DNS Firewall: What it is, why it helps, and how to deploy it safely

Gridinsoft Help Center

Why it matters

Most attacks start with a click or a background connection. Stopping bad domains at the DNS layer cuts off malware downloads, phishing pages, and command-and-control beacons without slowing users or changing their workflow.

How it works

- Device asks DNS for a domain’s IP.
- DNS firewall checks live threat feeds and your allow/deny policies.
- It returns a normal answer for safe domains-or blocks/redirects risky ones.
- Supports response policies (RPZ), categories (malware, phishing, adult, crypto-mining), and custom lists.

Good uses

- Security: block malware/phishing/C2 by default.
- Compliance & productivity: restrict categories at work/school.
- Home networks: one setting protects every device behind the router.

Limits to know

- Won’t catch IP-only traffic or some VPN/Tor tunnels.
- Users can try alternate DNS unless you enforce it on the network.
- False positives happen-keep an allowlist and review logs.

Quick setup

- Choose a reputable DNS firewall (managed service or on-prem with RPZ).
- Force all DNS to it at the router/firewall; block outbound 53/853 to others.
- Enable DoH/DoT to your resolver to prevent tampering.
- Start in monitor mode for a week, then enforce.
- Maintain custom allow/deny lists; alert on malware and phishing blocks.