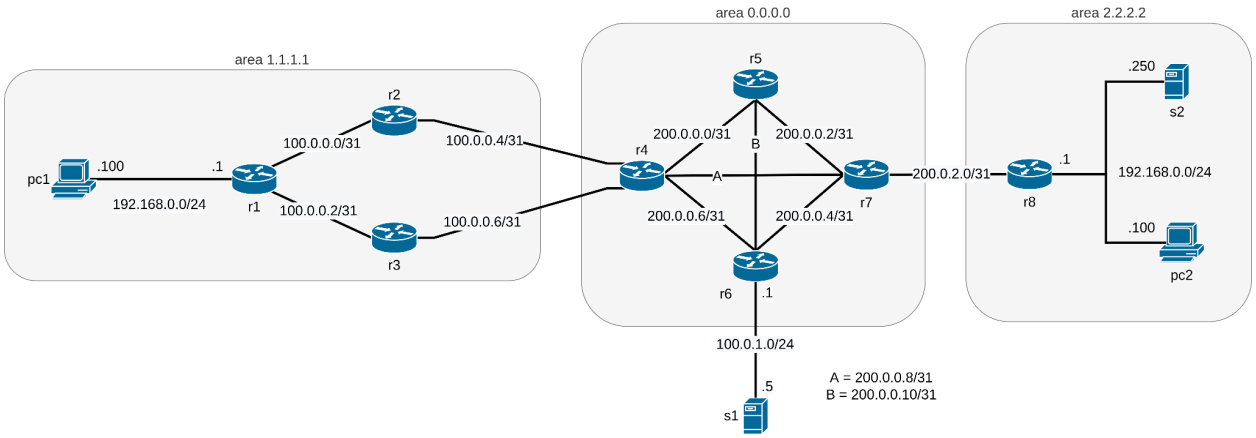
Network Infrastructures – Second Midterm



Given the topology in figure, reproduce it in Kathara. You must use container names and addresses specified in the figure above. Container names should be all in lowercase.
For /31 subnets, the addresses are assigned with the following rule: the lower router number takes the even address. The maximum points are **10** and are assigned as follows:

1. +0.25 points: Lab created with correct lab.conf and folders created correctly. Assign to all routers, PC and servers static IP addresses via /etc/network/interfaces.
2. +0.25 points: Configure OSPF on routers. Respect areas given in figure.
3. +0.5 points: Set up private addresses with a NAT on r1 and r8 for subnets 192.168.0.0/24
4. +1 points: Set up a firewall on r1 and r8 blocking all traffic unless is instantiated by the respective NATted subnets
5. +1 points: Set Up a SSH server on s1 with a user “myuser1” and on s2 with a user “myuser2”, both accessible via pubkey authentication by pc1.
6. +1 points: Add firewall rules enabling you to redirect incoming SSH traffic on r8 to s2. If done correctly, on pc1 you should be able to connect via SSH to s2 by specifying r8’s public address.
7. +0.5 points: Add a firewall rule on s2 such that it drops every packet which is not SSH or OpenVPN
8. +0.5 points: Add a firewall rule on r4 blocking all TCP or UDP connections originated from pc1 and directed to the public IP of r8. Now you should no longer be able to connect via SSH from pc1 to s2

9. +1 point: On pc1, configure a SSH port forwarding using the server s1, enabling you to connect via SSH from pc1 to s2.
10. +1.5 points: Set Up a new CA and generate a certificate for a server with CN “myserver” and two for two clients with CN “pc1” and “s2”
11. +2 points: Set Up an OpenVPN server on s1 and an OpenVPN client on pc1 and s2. Use the certificates you generated in the previous point. In the server configuration file add the directive “`client-to-client`”, which enables two clients to “see” each other on the VPN. The subnet of the VPN is 10.0.0.0/24. The VPN ip address of the server and of pc1 should be the default one. The VPN ip address of s2 should be 10.0.0.100.
12. +0.5 points: You should be able to connect from pc1 to s2 using the VPN. Why is the r4’s firewall not blocking the connection? Capture SSH traffic over the VPN on r4 and save it in “shared/capture.pcap”.

In the lab folder, create a text file “`commands.txt`” and write down the SSH port forwarding command of point 9.

It is not required to perform SSH key generation, SSH port forwarding and CA certificate generation at startup.

Tip: remember to use “`kathara connect`” if you need multiple terminals on the same node

Restart of all the daemons is required.