NAT und Firewalls

Jörn Stuphorn
stuphorn@rvs.uni-bielefeld.de

Stand der Veranstaltung

13. April 2005	Unix-Umgebung
20. April 2005	Unix-Umgebung
27. April 2005	Unix-Umgebung
4. Mai 2005	ARP, ICMP, ping
11. Mai 2005	IP-Adressen & Subnetzmasken
18. Mai 2005	Einführung in Bridging, Routing, ...
25. Mai 2005	IOS, Spanning-Tree
1. Juni 2005	IOS Befehle, Brigding, Routing
8. Juni 2005	Statisches Routing
15. Juni 2005	UDP-, MTU- und IP-Fragmentierung
22. Juni 2005	TCP-Verbindungen und -Datenfluss
29. Juni 2005	DHCP und NTP
6. Juli 2005	***NAT und Firewalls***
13. Juli 2005	*Verschlüsselung, Vertraulichkeit, Authentisierung*
20. Juli 2005	*Sichere Anwendungen*

Network Address Translator

- Unterschiedliche Kommentare:
  - klasse Problemlösung
  - Verstoß gegen die IP Philosophie
- NAT: Abbildung von
  - 1 IP Adressbereich (meist privat)
  - auf 1 IP Adressbereich (öffentlich)
- Nutzen:
  - Verwendung eines begrenzten Adressbereich für größeres Netzwerk
  - Sicherheit:
    - internes Netz kann nach außen versteckt werden

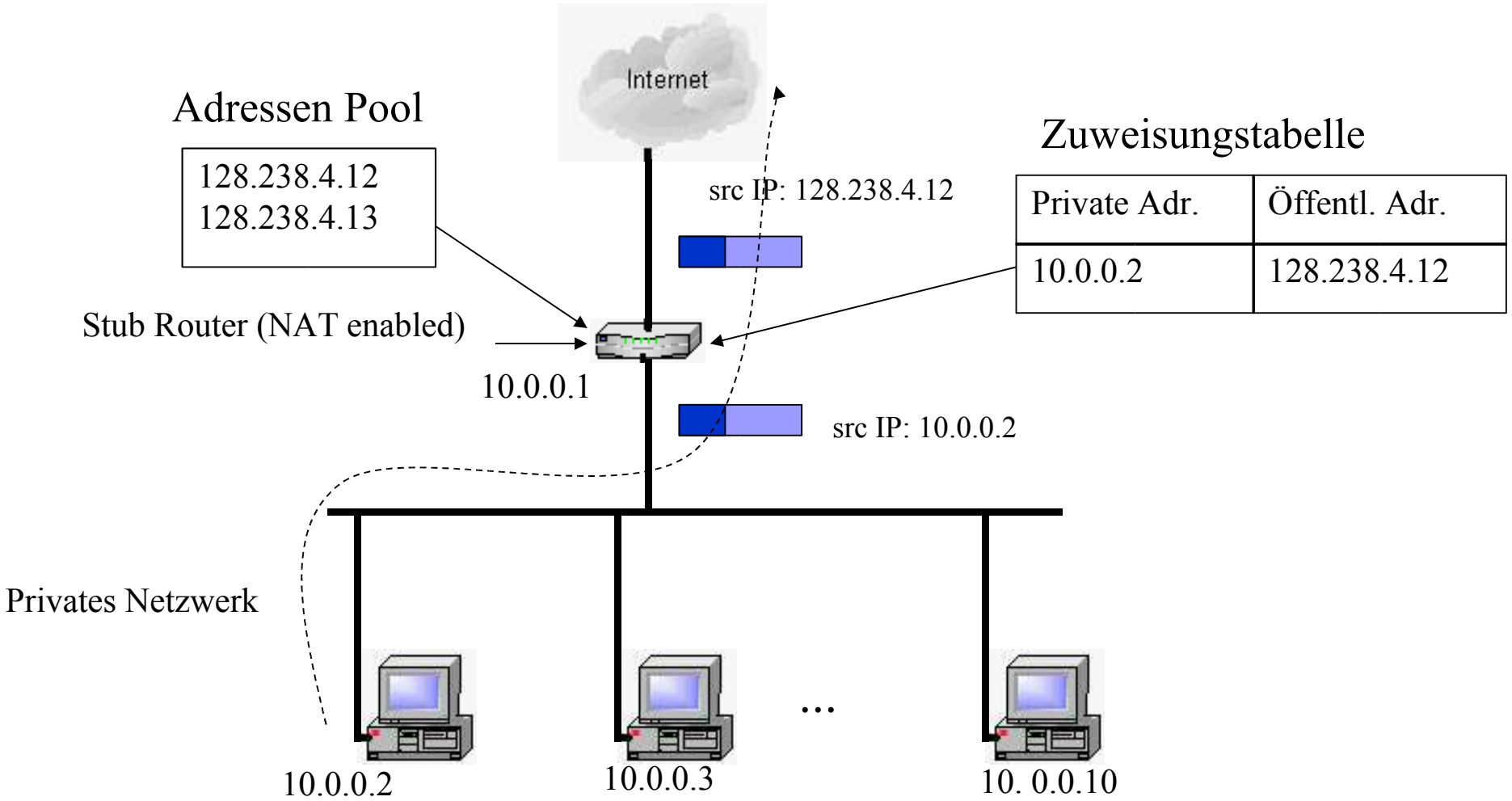
Funktionsweise

- 2 Netze
  - 1 externes Netz, z.B. Internet
  - 1 privates/internes Netz
- 2 Adressbereiche:
  - IP Adresse des externen Netzes durch IANA vergeben
  - Internes Netz:
    - prinzipiell frei wählbar
    - sollte aus privaten Adressraum stammen (nur diese sind als nicht eindeutig bekannt)
- Stub Router
  - übersetzen Adressbereiche in einander
  - modifizieren ICMP Payload
- NAT Zuweisung:
  - Statisch
    1 interne IP bekommt immer 1 externe IP (z.B. für Server)
  - Dynamisch
    IP Adresse wird zufällig aus Pool genommen

Operationen

- Address binding
  - Zuordnung von privater IP Adresse gegen externe Adresse
  - Router führt Tabelle über diese Zuweisungen
- Lookup und Translation
  - Outgoing Packets:
    Source IP Adresse wird gegen zugewiesen externe IP Adresse getauscht
  - Incoming Packets:
    Ziel IP Adresse wird gegen entsprechende interne IP Adresse getauscht
- Address unbinding
  - Nach Beendigung der Sitzung
    - Entfernen des Eintrags aus der Tabelle
    - Anderer interner Host kann externe Adresse benutzen

Beispiel


Internet
Adressen Pool
128.238.4.12
128.238.4.13
Zuweisungstabelle
Private Adr.
Öffentl. Adr.
10.0.0.2
128.238.4.12
src IP: 128.238.4.12
Stub Router (NAT enabled)
10.0.0.1
src IP: 10.0.0.2
Privates Netzwerk
10.0.0.2
10.0.0.3
...
10. 0.0.10

Port Address Translation

- NAT beschränkt sich auf Zuweisung von IP Adressen
  - Für jeden internen Host, der mit externem Netz kommuniziert wird 1 IP benötigt
- PAT benutzt auch Transport Identifiers (TCP port numbers, UDP query identifiers)
  - Viele interne Hosts können über 1 externe IP Adresse erreichbar sein.
  - PAT kann mit NAT kombiniert werden

Funktionsweise

- Assoziationstabelle
  - Tablle, die IP Adresse, Port Nummer und ICMP query ID enthält
- Outgoing Packets
  - Übersetzen von
    - Source IP Adresse
    - Source Transport ID
    - ICMP query ID und zugehörige Felder, wie IP, TCP, UDP, ICMP Header, Checksum
- Incoming Packets
  - Übersetzen von
    - Ziel IP Adresse
    - Ziel Transport ID
    - IP und Transport Checksums

Bemerkungen

- ICMP Fehlernachrichten müssen modifiziert werden
- Das IP Packet in der ICMP Nachricht muss verändert werden

- Sicherheit:
  - Eingeschränkter Zugriff von extern nach intern
  - Nur definierter Übergang von intern nach extern
  - In Verbindung mit Firewall filtern von ungewünschtem Traffic möglich

- Sicherheitstechniken, die auf IP Adresse arbeiten können ausgehebelt werden
- Rechenintensiv
  - Router kann zu Flaschenhals werden

- Anwendungen, die auf IP oder abhängigen Kontrollsessions basieren (SMNP, H.232, FTP) benötigen speziellen Gateway

Übung

- NAT mit Router als NAT stub router (ex.10)
- Versuch, Verbindung extern -> intern (ex.11)
- ICMP Messages (ex.12)
- PAT (ex.13)

Firewalls

- Implementiert durch Gerät oder Programm
- befindet sich am Übergang zwischen internem und externen Netz
  - Achtung: externes Netz ist nicht gleich Internet!
- Verwendet, z.B. um
  - unerwünschten Traffic von extern zu blocken
  - verhindern, dass interner Nutzer unautorisierte externe Dienste verwendet

Arten von Firewall

- Packet filter
  - blockieren von ausgewählten Netzwerk Paketen
- Anwendungs Gateway/Proxy Server
  - zentraler Dienst, der Zugriff auf externe Dienste regelt
- Circuit-Level Gateway
  - wie eine Schalttafel
  - eine interne Verbindung wird einer externen Verbindung zugewiesen

iptables

- Standard Firewall seit Linux Kernel 2.4
- Firewallregel besteht aus
  - Bedingung
    - z.B. Zielportnummer, Adressbereich, ...
  - Reaktion auf Bedingung
    - allow, drop, reject
- Regeln in 3 Tabellen organisiert
  - Filter
    - Standard Tabelle
    - filtern von Packeten
  - NAT
    - Veränderung von Paketen, die eine neue Verbindung aufbauen
  - Mangle
    - Spezielle Veränderungen von Paketen, z.B. Änderung vor Routing, etc.

iptables Tabellen

- Jeder Tabelle sind chains zugewiesen
- chains enthalten Regeln

- Filter Tabelle - Chains:
  - INPUT
    - Regeln für eingehende Pakete
  - OUTPUT
    - Regeln für ausgehende Pakete
  - FORWARD
    - Regeln für Pakete, die weitergeleitet werden sollen

- Syntax des iptables-Aufrufs:
  iptables *[-t table] Kommando Chain Parameter1 Option1 ... ParameterN OptionN*
- Kommandos:
  - -A append, anhängen einer Regel
  - -F flush, löschen von Regeln

Parameter & Optionen

- Parameter:
  - -d Destination-Host
  - -s Source-Host
  - -i Interface
  - -p Protokoll
- Optionen:
  - ACCEPT (akzeptiere Paket)
  - DROP (Paket verfällt ohne Nachricht an Sender)
  - REJECT (Paket verfällt mit Nachricht an Sender)
  - QUEUE (Paket wird an User-Appl. Queue weitergegeben)
  - RETURN (Bearbeitung der Chain wird abgebrochen)
  - LOG (Protokollierung in Systemlog)

Übung (ex.8&9)

- Welche Regeln sind eingetragen? *iptables -L -v*
- Regel anhängen
  iptables -A INPUT -v -p TCP --dport 22 -j DROP
- Welche Regeln sind eingetragen?

- Teste ssh *yoda*

- Lösche die vorher eingefügte Regel
  iptables -D INPUT -v -p TCP --dport 22 -j DROP
- neue Regel:
  iptables -A INPUT -v -p TCP --dport 22 -j REJECT --reject-with tcp-reset
- *Welche Regeln sind eingetragen?*

- *Teste ssh yoda*

- Was bewirken die Regeln?