Firewalling v Linuxe

Úloha firewallu

- na koncovom počítači
  - obmedzenie prístupnosti sieťových služieb
  - obmedzenie odchádzajúcej komunikácie
- na routeri
  - obmedzenie komunikácie medzi sieťami
  - network address translation (NAT)
    - umožnenie komunikácie zo siete so súkromnými (neroutovateľnými) adresami

Delenie firewallov

- stateless firewall
  - každý paket posudzuje samostatne
    - na základe hlavičiek sieťovej a transportnej vrstvy
  - nenáročný na výkon a pamäť
  - len jednoduchá politika
- stateful firewall
  - udržiava si prehľad o „spojeniach“
  - náročnejší na pamäť a CPU
  - umožňuje zložitejšiu politiku

Firewall v Linuxe

- súčasť jadra (kernelu) systému
  - subsystém **netfilter**
- stateful firewall
  - implementuje connection tracking
    - TCP, UDP
    - pomocné moduly pre niektoré „problematické“ aplikačné protokoly (napr. FTP)
- aj stateless firewall
  - bez využitia connection tracking-u

Firewall v Linuxe

- činnosť riadená tabuľkami (IP tables)
  - filter
    - filtrovanie paketov
  - nat
    - realizácia NAT
  - mangle
    - manipulácia s niektorými atribútmi paketov

Firewall v Linuxe

- tabuľka obsahuje reťaze (chains) pravidiel
  - filter
    - INPUT – pre prichádzajúce pakety
    - OUTPUT – pre odchádzajúce pakety
    - FORWARD – pre prechádzajúce pakety
  - nat
    - PREROUTING – pred routovaním (prechádzajúce pakety)
    - OUTPUT – odchádzajúce pakety pre routovaním
    - POSTROUTING – po routovaní
  - reťaze je možné pridávať

Firewall v Linuxe

- reťaze obsahujú pravidlá
  - test
  - cieľ
    - ACCEPT – paket posunúť na ďalšie spracovanie
    - DROP – paket zahodiť
    - meno administrátorom definovanej reťaze
      - pokračovať pravidlami v uvedenej reťazi
    - RETURN – pokračovať v predchádzajúcej reťazi
    - ďalšie
- preddefinované reťaze majú default cieľ

Firewall v Linuxe

- použitie pravidiel
  - ak test sedí, použije sa uvedený cieľ
  - ak test nesedí, použije sa ďalšie pravidlo
  - na konci administrátorom definovanej reťaze sa použije ďalšie pravidlo predchádzajúcej reťaze
  - na konci preddefinovanej reťaze sa použije default cieľ

Firewall v Linuxe

- príkaz `iptables`
  - `-t tabuľka` – tabuľka, ktorá sa má použiť
  - `-A reťaz pravidlo` – pridá pravidlo na koniec reťaze
  - `-I reťaz [poradie] pravidlo` – vloží pravidlo
  - `-D reťaz poradie` – vymaže pravidlo
  - `-L [reťaz]` – vypíše pravidlá
  - `-F [reťaz]` – vymaže všetky pravidlá
  - `-N reťaz` – definuje reťaz

Firewall v Linuxe

  - `-X [reťaz]` – zruší reťaz
  - `-P reťaz cieľ` – nastaví default cieľ
- pravidlá (! neguje test)
  - `-p [!] protokol` – protokol trasportnej vrstvy
  - `-s [!] adresa/maska` – zdrojová IP adresa
  - `-d [!] adresa/maska` – cieľová IP adresa
  - `-i [!] interface` – vstupný interface
  - `-o [!] interface` – výstupný interface
  - `-j cieľ` – cieľ pravidla

Firewall v Linuxe

- rozšírenie testov pre protokol tcp
  - `--sport [!] port[:port]` – zdrojový port, rozsah portov
  - `--dport [!] port[:port]` – cieľový port, rozsah portov
  - `--tcp-flags [!] mask hodnota`
    - SYN, ACK, FIN, RST, URG, PSH, ALL, NONE
  - `[!] --syn`
    - --tcp-flags SYN,RST,ACK,FIN SYN

Firewall v Linuxe

- rozšírenie testov pre protokol udp
  - `--sport [!] port[:port]` – zdrojový port, rozsah portov
  - `--dport [!] port[:port]` – cieľový port, rozsah portov

Firewall v Linuxe

- rozšírenie testov pre stateful firewall
  - `-m state` – zavedenie rozširujúceho modulu state
  - `--state stav` – testuje stav spojenia
    - NEW – nový paket – začiatok spojenia
    - ESTABLISHED – paket je súčasťou existujúceho spojenia
    - RELATED – paket je začiatkom očakávaného spojenia
    - INVALID – neidentifikovateľný paket

Firewall v Linuxe

- ďalšie ciele
  - `REJECT [--reject-with typ]` – zahodí paket a pošle ICMP paket s typom chyby
    - icmp-net-unreachable
    - icmp-host-unreachable
    - icmp-port-unreachable
    - icmp-proto-unreachable
    - icmp-net-prohibited
    - icmp-host-prohibited
    - icmp-admin-prohibited

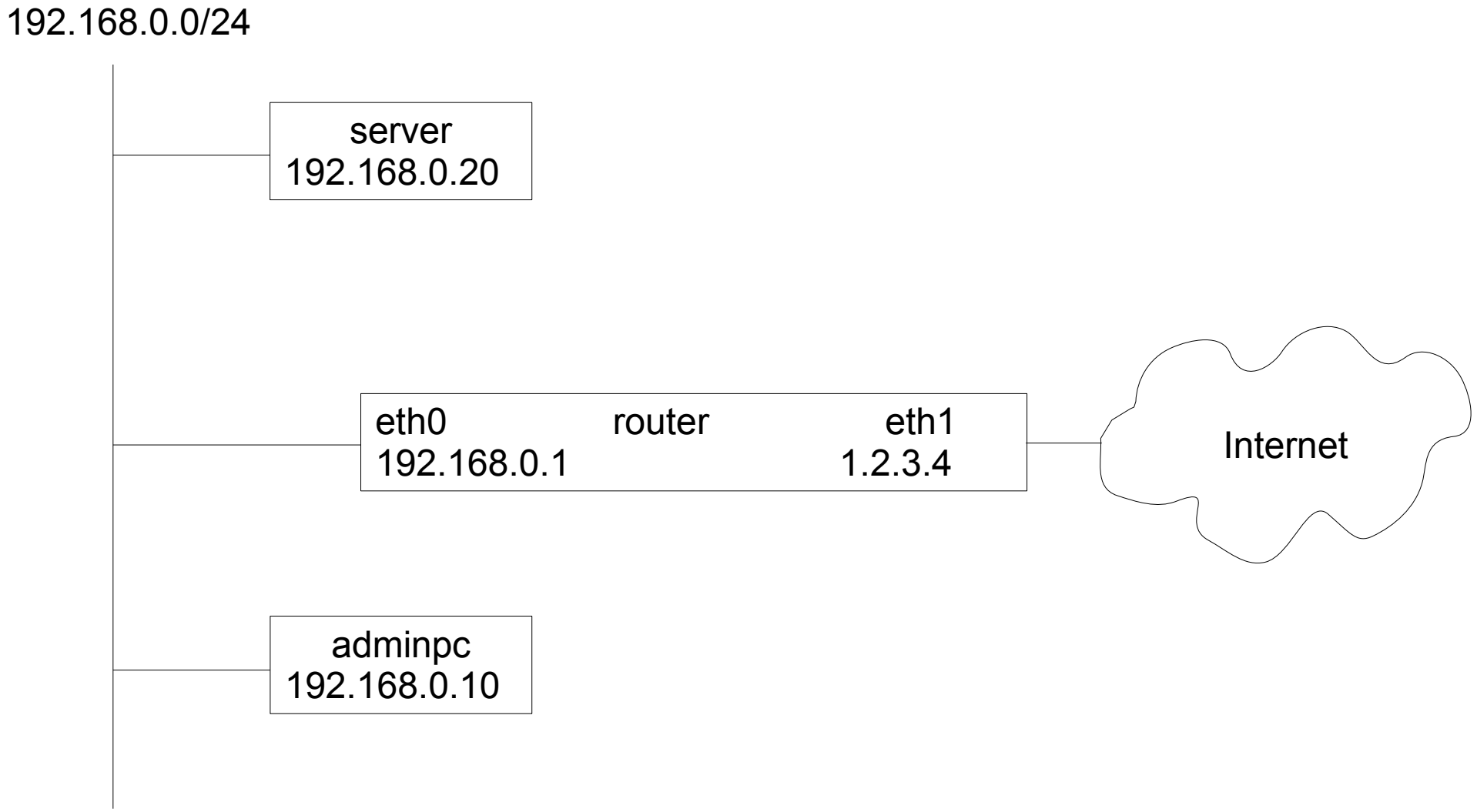
Firewall v Linuxe

- `REDIRECT [--to-ports port[-port]]`
  - presmeruje paket na vlastnú adresu na uvedený port (rozsah portov)
  - používa sa na realizáciu transparentných (neviditeľných) proxy serverov
- `SNAT –to-source ipaddr[-ipaddr]`
  - prepíše zdrojovú adresu (v POSTROUTING v nat)
  - ďalšie pakety spojenia sú prepisované rovnako/inverzne
- `DNAT –to-destination ipaddr`
  - prepíše cieľovú adresu (PREROUTING, OUTPUT v nat)
  - ďalšie pakety spojenia sú prepisované rovnako/inverzne

Príklad – ochrana počítača

```
iptables -F
iptables -P INPUT DROP
iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
iptables -A INPUT -p tcp --dport 22 -s 192.168.0.0/24 -j ACCEPT
iptables -A INPUT -p tcp --dport 80 -j ACCEPT
```

Príklad – router



Príklad – router

```
iptables -F
iptables -X
iptables -N odchadzajuce
iptables -N server
iptables -P FORWARD DROP
iptables -P INPUT DROP
iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
iptables -A INPUT -s 192.168.0.10 -p tcp --dport 22 -j ACCEPT
iptables -A FORWARD -s 192.168.0.0/24 -i ! eth0 -j DROP
iptables -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT
iptables -A FORWARD -d 192.168.0.20 -j server
iptables -A FORWARD -s 192.168.0.0/24 -j odchadzajuce
iptables -A odchadzajuce -p tcp --dport 25 -j DROP
iptables -A odchadzajuce -j ACCEPT
iptables -A server -p tcp --dport 80 -j ACCEPT
iptables -A server -p tcp --dport 443 -j ACCEPT
iptables -A server -p udp --dport 53 -j ACCEPT
iptables -A server -p tcp --dport 53 -j ACCEPT
```

Príklad – router

```
iptables -t nat -F
iptables -t nat -A POSTROUTING -s 192.168.0.0/24 -o eth1 -j SNAT
  --to-source 1.2.3.4
iptables -t nat -A PREROUTING -p tcp --dport 80 -j DNAT
  --to-destination 192.168.0.20
iptables -t nat -A PREROUTING -p tcp --dport 443 -j DNAT
  --to-destination 192.168.0.20
iptables -t nat -A PREROUTING -p tcp --dport 53 -j DNAT
  --to-destination 192.168.0.20
iptables -t nat -A PREROUTING -p udp --dport 53 -j DNAT
  --to-destination 192.168.0.20
```