SPS

Firewall a iptables a nftables

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

Firewall

- 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.

Nutno rozlišovat

- Firewall
- Packet filter
- Stateful filter
- Proxy

- Router
- NAT

Paketový filtr

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

Proxy

- 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

Stateful filter

- 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/Iptables

- Netfilter je framework pro manipulaci s pakety, přicházejícími do síťových rozhraní (kernelspace)
- Iptables je userspace utilita pro manipulaci s ”hooks”

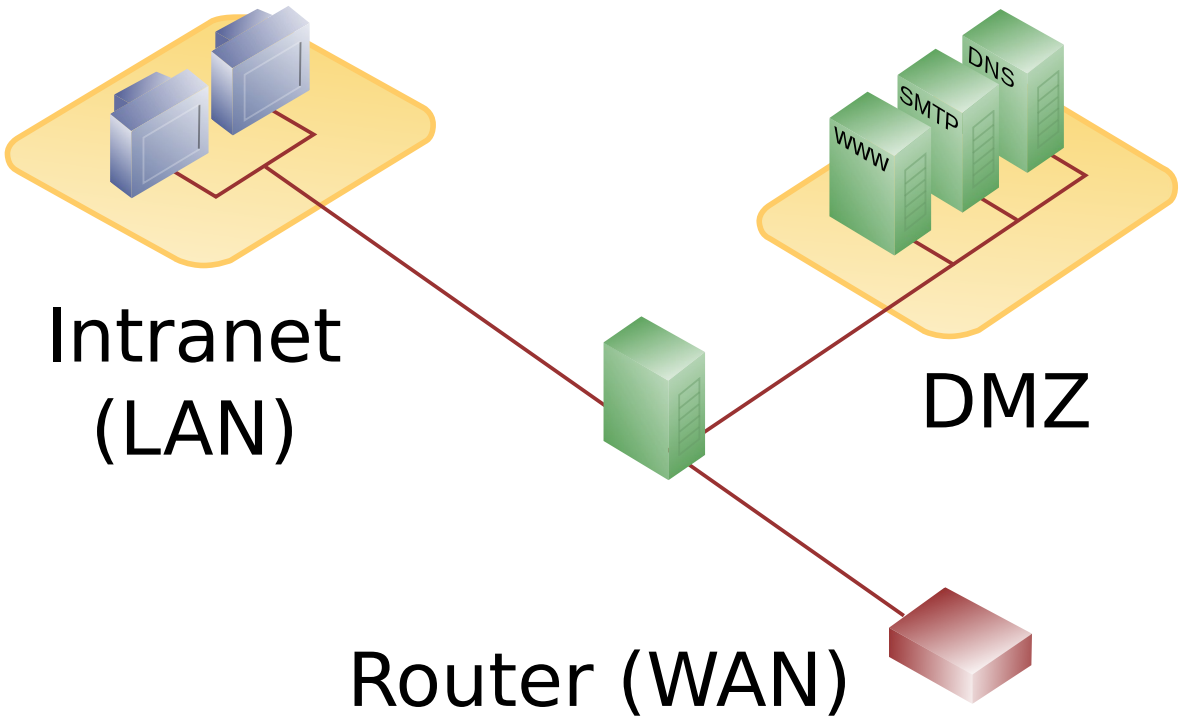
Chain

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

Table

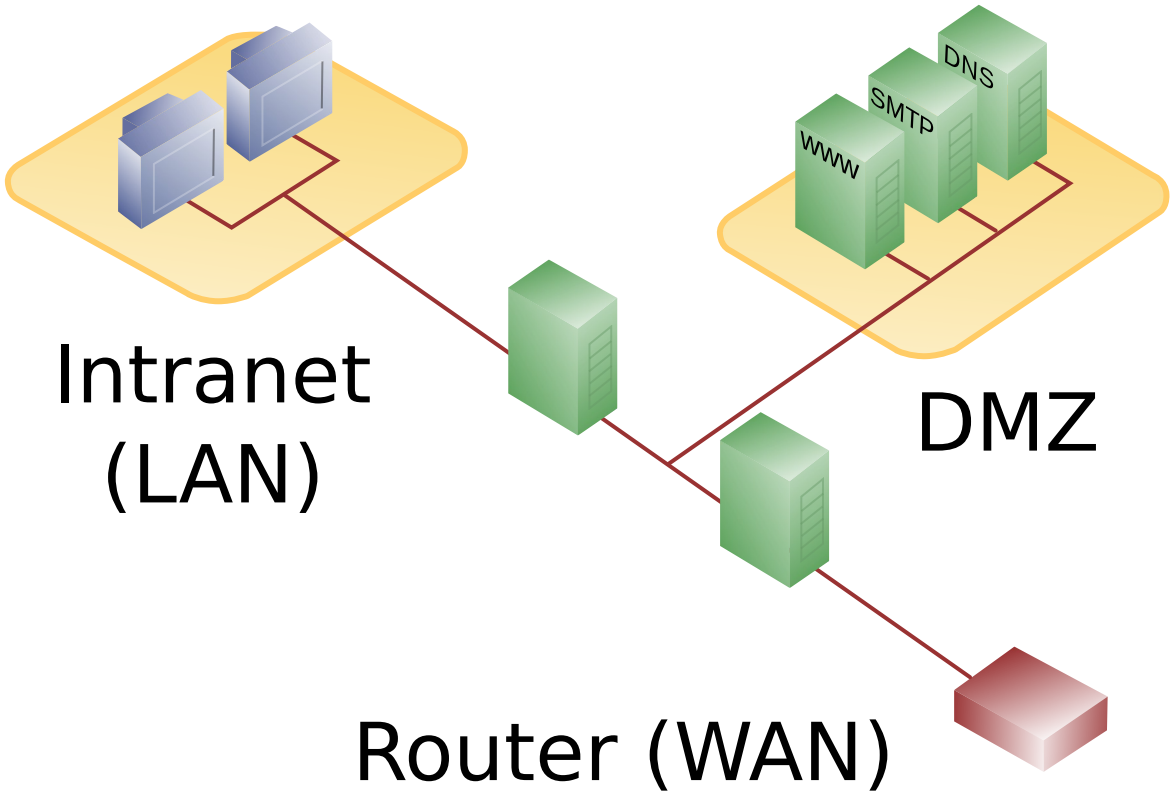
- Table – Každá tabulka má vlastní účel:
  - raw – holá data
  - nat – překlad adres
  - mangle – modifikace paketů
  - filter – filtrování paketů (výchozí tabulka)

Zóny pro firewall



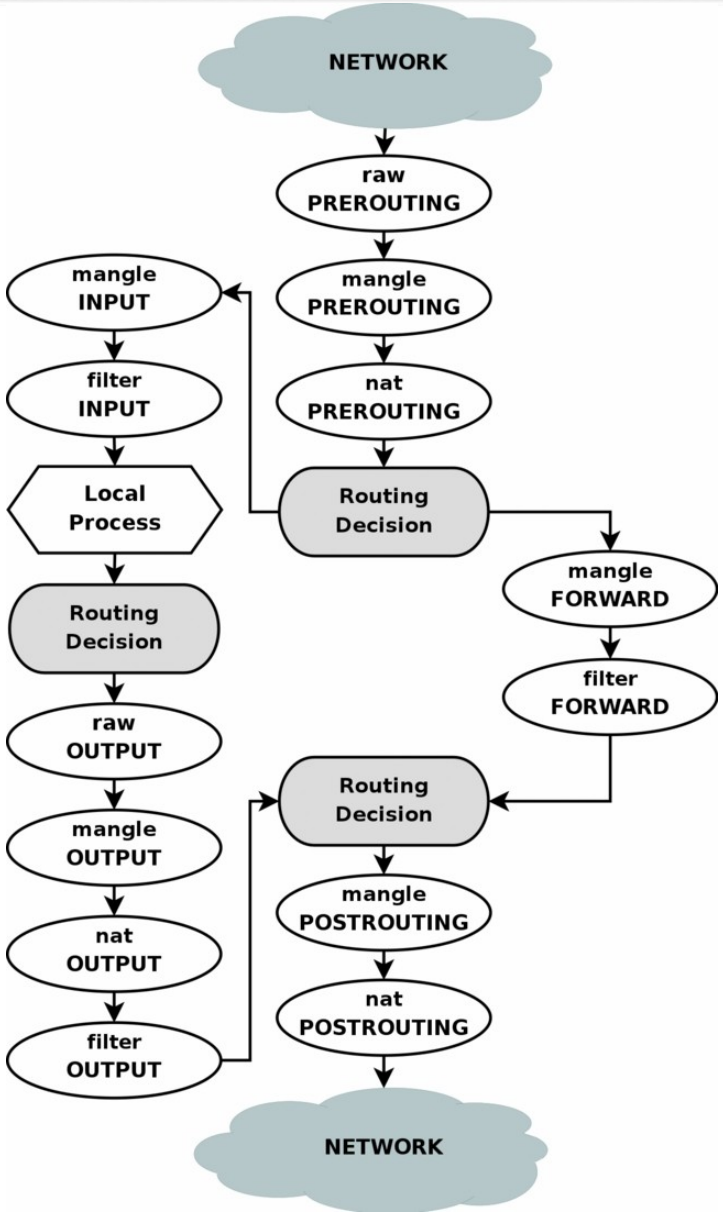
- Internal network – síť která za žádných okolností není dostupná zvenčí
- DMS – servery, které jsou dostupné i z internetu i z lokální sítě

Zóny pro firewall



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

Příprava firewallu

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

iptables

- 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

Specifikace cíle/zdroje

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

Další parametry

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

Chains

- -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)

Mazání pravidel

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

Jak na to...

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

nftables

- 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 ; }'

nftables

- 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>

- počítadla
  - 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

- https://www.root.cz/serialy/firewalld-a-rizeni-site-v-zonach/
- frontend k nftables (iptables)
- integrace s NetworkManagerem
- založený na zónách
- zóny
  - rozdělení síťového prostředí
    - /usr/lib/firewalld/zones/
  - v každé zóně alespoň jedno rozhraní
  - vstup, výstup, NAT
  - provoz mezi právě dvěma zónami

Pravidla

- firewall-cmd
- dočasná x perzistentní
- perzistentní
  - --permanent, –reload a –runtime-to-pernament
- zjištění stavu
  - --get-active-zones, --get-default-zone, --list-all,
  - --get-services, --info-service <service>

Konfigurace

- přidání interface do zóny
  - # firewall-cmd --permanent --zone=home --add-interface=enp0s8
  - # nmcli connection modify interni connection.zone home
- práce se službami
  - /usr/lib/firewalld/services/ , /etc/firewalld/services/
  - vytvoření, aktivace, deaktivace, dočasná aktivace
    - # firewall-cmd --permanent --new-service=home-assistant
    - # firewall-cmd --permanent --service=home-assistant --set-description="Home Assistant"
    - # firewall-cmd --permanent --service=home-assistant --set-short=ha
    - # firewall-cmd --permanent --service=home-assistant --add-port=8123/tcp
    - # firewall-cmd --permanent --zone=public --add-service=ssh
    - # firewall-cmd --permanent --zone=public --remove-service=ssh
    - # firewall-cmd --timeout=3h --zone=public --add-service=ssh
- porty
  - otevření a zavření
    - # firewall-cmd --permanent --zone=home --add-port=22/tcp
    - # firewall-cmd --permanent --zone=home --remove-port=22/tcp

Zóny

- defaultní zóny
  - /usr/lib/firewalld/zones/ , /etc/firewalld/zones/
    - # firewall-cmd --get-zones
    - block dmz drop external home internal public trusted work
    - # firewall-cmd --permanent –new-zone=web
- vlastní zóna
    - # firewall-cmd --permanent --zone=web --set-description="Zona pro webovy server"
    - # firewall-cmd --permanent --zone=web --set-target=REJECT
    - # firewall-cmd --permanent --zone=web --add-service=ssh

IP set

- různé typy
- vytvoření, konfigurace, použití
  - # firewall-cmd --permanent --new-ipset=privatni --type=hash:net
  - # firewall-cmd --permanent --ipset=privatni --add-entry=192.168.0.0/24
  - # firewall-cmd --permanent --ipset=privatni --add-entries-from-file=adresy.txt
  - # firewall-cmd --permanent --zone=trusted --add-source=ipset:privatni

Politiky

- oproti zónám různé směry
- HOST, ANY
- priorita
  - nejnižší (i záporná) první
- výchozí TARGET CONTINUE

Modifikace provozu

- masquerade
  - # firewall-cmd --permanent --zone=external --add-masquerade
- snat
  - firewall-cmd --zone=public --add-masquerade --source=10.10.10.0/24 --to-source=11.11.11.1
- dnat
  - # firewall-cmd --permanent --zone=external --add-forward-port=port=80:proto=tcp:toport=8080:toaddr=10.1.2.20

No a dál

- práce s ICMP
- helpery
- komplexní pravidla
  - rule [family="rule family"]

    [source [NOT] [address="address"] [mac="mac-address"] [ipset="ipset"]]

    [destination [NOT] address="address"]

    [element]

    [[log [prefix="prefix text"] [level="log level"] [limit value="rate/duration"]]

    [audit]

    [action]
-

Obecně

- používejte jen jednu technologii na jednom stroji
- pozor na pořadí pravidel
  - funkce, výkon
- výkon
  - sety, počet pravidel
- vzdálené stroje
  - opravovací skript

Zdroje

- 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-odlehcete-pretizenym-iptables/
- https://www.root.cz/serialy/firewalld-a-rizeni-site-v-zonach/
-