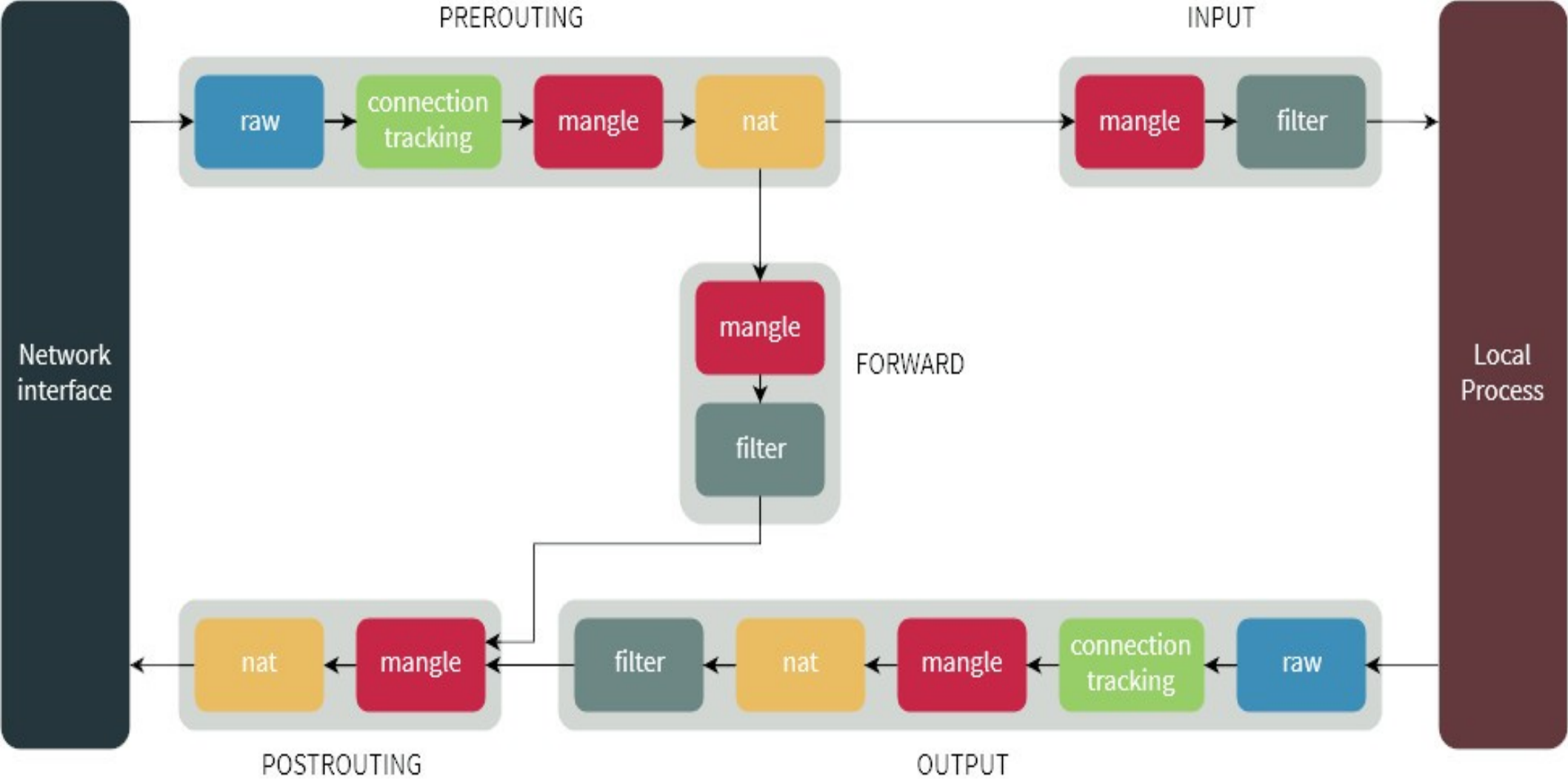
Firewall (ohňova scena?)

kriza (Richard Staňa)
kr1za.github.io/
UPJŠ - AOS

iptables

netfilter.org is home to the software of the packet filtering framework inside the Linux 2.4.x and later kernel series. Software commonly associated with netfilter.org is iptables.

Software inside this framework enables packet filtering, network address [and port] translation (NA[P]T) and other packet mangling. It is the re-designed and heavily improved successor of the previous Linux 2.2.x ipchains and Linux 2.0.x ipfwadm systems.



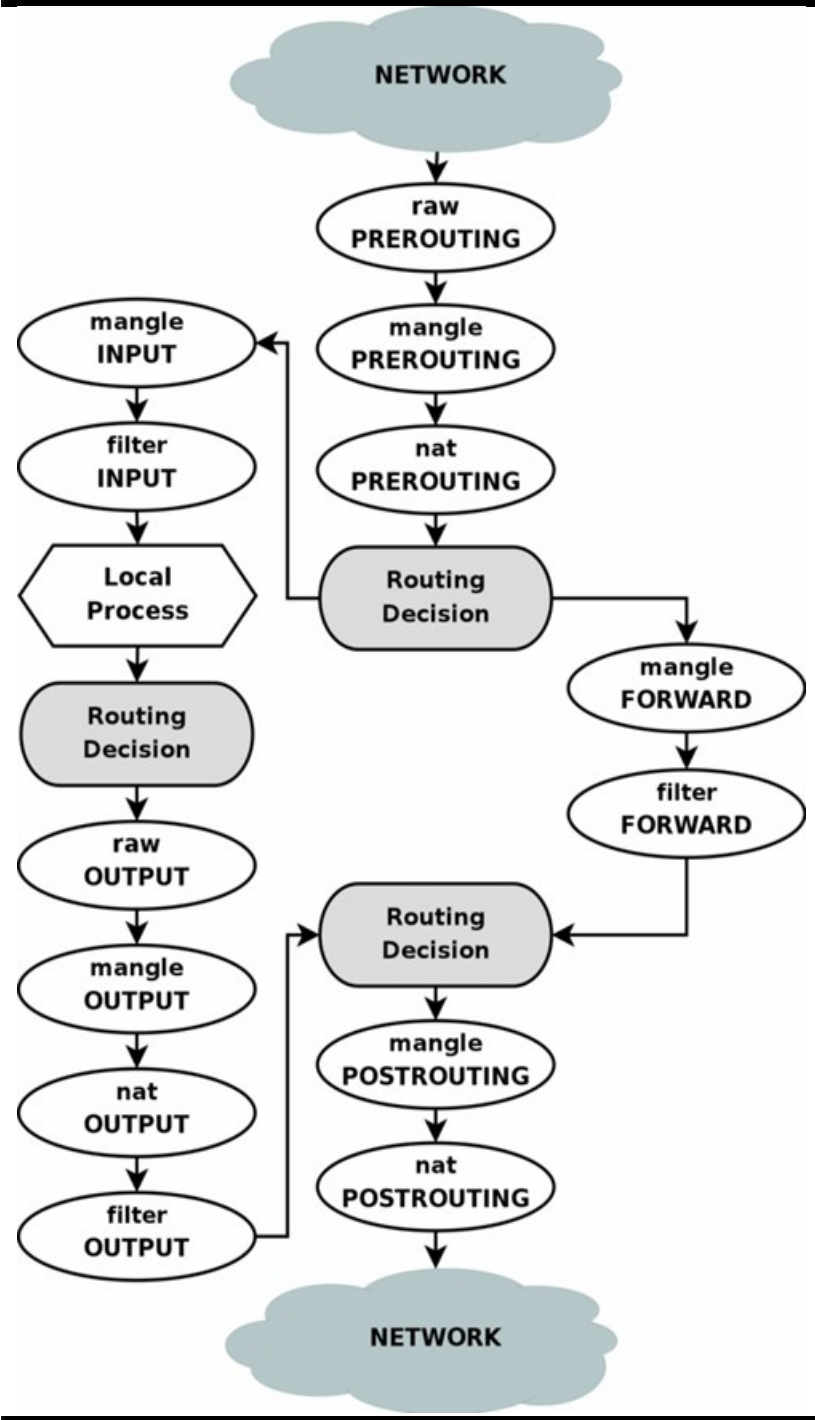
filter – je východzia tabuľka určená na uchovávanie pravidiel filtrovania paketov

nat – je tabuľka používaná len paketmi vytvárajúcimi nové spojenie

mangle – je tabuľke na špeciálnu manipuláciu s paketmi

raw – je tabuľka na výnimky zo sledovania stavu a je spracovaná ako prvá.

https://www.booleanworld.com/depth-guide-iptables-linux-firewall/



Reťaze čo?

Štandardne pracujeme s tabuľkou filter!

Čo môžeme nastavovať?

- Tabuľku
- Reťazec
- Adresu
- Port
- Zariadenie
- iptables can use extended packet matching modules. These are loaded in two ways: implicitly, when -p or --protocol is specified, or with the -m or --match options, followed by the matching module name
  - -m napr Stav
- ...

Take stavy, ...

- NEW: first package of any new connection
- ESTABLISHED: at least one reply has been sent to the NEW package for this connection. All other now have ESTABLISHED state.
- RELATED: packets are connected to another connection (e.g., FTP data traffic could be related to the control traffic)
- INVALID: means that iptables is confused
- UNTRACKED: the packet was marked as NOTRACK in the raw table

Poďme sa hrať

- Na klientovi nainštalujeme ssh server
- Otestujeme, zakážeme, povolíme, ...

The policy defines the target for packets that get to the end of the chain.

DROP

- Všetko zahodím
- Výhody?
- Nevýhody?

ACCEPT

- Všetko povolím
- Výhody?
- Nevýhody?

Poďme sa hrať

- iptables -P/--policy INPUT/FORWARD/OUTPUT DROP/ACCEPT
- iptables -t názov -S -v alebo iptables -t názov -L -n -v –line-numbers
  - -t/--table ktorá tabuľka
  - -S/--list-rules vypíš všetky pravidlá vo vybranom reťazci
  - -v/--verbose buď ukecaný
  - -L/--list vypíš všetky pravidlá vo vybranom reťazci
  - -n/--numeric numericky formát namiesto hostname, servisu, ...
  - --line-numbers čísla riadkov

iptables [tabuľka] [operácia] <reťazec> [pravidlo]

- iptables [-t table] {-A|-C|-D} chain rule-specification
- ip6tables [-t table] {-A|-C|-D} chain rule-specification
- iptables [-t table] -I chain [rulenum] rule-specification
- iptables [-t table] -R chain rulenum rule-specification
- iptables [-t table] -D chain rulenum
- iptables [-t table] -S [chain [rulenum]]
- iptables [-t table] {-F|-L|-Z} [chain [rulenum]] [options…]
- iptables [-t table] -N chain
- iptables [-t table] -X [chain]
- iptables [-t table] -P chain target
- iptables [-t table] -E old-chain-name new-chain-name
- rule-specification = [matches...] [target]
- match = -m matchname [per-match-options]
- target = -j targetname [per-target-options]

-A –append, -C –check, -D –delete, -I –insert, -R – replace, -L –list, -F –flush, ...

Poďme sa hrať

- Pokašlali sme to?
  - iptables -F
- Čo potrebujeme pre základné internety?

Vlastné reťazce

- iptables -N whitelist
- iptables -N blacklist

Logovanie

- iptables -A INPUT -s 10.0.0.0/8 -j LOG --log-prefix "Log-test: "

Modul Limit

- Tento modul rozširuje pravidlá o možnosť limitovania počtu paketov za nejakú časovú jednotku.
  - iptables –A <reťazec> -m limit –limit <časová jednotka > -limit-burst <číslo>
    - --limit rate[/sekunda|/minúta|/hodina|/deň]
      - Maximálna priemerna zodpovedajúca rýchlosť
      - defaultne sú 3 hodiny.
    - --limit-burst číslo
      - Maximálny počiatočný počet packetov, ktoré zodpovedajú
      - defaultne je 5 packetov
- iptables -A INPUT -p icmp --icmp-type echo-request -m limit --limit 1/s --limit-burst 10 -j ACCEPT

Porty len po jednom??

- iptables –A <reťazec> –p <tcp,udp> -m multiport --sports <port, port:port>
- iptables –A <reťazec> –p <tcp,udp> -m multiport --dports <port, port:port>
- iptables –A <reťazec> –p <tcp,udp> -m multiport --sports ! <port, port:port>
- iptables –A <reťazec> –p <tcp,udp> -m multiport --dports ! <port, port:port>

Tento modul možno použiť len v spojení s podmienkou –p tcp –p udp (nemožno definovať port, ak nemáme zadefinovaný protokol tcp alebo udp).

Čo urobí reštart?

To fakt?? Znova?? WF*?

Čo urobí reštart?

- iptables-save > /etc/iptables.rules

  /etc/network/interfaces pridáme riadok:

- pre-up iptables-restore < /etc/iptables.rules

?Otázky?