NAT (Network Address Translation)

Inhaltsverzeichnis

NAT übersetzt IP-Adressen beim Übergang zwischen Netzwerken – typischerweise von privaten internen Adressen auf eine öffentliche Adresse. So können viele Geräte hinter einer gemeinsamen Internet-IP kommunizieren.

1 Funktionsweise

Ein Router oder Firewall ersetzt Quell- oder Zieladressen in IP-Paketen. Am häufigsten ist Source-NAT/Masquerading: Interne Clients behalten private IPs, nach außen erscheint die öffentliche Adresse des Gateways.

- **SNAT / Masquerading:** interne ? öffentliche Adresse beim Outbound-Traffic.
- **DNAT / Port Forwarding:** eingehende Anfragen auf interne Dienste umleiten.
- **Connection Tracking:** zugehörige Antwortpakete werden korrekt zurückübersetzt.

2 Typische Einsatzbereiche

- Heim- und Firmennetze hinter einer öffentlichen IPv4-Adresse
- Portfreigaben für Webserver, VPN oder Mail im LAN
- Übergänge zwischen unterschiedlichen Adressräumen

3 Grenzen & Hinweise

- NAT ist kein Ersatz für eine Firewall, auch wenn es Angriffsflächen reduziert.
- Eingehende Verbindungen brauchen explizite Freigaben (DNAT).
- Mit IPv6 entfällt der Adressmangel; Segmentierung und Firewall bleiben trotzdem nötig.

4 Fazit

NAT ist in IPv4-Umgebungen Alltag und ermöglicht die gemeinsame Nutzung öffentlicher Adressen – mit klarem Blick auf Portfreigaben, Sicherheit und die Grenzen gegenüber echter Ende-zu-Ende-Erreichbarkeit.