

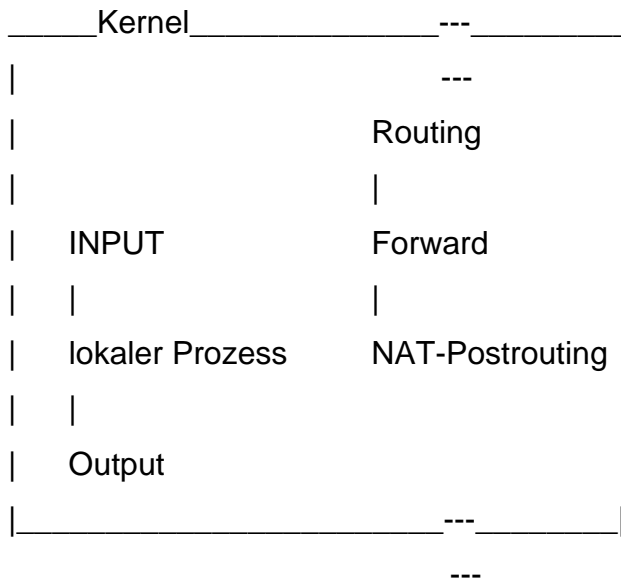
1. Verzeichnisse komprimieren:

- komprimieren von Dateien mit: "gzip"
- Verzeichnisse müssen vorher in Dateien umgewandelt werden mit: "tar"
- Kommando "dd"
 - "diskdump"
 - Syntax: "# dd if=... of=..." //if: inputfile of: outputfile

2. IP-Paketfilter:

- iptables
 - überprüft den Header des IP-Paketes
 - besteht aus 3 Filtertabellen => enth Regeltab:
 - 1) "Filtertabelle": INPUT
FORWARD
OUTPUT
 - 2) "NAT-Tabelle":(network adress translator)
OUTPUT
PREROUTING
POSTROUTING
 - 3) "Mangle-Tabelle": PREROUTING
OUTPUT
 - => 2: - für Gateways und Router
 - Maskerading
 - => 3: - für Spezialaufgaben
 - Adressmanipulation
 - => 1: Defaulteinstellungen (von iptables)
 - alle 3 Tabellen bestehen
 - 1) enthält alle 3 Regelketten, läßt aber alles durch

LAN/WWW



LAN/WWW

*1: falls es weitergeleitet werden soll

*2: ist für den eigenen Rechner

*3: senden

- Kommandos (siehe IPTABLES-Syntax-Blatt):

- "# iptables -L" --> zeigt die Definitionen der Regelketten an
- "# iptables -A INPUT -d xyz -j ACCEPT" --> Definition einer Regel
- Module: state (prüft Flags bei Kontaktaufnahme)

syn

syn + ack

ack

--> es können alle Pakete, die nur das syn-Flag gesetzt haben blockiert werden (Rechner, die versuchen aus dem Internet eine Verbindung aufzupassen)

3. Aufgabe:

1. alle Verbindungen verbieten; möglich soll sein PING und FTP (nur auf 143.93.53.17); FTP auf eigenen Rechner verbieten

Lösung:

- a) alles Verbieten:

```
„iptables -P INPUT DROP“
```

```
„iptables -P OUTPUT DROP“
```

```
„iptables -P FORWARD DROP“
```

- b) Ping möglich machen:

```
„iptables -A INPUT -p icmp -j ACCEPT“
```

```
„iptables -A OUTPUT -p icmp -j ACCEPT“
```

- c) FTP auf 143.93.53.17 möglich machen:

```
„iptables -A INPUT -s 143.93.53.17 -m state --state ESTABLISHED  
-j ACCEPT“
```

```
“iptables -A OUTPUT -p tcp --dport 1024:65535 -j ACCEPT”
```

```
“iptables -A INPUT -p tcp --dport 21 -j ACCEPT”
```
