

Co je proxy server

Poslední aktualizace 21 února, 2025

Proxy server přeposílá požadavky uživatele na webové stránky nebo jiné internetové služby a následně doručuje odpovědi zpět k uživateli.

Funguje jako prostředník mezi klientem (například vaším počítačem) a cílovým [serverem](#), což má hned několik výhod:

1. **Anonymizace:** Proxy umí skrýt [IP adresu](#). Cílový server uvidí pouze IP adresu proxy serveru, nikoliv vaši skutečnou adresu.
2. **Bezpečnost:** Proxy servery mohou filtrovat a blokovat nebezpečné stránky nebo obsah, a chránit vás tak před malwarem a napadením, nebo šifrovat přenos dat.
3. **Zrychlení přenosu dat:** Proxy servery umí [cachovat](#) často navštěvované stránky.
4. **Správa přístupu a filtrování obsahu:** Proxy se využívá i k blokování konkrétních webů, omezení přístupu na základě nastavených pravidel nebo sledování internetového provozu, což se uplatňuje například ve školách nebo firmách.

Kdy se proxy servery nejčastěji používají?

- K řízení přístupu zaměstnanců na internet, filtrování nevhodného obsahu nebo zvýšení bezpečnosti sítě.
- K omezení přístupu studentů na konkrétní webové stránky a kontrole používání internetu.
- Pro ukládání do cache a zrychlení načítání stránek, případně ke kontrole provozu.
- Pro zvýšení anonymity a přístup na stránky s geografickým omezením nebo pro bezpečnější prohlížení.

Typy proxy serverů

Proxy servery se dělí na 5 základních typů podle výše zmíněného použití:

- **Forward proxy** řeší na odchozí data. Používá se pro blokování nevhodného obsahu, sledování síťové aktivity, nebo pro anonymizaci IP adres uživatelů.
- **Reverse proxy** kontroluje příchozí data. Slouží k vyvažování zátěže (load balancing), zlepšení bezpečnosti (skrytí interních serverů), a také ke [cachování](#) obsahu, což zrychluje načítání stránek.
- **Transparent proxy** se používá v síťových prostředích, jako jsou školy nebo

veřejné [Wi-Fi](#), kde administrátoři chtějí monitorovat nebo filtrovat provoz bez zásahu uživatelů.

- **Web proxy** je dobrá pro anonymizaci prohlížení a přístupu na určité weby. Umožňuje obcházet regionální omezení nebo firemní blokace některých webů (podobně jako [VPN](#)).
- **SOCKS proxy** je ideální pro aplikace vyžadující širší spektrum přenosů dat, jako jsou torrenty, herní aplikace nebo některé typy zabezpečené komunikace.

Jak si proxy server zřídit?

Řada různých nástrojů poskytuje proxy jako doplňkovou službu (například poskytovatelé [VPN](#) nebo další bezpečnostní programy).

Je také důležitou součástí webhostingů a serverových služeb (kde se zřizuje pomocí softwarů jako [Apache HTTP](#), [HAProxy](#) nebo [Nginx](#)).

Samostatný proxy server si pak můžete pořídit od společností, jako je [Proxy Seller](#) nebo [Oxylabs](#).

Jak se využívá proxy u webhostingu

Proxy servery jsou pro webhosting klíčové k řízení provozu, zabezpečení serverů a zajištění rychlého načítání a vysoké dostupnosti hostovaných webů.

Webhostingové společnosti využívají zejména reverse proxy servery, a to pro

- **cachování** webového obsahu (u [Endora](#) například můžete zdarma využít speciální službu [Endora Cache](#))
- **load balancing**, tzn. dělení příchozích požadavků mezi více serverů, což zajistí, že žádný server nebude přetížen
- **zabezpečení**, např. před [DDoS útoky](#), opět pomocí load balancingu, blokace podezřelého provozu a skrývání IP adres
- **HTTPs šifrování** pomocí [SSL](#), což ulehčí hlavním serverům a zvyšuje efektivitu zabezpečení
- zajištění geografické dostupnosti pro rychlejší načítání obsahu pro uživatele z různých zemí ([CDN](#))