UNIVERSIDADE FEDERAL DO AMAZONAS
PRO REITORIA DE PESQUISA E PÓS-GRADUAÇÃO
DEPARTAMENTO DE APOIO A PESQUISA
PROGRAMA INSTITUCIONAL DE INICIAÇÃO CIENTÍFICA

REMEDIAÇÃO DE ATAQUES EM REDE DEFINIDA POR SOFTWARE, UTILIZANDO PRIMITIVAS DE SEGURANÇA

Bolsista: Jordan de Sá Queiroz, FAPEAM

MANAUS
2015

UNIVERSIDADE FEDERAL DO AMAZONAS
PRO REITORIA DE PESQUISA E PÓS-GRADUAÇÃO
DEPARTAMENTO DE APOIO A PESQUISA
PROGRAMA INSTITUCIONAL DE INICIAÇÃO CIENTÍFICA

RELATÓRIO PARCIAL
PIB-E/0208/2014
REMEDIAÇÃO DE ATAQUES EM REDE DEFINIDA POR SOFTWARE, UTILIZANDO PRIMITIVAS DE SEGURANÇA

Bolsista: Jordan de Sá Queiroz, FAPEAM
Orientador: Prof° Dr° Alexandre Passito de Queiroz

MANAUS
2015

Esta pesquisa é financiada pela Fundação de Amparo à Pesquisa do Estado do Amazonas - FAPEAM, através do Programa Institucional de Bolsas de Iniciação Científica da Universidade Federal do Amazonas.

RESUMO

O trabalho discorre sobre uma proposta de solução para remediar ataques Distribuídos de Negação de Serviço (*Distributed Denial of Service - DDoS*) em um novo paradigma de redes, conhecido como Rede Definida por Software (Software-Defined Networking - SDN). SDN fornece novas possibilidades que as redes atuais, também conhecidas como redes legadas, não provêm. Então, a solução aqui proposta explora os novos conceitos e meios de SDN para impedir, da forma mais eficiente possível, os tipos de ataque mencionados anteriormente. Para o problema ser melhor entendido, foram estudados *papers*, tutoriais sobre as ferramentas que foram utilizadas, cursos a distância sobre as tecnologias que foram usadas para realizar os experimentos, e seminários técnicos semanais sobre os sobre os *papers* recentemente estudados pelos membros do grupo de pesquisa. Esses estudos chegaram em fase de conclusão, juntamente com os experimentos, que foram executados em ambiente virtual. Para os experimentos que realizados, notou-se que um simples controlador não é o suficiente para tirar o máximo proveito de SDN, porque embora seja possível controlar componentes da rede utilizando-os, os controladores permitem que as aplicações conversem diretamente com os dispositivos, quase a um nível de tradução, mas essas aplicações desenvolvidas precisam ser executadas em um ambiente com mais resiliência, confiabilidade, ou seja, em um ambiente que possa prover mais do que um "serviço" de tradução. Um sistema operacional (Network Operating System - NOS) de redes suporta as aplicações que são desenvolvidas, oferecendo mais serviços e abstrações que um controlador por si só não tem (i.e resiliência, melhor visão da topologia da rede, maior facilidade para fazer *deploy* de novos componentes, compatibilidade com redes legadas). Como resultado, uma ferramenta com o objetivo de mitigar ataques DDoS foi implementada e testada.

Palavras chave: DDoS, SDN, NOS, mitigação

ABSTRACT

This work talks about a solution to mitigate Distributed Denial of Service (DDoS) attacks in a new computer networking paradigm, known as Software-Defined Networking (SDN). SDN provides new possibilities that the current computer networking paradigm, known as legacy networks doesn’t do. Therefore, the solution proposed here exploits new concepts and methodology in SDN to mitigate, more efficiently, the kind of attacks shown above. To better understand the problem, it has been studied papers, tutorials about the tools that were used, distance course about technologies that was used to do experiments, weekly technical sessions about recent-studied papers by the research group’s members. These studies has been with experiments, that are were run on virtual environment. For the experiments, it is possible to note that a simple network controller is not enough to make a better use of SDN’s features , even though it is possible to control network components by using a network controller, these controllers allow the network application to directly communicate with the network devices, in an almost translation level, but these network applications need to be executed in a more resilient, trustworthy environment, in other words, they must be executed in a platform that provides more than just a “translation service”. A network operating system (NOS) supports network applications, providing them more services and abstractions that a simple controller by itself does not (i.e resilience, better vision of the topology, a easier way to deploy new components, backward compatibility with legacy computer networking). As a final result, a mechanism in which the objective is to mitigate DDoS attacks was implemented and tested.

Key words: DDoS, SDN, NOS, mitigating

SUMÁRIO

INTRODUÇÃO..... 7
REVISÃO BIBLIOGRÁFICA..... 11
2.1 OpenFlow: Enabling Innovation in Campus Networks..... 11
2.2 The Case for Separating Routing From Routers..... 11
2.3 The Road To SDN..... 11
2.4 ONOS: Towards an Open, Distributed SDN OS..... 12
2.5 DDoS Attack Protection in the
Era of Cloud Computing and Software-Defined Networking..... 12
2.6 A Survey of Defense Mechanisms
Against Distributed Denial of Service (DDoS) Flooding Attacks..... 12
2.7 Software-Defined Networking: A Comprehensive Survey..... 13
2.8 To Filter or to Authorize: Network-Layer
DoS Defense Against Multimillion-node Botnets..... 13
2.9 Redes de Computadores e A Internet -
Uma Abordagem Top-Down - 6ª Ed. 2013..... 13
DESENVOLVIMENTO..... 14
RESULTADOS E DISCUSSÕES..... 18
REFERÊNCIAS..... 20

INTRODUÇÃO

Ataques Distribuídos de Negação de Serviço (Distributed Denial of Service - DDoS) exploram falhas em protocolos da Internet. Tais ataques são capazes de impossibilitar que um usuário autêntico usufrua de algum serviço na Internet ou impedem algum serviço de funcionar normalmente, podendo, assim, acarretar grandes danos financeiros. Entende-se serviço como sites que fornecem algo de utilidade para alguém, por exemplo, sites de compras, pesquisa, entre outros.

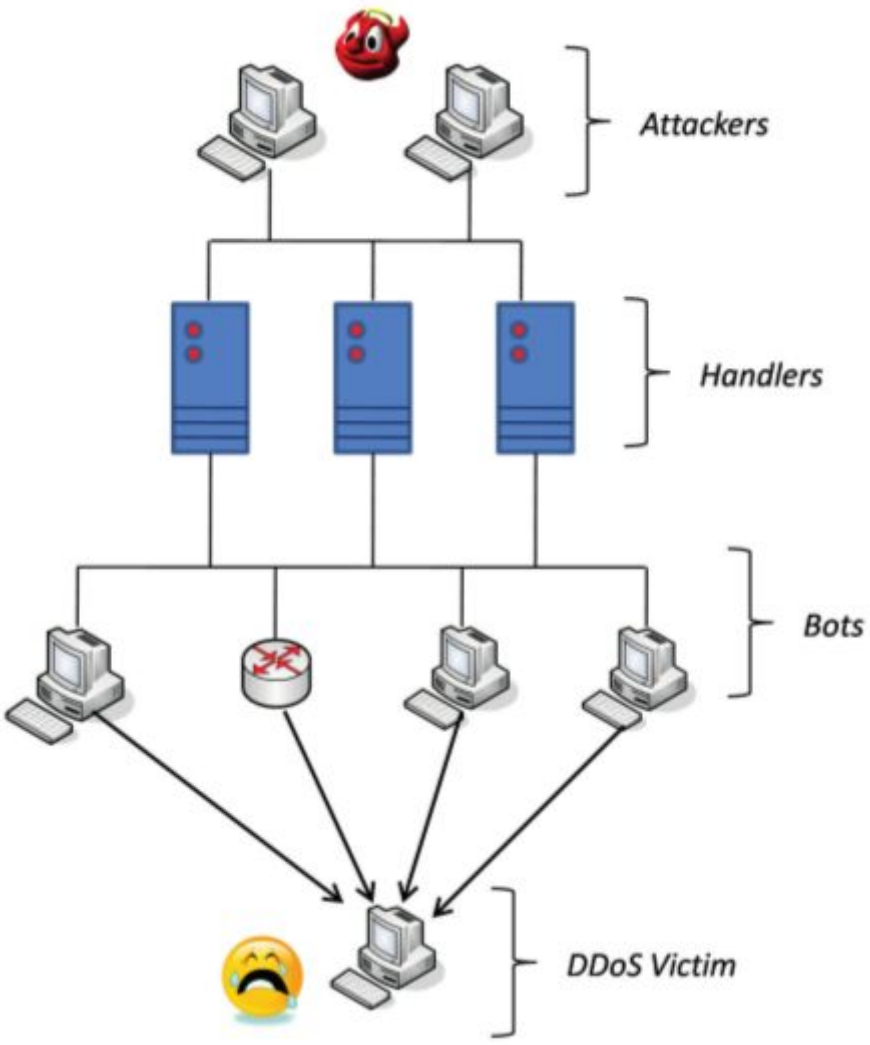

Figura 1: Arquitetura de um ataque DDoS. Fonte: A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks.

Esses ataques são criados através do uso de dispositivos infectados que estão conectados em uma rede. Tais equipamentos, muitas das vezes colaboram para realizar essas atividades sem mesmo saber que a estão fazendo. O atacante explora as vulnerabilidades de uma rede, para então ganhar acesso a mesma e, consequentemente, poder criar e organizar um exército de computadores zumbis que vão acatar todas as suas ordens, tais zumbis também são conhecidos como Botnets.

Uma vez que um atacante tenha o controle sobre as máquinas e uma vez que os botnets são criados, ele pode organizar, dando ordens para os computadores infectados, cada um sendo controlado a partir de um Botnet, um ataque DDoS contra um alvo específico. O quanto mais computadores infectados o atacante tiver sob controle, mais danos o ataque vai conseguir desencadear. É importante lembrar que esses dispositivos de redes podem estar no mesmo local (i.e na mesma casa) ou podem estar em um outro país e/ou continente. Daí o motivo de ser distribuído. Além da capacidade do atacante infectar os computadores em uma rede, os próprios computadores que já estão com o botnet podem infectar outros computadores, deixando o ataque cada vez mais potente e escalável.

Existem pesquisas nessa área, mas a grande maioria dela são soluções para as redes de computadores como conhecemos amplamente e atualmente a utilizamos, um paradigma de rede conhecido como rede legada. Em redes legadas, os dispositivos de redes possuem o plano de dados (responsável por transmitir pacotes) e a o plano de controle (o cérebro da rede) acoplados no mesmo dispositivo.

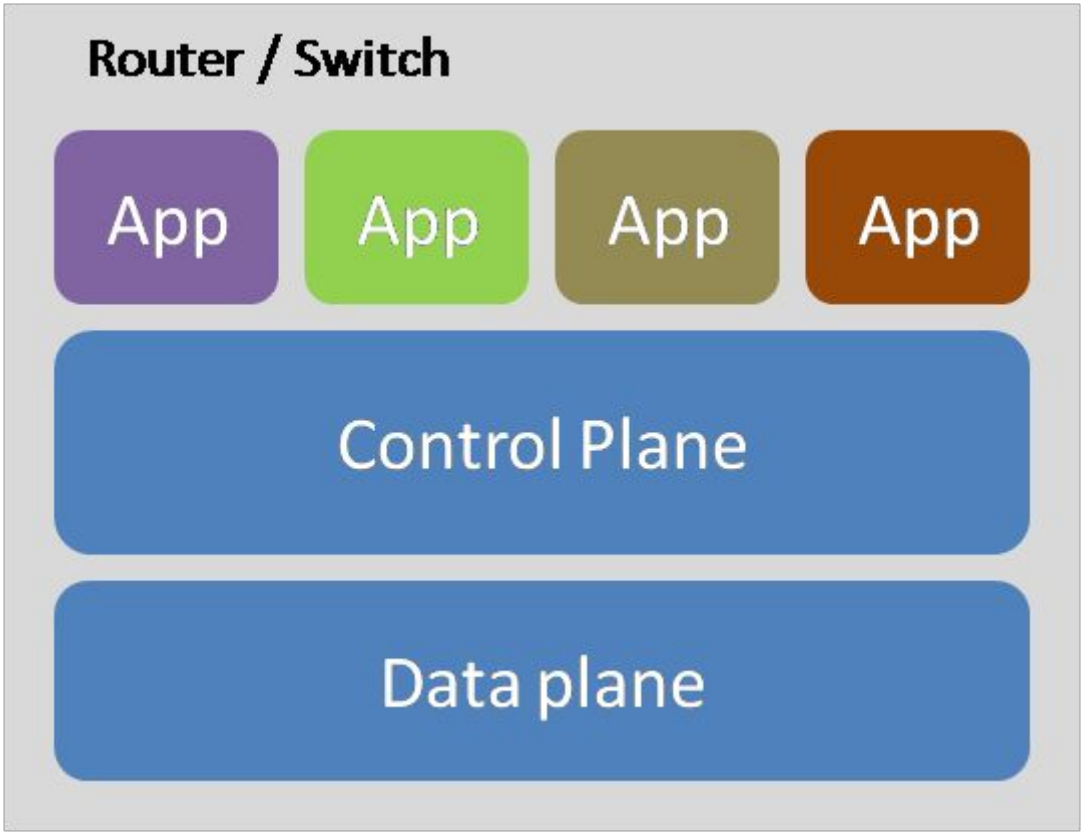

Figura 22: Estrutura das redes legadas. Fonte: http://3.bp.blogspot.com/-k_Prr-4E220/UNl0smmjkJI/AAAAAAAAK4s/-W998dpkjiQ/s1600/Figure+1+-+Legacy+Network+Architecture.png

O objetivo desse trabalho é pesquisar e desenvolver uma solução para o problema de ataque DDoS, mas para um novo paradigma de redes, que surgiu por volta de 2008. Esse novo paradigma é conhecido como Rede Definida por Software (Software-Defined Networking - SDN). Em SDN, ao contrário das redes legadas, os o plano de dados é desacoplado do plano de controle, sendo que este último fica executando (i.e rodando) em um computador dedicado e o primeiro fica nos dispositivos de repasse da rede (i.e *switches*).

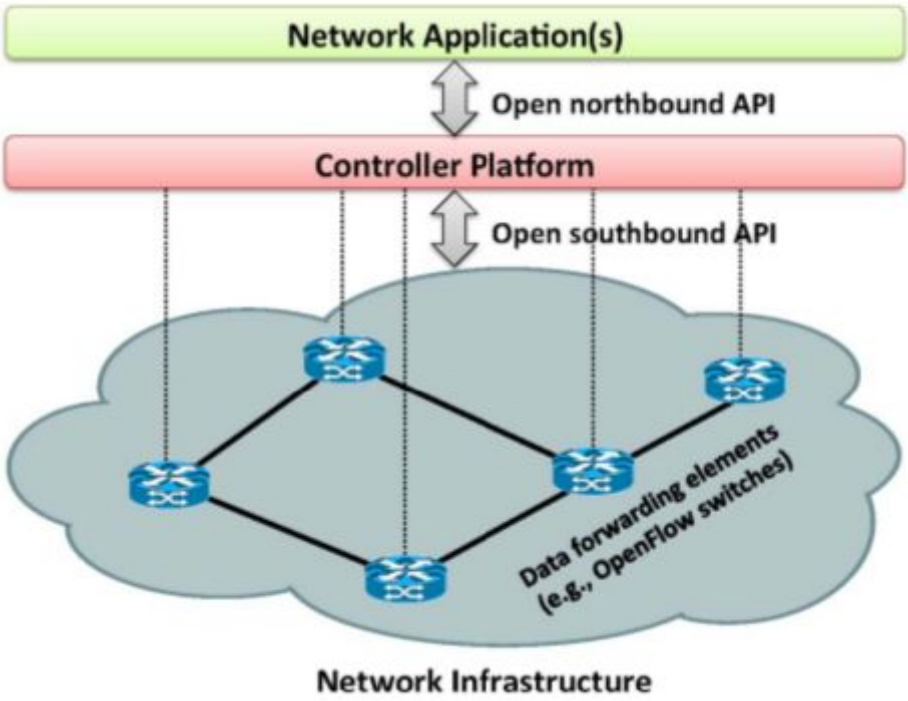

Figura 3: Infraestrutura da SDN. Fonte: Software-Defined Networking: A Comprehensive Survey.

Essa solução tem como objetivo explorar os novos mecanismos que SDN provê, afim de deixar a Internet mais segura, tentando sempre impedir ou, pelo menos reduzir ao máximo os danos e prejuízo que os ataques DDoS podem desencadear.

Remediar esses ataques é de extrema importância pois eles podem gerar muitos prejuisos tanto para as empresas, para o governo e para as pessoas. Suponha que o site da Fazenda esteja sobre um ataque desses, tanto o governo quanto as pessoas ficarão muito prejudicadas. Impedir que esses ataques aconteçam é uma das maiores preocupações dos especialistas em segurança de rede. Por tanto, um dos objetivos deste trabalho é contribuir mais para a segurança da Internet.

REVISÃO BIBLIOGRÁFICA

2.1 OpenFlow: Enabling Innovation in Campus Networks

O artigo faz uma proposta de um novo protocolo aberto que permite redes de testes coexistir com redes de produção. De acordo com o artigo, esse protocolo pode ser instalado em dispositivos de redes, bastando o fabricante realizar essa instalação sem precisar fazer alterações no *hardware* do componente de rede. Uma das vantagens desse protocolo, segundo o *paper*, é que com uma interface aberta e padronizada (nesse caso, o *OpenFlow*), é possível ficar livre das restrições e limitações impostas por protocolos fabricados pelas empresas dos equipamentos de rede.

2.2 The Case for Separating Routing From Routers

O artigo mostra que o roteamento das redes legadas começou a ficar cada vez mais complexos por causa dos vários dispositivos e hosts que estão conectados à rede, além disso, os dispositivos estão espalhados pela rede de forma distribuída e cada um deles, por tanto, executa um algoritmo também de forma distribuída, colaborando mais ainda para a complexidade da rede, tornando-a mais difícil de ser gerenciada. Então esse *paper* propõe separar o roteamento (feito pelos protocolos, a parte inteligente) da parte responsável por realizar os repasses dos pacotes (feito pelo próprio dispositivo de rede). Conseguindo separar esses dois elementos, é possível tornar uma rede algo menos complexo de gerenciar.

2.3 The Road To SDN

O *paper* mostra um novo paradigma de rede, onde é mais fácil de gerenciar as redes. O resultado desse novo paradigma, segundo o artigo, foram as pesquisas anteriormente feitas, na tentativa de deixar as redes de computadores mais programáveis, independente do fabricante de um determinado equipamento de rede (e.g *switch* ou roteador). Além da gerência mais facilitada, SDN também separa a camada de dados (onde ficam os protocolos) da camada de repasse (responsável por repassar os pacotes para outro dispositivos ou *host* final), alegando de que dessa

maneiras, com os dois elementos separados, ambos podem evoluir independentemente um do outro e permitir mais inovação.

2.4 ONOS: Towards an Open, Distributed SDN OS

Esse *paper* apresenta experimentos feitos em dois protótipos do ONOS, um sistema operacional de redes que possui foco em performance, escalabilidade e disponibilidade. O primeiro experimento realizado teve como objetivo permitir que ONOS fosse tolerante a falhas, distribuído (mas logicamente centralizado) e escalável. O segundo experimento teve como objetivo aumentar a performance do do sistema. Esse sistema operacional provê a infraestrutura necessárias para se programar e executar aplicações capazes de controlar uma rede de computadores.

2.5 DDoS Attack Protection in the Era of Cloud Computing and Software-Defined Networking

Esse artigo apresenta uma proposta para defender as redes de empresas que trabalham com *cloud computing* e que ao mesmo tempo usam SDN para prover tal serviço para os clientes. Os desafios de segurança que apareceram com a junção dessas duas tecnologias são grandes e precisam ser resolvidos, então os autores do *paper* propuseram uma ferramenta de detecção e mitigação de ataque DDoS que pudesse solucionar as falhas de segurança que foram identificadas.

2.6 A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks

Esse *paper* mostra o escopo dos ataques DDoS, classificando-os e mostrando algumas das principais razões que levam a alguém praticar esses tipos de ataque, bem como os grandes prejuízos que esse tipo de ataque pode causar para a vítima. O artigo também apresenta algumas medidas já propostas e desenvolvidas para combater essa ameaça, sendo que cada uma delas possui uma classificação na taxonomia dos ataques DDoS.

2.7 Software-Defined Networking: A Comprehensive Survey

Esse artigo mostra o que é SDN e como esse paradigma de redes difere da rede legada, que hoje são usadas em larga escala. Algumas motivações para a adoção de SDN também é mostrada, além das explicações dos conceitos e de como é a arquitetura, em camadas, de SDN. A apresentação das camadas é feita no estilo bottom-up.

2.8 To Filter or to Authorize: Network-Layer DoS Defense Against Multimillion-node Botnets

Esse artigo apresenta uma ferramente de mitigação contra ataques DDoS, o *StopIt*. Esse mecanismo de defesa é híbrido, baseado em filtros e feito para combater ataques a nível de rede que tem como alvo um *end-host*. Ao final de descrever a ferramenta, é feita uma comparação do desempenho da mesma com outras ferramentas que possuem uma classificação diferente da do *StopIt*, nesse caso, os sistemas de mitigação baseado em capacidades (ou *capabilities*, em inglês). Além disso, na sessão de análises, o artigo mostra o "momento certo" de quando melhor usar uma ferramenta de mitigação baseada em filtros (*filter-based*) e ferramentas baseadas em capacidades (*capability-based*)

2.9 Redes de Computadores e A Internet - Uma Abordagem Top-Down - 6ª Ed. 2013

O livro apresenta conceitos de redes e ensina como a internet está organizada, mostrando as camadas de protocolos e explicando como cada uma delas funciona, incluindo os seus algoritmos. Esse livro usa a abordagem *top-down* para apresentar as camadas de rede.

DESENVOLVIMENTO

Afim de começar o experimento de mitigação de ataque DDoS, foram pesquisadas ferramentas capazes de simular tais ataques em um ambiente controlado, de forma a não comprometer outros computadores na rede. Essa simulação será executada em ambiente virtual, com a topologia de rede *single* e *linear*, cada uma delas com vinte e quatro *hosts*.

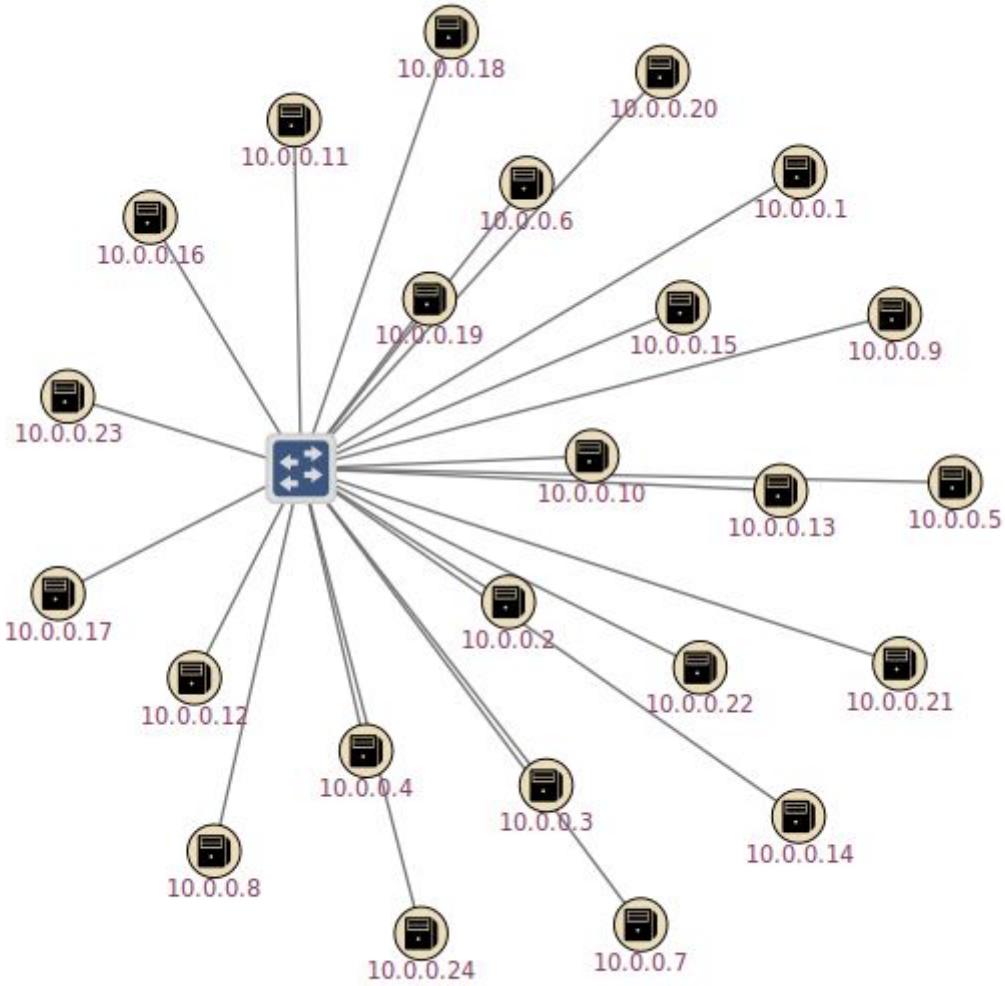

Figura 44: Topologia single com 24 hosts

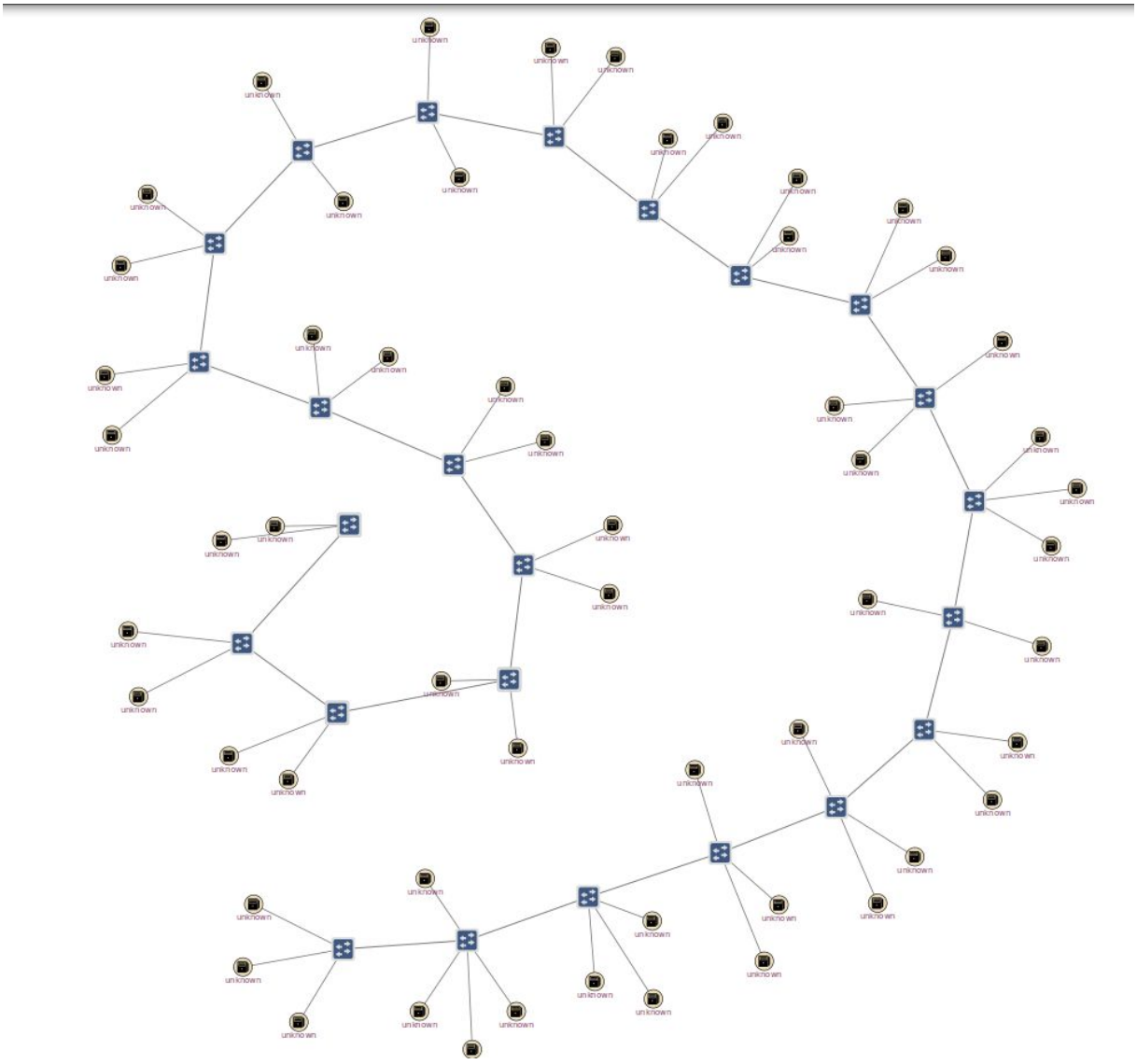

Figura 5: Topologia linear com 24 hosts

Alguns experimentos foram realizados utilizando equipamentos de redes (i.e *switches*) físicos que suportam o protocolo *OpenFlow*. Esses switches são do modelo P-3290, com 48 portas de produção e dão suporte às versões 1.0, 1.1, 1.2 e 1.3 do OpenFlow, fabricado pela Pica8. Esses experimentos têm como objetivo capacitar os membros do grupo a operar dispositivos físicos e fazer estudos de casos e um ambiente real.

Para controlar a rede, inicialmente se utilizou o NOX, um controlardor de rede que dá suporte apenas ao OpenFlow 1.0, embora exista um *fork* desse controlador que suporta algumas versões posteriores (i.e 1.1, 1.2,

1.3). Um dos experimentos feitos usando esse controlador foi a implementação de um firewall simples e a conexão do *switch* físico com esse controlador, para controlar uma rede experimental de computadores. Depois de algum tempo, foi decidido trocar o NOX pelo ONOS (*Open Network Operating System*), o primeiro sistema operacional de redes que provê várias funcionalidades e suporte para as aplicações implementadas nele. O ONOS é um controlador *open source*, agnóstico ao tipo de protocolo utilizado, ou seja, não está limitado ao *OpenFlow*. Essa possibilidade de trabalhar com vários protocolos e o amplo suporte da comunidade são um dos motivos que justificam a troca do NOX pelo ONOS no contexto desse trabalho.

Propõe-se um componente de mitigação de ataques DDoS para SDN, essa proposta é de criá-lo com base em conceitos já conhecidos em redes legadas, no caso dessa aplicação, ela será baseada em uma outra aplicação de mitigação existente, o *StopIt*.

O *StopIt* foi escolhido porque ele é híbrido, isso significa que ele pode ser instalado em qualquer lugar da rede (e.g perto do atacante, perto da vítima, ou entre o atacante e vítima), facilitando a atividade de detecção proposta pela pesquisa "detecção de ataques em redes definidas por software", que é mais fácil de ser feita perto da vítima e facilitando também a mitigação, que é mais eficiente se for feita o mais perto possível da fonte do ataque. Além disso, o *StopIt* é baseado em filtro, o que o torna eficiente quando o alvo do ataque é um *end-host*, e a proposta do novo componente de mitigação é proteger os *end-hosts.*

Embora o *StipoIt* tenha muitas qualidades boas, a implementação do mesmo pode ser muito custosa, devido às configurações manuais que precisam ser feitas em computadores, servidores e em roteadores. Pode ser um problema implantar o *StopIt* em uma rede que possui uma topologia muito grande, devido a quantidade de trabalho para fazer a configuração.

Então a proposta é aproveitar os pontos fortes do *StopIt* e criar um componente de mitigação DDoS baseado nele, mas para SND, afim de reduzir a complexidade da configuração manual em cada dispositivo de rede.

A aplicação foi desenvolvida em Java e a abordagem da mesma é fazer o bloqueio considerando as seguintes características: Porta do protocolo da camada de transporte e o endereço MAC. A razão dessa decisão é que em uma rede pode haver algum *host* mal intencionado se comunicando com vários outros *hosts* na mesma rede, mas não necessariamente atacando a todos. Isso quer dizer que embora mal intencionado, o atacante deve ser impedido apenas de enviar pacotes maliciosos, mas não deve ter a comunicação totalmente cortada, pois o *host* mal intencionado não está atacando todos na rede, apenas um alvo específico.

Então a filtragem utilizando essas duas características ajudam a tratar essa situação, pois é possível saber com mais detalhes quem é o *host* mal intencionado e que tipo de pacotes ele está enviando afim de prejudicar outro *host* na rede. Sabendo disso, é possível impedir a comunicação que é indesejada, sem precisar cortar todas as outras comunicações do *host* que está disparando ataques contra um alvo. O motivo dessa preocupação em não bloquear todos os tráfegos de um dado *host* é que pode haver uma pessoa cujo computador está infectado por um *botnet* (o usuário do computador pode nem saber disso) e atacando algum *site* diferente daquele que pessoa está visitando.

A aplicação consegue diferenciar pacotes ICMP, TCP e UDP na versão 4 do protocolo IP (IPv4), mas a filtragem só funciona nos os protocolos UDP e TCP. Mesmo assim, a aplicação consegue analisar para qual porta da camada de transporte (e.g UDP ou TCP) um pacote que chegou ao dispositivo de rede se destina, desse modo tornando o filtro mais forte e mais personalizável do que simplesmente informar um endereço MAC de um *host* mal intencionado.

O filtro é montado pelo usuário da aplicação de mitigação através da edição de um arquivo.txt, que por sua vez é lido pela aplicação. Nesse aquivo podem ser listados os *hosts* mal intencionados e quais as portas esses *hosts* estão proibidos de enviar pacotes.

RESULTADOS E DISCUSSÕES

Pode-se concluir que essa aplicação atende os requisitos de *filter-based*, pois ela utiliza filtros para remediar ataques DDoS e esses filtros atuam na camada de transporte e são instalados na fonte de onde se origina o ataque.

Também é possível concluir que essa aplicação funciona se o *host* mal intencionado estiver na mesma rede da vítima, não em uma rede externa. Há alguns ataques DDoS que são originados de dentro de organizações, podendo atacar hosts em redes externas e internas, por tanto a mitigação de um elemento mal intencionado que está em uma rede interna (na mesma rede em que a vítima se encontra) é algo a ser considerado importante.

Pode-se concluir que quando o tráfego usado por *hosts* mal intencionados utilizam pacotes TCP, nem sempre a aplicação consegue bloquear 100% esse tráfego. Em alguns casos, o taxa de transmissão de um elemento mal intencionado é extremamente reduzida, por exemplo, um *host* legítimo normalmente envia um pacote TCP a 35GBp/s, já um *host* mal intencionado, quando não é totalmente bloqueado, consegue apenas a vazão de 15Kbp/s. Dessa forma, mesmo com o bloqueio em alguns casos não funcionando 100%, é possível perceber que os danos podem ser muito reduzidos ou até mesmo evitados, contribuindo assim para a mitigação de um ataque DDoS a um *end-host.*

É possível concluir que quando o tráfego malicioso contém pacotes UDP, esses pacotes conseguem trafegar normalmente na rede, mas a diferença é o servidor os rejeita. Com isso é possível afirmar as seguintes situações: (1) O ataque DDoS é mitigado, pois a aplicação tem como objetivo proteger o *end-host*, ou seja, o próprio servidor (e.g servidor *web*), proteger a vítima de um ataque direto. O objetivo dessa aplicação não é mitigar um ataque capaz de inundar um link compartilhado pela vítima, pois para esses casos, mecanismos que são baseados em capacidade (*capability-based*) são mais recomendados. (2) O mecanismo é vulnerável a

ataques DDoS que não visam atacar a vítima diretamente, mas que têm como objetivo inundar um link compartilhado pela vítima do ataque.

REFERÊNCIAS

[MCKEOWN et al. 2008] MCKEOWN, Nick. "OpenFlow: enabling innovation in campus networks." Newsletter ACM SIGCOMM Computer Communication Review, 2008, pg. 69-74, Volume 38 Issue 2.

[FEAMSTER et al. 2004] FEAMSTER, Nick. "The Case for Separating Routing From Routers". Proceeding FDNA '04 Proceedings of the ACM SIGCOMM workshop on Future directions in network architecture, 2008, pg 5-12.

[FEAMSTER et al. 2013] FEAMSTER, Nick. "The Road To SDN". Magazine Queue - Large-Scale Implementations Volume 11 Issue 12, 2013, pg 20.

[BERDE et al. 2014] BERDE, Pankaj. "ONOS: Towards an Open, Distributed SDN OS". Proceeding HotSDN '14. Proceedings of the third workshop on Hot topics in software defined networking, 2014, Pg 1-6.

[WANG et al. 2014] WANG, Bing. "DDoS Attack Protection in the Era of Cloud Computing and Software-Defined Networking". Network Protocols (ICNP), IEEE 22nd International Conference, 2014, pg 624 - 629.

[ZARGAR et al. 2013] ZARGAR, Saman. "A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks". Communications Surveys & Tutorials, IEEE (Volume:15 , Issue: 4), 2013, pg: 2046 - 2069.

[KREUTZ et al. 2014] KREUTZ, Diego. "Software-Defined Networking: A Comprehensive Survey". Proceedings of the IEEE (Volume:103 , Issue: 1), 2014, pg 14 - 76.

[LIU, et al. 2008] LIU, Xin. "To Filter or to Authorize: Network-Layer DoS Defense Against Multimillion-node Botnets". Proceeding SIGCOMM '08 Proceedings of the ACM SIGCOMM 2008 conference on Data communication, 2008, pg 195-206.

[KUROSE et al. 2013] KUROSE, James. Redes de Computadores e a Internet: Uma Abordagem Top-down. ed. 6o. Brasil, Pearson Education.