UNИX/lectures

Межсетевые экраны в “UNIX”

Iptables и с чем его едят

Фильтрация в Linux
Основные понятия
Общая схема
Connection tracking
Примеры

Фильтрация в GNU/Linux

Kernel-space фильтрация: netfilter
User-space инструменты для настройки:
  iptables
User-space фильтрация аналог divert socket
Ручки к tcp/ip стеку и netfilter в /proc/sys/net/
  {ipv4,ipv6}

Решаемые задачи

Layer-2 filtering
Layer-3 filtering
Other levels?

Stateless filtering
Statefull filtering

Packet mangling
NAT

Правила

- Matches
- Targets/jumps
  - terminating
  - non-terminating
- Modules

Цепочки

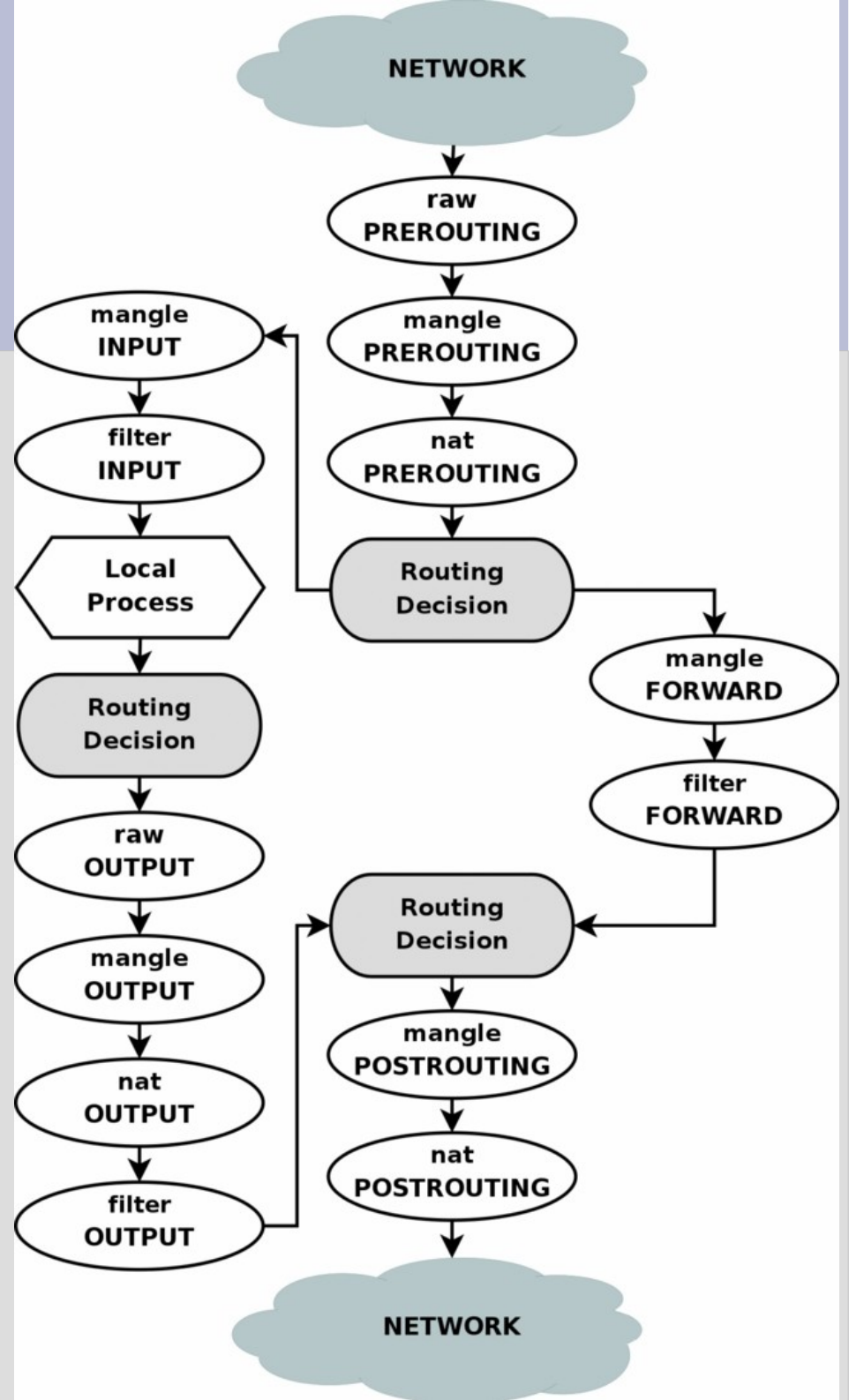
Цепочка – последовательность правил.
Последовательность обработки правил в цепочке.
Политика по-умолчанию.
Пользовательские цепочки, jump.

Таблицы

filter
nat
mangle
raw

Общая схема

3 пути пакета
Таблицы из цепочек
vs. цепочки из таблиц



Правила: matches

protocol
source (range)
destination (range)
in-interface/out-interface
port/icmp-type (multiport)
source-port/destination-port
TCP-flags etc.
Mac
Addrtype matches

Правила: targets

ACCEPT
DROP
REJECT
LOG/ULOG
TRACE
RETURN
MIRROR
QUEUE/NFQUEUE

Connection tracking

state match:

- NEW
- ESTABLISHED
- RELATED
  - Icmp
  - Ftp
  - Irc
  - Pptp
  - Sip
  - ...
- INVALID

NOTRACK target

MARK/CONNMARK

Пометить пакет
- mark match
- MARK target

Пометить соединение
- connmark match
- CONNMARK target

Утилиты

iptables [-t table]
-N chain
-P chain POLICY
-F chain
-L [chain]
-A chain rule-specificator
-D chain rule-specificator
-I chain number rule-specificator
-D chain number

Rule-specificator :=
{[[-m module] [!] match]} -j TARGET [--target-options]

Пример работы

```
iptables -P INPUT DROP
iptables -P FORWARD DROP
iptables -P OUTPUT DROP
iptables -A INPUT -m state \
      --state RELATED,ESTABLISHED -j ACCEPT
iptables -A INPUT -i lo0 -j ACCEPT
iptables -A INPUT -p tcp -m tcp --dport 80 \
      -j ACCEPT
iptables -A OUTPUT -m state \
      --state RELATED,ESTABLISHED -j ACCEPT
iptables -A OUTPUT -o lo0 -j ACCEPT
iptables -A OUTPUT -d 192.168.128.1/32 -p
  udp \
      -m udp --dport 53 -j ACCEPT
iptables -A OUTPUT -d 192.168.128.4/32 -p tcp
      -m tcp --dport 25 -j ACCEPT
```

Утилиты 2

iptables -L -nv --line-numbers

modprobe :-)

iptables-save/iptables-restore

```
# Generated by iptables-save v1.4.2
*filter
:INPUT ACCEPT [2681429:2895113549]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [1534731:149800594]
:test - [0:0]
-A INPUT -j test
-A OUTPUT -j test
COMMIT
# Completed on Wed Mar 25 16:08:20 2009
```

ip6tables{,-save,-restore}

TCPMSS

“This target is used to overcome criminally braindead ISPs or servers which block "ICMP Fragmentation Needed" or "ICMPv6 Packet Too Big" packets.”

```
iptables -t mangle -A FORWARD \
                    -m tcp -p tcp \
                --tcp-flags SYN,RST SYN \
                -j TCPMSS --clamp-mss-to-pmtu
```

NAT

MASQUERADE
SNAT
DNAT
NETMAP
SAME
REDIRECT

Поддержка со стороны conntrack

Patch-o-matic

mport
time
TARPIT
random
Conntrack modules

Литература

http://iptables-tutorial.frozentux.net/
Iptables Tutorial by Oskar Andreasson

http://www.opennet.ru/docs/RUS/iptables/
Руководство по iptables (перевод Андрей Киселев)

iptables(8)