Experiências com uso da ferramenta SDN-IPS no testbed FIBRE para práticas de ensino de redes e cibersegurança

Italo Valcy S. Brito[1], **Adriana Viriato Ribeiro**[1], **Leobino N. Sampaio**[1]

[1]Programa de Pós Graduação em Ciência da Computação (PGCOMP)
Universidade Federal da Bahia (UFBA)
Salvador – BA – Brasil

{italovalcy,adrianavr,leobino}@ufba.br

Abstract. *The harmonious use of theory and practice for teaching computer networks and security is challenging and paramount. The balance between theoretical principles and experimentation plays a key role to produce accessible methods for students to build up their knowledge. Thus, the use of testbed environments for education purposes benefits the learning process, providing experiences beyond traditional practices in restricted or emulated scenarios. This paper presents a study-case related to the use of FIBRE testbed and SDN-IPS application in a semi-distance course of networks and security. The evaluation demonstrates that such actions produced excellent results and helped students in their academic and professional career.*

Resumo. *Um desafio no ensino de Redes e Cibersegurança é a conciliação entre teoria e prática. A partir do equilíbrio entre os princípios teóricos e a experimentação tem-se, de fato, métodos acessíveis ao aluno para melhor aquisição do conhecimento. Nesse sentido, o uso de ambientes de testbed, como o FIBRE, para fins de educação enriquece o processo de ensino e aprendizagem, proporcionando experiências que vão além das práticas convencionais em cenários restritos ou emulados. Este artigo apresenta um relato de experiências no uso do FIBRE e da ferramenta SDN-IPS na execução de um curso semi-presencial de redes e segurança. O feedback dos alunos mostra a importância de ações como essa no seu processo de formação.*

1. Introdução

Um dos principais desafios no processo de ensino e aprendizagem de Redes de Computadores e Segurança da Informação é a conciliação dos conceitos abordados em aula com a prática nos laboratórios [Kaabi et al. 2016, Xu et al. 2014]. A partir do equilíbrio entre os princípios teóricos e a experimentação tem-se, de fato, métodos acessíveis ao aluno para aprendizado dessas áreas [Kurose and Ross 2013]. Não obstante, as limitações no ambiente de testes, a concorrência pelo uso de recursos, as restrições de local e horário de acesso e até mesmo a ausência de equipamentos apropriados limitam a aplicação de atividades práticas. Mesmo com o uso de emuladores ou recursos locais da instituição, os alunos ficam restritos à testes em pequena escala ou deixam de desenvolver a capacidade de resolução de problemas que tipicamente ocorrem em ambientes reais [Xu et al. 2014].

Nesse contexto, a utilização de ambientes de experimentação pode auxiliar a aplicação de metodologias didático-pedagógicas com foco no uso de laboratórios práticos

para ensino de redes e segurança. O FIBRE (do inglês, *Future Internet Brazilian environment for Experimentation*) é uma estrutura de experimentação que permite que estudantes, professores e pesquisadores testem novas arquiteturas de redes, protocolos e aplicações em condições próximas ao mundo real, podendo ser utilizado para potencializar a experiência prática dos alunos [Ciuffo et al. 2016].

No que tange ao ensino de Redes de Computadores, o surgimento do paradigma de Redes Definidas por Software (do inglês, *Software-Defined Networking* – SDN) [Kreutz et al. 2014], por exemplo, abre diversas perspectivas para criação de objetos de aprendizagem para os alunos, como a metodologia de modelagem da rede em grafos, a programação de funções de rede no controlador ou ainda a definição de APIs para gerenciamento da rede pelos operadores. A programabilidade da rede permite que o estudante implemente e teste diversas funcionalidades independente de fabricantes, culminando em um melhor entendimento dos conceitos e das aplicações. Em relação à Segurança da Informação, apresentar os princípios, diversidade de ataques e mecanismos de detecção/defesa, combinando teoria e prática em ambiente controlado, constitui-se um grande desafio ao professor [Xu et al. 2014]. Além disso, há uma preocupação em educar os alunos para que, ao realizar testes de segurança, o façam de forma ética, controlada, autorizada e sem causar quaisquer danos à terceiros [Kaabi et al. 2016].

Tendo em vista os desafios e oportunidades supracitados e considerando a importância do equilíbrio entre teoria e prática, foi desenvolvido um curso de extensão na Universidade Federal da Bahia (UFBA) que demonstra o uso da ferramenta SDN-IPS e do *testbed* FIBRE no ensino de redes e segurança. O conteúdo do curso aborda desde assuntos básicos como configuração de endereços de rede e VLAN, a assuntos mais avançados, como roteamento interdomínio com BGP e funcionamento de uma arquitetura SDN. O curso contempla ainda temas de Segurança da Informação, como: ferramentas para detecção de atividade maliciosa, caracterização de ataques e construção de um Sistema de Prevenção de Intrusos (IPS) baseado em SDN. Este artigo, portanto, apresenta um relato de experiências na realização do curso e no uso do SDN-IPS e do FIBRE para fins didático-pedagógicos, como mecanismos auxiliares nas práticas de ensino.

Este artigo está organizado da seguinte forma: a Seção 2 expõe a arquitetura e as funcionalidades do SDN-IPS. A Seção 3 descreve o uso do FIBRE na execução dos experimentos com a ferramenta. A Seção 4 relata os desafios, experiências e lições aprendidas na realização do curso. E a Seção 5 discute as conclusões e trabalhos futuros.

2. A Ferramenta SDN-IPS

O SDN-IPS pode ser visto como um IPS baseado em OpenFlow cuja finalidade é orquestrar a rede e prover capacidade de detecção e contenção de ataques. Sua arquitetura é apresentada na Figura 1, cujos principais módulos são descritos a seguir:

- **Gestão da topologia (*Topology Manager*)**: Este módulo é responsável pela modelagem da rede na forma de um grafo dirigido. Utilizando a biblioteca NetworkX e a aplicação LLDP para descoberta de links, o SDN-IPS consegue mapear toda a topologia da rede, atributos do enlace, dentre outros. O estudo sobre a modelagem da rede em um grafo, com suas propriedades e algoritmos, constitui-se um importante objeto de aprendizagem para estudantes de redes de computadores.

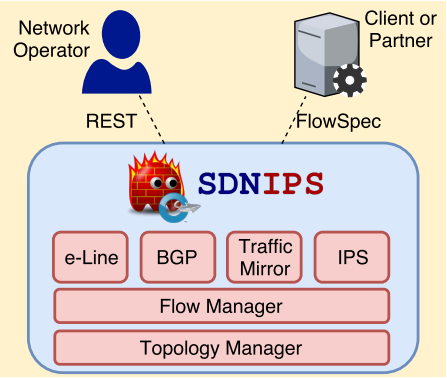

Figura 1. Diagrama da Arquitetura da SDN-IPS.

- **Gestão de Fluxos (*Flow Manager*)**: Realiza o armazenamento e checagem da consistência dos fluxos instalados em cada *switch*. O SDN-IPS utiliza a lista de fluxos para modificá-los frente à uma solicitação de contenção na rede. A gestão da tabela de fluxos, checagem de consistência e modo proativo versus reativo do OpenFlow são alguns dos temas explorados em sala de aula com os alunos.
- **Espelhamento de Tráfego (*Traffic Mirror*)**: Permite que o operador da rede faça o espelhamento de tráfego com base nos fluxos de um *switch* para um equipamento remoto, tipicamente um IDS, para análise de tráfego malicioso. Através da integração com o IDS, o SDN-IPS recebe alertas de detecção de ataques e realiza ações de contenção. Este módulo destaca-se pelo desafio apresentado aos alunos de modificação das ações na tabela de fluxos para espelhamento do tráfego, bem como o desafio de encapsulamento do tráfego para encaminhamento remoto.
- **Contenção de ataques (IPS)**: O SDN-IPS implementa diversos mecanismos para contenção de ataques: bloqueio (*drop*); limitação de banda e de requisições (*rate-limit*); e redirecionamento de tráfego para VLAN de quarentena. Em particular, a estratégia de quarentena desperta atenção nos alunos em relação à sua implantação, visto que se baseia em uma tradução de endereços de rede com o desafio de utilizar uma tabela de fluxos OpenFlow *stateless*. Este módulo oportuniza a revisão de conceitos de Firewall, NAT e gerenciamento da tabela de conexões e permite a correlação entre esses conceitos e a arquitetura SDN/OpenFlow.
- **Contenção colaborativa**: Através do BGP FlowSpec [Marques et al. 2009], o SDN-IPS permite que clientes e parceiros solicitem a contenção de ataques, provendo um serviço colaborativo de bloqueio remoto de atividade maliciosa. Além de permitir aprofundamento em temas como BGP e FlowSpec, esse módulo aborda ainda os desafios da validação do pedido de bloqueio pelos clientes.
- **Outras aplicações (BGP e e-Line)**: O SDN-IPS pode ser integrado com outras aplicações no controlador SDN. Em particular, dois módulos pré-integrados ao SDN-IPS são: i) roteamento interdomínio através do protocolo BGP e ii) criação de enlaces ethernet de acordo com o padrão e-Line do MetroEthernet Fórum[1].

A documentação completa do SDN-IPS pode ser encontrada no site `http://insert.ufba.br/sdn-ips`. Nele estão disponíveis o código-fonte, descrição da arquitetura, publicações, manuais e vídeos explicativos sobre instalação e funcionalidades.

[1]https://wiki.mef.net/display/CESG/E-Line

3. Práticas utilizando o SDN-IPS no FIBRE

O funcionamento do SDN-IPS pode ser demonstrado em uma topologia no ambiente do FIBRE, conforme Figura 2, onde é possível modelar o cenário de rede com dois Sistemas Autônomos (AS), em que o AS 100 será orquestrado pelo SDN-IPS e o AS 666 com ferramentas de roteamento tradicionais. A Figura 3 ilustra a criação do cenário no OCF, o *framework* de controle do FIBRE. Os experimentos foram divididos em quatro etapas:

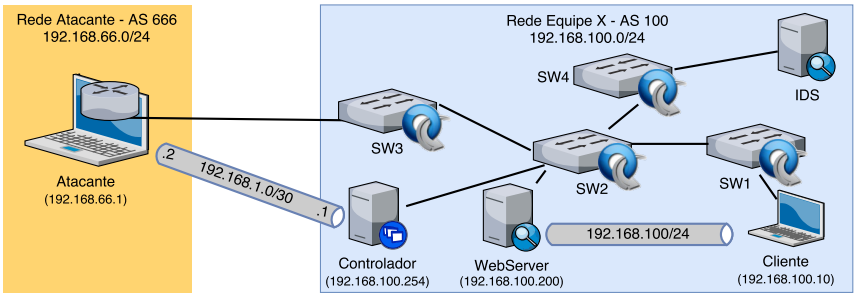

Figura 2. Topologia proposta para demonstração no SBRC.

- **Configuração do ambiente e conectividade**: nesse momento os alunos são levados a preparar o ambiente de experimentação no FIBRE, instalar e configurar o controlador SDN e a aplicação SDN-IPS e, por fim, estabelecer a conectividade ponto-a-ponto entre os servidores do AS 100 e entre o controlador e o atacante.
- **Roteamento interdomínio**: nesta prática os alunos desenvolvem parte de uma aplicação SDN. Para programar a funcionalidade de comunicação BGP no controlador, o aluno deve modificar a aplicação SDN-IPS e integrá-la com a biblioteca BGP do Ryu[2]. Já na configuração do AS 666, o aluno tem oportunidade de executar comandos de configuração em um roteador BGP convencional, o Quagga.
- **Configuração do IDS**: esta prática envolve a instalação da ferramenta Suricata IDS, ativação de assinaturas de ataques disponíveis em fontes abertas e criação de regras customizadas para detecção de ataques específicos de Negação de Serviço (e.g. TCP SynFlood). Por fim, os alunos são orientados a compreender e ativar o espelhamento de tráfego no controlador SDN para o servidor IDS.
- **Mecanismos de contenção**: neste laboratório é realizada a configuração de ações de contenção, que ocorrem de forma diferenciada para hosts intrusos internos e externos. Para permitir a integração entre o Suricata IDS e o SDN-IPS, o aluno deve instalar e configurar a ferramenta *Guardian Active Response*[3], customizando-a para diferenciar as ações de contenção com base no segmento de rede.

Os mecanismos de contenção ora implementados são ilustrados nos cenários das Figuras 4 e 5. Na Figura 4, uma máquina interna infectada com vírus realiza acesso a um IP malicioso (1) de Comando e Controle[4]. Em seguida, o sistema IDS, para o qual o tráfego é espelhado, identifica aquela requisição anômala (2) e notifica via API REST o SDN-IPS (3), que cria regras para redirecionar todo o tráfego para o servidor de quarentena. Assim, ao realizar novas requisições, a máquina ficará restrita ao ambiente de quarentena (4) até que seja efetuada uma análise com antivírus para limpar a máquina.

[2]http://ryu.readthedocs.io/en/latest/library_bgp_speaker_ref.html
[3]http://www.chaotic.org/guardian/
[4]Um servidor de Comando e Controle (C&C) é usado para controlar máquinas infectadas remotamente.

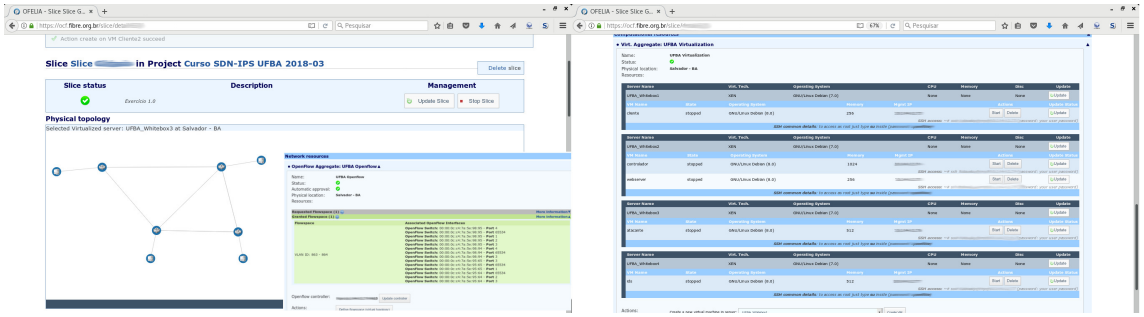

Figura 3. Tela do OCF com o setup do experimento para o SDN-IPS.

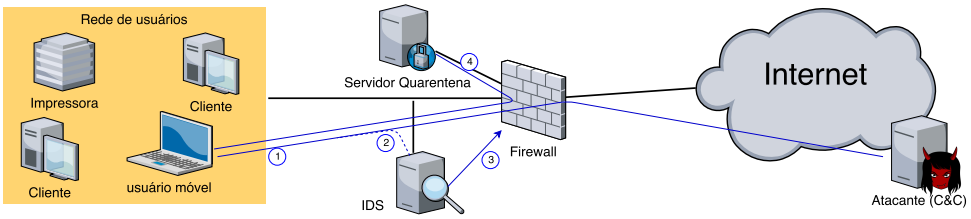

Figura 4. Ilustração da SDN-IPS com contenção via quarentena.

Já na Figura 5 é demonstrada uma situação de bloqueio de tráfego. Trata-se de um ataque de Negação de Serviço do tipo TCP Synflood disparado contra o servidor web da organização, utilizando a ferramenta *HPING3*. Em (1) o ataque é iniciado pelo servidor malicioso. Em seguida, o Suricata IDS identifica o tráfego malicioso (2) e notifica via REST o SDN-IPS (3). Como trata-se de um ataque externo, nesse caso, a ação de contenção realizada é o bloqueio (4) da máquina atacante.

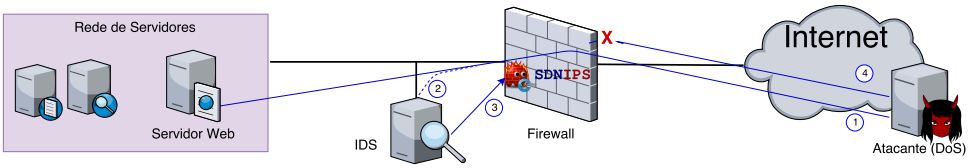

Figura 5. Ilustração da SDN-IPS com contenção via descarte de tráfego.

Além dos cenários apresentados anteriormente, uma notificação de atividade maliciosa pode ser reportada por um cliente ou provedor parceiro através do módulo de contenção colaborativa do SDN-IPS. Este módulo recebe mensagens de BGP do tipo FlowSpec IPv4 e converte-as em *matches* e *actions* para então serem enviadas via OpenFlow para os *switches* de borda. Para simular o cliente, pode ser executado o roteador virtual *ExaBGP*[5] para estabelecer um *peering* com o SDN-IPS e enviar um BGP FlowSpec de solicitação de bloqueio para o IP externo do atacante.

4. Curso semi-presencial de Prevenção de Intrusão baseado em SDN

Foi desenvolvido um curso de extensão semi-presencial na UFBA explorando o potencial da ferramenta SDN-IPS e do *testbed* FIBRE para fins didático-pedagógicos. Esta seção descreve mais informações sobre o curso, experiências e lições aprendidas.

[5]https://github.com/Exa-Networks/exabgp

4.1. Visão geral do curso

O curso de curso de extensão semi-presencial foi realizado entre os dias 08/03 e 05/04 de 2018. As aulas presenciais ocorreram no Laboratório da Superintendência de TI da UFBA e o acompanhamento à distância foi realizado através do Moodle[6]. Devido ao caráter de turma piloto, a divulgação foi restrita[7], mas foram recebidos muitos pedidos de inscrição, dos quais selecionou-se 21 alunos de acordo com os requisitos do curso e criou-se uma lista de espera para novas edições. A Figura 6 ilustra um dia de aula presencial do curso.

Figura 6. Fotos do curso de extensão SDN-IPS realizado na UFBA.

A Figura 7 apresenta a tela inicial do ambiente virtual de aprendizagem (AVA) utilizado no curso SDN-IPS. O AVA configurou-se como um momento complementar às aulas expositivas, e através dele foi possível concentrar a divulgação de materiais adicionais, a realização de atividades avaliativas e discussões sobre os temas do curso. Ademais, uma das grandes vantagens desse ambiente é funcionar como uma memória viva do curso, onde novas turmas poderão se beneficiar de tudo que foi construído em conjunto e compartilhado pelos alunos egressos, além de produzir novos conteúdos.

Figura 7. Tela do Ambiente Virtual de Aprendizagem e do Fórum de Discussão.

É importante destacar a participação dos alunos no AVA, seja para tirar dúvidas sobre as práticas, para reportar problemas na infraestrutura ou no material e até para

[6]https://www.moodle.ufba.br

[7]O curso foi divulgado para profissionais e alunos de graduação e pós-graduação da UFBA e outras universidades de Salvador. Mais informações: `https://sti.ufba.br/curso-sdnips`

compartilhar lições aprendidas ou materiais relacionados. Os alunos utilizaram o Fórum de Discussões de forma bastante proveitosa, conforme Figura 7. Ao longo do curso, foram criados mais de 25 tópicos, com mais de 80 interações entre alunos e instrutores.

4.2. Perfil dos alunos

Para validar os pré-requisitos teóricos e mensurar a experiência prática dos alunos, foi aplicado um formulário composto por 15 questões que serviu como insumo para identificação do perfil dos estudantes e composição das aulas teóricas.

Em geral, observou-se variação no perfil dos alunos em relação à faixa etária, escolaridade, perfil profissional e experiência nas áreas de redes e segurança da informação. Essa heterogeneidade traz consigo o desafio de balancear o nível de exposição dos assuntos de maneira adequada aos diferentes públicos. Desta forma, foi realizada uma avaliação em relação aos conteúdos que seriam abordados para que fosse verificado quais assuntos deveriam ser mais explorados. A relação do nível de conhecimento dos alunos por tema pode ser observada na Tabela 1, que sumariza a avaliação dos alunos em graus de 1 a 5 (1 indicando pouco ou nenhum conhecimento e 5 indicando muito conhecimento) e indica o perfil da turma em relação aos tópicos que seriam apresentados durante o curso.

Tabela 1. Avaliação inicial do conhecimento dos alunos em relação aos assuntos abordados no curso.

	1	2	3	4	5
Arquitetura e Protocolos TCP/IP		15%	15%	55%	15%
VLAN	5%	30%	15%	30%	20%
Endereçamento e Segmentação de rede	10%	20%	25%	30%	15%
Padrões de conectividade de enlace metroethernet	35%	25%	25%	15%	
Sistemas Autônomos	30%	25%	40%	5%	
Roteamento entre Sistemas Autônomos	30%	30%	35%	5%	
Protocolo BGP	40%	20%	40%		
Software-Defined Networking	35%	15%	30%	20%	
OpenFlow	35%	20%	35%	10%	
Redes de testebed	50%	15%	30%	5%	
FIBRE	55%	25%	20%		
Segurança da Informação		30%	35%	30%	5%
Ataques na camada de rede	20%	15%	45%	20%	
Ataques na camada de aplicação	15%	25%	30%	30%	
Sistemas de Detecção de Intrusão	20%	25%	35%	15%	5%
Mecanismos de contenção de ataques	25%	30%	25%	15%	5%

De acordo com a tabela, aproximadamente 50% da turma tinha conhecimento intermediário/avançado nos tópicos básicos em redes, enquanto os temas relacionados à segurança tiveram sua distribuição entre os níveis básico/intermediário. Além desse sumário, ao verificar o conhecimento em relação às ferramentas utilizadas, mais de 50% tinha pouco/nenhum conhecimento; em relação ao Quagga, por exemplo, esse valor chegou a representar 85% da turma, fato que pode evidenciar um desequilíbrio entre teoria/prática na formação anterior dos estudantes. Outro fator relevante é que aproximadamente 50% da turma não conhecia o FIBRE ou o uso de *testbed*.

Além de utilizar esse sumário para produzir as aulas, pretende-se avaliar, posteriormente, o impacto do FIBRE no aprendizado, de acordo com os perfis dos alunos.

4.3. Testemunho dos alunos

Na reta final do curso, formulários de avaliação foram encaminhados a alguns alunos para colher feedbacks e oportunidades de melhoria que pudessem ser endereçadas nesta ou em novas edições. A Tabela 2 apresenta um sumário com alguns comentários dos alunos. Um dos aspectos positivos diz respeito ao equilíbrio na metologia utilizada e no material de apoio com as práticas, conforme resposta à questão A.

Destaca-se também o impacto positivo e a alta relevância do uso do FIBRE no processo de aprendizagem dos alunos, novamente, buscando-se uma harmonização dos princípios com a prática, dos conceitos com o laboratório, da teoria com as situações reais do dia a dia, conforme notado nas respostas B e C. Por fim, os comentários dos alunos apontam diversas oportunidades de melhoria para o curso e para o projeto FIBRE em si (respostas D e E), pontos que serão alvo de maior detalhamento na seção seguinte.

4.4. Desafios e Lições Aprendidas Durante o Curso

O caráter inovador de utilizar o FIBRE pela primeira vez em um curso de redes e cibersegurança na UFBA trouxe muitos aprendizados, desafios e, principalmente, enriqueceu o processo de ensino e aprendizagem. A seguir são listados alguns desafios e lições aprendidas ao longo do curso:

- **Problemas nas ilhas do FIBRE**: ao longo do curso, diversos problemas ocorreram nas ilhas que estavam sendo utilizadas (UFBA, UFPE e RNP). Os problemas incluem lentidão nos recursos, problemas em equipamentos, falta de espaço em disco para novas máquinas e *bugs* no OCF que demandaram a recriação de *slices*. Ao identificar esses problemas, a equipe do FIBRE prontamente alocou um analista para acompanhar e apoiar a realização das aulas. Além disso, concentrar os experimentos em uma única ilha, na qual a equipe executora do curso possui maior proximidade com os operadores, também diminuiu a incidência dos problemas.
- **Visão da topologia no OCF**: do ponto de vista didático, foi ruim para os alunos identificar a topologia configurada na definição do slice (*Define flowspace > User's topology*) com a topologia apresentada na página de visão geral do slice (*Physical topology*) no OCF. Seria interessante que a visão geral do slice refletisse a topologia escolhida pelo usuário na sua definição. Dessa forma, o aluno visualizaria rapidamente as características do seu experimento, bem como facilitaria para o professor produzir um material que seja claro, didático e determinístico.
- **Resolução de problemas e visibilidade do switch OpenFlow**: em alguns momentos é importante mostrar para os alunos o estado da tabela OpenFlow e como as regras foram inseridas, inclusive possivelmente regras de outros *slices*. Embora esse requisito não seja importante ou mesmo desejável para uso do FIBRE por experimentadores, do ponto de vista didático-pedagógico, é importante o aluno ter essa visão concreta da tabela e, inclusive, enviar comandos para o switch (e.g. *dpctl*). Essa possibilidade ajuda na resolução de problemas: um aluno teria à disposição mais informações para ajudá-lo no diagnóstico da causa raiz do mal funcionamento da rede. Viabilizar o desenvolvimento da capacidade de diagnóstico e resolução de problemas seria um diferencial expressivo do ambiente.

Tabela 2. Respostas dos alunos ao formulário de avaliação na reta final do curso.

Pergunta	Resposta
A - Qual a sua avaliação sobre o curso SDN-IPS?	
	MUITO BOM! (...) gostei bastante da estrutura, de uma apresentação para nivelamento sobre o tópico, em seguida um aprofundamento e por fim uma parte prática para fixar os conceitos aprendidos.
	Instrutores super capacitados com domínio nos temas abordados e principalmente sabendo passar todo esse conhecimento para os alunos e material didático muito bem explicativo para acompanhamento do curso
B - Este foi o primeiro contato com o FIBRE? Como foi a experiência?	
	Sim, foi meu primeiro contato na prática. (...) à medida que o curso avançava tornou-se evidente a real dimensão de todos os conceitos mostrados em sala uma vez que a teoria repassada foi realmente aplicada em um cenário que, apesar de controlado, representa situações reais enfrentadas no cotidiano de empresas/universidades/organizações.
	Sim, excelente. Se todo curso/estudo tivesse o fibre como apoio seria muito mais fácil aprender
C - Quais vantagens observadas no uso do FIBRE durante o curso?	
	Utilização de um cenário real para execução de experimentos; Realização de troubleshooting na prática; Rapidez na alocação de recursos.
	Colocar o que aprendemos em prática, auxilia e muito no aprendizado
D - Quais as oportunidades de melhoria você observou no uso do FIBRE?	
	(...) oportunidade de melhoria é no sistema que está meio instável com alguns problemas, uma opção que seria uma boa ter era SNAPSHOT, por conta de estar fazendo teste constante isso vai ser uma boa.
	Em alguns momentos o ambiente se mostrou instável sem indicar nenhuma mensagem (...) Portanto, a instabilidade e o tratamento de mensagens (feedback), considero pontos de melhoria.
E - Comentários adicionais	
	O testbed FIBRE, apesar da iniciativa do curso SDNIPS, tem permanecido fora do conhecimento de grande parte dos estudantes.
	Necessitamos de mais oportunidades de cursos como este!

- **Problemas com o funcionamento do *datapath* OpenFlow**: foram identificados alguns problemas específicos no funcionamento do *datapath* OpenFlow ao longo das práticas, seja por ocasião do Flowvisor ou do próprio switch OpenFlow. Um deles foi em relação ao isolamento de experimentos, onde regras muito genéricas inseridas no switch acabavam gerando tráfego inesperado na aplicação de outro *slice*. Houveram problemas também nas ações de reescrita de campos como IP ToS e VLAN PCP. Outro problema foi observado durante o envio de mensagens Flow-Mod com *match* incluindo o ether-type. Nesse caso, o fluxo é inserido pelo FlowVisor sem o VLAN ID, convencionalmente utilizado para isolamento dos *slices*, o que termina impactando, por exemplo, na limpeza de regras na reinicialização do controlador. Todos os problemas foram reportados à equipe do FIBRE, que está endereçando internamente cada questão.

- **Necessidade da VPN e console SSH para acesso às máquinas**: alguns alunos sugeriram que a interface do OCF disponibilizasse *consoles* virtuais web, para que o acesso às máquinas seja simplificado e todos os laboratórios possam ser realizados através de um simples navegador web.
- **Armazenamento do estado das máquinas**: com as instabilidades do ambiente ou para realização de práticas divididas em múltiplas aulas, seria interessante que as máquinas pudessem ter seu estado salvo, com uso de *SNAPSHOT*, por exemplo.

5. Conclusões e Trabalhos Futuros

Este artigo apresentou um relato de experiências no uso do FIBRE e do SDN-IPS no ensino de redes e segurança na UFBA. Através do material teórico, das aulas expositivas e das práticas utilizando o SDN-IPS no FIBRE, foi possível viabilizar uma aprendizagem progressiva, consistente e com foco na solução de problemas reais, de forma inovadora.

As lições aprendidas e os feedbacks confirmam que a harmonização entre teoria e prática é essencial para formação de alunos na área de redes e segurança. Do ponto de vista do professor, o uso de *testbeds* como o FIBRE abre novas perspectivas para construção de objetos de aprendizagem, bem como simplifica a busca por recursos para realização de laboratórios práticos. É importante destacar ainda as questões relacionadas à *hacking ético*, na qual o estudante é apresentado à técnicas ofensivas e defensivas, sendo orientado sobre os princípios que disciplinam sua atuação. Nesse sentido, o uso FIBRE permite o equilíbrio entre um cenário com equipamentos reais em ambiente controlado.

Em trabalhos futuros espera-se dar continuidade à realização de cursos como esse, inclusive incorporando-o em outros níveis da educação, e colaborar com o FIBRE na melhoria do projeto em relação aos desafios ora enfrentados. Em especial, aprimorar as estratégias de divulgação e aproximação do FIBRE junto às instituições de ensino é uma ação estratégica, pois dessa forma os benefícios de seu uso serão potencializados.

Referências

Ciuffo, L., Salmito, T., Rezende, J., and Machado, I. (2016). Testbed FIBRE: passado, presente e perspectivas. In *Workshop de Pesquisa Experimental da Internet do Futuro (WPEIF)*, pages 3–6.

Kaabi, S. A., Kindi, N. A., Fazari, S. A., and Trabelsi, Z. (2016). Virtualization based ethical educational platform for hands-on lab activities on DoS attacks. In *IEEE EDUCON*, pages 273–280.

Kreutz, D., Ramos, F. M. V., Veríssimo, P., Rothenberg, C. E., Azodolmolky, S., and Uhlig, S. (2014). Software-Defined Networking: A Comprehensive Survey. *Proceedings of the IEEE*, 103(1):63.

Kurose, J. and Ross, K. (2013). *Redes de computadores e a Internet: uma abordagem top-down*. Pearson.

Marques, P., Sheth, N., Raszuk, R., Greene, B., Mauch, J., and McPherson, D. (2009). Dissemination of Flow Specification Rules. RFC 5575 (Proposed Standard).

Xu, L., Huang, D., and Tsai, W. T. (2014). Cloud-Based Virtual Laboratory for Network Security Education. *IEEE Transactions on Education*, 57(3):145–150.