DNS over HTTPS (DoH)

Inhaltsverzeichnis

DNS over HTTPS (DoH) verschlüsselt DNS-Anfragen in HTTPS-Verbindungen. Damit werden Abfragen vor Mithören und Manipulation auf dem Transportweg geschützt und lassen sich schwerer als klassisches DNS filtern.

1 Funktionsweise

Der Client sendet DNS-Fragen an einen DoH-Endpunkt per HTTPS statt unverschlüsselt an Port 53. Antworten kommen ebenfalls geschützt zurück.

- **TLS-Tunnel:** Schutz von Inhalt und Integrität
- **Standard-HTTPS:** oft Port 443, ähnlich normalem Webtraffic
- **Resolver-Wahl:** Vertrauen in den DoH-Anbieter nötig

2 Typische Einsatzbereiche

- Privacy auf offenen/unsicheren Netzen
- Browser- und System-Resolver mit DoH-Support
- Umgehung einfacher DNS-Manipulation im lokalen Netz

3 Wichtige Hinweise

- Enterprise-Filter über klassisches DNS können wirkungslos werden.
- Der DoH-Anbieter sieht weiterhin die Abfragen.
- DoT (DNS over TLS) ist die verwandte Alternative.

4 Fazit

DoH erhöht den Transportschutz von DNS spürbar – mit dem Trade-off, dass Sichtbarkeit und Kontrolle ins Resolver-Vertrauensmodell wandern.