



U F *m* G

UNIVERSIDADE FEDERAL
DE MINAS GERAIS

USP

Virtualização de Funções de Rede na IoT: Um Panorama do Gerenciamento de Desempenho x Segurança

Simpósio Brasileiro de Redes de Computadores e
Sistemas Distribuídos (SBRC 2021)
16 de agosto de 2021

FAPESP



cgi.br
Comitê Gestor da
Internet no Brasil





- **Guilherme Werneck de Oliveira (USP)**
- **Jonathan Rangel Porto (USP)**
- **Nelson Gonçalves Prates Jr. (UFMG)**
- **Aldri Luiz dos Santos (UFMG)**
- **Michele Nogueira (UFMG)**
- **Daniel Macêdo Batista (USP)**

Agenda



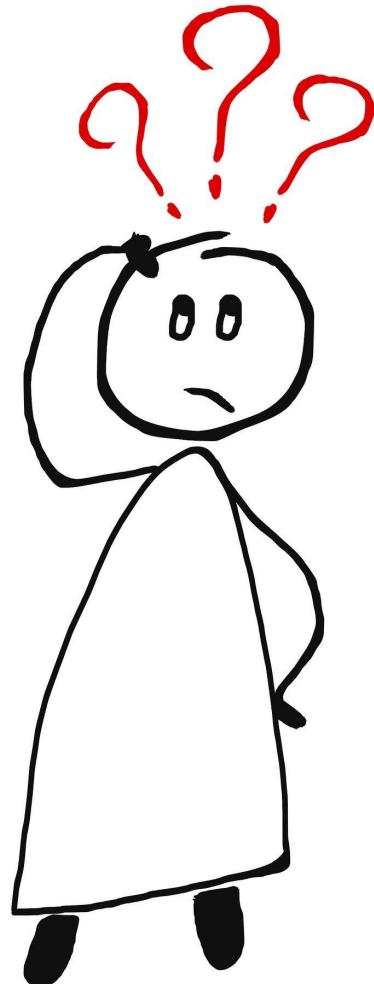
MENTORED

- **Introdução**
- **Fundamentos**
- **Gerenciamento de Desempenho e Segurança em IoT com NFV**
- **Estudo de Caso: MENTORED Testbed**
- **Principais Desafios e Limitações**
- **Considerações Finais**

Dúvidas e Questões



MENTORED



A qualquer momento



- **IoT - Internet das Coisas**
- **NFV - Virtualização de Funções de Rede**
- **VNF - Função de Rede Virtualizada**
- **SFC - Encadeamento de Funções de Serviço**
- **IDS - Sistema de Detecção de Intrusão**
- **DPI - Inspeção Profunda de Pacotes**
- **SDN - Rede Definida por Software**
- **VM - Máquina Virtual**



Introdução



Introdução



MENTORED

Abrangência da IoT



- Marcapassos cardíacos
- Coletores de glicose
- Monitoramento contínuo
- Sensores ingeríveis

Introdução



MENTORED

Abrangência da IoT

- Monitoramento da fauna
- Mudanças climáticas
- Agricultura inteligente



Introdução



MENTORED

Abrangência da IoT



- **Cidades inteligentes**
- **Monitoramento do transporte público**
- **Otimização de rotas e semáforos**
- **Manutenção de veículos**
- **Veículos autônomos**

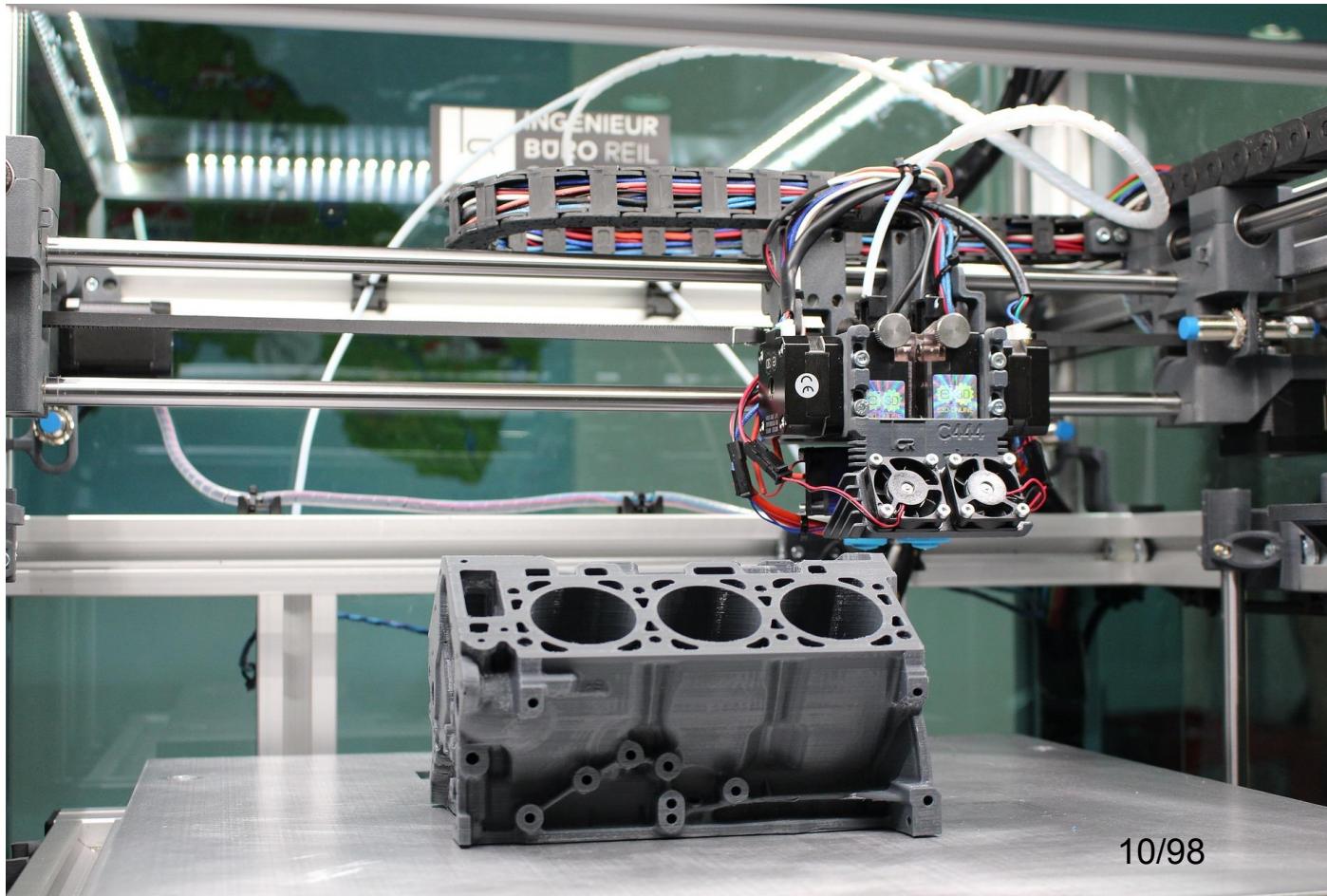
Introdução



MENTORED

Abrangência da IoT

- Processos orientados por temperatura e umidade
- Redução de riscos de acidentes
- Monitoramento de máquinas



Introdução



MENTORED

Abrangência da IoT



- **Interações por voz**
- **Energia eficiente**
- **Segurança**



Abrangência da IoT



Heterogeneidade de dispositivos

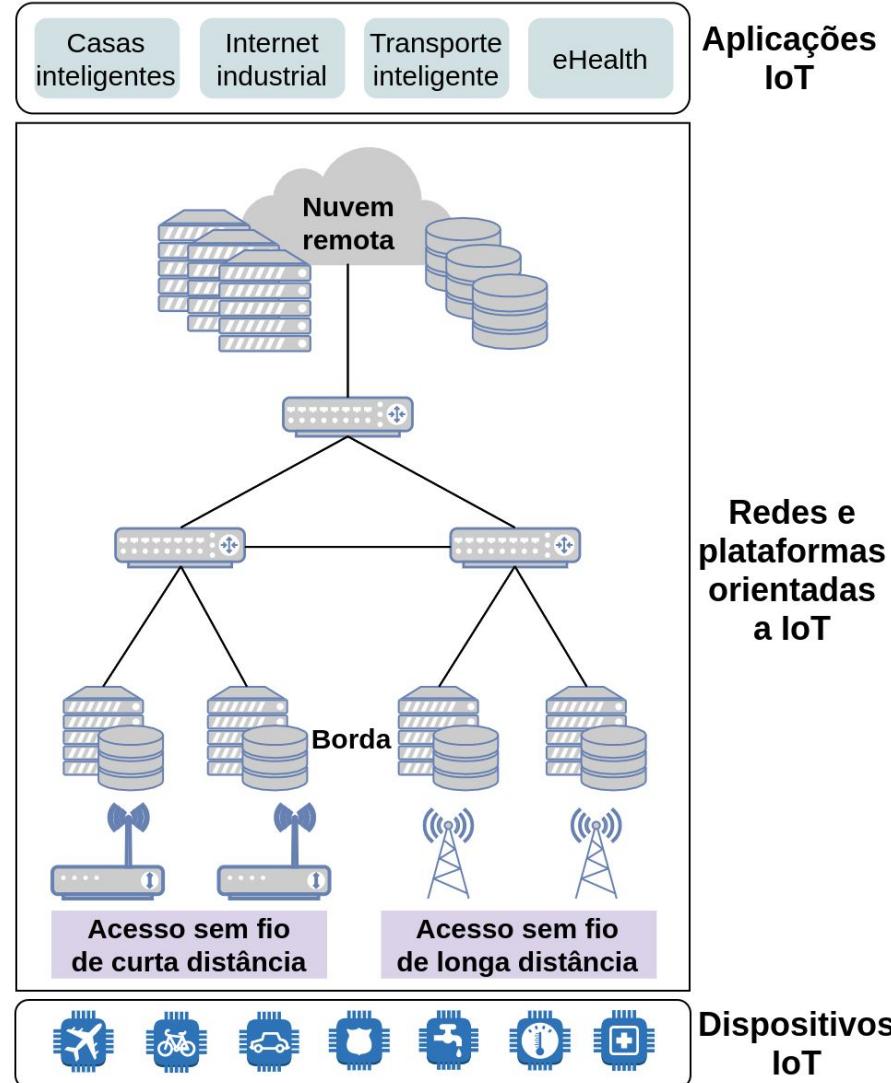


Infraestruturas complexas

Introdução



MENTORED



Desempenho

+

Segurança



kaspersky

16 de outubro de 2019

Brasil é o segundo país com mais ataques a dispositivos IoT

No primeiro semestre deste ano, a Kaspersky registrou mais de 100 milhões de ataques – quantidade cerca de nove vezes maior do que o mesmo período em 2018

Quase 30% das empresas que usam IoT sofreram incidentes de segurança

Pesquisa mostra ainda que tais riscos não desmotivam os investimentos das empresas em IoT, mas elas precisam tomar cuidados com a implementação de medidas de segurança

Introdução



MENTORED



Keeping the gate locked on your IoT devices: Vulnerabilities found on Amazon's Alexa

August 13, 2020

**Mais de 100 milhões
de ataques contabilizados!**



Ameaças na IoT



NFV



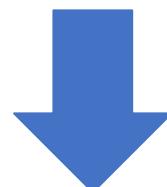
Gerenciamento de desempenho



Ameaças na IoT



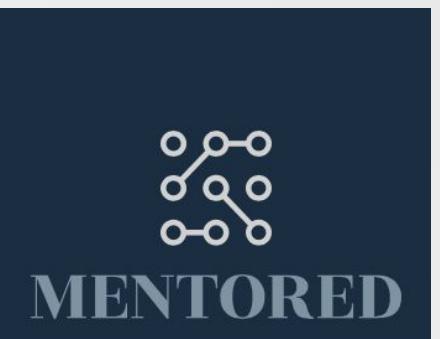
NFV



Gerenciamento de desempenho



Estado da arte



Conceitos Básicos



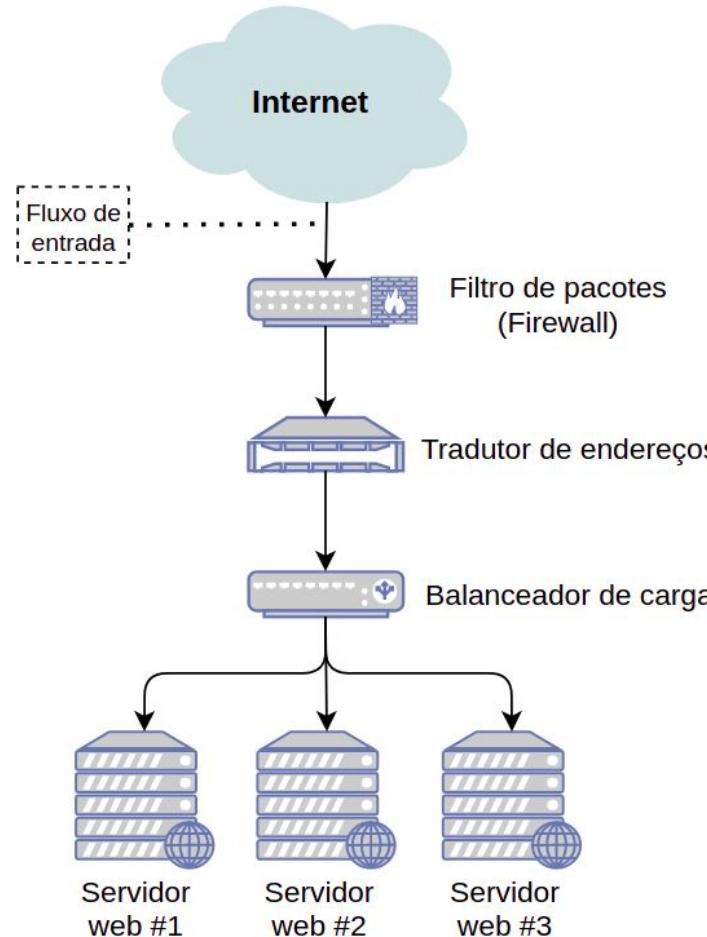
Conceitos Básicos

Virtualização de Funções de Rede (NFV)



MENTORED

Encadeamento de Funções em Redes Tradicionais



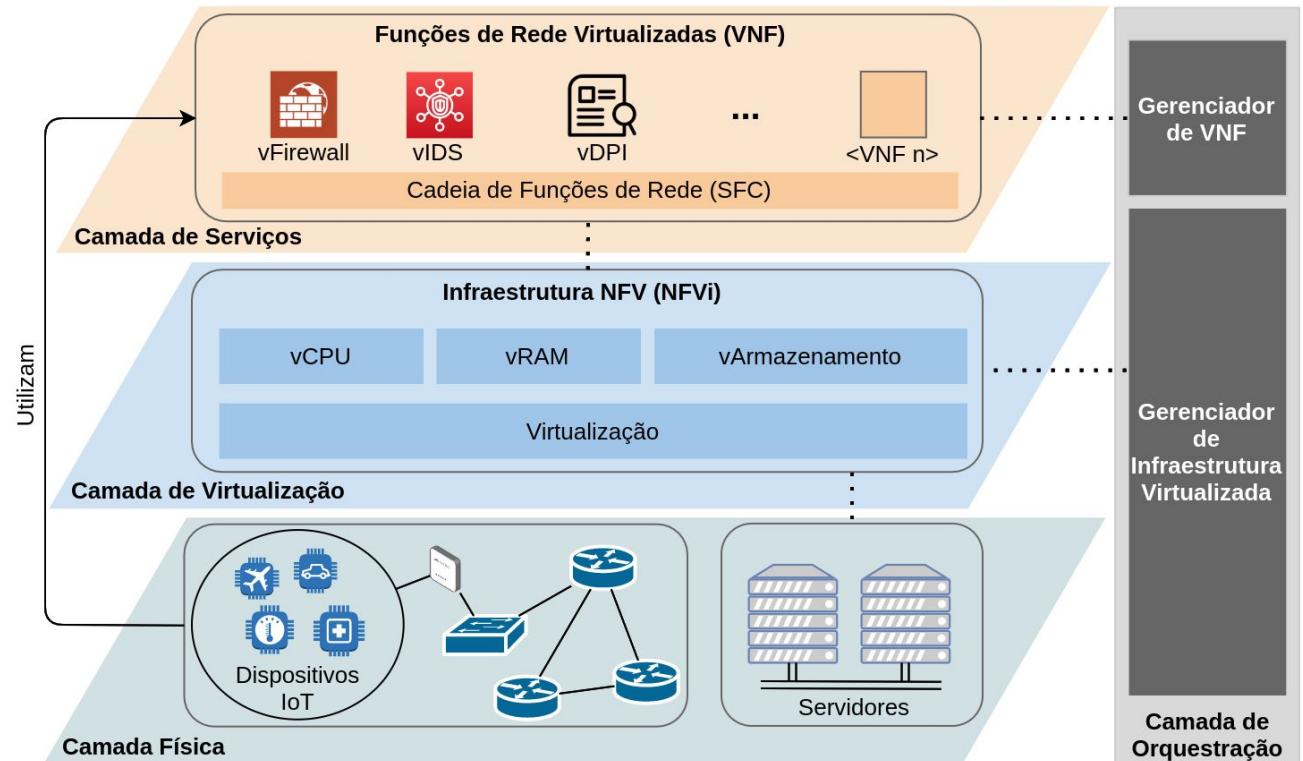
- **Filtragem de pacotes**
 - Verifica se características do fluxo coincidem com alguma regra que representa um potencial ataque
- **Tradução de endereços**
 - Repassa os pacotes da requisição para uma rede interna com endereços IP não roteáveis na Internet
- **Balanceamento de carga**
 - Distribui as requisições entre o conjunto de servidores web, reduzindo a chance de sucesso de um ataque de negação de serviço

Conceitos Básicos



MENTORED

- **Virtualização de Funções de Rede (NFV)**
- **Redes IoT e Aplicações**
- **Gerenciamento de Redes com NFV**
- **Questões de Desempenho x Segurança com NFV na IoT**



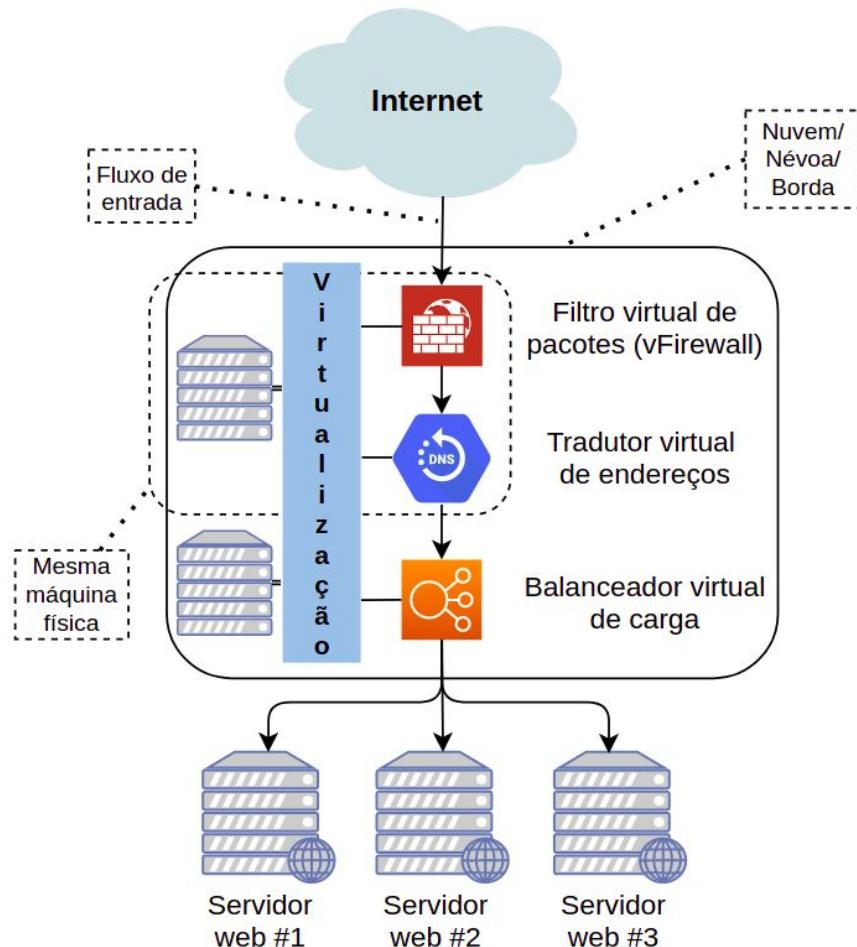
Conceitos Básicos

Virtualização de Funções de Rede (NFV)



MENTORED

Encadeamento de Funções em Redes Tradicionais



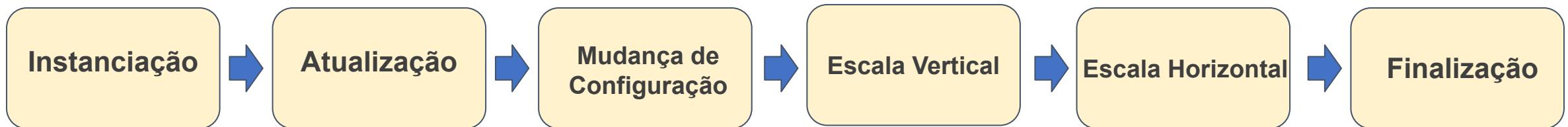
Conceitos Básicos

Gerenciamento de Redes com NFV



MENTORED

Ciclo de Vida de uma VNF



Conceitos Básicos

Redes IoT e Aplicações



MENTORED

Arquitetura em Camadas da IoT



• Camada de aplicação

- Implementação das aplicações. Exemplos: aplicativos de cidades inteligentes, indústrias inteligentes e casas inteligentes

• Camada de rede

- Integra diversos dispositivos de interconexão, como switches e pontos de acesso, a várias tecnologias de comunicação, como Bluetooth e Wi-Fi

• Camada de percepção

- Interação com os dispositivos e componentes físicos dos objetos inteligentes, obtendo dados e enviando comandos



Desempenho

Métricas
+
Medições

ISO/IETF

ou

Indicadores
+
Avaliações

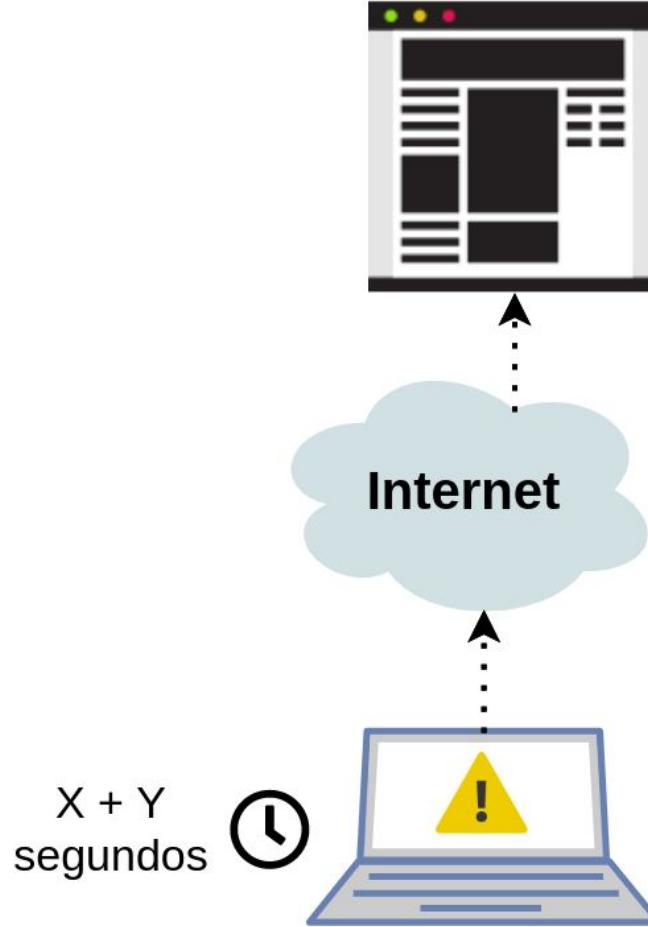
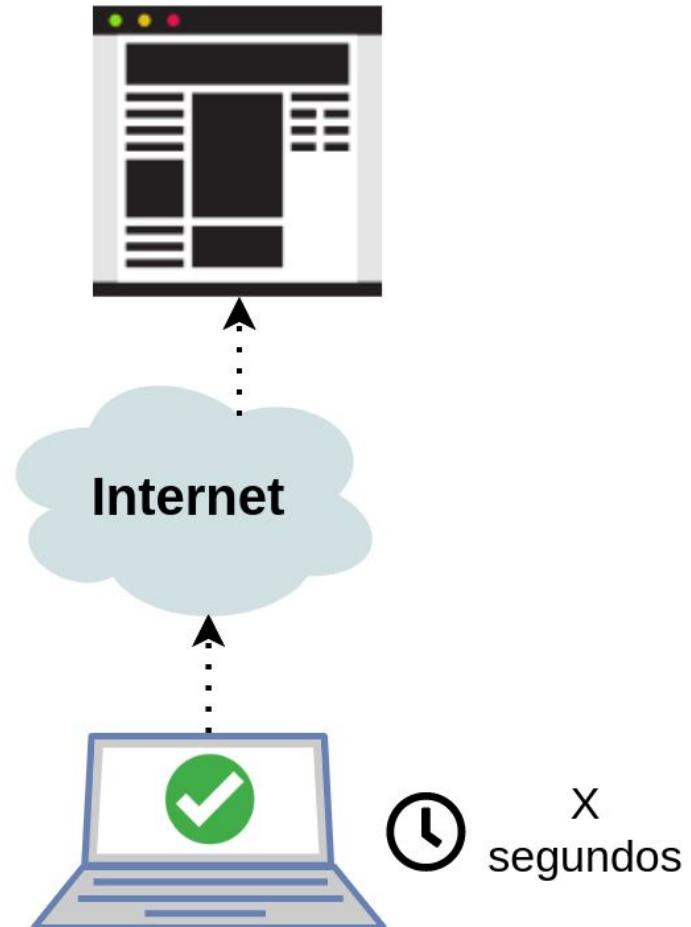
Literatura

Conceitos Básicos

Questões de Desempenho x Segurança com NFV na IoT



MENTORED





NFV

ETSI

(European Telecommunications Standards Institute)

Velocidade

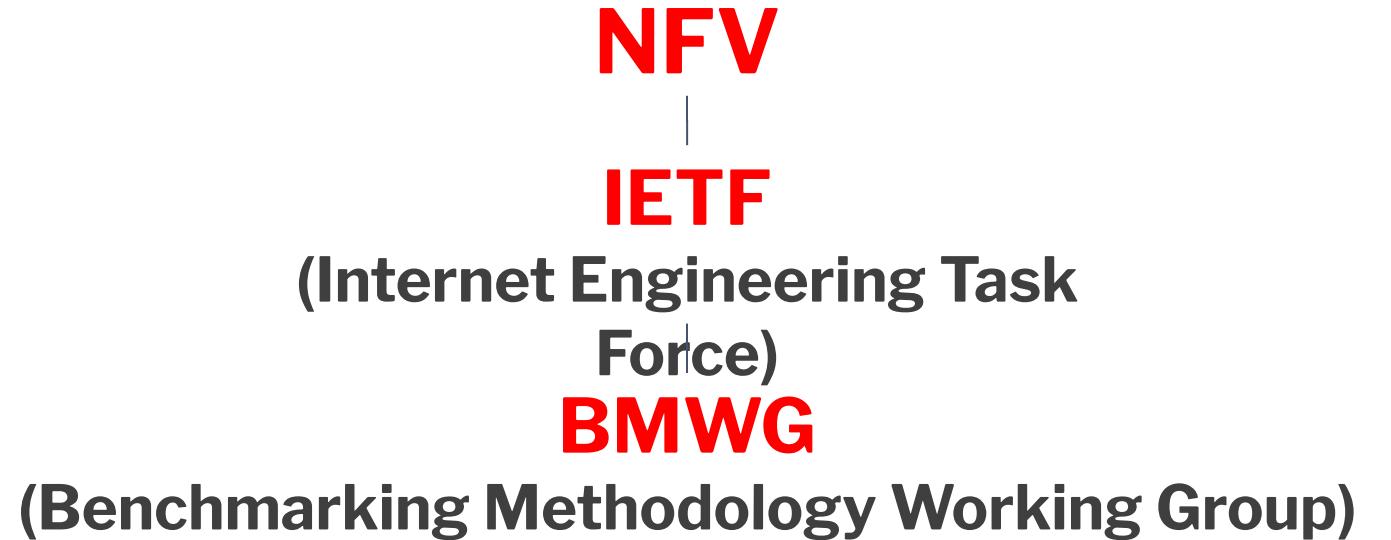
- Latência de provisionamento de VM
- Latência de provisionamento de Rede Virtual (VN)
- Atraso e taxa de transferência de pacotes

Acurácia

- Política de conformidade da VM
- Erro de *clock* da VM
- Taxa de perda de pacotes

Confiabilidade

- Provisionamento de VM
- Taxa de liberação prematura de VM
- Provisionamento de VN
- Conexão interrompida



Recurso

- Consumo de CPU
- Consumo de memória (RAM)

Rede

- Taxa de transferência
- Taxa de perda de quadros
- Latência



NFV – Autores

¹ Gupta et al. 2019

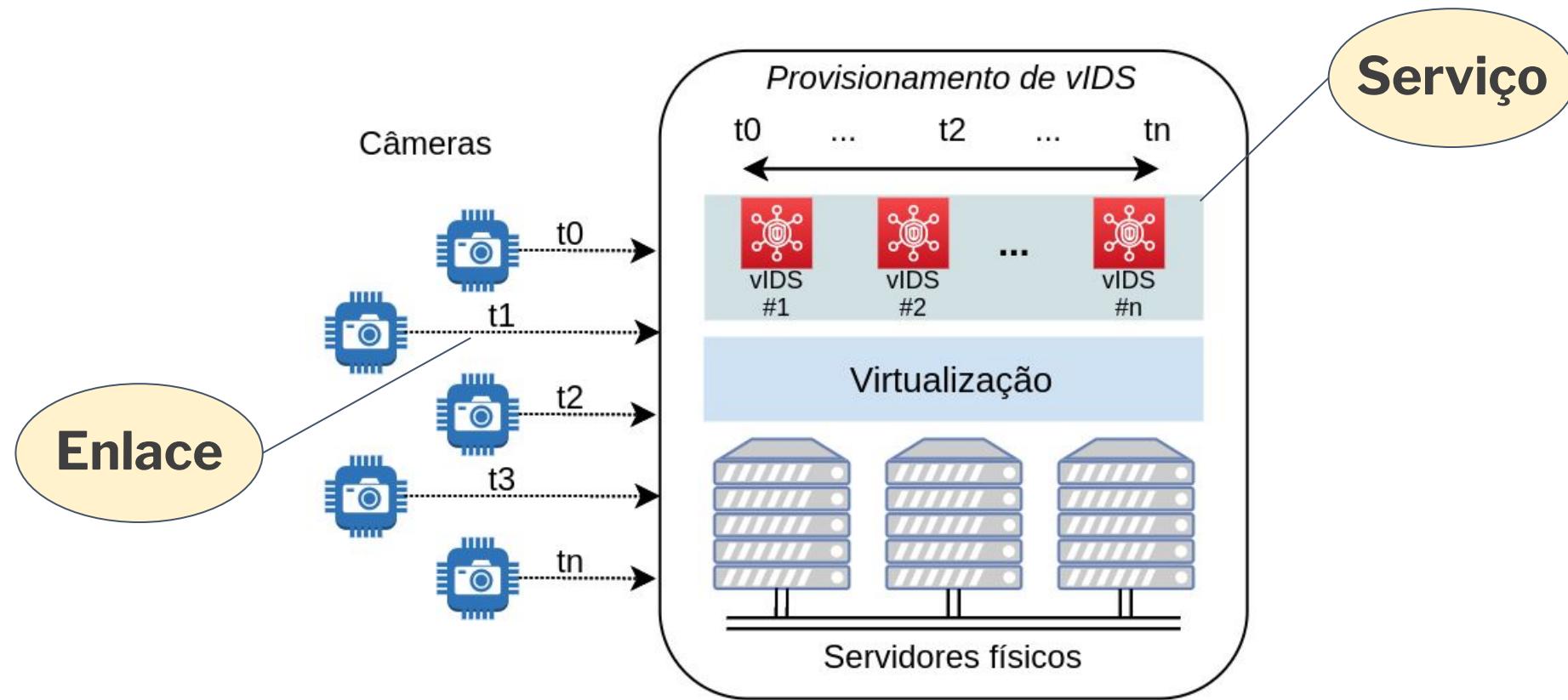
- Tolerância a falhas (1)
- Consumo de CPU (2, 3)
- Consumo de Memória (2)
- Taxa de E/S de armazenamento (2)
- Tempo de recuperação de VNF (2)
- Taxa de transferência de pacotes (1, 2, 3)
- Taxa de perda de pacotes (1)
- Latência de rede (2, 3)

² Kim et al. 2015

³ Zhang et al. 2016



IoT - Baixo Consumo de Energia + Computação Limitada



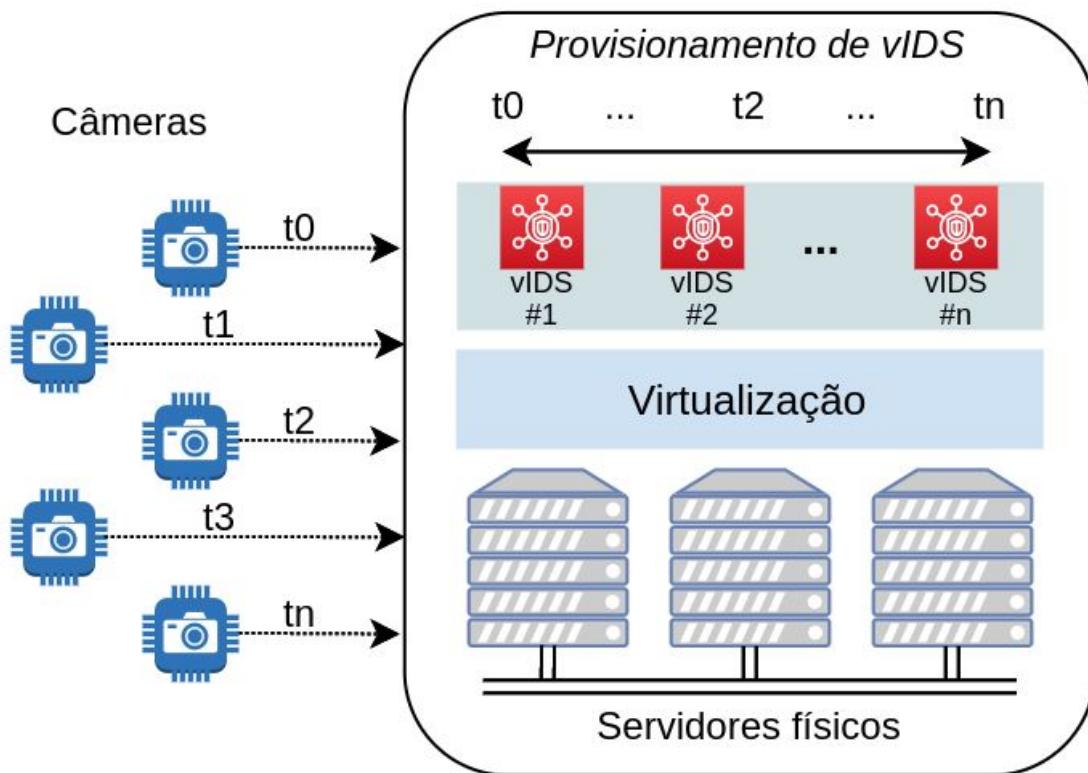
Conceitos Básicos

Questões de Desempenho x Segurança com NFV na IoT

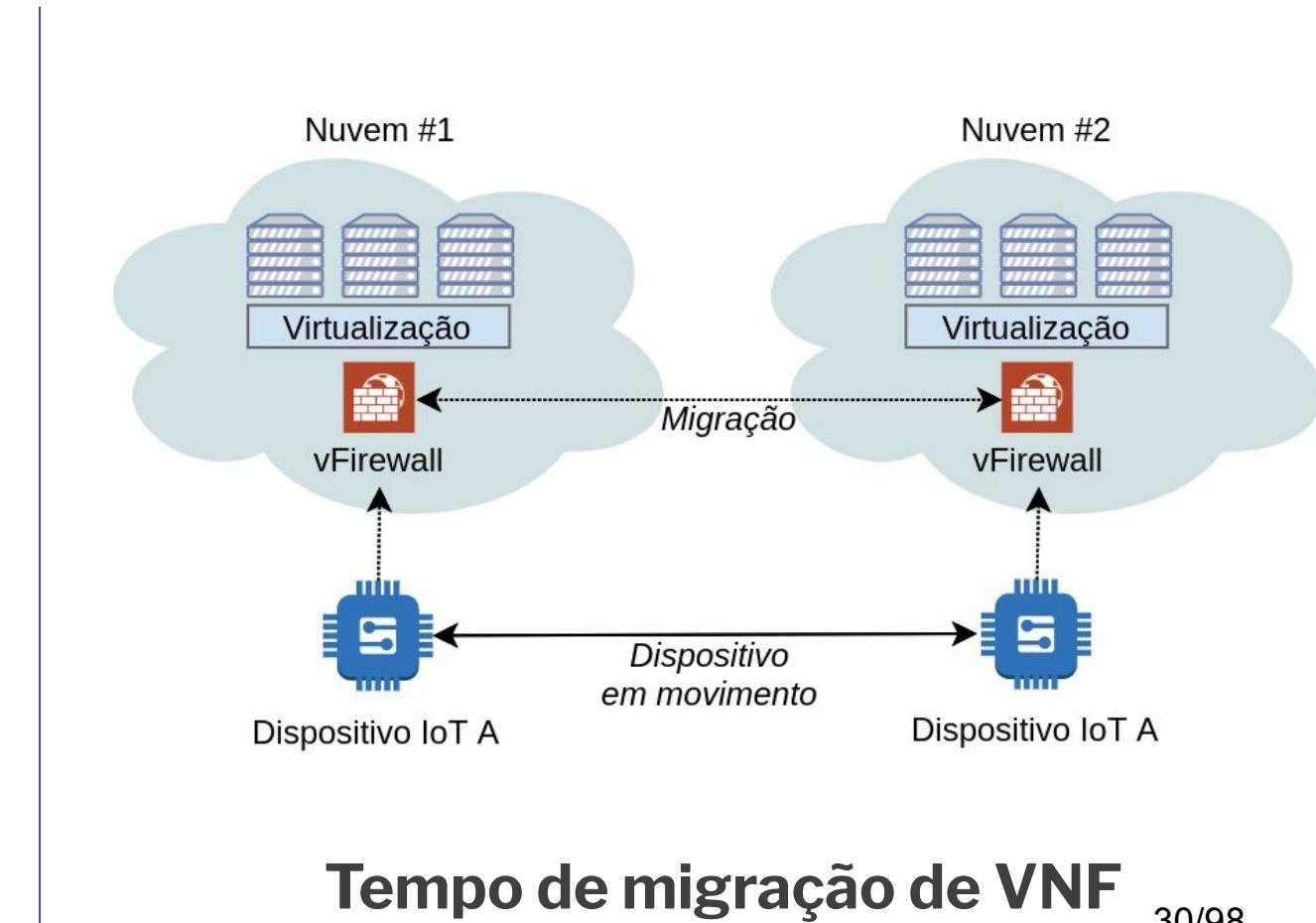


MENTORED

RFC 8172



Tempo de implantação de VNF

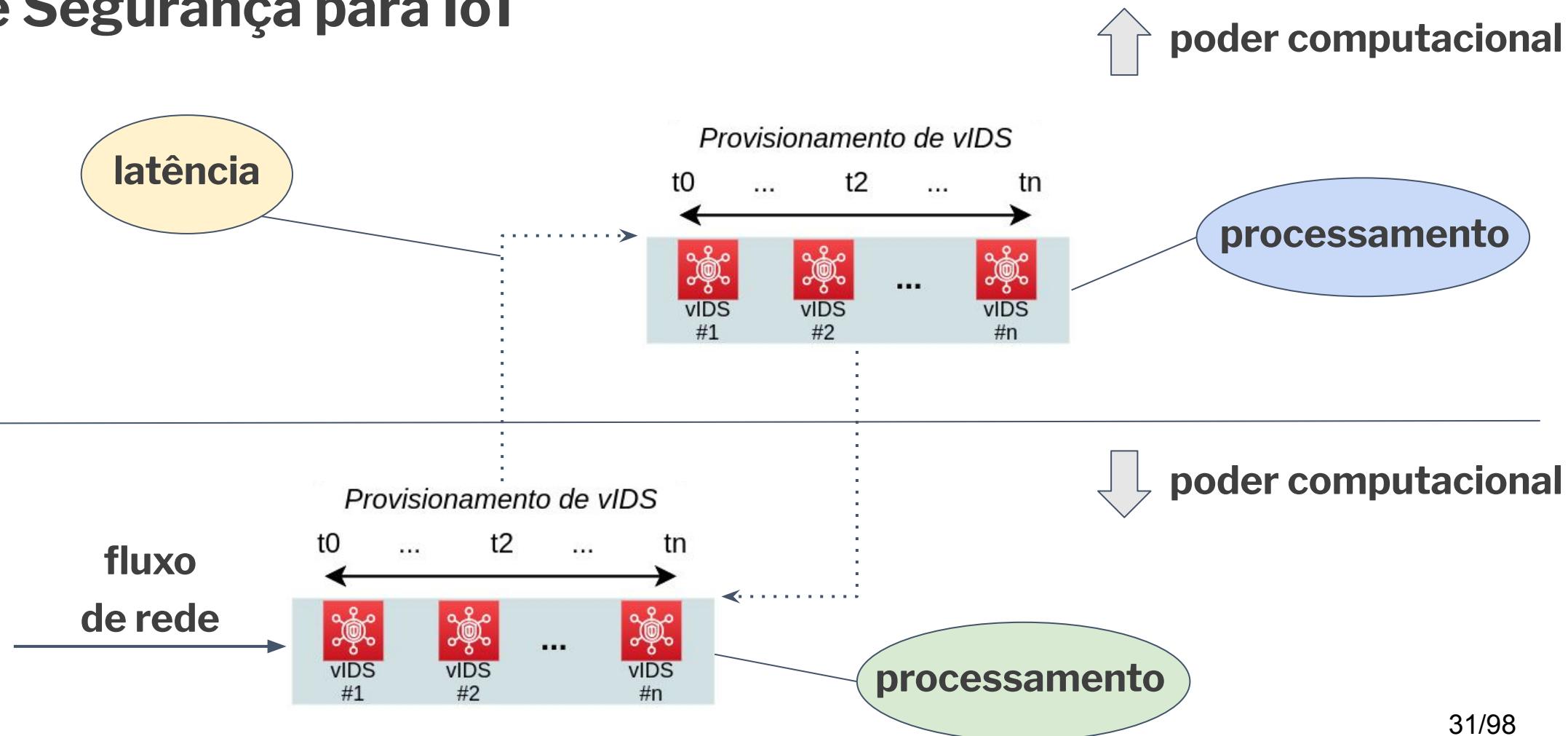


Tempo de migração de VNF



NFV de Segurança para IoT

Remoto

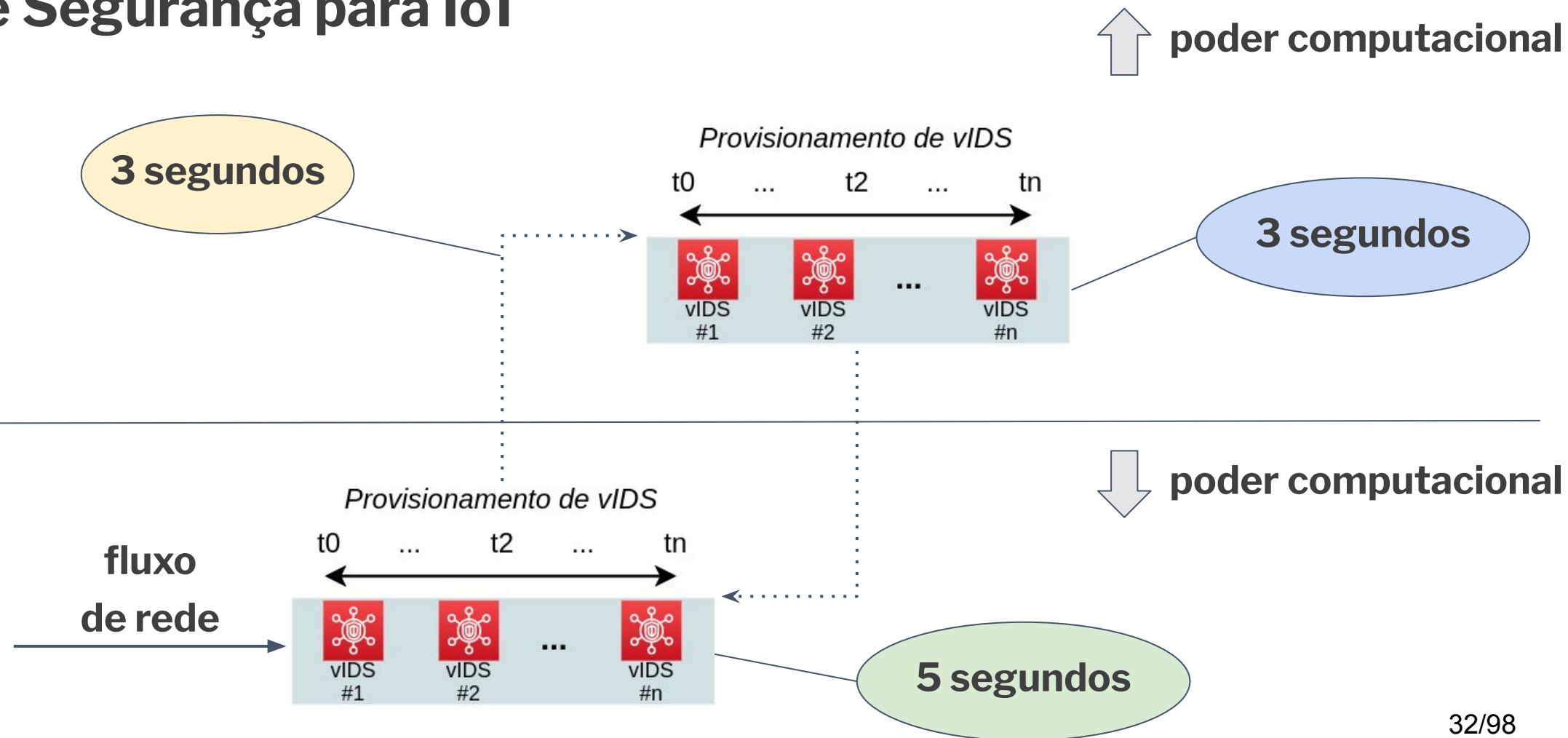


Local



NFV de Segurança para IoT

Remoto



Local

Conceitos Básicos

Questões de Desempenho x Segurança com NFV na IoT



MENTORED

NFV de Segurança para IoT - Para Farris et al. 2019

Separação do software de segurança do hardware

**Escalabilidade sob demanda e tolerância
a falhas para VNF de segurança**

Suporte à mobilidade de VNF de segurança

**Encadeamento de serviços
de segurança de rede**



NFV de Segurança para IoT - Para Farris et al. 2019 - Indo Além

Separação do software de segurança do hardware

Escalabilidade sob demanda e tolerância
a falhas para VNF de segurança

Suporte à mobilidade de VNF de segurança

Encadeamento de serviços
de segurança de rede

VNF para modelos de
aprendizado de segurança



NFV de Segurança para IoT - Para Farris et al. 2019

Separação do software de segurança do hardware

Bremler-Barr et al. 2014

vDPI

x Middleboxes

Taxa de transferência de pacotes



NFV de Segurança para IoT - Para Farris et al. 2019

Separação do software de segurança do hardware

Bremler-Barr et al. 2014

Montero et al. 2015

TVD (*Trusted Virtual Domain*)

Prevenção



NFV de Segurança para IoT - Para Farris et al. 2019

Separação do software de segurança do hardware

Bremler-Barr et al. 2014

Montero et al. 2015

Yu et al. 2015



IoTSec

VNF

μboxes

gateways de
segurança



NFV de Segurança para IoT - Para Farris et al. 2019

Escalabilidade sob demanda e tolerância
a falhas para VNF de segurança

Cao et al. 2015

NFV-VITAL

Desempenho

VNF



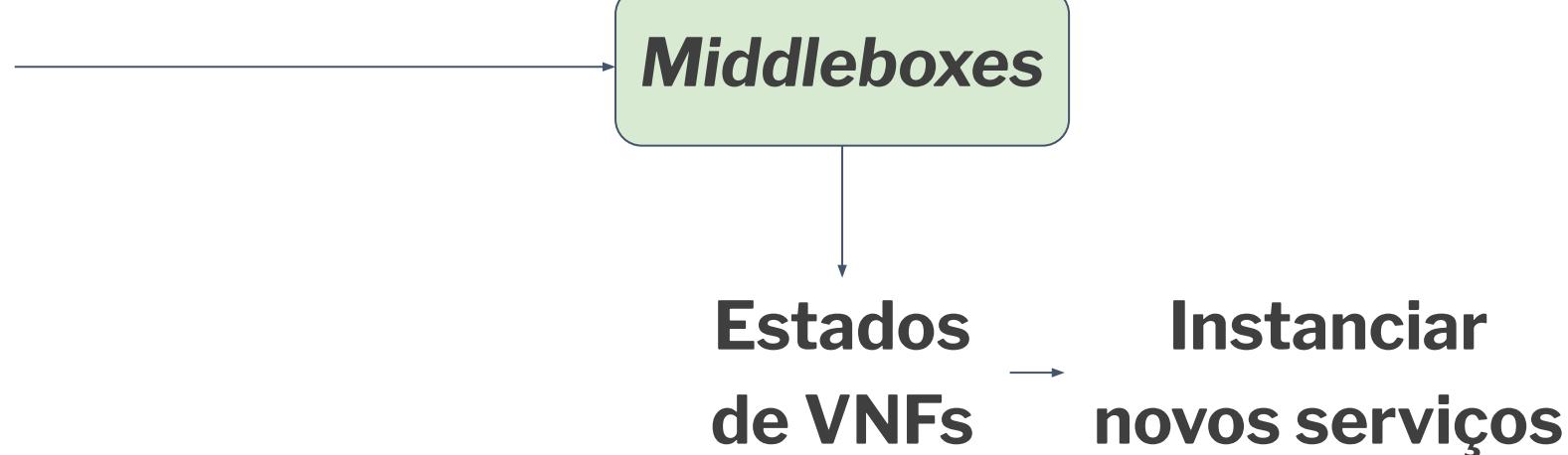


NFV de Segurança para IoT - Para Farris et al. 2019

Escalabilidade sob demanda e tolerância
a falhas para VNF de segurança

Cao et al. 2015

Hafeez et al. 2016

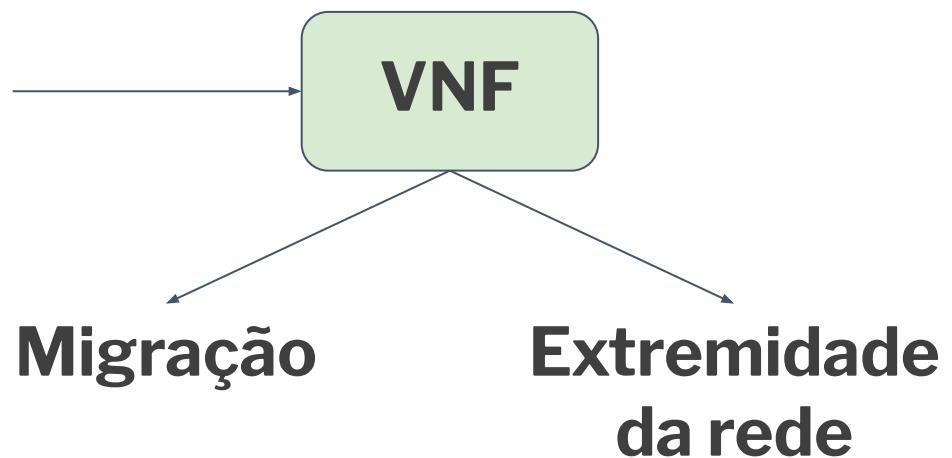




NFV de Segurança para IoT - Para Farris et al. 2019

Suporte à mobilidade de VNF de segurança

Montero e Serral-Gracià 2016





NFV de Segurança para IoT - Para Farris et al. 2019

Encadeamento de serviços de segurança de rede

Gember-Jacobson et al. 2014

OpenNF

Controle
do estado

VNF

Rede



NFV de Segurança para IoT - Para Farris et al. 2019

Encadeamento de serviços de segurança de rede

Gember-Jacobson et al. 2014

Qazi et al. 2013

**SIMPLE (Software-defined
Middlebox PoLicy Enforcement)**

SDN

Middleboxes



NFV de Segurança para IoT - Para Farris et al. 2019

Encadeamento de serviços de segurança de rede

Gember-Jacobson et al. 2014

Qazi et al. 2013

Wang et al. 2021

Aprendizagem por
Reforço Profundo

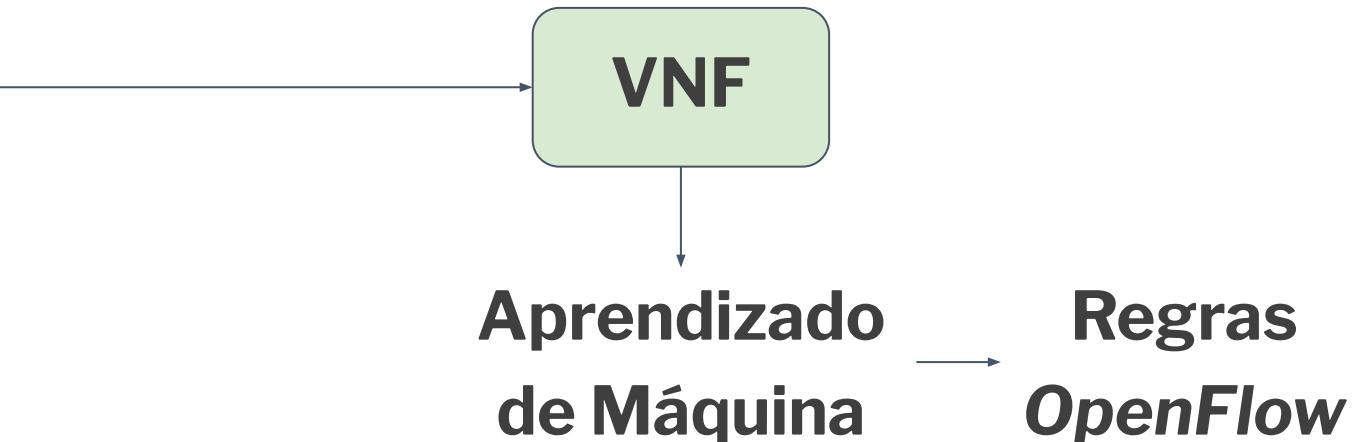
Posicionamento
de SFC



NFV de Segurança para IoT - Para Farris et al. 2019 - Indo Além

VNF para modelos de aprendizado de segurança

Bülbül e Fischer 2020





NFV de Segurança para IoT - Para Farris et al. 2019 - Indo Além

VNF para modelos de aprendizado de segurança

Bülbül e Fischer 2020

Jia et al. 2020

FlowGuard

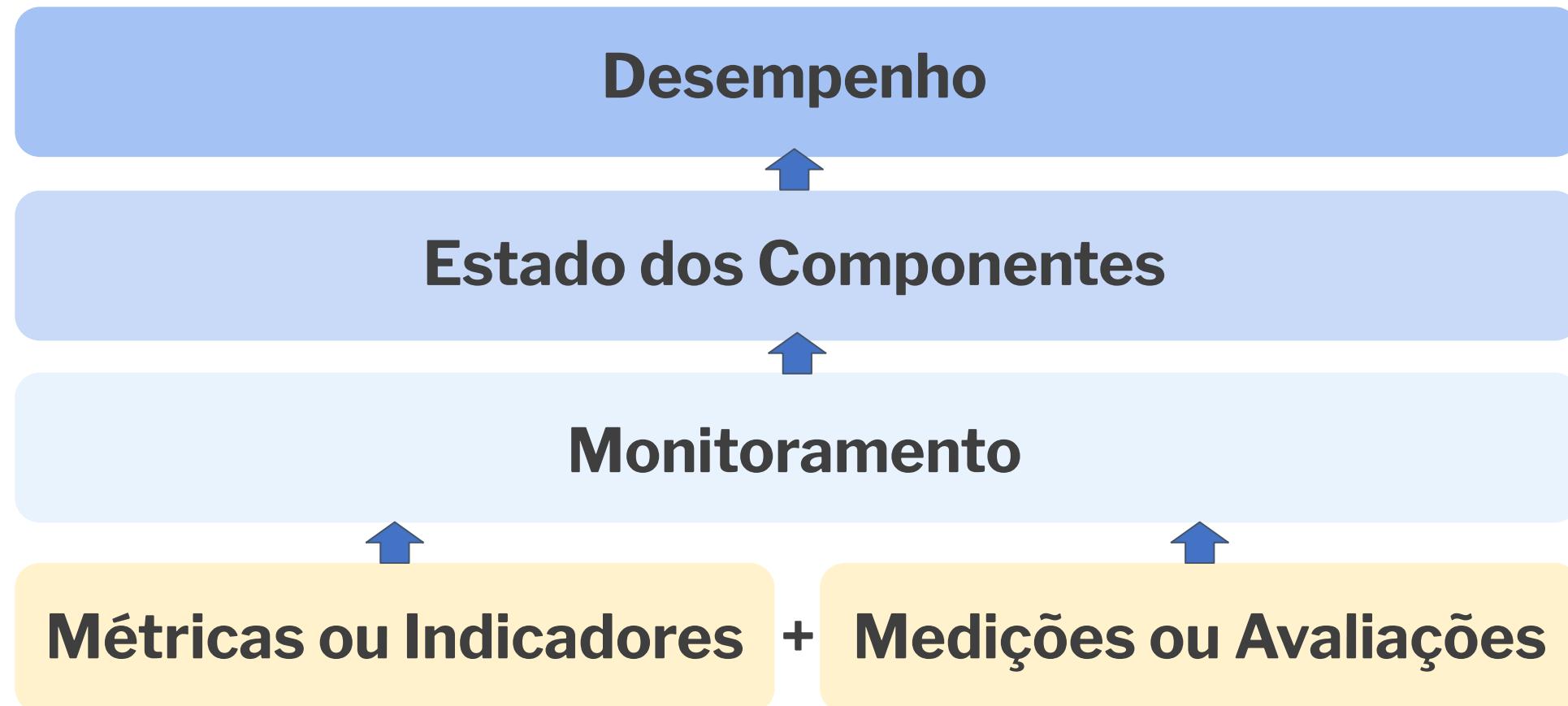
Fluxos

Filtro

Manipulação



NFV de Segurança para IoT - Desempenho





NFV de Segurança para IoT - Desempenho - NFV + IoT

Redes Tradicionais

- Transferência de dados
- Tempo de resposta da rede
- Perda de pacotes
- Uso dos recursos
- Utilização do enlace

Redes IoT

- IoT: tipos de dispositivos e protocolos
- NFV: provisionamento, escalabilidade, conexões de rede e orquestração
- Segurança: ferramentas, algoritmos, tempo de detecção e mitigação de ameaças



Desempenho



Gerenciamento de Desempenho e Segurança em IoT com NFV



Gerenciamento de Desempenho e Segurança em IoT com NFV



MENTORED

Análise da Literatura

Gerenciamento de Desempenho

IoT

Segurança

Indicadores

Dispositivos

Protocolos

Arquitetura

Abordagem

Ataque

Gerenciamento de Desempenho e Segurança em IoT com NFV



MENTORED

Análise da Literatura

IoT

Dispositivos
Protocolos
Arquitetura

Camada	Protocolo
Aplicação	HTTP(S), MQTT, CoAP, AMQP, LLAP, SMCP, DDS, XMPP
Rede	TCP, UDP, UIP, ROLL, RPL, DTLS, Zigbee, Z-Wave, IPV6, 6LoWPAN, LoRaWAN, BLE
Percepção	IEEE 802.15.4, IEEE 802.15.4E, TSMP

Gerenciamento de Desempenho e Segurança em IoT com NFV

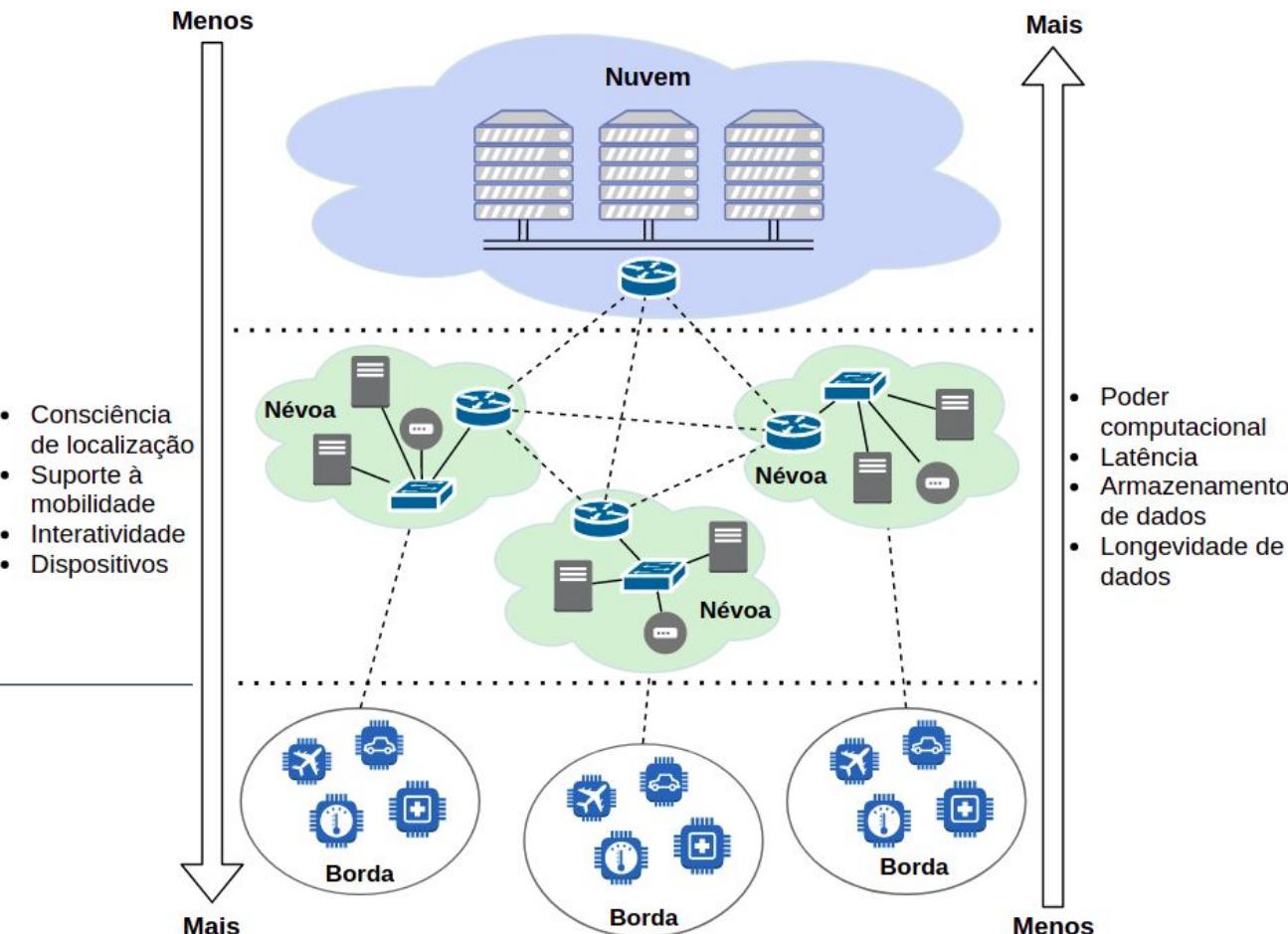


MENTORED

Análise da Literatura

IoT

Dispositivos Protocolos Arquitetura



Gerenciamento de Desempenho e Segurança em IoT com NFV



MENTORED

Análise da Literatura

Segurança

Abordagem

Ataque

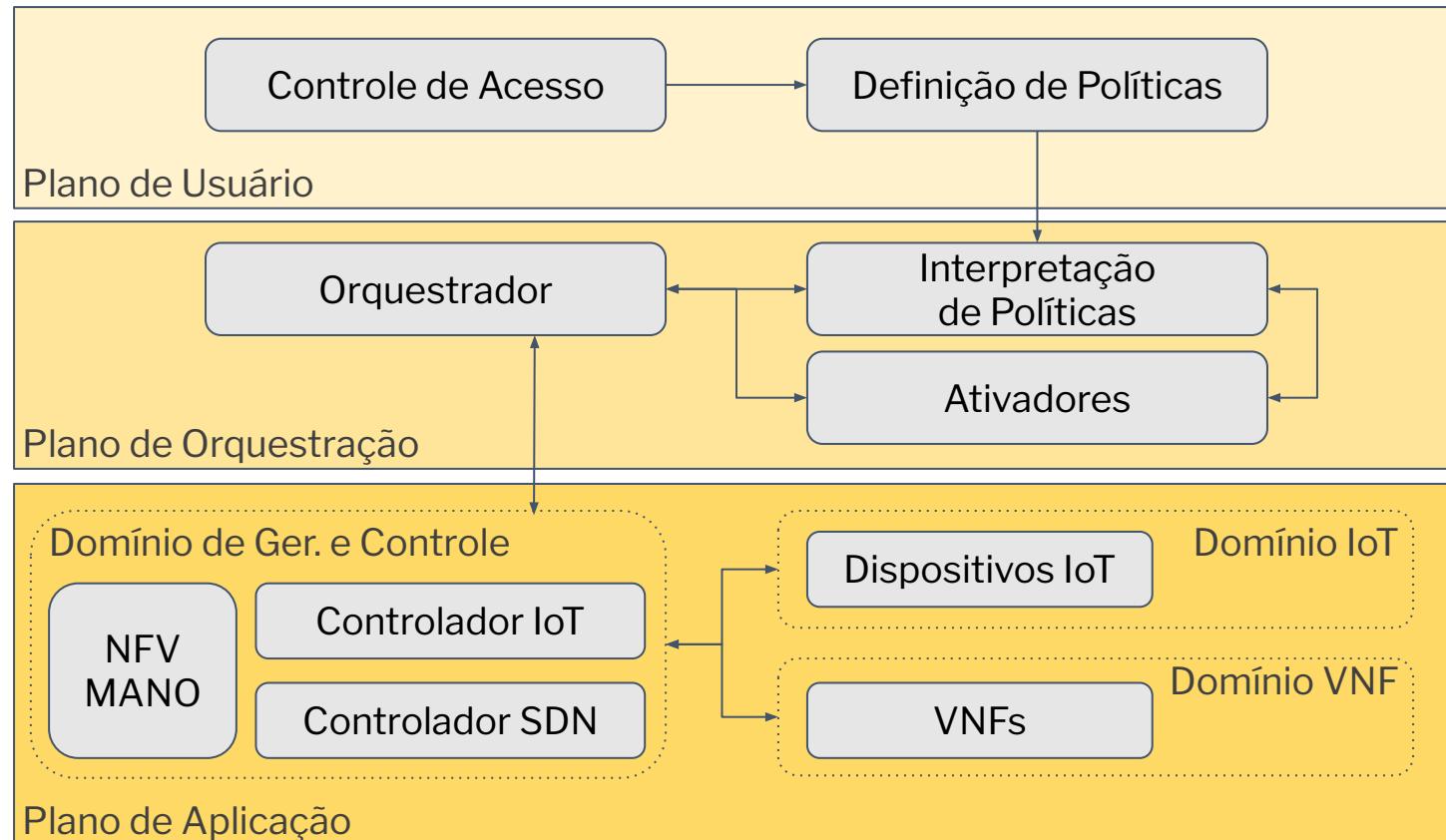
- Prevenção
- Detecção
- Mitigação

Gerenciamento de Desempenho e Segurança em IoT com NFV



MENTORED

Farris et al. 2017 - Towards Provisioning of SDN/NFV-Based Security Enablers for Integrated Protection of IoT Systems



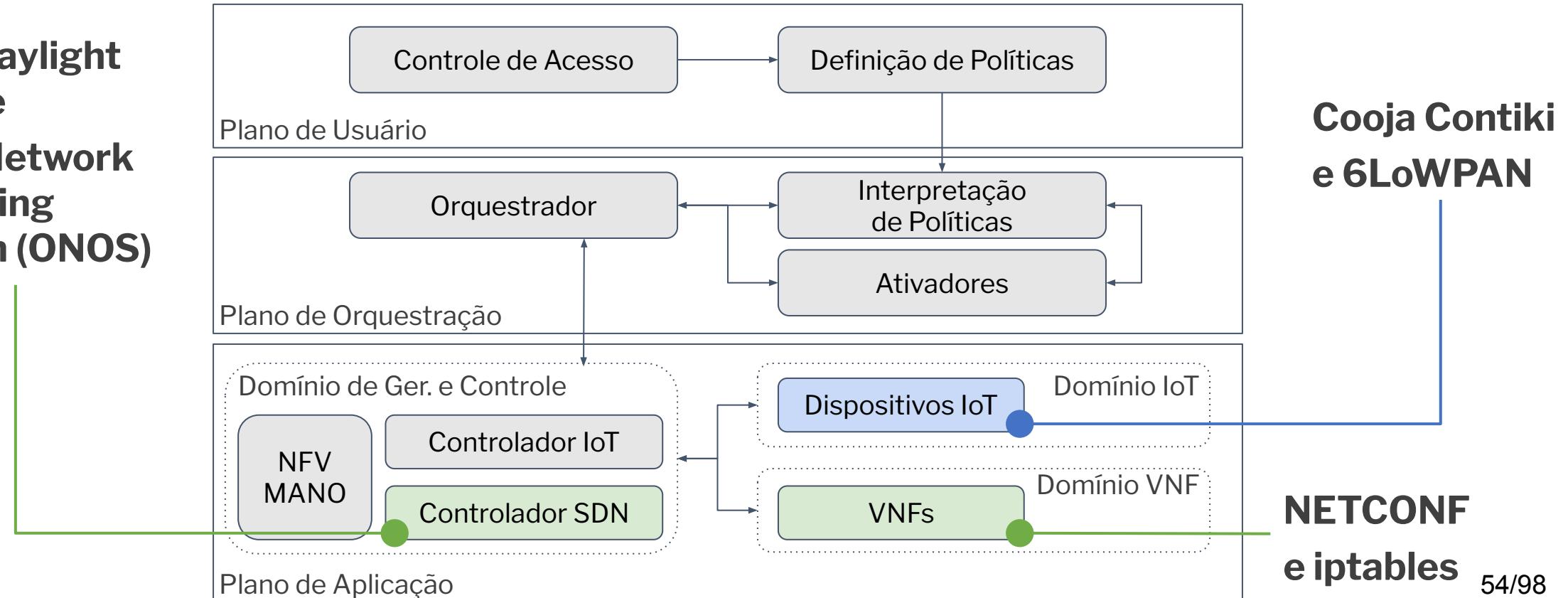
Gerenciamento de Desempenho e Segurança em IoT com NFV



MENTORED

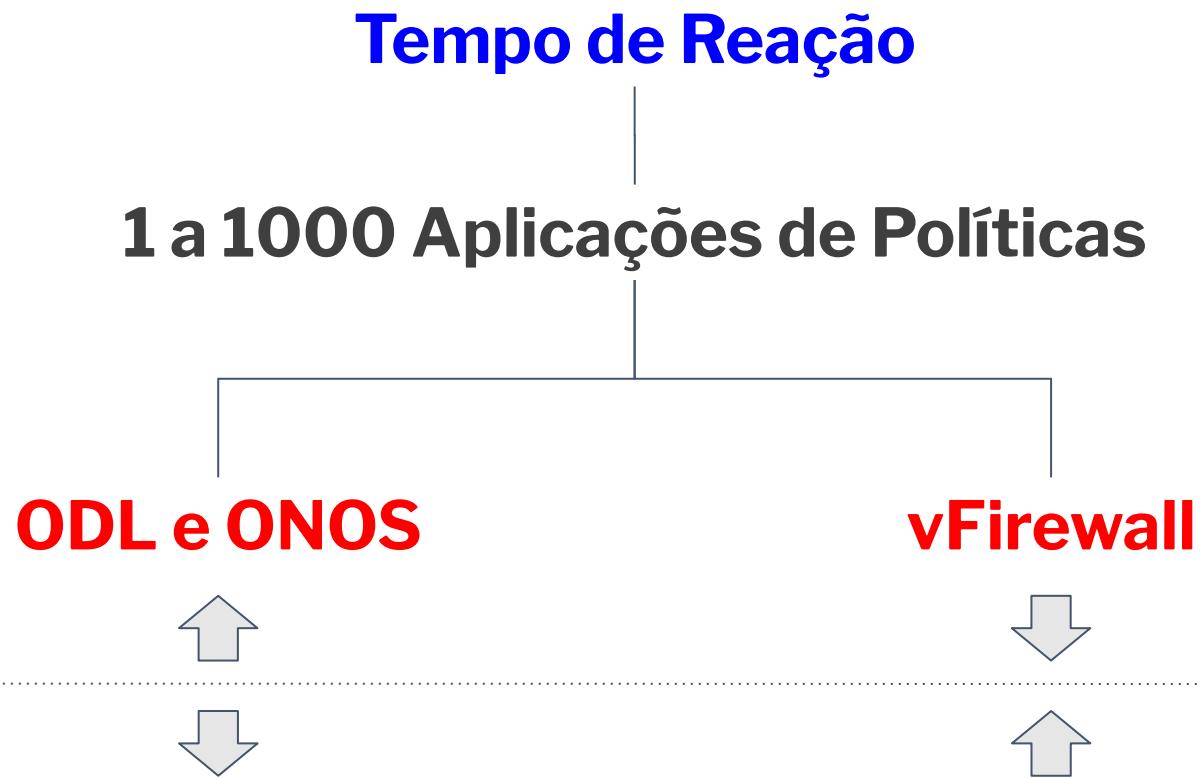
Zarca et al. 2018 - Enhancing IoT Security Through Network Softwarization and Virtual Security Appliances

**OpenDaylight
(ODL) e
Open Network
Operating
System (ONOS)**





Zarca et al. 2018 - Enhancing IoT Security Through Network Softwarization and Virtual Security Appliances

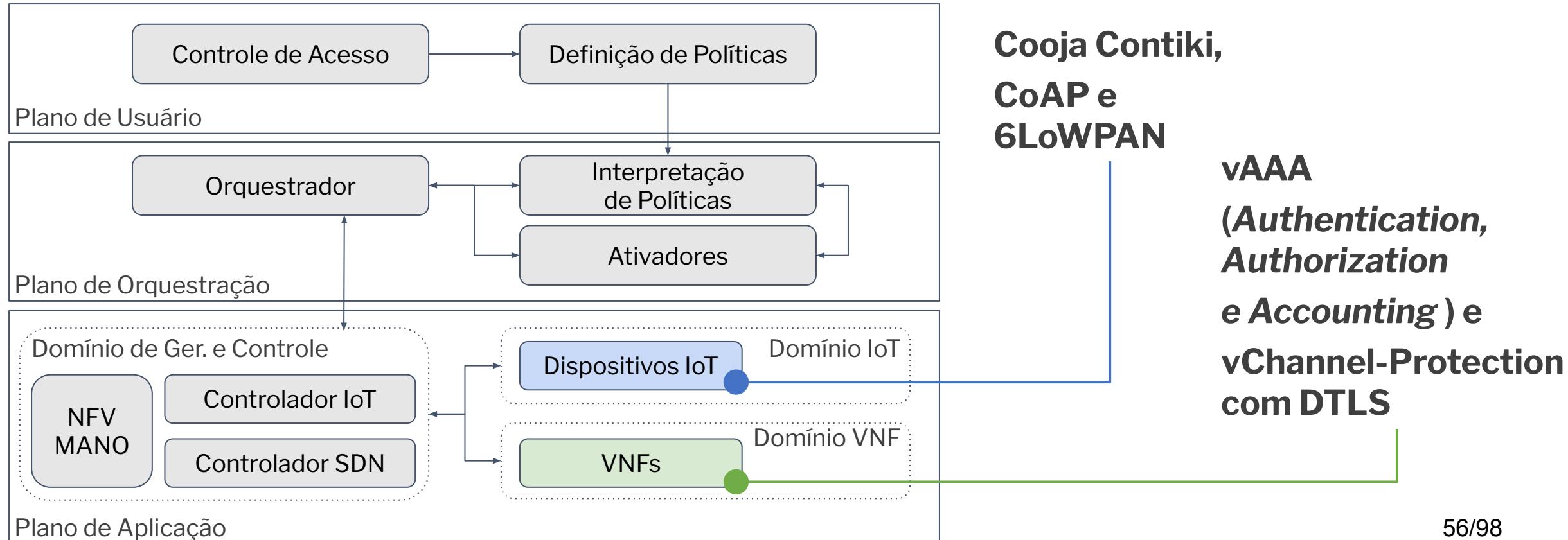


Gerenciamento de Desempenho e Segurança em IoT com NFV



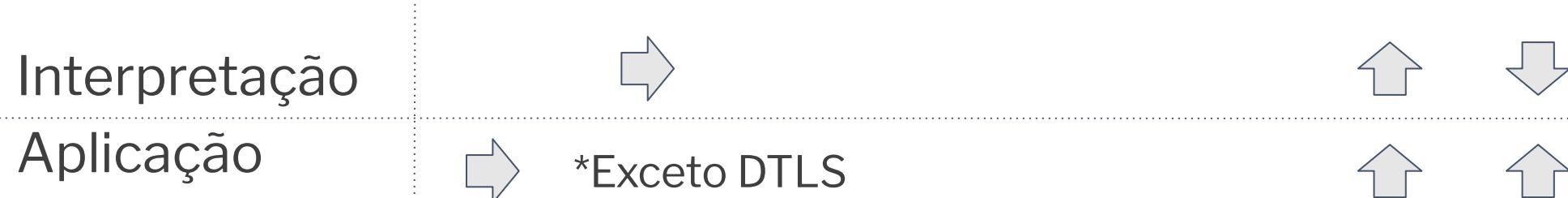
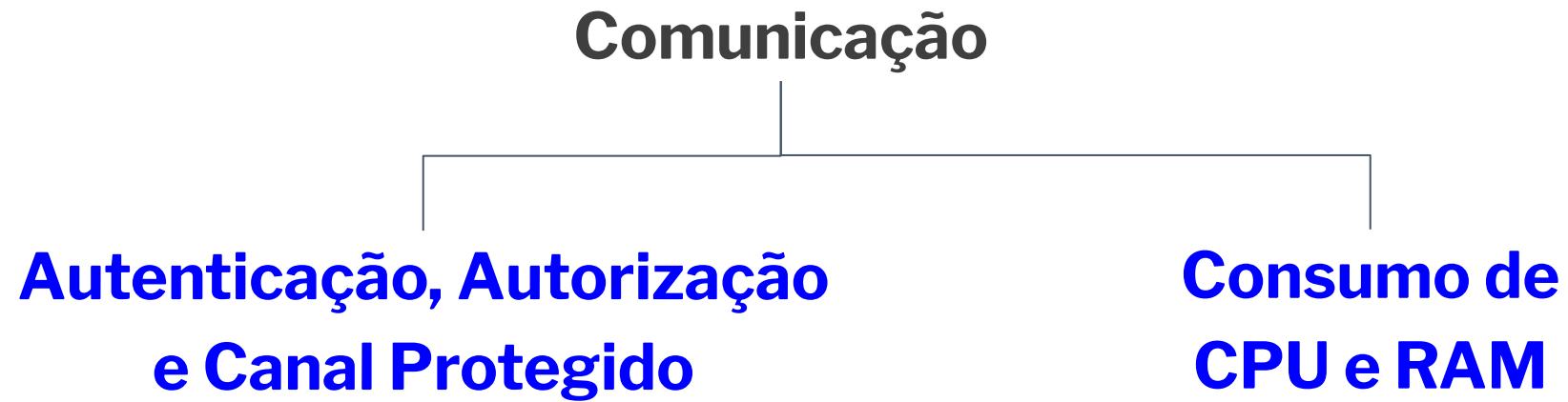
MENTORED

Zarca et al. 2019b - Enabling Virtual AAA Management in SDN-Based IoT Networks





Zarca et al. 2019b - Enabling Virtual AAA Management in SDN-Based IoT Networks

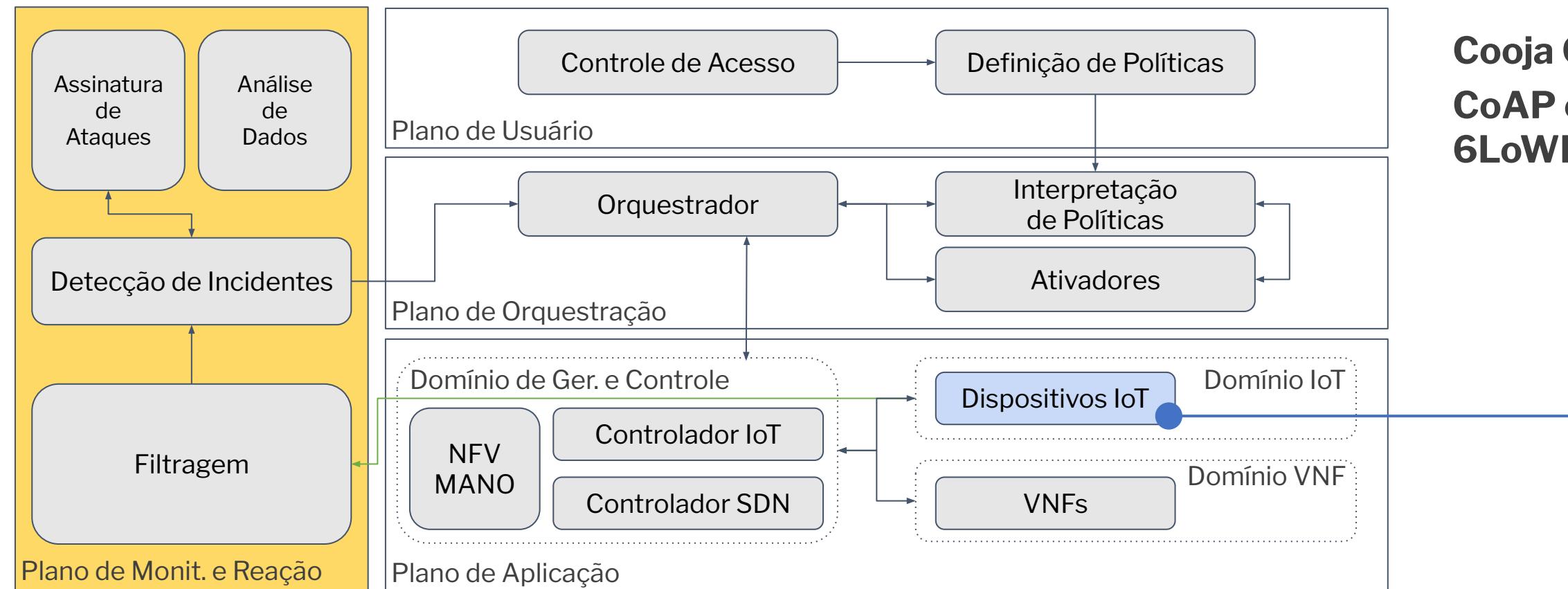


Gerenciamento de Desempenho e Segurança em IoT com NFV



MENTORED

Zarca et al. 2019a - Security Management Architecture for NFV/SDN-Aware IoT Systems



Gerenciamento de Desempenho e Segurança em IoT com NFV



MENTORED

Zarca et al. 2019a - Security Management Architecture for NFV/SDN-Aware IoT Systems

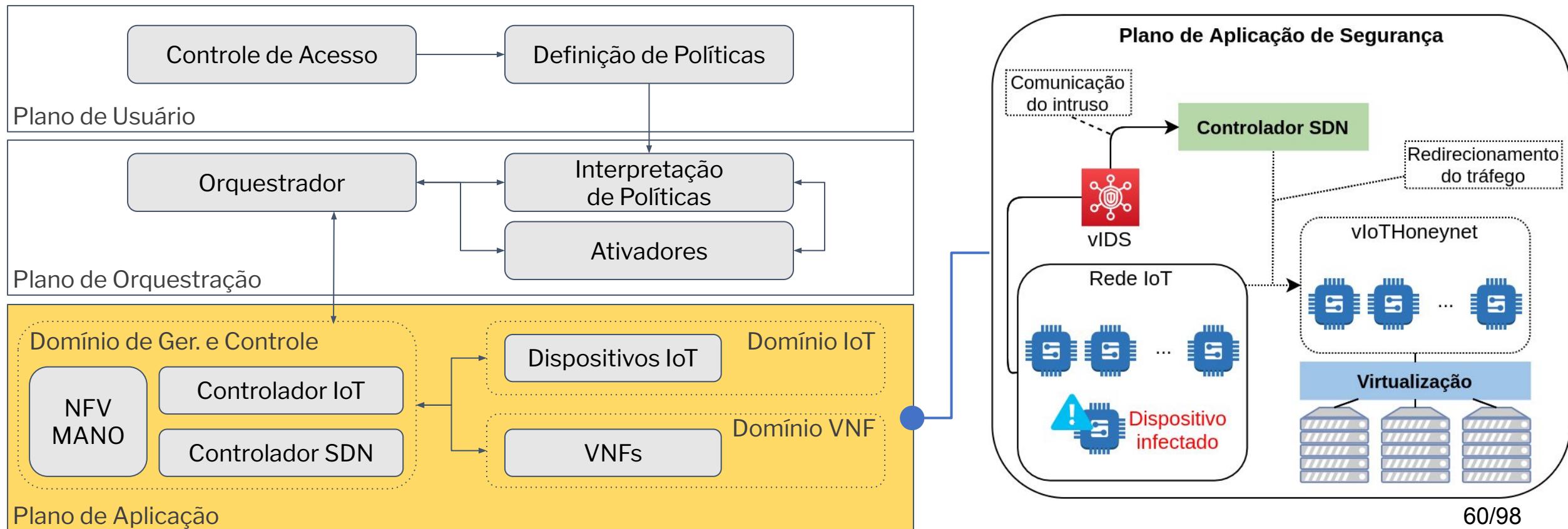


Gerenciamento de Desempenho e Segurança em IoT com NFV



MENTORED

Zarca et al. 2020b - Virtual IoT HoneyNets to Mitigate Cyberattacks in SDN/NFV-Enabled IoT Networks



Gerenciamento de Desempenho e Segurança em IoT com NFV



MENTORED

Zarca et al. 2020b - Virtual IoT HoneyNets to Mitigate Cyberattacks in SDN/NFV-Enabled IoT Networks

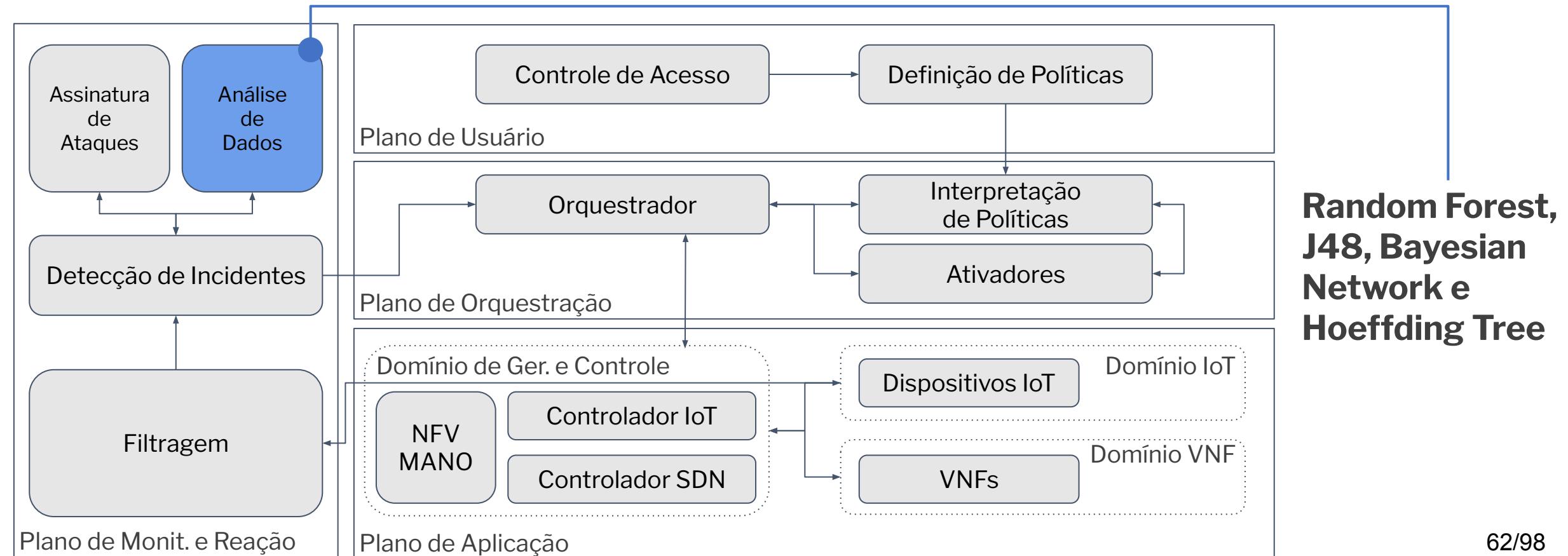
	Tempo de Reação		Consumo de CPU e RAM
	Configuração	Estabelecimento	
20 disp. IoT	15 s	36 s	
50 disp. IoT	45 s	115 s	

Gerenciamento de Desempenho e Segurança em IoT com NFV



MENTORED

Bagaa et al. 2020 - A Machine Learning Security Framework for IoT Systems



Gerenciamento de Desempenho e Segurança em IoT com NFV



MENTORED

Bagaa et al. 2020 - A Machine Learning Security Framework for IoT Systems

Acurácia

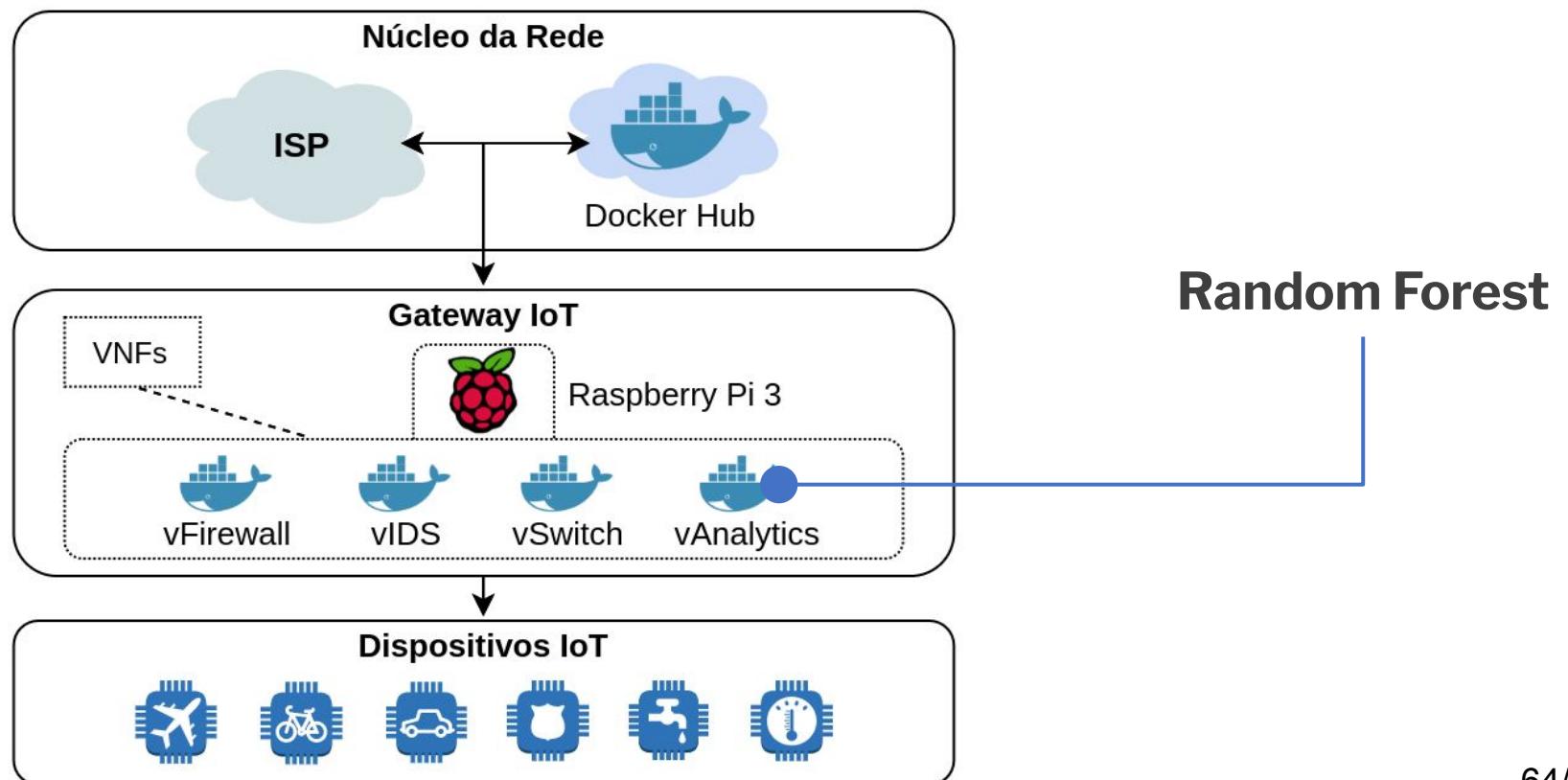
	J48	Byes Net	RandomForest	Hoeffding Tree
DoS	99.9%	99.9%	100%	99.3%
U2R	70.0%	4.8%	82.1%	11.5%
U2L	97.5%	62.7%	99.3%	35.2%
Probe	99.4%	84.2%	99.9%	98.1%
Normal	99.8%	97.3%	99.9%	95.2%
Time(s)	35.35	6.97	74.94	5.1
Precision	99.8%	96.7%	99.9%	96.4%
FPR	0.2%	1.8%	0.1%	3.3%
Detection Rate	99.8%	95.7%	99.9%	96.8%

Gerenciamento de Desempenho e Segurança em IoT com NFV



MENTORED

Sairam et al. 2019 - NETRA: Enhancing IoT Security Using NFV-Based Edge Traffic Analysis



Gerenciamento de Desempenho e Segurança em IoT com NFV



MENTORED

Sairam et al. 2019 - NETRA: Enhancing IoT Security Using NFV-Based Edge Traffic Analysis

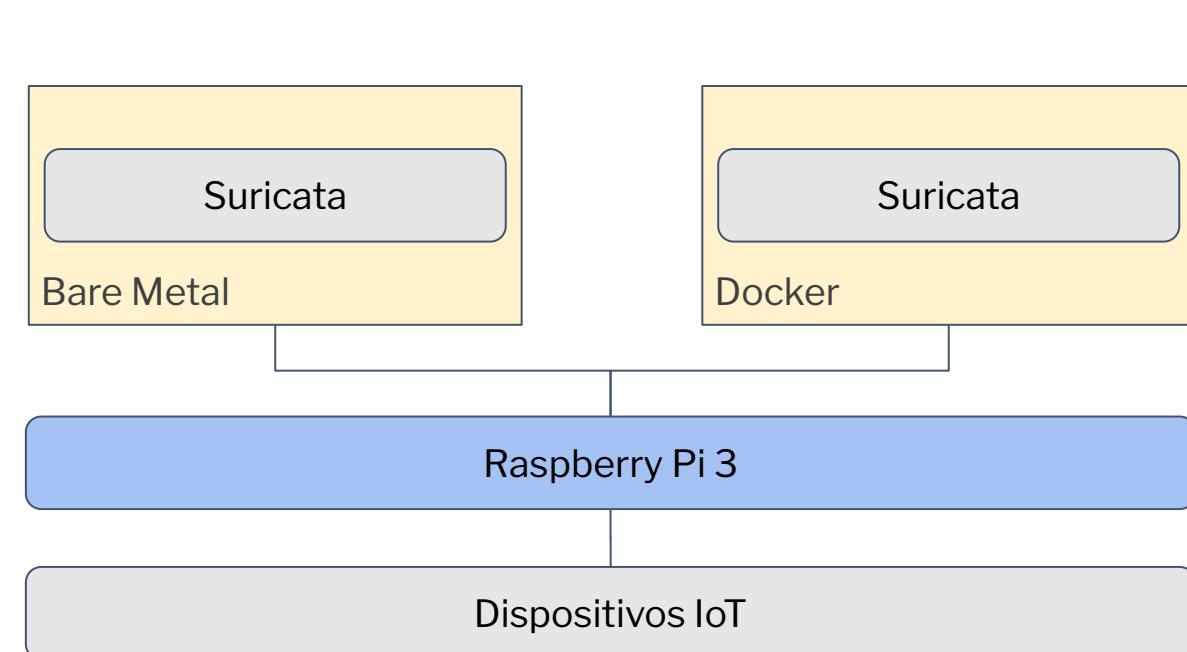
	Máquina Virtual	Container
Armazenamento	72 GB	465 MB
RAM	140 MB	110 MB
Latência	0,83 ms	0,53 ms
Escalabilidade	20 min + 5 min	4 min + 9 s ou <1 s
DDoS	Acurácia	94,4% e <1 s

Gerenciamento de Desempenho e Segurança em IoT com NFV



MENTORED

Boudi et al. 2019 - Assessing Lightweight Virtualization for Security-as-a-Service at the Network Edge



Comparação

N. Pacotes
Processados, Taxa
de Transferência,
Consumo de CPU e
RAM

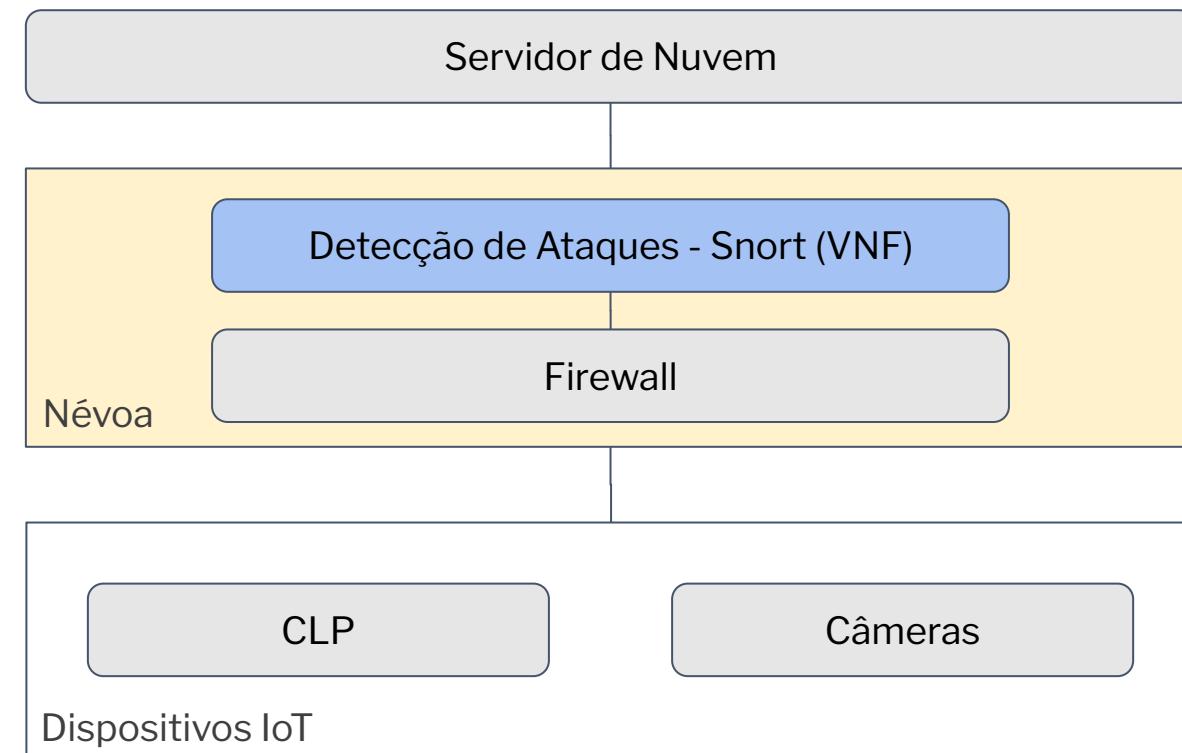
CPU
Docker (10%) < BM

Gerenciamento de Desempenho e Segurança em IoT com NFV



MENTORED

Zhou et al. 2019 - A Fog Computing Based Approach to DDoS Mitigation in IIoT Systems



Comparação

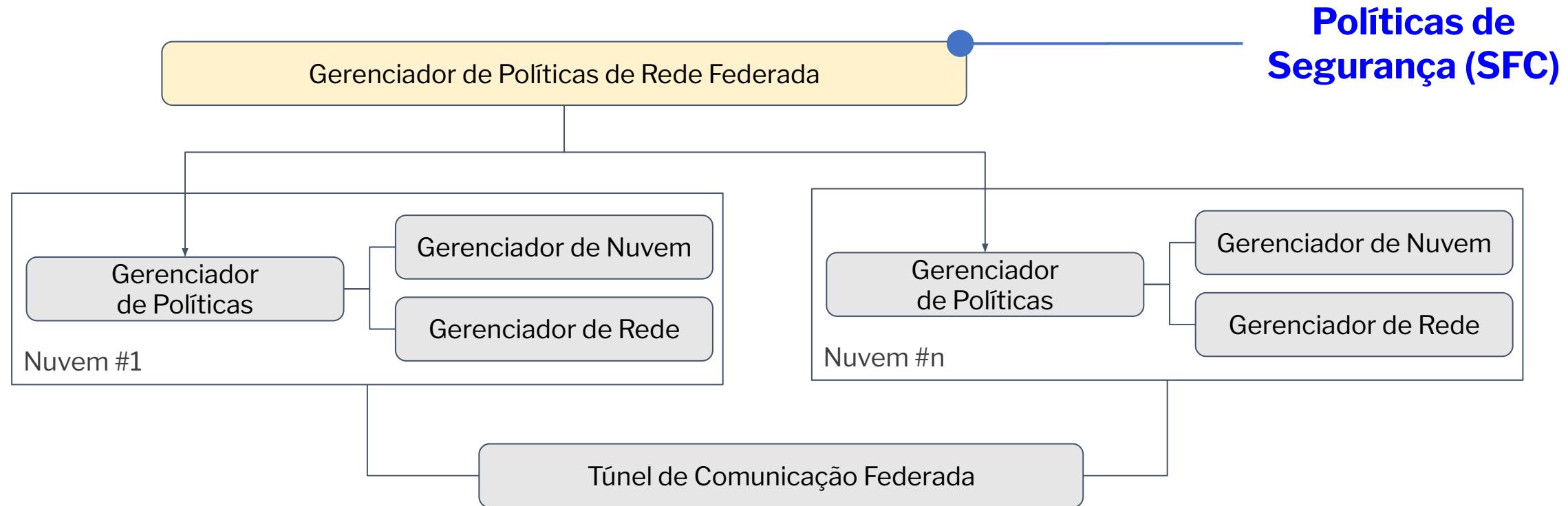
Local	Névoa
240 ms	137 ms
84,95% ms	93,93% ms

Gerenciamento de Desempenho e Segurança em IoT com NFV



MENTORED

Massonet et al. 2017 - Security in Lightweight Network Function Virtualisation for Federated Cloud and IoT

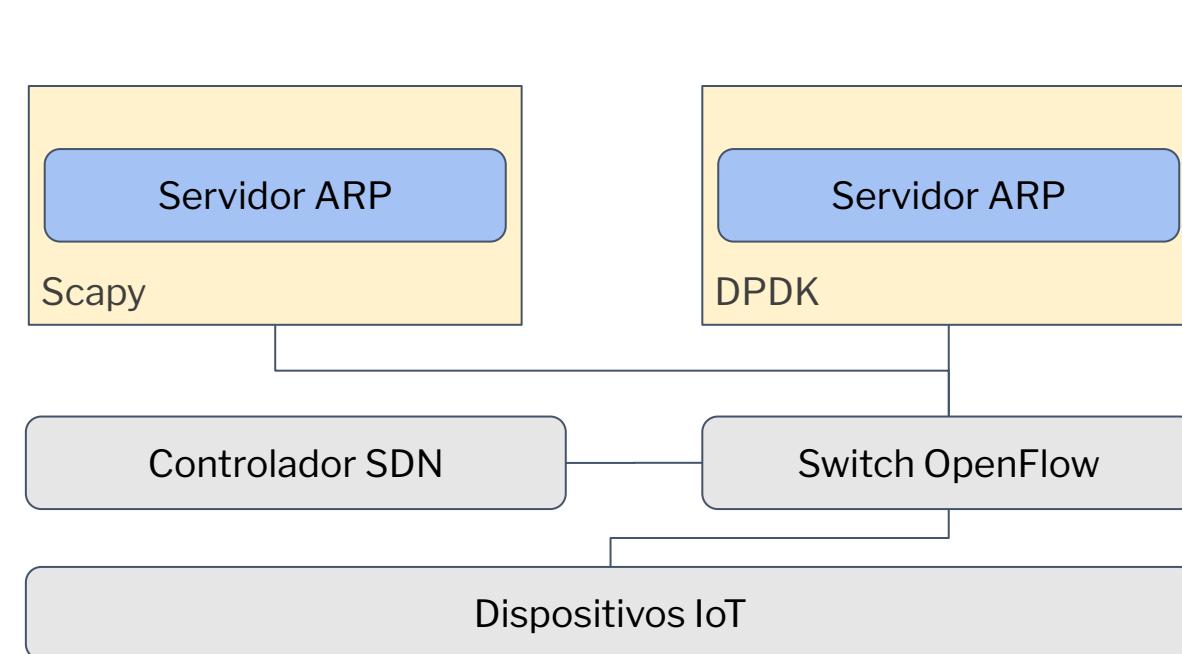


Gerenciamento de Desempenho e Segurança em IoT com NFV



MENTORED

**AI-Shaboti et al. 2018 - Towards Secure Smart Home IoT:
Manufacturer and User Network Access Control Framework**



Comparação

Scapy

85 ms

DPDK

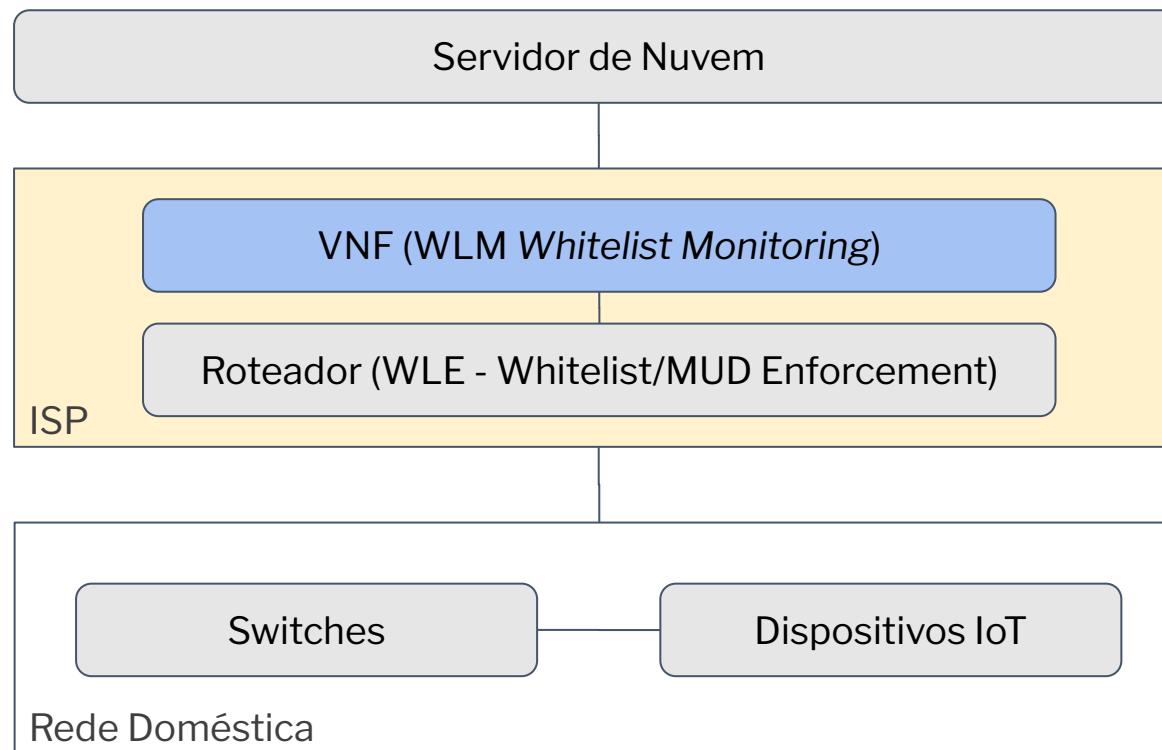
0,57 ms

Gerenciamento de Desempenho e Segurança em IoT com NFV



MENTORED

Afek et al. 2020 - NFV-Based IoT Security for Home Networks using MUD

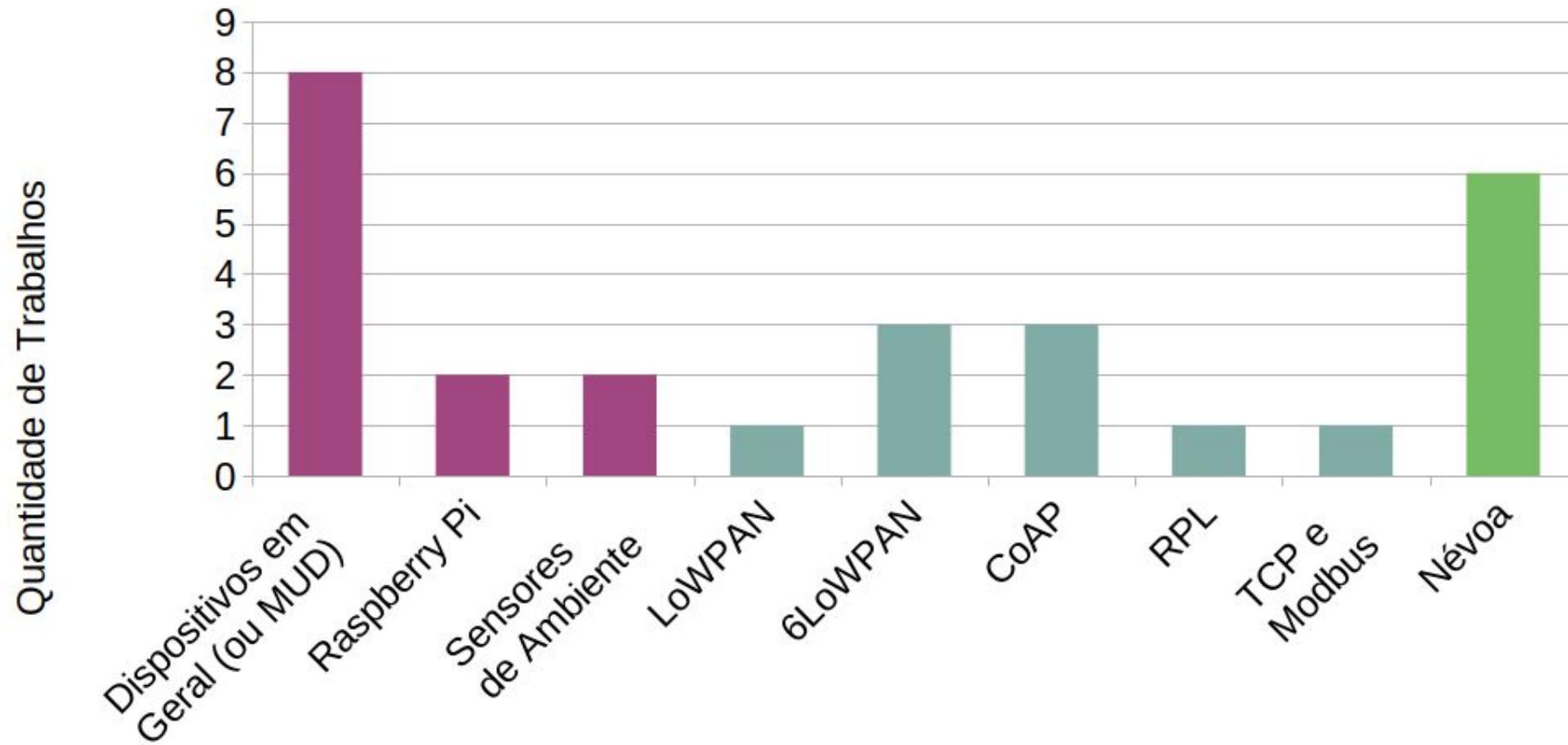


Gerenciamento de Desempenho e Segurança em IoT com NFV



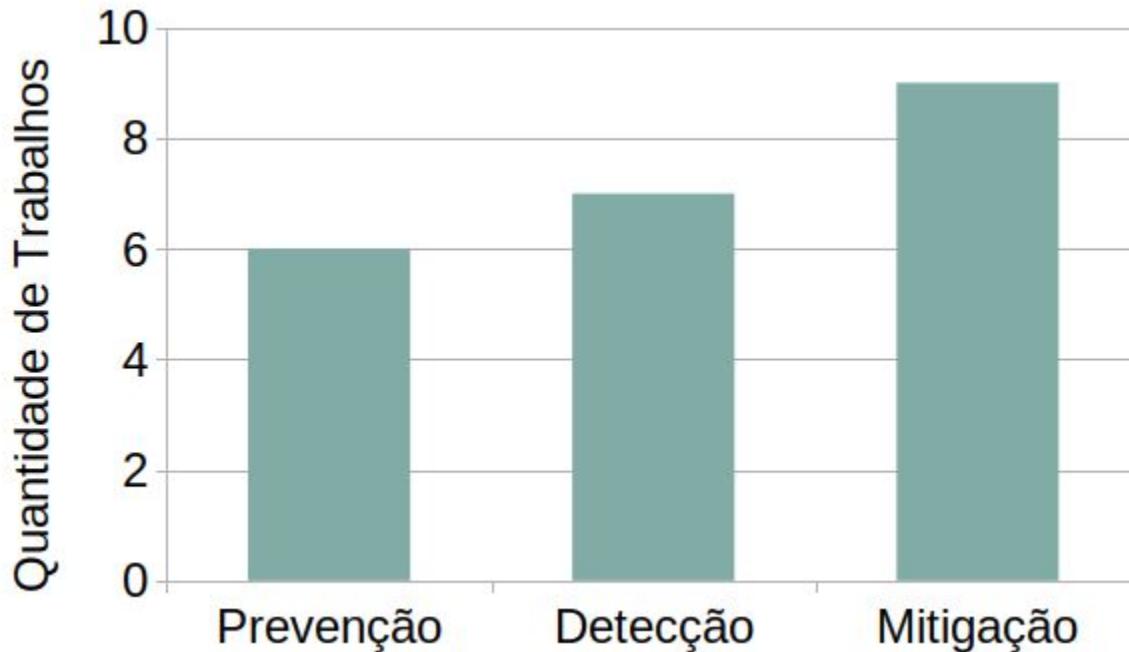
MENTORED

Panorama - IoT - Dispositivos, Protocolos e Arquitetura





Panorama - Segurança - Abordagem e Ataque

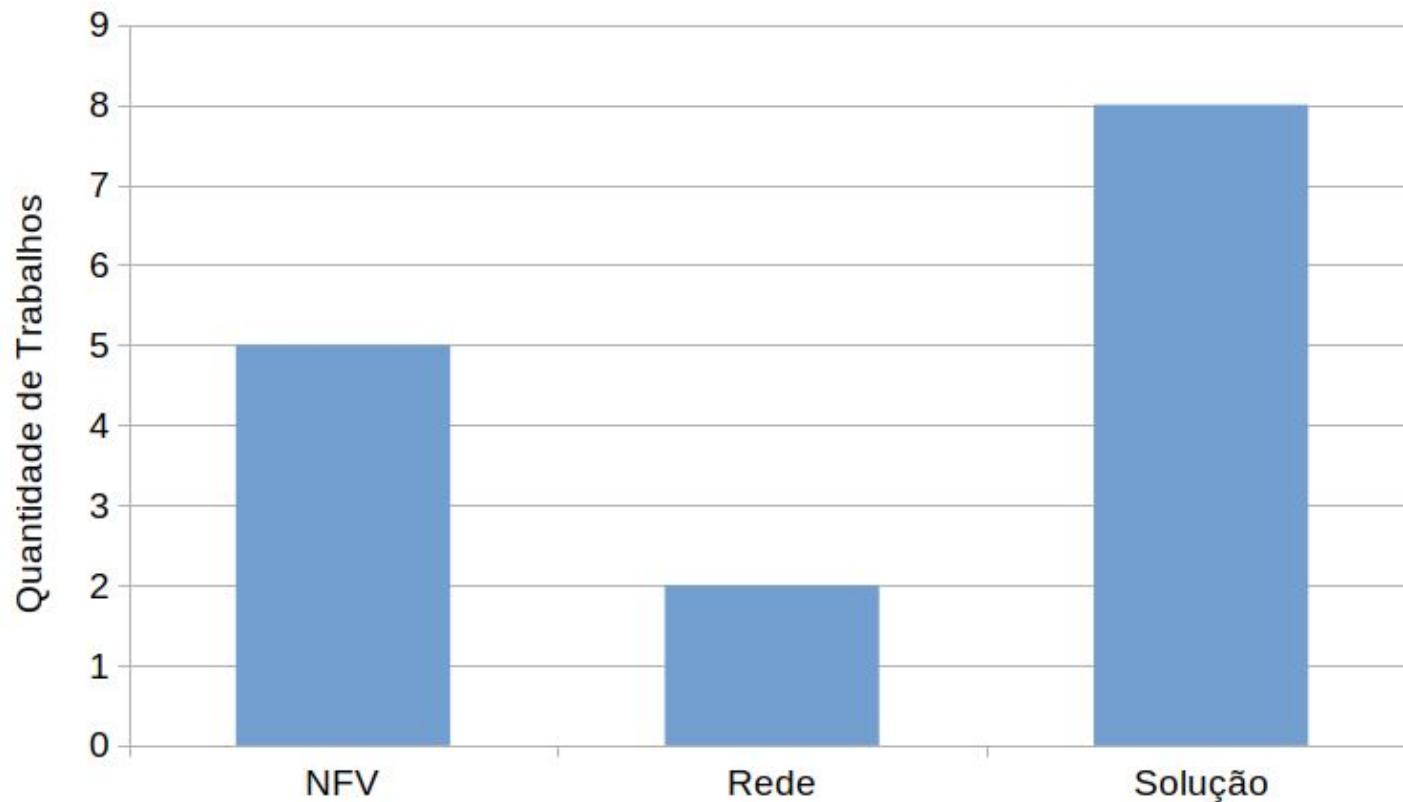


Gerenciamento de Desempenho e Segurança em IoT com NFV



MENTORED

Panorama - Gerenciamento de Desempenho - Indicadores





Estudo de Caso: MENTORED Testbed

<https://github.com/ccsc-research/sbcc2021-minicurso-nfv-iot-security>

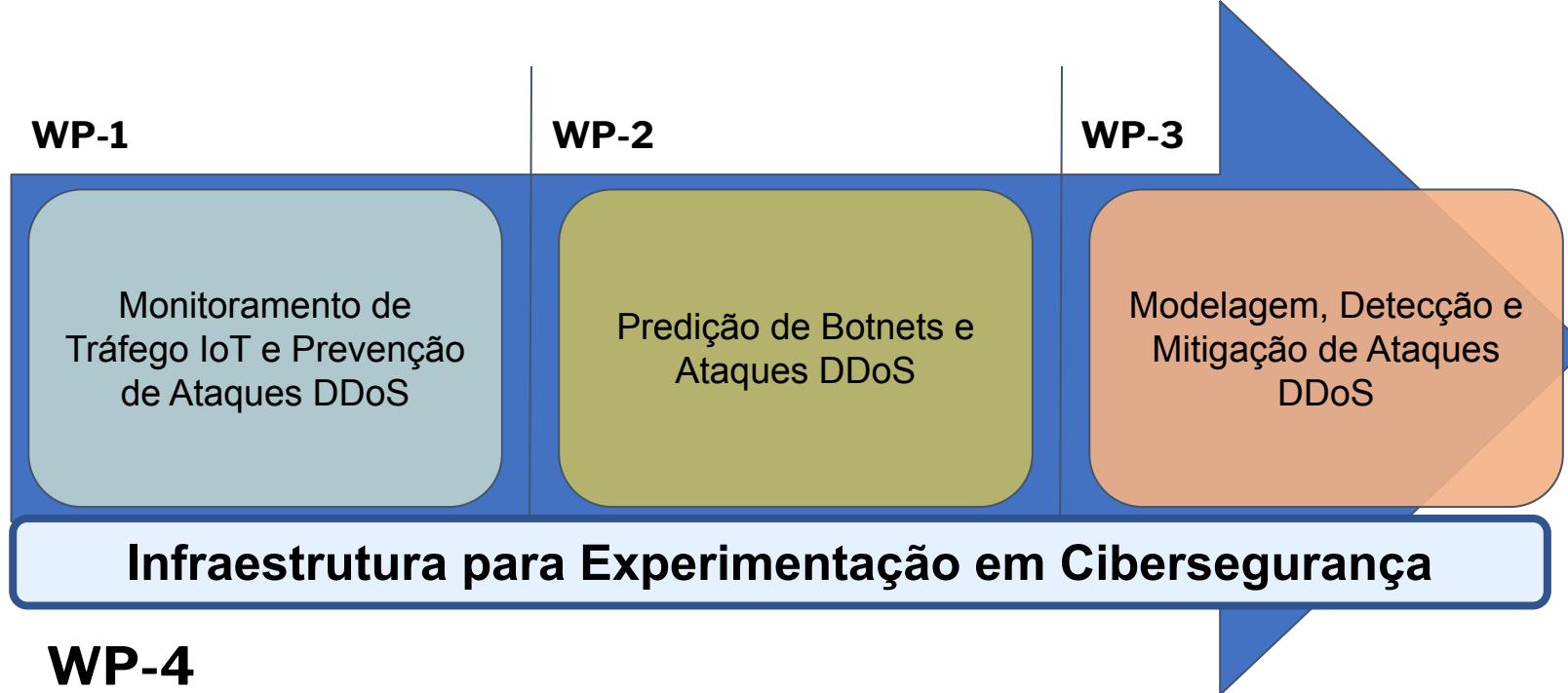


Projeto MENTORED

Visão Geral



MENTORED



Pacote de Trabalho 4 (WP4)

Objetivos Específicos



MENTORED



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)

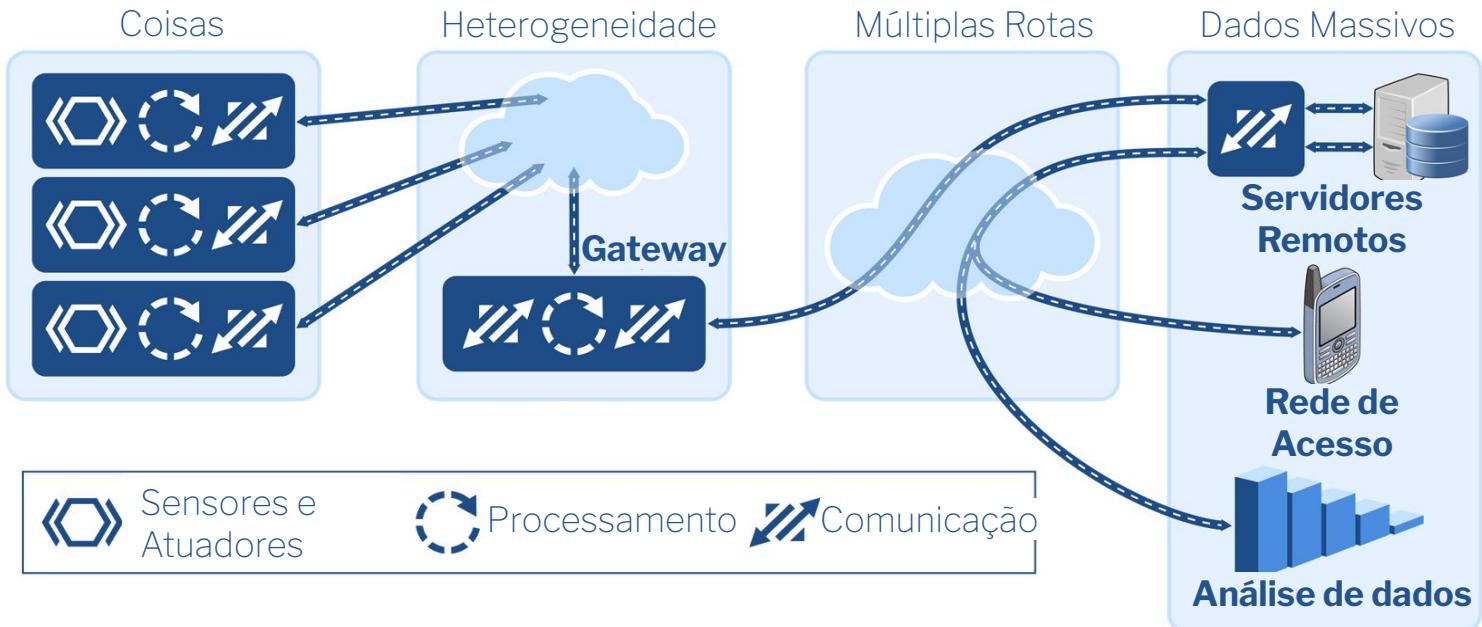
Pacote de Trabalho 4 (WP4)

Requisitos - Testbed Cibersegurança



MENTORED

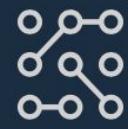
- Fidelidade
- Validade
- Escalabilidade
- Segurança
- Reprodutibilidade
- Flexibilidade
- Transparência
- Acesso em tempo real
- Perspectiva centrada no usuário



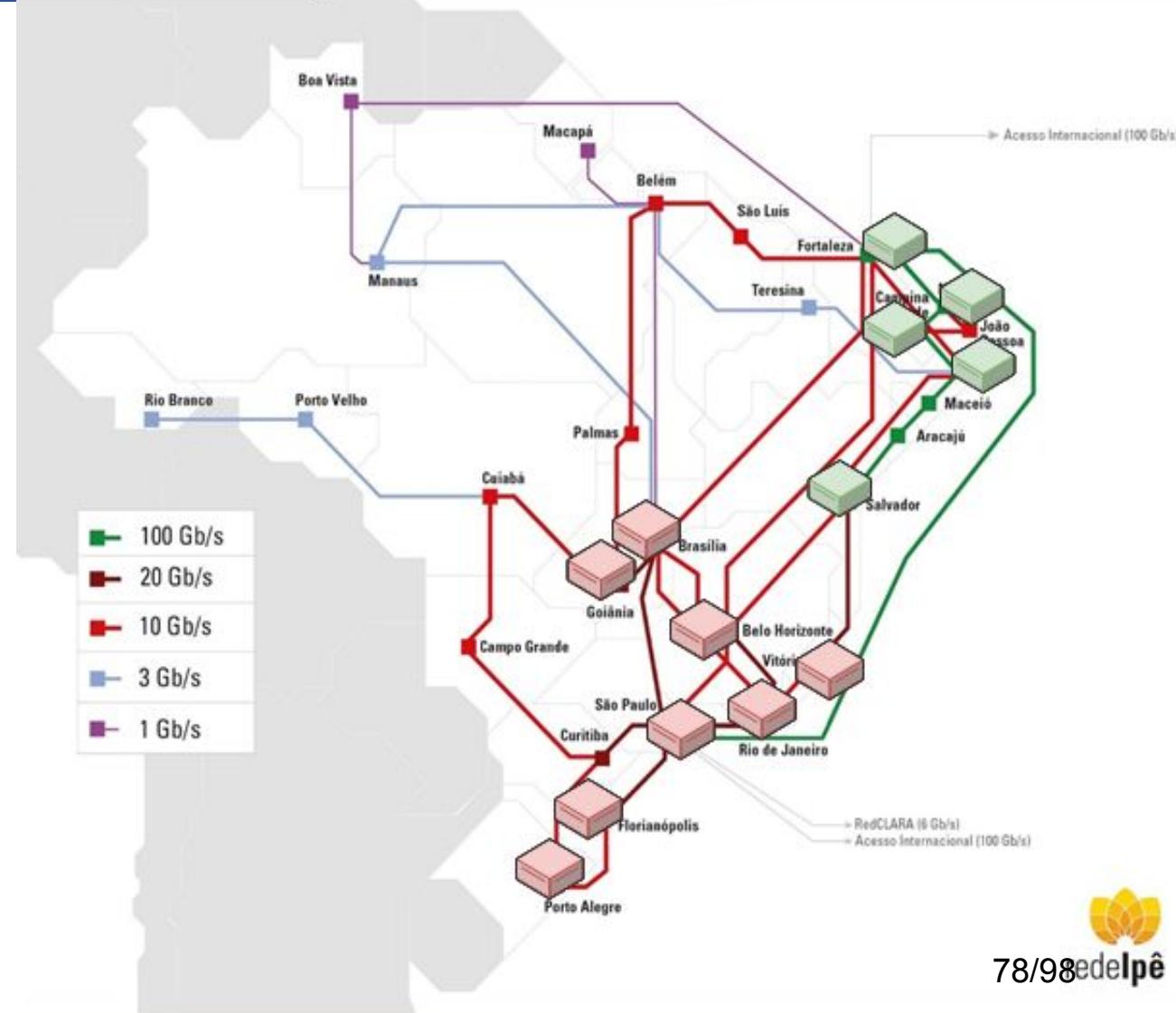
Infraestrutura Definida por Software (IDS-RNP)

Vantagens

- Processamento e armazenamento
- Rede customizável e de longa distância
- Configurações sob-demanda
- Suporte a redes de borda
- Software livre
- Equipe de apoio da RNP
- **Mecanismos para Experimentação**



MENTORED



kubernetes

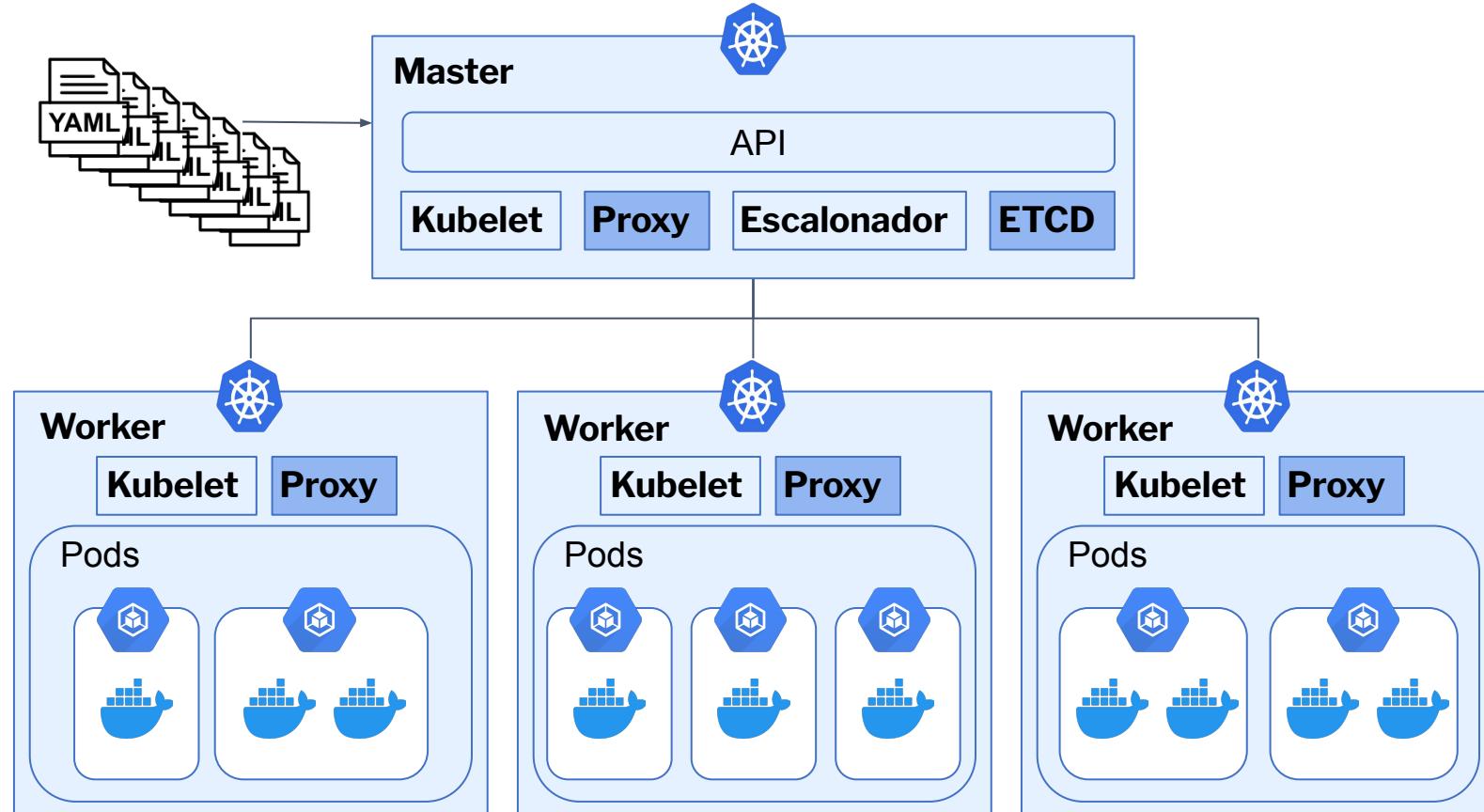


Infraestrutura Definida por Software (IDS-RNP)

Kubernetes



MENTORED

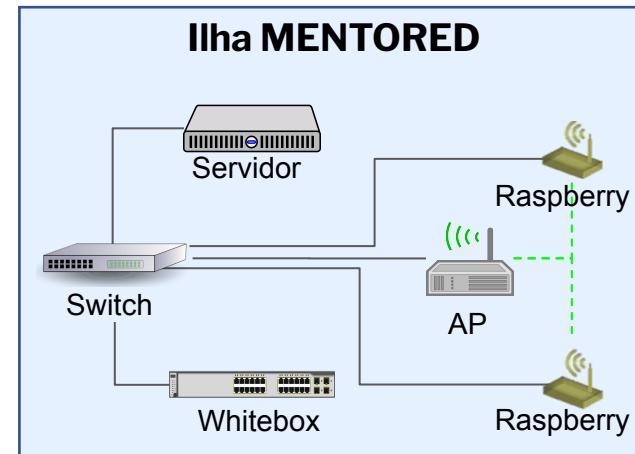
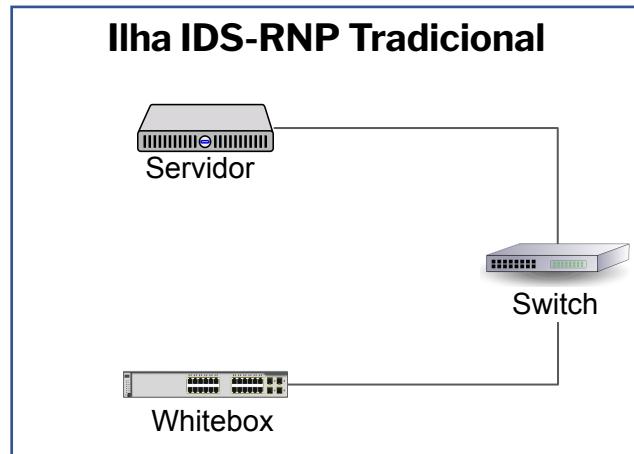


MENTORED Testbed

Ilhas de Recursos Computacionais



MENTORED



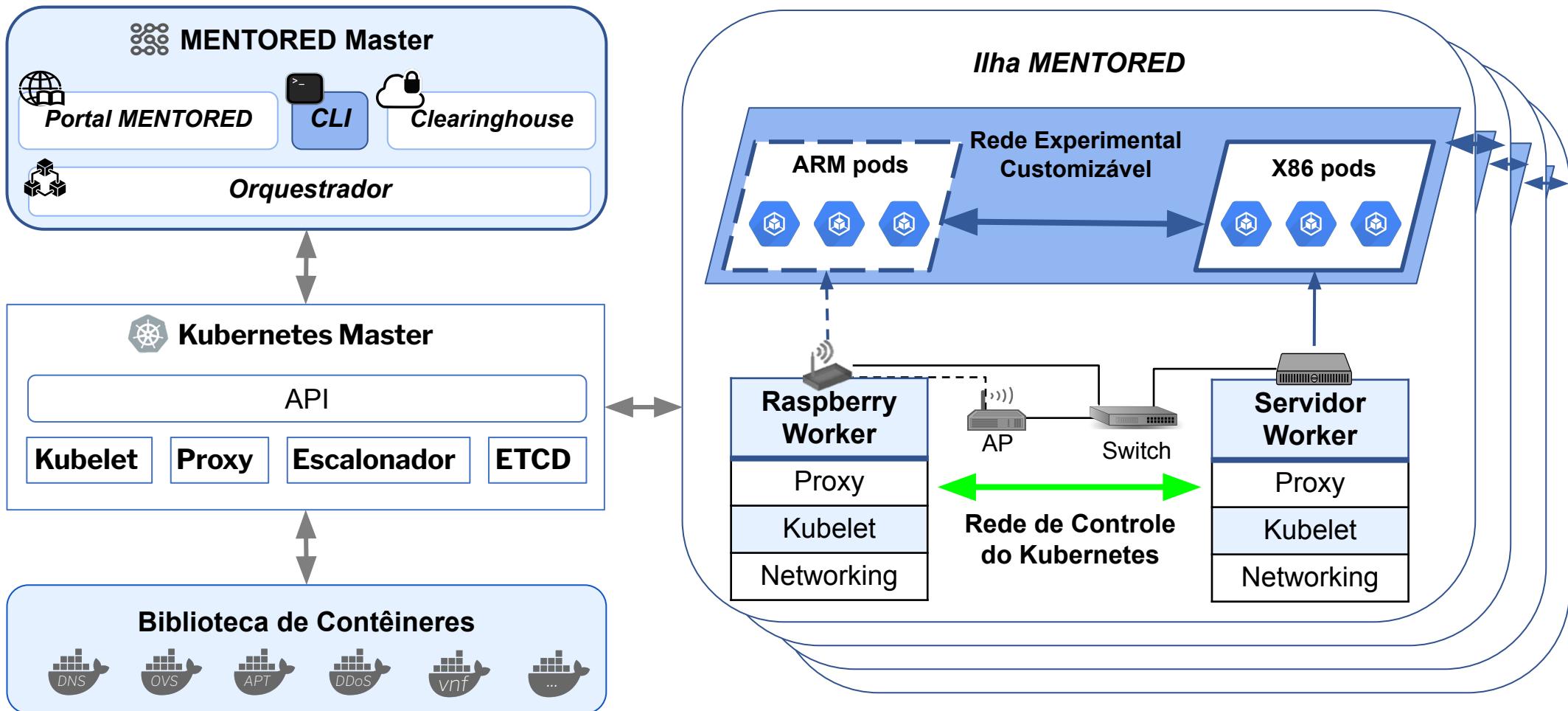
- Rede local com/sem fio
- Sensores e módulos USB/shields
- Escalabilidade
- Reproduzir firmwares e vulnerabilidades de dispositivos ARM

MENTORED Testbed

Arquitetura



MENTORED

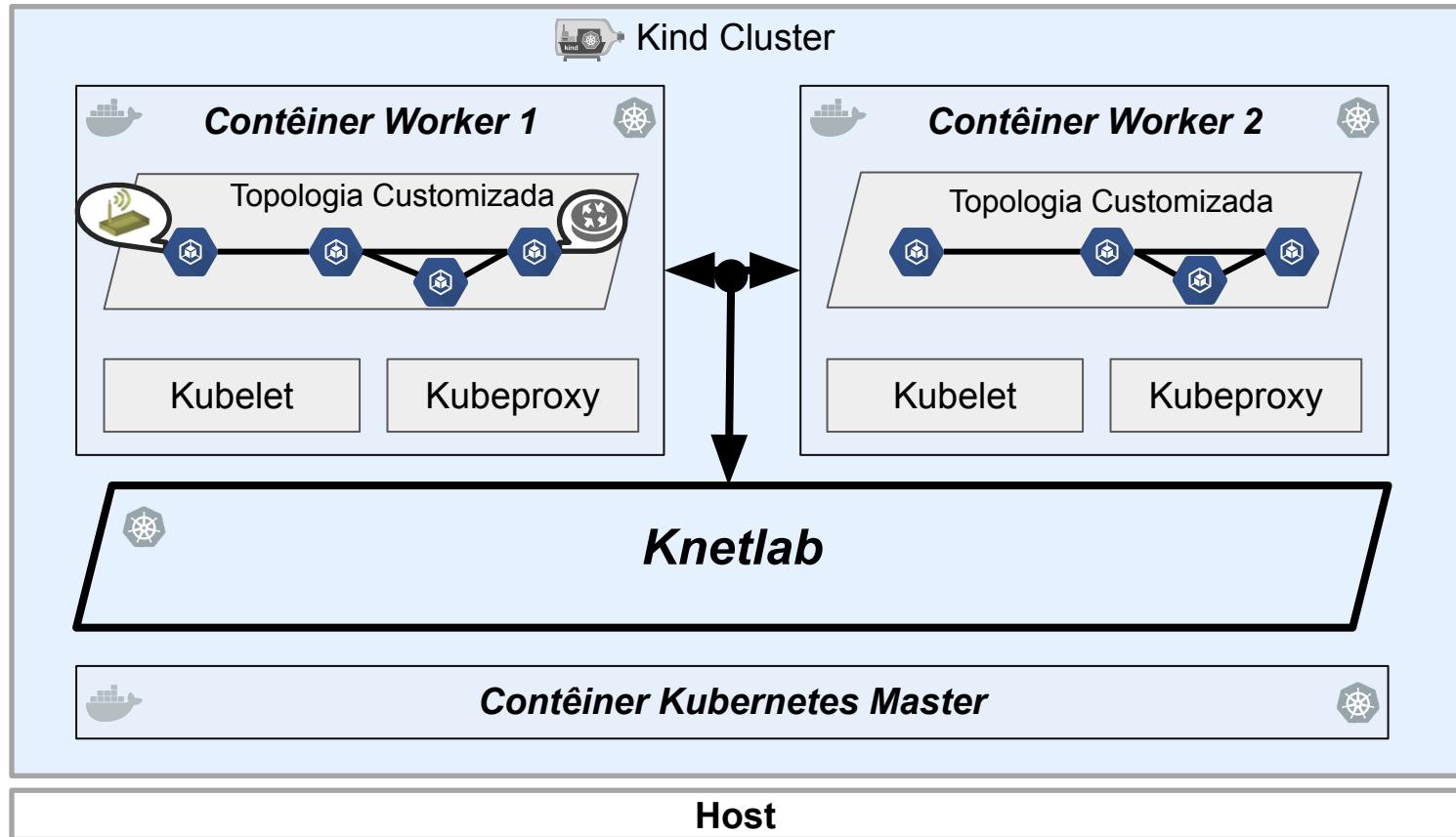


Cenário de Rede

Knetlab



MENTORED

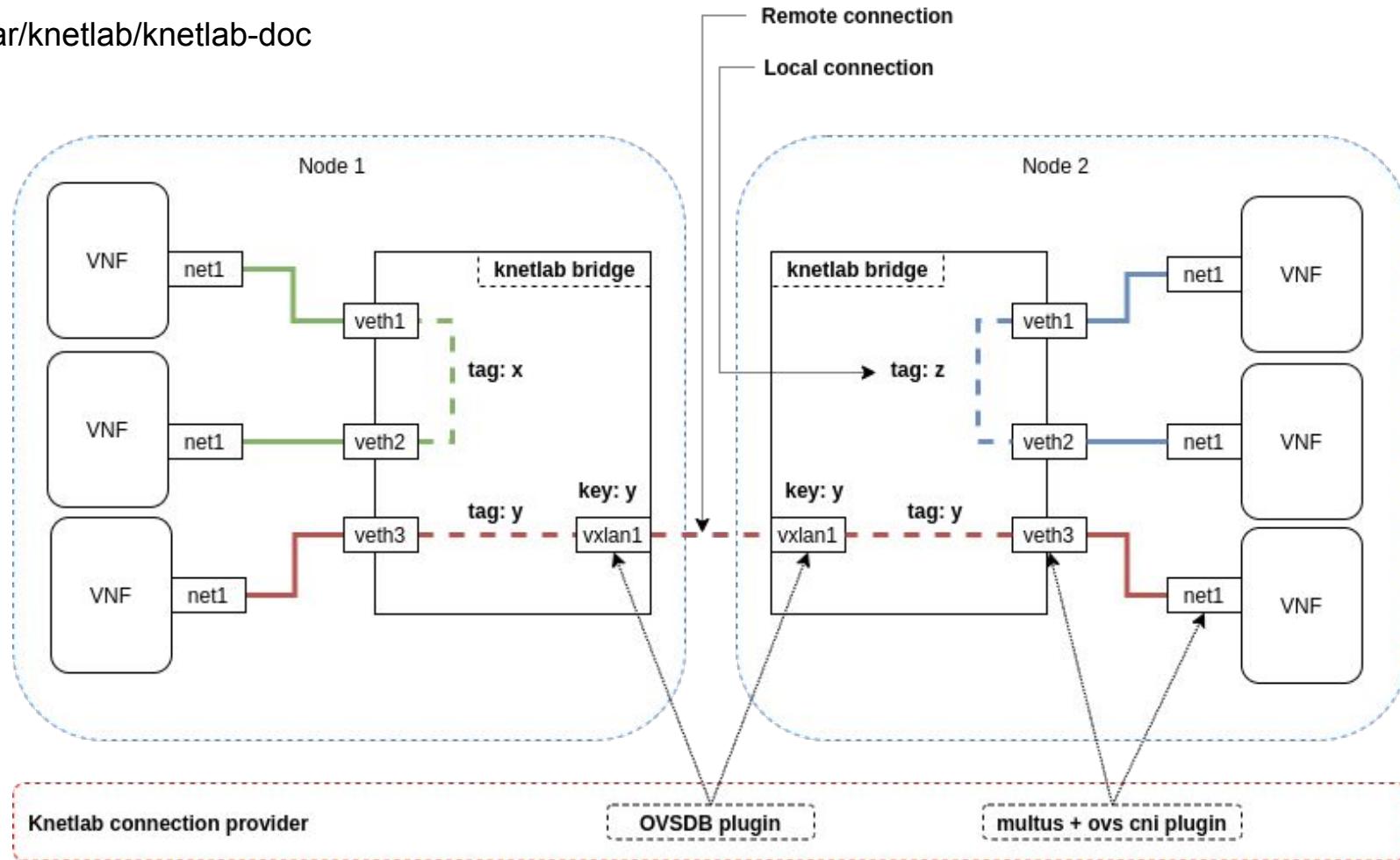


Cenário de Rede **Knetlab**



MENTORED

<https://git.rnp.br/cnar/knetlab/knetlab-doc>

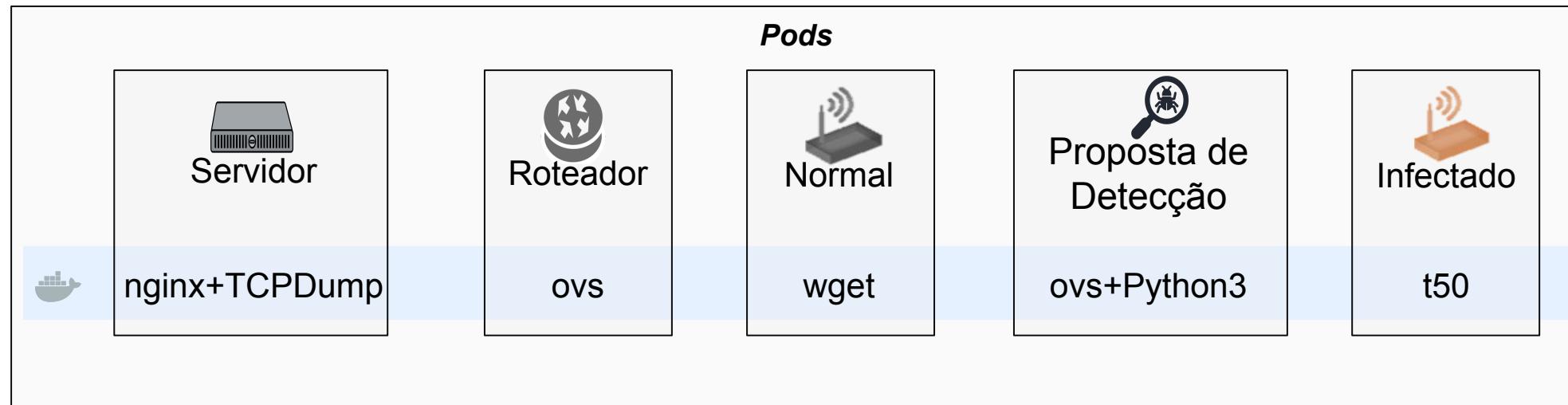


Cenário de Rede

Agentes



MENTORED

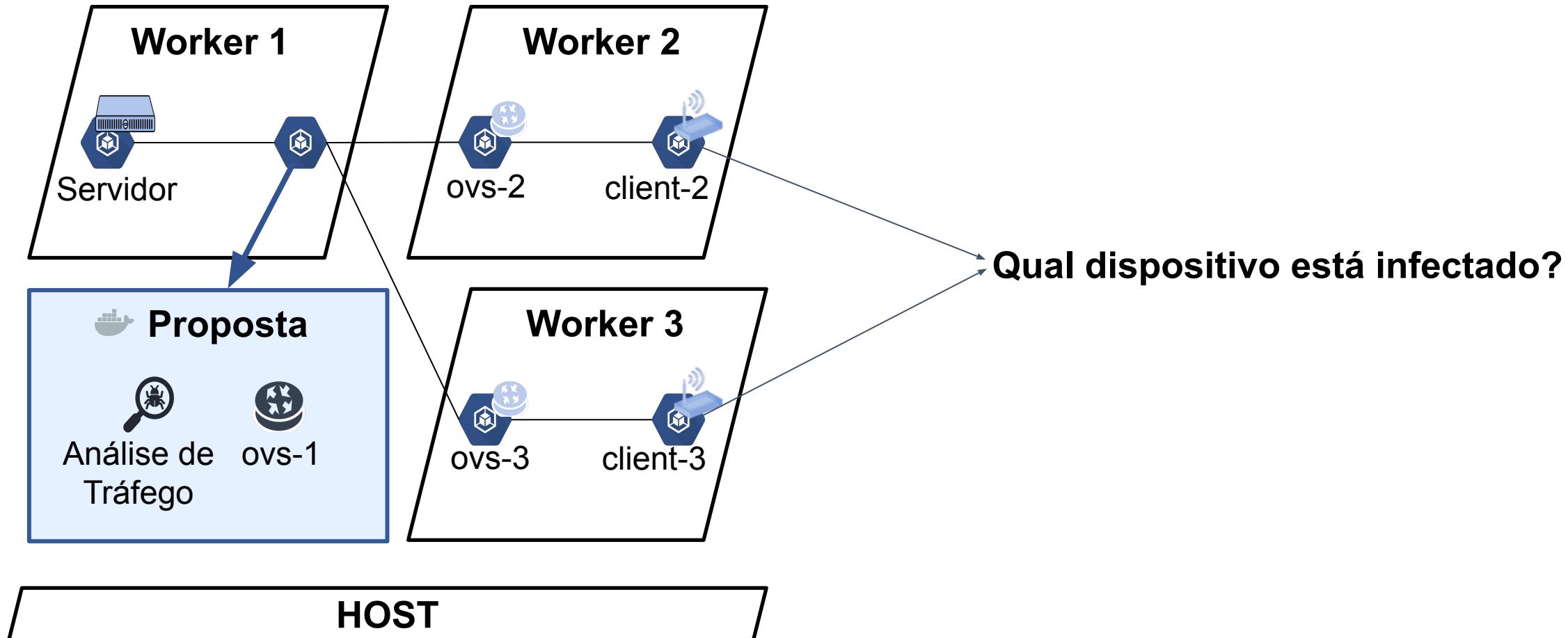


Cenário de Rede

Topologias



MENTORED



Demonstração Prática



MENTORED

1. Inicializar o cluster KinD
2. Instalar as dependências nos nodes
3. Configurar os containers Docker
4. Configurar os módulos de rede
5. Definir os dispositivos e a topologia
6. Executar o experimento
7. Coletar os resultados



Principais Desafios e Limitações



Principais Desafios e Limitações



MENTORED

Aplicação de Políticas de Segurança



Principais Desafios e Limitações



MENTORED

Escolha, Localização e Configuração

Execução de VNF

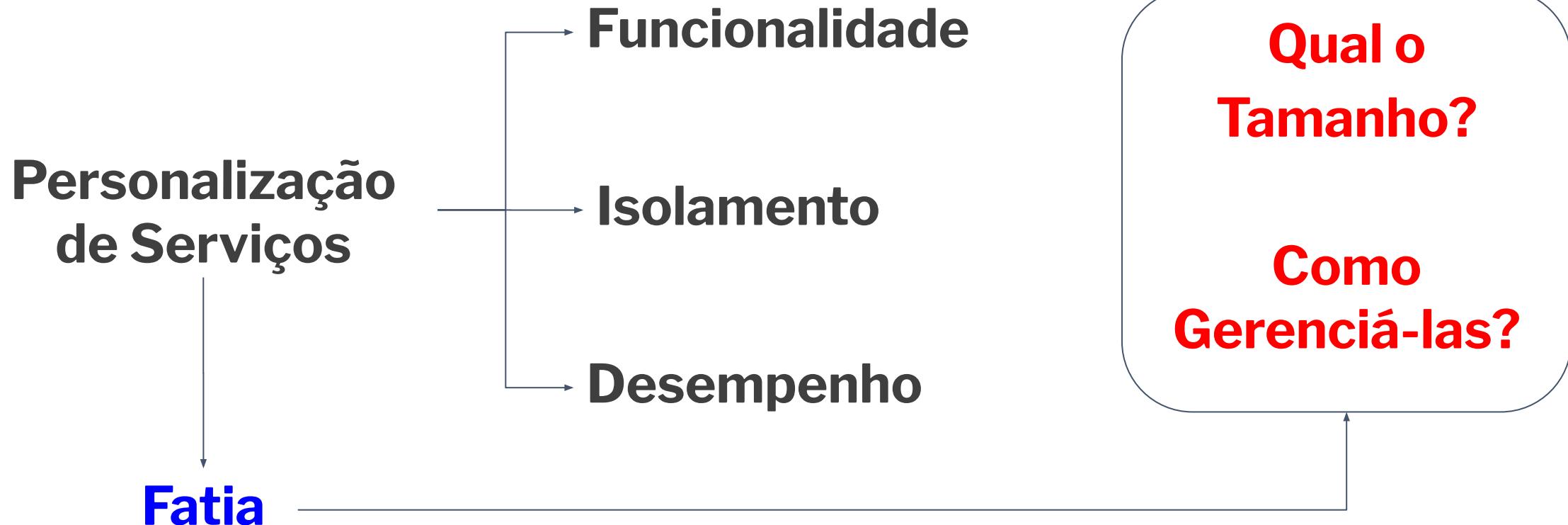
Qual(is)
Serviço(s)?

Onde
Colocá-los?

Como
Configurá-los?



Fatiamento da Rede (*Network Slicing*)

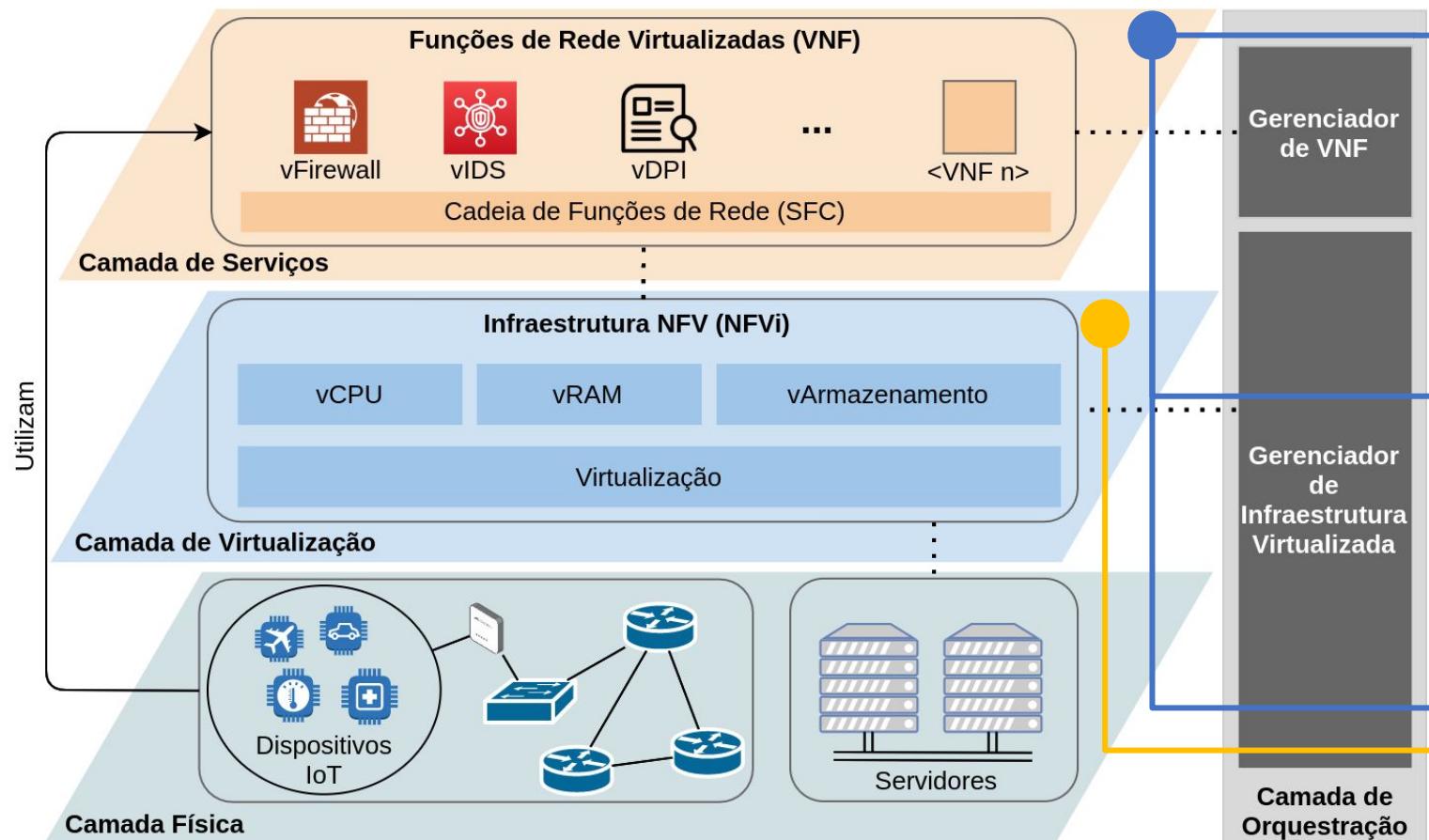


Principais Desafios e Limitações



MENTORED

Estruturas Lógicas da NFV



Gerenciamento de Imagens

Políticas de Autenticação e Autorização

Isolamento



Considerações Finais





Vantagens da NFV na IoT



Desacoplamento

e

Escalabilidade



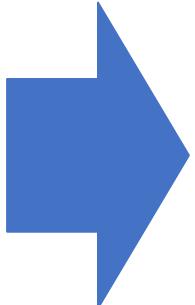
Vantagens da NFV na IoT



Desacoplamento

e

Escalabilidade



Desempenho

e

Qualidade de Serviço

Considerações Finais



MENTORED

Estatística dos Trabalhos



Desempenho de NFV



Desempenho de Rede



Eficácia da Solução

Considerações Finais



MENTORED

Desafios



Desempenho de NFV



Desempenho de Rede



Eficácia da Solução

+

Desafios

Considerações Finais



MENTORED

Trabalhos em Andamento

MENTORED Testbed

***Predicting Response
Time in SDN-Fog
Environments for IIoT
Applications***

Referências



MENTORED

- **Imagens de não produção própria: www.pixabay.com e www.pexels.com**
- **As referências das demais imagens utilizadas podem ser encontradas com detalhes no capítulo deste minicurso**



www.mentoredproject.org

