

..

Zabezpečení sítě a NAT (Překlad síťových adres)

V dobách počátků internetu se předpokládalo, že každé připojené zařízení bude mít svou vlastní veřejnou IP adresu a bude s ostatními komunikovat napřímo. S masivním nárůstem počtu počítačů, smartphonů a IoT zařízení však nastal akutní nedostatek adres IPv4.

Jako dočasné řešení byla zavedena technologie **NAT**, která měla primárně šetřit IP adresy. Postupem času se však stala jedním ze základních (byť často nepochopených) pilířů zabezpečení domácích i firemních sítí.

Co je to NAT a jak funguje?

NAT (*Network Address Translation* – Překlad síťových adres) je mechanismus, který běží na tvém routeru nebo firewallu. Umožňuje, aby celá lokální síť (LAN) vystupovala do vnějšího internetu pod **jedinou společnou veřejnou IP adresou**.

Když zařízení z vnitřní sítě (např. s privátní IP adresou `192.168.1.50`) pošle požadavek na webovou stránku v internetu:

1. Router vezme tento datový paket a přepíše zdrojovou privátní IP adresu na svou vlastní ****veřejnou IP adresu****.
2. Aby router věděl, komu má pak vrátit odpověď, přiřadí tomuto spojení unikátní číslo portu (tato specifická verze NATu se nazývá ****PAT**** – //Port Address Translation//).
3. Jakmile dorazí odpověď z internetu, router se podívá do své překladové tabulky (NAT table), přepíše adresu zpět na privátní adresu počítače a data mu doručí.

Bezpečnostní aspekt NATu: Mýtus vs. Realita

Mezi uživateli i správci sítí často panuje představa, že NAT funguje jako plnohodnotný firewall. To je pravda jen částečně.

Proč NAT zvyšuje bezpečnost (Mýtus o firewallu)

Hlavní bezpečnostní přínos NATu spočívá v **obousměrnosti spojení**. Z principu své funkce NAT propustí do vnitřní sítě pouze ty pakety, které jsou **přímou odpovědí** na požadavek, jenž vyšel zevnitř sítě.

Pokud se útočník z internetu pokusí naskenovat nebo napadnout zařízení uvnitř sítě (např. tvůj chytrý

termostat), narazí na router. Router se podívá do své NAT tabulky, zjistí, že žádné vnitřní zařízení o komunikaci s tímto útočníkem nežádalo, a paket jednoduše **zahodí**. Vnitřní síť je tak pro vnější svět neviditelná (skrytá).

Proč samotný NAT nestačí (Realita)

NAT **není** stavový firewall (Stateful Firewall).

- NAT nekontroluje, zda je obsah paketu bezpečný. Pokud uživatel uvnitř sítě klikne na podvodný odkaz nebo si stáhne malware, NAT tomuto škodlivému spojení poslušně otevře cestu ven i dovnitř.
- NAT nechrání síť před útoky, které přicházejí zevnitř (např. infikovaný notebook připojený k domácí Wi-Fi může napadnout ostatní zařízení v LAN).

Proto musí být NAT vždy kombinován se skutečným **firewallem**, který analyzuje samotný provoz a filtruje ho na základě pokročilých bezpečnostních pravidel.

Komplikace, které NAT přináší

Ačkoliv NAT pomohl zachránit IPv4 a přidal vrstvu anonymity, pro moderní síťovou komunikaci představuje obrovskou komplikaci:

- **Problém s P2P a VoIP:** Služby jako online hry, IP telefonie (VoIP) nebo videohovory potřebují, aby se dvě zařízení v internetu spojila napřímo. NAT to komplikuje, protože ani jedno zařízení nemá veřejnou IP adresu.
- **Nutnost Port Forwardingu:** Pokud chceš mít doma spuštěný vlastní webový server, NAS úložiště nebo IP kameru přístupnou zvenčí, musíš na routeru nastavit tzv. **přesměrování portů** (Port Forwarding). Tím útočníkům otevřeš permanentní díru do sítě.
- **Ztráta dohledatelnosti (Traceability):** Pokud z jedné firmy odchází veškerý provoz pod jednou IP adresou, je pro vnější servery velmi těžké identifikovat konkrétní počítač, který např. provádí nelegální činnost nebo rozesílá spam.

Budoucnost: Přejít na IPv6

Jak bylo zmíněno v článku o IPv6, nová generace internetového protokolu NAT k životu nepotřebuje. Každé zařízení má svou unikátní veřejnou adresu.

S příchodem IPv6 sice zmizí „bezpečnostní clona“ v podobě NATu, ale zabezpečení sítě se tím nesníží – jeho roli plně přebírají **stavové firewally (Stateful Firewalls)** integrované v moderních routerech. Ty blokují nevyžádanou příchozí komunikaci úplně stejně jako NAT, ale bez nutnosti složitě přepisovat IP adresy v každém paketu.

Související články:

- [IPv6 - Proč potřebujeme více IP adres pro IoT](#)

- [Typy firewallů a jak je správně nastavit](#)
- [Návod: Jak nastavit Port Forwarding na routeru](#)

From:

<https://www.serviceit.cz/> - **IT ENCYKLOPEDIE**

Permanent link:

<https://www.serviceit.cz/doku.php?id=it:sec:firewall>

Last update: **2026/05/30 18:09**

