Lab Exercise Sheet 3

Document and analyze your experimental procedures by using your Wireshark and terminal recordings. Note all relevant intermediate steps. Mark and explain all relevant information, such as protocol header fields, MAC addresses, IP addresses, port numbers. If you have little experience with Linux, you may need to do some research. **Send your self prepared experiment documentation in the PDF file format to cocos@stud.fra-uas.de and christianbaun@fb2.fra-uas.de. Alternatively, fill out the document, print it out, and submit it during one of the exercise sessions.**

First name:	
Last name:	
Student number:	

1. In the last exercise sheet you set up a network using four VMs. In this exercise sheet you will use the network you set up to configure a firewall using the command-line tool `iptables`. You will have to perform the steps listed below in order to configure a secure network.

   - Install `iptables` on the `mastervm` of your setup.
   - Set up suitable firewall rules on the `mastervm`.
   - Test your setup and document the necessary steps.

   The rules and tests you need to perform are stated in the exercises. The folowing sources will provide helpful information in order to solve the exercises. [1] [2] [3]

2. The digram in figure 1 shows the flow of packets that are processed by a packet filter. Please fill in the gaps the rule chains that are applied by the router.

[1] `https://www.howtogeek.com/177621/the-beginners-guide-to-iptables-the-linux-firewall/`
[2] `https://www.karlrupp.net/de/computer/nat_tutorial`
[3] `https://www.hostinger.com/tutorials/iptables-tutorial#gref`

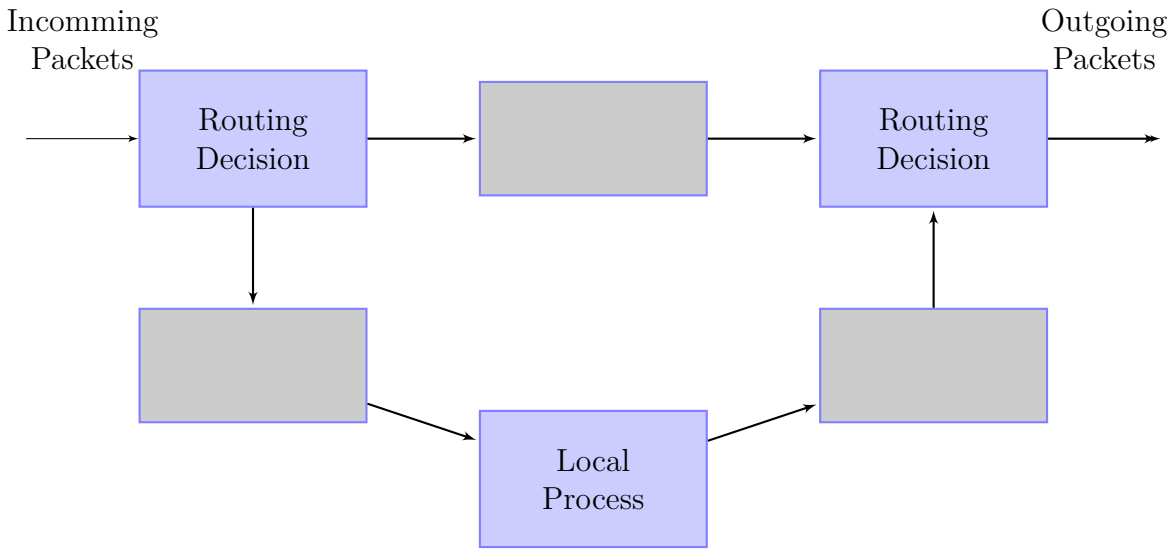

Figure 1: Flow of packets trough a packet filter

3. Check the relevant MAC addresses and write them into this table:

Your local Router to the internet:	
Physical network interface of your host:	
`mastervm` (bridged interface):	
`mastervm` (internal interface 1):	
`mastervm` (internal interface 2):	
`mastervm` (internal interface 3):	
`clonevm1` (internal interface):	
`clonevm2` (internal interface):	
`clonevm3` (internal interface):	

The `mastervm` should operate as a Router between the three new network interfaces for `clonevm[1-3]`, which are attached to the internal networks `lan[1-3]` and the wan interface (network interface connected to the internet) of the `mastervm`.

a) In order to setup the firewall you have to:

- Specify for `lan[1-3]` three independent address spaces (e.g. `192.168.10.0/24`, `172.22.0.0/16` and `192.168.60.0/24`). Assign[4] valid IP addresses and further network configuration parameters to the virtual network devices inside the `mastervm` and `clonevm[1-3]`. Implement IP package forwarding (NAT-Masquerading)[5].

[4]This can be done with command line tools like `ip` or `ifconfig` or inside the file `/etc/network/interfaces`.

[5]This can be done with command line tools like `ip` or `iptables` or inside the file `/etc/network/interfaces`.

4. Please answer the following Questions:

   a) Please explain briefly what `iptables` is used for?

   b) What is the `INPUT` rule chain and what is it used for?

   c) What is the `OUTPUT` rule chain and what is it used for?

   d) What is the `FORWARD` rule chain and what is it used for?

e) Write down the rules you need to setup in `iptables` in order to fulfil the following behavior:

Forward all incomming packets.

Accept all incomming HTTP traffic

Accept all outgoing HTTP traffic.

Forward all incomming HTTPS requests.

Reject all incomming packets for ICMP requests.

Reject all incomming packets for SSH connections.

Block all incomming packets for TELNET connections.

Block all incomming packets for HTTP requests.

Deny all incomming traffic.

What is a Policy and what does it specify?

What kind of policies do exist?

5. Please setup the following rules in your network environment and test your firewall settings. State your rules configured with `iptables` and document your results with excerpts of your terminal output and messages from wireshark.

   a) Block ICMP requests from the computer `clone1` to the `mastervm`.

   b) Reject ICMP Reqests from the computer `clone2` to the `mastervm`.

   c) Reject SSH connections from computer `clone3` to the `mastervm`.

d) Block all traffic from computer `clone1` to the internet.