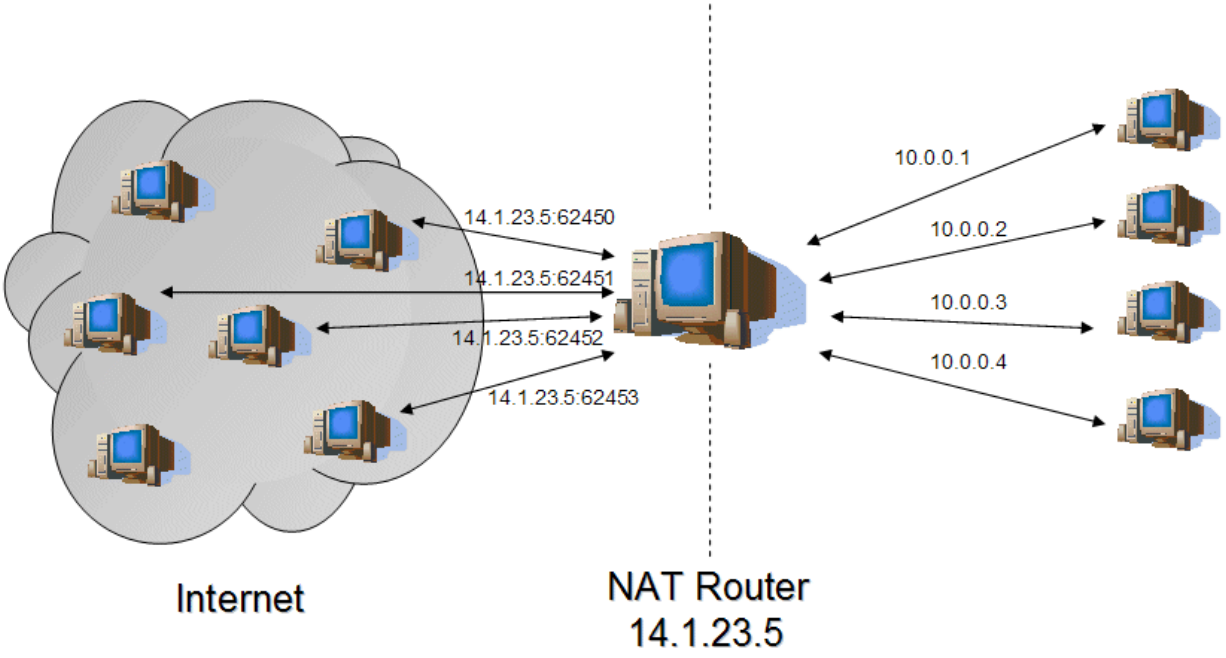
NAT - Network Address Translation



Studiengang:	Medieninformatik WiSe15/16
Modul:	Informationssicherheit - Labor
Laborgruppe:	Gruppe Z (C)
Bericht von:	Arthur Jaks
	Tobias Winkler
	Emel Altmisoglu

Inhaltsangabe

Einleitung

Zum Austausch von Informationen innerhalb eines Netzwerkes werden IP Adressen zur Erkennung des Senders und Empfängers genutzt. Das Internetprotokoll IPv4 ist jedoch aufgeteilt in private und öffentliche IP Adressen, welches eine Kommunikation von physikalisch nicht verbundenen Netzen durch ihre privaten IP Adresse nicht ermöglicht. Die öffentlichen IP Adressen reichen auch nicht aus um alle Geräte mit dem Internet zu verbinden. Deshalb werden die Daten der private Adressen über die öffentliche Adresse versendet. Für die Identifikation des Senders merkt sich der Router durch NAT welche Datenpakete zu welcher TCP Verbindung gehören. Durch dieses Verfahren können private IP Adressen mehrfach verwendet werden. Bis zur Benutzung von IPv6 ist dies ein Ausweg um die Adressknappheit zu umgehen.
NAT kommt auf dem Router zum Einsatz, welcher eine öffentliche Adresse Zugewiesen bekommen hat und somit auch mit dem WAN verbunden ist. Dieser Router bekommt auch eine private IP Adresse, welches dann als Default Gateway und somit als eine zwischen Station seines LANs mit dem WAN ist. Alle mit diesem Router verbunden Geräte bekommen dann private IP Adressen zugewiesen und vermitteln ihre Datenpakete über ihr Default Gateway an das WAN. Der Router ersetzt die privaten IP Adressen mit seiner öffentlichen IP Adresse und die Port Nummern (ob TCP oder UDP) auch mit einer anderen. Hierfür merkt sich der Router in einer Tabelle die geänderten Adressen und Ports um die Antwortpakete zum richtigen Empfänger weiterzuleiten.

Versuchsaufbau

Für die Konfiguration von NAT wird ein eingerichtetes Lokales Netzwerk mit 1 oder mehr Geräten sowie der Router mit Zugang zum WAN benötigt. Zunächst sollte überlegt werden, welcher private IP Adressbereich mittels NAT umgewandelt werden soll. Welche äußeren Schnittstellen sollen verwendet werden, um die Datenpakete über das Internet zu verschicken? Nach dem das Netzwerk, sowie auch die Planung der Adressen vorhanden ist, kann mit der Einrichtung des NAT begonnen werden.

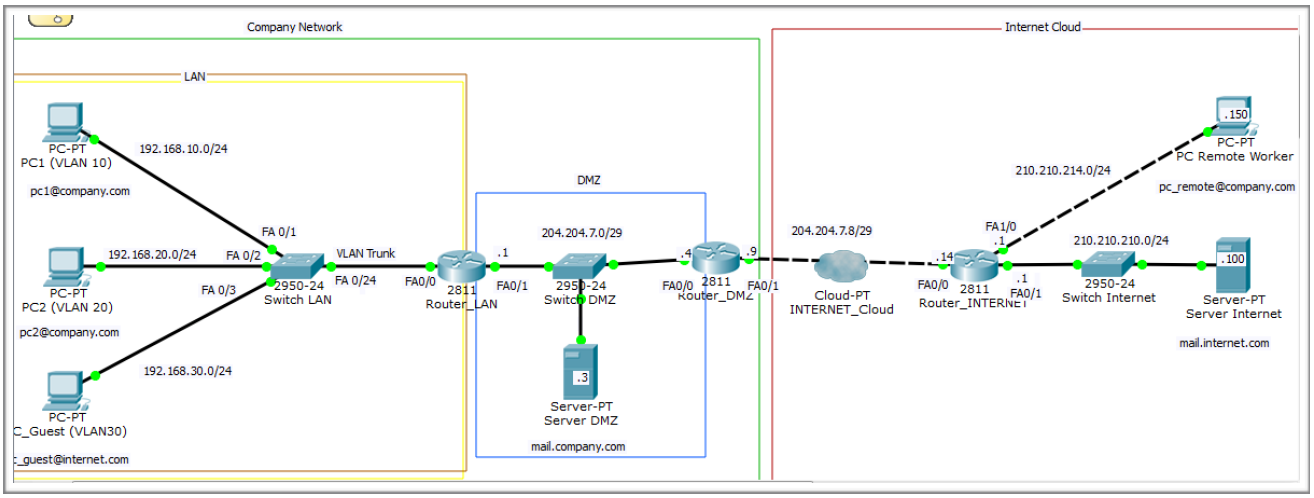


Abb. 2: Fertiges Netzwerk zur Konfiguration von NAT

Versuchsdurchführung

Der ausgewählte Adressbereich wird dann an dem Router durch ein Access List Control angelegt.
Der Router kennt den Adressbereich durch die Eingabe der Start IP Adresse und der Wildcard.

```
Router_LAN#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router_LAN(config)#access-list 10 permit 192.168.0.0 0.0.255.255
Router_LAN(config)#
```

Abb. 3: ACL Konfiguration an einem Router

Die Wildcard gibt an, wie groß der Adressbereich sein soll, wodurch der Router dann auch die Endadresse, wie auch den gesamten Adressbereich dazwischen kennt. Eine Wildcard setzt sich ähnlich wie eine Subnetzmaske zusammen, nur das die 0 darstellt, welche Bytes genau gleich sein müssen und die 255 zeigt, dass dieser Block an Bytes nicht mit der Startadresse übereinstimmen muss. Dadurch wird der Adressbereich definiert. Mit dem Befehl „permit“ werden sie also zugelassen und mit „deny“ ausgeschlossen.

Nun werden die äusseren IP Adressen hinzugefügt, welche mit dem zuvor eingerichteten inneren Adressbereich kommunizieren sollen. Dafür wird ein NAT Pool eingerichtet, welcher die öffentliche IP Adresse als Start- sowie auch Endadresse erhält.

```
Router_LAN(config)#ip nat pool NAT_POOL1 204.204.7.1 204.204.7.1 netmask
255.255.255.255
Router_LAN(config)#
```

Abb. 4: Einrichten eines NAT Pools

Die Schnittstellen, welche durch die IP Adressen im Pool als „outside“ Schnittstellen eingerichtet werden, nutzen dann NAT und leiten die Datenpakete der inneren Schnittstellen weiter und auch wieder an sie zurück.
Die inneren Schnittstellen, welche vom NAT umgewandelt werden sollen, müssen somit als „inside“ Interfaces dem NAT Pool hinzugefügt werden.

```
Router_LAN(config)#ip nat pool NAT_POOL1 204.204.7.1 204.204.7.1 netmask
255.255.255.255
Router_LAN(config)#interface fa0/0.10
Router_LAN(config-subif)#ip nat inside
Router LAN(config-subif)#exit
```

Abb. 5: Äussere wie auch innere Schnittstellen dem NAT Pool hinzufügen

Sofern alles konfiguriert ist, muss das NAT nur noch aktiviert werden. Dies erfolgt mit dem Befehl “*ip nat inside source list <ACL number> pool <Name of NAT pool> overload*“. Die Nummer, welche dem ACL zuvor vergeben wurde wird hier zur Wiedererkennung eingetragen sowie auch der Name des NAT Pools. Damit auch mehrere innere Adressen von einer einzigen äusseren Adresse genutzt werden können, wird der Befehl „overload“ mit angefügt.

Versuchsergebnisse

Somit ist der Router konfiguriert und die Geräte mit privater IP Adresse können nun Datenpakete an das Internet versenden und auch erhalten. Um dies zu überprüfen, kann mit dem Befehl “debug ip packet” auf dem Router ein Debugging angestellt werden. Hier wird erkenntlich, das ein Ping vor der Einrichtung von NAT die private IP Adresse des Senders enthält, und nach der Einrichtung ihre umgewandelte IP Adresse

```
Router_DMZ#
IP: tableid=0, s=192.168.10.11 (FastEthernet0/0), d=204.204.7.4 (FastEthernet0/0), routed via RIB

IP: s=192.168.10.11 (FastEthernet0/0), d=204.204.7.4 (FastEthernet0/0), len 128, rcvd 3
```

Abb. 6: Mitschnitt eines Pings vor der Konfiguration von NAT

```
Router_DMZ#
IP: tableid=0, s=204.204.7.1 (FastEthernet0/0), d=204.204.7.4 (FastEthernet0/0), routed via RIB

IP: s=204.204.7.1 (FastEthernet0/0), d=204.204.7.4 (FastEthernet0/0), len 128, rcvd 3
```

Abb. 7: Mitschnitt eines Pings nach der Konfiguration von NAT

Eine weitere Überprüfung erfolgt durch den Aufruf einer Webseite über die PCs. Der Router, welcher NAT zur Umwandlung der Adressen benutzt, speichert diese Daten in einer Tabelle ab, welche über den Befehl „show ip nat translations“ eingesehen werden kann.
Hierbei wird erkenntlich, das die private IP Adresse des PCs sowie sein Port mit der öffentlichen IP Adresse des Routers sowie eines seiner freien Ports ersetzt wurde.

```
Router_LAN>show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
tcp 204.204.7.1:1024   192.168.20.11:1025 204.204.7.3:80     204.204.7.3:80
tcp 204.204.7.1:1025   192.168.10.11:1025 204.204.7.3:80     204.204.7.3:80

Router_LAN>
```

Abb. 8: NAT Tabelle des Routers

Zuvor hatte der Router eine Routingtabelle um zu erkennen, an welches Gerät die Daten innerhalb seines Netzes versendet werden sollen, dies ist für diejenigen Adressen, welche nun im NAT Pool enthalten sind, nicht mehr von Nöten, da der Router die Adressen ja eh schon durch NAT kennt und an diese die Pakete versenden kann.

Quellenverzeichnis

Aulis /Informationssicherheit Laboraufgabe IS_Activity_Lab2_NAT_20131016 08.10.2015

http://www.elektronik-kompendium.de/sites/net/0812111.htm 09.10.2015

Abbildungsverzeichnis