Firewalling

- 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 síťové zařízení, které slouží k řízení a zabezpečování síťového provozu mezi sítěmi s různou úrovní důvěryhodnosti a/nebo zabezpečení.

Nutno rozlišovat

- Firewall
- Packet filter
- Stateful filter
- Proxy
- Gateway
- Router

Firewall – jiná definice

- Firewall is a router that can say ”no”.

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”
-

Table

- Table – Každá tabulka má vlastní účel:
  - raw – holá data
    - přístup datům před connection tracking
  - nat – překlad adres
    - SNAT, DNAT, MASQUERADE
  - mangle – modifikace paketů
    - MARK, TTL, ToS,
  - filter – filtrování paketů (výchozí tabulka)
    - ACCEPT, REJECT, DROP, LOG

Chain

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

Chains

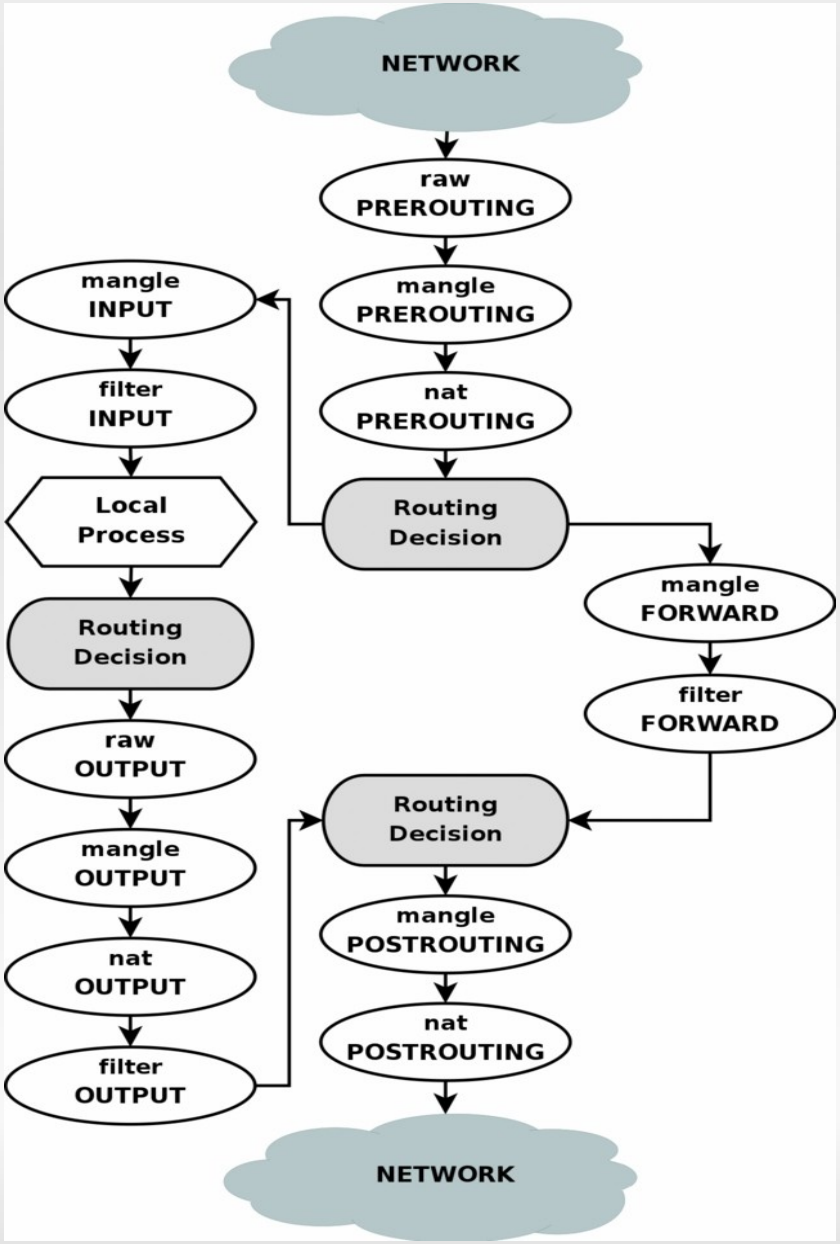
- PREROUTING
  - všechny pakety, přicházející na interface
- INPUT
  - všechny pakety, adresované firewallu
- FORWARD
  - všechny pakety, směrované přes firewall

Chains II

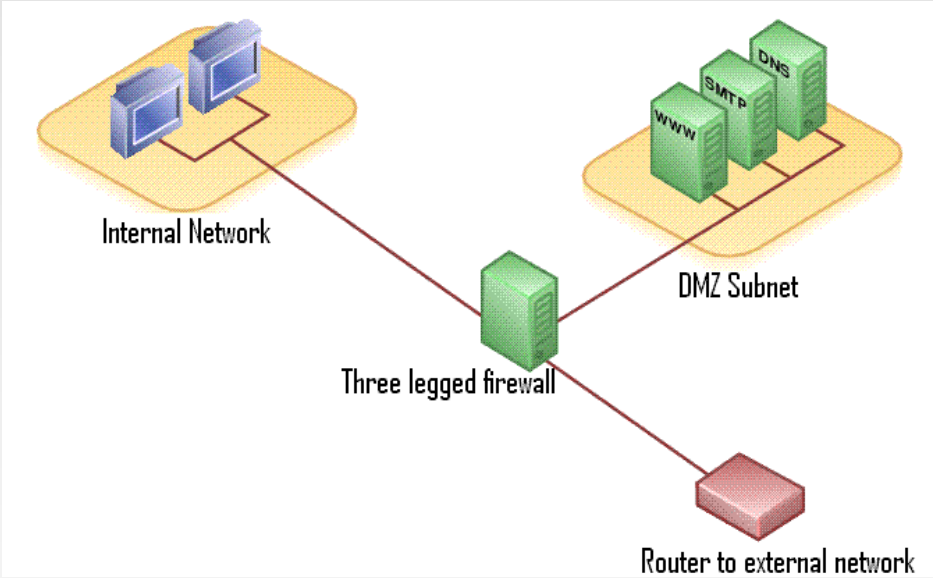
- OUTPUT
  - všechny pakety, generované firewallem
- POSTROUTING
  - všechny pakety, opouštějící interface

Jak to v tom kernelu je...

Step	Table	Chain	Comment
1			On the wire (i.e., Internet)
2			Comes in on the interface (i.e., eth0)
3	mangle	PREROUTING	This chain is normally used for mangling packets, i.e., changing TOS and so on. This is also where the non-locally generated connection tracking takes place.
4	nat	PREROUTING	This chain is used for DNAT mainly. SNAT is done further on. Avoid filtering in this chain since it will be bypassed in certain cases.
5			Routing decision, i.e., is the packet destined for our local host or to be forwarded and where.
6	mangle	FORWARD	The packet is then sent on to the FORWARD chain of the mangle table. This can be used for very specific needs, where we want to mangle the packets after the initial routing decision, but before the last routing decision made just before the packet is sent out.
7	filter	FORWARD	The packet gets routed onto the FORWARD chain. Only forwarded packets go through here, and here we do all the filtering. Note that all traffic that's forwarded goes through here (not only in one direction), so you need to think about it when writing your rule-set.
8	mangle	POSTROUTING	This chain is used for specific types of packet mangling that we wish to take place after all kinds of routing decisions have been done, but still on this machine.
9	nat	POSTROUTING	This chain should first and foremost be used for SNAT. Avoid doing filtering here, since certain packets might pass this chain without ever hitting it. This is also where Masquerading is done.
10			Goes out on the outgoing interface (i.e., eth1).
11			Out on the wire again (i.e., LAN).


NETWORK
raw
PREROUTING
mangle
PREROUTING
nat
PREROUTING
Routing
Decision
mangle
INPUT
filter
INPUT
Local
Process
Routing
Decision
raw
OUTPUT
mangle
OUTPUT
nat
OUTPUT
filter
OUTPUT
mangle
FORWARD
filter
FORWARD
Routing
Decision
mangle
POSTROUTING
nat
POSTROUTING
NETWORK

Zóny pro firewall



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

Příprava firewallu

- Rozdělení na zóny
- Příprava bezpečnostní politiky ”na papír”
- Konzultace
- Volba výchozí politiky:
  - DROP, REJECT, ACCEPT

iptables

- iptables -L -n – výpis pravidel tabulky filter
- iptables -L -n -t nat – tabulka nat
- iptables -A <CHAIN> -j <POLICY>
- iptables -P <CHAIN> -j <POLICY>

iptables

- 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

Zbyl čas?

- Cisco ACL...