SDN-IPS - Uma solução para contenção de ataques cibernéticos usando SDN/OpenFlow

Adriana Viriato Ribeiro (UFBA e PoP-BA/RNP)
Italo Valcy S. Brito (UFBA e PoP-BA/RNP)

{adrianavr, italovalcy}@ufba.br

Motivação

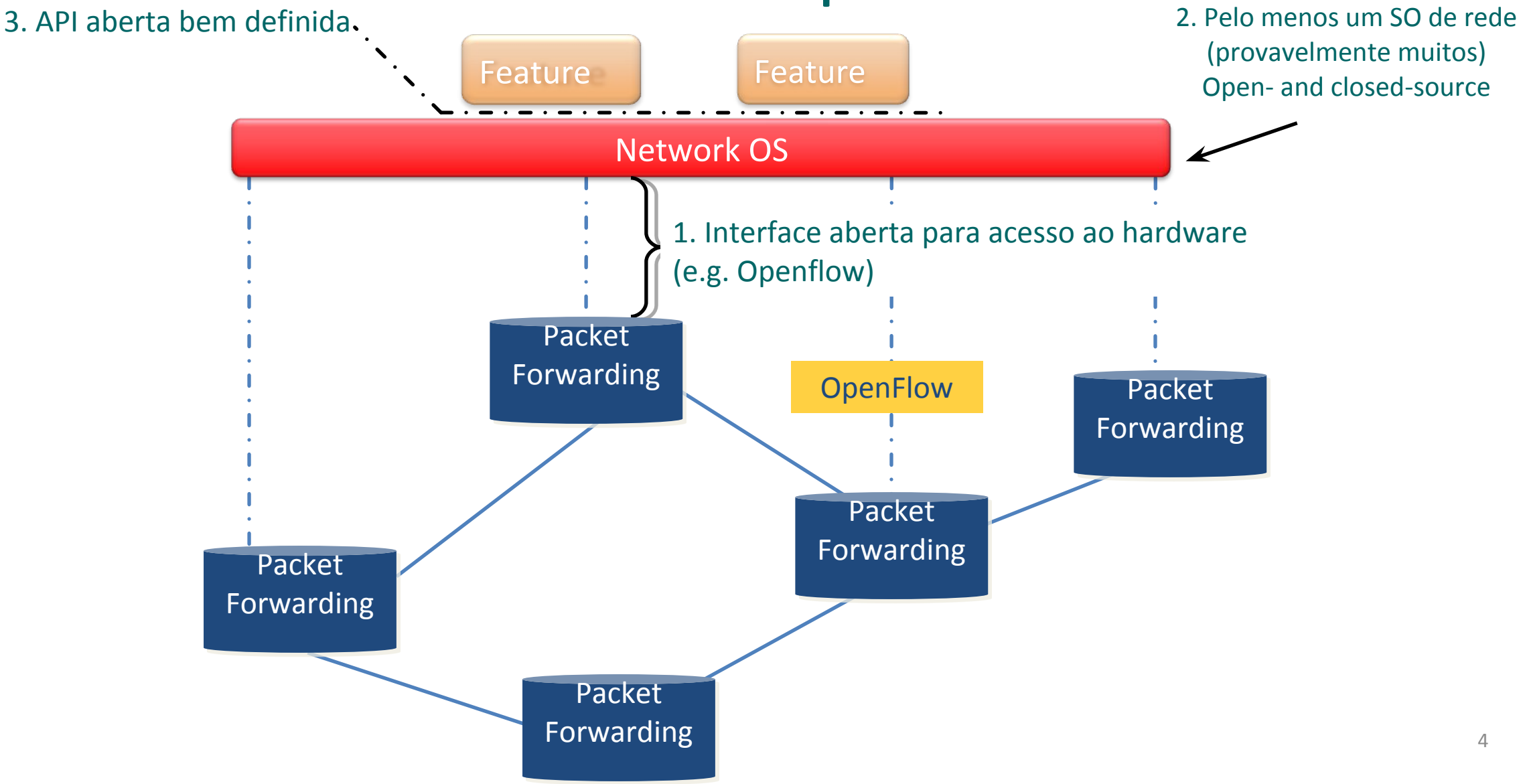
- Crescimento na quantidade e diversidade de ataques cibernéticos
  - Necessidade de ações de contenção especializadas
  - Automação e baixo tempo de resposta
  - Integração com diferentes abordagens de detecção de intrusos

- Paradigma SDN abre diversas perspectivas
  - Flexibilidade e granularidade na tomada de decisões
  - Visão global da rede e modelagem em grafo para melhor local de contenção

Limitações da rede atual à inovação

- Múltiplas sintaxes de CLI;
- Funcionalidades dependentes de fabricante – tempo de implantação;
- Licenciamento por funcionalidade;
- Impossibilidade de testar novas funcionalidades de rede (protocolos);
- Customizações são restritas aos parâmetros de configuração;
- Rede com pouca flexibilidade.

A “Rede Definida por Software”



SDN e contenção de ataques

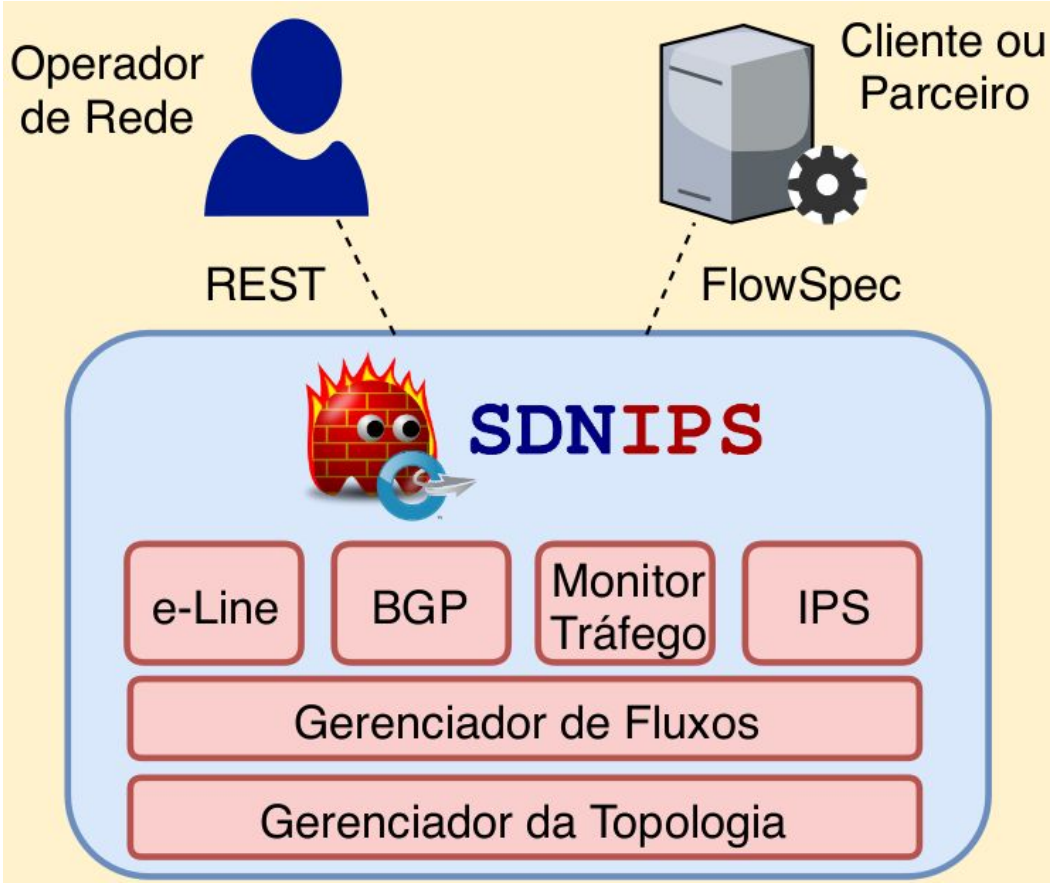
- Flexibilidade na tomada de decisão para contenção
  - Cada ataque exige tomada de ações de contenção específica
  - Granularidade e programabilidade do comutador para customizar a tomada de decisão
- Visão logicamente centralizada da rede
  - Contenção mais próxima da origem
  - Otimização de caminhos para espelhamento de tráfego

Exemplos de tipos de Ataque e Contenção

- Ataque de negação de serviço *slowloris*
  - Bloqueio por IP, bloqueio por rede
- Ataque de negação de serviço distribuído contra DNS autoritativo
  - Rate-limit
  - Limpeza de tráfego
- Comunicação C&C
  - Tráfego de controle: desvio para *honeypot*
  - Comandos de ataque: bloqueio
- Máquina infectada com vírus
  - Isolamento em Quarentena

SDN-IPS

- IPS (*Intrusion Prevention System*) baseado em OpenFlow
- Realiza orquestração da rede
- Provê capacidade de detecção e prevenção de intrusos
- Provê contenção customizada contra ataques
- http://insert.ufba.br/sdn-ips/



Arquitetura SDN-IPS

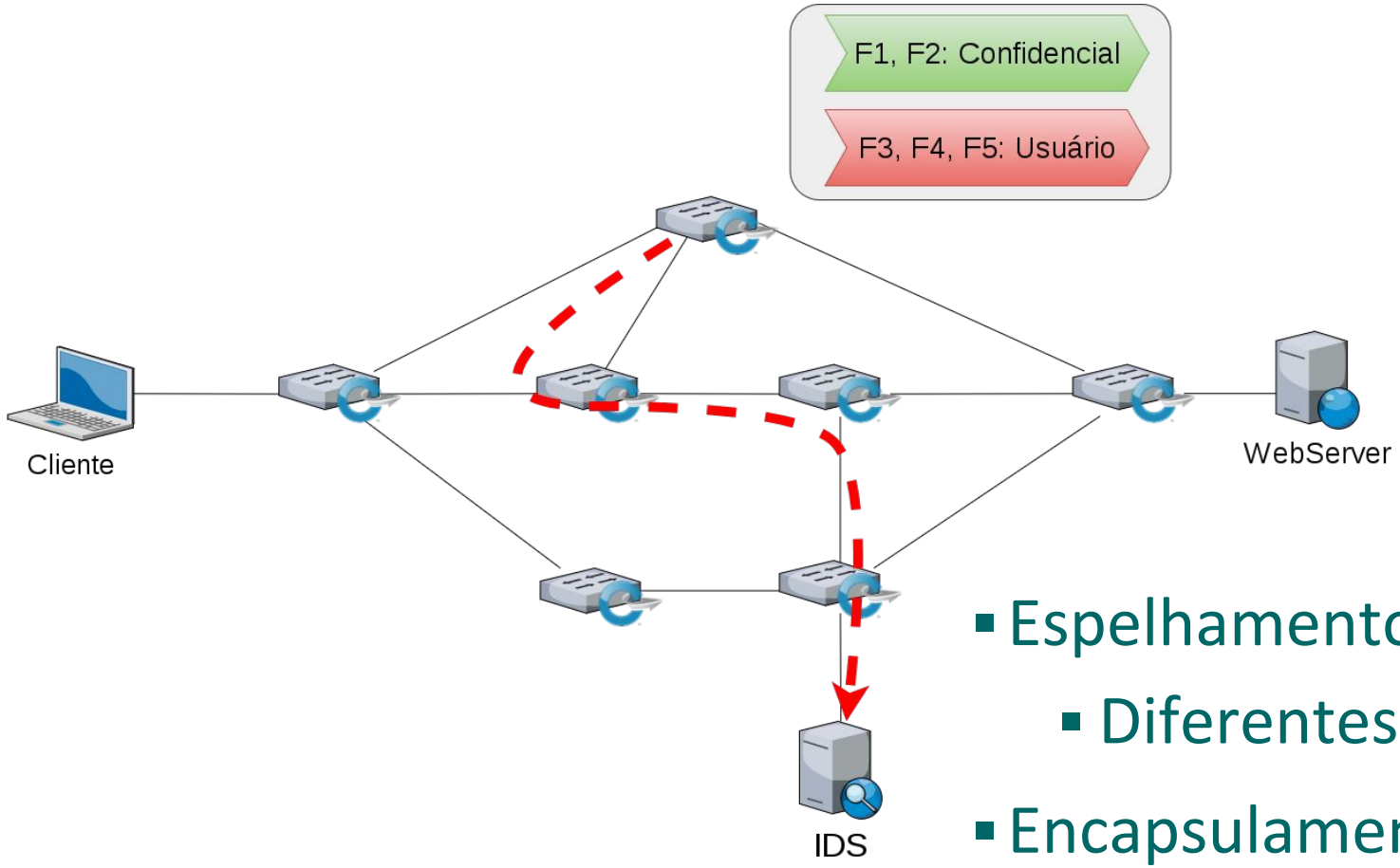
- **Gerenciador de Topologia**
  - Modelagem da rede em grafos
  - Descoberta de enlaces através de LLDP

- **Gerenciador de Fluxos**
  - Funcionamento da tabela de fluxos e roteamento
  - Checagem de consistência dos fluxos
  - OpenFlow

Arquitetura SDN-IPS

- **Espelhamento de tráfego**
  - Modificações nas tabelas de fluxos e tipos de espelhamento de tráfego
  - Encapsulamento do tráfego (Ex: VLAN)
  - Sistema de Detecção de Intrusos
  - Análise de tráfego

Espelhamento de tráfego



- Espelhamento granular
  - Diferentes sistemas de análise de tráfego
- Encapsulamento para alvo remoto
- Separação de papéis (escalabilidade)

Arquitetura SDN-IPS

- **Contenção Colaborativa**
  - BGP e FlowSpec
  - Validação de pedidos de bloqueio

- **Outras aplicações**
  - Roteamento interdomínio utilizando BGP
  - Criação de enlaces ethernet no padrão e-Line do MetroEthernet Fórum

Estratégias de contenção

- Bloqueio
- Limitação de banda
- Redirecionamento/Quarentena
- Limpeza de Tráfego
- Contenção Colaborativa

Exemplo de Quarentena com OpenFlow 1.0

e-Line

#	Prio.	Matches	Actions
1	65533	in_port=1,dl_vlan=100	output:2
2	65533	in_port=2,dl_vlan=100	output:1
3	65534	in_port=1, dl_vlan=100, nw_src=10.0.0.100	output:CONTROLLER
4	65535	in_port=1, dl_vlan=100, nw_src=10.0.0.100,nw_dst=6.6.6.6	set_nw_dst=192.168.0.10, output:2
5	65535	in_port=2, dl_vlan=100, nw_src=192.168.0.10,nw_dst=10.0.0.100	set_nw_src=6.6.6.6, output:1

Exemplo de Quarentena com OpenFlow 1.0

#	Prio.	Matches	Actions
1	65533	in_port=1,dl_vlan=100	output:2
2	65533	in_port=2,dl_vlan=100	output:1
3	65534	in_port=1, dl_vlan=100, nw_src=10.0.0.100	output:CONTROLLER
4	65535	in_port=1, dl_vlan=100, nw_src=10.0.0.100,nw_dst=6.6.6.6	set_nw_dst=192.168.0.10, output:2
5	65535	in_port=2, dl_vlan=100, nw_src=192.168.0.10,nw_dst=10.0.0.100	set_nw_src=6.6.6.6, output:1

Ctrl

Exemplo de Quarentena com OpenFlow 1.0

#	Prio.	Matches	Actions
1	65533	in_port=1,dl_vlan=100	output:2
2	65533	in_port=2,dl_vlan=100	output:1
3	65534	in_port=1, dl_vlan=100, nw_src=10.0.0.100	output:CONTROLLER
4	65535	in_port=1, dl_vlan=100, nw_src=10.0.0.100,nw_dst=6.6.6.6	set_nw_dst=192.168.0.10, output:2
5	65535	in_port=2, dl_vlan=100, nw_src=192.168.0.10,nw_dst=10.0.0.100	set_nw_src=6.6.6.6, output:1

Redirect

Exemplo de Quarentena com OpenFlow 1.0

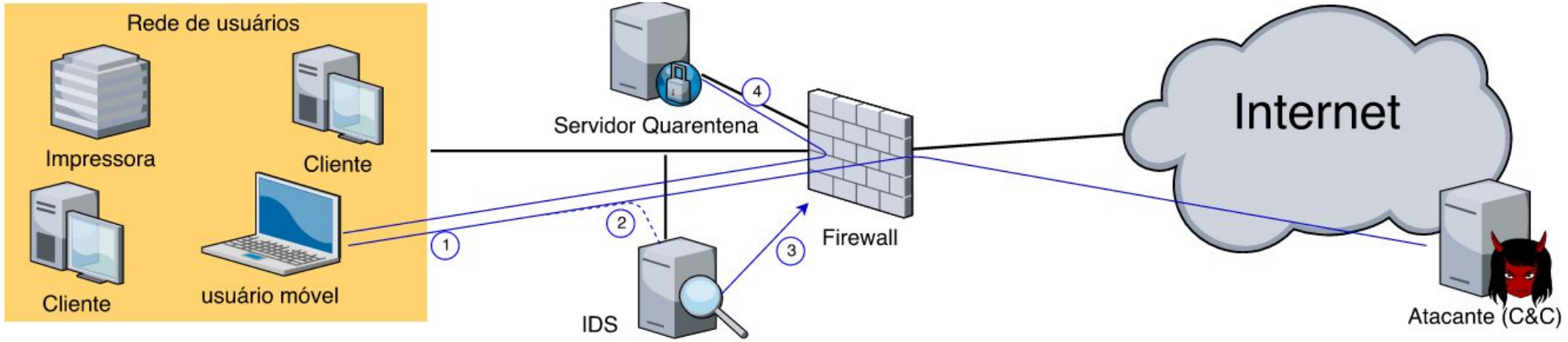
- OpenFlow 1.0 possui diversas limitações em termos de matches e actions disponíveis ao usuário
- Implementação de Quarentena via PBR requer manutenção de estado das conexões
- Desafio: aplicação de PBR no tráfego malicioso a partir de regras OpenFlow 1.0
  - Solução baseada na combinação de regras pró-ativas e reativas

Contenção Colaborativa

- Provedores de trânsito podem ofertar serviços de RTBH (Remote Triggered Black Hole)
  - Protocolo BGP FlowSpec [RFC 7674]
- Filtragem remota, mais próximo da origem do ataque
- Integração com controlador SDN, conversão dos flows BGP para regras OpenFlow

Casos de Uso: Quarentena

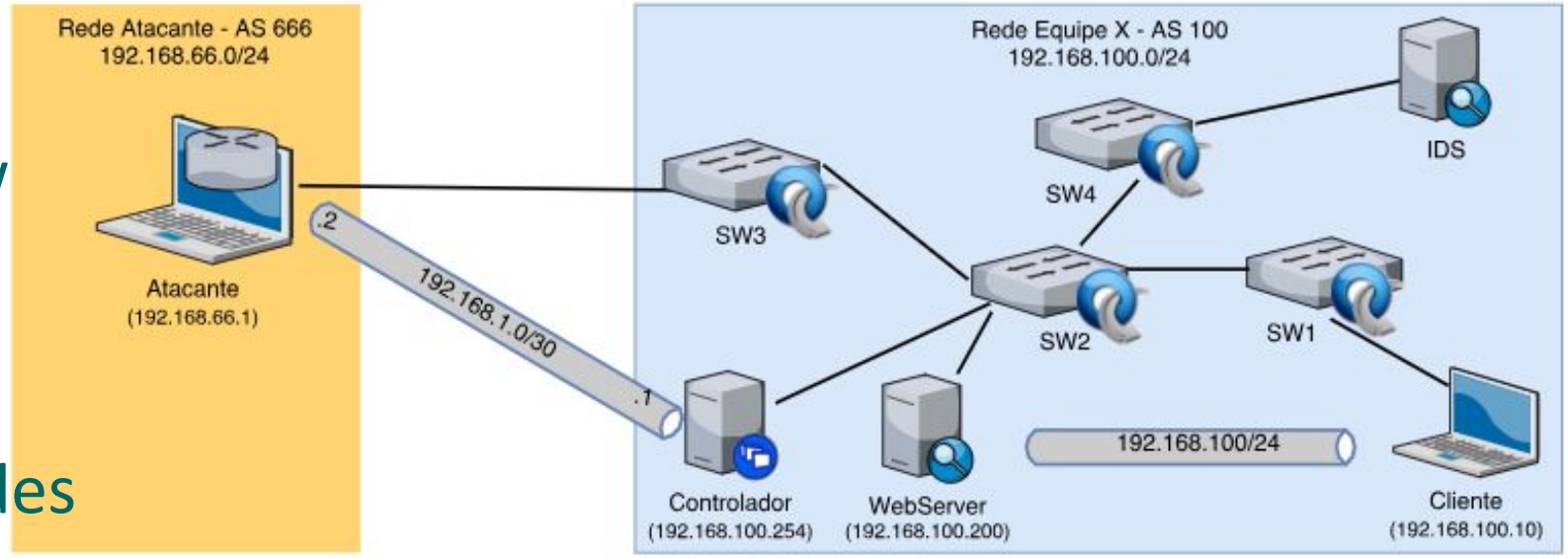
- Exemplo 1: máquina infectada com vírus e redirecionamento para servidor de quarentena.



Ambiente de Experimentação

FIBRE: (Future Internet Brazilian environment for Experimentation)

- https://fibre.org.br/
- Cenário com equipamentos reais
- Recursos disponíveis:
  - Máquinas virtuais
  - Switches OpenFlow
  - Redes sem fio
  - Redes ópticas
- Experimentações:
  - Arquiteturas de redes
  - Protocolos
  - Aplicações



Conclusões e Trabalhos Futuros

- Necessidade de ferramentas para contenção automatizada e colaborativa de atividade maliciosa na rede
- Esse trabalho apresentou o SDN-IPS:
  - Agrega a visibilidade dos IDS com a programabilidade do paradigma SDN
  - Cria uma solução de contenção de ataques através de estratégias como bloqueio e isolamento em quarentena
  - Adaptável a diferentes tipos de IDS
- Potencial de uso para redes de campus e *backbone*
- Possibilidade de integração com ferramentas de detecção de intrusos (e.g. IoT, SDN control plane, IDS anomalia, etc)

SDN-IPS: Uma solução para Contenção Automatizada e Colaborativa de Ataques Cibernéticos baseada em SDN

Dúvidas

http://insert.ufba.br/sdn-ips

Adriana Viriato Ribeiro (UFBA e PoP-BA/RNP)
Italo Valcy S. Brito (UFBA e PoP-BA/RNP)

{adrianavr, italovalcy}@ufba.br

24 a 28 de Setembro de 2018