

Encrypted SNI

<https://tools.ietf.org/html/draft-rescorla-tls-esni-00>

Problem: How to protect TLS SNI from passive eavesdroppers?

Approach: Encrypt SNI “using keys” privately fetched from DNS

Team

- Fastly
- Cloudflare
- Mozilla
- Apple

Implementations

- picotls (client and server)
- NSS (client and server)
- BoringSSL (client)

Results

- Two servers:
 - esni.example.net
 - cloudflare-esni.com
- Firefox integration complete, Safari experiment in progress

