D

DNS Tunneling: How It Works, Detection, and Prevention

Learn how attackers encode command traffic or stolen data in DNS queries, which signals are useful, and how resolver controls reduce risk.

PUBLISHER
Gridinsoft Support

UPDATED
Oct 8, 2026

READ TIME
3 min

CONTENTS

In this guide

01 How DNS tunneling works
02 DNS tunneling vs. ordinary DNS
03 Detection signals
04 How to investigate suspected tunneling
05 How to prevent DNS tunneling
06 Containment and response
07 Common detection mistakes
08 DNS logging and privacy

DNS tunneling uses DNS queries and responses to carry data that is not ordinary name-resolution information. Legitimate products may use DNS for specialized functions, but attackers can create a covert channel for command and control or data exfiltration when

DNS is widely allowed through a network.

A tunnel is not identified simply because a domain has many subdomains. Detection needs context, baselines, and multiple signals to avoid blocking content delivery, email authentication, telemetry, or other legitimate uses.

01 How DNS tunneling works

1. An attacker controls a domain and its authoritative DNS server.
2. Malware encodes data into subdomain labels or selected query fields.
3. The organization's resolver forwards the query toward the attacker's server.
4. The server decodes the data and may encode instructions in the response.
5. Repeated queries form a low-bandwidth channel through normal DNS infrastructure.

Caching, label-length limits, and resolver behavior constrain the channel, so tools split and encode data across many queries.

For example, malware can encode a small fragment of stolen data into a label such as `encoded-data.example.com`. Recursive resolvers carry the lookup to the authoritative server controlled by the attacker, where the fragment can be recorded and decoded. Responses can carry small commands back to the infected device.

02 DNS tunneling vs. ordinary DNS

Normal DNS maps names to records and supports functions such as email routing and domain verification. Tunneling treats names or responses as a transport. Some security and networking products also use unusual DNS patterns legitimately. Classification should consider the requesting process, destination domain, query history, and business purpose.

03 Detection signals

- Very long, high-entropy, or frequently changing subdomain labels.

- Large volumes of unique queries beneath one parent domain.
- Unusual TXT or other record types for a user or device.
- Regular beacon-like timing or queries continuing while the user is idle.
- High NXDOMAIN rates or abnormal request-to-response sizes.
- A process making DNS requests that does not normally need network access.

Encrypted DNS can reduce visibility at a network sensor, which makes endpoint and approved-resolver telemetry more important.

04 How to investigate suspected tunneling

1. Identify the source device, user, process, resolver, and first-seen time.
2. Group queries by registered domain and decode samples only in an authorized analysis environment.
3. Review endpoint process trees, persistence, files, and network connections.
4. Check domain registration, authoritative name servers, and activity elsewhere in the organization.
5. Preserve raw DNS, endpoint, identity, and proxy logs before retention expires.

05 How to prevent DNS tunneling

Require clients to use managed resolvers and block direct outbound DNS to the Internet except from those resolvers. Control unapproved DNS-over-HTTPS and DNS-over-TLS according to policy. Apply DNS filtering, threat intelligence, query analytics, and egress restrictions. Endpoint controls should prevent unknown programs from running even when a DNS channel is available.

06 Containment and response

Isolate the affected host, block confirmed malicious domains and infrastructure, and remove the initiating malware or unauthorized tool. Determine what data may have crossed the channel and whether other command paths exist. Rotate credentials or secrets accessible to the process, then eradicate persistence and patch the initial access vector before restoration.

07 Common detection mistakes

Do not rely only on domain blocklists or a fixed label-length threshold. Attackers can rotate domains and use low-volume channels, while legitimate services can create random-looking labels. Baseline by device and application, combine statistical signals with endpoint context, and give analysts the original query—not only an alert score.

08 DNS logging and privacy

DNS logs can reveal users’ browsing and application activity. Restrict access, define retention, minimize unnecessary collection, and document monitoring. Security value comes from timely, well-scoped telemetry rather than retaining every query indefinitely.

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