

Lab Exercise Sheet 3 – (Sample Solution)

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.**

Sample Solution (No Guarantee !!!)

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 following 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/>

²https://www.karlsruhp.net/de/computer/nat_tutorial

³<https://www.hostinger.com/tutorials/iptables-tutorial#gref>

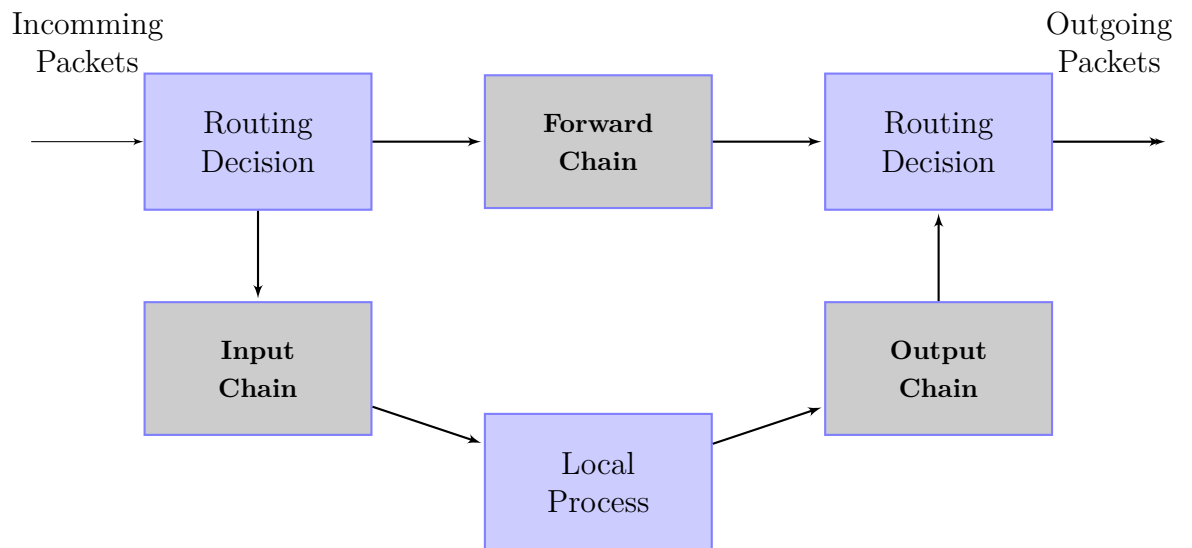


Figure 1: Flow of packets through a packet filter

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

Your local Router to the internet:	34:31:c4:74:70:92
Physical network interface of your host:	4c:34:88:9e:4d:28
<code>mastervm</code> (bridged interface):	08:00:27:52:da:cd
<code>mastervm</code> (internal interface 1):	08:00:27:ff:6d:96
<code>mastervm</code> (internal interface 2):	08:00:27:33:3c:aa
<code>mastervm</code> (internal interface 3):	08:00:27:28:73:72
<code>clonevm1</code> (internal interface):	08:00:27:e8:a4:af
<code>clonevm2</code> (internal interface):	08:00:27:a1:25:5c
<code>clonevm3</code> (internal interface):	08:00:27:cb:0f:3e

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`). Assign⁴ 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. Please answer the following Questions:

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

`iptables` is a command-line tool that enables you to specify policies and rules for your firewall. Those rules help to secure a network. The specified policies and rules block unwanted connections to an internal network by applying filter rules on incoming connections by a gateway router.

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

The `INPUT` rule chain specifies rules for incoming packets. The rules configured in this rule chain filter all incoming packets according to the specified rules and decides whether the incoming packets are processed or not. This rule chain is used to secure a computer against unwanted connections and packets.

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

The `OUTPUT` rule chain specifies rules for all outgoing packets. The rules configured in this rule chain filter all outgoing packets according to the specified rules and decides whether the outgoing packets are sent further or not. This rule chain is used to secure a network against unwanted connections to the internal network or the internet.

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

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

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

The **FORWARD** rule chain specifies rules for all packets that should be forwarded through the computer that applies the forwarding filter. This rule chain is used to check connections and packets and decides whether the incoming packets should be forwarded to an other specified interface or not.

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

In order to test the following rules you need to install **iptables** and configure the **mastervm** accordingly! You can answer the questions from consulting the web, but it is an easy task to test the commands and inspect their behaviour.

Forward all incoming packets.

```
iptables -P FORWARD ACCEPT
```

Accept all incoming HTTP traffic

```
iptables -A INPUT -p tcp -dport 80 -j ACCEPT
```

Accept all outgoing HTTP traffic.

```
iptables -A OUTPUT -p tcp -sport 80 -j ACCEPT
```

Forward all incoming HTTPS requests.

```
iptables -A FORWARD -p tcp -dport 443 -j ACCEPT
```

Reject all incoming packets for ICMP requests.

```
iptables -A INPUT -p icmp -j REJECT
```

Reject all incoming packets for SSH connections.

```
iptables -A INPUT -p tcp -dport 22 -j REJECT
```

Block all incoming packets for TELNET connections.

```
iptables -A INPUT -p tcp -dport 23 -j DROP
```

Block all incoming packets for HTTP requests.

```
iptables -A INPUT -p tcp -dport 80 -j DROP
```

Deny all incoming traffic.

```
iptables -P INPUT DROP
```

What is a Policy and what does it specify?

A policy specifies the rules that are applied to a type of connection. The policy checks the incoming and outgoing packets.

What kind of policies do exist?

- **ACCEPT** -> accepts all incoming packets
- **DROP** -> drops all incoming packets. The sender gets no error message
- **REJECT** -> rejects all incoming packets. The sender gets an error message

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**.

```
iptables -A INPUT -p ICMP -s 192.168.1.10 -j DROP
```

- b) Reject ICMP Requests from the computer **clone2** to the **mastervm**.

```
iptables -A INPUT -p ICMP -s 192.168.2.20 -j REJECT
```

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

```
iptables -A INPUT -p tcp -dport ssh -s 192.168.3.30 -j REJECT
```

- d) Block all HTTP traffic from computer **clone1** to the internet.

```
iptables -A FORWARD -s 192.168.1.10 -j DROP
```