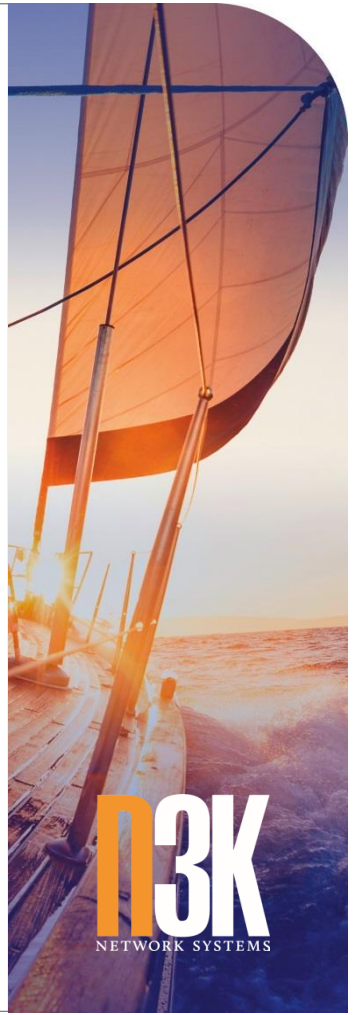
n3k
NETWORK SYSTEMS

DNS – Verschlüsselung mit DNS over TLS und DNS over HTTPS

n3k NETWORK SYSTEMS

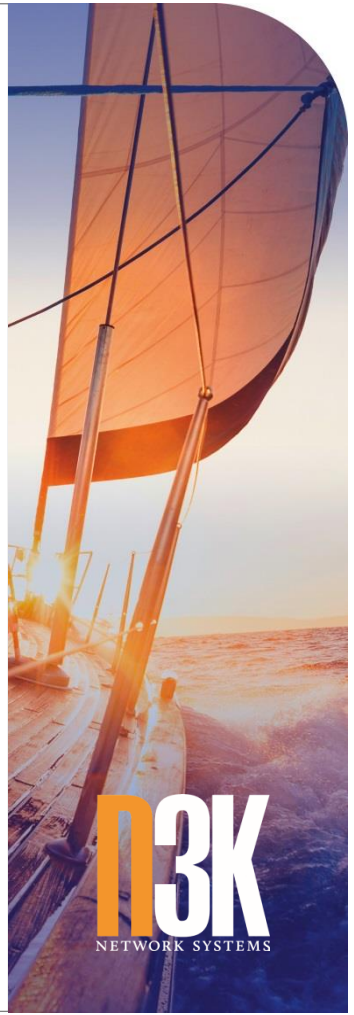
Warum DNS-Anfragen verschlüsseln?

- Ausspähen von DNS-Verkehr möglich
- DNSSEC kann Authentizität einer DNS-Antwort nur bis zum DNS-Server sicherstellen
- Beides insbesondere bei Nutzung von Cloud-DNS-Diensten problematisch

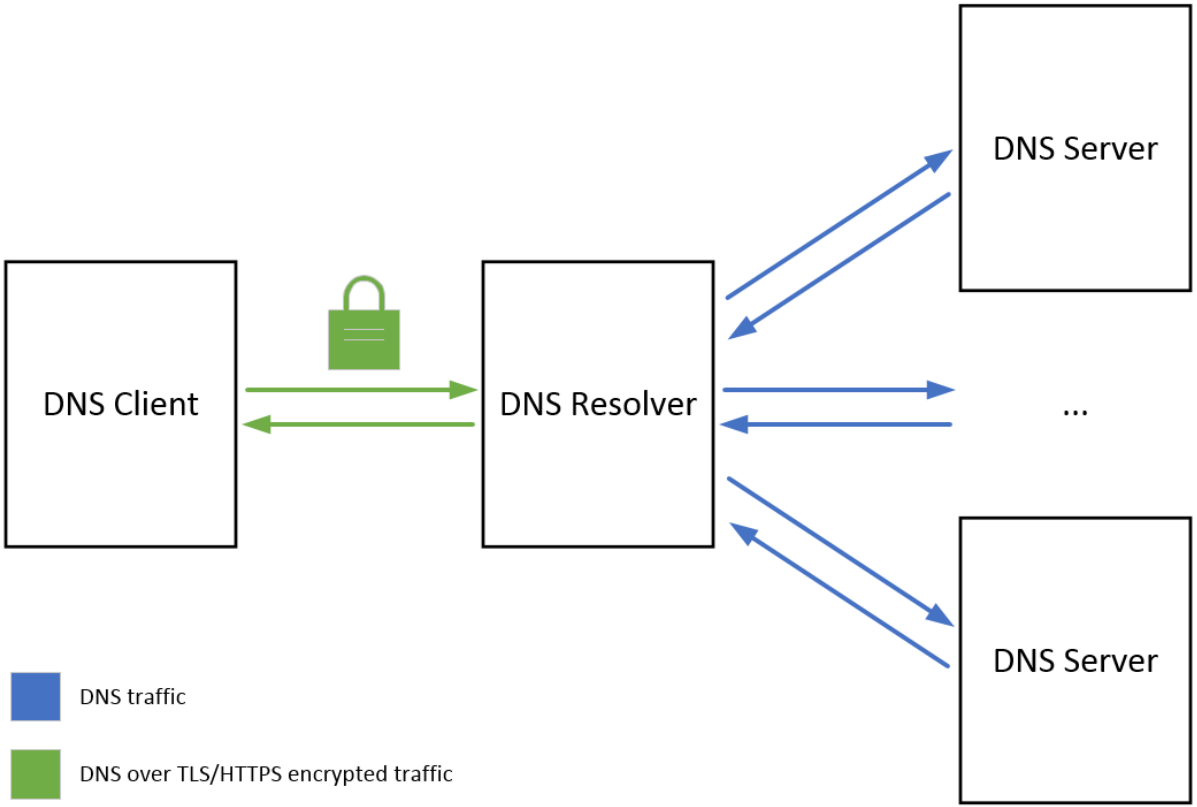


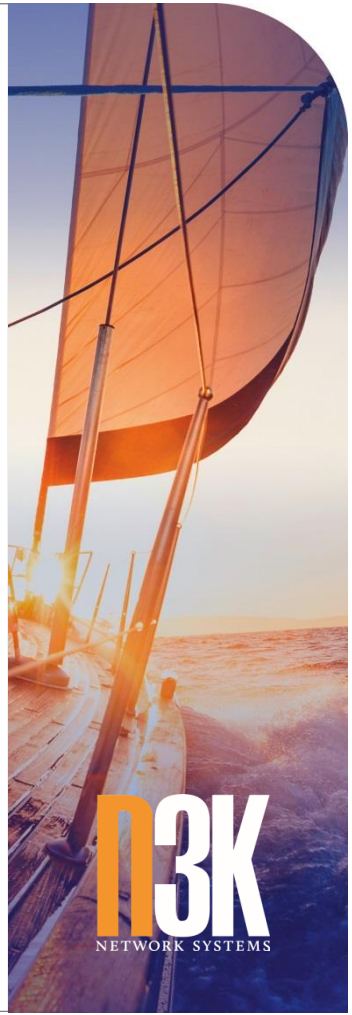
DNS over TLS/HTTPS

- Absicherung der „Last Mile“
- Verschlüsselte Verbindung zwischen DNS-Client und DNS-Resolver
  - Schützt die Vertraulichkeit (und Integrität) der Daten
  - Verhindert Ausspähen und Angriffe innerhalb dieser Verbindung



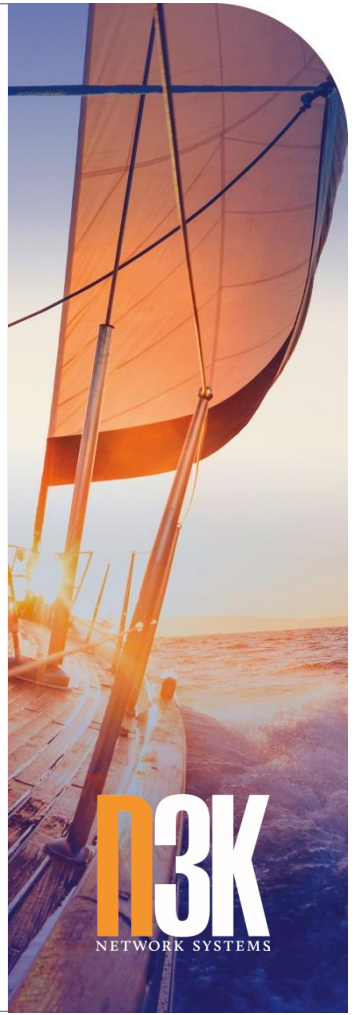
DNS over TLS/HTTPS



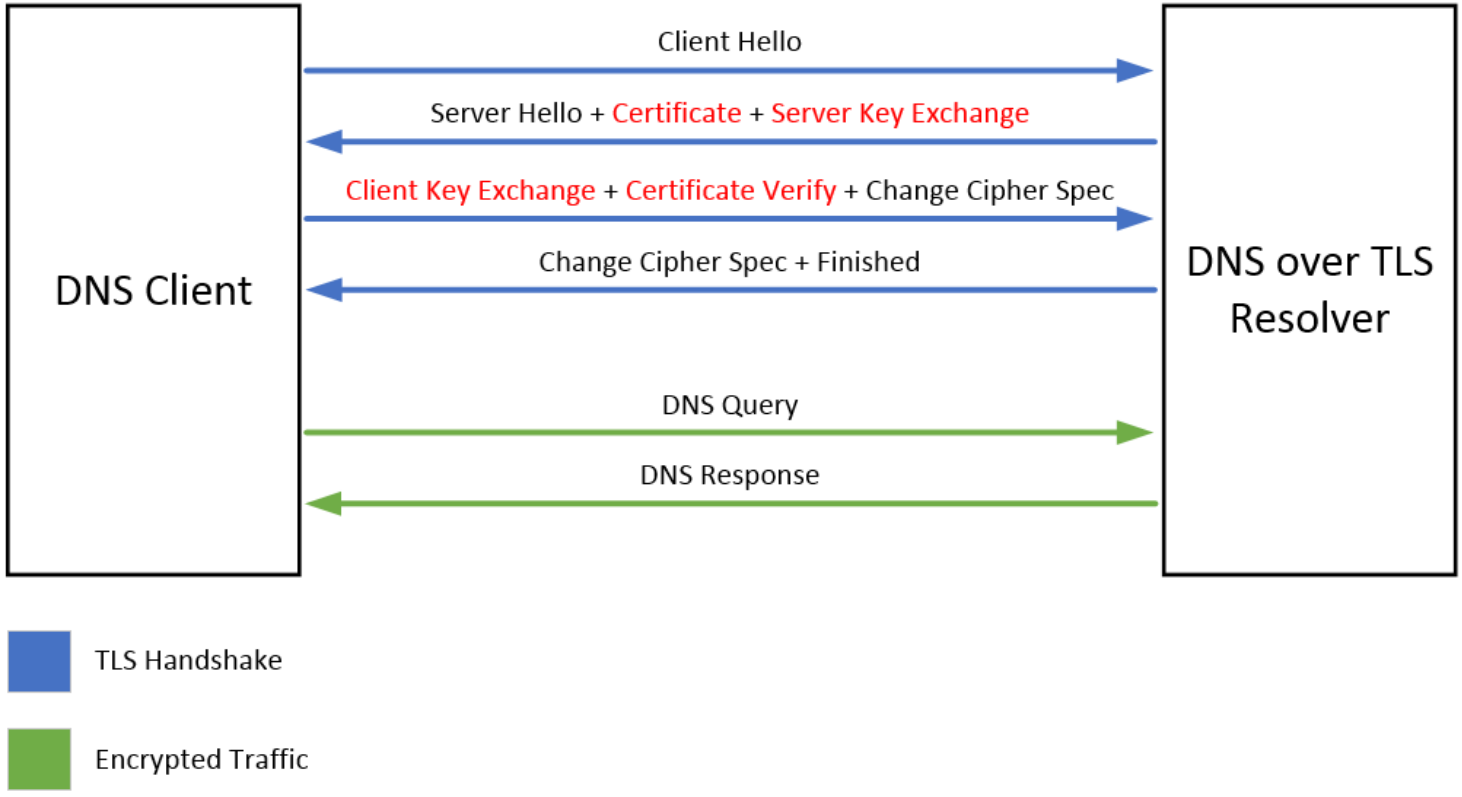


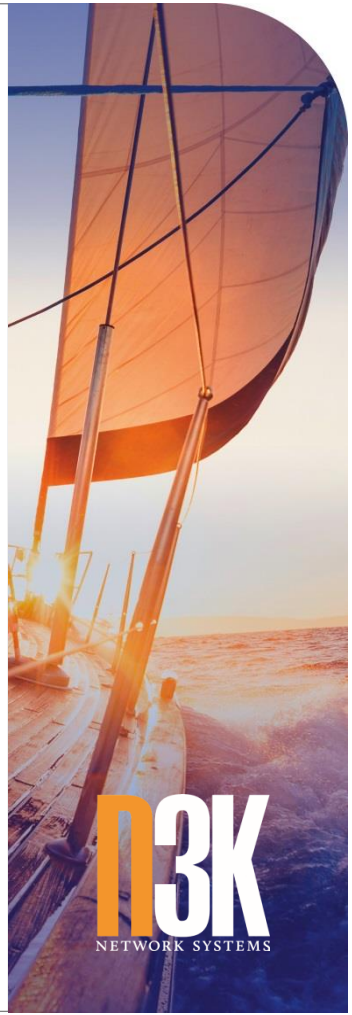
DNS over TLS (DoT)

- Erste Spezifikation im Mai 2016 (RFC 7858)
- Kommunikation über Port 853 mit TLS (und TCP)
- Verschlüsselung mit TLS
  - DNS-Server liefert Zertifikat zur Bestätigung seiner Identität
  - Schlüsselaustausch



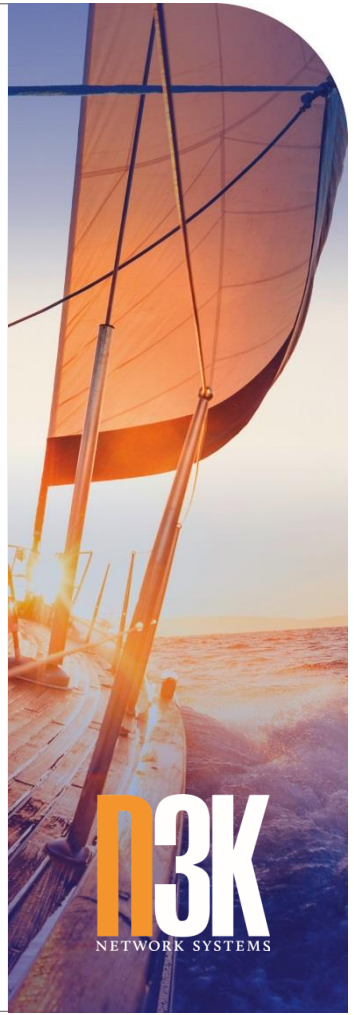
DoT - Ablauf


DNS Client
Client Hello
Server Hello + Certificate + Server Key Exchange
Client Key Exchange + Certificate Verify + Change Cipher Spec
Change Cipher Spec + Finished
DNS over TLS Resolver
DNS Query
DNS Response
TLS Handshake
Encrypted Traffic


n3k
NETWORK SYSTEMS

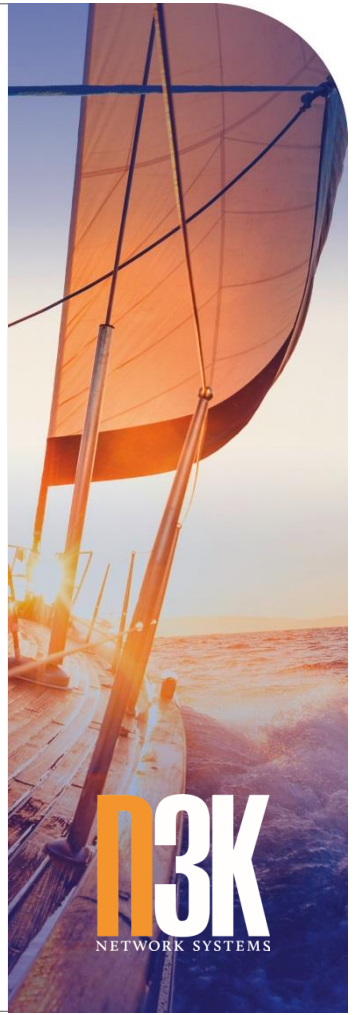
DoT – Nutzungsprofile für Clients

- Opportunistic Privacy
  - Verbindung über DoT falls vom DNS-Server unterstützt, ansonsten unverschlüsselt
  - Client kann optional die Identität des DoT-Servers überprüfen
  - Vertraulichkeit wird bevorzugt
  - Kompatibilität geht über Sicherheit
- Strict Privacy
  - Verbindung muss verschlüsselt sein
  - Identität des DoT-Servers muss bestätigt werden können
  - Vertraulichkeit ist zwingend erforderlich
  - Sicherheit hat Vorrang vor Kompatibilität (potentiell keine DNS-Auflösung)



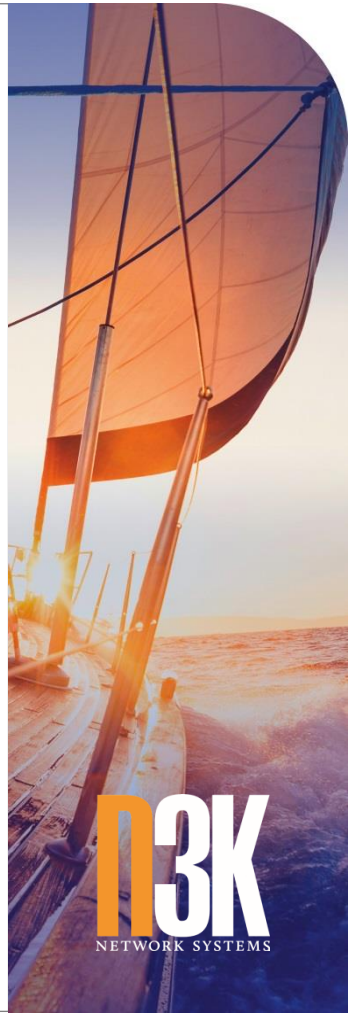
DoT - Anforderungen

- Mehr Rechenleistung durch TLS-Operationen erforderlich (Kryptographische Operationen)
- Mehr Speicherauslastung durch aktive Verbindungen
  - Speicherverbrauch um 3,6 GB höher bei 24.000 aktiven Verbindungen
- Auf Port 853 dürfen keine unverschlüsselten Kommunikationen ablaufen

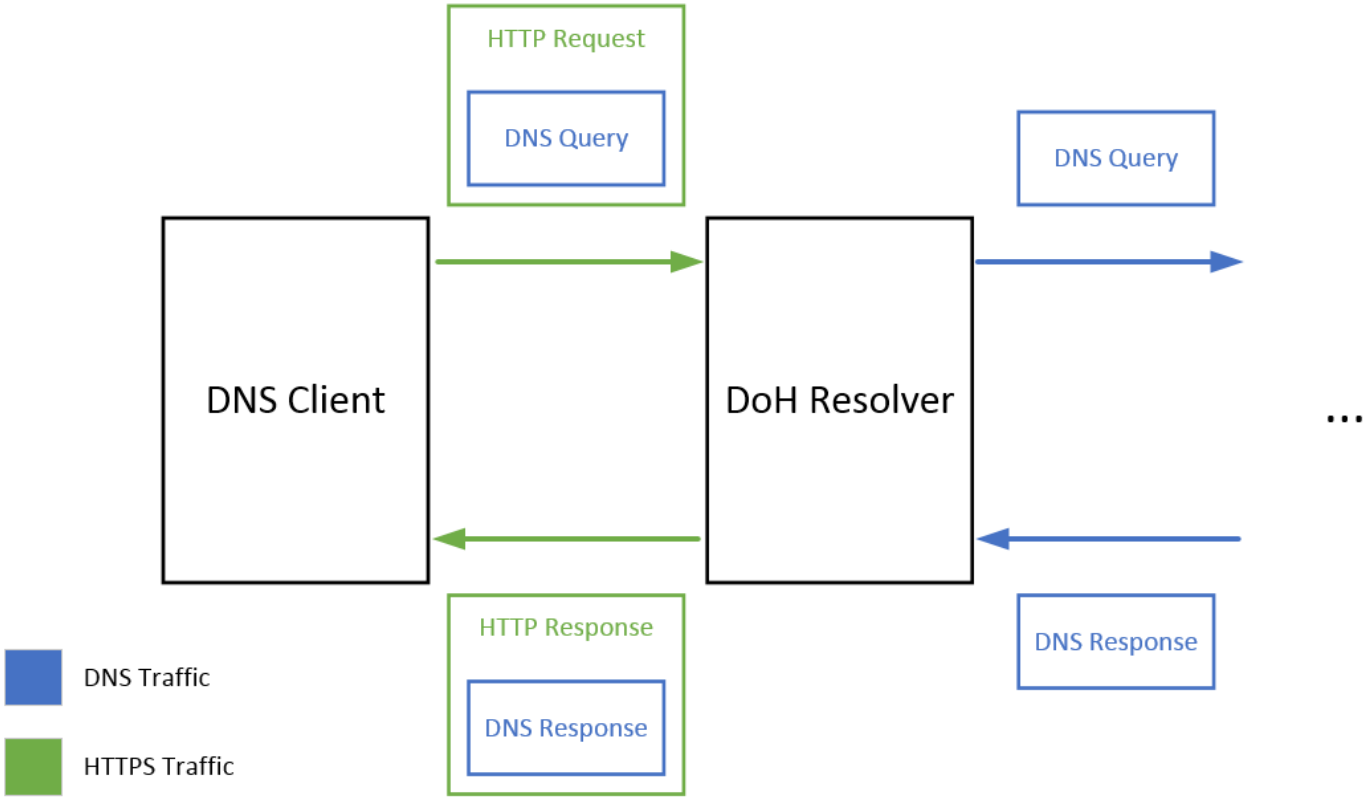


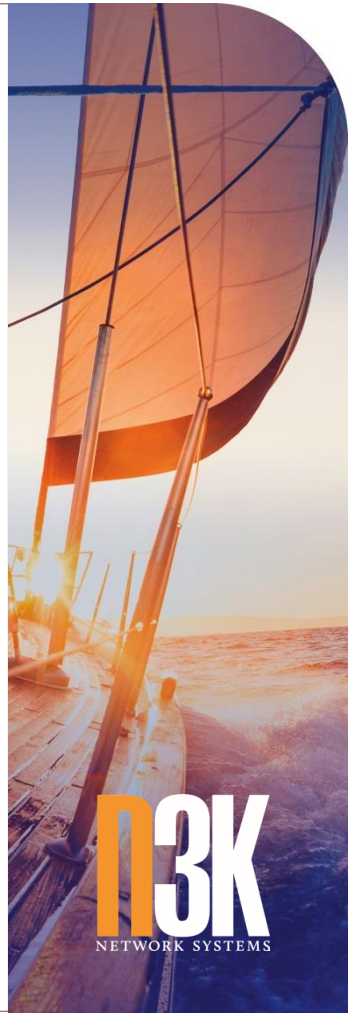
DNS over HTTPS

- Spezifikation im Oktober 2018 (RFC 8484)
- Kommunikation über Port 443 mit HTTPS
  - Keine Unterscheidung zwischen DNS- und HTTPS-Anfragen möglich



DoH - Ablauf

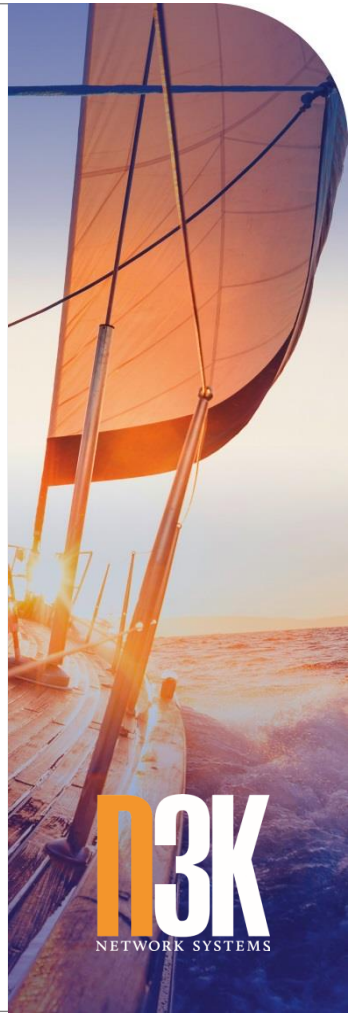

HTTP Request
DNS Query
DNS Query
DNS Client
DoH Resolver
...
HTTP Response
DNS Response
DNS Response
DNS Traffic
HTTPS Traffic


NETWORK SYSTEMS

DoH - Format

- Jede HTTP-Anfrage/Antwort beinhaltet nur ein DNS-Paket
- URI-Template: /dns-query
- HTTP-Methoden: GET, POST
- Bei POST-Anfragen: DNS-Paket wird als POST-Data mitgesendet

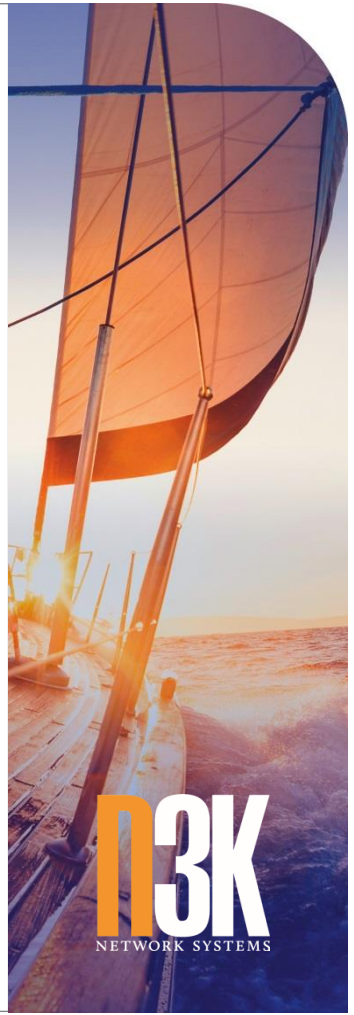
```
POST /dns-query
HTTP/2.0
Host: example.com
Content-Type: application/dns-message
00 00 01 00 00 01 00 00 00 00 00 00 07 65 78
61 6d 70 6c 65 03 63 6f 6d 00 00 01 00 01
```



DoH - Format

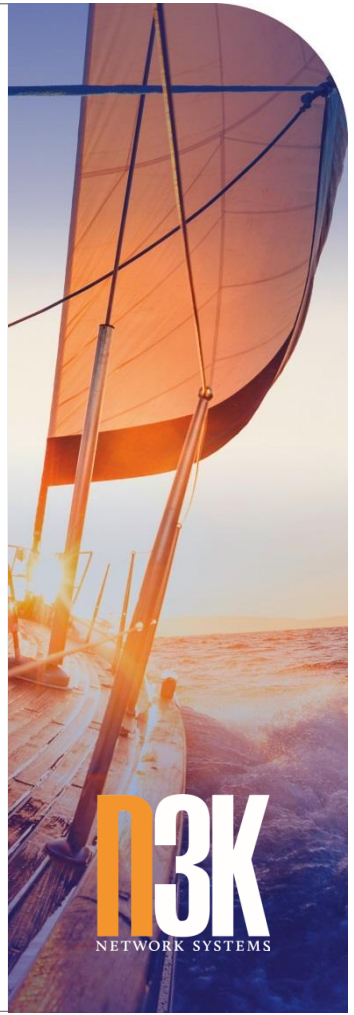
- Bei GET Anfragen: DNS-Paket ist ein GET Parameter (base64url kodiert)

```
https://example.com/dns-query?dns=
AAABAAABAAAAAAAAB2V4YW1wbGUDY29tAAABAAE
```



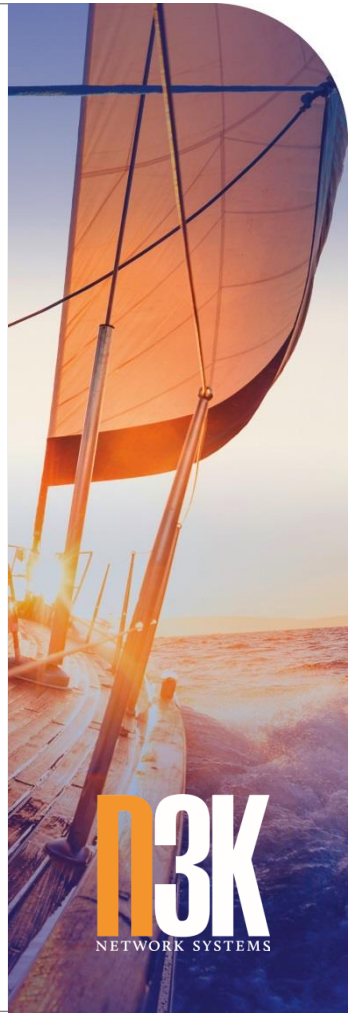
DoH - Anforderungen

- HTTPS verwendet TLS, DoT-Anforderungen treffen daher ebenfalls zu
- GET und POST-Anfragen müssen unterstützt werden
- HTTP/2 wird als Mindestversion empfohlen
- Client muss das URI-Template des DoH-Servers kennen



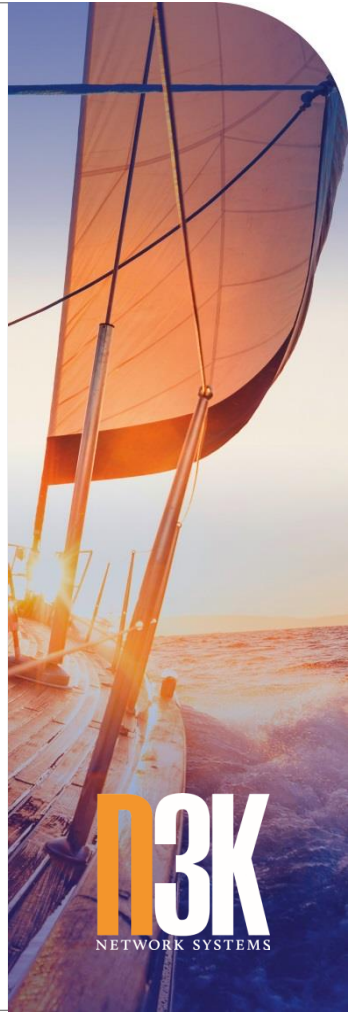
DoT/DoH - Verbreitung

- Nur wenige DNS-Server-Implementationen unterstützen DoT/DoH
- Große Anbieter wie Google, Cloudflare und Quad9 stellen DoT/DoH-Server bereits zur Verfügung
- Firefox unterstützt DNS over HTTPS
- Android 9 unterstützt DNS over TLS auf Betriebssystemebene



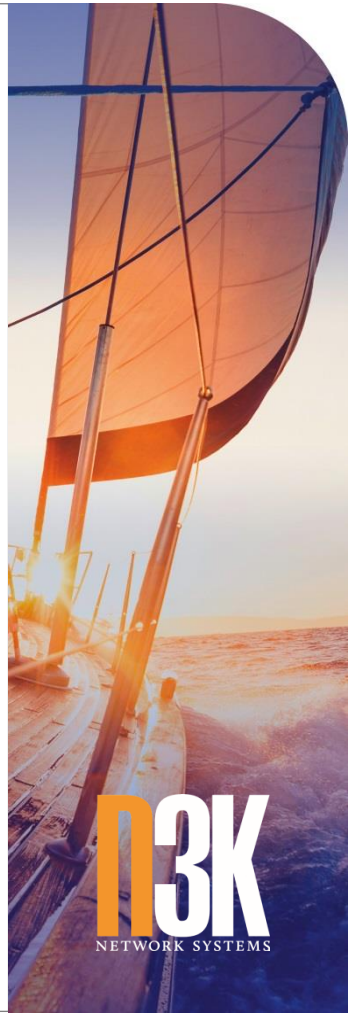
DoT/DoH - Probleme

- Wie können Clients DoT/DoH-Server im Netz finden?
- (Fast) alle Implementierungen sind auf Anwendungsebene
  - Anwendungen bestimmen DNS-Resolver selbst
  - DNS-Server des Betriebssystems wird ignoriert
- Anwendungen sind vom internen DNS abgeschottet
  - Interne DNS-Daten können nach außen geleakt werden
  - Interne DNS-Sicherheitsbeschränkungen werden umgangen
  - Gefahr durch Schadsoftware, die die Firewall durchdringt



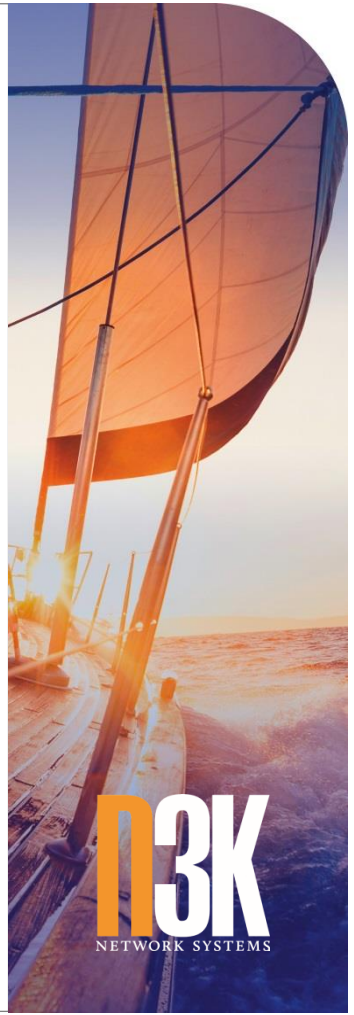
DoT/DoH - Probleme

- Kein Schutz vor extern manipulierten DNS-Daten
  - DNSSEC muss weiterhin eingesetzt werden
- Fehlerbehebung im DNS wird schwieriger
- DoT und DoH sind anfällig für TLS Angriffe und Schwachstellen



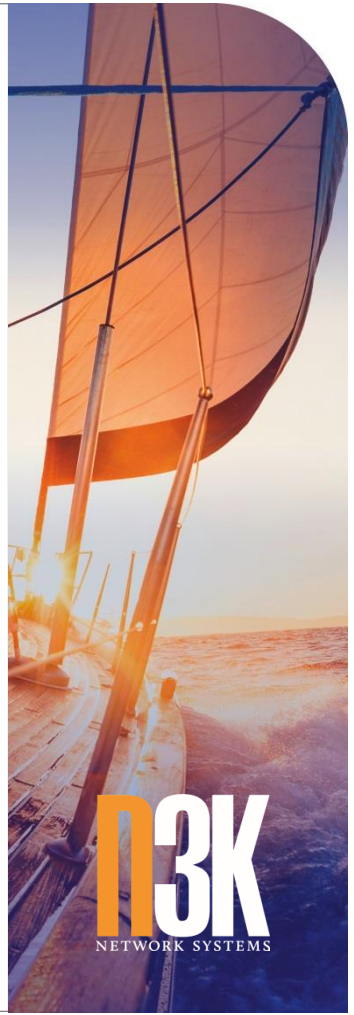
DoH - Diskussionen

- „Britische Lords diskutierten Gefährdung durch DoH“
  - Aushebelung von Kindersicherungen
  - Erschwert oder verhindert die Arbeit von Organisationen wie „Internet Watch Foundation“
- „DNS over HTTPS: Ein Problem gelöst, mehrere neue geschaffen“
  - Aushebelung von Gesetzen zur Inhaltsblockierung
  - Verlagerung des DNS-Verkehrs auf wenige große Plattformen



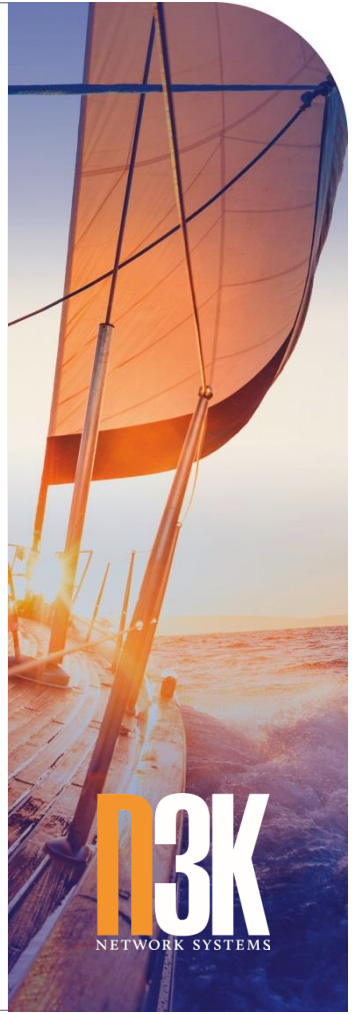
DoH – Problem: Große Provider

- DoH soll für alle Firefox Nutzer standardmäßig aktiviert sein
- Szenario: Google Chrome aktiviert DoH für alle Benutzer
  - Marktanteil von Google Chrome im April 2019: 63,16%
- Deutlich mehr als die Hälfte des DNS-Verkehrs durch Web Browsing landen bei großen Anbietern
- Ausfall eines Providers hat signifikante Auswirkungen



Umgang mit DoT/DoH im Firmennetz

- Externe DoT/DoH-Anbieter blockieren
  - DoT: Port 853 blockieren
  - DoH: Blockieren durch (HTTP-)Proxyserver
- Interne DoT/DoH-Resolver bei Bedarf zur Verfügung stellen



NETZWERKE FÜR DAS 3. JAHRTAUSEND

n3k NETWORK SYSTEMS