
03 Common blocking responses
04 What DNS filtering can block
05 DNS filtering versus DNSSEC and encrypted DNS
06 Limitations
07 Safe deployment checklist
08 Troubleshoot a blocked domain

DNS filtering applies security or acceptable-use policy when a device asks a DNS resolver for a domain name. The resolver can return the normal answer, refuse the request, return `NXDOMAIN`, or redirect the user to a block page. Because the decision happens before a connection to the destination, DNS filtering can stop many phishing, malware, command-and-control, and prohibited-domain requests early.

01 DNS filtering vs. web and URL filtering

DNS filtering normally makes a decision for an entire domain before a connection begins. URL or web filtering can evaluate a complete address, page category, request, or downloaded content, so it can be more granular but requires visibility at a later layer. DNS filtering is lightweight and broadly applicable; it should complement rather than be confused with secure web gateways, browser controls, or file inspection.

02 How DNS filtering works

1. A device asks its configured recursive DNS resolver for a domain such as `example.com`.
2. The resolver checks local policy, threat intelligence, category data, allowlists, and blocklists.
3. If the domain is allowed, the resolver completes normal resolution and returns the appropriate records.
4. If policy blocks the domain, the resolver returns a controlled response and records the event when logging is enabled.

Filtering can run on a home router, endpoint agent, enterprise resolver, cloud protective-DNS service, or a combination of these. The enforcement point must actually receive the device's DNS queries.

03 Common blocking responses

Response	Effect and consideration

`NXDOMAIN`	Tells the client that the domain does not exist. Simple, but users may not know a policy caused the failure.
`REFUSED`	The resolver declines to answer under its policy.
Sinkhole address	Returns a controlled address for monitoring or containment. Protect the sinkhole and avoid collecting unnecessary data.
Block-page redirect	Explains the policy and reporting process, but HTTPS and certificate behavior make transparent redirects difficult for many sites.

04 What DNS filtering can block

- Domains associated with phishing, malware delivery, scams, or command-and-control infrastructure.
- Newly registered or newly observed domains when organizational policy treats them as higher risk.
- Content categories prohibited by a school, family, or workplace policy.
- Custom domains identified during an incident.
- Known tracking or advertising domains when privacy policy allows that use.

Category and reputation systems are not perfect. A legitimate site can be compromised, a malicious site can use a reputable hosting platform, and a newly created domain may not yet have a classification.

05 DNS filtering versus DNSSEC and encrypted DNS

DNSSEC validates signed DNS data and helps detect forged or altered answers. It does not decide whether a legitimate domain is safe and does not replace filtering.

DNS over HTTPS (DoH) and **DNS over TLS (DoT)** encrypt traffic between the client and resolver. They protect DNS privacy in transit, but an unmanaged resolver can bypass an organization's filtering policy. Managed environments should define which encrypted resolvers

are permitted and prevent fallback to unauthorized alternatives without disabling encrypted DNS unnecessarily.

06 Limitations

- It normally evaluates domains, not the full path after the slash. It may be unable to block one malicious page on an otherwise legitimate platform.
- A direct IP connection can bypass a domain decision.
- Cached answers can delay a new policy until their TTL expires.
- VPNs, proxies, browsers, or malware may use another resolver.
- DNS filtering does not inspect downloaded files or replace endpoint, email, identity, browser, and network controls.

07 Safe deployment checklist

1. Define security and acceptable-use objectives before choosing categories.
2. Cover remote devices as well as the office network.
3. Start with monitoring where practical and measure false positives.
4. Create a documented process for narrow, time-limited exceptions.
5. Protect resolver administration with MFA and least privilege.
6. Retain only the DNS logs needed for security and compliance, with appropriate access and expiration.
7. Test IPv4, IPv6, VPN, guest, mobile, and encrypted-DNS paths.

08 Troubleshoot a blocked domain

Compare the answer from the managed resolver with an approved diagnostic resolver, review the policy category, and check whether a CNAME or newly added subdomain caused the block. Commands such as `nslookup` or `dig` can show the returned status and address. Do not bypass a security block before independently verifying the destination.

For operational implementation and exception handling, see DNS Blocking. For a threat-intelligence-driven protective resolver, see DNS Firewall.

NEED MORE HELP?

We are here when the guide is not enough.

Visit the Gridinsoft Support Center for current product guidance or submit a support request with the details of your case.

Open this guide online at support.gridinsoft.com