IPSFlow – Uma Proposta de IPS Distribuído para Captura e Bloqueio Seletivo de Tráfego Malicioso em Redes Definidas por Software

Fábio Yu Nagahama[1], Fernando Farias[1], Elisângela Aguiar[1], Luciano Gaspary[2], Lisandro Granville[2], Eduardo Cerqueira[1], Antônio Abelém[1]

[1]Instituto de Tecnologia - Universidade Federal do Pará (UFPA)
[2]Instituto de Informática – Universidade Federal do Rio Grande do Sul (UFRGS)
{nagahama, fernnf, eaguiar, cerqueira, abelem}@ufpa.br,
{paschoal, granville}@inf.ufrgs.br

Abstract. *Traditional Intrusion Prevention Systems (IPS) have limitations in their operations. When running in active mode, IPSes do not have a wide coverage on the network and when capturing mirrored traffic they only block malicious one when working together with network devices from the same vendor or same solution. In this scenario, we introduce in this paper the IPSFlow, an IPS framework for Software Defined Networks (SDN) that, through the OpenFlow protocol, allows the creation of an IPS with wide coverage on the network, allowing the selective capture and automated blocking of malicious traffic near its source by combining the results of different techniques of traffic analysis.*

Resumo. *Os tradicionais sistemas de prevenção de intrusão (Intrusion Prevention Systems – IPS) possuem limitações em sua atuação. Quando operam no modo ativo, não possuem uma ampla cobertura na rede, e quando capturam tráfego espelhado, só bloqueiam o tráfego malicioso se atuarem em conjunto com equipamentos de rede do mesmo fabricante ou solução. Neste contexto, propomos neste artigo o IPSFlow, um framework de IPS para Redes Definidas por Software (Software Defined Networks - SDN) que, através do protocolo Openflow, possibilita a criação de um IPS com ampla cobertura na rede, permitindo a captura seletiva e o bloqueio automatizado de tráfego malicioso o mais próximo de sua origem, através da combinação dos resultados de diferentes técnicas de análise de tráfego.*

1. Introdução

A cada dia, novos ataques ou mesmo variações de ataques conhecidos surgem e são lançados na rede em busca de vulnerabilidades. De acordo com o Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br), só em 2011, foram quase 400.000 incidentes reportados [CERT 2012]. Desta forma, ferramentas que permitam a identificação e o tratamento automatizado de incidentes de segurança na rede tornam-se cada vez mais importantes na atividade realizada por um administrador.

Sistemas de Detecção de Intrusão de Rede (*Network Intrusion Detection Systems* – NIDSs) são ferramentas que capturam tráfego de rede, analisam e notificam o administrador quando da detecção de um possível tráfego malicioso. Já um Sistema de Prevenção de Intrusão (*Intrusion Prevention System* – IPS) estende a funcionalidade de

um IDS e, além de notificar, tem a capacidade de bloquear automaticamente o tráfego malicioso [Mukhopadhyay 2011].

Os IPSs e IDSs convencionais possuem limitações em sua atuação e necessitam de alguns cuidados em suas instalações. Dependendo do local de instalação, eles podem ter uma cobertura restrita, passando a falsa sensação de proteção. Aspectos de desempenho também devem ser considerados no dimensionamento do *hardware* utilizado nestas ferramentas para que não impactem no funcionamento da rede, permitindo, desta forma, uma análise mais apurada do tráfego capturado [Snyder 2008].

No geral, um IDS ou IPS utiliza apenas uma técnica de classificação e análise de tráfego, o que pode acarretar em uma atuação ineficiente ao considerar as taxas de detecção e falsos alarmes. A combinação de diferentes classificadores para a construção de um IDS híbrido vem sendo estudada, apresentando bons resultados [Panda, 2012].

Em uma Rede Definida por *Software* (*Sofware Defined Network* – SDN), o plano de controle é separado do plano de dados e é delegado a um elemento externo, permitindo que pesquisadores, administradores e usuários programem o comportamento da rede. Nesta arquitetura, a definição do funcionamento interno dos equipamentos de rede como *switches* e roteadores continua sob a responsabilidade de seus fabricantes.

O OpenFlow, proposto por McKeown *et al*. [McKeown 2008], é um *framework* aberto nos moldes das SDNs, que através do protocolo OpenFlow disponibiliza interfaces de programação para construção de controladores de rede. Em uma rede OpenFlow, o controlador tem uma visão completa da rede e, assim, tem a capacidade de manipular os fluxos de dados logo que estes são recebidos em qualquer *switch* que implemente as funcionalidades contidas na especificação [Openflow 2011]. O uso do OpenFlow, na área de segurança e monitoramento de redes, já foi abordado em pesquisas anteriores, como, por exemplo, nas pesquisas de Ballard *et al.* [Ballard 2010], Braga *et al.* [Braga 2010] e Mehdi *et al.* [Mehdi 2011].

Em Ballard *et al.* [Ballard 2010], o OpenSAFE foi proposto como uma solução para redirecionamento de tráfego com propósitos de monitoramento em conjunto com uma linguagem de alto nível que especifica fluxos, chamada de ALARMS (*A Language for Arbitrary Redirection for Measuring and Security*). No trabalho de Braga *et al.* [Braga 2010], o OpenFlow foi usado em conjunto a uma rede neural artificial do tipo SOM (*Self Organizing Maps*) para a detecção de ataques DDoS (*Distributed Denial of Service*), obtendo bons resultados. Mehdi *et al.* [Mehdi 2011] propuseram e avaliaram o uso do OpenFlow na captura de tráfegos anômalos nas redes de usuários domésticos ou de pequenas empresas conectadas a um provedor de serviço de Internet.

Apesar da existência dos trabalhos mencionados, ainda não se tem notícias de um ambiente que permita a captura seletiva do tráfego e o uso do resultado do IDS para bloqueio automatizado do tráfego malicioso, tal como é proposto neste artigo. Desta forma, devido à flexibilidade permitida pelas SDNs, apresentamos neste artigo o IPSFlow, um *framework* que utiliza o OpenFlow para a construção de um IPS com captura seletiva e distribuída de tráfego nos *switches* para análise em um ou mais IDSs. No IPSFlow, de acordo com o resultado da análise, o controlador OpenFlow poderá bloquear o fluxo de forma automática no *switch* mais próximo da origem do tráfego.

O restante deste artigo está organizado da seguinte forma. A seção 2 apresenta algumas dificuldades envolvidas no uso de um IPS na rede. Na seção 3, a arquitetura

das SDNs e o OpenFlow são abordados. A proposta da solução IPSFlow é explicada na seção 4. Por fim, as considerações finais e trabalhos futuros são discutidos na seção 5.

2. Desafios em Sistemas de Detecção e Prevenção de Intrusão na Rede

De acordo com o local de instalação de um sensor, este pode atuar como IDS ou IPS e possuir coberturas distintas. A Figura 1 representa uma visão simplificada de uma rede típica composta por um *switch* de núcleo interligando as demais redes através de *switches* de distribuição ou acesso. As posições identificadas com as letras A, B e C indicam alguns locais onde os sensores IPS ou IDS podem ser instalados. As linhas tracejadas identificadas com os números 1, 2 e 3 exemplificam alguns tipos de tráfego que uma estação interna à rede pode iniciar.

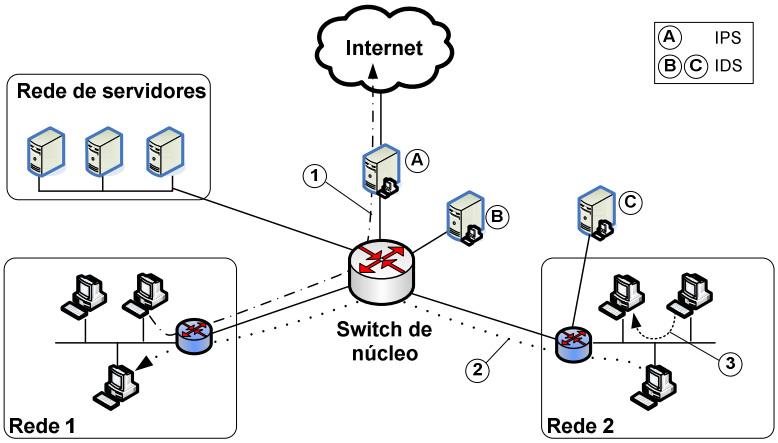

Figura 1. Visão geral de uma rede com IPS e IDSs.

Na posição A, o IPS atua no modo ativo (*inline)* e só consegue capturar e analisar o tráfego passante (*i.e.*, fluxo 1), não tendo ações sobre os demais tráfegos confinados dentro da rede (*i.e.*, fluxos 2 e 3). Para capturar os fluxos do tipo 2 e 3, o IPS pode ser conectado ao *switch* central (posição B) ou nos *switches* de distribuição (posição C) e receber uma cópia do tráfego através do espelhamento de portas (modo passivo). Porém, uma vez que apenas uma cópia do tráfego é recebida, o bloqueio de tráfego malicioso torna-se inviável e sua atuação fica restrita a apenas gerar alertas de forma semelhante a um IDS. Para que um tráfego seja bloqueado nas posições B e C, o IPS necessitaria atuar em conjunto com um equipamento capaz de bloquear o tráfego malicioso e esta é uma situação rara de acontecer devido à variedade de fabricantes e modelos de equipamentos utilizados nas redes.

Em quaisquer das posições (A, B ou C), não é comum que o tipo de tráfego a ser encaminhado aos IDSs e IPSs seja filtrado previamente. Assim, o *hardware* destas ferramentas deve ser devidamente dimensionado para que as etapas de captura, análise e eventual reencaminhamento do tráfego não adicionem retardos excessivos aos pacotes (no caso do IPS) ou para que todos os pacotes copiados sejam recebidos e analisados adequadamente para uma avaliação mais apurada (no caso do IDS).

Balancear a carga adicionando mais IPSs e/ou IDSs pode evitar um eventual superdimensionamento do *hardware*. Porém, a adição de IPSs *inline* pode acarretar na adição de mais retardo nos pacotes. Para o caso de IDSs passivos, a limitação passa a ser dos *switches*, visto que nem todos são capazes de realizar o espelhamento de um

número elevado de portas [Ballard 2010]. Além disso, pelos mesmos motivos expostos, o uso de diferentes sensores com diversas técnicas de análise torna-se inviável.

A atuação limitada dos IDSs leva a crer que a distribuição de IPSs ao longo da rede tende a ser uma solução inevitável. Porém, a sincronização e a administração de diversos sensores tornam-se tarefas onerosas e inviáveis para o administrador da rede. As soluções de IPSs *inline* distribuídos de grandes fabricantes facilitam a administração, mas implicam na dependência de seus clientes com os fornecedores. Nesses casos, a adição de módulos ou mesmo a atualização do ambiente tendem a ser restritos apenas ao fornecedor, inviabilizando qualquer tipo de personalização por parte do administrador da rede. Mesmo em soluções com *softwares* livres, questões como desempenho, administração onerosa e sincronização de informação tornam-se um problema.

3. Redes Definidas por *Software*

Os equipamentos de redes como *switches* e roteadores convencionais implementam os planos de controle e de dados acoplados dentro do mesmo *hardware*. Desta forma, qualquer funcionalidade nova só pode ser definida pelo fabricante do equipamento, tornando-se uma arquitetura engessada do ponto de vista de novas funcionalidades. Já na arquitetura das Redes Definidas por *Software*, os planos de controle e de dados são separados, e com isso a definição do funcionamento da rede fica a cargo do administrador, enquanto que a implementação do mecanismo de comutação dos dados permanece sob o sigilo dos fabricantes. Portanto, a inteligência e o estado da rede são logicamente centralizados e, como resultado, as redes têm potencial para se tornarem mais flexíveis e facilmente adaptáveis [OpenFlow 2011].

Com as SDNs, o administrador passa a ter o controle da rede através de um ponto lógico central independentemente do fabricante do equipamento, o que simplifica bastante sua operação. Através da centralização do plano de controle, as SDNs permitem que a rede seja dinamicamente configurada por aplicações desenvolvidas pelos próprios administradores ou usuários da rede.

O OpenFlow é o primeiro padrão de interface de comunicação que especifica um protocolo com o propósito de interconectar os planos de controle e de dados definidos pela arquitetura de SDN, e vem recebendo o reconhecimento e apoio de grandes fabricantes e empresas de Tecnologia da Informação. Ele trabalha com o conceito de fluxos para definir tráfegos de rede baseado em regras predefinidas, que podem ser configuradas de forma estática ou dinâmica por um controlador SDN.

O *framework* Openflow é composto basicamente por 5 componentes: o controlador, que define o plano de controle; o *switch* (também conhecido como *datapath*), que continua sendo o responsável pelo encaminhamento dos pacotes no plano de dados; o canal seguro para a comunicação entre o controlador e o *datapath*; o protocolo OpenFlow, que define como a comunicação entre o controlador e o *datapath* é realizada; e a tabela de fluxos, que é o local onde as ações para os fluxos são definidas dentro do *datapath*.

O funcionamento básico do OpenFlow consiste em, ao receber o primeiro pacote do fluxo no primeiro *datapath* da rede, verificar se há algum tratamento definido na tabela de fluxos. Havendo uma entrada na tabela de fluxos, a ação definida é executada. Caso contrário, os dados do fluxo são extraídos, encapsulados e encaminhados ao controlador para tomada de decisão. O controlador consulta a aplicação utilizada na

rede e decide como o tráfego deve ser tratado. Uma resposta é enviada ao *datapath* que atualiza a tabela de fluxos com as instruções recebidas e os pacotes subsequentes do mesmo fluxo receberão o mesmo tratamento, até que a entrada na tabela de fluxos seja removida [Openflow 2011].

Diante do exposto, a arquitetura de SDNs torna-se uma grande aliada na administração de IPSs, pois combina a rápida comutação de pacotes no plano de dados com a flexibilidade e a visão única do plano de controle [Lantz 2010]. Desta forma, o uso da arquitetura SDN favorece o aumento da área de abrangência do IPS, permitindo este atuar de uma maneira mais proativa na origem do problema.

4. IPSFlow

Diante do apresentado, este artigo propõe um *framework* de IPS denominado de IPSFlow, que utiliza uma rede baseada no modelo de SDN em conjunto com o protocolo OpenFlow e possibilita a criação de um IPS com ampla cobertura na rede e a capacidade de capturar seletivamente um fluxo para posterior análise em um ou mais IDSs. Além disso, o IPSFlow prevê mecanismos para que os resultados de diferentes IDSs sejam combinados para o bloqueio automático de um tráfego malicioso, o mais próximo de sua origem. O IPSFlow possui dois elementos fundamentais: uma aplicação denominada de IPSFlowApp, que define como a SDN baseada no OpenFlow deve funcionar, e um ou mais IDSs para análise do tráfego.

4.1. Arquitetura e funcionamento do IPSFlow

A Figura 2(i) apresenta uma visão geral da composição do IPSFlow em uma SDN. Quando o primeiro pacote de um fluxo é recebido no primeiro *datapath* (passo 1), o processo de consulta à tabela de fluxos e o controlador seguem conforme especificado no OpenFlow [Openflow 2011] (passo 2). Ao receber uma consulta de um *datapath*, o controlador verifica se no IPSFlowApp há uma regra definida para captura e análise do tráfego recebido (passo 3).

Caso o fluxo esteja definido para ser analisado, este pode ser tratado de duas formas no *datapath.* Na primeira, o fluxo pode ser encaminhado para o destinatário (passo 4) e uma cópia enviada para análise em um conjunto de IDSs (passo 5). Ao se concluir que o fluxo se trata de um tráfego malicioso, os IDSs enviam o resultado ao controlador (passo 6) para que o tráfego passe a ser bloqueado no *datapath*. Esta decisão pode ser armazenada no controlador para ser reutilizada em futuras consultas.

Na segunda forma, o fluxo pode ser retido no *datapath* e uma cópia enviada para análise em um conjunto de IDSs. Neste momento, um contador decrescente definido pelo administrador é inicializado. Caso a análise conclua que o tráfego seja malicioso antes do contador chegar a zero, o resultado é enviado ao controlador para instruir o *datapath* a descartar os pacotes retidos. Caso o contador chegue a zero, o tráfego é liberado para o seu destino. Se após a liberação do tráfego, for constatado que este se tratava de um tráfego malicioso, a tabela de fluxo é alimentada para descartar pacotes subsequentes daquele fluxo.

4.2. A aplicação IPSFlowApp

Os elementos que compõem o IPSFlowApp são apresentados na Figura 2(ii): módulo de configuração (a), base de regras (b), agente (c) e módulo de alertas (d). O módulo de

configuração é o ponto de comunicação entre a aplicação e o administrador e é neste módulo que ocorre toda a definição de quais ações devem ser tomadas nos fluxos. Estas decisões são armazenadas na base de regras para serem consultadas pelo agente. Ele também é responsável por receber e tratar as notificações de alertas, podendo reconfigurar automaticamente a base de regras de acordo com as definições do administrador e acionar o agente para realizar o descarte do tráfego malicioso.

A base de regras é o local onde todas as ações a serem tomadas com os fluxos são armazenadas, por exemplo, bloqueio de fluxo, encaminhamento de fluxo por uma porta com cópia para análise ou retenção com cópia para análise (como apresentadas anteriormente).

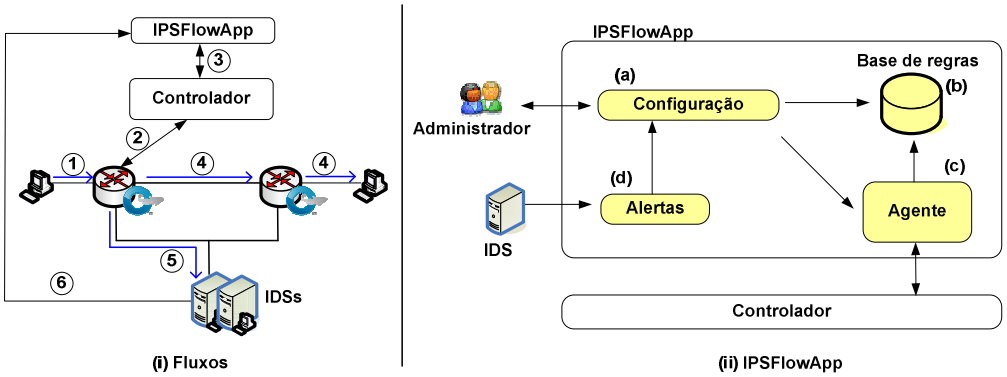

Figura 2. *Framework* IPSFlow.

O agente é o elemento responsável pela comunicação entre o controlador e a aplicação. É ele que recebe a consulta do controlador, extrai as informações necessárias e pesquisa na base de regras à procura de ações que devam ser tomadas para o fluxo recebido. Havendo uma regra definida, a ação é encaminhada ao controlador para as devidas configurações nos *datapaths*. Caso não haja regra alguma, uma regra padrão de encaminhamento adiante pode ser dada como resposta. Ele também é responsável por instruir o controlador a descartar fluxos detectados como maliciosos.

O módulo de alertas é o responsável por receber, tratar o resultado da análise dos IDSs e notificar o módulo de configuração. Para permitir a utilização de diversos IDSs, o módulo de alerta define um formato padrão esperado para receber os resultados de forma semelhante ao documento experimental 4765 do IETF [Debar, 2007].

É válido ressaltar que a utilização de SDNs para propósitos de segurança mostrou-se bastante promissora em trabalhos anteriores [Ballard 2010], [Braga 2010] e [Mehdi 2011]. Porém, estes trabalhos se limitaram a apenas detectar e alertar a ocorrência de tráfegos maliciosos na rede. A proposta do IPSFlow é estender estes trabalhos, uma vez que passa a ter uma visão centralizada e completa da rede e assim permitir a captura do tráfego em qualquer local da rede, encaminhar o tráfego para análise em um ou mais IDSs e utilizar o resultado das análises para a reconfiguração automática das tabelas de fluxos dos *datapaths*.

5. Considerações finais e trabalhos futuros

Com o crescimento das redes, a diversificação dos dispositivos de rede utilizados e o aumento de usuários conectados em rede, o aumento de incidentes de segurança torna-

se inevitável. Desta forma, cada vez mais ferramentas como IDSs e IPSs se fazem necessários na administração da segurança de uma rede.

O IPSFlow proposto neste artigo utiliza o protocolo OpenFlow e viabiliza uma administração simplificada e centralizada, com solução aberta e flexível permitindo a análise do tráfego por um ou IDSs. Além disso, uma vez que o IPSFlow prevê a captura seletiva, esta não exige o uso de *hardwares* superdimensionados nos IDSs, possibilitando inclusive o uso de diversos tipos de IDSs com especialidades distintas. Com atuação em todos os *switches* da rede, o IPSFlow potencialmente apresenta uma cobertura mais ampla e com a captura de tráfego sendo feita sem a necessidade de espelhamento de portas, permite o bloqueio do tráfego malicioso o mais próximo de sua origem.

Para trabalhos futuros, tem-se o desenvolvimento da aplicação IPSFlowApp e a validação da proposta através da criação de um *testbed* utilizando tráfego capturado em uma rede real. Testes de desempenho da solução variando e/ou combinando diversos tipos de IDSs também deverão ser executados para coleta e comparação de resultados.

Referências

Ballard, J., Rae, I., Akella, A. **Extensible and Scalable Network Monitoring Using OpenSAFE**. Internet Network Management Workshop / Workshop on Research on Entreprise Networking. San Jose, CA. 27 Abr. 2010.

Braga, R. S., Mota, E., Passito, A. **Lightweight ddos floding attack detection using nox/openfow**. IEEE Conference on Local Computer Networks (2010), IEEE.

CERT, **Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil**. Disponível em: <http://www.cert.br>. Acesso em 25 out. 2011.

Debar, H., Curry, D., Feinstein, B. **The Intrusion Detection Message Exchange Format**. 2007. Disponível em: <http://tools.ietf.org/html/rfc4765>. Acesso em 20 mai. 2012.

Lantz, B., Heller, B., and McKeown, N. (2010). **A network in a laptop: rapid prototyping for software-defined networks**. ACM SIGCOMM Workshop on Hot Topics in Networks, Hotnets '10, pages 19:1–19:6, New York, NY, USA. ACM

McKeown, N., Anderson, et al. **OpenFlow: Enabling Innovation in Campus Networks**. Computer Communication Review. 2008. Disponível em: <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.141.2269&rep=rep1&type=pdf >. Acesso em 20 ago. 2011.

Mehdi, S. Khalid, J., Khayam, S. **Revisiting Traffic Anomaly Detection using Software Defined Networking.** Recent Advances in Intrusion Detection (RAID), 2011. Disponível em: < http://www.wisnet.seecs.nust.edu.pk/publications/2011/raid2011_paper.pdf>. Acesso em 21 jan. 2012.

Mukhopadhyay, I., Chakraborty, M., Chakrabarti, S. **A Comparative Study of Related Technologies of Intrusion Detection & Prevention Systems**. Journal of Information Security, 2011, v. 2, p. 28-38.

OpenFlow. **The OpenFlow Switch Specification**. Disponível em: <http://OpenFlowSwitch.org>. Fevereiro 2011. Acesso em 27 set. de 2011.

Panda, M., Abraham, A., Patra, M. R. **A Hybrid Intelligent Approach for Network Intrusion Detection**. Procedia Engineering, 2012, v. 30, p. 1-9.

Snyder, J. **Guide to Network Intrusion Prevention Systems.** Disponível em: <http://www.pcworld.com/businesscenter/article/144634/guide_to_network_intrusion_prevention_systems.html>. Outubro 2008. Acesso em 20 fev. 2012.

