Protokol WireGuard

Gašper Spagnolo

March 11, 2023

Contents

1 Uvod

Protokol WireGuard je sodoben in enostaven za uporabo protokol za izgradnjo varnih in zanesljivih virtualnih zasebnih omrežij (VPN). Omogoča hitro in učinkovito vzpostavitev VPN povezave, ki temelji na najnovejših kriptografskih algoritmih in prinaša številne prednosti v primerjavi s tradicionalnimi protokoli za VPN.

2 Kakšen je namen protokola wireguard, za kaj se uporablja, kdo so akterji, ki komunicirajo?

WireGuard je sodoben in varčen protokol virtualne zasebne mreže (VPN), ki zagotavlja varno povezavo med različnimi napravami preko interneta. Namen protokola WireGuard je nadomestiti obstoječe VPN protokole in ponuditi boljšo varnost, zanesljivost, hitrost in preprostost uporabe. WireGuard se uporablja za vzpostavitev varne povezave med različnimi napravami preko interneta, kot so računalniki, pametni telefoni, usmerjevalniki in strežniki. Ta povezava omogoča prenos podatkov med napravami na način, da so vsi podatki šifrirani in zavarovani pred prisluškovanjem, vdori in drugimi nevarnostmi. Akterji, ki komunicirajo preko WireGuard protokola, so uporabniki, ki želijo varno povezavo s svojimi napravami preko interneta. To so lahko posamezniki, podjetja, organizacije ali druge skupine, ki želijo vzpostaviti varno in zanesljivo povezavo med svojimi napravami. WireGuard protokol je odprtokodni in je na voljo za različne operacijske sisteme, kot so Linux, Windows, macOS, Android in iOS. Poleg tega je WireGuard zelo priljubljen med ponudniki VPN storitev, ki želijo ponuditi svojim uporabnikom visokokakovostno in varno storitev VPN. V primeru, ko uporabnik uporablja WireGuard VPN storitev, se namesto neposredne komunikacije med napravami, podatki najprej pošljejo do VPN strežnika, ki preusmeri podatke na ciljno napravo. S tem se izognemo neposredni povezavi in lahko zagotovimo dodatno varnost in anonimnost med komunikacijo.

V kontekstu protokola WireGuard, je pomembno, da dodamo DNS resolver serverje v konfiguracijo vsakega klienta, da zagotovimo zasebnost in varnost DNS poizvedb. Če tega ne storimo, se bodo DNS poizvedbe, ki jih uporablja klient, poslale prek standardnega DNS strežnika vašega ponudnika internetnih storitev (ISP). To pomeni, da bodo vsi vaši DNS poizvedbe razumljive v obliki besedila, kar pa lahko ogrozi vašo zasebnost. S povezavo preko VPN-ja, kot je WireGuard, se vsi podatki med klientom in strežnikom šifrirajo. Vendar pa to ne vključuje tudi DNS poizvedb. Če ne dodamo ločenega DNS resolverskega strežnika v konfiguracijo, se bodo DNS poizvedbe še vedno poslale neposredno prek standardnega DNS strežnika vašega ISP-ja, kar pomeni, da bo vaš ISP lahko videl, katere spletne strani obiščete. Z dodajanjem DNS resolver strežnika v konfiguracijo WireGuard klienta pa se zagotovi, da bodo vsi DNS poizvedbe uporabnika šifrirane in poslane prek VPN povezave. To zagotavlja, da nihče ne more prestreči vaših DNS poizvedb in ugotoviti, katere spletne strani obiskujete.

3 Tipičen primer uporabe protokola wireuard

Tipičen primer uporabe protokola WireGuard je vzpostavitev varne in zasebne VPN povezave med oddaljenimi napravami. Recimo, da želite vzpostaviti VPN povezavo med dvema oddaljenima lokacijama, kot sta pisarna in domači računalnik. V tem primeru bi lahko uporabili protokol WireGuard za ustvarjanje varne VPN povezave med tema dvema lokacijama. Prvi korak bi bil, da na obeh lokacijah namestite WireGuard strežnik in ustvarite konfiguracijsko datoteko za vsakega klienta (računalnik ali mobilna naprava), ki se bo povezoval s tem strežnikom. Vsakemu klientu bi dodelili enoličen ključ, ki bi ga uporabljali za šifriranje in dešifriranje prometa. Nato bi izmenjali konfiguracijske datoteke med strežnikom in klienti, tako da bi vsak klient imel konfiguracijsko datoteko za povezavo z WireGuard strežnikom na drugi lokaciji. Ko bi bile konfiguracijske datoteke uvožene, bi se lahko klienti povezali s strežnikom in začeli uporabljati VPN povezavo. Vsa komunikacija med klientom in strežnikom bi bila šifrirana in varna, kar bi omogočilo varno in zasebno deljenje občutljivih podatkov prek interneta. Uporaba WireGuarda v primeru VPN povezave zagotavlja boljšo zmogljivost in zmanjšuje zamude, saj je protokol zasnovan za uporabo v modernih omrežjih z visoko zmogljivostjo. Poleg tega je WireGuard tudi preprost za uporabo in nastavitev, zato je priljubljen med uporabniki, ki želijo enostavno in učinkovito VPN rešitev.

4 Scenarij komunikacije protokola wireguard

Tipičen Scenarij komunikacije protokola WireGuard bi se lahko odvijal na naslednji način:

1. **Vzpostavitev povezave**: Ko se uporabnik poveže z VPN strežnikom preko protokola WireGuard, uporabnikova naprava pošlje zahtevo za vzpostavitev povezave na strežnik
2. **Avtentikacija**: VPN strežnik preveri identiteto uporabnika, tako da preveri uporabnikov ključ.
3. **Izmenjava ključev**: VPN strežnik in uporabnik si izmenjata javne ključe, ki jih bosta uporabljala za šifriranje in dešifriranje prometa.
4. **Šifriranje prometa**: Ko se VPN povezava vzpostavi, vsi podatki, ki jih uporabnik pošilja preko VPN, se šifrirajo in pošiljajo preko protokola WireGuard. To zagotavlja, da so vsi podatki, ki potujejo med uporabnikovo napravo in VPN strežnikom, šifrirani in varni.
5. **Dekodiranje prometa**: VPN strežnik dekodira promet, ki ga prejme preko protokola WireGuard, in ga pošlje naprej do končne destinacije (npr. spletnega strežnika).
6. **Odgovor**: Ko se prejme odgovor od spletnega strežnika, VPN strežnik kodira odgovor in ga pošlje nazaj do uporabnika preko protokola WireGuard
7. **Rušenje povezave**: Ko uporabnik zaključi povezavo, se vsi ključi in seje, ki so bili uporabljeni med povezavo, izbrišejo.

5 Kratek opis specifikacije (RFC)

RFC specifikacija za protokol WireGuard še ni bila objavljena. Čeprav je protokol že dolgoletno uporabljen in široko sprejet v IT skupnosti, je bil proces standardizacije šele nedavno začet. Trenutno je na voljo precej tehnične dokumentacije, na primer spletna stran WireGuarda vsebuje specifikacije protokola in celoten kodek za WireGuard VPN. Prav tako pa obstajajo priročniki in navodila za uporabo WireGuarda v različnih operacijskih sistemih.

6 Format pomembnejših sporočil

Pri protokolu WireGuard se uporabljajo različna sporočila za vzpostavitev varne VPN povezave med strežnikom in klientom. Sporočila so oblikovana v enostavni binarni obliki, da se izboljša učinkovitost in hitrost prenosa podatkov. Nekatera pomembnejša sporočila, ki se uporabljajo pri protokolu WireGuard, so:

1. **Handshake Initiation Message**: To sporočilo se pošlje med strankama, ko se želita povezati. Vsebuje informacije, kot so javni ključ in IP naslov stranke.
2. **Handshake Response Message**: Ta sporočilo se pošlje kot odgovor na sporočilo *Handshake Initiation*. Vsebuje javni ključ in IP naslov strežnika.
3. **Data Message**: To sporočilo se uporablja za prenos podatkov preko VPN povezave. Vsebuje šifrirane podatke, ki jih je mogoče dešifrirati le s pomočjo ključa, ki je bil izmenjan med *Handshake Initiation* in *Handshake Response*.
4. **Keepalive Message**: Ta sporočilo se pošlje periodično med strankama, da se prepreči prekinitev povezave zaradi neaktivnosti.

Keepalive sporočila pri protokolu WireGuard so namenjena ohranjanju aktivne VPN povezave med strankama, ki se povezujeta preko protokola. Ker protokol WireGuard deluje na osnovi UDP (User Datagram Protocol), ki je protokol brez povezave, ne obstaja prava povezava med klientom in strežnikom, tako kot pri protokolu TCP. To pomeni, da se ne more uporabiti mehanizma, ki ga uporablja TCP, da bi preverjal, ali je povezava še vedno aktivna. Zato se pri protokolu WireGuard uporabljajo keepalive sporočila, ki se pošiljajo redno med strankama, da se prepreči prekinitev povezave zaradi neaktivnosti. To sporočilo vsebuje poseben paket, ki se pošlje preko VPN povezave, da se ohrani aktivnost povezave. Če katera od strank ne prejme keepalive sporočila v določenem času, se šteje, da je povezava prekinjena. Keepalive sporočila so zelo koristna, saj omogočajo ohranjanje aktivne VPN povezave brez prekinitev in posledično izboljšajo delovanje protokola. Hkrati pa ne porabljajo veliko pasovne širine, saj so sporočila zelo majhna in se pošiljajo le periodično.

7 Zakjlucek

Protokol WireGuard ima številne prednosti, ki ga naredijo odlično izbiro za vzpostavitev varne in zanesljive VPN povezave. Med njegovimi glavnimi prednostmi so:

- **Hitrost**: WireGuard je izjemno hiter protokol, ki je v primerjavi z drugimi VPN protokoli lahko tudi do desetkrat hitrejši.
- **Enostavnost uporabe**: WireGuard je izjemno enostaven za uporabo, saj ne zahteva veliko konfiguracije in je lahko nameščen na različne platforme, vključno z mobilnimi napravami.
- **Zanesljivost**: WireGuard je zasnovan tako, da zagotavlja zanesljivo povezavo, ki se samodejno obnavlja ob izgubi povezave.
- **Varnost**: WireGuard uporablja najnovejše in najbolj varne kriptografske algoritme, ki zagotavljajo visoko stopnjo varnosti in zasebnosti.
- **Prilagodljivost**: WireGuard omogoča povezovanje več točk v virtualno zasebno omrežje, kar omogoča fleksibilnost pri načrtovanju in upravljanju VPN povezav.

Zaradi teh prednosti se WireGuard pogosto uporablja za zagotavljanje varnih in hitrih VPN povezav v različnih okoljih, od osebne uporabe do poslovnih omrežij. Prav gotovo, lahko napišem, da je WireGuard super protokol, ki ga tudi sam uporabljam za dostop do lokalne mreže in se mi zdi odličen. Deluje hitro in zanesljivo, tudi preklop med mobilnimi podatki in WiFi-jem deluje brez težav in brez prekinitev povezave. Poleg tega sem zelo zadovoljen s preprostostjo uporabe in enostavno konfiguracijo, kar omogoča, da lahko hitro in enostavno vzpostavim varno VPN povezavo kadarkoli in kjerkoli.