Firewall, mac filtering, address filtering, port forwarding, dmz

Ondřej Vojtíšek, Jakub Niedermertl

Firewall obecně

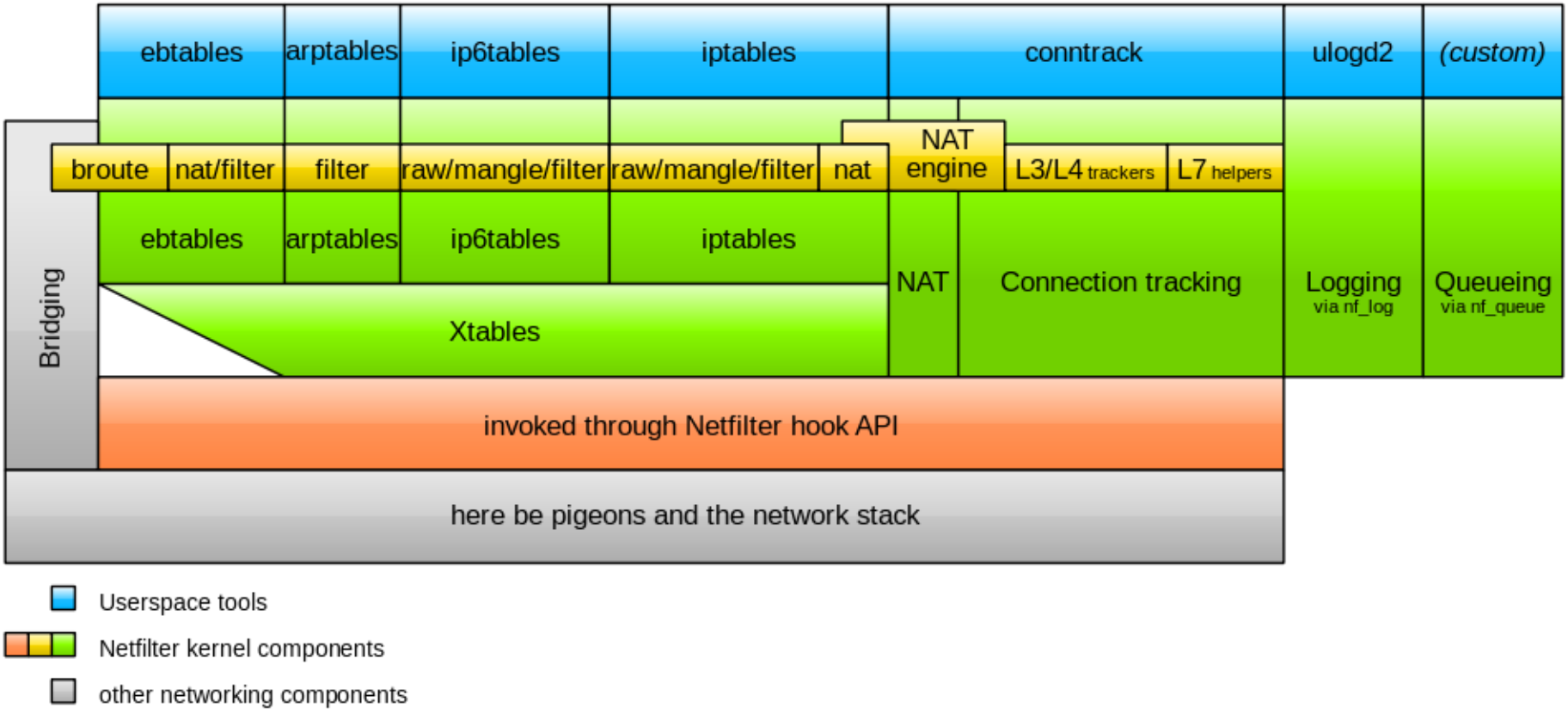
- Síťový HW/SW prvek, který slouží k zabezpečení/omezení komunikace vedené mezi částmi počítačové sítě
- Rozdělení:
  - Paketové / aplikační (IPS) / proxy firewall
  - Stateful / stateless
- Příklady firewallů:
  - unix: ipfw, ipchains, netfilter, ...
  - windows: Comodo, ZoneAlarm, ...

Netfilter

- framework umožňující filtrování paketů a překlad adres a portů (NAT)
- userspace aplikace a moduly do jádra
- iptables, ip6tables, ebtables, ...
- iptables-save, iptables-restore

Netfilter components

Jan Engelhardt, last updated 2011-03-05 (initial: 2008-06-17)

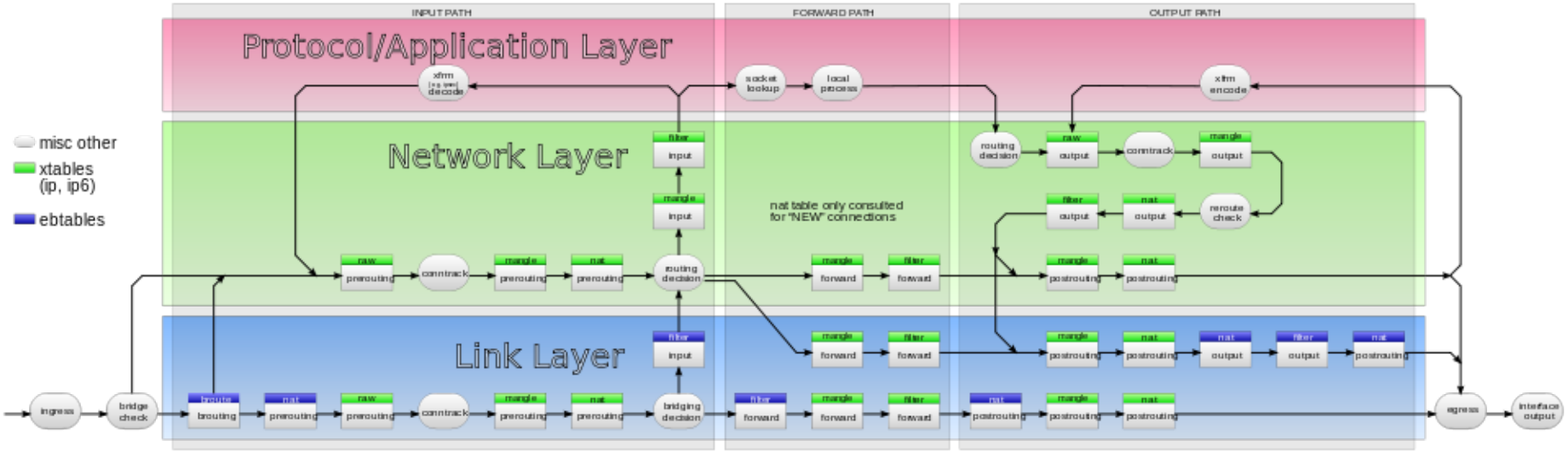


Zpracování paketu

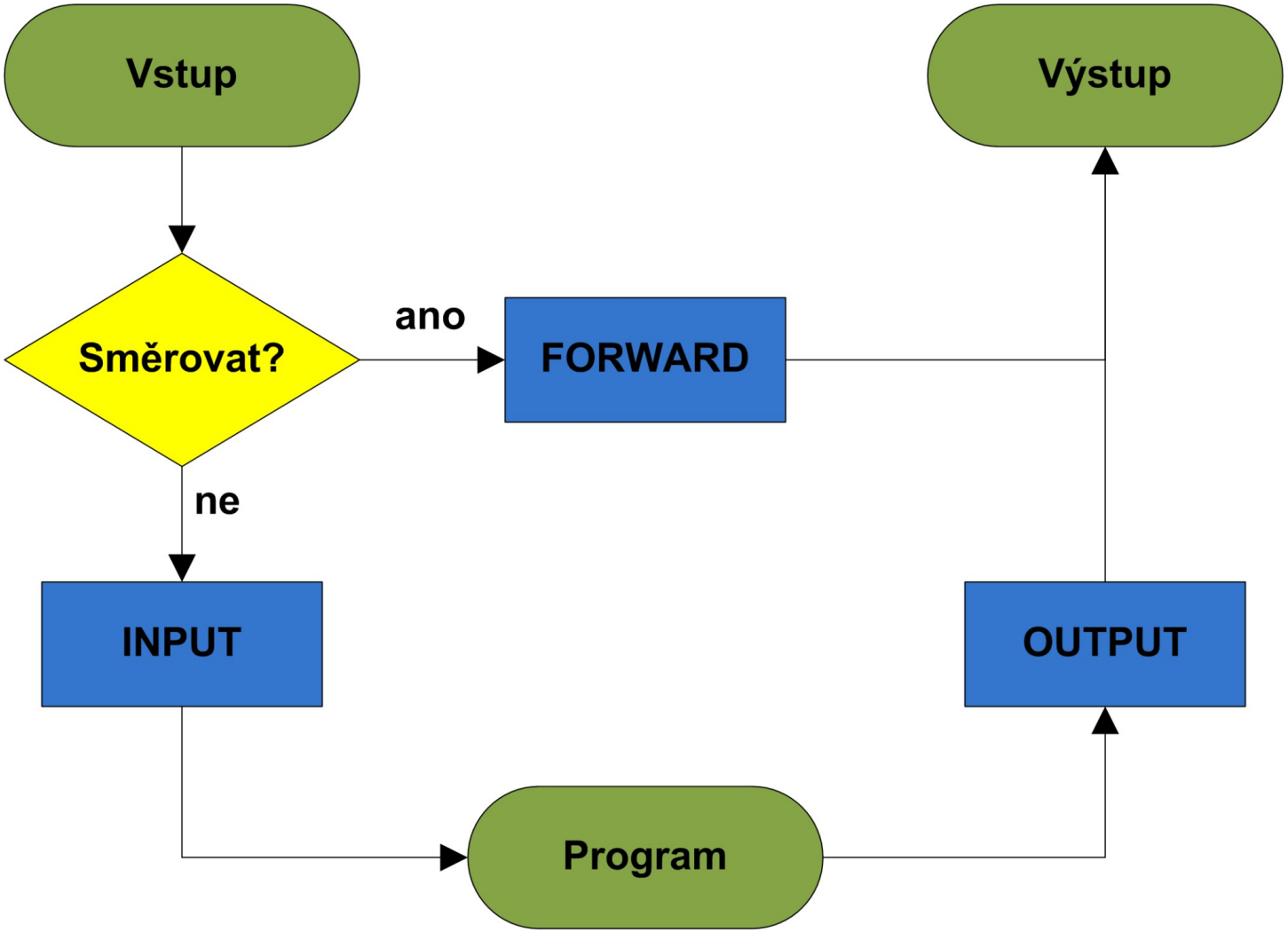
- tabulky a předefinované chainy
  - filter: INPUT, FORWARD, OUTPUT
  - nat: PREROUTING, POSTROUTING, OUTPUT
  - mangle: PREROUTING, INPUT, FORWARD, OUTPUT, POSTROUTING
  - raw: PREROUTING, OUTPUT
- pro každý paket je vyvoláván seznam chainů dokud paket neprojde systémem nebo není zahozen

Netfilter packet flow; hook/table ordering

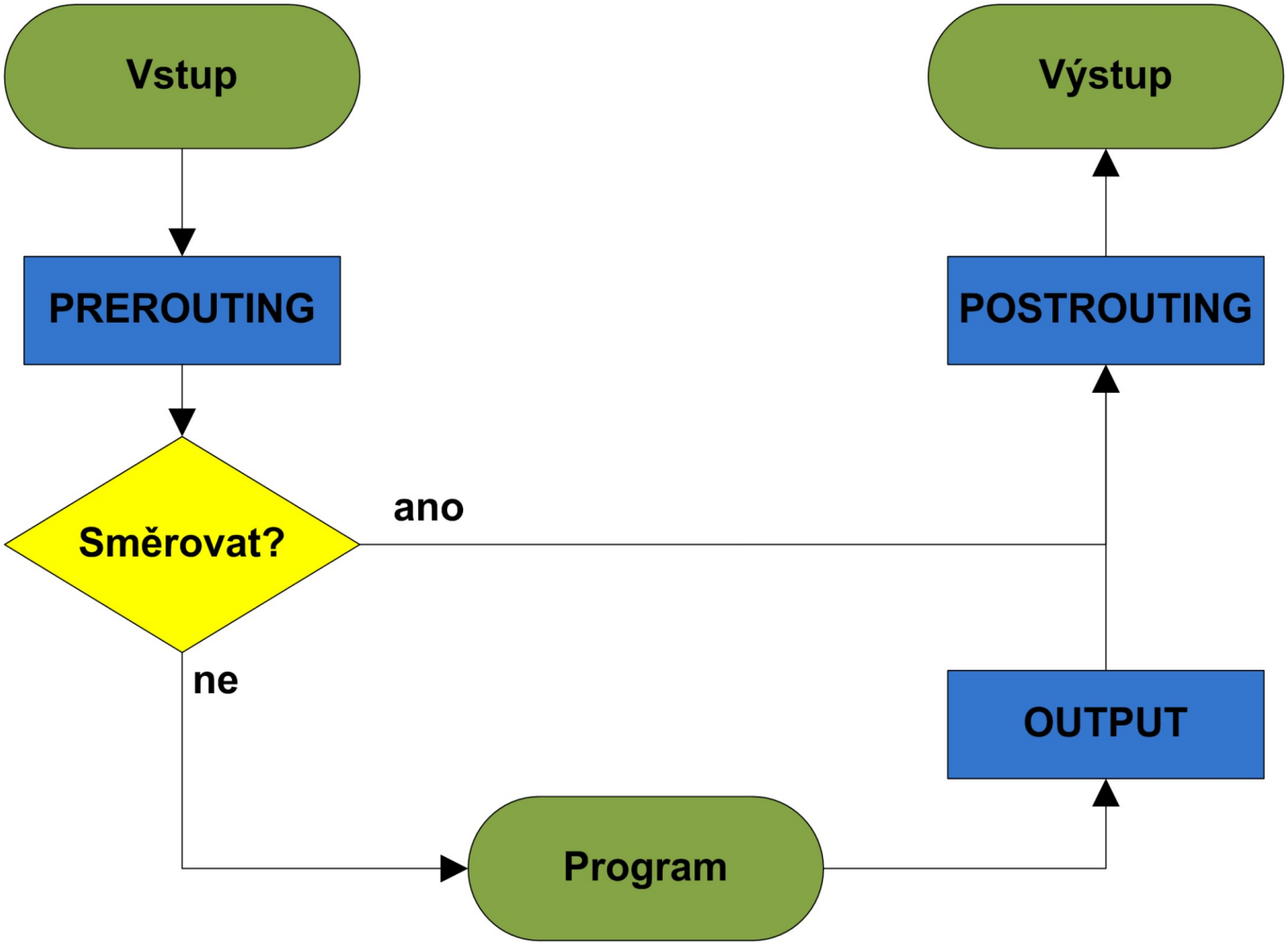
by Jan Engelhardt, last updated 2011-Dec-18
based in part on Joshua Snyder's graph



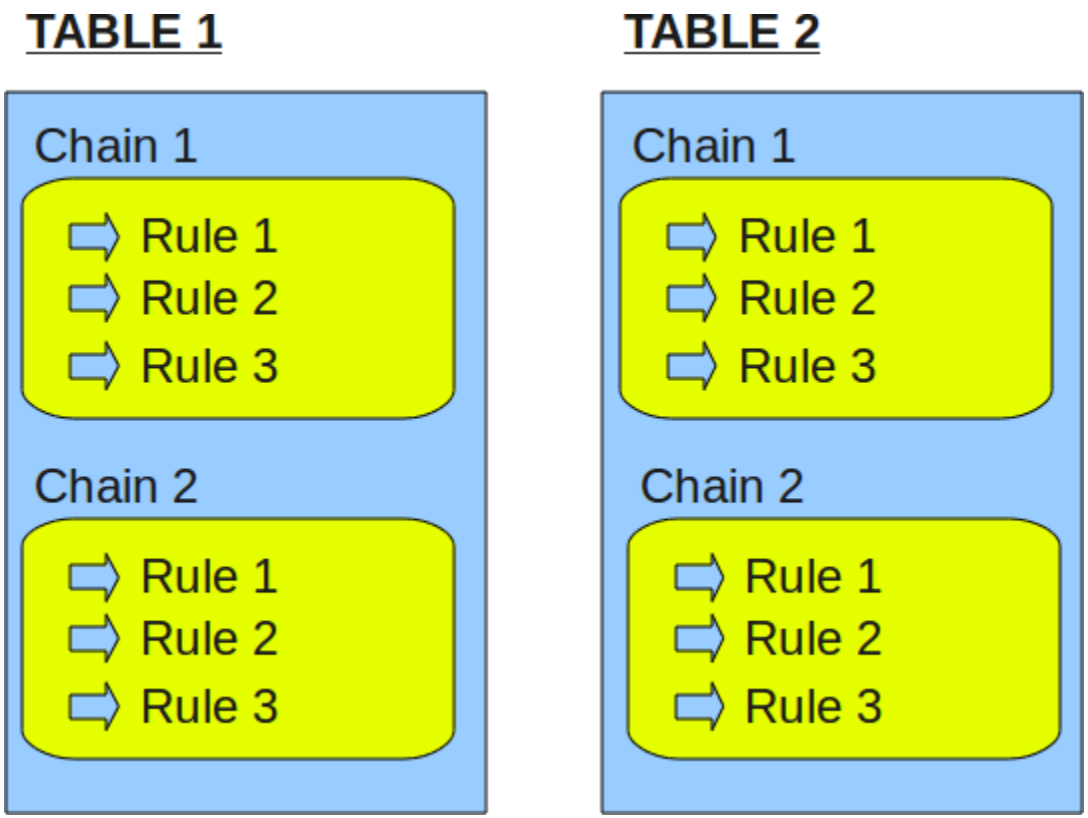
Funkce tabulky filter



Funkce tabulky nat



Logická struktura iptables



Chains

- seznam pravidel
- pravidla jsou procházena sekvenčně
- předdefinované, možnost přidat vlastní
- chain jako funkce
  - vrací ACCEPT, DROP nebo REJECT
- polices - výchozí návratová hodnota
- výchozí konfigurace iptables - povolit vše
- vnořování chainů
  - --jump <chain_name>
  - --goto <chain_name>
  - --jump RETURN

Pravidla

- obecný tvar:
  - podmínka + cíl
  - cíl se provede, pokud je splněna podmínka, pokračuje se dalším pravidlem
  - iptables [tabulka] [akce] [chain] [match] [cíl] [detaily cíle]
- příkazy provádí řádkovou editaci chainu
- ladění
  - počítadla: `iptables -L -v , iptables -Z`
  - logování: `iptables -t filter -A INPUT -p tcp -j LOG --log-prefix "INPUT packets"`

Packet matching

- aktivace rozšíření -p <protokol>, -m <modul>
- podmínky svým vyhodnocováním mohou měnit stav, proto pravidlo nemusí obsahovat cíl
- více podmínek spojeno logickým AND
- negace '!'
- základní podmínky
  - -p <protokol>
  - -s <source_address>
  - -d <destination_address>
  - -i <input_interface>
  - -o <output_interface>

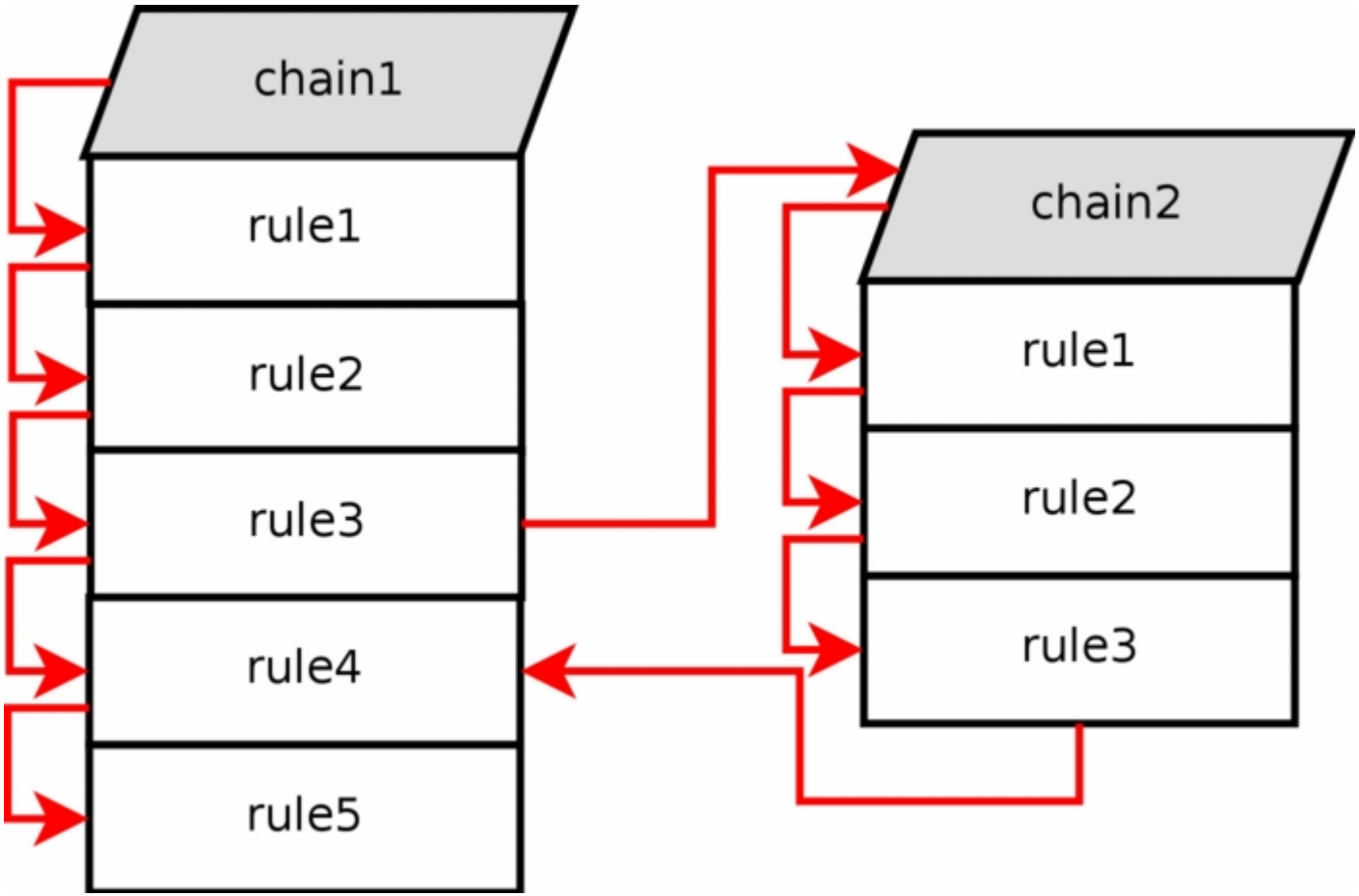
Packet matching II

- rozšiřující moduly
  - time, limit, iprange, ...
- příklady
  - `iptables -A INPUT -m time --timestart 8:00 --timestop 18:00 --days Mon,Tue,Wed,Thu,Fri -j ACCEPT`
  - `iptables -A INPUT -i eth0 -p ! tcp -j DROP`

Cíle

	zastavuje prochazení	omezení dostpnosti
ACCEPT	✔	
DROP	✔	
REJECT	✔	
LOG		
RETURN		
QUEUE		
SNAT		nat / POSTROUTING
DNAT		nat / PREROUTING, OUTPUT
MASQUERADE		nat / POSTROUTING
<chain_name>		

Subchains


chain1
rule1
rule2
rule3
rule4
rule5
chain2
rule1
rule2
rule3

Address filtering

- založeno na IP nebo na MAC adresách
- IP adresy mohou být zadány přímo nebo rozsahem (modul iprange)
- příklady:
  - `iptables -A INPUT -i eth0 -s 192.168.0.2 -j ACCEPT`
  - `iptables -A INPUT -p tcp -m iprange --dst-range 192.168.0.1-192.168.0.10 -j ACCEPT`

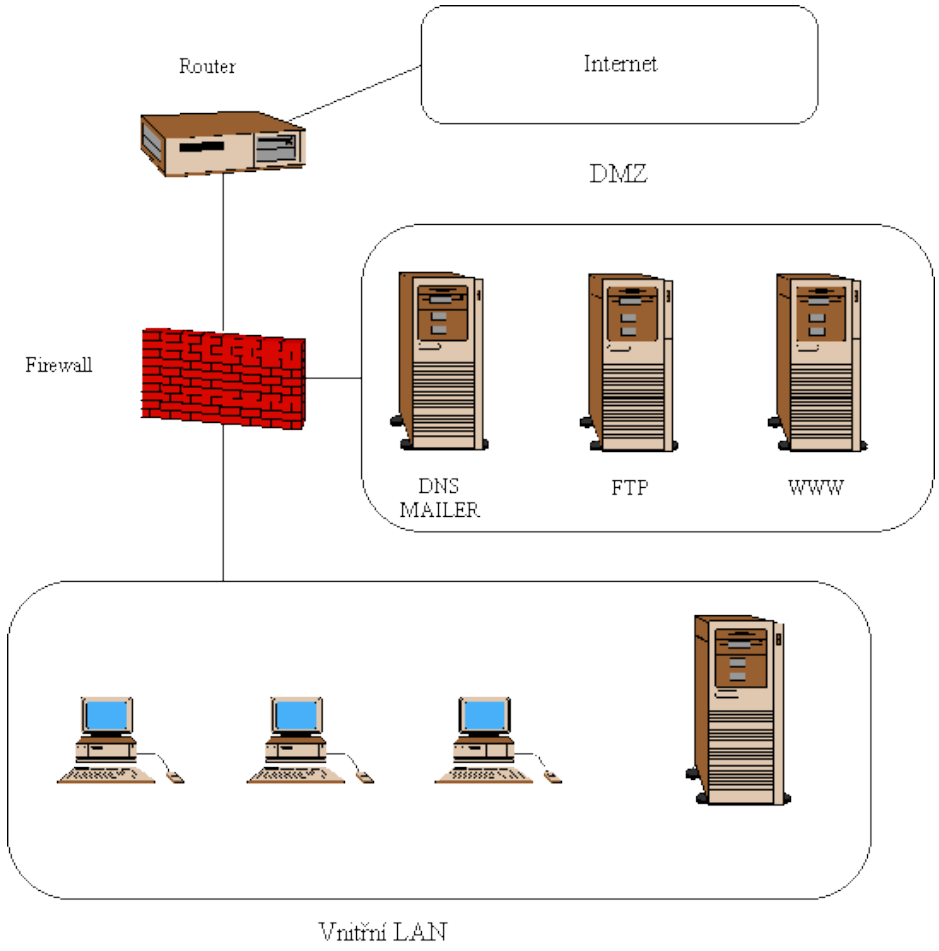
MAC filtering

- blacklist / whitelist resp. allow / deny list
- problémem je jednoduchá změna MAC adresy
  - nástroj pro hacking této formy zabezpečení - airodump-ng
- zabezpečení na L2 - smysl pouze pro LAN
- příklady:
  - `iptables -A INPUT -m mac –mac-source 00:01:02:03:04:05 -j ACCEPT`

Port forwarding

- pevné přesměrování komunikace z vnějšku na vybraném portu na zvolený vnitřní stroj a jeho port
- příklad použití (HTTP, SSH, FTP server)
- port triggering
  - dynamické přesměrování portů
  - iniciováno komunikací vnitřního stroje na zvoleném portu
- příklady:
  - `iptables -A PREROUTING -p tcp -m tcp -d $wan_ip --dport $wan_port -j DNAT --to-destination $lan_ip:$lan_port`
  - `iptables -A POSTROUTING -p tcp -m tcp -s $lan_ip --sport $lan_port -j SNAT --to-source $wan_ip`

DMZ (DeMilitarized Zone)



DMZ II

- oddělená podsíť volně přístupná z vnější sítě
- účel
  - poskytování veřejně přístupných služeb
  - server předsazený firewallu
  - FTP, HTTP, SNMP, ...

- honeypot
  - podobný princip - oproti DMZ neobsahuje nic cenného
  - nechráněná neaktivní stanice zaznamenávající průniky

Použité zdroje

- http://www.root.cz/serialy/vse-o-iptables/
- http://wiki.openwrt.org/doc/uci/firewall
- http://www.osu.cz/~jura/doc/iptables.pdf
- man iptables
- http://en.wikipedia.org/wiki/Netfilter
- http://www.faqs.org/docs/iptables
- studijní materiály do předmětu PA160 (autorem je RNDr. Tomáš Rebok, Ph.D.)

Otázky

Děkujeme za pozornost.