SEGURANÇA EM REDES: REDE DESMILITARIZADA COM FIREWALL PFSENSE E AKER

ZOREK, Ricardo[1]
ZANINI, Elaine[2]
ricardozdaniel@live.com

RESUMO

Este artigo tem como objetivo desenvolver uma DMZ, com o intuito de aumentar a segurança do ambiente de rede empresarial por meio da implantação da mesma, onde serão transferidos os servidores públicos, assim garantindo uma maior segurança para o ambiente da rede local e justifica-se pelos prejuízos que estas ameaças trazem para tal ambiente, aonde a implantação de ferramentas de segurança dificulta a invasão de *hacker* na rede e diminuem os danos causados nas empresas. 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.

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

1 INTRODUÇÃO

A área de TI (Tecnologia de Informação) está presente em praticamente todas as empresas do mundo, seja de pequeno porte com uma rede *LAN* (*Local Área Network*) com um ou dois computadores ou uma empresa de grande porte, como por exemplos multinacionais com mais de mil dispositivos conectados à rede, com isso a área de segurança em redes é cada vez mais importante e exigente. Segundo Tanenbaum (2002) a segurança em sua maneira mais simples de explicação, se preocupa em garantir que pessoas mal-intencionadas não tenham acesso a documentos e informações.

---

[1] Acadêmico - Faculdade Assis Gurgacz

[2] Docente orientador – Faculdade Assis Gurgacz - Curso de Sistemas de Informação

Existem várias ameaças oriundas da rede mundial de comunicação como os vírus, T*rojan Horse, Backdoors*, etc., aonde todos agridem de alguma maneira a integridade de um computador ou de uma rede de computadores (REITER, 2008).

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

É importante reforçar que o *firewall* não é o único sistema/dispositivo de segurança que uma rede *LAN* (*local área network*) pode ter, existem muitos outros dispositivos que, com trabalho em conjunto são possíveis de oferecer um ambiente seguro e estável, evitando assim, a ocorrência de incidentes (LOPOLDINO, 2008).

O autor Reiter (2008) cita que um componente de segurança que pode ser utilizado em conjunto com o *firewall* é a rede DMZ (zona desmilitarizada), 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.

Baseado no cenário atual de segurança de redes em ambientes corporativos, esse artigo justifica-se pelos prejuízos que estas ameaças trazem para tal ambiente, aonde a implantação de ferramentas de segurança dificulta a invasão de *hacker* na rede e diminuem os danos causados nas empresas.

E desta forma, esse artigo tem como objetivo desenvolver uma DMZ, com o intuito de aumentar a segurança do ambiente de rede empresarial por meio da implantação da mesma, onde serão transferidos os servidores públicos, assim garantindo uma maior segurança para o ambiente da rede local.

Este artigo está dividido em cinco seções, na primeira seção é apresentada a introdução, na segunda seção expõe-se um estudo bibliográfico onde é descrito sobre segurança de informação, *firewall* e DMZ, a terceira seção apresenta a metodologia aplicada nesse artigo, na quarta seção há a exposição dos resultados e discussões bem como, uma demonstração do ambiente de teste e aplicação do trabalho, e, por fim a conclusão final do artigo.

Comentado [EHS1]: Gostei da introdução. Eu normalmente não exijo que se façam referências teóricas nesse parágrafo, no entanto, não há nenhum mal em apresentá-las. Você já as lançou como argumento inicial e está bem estruturado.

Sem alterações na introdução.

2 REVISÃO BIBLIOGRÁFICA

As redes de computadores e os sistemas de gerenciamento se tornam cada vez mais essenciais no mundo empresarial, à medida que as empresas crescem, sua estrutura de redes também fica maior, tornando-se complexo para administrar está grande estrutura de servidores, serviços e usuários, contudo a disponibilidade e a segurança da rede fica indispensável em uma corporação (KOUCH, 2008). Nas próximas seções serão abordados assuntos relacionados a redes de computadores, origem e seus conceitos.

2.1 REDE DE COMPUTADORES: ORIGEM E CONCEITOS

Para Castells (2003) a origem da rede de computadores aconteceu com *ARPA (Advanced Research Projects Agency)*, que foi formado pelo Departamento de Defesa dos Estados Unidos com intuito de melhorar as defesas do país e alcançar superioridade nas tecnologias militares. Para montar essa rede de computadores foi utilizado a comutação de pacotes, onde se verifica a conexão, manda informação e finaliza conexão, interligando três universidades, SRI (*Stanford Research Institute*), Universidade da Califórnia em Santa Barbara e na Universidade de Utah.

Segundo Maya (2016) as redes de computadores são um conjunto 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.

Constitui a rede de computadores os circuitos necessários para conectar todos 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).

Forouzan (2009) comenta que 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. Uma empresa grande precisa de vários equipamentos interligados para assim formar uma rede LAN.

De acordo com Forouzan (2009) as redes e sistemas de comunicação de dados talvez sejam as tecnologias que crescem com maior rapidez em nossa cultura hoje em dia. Uma das consequências deste crescimento é um aumento surpreendente no número de profissões em que se utiliza a tecnologia, é assim a garantia da funcionalidade da TI é essencial para o êxito na carreira de um bom profissional e o crescimento das empresas.

Já nas redes corporativas a infraestrutura de rede é o ambiente encarregado por conectar e sustentar todos equipamentos de tecnologia da empresa, desde os computadores e servidores

até mesmo máquinas de produção, permitindo que interligue toda empresa e que os colaboradores tenham acesso ao sistema e recursos de TI (SERCOMPE, 2016).

A seguir será abordado o tema sobre segurança de redes que apresenta uma grande importância para um desempenho satisfatório em uma rede de computadores.

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 etc. Ainda para o mesmo autor, a segurança de rede é uma combinação de múltiplas camadas de defesa a fim de proteger o uso e integridade das conexões e 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 para Lawrie (2014) é separada em três objetivos que são fundamentais para segurança de redes.

- Confidencialidade de dados: Garante que dados privados e confidencias não fiquem acessíveis à indivíduos que não são autorizados. Proporcionado aos responsáveis que controlem quaisquer informações coletadas e/ou armazenadas.
- Integridade: Garante que dados sejam modificados somente da maneira especificada e autorizada, e que, os sistemas desempenhem suas funções predefinidas, sem modificações indesejadas.
- Disponibilidade: Garante que o sistema e rede funcionem prontamente e que não ocorra indisponibilidade ao usuário autorizado.

Na seção seguinte será explanado o tema que aborda as políticas de segurança, que se fazem necessárias em uma empresa para o controle e a segurança da infraestrutura e seus dados.

2.3 POLITICA DE SEGURANÇA

Para Moreira (2017) uma empresa que se baseia em meios digitais para fazer o seu trabalho, precisa lidar com crescimento da estrutura de TI, para que essas ações tenham êxito, o componente que deve ser priorizado é a segurança para que não ocorram problemas e nem

perca de dados, para tanto, é necessário que se tenha uma política de segurança planejada e, cumprida por todos os responsáveis.

Segundo Dantas (2011) a política de segurança é um documento que estabelece regras, valores, comprometimento, requisitos e responsabilidades sobre o que deve ser feito para alcançar aquele padrão desejado de proteção das informações e dados, sendo basicamente um manual de procedimentos que reproduz como os recursos de TI da empresa devem ser utilizados e protegidos.

Depois de expostos alguns conceitos sobre a importância das políticas de segurança, o próximo tópico está relacionado a vulnerabilidades existentes, possíveis ameaças em redes de computadores e qual contramedida pode ser aplicada.

2.4 VULNERABILIDADE DE REDE: AMEAÇAS, ATAQUES E CONTRAMEDIDAS

De acordo com Reis (2015) todas as empresas do mundo sofrem com milhares de vulnerabilidades que podem ser exploradas por *hackers*, embora pareça ser algo assustador para usuários, para um profissional de TI, é uma realidade do seu dia a dia de trabalho. Na verdade, é impossível dizer que não se tenha nenhuma vulnerabilidade de TI nas empresas, não importa o quanto seja gasto em ferramentas para impedir os ataques, sempre existirá algum serviço, ou um usuário dessa rede que possa fazer algo que deprecie as proteções.

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. Ataque de rede é qualquer modo específico usado para explorar uma vulnerabilidade de rede (TEIXEIRA, 2015).

Os ataques mais comuns nas redes de corporações parte de *hackers* que utilizam ferramentas e softwares não desejados para auxiliar nos seus planos de ataques, que são chamados de *malware* alguns exemplos são: vírus, *worms, trojans, phishing, spam, rootkits, sniffers,* etc (REITER, 2008).

Para evitar esse tipo de ataques, a equipe de TI da empresa deve realizar contramedidas, que é um passo dado antes de ser invadido ou atacado, 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 f*irewall* na tradução do inglês é um “muro de fogo” ou “porta corta fogo”, ou seja, uma barreira para evitar a propagação de incêndios, mas na realidade é um recurso primordial em uma rede empresarial, nenhum administrador de redes pode deixar seus servidores, computadores e usuários sem esse recurso de segurança.

De acordo com Souza (2010) 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 a mais para a rede local e dificultando a exploração de vulnerabilidade na rede por pessoas mal-intencionadas.

Comentado [EHS2]: Dá uma revisada na estrutura do parágrafo: “... ao tamanho da infraestrutura, grau de dificuldade..”???

2.4.1.1 Tipos de *firewall*

O trabalho de um *firewall* pode ser realizado de várias maneiras, o que define a metodologia que vai ser utilizada são os fatores de qual é a necessidade da empresa e os critérios do administrador, é por esse motivo que podemos encontrar mais de um tipo de *firewall* (HELPDIGITAL, 2017).

- 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 internet que irão prover os serviços solicitados.
- *Firewall* 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.

2.4.2 Arquitetura de *Firewall*

As arquiteturas clássicas do *firewall* são:

- *Dual-homed host architecture:* É a arquitetura (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 é obrigado 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, comisso não ocorre na arquitetura *screened subnet*. a DMZ, que é uma zona de confinamento entre a rede externa e a rede interna, que 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 foi criado no Brasil (agora denominada Ogasec), em Brasília e atua em todo território brasileiro e no exterior, foi fundada em 1997 com uma equipe especializada na parte de segurança.

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

O *firewall* roda sobre o sistema operacional Fedora, devido ao fato desse sistema operacional ser gratuito, tem fácil acesso e é possível encontrar suas versões de download na internet, porém o AKER é um software que funciona através de licença, sendo necessário fazer aquisição para uso (AKER, 2015).

AKER *Security Solutions*, fabricante de soluções de segurança da informação, é a primeira empresa brasileira a disponibilizar produtos e serviços que garantem a máxima

proteção dos dados. Oferece soluções como: *firewall, antispam,* VPN *(virtual private network*), filtro de conteúdo e monitoramento remoto (BASSO, 2015).

2.4.4 Pfsense

Drake (2018) comenta que o projeto PFSENSE foi criado na metade de setembro de 2004 por Chris Buechler e Scott Ullrich. Chris foi um contribuinte dedicado de códigos por muito tempo do projeto M0n0wall, o que PFSENSE tem de diferencial é que seu foco desde o princípio foi a funcionalidade em qualquer dispositivo que seja possível a instalação de um sistema operacional, diferente do projeto que trabalhava antes que era focado somente em *appliances*.

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

Para Heinzelmann (2016) a finalidade do PFSENSE vai muito além de *firewall* comum, podendo trabalhar com VPN`s, servidor *proxy*, autenticação de usuário, Servidor DNS (*Domain Name System*), Servidor DHCP (*Dynamic Host Configuration Protocol*), IDS (Sistema de Detecção de Intruso) entre outras funcionalidades.

Para Williamson (2011) o PFSENSE é um sistema operacional que foi baseado em FreeBSD que origina do Unix, assim trazendo 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 de onde ele integra.

O próximo tópico está relacionado à 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) ainda afirma que uma a área desmilitarizada corresponde ao segmento de uma rede parcialmente protegida, que está localiza entre a rede interna da empresa e a rede externa (internet), nela será localizada todos os serviços de acesso públicos 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 cuja o acesso à internet é necessário, a lógica de separar este servidores se deve pelo fato que se houver uma invasão, serão por meio de tais servidores, e com isso o acesso a rede internar será facilitado já que este se encontra dentro da rede local.

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

Comentado [EHS3]: Todos os elementos que circundam o alvo do trabalho estão abordados aqui. As bibliografias escolhidas são de procedência. Vejo oportunidade apenas de se fazer uma revisão de ordem gramatical e semântica. Nada tão relevante, mas importante.

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

A seguir serão apresentados os procedimentos metodológicos da pesquisa, bem como as ferramentas que serão utilizadas para atingir o objetivo proposto.

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, um método que atinge tudo, técnica de coleta de dados, planejamento e análise dos mesmos. As informações geradas a partir de um estudo de caso não são similares a resultados obtidos a partir de outras pesquisas, estudo de caso, contém informações mais detalhadas e concretas.

A pesquisa é exploratória em busca de ferramentas, a que possa se encaixar no ambiente da empresa. Taupp (2003) destaca que esse tipo de pesquisa é desenvolvido para ter uma visão geral, no caso desse artigo conhecer a ferramentas por completo, como cada ambiente tem particularidade, então a necessidade de fazer um estudo sobre ela nesse local. Para Vergara (2000), as pesquisas exploratórias são realizadas em áreas que existem poucas informações.

A pesquisa é do tipo qualitativa, 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, que já não teria na forma quantitativa. No próximo tópico serão citadas as metodologias usadas para criação e implementação do ambiente.

3.2 PROCEDIMENTOS METODOLÓGICOS

Para esse projeto foi criado um ambiente de teste que é composto de equipamentos físicos e rack de rede, sendo: dois *firewalls* (PFSENSE e AKER), um servidor apache Linux, um switch e um roteador WIFI.

Para o desenvolvimento da pesquisa foi utilizado *firewalls* do tipo interno e arquitetura *Screened subnet architecture. Neste contexto* será realizado testes de funcionalidades de uma área desmilitarizada focando em aumentar a segurança de uma rede já existente no Grupo Mascarello e movendo servidores que há a necessidade de acessos externos para essa rede. Na sequência serão feitos testes e a coleta de informações das melhorias da segurança e da estrutura, visando uma possível implantação na forma definitiva, com autorização da diretoria e responsável pelo TI da empresa.

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

Comentado [EHS4]: Sugiro escrever com outras palavras. Veja que o primeiro parágrafo ficou "Para o desenvolvimento..." e o segundo também...

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 será exposto 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 IP (*Internet Protocol*) fixo dedicado somente para o ambiente de teste.

Para composição da rede foram utilizados os seguintes hardwares:

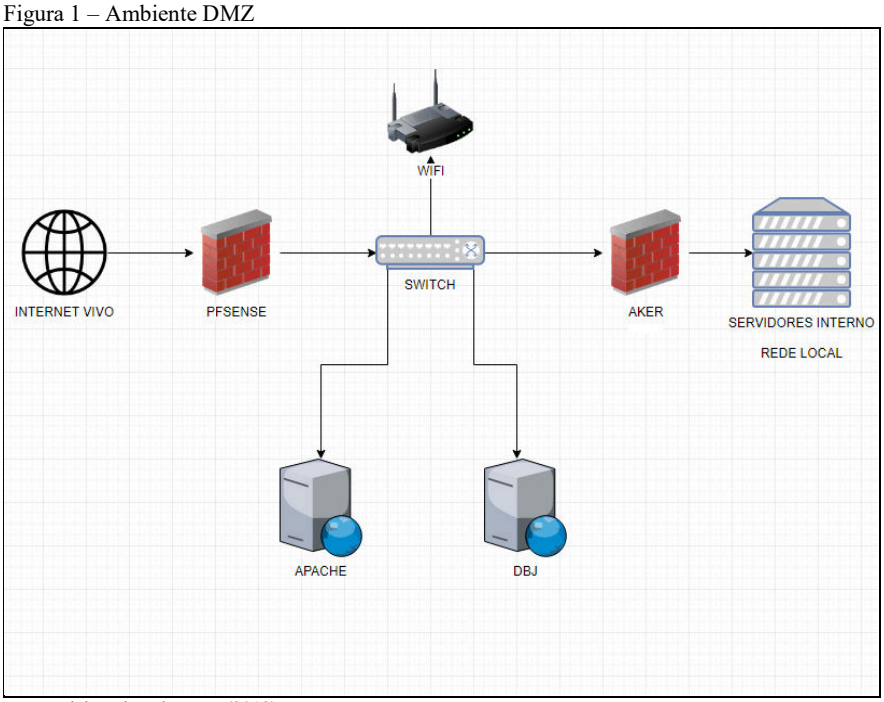
- A instalação do *firewall* PFSENSE foi realizada em uma máquina de configurações: processador I686 c7 1500 MHZ, memória DDR 2 de 512 MB;
- Um s*witch* Edge-cor modelo ECS2000 com 26 portas, sendo 24 de cabo de rede RJ45 e duas de fibras mini GBIC;
- Um servidor DBJ foi estruturado em uma máquina de 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 será mostrado as configurações da rede e de como foi montando o ambiente.

4.2 Configuração da rede

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

Figura 1 – Ambiente DMZ



Fonte: Elaborado pelo autor (2018)

Especificações da rede:

- **INTERNET VIVO:** 177.204.154.12
- **PFSENSE:**
  - **WAN:**177.204.154.12
  - **LAN:** 192.168.100.1
  - **LINK EXTERNO:** http://177.204.154.12/
- **SWITCH:** 192.168.100.248
- **WIFI DMZ:** 192.168.100.249
- **APACHE**
  - **LAN:** 192.168.100.250
  - **LINK EXTERNO:** http://177.204.154.12:8086/
- **DBJ**

- **LAN:** 192.168.100.247
- **LINK EXTERNO:** http://177.204.154.12:8085/Portal

– **AKER**

- **WAN:** 192.168.100.251
- **LAN:** 192.168.0.254

No tópico abaixo 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, 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.

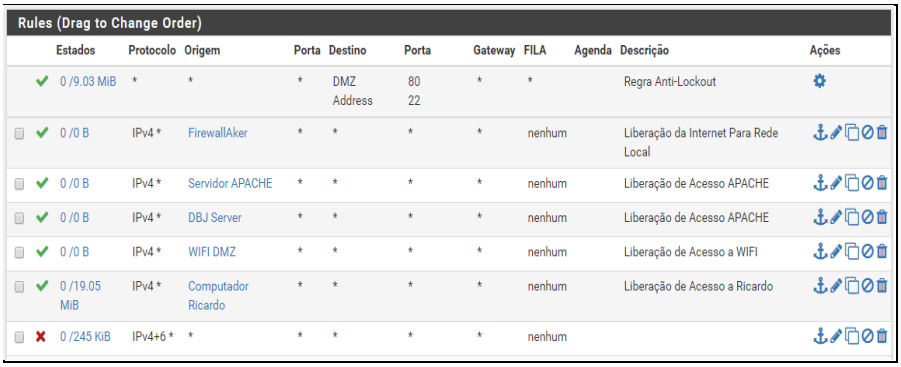
3ª e 4ª regras: São as liberações para internet dos servidores Apache e DBJ.

5ª regra: Para WIFI e o roteador é criado uma VLAN diferente da DMZ, e tudo que estiver conectado nela pode enviar informações para internet, essa regra é utilizado para visitantes, representantes que queiram acesso à internet através de notebook ou celular, para acessos temporário, tendo como intenção não ter acesso a rede local da empresa.

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

7ª regra: Bloqueia tudo que não foi tratado nas regras anteriores.

Figura 2 – Configurações Regras Porta DMZ



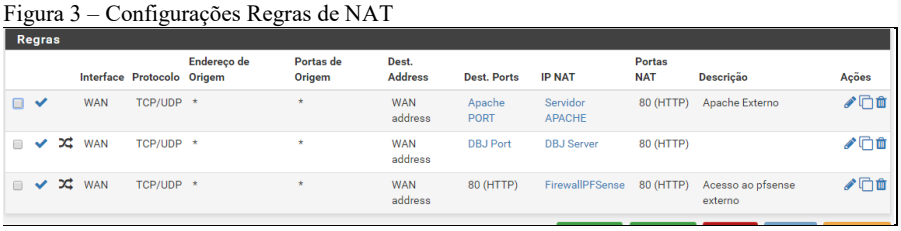
Rules (Drag to Change Order)

	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 NAT (*Network Address Translation*) onde são realizados os redirecionamentos das portas que são acessados externo 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



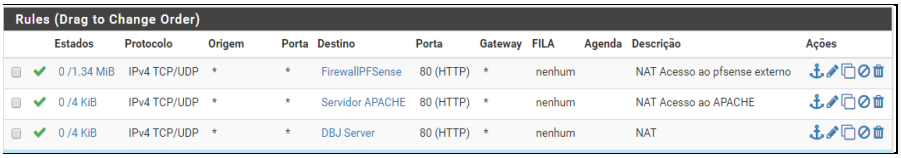
Regras

	Interface	Protocolo	Endereço de Origem	Portas de Origem	Dest. Address	Dest. Ports	IP NAT	Portas NAT	Descrição	Ações
✓	WAN	TCP/UDP	*	*	WAN address	Apache PORT	Servidor APACHE	80 (HTTP)	Apache Externo	
✓	WAN	TCP/UDP	*	*	WAN address	DBJ Port	DBJ Server	80 (HTTP)		
✓	WAN	TCP/UDP	*	*	WAN address	80 (HTTP)	FirewallPFSense	80 (HTTP)	Acesso ao pfsense externo	

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



Rules (Drag to Change Order)

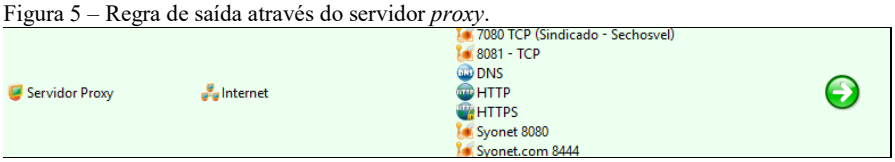
	Estados	Protocolo	Origem	Porta	Destino	Porta	Gateway	FILA	Agenda	Descrição	Ações
☐ ✔	0 /1.34 MiB	IPv4 TCP/UDP	*	*	FirewallPFSense	80 (HTTP)	*	nenhum		NAT Acesso ao pfsense externo	
☐ ✔	0 /4 KiB	IPv4 TCP/UDP	*	*	Servidor APACHE	80 (HTTP)	*	nenhum		NAT Acesso ao APACHE	
☐ ✔	0 /4 KiB	IPv4 TCP/UDP	*	*	DBJ Server	80 (HTTP)	*	nenhum		NAT	

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 especificas utilizadas na empresa.

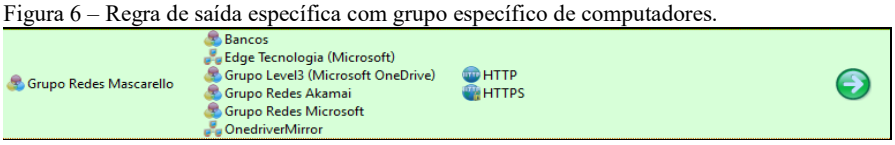
Figura 5 – Regra de saída através do servidor *proxy*.



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)

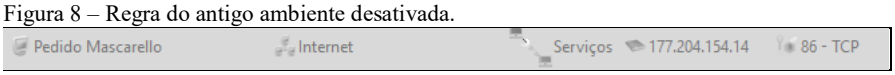
A regra apresentada na Figura 7 é a que realiza o bloqueio total das conexões que não se encaixam nas regras apresentadas anteriormente, ou seja, não conseguem sair ou entrar no *firewall*.

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.



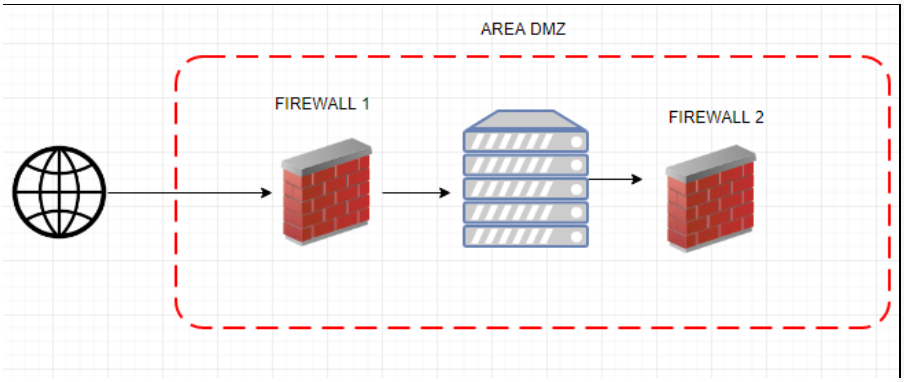
Fonte: Elaborado pelo autor (2018)

4.5 Zona Desmilitarizada

Vamos mexer neste paragrafo juntos....

A DMZ é composta por dois *firewalls* e seus servidores que ficam entre eles, o *firewall* um fica responsável por pela DMZ, onde ele vai ter as regras que permitem os acessos externos e matem a segurança dessa zona, esses *firewall* foram movido para essa parte pois possuem tanto acesso externo e isso, do jeito que estava alocado tornava toda a rede vulnerável, agora caso seja feito algum ataque ou invasão, o indivíduo ficara entre os dois *firewall* e assim dificultando o acesso a rede local, já que no caso teria a outro *firewall*, o segundo *firewall* não permite a entrada de nada, apenas deixa que rede local sai para internet caso se enquadre nas regras que foi realizada.

Figura 9 – DMZ

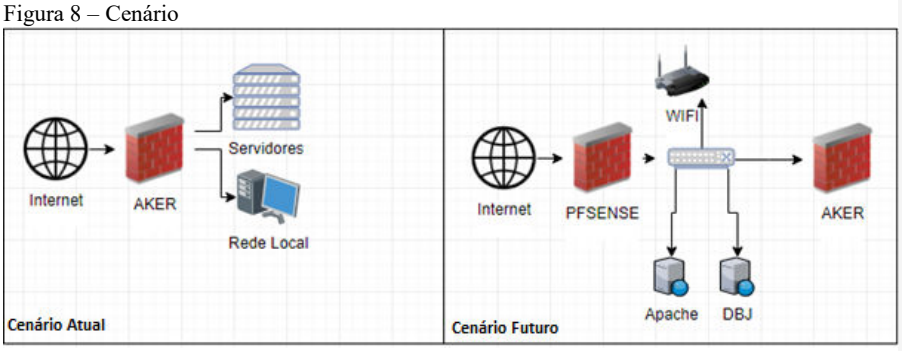


Fonte: Elaborado pelo autor (2018)

4.6 Comparação e resultados

Com a implantação da zona DMZ, a melhoria na segurança da rede de computadores é significativa, baseando-se no ambiente atual com o futuro como demonstra a Figura 8, assim podemos ver que se houver a intenção de invasão no ambiente de redes o hacker teria que passar a primeira e a segunda camada de firewalls, para chegar a um servidor que contenha informações importante para empresa, assim a área atual que já é segura, tornaria isso mais difícil de ser invadido com segundo *firewall*. E também a mudança dos servidores que tem acesso liberado para usuários externos para dentro da rede DMZ, deste modo deixando a rede interna sem vulnerabilidades e assim muito mais confiável.

Figura 8 – Cenário



Fonte: Elaborado pelo autor (2018)

Na Tabela 1 é demostrado melhorias que foi identificado no ambiente de teste tendo base com o ambiente atual e o futuro cenário, assim transformando um ambiente que já é considerado seguro, para um melhoramento de suas estruturas.

Tabela 1 – Cenário atual e futuro.

Cenário Atual	**Cenário Futuro**
Acessos externos dentro da rede local	Acessos Externos, somente na DMZ
Uma VLAN para todos os servidores.	Uma rede especificas 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, e 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).

5 CONCLUSÕES/CONSIDERAÇÕES FINAIS

REFERÊNCIAS

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

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

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

CASTELLS, M. **A Galáxia Internet:** reflexões sobre a internet, negócios e a sociedade. Rio de Janeiro: ZAHAR, 2003.

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

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

LEOPOLDINO, S. A. REITER, C. C. **Segurança de Redes.** SENAI, 2008.

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

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

MOREIRA, E. **O que é a Política de Segurança da informação?** Disponível em: **<**http://introduceti.com.br/blog/o-que-e-a-politica-de-seguranca-da-informacao-psi>. 2017. 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.** Disponível em: <https://www.projetoderedes.com.br/artigos/artigo_redes_de_perimetro.php>. 2004. Acesso em: 15 jul. 2018.

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

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

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

SOUSA, J.C. **Segurança em redes Linux Firewall IPtables** Centro Universitário Eniac, Guarulhos, São Paulo, 2009.

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.

APÊNDICES

Documento complementar elaborado pelo autor do trabalho. **(Caso seja necessário).**

ANEXOS

Documentos não elaborados pelo autor, mas utilizados para fundamentação, comprovação ou ilustração. **(Caso seja necessário).**

INFORMAÇÕES QUANTO A FORMATAÇÃO DO TEXTO

Para o texto, orienta-se a utilização de fonte tipo Times New Roman ou Arial, tamanho 12 para texto e paginação, tamanho menor (10) para citações diretas com mais de 3 linhas, legenda das ilustrações e tabelas, resumo, notas de rodapé e nota da folha de rosto (natureza do trabalho).

MARGENS

a) margem superior de 3 cm;
b) margem inferior de 2 cm;
c) margem esquerda de 3 cm;
d) margem direita de 2 cm

Todo texto deve ser digitado com espaço 1,5 de entrelinhas. O espaçamento de entrelinhas simples, porém, deverá ser utilizado nas citações diretas de mais de três linhas, no título caso com mais de uma linha, nas notas, nas referências, nas legendas das ilustrações e tabelas, na nota descritiva da natureza do trabalho (nota de folha de rosto) e resumos.

A numeração da página será no canto superior direito conforme este modelo.

O artigo deverá conter um mínimo de 10 páginas e, no máximo, 20 páginas (Da introdução do trabalho até as considerações finais).