

Forum:[Hack Forums](#)

Thread: [DoH vs DoT?](#)

schassis - August 2, 2025, 8:28 pm

When should I use DoH instead of DoT or vise versa?

skull - August 3, 2025, 3:17 am

Both requests are encrypted.

Only difference is which port I turns over, DoH allows a DNS lookup to run on port 443, simulating a HTTPS request instead of a DNS request.

So use DoH when you wish for your DNS request to blend in with any other HTTPS requests.

??????????? - August 4, 2025, 3:22 am

(Aug 2, 2025 08:28 PM)schassis Wrote: [\[CITE\]](#) When should I use DoH instead of DoT or vise versa?

Feature -- DoH (DNS over HTTPS) VS DoT (DNS over TLS)

TransportHTTPS (TCP 443)TLS (TCP 853)

Visibility to networkBlends into regular HTTPS (harder to distinguish)Distinct traffic on port 853 (easier to monitor/control)

Blocking resistanceHigher in censoring/restrictive networks (looks like normal web)Lower—can be blocked by filtering port 853

Deployment granularityPer-app (e.g., browser) or system if supportedTypically system-/router-wide

PrivacyGood, but can be centralized by resolver; hidden in HTTPSGood and more transparent to admins (less hidden layering)

PerformanceSlightly higher overhead due to HTTP framingLeaner (no HTTP layer)

Policy/controlHarder for enterprises to gate/inspectEasier to integrate with network policies

Typical use caseIndividual user privacy on untrusted networks or bypassing filteringSystem-wide encrypted DNS in managed or home environments

Final Thoughts: Use DoT for clean, system-wide encrypted DNS when you control the network or need straightforward policy enforcement; use DoH to blend into HTTPS for censorship resistance or per-application privacy.