Contatos:
igorborn@gmail.com
/igorbmachado

Curso Superior de Tecnologia em Redes de Computadores

TCC

Seminário Final

Orientador: Carlos Vinícius Rasch Alves

Igor Born Machado

Sumário

Introdução

Em um mundo onde a informação é cada vez mais digital e valiosa, o desafio de garantir segurança é crescente. Firewalls são a base para proteger uma rede, decidindo o que entra e o que sai, sendo assim devem ser soluções confiáveis e completas.

NGFW

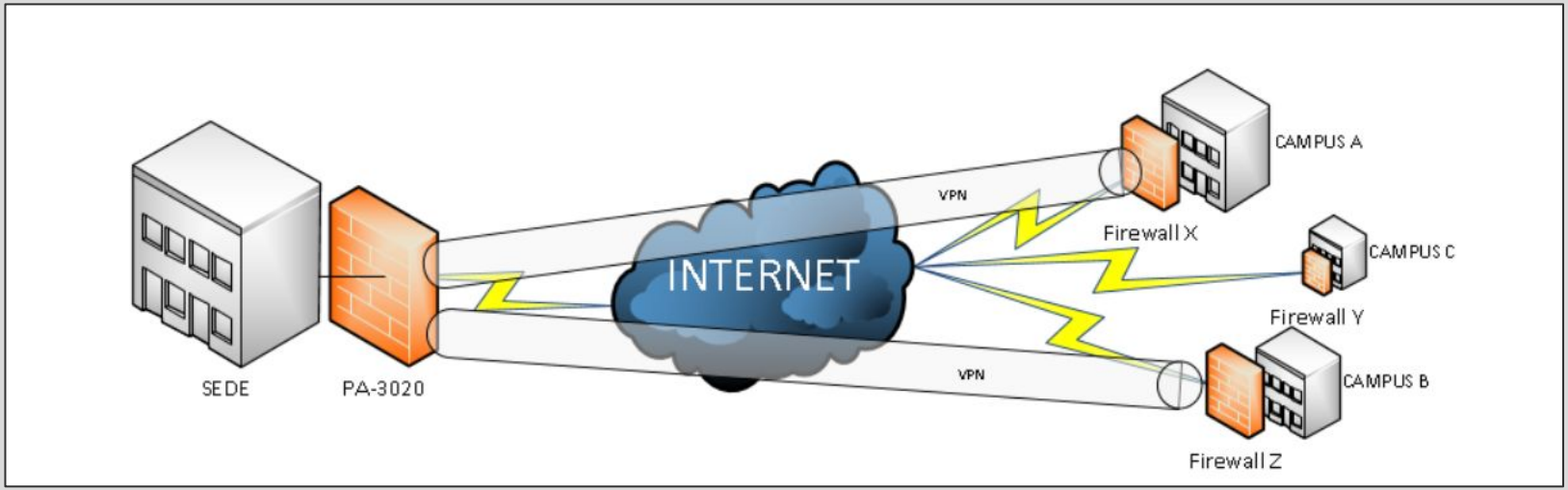
- Funcionalidades de um firewall tradicional;
- IPS integrado;
- Controle de aplicação;
- Identificar usuário de cada sessão.

Introdução

De acordo com a Gartner hoje em dia menos de 50% dos links corporativos são protegidos por NGFWs, mas as tendências indicam que esse número deva aumentar até pelo menos 90% em 2019 (Hils et al. 2016).

Objetivo Geral

Comparar solução de segurança comercial em produção com soluções Open Source.



Objetivo Geral

OPNsense®
Your next open source firewall

untangle™

netdeep® secure

Objetivos Específicos

- Pesquisar bibliografia;
- Estudar ferramenta comercial;
- Configurar soluções open source;
- Efetuar testes;
- Analisar resultados;
- Comparar soluções;
- Escrever o artigo.

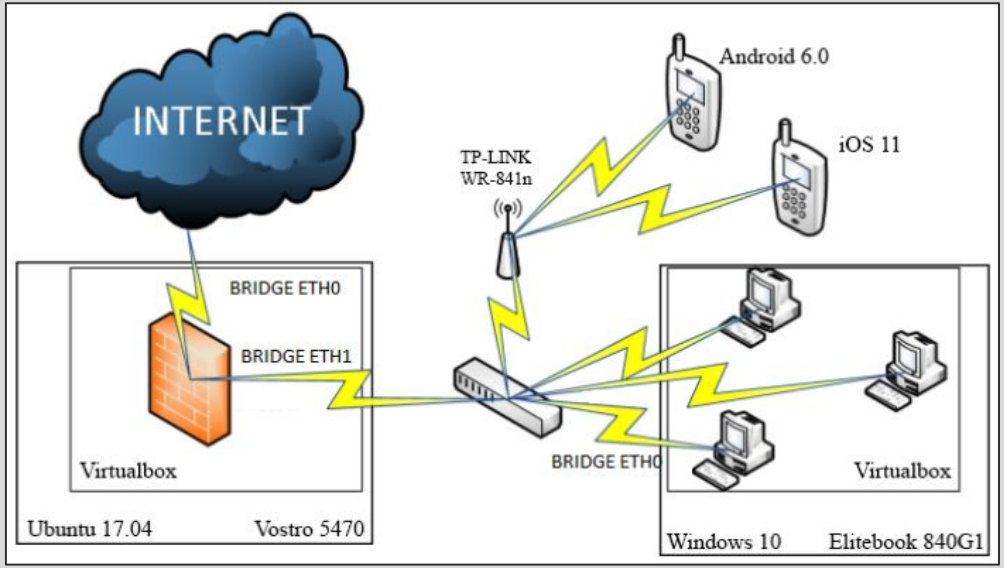
Funcionalidades

- Filtro de aplicação;
- IPS;
- VPN IPsec;
- Controle de Banda.

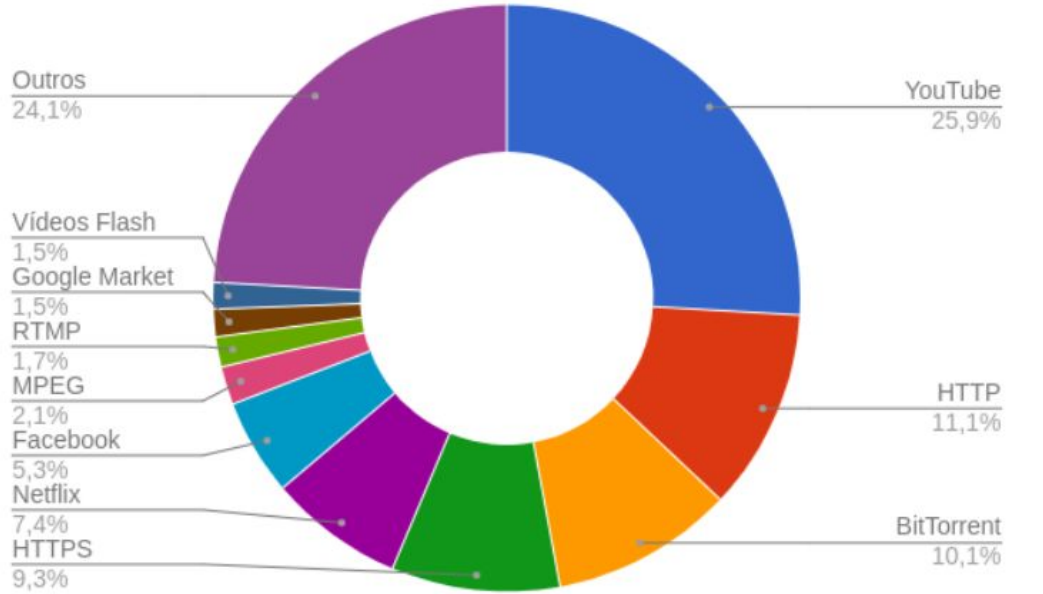
Testes

Especificações da máquina virtual com a solução *open source*

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



Resultados - Filtro de Aplicação

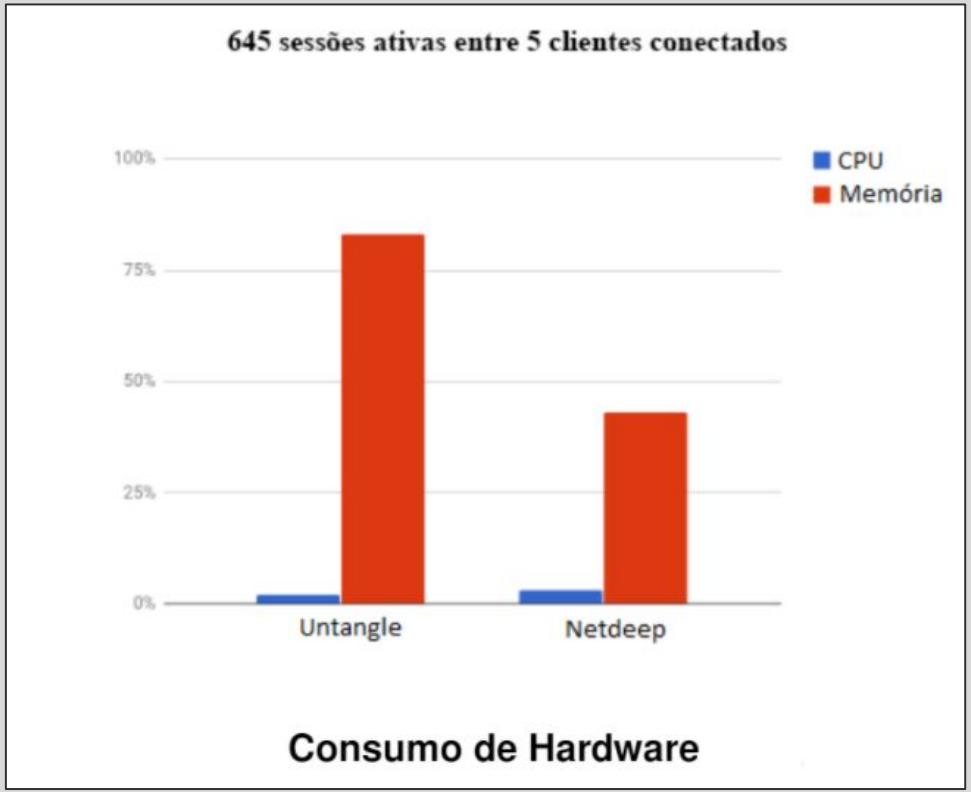


Estatísticas de consumo da Internet fixa por aplicação na América Latina em 2016. Fonte:[Sandvine 2016]

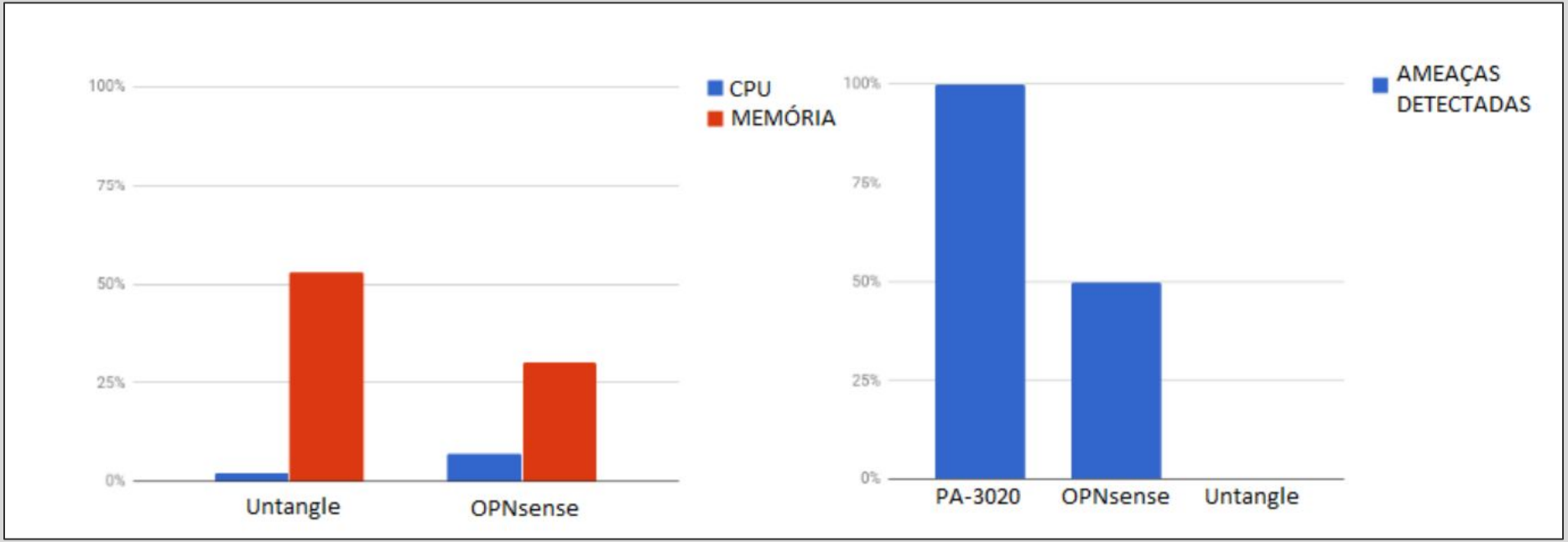
Resultados - Filtro de Aplicação

Solução	Bittorrent	Youtube	Facebook	Netflix
PA-3020	Bloqueado	Bloqueado	Bloqueado	Bloqueado
NetDeep	Funcional	Funcional	Funcional	Funcional
Untangle Trial	Bloqueado	Bloqueado	Bloqueado	Bloqueado
Untangle Lite	Bloqueado	Funcional	Funcional	Bloqueado
OPNsense	NA	NA	NA	NA

Resultados - Filtro de Aplicação



Resultados - IPS



Resultados - Controle de Banda

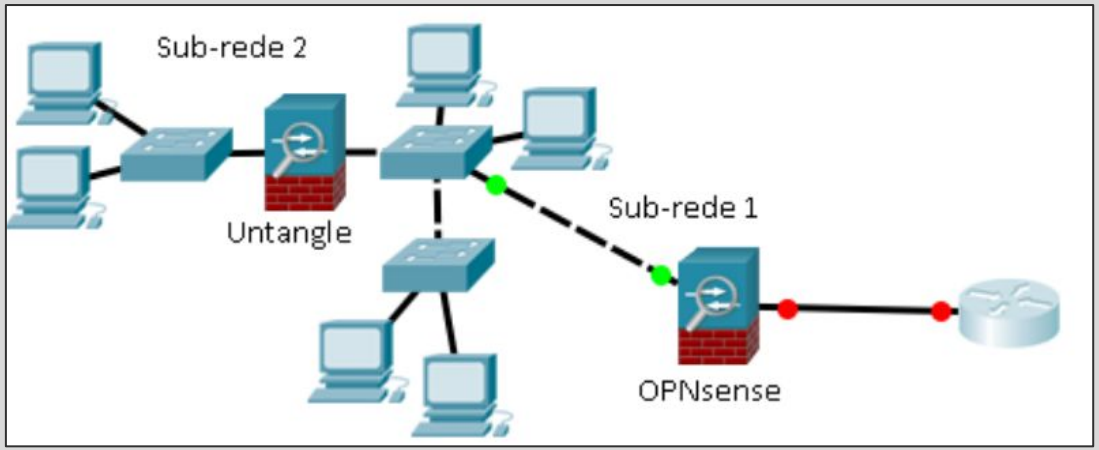
PA-3020	Possui com recursos avançados
OPNsense	Possui com recursos avançados
Untangle	Possui somente na versão paga
Netdeep	Possui com recursos limitados

Resultados - VPN IPsec

PA-3020	Possui várias VPNs já implementadas
OPNsense	Possui implementado com sucesso
Untangle	Possui somente na versão paga
Netdeep	Possui mas não funcional

Considerações Finais

Nenhuma solução open source se mostrou capaz de atender as todas as funcionalidades.
Sendo um cenário sugerido a união das ferramentas.



Dificuldades Encontradas

- Configurações fora da interface web em versões personalizadas;
- Ajuste filtro de aplicação.

Trabalhos Futuros

Implantação das soluções em um ambiente de produção para análise com tráfego real.

Cronograma

Atividade	Março	Abril	Maio	Junho
Pesquisar Bibliografia	X	X		
Estudar ferramenta comercial	X	X	X	
Configurar soluções open source			X	
Efetuar testes			X	
Analisar resultados			X	X
Comparar Soluções			X	X
Escrever o artigo		X	X	X

Wiki

Acesso Externo:

http://187.7.106.14/wiki2017_1/doku.php?id=projeto13:start

Acesso Interno:

http://192.168.200.3/wiki2017_1/doku.php?id=projeto13:start

Referências

- Almeida, G. (2013). Soluc¸ao integrada de seguranc¸a: existe diferenc¸a entre UTM éNGFW? https://goo.gl/RNU4cV. [Acessado em: 2017-07-03].
- 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://goo.gl/xPNpuR. [Acessado em: 2017-07-03].
- 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://goo.gl/fCBbuf. [Acessado em: 2017-07-03].
- Kurose, J. F. and Ross, K. W. (2006). Redes de Computadores e a Internet: Uma abordagem top-down. Pearson, Sao 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).

Referências

- 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://goo.gl/rdEGAZ. [Acessado em: 2017-07-03].
- 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 aplicacão. 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].
- Virtualbox (2017). Virtualbox. https://www.virtualbox.org/. [Acessado em: 2017-06-26].
- Wicar (2017). Wicar.org. http://www.wicar.org/. Acessado em: 2017-06-26.

Perguntas

Contatos:
igorborn@gmail.com
/igorbmachado

?