SDN-IPS: Uma Ferramenta para Contenção Automatizada e Colaborativa de Ataques Cibernéticos Baseada em SDN

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 growth and diversity of cyber attacks imply stricted temporal requirements and flexibility in security controls deployment. Therefore, automation and collaborative actions are essencials in such scenarios. This paper presents SDN-IPS, a tool that put together the visibility of Intrusion Detection Systems with SDN's programability in order to create a solution for attacks contention through blocking, rate limit, and quarantine strategies. SDN-IPS can be used for technical purposes, in campus and backbone networks, or to networks and secutity teaching. Thus, it can help network operators and researchers in malicious activity detection and containment. Demonstrations will be performed using FIBRE testebed with MetroEthernet links (e-Line) and interdomain routing (BGP) applications.*

Resumo. *O crescimento e diversidade dos ataques cibernéticos impõem requisitos temporais estritos e necessidade de flexibilidade na aplicação de controles de segurança. A automação e atuação colaborativa tornam-se, portanto, abordagens imprescindíveis nesse cenário. Este artigo apresenta o SDN-IPS, uma ferramenta que agrega a visibilidade dos Sistemas de Detecção de Intrusos com a programabilidade do paradigma SDN, criando uma solução para contenção de ataques através de estratégias de bloqueio, restrição de banda ou isolamento em quarentena. Com aplicabilidade técnica, tanto em redes de campus quanto em redes de backbone, e didática, para ensino de redes e segurança, o SDN-IPS pode beneficiar operadores e pesquisadores na detecção e contenção de atividade maliciosa na rede. A ferramenta será demonstrada através do testbed FIBRE, integrada, como estudo de caso, a uma aplicação de enlaces metro-ethernet (e-Line) e roteamento inter-AS (BGP).*

1. Introdução

A quantidade e variedade de ataques, desde Negação de Serviço Distribuído (do inglês, *Distributed Denial of Service* – DDoS) à acessos a conteúdos maliciosos, têm crescido significativamente nos últimos anos [Yang et al. 2017, CERT.br 2017]. Isso torna a operação de um centro de segurança cibernético cada vez mais complexa e impõe requisitos de tempo de resposta mais estritos. A automação torna-se, portanto, uma abordagem imprescindível, podendo ser apoiada pela visibilidade dos Sistemas de Detecção de Intrusos (do inglês, *Intrusion Detection System* – IDS) e pela programabilidade da rede através do paradigma de Redes Definidas por Software (do inglês, *Software Defined Networking*

– *SDN)* [Kreutz et al. 2014]. Ademais, a atuação colaborativa, que consiste em prover capacidade de prevenção de ataques remotamente para clientes e provedores parceiros, potencializa essas ações, visto que o ataque pode ser contido mais próximo da origem.

Uma das abordagens utilizadas para detectar as ameaças é a verificação de assinaturas de ataques no tráfego interno e externo da organização [Chi et al. 2017]. A partir dos ataques detectados pelo IDS, inicia-se o processo de contenção, que visa impedir a continuidade do incidente. Na contenção, pode-se utilizar estratégias de bloqueio, restrição de banda ou isolamento em quarentena, conforme sentido do tráfego, políticas da organização e funcionalidades disponíveis nos equipamentos de rede. Em particular, o uso de SDN e do protocolo OpenFlow podem aumentar a flexibilidade na integração do IDS com os elementos de rede [Chi et al. 2017], potencializando as ações de contramedida e transformando o sistema de orquestração da rede em um Sistema de Prevenção de Intrusos (do inglês, *Intrusion Prevention System* – IPS).

Este artigo apresenta o SDN-IPS, uma ferramenta que incorpora a capacidade de detecção e contenção de intrusos em uma rede SDN. Através do SDN-IPS, o administrador pode integrar aplicações de orquestração da rede (e.g. configuração de enlaces *Ethernet* ou roteamento interdomínio) à capacidade de análise de tráfego e tomada de decisões para contenção de acessos maliciosos. Desta forma, o SDN-IPS pode ser utilizado como uma solução técnica de segurança, aplicada tanto em cenários de redes de campus quanto em redes de *backbone*. A ferramenta também pode ser utilizada para fins didático-pedagógicos, auxiliando nas práticas de ensino de redes e segurança de sistemas.

A ferramenta foi desenvolvida em Python no controlador Ryu[1], e é composta por seis módulos cujas funções variam desde a modelagem da topologia até a aplicação de regras de contenção nos comutadores SDN. O SDN-IPS será demonstrado utilizando o *testbed* FIBRE (do inglês, *Future Internet Brazillian Environment for Experimentation*)[2], mantido pela Rede Nacional de Ensino e Pesquisa (RNP), que funciona como um laboratório virtual de larga escala para estudantes e pesquisadores testarem novas aplicações e modelos de arquitetura de rede. Nesse ambiente, será montada uma topologia com múltiplos sistemas autônomos (do inglês, *Autonomous Systems* – ASs) com capacidade de detectar intrusos e executar ações de prevenção.

O artigo está organizado da seguinte forma: a Seção 2 apresenta a arquitetura e as funcionalidades da ferramenta, a Seção 3 descreve o planejamento da demonstração no SBRC, bem como algumas informações de documentação e uso da ferramenta. Por fim, a Seção 4 discute as conclusões e os trabalhos futuros.

2. A Ferramenta SDN-IPS

O SDN-IPS pode ser visto como um IPS baseado em OpenFlow que tem por finalidade orquestrar a rede e prover a capacidade de detecção e contenção de ataques. Nesta seção serão apresentadas sua arquitetura e principais funcionalidades, bem como casos de uso.

2.1. Arquitetura e Funcionalidades

A Figura 1 apresenta um diagrama que descreve a arquitetura do SDN-IPS. Os principais módulos da ferramenta são descritos a seguir:

[1]https://osrg.github.io/ryu/ (Acesso em: 11 abr. 2018)

[2]http://fibre.org.br (Acesso em: 11 abr. 2018)

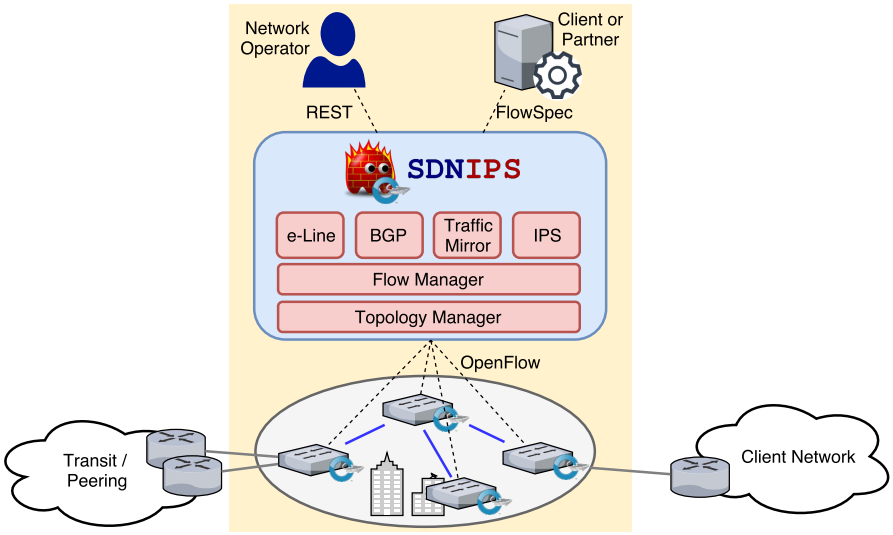

Figura 1. Diagrama da Arquitetura da SDN-IPS.

- **Gestão da topologia (*Topology Manager*)**: neste módulo, a rede é modelada como um grafo dirigido $D = (V, A)$, no qual o conjunto de vértices V representa os comutadores SDN e o conjunto de arcos A representa os pares ordenados de enlaces entre os comutadores. Uma associação entre dois comutadores (C_1, C_2) ocorre quando uma mensagem de descoberta de enlace (LLDP) transmitida por C_1 é recebida em C_2. Nesse momento também é possível distinguir as portas de *backbone* das portas de acesso em C_2, visto que as portas de acesso não recebem LLDP. Para armazenar o grafo da rede, foi utilizada a biblioteca Python NetworkX[3].
- **Gestão de Fluxos (*Flow Manager*)**: realiza o armazenamento e checagem da consistência dos fluxos instalados em cada *switch*. Dessa forma, cada vértice do grafo possui uma lista de fluxos instalados e cada arco possui uma referência aos fluxos, cujos campos de *match* ou *actions* envolvem alguma das portas daquele enlace. A partir dessa premissa, é possível modificar dinamicamente uma regra de encaminhamento para bloquear determinado *host* malicioso ou até mesmo criar regras mais específicas e com maior prioridade para redirecionamento de tráfego.
- **Espelhamento de Tráfego (*Traffic Mirror*)**: em uma rede convencional, o espelhamento de tráfego pode ser habilitado com base em portas físicas ou em VLANs (independente da porta). Além destas possibilidades, com o uso do SDN-IPS, o operador da rede pode escolher fazer o espelhamento por regra da tabela de fluxos, aumentando a granularidade com qual o tráfego será analisado. Após escolher os fluxos que serão espelhados, o operador deverá especificar um *switch* e uma porta de acesso remota na qual o tráfego será entregue. A partir daí, o SDN-IPS fará a configuração OpenFlow nos *switches* intermediários para espelhamento remoto do tráfego. É possível especificar ainda uma VLAN ou MAC de destino que receberá o tráfego, funcionalidade útil para ambientes compartilhados como redes de campus ou como a infraestrutura do FIBRE com múltiplas fatias (*slices*). A partir do tráfego espelhado, o SDN-IPS pode ser integrado a um IDS para detecção de ataques e geração de alertas, culminando, posteriormente, em ações de contenção.

[3]https://networkx.github.io/ https://networkx.github.io/ (Acesso em: 11 abr. 2018)

- **Contenção de ataques (IPS)**: a partir dos alarmes gerados na fase de detecção, o módulo IPS executa ações de contenção para interromper o ataque e evitar danos à rede. Essas ações podem ser das mais variadas naturezas, por exemplo: (i) cancelamento da conexão em andamento (ex: TCP RST); (ii) bloqueio do *host* atacante (*drop*); (iii) limitação de banda ou de requisições do atacante (*rate-limit*); (iv) redirecionamento de tráfego para quarentena; (v) limpeza do tráfego. No SDN-IPS foram implementadas as ações de contenção baseadas em quarentena e bloqueio. A ação de restrição de banda, apesar de disponível, requer acesso remoto ao plano de gerência dos comutadores SDN para criação de filas QoS, funcionalidade não disponível, por exemplo, no FIBRE. As ações de contenção são disponibilizadas pelo SDN-IPS através de uma API norte baseada em abstrações REST, permitindo, por exemplo, integração com sistemas IDS existentes e soluções de automação.
- **Contenção colaborativa**: além de realizar a contenção baseada no tráfego malicioso identificado pelo IDS, é importante estar preparado para contenção colaborativa, realizada com base em listas de perfis de tráfego malicioso enviadas por clientes ou parceiros. Ao realizar a contenção mais próximo da origem do ataque, a utilização dos recursos de rede é otimizada, evitando impacto no tráfego de produção do provedor. Uma das abordagens que vem sendo utilizada pelos provedores é o padrão BGP FlowSpec [Marques et al. 2009], no qual um provedor pode solicitar remotamente o tratamento de tráfego malicioso contra seus prefixos através das ações de contenção supracitadas. Para isso, o SDN-IPS estende o funcionamento da API do BGP disponível no Ryu, tratando as mensagens de *UPDATE* do BGP FlowSpec IPv4 e convertendo-as em solicitações de contenção.
- **Outras aplicações (BGP e e-Line)**: além das funcionalidades dos módulos detalhados anteriormente, o operador da rede pode executar módulos SDN adicionais. Como estudo de caso, o SDN-IPS possui dois módulos pré-integrados: um para roteamento interdomínio através do protocolo BGP e outro para criação de enlaces *Metroethernet* em conformidade com o padrão *e-Line* do *MetroEthernet Forum*[4]. Assim, a aplicação pode ser utilizada para orquestração de uma rede de campus com múltiplos segmentos de rede, ou seja, múltiplos *e-Line*, bem como atuar como uma rede de *backbone* para clientes BGP e provedores de trânsito ou *peering*.

2.2. Funcionamento da ferramenta

A estratégia de contenção de ataques baseada em quarentena possui desafios intrínsecos à sua implantação em tabelas de fluxos de equipamentos OpenFlow. O principal está no fato de que a tabela de fluxos do OpenFlow 1.0 não armazena o estado das conexões, tornando complexa a reescrita dos cabeçalhos de rede para redirecionamento de tráfego nas requisições de acesso. Uma alternativa seria realizar marcações no próprio cabeçalho do pacote, através de campos geralmente não utilizados como IP ToS ou VLAN PCP. Não obstante, além do risco desses campos serem alterados pelo usuário malicioso, ambientes que utilizam o Flowvisor para segmentação e experimentação compartilhada, como o FIBRE, não dão suporte correto a essas ações.

Dessa forma, para superar esse desafio, o SDN-IPS cria regras com diferentes prioridades: i) primeiro, cria-se uma regra de maior prioridade para encaminhar ao controlador todo o tráfego do *host* malicioso; em seguida, ii) dinamicamente, o controlador cria

[4]https://wiki.mef.net/display/CESG/E-Line (Acesso em: 11 abr. 2018)

um conjunto de regras específicas para fazer o redirecionamento do tráfego para a quarentena. A Tabela 1 ilustra tal cenário: as regras 1 e 2 são usadas para configuração do *e-Line* no acesso do cliente. Ao receber uma requisição para contenção do *host* 10.0.0.100, o SDN-IPS cria a regra 3, com maior prioridade que 1 e 2, a fim de enviar aquele tráfego para o controlador. Logo, quando o *host* 10.0.0.100 enviar qualquer requisição (e.g., para 6.6.6.6), a requisição será enviada ao controlador e o SDN-IPS criará, dinamicamente, regras de quarentena (regras 4 e 5) para tal tráfego (e.g., redirecionando para 192.168.0.10).

Tabela 1. Exemplo da tabela de fluxos para configuração da quarentena na SDN-IPS

#	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

Os mecanismos de contenção implementados permitem redirecionamento de tráfego (quarentena) e bloqueio, sendo o bloqueio tipicamente utilizado para máquinas externas à rede e a quarentena para máquinas internas. Tal comportamento pode ser alterado pelo administrador ao modificar a chamada REST do SDN-IPS no servidor IDS, variando a ação tomada para cada regra de detecção de intrusos que desejar. Exemplos dessas duas formas de contenção podem ser observados nas Figuras 2 e 3.

Na Figura 2, uma máquina interna comprometida (e.g., usuário clicou em um anexo infectado) realiza acesso a um IP malicioso (1) de servidor de Comando e Controle (C&C)[5]. 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. A partir daí, ao realizar qualquer outro tipo de acesso, a máquina ficará restrita ao ambiente de quarentena (4) até que seja efetuada uma análise com antivírus e *antimalware* para limpar a máquina. O servidor de quarentena disponibiliza uma página web simples para informar ao usuário que sua máquina está possivelmente comprometida e ele deve procurar o suporte.

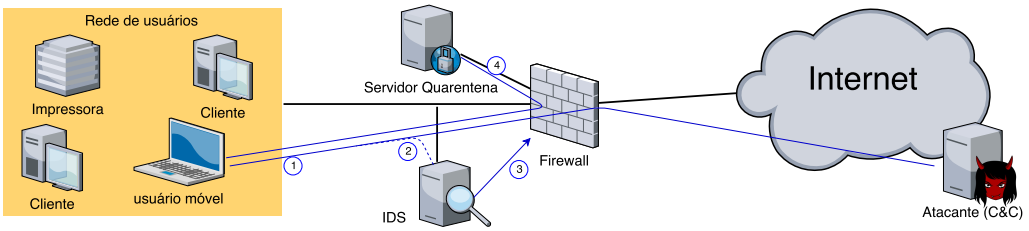

Figura 2. Ilustração da SDN-IPS com contenção via quarentena.

Já na Figura 3 é demonstrada uma situação de bloqueio de tráfego. Trata-se de um ataque de Negação de Serviço (DoS) disparado contra o servidor web da organização.

[5]Um servidor de Comando e Controle é usado para controlar máquinas infectadas remotamente.

Em (1) o ataque (e.g. SYNFLOOD) é iniciado pelo servidor malicioso. Em seguida, o sistema IDS identifica o tráfego como uma anomalia (2) e notifica o SDN-IPS (3), que passa a bloquear (4) todo o tráfego cuja origem é o servidor identificado como malicioso.

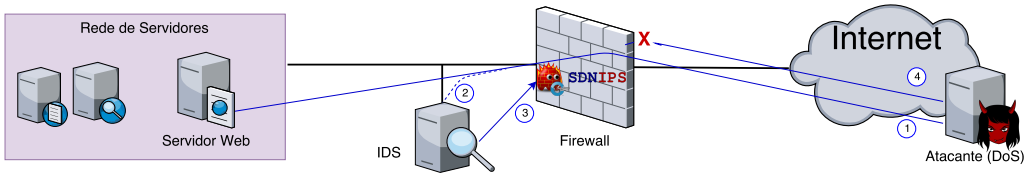

Figura 3. Ilustração da SDN-IPS com contenção via descarte de tráfego.

Além dos cenários de detecção e contenção exemplificados anteriormente, uma notificação de atividade maliciosa pode ser enviada através de um cliente ou parceiro externo. Essa notificação é recebida pelo SDN-IPS através do módulo de contenção colaborativa, utilizando BGP. Este módulo recebe as mensagens de BGP *UPDATE* e extrai aquelas cujo *address family* refere-se ao tipo FlowSpec IPv4. A partir dessas mensagens, os atributos do caminho são convertidos em *matches* e as *actions* são extraídas a partir das comunidades BGP, em conformidade com a especificação do FlowSpec, para então serem enviadas via OpenFlow para os *switches* de borda. Tendo em vista as interfaces de conexão via REST e BGP FlowSpec, o SDN-IPS pode ser integrado à qualquer sistema IDS do provedor, cliente ou parceiro, sem acarretar custos adicionais de compatibilização.

2.3. Casos de Uso

A ferramenta SDN-IPS pode ser empregada em diferentes cenários, tanto como uma solução técnica para contenção de ataques quanto para apoio no ensino de redes e segurança, conforme detalhado a seguir:

- **Implantação de segurança em redes de campus**: a heterogeneidade das redes de campus, seja em termos de equipamentos ou perfil de tráfego dos usuários, requer flexibilidade e automação na tomada de ações de segurança. O SDN-IPS pode ser uma solução efetiva para este cenário, pois o administrador poderá escolher de forma granular quais regras deseja monitorar no IDS e tomar ações de contenção que sejam mais apropriadas para o segmento de rede em questão. Por exemplo, alarmes no IDS relacionados à *hosts* de laboratórios ou rede sem fio poderão ser isolados em quarentena para posterior tratamento, ao passo que ataques externos contra os servidores da organização devem ser imediatamente bloqueados.
- **Implantação de segurança em redes de *backbone***: em cenários de rede *backbone* a aplicação das ações de contenção deve ser validada em relação à origem da solicitação e ocorrer apenas em alguns equipamentos de borda do provedor. Em termos de validação da origem da solicitação, um cliente, por exemplo, pode solicitar contenção apenas de tráfego relacionado com seus prefixos. O padrão BGP FlowSpec possui mecanismos efetivos tanto para prover granularidade aos bloqueios quanto para validar a autoridade na solicitação. Ao estender o Ryu para dar suporte à mensagens de BGP FlowSpec, o SDN-IPS provê tanto um serviço completo de detecção e contenção de intrusos, quanto permite que o próprio cliente faça a detecção e solicite o bloqueio, de forma automatizada, via FlowSpec.

- **Ensino de Redes e Segurança**[6]: diversas técnicas empregadas no SDN-IPS para viabilizar suas funcionalidades podem servir de base para o ensino dos conceitos de SDN/OpenFlow e Segurança. As manipulações aplicadas na tabela de fluxos pelo SDN-IPS, por exemplo, podem ajudar um aluno a compreender diversas características da arquitetura SDN, do protocolo OpenFlow, de manutenção da tabela de fluxos, dentre outros. Além disso, a vasta documentação acerca das tecnologias envolvidas, disponibilizada em conjunto com a ferramenta, ajuda o leitor na aquisição de conhecimento, desenvolvendo ou aperfeiçoando de forma gradual os conceitos apresentados no seu processo de aprendizagem.

3. Planejamento de demonstração

O SDN-IPS, seus manuais e alguns vídeos explicativos sobre sua instalação e funcionalidades podem ser encontrados em `http://insert.ufba.br/sdn-ips`. A demonstração da ferramenta dar-se-á com o suporte de um computador e uma televisão. Nesta oportunidade, será criada uma topologia no FIBRE, conforme descrito na Figura 4. A topologia é composta por uma máquina de cliente, uma máquina atacante, um controlador SDN, um IDS e um servidor Web, que serve como ambiente de quarentena e prestação de serviços para Internet. Através de tal estrutura, a demonstração visará ilustrar a capacidade de detecção e contenção do SDN-IPS.

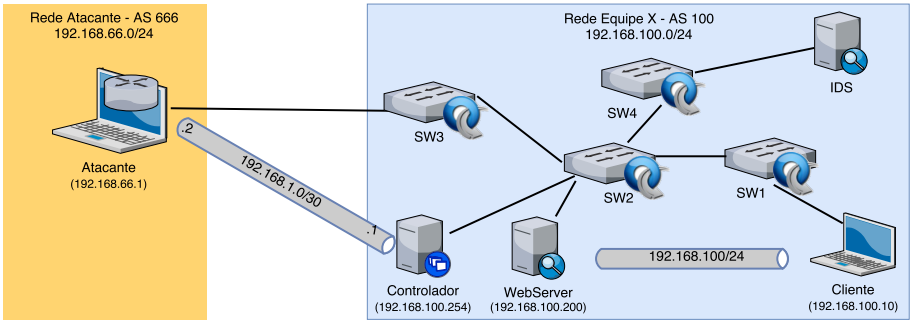

Figura 4. Topologia proposta para demonstração no SBRC.

A topologia descrita permite a demonstração dos três exemplos apresentados na Seção 2. No cenário 1, será simulado um acesso a IP malicioso de C&C por uma máquina da rede interna. Para isso, será utilizado o repositório de *hosts* controladores do *Trojan Feodo*[7] onde será escolhido um IP malicioso de C&C que esteja online. Após uma tentativa de acesso ao IP malicioso, será possível identificar, nos *logs* do IDS Suricata[8], o alerta de intrusão. Uma vez que o IDS identifica uma ameaça, o mecanismo de contenção é ativado. A integração entre o Suricata e o SDN-IPS é realizada através da API REST. Como o mecanismo de contenção utilizado para ataques internos é a quarentena, as mensagens enviadas por esse cliente serão redirecionadas para o WebServer, que irá responder com uma mensagem que informa ao cliente que a máquina dele possivelmente foi infectada e que ele precisa entrar em contato com o setor de TI da organização.

[6]Foi desenvolvido um curso de extensão para alunos de graduação, pós graduação e profissionais da área de redes, utilizando o SDN-IPS no ambiente do FIBRE, com o intuito de avaliar a usabilidade e eficiência da ferramenta no ensino de redes e segurança. Mais informações: `https://sti.ufba.br/curso-sdn-ips`

[7]https://feodotracker.abuse.ch/ (Acesso em: 11 abr. 2018)

[8]https://suricata-ids.org/ (Acesso em: 11 abr. 2018)

Com o objetivo de demonstrar o processo de bloqueio de um atacante externo, no cenário 2 será simulado um ataque de negação de serviço via TCP SYNFLOOD, utilizando o HPING3[9], contra o WebServer. Assim como no processo anterior, o Suricata irá fazer a detecção do ataque e, através de uma chamada REST acionada pelo Guardian, o SDN-IPS irá ativar o mecanismo de contenção. Como trata-se de um ataque externo, nesse caso, a ação de contenção realizada é o bloqueio da máquina atacante.

O terceiro cenário demonstrado é a inserção de uma ação de contenção solicitada de forma colaborativa por um cliente ou parceiro do provedor. Neste cenário, o cliente solicita, via FlowSpec, o bloqueio de um IP que está atacando sua infraestrutura. Em seguida, o SDN-IPS realiza as validações de autoridade da solicitação e converte-as em requisições OpenFlow a serem enviadas para os switches de borda. Para simular o cliente, será executado o roteador virtual *ExaBGP*[10] para estabelecer um *peering* com o SDN-IPS e enviar um BGP UPDATE de solicitação de bloqueio ou quarentena relacionado ao IP externo. A partir daí, o *host* bloqueado não terá mais conectividade com a rede do cliente.

4. Conclusões e Trabalhos Futuros

O crescimento na quantidade e complexidade dos ataques cibernéticos torna evidente a necessidade de ferramentas para contenção automizada e colaborativa de atividade maliciosa na rede. Este artigo apresentou o SDN-IPS, uma ferramenta que agrega a visibilidade dos sistemas IDS com a programabilidade do paradigma SDN, para criar uma solução de contenção de ataques através de estratégias de bloqueio e isolamento em quarentena. Com potencial de uso para redes de campus e backbone, a ferramenta será demonstrada utilizando o *testbed* FIBRE, confirmando sua aplicabilidade prática em cenários reais.

Como trabalhos futuros, espera-se investigar a implantação de novos mecanismos de contenção como, por exemplo, aplicação de restrição de tráfego e limpeza de tráfego antes da entrega para o cliente. Além disso, serão avaliados outros modelos de integração do SDN-IPS com aplicações de orquestração (e.g., através do Flowvisor).

Referências

CERT.br (2017). Estatísticas dos Incidentes Reportados ao CERT.br. `https://www.cert.br/stats/incidentes/`. Último acesso em 09 de Março de 2018.

Chi, Y., Jiang, T., Li, X., and Gao, C. (2017). Design and implementation of cloud platform intrusion prevention system based on sdn. In *IEEE 2nd International Conference on Big Data Analysis (ICBDA)*, pages 847–852.

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.

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

Yang, X., Han, B., Sun, Z., and Huang, J. (2017). SDN-based DDoS Attack Detection with Cross-Plane Collaboration and Lightweight Flow Monitoring. GLOBECOM.

[9]http://www.hping.org/ (Acesso em: 11 abr. 2018)

[10]https://github.com/Exa-Networks/exabgp (Acesso em: 11 abr. 2018)