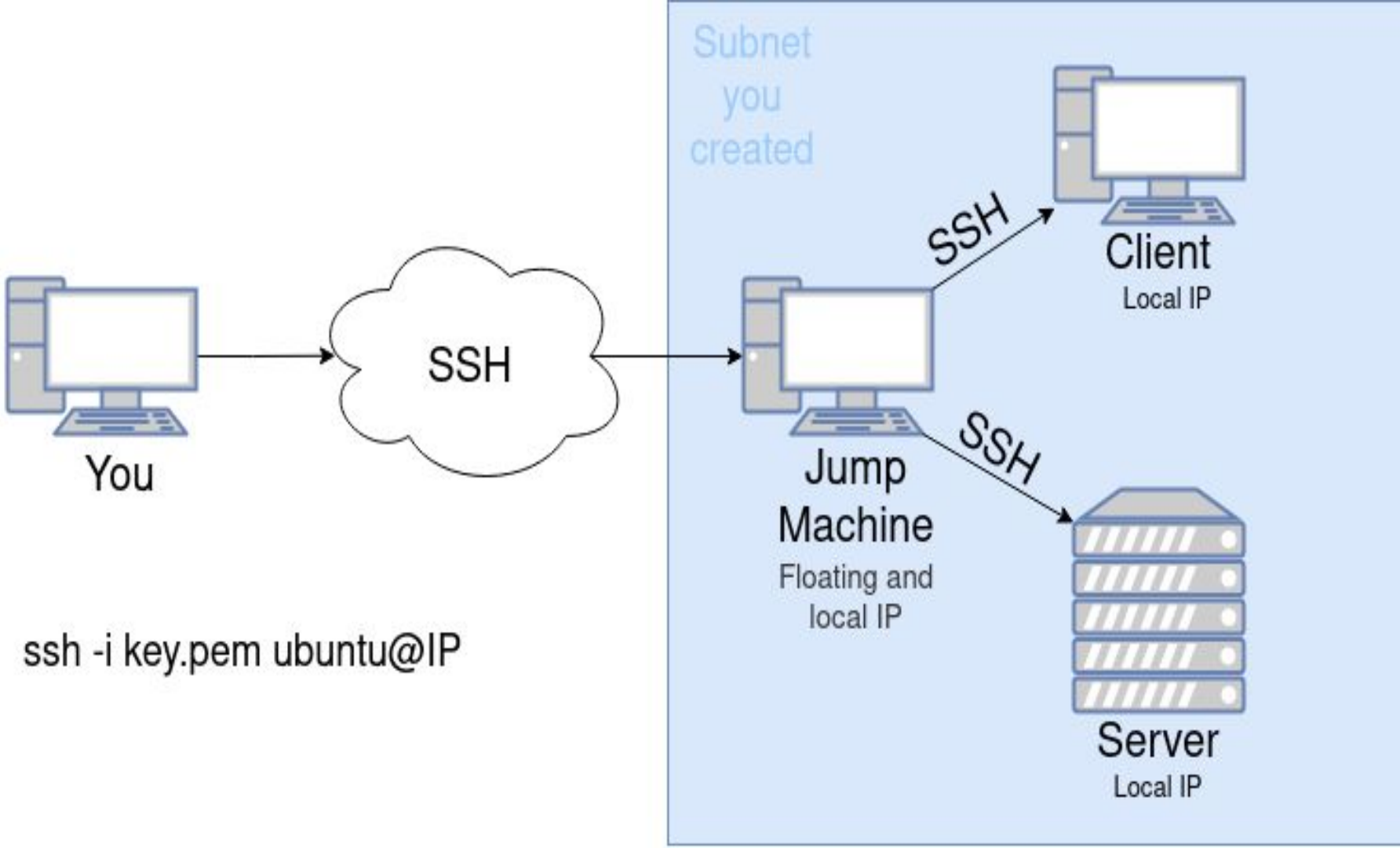
Assignment 4

Configuration & Set up of Filtering Rules, IDS/IPS

Kristoffer Björklund & Nikolaos Papadopoulos
kb222wa@student.lnu.se np222fc@student.lnu.se

Tools and Requirements

- Built-in firewall tool for GNU/Linux, *iptables*
- An FTP Server (vsftpd) and an FTP Client(Within terminal)
- CScloud as your infrastructure
- Remote connection over SSH
- Configure
  - A router, a network
  - A key-pair for SSH connectivity, a security group for SSH connectivity
  - 3 Ubuntu machines (1 as jump machine)

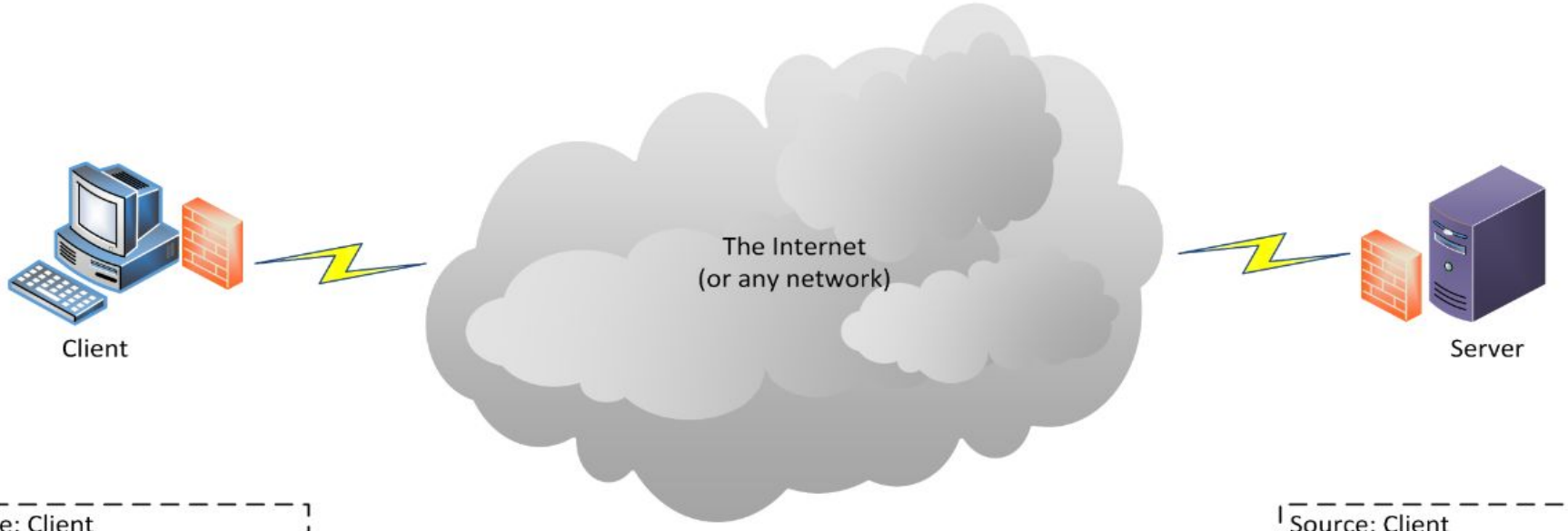

Subnet
you
created
SSH
Client
Local IP
You
SSH
Jump
Machine
Floating and
local IP
SSH
Server
Local IP
ssh -i key.pem ubuntu@IP

Tools and requirements

- Pay attention to keywords: **manually** and **stateful**
- Think about the real-world
  - There are other computers on the network.
- Be meticulous!

Firewalls

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



Source: Client
Traffic: Outbound
Source IP Address (Client)
Source Port (Client)
Destination IP Address (Server)
Destination Port (Server)

Request

Source: Client
Traffic: Inbound
Source IP Address (Client)
Source Port (Client)
Destination IP Address (Server)
Destination Port (Server)

Source: Server
Traffic: Inbound
Source IP Address (Server)
Source Port (Server)
Destination IP Address (Client)
Destination Port (Client)

Response

Source: Server
Traffic: Outbound
Source IP Address (Server)
Source Port (Server)
Destination IP Address (Client)
Destination Port (Client)

File Transfer Protocol

- Traffic in both directions, two channels
- Two modes with different operational details:
  - Active
  - Passive
  - Learn how they work

Controlled experiment

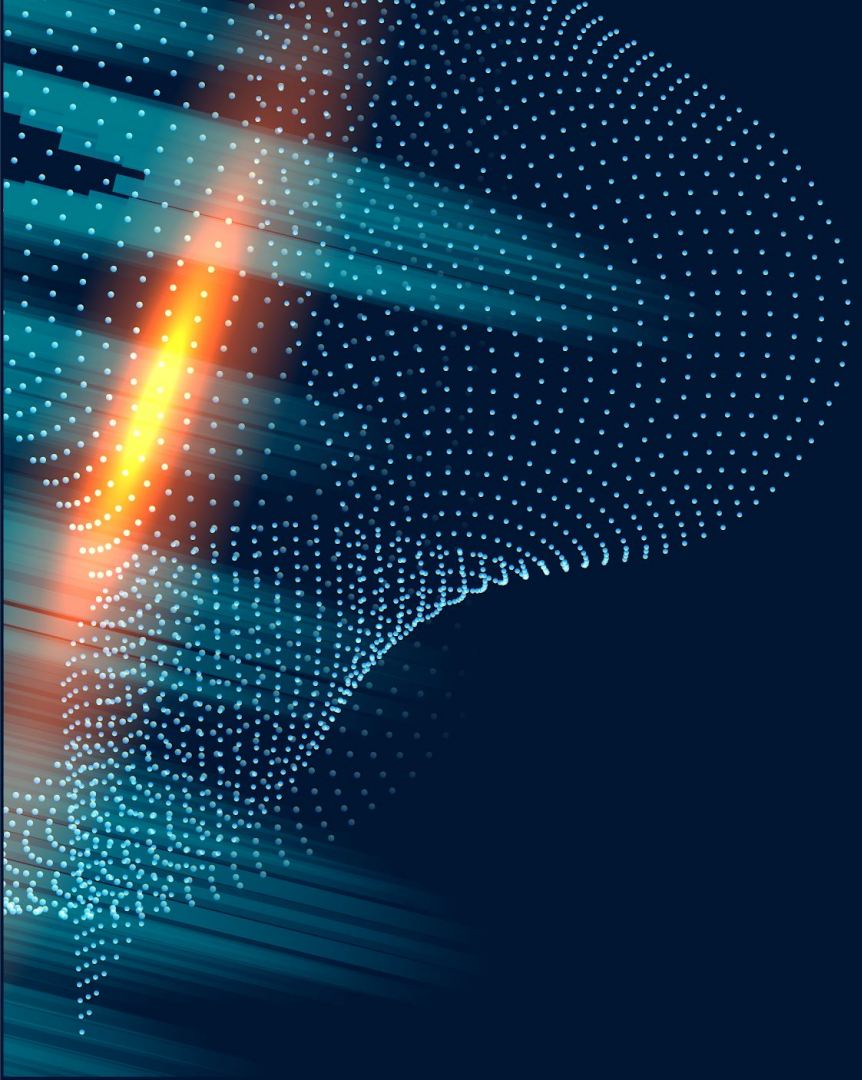
- Experiments are complex, too many variables
- Third party devices will not restrict traffic
  - CScloud provides you with a clean setup
- Do not add unnecessary software or packages

IDS/IPS

- Find different categories
- Elaborate on *Extrusion Detection*
- Suricata is a good open-source example:
  - Check docs to learn its rule syntax
  - Explain!

Useful Links

- LNU CScloud
- CScloud tutorial
- GNU/Linux Command-Line Tools Summary
- Iptables
- vsftpd



Gentle reminder!

Tough time never lasts, only tough people last.