

Включение ESNI и DNS over HTTPS в Firefox

Включения **network.security.esni.enabled=true** в about:config **недостаточно** для активации в Firefox TLS-расширения ESNI (Encrypted Server Name Indication), обеспечивающего шифрование данных о хосте, запрашиваемом в рамках HTTPS-соединения.

На данный момент ESNI не работает без использования встроенного в Firefox резолвера "DNS over HTTPS" (network.trr.mode = 2). Использовать ESNI пока можно только при активации "DNS over HTTPS".

Для включения "DNS over HTTPS" в about:config следует **изменить** значение переменной **network.trr.mode**. Значение 0 полностью отключает DoH;
1 - используется DNS или DoH, в зависимости от того, что быстрее;
2 - используется DoH по умолчанию, а DNS как запасной вариант;
3 - используется только DoH;
4 - режим зеркалирования при котором DoH и DNS задействованы параллельно.

По умолчанию используется **DNS-сервер CloudFlare**, но его можно изменить через параметр **network.trr.uri**, например, можно **установить**:

- * <https://dns.google.com/experimental>
- * <https://cloudflare-dns.com/dns-query>
- * <https://dns.quad9.net/dns-query> (он же <https://9.9.9.9/dns-query>)
- * <https://doh.powerdns.org>
- * <https://doh.cleanbrowsing.org/doh/family-filter/> (с родительским контролем)
- * <https://doh2.dnswarden.com> (с родительским контролем)
- * <https://dns.dnsoverhttps.net/dns-query> (проброс запросов через tor)
- * <https://doh.securedns.eu/dns-query> (заявлено об отсутствии ведения логов)
- * <https://doh.crypto.sx/dns-query> (на базе doh-proxy)
- * <https://doh-de.blahdns.com/dns-query> (используется реализация на Go)
- * <https://dns.dns-over-https.com/dns-query> (используется реализация на Go)
- * <https://commons.host> (реализация на Node.js)