



IX FÓRUM
R E G I O N A L
Incentivando o diálogo sobre os
Pontos de Troca de Tráfego Internet

Laboratório Virtual para Práticas de Redes e Segurança: estudo de caso do PoP-BA/UFBA com FIBRE

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

{italovalcy, adrianaavr}@ufba.br



FUTURE INTERNET
BRAZILIAN ENVIRONMENT
FOR EXPERIMENTATION

05 de Outubro de 2018 - Salvador - BA

Agenda

- Introdução
- A ferramenta SDN-IPS
- Práticas utilizando o SDN-IPS no FIBRE
- Conclusões e Trabalhos Futuros

Desafios no ensino/aprendizagem de Redes de Computadores e Segurança da Informação

- Desafio no processo de ensino/aprendizagem em Redes de Computadores e Segurança da Informação:
 - Conciliar teoria e prática
 - Limitações no ambiente de testes
 - Concorrência de recursos, restrições de local e horário de acesso
 - Ausência de equipamentos apropriados
- Alternativa: utilização de simuladores e emuladores
 - Dificuldade em testes de escalabilidade
 - Abstrações
 - Menor oportunidade de desenvolver habilidade de resolução de problemas

FIBRE

- Solução: utilização de ambientes de experimentação
 - FIBRE (*Future Internet Brazilian environment for Experimentation*)
 - Arquiteturas de redes
 - Protocolos
 - Aplicações

Potencializa experiência prática dos alunos

Ensino de Redes de Computadores

- *Software-Defined Networking:*
 - Auxílio no ensino de Redes de Computadores
 - Programabilidade da rede
 - Modelagem de redes em grafos
 - Programação de funções de rede
 - Definição de APIs para gerenciamento de redes pelos operadores
 - Independe de fabricantes

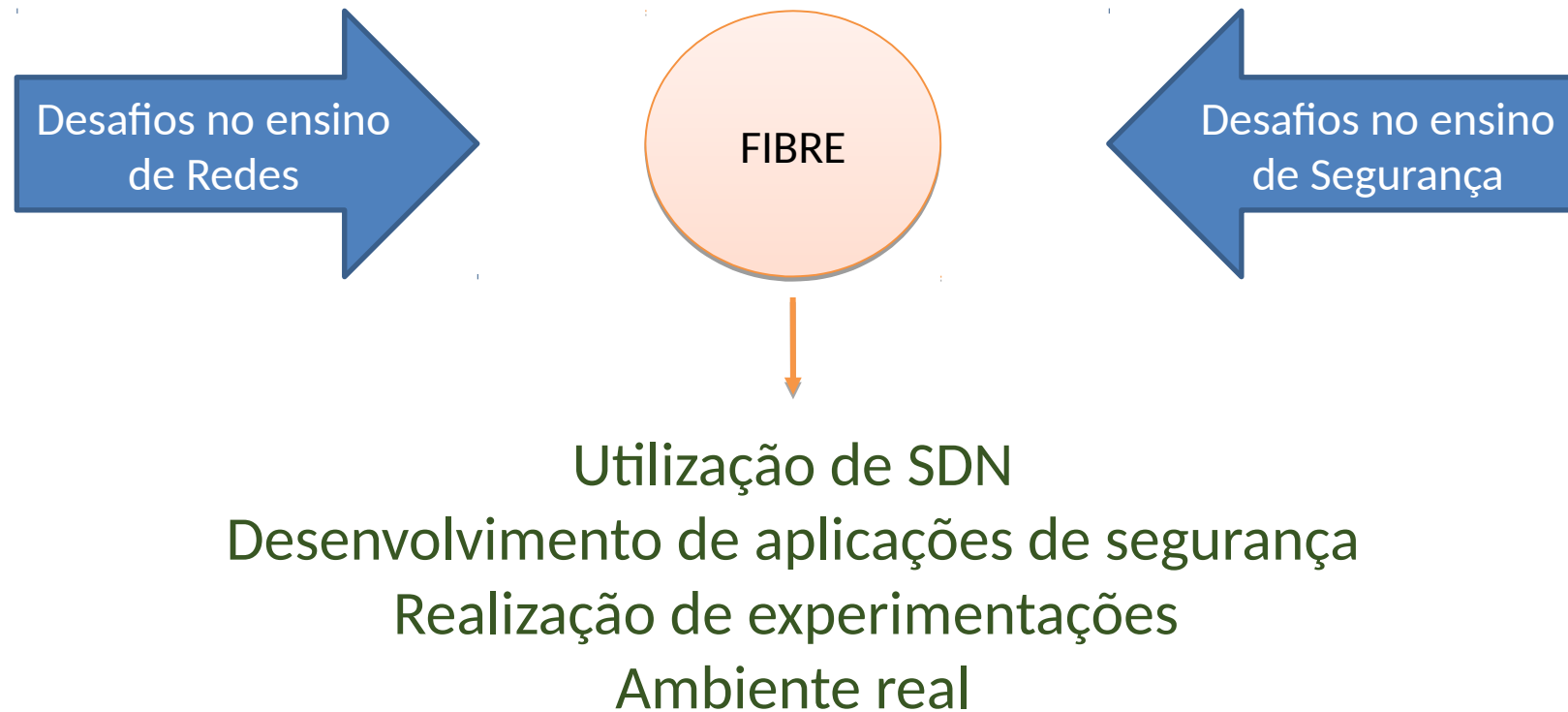
Utilização de equipamentos OpenFlow no FIBRE

Ensino de Segurança da Informação

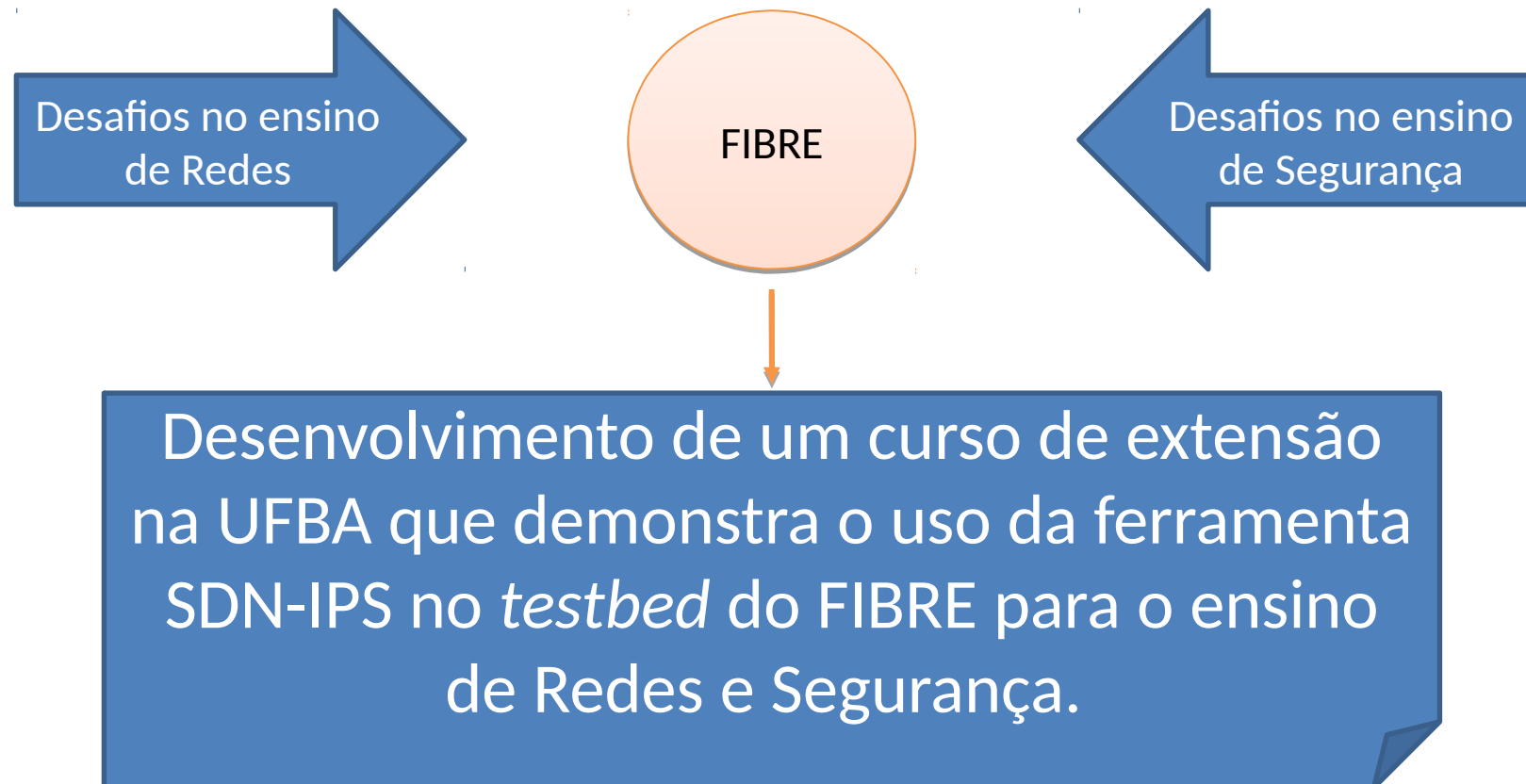
- Desafios:
 - Apresentar os princípios, diversidade de ataques e mecanismos de detecção e defesa
 - Necessidade de um ambiente de testes controlado
 - Conscientização em testes de Segurança da Informação:
 - Ética
 - Ambiente controlado
 - Autorização
 - Cuidado com danos

Desenvolvimento de aplicações de segurança com SDN, testadas em ambientes de experimentação

Ensino de Redes e Segurança utilizando o FIBRE



Ensino de Redes e Segurança utilizando o FIBRE

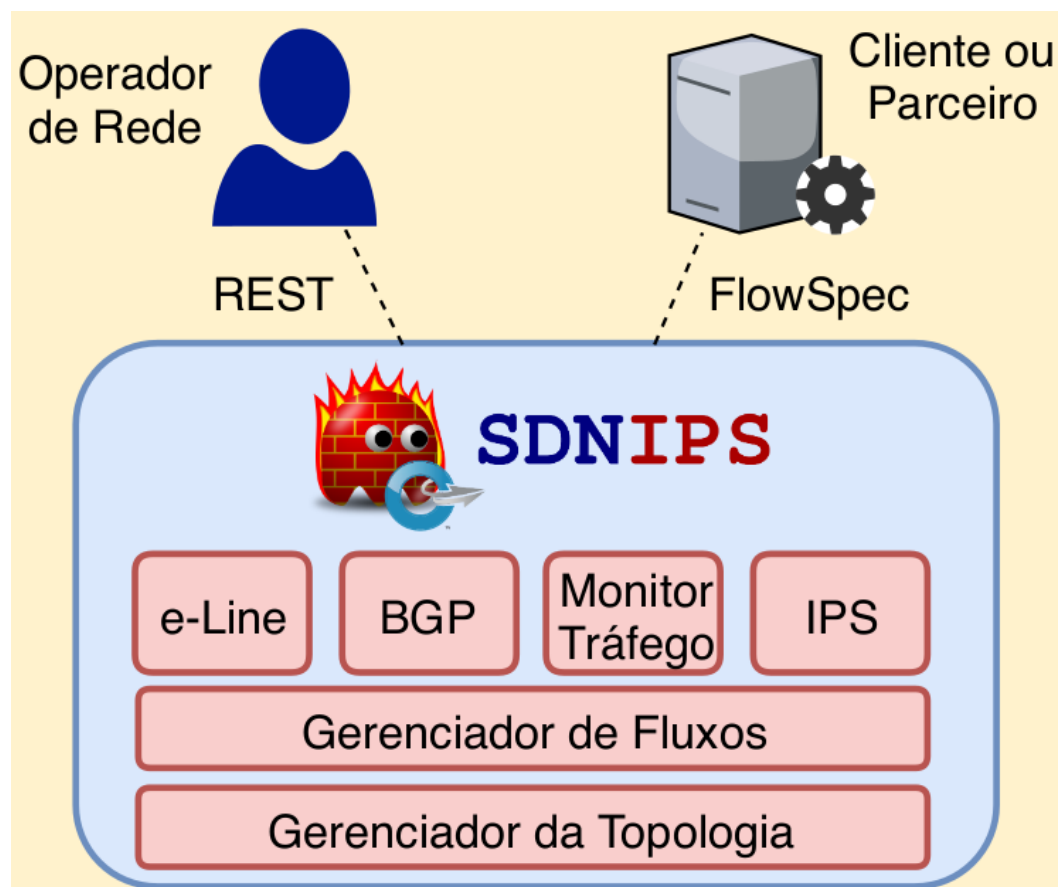


A Ferramenta SDN-IPS

- IPS (*Intrusion Prevention System*) baseado em OpenFlow
- Realiza orquestração da rede
- Provê capacidade de detecção e prevenção de intrusos
- Provê contenção contra ataques



A arquitetura do SDN-IPS



- Gerenciador de Topologia
- Gerenciador de Fluxos
- Espelhamento de Tráfego
- Contenção de Ataques
- Contenção Colaborativa
- Outras aplicações (BGP + e-Line)

Arquitetura do SDN-IPS e aprendizado

- Gerenciador de Topologia
 - Modelagem da rede em grafos
- Gerenciador de Fluxos
 - Funcionamento da tabela de fluxos e roteamento
 - Checagem de consistência dos fluxos
 - OpenFlow
- Espelhamento de tráfego
 - Modificações nas tabelas de fluxos e tipos de espelhamento de tráfego
 - Encapsulamento do tráfego
 - Sistema de Detecção de Intrusos
 - Análise de tráfego

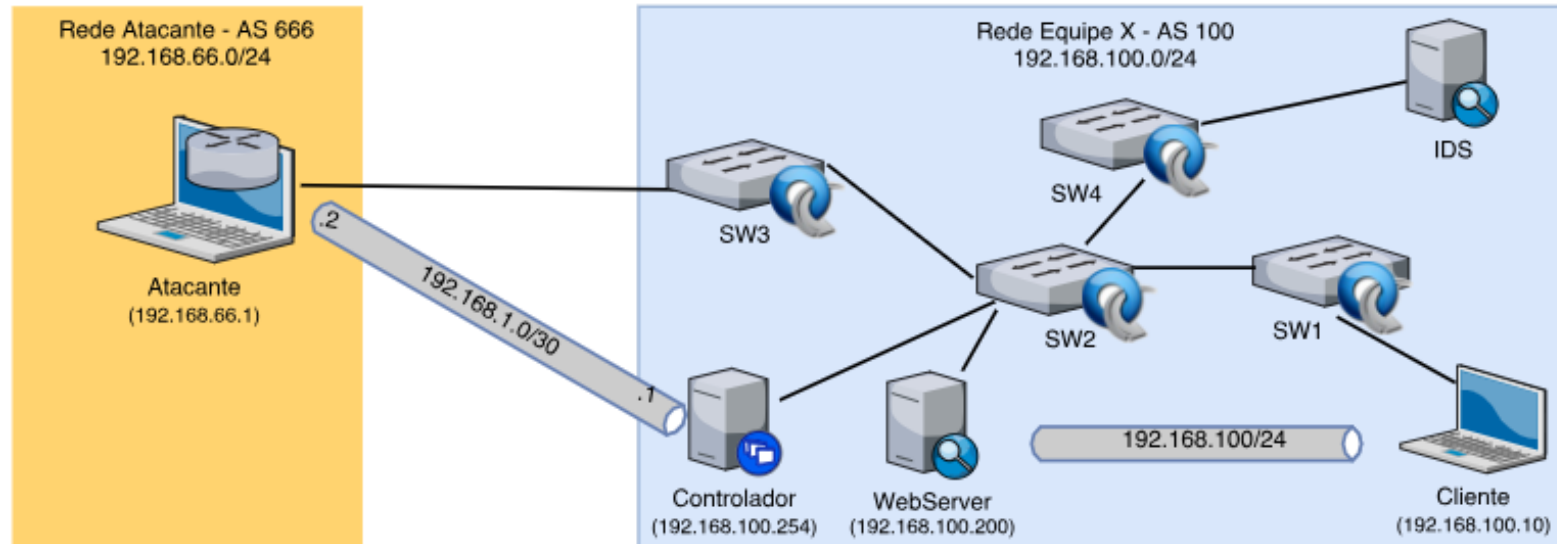
Arquitetura do SDN-IPS e aprendizado

- Contenção de Ataques
 - VLAN
 - Conceitos de Firewall, NAT
 - Gerenciamento de tabelas de conexões
 - Estratégias de contenção
- 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

Topologia da Rede



- Dois ASes
- AS 100 orquestrado pelo SDN-IPS
- AS 666 com ferramentas de roteamento tradicionais

Etapas de experimentação

- Configuração do ambiente e conectividade
- Roteamento interdomínio
- Configuração do IDS
- Mecanismos de contenção

Configuração do ambiente e conectividade

The screenshot displays the OFELIA web interface for slice management. It is divided into several sections:

- Slice Slice [redacted] in Project Curso SDN-IPS UFBA 2018-03**: Shows a table with slice status and management options.
- Physical topology**: A network diagram showing a central node connected to four peripheral nodes.
- Network resources**: Details for the 'UFBA Openflow' aggregate, including requested and granted flowspace, and associated OpenFlow switch interfaces.
- Virtualization Resources**: A detailed view of the 'UFBA Virtualization' aggregate, listing VMs and their configurations.

Slice status	Description	Management
✔	Exercício 1.0	Update Slice Stop Slice

Physical topology
Selected Virtualized server: UFBA_Whitebox3 at Salvador - BA

Network resources
• OpenFlow Aggregate: UFBA Openflow

Name: UFBA Openflow
Status: ✔
Automatic approval: ✔
Physical location: Salvador - BA
Resources:

Requested Flowspace (1) [More Information](#)
Granted Flowspace (1) [More Information](#)

Flowspace	Associated OpenFlow Interfaces
VLAN ID: 863 - 864	OpenFlow Switch: 00:00:0c:c4:7a:5e:98:95 - Port 4
	OpenFlow Switch: 00:00:0c:c4:7a:5e:98:95 - Port 5534
	OpenFlow Switch: 00:00:0c:c4:7a:5e:98:95 - Port 1
	OpenFlow Switch: 00:00:0c:c4:7a:5e:98:95 - Port 2
	OpenFlow Switch: 00:00:0c:c4:7a:5e:98:95 - Port 3
	OpenFlow Switch: 00:00:0c:c4:7a:5e:98:94 - Port 4
	OpenFlow Switch: 00:00:0c:c4:7a:5e:98:94 - Port 5534
	OpenFlow Switch: 00:00:0c:c4:7a:5e:98:94 - Port 3
	OpenFlow Switch: 00:00:0c:c4:7a:5e:95:65 - Port 3
	OpenFlow Switch: 00:00:0c:c4:7a:5e:95:65 - Port 5534
	OpenFlow Switch: 00:00:0c:c4:7a:5e:95:64 - Port 2
	OpenFlow Switch: 00:00:0c:c4:7a:5e:95:64 - Port 3

Openflow controller: Update controller

Actions: Define flowspace (virtual location)

Virtualization Resources
• Virt. Aggregate: UFBA Virtualization

Name: UFBA Virtualization
Status: ✔
Physical location: Salvador - BA
Resources:

Server Name	Virt. Tech.	Operating System	CPU	Memory	Disc	Update
UFBA_Whitebox1	XEN	GNU/Linux Debian (7.0)	None	None	None	Update
VM Name	State	Operating System	Memory	Mgmt IP	Actions	Update Status
cliente	stopped	GNU/Linux Debian (8.0)	256	<input type="text"/>	Start Delete	Update
SSH common details: to access as root just type <code>su</code> inside (password: your user password)						

Server Name	Virt. Tech.	Operating System	CPU	Memory	Disc	Update
UFBA_Whitebox2	XEN	GNU/Linux Debian (7.0)	None	None	None	Update
VM Name	State	Operating System	Memory	Mgmt IP	Actions	Update Status
controlador	stopped	GNU/Linux Debian (8.0)	1024	<input type="text"/>	Start Delete	Update
webserver	stopped	GNU/Linux Debian (8.0)	256	<input type="text"/>	Start Delete	Update
SSH common details: to access as root just type <code>su</code> inside (password: your user password)						

Server Name	Virt. Tech.	Operating System	CPU	Memory	Disc	Update
UFBA_Whitebox3	XEN	GNU/Linux Debian (7.0)	None	None	None	Update
VM Name	State	Operating System	Memory	Mgmt IP	Actions	Update Status
atacante	stopped	GNU/Linux Debian (8.0)	512	<input type="text"/>	Start Delete	Update
SSH common details: to access as root just type <code>su</code> inside (password: your user password)						

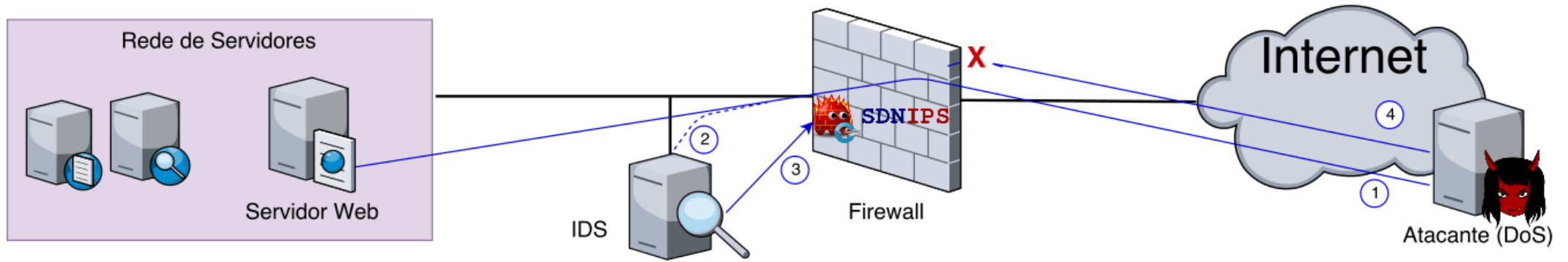
Server Name	Virt. Tech.	Operating System	CPU	Memory	Disc	Update
UFBA_Whitebox4	XEN	GNU/Linux Debian (7.0)	None	None	None	Update
VM Name	State	Operating System	Memory	Mgmt IP	Actions	Update Status
ids	stopped	GNU/Linux Debian (8.0)	512	<input type="text"/>	Start Delete	Update
SSH common details: to access as root just type <code>su</code> inside (password: your user password)						

Actions: Create a new virtual machine in server: UFBA_Whitebox1 Create VM

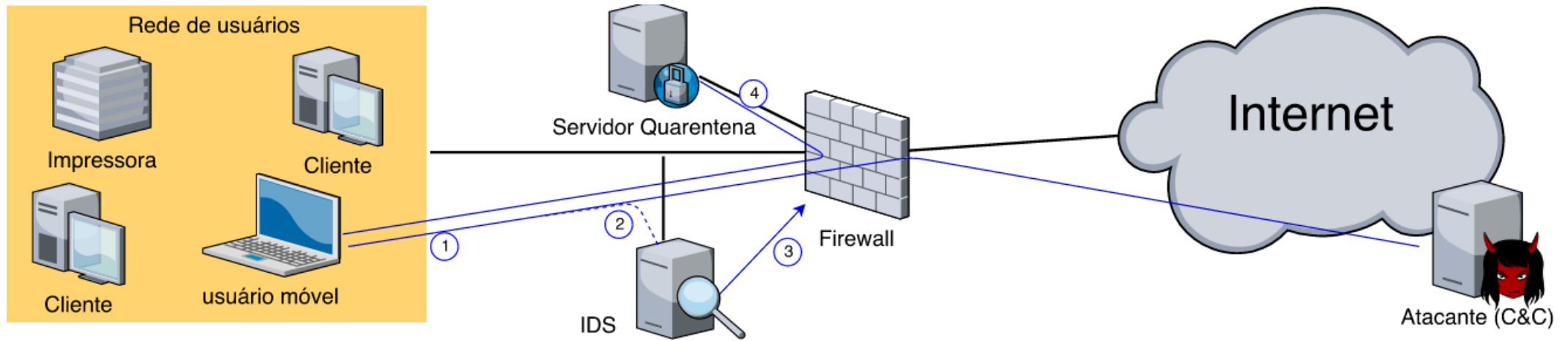
Mecanismos de Contenção

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

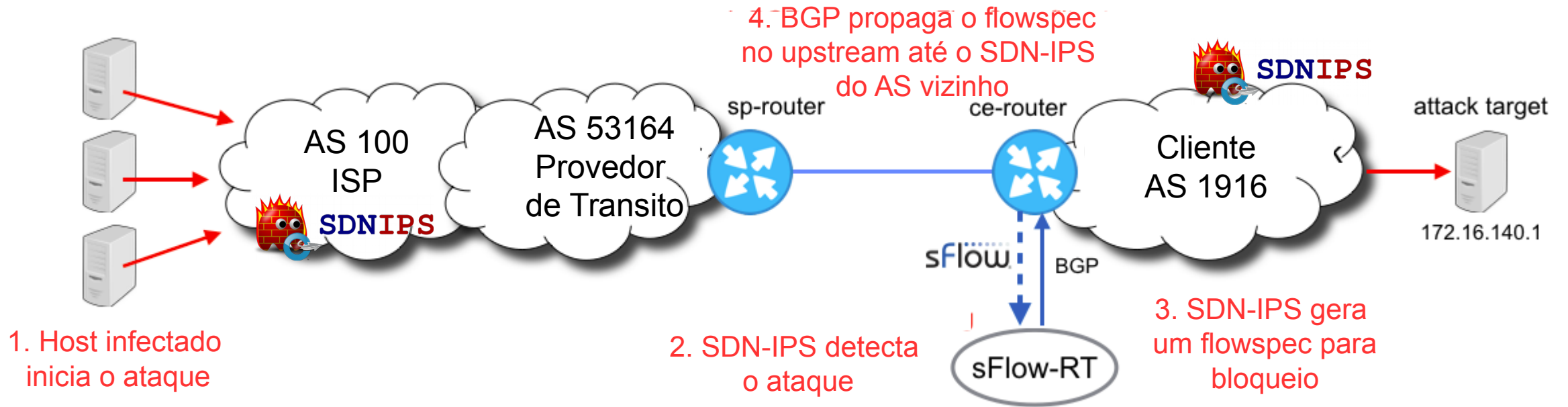
Contenção via Bloqueio de tráfego



Contenção via Quarentena



Contenção Colaborativa



Curso semi-presencial de Prevenção de Intrusão baseado em SDN



Curso semi-presencial de Prevenção de Intrusão baseado em SDN

Curso SDN/IPS

Accessibility

Search forums

Latest announcements

Problema de configuração

Ilha UFPE

Older topics ...

General



SDNIPS

Sistema de Prevenção de Intrusão baseado em SDN/OpenFlow

Sejam bem-vindos
Vejam abaixo os avisos e links

- Fórum de discussões
- Plano de Ensino
- Instrutores do curso
- Links úteis
- Material de apoio curso SDN/IPS
- Atividade avaliativa inicial

Fórum de discussões

Discussion	Started by	Replies	Last post
Ilha RNP Brasília Problema	[User]	2	Sat, 24 Mar 2018, 10:59 PM
Correções ou melhorias nos roteiros de laboratório	[User]	6	Sat, 24 Mar 2018, 9:36 PM
Problema de configuração	[User]	6	Sat, 24 Mar 2018, 8:40 PM
Configuração	[User]	4	Fri, 23 Mar 2018, 6:42 PM
Ilha UFPE	[User]	2	Fri, 23 Mar 2018, 6:29 PM
Acesso ao ambiente de experimentação	[User]	31	Wed, 14 Mar 2018, 8:54

Testemunho dos alunos

- Uma boa avaliação do curso em relação ao conteúdo e aos instrutores
- Uma boa avaliação em relação ao uso do FIBRE para aprendizado
 - Permitir relacionar os conceitos teóricos no ambiente de experimentação
 - Realizar *troubleshooting*
 - Velocidade na alocação de recurso
- Pouco conhecimento em relação ao FIBRE
- **Necessidade de mais cursos desse tipo**

Desafios e Lições Aprendidas durante o curso

- Problemas nas ilhas do FIBRE
 - Limitações de *matches* e *actions* no Flowvisor (e.g. ip tos, vlan pcp, etc)
 - Falha no isolamento de experimentos entre slices (e.g. devido à app ou ao controlador)
- Resolução de problemas e visibilidade do switch OpenFlow
- Problemas com o funcionamento do datapath OpenFlow

Conclusões e Trabalhos Futuros

- O artigo apresentou um relato de experiências no uso do FIBRE e do SDN-IPS no ensino de redes e segurança na UFBA
- Foi possível viabilizar uma aprendizagem progressiva, consistente e com foco em problemas reais
- As lições aprendidas e os feedbacks demonstram que é necessário um equilíbrio entre teoria e prática
- O uso de testbeds como o FIBRE abre novas perspectivas para o ensino
- Pretende-se fazer mais cursos como esse e colaborar com o FIBRE na melhoria do projeto, além de incentivar o uso do FIBRE junto às instituições de ensino

Publicações, Palestras e Oficinas

- SDN-IPS
 - Melhor ferramenta no Salão de Ferramentas do SBRC
 - http://www.sbrc2018.ufscar.br/wp-content/uploads/2018/04/180613_1.pdf
 - Apresentação no Workshop FIBRE – CSBC 2018
 - Palestra/Tutorial no LACNIC/LACNOG 2018
- Nova edição da oficina utilizando o FIBRE prevista para Nov/2018
 - Diversos outros treinamentos no NEXT STI-UFBA

Agradecimentos



Obrigada!



IX FÓRUM REGIONAL

Incentivando o diálogo sobre os
Pontos de Troca de Tráfego Internet

{italovalcy, adrianaavr}@ufba.br