CHECKLIST

Checklist: Detecting DNS Tunneling in Encrypted Traffic

A practical, vendor-neutral checklist for validating suspicious encrypted DNS activity using resolver logs, endpoint telemetry, flow patterns, and baseline comparison before taking action.

Checklist: Detecting DNS Tunneling in Encrypted Traffic

Use this checklist when encrypted DNS traffic looks unusual and you need to decide whether it is normal privacy traffic, a misconfiguration, or a covert channel.

1) Confirm the transport and scope

- [ ] Verify the traffic is actually encrypted DNS (DoH, DoT, or similar), not generic TLS.
- [ ] Identify the client, user, host role, and network segment involved.
- [ ] Determine whether the endpoint is expected to use encrypted DNS.
- [ ] Confirm whether the organization permits encrypted DNS to external resolvers.
- [ ] Check whether the traffic is from a browser, OS resolver, security agent, VPN client, or unknown process.

2) Establish a baseline before judging behavior

- [ ] Compare current activity to the host?s normal DNS behavior.
- [ ] Compare the host to peer systems with the same role.
- [ ] Review whether the destination resolver is common in the environment.

- [ ] Check whether the volume, cadence, and session duration are new or unusual.
- [ ] Look for recent software installs, browser changes, or policy changes that could explain the behavior.

3) Review resolver-side telemetry

If you can inspect the recursive resolver, review the following:

- [ ] Query names for long labels or unusual structure.
- [ ] Subdomains that appear random, encoded, compressed, or base64-like.
- [ ] Repetitive requests with little variation.
- [ ] Many short-lived lookups to the same parent domain.
- [ ] Low cache reuse or a high rate of unique names.
- [ ] Queries from a single host that appear in a steady, automated pattern.

Resolver red flags

- [ ] Long, variable subdomains that resemble data chunks.
- [ ] High-frequency lookups with minimal business justification.
- [ ] The same domain queried across many unique labels.
- [ ] Query bursts that continue for long periods without user activity.

4) Review endpoint and host telemetry

- [ ] Identify the process generating encrypted DNS traffic.
- [ ] Check parent process, command line, and file location.
- [ ] Confirm whether the process is expected to use DNS at all.
- [ ] Review whether the host bypasses managed resolver settings.
- [ ] Check for recent persistence mechanisms, scheduled tasks, or startup items.

- [ ] Correlate activity with user logon sessions and interactive use.

Endpoint red flags

- [ ] A non-browser process initiating encrypted DNS.
- [ ] A newly installed or unknown process making regular DNS requests.
- [ ] A workstation acting like an automated service.
- [ ] A server or kiosk using browser-oriented DNS behavior.

5) Analyze flow and timing patterns

- [ ] Measure session duration and request cadence.
- [ ] Look for fixed intervals or highly regular bursts.
- [ ] Check whether traffic is concentrated to a narrow set of destinations.
- [ ] Review message size consistency and repetition.
- [ ] Compare timing against normal application behavior on the same host.

Flow red flags

- [ ] Requests at a steady cadence with little jitter.
- [ ] Small, repetitive exchanges over long periods.
- [ ] A narrow destination set with no clear business purpose.
- [ ] New encrypted DNS destinations that are rare across the environment.

6) Correlate signals before escalating

Require multiple weak indicators rather than one isolated anomaly.

- [ ] One signal: unusual destination.

- [ ] Second signal: unusual query cadence or volume.
- [ ] Third signal: long, random-looking, or repetitive names in resolver logs.
- [ ] Fourth signal: unexpected process or recent installation on the host.

If you have at least two independent anomalies, escalate for deeper review.

7) Decide whether the behavior is likely benign or suspicious

Likely benign

- [ ] A known browser or privacy tool using an approved resolver.
- [ ] Traffic consistent with the host?s historical baseline.
- [ ] A common resolver service used broadly across the environment.
- [ ] No unusual process, timing, or naming patterns.

Likely suspicious

- [ ] The host uses external encrypted DNS outside approved paths.
- [ ] Resolver logs show encoded or high-entropy-looking labels.
- [ ] Requests are repetitive, frequent, and machine-like.
- [ ] The activity comes from an unexpected process.
- [ ] The destination is rare or newly observed in the environment.

8) Validate before blocking or changing policy

- [ ] Estimate the blast radius of any enforcement change.
- [ ] Test whether the destination is required by a legitimate application.

- [ ] Confirm whether blocking would break browsing, update services, VPNs, or security tools.
- [ ] Prepare a rollback path.
- [ ] If possible, test enforcement on a small scope first.
- [ ] Document the evidence used to reach the decision.

9) Recommended investigation questions

- [ ] What changed on the host before the behavior started?
- [ ] Is the destination resolver approved for this endpoint type?
- [ ] Does the resolver see long or structured labels?
- [ ] Does the process match the user?s normal software set?
- [ ] Do peer hosts show the same encrypted DNS pattern?
- [ ] Is the behavior tied to a specific application, user action, or schedule?

10) Quick triage decision guide

Treat as lower priority when

- [ ] The traffic is from a known application.
- [ ] The destination is approved and common.
- [ ] The pattern matches the host?s baseline.
- [ ] No resolver-side anomalies are present.

Escalate when

- [ ] The host bypasses managed resolver controls.

- [ ] Resolver logs show encoded, repetitive, or high-entropy-looking subdomains.
- [ ] The process is unexpected or newly installed.
- [ ] The timing is regular and automated.
- [ ] The destination is rare and the behavior differs from peers.

Analyst note

Encrypted DNS does not make tunneling invisible. The best approach is to combine resolver-side evidence, endpoint telemetry, flow timing, and baseline comparison. Avoid acting on a single weak signal. Validate first, then enforce.

Optional evidence log

- Host: _____
- User: _____
- IP address: _____
- Encrypted DNS type: _____
- Destination resolver: _____
- Process name: _____
- Parent process: _____
- Key anomalies observed: _____
- Baseline comparison result: _____
- Decision: _____
- Rollback plan: _____