UNIVERSITÄT PASSAU

5823UE Security Insider Lab I - Infrastructure Security (Sicherheits-Infrastruktur) - WS2021

Part 3: Subnetting / Firewalls / DNS / NAT

Time:	Wednesday 14:00-20:00
Location:	ITZ SR 001
Organiser:	Korbinian Spielvogel [korbinian.spielvogel@uni-passau.de]

Part 3: Subnetting / Firewalls / DNS / NAT

Objectives

- Learn how to partition network ranges (sub-netting)
- Learn how to configure a Linux router
- Learn basics about DNS
- Learn how to use NAT
- Learn how to use Linux IPTABLES to configure a Firewall

Methods

- Use Linux in your VM environment to build a router / firewall
- Build a test network within the VM environment
- Configure a DNS server
- Enable NAT on the router's outbound interface
- Configure and test firewall rule sets

Schedule

- 3 weeks

Report

- Deadline: 08.12.2021 (11:59 am)
- Send it to korbinian.spielvogel@uni-passau.de (Subject [SecLab21])
- Maximum 30 pages

Oral Exam

- 01.12.2021 (End of session)

Introduction to Subnetting

In order to ease administrative tasks, an additional level of addressing can be introduced in the network, called subnetting. With subnetting the network can be divided into several 'subnetworks'. Recall that with a thirty-two bit IP-address there are roughly four billion possible addresses (less than one per person in the planet). This is referred to as the total IP address space.
This overall space is divided up into three kinds of networks: class A, class B and class C.
Class A: 001.hhh.hhh.hhh through 126.hhh.hhh.hhh
Class B: 128.001.hhh.hhh through 191.254.hhh.hhh
Class C: 192.000.001.hhh through 223.255.254.hhh

A subnet mask allows the host portion of an Internet address to be divided into two parts:

- The first part is used to identify the subnet number
- The second part is used to identify the host

A host or router uses the leading bits of an IP address to determine its class. Once the class of an address is determined, the host can easily distinguish between the bits used to identify the network number part of the address, and the bits used to identify the host part of the address.

Exercise 1: Theoretical subnetting

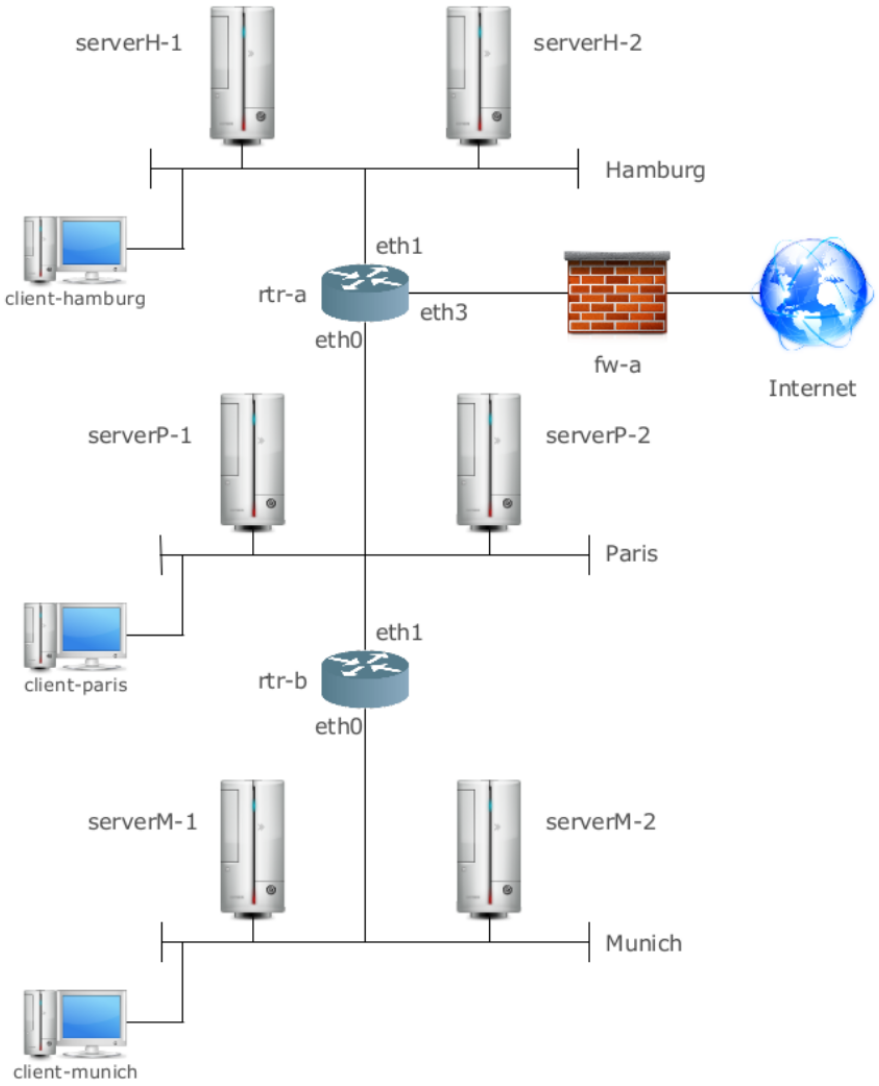

Figure 1: Theoretical Subnetting

1.1 Subnet

Subnet the example network depicted in Figure 1 and give each network interface an IP address (hosts, routers, firewalls, clients, servers, etc.).

1.2 What is the gateway address that client-hamburg needs to use if it wants to connect to a server on the Internet?

1.3 What is the broadcast address to reach only all the hosts that are connected to the Paris' network?

Exercise 2: Practical subnetting

This exercise involves working with multiple IP segment networks. There are two workstations and one router, and you will build the network shown in figure 2 with Virtual Machines.
Choose an IP range for subnetting and for attributing to different nodes. Configure the interfaces on the VMs accordingly, and manually set the routing tables to the correct values.

Once all interfaces are set up, ping all machines from all machines on both networks:

1. From **server-HH** send ping messages to the router and to **client-PA**
2. From the router send ping messages to **server-HH** and to **client-PA**
3. From **client-PA** send ping messages to the router and to **server-HH**
4. Record the content of the routing table on all machines before you continue.

Set up the routing tables as required and configure the router. Your task is completed when you can send a ping to all other hosts and get a reply.
Show the working setup to your supervisors.

Exercise 3: Routing and DNS

To complete this lab exercise you will need three linux computers and two firewalls / routers (= 5 VM Images). You will be setting up a network as depicted in Figure 3, the machines that need to be set up inside a VM are marked and named.

After cloning / installing / configuring the necessary VMs, **change the names of the VMs to match the names shown in Figure 3**.

You need to set up your three internal networks (Hamburg, Passau and Munich).
The 2 firewalls will connect the three subnets as depicted in the diagram in Figure 3.
To ensure this you should setup a DNS server on server-HH.
The global domain of your internal structure is 'GROUPx.EXAMPLE.ORG'. Make sure each of your machines are in this domain, e.g. '**client-PA.group1.example.org**' is the name of the VM in the PASSAU subnet for group #1.

Make sure all hosts are reachable from each other, so make sure the routing works. You should also be able to open a ssh session from **client-PA** to **server-HH**.
As usual, document all the necessary steps in your lab-report, and show the working set-up to your supervisor.

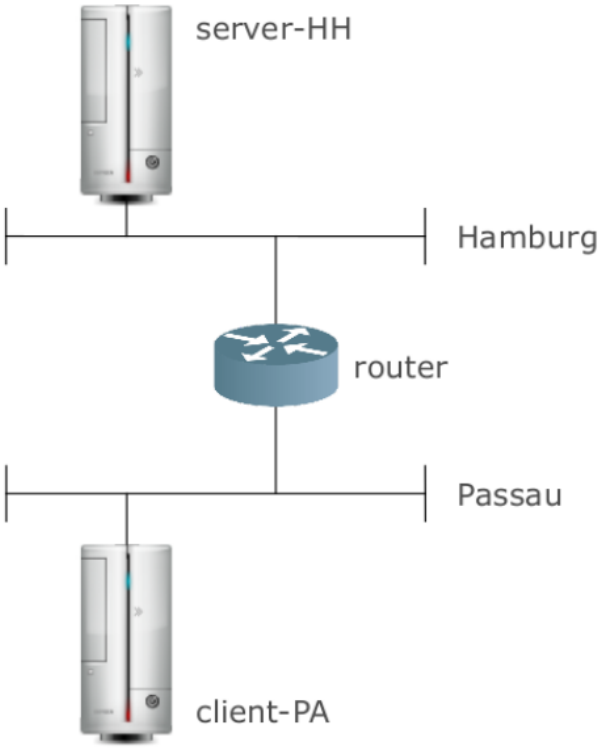

Figure 2: Practical Subnetting

Exercise 3: NAT

Make sure that all the machines inside the three subnets (HAMBURG, PASSAU, MUNICH) can still reach webservers (http, https) on the Internet.

3.1 Explain

Explain the functionality enabled by the keyword 'MASQUERADE' in the context of the NAT configuration. Have you used it in your configuration?

Hint: Suppose your Internet service provider (e.g. Telekom) provides you with a public IP address. Furthermore the IP of your firewall interface connected to the internet is dynamic (e.g. forced reconnect on DSL). In this case you cannot predict what IP (aaa.bbb.ccc.ddd) your firewall interface will be obtaining from your internet provider. How can you do NAT in this case?

Exercise 4: Firewalling

You will be working with iptables on the firewalls only. In order to enforce the following restrictions you need to change your firewall's rulesets.
Document the active rulesets of both FWs and indicate the changes you made to accomplish each step. Also

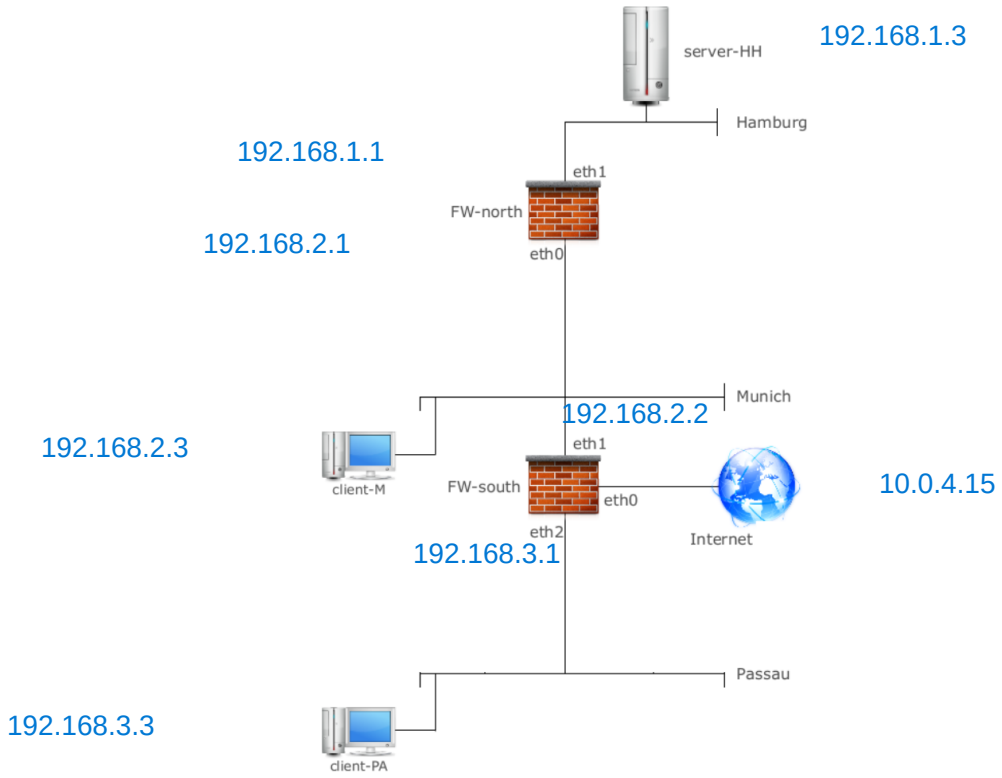

Figure 3: Firewalled networks

write down and explain what you did to test them and if it worked.

4.1 Set the firewalls to deny all connections by default.

4.2 Prohibit machines on the internal network to provide services to the outside (e.g. an Internet reachable webserver on client-PA shall be prohibited), but allow all machines to use any service on any machine (internal subnets & Internet) as long as they initiate the connection.

1. Explain the differences between dynamic and static packet filtering. You should have used a dynamic filtering rule in the exercise above, state which and explain how it works.

2. Explain in what form dynamic filtering is better than static filtering?

4.3 Tell the firewall FW-south to REJECT all icmp requests from the PA Subnet and the Lab's network. Test this by trying to ping from client-PA, but also try if the reverse succeeds (e.g. it shall still be possible to ping the computer client-PA from server-HH).

4.4 Remove the ability to ping the firewalls themselves. This means you must tell the firewall to REJECT all icmp requests addressed to the FW-north and FW-south.

4.5 SSH sessions are only allowed to server-HH, all other ssh connections (despite of their destination or origin) shall be blocked.

4.6 Make sure that the FW facing the Internet (Lab's Net) prohibits that IP packets with a source address of the internal subnets arrive on the external interface (i.e. eth0 on FW-south).

1. (10%) What is the reason to have FW rules that prohibit IP packets with a source address inside the internal subnet to leave to the external interface?

Exercise 5: Firewalling continued

You will allow certain services, again only working with iptables on the firewalls. In order to enforce the following restrictions you need to change your firewall rulesets. Please document the active rulesets of both FWs and indicate the changes you made to accomplish each step.

Also write down and explain what you did to TEST if it works.

5.1 Give the iptables commands / rules that allow users on subnet PASSAU to view web pages (http, https) on a web server running in subnet HAMBURG (start/install web-server on server-HH). The rules shall block access to this server from the MUNICH subnet.

5.2 Write the iptables commands / rules to allow HTTP and HTTPS traffic from the Internet (Lab's Net) into the HAMBURG subnet. This includes access to a web server on server-HH.

5.3 Do not allow nor route any packets that try to use any host other than server-HH as their DNS nameserver. The DNS server port is 53. DNS can use both the tcp and udp protocols (udp by default).

5.4 Can you still browse the internet? Explain why / why not. You still want all machines (in all three subnets) to browse the World wide Web (http/https). There are, roughly speaking, ways to accomplish this in regard to DNS resolution.

HINT: There is one easy solution (firewall rule based) that you can use. The more complicated involves working on the DNS server. Shortly explain the difference between the two solutions, choose one solution, and implement it.

Show the working setup to your supervisors.

5.5 Log all traffic that attempts to connect to server-HH.

5.6 Log all attempts to scan the standard ports for Microsoft networking from the Lab's Net.

5.7 In the exercise above you have enabled logging of certain events. Why is it important to keep and analyze the logs? What can you do with them?

Exercise 6: -EXTRA-CREDITS- DNS in more detail(+20% - Optional)

You have set up a DNS server on **server-HH**. Assume your subnets are larger now, thus you have a lot of DNS entries for each of your subnets. Under this scenario, it might be interesting to have several DNS servers. Also, assume you have no globally acting administrator, thus every subnet's DNS server is being administered individually.

Subdomains and different zones
You will create three subdomains (PASSAU; MUNICH; HAMBURG).
The IT department of Passau will manage the small Munich office, so you will only need a DNS zone in the south that caters for the subdomains PASSAU and MUNICH. Therefore, you need one for HAMBURG in the north.

You will have three subdomains and two zones: One (called 'south') for PASSAU and MUNICH, and the second (called 'north') for HAMBURG.
Consecuently, the name of the VM in the subnet PASSAU will change from '**client-PA.groupX.example.org**' to '**client-PA.passau.groupX.example.org**'.
The machine **client-PA** will become the DNS server to manage the 'south' zone, so install all the necessary software.

6.1 Explain the concept of DNS zones. Explain the difference between a 'managed' and a 'delegated' zone.

6.2 Explain shortly (no more than 10 sentences) how the Internet's DNS system is set up (e.g. root servers, zones, registrars ...).

Reverse DNS lookup
Allow reverse lookups.

DNS Forwarding
There are two ways to allow internal clients to resolve DNS names outside your own network. This 'problem' also occurred in Exercise P.3.5.d. Now we want to solve this problem 'inside' the DNS server. You will set the **server-HH** to act as a DNS forwarder for the example.org domain.

6.3 Explain the concept of DNS forwarding? Are there any security gains when DNS forwarding is used? Is there any additional filtering that would be possible (give an example)?

Zone Transfers
One of the neat concepts of DNS is the hierarchical structure and the fact that two or more servers might be able to provide answers to DNS queries. We want to use this redundancy within our network too. Otherwise, if a single server is used and that server is not responding, queries for names in the zone can fail.

6.4 Explain in detail what a zone transfer is? Why is it needed? What is the difference between a zone transfer and a zone replication?

6.5 What is the concept/idea behind 'Incremental zone transfers' ? What is the gain? Are they widely used in today's DNS system?

For additional fail safety we want our DNS server for the 'south' to allow zone transfers. Enable it to provide the necessary information when asked. For example use an 'nslookup ls' command from a different machine to dump the DNS records of **client-PA**.

6.6 Can you think of any malicious attacks? Give some details how you would carry out such attacks.

Restrict zone transfers
We do want to increase the security, but still allow zone transfers to happen.
What are the steps you can take to allow zone transfers only among certain entities? Shortly explain and then implement the necessary steps to restrict the zone transfer to **client-PA** and **server-HH**.

Secure zone transfers between certain groups
If there are other groups doing this exercise, try to securely transfer one of your zones (south or north) between your DNS server on **server-HH** and their DNS server on **server-HH**. This might involve changing firewall rules too.

Document each step in detail very carefully.

Hint: there are several security options to choose from. Start from the lowest set of options, and try to move to a more secure set of options only after it worked. Remember that you can save the state of your VMs before changing the rulesets!

6.7 Whether or not you succeeded: What are the general options to secure DNS transfers? How do they roughly work? What do they rely on (in terms of relationships)?