EFF'S SURVEILLANCE SELF-DEFENSE

KUELEWA NA KUKWEPA UDHIBITI WA MTANDAO

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

LOCALIZATION LAB

Kuelewa na Kukwepa Udhibiti wa Mtandao

Last reviewed in English: 4-25-2020

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

Serikali, makampuni, shule, na watoaji wa huduma za mitandao wakati mwingine hutumia programu kuzuia watumiaji wao kupata baadhi ya tovuti na huduma ambazo zinapatikana kwenye wavuti. Hii inaitwa Uchujaji wa Intaneti au kuzuia mtandao, na ni aina ya udhibiti. Kuchuja huja kwa aina tofauti. Hata kwa usimbuaji fiche, vidhibiti vinaweza kuzuia tovuti zote, watoa huduma, au teknolojia za mtandao. Wakati mwingine, yaliyomo yanazuiliwa kulingana na maneno muhimu yaliyomo. Wakati tovuti hazijasimbwa kwa njia fiche, wadhibiti wanaweza pia kuzuia kurasa za wavuti za kibinafsi

Kuna njia tofauti za kupiga udhibiti wa mtandao. Nyingine zinakukinga kutokana na ufuatiliaji, lakini nyingine hazikulindi. Wakati mtu ambaye anadhibiti vichungi vyako vya wavu au anazuia wavuti, unaweza karibu kila wakati kutumia zana ya kukwepa kupata habari unayohitaji.

> Kumbuka: Zana za kukwepa ambazo zinaahidi faragha au usalama sio za faragha au salama kila wakati. Na zana ambazo hutumia maneno kama "anonymizer" sio kila wakati zinaweka utambulisho wako kuwa siri kabisa.

Zana ya kukwepa ambayo ni bora kwako inategemea mpango wako wa usalama. Ikiwa hauna hakika jinsi ya kuunda mpango wa usalama, anza hapa. Wakati unaunda mpango wa usalama, fahamu kuwa mtu anayedhibiti muunganisho wako wa Mtandao anaweza kugundua kuwa unatumia zana au mbinu fulani ya kukwepa, na achukue hatua tena ni wewe au wengine

Katika makala haya, tutazungumza juu ya kuelewa udhibiti wa mtandao, ni nani anayeweza kuifanya, na jinsi inavyofanyika.

- Kutumia Mtandao wa Kibinafsi wa Virtual (VPN) au proksi iliyosimbwa kwa wavuti kufikia tovuti au huduma zilizozuiwa.
- Kutumia Kivinjari cha Tor kufikia tovuti iliyozuiwa au kulinda kitambulisho chako

Kuelewa udhibiti wa mtandao na ufuatiliaji

Mtandao una michakato mingi ambayo yote inapaswa kufanya kazi vizuri ili kupata mawasiliano yako kutoka sehemu moja hadi nyingine. Ikiwa mtu anajaribu kuzuia sehemu za mtandao, au shughuli zingine, zinaweza kulenga sehemu nyingi tofauti za mfumo. Njia wanazotumia zinaweza kutegemea ni teknolojia gani na vifaa ambavyo wanadhibiti, maarifa yao, rasilimali zao, na ikiwa wako katika nafasi ya nguvu kuwaambia wengine nini cha kufanya

Ufuatiliaji na Udhibiti wa mawasiliano: Pande mbili za Sarafu Moja

Ufuatiliaji wa mawasiliano huenda sambamba na udhibiti wa mtandao. Udhibiti wa mtandao ni mchakato wa hatua mbili

1. Kutambua shughuli “zisizokubalika” mtandaoni
2. Kuzuia shughuli “zisizokubalika” mtandaoni

Mchakato wa kutambua shughuli "zisizokubalika" ni sawa na ufuatiliaji wa kimtandao. Ikiwa wasimamizi wa mtandao wanaweza kuona unachokifanya kwenye mtandao, wanaweza kuamua kuzuia au kutokuzuia. Kwa kutetea zana na teknolojia za faragha za mtandao na data, tunaweza pia kufanya uchujaji wa mtandao na kuzuia kuwa ngumu zaidi.

Mbinu nyingi za kuzuia vivyo hivyo zina faida ya ziada ya kulinda taarifa zako kutoka kwa wasikilizaji wa mtandao unapoingia mtandaoni.

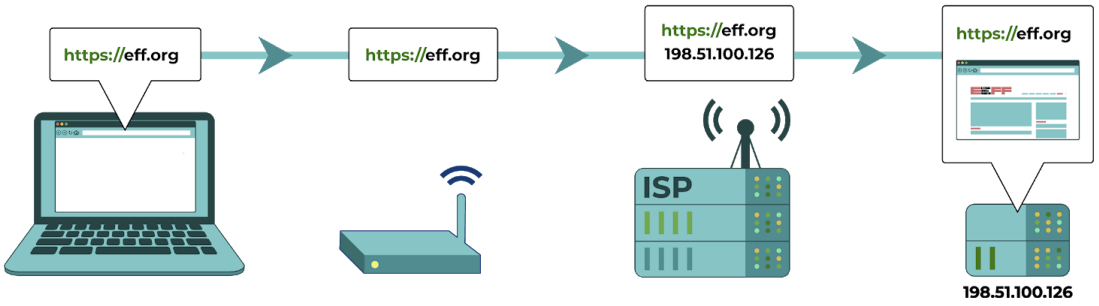
Gharama za Ufuatiliaji

Kuzuia msongamano wa taarifa katika mtandao hugharimu, na kuzuia zaidi kunaweza kuja kuwa gharama kubwa zaidi. Mfano maarufu ni kwamba serikali ya China haifutii wavuti ya GitHub, ingawa majarida mengi yanayopinga serikali yanapatikana kwenye wavuti hiyo. Watengenezaji wa programu za teknolojia wanahitaji kutumia GitHub kufanya kazi ambayo ina faida kwa uchumi wa China. Hivi sasa, wadhibiti hawa wameamua kuzuia Github kutokana na gharama ambazo zita waletea hasara.

Sio wachunguzi wote wangefanya uamuzi sawa. Kwa mfano, kuzimwa kwa mtandao kwa muda kunazidi kuwa kawaida, ingawa hatua hizi zinaweza kudhuru uchumi wa ndani.

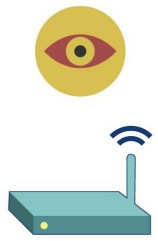
Udhibiti na ufuatiliaji hufanyika wapi na kwa namna gani

Uzuiaji unatokea wapi?



Kompyuta/tarakilishi yako inajaribu kuunganishwa na https://eff.org, ambayo iko kwenye anwani kupitia Itifaki ya wavuti (IP) iliyoorodheshwa (mlolongo uliohesabiwa kando ya seva inayohusishwa na wavuti ya EFF). Ombi la tovuti hiyo hufanywa na kupitishwa kwa vifaa anuwai, kama vile njia yako ya mtandao wa nyumbani na Mtoa Huduma wako wa Mtandao (ISP), kabla ya kufikia anwani kupitia Itifaki ya Wavuti inayokusudiwa ya https://eff.org. Tovuti imefanikiwa kuunganishwa na kompyuta yako.

(1) Uzuiaji au uchujaji kwenye vifaa vyako. Hii ni kawaida sana shuleni na mahali pa kazi. Mtu ambaye anaweka au kusimamia kompyuta na simu zako anaweza kuweka programu ambazo zinazuia matumizi ya vifaa vyako. Programu inabadilisha jinsi kifaa hufanya kazi na inaweza kuifanya ishindwe kufikia tovuti fulani, au kuwasiliana mkondoni kwa njia fulani. Spyware inaweza kufanya kazi kwa njia sawa.



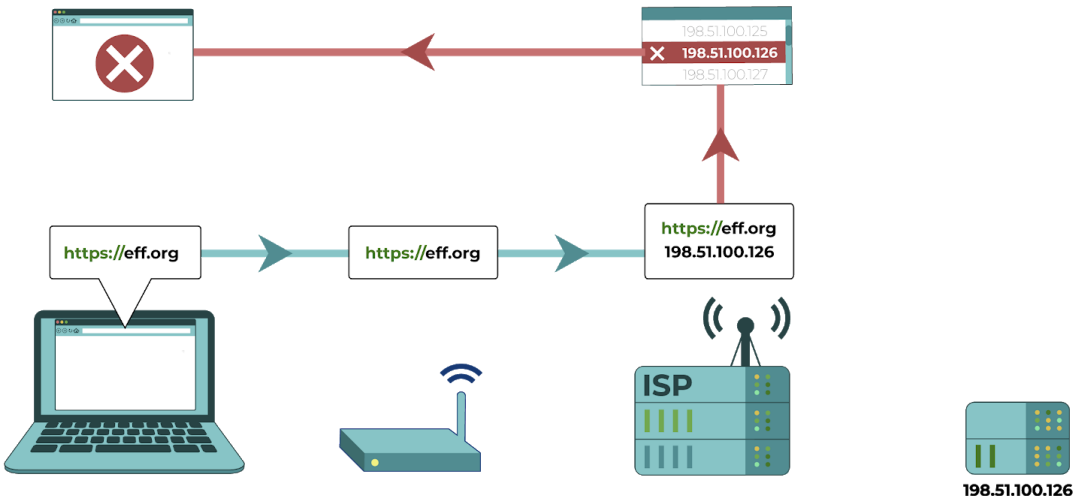
(2) Uchujaji wa mtandao kiambo. Hii ni kawaida sana shuleni na mahali pa kazi. Mtu anayesimamia mtandao kiambo (kama mtandao wa WiFi) huweka mipaka kwenye shughuli za kimtandao, kama vile ufuatiliaji au udhibiti wa unachokifanya mkondoni au unapotafuta maneno kadhaa.

(3) Uzuiaji au uchujaji. unaweza kwa ujumla kufanya aina sawa ya kuchuja kama msimamizi wa mtandao wako wa ndani. ISP katika nchi nyingi wanalazimishwa na serikali yao kufanya uchujaji wa kawaida wa mtandao na kudhibiti. ISP za kibiashara zinaweza kufanya uchujaji kama huduma kwa kaya au waajiri. Watoaji wa huduma za mtandao wa makazi wanaweza kuuza miunganisho iliyochujwa moja kwa moja kwa wateja kama chaguo, na watumie kiatomati njia maalum za kudhibiti (kama zile zilizoelezwa hapo chini) kwa unganisho zote kwenye ISP zao. Wanaweza kufanya hivyo hata ikiwa haihitajiki na serikali, kwa sababu baadhi ya wateja wao wanahitaji.

Ni jinsi gani kizuizi kinaweza kutokea?

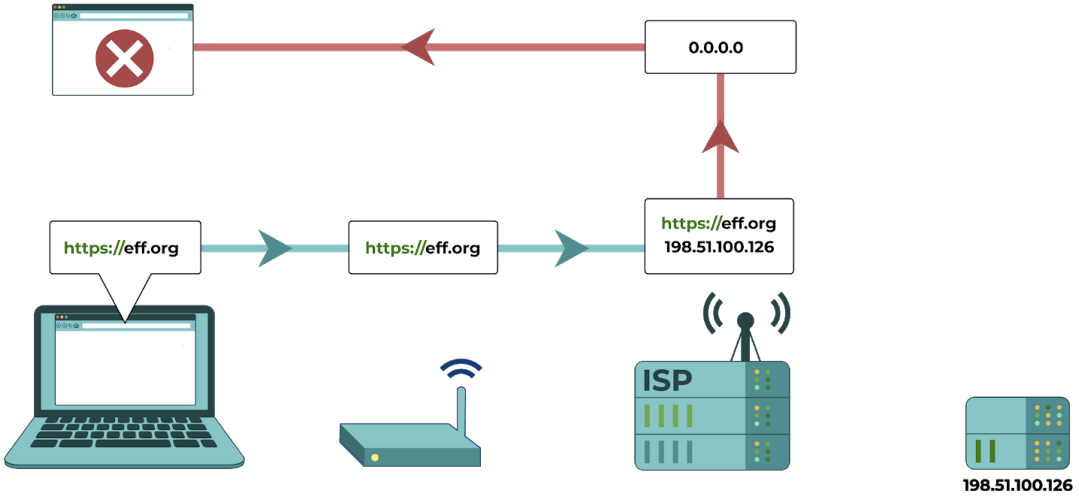
Uzuiaji wa anwani ya IP. “Anwani za IP” ni maeneo ya kompyuta kwenye mtandao. Kila kipande cha maelezo ambacho kimetumwa kwenye mtandao kina anuani itokapo na iendapo. Watoa huduma za mitandao na usimamizi wa mitandao wanaweza kutengeneza orodha ya maeneo yanayoendana na huduma unayotaka kuzuia. Kisha wanaweza kuzuia taharifa yoyote kwenye mtandao ambayo inapokelewa au kutoka kwenye maeneo hayo.

Hii inaweza kusababisha kuzuia zaidi, kwani huduma nyingi zinaweza kubebwa kwenye eneo moja au anwani moja. Vivyo hivyo watu wengi huishia kushirikiana anwani yoyote ile ya IP kufikia mtandao.



*Katika mchoro huu, mtoa huduma ya mtandao hukagua anwani ya IP aliyoombwa katika orodha ya anwani zilizozuiwa. Inaamua kua anwani ya eff.org inalingana na ile ya anwani ya IP iliyozuiwa na inazuia ombi kwa wavuti***.**

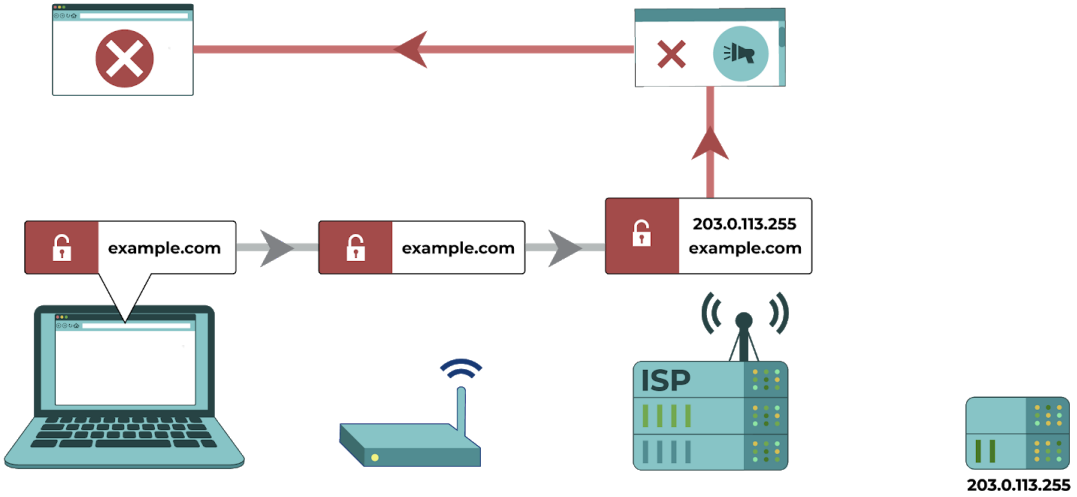
Uzuiaji wa DNS. Kifaa chako kinauliza kompyuta zinazoitwa “visuluhishi vya DNS” mahali tovuti zilizo. Unapounganisha kwenye mtandao, kitatuaji chaguo msingi cha DNS ambacho kifaa chako hutumia kawaida ni cha mtoa huduma wako wa mtandao. ISP inaweza kupanga suluhisho la DNS kutoa jibu lisiso sahihi au lisitoe jibu, wakati wowote mtumiaji atakapo jaribu kutafuta eneo la tovuti ama eneo lililozuiwa. Kama ukibadilisha kitatuzi chako cha DNS lakini hauna uhusiano na njia fiche, ISP yako bado inaweza kuchagua au kubadilisha majibu kwa huduma zilizozuiwa.



Katika Mchoro huu, ombi la anwani ya IP ya ya eff.org’s imebadilishwa katika huduma za mtandao. ISP inaingiliana na suluhisho la DNS , na anwani ya IP inaelekezwa tena ili kutoa lisilo sahihi ama kutotoa jibu kabisa.

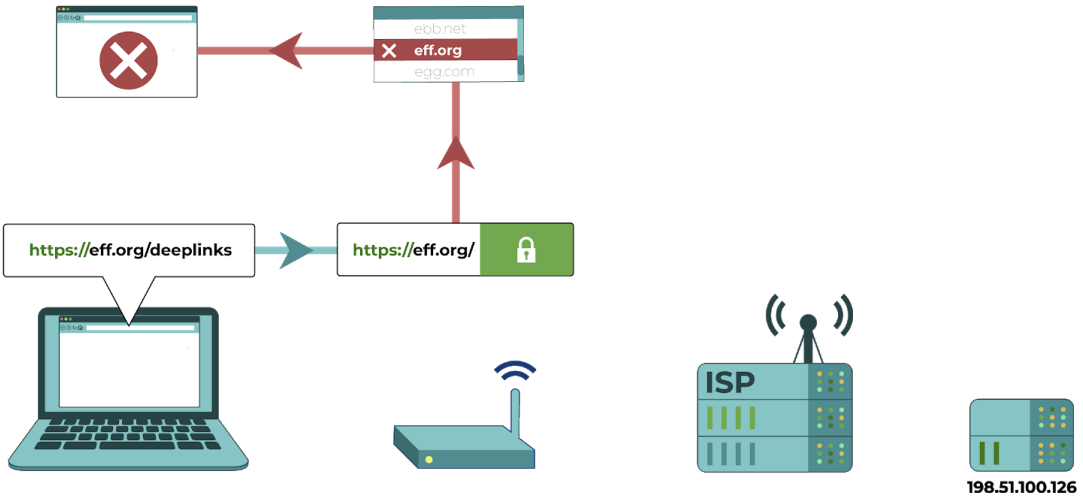
Kuchuja neno muhimu. Kama trafiki haijasimbwa kwa njia fiche, Watoa Huduma wa Mtandao wanaweza kuzuia ukurasa wa wavuti kwa yaliyomo. Pamoja na ongezeko la jumla la tovuti zinazosimbwa kwa njia fiche aina hii ya uchujaji inazidi kupungua umaarufu.

Tahadhari moja ni kwamba wasimamizi wanaweza kusimbua shughuli fiche ikiwa watumiaji watasakinisha “cheti cha CA” iliotolewa na wasimamzi wa kifaa chao. Kwa kuwa mtumiaji wa kifaa lazima asakinishe cheti, hii ni mazoea ya kawaida zaidi kwa mitandao ya ndani kwenye maeneo ya kazi na shule lakini chini ya kawaida katika ngazi ya ISP.



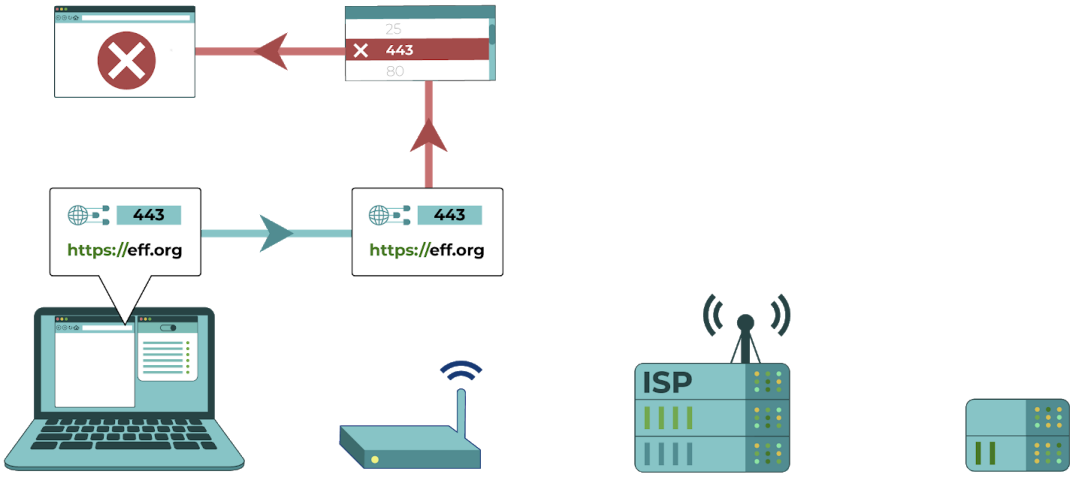
Kwenye unganisho la wavuti ambalo halijasimbwa Mtoa Huduma wa Mtandao (ISP) anaweza kuangalia faili ya yaliyomo kwenye wavuti dhidi ya aina zake za yaliyofungwa. Katika mfumo huu, hutaja mazungumzo ya bure kuongoza kwa kuzuia moja kwa moja kwenye wavuti.

Kuchuja HTTPS. Wakati wa kufikia tovuti juu ya HTTPS, yaliyomo yote yameandikwa kwa njia fiche isipokua jina la tovuti. Kwakua bado wanaweza kuona jina la tovuti watoa huduma za mtandao au wandani wasimamizi wa mtandao wanaweza kuamua ni tovuti gani za kuzuia ufikiaji.



Katika mchoro huu, kompyuta inajaribu kupata eff.org/deeplinks. Msimamamizi wa mtandao (anayewakilishwa na kipangishi njia) anauwezo wa kuona kikoa (eff.org) lakini sio anwani kamili baada ya kukata. Msimamazi wa mtandao anaweza kuamua ni vikao vipi vya kuzuia mfikiaji.

Itifaki na kuzuia bandari. Firewall au router inaweza kujaribu kutambua ni mtandao gani tecknolojia mtu anatumia kuwasiliana, na kuzia zingine kwa kutambua kiufundi maelezo ya jinsi wanavyowasiliana (itifaki na nambari za bandari ni mifano ya bahari ambayo inaweza kutumika kutambua ni tecknolojia gani inayotumiwa).ikiwa firewall inaweza kutambua kwa usahihi nini aina ya mawasiliano inafanyika au tecknolojia gani inatumiwa, inaweza kusaidiwa sio kupitisha mawasiliano hayo. Kwa mfano, mitandao mingine inaweza kuzuia tecknolojia zinazotumiwa na VoIP fulani (simu ya mtandao) au matumizi ya VPN.



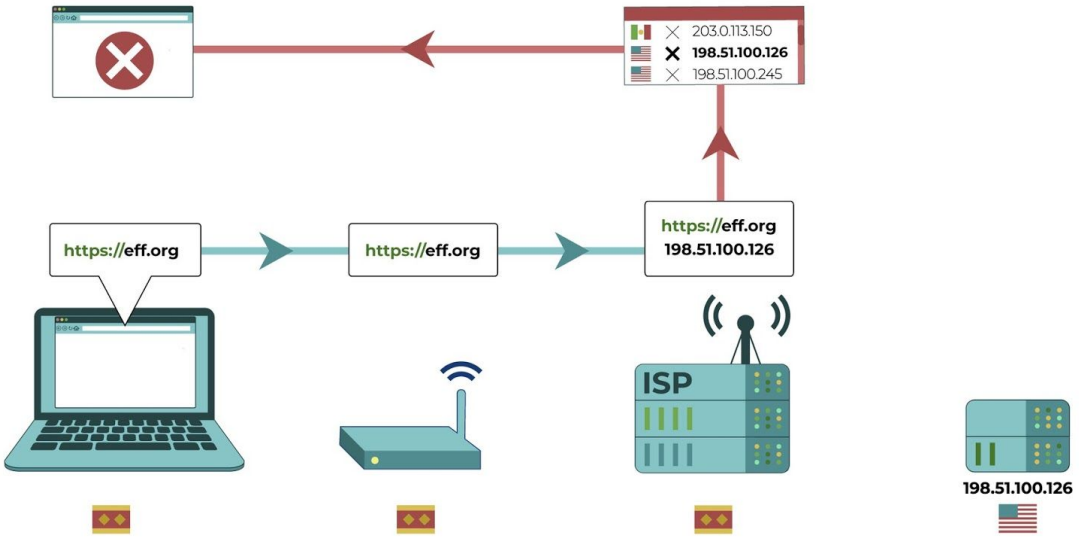
Katika mchoro huu, router inatambua kompyuta inayojaribu kuungana na tovuti ya HTTPS, ambayo inatumia kituo tarishi 443. Kituo tarishi 443 ipo kwenye orodha ya router hii ya itifaki zilizozuiwa.

Aina zingine za uzuiaji

Kwa kawaida, uzuiaji na uchujaji hutumiwa kuwazuia watu dhidi ya kufikia tovuti au huduma mahsusi. Hata hivyo, aina tofautiz za uzuiaji zinakuwa maarufu pia.

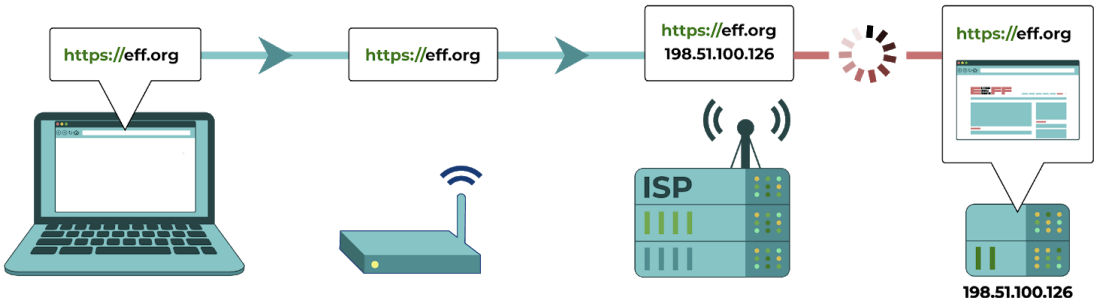
Kusimwa kwa mtandao. Kuzimwa kwa mtandao kunaweza pia kuhusisha kuondoa miundombinu ya mitandao, kama mkongo wa mawasilianomkongo wa mawasiliano, nyaya za mtandao, au minara ya mitandao ya simu, ili unganisho lizuiwe ana kwa ana au inakua mbaya sana kiasi kwamba haiwezi kutumiwa.

Hii inaweza kuwa kesi maalum ya kuzuia anwani ya IP, ambayo anwani zote za IP au nyingi zimezuiwa. Kwa sababu mara nyingi inawezekana kusema ni anwani gani ya IP inatumiwa, nchi zingine pia zimejaribu kuzuia kwa muda anwani zote za IP au za kigeni, ikiruhusu unganisho fulani ndani ya nchi lakini izuie uhusiano mwingi unaokwenda nje ya nchi**.**



Kompyuta inajaribu kuungana na anwani ya IP ya Amerika ya eff.org. Katika kiwango cha Mtoa Huduma ya Mtandao, ombi hukaguliwa: anwani ya IP ya eff.org inachunguzwa dhidi ya orodha ya anwani za IP za kimataifa zilizozuiwa, na inafungwa.

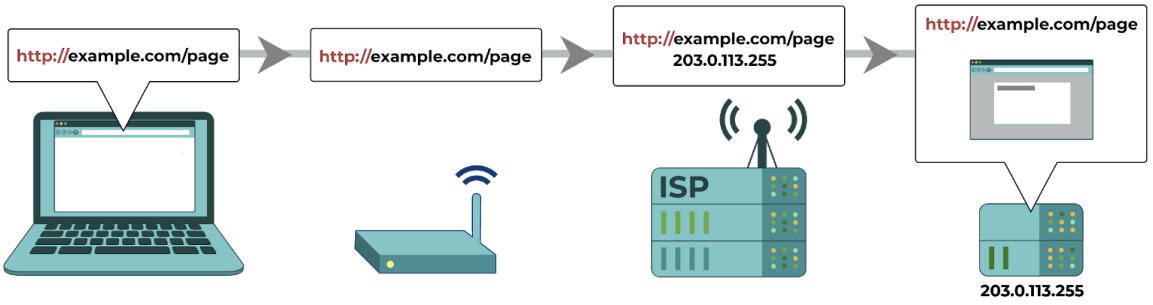
Kizuizi Mtandao. Watoaji wa Huduma za Mtandao wanaweza kuchagua, au kupunguza kasi, aina tofauti za usafirishajiusafirishaji wa kimitandao. Wachunguzi wengi wa serikali wameanza kupunguza uunganisho kwenye wavuti zingine badala ya kuzizuia kabisa. Aina hii ya kuzuia ni ngumu kutambua, na inaruhusu ISP kukana kwamba inazuia ufikiaji. Watu wanaweza kufikiria muunganisho wao wa mtandao ni wa polepole tu, au huduma ambayo wanaunganisha haifanyi kazi.



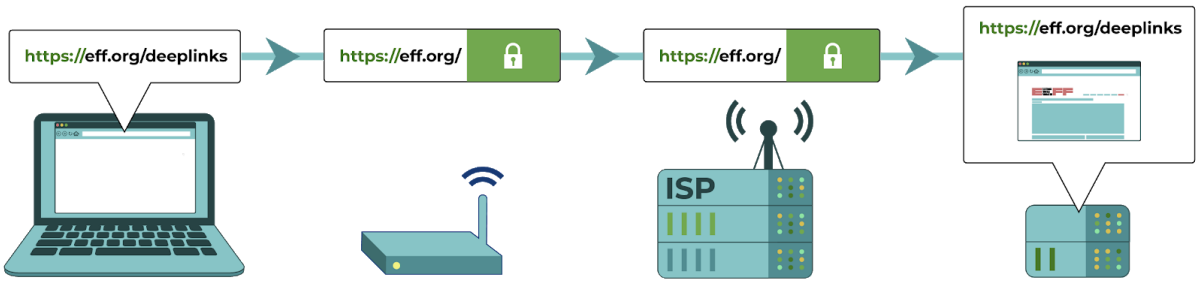
Kompyuta inajaribu kuungana na eff.org. Mtoa Huduma wao wa Mtandao hupunguza kasi ya muunganisho wao.

Mbinu za kuondoa vikwazo

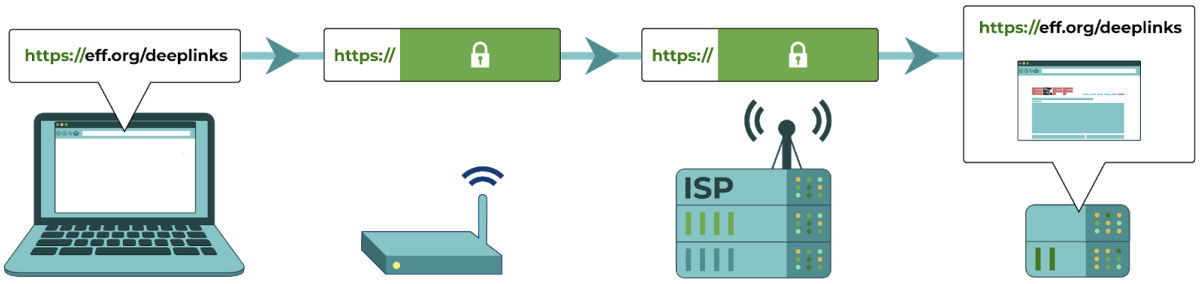
Kwa ujumla, ikiwa kuna habari ndogo juu ya shughuli zako za mtandao, inaweza kuwa ngumu kwa mtoa huduma wako wa mtandao au msimamizi wa mtandao kuzuia aina fulani za shughuli. Ndio sababu kutumia viwango vya usimbuaji pana vya mtandao vinaweza kusaidia.



HTTP inalinda kidogo taarifa zako za kuvinjari…



... HTTPS inalinda zaidi…



… DNS iliyosimbwa na itifaki zingine zitalinda jina la tovuti pia.

Kubadilisha mtoa huduma wako wa DNS na kutumia DNS iliyosimbwa kwa njia fiche

IIkiwa Watoa Huduma za Mtandao wanategemea tu **kuzuia DNS**, kubadilisha mtoa huduma wako wa DNS na kutumia DNS iliyosimbwa kwa fiche kunaweza kurudisha ufikiaji wako wa mtandao.

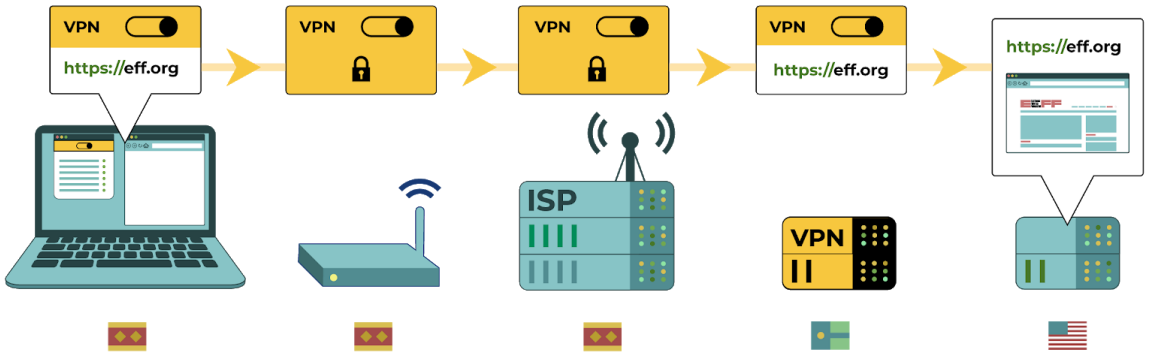
Kubadilisha mtoa huduma wako wa DNS. Hii inaweza kufanywa katika mipangilio ya mtandao ya kifaa chako (simu au kompyuta). Kumbuka kuwa mtoa huduma wako mpya wa DNS atapata habari kuhusu shughuli yako ya kuvinjari ambayo ISP yako ilikuwa nayo mara moja, ambayo inaweza kuleta wasiwasi wa faragha kulingana na mtindo wa vitisho. Mozilla

inakusanya orodha ya watoa huduma ya DNS ambapo wana sera na dhamira thabiti za kutosambaza data yako ya kuvinjari.

Kutumia DNS iliyosimbwa kwa njia fiche. Teknolojia zilizosimbwa za DNS zinaendelea kutolewa kwa sasa. Hii inazuia muigizaji yeyote wa mtandao kuona (na kuchuja) upelekaji wako wa DNS. Unaweza kutafuta DNS-over-HTTPS kwa urahisi kwenye Firefox na kutafuta DNS-over-TLS kwenye Android.

Hivi sasa, hakuna njia rahisi kwa watumiaji kufanya haya katika programu-tumizi zingine.

Kwa kutumia VPN au Proksi Iliyosimbwa



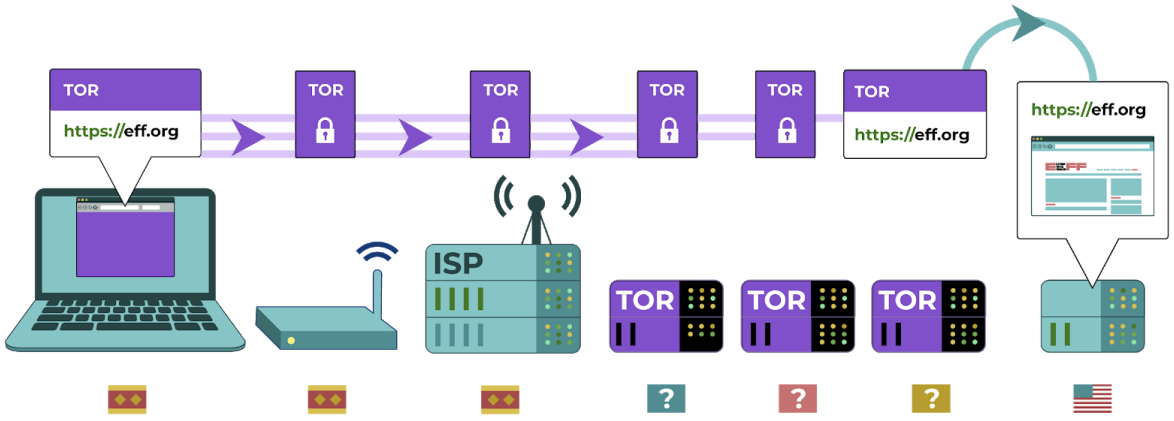
Katika mchoro huu, kompyuta hutumia VPN, ambayo inasimba trafiki yake na inaunganisha kwa eff.org. Router ya mtandao na mtoa huduma wa mtandao anaweza kuona kuwa kompyuta inatumia VPN, lakini data imesimbwa kwa njia fiche. Mtoa huduma wa mtandao huonyesha njia za unganisho kwenye seva ya VPN katika nchi zingine. VPN hii kisha inaunganisha kwenye tovuti ya eff.org.

Mtandao wa Kibinafsi wa Virtual (VPN) huandika na kutuma data zote za mtandao kutoka kwa kompyuta yako kupitia seva (kompyuta nyingine).Kompyuta hii inaweza kuwa ya huduma ya kibiashara au isiyo ya faida ya VPN, kampuni yako, au mwasiliani anayeaminika. Ikiwa huduma ya VPN imesanidiwa kwa usahihi, unaweza kuitumia kufikia kurasa za wavuti, barua pepe, ujumbe wa papo hapo, VoIP, na huduma yeyote ya kimtandao. VPN inalinda trafiki yako kutoka kwa kupelelezwa ndani, lakini mtoa huduma wako wa VPN bado anaweza kuweka rekodi (pia inajulikana kama logs) ya wavuti unazofikia, au hata amruhusu mtu mwingine aangalie moja kwa moja kwenye kuvinjari kwa wavuti yako. Kulingana na mtindo wako wa tishio, uwezekano wa serikali kusikiza uunganisho wako wa VPN au ufikiaji wa logs zako za VPN inaweza kuwa hatari kubwa. Kwa watumiaji wengine, hii inaweza kuzidi faida za muda mfupi za kutumia VPN.

Angalia mwongozo wetu kuhusu kuchagua huduma maalum za VPN.

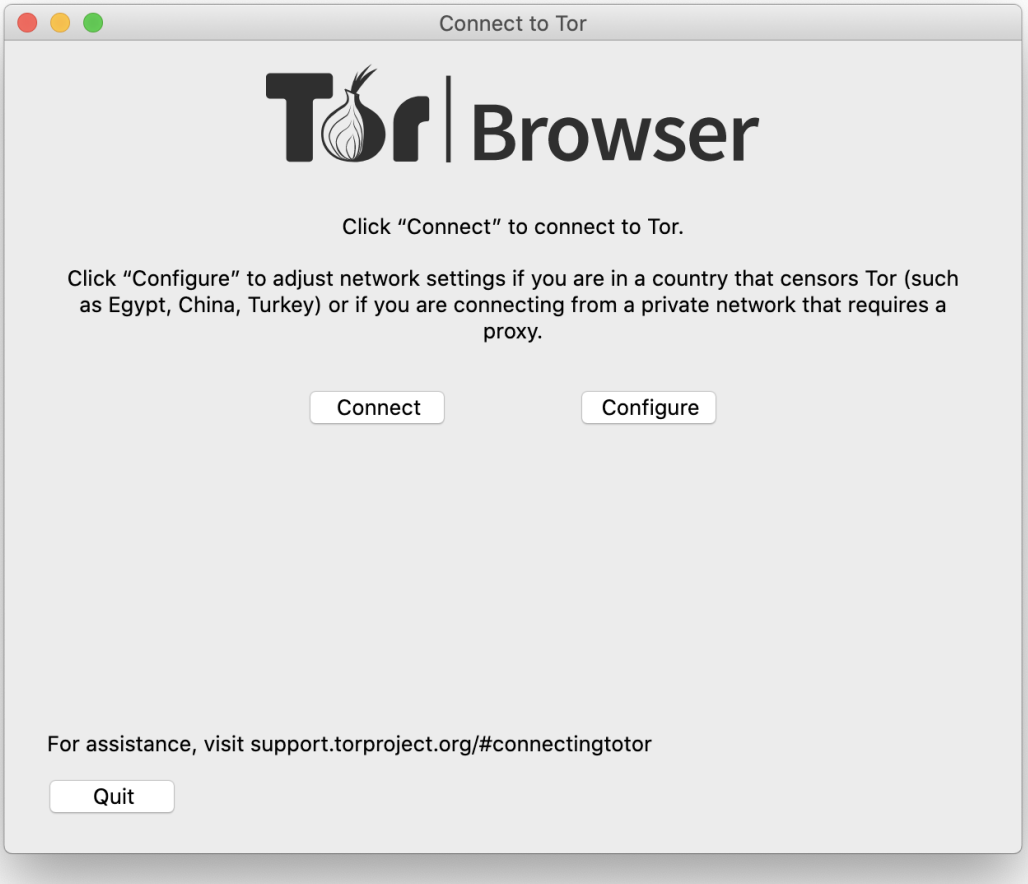
Jinsi ya kutumia kivinjari cha Tor

Tor anonTor ni programu ya chanzo-wazi iliyoundwa kukupa kutokujulikana kwenye wavuti. Kivinjari cha Tor ni kivinjari kilichojengwa juu ya mtandao rafiki. Kwa sababu ya jinsi Tor inavinjari trafiki yako ya kuvinjari wavuti, pia hukuruhusu kukwepa udhibiti. (Angalia jinsi ya: Kutumia mwongozo wa Tor kwa Linux, macOS, Windows na Android).



Kompyuta inatumia Tor kuunganisha eff.org. Tor ni njia ya uunganisho kupitia relay mbalimbali, ambazo zinaweza kuendeshwa na watu binafsi au mashirika duniani kote. Relay ya kutoka ya mwisho inaunganishwa kwa eff.org. ISP wanaweza kuona kuwa unatumia Tor lakini, haiwezi kuona kwa urahisi tovuti unayopitia. Mmliki wa eff.org, vivyo hivyo, anaweza kujua kuwa mtu anayetumia Tor ameunganishwa kwenye tovuti yake, lakini hawezi kujua mtumiaji anatokea wapi.

Unapoanza kutumia kivinjari cha Tor, unaweza kubainisha chaguo kuwa upo kwenye mtandao uliokaguliwa:



Tor haitapita tu udhibiti wa kitaifa, lakini, ikiwa imewekwa vizuri, inaweza pia kulinda kitambulisho chako kutoka kwa mpinzani anayesikiliza kutoka kwenye mtandao wa nchi yako. Japo kuwa inaweza ikawa polepole na ngumu kutumia, na mtu yoyote anayeweza kuona shughuli zako za kimtandao anaweza kugundua kuwa unatumia Tor.

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

Jifunze jinsi ya kutumia Tor kwenye Linux, macOS, Windows, na Android, lakini tafadhali hakikisha “Kusanidi” badala ya “Kuunganisha” kwenye window iliyozinzewa hapo juu.