Plataformas de *firewall* - *open source* como alternativa a plataformas comerciais

Igor Born Machado[1], **Carlos Vinícius Rasch Alves**[1]

[1]Curso de Tecnologia em Redes de Computadores
Faculdade de Tecnologia SENAC Pelotas (FATEC)
Rua Gonçalves Chaves 602 – 96015560 – Pelotas – RS – Brazil

igorborn@gmail.com ,cvalves@senacrs.edu.br

Abstract. *This article is an analysis of firewall plataforms. Comparing open source tools with a pre-installed comercial plataform, will be sought an alternative that can better equate the commercial one. Keywords: Firewall, Comercial, Open Source, NGFW, IPS, Application Filter*

Resumo. *Este artigo é uma análise de plataformas de firewall. Comparando ferramentas open source com uma plataforma comercial já instalada, será buscada uma alternativa que consiga melhor se equiparar a ferramenta comercial. Palavras-Chave: Firewall, Comercial, Open Source, NGFW, IPS, Filtro de Aplicação*

1. Introdução

Segurança operacional é uma das propriedades para uma comunicação segura [Kurose and Ross 2006]. Com a maioria das organizações tendo suas redes internas conectadas a internet, pessoas má intencionadas podem tentar invadir essas redes em busca de segredos corporativos, ou até mesmo prejudicar o funcionamento delas, prejudicando assim a organização como um todo, tanto na execução de suas funções quanto na sua reputação. *Firewalls*, sistemas de detecção (*IDSs - Intrusion Detection Systems*) e prevenção (*IPSs - Intrusion Prevention Systems*) de intrusão são algumas das ferramentas utilizadas na proteção de uma rede corporativa. Eles são posicionados em pontos estratégicos da rede, e são eles que irão analisar todos os pacotes, decidindo se esse será transmitido para seu destino ou não.

VPNs (*Virtual Private Networks*) são redes com a maioria das propriedades de redes privadas, mas que se sobrepõem a redes públicas, utilizando a estrutura dela, mas ainda assim garantindo uma comunicação segura, graças a troca de chaves criptográficas entre os *hosts* envolvidos [Tanenbaum 2003].

Dentro destes conceitos, esse artigo estuda soluções de segurança em uma instituição de ensino descentralizada, formada por diversos campus em diferentes distâncias geográficas. Nessa estrutura, uma plataforma comercial com recursos avançados de hardware e software já está instalada na sede da instituição, onde se encontram centralizados diversos serviços essenciais que são acessados por todos os campus, mas devido ao custo elevado e a ausência de serviços essenciais, o mesmo não foi adquirido para todos os campus, gerando assim uma possível dificuldade na replicação das mesmas políticas no restante da instituição devido aos recursos avançados existentes na solução comercial. Serão pesquisadas alternativas em código aberto, buscando saber se

alguma apresenta recursos semelhantes, facilitando assim uma padronização das políticas na instituição.

2. Fundamentação Teórica

Nesta seção serão abordados alguns conceitos importantes para um melhor entendimento de segurança de uma redes, além de alguns termos utilizados pelo mercado de segurança da informação.

2.1. *Firewall*

Firewall é uma combinação de hardware e software responsável por filtrar o tráfego da rede [Kurose and Ross 2006]. Todo o tráfego deve passar pelo *firewall* independente do sentido, se entrando ou saindo da rede interna. Embora empresas maiores possam ter uma estrutura mais complexas, com diversos *firewalls* posicionados em diferentes subredes, o *firewall* de borda será a peça principal para o gerenciamento da *LAN (Local Area Network)*. Somente tráfego autorizado deve passar, sendo este definido por políticas de segurança locais onde todo o restante do tráfego será bloqueado.

Duas das categorias de *firewalls* possíveis são filtros de pacotes tradicionais e filtros de estado [Tanenbaum 2003]. Filtros de pacotes tradicionais analisam cada pacote individualmente, determinando se deve passar ou não usando regras especificas que tem como base endereço de origem ou destino, porta de origem ou destino, entre outros. Já um filtro de estado não analisa pacotes individualmente, mas rastreia conexões e usam essa informação para tomar decisões sobre filtragem. Rastreando todo os estado da conexão podem ser evitados ataques que explorariam vulnerabilidades do filtro de pacotes.

2.2. *IDS - Intrusion Detection System*

Sistemas de Detecção de Intrusão (*IDS*) tem a função de detectar ameaças a *LAN*. Para isso se posicionam fora de banda na rede, pois como se utilizam de uma análise profunda de pacotes e podem ser uma gargalo se não robustos o suficientes. Dessa maneira para não prejudicar o desempenho da rede, analisam não o tráfego em tempo real, mas sim uma cópia dele [Simkin 2017a].

2.3. *IPS- Intrusion Prevention System*

Sistemas de Prevenção de Intrusão (*IPS*) examinam fluxos de rede detectando e prevenindo que vulnerabilidades de aplicativos da *LAN* sejam explorados por atacantes [Simkin 2017b]. Para essa proteção ativa, eles são posicionados dentro da estrutura da rede analisando o tráfego em tempo real. Um *IPS* tem as seguintes características de enviar um alarme ao administrador da rede (como poderia ser em um *IDS*), derrubar pacotes maliciosos, bloquear o tráfego a partir do endereço de origem e redefinir a conexão.

2.4. IPSEC

IPSec (*Internet Protocol Security*) é um conjunto de protocolos que funciona em cima da camada de rede criando uma segurança na comunicação que ocorre nela. É utilizado comumente em *VPNs* (*Virtual Private Networks*) permitindo uma comunicação segura entre redes ou *hosts*, autenticando e encriptando cada pacote de uma sessão. Utiliza geralmente o protocolo *IKE* (*Internet Key Exchange*) para a negociação e gerência de chaves de maneira dinâmica [Frankel and Krishnan 2011].

2.5. Next Generation Firewall

De acordo com suposições de planejamento estratégico publicadas pela empresa de consultoria em tecnologia Gartner, hoje em dia menos de 50% dos links corporativos são protegidos utilizando *NGFWs (Next Generation Firewalls)*. Mas estima-se que até o final do ano de 2019 esse número aumente para pelo menos 90% [Hils et al. 2016].

NGFWs são *firewalls* que realizam uma análise profunda de pacotes, não limitando bloqueios somente a portas e protocolos, mas realizando uma filtragem em nível de camada de aplicação, onde analisando cada pacote e sessão baseado nas características de cada aplicação associando à análise de todas as camadas anteriores do pacote para a filtragem [Almeida 2013]. Essa tecnologia também traz um inteligência externa, pois atualiza sua base de conhecimento de aplicações e outros serviços através de servidores de terceiros dinamicamente. Suas características fundamentais são possuir funcionalidades de um *firewall* tradicional, possuir um *IPS* integrado, realizar controle de aplicação e identificar o usuário de cada sessão.

Um outro conceito em segurança muitas vezes se confunde com *NGFWs*. *UTM* (*Unified Threat Management*) traz uma gestão unificada de segurança que pode muito bem ser confundida pois traz muitas características do *NGFW*, mas tem não tem o foco em controle de aplicação como o *NGFW*. Mas cabe lembrar que segundo [Almeida 2013] são termos muito mais voltados ao marketing e mercado do que quanto as características da solução.

3. Ferramentas

Aqui serão abordadas as soluções de segurança estudadas na pesquisa.

3.1. PA-3020

Produto da Palo Alto Networks, uma das empresas líderes do mercado de *firewalls* corporativos [Hils et al. 2016, p. 3]. A empresa é voltada inteiramente para área segurança de redes, possui mais de 39000 clientes em 150 países [Alto 2017a].

Possui diversos níveis de soluções de segurança, desde equipamentos voltados a pequenas empresas ou escritórios remotos, até chassis modulares de alto desempenho para grandes *data centers*. Utiliza uma arquitetura *single-pass*, classificando o tráfego de uma forma mais completa e analisando todo o seu contexto em diferentes camadas para então além de aplicar as regras necessárias poder também prevenir ameaças [Alto 2017b]. A Figura 1 mostra o funcionamento do *single-pass* e a arquitetura de hardware do PA-3020, vital para permitir essa análise profunda em tempo real sem gerar gargalos na rede.

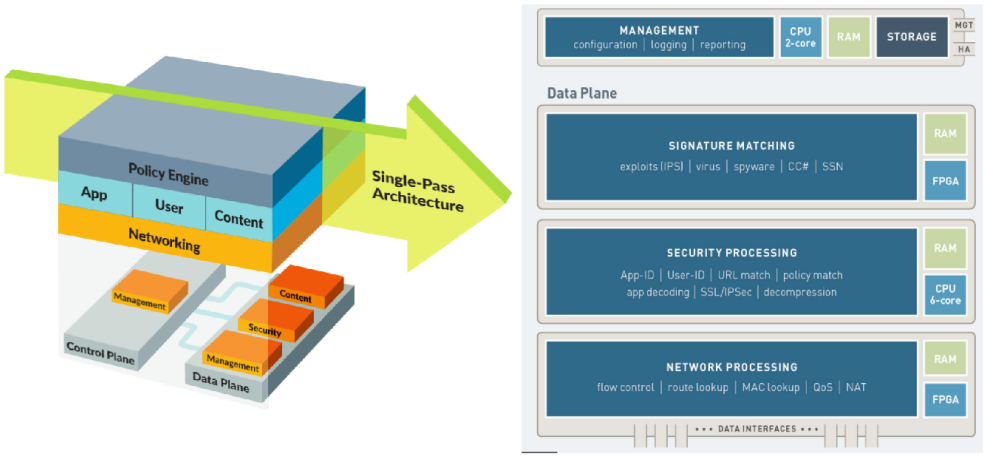

Figura 1. A esq. Arquitetura *single-pass*. A dir. Arquitetura da série PA-3000 da Palo Alto Networks. Fonte: [Alto 2017b]

3.2. OPNsense

OPNsense é um projeto *open source* que teve início como um *fork* do pfSense e mOnOwall em 2014. Sua primeira versão oficial foi disponibilizada em janeiro de 2015, tendo como base o FreeBSD e seguindo assim desde então . O projeto anuncia sua missão como ”fazer do OPNSense a plataforma de segurança mais amplamente utilizada, dando a usuários, desenvolvedores e negócios um ambiente amigável, estável e transparente.”O nome do projeto é uma união das palavras ”*open*”e ”*sense*”querendo significar ”*open (source) makes sense*”, ou, ”*open (source)* faz sentido”[OPNsense 2017].

3.3. Untangle NG Firewall

Solução criada pela Untangle, empresa focada em segurança de redes. A Untangle afirma que suas soluções possuem capacidades de níveis corporativos com a simplicidade de uso de um consumidor final para organizações com recursos de TI limitados. O foco das soluções são para pequenas e médias empresas, escolas e organizações governamentais [Untangle 2017b].

3.4. Netdeep Secure Firewall

Solução de segurança open source, o Netdeep Secure é desenvolvido pela Netdeep Tecnologias. Sendo a versão livre, a *start* [Netdeep 2017].

4. Cenário

Este estudo considerou uma instituição de ensino com campus espalhados em diversas cidades. A mesma possui em em sua sede uma estrutura de *datacenter* onde são hospedados diversos serviços que são acessados por todos os campus. Na borda dessa rede está um *NGFW* da Palo Alto Networks, o PA-3020, responsável por analisar e filtrar todo o tráfego de entrada e saída da rede. Como cada campus possui autonomia para definir sua política de acesso a rede, estas não são padronizadas com o restante da instituição. Cada um possui também autonomia no seu orçamento para investimentos, sendo um grande obstáculo para a padronização, as limitações nos recursos de TI de cada um e as diferentes soluções

de segurança de rede adotadas onde alguns campus já possuem *VPNs* implementadas enquanto outros não. Como o PA-3020 é uma solução comercial a qual ainda possui uma das relações de custo por gigabit protegido mais alta do mercado [Hils et al. 2016, p. 17], a sua instalação nos campus menores se tornou inviável. A Figura 2 representa a estrutura da instituição.

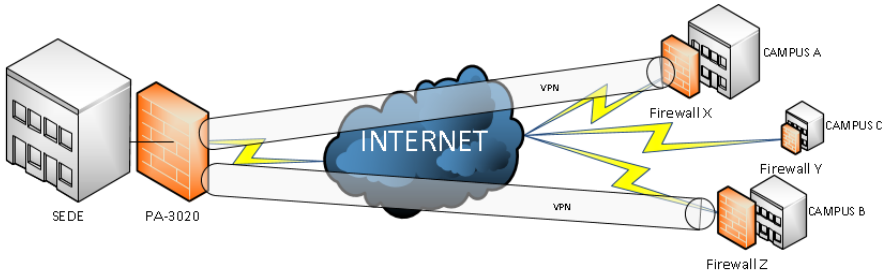

Figura 2. Cenário da Instituição. Alguns campus já possuem VPNs implementadas

5. Testes

Tendo como base a estrutura da sede, foram elencadas as principais funcionalidades do PA-3020 que seriam indispensáveis na implementação de ferramentas *open source* nos campus.

5.1. Filtro de Aplicação

Para [Pandini 2016], poder controlar o tráfego a nível de aplicação permite bloquear centenas de aplicações de uma forma fácil e rápida. Levando em conta o consumo de internet fixa na América do Sul conforme Figura 3 foram escolhidas as aplicações que representam uma parcela maior desse consumo de banda. Considerando o tráfego de aplicações *HTTP* e *HTTPS* como válido e não podendo este ser restringido, as 4 aplicações que então representaram quase 50% do tráfego de internet fixa em 2016 foram *Youtube, Bittorrent, Netflix e Facebook*. Conseguir filtrar o acesso a essas aplicações pode significar um grande aproveitamento de um recurso as vezes muito limitado em campus instalados em locais remotos que é o link de acesso a internet.

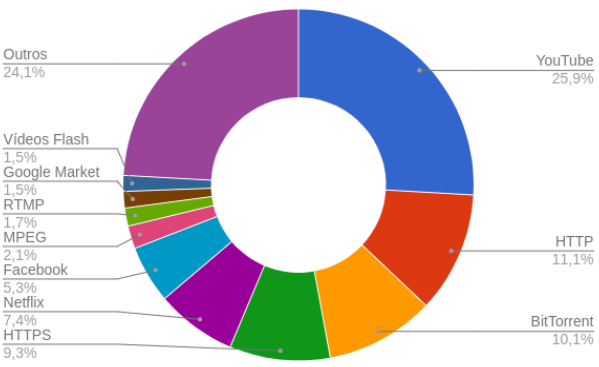

Figura 3. Estatísticas de consumo da internet fixa por aplicação na América Latina em 2016. Fonte:[Sandvine 2016]

5.2. VPN IPsec

Poder trafegar dados críticos através de uma rede segura é muito importante para uma organização, mas a aplicação de regras também deve ser considerada. A sede possui algumas *VPNs* implementadas com outros campus para a comunicação de algumas sub-redes específicas as quais sofrem pesadas restrições quanto ao tráfego permitido. Hoje em dia essa comunicação é toda feita através de IPsec, onde somente alguns campus possuem essa comunicação. Será analisado o suporte a IPsec da solução e seus recursos.

5.3. Prevenção de Intrusão

Os métodos de detecção de intrusos em um *IPS* são a detecção baseada em assinaturas e a detecção baseada em anomalias estatísticas [Santos 2010]. Quando por assinaturas o sistema busca em um dicionário se a assinatura do tráfego analisado está marcada como perigosa, representando uma ameaça. Quando por anomalias estatísticas, o tráfego analisado de tempos em tempos cria um patamar para desempenho da rede, caso este seja alterado o *IPS* realiza uma ação para que este retorne ao normal. Serão testados os métodos presentes nas soluções e sua eficácia expondo clientes a *malwares*.

5.4. Controle de Banda

Alguns campus apresentam sub-redes que necessitam de restrições de consumo de banda devido a limitação da largura de banda do *link* de Internet. Será analisada a existência dessa funcionalidade e como esta é implantada.

5.5. Cenário de Testes

Enquanto o PA-3020 se encontra em uma ambiente de produção, já posicionado na borda da rede da instituição, as soluções *open source* foram instaladas em máquinas virtuais e testadas em um ambiente controlado conforme mostra a Figura 4. Como hoje em dia 13% do tráfego de rede é proveniente de *smartphones*, número que deve crescer para 33% em 2021 [Cisco 2017], foi instalado um ponto de acesso sem fio para testar a eficácia dos filtros e recursos também nesse tipo de aparelho, onde a aplicação pode possuir nele um aplicativo especifico, não se limitando ao acesso via *browser* .

As máquinas virtuais para hospedagem das soluções *open source* foram configurada com o mesmo hardware dentro do virtualizador, conforme tabela 1.

Tabela 1. Especificações da máquina virtual com a solução *open source*

	CPU	Memória	WAN	LAN
Máquina Virtual	1 core 1.6 GHz	2GB	Bridge - Wireless	Bridge - Cabeada

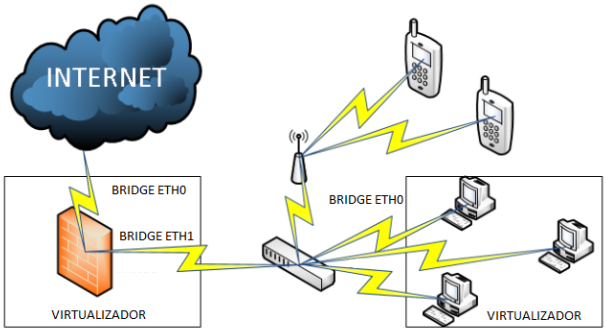

Figura 4. Cenário de testes em máquinas virtualizadas

6. Resultados

Nessa seção serão expostos os resultados adquiridos nessa pesquisa de acordo com os testes definidos na seção anterior.

6.1. Filtro de aplicação

Nessa subseção será mostrado o funcionamento desse recurso em cada ferramenta e sua efetividade em bloquear o tráfego. O OPNsense não possui qualquer tipo de implementação de filtro de aplicação, sendo assim não apresenta resultados.

6.1.1. PA-3020

No Palo Alto a implementação de filtros em camada de aplicação se apresentou de forma simples e funcional em todos os protocolos. Conseguindo restringir o acesso totalmente a todas as aplicações definidas.

6.1.2. Netdeep Secure Firewall

Embora tenha sido eficiente no bloqueio da aplicação *Netflix*, não foi 100% eficaz no bloqueio do *Facebook, Youtube* e *Bittorrent*. Foi capaz de identificar e descartar vários pacotes em todos os casos, mas muitos seguiram passando pelo filtro, não impedindo o uso da aplicação. No caso do *Facebook* houveram bloqueios a algumas aplicações como o *messenger*, que não ficou funcional nos *smartphones*. No caso do *Bittorrent*, onde quase todos os pacotes eram descartados, mas pacotes em portas conhecidas como a 80, estavam sendo permitidos pelo *firewall*.

6.1.3. Untangle NG Firewall

O filtro de aplicação apresenta 2 versões. Na *trial*, disponível por 14 dias antes de ser bloqueada, é possível realizar a filtragem de forma mais simples, selecionando a aplicação e a ação a ser tomada. Sendo disponível bloquear o tráfego ou então colocá-lo num *tarpit* (poço de piche) [Untangle 2017a]. O *tarpit* funciona manejando o tráfego de uma forma mais silenciosa. No caso do TCP, a conexão não é resetada como no caso de um

bloqueio tradicional, mas todos os pacotes de dados dessa conexão serão descartados. No caso de uma sessão UDP esta também será mantida aberta, assim o próximo pacote será descartado ao invés de categorizado em uma nova sessão. Na versão trial foi possível bloquear as 4 aplicações definidas.

Na versão *Lite* do controle de aplicação, de uso livre e sem limite de tempo. Ao invés da escolha de uma lista de aplicações conhecidas, o bloqueio será feito por assinaturas baseadas em expressões regulares. Será feita a análise do tráfego e caso a assinatura seja encontrada o tráfego será bloqueado. Na versão *Lite* não foi possível o bloqueio das aplicações *Youtube* e *Facebook* de modo satisfatório, sendo possível o bloqueio somente de *Bittorrent* e *Netflix*. Foi possível o bloqueio de todas as aplicações através de uma expressão regular para bloqueio de vídeos, mas como esta descartaria qualquer aplicação de vídeo podendo gerar muitos falsos positivos, foi inviável a aplicação dessa regra.

6.1.4. Comparação

Após as análises, a capacidade de filtro de aplicação em cada solução se apresentou conforme a tabela 2, onde a aplicação seguiu funcional, ou teve seu uso bloqueado. Entre as soluções *open source* o consumo de hardware em cada ferramenta com 5 clientes conectados em 645 sessões ativas se mostrou como na Figura 5.

Tabela 2. Resumo dos filtros

Solução		Bittorrent	Youtube	Facebook	Netflix
Palo Alto		**Bloqueado**	**Bloqueado**	**Bloqueado**	**Bloqueado**
NetDeep		Funcional	Funcional	Funcional	**Bloqueado**
Untangle	Trial	**Bloqueado**	**Bloqueado**	**Bloqueado**	**Bloqueado**
	Lite	**Bloqueado**	Funcional	Funcional	**Bloqueado**
OPNSense		Não se aplica	Não se aplica	Não se aplica	Não se aplica

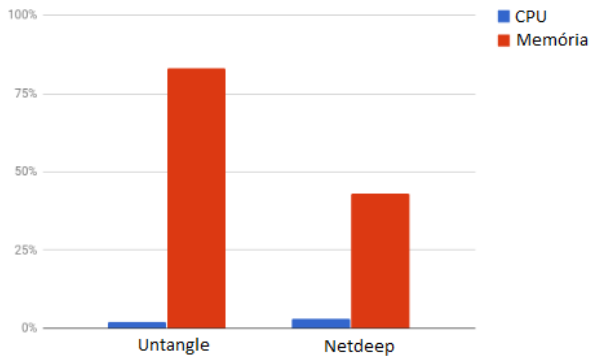

Figura 5. Consumo de Hardware. 645 sessões ativas entre 5 clientes conectados

6.2. Controle de Banda

Nessa subseção será mostrado o funcionamento desse recurso em cada ferramenta.

6.2.1. PA-3020

No Palo Alto é possível a marcação de tráfego em classes de 1 a 8. A marcação da classe no tráfego pode ser definida pela camada de aplicação, rede ou transporte desse pacote, onde então são definidas larguras de banda máxima e garantida para a conexão, prioridade além de número máximo de sessões.

6.2.2. NetDeep Secure Firewall

Possui uma controlador de tráfego simples mas funcional, permitindo somente definir uma largura de banda para *download* e uma para *upload*. Pode também ser definida uma prioridade Alta/Média/Baixa para uma porta TCP/UDP.

6.2.3. OPNsense

Utiliza o filtro de pacotes alterando o campo ToS (Type of Service) do cabeçalho caso a regra se aplique. Também possui um filtro de trafégo onde são criados "*pipes*"com larguras de banda definidas e "*queues*"que utilizarão esse "*pipe*". Cada *pipe* pode conter várias filas e um peso pode ser atribuído para cada fila, definido sua importância dentro desse *pipe*. Os critérios para o uso do *pipe* ou da fila são definidos por IP ou porta, de origem ou destino. Este recurso se mostrou funcional.

6.2.4. Untangle NG Firewall

O Untangle possui o um controlador de largura de banda somente no modo *trial* onde é possui criar regras de análise de tráfego em todas as camadas, como no PA-3020. No tipo de ação é possível selecionar uma quota para um período diário, semanal, ou mensal. Também definir uma prioridade para ele ou então penalizar o cliente que possua esse tipo de tráfego, bloqueando ele por um determinado período de tempo. Não há um módulo grátis para essa função.

6.3. Prevenção de Intrusão

Para os testes dos sistemas de prevenção de intrusão foram utilizados 12 arquivos de *malwares* disponibilizados no site "wicar.org"[Wicar 2017]. O site disponibiliza arquivos não perigosos, mas com características de tráfego que testarão a eficiência das soluções em acionar os seus *IPSs* para agirem. O Netdeep não possui nenhuma ferramenta de IPS implementada sendo assim não consta resultado.

6.3.1. PA-3020

Possui um sistema de *subscription* na sua licença, a qual durante o período contratado dará direito a seus dicionários de assinaturas de tráfego malicioso. Estas assinaturas são classificadas nos dicionários com um nível de severidade e então pode ser selecionada uma ação para cada nível de severidade, como por exemplo, resetar uma conexão em

ameaças criticas, ou simplesmente gerar um alerta em ameaças não tão severas. O PA-3020 foi eficaz ao bloquear todas as ameaças.

6.3.2. OPNsense

Vem com uma instalação do Suricata como o módulo de *IDS* e permitindo ser utilizado como *IPS*. Baixa suas regras diretamente de dicionários externo como ”abuse.ch”e ”emergingthreats.net”. Foi capaz de detectar e bloquear 6 das 12 ameaças.

6.3.3. Untangle NG Firewall

O Untangle NG Firewall possui o *IPS* como um módulo grátis, onde possui uma base extensa de regras separadas por classes e categorias, podendo cada regra ser editada conforme necessidade. Apesar desse vasto dicionário, onde inclusive várias CVEs [Mitre 2017] que eram anunciadas nos *malwares* da ”Wicar.org”e mesmo as sessões infectadas sendo escaneadas efetivamente pelo Untangle, nenhuma das ameaças foi detectada pelo *IPS*.

6.3.4. Comparação

Na Figura 6 pode se ver uma comparação entre as ferramentas executando o IPS. A esquerda o consumo de de hardware das soluções *open source* executando o escaneamento em 5 clientes, e a direita a efetividade de cada ferramenta em detectar as ameaças.

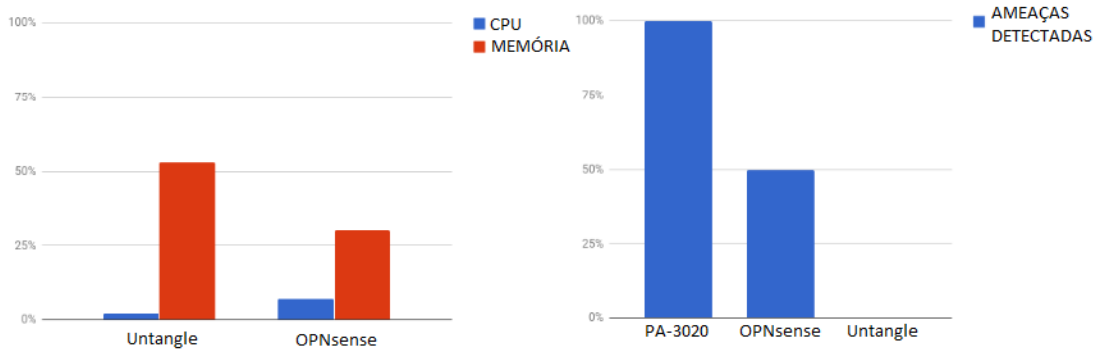

Figura 6. A esq. consumo de *hardware*. A dir. porcentagem de ameaças bloqueadas em cada ferramenta

6.4. VPN IPsec

Tendo em vista que o PA-3020 já possui diversos túneis implementados com outros campus por onde sub-redes específicas trafegam respeitando as politicas de segurança definidas. O mesmo só foi possível ser aplicado também no OPNsense, caso em que a VPN se mostrou funcional, enquanto no Netdeep apesar de configurável a VPN IPsec, esta não ficou ativa em nenhum momento. O Untangle possui suporte somente no modo *trial*, onde está se mostrou funcional, mas não havendo um módulo grátis para essa funcionalidade.

7. Considerações Finais

Filtrar acesso a aplicações e controlar o consumo de banda são funções onde além da primeira ter importância no garantir a segurança a rede, está importância será ainda maior quanto ao otimizar o uso do link de internet, um recurso muito limitado nestes locais. O filtro de aplicação será ainda mais vital em uma internet onde 73% do tráfego IP já é composto por vídeo disponibilizado nas mais diversas formas [Cisco 2017].

Uma *VPN* será indispensável para o acesso a serviços chave na comunicação entre a sede e os campus, não podendo estes trafegarem livres pela internet, além do sistema de prevenção de intrusão que garantirá que mesmo clientes não protegidos por anti-vírus fiquem protegidos dentro da dele.

A partir disto, como nas soluções de segurança estudadas nenhuma ainda se apresentou como um substituto direto ao PA-3020, e como dentro dos recursos de segurança que cada uma apresentou, nenhum se mostrou tão eficiente ao executar sua função quanto o PA-3020. Dessa maneira a alternativa ideal para o atendimento desses campus remotos seria a união das ferramentas *open source* até mesmo pela impossibilidade de atingirem uma robustez como a da solução Palo Alto.

No cenário proposto o OPNsense na Figura 7 estaria posicionado na borda da *LAN* executando as funções da *VPN*, controle de banda e *IPS*, enquanto um Untangle estaria posicionado na borda da sub-rede acadêmica, e dedicado ao filtro de aplicação especificamente desta, sendo está uma rede com necessidade de maiores restrições, podendo até mesmo em casos extremo ser bloqueado qualquer acesso a vídeo, visto o quanto esse é oneroso a rede.

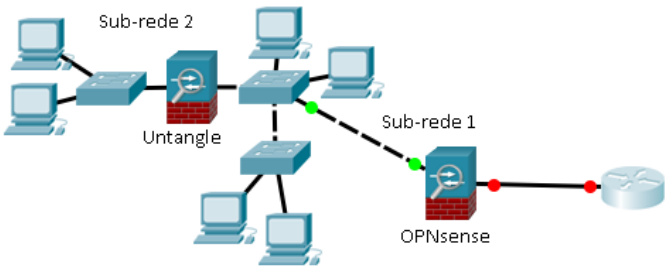

Figura 7. Cenário sugerido

7.1. Dificuldades Encontradas

Mesmo se tratando de plataformas que usam código aberto como base, tanto do caso do OPNsense (FreeBSD), quanto Untangle e Netdeep (Linux) houve uma certa dificuldade nas configurações quando estas não estavam dispostas na interface web de cada um, como no caso da criação de rotas para a configuração das *VPNs* tanto no Untangle quanto no Netdeep. A definição de assinaturas no filtro de aplicações livre do Untangle também se mostrou um desafio, sendo um processo de ajuste fino bastante demorado e que se baseando na forma de funcionamento de aplicações web as quais podem alterar com o tempo, não se apresenta tão prático quanto as demais que usam uma inteligência externa, mas ainda assim garantem uma maior liberdade do que no caso do Netdeep por exemplo em que o filtro de aplicação ao não ser funcional não há nada que possa ser feito.

7.2. Trabalhos Futuros

A presente pesquisa buscou um entendimento referente ao recursos presentes nas soluções de *firewall* disponíveis atualmente e em como dentre elas, as soluções *open source* poderiam se apresentar como uma alternativa na infraestrutura de redes de campus menores de uma instituição de ensino. A pesquisa poderia apresentar continuidade na implantação dessas ferramentas em um ambiente de produção, sendo inseridas na rede desses campus para então com o tráfego real poder se realizar uma análise de desempenho mais completa.

Referências

Almeida, G. (2013). Solução integrada de segurança: existe diferença entre UTM e NGFW? https://realprotect.net/blog/solucao-integrada-de-seguranca-existe-diferenca-entre-utm-e-ngfw/. [Acessado em: 2017-06-26].

Alto, P. (2017a). Company Fast Facts. https://www.paloaltonetworks.com/company/company-fast-facts. [Acessado em: 2017-06-26].

Alto, P. (2017b). Single-Pass Architecture. https://www.paloaltonetworks.com/technologies/single-pass-architecture. [Acessado em: 2017-06-26].

Cisco (2017). Cisco Visual Networking Index: Forecast and Methodology, 2016–2021. Technical report.

Frankel, S. and Krishnan, S. (2011). IP Security (IPsec) and Internet Key Exchange (IKE) Document Roadmap. RFC 6071.

Hils, A., D'Hoinne, J., Kaur, R., and Young, G. (2016). Magic Quadrant for Enterprise Network Firewalls. https://www.amerinet.com/sites/default/files/2016%20FW%20gartner%20report.pdf. [Acessado em: 2017-06-26].

Kurose, J. F. and Ross, K. W. (2006). *Redes de Computadores e a Internet: Uma abordagem top-down*. Pearson, São Paulo, trad. 5 ed. edition.

Mitre (2017). Common vulnerabilities and exposures-the standard for information security vulnerability names. https://cve.mitre.org/. Acessado em: 2017-06-26.

Netdeep (2017). Netdeep. http://www.netdeep.com.br/secure/firewall/. [Acessado em: 2017-06-26].

OPNsense (2017). OPNsense. https://opnsense.org/. [Acessado em: 2017-06-26].

Pandini, W. (2016). O que é controle de aplicação? https://blog.ostec.com.br/seguranca-perimetro/o-que-e-controle-de-aplicacao. [Acessado em: 2017-06-26].

Sandvine (2016). Global internet phenomena - latin america & north america. Technical report, Sandvine Incorporated ULC.

Santos, V. (2010). Sistemas de Detecção de Intrusões (IDS – Intrusion Detection Systems) usando unicamente softwares

Open Source. https://seginfo.com.br/2010/06/21/sistemas-de-deteccao-de-intrusoes-ids-intrusion-detection-systems-usa#formas-de-deteccao. [Acessado em: 2017-06-26].

Simkin, S. (2017a). WHAT IS AN INTRUSION DETECTION SYSTEM? - IDS Technology and Deployment. https://www.paloaltonetworks.com/cyberpedia/what-is-an-intrusion-detection-system-ids. [Acessado em: 2017-06-26].

Simkin, S. (2017b). WHAT IS AN INTRUSION PREVENTION SYSTEM? - Intrusion Prevention and Detection System Basics. https://www.paloaltonetworks.com.br/resources/learning-center/what-is-an-intrusion-prevention-system-ips.html. [Acessado em: 2017-06-26].

Tanenbaum, A. (2003). *Redes de computadores*. CAMPUS - RJ.

Untangle (2017a). Controle de aplicação. https://wiki.untangle.com/index.php/Application_Control. Acessado em: 2017-06-26.

Untangle (2017b). Untangle. https://www.untangle.com. [Acessado em: 2017-06-26].

Wicar (2017). Wicar.org. http://www.wicar.org/. Acessado em: 2017-06-26.