8bit-Zahl . 8bit-Zahl . 8bit-Zahl . 8bit-Zahl
z.B. 10.0.28.21

Von diese 4x8 bit sind einige reserviert für "besondere Aufgaben".

Eine Netzmaske gibt an, welcher Teil der IP-Adresse für das Netzwerk, und welcher für den einzelnen Computer verwendet wird.

1.2.3.4 mit einer Netzmaske 255.255.255.0

bedeutet: Alle 254 Rechner (letzte Zahl) im Netzwerk 1.2.3 können sich ohne Routing "unterhalten"

Sind in der Rechner-Adresse (letzte Zahl(en)) alle Bits gesetzt, dann handelt es sich um eine Broadcast-Adresse, bei der ALLE Rechner im Netzwerk angesprochen werden.
1.2.3.255 ist für das Netzwerk 1.2.3 die Broadcast-Adresse.

Sollen Daten mit einem Computer außerhalb des eigenen Netzes geschickt werden, z.B.

von 10.0.28.21 nach 85.214.68.145, dann ist mindestens ein Router erforderlich, der die Pakete aktiv weiterleitet!

Ein Router hat für jedes Netzwerk, das er bedient, eine Schnittstelle, die in dieses Netzwerk mündet.

Ein "Gateway" ist ein Router, der den Rechnern in einem Netzwerk den Zugang "nach außen" erlaubt, also in andere Netzwerke und ins Internet. "Ausgang".

Das "Default-Gateway" erlaubt für ALLE Zieladressen die Weiterleitung von Daten. Es hat bei IPV4 immer die Routing-Adresse 0.0.0.0, und eine eigene IP-Adresse, die sich im Netzwerk Ihres eigenen Rechners befinden MUSS!

Die aktuelle Routing-Tabelle kann man sich
unter Windows mit "route print"
unter Linux mit "route -n"
anschauen. Der Eintrag mit "0.0.0.0" enthält (weiter rechts) die IP-Adresse des Default-Gateway.

Das Programm "traceroute ip-adresse"
(Windows: tracert adresse) zeigt die
Liste der Router an, die zwischen Ihrem Rechner
und dem Ziel liegen.

Jeder Router zwischen der Quelle (Source Adresse im IP-Paket) und dem Ziel (Zieladresse im IP-Paket) kann das Paket weiterleiten, verändern, untersuchen... oder auch nicht.

IPV6-Adressen sind etwas anders aufgebaut.
Die letzten 4x8bit können einer IPV4-Adresse entsprechen.

Woher kommen die IP-Adressen?

1. vom DHCP-Server (lokal)
2. Vom Internet-Provider ("Internet-Zugang")
3. IANA (Internet Assigned Numbers Authority)

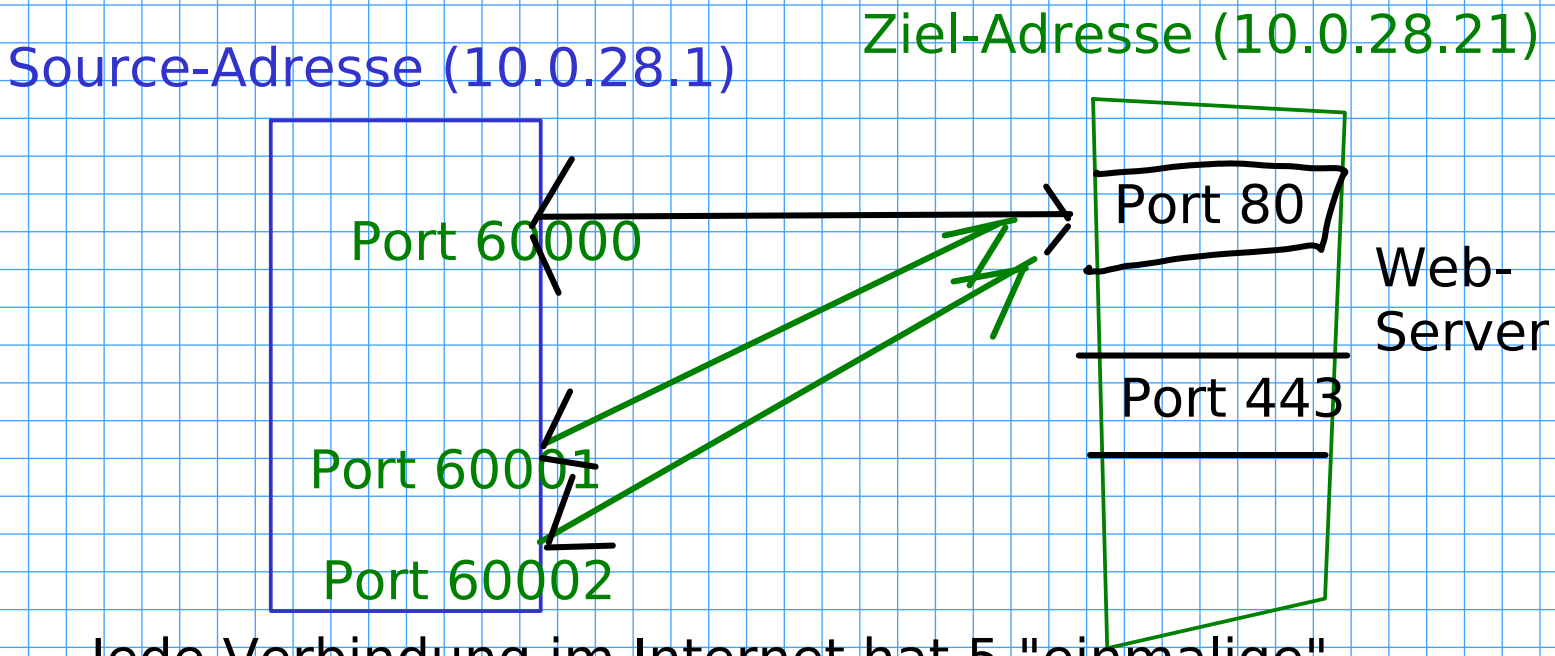
Lokal können "private" Netze vergeben werden, die nicht im Internet verwendet werden.

Einige IPV4-Adressen sind regelrecht "berühmt":
8.8.8.8 (Google-Nameserver)
9.9.9.9 (Alternativ-Nameserver)

Ein Nameserver ist eine Netzwerk-Datenbank, die Anfragen der Form "Welche IP-Adresse hat knopper.net" mit der entsprechenden Information beantwortet. Adressen, die z.B. im Browser eingegeben werden, führen zu einer Nameserver-Abfrage, da die IP-Pakete nur an Adressen und nicht an "Namen" geschickt werden können.

Sicherheitstechnisch kritisch: Wer den Nameserver übernimmt, kann Adressen "umleiten"!

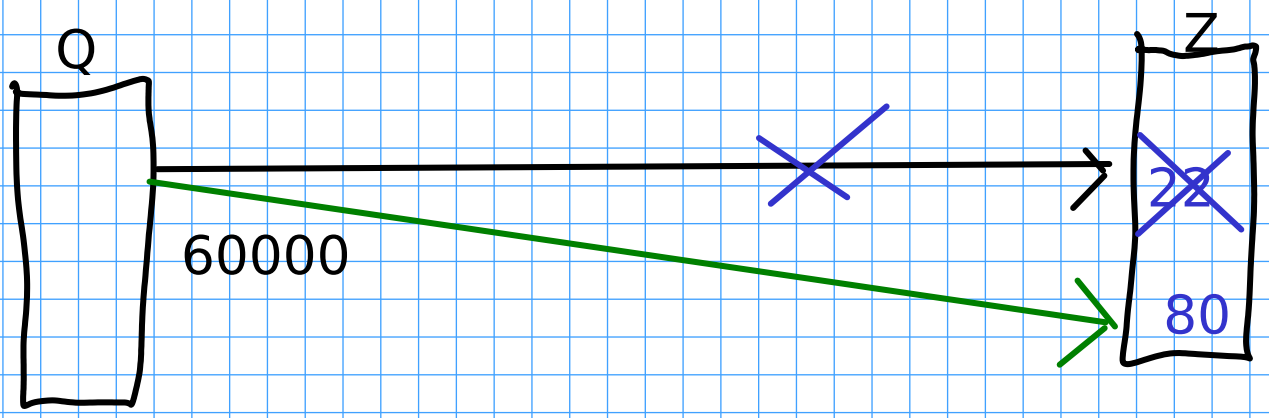
Schutz: SSL-Zertifikate "passen" nur auf den richtigen Rechner, der Browser meldet also, wenn eine ungültige Signatur der Webseite erkannt wird.



Jede Verbindung im Internet hat 5 "einmalige" Parameter: Source-IP, Source-Port, Ziel-IP, Ziel-Port TCP oder UDP, es kann keine zweite parallele Verbindur mit den gleichen Parametern geben!

Ein Server-Dienst (gleiche Portnummer, z.B. 80) kann also mehrere Clients bedienen (unterschiedliche Portnummer und/oder Quelle-Adresse), und ein Client kann mehrere Verbindungen aufbauen, die jeweils unterschiedliche Quell-Ports besitzen. Man kann vom gleichen Quell-Port auch viele gleichzeitige Verbindungen zu unterschiedlichen Zielrechnern und/oder Zielports aufbauen

Wie funktioniert ein Firewall?



Der (oder die) Firewall filtert nach Adresse oder Port, und kann so z.B. auf dem Zielrechner Verbindungen zu Port 22 unterbinden, während sie für Port 80 erlaubt sind.

Auf dem Rechner "Z" mit iptables:
iptables -I INPUT -p tcp --dport 22 -j REJECT

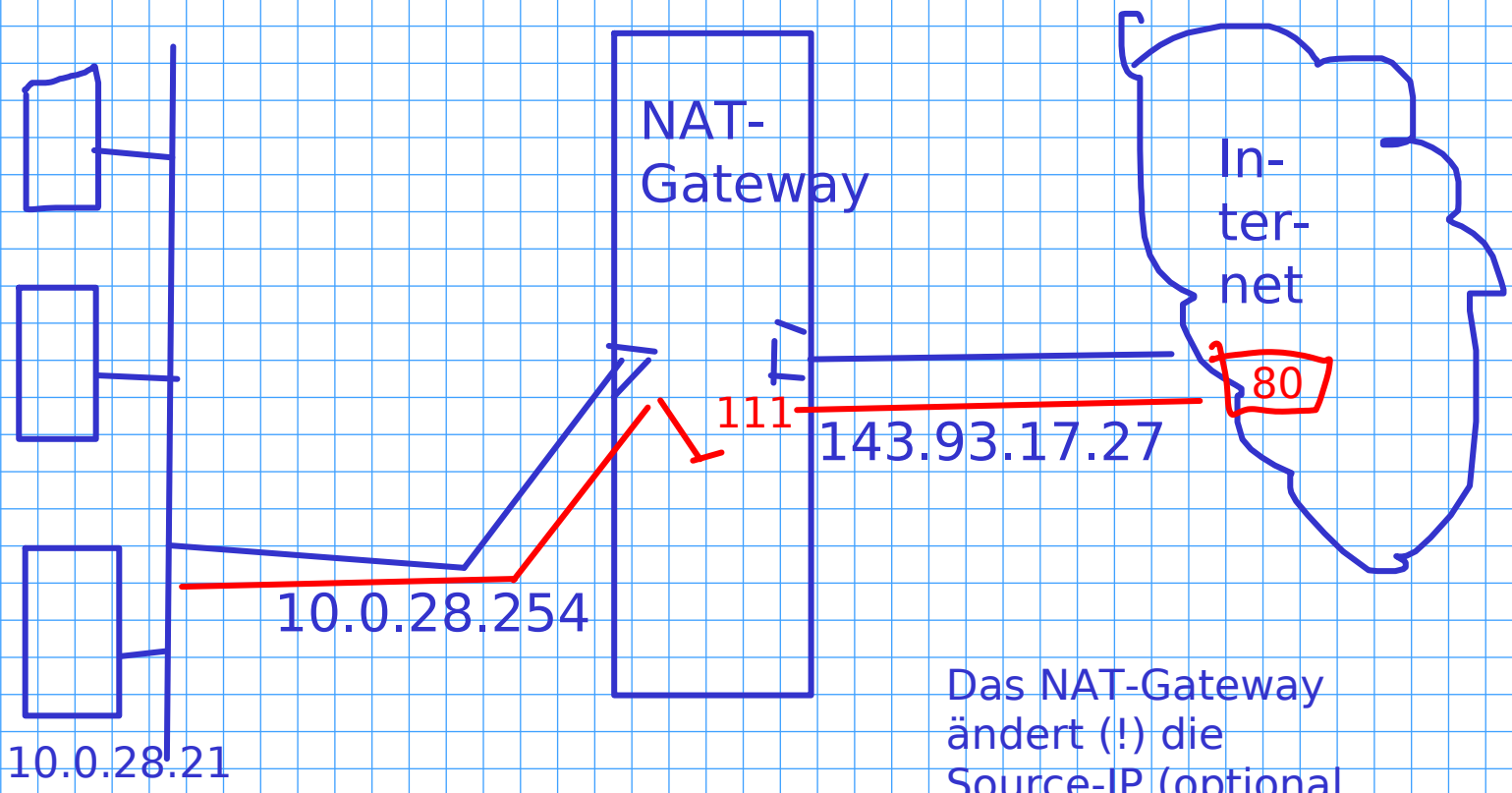
Verbindungen zu Port 22 des Rechners Z über tcp werden jetzt zurückgewiesen!

Mit
iptables -I INPUT -p tcp --dport 22 -j DROP
werden Verbindungsanfragen sogar "verschluckt", der kontaktaufnehmende Rechner erfährt nie, ob angefragte Rechner überhaupt existiert.

Mit
nmap ip-adresse
lässt sich herausfinden, welche Dienste auf einem Rechner offene Ports anbieten.

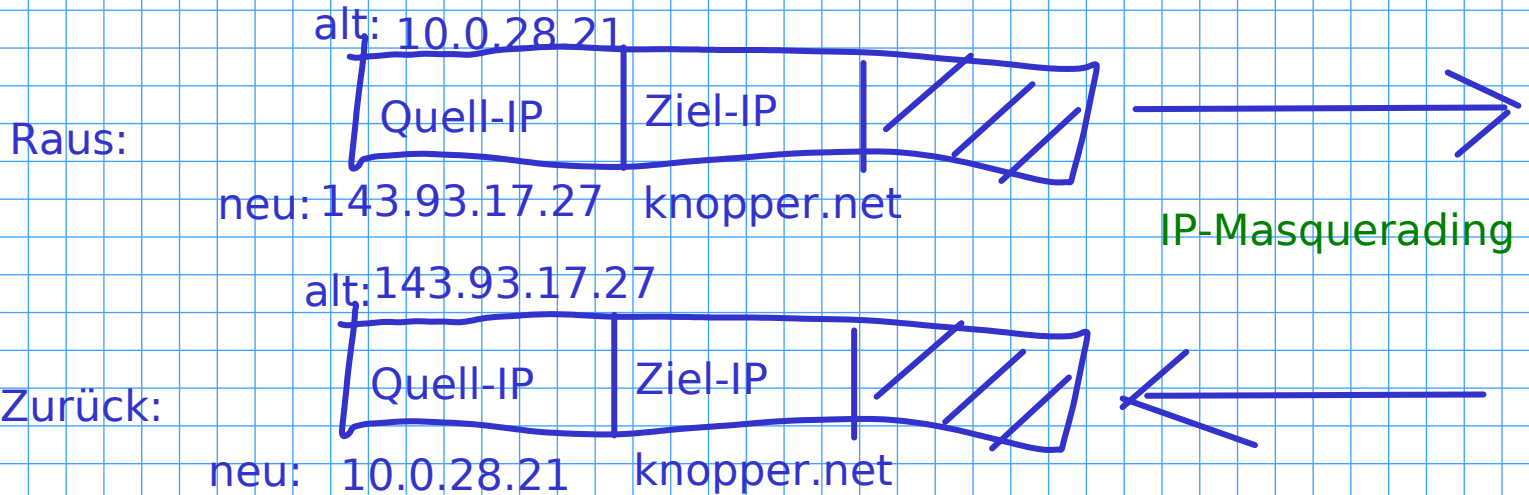
Private IP-Adressen 10.*.*.* und 192.168.*.*
sind immer LOKALE Adressen und werden
im Internet nicht geroutet!

NAT (Network Address Translation)
und Masquerading



Das NAT-Gateway
ändert (!) die
Source-IP (optional
auch die Ziel-IP)!

Änderung eines IP-Pakets:



Durch die Address Translation ist das NAT-Gateway eigentlich schon ein guter Firewall: Es lässt Verbindungen vom internen Netz (10.*.*.*) ins Internet zu, und lässt auch Daten, die über die gleiche Verbindung zurück laufen durch, aber ein Verbindungsaufbau von Außen auf eine private Adresse ist unmöglich!

Die Angreifer, die ins interne Netz wollen, müssten also zunächst einen Zugang auf das Gateway erhalten ("Accesspoint hacken"), bevor sie weiter kommen.

Das ist leider durch herstellerspezifische "Wartungs-Hintertüren" nicht ganz abwegig...

Ein einfaches NAT-Gateway mit Linux:

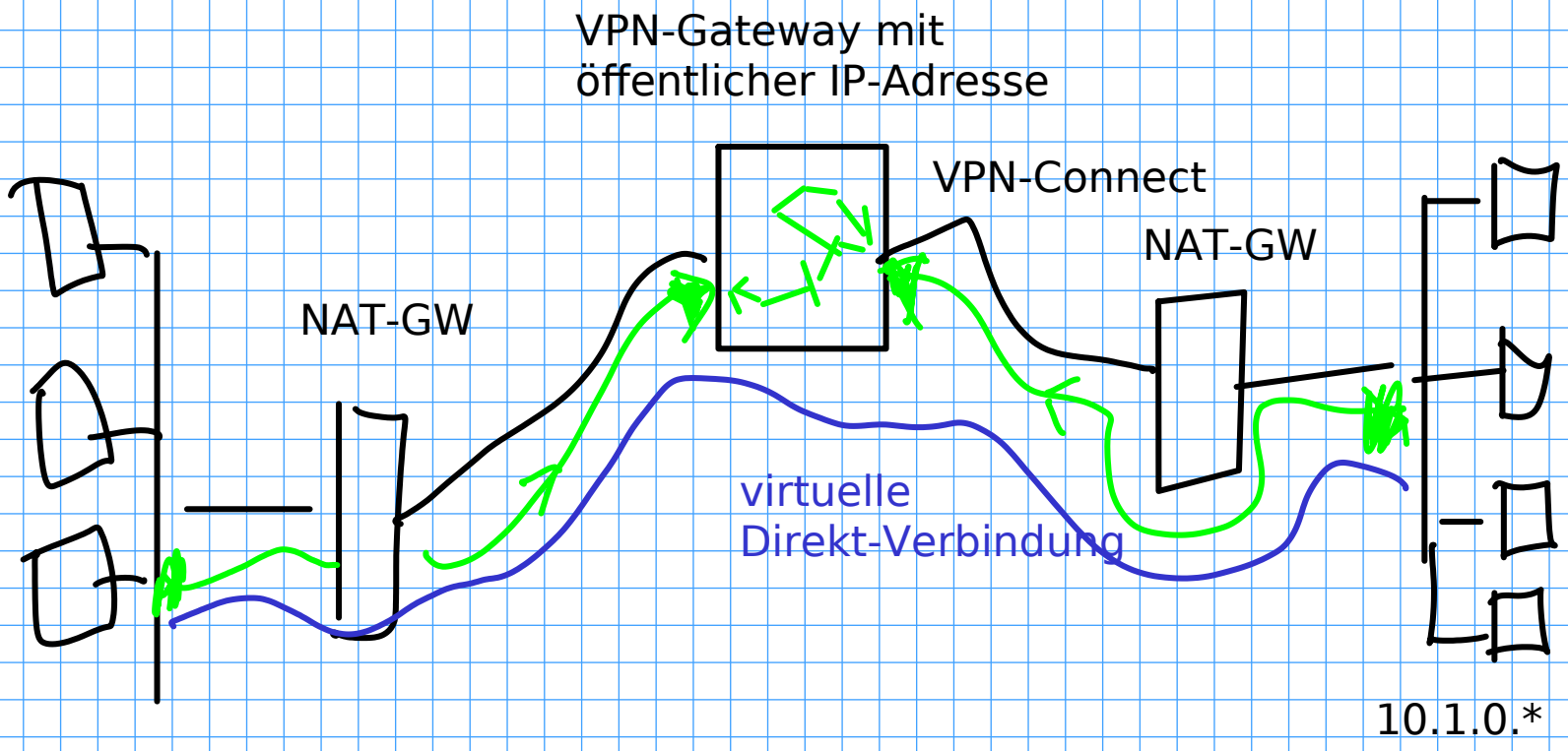
Schaltet Masqueraring für ausgehende Pakete auf der Netzwerkkarte eth0 ein:

iptables -t nat -I POSTROUTING -o eth0 -j MASQUERADE

Frage: Wie könnte ein Angreifer jetzt noch Zugang zu Computern im internen (10.*.*.*)-Netz erhalten, wenn er das NAT-Gateway nicht kompromittieren kann?

Antwort: Der Angreifer muss einen Trojaner auf einen Rechner im Intranet bringen, der wiederum eine Verbindung NACH AUßEN (!) aufbaut! Hierzu ist ein Rechner im Internet erforderlich, der als "Relay" dient. Ist die Verbindung von innen nach außen einmal aufgebaut, kann das Relay über die bestehende Verbindung den Rechner im Intranet "Fernsteuern".

VPNs mit Rechnern in Intranets funktionieren übrigens genauso. Hier wird eine Verbindung zu einem Relay mit erreichbarer Adresse aufgebaut, von allen Beteiligten. Über dieses Relay können Daten untereinander versandt werden.



Wie kann man die Schwachstelle des Verbindungsaufbaus von innen nach außen unterbinden oder einschränken?
Lösung: Alle Verbindungsaufbauten von innen nach außen, die NICHT gebraucht werden, ABSCHALTEN!

Beispiel: (erst mal "alles aus"):

iptables -P OUTPUT -j DROP

Jetzt bestimmte Dienste wieder freischalten:

(Lokale Dienste auf dem gleichen Rechner erlauben)
iptables -I OUTPUT -p tcp -s 127.0.0.1 -j ACCEPT
(Port 80 Abruf erlauben)
iptables -I OUTPUT -p tcp -s 10.0.0.0/24 --sport 80 -j ACCEPT
Schaltet den Abruf won Webseiten von Port 80 dieses Servers wieder frei.
(Port 22 SSH erlauben)
iptables -I OUTPUT -p tcp --sport 22 -j ACCEPT

Wenn ein Gateway/Firewall nur bestimmte Ports nach außen durchlässt, kann man sich mit Software behelfen, die sog. "Firewall-Piercing" realisiert. Hier wird auf der Seite des Intranet ein http-Client (z.B. htc aus httptunnel) installiert, der eine virtuelle Netzwerkkarte erstellt. Dieser Client verbindet sich mit einem speziellen http-Server (hts) Port 80 im Internet, der dann aus den scheinbaren http-Abfragen tcp-Pakete erstellt, die normal im Internet geroutet werden.

Das besonders praktische: httptunnel funktioniert auch über einen Zwangs-Proxy! :-)

Anleitung für httptunnel: http://linuxwiki.de/HttpTunnel