Network Address Translation

Netzwerkgrundlagen (NWG2)

Markus Zeilinger[1]

[1]FH Oberösterreich
Department Sichere Informationssysteme

Sommersemester 2023

FH OBERÖSTERREICH
UNIVERSITY OF APPLIED SCIENCES UPPER AUSTRIA

Wichtiger Hinweis

Alle Materialien, die im Rahmen dieser LVA durch den LVA-Leiter zur Verfügung gestellt werden, wie zum Beispiel Foliensätze, Audio-Aufnahmen, Übungszettel, Musterlösungen, ... dürfen ohne explizite Genehmigung durch den LVA-Leiter NICHT weitergegeben werden!

Network Address Translation (NAT)

- Mechanismen zur transparenten Änderung von Quelle und/oder Ziel (Quell-/Ziel-adresse, Quell-/Ziel-Port) in einem Paket.
- Die aktuellen Zuordnungen müssen auf dem NAT (Network Address Translator [NAT]) verwaltet werden (NAT [State] Table).
- Motivation
  - Adressknappheit in IPv4 ("öffentliche" Adressen sind knapp) (s. NWG IP Adressierung, CIDR & Org, RFC 1380).
  - Sicherheitsaspekte (Verstecken des internen Netzwerks) folgten erst später.
- Verwendete Adressen netzintern: Private IP-Adressen nach RFC 1918
  - $10.0.0.0/8 = 10.0.0.0 - 10.255.255.255$
  - $172.16.0.0/12 = 172.16.0.0 - 172.31.255.255$
  - $192.168.0.0/16 = 192.168.0.0 - 192.168.255.255$
- Keine Standardisierung (alle RFCs sind nur „informational“ oder „BCP“); relevante RFCs: RFC 2663, 3022, 8489, 4787, 6888 und 7857.

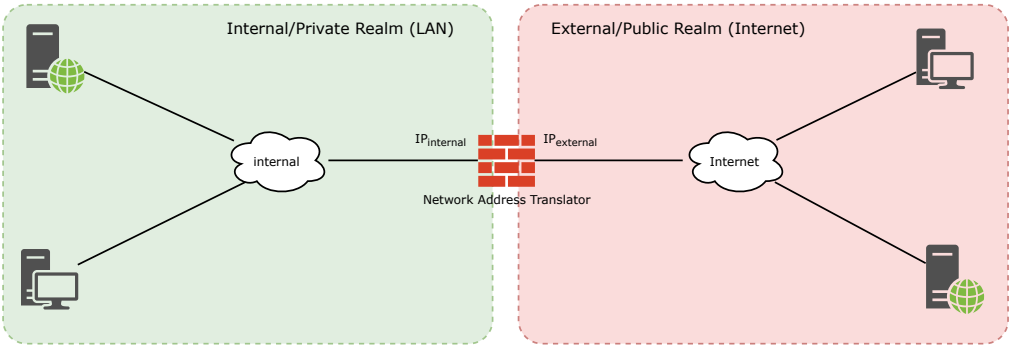
Begriffe I

- Internal/Private und External/Public Realm
  - Gültigkeitsbereich von Adressen und damit Routing-Information (intern/privat [=LAN] und extern/öffentlich [= Internet]).
- Basic NAT
  - Mapping einer Gruppe von IP-Adressen in einem Realm auf eine andere Gruppe von IP-Adressen in einem anderen Realm (n:n-Mapping).
- Network Address and Port Translation (NAPT)
  - Mapping einer Gruppe von IP-Adressen in einem Realms auf eine einzige (oder wenige) IP-Adressen in einem anderen Realm (z. B. n:1-Mapping) durch Umschreiben von Merkmalen im Transportprotokoll (Ports, ICMP Query Identifiers).

Begriffe II

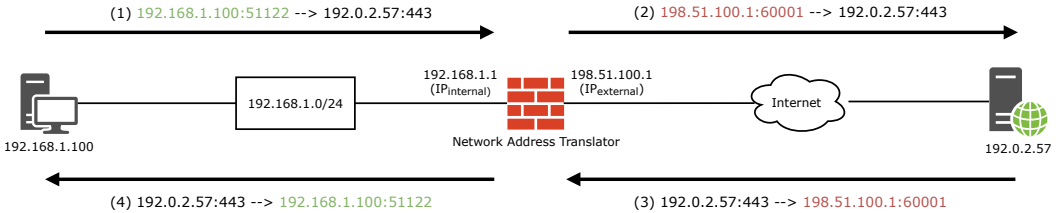
- Inbound/Outbound/Two-Way NAT
  - Adressumsetzung für Zugriffe von außen (inbound, Public → Private Realm), von innen (outbound, Private → Public Realm) oder beides (two-way)
- Static/Dynamic NAT
  - Mapping ist statisch (static) konfiguriert oder passiert dynamisch (dynamic) zum Zeitpunkt der Übertragung.

Schema



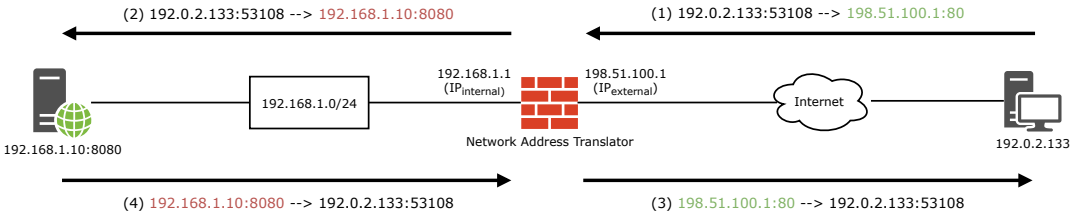
Praxis: Source NAT (SNAT) & Masquerading

- Mapping eines Quell-Adress-Port-Tupels im Private Realm in ein Quell-Adress-Port-Tupel im Public Realm.
  - Zweck: Zugriff für interne Systeme auf das Internet.
  - Private Realm bleibt "versteckt", kein direkter Zugriff aus dem Public Realm.



Praxis: Destination NAT (DNAT) (aka Port Forwarding)

- Mapping eines Ziel-IP-Port-Tupels im Public Realm auf ein Ziel-IP-Port-Tupel im Private Realm.
  - Zweck: Verfügbarmachen von Diensten/Systemen im Internet.
  - Statische Konfiguration im NAT (Static NAT).



Probleme mit NAT

- NAT verletzt das wichtige Designprinzip der Ende-zu-Ende Transparenz.
  - Anwendungen, die darauf bauen, bereiten Schwierigkeiten (z. B. FTP).
- NAT bereitet Probleme mit Sicherheitsprotokollen wie IPsec.
  - NAT modifiziert die Header des Netzwerk- und Transportprotokolls!
- NAT bereitet Probleme mit diversen Anwendungsprotokollen.
  - Beispiel FTP: Signalisierung der Kommunikationsendpunkte für die Datenverbindung im Anwendungsprotokoll.
  - Beispiel SIP (Session Initiation Protocol): Signalisierung der Kommunikations endpunkte für die Sprachkommunikation (z.B. RTP [Realtime Transport Protocol]) im Anwendungsprotokoll.
- NAT bereitet Probleme mit Peer-to-Peer Kommunikation.
  - z. B. beide Kommunikationspartner liegen hinter NATs und sind nicht direkt aus dem unsicheren Netzwerk (Internet) erreichbar.

Lösungsansätze

- NAT Traversal (= Herstellung einer Direktverbindung zwischen Hosts in NAT-Umgebungen); Ermitteln der NATs und der verwendeten externen Adressen
  - UDP/TCP Hole Punching
  - RFC 8489 Session Traversal Utilities for NAT (STUN)
  - RFC 8656 Traversal Using Relays around NAT (TURN): Relay Extensions to Session Traversal Utilities for NAT (STUN)
  - RFC 8445 Interactive Connectivity Establishment (ICE): A Protocol for Network Address Translator (NAT) Traversal
  - RFC 6887 Port Control Protocol (PCP)
  - Universal Plug and Play (UPnP) Internet Gateway Device (IGD)
- RFC 3947 + 3948 NAT-T + UDP Encapsulation of IPsec ESP packets

Zusammenfassung

- NAT ist State-of-the-Art für IPv4 → sehr weite Verbreitung, da es sehr einfach den Betrieb mehrerer Systeme hinter einer externen Adresse ermöglicht (z.B. SOHO Router).
- Verstecken des internen Netzwerks möglich → kein direkter Zugriff auf interne Systeme von extern (z.B. aus dem Internet) möglich.
- Probleme mit NAT → diverse Lösungsansätze (Komplexität!)
- Kein einheitliche Standardisierung/Terminologie (viel Wildwuchs, z. B. verschiedene Mapping-Strategien).
- NAT für IPv6 (z. B. Überlegungen des IAB dazu in RFC 5902).

UNIVERSITY OF APPLIED SCIENCES UPPER AUSTRIA
OBERÖSTERREICH