**Proxy sau VPN: Care instrument de securitate este mai bun?**

**Ce este un VPN?**

[**VPN-ul**](https://ro.wizcase.com/blog/ghid-complet-despre-vpn-uri-pentru-incepatori/)**, sau o Rețeaua Privată Virtuală va redirecționa activitatea voastră online de pe serverele ISP-ului către un server la distanță.**După ce vă conectați la serverul la distanță**, veți primi o nouă adresă de IP în funcție locul în care este găzduit serverul, indiferent de locația voastră reală.**

Există sute de VPN-uri dintre care puteți să alegeți, unele dintre ele gratuite iar altele necesită un abonament. Singurul lucru pe care îl au în comun este acela că **trebuie să descărcați software-ul pentru a le utiliza. După conectare, acestea vor redirecționa tot traficul, nu doar anumite aplicații prin tunelul securizat**. Trebuie să menționăm că există unele VPN-uri care oferă **„tunelare divizată”**, ceea ce permite ca o parte din trafic să treacă prin ISP, în timp ce numai anumite aplicații ajung la serverele VPN-ului.

Cu toate acestea, funcția aceasta nu vine în mod implicit și depinde de voi să decideți când și dacă doriți să o activați. **Datele care ies din dispozitiv sunt criptate**, astfel încât toate informațiile de navigare și **datele private sunt păstrate în siguranță**, părând că utilizați o **rețea privată** și nu adresa de IP și locația voastră.

Utilizarea unui VPN oferă **avantaje grozave** atunci când se ia în considerare **securitatea**, deoarece acesta reduce șansele ca activitatea voastră din mediul online să fie urmărită, **parolele și alte informații sensibile să fie furate sau să fiți expuși la diverse alte amenințări.**

**VPN-ul răspunde nevoile voastre?**



**Un VPN bun vă va permite să navigați în siguranță și anonimitate pe internet** de pe orice conexiune privată sau publică. De asemenea, **VPN-urile oferă măsuri suplimentare de securitate și criptare pentru a vă proteja informațiile** atunci când navigați pe Wi-Fi.

Chiar dacă un hacker încearcă să obțină acces la informațiile voastre, **criptarea va asigura că datele sunt inutilizabile**. **Dacă sunteți în căutare de securitate online și confidențialitate**, **veți avea nevoie de un VPN cu criptare robustă și o serie de protocoale de securitate** precum OpenVPN și SSTP.

Un alt avantaj**al criptării datelor este acela că ISP-ul (furnizorul de servicii de internet) nu poate vedea ce faceți online**.

Acest lucru este benefic din mai multe motive.

1. **ISP-urile sunt cunoscute pentru limitările de viteză** pe care le instituie utilizatorilor pe site-urile cu consum de date intensiv
2. **Anonimizează activitatea online**.
3. Puteți să face **torrenting fără frica** divulgării informațiilor voastre către autorități

Nu toate VPN-urile sunt la fel, unele sunt mai bune decât altele atunci când vine vorba despre anumite nevoi**.**

Asta nu înseamnă că totul este perfect la VPN-uri. Ca orice altceva, are unele dezavantaje.

*Un exemplu bun este prețul acestora.*

Dacă doriți un VPN fiabil și securizat care poate face ceea ce aveți nevoie, va trebui să plătiți pentru acesta. Majoritatea VPN-urilor oferă o**reducere a prețului**dacă achiziționați un abonament mai lung de o lună. De asemenea, puteți găsi [**cupoane de VPN-uri**](https://www.wizcase.com/blog/best-vpn-coupons/) tot anul, care vă pot economisi sume importante.

**Ce este un Proxy?**

Proxy-ul este un **instrument de confidențialitate** care vă poate **ascunde adresa de IP** pentru a face să pară că vă aflați într-o altă locație. Spre deosebire de VPN-uri, nu există niciun program pe care trebuie să îl descărcați, ci vă conectați doar pentru o anumită aplicație, nu pentru întreaga rețea.

Atunci când utilizați un proxy cu browser-ul de internet, puteți seta ca Internetul să meargă mai întâi la servere independente, permițând ascunderea adresei de IP. Acest lucru vă oferă **anonimat în timpul navigării sau al streaming-ului pe internet.** De asemenea, acesta vă maschează locația, deci dacă doriți să accesați site-uri care sunt blocate în țara de origine, proxy-ul este un mod de a ocoli restricțiile. Cu toate acestea,**nu există măsuri de securitate online precum criptarea protocoalelor de securitate** ca de exemplu OpenVPN.

Utilizarea principală a unui proxy este aceea de a **evita filtrele** precum restricțiile de locație geografică sau restricțiile anumitor site-uri de către școli, biblioteci sau universități. De exemplu, dacă o bibliotecă blochează accesul la un site de social-media, puteți utiliza un proxy pentru a-l accesa.

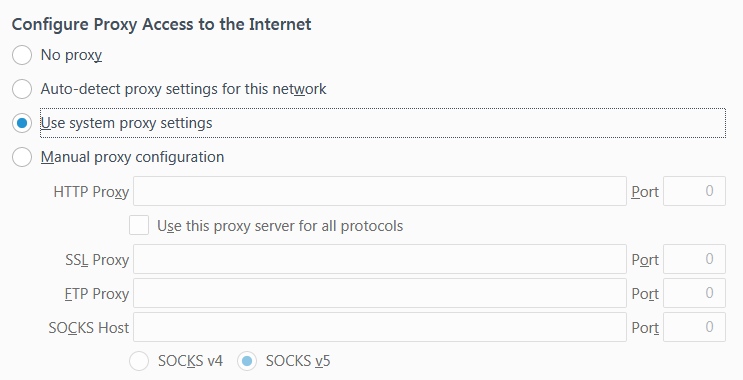
Există mai multe tipuri de proxy-uri. Cele mai frecvente sunt:

1. **Proxy anonim**  
   Este proxy-ul standard, disponibil gratuit pe internet. **Acesta vă ascunde adresa de IP și vă va permite să ocoliți cookie-urile și campaniile de remarketing**. Cu toate acestea, nu ascunde și faptul că adresa voastră de IP este conectată la un proxy. Există dezavantaje semnificative cu acest tip de proxy, printre care și riscurile de securitate și vitezele foarte scăzute.
2. **Proxy de mare anonimitate**  
   Aceasta vă ascunde adresa de IP, **dar și faptul că utilizați un proxy**. Șansele de accesare a conținuturilor geo-restricționate sunt mai mari atunci când se utilizează opțiunea de anonimat ridicat.
3. **Server SOCKS5**  
   Acest server proxy este de **nivel superior celor anonime și cu anonimitate ridicată**, datorită modului în care vă gestionează traficul online. **Poate fi folosit atunci când călătoriți în China și pentru torrenting anonim. Spre deosebire de alte proxy-uri, nu este gratuit**.

**Proxy-ul poate răspunde nevoilor voastre?**

Proxy-ul vă oferă **protecție de bază** atunci când vine vorba de intimitate. Datorită faptului că toate datele de pe internet sunt trimise mai întâi la un server proxy și apoi la site-ul dorit, puteți să vă păstrați adresa de IP și locația ascunse deoarece site-ul va vedea numai adresa serverului proxy. Acest lucru vă oferă **protecție împotriva supravegherii externe**, dar trebuie să aveți în vedere faptul că proprietarul serverului proxy poate accesa datele voastre și, de obicei va înregistra log-uri.

De asemenea, proxy-ul ajută la limitarea cantității de reclame pe care le veți vedea deoarece adresa de IP este ascunsă. Dacă sunteți interesați de reclame, trebuie să vă asigurați că selectați proxy-ul corect deoarece **unele își plasează propriile reclame pe site-urile pe care le vizitați, blocându-le pe altele sau înlocuindu-le**.



Serverul de proxy selectat este setat din browser-ul de internet pe care îl utilizați și**nu are nevoie de descărcarea unui software**, ceea ce simplifică și ușurează configurarea. Deoarece nu aveți nevoie de descărcări de software,**spațiul hard disk-ului nu este afectat**. Cu toate acestea, este afectată viteza internetului deoarece există un pas suplimentar la fiecare solicitare pe măsură ce trece prin serverul proxy.

În funcție de locația serverului proxy, **anumite conținuturi vor fi restricționate iar altele nu.** Dacă nu puteți vedea un site din Anglia, dar serverul proxy se află în Australia, este posibil să aveți acces la acesta. Acest lucru poate fi benefic pentru unii utilizatori, dar poate fi și frustrant dacă trebuie să accesați site-uri din diferite regiuni. Prin urmare, probabil va trebui să **resetați setările de fiecare dată** când aveți nevoie să accesați un site geo-restricționat, pentru a putea accesa un server potrivit.

Utilizarea proxy-ului este o opțiune simplă și ușoară de securitate pentru utilizatorii care caută o soluție temporară în funcție de locația lor sau dacă folosesc un sistem restricționat. Atunci când utilizați un proxy, este vital să găsiți un server legal și de încredere. Trebuie să rețineți că deși primiți anonimatul dorit, proprietarul serverului de proxy este un necunoscut. În plus, deoarece **proxy-urile sunt de obicei gratuite**, acestora **le lipsește securitatea, iar** **confidențialitatea și anonimatul pot să aibă de suferit.**

**VPN vs. proxy: răspunsul ar trebui să fie evident**

Această bătălie seamănă cu lupta dintre David și Goliat, dacă Goliat câștigă cu mâinile la spate.

**VPN-ul îndeplinește toate funcțiile unui proxy,** dar are și multe alte funcționalități care oferă mai multă **siguranță, securitate și robustețe.**Dacă sunteți în căutarea unei soluții pe termen lung de protejare a datelor și pentru securitate,**un VPN este cea mai bună alegere**.

Singura situație când un proxy poate fi o alegere mai bună decât un VPN este dacă trebuie să ocoliți rapid un firewall. De exemplu, dacă sunteți la serviciu sau la școală și doriți să vă verificați contul Facebook, dar firewall-ul blochează site-urile de social-media, un proxy este de ajuns.

Dacă vă uitați la un proxy plătit precum unul de tip **SOCKS5**, veți cheltui aceeași sumă de bani sau chiar mai mult decât pe un VPN și veți obține doar o parte din beneficii.