D

DNS Firewall: Protective DNS, Threat Intelligence, and Deployment

Understand how a DNS firewall combines resolver policy, threat intelligence, logging, and automated response, and how it differs from DNS filtering and network firewalls.

PUBLISHER
Gridinsoft Support

UPDATED
Oct 8, 2026

READ TIME
3 min

CONTENTS

In this guide

01 Two meanings of DNS firewall
02 How a DNS firewall works
03 DNS firewall versus related controls
04 Useful capabilities
05 Deployment architectures
06 Encrypted DNS and bypass prevention
07 Limitations
08 Evaluation checklist

A **DNS firewall** is a protective DNS service that evaluates domain lookups against security policy and threat intelligence. It can block or sinkhole domains associated with phishing, malware, command-and-control, or data exfiltration and produce DNS telemetry for investigation. The term describes a security role; it is not the same as a packet-filtering network firewall.

01 Two meanings of DNS firewall

The name is used for two related but different services. A **recursive protective-DNS firewall** evaluates lookups made by users and devices, blocking destinations under policy. An **authoritative DNS firewall** or DNS proxy protects an organization's authoritative name servers from attacks and abusive query traffic while caching valid answers. Confirm which direction and assets a product protects before comparing features.

02 How a DNS firewall works

1. Managed devices send DNS queries to an approved recursive resolver.
2. The service evaluates the domain, request context, organizational policy, and current threat intelligence.
3. Allowed queries receive normal validated DNS processing.
4. Blocked queries receive a controlled response such as `NXDOMAIN`, `REFUSED`, or a sinkhole address.
5. The event can create an alert, enrich an incident, or trigger an authorized response workflow.

03 DNS firewall versus related controls

Control	Primary decision point
DNS filtering	Broad concept of applying security or content policy during name resolution.

Control	Primary decision point
DNS blocking	Specific rule or action that prevents a domain from resolving normally.
DNS firewall / protective DNS	Managed security capability combining filtering, threat intelligence, telemetry, and operations.
Network firewall	Filters connections by addresses, ports, protocols, state, and sometimes application identity.
Secure web gateway	Evaluates web requests and content, often including full URLs, files, users, and browser policy.

04 Useful capabilities

- Rapid threat-intelligence updates and custom incident blocklists.
- Support for RPZ or equivalent policy distribution.
- Coverage for on-premises, roaming, cloud, and remote devices.
- Visibility into blocked queries, requesting assets, and policy reasons.
- Integration with SIEM, SOAR, EDR, asset inventory, and incident workflows.
- Protection against selected domain-generation, look-alike, newly observed, or DNS-tunneling patterns.

Machine-learning labels and “new domain” categories are probabilistic. They need monitoring, exception handling, and human review for significant business impact.

05 Deployment architectures

- **Forwarding resolver:** internal resolvers forward eligible queries to the protective service.
- **Direct endpoint:** managed devices use a cloud resolver or agent, including away from the office.
- **Hybrid:** internal names stay on enterprise resolvers while public queries receive protective processing.

- **Cloud-native:** cloud workloads use provider or security-service integrations with centralized policy and logging.

Preserve split-horizon and private DNS behavior. Sending internal names to an external resolver can leak architecture details or break applications.

06 Encrypted DNS and bypass prevention

DoH and DoT can secure traffic to the approved resolver. The deployment should support encrypted transport while controlling unauthorized resolvers on managed devices. Test browser-specific settings, VPN clients, guest networks, IPv6, containers, and mobile devices. Avoid blocking encrypted DNS globally when allowlisting managed endpoints can meet both security and privacy needs.

07 Limitations

- DNS sees domain requests, not every full URL or downloaded file.
- Direct IP connections and unmanaged resolvers can bypass policy.
- Shared hosting and compromised legitimate services complicate domain-level blocking.
- Cached answers can postpone a new block.
- DNS telemetry cannot by itself prove that a user visited or interacted with a site.

08 Evaluation checklist

1. Measure resolver uptime, latency, geographic coverage, and failover behavior.
2. Test detection quality and false-positive response time.
3. Confirm logging fields, retention, export, privacy, and tenant separation.
4. Evaluate remote-device, IPv6, encrypted-DNS, and private-zone support.
5. Verify administrative MFA, role separation, change history, and API security.
6. Run a pilot with realistic domains and documented rollback.

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