TÉCNICO LISBOA

Lab 5: Firewalls & NATs

Learning iptables

Goals

1. Explore different firewall rules using iptables
2. Configure network address translation (NAT)
3. Learn how to implement port forwarding

Evaluation

- Where
  - *Lab 5: Firewall & NAT* on Moodle
- Submission due
  - Sunday, December 3, 23h59

Firewall & iptables

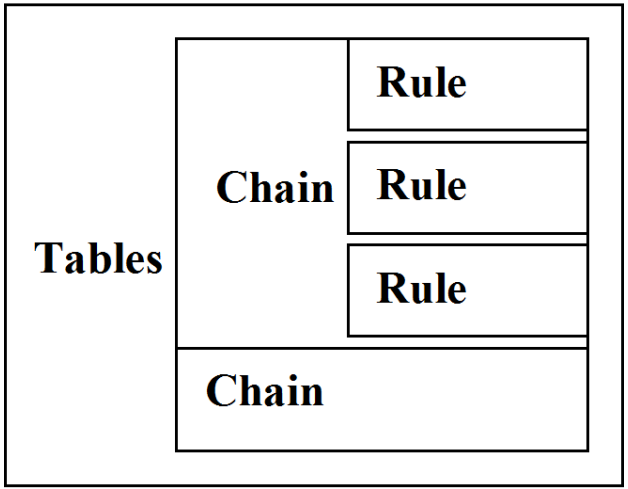
- **Firewall:** mechanism that controls incoming and outgoing network traffic according to configured security rules
- **Iptables:** a Linux utility that allows the definition and configuration of IP packet filter rules on a network host

iptables -I INPUT -p tcp -j DROP

"Drop all incoming tcp packets."

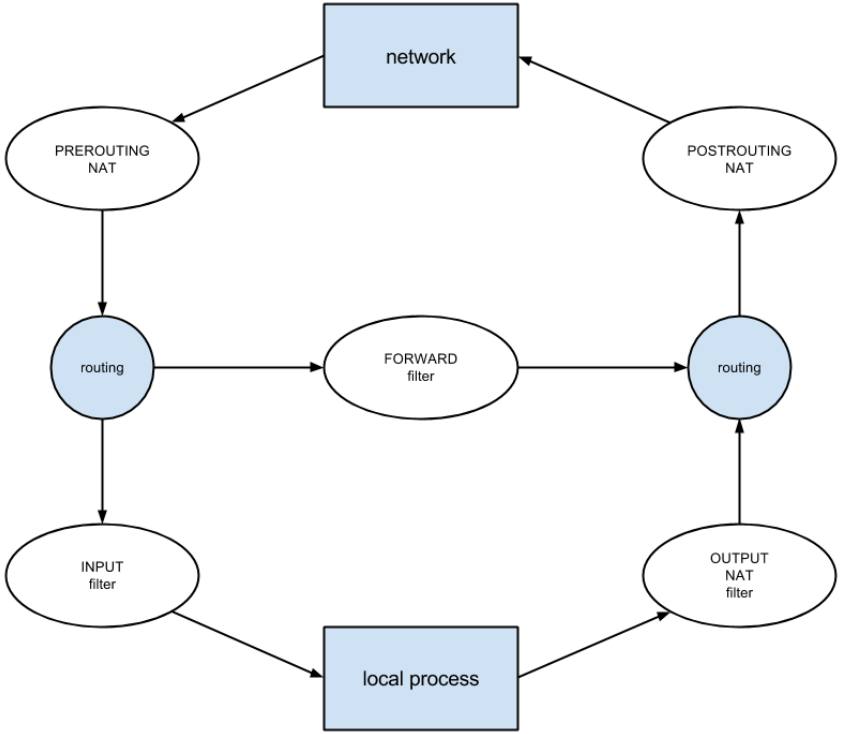
iptables - Structure

- System is divided into various **tables**
- Each table has several rule **chains**
  - Sequence of rules executed in order
- Each **rule** matches certain packets
  - When matching, triggers action



iptables – Packet Flow

- Packets pass through *relevant chains*
- Packets follow rules *sequentially*
- Rules can “call” other *user-defined* chains

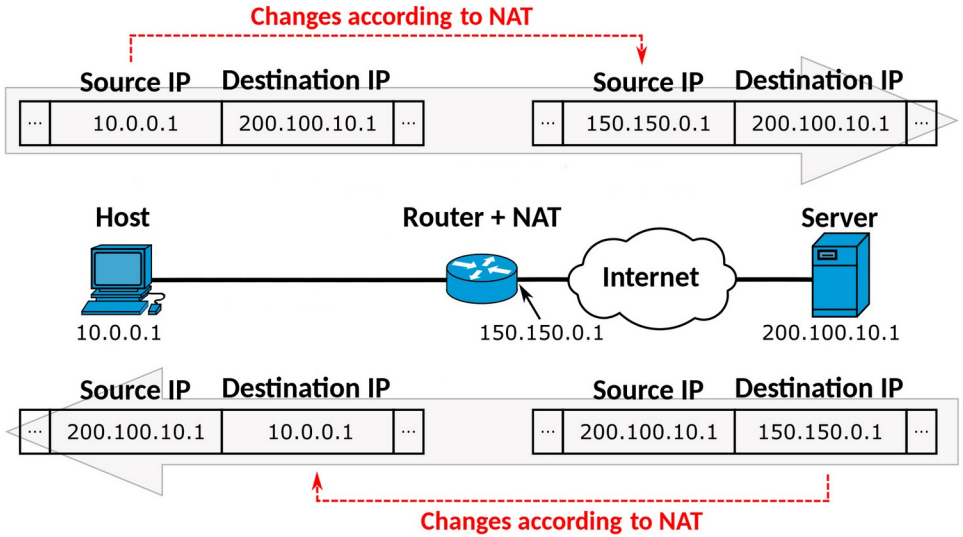


Network Address Translation (NAT)

- Rewrite source/destination IP/Port
- Remember flows to reverse changes on return path
- Built-in NAT table allows both *Source NAT (SNAT)* and *Destination NAT (DNAT)*
  - PREROUTING chain → Change destination before routing
  - POSTROUTING chain → Change source after routing

Internet Connection Sharing

- Allows multiple hosts in private network to share a single public IP
  - Mitigate IPv4 shortages
- Considered SNAT, as it modifies a packet's source



Port Forwarding

- Forwards traffic for a port to another host
- Considered a DNAT operation, as it modifies a packet's destination