

DNS-Performance

Definieren, Analysieren & Optimieren

JÖRG BACKSCHUES – DDI USER GROUP – WIEN 06/2025

Am Anfang..., der Kunde, ...

- „Wir haben Performance-Probleme auf unserem E-Mail Security Gateway.“
- „Unsere Mail-Queue läuft ständig voll.“
- „Wir haben bei uns eine DNS-Security Cloud Lösung eingeführt.“

Was ist DNS-Performance?

- **Focus**
Latenz von DNS-Anfragen gemessen am Client Stub-Resolver
- **„Klassifizierung“ (ISC)**
 - Cache Hits < 1 ms
 - Cache Misses < 100 ms
 - Problematic Cache Misses < 1000 ms

Messung der DNS-Performance

- **Unix-Systeme (Linux, MacOS, ...)**
 - **dig**
DNS53, DNSSEC, Stub-Resolver Cache Bypass
 - **kdig**
DNS53, DNSSEC, Stub-Resolver Cache Bypass, DoT, DoH, DoQ
- **Microsoft Windows**
 - Measure-Command {nslookup} ?
DNS53
 - Measure-Command {Resolve-DnsName} ?
DNS53, DNSSEC, Stub-Resolver Cache Bypass
- **Appliances (Firewall, E-Mail Security, ...)**
 - Debug-Log ?

Unterschiedliche DNS-Performance

- **Cache Misses**

```
dig a ip.backschues.net
ip.backschues.net.      3600 IN A 85.183.142.13
;; Query time: 53 msec
```

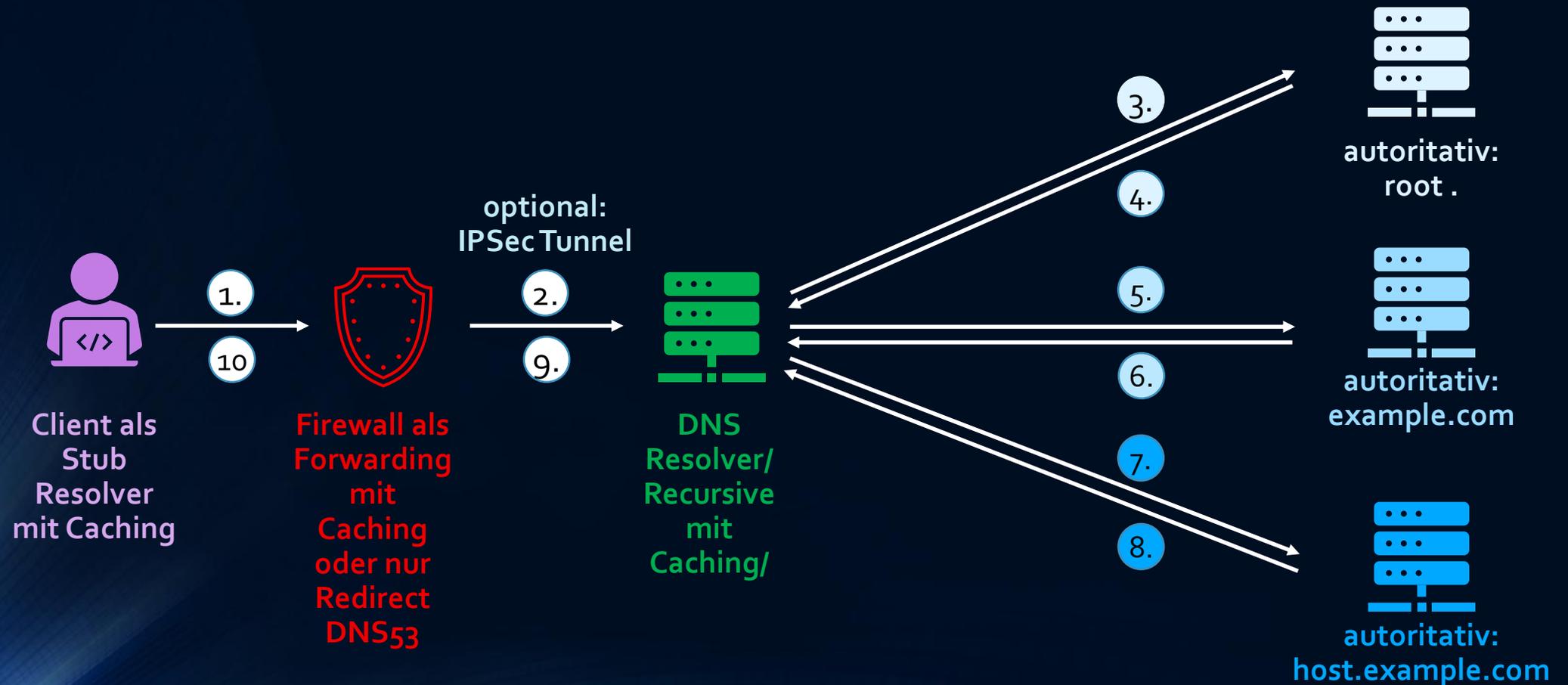
- **Cache Hits**

```
dig a ip.backschues.net
ip.backschues.net.      3599 IN A 85.183.142.13
;; Query time: 0 msec
```

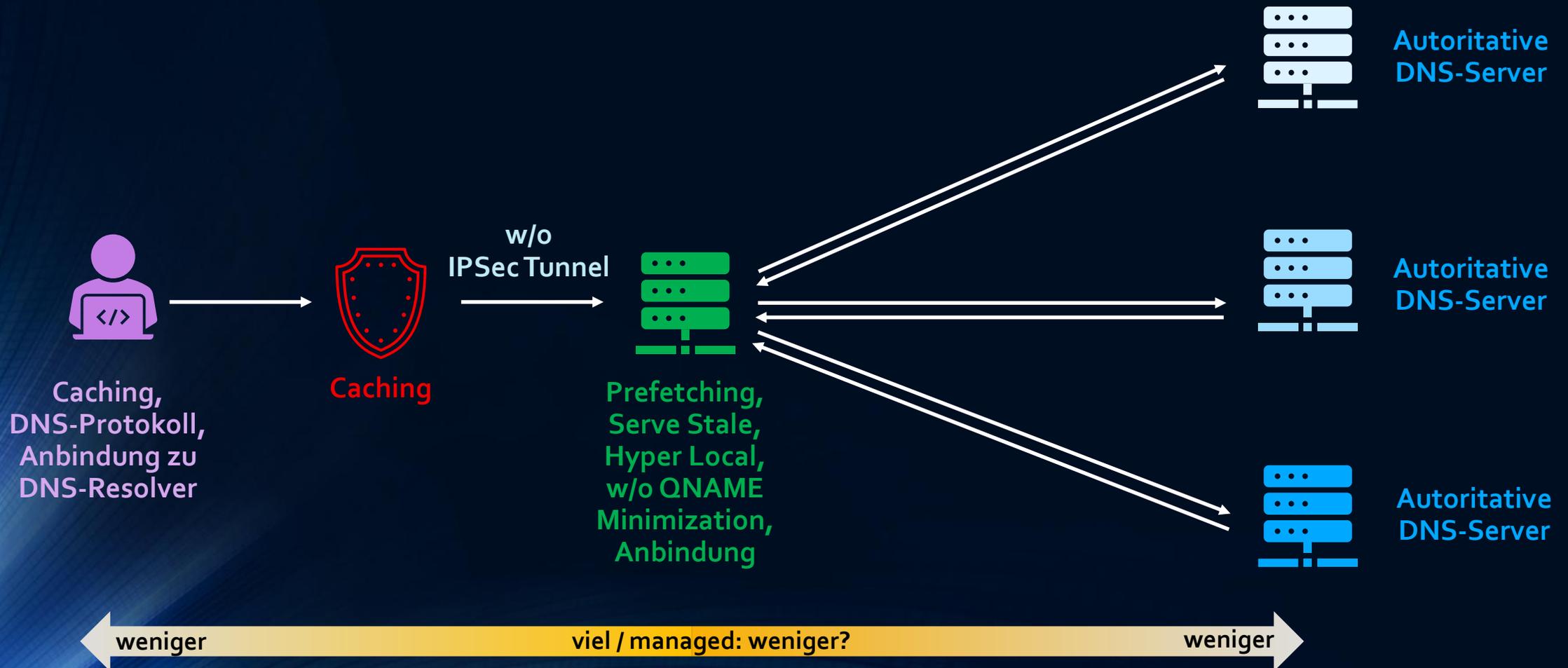
- **Cache Hits mit 12 ms RTT zwischen Client Stub- und DNS-Resolver**

```
dig a ip.backschues.net
ip.backschues.net.      3599 IN A 85.183.142.13
;; Query time: 12 msec
```

Typischer Aufbau des DNS-Resolving



Potential für Performance-Optimierungen



Potential für Performance-Optimierungen

- **Client Stub-Resolver**

- Findet auf dem Stub-Resolver ein lokales Caching statt?
Welches DNS Resolver-Protokoll unterstützt lokales Caching?
- Welches DNS Resolver-Protokoll hat Performance Vor- bzw. Nachteile?
- Anbindung des Client Stub-Resolvers an DNS-Resolver (z.B. Tunnel)

- **Forwarding (auf Firewall o.ä.)**

- Findet auf dem Forwarder ein lokales Caching statt?
- Welches Resolver-Protokoll kommt zum Einsatz (DNS53, DoT, DoH, DoQ, ...)?

Potential für Performance-Optimierungen

- **DNS-Resolver**
 - Prefetching bevor TTL eines Eintrages im Cache abläuft
 - gute Anbindung an autoritative DNS-Server
 - lokale Kopie der root Zone (Hyper Local)
 - Serve Stale im Cache bei Ausfällen
 - QNAME Minimization ja/nein
 - Integration interne Zonen

Analyse der DNS-Performance

- **Werkzeuge**

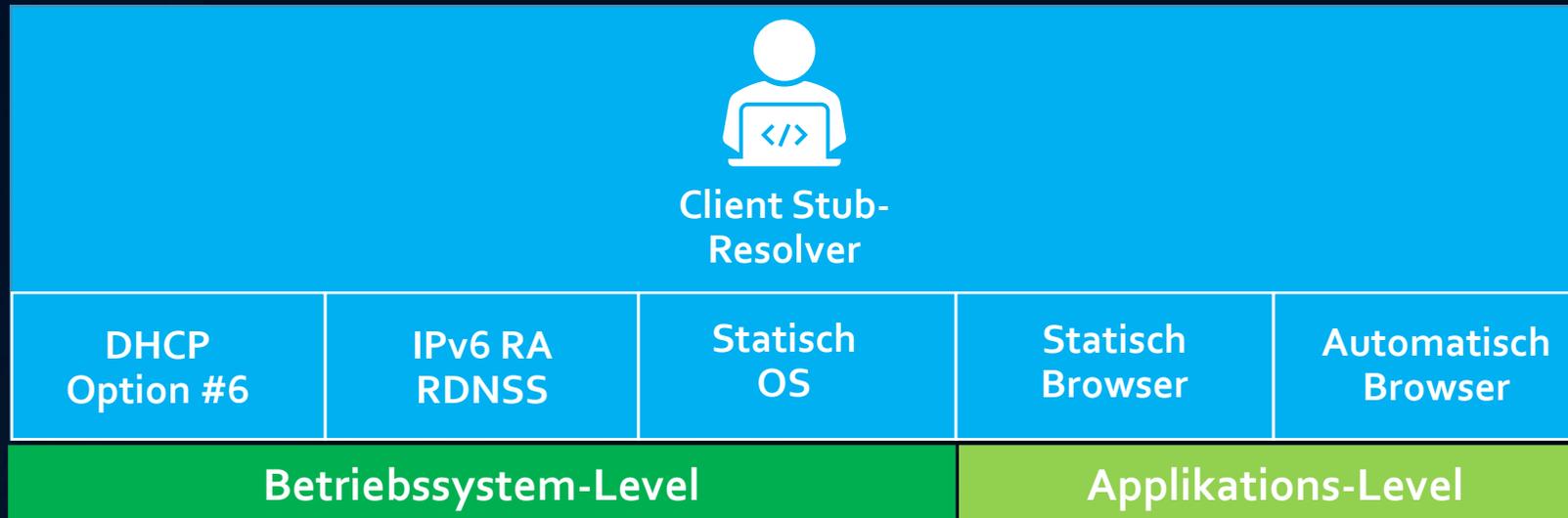
Linux VM / Raspberry Pi 

- bestehendes DNS-Resolving Analyse mit dig / kdig
- Lokaler unbound DNS-Resolver Instanz für DNS53 & DoT
- Lokaler dnsmasq DNS-Resolver Instanz für DoH & DoQ 

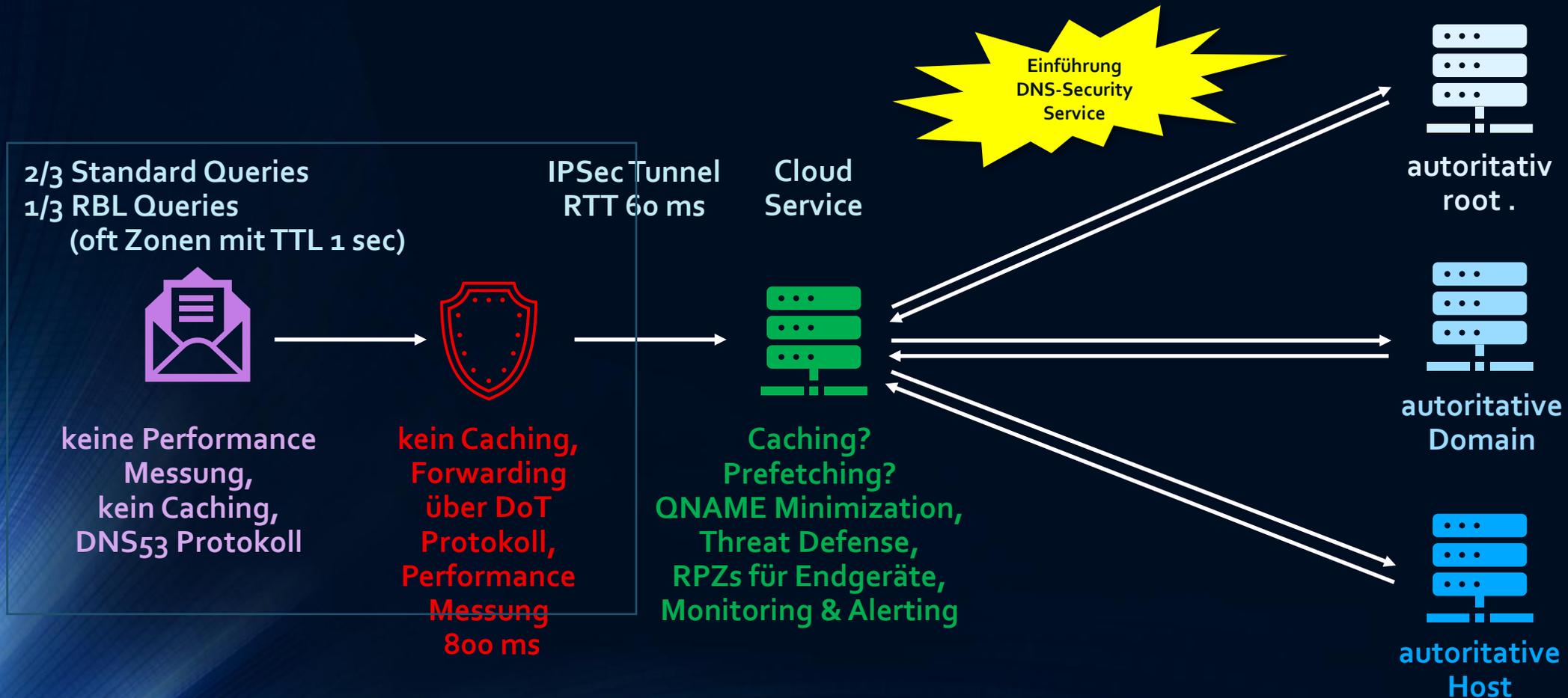
- **Vorgehensweise**

1. Analyse des bestehenden DNS-Resolving mit dig / kdig
2. dediziert DNS Traffic auf Linux VM / Raspberry Pi umleiten
3. DNS Traffic analysieren
 - Welche Protokolle kommen zum Einsatz (DNS53, DoT, DoH, DoQ) ?
 - Welche DNS-Abfragen finden statt? (z.B. A, AAAA, PTR, TXT, DNSSEC, RBLs, ...)

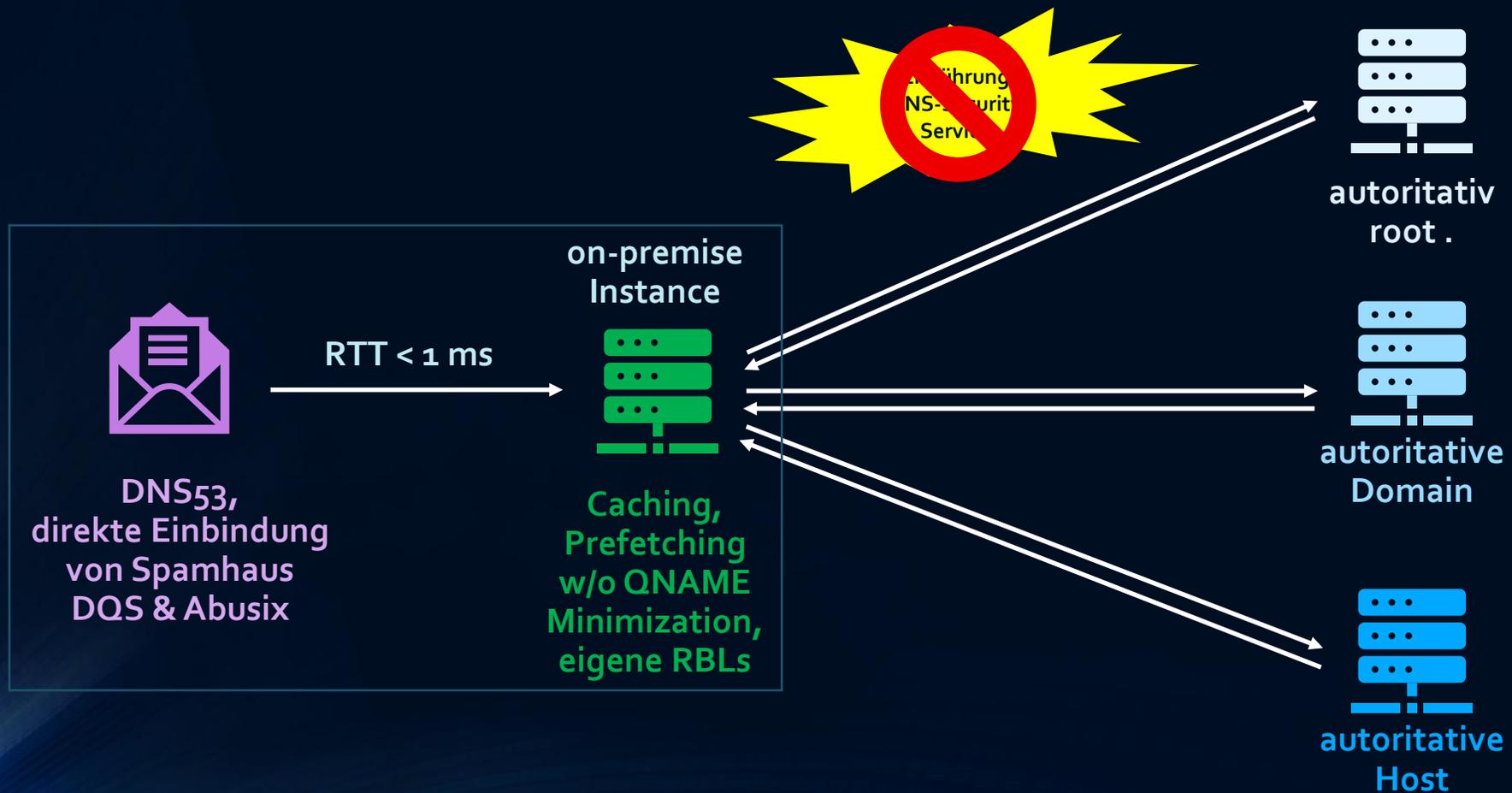
DNS Client Stub-Resolver Protokolle



E-Mail Security Appliance DNS-Anbindung



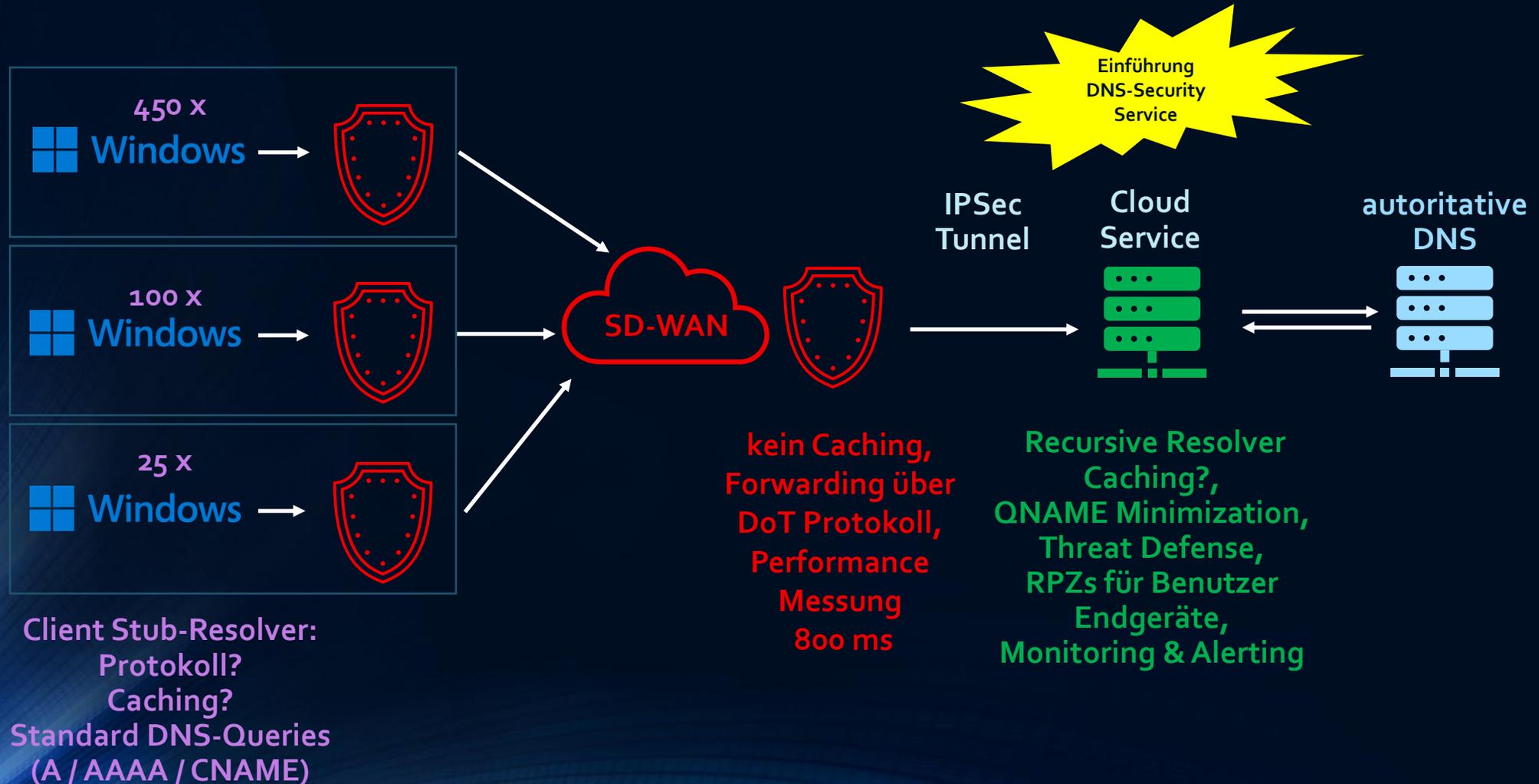
Redesign der DNS-Anbindung der Appliance



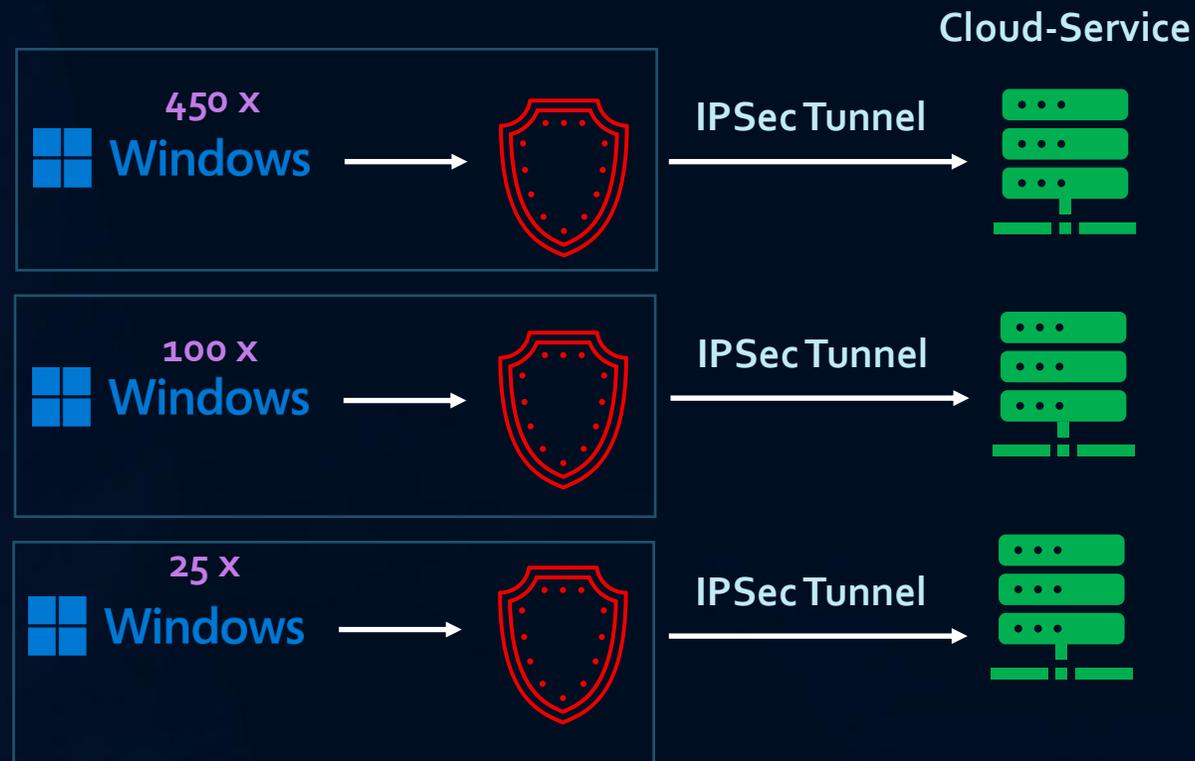
Der Kunde und das nächste Thema ...

- „Der Aufruf von Web-Seiten in unseren Außenstellen ist seit Einführung der DNS-Security Cloud Lösung langsam geworden.“

Benutzer Client DNS-Anbindung



V1 Redesign: Endgeräte DNS-Anbindung

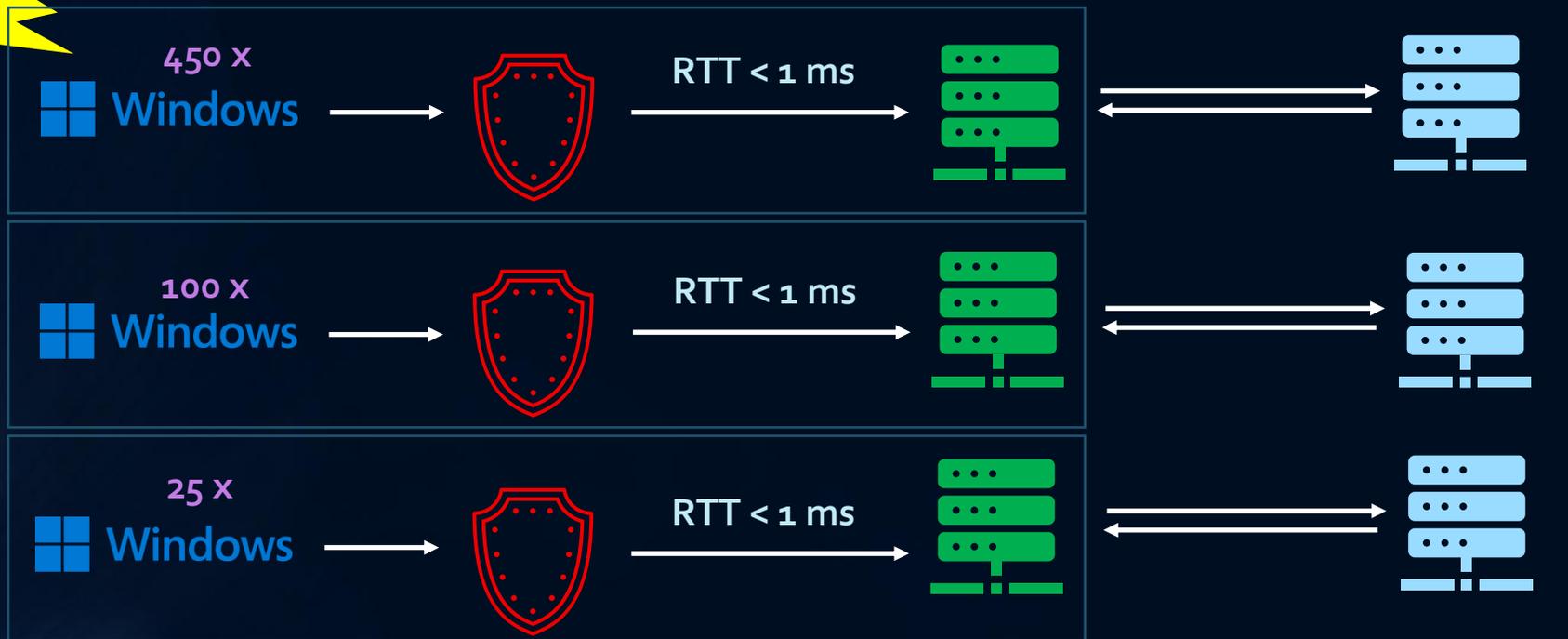


Einführung
DNS-Security
Service

Performance Messung
ca. bei 800 ms

V2 Redesign: Endgeräte DNS-Anbindung

Einführung
DNS-Security
Service on
premise



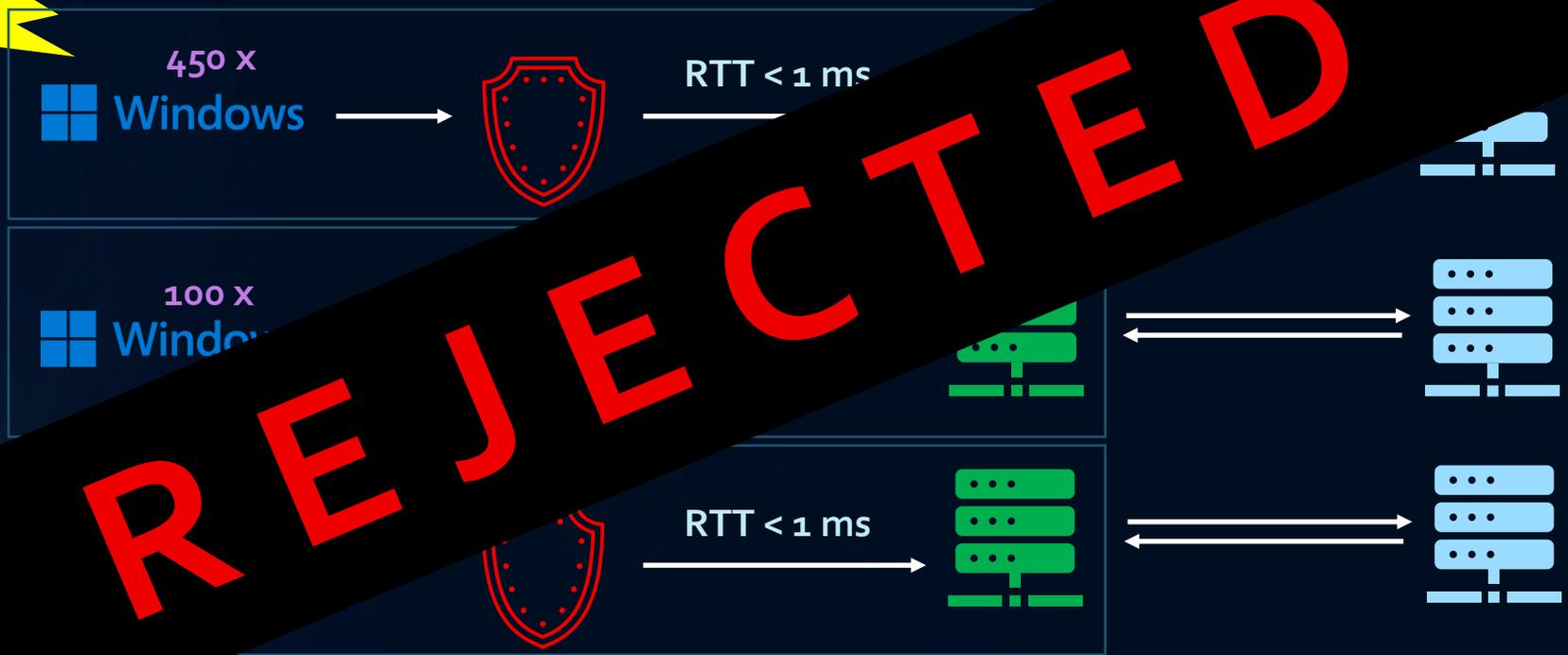
Performance Messung
ca. bei 15 ms

lokaler Resolver
Caching/Recursive

autoritative
DNS

V2 Redesign: Endgeräte DNS-Anbindung

Einführung
DNS-Security
Service on
premise



REJECTED

Performance Messung
ca. bei max. 15 ms
Performance Messung
ca. bei 800 ms

lokaler Resolver
Caching/Recursive

autoritative
DNS

DNS Performance Best Practices

- Optimierung Verbindung (Minimierung RTT) Client Stub-Resolver an Caching/Recursive DNS-Resolver RTT.
- lokalen Breakout zu autoritativen DNS-Servern nutzen.
- Caching, Hyper Local sowie Prefetching aktivieren.
- Verwendung von QNAME Minimization klären.
- Applikations "spezifische" RPZs verwenden.
- Einbinden von lokalen RBLs ermöglichen.

Vorab-Prüfungen

- **Verbindung zwischen Client Stub-Resolver und Caching & Recursive DNS-Resolver überprüfen.**
- **Welcher Host benötigt welche Informationen aus dem DNS?**
- **Welche DNS Stub-Resolver Protokolle kommen zum Einsatz?**

Offen für den Dialog

#ItsAlwaysDNS

JÖRG BACKSCHUES – JB@DNS.EXPERT