SPS

Firewall a iptables

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”

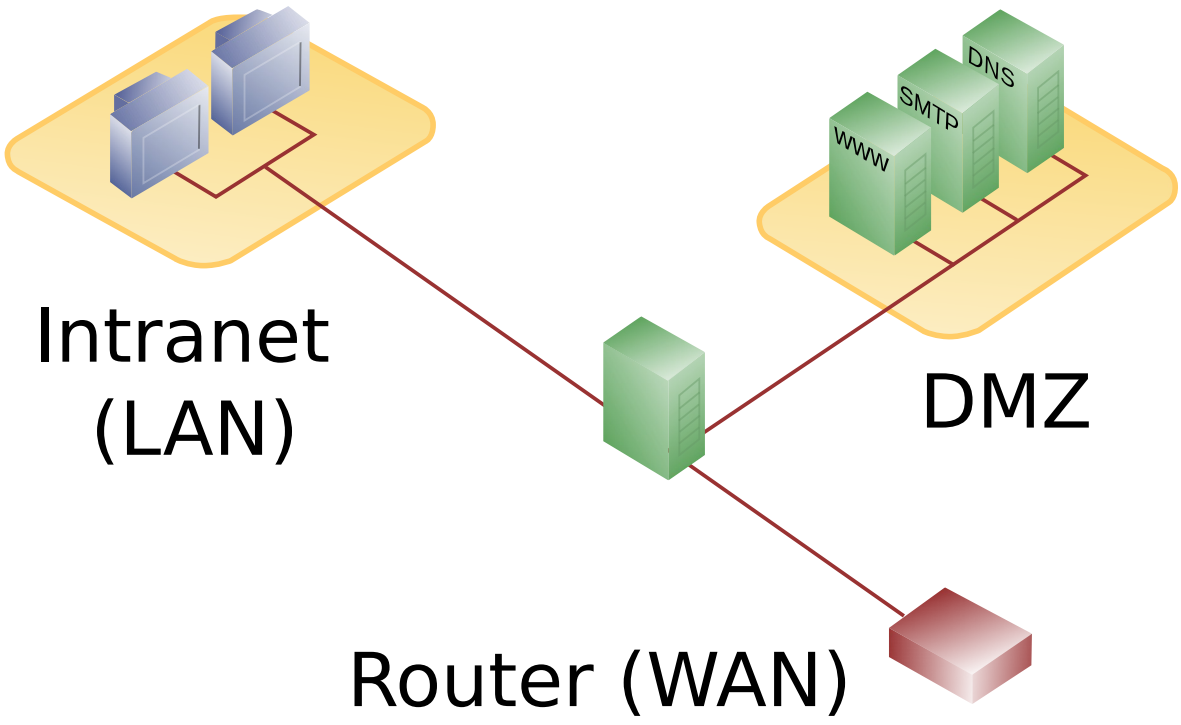
Chain

- 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)

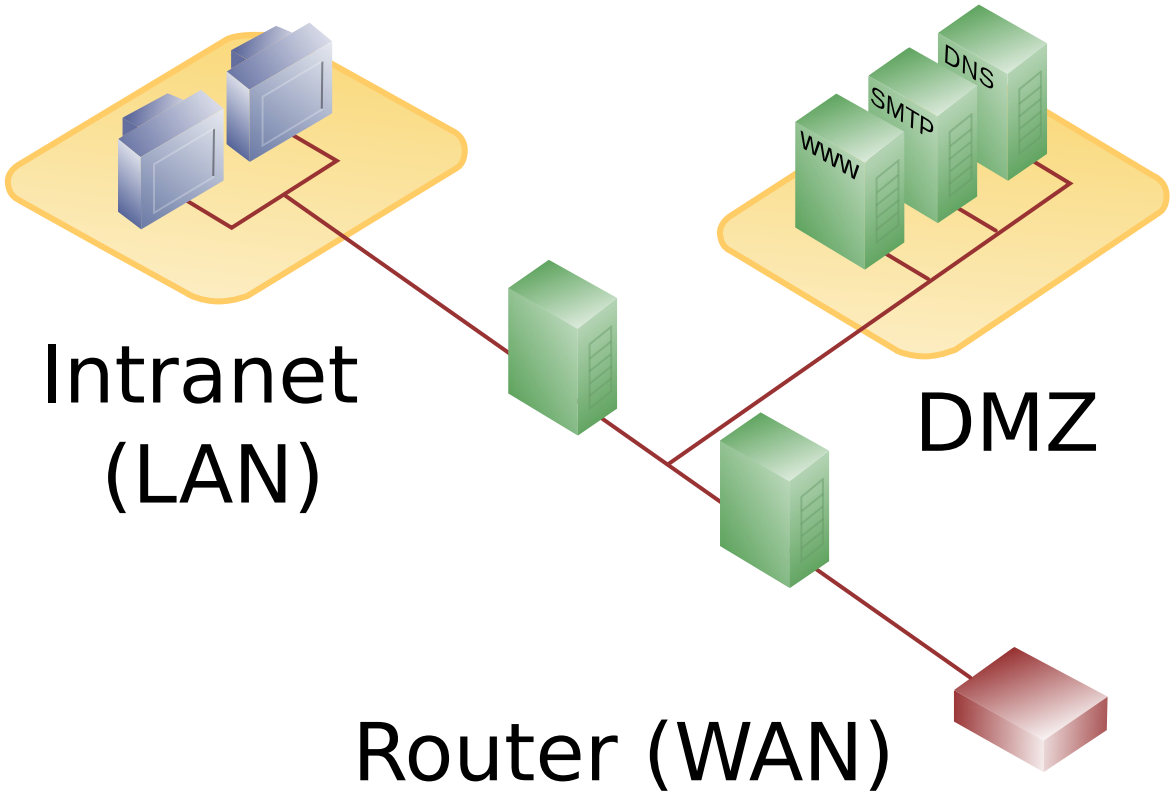
Zóny pro firewall



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

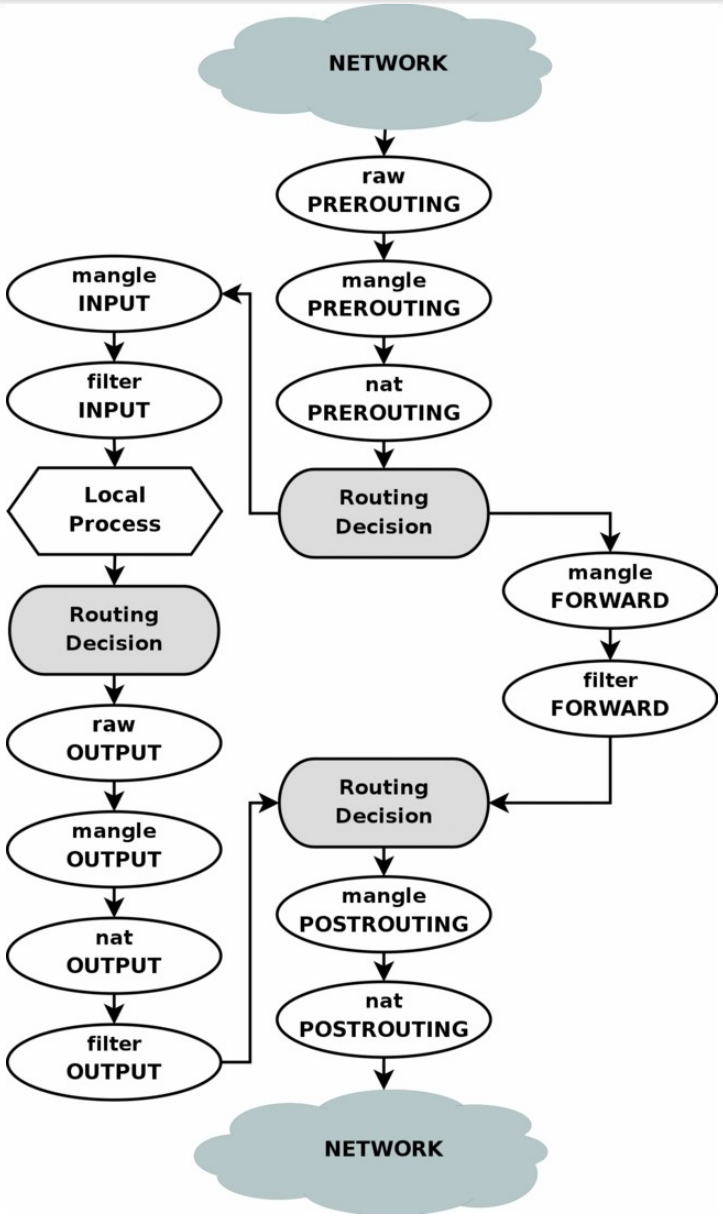
By en:User:Pbroks13 - http://en.wikipedia.org/wiki/Image:DMZ_network_diagram_1_firewall.png, Public Domain, https://commons.wikimedia.org/w/index.php?curid=4045242

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