WP4

MENTORED

www.mentoredproject.com

Um Ambiente de Experimentação em Cibersegurança para a Internet das Coisas

Apresentador:
- Nelson G. Prates Junior

Julho, 2021

FAPESP

MCTIC

cgi.br
Comitê Gestor da Internet no Brasil

Agenda

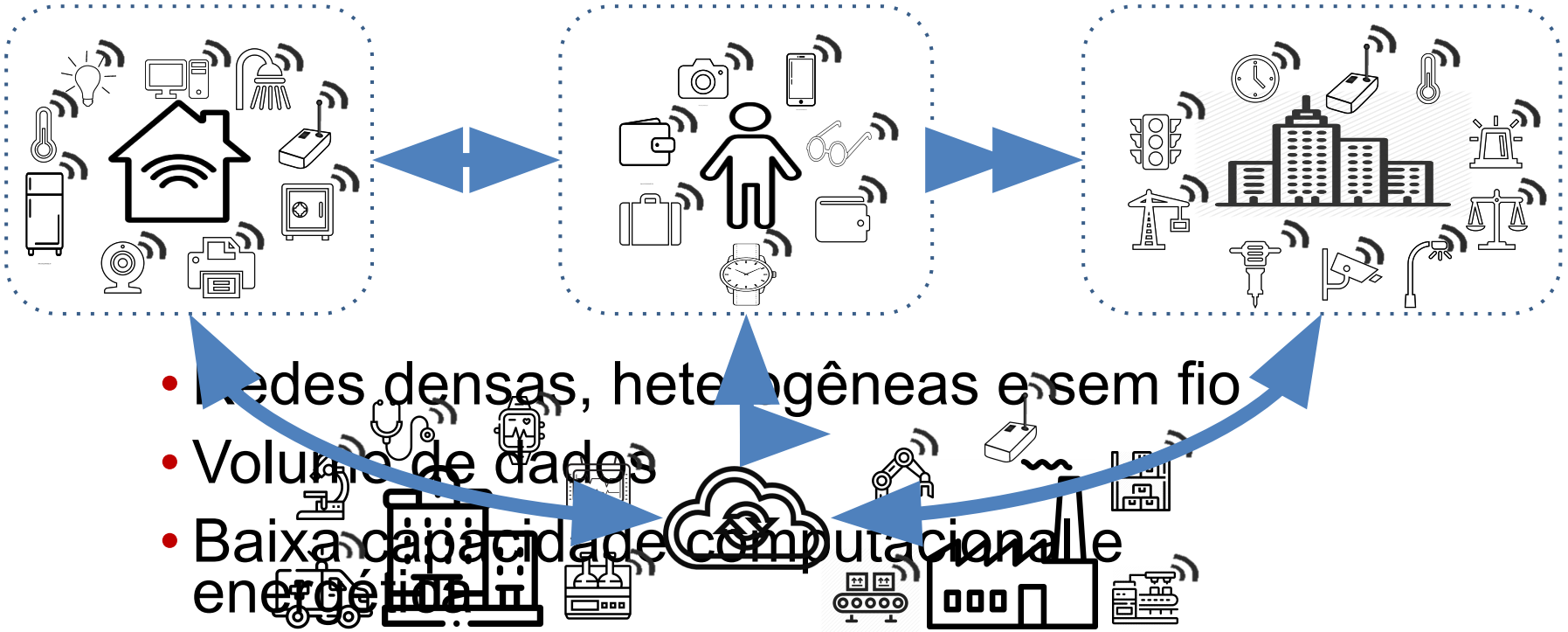
WP4

MENTORED

- Introdução
- Projeto Mentored
- Infraestrutura Definida por Software (IDS-RNP)
- Mentored Testbed
- Estudo de Caso
- Conclusão
- Trabalhos Futuros

Introdução

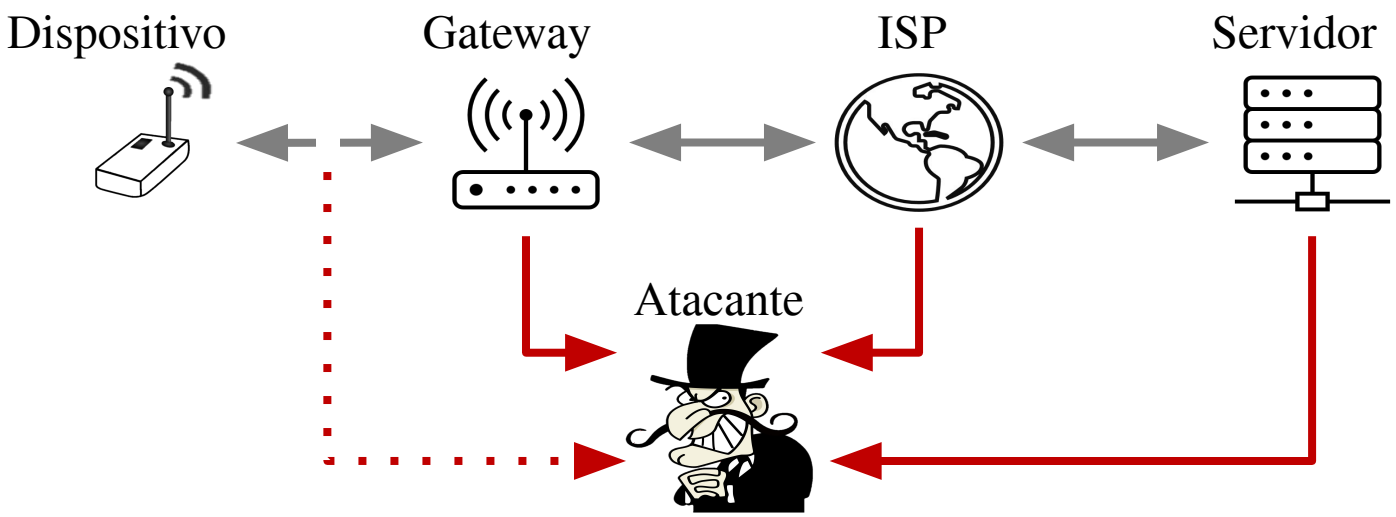
Internet das Coisas



- Redes densas, heterogêneas e sem fio
- Volume de dados
- Baixa capacidade computacional e energética

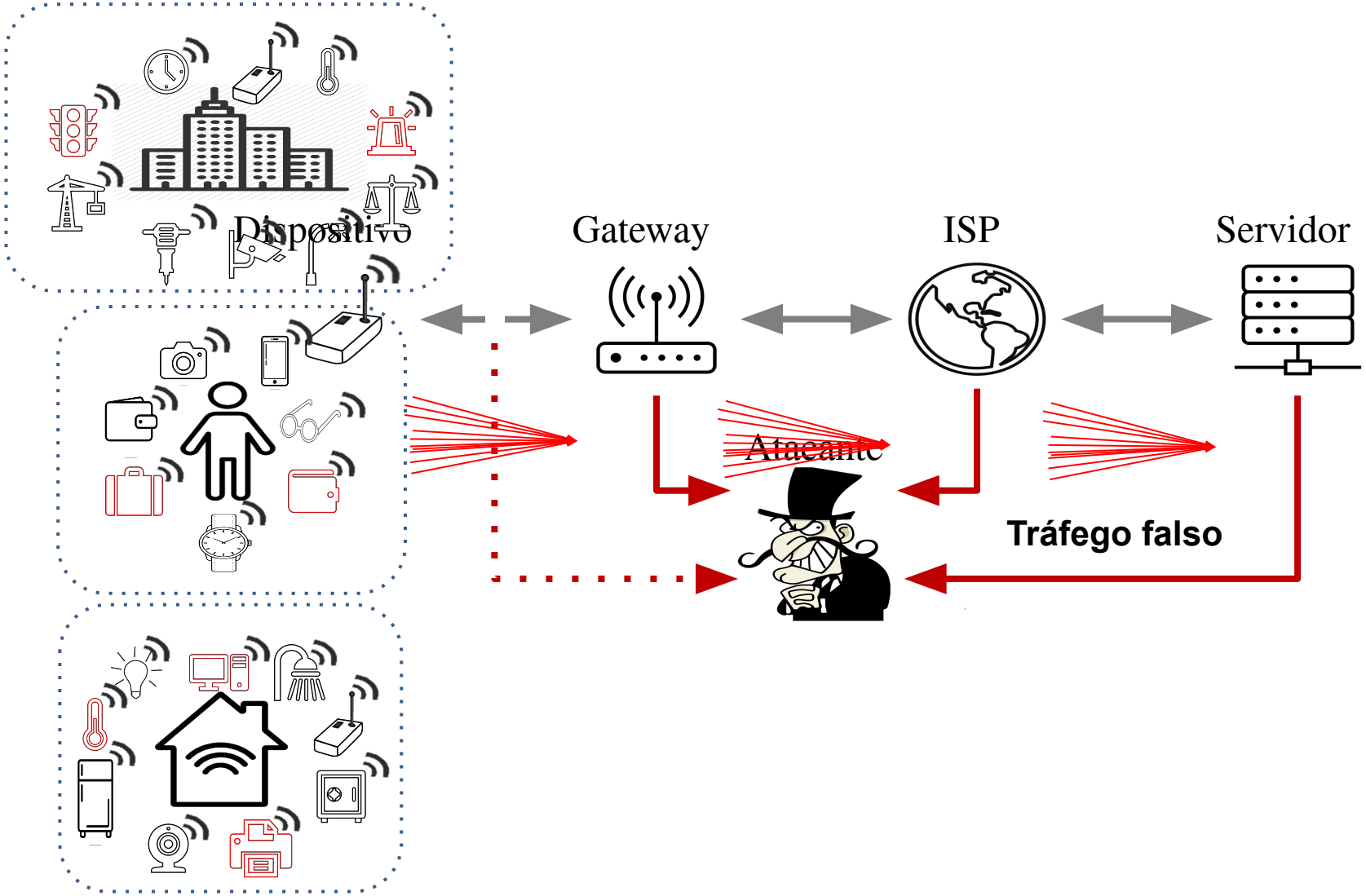
Introdução

Vulnerabilidades na Internet das Coisas



Introdução

Vulnerabilidades na Internet das Coisas



Introdução
Prejuízos

WP4

MENTORED

+90%

Aumento dos ataques no Brasil

R$ 1500/h

Brasil tem 2º maior custo de *downtime* do mundo

Sistema Social Itália

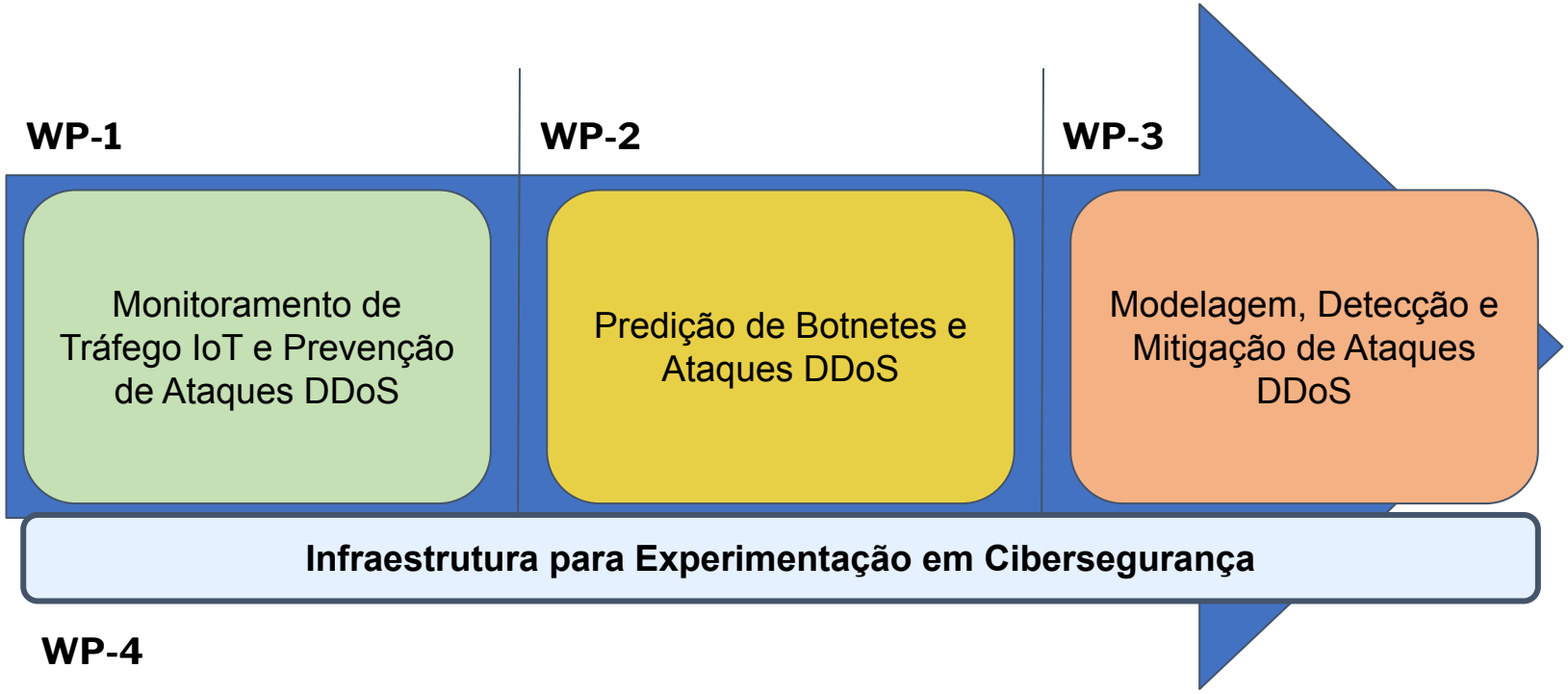
Agência Saúde EUA

Projeto MENTORED

Visão Geral

WP4

MENTORED



MCTI

FAPESP

RNP REDE NACIONAL DE ENSINO E PESQUISA

cgi.br Comitê Gestor da Internet no Brasil

Pacote de Trabalho 4 (WP4)

Objetivo Geral

WP4

MENTORED

Prover um ambiente controlado para experimentação (*testbed*) com cenários da IoT para avaliar propostas de cibersegurança

Quem?

- 1º Pesquisadores dos WPs
- 2º Comunidade de Segurança

Pacote de Trabalho 4 (WP4)

Objetivos Específicos

WP4

MENTORED

- Oferecer recursos para experimentação em cenários realistas:

Avaliar soluções contra ataques DDoS e de botnets baseados na IoT

Desenvolver metodologias avançadas para prover pesquisa experimental em cibersegurança sob demanda

Apoiar - EaD, Capacitações e disseminação (ataques e soluções de segurança)

Pacote de Trabalho 4 (WP4)

Testbeds de Referência

WP4

MENTORED

FIT IOT-LAB

The DETER Project

- Metodologia de experimentação em cibersegurança
  - Experimentação replicável, escalável e cientificamente verificável
  - Diminuir a complexidade ao criar experimentos de cibersegurança
- Recursos:
  - Acesso aos recursos físico como servidores e dispositivos IoT

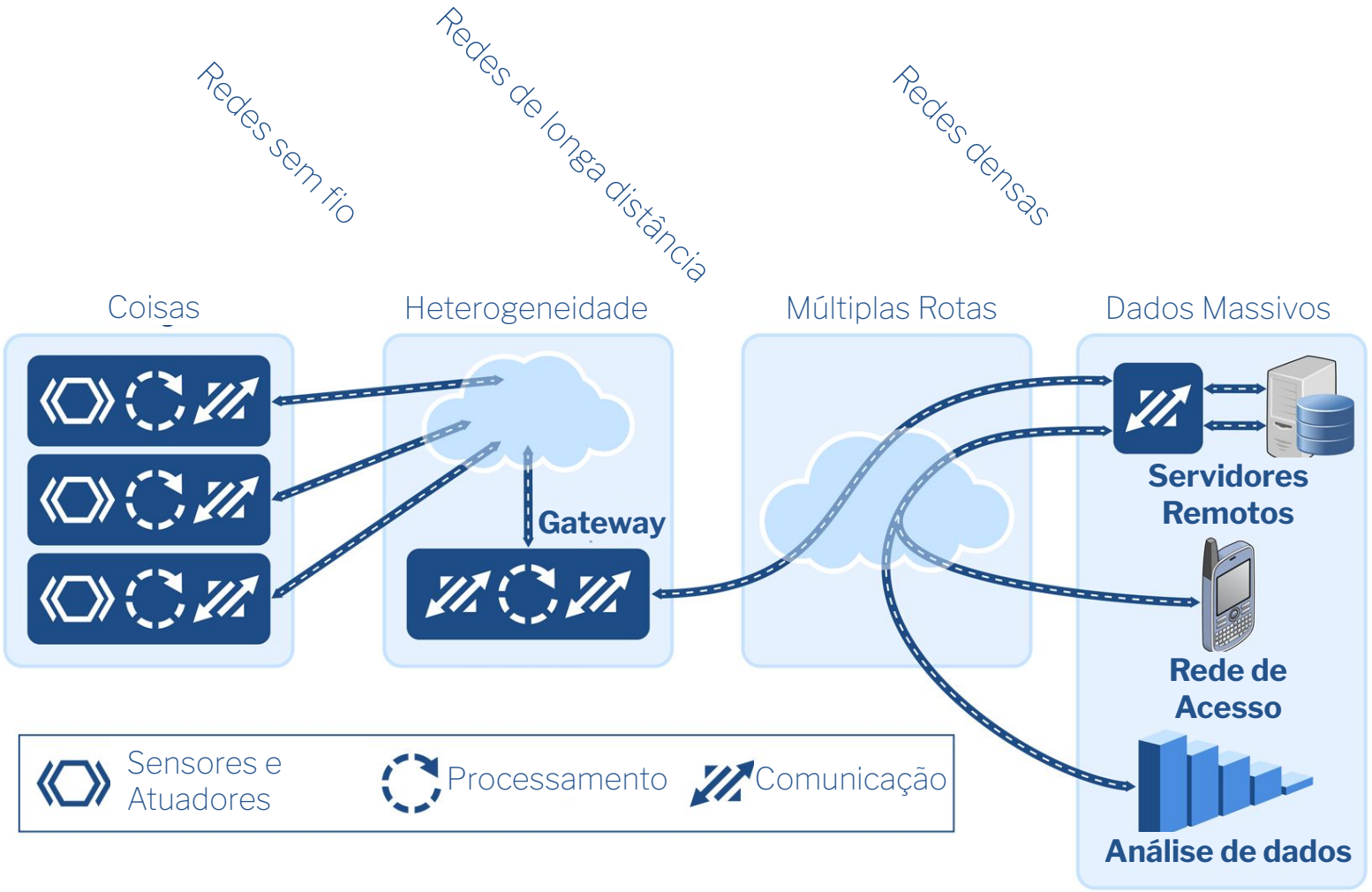
Pacote de Trabalho 4 (WP4)

Requisitos de um Testbed IoT

WP4

MENTORED

- Fidelidade
- Validade
- Escalabilidade
- Segurança
- Reprodutibilidade
- Flexibilidade
- Transparência
- Acesso em tempo real
- Perspectiva centrada no usuário (Pesquisador)

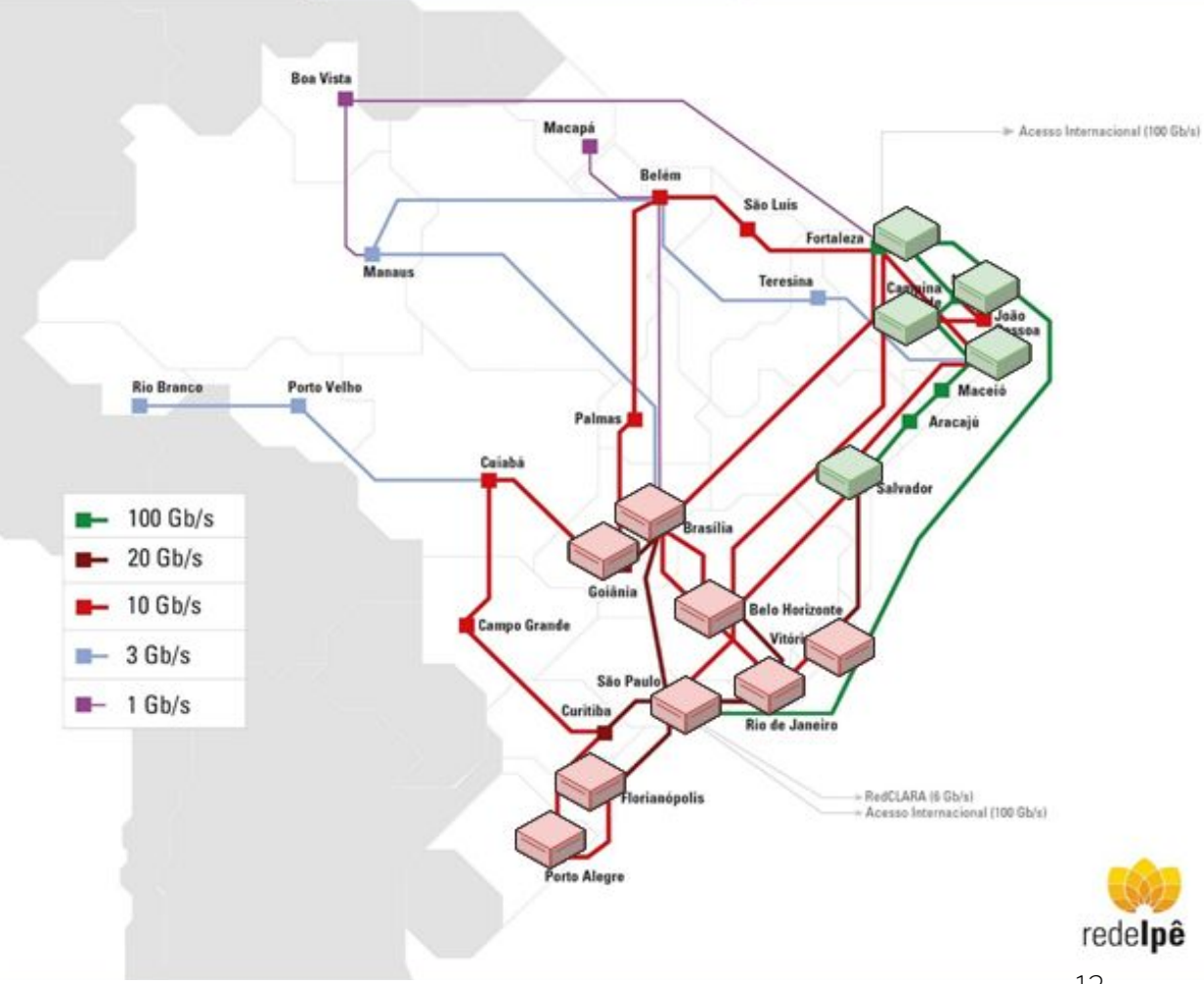


Infraestrutura Definida por Software (IDS-RNP)
Visão Geral

WP4

MENTORED

- **Recursos**
  - Servidores *bare metal*
  - Links de alta velocidade - 1 a 100Gbps
- **Modelo de Uso**
  - Sob demanda (requer setup inicial)
- **Propósito**
  - Infraestrutura virtualizável e programável
  - Orquestração de recursos em paradigma Cloud-Native



RNP REDE NACIONAL DE ENSINO E PESQUISA

MCTI

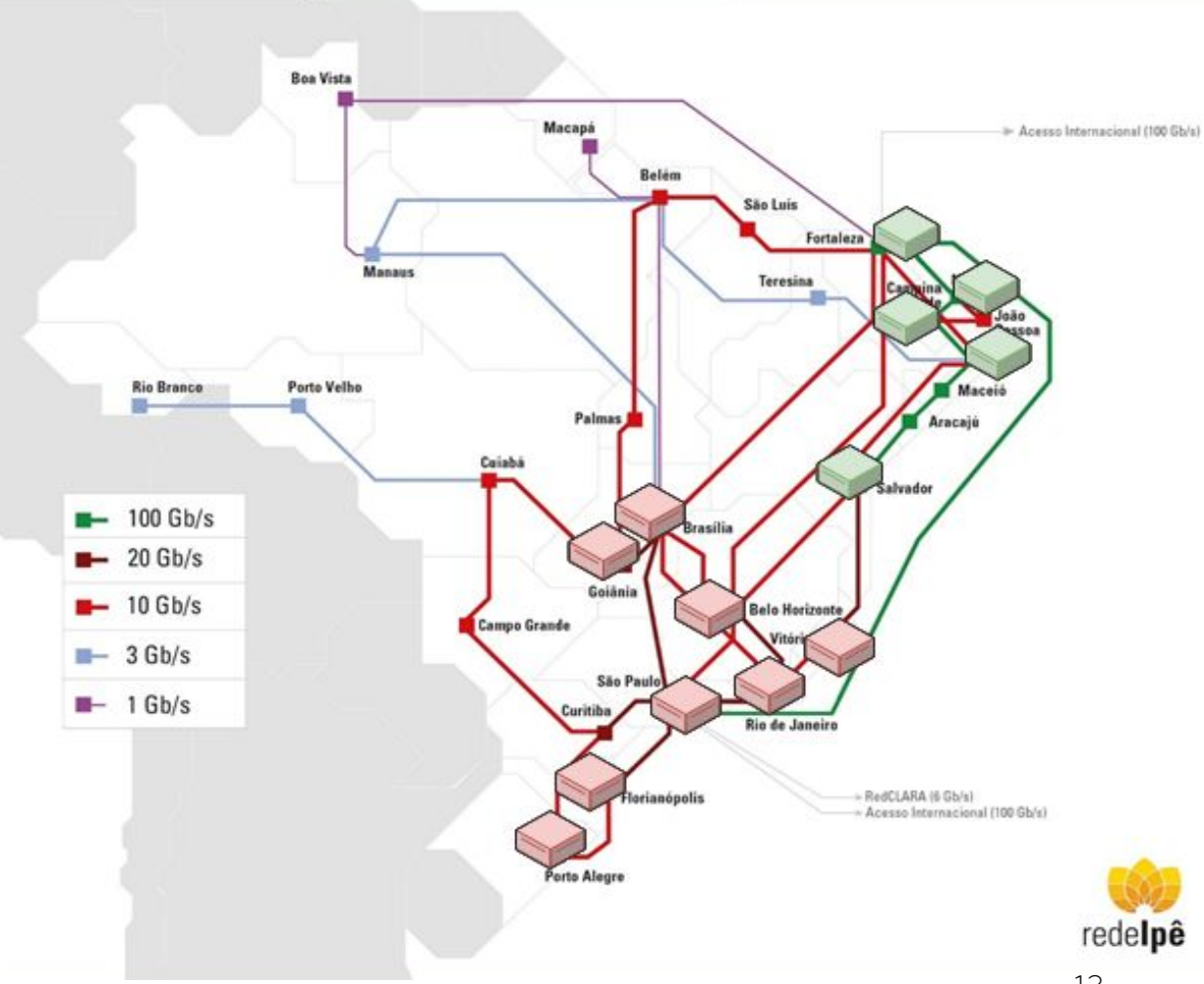
redeIpê

Infraestrutura Definida por Software (IDS-RNP)
Vantagens

WP4

MENTORED

- Processamento e de armazenamento
- Rede customizável e de longa distância
- Software Livre
- Configurações sob-demanda
- Suporta a inclusão de redes de borda
- Equipe de apoio da RNP



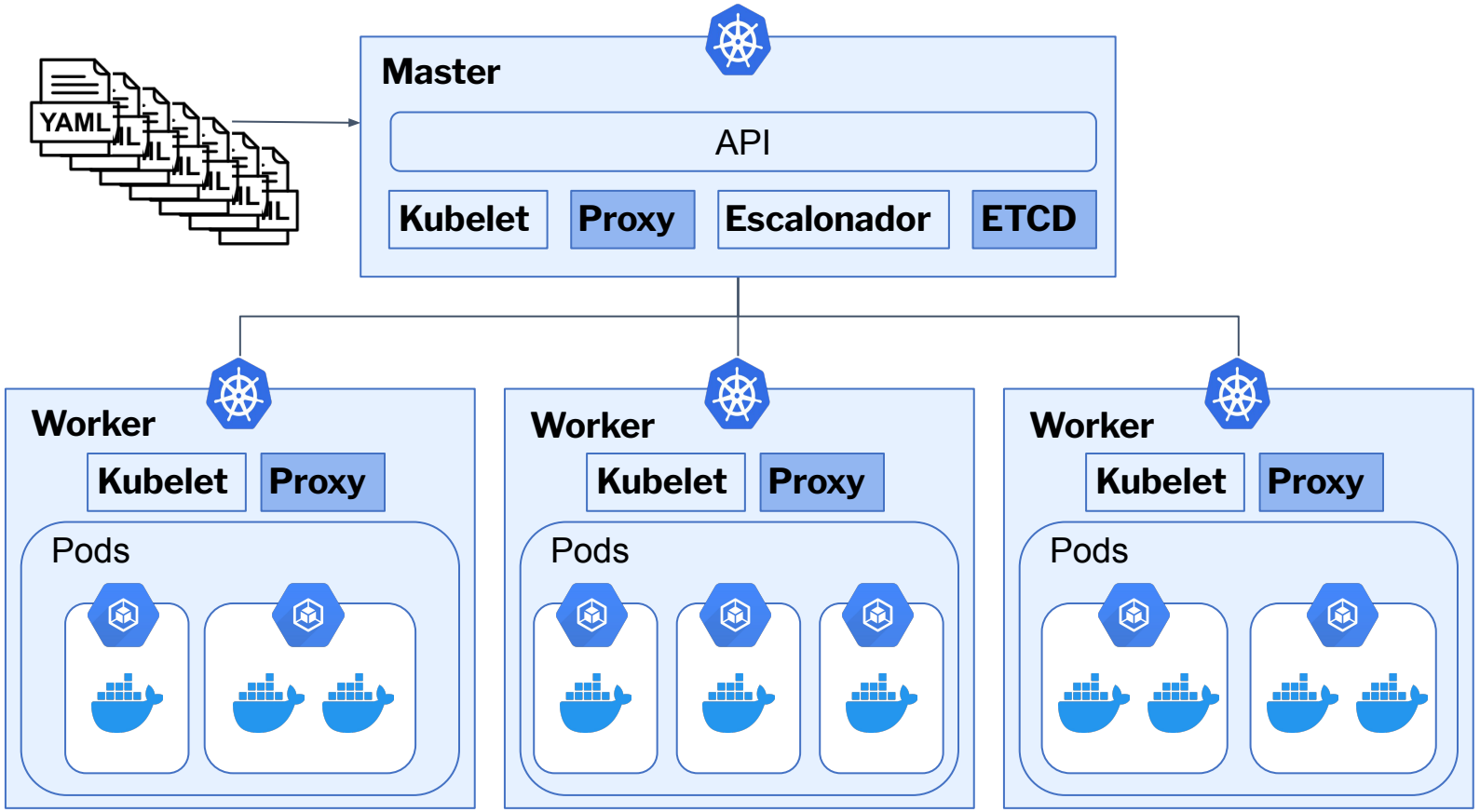
kubernetes docker

redelpê

Infraestrutura Definida por Software (IDS-RNP)
Kubernetes

WP4

MENTORED

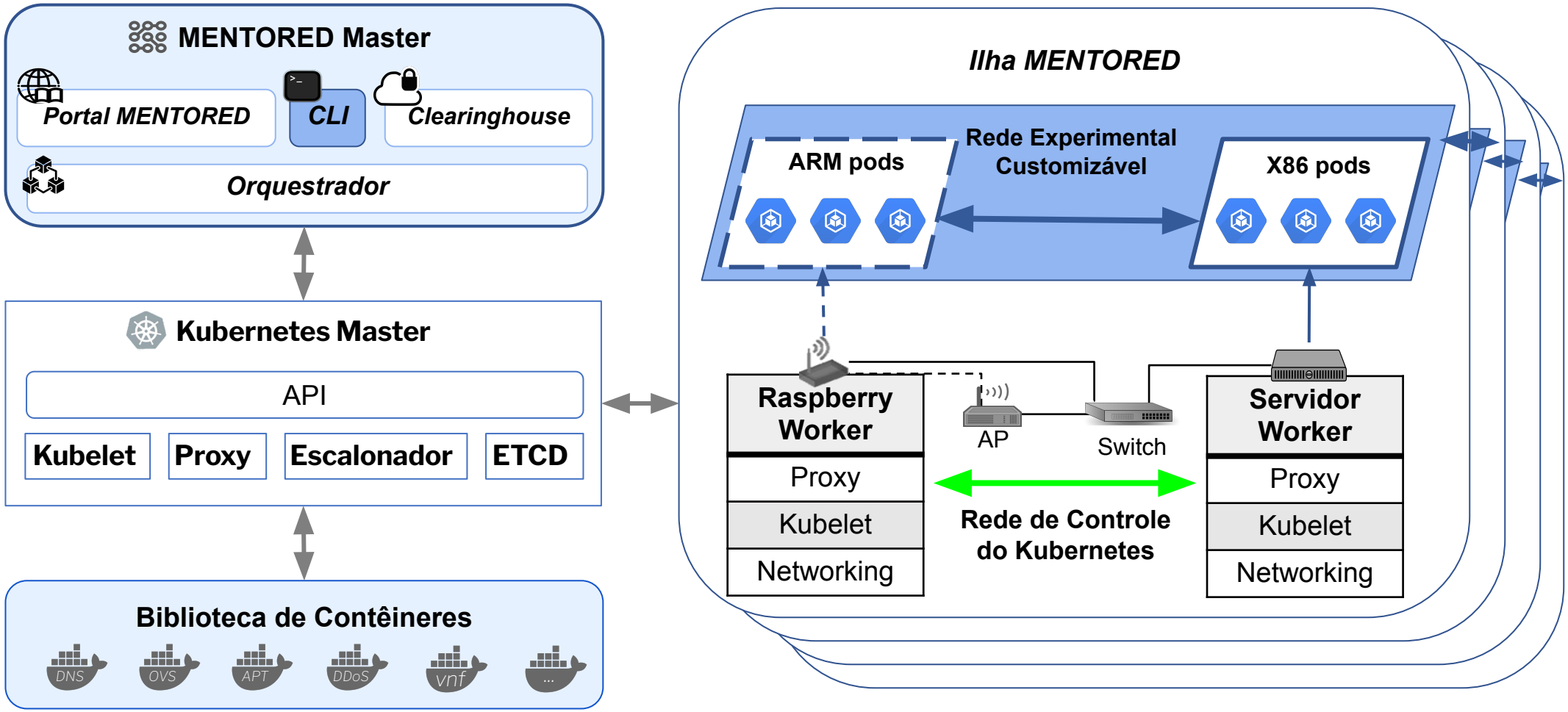


MENTORED Testbed

Arquitetura

WP4

MENTORED

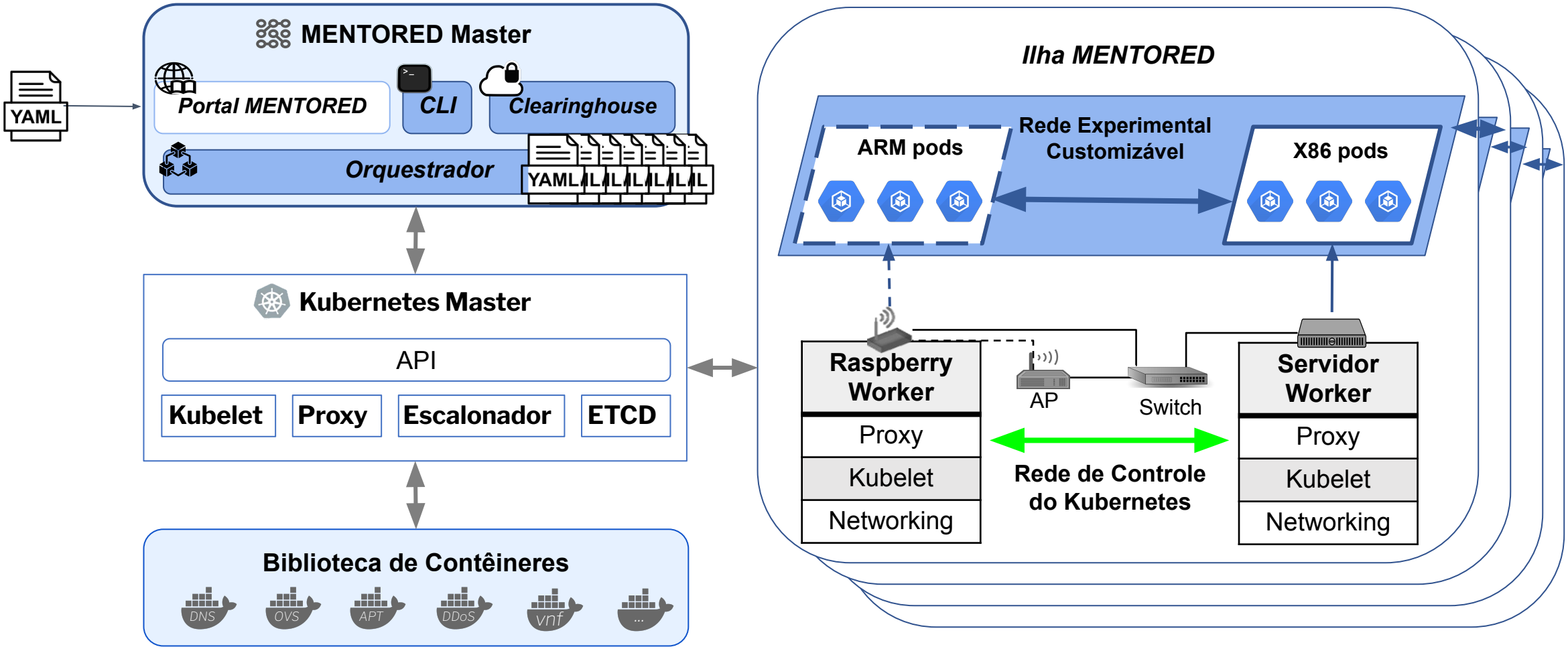


MENTORED Testbed

Arquitetura

WP4

MENTORED

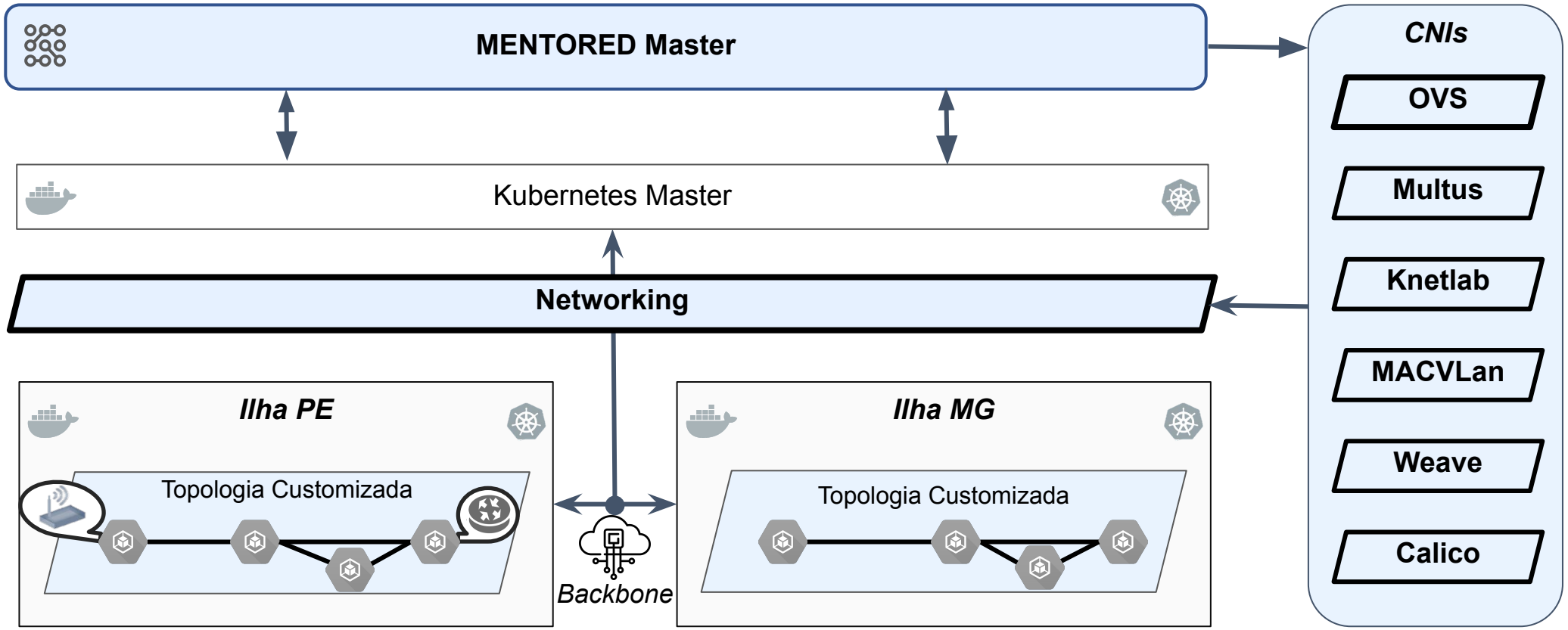


MENTORED Testbed

Container Network Interfaces - CNIs

WP4

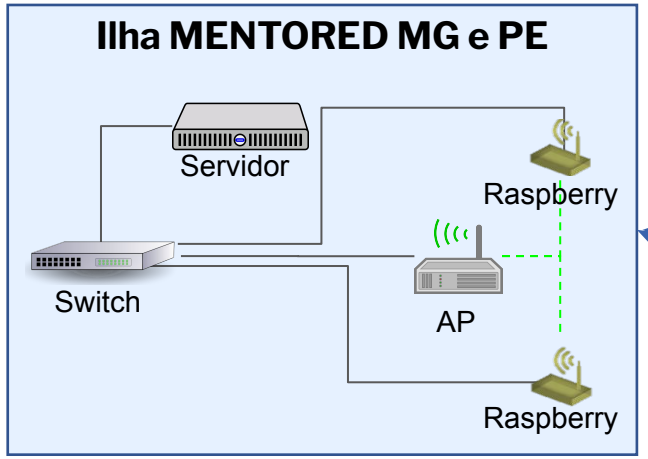
MENTORED

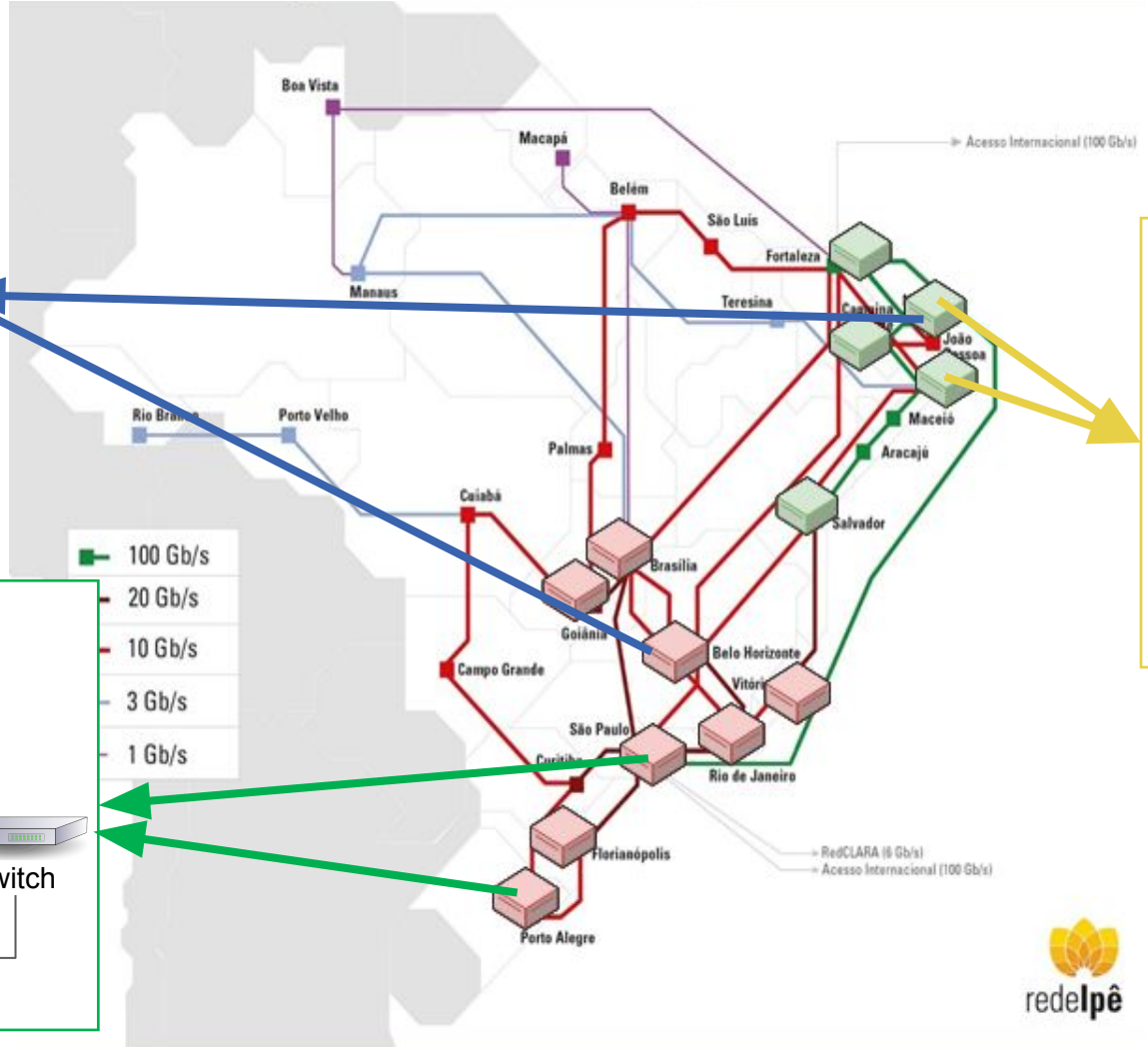


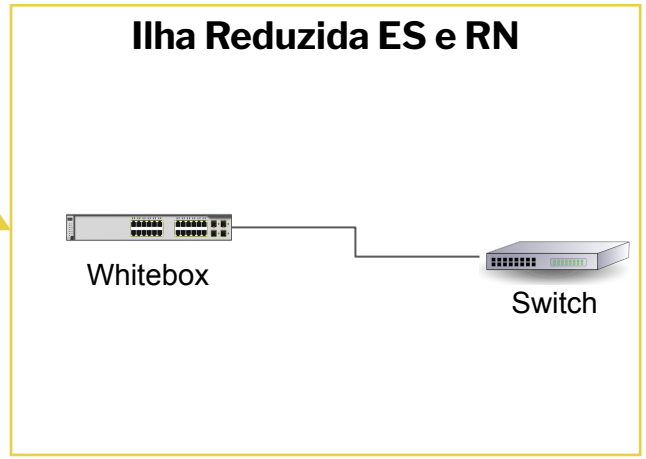
Estudo de caso botnets
Infraestrutura

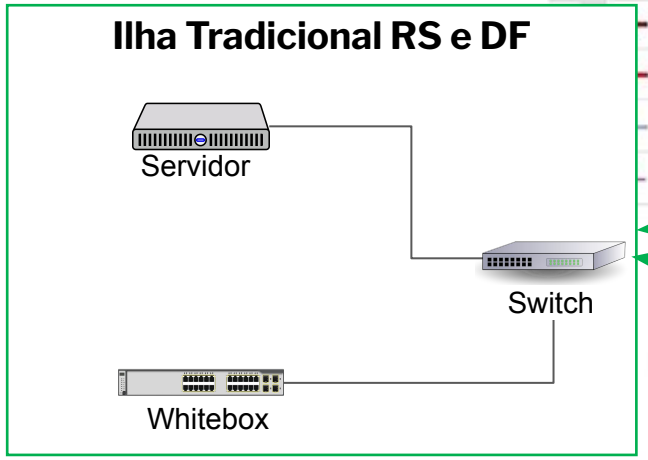
WP4

MENTORED









Estudo de caso botnets
Botnet

WP4

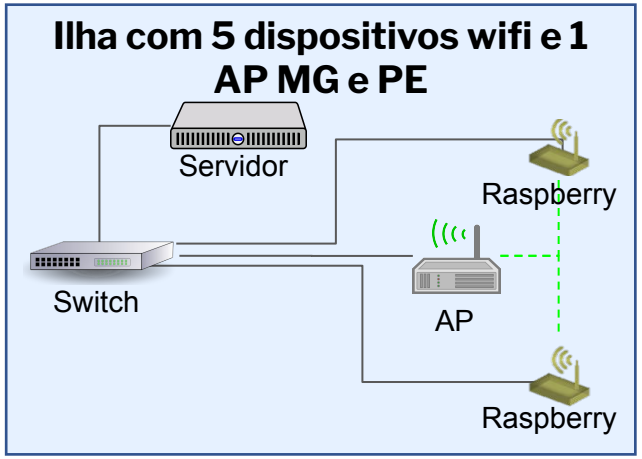
MENTORED

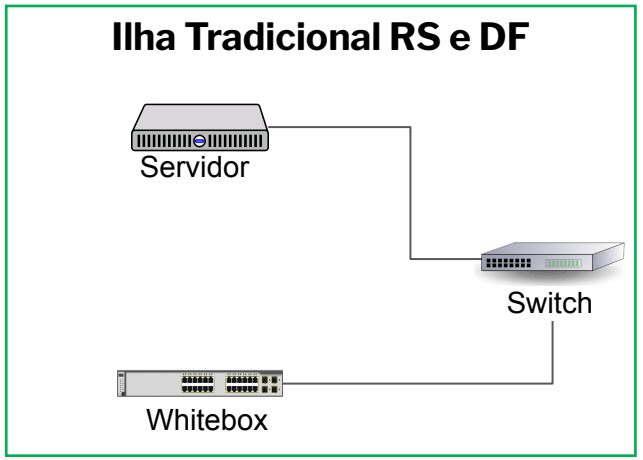
Atacante

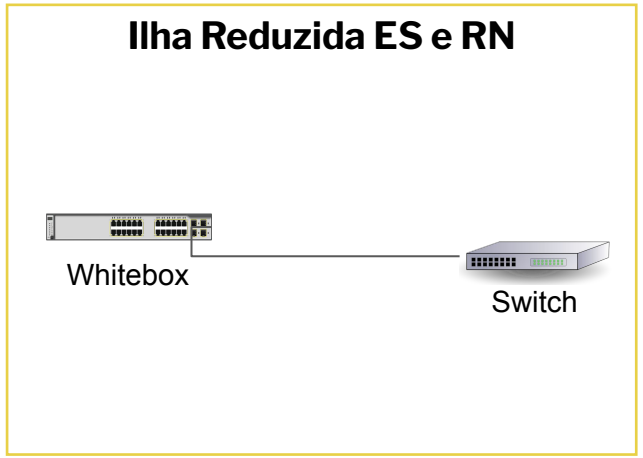
Servidores de Comando e Controle (CNC), Loader e Report

Malware

Dispositivos, serviços, protocolos e/ou aplicações vulneráveis ou não



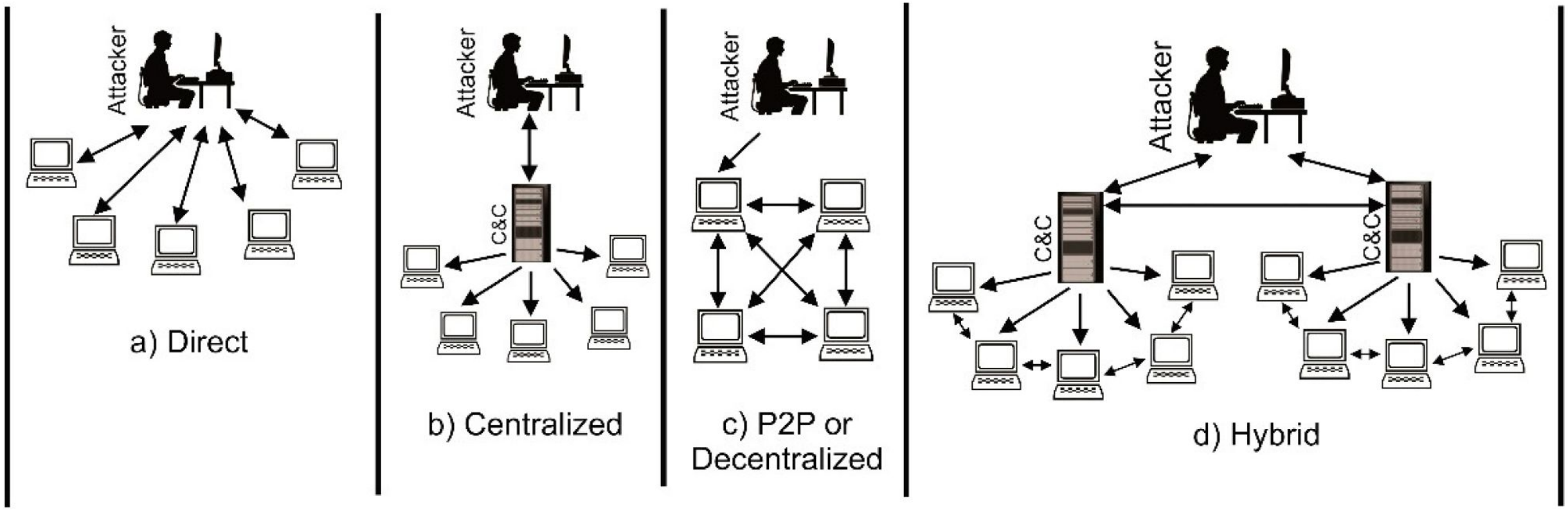




Estudo de caso botnets
Cenário de rede

WP4

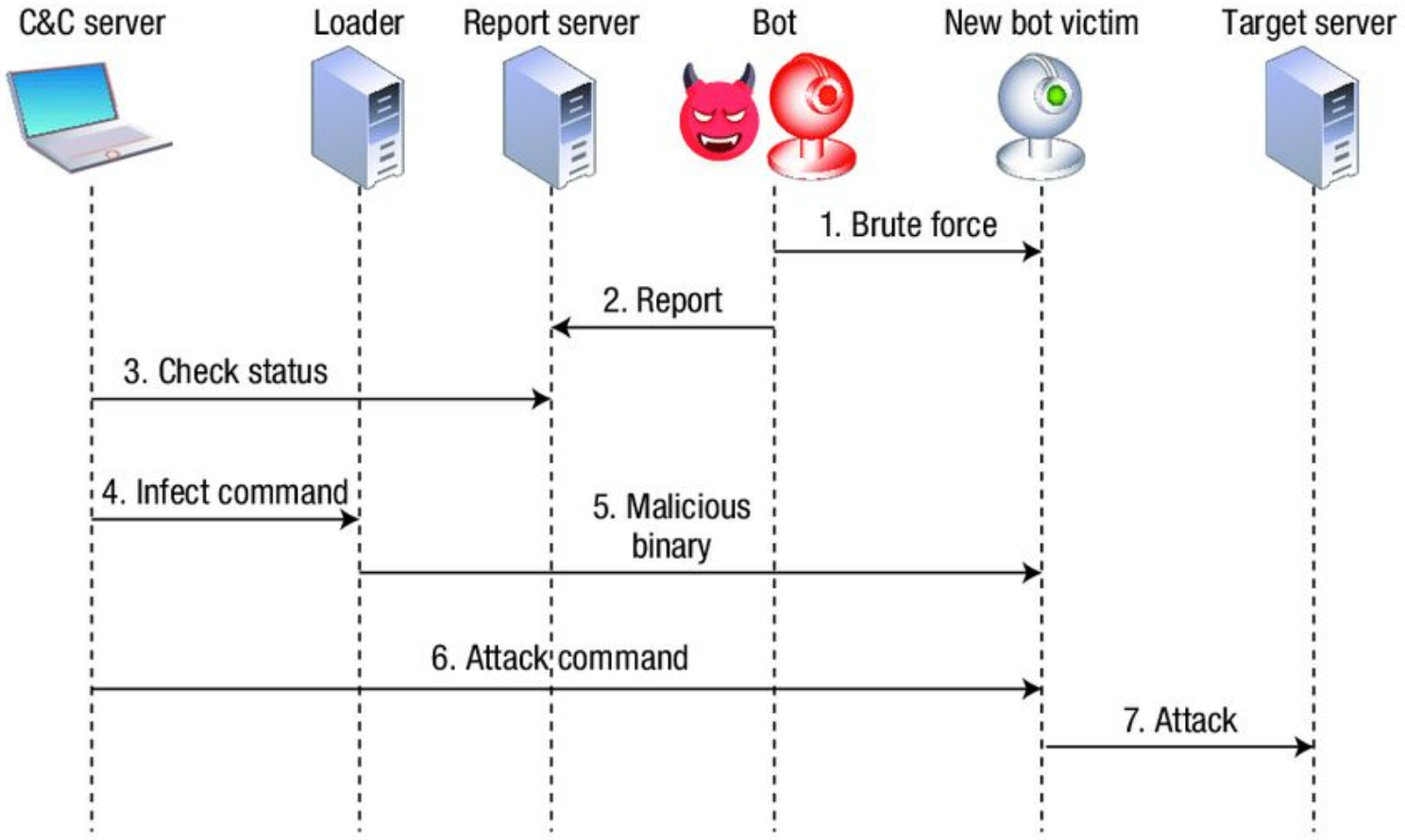
MENTORED



Estudo de caso botnets
Botnet

WP4

MENTORED

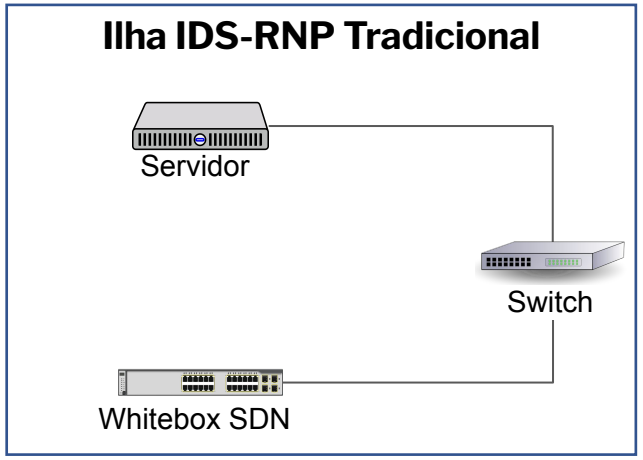


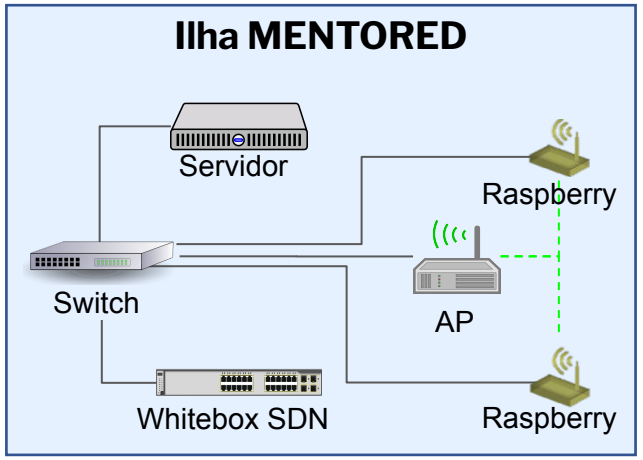
MENTORED Testbed

Ilhas de recursos computacionais

WP4

MENTORED





- Rede local com/sem fio
- Sensores e módulos USB/shields
- Escalabilidade
- Reproduzir firmwares e vulnerabilidades de dispositivos ARM

IDS-RNP e MENTORED Testbed

Metodologia de Desenvolvimento

WP4

MENTORED

- **Ciclos iterativos de desenvolvimento e teste**
  - Definir a demanda
  - Selecionar as ferramentas
  - Criar cenários com as vulnerabilidades, topologias e configurações específicas
  - Automatizar a criação dos cenários
  - Adicionar ao banco de experimentos
  - Documentar

- **Demandas dos demais WPs e da Comunidade**

Estudo de Caso

Objetivos e Infraestrutura

WP4

MENTORED

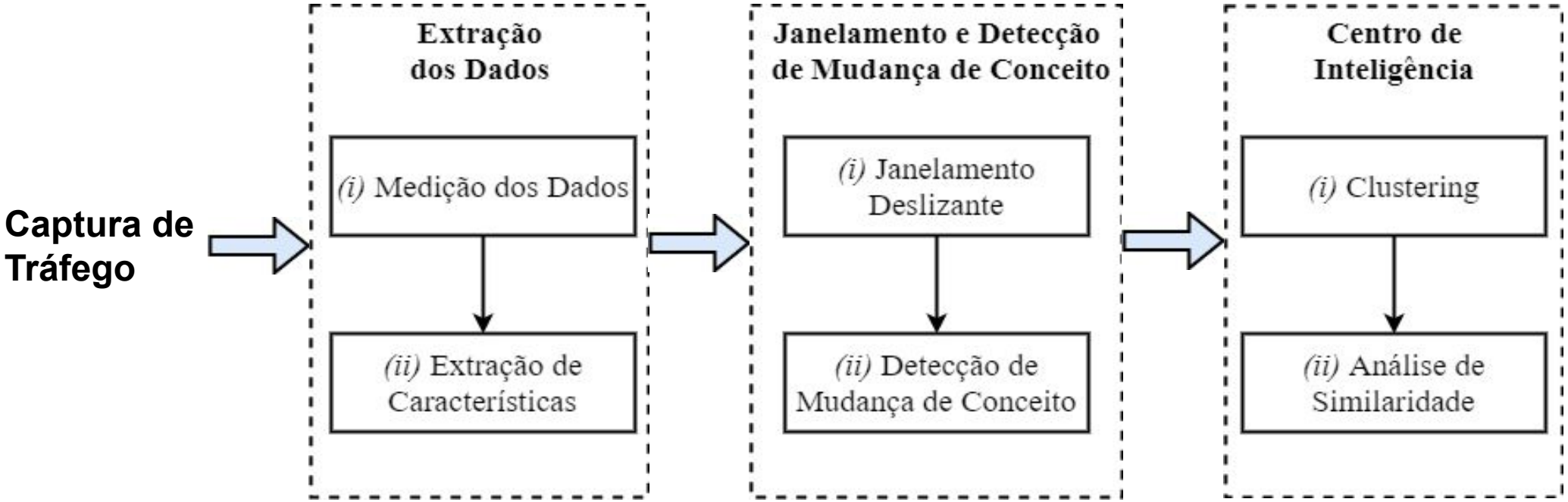
- **Avaliar proposta de detecção de bots no IDS-RNP**
  - Configurar a rede experimental
  - Executar o tráfego da botnet de forma segura
  - Monitorar o tráfego
  - Posicionar a proposta
  - Coletar os resultados
  - Automatizar os processos
- **Reproduzir o tráfego**
  - 4x cenários da CTU-13
  - 2x Variedades: Rbot e Virut
- **Infraestrutura**
  - 2x Ilhas, RS e MG
  - Docker + netvlan

Estudo de Caso

Proposta Avaliada

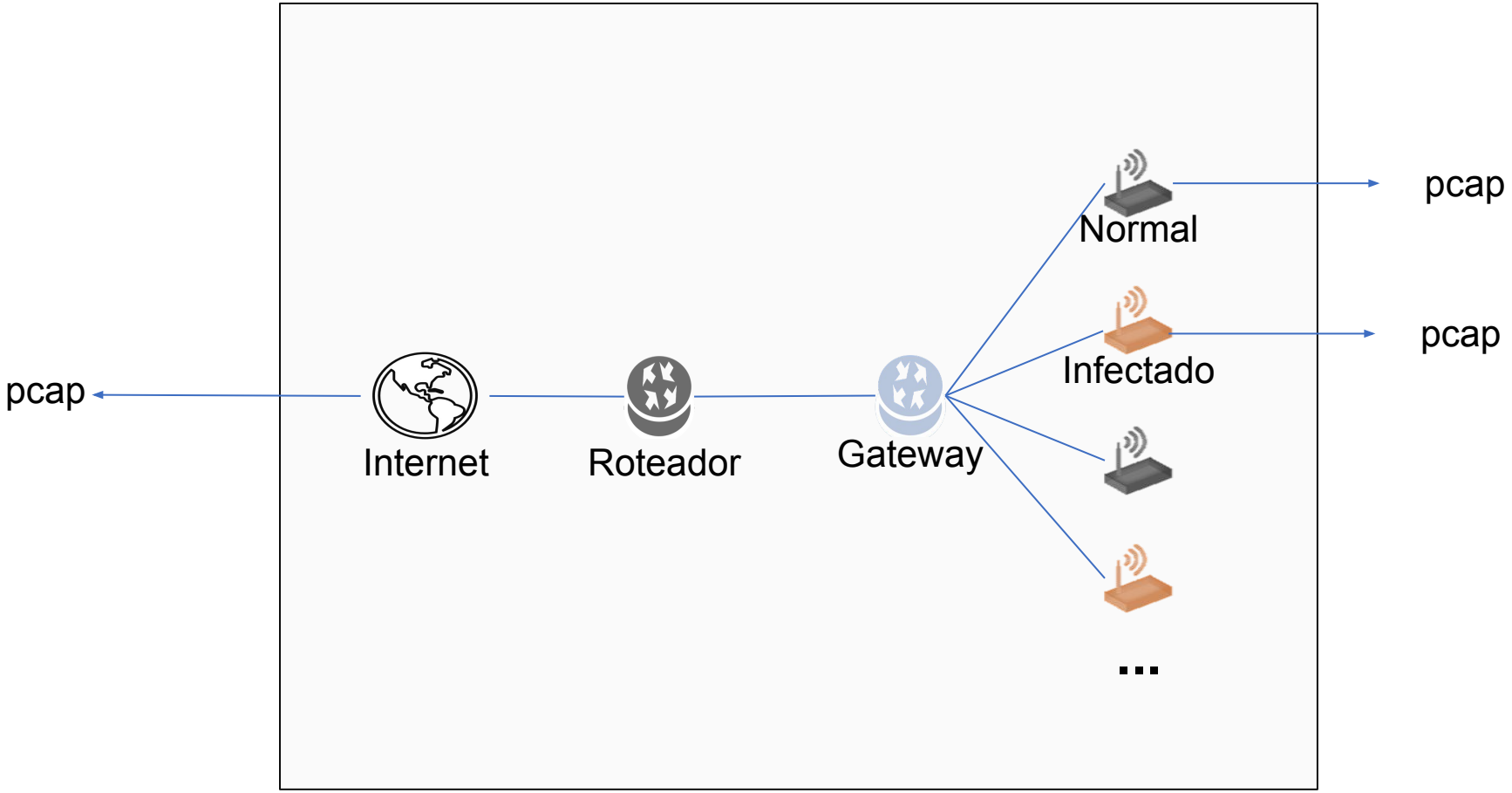
WP4

MENTORED



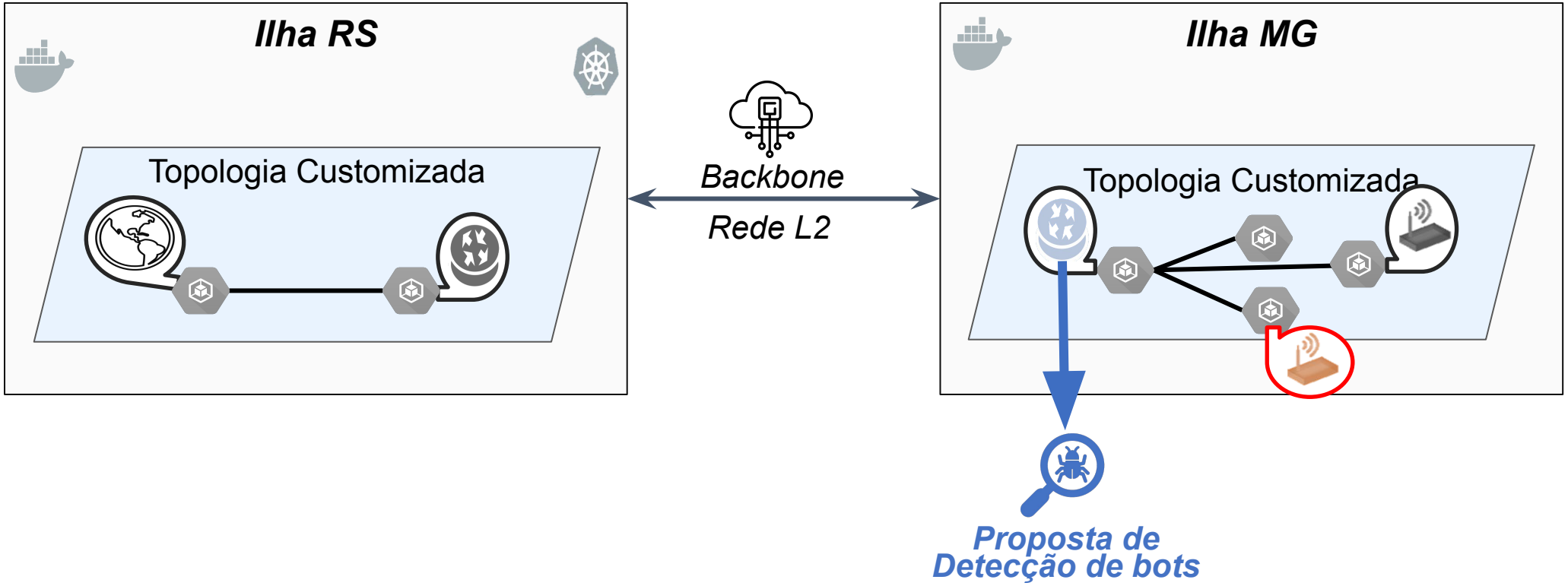
Estudo de Caso

Cenário de Rede



Estudo de caso

Cenário

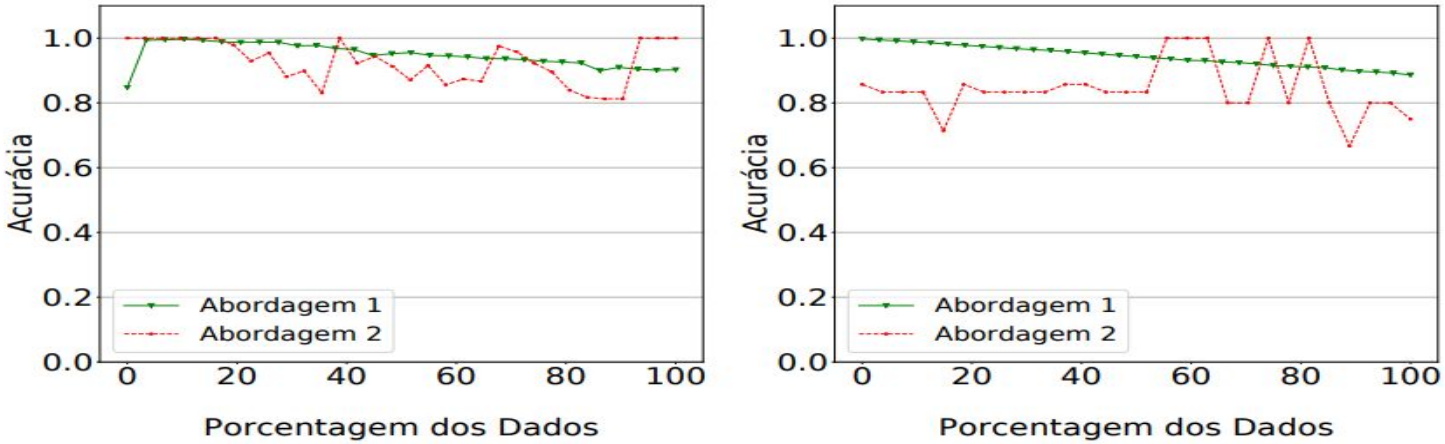


Estudo de Caso

Resultados

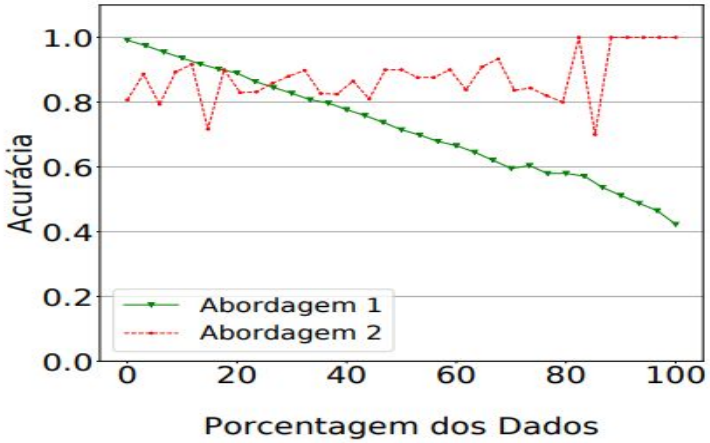
WP4

MENTORED

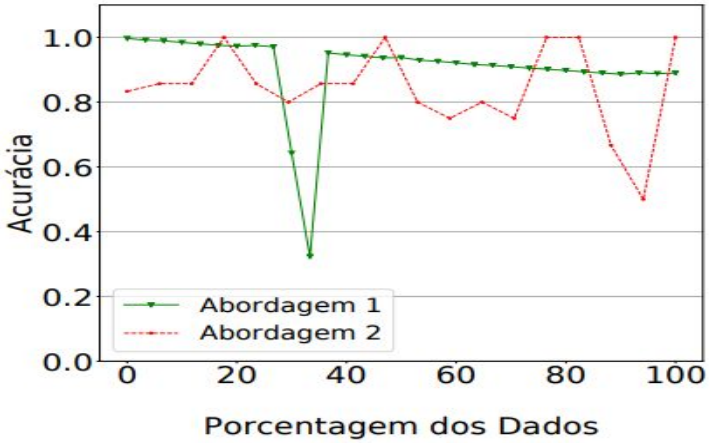


(a) Captura 4

(b) Captura 5



(c) Captura 10



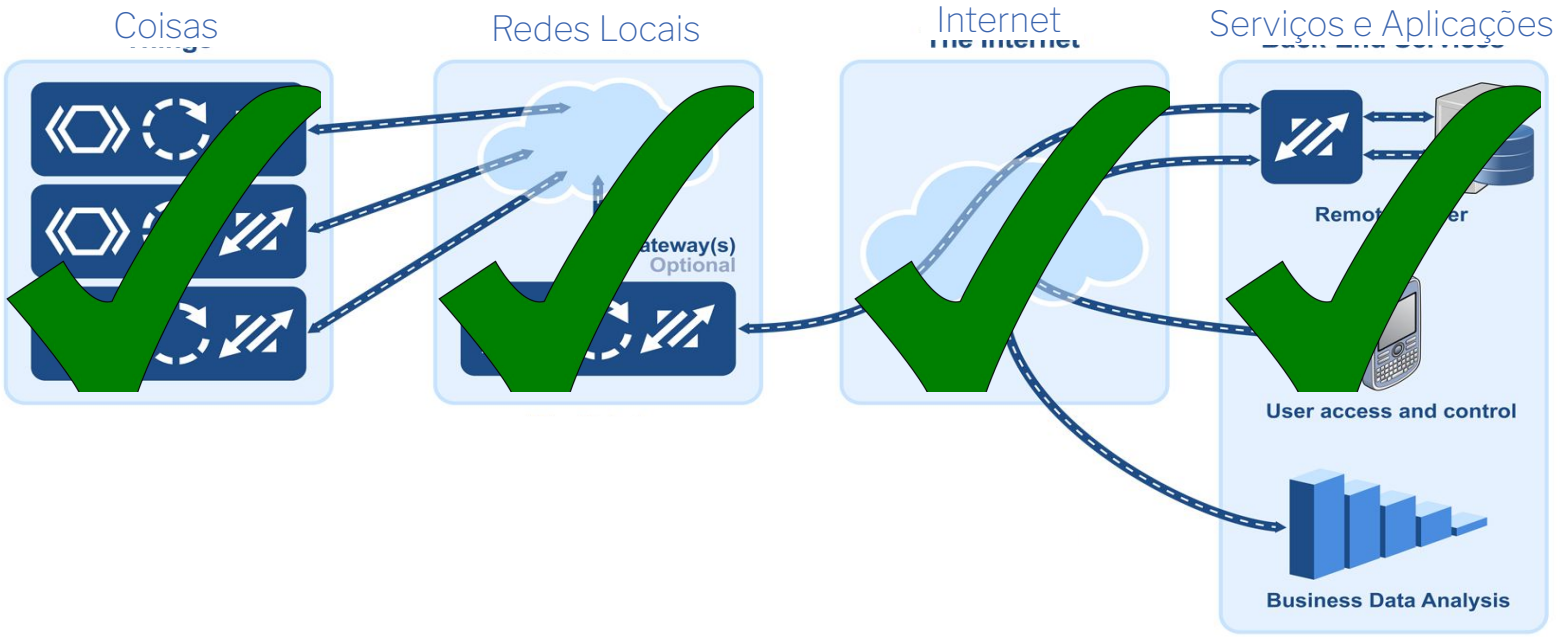
(d) Captura 11

Conclusão

WP4

MENTORED

- Requisitos ✓
  - Fidelidade
  - Validade
  - Escala
  - Segurança
  - Reprodutibilidade
- Estudo de Caso
- O IDS-RNP pode suportar experimentos de cibersegurança



Trabalhos Futuros

WP4

MENTORED

- Melhorar os requisitos no IDS-RNP com novas ferramentas
- Compartilhamento da Infraestrutura
  - Isolamento e QoS
- Melhorar monitoramento dos servidores bare metal
- Conduzir experimentos em outros contextos (carga e escala)
- Desenvolver o Portal do MENTORED testbed e a Clearinghouse
- Liberar o MENTORED Testbed para a comunidade

Q&A

WP4

MENTORED

nelsonprates@ufmg.br