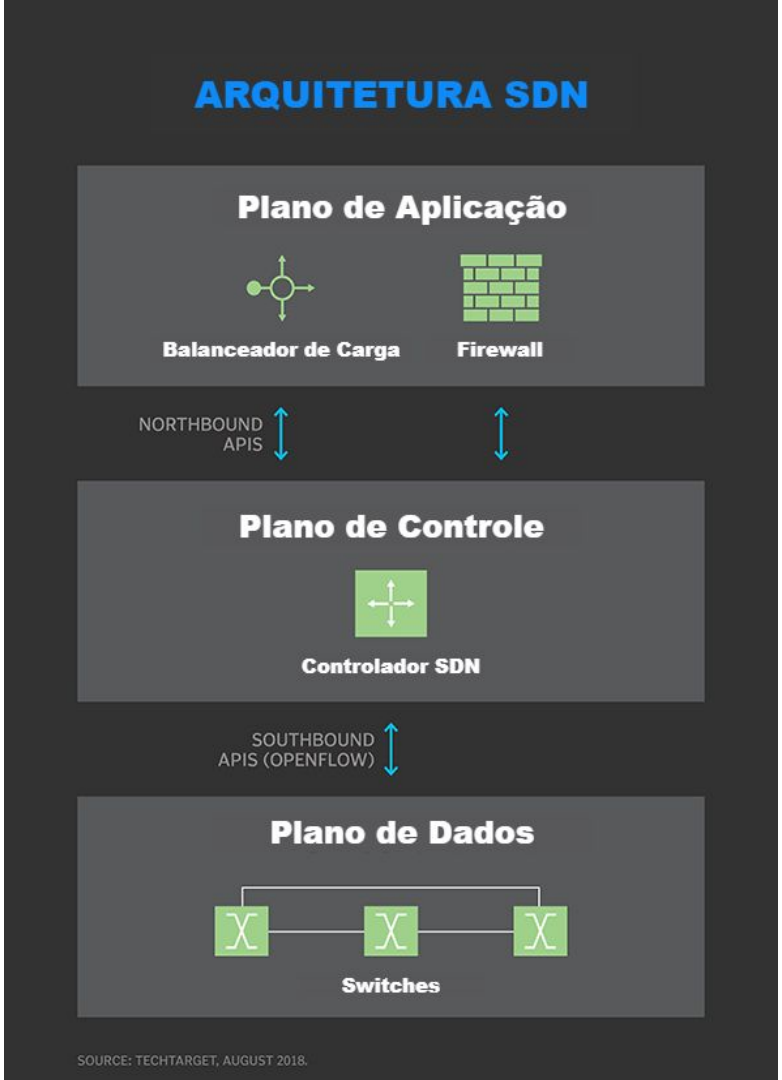
Automação e Cibersegurança: Criando uma Ferramenta de Testes para Redes SDN

Ryan M. S. Leal, Johan K. E. Freitas, Francisco A. C. Albuquerque Júnior, Waslon T. A. Lopes, Fabrício B. S. Carvalho e Iguatemi E. Fonseca

Centro de Informática - UFPB
Centro de Energias Alternativas e Renováveis - UFPB

Redes SDN

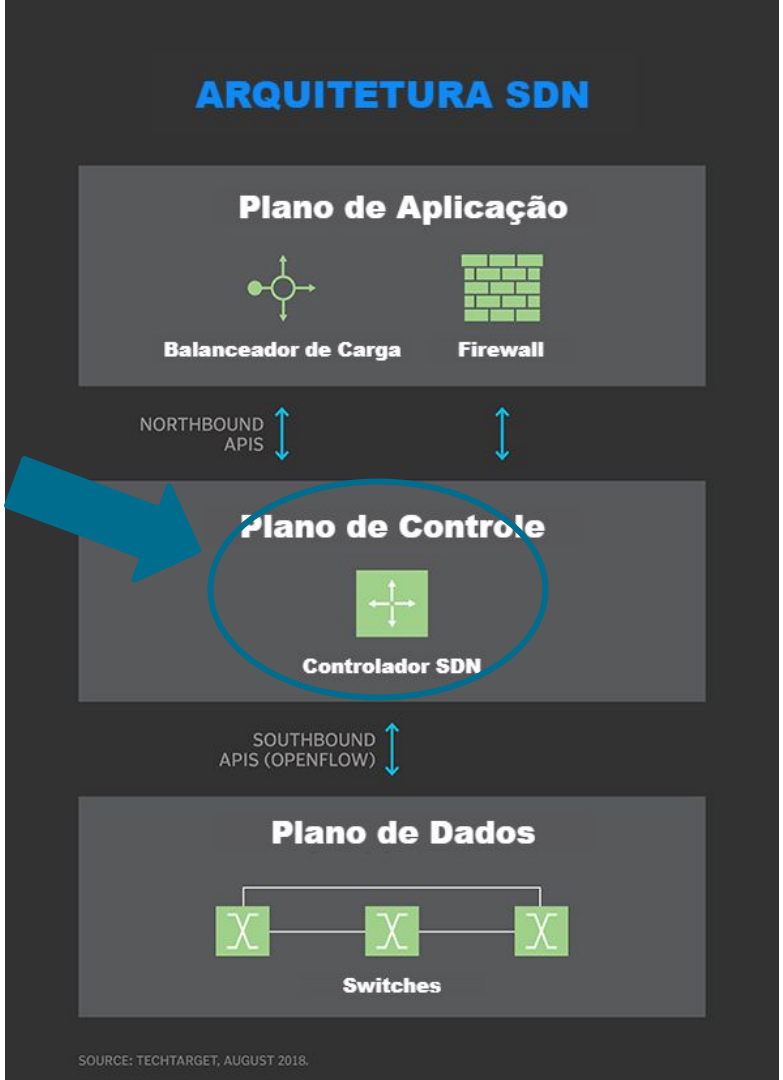
- Centralização da lógica de controle
- Divisão em planos
- Programabilidade



Fonte: Adaptado de ComputerWeekly.

Redes SDN

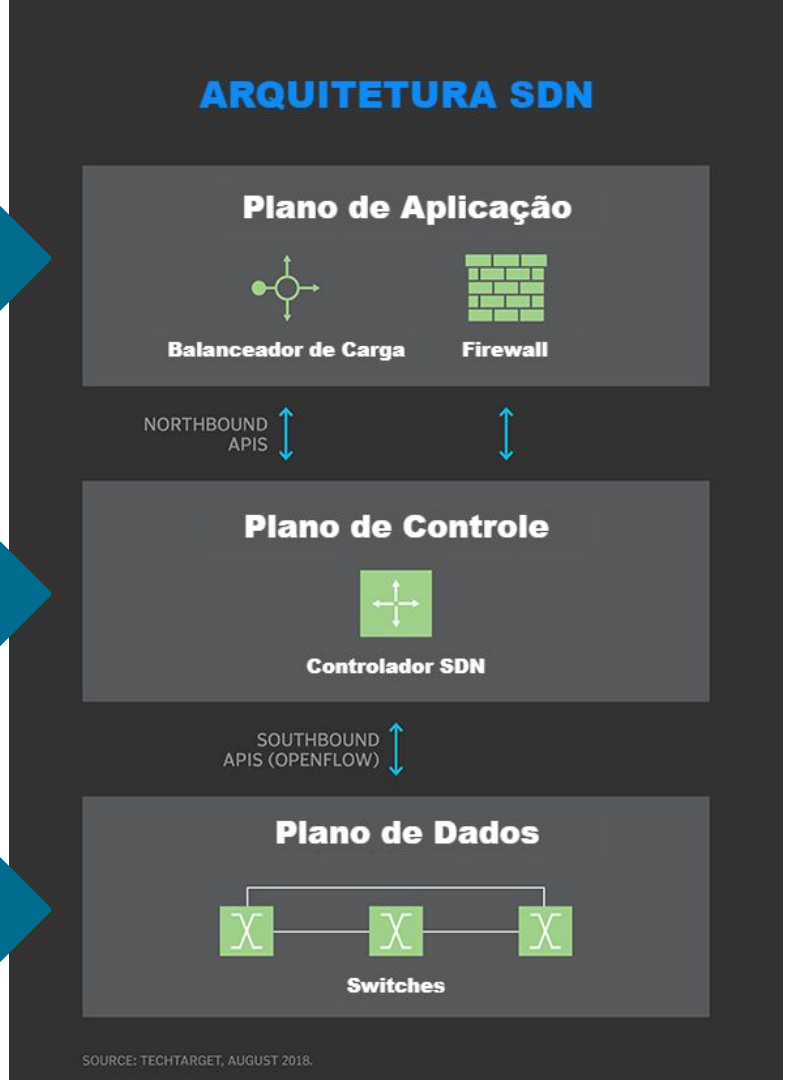
- Centralização da lógica de controle
- Divisão em planos
- Programabilidade



Fonte: Adaptado de ComputerWeekly.

Redes SDN

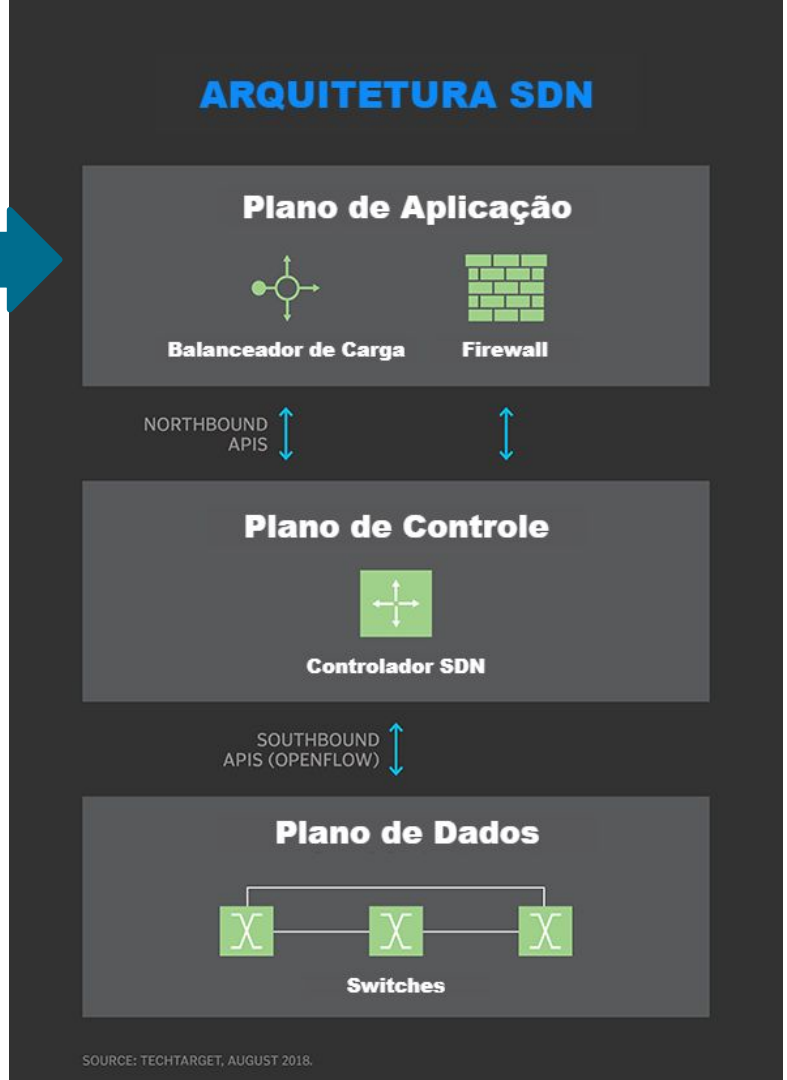
- Centralização da lógica de controle
- Divisão em planos
- Programabilidade



Fonte: Adaptado de ComputerWeekly.

Redes SDN

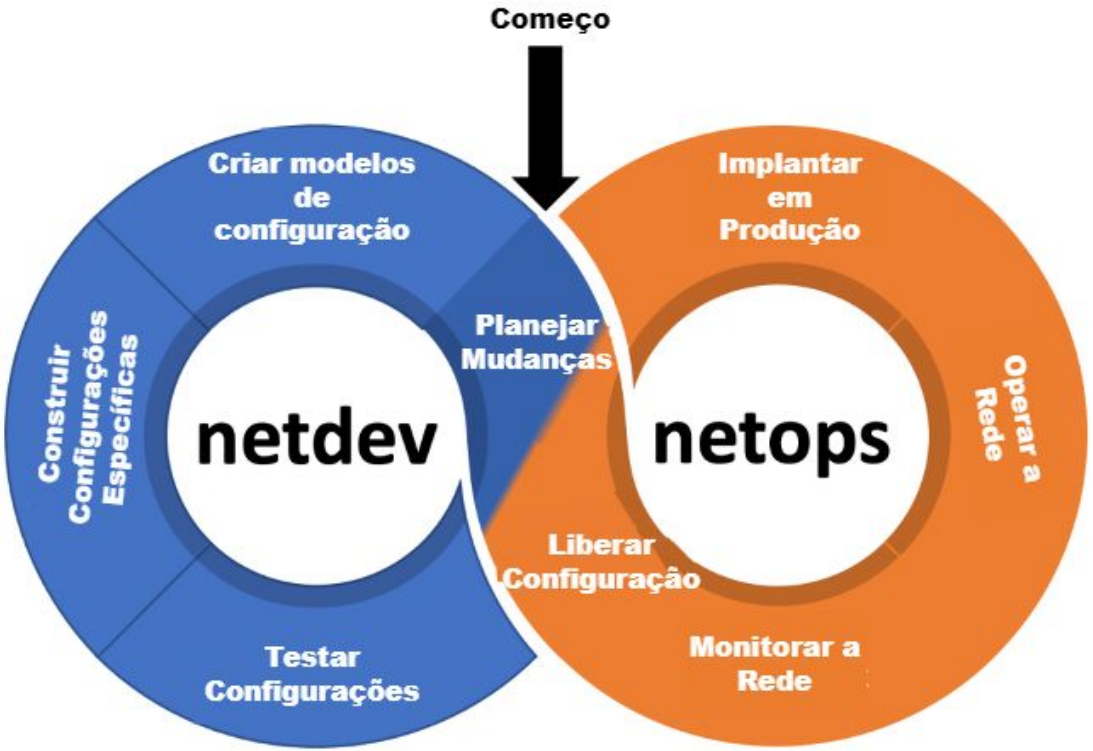
- Centralização da lógica de controle
- Divisão em planos
- Programabilidade



Fonte: Adaptado de ComputerWeekly.

Redes SDN

- Redes 5G
  - Virtualização de rede
  - Networking Slicing
- CI/CD
- Orquestração



Fonte: Adaptado de AWS.

Segurança em Redes SDN

- Centralização -> Ponto de falha
- Problema do Acoplamento de Switches
- Limitação de TCAM
- Negação de Serviço (DoS)
  - Alta Taxa
  - Baixa Taxa

Motivação

Fonte: ONF.

Fonte: RNP.

MONITORING AND MEASUREMENT

Software Defined Traffic Measurement with OpenSketch, Minlan Yu, Lavanya Jose, Rui Miao, NSDI 2013

FlowSense: Monitoring Network Utilization with Zero Measurement Cost, Curtis Yu, Cristian Lumezanu, Vishal Singh, Yueping Zhang, Guofei Jiang, Harsha V. Madhyastha, PAM 2013

Software-defined Latency Monitoring in Data Center Networks, Curtis Yu, Cristian Lumezanu, Abhishek Sharma, Qiang Xu, Guofei Jiang, Harsha V. Madhyastha, PAM 2015

Fonte: ONF.

Motivação

SECURITY

Ethane: Taking Control of the Enterprise, Martìn Casado, Michael J. Freedman, Justin Pettit, Jianying Luo, Nick McKeown, Scott Shenker, Sigcomm 2007

Resonance: Dynamic Access Control in Enterprise Networks, Ankur Nayak, Alex Reimers, Nick Feamster, Russ Clark, WREN 2009

OpenFlow Random Host Mutation: Transparent Moving Target Defense using Software Defined Networking, Jafar Haadi Jafarian, Ehab Al-Shaer, Qi Duan, HotSDN 2012

CLOUD

Effective Resource Control Strategies using OpenFlow in Cloud Data Center, Adami D., Martini B., Antichi G., Giordano S., Gharbaoui M., Castoldi P., IFIP/IEEE IM 2013

On Virtualization-aware Traffic Engineering in OpenFlow Data Centers networks, Gharbaoui M., Martini B., Adami D., Antichi G., Giordano S., Castoldi P., IFIP/IEEE NOMS 2014

Applying NOX to the Datacenter, Arsalan Tavakoli, Martìn Casado, Teemu Koponen, Scott Shenker, HotNets 2009

Fonte: ONF.

Problema(s)

Fonte: OWASP.

Fonte: IEEXPLORE.

Desafio(s)

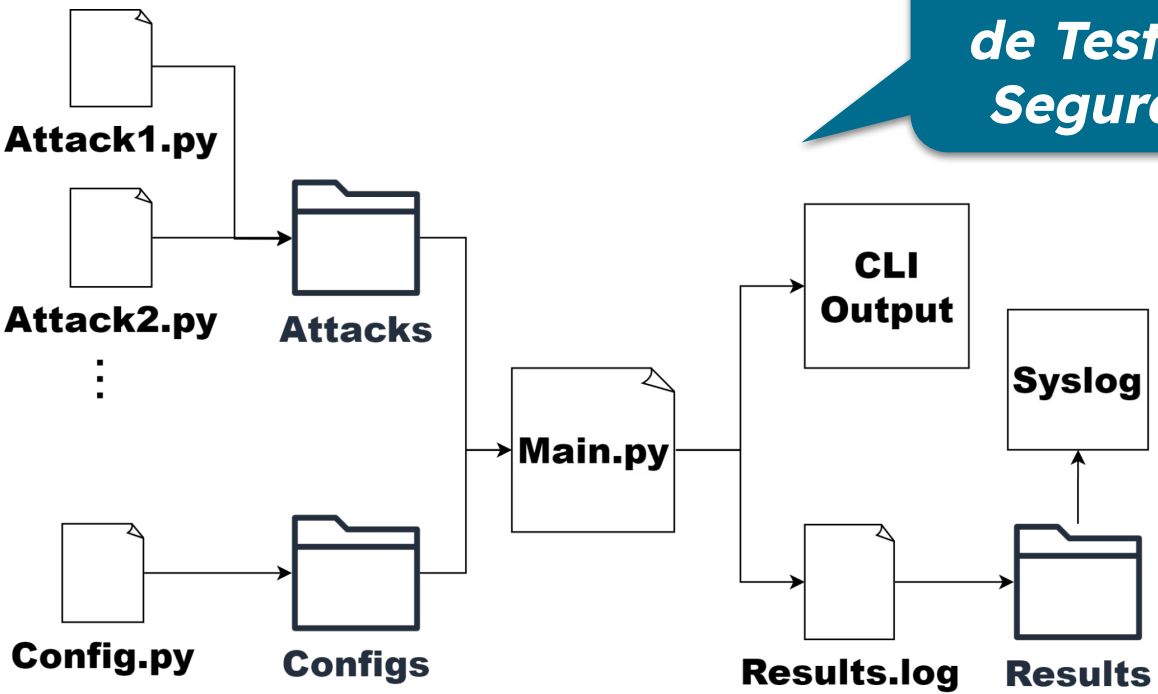
Fonte: 8icons.

Limitações Humanas

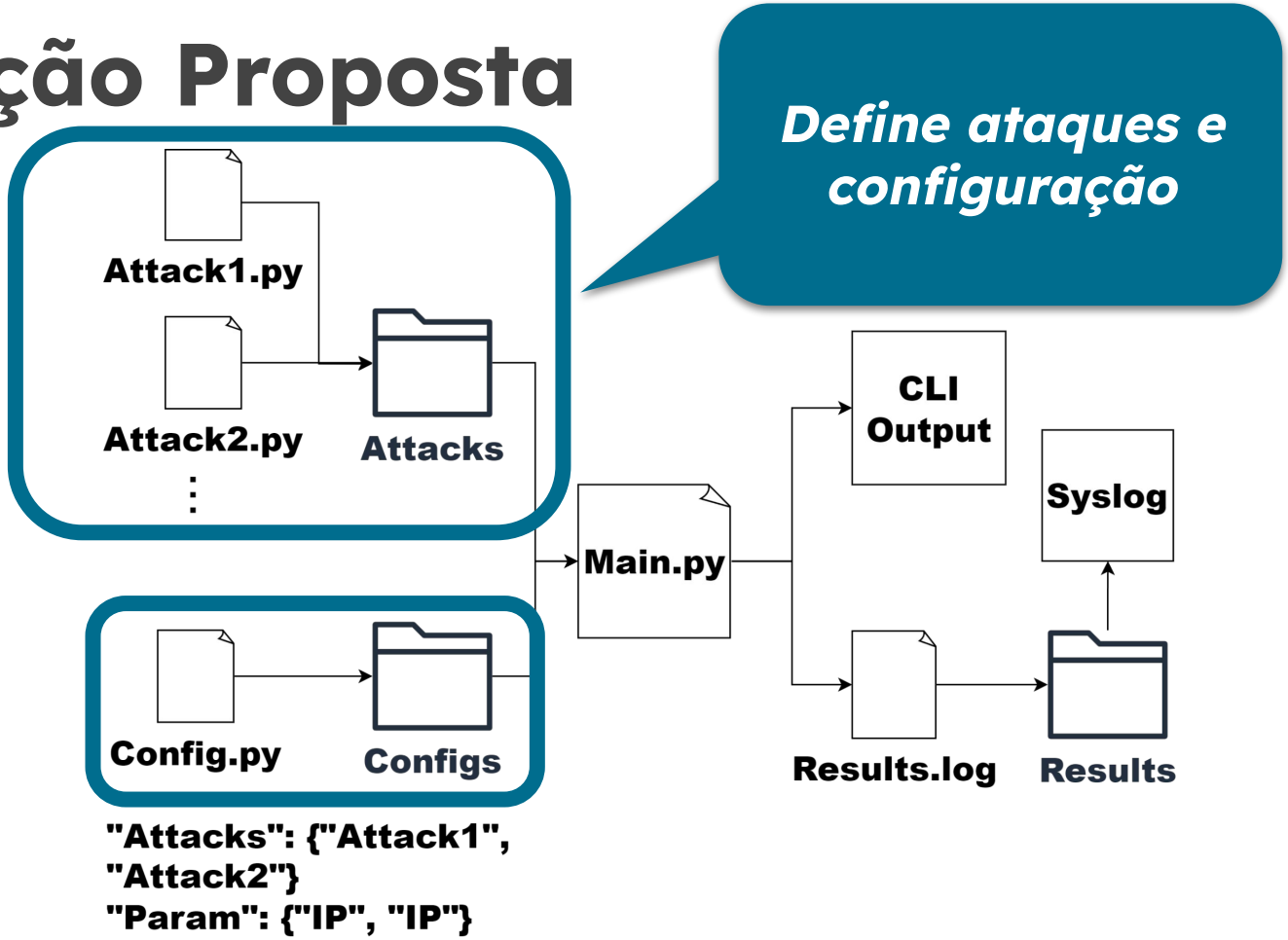
Fonte: 8icons.

Complexidade

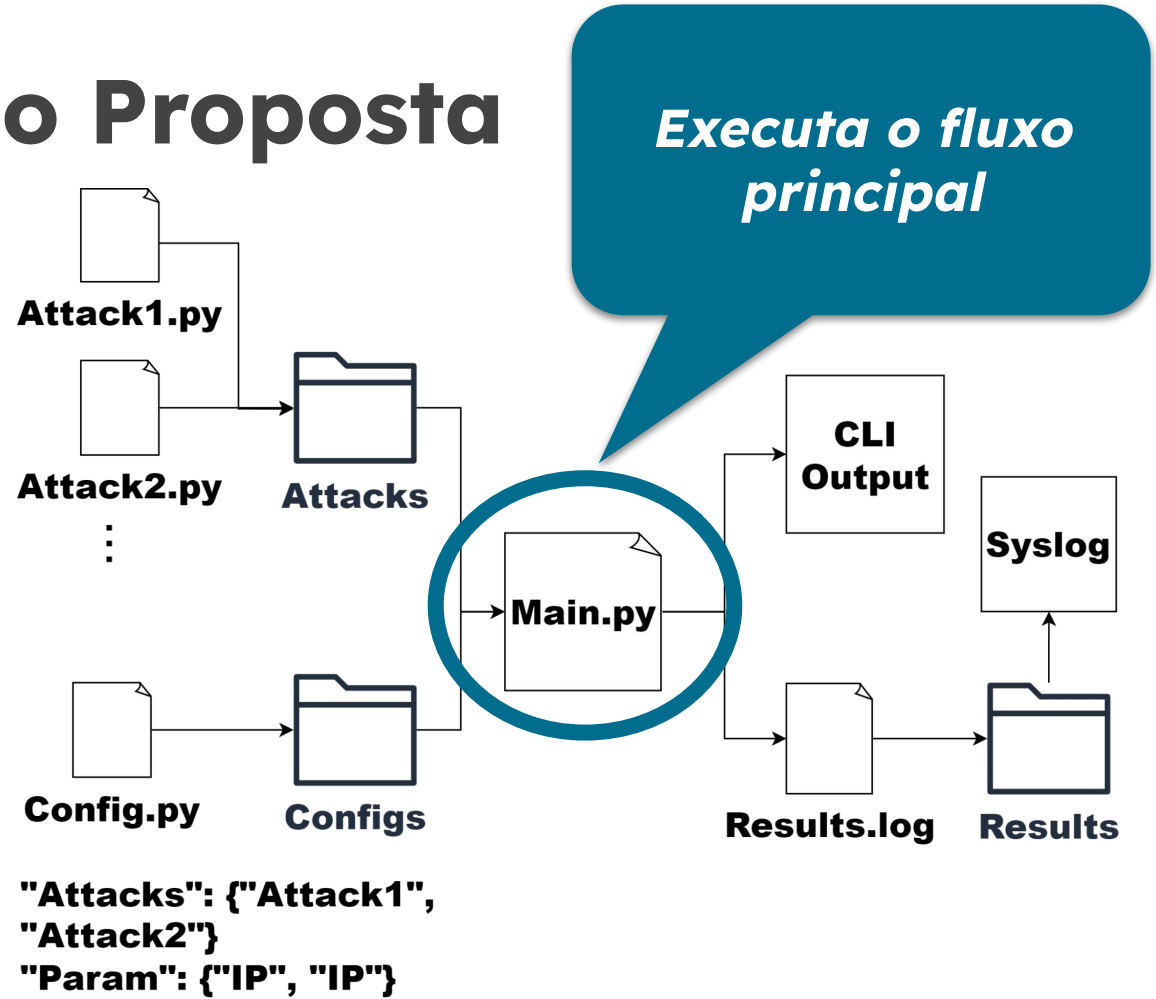
Solução Proposta



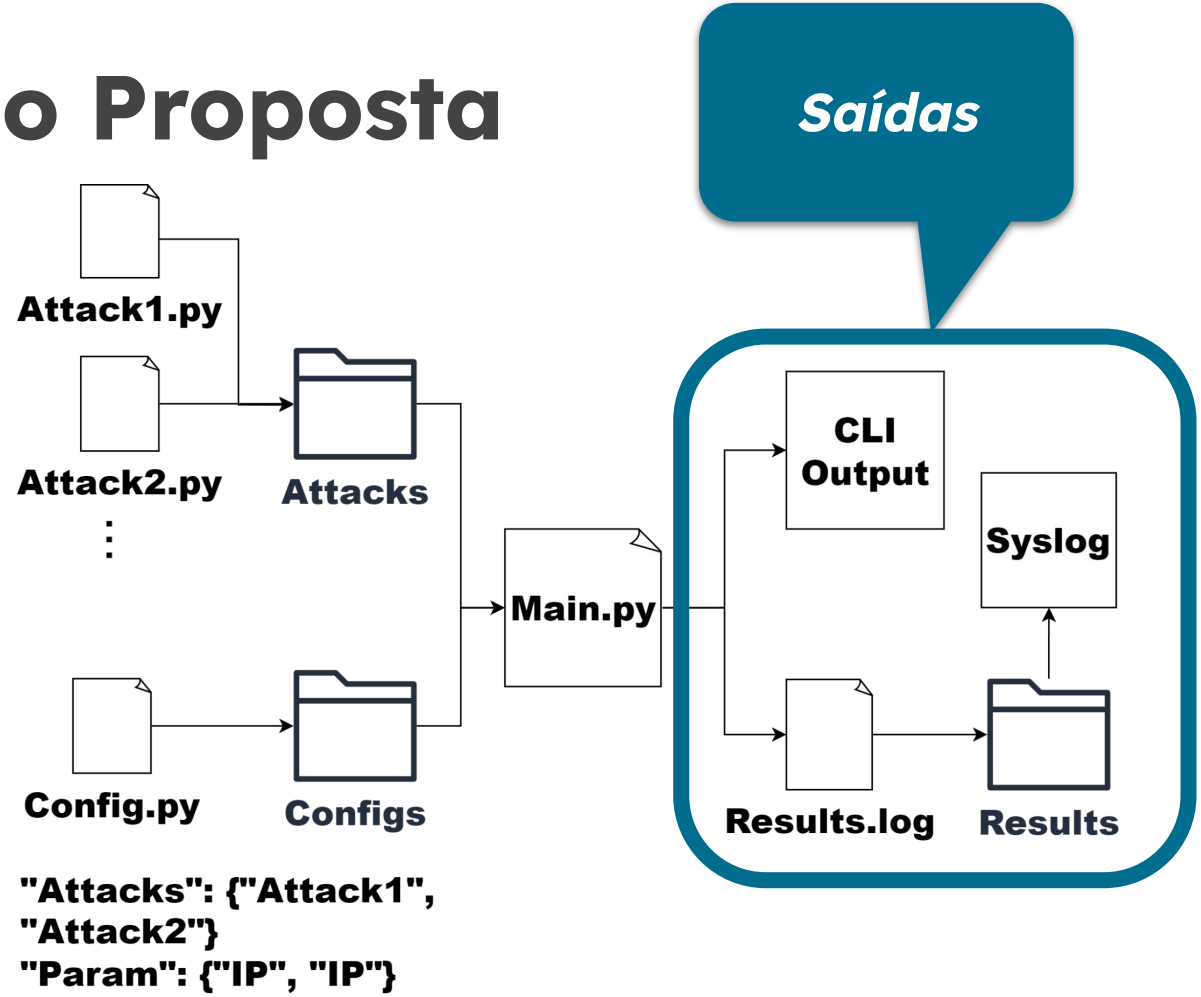
Solução Proposta



Solução Proposta



Solução Proposta



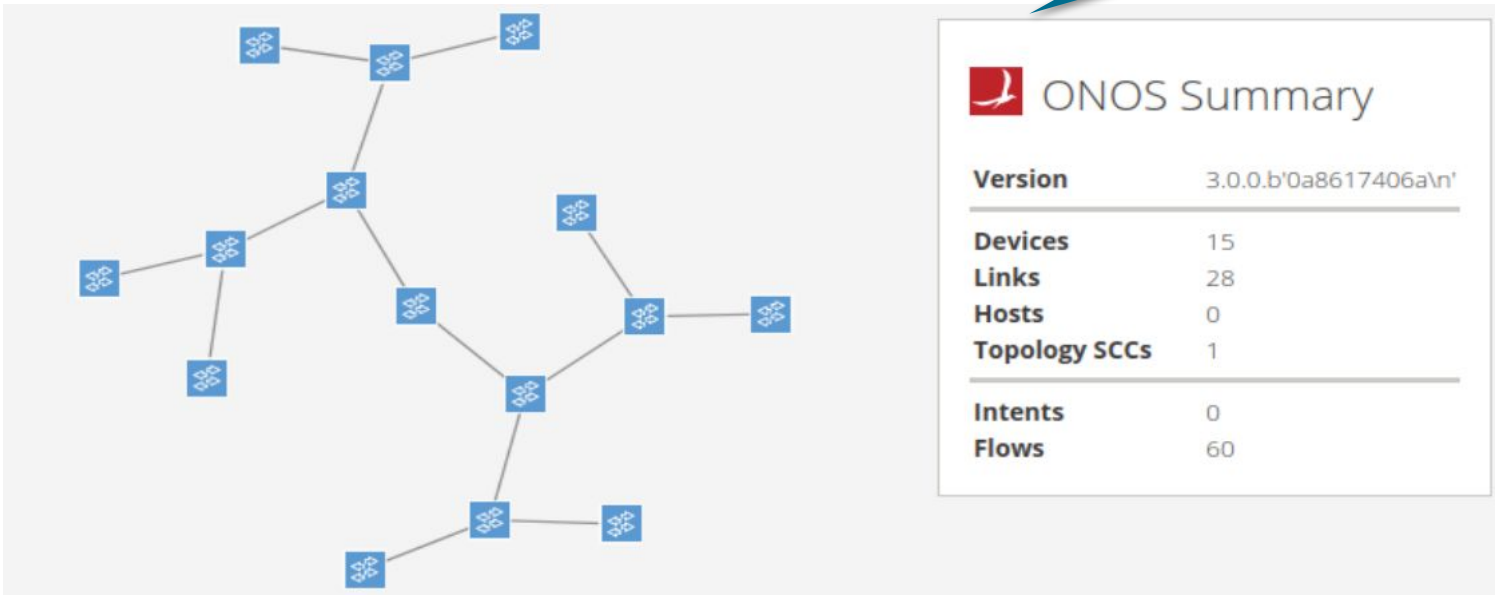
Avaliação - Testes

Ataques Utilizados nos testes

- MAC Address Flooding
- TCP SYN Flood
- UDP Flood
- ICMP Flood

Avaliação - Testes

ONOS + Mininet - Topologia de Teste



ONOS Summary

Version	3.0.0.b'0a8617406a\n'
Devices	15
Links	28
Hosts	0
Topology SCCs	1
Intents	0
Flows	60

Avaliação - Testes

Configuração de 2 ataques

```
ATTACK_SCRIPTS = [
    {'module': 'macof_attack', 'params': {'interface': 'INTERFACE'}},
    {'module': 'hping_attack', 'params': {'target': 'IP', 'interface': 'INTERFACE'}},
    # Adicione mais ataques conforme necessário
]

TARGET_INFO = {
    'IP': '10.0.0.5',
    'INTERFACE': 'h5-eth0'
}
```

Avaliação - Testes

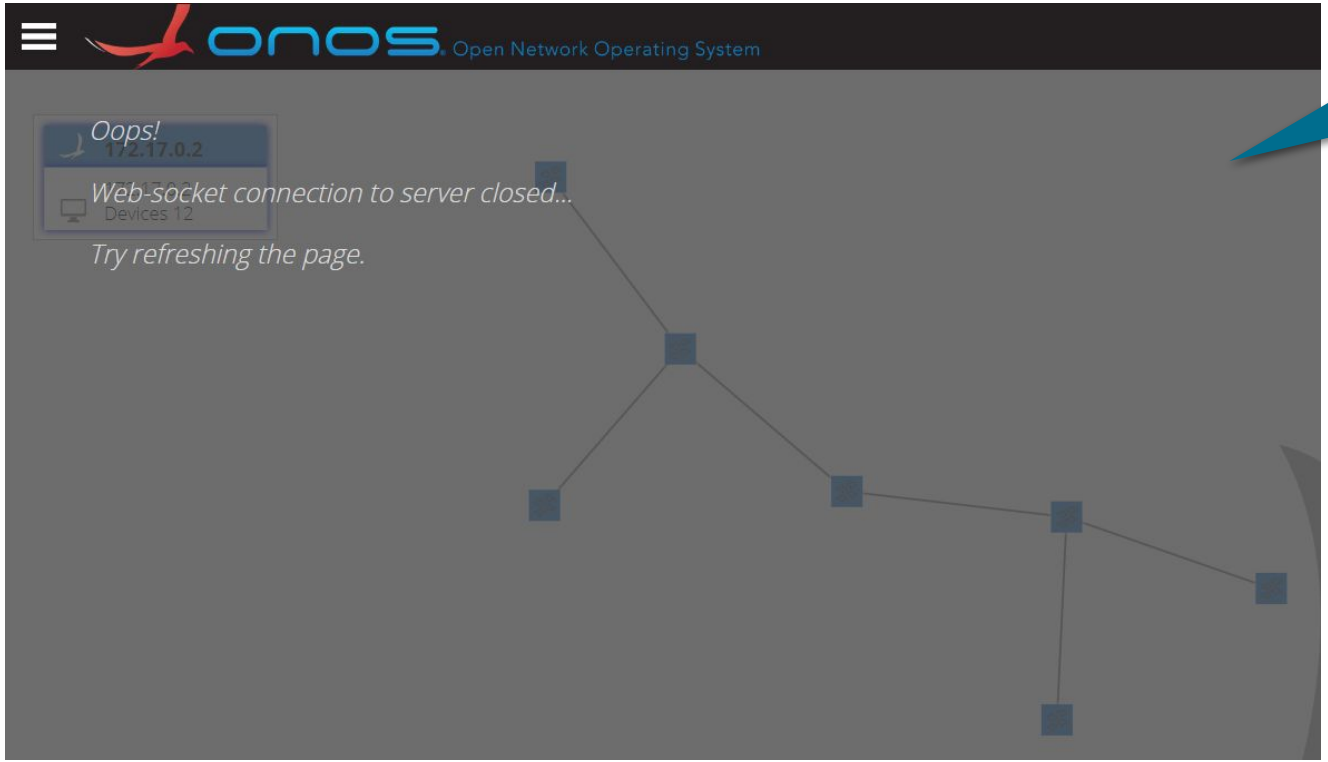
```python
ATTACK_SCRIPTS = [
    {'module': 'syn_flood_attack', 'params': {'target_ip': 'IP', 'target_port': 'PORT', 'duration': 'DURATION'}},
    {'module': 'icmp_flood_attack', 'params': {'target_ip': 'IP', 'duration': 'DURATION'}},
    {'module': 'udp_flood_attack', 'params': {'target_ip': 'IP', 'target_port': 'PORT', 'duration': 'DURATION'}},
    {'module': 'hping_attack', 'params': {'target_ip': 'IP', 'interface': 'INTERFACE'}},
    {'module': 'macof_attack', 'params': {'interface': 'INTERFACE'}}
]

TARGET_INFO = {
    'IP': '10.0.0.16',
    'PORT': '80',
    'DURATION': '10',
    'INTERFACE': 'h16-eth0'
}
```

Configuração de 5 ataques

Avaliação - Testes


```
2732024-06-18 21:21:22,444 - attack_scripts.udp_flood_attack - INFO - Iniciando ataque UDP Flood no IP
   10.0.0.16, porta 80 por 10 segundos
2742024-06-18 21:21:32,455 - attack_scripts.udp_flood_attack - INFO - Ataque UDP Flood concluído. 293 pacotes
   enviados.
2752024-06-18 21:21:32,458 - __main__ - INFO - Ataque udp_flood_attack concluído com sucesso em 10.01 segundos
2762024-06-18 21:21:32,458 - results.result_logger - INFO - Resultado do udp_flood_attack: Ataque UDP Flood
   concluído. 293 pacotes enviados.
2772024-06-18 21:21:32,458 - __main__ - INFO - Executando ataque: hping_attack com parâmetros: {'target_ip':
   '10.0.0.16', 'interface': 'h16-eth0'}
2782024-06-18 21:21:32,459 - attack_scripts.hping_attack - INFO - Executando Hping no IP 10.0.0.16 através da
   interface h16-eth0 com timeout de 30 segundos
2792024-06-18 21:22:02,523 - attack_scripts.hping_attack - ERROR - Hping expirou após 30 segundos
2802024-06-18 21:22:02,523 - __main__ - INFO - Ataque hping_attack concluído com sucesso em 30.06 segundos
```

Avaliação - Testes



Negação de Serviço

Avaliação - Ganhos de Tempo

	TEMPO	
	2 Scripts	5 Scripts
Manual	1min40s	3min19s
Ferramenta	1min05s	1min34s

Ganho de 53,8%

Avaliação - Ganhos de Tempo

	TEMPO	
	2 Scripts	**5 Scripts**
Manual	1min40s	3min19s
Ferramenta	1min05s	1min34s

Ganho de 111,7%

Considerações finais

- Negação de serviço é perigo real
- Livrar de erros humanos - Facilidade de uso
- Ganho de tempo na automação
- Aplicação da Ferramenta no Testbed do OpenRAN Brasil

Trabalhos futuros

- Novos ataques - focados em SDN
- Visualização para os logs
- Testes em ambientes reais de CI/CD
- Melhorias técnicas do código
- Melhorias de interface

Contatos

- Ryan M. S. Leal (ryanleal@cc.ci.ufpb.br)
- Iguatemi E. Fonseca (iguatemi@ci.ufpb.br)
- Waslon T. A. Lopes (waslon@cear.ufpb.br)
- Fabrício B. S. Carvalho (fabricio@cear.ufpb.br)
- Francisco A. C. A. Júnior (facajx@gmail.com)
- Johan K. E. Freitas (johankevin33@gmail.com)

Obrigado!

SBSeg24
SÃO JOSÉ DOS CAMPOS

Dúvidas?

CNPq RNP