EFF'S SURVEILLANCE SELF-DEFENSE

JINSI YA: KUELEWA NA KUEPUKA UDHIBITI WA MTANDAO

https://ssd.eff.org/en/about-surveillance-self-defense

ELECTRONIC FRONTIER FOUNDATION

LOCALIZATION LAB

Huu ni muhtasari wa udhibiti wa mtandao, lakini sio wa kina.

Serikali, kampuni, shule na watoa huduma za tovuti wakati mwingine hutumia programu ili kuzuia watumiaji wao kufikia wavuti na huduma fulani ambazo zinapatikana kwenye wavuti huria. Hili linaitwa uchujaji wa tovuti au kuzuia na ni aina ya udhibiti. Uchujaji hutokea kwa aina tofauti. Hata kwa usimbaji fiche, vidhibiti vinaweza kuzuia nyavuti zote, watoa huduma za kukaribisha au teknolojia za tovuti. Wakati mwingine, maudhui huzuiwa kulingana na maneno muhimu yaliyomo. Wakati wavuti hazijasimbwa kwa njia fiche, vidhibiti vinaweza pia kuzuia kurasa binafsi za wavuti.

Kuna njia tofauti za kukwepa udhibiti wa tovuti. Baadhi ya njia hizi zinakulinda kutokana na ufuatiliaji, lakini nyingi hazifanyi hivyo. Wakati mtu anayedhibiti muunganisho wako wa mtandao anachuja au anazuia wavuti, unaweza karibu kila wakati kutumia zana ya kuepuka ili kupata taarifa unayohitaji.

> Kumbuka: zana za kuepuka zinazoahidi ufaragha au usalama hazikuhakikishii faragha au usalama kila wakati. Zana zinazotumia maneno kama vile “kuzuia utambulisho” huwa hazifichi utambulisho wako vikamilifu.

Zana ya kuepuka ambayo ni bora kwako inategemea mpango wako wa usalama. Ikiwa huna uhakika wa jinsi ya kuunda mpango wa usalama, anza hapa . Unapounda mpango wa usalama, fahamu kwamba mtu anayedhibiti muunganisho wako wa tovuti anaweza kugundua kuwa unatumia zana au mbinu fulani ya kuepuka na kuchukua hatua dhidi yako au wengine.

Katika mwongozo huu, tutazungumza kuhusu kuelewa udhibiti wa tovuti, ni nani anayeweza kuutekeleza na jinsi inavyofanyika, kabla ya kuzungumzia kile unachoweza kufanya ili kuukwepa.

- Kuelewa udhibiti na ufuatiliaji wa tovuti
    - Udhibiti na Ufuatiliaji: Pande Mbili za Sarafu Moja
    - Gharama ya Ufuatiliaji
- Udhibiti na ufuatiliaji wa mtandao unafanyika wapi na kwa jinsi gani
    - Je, Uzuiaji Unatokea Wapi?
    - Je, Uzuiaji Unafanyika Vipi?
- Mbinu za Kuepuka
    - Kubadilisha mtoa huduma wako wa DNS ili Kufikia nyavuti au Huduma Zilizozuiwa

- Kutumia Mtandao Pepe Binafsi (VPN) au Proksi ya Wavutu Iliyosimbwa kwa Njia Fiche ili Kufikia Wavuti au Huduma zilizozuiwa.
- Kwa kutumia Kivinjari cha Tor ili Kufikia Wavuti Uliozuiwa au Kulinda Utambulisho Wako.

Kuelewa Udhibiti na Ufuatiliaji wa Tovuti

Tovuti ina michakato mingi ambayo yote inapaswa kufanya kazi pamoja vizuri ili kusambaza mawasiliano yako kutoka sehemu moja hadi nyingine. Ikiwa mtu anajaribu kuzuia sehemu za tovuti au shughuli fulani, anaweza kulenga sehemu nyingi tofauti za mfumo. Mbinu wanazotumia zinaweza kutegemea teknolojia na vifaa wanavyoweza kudhibiti, ujuzi wao, rasilimali zao na ikiwa wana uwezo wa kuwaambia wengine la kufanya.

Ufuatiliaji na Udhibiti: Pande Mbili za Sarafu Moja

Ufuatiliaji wa tovuti na udhibiti huenda pamoja. Udhibiti wa Tovuti ni mchakato wa hatua mbili:

1. Gundua shughuli "isiyokubalika"
2. Zuia shuguli "isiyokubalika"

Kugundua shughuli "isiyokubalika" ni sawa na ufuatiliaji wa tovuti. Ikiwa wasimamizi wa tovuti wanaweza kuona unapoenda kwenye mtandao, wanaweza kuamua kuuzuia. Kwa kutetea zana na teknolojia za faragha za tovuti na data, tunaweza pia kufanya uchujaji wa tovuti na uzuiaji kuwa mgumu zaidi.

Mbinu nyingi za kuepuka zina manufaa ya ziada ya kulinda maelezo yako kutoka kwa wasikilizaji wa mtandao unapoingia mtandaoni.

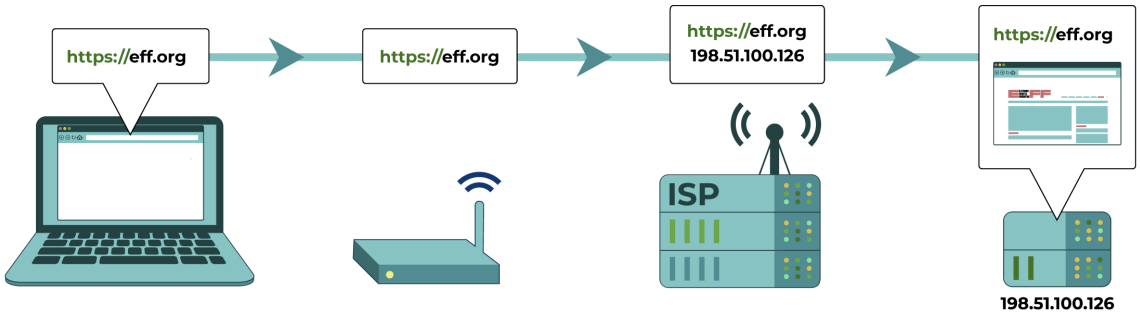
Gharama ya Ufuatiliaji

Kuzuia trafiki ya tovuti huja kwa gharama na uzuiaji kupita kiasi unaweza kuja kwa gharama kubwa zaidi. Mfano maarufu ni kwamba serikali ya Uchina haidhibiti wavuti wa GitHub, hata ingawa wavuti huo unahifadhi majarida mengi ya kupinga serikali. Watengenezaji wa programu wanahitaji ufikiaji wa GitHub ili kufanya kazi ambayo ina faida kwa uchumi wa nchi ya Uchina. Hivi sasa, huduma ya vidhibiti imeamua kwamba itawagharimu zaidi kuzuia Github kuliko kile ambacho wangeweza kupata kwa kuizuia.

Sio sensa zote vinaweza kufanya uamuzi sawa. Kwa mfano, kukatika kwa tovuti kwa muda kunazidi kuwa jambo la kawaida, ingawa hatua hizi zinaweza kudhuru uchumi wa eneo husika.

Jinsi na Mahali Ambapo Udhibiti na Ufuatiliaji Hutokea

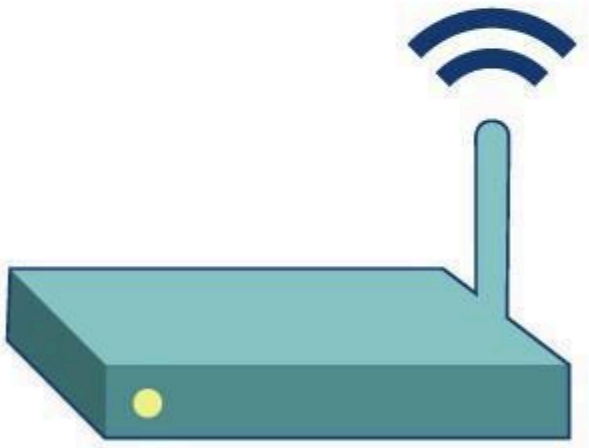
Je, Uzuiaji Unatokea Wapi?



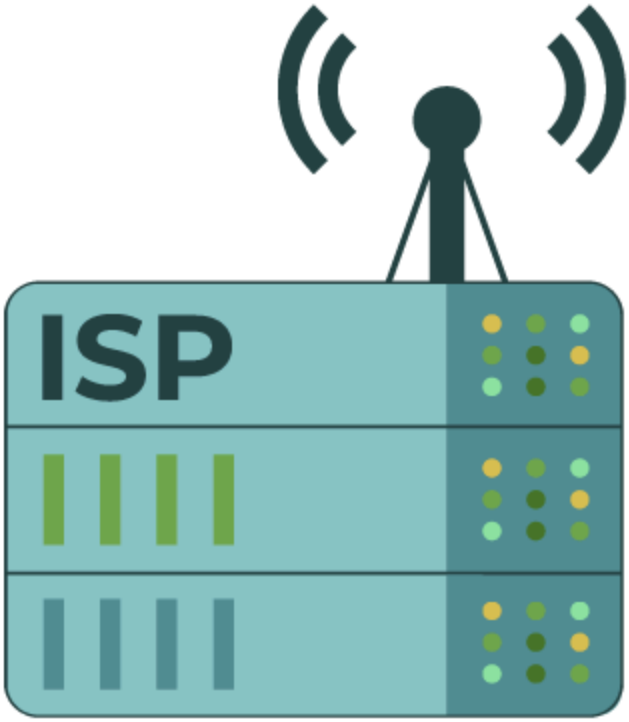
Kompyuta yako hujaribu kuunganisha kwenye https://eff.org, ambayo iko kwenye anwani ya IP ya Wavuti iliyoorodheshwa (mfuatano uliowekwa nambari kando ya seva inayohusishwa na wavuti wa EFF). Ombi la tovuti hiyo hutengenezwa na kutumwa kwa vifaa mbalimbali, kama vile ruta ya mtandao wako wa nyumbani na Mtoa Huduma wako wa tovuti (ISP), kabla ya kufikia anwani ya IP ya Wavuti iliyokusudiwa ya https://eff.org. Wavuti huo hutafuta na kufunguka kwenye kompyuta yako.

(1) Uzuiaji au uchujaji kwenye vifaa vyako. Hili ni jambo la kawaida hasa shuleni na kwenye sehemu za kazi. Mtu anayeweka au kudhibiti kompyuta na simu zenu anaweza

kuziwekea programu zinazoweka kikomo cha jinsi zinavyoweza kutumika. Programu hiyo hubadilisha jinsi kifaa kinavyofanya kazi na inaweza kukifanya kisiweze kufikia tovuti fulani au kuwasiliana mtandaoni kwa njia fulani. Programu ya kupeleleza inaweza kufanya kazi kwa njia hiyohiyo.



(2) Uchujaji wa mtandao wa eneo lako. Jambo hili pia ni la kawaida katika shule na sehemu za kazi. Mtu anayedhibiti mtandao wa eneo lako (kama mtandao wa WiFi) huweka vikomo fulani kwenye shughuli zako za mtandaoni, kama vile kufuatilia au kudhibiti unapoenda mtandaoni au unapotafuta maneno muhimu fulani.



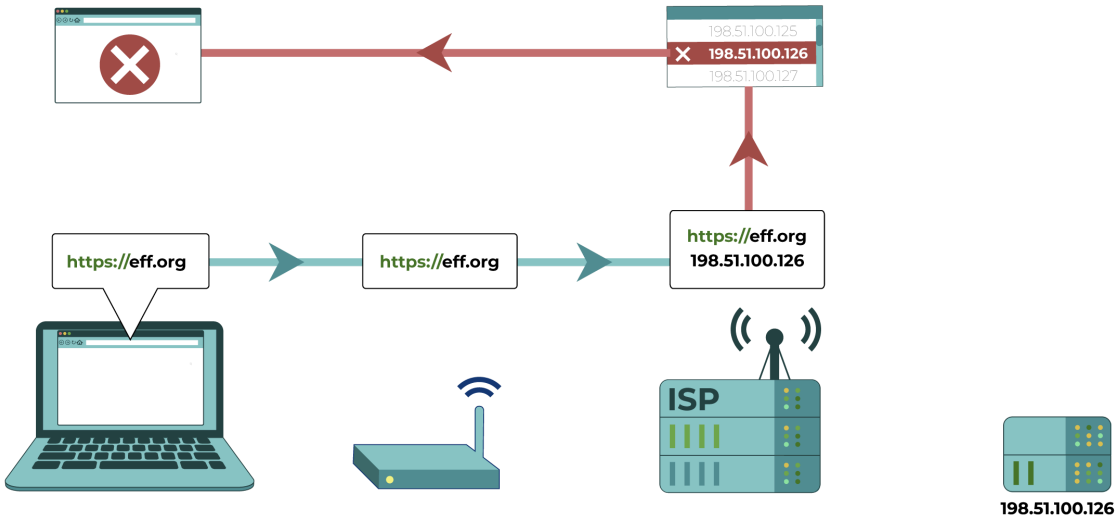
(3) Uzuiaji au uchujaji unaofanywa na Watoa Huduma za Tovuti (ISPs). Mtoa Huduma za Tovuti wako kwa ujumla anaweza kutekeleza aina sawa ya uchujaji kama

msimamizi wa mtandao wako. Watoa Huduma za Tovuti katika nchi nyingi wanalazimishwa na serikali yao kufanya uchujaji wa tovuti mara kwa mara na udhibiti. Watoa Huduma za Kibiashara wanaweza kufanya uchujaji kama huduma kwa familia au waajiri. Watoa huduma mahususi wa tovuti ya makazi wanaweza kutangaza miunganisho iliyochujwa moja kwa moja kwa wateja kama chaguo na kutumia kiotomatiki mbinu mahususi za udhibiti (kama zile zilizofafanuliwa hapa chini) kwa miunganisho yote iliyo kwenye Watoa Huduma za Tovuti. Wanaweza kufanya hivi hata kama haitakiwi na serikali, kwa sababu baadhi ya wateja wao wanataka ifanywe.

Je, Uzuiaji Unafanyika Vipi?

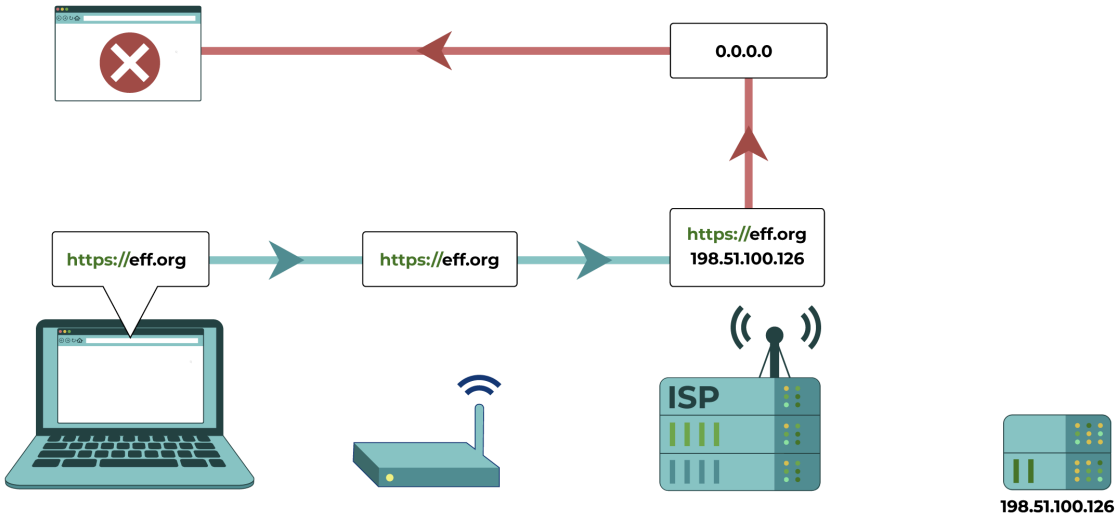
Uzuiaji wa anwani ya IP ya Wavuti: "anwani za IP za Wavuti" ni maeneo ya kompyuta kwenye Tovuti. Kila taarifa inayotumwa kwenye tovuti ina anwani ya "Kwa" na "Kutoka". Watoa Huduma za Intaneti au wasimamizi wa mtandao wanaweza kuunda orodha za maeneo ambayo yanalingana na huduma wanazotaka kuzuia. Kisha wanaweza kuzuia sehemu zozote za taarifa kwenye mtandao zinazosambazwa kutoka kwa maeneo hayo.

Hili linaweza kusababisha uzuiaji kupita kiasi, kwa kuwa huduma nyingi zinaweza kuhifadhiwa katika eneo moja au anwani ya IP ya Wavuti. Vile vile, watu wengi huishia kushiriki anwani yoyote ya IP ya wavuti kwa ufikiaji wao wa tovuti.



Katika mchoro huu, Mtoa Huduma ya Tovuti hukagua kwa njia tofauti anwani ya IP ya Wavuti iliyoombwa dhidi ya orodha ya anwani za IP za Wavuti zilizozuiwa. Unabainisha kuwa anwani ya IP ya Wavuti ya eff.org inalingana na anwani ya IP ya Wavuti iliyozuiwa na inazuia ombi kwenye wavuti.

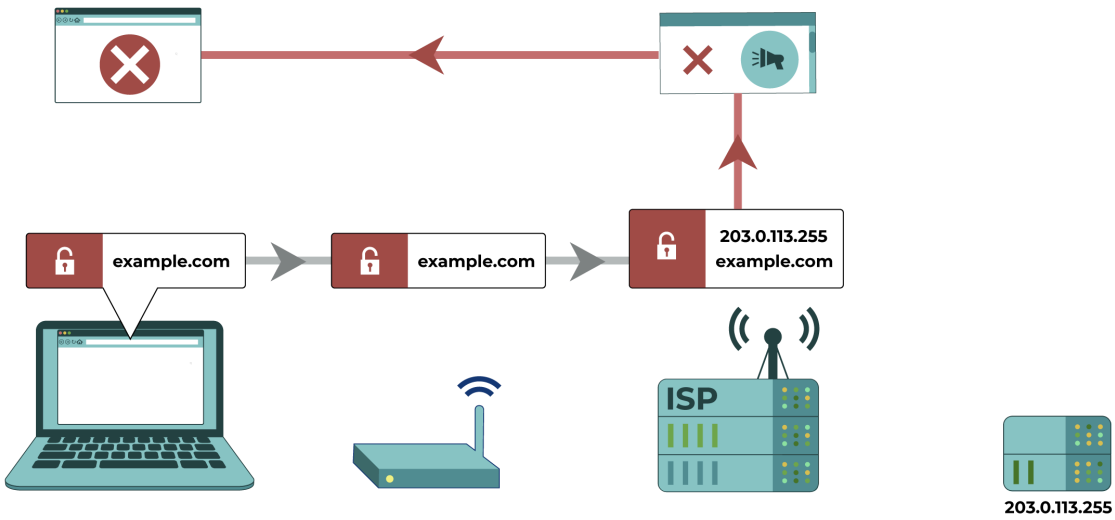
Uzuiaji wa DNS: Kifaa chako huuliza kompyuta zinazofahamika kama "DNS solvers" mahali tovuti ziko. Unapounganisha kwenye Tovuti, kisuluhishi chaguo-msingi cha DNS ambacho kifaa chako hutumia kwa kawaida huwa ni cha Mtoa Huduma wako wa Tovuti. Mtoa Huduma ya Tovuti anaweza kuunda kisuluhishi chake cha DNS ili kutoa jibu lisilo sahihi au kutoa jibu, wakati wowote mtumiaji anapojaribu kutafuta eneo la tovuti au huduma iliyozuiwa. Ukibadilisha kisuluhishi chako cha DNS, lakini muunganisho wako wa DNS haujasimbwa kwa njia fiche, Mtoa Huduma wako wa Tovuti bado anaweza kuzuia au kubadilisha majibu kwa huduma zilizozuiwa kwa kuchagua.



Katika mchoro huu, ombi la anwani ya IP ya Wavuti wa eff.org linarekebishwa katika kiwango cha Mtoa Huduma ya Tovuti. Mtoa Huduma ya Intaneti huingilia kisuluhishi cha DNS na anwani ya IP ya Wavuti inaelekezwa vingine ili kutoa jibu lisilo sahihi au kutotoa jibu.

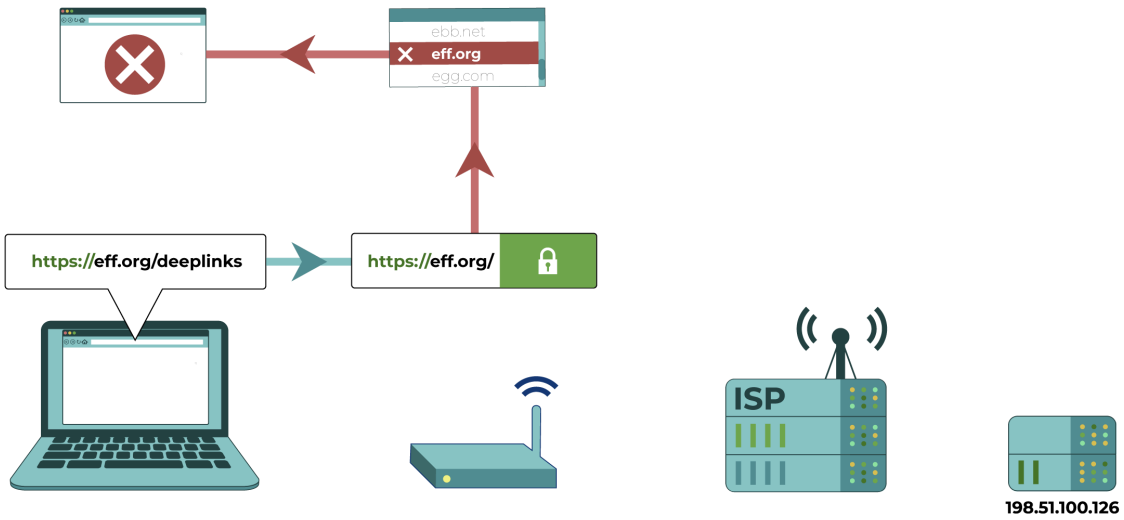
Uchujaji wa maneno muhimu: Ikiwa trafiki haijasimbwa, Watoa Huduma za Tovuti wanaweza kuzuia kurasa za wavuti kulingana na maudhui yaliyomo. Kwa ongezeko la jumla la tovuti zilizosimbwa kwa njia fiche, aina hii ya uchujaji inazidi kupunguza umaarufu.

Tahadhari moja ni kwamba wasimamizi wanaweza kusimbua shughuli iliyosimbwa kwa njia fiche ikiwa watumiaji watasakinisha “cheti cha CA” kinachoaminika kinachotolewa na wasimamizi wa kifaa chao. Kwa kuwa mtumiaji wa kifaa lazima asakinishe cheti, hii ni desturi ya kawaida zaidi kwa mitandao ya mahali ulipo kazini na shuleni, lakini si desturi ya kawaida sana katika kiwango cha Mtoa Huduma ya Tovuti.



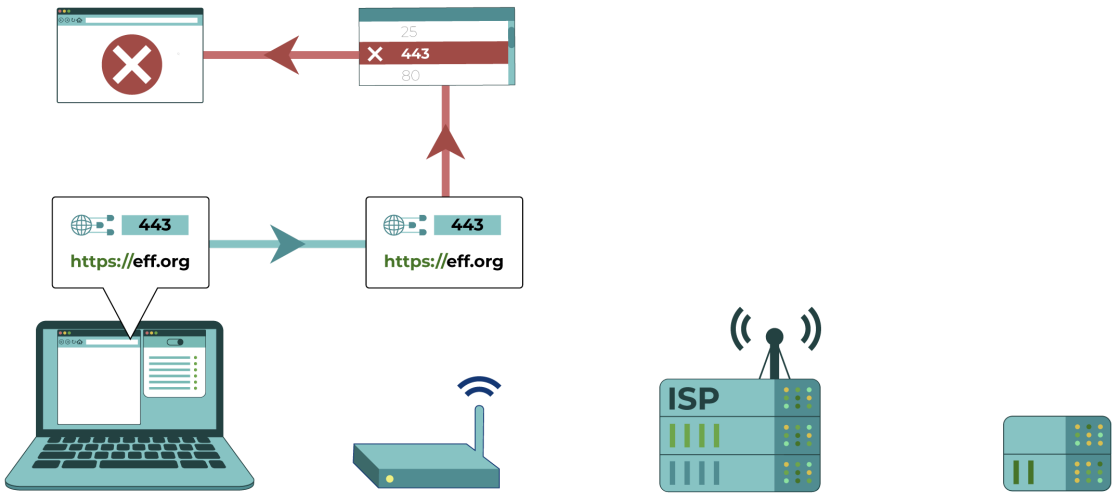
Kwenye muunganisho wa tovuti ambao haujasimbwa kwa njia fiche, Mtoa Huduma ya Mtandao anaweza kukagua maudhui ya tovuti dhidi ya aina zake za maudhui zilizozuiwa. Katika mfano huu, kutaja uhuru wa kujieleza husababisha akaunti kuzuiwa kiotomatiki.

Uchujaji wa wavuti wa HTTPS: Unapofikia tovuti kupitia HTTPS, maudhui yote yamesimbwa kwa njia fiche isipokuwa jina la tovuti. Kwa kuwa bado wanaweza kuona jina la wavuti, Wato Huduma za Tovuti au wasimamizi wa mtandao wako wanaweza kuamua ni tovuti zipi watazuia ufikiaji.



Katika mchoro huu, kompyuta inajaribu kufikia eff.org/deeplinks. Msimamizi wa mtandao (anayewakilishwa na ruta) anaweza kuona kikoa (eff.org) lakini si anwani kamili ya tovuti baada ya alama ya mlazo. Msimamizi wa mtandao anaweza kuamua ni vikoa vipi vya kuzuia ufikiaji.

Uzuiaji wa itifaki na poti: Ngome ya mtandao au ruta inaweza kujaribu kutambua ni aina gani ya teknolojia ya mtandao ambayo mtu anatumia kuwasiliana, kisha kuzuia baadhi kwa kutambua maelezo ya kiufundi ya jinsi wanavyowasiliana (itifaki na nambari za poti ni mifano ya taarifa inayoweza kutumika kutambua teknolojia inayotumika). Ikiwa ngome ya mtandao inaweza kutambua kwa usahihi aina ya mawasiliano yanayofanyika au ni teknolojia inayotumika, inaweza kusanidiwa ili isisambaze mawasiliano hayo. Kwa mfano, baadhi ya mitandao inaweza kuzuia teknolojia zinazotumiwa na baadhi ya VoIP (mawasiliano ya simu ya mtandaoni), programu ya kushiriki faili au programu za Mtandao Pepe Binafsi.



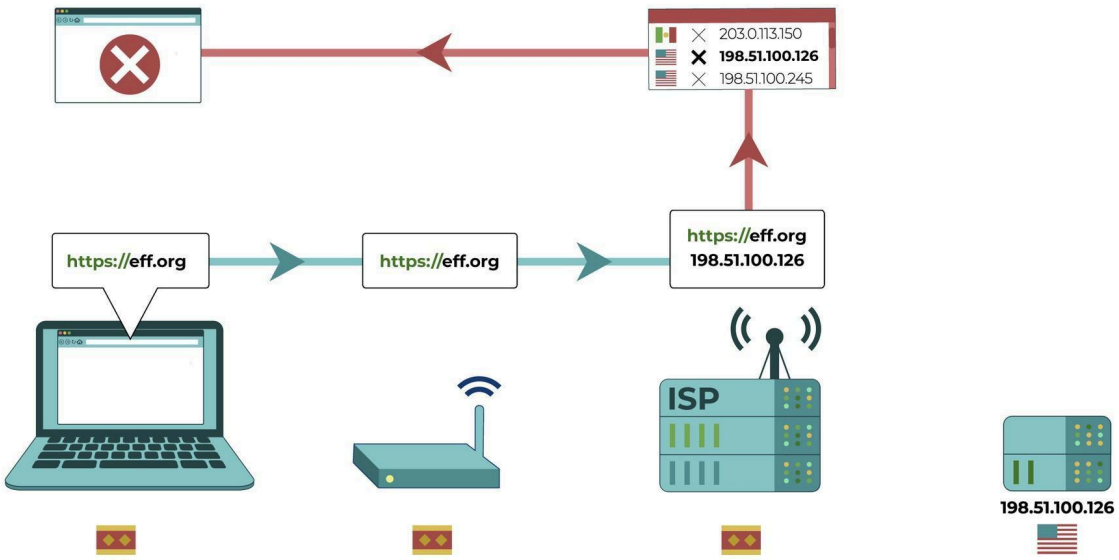
Katika mchoro huu, ruta hutambua kompyuta inayojaribu kuunganisha kwenye wavuti wa HTTPS, ambayo inatumia Port 443. Port 443 iko kwenye orodha ya ruta hii ya itifaki zilizozuiwa.

Aina nyingine za uzuiaji

Kwa kawaida, kuzuia na kuchuja hutumiwa kuzuia watu kufikia tovuti au huduma maalum. Hata hivyo, aina tofauti za uzuiaji zinazidi kuwa za kawaida pia.

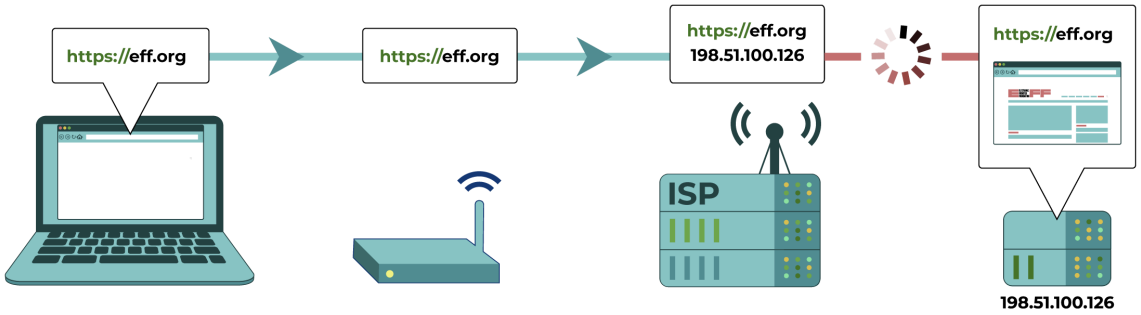
Kuzimwa kwa mtandao: Kuzimwa kwa mtandao kunaweza kuhusisha uondoaji wa miundomsingi ya mtandao, kama vile ruta, kebo za mtandao au minara ya simu, ili miunganisho izuiwe au iwe mbaya hadi kiwango cha kutotumika.

Hii inaweza kuwa hali maalum ya kuzuia anwani ya IP ya Wavuti, ambapo anwani zote za IP za Wavuti au nyingi zimezuiwa. Kwa sababu mara nyingi inawezekana kutambua nchi inayotumia anwani ya IP ya Wavuti, baadhi ya nchi pia zimejaribu kuzuia kwa muda anwani zote au nyingi za IP za wavuti za kigeni, kuruhusu baadhi ya miunganisho iliyo nchini lakini kuzuia miunganisho mingi inayoenda nje ya nchi.



Kompyuta inajaribu kuunganisha kwenye anwani ya IP ya Wavuti wa eff.org ya Marekani. Katika kiwango cha Mtoa Huduma ya tovuti, ombi hukaguliwa: anwani ya IP ya wavuti wa eff.org inakaguliwa kwa kulinganishwa na orodha ya anwani za kimataifa za IP za Wavuti zilizozuiwa na inazuiwa.

Kupunguza Kasi ya Tovuti: Watoa Huduma za Tovuti wanaweza kupunguza (kupunguza kasi) aina tofauti za trafiki kwa kuchagua. Vidhibiti vingi vya serikali hupunguza kasi ya miunganisho kwenye tovuti fulani badala ya kuzizuia kabisa. Uzuiaji wa aina hii ni ngumu zaidi kuutambua na huruhusu Mtoa Huduma kukataa kuwa anazuia ufikiaji. Watu wanaweza kufikiri kwamba muunganisho wao wa tovuti unakasi ya chini au kwamba huduma wanayounganisha haifanyi kazi.

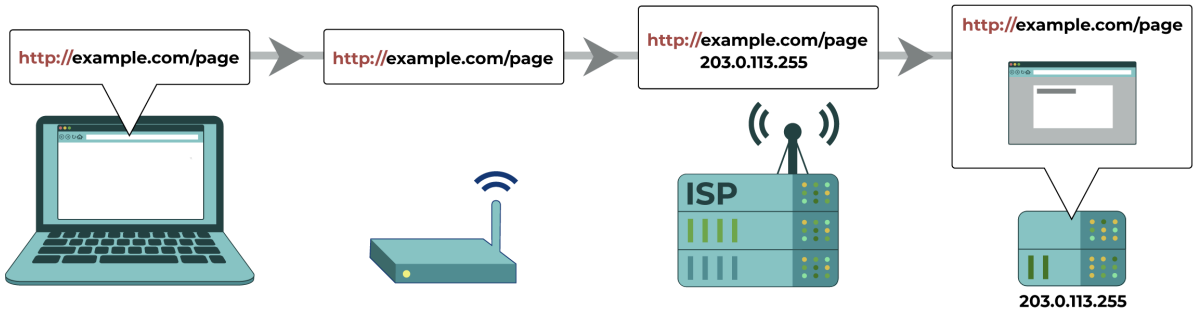


Kompyuta inajaribu kuunganisha kwenye eff.org. Mtoa Huduma wao wa tovuti hupunguza kasi ya muunganisho wao.

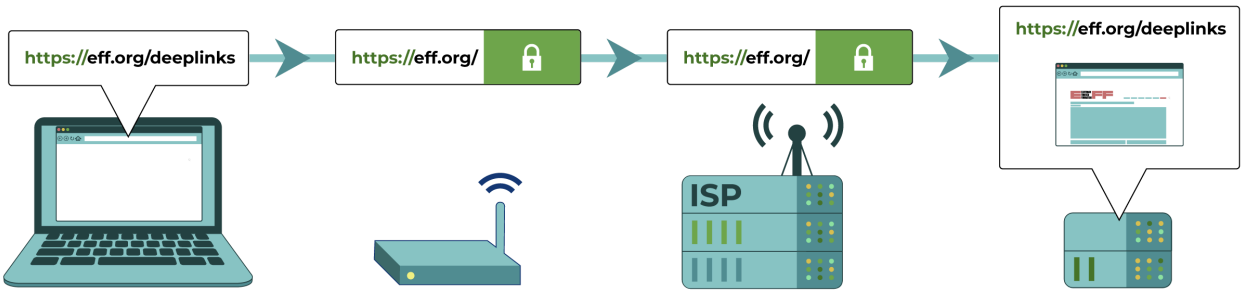
Mbinu za Kuepuka

Vipengele kama vile eneo lako na aina gani ya udhibiti wa mtandao unaokumbana nao husaidia kubainisha ni mbinu gani ya kukwepa itakayokufaa zaidi. Iwapo huna uhakika ni aina gani ya uzuiaji unaokabiliana nao, zana kama vile OONI Probe inaweza kukusaidia kutambua ni aina gani za uzuiaji unaokuathiri. Lakini, tahadhari kuwa kutumia zana hii kunaweza kukuweka hatarini kwa sababu yeyote anayesimamia mtandao wako atajua kuwa unatumia programu hiyo na nchi fulani zinaweza kuzuia zana hii kabisa.

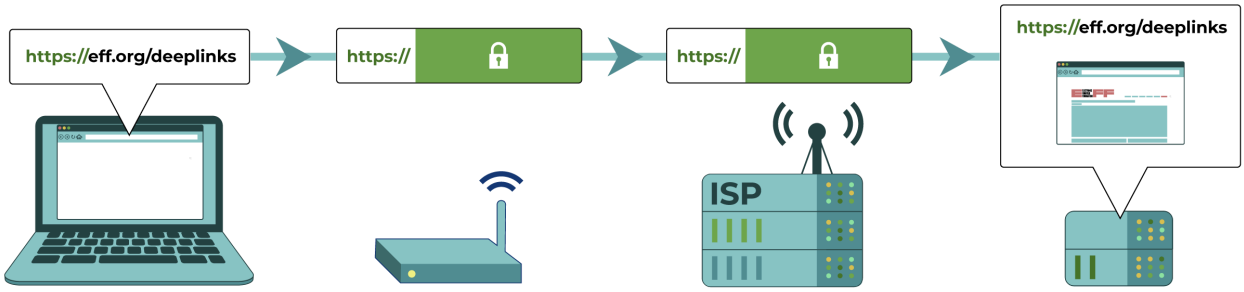
Kadiri kuna maelezo machache kuhusu shughuli yako ya mtandaoni, ndivyo inavyoweza kuwa vigumu kwa Mtoa Huduma yako ya Tovuti au msimamizi wa mtandao kuzuia kwa kuchagua aina fulani za shughuli. Ndiyo maana kutumia viwango vya usimbaji fiche vya kote mtandaoni, kama vile HTTPS na DNS iliyosimbwa kwa njia fiche, kunaweza kusaidia katika baadhi ya matukio.



HTTP hulinda maelezo yako machache ya kuvinjari...



..HTTPS inalinda mengi zaidi...



…DNS iliyosimbwa kwa njia fiche na itifaki zingine zitalinda jina la wavuti, pia.

Badilisha Mtoa Huduma wako wa DNS na Utumie DNS Iliyosimbwa kwa Njia Fiche

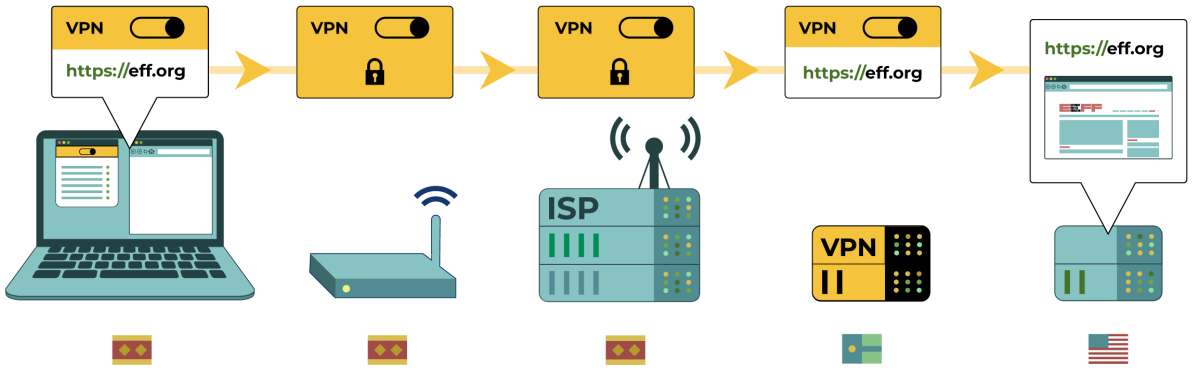
Ikiwa Watoa Huduma ya Tovuti wanategemea tu **uzuiaji wa DNS,** kubadilisha mtoa huduma wako wa DNS na kutumia DNS iliyosimbwa kwa njia fiche kunaweza kurejesha ufikiaji wako.

Badilisha mtoa huduma wako wa DNS: Hili linaweza kufanywa katika sehemu ya "mipangilio ya mtandao" iliyo kwenye kifaa chako (simu au kompyuta). Kumbuka kuwa mtoa huduma wako mpya wa DNS atapata taarifa kuhusu shughuli yako ya kuvinjari ambayo Mtoa Huduma wako wa Intaneti aliwahi kuwa nayo, jambo ambalo linaweza kuwa suala la faragha kulingana na mfano wako wa tishio. Mozilla hukusanya orodha ya watoa huduma ya DNS ambao wana sera thabiti za faragha na ahadi za kutoshiriki data yako ya kuvinjari.

Tumia DNS iliyosimbwa kwa njia fiche: Teknolojia za DNS zilizosimbwa kwa njia fiche huzuia msimamizi yeyote wa mtandao kuona (na kuchuja) trafiki yako ya DNS. Lakini kulingana na ripoti ya mwaka wa 2022 , baadhi ya serikali zimezuia miisho inayojulikana ya DNS kupitia HTTPS na DNS kupitia TLS. Iwapo unatumia huduma zozote maarufu za DNS zilizosimbwa kwa njia fiche kama vile 1.1.1.1 au 8.8.8.8, fahamu kuwa serikali zinaweza kulenga miisho hii na kuizuia pia.

Unaweza kusanidi itifaki ya DNS-juu ya-HTTPS kwenye Firefox. Chrome na Microsoft Edge zote zinakubali itifaki ya DNS-juu ya-HTTPS, ingawa zote zinairejelea kama "DNS Salama." Unaweza pia kusanidi itifaki ya DNS kupitia TLS kwenye Android. Mifumo ya iOS na macOS yote inakubali itifaki ya DNS-juu ya-HTTPS, ingawa zinahitaji usakinishe wasifu wa wahusika wengine na hazijawezeshwa kwa chaguo-msingi.

Tumia VPN



Katika mchoro huu, kompyuta inatumia VPN, ambao husimba trafiki yake na kuunganishwa na eff.org. Ruta ya mtandao na Mtoa Huduma ya Intaneti wanaweza kuona kwamba kompyuta inatumia VPN, lakini data imesimbwa kwa njia fiche. Mtoa Huduma ya Tovuti huelekeza muunganisho kwenye seva ya VPN katika nchi nyingine. VPN hiyo basi huunganishwa kwenye wavuti wa eff.org.

Ukikumbana na aina fulani za uzuiaji wa IP ya Wavuti wa eneo au jimbo, VPN inaweza kuwa muhimu katika kuepuka mbinu hizi, ingawa unakuja na tahadhari zake za matumizi na huenda usifanye kazi hata kidogo.

Mtandao Pepe Binafsi (VPN) husimba na kutuma data yote ya mtandao kutoka kwa kompyuta yako kupitia seva (kompyuta nyingine), ambayo inaweza kuwa katika nchi nyingine kwa hiari. Katika baadhi ya matukio, hii inaweza kukusaidia kufikia tovuti ambazo hazipatikani katika kaunti yako. Kompyuta hii inaweza kuwa ya huduma ya kibiashara au isiyo ya faida ya VPN, kampuni yako au ya mtu unayemwamini. Mara tu huduma ya VPN inaposanidiwa kwa usahihi, unaweza kuitumia kufikia kurasa za wavuti, barua pepe, ujumbe wa papo hapo, VoIP, na huduma nyingine yoyote ya

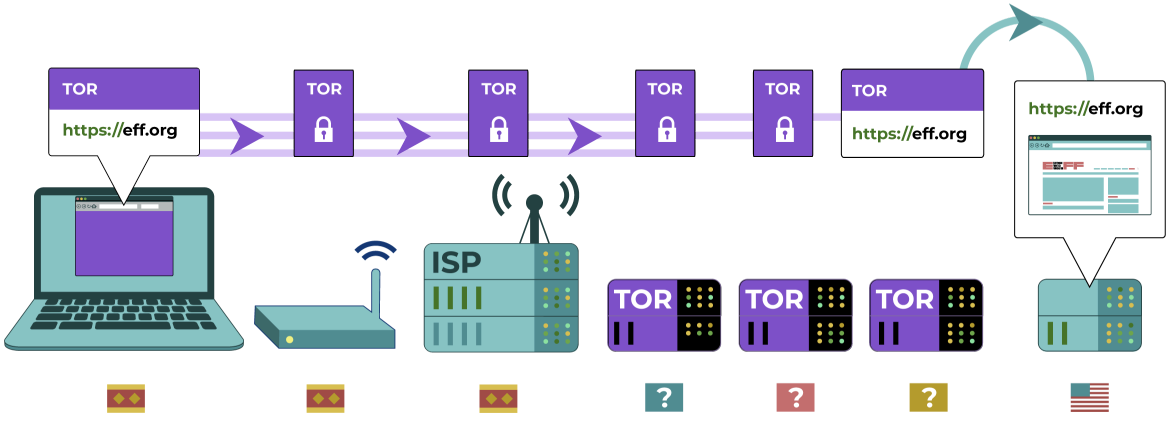
mtandaoni. VPN hulinda trafiki yako dhidi ya kupelelezwa katika eneo lako, lakini mtoa huduma wako wa VPN bado anaweza kuweka rekodi (pia hujulikana kama kumbukumbu) za tovuti unazofikia au hata kuruhusu mtu mwingine atazame moja kwa moja katika kuvinjari kwako kwa wavuti. Kulingana na mfano wa tishio lako, uwezekano wa serikali kuchunguza muunganisho wako wa VPN au kupata ufikiaji wa kumbukumbu zako za VPN zinaweza kuwa hatari kubwa. Kwa watumiaji wengine, hili linaweza kuwa na athari kubwa ikilinganishwa na faida za muda mfupi za kutumia VPN.

Angalia mwongozo wetu kuhusu kuchagua huduma mahususi za Mtandao Pepe Binafsi (VPN).

Tumia Kivinjari cha Tor

Ukikumbana na uzuiaji wa itifaki au poti, uzuiaji wa anwani ya IP ya Wavuti, uzuiaji wa DNS au ikiwa VPN haikusaidii kuepuka udhibiti, basi kivinjari cha Tor kinaweza kukusaidia. Kivinjari cha Tor kina chaguo kadhaa za kuepuka aina mbalimbali za udhibiti, lakini kumbuka kuwa mtu yeyote anayeweza kuona shughuli zako za mtandaoni atajua kuwa unatumia Tor.

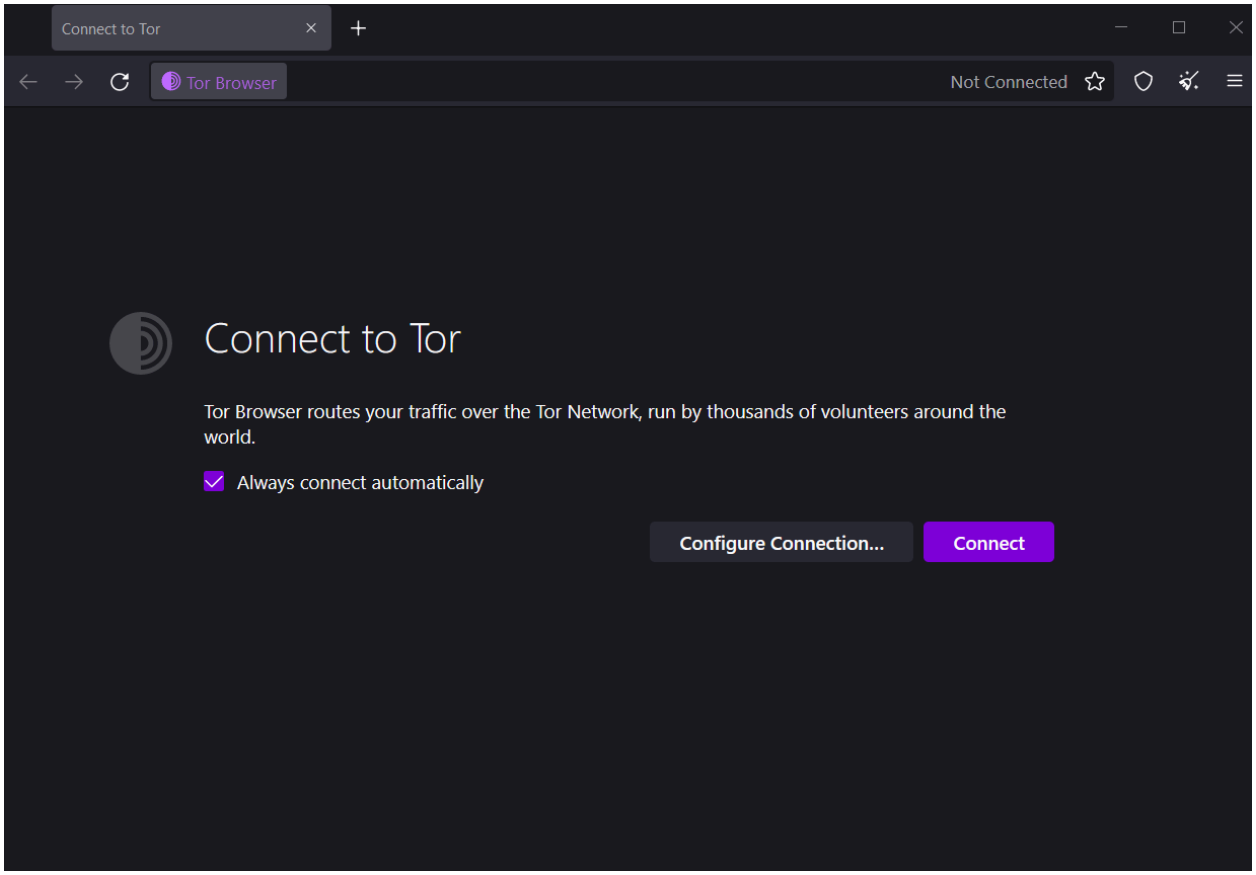
Tor ni programu huria iliyoundwa ili kukupa hali ya kutojulikana kwenye wavuti. Kivinjari cha Tor ni kivinjari cha wavuti kilichojengwa juu ya mtandao wa kutokujulikana wa Tor. Kwa sababu ya jinsi Tor huelekeza trafiki yako ya kuvinjari kwenye wavuti, pia hukuruhusu uepuke udhibiti.



Kompyuta hiyo hutumia Tor kuunganisha kwenye eff.org. Tor huelekeza muunganisho kupitia "rilei" kadhaa, ambazo zinaweza kuendeshwa na watu binafsi au mashirika mbalimbali kote duniani. "Rilei ya kutoka" ya mwisho huunganishwa kwenye eff.org.

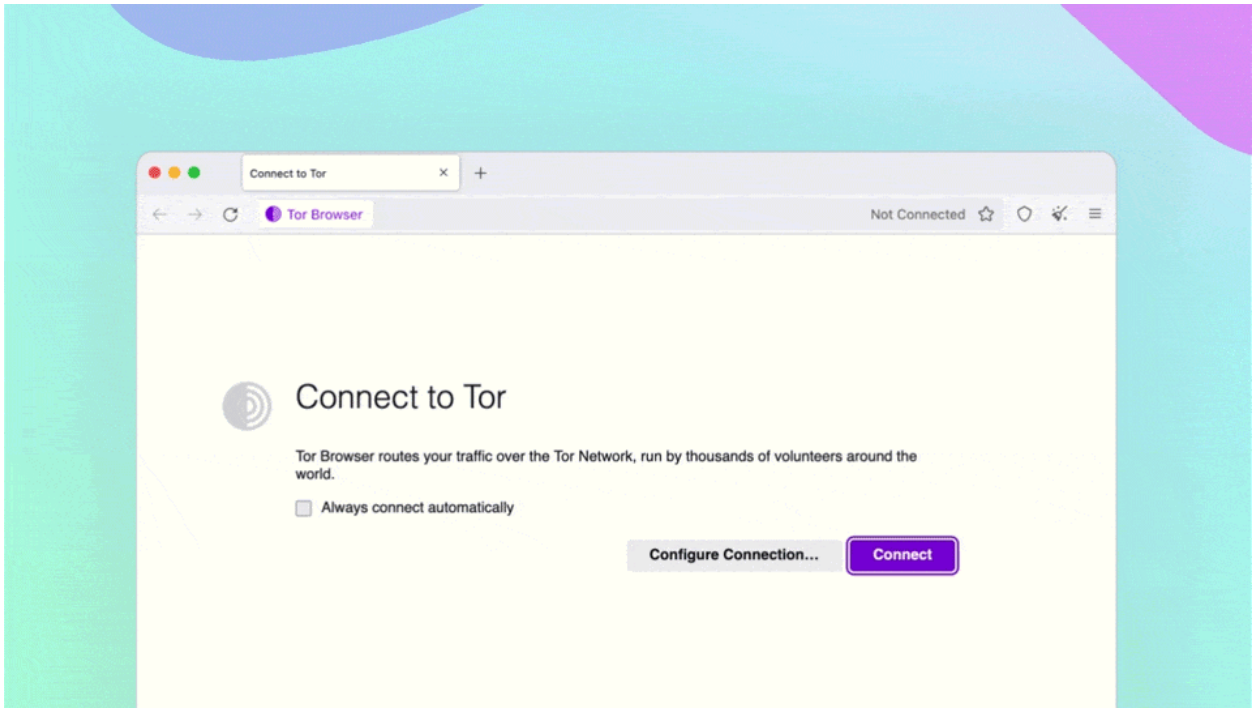
Mtoa Huduma ya Intaneti anaweza kuona kuwa unatumia Tor, lakini hawezi kuona kwa urahisi ni tovuti gani unatembelea. Mmiliki wa eff.org, vile vile, anaweza kutambua mtu anayetumia Tor ameunganisha kwenye tovuti yake, lakini hajui mtumiaji huyo anatokea wapi.

Unapowasha Kivinjari cha Tor kwa mara ya kwanza, bofya kitufe cha "Sanidi Muunganisho..." ili kubadilisha mipangilio ya muunganisho upendavyo wewe mwenyewe au ubofye tu "Unganisha" ili kuanza:



Kivinjari cha Tor hakitaepuka tu udhibiti fulani wa kitaifa, lakini, ikiwa kimesanidiwa vizuri, kinaweza pia kulinda utambulisho wako dhidi ya adui anayesikiliza kwenye mitandao ya nchi yako. Hata hivyo, inaweza kuwa na kasi ya chini na pia ugumu wa kutumia na mtu yeyote anayeweza kuona shughuli zako za mtandaoni anaweza kutambua kuwa unatumia Tor.

Ikiwa kwa sababu yoyote Tor imezuiwa kwako. Kipengele cha "Usaidizi wa Muunganisho" kinaweza kukusaidia kuchagua "daraja" kwa ajili yako kwa kutumia eneo lako.



Kumbuka: Hakikisha unapakua Kivinjari cha Tor kutoka kwenye tovuti rasmi.

Jifunze jinsi ya kutumia Tor kwenye mifumo ya Linux,macOS,Windowsnasimu maizi.

Kutumia Seva za Proksi kwenye Programu za Kutuma Ujumbe

Ikiwa huwezi kufikia programu salama za kutuma ujumbe kama vile WhatsApp au Signal katika eneo lako, unaweza kutumia seva ya proksi ili kuepuka baadhi ya aina za udhibiti. Hili linawezekana ili uweze kuwasiliana na wengine wakati programu imezuiwa. Seva hizi za proksi zinaendeshwa na watu waliojitolea, lakini mawasiliano yako yatasalia yakiwa yamesimbwa kwa njia fiche kutoka mwisho hadi mwisho, kuhakikisha kwamba hakuna mtu yeyote, ikiwa ni pamoja na wale wanaoendesha seva ya proksi, wanaweza kuona maudhui ya ujumbe. Hata hivyo, mtoa huduma ya proksi ataweza kuona anwani yako ya Itifaki ya wavuti.

Jifunze jinsi ya kutumia seva za proksi kwenye SignalnaWhatsapp.