



The Brazilian Cybersecurity Testbed

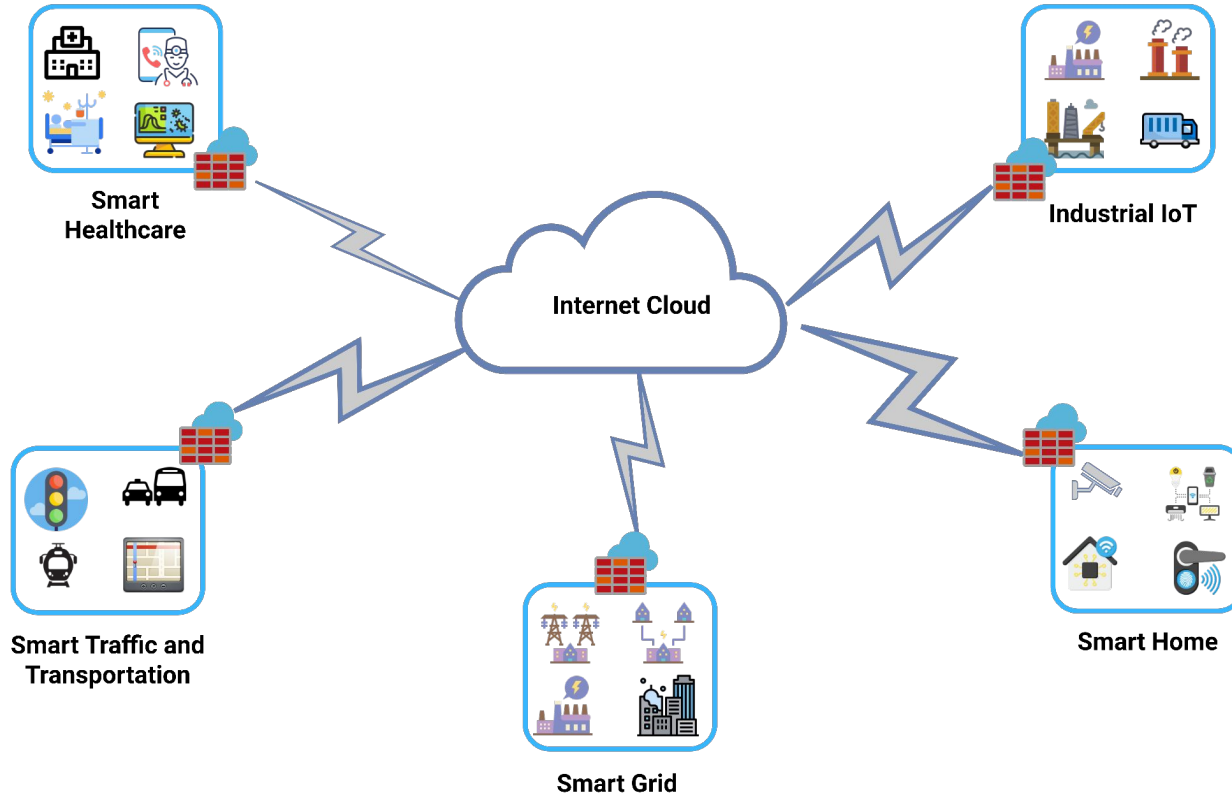
Bruno H. Meyer, Davi D. Gemmer, Marcos F. Schawarz, Emerson R. de Mello, Michelle S. Wangham

mentored.project@gmail.com

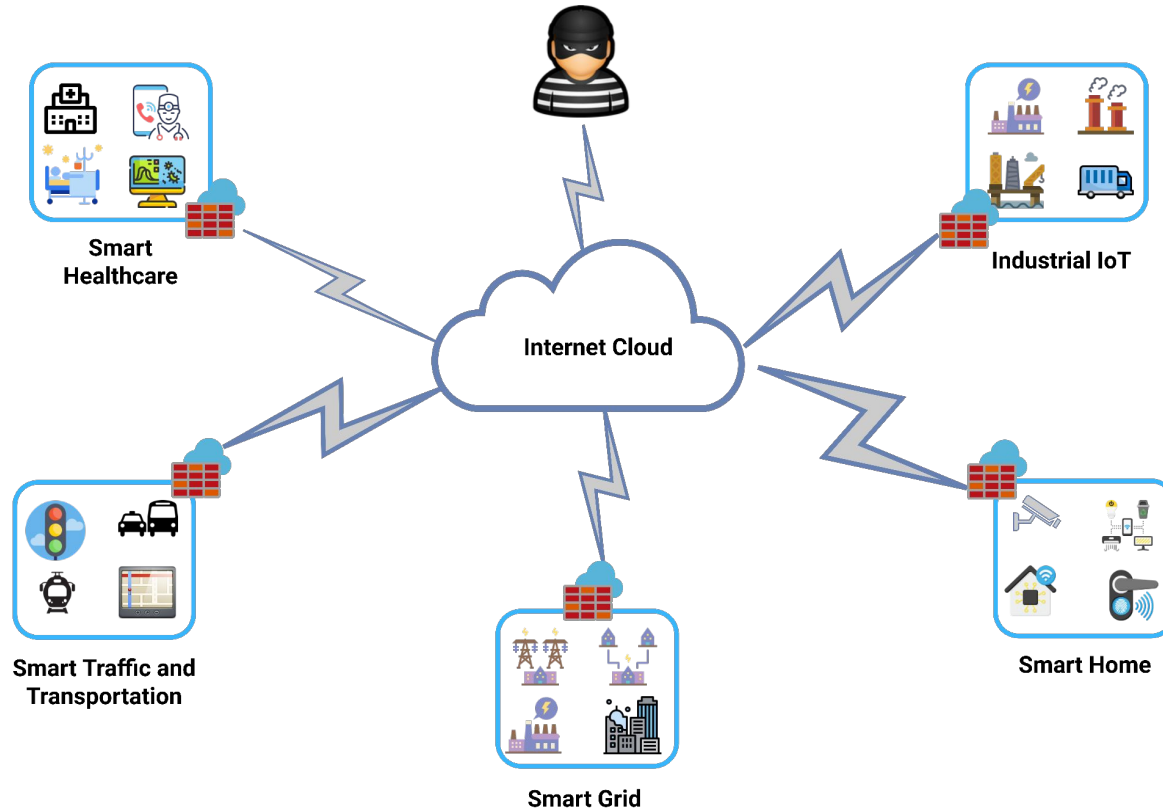
GLOBECOM 2022



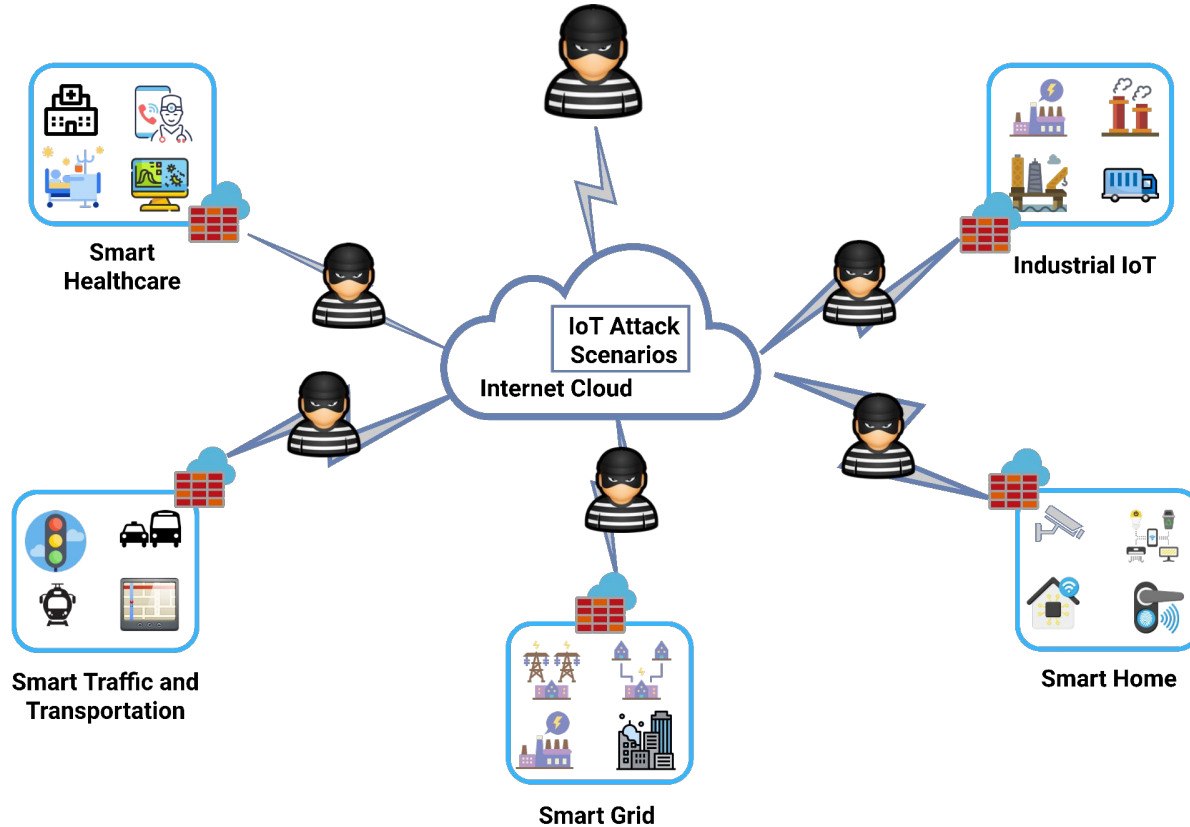
Internet of Things (IoT)









IoT Security

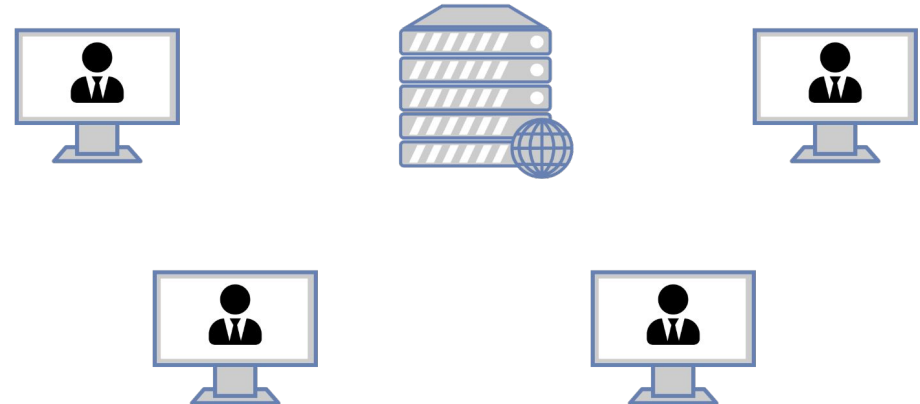


IoT Security









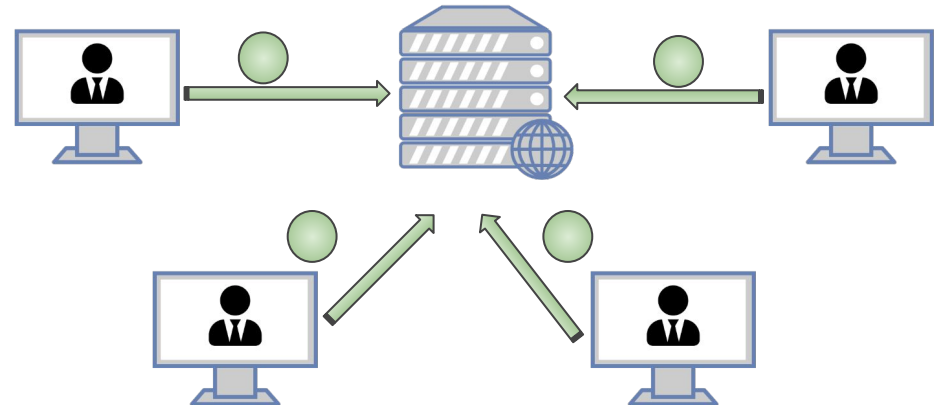
DDoS Attacks

-  Benign traffic
-  Malicious traffic
-  Clients
-  Attackers
-  Server (DDoS Target)
-  Failed connection









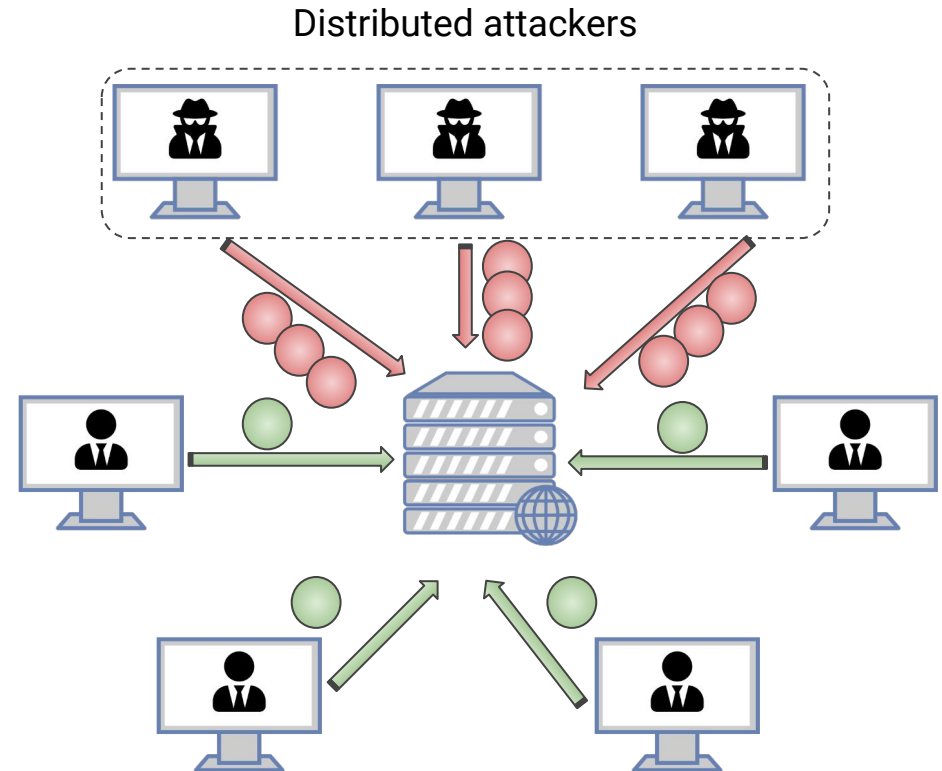
DDoS Attacks

-  Benign traffic
-  Malicious traffic
-  Clients
-  Attackers
-  Server (DDoS Target)
-  Failed connection









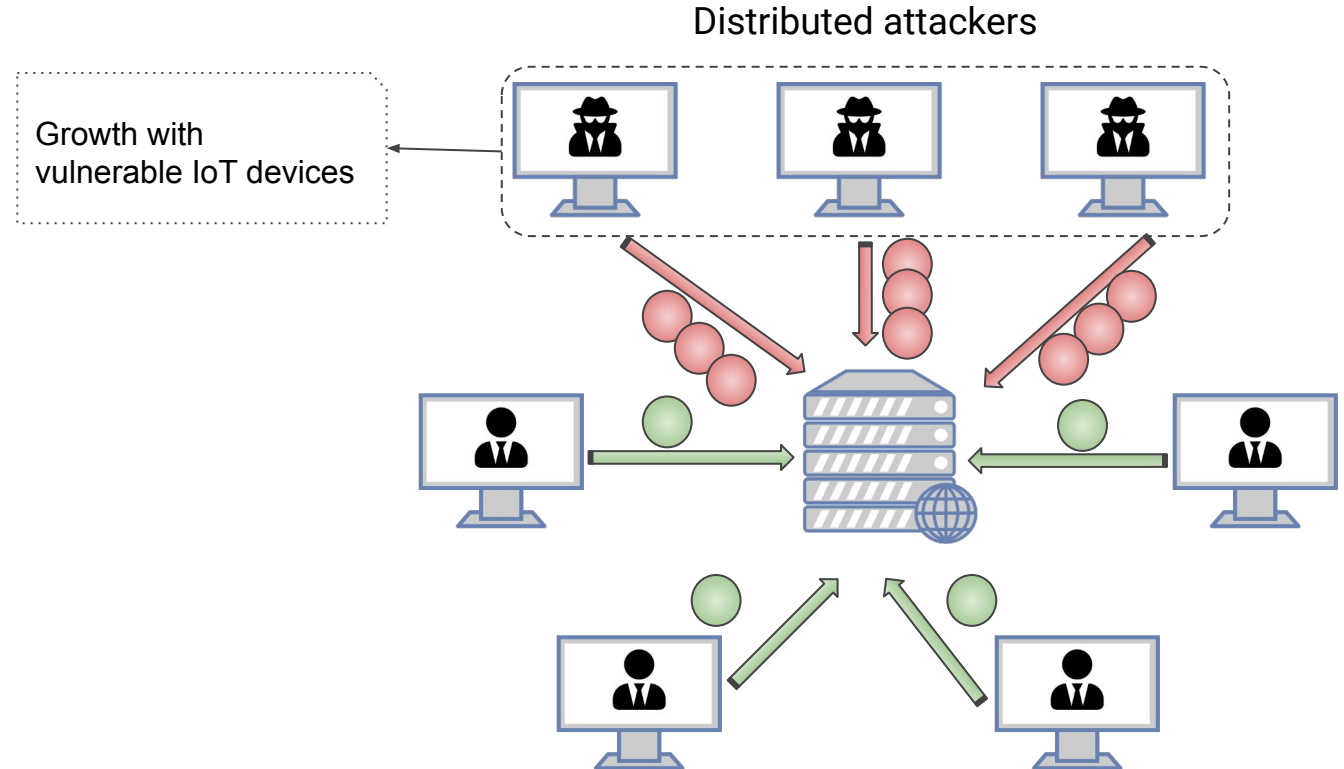
DDoS Attacks

-  Benign traffic
-  Malicious traffic
-  Clients
-  Attackers
-  Server (DDoS Target)
-  Failed connection









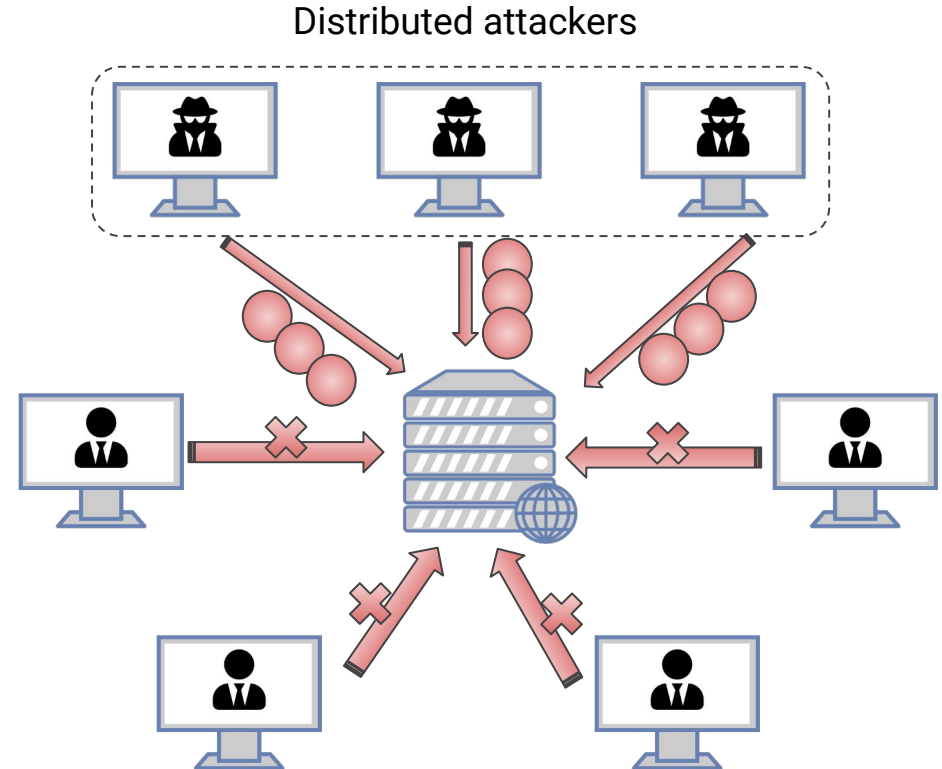
DDoS Attacks

-  Benign traffic
-  Malicious traffic
-  Clients
-  Attackers
-  Server (DDoS Target)
-  Failed connection



DDoS Attacks

-  Benign traffic
-  Malicious traffic
-  Clients
-  Attackers
-  Server (DDoS Target)
-  Failed connection



Motivation



- IoT Testbeds
 - Need for **scalability** and **usability** in a real, large-scale environment for cybersecurity experimentation
 - Must consider a **heterogeneous** infrastructure
 - **Generic** testbeds: serve to multiple applications
 - Support to **cybersecurity** experiments

The MENTORED Project¹



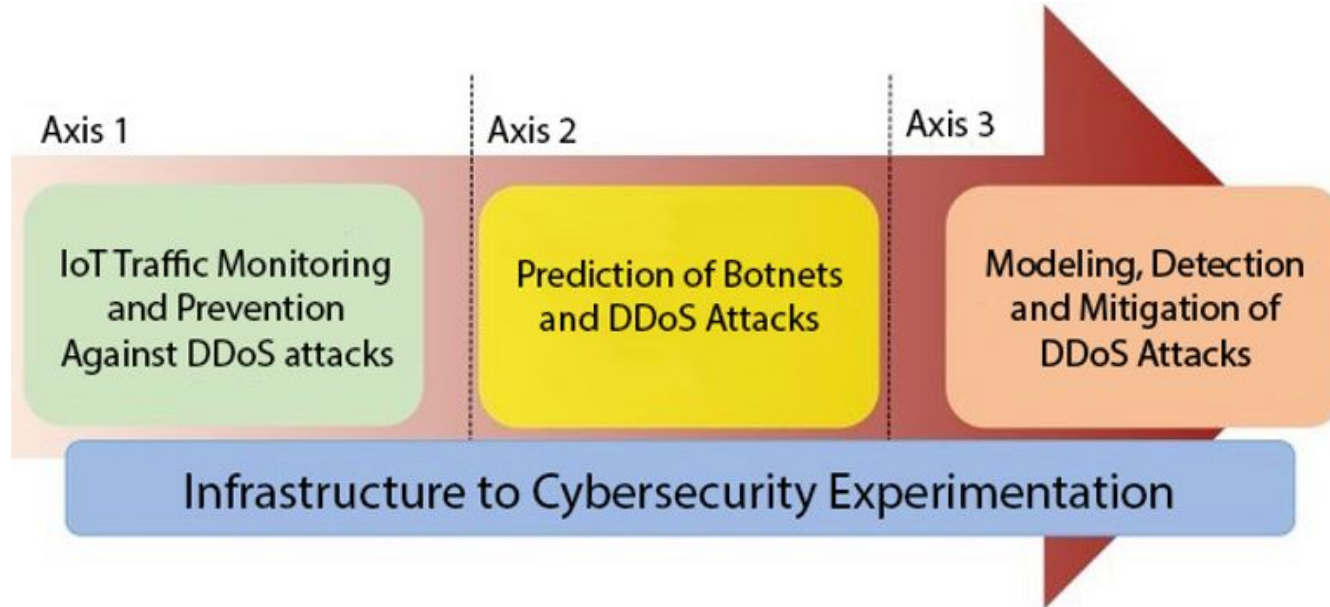
"Our mission is to combat DDoS attacks effects and provide an experimental environment to allow researchers to test their solutions against DDoS attacks generated with the support of IoT networks."

The Mentored Project Team



¹ <https://www.mentoredproject.org/>

The MENTORED Project



Problem Statement



- How to provide an academic Brazilian cybersecurity testbed for Distributed Denial of Service and zero-day attacks?
- How to define usage policies and technologies that efficiently control the resources?

Purpose for this Demo

Defined in this project

Focused Requirements in this Demo

Real-time monitoring

User-Centric Perspective

Scalability

Fidelity

Flexibility

Repeatability

Validity

Safety

Solution

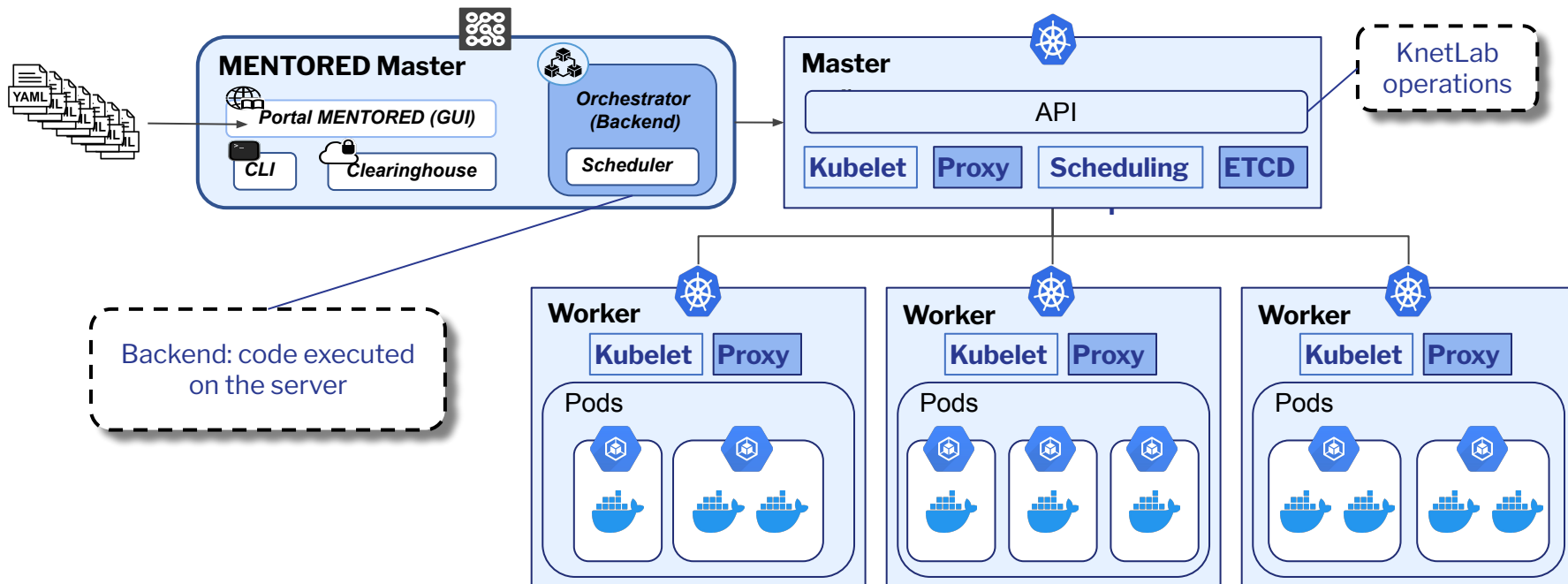
The MENTORED Testbed

Supported by the Software-Defined
Infrastructure of the National
Education and Research Network
(IDS-RNP)

IDS-RNP: geographically distributed
Kubernetes cluster in Brazil

Testbed Architecture

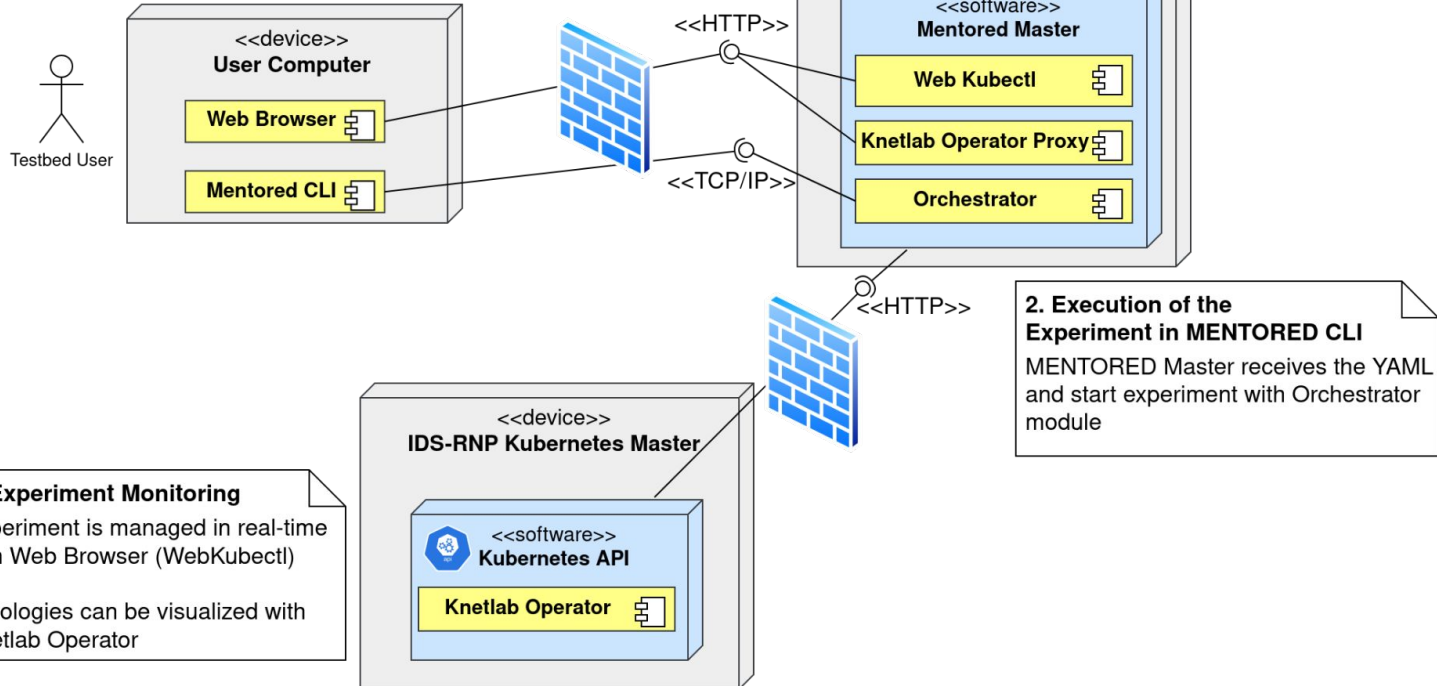
Details



Workflow

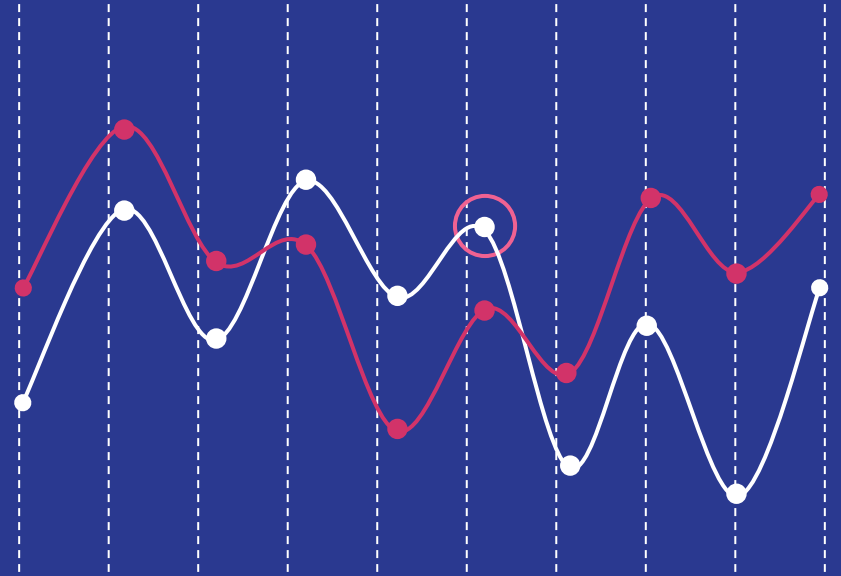
1. Experiment Definition

YAML following Docker and Kubernetes syntaxes

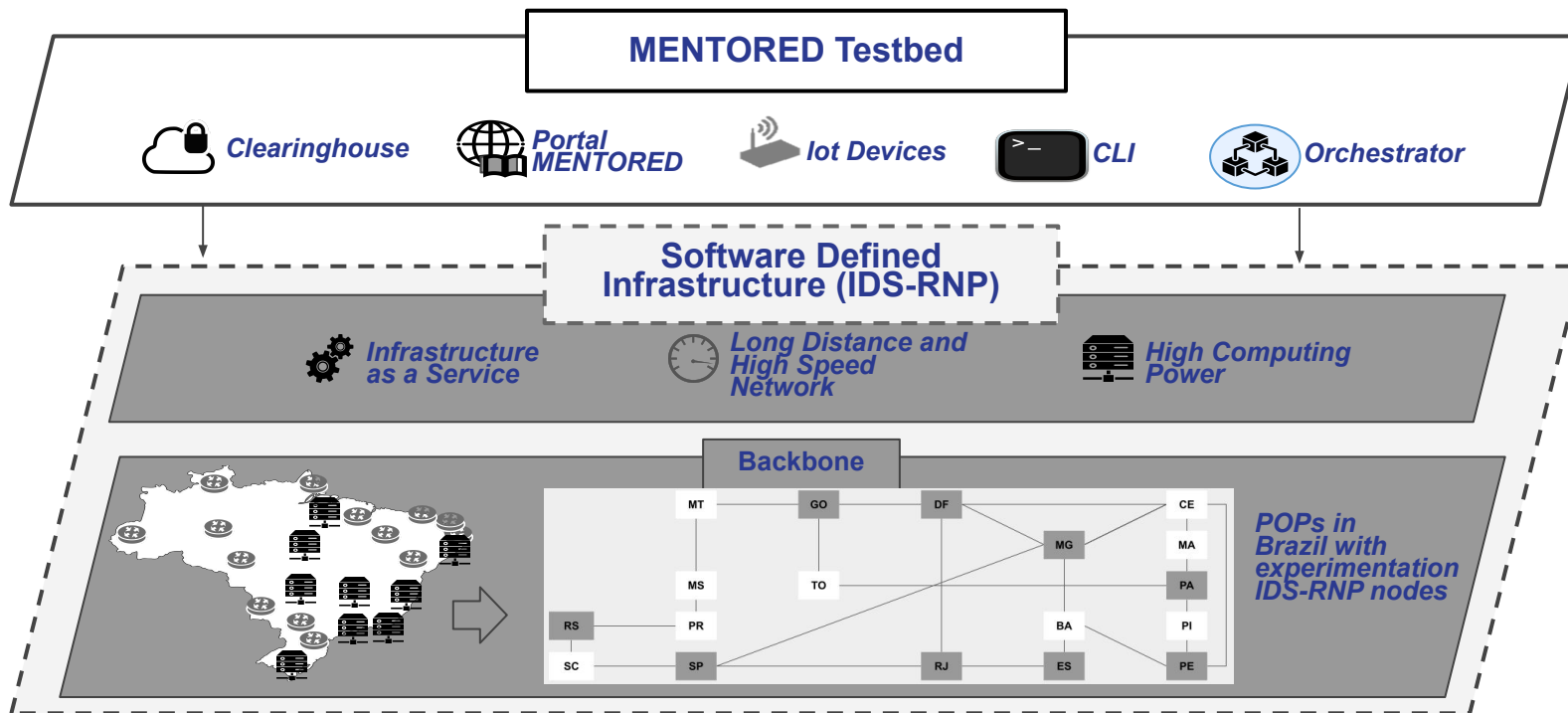


Demo

User perspective:
from the definition to the
execution of a experiment



IT Infrastructure



IT Infrastructure



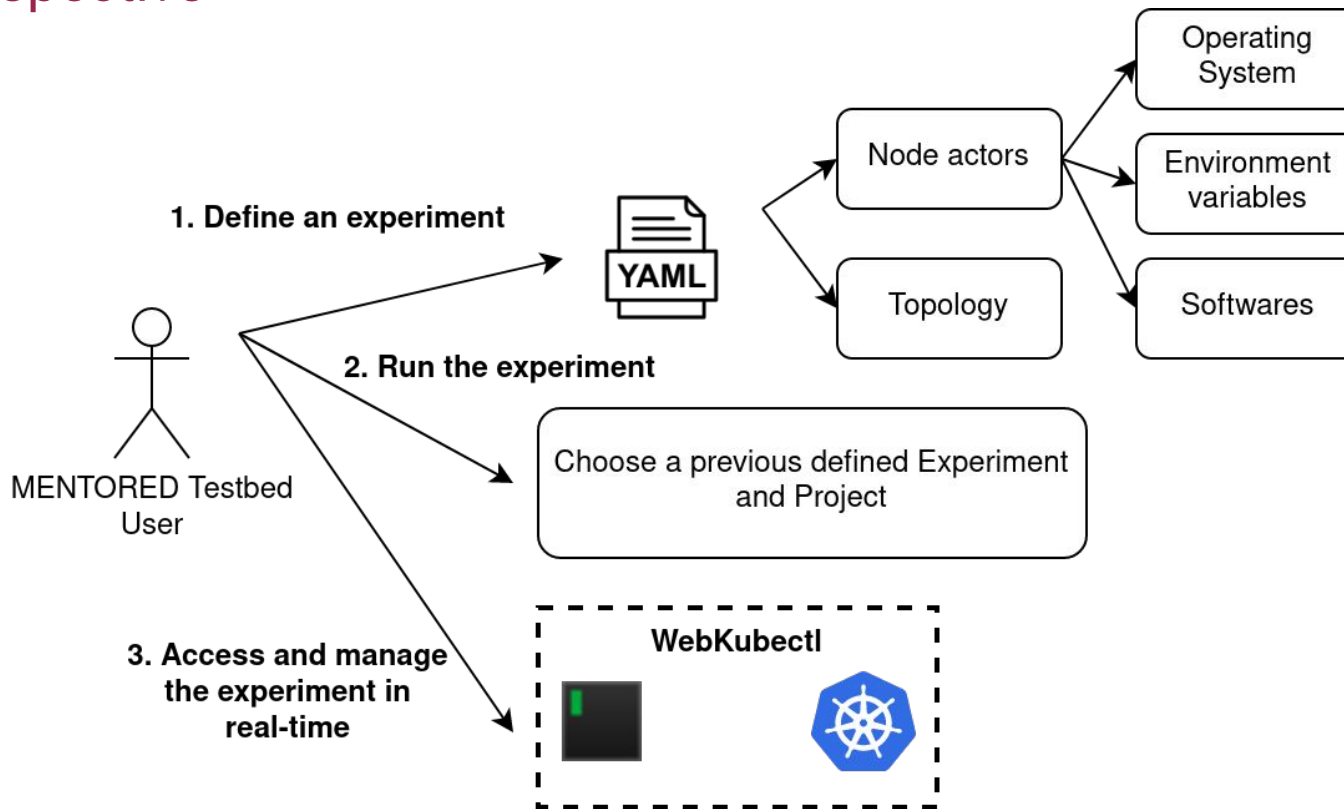
- Backend
 - Kubernetes
 - Python 3
 - Kubernetes Python API
 - WebkubectI²
 - Django (Development of a REST API)
 - Knetlab¹

¹ <https://git.rnp.br/cnar/knetlab>

² <https://github.com/KubeOperator/webkubectI>

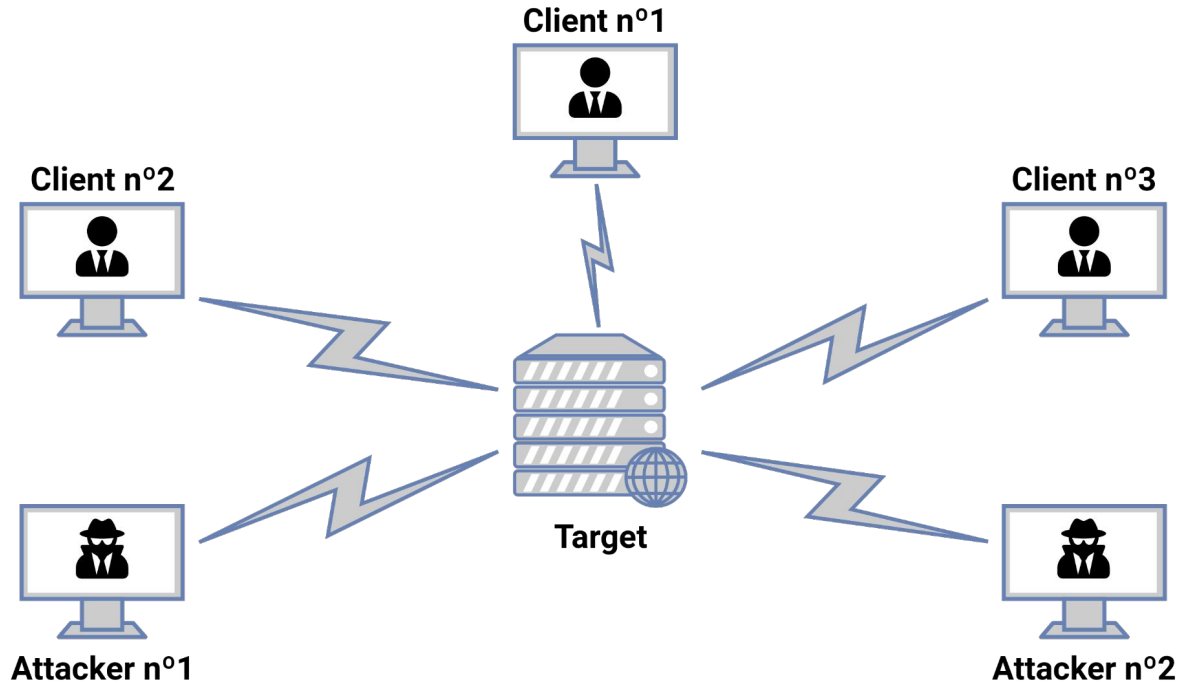
Demo Description

User perspective



Experimentation

Application demo



DDoS Target: Web Server NGINX



Client: Resquest at 0.5 second intervals



Attacker: Use hping software for attack, make 100 requests per second

Parameters

YAML experiment definition

- Node actors
 - Link to docker images (softwares)
 - Number of replicas
 - Environment variables
 - Kubernetes parameters
- Type of topology
 - Predefined patterns
 - Custom topology specified by the user

Running an Experiment



Rest HTTP (API): Accessed by interfaces as python, web page, others

MENTORED Testbed

Username:

Password:

[Log in](#)

MENTORED Testbed

Log in

Api Root

Api Root

The default basic root view for DefaultRouter

GET /

HTTP 200 OK
Allow: GET, HEAD, OPTIONS
Content-Type: application/json
Vary: Accept

```
{
  "users": "http://mentored-testbed.cafeexpresso.rnp.br/users/",
  "groups": "http://mentored-testbed.cafeexpresso.rnp.br/groups/",
  "experiments": "http://mentored-testbed.cafeexpresso.rnp.br/experiments/",
  "projectrequests": "http://mentored-testbed.cafeexpresso.rnp.br/projectrequests/",
  "projects": "http://mentored-testbed.cafeexpresso.rnp.br/projects/",
  "experimentexecutions": "http://mentored-testbed.cafeexpresso.rnp.br/experimentexecutions/"
}
```


Running an Experiment

Experiment configuration



A label for each scenario
Public scenario offered to different users

Raw data

HTML form

Exp name

demo

Yaml description

```
region: 'ids-mg'  
topology: 'ovs_fully_connected'
```

POST

Running an Experiment

Raw data HTML form

Project Projeto: demo

Experiment Experimento: demo

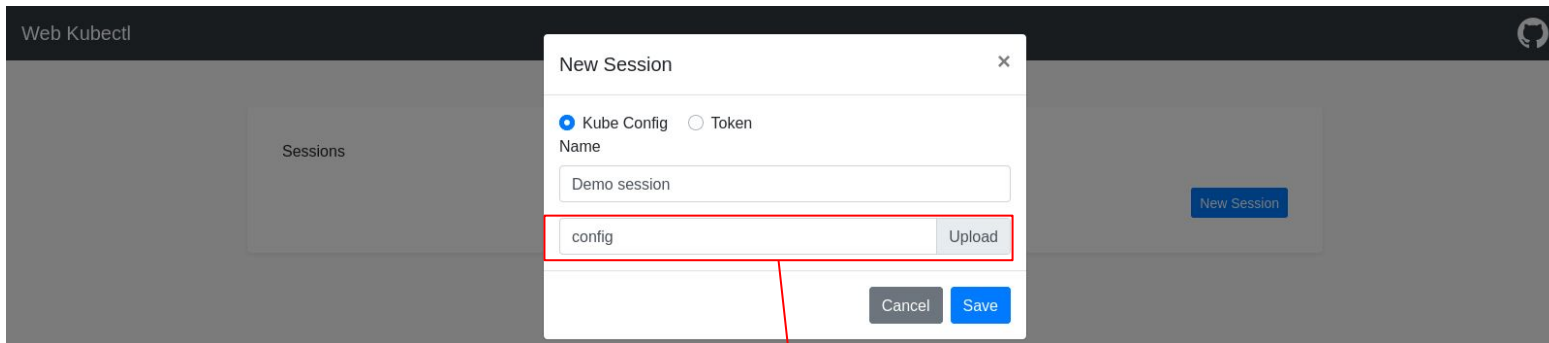
Execution time 300

POST

Maximum time of an experiment and all containers

Running an Experiment

Webkubectl



File related to the experiment obtained from the API

Running an Experiment

Webkubectl



Web Kubectl



Sessions

Demo session Kube Config	Connect Delete
------------------------------------	--

[New Session](#)

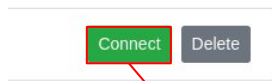
List of allowed sessions for the user to access any container experiment in real-time

Running an Experiment

Webkubectl



Temporary terminal session with unix commands and kubernetes client



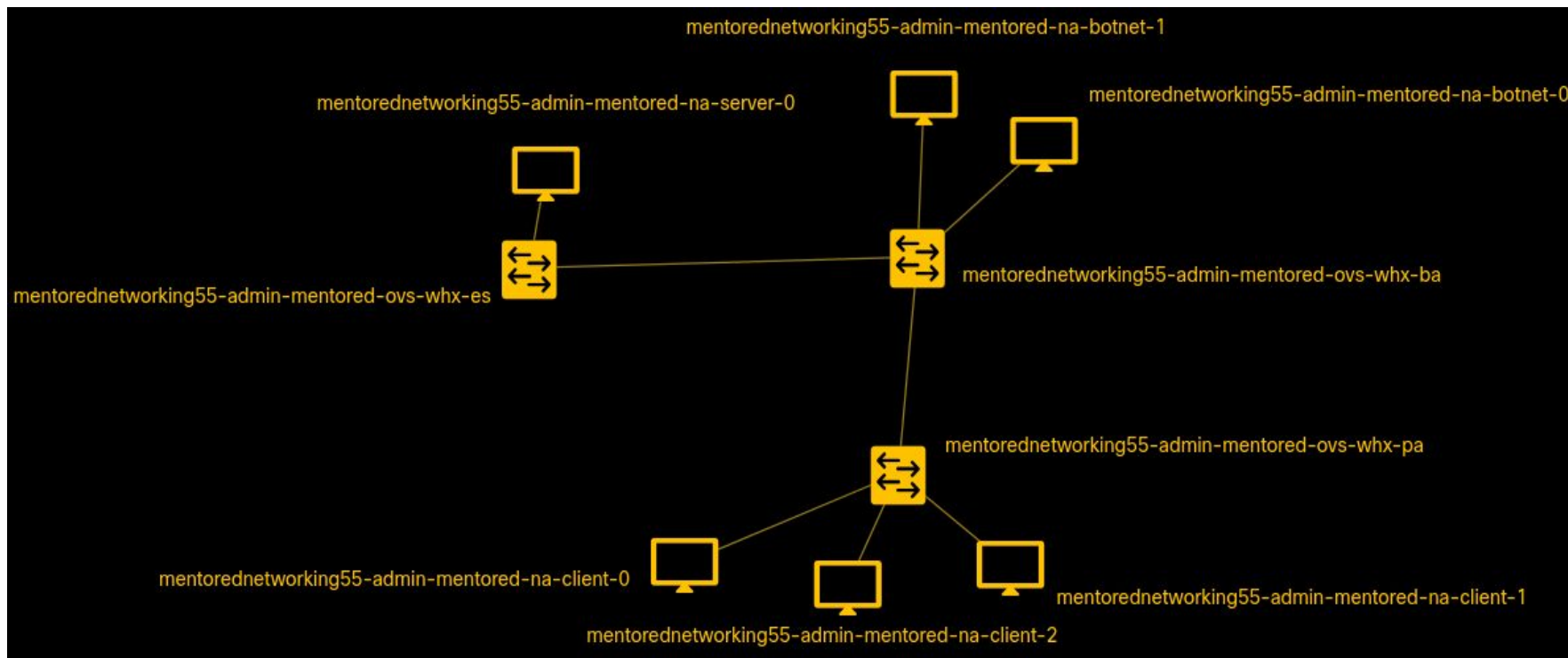
```
Welcome to Web Kubectl, try kubectl --help.
```

```
> kubectl get pods -n test-knetlab
```

```
NAME                                READY   STATUS    RESTARTS   AGE
knetlab-operator-5d78f648df-42vqd    1/1     Running   0           13m
mentorednetworking46-admin-mentored-lan-2-0-745f9c8bdb-m9z7k  1/1     Running   0           80s
mentorednetworking46-admin-mentored-lan-2-1-84f6c7d474-5hndv  1/1     Running   0           80s
mentorednetworking46-admin-mentored-lan-3-0-6d76b55bb9-9mbzk  1/1     Running   0           84s
mentorednetworking46-admin-mentored-lan-3-1-65cf98bcfc-lxvfm  1/1     Running   0           79s
mentorednetworking46-admin-mentored-na-server-0-844b78dfccg9gg8 1/1     Running   0           83s
mentorednetworking46-admin-mentored-ovs-ids-es-5dd9b74759-phdwn 1/1     Running   0           82s
mentorednetworking46-admin-mentored-ovs-ids-mg-764bbdc479-g72rv 1/1     Running   0           81s
mentorednetworking46-admin-mentored-ovs-whx-es-74f578f9f7-q85xq 1/1     Running   0           80s
> kubectl exec -n test-knetlab -it --tty mentorednetworking46-admin-mentored-lan-2-0-745f9c8bdb-m9z7k -- /bin/bash
root@mentorednetworking46-admin-mentored-lan-2-0-745f9c8bdb-m9z7k:/# ls
MENTORED_IP_LIST.json  MENTORED_READY  boot                dev                etc                lib                media              opt                root                sbin                sys                usr
MENTORED_IP_LIST.yaml  bin              create_env_from_mentored_ip_list.py  entry.sh           home              lib64              mnt                proc                run                srv                tmp                var
root@mentorednetworking46-admin-mentored-lan-2-0-745f9c8bdb-m9z7k:/#
```

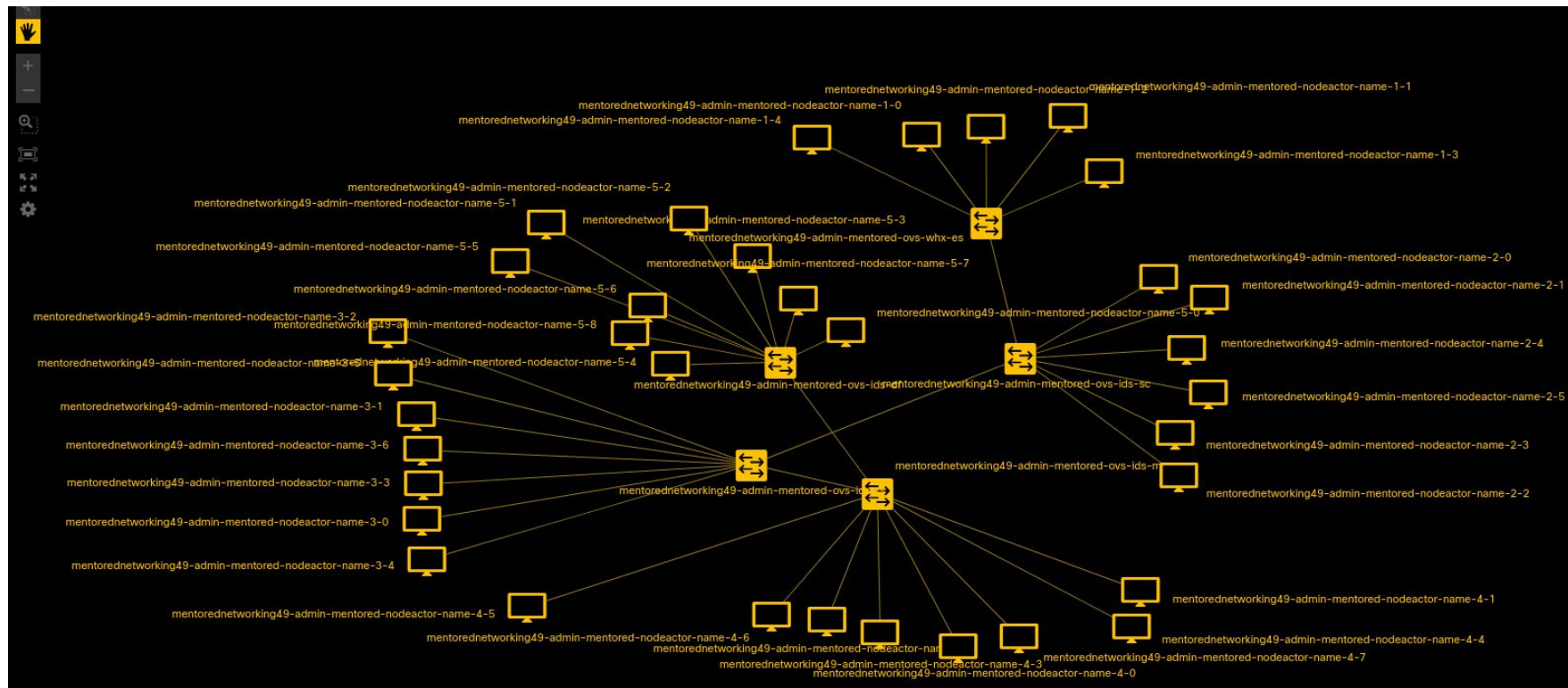
Running an Experiment

Knetlab topology visualizer



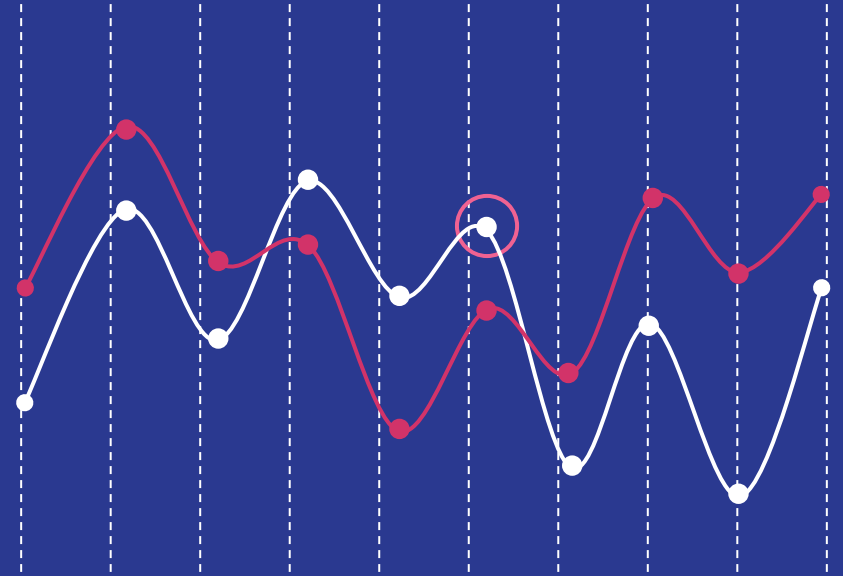
Running an Experiment

Knetlab topology visualizer



Results

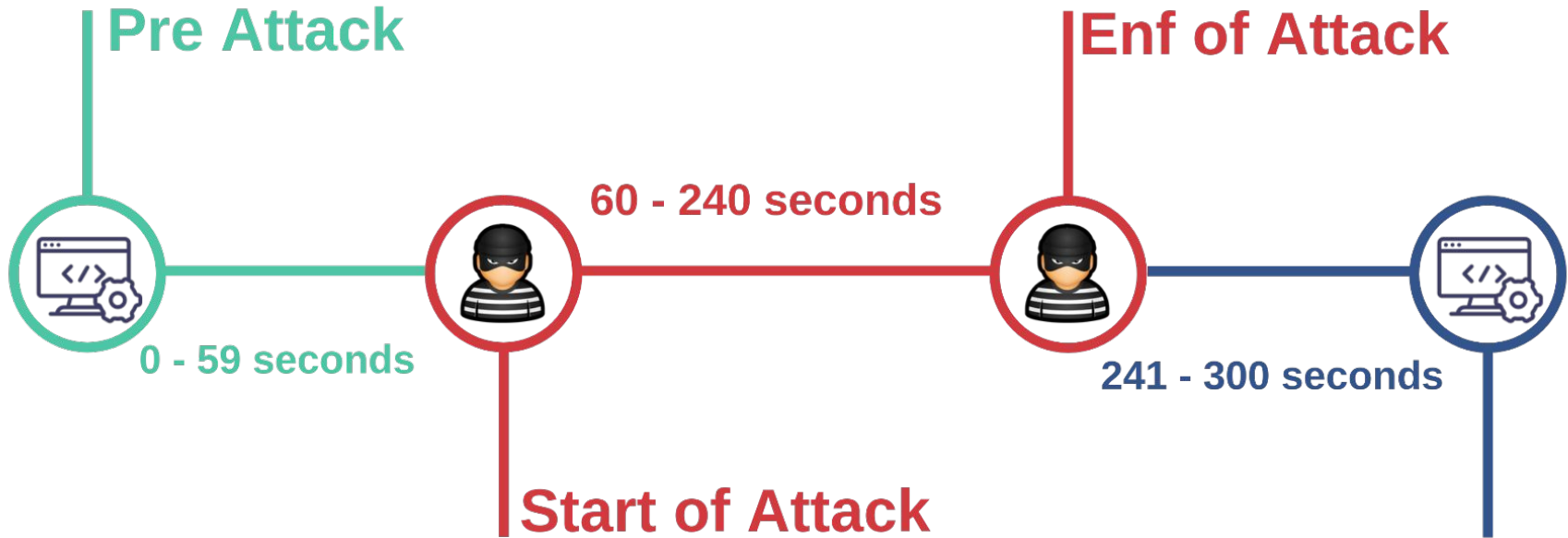
Attack sequence and results



—

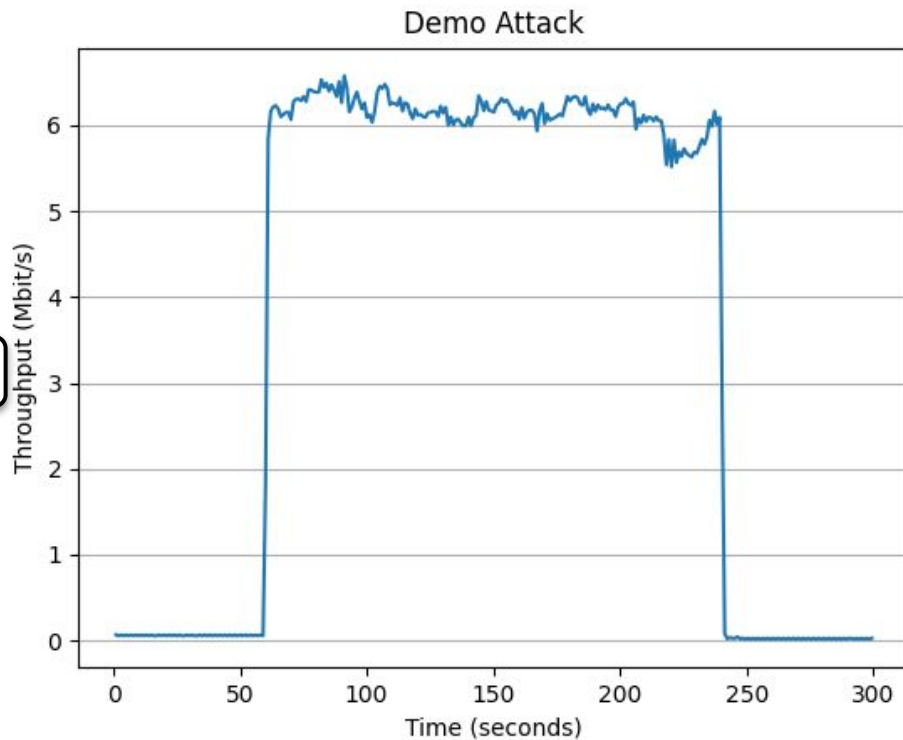
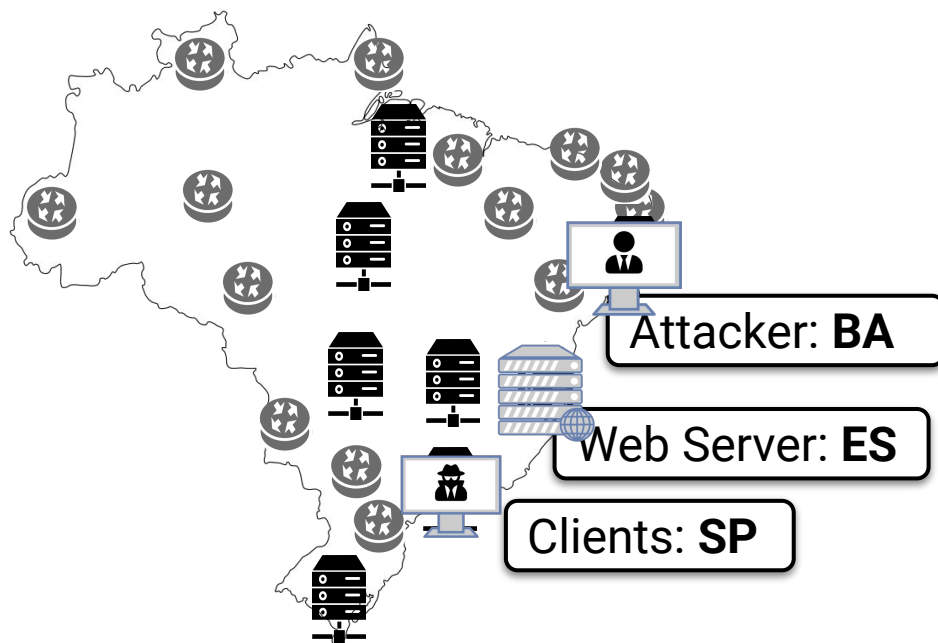
Results

Application example



Results

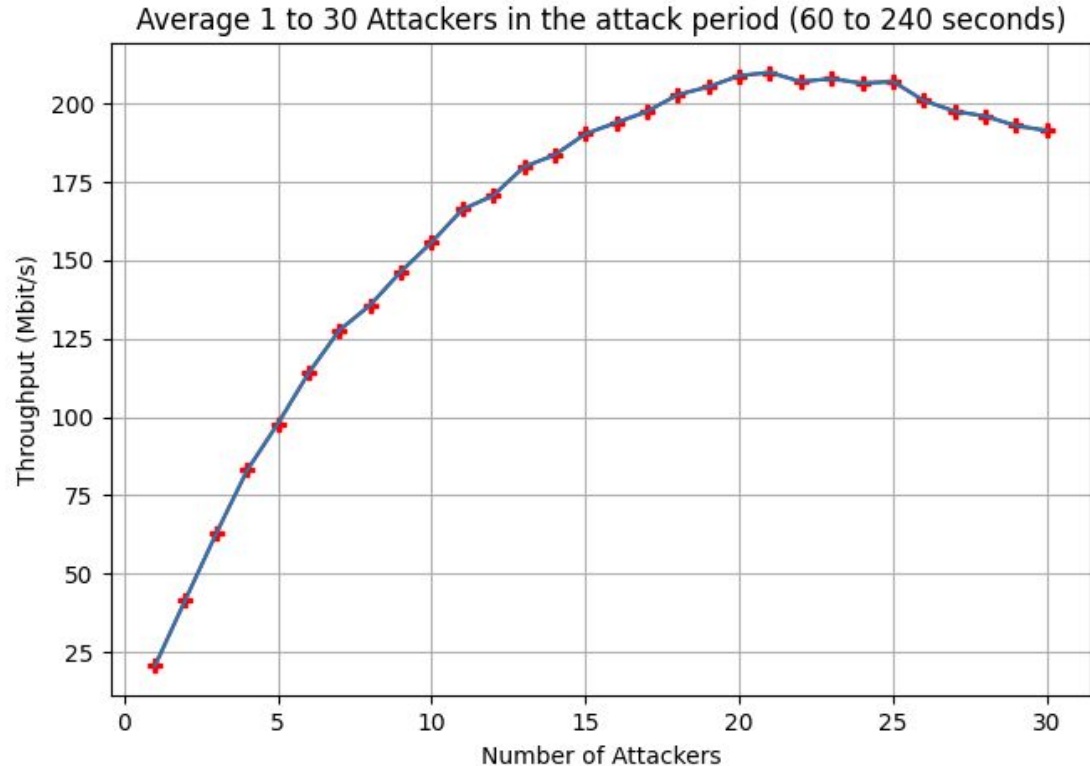
Distributed scenario



Results

Local scenario

- Scalability
- Local scenario:
optimal number of
attackers per region



Final Considerations



- MENTORED: The Brazilian testbed for IoT cybersecurity
 - DDoS and zero-day attacks
- Topology modeling through .yaml files
- REST API in the execution of the experiment
- Preliminary results of distributed and local attacks

Future Works



- Experiment more scenarios
 - E.g., a greater number of physical and virtual nodes
- Evaluate other technologies for creating virtual networks
- Analyze other attack scenarios

Link - Video



- <https://youtu.be/o56IBG80CpY>



The Brazilian Cybersecurity Testbed

Bruno H. Meyer, Davi D. Gemmer, Marcos F. Schawarz, Emerson R. de Mello, Michelle S. Wangham

mentored.project@gmail.com

GLOBECOM 2022

