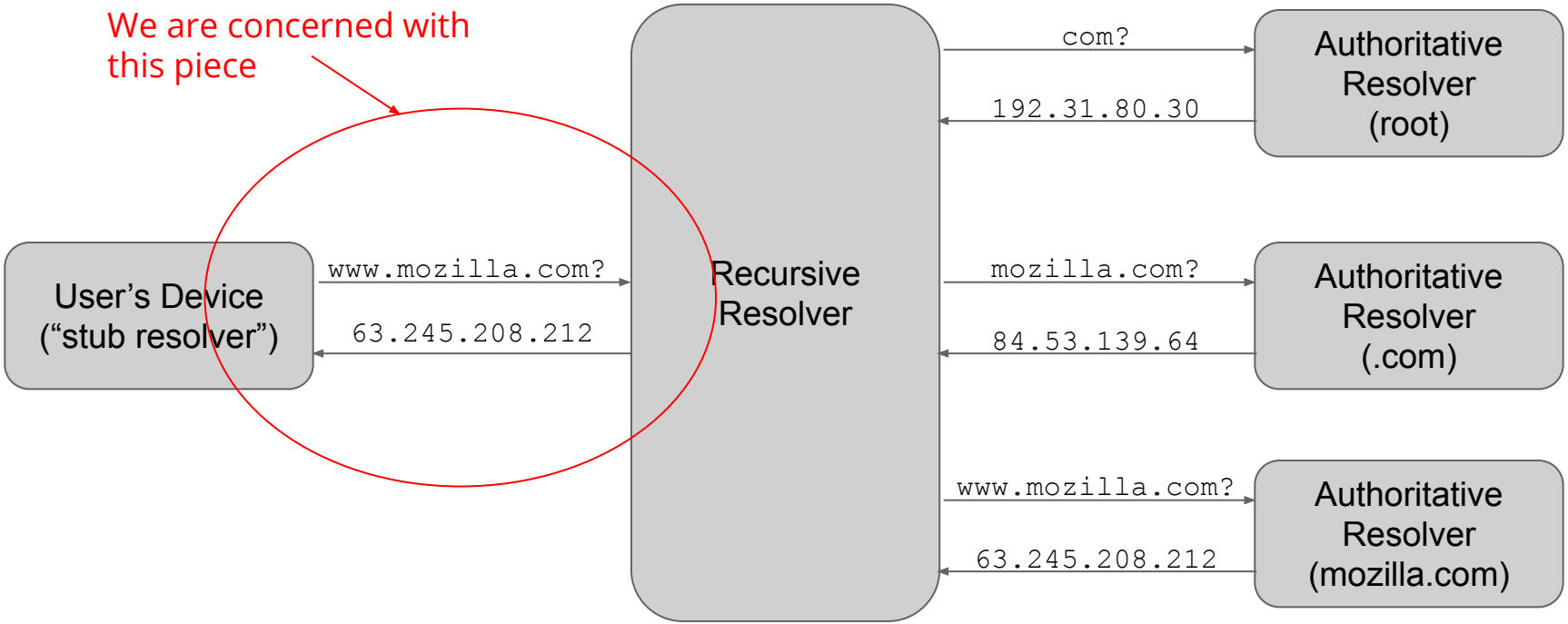
Firefox DoH/TRR Status

Eric Rescorla
CTO, Firefox
February 8, 2020

moz://a

Mozilla Principle #4: Individuals' security and privacy on the internet are fundamental and must not be treated as optional.

What problem are we trying to solve?



This architecture has two security problems

- How do I select a resolver to talk to?
  - ... and how do I know it’s not an attacker?
- How do I securely connect to the selected resolver?
  - Prevent attackers from observing requests and responses
  - Prevent attackers from delivering false responses

Secure resolution requires addressing both of these issues

Where do you get your recursive resolver

- Typically provided by your local network
  - Usually this means your ISP
  - Or your enterprise network
  - ... or the coffee shop/airport network you joined
  - Opaque to the user
  - No real way to know its policies
- Some users choose their own resolvers
  - Google Public DNS, Cloudflare, Quad9, Umbrella
  - These resolvers have varying security and privacy policies

Long History of Attacks on DNS

- **Stub → Recursive:** DNS manipulation is a key part of the Great Firewall / Great Cannon and similar systems in Iran, Syria, and elsewhere
- **At Recursive:** CenturyLink and Comcast have injected ads, and “no record” responses are routinely modified to direct users to ads
- **Recursive → Auth.:** DNS cache poisoning has been used to send Google users to a defaced site and steal ~£300k worth of cryptocurrency
- **At Authoritative:** DNS reflection / amplification are routinely used for DDoS

Attacks on DNS

We are concerned with this piece

- **Stub → Recursive:** DNS manipulation is a key part of the Great Firewall / Great Cannon and similar systems in Iran, Syria, and elsewhere
- **At Recursive:** CenturyLink and Comcast have injected ads, and “no record” responses are routinely modified to direct users to ads
- **Recursive → Auth.:** DNS cache poisoning has been used to send Google users to a defaced site and steal ~£300k worth of cryptocurrency
- **At Authoritative:** DNS reflection / amplification are routinely used for DDoS

“Legitimate Exploits”

- Enterprise firewalls often use DNS data to identify malicious activity
- ISPs and other resolvers use DNS manipulation to deliver services that users have opted into (blocking, tracking, etc.)
- … or which the ISPs impose unilaterally, e.g., based on government requirements

To the client these are technically indistinguishable from an attacker on the network

Our Approach

- Trusted Recursive Resolvers (TRR)
  - Selects a resolver that Mozilla has vetted
  - Security and privacy policies guaranteed by contract
- DNS over HTTPS (DoH)
  - IETF Proposed Standard (RFC 8484)
  - Secures data between you and the recursive resolver
  - Protects you against attackers on your network
  - Guarantees that you are talking to a TRR

Why not DNS over TLS?

- IETF has standardized two DNS channel security protocols
  - DNS over TLS (RFC 7858) and DNS over HTTPS (RFC 8484)
  - Either would have worked
  - We chose DNS over HTTPS
- Why?
  - Firefox has a very mature HTTP stack and lots of HTTP expertise
  - Some potential technical benefits (HTTP multiplexing, push, easy transition to QUIC)
- Isn’t DoT easier to block?
  - Yes, but we don’t consider this an advantage

What about DNSSEC?

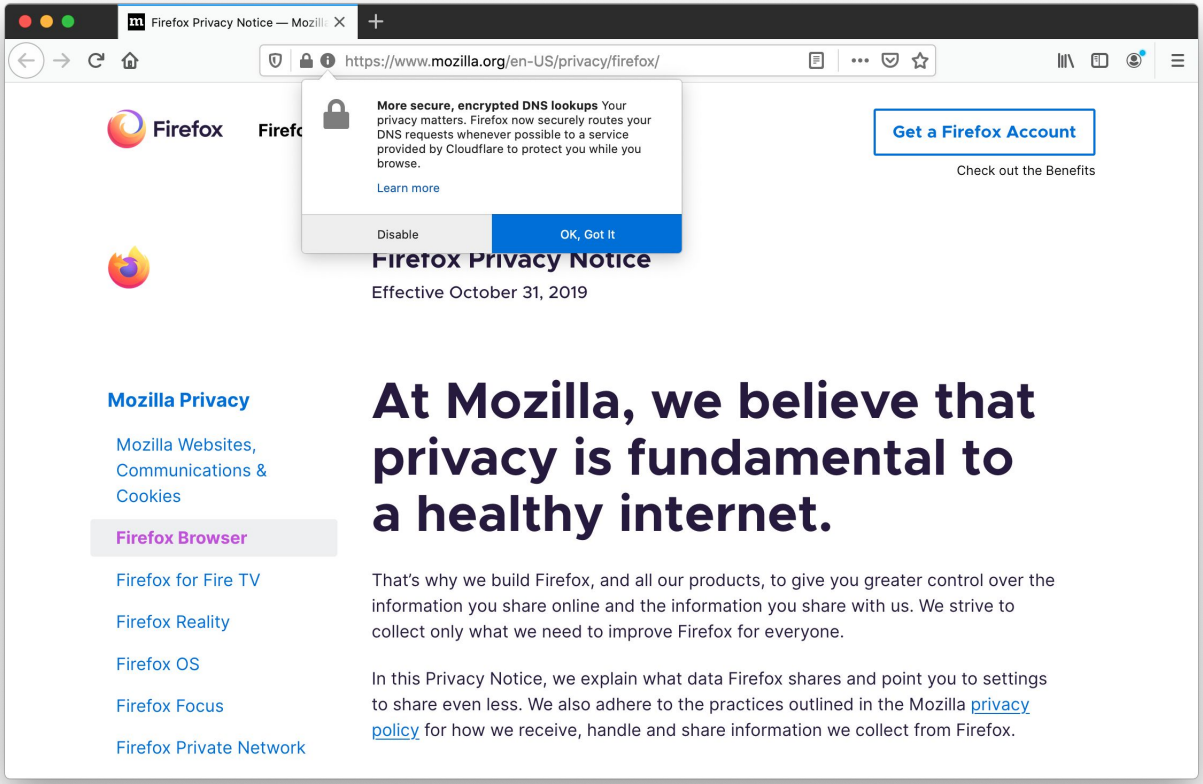
- These are complementary technologies
- DNSSEC solves a different problem
  - End-to-end integrity for the DNS
  - Doesn’t provide confidentiality at all
- DoH is an enabling technology for end-to-end DNSSEC
  - Guarantees a clean path between the stub and the recursive
  - Avoids false positive DNSSEC failures from bad middleboxes[1]

1. The latest data here is quite old. New measurements wanted.

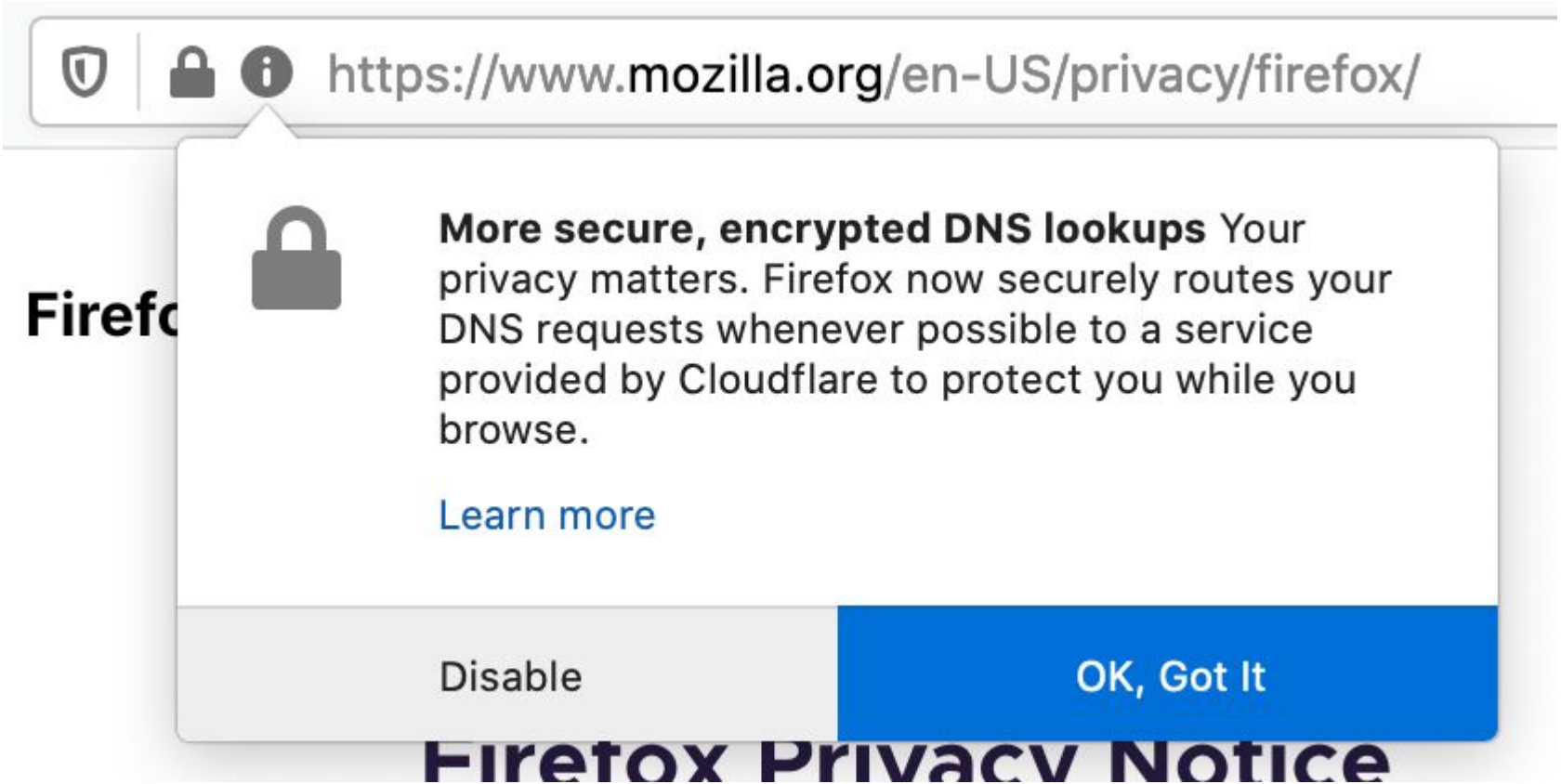
Our strategic approach to rolling out DoH

- Roll out DoH enabled by default
- Allow users to disable DoH or select their own resolver
- Honor enterprise configurations
- Honor opt-in DNS filtering and work with ISPs to support better detection of opt-in filtering
- Create and publish policies that improve privacy and security of the Internet

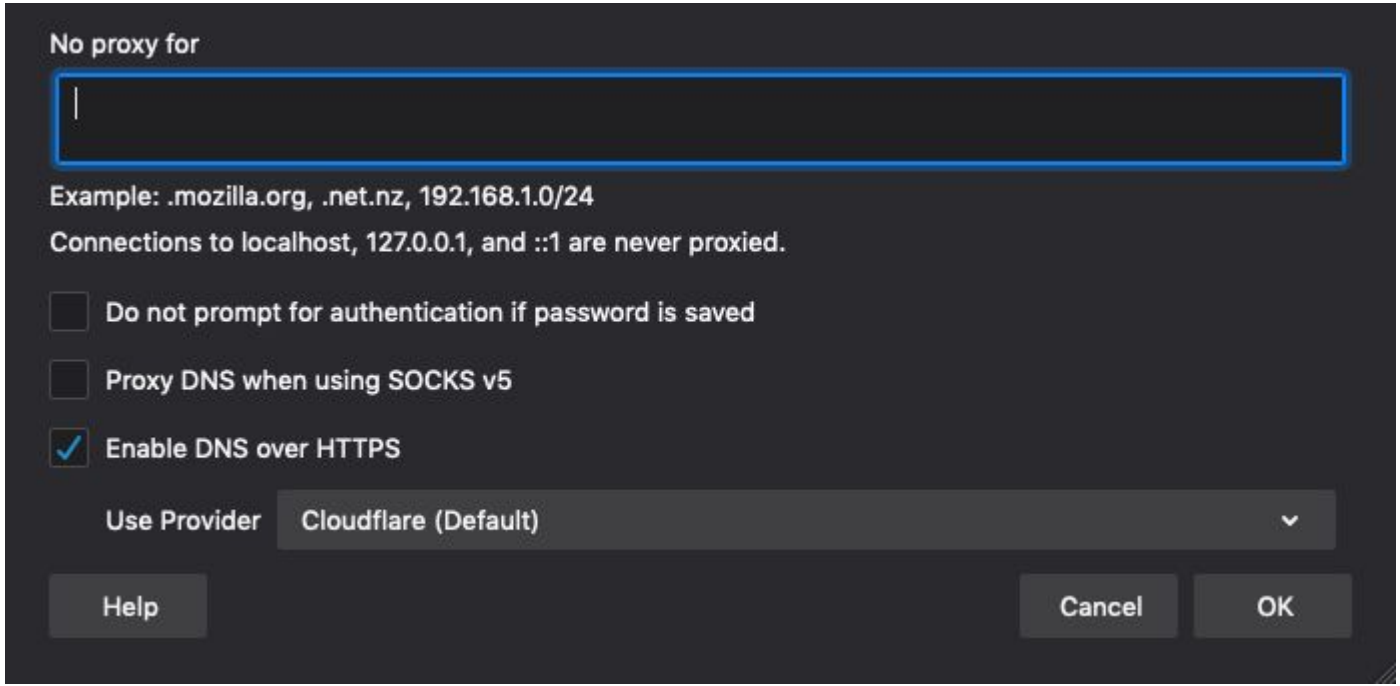
User prompt


Firefox Privacy Notice — Mozill
https://www.mozilla.org/en-US/privacy/firefox/
More secure, encrypted DNS lookups Your privacy matters. Firefox now securely routes your DNS requests whenever possible to a service provided by Cloudflare to protect you while you browse.
Learn more
Disable
OK, Got It
Firefox
Get a Firefox Account
Check out the Benefits
Firefox Privacy Notice
Effective October 31, 2019
Mozilla Privacy
Mozilla Websites, Communications & Cookies
Firefox Browser
Firefox for Fire TV
Firefox Reality
Firefox OS
Firefox Focus
Firefox Private Network
At Mozilla, we believe that privacy is fundamental to a healthy internet.
That's why we build Firefox, and all our products, to give you greater control over the information you share online and the information you share with us. We strive to collect only what we need to improve Firefox for everyone.
In this Privacy Notice, we explain what data Firefox shares and point you to settings to share even less. We also adhere to the practices outlined in the Mozilla privacy policy for how we receive, handle and share information we collect from Firefox.

User prompt


https://www.mozilla.org/en-US/privacy/firefox/
More secure, encrypted DNS lookups Your privacy matters. Firefox now securely routes your DNS requests whenever possible to a service provided by Cloudflare to protect you while you browse.
Learn more
Disable
OK, Got It
Firefox Privacy Notice

Changeable in network preferences



Enterprise support

We plan to disable DoH if we detect an enterprise configuration and DoH was not explicitly enabled.

- Enterprise policy configuration is used by corporations, schools, governments, any centralized software deployment use case.
  - A new trust anchor, Firefox enterprise config, etc.
- Recommendation to network administrators is to explicitly configure a policy for DoH.
- Fall back to system DNS on failure handles some split horizon cases

Detecting opt-in DNS filtering

Heuristics for detecting that a user has opted into parental controls or some other kind of filtering include:

- OS-level parental controls have been enabled.
- Use of “safe search” URLs on major search engines (indicates parental controls were turned on for search).
- ISP-provided canary domains (unique to each major ISP) which resolve properly.

Canary domain proposal

In addition, we have established our own canary domain to identify parental controls and that parental control providers can use.

- Assumption is that parental controls are opt-in.
- Widespread adoption of the canary domain in opt-out scenarios will make this useless.
- Initial talks with parental control software providers indicates this is a good initial deployment strategy.

Respecting user choice

Our strategy for deployment in the US results in:

- More secure DNS overall
- Respecting enterprise configurations
- Respecting opt-in parental controls

We’re also exploring non-default DoH providers that might include additional filtering.

DOH Resolver Policy Specifics

Privacy Requirements

The resolver may retain user data but should do so only for the purpose of operating the service and must not retain that data for longer than 24 hours.

Transparency Requirements

Privacy Notice. There must be a public privacy notice specifically for the resolver service that documents the specific fields for data that will be retained for 24 hours ...

Transparency Report. There must be a transparency report published at least yearly that documents the policy for how the party operating the resolver will handle law enforcement that documents the types and number of requests received and answered.

For the full policy see https://wiki.mozilla.org/Security/DOH-resolver-policy

DOH Resolver Policy Cont.

Blocking & Modification Prohibitions

1. The party operating the resolver should not by default block or filter domains unless specifically required by law in the jurisdiction in which the resolver operates. Mozilla will generally seek to work with DNS resolvers that provide unfiltered DNS responses…

- Resolvers may block or filter content with the user's explicit consent.

2. For any filtering that does occur under the above requirement, the party must maintain public documentation of all domains that are blocked and a log of when particular domains are added and removed from any blocklist.

Intent of #2 is to ensure for accountability & oversight that often does not exist today.

DOH Resolver Policy Cont.

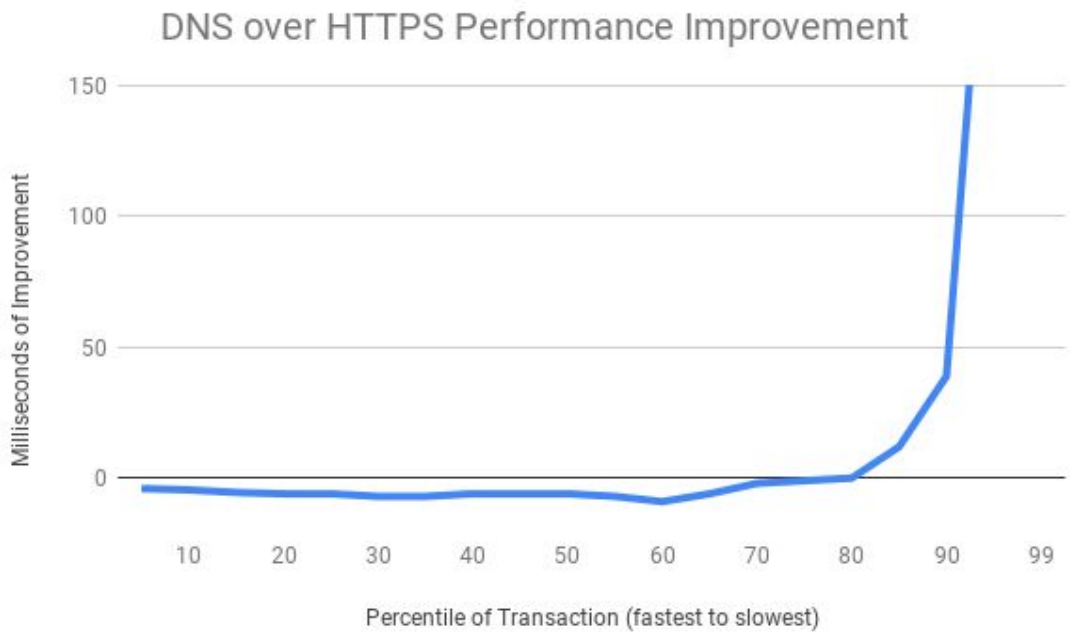
We plan to put our policies for public comment early this year:

> “The goal of this policy process will be to determine if and how our policies can be changed to make them more applicable globally, without substantively weakening the protections they offer to our users.”
>
> - *Mozilla commitment to DCMS, letter sent September 2019*.

Rollout Experiments

- This is a big change and we’re proceeding cautiously
- Ran a series of experiments over the past year+
- Resolver performance
- Page load performance
- Impact of EDNS-Client-Subnet
- Prevalence of parental controls and split horizon
- All signs point to yes

DoH shows comparable performance to Do53



Current Status

- Rollout only in the US
- Two TRRs: Cloudflare and NextDNS
  - Cloudflare is the default
- Currently at ~1% deployment
  - Technically an A/B test on 2% of the population
  - Measuring opt-out, error, and retention rates
- Planned progressive rollout in February
  - Nightly/Beta 2/11
  - Release 5% rollout 2/18
    - Will gradually dial up

Questions