Client Authentication Recommendations for Encrypted DNS (CARED)

Jeffrey Damick

Amazon Route 53

Tommy Jensen

Microsoft

Authors:
Tommy Jensen (Microsoft)
Jessica Krynitsky (Microsoft)
Jeffrey Damick (Amazon)
Matt Engskow (Amazon)
Joe Abley (Cloudflare)

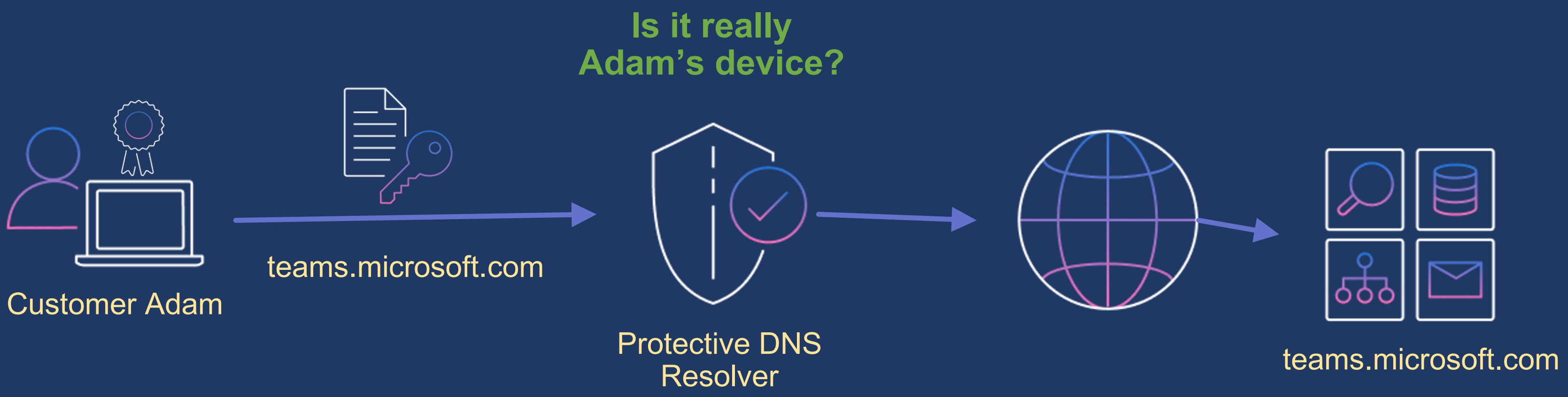
Client Authentication Recommendations

How can DNS clients provide verifiable proof of identity?

How can this identity be tied to machines so recursive resolvers can make resolution decisions based on human-affiliated identities?

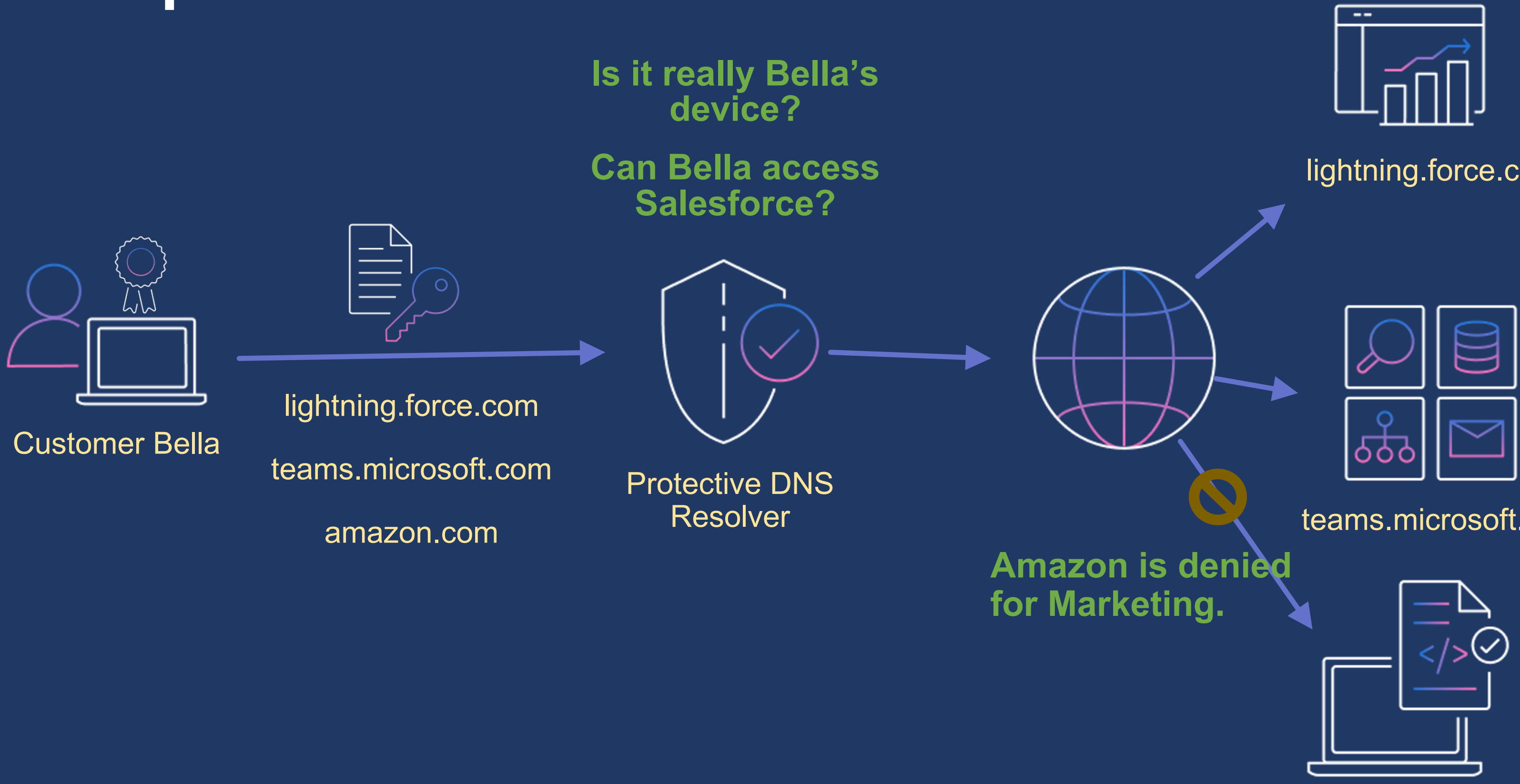
Use Case 1: Managed Access

- Adam has a machine with a certificate associated with him.
- Adam needs to access teams.microsoft.com.
- Protective DNS Resolver will verify the machine's identity and authorize it to receive the Teams DNS records because the machine belongs to Adam.



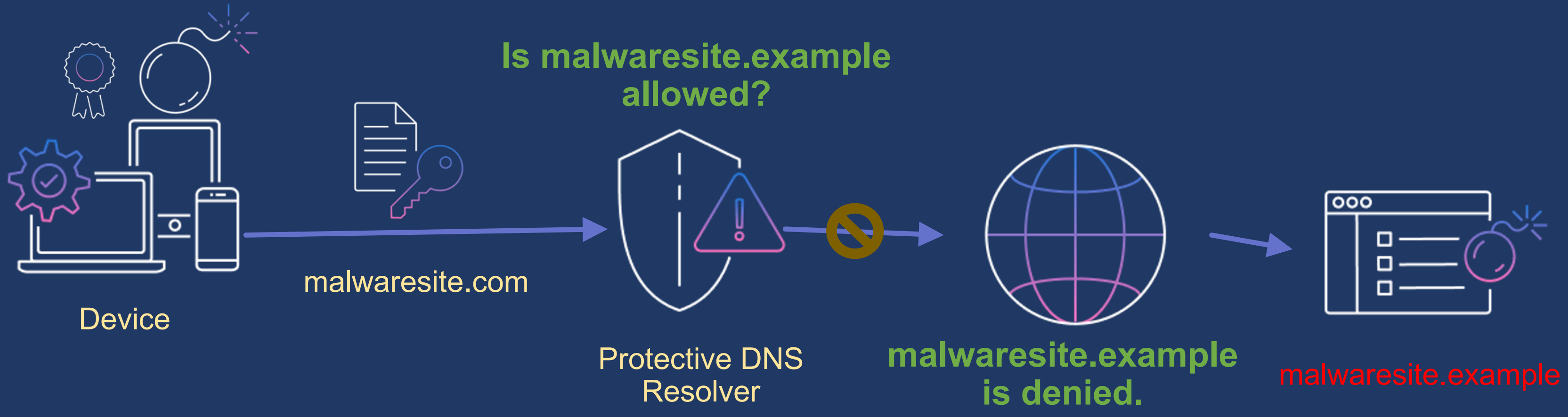
Use Case 2: Group Access Levels

- Bella has a machine with a certificate associated with her.
- Bella is in Marketing and needs to access salesforce.com
- Bella also needs to access teams.microsoft.com.
- Bella attempts to access amazon.com but this is against company policy.
- Protective DNS Resolver will verify the identity and authorize Bella to receive the teams & salesforce DNS records but deny Amazon.



Use Case 3: Device Access

- Device has an issued certificate on the machine.
- Malware on the Device attempts to connect to its Command and Control server at malwaresite.example.
- Protective DNS Resolver will verify the identity and determine malwaresite.example is bad and deny DNS records.



Requirements for Identity Proof

- DNS clients provide securely verifiable identity
- DNS servers & recursive resolvers must be able to provide device specific logs
- Authentication must be applied at the connection-level (avoid per query impact)
- Authentication must support DoH, DoT, and DoQ minimally
- Identity proof must be renewable and revocable
- Authentication must be compatible with the existing DNS protocol

Solution Options

- HTTP Authentication
  - Lacks support for DoT or DoQ
- JSON Web Tokens (JWT)
  - Similar to HTTP Authentication it lacks support for DoT or DoQ
- Microsoft Entra Verified ID and Azure Active Directory
  - Similar to JWT and lacks support for DoT or DoQ
- Create a new solution
  - Significant invest and adoption would be required – worth investigating long-term
- Mutual TLS (mTLS)
  - Meets goals and works across platforms
  - Requires a mechanism to distribute certificates and manage devices

Why create a draft?

Maximize interop between DNS implementations by recommending best practices for authentication.

Codify appropriate use of client auth with encrypted DNS to satisfy user privacy concerns.

https://datatracker.ietf.org/doc/draft-jaked-cared/