SEGURANÇA EM REDES: REDE DESMILITARIZADA COM *FIREWALL* PFSENSE E AKER

ZOREK, Ricardo[1]
FONTANA, Fabiane S.[2]
ricardozdaniel@live.com

RESUMO

Uma Rede Desmilitarizada (DMZ) é uma estrutura de rede que oferece maior segurança para a organização que à utiliza, nela os servidores ficam estrategicamente situados entre dois ou mais *firewalls.* Este artigo tem como objetivo o desenvolvimento de uma DMZ, que foi estruturada com o intuito de promover o aumento de segurança de um ambiente de rede empresarial, já considerado seguro. O estudo foi realizado em um ambiente de teste construído com *hardwares* físicos, utilizando dois *firewalls* (PFSense e Aker) e servidores para simulação do mesmo. O protótipo foi desenvolvido no ambiente empresarial do Grupo Mascarello, sendo esta uma empresa de grande porte, possuindo diversos serviços que exigem o máximo de segurança possível, uma vez que, suas informações são a chave do negócio e o roubo das mesmas poderiam comprometer a linha de produção. Ao fim da estruturação da rede, concluiu-se que, com a utilização da DMZ, vários aspectos de segurança seriam reforçados dentro da rede, visto que um *firewall* apoiaria o outro através das configurações de suas regras, uma invasão neste ambiente seria praticamente descartada com a utilização destes filtros duplos de segurança.

PALAVRAS-CHAVE: *Firewall*, Rede Desmilitarizada, Segurança.

1 INTRODUÇÃO

A área de Tecnologia de Informação (TI) está presente na maioria das empresas do mundo, seja de pequeno porte, em um equipamento isolado ou em uma rede local - *Local Area Network* (LAN) com dois computadores ou em empresas de grande porte, como exemplo de multinacionais com mais de mil dispositivos conectados à rede. Consequentemente, a área de segurança em redes se torna cada vez mais importante e exigente. Tanenbaum (2002) define

[1] Discente do curso de Sistemas de Informação no Centro Universitário Assis Gurgacz.
[2] Mestra em Engenharia Agrícola pela Universidade Estadual do Paraná, Bacharel em Ciência da Computação pela Faculdade de Ciências Aplicadas de Cascavel, Docente do Curso de Sistemas de Informação no Centro Universitário Assis Gurgacz.

segurança em redes de uma forma simples, como recursos que visam garantir que indivíduos ou grupos mal-intencionados não tenham acesso à dados, documentos e informações privadas.

Existem diversas ameaças provenientes da rede mundial de comunicação, como os conhecidos vírus, *Trojan Horse, Backdoors*, *Conficker*, *Sality*, entre outros, os quais agridem de alguma maneira a integridade de um computador ou de uma rede de computadores (REITER, 2008).

Para que as ameaças existentes sejam minimizadas, Reiter (2008) fala sobre os dispositivos de segurança que foram criados, dentre eles, destaca-se o *firewall*, dispositivo que, quando associado à rede local, cria uma barreira entre a rede interna e externa, com o objetivo de evitar ataques. Esse dispositivo é responsável pela segurança de um perímetro, impedindo conexões indesejadas, filtrando-as e permitindo apenas as desejadas (ALECRIM, 2013).

Contudo, o *firewall* não é o único sistema/dispositivo de segurança que uma LAN pode ter, existem vários outros dispositivos, que através do trabalho em conjunto passam a oferecer um ambiente seguro e estável, evitando a ocorrência de possíveis incidentes (REITER, 2008). Um componente de segurança que pode ser utilizado em conjunto com o *firewall* é a de perímetro, conhecido como zona desmilitarizada, em inglês, *Demilitarized Zone* (DMZ). Essa rede fica situada entre a rede local e a internet, ou seja, entre a rede confiável e a não confiável, sua função principal é manter todos os serviços que sejam necessários ao acesso externo, fora da rede local, limitando o risco de invasores. (REITER,2008).

Considerando o cenário atual de segurança de redes em ambientes corporativos, a necessidade deste estudo se justifica pelos prejuízos que as ameaças trazem para tal ambiente, no qual a implantação de ferramentas de segurança tem por finalidade aumentar a segurança e garantir a proteção de dados arquivos e projetos, assim dificultar a invasão de *hackers* na rede, diminuindo os danos causados nas empresas. Desse modo, o objetivo desse artigo é relatar o desenvolvimento de uma DMZ aplicada com intuito de promover o aumento da segurança do ambiente de uma rede empresarial, por meio da implantação da mesma, onde foram transferidos os servidores públicos, garantindo, assim, uma maior segurança para o ambiente da rede local.

O artigo está dividido em cinco seções: A primeira parte, compreende a apresentação e introdução do tema; em seguida, na revisão bibliográfica, onde é feita a descrição sobre o tema de segurança de informação, *firewall* e DMZ; na terceira seção, encontra-se a metodologia aplicada no estudo; na quarta os resultados e discussões, bem como, uma demonstração do ambiente de teste e aplicação do trabalho. Na quinta, as considerações finais serão apresentadas.

2 REVISÃO BIBLIOGRÁFICA

As redes de computadores e os sistemas de gerenciamento se tornaram cada vez mais essenciais no mundo empresarial, à medida que as empresas crescem, sua estrutura de redes também fica maior, tornando complexa a administração da grande estrutura de servidores, serviços e usuários, contudo, a disponibilidade e a segurança da rede se tornou indispensável em uma corporação (Kouch, 2008). Nessa seção, serão abordados assuntos relacionados a redes de computadores, origem e seus conceitos.

2.1 REDE DE COMPUTADORES: ORIGEM E CONCEITOS

As redes locais são conjuntos de sistemas de computadores e outros aparelhos de *hardware*, que estão interligados através de rede de cabos ou rede sem fio, com o intuito de compartilhar recursos e dados entre pessoas (MAYA,2016). As redes de computadores são circuitos necessários para conectar todos os equipamentos entre diferentes lugares, como conectores, *switches*, *patch panels*, cabos ou dispositivos sem fios, esses recursos são responsáveis pelo desempenho e por parte da segurança de um ambiente de TI (SERCOMPE, 2016).

Para Forouzan (2009), uma LAN é um sistema de comunicação de dados que permite a ligação direta entre vários dispositivos independentes, em uma área geográfica limitada, como um departamento, um edifício ou um campus universitário. Uma empresa grande precisa de vários equipamentos interligados para formar uma rede LAN. De acordo com Forouzan (2009), as redes e sistemas de comunicação de dados, São tecnologias com mais rápido crescimento. Consequentemente, ocorreu um aumento surpreendente no número de profissões em que se utiliza a tecnologia. Nesse sentido, garantir a funcionalidade de uma rede de infraestrutura, se torna essencial para o êxito na carreira de um bom profissional de TI, o que também promove o crescimento das empresas.

A infraestrutura de rede, nas redes corporativas, é um ambiente encarregado por conectar e sustentar todos os equipamentos de tecnologia da empresa em que está instalada, desde os computadores e servidores até mesmo as máquinas de produção, permitindo que interligue toda a empresa e que os colaboradores tenham acesso ao sistema e recursos de TI (Sercompe, 2016). Outro ponto fundamental, para o desempenho satisfatório em uma rede de computadores, é a segurança de rede.

2.2 SEGURANÇA DE REDE

O termo segurança de rede de acordo com Sousa (2013) significa o conjunto de processos em dispositivos de medidas que buscam precauções, assim, asseguram o sucesso de um empreendimento, do funcionamento preciso de um objeto, do cumprimento de alguns planos, entre outros. O processo de segurança de rede é uma combinação de múltiplas camadas de defesa a fim de proteger o uso e integridade das conexões e dos dados. Tradicionalmente integra a tecnologia de *hardware* e *software*, gerenciando, assim, os acessos e buscando impedir que ameaças entrem na rede, e que a empresa seja afetada com a perca de dados ou serviço inoperante.

A definição de segurança para Lawrie (2014) é separada em três objetivos fundamentais: O primeiro, a confidencialidade de dados: Garante que dados privados e confidencias não fique acessível a indivíduos que não são autorizados e garanta que os responsáveis controlem ou influencie quaisquer informações sobre o que pode ser coletado e armazenado. O segundo, a integridade: garante que dados sejam modificados somente da maneira especificada e autorizada, e que, os sistemas desempenhem suas funções predefinidas, sem modificações indesejadas. O terceiro, a disponibilidade: garante que o sistema de rede funcione prontamente, e que não ocorra indisponibilidade ao usuário autorizado.

Dada a compreensão do que é a segurança de rede, passamos a falar sobre as políticas de segurança, que se fazem necessárias em uma empresa, como o intuito de promover o controle e a segurança da infraestrutura e seus dados.

2.3 POLÍTICA DE SEGURANÇA

Para Moreira (2017), uma empresa que se baseia em meios digitais para fazer o seu trabalho, precisa lidar com o crescimento da estrutura de TI para que essas ações tenham êxito, o componente que deve ser priorizado é a segurança, com o objetivo de evitar problemas como a perca de dados, para tanto, é necessário que se tenha uma política de segurança planejada e cumprida por todos os responsáveis. A política de segurança, geralmente são documentos que estabelecem regras, valores, comprometimento, requisitos e responsabilidades sobre o que deve ser feito para alcançar o padrão desejado de proteção das informações e dados, sendo basicamente um manual de procedimentos, que reproduz, como os recursos de TI de determinada empresa devem ser utilizados, e protegidos. (DANTAS, 2011).

Após exposto o conceito e a importância das políticas de segurança, o próximo tópico abordará as vulnerabilidades existentes, as possíveis ameaças em redes de computadores e algumas contramedidas que podem ser aplicadas.

2.4 VULNERABILIDADE DE REDE: AMEAÇAS, ATAQUES E CONTRAMEDIDAS

De acordo com Reis (2015), é possível que todas as empresas do mundo sofram com milhares de vulnerabilidades, que podem ser exploradas por *hackers*, embora pareça ser algo assustador para usuários, para um profissional de TI é a realidade do seu dia a dia de trabalho. Nenhuma empresa está imune as vulnerabilidades da segurança na área de TI, independente do quanto seja investido em ferramentas para impedir ataques, ainda existe possibilidade de algum serviço ou usuário dessa rede, desconsidere ou deprecie, as normas de proteções estabelecidas, abrindo brechas no sistema de segurança.

Uma ameaça de rede para Teixeira (2015), é quando qualquer equipamento, *software* ou processo, que afete o funcionamento das operações, a disponibilidade e integridade da rede ou sistema, pode estar sujeito a um ataque. Ataque de rede, é qualquer modo específico usado para explorar uma vulnerabilidade de rede. Os ataques mais comuns nas redes de corporações ocorrem por parte de *hackers*, que utilizam ferramentas e *softwares* não desejáveis para auxiliar nos seus planos de ataques, que são chamados de *malware*, alguns exemplos são: vírus, *worms, trojans, phishing, spam, rootkits*, *sniffers*, entre outros. (REITER, 2008).

Para evitar tais ataques, a equipe de TI deve realizar contramedidas, ou seja, ações de proteção tomadas antes que ocorra qualquer invasão ou ataque, , isso para quem quer se defender, e assim fechando ou compensado alguma vulnerabilidade no sistema de redes da empresa. (TEIXEIRA, 2015).

2.4.1 *Firewall*

Para Naves (2010), um *firewall* na tradução do inglês, “muro de fogo” ou “porta corta fogo”, é uma barreira para evitar a propagação de incêndios. Essa é a descrição metafórica do recurso primordial em uma rede empresarial, nenhum administrador de redes pode deixar seus servidores, computadores e usuários sem esse recurso de segurança. O uso do *firewall* está ligado ao tamanho da infraestrutura de rede, buscando controlar os dados de entrada e saída de

uma empresa, dando assim, uma segurança maior para a rede local, dificultando a exploração de vulnerabilidade na rede por indivíduos ou grupos mal-intencionados. (SOUZA, 2014).

O trabalho de um *firewall* pode ser realizado de várias maneiras, o que define a metodologia que vai ser utilizada são os fatores de necessidade da empresa e os critérios do administrador, é por esse motivo que podemos encontrar mais de um tipo de *firewall* como por exemplo:

- Filtro de pacote: Sistema de filtragem de pacotes que roteiam os pacotes entre máquinas internas e externas de forma seletiva.

Proxy: São programas de aplicações que recebem de clientes, requisições da internet, analisando e redirecionado estas requisições, caso aceitas, são enviadas para os servidores de intersnet que irão prover os serviços solicitados.

- Internos: São *firewalls* dentro da própria rede local, que separa e protege determinados computadores ou servidores.
- Híbridos: é a mistura das funcionalidades dos *firewalls* citados acimas, que garante proteção aos serviços que existem alto grau de segurança. (HELPDIGITAL, 2017).

2.4.2 Arquitetura de *firewall*

Existem diferentes modelos de arquitetura de *firewall*, listamos a seguir alguns modelos de arquiteturas clássicas:

- *Dual-homed host architecture:* Este modelo de arquitetura é (mais comum) formada por um equipamento que tem duas interfaces de rede e funciona como um separador entre as duas redes, assim, tudo que entra ou sai, tende obrigatoriamente a passar pelo *firewall.* (NAKAMURA, 2007).
- *Screened host architecture:* Essa arquitetura é formada por um filtro de pacotes e um *bastion host*. O filtro deve ter regras que permitam o tráfego para a rede interna somente por meio do *bastion host,* de modo que os usuários externos que queiram acessar um sistema da rede interna devem, primeiramente, se conectar ao *bastion host* (PROSDOCIMO, 2014).
- *Screened subnet architecture:* Essa arquitetura aumenta o nível de segurança com relação à arquitetura *screened host* ao adicionar a rede DMZ. Se antes um ataque de rede significava que o invasor já estaria com a rede interna disponível

> para ele, isso não ocorre na arquitetura *screened subnet*, onde a DMZ, que é uma zona de confinamento entre a rede externa e a rede interna, fica entre dois filtros. A DMZ evita que um ataque ao *bastion host* ou outro servidor resulte, por exemplo, na utilização de um *sniffer* para a captura de pacotes de usuários internos (NAKAMURA, 2007).

2.4.3 Aker

O Aker é um *firewall* brasileiro, desenvolvido na cidade de Brasília em 1997, por uma equipe especializada na parte de segurança. Desenvolvido pela Aker *Security Solutions*, especializada em desenvolvimento de soluções para segurança da informação, é a primeira empresa nacional a disponibilizar produtos e serviços para a proteção dos dados. Os produtos são utilizados em todo território brasileiro, como também no exterior. A empresa oferece produtos como: *firewall, antispam*, VPN *(virtual private network*), filtro de conteúdo e monitoramento remoto (BASSO, 2015).

Este *firewall* é comercializado em duas modalidades, a primeira em *software* no qual o cliente tem o *hardware* no qual será instalado o *firewall*, e a segunda é o *appliance*, que é um *hardware* projetado para rodar o Aker. Seus produtos são vendidos por meio de revendas cadastradas e qualificadas. Atualmente, a empresa possui mais de cem parceiros distribuídos por todo Brasil, com atendimento de clientes com portes variados, em diversos segmentos das esferas públicas e privadas. (BASSO, 2015).

O *firewall* roda sobre o sistema operacional Fedora, que é um sistema operacional gratuito, de fácil acesso, e com suas versões disponível para o *download* na internet. No entanto, o Aker é um *software* que funciona através de licença, sendo necessário a sua aquisição para o uso. (AKER, 2015).

2.4.4 PFSense

O projeto PFSense foi criado na metade de setembro de 2004 por Chris Buechler e Scott Ullrich. Chris contribuiu com códigos de forma assídua e dedicada por muito tempo com o projeto *M0n0wall* que era um projeto que visava criar um pacote de software firewall, que quando utilizado juntamente com um PC forneça todas as características de um Firewall

embutido. Contudo, o PFSense possui um diferencial, seu foco desde o princípio foi a funcionalidade em qualquer dispositivo que seja possível a instalação de um sistema operacional, diferente do projeto M0n0wall, que é focado somente em *appliances*. (DRAKE, 2018).

PFSense é um *software* livre que é ajustado para funcionar como um *firewall*. Heinzelmann (2016) aponta que ele foi customizado para trabalhar sobre o sistema operacional FreeBSD e pode ser completamente gerenciado por uma interface gráfica web, como também por linha de comando, tanto local, como por *Secure Shell* (SSH).

A finalidade do PFSense, para Heinzelmann (2016) vai muito além de um *firewall* comum, podendo trabalhar com *Virtual Private Network* (VPN), servidor *proxy*, autenticação de usuário, Servidor *Domain Name System* (DNS), Servidor *Dynamic Host Configuration Protocol* (DHCP) e o Sistema de Detecção de Intruso (IDS), entre outras funcionalidades.

Para Williamson (2011), o PFSense é um sistema operacional que foi baseado em FreeBSD que se originou do Unix, trazendo, assim, uma compilação que carrega vários serviços consigo, alguns exemplos são: *firewall*, *proxy*, controle de acesso de usuário entre outras funcionalidades. O uso do PFSense facilita o gerenciamento e aumenta a segurança de rede, a qual ele integra.

No próximo tópico será apresentado a conceituação de uma DMZ, onde será apresentado sua forma de estruturação e funcionamento.

2.7 ZONA DESMILITARIZADA (DMZ)

Para Mauser (2015), a DMZ ou zona desmilitarizada, é uma forma clássica de segmento, com objetivo de maior segurança em uma rede empresarial. Esta área pode ser definida como física ou lógica, e pode conter componentes de redes, normalmente são utilizados servidores que precisam ser acessados externamente, como servidor web, e-mail e FTP (*file transfer protocol*).

Pinheiro (2004) afirma que uma área desmilitarizada corresponde ao segmento de uma rede parcialmente protegida, que está localizada entre a rede interna da empresa, e a rede externa (internet), nela estará localizada todos os serviços de acesso público da empresa, onde se localiza a zona com mais acessos e maiores riscos.

A DMZ possui um papel essencial na arquitetura, pois permite que serviços sejam providos para os usuários externos, ao mesmo tempo em que protegem a rede interna dos

acessos externos. Essa proteção da rede interna é feita pelo confinamento dos acessos externos nessa rede desmilitarizada, de modo que se um servidor da DMZ for atacado, o atacante não tem condições de chegar aos recursos internos (NAKAMURA, 2007).

De acordo com Pinheiros (2004), as redes DMZ, são sub-redes que hospedam servidores cujo o acesso à internet é necessário, a lógica de separar este servidores se deve ao fato que se houver uma invasão será por meio de tais servidores, e com isso o acesso a rede interna pelos invasores ou vírus será dificultado já que este se encontra em outra rede.

A seguir será descrita a metodologia utilizada nesse artigo, a caracterização geral do método e os procedimentos metodológicos.

3 METODOLOGIA

O presente estudo foi realizado nas empresas do Grupo Mascarello, onde foi montado um ambiente de teste para realizar a avaliação de uma zona DMZ, a rede possui dois *firewalls* de teste: Aker e PFSense, contando com um switch entre os dois *firewall* e servidores de teste.

O PFSense foi o *firewall* escolhido por possuir grande popularidade, além de possuir uma base de dados bibliográfica e documental disponível na internet, o que facilita o estudo aprofundado e oferece grande apoio em relação aos processos como instalação, configuração e resolução de problemas. Já o Aker foi selecionado por ser o único *firewall*, já utilizado na empresa.

A DMZ foi escolhida, considerando a grande quantidade de ataques e roubos de informações ocorridos em empresas. Com a sua implantação, a estrutura pode aumentar a segurança e agregar uma solução necessária contra a invasão de uma rede empresarial.

3.1 CARACTERIZAÇÃO GERAL DO MÉTODO

O método utilizado para o desenvolvimento desta pesquisa foi o estudo de caso, que tem como objetivo principal aumentar a segurança da rede de computadores no Grupo Mascarello.

Para Yin (2005), o estudo de caso é uma investigação empírica e bibliográfica, um método que atinge técnica de coleta de dados, planejamento e análise dos mesmos. As informações geradas a partir de um estudo de caso não são similares à os resultados obtidos a

partir de outros tipos de pesquisas, estudo de caso, contém informações muito mais detalhadas e concretas gerando um resultado próximo ao ideal.

A pesquisa é exploratória em busca de ferramentas, que poderiam ser encaixadas no ambiente da empresa. Taupp (2003) destaca que esse tipo de pesquisa é desenvolvida para se ter uma visão geral, como no caso deste trabalho, que teve como propósito conhecer as ferramentas por completo. Como cada ambiente tem particularidades, então há necessidade de fazer um estudo sobre tais ferramentas neste local. Para Vergara (2000), as pesquisas exploratórias são realizadas em áreas que existem poucas informações.

A pesquisa é do tipo qualitativa em relação aos resultados, de acordo com Taupp (2003) as pesquisas qualitativas trazem uma análise mais profundas sobre o que está sendo estudado, tendo detalhes para todos os resultados. No próximo tópico serão citadas as metodologias usadas para criação e implementação do ambiente.

3.2 PROCEDIMENTOS METODOLÓGICOS

Para o desenvolvimento desse projeto foi criado um ambiente de teste que é composto por equipamentos físicos e *racks* de rede, sendo: dois *firewalls* (PFSense e Aker), um servidor Apache Linux, um *switch* e um roteador (*wireless Fidelity*) WIFI.

Foram utilizados *firewalls* do tipo interno e arquitetura *screened subnet architecture.* Neste contexto, foram realizados testes de funcionalidades de uma DMZ, focando em aumentar a segurança de uma rede já existente no Grupo Mascarello, movendo servidores que oferecem acessos externos para essa rede. Na sequência foram feitos testes, e coleta de informações das melhorias da segurança e da estrutura, visando uma possível implantação de forma definitiva, com autorização da diretoria e responsável pela área de TI da empresa.

Na sequência serão apresentados e discutidos os resultados obtidos com o estudo realizado.

4 APRESENTAÇÃO E DISCUSSÃO DOS RESULTADOS

O estudo em questão foi realizado através da implantação da uma zona desmilitarizada na empresa Grupo Mascarello, onde foram utilizados dois *firewalls*: PFSense como defesa de

frente e o Aker como defesa de rede local. Adiante serão expostos os componentes e configurações usadas para criação do ambiente.

4.1 COMPONENTES UTILIZADOS

Todos os componentes deste experimento físico são interligados através de cabos de rede e *switch*. Foi utilizada banda larga da operadora Vivo, onde foi inserido um *Internet Protocol* (IP) fixo dedicado somente para o ambiente de teste.

Para composição da rede foram utilizados os seguintes *hardwares*:

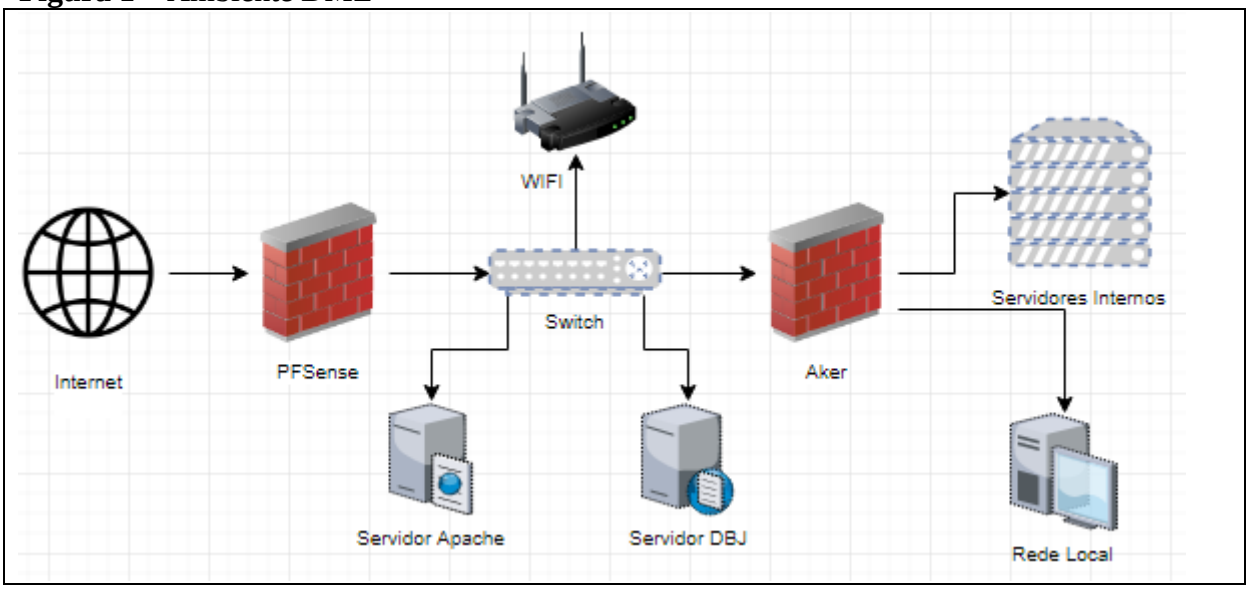
- A instalação do *firewall* PFSense foi realizada em uma máquina de configurações: processador I686 c7 1500 MHZ, memória DDR 2 de 512 MB;
- Um s*witch* Edge-cor modelo ECS2000 com 26 portas, sendo 24 de cabo de rede RJ45 e duas de fibras mini GBIC;
- Um servidor DBJ foi estruturado em uma máquina de configurações: Processador Pentium 4 1800 MHZ, memoria DIMM de 128 MB;
- Um servidor Apache foi estruturado em uma máquina de configurações: Processador I686 c7 1500 MHZ, memória DDR 2 de 512 MB;
- Um *access point* Linksys model WRT54G;
- Um *firewall* Aker *firewall enterprise box* modelo 837 *appliances;*
- Cinco *patch cords*, categoria 6 Furukawa.

A seguir serão descritas as configurações da rede e de como foi montando o ambiente.

4.2 CONFIGURAÇÃO DE REDE

A Figura 1 apresenta o ambiente de teste da forma como o mesmo foi estruturado e planejado para o experimento.

Figura 1 – Ambiente DMZ



Fonte: Elaborado pelo autor (2018)

Especificações da rede:

- **INTERNET VIVO:** *Link* Valido.
- **PFSENSE:**
  - **WAN:**177.204.154.12
  - **LAN:** 192.168.100.1
  - ***LINK* EXTERNO:** *Link* Valido.
- **SWITCH:** 192.168.100.248
- **WIFI DMZ:** 192.168.100.249
- **APACHE**
  - **LAN:** 192.168.100.250
  - ***LINK* EXTERNO:** *Link* Valido.
- **DBJ**
  - **LAN:** 192.168.100.247
  - ***LINK* EXTERNO:** *Link* Valido.
- **AKER**
  - **WAN:** 192.168.100.251
  - **LAN:** 192.168.0.254

No tópico a seguir serão expostas às regras implantadas e provenientes dos dois *firewalls* utilizados para criação do ambiente DMZ.

4.3 REGRAS FORMULADAS NO PFSENSE

O PFSense foi instalado e configurado especialmente para esse ambiente, buscando uma maior segurança para ambiente novo da DMZ, onde cada regra foi escrita para atender todos os servidores presente.

No que diz respeito às regras junto ao *firewall*, este experimento foi configurado na porta *ethernet* DMZ (Figura 2), conforme segue:

1ª regra: A primeira regra é para o *firewall* PFSense sendo um padrão que permite o acesso através do SSH para configuração em modo texto, ou através da porta 80, que permite a configuração via *browser*.

2ª regra: A segunda regra é para o *firewall* Aker, liberando para saída (nada entra a não ser que uma resposta foi solicitada) na internet tudo que vem dele, sendo um dispositivo confiável que já possui suas próprias regras.

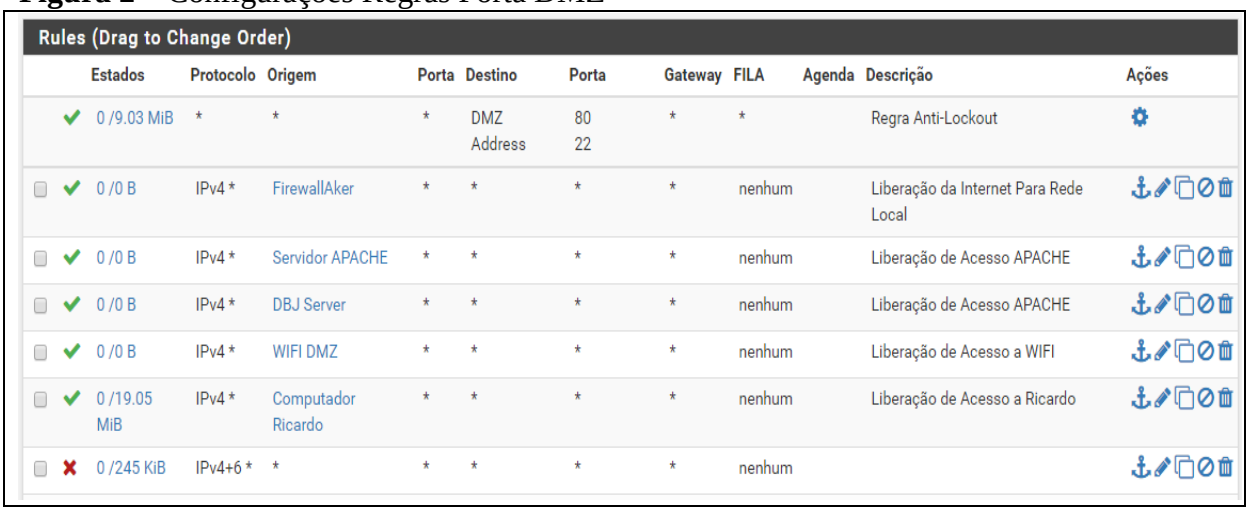
3ª e 4ª regras: A terceira e quarta regras são as liberações para internet dos servidores Apache e DBJ.

5ª regra: A quinta regra é para WIFI e o roteador é criada uma *Virtual Local Area Network* (VLAN) diferente da DMZ, e tudo que estiver conectado à ela pode enviar informações para internet, essa regra, é utilizada para visitantes, representantes que queiram acesso à internet, através de notebook ou celular, para acessos temporário, não tendo como intenção o acesso a rede local da empresa.

6ª regra: A Sexta regra é utilizada pelo computador que está fazendo as configurações para saída da internet.

7ª regra: A sétima regra bloqueia tudo o que não foi tratado nas regras anteriores.

Figura 2 – Configurações Regras Porta DMZ



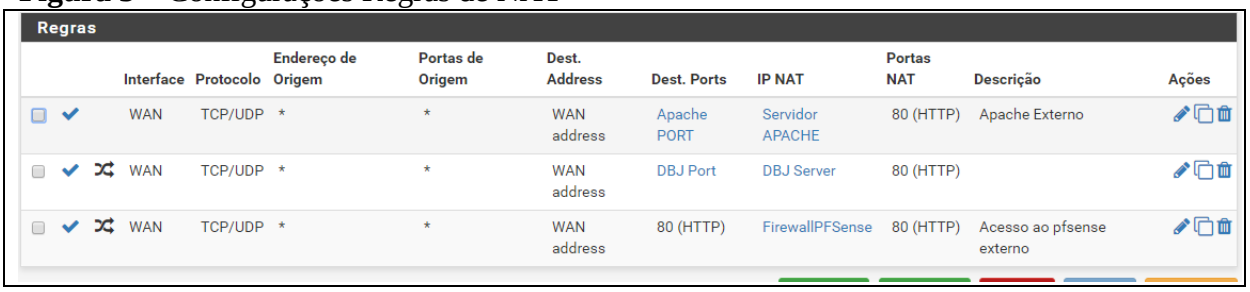
Rules (Drag to Change Order)

	Estados	Protocolo	Origem	Porta	Destino	Porta	Gateway	FILA	Agenda	Descrição	Ações
✓	0 /9.03 MiB	*	*	*	DMZ Address	80 22	*	*		Regra Anti-Lockout	⚙
✓	0 /0 B	IPv4 *	FirewallAker	*	*	*	*	nenhum		Liberação da Internet Para Rede Local	⚓✎⧉⊘🗑
✓	0 /0 B	IPv4 *	Servidor APACHE	*	*	*	*	nenhum		Liberação de Acesso APACHE	⚓✎⧉⊘🗑
✓	0 /0 B	IPv4 *	DBJ Server	*	*	*	*	nenhum		Liberação de Acesso APACHE	⚓✎⧉⊘🗑
✓	0 /0 B	IPv4 *	WIFI DMZ	*	*	*	*	nenhum		Liberação de Acesso a WIFI	⚓✎⧉⊘🗑
✓	0 /19.05 MiB	IPv4 *	Computador Ricardo	*	*	*	*	nenhum		Liberação de Acesso a Ricardo	⚓✎⧉⊘🗑
✗	0 /245 KiB	IPv4+6 *	*	*	*	*	*	nenhum			⚓✎⧉⊘🗑

Fonte: Elaborado pelo autor (2018)

A Figura 3 demostra as regras de *Network Address Translation* (NAT), onde são realizados os redirecionamentos das portas que são acessadas externamente para a porta 80. Quando o *link* direto é acessado externamente, o mesmo é redirecionado a porta 80, que vai para o PFSense, quando é utilizada a porta 8085, no final do link o mesmo é redirecionado para a porta 80 do servidor DBJ, e quando é inserido a porta 8086, o *link* é redirecionado a porta 80 do servidor Apache.

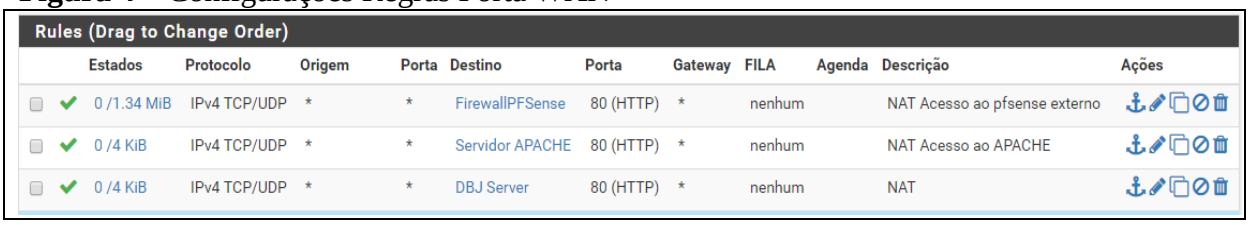
Figura 3 – Configurações Regras de NAT



Fonte: Elaborado pelo autor (2018)

As regras presentes na Figura 4, são configuradas na porta *ethernet* WAN, que controlam os acessos que chegam da internet para os *links* destinados. As regras mencionadas liberam os servidores e o *firewall* PFSense para acesso externo na porta 80.

Figura 4 – Configurações Regras Porta WAN

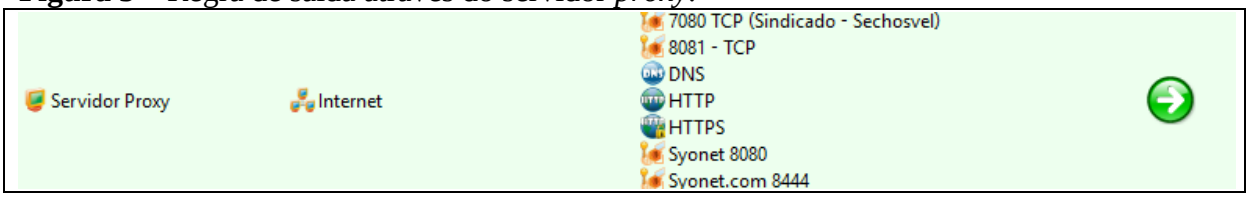


Fonte: Elaborado pelo autor (2018)

4.4 AKER

O *Firewall* Aker já está presente no ambiente de rede da empresa, portanto as configurações padrões continuaram normais. Como a empresa tem uma proteção a mais, que é realizada pelo servidor *proxy*, foi necessário que a rede local passasse pelos filtros deste dispositivo antes de sair da mesma, na Figura 5 é apresentada a liberação inserida para o servidor *proxy*, que após realizar filtragens pré-definidas na rede, tenha acesso as portas padrões e algumas específicas utilizadas na empresa.

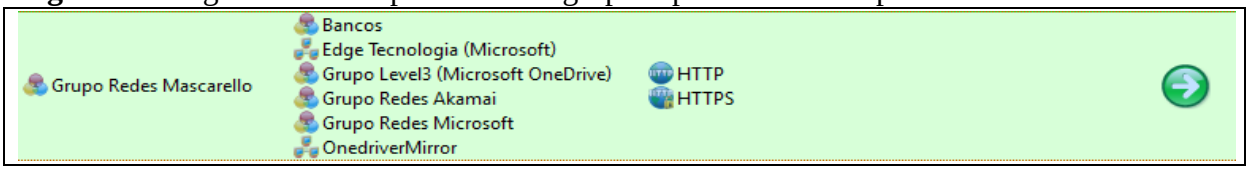
Figura 5 – Regra de saída através do servidor *proxy*.



Fonte: Elaborado pelo autor (2018)

Como a empresa utiliza alguns *softwares* obrigatórios por bancos ou governo, onde alguns não são compatíveis com *proxy* utilizado, foi necessário fazer algumas liberações especificas para o grupo de computadores que realizarão o acesso junto aos mesmos, como é mostrado na Figura 6.

Figura 6 – Regra de saída específica com grupo específico de computadores.



Fonte: Elaborado pelo autor (2018)

A regra apresentada na Figura 7 é a que realiza o bloqueio total das conexões que não se encaixam nas regras apresentadas anteriormente, ou seja, não conseguem sair ou entrar no *firewall*.

Figura 7 – Regra de bloqueio total

Fonte: Elaborado pelo autor (2018)

A regra mostrada na Figura 8, que se encontra desativada no ambiente DMZ, demonstra que anteriormente havia esta regra liberando acesso externo ao servidor DBJ, em nosso ambiente de estudo essa regra não se faz necessária, visto que o servidor foi movido para o ambiente DMZ.

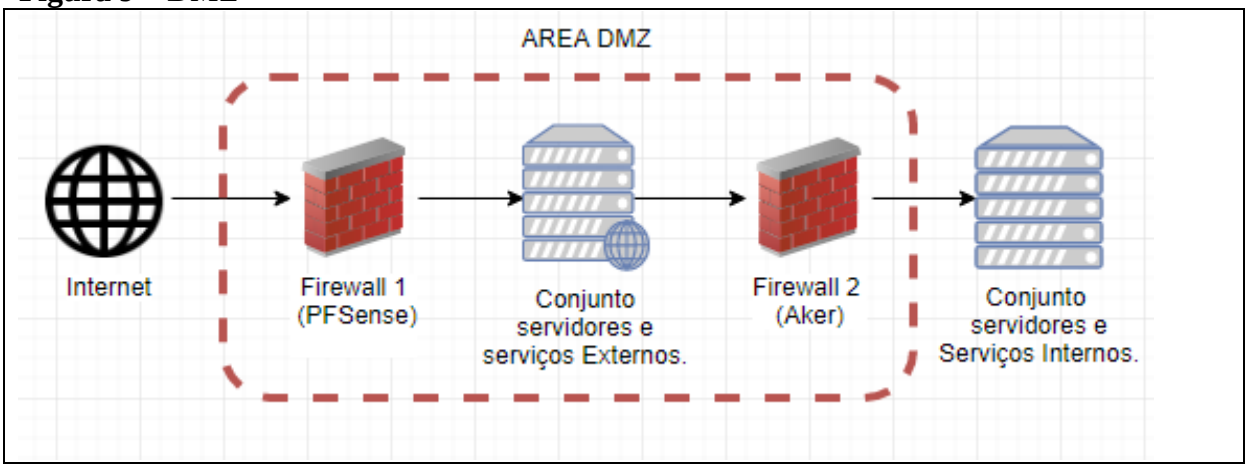
Figura 8 – Regra do antigo ambiente desativada.

Fonte: Elaborado pelo autor (2018)

4.5 ZONA DESMILITARIZADA

A DMZ (Figura 9) é composta por dois *firewalls* e seus servidores que ficam entre eles. O primeiro *firewall* fica responsável por toda a DMZ, sendo configurado nele as regras que permitem os acessos externos, mantendo a segurança dessa zona. Esses *firewalls* foram dispostos desta forma pelo fato de os servidores possuírem acesso interno e externo. Na estrutura antiga, a disposição do único *firewall* tornava toda a rede vulnerável, agora, caso seja realizado algum ataque ou invasão, o indivíduo ficara entre os dois *firewalls*, dificultando, assim, o acesso à rede local. O segundo *firewall* não permite a entrada de dados, apenas deixa com que a rede local envie dados para internet, caso, se enquadre nas regras que foram configuradas.

Figura 9 – DMZ

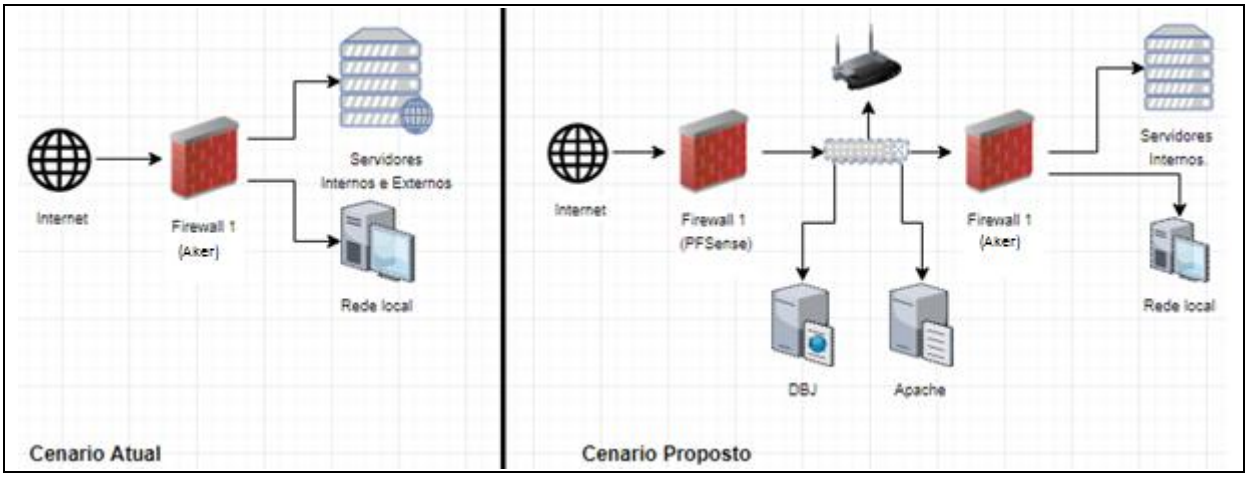


Fonte: Elaborado pelo autor (2018)

4.6 RESULTADOS

Com a implantação da zona DMZ, a melhoria na segurança da rede de computadores foi significativa, baseando-se no cenário atual versus cenário proposto (Figura 10), é possível notar que caso haja a intenção de invasão no ambiente de redes, o *hacker* terá que ultrapassar a primeira e segunda camada dos *firewalls*, para, na sequência, chegar à um servidor que contenha informações importante para empresa. Assim, a área atual que já é segura, foi reforçada com a utilização do segundo *firewall*. A mudança dos servidores que promovem acesso liberado para usuários externos à rede DMZ, também influenciou na qualidade da segurança, deixando a rede interna sem vulnerabilidades e muito mais confiável.

Figura 10 – Cenários



Fonte: Elaborado pelo autor (2018)

A Tabela 1 demonstra as melhorias que foram realizadas no ambiente de teste, tendo como base o cenário atual versus cenário proposto, assim, transformando um ambiente que já é considerado seguro, em um ambiente com dupla segurança de filtros.

Tabela 1 – Cenário atual x cenário proposto.

Cenário Atual	**Cenário Proposto**
Acessos externos dentro da rede local	Acessos externos, somente na DMZ
Uma VLAN para todos os servidores.	Uma rede específica somente para servidores com acesso externo.
VLAN única, risco de infecção de todo os servidores e com acesso interno risco de ser transmitido para máquinas locais.	Como é uma rede separada das demais, servidores que correm risco, são apenas os de acesso externo, tendo uma maior facilidade de contenção.
Roubo de informações do coração da empresa como desenhos de engenharia, contabilidade de fornecedor e clientes.	A criação da DMZ deixa os arquivos compartilhados fora do acesso local.
Único *Firewall*, se invadido o invasor estará na rede local com acesso a toda a rede.	Dois *Firewalls* de fabricantes diferentes, aumentando a dificuldade de invasões.
Há permissões de entrada externa para alguns servidores dentro da rede de servidores.	Não há nenhuma permissão de entrada externa na rede local ou de servidores usados internamente, apenas na rede DMZ.

Fonte: Elaborado pelo autor (2018).

O papel dos administradores de TI e Segurança da Informação é entender e prever as falhas humanas detectadas no processo de controle de vulnerabilidade e riscos e trata-las de forma proativa, assim como estar preparados para prováveis ocorrências e responder a elas no menor tempo possível, evitando assim, perda de capital. (ARAÚJO, 2013)

5 CONCLUSÕES/CONSIDERAÇÕES FINAIS

Com este artigo foi possível demonstrar a importância e vantagens da implantação de uma DMZ com a utilização dois *firewalls*, sendo os mesmos de fabricante diferentes, que se implantados na estrutura da empresa, objeto de análise, poderá agregar na segurança da mesma.

A inserção do segundo *firewall (PFSense),* um *software* livre, mostra que a melhora na infraestrutura de segurança não teve custo adicional, acrescentando a ela uma segunda camada de filtros que, conciliados ao primeiro (Aker), torna a rede ainda mais segura.

A alteração da estrutura do cenário atual, que resultou na inclusão dos servidores de uso público (acessos externos), para o interior da DMZ, fornece à infraestrutura de rede uma maior segurança para sua rede local, já que o usuário externo, não realiza seu acesso junto a mesma. Com a configuração das regras dos *firewalls é* possível bloquear por completo as conexões externas da rede, tornando possível, apenas, o acesso na área DMZ. Assim, se esses servidores forem afetados por *hacker*, ou seja, se o primeiro *firewall* for burlado, através de acessos externos ou compartilhamento de arquivos, apenas uma pequena área será afetada, tendo ainda como reforço o segundo *firewall*, que protege a rede local onde os arquivos considerados mais importantes ficam armazenados.

REFERÊNCIAS

AKER. **Informações sobre a Aker Security Solutions.** 2015. Disponível em: <http://www.aker.com.br>. Acesso em: 21 ago. 2018.

ALECRIM, E. **O que é um *Firewall*?** Conceitos, tipos e arquitetura. Disponível em: <https://www.infowester.com/firewall.php>. 2013. Acesso em: 4 ago. 2018.

ARAÚJO, R. O. **Ameaças Internas:** Desafios da segurança e impactos causados por colaboradores no ambiente de TI. 2013. Universidade Tecnológica Federal do Paraná, Medianeira, Paraná.

BASSO, E. D. **Análise de soluções UTM e ameaças digitais.** 2015. Universidade Tecnológica Federal do Paraná, Curitiba, Paraná.

DANTAS, L. M. **Segurança da Informação:** Uma abordagem focada em gestão de riscos. Olinda, Pernambuco. Livro Rápido, 2011.

DRAKE, N. **Análise de Sistema Operacional:** PFSense**.** Disponível em: <https://unixuniverse.com.br/bsd/analise-do-pfsense>. 2018. Acesso em: 25 jul. 2018.

FOROUZAN, B. A. **Comunicação de Dados e Redes de Computadores.** 4. ed. São Paulo: AMGH, 2009.

FOROUZAN, B. A. **Protocolo TCP/IP**. 3 ed. São Paulo: AMGH, 2009.

HEINZELMANN, O. R. **Plataforma de Computação em Nuvem Com Serviços Orquestrados**. Universidade Federal do Rio de Janeiro, Rio de Janeiro, 2016.

HELPDIGITAL, **O que é *firewall*? Conceitos, tipos e arquiteturas.** 2017. Disponível em: <http://helpdigitalti.com.br/blog/o-que-e-firewall-conceito-tipos-e-arquiteturas/>. acesso em: 20 ago. 2018.

KOUCH, M. **Uma Proposta de Solução de Gerenciamento de Contabilização Utilizando Nagios e Cacti.** Repositório Digital da Universidade Federal do Rio Grande do Sul, Porto Alegre, 2008.

LAWRIE, B. **Segurança de computadores:** Princípio e Práticas. 2 ed. Rio de Janeiro, Elsevier, 2014.

MAUSER, D. **Certificação Security+**. Rio de Janeiro: Novaterra, 2015.

MAYA, A. **O Que São Redes de Computadores?** 2016. Disponível em: <http://www.alcidesmaya.com.br/blog/o-que-sao-redes-de-computadores>. Acesso em: 12 jul. 2018.

MOREIRA, E. **O que é a Política de Segurança da informação?** 2017. Disponível em: <http://introduceti.com.br/blog/o-que-e-a-politica-de-seguranca-da-informacao-psi>. Acesso em: 10 jul. 2018.

NAVES, M, H. **Segurança de Redes Utilizando IDS's e HoneyPots.** Faculdade Cenecista de Varginha. Varina, Minas Gerais, 2010.

NAKAMURA, T. E **Segurança de redes em ambientes cooperativos.** São Paulo, Novatec, 2007.

PROSDOCIMO, L. W. **Métodos de análise, otimização e verificação do conjunto de regras de um *firewall*.** Universidade Tuiuti do Paraná, Curitiba, Paraná, 2014.

PINHEIROS, S. J. **Redes de Perímetro.** 2004. Disponível em: <https://www.projetoderedes.com.br/artigos/artigo_redes_de_perimetro.php>. Acesso em: 15 jul. 2018.

REIS, M. **Vulnerabilidades:** Blindar completamente a rede é impossível. 2015. Disponível em: <https://www.proof.com.br/blog/vulnerabilidade-de-ti-blindar-completamente-a-rede-e-impossivel>. Acesso em: 03 jul. 2018.

REITER, C. C. **Segurança de Redes.** SENAI, 2008.

SERCOMPE. **Infraestrutura de redes:** entenda o valor desse investimento para sua empresa. 2016. Disponível em: <http://blog.sercompe.com.br/2016/09/29/infraestrutura-de-redes-entenda-o-valor-desse-investimento-para-sua-empresa>. Acesso em: 10 jul. 2018.

SOUZA, H. G. **Proposta Para Solução da Segurança de Redes Escolares:** Importância do *Firewall*. São Paulo, Mococa. Clube dos Autores, 2014.

SOUSA, J.C. **Segurança em redes Linux *Firewall* IPtables.** 2013. Centro Universitário Eniac, Guarulhos, São Paulo.

TANENBAUM. A. S. **Computer Networks.** 4 ed. Prentice Hall, Amsterdam, Holanda. 2002.

TAUPP, F. M.; BEUREN, I. M. **Metodologia da pesquisa aplicável às ciências sociais - como elaborar trabalhos monográficos em contabilidade:** teoria e prática. São Paulo: Atlas, 2003.

VERGARA, S. C. **Projeto e relatórios de pesquisa em administração.** 3 ed. São Paulo: Atlas, 2000.

TEIXEIRA, M. M. **Redes de Computadores:** Da teoria a pratica com *NETKIT*. Rio de Janeiro. Elsevier, 2015.

WILLIAMSON, M. **PFSENSE**. Birmingham, Reino Unido. PACKT 2011.

YIN, R.K. **Estudo de Caso:** planejamento e método. 3. Ed. Porto Alegre: Bookman, 2005.