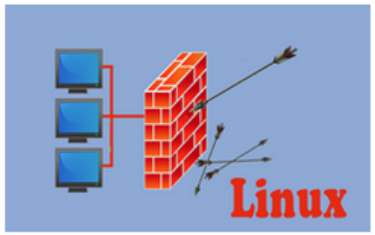
Firewall

(some slides based on SEED LAB)

Linux Firewall Exploration Lab

SEED Lab: A Hands-on Lab for Security Education

Overview



The learning objective of this lab is for students to gain the insights on how firewalls work by playing with firewall software and implement a simplified packet filtering firewall. Firewalls have several types; in this lab, we focus on two types, the *packet filter* and application firewall.

Packet filters act by inspecting the packets; if a packet matches the packet filter's set of rules, the packet filter will either drop the packet or foward it, depending on what the rules say. Packet filters are usually *stateless*; they filter each packet based only on the information contained in that packet, without paying attention to whether a packet is part of an existing stream of traffic. Packet filters often use a combination of the packet's source and destination address, its protocol, and, for TCP and UDP traffic, port numbers.

Application firewall works at the application layer. A widely used application firewall is web proxy, which is primarily used for egress filtering of web traffic. In this lab, students will play with both types of firewalls, and also through the implementation of some of the key functionalities, they can understand how firewalls work.

Lab Tasks (Description)

- **VM version:** This lab has been tested on our pre-built `SEEDUbuntu16.04` VM.

Recommended Time

- Supervised situation (e.g. a closely-guided lab session): **2 hours**
- Unsupervised situation (e.g. take-home project): **1 week**

Videos (New)

- This topic is covered in my Udemy course: Internet Security: A Hands-on Approach.
- If you are in Mainland China, you can access the same course from the NetEase platform.

Suggested Reading

SEED Labs

- Home Page

SEED Books

- The 2nd Edition

SEED Lectures

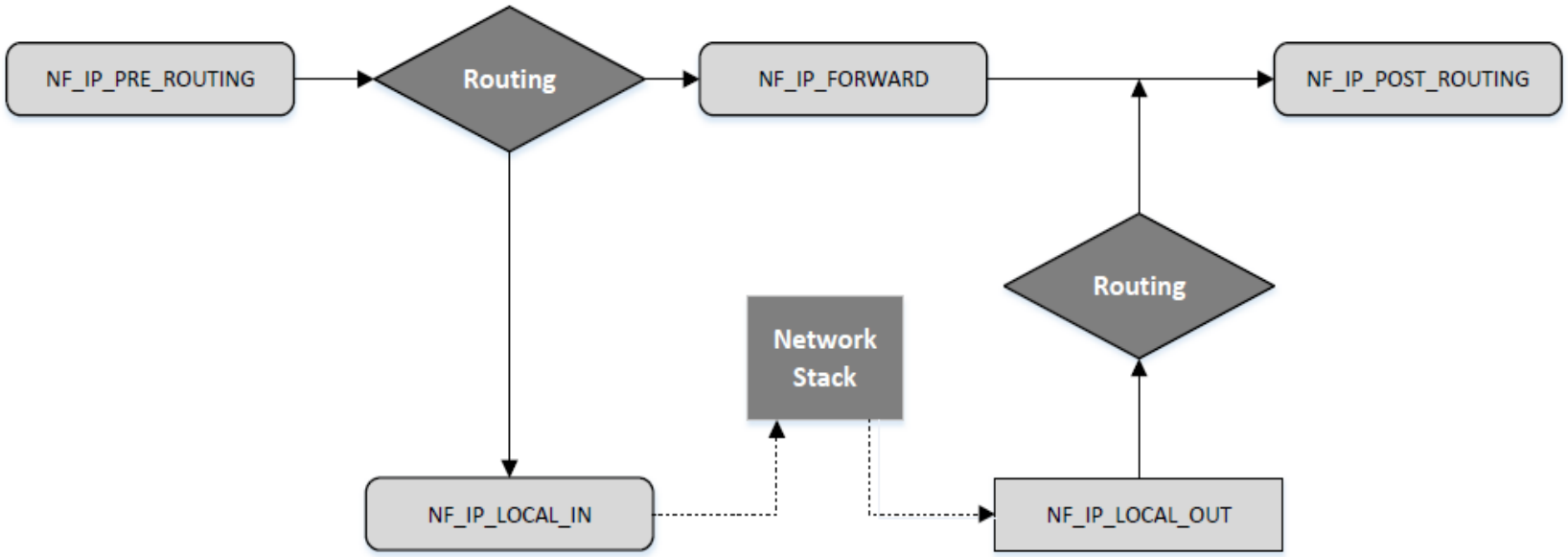
- Udemy Courses

Firewall Concepts

- Ingress: for incoming traffic
- Egress: for outgoing traffic

- Type of firewall
  - Packet Filter Firewall
  - Stateful Firewall
  - Application/Proxy Firewall

Netfilter Hooks



Iptables Firewall in Linux

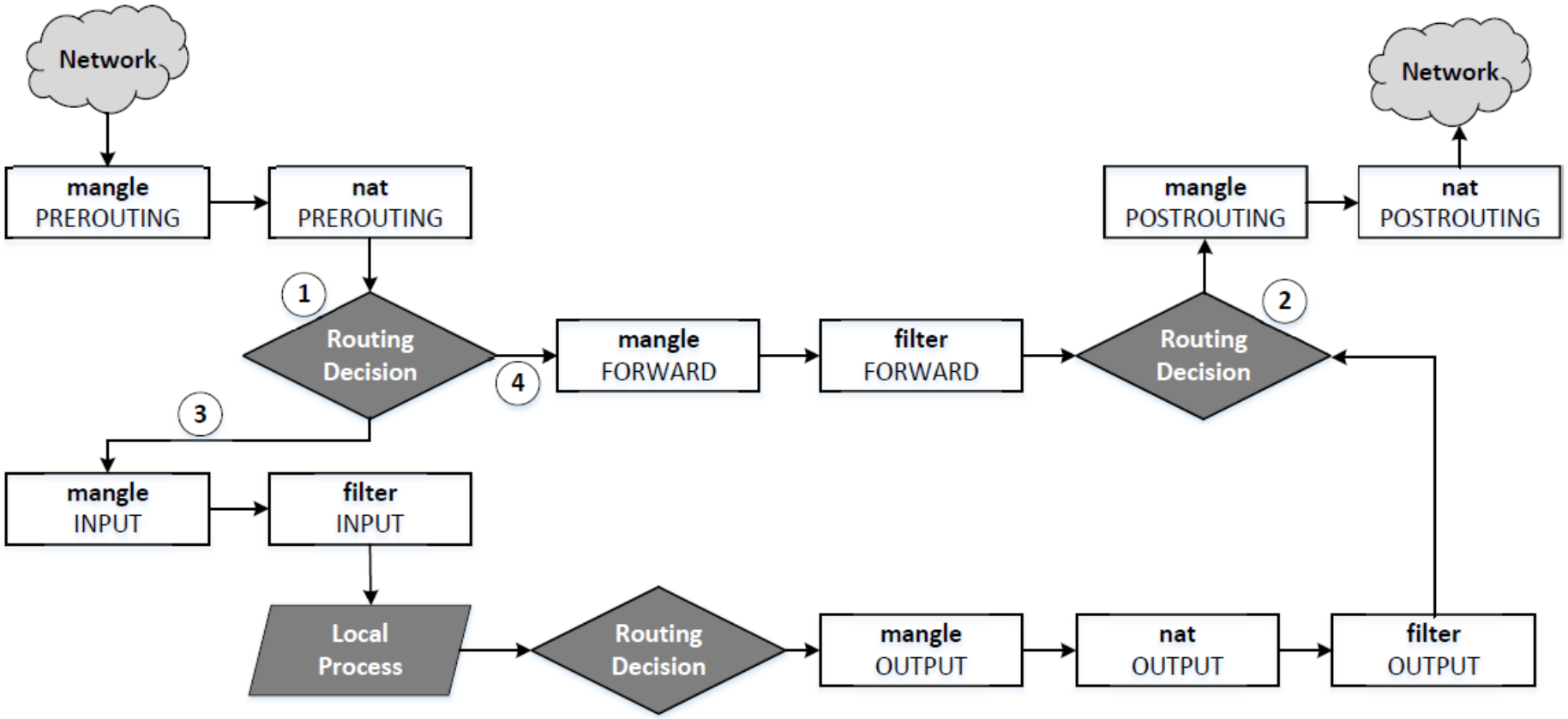
- Iptables is a built-in firewall based on netfilter.
- User-space program: iptables
- Rules are arranged in hierarchical structure as shown in the table.

Table	Chain	Functionality
filter	INPUT FORWARD OUTPUT	Packet filtering
nat	PREROUTING INPUT OUTPUT POSTROUTING	Modifying source or destination network addresses
mangle	PREROUTING INPUT FORWARD OUTPUT POSTROUTING	Packet content modification

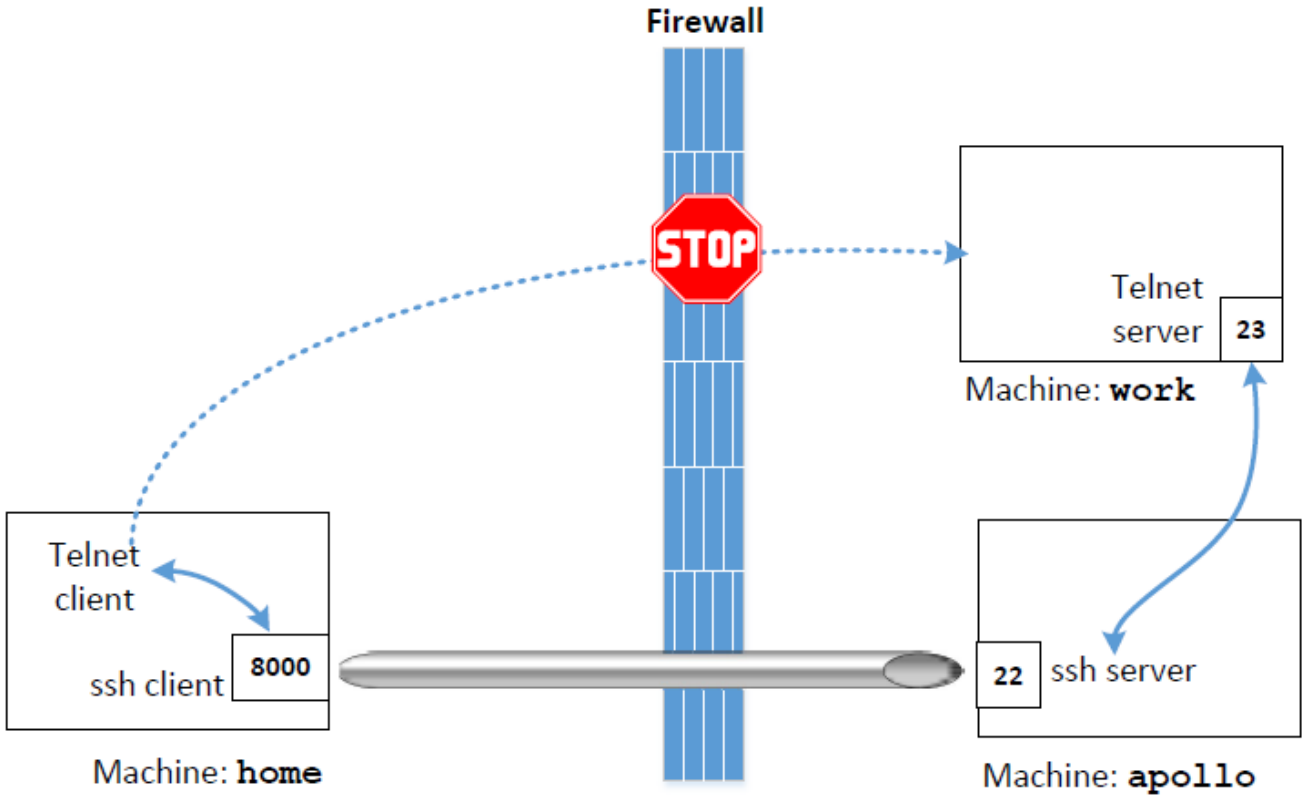
Iptables Firewall - Structure

- Each table contains several chains, each of which corresponds to a netfilter hook.
- Each chain indicates where its rules are enforced.
  - Example : Rules on FORWARD chain are enforced at NF_IP_FORWARD hook and rules on INPUT chain are enforced at NF_IP_LOCAL_IN hook.
- Each chain contains a set of firewall rules that will be enforced.
- User can add rules to the chains.
  - Example : To block all incoming telnet traffic, add a rule to the INPUT chain of the filter table

iptables


Network
mangle
PREROUTING
nat
PREROUTING
1
Routing
Decision
4
mangle
FORWARD
filter
FORWARD
Routing
Decision
2
mangle
POSTROUTING
nat
POSTROUTING
Network
3
mangle
INPUT
filter
INPUT
Local
Process
Routing
Decision
mangle
OUTPUT
nat
OUTPUT
filter
OUTPUT

SSH Tunneling to Evade Firewalls



- Establish a ssh tunnel between “home” and “apollo”.
- On the “home” end, the tunnel receives TCP packets from the telnet client.
- It forwards the TCP data to “apollo” end, from where the data is out in another TCP packet which is sent to machine “work”.
- The firewall can only see the traffic between “home” and “apollo” and not from “apollo” to “work”. Also ssh traffic is encrypted.