



SPS

Firewall a iptables a nftables



<https://www.bit.nl/news/115/88/Cut-here-to-activate-firewall-layer-1-firewalls-op-OHM2013>



- A firewall is a hardware or software device which is configured to permit, deny, or proxy data through a computer network which has different levels of trust.
- Jiná definice - firewall je software, který na základě znalosti protokolů a pravidel umí manipulovat s průchozími daty.



- Firewall
- Packet filter
- Stateful filter
- Proxy

- Router
- NAT



- Paket dorazí na vstupní rozhraní
- Automat rozhodne, zda paket vyhovuje vstupním pravidlům
- Podle politiky s paketem naloží:
 - přeposlat cíli
 - vyhodit
 - odmítnout



- Paket dorazí
- Proxy iniciuje vlastní spojení na cílový hostitel
- Iniciátorovi spojení pošle výsledek akce
 - Iniciátor vůbec nekomunikuje přímo
 - Proxy je prostředníkem komunikace
 - Proxy jsou
 - Transparentní
 - Netransparentní



- Udržuje informace o všech spojeních
- Náročnější na implementaci, protože vyžaduje hodně zdrojů (paměť, výpočetní čas)
- Výhody
 - může chránit před DoS útoky
 - odfiltruje nežádoucí chování síťového spojení



- Netfilter je framework pro manipulaci s pakety, přicházejícími do síťových rozhraní (kernel space)
- Iptables je userspace utilita pro manipulaci s "hooks"



- Chain – řetěz – obsahuje sadu pravidel, která jsou aplikována na každý paket, který prochází tímto chainem.
 - INPUT
 - OUTPUT
 - FORWARD
 - PREROUTING
 - POSTROUTING

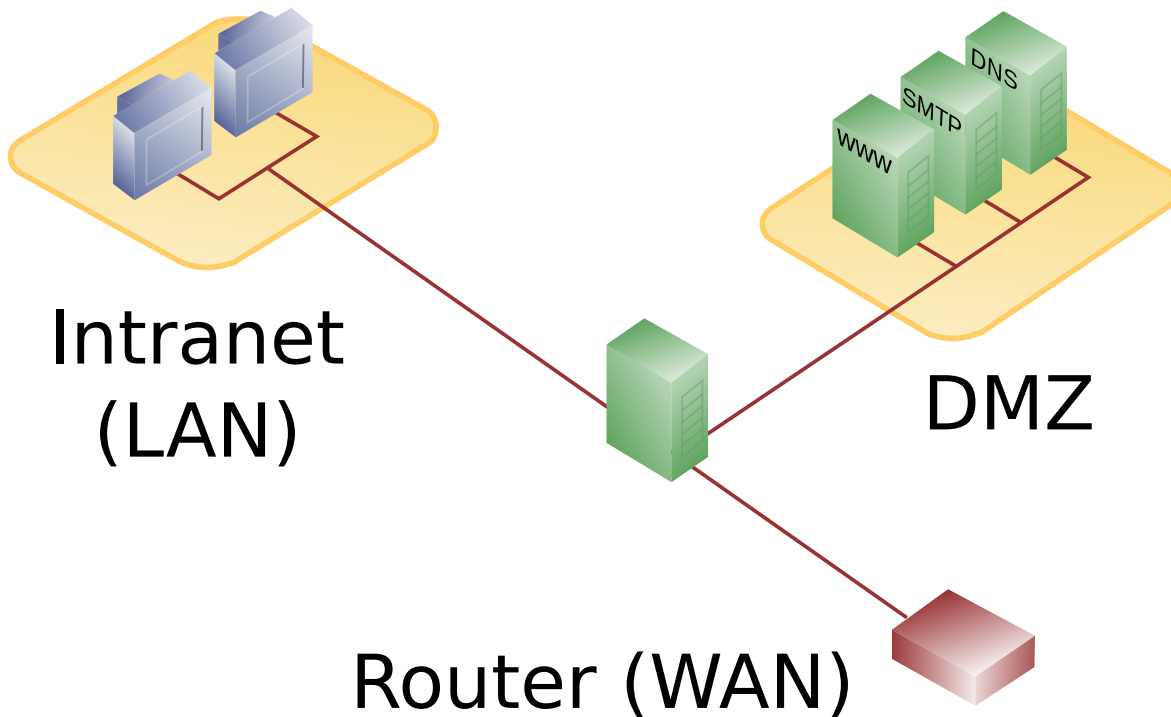


- Table – Každá tabulka má vlastní účel:
 - raw – holá data
 - nat – překlad adres
 - mangle – modifikace paketů
 - filter – filtrování paketů (výchozí tabulka)



Zóny pro firewall

approved by
dsn.felk.cvut.cz

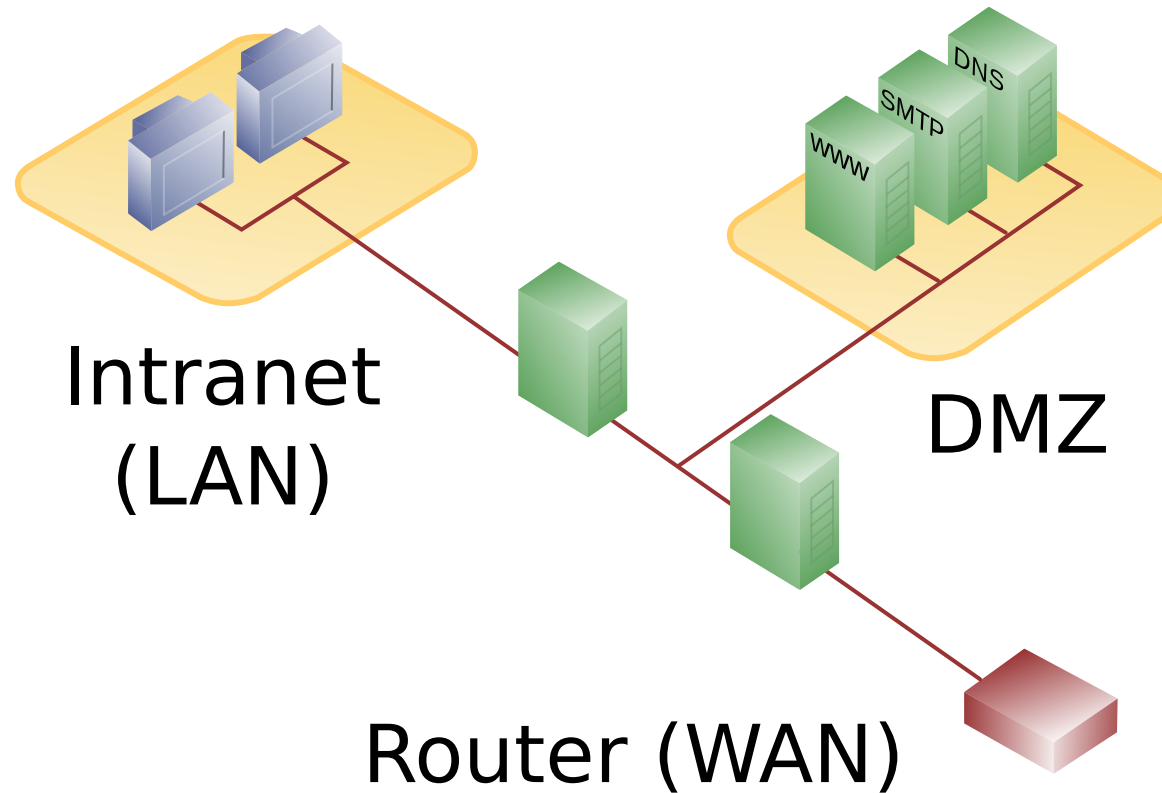


- Internal network – síť která za žádných okolností není dostupná zvenčí
- DMZ – servery, které jsou dostupné i z internetu i z lokální sítě



Zóny pro firewall

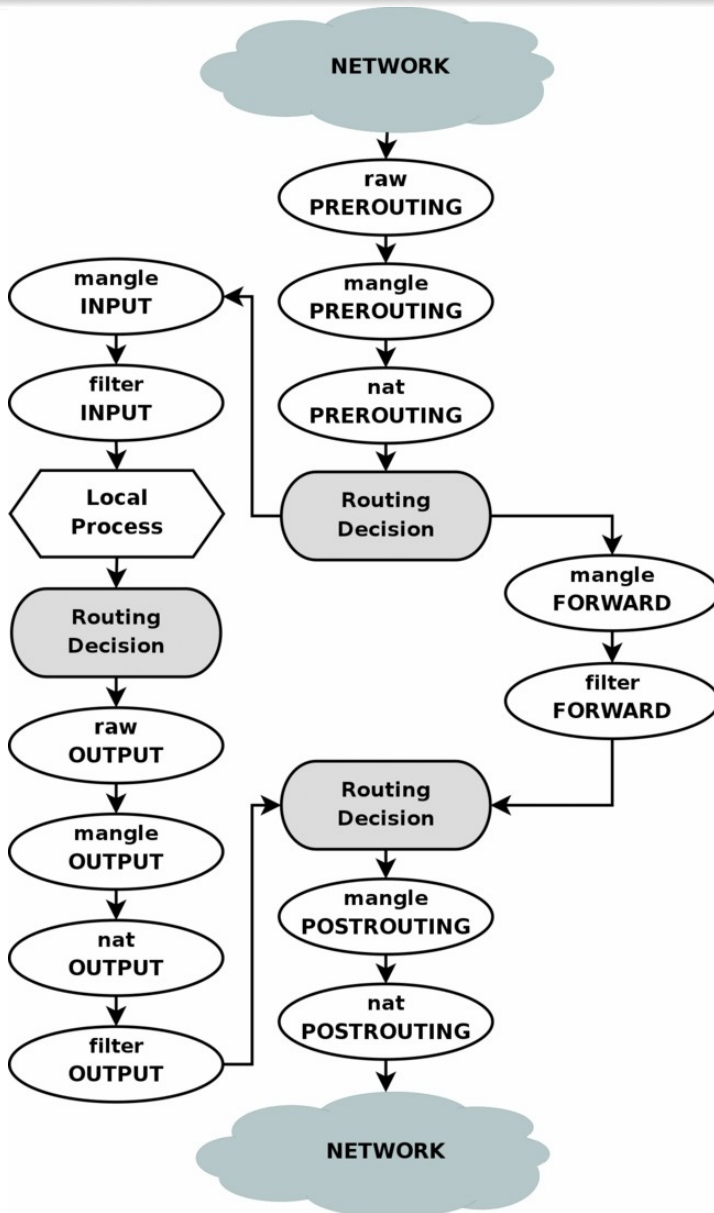
approved by
dsn.felk.cvut.cz



By en:User:Pbroks13 - http://en.wikipedia.org/wiki/Image:DMZ_network_diagram_2_firewalls.png, Public Domain, <https://commons.wikimedia.org/w/index.php?curid=4045251>



Zpracování paketu



- PREROUTING
- POSTROUTING
- INPUT
- OUTPUT
- FORWARD



- Rozdělení na zóny
- Promyšlení chainů
- Příprava "na papír"
- Volba výchozí politiky:
 - DROP
 - REJECT
 - ACCEPT
 - LOG



- iptables -L -n
- iptables -L -n -t nat
- iptables -A <CHAIN> -j <POLICY>
- iptables -P <CHAIN> -j <POLICY>

- iptables -P INPUT ACCEPT
- iptables -P INPUT DROP
- iptables -A INPUT -j LOG



- iptables -A <CHAIN> -s <zdroj> -d <cil> -j <policy>
 - <zdroj>/<cil>
 - IP adresa
 - subnet/maska
 - ! - negace (pozor na bash)
 - -p <protokol>
 - tcp
 - udp ...



- --sport <cislo> = zdrojový port
- --dport <cislo> = cílový port
 - <cislo> může být rozsah např. 0:1023
- -m <modul>
 - state
 - owner
 - ...



- -Z = vynuluje čítače
- -F = flush (vymaže všechny pravidla z chainu)
- -X = smaže chain (bez referencí, bez pravidel)
- -N = vytvoří chain
- -j = join chain (do jiného)



- -F či -X
- -D <chain> <rule-specification>
- -D <chain> <rulenum>



- Pište pravidla do příkazového řádku, okamžitě se projevují
- Napište si skript, který poté spustíte
- Použijte nějaký skript třetí strany, který za vás pravidla vygeneruje (např. Shorewall)
- iptables-save, iptables-restore
- cron script



- nft
- tabulky (ip, ip6, inet, arp, bridge)
 - nft add table inet filter
 - nft list tables
 - nft list|delete|flush table inet filter
- chain (regular, base (hook) (filter, route, nat))
 - nft add chain inet filter webfilter
 - hook: prerouting, input, forward, output, postrouting
 - nft add chain inet filter inputchain '{ type filter hook input priority 0; }'
 - nft chain inet filter inputchain '{ policy drop ; }'



- rule
 - `nft add rule inet filter inputchain tcp dport { ssh, https } accept`
- stav
 - `nftables.service, /etc/nftables.conf`
 - `nft list ruleset > /etc/nftables.conf`
 - `nft flush ruleset`
 - `nft -f /etc/nftables.conf`



- operace s pravidly
 - add, insert, add position #, replace handle #, delete handle #
- parametry pravidel
 - meta - meta informace, například o rozhraní
 - oif <index výstupního rozhraní>, iif <index vstupního rozhraní>, oifname <název výstupního rozhraní>, iifname <název vstupního rozhraní>
 - icmp - protokol ICMP
 - type <typ icmp>
 - icmpv6 - protokol ICMP
 - type <typ icmpv6>
 - ip - protokol IPv4
 - protocol <protokol>, daddr <cílová adresa>, saddr <zdrojová adresa>
 - ip6 - protokol IPv6
 - daddr <cílová adresa>, saddr <zdrojová adresa>
 - tcp - protokol TCP
 - dport <cílový port>, sport <zdrojový port>
 - udp - protokol UDP
 - dport <cílový port>, sport <zdrojový port>
 - sctp - protokol SCTP
 - dport <cílový port>, sport <zdrojový port>
 - ct - connection tracking, sledování spojení
 - state <new | established | related | invalid>



- počítačidla
 - counter
- komentáře
 - comment \"DNS resolver Google\"
- operace
 - accept, drop, reject, reject with icmp type, reject with icmpv6 type
- skok
 - nft add rule ip filter input ip protocol udp jump|goto udp-chain
 - jump – návrat, goto – default politika nového řetězce



- logování
 - nft add rule filter input tcp dport 22 ct state new log prefix \"SSH spojeni: \" accept
 - nft add rule filter input iif eth0 log tcp dport 22 accept
- NAT
 - SNAT
 - nft add table nat
 - nft add chain nat prerouting { type nat hook prerouting priority 0 \; }
 - nft add chain nat postrouting { type nat hook postrouting priority 100 \; }
 - nft add rule nat postrouting ip saddr 192.168.1.0/24 oif eth0 snat 203.0.113.10



- masquerade
 - `nft add rule nat postrouting masquerade`
- DNAT
 - `nft add table nat`
 - `nft add chain nat prerouting { type nat hook prerouting priority -100 ; }`
 - `nft add rule nat prerouting iif eth0 tcp dport { 80, 443 } dnat 192.168.1.200`
- forwarding
 - `nft add rule nat prerouting tcp dport 8080 redirect to 80`
- bezestavový NAT
 - `nft add rule ip raw prerouting ip protocol tcp ip daddr set 192.168.1.100 tcp dport set 10 notrack`



- výkon
 - set
 - slovník
 - mapa
 - rozsah
 - řetězení



firewalld

approved by
dsn.felk.cvut.cz



- <https://www.root.cz/serialy/vse-o-iptables/>
- https://www.petrkrcmar.cz/prednasky/nftables_2017.pdf
- <https://wiki.nftables.org>
- <https://www.root.cz/serialy/firewall-s-nftables/>
- <https://www.root.cz/serialy/firewalld-a-rizeni-site-v-zonach/>
- <https://www.root.cz/clanky/ipset-odlehcte-pretizenym-iptables/>
-