



# ASSIGNMENT 4

Configuring filtering rules,  
IDS/IPS

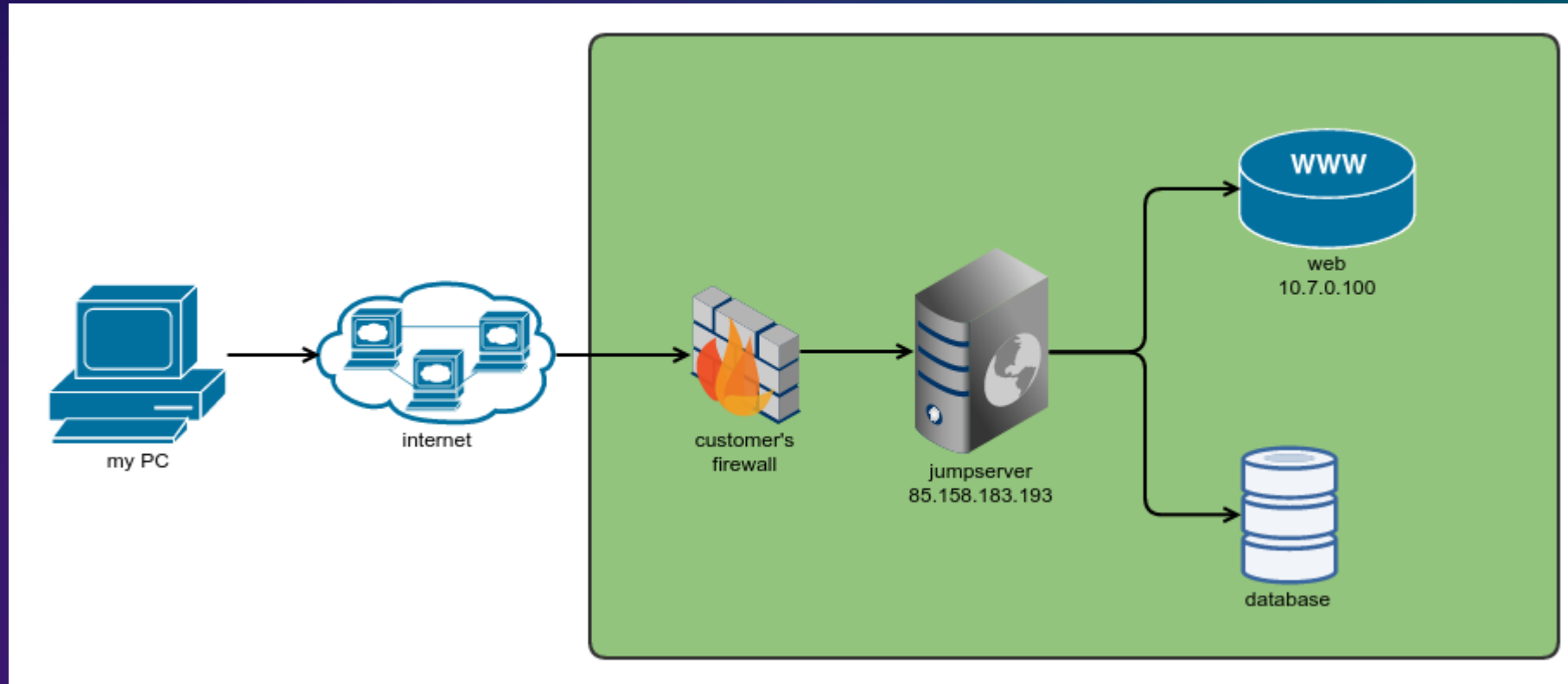
Paolo Molinaro  
pm222py@student.lnu.se



## TOOLS AND REQUIREMENTS

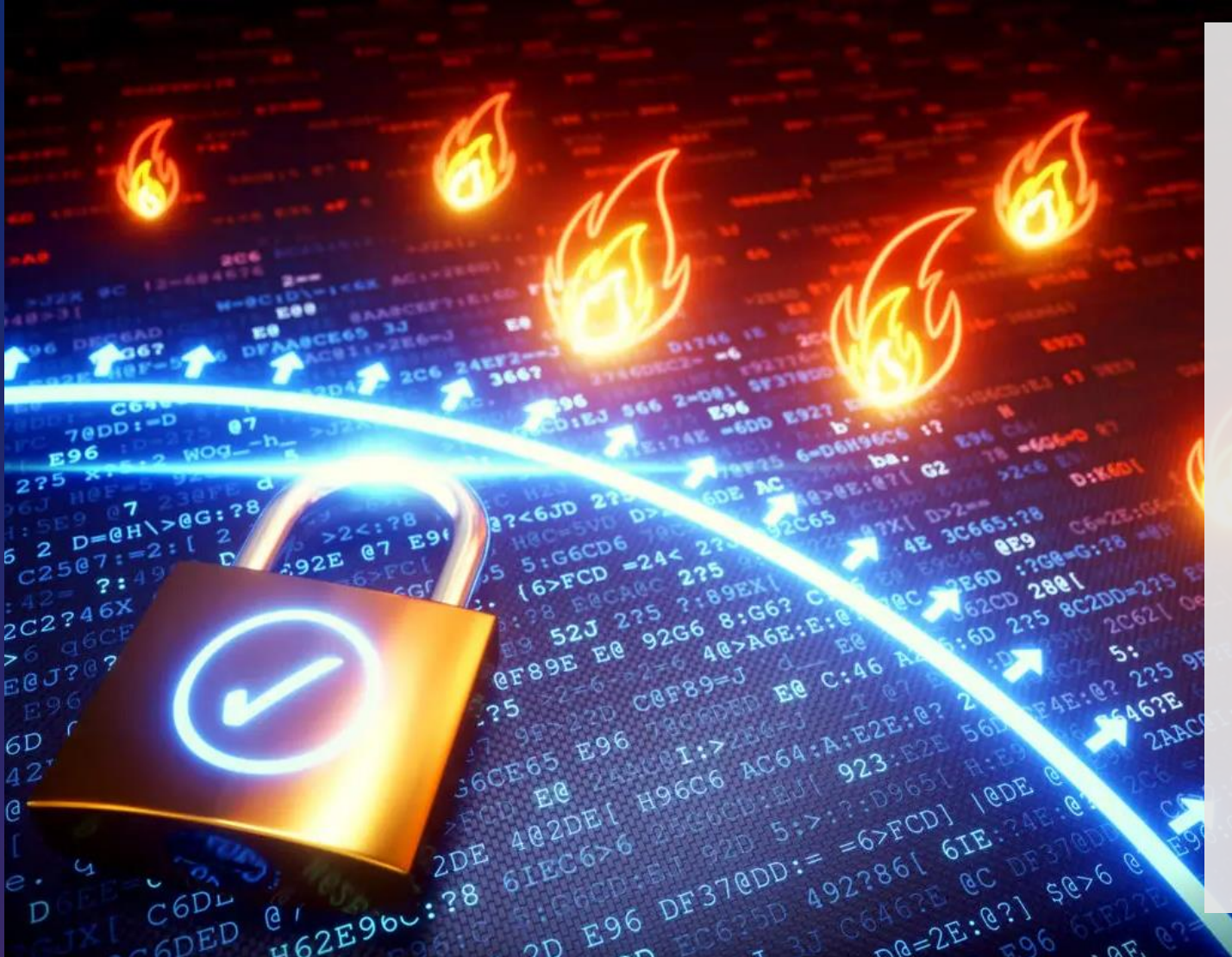
- Built-in firewall tool for Linux, iptables
- FTP server (use vsftpd) and FTP client
- CScloud as infrastructure
- Remote connection over SSH
- Configure
  - A router, a network
  - Key-pair for SSH, security group for SSH
  - 3 Ubuntu machines (1 as a jump machine)
- 8-pages limit!

# TOPOLOGY



# REQUIREMENTS

- Pay extra attention to keywords: **manually** and **stateful**.
- Think about the real-world.
  - There are other computers on the network that must communicate with this machine!
- Detail is important here!
  - Be precise with your rules and explain why they work.



# FIREWALLS

- A firewall is a system, or group of systems that enforces an access control policy between networks.
- Rule-based inspection of traffic.
- Inbound and outbound traffic.
- You will try:
  - **Stateless** approach.
  - **Stateful** approach.

# FILE TRANSFER PROTOCOL

Has a control and data channel, making it more complicated to filter and manage in a firewall.

- Has two modes of operation
  - **Passive**
  - **Active**

You must learn how these work!



# IDS/IPS

- A firewall is a system, or group of systems that enforces an access control policy between networks.
- Rule-based inspection of traffic.
- Inbound and outbound traffic.
- You will try:
  - **Stateless** approach.
  - **Stateful** approach.

## USEFUL LINKS

- [cscloud](#)
- [Tutorial for cscloud](#)
- [GNU/Linux tool summary and usage](#)
- [Iptables](#)
- [vsftpd](#)
- [tldr](#)