Universidade Estadual Paulista “Júlio de Mesquita Filho” - UNESP

Mitigação Flexível de Ataques Usando SDN

Leandro Bertini Lara Gonçalves[1]
Marcelo Boeira de Barcelos[2]

[1]ACME! Cybersecurity Research
[2]DATACOM

Agenda

- Introdução
- Objetivos
- Arquitetura
- Projeto
- Aplicação
- Conclusão

Introdução

Sistemas de Detecção de Intrusão (IDSs)

- Podem inspecionar cabeçalhos e conteúdos de pacotes
- Detectam eventos de segurança na rede ou em hosts

Introdução

Sistemas de Detecção de Intrusão (IDSs)

- Emitem alertas de eventos encontrados
- Porém, não são perfeitos
  - Podem gerar falsos-positivos e falsos-negativos

Introdução

Snort

- Bem consolidado
- Baseado em abuso
- Faz uso de assinaturas
- Capaz de alta precisão
  - Desde que as assinaturas sejam bem definidas

Introdução

Redes Definidas por Software (SDN)

- Permite o controle da rede
  - Planos de dados e controle em dissociados
- Protocolo Openflow
  - Interface switch-controlador
  - Mais difundido
  - Permite controle da rede a distância
- Permite mitigação direta no elemento de comutação de dados

Introdução

Floodlight

- Controlador Openflow
- Oferece alto desempenho
  - Explora paralelismo
  - Projetado para ambiente de produção
- Estrutura modular
  - Simplifica modificação de funcionalidades
- Código aberto
  - Possibilidade de alteração de trechos do software

Objetivos

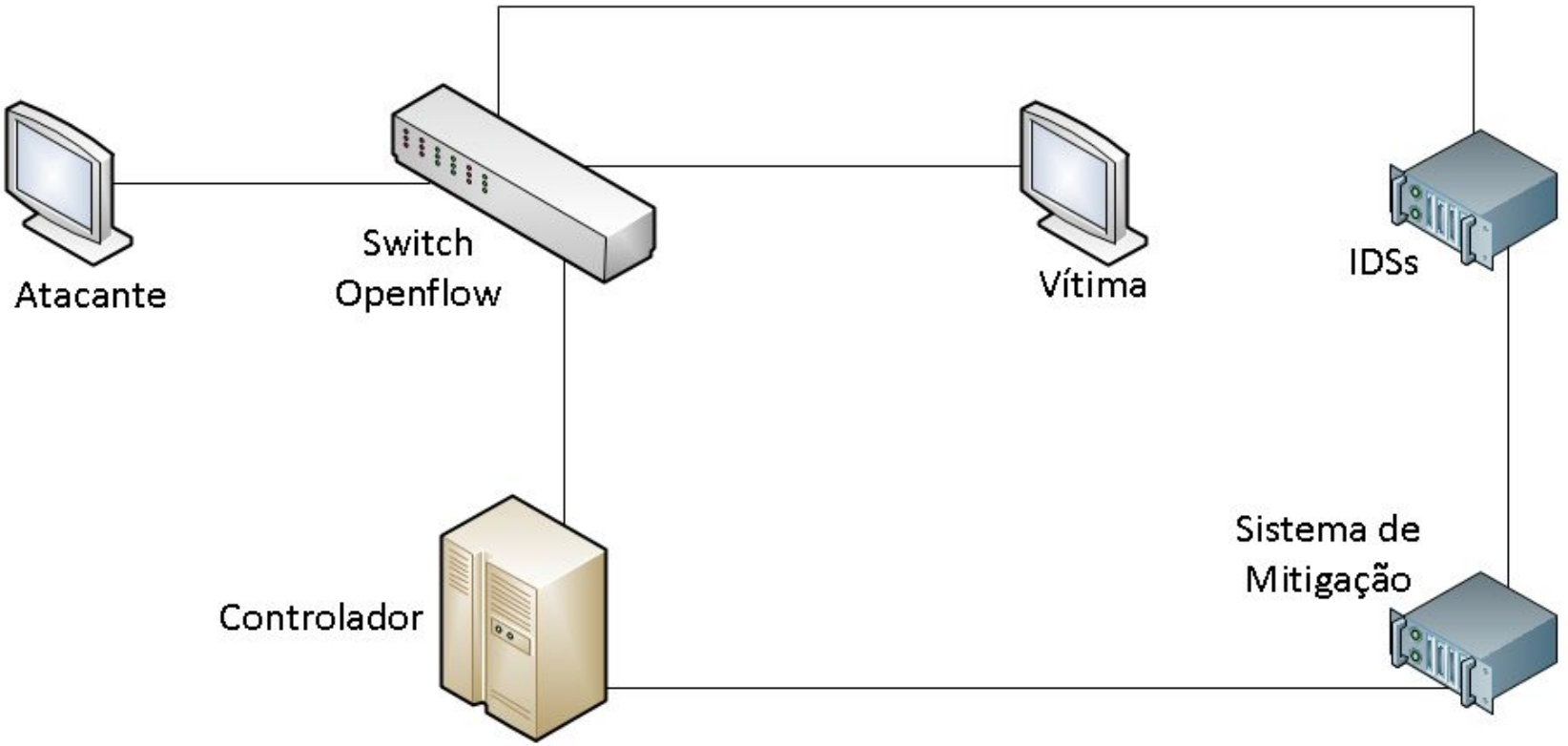
- Automatizar a mitigação por meio de SDN
  - Aliar a capacidade de detecção dos IDSs com a flexibilidade das SDNs
- Ser flexível
  - Aceitar diversos padrões de entrada de dados
  - Processar entradas conforme decisão do usuário
  - Realizar saída de dados para todos os dispositivos desejados pelo usuário

Arquitetura

Arquitetura utilizada

- Incorpora IDSs ou sistemas geradores de alertas
- Utiliza protocolo Openflow
- Atua nos elementos de comutação da rede para resposta a ataques

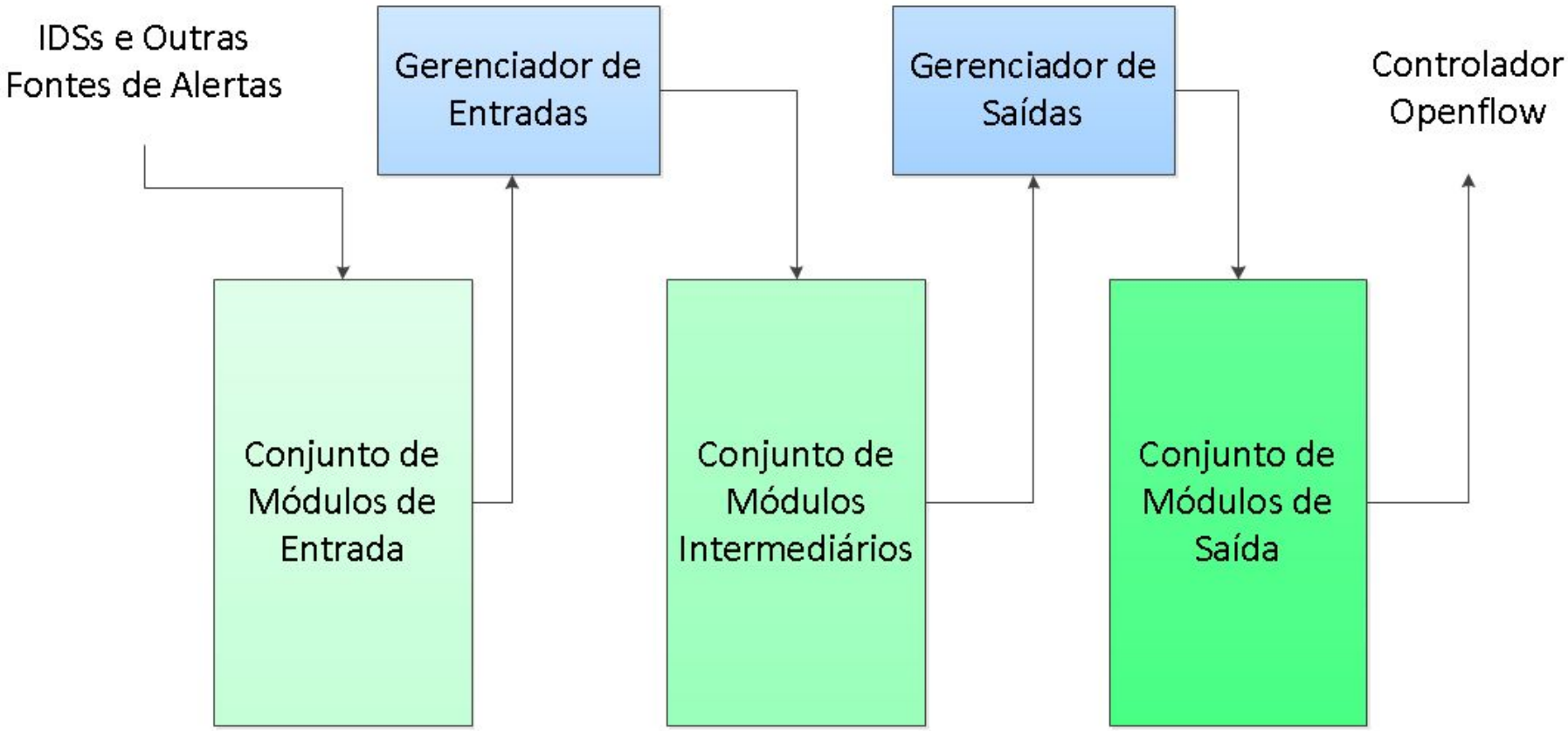
Arquitetura



Projeto

- Composição modular:
  - Permite a adição de novas funcionalidades
    - Fácil e rapidamente
    - Implementação simples de módulos
  - Flexibilidade de adaptação na rede
- Alto desempenho
  - Integração com controlador Floodlight na fase de desenvolvimento
- Portável
  - Implementado utilizando Java

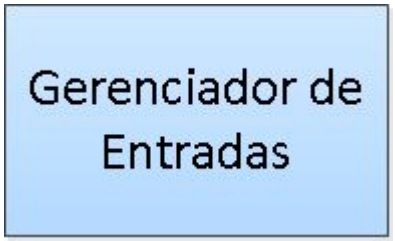
Projeto


IDSs e Outras Fontes de Alertas
Gerenciador de Entradas
Gerenciador de Saídas
Controlador Openflow
Conjunto de Módulos de Entrada
Conjunto de Módulos Intermediários
Conjunto de Módulos de Saída

Projeto

- Um módulo para cada tipo de entrada
- Permite diversas entradas de diversos elementos distintos
- Aceita múltiplos formatos

Projeto

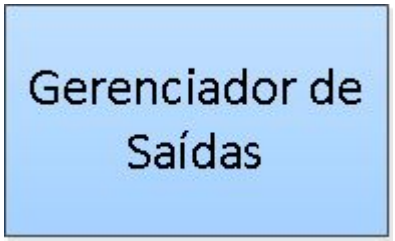


- Parte do núcleo da aplicação
- Organiza o fluxo de dados de entrada
- Redistribui os dados coletados para os módulos intermediários

Projeto

- Processa os dados de entrada recebidos
- Núcleo responsável pela tomada de decisões de mitigação
- Encaminha o resultado das entradas para o Gerenciador de Saída

Projeto

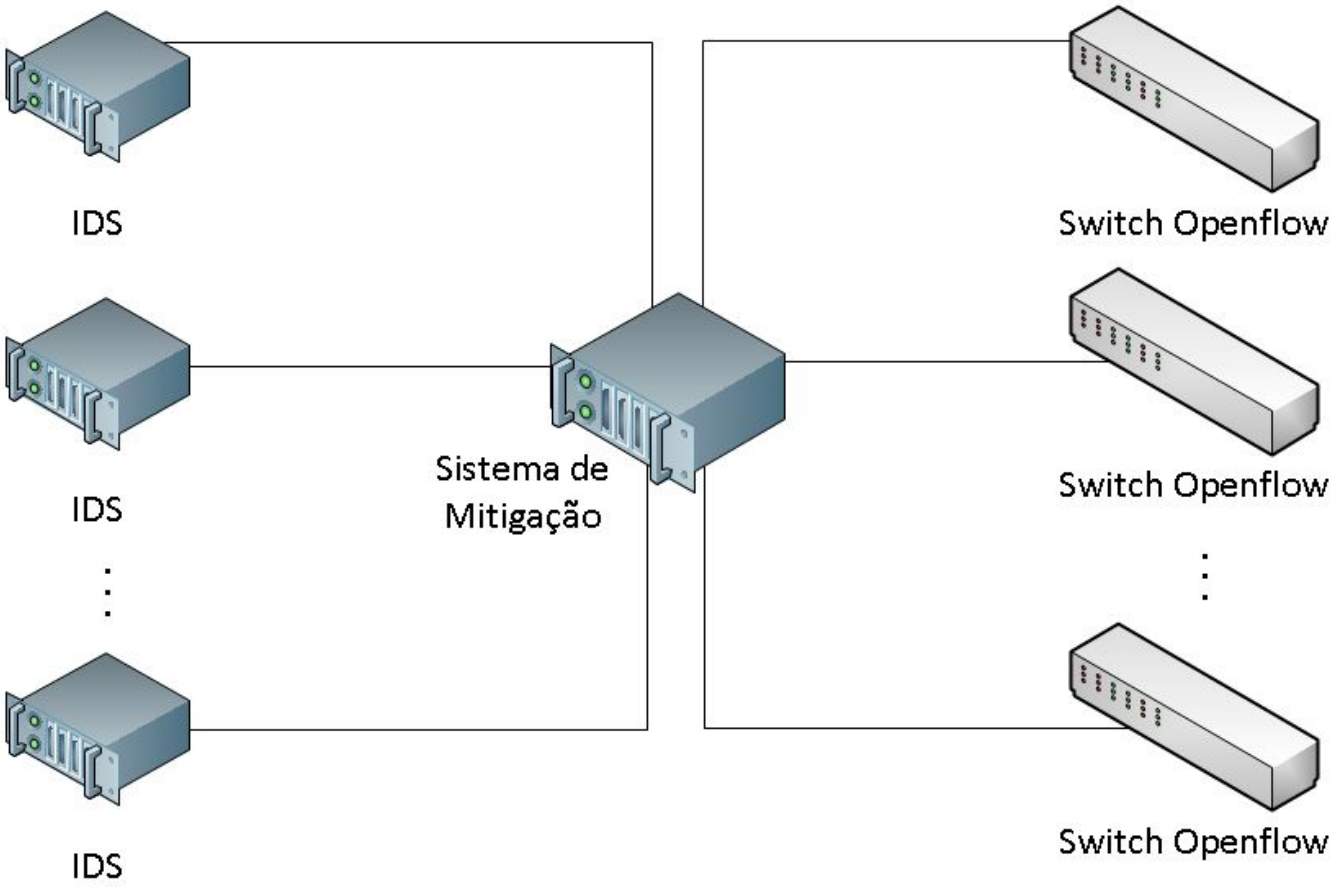


- Parte do núcleo da aplicação
- Coordena a chamada dos módulos de saída
- Redistribui os dados processados para a sua expotação ou armazenamento

Projeto

- Processa os dados para a saída do programa
- Responsável por formatar e enviar as regras para os controladores
- Permite a criação de alarmes de eventos, ou o armazenamento do histórico de eventos

Projeto



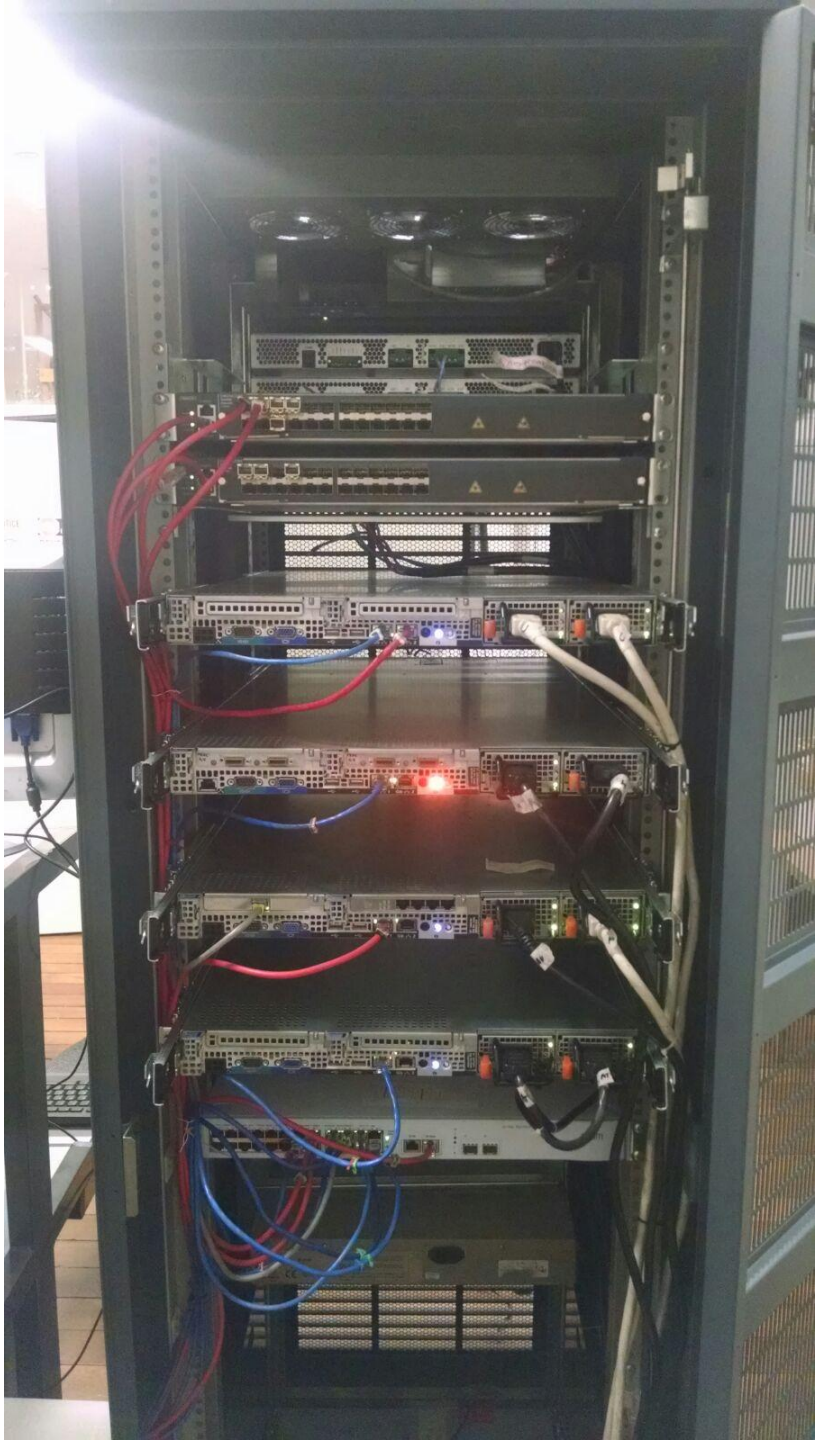
Multiplicidade de elementos de entrada e saída do Sistema de Mitigação

Aplicação

Prova de conceito da arquitetura proposta:

- Utilizada switch openflow Datacom
- Snort capturando fluxo do link do atacante
- Realizado Fin Scan de 100 portas
- Fluxo de dados via arquivos
  - Temporário, para prova de conceito
  - Gera pequeno atraso


DM4001
DATACOM
DM4001
DATACOM



Aplicação

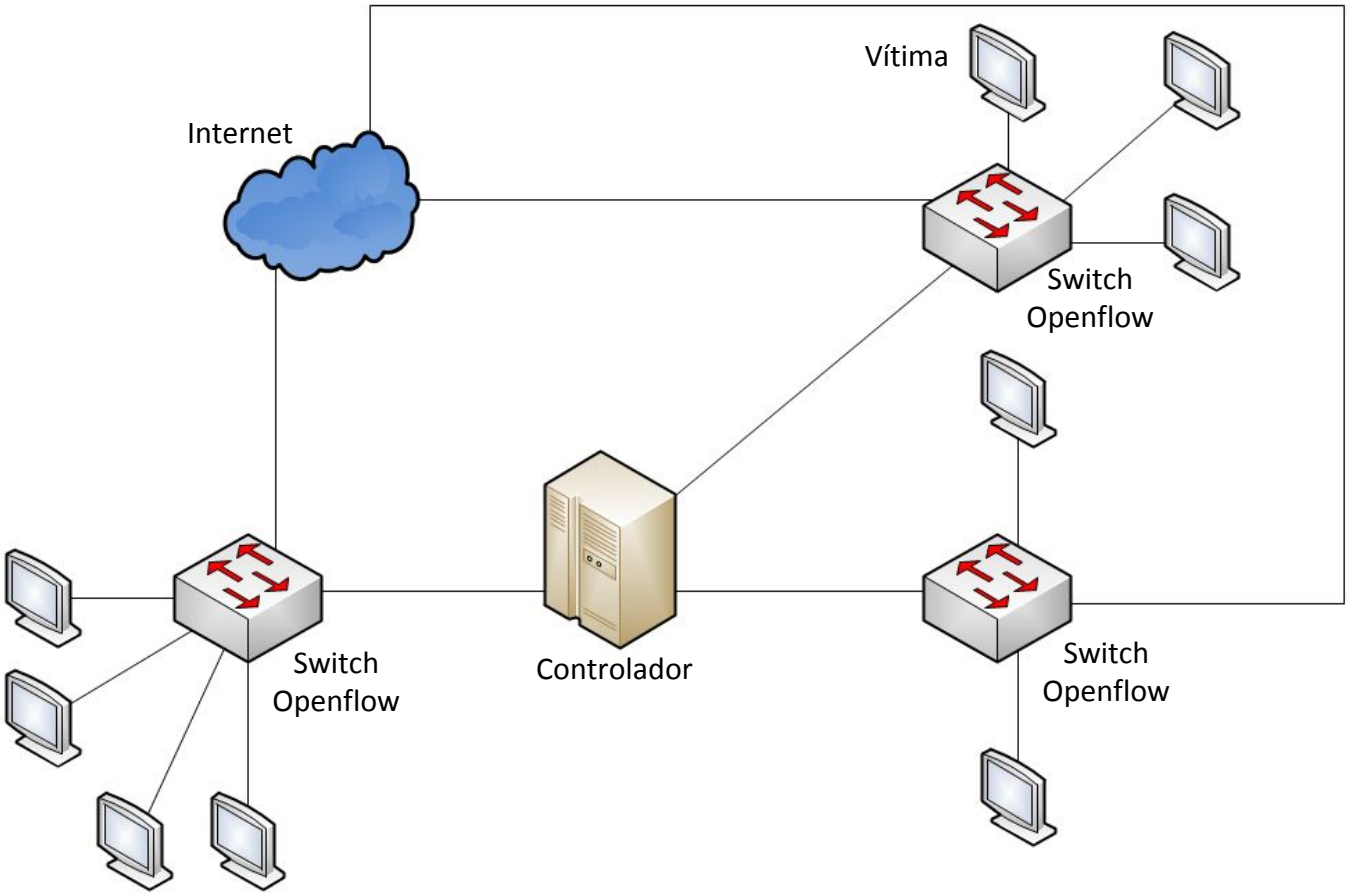
Vídeo
Prova de Conceito

Aplicação

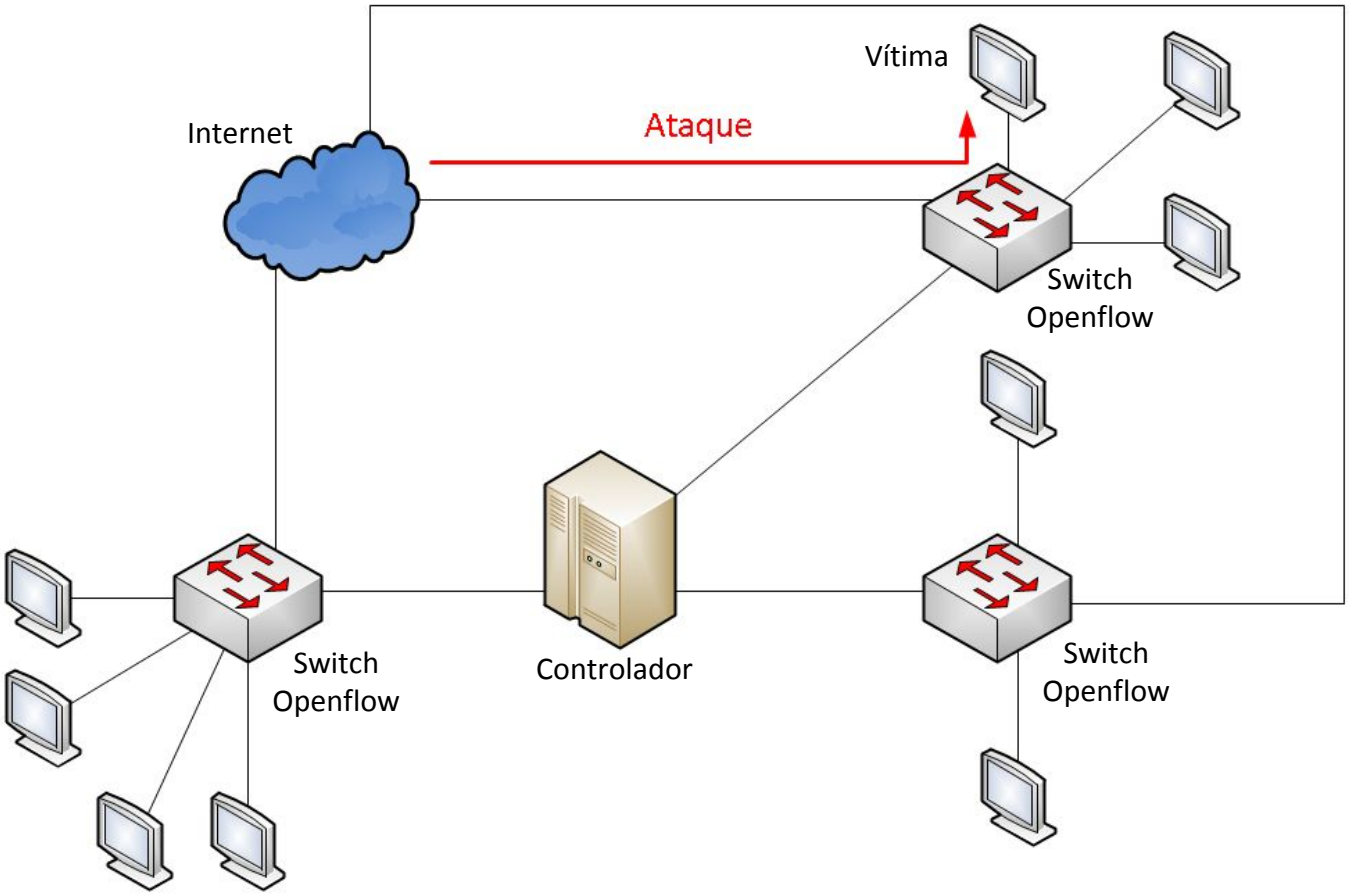
Aplicação do sistema para permitir o controle da segurança de diversas redes

- Um ataque em uma rede permite a segurança proativa nas demais redes controladas
- Melhor prevenção contra ataques

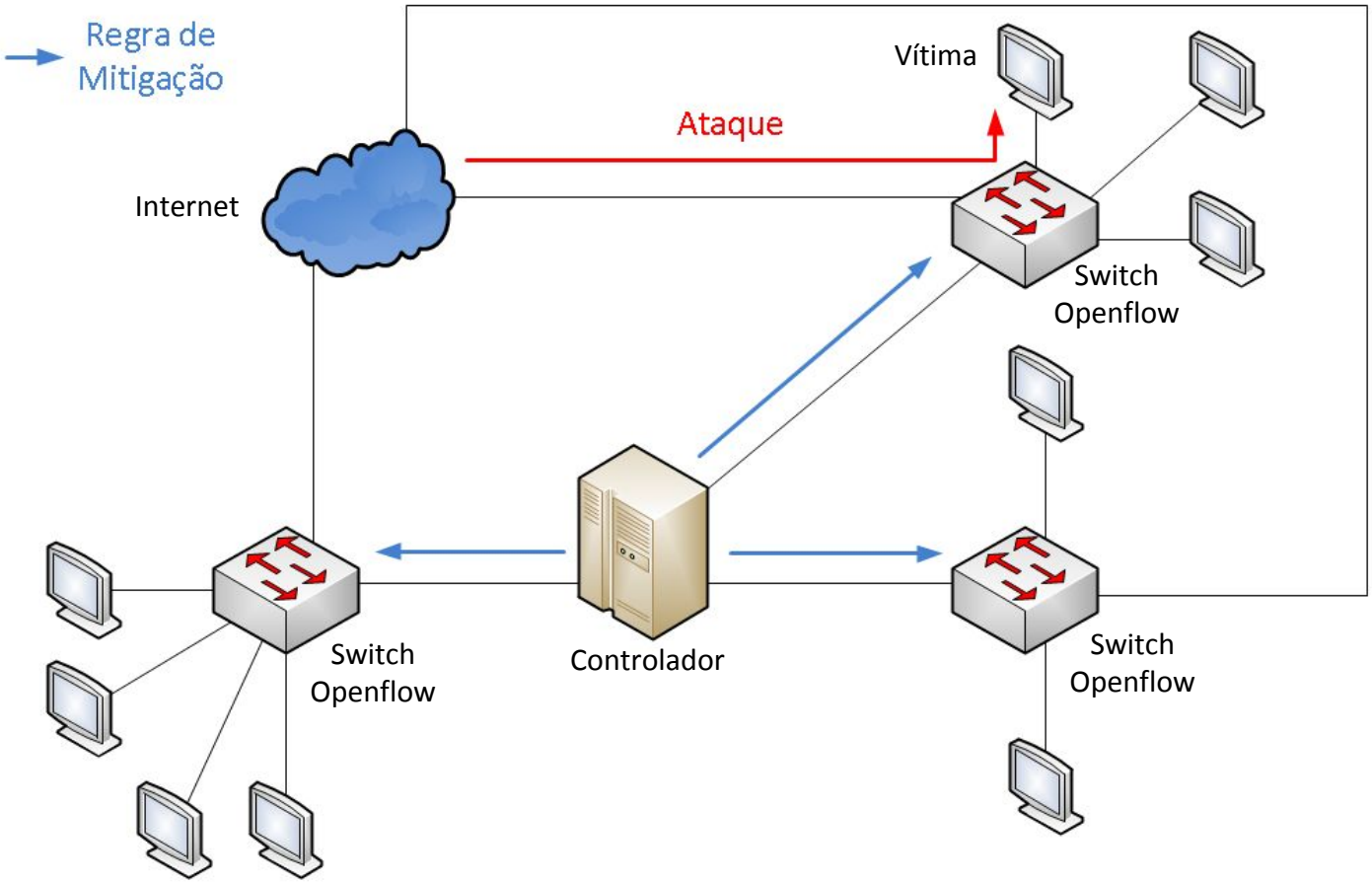
Aplicação


Vítima
Internet
Switch
Openflow
Switch
Openflow
Controlador
Switch
Openflow

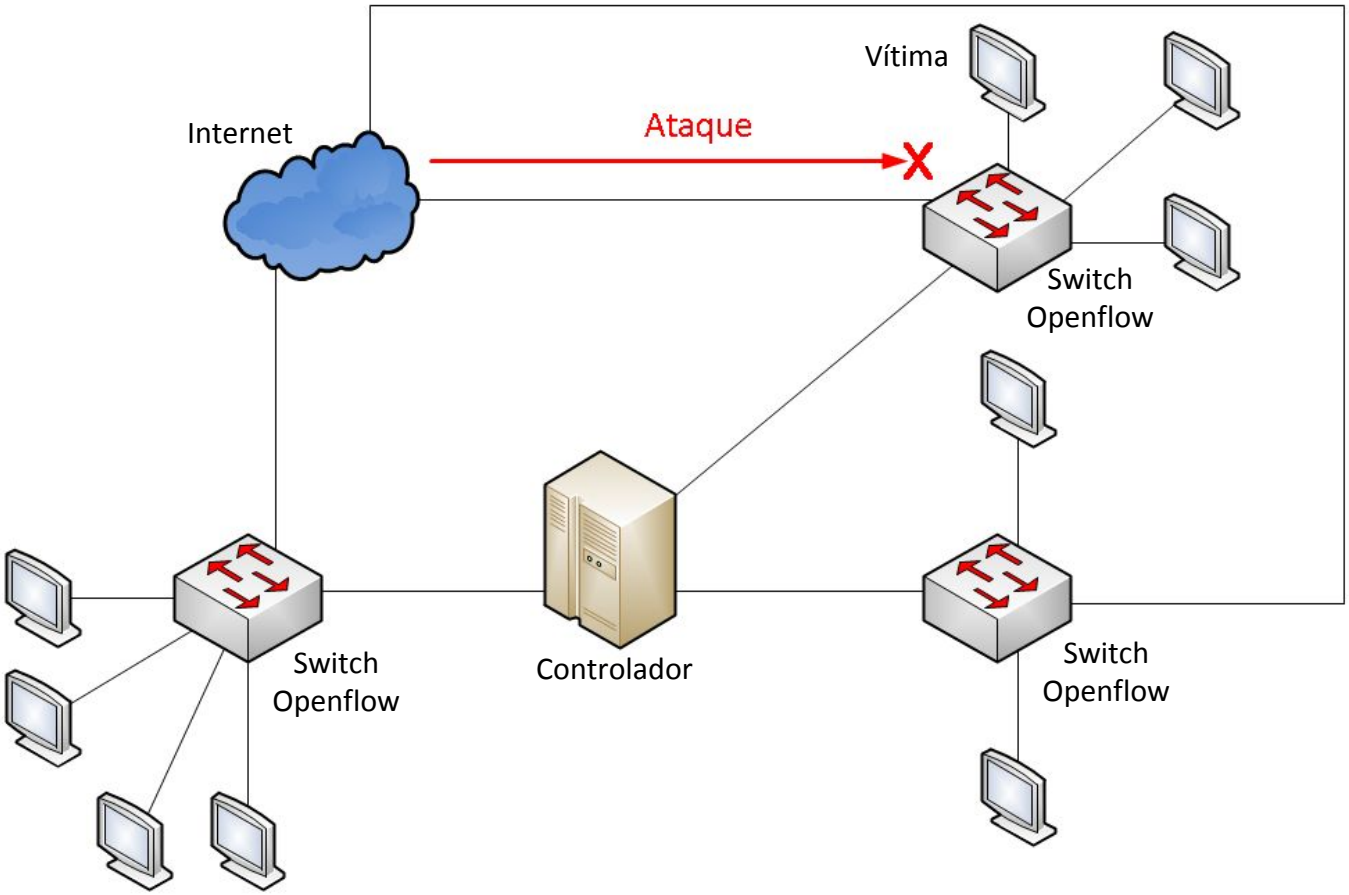
Aplicação


Vítima
Internet
Ataque
Switch
Openflow
Switch
Openflow
Controlador
Switch
Openflow

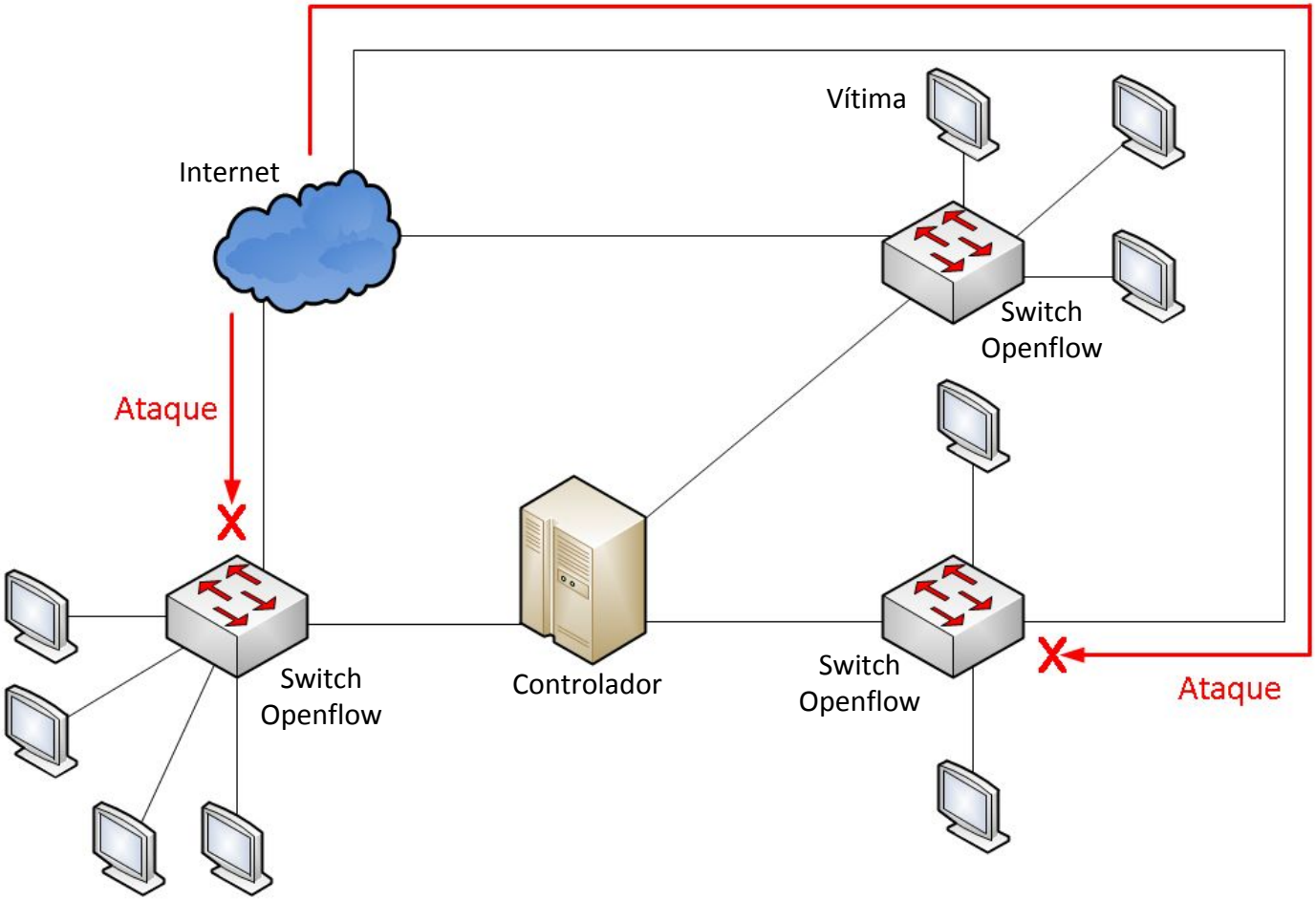
Aplicação


Regra de Mitigação
Vítima
Ataque
Internet
Switch Openflow
Controlador
Switch Openflow
Switch Openflow

Aplicação


Vítima
Internet
Ataque
Switch
Openflow
Switch
Openflow
Controlador
Switch
Openflow

Aplicação


Vítima
Internet
Switch
Openflow
Ataque
Switch
Openflow
Controlador
Switch
Openflow
Ataque

Conclusão

- Sucesso no uso de SDN para mitigação automatizada de ataques
  - Dados da aplicação de segurança permitiu a mitigação de ataque
- Sistema de Mitigação aceita:
  - Diversos padrões de entrada
  - Processamento de entradas customizável
  - Realiza saídas para os dispositívos e conforme o desejo do usuário

Agradecimentos

Instituto UNIEMP - Bolsa de estudos de iniciação científica em parceria com a DATACOM

NIC.BR pela oportunidade de apresentação

Obrigado!

Dúvidas?