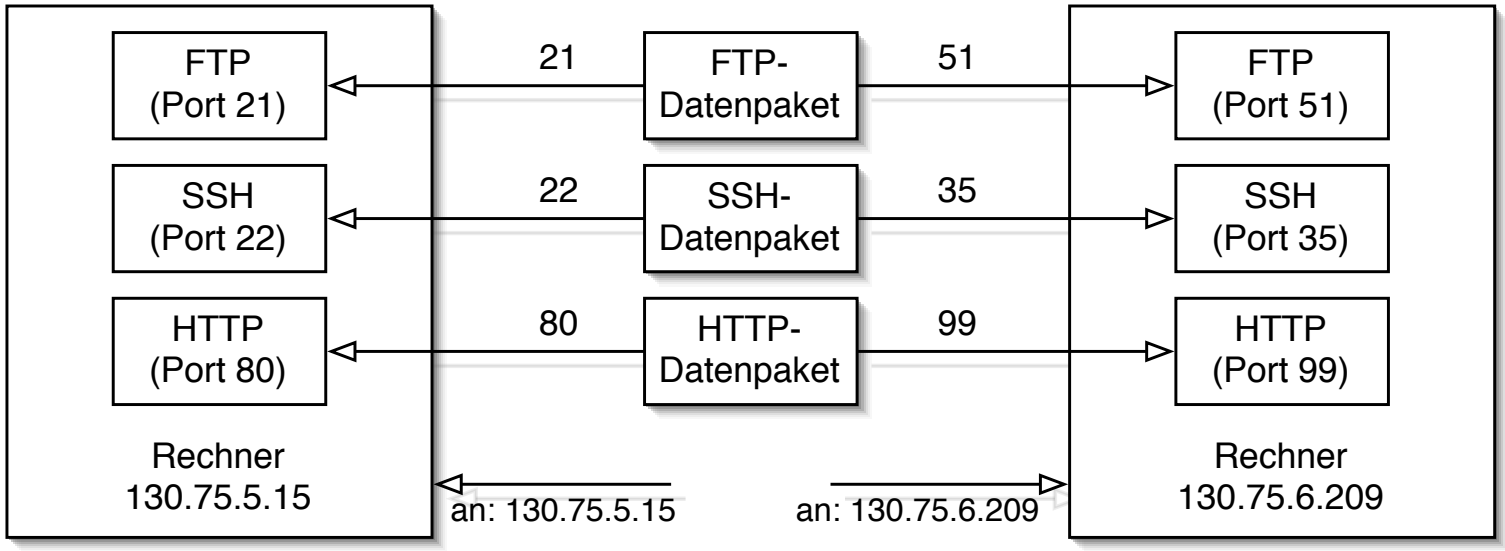
Sicherheitstage Sommer 2005
IPTables und Tripwire

Mark Heisterkamp

8. Juni 2005

Anwendungen und ihre Ports



Ein Datenpaket enthält Absenderadresse, Empfängeradresse und den Port der Anwendung am Zielrechner.

Gewisse Standardports sind bestimmten Anwendungen zugeordnet, können aber dennoch frei gewählt werden.

IPTables

IPTables ist eine Filterfunktion des Kernels unter Linux.

Mittels Regeln wird der Verlauf eines TCP/IP-Datenpaketes beeinflusst. Dabei kann eine Datenpaket entweder

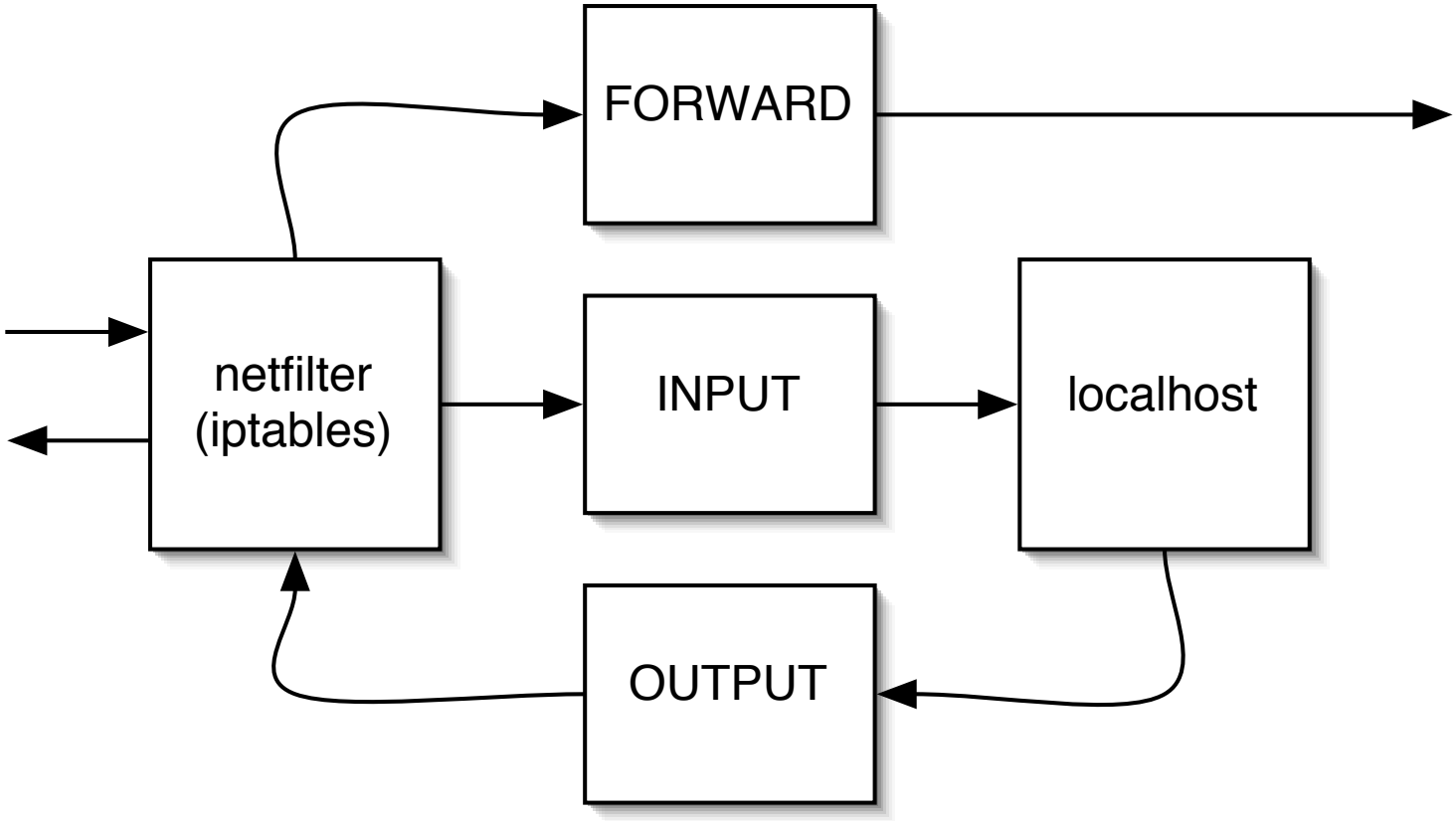
- verworfen (DROP),
- zurückgewiesen (REJECT) oder
- angenommen (ACCEPT)

werden.

Ein Paket durchläuft normalerweise eine von drei möglichen sogenannten *Ketten*:

- FORWARD
- INPUT
- OUTPUT

IPTables



IPTables-Regeln

Eine IPTables-Regel hat den allgemeinen Aufbau:

```
iptables [-t Tabelle] -A <Kette> <Regel>
```

wobei drei Tabellen zur Verfügung stehen:

- filter (Standard)
- mangle
- nat

Über entsprechende Abkürzungen werden dann die Regeln aufgebaut. Wird eine Regel eingegeben, so wird sie *sofort* wirksam.

Regelbeispiel

Das folgende Beispiel für einen Satz Filterregeln sollte als Quasi-Standard am RRZN gelten, sobald ein Server aufgesetzt wird noch bevor er endgültig ans Netz geht:

```
iptables  -L
iptables  -P INPUT DROP
iptables  -P FORWARD DROP
iptables  -A INPUT -m state --state ESTABLISHED \
          -j ACCEPT
iptables  -A INPUT -s 130.75.5.0/255.255.255.0 \
          -p tcp --dport 22 -j ACCEPT
iptables  -A INPUT -s 127.0.01 -i lo -j ACCEPT
```

```
iptables  -A INPUT -p tcp --dport 22 -j ACCEPT
```

Speichern und Laden von Filterregeln

Mittels

```
iptables-save > <DATEI>
```

und

```
iptables-restore < <DATEI>
```

können aktuelle Regeln in `DATEI` gespeichert werden bzw. daraus gelesen werden.

Regelsatz für den Serverbetrieb am RRZN

```
*filter
:INPUT DROP [0:0]
:FORWARD DROP [0:0]
:OUTPUT ACCEPT [0:0]
-A INPUT -m state --state RELATED,ESTABLISHED \
-j ACCEPT
-A INPUT -s 127.0.0.1 -i lo -j ACCEPT
-A INPUT -s 130.75.1.32 -i eth0 -j ACCEPT
-A INPUT -s 130.75.1.40 -i eth0 -j ACCEPT
-A INPUT -s 130.75.5.0/255.255.255.0 -i eth0 -j
ACCEPT
COMMIT
```

Aktives FTP und IPTables

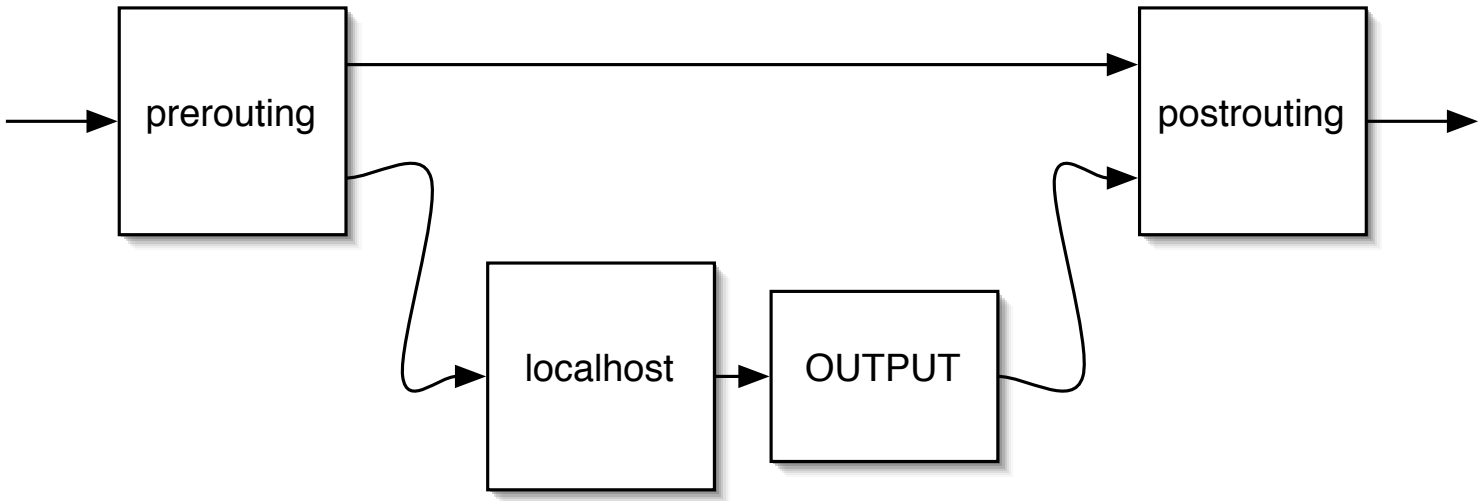
Für den Serverbetrieb kannn es notwendig sein, FTP freizuschalten. Aktives FTP kann allerdings durch die intuitiven Filterregeln allein noch nicht genutzt werden:

```
iptables  -A INPUT -p tcp --dport 21 -j ACCEPT
iptables  -A INPUT -m state
          --state RELATED,ESTABLISHED -j ACCEPT
```

Bei aktivem FTP wird von der Gegenseite bei Kontaktaufnahme eine völlig neue Verbindung aufgebaut, die vom Netfilter nicht als *established* oder *related* erkannt wird. Erst das Kernel-Modul `ip_conntrack_ftp` ermöglicht aktives FTP zusammen mit dem Netfilter.

$\Rightarrow$ `modprobe ip_conntrack_ftp`

Network Address Translation (NAT)



Masquerading (SNAT)

Die Befehle, die notwendig sind, um Masquerading zu aktivieren, lauten:

```
echo "1" > /proc/sys/net/ipv4/ip_forward
iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
```

Tripwire

Tripwire ist ein Programm, das aufgrund von Zeitstempeln, Größenveränderungen und ähnlichen Details vorgegebene Dateien überwacht und gegebenenfalls Alarm auslöst, falls Änderungen aufgetreten sind.

Der Vergleichszustand ist in einer Datenbank eingefroren und sollte unveränderlich gespeichert werden. Wird das überwachte System durch administrative Pflege verändert, so muss unter Umständen auch die Datenbank neu erzeugt werden.

Tripwire existiert in einer kostenpflichtigen und einer kostenlosen Version. Ich beziehe mich auf die kostenlose Variante die unter

http://www.tripwire.org

erhältlich ist.

Tripwire-Installation

Die Tripwire-Installation besteht im Wesentlichen aus drei Schritten:

1. Definition der Default-Policy (`twpol.txt`) aller überwachten Dateien, Verzeichnisse, Meldeadressen etc.
2. Initialisierung der Datenbank
   `tripwire --init`
3. Systemcheck, beispielsweise per Cron-Dämon
   `tripwire --check`

Um die Default-Policy zu erstellen, können vorgefertigte Skripte genutzt werden, die die Arbeit erheblich erleichtern.

Wartung

Sollte durch Updates oder andere Veränderungen des Systems die Datenbank veralten, so muss mittels `tripwire --init` die Datenbank neu initialisiert werden.

Es empfiehlt sich aus Sicherheitsgründen, die Datenbank auf einen anderen Rechner bzw. ein ausschließlich lesbares Medium auszulagern. Entsprechende Tests stehen am RRZN noch aus.

Nützliche Webadressen:

- `www.tripwire.org`
- `www.rrze.uni-erlangen.de/dienste/arbeiten-rechnen/linux/sicherheit/policy.tgz`
- `www.rrze.uni-erlangen.de/dienste/arbeiten-rechnen/linux/sicherheit/tripwire.shtml`