DNS Tunneling: What it is, red flags to spot, and how to block it fast

Gridinsoft Help Center

What it is

How it works

- Malware on a device chops data into tiny chunks and encodes it in subdomains.
- Your resolver forwards those lookups to the attacker’s authoritative DNS server.
- The attacker decodes the data from the queries or sends back instructions in DNS answers.
- Result: command-and-control and data exfiltration that looks like normal DNS traffic.

What you might notice

- Lots of very long or random-looking domains (gibberish labels).
- Unusual spikes in TXT record queries or NXDOMAIN responses.
- Constant DNS traffic to a single strange domain or newly registered zones.
- Endpoints making DNS queries at odd hours with steady, periodic bursts.

If you suspect it

- Block the suspicious domain/NS at DNS and firewall; capture samples.
- Isolate affected hosts and run a full malware/EDR sweep.
- From a clean admin box, rotate credentials and tokens used on that host.
- Review logs to scope what left and who else is talking to the same domain.

Prevent it

- Use a DNS filter/firewall with tunneling detections (length, entropy, TXT/NXDOMAIN heuristics).
- Egress control: only allow DNS to approved resolvers; block outbound 53/853 elsewhere.
- Turn on DoH/DoT to your resolver; log queries centrally and alert on anomalies.
- Segment networks and least-privilege access so one host isn’t a gateway to all data.
- Keep endpoints patched and monitored (EDR) to stop the malware that starts the tunnel.