Analisando ataques Slowloris com o MENTORED *Testbed*

Apresentadores:

- **Michelle S. Wangham | UNIVALI/RNP**
- **Davi D. Gemmer | RNP**

AGENDA

- MENTORED *Testbed*
  - Arquitetura da implementação
  - Fluxo de execução de um experimento

- Demonstração
  - Características do ataque
  - Distribuição geográfica do ataque
  - Comportamento do ataque
  - Configuração do ataque
  - Execução do ataque
  - Resultados dos ataques

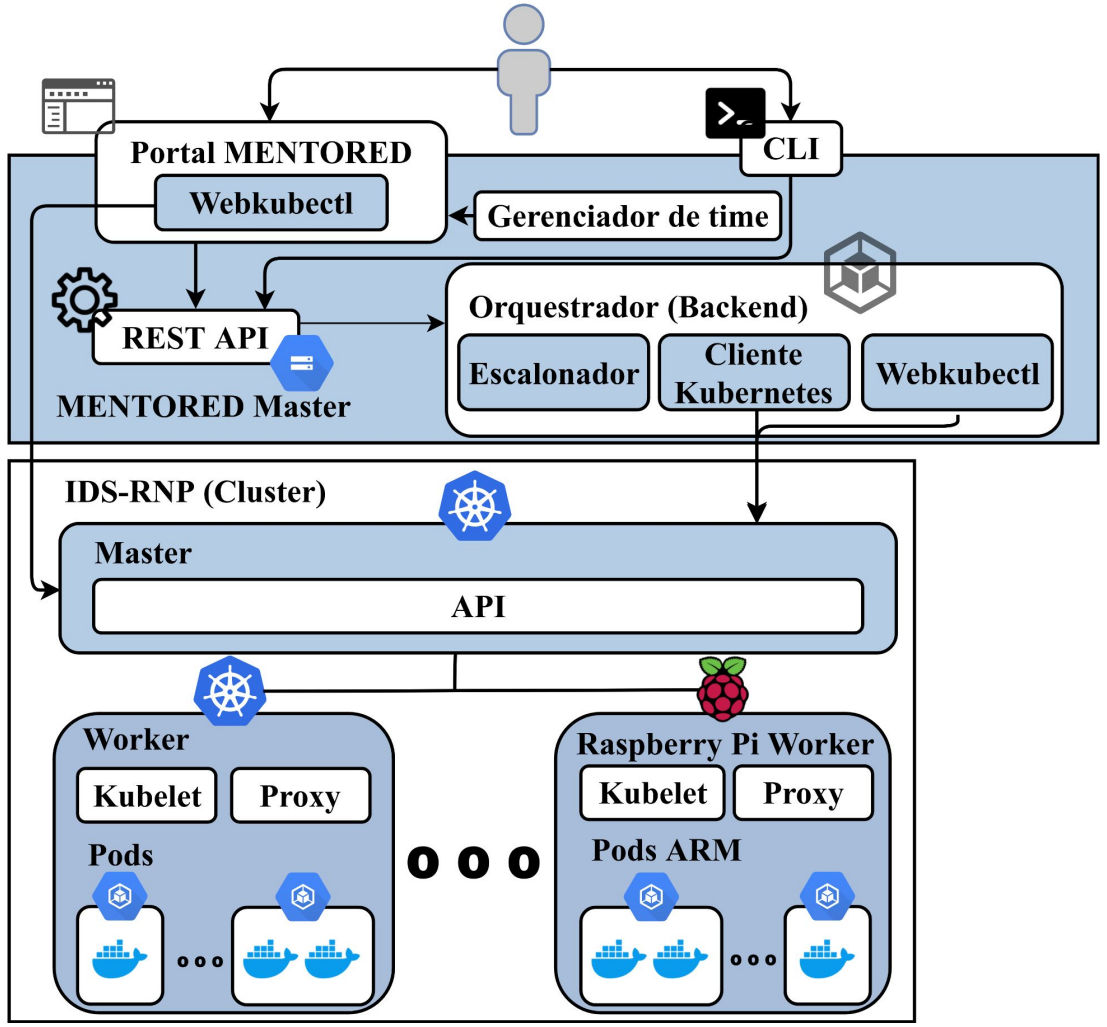
Projeto MENTORED

- Identificar, modelar e avaliar comportamentos maliciosos relacionados à IoT;
- Auxiliar na construção de soluções avançadas e coordenadas para possibilitar à **prevenção**, **predição**, **detecção** e **mitigação** de **ataques DDoS**;
- Fornecer a comunidade científica em Cibersegurança um ***testbed*** para permitir que pesquisadores experimentem suas soluções em relação a ataques DDoS.

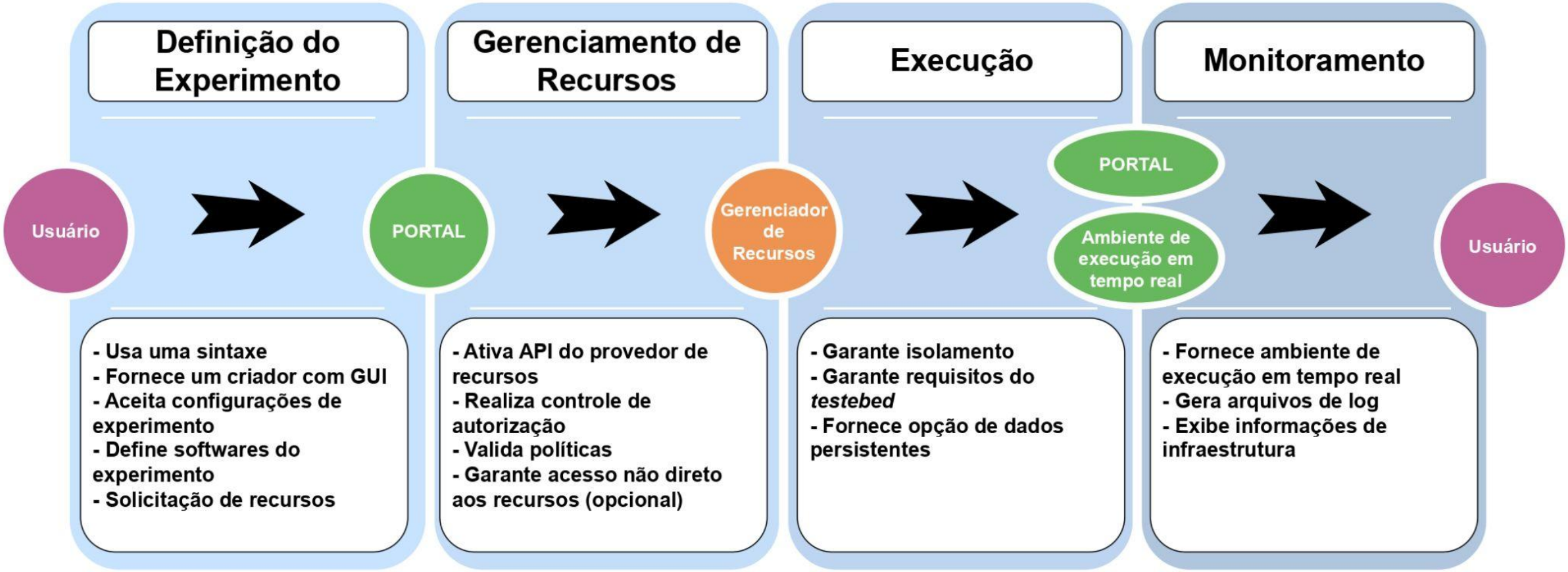
FAPESP/MCTIC 2018/23098-0

MENTORED *Testbed*
Arquitetura da implementação

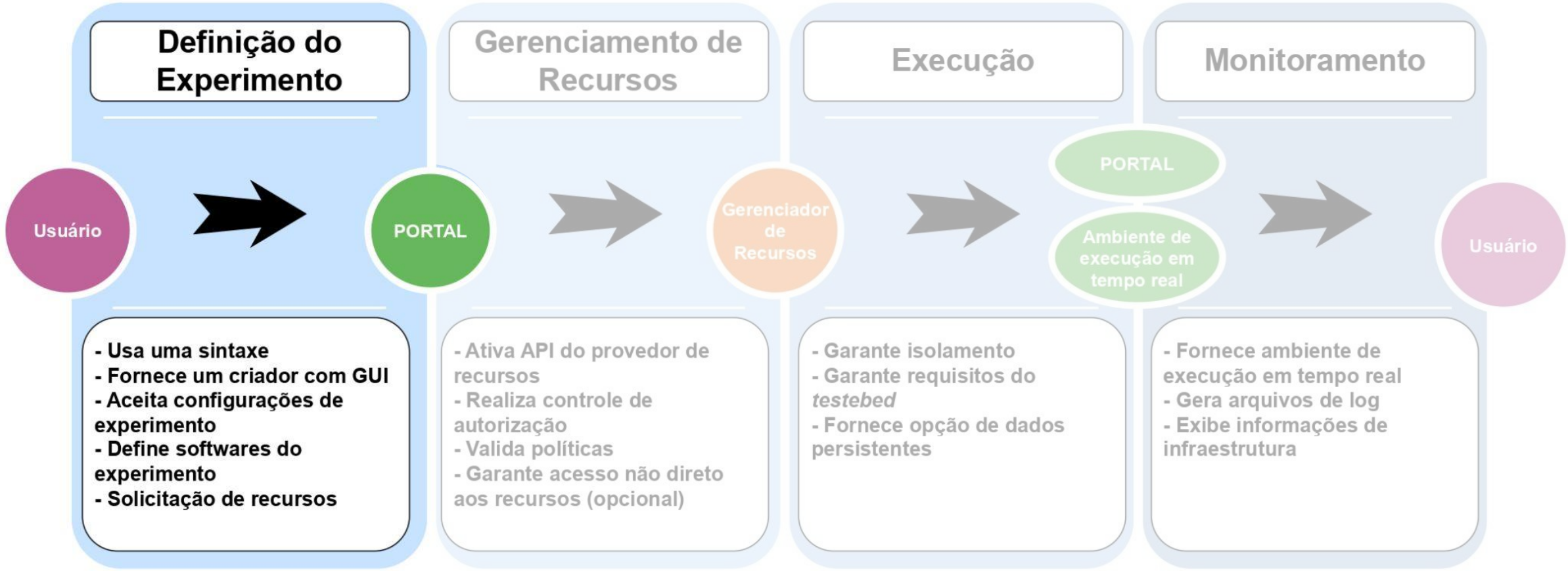
- Principais tecnologias:
  - Kubernetes (cluster)
  - WebKubectl (**Terminal no *browser***)
  - React (**Portal**)
  - Django REST (**API**)
  - COmanage (Gerenciador de time)
- Desafios
  - Cluster é dinâmico
  - Múltiplos experimentadores
  - **Recursos finitos**



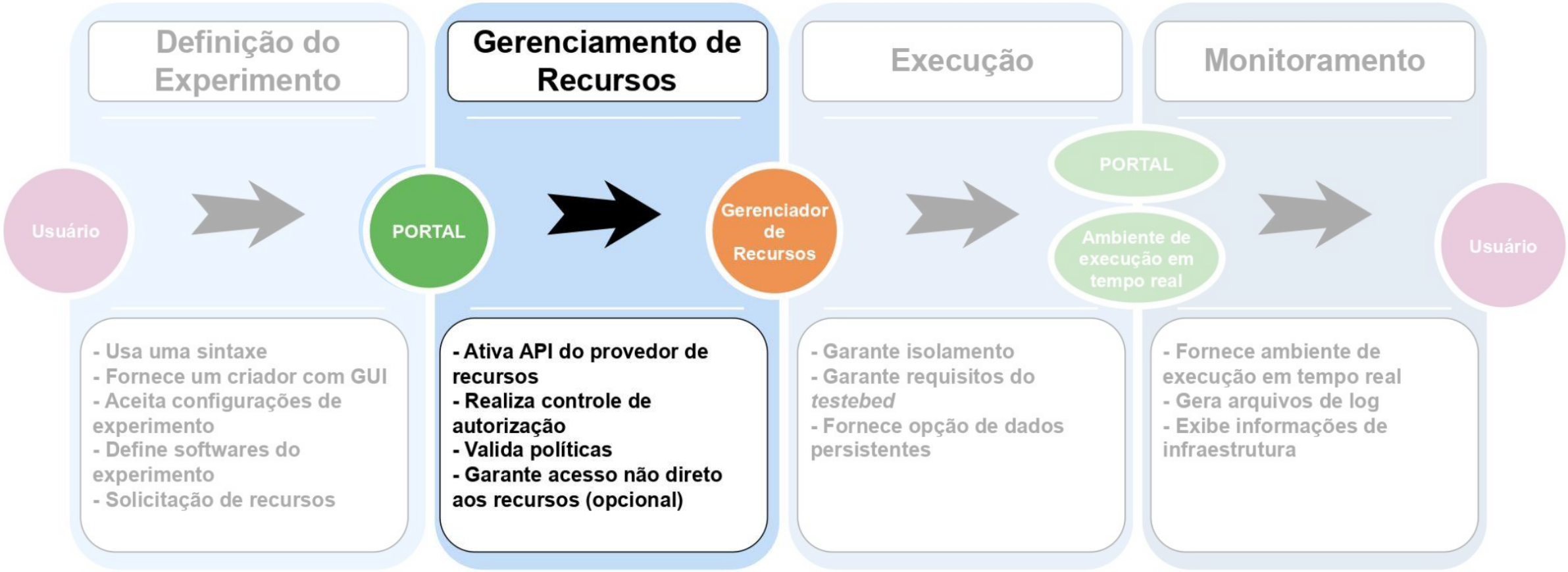
MENTORED *Testbed*
Fluxo de execução de experimento



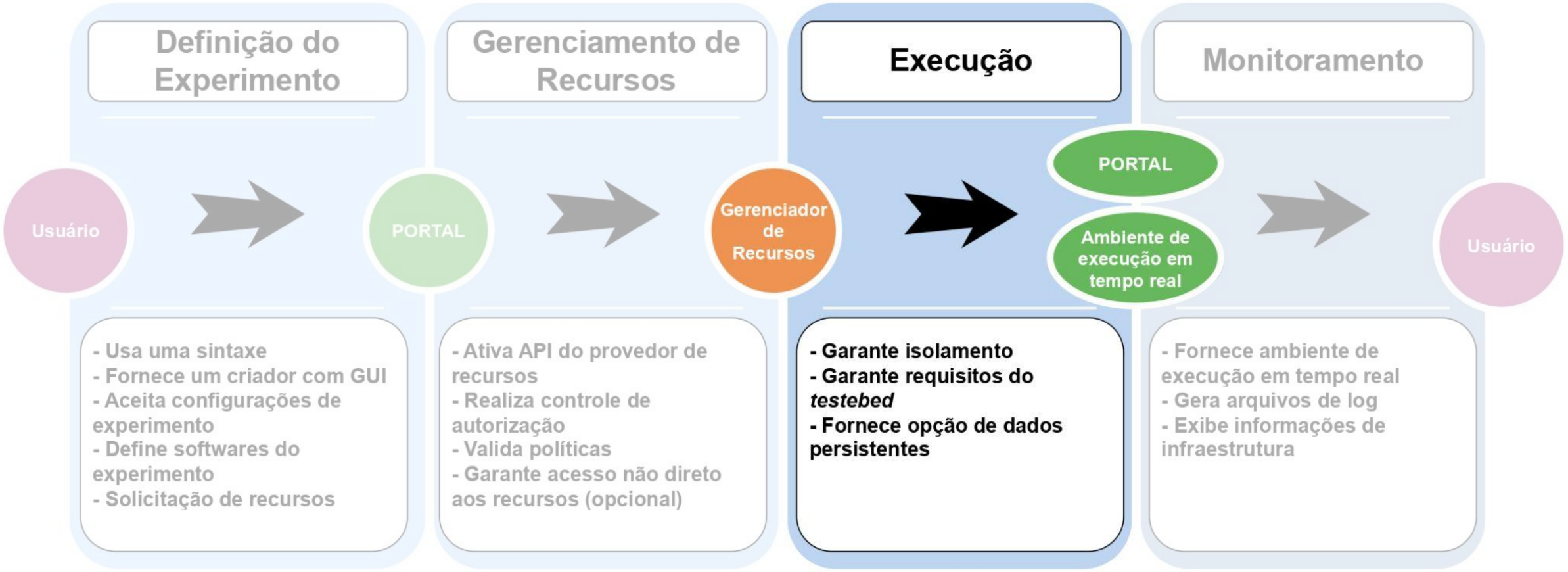
MENTORED *Testbed*
Definição do experimento



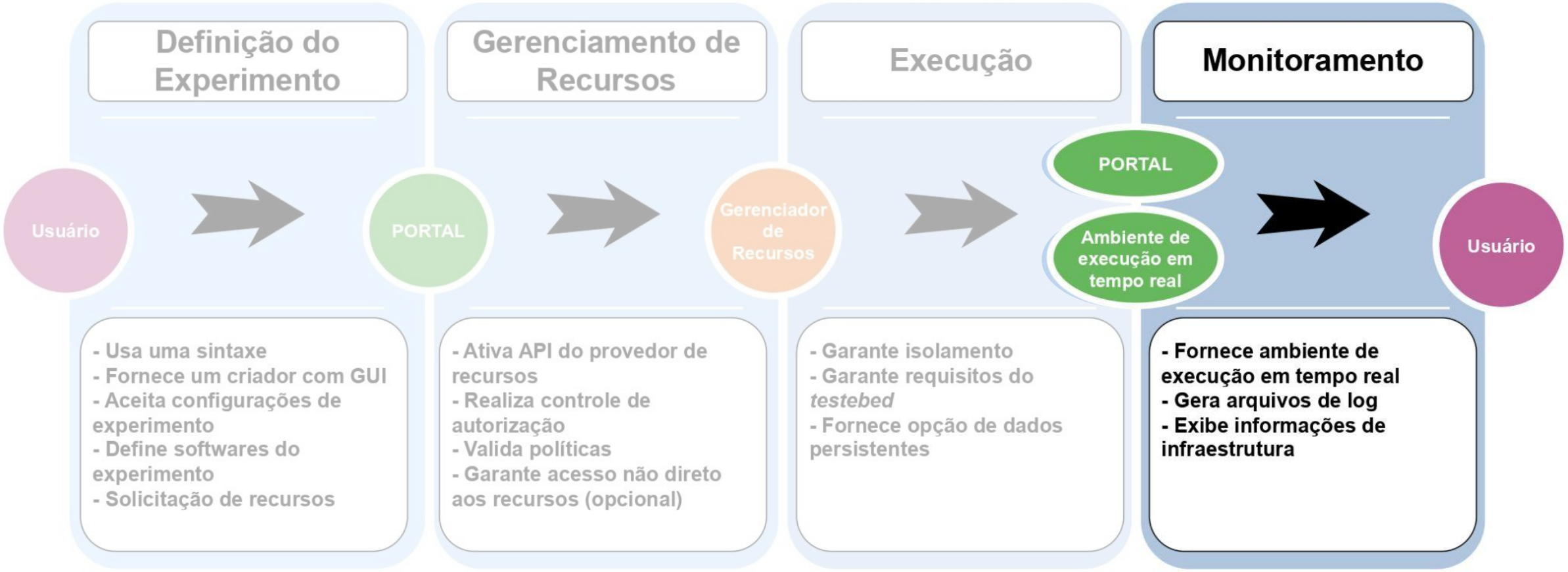
MENTORED *Testbed*
Gerenciamento de recursos



MENTORED *Testbed*
Execução



MENTORED *Testbed*
Monitoramento



Demonstração

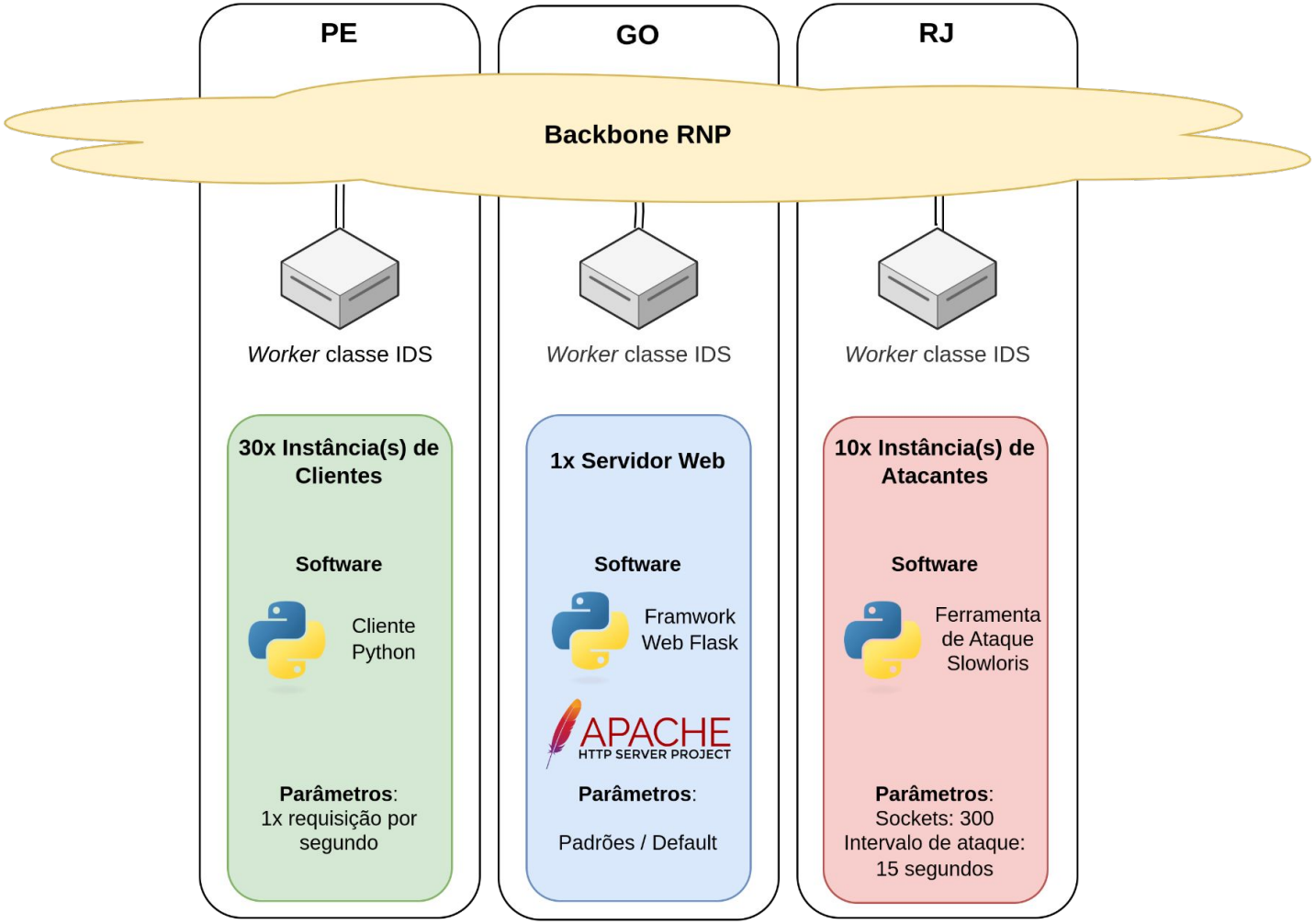
Demonstração
Ataque Slowloris

- *Um ataque "low and slow" é um tipo de ataque DoS ou DDoS que depende de um pequeno streaming de tráfego muito lento visando recursos de aplicativos ou servidores;*
- *Layer 7* - Aplicações como servidores *Web;*
- Baixo consumo de rede.

Demonstração
Configuração do servidor *Web*

- Ataque nº 1
  - Ataque Slowloris com servidor Apache2 *default*
    - Versão ***default*** do Apache2
- Ataque nº 2
  - Ataque Slowloris com servidor Apache2 modificado
    - Ativação do módulo ***mod_reqtimeout*** no código do Apache2.

Demonstração
Configuração do ataque com Slowloris



Experimentos
Comportamento do ataque

Vítima - Ataque nº 1
Parte do código responsável pelo servidor

```
Experiment:
  name: mentored_experiment
  nodeactors:
    - name: 'na-server'
      persitent_volume_path: "/app/packets.pcap"
      replicas: 1
      containers:
        - name: tshark
          image: ghcr.io/mentoredtestbed/mentored-tshark
          command: ["/entry.sh"]
          args: ["tshark", "-i", "net1", "-x", "-w", "packets.pcap"]
          env:
            - name: TIMEOUT_CMD
              value: "300"
        - name: 'server'
          image: ghcr.io/mentoredtestbed/generic-apache-flask-webserver:latest
          ports:
            - containerPort: 80
          resources:
            requests:
              memory: 1G"
              cpu: "1"
            limits:
              memory: "2G"
              cpu: "2"
      region: 'ids-go'
```

Clientes
Parte do código responsável pelos clientes

```
- name: 'generic-client-pe'
  persitent_volume_path: "/client_delay.csv"
  replicas: 30
  containers:
    - name: 'client-rn'
      image: ghcr.io/mentoredtestbed/generic-client:latest
      imagePullPolicy: "Always"
      command: ["/entry.sh"]
      args: ['python3', 'client_web_metrics.py', "1", "1"]
      env:
        - name: TIMEOUT_CMD
          value: "300"
        - name: ADD_SERVER_IP_TO_COMMAND
          value: "true"
      resources:
        requests:
          memory: "64Mi"
          cpu: "100m"
        limits:
          memory: "128M"
          cpu: "200m"
  region: 'ids-pe'
```

Atacante
Parte do código responsável pelos atacantes

```yaml
- name: 'generic-botnet-rj'
  persitent_volume_path: "/MENTORED_IP_LIST.yaml"
  replicas: 10
  containers:
    - name: 'botnet-rn'
      image: ghcr.io/mentoredtestbed/generic-botnet:latest
      command: ["/entry.sh"]
      args: ["slowloris", "-p", "80", "--randuseragents", "-s", "300"]
      # args: ["hping3", "-S", "--flood", "-S", "-d 1024", "-p", "80"]
      env:
        - name: PROTOCOL
          value: "ICMP"
        - name: TIMEOUT_CMD
          value: "180"
        - name: TIME_WAIT_START
          value: "60"
        - name: ADD_SERVER_IP_TO_COMMAND
          value: "true"
      securityContext:
        privileged: true
      resources:
        requests:
          memory: "64Mi"
          cpu: "100m"
        limits:
          memory: "128M"
          cpu: "200m"
  region: 'ids-rj'
```

Vítima - Ataque nº 2
Parte do código responsável pelo servidor

```
Experiment:
  name: mentored_experiment
  nodeactors:
    - name: 'na-server'
      persitent_volume_path: "/app/packets.pcap"
      replicas: 1
      containers:
        - name: tshark
          image: ghcr.io/mentoredtestbed/mentored-tshark
          command: ["/entry.sh"]
          args: ["tshark", "-i", "net1", "-x", "-w", "packets.pcap"]
          env:
            - name: TIMEOUT_CMD
              value: "300"
        - name: 'server'
          image: ghcr.io/mentoredtestbed/generic-apache-flask-webserver:latest
          env:
           - name: ENABLE_SLOWLORIS_DEFENSE
             value: "true"
          ports:
            - containerPort: 80
          resources:
            requests:
              memory: 1G"
              cpu: "1"
            limits:
              memory: "2G"
              cpu: "2"
      region: 'ids-go'
```

```
# Check if the variable ENABLE_SLOWLORIS_DEFENSE is true
<IfModule mod_reqtimeout.c>
    RequestReadTimeout header=20-40,MinRate=500 body=20-40,MinRate=500
</IfModule>
```

Vítima - Troca de Imagem
Parte do código responsável pelo servidor

```
Experiment:
  name: mentored_experiment
  nodeactors:
    - name: 'na-server'
      persitent_volume_path: "/app/packets.pcap"
      replicas: 1
      containers:
        - name: tshark
          image: ghcr.io/mentoredtestbed/mentored-tshark
          command: ["/entry.sh"]
          args: ["tshark", "-i", "net1", "-x", "-w", "packets.pcap"]
          env:
            - name: TIMEOUT_CMD
              value: "300"
        - name: 'server'
          image: ghcr.io/mentoredtestbed/generic-apache-flask-webserver-modqos:latest
          ports:
            - containerPort: 80
          resources:
            requests:
              memory: 1G"
              cpu: "1"
            limits:
              memory: "2G"
              cpu: "2"
      region: 'ids-go'
```

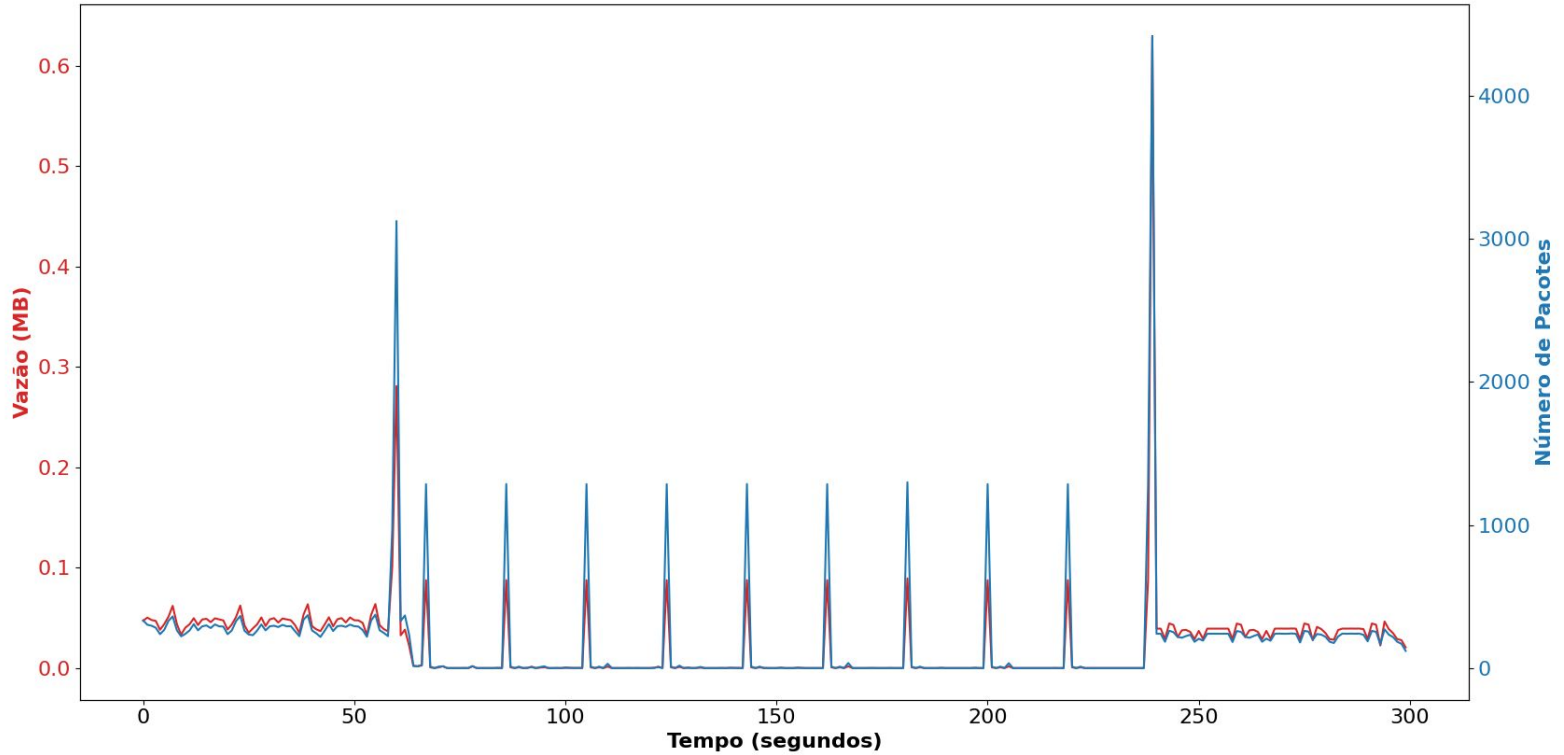
Atividade Prática
Login no portal do MENTORED *Testbed*

*https://portal.mentored.ccsc-research.org

Resultado
Arquivos resultantes do ataque

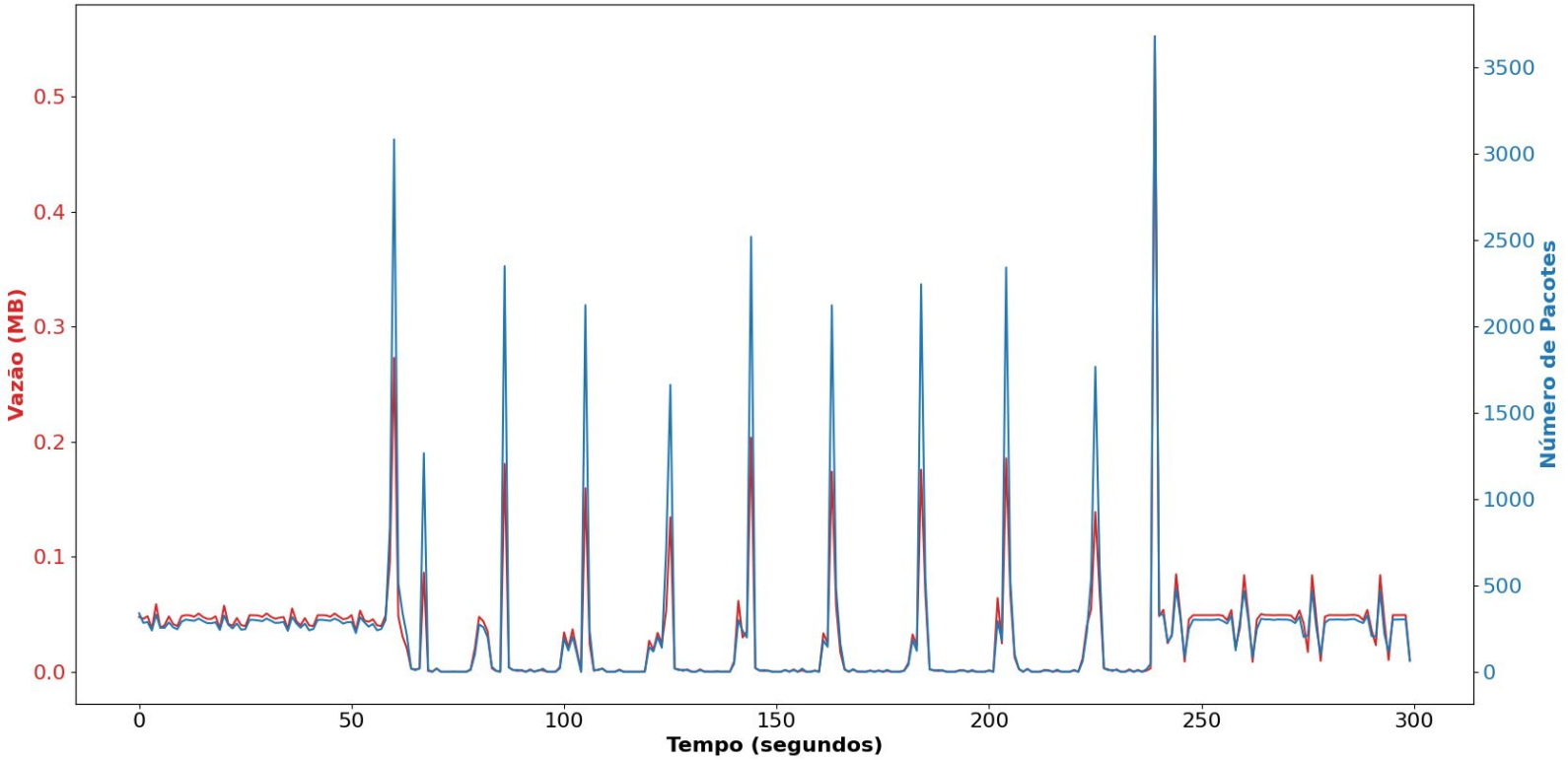
- Arquivo com a captura de tráfego da vítima;
  - *packets.pcap*
- Arquivos com o tempo de respostas das requisições GET dos clientes;
  - *client_delay.csv*
- Arquivo contendo a lista de todos os IPs classificados por tipo e região;
  - *MENTORED_IP_LIST.yaml*
- Arquivo contendo os *logs* do experimento;
  - *experiment_logs.tar*
- Ferramentas utilizadas na criação dos gráficos;
  - *https://github.com/mentoredtestbed/demo-wtestbed-csbc-2024*

Ataque nº 1
Resultado do ataque com Slowloris *default*



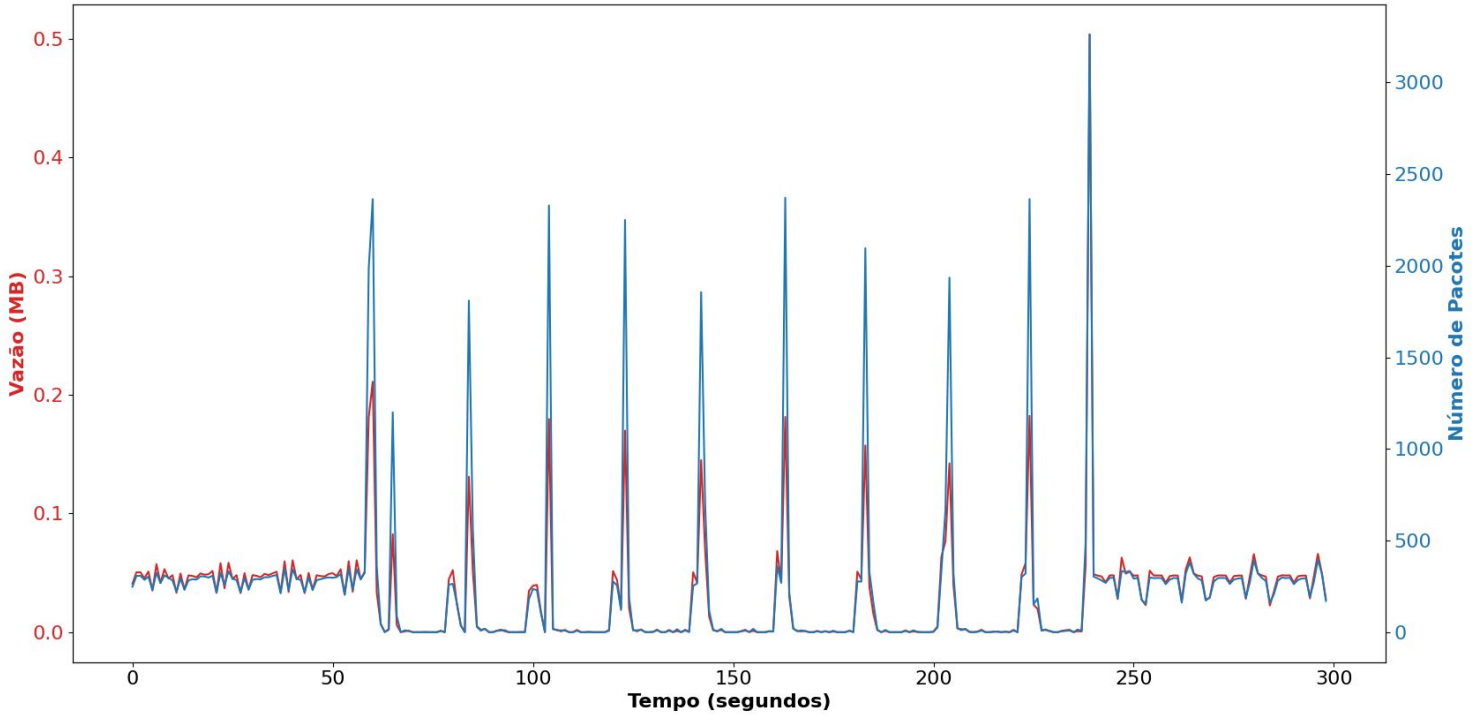

```
Running experiment analyzer...
100%|                                                  | 30/30 [00:00<00:00, 3520.29it/s]
Average time for client response (Before 60 seconds)    : 0.066
Average time for client response (60 - 240 seconds)      : 110.599
Average time for client response (After 240 seconds)     : 0.066
Experiment analyzer finished
```

Ataque nº 2
Resultado do ataque com Slowloris modificado




```
Running experiment analyzer...
100%|                                                                                |
Average time for client response (Before 60 seconds)    : 0.066
Average time for client response (60 - 240 seconds)      : 43.005
Average time for client response (After 240 seconds)     : 0.067
Experiment analyzer finished
```

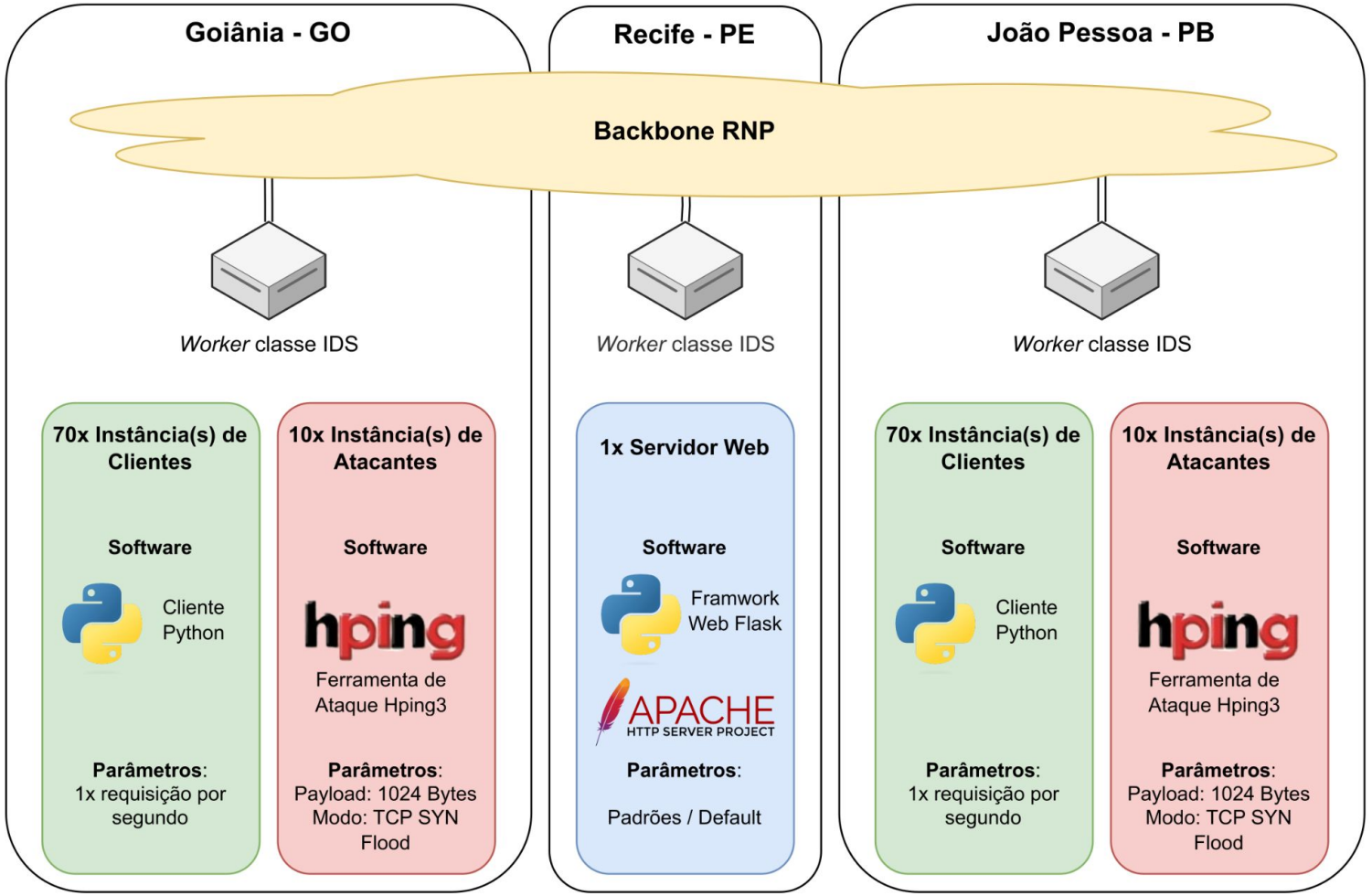
Exemplo
Resultado do ataque com Slowloris mod_qos




```
Running experiment analyzer...
100%|                                                                                |
Average time for client response (Before 60 seconds)     : 0.066
Average time for client response (60 - 240 seconds)       : 41.559
Average time for client response (After 240 seconds)      : 0.067
Experiment analyzer finished
```

Capítulo do Livro
Configuração do ataque com Hping3

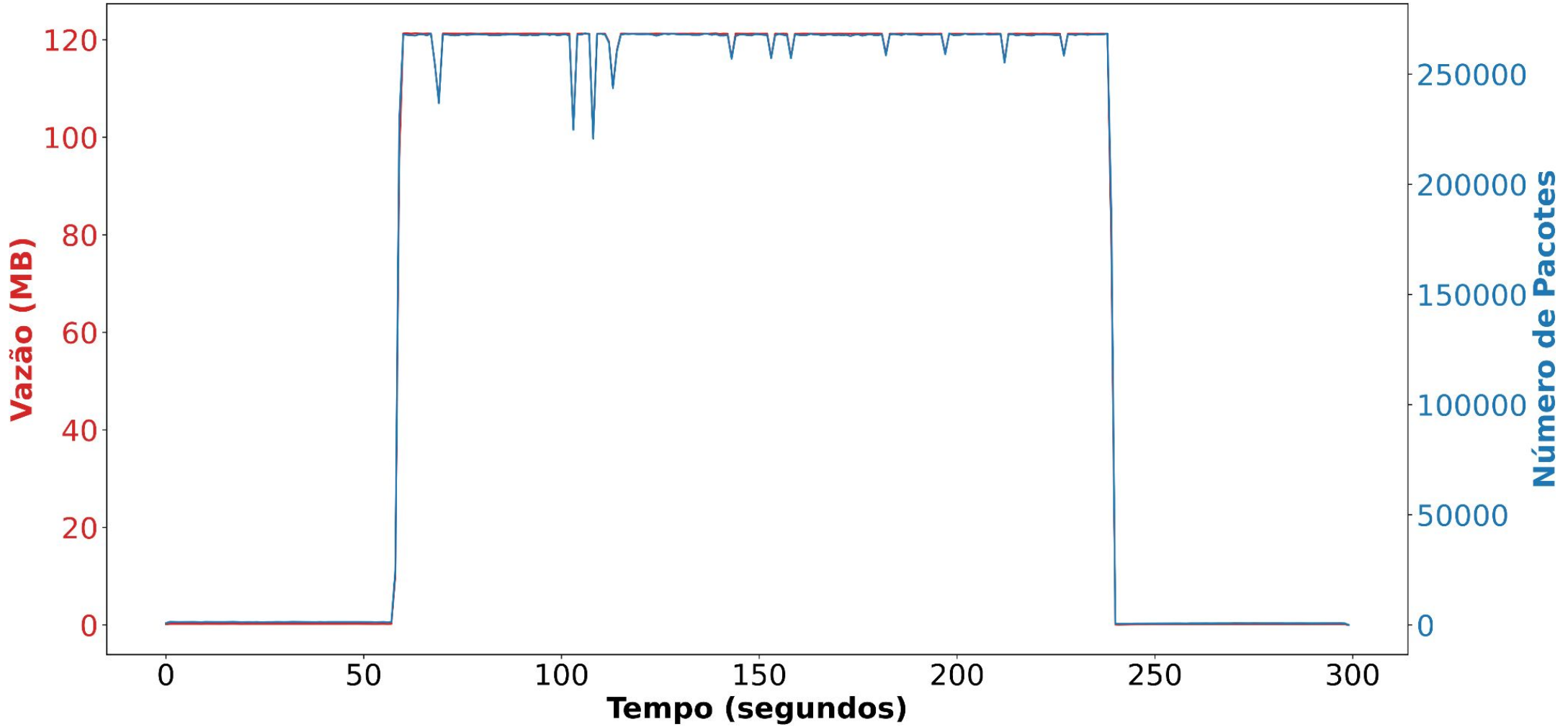
Capítulo
Minicurso SBRC 2024



Repositório GitHub
Minicurso SBRC 2024

Hping3

Gráfico com o ataque utilizando o Hping3



Considerações Finais

Q&A

Site do Projeto
MENTORED

Repositório GitHub
Demo *WTestbed* CSBC 2024

Analisando ataques Slowloris com o MENTORED *Testbed*

Apresentadores:

- **Michelle S. Wangham | UNIVALI/RNP**
- **Davi D. Gemmer | RNP**