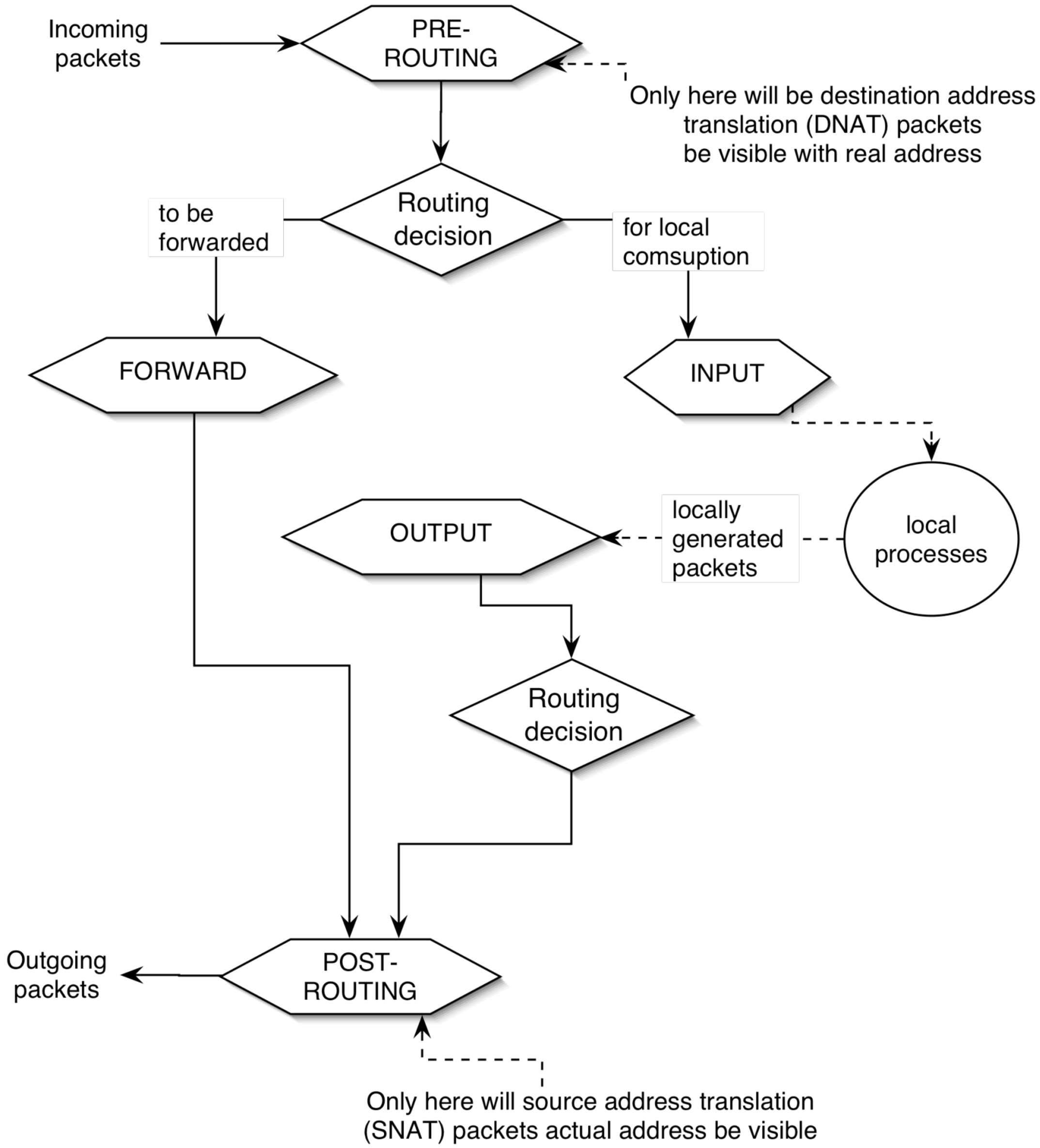
IPtables

Breno de Medeiros

Using IPtables

- Iptables succedds the earlier packet-filtering package ipchains.
- Iptables define sequences of filtering rules, called *chains*.
  - There are a minimum of 3 built-in chains `INPUT`, `OUTPUT` and `FORWARD`
  - Other chains can be added.

IPtables


Incoming packets
PRE-ROUTING
Only here will be destination address translation (DNAT) packets be visible with real address
Routing decision
to be forwarded
for local comsuption
FORWARD
INPUT
local processes
locally generated packets
OUTPUT
Routing decision
POST-ROUTING
Outgoing packets
Only here will source address translation (SNAT) packets actual address be visible

Syntax of IPtables commands

- iptables -A/D (INPUT/ OUTPUT/ FORWARD/ PREROUTING/ POSTROUTING) -s (source address) -p (protocol) - d (destination) (DROP/REJECT/LOG/ACCEPT/ User-defined chain)

Chain manipulation rules

- Create a new chain (-N)
- Delete an empty chain (-X)
- Change the policy for a built-in chain. (-P)
- List the rules in a chain (-L)
- Flush the rules out of a chain (-F)
- Zero the packet and byte counters on all rules in a chain (-Z)

Example:
```
# iptables -L -Z FORWARD
```

Rule manipulation within a chain

- Append a new rule to a chain (-A)
- Insert a new rule at some position in a chain (-I)
- Replace a rule at some position in a chain (-R)
- Delete a rule at some position in a chain, or the first that matches (-D)

Examples:

- `iptables -A INPUT -s 127.0.0.1 -p icmp -j DROP`
- `iptables -D INPUT -s 127.0.0.1 -p icmp -j DROP`

Example usage + testing

- Using the `ping' program to generate such packets (it simply sends an ICMP type 8 (echo request) which hosts should respond to with an ICMP type 0 (echo reply) packet).

-
  ```
  # ping -c 1 127.0.0.1
  ```

  -
    ```
    PING 127.0.0.1 (127.0.0.1): … 1 packets
    transmitted, 1 packets received, 0% packet loss
    round-trip min/avg/max = 0.2/0.2/0.2 ms#
    ```

-
  ```
  #iptables -A INPUT -s 127.0.0.1 -p icmp -j DROP
  ```

-
  ```
  #ping -c 1 127.0.0.1
  ```

  -
    ```
    PING 127.0.0.1 (127.0.0.1): … 1 packets
    transmitted, 0 packets received, 100% packet loss
    ```

Protocol-specific filtering

- Protocols specified by numbers (standard protocol values for IP) or by name for `TCP', `UDP' or `ICMP'.
  - The protocol name can be prefixed by a `!', to invert it, such as `-p ! TCP' to specify packets which are **not** TCP
- Protocol options to deal with multiple interface machines:
  - `-i' (or `--in-interface') and
  - `-o' (or `--out-interface')

Dealing with fragmentation

- The first fragment is treated like any other packet
- Second and further fragments do not match rules
  - E.g. a rule containing `”-p TCP --sport www”` (specifying a source port of `www') will never match a fragment (other than the first fragment), because such information (TCP ports) is not available in the fragments

  - To achieve correct results, you can specify rules for second and further fragments using `-f' (or `--fragment') flag

IPTables is **extensible**

- Some protocols automatically offer new tests: currently TCP, UDP and ICMP;
  - Possible to specify new tests on the command line after the `-p' option, which loads the extension.
- For explicit new tests, the `-m' option loads the extension, making the extended options available
- To get help on an extension, use option to load it (`-p', `-j' or `-m') and `-h' or `--help',
  - eg:`# iptables -p tcp --help#`

Address Translation

- Source address translation (SNAT)
  - Used to multiplex a single IP address to provide internet connectivity to multiple boxes (clients); called “masquerading”
- Destination address translation (DNAT)
  - Allows to use several servers with a single IP address (for load balancing) or because of having a single IP for multiple servers on different ports “port forwarding”

NAT and filtering

- The way the NAT rules are arranged with respect to regular filtering rules allows you to ignore routing when performing filtering
  - The addresses visible to the rules will be the native addresses, not the translated addresses for public consumption