CENTRO PAULA SOUZA

Faculdade de Tecnologia de Americana

Curso Superior de Tecnologia em Segurança da Informação

KARINA ARAUJO DOS SANTOS

UM ESTUDO COMPARATIVO ENTRE OS FIREWALLS IPFW E PF

Americana/SP

2016

CENTRO PAULA SOUZA

Faculdade de Tecnologia de Americana

Curso Superior de Tecnologia em Segurança da Informação

KARINA ARAUJO DOS SANTOS

santoskarinaaraujo@gmail.com

UM ESTUDO COMPARATIVO ENTRE OS FIREWALLS IPFW E PF

Projeto desenvolvido como requisito parcial para obtenção do título de Tecnólogo em Segurança da Informação do Curso Superior de Tecnologia em Segurança da Informação da Fatec-Americana, sob a orientação do Prof° Me. Henri Alves de Godoy.

Área: Segurança da Informação

Americana/SP

2016

FICHA CATALOGRÁFICA – Biblioteca Fatec Americana - CEETEPS
Dados Internacionais de Catalogação-na-fonte

Santos, Karina Araújo dos
S235u Um estudo comparativo entre os firewalls IPFW e PF. / Karina Araújo dos Santos. – Americana: 2016.
52f.

Monografia (Graduação em Tecnologia em Segurança da Informação). - - Faculdade de Tecnologia de Americana – Centro Estadual de Educação Tecnológica Paula Souza.
Orientador: Prof. Me. Henri Alves de Godoy

1. Segurança em sistemas de informação I. Godoy, Henri Alves de II. Centro Estadual de Educação Tecnológica Paula Souza – Faculdade de Tecnologia de Americana.

CDU: 681.518.5

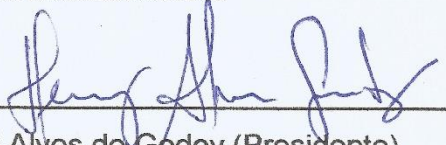
Karina Araujo dos Santos

UM ESTUDO COMPARATIVO ENTRE OS FIREWALLS IPFW E PF

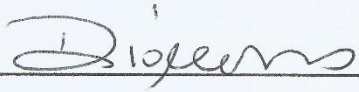
Projeto desenvolvido como requisito parcial para obtenção do título de Tecnólogo em Segurança da Informação do Curso Superior de Tecnologia em Segurança da Informação da Fatec-Americana, sob a orientação do Prof° Me. Henri Alves de Godoy.
Área: Segurança da Informação

Americana, 23 de junho de 2016.

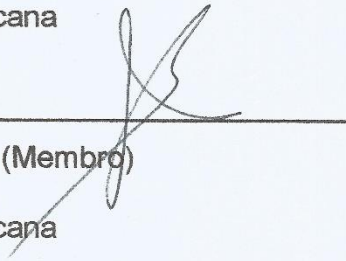
Banca examinadora:



Henri Alves de Godoy (Presidente)
Mestre
Fatec Americana



Diógenes de Oliveira (Membro)
Mestre
Fatec Americana



Adnan Bakri (Membro)
Especialista
Fatec Americana

AGRADECIMENTOS

Em primeiro lugar, agradeço a minha família, pelo apoio e incentivo tanto ao cursar Segurança da Informação quanto no desenvolvimento dessa monografia.

Aos meus amigos pela amizade, companheirismo e principalmente pelo suporte no aprendizado.

Ao meu amigo e antigo chefe Eder de Souza, por me ajudar na escolha deste tema e pela paciência, orientação e incentivo.

A professora, Juliana Borsato Beckedorff Pinto, pela ajuda com materiais, como livros e vídeos, que me ajudaram muito na conclusão desta monografia.

E por fim, meu orientador Henri Alves de Godoy, que também me ajudou muito com materiais que foram à base no desenvolvimento desta monografia e pelo apoio, paciência, orientação e amizade.

DEDICATÓRIA

A minha família, por estar sempre ao meu lado, pelo carinho e amor e principalmente ao meu namorado, Wilson Roberto de Oliveira Santos Filho, por ser a pessoa especial que é, e pelo incentivo que sempre me proporciona.

RESUMO

Esta monografia visa comparar dois *firewalls*, o IPFW e o PF implementados em um sistema operacional FreeBSD, que foram testados por meio da ferramenta IPERF que analisa o desempenho da rede. Por ser um assunto de Segurança da Informação um capítulo será atribuído para explicação da mesma. Uma rede foi implementada, para que o *firewall* estivesse entre uma rede interna e a externa, sendo realizadas suas configurações e construção de regras para controle da rede, visando minimizar as vulnerabilidades. Foram utilizados os métodos: Dedutivo e Comparativo.

As regras dos *firewalls* foram configuradas da maneira mais idêntica possível, com o objetivo de avaliar os resultados e diferenças de ambos via IPERF.

Os resultados obtidos durante os testes mostram que os *firewalls* possuem diferenças mínimas no resultado final, entretanto devido a maior facilidade na criação das regras com o *firewall* PF, o mesmo pode ser avaliado como o mais prático para a obtenção dos resultados almejados.

Palavras Chave: *Firewall*; Controle de tráfego; FreeBSD.

ABSTRACT

This document aims to compare two firewalls, the IPFW and PF implemented in an operating system FreeBSD, which have been tested by IPERF tool that analyzes network performance. Being a matter of Information Security, a chapter will be assigned to the explanation of this topic. A network was implemented, so the firewall can be between an internal network and an external network, the settings and building of the rules was made for the control of the network, aiming to minimize vulnerabilities. The methods that were used are Deductive and Comparative.

The rules of the firewalls were configured in the most identical way as possible, in order to evaluate the results and differences of both via IPERF.

The results obtained during the tests show that firewalls have minimal differences in the final result, however due to greater ease in the creation of rules with the PF firewall, it can be evaluated as the most practical to obtain the desired results.

Keywords: Firewall; Traffic Control; FreeBSD.

LISTA DE FIGURAS

LISTA DE SIGLAS

DHCP: Dynamic Host Configuration Protocol (Protocolo de Configuração Dinâmica de host).

DNS: Domain Name System (Sistema de Nomes de Domínios).

FTP: File Transfer Protocol (Protocolo de Transferência de Arquivos).

HTTP: Hypertext Transfer Protocol (Protocolo de Transferência de Hipertexto).

HTTPS: Hypertext Transfer Protocol Secure (Protocolo de Transferência de Hipertexto Seguro).

IP: Internet Protocol (Protocolo de Internet).

IPFW: IPFIREWALL.

NAT: Network Address Translation (Tradução de Endereços de Rede).

PF: Packet Filter.

PSI: Política da Segurança da Informação.

SSH: Secure Shell.

TI: Tecnologia da Informação.

SUMÁRIO

1 INTRODUÇÃO

O *firewall* é um mecanismo de segurança que permite a implementação de regras para controle de tráfego de uma rede. Para proteger a rede é utilizado em uma máquina especifica entre o *link* de Internet e a rede interna da empresa, portanto todo o tráfego de saída e entrada da rede passa pelo *firewall*, segundo Alecrim (2013):

> *Firewall* é uma solução de segurança baseada em *hardware* ou *software* (mais comum) que, a partir de um conjunto de regras ou instruções, analisa o tráfego de rede para determinar quais operações de transmissão ou recepção de dados podem ser executadas.

Para que funcione corretamente e que as regras sejam construídas com melhor nível de segurança possível, e atenda aos requisitos da empresa uma política de segurança é recomendada.

Este trabalho visa a comparação entre dois *firewalls* o IPFW e o PF*,* que são utilizados para implementar essas regras, permitindo a filtragem e tradução de IP's (NAT). Para realizar as análises destes *firewalls,* foram realizados experimentos em um ambiente controlado simulando uma rede com a utilização de dois *notebooks*, sendo um com o sistema operacional [1]FreeBSD utilizado para a implementação dos *firewalls* e o outro com os servidores dos tipos SSH, DNS, FTP e WEB, através de maquinas virtuais, dois adaptadores de placa de rede USB, cabo de rede padrão CAT5 e uma máquina *desktop* operando como uma máquina cliente. O *notebook* com o sistema FreeBSD ficará entre a rede externa (Internet) e as redes internas (servidores e clientes). A instalação do adaptador possibilitará conectar os outros computadores e realizar testes de filtragem e tradução de IP's (NAT).

A escolha deste tema, ocorreu devido ao interesse por *firewalls*, bem como IPFW e PF em conjunto com o sistema operacional FreeBSD.

Considerou-se também o fato de que o aprendizado sobre outras ferramentas é sempre importante para os profissionais da área de TI (Tecnologia da

[1] Sistema Operacional com código livre, distribuição do BSD, que é baseado em UNIX e criado na Universidade da California, Berkely.

Informação), pois o objetivo de estudo deste trabalho, é observar qual é o *firewall* com melhor desempenho e com comandos mais práticos para realizar o trabalho.

Em relação ao problema estudado, é analisado que para se manter a segurança da rede, podem ser utilizadas diversas barreiras, dos tipos físicas e lógicas. Essas barreiras quando implementadas de forma adequada se transformam em fatores importantes de mitigação de problemas de segurança. O problema apresentado neste trabalho relaciona-se com a utilização das barreiras lógicas que são o IPFW e o PF*,* e qual dos dois *firewalls* podem auxiliar melhor na manutenção da segurança da rede.

A pergunta criada foi, entre os *firewalls* IPFW e PF qual possuí o melhor desempenho para o controle da rede?

Nas hipóteses foi observado que existem três:

- Hipótese Favorável: Aplicar os *firewalls* IPFW e PF com as devidas regras e por fim concluir qual possuí um desempenho melhor.
- Hipótese Desfavorável: Construir a rede para teste e não implementar os *firewalls*.
- Hipótese Parcialmente Desfavorável: Aplicar os firewalls e não obter um resultado coerente sobre seus desempenhos.

O objetivo geral, consistiu na implementação parcial dos *firewalls* no FreeBSD, visando a comparação de ambos.

E como objetivos específicos:

- Explicar Segurança da Informação e seu tripé.
- Explicar como um *firewall* funciona, apresentando como o mesmo limita uma rede, deixando a rede o mais segura possível, permitindo acessos e bloqueios.
- Apresentar o PF, demonstrando suas características e seu funcionamento, utilizando a tabela FILTER e NAT.
- Apresentar o IPFW*,* mostrando suas características e seu funcionamento utilizando a tabela FILTER e NAT.
- Demonstrar os passos para a implementação do IPFW e PF no FreeBSD, deixando claro seu processo de filtragem e tradução de IP’s (NAT).

- Concluir qual dos *firewalls* apresentou o melhor desempenho.

Por fim o método de pesquisa abordado neste trabalho é o método dedutivo e comparativo, pois procura-se confirmar as hipóteses, que neste caso afirmam que realizando os devidos testes uma avaliação dos *firewalls* será possível e por ser uma comparação entre eles.

Devido à análise com a implementação do IPFW e PF no sistema operacional FreeBSD o método de procedimento deste trabalho, é um experimento em ambiente controlado. Tratando-se de uma pesquisa aplicada e a coleta de dados será feita por método de observação.

Quanto às técnicas de pesquisa, este trabalho se enquadra nas seguintes técnicas: pesquisa aplicada, qualitativa, descritiva e experimental.

O trabalho foi estruturado em cinco capítulos, o primeiro com a introdução, o segundo capítulo apresentará a segurança da informação e sua importância, assim como as dificuldades em sua implementação e alguns conceitos que ajudam na segurança da informação, buscando uma rede mais segura possível.

O terceiro capítulo, sobre *firewall*, explicará como o *firewall* funciona, conceitos importantes para sua implementação, como o NAT, além de especificar a estrutura das regras dos *firewalls* IPFW, PF e PFSENSE.

No quarto capítulo será abordado o ambiente de teste, explicando como os *firewalls* IPFW e PF foram implementados, configurações para implementa-los, as regras que foram construídas e como a comparação entre ambos foi realizada, assim como os testes efetuados para a comparação.

O último capítulo apresentará a conclusão deste trabalho, mostrando qual dos dois *firewalls* obteve um melhor desempenho.

2 SEGURANÇA DA INFORMAÇÃO

Segurança da Informação como o próprio nome sugere, é a proteção das informações, sejam elas pessoais ou de uma empresa. Sua implementação é de grande importância, porem o grande problema é como fazer corretamente.

Existem vários elementos que podem ajudar, como por exemplo, câmeras, extintores, o cabeamento estar bem estruturado, antivírus, backup, manutenção preventiva dos equipamentos, dentre vários outros. Esses elementos são chamados de barreiras e são divididos entre as barreiras lógicas e físicas, (INNARELLI, 2013). Mas sem um planejamento para uma melhor administração, o resultado pode não ser o esperado, mantendo em mente também que não existe uma rede, um sistema ou um site 100% seguros, existe a possibilidade do mais seguro possível, mas é impossível conseguir uma rede 100% segura, a partir do momento que algo está na rede, que se conecta à Internet, o mesmo estará exposto a diversos riscos, é o objetivo da segurança da informação tentar evitar esses riscos, protegendo a rede o máximo possível, (ASSUMPÇÃO, 2010).

Os *hackers* normalmente rastreiam até encontrar uma vulnerabilidade, em alguns casos, eles já sabem qual vulnerabilidade a ser explorada, o que torna a situação mais perigosa, enquanto isso o administrador de sistemas tem que estar preparado para estas situações, procurando por vulnerabilidades, reparando a mesma e desenvolvendo um plano de resposta ao incidente, caso a vulnerabilidade seja explorada, estes assuntos serão abordados nos capítulos a seguir.

Um *hacker* pode causar diversos problemas ao sistema, os administradores do sistema devem estar sempre atentos, existem situações que o próprio funcionário está por traz da invasão, tendo como objetivo alterar ou simplesmente tentar extrair informações confidenciais, com o intuito de prejudicar a empresa de alguma forma, segundo Stallings (2015, p.17).

> Um hacker pode ser alguém que, sem intenção maliciosa, simplesmente se satisfaz em romper e entrar em um sistema de computadores. Ou, então, o intruso pode ser um funcionário aborrecido, que deseja causar danos, ou um criminoso que busca explorar recursos do computador para obter lucro financeiro (exemplo, obter números de cartão de credito ou realizar transferências ilegais de dinheiro).

Além disso, os ataques evoluem a todo momento, o que ocasiona em uma boa preparação dos profissionais de TI contra esses ataques, sendo o mais eficiente e eficaz possível, isto é, procurar estar sempre atualizado sobre possíveis técnicas de invasão, não ser dependente das ferramentas, é o administrador quem deve direcionar a defesa, se o mesmo não estiver atualizado, a invasão pode acontecer e gerar grandes prejuízos, conforme Nakamura e Geus (2007, p.25).

> O mundo da segurança, seja pensando em violência urbana ou em hackers, é peculiar. Ele é marcado pela evolução contínua, no qual novos ataques têm como resposta novas formas de proteção, que levam ao desenvolvimento de novas técnicas de ataques, de maneira que um ciclo é formado. Não é por acaso que é no elo mais fraco da corrente que os ataques acontecem. De tempos em tempos os noticiários são compostos por alguns crimes 'da moda', que vêm e vão. Como resposta, o policiamento é incrementado, o que resulta na inibição daquele tipo de delito. Os criminosos passam então a praticar um novo tipo de crime, que acaba virando notícia. E o ciclo assim continua. Já foi comprovada uma forte ligação entre sequestradores e ladrões de banco, por exemplo, no qual existe uma constante migração entre as modalidades de crimes, onde o policiamento é geralmente mais falho.

Isso acontece devido à constante evolução da tecnologia, e à constante dependência adquirida, a maioria dos equipamentos utilizam energia, basta lembrar-se que, se repentinamente a energia elétrica acaba, equipamentos eletrônicos e eletroeletrônicos dependentes da mesma como, por exemplo, fogão, geladeira, luz, computadores, etc., deixam de funcionar. Diante destas situações a segurança é necessária, pois como grande parte dos equipamentos modernos são conectados à rede Internet nos dias de hoje, como podemos viver sem as devidas proteções de nossas informações?

A necessidade atual de querer tudo da maneira mais fácil, e rápido possível, acaba prejudicando a atenção com a segurança, acarretando no esquecimento de certos cuidados como, por exemplo, senhas simples demais, senhas com nome de pessoas ou de parentes ou datas importantes como nascimento.

Os usuários acabam escolhendo uma senha qualquer ou informando a senha a terceiros que não deveriam ter acesso ou até mesmo anotando a senha e deixando está em locais visíveis, como mostra Stallings (2015, p.10), "Muitos usuários, e até mesmo administradores de segurança, veem uma segurança forte como um impedimento à eficiência e a operação amigável de um sistema de informação ou do uso da informação".

Alguns dos elementos que ajudam na administração da segurança da informação é a análise de risco, ter consciência do fator humano, política da segurança da informação, resposta a incidentes de segurança e por fim o tripé da segurança da informação, que serão abordados nos capítulos seguintes.

2.1 ANÁLISE DE RISCO

Em um cenário em que está tudo bem, sem nenhum problema aparente, existe a falsa sensação de segurança, sendo difícil a percepção dos benefícios que a mesma traz, o que acaba gerando a falta de investimento, este assunto normalmente volta a ser discutido quando algum incidente já ocorreu, (STALLINGS, 2015, p.10).

Tudo isso acaba gerando ataques que acontecem por meio dessas vulnerabilidades, os ativos, ou seja, algo de valor, que proporcionam benefício de alguma forma ao indivíduo ou empresa, possuem vulnerabilidades, que por sua vez causam as ameaças, que são cenários de risco que podem causar algum impacto, e isto tende a aumentar cada vez mais devido à evolução da tecnologia, como mostra Nakamura e Geus (2007, p.47), “[...] Os avanços tecnológicos vêm resultando em grandes oportunidades de negócios, porém, quanto maior essa evolução, maiores as vulnerabilidades que aparecem e que devem ser tratadas com a sua devida atenção[...]”.

Dentro das vulnerabilidades, existem as internas e externas, normalmente as empresas tendem a se preocupar mais com as externas, sendo que são as vulnerabilidades internas que causam os maiores danos, conforme Nakamura e Geus, (2007, p.68), “Apesar de as pesquisas mostrarem que o número de ataques partindo da Internet já é maior do que os ataques internos, os maiores prejuízos ainda são causados por incidentes internos”. Estes incidentes internos são causados, pois o foco está na segurança do sistema, isto é, parte lógica e física, que são de grande importância, mas acabam esquecendo-se de uma parte que também deve ser analisada, o fator humano, (BORTOLETO, 2015), assunto que será discutido no próximo capítulo.

A análise desse cenário pode ser avaliada com a análise de risco, esses dados são importantes para realizar um plano de contingência e a política de segurança da informação, podendo criar posteriormente controles para as vulnerabilidades encontradas, minimizando os riscos.

Essa análise pode mudar dependendo da empresa, pois uma é diferente da outra, portanto as vulnerabilidades encontradas podem ser diferentes.

Nesta etapa é feito uma lista das possíveis vulnerabilidades para determinados ativos e ameaças que as vulnerabilidades podem causar e por fim os riscos (impacto), como mostram as figuras 1 e 2.

Figura 1: Empresa A – Avaliação de Risco.

ATIVOS	VULNERABILIDADES	AMEAÇAS	RISCOS
MÁQUINAS	Perda de conexão.	Cascateamento incorreto de switch.	Computadores inoperantes.
	Refrigeração imprópria.	Aquecimento do equipamento.	Queima de equipamentos.
SERVIDOR	Refrigeração imprópria.	Aquecimento de equipamento.	Queima de equipamentos/dispositivos.
	Fácil acesso.	Poderá ser danificado.	Perda de dados e equipamento.
	Perda de conexão.	Cascateamento incorreto de switch.	Serviços inoperantes.
SWITCH	Cascateamento incorreto de switch.	Algum switch pode perder a conexão.	Lentidão ou perda de conexão.
	Falta de padronização.	Configurações incorretas.	Lentidão na rede.
	Fácil acesso.	Poderá ser danificado	Perda de dados e equipamento.

Fonte: Autoria própria.

Figura 2: Empresa B – Avaliação de Risco.

ATIVOS	VULNERABILIDADES	AMEAÇAS	RISCOS
SERVIDOR - AD E DNS	Configurações incorretas.	Bloqueio ou permissão inapropriadas.	Falta de disponibilidade e confidencialidade.
	Controle inexistentes.	Máquina do servidor com problema físico.	Serviços inoperantes.
SERVIDOR - ARQUIVOS E DHCP	Controle inexistentes.	Máquina do servidor com problema físico.	Serviços inoperantes.
			Distribuição de IP's inoperante.
SWITCH	Falta de padronização.	Configurações incorretas.	Lentidão na rede.
MÁQUINAS	Invasão da máquina.	Deixar a máquina infectada.	Lentidão da máquina

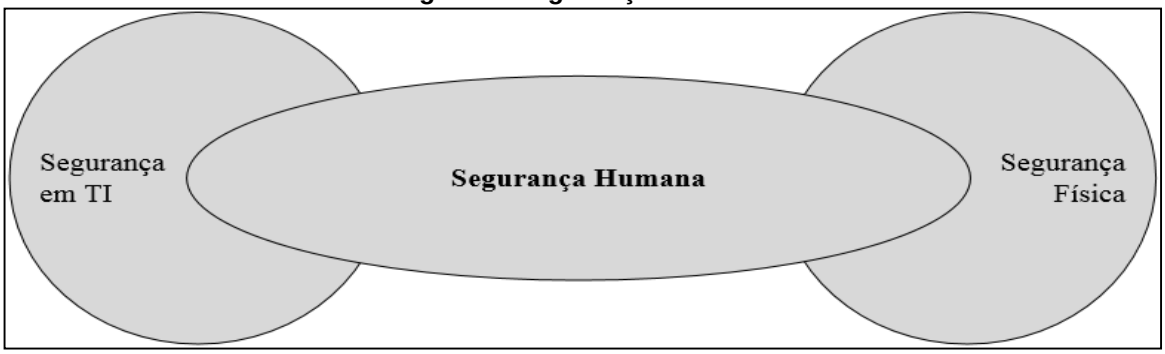
Fonte: Autoria própria.

Essa avaliação de risco em uma empresa seria muito mais detalhada e é claro que existe uma grande dificuldade para catalogar todas as vulnerabilidades existentes, o que torna este processo árduo.

2.2 FATOR HUMANO

O fator humano não é muito trabalhado nas empresas, é frequentemente esquecido e que ao ser explorado causa grande impacto, como mostra a figura 3, pois existem ataques que são utilizados pelos hackers que usam apenas o fator humano como meio de invasão, sem precisar abordar as barreiras lógicas ou físicas, (MANN, 2011, p. 9).

Figura 3: Segurança Humana.



Fonte: Adaptado de Mann (2011, p.10).

Essa técnica utilizada pelos hackers que procura explorar o elo mais fraco utilizando a persuasão para obter informação é chamada de engenharia social, conforme Ferreira (2014).

> A engenharia social é a arte de manipular as pessoas para conseguir informações confidenciais. No ataque de engenharia social, um atacante utiliza a interação humana (habilidades sociais e psicológicas) para obter informações ou conseguir comprometer o computador e sistemas de uma empresa ou pessoa.

Através de engenharia social, normalmente funcionários sem certos conhecimentos prejudicam a empresa, vazando informações da mesma sem perceber o que está acontecendo.

Para evitar situações como esta deve ser construída uma boa política de segurança, além de treinamento dos funcionários, evitando situações como, um funcionário informar sua senha, ou outras informações referentes a empresa por telefone, descartar o lixo da empresa de forma indevida, deixando informações intactas ou parcialmente intactas, possibilitando o acesso do hacker a elas, deixar muita informação restrita a um funcionário sem que o mesmo tenha assinado um documento de confidencialidade com a empresa.

2.3 POLÍTICA DA SEGURANÇA DA INFORMAÇÃO

A política da segurança da informação é um recurso que podemos utilizar para resolver esse problema, pois após a elaboração da análise de risco, sua criação

se torna mais efetiva, e sua elaboração também é feita de acordo com a empresa, assim como o plano de contingencia ou avaliação de risco, com a política podemos obter uma padronização da segurança, por exemplo, especificar o que deve e o que não deve ser bloqueado pelo *firewall*, ou quantos caracteres uma senha deve ter, se os funcionários bloqueiam suas máquinas ao saírem. Diante disto a política de segurança da informação ou PSI torna-se essencial para uma empresa e auditorias.

Para que funcione adequadamente ela deve ser aprovada e comunicada a todos os funcionários, todos devem saber e seguir essa norma, segundo Basto (2015).

> A Política de Segurança da Informação – PSI é um documento que registra os princípios e as diretrizes de segurança adotado pela organização, a serem observados por todos os seus integrantes e colaboradores e aplicados a todos os sistemas de informação e processos corporativos.

Proporciona a mitigação de incidentes relacionados com o fator humano, por isso a importância de ser propriamente divulgada.

2.4 RESPOSTA A INCIDENTES DE SEGURANÇA

Caso alguma violação da segurança da informação tenha ocorrido, a melhor forma de se reestabelecer o sistema o mais rápido possível minimizando os riscos é por meio de um bom plano de resposta a incidentes de segurança, (MCCARTHY, 2014, p.36).

Seus principais princípios são:

- Identificação do incidente, que comprova se o mesmo existe e seu impacto;
- Coordenação do incidente, cabe a essa etapa verificar o dano causado e com base nos dados coletados nessa e na etapa anterior formular possíveis meios de mitigação;
- Mitigação do incidente, que implementa uma solução ou controle;
- Investigação do incidente, que coleta as informações do porque o incidente ocorreu e como foi resolvido.

Por meio desses princípios a quebra da segurança pode ser restaurada, isto é independente da causa, por exemplo, *hackers,* greves, fator humano, inundação, tempestade, e para que no futuro, caso ocorra o mesmo incidente ou um semelhante o plano de resposta ao incidente desenvolvido possa identificar e mitigar facilmente, (ARANHA, 2015).

E a probabilidade de ocorrência auxilia a manter uma prioridade e atenção a certos incidentes, (MCCARTHY, 2014, p.48).

> Se o risco que você está combatendo for um evento de alta probabilidade, o melhor pode ser organizar sua estrutura cotidiana para reagir a ele. Se for um evento de baixa probabilidade que possa nem ocorrer à sua empresa, faz sentido que essa estrutura adequada esteja pronta para ser implementada durante o momento de crise.

A figura 4 demonstra uma simulação de probabilidade de ocorrência de incidentes.

Figura 4: Simulação da probabilidade de ocorrência de incidentes em uma empresa X.

Probabilidade de Ocorrência	Baixa	Média	Alta
Tempestade			X
Incêndio		X	
Roubo	X		
Falhas humanas			X
Acesso não autorizado			X
Greves	X		
Violência no Local de Trabalho	X		

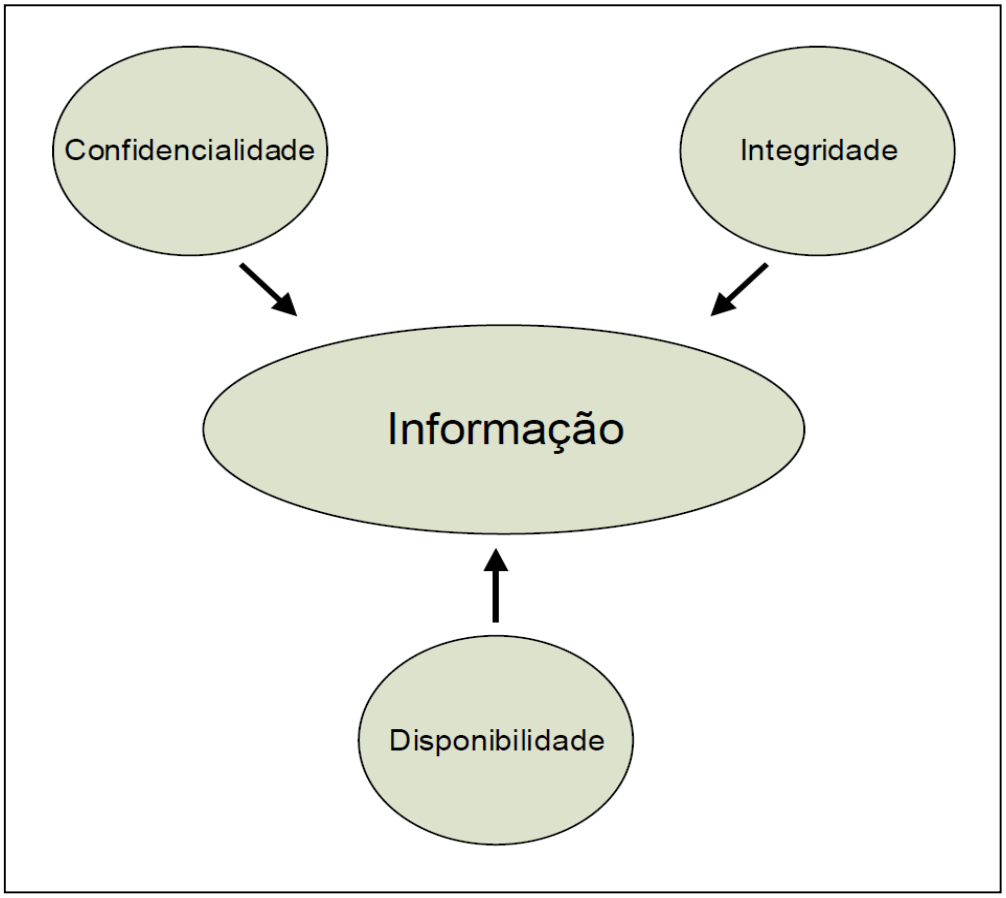
Fonte: Autoria própria.

Uma política de backup também deve ser definida, isto é, lugar do armazenamento, no mínimo dois lugares e distantes um do outro e de quanto em quanto tempo será realizado, definir plano de continuidade para os recursos afetados, como por exemplo, climatização, acesso e incêndio, infraestrutura elétrica, como a instalação de um segundo gerador, (ARANHA, 2015).

2.5 TRIPÉ DA SEGURANÇA DA INFORMAÇÃO

E mesmo com todos esses fatores comentados anteriormente nada dentro da segurança da informação funcionará corretamente sem colocar certos princípios em mente para se obter o maior nível de segurança possível, são eles: Confidencialidade, Integridade e Disponibilidade, como mostra a figura 5.

Figura 5: Relação entre Informação e o tripé da Segurança da Informação.



Fonte: Adaptado de Nakamura e Geus (2007, p.44).

Esses três conceitos são os foco da segurança, ou seja, quanto menor for a preocupação com o tripé maior será o prejuízo da empresa, pois o tripé possibilita o crescimento, mais oportunidades, variadas estratégias, planejamento da segurança, mas como já foi dito, o que acontece hoje são tentativas de se recuperar de algum ataque, porque a preocupação com a segurança vem quando algo deu errado e não antes Stallings (2015, p.7), mas o que as empresas ou individuo precisam entender é

que hoje uma das principais armas do mercado é o conhecimento, assim como cita Nakamura e Geus (2007, p.70).

> (...)a economia, hoje, tem como base o conhecimento, de modo que a própria informação constitui um dos grandes fatores para a vantagem competitiva. Isso faz com que as consequências de um incidente envolvendo segurança sejam potencialmente desastrosas, influenciando até mesmo a própria sobrevivência da organização(...).

Esse conhecimento quando explorado seja por rivais ou *hackers*, pode quebrar a imagem da empresa, causando apenas prejuízo, sendo que a confiança dos clientes é um fator importante para que a empresa continue crescendo.

Portanto, a proteção das informações deve ser vista como necessária para o desenvolvimento da confiança com os clientes e andamento dos negócios, (MÉDICE, 2013).

O *firewall,* como já foi dito, é uma barreira lógica que filtra a rede, portanto consegue auxiliar nos princípios, dificultando invasões tanto de indivíduos maliciosos quanto de *malwares*.

> Os malwares, conhecidos pelo termo *malicious software* (do inglês software malicioso), são programas desenvolvidos para executarem ações danosas e ilícitas em um sistema. Entre os danos mais conhecidos, podem ser destacados a perda de dados e o roubo de informações sigilosas (BITTENCOURT, 2013).

- CONFIDENCIALIDADE - Em uma política deve ser definido quem possuí acesso a determinada informação, apenas pessoas autorizadas podem ter acesso dificultando a invasão de terceiros, conforme Maia (2013), “Confidencialidade, diferente de ser um segredo ou algo inacessível, é um conceito no qual o acesso à informação deve ser concedido a quem de direito, ou seja, apenas para as entidades autorizadas pelo proprietário ou dono da informação”.
- INTEGRIDADE - A informação deve estar inteira, isto é, não corrompida ou alterada por terceiros, conforme Moraes (2015, p.20), “A integridade é o serviço de segurança que garante que a informação não será alterada, intencionalmente ou não, durante seu armazenamento ou processamento. Garantir a integridade é uma tarefa fundamental”.

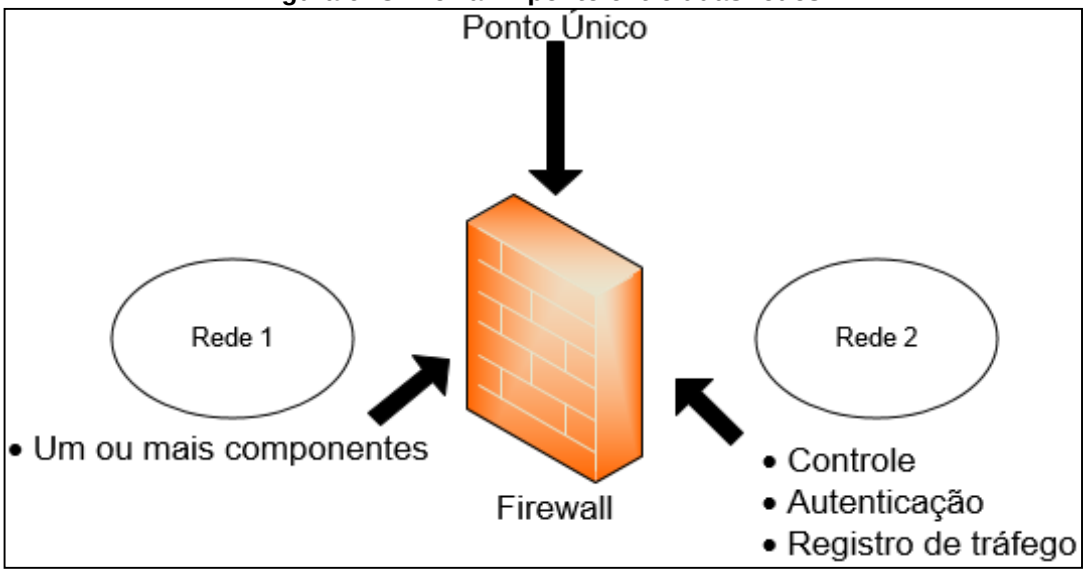
- DISPONIBILIDADE - O acesso deve estar permitido e disponível quando pessoas autorizadas quiserem o acesso a informação, conforme Benetti (2015), “[...] significa garantir que a informação possa ser obtida sempre que for necessário, isto é, que esteja sempre disponível para quem precisar dela no exercício de suas funções”.

3 FIREWALL

O *firewall* age como um controle de acesso à rede, que pode determinar as permissões e bloqueios dependendo da política de segurança da empresa.

Um ponto entre duas ou mais redes, como demonstrado na figura 6, que protege e que também caso configurado pode gerar um arquivo de log com informações dos pacotes que entram, saem ou que ficam bloqueados, essa informação pode ser consultada para administração da rede caso haja algum problema na mesma, por exemplo, um determinado computador não consegue acessar a Internet, neste caso o administrador da rede pode consultar e analisar o log como forma de determinar qual o problema e assim chegar a soluciona-lo.

Figura 6: O firewall – ponto entre duas redes.



Fonte: Adaptado de Nakamura e Geus (2007, p.222).

O *firewall* é a primeira barreira lógica que um *hacker* enfrenta em uma invasão, por isso a sua importância, (NAKAMURA e GEUS 2007, p.187) ou como mostra Moraes (2015, p.24), “O *firewall*, ou “parede de fogo”, tem um papel fundamental, porque é ele que vai separar a rede protegida – ou seja, a rede interna – da rede externa, que é desprotegida. Portanto, o *firewall* é a base da proteção perimetral”.

O *firewall* é construído por meio de regras, e essas regras podem seguir dois princípios:

- O tráfego estar bloqueado para depois ser criada as regras de permissão, (ALECRIM, 2013);
- O de estar permitido para depois ser criada as regras de bloqueio, (ALECRIM, 2013).

Portanto suas regras devem ser devidamente implementadas, procurando minimizar as falhas, ou só aumentará as vulnerabilidades da rede.

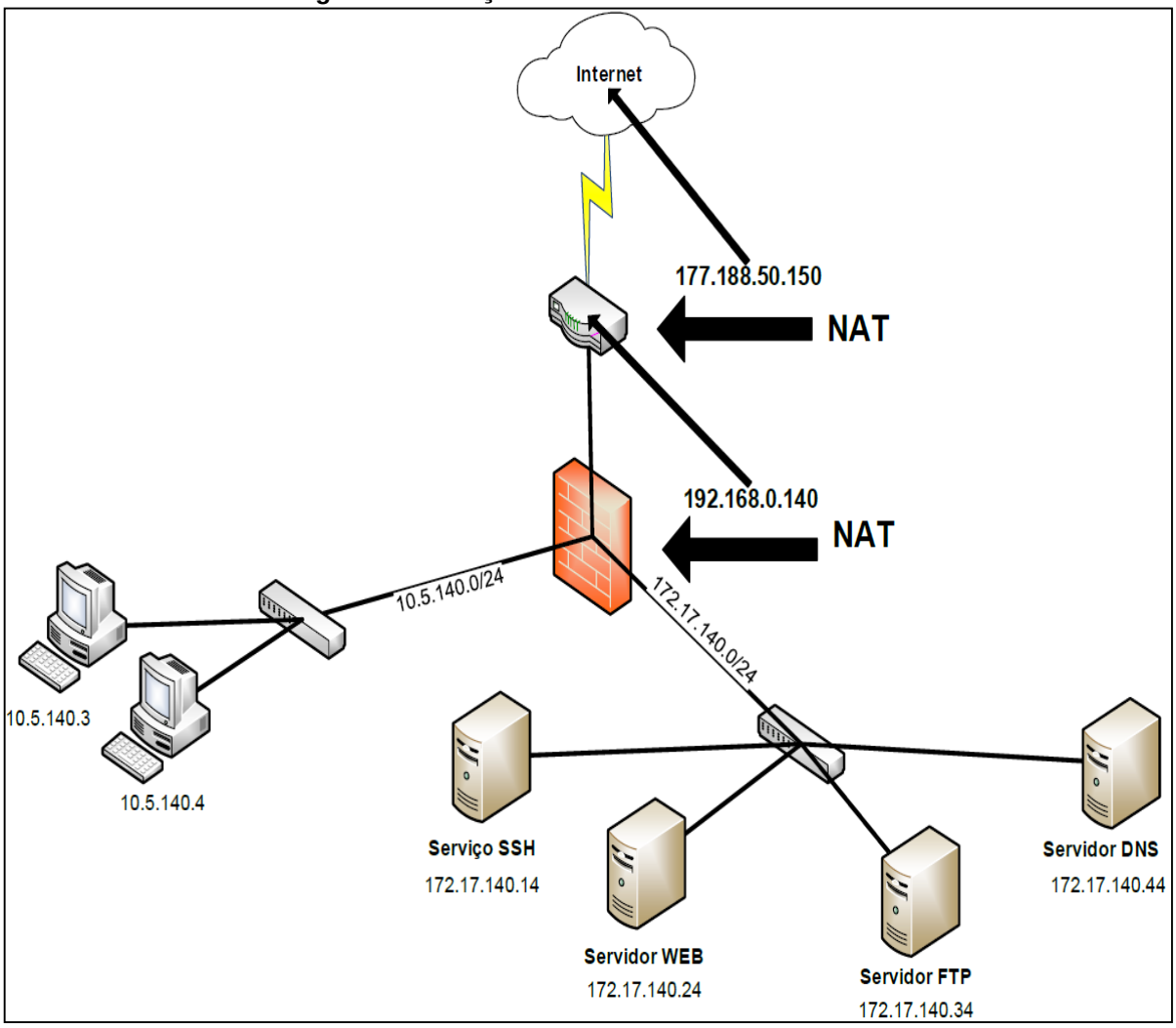
As regras de permissão do tráfego precisam ser avaliadas cuidadosamente para não permitir o acesso indevido, segundo Nakamura e Geus (2007, p.131).

> Os *firewalls*, se bem configurados, dificultam muito a efetividade e eficiência dos ataques, de modo que os hackers passaram a buscar outras formas de invadir a rede interna das organizações, por meio da utilização do tráfego permitido pelo *firewall*.

Outro recurso do *firewall* é o NAT (Network Address Translation), este protocolo traduz um número IP por outro número IP, existem aparelhos com essa função de “nateamento”, como roteadores ou no caso deste trabalho o *firewall.*

Por exemplo, uma rede interna que possuí um computador com o número de IP 10.5.140.3 e um *firewall* com o número de IP 192.168.0.140, o *firewall* recebe a requisição do computador e traduz para sair na rede externa com o número de IP do *firewall* 192.168.0.140, os números IP’s da rede interna não são conhecidos na externa, apenas o número transmitido por meio do “nateamento”, assim como mostra a figura 7.

Figura 7: Tradução de números IP's com o NAT.



Fonte: Autoria própria.

Os números de endereço IPv4 que permitem o acesso à Internet já acabaram, o NAT teve como proposito resolver os problemas relacionados ao esgotamento desses números e não como propósito de segurança, (PINTO, 2015). Mas que no fim ajuda na mesma, pois máscara o número de IP privado, (MORAES, 2015, p.40).

Rede pública é aquela reconhecida dentro da Internet, uma requisição de consulta a mesma não reconhece IP's privados, esses IP's são usados apenas em redes internas, conforme Pinto (2009).

> Quanto a endereços privados, estes não nos permitem acesso direto à Internet, no entanto esse acesso é possível mas é necessário recorrer a mecanismos de tradução como o NAT (Network Address Translation) que traduzem o nosso endereço privado para um endereço público.

3.1 IPFW

O IPFW é um *firewall* baseado em software para o sistema operacional FreeBSD, ou seja, ele vem integrado ao sistema.

Tem por padrão regras sequenciais, ou seja, a leitura das regras ocorre de cima para baixo, porém, assim que um pacote se equipara a regra, ele interrompe o processo, não lendo a regra seguinte, (LUCAS, 2002, p.295).

A sequência não ocorre necessariamente pela ordem em que as regras são definidas e sim pela ordem de acordo com a numeração atribuída. Por exemplo, se for criada uma regra com a numeração 50 e depois uma regra com a numeração 10, o *firewall* ira priorizar a regra 10.

A numeração inicia de 1 até 65534, possuindo também uma regra oculta de número 65535, a qual nega todos os pacotes, ou seja, sem uma regra de permissão o *firewall* nega todos os pacotes, pois já é configurado para isso, (LUCAS, 2002, p.294).

Abaixo um exemplo de sintaxe do IPFW e significados:

- Ipfw add [número da regra] [permissão] [protocolo] from [origem] to [destino] via [interface]

- **Permissão:** Permite o administrador negar (deny) ou permitir (allow) os pacotes.
- **Protocolo:** Permite selecionar o protocolo desejado.
- **Origem:** Define o endereço IP que receberá as permissões do *firewall*.
- **Destino:** Define o endereço IP do destino onde a origem será permitida ou negada.
- **Interface:** Permite selecionar a interface de rede que deseja atribuir as regras.

Para poder habilitar o IPFW no FreeBSD é necessário abrir um arquivo de configuração padrão do sistema o **/etc/rc.conf** e editá-lo.

Assim como demostrado na figura 8, a primeira linha habilita o IPFW, a segunda indica o tipo de *firewall* e a última o caminho do arquivo onde as regras serão implementadas.

Figura 8: Habilitando o IPFW.

```
#Configuracao IPFW
firewall_enable="yes"
firewall_type="open"
firewall_script="/etc/ipfw.conf"
```

Fonte: Autoria própria.

3.2 PF

O PF também é um *firewall* baseado em software, originalmente foi criado para o sistema operacional OpenBSD, mas hoje já é integrado ao sistema operacional FreeBSD.

No passado o *firewall* utilizado era conhecido como IPFilter, desenvolvido por Darren Reed. Posteriormente em 2001 foi descoberto que este *firewall* não permitia alterações nas linhas do código, por este motivo o IPFilter foi posteriormente retirado de uso. Devido a este ocorrido com o IPFilter, houve a necessidade da criação de um novo tipo de *firewall*, conhecido como PF. O *firewall* PF que já estava sendo desenvolvido foi oficialmente lançado em sua versão 3.0 no ano de 2001, (HANSTEEN, 2014, p.04).

Assim como o IPFW o PF verifica as regras de cima para baixo, entretanto este não interrompe a leitura do pacote assim que o mesmo se equipara a alguma regra definida. Por este motivo a regra para bloquear todo o *firewall* está na primeira linha do PF e no caso do IPFW encontra-se na última linha.

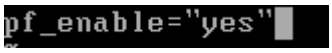
Por motivos de segurança, é recomendado que o *firewall* esteja primeiro bloqueado para depois ser liberado (permitido), aumentando a dificuldade na elaboração das regras, porem aumentando a segurança (LUCAS, 2007, p.273).

Abaixo um exemplo de sintaxe do PF, os significados a seguir são os mesmos citados no capitulo 3.1 IPFW:

- [permissão] on [interface] proto [protocolo] from [origem] to [destino]

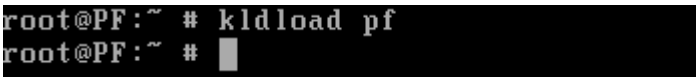
Assim como o IPFW, para habilitar o PF no sistema FreeBSD é necessário abrir um arquivo de configuração padrão do sistema, o **/etc/rc.conf** e editá-lo, para em seguida executar um comando, como mostram as figuras 9 e 10.

Figura 9: Habilitando o PF.



Fonte: Autoria própria.

Figura 10: Comando para habilitar o PF.



Fonte: Autoria própria.

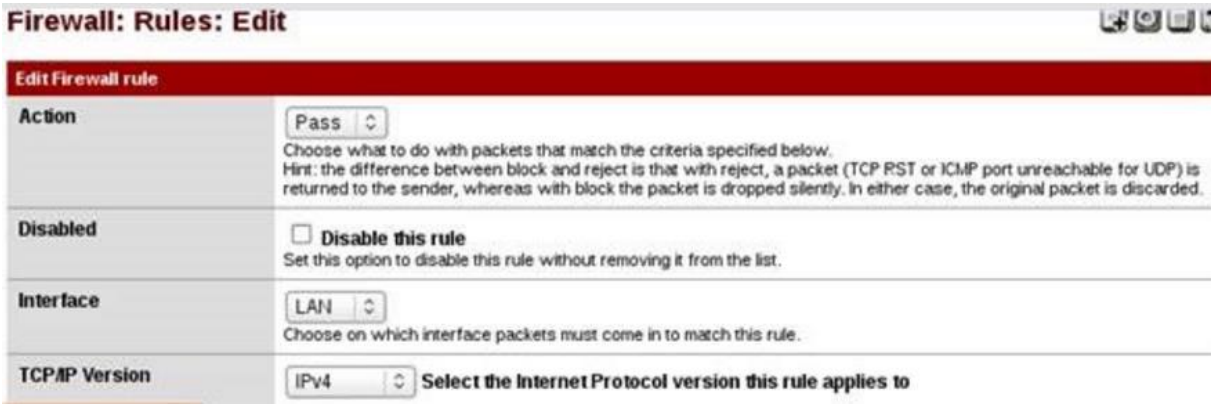
3.3 PFSENSE

O *firewall* baseado em software de nome pfSense começou a ser projetado no ano de 2004 por Chis Buechler e Scott Ullrich, feito originalmente para o sistema operacional FreeBSD, vem se tornando muito reconhecido, pois diferente dos *firewalls* IPFW e PF, o pfSense possuí uma interface gráfica, facilitando a interação do administrador com as configurações, (BUECHLER e PINGLE, 2009, p.01).

Segundo Mazuco (2015), “Ele é um *software* com a licença BSD, ou seja, você não precisa pagar nada para poder usar. Ele possui recursos que muitas vezes, só encontrada em *firewalls* comerciais muito caros. O que torna uma poderosa ferramenta”.

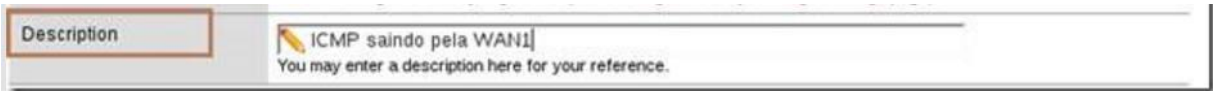
O pfSense é bem prático para criação das regras, possibilitando uma melhor organização, pois existem as explicações das ações e possibilitando ao administrador descrever o significado de cada uma das regras, como mostram as figuras 11 e 12.

Figura 11: Configuração de regras no pfSense.



Fonte: Adaptado de Galvão (2014).

Figura 12: Descrição das regras no pfSense.



Fonte: Adaptado de Galvão (2014).

O resultado final é uma administração coesa e organizada da rede, pois a visualização da mesma se torna bem estruturada. A figura 13 demonstra claramente a estrutura da configuração.

Figura 13: Visualização das regras no pfSense.

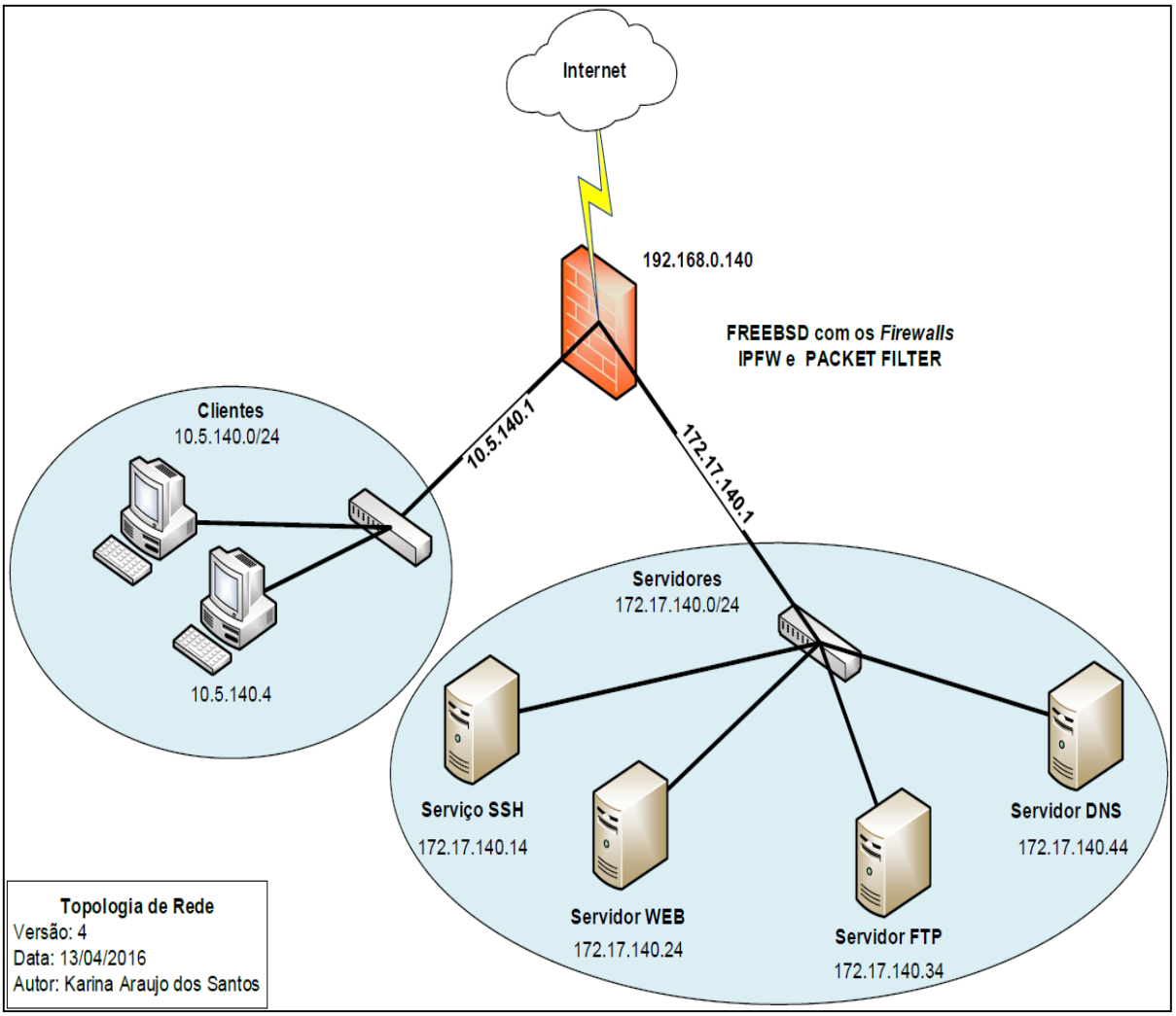
Proto	Source	Port	Destination	Port	Gateway	Schedule	Description
TCP	LAN net	*	*	80 (HTTP)	*	BusinessHours	Block Web Access during Business Hours

Fonte: Adaptado de Buechler e Pingle (2009, p.106).

4 AMBIENTE DE TESTE

Para a análise e comparação entre os *firewalls* IPFW e PF, no sistema operacional FreeBSD, foi utilizado um *notebook*, com quatro máquinas virtuais, todas utilizando o sistema FreeBSD, simulando os servidores, e também foi utilizado um *desktop* (PC) rodando o sistema operacional Windows 7, simulando um cliente "funcionário". O tráfego da rede servidores e da rede clientes passa pelo *firewall* e o mesmo, de acordo com as regras implementadas, determina o destino dos pacotes, assim como demonstrado pela figura 14.

Figura 14: Topologia de Rede.



Fonte: Autoria própria e efetuado através da ferramenta Visio 2013.

Os servidores implementados foram:

- Secure Shell (SSH) é possível realizar conexões de um computador para outro, segundo Arruda (2010), “[...] o SSH criptografa os dados trafegados entre os computadores, dificultando assim a interceptação dos mesmos por pessoas mal-intencionadas”.

- Web é responsável pelas “páginas da Internet”, ou seja, ou realizar uma solicitação de acesso a qualquer site, esse site precisa estar hospedado em um servidor Web, assim como mostra Oliveira (2016).

> O servidor web é a peça mais importante da infraestrutura de um site na Internet. Ele é um programa que usa o HTTP (Hypertext Transfer Protocol) para servir os arquivos que formam páginas da web para os usuários, em resposta aos seus pedidos, que são encaminhadas pelos clientes HTTP de seus computadores.

- File Transfer Protocol (FTP), realiza como o próprio nome descreve, a transferência de arquivos entre locais, (FEDEL, 2013).

- Domain Name System (DNS) faz a tradução do endereço do site, como www.google.com.br para o IP, exemplo, o IP 192.168.200.57 é o IP de um determinado site, caso não existisse DNS para fazer essa tradução em uma consulta teríamos que procurar pelo IP 192.168.200.57 e não pelo nome o que causaria dificuldade e confusão aos usuários. O DNS também possui um sistema de cache, caso um usuário tenha realizado uma solicitação de acesso ao uol, por exemplo, a segunda vez que aquele usuário ou outros usuários da mesma rede fizerem a mesma solicitação a resposta será mais rápida, pois o servidor não procura por esse site mais uma vez, a informação ficou guardada no cache, (FEDEL, 2013).

O *firewall* deverá possuir três interfaces de rede, uma para se conectar com a rede externa (Internet), outra para a rede interna de servidores e outra para a rede interna de clientes, como mostra a figura 14. A configuração das interfaces de rede é a primeira configuração que foi realizada para que o cenário montado funcionasse corretamente. Esta configuração foi efetuada no arquivo **/etc/rc.conf**, como demonstrado na figura 15.

Figura 15: Configuração das redes em cada interface de rede.

```
#Configuracao de rede, definindo IP e mascara para esta maquina, rede clientes e
 servidores:
#ifconfig_re0="DHCP"
ifconfig_re0="inet 192.168.0.140 netmask 255.255.255.0"
ifconfig_ue0="inet 172.17.140.1 netmask 255.255.255.0"
ifconfig_ue1="inet 10.5.140.1 netmask 255.255.255.0"
#Definindo gateway para esta maquina:
defaultrouter="192.168.0.1"
```

Fonte: Autoria própria.

A configuração de rede da placa que se comunica com a Internet depende da rede em que está conectada. Ao mudar de rede seu endereço IP e *gateway* deverão ser mudados ou até deixados como DHCP, que é um protocolo que atribuí um IP no dispositivo que entrar na rede e solicitar, possibilitando obter um IP automaticamente, normalmente ele atribui o primeiro IP disponível na rede, (FEDEL, 2013). Portanto a rede que ficará para os servidores (172.17.140.0/24) e a rede de clientes (10.5.140.0/24) continuará com as mesmas configurações.

Uma vez configurado, o *firewall* consegue se comunicar com as outras máquinas que estão na mesma rede, ou seja, a rede de servidores e de clientes, porém não consegue se comunicar com a Internet. Diante disto é necessário configurar o DNS em um arquivo do sistema FreeBSD **/etc/resolv.conf**, para que ocorram as traduções de nomes, assim como mostra a figura 16.

Figura 16: Configurando o arquivo resolv.conf com o DNS do google.

```
nameserver 8.8.8.8
```

Fonte: Autoria própria.

Uma outra configuração necessária, é tornar o *firewall* em um *gateway* no arquivo **/etc/rc.conf**, isto é, um “portão”, o caminho que a rede interna deverá seguir para conseguir acessar a rede externa e as outras redes. Esta configuração é demonstrada na figura 17.

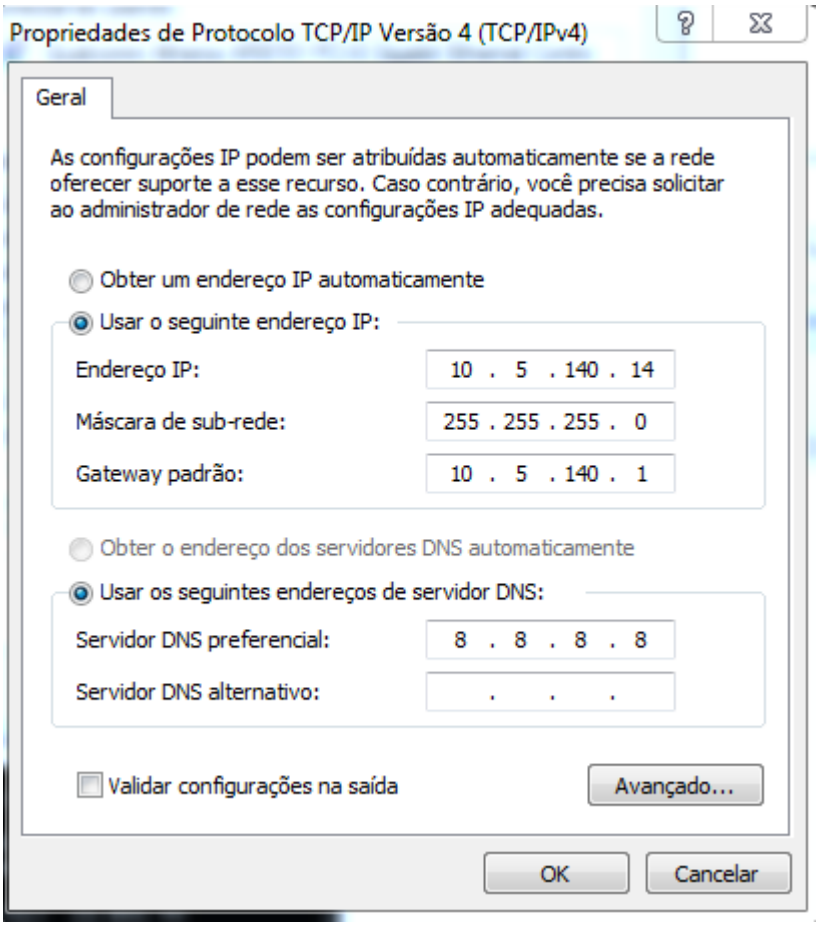
Figura 17: Habilitando a máquina para funcionar como gateway.

```
gateway_enable="yes"
```

Fonte: Autoria própria.

Para finalizar, os IP's também foram configurados nos servidores que por estarem com o sistema operacional FreeBSD as configurações são parecidas com as realizadas no *firewall*, assim como mostra a figura 15, mas com as configurações da rede 172.17.140.0/24. Configurações realizadas também na máquina cliente da rede 10.5.140.0/24, como mostra a figura 18.

Figura 18: Configurando interface na máquina cliente.



Fonte: Autoria própria.

4.1 CONFIGURAÇÃO DE NAT COM O IPFW E PF

Para que os testes funcionassem, foi necessário que em cada *firewall*, tanto no IPFW quanto no PF fosse configurado o NAT, pois sem ele a rede interna não conseguiria alcançar a rede externa (Internet).

Para habilitar o NAT no IPFW foi necessário habilitar e configurar o NATD, recurso existente neste *firewall* e responsável pelo NAT, sendo o mais importante destas configurações indicar a interface de rede que se conecta à Internet, pois é nela que o NAT será implementado, porque é o IP do *firewall* que será reconhecido e não o IP da rede interna.

No mesmo arquivo que foi habilitado o IPFW o **/etc/rc.conf,** também será habilitado o NAT e deverá ser apontado o arquivo de configuração do mesmo, assim como demonstrado na figura 19, as configurações de NAT foram efetuadas no arquivo **/etc/natd.conf** e são demonstradas na figura 20.

Figura 19: Habilitando NATD.

```
#Configuracao IPFW NAT
natd_enable="yes"
natd_flags="-f /etc/natd.conf"
natd_interface="re0"
```

Fonte: Autoria própria.

Figura 20: Configurando NATD.

```
interface re0
dynamic yes
same_ports yes
use_sockets yes
```

Fonte: Autoria própria.

Após realizadas estas configurações, as regras de NAT poderão ser adicionadas no arquivo das regras de *firewall* do IPFW, no caso desta monografia o **/etc/ipfw.conf**.

A figura 21 demonstra a regra que redireciona toda a rede interna, possibilitando o acesso a qualquer endereço (lugar) por meio da interface de rede da Internet, devendo estar antes das regras de permissões e bloqueios, ou a regra não funcionará. Caso isso não seja feito, o *firewall* não realizará o NAT antes de controlar os pacotes.

Figura 21: Adicionando regras de NAT com o IPFW.

```
ipfw 10 add divert natd all from any to any via re0
```

Fonte: Autoria própria.

No IPFW as configurações de NAT são mais complexas que no PF, não basta apenas criar uma regra de direcionamento no *firewall*, é necessário também habilitar o NATD no arquivo **/etc/rc.conf**. No PF é necessário apenas adicionar as regras e reiniciar para que as mudanças dentro do arquivo de regras do *firewall* PF, que nesta monografia se encontra no **/etc/pf.conf**, sejam devidamente aplicadas, como mostram as figuras 22 e 23.

Figura 22: Adicionando regras de NAT com o PF.

```
nat on re0 from 10.5.140.0/24 to any -> re0
nat on re0 from 172.17.140.0/24 to any -> re0
```

Fonte: Autoria própria.

Figura 23: Reiniciando PF para a aplicação das regras.

```
root@PF:~ # pfctl -f /etc/pf.conf
No ALTQ support in kernel
ALTQ related functions disabled
```

Fonte: Autoria própria.

4.2 REGRAS

Para realizar o teste de comparação os dois *firewalls* foram implementados com as mesmas configurações de regras, sendo todas as permissões e bloqueios idênticos, para que a os resultados que levam a conclusão desta monografia fossem os mais corretos possíveis.

Primeiro foram configurados alguns macros, para facilitar a elaboração das regras, por meio dos macros é possível “gravar” uma linha de comando em alguma palavra pequena, para diminuir o tamanho das regras, quando esse recurso é utilizado, é necessário colocar o caracter “$” antes do macro. No caso do comando ipfw add, do *firewall* IPFW que é colocado no início de qualquer regra, pois indica a inclusão de uma regra, foi possível usar o macro e declará-lo como cmd. Além de declarar todas as portas de serviços utilizadas, que são SSH (22), FTP (21), HTTP (80) e HTTPS (443), que são necessárias para os serviços do servidor WEB e por fim o IPERF (5001).

O keep-state é um meio de fazer o *firewall* “lembrar” da requisição, por meio deste recurso é possível criar regras com uma informação menor, exemplo, na regra que libera o *firewall*, caso não houvesse o keep-state, duas linhas seriam necessárias, uma que libera o *firewall* para qualquer endereço e outra que libera qualquer endereço para o *firewall*:

As configurações de macro realizados no IPFW e PF são demonstradas pela figura 24.

Figura 24: Macros.

• Cmd=”ipfw –q add” • Tcp_services=”22,21,80,443,5001” • Ks=”keep-state”	• tcp_services = “{ 22, ftp, 53, http, https, 5001 }” • udp_services = “{ 53 }” • icmp_types = “echoreq”

Fonte: Autoria própria.

A regra de NAT troca um IP por outro IP, neste caso indica a interface re0 que é a interface de rede externa (Internet), para ser aplicado o NAT, ou seja, tudo que sair do *firewall* para a Internet estará com o IP do *firewall* (192.168.0.140), como mostra a figura 25.

Figura 25: Regras de NAT.

• $cmd 00005 divert natd all from any to any via re0	• nat on re0 from 10.5.120.0/24 to any -> re0 • nat on re0 from 172.17.140.0/24 to any -> re0

Fonte: Autoria própria.

O PF como dito anteriormente necessita de uma regra para bloquear todo o tráfego da rede antes das regras de permissão, por motivos de segurança, esta regra é demonstrada na figura 26.

Figura 26: Regra para bloquear tráfego - PF.

IPFW	PF
•	• Block all

Fonte: Autoria própria.

A figura 27 mostra a regra que libera o protocolo ICMP, o qual é o responsável pelo PING, um recurso muito utilizado, pois através do PING podemos verificar se uma máquina está ou não recebendo e enviando os pacotes na rede, assim como mostra Nascimento (2015), “O ICMP é um protocolo integrante do Protocolo IP, definido pela RFC 792, e utilizado para fornecer relatórios de erros ao host que deu origem aos pacotes enviados na rede”.

Figura 27: Regras de ICMP.

• $cmd 00010 allow icmp from any to any	• Pass inet proto icmp icmp-type $icmp_types

Fonte: Autoria própria.

A figura 28 mostra a regra de liberação do *firewall* para tudo. Esta regra é importante, pois sem essa liberação o *firewall* estaria bloqueado.

Portanto mesmo se acrescentasse uma regra permitindo qualquer coisa, a mesma não funcionaria, pois, ao passar pelo *firewall* sem acesso, os pacotes não conseguiriam chegar até a rede externa (internet).

Figura 28: Regras de liberação do firewall.

• $cmd 00015 allow log all from 192.168.0.140 to any out via re0 $ks	• Pass from 192.168.0.140 to any

Fonte: Autoria própria.

A figura 29 mostra a regra de liberação do servidor DNS, para que o mesmo acesse tudo por meio da interface de Internet. Sem essa regra as consultas a este servidor não funcionariam.

Figura 29: DNS.

IPFW	PF
• $cmd 00020 allow log all from 172.17.140.44 to any in via ue0 $ks	• Pass quick from 172.17.140.44 to any

Fonte: Autoria própria.

A figura 30 mostra a liberação de acesso da rede cliente para o servidor DNS, por meio desta regra a rede de clientes consulta o servidor DNS.

Figura 30: Consulta ao servidor DNS.

• $cmd 00030 allow udp from 10.5.140.0/24 to 172.17.140.44 53 in via ue1 $ks	• Pass quick proto udp from 10.5.140.0/24 to 172.17.140.44 port 53

Fonte: Autoria própria.

A figura 31 mostra a liberação de acesso da rede cliente para os serviços HTTP e HTTPS. Por meio desta regra e da regra demostrada na figura 30 a rede cliente pode acessar a WEB.

Figura 31: Acesso Web.

• $cmd 00040 allow log tcp from 10.5.140.0/24 to any 80,443 in via ue1 $ks	• Pass quick proto tcp from 10.5.140.0/24 to any port { 80, 443 }

Fonte: Autoria própria.

A figura 32 mostra a liberação de acesso SSH de uma máquina na rede de servidores para o *firewall*. Por meio desta regra a máquina 172.17.140.4 é capaz de acessar o *firewall* remotamente com o SSH.

Figura 32: SSH.

• $cmd 00050 allow log tcp from 172.17.140.4 to 192.168.0.140 22 in via ue0 $ks	• Pass on ue0 proto tcp from 172.17.140.4 to 192.168.0.140 port 22

Fonte: Autoria própria.

A figura 33 mostra a liberação de acesso da rede cliente para a rede de servidores, serviços: FTP, SSH, HTTP, HTTPS e porta 5001 (IPERF).

Figura 33: Regra de liberação para o acesso da rede servidores.

• $cmd 00060 allow log tcp from 10.5.140.0/24 to 172.17.140.0/24 $tcp_services in via ue1 $ks	• Pass on ue1 proto tcp from 10.5.140.0/24 to 172.17.140.0/24 port $tcp_services • Pass on ue0 proto tcp from 10.5.140.0/24 to 172.17.140.0/24 port $tcp_services

Fonte: Autoria própria.

Por fim a última regra do IPFW, ilustrada pela figura 34, a qual bloqueia todos os pacotes. Como existe a regra 65535 que é oculta no IPFW, e que também bloqueia todos os pacotes, não é necessário o acréscimo desta regra, pois esta foi implementada neste trabalho devido a necessidade do uso dos logs do sistema.

Figura 34: Regra para bloquear tráfego – IPFW.

• $cmd 00999 deny log all from any to any	•

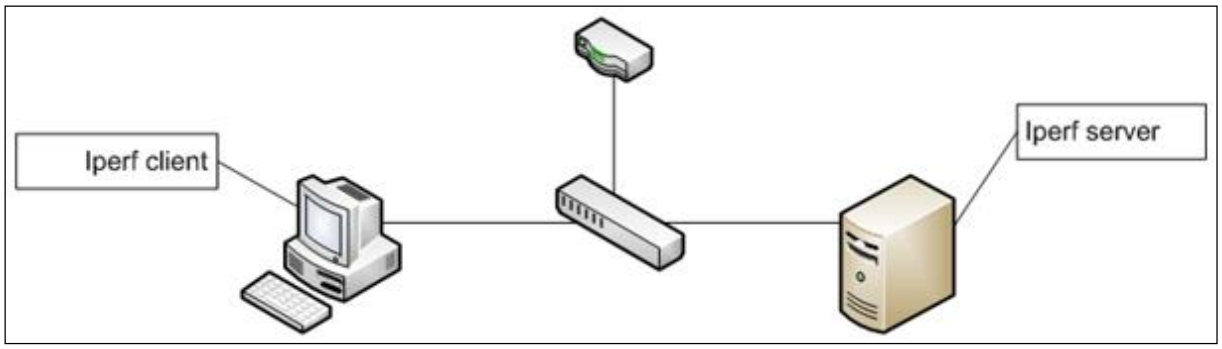
Fonte: Autoria própria.

4.3 IPERF

O IPERF é um software livre, desenvolvido pela National Laboratory for Applied Network Research (NLANR), que permite verificar o desempenho da rede testando a largura da banda. Por isso foram utilizados os testes com essa ferramenta,

sendo estes testes efetuados nos dois *firewalls*, para verificar os respectivos desempenhos, sendo necessário duas máquinas, uma agindo como servidor e a outra como cliente, conforme demonstrado na figura 35.

Figura 35: Conexão IPERF.



Fonte: Adaptado de Pinto (2015).

> Em síntese a operação do Iperf se resume à sua execução entre duas máquinas, uma em modo servidor que ficará "ouvindo" as requisições e outra em modo cliente que ficará responsável por gerar tráfego para estressar a rede e extrair as medidas de desempenho, (BRITO, 2013).

Possui como porta padrão a 5001, por isso a sua liberação na regra de *firewall* demonstrada pela figura 33.

Depois da instalação da ferramenta IPERF, os seguintes comandos para tornar as máquinas em servidor e cliente são necessários:

- Iperf –s
- Iperf –c [IP do sevidor]

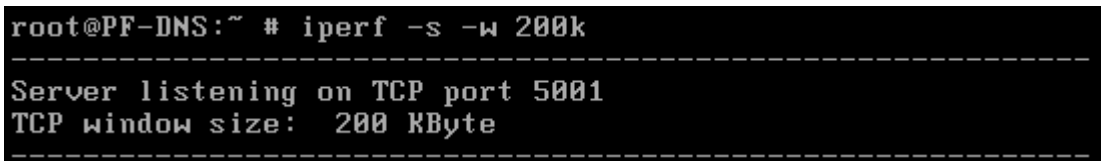
4.4 TESTE DE COMPARAÇÃO COM A FERRAMENTA IPERF

O seguinte teste com IPERF é realizado com a máquina da rede cliente e o servidor DNS, o servidor de DNS com o número de IP 172.17.140.44 foi utilizado como servidor IPERF e a máquina da rede cliente como o cliente IPERF.

No primeiro teste foi utilizando 200 Kilobytes no tamanho do buffer para transmissão, a opção –w que determina este tamanho, (FERRARI, 2007), como mostra a figura 36.

> Um buffer é uma pequena área de memória ultra-rápida usada para melhorar a velocidade de acesso a um determinado dispositivo. É encontrado em HDs, gravadores de CD, modems, e muitos outros. Apesar de serem sinônimos, o termo "buffer" é mais usado em relação aos dispositivos anteriormente citados enquanto o termo "cache" é mais usado com relação aos processadores e memória RAM. (MORIMOTO, 2005).

Figura 36: 1° Teste IPFW - Servidor DNS como servidor IPERF.

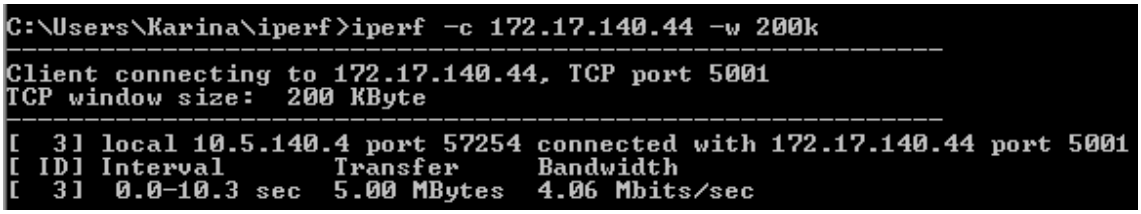


Fonte: Autoria própria.

Ao realizar o comando do iperf nota-se que a máquina permanece “escutando”, esperando pelo comando do cliente para testar o desempenho, como demonstrado pela figura 36.

Com o comando efetuado na máquina cliente, os pacotes são mandados para o servidor, como mostra a figura 37.

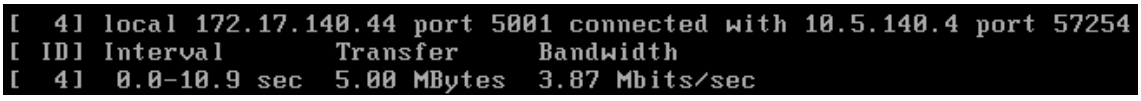
Figura 37: 1° Teste IPFW - Cliente como cliente IPERF.



Fonte: Autoria própria.

O resultado logo aparece na máquina servidor, como mostra a figura 38.

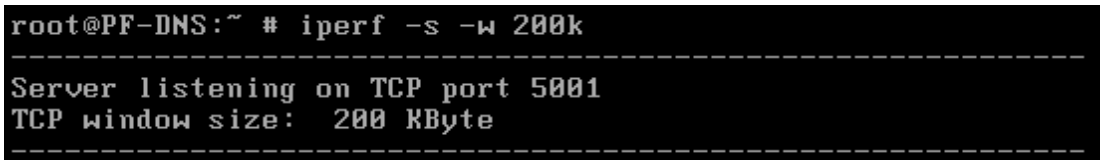
Figura 38: 1° Teste IPFW - Resultado do teste no servidor DNS.



Fonte: Autoria própria.

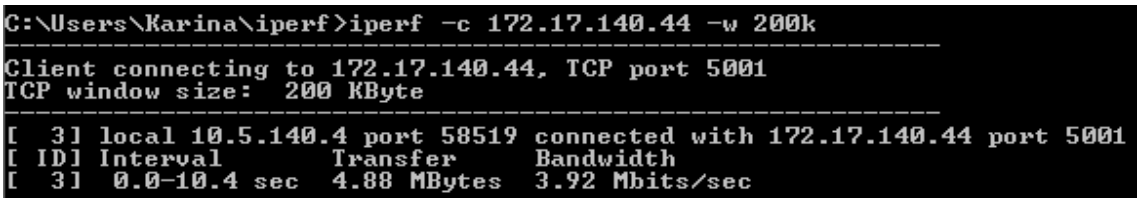
O teste que também foi realizado no PF e mostrado nas figuras 39, 40 e 41, mostram uma diferença mínima em relação aos *firewalls*:

Figura 39: 1° Teste PF - Servidor DNS como servidor IPERF.



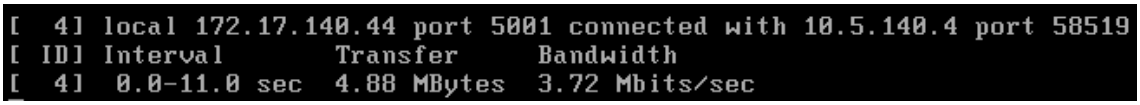
Fonte: Autoria própria.

Figura 40: 1° Teste PF - Cliente como cliente IPERF.



Fonte: Autoria própria.

Figura 41: 1° Teste PF - Resultado do teste no servidor DNS.

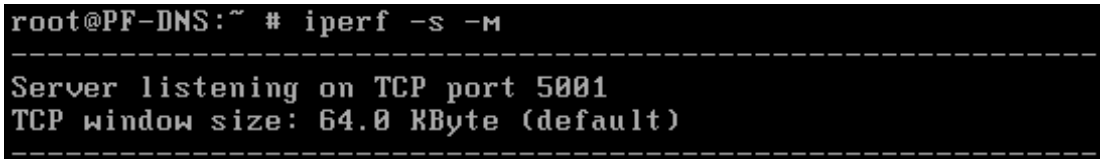


Fonte: Autoria própria.

Para confirmar o resultado acima foi realizado um segundo teste, como mostram as figuras 42, 43 e 44. Dessa vez com o comando –m que, segundo Ferrari (2007).

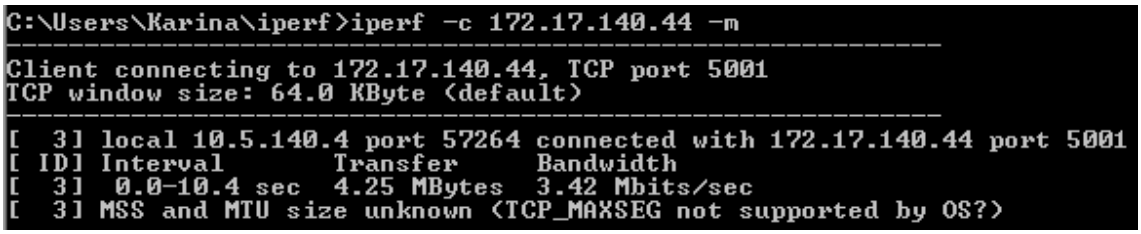
> Teste do MSS (Maximum Segment Size) que representa o tamanho do maior bloco de dados que poderá ser enviado para o destino. Não é negociável, cada host divulga o seu MSS. Default: 536 bytes (20 bytes IP, 20 bytes TCP, para um total de 576 bytes). Ethernet: 1460 bytes (20 bytes IP, 20 bytes TCP, para um total de 1500 bytes).

Figura 42: 2° Teste IPFW - Servidor DNS como servidor IPERF.



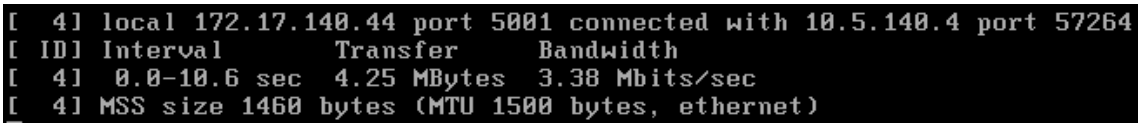
Fonte: Autoria própria.

Figura 43: 2° Teste IPFW - Cliente como cliente IPERF.



Fonte: Autoria própria.

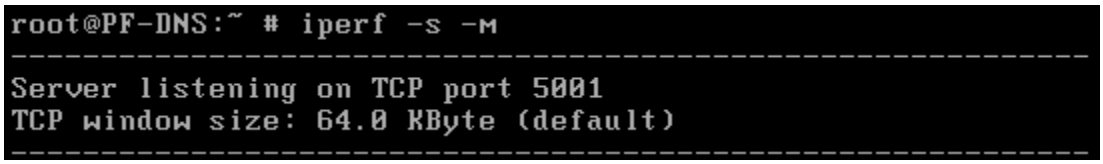
Figura 44: 2° Teste IPFW - Resultado do teste no servidor DNS.



Fonte: Autoria própria.

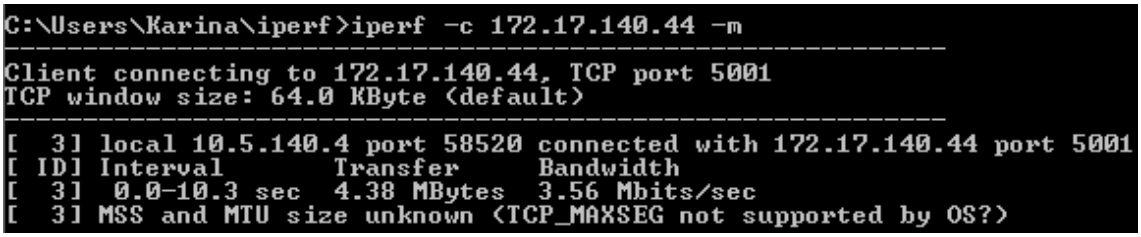
O mesmo teste foi realizado com o PF conforme as figuras 45, 46 e 47.

Figura 45: 2° Teste PF - Servidor DNS como servidor IPERF.



Fonte: Autoria própria.

Figura 46: 2° Teste PF - Cliente como cliente IPERF.



Fonte: Autoria própria.

Figura 47: 2° Teste PF - Resultado do teste no servidor DNS.

Fonte: Autoria própria.

O segundo teste demonstrado pelas figuras 42, 43, 44, 45, 46 e 47, também apresentaram pouca diferença de desempenho entre os *firewalls* IPFW e PF.

5 CONSIDERAÇÕES FINAIS

Este trabalho teve como objetivo analisar dois *firewalls*, com o intuito de avaliar se havia alguma diferença entre os dois, e assim definir qual o melhor *firewall* a ser implementado de acordo com o desempenho de ambos.

É necessário destacar a importância do tripé da segurança da informação e de temas como o fator humano, que são essenciais para se obter uma segurança sólida, e que também devem ser conhecidos pelos profissionais de TI.

Com a realização dos testes para análise e comparação dos *firewalls*, conclui-se que a diferença entre estes é mínima, ocorrendo devido apenas pelo método de criação das regras de permissões e não pelo desempenho dos *firewalls*.

Com a constante utilização de ambos, conclui-se, que o *firewall* PF é mais prático de ser utilizado, pois a implementação de suas regras se dá por meios mais objetivos, em comparação ao *firewall* IPFW que tem uma curva de aprendizado mais complexa. Um exemplo é a regra de NAT, que no PF exige menos linhas de comando no arquivo de regras do que no IPFW, pois no IPFW, além de ter que definir as regras de NAT, ainda é preciso habilitar o NATD para poder funcionar corretamente. No entanto essa configuração foi realizada assim como consta nos materiais de referências, ocorrendo inúmeros erros nas primeiras tentativas. Além desses *firewalls* também foi citado o pfSense que pode servir de alternativa para quem procura um *firewall* mais objetivo e que possibilita uma administração coesa e organizada da rede.

Uma vez que se tem o domínio e tudo se torna mais prático no IPFW, nota-se que o mesmo também é uma ferramenta extraordinária de *firewall* em par com o PF.

REFERÊNCIAS

ALECRIM, E. **O que é firewall?**: conceitos, tipos e arquiteturas. Disponível em: <http://www.infowester.com/firewall.php>. Acesso em: 08 abr. 2015.

ARANHA, C. Resposta a incidentes e plano de continuidade de negócios. Americana: Fatec. 2015. Conteúdo didático.

ARRUDA, F. **Qual a diferença de SSH para FTP?** Disponível em: <http://www.tecmundo.com.br/internet/6627-qual-a-diferenca-de-ssh-para-ftp-.htm>. Acesso em: 20 abr. 2016.

ASSUMPÇÃO, M. **Os 5 princípios básicos de segurança para empresas**. Disponível em: <https://www.vivaolinux.com.br/artigo/Os-5-principios-basicos-de-seguranca-para-empresas>. Acesso em: 29 mar. 2016.

BASTO, F. **Política de Segurança da Informação**: Como fazer? Disponível em: http://analistati.com/politica-de-seguranca-da-informacao-como-fazer/. Acesso em: 20 mai. 2016.

BENETTI, T. **Segurança da informação**: confidencialidade, integridade e disponibilidade (cid). Disponível em: https://www.profissionaisti.com.br/2015/07/seguranca-da-informacao-confidencialidade-integridade-e-disponibilidade-cid/>. Acesso em: 04 mai. 2016.

BITTENCOURT, T. **Saiba o que são spywares, vírus, e outros malwares:** veja como se proteger. Disponível em: <http://www.techtudo.com.br/artigos/noticia/2013/06/entenda-o-que-sao-virus-spywares-trojans-worms-e-saiba-como-se-proteger.html>. Acesso em: 08 mai. 2016.

BORTOLETO, K. **A importância da segurança da informação em gestão de pessoas.** Disponível em: <https://unisalgp.wordpress.com/2015/06/08/a-importancia-da-seguranca-da-informacao-em-gestao-de-pessoas/>. Acesso em: 4 abr. 2016.

BRITO, S.H.B. **Iperf no Monitoramento de Desempenho em Redes.** Disponível em: <http://labcisco.blogspot.com.br/2013/04/iperf-no-monitoramento-de-desempenho-em.html>. Acesso em: 13 fev. 2016.

BUECHLER, C.M; PINGLE, J. **PfSense:** The Definitive Guide. USA: Reed Media Services, 2009. 516p.

FEDEL, G. Tecnologias de redes de computadores. Americana: Fatec. 2013. Conteúdo didático.

FERRARI, S.R. **Análise de desempenho com Iperf.** Disponível em: <https://www.vivaolinux.com.br/dica/Analise-de-desempenho-com-Iperf>. Acesso em: 18 mar. 2016.

FERREIRA, M. **O que é engenharia social?**: 6 dicas para se proteger das armadilhas. Disponível em: <https://www.trustsign.com.br/portal/blog/o-que-e-engenharia-social-6-dicas-para-se-proteger-das-armadilhas/>. Acesso em: 20 jan. 2016.

FREEBSD.ORG. **About Freebsd.** Disponível em: <https://www.freebsd.org/about.html>. Acesso em: 15 jun. 2015.

GALVÃO, I. **Pfsense:** Ajustando regras de firewall, direcionando tráfego nas interfaces WAN. Disponível em: <http://www.ivanildogalvao.com.br/seguranca/pfsense_trafego>. Acesso em: 20 abr. 2016.

HANSTEEN, P. **The book of PF**. 3. ed. USA: No Starch Press, 2014.

INNARELLI, H.C. Diagnóstico e soluções de problemas de tecnologia da informação. Americana: Fatec. 2013. Conteúdo didático.

LUCAS, M.W. **Absolute FreeBSD:** The Complete Guide to FreeBSD. 2. ed. USA: No Starch Press, 2007. 744p.

LUCAS, M; HUBBARD, J. **Absolute BSD:** The Ultimate Guide to FreeBSD. USA: No starch press, 2002. 565p.

MAIA, M.A. **O que é Segurança da informação.** Disponível em: http://segurancadainformacao.modulo.com.br/seguranca-da-informacao>. Acesso em: 04 de mai. 2016.

MANN, I. **Engenharia social**. São Paulo: Blucher, 2011. 236p.

MAZUCO, V. **10 motivos para considerar o pfsense como o gateway da sua rede.** Disponível em: <https://www.escolalinux.com.br/blog/10-motivos-para-considerar-o-pfsense-como-o-gateway-da-sua-rede>. Acesso em: 10 jan. 2016.

MCCARTHY, N. K. **Resposta a Incidentes de Segurança em Computadores**: planos para proteção de informação em risco. Porto Alegre: Bookman, 2014. 209p.

MÉDICE, R. **A importância da segurança da informação**: visão corporativa. Disponível em: <https://www.profissionaisti.com.br/2013/07/a-importancia-da-seguranca-da-informacao-visao-corporativa/>. Acesso em: 13 jan. 2016.

MORAES, A. F. **Firewalls**: segurança no controle de acesso. São Paulo: Érica, 2015. 120p.

MORIMOTO, C. **Buffer.** Disponível em: <http://www.hardware.com.br/termos/buffer>. Acesso em: 21 mai. 2016.

NAKAMURA, E.T. e GEUS, P.L. **Segurança de redes em ambientes cooperativos**. São Paulo: Novatec, 2007. 488p.

NASCIMENTO, M. **Protocolo ICMP, Ping e Traceroute.** Disponível em: <http://www.dltec.com.br/blog/cisco/protocolo-icmp-ping-e-traceroute/>. Acesso em: 26 jan. 2016.

OLIVEIRA, P. Servidor Web: **O que é e como escolher um para seu site!**. Disponível em: <https://www.escolalinux.com.br/blog/servidor-web-o-que-e-e-como-escolher-um-para-seu-site>. Acesso em: 05 jan. 2016.

OPENBSD.ORG. **PF**: the openBSD packet filter. Disponível em: <http://www.openbsd.org/faq/pf/>. Acesso em: 20 abr. 2015.

PINTO, J.B. Segurança em sistemas operacionais e redes de computadores. Americana: Fatec. 2015. Conteúdo didático.

PINTO, P. **Iperf**: é fácil medir a largura de banda em TCP e UDP. Disponível em: <http://pplware.sapo.pt/microsoft/windows/iperf-e-facil-medir-a-largura-de-banda-em-tcp-e-udp/>. Acesso em: 18 mar. 2016.

PINTO, P. **Endereços públicos e privados**. Disponível em: <http://pplware.sapo.pt/truques-dicas/enderecos-publicos-e-privados/>. Acesso em: 10 mai. 2016.

STALLINGS, W. **Criptografia e segurança de redes:** princípios e práticas. 6. Ed. São Paulo: Pearson, 2015. 576p.

VIVAOLINUX. **Usando o PF:** packet filter. Disponível em: <http://www.vivaolinux.com.br/artigo/Usando-o-PF-Packet-Filter?pagina=1>. Acesso em: 5 mai. 2015.