

목차

Firefox ESNI 적용하기(warning차단우회)

3

준비

3

파이어폭스에서 ESNI 를 사용하도록 설정하기

3

참조링크

7

Firefox ESNI 적용하기(warning차단우회)

출처: <http://jaewook.net/archives/9176>

본 내용은 파이어폭스 v85 이후 버전에서는 작동하지 않습니다. v85 이후버전은 [Firefox ECH 적용하기\(warning차단우회\)](#) 문서를 참고하시기 바랍니다. 단, 아직까진 ECH를 지원하는 사이트가 많지 않기때문에 아래 Firefox ESR버전을 설치하여 ESNI를 사용하시기 바랍니다.

ESNI가 지원되는 v85 이전버전을 사용하시려면 <https://www.mozilla.org/ko/firefox/all/#product-desktop-esr> 에서 ESR 버전을 다운받아 사용하시면 됩니다.

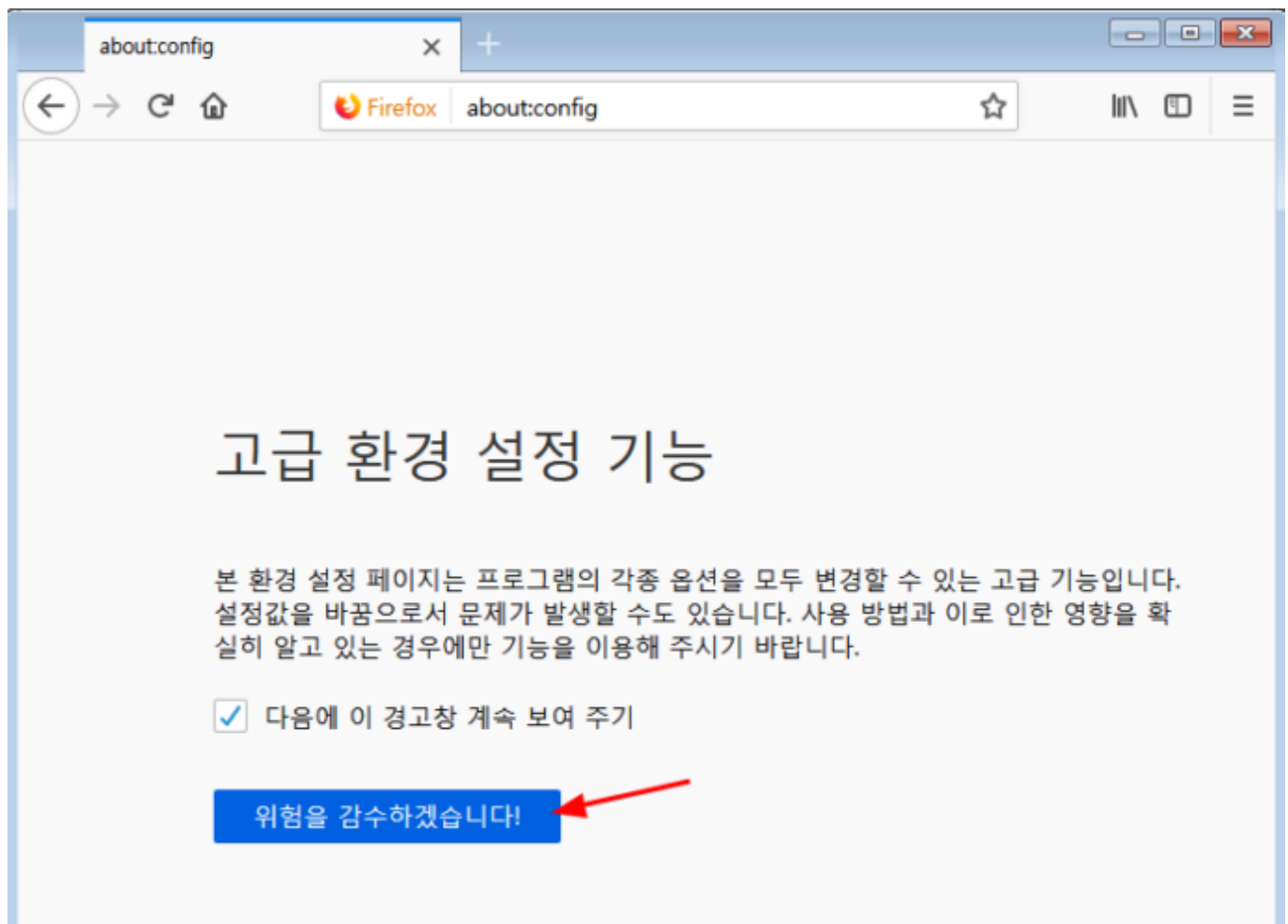
준비

아래 사이트에서 먼저 Firefox 최신버전을 다운로드하여 설치해주세요 ESNI통신을 지원하는 Firefox버전은 64.0.0 부터입니다.

○ 설치버전: <https://www.mozilla.org/ko/firefox/new/>

파이어폭스에서 ESNI를 사용하도록 설정하기

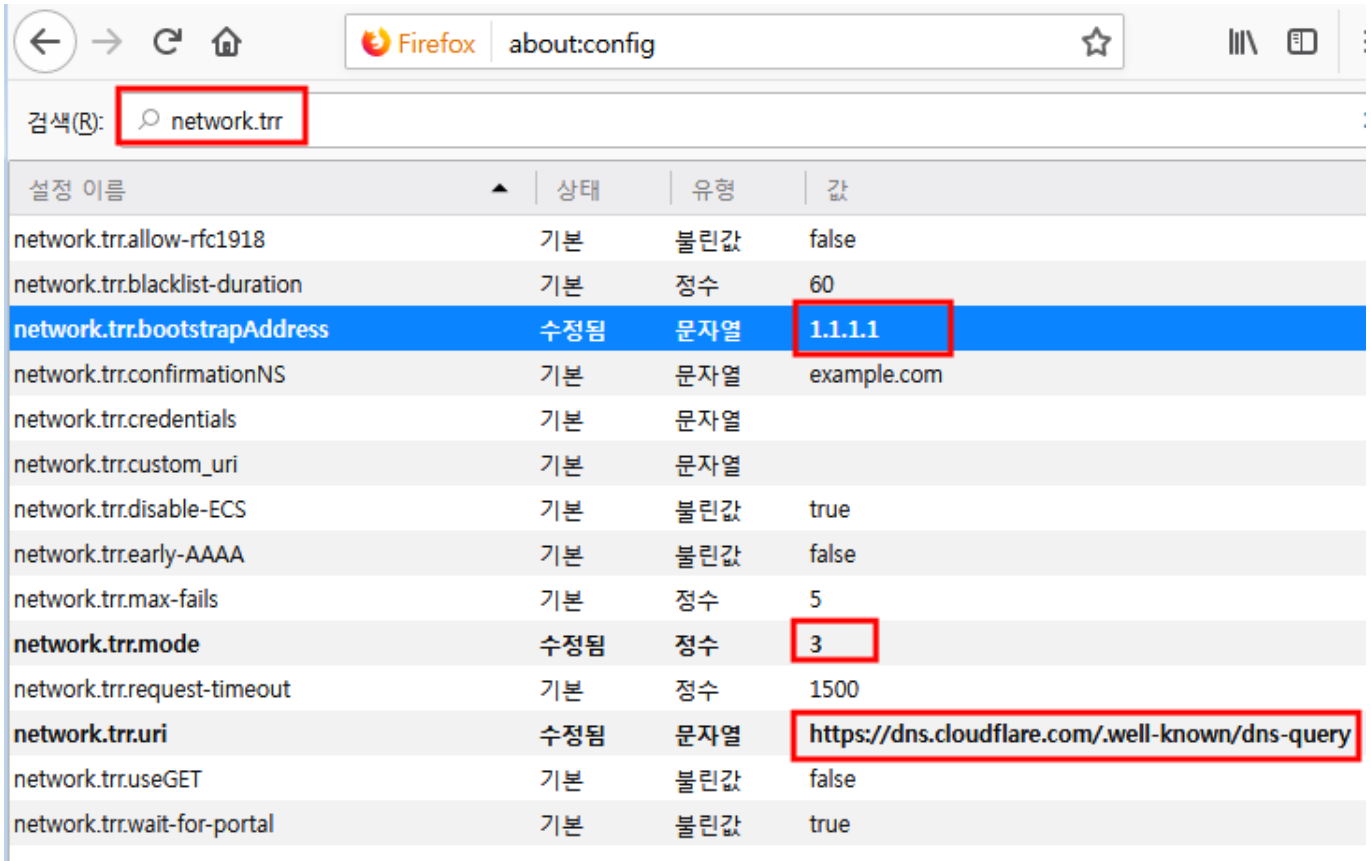
- 파이어폭스 주소창에 `about:config`를 입력하여 고급환경설정 메뉴로 이동합니다.
- 고급환경설정 기능 창이 뜨는데..[위험을 감수하겠습니다]라는 버튼을 클릭해주세요



- 먼저 암호화된 DNS통신을 사용하도록 설정해주세요 (Dns over https 관련 설정)

검색창에서 `network.trr` 이라고 입력해서 나오는 항목중 아래의 세가지를 수정해줍니다. ※ 요즘 `network.trr.uri` 항목의 경우 Firefox기본값이 바뀌어서 수정하지 않아도 되는 것 같습니다.

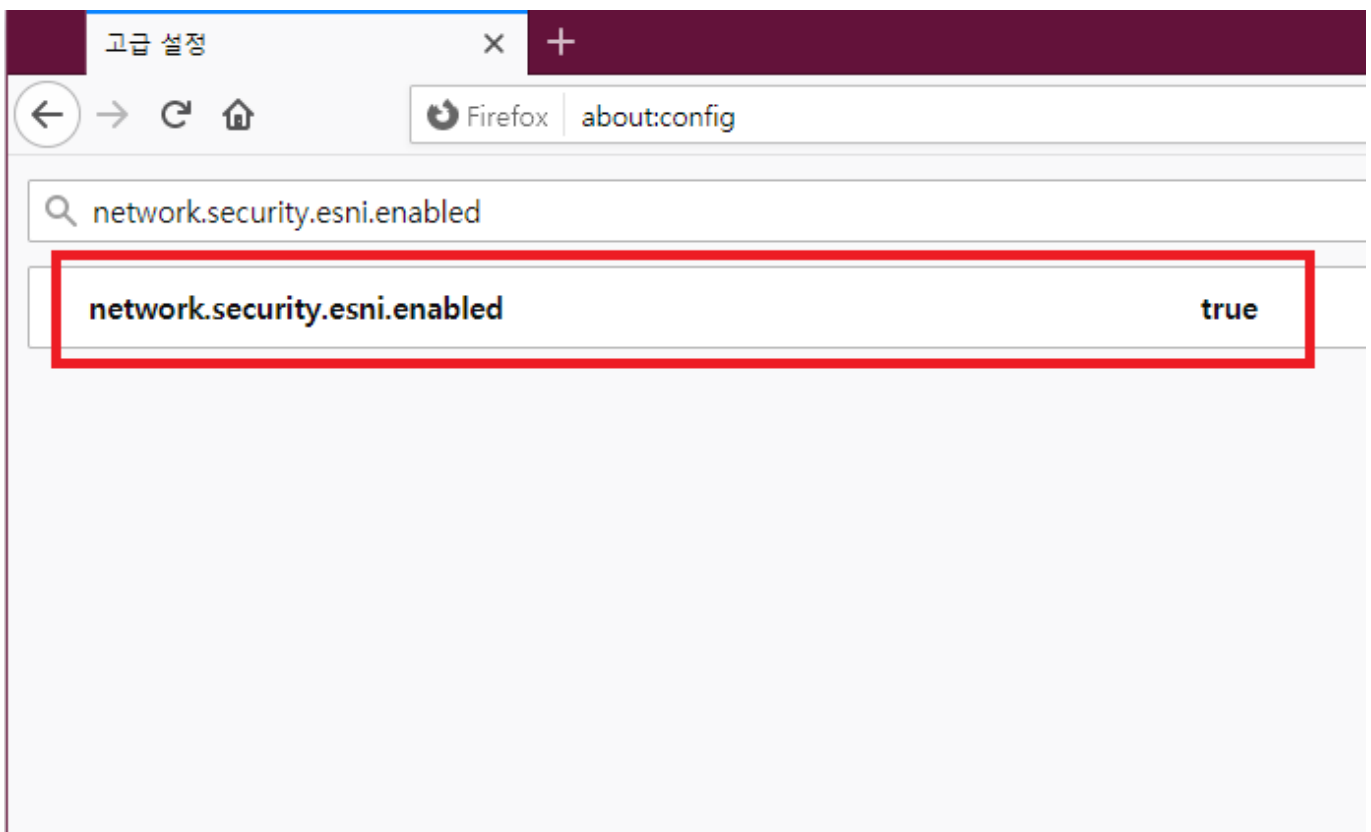
```
network.trr.bootstrapAddress 1.1.1.1
network.trr.mode 3
network.trr.uri https://dns.cloudflare.com/.well-known/dns-query
```



설정 이름	상태	유형	값
network.trr.allow-rtc1918	기본	불린값	false
network.trr.blacklist-duration	기본	정수	60
network.trr.bootstrapAddress	수정됨	문자열	1.1.1.1
network.trr.confirmationNS	기본	문자열	example.com
network.trr.credentials	기본	문자열	
network.trr.custom_uri	기본	문자열	
network.trr.disable-ECS	기본	불린값	true
network.trr.early-AAAA	기본	불린값	false
network.trr.max-fails	기본	정수	5
network.trr.mode	수정됨	정수	3
network.trr.request-timeout	기본	정수	1500
network.trr.uri	수정됨	문자열	https://dns.cloudflare.com/well-known/dns-query
network.trr.useGET	기본	불린값	false
network.trr.wait-for-portal	기본	불린값	true

- ESNI 설정을 활성화시켜줍니다.

검색창에서 esni라고 입력해서 나오는 항목중 network.security.esni.enabled를 true로 변경해 주세요 이것으로 설정은 끝이 났습니다.

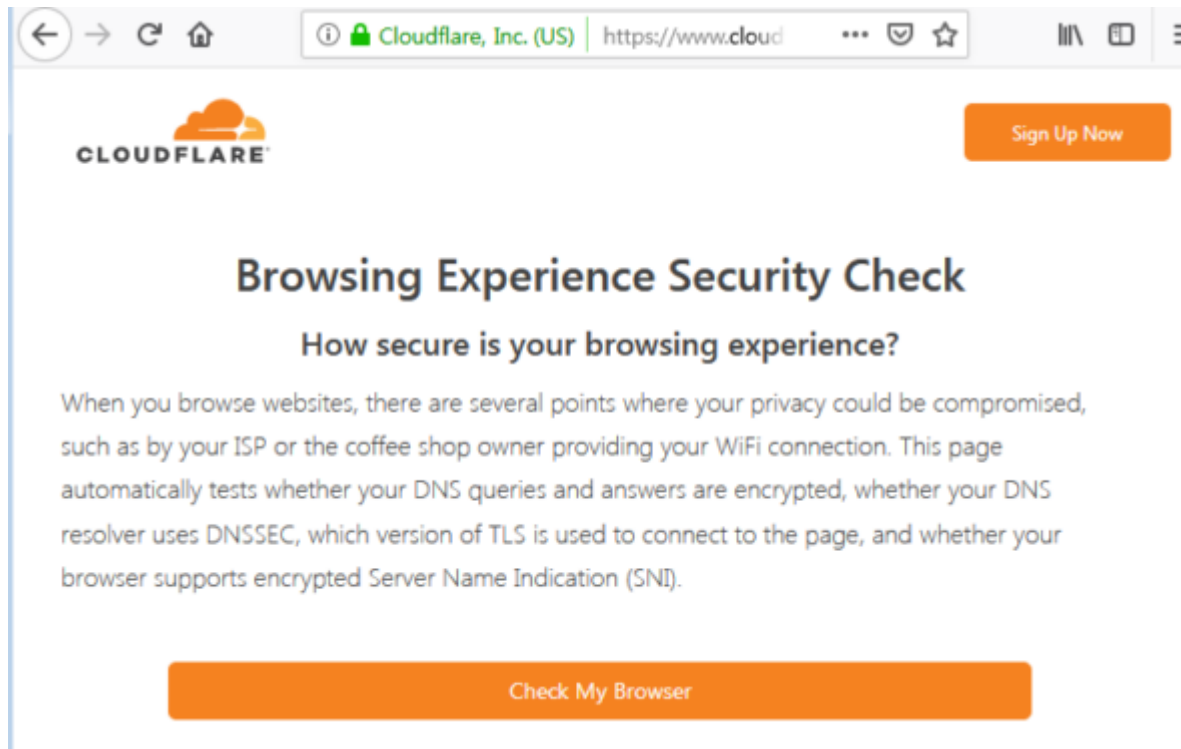


고급 설정
network.security.esni.enabled
network.security.esni.enabled
true

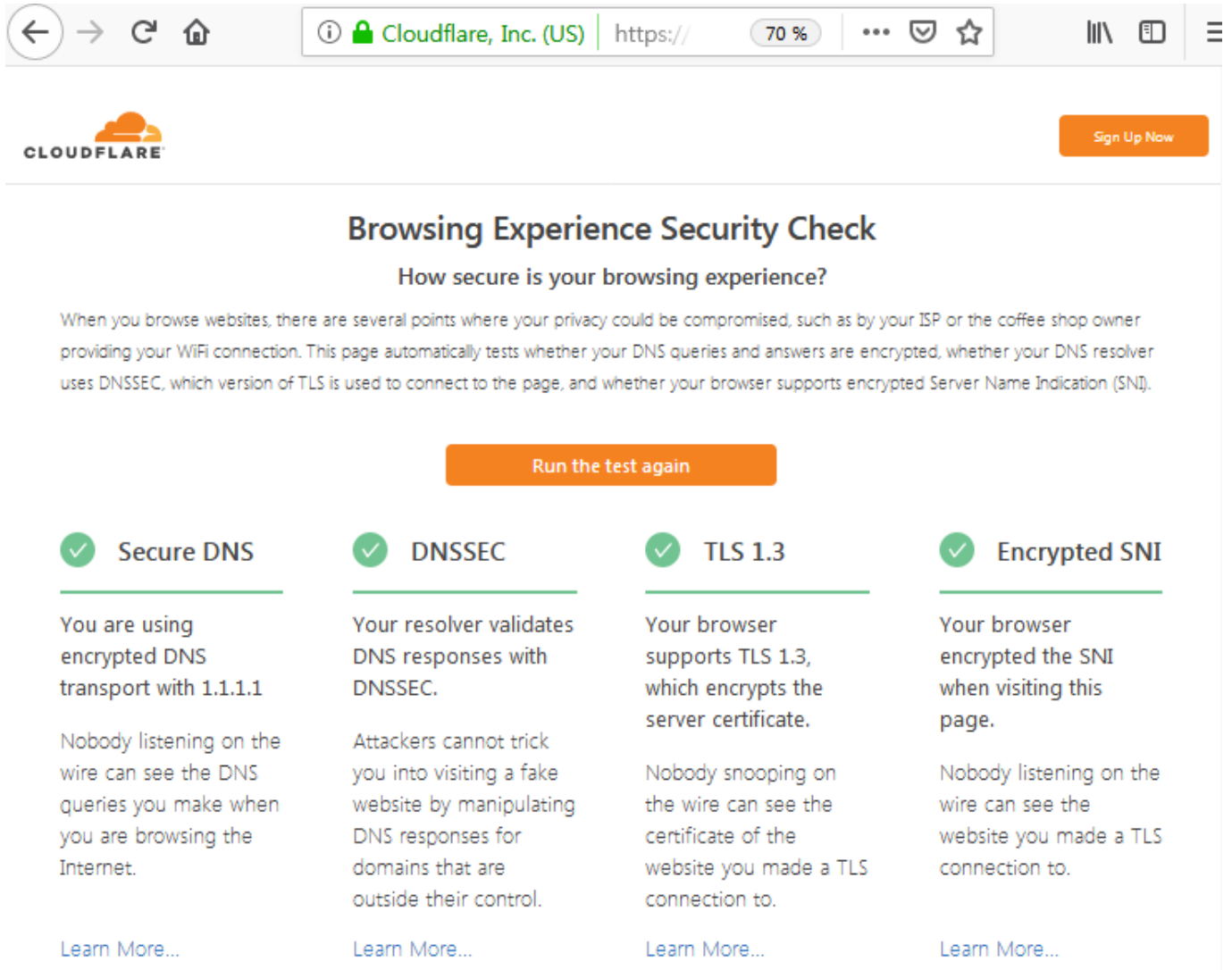
- ESNI통신이 잘 설정되었는지 검증해볼 단계입니다.

Firefox 로 아래 사이트에 접속해서 [Check My Browser]버튼을 클릭해주세요

<https://www.cloudflare.com/ssl/encrypted-sni/>



암호화된 DNS 통신이 잘 이루어지고 있다는 결과를 확인할 수 있습니다.



Browsing Experience Security Check

How secure is your browsing experience?

When you browse websites, there are several points where your privacy could be compromised, such as by your ISP or the coffee shop owner providing your WiFi connection. This page automatically tests whether your DNS queries and answers are encrypted, whether your DNS resolver uses DNSSEC, which version of TLS is used to connect to the page, and whether your browser supports encrypted Server Name Indication (SNI).

[Run the test again](#)

✓ Secure DNS	✓ DNSSEC	✓ TLS 1.3	✓ Encrypted SNI
You are using encrypted DNS transport with 1.1.1.1	Your resolver validates DNS responses with DNSSEC.	Your browser supports TLS 1.3, which encrypts the server certificate.	Your browser encrypted the SNI when visiting this page.
Nobody listening on the wire can see the DNS queries you make when you are browsing the Internet.	Attackers cannot trick you into visiting a fake website by manipulating DNS responses for domains that are outside their control.	Nobody snooping on the wire can see the certificate of the website you made a TLS connection to.	Nobody listening on the wire can see the website you made a TLS connection to.
Learn More...	Learn More...	Learn More...	Learn More...

- Firefox로 SNI 차단된 사이트에 접속해보면 잘 연결되는 것을 확인할 수 있습니다.

Firefox로 접속해보면 해당 사이트가 잘 연결되는 것을 확인할 수 있습니다. 하지만 크롬과 익스플로어로 해당 사이트를 접속하면 연결할 수 없다거나 이 페이지를 표시할 수 없다는 메시지가 나오는 것을 확인할 수 있습니다.

※ 이 방법은 PC의 설정을 변경시키지 않고 Firefox설치 및 설정만으로 SNI차단우회 가능한 것을 알 수 있습니다.

참조링크

- <http://jaewook.net/archives/9176>

From: <https://atl.kr/dokuwiki/> - AllThatLinux!

Permanent link: https://atl.kr/dokuwiki/doku.php/firefox_esni_%EC%A0%81%EC%9A%A9%ED%95%98%EA%B8%B0_warning%EC%B0%A8%EB%8B%A8%EC%9A%B0%ED%9A%BC

Last update: 2021/04/07 02:20

