DNS over TLS (DoT)

Inhaltsverzeichnis

DNS over TLS (DoT) verschlüsselt DNS-Traffic über einen dedizierten TLS-Kanal, typischerweise Port 853. Es schützt Abfragen vor passivem Mithören und Pfadmanipulation.

1 Funktionsweise

Client und Resolver bauen eine TLS-Sitzung auf und tauschen darüber DNS-Nachrichten aus. Im Gegensatz zu DoH bleibt es ein eigenes DNS-Protokoll hinter TLS.

- **Port 853:** üblicher DoT-Endpunkt
- **TLS-Auth:** Serverzertifikat prüfbar
- **Stub-/Upstream-Resolver:** lokal oder zentral nutzbar

2 Typische Einsatzbereiche

- Härtung von Stub-Resolvern auf Clients und Servern
- Verschlüsselter Upstream zu öffentlichen oder eigenen Resolvern
- Privacy in Netzen ohne vertrauenswürdige DNS-Infrastruktur

3 Wichtige Hinweise

- DoT ist oft leichter zu erkennen/filtern als DoH.
- Zertifikats- und Resolver-Pinning erhöhen Sicherheit.
- Interne Split-DNS-Szenarien brauchen passende Architektur.

4 Fazit

DoT ist der direkte Weg zu verschlüsseltem DNS – klarer als DoH im Protokoll, mit vergleichbarem Schutz auf dem Transportweg.