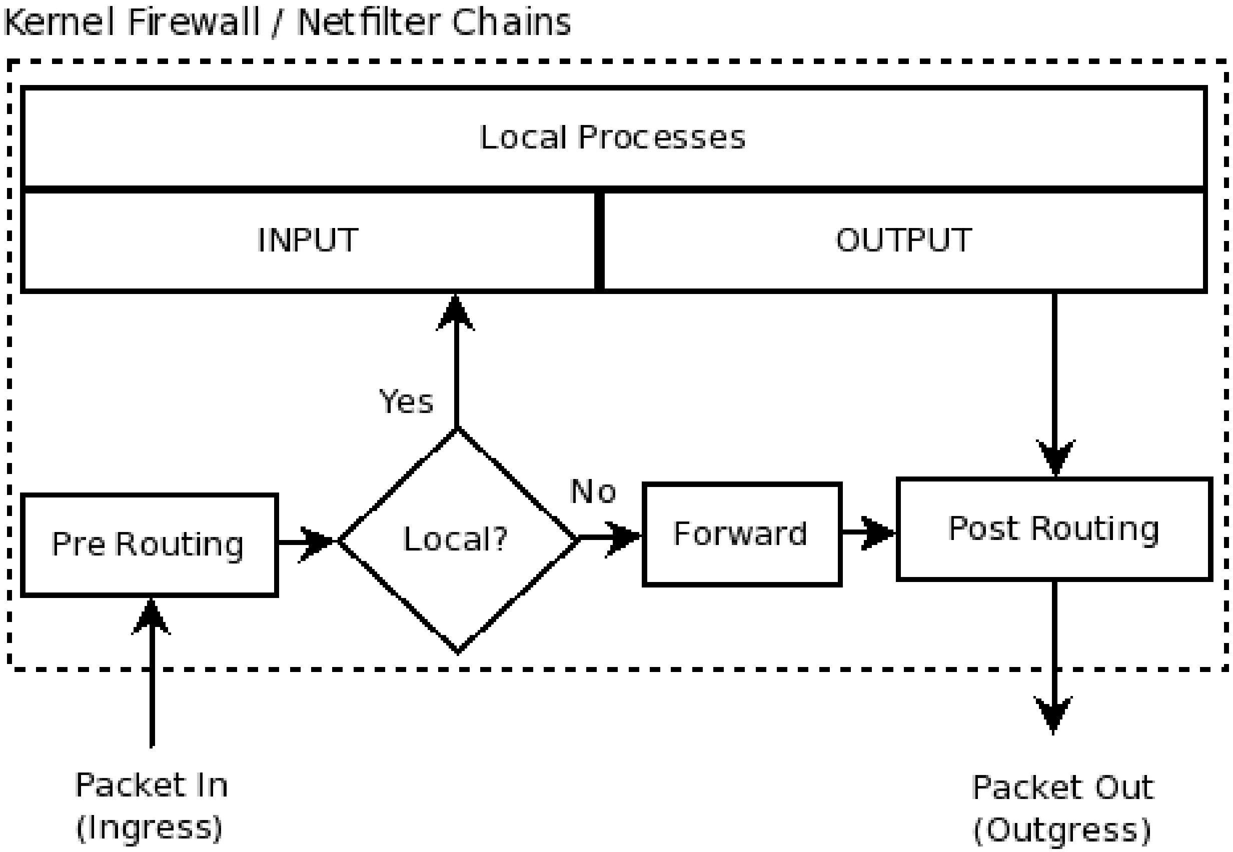
Technische Universität Berlin

IPv4 - iptables

Training for Afghan System Administrators

How packet filtering with iptables works (simplified)



Questions

What are chains?

Why is the chain order important?

What is a chain policy?

What is a target? Which defaults targets are there?

Important iptables options and switches

`-j`	`Specifies the target (--jump)`
`-i`	`Specifies the input interface (--in-interface)`
`-o`	`Specifies the output interface (--out-interface)`
`-p`	`Specifies the protocol (--proto)`
`-s`	`Specifies the source address (--source)`
`-d`	`Specifies the destination address (--destination)`
`--source-ports`	`Specifies the source ports`
`--destination-ports`	`Specifies the destination ports`
`-P`	`Specifies the default policy of the chain (TARGET)`
`--mac-source`	`Specifies the mac address`
`!`	`Inverts the sense of the filter rule (match addresses NOT equal to)`

Examples

```
iptables -A INPUT -p tcp -j ACCEPT
iptables -A INPUT -s 10.1.1.25 -p tcp --destination-port 23 -j DROP
iptables -A INPUT -s 10.1.1.25 -p tcp ! --destination-port 23 -j DROP
iptables -A INPUT -s 10.1.1.0/24 -p tcp --destination-port 23 -j DROP
Iptables -A FORWARD ! -o eth2 -j DROP
iptables -A FORWARD -s 10.1.1.25 -j DROP
iptables -A FORWARD -p tcp -s 192.168.10.0/255.255.255.0 --dport 80 -j REJECT
```

Excercises

1. Reject all ftp connections to the Internet from the local host!
2. Reject all incoming ssh connections to the host!
3. Reject all DNS connections to 130.149.17.4 (UDP)!
4. Reject all Yahoo Messenger connections from your host to the Internet!
5. Reject all NTP connections (time server) from your host to the Internet, but allow to the TU Berlin time server (times.tubit.tu-berlin.de)!