UNIVERSIDADE DE SANTA CRUZ DO SUL
DEPARTAMENTO DE COMPUTAÇÃO
CURSO DE ENGENHARIA DE COMPUTAÇÃO

UMA PROPOSTA DE IPS PARA SDN UTILIZANDO O PROTOCOLO OPENFLOW

Por

Cássio Giordani Tatsch

Proposta para Trabalho de Conclusão

Prof. Me. Charles Varlei Neu
Orientador

Prof. Me. Daniel Assmann
Prof. Me. Gilson Augusto Helfer
Prof. Me. Lucas Fernando Muller
Avaliadores

Santa Cruz do Sul, agosto de 2016

SUMÁRIO

INTRODUÇÃO

Com o advento de novos recursos que podem ser provisionados sob demanda através da Internet, a chamada 'nuvem' envolve milhares de conexões entre servidores e usuários, provendo armazenamento, comunicações unificadas e alocação de recursos. Pessoas passaram a estar conectadas o tempo todo, com qualquer dispositivo que permita o intercâmbio de dados (SEEBER, 2015). As tecnologias atuais de rede já não estão dando conta de todas as exigências dos usuários e das empresas devido a complexidade e a quantidade de protocolos usados. Geralmente são desenvolvidas e definidas de forma isolada e, para dificultar ainda mais, alguns fabricantes desenvolvem protocolos proprietários (KIM; FEAMSTER 2013; SOARES et al., 2015).

Desta forma, a tarefa de alocar novos dispositivos para escalar a rede torna-se cada vez mais complexa e lenta inviabilizando a implantação de novas tecnologias em uma rede já existente (KREUTZ et al., 2014). Pensando neste problema surgiu a arquitetura *Software Defined Networking* (SDN), ou Redes definidas por Software, um paradigma emergente que propõe uma arquitetura dinâmica, gerenciável e com custo-benefício adequado, tornando-se ideal para a alta largura de banda e a natureza dinâmica dos aplicativos atuais (SCHEHLMANN et al., 2014; SATHYA; THANGARAJAN, 2015).

O objetivo da arquitetura SDN é possibilitar a rápida configuração de uma rede conforme a demanda de serviços, além de permitir adição de recursos, independente da fabricante (SAYEED et al., 2015). A arquitetura SDN provê uma abstração entre o plano de controle e o plano de dados, transformando *switches* de rede em encaminhadores de pacote e a lógica, por sua vez, passa para controladores centralizados (KREUTZ, 2013).

Os controladores SDN possuem a inteligência da rede, podendo ser programados e configurados dinamicamente. Além disso, a lógica e o gerenciamento centralizado, permitem um monitoramento global da rede (JANKOWSKI; AMANOWICZ, 2015). A comunicação entre o controlador e os dispositivos de rede é realizada através do protocolo OpenFlow, que é padronizada pela Open Networking Foundation (ONF) e foi projetada especificadamente para SDN (ONF, 2016).

Os métodos de encaminhamento de pacotes são definidos em tabelas de fluxo (*flow tables*) armazenadas no controlador central e na memória dos dispositivos de rede. Essas tabelas contém um conjunto de entradas de fluxo, indicadores de atividade e um conjunto de zero ou mais ações a serem aplicados aos pacotes. Todos os pacotes processados pelo comutador, são comparados com a tabela de fluxo. Se uma entrada correspondente for

encontrada, uma ação é tomada (por exemplo, transmitir um pacote para determinada porta). Se nenhuma correspondência for encontrada, o pacote é encaminhado para o controlador através de um canal seguro. O controlador passa a ser responsável por determinar as ações a serem tomadas para pacotes sem entradas de fluxo válidos, adicionando ou removendo entradas da tabela (ONF, 2009).

Os indicadores de atividade, por sua vez, possuem contadores que tem por finalidade manter estatísticas sobre o fluxo da rede, conforme o Quadro 1 (ONF, 2009). Essas estatísticas são importantes para o monitoramento de possíveis falhas e para a detecção de comportamentos anômalos na rede, como por exemplo, o recebimento de ataques que, segundo Zanna et al. (2014), são cada vez mais comuns e sofisticados.

Com o intuito de prover uma maior segurança em redes com arquitetura SDN, este trabalho propõe um sistema de detecção e prevenção de intrusão (IPS), fazendo uso do protocolo OpenFlow para obtenção de estatísticas de fluxo e controle de encaminhamento de pacotes em toda planta de rede, objetivando a detecção de ataques logo nos primeiros nodos.

Quadro 1 - Contadores do Indicador de Atividades

Contator	Tamanho em bits
Por Tabela	
Número de entradas Ativas	32
Número de pacotes pesquisados	64
Número de pacotes encontrados na tabela	64
Por fluxo	
Número de pacotes recebidos	64
Número de bytes recebidos	64
Duração (segundos)	32
Duração (nano segundos)	32
Por porta	
Número de pacotes recebidos	64
Número de pacotes transmitidos	64
Número de bytes recebidos	64
Número de bytes transmitidos	64
Número de pacotes perdidos no recebimento	64
Número de pacotes perdidos na transmissão	64
Número de erros recebidos	64

Número de erros transmitidos	64
Número de erros de alinhamento de frame	64
Numero de pacotes com saturação no recebimento	64
Numero de erros de CRC	64
Número de colisões	64
Por fila	
Número de pacotes transmitidos	64
Número de bytes transmitidos	64
Número de pacotes perdidos por saturação	64

Fonte: ONF (2009)

JUSTIFICATIVA

O fato de prover um sistema de detecção e prevenção de ataques constitui-se de uma premissa de que a arquitetura SDN, por ser relativamente nova, possui poucos trabalhos relacionados. Algumas propostas proveem mecanismos de bloqueio automático de tráfego malicioso, mas para isso o tráfego é duplicado para análise, gerando novos fluxos na rede. Além disso, a análise é feita de maneira seletiva, existindo assim uma grande possibilidade de não inspeção de fluxos maliciosos. Outro ponto a destacar é que o método proposto terá baixo consumo de recursos, um dos grandes problemas da maioria dos métodos de IDS/ISP.

A justificativa científica do trabalho é comprovar a viabilidade da implantação de um IPS de forma com que fluxos maliciosos possam ser eliminados mais próximos à origem, reduzindo assim o tráfego na rede. Já a justificativa empresarial para o desenvolvimento, é a possibilidade que o trabalho traria para um melhor funcionamento das redes reduzindo quedas no serviço ou ataques.

Considerando as informações apresentadas acima, o atual trabalho, tem como problema de pesquisa: Como é possível, utilizando estatísticas de fluxo de dados, analisar, detectar e prevenir intrusões em SDN de forma eficaz?

OBJETIVOS

O objetivo principal é desenvolver um sistema de detecção e prevenção de intrusão em redes de arquitetura SDN baseado em estatísticas do fluxo de dados em diferentes dispositivos.

Pretende-se atingir os seguintes objetivos específicos:

- Obter uma base de dados consistente de regras para identificação de ataques conhecidos;
- Analisar os dados de diferentes dispositivos e identificar eventuais ameaças;
- Criar regras para encaminhamento de pacotes e configurar os dispositivos da rede para que descartem pacotes de fluxos maliciosos;
- Avaliar o número de falsos positivos e realizar o encaminhamento do mesmo para um IDS mais completo, não baseada em fluxo, antes de identificá-lo como malicioso.
- Validar os resultados da análise com testes e simulações de ataques, através de virtualização e em rede de experimentações (*testbeds*).

METODOLOGIA

Esta seção apresenta a caracterização da pesquisa e os procedimentos metodológicos definidos para este trabalho.

Caracterização da pesquisa

A pesquisa é exploratória, uma vez que serão analisados trabalhos relacionados sobre os temas de arquitetura SDN, protocolo OpenFlow e Sistemas de Detecção de Intrusão. O objetivo é conhecer as técnicas utilizadas em redes atuais, a fim de escolher a mais apropriada para o caso que se está resolvendo.

Quanto ao ambiente, a pesquisa é bibliográfica, já que a pesquisa será realizada com base em artigos publicados sobre Sistemas de Detecção de Intrusão, protocolo OpenFlow e arquitetura SDN. A pesquisa é de laboratório, pois serão reproduzidos testes e simulações de ataques. Através da coleta de dados reais dos principais padrões de ataque conhecidos, a pesquisa também será de campo.

Com relação ao procedimento técnico, a pesquisa será de caráter experimental, pois será necessário o estudo, testes e simulações a fim de comprovar a eficácia e a viabilidade do projeto.

Sobre a natureza da pesquisa, ela será quantitativa pelo levantamento de informações estatísticas do fluxo de dados que serão classificados; e qualitativa pela análise a fim de reconhecer padrões de fluxos maliciosos.

Procedimentos Metodológicos

Para a realização do trabalho de conclusão serão necessárias as seguintes etapas:

I. Elaboração da proposta de TC. Esta etapa será realizada em agosto de 2016.

II. Entrega da proposta de TC. Entrega será em agosto de 2016.

III. Pesquisa sobre assuntos relacionados a Sistemas de Detecção de Intrusão, protocolos de rede e OpenFlow e arquitetura SDN. Esta etapa será realizada entre os meses de agosto e setembro de 2016.

IV. Pesquisa sobre trabalhos relacionados à IPS com OpenFlow. Etapa que deverá ocorrer entre agosto e setembro de 2016.

V. Análise dos principais fatores que interferem na eficácia da comunicação. Será realizada em setembro de 2016.

VI. Escolha de uma técnica de coleta de dados para obtenção de fluxos maliciosos com base em técnicas já estudadas. Será realizada entre os meses de setembro e outubro de 2016.

VII. Modelagem da técnica escolhida para o domínio, segundo os fatores a serem analisados. Esta etapa será realizada entre outubro e novembro de 2016 durante o desenvolvimento do TC I, e em março de 2017 no desenvolvimento do TC II.

VIII. Escrita do TC I. Se dará entre os meses de setembro e novembro de 2016.

IX. Entrega do TC I. A entrega ocorrerá em dezembro de 2016.

X. Desenvolvimento de um sistema computacional, utilizando protocolo OpenFlow em ambiente SDN que analisa fluxos de dados e previne, através de descarte de pacotes, o envio de fluxos maliciosos pela rede. Etapa a realizar-se entre os meses de março e maio de 2017.

XI. Validação do resultado através de simulação com softwares e aplicação em rede de experimentações (*testbeds*). A validação será realizada nos meses de maio e junho de 2017.

XII. Apresentação no Seminário de andamento do TCII. Apresentação a ser realizada em junho de 2017.

XIII. Escrita do TC II. Etapa a ser realizada entre abril e junho de 2017.

XIV. Entrega do TC II. A entrega do TC II será em junho de 2017.

XV. Defesa do Trabalho de Conclusão. Evento que se realizará em julho de 2017.

CRONOGRAMA

As atividades serão desenvolvidas conforme cronograma a seguir.

	2016/2					2017/1				
	AGO	SET	OUT	NOV	DEZ	MAR	ABR	MAI	JUN	JUL
I	X									
II	X									
III	X	X								
IV		X								
V		X								
VI		X	X							
VII			X	X		X				
VIII		X	X	X						
IX					X					
X						X	X	X		
XI								X	X	
XII								X		
XIII							X	X	X	
XIV									X	
XV										X

REFERÊNCIAS

JANKOWSK,I D.; AMANOWICZ, M.. Intrusion Detection in Software Defined Networks with Self-organized Maps. Journal os Telecommunications and Information Technology (JTIT), Warsaw, Polônia, abr. 2015.

KIM, H.; FEAMSTER, N..Improving network manegement with software defined networking. IEEE Communications Magazine, v. 151, p. 114 - 119, fev. 2013.

KREUTZ, D. et al.. Software-Defined Networking A Comprehensive Survey. Cornell University Library. New York, 2014.

KREUTZ, D. et al.. Towards Secure and Dependable Software-Defined Networks. Proceendings of the second ACM SIGCOMM Workshop on Hot Topics in Software Defined Networking. Hong Kong, p. 55 - 60, ago. 2013.

ONF, OPEN NETWORKING FOUNDATION. OpenFlow. Disponível em: <https://www.opennetworking.org/sdn-resources/openflow>. Acesso em: 11 ago. 2016.

ONF, OPEN NETWORKING FOUNDATION. OpenFlow Switch Specification. Versão 1.0.0 (Wire Protocol 0x01). Dez. 2009. 44 p.

SATHYA, R.; THANGARAJAN, R.. Eficient Anomaly Detection and Mitigation in Software Defined Networking Environment. IEEE 2nd International Conference on Electronics and Communication Systems (ICECS). Coimbatore, p. 479 - 484, fev. 2015.

SAYEED, M. A. et al.. Intrusion Detection System based on Software Defined Network Firewall.1st International Conference on Next Generation Computing Technologies (NGCT). Dehradun, p. 379 - 382, set. 2015.

SCHEHLMANN, L. et al. Blessing or curse? Revisiting security aspects of Software-Defined Networking. IEEE 10th INternational Conference on Network and Service Management (CNSM) and Workshop. Rio de Janeiro, p. 382 - 387, nov. 2014.

SEEBER, S. et al.. Towards an SDN-enabled IDS environment. 2015 IEEE Conference on Communications and Network Security (CNS). Florence, p. 751 - 752, set. 2015.

SOARES, A. G. L. et al.. Estudo da Implementação de VoIP em redes SDN. Revista Científica Tecnologus. Recife, dez. 2015.

ZANNA, P. et al.. Adaptive Threat Management through the Integration of IDS into Software Defined Networks. IEEE International Conference and Workshop on the Network of the Future (NOF). Paris, p. 1 - 5, dez. 2014